ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES

"ANALISIS DE LOS PROTOCOLOS VRRP Y CARP APLICADO A LA REDUNDANCIA DE GATEWAY USANDO GNU/LINUX PARA LA EMPRESA INFOQUALITY S.A."

TESIS DE GRADO

PREVIA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN ELECTRÓNICA Y COMPUTACIÓN

PRESENTADO POR:

ERIK DAVID ESPINOSA CARRILLO

JORGE STEVEN MONCAYO VALLEJO

RIOBAMBA - 2010

A NUESTRAS FAMILIAS:

Por su inigualable amor, comprensión y sacrificio, que con ternura perdurable han sido el pilar fundamental en nuestras vidas

NOMBREFIRMAFECHA

ING. IVÁN MENES
DECANO DE LA FACULTAD DE INFORMATICA Y ELECTRÓNICA.....

ING. JOSÉ GUERRA
DIRECTORDE ESCUELA DE INGENIERIA ELECTRÓNICA .....

ING.EDWIN ALTAMIRANO
DIRECTORDETESIS ..... ….....

ING. DANILO PASTOR
MIEMBRODELTRIBUNAL.....

LCDO. CARLOS RODRÍGUEZ
DIRECTOR CENTRO DOCUMENTACIÓN.....

NOTADELATESIS….....

“Nosotros, Erik David Espinosa Carrillo y Jorge Steven Moncayo Vallejo, somos responsables de las ideas, doctrinas y resultados expuestos en esta tesis; y, el patrimonio intelectual de la Tesis de Grado pertenece a la ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO”.

Erik David Espinosa Carrillo

Jorge Steven Moncayo Vallejo

ABREVIATURAS

ARP	*AddressResolutionProtocol* (Protocolo de resolución de direcciones)
DHCP	*Dynamic Host ConfigurationProtocol* (Protocolo de configuración dinámica de host)
DISC	DynamicInformationSystemsCorporation (Corporación de Sistemas de Información Dinámica)
DNS	*DomainNameSystem* / Service (Sistema de nombre de dominio)
GNU	*is Not Unix (No es Unix)*
HMAC	Hash-basedMessageAuthenticationCode (Código de Mensaje de Autentificación basado en hash)
HTML	HyperTextMarkupLanguage (Lenguaje de Marcado de Hipertexto)
IANA	Internet AssignedNumbersAuthority (Asiganción de números de Internet)
ICMP	*Internet Control MessageProtocol (Protocolo de Mensajes de Control de Internet)*
IEEE	Institute of Electrical and ElectronicsEngineers (Instituto de Ingenieros Eléctricos y Electrónicos)
IP	Internet Protocol (Protocolo de Internet)
ISP	Internet ServiceProvider (Proveedor de Servicios e Internet)
LAN	Local Area Network (Red de Area Local)
MAC	Media Access Control (Control de Acceso al Medio)
OSPF	*Open ShortestPathFirst (Abrir primero la ruta más corta)*
PHP	***H****ypertext****P****re-processor (Pre - procesador de Hiper Texto)*
RFC	*RequestForComments (Solicitud de comentarios)*
RIP	*RoutingInformationProtocol* (Protocolo de encaminamiento de información)
SHA	*Secure Hash Algorithm (Algoritmo de seguridad de tipo hash)*
TCP	Transmission Control Protocol (Protocolo de Control de Transmisión)
VLAN	Virtual Local Area Network (Red de Área Local Virtual)
WAN	Wide Area Network (Red de Area Amplia)
XML	Extensible MarkupLanguage (Lenguaje de Etiquetado Extensible)

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

INTRODUCCION

La necesidad de una conexión a internet en la actualidad se ha vuelto sumamente importante en los hogares y mucho más para las empresas. El tener un mecanismo transparente para los usuarios que proporcione redundancia en la salida a internet en caso de que esta falle es una característica altamente deseable para la empresa Infoquality S.A.

La implementación de Gateway redundantes supone el estudio de un mecanismo que permita al equipo terminal utilizar el Gateway alternativo en caso de ser necesario. Un protocolo de redundancia de Gateway consiste en un conjunto de reglas usadas por un grupo de computadores para administrar dinámicamente la puerta de enlace predeterminada de una red.Todos los protocolos de redundancia de Gateway se centran en la utilización de una dirección MAC y una dirección IP virtual que definen en conjunto un Gateway Virtual.

Los protocolos de redundancia de Gateway que van a ser analizados en la presente tesis son VRRP y CARP, dichos protocolos reducirán el tiempo medio entre fallos de la salida a internet en la red LAN de la empresa. VRRP y CARP también serán comparados en base a distintas variables e indicadores para determinar cuál de los dos protocolos es el más adecuado como una solución definitiva para Infoquality S.A.

La situación actual de la red LAN de Infoquality S.A. no brinda las facilidades necesarias para el trabajo diario de los empleados por lo que se analizara los requerimientos de los mismos para presentar una solución con un diseño de red LAN y el protocolo de redundancia de Gateway apropiado.

CAPITULO I

MARCO PROPOSITIVO

1.1. ANTECEDENTES

Hoy en día cada vez las empresas dependen más de internet, servicios como correo electrónico, búsqueda de información, mensajería instantánea, etc., y no digamos de aquellas empresas en las que Internet es base fundamental para su trabajo, empresas de seguridad que controlen cámaras IP, servicios de tele mantenimiento y telecontrol entre otras operaciones.

A un particular el hecho de quedarse sin internet a causa de un problema con una avería en la línea telefónica puede suponerle molestias pero normalmente no lleva a graves complicaciones. A una empresa grande o de mediano tamaño puede suponerle unas pérdidas económicas importantes.

En este sentido, agregar un segundo Router con un nuevo enlace de salida a internet con un proveedor diferente, es un esquema de redundancia que se podría ver como una posible solución.

El inconveniente de esto es que sin la utilización de un protocolo de redundancia de Gateway la pérdida de internet en uno de los enlaces requiere cambios en la configuración de equipos de ruteo, computadoras, servidores, etc., teniendo que pasar por este proceso cada vez que la conexión presente problemas y/o cada vez que se desee volver a la configuración predeterminada.

Infoquality S.A. es una empresa que se dedica al desarrollo de portales web basados con tecnologías Open Source. Las soluciones desarrolladas por el equipo de diseñadores y programadores aprovechan al máximo el desarrollo y las tendencias actuales. Dichas soluciones están desplegadas en la tecnología Web 2.0 y con el código de programación HTML, PHP, XML, Javascript, JAVA, AJAX, entre otros.
La empresa también ofrece soluciones en el área de software en Sistemas de Gestión, Sistemas de Administración Empresarial, Sistemas de Banca Electrónica, Web Hosting y Registro de Dominios.

Uno de los problemas más importantes que esta empresa tiene que enfrentar en su día a día es la conectividad a internet. La pérdida de conexión con sus proveedores de servicio de internet ocasiona retrasos en el trabajo lo que conlleva a molestias en sus clientes y en algunos casos la pérdida de dinero.

Infoquality accede a internet por medio de dos proveedores de internet que son Telmex y Transtelco. Haciendo uso de un sistema de redundancia de Gateway sumamente rustico, sin aplicación de protocolos adecuados que se ajusten a las necesidades e infraestructura de la empresa.

Los cambios de configuración en los equipos se los realiza manualmente cada vez que se necesite de una puerta de salida distinta. Este proceso es ejecutado de máquina en máquina al igual que en los servidores que se utilizan dentro de la empresa.

Mientras se soluciona de alguna forma el problema de disponibilidad, en la práctica el diseño aplicado no es el más conveniente ni el más práctico ya que no es transparente para los empleados en la empresa y provoca contrariedades e inconvenientes constantes para volver a la configuración anterior.

1.2. JUSTIFICACIÓN

La redundancia en la salida a Internet, o a cualquier otro tipo de conexión WAN, es una característica altamente deseable en función de brindar a nuestras redes un esquema eficiente de soporte ante eventuales fallos en el proveedor de servicios.

La disponibilidad en las redes requiere un nivel cada vez más elevado, y en lo posible descartar completamente la posibilidad de interrupciones en las operaciones. Es por esto

que la redundancia es una herramienta recurrente de los administradores de red. Algunos ejemplos de redundancia se ven presentes a continuación:

- Suministro de energía (Capa 1)
- Redundancia en capa 2
- Redundancia en capa 3 (Gateway)

En el caso particular de la capa 3, la implementación de Gateway redundantes supone un desafío, ¿Cuál es el mecanismo más transparente que asegura la mayor disponibilidad en la salida de la red o subred?

La implementación de Gateway redundantes supone la creación de una técnica que permita al equipo terminal utilizar una puerta de enlace alternativa en caso de ser necesario.

Para esto existen varios mecanismos posibles:

- ARP Proxy
- ICMP Redirect
- Rutas estáticas
- Rutas dinámicas
- Protocolos dinámicos de administración del Gateway

Son varios los protocolos que permiten administrar dinámicamente la redundancia en la puerta de enlace. Todos ellos se centran en la utilización de una dirección IP y una

dirección MAC virtuales que definen un "Gateway virtual" el que es mantenido merced al intercambio de mensajes de “hello” entro los diferentes dispositivos que están adheridos al mismo Gateway virtual.

Al utilizar protocolos de redundancia obtenemos muchas ventajas como por ejemplo:

- Los protocolos VRRP y CARP pueden operar en una variedad de tecnologías que soportan multi-acceso LAN IP, ya que los mensajes de protocolo son enviados por medio de mecanismos de multidifusión.
- Reducir al mínimo la interrupción de servicios
- Incorpora optimizaciones para un alto rendimiento y disponibilidad a la salida del internet.

Atendiendo la necesidad de la empresa Infoquality S.A. de resolver su problema de acceso y disponibilidad a internet, se ha diseñado el presente proyecto de tesis utilizando protocolos estándar y software libre GNU/Linux.

El aplicar uno de estos protocolos nos ayuda a reducir el MTBF, que es el Tiempo Medio Entre Fallos, típicamente se usa como parte de un modelo que asume que el sistema fallido se repara inmediatamente (el tiempo transcurrido entre perdida y recuperación de conexión es aproximadamente cero), como parte de un proceso de renovación.

Después de realizar un debido análisis y estudio comparativo con los protocolos CARP y VRRP, se elegirá el más adecuado y que mejor se adapte para solventar los requerimientos de la empresa. Al terminar la implementación del sistema redundante, para todos los trabajadores de la empresa la perdida y recuperación de uno de los enlaces al proveedor de servicios de internet será completamente transparente.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Analizar los protocolos VRRP y CARP para seleccionar el más idóneo y aplicar la redundancia de Gateway usando GNU/Linux en la empresa Infoquality S.A.

1.3.2. OBJETIVOS ESPECÍFICOS

- Estudiar la tecnología de redundancia de Gateway.
- Estudiar el funcionamiento de los protocolos VRRP y CARP.
- Proponer un diseño para la red de la empresa.
- Implementar un prototipo de red para cada uno de los protocolos en estudio.
- Realizar el estudio comparativo para seleccionar el protocolo más adecuado.
- Implementar físicamente la red redundante con el protocolo seleccionado en el estudio comparativo.

1.4. HIPÓTESIS

La aplicación de un protocolo de Redundancia adecuado reducirá los porcentajes del Tiempo Medio entre Fallos (MTBF) en la empresa Infoquality S.A

CAPITULO II

MARCO TEORICO

2.1. PROTOCOLOS DE REDUNDANCIA DE GATEWAY

Son varios los protocolos que permiten administrar dinámicamente la redundancia en el Gateway. Todos ellos se centran en la utilización de una dirección IP y una MAC virtuales que definen un "Gateway virtual" el que es mantenido merced al intercambio de mensajes de “hello” entre los diferentes dispositivos que están adheridos al mismo Gateway virtual.

2.1.1. CARACTERÍSTICAS

HSRP - Hot Standby Router Protocol

- Protocolo propietario de Cisco
- Utiliza una IP virtual y define automáticamente una MAC virtual para el clúster.
- Entre los Routers asociados al Router virtual se define un Router activo y otro de respaldo.

- No realiza balanceo de tráfico, solo un Gateway permanece activo mientras los demás están es espera.

VRRP - Virtual Router RedundancyProtocol

- Establecido por el RFC 3768
- Utiliza una IP virtual y define automáticamente una MAC virtual para el clúster.
- Dentro del clúster se elige un Router como activo y todos los demás permanecen como Routers de respaldo.
- No incorpora un mecanismo que permita el balanceo de tráfico entre múltiples Gateway.

GLBP - Gateway Load Balancing Protocol

- Protocolo propietario de Cisco.
- Utiliza una única IP virtual y múltiples direcciones MAC virtuales (una por cada dispositivo que integra el clúster).
- Sólo un dispositivo actúa como máster y responde las solicitudes ARP, pero todos permanecen activos y reenvían el tráfico que está dirigido a la dirección MAC virtual que les ha sido asignada.
- El reenvío de tráfico es realizado por cada uno de los Routers del clúster de acuerdo a la dirección MAC virtual a la cual es enviado el tráfico por la terminal.

CARP – Common Address Redundancy Protocol

- Protocolo creado por el grupo de OpenBSD.
- Permite a varios hosts en la misma red local para compartir un conjunto de direcciones IP.
- Su objetivo principal es proporcionar conmutación por error de redundancia.
- Usado generalmente con servidores de seguridad en conjunto con pfsync.
- Solo una terminal permanece activa mientras las demás se encuentran en estado de respaldo.
- Proporciona balanceo de carga en la LAN mediante análisis de paquetes ARP.

2.2. VRRP

Hay un sin número de métodos para que un terminal final pueda determinar su primer salto hacia una IP particular de un destino. Estos incluyen correr un protocolo de ruteo dinámico como el Protocolo de Información de Ruteo (RIP) u OSPF versión 2 (OSPF), correr un cliente ICMP de descubrimiento de Router (DISC) o usar una ruta por defecto configurada estáticamente.

Correr un protocolo de ruteo dinámico en cada terminal final puede ser inviable por diferentes razones, entre estas podemos incluir gastos generales administrativos, alto procesamiento, problemas de seguridad, o la falta de un protocolo implementado para diferentes plataformas. Protocolos de descubrimiento de vecinos pueden requerir una participación activa de todas las terminales en la red, esto puede resultar en tiempos de convergencia grandes en dependencia del número de terminales en la red, retardo en la

detección de un vecino perdido (ej. muerto), introduce periodos de “agujero negros” sumamente largos e inaceptables.

El uso de una ruta por defecto configurada estáticamente es muy popular; esto minimiza la configuración y el alto procesamiento en la terminal final y esta soportado virtualmente por cada implementación IP. Este modo de operación es probable que persista mientras es desplegado el protocolo de configuración de host dinámico (DHCP), el cual típicamente proporciona configuración de dirección IP y puerta de enlace por defecto para una terminal final. Sin embargo, esto provoca un punto de fallo único. La pérdida de la puerta de enlace por defecto resultaría en un evento catastrófico, aislando todas las terminales finales que no serán capaces de detectar un camino alternativo que podría estar disponible.

El Protocolo de Redundancia de Router Virtual (VRRP) es designado para eliminar el punto de fallo único heredado del ambiente de ruta por defecto configurada estáticamente. VRRP especifica un protocolo de elección que dinámicamente asigna responsabilidad sobre un Router virtual a uno de los Routers VRRP en una red LAN. El Router VRRP controlando la(s) dirección(es) IP asociadas con un Router virtual es llamado el Router Maestro, y reenvía los paquetes enviados a esta(s) dirección(es) IP. El proceso de elección dinámica proporciona conmutación por error en la responsabilidad de reenvió de paquetes si el Router Maestro no está disponible. Cualquiera de las direcciones IP virtuales de un Router en la red LAN podrán entonces ser usadas como el Router de primer salto por las terminales finales. La ventaja obtenida por usar VRRP es una más alta disponibilidad de un

camino por defecto sin la necesidad de configuración de un protocolo de ruteo dinámico o protocolos de descubrimiento de Router en cada terminal final.

VRRP proporciona una función similar al protocolo propietario de Cisco Sytems Inc., llamado Protocolo de Ruteo de Espera en Caliente (HSRP) y al protocolo propietario de Digital EquipmentCorporation Inc., llamado Protocolo IP en Espera (IPSTB).

2.2.1. VISIÓN GENERAL DEL PROTOCOLO VRRP

VRRP especifica un protocolo de elección para realizar la función de Router Virtual descrita anteriormente. Todo el proceso de envió de mensajes de protocolo se realiza mediante datagramas IP de multidifusión, de esta manera el protocolo puede operar sobre una variedad de tecnologías LAN de acceso múltiple que soportan IP multidifusión. Cada Router Virtual VRRP tiene una única dirección MAC bien conocida que es asignada a él. Dado el ambiente en el que se aplicara el presente trabajo este documento solo cubrirá el mapeo de redes que hacen uso de direcciones MAC de 48-bit IEEE 802. La dirección MAC del Router Virtual es usada como la fuente de todos los mensajes VRRP periódicos enviados por el Router Maestro para permitir el aprendizaje de un puente en una red LAN extendida.

Un Router Virtual es identificado por un Identificador de Router Virtual (VRID) y un conjunto de direcciones IP. Un Router VRRP puede asociar a un Router Virtual con su dirección real de interfaz, y puede también ser configurado con asignaciones adicionales de

Router Virtual y la prioridad de Routers Virtuales que está dispuesto a respaldar. El mapeo entre el VRID y las direcciones IP deben ser coordinadas entre todos los Routers VRRP en la red LAN.

Sin embargo no hay ninguna restricción en contra de la reutilización de un VRID con una asignación de una dirección IP diferente en una red LAN distinta. El alcance de cada Router virtual se limita a una sola red LAN.

Para minimizar el tráfico de red, solo el Maestro de cada Router Virtual envía mensajes periódicos de anuncio VRRP. Un Router de respaldo no intentara anticiparse a un Maestro a menos que tenga una mayor prioridad. Esto elimina la interrupción del servicio a menos que una mejor ruta esté disponible. También es posible prohibir administrativamente todos los intentos de anticipación. La única excepción es que un Router VRRP siempre se convertirá en Maestro de cualquier Router Virtual asociado con direcciones IP de su propiedad. Si el Maestro no está disponible entonces el Router de respaldo con la más alta prioridad hará la transición a Maestro después de una breve demora, proporcionando una transición controlada de la responsabilidad de Router Virtual con una mínima interrupción del servicio.

VRRP define tres tipos de autenticación proveyendo una sencilla implementación en ambientes inseguros, mayor protección en contra de configuraciones erróneas, y fuerte autenticación de remitente en ambientes con conciencia en la seguridad. Además nuevos

tipos de autenticación y datos pueden ser definidos en el futuro, sin afectar el formato de la parte fija del paquete del protocolo, preservando así una compatibilidad hacia atrás.

El diseño del protocolo VRRP proporciona una rápida transición de Router de respaldo a Router Maestro para minimizar la interrupción del servicio, e incorpora optimizaciones que reducen la complejidad del protocolo garantizando la transición controlada de Router Maestro para escenarios típicos de funcionamiento. Las optimizaciones resultan en un protocolo de elección con requisitos mínimos de estado de tiempo de ejecución, mínimos estados activos del protocolo, y un tipo único de mensaje y remitente. Los escenarios típicos de funcionamiento se definen como dos Routers redundantes y/o caminos distintos entre cada enrutador. Un efecto secundario que se produce cuando se violan estos supuestos escenarios típicos (ej. Más de dos caminos redundantes con igualdad de preferencia) es que paquetes duplicados pueden ser reenviados por un breve periodo de tiempo mientras se realiza la elección de Router Maestro. Sin embargo, las hipótesis de escenarios típicos probablemente cubrirán la gran mayoría de implementaciones, la pérdida del Router Maestro no es frecuente, y la duración prevista en la convergencia de la elección de Router Maestro es bastante pequeña (aproximadamente << 1 segundo). Así, las optimizaciones de VRRP representan una notable simplificación en el diseño del protocolo, incurriendo en una insignificante probabilidad de una breve degradación de la red.

2.2.2. EJEMPLO DE CONFIGURACIONES

CONFIGURACIÓN 1

La siguiente figura muestra una red simple con dos Routers VRRP implementando un Router Virtual. Este es solo un ejemplo para ayudar al entendimiento del protocolo y puede que en una práctica real no ocurra.

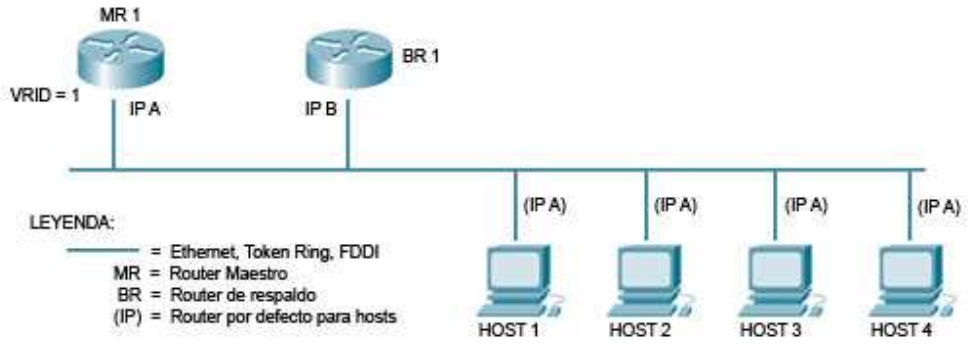


Figura II.1: Esquema uno de configuración VRRP.

La configuración anterior muestra un escenario VRRP muy simple. En esta configuración, las terminales finales instalan una ruta por defecto a la dirección IP del Router Virtual #1 (IP A) y ambos Routers corren VRRP. El Router en la izquierda se convierte en Router Maestro para el Router Virtual #1 (VRID = 1) y el Router en la derecha es el de respaldo para el Router Virtual #1. Si el Router en la izquierda debería fallar, el de la derecha tomaría control sobre el Router Virtual #1 y sus direcciones IP, y proveerá servicio ininterrumpido para las terminales.

Nótese que en este ejemplo, IP B no es respaldada por el Router en la izquierda. IP B es únicamente usado por el Router en la derecha como su dirección de interfaz. En orden para respaldar IP B, un segundo Router virtual debería ser configurado.

CONFIGURACIÓN 2

La siguiente figura muestra una configuración con dos Routers Virtuales con las terminales dividiendo el tráfico entre ellos. De este ejemplo se espera que sea muy común en práctica real.

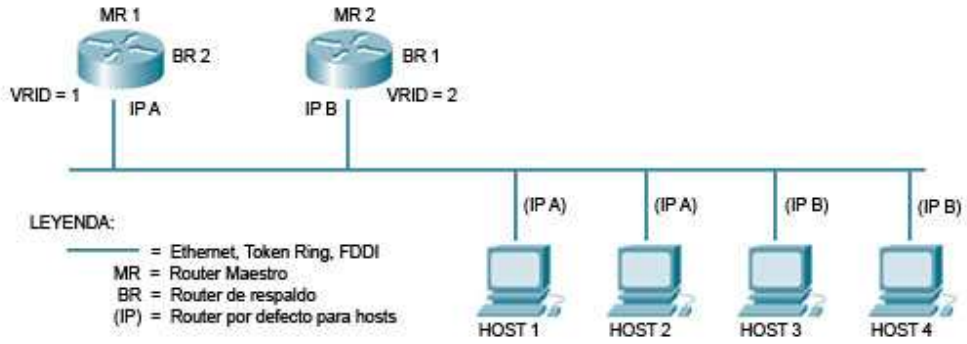


Figura II.2: Esquema dos de configuración VRRP

En la configuración anterior, la mitad de las terminales instalan como puerta determinada por defecto a la dirección IP del Router Virtual numero 1 (IP A), y la otra mitad de los terminales instalan como puerta determinado por defecto la dirección IP del Router Virtual numero 2 (IP B). Esto tiene el efecto de balanceo de carga para el tráfico saliente, así como también provee completa redundancia de Gateway.

2.2.3. PROTOCOLO

El propósito del paquete VRRP es comunicar a todos los Routers VRRP la prioridad y el estado del Router Maestro asociados con la identificación (ID) del Router Virtual.

Los paquetes VRRP están encapsulados en paquetes IP. Estos son enviados por multidifusión a la dirección IP versión 4 (IPv4) asignada a VRRP.

2.2.4. FORMATO DEL PAQUETE VRRP

Esta sección define el formato de un paquete VRRP y los campos relevantes en la cabecera IP.

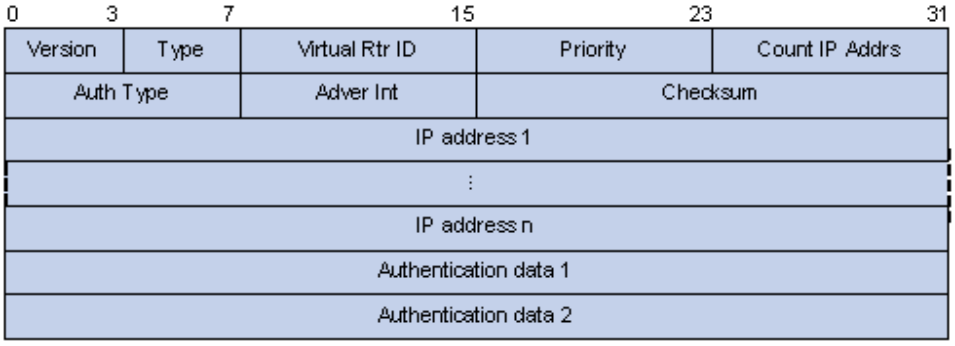


Figura II.3: Formato paquete VRRP.

2.2.5. DESCRIPCIÓN DE CAMPOS IP

Dirección de origen.- La dirección IP primaria de la interfaz de la cual es enviado el paquete.

Dirección de destino.- La dirección IP de multidifusión que es asignada por la IANA para VRRP:

224.0.0.18

Esta dirección de multidifusión es un vínculo de ámbito local. Los Routers no deben remitir un datagrama con esta dirección de destino, independientemente de su TTL.

TTL.- El TTL debe ser establecido a 255. Un Router VRRP que reciba un paquete con un TTL que no sea igual a 255 debe descartarlo.

Protocolo.- El número de protocolo IP asignado por la IANA para VRRP es 112 en decimal.

2.2.6. DESCRIPCIÓN DE CAMPOS VRRP

Versión.- El campo de versión especifica la versión de protocolo VRRP de este paquete. Podría ser versión 2 o versión 3 en el caso de requerir soporte para IPv6.

Tipo.- El campo tipo define cuál es el tipo de paquete VRRP. El único tipo de paquete definido en esta versión del protocolo es:

1. ADVERTISEMENT

Un paquete con un tipo desconocido debe ser descartado.

Identificación de Router Virtual (VRID).- El campo identificador de Router Virtual identifica el Router Virtual para el cual el paquete está reportando el estado.

Prioridad.- El campo de prioridad especifica la prioridad de envió de paquetes VRRP para el Router Virtual. Valores elevados significan prioridad alta. Este es un campo de entero de 8 bit sin signo.

El valor de prioridad para el Router VRRP que posee las direcciones IP asociadas con las del Router Virtual debe ser de 255 en decimal.

Routers VRRP que estén respaldando a un Router Virtual deben usar un valor de prioridad de 1 a 254 en decimal. El valor de prioridad por defecto para Routers VRRP que estén respaldando a un Router Virtual es de 100 en decimal.

El valor de prioridad cero (0) tiene un significado especial, indicando que el Router Maestro actual ha dejado de participar en el proceso VRRP. Esto es usado para disparar Routers de respaldo en el proceso de transición a Maestro sin tener que esperar por el Router Maestro actual agote su tiempo de publicidad.

Contador de direcciones IP (Count IP Addrs).- El número de direcciones IP contenidas en este anuncio VRRP.

Tipo de autenticación.- El campo de autenticación identifica el método de autenticación que está siendo utilizado. El tipo de autenticación es único por cada interfaz. El campo de autenticación es un entero de 8 bit sin signo. Un paquete con un tipo de autenticación desconocido o que no coincide con la autenticación que ha sido configurada en la interfaz debe ser descartado.

Los métodos de autenticación que están actualmente definidos son:

0 - No autenticación

1 - Contraseña simple en texto plano

2 - Autenticación de cabecera IP

No autenticación

El uso de este tipo de autenticación significa que los intercambios del protocolo VRRP no son autenticados. Los contenidos de los datos del campo de autenticación deberán ser establecidos en cero en la transmisión e ignorados en la recepción.

Contraseña simple en texto plano

El uso de este tipo de autenticación significa que los intercambios del protocolo VRRP son autenticados por una contraseña sin cifrado. Los contenidos de los datos en el campo de autenticación deberán ser establecidos con la contraseña configurada localmente en la transmisión. No existe contraseña por defecto. El receptor deberá revisar que los datos de

autenticación coinciden con la cadena de autenticación configurada localmente. Los paquetes que no coinciden deberán ser descartados.

Nótese que existen implicaciones de seguridad en la utilización de una contraseña en texto plano para la autenticación del intercambio de paquetes VRRP.

Autenticación por cabecera IP

El uso de este tipo de autenticación significa que el protocolo VRRP intercambiara paquetes usando los mecanismos definidos por la Autenticación de Cabecera IP (AUTH) usando "HMAC-MD5-96 dentro de ESP y AH" (HMAC) para su autenticación. Las llaves podrían ser configuradas manualmente o por un protocolo de distribución de llaves.

Si un paquete es recibido y no pasa la revisión de autenticación debido a una falta de autenticación por cabecera o una des concordancia en el mensaje encriptado de autenticación, el paquete deberá ser descartado. Los contenidos de los datos del campo de autenticación deberán ser establecidos en cero en la transmisión e ignorados en la recepción.

Intervalo de publicidad (AdvertInt).- El intervalo de publicidad indica el intervalo de tiempo (en segundos) entre avisos de publicidad. Por defecto es 1 segundo. Este campo es usado para solucionar problemas en Routers mal configurados.

Suma de Comprobación.- El campo de suma de comprobación es usado para detectar si existe corrupción en los datos de un mensaje VRRP.

La suma de comprobación es el complemento a uno de 16 bit de la suma en complemento a uno de todo el mensaje VRRP empezando por el campo de versión. Para calcular la suma de comprobación el campo de control se establece en cero.

Direcciones IP.- Una o más direcciones IP que están asociadas a un Router Virtual. El número de direcciones incluidas está especificado en el campo "Contador de direcciones IP". Estos campos son usados para solucionar problemas en Routers mal configurados.

Datos de autenticación.- La cadena de autenticación es únicamente utilizada en la autenticación por contraseña en texto plano, es similar a la autenticación de texto simple encontrado en el protocolo de ruteo Primero el Camino Abierto más Corto (OSPF). Consta hasta de ocho caracteres en texto plano. Si es configurada una cadena de autenticación menor a ocho caracteres (8 byte), el resto de bytes deberá ser rellenado con ceros. Cualquier paquete VRRP recibido que no concuerde con la cadena de autenticación configurada localmente deberá ser descartado. La cadena de configuración es única por cada interfaz configurada.

No hay valor por defecto para este campo.

2.2.7. ESTADO DEL PROTOCOLO POR MAQUINA

PARÁMETROS

Parámetros por interfaz

Tipo de autenticación.- El tipo de autenticación que está siendo usado. Los valore están definidos en la sección x.x.x.x

Datos de autenticación.- Los datos de autenticación específicos para el tipo de autenticación que está siendo usado.

Parámetros por Router virtual

VRID.- Identificador de Router Virtual. Dato configurado en el rango de 1 a 255 en decimal. No existe valor por defecto.

Prioridad.- Valor de prioridad que será utilizado por este Router Virtual. El valor de 255 en decimal está reservado para el Router que tiene propiedad sobre las direcciones IP asignadas al Router Virtual. El valor de 0 (cero) es reservado al Router Maestro para indicar que se libera de responsabilidad sobre el Router Virtual. El rango entre 1 a 254 en decimal está disponible para los Routers VRRP de respaldo del Router Virtual. El valor por defecto es de 100 en decimal.

Direcciones IP.- Una o más direcciones IP asociadas a este Router Virtual. Este campo es configurado y no posee un valor por defecto.

Intervalo de Publicidad (Advertisement_Interval).- Es el intervalo en segundos para envió de publicaciones VRRP. El valor por defecto es de 1 segundo.

Tiempo de Rasgado (Skew_Time).- Tiempo para rasgar el Intervalo de Caída Maestro en segundos. Calculado como:

((256 – Prioridad) / 256)

Intervalo de Caída Maestro (Master_Down_Interval).- Intervalo de tiempo para que un Router de respaldo de por declarado un Router Maestro como caído. Calculado como:
(3 * Intervalo de Publicidad) + Tiempo de Rasgado

Modo de adelantamiento (Preempt_Mode).- Controla si es que un Router de respaldo con una prioridad más alta debería adelantarse a un Router Maestro con prioridad baja. Los valores pueden ser de verdadero para permitir el adelantamiento y de falso para prohibir adelantamiento. Por defecto es verdadero.

La excepción de este comportamiento es cuando un Router que posee las direcciones IP asociadas con un Router Virtual siempre se adelanta independientemente de la configuración de este valor.

TEMPORIZADORES

Temporizador de Caída Maestro (Master_Down_Timer).- Es un temporizador que se activa cuando un aviso de publicidad no ha sido escuchado para este intervalo.

Temporizador de Aviso de Publicidad (Adver_Timer).- Temporizador que se activa para disparar el envío de avisos de publicidad basado en el intervalo de aviso de publicidad.

2.2.8. DIAGRAMA DE TRANSICIÓN DE ESTADO

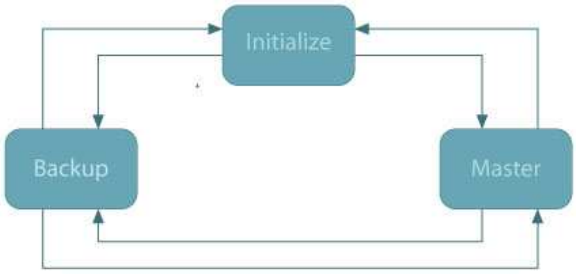


Figura II.4: Diagrama de Transición de Estado VRRP.

DESCRIPCIONES DE ESTADOS

Un Router VRRP hace una implementación del estado de máquina para cada elección de Router Virtual en la que participa.

ESTADO DE INICIALIZACIÓN

El propósito de este estado es el de esperar por un evento de inicio. Si un evento de inicio es recibido entonces:

- Si la prioridad es igual a 255 (ej. El Router es dueño de las direcciones IP asociadas con el Router Virtual)
    - Enviar un mensaje de Publicidad.
    - Difundir una petición ARP gratuita conteniendo la dirección MAC del Router Virtual para cada dirección IP asociada con el Router Virtual.
    - Establecer el Adver_Timer como Advertisement_Interval.
    - Hacer transición al estado de Maestro.

- Si la prioridad no es igual a 255
    - Establecer el Master_Down_Timer como Master_Down_Interval.
    - Hacer transición al estado de Respaldo.

ESTADO DE RESPALDO

El propósito del estado de Respaldo es de monitorear el estado y la disponibilidad del Router Maestro.

Mientras se esté en este estado, un Router VRRP debe hacer lo siguiente:

- No debe responder a peticiones ARP de las direcciones IP asociadas con el Router Virtual.
- Debe descartar paquetes destinados a la capa de enlace con dirección MAC igual a la dirección MAC del Router Virtual.

- No debe aceptar paquetes direccionados a cualquiera de las direcciones IP asociadas con el Router Virtual.
- Si un evento de cierre es recibido, entonces:
    - Cancelar el Master_Down_Timer.
    - Hacer transición al estado de Inicialización.

- Si se dispara el Master_Down_Timer, entonces:
    - Enviar un mensaje de Publicidad.
    - Difundir una petición ARP gratuita conteniendo la dirección MAC del Router Virtual para cada dirección IP asociada con el Router Virtual.
    - Establecer Adver_Timer como Advertisment_Interval.
    - Hacer transición al estado Master.
- Si un mensaje de Publicidad es recibido, entonces:
    - Si la prioridad en el mensaje de publicidad es cero, entonces:
        - Establecer el Master_Down_Timer como Skew_Time.
    - Si la prioridad del mensaje de publicidad es diferente de cero, entonces:
        - Si el modo de Adelantamiento (Preempt_Mode) es falso, o si la prioridad en el mensaje de Publicidad es mayor o igual a la prioridad local, entonces:
            - Reiniciar el Master_Down_Timer a Master_Down_Interval.
        - Sino:
            - Desechar el mensaje de Publicidad.

ESTADO MAESTRO

Mientras que en el estado Maestro el Router funciona como un Router de reenvió para las direcciones IP asociadas con el Router Virtual.

En este estado un Router VRRP debe hacer lo siguiente:

- Debe responder a las peticiones ARP para las direcciones IP asociadas con el Router Virtual.
- Debe reenviar paquetes que tengan como destino en la capa de enlace una dirección MAC igual a la dirección MAC del Router Virtual.
- No debe aceptar paquetes direccionados a las direcciones IP asociadas con el Router Virtual si no es el dueño de estas direcciones.
- Debe aceptar paquetes direccionados a las direcciones IP asociadas con el Router Virtual si él es dueño de las mismas.
- Si un evento de cierre es recibido, entonces:
    - Cancelar el Advert_Timer.
    - Enviar un mensaje de Publicidad con prioridad de cero.
    - Hacer una transición al estado de Inicialización.
- Si se dispara el Advert_Timer, entonces:
    - Enviar un mensaje de Publicidad.
    - Reiniciar el Advert_Timer a Advertisement_Interval.
- Si un mensaje de Publicidad es recibido, entonces:
    - Si la prioridad del mensaje de Publicidad es cero, entonces:
        - Enviar un mensaje de Publicidad.

        - Reiniciar el Advert_Timer a Advertisement_Interval.
    - Si la prioridad del mensaje de Publicidad es mayor que la prioridad local o si la prioridad en el mensaje de Publicidad es igual a la prioridad local y la dirección IP primaria del remitente es mayor que la prioridad de la dirección IP local, entonces:
        - Cancelar Advert_Timer.
        - Establecer Master_Down_Timer como Master_Down_Interval.
        - Hacer transición al estado de Respaldo.
    - Sino:
        - Descartar mensaje de Publicidad.

2.2.9. ENVIÓ Y RECEPCIÓN DE PAQUETES VRRP

RECEPCIÓN DE PAQUETES VRRP

Las siguientes funciones son ejecutadas cuando un paquete VRRP es recibido:

- Se verifica que el TTL IP es 255.
- Verifica la versión VRRP.
- Se verifica que la longitud del paquete recibido es mayor o igual que la cabecera VRRP.
- Comprueba la suma de redundancia cíclica VRRP.
- Realiza el tipo de autenticación especificado por AuthType.
- Se comprueba que el VRID es válido por la interfaz que se recibió.
- Se debe verificar que las direcciones IP asociadas con el VRID son válidas.

- Debe verificar que el Advert_Interval en el paquete es el mismo que el configurado localmente para este Router Virtual.

Si alguna de las verificaciones anteriores falla, entonces el receptor debe descartar el paquete, debería registrar el evento e indicarlo mediante algún administrador de red SMNP que fue detectado alguna configuración errónea.

TRANSMISIÓN DE PAQUETES VRRP

Las operaciones que se realizan para la transmisión de un paquete VRRP son:

- Se llenan los campos en el paquete VRRP con las configuraciones apropiadas para el estado del Router Virtual.
- Se calcula la suma de comprobación VRRP.
- Establece la dirección MAC de origen con la dirección MAC del Router Virtual.
- Establece la dirección IP de origen con la dirección IP primaria de la interfaz.
- Se establece el protocolo IP como VRRP.
- Se envía el paquete VRRP a la dirección IP de multidifusión del grupo VRRP.

Los paquetes VRRP son transmitidos con la dirección MAC del Router Virtual como dirección MAC de origen para asegurar que el proceso de aprendizaje de los puentes correctamente determine a cual segmento de red del Router Virtual está conectado.

2.2.10. DIRECCIÓN MAC DE ROUTER VIRTUAL

La dirección MAC asociada al Router Virtual es una dirección MAC IEEE 802 en el siguiente formato:

00-00-5E-00-01-{VRID} (hexadecimal en formato bit-order estándar de internet)

Los primeros tres octetos son derivados de la IANA OUI. Los siguientes dos octetos (00-01) indican el bloque de direcciones asignadas al protocolo VRRP. VRID es el identificador de Router Virtual VRRP. Este mapeo provee direcciones hasta para 255 Routers VRRP en una red.

2.3. CARP

El Protocolo de Redundancia de Dirección Común o CARP es un protocolo que permite a varios terminales en la misma red local para compartir un conjunto de direcciones IP. Su objetivo principal es proporcionar redundancia contra fallos en la puerta de enlace.

El uso más común de CARP es el de crear un grupo de firewalls redundantes. Por ejemplo, si hay un solo equipo que ejecute un filtrado de paquetes, y se cae, entonces o bien las redes a ambos lados del filtro de paquetes ya no podrán comunicarse entre sí, o se comunicaran sin ningún tipo de filtrado de paquetes.

Sin embargo, si hay dos equipos con un filtro de paquetes ejecutando CARP, si uno falla, el otro entrar a funcionar en lugar del caído y se hará cargo de su operación, y los equipos de ambos lados del filtro de paquetes no se darán cuenta del error. Así que la operación

continuará de forma normal. Con el fin de asegurarse de que el nuevo terminal maestro funciona igual que el anterior, se utiliza la herramienta pfsyncd.

En algunas configuraciones CARP también puede proporcionar la funcionalidad de balanceo de carga. Un grupo de terminales usando CARP toma el nombre de "grupo de redundancia". Al grupo de redundancia se asigna una dirección IP que se comparte o se divide entre los miembros del grupo. Dentro de este grupo, un terminal es designado como "maestro" mientras que los otros miembros son llamados "terminales de respaldo". El terminal principal es el que toma la dirección IP virtual compartida. Responde a cualquier tráfico o petición ARP que sea dirigido a esta dirección. Cada terminal puede pertenecer a varios grupos de redundancia.

Cabe señalar que cada equipo debe tener una segunda dirección IP única. Un uso común del Protocolo de Redundancia de Dirección Común (CARP) es la creación de un grupo de servidores de seguridad redundantes (Firewall). La dirección IP virtual asignada al grupo de redundancia es configurada como la dirección de salida por defecto (Gateway) en los equipos detrás de este grupo de servidores de seguridad. Si el Firewall principales se daña o se desconecta de la red, la dirección IP virtual será tomada por un Firewall dentro de los terminales de respaldo y la disponibilidad del servicio no será interrumpido.

2.3.1. FORMATO DEL PAQUETE CARP

El formato de un paquete CARP es muy parecido al de un paquete VRRP, a continuación describiremos los campos más importantes de este paquete.

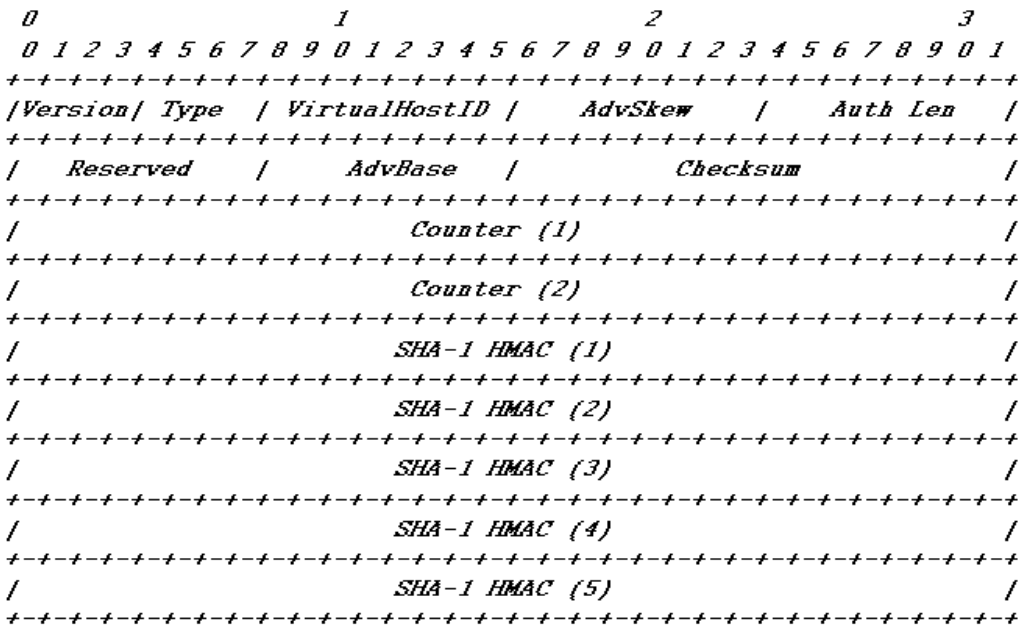


Figura II.5: Formato paquete CARP.

2.3.2. DESCRIPCIÓN DE CAMPOS IP

Dirección de origen.- La dirección IP primaria de la interfaz de la cual es enviado el paquete.

Dirección de destino.- La dirección de destino será la dirección de multidifusión 224.0.0.18.

TTL.- El valor del tiempo de vida del paquete será establecido en 255.

Protocolo.- Al igual que VRRP el número de protocolo IP utilizado por CARP es 112. Cabe resaltar que este número de protocolo es utilizado sin autorización de la IANA.

2.3.3. DESCRIPCIÓN DE CAMPOS CARP

Versión.- Este campo especifica la versión del protocolo CARP. El valor usado es versión 2.

Tipo.- El campo tipo define cuál es el tipo de paquete CARP que es enviado. Los tipos de paquetes definidos en el protocolo son:

2. 0x01 – ADVERTISEMENT
3. 20 – Hash SHA1 de la contraseña

ID de Host Virtual.- Este es el identificador de Router Virtual que es compartido por el grupo de redundancia.

AdvSkew.- Este valor es usado para sesgar el intervalo de anuncio a fin de lograr que el terminal se vuelva más o menos preferido para convertirse en terminal maestro. El rango valido es de 0 a 254, mientras los valores sean más bajos el host se vuelve más preferido a convertirse en maestro.

AuthLen.- Es el número de grupos de 32 bit para los campos Counter y SHA-1 HMAC.

Reserved.- Reservado para futura expansión del protocolo.

AdvBase.- Este es la base del intervalo al cual CARP enviara los mensajes de anuncio. El valor por defecto es de 1 segundo.

CheckSum.- La suma de comprobación es el resultado del complemento a uno de 16 bit de la suma en complemento a uno de todo el paquete CARP. Es usado para comprobar si existe corrupción de datos en el paquete.

SHA-1 HMAC.- Es el hash SHA-1 (20 bytes) de la contraseña utilizada en la configuración de CARP dividido en cinco grupos de 32 bits.

2.3.4. OPERACIÓN DEL PROTOCOLO DE REDUNDANCIA DE DIRECCIÓN COMÚN

En la mayoría de las redes, el firewall es un punto único de fallo. Cuando el servidor de seguridad deja de funcionar, lo usuarios en la intranet pierden acceso a todo lo que es el internet. Si se tiene un servidor de correo electrónico, servidor de archivos o servidor web; estos no serán accesibles para el mundo entero deteniendo su funcionamiento. Desde la versión 3.5 de OpenBSD, se ha incluido una serie de componentes que puedan ser utilizados para resolver este problema, mediante la colocación de dos servidores de seguridad en paralelo. Todo el tráfico originado en la red interna pasa a través del firewall primario, cuando este falla por algún motivo el firewall de respaldo asume la identidad del servidor de seguridad primario y continua en donde este fallo. Las conexiones existentes se

mantienen dependiendo de la configuración en la que esté trabajando CARP, y el tráfico sigue como si nada hubiera pasado.

Este tipo de configuraciones no solo aumenta la fiabilidad de la red, sino que también puede aumentar la seguridad de una manera sutil. Ahora hacer una actualización en los equipos es una tarea trivial que puede desarrollarse desconectando de uno en uno los servidores de seguridad. Teniendo como resultado que el firewall se actualice con más frecuencia y que exista menos resistencia para aplicar cualquier parche en el sistema operativo por motivos de impacto sobre la red. Además en muchos entornos corporativos existe una fuerte presión para mantener la conectividad de la red en un 99.99% del tiempo, lo que en ocasiones implica tener un firewall desprotegido hasta esperar que uno nuevo entre en su reemplazo.

Los miembros de un grupo de redundancia comparten una dirección MAC Virtual que está en el formato de 00-00-5E-00-01-XX donde el ultimo octeto es llenado con el ID de Host Virtual. CARP hace uso del protocolo IP para enviar los anuncios de los respectivos grupos de redundancia, el número de protocolo IP que utiliza es el 112.
El envío de los anuncios es realizado en la dirección de multidifusión 2224.0.0.18 para IPv4 o la dirección FF:02::12 para el grupo de multidifusión en IPv6.

El tiempo de vida de un anuncio CARP siempre es enviado con un valor de 255. Esto es que si por algún motivo un paquete CARP cruzo la frontera de una sub red, por ejemplo el paquete fue pasado por un Router, pueda ser reconocido y rechazado.

El terminal maestro en el grupo envía anuncios regularmente a la red local para que los terminales de respaldo estén enterados que sigue vivo. Si los terminales de respaldo no escuchan un anuncio del terminal maestro durante un período determinado de tiempo, entonces uno de ellos asumirá las funciones del terminal maestro.

El terminal de respaldo que tenga configurado los valores más pequeños para las variables advbase y advskew, será el que se convierta en terminal maestro. Esto quiere decir que el terminal que se anuncie con la mayor frecuencia se convertirá en el terminal maestro del grupo de redundancia si es que advskew es el mismo para todos los terminales. Los valores de los temporizadores configurados en cada terminal son enviados como parte del anuncio CARP para que los otros terminales del grupo puedan determinar la decisión de cuál será el terminal que se convertirá en maestro.

La ventana entre cada anuncio es calculado tomando el valor de advskew, se divide el valor para 256 y se lo suma el valor de advbase. Este valor será el tiempo en segundos para el envío de un anuncio.
Es posible que existan varios grupos de redundancia CARP dentro del mismo segmento de red. Los anuncios CARP contienen el ID de Host Virtual que permite a los miembros del grupo de redundancia identificar para qué grupo de redundancia pertenece el anuncio.

Con el fin de evitar que un usuario malicioso en el segmento de red envié una falsificación de anuncios CARP, cada grupo puede ser configurado con una contraseña. Cada paquete CARP enviado al grupo es entonces protegido por un mecanismo SHA1- HMAC.

2.3.5. EJEMPLO DE CONFIGURACIONES

CONFIGURACIÓN 1

La configuración de la figura muestra dos servidores de seguridad creando dos grupos de redundancia en cada una de sus interfaces EM mediante el protocolo CARP.

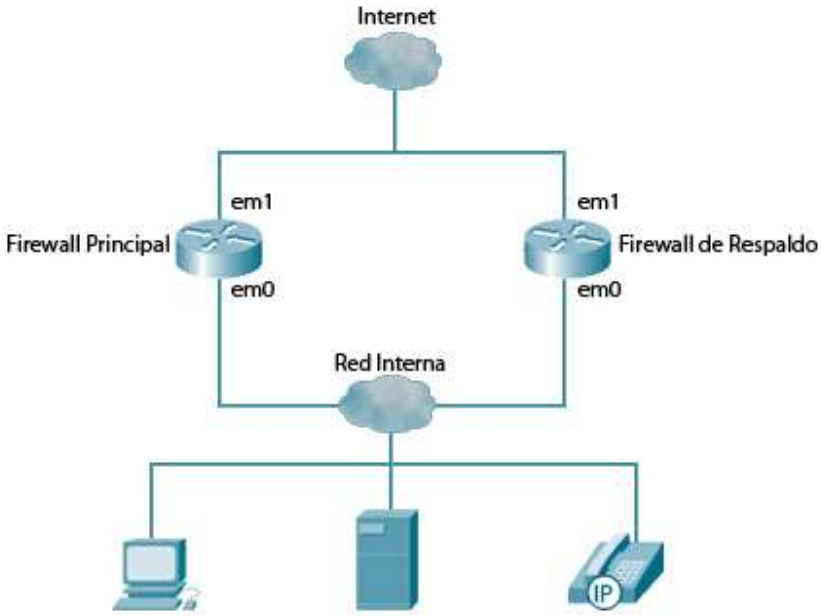


Figura II.6: Configuración uno protocolo CARP.

La configuración de CARP para este escenario es una de las más simples. El grupo de redundancia CARP en las interfaces em0 de cada firewall es usado para la red interna asignando la dirección de Router Virtual del grupo a las terminales de la red como puerta predeterminada de salida. El siguiente grupo de redundancia es creado en las interfaces em1 y esta dirección será utilizada para la salida hacia la WAN.

CONFIGURACIÓN 2

A continuación se describe el ejemplo de una configuración más compleja en la que se combinan características del protocolo CARP junto con pfsync, en la que un grupo de dos o más servidores de seguridad pueden ser utilizados para crear un clúster de firewall altamente disponibles y completamente redundantes.

En el diseño, CARP se encarga de realizar la transición de un firewall a otro en el evento de una caída de servicio mientras que pfsync se sincroniza la tabla de estados del firewall entre todos los miembros del grupo.

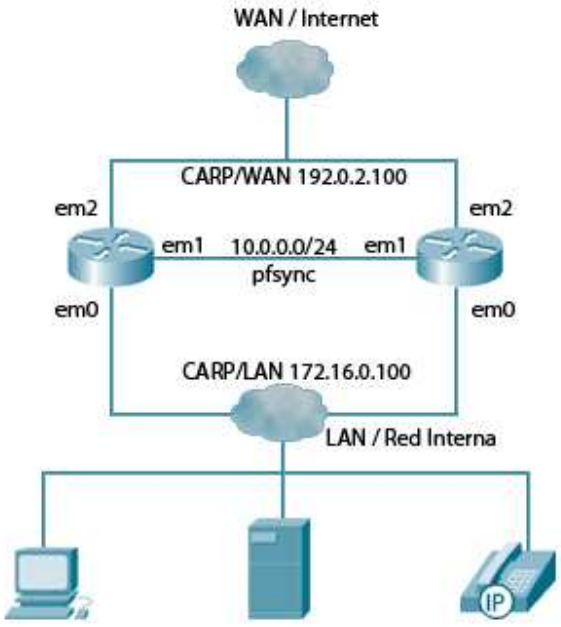


Figura II.7: Configuración dos protocolo CARP.

Dos grupos de redundancia CARP son creados sobre las interfaces em2 para la red externa WAN y em0 para la red interna LAN. En las interfaces em1 de los servidores de seguridad se ha creado un enlace dedicado mediante un cable cruzado para uso exclusivo del protocolo pfsync que sincronizara los dos terminales.

CONFIGURACIÓN 3

En muchos entornos de red a parte de tener una redundancia en la puerta de enlace es muy deseable lograr un balanceo de carga entre los distintos enlaces hacia el proveedor de servicios de internet.

El Protocolo de Redundancia de Dirección Común proporciona un mecanismo para solventar este problema mediante un balanceo de tráfico usando ARP o IP. Para poder lograr la operación de balanceo se necesitara de varias interfaces CARP que estarán configuradas con la misma dirección IP de Router Virtual, pero con diferentes Identificadores de Host Virtual. Cuando una solicitud es recibida por el grupo de terminales, el protocolo CARP usara una función de tipo hash con la dirección de origen en el paquete para determinar cuál debería ser el VHID que responda a la llamada.

El siguiente esquema muestra un sistema redundante haciendo uso del balanceo proporcionado por CARP.

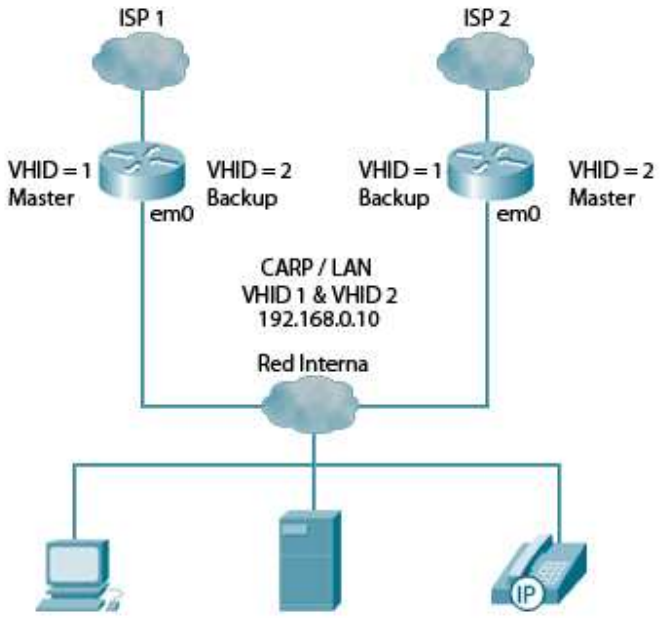


Figura II.8: Configuración tres protocolo CARP.

Se muestra dos grupos de redundancia creados en los terminales en el mismo segmento de red cada uno con un terminal distinto como Router maestro para cada VHID.

2.3.6. BALANCEO DE CARGA

CARP proporciona dos mecanismos para equilibrar la carga de tráfico entrante en un grupo de terminales CARP: balanceo mediante ARP y balanceo mediante IP.

Cual utilizar depende principalmente del entorno de red en el cual CARP está siendo usado. Balanceo mediante ARP tiene limitadas capacidades para balancear la carga en el tráfico entrante de los terminales en la red Ethernet. Este método únicamente funciona para clientes en la red local, ya que el balanceo ARP distribuye la carga mediante la variación de

las respuestas ARP basado en la dirección MAC de origen del paquete que envía la consulta. Por lo tanto, no puede equilibrar el tráfico que atraviesa el Router.

El balanceo IP no depende de ARP por lo tanto también trabaja con el tráfico que viene desde el Router. Este método debería funcionar en todos los ambientes y también puede proporcionar un balanceo de carga de mucha mejor calidad que el realizado por ARP. La desventaja de este tipo de balanceo es que requiere que el tráfico destinado a la dirección IP que realizara el balanceo también sea recibido por todos los terminales del grupo de redundancia. Si bien este siempre será el caso cuando se conecte a un HUB, tiene que jugar algunos trucos en redes conmutadas, lo que podría provocar en un aumento en la carga de la red.

Una regla de oro podría ser el uso de balanceo ARP si hay muchas maquinas en el mismo segmento de red y utilizar el balanceo IP para todos los demás casos.

2.3.6.1. Balanceo ARP

Para utilizar balanceo ARP, se tiene que configurar múltiples nodos CARP, carpnodes, y elegir el modo de balanceo ARP, balancingarp.

Una vez que una petición ARP se recibe, el protocolo CARP utilizara una función de tipo HASH con la dirección MAC de origen en la solicitud ARP para determinar a qué nodo CARP pertenece la solicitud. Si el correspondiente nodo CARP se encuentra en el estado maestro, la petición ARP será respondida, de lo contrario será ignorado.

Las limitaciones de este método pueden llevar a un ruteo asimétrico del tráfico entrante y saliente, por lo que requiere un cuidado especial cuando se lo utilice junto a pfsync. El balanceo ARP solo funciona en el segmento local de la red. No puede realizar el balanceo con el tráfico que cruza el Router.

2.3.6.2. Balanceo IP

El balanceo de carga IP funciona mediante la utilización de la propia red para distribuir el tráfico de entrada a todos los nodos del clúster CARP. Cada paquete se filtra en la interfaz CARP de entrada para que solo uno de los nodos del clúster acepte el paquete. Todos los demás nodos del grupo silenciosamente dejaran caer el paquete. La función de filtrado utiliza un HASH sobre la dirección de origen y destino del paquete IPv4 y compara el resultado contra el estado del nodo CARP.

El balanceo IP se activa estableciendo el modo de balanceo a IP, balancingip. Esta es la configuración recomendada por defecto. En este modo, CARP utiliza una dirección de multidifusión, de manera que el conmutador envía el tráfico entrante a todos los nodos CARP.

2.3.7. ADELANTAMIENTO

En muchos casos, los terminales en el grupo son idénticos y no importa cuál de ellos es actualmente el maestro. Permitir que terminales se mantengan con la dirección virtual indefinidamente reduce el número de transiciones, pero si por alguna razón es preferible que un firewall maneje todo el tráfico siempre que sea posible entonces el firewall en cuestión puede ser ordenado que se adelante al firewall de respaldo y tome de regreso la dirección virtual.

Cuando el modo de adelantamiento está habilitado, cada terminal CARP revisara el parámetro de advskew en el anuncio que es enviado por el terminal maestro para intentar determinar si el terminal puede anunciar con una mayor frecuencia. Si este es el caso, el terminal empezara a anunciarse y el terminal maestro actual, ya que hay otro terminal que tiene un valor de advskew inferior, se retirara.

En el modo de adelantamiento cuando una interfaz física del terminal falla, el valor de advskew es ajustado en 240 para todas las interfaces CARP. Esto obliga a que el terminal entregue el control de las direcciones virtuales de todas sus interfaces CARP y no solo en la que hubo el fallo.

2.3.8. SECUENCIA DE FALLO DE CARP

Si una terminal de respaldo de un grupo de redundancia CARP no ve un anuncio del terminal maestro durante tres ventanas de tiempo consecutivas, entonces esta terminal

asume que el maestro se ha caído. El terminal de respaldo que tenga que envié anuncios con la mayor frecuencia se hará cargo del grupo de redundancia CARP y empezara a anunciarse a sí mismo como el maestro. El número de ventanas de anuncio CARP que se tiene que esperar antes de asumir que el terminal maestro se ha caído no es un parámetro configurable ni ajustable.

En el caso de que dos o más terminales tengan configurado los mismos valores para los temporizadores, el comportamiento resultante podría ser:

- Si el modo de adelantamiento esta deshabilitado: cualquier terminal que empiece a anunciarse primero (Ej. Fue configurado primero) se convertirá en el terminal maestro y se mantendrá como maestro mientras no presente fallos.
- Si el modo de adelantamiento está habilitado: cualquier terminal que empiece a anunciarse primero se convertirá en el terminal maestro pero será rechazado cuando el terminal que fue configurado como maestro este funcional nuevamente.

SECUENCIA DE FALLO DE CARP EN CONFIGURACIÓN CON PFSYNC

El diagrama anterior ilustra una línea de tiempo de los acontecimientos en una falla de terminal típica, e ilustra lo que sucede cuando el modo de adelantamiento está habilitado. Cuando la interfaz que utiliza pfsync es levantada en primer lugar, pfsync envía una difusión para solicitar una actualización masiva de la tabla de estado. Después de esto, todas las actualizaciones de la tabla de estado son enviadas en base a una entrega a mejor

esfuerzo. pfsync intenta prevenir a CARP que tome propiedad de la interfaz de Router Virtual hasta que la actualización de la tabla termine.

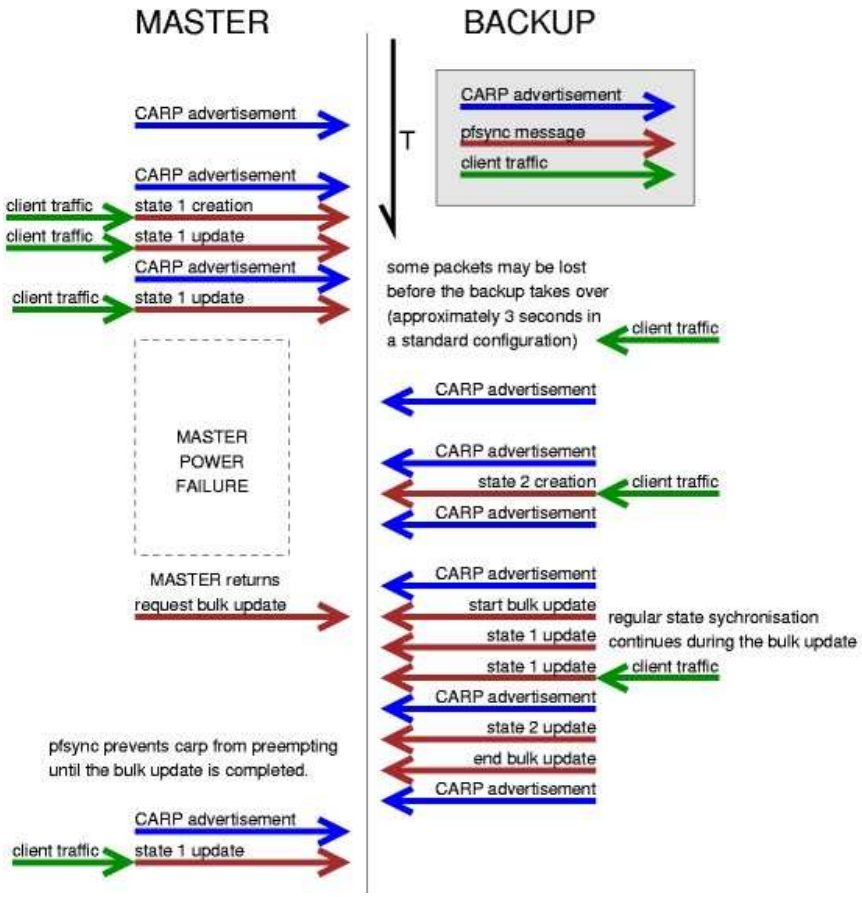


Figura II.9: Secuencia de fallo CARP con pfsync.

2.4. VRRPD

El demonio VRRP (vrrpd) es una implementación del protocolo VRRP versión 2 tal como está especificado en el RFC 2338. Fue diseñado para ejecutarse en espacio de usuario en el sistema operativo GNU/Linux.

Fue desarrollado con la intención de ser fácil de instalar y configurar. El protocolo es sumamente simple por lo que vrrpd ha sido diseñado para ser igual. Un criterio de diseño importante en el cual está basado vrrpd es “mantenlo tan simple como sea posible pero no más” por lo que un único demonio vrrpd es usado en cada terminal.

2.4.1. PORTABILIDAD

Vrrpd es desarrollado bajo GNU/Linux y usa varias características de bajo nivel, como la modificación de la dirección de hardware de una interfaz de red o el manejo de paquetes directamente al nivel IP. El acceso de funciones de bajo nivel desde el espacio de usuario no está normalmente estandarizado por lo portar vrrpd a una plataforma distinta de GNU/Linux se convierte en una tarea no trivial.

2.5. uCARP

uCARP permite a un grupo de terminales compartir una dirección IP virtual común para proporcionar una protección contra fallos automática. Se trata de implementación portable,

que se ejecuta en el espacio de usuario, del protocolo seguro y libre de patentes CARP creado por el grupo OpenBSD.

CAPITULO III

ESTUDIO COMPARATIVO ENTRE LOS PROTOCOLOS DE REDUNDANCIA DE GATEWAY Y COMPROBACIÓN DE LA HIPÓTESIS

3.1. INTRODUCCION

Para poder determinar la mejor solución que se ajuste y que satisfaga los requerimientos de la empresa Infoquality S.A., se debe realizar un estudio minucioso entre los dos protocolos que se habla en el presente documento, determinando por medio de comparaciones o análisis de variables la más factible resolución para el problema planteado, cabe recalcar que esta decisión es la de mayor trascendencia para no acarrear inconvenientes de interconectividad dentro de Infoquality S.A.

La implementación y configuración de los dos esquemas de solución están realizadas bajo una plataforma de Software Libre, a su vez las características de los dos protocolos son de código libre por lo que son factibles de ser estudiados sin inconveniente alguno.

En este capítulo se expondrá un análisis comparativo de las posibles variables por medio de las cuales se calificarácualitativa y cuantitativamente los dos protocolos VRRP y CARP

para la solución de redundancia de Gateway en Infoquality S.A, sabiendo que la recolección de los datos fue realizada en el transcurso de la implementación

3.2. ANALISIS COMPARATIVO

3.2.1. MARCO CONCEPTUAL DEL ANALISIS COMPARATIVO

Por medio del análisis comparativo se escogerá el protocolo más adecuado que brinde mayor prestación al prototipo planteado para brindar la solución al momento que uno de los proveedores de internet deja de operar.

3.2.2. OPERATIVIDAD DE LAS VARIABLES

En las siguientes tablas se detalla la operatividad conceptual y metodológica de las variables, las mismas que han sido identificadas de acuerdo al contexto de la hipótesis planteada.

Tabla III.I: Operatividad de las variables

Variable	**Tipo**	**Definición**
V1. Análisis de protocolos de Redundancia de Gateway	Independiente	Estudio de 2 protocolos de redundancia de Gateway basados en plataformas Open Source
V2. Operatividad	Dependiente	Características, funcionamiento, configuración de cada uno de los dos

		protocolos, para brindar un servicio transparente de conexión al internet hacia los usuarios
V3. Seguridad	Dependiente	Seguridad que brindan las posibles configuraciones en cuanto a confiabilidad de conexión
V4. Soporte	Dependiente	Asistencia que se puede brindar referente a hardware y software con respecto al esquema de configuración

3.2.3. OPERATIVIDAD METODOLOGICA

Tabla III.II: Operatividad metodológica.

Variables	**Categoría**	**Indicadores**	**Técnicas**	**Fuente de Verificación**
V1.Independiente. Análisis de protocolos de redundancia de Gateway	Compleja	**I1.** Modo de Funcionamiento **I2.** Complejidad en la implementación.	Análisis de Documentación oficial Desarrollo de la implementación	Información Científica (libros, intenet) Experiencia

		I3. Licencias y Patentes **I4.** Esquemas de Implementación **I5.** Popularidad del protocolo	Estudio Científico Experimentación Recopilación de Información	personal de técnicos en el área

Tabla III.III: Variable Dependiente Operatividad

Variables	**Categoría**	**Indicadores**	**Técnicas**	**Fuente de Verificación**
V2. Dependiente. Operatividad	Compleja	**I6.** Instalación y configuración inicial **I7.** Complejidad de configuración en clientes **I8.** Tiempo de Transición	Pruebas Conclusiones	Información Científica (libros, intenet) Experiencia personal de técnicos en el área

		I9. Equilibrio en el balanceo **I10.** Documentación		

Tabla III.IV: Operatividad Metodológica de la variable dependiente Seguridad

Variables	**Categoría**	**Indicadores**	**Técnicas**	**Fuente de Verificación**
V3.Dependiente Seguridad	Compleja	**I11.** Vulnerabilidad **I12.** Métodos de autentificación **I13.** Futuros Fallos	Pruebas Conclusiones	Información Científica (libros, intenet) Experiencia personal de técnicos en el área

Tabla III.V: Operatividad Metodológica de la variable dependiente Soporte

Variables	**Categoría**	**Indicadores**	**Técnicas**	**Fuente de Verificación**
V4.Dependiente Soporte	Compleja	**I14.** Análisis de configuración **I15.** Herramientas de monitoreo	Pruebas Conclusiones	Información Científica (libros, intenet) Experiencia personal de técnicos en el área

3.2.4 DESCRIPCION DE LAS VARIABLES CON SUS RESPECTIVOS INDICADORES

Para el análisis de los 2 protocolos que nos sirven para le implementación de los esquemas de redundancia de Gateway bajo una plataforma GNU / Linux se determinaron ciertos indicadores que nos servirán para demostrar cuál de los dos es el más adecuado para brindar una solución para Infoquality S.A.

3.2.4.1 V1. Variable independiente: ANÁLISIS DE PROTOCOLOS DE REDUNDANCIA DE GATEWAY

INDICADORES

I1. MODO DE FUNCIONAMIENTO

El modo de funcionamiento es como los dos protocolos trabajaran al momento que se necesite brindar redundancia de Gateway para que los usuarios no pierdan conexión a internet.

I2. COMPLEJIDAD EN LA IMPLEMENTACION

Grado de dificultad para poner a punto a los dos protocolos en sus respectivos esquemas de configuración.

I3. LICENCIAS Y PATENTES

Restricciones de tipo legal con derechos de autor por la utilización de los protocolos en los esquemas de solución.

I4. ESQUEMAS DE IMPLEMENTACION

El esquema que mejor se ajuste a una solución confiable para la empresa.

I5. POPULARIDAD DEL PROTOCOLO

Cuanta información se encuentra con respecto a la teoría científica de estos dos protocolos.

3.2.4.1.2 V2. Variable dependiente: Operatividad

I6. INSTALACION Y CONFIGURACION INICIAL

Dificultad al momento de instalar inicialmente los dos protocolos con sus respectivos esquemas de solución al problema planteado.

I7. COMPLEJIDAD DE CONFIGURACION EN CLIENTES

Grado de dificultad para que los clientes puedan ser agregados en el esquema que brinda la solución para un acceso transparente al internet.

I8. TIEMPOS DE TRANSICION

Tiempo en que los clientes que pertenecen a un ISP tardan en conectarse hacia el otro proveedor de Internet.

I9. EQUILIBRIO EN EL BALANCEO

Distribución equitativa en el número de asignaciones IP al momento que se produce el fallo para solventar la demanda de conexiones que se presente en ese instante.

I10. DOCUMENTACION

En este indicador se recopilan los documentos, textos, libros, información extraída del Internet que sirve para explicar el por qué y cómo se utilizó los conceptos de los dos protocolos para brindar la solución.

3.2.4.1.3 V3. Variable dependiente: Seguridad

I11. VULNERABILIDADES

En este punto se refiere a los posibles fallos de seguridad que puede tener el esquema implementado con respecto a la configuración y estructura de cada uno de los protocolos en estudio

I12. METODOS DE AUTENTIFICACION

Característica que brinda el sistema a posibles suplantaciones, donde se asegura que la información llegue sin ningún inconveniente desde se origen hacia su destino predeterminado.

I13. FUTUROS FALLOS

Monitoreo del esquema luego de haber realizado la redundancia, para no tener futuras fallas donde los clientes pierdan la conexión a internet nuevamente.

3.2.4.1.4 V4.Variable dependiente: Soporte

I14. ANALISIS DE CONFIGURACION

Implica una revisión de la configuración física y de la configuración lógica, para determinar el probable fallo por lo que el esquema de solución no trabaje con normalidad.

I15. HERRAMIENTAS DE MONITORIZACION

Con estas herramientas de monitorización se puede vigilar que la conexión a internet para los clientes sea confiable y a su vez, al momento de que se presente el fallo la redundancia funcione con normalidad.

3.3 POBLACION Y MUESTRA

En esta investigación la población constituye los protocolos de redundancia de Gateway, que nos pueden brindar una solución para Infoquality y escogidos porque deben trabajar sobre ambientes Open Source y GNU Linux.

MUESTRA

- Para la configuración e implementación de la solución el esquema se basó en las características de dos protocolos: VRRP y CARP, que trabajan bajo GNU Linux.
- Para poder determinar la operatividad, la seguridad y el soporte de los dos protocolos, las pruebas se realizaron desde el momento de la instalación, configuración, ajustes necesarios y trabajo en si en los escenarios de prueba implementados.
- Las muestras para analizar el comportamiento de los dos protocolos al momento de funcionamiento de los esquemas planteados se las realizaron en las oficinas de Infoquality S.A.

3.4 PROCESAMIENTO DE LA INFORMACION

Para la determinación del mejor protocolo para realizar el diseño e implementación de la redundancia de Gateway sobre plataformas de Software Libre, GNU Linux, se realizará una comparación entre los protocolos VRRP y CARP, en la empresa Infoquality S.A. ubicada en la ciudad de Quito en la provincia de Pichincha.

Para poder escoger el mejor protocolo se va a efectuar un estudio comparativo donde se va a calificar cualitativa y cuantitativamente los indicadores de las variables dependientes.

VARIABLE DEPENDIENTE: OPERATIVIDAD

- Instalación y configuración inicial.
- Complejidad de configuración en clientes
- Tiempos de transición
- Equilibrio en el balanceo
- Documentación

VARIABLE DEPENDIENTE: SEGURIDAD

- Vulnerabilidades
- Métodos de autentificación
- Futuros fallos

VARIABLE DEPENDIENTE: SOPORTE

- Análisis de Configuración
- Herramientas de Monitorización

Cabe recalcar que pueden existir muchas más variables asociadas con varios indicadores más que pueden intervenir en el estudio, pero que no tienen una gran relevancia, las que hemos citado anteriormente han sido escogidas bajo nuestro criterio ya que son las que consideramos con más importancia para implementar el esquema de solución a la falta de una conexión transparente al momento que uno de los enlaces pierde interconectividad.

3.5 ESTUDIO COMPARATIVO

En esta sección se va detallar el estudio comparativo entre los protocolos VRRP y CARP para la implementación de un esquema de redundancia de Gateway, a manera de cuadros comparativos, en donde se va a calificar los indicadores de cada variable cualitativamente según, el criterio de los autores teniendo un sustento en el contenido científico, teórico y práctico; también se efectuará una calificación de las variables, con la interpretación respectiva de los resultados que nos arrojen las comparaciones de la variable independiente y de las variables dependientes que han sido expuestas con anterioridad.

3.5.1 ESTUDIO COMPARATIVO DE LA VARIABLE INDEPENDIENTE

A continuación se detalla la escala de valorización para los indicadores de la variable independiente, para poder obtener un total.

Valor de 1:

Si el indicador tiene una respuesta positiva al momento de ser evaluado, tiene un valor de 1

Valor de 0:

Si el indicador tiene una respuesta negativa al momento de ser evaluado, tiene un valor de 0

INDICADOR 1: MODO DE FUNCIONAMIENTO

Tabla III.VI Modo de Funcionamiento

	VRRP	**CARP**
Correcto	1	1

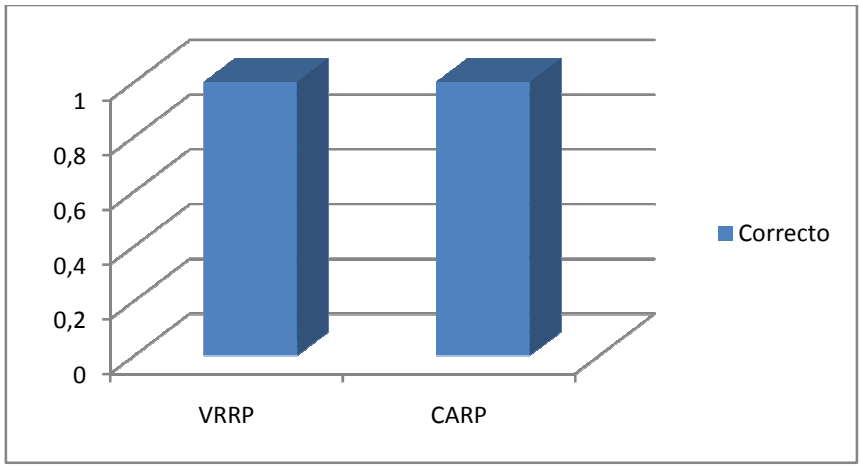


Figura III.1: Modo de Funcionamiento

Interpretación:

En la gráfica se puede evidenciar que los dos protocolos funcionan correctamente al momento que el sistema entra a trabajar con los esquemas de los que son participes para

brindar la solución a lo que la conexión de uno de los proveedores deja de entregar el servicio de internet, para los clientes el proceso de reconexión fue transparente sin presencia de inconvenientes.

INDICADOR 2: COMPLEJIDAD EN LA IMPLEMENTACION

Tabla III.VII: Complejidad en la implementación

	VRRP	CARP
Facilidad	0	1

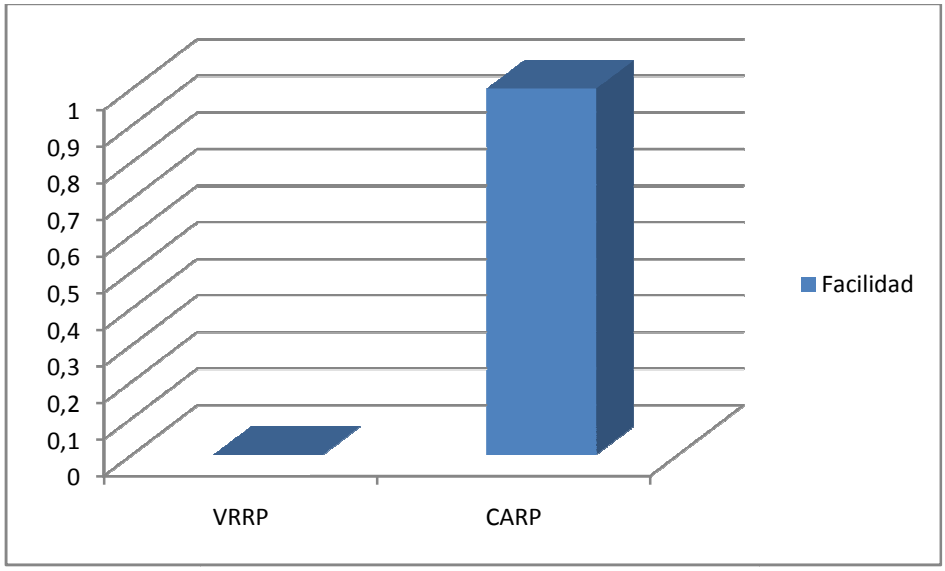


Figura III.2: Complejidad en la implementación

Interpretación:

En la imagen 2 demuestra que se tuvo mayor facilidad en la implementación en el esquema basado con el protocolo CARP ya que el sistema se levantaba automáticamente con los archivos de configuración propios del sistema además para realizar el nating utiliza PF

(packetfilter), que facilita este proceso; en cambio el esquema que utiliza VRRP para que se levante hubo la necesidad de la creación de un script que se ejecute automáticamente al momento que se producía el fallo, siendo este un agregado más a parte de la configuración original, y a su vez para realizar el nating utiliza Net Filter que es basado en Iptables que demanda un grado más de complejidad para que el sistema brinde la solución adecuada.

INDICADOR 3: LICENCIAS Y PATENTES

Tabla III.VIII: Licencias y Patentes

	VRRP	CARP
Licencias	1	1
Patentes	0	1

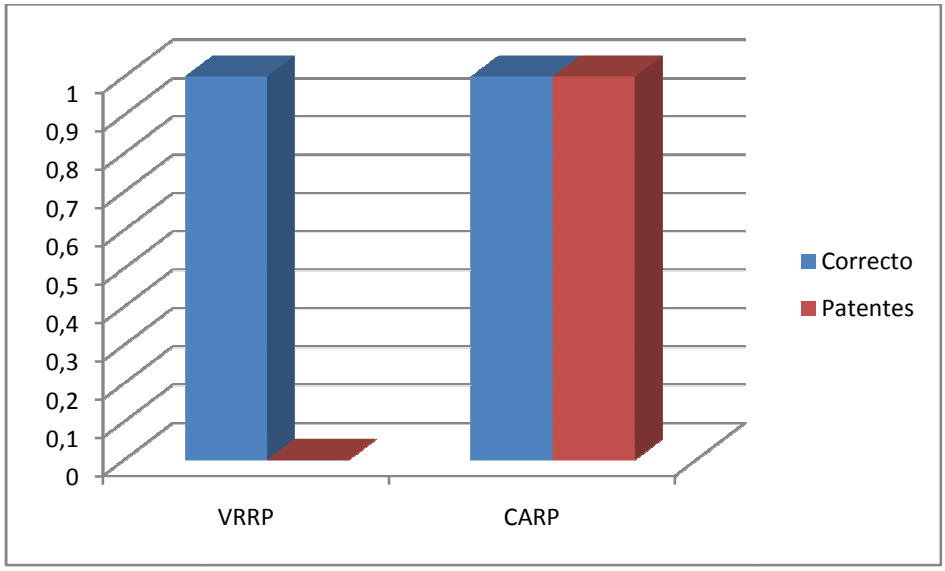


Figura III.3: Licencias y Patentes

Interpretación:

CARP no presenta ningún inconveniente en cuanto a licenciamiento, al igual que VRRP; las patentes tampoco son un problema para CARP pero VRRP presenta ciertas discrepancias en cuanto a patentes ya que Cisco es propietario del protocolo, HSRP, que presenta características similares en cuanto a estructura y detalles de funcionamiento; es por lo que Cisco reclama que su patente fue violada por los mentalizadores del protocolo VRRP.

INDICADOR 4: ESQUEMAS DE IMPLEMENTACION

Tabla III.IX: Esquemas de implementación

	VRRP	CARP
Sencillez	1	1

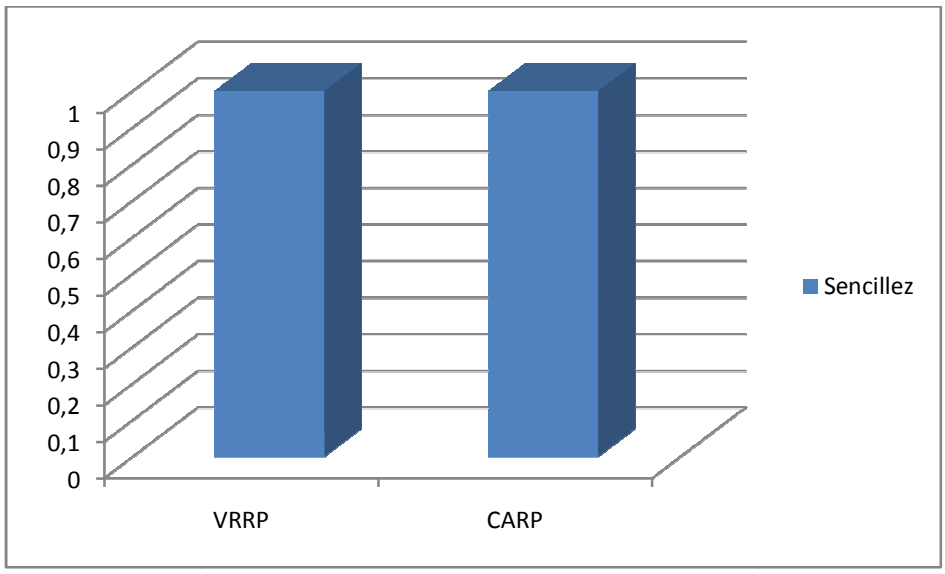


Figura III.4: Esquemas de implementación

Interpretación:

Los dos protocolos presentan esquemas de implementación que no tienen mayores complicaciones en cuanto a configuración física ya que los dos necesitan un servidor seguridad para que realice el trabajo de redundancia sobre los Gateway's, como se puede observar en las gráficas explicativas de los esquemas de solución planteados.

INDICADOR 5. POPULARIDAD DE LA HERRAMIENTA

Tabla III.X: Popularidad de la herramienta

	VRRP	CARP
Muy Conocida	1	1

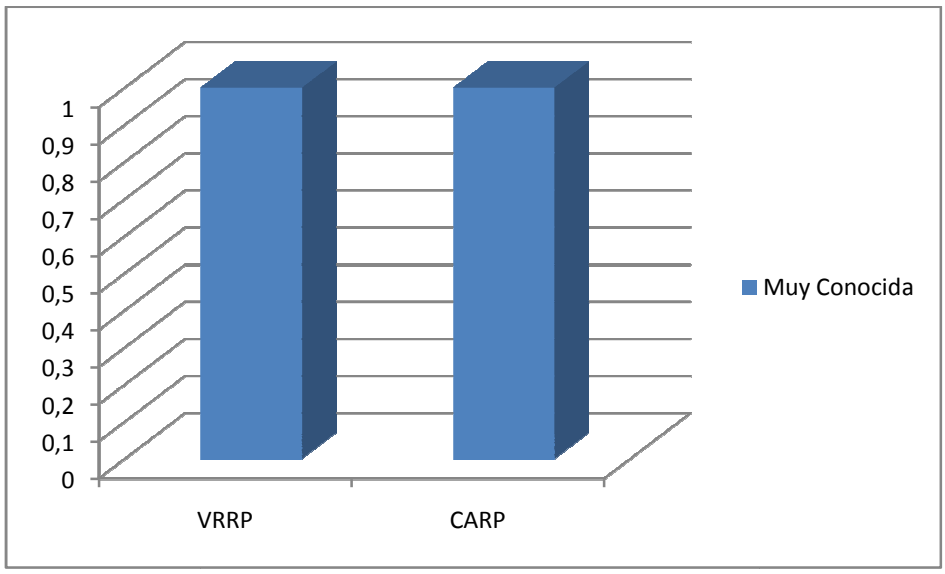


Figura III.5: Popularidad de la herramienta

Interpretación:

Según el personal que trabaja y posee experiencia en la utilización con estos protocolos nos confirma que poseen una gran popularidad debido a que se manejan bajo código libre (Open Source) y que aportan varias soluciones que se ajustan a los requerimientos que se necesite por la versatilidad del código en el que fueron desarrollados.

3.5.1.1 TABLA DE RESUMEN DE LA VARIABLE INDEPENDIENTE

Tabla III.XI: Resumen de la variable independiente

V1. Análisis de Protocolos de Redundancia de Gateway	**Parámetros**	**VRRP**	**CARP**
I1. Modo de Funcionamiento	Correcto	1	1
I2. Complejidad en la implementación	Facilidad	0	1
I3. Licencias y Patentes	Licencias	1	1
	Patentes	0	1
I4. Esquemas de implementación	Sencillez	1	1
I5. Popularidad del protocolo	Muy Conocida	1	1
TOTAL		**4**	**6**

Como se puede ver en la tabla, el protocolo CARP es la que más prestaciones tiene en comparación con VRRP luego de haber realizado el estudio comparativo sobre la variable independiente 1.

3.5.2 ESTUDIO COMPARATIVO DE LAS VARIABLES DEPENDIENTES

Para continuar el estudio comparativo se va a realizar una recapitulación de los datos obtenidos en las pruebas según los indicadores de cada una de las variables dependientes, haciendo el respectivo análisis en cuanto al funcionamiento de los esquemas planteados para la solución brindada a Infoquality S.A.

A los indicadores de cada una de las variables propuestas se les asignará un puntaje de acuerdo a la información obtenido en el estudio científico y teórico, utilizando la siguiente escala de valoración cualitativa, los mismos que permitirán cuantificar los resultados para cada una de las variables que intervienen en la elección del mejor protocolo VRRP o CARP.

Tabla IV.XII: Cuantificadores y Abreviaturas de calificación de los parámetros

0		1		2		3		4 en adelante	
Ninguno	NG	Poco	P	Limitado	L	Algunos	A	Mucho	M
Difícil	D	Parcialmente Difícil	PD	Mediamente Fácil	MF	Fácil	F	Totalmente Fácil	TF
Deficiente	DF	Poco	PE	Limitada	L	Eficiente	E	Muy	ME

		Eficiente						Eficiente	
Ninguno	NG	Parcialmente	PA	Limitada	L	En su mayor parte	MP	Totalmente	T
Inadecuado	IN	Más o Menos Adecuado	MM	Limitado	L	Adecuado	AD	Muy Adecuado	MA
No	N							Si	S

3.5.2.1 V2: Operatividad variable dependiente

INDICADOR 6: INSTALACION Y CONFIGURACION

Tabla III.XIII: Instalación y Configuración

	VRRP		**CARP**	
Llamado al kernel para uso del protocolo	MF	2	TF	4
Configuración de interfaces de red	F	3	F	3
Configuración de firewall	E	3	ME	4
Filtrado de paquetes	PD	1	F	3
Ejecución del protocolo	T	4	T	4

en momento de fallo				
Ausencia de errores luego de ejecución	S	4	S	4
Valoración Total de I6.		**17**		**22**

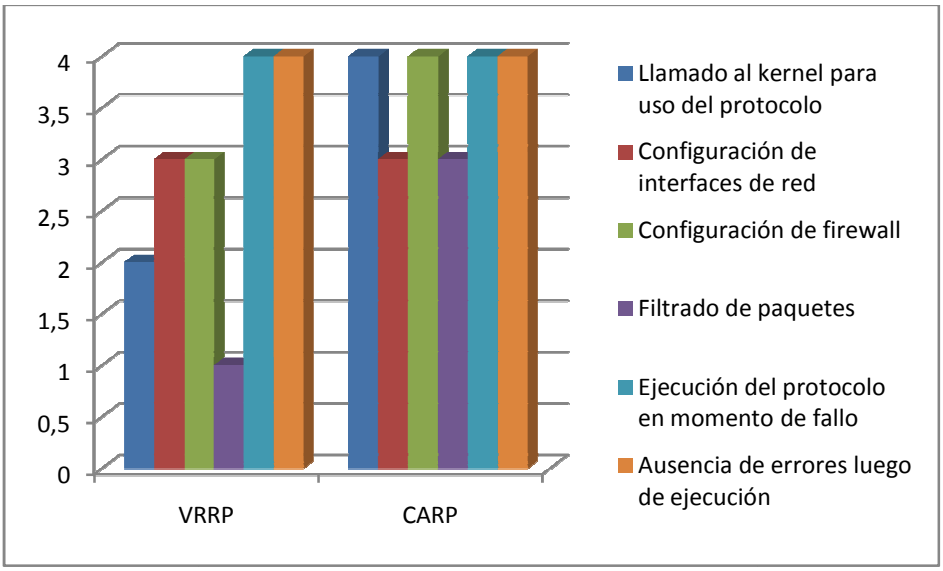


Figura III.6: Instalación y Configuración

Interpretación:

Como queda demostrado el protocolo CARP ofrece más prestaciones que CARP, según la gráfica presentan iguales cuantificaciones con respecto a la ejecución del protocolo al momento del fallo y que no tienen errores luego de la ejecución, pero se presenta una considerable diferencia en el filtrado de paquetes ya que CARP ofrece una solución más fácil que VRRP ya que ocupa el PF (PacketFilter) que tiene gran facilidad de configuración, con respecto a al manejo de Iptables, como se sabe requiere de un mayor

esfuerzo en la puesta a punto; además el llamado al kernel para poder trabajar con CARP es mucho más sencillo por el menor número de sentencias utilizadas.

INDICADOR 7: COMPLEJIDAD DE CONFIGURACION EN CLIENTES

Tabla III.XIV: Complejidad de configuración en clientes

	VRRP		**CARP**	
Transparencia para los clientes	MP	3	T	4
Menor tiempo de configuración	A	3	M	4
Valoración Total de I7.		**6**		**8**

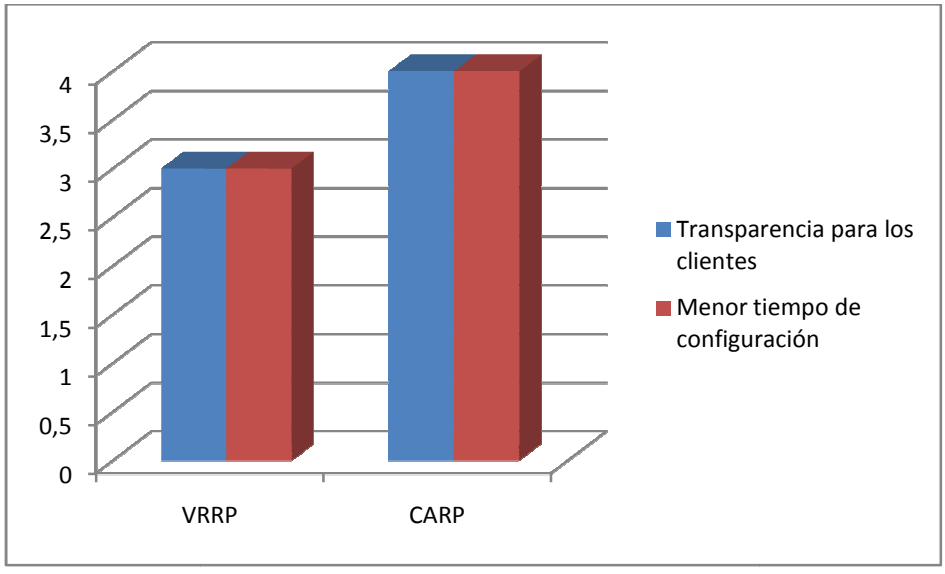


Figura III.7: Complejidad de configuración en clientes

Interpretación:

En la complejidad de configuración en los clientes no son grandes las diferencias, a penas de un punto en la escala de valorización planteada con anterioridad, en el tiempo de configuración para el protocolo VRRP va a ser un poco más extenso que el tiempo requerido para la configuración el ambiente de CARP, ya que se debe configurar manualmente los Gateway en las terminales a diferencia que en el otro protocolo el DHCP es el encargado de entregar todos esos datos, sin necesidad de que el usuario se preocupe de configuración alguna.

INDICADOR 8: TIEMPO DE TRANSICIÓN

Tabla III.XV: Tiempo de Transición

	VRRP		**CARP**	
Ausencia de molestias en los clientes	L	2	MP	3
Ausencia de pérdida de paquetes	PA	1	MP	3
Valoración Total de I8.		**3**		**6**

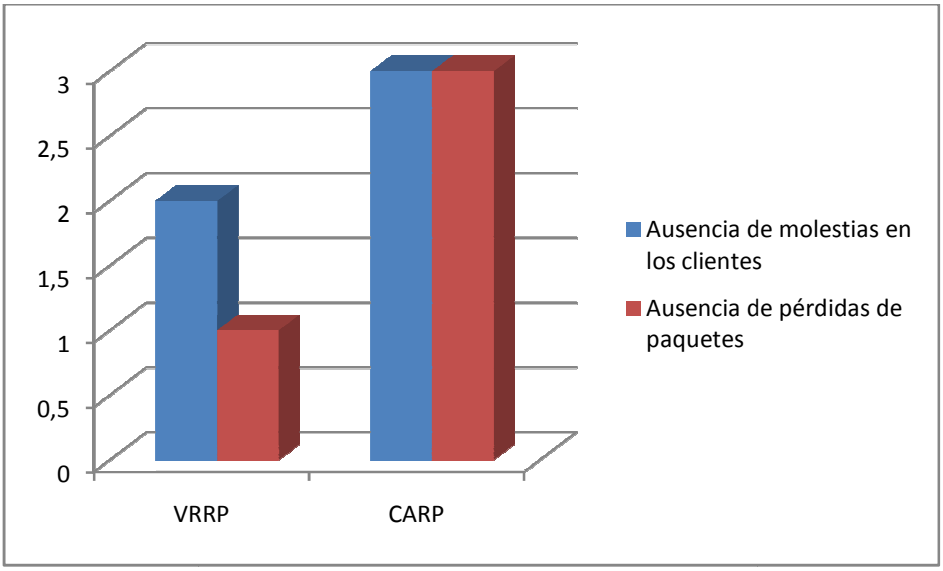


Figura III.8: Tiempos de transición

Interpretación:

En los tiempos de transición se puede ver claramente que CARP lleva una ventaja sobre VRRP, en los dos casos se presenta pérdidas en los paquetes transmitidos, pero en VRRP el número es mayor que CARP, esto pudimos comprobarlo haciendo ping y traceroute herramientas simples de comprobación que no necesitan configuración alguna, y uqe encontramos en cualquiera de las dos plataformas en las que se hizo los escenarios de pruebas; los clientes no presentaron inconvenientes al momento de transmisión, cabe recalcar que pérdidas si existió en los dos casos pero que no fueron evidenciadas por los usuarios finales.

INDICADOR 9: EQULIBRIO EN EL BALANCEO

Tabla III.XVI: Equilibrio en el balanceo

	VRRP		**CARP**	
Balanceo equitativo	ME	4	E	3
Valoración Total de I9.		**4**		**3**

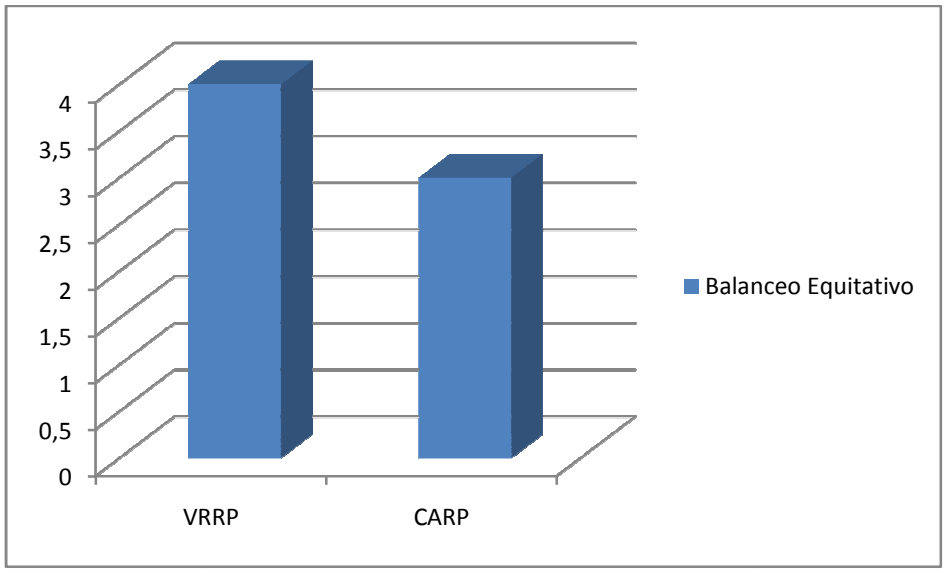


Figura III.9: Balanceo Equitativo

Interpretación:

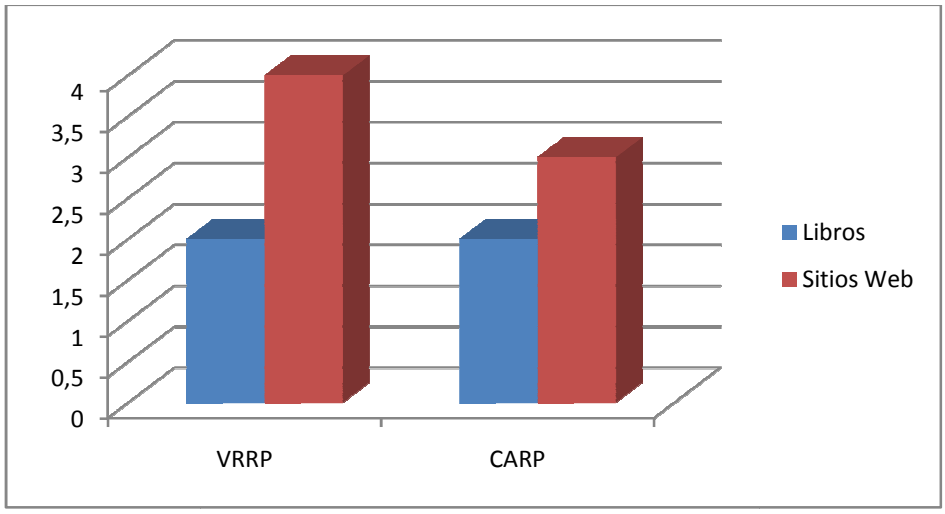
En este caso VRRP ofrece un mejor balanceo en cuanto a la carga ya que la configuración de las ips de los terminales es de tipo manual donde se obtendría una distribución al 100% equitativa, en los dos grupos de red que tiene Infoquality S.A, CARP al funcionar con un

DHCP para asignar ips no se garantiza que se pueda tener una distribución completamente igual con respecto a los dos segmentos de red.

INDICADOR 10: DOCUMENTACIÓN

Tabla III.XVII: Documentación

	VRRP		**CARP**	
Libros	L	2	L	2
Sitios Web	ME	4	E	3
Valoración Total de I10.		**6**		**5**



FiguraIII.10: Documentación

Interpretación:

Información de libros no lo pudimos extraer en gran cantidad, no existen autores que se hayan dedicado enteramente a editar un libro relacionado a estos temas; en cambio, la información en la web fue más amplia ya que los desarrolladores de estos dos protocolos publicaban sus datos científicos de una manera ortodoxa, para poder elaborar el presente documento guiado en esos textos hubo que realizar las pruebas reales para poder aseverar las especificaciones técnicas utilizadas en la implementación.

3.5.2.2 V3. Seguridad variable dependiente

INDICADOR 11. VULNERABILIDADES

Tabla III.XVIII: Vulnerabilidades

	VRRP		**CARP**	
Resueltas	PA	1	MP	3
Valoración Total de I11.		**1**		**3**

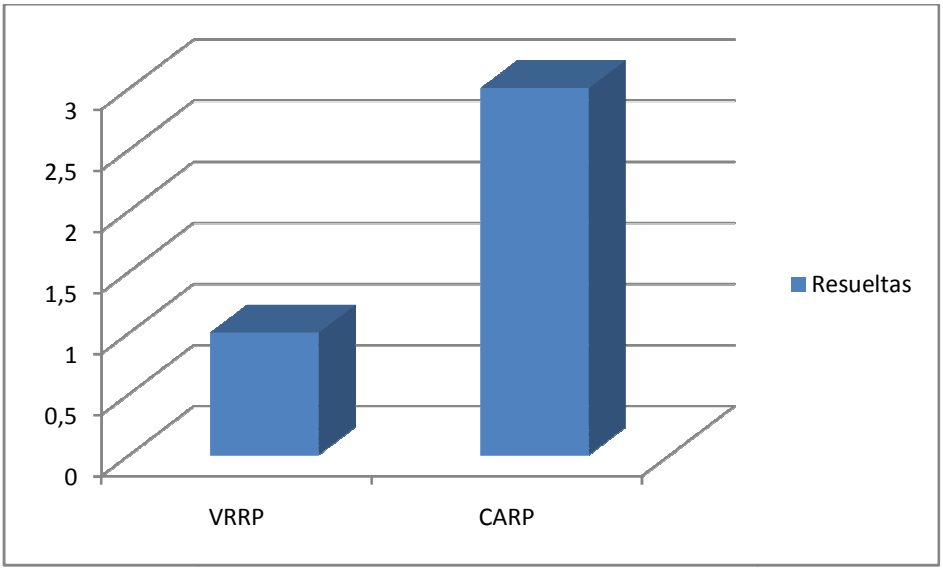


Figura III.11: Vulnerabilidades

Interpretación:

Los desarrolladores y encargados del proyecto CARP continúan trabajando sobre este protocolo mejorando sus funcionalidades y por ende ofreciendo parches de seguridad a posibles vulnerabilidades que se puedan presentar; en cambio, la gente de VRRP a dejado un poco de lado su trabajo sobre el protocolo por motivos que tienen inconvenientes con las patentes ya que Cisco reclama que es una fiel copia de HSRP, por este motivo el desarrollo se ha visto estancado.

INDICADOR 12. METODOS DE AUTENTIFICACION

Tabla III.XIX: Métodos de Autentificación

	VRRP		**CARP**	
Seguridad en contraseñas	NG	0	T	4
Valoración Total de I12.		**0**		**4**

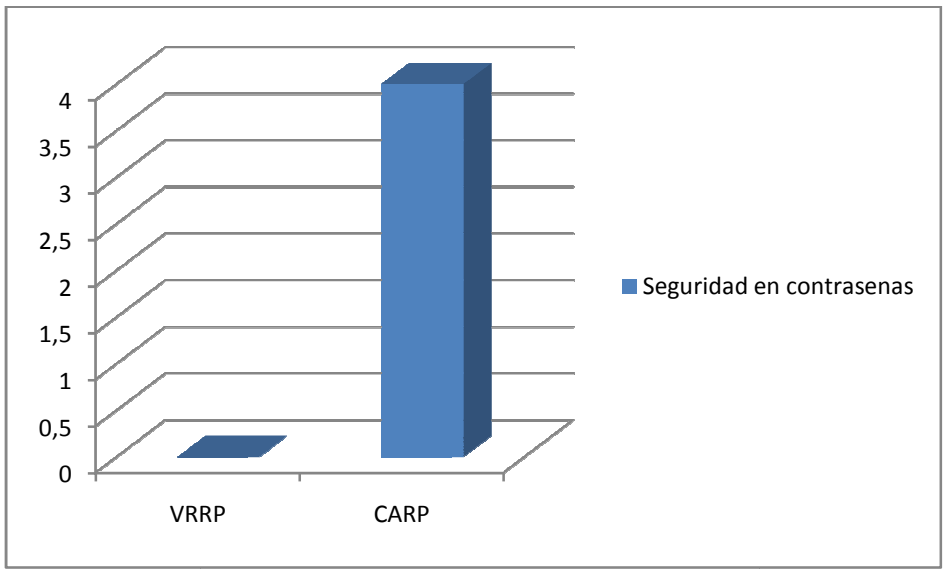


Figura III.12: Seguridad en contraseñas

Interpretación:

Claramente CARP lleva una gran ventaja sobre VRRP en este punto, ya que las contraseñas de autentificación al momento de envío de paquetes de este último son en texto plano y no

ofrecen algún tipo de seguridad, lo que no ocurre con CARP este utiliza SHA1 para brindar encriptación en las contraseñas.

INDICADOR 13: FUTUROS FALLOS

Tabla III.XX: Futuros Fallos

	VRRP		**CARP**	
Ausencia de futuros fallos	T	4	T	4
Valoración Total de I13.		**4**		**4**

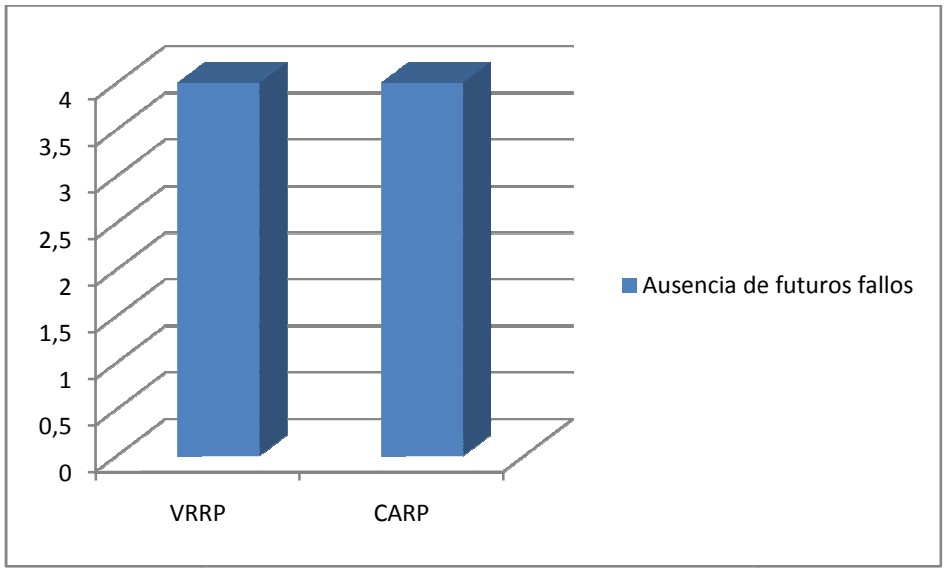


Figura III.13: Futuros Fallos

Interpretación:

En los casos para VRRP y CARP se pudo comprobar que los esquemas de solución eran estables luego de empezar a trabajar los protocolos presentado el fallo. Brindando el servicio de internet sin interrupciones para los dos segmentos de red.

3.5.2.3 V4. Soporte variable dependiente

INDICADOR 14: ANÁLISIS DE CONFIGURACION

Tabla III.XXI: Análisis de Configuración

	VRRP		**CARP**	
Física	TF	4	TF	4
Lógica	TF	4	TF	4
Valoración Total de I14.		**8**		**8**

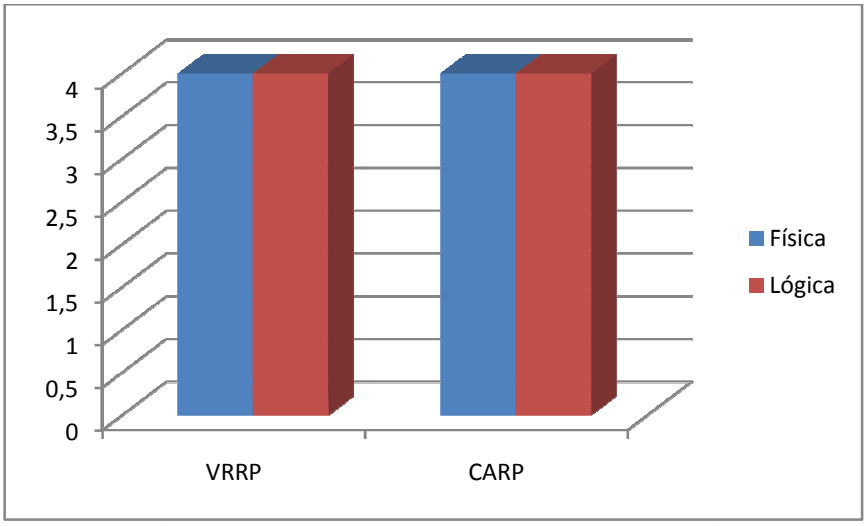


Figura III.14: Análisis de Configuración

Interpretación:

Al saber el proceso de configuración inicial, la revisión no presenta ningún inconveniente y ningún grado de dificultad para los dos casos.

INDICADOR 15: HERRAMIENTAS DE MONITORIZACION

Tabla III.XXII: Herramientas de monitorización

	VRRP		**CARP**	
Ping	ME	4	ME	4
Traceroute	ME	4	ME	4
Valoración Total de I15.		**8**		**8**

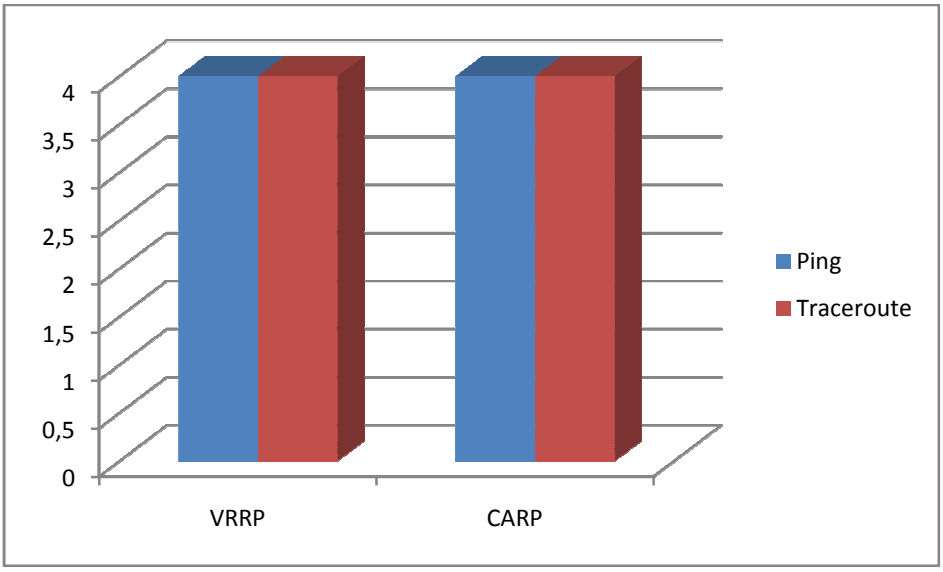


Figura III.15: Herramientas de monitorización

Interpretación:

Para los dos protocolos se pudo monitorizar el funcionamiento en la transmisión de los paquetes por medio del ping y del traceroute, donde se podía comprobar si existía conectividad o pérdida de paquetes.

3.6 PUNTAJES TOTALES

A continuación se presentan los resultados generales del estudio comparativo entre los protocolos VRRP y CARP

Tabla III.XXIII: Resultados Generales

Variables	Indicadores	VRRP	CARP
Operatividad	I6	17	22
	I7	6	8
	I8	3	6
	I9	4	3
	I10	6	5
Total 1		**36**	**44**
Seguridad	I11	1	3
	I12	0	4
	I13	4	4
Total 2		**5**	**11**
Soporte	I14	8	8
	I15	8	8
Total 3		**16**	**16**
$\sum$ total = Total1 + Total2 + Total3		**57**	**71**

Como resultado del estudio de las variables con sus respectivos indicadores y con los puntajes obtenidos se llegó a la conclusión que el protocolo CARP fue el ganador consiguiendo un puntaje de 71 puntos versus los 57 puntos que obtuvo el protocolo VRRP.

3.7 RESULTADOS DEL ESTUDIO COMPARATIVO

Una vez aplicado el estudio comparativo sobre los protocolos VRRP y CARP que ofrecen un esquema de solución para el problema planteado, utilizando las variables definidas por los autores las cuales fueron elegidas para el análisis; siendo calificadas con respecto a la tabla de valorización propuesta, se obtuvo resultados que permite presentar el siguiente conjunto de conclusiones:

- En el análisis de la operatividad el protocolo VRRP obtuvo un puntaje de de 36 puntos y CARP un total de 44 puntos siendo este el ganador, ya que al momento de llamar al kernel para que pueda trabajar el protocolo hubo más facilidad de configuración, en cuanto a la configuración en los clientes fue fácil para los dos ya que no requiere de un conocimiento amplio en el tema sino más bien conocimiento básico para que los clientes puedan obtener la ip para poder estar dentro del esquema de solución; en cuanto al firewall CARP lo supera ya que utiliza el PacketFilter que para su configuración es mucho más simple que el de VRRP ya que este trabaja con IpTables que tiene un grado más complejo en su configuración; esto arroja una relación directa con respecto al filtrado de paquetes teniendo CARP mayor eficiencia; los dos protocolos luego de empezar a trabajar en su respectivo esquema de implementación no presentan inconvenientes operando con absoluta normalidad.
- En los resultados que se obtuvo para la variable Seguridad también tiene ventaja el protocolo CARP con un puntaje de 11 versus los 5 puntos de VRRP, teniendo como mayor característica en este caso que las contraseñas de autentificación presentan

codificación con SHA1 a diferencia de VRRP que este se presenta como texto plano, además las vulnerabilidades son cada vez solventadas con parches de seguridad que ofrecen los desarrolladores y encargados del proyecto CARP, este estudio constante en VRRP se vio estancado ya que tienen algunos inconvenientes con patentes que reclaman la gente de CISCO atribuyendo que es una fiel copia el funcionamiento de su protocolo HSRP.

- En cuanto a la variable Soporte se presenta un empate técnico de 16 puntos los dos protocolos ya que sus indicadores: Análisis de Configuración y Herramientas de monitorización, tienen iguales características en el modo de operación y por consiguiente arrojando datos similares para el estudio comparativo.
- Por todo lo expuesto anteriormente y teniendo un sustento real con los resultados del estudio el protocolo CARP con un total de 71 puntos con respecto a los 57 que obtuvo VRRP, es el indicado para poder implementar el esquema de solución para la redundancia de Gateway en la empresa Infoquality S.A., permitiendo que al momento de caída de uno de los dos proveedores de Internet los usuarios tengan una conexión segura al internet.

3.8 COMPROBACION DE LA HIPOTESIS GENERAL

Los siguientes indicadores que se van a exponer nos ayudan a comprobar la hipótesis general planteada en el inicio del presente documento; los indicadores tienen una relación directa con los tiempos empleados al momento de operación del protocolo escogido anteriormente, con respecto al tiempo medio entre fallos (MTBF)

3.8.1 DESCRIPCION DE LOS INDICADORES

- **Tiempo de Configuración:** es el tiempo empleado para preparar la configuración, para que al momento del fallo entre a operar la redundancia de Gateway.*
- **Tiempo de Transición:** es el tiempo que se toma en cuenta desde el momento que se produce el fallo hasta que el esquema de solución entra en operación.
- **Tiempo de Restauración:** es el momento en que el operador de internet que dejo de brindar el servicio, reinicia su operación normal hasta el tiempo en que el esquema de solución deja de funcionar y entra a trabajar con normalidad la red antes de haberse producido el fallo.*

3.8.2 DESCRIPCION DE LOS RESULTADOS OBTENIDOS

En la siguiente tabla se detalla los tiempos específicos según los indicadores expuestos anteriormente; por motivos de comprobación solo se hicieron mediciones de los dos últimos meses (Julio y Agosto) para poder verificar con los datos que tenemos en el certificado del anexo 7

Tabla III.XXIV: Tiempos Totales de Fallos antes de implementación

Indicadores ↓	**Julio**		**Agosto**	
	# de fallos	**Tiempo de Fallo (min)**	**# de fallos**	**Tiempo de Fallo (min)**
TOTAL	6	30	8	40

Tabla III.XXV: Tiempos Total de Fallos después de implementación

Indicadores ↓	**Julio**		**Agosto**	
	# de fallos	**Tiempo de Fallo**	**# de fallos**	**Tiempo de Fallos**
Tiempo de Configuración	6	6 min	8	8 min
Tiempo de Transición		27 seg		36 seg
Tiempo de Restauración		6 seg		8 seg
	TOTAL	**6 min 33 seg**	**TOTAL**	**8 min 44 seg**

Interpretación de los resultados obtenidos:

En la tabla III. XXV se especifica los tiempos para cada uno de los indicadores, luego de haber realizado las pruebas correspondientes los valores por cada uno de estos son los siguientes:

- Tiempo de Configuración (Indicador 1): 1 min
- Tiempo de Transición (Indicador 2): 4.5 seg
- Tiempo de Restauración (Indicador 3): 1 seg

La suma de los valores indicados anteriormente suman un total de 1 min 5.5 seg por cada fallo que se ocasione. En el mes de Julio nos dio un total de 6 minutos con 33 segundos, y en el mes de Agosto tenemos un total de 8 minutos con 44 segundos.

Haciendo una relación con la tabla III.XXIV y los datos expuestos en la tabla III.XXV se ve una notable diferencia entres los tiempos medios de fallos para el esquema antiguo que

presentaba la empresa versus el esquema con la implementación de la redundancia de Gateway basado en el protocolo CARP, la reducción del tiempo para el mes de Julio fue de 23 minutos con 27 segundos; y para el mes de Agosto 31 minutos con 16 segundos.

Estos resultados demuestran que con la implementación

3.8.3 RESULTADO OBTENIDO

La aplicación de un protocolo de Redundancia, en nuestro caso CARP, redujo los porcentajes del Tiempo Medio entre Fallos (MTBF) en la empresa Infoquality S.A, para el mes de julio en un 78% y para el mes de agosto un 71%.

CAPITULO IV

DISEÑO DE LA RED INTERNA E IMPLEMENTACIÓN DEL PROTOCOLO DE REDUNDANCIA DE GATEWAY PARA LA EMPRESA INFOQUALITY S.A.

4.1. GENERALIDADES

Dentro de este capítulo se toma en cuenta todo lo referente a la definición de objetivos, alcance y planificación, que ayuda a guiarse durante la elaboración del diseño de red.

4.1.1. INTRODUCCIÓN

La empresa Infoquality S.A. ubicada en la ciudad de Quito, Provincia de Pichincha., se dedica al desarrollo de portales web basado en tecnologías Open Source.

Infoquality S.A. al igual que la mayoría de las empresas que basan sus actividades diarias con el uso de Internet poseen un mismo problema que es la posible falla en el enlace con el proveedor de servicios. Por lo tanto la necesidad primordial es mantener el tiempo de fallo de conexión lo más reducido posible de una forma fácil y segura. La empresa en su afán de conservar este tiempo de caída sumamente bajo, ha contratado la conexión a internet

mediante dos proveedores de servicio de internet distintos. Aunque esta solución proporciona un cierto grado de redundancia en la conexión a internet, el esfuerzo requerido para lograr que el tiempo medio entre fallos disminuya aun no es eficiente. Debido a esto se propone la utilización de un protocolo de redundancia de Gateway que facilite la administración de la red y brinde una mejor efectividad en el momento de producirse un fallo y un mejor uso de las conexiones de internet.

4.1.2. ALCANCE

El alcance que el diseño de la Red Redundante de Gateway pretende, es el de tener la documentación fuente para la implementación de un protocolo de redundancia de Gateway usando GNU/Linux en la empresa Infoquality S.A., identificando todos los aspectos técnicos de infraestructura, interconexión y configuración requerida para que la empresa tenga un rendimiento óptimo.

4.1.3. OBJETIVO GENERAL

Diseñar la Red de Redundancia de Gateway, capaz de reducir el tiempo medio entre fallos de la conexión a internet en la empresa Infoquality S.A.

4.1.4. OBJETIVOS ESPECÍFICOS

- Identificar las necesidades de una conexión ininterrumpida al internet.
- Poseer una documentación técnica que sirva como guía para la implementación de la Red de Redundancia de Gateway.

4.2. ANÁLISIS PRELIMINAR

4.2.1. ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA RED.

4.2.1.1. Antecedentes y referencias generales de la organización

a) Objetivos de la empresa Infoquality S.A.

- Agregar valor a empresas públicas y privadas a través de la tecnología web
- Asesorar en la constitución de soluciones de internet enmarcados al desarrollo y potenciación de las cualidades competitivas de nuestros clientes
- Entregar a nuestros clientes productos únicos y de mucha calidad creativa respetando las particularidades innatas de la identidad corporativa

b) Visión

Constituirnos en una empresa líder a nivel regional en el empleo de herramientas de interrelación socio - tecnológicas entre nuestros clientes y sus públicos de interés

c) Misión

Atender las necesidades de tecnología de información a través de productos y soluciones orientados a potencializar el valor y el prestigio de nuestros clientes

d) Referencias generales de la empresa Infoquality S.A.

Infoquality S.A. es una empresa ecuatoriana creada en el año 2007, pero sus operaciones se inician en el año 2008.

A pesar de ser una compañía relativamente nueva en el mercado, ha logrado satisfacer y superar las expectativas de sus nuestros clientes con un servicio competitivo, innovador y funcional.

La fortaleza corporativa es brindar una verdadera asesoría que permite incorporar ideas y materializarlas en soluciones tecnológicas cada vez más demandantes en la evolución de las empresas e instituciones.

Infoquality S.A. cuenta con un equipo de profesionales jóvenes especialistas en las áreas de desarrollo de software, diseño multimedia, infraestructura y comunicación corporativa que integrados conforman soluciones innovadoras y de alto impacto creativo.

Ubicación geográfica del área de trabajo

Provincia: Pichincha

Cantón: Quito

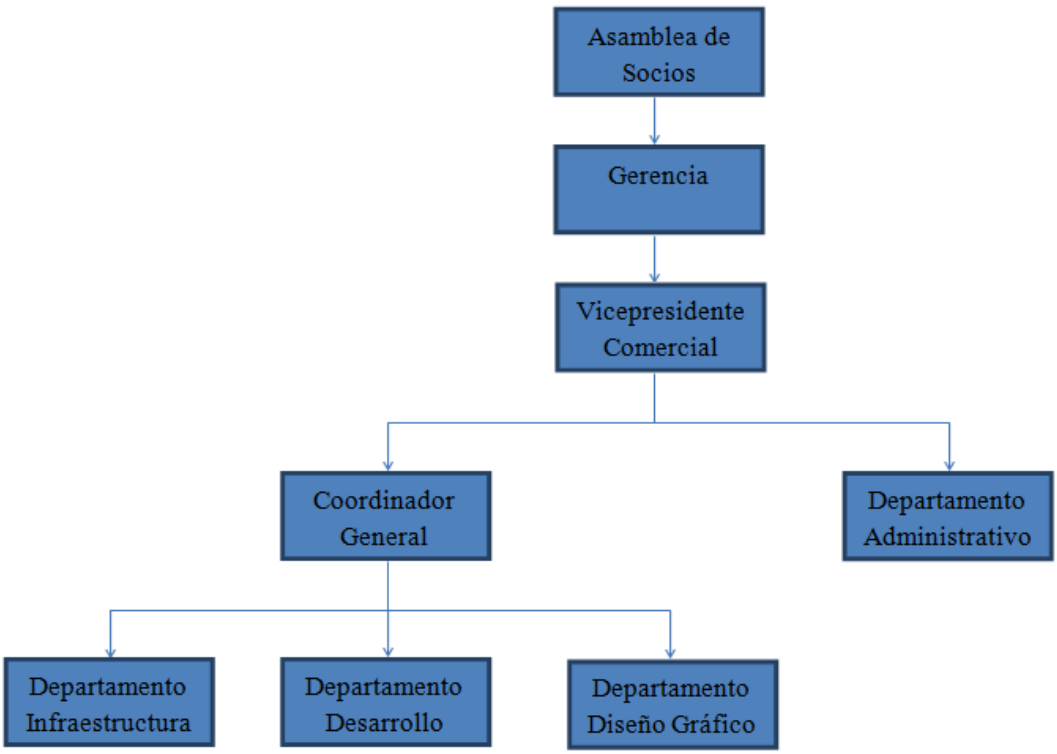
Ubicación: Diego de Almagro 1550 y Pradera. Edificio Posada de las Artes Kingman, oficina 2C.

Teléfono: (02) 2 569-664 – (02) 2 543101 – (09) 8 356175

Email: ventas@infoquality.com.ec

Web: www.infoquality.com.ec

e) Estructura orgánica funcional



4.2.1.2 Sistema de Red

a) Usuarios de Red

Tabla IV.I: Usuarios de la Red de la empresa Infoquality S.A.

Infoquality S.A.	
Departamentos	**Numero de Computadoras**
Administrativo	4
Infraestructura	4
Diseño Gráfico	5
Desarrollo	8
Servidores	3
Dispositivos de Red	4

CARP/VRRP	2

b) Aplicaciones de red

La empresa Infoquality S.A. cuenta con varias herramientas para su funcionamiento instalados en los distintos servidores.

- Apache
- MySQL
- SharePoint
- TeamFoundation Server
- Tomcat
- Active Directory

4.2.1.3 Análisis FODA de la red existente

El equipamiento y al infraestructura constituyen la base de las fortalezas en el desarrollo de las actividades que realiza la empresa Infoquality S.A. Esta matriz nos ayuda a determinar las fortalezas, oportunidades, debilidades y amenazas de la red existente y para dar solución y justificar la necesidad de una nueva red.

Tabla IV.II: Análisis FODA red existente.

Fortalezas	**Oportunidades**

• Disponer de hardware actualizado. • Contar con un correcto cableado estructurado. • Disponer de distintas conexiones a internet. • La empresa cuenta con una página web informativa. • Uso de software Open Source para desarrollar soluciones a medida.	• Disponibilidad de herramientas y servicios bajo plataforma GNU/Linux. • Hacer uso de los últimos avances tecnológicos en el diseño de redes redundantes. • Eficiente uso de los distintos enlaces hacia internet. • Potenciar el uso de los servidores internos.
Debilidades • Uso inadecuado de los recursos de red. • Un mal diseño de la red interna. • El sitio web de Infoquality S.A. no ofrece una completa visión de todo el trabajo realizado por la empresa.	**Amenazas** • Caída de la conexión a Internet. • Retrasos en los trabajos. • Perdida de contacto con los clientes. • Clientes insatisfechos. • Pérdidas de producción.

4.2.1.4 Descripción de la red actual.

En la empresa Infoquality S.A. se cuenta con un cableado estructurado, el cual permite tener a todas las dependencias conectadas en la red de área local, para compartir información, permitir el acceso a los distintos servidores internos, y compartir la conexión a internet. El hardware existente para el funcionamiento de la red actual es el siguiente:

Tabla IV.III: Hardware de la Red de la empresa Infoquality S.A.

Descripción	**Cantidad**

Servidor IBM X3200 M2 Ram: 8GB Disco Duro: 3 discos 250GB HotSwap Procesador: Intel XeonQuadCore 3Ghz Puertos de Red: Ethernet 1GB	1
Servidor IBM X3200 M2 Ram: 4GB Disco Duro: 3 discos 250GB HotSwap Procesador: Intel XeonQuadCore 2.4Ghz Puertos de Red: Ethernet 1GB	2
Switch 3Com BaseLine 2024	2
D-Link DIR-600	1
D-Link DIR-635	1

Los proveedores de internet contratados por la empresa para el funcionamiento de sus actividades diarias son los siguientes:

Tabla IV.IV Proveedores de internet empresa Infoquality S.A.

Proveedor	**Velocidad**
Telmex	1024Kbps x 256Kbps

TVCable	550Kbps x 150Kbps

A continuación se describe gráficamente la estructura de red con la que cuenta la empresa Infoquality S.A.

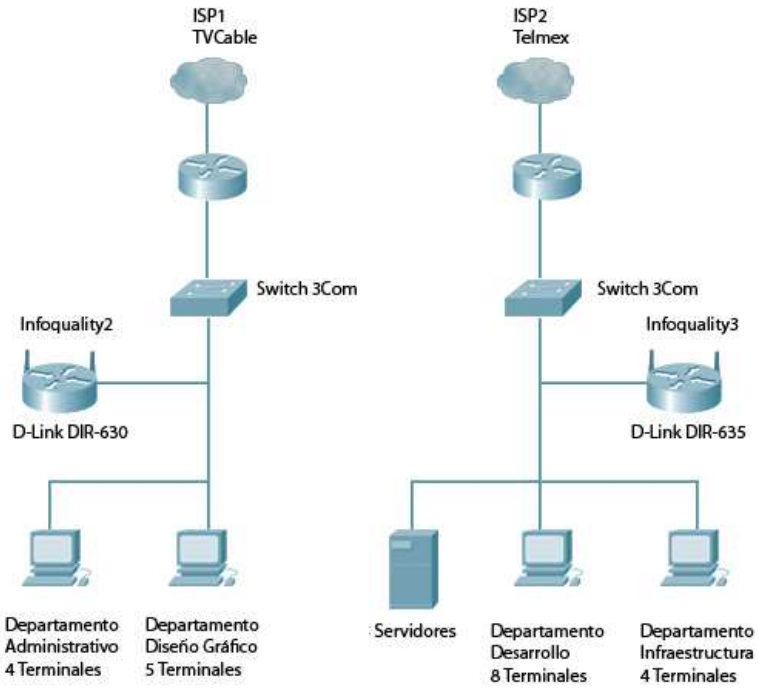


Figura IV.1: Esquema de red Infoquality S.A.

4.2.2 ANÁLISIS DE REQUERIMIENTOS

4.2.2.1 Análisis de usuarios

Tabla IV.V: Requerimiento de Usuarios.

Áreas de Trabajo	**Usuarios**	**No. PC**	**Acceso Internet**
Departamento Administrativo	Gerencia Contabilidad Secretaria	1 2 1	Si Si Si
Departamento Grafico	Gerente de Área Diseñadores	1 4	Si Si
Departamento Desarrollo	Gerente de Área Desarrolladores Microsoft Desarrolladores Open Source	1 3 4	Si Si Si
Departamento Infraestructura	Gerente de Área Ingenieros Infraestructura	1 3	Si Si
Parámetro	**Descripción**		
Interactividad	Los usuarios requieren que la red les brinde la facilidad de interactuar directamente con la información, accediendo a todos los servicios que el administrador les conceda.		
Confiabilidad	Requiere un mínimo riesgo de caída de interconexión con el internet para reducir lo máximo posible la perdida de trabajo.		
Calidad	Se requiere un control absoluto de la red por parte del administrador con un mantenimiento de la misma relativamente fácil sin necesidad de realizar configuraciones complicadas para solventar una posible caída de internet.		
Flexibilidad	La red debe estar creada de tal manera que permita un crecimiento en sus estaciones de trabajo para sus distintas áreas.		
Seguridad	La red debe tener un nivel mínimo de seguridad para que los paquetes enviados por el protocolo elegido no puedan ser suplantados.		

Fuente: Gerente de Infraestructura.

4.2.2.2 Análisis de Servidores

Tabla IV.VI: Requerimiento de Servidores.

Tipo de Servidor	**Equipo**	**Acceso Internet**	**Acceso desde Internet**
DHCP	D-Link DIR-635	Si	No
Repetidor Universal	D-Link DIR-630	Si	No
Share Point	Servidor IBM X3200 M2	Si	No
TeamService	Servidor IBM X3200 M2	Si	No
Apache + MySQL	Servidor IBM X3200 M2	Si	Si

Fuente: Gerente de Infraestructura.

El área critica de la empresa Infoquality S.A.es la administración de los servidores internos de los cuales hacen uso todos los departamentos de la empresa. Aunque el trabajo realizado sobre ellos es local, muchos de los clientes de la empresa se conectan al servidor web para supervisar el avance del trabajo realizado.

4.2.2.3 Análisis de especificaciones Técnicas

Se describirá las configuraciones para la implementación del protocolo seleccionado en software y hardware.

Características Técnicas Hardware

Tabla IV.VII: Características hardware para implementación de protocolo.

Equipo	Características	No. De Servidores
Equipo genérico Clon	Ram: 2GB Disco Duro: 250GB Procesador: Intel DualCore 2.2Ghz Puertos de Red: 2 puertos Ethernet 10/100/1000 Mbps	2

Características Técnicas Software

Tabla IV.VIII: Característica de software utilizado para implementación de protocolo.

Software utilizado	Descripción
Sistema Operativo GNU/Linux IQ-Linux 1.0	Se compilo una versión personalizada de GNU/Linux la cual fue llamada IQ-Linux en homenaje a la empresa en la cual será utilizado.
PacketFilter	Software utilizado para hacer filtrado de paquetes y traducción de direcciones de red.

Protocolo de Redundancia de Gateway

Tabla IV.IX: Características del protocolo a ser implementado.

Características	Descripción
CARP	El protocolo a utilizar será el Protocolo de Redundancia de Dirección Común.
Algoritmo de encapsulación	Protocolo de Internet (IP)

Seguridad	El protocolo usa un encriptado en los paquetes mediante SHA1-HMAC

4.2.2.4 Requerimiento de Red

Cuál será el tipo de red implementada en la empresa, velocidad de funcionamiento y número de equipos.

Tabla IV.X: Requerimientos de red para implementación de protocolo.

Tipo de Red	**Características**	**No. De Equipos**	**Localización**
LAN	Red privada de alcance local Fast Ethernet 10/100/1000. Cableado estructurado UTP categoría 5e	30	Infoquality S.A.

4.2.2.5 Requerimientos de interconexión

La intranet será configurada bajo un direccionamiento privado de clase C, lo que satisface las necesidades de todos los equipos que estarán interconectados en la red de área local. En la siguiente tabla se describe la red que se utilizara en la LAN teniendo en cuenta que para la salida a internet se utilizara dos direcciones IP publicas proporcionadas por cada ISP.

Tabla IV.XI: Direccionamiento de interconexión.

Dirección IP de Red	**Tipo de Red**	**Mascara de Red**

192.168.1.0	LAN tipo C	255.255.255.0

4.2.3 Análisis de Riesgos

A continuación consideraremos los riesgos del proyecto y de la aplicación del Protocolo de Redundancia de Gateway a los cuales se les proveerá solución.

4.2.3.1 Fase de identificación de riesgos

Tabla IV.XII: Identificación de posibles riesgos en la implementación.

Riesgo	**Amenaza**	**Impacto**	**Consecuencia**
1.- El diseño no cumple con las expectativas de los usuarios	No se implementara el diseño de red propuesto	Pérdida de tiempo en el trabajo lo que conlleva a la pérdida económica para la empresa	La empresa mantiene los problemas con los que ha venido trabajando
2.- El desarrollo de la solución no se realiza en los tiempos establecidos	Retraso en la entrega del proyecto	Pérdida económica para la empresa por recursos	Inconvenientes para el trabajo diario de los empleados de la empresa
3.- Negación del servicio	Perdida de conexión con los proveedores de internet	Económico, social y de imagen por falta de comunicación con los clientes	Clientes insatisfechos con el desempeño de la empresa
4.- Daño físico	Fallas de energía	Económico por perdida de	Clientes

	eléctrica, daño en los equipos que implementan el protocolo CARP	recursos	insatisfechos con el desempeño de la empresa

4.2.3.2 Fase de solución de riesgos

Tabla IV.XIII: Solución a los posibles riesgos en la implementación.

Riesgo	**Medida a tomar**
1.	Realizar el diseño y la implementación en base a los requerimientos establecidos
2.	Cumplir la planificación propuesta
3.	Contar con una conexión a internet corporativa que brinda mayores garantías para las empresas.
4.	Acceso restringido a los servidores y equipos de comunicación, instalación de UPS y un mantenimiento constante a los servidores que proporcionan el servicio de redundancia con CARP teniendo todos sus paquetes actualizados.

4.2.4 Gestión de administración y seguridad de la red

En cuanto a la gestión y administración de la red con la implementación del protocolo de redundancia de Gateway CARP, es necesario saber que CARP maneja una seguridad mediante encriptación de los paquetes que sus servidores transmiten entre sí.

a) Administración

El protocolo CARP permite una administración relativamente fácil y segura de la red en la que es implementada. Teniendo necesario el uso de una solo puerta de salida por defecto para todos los host de la red y un control del filtrado de paquetes sencillo mediante la gran integración con packetfilter.

b) Monitoreo

Para monitorear el estado de la conexión y comprobar que los dos servidores de servicio están funcionales, se lo puede realizar por medio de líneas de comando sobre la consola de cualquier terminal en la red con la herramienta tracert en Windows o traceroute en ambientes Unix / Linux. Al igual que con la herramienta ping en cualquiera de los sistemas operativos.

c) Seguridad

A continuación se van a especificar ciertas políticas de seguridad que la empresa deberá considerar en la administración de la red.

- El personal autorizado para el acceso a los servidores CARP son el administrador de la red y en caso de existir el asistente correspondiente.
- Cualquiera que se encuentre conectado físicamente dentro de la red no debe estar capacitado para descifrar los mensajes enviados por el protocolo, esto lo garantiza CARP.
- El administrador debe proporcionar seguridad manteniendo las contraseñas de conexión a los servidores en un lugar seguro y creando estas credenciales con un cierto nivel de dificultad.

- Implementar políticas de seguridad en el firewall CARP para el acceso a los servidores desde el exterior y un buen control del ancho de banda para el buen funcionamiento de la red.

4.3 DISEÑO LÓGICO

4.3.1 DISTRIBUCIÓN DE LAS DIRECCIONES IP SERVIDORES CARP

Las direcciones IP de los firewalls redundantes utilizadas para establecer el funcionamiento del protocolo CARP se las asignara estáticamente usando direcciones privadas de clase C. Las direcciones IP públicas con las que se accederá al internet serán proporcionadas por cada uno de los proveedores de servicio.

a) Configuración interfaces reales

Tabla IV.XIV: Distribución de direcciones de red IP para protocolo CARP.

Nombre del equipo	Dirección IP privada	Interfaz	Dirección IP pública	Interfaz
Firewall Neo	192.168.1.253	em1	No se da a conocer por razones de seguridad	em0
Firewall Trinity	192.168.1.254	em1	No se da a conocer por razones de seguridad	em0

b) Configuración interfaces virtuales

Tabla IV.XV: Configuración de interfaces Virtuales CARP.

Nombre del equipo	Dirección IP privada	Interfaz	vhid	advskew	vhid	Advskew
Firewall Neo	192.168.1.1	carp0	1	0	2	100
Firewall Trinity	192.168.1.1	carp0	1	100	2	0

4.3.2 DISTRIBUCIÓN DE LAS DIRECCIONES IP PARA SERVIDORES Y DEPARTAMENTOS

Se establecerá un rango para la utilización de las direcciones IP utilizadas por los servidores y por los empleados de cada departamento. Al no contar con el hardware necesario para la división lógica de una manera más segura con el uso de VLANS se procederá de la siguiente manera:

Tabla IV.XVI: Distribución de rango de direcciones IP para departamentos.

Detalle	Rango	Network	Difusión	Gateway
Servidores	192.168.1.10 – 192.168.1.20	192.168.1.0	255.255.255.0	192.168.1.1
Departamentos	192.168.1.100 – 192.168.1.200	192.168.1.0	255.255.255.0	192.168.1.1

El detalle de las configuraciones para los servidores es el siguiente:

Tabla IV.XVII: Detalle de direcciones IP para configuración de servidores.

Dispositivo	Descripción	Dirección IP privada
D-Link DIR-635	Servidor DHCP	192.168.1.10

D-Link DIR-630	Repetidor Universal	N/A
Servidor IBM X3200 M2	Share Point	192.168.1.11
Servidor IBM X3200 M2	TeamService	192.168.1.12
Servidor IBM X3200 M2	Apache + MySQL	192.168.1.13

4.4 DISEÑO FÍSICO

4.4.1 CARACTERÍSTICAS DEL SERVICIO DE INTERNET

La empresa Infoquality S.A. cuenta con salida a internet por medio de dos proveedores de internet, a continuación se describen las características.

Tabla IV.XVIII: Características proveedores de internet.

Proveedor	**Horario de Acceso**	**Velocidad**	**Costo Mensual**
Telmex	24 Horas	1024Kbps x 256Kbps	$29.90 USD
TVCable	24 Horas	550Kbps x 150Kbps	$22.00 USD

4.4.2 DIAGRAMA FÍSICO DE LOS EQUIPOS DE LA RED LAN

El siguiente esquema demuestra la disposición física que tendrán los equipos en lo que respecta a conexiones.

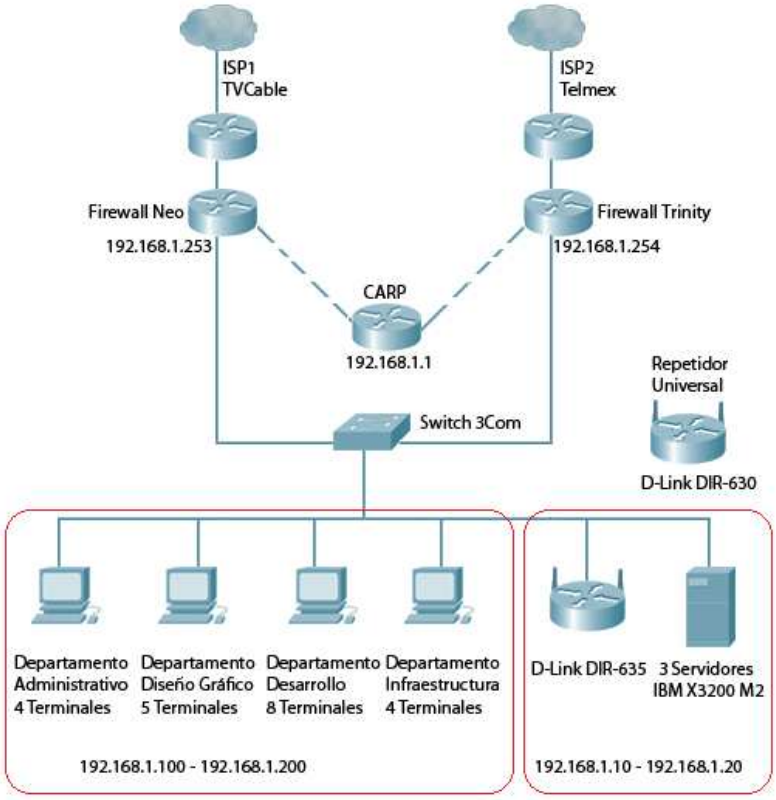


Figura IV.2: Esquema de la nueva red de Infoquality S.A.

4.5 INSTALACIÓN Y CONFIGURACIÓN DE LOS SERVIDORES DE REDUNDANCIA

La instalación y configuración se realizó bajo la plataforma GNU/Linux en la compilación que llamamos IQ-Linux 1.0 utilizando el protocolo CARP, el cual fue la mejor alternativa del estudio comparativo realizado en el capítulo III. A continuación se presentan los pasos necesarios para la instalación y configuración de los servidores CARP.

Paso 1.- Lo primero que se tendrá que hacer es realizar las llamadas necesarias al kernel para el uso de CARP y el reenvío de paquetes IP.

```
# cat /etc/sysctl.conf | grep -v ^#
net.inet.ip.forwarding=1        # 1=Permit forwarding (routing) of IPv4 packets
net.inet.carp.allow=1           # 1=Enable the carp(4) Protocol
net.inet.carp.preempt=1         # 1=Enable carp(4) preemption
                                # required by some ports
# _
```

Figura IV.3: Llamadas de kernel CARP.

Paso 2.- Configuración de las interfaces de red.

```
# cat /etc/hostname.em0
dhcp
# _
```

Figura IV.4: Configuración interfaz de red con el ISP para los firewall Neo y Trinity.

Firewall Neo

```
# cat /etc/hostname.em1
inet 192.168.1.253 255.255.255.0 NONE
#
```

Figura IV.5: Configuración interfaz de red interna firewall Neo.

Firewall Trinity

```
# cat /etc/hostname.em1 > /dev/null && echo "inet 192.168.1.254 255.255.255.0 >
inet 192.168.1.254 255.255.255.0 NONE
# _
```

Figura IV.6: Configuración interfaz de red interna firewall Trinity.

Paso 3.- Configuración de la interfaz virtual CARP.

Firewall Neo

```
# cat /etc/hostname.carp0
inet 192.168.1.1 255.255.255.0 192.168.1.255 balancing ip carpnodes 1:0,2:100 ca
rpdev em1 pass espoch2010
# _
```

Figura IV.7: Configuración interfaz virtual CARP firewall Neo.

Firewall Trinity

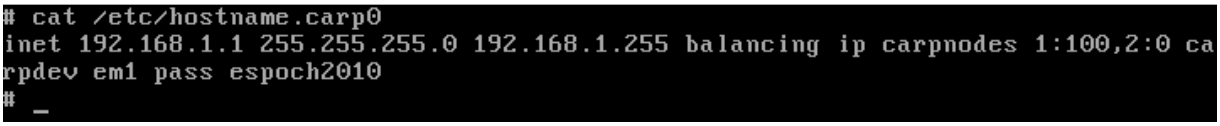


Figura IV.8: Configuración interfaz virtual CARP firewall Trinity.

Paso 4.- Habilitación del filtrado de paquetes con pf (packetfilter).

Figura IV.9: Configuración de pf para los firewall Neo y Trinity.

Paso 5.- Reglas de pf para la traducción de direcciones de red.

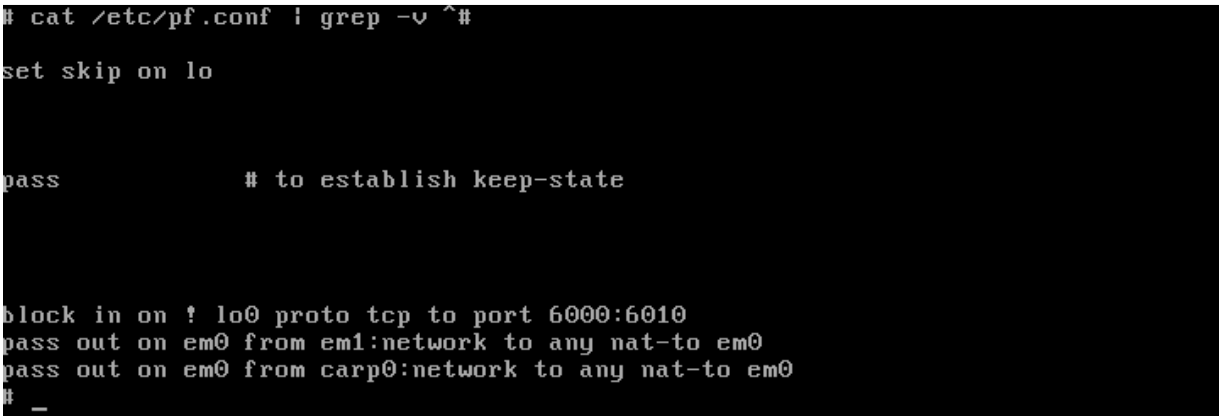


Figura IV.10: Reglas de pf para los firewall Neo y Trinity.

Paso 6.- Creación de un fichero script el cual lee direcciones de internet de un archivo de texto para la comprobación del servicio de internet en la interfaz de salida de cada firewall (Neo y Trinity).

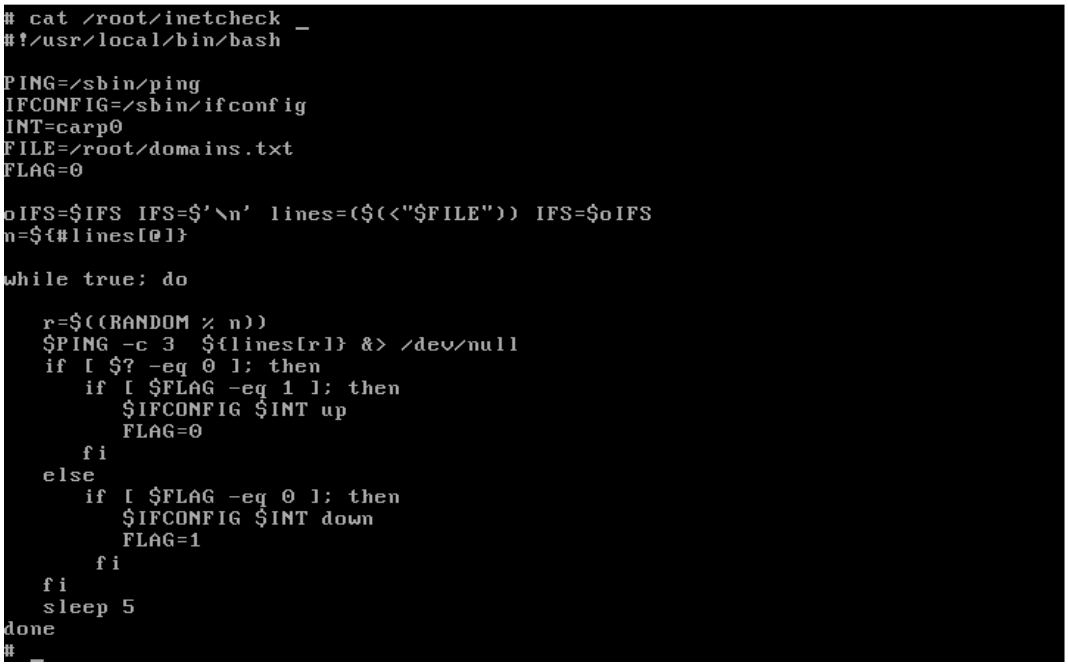


Figura IV.11: Script para la comprobación de internet en las interfaces de conexión ISP.

Archivo de direcciones de internet las cuales fueron seleccionadas teniendo en mente la disponibilidad de los sitios. Se utiliza nombres de dominios y no direcciones IP para comprobar el correcto funcionamiento de los servicios DNS

Figura IV.12: Ejemplo de archivo con dominios para utilización de script inetcheck.

Paso 7.- Se automatiza la ejecución del script con el arranque del sistema.

```
# cat /etc/rc.local | grep -v ^#

echo -n 'starting local daemons:'

/root/inetcheck &> /dev/null &

echo '.'

# _
```

Figura IV.13: Automatización de la ejecución del script inetcheck.

4.6 CONFIGURACIÓN DE LOS TERMINALES DE RED

Dado que el uso del protocolo CARP hace sumamente sencilla la configuración de los terminales de los distintos departamentos, en esta sección mostraremos los pasos para comprobar que estos están utilizando DHCP para obtener su dirección de red.

Paso 1.- Nos dirigimos al panel de control de Windows.

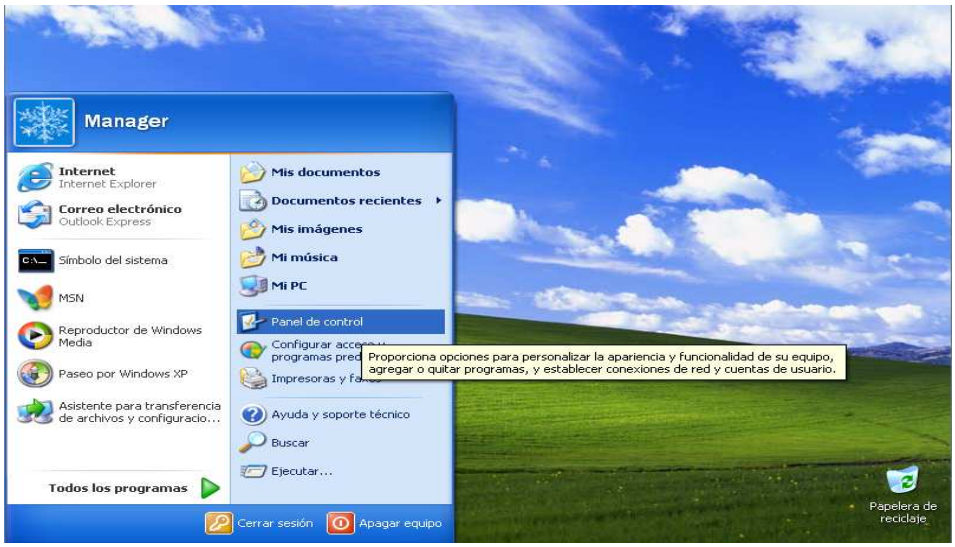


Figura IV.14: Acceso panel de control en maquina cliente.

Paso 2.- Accedemos a las conexiones de red.

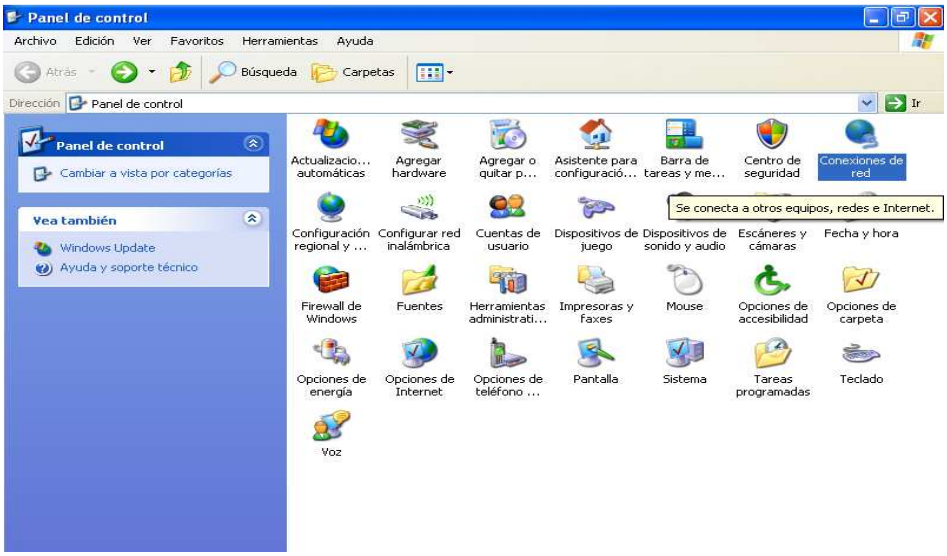


Figura IV.15: Configuraciones de red.

Paso 3.- Hacemos clic derecho sobre la tarjeta de red y seleccionamos propiedades.

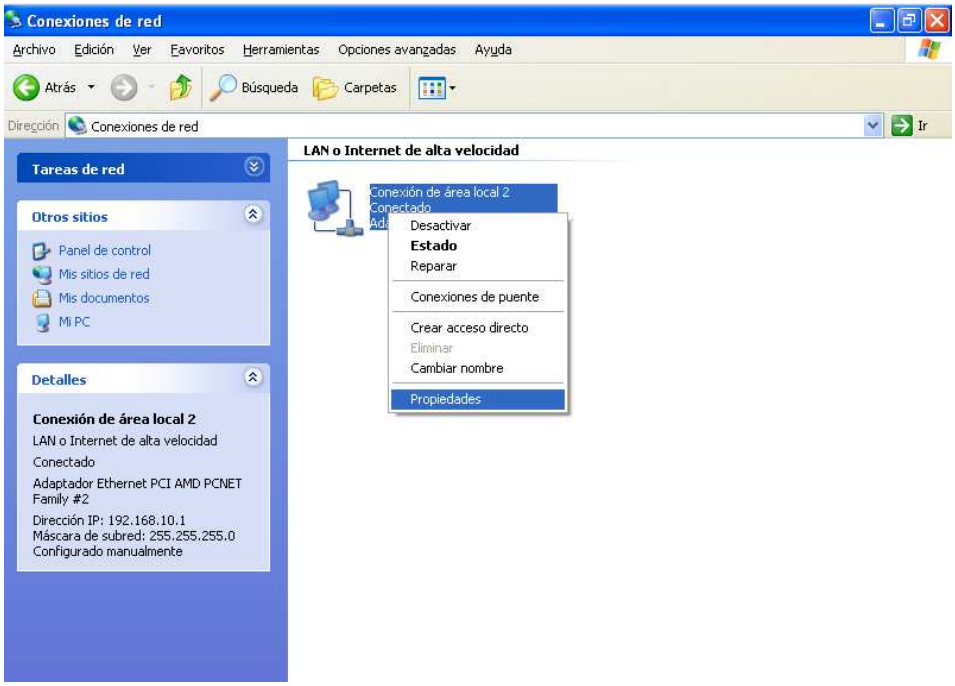


Figura IV.16: Configuración de interfaz de red.

Paso 4.- Ubicamos Protocolo Internet (TCP/IP) y accedemos a sus propiedades

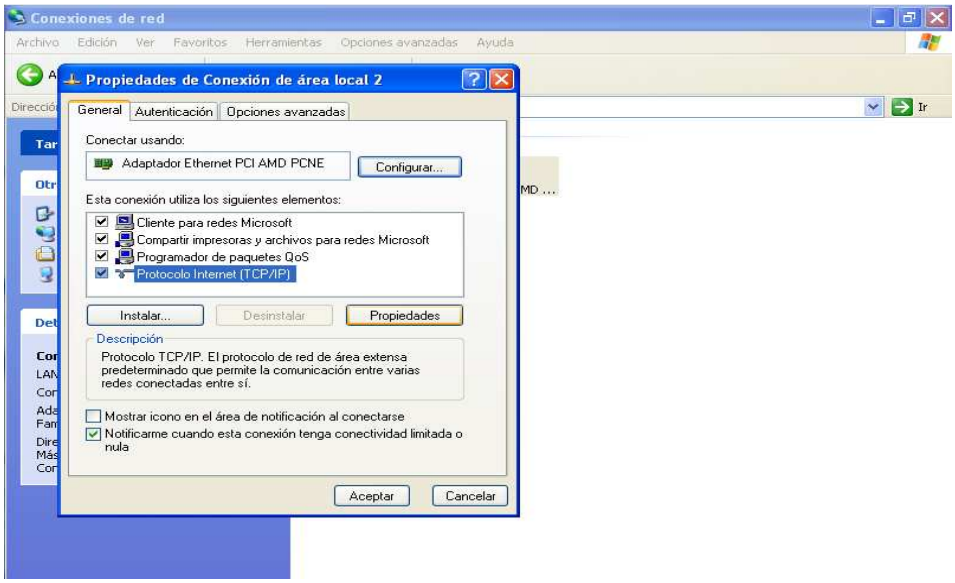


Figura IV.17: Propiedades de interfaz de red.

Paso 5.- Confirmamos que este las opciones obtener una dirección IP automáticamente y obtener la dirección del servidor DNS automáticamente estén seleccionadas y hacemos clic en aceptar.

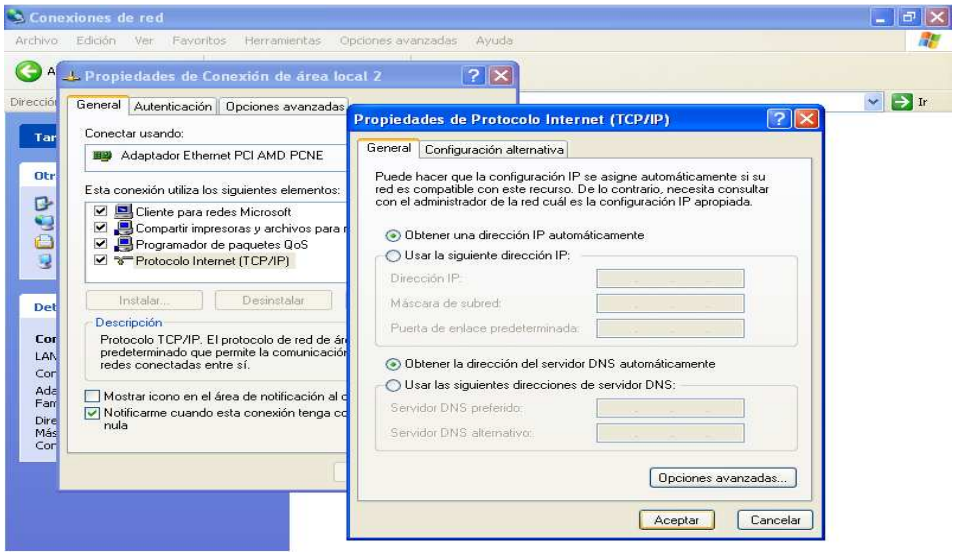


Figura IV.18: Correcta configuración de los terminales de red.

En el caso de los servidores de la empresa Infoquality S.A. cada tiene configurada la dirección IP correspondiente de manera estática por el administrador de red.

4.7 PRUEBAS DE VERIFICACIÓN

Para comprobar que todo está correctamente configurado y funcionando incluso después de reiniciar cualquiera de los dos firewall se podrán realizar cualquiera de las siguientes pruebas.

a) ifconfig

Con la utilidad ifconfig se podrá ver el estado de las interfaces virtuales en cada uno de los servidores CARP. Los parámetros importantes que se deberán tener en cuenta son:

- flags, si la interfaz tiene la bandera RUNNING activa.
- carp, si el modo de balanceo aplicado es balancingip.
- state, si el estado del firewall es INIT, BACKUP, MASTER para cada uno de los identificadores de terminal virtual (VHID).

Firewall Neo

```
# ifconfig carp0
carp0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        lladdr 01:00:5e:00:01:01
        priority: 0
        carp: carpdev em1 advbase 1 balancing ip
                state MASTER vhid 1 advskew 0
                state BACKUP vhid 2 advskew 100
        groups: carp
        inet6 fe80::a00:27ff:fe0e:f3f4%carp0 prefixlen 64 scopeid 0x5
        inet 192.168.1.1 netmask 0xffffff00 broadcast 192.168.1.255
#
```

Figura IV.19: Ejecución comando ifconfig firewall Neo.

Firewall Trinity

Figura IV.20: Ejecución comando ifconfig firewall Trinity.

b) inetcheck

Con la siguiente prueba se confirmará que el script de comprobación de internet está ejecutándose correctamente en el equipo.

Figura IV.21: Comprobación de ejecución del script inetcheck.

c) systat

Con el comando #systatstates se podrá revisar parámetros importantes de la interfaz virtual CARP.

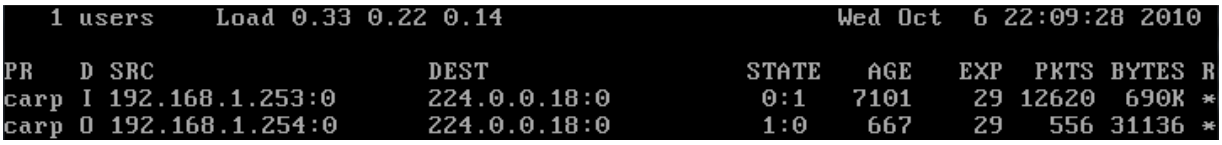


Figura IV.22: Información de las interfaces virtuales CARP.

d) traceroute y tracert

Haciendo uso de la herramienta de consola traceroute en ambientes Unix/Linux y tracert en ambientes Windows se podrá realizar una de las pruebas más importantes de este estudio que será ver el camino que están tomando los paquetes que salen al internet desde la red interna LAN.

Se logrará tener claro que se realiza un balanceo de carga por parte del protocolo CARP e igualmente cual es comportamiento del protocolo cuando una de las conexiones se cae y cuando esta vuelve a levantarse.

Por motivos de políticas de seguridad de la empresa, las pruebas realizadas en Infoquality S.A., no podrán ser publicadas en este documento por lo que haremos referencia a los anexos en los prototipos de prueba.

4.8 SERVICIOS COMPLEMENTARIOS PARA LA RED

Los servicios adicionales que aseguran un buen desempeño de la red son:

- Filtrado de paquetes
- Proxy

El firewall de redundancia de Gateway CARP puede ser complementado con pf para realizar un filtrado de paquetes dejando pasar y salir solo el tráfico de los equipos permitidos (de acuerdo a los requerimientos de los empleados) y el acceso desde internet a los servidores internos (de acuerdo a los requerimientos de los clientes).

El proxy transparente conjuntamente con dansguardian permitirá filtrar la navegación web a sitios que no tienen ninguna importancia para el desenvolvimiento de la empresa, permitiendo hacer un buen uso del ancho de banda.

CONCLUSIONES

1. La redundancia en las redes informáticas es una característica altamente deseable lo que es posible descartarla completamente con la finalidad de prevenir las interrupciones de servicio.
2. Los protocolos de redundancia de Gateway están enfocados en proveer una administración transparente de la puerta de enlace predeterminada. Para esto todos se centran en la utilización de una dirección IP virtual que define un Router virtual el que es mantenido a merced del intercambio de paquetes de anuncio de publicidad entre los dispositivos que forman parte del grupo del Router virtual.
3. Utilizando ambientes de simulación donde se configuro y explotó todas las características de los dos protocolos de redundancia VRRP y CARP, se demostró que la utilización de estosprotocolos reduce significativamente el tiempo medio entre fallos, logrando que los fallos en el proveedor de servicio de internet sean imperceptibles para los usuarios de la red.
4. Existen soluciones de software libre que son de muy alto nivel como lo es CARP en comparación a soluciones patentadas como HSRP de la empresa CISCO. Por otro lado VRRP es un desarrollo que fue concebido como solución de código libre basado en los conceptos del protocolo HSRP por lo que ahora se debate una batalla legal sobre infracción de patente.
5. Después de realizar un estudio comparativo entre los protocolos VRRP y CARP para determinar cuál de los dos protocolos debería implementarse en la empresa Infoquality S.A. para mejorar el tiempo medio entre fallos, se llegó a la conclusión de que el

protocolo CARP brinda mejores prestaciones sobre VRRP y sería la solución adecuada para solucionar los problemas de la empresa.

6. Con la implementación de una red redundante en Gateway para la empresa Infoquality S.A. y el uso del protocolo CARP, se logró brindar una mejor administración de los recursos de la empresa para el uso de sus colaboradores.
7. Con el uso del protocolo de redundancia de Gateway CARP se logró una fácil administración de la red de la empresa, brindando la posibilidad para que la misma crezca en terminales de trabajo sin necesidad de la realización de un mantenimiento complejo en la misma para integrar los nuevos dispositivos.
8. La seguridad implementada por CARP brinda seguridad al administrador de red y la confianza necesaria para saber que ninguna persona analizando el tráfico de la red podrá alterar el funcionamiento de los firewall redundantes. El enfoque principal de CARP es en la criptografía y la seguridad, por lo que todos los mensajes compartidos por el protocolo no podrán ser decodificados.
9. Los tiempos medios entre fallos (MTBF) se redujeron para los meses de julio en un 78% y en el mes de agosto en un 71 %, demostrando que la solución propuesta con el protocolo CARP en la empresa Infoquality S.A, ayudó a eliminar los inconvenientes de conexión.

RECOMENDACIONES

1. Aunque con el uso de un protocolo de redundancia de Gateway se puede mejorar el tiempo medio entre fallos en la conexión a internet, también es recomendable ante de nada tener unos buenos proveedores de internet. Compañías que respalden a las empresas que hacen uso de su servicio, que cuenten con buenos equipos, un buen soporte al cliente.
2. La implementación de reglas de filtrado de paquetes con pf es una buena práctica para mejorar el desempeño de la red. pf tiene una excelente integración con CARP que puede ser aprovechado por el administrador de la red para un mayor control sobre el tráfico que es generado en la red hacia el internet y desde el internet hacia la red interna.
3. Aunque la red permite una expansión de hasta 200 terminales, es recomendable utilizar hardware que permita realizar una segmentación de la red haciendo uso de VLANS por departamento. Esto aumentara la seguridad en la información que es procesada dentro de la empresa y un mejor control del ancho de banda necesario para cada grupo de personas.
4. El uso de VRRP y CARP no solo se limita a la aplicación en la WAN, cuando se tiene servidores importantes que no pueden dejar de brindar servicio a los usuarios se recomienda usar un espejo que este configurado con uno de los dos protocolos para lograr una disponibilidad máxima.
5. Impulsar el uso de herramientas que permitan crear redundancia en los distintos niveles de una red, asegurando un funcionamiento del 99.9999% de los servicios más críticos.

RESUMEN

La implementación de un esquema que se basa en redundancia de Gateway, aplicado con el protocolo CARP o VRRP sobre GNU/Linux brinda una conexión permanente hacia el internet para equipos de cómputo que se encuentran divididos en dos grupos.

Para poder escoger el protocolo más adecuado se realizó un estudio comparativo mediante un muestreo de variables, con sus respectivos indicadores, y además una comparación de un antes y un después de los tiempos medios entre fallos.

Se debe plantear dos esquemas de solución para cada protocolo; el primero, para VRRP presenta dos Routers Virtuales 1 y 2 donde la mitad de equipos configuran como puerta de enlace predeterminado la ip del Router Virtual 1 y la otra mitad la del Router Virtual 2. Con CARP se crea un grupo de firewall redundantes, dos equipos realizan el filtrado de paquetes si uno falla el otro se hará cargo de la operación que realizaba el firewall que falló.

Los resultados que se obtienen es una conexión confiable al internet, con tiempos de transición transparentes para el usuario.

Mediante el análisis de los dos protocolos, obtiene la conclusión que CARP ofrece más viabilidad para implantar la solución, y además los tiempos medios entre fallos se disminuyen en relación a los datos originales.

Se recomienda antes de plantear los esquemas de solución obtener la mayor información científica sobre el fundamento teórico de los protocolos, para no tener inconvenientes al momento de la implementación.

SUMMARY

The implementation of a scheme that is based on redundancy Gateway, applied with the CARP or VRRP protocol on GNU / Linux, provides a permanent connection to the Internet for computers which are divided into two separate groups.

In order to be able to choose the best protocol, it was performed a comparative study on a sample of variables with their indicators, and also a comparison of before and after the mean time between failures.

It should be considered two solution schemes for each protocol, the first one for VRRP has two Virtual Routers 1 and 2 where half of the computers group was set up as default gateway the Virtual Router 1 IP and the other half the Virtual Router 2 IP. With CARP it was created a redundant firewall group, two servers perform packet filtering if one fails the other will take over the operation that carried out the failed firewall.

The result obtained is a reliable connection to the internet, with times of transition transparent to the final user.

By analyzing the two protocols, it gets the conclusion that CARP provides more feasibility to be implemented as the solution, and also the average time between failures was decreased in relation to the original data.

It is recommended before considering the solution schemes to obtain as much scientific information on the theoretical foundation of the protocols as possible, to avoid any inconvenience at the implementation time.

BIBLIOGRAFÍA

1.- SRIKANTH A. VRRP: Increasing Reliability and Failover with the Virtual Router Redundancy Protocol.Pearson Education S. A. Boston, EstadosUnidos. 2002. 560p.

2.- SURHONE M. Common Address redundancy Protocol.BetascriptPubllishing. Ohio, Estados Unidos. 2010. 146p.

3.- HANSTEEN P. The Book of PF: A No-Nonsense Guide to the OpenBSD Firewall. No Strach Press. Toronto, Canada. 2008. 184p.

4.- KROAH-HARTMAN G.Linux Kernel in a Nutshell.O'Reilly Media. New Jersey, Estados Unidos.2009. 198p.

DIRECCIONES DE INTERNET

5.- Kernel Trap: Porting CARP to kernel 2.6. (2004/06/20)

http://kerneltrap.com/node/3496

(2010/06/20)

6.- Kernel Trap: CARP: Common Address Redundancy Protocol for Linux kernel release. (2008/06/14)

https://kerneltrap.org/mailarchive/linux-netdev/2008/6/14/2126334

(2010/07/14)

7.-HowtoForge: Step-By-Step Configuration of NAT with iptables (2006/11/08)

http://grouper.ieee.org/groups/802/11

(2010/07/28)

8.- Introduction to the Common Address Redundancy Protocol (CARP) (2010/01/16)

http://www.netbsd.org/docs/guide/en/chap-carp.html#chap-carp-force

(2010/06/16)

9.- Tablas Estadísticas: Chi Cuadrado (2009/05/16)

http://www.wiphala.net/research/manual/statistic/chi_cuadrado.html

(2010/08/10)

10.- Mis Libros de Networking (2009/08/25)

http://librosnetworking.blogspot.com/2009/08/redundancia-de-gateway.html

(2010/07/25)

ANEXOS

ANEXO 1

Prototipo de prueba VRRP

1.- Descripción de la red

Para realizar las pruebas de funcionalidad y poder realizar el estudio comparativo de los protocolos se implementaron prototipos de red. En el caso de VRRP el diseño de red utilizado es el siguiente:

a) Hardware

Se utilizó seis máquinas virtuales usando el software libre Oracle VM VirtualBox.

Nombre Máquina Virtual	**Sistema Operativo**	**Descripción**
ISPA	Windows XP	Utilizado como proveedor de servicio de internet
ISPB	Windows XP	Utilizado como proveedor de servicio de internet
FWA_LINUX	Ubuntu Server 10.4	Utilizado como Router VRRP conectado a ISPA
FWB_LINUX	Ubuntu Server 10.4	Utilizado como Router VRRP conectado a ISPB
TERMINAL_A	Ubuntu Desktop 10.4	Utilizado como terminal de la red interna
TERMINAL_B	Ubuntu Desktop 10.4	Utilizado como terminal de la red interna

b) Direccionamiento lógico

Las direcciones IP utilizadas en el esquema de red.

Nombre Máquina Virtual	**Dirección IP**	**Dirección IP**	**Gateway**

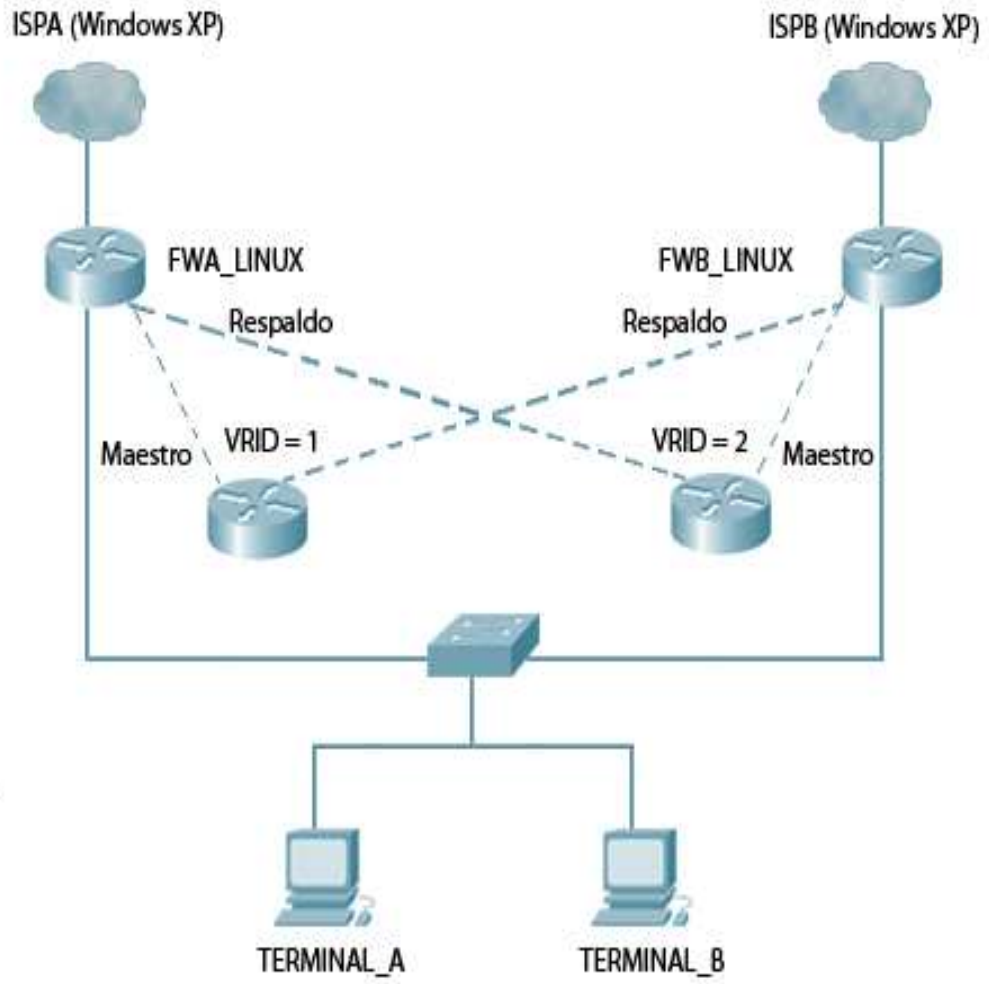
ISPA	192.168.10.1	-	-
ISPB	192.168.20.1	-	-
FWA_LINUX	192.168.10.2	10.10.10.10	192.168.10.1
FWB_LINUX	192.168.20.2	10.10.10.11	192.168.20.1
TERMINAL_A		10.10.10.100	10.10.10.1
TERMINAL_B		10.10.10.200	10.10.10.2

c) Configuración VRRP

Parámetros utilizados para la configuración del protocolo VRRP

Router VRRP	**Interfaz**	**VRID**	**Dirección Virtual**	**Prioridad**	**Estado**
FWA_LINUX	eth1	1	10.10.10.1	150	Maestro
FWA_LINUX	eth1	2	10.10.10.2	100	Respaldo
FWB_LINUX	eth1	1	10.10.10.1	100	Respaldo
FWB_LINUX	eth1	2	10.10.10.2	150	Maestro

2.- Esquema de red



3.- Instalación y configuración

Paso 1.- Se configurara las interfaces de red en cada uno de los servidores.

FWA_LINUX

```
manager@FWA:~$ cat /etc/network/interfaces | grep -v ^#

auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.10.2
gateway 192.168.10.1
netmask 255.255.255.0
network 192.168.10.0
broadcast 192.168.10.255

auto eth1
iface eth1 inet static
address 10.10.10.10
netmask 255.255.255.0
network 10.10.10.0
broadcast 10.10.10.255
manager@FWA:~$
```

FWB_LINUX

```
manager@FWB:~$ cat /etc/network/interfaces | grep -v ^#

auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.20.2
netmask 255.255.255.0
network 192.168.20.0
broadcast 192.168.20.255
gateway 192.168.20.1

auto eth1
iface eth1 inet static
address 10.10.10.11
netmask 255.255.255.0
network 10.10.10.0
broadcast 10.10.10.255
manager@FWB:~$
```

Paso 2.- Hacer las llamadas necesarias al kernel para habilitar el reenvío de paquetes IP.

```
manager@FWB:~$ cat /etc/rc.local | grep -v ^#

sysctl -w net.ipv4.ip_forward=1
```

Paso 3.- Se crea un script que para realizar las siguientes funciones:

- Realizar las reglas de netfilter para la habilitación de la traducción de direcciones de red.
- Configurar el protocolo VRRP

FWA_LINUX

```
manager@FWA:~$ cat /etc/vrrpd/vrrp | grep -v ^$
#!/bin/bash
# GLOBAL VARIABLES
IPT=/sbin/iptables
ECHO=/bin/echo
EXT=eth0
INT=eth1
VRRPD=/usr/sbin/vrrpd
VRRPDIP_MASTER=10.10.10.1
VRRPDIP_BACKUP=10.10.10.2
# IP FORWARD
$ECHO 1 > /proc/sys/net/ipv4/ip_forward
# NAT CONFIGURATION
$IPT --flush
$IPT --table nat --flush
$IPT --delete-chain
$IPT --table nat --delete-chain
$IPT --table nat --append POSTROUTING --out-interface $EXT -j MASQUERADE
$IPT --append FORWARD --in-interface $INT -j ACCEPT
# VRRP CONFIGURATION
$VRRPD -n -i $INT -v 1 -p 150 $VRRPDIP_MASTER -D
$VRRPD -n -i $INT -v 2 -p 100 $VRRPDIP_BACKUP -D
manager@FWA:~$ _
```

FWB_LINUX

```
manager@FWB:~$ cat /etc/vrrpd/vrrp | grep -v ^$
#!/bin/bash
# GLOBAL VARIABLES
IPT=/sbin/iptables
ECHO=/bin/echo
EXT=eth0
INT=eth1
VRRPD=/usr/sbin/vrrpd
VRRPDIP_MASTER=10.10.10.2
VRRPDIP_BACKUP=10.10.10.1
# IP FORWARD
$ECHO 1 > /proc/sys/net/ipv4/ip_forward
# NAT CONFIGURATION
$IPT --flush
$IPT --table nat --flush
$IPT --delete-chain
$IPT --table nat --delete-chain
$IPT --table nat --append POSTROUTING --out-interface $EXT -j MASQUERADE
$IPT --append FORWARD --in-interface $INT -j ACCEPT
# VRRP CONFIGURATION
$VRRPD -n -i $INT -v 2 -p 150 $VRRPDIP_MASTER -D
$VRRPD -n -i $INT -v 1 -p 100 $VRRPDIP_BACKUP -D
manager@FWB:~$ _
```

Paso 4.- Creación de un fichero script el cual lee direcciones de internet de un archivo de texto para la comprobación del servicio de internet en la interfaz de salida.

```
manager@FWB:~$ cat /etc/vrrpd/inetcheck
#!/bin/bash

PING=/bin/ping
IFCONFIG=/sbin/ifconfig
INT=eth1
FILE=/etc/vrrpd/domains.txt
FLAG=0

oIFS=$IFS IFS=$'\n' lines=($(<"$FILE")) IFS=$oIFS
n=${#lines[@]}

while true; do

   r=$((RANDOM % n))
   $PING -c 3  ${lines[r]} &> /dev/null
   if [ $? -eq 0 ]; then
      if [ $FLAG -eq 1 ]; then
         $IFCONFIG $INT up
         FLAG=0
      fi
   else
      if [ $FLAG -eq 0 ]; then
         $IFCONFIG $INT down
         FLAG=1
       fi
   fi
   sleep 5
done
manager@FWB:~$
```

Archivo de direcciones de internet las cuales fueron seleccionadas teniendo en mente la disponibilidad de los sitios. Se utiliza nombres de dominios y no direcciones IP para comprobar el correcto funcionamiento de los servicios DNS

```
manager@FWB:~$ cat /etc/vrrpd/domains.txt
www.google.com
www.yahoo.com
www.youtube.com
www.terra.es
manager@FWB:~$
```

Cabe resaltar que para los dos servidores CARP se utilizara el mismo script.

Paso 5.- Se automatiza la ejecución de los dos scripts con el arranque del sistema.

```
manager@FWB:~$ cat /etc/rc.local
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.

sysctl -w net.ipv4.ip_forward=1
/etc/vrrpd/vrrp
/etc/vrrpd/inetcheck &> /dev/null &

exit 0
```

4.- Pruebas de verificación

a) Ejecución del protocolo

Para comprobar que el protocolo esté funcionando correctamente se revisara la ejecución del script vrrp y el script inetcheck.

```
manager@FWB:~$ ps waux | grep vrrp
root       707  0.0  0.2   4032   540 ?        Ss   16:06   0:01 /usr/sbin/vrrpd
 -n -i eth1 -v 2 -p 150 10.10.10.2 -D
root       709  0.0  0.2   4032   548 ?        Ss   16:06   0:01 /usr/sbin/vrrpd
 -n -i eth1 -v 1 -p 100 10.10.10.1 -D
root       710  0.0  0.6  17676  1512 ?        S    16:06   0:00 /bin/bash /etcv
rrpd/inetcheck
manager   2168  0.0  0.3   7624   912 tty1     S+   18:05   0:00 grep --color=au
to vrrp
manager@FWB:~$ ps waux | grep inetcheck
root       710  0.0  0.6  17676  1512 ?        S    16:06   0:00 /bin/bash /etc/
vrrpd/inetcheck
manager   2178  0.0  0.3   7624   916 tty1     S+   18:07   0:00 grep --color=au
to inetcheck
manager@FWB:~$ _
```

b) Funcionamiento de protocolo

En esta sección comprobaremos el comportamiento del protocolo ante fallas de uno de sus proveedores de servicio de internet.

I) Ejecución del comando ping

Ejecutando el comando ping podremos confirmar la conectividad hacia internet cuando todo está funcionando normalmente.

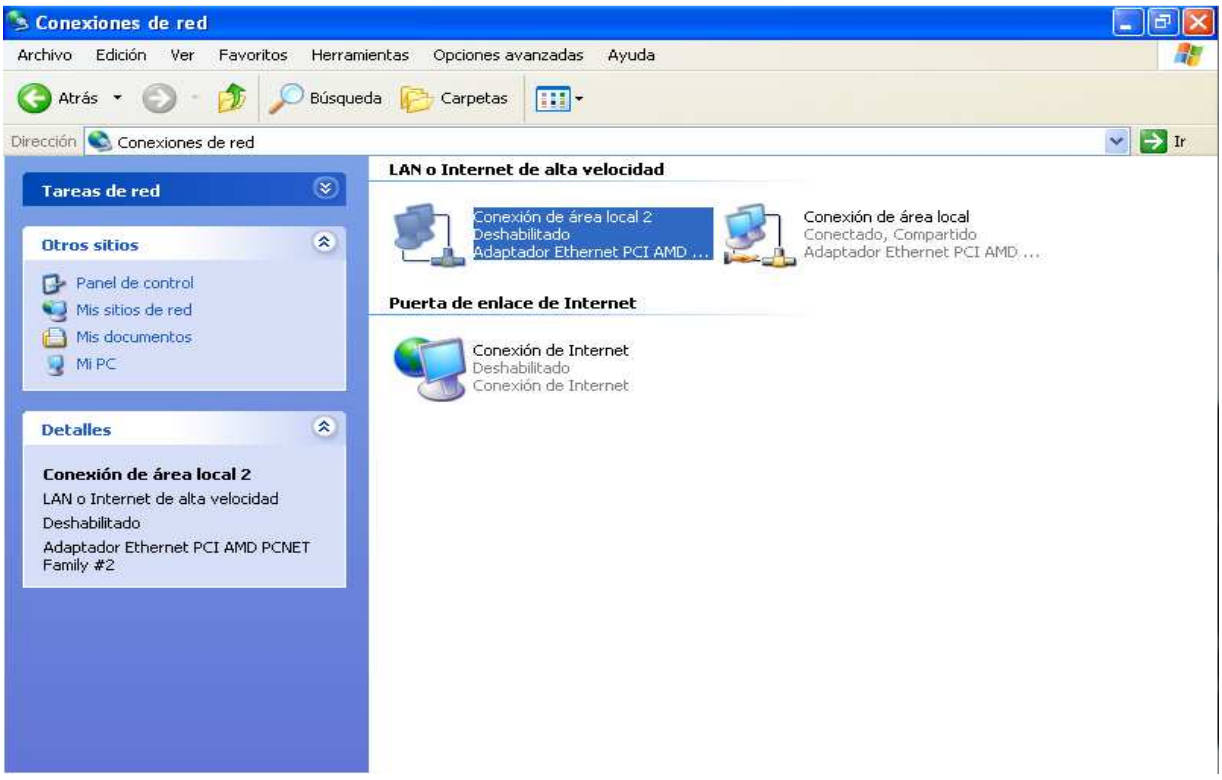
```
manager@terminal-a:~$ ping www.google.com -c 10
PING www.l.google.com (74.125.47.106) 56(84) bytes of data.
64 bytes from yw-in-f106.1e100.net (74.125.47.106): icmp_seq=1 ttl=47 time=121 m
s
64 bytes from yw-in-f106.1e100.net (74.125.47.106): icmp_seq=2 ttl=47 time=144 m
s
64 bytes from yw-in-f106.1e100.net (74.125.47.106): icmp_seq=3 ttl=47 time=115 m
s
64 bytes from yw-in-f106.1e100.net (74.125.47.106): icmp_seq=4 ttl=47 time=118 m
s
64 bytes from yw-in-f106.1e100.net (74.125.47.106): icmp_seq=5 ttl=47 time=149 m
s
64 bytes from yw-in-f106.1e100.net (74.125.47.106): icmp_seq=6 ttl=47 time=142 m
s
64 bytes from yw-in-f106.1e100.net (74.125.47.106): icmp_seq=7 ttl=47 time=112 m
s
64 bytes from yw-in-f106.1e100.net (74.125.47.106): icmp_seq=8 ttl=47 time=99.9
ms
64 bytes from yw-in-f106.1e100.net (74.125.47.106): icmp_seq=9 ttl=47 time=175 m
s
64 bytes from yw-in-f106.1e100.net (74.125.47.106): icmp_seq=10 ttl=47 time=148
ms

--- www.l.google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9019ms
rtt min/avg/max/mdev = 99.965/132.780/175.167/21.528 ms
manager@terminal-a:~$ _
```

II) Ejecución del comando traceroute para comprobar el camino que están tomando los paquetes que salen desde la red interna al internet.

```
manager@terminal-a:~$ traceroute www.google.com -m 10
traceroute to www.google.com (74.125.65.105), 10 hops max, 60 byte packets
 1  10.10.10.10 (10.10.10.10)  2.379 ms  2.311 ms  2.255 ms
 2  ispa.mshome.net (192.168.10.1)  3.810 ms  3.761 ms  3.706 ms
 3  192.168.0.1 (192.168.0.1)  4.976 ms  5.955 ms  5.905 ms
 4  host-200-124-230-65.ecutel.net (200.124.230.65)  250.230 ms  251.179 ms  254
.107 ms
 5  172.21.21.126 (172.21.21.126)  254.060 ms  254.018 ms  254.017 ms
 6  172.21.16.58 (172.21.16.58)  256.533 ms  247.322 ms  249.144 ms
 7  172.21.0.240 (172.21.0.240)  249.793 ms  874.783 ms  878.288 ms
 8  172.21.0.253 (172.21.0.253)  878.242 ms  881.970 ms  883.101 ms
 9  customer-205-126.porta.net (200.25.205.126)  883.052 ms  882.999 ms  882.946
 ms
10  so-7-3-0.usa.nmi-core02.columbus-networks.com (63.245.20.57)  885.592 ms  88
5.552 ms  886.036 ms
manager@terminal-a:~$ _
```

III) Ejecución del comando ping y simulación de la caída en la conexión con ISPA

Para simular una caída en la conexión de internet, se deshabilitara la interfaz que está conectada a FWA_LINUX en la máquina virtual ISPA.



A continuación el script inetcheck al detectar que la conexión se perdió con el proveedor de servicio de internet ISPA, este se encargara de deshabilitar la interfaz que utiliza el protocolo

VRRP (eth1 en FWA_LINUX) obligando al Router de respaldo a tomar la dirección IP virtual (FWB_LINUX).

```
manager@FWA:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ab:dc:b7
          inet addr:192.168.10.2  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feab:dcb7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:512 errors:0 dropped:0 overruns:0 frame:0
          TX packets:778 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:82781 (82.7 KB)  TX bytes:62191 (62.1 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:81 errors:0 dropped:0 overruns:0 frame:0
          TX packets:81 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:8187 (8.1 KB)  TX bytes:8187 (8.1 KB)

manager@FWA:~$
```

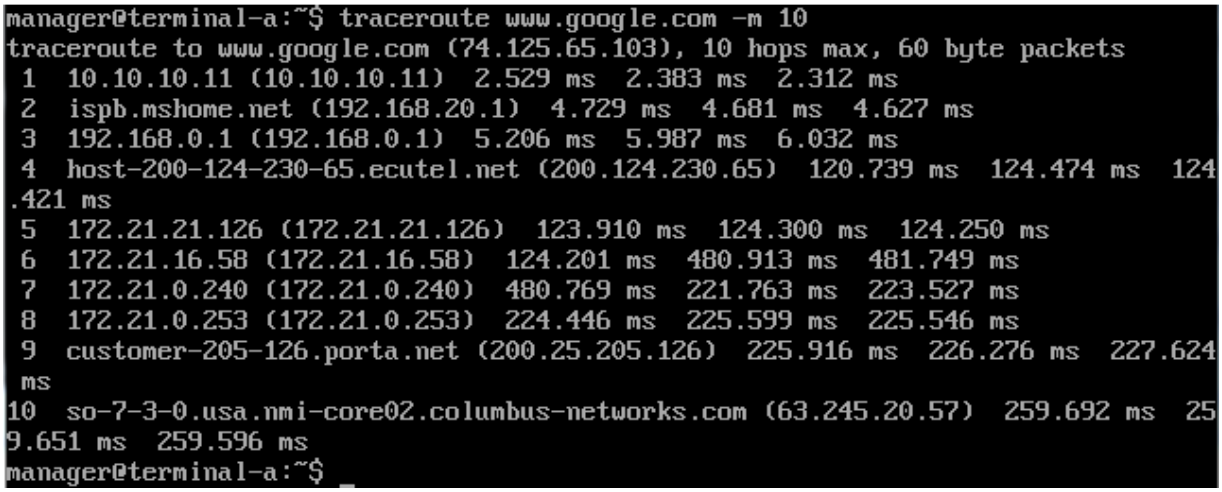
Al momento de producirse la caída en la conexión a internet se puede observar que en el tiempo de transición de estados en los Router VRRP existe una pérdida de 14 paquetes que significa una pérdida de conexión de aproximadamente 13.53 segundos.

```
manager@terminal-a:~$ ping www.google.com -c 30
PING www.l.google.com (72.14.253.104) 56(84) bytes of data.
64 bytes from mia04s03-in-f104.1e100.net (72.14.253.104): icmp_seq=1 ttl=53 time
=93.4 ms
64 bytes from mia04s03-in-f104.1e100.net (72.14.253.104): icmp_seq=2 ttl=53 time
=80.1 ms
64 bytes from mia04s03-in-f104.1e100.net (72.14.253.104): icmp_seq=3 ttl=53 time
=2798 ms
64 bytes from mia04s03-in-f104.1e100.net (72.14.253.104): icmp_seq=4 ttl=53 time
=1791 ms
64 bytes from mia04s03-in-f104.1e100.net (72.14.253.104): icmp_seq=5 ttl=53 time
=784 ms
64 bytes from mia04s03-in-f104.1e100.net (72.14.253.104): icmp_seq=6 ttl=53 time
=129 ms
64 bytes from mia04s03-in-f104.1e100.net (72.14.253.104): icmp_seq=20 ttl=53 tim
e=87.2 ms
64 bytes from mia04s03-in-f104.1e100.net (72.14.253.104): icmp_seq=21 ttl=53 tim
e=84.8 ms
```

```
=784 ms
64 bytes from mia04s03-in-f104.1e100.net (72.14.253.104): icmp_seq=6 ttl=53 time
=129 ms
64 bytes from mia04s03-in-f104.1e100.net (72.14.253.104): icmp_seq=20 ttl=53 tim
e=87.2 ms
64 bytes from mia04s03-in-f104.1e100.net (72.14.253.104): icmp_seq=21 ttl=53 tim
e=84.8 ms
64 bytes from mia04s03-in-f104.1e100.net (72.14.253.104): icmp_seq=22 ttl=53 tim
e=88.5 ms
64 bytes from mia04s03-in-f104.1e100.net (72.14.253.104): icmp_seq=23 ttl=53 tim
e=224 ms
64 bytes from mia04s03-in-f104.1e100.net (72.14.253.104): icmp_seq=24 ttl=53 tim
e=445 ms
64 bytes from mia04s03-in-f104.1e100.net (72.14.253.104): icmp_seq=25 ttl=53 tim
e=108 ms
64 bytes from mia04s03-in-f104.1e100.net (72.14.253.104): icmp_seq=26 ttl=53 tim
e=191 ms
64 bytes from mia04s03-in-f104.1e100.net (72.14.253.104): icmp_seq=27 ttl=53 tim
e=79.9 ms
64 bytes from mia04s03-in-f104.1e100.net (72.14.253.104): icmp_seq=28 ttl=53 tim
e=717 ms
64 bytes from mia04s03-in-f104.1e100.net (72.14.253.104): icmp_seq=29 ttl=53 tim
e=127 ms
64 bytes from mia04s03-in-f104.1e100.net (72.14.253.104): icmp_seq=30 ttl=53 tim
e=84.0 ms

--- www.l.google.com ping statistics ---
30 packets transmitted, 17 received, 43% packet loss, time 75057ms
rtt min/avg/max/mdev = 79.941/465.673/2798.798/722.226 ms, pipe 3
manager@terminal-a:~$
```

IV) Ejecución del comando traceroute y simulación de la caída en la conexión con ISPA

Para simular una caída en la conexión de internet, se realizara el mismo proceso de la sección anterior. Una vez que FWB_LINUX esté en control del Router virtual VRID = 1, el terminal TERMINAL_A podrá navegar a través del ISPB a internet.


manager@terminal-a:~$ traceroute www.google.com -m 10
traceroute to www.google.com (74.125.65.103), 10 hops max, 60 byte packets
1 10.10.10.11 (10.10.10.11) 2.529 ms 2.383 ms 2.312 ms
2 ispb.mshome.net (192.168.20.1) 4.729 ms 4.681 ms 4.627 ms
3 192.168.0.1 (192.168.0.1) 5.206 ms 5.987 ms 6.032 ms
4 host-200-124-230-65.ecutel.net (200.124.230.65) 120.739 ms 124.474 ms 124
.421 ms
5 172.21.21.126 (172.21.21.126) 123.910 ms 124.300 ms 124.250 ms
6 172.21.16.58 (172.21.16.58) 124.201 ms 480.913 ms 481.749 ms
7 172.21.0.240 (172.21.0.240) 480.769 ms 221.763 ms 223.527 ms
8 172.21.0.253 (172.21.0.253) 224.446 ms 225.599 ms 225.546 ms
9 customer-205-126.porta.net (200.25.205.126) 225.916 ms 226.276 ms 227.624
ms
10 so-7-3-0.usa.nmi-core02.columbus-networks.com (63.245.20.57) 259.692 ms 25
9.651 ms 259.596 ms
manager@terminal-a:~$

ANEXO 2

Prototipo de prueba CARP

1.- Descripción de la red

Para realizar las pruebas de funcionalidad y poder realizar el estudio comparativo de los protocolos se implementaron prototipos de red. En el caso de CARP el diseño de red utilizado es el siguiente:

a) Hardware

Se utilizó seis máquinas virtuales usando el software libre Oracle VM VirtualBox.

Nombre Máquina Virtual	**Sistema Operativo**	**Descripción**
ISPA	Windows XP	Utilizado como proveedor de servicio de internet
ISPB	Windows XP	Utilizado como proveedor de servicio de internet
FWA_IQLINUX	IQ Linux 1.0	Utilizado como firewall CARP conectado a ISPA
FWB_IQLINUX	IQ Linux 1.0	Utilizado como firewall CARP conectado a ISPB
TERMINAL_A	Ubuntu Desktop 10.4	Utilizado como terminal de la red interna
TERMINAL_B	Ubuntu Desktop 10.4	Utilizado como terminal de la red interna

b) Direccionamiento lógico

Las direcciones IP utilizadas en el esquema de red.

Nombre Máquina Virtual	**Dirección IP**	**Dirección IP**	**Gateway**
ISPA	192.168.10.1	-	-

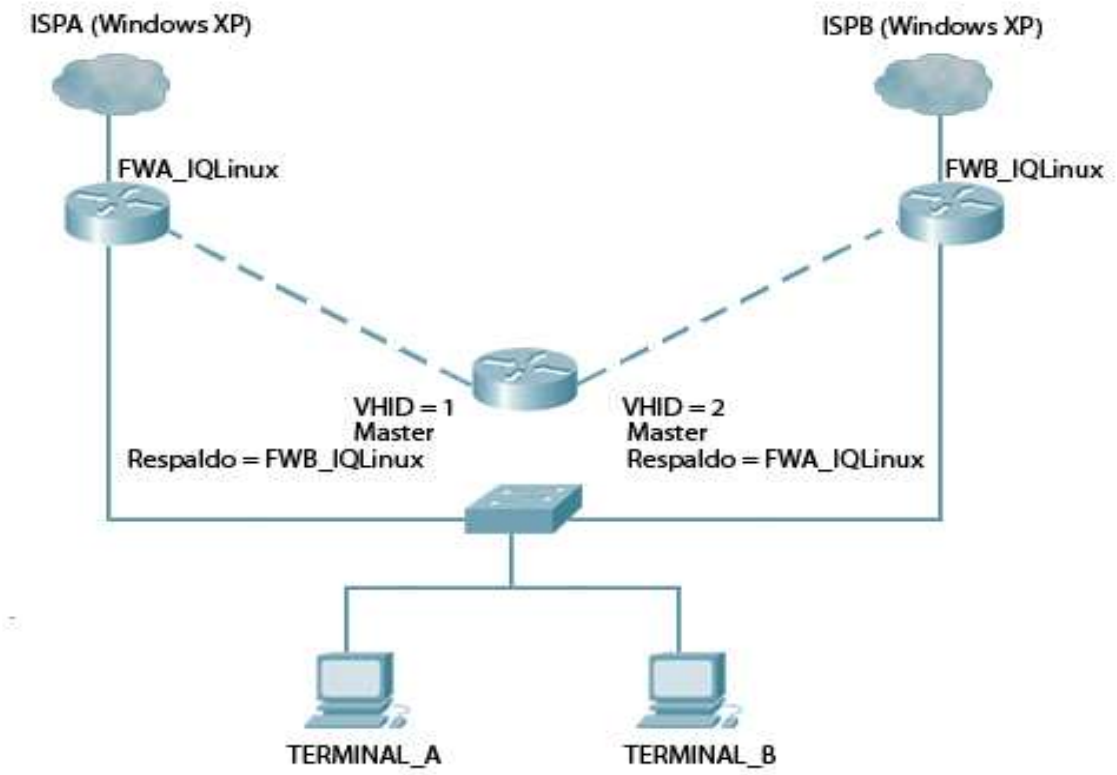
ISPB	192.168.20.1	-	-
FWA_IQLINUX	192.168.10.2	10.10.10.10	192.168.10.1
FWB_IQLINUX	192.168.20.2	10.10.10.11	192.168.20.1
TERMINAL_A		10.10.10.100	10.10.10.1
TERMINAL_B		10.10.10.200	10.10.10.1

c) Configuración CARP

Parámetros utilizados para la configuración del protocolo CARP

Firewall CARP	**Interfaz**	**VHID**	**Dirección Virtual**	**ADVSKEW**	**Estado**
FWA_IQLINUX	carp0	1	10.10.10.1	0	Maestro
FWA_IQLINUX	carp0	2	10.10.10.1	100	Respaldo
FWB_IQLINUX	carp0	1	10.10.10.1	100	Respaldo
FWB_IQLINUX	carp0	2	10.10.10.1	0	Maestro

2.- Esquema de red



3.- Instalación y configuración

Paso 1.- Lo primero que se tendrá que hacer es realizar las llamadas necesarias al kernel para el uso de CARP y el reenvío de paquetes IP.

```
# cat /etc/sysctl.conf | grep -v ^#
net.inet.ip.forwarding=1        # 1=Permit forwarding (routing) of IPv4 packets
net.inet.carp.allow=1           # 1=Enable the carp(4) Protocol
net.inet.carp.preempt=1         # 1=Enable carp(4) preemption
                                # required by some ports
# _
```

Paso 2.- Configuración de las interfaces de red.

FWA_IQLINUX

```
# cat /etc/hostname.em0
inet 192.168.10.2 255.255.255.0 NONE
# cat /etc/hostname.em1
inet 10.10.10.10 255.255.255.0 NONE
# _
```

FWB_IQLINUX

```
# cat /etc/hostname.em0
inet 192.168.20.2 255.255.255.0 NONE
# cat /etc/hostname.em1
inet 10.10.10.11 255.255.255.0 NONE
# _
```

Paso 3.- Configuración de la interfaz virtual CARP.

FWA_IQLINUX

```
# cat /etc/hostname.carp0
inet 10.10.10.1 255.255.255.0 10.10.10.255 balancing ip carpnodes 1:0,2:100 carp
dev em1 pass espoch2010
# _
```

FWB_IQLINUX

```
# cat /etc/hostname.carp0
inet 10.10.10.1 255.255.255.0 10.10.10.255 balancing ip carpnodes 1:100,2:0 carp
dev em1 pass espoch2010
# _
```

Paso 4.- Habilitación del filtrado de paquetes con pf (packetfilter).

```
# cat /etc/rc.conf | grep ^pf
pf=YES                  # Packet filter / NAT
pf_rules=/etc/pf.conf           # Packet filter rules file
pflogd_flags=                   # add more flags, ie. "-s 256"
# _
```

Paso 5.- Reglas de pf para la traducción de direcciones de red.

```
# cat /etc/pf.conf | grep -v ^#

set skip on lo



pass            # to establish keep-state



block in on ! lo0 proto tcp to port 6000:6010
pass out on em0 from em1:network to any nat-to em0
pass out on em0 from carp0:network to any nat-to em0
# _
```

Paso 6.- Creación de un fichero script el cual lee direcciones de internet de un archivo de texto para la comprobación del servicio de internet en la interfaz de salida de cada firewall.

```
# cat /root/inetcheck _
#!/usr/local/bin/bash

PING=/sbin/ping
IFCONFIG=/sbin/ifconfig
INT=carp0
FILE=/root/domains.txt
FLAG=0

oIFS=$IFS IFS=$'\n' lines=($(<"$FILE")) IFS=$oIFS
n=${#lines[@]}

while true; do

   r=$((RANDOM % n))
   $PING -c 3  ${lines[r]} &> /dev/null
   if [ $? -eq 0 ]; then
      if [ $FLAG -eq 1 ]; then
         $IFCONFIG $INT up
         FLAG=0
      fi
   else
      if [ $FLAG -eq 0 ]; then
         $IFCONFIG $INT down
         FLAG=1
       fi
   fi
   sleep 5
done
# _
```

Archivo de direcciones de internet las cuales fueron seleccionadas teniendo en mente la disponibilidad de los sitios. Se utiliza nombres de dominios y no direcciones IP para comprobar el correcto funcionamiento de los servicios DNS

```
# cat /root/domains.txt
www.google.com
www.yahoo.com
www.youtube.com
www.terra.es
# _
```

Paso 7.- Se automatiza la ejecución del script con el arranque del sistema.

```
# cat /etc/rc.local | grep -v ^#

echo -n 'starting local daemons:'

/root/inetcheck &> /dev/null &

echo '.'

# _
```

4.- Pruebas de verificación

a) Ejecución del protocolo

Para comprobar que el protocolo esté funcionando correctamente se revisara la configuración de la interfaz virtual con el comando ifconfig.

```
carp0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        lladdr 01:00:5e:00:01:01
        priority: 0
        carp: carpdev em1 advbase 1 balancing ip
                state MASTER vhid 1 advskew 0
                state BACKUP vhid 2 advskew 100
        groups: carp
        inet6 fe80::a00:27ff:fe0e:f3f4%carp0 prefixlen 64 scopeid 0x5
        inet 10.10.10.1 netmask 0xffffff00 broadcast 10.10.10.255
# _
```

También se comprobará la ejecución del script inetcheck.

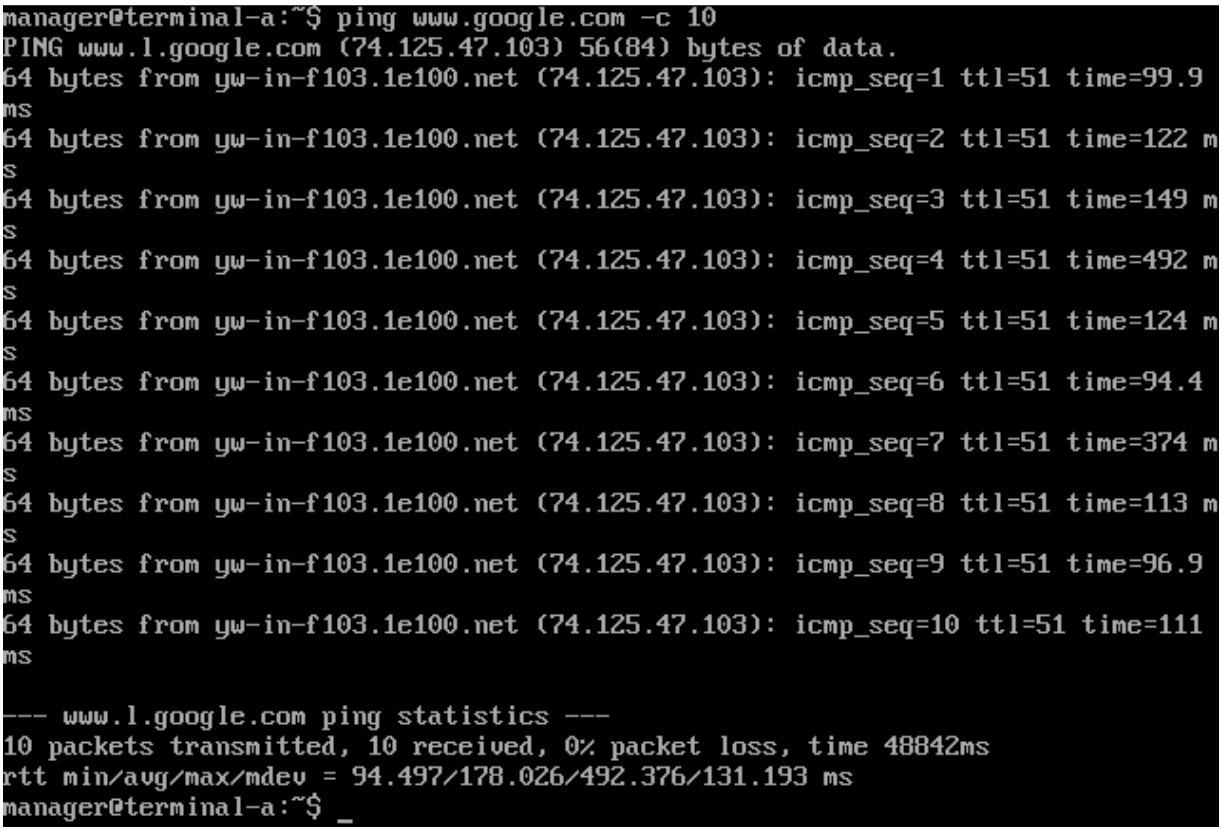
```
# ps waux | grep inetcheck
root     20921  0.0  0.5   692  1260 C0  I     10:04PM    0:00.10 bash inetcheck
# _
```

b) Funcionamiento de protocolo

En esta sección comprobaremos el comportamiento del protocolo ante fallas de uno de sus proveedores de servicio de internet.

I) Ejecución del comando ping

Ejecutando el comando ping podremos confirmar la conectividad hacia internet cuando todo está funcionando normalmente.

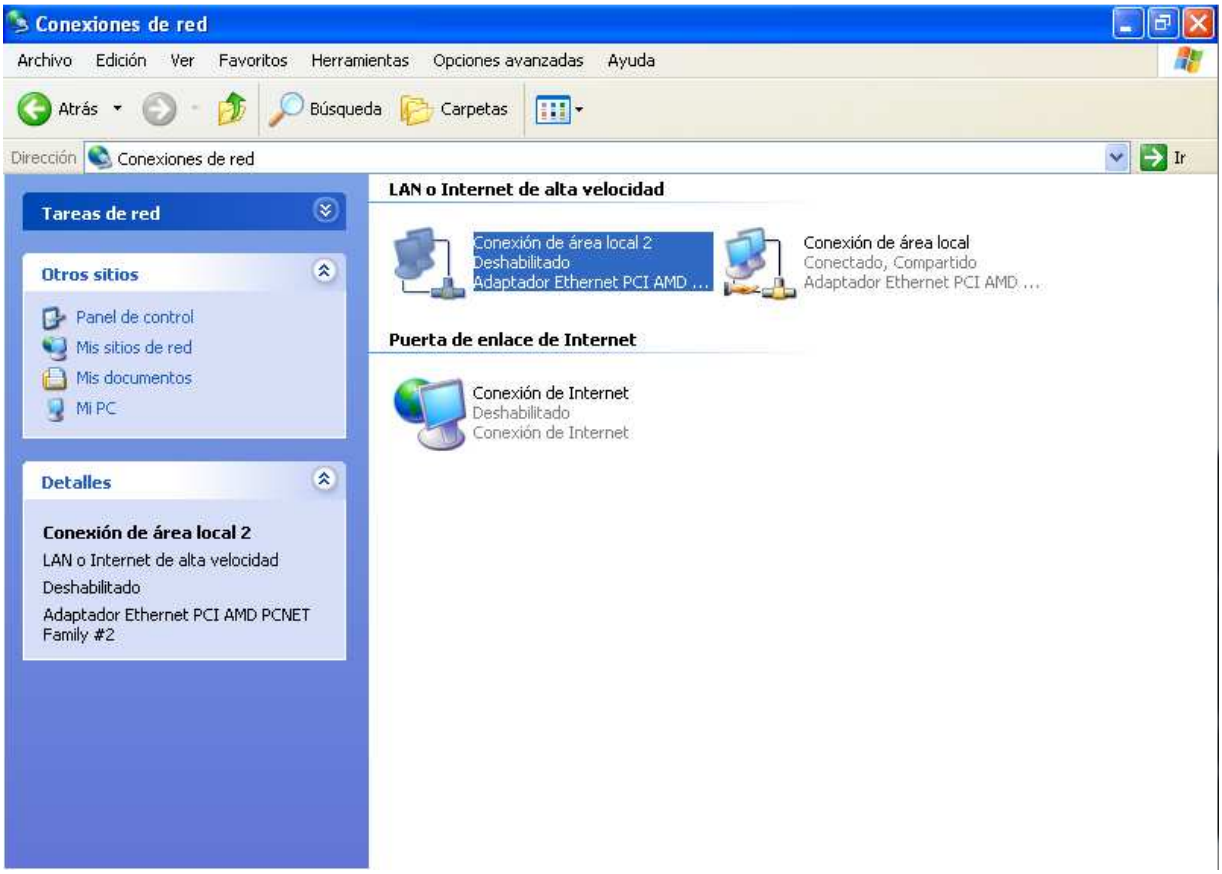


II) Ejecución del comando traceroute para comprobar el camino que están tomando los paquetes que salen desde la red interna al internet. También podremos ver el balanceo de carga que realiza el protocolo CARP sin necesidad de tener varias puertas de salida distintas.

```
manager@terminal-a:~$ traceroute www.google.com -m 5
traceroute to www.google.com (72.14.253.104), 5 hops max, 60 byte packets
 1  10.10.10.10 (10.10.10.10)  0.598 ms  0.489 ms  0.429 ms
 2  192.168.10.1 (192.168.10.1)  3.456 ms  3.398 ms  3.330 ms
 3  192.168.0.1 (192.168.0.1)  1598.995 ms  1598.963 ms  1598.909 ms
 4  * * *
 5  225.177.uio.satnet.net (200.69.177.225)  1598.638 ms  1598.921 ms  1598.954
ms
manager@terminal-a:~$ traceroute www.google.com -m 5
traceroute to www.google.com (72.14.253.104), 5 hops max, 60 byte packets
 1  10.10.10.10 (10.10.10.10)  1.022 ms  0.935 ms  0.803 ms
 2  192.168.10.1 (192.168.10.1)  6.983 ms  6.939 ms  6.884 ms
 3  192.168.0.1 (192.168.0.1)  148.759 ms  148.833 ms  149.315 ms
 4  * * *
 5  225.177.uio.satnet.net (200.69.177.225)  149.262 ms  149.212 ms  149.159 ms
manager@terminal-a:~$ traceroute www.google.com -m 5
traceroute to www.google.com (74.125.47.99), 5 hops max, 60 byte packets
 1  10.10.10.11 (10.10.10.11)  1.309 ms  0.970 ms  0.907 ms
 2  ispb.mshome.net (192.168.20.1)  9.396 ms  9.350 ms  9.277 ms
 3  192.168.0.1 (192.168.0.1)  17.725 ms  17.677 ms  17.624 ms
 4  * * *
 5  225.177.uio.satnet.net (200.69.177.225)  39.981 ms  39.726 ms  39.695 ms
manager@terminal-a:~$
```

III) Ejecución del comando ping y simulación de la caída en la conexión con ISPA

Para simular una caída en la conexión de internet, se deshabilitara la interfaz que está conectada a FWA_IQLINUX en la máquina virtual ISPA.



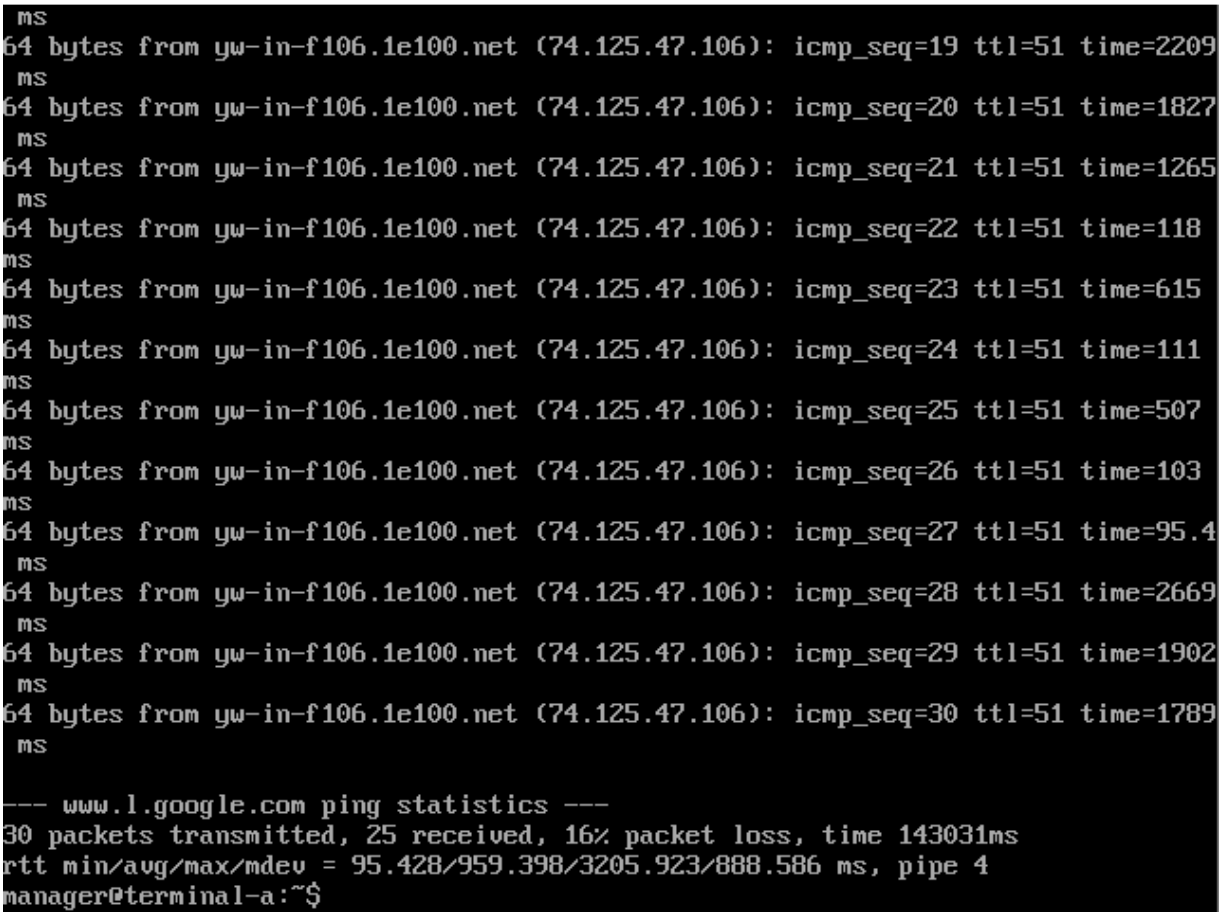
A continuación el script inetcheck al detectar que la conexión se perdió con el proveedor de servicio de internet ISPA , este se encargara de deshabilitar la interfaz virtual que utiliza el protocolo CARP (carp0) obligando al firewall de respaldo a tomar la dirección IP virtual (FWB_IQLINUX).

```
manager@FWA:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ab:dc:b7
          inet addr:192.168.10.2  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feab:dcb7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:512 errors:0 dropped:0 overruns:0 frame:0
          TX packets:778 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:82781 (82.7 KB)  TX bytes:62191 (62.1 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:81 errors:0 dropped:0 overruns:0 frame:0
          TX packets:81 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:8187 (8.1 KB)  TX bytes:8187 (8.1 KB)

manager@FWA:~$
```

Al momento de producirse la caída en la conexión a internet se puede observar que en el tiempo de transición de estados en los firewall CARP existe una pérdida de 5 paquetes que significa una pérdida de conexión de aproximadamente 4.5 segundos.

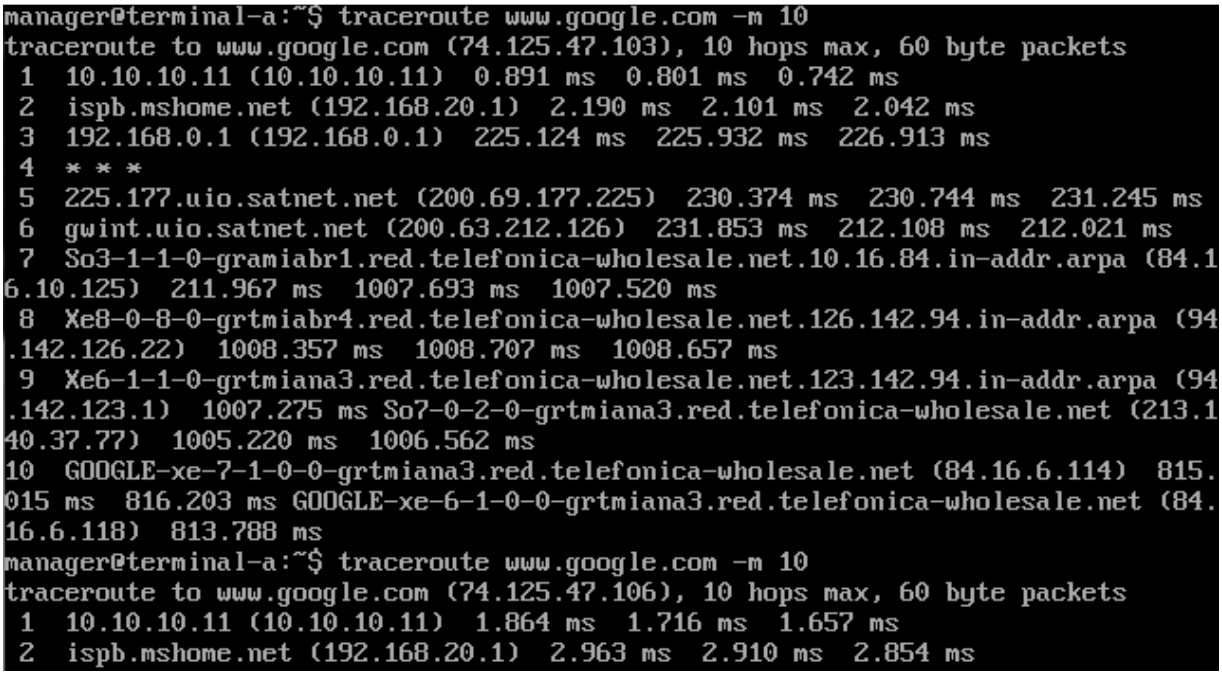
Cabe resaltar que dado que el protocolo CARP realiza un balanceo de carga dinámico entre los dos grupos de redundancia CARP VHID =1 y VHID =2 desde la misma dirección IP virtual compartida, la probabilidad de que un usuario tenga conocimiento de la caída de uno de los proveedores de internet es remota. Solo cuando una conexión ya ha sido establecida por medio de uno de los ISP se podrán apreciar las pérdidas de paquetes mientras se realiza la transición del protocolo.

```
manager@terminal-a:~$ ping www.google.com -c 30
PING www.l.google.com (74.125.47.106) 56(84) bytes of data.
64 bytes from yw-in-f106.1e100.net (74.125.47.106): icmp_seq=1 ttl=51 time=473 m
s
64 bytes from yw-in-f106.1e100.net (74.125.47.106): icmp_seq=2 ttl=51 time=1843
ms
64 bytes from yw-in-f106.1e100.net (74.125.47.106): icmp_seq=3 ttl=51 time=1158
ms
64 bytes from yw-in-f106.1e100.net (74.125.47.106): icmp_seq=9 ttl=51 time=1104
ms
64 bytes from yw-in-f106.1e100.net (74.125.47.106): icmp_seq=10 ttl=51 time=1063
 ms
```



IV) Ejecución del comando traceroute y simulación de la caída en la conexión con ISPA

Para simular una caída en la conexión de internet, se realizara el mismo proceso de la sección anterior. Una vez que FWB_IQLINUX esté en control del Router virtual VHID = 1 este se encontrará como Router maestro en la interfaz virtual carp0 para VHID = 1 and VHID = 2. Todos los terminales navegarán a internet a través de ISPB.



ANEXO 3

Compilación de un kernel a medida y creación de GNU/IQ-Linux 1.0

El kernel es el núcleo de un sistema operativo. Es responsable de la gestión de memoria, la aplicación de controles de seguridad, redes, acceso a disco, y mucho más. Aunque el kernel de los sistemas GNU/Linux se vuelve cada día más dinámicamente configurable es aun ocasionalmente necesario la reconfiguración y recopilación del mismo.

¿Por qué construir un kernel personalizado?

Tradicionalmente el kernel solía ser un gran programa, soportando una lista fija de dispositivos, y si se deseaba cambiar el comportamiento del núcleo, entonces se tenía que compilar un nuevo kernel, y luego reiniciar el ordenador con el nuevo kernel.

Hoy en día, el kernel se está moviendo rápidamente a un modelo donde la mayor parte de la funcionalidad del núcleo se encuentra en módulos que pueden ser cargados y descargados dinámicamente desde el kernel cuando sea necesario. Esto permite que el núcleo se adapte a nuevo hardware tan pronto esté disponible, o para introducir nuevas funcionalidades en el núcleo que no estuvieron necesariamente presentes cuando el kernel fue originalmente compilado. Esto se conoce como un kernel modular.

A pesar de ello, todavía es necesario realizar alguna configuración estática en el kernel. En algunos casos esto se debe a que la funcionalidad está tan ligada al núcleo que no puede ser cargada de forma dinámica. En otros, puede ser simplemente porque nadie ha tomado el tiempo necesario para escribir un módulo que pueda ser cargado en el kernel para brindar la funcionalidad deseada.

Este proceso, mientras que consume tiempo, proporcionará muchos beneficios al sistema operativo. A diferencia de un kernel genérico, que debe ser compatible con una amplia gama de hardware, un kernel personalizado sólo incluye soporte para el hardware del ordenador específico donde se ejecutara. Esto tiene una serie de beneficios, tales como:

- Menor tiempo de arranque. Dado que el núcleo sólo probara el hardware que tiene instalado el ordenador, el tiempo que tarda el sistema para arrancar puede disminuir drásticamente.
- Bajo uso de memoria. Un kernel personalizado a menudo utiliza menos memoria que el kernel genérico por omitir las características no utilizadas y los controladores de estos dispositivos. Esto es importante porque el código del núcleo permanece residente en memoria física en todo momento, evitando que la memoria sea utilizada por las aplicaciones innecesarias. Por esta razón, un kernel personalizado es especialmente útil en un sistema con una pequeña cantidad de memoria RAM.
- Soporte de hardware adicional. Un núcleo a medida le permite añadir el soporte para dispositivos que no están presentes en el kernel genérico, tales como tarjetas de sonido.

Construcción e instalación del kernel personalizado.

Actualmente existen alrededor de 600 distintas distribuciones del sistema operativo GNU/Linux. Muchas de estas distribuciones se encuentran activas, siendo mantenidas por corporaciones o comunidades de usuarios de todas partes del mundo.

Como base para el sistema operativo GNU/IQ-Linux se ha seleccionado la distribución Debian GNU/Linux, siendo una de las más antiguas que esta activamente mantenida por una comunidad de más de mil voluntarios que colaboran a través de internet.

También es la distribución con probablemente el repositorio de aplicaciones más grande en el internet con cerca de 27000 aplicaciones empaquetadas. Igualmente tiene un gran soporte para varias arquitecturas, soportando 12 distintas arquitecturas en su versión estable.

El kernel que estaremos modificando será Debian GNU/kFreeBSD, ya que brinda un mejor soporte para incluir las funcionalidades de PF y CARP.

Prerrequisitos de kernel

Lo primero que se necesita al momento de compilar un núcleo es descargar el código fuente del mismo.

```
root@iqlinux:~# apt-cache search kfreebsd
```

```
kfreebsd-headers-8-686 - header files for kernel of FreeBSD 8
kfreebsd-headers-8.1-1-486 - header files for kernel of FreeBSD 8.1
kfreebsd-headers-8.1-1-686-smp - header files for kernel of FreeBSD 8.1
kfreebsd-headers-8.1-1-686 - header files for kernel of FreeBSD 8.1
kfreebsd-headers-8.1-1 - Common architecture-specific header files for kernel of
 FreeBSD 8.1
kfreebsd-image-8-486 - kernel of FreeBSD 8 image
kfreebsd-image-8-686-smp - kernel of FreeBSD 8 image
kfreebsd-image-8-686 - kernel of FreeBSD 8 image
kfreebsd-image-8.1-1-486 - kernel of FreeBSD 8.1 image
kfreebsd-image-8.1-1-686-smp - kernel of FreeBSD 8.1 image
kfreebsd-image-8.1-1-686 - kernel of FreeBSD 8.1 image
kfreebsd-source-8.1 - source code for kernel of FreeBSD 8.1 with Debian patches
kfreebsd-kernel-headers - kernel of FreeBSD headers for development
ftpd - File Transfer Protocol (FTP) server
lsb-core - Linux Standard Base 3.2 core support package
lsb-cxx - Linux Standard Base 3.2 C++ support package
lsb-desktop - Linux Standard Base 3.2 Desktop support package
lsb-graphics - Linux Standard Base 3.2 graphics support package
lsb-languages - Linux Standard Base 3.2 Runtime Languages package
lsb-multimedia - Linux Standard Base 3.2 Multimedia package
lsb-printing - Linux Standard Base 3.2 Printing package
lsb-qt4 - Linux Standard Base 3.2 Qt4 support package
type-handling - dpkg architecture generation script
```

Se localiza el paquete para la instalación que en el ejemplo será kfreebsd-source-8.1. La aplicación procederá a descargar el paquete desde un repositorio de la comunidad Debian o nos informara que el paquete ya se encuentra en el sistema.

```
root@iqlinux:~# apt-get install kfreebsd-source-8.1
Reading package lists... Done
Building dependency tree
Reading state information... Done
kfreebsd-source-8.1 is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@iqlinux:~#
```

Una vez descargado el código fuente, se necesitara acceder al mismo que se encuentra bajo la carpeta /usr/src en donde se llevara a cabo toda la configuración del nuevo kernel.

```
root@iqlinux:~# cd /usr/src/kfreebsd-source-8.1/sys/
root@iqlinux:/usr/src/kfreebsd-source-8.1/sys#
```

Personalización del kernel

Para empezar la personalización del kernel hay que dirigirse al directorio arch/conf, siendo arch la arquitectura para la cual se compilara el nuevo núcleo (Ej. I386), donde se copiara el archivo de configuración GENERIC por el nombre con el que se desea llamar al nuevo kernel.

```
root@iqlinux:/usr/src/kfreebsd-source-8.1/sys# cd i386/conf/
root@iqlinux:/usr/src/kfreebsd-source-8.1/sys/i386/conf# cp GENERIC IQLINUX
root@iqlinux:/usr/src/kfreebsd-source-8.1/sys/i386/conf#
```

Utilizando el editor de preferencia se procederá a modificar el archivo de configuración IQLINUX.

```
root@iqlinux:/usr/src/kfreebsd-source-8.1/sys/i386/conf# vi IQLINUX
```

Integración de PF en el kernel IQ-Linux

La elección de pf en lugar de Netfilter (iptables) se da por las siguientes razones:

- La sintaxis de pf es mucho más fácil de leer e interpretar por un usuario, se trata de sentencias escritas como oraciones en inglés.
- Iptables utiliza varias cadenas de reglas operando sobre el mismo paquete, lo que ocasiona confusión al momento de ubicarlas y en el orden en el que deberían ir.
- pf proporciona la capacidad de permitir únicamente conexiones que han sido autenticadas haciendo uso de authpf.
- Ya que pf fue desarrollado por OpenBSD, el cual está enfocado sobre todo en la seguridad, se puede esperar que pf sea mucho más seguro que iptables.

Para integrar el soporte de pf en el nuevo kernel, se agregaran las siguientes líneas en el archivo de configuración.

```
device          pf
device          pflog
device          pfsync
```

Integración de CARP en el kernel IQ-Linux

Aunque uCARP es una muy buena solución para la integración del protocolo CARP en GNU/Linux, no proporciona todas las características que el protocolo original creado por OpenBSD lo hace. Muchas de estas características son muy importantes y solo pueden ser utilizadas desde el espacio del núcleo. uCARP se ejecuta desde el ambiente de usuario lo que hace imposible hacer uso de ciertas funciones como:

- Balanceo de carga por ARP
- Balanceo de carga por IP
- Habilitar/deshabilitar el modo de adelantamiento cuando sea necesario
- La creación de una interfaz virtual carp#

Para integrar el soporte de CARP como parte del kernel, se agregara la siguiente línea en el archivo de configuración.

```
device          carp
```

Compilación del kernel

Una vez realizado todos los cambios necesarios en el código fuente del núcleo, se procederá a compilarlo, para esto se instalan las herramientas adecuadas para la compilación y se ejecutan los siguientes comandos:

```
root@iqlinux:/usr/src/kfreebsd-source-8.1/sys/i386/conf# cd ../../../
root@iqlinux:/usr/src/kfreebsd-source-8.1# apt-get build-dep kfreebsd-8
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  autopoint binutils build-essential bzip2 cpp cpp-4.3 cpp-4.4 debhelper
  diffstat dpkg-dev fakeroot flex-old g++ g++-4.4 gcc gcc-4.3 gcc-4.3-base
  gcc-4.4 gettext git html2text intltool-debian libalgorithm-diff-perl
  libalgorithm-diff-xs-perl libalgorithm-merge-perl libbsd-dev libc-dev-bin
  libc0.1-dev libcroco3 libcurl3-gnutls libdb-dev libdb4.8-dev
  libdigest-sha1-perl libdpkg-perl liberror-perl libglib2.0-0 libglib2.0-data
  libgmp3c2 libgomp1 libmail-sendmail-perl libmpfr4 libsbuf-dev
  libstdc++6-4.4-dev libsys-hostname-long-perl libtimedate-perl libunistring0
  manpages-dev po-debconf quilt rsync shared-mime-info sharutils
0 upgraded, 52 newly installed, 0 to remove and 0 not upgraded.
Need to get 37.5 MB of archives.
After this operation, 102 MB of additional disk space will be used.
Do you want to continue [Y/n]?
```

```
Setting up libalgorithm-merge-perl (0.08-2) ...
Setting up libbsd-dev (0.2.0-1) ...
Setting up libglib2.0-data (2.24.2-1) ...
Setting up libsys-hostname-long-perl (1.4-2) ...
Setting up libmail-sendmail-perl (0.79.16-1) ...
Setting up libsbuf-dev (8.1-5) ...
Setting up manpages-dev (3.25-1) ...
Setting up quilt (0.48-7) ...
Setting up rsync (3.0.7-2) ...
update-rc.d: using dependency based boot sequencing
Setting up shared-mime-info (0.71-3) ...
Setting up sharutils (1:4.9-1) ...
Setting up flex-old (2.5.4a-8) ...
Ignoring install-info called from maintainer script
The package flex-old should be rebuilt with new debhelper to get trigger support

Setting up libdb4.8-dev (4.8.30-2) ...
Setting up libdb-dev (4.8) ...
Setting up libstdc++6-4.4-dev (4.4.5-4) ...
Setting up g++-4.4 (4.4.5-4) ...
Setting up g++ (4:4.4.5-1) ...
update-alternatives: using /usr/bin/g++ to provide /usr/bin/c++ (c++) in auto mo
de.
Setting up build-essential (11.5) ...
root@iqlinux:/usr/src/kfreebsd-source-8.1#
```

Un inconveniente que se tiene con la última versión del kernel 8.1 es que el código fuente no viene en un formato compatible con Debian, por lo que se instalara el código fuente del kernel en la versión 8 para crear la estructura de directorios necesitada.

```
root@iqlinux:/usr/src/kfreebsd-source-8.1# apt-get source kfreebsd-8
Reading package lists... Done
Building dependency tree
Reading state information... Done
NOTICE: 'kfreebsd-8' packaging is maintained in the 'Svn' version control system
 at:
svn://svn.debian.org/glibc-bsd/trunk/kfreebsd-8/
Need to get 31.2 MB of source archives.
Get:1 http://ftp.us.debian.org/debian/ squeeze/main kfreebsd-8 8.1-5 (dsc) [1,86
3 B]
Get:2 http://ftp.us.debian.org/debian/ squeeze/main kfreebsd-8 8.1-5 (tar) [31.2
 MB]
17% [2 kfreebsd-8 5,617 kB/31.2 MB 18%]                    43.4 kB/s 9min 50s
```

```
root@iqlinux:/usr/src/kfreebsd-source-8.1# dpkg-buildpackage
```

```
patching file sys/modules/iwifw/iwi_monitor/Makefile
patching file sys/modules/wpifw/Makefile
patching file sys/modules/iwnfw/Makefile.inc
patching file sys/modules/runfw/Makefile

Applying patch 914_psm.diff
patching file sys/dev/atkbdc/psm.c

Applying patch 915_ip6.v6only.diff
patching file sys/netinet6/in6_proto.c

Applying patch 950_no_stack_protector.diff
patching file sys/conf/kern.mk
Hunk #1 succeeded at 123 (offset 12 lines).
patching file sys/conf/kmod.mk

Applying patch 999_config.diff
patching file sys/amd64/conf/GENERIC
patching file sys/i386/conf/GENERIC

Now at patch 999_config.diff
mkdir /root/kfreebsd-8-8.1/src
cp -af /root/kfreebsd-8-8.1/sys /root/kfreebsd-8-8.1/usr.sbin /root/kfreebsd-8-8
.1/src
```

```
dpkg-deb: building package `kfreebsd-headers-8.1-1-486' in `../kfreebsd-headers-
8.1-1-486_8.1-5_kfreebsd-i386.deb'.
dpkg-deb: building package `kfreebsd-headers-8-486' in `../kfreebsd-headers-8-48
6_8.1-5_kfreebsd-i386.deb'.
dpkg-deb: building package `kfreebsd-image-8.1-1-686' in `../kfreebsd-image-8.1-
1-686_8.1-5_kfreebsd-i386.deb'.
dpkg-deb: building package `kfreebsd-image-8-686' in `../kfreebsd-image-8-686_8.
1-5_kfreebsd-i386.deb'.
dpkg-deb: building package `kfreebsd-headers-8.1-1-686' in `../kfreebsd-headers-
8.1-1-686_8.1-5_kfreebsd-i386.deb'.
dpkg-deb: building package `kfreebsd-headers-8-686' in `../kfreebsd-headers-8-68
6_8.1-5_kfreebsd-i386.deb'.
dpkg-deb: building package `kfreebsd-image-8.1-1-686-smp' in `../kfreebsd-image-
8.1-1-686-smp_8.1-5_kfreebsd-i386.deb'.
dpkg-deb: building package `kfreebsd-image-8-686-smp' in `../kfreebsd-image-8-68
6-smp_8.1-5_kfreebsd-i386.deb'.
dpkg-deb: building package `kfreebsd-headers-8.1-1-686-smp' in `../kfreebsd-head
ers-8.1-1-686-smp_8.1-5_kfreebsd-i386.deb'.
dpkg-deb: building package `kfreebsd-headers-8-686-smp' in `../kfreebsd-headers-
8-686-smp_8.1-5_kfreebsd-i386.deb'.
 dpkg-genchanges  >../kfreebsd-8_8.1-5_kfreebsd-i386.changes
dpkg-genchanges: including full source code in upload
 dpkg-source --after-build kfreebsd-8-8.1
dpkg-buildpackage: full upload; Debian-native package (full source is included)
root@iqlinux:/usr/src/kfreebsd-source-8.1#
```

Una vez terminada la compilación se procede a la instalación del nuevo kernel.

```
root@iqlinux:/usr/src/kfreebsd-source-8.1# cd ..
root@iqlinux:/usr/src#
```

```
root@iqlinux:/usr/src# ls
kfreebsd-8-8.1
kfreebsd-8_8.1-5.dsc
kfreebsd-8_8.1-5_kfreebsd-i386.changes
kfreebsd-8_8.1-5.tar.gz
kfreebsd-headers-8.1-1-486_8.1-5_kfreebsd-i386.deb
kfreebsd-headers-8.1-1-686_8.1-5_kfreebsd-i386.deb
kfreebsd-headers-8.1-1-686-smp_8.1-5_kfreebsd-i386.deb
kfreebsd-headers-8.1-1_8.1-5_kfreebsd-i386.deb
kfreebsd-headers-8-486_8.1-5_kfreebsd-i386.deb
kfreebsd-headers-8-686_8.1-5_kfreebsd-i386.deb
kfreebsd-headers-8-686-smp_8.1-5_kfreebsd-i386.deb
kfreebsd-image-8.1-1-486_8.1-5_kfreebsd-i386.deb
kfreebsd-image-8.1-1-686_8.1-5_kfreebsd-i386.deb
kfreebsd-image-8.1-1-686-smp_8.1-5_kfreebsd-i386.deb
kfreebsd-image-8-486_8.1-5_kfreebsd-i386.deb
kfreebsd-image-8-686_8.1-5_kfreebsd-i386.deb
kfreebsd-image-8-686-smp_8.1-5_kfreebsd-i386.deb
kfreebsd-source-8.1
kfreebsd-source-8.1_8.1-5_all.deb
kfreebsd-source-8.1.tar
root@iqlinux:/usr/src#
```

```
root@iqlinux:/usr/src# ls
kfreebsd-8-8.1
kfreebsd-8_8.1-5.dsc
kfreebsd-8_8.1-5_kfreebsd-i386.changes
kfreebsd-8_8.1-5.tar.gz
kfreebsd-headers-8.1-1-486_8.1-5_kfreebsd-i386.deb
kfreebsd-headers-8.1-1-686_8.1-5_kfreebsd-i386.deb
kfreebsd-headers-8.1-1-686-smp_8.1-5_kfreebsd-i386.deb
kfreebsd-headers-8.1-1_8.1-5_kfreebsd-i386.deb
kfreebsd-headers-8-486_8.1-5_kfreebsd-i386.deb
kfreebsd-headers-8-686_8.1-5_kfreebsd-i386.deb
kfreebsd-headers-8-686-smp_8.1-5_kfreebsd-i386.deb
kfreebsd-image-8.1-1-486_8.1-5_kfreebsd-i386.deb
kfreebsd-image-8.1-1-686_8.1-5_kfreebsd-i386.deb
kfreebsd-image-8.1-1-686-smp_8.1-5_kfreebsd-i386.deb
kfreebsd-image-8-486_8.1-5_kfreebsd-i386.deb
kfreebsd-image-8-686_8.1-5_kfreebsd-i386.deb
kfreebsd-image-8-686-smp_8.1-5_kfreebsd-i386.deb
kfreebsd-source-8.1
kfreebsd-source-8.1_8.1-5_all.deb
kfreebsd-source-8.1.tar
root@iqlinux:/usr/src# dpkg -i kfreebsd-image-8.1-1-686_8.1-5_kfreebsd-i386.deb
```

```
IQLinux/i386 (fwa.infoquality.com.ec) (ttyC0)

login: _
```

ANEXO 4

DISTRIBUCION JI - CUADRADO (χ^2)

Grados de Libertad	Probabilidad acumulada									
	0.300	0.350	0.400	0.450	0.500	0.550	0.600	0.650	0.700	0.750
1	0.148	0.206	0.275	0.357	0.455	0.571	0.708	0.873	1.074	1.323
2	0.713	0.862	1.022	1.196	1.386	1.597	1.833	2.100	2.408	2.773
3	1.424	1.642	1.869	2.109	2.366	2.643	2.946	3.283	3.665	4.108
4	2.195	2.470	2.753	3.047	3.357	3.687	4.045	4.438	4.878	5.385
5	3.000	3.325	3.655	3.996	4.351	4.728	5.132	5.573	6.064	6.626
6	3.828	4.197	4.570	4.952	5.348	5.765	6.211	6.695	7.231	7.841
7	4.671	5.082	5.493	5.913	6.346	6.800	7.283	7.806	8.383	9.037
8	5.527	5.975	6.423	6.877	7.344	7.833	8.351	8.909	9.524	10.22
9	6.393	6.876	7.357	7.843	8.343	8.863	9.414	10.01	10.66	11.39
10	7.267	7.783	8.295	8.812	9.342	9.892	10.47	11.10	11.78	12.55
11	8.148	8.695	9.237	9.783	10.34	10.92	11.53	12.18	12.90	13.70
12	9.034	9.612	10.18	10.76	11.34	11.95	12.58	13.27	14.01	14.85
13	9.926	10.53	11.13	11.73	12.34	12.97	13.64	14.35	15.12	15.98
14	10.82	11.45	12.08	12.70	13.34	14.00	14.69	15.42	16.22	17.12
15	11.72	12.38	13.03	13.68	14.34	15.02	15.73	16.49	17.32	18.25
16	12.62	13.31	13.98	14.66	15.34	16.04	16.78	17.56	18.42	19.37
17	13.53	14.24	14.94	15.63	16.34	17.06	17.82	18.63	19.51	20.49
18	14.44	15.17	15.89	16.61	17.34	18.09	18.87	19.70	20.60	21.60
19	15.35	16.11	16.85	17.59	18.34	19.11	19.91	20.76	21.69	22.72
20	16.27	17.05	17.81	18.57	19.34	20.13	20.95	21.83	22.77	23.83
21	17.18	17.98	18.77	19.55	20.34	21.15	21.99	22.89	23.86	24.93
22	18.10	18.92	19.73	20.53	21.34	22.17	23.03	23.95	24.94	26.04
23	19.02	19.87	20.69	21.51	22.34	23.19	24.07	25.01	26.02	27.14
24	19.94	20.81	21.65	22.49	23.34	24.20	25.11	26.06	27.10	28.24
25	20.87	21.75	22.62	23.47	24.34	25.22	26.14	27.12	28.17	29.34
26	21.79	22.70	23.58	24.45	25.34	26.24	27.18	28.17	29.25	30.43
27	22.72	23.64	24.54	25.44	26.34	27.26	28.21	29.23	30.32	31.53
28	23.65	24.59	25.51	26.42	27.34	28.27	29.25	30.28	31.39	32.62
29	24.58	25.54	26.48	27.40	28.34	29.29	30.28	31.33	32.46	33.71
30	25.51	26.49	27.44	28.39	29.34	30.31	31.32	32.38	33.53	34.80
35	30.18	31.25	32.28	33.31	34.34	35.39	36.47	37.62	38.86	40.22
40	34.87	36.02	37.13	38.23	39.34	40.46	41.62	42.85	44.16	45.62
45	39.58	40.81	42.00	43.16	44.34	45.53	46.76	48.06	49.45	50.98
50	44.31	45.61	46.86	48.10	49.33	50.59	51.89	53.26	54.72	56.33
55	49.06	50.42	51.74	53.04	54.33	55.65	57.02	58.45	59.98	61.66
60	53.81	55.24	56.62	57.98	59.33	60.71	62.13	63.63	65.23	66.98
65	58.57	60.07	61.51	62.92	64.33	65.77	67.25	68.80	70.46	72.28
70	63.35	64.90	66.40	67.87	69.33	70.82	72.36	73.97	75.69	77.58
75	68.13	69.74	71.29	72.81	74.33	75.88	77.46	79.13	80.91	82.86
80	72.92	74.58	76.19	77.76	79.33	80.93	82.57	84.28	86.12	88.13
85	77.71	79.43	81.09	82.71	84.33	85.98	87.67	89.43	91.32	93.39
90	82.51	84.29	85.99	87.67	89.33	91.02	92.76	94.58	96.52	98.65
95	87.32	89.14	90.90	92.62	94.33	96.07	97.85	99.72	101.7	103.9
100	92.13	94.00	95.81	97.57	99.33	101.1	102.9	104.9	106.9	109.1
110	101.8	103.7	105.6	107.5	109.3	111.2	113.1	115.1	117.3	119.6
120	111.4	113.5	115.5	117.4	119.3	121.3	123.3	125.4	127.6	130.1
200	189.0	191.7	194.3	196.8	199.3	201.9	204.4	207.1	210.0	213.1

ANEXO 5

ANEXO 6

ANEXO 7