



ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

**“DISEÑO DE UN SISTEMA DE ALTA DISPONIBILIDAD PARA
ACCESO A INTERNET ORIENTADO A PYMEs”**

INFORME DE MATERIA INTEGRADORA

Previo a la obtención del Título de:

**INGENIERO/A EN ELECTRÓNICA Y
TELECOMUNICACIONES**

ESCARLETH KATHERINE RUEDA HORMAZA

GABRIEL RAÚL ANDRADE MORA

GUAYAQUIL – ECUADOR

AÑO: 2017

AGRADECIMIENTOS

Una flor hoy brota en mi árbol, agradezco por ella a Dios por darme la constancia, mi familia por el apoyo, mi tutor de proyecto Ing. Cesar Yépez por sus conocimientos y sin duda alguna a mis amigos por todo el tiempo compartido conmigo.

Escarleth Katherine Rueda Hormaza

Agradezco a Dios por darme fuerza y salud necesaria para lograr esta meta, sin el nada de esto sería posible.

A mis padres por ser el apoyo incondicional en mi vida, por sus consejos y por la motivación aportada a lo largo de la carrera.

A mi tutor de proyecto el Ing. Cesar Yépez por sus conocimientos y ayuda brindada en el tema.

A mis amigos por compartir esta etapa de mi vida.

Gabriel Raúl Andrade Mora

DEDICATORIA

El presente proyecto es dedicado a Dios, a nuestras familias y a todas las personas que han sido un apoyo durante esta etapa de nuestra vida.

TRIBUNAL DE EVALUACIÓN

.....
Ing. César Eduardo Yépez Flores

PROFESOR EVALUADOR

.....
Dr. Germán Ricardo Vargas López

PROFESOR EVALUADOR

DECLARACIÓN EXPRESA

"La responsabilidad y la autoría del contenido de este Trabajo de Titulación, nos corresponde exclusivamente; y damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

.....
Escarleth Katherine Rueda Hormaza

.....
Gabriel Raúl Andrade Mora

RESUMEN

En Ecuador actualmente las PYMEs (conjunto de pequeñas y medianas empresas) forman parte del sector económico siendo una gran fuente de generación de empleo en el país. Debido a que constantemente están en un avance productivo requieren de una disponibilidad constante de su información, ingresos, productividad, entre otros. En estos últimos años el internet ha llegado convertirse en una herramienta imprescindible para la organización de una empresa ofreciendo diferentes funciones como: publicitaria, administración, respaldo de información, entre otras. Por esta razón es necesario mantener un acceso a internet continuo dentro de las PYMEs.

No contar con este acceso continuo a internet en una empresa, produce pérdidas de productividad y de sus ingresos, por esta razón se diseñara un sistema de alta disponibilidad para acceso a internet orientado a PYMEs. El diseño propuesto se basa en utilizar dos Proveedores de Internet (ISP) diferentes una red LAN en la cual se utiliza el balanceador de carga, el cual mediante el uso de algoritmos de balanceo distribuirá el tráfico de la red LAN entre los dos ISP mejorando así el uso del ancho de banda ofreciendo un servicio de alta disponibilidad.

De esta manera se plantean tres escenarios más comunes para la administración del ancho de banda dentro de una red LAN, en los cuales se utilizan algoritmos de balanceo. El diseño planteado constituye una buena alternativa, no solo por su diseño sencillo sino por los beneficios de monitoreo y control en tiempo real que ofrecen los equipos. Para comprobar que el sistema planteado brinde alta disponibilidad, la red propuesta fue implementada y sometida a prueba de fallo (Fail-over); en donde se logró observar el funcionamiento de alta disponibilidad.

ÍNDICE GENERAL

AGRADECIMIENTOS	ii
DEDICATORIA	iii
TRIBUNAL DE EVALUACIÓN.....	iv
DECLARACIÓN EXPRESA.....	v
RESUMEN.....	vi
ÍNDICE GENERAL	vii
CAPÍTULO 1.....	1
1. PLANTEAMIENTO DEL PROBLEMA.	1
1.1 Descripción del problema.....	1
1.2 Justificación del problema.....	1
1.3 Objetivos.....	2
1.3.1 General.....	2
1.3.2 Específicos.....	2
1.4 Metodología.	2
1.5 Resultados esperados.	3
1.6 Elementos diferenciadores.....	3
CAPÍTULO 2.....	5
2. DEFINICIÓN DE UN SISTEMA DE ALTA DISPONIBILIDAD.	5
2.1 Disponibilidad: Conceptos básicos.	5
2.2 Proveedores de servicio de internet.....	8
2.3 Balanceador de carga.....	9

2.4 Algoritmos de balanceo.....	11
CAPÍTULO 3.....	13
3. CONFIGURACIÓN DEL BALANCEADOR DE CARGA.....	13
3.1 Diseño de la red.....	13
3.2 Configuración del router para tráfico de paquetes.....	14
3.2.1 Configuración de interfaces.....	15
3.2.2 Configuración del NAT.....	17
3.2.3 Configuración del Servidor DNS.....	19
3.3 Configuración de interfaces del balanceador de carga.....	24
3.3.1 Configuración de las interfaces LAN.....	25
3.3.2 Configuración de las interfaces WAN.....	27
3.4 Configuración del servidor DNS.....	28
3.5 Configuración Calidad de servicio (Qos).....	29
3.6 Configuración Firewall.....	30
3.7 Configuración de reglas de balanceo.....	32
3.7.1 Primer escenario.....	32
3.7.2 Segundo escenario.....	34
3.7.3 Tercer Escenario.....	36
CAPITULO 4.....	38
4. ANÁLISIS DE TRÁFICO Y RESULTADOS.....	38
4.1 Primer escenario.....	38
4.2 Segundo escenario.....	41
4.3 Tercer Escenario.....	45

CONCLUSIONES RECOMENDACIONES	48
BIBLIOGRAFÍA.....	49
ANEXOS.....	50

ÍNDICE DE FIGURAS

Figura 2.1 Tiempo de Inactividad. [1].....	6
Figura 1.2 Diseño de la red propuesta.....	12
Figura 2.1 Tabla de interfaces del Router RB 750.....	15
Figura 3.2 Dirección IP privada interfaz 2-WAN.....	16
Figura 3.3 Dirección IP privada interfaz 4-WAN2.....	16
Figura 3.4 Interfaces de Router RB.	17
Figura 3.6 Habilitación Masquerade.	18
Figura 3.5 Configuración del NAT en 2-WAN1.	18
Figura 3.8 Habilitación Masquerade.	18
Figura 3.7 Configuración del NAT en 4-WAN2.	18
Figura 3.9 Configuración del NAT en router RB 750.....	19
Figura 3.10 Direcciones IP pública de los servidores DNS.....	19
Figura 3.11 Configuración de marca.....	20
Figura 3.12 Configuración de marca.....	20
Figura 3.14 Configuración de marca.....	20
Figura 3.13 Configuración de marca.....	20
Figura 3.15 Configuración de marca del tráfico.	21
Figura 3.16 Direccionamiento ISP-1.	21
Figura 3.17 Direccionamiento ISP-2.	22
Figura 3.18 Direccionamiento.	22
Figura 3.19 Límite de ancho de banda en interfaz WAN1.	23
Figura 3.20 Límite de ancho de banda en interfaz WAN2.	23
Figura 3.21 Límite de ancho de banda de las interfaces del router.	24
Figura 3.22 Página de inicio del administrador web del balanceador.	25
Figura 3.23 Configuración de la dirección IP del balanceador.....	25
Figura 3.24 Configuración del servidor DHCP del balanceador.....	26
Figura 3.25 Configuración de la interfaz WAN.....	27

Figura 3.26 Configuración de la interfaz WAN2.	28
Figura 3.27 Configuración de las direcciones IP de los servidores DNS.	28
Figura 3.28 Configuración del chequeo de salud de los WAN.	29
Figura 3.29 Configuración de la prioridad de las aplicaciones.	29
Figura 3.30 Configuración del bloqueo al sitio web el universo.	30
Figura 3.31 Configuración del bloqueo al sitio web de Facebook.	31
Figura 3.32 Reglas de balanceo aplicadas al balanceador.	31
Figura 3.33 Configuración para prevención de ataques DoS	31
Figura 3.34 Configuración del algoritmo de distribución por peso.	33
Figura 3.35 Configuración del algoritmo de prioridad para la PC1.	35
Figura 3.36 Configuración del algoritmo de prioridad para la PC2.	36
Figura 3.37 Configuración del enlace WAN2 como backup.	37
Figura 3.38 Configuración del algoritmo de prioridad estableciendo el enlace WAN2 como Backup.	37
Figura 4.1 Tráfico de descarga del enlace WAN1 en el escenario 1.	38
Figura 4.2 Tráfico de descarga del enlace WAN2 en el escenario 1.	39
Figura 4.3 Tráfico total de descarga en el escenario 1.	39
Figura 4.4 Tráfico de descarga del enlace WAN1 en el escenario 1 realizando pruebas de error.	40
Figura 4.5 Tráfico de descarga del enlace WAN2 en el escenario 1 realizando pruebas de error.	40
Figura 4.6 Tráfico de descarga total en el escenario 1 realizando pruebas de error.	41
Figura 4.7 Tráfico de descarga del enlace WAN1 en el escenario 2 para PC1.	42
Figura 4.8 Tráfico de descarga del enlace WAN2 en el escenario 2 para PC1.	42
Figura 4.9 Tráfico de descarga total en el escenario 2 para PC1.	43
Figura 4.10 Tráfico de descarga del enlace WAN2 en el escenario 2 para PC2.	44

Figura 4.11 Tráfico de descarga del enlace WAN1 en el escenario 2 para PC2.	44
Figura 4.12 Tráfico de descarga total en el escenario 2 para PC2.	45
Figura 4.13 Enlace WAN2 en estado de Standby.....	45
Figura 4.14 Enlace WAN2 en estado conectado.	46
Figura 4.15 Tráfico de descarga del enlace WAN1 en el escenario 3.	46
Figura 4.16 Tráfico de descarga del enlace WAN2 en el escenario 3.	47
Figura 4.17 Tráfico de descarga total en el escenario 3.	47

ÍNDICE DE TABLAS

Tabla 1: Niveles de Disponibilidad. [2]	8
Tabla 2: Especificaciones del Router RB 750. [6]	14
Tabla 3: Direcciones Públicas ISP1	15
Tabla 4: Direcciones Públicas ISP2	16
Tabla 5: Direcciones IP reservadas para la red LAN.	26
Tabla 6: Asignacion de peso a los enlaces WAN.....	33
Tabla 7: Enlaces WAN primario y secundario de cada host	35

CAPÍTULO 1

1. PLANTEAMIENTO DEL PROBLEMA.

1.1 Descripción del problema.

Los conjuntos de pequeñas y medianas empresas (PYMES) en la actualidad son una fuente de generación de empleo y un medio para ofrecer servicios en mercados de menor tamaño.

Actualmente las empresas requieren una conexión constante a internet para mantener así todos sus servicios disponibles; la falta de capital o el diseño incorrecto de sus infraestructuras de redes lo impiden; por lo tanto se propone una alternativa para ofrecer condiciones de alta disponibilidad de acceso a internet para PYMES mediante el diseño de una red acorde a las necesidades prioritarias que requiere la empresa.

1.2 Justificación del problema.

Las PYMES se encuentran en todas las áreas económicas siendo la base del desarrollo social de un país, por esta razón es una de las principales fuentes de riqueza y empleo del país.

Hoy en día el internet se ha convertido en una herramienta potencial para las empresas ofreciendo diferentes funciones como: publicitaria, administración, respaldo de información, entre otras.

No contar con un acceso continuo al internet en las PYMES conduce a pérdidas de productividad y de ingresos, dañando así las relaciones con los clientes. Por esta razón es de vital importancia implementar una alternativa que ofrezca condiciones de alta disponibilidad de acceso a internet.

1.3 Objetivos.

1.3.1 General.

Ofrecer condiciones de alta disponibilidad de acceso a internet para PYMEs.

1.3.2 Específicos.

- Resolver o aumentar la disponibilidad de acceso a internet a PYMEs.
- Balancear el tráfico para asegurar alta disponibilidad.
- Monitorear y Controlar el uso de ancho de banda de los usuarios en tiempo real.

1.4 Metodología.

Para llevar acabo los objetivos planteados en este proyecto es necesario conocer previamente los criterios y necesidades de la empresa donde se implementará esta solución.

Uno de los criterios que se deberá definir es la dimensión de la red, para el respectivo caso de estudio solo se conectarán 2 computadoras (PCs) en la red de área local (Local Area Network -LAN), se deberá contar con dos proveedores de servicio de internet (ISP) para evitar una caída de servicio perceptible para el usuario. Para administrar el ancho de Banda se utilizará un balanceador de carga PEPLINK BALANCE 310 el cual dividirá el trabajo entre los dos ISP conectados.

La metodología que se utilizará en este proyecto es de acuerdo a la ejecución de las actividades descritas a continuación:

- Diseñar un diagrama esquemático utilizando dos ISPs para aumentar la disponibilidad del servicio de internet a usuarios.

- Configurar un balanceador de carga existente en el mercado, definiendo reglas de balanceo de tráfico, habilitando cortafuegos (Firewall) y estableciendo calidad de servicio (QoS) para los usuarios de la red.
- Utilizar una interfaz para el monitoreo del tráfico consumido por usuarios de la red.

1.5 Resultados esperados.

Utilizando este diseño se espera brindar una arquitectura empresarial eficiente que mantenga acceso continuo a internet y brinde un concepto de alta disponibilidad, ofreciendo los siguientes beneficios:

- Mejorar el uso del ancho de Banda: Administración adecuada del acceso de ancho de banda de los host de la red LAN
- Tolerancia a Fallos: Si falla el acceso a internet de uno de los ISP, continúa automáticamente la conexión utilizando exclusivamente la conexión restante.
- Balanceo de Carga: Se administra el acceso a internet para los host de la red LAN mediante algoritmos de balanceo.

1.6 Elementos diferenciadores.

La existencia de nuevos mercados ha permitido que aumente la competitividad entre las empresas y exige una mayor optimización de ellas, por lo cual es importante que se enfoquen en las operaciones claves que le permitan ser más productivas y rentables como es mantener conectividad.

Este proyecto da importancia al gran reto que tienen las PYMES el cual es adaptarse al rápido cambio tecnológico logrando aprovechar las ventajas de las nuevas tecnologías.

El respectivo tema ayuda a las PYMES a desarrollar una alternativa que les ayude a adaptarse al cambio continuo en lo referente a tecnología implementando mecanismos para adaptarse a ellos adecuadamente para poder ofrecer servicios que mejoren el desempeño de los trabajadores; por esta razón resulta necesario implementar una red que permita satisfacer las necesidades del personal y los requerimientos de la empresa, el cual es el objetivo principal de esta investigación.

CAPÍTULO 2

2. DEFINICIÓN DE UN SISTEMA DE ALTA DISPONIBILIDAD.

2.1 Disponibilidad: Conceptos básicos.

Una de las características que se debe tener en cuenta es la medición del grado de disponibilidad de los recursos para el usuario en un sistema durante un tiempo determinado. Debido a la importancia de mantener constante el acceso a internet en las empresas, es necesario entender y aplicar el concepto de alta disponibilidad.

La medida en que un sistema informático es capaz de proveer servicio ininterrumpido a sus usuarios se le denomina "Disponibilidad", actualmente se habla de sistemas que brindan alta disponibilidad. Conceptualmente se define alta disponibilidad al diseño e implementación de un sistema que asegura cierto grado de continuidad operacional durante un periodo de medición dado. [1]

Se denomina también como la habilidad que tienen los usuarios para realizar, alterar o actualizar nuevos trabajos en el sistema [1]; se dice que si un usuario no puede acceder al sistema entonces no está disponible, y el tiempo que el usuario tarda en acceder se denomina tiempo de inactividad el cual se usa para definir cuando un sistema no está disponible.

El tiempo de inactividad se clasifica en planificado y no planificado. El tiempo de inactividad planificado es el tiempo invertido en el mantenimiento del sistema mientras que el tiempo de inactividad no planificado surge de eventos tales como fallos en el hardware, caída por sobrecalentamiento, ruptura física en las conexiones de la red, fallos en el sistema operativo entre otras.

El tiempo de inactividad se clasifica como se muestra en la figura 2.1.

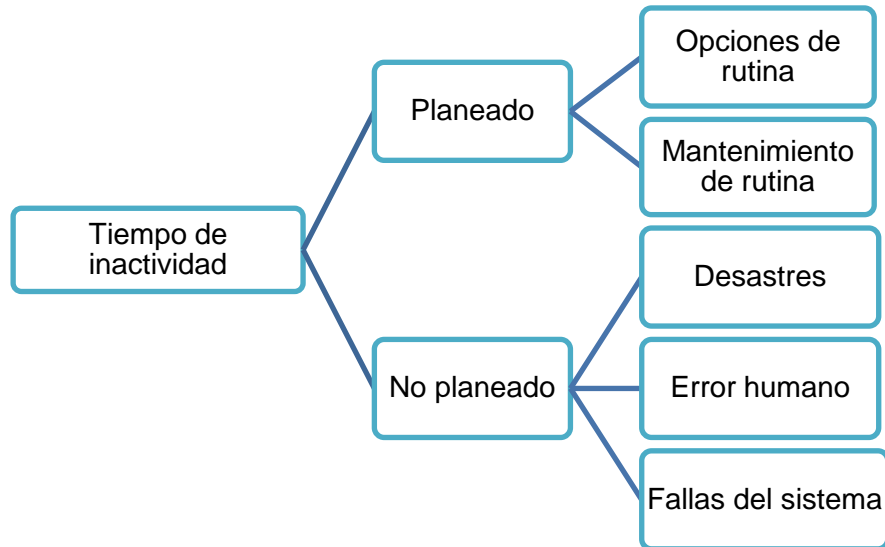


Figura 2.1 Tiempo de Inactividad. [1]

En algunos casos el tiempo de inactividad no planeado no se lo toma en cuenta debido a que se asume incorrectamente que tiene poco o ningún impacto sobre los usuarios. Entonces si solo se toma en cuenta el tiempo de inactividad planeado muchos sistemas pueden indicar que tienen alta disponibilidad lo que da como resultado una disponibilidad continua que implica un servicio sin interrupciones. Se conocen sistemas que si brindan verdaderamente alta disponibilidad pero son comparativamente pocos y caros, conocidos como “Sistemas de misión crítica”. [1]

Se entiende por Sistemas de misión crítica a servidores donde no son tolerables las caídas del servicio debido a que ejecutan operaciones importantes en donde si sufren una caída tendría como resultado un gran impacto en la empresa o institución que dependa de esta información. El correo electrónico, sistemas de administración de inventario de una empresa, banca virtual de los bancos donde se realiza transferencias o bien la aplicación del seguro social (IEES) son ejemplos de aplicaciones de vital importancia.

La disponibilidad continua es conceptualmente diferente a tener Alta disponibilidad, a esta diferencia se denomina tolerancia a fallas, la cual se refiere a un ambiente donde no existe la posibilidad de perder ni un solo minuto de trabajo en producción. A simple vista todas las empresas quisieran tener un sistema con tolerancia a fallas es decir no tener caídas de producción jamás, pero debido a su alto costo queda en sueños y generalmente la solución es implementar un sistema de alta disponibilidad lo que implica que el tiempo de caída debe ser muy corto durante un periodo anual.

La disponibilidad se mide utilizando el índice de disponibilidad, el cual es un porcentaje que se calcula dividiendo el tiempo de disponibilidad del servicio por el tiempo total. Comúnmente se expresa como un porcentaje del tiempo de funcionamiento durante un año.

Todo sistema tiene un Acuerdo de Nivel de Servicio (Service Level Agreement – SLA) el cual define el horario y cuánto tiempo debe estar en línea; para aplicaciones de baja criticidad, el SLA puede ser de 8*5 horas por semana donde no se considera días festivos . En cambio un sistema con mayor criticidad como una red de cajeros tiene un SLA de 24*364 horas al año.

Una vez identificado el SLA se puede proceder a calcular la disponibilidad del sistema

$$\text{Disponibilidad} = [(A - B)/A] * 100\% \quad (2.1) [2]$$

Donde:

A = Horas comprometidas de disponibilidad: 24 x 365 = 8,760 Horas/año.

B = Número de horas fuera de línea (Horas de "caída del sistema" durante el tiempo de disponibilidad comprometido) [2].

Cuando se vaya a realizar un sistema con disponibilidad se requiere previamente conocer cuáles son los objetivos del usuario para conocer qué nivel de

disponibilidad deseada. Las aplicaciones de misión crítica requieren 99,9% o más. Estos valores se catalogan como Alta Disponibilidad (HA, High Availability). La tabla 1 muestra los índices de disponibilidad con su respectiva duración de tiempo de inactividad.

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: Niveles de Disponibilidad. [2]

2.2 Proveedores de servicio de internet.

En este proyecto se requiere aplicar alta disponibilidad al acceso de internet en las PYMES, para lograrlo se utilizará proveedores de internet. Se define Proveedores de internet o ISP por la sigla inglesa de Internet Service Provider a una empresa dedicada a conectar a Internet a los usuarios o las distintas redes que tengan, y dar el mantenimiento necesario para que el acceso funcione correctamente [3]. También ofrecen servicios relacionados, como alojamiento web o registro de dominios entre otros”.

2.3 Balanceador de carga.

Balanceador de carga es un dispositivo que gestiona el trabajo a realizar entre varios elementos de una red, esto se logra mediante algoritmos que dividen de forma más precisa y equitativa el trabajo. Su función varía dependiendo del objetivo principal de la empresa.

En el mercado actual hay balanceadores de carga orientados a servidores web que distribuyen las peticiones de usuarios a través de un clúster de servidores web disponibles, o pueden utilizarse en una red con múltiples enlaces de red de área amplia (Wide area network – WAN) para proporcionar una salida de tráfico con un ancho de banda eficiente y optimizada.

Los algoritmos de balanceo dependen de la función que va a desempeñar el balanceador, los cuales se pueden aplicar en base a las direcciones IP de origen y destino, los puertos u otros factores.

Una de las ventajas que tienen estos equipos es que realizan tareas adicionales como: Comprobar la disponibilidad de los servidores, proteger los equipos de la red de ataques, implementación de calidad de servicio (QoS) y puede cumplir la función de un cortafuegos (firewall).

Se entiende como Calidad de servicio (QoS) al conjunto de tecnologías que brindan la capacidad para administrar tráfico de una red, mejorando la experiencia de usuario en las empresas, oficinas e incluso entornos de red domésticos.

Firewall es un mecanismo que filtra selectivamente el tráfico de datos entre el lado WAN (Internet) y el lado LAN de la red. Puede proteger la red local de posibles ataques de hackers, sitios web ofensivos y / u otros usos inapropiados.[4]

El balanceador de carga aporta los siguientes beneficios:

- Escalabilidad: El balanceador distribuye las peticiones de los usuarios, haciendo que la capacidad global del proceso y servicio crezca.
- Disponibilidad: El balanceador monitoriza el estado de los servidores, aplicaciones y enlaces WAN de forma que si encuentra que uno de estos ha fallado utilizará otro que esté disponible.
- Mantenimiento: Brinda la opción al administrador de dar mantenimiento a un servidor, aplicación o enlace WAN sin que la red se vea afectada
- Seguridad: Es la primera línea de defensa, donde se rechaza varios tipos de ataques, además al hacer NAT protege a los dispositivos de la red de accesos desde el exterior.
- Calidad de servicio: Se refiere al tiempo de respuesta, a la disponibilidad o a la capacidad de ofrecer servicios en función del tipo de usuario.

2.4 Algoritmos de balanceo.

En el respectivo estudio se analizará los algoritmos de balanceo que estén orientados a enlaces WAN.

- *Distribuido (Weighed Balance)*

Se utiliza para asignar mayor o menor tráfico en función de la densidad del ancho de banda requerida, estableciendo un valor para cada conexión, de forma que el tráfico saliente se distribuirá proporcionalmente.[5]

- *Prioridad (Priority)*

Se utiliza para establecer un orden de prioridad para que su tráfico salga por una línea específica, en caso de que la línea prioritaria caiga saldrá por la línea secundaria.[5]

- *Desbordamiento (Overflow)*

Evita que el flujo de tráfico determinado se ralentice cuando la conexión se queda sin ancho de banda disponible. [5]

- *Persistente (Persistence)*

Evita problemas de expiración de sesión al intentar entrar a servicios como HTTPS, El tráfico mantendrá el enrutamiento en la misma conexión hasta que finalice la sesión. [5]

- *Menos usado (Least used)*

Ayuda a elegir la conexión con más ancho de banda libre en el momento. [5]

- *Menor latencia (Lowest latency)*

El tráfico se asigna a la conexión con el tiempo de latencia más baja. [5]

- *Forzado (Enforced)*

Brinda la opción de seleccionar una conexión específica siempre y cuando la conexión este activa. [5]

Una vez definido los conceptos básicos que se deben tomar en cuenta en la implementación de un sistema de alta disponibilidad, se procederá a definir una solución. La propuesta se basará en el diseño de una red que cuente con los parámetros esenciales para asegurar una alta disponibilidad de acceso al internet, la cual podrá ser implementada en cualquier empresa pero en este proyecto estará enfocada para las PYMES.

La red propuesta es la siguiente:

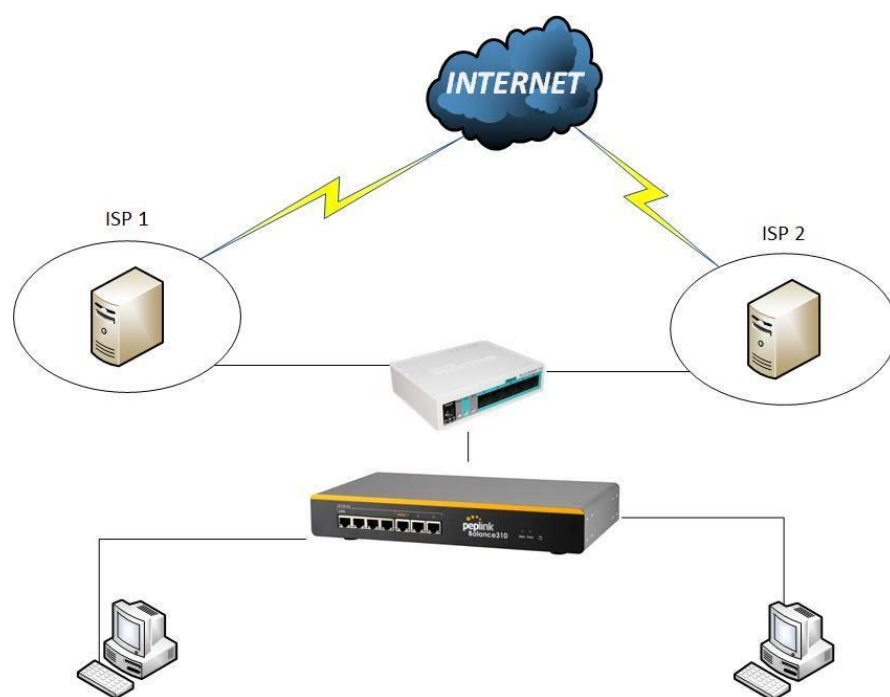


Figura 1.2 Diseño de la red propuesta.

En los siguientes capítulos se analizará en detalle la red mostrada en la figura 1.2, mostrando las configuraciones de cada equipo, su función y el beneficio que aporta a la red.

CAPÍTULO 3

3. CONFIGURACIÓN DEL BALANCEADOR DE CARGA.

3.1 Diseño de la red.

En la red planteada se utilizarán dos ISP`s, un router, un balanceador de carga y dos host; en donde cada uno cumple una función específica, a continuación se detallará el funcionamiento de cada uno de estos dispositivos.

Una solución para mantener el acceso continuo de internet en pequeñas y medianas empresas es tener dos proveedores de internet distintos, uno de los beneficios es que proporciona a la red LAN un tráfico con un ancho de banda eficiente y optimizado; o también como respaldo (backup) en caso de fallo de uno de los dos ISP`s.

Para aislar la red del proveedor y la red LAN de la PYME es necesario colocar un router entre la red del proveedor y la red LAN de la PYME, en este caso de estudio sería antes del balanceador de carga; de esta manera se logrará que el proveedor no tenga acceso a la red LAN de la PYME y viceversa.

En el mercado existen diferentes marcas y modelos de router, para el respectivo proyecto se elegirá el router Mikrotik modelo RB750 por facilidad de estudio. Este equipo trabaja en capa 3 y capa 2 simplificando de esta manera la incorporación de nuevos dispositivos (switch) en el caso de que sea necesario. Su función principal será hacer traducciones de direcciones de red (Network Address Translation - NAT) a las IP públicas de los ISP`s, evitando así el acceso de usuarios externos a la red LAN. Otra función es administrar el ancho de banda que se ofrecerá a cada host de la red LAN. La tabla 2 muestra las especificaciones del router RB 750.

Frecuencia nominal del CPU	850 MHZ
Número de núcleos en el CPU	1
Tamaño de memoria RAM	64 MHZ
Puertos Ethernet 10/100	5
Sistema Operativo	RouterOS

Tabla 2: Especificaciones del Router RB 750. [6]

El balanceador de carga administra el acceso de internet de los usuarios (host) de la red LAN mediante los algoritmos de balanceo, restringe el acceso de páginas web, ofrece calidad de servicio y administra las IP privada de la red LAN dependiendo de la dirección MAC de cada dispositivo. Para esta red se utilizará el balanceador de carga PEPLINK BALANCE 310 por facilidad de estudio.

Para realizar las pruebas del funcionamiento de la red se utilizaran únicamente dos usuarios debido a la facilidad de análisis, cabe recalcar que el número de usuarios máximo que se pueden conectar en el balanceador es cuatro. Si se desea ampliar de manera significativa el número de usuarios se deberá utilizar un dispositivo adicional de capa 2.

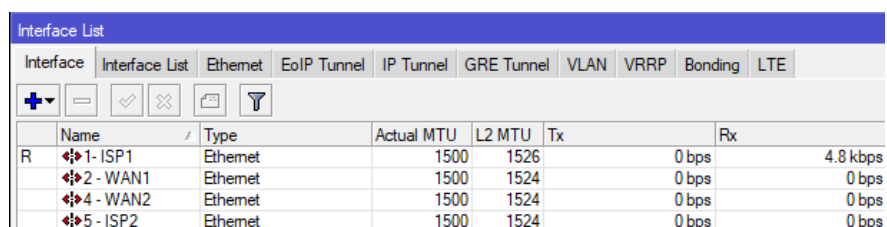
3.2 Configuración del router para tráfico de paquetes.

El router RB 750 Mikrotik tiene 5 puertos Ethernet los cuales pueden ser configurados a conveniencia del cliente como puertos LAN o WAN. Se puede utilizar a grande o mediana escala debido a la versatilidad que ofrece. Es un dispositivo fácil de configurar y en el mercado se encuentra con un costo accesible.

Para la implementación se deberá configurar el router utilizando el software Winbox. A continuación se muestran las configuraciones que se llevarán a cabo.

3.2.1 Configuración de interfaces.

Se debe configurar cuatro interfaces del router, dos para la conexión de los ISP que llevan por nombre ISP1 e ISP2, y dos para los enlaces WAN que se conectarán al balanceador de carga que llevan por nombre WAN1 y WAN2 ; las cuales se observan en la figura 2.1.



Interface List									
Interface	Interface List	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VRRP	Bonding	LTE
R	1- ISP1	Ethernet	1500	1526	0 bps	4.8 kbps			
	2 - WAN1	Ethernet	1500	1524	0 bps	0 bps			
	4 - WAN2	Ethernet	1500	1524	0 bps	0 bps			
	5 - ISP2	Ethernet	1500	1524	0 bps	0 bps			

Figura 2.1 Tabla de interfaces del Router RB 750.

Cada ISP establece las siguientes direcciones IP públicas, las cuales serán colocadas en las interfaces ISP1 Y ISP2 respectivamente. La tabla 3 y tabla 4 indican la información de direcciones IP del ISP1 e ISP2 respectivamente.

ISP1	
IP address	200.90.157.147
Mask	255.255.255.224
Gateway	200.90.157.129
DNS	200.90.152.4

Tabla 3: Direcciones Públicas ISP1.

ISP2	
IP address	200.90.156.100
Mask	255.255.255.224
Gateway	200.90.156.97
DNS	200.90.153.4

Tabla 4: Direcciones Públicas ISP2.

Para uso interno de la red, se definirán IP privadas en las interfaces 2-WAN1 y 3-WAN2 del router como se muestra en las siguientes figuras (3.2, 3.3).

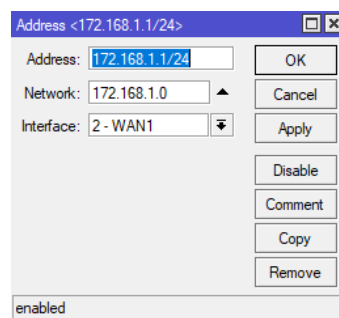


Figura 3.2 Dirección IP privada interfaz 2-WAN.

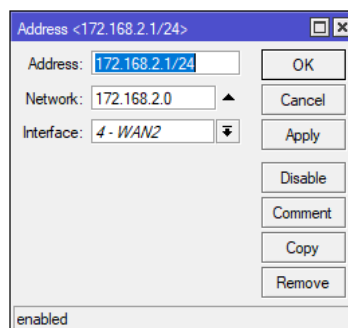
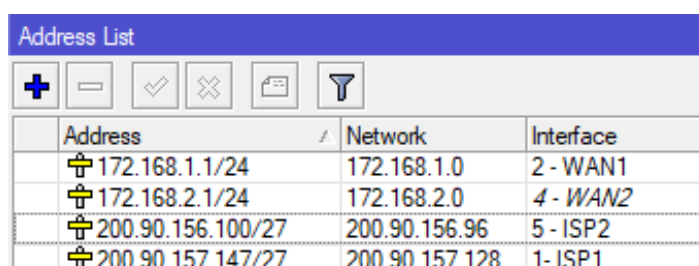


Figura 3.3 Dirección IP privada interfaz 4-WAN2.

De esta manera se habrá configurado las 4 interfaces del router RB 750, las cuales se observan en la figura 3.4.



Address	Network	Interface
172.168.1.1/24	172.168.1.0	2 - WAN1
172.168.2.1/24	172.168.2.0	4 - WAN2
200.90.156.100/27	200.90.156.96	5 - ISP2
200.90.157.147/27	200.90.157.128	1 - ISP1

Figura 3.4 Interfaces de Router RB.

3.2.2 Configuración del NAT.

La traducción de direcciones de red (Network address translation - NAT), es un estándar de internet que permite a los usuarios de una red LAN usar un set de direcciones IP para comunicaciones internas y otro set de direcciones IP para comunicaciones externas. [7]

Se procederá a realizar NAT para cada interfaz con dirección IP privada (WAN1 y WAN2), utilizando el tipo de NAT "srcnat" propio de los dispositivos Mikrotik, cuya función será permitir que la red conectada a la interfaz WAN1 tenga la dirección IP pública de la interfaz ISP1 mientras que la red conectada a la interfaz WAN2 tenga la dirección IP pública de la interfaz ISP2.

Se habilitará la opción "masquerade" la cual mejorará el tiempo de recuperación del sistema en el caso de que el servidor DHCP cambie las IP públicas. Las respectivas configuraciones se observan en las siguientes figuras (3.5, 3.6, 3.7, 3.8).

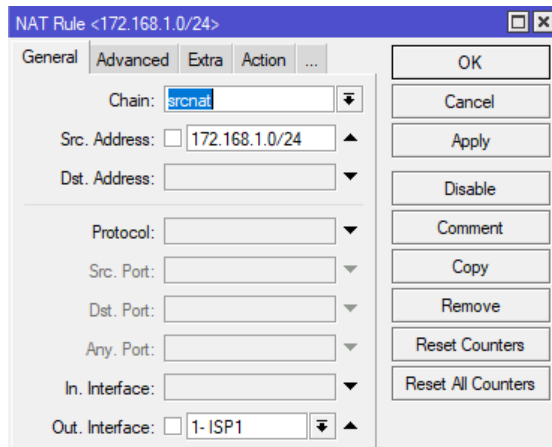


Figura 3.5 Configuración del NAT en 2-WAN1.

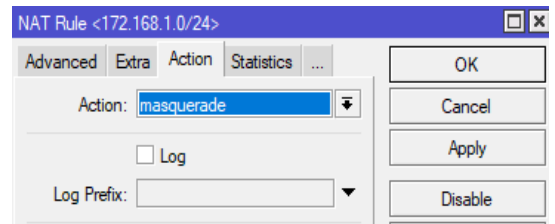


Figura 3.6 Habilidad Masquerade.

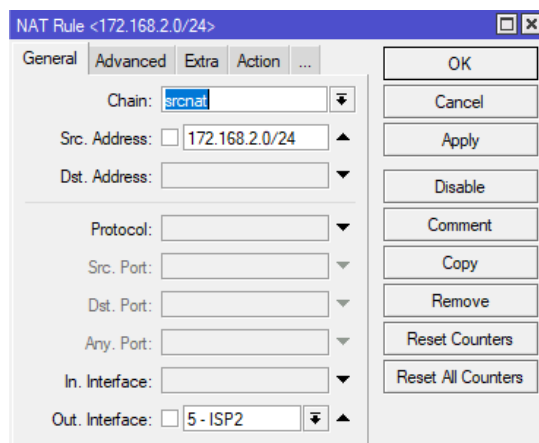


Figura 3.7 Configuración del NAT en 4-WAN2.

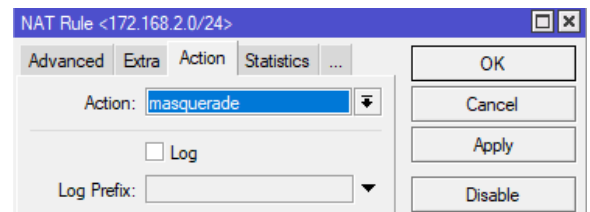
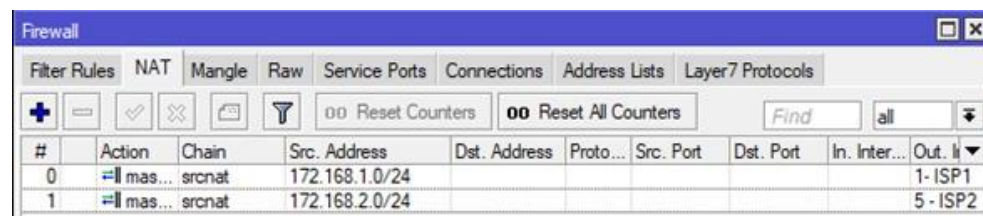


Figura 3.8 Habilidad Masquerade.

Finalmente, la configuración del NAT en el router RB 750 se muestra en la figura 3.9.

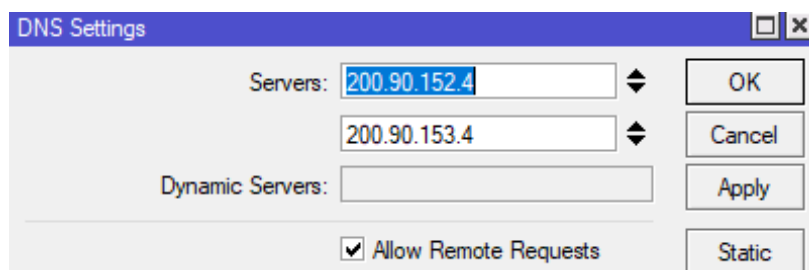


#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. I...
0	mas...	srcnat	172.168.1.0/24						1-ISP1
1	mas...	srcnat	172.168.2.0/24						5-ISP2

Figura 3.9 Confiaguración del NAT en router RB 750.

3.2.3 Configuración del Servidor DNS.

Se agregan las direcciones IP de cada servidor de sistema de nombres de dominio (Domain Name Service – DNS), los cuales traducen los nombres de dominio a IPs. Estas direcciones fueron facilitadas por cada ISP previamente. En la figura 3.10 se observan las direcciones IP de los servidores DNS configurados.



DNS Settings

Servers: 200.90.152.4
200.90.153.4

Dynamic Servers:

Allow Remote Requests

OK
Cancel
Apply
Static

Figura 3.10 Direcciones IP pública de los servidores DNS.

El siguiente paso será re direccionar el tráfico, se requiere que el tráfico proveniente de la interfaz ISP1 pase por la interfaz WAN1, y que el tráfico proveniente de la interfaz ISP2 pase por la interfaz WAN2. Para que este proceso se logre es necesario crear marcas en los paquetes, dicho proceso se observa en las siguientes figuras (3.11, 3.12, 3.13, 3.14, 3.15).

Marca para la interfaz "WAN1"

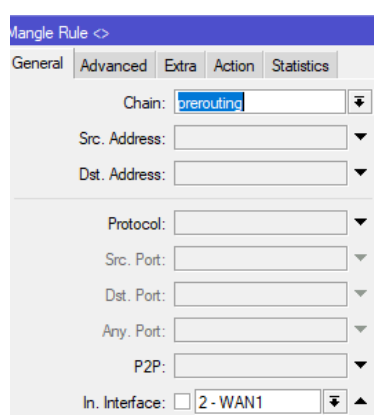


Figura 3.11 Configuración de marca.

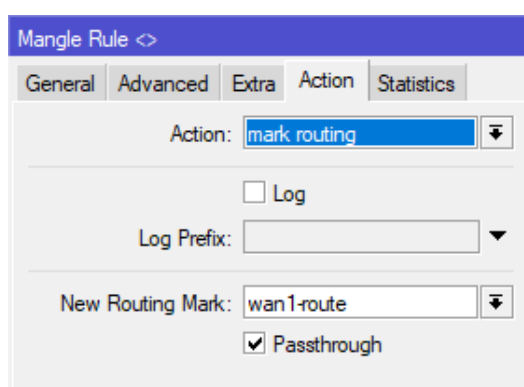


Figura 3.12 Configuración de marca.

Marca para la interfaz "WAN2"

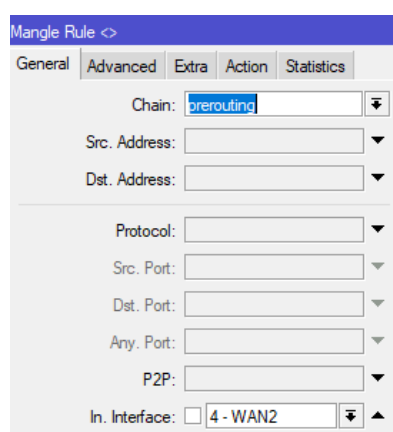


Figura 3.13 Configuración de marca.

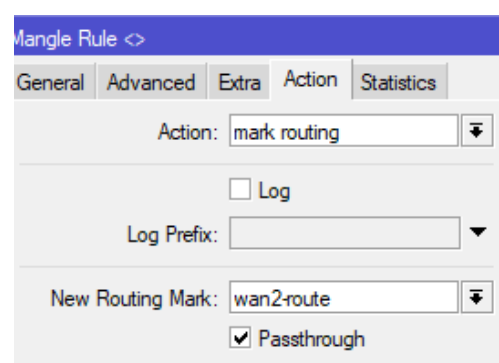


Figura 3.14 Configuración de marca.

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Interface	Out. Int...	Bytes	Packets
Firewall											
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols											
+ [Icons] 00 Reset Counters 00 Reset All Counters											
::: Lan 172.168.1.1/24											
0	✓ mar...	prerouting						2 - WAN1		1051.8 KiB	12 610
::: Lan 172.168.2.1/24											
1	✓ mar...	prerouting						4 - WAN2		882.1 KiB	10 204

Figura 3.15 Configuración de marca del tráfico.

Establecidas previamente las marcas se procederá a añadir una ruta para el direccionamiento de los paquetes hacia el exterior; dicho proceso se muestra en las figuras (3.16, 3.17).

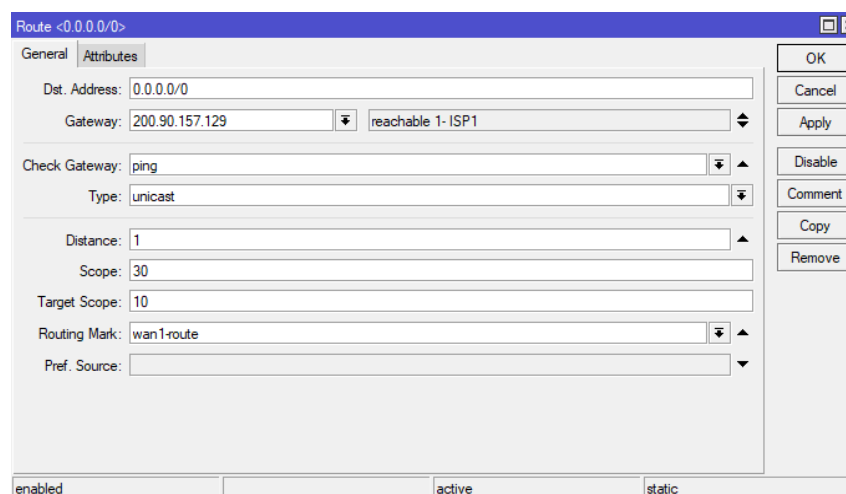


Figura 3.16 Direccionamiento ISP-1.

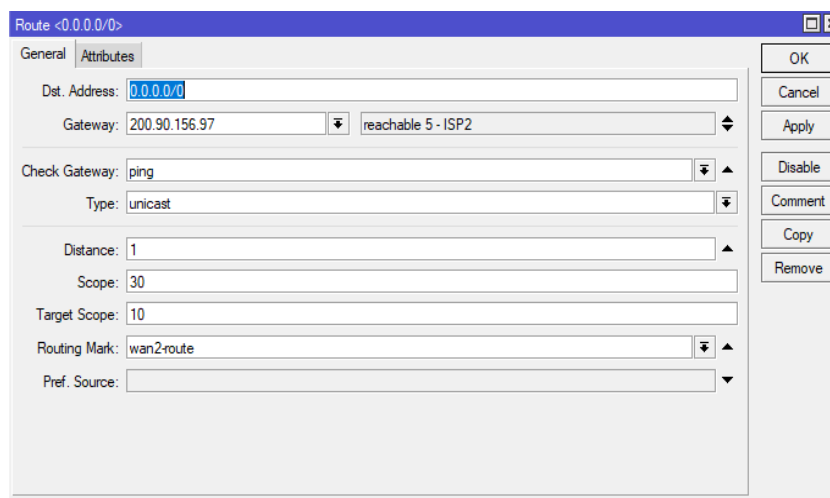


Figura 3.17 Direccionamiento ISP-2.

Finalmente la ruta queda configurada como se muestra en la figura 3.18.

Route List					
Routes					
	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAC	200.90.157.128/27	1-ISP1 reachable	0		200.90.157.147
DAC	172.168.1.0/24	2 - WAN1 reachable	0		172.168.1.1
AS	0.0.0.0/0	200.90.156.97 reachable 5 - ISP2	1	wan2-route	
AS	0.0.0.0/0	200.90.157.129 reachable 1-ISP1	1	wan1-route	
DAC	172.168.2.0/24	4 - WAN2 reachable	0		172.168.2.1
DAC	200.90.156.96/27	5 - ISP2 reachable	0		200.90.156.100

Figura 3.18 Direccionamiento.

Se controlará el ancho de banda para cada interfaz WAN-1 y WAN-2, se definirá 10 M y 5M de subida y bajada respectivamente. Estos valores pueden ser modificados dependiendo la necesidad del PYME. Dichas configuraciones se muestran en las siguientes figuras (3.19, 3.20, 3.21).

Simple Queue <WAN1>

General | Advanced | Statistics | Traffic | Total | Total Statistics

Name: WAN1

Target: 2 - WAN1

Dst.:

	Target Upload	Target Download
Max Limit:	10M	10M
Burst Limit:	unlimited	unlimited
Burst Threshold:	unlimited	unlimited
Burst Time:	0	0

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
Torch

Figura 3.19 Límite de ancho de banda en interfaz WAN1.

Simple Queue <WAN2>

General | Advanced | Statistics | Traffic | Total | Total Statistics

Name: WAN2

Target: 4 - WAN2

Dst.:

	Target Upload	Target Download
Max Limit:	5M	5M
Burst Limit:	unlimited	unlimited
Burst Threshold:	unlimited	unlimited
Burst Time:	0	0

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
Torch

Figura 3.20 Límite de ancho de banda en interfaz WAN2.

Queue List						
Simple Queues		Interface Queues		Queue Tree	Queue Types	
+		-		✓	✗	📄
				🔍	00 Reset Counters	00 Reset All Counters
#	Name	Target	Upload Max Limit	Download Max Limit	Packet Marks	Total Max Limit (bits/s)
0	WAN1	2 - WAN1	10M	10M		
1	WAN2	4 - WAN2	5M	5M		

Figura 3.21 Límite de ancho de banda de las interfaces del router.

3.3 Configuración de interfaces del balanceador de carga.

El Balanceador de carga PEPLINK BALANCE 310 tiene 3 puertos WAN y 4 puertos LAN, de los cuales solo se utilizará dos puertos respectivamente. Las interfaces WAN1 y WAN2 del balanceador se conectarán a las interfaces WAN1 y WAN2 previamente configuradas en el router RB 750; mientras que en los puertos LAN se conectarán los hosts.

El Balanceador de carga se configurará de tal manera que brinde a las redes LAN una conexión continua al internet ofreciendo un control y monitoreo continuo del ancho de banda.

Para comenzar la configuración se deberá conectar el dispositivo a una PC utilizando un cable de red, posteriormente se ingresará la dirección IP por default 192.168.1.1 en un navegador web. Se debe ingresar "admin" como username y password, de esta manera se ingresará al administrador Web del Balanceador como se muestra en la figura 3.22.

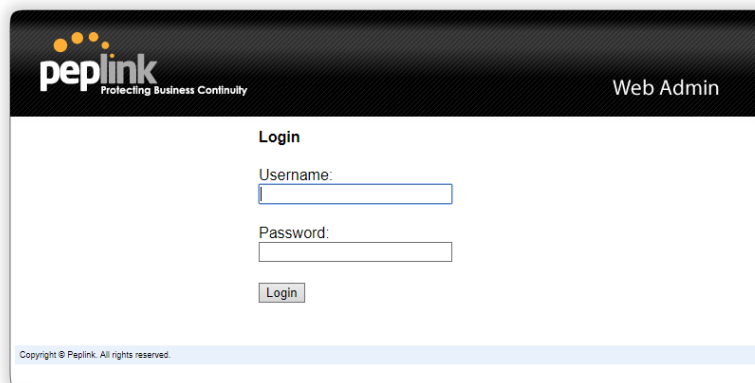


Figura 3.22 Página de inicio del administrador web del balanceador.

Se procederá primero a realizar el cambio de dirección IP y su respectiva máscara: 172.168.12.1/24 como se indica en la figura 3.23.

IP Settings	
IP Address *	<input type="text" value="172.168.12.1"/>
Subnet Mask *	<input type="text" value="255.255.255.0 (/24)"/> ▼
Speed ?	<input type="text" value="Auto"/> ▼

Figura 3.23 Configuración de la dirección IP del balanceador.

3.3.1 Configuración de las interfaces LAN.

Para configurar las interfaces LAN del balanceador se habilitará su servidor DHCP, el cual asignará una dirección IP a cada computadora que esté conectada vía LAN. El rango de direcciones IP que serán asignadas por el servidor DHCP serán desde la 172.168.12.100 hasta la 172.168.12.254. De esta manera se evitará configurar la dirección IP, máscara y el Gateway para cada dispositivo nuevo que se desea añadir a la red.

Para la implementación se reservará las direcciones IP para los dos hosts que estarán conectados al balanceador. La dirección IP es asignada de acuerdo a la dirección MAC de cada computadora como se muestra en la tabla 5.

Host	Dirección IP	Dirección MAC
PC1	172.168.12.2	64:31:50:1E:31:B6
PC2	172.168.12.3	74:D4:35:EA:6B:9F

Tabla 5: Direcciones IP reservadas para la red LAN.

Se añadirá las direcciones IP de los servidores DNS, para que automáticamente el servidor DHCP asigne estas direcciones a cada host, la respectiva configuración se muestra en la figura 3.24.

DHCP Server Settings																			
DHCP Server	<input checked="" type="checkbox"/> Enable																		
IP Range	172.168.12.100 - 172.168.12.254																		
Subnet Mask	255.255.255.0 (/24)																		
Lease Time	1 Days 0 Hours 0 Mins 0 Seconds																		
DNS Servers	<input type="checkbox"/> Assign DNS server automatically DNS server 1: 200.90.152.4 DNS server 2: 200.90.153.4																		
WINS Servers	<input type="checkbox"/> Assign WINS server																		
Extended DHCP Option	<table border="1"> <thead> <tr> <th>Option</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td colspan="2" style="text-align: center;">No Extended DHCP Option</td> </tr> <tr> <td colspan="2" style="text-align: center;"><input type="button" value="Add"/></td> </tr> </tbody> </table>			Option	Value	No Extended DHCP Option		<input type="button" value="Add"/>											
Option	Value																		
No Extended DHCP Option																			
<input type="button" value="Add"/>																			
DHCP Reservation	<table border="1"> <thead> <tr> <th>Name</th> <th>MAC Address</th> <th>Static IP</th> <th></th> </tr> </thead> <tbody> <tr> <td>PC1</td> <td>64:31:50:1E:31:B6</td> <td>172.168.12.2</td> <td style="text-align: center;">✖</td> </tr> <tr> <td>PC2</td> <td>74:D4:35:EA:6B:9F</td> <td>172.168.12.3</td> <td style="text-align: center;">✖</td> </tr> <tr> <td></td> <td></td> <td></td> <td style="text-align: center;">+</td> </tr> </tbody> </table>			Name	MAC Address	Static IP		PC1	64:31:50:1E:31:B6	172.168.12.2	✖	PC2	74:D4:35:EA:6B:9F	172.168.12.3	✖				+
Name	MAC Address	Static IP																	
PC1	64:31:50:1E:31:B6	172.168.12.2	✖																
PC2	74:D4:35:EA:6B:9F	172.168.12.3	✖																
			+																

Figura 3.24 Configuración del servidor DHCP del balanceador.

3.3.2 Configuración de las interfaces WAN.

Se configurará las interfaces WAN1 y WAN2 del balanceador, para ello primero se definirá el método de conexión el cual será DHCP, debido a que a través de este protocolo se reciben las direcciones IP de las interfaces WAN1 y WAN2 del router. Posteriormente se habilitará el NAT, el cual se aplicará al tráfico enrutado a través de la conexión WAN.

Debido a que se utilizará las dos conexiones WAN al mismo tiempo, es necesario colocar la conexión WAN como habilitada caso contrario una de las dos conexiones será utilizada como respaldo (backup).

Como medida de protección contra cualquier ataque informático se deshabilitará el protocolo ICMP para que las interfaces WAN1 y WAN2 no respondan a solicitudes de PING. Se Colocará el ancho de banda de subida y de bajada que se estableció en el router para la interfaz WAN1 y WAN2. Las configuraciones de las interfaces WAN se observan en las figuras (3.25, 3.26).

Connection Settings	
WAN Connection Name *	WAN 1
Enable	<input checked="" type="checkbox"/>
Connection Method	<input type="button" value="?"/> DHCP <input type="button" value="v"/> Click here to edit Connection settings
Routing Mode	<input type="button" value="?"/> <input checked="" type="radio"/> NAT
Connection Type	<input type="button" value="?"/> <input checked="" type="radio"/> Always-on <input type="radio"/> Backup Priority
Reply to ICMP PING	<input type="button" value="?"/> <input type="checkbox"/> Enable
Upload Bandwidth *	<input type="button" value="?"/> 10 <input type="button" value="v"/> Mbps
Download Bandwidth *	<input type="button" value="?"/> 10 <input type="button" value="v"/> Mbps

Figura 3.25 Configuración de la interfaz WAN.

Connection Settings	
WAN Connection Name *	WAN 2
Enable	<input checked="" type="checkbox"/>
Connection Method	DHCP <input type="button" value="v"/> Click here to edit Connection settings
Routing Mode	<input checked="" type="radio"/> NAT
Connection Type	<input checked="" type="radio"/> Always-on <input type="radio"/> Backup Priority
Reply to ICMP PING	<input type="checkbox"/> Enable
Upload Bandwidth *	5 <input type="button" value="v"/> Mbps
Download Bandwidth *	5 <input type="button" value="v"/> Mbps

Figura 3.26 Configuración de la interfaz WAN2.

3.4 Configuración del servidor DNS

Se añade las direcciones IP de los servidores DNS como se muestra en la figura 3.27.

DHCP Settings	
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically <input checked="" type="checkbox"/> Use the following DNS server address(es) DNS server 1: 200.90.153.4 DNS server 2: 200.90.152.4
Hostname (Optional)	<input type="button" value="v"/> <input type="checkbox"/> Use custom hostname

Figura 3.27 Configuración de las direcciones IP de los servidores DNS.

El balanceador provee la funcionalidad de periódicamente revisar la salud de cada conexión WAN, para activar esta función se debe habilitar la función DNS lookup, la cual comprobará la conectividad con los servidores DNS previamente establecidos; posteriormente se añade el periodo de comprobación. Las respectivas configuraciones se observan en la figura 3.28.

Health Check Settings	
Method	? DNS Lookup
Health Check DNS Servers	Host 1: 200.90.152.4 Host 2: 200.90.153.4 <input type="checkbox"/> Use first two DNS servers as Health Check DNS Servers <input checked="" type="checkbox"/> Include public DNS servers
Timeout	? 5 second(s)
Health Check Interval	? 5 second(s)
Health Retries	? 3
Recovery Retries	? 3

Figura 3.28 Configuración del chequeo de salud de los WAN.

3.5 Configuración Calidad de servicio (Qos)

Para brindar calidad de servicio al diseño de la red planteada es necesario implementar un control al tráfico de las aplicaciones; para ello no es necesario agregar otro dispositivo debido que el Balanceador Peplink ofrece Calidad de servicio (QoS).

El balanceador Peplink realiza una inspección del contenido de los paquetes, de esta manera las aplicaciones pueden ser priorizadas en tres categorías: Alta, mayor y baja, las cuales son aplicadas dependiendo de las necesidades o requerimientos del usuario. Para este caso de estudio se eligieron las siguientes aplicaciones con sus respectivas prioridades, tal como se muestra en la figura 3.29.

Application	Priority	Action
Skype	↑ High	✘
All Supported Streaming Applications	↓ Low	✘
Mail	↑ High	✘
Add		

Figura 3.29 Configuración de la prioridad de las aplicaciones.

3.6 Configuración Firewall

Para proteger la red local de potenciales ataques de hackers, sitios web ofensivos u otro uso inapropiado; es necesario contar con un mecanismo que filtre selectivamente el tráfico de datos entre el lado WAN y el lado LAN de la red. El balanceador Peplink brinda esta función, para ello solo se requiere activarlo.

Para este caso de estudio se seleccionaron dos sitios webs: El UNIVERSO y FACEBOOK a los cuales se les aplicará reglas de bloqueo.

Para el host con la dirección IP 172.168.12.2 se denegó el acceso al sitio web del diario El UNIVERSO; mientras que para toda la red se denegó el acceso al sitio web de FACEBOOK. Las configuraciones del firewall se observan en las figuras (3.30, 3.31).

No ElUniverso	
Rule Name *	No ElUniverso
Enable	<input checked="" type="checkbox"/>
Protocol	Any ◯ ← :: Protocol Selection Tool :: ◯
Source IP & Port	Single Address ◯ IP: 172.168.12.2
Destination IP & Port	Domain Name ◯ eluniverso.*
Action	<input type="radio"/> Allow <input checked="" type="radio"/> Deny
Event Logging	<input checked="" type="checkbox"/> Enable

Figura 3.30 Configuración del bloqueo al sitio web el universo.

No Facebook	
Rule Name *	No Facebook
Enable	<input checked="" type="checkbox"/>
Protocol	Any ← :: Protocol Selection Tool ::
Source IP & Port	Any Address
Destination IP & Port	Domain Name facebook.*
Action	<input type="radio"/> Allow <input checked="" type="radio"/> Deny
Event Logging	<input checked="" type="checkbox"/> Enable

Figura 3.31 Configuración del bloqueo al sitio web de Facebook.

Finalmente las reglas de bloqueo en el balanceador PEPLINK quedan configuradas como se muestran en la figura 3.32.

Outbound Firewall Rules (Drag and drop rows to change rule order)					
Rule	Protocol	Source IP Port	Destination IP Port	Policy	
No ElUniverso	Any	172.168.12.2	eluniverso.*	Deny	<input checked="" type="checkbox"/>
No Facebook	Any	Any	facebook.*	Deny	<input checked="" type="checkbox"/>
Default	Any	Any	Any	Allow	
<input type="button" value="Add Rule"/>					

Figura 3.32 Reglas de balanceo aplicadas al balanceador.

El balanceador soporta la detección, prevención de intrusiones, y ataques de denegación de servicio (DoS) de internet. Cuando esta función está habilitada, el balanceador detectará y lo protegerá de ataques. La figura 3.33 muestra la configuración para la prevención de ataques DoS.

Intrusion Detection and DoS Prevention	
Enabled	<input type="checkbox"/>

Figura 3.33 Configuración para prevención de ataques DoS

3.7 Configuración de reglas de balanceo

Basándose en los algoritmos de Balanceo del PEPLINK 310, se seleccionarán tres escenarios en donde se aplicarán reglas de balanceo acorde a las prioridades establecidas por el administrador de la red LAN.

3.7.1 Primer escenario

El PYME posee enlaces WAN con anchos de banda diferentes y el administrador requiere que estos enlaces trabajen simultáneamente.

Solución

Cuando se tiene este escenario se recomienda aplicar el algoritmo “Distribución por Peso (Weighted Balance)”, en donde se asigna un peso ponderado a cada uno de los enlaces WAN; logrando que la cantidad de tráfico que es proporcionada a un enlace WAN sea en función al peso ponderado.

Configuración

Se debe definir un nombre para identificar el algoritmo, para este caso se seleccionó el nombre ‘PESO’; si se desea aplicar este algoritmo en toda la red se debe colocar ‘ANY’ en el campo “destination”, caso contrario se deberá colocar la dirección IP del host al que se le aplicará el algoritmo. Se asigna la cantidad del peso ponderado a cada enlace WAN de la red como se muestra en la tabla 6.

WAN	PESO
1	8
2	7
3	0
PESO TOTAL: 8+7+0= 15	

Tabla 6: Asignacion de peso a los enlaces WAN.

El tráfico distribuido al enlace WAN 1= $(8/15)*100$

El tráfico distribuido al enlace WAN 1= 53.33%

El tráfico distribuido al enlace WAN 2= $(7/15)*100$

El tráfico distribuido al enlace WAN 2= 46.66%

La figura 3.34 muestra las configuraciones del algoritmo aplicado.

PESO	
Service Name *	PESO
Enable	<input checked="" type="checkbox"/>
Source	Any
Destination	Any
Protocol	Any :: Protocol Selection Tool
Algorithm	Weighted Balance
Load Distribution Weight	WAN 1 8 WAN 2 7 WAN 3 0
Terminate Sessions on Link Recovery	<input type="checkbox"/> Enable

Figura 3.34 Configuración del algoritmo de distribución por peso.

3.7.2 Segundo escenario

El PYME posee enlaces WAN con anchos de banda diferentes y el administrador requiere que cada host de la red LAN esté conectado a un enlace WAN diferente, y a su vez cada host tenga como respaldo (backup) el enlace WAN al que no esté conectado.

Solución

Cuando se tiene este escenario se recomienda aplicar el algoritmo "PRIORITY", en donde se asigna la prioridad de los enlaces WAN que serán utilizados en la red. El enlace con la prioridad más alta disponible siempre será usado para el direccionamiento del tráfico, mientras que el enlace WAN con la menor prioridad será usado solo si los enlaces de mayor prioridad dejan de estar disponibles.

Configuración

El host con la dirección IP 172.168.12.2 se conectará a la WAN1 y en caso de que esta conexión falle se conectara a la WAN2; mientras que el host con la dirección 172.168.12.3 ocurrirá lo contrario, se conectará a la WAN2 y en caso de fallo se conectará a la WAN1.

Para este caso de estudio se definirá la prioridad como se muestra en la tabla 7.

DIRECCIÓN IP DEL HOST	ENLACE WAN PRIMARIO	ENLACE WAN SECUNDARIO
172.168.12.2	WAN1	WAN2
172.168.12.3	WAN2	WAN1

Tabla 7: Enlaces WAN primario y secundario de cada host

Las configuraciones del algoritmo aplicado se muestran en las figuras (3.35, 3.36).

PC1									
Service Name *	PC1								
Enable	<input checked="" type="checkbox"/>								
Source	Any								
Destination	IP Address 172.168.12.2								
Protocol	Any :: Protocol Selection Tool								
Algorithm	Priority								
Priority Order	<table border="1"> <tr> <td>Highest Priority</td> <td>Not In Use</td> </tr> <tr> <td>WAN: WAN 1</td> <td>WAN: WAN 3</td> </tr> <tr> <td>WAN: WAN 2</td> <td></td> </tr> <tr> <td>Lowest Priority</td> <td></td> </tr> </table>	Highest Priority	Not In Use	WAN: WAN 1	WAN: WAN 3	WAN: WAN 2		Lowest Priority	
Highest Priority	Not In Use								
WAN: WAN 1	WAN: WAN 3								
WAN: WAN 2									
Lowest Priority									
Terminate Sessions on Link Recovery	<input checked="" type="checkbox"/> Enable								

Figura 3.35 Configuración del algoritmo de prioridad para la PC1.

PC2									
Service Name *	PC2								
Enable	<input checked="" type="checkbox"/>								
Source	Any								
Destination	IP Address 172.168.12.3								
Protocol	Any ← :: Protocol Selection Tool ::								
Algorithm	Priority								
Priority Order	<table border="1"> <tr> <td>Highest Priority</td> <td>Not In Use</td> </tr> <tr> <td>WAN: WAN 2</td> <td>WAN: WAN 3</td> </tr> <tr> <td>WAN: WAN 1</td> <td></td> </tr> <tr> <td>Lowest Priority</td> <td></td> </tr> </table>	Highest Priority	Not In Use	WAN: WAN 2	WAN: WAN 3	WAN: WAN 1		Lowest Priority	
Highest Priority	Not In Use								
WAN: WAN 2	WAN: WAN 3								
WAN: WAN 1									
Lowest Priority									
Terminate Sessions on Link Recovery	<input checked="" type="checkbox"/> Enable								

Figura 3.36 Configuración del algoritmo de prioridad para la PC2.

3.7.3 Tercer Escenario

El PYME posee enlaces WAN con anchos de banda diferentes y el administrador requiere que toda la red LAN se conecte solo a un enlace WAN manteniendo como respaldo (backup) el enlace WAN al que no esté en uso.

Solución

Cuando se tiene este escenario se recomienda aplicar el algoritmo "PRIORITY", en donde se asigna la prioridad de los enlaces WAN que serán utilizados en la red. El enlace con la prioridad más alta disponible siempre será usado para el direccionamiento del tráfico, mientras que el enlace WAN con la menor prioridad será usado solo si los enlaces de mayor prioridad dejan de estar disponibles.

Configuración

Se elige el enlace WAN el cual funcionará como backup, en este caso se elegirá WAN2 debido que posee menor ancho de banda. En las configuraciones de la WAN2 se cambiará el tipo de conexión a “Backup priority” para que el enlace WAN2 solo se active si el enlace WAN1 se encuentre inactivo. La respectiva configuración se observa en las siguientes figuras (3.37, 3.38).

Connection Settings	
WAN Connection Name *	WAN 2
Enable	<input checked="" type="checkbox"/>
Connection Method	DHCP Click here to edit Connection settings
Routing Mode	<input checked="" type="radio"/> NAT
Connection Type	<input type="radio"/> Always-on <input checked="" type="radio"/> Backup Priority Group 1 (Highest) ▾
Reply to ICMP PING	<input type="checkbox"/> Enable
Upload Bandwidth *	5 Mbps ▾
Download Bandwidth *	5 Mbps ▾

Figura 3.37 Configuración del enlace WAN2 como backup.

WAN2 Backup									
Service Name *	WAN2 Backup								
Enable	<input checked="" type="checkbox"/>								
Source	Any ▾								
Destination	Any ▾								
Protocol	Any ▾ ← :: Protocol Selection Tool :: ▾								
Algorithm	Priority ▾								
Priority Order	<table border="1"> <tr> <td>Highest Priority</td> <td>Not In Use</td> </tr> <tr> <td>WAN: WAN 1</td> <td>WAN: WAN 3</td> </tr> <tr> <td>WAN: WAN 2</td> <td></td> </tr> <tr> <td>Lowest Priority</td> <td></td> </tr> </table>	Highest Priority	Not In Use	WAN: WAN 1	WAN: WAN 3	WAN: WAN 2		Lowest Priority	
Highest Priority	Not In Use								
WAN: WAN 1	WAN: WAN 3								
WAN: WAN 2									
Lowest Priority									
Terminate Sessions on Link Recovery	<input checked="" type="checkbox"/> Enable								

Figura 3.38 Configuración del algoritmo de prioridad estableciendo el enlace WAN2 como Backup.

CAPITULO 4

4. ANÁLISIS DE TRÁFICO Y RESULTADOS

Para cada uno de los escenarios planteados en el capítulo 3 se hará un análisis del comportamiento de la red en tiempo real realizando pruebas de fallo (Fail-over). Para todas las pruebas se realizó un alto consumo de ancho de banda.

4.1 Primer escenario

En este escenario se definió el algoritmo de balanceo “Distribución por Peso (Weighted Balance)”; en las figuras (4.1, 4.2, 4.3) se observa el funcionamiento de los dos enlaces WAN, en donde ambos enlaces funcionan al mismo tiempo y el tráfico de la red LAN es distribuido hacia cada enlace dependiendo del peso con el que fueron configurados en el capítulo 3.

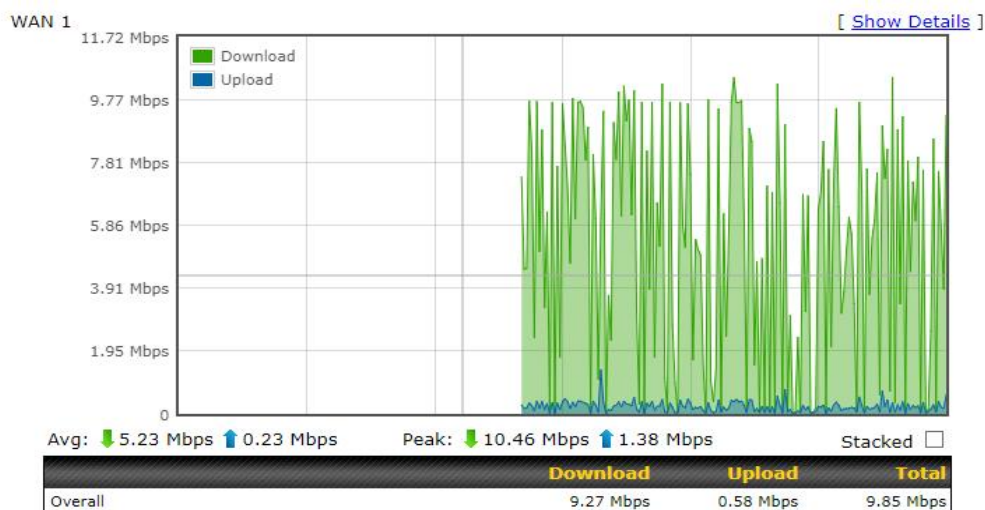


Figura 4.1 Tráfico de descarga del enlace WAN1 en el escenario 1.

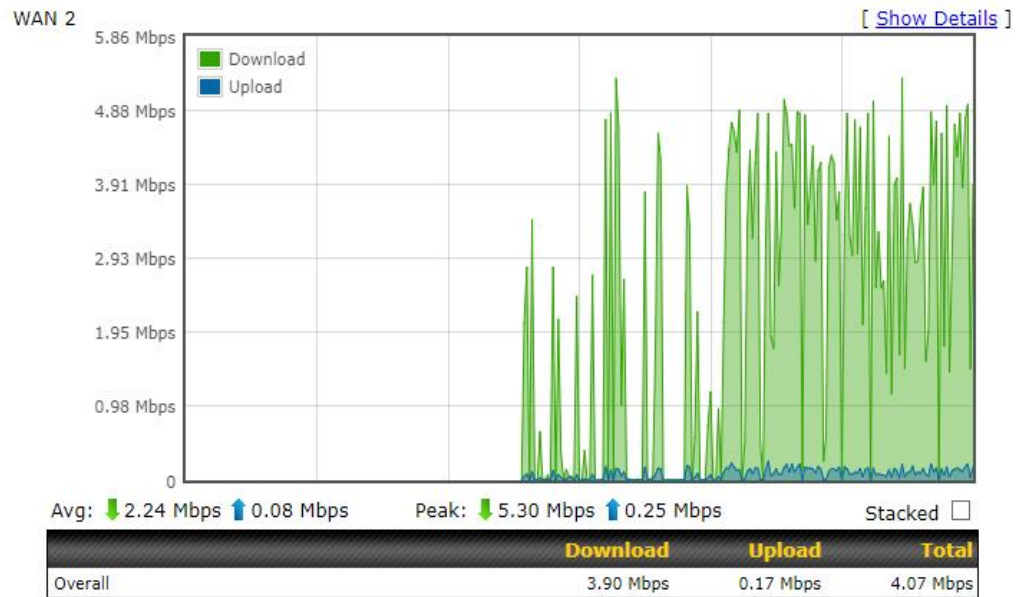


Figura 4.2 Tráfico de descarga del enlace WAN2 en el escenario 1.

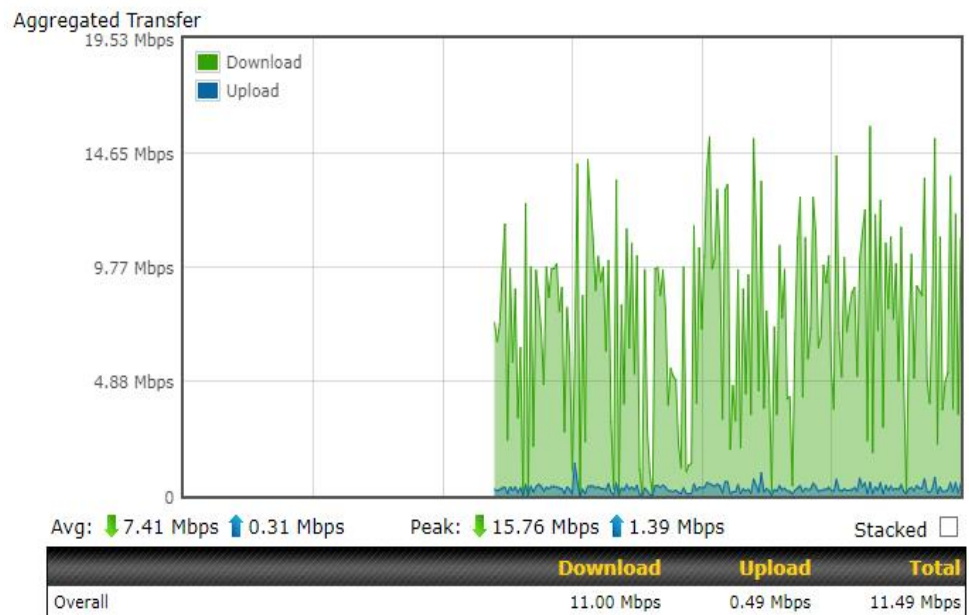


Figura 4.3 Tráfico total de descarga en el escenario 1.

Se realizará pruebas de fallo (Fail-over) para comprobar alta disponibilidad de acceso a internet en la red. Para ello se procederá a realizar las pruebas de fallo (Fail-over) en donde se desconectara respectivamente un enlace WAN para observar que todo el tráfico de la red LAN se re-direcciona al enlace WAN disponible, tal como se muestra en las figuras (4.4, 4.5, 4.6).

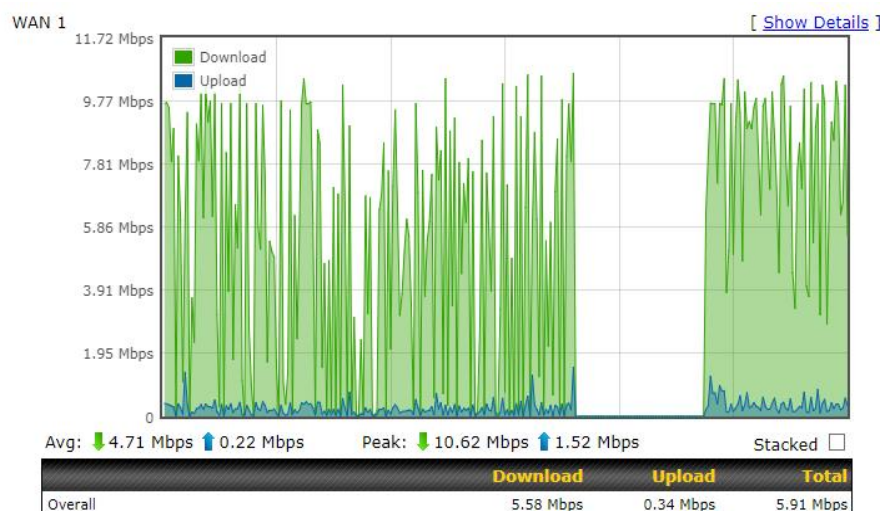


Figura 4.4 Tráfico de descarga del enlace WAN1 en el escenario 1 realizando pruebas de error.

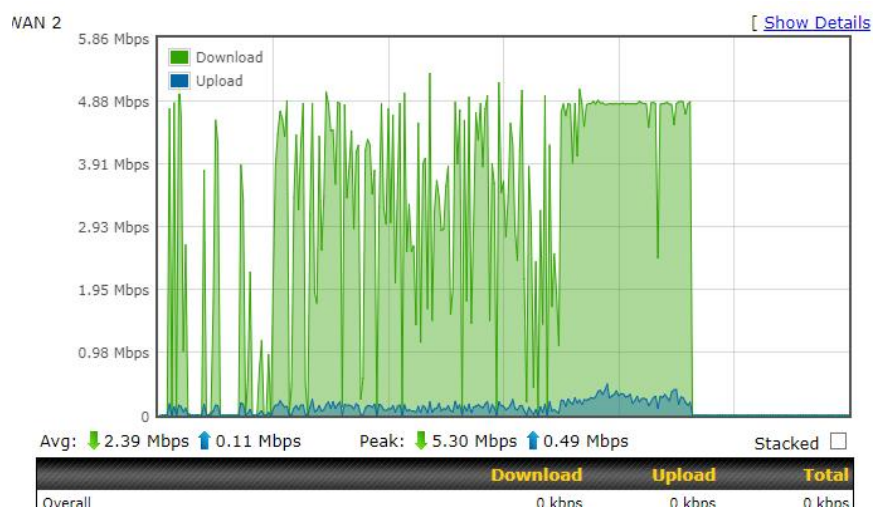


Figura 4.5 Tráfico de descarga del enlace WAN2 en el escenario 1 realizando pruebas de error.

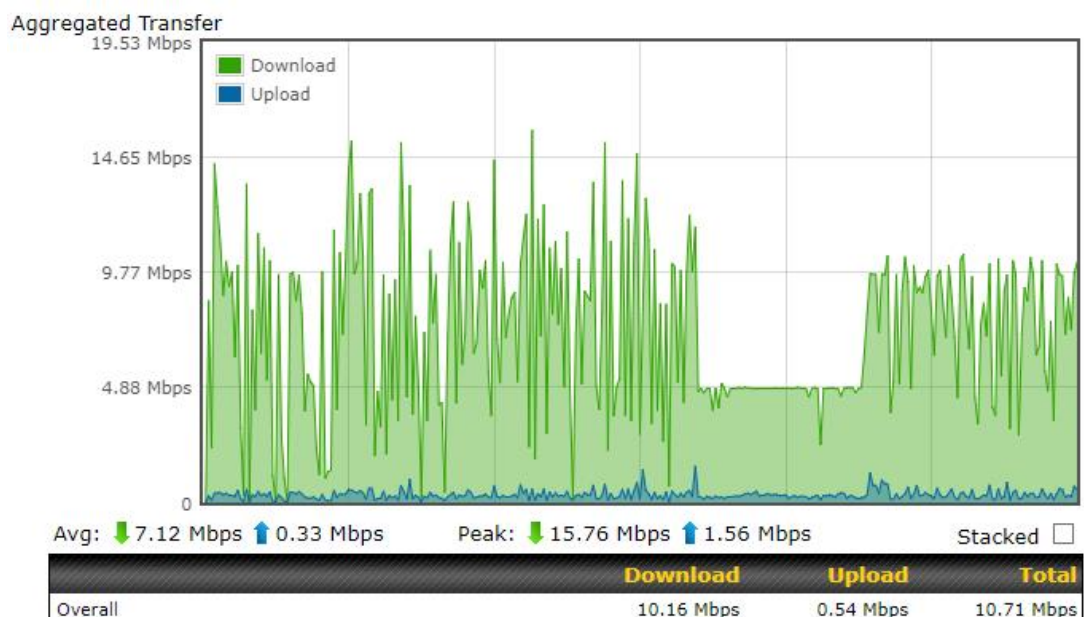


Figura 4.6 Tráfico de descarga total en el escenario 1 realizando pruebas de error.

4.2 Segundo escenario

En este escenario se definió el algoritmo de balanceo “PRIORITY” para conectar cada host de la red LAN un enlace WAN diferente.

El host con la dirección IP 172.168.12.2 tiene al enlace WAN1 como principal y como backup el enlace WAN2; para comprobar alta disponibilidad de acceso a internet en la red, se realizará prueba de fallo (Fail-over) en donde se deshabilitará el enlace WAN1 y automáticamente se conectará la red al enlace WAN2, tal como se muestra en las figuras (4.7, 4.8, 4.9).

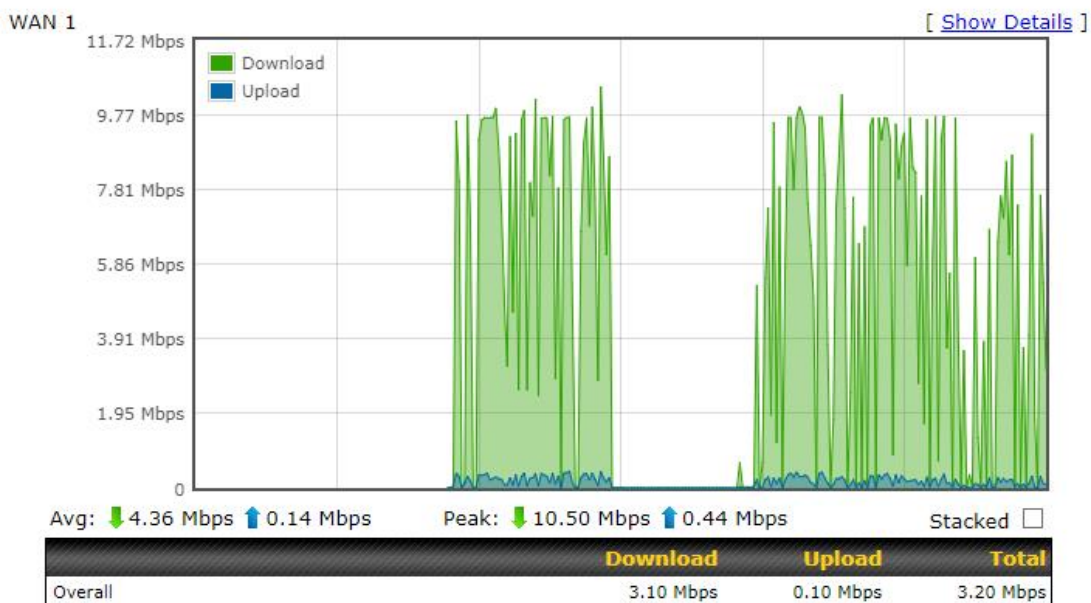


Figura 4.7 Tráfico de descarga del enlace WAN1 en el escenario 2 para PC1.

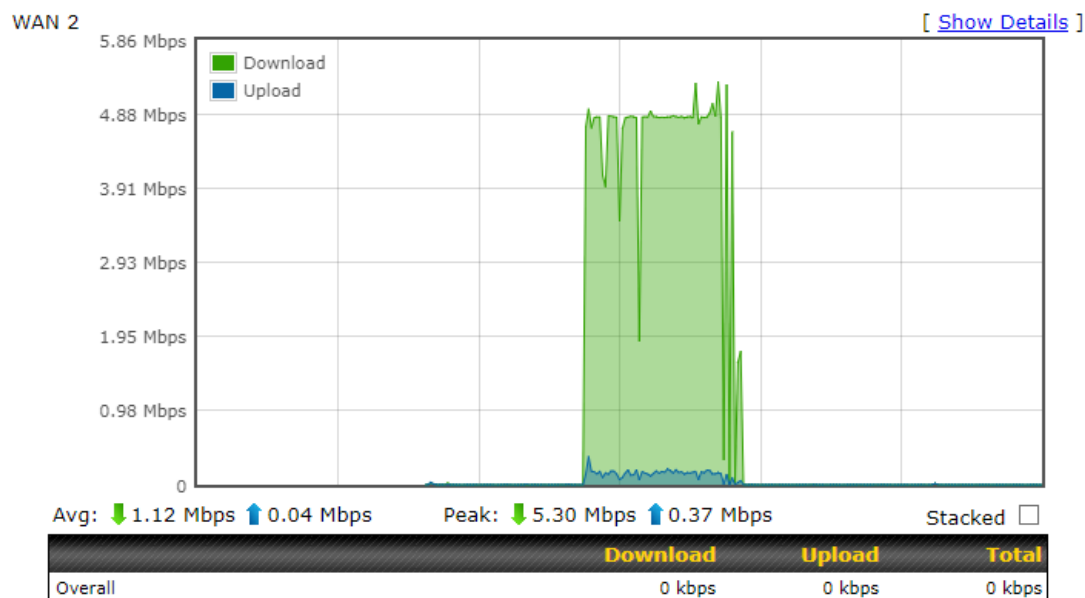


Figura 4.8 Tráfico de descarga del enlace WAN2 en el escenario 2 para PC1.

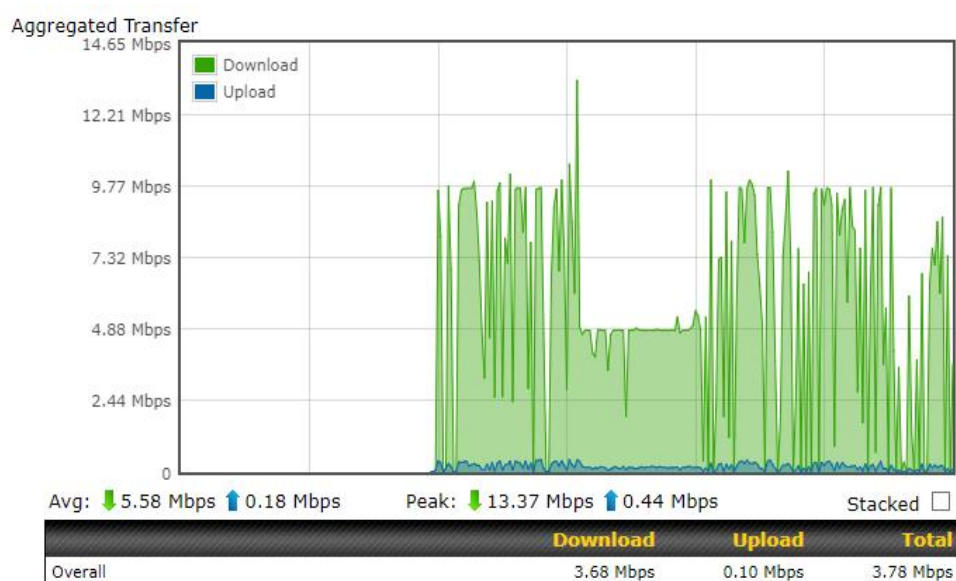


Figura 4.9 Tráfico de descarga total en el escenario 2 para PC1.

El host con la dirección IP 172.168.12.3 tiene al enlace WAN2 como principal y como backup el enlace WAN1; para comprobar la alta disponibilidad de acceso a internet en la red, se realizará prueba de fallo (Fail-over) en donde se deshabilitará el enlace WAN2 y automáticamente se conectará la red al enlace WAN1, tal como se muestra en las figuras (4.10, 4.11, 4.12).

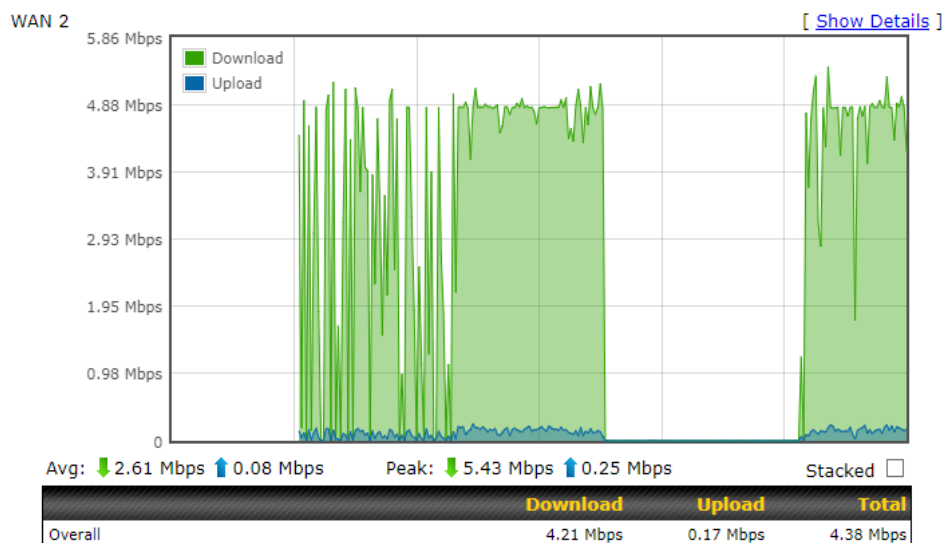


Figura 4.10 Tráfico de descarga del enlace WAN2 en el escenario 2 para PC2.

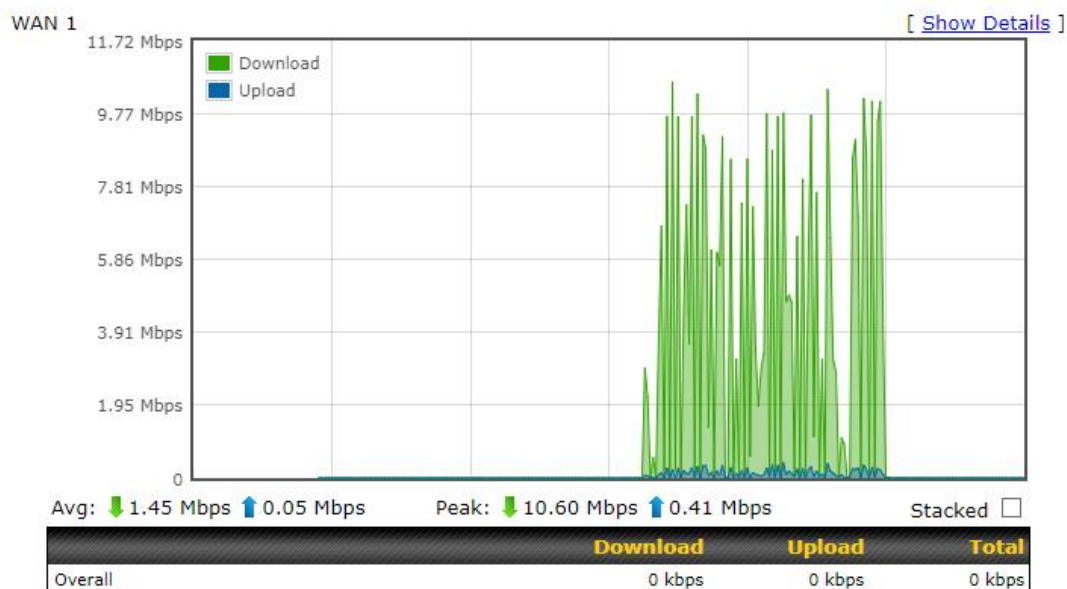


Figura 4.11 Tráfico de descarga del enlace WAN1 en el escenario 2 para PC2.

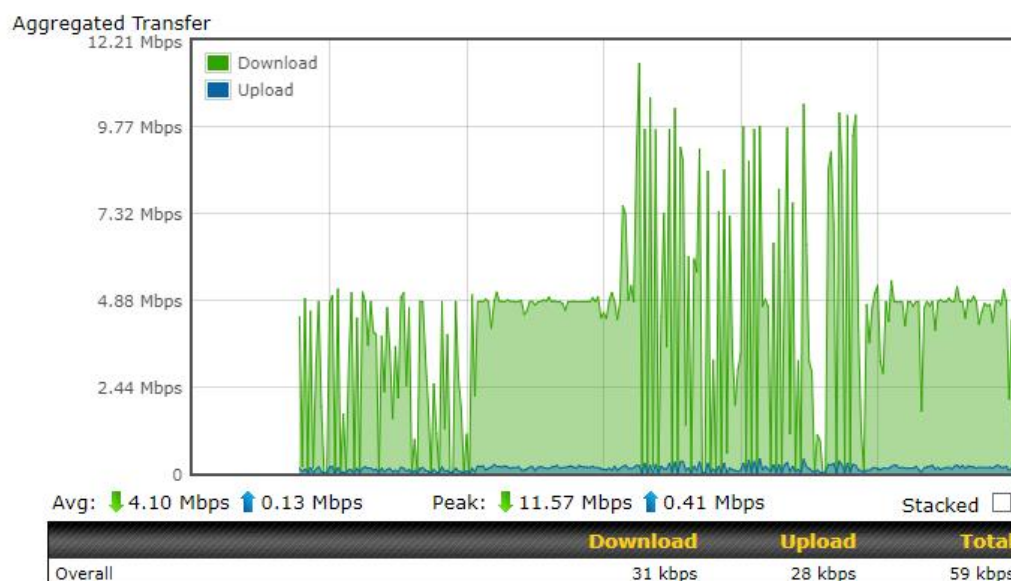


Figura 4.12 Tráfico de descarga total en el escenario 2 para PC2.

4.3 Tercer Escenario

En este escenario se definió el algoritmo de balanceo “PRIORITY” para conectar toda la red LAN al enlace WAN1 manteniendo como backup el enlace WAN2, tal como se muestra en la figura 4.13.

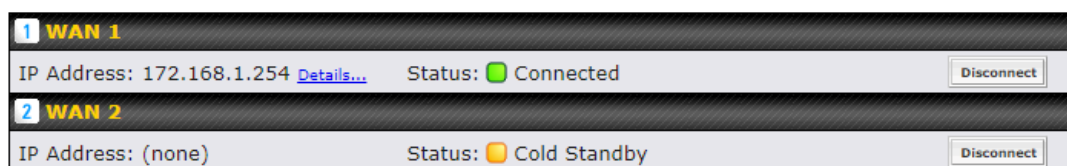


Figura 4.13 Enlace WAN2 en estado de Standby.

Para comprobar la alta disponibilidad de acceso a internet en la red, se realizará prueba de fallo (Fail-over) en donde se deshabilitará el enlace WAN1 y automáticamente se conectará toda la red al enlace WAN2, tal como se muestra en las figuras (4.14, 4.15, 4.16, 4.17).

1 WAN 1	IP Address: (none)	Status: ● Disconnected (Manual)	Connect
2 WAN 2	IP Address: 172.168.2.249 Details...	Status: ● Connected	Disconnect

Figura 4.14 Enlace WAN2 en estado conectado.

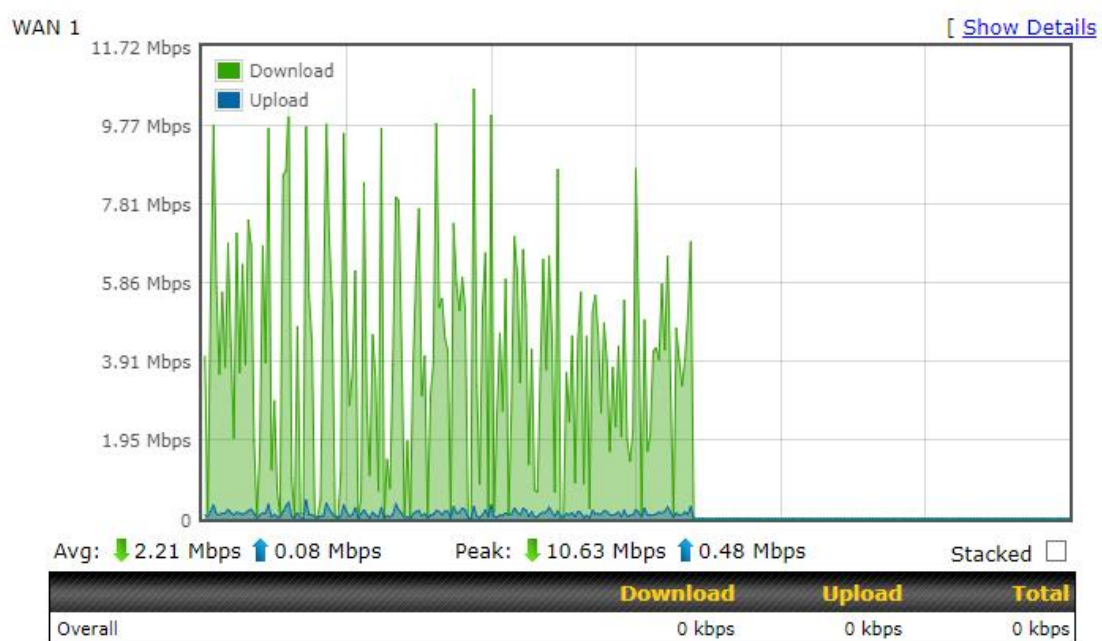


Figura 4.15 Tráfico de descarga del enlace WAN1 en el escenario 3.

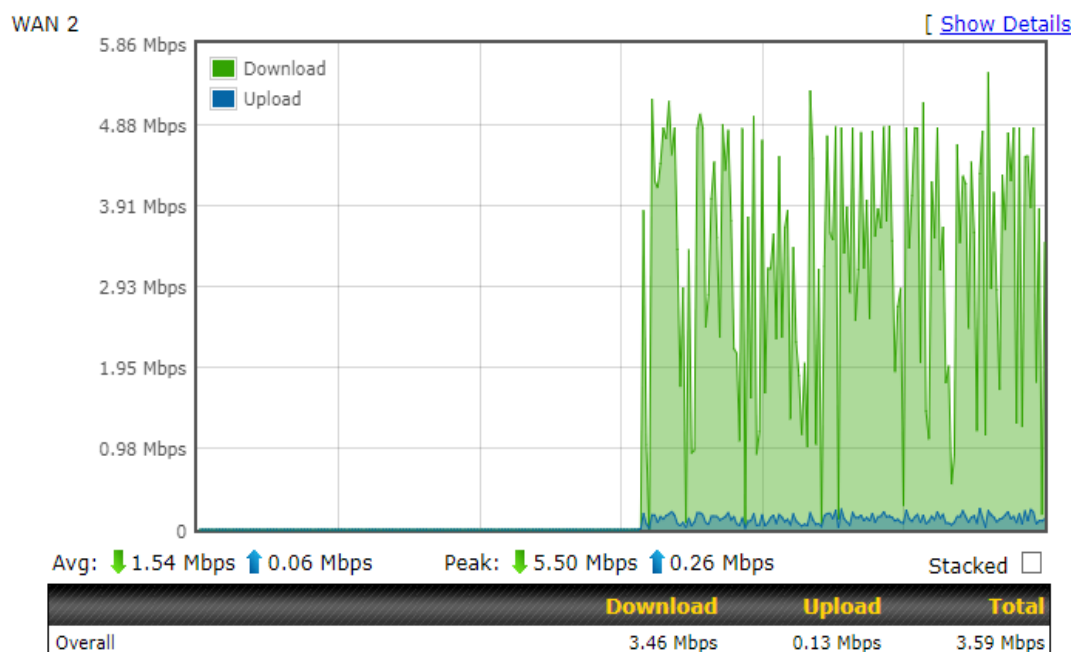


Figura 4.16 Tráfico de descarga del enlace WAN2 en el escenario 3.

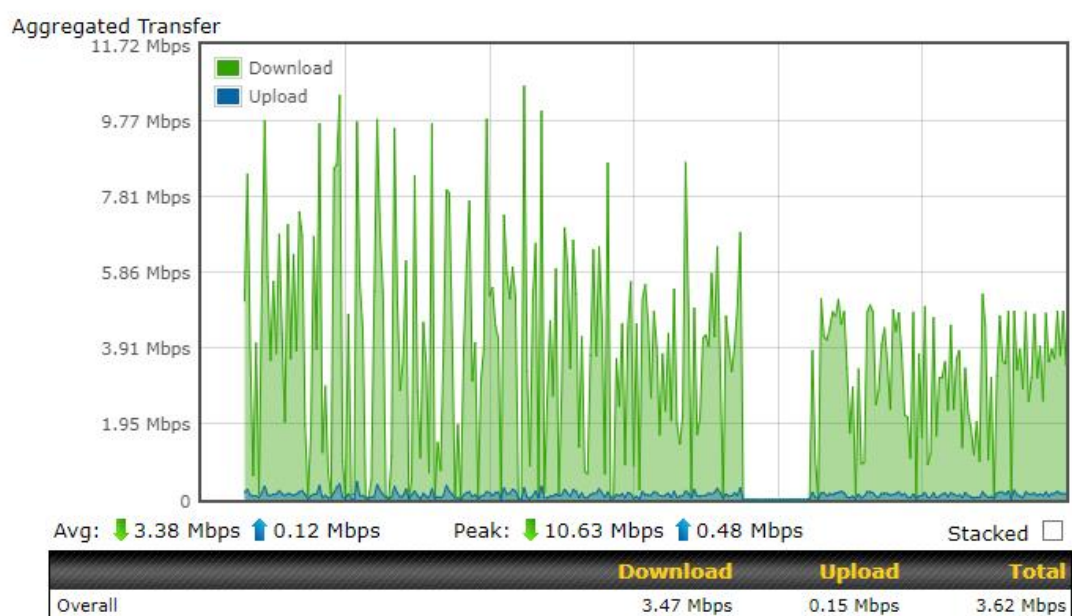


Figura 4.17 Tráfico de descarga total en el escenario 3.

CONCLUSIONES RECOMENDACIONES

El proyecto logra garantizar el acceso continuo a internet para la red LAN utilizando algoritmos de balanceo que vayan acorde a la necesidad de la PYME. Pese a que existen algunas alternativas para brindar alta disponibilidad se fijó un diseño de red en donde se utilizó el balanceador PEPLINK BALANCE 310.

Los tres escenarios fueron elegidos debido a que son los casos más comunes para la administración del ancho de banda dentro de una red LAN.

La solución planteada cuenta con un diseño sencillo que brinda beneficios de monitoreo y control en tiempo real; en donde los equipos propuestos se pueden adquirir fácilmente en el mercado y a costo accesible

Se recomienda realizar un estudio correcto para conocer los requerimientos de administración de la red LAN para elegir adecuadamente el algoritmo de balanceo a implementar.

Conocer todas las funciones, recursos y ventajas que ofrecen los equipos de la red diseñada para configurarlos correctamente evitando problemas en su funcionamiento.

BIBLIOGRAFÍA

- [1] C. Vialfa. (2016, Octubre 17). Alta disponibilidad (3ra ed.) [Online].
Disponibile en: <http://es.ccm.net/contents/634-alta-disponibilidad>
- [2] J. Garzón. (2012, Junio 12). Sistemas distribuidos y cluster (1ra ed.) [Online].
Disponibile en: <https://sites.google.com/site/sistemasdistribuidosycluster/alta-disponibilidad>
- [3] XFINITY (2017, Julio 6). ¿Qué son los proveedores de servicio de Internet? (1ra ed.) [Online].
Disponibile en: <https://es.xfinity.com/hub/internet/internet-service-providers>
- [4] CISCO (2015, Febrero 22). ¿What is firewall? (1ra ed.) [Online].
Disponibile en: <https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html>
- [5] 1&1 (2017, Mayo 2). Servidores (1ra ed.) [Online].
Disponibile en: <https://www.1and1.es/digitalguide/servidores/knowhow/balanceo-de-carga-conoce-a-fondo-sus-ventajas/>
- [6] MIKROTIK (2016, Agosto 18). MIKROTIK RB750 (2ra ed.) [Online].
Disponibile en: <http://www.mikrotik.com/products/group/ethernet-routers>
- [7] XATAKA (2014, Marzo 8). ¿Qué es y cómo funciona NAT? (2ra ed.) [Online].
Disponibile en: <https://www.xataka.com/vodafoneadslafondo/que-es-y-como-funciona-la-nat>

ANEXO A

MANUAL DE USUARIO DEL ROUTER RB750

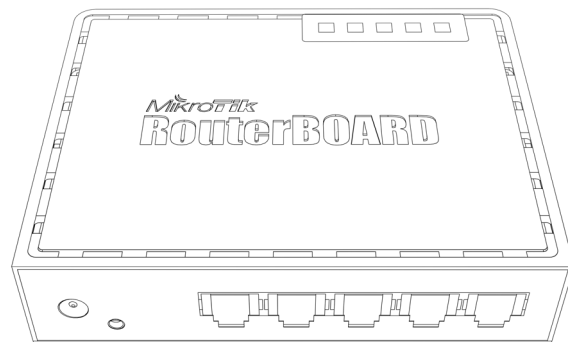
RouterBOARD 750

The RB750 is a low cost Ethernet router. It has five Gigabit Ethernet ports.

Quick Setup Guide and Warranty Information

First use

1. Connect your WAN cable to port 1, and LAN computers to ports 2-5
2. Set LAN computer IP configuration to *automatic* (DHCP)
3. RB750 Default IP address from LAN is 192.168.88.1



Powering

The board accepts powering from the power jack or from the first Ethernet port (Passive PoE):

- Direct-input power accepts 8..28V DC, device comes bundled with a
- First Ethernet port accepts passive Power over Ethernet accepts 8-28V DC

Normally the power consumption of this device is 2.4W, under maximum load - 3.6W

Booting process

RouterOS is the operating system of all RouterBOARD routers. Please see detailed configuration guide here:

<http://wiki.mikrotik.com/wiki/Category:Manual#list>

This device doesn't come fitted with a Serial Port connector, so initial connection has to be done via the Ethernet cable, using the MikroTik Winbox utility. Winbox should be used to connect to the default IP address of **192.168.88.1** with the username **admin** and **no password**.

In case you wish to boot the device from network, for example to use MikroTik Netinstall, hold the RESET button of the device when starting it until the LED light turns off, and Groove will start to look for Netinstall servers.

In case IP connection is not available, Winbox can also be used to connect to the MAC address of the device. More information here: http://wiki.mikrotik.com/wiki/First_time_startup

Extension Slots and Ports

Five individual Gigabit Ethernet ports, supporting automatic cross/straight cable correction (Auto MDI/X), so you can use either straight or cross-over cables for connecting to other network devices. The First Ethernet port accepts 8..28 V DC powering from a passive PoE injector.

Resetting the device

In case you wish to return the RB750 device to its original configuration, you can use the RESET button which is located to the left of the Ethernet ports.

Hold this button during boot time until LED lights start flashing, then release the button to **reset RouterOS configuration**. You can use this procedure if you have forgotten the password to access the device, or simply wish to return the unit to its default configuration state.

Buttons and Jumpers

- RouterOS reset jumper hole (on the bottom of case, behind one of the rubber feet) – resets RouterOS software to defaults. Must short circuit the metallic sides of the hole (with a screwdriver, for example) and boot the device. Hold screwdriver in place until RouterOS configuration is cleared.
- RouterBOOT reset button (RESET, front panel) has two functions:
 - ✓ Hold this button during boot time until LED light starts **flashing**, release the button to **reset RouterOS configuration** (same result as with RouterOS reset hole)
 - ✓ Hold this button during boot time longer, until **LED turns off**, and then release it to make RB750 **look for Net-install servers**.

Operating System Support

Currently tested operating system is MikroTik RouterOS starting from version v5.

Copyright and Warranty Information

Copyright MikroTik SIA. This manual contains information protected by copyright law. No part of it may be reproduced or transmitted in any form without prior written permission from the copyright holder. RouterBOARD, RouterOS, RouterBOOT and MikroTik are trademarks of MikroTik SIA. All trademarks and registered trademarks appearing in this manual are the property of their respective holders.

Hardware. MikroTik warrants all RouterBOARD series equipment for the term of twelve (12) months from the shipping date to be free of defects in materials and workmanship under normal use and service, except in case of damage caused by mechanical, electrical or other accidental or intended damages caused by improper use or due to wind, rain, fire or other acts of nature.

To return failed units to MikroTik, you must perform the following RMA (Return Merchandise Authorization) procedure. Follow the instructions below to save time, efforts, avoid costs, and improve the speed of the RMA process.

1. If you have purchased your product from a MikroTik Reseller, please contact the Reseller Company regarding all warranty and repair issues, the following instructions apply **ONLY** if you purchased your equipment directly from MikroTik in Latvia.
2. We do not offer repairs for products that are not covered by warranty. Exceptions can be made for RB1000, RB1100 and RB1200.
3. Out-of-warranty devices and devices not covered by warranty sent to MikroTik will be returned to the sender at sender's cost.

RMA Instructions are located on our webpage here: <http://rma.mikrotik.com>

Manual. This manual is provided “as is” without a warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of merchantability and fitness for a particular purpose. The manufacturer has made every effort to ensure the accuracy of the contents of this manual; however, it is possible that it may contain technical inaccuracies, typographical or other errors. No liability is assumed for any inaccuracy found in this publication, nor for direct or indirect, incidental, consequential or other damages that may result from such an inaccuracy, including, but not limited to, loss of data or profits. Please report any inaccuracies found to support@mikrotik.com

ANEXO B

MANUAL DE USUARIO DEL PEPLINK BALANCE 310

Peplink Balance Multi-WAN Bonding Routers

User Manual

For Model 20/30/210/310/305/380/580/710/1350/2500

Peplink Balance Firmware 5.4

December 2013



Copyright & Trademarks Specifications are subject to change without prior notice. Copyright © 2013 Peplink International Ltd. All Rights Reserved. Peplink and the Peplink logo are trademarks of Peplink International Ltd. Other brands or products mentioned may be trademarks or registered trademarks of their respective owners.

14.2.1 Algorithm: Weighted Balance

This setting specifies the ratio of WAN connection usage to be applied on the specified IP Protocol & Port, and is applicable only when Algorithm is set to **Weighted Balance**.

Algorithm	<input type="text" value="Weighted Balance"/>
Load Distribution Weight	<p>WAN1 10 <input type="range" value="10"/></p> <p>WAN2 10 <input type="range" value="10"/></p> <p>WAN3 10 <input type="range" value="10"/></p> <p>Mobile Internet 10 <input type="range" value="10"/></p>

The amount of matching traffic that is distributed to a WAN connection is proportional to the weight of WAN connection relative to the total weight. Use the sliders to change each WAN's weight.

Example: With the following weight settings on a Peplink Balance 310:

- WAN1: 10
- WAN2: 10
- WAN3: 5

Total weight is 25 = (10 + 10 + 5)

Matching traffic distributed to WAN1 is 40% = (10 / 25) x 100%

Matching traffic distributed to WAN2 is 40% = (10 / 25) x 100%

Matching traffic distributed to WAN3 is 20% = (5 / 25) x 100%

14.2.2 Algorithm: Persistence

The configuration of Persistent Services is the solution to the few situations where link load distribution for Internet services is undesirable.

For example, many e-banking and other secure websites, for security reasons, terminate the session when the client computer's Internet IP address changes mid-session.

In general, different Internet IP addresses represent different computers. The security concern is that an IP address change during a session may be the result of an unauthorized intrusion attempt. Therefore, to prevent damages from the potential intrusion, the session is terminated upon the detection of an IP address change.

Peplink Balance can be configured to distribute data traffic across multiple WAN connections. Also, the Internet IP depends on the WAN connections over which communication actually takes place. As a result, a LAN client computer behind Peplink Balance may communicate using multiple Internet IP addresses. For example, a LAN client computer behind a Peplink Balance 310 with three WAN connections may communicate on the Internet using three different IP addresses.

With the Persistency feature of PeplinkBalance, rules can be configured to enable client computers to persistently utilize the same WAN connections for e-banking and other secure websites. As a result, a client computer will communicate using one IP address and eliminate the issues.

Algorithm	<input type="text" value="Persistence"/>
Persistence Mode	<input type="radio"/> By Source <input checked="" type="radio"/> By Destination
Load Distribution	<input type="radio"/> Auto <input checked="" type="radio"/> Custom
Load Distribution Weight	<p>WAN1 10 <input type="range" value="10"/></p> <p>WAN2 10 <input type="range" value="10"/></p> <p>WAN3 10 <input type="range" value="10"/></p> <p>Mobile Internet 10 <input type="range" value="10"/></p>

There are two Persistent Modes. One is **by source** and the other **by destination**.

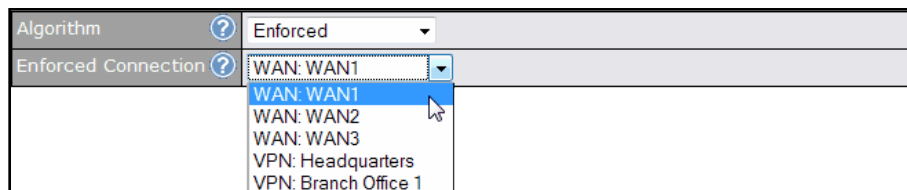
By Source:	The same WAN connection will be used for traffic matching the rule and originating from the same machine regardless of its destination. This option will provide the highest level of application compatibility.
By Destination:	The same WAN connection will be used for traffic matching the rule, originating from the same machine, and going to the same destination. This option can better distribute load to WAN connections when there are only a few client machines.

The default Mode is **By Source**.

When there are multiple client requests, they can be distributed (persistently) to WAN connections with a weight. If you choose **Auto in Load Distribution**, the weights will be automatically adjusted according to each WAN's **Download Bandwidth** which is specified in the WAN settings page (see Section 11 Configuration of WAN Interface(s)). If you choose **Custom**, you can customize the weight of each WAN manually by using the sliders.

14.2.3 Algorithm: Enforced

This setting specifies the WAN connection usage to be applied on the specified IP Protocol & Port, and is applicable only when the Algorithm is set to **Enforced**.

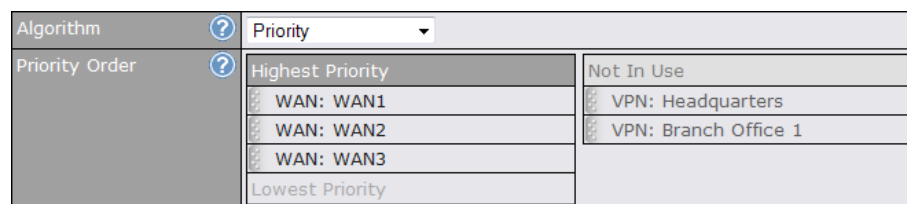


Matching traffic will be routed through the specified WAN connection regardless of health check status of the WAN connection.

Starting from firmware 5.2, outbound traffic can be enforced to go through a specified SpeedFusion™ connection. **(Available on Peplink Balance 210+)**

14.2.4 Algorithm: Priority

This setting specifies the priority of the WAN connections to be utilized to route the specified network service. The highest priority WAN connection available will always be used for routing the specified type of traffic. A lower priority WAN connection will be used only when all higher priority connections have become unavailable.



Starting from firmware 5.2, outbound traffic can be prioritized to go through SpeedFusion™ connection(s). By default, VPN connections are not included in the priority list. **(Available on Peplink Balance 210+)**

Tip

Configure multiple distribution rules to accommodate different kinds of services.

14.2.5 Algorithm: Overflow

The traffic matching this rule will be routed through the healthy WAN connection that has the highest priority and is not in full load. When this connection gets saturated, new sessions will be routed to the next healthy WAN connection that is not in full load.

Algorithm	Overflow
Overflow Order	<div style="border: 1px solid gray; padding: 2px;"> Highest Priority WAN1 WAN2 WAN3 Mobile Internet Lowest Priority </div>

Drag and drop to specify the order of WAN connections to be used for routing traffic. Only the highest priority healthy connection that is not in full load will be utilized.

14.2.6 Algorithm: Least Used

(Available on Peplink Balance 210+)

Algorithm	Least Used
Connection	<input checked="" type="checkbox"/> WAN1 <input checked="" type="checkbox"/> WAN2 <input checked="" type="checkbox"/> WAN3 <input checked="" type="checkbox"/> Mobile Internet

The traffic matching this rule will be routed through the healthy WAN connection that is selected in the field **Connection** and has the most available download bandwidth. The available download bandwidth of a WAN connection is calculated from the total download bandwidth specified in the WAN settings page and the current download usage. The available bandwidth and WAN selection is determined every time when an IP session is made.

14.2.7 Algorithm: Lowest Latency

(Available on Peplink Balance 210+)

Algorithm	Lowest Latency <small>Note: Use of Lowest Latency will incur additional network usage.</small>
Connection	<input checked="" type="checkbox"/> WAN1 <input checked="" type="checkbox"/> WAN2 <input checked="" type="checkbox"/> WAN3 <input checked="" type="checkbox"/> Mobile Internet

The traffic matching this rule will be routed through the healthy WAN connection that is selected in the field *Connection* and has the lowest latency. Latency checking packets are issued periodically to a nearby router of each WAN connection to determine its latency value. The latency of a WAN is the packet round trip time of the WAN connection. Additional network usage may be incurred as a result.

Tip

The round trip time of a “6M down /640k up” link can be higher than that of a “2M down /2M up” link. It is because the overall round trip time is lengthened by its slower upload bandwidth despite of its higher downlink speed. Therefore this algorithm is good for two scenarios:

- All WAN connections are symmetric; or
- A latency sensitive application requires to be routed through the lowest latency WAN regardless the WAN's available bandwidth.