ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN SISTEMAS

TEMA:

ANÁLISIS DE LOS PROTOCOLOS DE ALTA DISPONIBILIDAD DE GATEWAYS EN LA INTERCONECTIVIDAD LAN/WAN APLICADAS AL DISEÑO DE REDES DE CAMPUS

TESIS DE GRADO PREVIA LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS

PRESENTADO POR:

NATALI DEL ROCÍO YEROVI LLUAY
JENNY VALERIA FLORES ORTIZ

RIOBAMBA – ECUADOR
2010

PORTADA

AGRADECIMIENTO

DEDICATORIA

ÍNDICEGENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

CAPITULO I

MARCO REFERENCIAL

1.1 ANTECEDENTES

Las empresas necesitan interconectar los procesos, personas e información tanto con la propia organización como atravesando sus fronteras con agencias externas y socios comerciales. La falta de una red estable, hace que se pierdan datos importantes y tiempo en el momento de estar trabajando a través de ella y de estar intercambiando información.

Las compañías cada vez más buscan un tiempo de actividad de 24 horas al día y siete días por semana para sus redes informáticas. Lograr el 100% de tiempo de actividad tal vez es imposible, pero asegurar un tiempo de actividad de 99,999% o de cinco nueves es un objetivo que las organizaciones se plantean. Esto se interpreta como un día de tiempo de inactividad, en promedio, por cada 30 años, o una hora de tiempo de Redes de Área Local inactiva, en promedio, por cada 4000 días, o 5,25 minutos de tiempo de inactividad por año.

En un sistema informático actual, existen muchos componentes necesarios para que este funcione, cuanto más componentes, más probabilidad tenemos de que algo falle. Estos problemas pueden ocurrir en el propio servidor, fallos de discos, fuentes de alimentación, tarjetas de red, etc y en la infraestructura necesaria para que el servidor se pueda utilizar, componentes de red, acceso a internet y sistema eléctrico.

A los administradores de red les preocupa tener puntos de fallo únicos en la red. Es decir desean proporcionar tanto rutas de acceso redundantes como equipo redundante en lugares clave de la red para evitar que cualquier dispositivo cause que los recursos vitales de la red dejen de poder utilizarse.

Cuando se tienen sistemas críticos que tienen que estar disponibles y funcionando 24 horas al día, 365 días al año, hay que intentar minimizar los fallos que puedan afectar al funcionamiento normal del sistema. Fallos van a ocurrir, pero existen técnicas y configuraciones que ayudan a tener sistemas redundantes, en los que ciertas partes pueden fallar sin que esto afecte al funcionamiento del mismo y los ingresos económicos de las empresas.

El grado de redundancia de un sistema, dependerá de su importancia y del dinero que perdamos cuando el sistema no esté disponible por un fallo. No nos merecerá la pena

invertir en ‘redundancia’, si la inversión necesaria para tener un sistema redundante cuesta más de lo que perderíamos en dinero, reputación y horas de trabajo, si el sistema fallara.

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 está disponible al intercambio de mensajes de hello entre los diferentes dispositivos que adheridos al mismo gateway virtual.

Para administrar la redundancia existen protocolos propietarios cisco como el HSRP, GLBP, y protocolos estándares como VRRP y CARP, los mimos que permitan una alta disponibilidad en las redes LAN/WAN.

Análisis

El trabajo de investigación se centrará en el análisis de los protocolos de alta disponibilidad de gateways en la interconectividad Lan/Wan aplicadas al diseño de redes de campus a través de un estudio mediante equipos CISCO y GNU- LINUX con sus respectivos protocolos, se establecerá además las ventajas respectivas que ofrecerán estos protocolos y como van a ser usados.

Lugar de Aplicación

La investigación se la aplicará en la Academia Local Cisco en la ESPOCH, debido a que este posee equipos óptimos para el estudio de cada uno de los protocolos, es decir para configurarlos y determinar cuál es el mejor a través de su aplicación mediante un prototipo y así concluir cual es el que se debe utilizar con un alto porcentaje de confiabilidad tanto para equipos CISCO como para software libre (GNU-LINUX).

Alcance

El tema propuesto contendrá el análisis de los protocolos de alta disponibilidad de gateways en la interconectividad Lan/Wan aplicadas al diseño de redes de campus.

1.2 INTRODUCCIÓN

La implementación de gateways redundantes supone un desafío y el uso de un mecanismo como es el uso de protocolos dinámicos de administración del Gateway ya que permiten administrar dinámicamente el gateway de la red o subred, de modo transparente para la terminal.

Lograr un objetivo semejante requiere redes extremadamente confiables. La confiabilidad en las redes se logra por medio de un equipamiento confiable y diseñando redes tolerantes a errores y fallos. La red está diseñada para reconverger rápidamente, por lo cual el fallo se pasa por alto.

Los protocolos de alta disponibilidad aseguran un cierto grado absoluto de continuidad operacional durante un período de medición dado, es decir la habilidad de la comunidad de usuarios para acceder al sistema, someter nuevos trabajos, actualizar o alterar trabajos existentes o recoger los resultados de trabajos previos. Si un usuario no puede acceder al sistema se dice que está no disponible.

Usaremos una red de área de campus ya que es una red de computadoras que conecta redes de área local a través de un área geográfica limitada, como un campus universitario, o una base militar. Puede ser considerado como una red de área metropolitana que se aplica específicamente a un ambiente universitario como lo es la escuela superior politécnica de Chimborazo. Por lo tanto, una red de área de campus es más grande que una red de área local pero más pequeña que una red de área amplia.

Los edificios de una universidad están conectados usando el mismo tipo de equipo y tecnologías de redes que se usarían en un LAN. Además, todos los componentes, incluyendo conmutadores, enrutadores, cableado, y otros, le pertenecen a la misma organización.

1.3 JUSTIFICACIÓN

1.3.1 Justificación Teórica

La redundancia en una red es extremadamente importante porque permite a las redes ser tolerantes a los fallos. Las topologías redundantes protegen contra el tiempo de inactividad de la red debido al fallo de un único enlace, puerto o dispositivo de networking. A menudo se requiere a los ingenieros de redes que tomen decisiones difíciles, equilibrando el costo de la redundancia con la necesidad de la disponibilidad en la red.

La redundancia en una red se requiere para protegerla contra la pérdida de conectividad debido a un fallo de un componente individual. Proporcionar esta redundancia, no obstante, resulta a menudo en topologías físicas con bucles. Los bucles de la capa física pueden ocasionar serios problemas en redes conmutadas.

Nuestras redes requieren un nivel de disponibilidad cada vez más elevado, y en lo posible descartar completamente la posibilidad de interrupciones de servicios. Es por esto que la redundancia en el Gateway es una herramienta vital.

Las redes con rutas y dispositivos redundantes permiten un mayor tiempo de actividad de la red. Las topologías redundantes eliminan los únicos puntos de fallo. Si una ruta o dispositivo falla, la ruta o dispositivo redundantes pueden asumir las tareas de la ruta o dispositivo fallidos.

La ventaja al diseñar redes de campus es que ellas son una alternativa para poder unir edificios distantes y en donde no es posible cablear con cobre o fibra óptica. En todo caso una buena red WLAN o de Campus no viene a sustituir el cableado, pero si a disminuir y a complementarlo. Son redes troncales de alta velocidad (Gigabit Ethernet,...), integrando diferentes entornos (SNA...) y servicios (voz, datos, video) en una única infraestructura IP, en ámbitos metropolitanos.

Al realizar un análisis de los protocolos de alta disponibilidad de gateways en la interconectividad Lan/Wan aplicadas al diseño de redes de campus deseamos conseguir que todos los programas, datos y equipo estén disponibles para cualquiera de la red que así lo solicite, proporcionar una alta fiabilidad, ahorro económico, aumentar el rendimiento y proporcionar un poderoso medio de comunicación entre personas que se encuentran muy alejadas.

1.3.2 Justificación Práctica Aplicativa

Se configurará cada uno de los protocolos de alta disponibilidad como son GLBP, HSRP Y VRRP en redes de campus en los equipos pertenecientes a la Academia Local Cisco, a fin de verificar físicamente como funcionan cada uno de ellos y así determinar cuál es libre(GNU-LINUX).

Para realizar la comparación de los protocolos de alta disponibilidad GLBP, HSRP Y VRRP; se crearán ambientes de prueba para determinar cuál es el que aporta mayores ventajas en el diseño de redes de campus.

1.4 OBJETIVOS

1.4.1 Objetivo General

- ✓ Analizar los protocolos que permiten una alta disponibilidad de gateways en las redes de campus, aplicado en un prototipo en la Academia Local Cisco.

1.4.2 Objetivos Específicos

- ✓ Utilizar métricas de comparación con la finalidad de establecer las ventajas y desventajas en el uso de cada uno de los protocolos de alta disponibilidad de gateway.

- ✓ Identificar a través del análisis comparativo cual es el protocolo que posee mayores beneficios para su utilización en las redes de campus dependiendo del entorno de trabajo ya sea CISCO o LINUX.

- ✓ Implementar un prototipo de red de campus utilizando los protocolos de alta disponibilidad de Gateway tanto para CISCO como para LINUX.

- ✓ Realizar pruebas de disponibilidad de los servicios a través de la configuración de cada uno de los protocolos para un escenario específico.

1.5 HIPÓTESIS

"Con el análisis comparativo de los protocolos de alta disponibilidad de gateways en el diseño de redes de campus, el tiempo de standby de los servicios y el porcentaje de pérdida de datos disminuirán"

CAPITULO II

PROTOCOLOS DE ALTA DISPONIBILIDAD Y REDES DE CAMPUS

2.1 PROTOCOLOS DE ALTA DISPONIBILIDAD

2.1.1 Introducción.

Es indispensable el uso de los protocolos de alta disponibilidad ya que típicamente existe un tiempo de inactividad que es perjudicial para la operación del sistema y usualmente no puede ser evitado con la configuración de los sistemas

actuales. Eventos que generan tiempos de inactividad quizás incluyen parches al software del sistema que requieran un rearranque o cambios en la configuración del sistema que toman efecto después de un rearranque. En general el tiempo de inactividad planificado es usualmente el resultado de un evento lógico o de gestión iniciado.

Muchos cybers excluyen tiempo de inactividad planificado de los cálculos de disponibilidad, asumiendo, correcta o incorrectamente, que el tiempo de actividad no planificado tiene poco o ningún impacto sobre la comunidad de usuarios.

Los protocolos de alta disponibilidad permiten que si un router “cae”, otro router tome el control, basándose en el uso de lo que se llama un “Router Virtual“. Este router virtual lo simulan el conjunto de routers reales que tengamos en la instalación y que se disponga de un protocolo y será también la IP de este router virtual la que tengan configurados los equipos de la red como gateway de salida hacia Internet.

Disponibilidad es usualmente expresada como un porcentaje del tiempo de funcionamiento en un año dado. En un año dado, el número de minutos de tiempo de inactividad no planeado es registrado para un sistema, el tiempo de inactividad no planificado agregado es dividido por el número total de minutos en un año (aproximadamente 525.600) produciendo un porcentaje de tiempo de inactividad; el complemento es el porcentaje de tiempo de funcionamiento el cual es lo que denominamos como disponibilidad del sistema. Valores comunes de disponibilidad, típicamente enunciado como número de "nueves" para sistemas altamente disponibles son:

- ✓ 99,9% = 43.8 minutos/mes u 8,76 horas/año ("tres nueves")
- ✓ 99,99% = 4.38 minutos/mes o 52.6 minutos/año ("cuatro nueves")
- ✓ 99,999% = 0.44 minutos/mes o 5.26 minutos/año ("cinco nueves")

Los protocolos disponibles permiten un tiempo de inactividad de solo 3 segundos que prácticamente el usuario ni siente la inactividad, lo que proporciona mayor confianza y veracidad en el servicio.

2.1.2 Características VRRP, HSRP, GLBP

2.1.2.1 VRRP (Virtual Router Redudancy Protocol)

- ✓ Se encarga de asignar dinámicamente la función de router virtual a uno de los routers dentro de una LAN.
- ✓ Mayor disponibilidad del router por defecto sin necesidad de configurar encaminamiento dinámico o protocolos de descubrimiento de routers en cada equipo final.
- ✓ Incrementa la disponibilidad de la puerta de enlace predeterminada en los hosts dentro de una misma subred.
- ✓ Es un protocolo abierto por lo que es compatible con los routers de gran envergadura como CISCO, JUNIPER, HUAWEI, e inclusive con el vrrpd de Linux.
- ✓ No anuncia rutas IP ni afecta a la tabla de encaminamiento.
- ✓ Está diseñado para eliminar la fuente de fallos inherentes a la estática enrutados por defecto en el medio ambiente.
- ✓ Soportado en interfaces Ethernet, Fast Ethernet y Gigabit Ethernet.
- ✓ Compatible con MPLS, VPNS y VLANS.

2.1.2.2 HSRP (Hot Standby Router Protocol)

- ✓ Permite el despliegue de routers redundantes tolerantes a fallos en una red.
- ✓ Posee un router de reserva en el mismo grupo que empieza a reenviar el tráfico.
- ✓ Es flexible ya que el administrador de red puede controlar todo el comportamiento de los routers de un grupo (incluyendo que router es el router de reenvío principal, cuales son los routers de reserva, si éstos conservan la función de reenvío cuando pueda volver a utilizarse el router de reenvío principal, y la capacidad de otra interfaz del router para conducir el trafico al router de reserva).
- ✓ A intervalos regulares, los routers, intercambian información para determinar cuáles de ellos siguen estando presentes y son capaces de reenviar tráfico.
- ✓ El router de reenvío principal y el de reserva introducen en la tabla ARP la dirección IP y la dirección MAC de la dirección virtual.
- ✓ Posee el comando show standby que muestra la información de HSRP, que incluye el estado de los reenvíos, la prioridad HSRP y las interfaces a las que realizan seguimientos del router al que se realizan consultas.
- ✓ No se limita a 2 routers, sino que se puede generar grupos de router que trabajen en conjunto de modo de tener múltiples dispositivos en situación standby.

- ✓ Evita la existencia de puntos de fallo únicos en la red mediante técnicas de redundancia y comprobación del estado de los routers.

2.1.2.2 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.
- ✓ Compartimiento de la carga: el tráfico desde los clientes de la LAN pueden ser compartidas por múltiples routers.
- ✓ Múltiple virtual routers: Hasta 1.024 routers virtuales (grupos de GLBP) pueden estar en cada interfaz física de un router, y allí pueden ser hasta cuatro routers virtuales de datos por grupo.
- ✓ Prioridad: puedes reemplazar un AVG con un gateway virtual de respaldo con una prioridad más alta (backup virtual gateway).
- ✓ Utilización eficiente de los recursos: cualquier router en el grupo puede servir de BACKUP, esto elimina la necesidad de dejar un router de

BACKUP dedicado por que todos los routers están habilitados para soportar tráfico desde la red.

2.1.3 Descripción General de VRRP, HSRP, GLBP

2.1.3.1 VRRP

Se basa en los conceptos de HSRP propiedad de Cisco. VRRP es realmente una versión estandarizada del HSRP de Cisco. Estos protocolos, similares en el concepto, no son compatibles. Por lo tanto, en nuevas instalaciones se recomienda implementar VRRP puesto que es el estándar.

Diseñado para aumentar la disponibilidad de la puerta de enlace por defecto dando servicio a máquinas en la misma subred. El aumento de fiabilidad se consigue mediante el anuncio de un router virtual como una puerta de enlace por defecto en lugar de un router físico. Dos o más routers físicos se configuran representando al router virtual, con sólo uno de ellos realizando realmente el enrutamiento. Si el router físico actual que está realizando el enrutamiento falla, el otro router físico negocia para sustituirlo. Se denomina router maestro al router físico que realiza realmente el enrutamiento y routers de respaldo a los que están en espera de que el maestro falle.

VRRP se puede usar sobre redes Ethernet, MPLS y Token Ring. El protocolo VRRP ha sido implementado más que sus competidores. Fabricantes como Extreme Networks, Dell, Nokia, Nortel, Cisco Systems, Inc, Allied Telesis, Juniper Networks, Huawei, Foundry Networks, Radware, Aethra y 3Com Corporation ofrecen routers y switches de nivel 3 que pueden utilizar el protocolo VRRP. También están disponibles implementaciones para Linux y BSD.

Hay que tener en cuenta que VRRP es un protocolo de router, no de routing. Cada instancia de VRRP se limita a una única subred. No anuncia rutas IP ni afecta a la tabla de encaminamiento.

2.1.3.1.1 Implementación

Un router virtual tiene que utilizar la siguiente dirección MAC: 00-00-5E-00-01-XX. El último byte de la dirección es el identificador de router virtual (Virtual Router Identifier o VRID), que es diferente para cada router virtual en la red. Esta dirección sólo la utiliza un único router físico a la vez, y es la única forma de que otros routers físicos puedan identificar el router maestro en un router virtual. Los routers físicos que actúan como router virtuales deben comunicarse entre ellos utilizando paquetes con dirección IP multicast y número de protocolo IP.

Los routers maestros tienen una prioridad de 255 y los de respaldo entre 1 y 254. Cuando se realiza un cambio planificado de router maestro se cambia su prioridad a 0 lo que fuerza a que los routers de respaldo se conviertan en maestros más rápidamente. De esta forma se reduce el periodo de agujero negro.

2.1.3.1.1.1 La elección del router maestro

Un fallo en la recepción de un paquete de multicast del master durante un tiempo superior a tres veces el tiempo de anuncio, hace que los routers de respaldo asuman que el router maestro está caído. El router virtual cambia su estado a "inestable" y se inicia un proceso de elección para seleccionar el siguiente router maestro de entre los routers de respaldo. Esto se realiza mediante la utilización de paquetes multicast.

Hay que hacer notar que los routers de respaldo únicamente envían paquetes multicast durante el proceso de elección. Una excepción a esta regla es cuando un router físico se configura para que derroque al master actual cuando se le introduzca en el router virtual. Esto permite al administrador de red forzar a que un router sea el maestro inmediatamente después de un arranque, por ejemplo cuando un router es más potente que otros o cuando un router utiliza el ancho de banda más barato. El router de respaldo con la prioridad más alta se convierte en el router maestro aumentando su prioridad a 255 y enviando paquetes ARP con la dirección MAC virtual y su dirección IP física. Esto redirige los paquetes del maestro caído al router maestro actual. En los casos en los que los routers de respaldo tengan todos la misma prioridad, el router de respaldo con la dirección IP más alta se convierte en el router maestro.

Todos los routers físicos que actúan como router virtual tienen que estar a un salto entre ellos. La comunicación dentro del router virtual se realiza periódicamente. Este periodo puede ajustarse cambiando el intervalo de anuncio. Cuanto más corto sea el tiempo de agujero negro será más pequeño a cambio de un aumento del tráfico de red. La seguridad se realiza respondiendo únicamente a los paquetes de primer salto, aunque se ofrecen otros mecanismos para su refuerzo, en particular para ataques locales.

La utilización de los routers de respaldo puede mejorarse mediante el balanceo de carga

2.1.3.1.2 Seguridad extensible

La funcionalidad del router virtual es aplicable a una amplia gama de entornos de interconexión que pueden emplear diferentes políticas de seguridad. El protocolo debe exigir un mínimo de configuración y sobrecarga en el funcionamiento inseguro, prever la autentificación fuerte cuando el aumento de la seguridad es

necesario, y permitirá la integración de los nuevos mecanismos de seguridad sin romper la operación compatible.

2.1.3.1.3 Protocolo

El objetivo del paquete VRRP es comunicar a todos los enrutadores VRRP la prioridad y el estado del router principal asociada con la ID del router virtual.

Los paquetes VRRP se envían encapsulados en paquetes IP. Estos son enviados a direcciones multicast IPV4 asignadas por VRRP.

2.1.3.1.4 Formato de paquetes

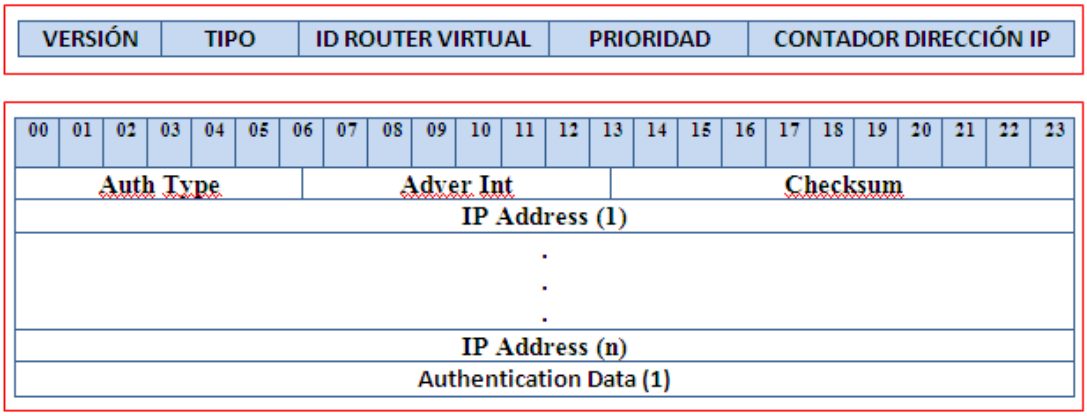


Figura II.01: Formato de paquetes VRRP

- ✓ **Versión.-** Específica la versión del protocolo VRRP de este paquete.

- ✓ **Tipo.-** Identifica el tipo de paquete VRRP, el único tipo de paquete definido en la versión del protocolo es ADVERTISEMENT**,** un paquete con protocolo desconocido debe ser rechazado.

- ✓ **ID Router Virtual.**- identifica el router virtual, este paquete está informando el estado para: Item de configuración en el rango 1-255(decimal). No hay por defecto
- ✓ **Prioridad.-** específica la prioridad de envio del router VRRP para el router virtual. Los valores más altos iguales a la prioridad más alta. Este campo es un entero sin signo de 8 bits.

- ✓ **Descripción de campos Ip**

- ✓ **Dirección Origen.-** La primera dirección Ip del paquete de direcciones está siendo enviada por Normas Hidden.

- ✓ **Dirección Destino.-** La dirección IP multicast asignado por IANA para VRRP es 224.0.0.18. Este es un enlace local de alcance a la dirección multicast. El router no debe reenviar un datagrama con esta dirección destino independientemente de su TTL.

- ✓ **TTL.-** deberá ser fijado en 255. Si un router VRRP recibe un paquete con el TTL diferente a 255, debe descartar el paquete.

- ✓ **Protocolo.-** El número de protocolo Ip asignado por la IANA para VRRP es el 112(decimal).

2.1.3.2 HSRP

El Hot Standby Router Protocol es un protocolo propiedad de CISCO que permite el despliegue de routers redundantes tolerantes a fallos en una red. Este protocolo evita la existencia de puntos de fallo únicos en la red mediante técnicas de redundancia y comprobación del estado de los routers. Es un protocolo muy similar a VRRP, que no es propietario. Es por ello que CISCO reclama que VRRP viola una serie de patentes que le pertenecen.

2.1.3.2.1 Funcionamiento

La mecánica es similar a la de los protocolos VRRP y CARP.
Supongamos que disponemos de una red que cuenta con dos routers redundantes, RouterA y RouterB. Dichos routers pueden estar en dos posibles estados diferentes: maestro (Router A) y respaldo (Router B). Ambos routers intercambian mensajes, concretamente del tipo HSRP hello, que le permiten a cada uno conocer el estado del otro. Estos mensajes utilizan la dirección multicast 224.0.0.2 y el puerto UDP 1985.

Si el router maestro no envía mensajes de tipo hello al router de respaldo dentro de un determinado periodo de tiempo, el router respaldo asume que el maestro está fuera de servicio (ya sea por razones administrativas o imprevistas, tales como un fallo en dicho router) y se convierte en el router maestro. La conversión a router activo consiste en que uno de los routers que actuaba como respaldo obtiene la dirección virtual que identifica al grupo de routers.

Elección del Router "maestro"
Para determinar cuál es el router maestro se establece una prioridad en cada router. La prioridad por defecto es 100. El router de mayor prioridad es el que se establecerá como activo. Hay que tener presente que HSRP no se limita a 2 routers, sino que soporta grupos de routers que trabajen en conjunto de modo que se dispondría de múltiples routers actuando como respaldo en situación de espera.

2.1.3.2.1.1 Paso de estado "respaldo" a estado "maestro"

El router en espera toma el lugar del router maestro, una vez que el temporizador holdtime expira (un equivalente a tres paquetes hello que no vienen desde el router activo, timer hello por defecto definido a 3 y holdtime por defecto definido a 10).

Los tiempos de convergencia dependerán de la configuración de los temporizadores para el grupo y del tiempo de convergencia del protocolo de enrutamiento empleado.

Por otra parte, si el estado del router maestro pasa a down, el router decrementa su prioridad. Así, el router respaldo lee ese decremento en forma de un valor presente en el campo de prioridad del paquete hello, y se convertirá en el router maestro si ese valor decrementado es inferior a su propia prioridad. Este proceso decremental puede ser configurado de antemano estableciendo un valor por defecto del decremento (normalmente, de 10 en 10).

2.1.3.2.2 Formato de Paquetes

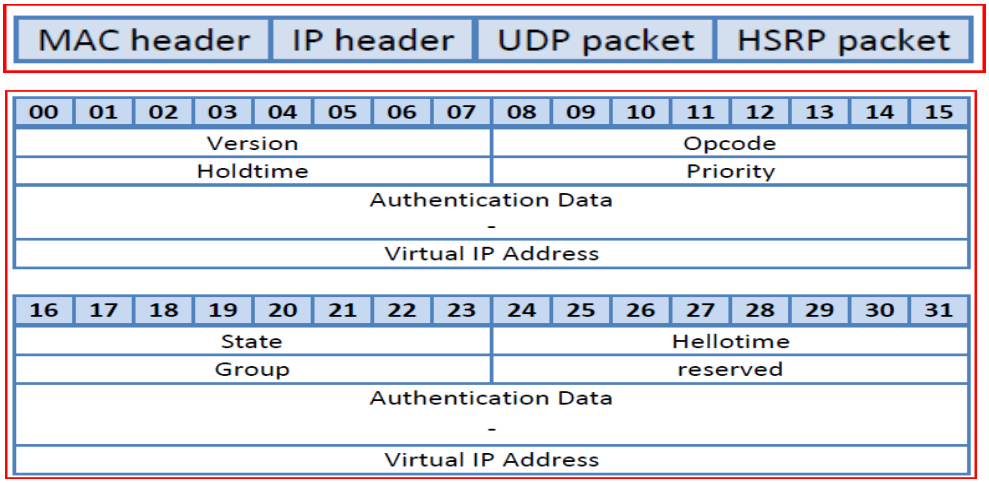


Figura II.02: Formato de paquetes HSRP

Descripción de campos

- ✓ **Versión** (8 bits): Número de versión HSRP

- ✓ **Código operación** (8 bits): Operación que se llevará a cabo.

Opcode	Función	Descripción
0	Hello	El router está funcionando y es capaz de convertirse en el router activo o de reserva.
1	Coup	El router desea convertirse en el router activo.
2	Resign	El router ya no desea ser el router activo.

Figura II.03: Código de Operación

- ✓ **Estado** (8 bits): Este campo describe el estado actual del router al enviar el mensaje.

State	Función	Descripción
0	Initial	Esta es la situación de partida y se indica que HSRP no se está ejecutando. Este estado es introducido a través de un cambio de configuración o cuando una primera interfaz aparece.
1	Learn	El router no ha determinado la dirección IP virtual, y todavía no ha visto autenticado el mensaje *Hello* desde el router activo. En este estado, el router sigue a la espera de escuchar desde el router activo.
2	Listen	El router conoce la dirección IP virtual, pero no es ni el router activo ni el router de espera. Está a la espera de comunicaciones de otros routers.
4	Speak	El router envía periódicamente mensajes *Hello* y participa activamente en la elección de los activos y/o routers de espera. Un router no puede entrar en estado *speak* a menos que tenga la dirección IP virtual.
8	Standby	El router es un candidato para convertirse en el router activo y envía mensajes periódicos *Hello*. Excluyendo condiciones transitorias, debe haber al menos un router en el grupo en estado de espera.
16	Active	El router actualmente se encuentra reenviando paquetes a la dirección del grupo MAC virtual. El router envía periódicamente mensajes de saludo. Excluyendo condiciones transitorias, debe haber al menos un router en estado activo en el grupo.

Figura II.04: Estado

- ✓ **Hellotime** (8 bits) Defecto = 3 segundos. Este campo sólo tiene sentido en mensajes Hello. Contiene el período aproximado entre los mensajes de saludo que el router envía. El tiempo se da en segundos. Si el Hellotime no está configurado en un router, entonces puede ser adquirido en el mensaje Hello del router activo. Un router que envía un mensaje Hello debe insertar el hellotime en el paquete.

- ✓ **Holdtime** (8 bits) Defecto = 10 segundos. Contiene la cantidad de tiempo que el actual Hello debe ser considerado válido. El tiempo se da en segundos. Si un router envía un mensaje Hello, a continuación, los receptores deberían considerar la validez en el tiempo Holdtime. El Holdtime debe ser de al menos tres veces el valor del Hellotime.

- ✓ **Prioridad** (8 bits) Este campo se utiliza para elegir a los routers activos y reservas. Al comparar las prioridades de los dos routers, gana el router con la prioridad más alta. En el caso de empate gana el de la dirección IP más grande.

- ✓ **Grupo** (8 bits) Este campo identifica el grupo de espera. Para Token Ring, los valores entre 0 y 2 inclusive son válidos. Para otros valores medios de comunicación entre 0 y 255 inclusive son válidos.

- ✓ **Reservados** (8 bits)

- ✓ **Datos de autenticación** (64 bits) Este campo contiene una contraseña de 8 caracteres reutilizados. Si no hay datos de autenticación se configura, el valor predeterminado recomendado es de 0x63 0x69 0x73 0x63 0x6F 0x00 0x00 0x00.

- ✓ **Dirección IP virtual** (32 bits) La dirección IP virtual utilizada por este grupo. Si la dirección IP virtual no está configurada en un router, entonces puede ser adquirida en el mensaje Hello desde el router activo. La dirección sólo se debe aprender si no se ha configurado la dirección y el mensaje Hello esta autenticado.

2.1.3.3 GLBP

Mientras HSRP Y VRRP proporcionan la elasticidad de gateway, el ancho de banda upstream no es usado por los miembros de reserva del grupo de redundancia mientras el dispositivo está en el modo de reserva. Sólo el router activo para grupos HSRP y VRRP expide (forwards) tráfico para la MAC virtual. Los recursos asociados con el router de reserva no son utilizados totalmente. Algún balanceo de carga puede ocurrir creando múltiples grupos y asignando múltiples default gateways, pero esta configuración crea una carga administrativa.

Cisco diseño el Gateway Load Balancing Protocol (GLBP) para permitir la selección automática, el empleo simultáneo de múltiples gateways, y failover automático entre aquellos gateways. Múltiples routers comparten la carga de tramas que, de una perspectiva de cliente, son enviados a una única dirección de default gateway.

Con GLBP, los recursos pueden ser utilizados totalmente sin la carga administrativa de la configuración de múltiples grupos y la gestión de múltiples configuraciones de default gateway como se requiere con HSRP Y VRRP.

2.1.3.3.1 GLBP posee las siguientes funciones

- ✓ **Active virtual gateway (AVG):** Los miembros de un grupo GLBP eligen un gateway para ser el AVG para aquel grupo. Otros miembros de grupo proporcionan el backup para el AVG si el AVG se vuelve no disponible. El AVG asigna una dirección MAC virtual a cada miembro del grupo.

- ✓ **Active virtual forwarder (AVF):** Cada gateway asume la responsabilidad para expedir (forwarding) paquetes enviados a la dirección de MAC virtual asignada por el AVG. Estos gateways son conocidos como AVFs por su dirección MAC virtual.

- ✓ **Comunicación:** Los miembros GLBP se comunican entre sí usando mensajes hello enviados cada 3 segundos a la dirección multicast 224.0.0.102, el Protocolo de Datagrama de Usuario (User datagram protocol: UDP) puerto 3222.

2.1.3.3.2 Identificación del Proceso de Operación GLBP

GLBP permite la selección automática y el empleo simultáneo de todos los gateways disponibles en el grupo. Los miembros de un grupo GLBP eligen un gateway para ser el AVG para aquel grupo. Otros miembros del grupo proporcionan backup para el AVG si este se vuelve no disponible (unavailable). El AVG asigna una dirección MAC virtual a cada miembro del grupo GLBP. Todos los routers se vuelven AVFs para tramas dirigidas a aquella dirección MAC virtual. Como los clientes envían peticiones (requests) Address resolution Protocol (ARP) para la dirección del default gateway, el AVG envía estas direcciones MAC virtuales en las respuestas de ARP. Un grupo GLBP puede tener hasta cuatro miembros de grupo.

2.1.3.3.3 Operaciones GLBP

GLBP soporta los siguientes modos operacionales para el balanceo de tráfico de carga a través de múltiples routers que revisan la misma dirección IP de default gateway:

- ✓ **Algoritmo de balanceo de carga ponderado (Weighted load-balancing algorithm):** La cantidad de carga dirigida a un router es dependiente del valor ponderado anunciado por aquel router.

- ✓ **Algoritmo balanceo de carga de host dependiente (Host-dependent load-balancing algorithm):** Un host es garantizado para usar la misma dirección MAC virtual mientras aquella dirección MAC virtual está participando en el grupo GLBP.

- ✓ **Algoritmo balanceo de carga round-robin (Round-robin load-balancing algorithm):** Como los clientes envían peticiones de ARP para resolver la dirección MAC de default gateway, la respuesta a cada cliente contiene la dirección MAC del próximo router posible en modo Round-robin. Todas las direcciones MAC de los routers toman turnos siendo incluidos en respuestas de resolución de dirección para la dirección IP del default gateway.

- ✓ GLBP automáticamente maneja la asignación de dirección de MAC virtual, determina quien maneja el forwarding, y asegura que cada estación tiene una ruta de forwarding para fallas de gateways o interfaces rastreadas. Si ocurren fallas, el ratio de balanceo de carga es ajustado entre los AVFs restante para que los recursos sean usados del modo más eficiente.

2.1.3.3.4 Formato de paquetes GLBP

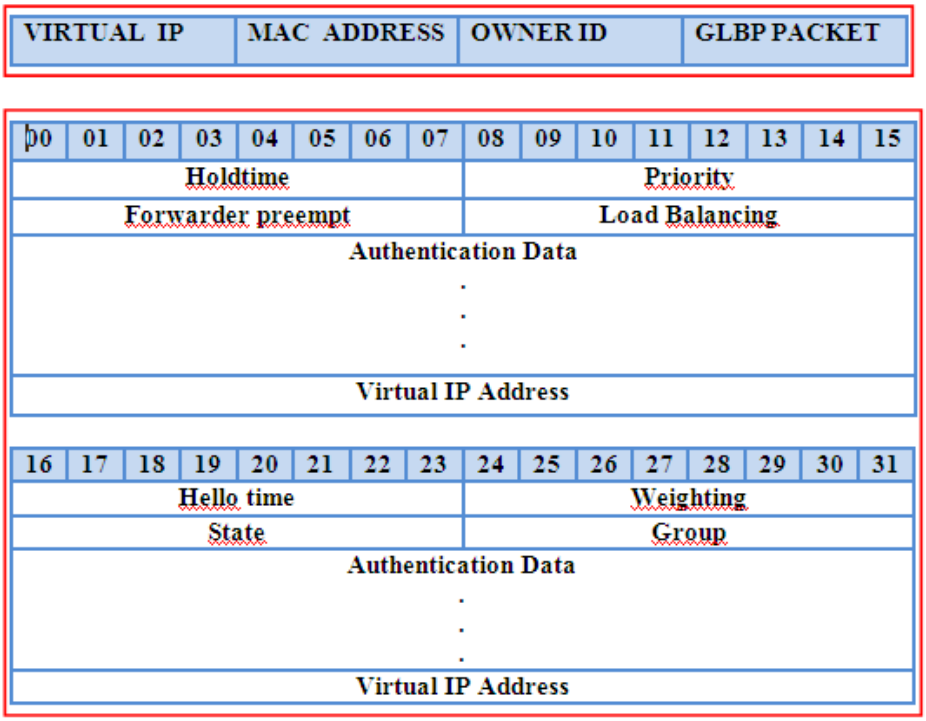


Figura II.05: Formato de paquetes GLBP

2.1.3.3.4.1 Virtual Asignación de direcciones MAC

Un grupo GLBP permite hasta cuatro direcciones MAC virtual por grupo. El AVG es responsable de asignar las direcciones MAC virtual a cada miembro del grupo. Otros miembros del grupo solicitan una dirección MAC virtual después de descubrir el AVG a través de mensajes de hello. Gateways asignan la siguiente dirección MAC en secuencia. Un fordwarder virtual asigna una dirección MAC virtual por el AVG conocido como un virtual primario. Otros miembros del grupo GLBP aprenden las direcciones MAC virtuales con mensajes hello. Un fordwaarder virtual que ha aprendido la dirección MAC virtual se conoce como forwarder virtual secundario.

2.1.3.3.4.2 Virtual Gateway de redundancia

GLBP opera redundanciavirtual en la misma forma que HSRP. Una puerta de enlace es elegido como el AVG, otra puerta de enlace es elegido como puerta de enlace virtual de espera, y las puertas de enlace restantes se colocan en un estado de escucha.

Si un AVG falla, el gateway virtual de espera asume la responsabilidad de la dirección IP virtual. Un nuevo gateway virtual de espera es electo para que los demás gateways estén en estado de alerta.

2.1.3.3.4.3 Prioridad de Gateway

Prioridad de puerta de enlace GLBP determina el papel que desempeña cada puerta de enlace GLBP y qué ocurre si el AVG falla.

Prioridad también determina si un router GLBP funciona como puerta de acceso virtual de copia de seguridad y el orden de ascenso a convertirse en un AVG, si el actual AVG falla. Usted puede configurar la prioridad de cada copia de seguridad del gateway virtual con un valor de 1 a 255 usando el comando de prioridad glbp.

2.1.3.3.4.4 Gateway de ponderación y de seguimiento

GLBP utiliza un sistema de ponderación para determinar la capacidad de transmisión de cada router en el grupo de GLBP. Las ponderaciones asignadas a un router en el grupo de GLBP determinan si va a reenviar paquetes y, si es así, la proporción de computadores en la LAN sabrán a que paquete enviará. Los umbrales pueden establecer en inhabilitar el reenvío cuando el peso cae por debajo de un determinado valor, y cuando se eleva por encima de otro el reenvío automáticamente se vuelve a habilitar.

La ponderación de grupo GLBP puede ser ajustado automáticamente por el seguimiento del estado de una interfaz en el router. Si una interfaz de seguimiento se baja, la ponderación del grupo GLBP se reduce en un valor determinado. Diferentes interfaces pueden ser rastreados para disminuir la ponderación GLBP por cantidades variables

2.1.4 Estándares de VRRP, HSRP Y GLBP

2.1.4.1 Estándar de VRRP

Virtual Router Redundancy Protocol (VRRP) es un protocolo de redundancia no propietario definido en el RFC 2338 en Abril de 1998 y luego modificado en el RFC 3768 de Abril del 2004, diseñado para aumentar la disponibilidad de la puerta de enlace por defecto dando servicio a máquinas en la misma subred. El aumento de fiabilidad se consigue mediante el anuncio de un router virtual como una puerta de enlace por defecto en lugar de un router físico. Dos o más routers

físicos se configuran representando al router virtual, con sólo uno de ellos realizando realmente el enrutamiento. Si el router físico actual que está realizando el enrutamiento falla, el otro router físico negocia para sustituirlo. Se denomina router maestro al router físico que realiza realmente el enrutamiento y routers de respaldo a los que están en espera de que el maestro falle.

Ámbito de Aplicación

En el RFC 2338 se describe las características, objetivos de diseño, y la teoría de operación de VRRP. Los formatos de mensaje, el protocolo de reglas de procesamiento y la máquina de estado para garantizar que se presenta la convergencia a un solo Router Virtual Maestro. Por último, las cuestiones operativas relacionadas con la asignación de direcciones MAC, el manejo de peticiones ARP, la generación de mensajes ICMP redirect, y los problemas de seguridad están dirigidas.
Este protocolo está diseñado para ser utilizado solamente con routers IPv4. Una especificación separada se producirá si se decide que una funcionalidad similar es deseable en un entorno IPv6.

Cambios del RFC 2338 en el 3768
Se han eliminado los métodos de autenticación de VRRP. Los cambios incluyen:

- ✓ Se ha quitado los valores de contraseña y la autenticación basada en IPSEC.

- ✓ Los campos y los valores se conservan para mantener la compatibilidad hacia atrás con la RFC 2338.

- ✓ Eliminada la sección sobre la seguridad extensibles

- ✓ Actualización de la seguridad considerando la sección para eliminar la discusión de distintos métodos de autenticación y añadir un nuevo texto que explica la motivación para el cambio y la descripción de las vulnerabilidades.

2.1.4.2 Estándar de HSRP

Hot Standby Router Protocol está definido en el estándar RFC 2281, un conjunto de routers trabajan en conjunto para presentar la ilusión de un único router virtual para los host de la LAN. Este conjunto se conoce como un HSRP o un grupo de espera. Un solo router electo del grupo es el encargado de transmitir los paquetes que los host envían al router virtual. Este router es conocido como el router activo. Otro router es elegido como el router de espera. En el caso de que el router activo falla, el que está en modo en espera asume las funciones de reenvío de paquetes del router activo. Aunque un número arbitrario de routers pueden funcionar HSRP, sólo el router activo envía los paquetes al router virtual.
Para minimizar el tráfico de red, sólo los routers activos y los routers de espera envían mensajes periódicos HSRP, una vez que el protocolo ha completado el proceso de elección. Si el router activo falla, el router standby asume el router activo. Si el router no espera o se convierte en el router activo, otro router es elegido como el router de espera.

En una LAN en particular, varios grupos de reserva pueden coexistir y superponerse. Cada grupo espera emular un router virtual. Para cada grupo de espera, una única dirección MAC conocida es asignada al grupo, así como una dirección IP. La dirección IP debe pertenecer a la subred primaria en el uso de la LAN, pero debe diferir de las direcciones de interfaz asignadas en todos los routers y los hosts en la LAN, incluyendo direcciones IP virtuales asignadas a otros grupos HSRP.

Si se utilizan varios grupos en una sola LAN, la división de la carga se puede lograr mediante la distribución de los host de los diferentes grupos de reserva. El resto de esta especificación describe el funcionamiento de un grupo de espera único. En el caso de varios grupos, cada grupo funciona de manera independiente de otros grupos de la LAN y de acuerdo con esta especificación. Tenga en cuenta que los routers individuales pueden participar en varios grupos. En este caso, el router mantiene el estado independiente y contadores de tiempo para cada grupo.

Condiciones de uso

N º Patente EE.UU. 5473599, asignados a Cisco Systems, Inc. pueden ser aplicables a HSRP. Si una aplicación requiere el uso de cualquier reclamo de la patente No. 5.473.599, Cisco tiene la licencia de tales reclamaciones en condiciones razonables y no discriminatorias para su uso en la práctica de la norma. Más concretamente, dicha licencia estará disponible para una sola vez, pagado honorarios.

Ámbito de aplicación

El RFC2281 describe los paquetes, mensajes, estados y eventos para implementar el protocolo. No hablar de gestión de red o problemas internos de aplicación.

2.1.4.3 Estándar GLBP

Gateway Load Balancing Protocol no tiene RFC (propietario de Cisco), se utiliza con routers Cisco, esta es una mejora sobre HSRP, ya que permite compartir la carga de forma predeterminada. Puede configurar GLBP de tal manera que el tráfico de clientes de LAN puede ser compartido por varios routers, con lo que comparten la carga de tráfico de manera más equitativa entre los routers

disponibles. GLBP soporta hasta 1024 routers virtuales (grupos GLBP) en cada interfaz física de un router, y hasta 4 agentes virtuales por grupo.

Cisco define en su documento lo que es necesario para este protocolo, es decir: GLBP Active Virtual Gateway, GLBP Virtual MAC Address Assignment, GLBP Virtual Gateway Redundancy, GLBP Virtual Forwarder Redundancy, GLBP Gateway Priority, GLBP Gateway Weighting and Tracking, GLBP Benefits

2.2.- Redes de Campus

2.2.1.- Definición

Una red de área de campus conocido como (CAN) se usa para interconectar las redes en la situación geográfica limitada como el campus universitario, bases militares, o campus de organización, etc. Esta puede ser tomada como una red metropolitana que tiene la configuración especifica en un área pequeña sólo como un laboratorio de cómputo en la universidad.

El área CAN (la Red de Área de Campus) es indudablemente más grande que una red del área local pero sigue siendo más pequeño una red del área amplia. Estas redes están diseñadas para un lugar en particular que incide el nivel más alto. Por ejemplo, varios laboratorios, oficinas múltiples en los edificios etc. la mayoría del tiempo, este término se conoce como el campus universitario pero cuando se usa al nivel de organización, lo llamamos la red del campus corporativa.

2.2.1.2.- Las tradicionales redes de campus

En los primeros días de la creación de redes, principalmente las universidades de investigación y los militares experimentaron las redes informáticas. El término red del campus deriva de las redes construidas en los campus universitarios. Hoy en día, el término se utiliza más ampliamente para incluir redes que se extienden

de las empresas "campus". El tamaño del Campus es un factor importante en el diseño de la red. Un campus grande tiene varios o muchos edificios co-localizados, un campus mediano es uno o algunos edificios co-localizados, mientras que un pequeño campus tiene un solo edificio.

Históricamente, las redes de campus consistía en una sola LAN a la que se añadian nuevos usuarios simplemente mediante la conexión en cualquier lugar de la LAN. Debido a las limitaciones de distancia de los medios de comunicación de redes, las redes de campus por lo general se limitan a un edificio o varios edificios muy cerca unos de otros, véase la **Figura II.06.**

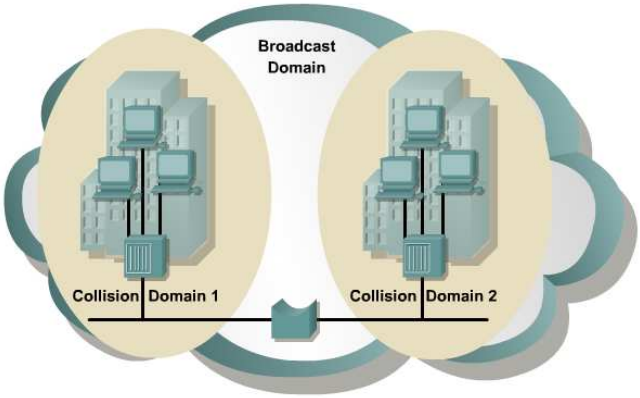


Figura II.06: Red de Campus

La LAN es una red física que conecta los dispositivos. En el caso de Ethernet, todos los dispositivos compartidos disponibles, half-duplex, de 10 megabits por segundo (Mbps). Debido a que se detecto la colisión de acceso múltiple por detección de portadora (CSMA / CD) método de acceso utilizado por Ethernet, toda la LAN era considerado un único dominio de colisión.

Pocas fueron las consideraciones de diseño necesarias para proporcionar al usuario acceso al backbone. Debido a las limitaciones inherentes de Ethernet, se conectaron a veces los usuarios físicamente adyacentes a un solo dispositivo de acceso para minimizar el número taps en la backbone. Aunque los hubs cumplen este requisito y se convirtió en un dispositivo estándar para el acceso a la red

múltiples, incrementó la demanda de los usuarios rápidamente y disminuyó el rendimiento de la red. **Figura II.07**

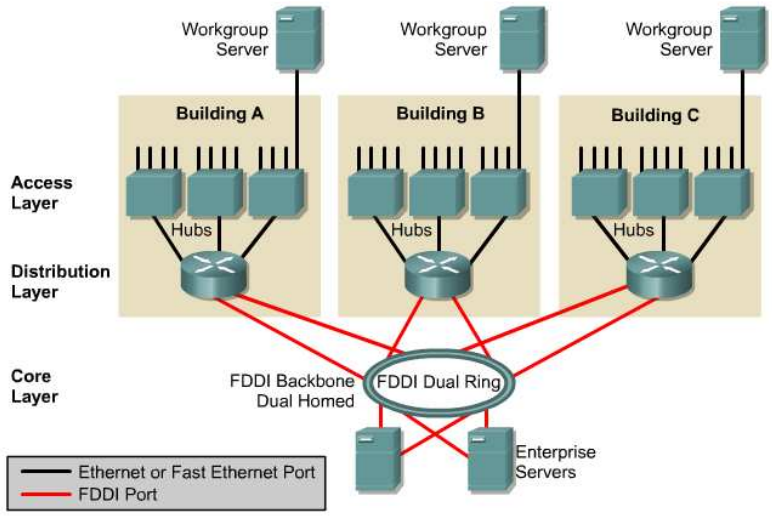


Figura II.07: Utilización del Hub

2.2.1.3 Problemas con los diseños tradicionales de red del campus

Los dos problemas principales con las redes tradicionales han sido siempre la disponibilidad y el rendimiento. Estos dos problemas son impactados por la cantidad de ancho de banda disponible. En un único dominio de colisión, las tramas son visibles para todos los dispositivos de la LAN y están libres de colisión.

Los dispositivos multipuerto de Capa 2, como bridges y switches, se utilizan para el segmento de LAN en dominios de colisión discreta y envian tramas de datos de nivel 2 solamente al segmento de la red que contiene la dirección de destino. Debido a que los puertos de capa 2 separan la LAN en los distintos segmentos físicos, también ayudan a resolver problemas relacionados con las limitaciones de distancia de Ethernet.

Sin embargo, la difusión de tramas que contiene la dirección MAC sigue inundadas a lo largo de toda la red. **Figura II.08**

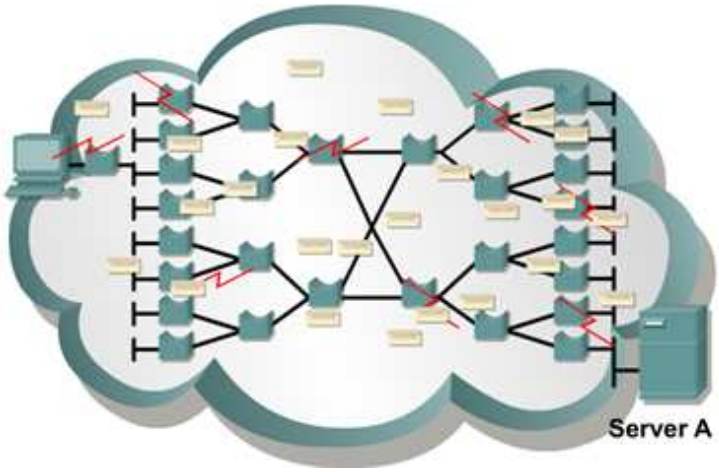


Figura II.08: Difusión de Tramas

Un solo dispositivo de red puede funcionar mal e inundar la red con "ruido" y esto podría provocar la caída de la red. Aquí es donde los routers entran. Los routers operan en la Capa 3 del modelo Open System Interconnection (OSI), éstos son capaces de tomar decisiones inteligentes sobre el flujo de datos hacia y desde un segmento de red.

El tráfico que puede afectar al rendimiento de la red es el tráfico que investiga sobre el estado de los componentes de red o la disponibilidad y lo anuncia. Los dos tipos comunes de transmisiones que se registra en la red son las solicitudes IP Address Resolution Protocol (ARP) como se muestra en la **Figura II.09** y el nombre de la petición NetBIOS. Estos broadcast se propagan normalmente a través de una subred completa y esperan que el dispositivo de destino responda directamente al broadcast.

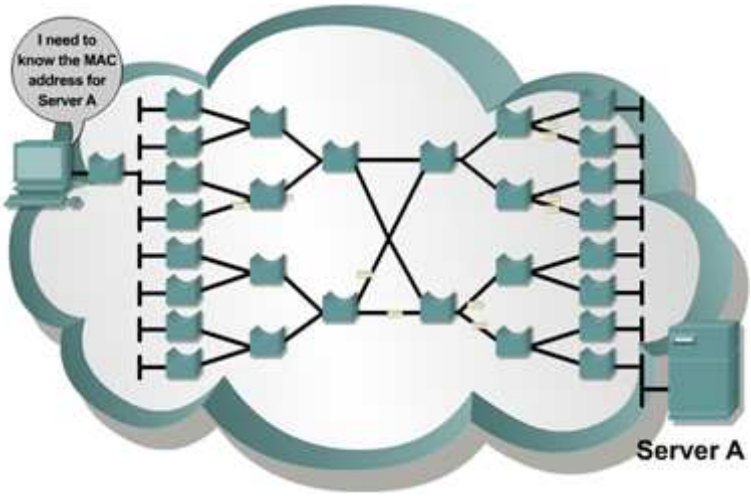


Figura II.09: Solicitudes IP

Además del broadcast, el tráfico multicast también puede consumir una gran cantidad de ancho de banda. El tráfico de multicast se propaga a un grupo específico de usuarios. Dependiendo del número de usuarios en un grupo multicast o el tipo de datos de aplicación que contuviera en el paquete multicast, este tipo de broadcast puede consumir la mayoria, si no todos, los recursos de red. Un ejemplo de una aplicación multicast es el streaming de audio y video que usa multicast para transportar paquetes multimedia.

A medida que las redes crecen, también lo hace la cantidad de tráfico de broadcast en la red. El broadcast excesivo reduce el ancho de banda disponible para los usuarios finales y forza a los nodos de los usuarios finales a desperdiciar ciclos del CPU con procesos innecesarios. En el peor de los casos, las tormentas de broadcast efectivamente puede cerrar la red monopolizando el ancho de banda disponible.

Con dos métodos se pueden resolver el problema de broadcast para los grandes sitios de LAN conmutada. La primera opción es utilizar routers para crear subredes múltiples y lógicamente segmentar el tráfico, como se muestra en la **Figura II.10** El broadcast no pasa a través de los routers. Aunque este enfoque contendrá tráfico de broadcast, la CPU de un router tradicional tendrá que procesar cada paquete. Esta situación puede crear un cuello de botella en la red.

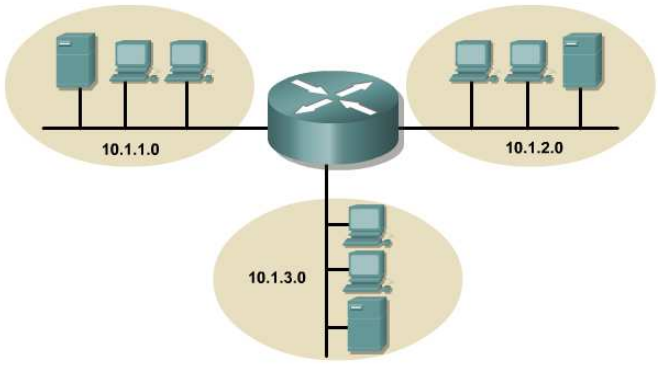


Figura II.10: Utilización del Router

Una segunda opción sería implementar redes de área local virtuales (VLAN) dentro de la red conmutada, como se muestra en la **Figura II.11**. A Las VLAN se define básicamente como dominios de broadcast. Una VLAN es un grupo de dispositivos finales que pueblan múltiples segmentos de LAN físico y los puertos del switch. Se comunican como si estuvieran en un solo segmento de LAN. Uno de los principales beneficios de conmutadores LAN con VLAN se pueden utilizar para contener con eficacia el tráfico de broadcasst y administrar los flujos de tráfico.

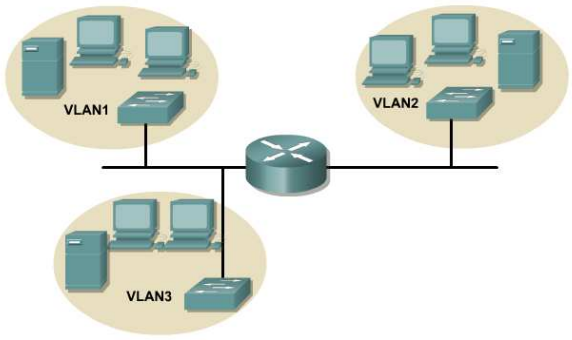


Figura II.11: Utilización de Vlans

2.2.1.4 Regla tradicional 80/20 de tráfico de la red

Idealmente, los usuarios finales con intereses comunes o patrones de trabajo se colocan en la misma red lógica que los servidores a los que acceden más. La mayoría del tráfico dentro de estas redes lógicas se encuentra en el segmento local de la LAN. Esta simple tarea eficaz reduce al mínimo la carga sobre la red troncal.

Como se muestra en la **Figura II.12**, la regla 80/20 establece una red bien diseñada, el 80 por ciento del tráfico en un segmento de red dada es local. No más de 20 por ciento del tráfico de red debe moverse a través del backbone de la red. La congestión de red troncal es una indicación de que los patrones de tráfico no están cumpliendo con la regla 80/20. En este caso, en lugar de agregar switches o reemplazar los hubs con switches, los administradores de red pueden mejorar el rendimiento de la red mediante uno de los siguientes:

- ✓ Traslado de recursos tales como aplicaciones, programas de software y archivos de un servidor a otro para contener el tráfico local dentro de un grupo de trabajo.
- ✓ Moviendo a los usuarios lógicamente, si no físicamente, de manera que los grupos de trabajo reflejen mejor los patrones de tráfico reales.
- ✓ Agregando los servidores para que los usuarios pueden acceder a ellos a nivel local sin tener que cruzar el backbone.

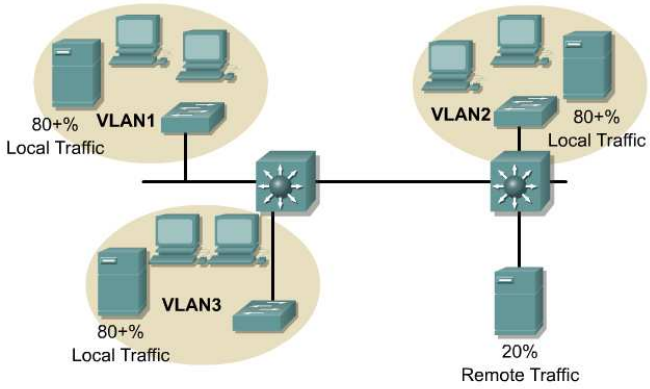


Figura II.12: Diseño de Red de Campus con la regla 80/20

2.2.1.5 La nueva regla 20/80 de tráfico de red

En las redes de hoy, los patrones de tráfico se están moviendo hacia lo que ahora se conoce como el modelo 20/80, como se muestra en la **Figura II.13**. En el modelo 20/80, sólo el 20 por ciento del tráfico sigue siendo local del grupo de trabajo de la LAN, y el 80 por ciento del tráfico sale de la red local.

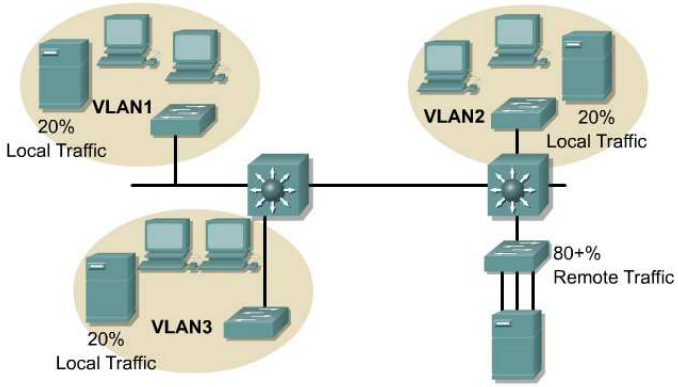


Figura II.13: Diseño de Red de Campus con la regla 20/80

Dos factores han contribuido a estos patrones de tráfico cambiantes:

- ✓ **El Internet -** Con la información basada en la web y las aplicaciones de Internet, un PC puede ser una herramienta para publicar y acceder a la información. Así que ahora la información puede venir de cualquier parte de la red, lo que puede crear grandes cantidades de tráfico que cruza las fronteras de subred. Los usuarios saltan de forma transparente entre servidores a través de la empresa mediante el uso de hipervínculos, sin tener que preocuparse de dónde se encuentran los datos.

- ✓ **Granjas de Servidores -** El segundo factor que conduce a la disminución de las redes locales centrado es el movimiento hacia la consolidación de servidores. Las empresas están implementando granjas de servidores centralizados para la seguridad, facilidad de manejo y reducción del costo de propiedad. Todo el tráfico de las subredes del cliente con estos servidores deben viajar a través del backbone del campus.

Sin embargo, este cambio en los patrones de tráfico requiere el rendimiento de nivel 3 para la aproximación de rendimiento del nivel 2. Porque el enrutamiento es un proceso intensivo del CPU, este procesamiento de capa 3 puede crear cuellos de botella. Esto es lo que impulsa el continuo aumento de las necesidades en redes de campus.

2.2.1.6 Los requisitos fundamentales de la evolución de la estructura del campus

Los requisitos clave de ejercer presión sobre los diseños del campus emergentes son los siguientes:

- ✓ **Convergencia Rápida.-** Este requisito se establece que la red debe ser capaz de adaptarse muy rápidamente a los cambios en la topología de red, como enlaces caídos y la inserción de nuevos dispositivos en la red. La convergencia rápida se torna aún más crítica cuando la red del campus

crece en el ámbito geográfico. Esto se ilustra en la **Figura II.14**, donde se presenta un ejemplo de falla del enlace.

- ✓ **Trayectorias deterministas.-** Este requisito permite que un dispositivo o un administrador tomar una decisión basada en la conveniencia de una ruta dada a un destino para determinadas aplicaciones o grupos de usuarios.

- ✓ **La redundancia.-** Este requisito especifica un mecanismo, como los enlaces redundantes, dispositivos o módulos, para asegurar que la red esté operativa en todo momento. En el gráfico, cada switch tiene enlaces redundantes.

- ✓ **Escalable.-** Este requisito establece que a medida que la red crece y se añaden nuevas aplicaciones, la infraestructura debe ser capaz de manejar las demandas de aumento del tráfico. El gráfico ilustra un diseño jerárquico altamente escalable.

- ✓ **Aplicaciones Centralizadas.-** Este requisito establece que las solicitudes centralizadas están disponibles para apoyar a la mayoría o a todos los usuarios de la red. En el gráfico, la granja de servidores se encuentra en una ubicación centralizada utilizando el mismo número de saltos para cada área de la red.

- ✓ **La nueva regla 20/80.-** Este requisito se centra en el cambio en los patrones de tráfico tradicionales.

- ✓ **Soporte multiprotocolo.-** Este requisito se especifica que las redes de campus deben ser capaces de soportar entornos multiprotocolo.

- ✓ **La multidifusión.-** Este requisito exige que las redes de campus pueden soportar tráfico IP multicast, además de tráfico IP unicast.

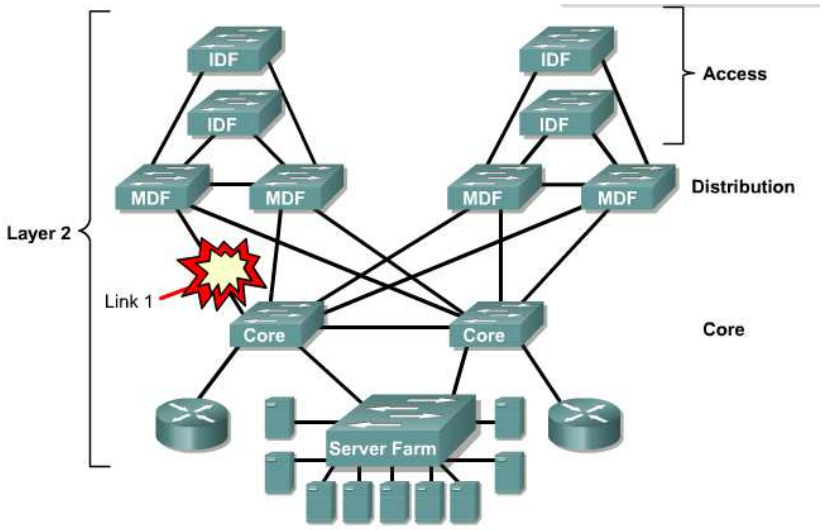


Figura II.14: Ejemplo de falla de enlace

2.2.1.7 La evolución de la estructura del campus

El aumento de demandas de los usuarios y las aplicaciones complejas han obligado a los diseñadores de redes a centrarse en los patrones de tráfico real en la red. Las redes ya no pueden ser divididas en subredes basándose únicamente en el número de usuarios. La aparición de servidores empresariales que ejecutan las aplicaciones al servicio de todos los usuarios también tiene un efecto directo sobre la carga a través de la red. Una carga de tráfico alta en toda la red, se traduce en la necesidad de una técnica eficiente de enrutamiento y conmutación. En el nuevo modelo de campus, los patrones de tráfico dictan la colocación de los servicios requeridos por el usuario final. Para dar servicio al tráfico local, los switch de nivel 2 se mueven hacia el borde de la red y en los armarios de cableado. Estos switch conectan los dispositivos de usuario final y los servidores en un grupo de trabajo común. Los servicios se pueden dividir en tres categorías diferentes:

- ✓ Los servicios locales
- ✓ Servicios a Distancia
- ✓ Servicios de Empresa

Un servicio local es aquella en las que las entidades que prestan el servicio residen en la misma subred, y por lo tanto, la misma red virtual que el usuario. Los servicios locales permanecen en áreas específicas de la red. El tráfico hacia y desde los servicios locales se limita a los vínculos entre el servidor, switches, y los usuarios finales. El tráfico local no entra en la red troncal, o pasa a través de un router. **Figura II.15.**

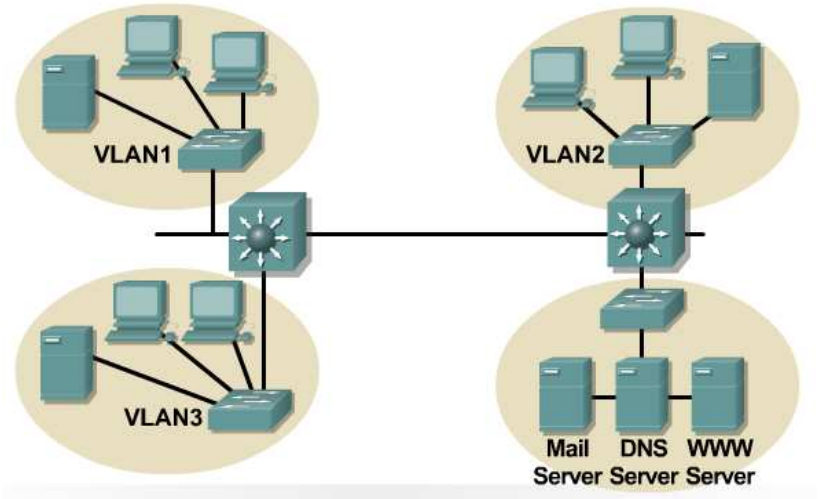


Figura II.15: Implementación de VLAN

Un servicio remoto o a distancia es una entidad que puede estar geográficamente cerca del usuario final, pero no en la misma subred o VLAN como el usuario. El tráfico hacia y desde los servicios a distancia puede o no puede cruzar el backbone. Las solicitudes de los servicios remotos tendrán que cruzar los límites de emisión de dominio debido a que estos servicios están a distancia para el usuario final solicitante. Por lo tanto, los switches deben conectarse a dispositivos de Capa 3 para permitir el acceso a servicios remotos.

Los servicios empresariales son los servicios comunes a todos los usuarios. Ejemplos de los servicios de la empresa son el correo electrónico, acceso a Internet y videoconferencia. Debido a que todos los usuarios necesitan acceder a los servicios de la empresa, estos servidores y servicios existentes en una subred independiente situados cerca del backbone **Figura II.16**. Dado que los servicios

de la empresa existen fuera del dominio de broadcast de los usuarios finales, los dispositivos de Capa 3 se requieren para acceder a estos servicios. Los servicios de la empresa pueden o no estar agrupados por switches de Capa 2.

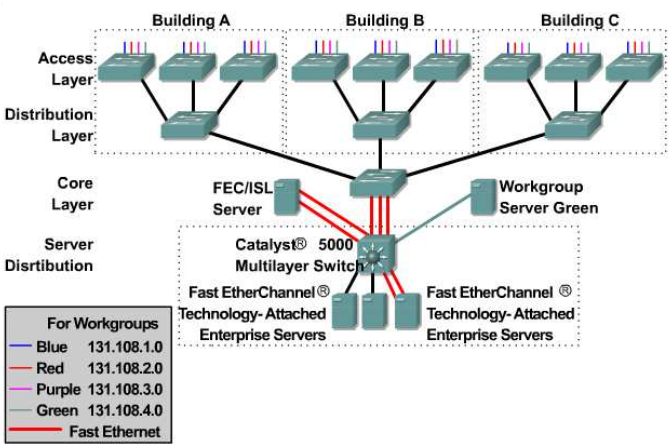


Figura II.16: Subred de Servidores

La colocación de los servidores de la empresa cerca del backbone asegura la misma distancia de cada usuario. Esto también significa que todo el tráfico va a un servidor de la empresa de hecho se cruza el backbone de la red.

2.2.2 Arquitectura de Red

Las redes deben admitir una amplia variedad de aplicaciones y servicios, como así también funcionar con diferentes tipos de infraestructuras físicas. El término arquitectura de red, en este contexto, se refiere a las tecnologías que admiten la infraestructura y a los servicios y protocolos programados que pueden trasladar los mensajes en toda esa infraestructura. Debido a que las redes evolucionan, descubrimos que existen cuatro características básicas que la arquitectura subyacente necesita para cumplir con las expectativas de los usuarios:

- ✓ Tolerancia a fallas
- ✓ Escalabilidad

- ✓ Calidad del servicio y
- ✓ Seguridad.

Tolerancia a fallas

Una red tolerante a fallas es la que limita el impacto de una falla del software o hardware y puede recuperarse rápidamente cuando se produce dicha falla. Estas redes dependen de enlaces o rutas redundantes entre el origen y el destino del mensaje. Si un enlace o ruta falla, los procesos garantizan que los mensajes pueden enrutarse en forma instantánea en un enlace diferente transparente para los usuarios en cada extremo. Tanto las infraestructuras físicas como los procesos lógicos que direccionan los mensajes a través de la red están diseñados para adaptarse a esta redundancia. Ésta es la premisa básica de la arquitectura de redes actuales.

Escalabilidad

Una red escalable puede expandirse rápidamente para admitir nuevos usuarios y aplicaciones sin afectar el rendimiento del servicio enviado a los usuarios actuales. La capacidad de la red de admitir estas nuevas interconexiones depende de un diseño jerárquico en capas para la infraestructura física subyacente y la arquitectura lógica. El funcionamiento de cada capa permite a los usuarios y proveedores de servicios insertarse sin causar disrupción en toda la red. Los desarrollos tecnológicos aumentan constantemente las capacidades de transmitir el mensaje y el rendimiento de los componentes de la estructura física en cada capa. Estos desarrollos, junto con los nuevos métodos para identificar y localizar usuarios individuales dentro de una internetwork, estan permitiendo a Internet mantenerse al ritmo de la demanda de los usuarios.

Calidad de servicio (QoS)

Las transmisiones de voz y video en vivo requieren un nivel de calidad consistente y un envío ininterrumpido que no era necesario para las aplicaciones informáticas tradiciónales. La calidad de estos servicios se mide con la calidad de experimentar la misma presentación de audio y video en persona. Las redes de voz y video tradicionales están diseñadas para admitir un único tipo de transmisión y, por lo tanto, pueden producir un nivel aceptable de calidad. Los nuevos requerimientos para admitir esta calidad de servicio en una red convergente cambian la manera en que se diseñan e implementan las arquitecturas de red.

Seguridad

Internet evolucionó de una internetwork de organizaciones gubernamentales y educativas estrechamente controlada a un medio ampliamente accesible para la transmisión de comunicaciones personales y empresariales. Como resultado, cambiaron los requerimientos de seguridad de la red. Las expectativas de privacidad y seguridad que se originan del uso de internetworks para intercambiar información empresarial crítica y confidencial excede lo que puede enviar la arquitectura actual. La rápida expansión de las áreas de comunicación que no eran atendidas por las redes de datos tradicionales aumenta la necesidad de incorporar seguridad en la arquitectura de red. Como resultado, se está dedicando un gran esfuerzo a esta área de investigación y desarrollo. Mientras tanto, se están implementando muchas herramientas y procedimientos para combatir los defectos de seguridad inherentes en la arquitectura de red.

2.2.3 EL MODELO DE REDES JERÁRQUICAS

La construcción de una LAN que satisfaga las necesidades de empresas pequeñas o medianas tiene más probabilidades de ser exitosa si se utiliza un modelo de diseño jerárquico. En comparación con otros diseños de redes, una red jerárquica

se administra y expande con más facilidad y los problemas se resuelven con mayor rapidez.

El diseño de redes jerárquicas implica la división de la red en capas independientes. Cada capa cumple funciones específicas que definen su rol dentro de la red general. La separación de las diferentes funciones existentes en una red hace que el diseño de la red se vuelva modular y esto facilita la escalabilidad y el rendimiento. El modelo de diseño jerárquico típico se separa en tres capas:

- ✓ Capa de acceso
- ✓ Capa de distribución y,
- ✓ Capa núcleo

2.2.3.1 Capa de acceso

La capa de acceso hace interfaz con dispositivos finales como las PC, impresoras y teléfonos IP, para proveer acceso al resto de la red. Esta capa de acceso puede incluir routers, switches, puentes, hubs y puntos de acceso inalámbricos. El propósito principal de la capa de acceso es aportar un medio de conexión de los dispositivos a la red y controlar qué dispositivos pueden comunicarse en la red.

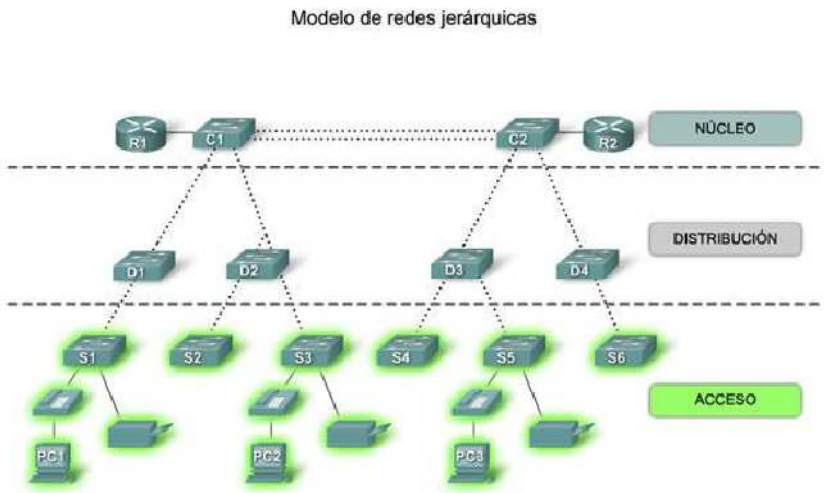


Figura II.17: Capa de Acceso

2.2.3.2 Capa de distribución

La capa de distribución agrega los datos recibidos de los switches de la capa de acceso antes de que se transmitan a la capa núcleo para el enrutamiento hacia su destino final. La capa de distribución controla el flujo de tráfico de la red con el uso de políticas y traza los dominios de broadcast al realizar el enrutamiento de las funciones entre las LAN virtuales (VLAN) definidas en la capa de acceso. Las VLAN permiten al usuario segmentar el tráfico sobre un switch en subredes separadas. Por ejemplo, en una universidad el usuario podría separar el tráfico según se trate de profesores, estudiantes y huéspedes.

Normalmente, los switches de la capa de distribución son dispositivos que presentan disponibilidad y redundancia altas para asegurar la fiabilidad.

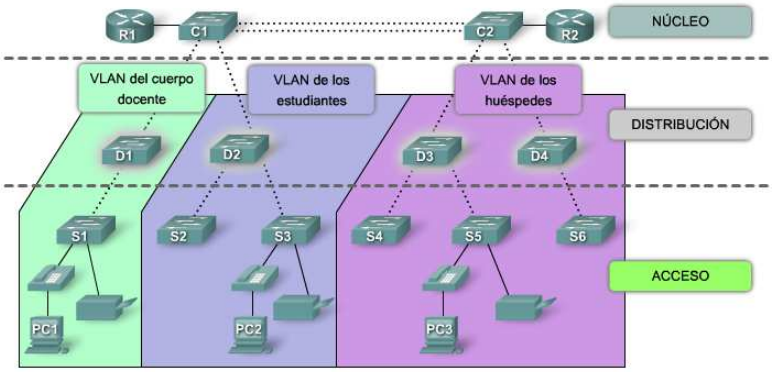


Figura II.18: Capa de distribución

2.2.3.3 Capa núcleo

La capa núcleo del diseño jerárquico es la backbone de alta velocidad de la internetwork. La capa núcleo es esencial para la interconectividad entre los dispositivos de la capa de distribución, por lo tanto, es importante que el núcleo sea sumamente disponible y redundante. El área del núcleo también puede conectarse a los recursos de Internet. El núcleo agrega el tráfico de todos los

dispositivos de la capa de distribución, por lo tanto debe poder reenviar grandes cantidades de datos rápidamente.

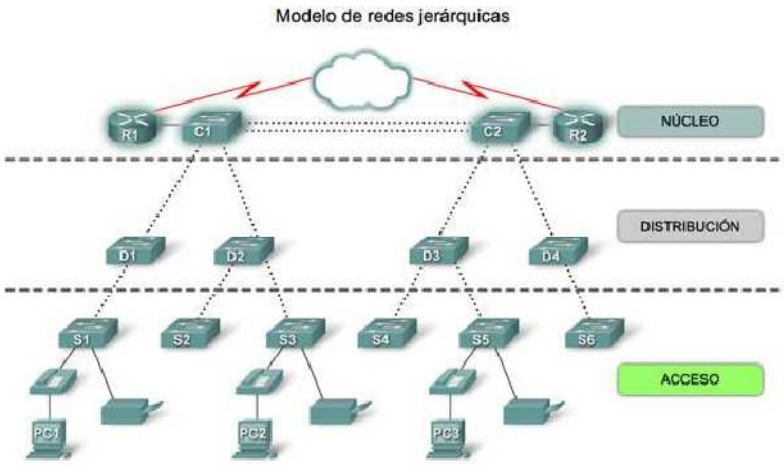


Figura II.19: Capa de Núcleo

Nota: En redes más pequeñas, no es inusual que se implemente un modelo de núcleo colapsado, en el que se combinan la capa de distribución y la capa núcleo en una capa.

2.2.3.4 Red jerárquica en una empresa mediana

Examinemos un modelo de red jerárquica aplicada a una empresa. En la figura, las capas de acceso, de distribución y núcleo se encuentran separadas en jerarquías bien definidas. Esta representación lógica contribuye a que resulte fácil ver qué switches desempeñan qué función. Es mucho más difícil ver estas capas jerárquicas cuando la red se instala en una empresa.

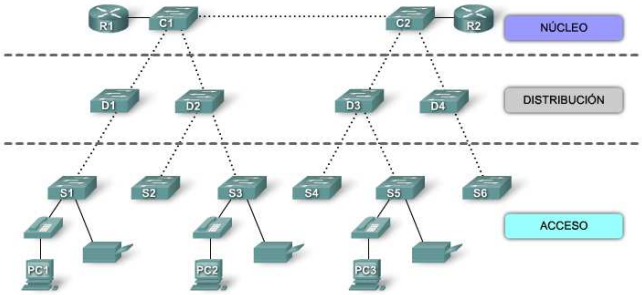


Figura II.20: Diseño lógico

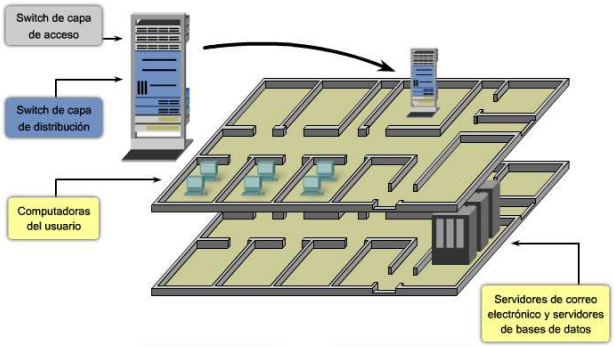


Figura II.21: Diseño físico

La **Figura II.21** muestra dos pisos de un edificio. Las computadoras del usuario y los dispositivos de la red que necesitan acceso a la red se encuentran en un piso. Los recursos, como servidores de correo electrónico y servidores de bases de datos, se ubican en otro piso. Para asegurar que cada piso tenga acceso a la red, se instalan la capa de acceso y los switches de distribución en los armarios de cableado de cada piso y se conectan a todos los dispositivos que necesitan acceso a la red. La **Figura II.21** muestra un pequeño bastidor de switches. El switch de la capa de acceso y el switch de la capa de distribución se encuentran apilados uno sobre el otro en el armario de cableado.

Aunque no se muestran los switches de la capa núcleo y otros switches de la capa de distribución, es posible observar cómo la distribución física de una red difiere de la distribución lógica de una red.

2.2.3.5 Beneficios de una red jerárquica

Existen muchos beneficios asociados con los diseños de la red jerárquica.

Escalabilidad

Las redes jerárquicas escalan muy bien. La modularidad del diseño le permite reproducir exactamente los elementos del diseño a medida que la red crece. Debido a que cada instancia del módulo es consistente, resulta fácil planificar e implementar la expansión. Por ejemplo, si el modelo del diseño consiste en dos switches de la capa de distribución por cada 10 switches de la capa de acceso, puede continuar agregando switches de la capa de acceso hasta tener 10 switches de la capa de acceso interconectados con los dos switches de la capa de distribución antes de que necesite agregar switches adicionales de la capa de distribución a la topología de la red. Además, a medida que se agregan más switches de la capa de distribución para adaptar la carga de los switches de la capa de acceso, se pueden agregar switches adicionales de la capa núcleo para manejar la carga adicional en el núcleo.

Redundancia

A medida que crece una red, la disponibilidad se torna más importante. Puede aumentar radicalmente la disponibilidad a través de implementaciones redundantes fáciles con redes jerárquicas. Los switches de la capa de acceso se conectan con dos switches diferentes de la capa de distribución para asegurar la redundancia de la ruta. Si falla uno de los switches de la capa de distribución, el switch de la capa de acceso puede conmutar al otro switch de la capa de distribución. Adicionalmente, los switches de la capa de distribución se conectan con dos o más switches de la capa núcleo para asegurar la disponibilidad de la ruta si falla un switch del núcleo. La única capa en donde se limita la redundancia es la capa de acceso.

Habitualmente, los dispositivos de nodo final, como PC, impresoras y teléfonos IP, no tienen la capacidad de conectarse con switches múltiples de la capa de acceso para redundancia. Si falla un switch de la capa de acceso, sólo se verían afectados por la interrupción los dispositivos conectados a ese switch en particular. El resto de la red continuaría funcionando sin alteraciones.

Rendimiento

El rendimiento de la comunicación mejora al evitar la transmisión de datos a través de switches intermediarios de bajo rendimiento. Los datos se envían a través de enlaces del puerto del switch agregado desde la capa de acceso a la capa de distribución casi a la velocidad de cable en la mayoría de los casos. Luego, la capa de distribución utiliza sus capacidades de conmutar el alto rendimiento para reenviar el tráfico hasta el núcleo, donde se enruta hacia su destino final. Debido a que las capas núcleo y de distribución realizan sus operaciones a velocidades muy altas, no existe contención para el ancho de banda de la red.

Como resultado, las redes jerárquicas con un diseño apropiado pueden lograr casi la velocidad de cable entre todos los dispositivos.

Seguridad

La seguridad mejora y es más fácil de administrar. Es posible configurar los switches de la capa de acceso con varias opciones de seguridad del puerto que proveen control sobre qué dispositivos se permite conectar a la red. Además, se cuenta con la flexibilidad de utilizar políticas de seguridad más avanzadas en la capa de distribución. Puede aplicar las políticas de control de acceso que definen qué protocolos de comunicación se implementan en su red y dónde se les permite dirigirse. Por ejemplo, si desea limitar el uso de HTTP a una comunidad de usuarios específica conectada a la capa de acceso, podría aplicar una política que

bloquee el tráfico de HTTP en la capa de distribución. La restricción del tráfico en base a protocolos de capas más elevadas, como IP y HTTP, requiere que sus switches puedan procesar las políticas en esa capa. Algunos switches de la capa de acceso admiten la funcionalidad de la Capa 3, pero en general es responsabilidad de los switches de la capa de distribución procesar los datos de la Capa 3, porque pueden procesarlos con mucha más eficacia.

Facilidad de administración

La facilidad de administración es relativamente simple en una red jerárquica. Cada capa del diseño jerárquico cumple funciones específicas que son consistentes en toda esa capa. Por consiguiente, si necesita cambiar la funcionalidad de un switch de la capa de acceso, podría repetir ese cambio en todos los switches de la capa de acceso en la red porque presumiblemente cumplen las mismas funciones en su capa. La implementación de switches nuevos también se simplifica porque se pueden copiar las configuraciones del switch entre los dispositivos con muy pocas modificaciones. La consistencia entre los switches en cada capa permite una recuperación rápida y la simplificación de la resolución de problemas. En algunas situaciones especiales, podrían observarse inconsistencias de configuración entre los dispositivos, por eso debe asegurarse de que las configuraciones se encuentren bien documentadas, de manera que pueda compararlas antes de la implementación.

Capacidad de mantenimiento

Debido a que las redes jerárquicas son modulares en naturaleza y escalan con mucha facilidad, son fáciles de mantener. Con otros diseños de la topología de la red, la administración se torna altamente complicada a medida que la red crece. También, en algunos modelos de diseños de red, existe un límite en cuanto a la extensión del crecimiento de la red antes de que se torne demasiado complicada y

costosa de mantener. En el modelo del diseño jerárquico se definen las funciones de los switches en cada capa haciendo que la selección del switch correcto resulte más fácil. La adición de switches a una capa no necesariamente significa que se evitará un cuello de botella u otra limitación en otra capa. Para que una topología de red de malla completa alcance el rendimiento máximo, es necesario que todos los switches sean de alto rendimiento porque es fundamental que cada switch pueda cumplir todas las funciones en la red. En el modelo jerárquico, las funciones de los switches son diferentes en cada capa. Se puede ahorrar dinero con el uso de switches de la capa de acceso menos costosos en la capa inferior y gastar más en los switches de la capa de distribución y la capa núcleo para lograr un rendimiento alto en la red.

2.2.3.6 PRINCIPIOS DE DISEÑO DE REDES JERÁRQUICAS

Sólo porque aparentemente una red presenta un diseño jerárquico, no significa que la red esté bien diseñada. Estas guías simples le ayudan a diferenciar entre redes jerárquicas con un buen diseño y las que presentan un diseño deficiente.

Diámetro de la red

Al diseñar una topología de red jerárquica, lo primero que debe considerarse es el diámetro de la red. Con frecuencia, el diámetro es una medida de distancia pero en este caso se utiliza el término para medir el número de dispositivos. El diámetro de la red es el número de dispositivos que un paquete debe cruzar antes de alcanzar su destino. Mantener bajo el diámetro de la red asegura una latencia baja y predecible entre los dispositivos.

En el modelo jerárquico de tres capas, la segmentación de la Capa 2 en la capa de distribución prácticamente elimina el diámetro de la red como consecuencia. En

una red jerárquica, el diámetro de la red siempre va a ser un número predecible de saltos entre el dispositivo origen y el dispositivo destino.

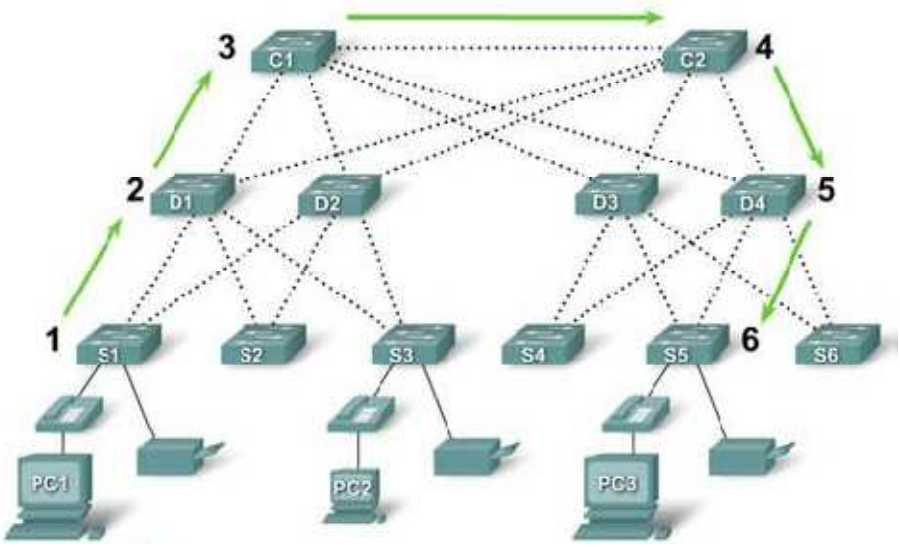


Figura II.22: Diámetro de la Red

Agregado de ancho de banda

Cada capa en el modelo de redes jerárquicas es una candidata posible para el agregado de ancho de banda. El agregado de ancho de banda es la práctica de considerar los requisitos de ancho de banda específicos de cada parte de la jerarquía. Después de que se conocen los requisitos de ancho de banda de la red, se pueden agregar enlaces entre switches específicos, lo que recibe el nombre de agregado de enlaces. El agregado de enlaces permite que se combinen los enlaces de puerto de los switches múltiples a fin de lograr un rendimiento superior entre los switches.

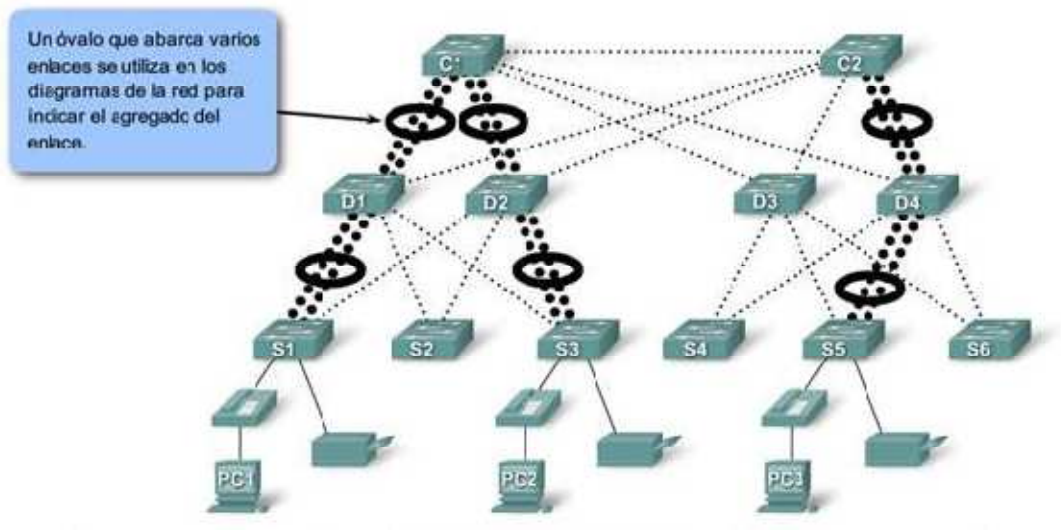


Figura II.23: Agregado de Ancho de Banda

Redundancia

La redundancia es una parte de la creación de una red altamente disponible. Se puede proveer redundancia de varias maneras. Por ejemplo, se pueden duplicar las conexiones de red entre los dispositivos o se pueden duplicar los propios dispositivos. Un análisis de la duplicación de los dispositivos de red y del empleo de protocolos especiales de red para asegurar una alta disponibilidad excede el alcance de este curso.

La implementación de los enlaces redundantes puede ser costosa. Imagine que cada switch en cada capa de la jerarquía de la red tiene una conexión con cada switch de la capa siguiente. Es improbable que sea capaz de implementar la redundancia en la capa de acceso debido al costo y a las características limitadas en los dispositivos finales pero puede crear redundancia en las capas de distribución y núcleo de la red.

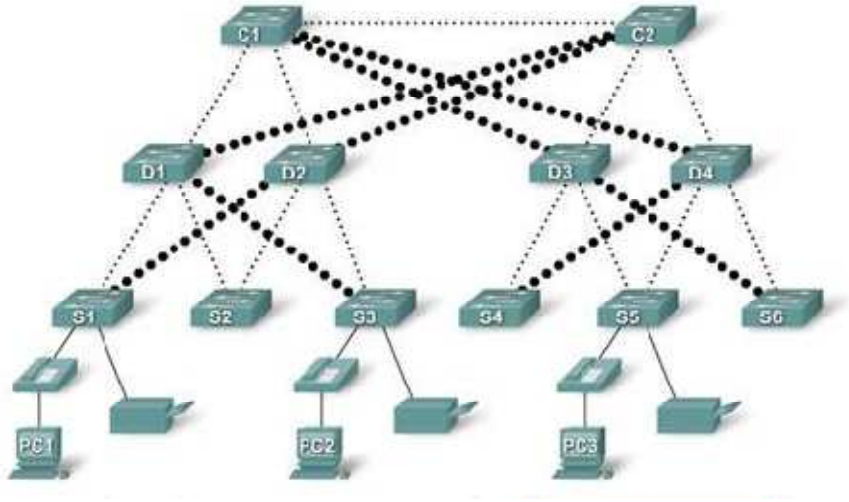


Figura II.24: Enlaces Redundantes

En la **Figura II.24**, los enlaces redundantes se observan en la capa de distribución y en la capa núcleo. En la capa de distribución existen dos switches de capa de distribución, el mínimo requerido para admitir redundancia en esta capa. Los switches de la capa de acceso, S1, S3, S4 y S6, se encuentran interconectados con los switches de la capa de distribución. Esto protege su red si falla uno de los switches de distribución. En caso de falla, el switch de la capa de acceso ajusta su ruta de transmisión y reenvía el tráfico a través del otro switch de distribución.

Ciertas situaciones de falla de la red nunca pueden impedirse, por ejemplo si la energía eléctrica se interrumpe en la ciudad entera o el edifico completo se derrumba debido a un terremoto.

Comience en la capa de acceso

Imagine que se requiere un diseño nuevo de redes. Los requisitos de diseño, como el nivel de rendimiento o la redundancia necesaria, están determinados por las metas comerciales de la organización. Una vez que se documentan los requisitos de diseño, el diseñador puede comenzar a seleccionar el equipo y la infraestructura para implementar el diseño.

Cuando se inicia la selección del equipo en la capa de acceso, puede asegurarse de que se adapta a todos los dispositivos de la red que necesitan acceso a la red. Después de tener en cuenta todos los dispositivos finales se tiene una mejor idea de cuántos switches de la capa de acceso se necesitan. El número de switches de la capa de acceso y el tráfico estimado que cada uno genera ayuda a determinar cuántos switches de la capa de distribución se necesitan para lograr el rendimiento y la redundancia necesarios para la red. Después de determinar el número de switches de la capa de distribución, se puede identificar cuántos switches de núcleo se necesitan para mantener el rendimiento de la red.

2.2.3.7 Diseño de una Gran Red de Campus

Las empresas que operan las redes universitarias son cada vez más grandes en busca de actualizaciones de infraestructura para:

- ✓ Manejar las aplicaciones de ancho de banda elevado, como voz, video, IP multicast y Mejorar la capacidad para compartir la red troncal de Ethernet o redes troncales del campus FDDI
- ✓ Soportar aplicaciones basadas en Novell IPX, DECnet, AppleTalk y SNA
- ✓ Ofrecer alta disponibilidad, rendimiento y facilidad de administración para la intranet de su empresa

Sugerencias de diseño

Use soluciones de Capa 2, Capa 3, o backbone ATM para ampliar su red de campus de gran tamaño. En los diseños típicos, los edificios o partes diferentes del campus se conectan entre sí a través de un alto rendimiento, conmutación de red troncal. La redundancia y alta disponibilidad de red se proporciona en cada capa. Una alta capacidad, la centralización de la granja de servidores proporciona recursos para el campus, y cuando se combina con Cisco IOS, la estrategia de

administración de red soporta calidad de servicio QoS, seguridad, solución de problemas, y otras características comunes de administración de extremo a extremo.

2.2.3.8 Diseño de una Red de Campus Mediana

Un campus mediano consiste en un gran edificio o varios edificios. La red de campus mediano está diseñada para alta disponibilidad, rendimiento y manejabilidad. Esto también es llamado “collapsed backbone” el diseño para las redes de campus mediana. Las necesidades adicionales de estos diseños suelen incluir:

- ✓ Alto rendimiento y disponibilidad para aplicaciones de ancho de banda como voz, video y multicast IP
- ✓ Ethernet compartidas o la construcción de red troncal FDDI que se está quedando sin capacidad.
- ✓ Soporte para aplicaciones basadas en Novell IPX, DECnet, AppleTalk y SNA Sobre la base de la arquitectura Cisco AVVID, estas plataformas de red inteligente y productos proporcionan la base para una solución de red completa.

Sugerencias de diseño

Esta solución de Cisco proporciona infraestructura conmutada manejable para una intranet del campus con más de mil dispositivos de red. El alto rendimiento de backbone colapsado utiliza tres capas de conmutación. La redundancia de red se proporciona a los clientes y servidores

2.2.3.9 Diseño de Red de Campus Pequeño

Las Redes de Campus pequeñas suelen estar contenidas dentro de un edificio. En la mayoría de los casos, la redundancia de la red no es la máxima prioridad, pero es la rentabilidad. Las necesidades adicionales de estos diseños suelen incluir:

- ✓ Alto rendimiento y disponibilidad para aplicaciones de ancho de banda como voz, video y multicast IP
- ✓ Ethernet compartidas o la construcción de red troncal FDDI que se está quedando sin capacidad.
- ✓ Soporte para aplicaciones basadas en Novell IPX, DECnet, AppleTalk y SNA

Sugerencias de diseño

La solución de Cisco proporciona un alto rendimiento infraestructura conmutada por una de tamaño intranet edificio con cientos de dispositivos de red. La columna vertebral de la red consiste en un interruptor de nivel 3. Capa de interruptores de acceso proporcionan conectividad con clientes y servidores. Software Cisco IOS soporta QoS, seguridad, solución de problemas y características comunes de gestión de extremo a extremo.

CAPITULO III

MARCO METODOLÓGICO E HIPOTÉTICO

3.1 DISEÑO DE LA INVESTIGACIÓN

El tipo de investigación aplicada para este trabajo, está basada en la investigación cuasi-experimental ya que los ambientes de pruebas y la información a transmitir en estos no serán tomados al azar, sino que están previamente establecidos y son los que a continuación se muestra en la **Tabla III.I**

Tabla III.I: Ambientes de prueba

AMBIENTE DE PRUEBAS	INFORMACIÓN A TRANSMITIR
LINUX	• ARCHIVOS PLANOS • ARCHIVOS MULTIMEDIA
CISCO	• ARCHIVOS PLANOS • ARCHIVOS MULTIMEDIA

3.2 TIPO DE ESTUDIO MÉTODOS, TÉCNICAS E INSTRUMENTOS

Para este proyecto se utilizarán los siguientes métodos de investigación.

Método Científico: Se utilizará este método ya que las ideas, conceptos, y teorías expuestas en este anteproyecto de tesis son verificables como válidos, además que servirá para recopilar la información necesaria de los protocolos que serán aplicados en los ambientes de prueba a ser planteados.
Las siguientes consideraciones fueron tomadas en cuenta para realizar esta investigación:

- ✓ Se plantea la investigación en base a la falta de una metodología que permita determinar el protocolo que brindará mayor disponibilidad y menor porcentaje de pérdida de datos en los ambientes cisco y Linux planteados anteriormente.
- ✓ Se plantean los objetivos de la investigación que permitirán resolver el problema de la falta de una metodología para determinar el protocolo que brindará mayor disponibilidad y menor porcentaje de pérdida de datos en los ambientes cisco y Linux planteados anteriormente

- ✓ Se justifica los motivos por los cuales se propone realizar la presente investigación.

- ✓ Se elabora un marco teórico que permita tener una visión general para la realización del trabajo.

- ✓ Se plantea una hipótesis la cual es una posible respuesta al problema planteado.

- ✓ Se propone la operacionalización de las variables en base a la hipótesis planteada

- ✓ Se realiza la recolección de datos de los índices e indicadores respectivos mediante las estadísticas de las interfaces de los equipos terminales.

- ✓ Se verifica la hipótesis con los resultados obtenidos.

- ✓ Se deducen las conclusiones y recomendaciones después de realizada la investigación.

Método Deductivo: mediante el completo estudio de los protocolos de alta disponibilidad de gateway se determinará la influencia de la implementación de estos para disminuir considerablemente el tiempo de standby de los servicios y la pérdida de datos en los equipos terminales de la red de campus.

Además se utilizará las técnicas que se detallan a continuación:

- ✓ Revisión Bibliográfica
- ✓ Pruebas
- ✓ Lluvia de ideas
- ✓ Recopilación de información.
- ✓ Y como fuentes de verificación se utilizarán:
- ✓ Información Bibliográfica y Linkográfica
- ✓ Transmisión de archivos

- ✓ Estadísticas de las Interfaces de los equipos clientes
- ✓ Simulación de los ambientes de prueba
- ✓ Analizador de tráfico
- ✓ Razonamiento

3.3 PLANTEAMIENTO DE LA HIPOTESIS

Con el análisis comparativo de los protocolos de alta disponibilidad de gateways en el diseño de redes de campus, el tiempo de standby de los servicios y el porcentaje de pérdida de datos disminuirán

3.4 DETERMINACION DE VARIABLES

Las variables de la investigación son aquellas propiedades o cualidades que se puede variar y dicha variación es susceptible de medición por medio de indicadores.
Esta investigación fundamenta su estudio basado en la manipulación de variables Dependientes e Independientes

Las Variables Independientes son aquellas que pueden ser observadas y manipuladas deliberadamente por el investigador.

Y las Variables Dependientes son consecuencia de la variable independiente, puede aparecer, desaparecer o modificarse

Basados en esta teoría hemos tomado las siguientes variables:

Variable Independiente

Implementación de los protocolos de alta disponibilidad de gateway en redes de campus

Variable Dependiente

Tiempo de standby

Porcentaje de pérdida de datos

La operacionalización conceptual y metodológica de las variables se muestra en la **Tabla III.II y Tabla III.III** respectivamente.

3.5 OPERACIÓN CONCEPTUAL DE LAS VARIABLES

Tabla III.II: Operacionalización conceptual de las variables del proyecto de investigación.

VARIABLE	TIPO	DEFINICION
Implementación de los protocolos de alta disponibilidad de gateway en redes de campus	**1.** Independiente	Los protocolos de alta disponibilidad 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 está disponible al intercambio de mensajes de hello entre los diferentes dispositivos adheridos al mismo gateway virtual.
Tiempo de standby	**2.** Dependiente	Disminución del tiempo de espera en recuperar los servicios.
Porcentaje de pérdida de datos	**3.** Dependiente	Es el porcentaje de paquetes perdidos durante la caída de un servicio

Fuente: Autoras

3.6 OPERACIÓN METODOLÓGICA DE LAS VARIABLES

Tabla III.III: Operacionalización metodológica de las variables del proyecto de investigación.

HIPÓTESIS	VARIABLES	INDICADORES	TECNICAS	FUENTES DE VERIFICACION
Con el análisis comparativo de los protocolos de alta disponibilidad de gateways en el diseño de redes de campus, el tiempo de standby de los servicios corporativos y el porcentaje de pérdida de datos disminuirán	**V. Independiente** Implementación de los protocolos de alta disponibilidad de gateway en redes de campus	**I1** Transferencia de archivos planos. **I2** Transferencia de archivos multimedia. **I3** Envio de paquetes ICMP (Ping)	4. Observación directa 5. Revisión Bibliográfica 6. Intuición 7. Pruebas	• Comportamiento de las aplicaciones • Información Bibliográfica y Linkográfica • Transmisión de archivos • Analizador de protocolos de red Wireshare
	V. Dependiente Tiempo de standby	**D1** Retardos de Transmisión	A. Observación Directa B. Pruebas	• Simulación de los ambientes de prueba • Analizador de de protocolos de red Wireshare • Software de medición de tiempo
	V. Dependiente Porcentaje de pérdida de datos	**D1** Cantidad de paquetes enviados y recibidos	A. Observación Directa B. Pruebas C. Recopilación de Información	• Simulación de los ambientes de prueba • Razonamiento

Fuente: Autoras

3.7 VALIDACIÓN DE INSTRUMENTOS

La validez de los instrumentos depende del grado en que se mide el dominio específico de las variables que intervienen en la investigación. Todo instrumento aplicado debe tener como característica fundamental: la validez y la confiabilidad. La validez se refiere al grado en que un instrumento realmente mide la variable que pretende medir.

Para la realización de pruebas se usarán las siguientes herramientas, las mismas que permitirán determinar la funcionalidad de los protocolos de alta disponibilidad al momento del falló del equipo master ya sea en su interfaz LAN o WAN.

3.7.1 PING

La primera herramienta utilizada para el monitoreo y captura de datos, en la transmisión de paquetes a través de las interfaces de los equipos conectados en el escenario es mediante el comando **ping dirección ip,** que permitirá calcular la pérdida de paquetes en la transmisión de archivos cuando , comando ampliamente utilizado por los administradores de red a nivel mundial por su confiabilidad y fácil uso ya que permite comprobar la conexión y perdida de paquetes en la transmisión como se observa en las **Figuras III.01, III.02, III.03, III.04, III.05, y III.06**.

Protocolo HSRP

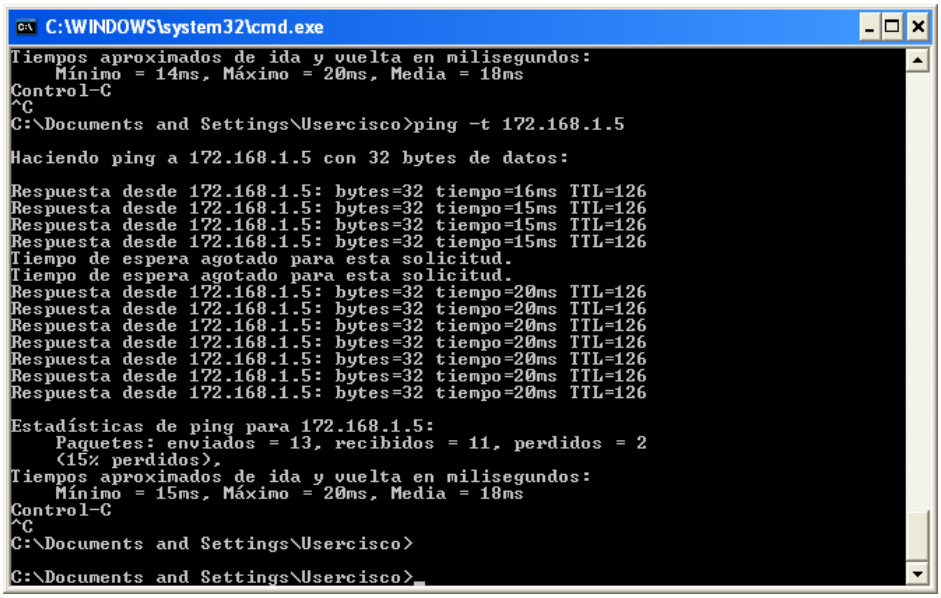


Figura III.01: Verificación de los paquetes perdidos desconectada al Lan

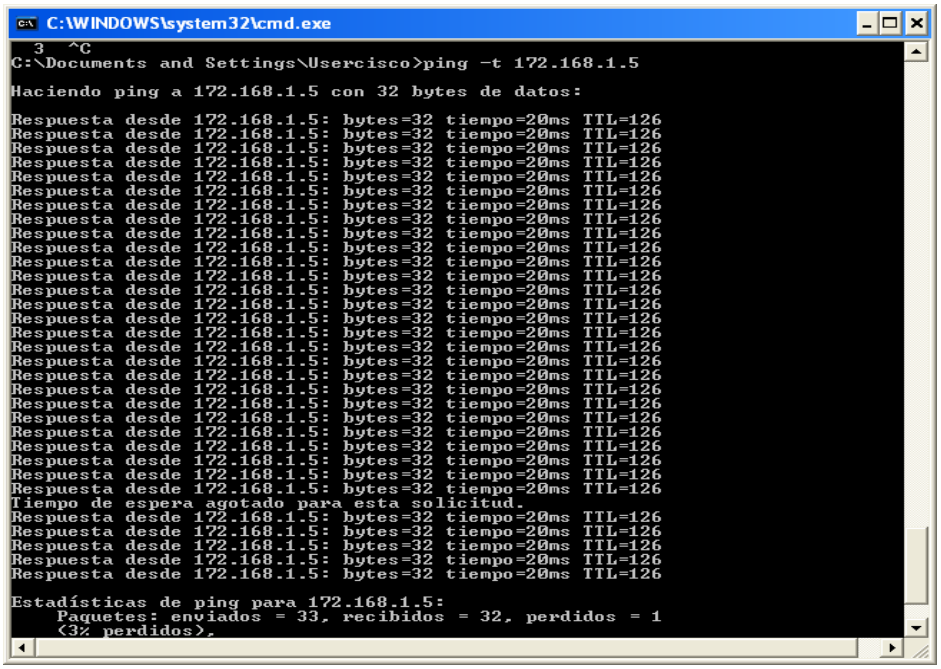


Figura III.02: Verificación de los paquetes perdidos desconectada al Wan

Protocolo GLBP

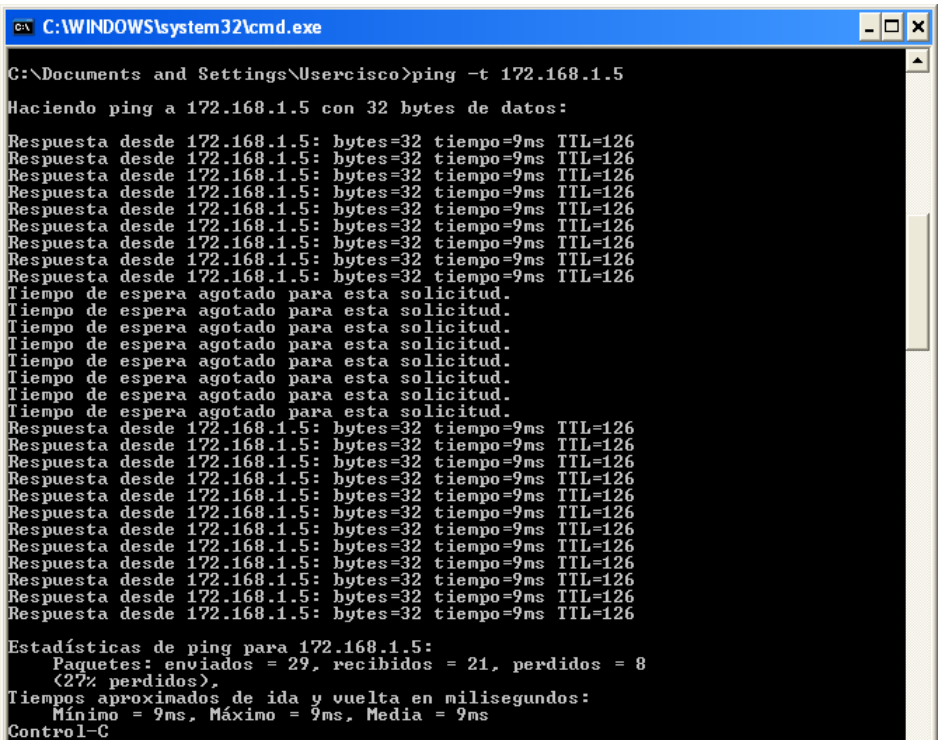


Figura III.03: Verificación de los paquetes perdidos desconectada la Lan

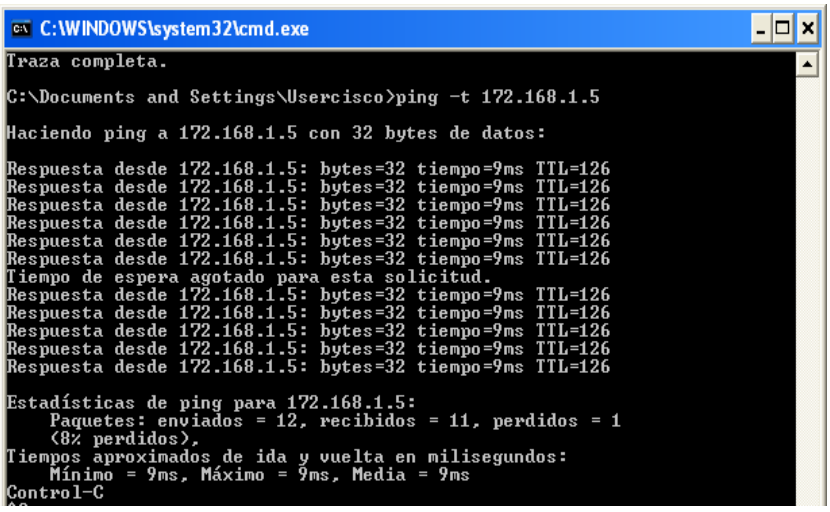


Figura III.04: Verificación de los paquetes perdidos desconectada la Wan

Protocolo VRRP

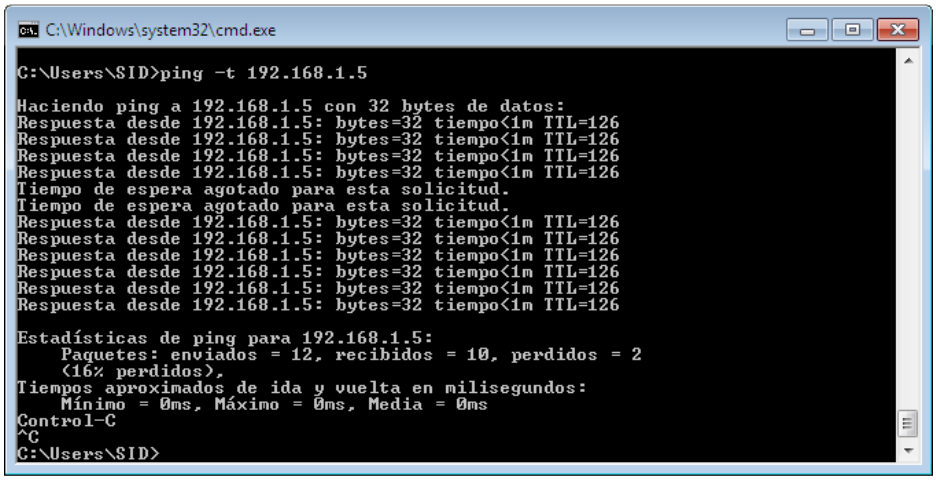


Figura III.05: Verificación de los paquetes perdidos desconectada la Lan

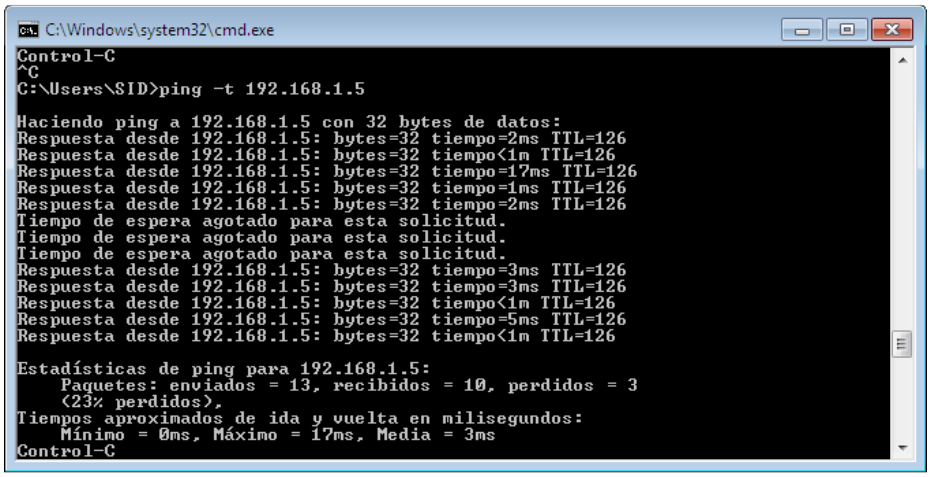


Figura III.06: Verificación de los paquetes perdidos desconectada la Wan

3.7.2 TRACERT

La segunda herramienta utilizada para el monitoreo, es mediante el comando **tracert dirección ip,** comando ampliamente utilizado para medir el tiempo que tarda un paquete en llegar desde un host (punto de red) a otro, el mismo que nos

que permitirá detallar los nodos por los que pasa el paquete de datos antes de llegar a los recursos del servidor, como se observa en las **Figuras III.07, III.08, III.09, III.10, III.11, y III.12**.

Protocolo HSRP

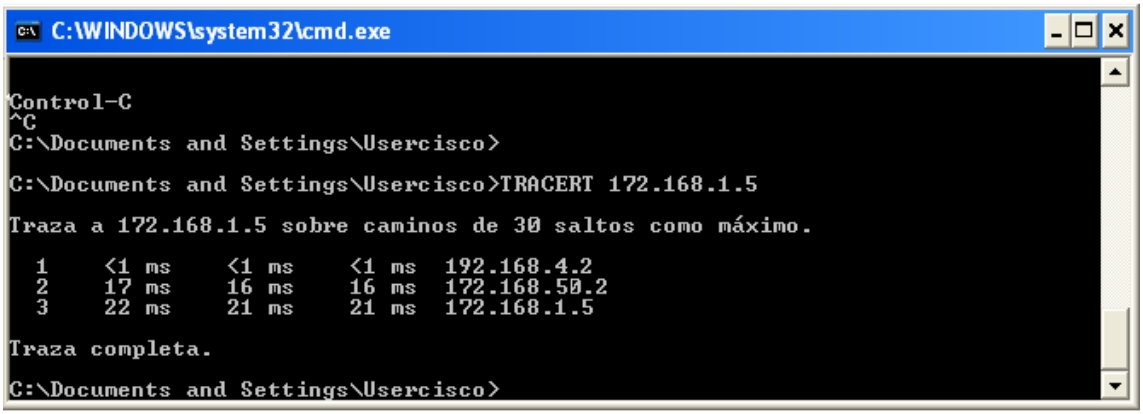


Figura III.07: Verificación de los nodos por los que pasa el paquete desconectada la Lan

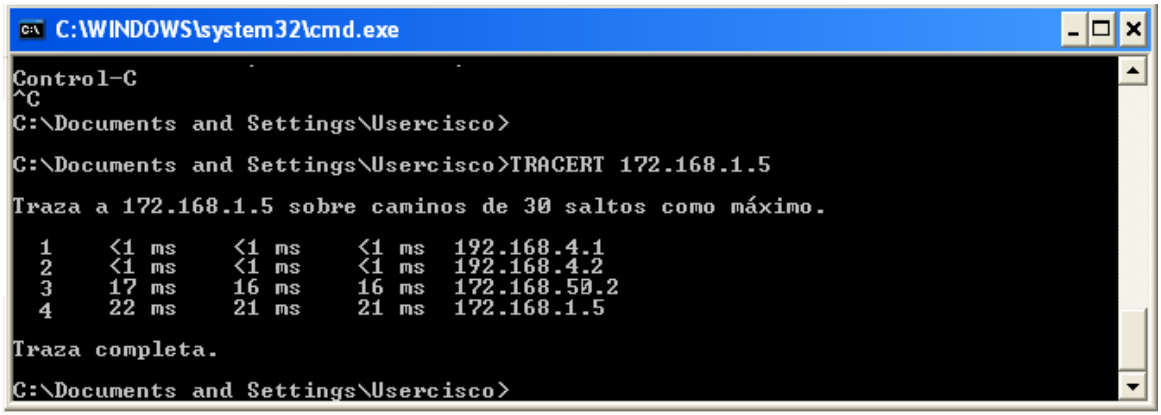


Figura III.0825: Verificación de los nodos por los que pasa el paquete desconectada la Wan

Protocolo GLBP

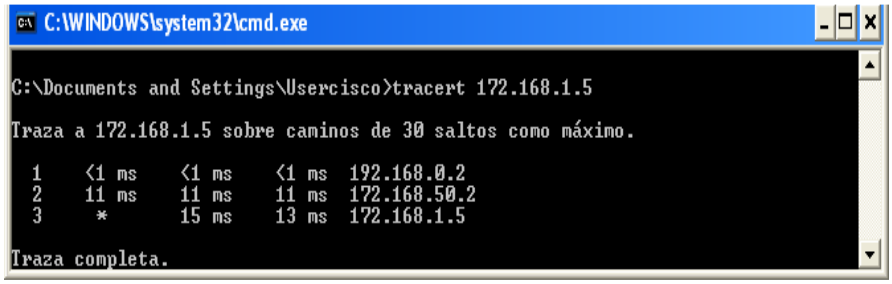


Figura III.09: Verificación de los nodos por los que pasa el paquete desconectada la Lan

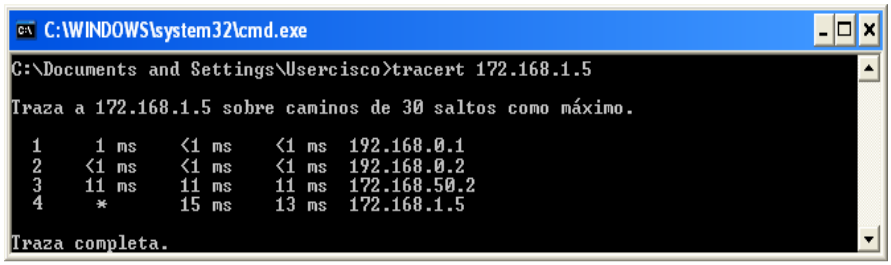


Figura III.1026: Verificación de los nodos por los que pasa el paquete desconectada la Wan

Protocolo VRRP

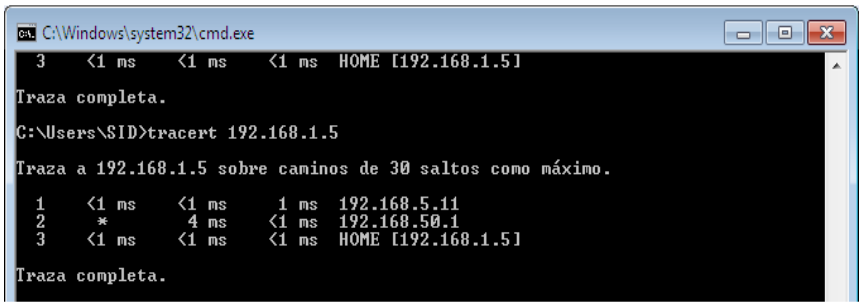


Figura III.1127: Verificación de los nodos por los que pasa el paquete desconectada la Lan

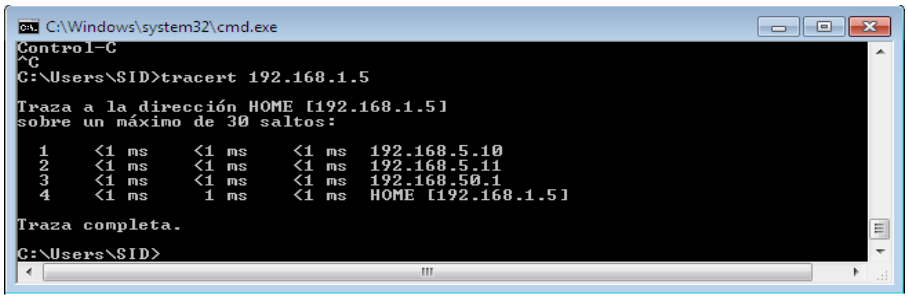


Figura III.12: Verificación de los nodos por los que pasa el paquete desconectada la Wan

3.7.3 FILEZILLA

La tercera herramienta utilizada para el monitoreo, es FileZilla la misma que fue usada para la transferencia de archivos desde un servidor a las computadoras locales de la red de campus y viceversa, la misma que permitirá determinar si la descarga de un archivo se reanuda al desconectar la Lan o la Wan de la red, como se muestra en las **Figuras III.13, III.14, III.15**.

Protocolo HSRP

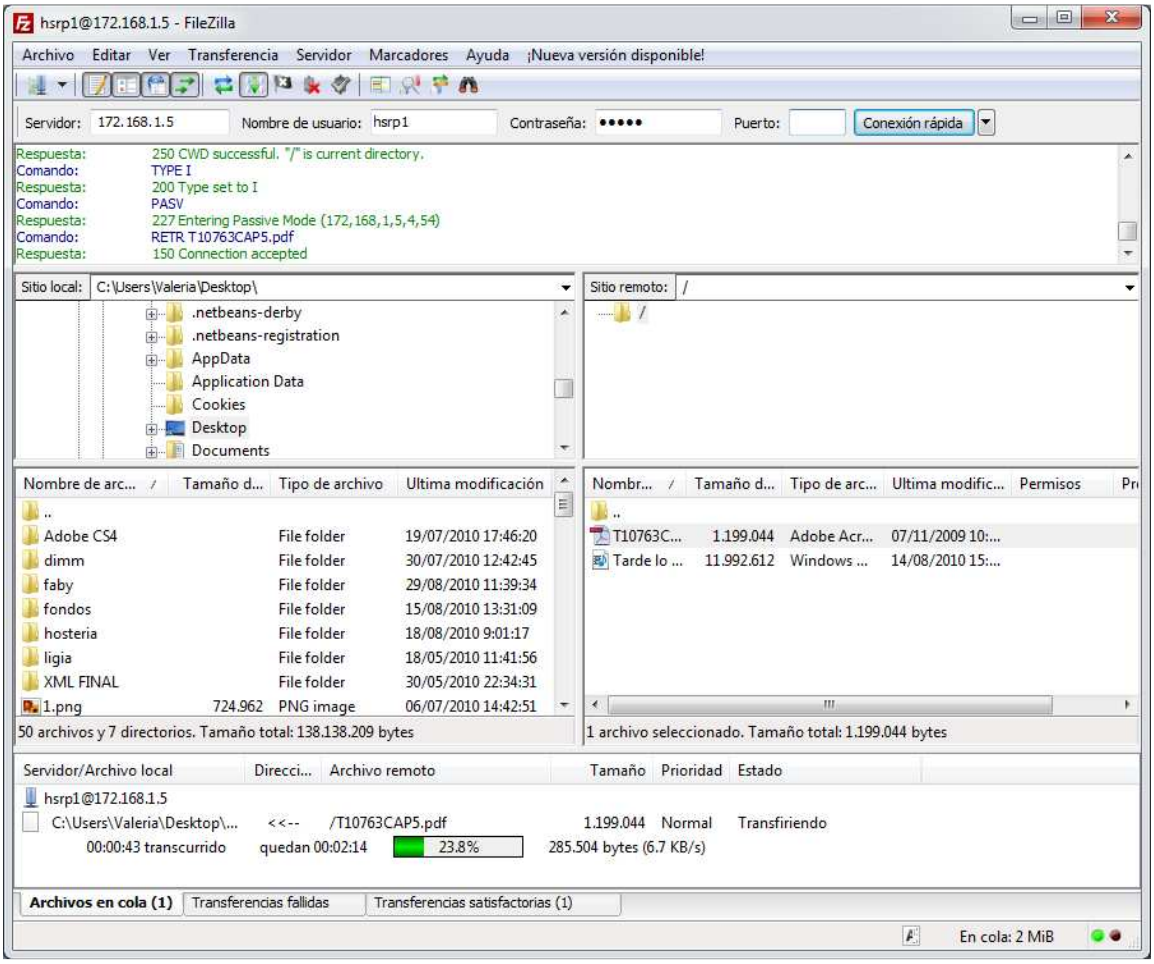


Figura III.13: Verificación de la transferencia de archivos en Hsrp.

Protocolo GLBP

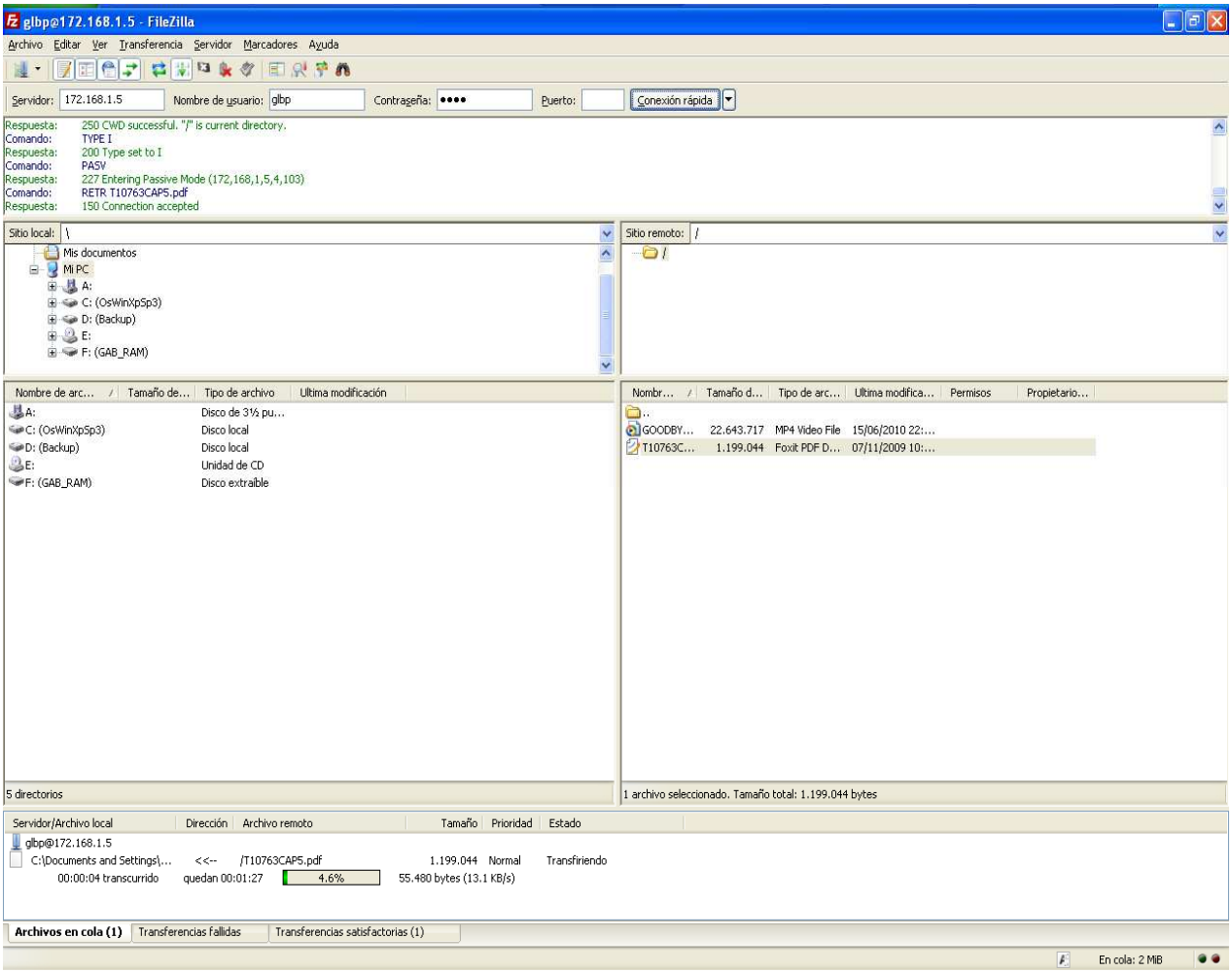


Figura III.14: Verificación de la transferencia de archivos en Glbp.

Protocolo VRRP

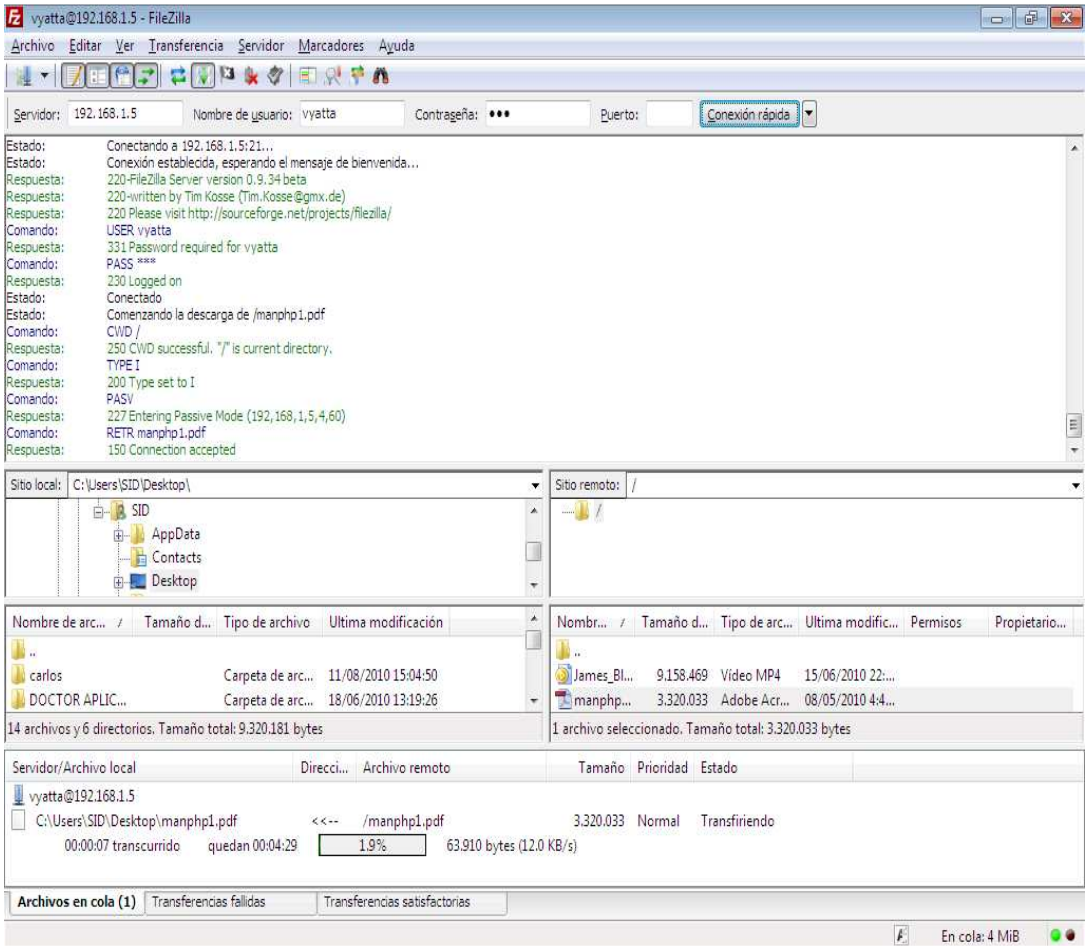


Figura III.15: Verificación de la transferencia de archivos en Vrrp.

3.7.4 WIRESHARK

La cuarta herramienta utilizada para el monitoreo, es WireShark un analizador de protocolos utilizado para el análisis y solución de problemas en redes de comunicaciones para desarrollo de software y protocolos, la misma que nos permitirá determinar el equipo master y el equipo backup de cada uno de los protocolos, así como su dirección multicast, como se muestra en las **Figuras III.16, III.17, III.18, III.19, III.20, y III.21**

Protocolo HSRP

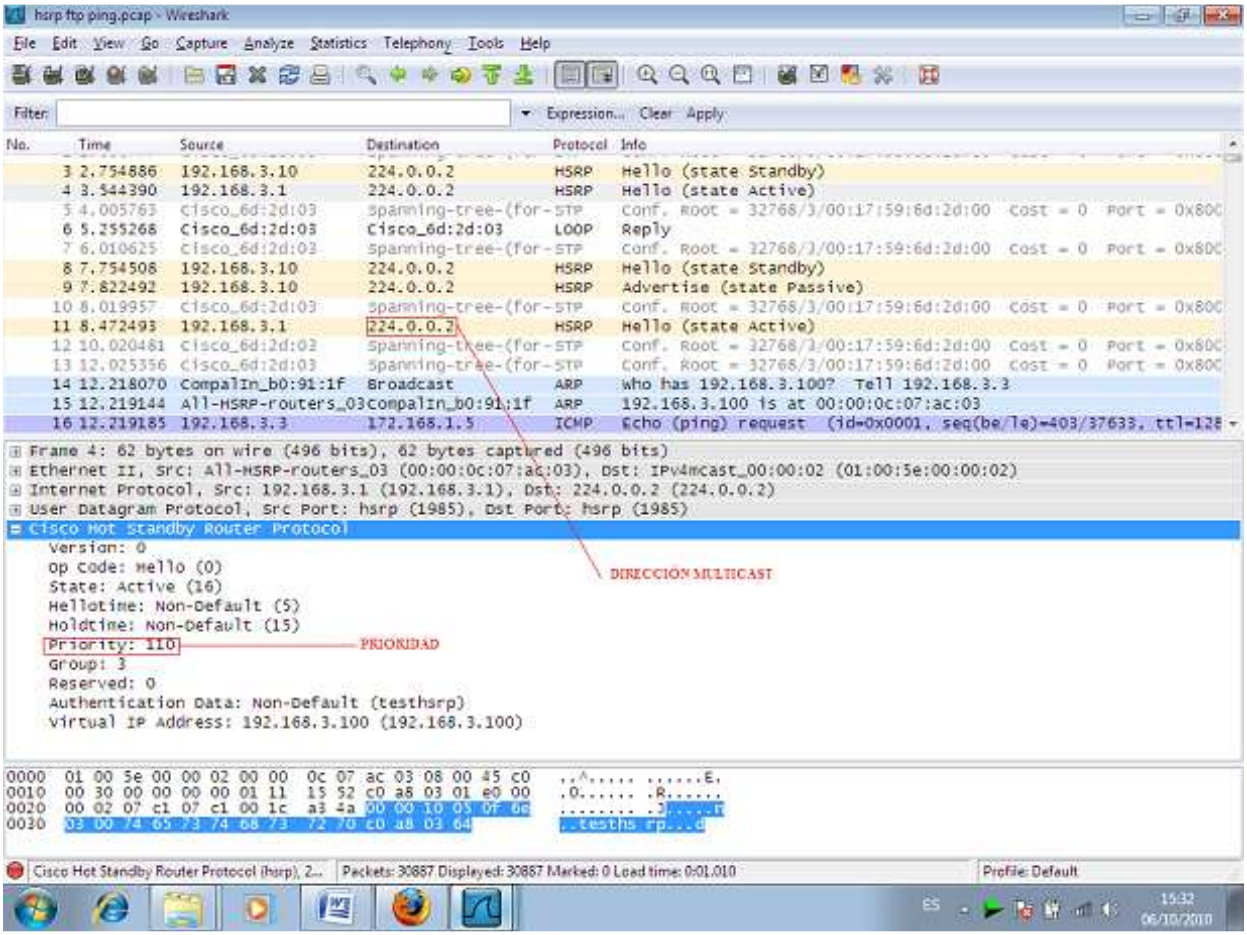


Figura III.16: Verificación de la dirección multicast (224.0.0.2) y la prioridad (110) del Master

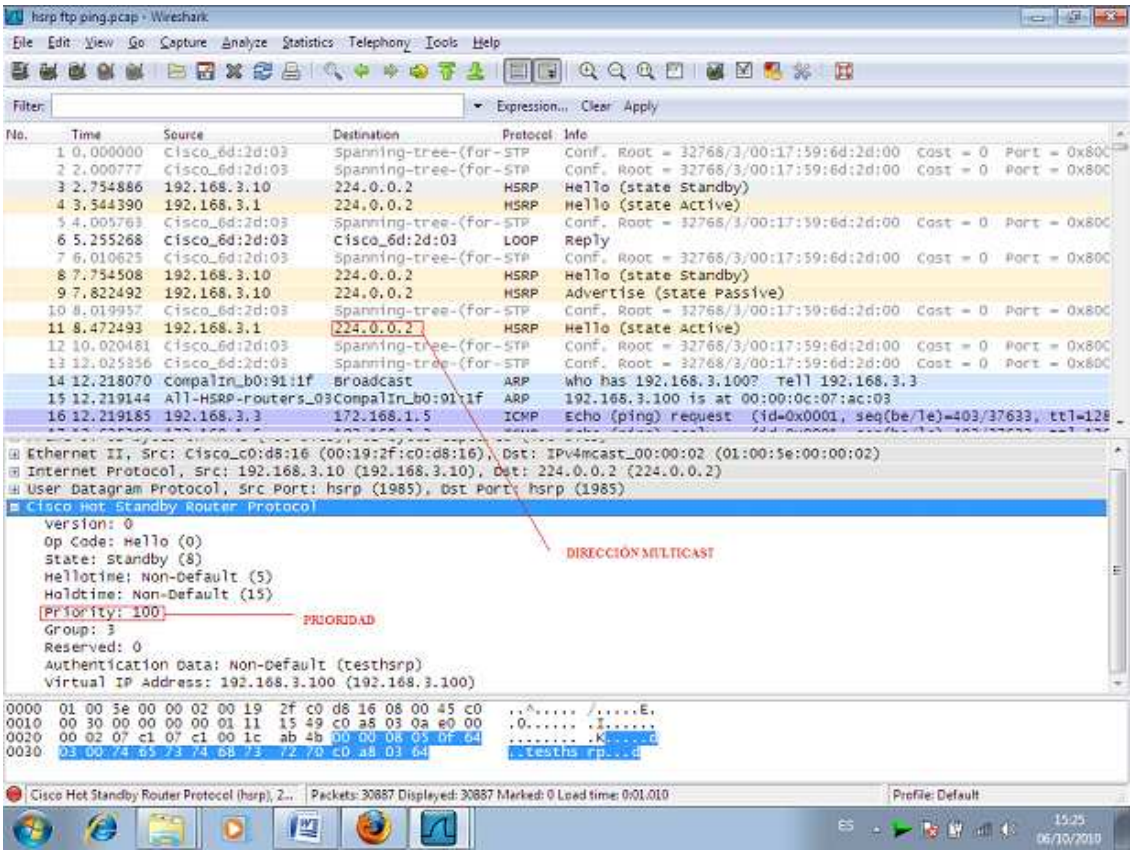


Figura III.17: Verificación de la dirección multicast (224.0.0.2) y la prioridad (100) del Backup

Protocolo GLBP

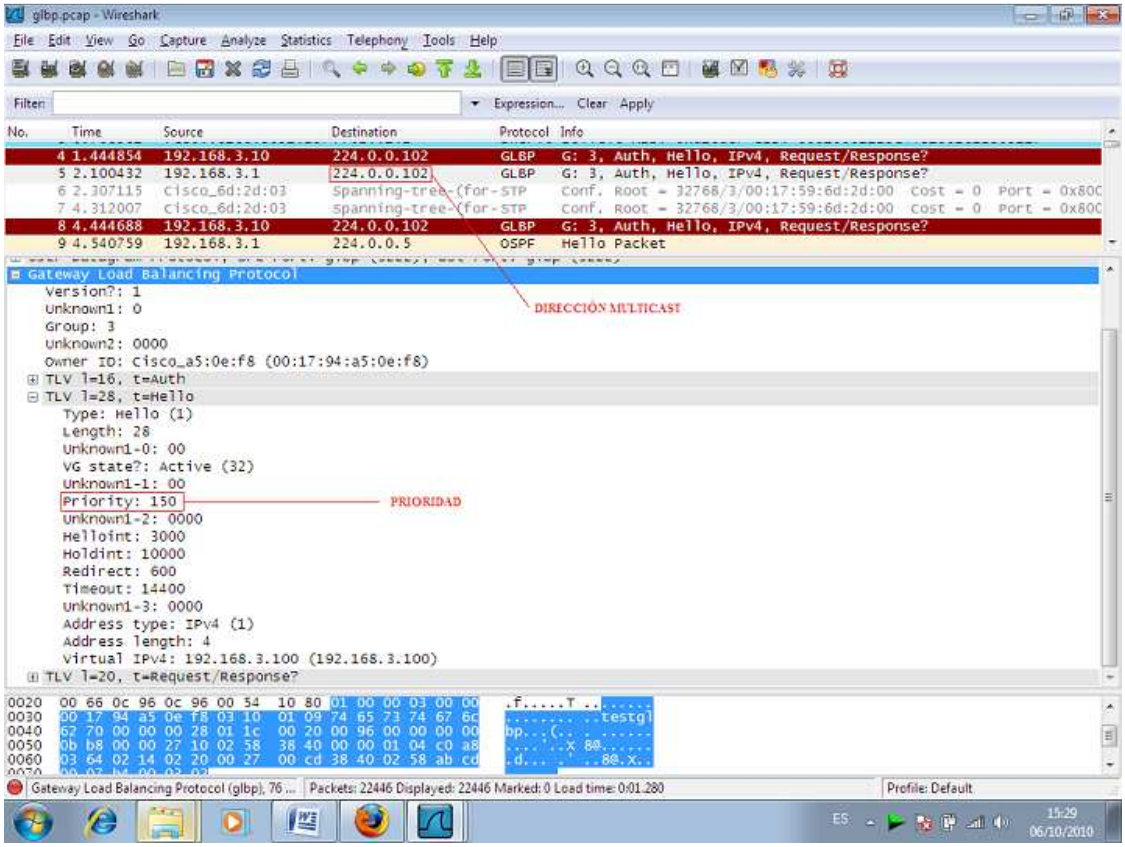


Figura III.18: Verificación de la dirección multicast (224.0.0.102) y la prioridad (150) Master

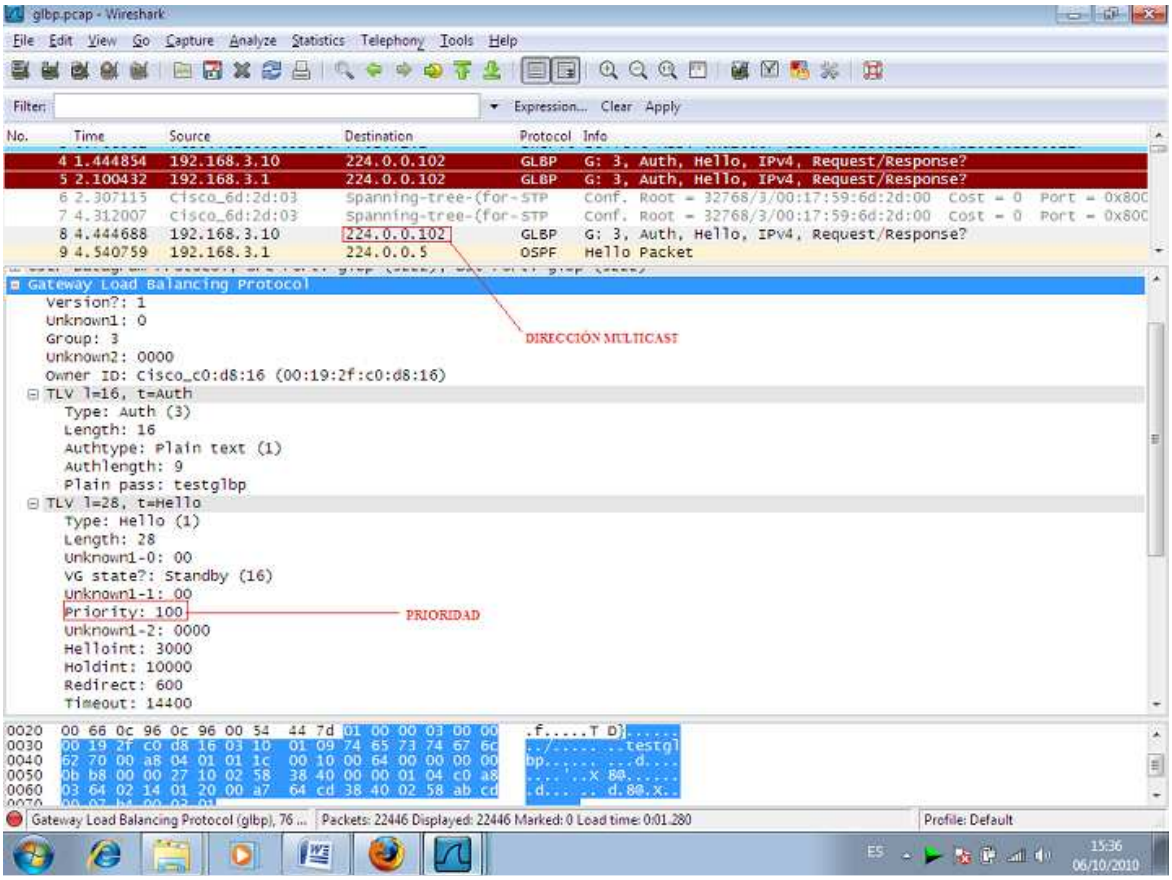


Figura III.19: Verificación de la dirección multicast (224.0.0.102) y la prioridad (100) Backup

Protocolo VRRP

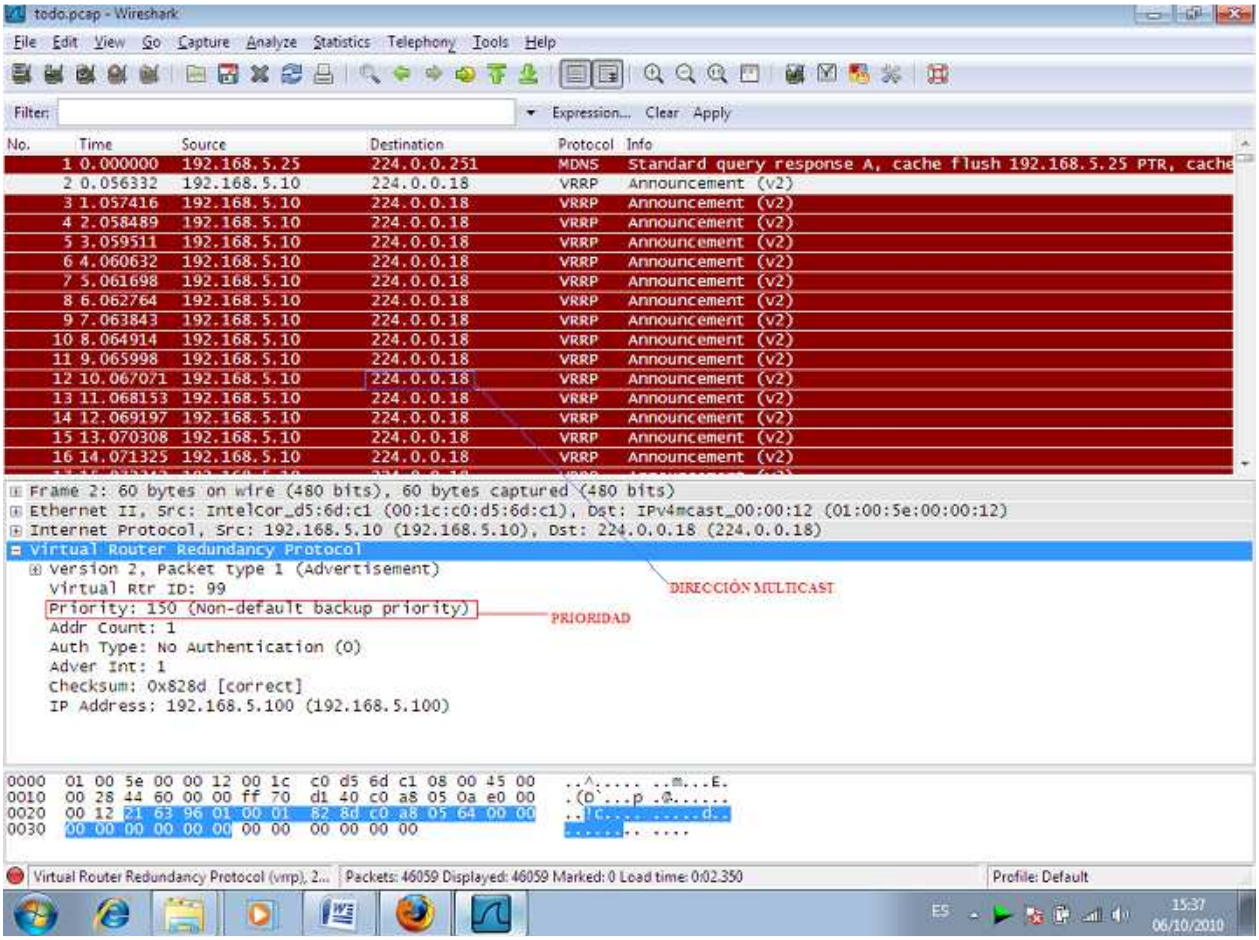


Figura III.20: Verificación de la dirección multicast (224.0.0.18) y la prioridad (150) Master

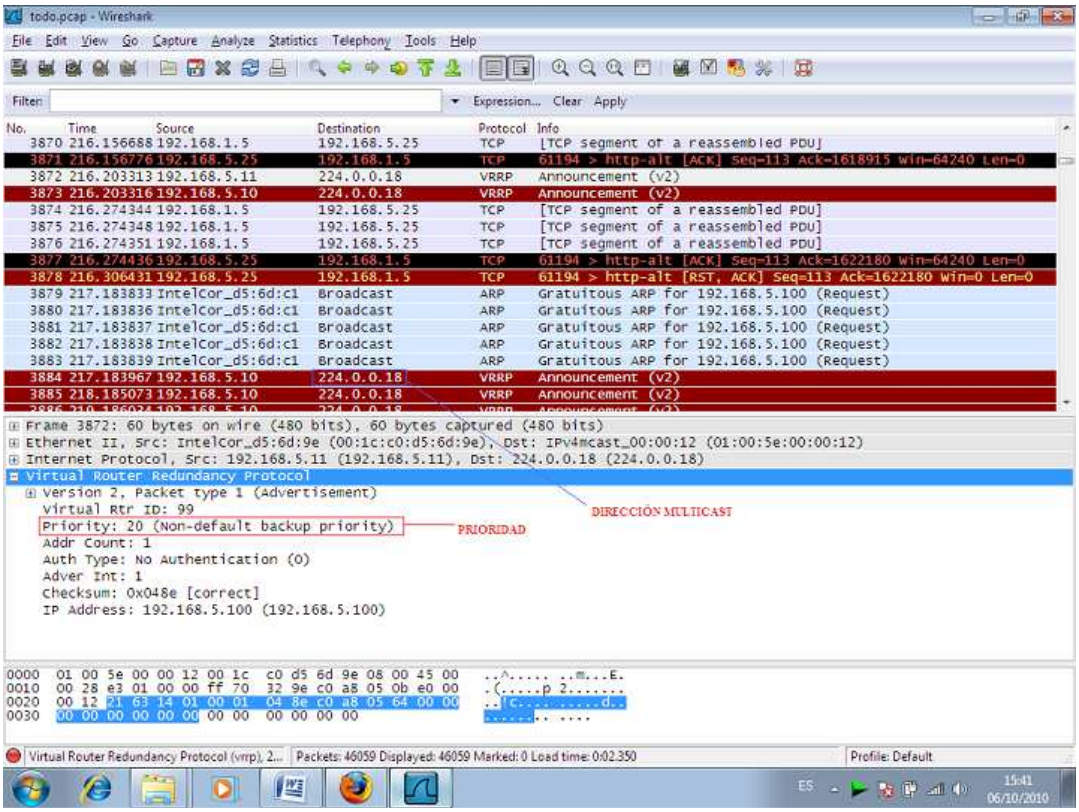


Figura III.21: Verificación de la dirección multicast (224.0.0.18) y la prioridad (150) Master

3.8 POBLACIÓN Y MUESTRA

La población es el conjunto de todos los elementos a ser evaluados y en nuestro caso de estudio está compuesta por los 2 escenarios de pruebas a analizar que son:

- ✓ Ambientes Linux,
- ✓ Ambientes CISCO

La muestra tomada para el presente trabajo de investigación está conformada por los tipos de archivos que serán transmitidos en los ambientes de pruebas establecidos.

- ✓ Archivos Planos,

- ✓ Paquetes ICMP

Se escogieron este tipo de archivos debido a que nos permiten determinar de manera clara cuantos paquetes se pierden con cada uno de los protocolos en el caso de paquetes ICMP, y en el caso de archivos planos para la transferencia, si esta se reanuda después de un cierto tiempo.

3.9 TÉCNICAS DE COMPROBACIÓN DE HIPOTESIS

Para la comprobación de la hipótesis planteada se utilizará una técnica de análisis no paramétrico; La prueba de significancia no paramétrica más popular en la investigación social se conoce como Chi cuadrada (X^2). Como veremos, la prueba se usa para hacer comparaciones entre dos muestras.

El test de chi–cuadrado (X^2) contrasta los resultados observados en una investigación con un conjunto de resultados teóricos, estos últimos calculados bajo el supuesto que las variables fueran independientes. La diferencia entre los resultados observados y esperados se resume en el valor que adopta el estadístico X^2, el cual tiene asociado un valor -p, por debajo del cual se acepta o rechaza la hipótesis de independencia de las variables. De esta forma, al someter los resultados de una investigación al test de chi–cuadrado (X^2) el investigador puede afirmar si dos variables en estudio están asociadas o bien son independientes una de la otra, afirmación que cuenta con un sustento estadístico en base al valor comparado con los definidos en la tabla de chi cuadrado ver Anexo 1.

La fórmula para el cálculo del test de chi cuadrado es la siguiente:

$$X^2 = \sum \frac{(f_0 - f_e)^2}{f_e}$$

Donde, fo (Frecuencia Observada) y fe (frecuencia esperada)

CAPITULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1 PROCESAMIENTO DE INFORMACIÓN

Para la obtención de los valores cuantitativos de cada uno de los indicadores de la variable dependiente, se implementó un escenario de simulación con routers cisco y con routers Linux, sobre el cual se transmitieron tráfico en tiempo real mediante Video LAN y FileZilla.

El escenario de simulación que se utilizó para la transmisión de tráfico en tiempo real para determinar el mejor de los protocolos en cada uno de los ambientes es:

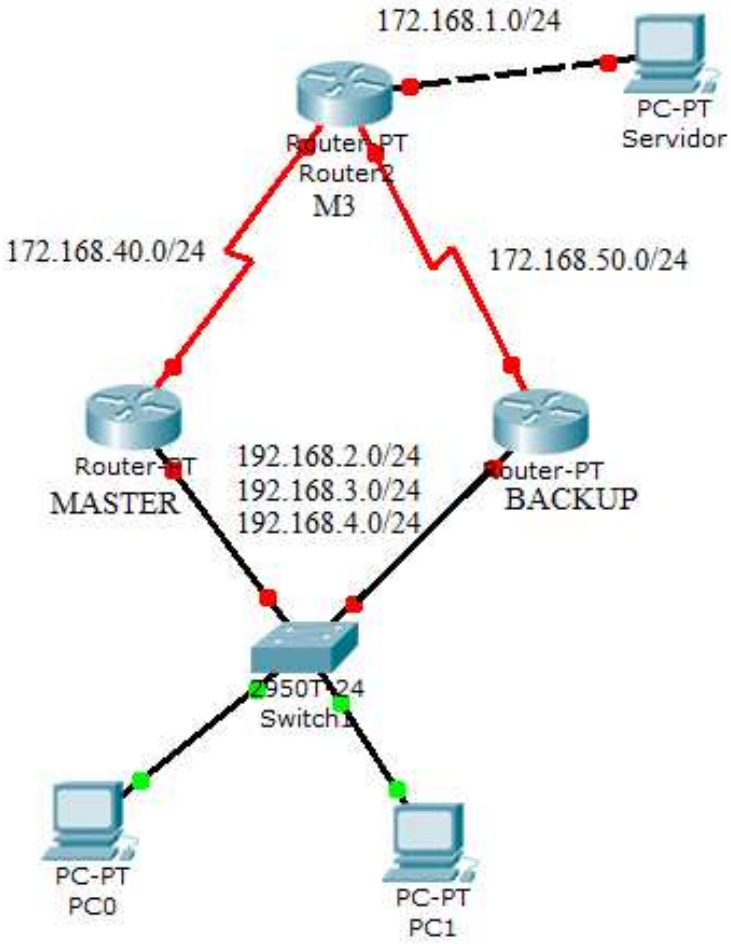


Figura IV.01: Escenario de prueba Cisco y Linux

El detalle de los equipos y software utilizados en el escenario propuesto se describe a continuación en las **Tablas IV.I, IV.II Y IV.III**:

HARDWARE

Tabla IV.I: Hardware utilizado en el escenario de pruebas en el ambiente Cisco

EQUIPOS	**DETALLE**	**DETALLE**
3 Routers Cisco 2800	ROUTER 1 =Máster	1 Interfaces Serial – 1 Interfaz Ethernet
	ROUTER 2 = Backup	1 Interfaz Serial – 1 Interfaz Ethernet
	ROUTER 3 = M3	2 Interfaces Seriales – 1 Interfaz Ethernet
1 Switch Catalyst 2950	SWITCH 1 = Switch	6 Interfaces FastEthernet (2 interfaces para track y 4 para vlans)
2 Cables Seriales DTE		
2 Cables Seriales DCE		
4 Cables Cruzados		
2 Cables Directos		
4 PCS	PC1 = SERVIDOR	Servidor de Archivos FTP
	PC2 – PC3 – PC4= MONITOREO	Maquinas Clientes conectadas respectivamente al switch

Fuente: Autoras

Tabla IV.II: Hardware utilizado en el escenario de pruebas en el ambiente Linux

EQUIPOS	DETALLE	DETALLE
3 Routers Vyatta (Linux)	PC1 = Máster	2 Interfaces FastEthernet
	PC2 = Backup	2 Interfaces FastEthernet
	PC3 = Router	3 Interfaces FastEthernet
1 Switch TPLINK	SWITCH NO ADMINISTRABLE	4 Interfaces FastEthernet
2 Cables Cruzados		
4 Cables Directos		
4 PCS	PC4 = SERVIDOR	Servidor de Archivos FTP y Video LAN
	PC5 – PC6 = MONITOREO	Maquinas Clientes conectadas respectivamente al Switch

Fuente: Autoras

SOFTWARE

Tabla IV.III: Software utilizado para la transmisión de información

PROGRAMAS	DETALLE	DETALLE
FTP	FILEZILLA	Es una aplicación diseñada para trabajar como servidor de ficheros FTP. Los servidores FTP, brindan acceso directo a ficheros, con la posibilidad de descargar su contenido de una manera más rápida.
	WIRESHARK	Es una utilidad que nos permite verificar el trafico que pasa a través de la red.
VIDEO LAN	VLC	Tiene la capacidad de transmitir datos streaming a través de redes.

Fuente: Autoras

El plan de direccionamiento diseñado para el escenario propuesto de pruebas se describe en la **Tabla IV.IV**

Tabla IV.IV: Direccionamiento utilizado en los equipos de prueba.

EQUIPOS	**DIRECCION IP**	**MASCARA**	**DEFAULT GATEWAY**
	172.168.1.0	255.255.255.0	
	172.168.40.0	255.255.255.0	
	172.168.50.0	255.255.255.0	
	192.168.2.0	255.255.255.0	
	192.168.3.0	255.255.255.0	
	192.168.4.0	255.255.255.0	
	172.168.1.5	255.255.255.0	172.168.1.1
	192.168.3.3	255.255.255.0	192.168.3.100
	192.168.4.4	255.255.255.0	192.168.4.100

Fuente: Autoras

4.2 DETERMINAR LOS INDICADORES.

Para el análisis de las variables dependientes planteadas en el presente trabajo de investigación, se consideró el estudio de dos indicadores que nos permitieron evaluar y comprobar que el tiempo de standby de los servicios y el porcentaje de pérdida de datos disminuirán.

Los indicadores que se plantearon para la investigación son:

- ✓ Indicador 1 para la Variable Tiempo de Standby: **Retardos de Transmisión (D1)**

- ✓ Indicador 2 para la Variable Porcentaje de Pérdida de datos: **Cantidad de Paquetes enviados y recibidos (D2)**

Estos indicadores fueron evaluados para cada uno de los protocolos de alta disponibilidad de gateway: HSRP, GLBP Y VRRP.

4.3 ANÁLISIS DEL TIEMPO DE STANDBY DE LOS SERVICIO MEDIANTE LOS PROTOCOLOS HSRP, GLBP Y VRRP

4.3.1 I1: TRANSFERENCIA DE ARCHIVOS PLANOS

Para la transmisión de Archivos planos se utilizó el servició FTP. Una vez realizadas las respectivas configuraciones de interfaces y ruteo, se procedió a instalar el software FileZilla Server en el computador que trabajó como Servidor Ftp y en cada cliente se ejecutó el FileZilla Client el cual permite copiar archivos de cualquier tipo, disponibles del servidor, los clientes se conectaron al servidor FTP que tenia previamente un archivo pdf y un video mp4 que se desea descargar por cada cliente simultáneamente. En nuestro caso el tamaño del archivo pdf 3,16 MB y del video mp4 21,5MB.

Cada cliente se conecta al servidor cuya dirección IP es: 172.16.1.5; Usuario: hsrp y Contraseña: hsrp en el protocolo HSRP, en el protocolo GLBP Usuario: glbp y Contraseña: glbp, y en el VRRP, Usuario: vrrp y Contraseña: vrrp

4.3.1.1 D1: RETARDOS DE TRANSMISIÓN

PROTOCOLO HSRP

Los resultados obtenidos para el retardo de transmisión que se presenta en cada uno de los clientes se muestran en la **Tabla IV.V.**

Tabla IV.V: Retardos de transmisión HSRP

CLIENTES	RETARDOS DE TRANSMISIÓN (ms)				$\bar{x}$
PC2	LAN(1,4)	13,9	9,3	12,6	11,9
	LAN(3,10)	13,5	12,8	14,5	13,6
	LAN(5,15)	24,6	25,2	23,1	24,3
	WAN(1,4)	8,4	9,3	7,5	8,4
	WAN(3,10)	8,8	8,7	8,5	8,7
	WAN(5,15)	9,3	8,6	8,9	8,9
PC3	LAN(1,4)	14,2	9,8	13,7	12,6
	LAN(3,10)	12,5	12,8	13,2	12,9
	LAN(5,15)	22,6	24,4	23,1	23,4
	WAN(1,4)	8,7	8,5	7,3	8,0
	WAN(3,10)	8,7	8,9	8,6	8,7
	WAN(5,15)	10,3	8,1	9,4	9,4
PROMEDIO DE LOS CLIENTES	LAN(1,4)	11,9	12,6		12,2
	LAN(3,10)	13,6	12,9		13,3
	LAN(5,15)	24,3	23,4		23,9
	WAN(1,4)	8,4	8,0		8,2
	WAN(3,10)	8,7	8,7		8,7
	WAN(5,15)	8,9	9,4		9,2

Fuente: Autoras

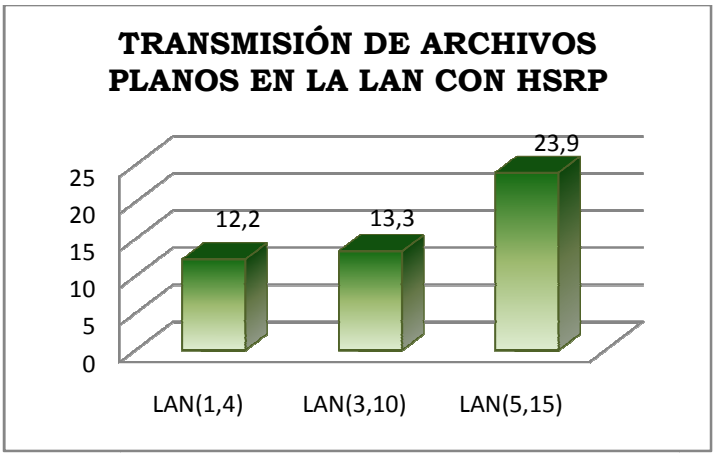


Figura IV.02: Retardos de Transmisión en la LAN (ms)

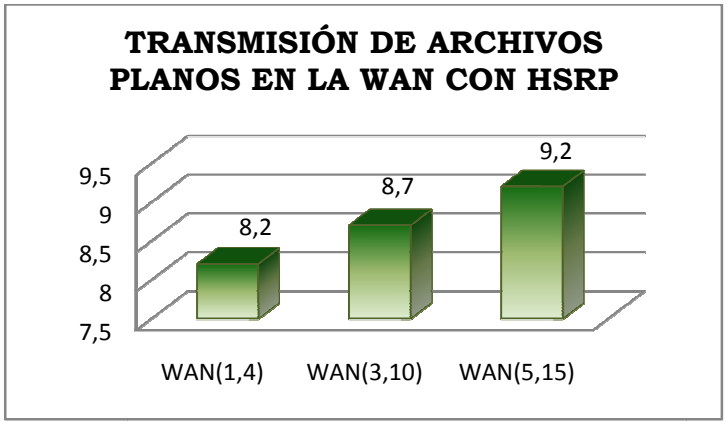


Figura IV.03: Retardos de Transmisión en la WAN (ms)

El menor retardo en la transmisión de archivos planos en la Lan es 12,3ms y en la Wan 8,2ms debido a que los tiempos de hellotime y de holdtime son menores. **Figura IV.02** y **Figura IV.03**

PROTOCOLO GLBP

El tiempo de retardo en la transmisión de archivos planos mediante Filezilla en GLBP no se pudo obtener debido a que la conexión nunca se pierde al momento de transferir un archivo aunque se desconecte la LAN o la WAN ya que existe balanceo de carga.

PROTOCOLO VRRP

Los resultados obtenidos para el retardo de transmisión que se presenta en un cliente se muestran en la **Tabla IV.VI**

Tabla IV.VI: Retardos de transmisión VRRP

PC2	LAN	18,5
	WAN	15,8

Fuente: Autoras

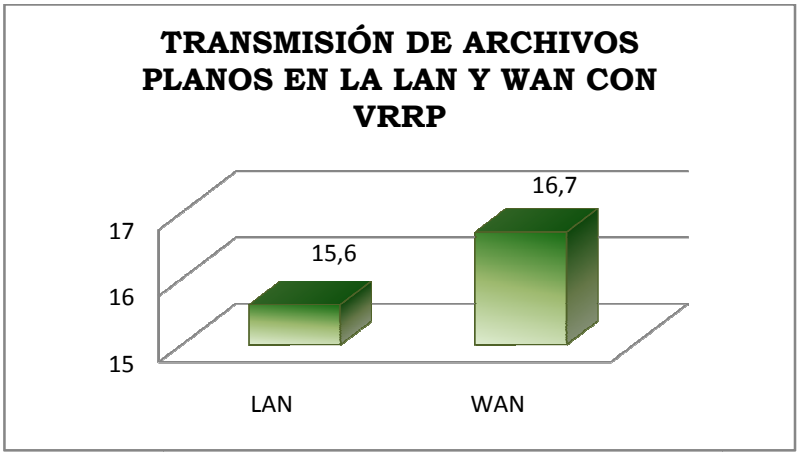


Figura IV.04: Retardos de Transmisión en la LAN y WAN (ms)

El menor retardo en la transmisión de archivos planos es en la WAN debido a que es aquí cuando se recupera más rápido la transmisión de archivos porque encuentra más rápido el otro camino. **Figura IV.04**

4.3.2 I2: TRANSFERENCIA DE ARCHIVOS MULTIMEDIA

Para la transmisión de archivos multimedia se utilizó la opción de video LAN como el VLC, el mismo que solo se probó con el protocolo VRRP, debido a que en HSRP y GLBP el video se transmite pero con baja calidad.

Para que se pueda realizar una transmisión con una buena calidad de video en lo equipos Cisco, es necesario controlar el uso compartido de los recursos de la red para satisfacer los requisitos de cada servicio. Una solución es usar calidad de servicio (QoS) es decir, hacer que los enrutadores y los conmutadores de red funcionen de maneras distintas para cada tipo de servicio (voz, datos y vídeo) del tráfico de la red. Al utilizar la Calidad de servicio (QoS), distintas aplicaciones de red pueden coexistir en la misma red sin consumir cada una el ancho de banda de las otras.

4.3.2.1 D1: RETARDO EN LA TRANSMISIÓN

PROTOCOLO VRRP

Los resultados obtenidos para el retardo de transmisión que se presenta en un cliente se muestran en la **Tabla IV.VII**

Tabla IV.VII: Retardos de transmisión VRRP

CLIENTE					
PC2	LAN	13,9	14,7	18,2	15,6
	WAN	12,8	21,8	15,6	16,7

Fuente: Autoras

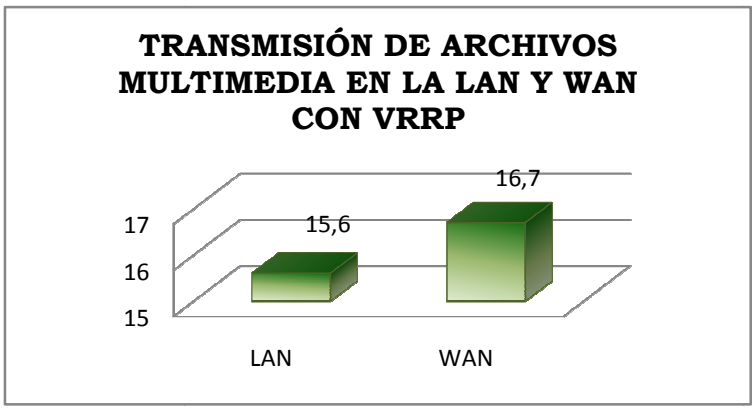


Figura IV.05: Retardos de Transmisión en la LAN y WAN (ms)

El menor retardo en la transmisión de archivos multimedia es en la LAN debido a que el video se recupera de manera rápida ya que gracias al gateway recorre un camino más corto. **Figura IV.05**

4.3.3 I3: ENVIO DE PAQUETES ICMP

Para comprobar el tiempo de standby mediante envió de paquetes ICMP se usan los mensajes del ping, los mismos que envían mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un Router o host no puede ser localizado, además usaremos el ping para determinar cuántos paquetes han sido enviados y cuantos han sido recibidos.

4.3.3.1 D1: RETARDO EN LA TRANSMISIÓN

PROTOCOLO HSRP

Los resultados obtenidos para el retardo de transmisión que se presenta en los clientes se muestran en la **Tabla IV.VIII.**

Tabla IV.VIII1: Retardos de transmisión HSRP

CLIENTES	**RETARDOS DE TRANSMISIÓN (ms)**				$\bar{x}$
PC2	LAN(1,4)	5,6	5,4	5,2	5,4
	LAN(3,10)	10,5	10,2	10,1	10,3
	LAN(5,15)	14,2	13,3	11,2	12,9
	WAN(1,4)	5,2	5,3	4,6	4,8
	WAN(3,10)	5,4	5,5	4,8	4,9
	WAN(5,15)	4,3	4,2	5,5	4,7

PC3	LAN(1,4)	4,2	5,1	4,6	4,6
	LAN(3,10)	8,8	9,2	8,8	8,9
	LAN(5,15)	14,2	14,4	14,5	14,4
	WAN(1,4)	5,4	4,6	5,7	4,1
	WAN(3,10)	5,4	5,7	6,2	4,6
	WAN(5,15)	3,9	4,8	5,4	4,7
PROMEDIO DE LOS CLIENTES	LAN(1,4)	5,4	4,6		5,0
	LAN(3,10)	10,3	8,9		9,6
	LAN(5,15)	12,9	14,4		13,7
	WAN(1,4)	4,8	4,1		4,5
	WAN(3,10)	4,9	4,6		4,8
	WAN(5,15)	4,7	4,7		4,7

Fuente: Autoras

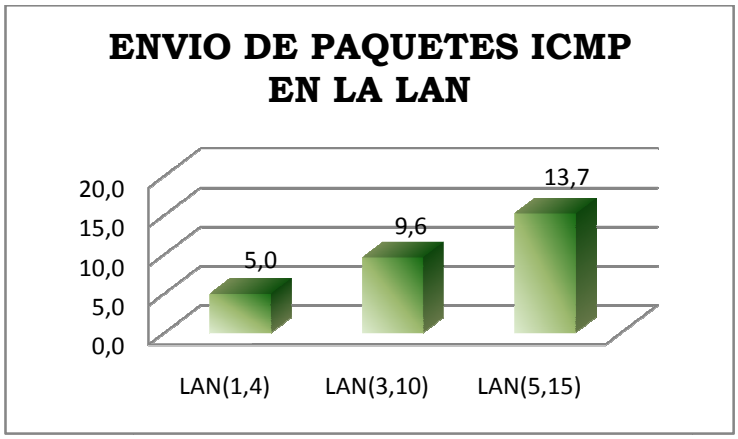


Figura IV.06: Retardos de Transmisión en la LAN (ms)

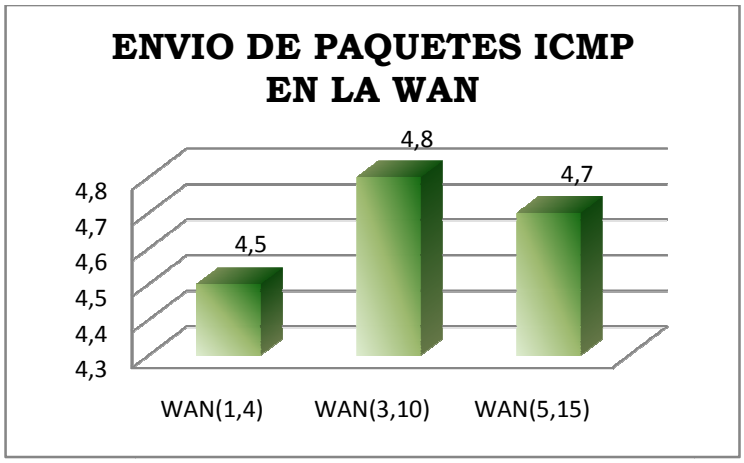


Figura IV.07: Retardos de Transmisión en la WAN (ms)

El menor retardo en la transmisión de mensajes icmp es de 5,0 ms en la LAN en la WAN de 4,5ms ya que aquí el hellotime y el holdtime son menores, es decir 1 y 4 segundos respectivamente. **Figura IV.06** y **Figura IV.07**

PROTOCOLO GLBP

Los resultados obtenidos para el retardo de transmisión que se presenta en los clientes se muestran en la **Tabla IV.IX.**

Tabla IV.IX2: Retardos de transmisión GLBP

CLIENTES	**RETARDOS DE TRANSMISIÓN (ms)**				
PC2	LAN(1,4)	8.9	9,8	10,8	6,9
	LAN(3,10)	10,9	12,1	12,8	11,9
	LAN(5,15)	14,4	14,2	17,6	15,4
	WAN(1,4)	5,2	5,3	4,6	5,0
	WAN(3,10)	4,4	5,5	5,4	5,1

	WAN(5,15)	5,8	5,8	6,4	6,0
PC3	LAN(1,4)	10,9	9,7	11,2	10,6
	LAN(3,10)	10,6	10,3	10,7	10,5
	LAN(5,15)	15,6	12,1	14,7	14,1
	WAN(1,4)	5,4	4,6	5,1	5,0
	WAN(3,10)	7,3	5,7	6,8	6,6
	WAN(5,15)	6,3	6,5	6,8	6,5
PROMEDIO DE LOS CLIENTES	LAN(1,4)	6,9	10,6		8,8
	LAN(3,10)	11,9	10,5		11,2
	LAN(5,15)	15,4	14,1		14,8
	WAN(1,4)	5,0	5,0		5,0
	WAN(3,10)	5,1	6,6		5,9
	WAN(5,15)	6,0	6,5		6,3

Fuente: Autoras

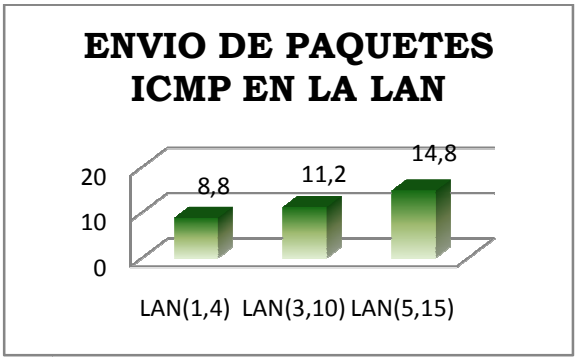


Figura IV.08: Retardos de Transmisión en la LAN (ms)

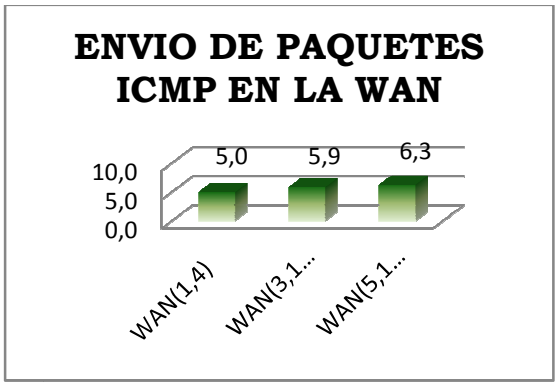


Figura IV.0928: Retardos de Transmisión en la WAN (ms)

El menor retardo en la transmisión de mensajes icmp es de 8,8ms en la LAN y de 5,0ms en la WAN debido a que aquí el tiempo de hellotime y el de holdtime es el menor, es decir 1 y 4 segundos respectivamente. **Figura IV.08** y **Figura IV.09**

PROTOCOLO VRRP

Los resultados obtenidos para el retardo de transmisión que se presenta en un cliente se muestran en la **Tabla IV.X.**

Tabla IV.X3: Retardos de transmisión VRRP

CLIENTE					
PC2	LAN	13,3	18,5	17,2	16,3
	WAN	36,3	46,9	39,4	40,9

Fuente: Autoras

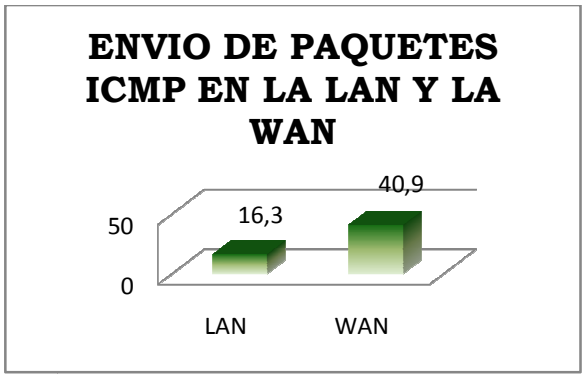


Figura IV.10: Retardos de Transmisión en la LAN y WAN (ms)

El menor retardo en la transmisión de mensajes icmp es en la LAN con un tiempo de 16,3ms. **Figura IV.10**

4.3.3.2 D2: CANTIDAD DE PAQUETES ENVIADOS Y RECIBIDOS

Para el análisis de la cantidad de paquetes enviados y recibidos se usa el ping, el mismo que en las estadísticas nos muestra los resultados, y se analizado en cada uno de los protocolos.

PROTOCOLO HSRP

Los resultados obtenidos en la cantidad de paquetes enviados y recibidos que se presenta en los clientes se muestran en la **Tabla IV.XI.**

Tabla IV.XI4: Cantidad de paquetes perdidos en HSRP

CLIENTE				
PC2	LAN(1,4)	LAN(3,10)	LAN(5,15)	
	1	2	3	2
	WAN(1,4)	WAN(3,10)	WAN(5,15)	
	1	1	2	1

Fuente: Autoras

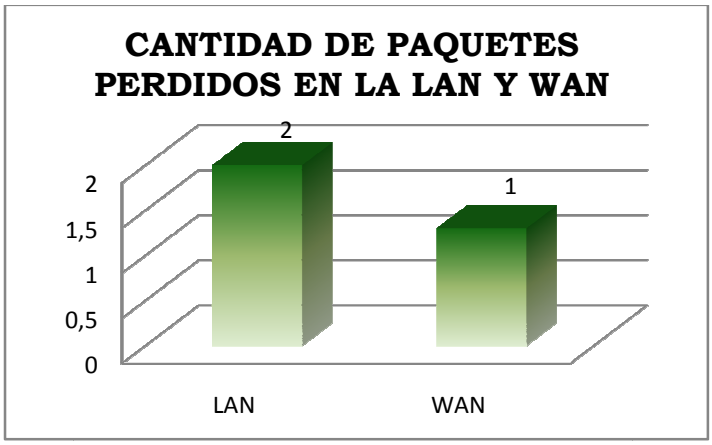


Figura IV.11: Cantidad de paquetes perdidos en la LAN y WAN (ms)

La menor pérdida de paquetes es en la WAN debido a que es aquí donde se configura un track serial el mismo que le indica por donde debe ir, en cambio en la LAN debe establecerse cuál es el máster y cuál es el backup por este motivo se demora en llegar y pierde más paquetes. **Figura IV.11**

PROTOCOLO GLBP

Los resultados obtenidos en la cantidad de paquetes enviados y recibidos que se presenta en los clientes se muestran en la **Tabla IV.XII**

Tabla IV.XII5: Cantidad de paquetes perdidos en GLBP

CLIENTE				
PC2	LAN(1,4)	LAN(3,10)	LAN(5,15)	
	2	2	3	2
	WAN(1,4)	WAN(3,10)	WAN(5,15)	
	1	2	3	2

Fuente: Autoras

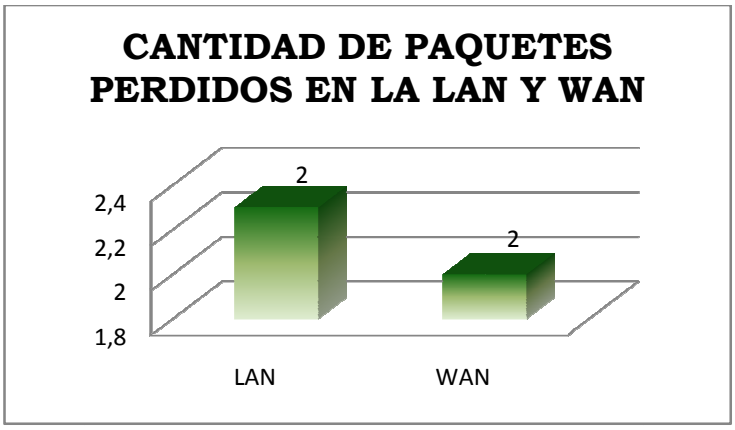


Figura IV.12: Cantidad de paquetes perdidos en la LAN y WAN (ms)

La menor pérdida de paquetes es en la WAN debido a que es aquí donde se configura un track serial el mismo que le indica por donde debe ir, en cambio en la LAN debe establecerse cuál es el máster y cuál es el backup por este motivo se demora en llegar y pierde más paquetes, al igual que en HSRP. **Figura IV.12**

PROTOCOLO VRRP

Los resultados obtenidos en la cantidad de paquetes enviados y recibidos que se presenta en los clientes se muestran en la **Tabla IV.XIII**.

Tabla IV.XIII6: Cantidad de paquetes perdidos en VRRP

CLIENTES				
	PC2	**PC3**	**PC4**	
LAN	2	3	2	2,3
WAN	8	2	3	4,3

Fuente: Autoras

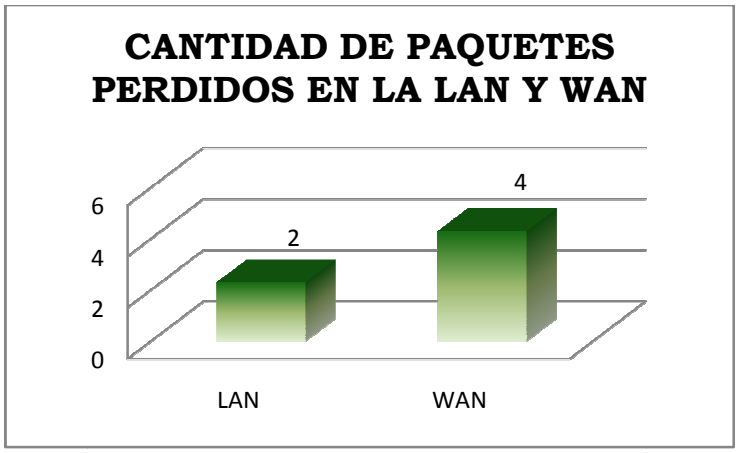


Figura IV.13: Cantidad de paquetes perdidos en la LAN y WAN (ms)

La menor pérdida de paquetes es en la LAN debido a que al configurar vrrp en Vyatta se lo hace a través de las PCs, es decir al desconectar la WAN se demora en encontrar la ruta. **Figura IV.13**

4.4 ANÁLISIS COMPARATIVO DE LOS INDICADORES POR ESCENARIOS

Luego de realizar el análisis individual de cada uno de los indicadores de los escenarios de prueba, se procedió a realizar un análisis comparativo de estos indicadores entre el escenario de transmisión CISCO frente al escenario de transmisión LINUX, para determinar y evaluar el mejoramiento en la transmisión de la información.

4.4.1 D1: RETARDOS EN LA TRANSMISIÓN

Los datos usados para la comparación de este indicador en los tres escenarios evaluados se muestran en la **Tabla IV.XIV**

Tabla IV.XIV7: Retardos en la transmisión en los escenarios de pruebas

PROTOCOLOS	HSRP	GLBP
LAN(1,4)	5,0	8,8
LAN(3,10)	9,6	11.2
LAN(5,15)	13,7	14,8
WAN(1,4)	4,5	5,0
WAN(3,10)	4,8	5,9
WAN(5,15)	4,7	6,3

Fuente: Autoras

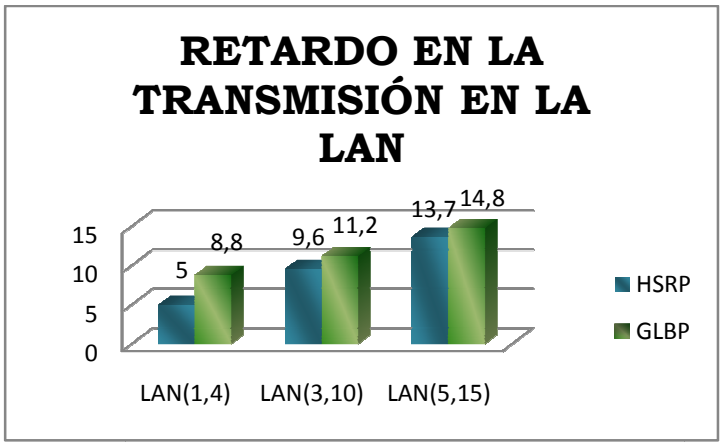


Figura IV.14: Retardo en la transmisión de mensajes ICMP

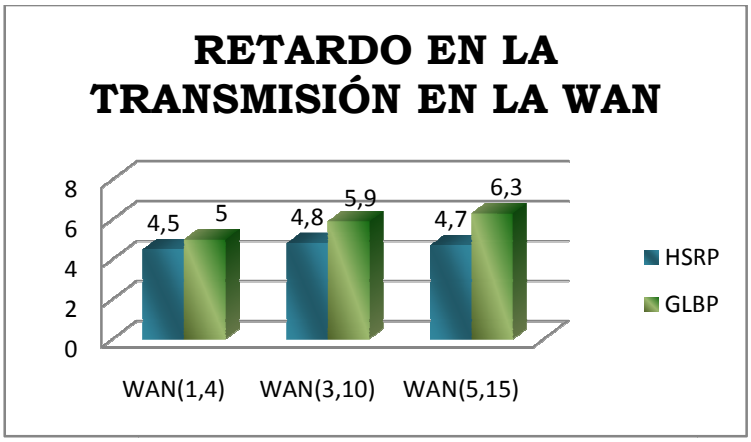


Figura IV.15: Retardo en la transmisión de mensajes ICMP

Como se puede observar tanto en la **Figura IV.14** y en la **Figura IV.15** el retardo en la transmisión es menor en HSRP, esto lo pudimos observar a través del envio de paquetes ICMP en el ambiente CISCO.

PROTOCOLO VRRP

Los resultados obtenidos para el retardo de transmisión que se presenta en el protocolo vrrp al enviar mensajes ICMP, se muestra en la **Tabla IV.XV**

Tabla IV.XV: Retardos de transmisión VRRP

VRRP	
LAN	16,3
WAN	40,9

Fuente: Autoras

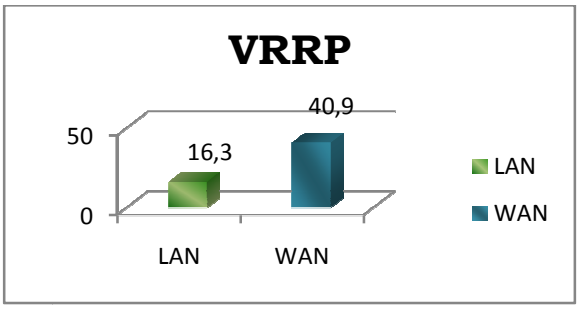


Figura IV.16: Retardos de Transmisión de mensajes ICMP

Como se puede observar en la **Figura IV.16** el retardo en la transmisión es menor en la LAN, esto lo pudimos observar a través del envío de paquetes ICMP en el ambiente LINUX.

4.4.2 D2: CANTIDAD DE PAQUETES ENVIADOS Y RECIBIDOS

Los datos usados para la comparación de este indicador en los tres escenarios evaluados se muestran en la **Tabla IV.XVI**

Tabla IV.XVI: Cantidad de paquetes perdidos en los escenarios de pruebas

PROTOCOLOS	HSRP	GLBP
LAN	2	2
WAN	1	2

Fuente: Autoras

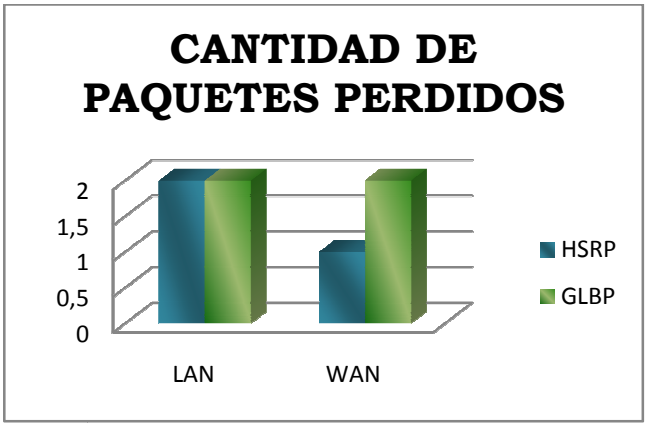


Figura IV.1729: Cantidad de paquetes perdidos

Como se puede observar tanto en la **Figura IV.17** la menor perdida de paquetes es en la Wan de GLBP debido a que aquí se realiza automáticamente balanceo de carga, esto lo pudimos observar a través del envío de paquetes ICMP en el ambiente CISCO.

PROTOCOLO VRRP

Los resultados obtenidos para los paquetes perdidos en el protocolo vrrp al enviar mensajes ICMP, se muestra en la **Tabla IV.XVII**.

Tabla IV.XVII8: Cantidad de paquetes perdidos

VRRP	
LAN	2
WAN	4

Fuente: Autoras

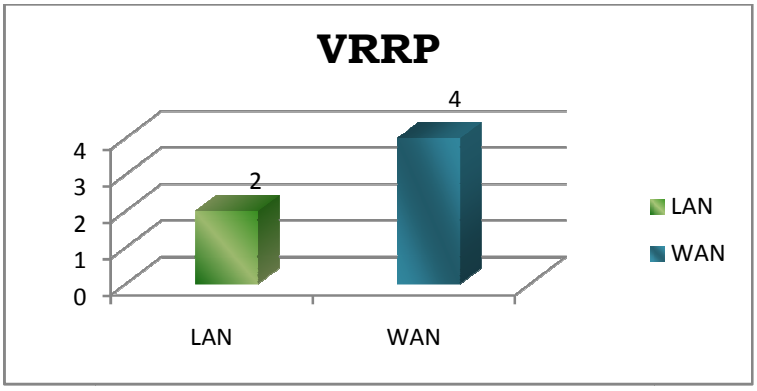


Figura IV.18: Cantidad de paquetes perdidos en la Lan yWan

Como podemos observar en la **Figura IV.18** la mayor cantidad de paquetes perdidos es en la Wan debido a que aquí se hace ruteo, esto lo pudimos observar a través del envío de paquetes ICMP en el ambiente LINUX.

4.5 COMPROBACION DE LA HIPOTESIS

Luego de haber realizado todas las pruebas se procedió a efectuar los cálculos para la comprobación de la hipótesis planteada en base a los resultados obtenidos en cada indicador, para esto se empleó la prueba del ji (chi-cuadrado) o X2.

Las hipótesis a considerar son:

Hipótesis Nula Ho: Con el análisis comparativo de los protocolos de alta disponibilidad de gateways en el diseño de redes de campus, el tiempo de standby de los servicios y el porcentaje de pérdida de datos no disminuirán.

.

Hipótesis de la investigación Hi: Con el análisis comparativo de los protocolos de alta disponibilidad de gateways en el diseño de redes de campus, el tiempo de standby de los servicios y el porcentaje de pérdida de datos disminuirán.

4.5.1 PRUEBA DE X2 - ESCENARIO CON HSRP CONTRA SIN ALTA DISPONIBILIDAD

En base a los resultados obtenidos en el apartados (4.4) se construyó las tablas de contingencias considerando la variable independiente: Implementación de los protocolos de alta disponibilidad de gateway en redes de campus y la variable dependiente: Tiempo de standby y Porcentaje de pérdida de datos

Donde la frecuencia observada está relacionada con el tiempo que se demora en reactivarse una red es decir 50 segundos sin incluir el tiempo que el usuario debe tomarse para llegar al punto donde debe arreglar la red y las frecuencias esperadas son relacionadas con los valores para Hsrp, Glbp y Vrrp. Con los cuales se crean las tablas de contingencias.

Posteriormente se procedió a construir la tabla de aplicación de la formula de Chi cuadrado, donde fo es la frecuencia observada y fe es la frecuencia esperada variables utilizadas para el cálculo de X 2 y determinar si su valor es o no significativo, determinando los grados de libertad (GL), aplicando la fórmula que se muestra a continuación:

GL = (f-1)(c-1)

Donde **f** es el número de filas de la tabla de contingencia y el **c** el número de columnas: por lo tanto el grado de libertad para la variable es:

GL = (6-1)(2-1)
GL = 5

Y el nivel de significancia con el cual se trabajó en la prueba de la hipótesis es de

α = 0,1.

Por lo cual la comprobación de cada resultado se debe comparar el valor de X^2 calculado y el que se encuentra analizando en la tabla que se muestra en el Anexo 1. Si el valor de x^2 calculado es menor que el valor de X^2 tabulado, se acepta la hipótesis nula y se rechaza la hipótesis de investigación.

Con **α** = 0,1 y 5 grados de libertad tenemos que para nuestra investigación el valor de x^2 tabulado es de 9,236.

En base a esta fórmula se calcula el chi cuadrado para cada uno de los escenarios propuestos para cada indicador planteado.

4.5.1.1 D1: RETARDOS EN LA TRANSMISIÓN

La tabla de contingencias para este indicador se muestra en la **Tabla IV.XVIII**

Tabla IV.XVIII9: Tabla de contingencias 6x2 HSRP vs SIN PROTOCOLO

PROTOCOLOS	HSRP	SPAINING TRHEE
LAN(1,4)	5,0	50000
LAN(3,10)	9,6	50000
LAN(5,15)	13,7	50000
WAN(1,4)	4,5	50000
WAN(3,10)	4,8	50000
WAN(5,15)	4,7	50000

Fuente: Autoras

En base a la tabla anterior se creó la tabla de Cálculo de $\mathbf{X^2}$, ver **Tabla IV.XIX**

Tabla IV.XIX10: Tabla de Cálculo de X2 HSRP vs SIN PROTOCOLO

Fo	fe	fo-fe	$(fo-fe)^2$	$(fo-fe)^2 / fe$
50000	5,0	49995,00	2499500025,00	499900005,00
50000	9,6	49990,40	2499040092,16	260316676,27
50000	13,7	49986,30	2498630187,69	182381765,53
50000	4,5	49995,50	2499550020,25	555455560,06
50000	4,8	49995,20	2499520023,04	520733338,13
50000	4,7	49995,30	2499530022,09	531314898,32
				X^2 = 2550102243,31

Fuente: Autora

4.5.1.2 D2: CANTIDAD DE PAQUETES ENVIADOS Y RECIBIDOS

GL = (2-1)(2-1)

GL = 1

Con **α** = 0,1 y 1 grados de libertad tenemos que para nuestra investigación el valor de x^2 tabulado es de 2,705.

La tabla de contingencias para este indicador se muestra en la **Tabla IV.XX**

Tabla IV.XX11: Tabla de contingencias 2X2 HSRP vs SIN PROTOCOLO

PROTOCOLOS	HSRP	SIN PROTOCOLO
LAN	2	50
WAN	1	50

Fuente: Autoras

En base a la tabla anterior se creó la tabla de Cálculo de $\mathbf{X^2}$, ver **Tabla IV.XXI**

Tabla IV.XXI12: Tabla de Cálculo de X^2 Paquetes enviados y recibidos HSRP vs SIN PROTOCOLO

Fo	fe	fo-fe	$(fo-fe)^2$	$(fo-fe)^2 / fe$
50	2	48	2304	1152
50	1	49	2401	2401
				$\mathbf{X^2 = 3553}$

Fuente: Autora

4.5.2 PRUEBA DE X2 - ESCENARIO CON GLBP CONTRA SIN ALTA DISPONIBILIDAD

Con α = 0,1 y 5 grados de libertad tenemos que para nuestra investigación el valor de x^2 tabulado es de 9,236.

4.5.2.1 D1: RETARDOS EN LA TRANSMISIÓN

La tabla de contingencias para este indicador se muestra en la **Tabla IV.XXII**

Tabla IV.XXII13: Tabla de contingencias 6x2 GLBP vs SIN PROTOCOLO

PROTOCOLOS	GLBP	SIN PROTOCOLO
LAN(1,4)	8,8	50000
LAN(3,10)	11.2	50000
LAN(5,15)	14,8	50000
WAN(1,4)	5,0	50000
WAN(3,10)	5,9	50000
WAN(5,15)	6,3	50000

Fuente: Autoras

En base a la tabla anterior se creó la tabla de Cálculo de **X^2**, ver **Tabla XXIII**

Tabla XXIII14: Tabla de Cálculo de X^2 GLBP vs SIN PROTOCOLO

fo	**Fe**	**fo-fe**	**$(fo-fe)^2$**	**$(fo-fe)^2$ / fe**
50000	8,8	49991,20	2499120077,44	283990917,89
50000	11.2	49988,80	2498880125,44	223114296,91
50000	14,8	49985,20	2498520219,04	168818933,72
50000	5,0	49995,00	2499500025,00	499900005,00
50000	5,9	49994,10	2499410034,81	423628819,46
50000	6,3	49993,70	2499370039,69	396725403,13
			X^2 =	**1996178376,11**

Fuente: Autoras

4.5.2.2 D2: CANTIDAD DE PAQUETES ENVIADOS Y RECIBIDOS

GL = (2-1)(2-1)

GL = 1

Con **α** = 0,1 y 1 grados de libertad tenemos que para nuestra investigación el valor de x^2 tabulado es de 2,705.

La tabla de contingencias para este indicador se muestra en la **Tabla IV.XXIV**

Tabla IV.XXIV: Tabla de contingencias 2X2 GLBP vs SIN PROTOCOLO

PROTOCOLOS	**GLBP**	**SIN PROTOCOLO**
LAN	2	50
WAN	2	50

Fuente: Autoras

En base a la tabla anterior se creó la tabla de Cálculo de **X^2**, ver **Tabla IV.XXV**

Tabla IV.XXV15: Tabla de Cálculo de X^2 Paquetes enviados y recibidos GLBP vs SIN PROTOCOLO

Fo	**fe**	**fo-fe**	**$(fo-fe)^2$**	**$(fo-fe)^2$ / fe**
50	2	48	2304	1152
50	2	48	2304	1152
			X^2	**= 2304**

Fuente: Autoras

4.5.3 PRUEBA DE X2 - ESCENARIO CON VRRP CONTRA SIN ALTA DISPONIBILIDAD

GL = (2-1)(2-1)

GL = 1

Con **α** = 0,1 y 1 grado de libertad tenemos que para nuestra investigación el valor de x^2 tabulado es de 2,705.

4.5.3.1 D1: RETARDOS EN LA TRANSMISIÓN

La tabla de contingencias para este indicador se muestra en la **Tabla XXVI**

Tabla XXVI16: Tabla de contingencias 2x2 VRRP vs SIN PROTOCOLO

PROTOCOLOS	**VRRP**	**SIN PROTOCOLO**
LAN	16,3	50000
WAN	40,9	50000

Fuente: Autoras

En base a la tabla anterior se creó la tabla de Cálculo de **X^2**, ver **Tabla XXVII**

Tabla XXVII17: Tabla de Cálculo de X^2 VRRP vs SIN PROTOCOLO

Fo	**fe**	**fo-fe**	**$(fo-fe)^2$**	**$(fo-fe)^2$ / fe**
50000,00	16,3	49983,70	2498370265,69	153274249,43
50000,00	40,9	49959,10	2495911672,81	61024735,28
				X^2 = 214298984,71

Fuente: Autoras

4.5.3.2 D2: CANTIDAD DE PAQUETES ENVIADOS Y RECIBIDOS

GL = (2-1)(2-1)

GL = 1

Con **α** = 0,1 y 1 grado de libertad tenemos que para nuestra investigación el valor de x^2 tabulado es de 2,705.

La tabla de contingencias para este indicador se muestra en la **Tabla IV.XXVIII**

Tabla IV.XXVIII18: Tabla de contingencias 2X2 VRRP vs SIN PROTOCOLO

PROTOCOLOS	**VRRP**	**SIN PROTOCOLO**
LAN	2	50
WAN	4	50

Fuente: Autoras

En base a la tabla anterior se creó la tabla de Cálculo de **X^2**, ver **Tabla XXIX**

Tabla XXIX19: Tabla de Cálculo de X^2 Paquetes enviados y recibidos VRRP vs SIN PROTOCOLO

Fo	**fe**	**fo-fe**	**$(fo-fe)^2$**	**$(fo-fe)^2$ / fe**
50	2	48	2304	1152
50	4	46	2116	529
			X^2	**= 1681**

Fuente: Autoras

4.5.4 RESUMEN DE LAS TABLAS DE CHI CUADRADO

El resumen de los valores calculados de chi cuadrado para cada uno de los indicadores de la variable dependiente se muestra en la **Tabla IV.XXX**

Tabla IV.XXX20: Tabla de resumen del cálculo de X2

ESCENARIO	INDICADOR	X^2
HSRP	D1: Retardo en la Transmisión	**25452064,32**
		
	D2: Cantidad de paquetes enviados y recibidos	**3553,00**
		
GLBP	D1: Retardos en la transmisión	**1996178376,11**
		
	D2: Cantidad de paquetes enviados y recibidos	**2304,00**

<table>
<tr><td></td><td colspan="2"> 
</td></tr>
<tr><td rowspan="4">VRRP</td><td>D1: Retardos de transmisión</td><td>214298984,70</td></tr>
<tr><td colspan="2"> 
</td></tr>
<tr><td>D2: Cantidad de paquetes enviados y recibidos</td><td>1681,00</td></tr>
<tr><td colspan="2"> 
</td></tr>
</table>

Fuente: Autoras

Como se puede observar en la tabla 4.30 todos los valores calculados de $\mathbf{X^2}$ son mayores que el valor de $\mathbf{X^2}$ tabulado que para el caso de la presente investigación es de 9,236 en el caso de retardos en la transmisión y de 2,705 en la cantidad de paquete perdidos y retardos en la transmisión en el caso de VRRP, por lo tanto, se rechaza la hipótesis nula y se acepta la hipótesis de investigación es decir: **Con el análisis comparativo de los protocolos de alta disponibilidad de gateways en el diseño de redes de campus, el tiempo de standby de los servicios y el porcentaje de pérdida de datos disminuirán.**

CONCLUSIONES:

- Los protocolos de alta disponibilidad permiten que los servicios estén disponibles la mayor parte del tiempo ya que poseen un equipo backup que actúa en el caso de que el equipo master haya perdido una conexión.

- Una red con Alta Disponibilidad provee rutas alternas a través de toda la infraestr uctura a fin de que el acceso a los servidores clave sea posible el 100% del tiempo

- Al trabajar con los protocolos de alta disponibilidad en el ambiente Cisco y Linux hemos utilizado herramientas que nos permitan determinar cuál de ellos es el mejor y así proporcionar a los usuarios una guía para el uso de los mismos.

- Gracias al análisis de cada protocolo y al estudio comparativo se ha podido determinar que el mejor protocolo en cuanto a retardo en la transmisión y a la cantidad de paquetes ICMP perdidos es Hsrp, en Cisco ya que los tiempos son menores.

- Para el ambiente Linux hemos determinado que Vrrp es un protocolo que permite trabajar de manera óptima en cuanto a la alta disponibilidad ya que su configuración y manejo es sencillo y proporciona grandes beneficios, aunque este protocolo también se puede configurar en Cisco, pero como nos dimos cuenta el mejor en este ambiente es Glbp.

- La herramienta usada para el análisis en transmisión de video fue VLC, la misma que permitía transferir videos a los clientes y gracias a ella hemos podido determinar que en los protocolos usados en los equipos Cisco es necesario aplicar calidad de servicio ya que el video que se transmite es de muy baja calidad y no permite determinar la pérdida de la conexión.

- Al usar el servidor FileZilla en el protocolo Glbp hemos podido determinar que la transmisión de archivos nunca se pierde ya que este protocolo incorpora balanceo de carga, es decir nunca un equipo está en estado pasivo.

- Al igual que Glbp el protocolo Vrrp también posee balanceo de carga lo que es beneficioso ya que todos los equipos van a estar trabajando.

- La configuración de los protocolos es sencilla, se debe tomar en cuenta las prioridades para así determinar cuál es el quipo máster y cuál es el backup.

- Hemos podido determinar que el protocolo de alta disponibilidad Carp en Linux que es libre, es muy bueno pero si se quiere aplicar a un escenario especifico que posea gateway virtuales en la Lan y en la Wan, es decir que tanto el master como el Backup deben poseer direcciones Lan en la misma red al igual que en la Wan.

- Los equipos pasan por una serie de estados al momento de configurar los protocolos, en el master los estados por los que pasan son: Deshabilitado, inicial, escucha, espera, habla y activo y en el equipo backup son: Deshabilitado, inicial, escucha y activo.

RECOMENDACIONES:

- Verificar las interfaces y las direcciones Mac al momento de configurar cada una de ellas, ya que si no se asigna bien la dirección Ip, no existe conexión y trae problemas.

- Determinar de manera clara cuales van a ser los factores a analizar para determinar cuál es el mejor de los protocolos y como se van a comparar para determinar el mejor.

- Es importante que las empresas usen el protocolo GLBP si poseen equipos Cisco para alta disponibilidad ya que este posee balanceo de carga y permite que la conexión siempre esté disponible para al menos un cliente.

- Para el ambiente Linux es importante el uso del protocolo Vrrp en vyatta ya que este es muy fácil de configurar y permite una alta disponibilidad, además vyatta es OpenBsd que se puede instalar o manejar desde un LiveCd en cualquier equipo.

- Verificar en el ambiente Cisco que equipos soportan los protocolos de alta disponibilidad para poder configurarlos en el mismo equipo y así determinar cuál es el mejor.

RESUMEN

Se procedió a analizar los protocolos que permiten una alta disponibilidad de gateways en las redes de campus, aplicado en un ambiente Cisco y en un ambiente Linux, con la finalidad de determinar cuál es el mejor protocolo para cada ambiente.

Para determinar cual protocolo de alta disponibilidad es el mejor se utilizó las estadísticas de las interfaces de los equipos terminales, así como el programa FileZilla para transmisión de archivos, el Wireshark para analizar los protocolos de red, el Ping en el envio de paquetes ICMP y el VLC para transmitir video.

Se determinó que el mejor protocolo de alta disponibilidad en el ambiente Cisco es el Gateway Load Balancing Protocol ya que proporciona menos retardo en la transmisión de paquetes y menos pérdida de los mismos, y en el ambiente Linux el mejor protocolo es el Virtual Router Redundancy Protocol ya que permite el balanceo de carga para que un router nunca este en estado pasivo.

Gracias al protocolo GLBP y al protocolo VRRP la transmisión de archivos, el envio de paquetes ICMP, la transmisión de video, etc están siempre disponibles aunque una conexión se pierda.

Es importante que las empresas usen el protocolo GLBP en equipos Cisco y VRRP en Linux para alta disponibilidad de servicios, para evitar pérdidas importantes de información y de dinero.

SUMMARY

Three high availability Gateway protocols were analyzed in order to determine which of the three was the most appropriate in field networks. Such protocols were applied under two work sceneries, i.e. Cisco and Linux.

In order to find the appropriate protocol, it was necessary to use certain statistical procedures for obtaining interface behavior on terminal equipment. In order to fulfill the stated requirements, it was necessary to rely on the following programs: FileZilla, Wireshark, Ping, and VLC.

Once the statistical study had been determined, it was concluded that, on the one hand, the Gateway Load Balancing Protocol is the best in Cisco because it provides both lesser retardation on packet transmission and lesser packet loss; on the other hand, the Virtual Router Redundancy Protocol is the best one in Linux because it allows the routers good load balance for avoiding router standby.

It can be concluded that both protocols the GLBP and the VRRP provide high availability service, for example, file transmission, ICMP packet delivery, and video transmission.

It is recommended that all business enterprises utilize GLBP protocol on Cisco equipment and VRRP protocol on Linux, which will avoid the loss of important information transmission and money.

BIBLIOGRAFIA

- **Alta Disponibilidad**
  URL: http://es.wikipedia.org/wiki/Alta_disponibilidad
  2009/10/12

- **Balanceo de Carga con equipos Cisco**
  URL:http://www.networkexperts.com.br/index.php/tutoriais/8-cisco/26-balanceamento-de-carga-com-equipamentos-cisco.html.
  2010/07/01

- **Como trabaja la red de campus**
  URL: http://www.freewimaxinfo.com/campus-area-network-can.html
  2010/05/10

- **Desde las tradicionales red de campus hasta la evolución de la estructura del campus.**
  Traducido del ccnp3
  2010/06/08

- **Diseño de redes de campus**
  URL: http://www.edrawsoft.com/Campus-Network.php
  2010/06/15

- **El protocolo Vrrp**
  URL: http://www.blogelectronica.com/protocolo-vrrp-router/
  2010/07/01

- **FileZilla**
  URL: http://es.wikipedia.org/wiki/FileZilla
  2010/09/08

- **Glbp**

  URL:
  http://www.cisco.com/en/US/does/ios/12_2t/12_2t15/feature/guide/ft_glbp.html
  2010/06/22

- **Gateway Load Balancing Protocol**

  URL: http://en.wikipedia.org/wiki/Gateway_Load_Balancing_Protocol
  2010/07/01

- **Guía CCNA V4**

  URL:
  http://www.cisco.com/en/US/does/ios/12_2t/12_2t15/feature/guide/ft_glbp.html
  2010/04/26

- **Hsrp**

  URL: http://es.wikipedia.org/wiki/HSRP
  2010/06/22

- **Hsrp**

  URL: http://wapedia.mobi/es/HSRP
  2010/06/22

- **Hsrp**

  URL: http://aprenderedes.com/2006/08/04/hot-standby-router-protocol-hsrpnoentra-en-el-ccna/ (04/08/2006)
  2010/07/01

- **Icmp**

  URL: http://www.elrincondejavier.net/html/Article395.html
  2010/09/29

- **Pfsense**
  URL:
  http://www.pfsense.org/index.php?option=com_content&task=view&id=50&Itemid=78
  2010/08/09

- **Redundancia de Gateway**
  URL: http://librosnetworking.blogspot.com/2009/08/redundancia-de-gateway.html
  2009/10/15

- **RFC 3768, Vrrp**
  URL: http://tools.ietf.org/html/rfc3768#section-13
  2010/08/09

- **Rutas Estáticas en Vyatta**
  URL:
  http://www.administraciondesistemasoperativos.com/wiki/index.php/4_Configuraci%C3%B3n_compleja
  2010/08/09

- **Uso de Hsrp en Enrutamiento**
  URL: http://www.cisco.com/en/US/does/internetworking/case/studies/es009.html
  2010/07/15

- **VLC**
  URL: http://es.wikipedia.org/wiki/VLC_media_player
  2010/09/08

- **Vrrp**

  URL:http://hondo.diatel.upm.es/manuales/Teldat/V_10_5/Dm759v10-5_Protocolo_VRRP.pdf

  2010/07/01

- **Vyatta**

  URL: http://www.vyatta.com/downloads/index.php

  2010/08/02

- **Wireshark**

  URL: http://es.wikipedia.org/wiki/Wireshark

  2010/09/08

GLOSARIO DE ACRÓNIMOS

HSRP	Hot Standby Route Protocol
GLBP	Gateway Load Balancing Protocol
VRRP	Virtual Router Redundancy Protocol
CARP	Common Address Redundancy Protocol
IANA	Internet Assigned Numbers Authority
RFC	Request For Comments (Registro Federal del Contribuyentes)
IETF	Internet Engineering Task Force
CAN	Campus Area Network
WAN	Wide Area Network
LAN	Local Area Network
VLAN	Virtual LAN
QoS	Quality of Service
ARP	Address Resolution Protocol
MAC	Media Access Control
IP	Internet Protocol
ICMP	Internet Control Message Protocol
TTL	Time to Live
FDDI	Fiber Distributed Data Interface
OSI	Open System Interconecction
IOS	Internetwork Operating System
ESPOCH	Escuela Superior Politécnica de Chimboraza
WLAN	Wireless Local Area Network
MPLS	Multiprotocol Label Switching
VPN	Virtual Private Network
VIRD	Virtual Router Identifier
IPV4	Internet Protocol versión 4
AVG	Active Virtual Gateway
AVF	Active Virtual Forwarder
IPSEC	Internet Protocol Security

CSMA/CD	Carrier Sense Multiple Access with Collision Detection
NetBIOS	Network Basic Input/Output System
CPU	Unidad Central de Procesamiento
ATM	Modo de Transferencia Asíncrona
SNA	Systems Network Architecture
PING	Packet Internet Groper
VLC	Video Lan
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
AVVID	Architecture for Voice, Video and Integrated Data

GLOSARIO DE TÈRMINOS

Hipótesis.- Es una proposición aceptable que ha sido formulada a través de la recolección de información y datos, aunque no está confirmada sirve para responder de forma tentativa a un problema con base científica.

Convergencia.- Capaz de adaptarse muy rápidamente a los cambios en la topología de red, como enlaces caídos y la inserción de nuevos dispositivos en la red.

Redundancia de Gateway.- Se refiere a que se debe disponer de equipos y enlaces que permitan que los servicios estén disponibles la mayor parte del tiempo, debido a la necesidad de tolerancia a fallos en nuestras redes.

Puerta de enlace (Gateway).- Es un dispositivo, con frecuencia un ordenador, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación.

Balanceo de carga.- Se refiere a la técnica usada para compartir el trabajo a realizar entre varios procesos, ordenadores, discos u otros recursos**.**

Dirección IP Virtual.- Es un mecanismo por medio del cual el resto de usuarios de IRC no tiene acceso a nuestra IP real, sino que ve una IP que no se corresponde con la realidad.

Backbone.- Columna Vertebral, es la infraestructura de la transmisión de datos en una red o un conjunto de ellas en internet.

Multicast.- Es un servicio de red en el cual un único flujo de datos, proveniente de una determinada fuente, puede ser enviada simultáneamente para diversos destinatarios.

Broadcast.- transmisión de un paquete que será recibido por todos los dispositivos en una red.

Standby.- se refiere al estado en el que un determinado objeto esta pasivo hasta que tenga que actuar.

Master.- Es cuando un equipo se encuentra activo, esperando que se caiga una conexión, es decir es el principal.

Backup.- Es cuando un equipo está en estado de espera, es decir no hace nada hasta que sea necesario.

Cuellos de botella.- Es cuando se realizan muchas solicitudes pero no pueden ser atendidas al mismo tiempo quedando en una fila de espera hasta llegar un punto que quien está atendiendo las solicitudes no puede más, saturándose y terminando el proceso.

Internetwork.- Es la práctica de conectar una red informática con otras redes a través de la utilización de puertas de enlace que proporcionan un método común de enrutamiento de información de los paquetes entre las redes.

Operacionalización.- Es el procedimiento por el cual se pasa de variables generales a indicadores, es el proceso de medición en las ciencias sociales y está compuesto por una serie de fases.

Estadística no paramétrica.- Es una rama de la estadística que estudia las pruebas y modelos estadísticos cuya distribución subyacente no se ajusta a los llamados criterios paramétricos.

Hellotime.- Es el tiempo entre mensajes hello que se envían desde un router y varían de acuerdo al protocolo, está dado en segundos.

Holdtime.- Es un temporizador usado para intercambiar mensajes de hello entre los router, es el tiempo máximo del hellotime.

ANEXO 1

TABLA 3-Distribución Chi Cuadrado χ^2

P = Probabilidad de encontrar un valor mayor o igual que el chi cuadrado tabulado, v = Grados de Libertad

v/p	0,001	0,0025	0,005	0,01	0,025	0,05	0,1	0,15	0,2	0,25	0,3	0,35	0,4	0,45	0,5
1	10,8274	9,1404	7,8794	6,6349	5,0239	3,8415	2,7055	2,0722	1,6424	1,3233	1,0742	0,8735	0,7083	0,5707	0,4549
2	13,8150	11,9827	10,5965	9,2104	7,3778	5,9915	4,6052	3,7942	3,2189	2,7726	2,4079	2,0996	1,8326	1,5970	1,3863
3	16,2660	14,3202	12,8381	11,3449	9,3484	7,8147	6,2514	5,3170	4,6416	4,1083	3,6649	3,2831	2,9462	2,6430	2,3660
4	18,4662	16,4238	14,8602	13,2767	11,1433	9,4877	7,7794	6,7449	5,9886	5,3853	4,8784	4,4377	4,0446	3,6871	3,3567
5	20,5147	18,3854	16,7496	15,0863	12,8325	11,0705	9,2363	8,1152	7,2893	6,6257	6,0644	5,5731	5,1319	4,7278	4,3515
6	22,4575	20,2491	18,5475	16,8119	14,4494	12,5916	10,6446	9,4461	8,5581	7,8408	7,2311	6,6948	6,2108	5,7652	5,3481
7	24,3213	22,0402	20,2777	18,4753	16,0128	14,0671	12,0170	10,7479	9,8032	9,0371	8,3834	7,8061	7,2832	6,8000	6,3458
8	26,1239	23,7742	21,9549	20,0902	17,5345	15,5073	13,3616	12,0271	11,0301	10,2189	9,5245	8,9094	8,3505	7,8325	7,3441
9	27,8767	25,4625	23,5893	21,6660	19,0228	16,9190	14,6837	13,2880	12,2421	11,3887	10,6564	10,0060	9,4136	8,8632	8,3428
10	29,5879	27,1119	25,1881	23,2093	20,4832	18,3070	15,9872	14,5339	13,4420	12,5489	11,7807	11,0971	10,4732	9,8922	9,3418
11	31,2635	28,7291	26,7569	24,7250	21,9200	19,6752	17,2750	15,7671	14,6314	13,7007	12,8987	12,1836	11,5298	10,9199	10,3410
12	32,9092	30,3182	28,2997	26,2170	23,3367	21,0261	18,5493	16,9893	15,8120	14,8454	14,0111	13,2661	12,5838	11,9463	11,3403
13	34,5274	31,8830	29,8193	27,6882	24,7356	22,3620	19,8119	18,2020	16,9848	15,9839	15,1187	14,3451	13,6356	12,9717	12,3398
14	36,1239	33,4262	31,3194	29,1412	26,1189	23,6848	21,0641	19,4062	18,1508	17,1169	16,2221	15,4209	14,6853	13,9961	13,3393
15	37,6978	34,9494	32,8015	30,5780	27,4884	24,9958	22,3071	20,6030	19,3107	18,2451	17,3217	16,4940	15,7332	15,0197	14,3389
16	39,2518	36,4555	34,2671	31,9999	28,8453	26,2962	23,5418	21,7931	20,4651	19,3689	18,4179	17,5646	16,7795	16,0425	15,3385
17	40,7911	37,9462	35,7184	33,4087	30,1910	27,5871	24,7690	22,9770	21,6146	20,4887	19,5110	18,6330	17,8244	17,0646	16,3382
18	42,3119	39,4220	37,1564	34,8052	31,5264	28,8693	25,9894	24,1555	22,7595	21,6049	20,6014	19,6993	18,8679	18,0860	17,3379
19	43,8194	40,8847	38,5821	36,1908	32,8523	30,1435	27,2036	25,3289	23,9004	22,7178	21,6891	20,7638	19,9102	19,1069	18,3376
20	45,3142	42,3358	39,9969	37,5663	34,1696	31,4104	28,4120	26,4976	25,0375	23,8277	22,7745	21,8265	20,9514	20,1272	19,3374
21	46,7963	43,7749	41,4009	38,9322	35,4789	32,6706	29,6151	27,6620	26,1711	24,9348	23,8578	22,8876	21,9915	21,1470	20,3372
22	48,2676	45,2041	42,7957	40,2894	36,7807	33,9245	30,8133	28,8224	27,3015	26,0393	24,9390	23,9473	23,0307	22,1663	21,3370
23	49,7276	46,6231	44,1814	41,6383	38,0756	35,1725	32,0069	29,9792	28,4288	27,1413	26,0184	25,0055	24,0689	23,1852	22,3369
24	51,1790	48,0336	45,5584	42,9798	39,3641	36,4150	33,1962	31,1325	29,5533	28,2412	27,0960	26,0625	25,1064	24,2037	23,3367
25	52,6187	49,4351	46,9280	44,3140	40,6465	37,6525	34,3816	32,2825	30,6752	29,3388	28,1719	27,1183	26,1430	25,2218	24,3366
26	54,0511	50,8291	48,2898	45,6416	41,9231	38,8851	35,5632	33,4295	31,7946	30,4346	29,2463	28,1730	27,1789	26,2395	25,3365
27	55,4751	52,2152	49,6450	46,9628	43,1945	40,1133	36,7412	34,5736	32,9117	31,5284	30,3193	29,2266	28,2141	27,2569	26,3363
28	56,8918	53,5939	50,9936	48,2782	44,4608	41,3372	37,9159	35,7150	34,0266	32,6205	31,3909	30,2791	29,2486	28,2740	27,3362
29	58,3006	54,9662	52,3355	49,5878	45,7223	42,5569	39,0875	36,8538	35,1394	33,7109	32,4612	31,3308	30,2825	29,2908	28,3361

ANEXO 2

CONFIGURACION HSRP

CONFIGURACION HSRP MASTER

```
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip address 192.168.2.1 255.255.255.0
 standby 2 ip 192.168.2.100
 standby 2 priority 110
 standby 2 preempt
 standby 2 authentication testhsrp
 standby 2 track Serial0/0/1 15
!
interface FastEthernet0/0.3
 encapsulation dot1Q 3
 ip address 192.168.3.1 255.255.255.0
 standby 3 ip 192.168.3.100
 standby 3 priority 110
 standby 3 preempt
 standby 3 authentication testhsrp
 standby 3 track Serial0/0/1 15
!
interface FastEthernet0/0.4
 encapsulation dot1Q 4
 ip address 192.168.4.1 255.255.255.0
 standby 4 ip 192.168.4.100
 standby 4 priority 110
 standby 4 preempt
 standby 4 authentication testhsrp
 standby 4 track Serial0/0/1 15
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/3/0
!
interface FastEthernet0/3/1
```

```
!
interface FastEthernet0/3/2
!
interface FastEthernet0/3/3
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 125000
!
interface Serial0/0/1
 ip address 172.168.40.1 255.255.255.0
 clock rate 56000
!
interface Serial0/2/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/2/1
 no ip address
 shutdown
 clock rate 2000000
interface Vlan1
 no ip address
ip forward-protocol nd
ip route 172.168.1.0 255.255.255.0 172.168.40.2
no ip http server
no ip http secure-server
control-plane
mgcp fax t38 ecm
gatekeeper
 shutdown
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
end

MASTER#
!
```

ESTADOS HSRP

MASTER#SHOW STANDBY
FastEthernet0/0.2 - Group 2
State is Active
130 state changes, last state change 00:08:33
Virtual IP address is 192.168.2.100
Active virtual MAC address is 0000.0c07.ac02
Local virtual MAC address is 0000.0c07.ac02 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.880 secs
Preemption enabled
Active router is local
Standby router is unknown
Priority 95 (configured 110)
Track interface Serial0/0/1 state Down decrement 15
Group name is "hsrp-Fa0/0.2-2" (default)
FastEthernet0/0.3 - Group 3
State is Active
128 state changes, last state change 00:08:32
Virtual IP address is 192.168.3.100
Active virtual MAC address is 0000.0c07.ac03
Local virtual MAC address is 0000.0c07.ac03 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 2.240 secs
Preemption enabled
Active router is local
Standby router is unknown
Priority 95 (configured 110)
Track interface Serial0/0/1 state Down decrement 15
Group name is "hsrp-Fa0/0.3-3" (default)
FastEthernet0/0.4 - Group 4
State is Active
122 state changes, last state change 00:08:35
Virtual IP address is 192.168.4.100
Active virtual MAC address is 0000.0c07.ac04
Local virtual MAC address is 0000.0c07.ac04 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 1.904 secs
Preemption enabled
Active router is local
Standby router is unknown
Priority 95 (configured 110)
Track interface Serial0/0/1 state Down decrement 15
Group name is "hsrp-Fa0/0.4-4" (default)

CONFIGURACION HSRP BACKUP

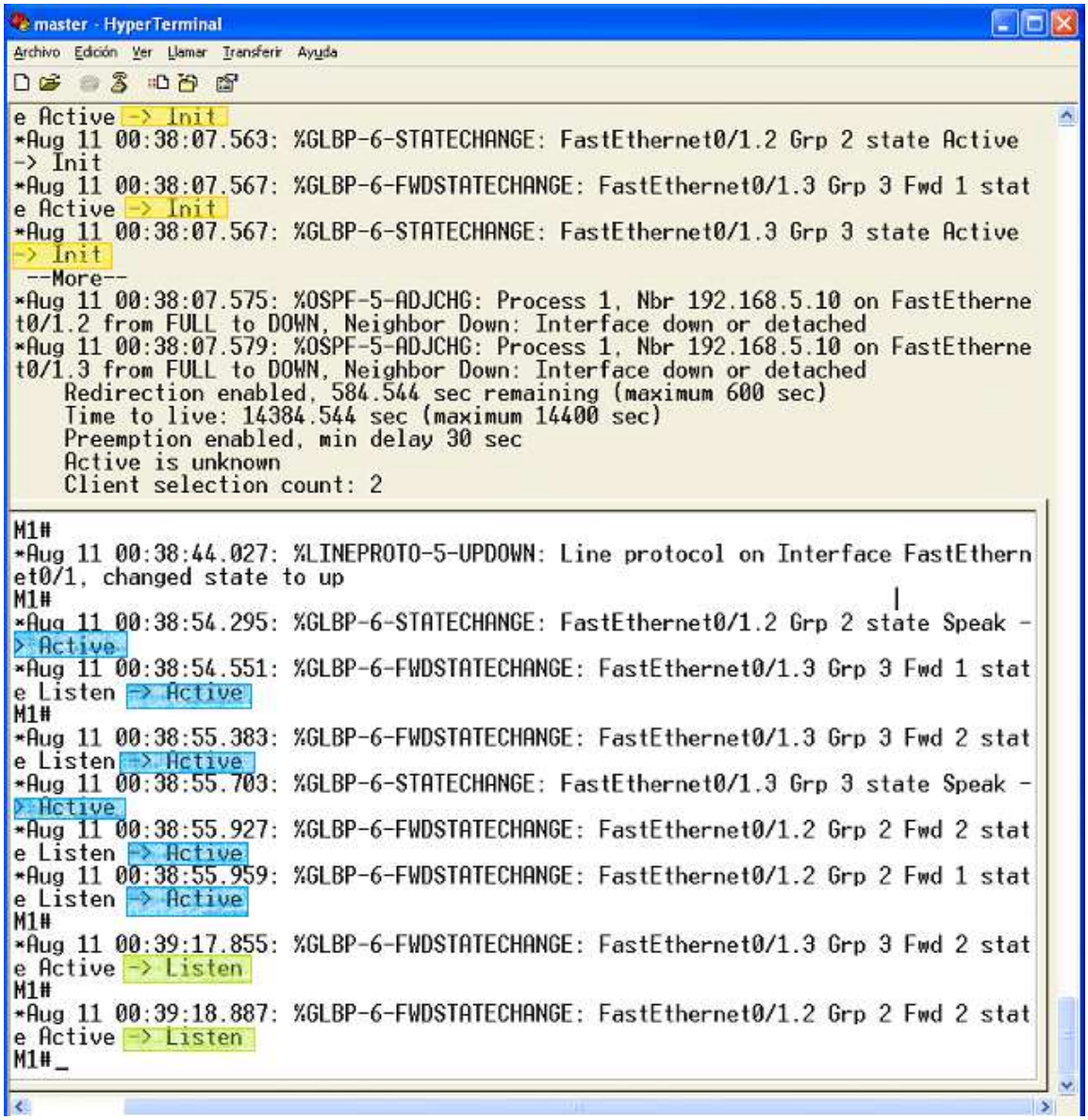
```
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip address 192.168.2.10 255.255.255.0
 standby 2 ip 192.168.2.100
 standby 2 preempt
 standby 2 authentication testhsrp
 standby 2 track Serial0/1/0
!
interface FastEthernet0/0.3
 encapsulation dot1Q 3
 ip address 192.168.3.10 255.255.255.0
 standby 3 ip 192.168.3.100
 standby 3 preempt
 standby 3 authentication testhsrp
 standby 3 track Serial0/1/0
!
interface FastEthernet0/0.4
 encapsulation dot1Q 4
 ip address 192.168.4.10 255.255.255.0
 standby 4 ip 192.168.4.100
 standby 4 preempt
 standby 4 authentication testhsrp
 standby 4 track Serial0/1/0
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1.1
!
interface Serial0/1/0
 ip address 172.168.50.1 255.255.255.0
 clock rate 56000
!
interface Serial0/1/1
 no ip address
 shutdown
 clock rate 2000000
```

ip route 172.168.1.0 255.255.255.0 172.168.50.2
!no ip http server
no ip http secure-server
control-plane
!line con 0
line aux 0
line vty 0 4
 login
scheduler allocate 20000 1000
end

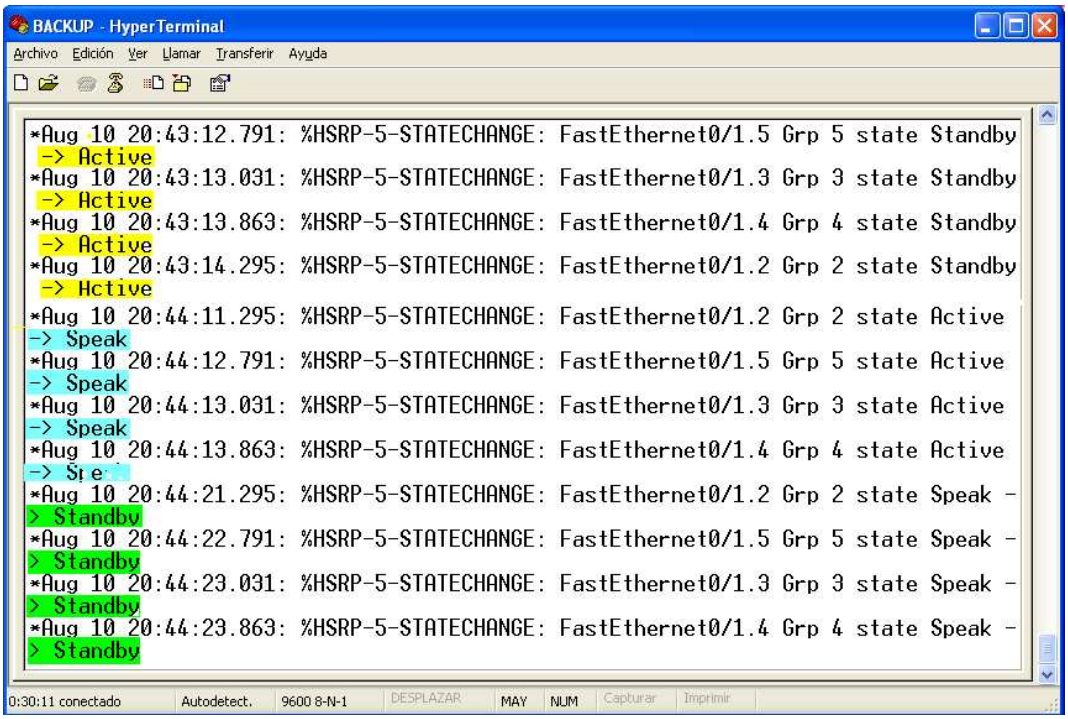
BACKUP#
CAIDA LA LAN DEL MASTER EL BACKUP TIENE EL ESTADO ACTIVO
BACKUP#show standby
FastEthernet0/0.2 - Group 2
  State is Active
    32 state changes, last state change 00:02:13
  Virtual IP address is 192.168.2.100
  Active virtual MAC address is 0000.0c07.ac02
    Local virtual MAC address is 0000.0c07.ac02 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.072 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 80 (configured 80)
    Track interface Serial0/1/0 state Up decrement 10
  IP redundancy name is "hsrp-Fa0/0.2-2" (default)
FastEthernet0/0.3 - Group 3
  State is Active
    32 state changes, last state change 00:02:15
  Virtual IP address is 192.168.3.100
  Active virtual MAC address is 0000.0c07.ac03
    Local virtual MAC address is 0000.0c07.ac03 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.488 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 80 (configured 80)
    Track interface Serial0/1/0 state Up decrement 10
  IP redundancy name is "hsrp-Fa0/0.3-3" (default)
FastEthernet0/0.4 - Group 4
  State is Active
    32 state changes, last state change 00:02:19
  Virtual IP address is 192.168.4.100

Active virtual MAC address is 0000.0c07.ac04
  Local virtual MAC address is 0000.0c07.ac04 (v1 default)
Hello time 3 sec, hold time 10 sec
  Next hello sent in 2.000 secs
Preemption enabled
Active router is local
Standby router is unknown
Priority 80 (configured 80)
  Track interface Serial0/1/0 state Up decrement 10
IP redundancy name is "hsrp-Fa0/0.4-4" (default)

ESTADOS POR LOS QUE PASA EL MASTER



ESTADOS POR LOS QUE PASA EL BACKUP AL VOLVER A CONECTAR LA LAN O LA WAN



SERVIDOR WEB EN HSRP

CONFIGURACION GLBP

CONFIGURACION MASTER

```
Building configuration...
Current configuration : 2232 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname MASTER
boot-start-marker
boot-end-marker
logging message-counter syslog
no aaa new-model
dot11 syslog
ip source-route
ip cef
no ipv6 cef
multilink bundle-name authenticated
voice-card 0
archive
 log config
  hidekeys
track 1 interface Serial0/0/1 ip routing
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip address 192.168.2.1 255.255.255.0
 glbp 2 ip 192.168.2.100
 glbp 2 priority 150
 glbp 2 preempt
 glbp 2 authentication text testglbp
 glbp 2 weighting track 1 decrement 100

interface FastEthernet0/0.3
 encapsulation dot1Q 3
 ip address 192.168.3.1 255.255.255.0
 glbp 3 ip 192.168.3.100
 glbp 3 priority 150
 glbp 3 preempt
 glbp 3 authentication text testglbp
 glbp 3 weighting track 1 decrement 100
!
```

```
interface FastEthernet0/0.4
 encapsulation dot1Q 4
 ip address 192.168.4.1 255.255.255.0
 glbp 4 ip 192.168.4.100
 glbp 4 priority 150
 glbp 4 preempt
 glbp 4 authentication text testglbp
 glbp 4 weighting track 1 decrement 100
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/3/0
!
interface FastEthernet0/3/1
!
interface FastEthernet0/3/2
!
interface FastEthernet0/3/3
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 125000
!
interface Serial0/0/1
 ip address 172.168.40.1 255.255.255.0
 clock rate 128000
!
interface Serial0/2/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/2/1
 no ip address
 shutdown
 clock rate 2000000
!
interface Vlan1
 no ip address
!
router ospf 1
```

```
 log-adjacency-changes
 network 172.168.40.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.3.0 0.0.0.255 area 0
 network 192.168.4.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
mgcp fax t38 ecm
gatekeeper
 shutdown
line con 0
line aux 0
line vty 0 4
 login
scheduler allocate 20000 1000
end
```

CONFIGURACION SHOW GLBP

```
MASTER#SHOW GLBP
FastEthernet0/0.2 - Group 2
  State is Active
    1 state change, last state change 00:13:10
  Virtual IP address is 192.168.2.100
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.504 secs
  Redirect time 600 sec, forwarder timeout 14400 sec
  Authentication text, string "testglbp"
  Preemption enabled, min delay 0 sec
  Active is local
  Standby is 192.168.2.10, priority 100 (expires in 8.160 sec)
  Priority 150 (configured)
  Weighting 100 (default 100), thresholds: lower 1, upper 100
    Track object 1 state Up decrement 100
  Load balancing: round-robin
  Group members:
    0017.94a5.0ef8 (192.168.2.1) local
    0019.2fc0.d816 (192.168.2.10)
  There are 2 forwarders (1 active)
  Forwarder 1
    State is Listen
      2 state changes, last state change 00:09:56
```

MAC address is 0007.b400.0201 (learnt)
Owner ID is 0019.2fc0.d816
Redirection enabled, 598.432 sec remaining (maximum 600 sec)
Time to live: 14398.432 sec (maximum 14400 sec)
Preemption enabled, min delay 30 sec
Active is 192.168.2.10 (primary), weighting 100 (expires in 10.176 sec)
Forwarder 2
State is Active
1 state change, last state change 00:09:46
MAC address is 0007.b400.0202 (default)
Owner ID is 0017.94a5.0ef8
Redirection enabled
Preemption enabled, min delay 30 sec
Active is local, weighting 100
FastEthernet0/0.3 - Group 3
State is Active
1 state change, last state change 00:04:59
Virtual IP address is 192.168.3.100
Hello time 3 sec, hold time 10 sec
Next hello sent in 1.440 secs
Redirect time 600 sec, forwarder timeout 14400 sec
Authentication text, string "testglbp"
Preemption enabled, min delay 0 sec
Active is local
Standby is 192.168.3.10, priority 100 (expires in 8.800 sec)
Priority 150 (configured)
Weighting 100 (default 100), thresholds: lower 1, upper 100
Track object 1 state Up decrement 100
Load balancing: round-robin
Group members:
0017.94a5.0ef8 (192.168.3.1) local
0019.2fc0.d816 (192.168.3.10)
There are 2 forwarders (1 active)
Forwarder 1
State is Listen
MAC address is 0007.b400.0301 (learnt)
Owner ID is 0019.2fc0.d816
Redirection enabled, 598.816 sec remaining (maximum 600 sec)
Time to live: 14398.816 sec (maximum 14400 sec)
Preemption enabled, min delay 30 sec
Active is 192.168.3.10 (primary), weighting 100 (expires in 9.184 sec)
Forwarder 2
State is Active
1 state change, last state change 00:04:36
MAC address is 0007.b400.0302 (default)
Owner ID is 0017.94a5.0ef8

Redirection enabled
Preemption enabled, min delay 30 sec
Active is local, weighting 100
FastEthernet0/0.4 - Group 4
State is Active
1 state change, last state change 00:09:01
Virtual IP address is 192.168.4.100
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.672 secs
Redirect time 600 sec, forwarder timeout 14400 sec
Authentication text, string "testglbp"
Preemption enabled, min delay 0 sec
Active is local
Standby is 192.168.4.10, priority 100 (expires in 9.856 sec)
Priority 150 (configured)
Weighting 100 (default 100), thresholds: lower 1, upper 100
Track object 1 state Up decrement 100
Load balancing: round-robin
Group members:
0017.94a5.0ef8 (192.168.4.1) local
0019.2fc0.d816 (192.168.4.10)
There are 2 forwarders (1 active)
Forwarder 1
State is Listen
2 state changes, last state change 00:03:11
MAC address is 0007.b400.0401 (learnt)
Owner ID is 0019.2fc0.d816
Redirection enabled, 598.432 sec remaining (maximum 600 sec)
Time to live: 14398.432 sec (maximum 14400 sec)
Preemption enabled, min delay 30 sec
Active is 192.168.4.10 (primary), weighting 100 (expires in 8.832 sec)
Client selection count: 1
Forwarder 2
State is Active
1 state change, last state change 00:02:58
MAC address is 0007.b400.0402 (default)
Owner ID is 0017.94a5.0ef8
Redirection enabled
Preemption enabled, min delay 30 sec
Active is local, weighting 100

CONFIGURACION BACKUP

Current configuration : 1579 bytes
!
version 12.4

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname BACKUP
!
boot-start-marker
boot-end-marker
no aaa new-model
resource policy
!
ip cef
voice-card 0
track 1 interface Serial0/1/0 ip routing
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 glbp 1 timers 5 15
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip address 192.168.2.10 255.255.255.0
 glbp 2 ip 192.168.2.100
 glbp 2 preempt
 glbp 2 authentication text testglbp
 glbp 2 weighting track 1 decrement 100
!
interface FastEthernet0/0.3
 encapsulation dot1Q 3
 ip address 192.168.3.10 255.255.255.0
 glbp 3 ip 192.168.3.100
 glbp 3 preempt
 glbp 3 authentication text testglbp
 glbp 3 weighting track 1 decrement 100
!
interface FastEthernet0/0.4
 encapsulation dot1Q 4
 ip address 192.168.4.10 255.255.255.0
 glbp 4 ip 192.168.4.100
 glbp 4 preempt
 glbp 4 authentication text testglbp
 glbp 4 weighting track 1 decrement 100
!
interface FastEthernet0/1
 no ip address
```

```
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1/0
 bandwidth 128
 ip address 172.168.50.1 255.255.255.0
 clock rate 128000

interface Serial0/1/1
 no ip address
 shutdown
 clock rate 2000000
router ospf 1
 log-adjacency-changes
 network 172.168.50.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.0.255 area 0
no ip http server
no ip http secure-server
control-plane
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
end
```

CONFIGURACION SHOW GLBP

FastEthernet0/0.2 - Group 2
State is Standby
4 state changes, last state change 00:14:30
Virtual IP address is 192.168.2.100
Hello time 3 sec, hold time 10 sec
Next hello sent in 2.644 secs
Redirect time 600 sec, forwarder time-out 14400 sec
Authentication text "testglbp"
Preemption enabled, min delay 0 sec
Active is 192.168.2.1, priority 150 (expires in 7.436 sec)
Standby is local
Priority 100 (default)
Weighting 100 (default 100), thresholds: lower 1, upper 100
Track object 1 state Up decrement 100
Load balancing: round-robin
Group members:

0017.94a5.0ef8 (192.168.2.1)
0019.2fc0.d816 (192.168.2.10) local
There are 2 forwarders (1 active)
Forwarder 1
State is Active
3 state changes, last state change 00:14:30
MAC address is 0007.b400.0201 (default)
Owner ID is 0019.2fc0.d816
Preemption enabled, min delay 30 sec
Active is local, weighting 100
Forwarder 2
State is Listen
MAC address is 0007.b400.0202 (learnt)
Owner ID is 0017.94a5.0ef8
Time to live: 14398.972 sec (maximum 14400 sec)
Preemption enabled, min delay 30 sec
Active is 192.168.2.1 (primary), weighting 100 (expires in 8.972 sec)

FastEthernet0/0.3 - Group 3
State is Standby
4 state changes, last state change 00:09:23
Virtual IP address is 192.168.3.100
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.336 secs
Redirect time 600 sec, forwarder time-out 14400 sec
Authentication text "testglbp"
Preemption enabled, min delay 0 sec
Active is 192.168.3.1, priority 150 (expires in 9.004 sec)
Standby is local
Priority 100 (default)
Weighting 100 (default 100), thresholds: lower 1, upper 100
Track object 1 state Up decrement 100
Load balancing: round-robin
Group members:
0017.94a5.0ef8 (192.168.3.1)
0019.2fc0.d816 (192.168.3.10) local
There are 2 forwarders (1 active)
Forwarder 1
State is Active
1 state change, last state change 00:12:26
MAC address is 0007.b400.0301 (default)
Owner ID is 0019.2fc0.d816
Preemption enabled, min delay 30 sec
Active is local, weighting 100
Forwarder 2
State is Listen

MAC address is 0007.b400.0302 (learnt)
Owner ID is 0017.94a5.0ef8
Time to live: 14399.964 sec (maximum 14400 sec)
Preemption enabled, min delay 30 sec
Active is 192.168.3.1 (primary), weighting 100 (expires in 9.964 sec)

FastEthernet0/0.4 - Group 4

State is Standby
4 state changes, last state change 00:07:43
Virtual IP address is 192.168.4.100
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.268 secs
Redirect time 600 sec, forwarder time-out 14400 sec
Authentication text "testglbp"
Preemption enabled, min delay 0 sec
Active is 192.168.4.1, priority 150 (expires in 8.316 sec)
Standby is local
Priority 100 (default)
Weighting 100 (default 100), thresholds: lower 1, upper 100
Track object 1 state Up decrement 100
Load balancing: round-robin
Group members:
0017.94a5.0ef8 (192.168.4.1)
0019.2fc0.d816 (192.168.4.10) local
There are 2 forwarders (1 active)
Forwarder 1
State is Active
3 state changes, last state change 00:07:44
MAC address is 0007.b400.0401 (default)
Owner ID is 0019.2fc0.d816
Preemption enabled, min delay 30 sec
Active is local, weighting 100
Forwarder 2
State is Listen
MAC address is 0007.b400.0402 (learnt)
Owner ID is 0017.94a5.0ef8
Time to live: 14399.704 sec (maximum 14400 sec)
Preemption enabled, min delay 30 sec
Active is 192.168.4.1 (primary), weighting 100 (expires in 9.704 sec)

ESTADOS DE GLBP MASTER

timers 3 10
*Sep 9 19:34:10.367: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to down
*Sep 9 19:34:10.367: %GLBP-6-FWDSTATECHANGE: FastEthernet0/0 Grp 1 Fwd 2 state
Active -> Init

*Sep 9 19:34:10.367: %GLBP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Active -> Init
*Sep 9 19:34:10.371: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.0.2 on FastEthernet 0/0 from FULL to DOWN, Neighbor Down: Interface down or detached
*Sep 9 19:34:31.915: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern et0/0, changed state to up
*Sep 9 19:34:49.519: %GLBP-6-FWDSTATECHANGE: FastEthernet0/0 Grp 1 Fwd 2 state Listen -> Active
*Sep 9 19:34:49.679: %GLBP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Speak -> Active
*Sep 9 19:34:49.871: %GLBP-6-FWDSTATECHANGE: FastEthernet0/0 Grp 1 Fwd 1 state Listen -> Active
*Sep 9 19:35:07.823: %GLBP-6-FWDSTATECHANGE: FastEthernet0/0 Grp 1 Fwd 1 state Active -> Listen
*Sep 9 19:35:11.923: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.0.2 on FastEthernet 0/0 from LOADING to FULL, Loading Done

ESTADOS DE GLBP BACKUP

*Sep 9 17:40:56.627: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.4.1 on FastEthernet 0/0 from LOADING to FULL, Loading Done
*Sep 9 17:43:21.815: %GLBP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Standby -> Active
*Sep 9 17:43:21.815: %GLBP-6-FWDSTATECHANGE: FastEthernet0/0 Grp 1 Fwd 2 state Listen -> Active
*Sep 9 17:43:47.331: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.4.1 on FastEthernet 0/0 from FULL to DOWN, Neighbor Down: Dead timer expired
*Sep 9 17:44:06.671: %GLBP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Active -> Speak
*Sep 9 17:44:06.671: %GLBP-6-FWDSTATECHANGE: FastEthernet0/0 Grp 1 Fwd 2 state Active -> Listen
*Sep 9 17:44:10.767: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.4.1 on FastEthernet 0/0 from LOADING to FULL, Loading Done

SERVIDOR WEB EN GLBP

CONFIGURACION VRRP

CONFIGURAR LAS INTERFACES

vyatta@R1#set interfaces ethernet eth# address 0.0.0.0/24
vyatta@R1#commit

CONFIGURAR EL GUI PARA ACCEDER VIA WEB

vyatta@R1#set service https
vyatta@R1#commit

CONFIGURACION MASTER VRRP

vyatta@R1# set interfaces ethernet eth0 vrrp vrrp-group 99
vyatta@R1# set interfaces ethernet eth0 vrrp vrrp-group 99 virtual-address 172.168.2.100/24
vyatta@R1# set interfaces ethernet eth0 vrrp vrrp-group 99 preempt true
vyatta@R1# set interfaces ethernet eth0 vrrp vrrp-group 99 priority 150
vyatta@R1# commit
vyatta@R1# show interfaces ethernet eth0 vrrp

CONFIGURACION BACKUP VRRP

vyatta@R2# set interfaces ethernet eth0 vrrp vrrp-group 99
vyatta@R2# set interfaces ethernet eth0 vrrp vrrp-group 99 virtual-address 172.16.0.24/24
vyatta@R2# set interfaces ethernet eth0 vrrp vrrp-group 99 preempt true
vyatta@R2# set interfaces ethernet eth0 vrrp vrrp-group 99 priority 20
Commit the configuration. vyatta@R2# commit

CONFIGURACION RUTAS ESTÁTICAS

vyatta@R1#set protocolos static route 0.0.0.0/0 nexthop 0.0.0.0
vyatta@R1#commit

ANEXO 3

Presentación

El Documento contiene información expresa de cómo se configura cada uno de los protocolos y como es su manejo en caso de que se pierda una conexión.

Requisitos mínimos del sistema

- Router Cisco 2800 Series
- Procesador Pentium IV
- Microsoft® Windows® /Me/Xp/Vista/
- Switch Catalyst 2950 Series o cualquier switch administrable.

Instrucciones de uso

Para configurar los protocolos Hsrp y Glbp en cisco se debe escoger los equipos adecuados que soporten estos protocolos, y en el ambiente Linux se debe ejecutar el Live Cd vyatta, el mismo que se puede descargar y quemar en un cd, este se puede obtener desde la página http://www.vyatta.com/downloads/index.php

CONFIGURACIÓN

PROTOCOLO HSRP

Para configurar hsrp en un router se debe seguir los siguientes comandos, como se configuro vlans, se crea un subintefaz para cada una de estas, dentro de la interfaz FastEthernet.

EQUIPO MASTER

VLAN 2
Router(config)#interface FastEthernet0/0.2
Router(config)#encapsulation dot1Q 2
Router(config)# ip address 192.168.2.1 255.255.255.0
Router(config)# standby 2 ip 192.168.2.100
Router(config)# standby 2 priority 110
Router(config)# standby 2 preempt
Router(config)# standby 2 authentication testhsrp
Router(config)# standby 2 track Serial0/0/1 15
VLAN 3
Router(config)#interface FastEthernet0/0.3
Router(config)#encapsulation dot1Q 3
Router(config)#ip address 192.168.3.1 255.255.255.0
Router(config)#standby 3 ip 192.168.3.100
Router(config)#standby 3 priority 110
Router(config)#standby 3 preempt
Router(config)#standby 3 authentication testhsrp
Router(config)#standby 3 track Serial0/0/1 15

VLAN 4
Router(config)#interface FastEthernet0/0.4
Router(config)#encapsulation dot1Q 4
Router(config)# ip address 192.168.4.1 255.255.255.0
Router(config)#standby 4 ip 192.168.4.100
Router(config)#standby 4 priority 110
Router(config)#standby 4 preempt
Router(config)#standby 4 authentication testhsrp
Router(config)#standby 4 track Serial0/0/1 15

INTERFAZ SERIAL
Router(config)#interface Serial0/0/1
Router(config)#ip address 172.168.40.1 255.255.255.0
Router(config)#clock rate 56000
Router(config)#no shutdown

RUTAS ESTÁTICAS
Router(config)#ip route 172.168.1.0 255.255.255.0 172.168.40.2

EQUIPO BACKUP

VLAN 2
Router(config)#interface FastEthernet0/0.2
Router(config)#encapsulation dot1Q 2

Router(config)# ip address 192.168.2.1 255.255.255.0
Router(config)# standby 2 ip 192.168.2.100
Router(config)# standby 2 preempt
Router(config)# standby 2 authentication testhsrp
Router(config)# standby 2 track Serial0/0/1 15

VLAN 3
Router(config)#interface FastEthernet0/0.3
Router(config)#encapsulation dot1Q 3
Router(config)#ip address 192.168.3.1 255.255.255.0
Router(config)#standby 3 ip 192.168.3.100
Router(config)#standby 3 preempt
Router(config)#standby 3 authentication testhsrp
Router(config)#standby 3 track Serial0/0/1 15

VLAN 4
Router(config)#interface FastEthernet0/0.4
Router(config)#encapsulation dot1Q 4
Router(config)# ip address 192.168.4.1 255.255.255.0
Router(config)#standby 4 ip 192.168.4.100
Router(config)#standby 4 preempt
Router(config)#standby 4 authentication testhsrp
Router(config)#standby 4 track Serial0/0/1 15

INTERFAZ SERIAL
Router(config)#interface Serial0/3/1
Router(config)#ip address 172.168.50.1 255.255.255.0
Router(config)#clock rate 56000
Router(config)#no shutdown

RUTAS ESTÁTICAS
Router(config)#ip route 172.168.1.0 255.255.255.0 172.168.50.2

PROTOCOLO GLBP
La configuración del protocolo GLBP en un equipo Cisco se debe hacer de la siguiente manera.

EQUIPO MASTER

VLAN 2
Router(config)#interface FastEthernet0/0.2
Router(config)#encapsulation dot1Q 2
Router(config)# ip address 192.168.2.1 255.255.255.0
Router(config)#glbp 2 ip 192.168.2.100
Router(config)#glbp 2 priority 150
Router(config)#glbp 2 preempt

Router(config)#glbp 2 authentication text testglbp
Router(config)#glbp 2 weighting track 1 decrement 100

VLAN 3
Router(config)#interface FastEthernet0/0.3
Router(config)#encapsulation dot1Q 3
Router(config)#ip address 192.168.3.1 255.255.255.0
Router(config)#glbp 3 ip 192.168.3.100
Router(config)#glbp 3 priority 150
Router(config)#glbp 3 preempt
Router(config)#glbp 3 authentication text testglbp
Router(config)#glbp 3 weighting track 1 decrement 100

VLAN 4
Router(config)#interface FastEthernet0/0.4
Router(config)#encapsulation dot1Q 4
Router(config)# ip address 192.168.4.1 255.255.255.0
Router(config)#glbp 4 ip 192.168.4.100
Router(config)#glbp 4 priority 150
Router(config)#glbp 4 preempt
Router(config)#glbp 4 authentication text testglbp
Router(config)#glbp 4 weighting track 1 decrement 100

INTERFAZ SERIAL
Router(config)#interface Serial0/0/1
Router(config)#ip address 172.168.40.1 255.255.255.0
Router(config)#clock rate 56000
Router(config)#no shutdown

RUTAS ESTÁTICAS
Router(config)#ip route 172.168.1.0 255.255.255.0 172.168.40.2

EQUIPO BACKUP

VLAN 2
Router(config)#interface FastEthernet0/0.2
Router(config)#encapsulation dot1Q 2
Router(config)# ip address 192.168.2.1 255.255.255.0
Router(config)#glbp 2 ip 192.168.2.100
Router(config)#glbp 2 preempt
Router(config)#glbp 2 authentication text testglbp
Router(config)#glbp 2 weighting track 1 decrement 100

VLAN 3
Router(config)#interface FastEthernet0/0.3
Router(config)#encapsulation dot1Q 3
Router(config)#ip address 192.168.3.1 255.255.255.0
Router(config)#glbp 3 ip 192.168.3.100
Router(config)#glbp 3 preempt
Router(config)#glbp 3 authentication text testglbp
Router(config)#glbp 3 weighting track 1 decrement 100

VLAN 4
Router(config)#interface FastEthernet0/0.4
Router(config)#encapsulation dot1Q 4
Router(config)# ip address 192.168.4.1 255.255.255.0
Router(config)#glbp 4 ip 192.168.4.100
Router(config)#glbp 4 preempt
Router(config)#glbp 4 authentication text testglbp
Router(config)#glbp 4 weighting track 1 decrement 100

INTERFAZ SERIAL
Router(config)#interface Serial0/0/1
Router(config)#ip address 172.168.50.1 255.255.255.0
Router(config)#clock rate 56000
Router(config)#no shutdown

RUTAS ESTÁTICAS
Router(config)#ip route 172.168.1.0 255.255.255.0 172.168.50.2

EQUIPO M3
En este equipo se debe configurar las interfaces seriales y las rutas estáticas para redundancia en la Wan, lo mismo se configura en Hsrp y en Glbp

Router(config)#interface Serial0/0/0
Router(config)#ip address 172.168.40.2 255.255.255.0

Router(config)#interface Serial0/0/1
Router(config)#ip address 172.168.50.2 255.255.255.0

RUTAS ESTÁTICAS
Router(config)#ip route 192.168.2.0 255.255.255.0 172.168.40.1
Router(config)#ip route 192.168.2.0 255.255.255.0 172.168.50.1
Router(config)#ip route 192.168.3.0 255.255.255.0 172.168.40.1
Router(config)#ip route 192.168.3.0 255.255.255.0 172.168.50.1
Router(config)#ip route 192.168.4.0 255.255.255.0 172.168.40.1
Router(config)#ip route 192.168.4.0 255.255.255.0 172.168.50.1

PROTOCOLO VRRP

EQUIPO MASTER

VLAN 2
vyatta@vyatta#edit interfaces ethernet eth1
vyatta@vyatta#set vif 2 address 192.168.2.1/24
vyatta@vyatta#set vif 2 vrrp vrrp-group 2 virtual.address 192.168.2.100/24
vyatta@vyatta#set vif 2 vrrp vrrp-group 2 preempt true
vyatta@vyatta#set vif 2 vrrp vrrp-group 2 priority 150
vyatta@vyatta#commit

VLAN 3
vyatta@vyatta#edit interfaces ethernet eth1
vyatta@vyatta#set vif 3 address 192.168.3.1/24
vyatta@vyatta#set vif 3 vrrp vrrp-group 3 virtual.address 192.168.3.100/24
vyatta@vyatta#set vif 3 vrrp vrrp-group 3 preempt true
vyatta@vyatta#set vif 3 vrrp vrrp-group 3 priority 150
vyatta@vyatta#commit

VLAN 4
vyatta@vyatta#edit interfaces ethernet eth1
vyatta@vyatta#set vif 4 address 192.168.4.1/24
vyatta@vyatta#set vif 4 vrrp vrrp-group 4 virtual.address 192.168.4.100/24
vyatta@vyatta#set vif 4 vrrp vrrp-group 4 preempt true
vyatta@vyatta#set vif 4 vrrp vrrp-group 4 priority 150
vyatta@vyatta#commit

EQUIPO BACKUP

VLAN 2
vyatta@vyatta#edit interfaces ethernet eth1
vyatta@vyatta#set vif 2 address 192.168.2.10/24
vyatta@vyatta#set vif 2 vrrp vrrp-group 2 virtual.address 192.168.2.100/24
vyatta@vyatta#set vif 2 vrrp vrrp-group 2 preempt true
vyatta@vyatta#set vif 2 vrrp vrrp-group 2 priority 20
vyatta@vyatta#commit

VLAN 3
vyatta@vyatta#edit interfaces ethernet eth1
vyatta@vyatta#set vif 3 address 192.168.3.10/24
vyatta@vyatta#set vif 3 vrrp vrrp-group 3 virtual.address 192.168.3.100/24
vyatta@vyatta#set vif 3 vrrp vrrp-group 3 preempt true
vyatta@vyatta#set vif 3 vrrp vrrp-group 3 priority 20
vyatta@vyatta#commit

VLAN 4
vyatta@vyatta#edit interfaces ethernet eth1
vyatta@vyatta#set vif 4 address 192.168.4.10/24
vyatta@vyatta#set vif 4 vrrp vrrp-group 4 virtual.address 192.168.4.100/24
vyatta@vyatta#set vif 4 vrrp vrrp-group 4 preempt true
vyatta@vyatta#set vif 4 vrrp vrrp-group 4 priority 20
vyatta@vyatta#commit

RUTAS ESTATICAS

MASTER
vyatta@vyatta#set protocols static route 172.168.1.0/24 next-hop 172.168.40.2 distance 3
vyatta@vyatta#set protocols static route 172.168.1.0/24 next-hop 192.168.2.10 distance 5
vyatta@vyatta#set protocols static route 172.168.1.0/24 next-hop 192.168.3.10 distance 5
vyatta@vyatta#set protocols static route 172.168.1.0/24 next-hop 192.168.4.10 distance 5
vyatta@vyatta#set protocols static route 172.168.50.0/24 next-hop 192.168.2.10
vyatta@vyatta#set protocols static route 172.168.50.0/24 next-hop 192.168.3.10
vyatta@vyatta#set protocols static route 172.168.50.0/24 next-hop 192.168.4.10
vyatta@vyatta#commit

BACKUP
vyatta@vyatta#set protocols static route 172.168.1.0/24 next-hop 172.168.50.2 distance 3
vyatta@vyatta#set protocols static route 172.168.1.0/24 next-hop 192.168.2.1 distance 5
vyatta@vyatta#set protocols static route 172.168.1.0/24 next-hop 192.168.3.1 distance 5
vyatta@vyatta#set protocols static route 172.168.1.0/24 next-hop 192.168.4.1 distance 5
vyatta@vyatta#set protocols static route 172.168.40.0/24 next-hop 192.168.2.1
vyatta@vyatta#set protocols static route 172.168.40.0/24 next-hop 192.168.3.1
vyatta@vyatta#set protocols static route 172.168.40.0/24 next-hop 192.168.4.1
vyatta@vyatta#commit

ROUTER
vyatta@vyatta#set protocols static route 192.168.0.0/21 next-hop 172.168.40.1
vyatta@vyatta#set protocols static route 192.168.0.0/24 next-hop 172.168.50.1
vyatta@vyatta#commit