TESIS USS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

UNA UNIVERSIDAD CON ALMA DE GUERRERO

IMPLEMENTACIÓN DE PROTOCOLOS DE COMUNICACIÓN PARA MEJORAR LA DISPONIBILIDAD DE UNA RED INFORMATICA

Tesis para optar por el Título de Ingeniero De Sistemas, que presenta el bachiller

AUTOR

Cesar Juniors Cordova Rengifo

ASESOR

MG. Alex Franklin Coronado Navarro

CHICLAYO - PERÚ 2016

UNIVERSIDAD SEÑOR DE SIPÁN

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Título del proyecto de la tesis

IMPLEMENTACIÓN DE PROTOCOLOS DE COMUNICACIÓN PARA MEJORAR LA DISPONIBILIDAD DE UNA RED INFORMATICA

Aprobación del proyecto

Bach. Cordova Rengifo Cesar Juniors
Tesista

Ing. Coronado Navarro Alex Franklin
Asesor especialista

Mg. Carrión Barco Gilberto
Presidente del jurado de tesis

Ing. Villegas Cubas Juan Elías
Secretario del jurado de tesis

Ing. Coronado Navarro Alex Franklin
Vocal del jurado de tesis

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

DEDICATORIA

Dedico la presente tesis con todo mi amor y cariño a mi familia, por estar siempre a mi lado brindándome su ayuda incondicional y apoyo. En especial a mi madre y padre que si no fuese por su esfuerzo y amor mis estudios no hubiesen sido posibles.

A mis amigos por estar junto a mí todo este tiempo ayudándome a que sea posible el desarrollo de este proyecto, siempre los llevare en mi corazón

AGRADECIMIENTO

Agradezco a Dios, por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante toda la mi vida estudiantil.

Este proyecto no se podría haber llevado a cabo sin la colaboración y ayuda de un gran número de personas.

Gracias a todo el personal de la dirección de tecnologías e información por acogerme durante mis practicas pre-profesionales, especialmente agradecer a mi asesor el Ing. Alex Franklin Coronado Navarro por las asesorías en el transcurso del desarrollo de la tesis y a los ingenieros Julio Cesar Altamirano , César Minguillo Rubio quienes compartieron sus enseñanzas y conocimiento.

Gracias a toda mi familia y amigos en especial a Renzo Augusto Ariansen Moncada y José Ivan Rojas Diaz por darme su apoyo durante toda carrera.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

ÍNDICE

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Tabla de Ilustraciones

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

RESUMEN:

El surgimiento de nuevos servicios disponibles a los usuarios y los clientes plantean nuevos desafíos para el manejo y procesamiento de la información y las comunicaciones dentro de cualquier institución o empresa, razón por el cual es necesario que los servicios brindados por estas instituciones y/o empresas estén disponibles las 24 horas del día, para permitir él envió y la obtención de información por parte de los usuarios y clientes.

Se plantea la comparación de los diferentes protocolos mediante su implementación y así contribuirán con el mejoramiento y el buen funcionamiento de una red informática.

PALABRAS CLAVES:

Protocolos de comunicación, Red informática, Alta disponibilidad.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

ABSTRACT

The emergence of new services available to users and customers pose new challenges for the management and processing of information and communications within any institution or company, reason why it is necessary that the services provided by these institutions and / or companies are available 24 hours a day, to allow the sending and obtaining information from users and customers.

Comparison of different protocols through its implementation arises and thus contributes to the improvement and proper functioning of a computer network.

KEYWORDS:

Communication protocols, Network, High Availability.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

INTRODUCCIÓN

En la actualidad las redes de datos permiten compartir con carácter universal la información entre grupos de computadoras y sus usuarios; un componente vital para las grandes empresas y que estas redes de datos estén disponible las 24 horas del día.

Los sistemas de alta disponibilidad están diseñados con el fin de minimizar los tiempos de recuperación en la comunicación de la disponibilidad de red informática ante cualquier fallo de cualquier tipo.

El objetivo de esta tesis en la implementar protocolos de comunicación para mejorar la disponibilidad de la red informática, para que sirva como referencia en el futuro con la implementación.

A continuación se describe el desarrollo de los capítulos de la investigación:

En el capítulo I se muestra el problema de la investigación, especificando la situación problema a nivel internacional, la formulación del problema, delimitaciones de la investigación, justificación e importancia, objetivos generales y específicos.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

En el Capítulo II se muestra el marco teórico que sustenta científicamente la propuesta de investigación.

En el Capítulo III se muestra el marco metodológico, el cual está estructurado por la hipótesis, variables, operacionalización, población y muestra, métodos de investigación, técnicas e instrumentos y métodos de análisis de datos.

En el Capítulo IV se muestran los resultados obtenidos, en base al análisis realizado a los protocolos de alta disponibilidad. Asimismo, se muestra la discusión de los resultados.

En el Capítulo V se muestra la propuesta de la investigación capturando con imágenes la configuración y algunos estados de los equipos de telecomunicación.

En el Capítulo VI se muestran Las conclusiones y recomendaciones, orientadas a los objetivos específicos.

Finalmente, se muestran las referencias bibliográficas y en los anexos la documentación tal como: las fichas de evaluación de la propuesta e instrumento de recolección de datos.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

CAPITULO I.PROBLEMA DE INVESTIGACIÓN

1.1. Situación problemática

1.1.1. A nivel internacional:

Las redes de datos son sistemas que se diseñan y construyen en arquitecturas que pretenden servir de la mejor forma a sus objetivos de uso, estos sistemas enlazan dos puntos a través de medios físicos, para así movilizar los paquetes de datos, durante esta movilización, dichos medios físicos llegan a producir errores, o bien pueden terminar deshabilitándose por algún fallo. Una red de datos tiene que ser lo suficientemente robusta, para poder soportar cualquier tipo de eventualidad, aun así, siempre quedan brechas por donde los problemas pueden filtrarse, una de las soluciones consiste en por lo menos, mantener los puntos más críticos de las redes de datos lo más protegidos posible, tanto nivel físico como también en el resto de los niveles de una arquitectura TCP/IP, así la información que recorre a través de la red siempre estará disponible, sin errores y lo más fluida posible.

Dentro de las redes de datos, uno de los dispositivos críticos importantes son los routers, debido a que estos son los equipos periféricos en la red y mantienen la conexión con internet junto a un firewall de protección; debido a esto los routers deben ser protegidos, pero siempre queda una brecha en la que un fallo

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

inminente puede producirse, entonces se deberá buscar una solución más segura. (GALIANO, 2012).

La disponibilidad de un sistema se puede ver afectada por diferentes averías de sus componentes, a pesar de utilizar componentes cotidianos sin características especiales de fiabilidad nos interesa disponer de un sistema fiable. Si ocurre un error durante la ejecución y ocasiona una ejecución incorrecta de las funciones del sistema, se tiene una avería. Estos pasos, no se producen de forma simultánea en el tiempo, sino que existe un tiempo de inactividad, llamado “latencia del error” desde el instante en que se produce el fallo hasta que se manifiesta el error. (Cecilia M. Lasserre, 2010)

La tolerancia a fallos se basa hoy día fundamentalmente en un concepto: redundancia (Guangping, Yong, Wenhui, Gang, & Xiaoguang., and Parallel/Distributed Computing,). La investigación busca proponer una solución disponibilidad y tolerancia a fallos, soportada en servicios, mediante la duplicación de sus elementos críticos y la disposición redundante de elementos software y hardware que cooperen, bien sea en forma activa-activa o activa-pasiva, siempre en forma transparente al

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

usuario final.

Las empresas necesitan interconectar los procesos e información de tanto con la propia organización como atravesando sus fronteras con agencia 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 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% 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

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

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 eléctricos.

A los administradores de red les preocupa tener puntos de fallos 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. (NATALI DEL ROCIO YEROVILLUAY, 2010).

1.2. Formulación del problema

¿Cómo mejorar la disponibilidad de una red informática?

1.3. Delimitación de la investigación

La presente investigación se desarrolló en las instalaciones de la universidad señor de sipan, a cargo del estudiante César Juniors Córdova Rengifo junto con el ingeniero Alex Franklin Coronado Navarro como asesor especialista en los meses de Abril a Diciembre del 2015.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

1.4. Justificación e importancia

1.4.1. Científica

El aumento de la disponibilidad (implementar una solución de alta disponibilidad) hace referencia a maximizar el porcentaje de tiempo durante el que los servicios del sistema están operativos. Para aumentar la disponibilidad, implementa topologías y tecnologías que introducen redundancia. El objetivo es reducir o eliminar el número de puntos únicos de anomalía. Los puntos únicos de anomalía son elementos cuya anomalía provoca la detención de la operación de aspectos críticos del sistema.

1.4.2. Institucional

Muchas empresas y/o personas que brindan algún tipo de servicio web se encuentran en problemática que sus servicios pueden no estar disponibles por un determinado tiempo y debido a factores diferentes. La falta de disponibilidad del servicio se refleja en la molestia de los usuarios ya que el servicio puede estar no disponible por un largo tiempo, o en la pérdida de dinero.

1.4.3. Social

Actualmente las organizaciones se basan cada día más en las redes de computadoras, para sus ingresos y operaciones por ende, requieren la implementación de sistemas adicionales para

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

asegurarse que sus sistemas y aplicaciones siempre estén disponibles.

Las IT en estas organizaciones deben ofrecer un nivel continuo de disponibilidad de sus servicios.

1.5. Limitación de la investigación

En esta investigación se trabajaran con protocolos de capa 3.

1.6. Objetivos de la investigación

1.6.1. Objetivo general

Implementar protocolos de comunicación para mejorar la disponibilidad de una red informática.

1.6.2. Objetivos específicos

a) Diagnosticar el estado actual de la disponibilidad de una red informática.

b) Analizar los factores influyentes en la disponibilidad de una red informática.

c) Implementar protocolos de comunicación para mejorar la disponibilidad de una red informática.

d) Estimar los resultados que generara la implantación de protocolos de comunicación en la disponibilidad de una red informática.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

CAPITULO II.MARCO TEÓRICO

2.1. Antecedentes de estudios

2.1.1. A Nivel Internacional:

ECUADOR, RIOBAMBA. (PALOMO, 2012). En su tesis titulada "ANÁLISIS Y DISEÑO DE UNA RED DE ALTA DISPONIBILIDAD PARA CENTRALES ASTERISK BASADA EN LA TECNOLOGÍA DUNDi" De acuerdo al estudio realizado acerca de las técnicas de alta disponibilidad en redes VoIP, Heartbeat es la mejor herramienta para dar alta disponibilidad a un servicio, en este caso Asterisk; ya que siendo un software libre se adapta a las necesidades del cliente y proporciona un clúster evitando en lo más mínimo la pérdida del servicio de telefonía. Esto se ve reflejado en la utilización de un servidor de respaldo que entrará en acción cuando ocurra alguna falla en el servidor principal, tomando el control del servicio.

Con Heartbeat, la adquisición de la IP se produce en menos de un segundo. DRBD se re-configura en casi 35 segundos y luego dependiendo de la plataforma de hardware y la complejidad de las aplicaciones que se ejecuten en Asterisk puede tardar entre 10-15 segundos para que Asterisk se ponga en marcha en el servidor secundario, se sincronizan los archivos de configuración

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

y está listo para procesar las llamadas en un promedio de 48,75 segundos.

El modelo implementado en un Ambiente de Prueba haciendo uso de DRBD junto con Heartbeat optimiza en un 99.999% la disponibilidad de la solución; puesto que se crea una partición virtual la misma que será compartida entre los servidores que se realice el clustering.

ECUADOR, GUAYAQUIL, (LEÓN FEIJOÓ, 2010). En su tesis titulada “DISEÑO DE ALTA DISPONIBILIDAD EN SERVIDORES SOLARIS 10 PARA APLICACIÓN EN EL CENTRO DE COMPUTO DE LA U.C.S.G”, En el proyecto se ha podido determinar que la situación actual del servidor de aplicaciones de la U.C.S.G, que debería mejorar con respecto a la alta disponibilidad que al momento no cuenta.

El diseño propuesto para este trabajo, consta de dos servidores con iguales o similares características, y un repositorio de la base de datos, el mismo que estará conectado a la red, para lograr la alta disponibilidad del servicio.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

SANGOLQUI, ECUADOR, (GALIANO, 2012). En su tesis titulada "Solución de Firewall con alta disponibilidad para redes corporativas utilizando Vyatta con virtualización". Como principal conclusión se determina que el sistema Vyatta cumple con todos los requerimientos de una red corporativa de pequeña o gran escala, si se desea usar la versión libre se pueden encontrar algunas limitaciones que se analizarán más adelante, pero en definitiva el sistema es completo y uno de los competidores más grandes, incluso para dispositivos físicos como Cisco, la facilidad que este provee para su configuración hace que aparte de dar varias opciones para solucionar problemas, también sean estas muy viables y de configuración rápida.

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

El protocolo VRRP que es el que se implementó para proveer de alta disponibilidad a la red corporativa usa paquetes que se envían después de intervalos de tiempo determinados, en

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

conclusión estos paquetes son bastante pequeños y el tiempo total que toma su análisis es despreciable por lo que el funcionamiento del sistema es bastante aceptable, una de las características que se debe tomar en cuenta es que, en el caso de que exista un fallo del sistema primario el sistema secundario inunda la red con paquetes ARP, informando del fallo a los distintos usuarios conectados, este intercambio de sistema toma tiempos menores a los 40 mili segundos, por lo que el índice de disponibilidad del sistema sería prácticamente del 100%, aun así no se debe dejar de tomar en cuenta, que la red en estudio es una red corporativa, en caso de redes más grandes este porcentaje aumentará, aun así el sistema es excelente para proveer tolerancia a fallos a las redes de datos. En relación a la configuración de stateful failover que se levantó en el sistema, se puede concluir mediante las pruebas que se hicieron, que el sistema respondió satisfactoriamente y como se esperaba, entre las pruebas de stateful failover y las de alta disponibilidad se deduce claramente que las sesiones levantadas en el sistema primario son transparentemente levantadas en el sistema backup, por lo que si existiese un fallo en el sistema primario el secundario tomará la administración del sistema rápida y efectivamente.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

ECUADOR, RIOBAMBA, (YEROVI & VALERIA, 2010). En su tesis titulada “Análisis de los protocolos de alta disponibilidad de gateways en la interconectividad LAN/WAN aplicadas al diseño de redes de campus”. Como conclusiones los protocolos de alta disponibilidad permiten que los servicios estén disponibles la mayor parte de tiempo ya que poseen un equipo backup que actúa en el caso de que el equipo master haya perdido.

Una red de alta disponibilidad provee rutas alternas a través de la infraestructura a fin de que le acceso a los servidores clave sea posible el 100% del tiempo.

Al trabajar con los protocolos de alta disponibilidad en el ambiente Cisco 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.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

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

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.

2.2. Estado del arte

1. 2002

Se pueden hablar de mecanismos que establecen las pautas de disponibilidad de acuerdo sobre todo a la tecnología que se esté empleando en cada momento.

De una forma genérica podríamos hablar del término "alta disponibilidad" aplicado a un sistema computacional del que se requiere un funcionamiento continuo. Para conseguir esto, los varemos son varios y se aplican en distintos niveles.

La alta disponibilidad se aplica a toda la gama de soluciones que

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

sostienen los sistemas de información de las empresas: bases de datos, cortafuegos, servidores web, etc. Si bien, los mecanismos que se emplean pueden ser distintos en función del entorno. (AVAILABILITY, 2002).

2. 2006

La influencia de la información de los fallos sobre el enrutamiento diverso. Además, hemos introducido un algoritmo de enrutamiento diverso que mejora la disponibilidad de las conexiones bajo demanda y hemos definido la duración umbral THT. (Luis Velasco, 2006).

3. 2010

Con los avances en la red de banda ancha, muchas personas y empresas dependen en gran medida en las aplicaciones y servicios de Internet. Instalaciones críticas, como los centros de datos, la comunicación centros comerciales, centros de servicios financieros y centros de servicios de telecomunicaciones deben garantizar un cierto grado de continuidad operacional durante el período de servicio. Por lo tanto, es importante para un proveedor de servicios para construir un entorno de alta disponibilidad para proporcionar servicios continuos para los usuarios, ya sea para

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

instalar nuevos componentes o repare los componentes existentes.

Si un sistema no se puede acceder, se dice que estará disponible. Generalmente, el término el tiempo de inactividad se usa para referirse a los períodos en que una red o sistema no está disponible.

Disponibilidad de la red se puede mejorar, ya sea por mejoras incrementales en el componente disponibilidad o mediante la provisión de componentes redundantes en paralelo. Pero es costoso de implementar o utilizar componentes de alta disponibilidad.

Por lo tanto, la adición de los routers redundantes a un router de red para lograr el objetivo de alta la disponibilidad es un diseño familiar. En general, este enfoque consiste en un grupo de routers, donde uno es el router activo y los otros están en espera. Es decir, el activo enrutador ejecuta el proceso de enrutamiento, mientras que un router de espera se prepara para asumir la el papel del router activo de inmediato si el router activo falló. Para establecer router de red redundancia, VRRP (Virtual Router Redundancy

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Protocol) y HSRP (Hot Standby Router Protocol) son dos diseños más familiares. VRRP es una redundancia no propietaria protocolo descrito en el RFC 3768 y HSRP es un protocolo propietario de Cisco redundancia se describe en el RFC 2281. VRRP se basa en los conceptos de propiedad HSRP de Cisco. Estas dos tecnologías son similares en concepto, pero no compatible. (CHIA-TAI TSAI, 2010).

4. 2011

Disponibilidad siempre han sido el área desafiante y mayormente enfocada más crítico de todos los campo en el mundo si se trata de tecnología de la información, Banca, ferroviario, aéreo, Salud, Transporte, Industria de Alimentos, Manufactura o cualquier negocio que está directamente relacionado con servicio, contrato, acuerdo de nivel de servicio y la riqueza. Ya que está directamente relacionado con los ingresos y dinero por lo que hoy todas las organizaciones relacionadas con gastar mucho tiempo y dinero en este campo para obtener alta disponibilidad para su respectivo entorno.

Hoy en día muchas de las opciones están disponibles en el mundo para lograr una alta disponibilidad para todos y cada uno

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

respectiva tecnología y la organización, por ejemplo en una pequeña prensa de impresión siempre hay una copia de seguridad de la máquina de impresión de manera que en caso de fallo de trabajo de la máquina primaria se puede hacer desde la máquina secundaria que también llaman ser la recuperación de desastres o de la máquina de conmutación por error. Pero sí que es un forma costosa para lograr una alta disponibilidad porque para eso se necesita una segunda máquina que hará causar el mismo costo que la máquina primaria, pero esto le dará una confianza que en caso de cualquier problema con la máquina, el trabajo y los ingresos primaria relacionada con el envío solicitado no será impacto. (Research Scholar, 2011).

5. 2012

La implementación de sistemas de alta disponibilidad, surge principalmente con el propósito de mitigar el problema de la pérdida del servicio por eventos inesperados. Dependiendo del entorno para el cual se pretende implementar, han sido desarrolladas una amplia variedad de herramientas informáticas para la gestión de clústeres, tanto en versiones pagas como gratuitas. (BECERRA, 2012).

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

6. 2013

La importancia actual de los servicios en la nube plantea un reto a las soluciones de alta disponibilidad y escalabilidad existentes. Cada vez se necesitan servidores más flexibles y más escalables, que sean capaces de atender a cambios bruscos en la demanda del servicio. El Departamento de Desarrollo Transversal de Telefónica I+D es consciente de esto y requiere de soluciones HA y de escalabilidad para sus servicios PopBox y Rush. (González, 2013).

7. 2015

En este trabajo he tenido la oportunidad de investigar y aprender un gran conjunto de nuevas tecnologías orientadas a web de alta disponibilidad. Gracias a esto, he podido comprender como funcionan los sistemas actuales, cuales son los actores participantes en montajes complejos e incluso llegar a montar uno propio.

Debido a esto, he conseguido plasmar mis nuevos conocimientos y trabajos en una guía en la que se explican las bases de los sistemas orientados a web, impartiendo unas explicaciones previas y proporcionando los ficheros específicos de

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

configuración para que cualquiera que lea este documento, con unas pequeñas bases, pueda montar un sistema similar que se adecue a sus necesidades. (Moreno, 2015).

2.3. Base teórica científicas

2.3.1. Disponibilidad:

La disponibilidad de un elemento, si un solo componente o un sistema más amplio, se define a menudo como:

$$A = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}}$$

Donde MTTF denota " Mean Time al fracaso " y MTTR " tiempo medio de reparación ", respectivamente. El cociente es fácil de interpretar como el tiempo que un sistema está disponible como una fracción de todos los tiempos. Una estimación más cautelosa es la disponibilidad encontrado por vez utilizando el " Máximo reparar ", que corresponde a un peor caso escenario.

La distribución exponencial es central en la mayor parte del trabajo es la fiabilidad y la distribución más utilizada en el análisis de confiabilidad aplicada. La razón de esto es su matemática simplicidad y el hecho de que da vida modelos realistas para ciertos tipos de artículos, por lo menos como una primera aproximación.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Si el tiempo hasta el fallo de un elemento T se distribuye de manera exponencial, que tiene la siguiente wellknown la función de densidad de probabilidad:

$$f(t) = \begin{cases} \lambda \cdot e^{-\lambda t} & \text{for } t > 0, \lambda > 0 \\ 0 & \text{otherwise} \end{cases}$$

El MTTF correspondiente es simplemente el recíproco del parámetro λ :

$$\text{MTTF} = \frac{1}{\lambda}$$

La asunción de vida distribuido exponencialmente tiene dos implicaciones importantes:

Un elemento utilizado es estocásticamente tan buena como una nueva, es decir, no hay ninguna razón para reemplazar un elemento de trabajo.

Cuando se estima MTTF etc., es suficiente para recoger datos sobre el tiempo observado en operación, y el número de fracasos. No hay necesidad de hacer un seguimiento de la edad de artículos.

Con las mismas hipótesis sobre el tiempo medio de reparación, esta distribución puede ser igualmente descrita por un parámetro

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

μ:

$$\mathrm{MTTR} = \frac{1}{\mu}$$

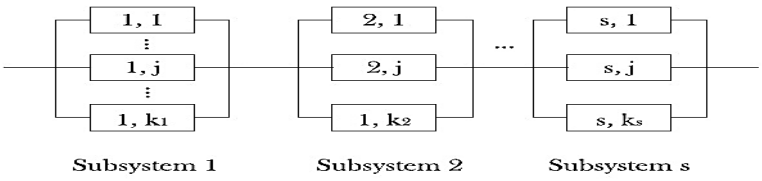
El A_{avg} la disponibilidad media de un componente de ahora se puede calcular a partir de:

$$A_{\mathrm{avg}} = \frac{\mu}{\mu + \lambda}$$

Sistemas rara vez constan de un solo componente, y muchas veces, estos componentes son conectados en paralelo. El caso en el que tenemos i subsistemas, donde cada subsistema consta de componentes k_i paralelas, y donde los subsistemas están conectados en serie es representado en la Ilustración 1.

Suponiendo MTTF distribuido de manera exponencial y MTTR, la disponibilidad promedio de este caso general se puede obtener como sigue.

Ilustración 1-Una muestra diagrama de bloques el caso general de series paralelas sistemas



$$A_{\mathrm{avg}} = \prod_{i=1}^{s}\left(1 - \left(\frac{\lambda_i}{\lambda_i + \mu_i}\right)^{k_i}\right) = \prod_{i=1}^{s}\left(1 - (1 - A_i)^{k_i}\right)$$

Fuente:http://link.springer.com/article/10.1007%2Fs11219-011-9141-z

Esto supone que las tasas de fallo y reparación son los mismos para todos i componentes de un subsistema $(\lambda_i \text{ and } \mu_i)$:

La asunción de las distribuciones exponenciales se discute más a fondo en la Sección.

Análisis de disponibilidad inter e intracomponentes

En la Ilustración 1, como en toda la sección de la teoría hasta ahora, la disponibilidad intrínseca de cada componente se tomado como un hecho bruto. En un sentido, los componentes se consideran como cajas negras, y todos los análisis se llevan a cabo a nivel de sistemas. Sin embargo, esto es claramente una simplificación. En realidad, las componentes no son cajas negras, pero tienen características incluyendo características internas que pueden ser afectados a fin de mejorar la disponibilidad resultante del sistema como un todo.

La principal contribución de este trabajo, sin embargo, es en el campo de lo que podría llamarse análisis por una disponibilidad se intentó encontrar las características internas de un único componente necesario para calcular su disponibilidad intrínseca. Más específicamente, los " componentes " bajo escrutinio son

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

componentes de TI de las grandes empresas, por así decirlo, pero partes de los grandes sistemas aún más grandes, son las arquitecturas empresariales enteros.

No hace falta decir, un modelo de disponibilidad completa para una empresa, la arquitectura formada por todos los sistemas de TI en una empresa necesita tener en cuenta tanto la disponibilidad inter e intracomponentes. Por lo tanto, mientras que la principal aportación del papel es un modelo bayesiano experto para predecir la disponibilidad de sistemas de TI de la empresa. (Ulrik Franke, 2012).

2.3.2. Metodología de Desarrollo CISCO

Según (METODOLOGÍA DEL DESARROLLO CON CISCO, 2014) Cisco, el mayor fabricante de equipos de red, describe las múltiples fases por las una red atraviesa utilizando el llamado ciclo de vida de redes PDIOO (Planificación –Diseño –Implementación –Operación –Optimización).

a) Fase de planificación: Los requerimientos detallados de red son identificados y la red existente es revisada.

b) Fase de diseño: La red es diseñada de acuerdo a los requerimientos iniciales y datos adicionales recogidos durante el análisis de la red existente. El diseño es refinado con el cliente.

c) Fase de implementación: La red es construida de acuerdo al diseño aprobado

d) Fase de operación: La red es puesta en operación y es monitoreada. Esta fase es la prueba máxima del diseño.

e) Fase de optimización: Durante esta fase, los errores son detectados y corregidos, sea antes que los problemas surjan o, si no se encuentran problemas, después de que ocurra una falla. Si existen demasiados problemas, puede ser necesario rediseñar la red.

FASE I:

Se presenta una descripción de las problemáticas bien detalladas y la propuesta del grupo de proyecto sobre cómo pueden trabajar contra la problemática por la que va pasando la empresa.

FASE II:

a) Se comienzan a recopilar todos los requerimientos de la empresa.

b) Se hace el subneteo.

c) Se asignan los Ip's para las computadoras de la empresa.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

FASE III:

a) Se hace el diseño físico de la red

b) Configuración de las VLAN'S y asignación de puertos a las VLAN'S.

c) Configuración de los servidores.

d) Modelo de red: Basado en servidor.

e) Configuración de los clientes de la red.

f) Distribución del cableado.

FASE IV:

a) Diseño físico y lógico de la red. Representado en el simulador GNS 3.

b) Diseño de la red LAN y VLAN.

2.3.3. Trama

Atributos de la trama de Ethernet

Encapsulamiento de Ethernet

Desde la creación de Ethernet en 1973, los estándares han evolucionado para especificar versiones más rápidas y flexibles de la tecnología. Esta capacidad que tiene Ethernet de evolucionar con el paso del tiempo es una de las principales razones por las que se ha popularizado. Las primeras versiones de Ethernet eran relativamente lentas, con una velocidad de

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

10 Mbps. Las últimas versiones de Ethernet funcionan a 10 Gigabits por segundo e incluso más rápido. En la Ilustración 2, se destacan los cambios en las diferentes versiones de Ethernet.

En la capa de enlace de datos, la estructura de la trama es casi idéntica para todas las velocidades de Ethernet. La estructura de la trama de Ethernet agrega encabezados y tráilers a la PDU de Capa 3 para encapsular el mensaje que se envía.

Tanto el tráiler como el encabezado de Ethernet cuentan con varias secciones de información que utiliza el protocolo Ethernet. Cada sección de la trama se denomina campo. Como se muestra en la figura 2, hay dos estilos de entramado de Ethernet:

El estándar IEEE 802.3 de Ethernet que se actualizó varias veces para incluir nuevas tecnologías.

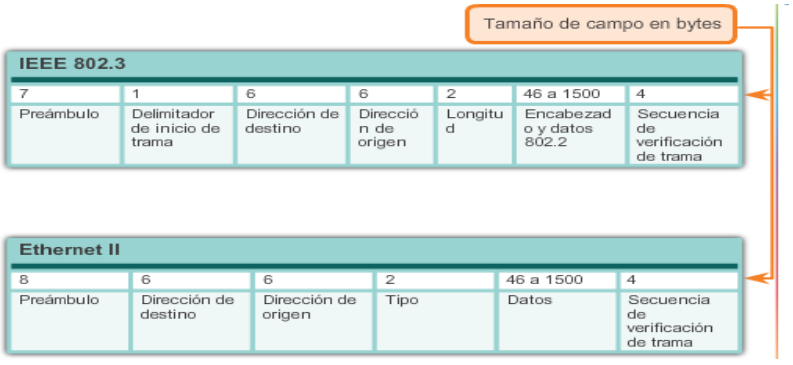
El estándar DIX de Ethernet que ahora se denomina “Ethernet II”.

Las diferencias entre los estilos de tramas son mínimas. La diferencia más importante entre los dos estándares es el agregado de un delimitador de inicio de trama (SFD) y el cambio del campo Tipo por el campo Longitud en el estándar 802.3.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Ethernet II es el formato de trama de Ethernet utilizado en las redes TCP/IP.

Ilustración 2- Comparación de estructuras de trama y tamaño de campo de Ethernet y del estándar 802.



http://aula.salesianosatocha.es/web/ccna5.1/course/module5/index.html#5.1.2.1

Tamaño de la Trama de Ethernet

Tanto el estándar Ethernet II como el IEEE 802.3 definen el tamaño mínimo de trama en 64 bytes y el tamaño máximo de trama en 1518 bytes. Esto incluye todos los bytes del campo Dirección MAC de destino a través del campo Secuencia de verificación de trama (FCS). Los campos Preámbulo y Delimitador de inicio de trama no se incluyen en la descripción del tamaño de una trama.

Cualquier trama con menos de 64 bytes de longitud se considera un "fragmento de colisión" o "runt frame" y las estaciones receptoras la descartan automáticamente.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

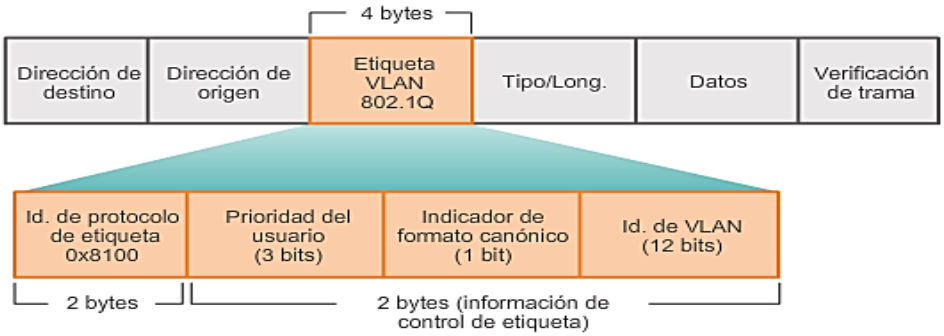
El estándar IEEE 802.3ac, publicado en 1998, amplió el tamaño de trama máximo permitido a 1522 bytes. Se aumentó el tamaño de la trama para que se adapte a una tecnología denominada Red de área local virtual (VLAN). Las VLAN se crean dentro de una red conmutada y se presentarán en otro curso. Además, muchas tecnologías de calidad de servicio (QoS) hacen uso del campo Prioridad del usuario para implementar diversos niveles de servicio, como el servicio de prioridad para el tráfico de voz. En la ilustración 3, se muestran los campos contenidos en la etiqueta VLAN 802.1Q.

Si el tamaño de una trama transmitida es menor que el mínimo o mayor que el máximo, el dispositivo receptor descarta la trama. Es posible que las tramas descartadas se originen en colisiones u otras señales no deseadas y, por lo tanto, se consideran no válidas.

En la capa de enlace de datos, la estructura de la trama es casi idéntica. En la capa física, las diferentes versiones de Ethernet varían en cuanto al método para detectar y colocar datos en los medios.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Ilustración 3- los 4 bytes adicionales permiten tecnologías de QoS y Vlan.



http://aula.salesianosatocha.es/web/ccna5.1/course/module5/index.html #5.1.2.1

Introducción a la Trama de Ethernet

Los campos principales de la trama de Ethernet son los siguientes:

1. **Campos Preámbulo y Delimitador de inicio de trama:** los campos Preámbulo (7 bytes) y Delimitador de inicio de trama (SFD), también conocido como "Inicio de trama" (1 byte), se utilizan para la sincronización entre los dispositivos emisores y receptores. Estos ocho primeros bytes de la trama se utilizan para captar la atención de los nodos receptores. Básicamente, los primeros bytes le indican al receptor que se prepare para recibir una trama nueva.
2. **Campo Dirección MAC de destino:** este campo de 6 bytes es el identificador del destinatario previsto. Como

recordará, la Capa 2 utiliza esta dirección para ayudar a los dispositivos a determinar si la trama viene dirigida a ellos. La dirección de la trama se compara con la dirección MAC del dispositivo. Si coinciden, el dispositivo acepta la trama.

Campo Dirección MAC de origen: este campo de 6 bytes identifica la NIC o la interfaz que origina la trama.

3. Campo Longitud: para todos los estándares IEEE 802.3 anteriores a 1997, el campo Longitud define la longitud exacta del campo de datos de la trama. Esto se utiliza posteriormente como parte de la FCS para garantizar que el mensaje se reciba adecuadamente. Por lo demás, el propósito del campo es describir qué protocolo de capa superior está presente. Si el valor de los dos octetos es igual o mayor que 0x0600 hexadecimal o 1536 decimal, el contenido del campo Datos se decodifica según el protocolo EtherType indicado. Por otro lado, si el valor es igual o menor que el hexadecimal de 0x05DC o el decimal de 1500, el campo Longitud se está utilizando para indicar el uso del formato de trama de IEEE 802.3. Así se diferencian las tramas de Ethernet II y 802.3.

4. Campo Datos: este campo (de 46 a 1500 bytes) contiene los datos encapsulados de una capa superior,

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

que es una PDU de capa 3 genérica o, más comúnmente, un paquete IPv4. Todas las tramas deben tener al menos 64 bytes de longitud. Si se encapsula un paquete pequeño, se utilizan bits adicionales conocidos como "relleno" para incrementar el tamaño de la trama al tamaño mínimo.

5. **Campo Secuencia de verificación de trama (FCS):** este campo de 4 bytes se utiliza para detectar errores en una trama. Utiliza una comprobación de redundancia cíclica (CRC). El dispositivo emisor incluye los resultados de una CRC en el campo FCS de la trama. El dispositivo receptor recibe la trama y genera una CRC para buscar errores. Si los cálculos coinciden, significa que no se produjo ningún error. Los cálculos que no coinciden indican que los datos cambiaron y, por consiguiente, se descarta la trama. Un cambio en los datos podría ser resultado de una interrupción de las señales eléctricas que representan los bits.

Ilustración 4- Campos de la Trama de Ethernet.

IEEE 802.3

7	1	6	6	2	46 a 1500	4
Preámbulo	Delimitador de inicio de trama	Dirección de destino	Dirección de origen	Longitud	Encabezado y datos de 802.2	Secuencia de verificación de trama

Fuente:http://aula.salesianosatocha.es/web/ccna5.1/course/module5/index.html#5.1.2.3

(Cisco Systems I. , Introducción a redes, 2013)

2.3.4. HSRP: Hot Standby Router Protocol

HSRP es el método estándar de Cisco de proporcionar alta disponibilidad de la red, proporcionando primer hop redundancia para hosts IP en una LAN IEEE 802 configurado con una dirección IP de puerta de enlace predeterminada. Permite a un conjunto de interfaces de router a trabajen juntos para presentar la apariencia de un solo enrutador o puerta de enlace predeterminada virtual para los host en un LAN. Cuando HSRP está configurado en una red o segmento, proporciona un control de acceso a medios virtuales (MAC) y una dirección IP que se comparte entre un grupo de routers configurados. HSRP permite dos o más routers HSRP estén configurados para utilizar la dirección MAC y la dirección de red IP de un router virtual.

En un grupo de Routers HSRP pueden ser cualquier interfaz del router que soporta HSRP, incluidos los puertos enrutados y cambiar las interfaces virtuales (SVIS) en el interruptor.

HSRP proporciona alta disponibilidad de la red al proporcionar redundancia para el tráfico IP de hosts en redes.

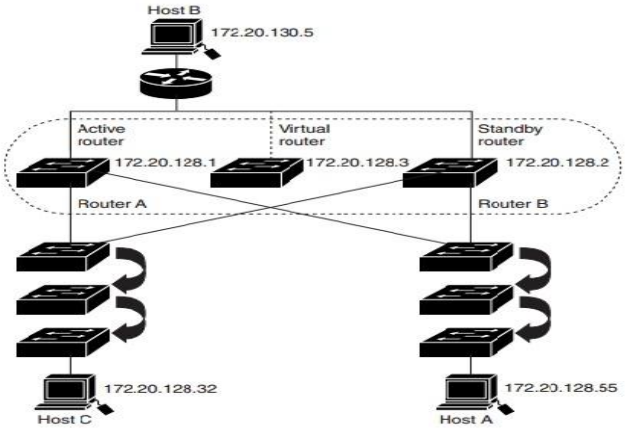
Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

La ilustración 5 muestra un segmento de una red configurada para HSRP. Cada router está configurado con el Dirección MAC y la dirección de red IP del router virtual. En lugar de la configuración de los hosts en la red con la dirección IP del router A, se les configura con la dirección IP del router virtual como su router por defecto. Cuando Host C envía paquetes al host B, que los envía a la dirección MAC del router virtual. Si por alguna razón, el Router A detiene la transferencia de paquetes, el router B responde a la dirección IP virtual y la dirección MAC virtual se convierte en el router activo, asumiendo las funciones de routers activos.

El Anfitrión C sigue utilizando la dirección IP del router virtual para hacer frente a los paquetes destinados por el Host B, el Router B ahora recibe y envía. Hasta el Router A reanuda el funcionamiento, HSRP permite Router B proporcionar un servicio ininterrumpido a los usuarios en el segmento de host de C que necesitan comunicarse con los usuarios de Host Segmento B y también sigue llevando a cabo su función normal de los paquetes de manejo entre el host A y Host B.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Ilustración 5- Típica Configuración HSRP



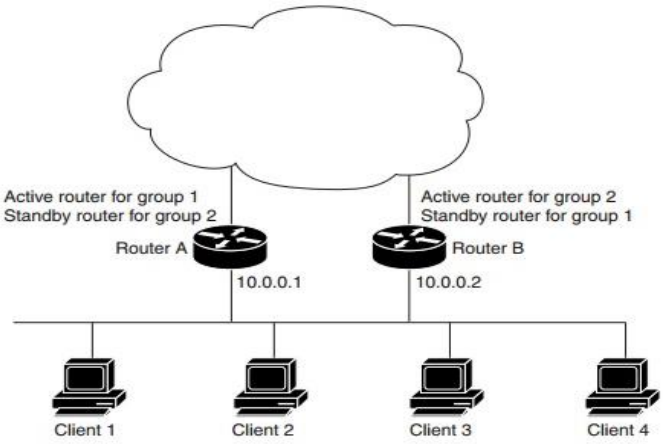
Fuente:http://www.cisco.com/c/en/us/td/docs/switches/metro/me3400e/software/release/12-2_58_se/configuration/guide/ME3400e_scg/swhsrp.pdf

HSRP Múltiple

El switch soporta HSRP múltiple (MHSRP), una extensión de HSRP que permite el intercambio de carga entre dos o más grupos HSRP. Puede configurar MHSRP para lograr el equilibrio de carga y de utilizar dos o más grupos de espera (y caminos) de una red de acogida a una red de servidores. En la Ilustración 6, la mitad de los clientes son configurados para el Router A, y la mitad de los clientes están configurados para el router B. En conjunto, la configuración para los Routers A y B establece dos grupos HSRP. Para el grupo 1, el Router A es el router activo por defecto porque tiene la prioridad más alta asignada, y Router B es el router

espera. Para el grupo 2, el Router B es el router activo por defecto, ya que tiene la prioridad más alta asignada, y el Router A es el modo de espera router. Durante el funcionamiento normal, los dos routers comparten la carga de tráfico IP. Cuando cualquiera de los enrutadores se convierte disponible, el otro router se activa y asume las funciones de transferencia de paquetes del router que no está disponible.

Ilustración 6- MHSRP Reparto De Carga



Fuente:http://www.cisco.com/c/en/us/td/docs/switches/metro/me3400e/software/release/12-2_58_se/configuration/guide/ME3400e_scg/swhsrp.pdf

Operación HSRP

La mayoría de los hosts IP tienen una dirección IP de un único dispositivo configurado como puerta de enlace predeterminada. Cuando se utiliza HSRP, el HSRP virtual Dirección IP está

configurado como puerta de enlace predeterminada del host en lugar de la Dirección IP del dispositivo.

Cuando HSRP se configura en un segmento de red, proporciona una dirección MAC virtual y una dirección IP que es compartida entre un grupo de dispositivos de funcionamiento HSRP. La dirección de este HSRP group se refiere a la dirección IP virtual. Uno de estos dispositivos es seleccionado por el protocolo que el dispositivo activo. El dispositivo activo recibe y enruta los paquetes destinados a la dirección de MAC del grupo. Para los dispositivos que ejecutan n HSRP, se asignan direcciones n + 1 IP y MAC.

HSRP detecta cuando el dispositivo activo designado falla, momento en el que un dispositivo de espera seleccionado asume el control de las direcciones MAC e IP del grupo Hot Standby. Un nuevo dispositivo de espera también se selecciona en ese momento.

HSRP utiliza un mecanismo de prioridad para determinar qué el dispositivo configurado es ser el dispositivo activo predeterminado. Para configurar un dispositivo como el

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

dispositivo activo, se le asigna una prioridad más alta que la prioridad de todos los demás dispositivos configurados HSRP. La prioridad por defecto es 100, por lo que si usted acaba de configurar un dispositivo a tener una prioridad más alta, ese dispositivo será el dispositivo activo por defecto.

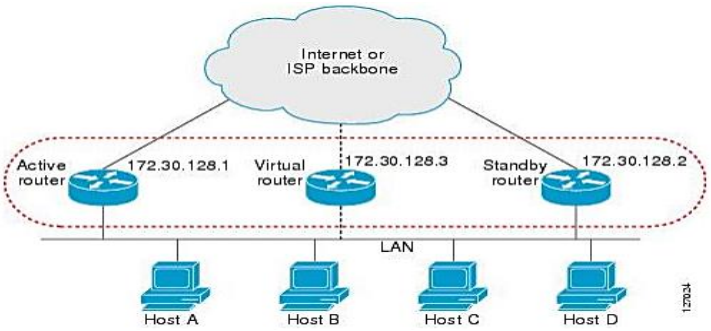
Los dispositivos que se están ejecutando envíos HSRP y reciben mensajes hola basado en UDP multidifusión para detectar fallo del dispositivo y para designar dispositivos activos y de reserva. Cuando el dispositivo activo falla para enviar un mensaje de saludo en un período de tiempo configurable, el dispositivo de espera con la prioridad más alta se convierte en el dispositivo activo. La transición de las funciones de reenvío de paquetes entre dispositivos es completamente transparente para todos los hosts de la red.

La siguiente ilustración 7 muestra una red configurada para HSRP. Al compartir una dirección IP y la dirección MAC virtual, dos o más dispositivos pueden actuar como un solo router virtual. El dispositivo virtual no existe físicamente, pero representa la puerta de enlace predeterminada común para los dispositivos que están configurados para proporcionar copia de seguridad el uno

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

al otro. No es necesario para configurar los hosts de la LAN con la dirección IP del dispositivo activo. En su lugar, les configura con la dirección IP (dirección IP virtual) del dispositivo virtual como su puerta de enlace predeterminada. Si el dispositivo activo falla para enviar un mensaje de saludo en el plazo de tiempo configurable, el dispositivo de espera se hace cargo y responde a las direcciones virtuales y se convierte en el dispositivo activo, asumiendo las funciones de dispositivos activos.

Ilustración 7- Topología HSRP



Fuente:http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-sy/fhp-15-sy-book/Configuring-HSRP.pdf

Beneficios HSRP

Redundancia

HSRP emplea un esquema de redundancia que es tiempo probado y desplegado ampliamente en redes de gran tamaño.

Conmutación por error rápida

HSRP proporciona conmutación por error rápida transparente del dispositivo de primer hop.

Preferencias:

Preemption permite que un dispositivo de espera convertirse en activo durante un período de tiempo configurable.

Autenticación:

HSRP Message Digest 5 (MD5) algoritmo de autenticación protege contra software HSRP-spoofing y usos el algoritmo MD5 estándar de la industria para mejorar la fiabilidad y la seguridad.

HSRP BFD Peering

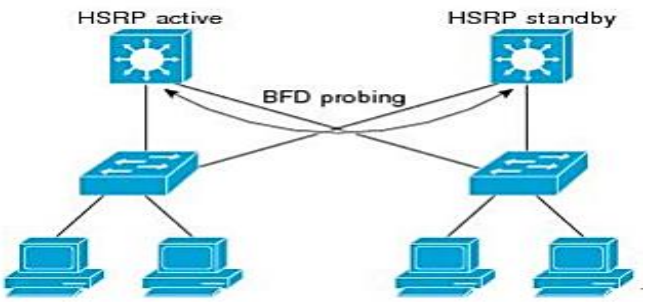
Esta función está activada de forma predeterminada. El dispositivo de espera HSRP aprende la dirección IP real del dispositivo activo y de los mensajes hello HSRP. El dispositivo de espera registra como cliente BFD y pide que se le notifique si el dispositivo activo y deja de estar disponible. Cuando BFD determina que las conexiones han fallado entre el dispositivo de espera y dispositivos activos, notificará HSRP en el dispositivo de espera que se llevará de inmediato el cargo de dispositivo activo.

BFD proporciona rápidamente la detección de fallos BFD pares

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

de tiempos independientes de todos los tipos de medios, encapsulados, topologías, y protocolos de enrutamiento como, Border Gateway Protocol (BGP), y el mejorado Routing Protocol (EIGRP), Hot Standby Router Protocol (HSRP), Sistema Intermedio a Intermedio System (IS-IS), y Open Shortest Path First (OSPF). Mediante el envío de avisos rápidos de detección de incumplimiento de los protocolos de enrutamiento en el dispositivo local para iniciar el proceso de recalculo de la tabla de enrutamiento, BFD contribuye a reducir en gran medida general el tiempo de convergencia de red. La siguiente figura muestra una red simple con dos dispositivos HSRP y BFD.

Ilustración 8- HSRP BFD Peering



Fuente: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-sy/fhp-15-sy-book/Configuring-HSRP.pdf

(Cisco Systems I. , Configuring HSRP, VRRP, and GLBP, 2012).

2.3.5. Virtual Router Redundancy Protocol (VRRP)

El Virtual Router Redundancy Protocol (VRRP) es un protocolo de elección que asigna dinámicamente la responsabilidad de uno o más enrutadores virtuales a los routers VRRP en una LAN, permitiendo que varios routers en un enlace multiacceso puedan utilizar la misma dirección IP virtual. Un router VRRP está configurado para ejecutar el VRRP protocolo junto con uno o más de otros routers conectados a una LAN. En una configuración de VRRP, uno enrutador es elegido como el maestro router virtual, con los otros routers en calidad de las copias de seguridad en caso de que lo virtual maestro enrutador falla.

Operación VRRP

Hay varias maneras de un cliente LAN puede determinar qué enrutador debe ser el primer salto a un particular, destino remoto. El cliente puede utilizar un proceso dinámico o configuración estática. Ejemplos de dinámica descubrimiento de enrutadores son los siguientes:

Proxy ARP-El cliente utiliza Address Resolution Protocol (ARP) para llegar al destino que quiere llegar, y un router

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

responderá a la petición ARP con su propia dirección MAC.

El protocolo de enrutamiento cliente escucha a las actualizaciones de protocolos de enrutamiento dinámico (por ejemplo, de Routing Information Protocol (RIP)) y forma su propia tabla de enrutamiento.

ICMP Router Discovery Protocol (PDRI) cliente, El cliente ejecuta un mensaje de control de Internet Protocolo (ICMP) cliente de descubrimiento de enrutadores.

El enrutador virtual, que representa un grupo de routers, también se conoce como un grupo VRRP.

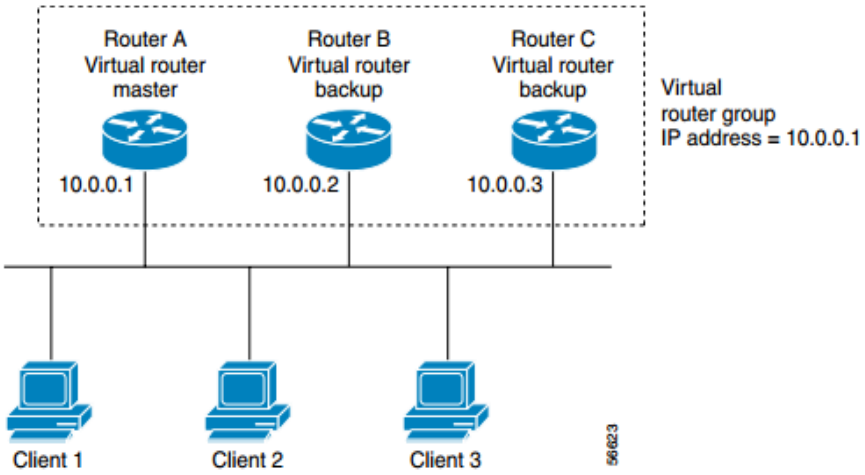
VRRP se admite en Fast Ethernet y las interfaces Gigabit Ethernet, en MPLS VPN, VRF-aware, VPNs MPLS y VLAN.

La Ilustración 9 muestra una topología de LAN en la que está configurado VRRP. En este ejemplo, Routers A, B, y C son Routers VRRP (routers que ejecutan VRRP) que componen un router virtual. La dirección IP del router virtual es el mismo que el configurado para la interfaz Gigabit Ethernet del Router A

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

(10.0.0.1).

Ilustración 9- Basic VRRP Topology



Fuente:http://www.cisco.com/c/en/us/td/docs/ios/ios_xe/ipapp/configuration/guide/2_xe/ipapp_xe_book/ipapp_vrrp_xe.pdf

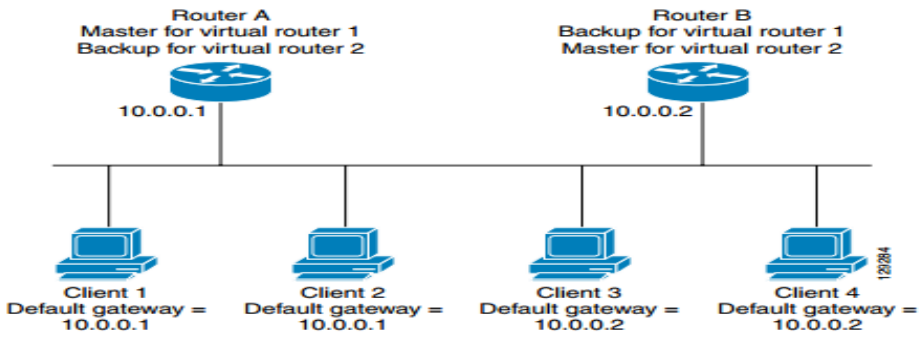
Debido a que el enrutador virtual utiliza la dirección IP de la interfaz física Gigabit Ethernet del Router A, Router A asume el papel del maestro enrutador virtual y también se conoce como el propietario de la dirección IP. Como el maestro enrutador virtual, el Router A controla la dirección IP del router virtual y es responsable de reenvío de paquetes enviados a esta dirección IP. Clientes 1 a 3 se configuran con la puerta de enlace predeterminada Dirección IP 10.0.0.1.

Routers B y el C sirven como copias de seguridad del router virtual. Si router virtual el maestro falla, el router configurado con

la prioridad más alta se convertirá en el maestro enrutador virtual y proporcionar ininterrumpido servicio para la LAN instalados. Cuando el Router A se recupera, se convierte en el maestro router virtual nuevo.

En la ilustración 10 muestra una topología de LAN en la que VRRP está configurado para que Routers A y B comparten el tráfico desde y hacia los clientes 1 a 4 y que los Routers A y B actúan como copias de seguridad del router virtuales.

Ilustración 10- Load Sharing and Redundancy VRRP Topology



Fuente:http://www.cisco.com/c/en/us/td/docs/ios/ios_xe/ipapp/configuration/guide/2_xe/ipapp_xe_book/ipapp_vrrp_xe.pdf

En esta topología, los dos routers virtuales se configuran. Para el router virtual 1, el Router A es el propietario de la dirección IP 10.0.0.1 y es el router virtual maestro, el router B es la copia de seguridad del router virtual al router A. Clientes 1 y 2 están configurados con la dirección IP de puerta de enlace

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

predeterminada de 10.0.0.1.

Para router virtual 2, Router B es el propietario de la dirección IP 10.0.0.2 y maestro router virtual, y el Router A es la copia de seguridad del router virtual al router B. Clientes 3 y 4 están configurados con la puerta de enlace predeterminada IP dirección 10.0.0.2.

Beneficios VRRP

Redundancia

VRRP permite configurar múltiples routers como el router de gateway por defecto, lo que reduce la posibilidad de un único punto de fallo en una red.

Reparto de carga

Puede configurar VRRP de tal manera que el tráfico hacia y desde los clientes LAN puede ser compartida por múltiples routers, compartiendo así la carga de tráfico de manera más equitativa entre los routers disponibles.

Múltiples Routers virtuales

VRRP soporta hasta 255 routers virtuales (grupos VRRP) en una

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

interfaz física del router, sujeto a la plataforma de apoyo a múltiples direcciones MAC. Permite implementar redundancia y carga compartida en la topología de LAN.

Múltiples direcciones IP

El router virtual puede administrar varias direcciones IP, incluyendo direcciones IP secundarias. Por lo tanto, si usted ha configurado varias subredes en una interfaz GigabitEthernet, puede configurar VRRP en cada subred.

Preferencias

El esquema de redundancia de VRRP le permite anticiparse a una copia de seguridad del router virtual que se ha hecho cargo de un maestro en su defecto del router virtual con un respaldo mayor prioridad router virtual que se ha dispuesto.

Prioridad del Router y preferencia VRRP

Un aspecto importante del esquema de redundancia VRRP es prioridad de enrutador VRRP. Prioridad determina el papel que desempeña cada uno de router VRRP y lo que sucede si el maestro router virtual falla.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Si un router VRRP posee la dirección IP del router virtual y la dirección IP de la interfaz física, este router funcionará como un maestro router virtual.

La prioridad también determina si un router VRRP funciona como una copia de seguridad del router virtual y el orden de ascenso para convertirse en un router virtual maestro si el router virtual maestro falla. Puede configurar la prioridad de cada enrutador virtual de copia de seguridad con un valor de 1 a través de 254 utilizando el comando de prioridad de VRRP. (Cisco Systems I. , Configuring VRRP, 2010)

2.3.6. Virtual Switching System (VSS)

Objetivos VSS

Los operadores de red aumentan la fiabilidad de la red mediante la configuración de pares redundantes de los dispositivos de red y enlaces. La ilustración 11 muestra una configuración de red de conmutación típica. Elementos de red redundantes y enlaces redundantes pueden agregar complejidad al diseño de la red y la operación. El sistema conmutación virtual simplifica la red reduciendo el número de elementos de red y ocultar la complejidad de la gestión de los interruptores y enlaces

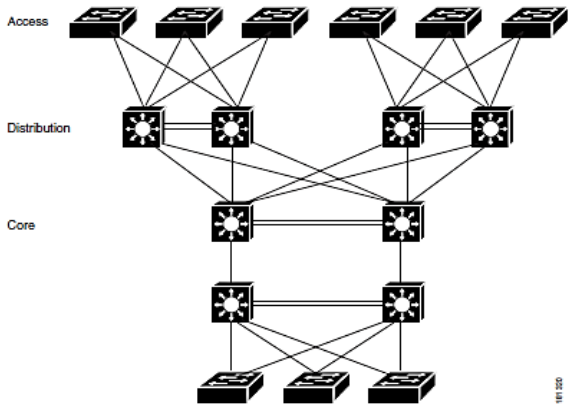
Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

redundantes.

El VSS combina un par de conmutadores de la serie Catalyst 6500 en un solo elemento de red. El VSS gestiona los enlaces redundantes, que actúan externamente como un único canal de puerto.

El VSS simplifica la configuración de la red y el funcionamiento mediante la reducción del número de Capa 3 vecinos de enrutamiento y proporcionan una topología de capa libre de 2 bucles.

Ilustración 11- Typical Switch Network Design



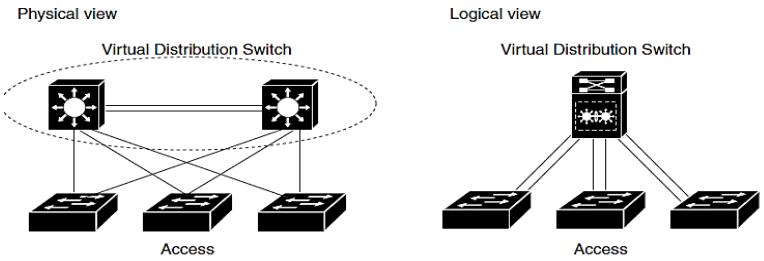
Fuente:http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-2SY/config_guide/sup2T/15_2_sy_swcg_2T/virtual_switching_systems.html

Virtual Switching System

El VSS combina un par de interruptores en un único elemento de red. Por ejemplo, un VSS en la capa de distribución de la red interactúa con las redes de acceso y núcleo como si se tratara de un único conmutador.

Un interruptor de acceso se conecta a ambos chasis del VSS usando un canal de puerto lógico. El VSS gestiona la redundancia y balanceo de carga en el canal del puerto. Esta capacidad permite a un switch de capa 2 topologías de red sin bucles. El VSS también simplifica la topología de red de capa 3 porque el VSS reduce el número de enrutamiento de pares en la red.

Ilustración 12- VSS in the Distribution Network



Fuente:http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-2SY/config_guide/sup2T/15_2_sy_swcg_2T/virtual_switching_systems.html

VSS activo y VSS en espera

Al crear o reiniciar un VSS, el chasis pares negocian sus roles. Un chasis se convierte en el chasis activo VSS, y el otro se convierte en el chasis de espera VSS.

El chasis activo controla el VSS. Se ejecuta los protocolos de Capa 2 y Capa 3 de control para los módulos de conmutación en ambos chasis. El chasis activo VSS también proporciona funciones de gestión para la VSS, como la inserción del módulo en línea y la eliminación (OIR) y la interfaz de la consola.

El chasis activo VSS espera realizar el reenvío de paquetes para el tráfico de datos de entrada en sus interfaces alojados localmente. Sin embargo, el chasis de espera VSS envía todo el tráfico de control al chasis activo VSS para su procesamiento.

Virtual Switch Link

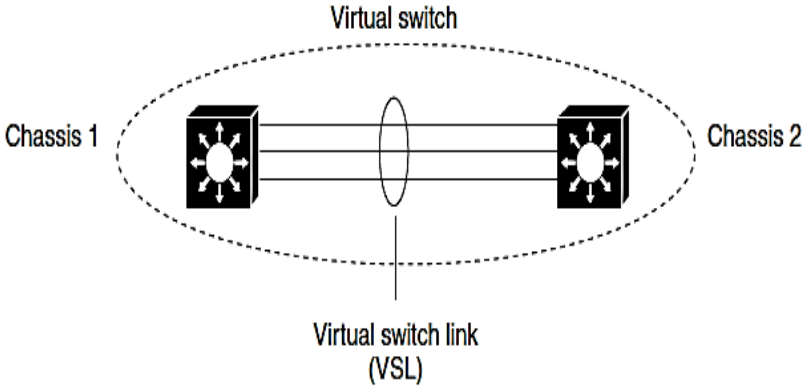
Para los dos chasis de la VSS para actuar como un elemento de red, tienen que compartir información de control y tráfico de datos.

El interruptor de enlace virtual (VSL) es un enlace especial que lleva el tráfico de control y de datos entre los dos chasis de un

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

VSS, como se muestra en la ilustración 13. El VSL se implementa como un EtherChannel con hasta ocho enlaces. El VSL da el tráfico de control mayor prioridad que el tráfico de datos de manera que los mensajes de control no se descartan. El tráfico de datos es carga equilibrada entre los enlaces VSL por el algoritmo de balanceo de carga EtherChannel.

Ilustración 13- Virtual Switch Link



Fuente:http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-2SY/config_guide/sup2T/15_2_sy_swcg_2T/virtual_switching_systems.html

Al configurar VSL todas las configuraciones existentes se eliminan de la interfaz a excepción de comandos específicos permitidos. Al configurar VSL, el sistema pone a la interfaz en un modo restringido.

Cuando una interfaz está en modo restringido, los comandos de configuración sólo específicos se pueden configurar en la

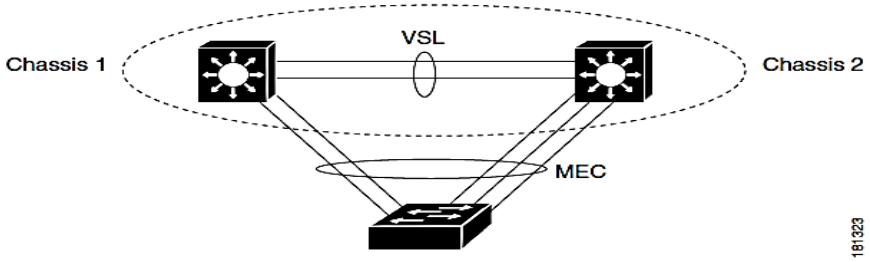
interfaz.

Multichassis EtherChannel

El EtherChannel multichasis (MEC) es un canal de puerto que se extiende por los dos chasis de un VSS. El interruptor de Acceso ve el MEC como un canal de puerto estándar.

El VSS admite un máximo de 512 EtherChannels. Este límite se aplica al total combinado de EtherChannels regulares y MEC. Debido VSL requiere dos números EtherChannel (uno para cada chasis), hay 510 EtherChannels configurables por el usuario. Si un módulo de servicio instalado utiliza un EtherChannel interna, que EtherChannel será incluido en el total.

Ilustración 14- VSS with MEC



Fuente:http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-2SY/config_guide/sup2T/15_2_sy_swcg_2T/virtual_switching_systems.html

Funcionalidad VSS

Redundancia y alta disponibilidad

En un VSS, opera entre el activo y VSS chasis de espera, utilizando conmutación de estado (SSO) y expedición sin parar (NSF). La información de configuración del chasis intercambio entre pares y el Estado a través de la VSL y el motor supervisor de VSS de espera se ejecuta en modo de espera VSS en caliente.

El chasis de espera VSS supervisa el chasis activo VSS usando el VSL. Si detecta fallos, el chasis VSS espera inicia una conmutación y asume el papel activo de VSS. Cuando el chasis no se recupera, que asume el papel de espera VSS.

Si el VSL falla completamente, el chasis VSS de espera supone que el chasis activo VSS ha fallado, e inicia una conmutación. Después de la conversión al sistema, si ambos chasis son VSS activa, la característica de doble activa de detección detecta esta condición y se inicia la acción de recuperación. Para obtener información adicional acerca de la detección de doble activo.

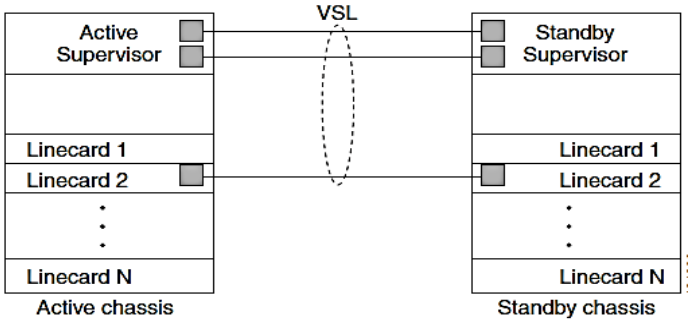
Ejemplo de Topología VSL

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

El VSS contiene dos chasis que se comunican mediante el VSL, que es un grupo de puerto especial.

Le recomendamos que configure los dos puertos 10-Gigabit Ethernet en los motores de supervisor como puertos VSL. Opcionalmente, también puede configurar el grupo de puertos VSL para contener módulo de conmutación de 10 puertos de Gigabit Ethernet. Esta configuración proporciona la capacidad VSL adicional. Vea la ilustración 15 para ver un ejemplo de topología.

Ilustración 15- VSL Topology Example



Fuente:http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-2SY/config_guide/sup2T/15_2_sy_swcg_2T/virtual_switching_systems.html

Redundancia RPR y SSO

Un VSS funciona con cambio de estado (SSO) de redundancia si cumple con los siguientes requisitos:

Ambos motores de supervisor deben ejecutar la misma versión de software.

Configuración relacionada VSL-en los dos chasis debe coincidir.

Modo PFC debe coincidir.

SSO y expedición sin parar (NSF) deben configurarse en cada chasis.

Con SSO redundancia, el motor supervisor de VSS de espera siempre está dispuesto a asumir el control después de una falla en el motor de supervisor activo VSS. Configuración, reenvío y la información de estado se sincronizan desde el motor de supervisor activo VSS para el motor de supervisor redundante en el arranque y siempre que los cambios en la configuración del motor de supervisor activo VSS ocurren. Si se produce una conmutación, la interrupción del tráfico se reduce al mínimo.

Si un VSS no cumple con los requisitos para SSO redundancia, el VSS utilizará redundancia procesador de ruta (RPR). En el modo de RPR, el motor de supervisor activo VSS no sincroniza los cambios de configuración o información de estado a la espera de VSS. El motor de supervisor de VSS de espera es

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

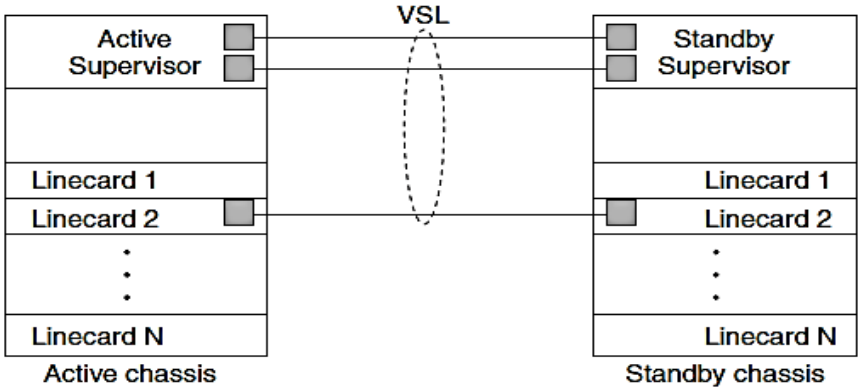
sólo parcialmente inicializado y los módulos de conmutación en el supervisor de VSS de espera no se encienden. Si una conmutación ocurre, el motor supervisor de VSS de espera completa su inicialización y enciende los módulos de conmutación. Tráfico se interrumpe durante el tiempo de reinicio normal del chasis.

El VSS normalmente ejecuta la conmutación de estado (SSO) entre los motores de supervisor activos VSS y espera VSS. El VSS determina el papel de cada motor supervisor de durante la inicialización.

El motor de supervisor en el chasis de espera VSS se ejecuta en modo de espera caliente. El VSS utiliza el enlace VSL para sincronizar datos de configuración de la VSS activa al motor supervisor de VSS de espera. Además, los protocolos y las características que soportan una alta disponibilidad sincronizan sus eventos y estado de la información al motor supervisor de VSS de espera.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Ilustración 16- Chassis Roles in a VSS



Fuente:http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-2SY/config_guide/sup2T/15_2_sy_swcg_2T/virtual_switching_systems.html

Multichassis EtherChannels

Un EtherChannel multichasis es un EtherChannel con los puertos que terminan en tanto chasis del VSS. Un VSS MEC puede conectarse a cualquier elemento de red que soporta EtherChannel (como un host, servidor, router o switch).

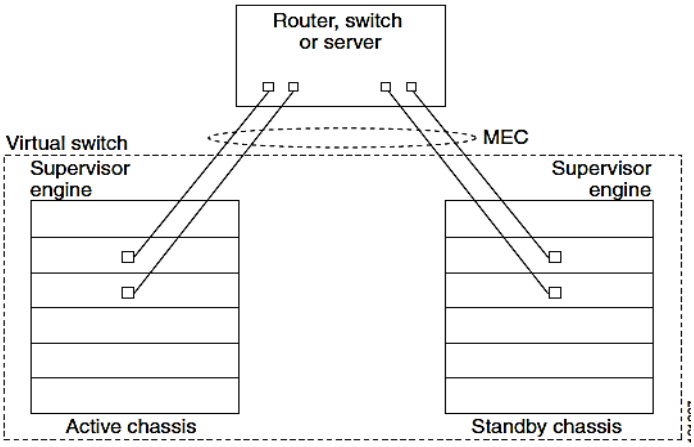
En la VSS, un MEC es un EtherChannel con capacidad adicional, el VSS equilibra la carga entre los puertos en cada chasis independiente. Por ejemplo, si el tráfico entra en el chasis activo VSS, el VSS seleccionará un enlace MEC desde el chasis activo VSS. Esta capacidad MEC asegura que el tráfico de datos no atraviesa innecesariamente el VSL.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Cada MEC opcionalmente se puede configurar para apoyar cualquiera PAGP o LACP. Estos protocolos sólo se ejecutan en el chasis activo VSS. Paquetes de control PAGP o LACP destinados a un enlace de MEC en el chasis de espera VSS se envían a través de VSL.

Un MEC puede soportar hasta ocho VSS enlaces físicos activos, que pueden ser distribuidos en cualquier proporción entre el chasis activo y VSS espera.

Ilustración 17- MEC Topology



Fuente:http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-2SY/config_guide/sup2T/15_2_sy_swcg_2T/virtual_switching_systems.html

(Cisco Systems I. , Virtual Switching Systems (VSS), 2015)

2.3.7. Transparent Interconnection of Lots of Links (TRILL) – Rbridges

Transparent Interconnection of Lots of Links (TRILL) es un estándar del Internet Engineering Task Force (IETF) que hace uso de las técnicas de encaminamiento de capa 3, para crear un conjunto grande de enlaces que se muestren frente a nodos IP como una única subred IP. Permite crear una nube de capa 2 de manera que los nodos se puedan mover dentro de ella sin cambiar sus direcciones IP, mientras que se utilizan todas las técnicas de encaminamiento de capa 3 que han ido evolucionando a lo largo de los años, incluyendo el uso de caminos mínimos y múltiples (multipath). Además, TRILL admite características de capa 2 como las VLANs, la habilidad de autoconfiguración (mientras que la configuración manual se puede realizar igualmente si se desea) y envío de tráfico multicast/broadcast sin necesidad de usar ningún protocolo adicional.

La ilustración 18 TRILL, como podrá verse en este apartado, es un protocolo de capa 2 y ½: Reúne los enlaces de manera que los nodos IP observen la nube que forman como un único enlace. Por

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

lo que TRILL está por debajo de la capa 3, pero por encima de la capa 2 dado que deja de lado el concepto de las nubes Ethernet tradicionales, tal y como hacen los routers IP.

En la ilustración 18 se muestran los conceptos básicos de TRILL a la hora de manejar un paquete unicast donde la localización del destino es conocida:

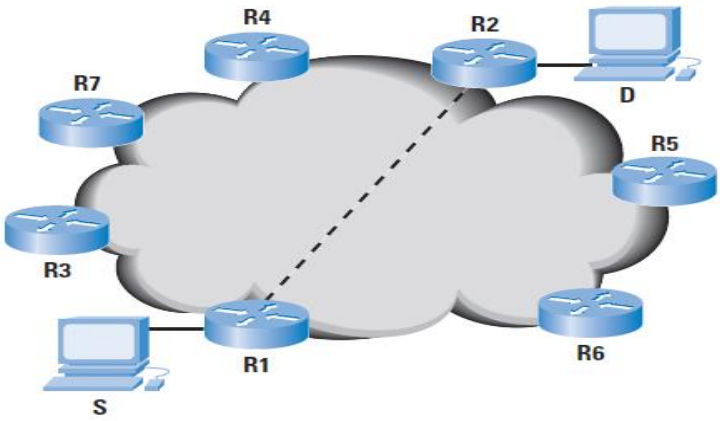
Los RBridges ejecutan un protocolo de estado de enlace, que le proporciona a cada uno información sobre la topología que consiste en todos los RBridges y todos los enlaces entre RBridges en la misma. Usando este protocolo, cada RBridge calcula caminos mínimos desde él mismo hasta cada uno de los demás RBridges, así como árboles para el reparto de tráfico multidestino.

Cuando un RBridge R1 recibe una trama Ethernet desde un nodo final S, con destino a la dirección Ethernet D, R1 encapsula la trama con una cabecera TRILL, haciendo que el paquete se dirija hacia el RBridge R2, que tiene a D directamente conectado. La cabecera TRILL contiene un campo para el “RBridge de entrada” (“ingress RBridge”) R1, otro para el “RBridge de salida” (“egress RBridge”) R2, y un campo contador de saltos (hop count).

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Cuando R2 recibe el paquete encapsulado, retira la cabecera TRILL y reenvía la trama Ethernet a D.

Ilustración 18- RBridging: El concepto de encaminamiento en las nubes formadas por RBridges



Fuente: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_14-3/index.html

La Cabecera TRILL

Los campos principales de la cabecera TRILL son: ingress RBridge nickname (16 bits), egress RBridge nickname (16 bits), hop count (6 bits), y un flag para indicar si es multidestino (1 bit). Una cabecera típica de capa 3 tendría una fuente, un destino y un contador de saltos. Por lo tanto TRILL es básicamente una cabecera de encapsulamiento con direcciones planas de 16 bits. El hecho de cómo los RBridges obtienen los “nicknames” se describe más adelante. La cabecera completa se puede ver en la Figura 22, donde los campos son:

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

TRILL Ethertype = Indica el tipo de payload (la parte de datos que envuelve la cabecera)

V = Versión (2 bits)

R = Reservado (2 bits)

M = Multidestino (1 bit)

OpLng = Longitud de las opciones de TRILL

Hop = Contador de saltos, TTL

Nicknames = Valores para designar el RBridge de entrada y de salida (16 bits)

Protocolos de estado de enlace Trill

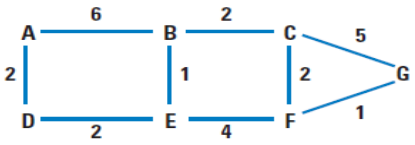
Los protocolos de estado de enlace que habitualmente se despliegan en TRILL son Intermediate System-to-Intermediate System (IS-IS) (RFC 1142) y Open Shortest Path First (OSPF). IS-IS, diseñado en los años 80 para encaminar DECnet, fue adoptado por la Organización Internacional de Normalización, International Organization for Standardization (ISO), puede encaminar tráfico IP y se usa por muchos proveedores de servicios de Internet, Internet Service Provider (ISP), para encaminar IP. IS-IS fue una elección natural para TRILL, dado que por su codificación permite fácilmente el uso de campos adicionales y además funciona directamente sobre capa 2, de manera que se autoconfigura, mientras que OSPF

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

funciona por encima de IP y requiere que todos los routers tengan direcciones IP.

La Figura 19 muestra una pequeña red, en la parte superior, que consiste en 7 routers. En la mitad inferior de la misma, se muestra la base de datos de los paquetes de estado de enlace LSP (Link State Packet); todos los routers tienen la misma base de datos porque todos ellos reciben y almacenan los LSP generados más recientemente por cada uno de los otros routers. Dicha base de datos proporciona toda la información necesaria para calcular los caminos. También da información suficiente para que todos los routers calculen el mismo árbol, sin necesidad de utilizar un algoritmo de árbol expandido aparte. Como se puede ver, TRILL requiere un árbol (al menos uno) para distribuir los paquetes multidestino.

Ilustración 19- Red de routers y estado de enlace



A	B	C	D	E	F	G
B/6	A/6	B/2	A/2	B/1	C/2	C/5
D/2	C/2	F/2	E/2	D/2	E/4	F/1
	E/1	G/5		F/4	G/1	

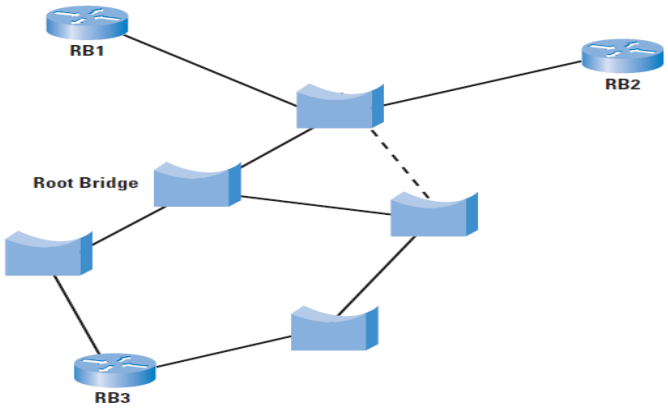
Fuente: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_14-

3/index.html

Interconexión de RBridges con otro tipo de bridges

TRIILL está diseñado de manera que cualquier subconjunto de bridges en una red pueden ser sustituidos por RBridges. Un conjunto de enlaces conectados por puentes serán percibidos por RBridges como un único enlace compartido que conecta a todos los RBridge unidos a dicho enlace. Los puentes dentro de ese enlace se comportarán como puentes normales, formando un árbol expandido y reenviando paquetes a través de dicho árbol. La ilustración 20 esta situación, en la que solo RB1, RB2, RB3 son RBridges en la topología Ethernet, el resto son puentes normales, y la línea de puntos se trata de un enlace que se ha seleccionado como backup por el árbol expandido.

Ilustración 20- RBridges conectados por una LAN de bridges

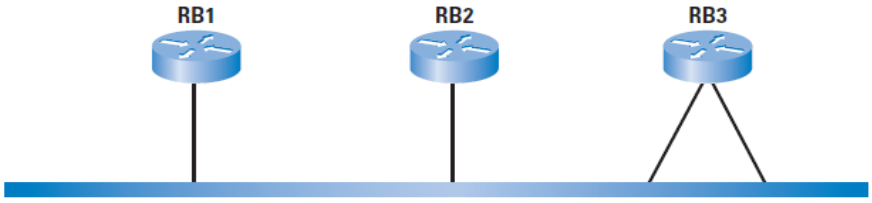


*Fuente: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_*

14-3/index.html

Los RBridges RB1, RB2 y RB3 perciben el enlace como en la siguiente ilustración 21, un enlace único compartido en el que RB3 tiene dos puertos conectados. Como consecuencia, introducir RBridges en una red Ethernet particiona los árboles expandidos en árboles expandidos más pequeños.

Ilustración 21- Perceivedby RBridges: un único enlace compartido en el que RB3 tiene dos puertos conectados



Fuente: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_14-3/index.html

Tipos de enlaces y la cabecera salto a salto (hop by hop)

Además de la cabecera TRILL, cuando un RBridge R1 está enviando una trama encapsulada con TRILL a un vecino RBRidge R2, hay una cabecera adicional que es específica al tipo de enlace que conecta R1 y R2. Aunque TRILL va por encima de Ethernet, un enlace entre dos RBridges o más podría ser cualquier tipo de enlace; por ejemplo, aparte de Ethernet, podría ser un enlace del

Point to Point Protocol (PPP), un túnel IP o IP Security (IPSec), un camino Multiprotocol Label Switching (MPLS), etc.

Si el enlace es Ethernet, la cabecera “externa” será una cabecera Ethernet. Si es un enlace PPP, será una cabecera PPP. La cabecera “externa” para Ethernet (en el caso de un enlace Ethernet) tiene dos propósitos:

Si hay puentes en el enlace, percibirán el paquete como un paquete Ethernet normal. Las tablas de aprendizaje de los puentes en dicho enlace verán sólo las direcciones de los RBridges en el mismo.

Permite a R1, cuando está enviando tráfico a un enlace con múltiples vecinos (digamos R2 y R3), especificar qué RBridge es el próximo para el envío, R2 o R3, mandando el paquete en unicast al RBridge del siguiente salto, next hop RBridge, elegido. Por ejemplo, podría ser que tanto R2 como R3 tuvieran el mismo coste hacia el destino, por lo que R1 debería especificar a cuál reenvía el paquete; de otro modo, ambos reenviarían el paquete y éste quedaría duplicado.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

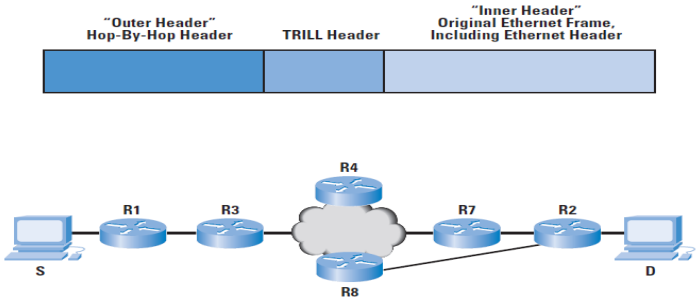
Por lo tanto, tal y como en la ilustración 22, un paquete con encapsulado TRILL puede tener tres cabeceras:

La cabecera exterior o cabecera hop by hop, que se renueva en cada salto, es específica al tipo de enlace que conecta a los RBridges vecinos y, cuando se reenvía entre R1 y R2, especifica R1 como origen y R2 como destino.

La cabecera TRILL, que de manera similar a una cabecera de capa 3 se mantiene intacta en su viaje desde el primer RBridge hasta el último, que especifica el primer RBridge (aquel que encapsuló el paquete con la cabecera TRILL) como el RBridge de entrada, y el último RBridge (aquel que desencapsulará el paquete) como el RBridge de salida.

La cabecera interna Ethernet, que especifica la pareja de nodos que se están comunicando como origen y destino.

Ilustración 22- Cabeceras de los paquetes TRILL



Fuente: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_14-3/index.html

Prestando atención al caso concreto de la ilustración 22, asúmase que S transmite un paquete Ethernet a D. La cabecera interna Ethernet tendrá origen = S y destino = D. Al llegar a R1, este RBridge la encapsulará con una cabecera TRILL, donde el RBridge de entrada = R1 y el RBridge de salida = R2. Finalmente la reenviará hacia R3, no sin antes añadir la cabecera apropiada para el enlace. Si el enlace de Ethernet, la cabecera externa indicará origen = R1 y destino = R3. Cuando R3 la reciba y reenvíe hacia R7, R3 mantendrá la cabecera TRILL tal y como está (lo único que variará será el contador de saltos, que disminuirá), pero quitará la cabecera externa y pondrá una nueva indicando origen = R3 y destino = R7. De manera similar, R7 reenviará la trama a R2. Si es un enlace PPP, no se indicará ni origen ni destino. Cuando R2 manda la trama a D, R2 quita primero la cabecera TRILL y D verá el paquete exactamente igual que S lo transmitió.

Implicaciones de VLAN en TRILL

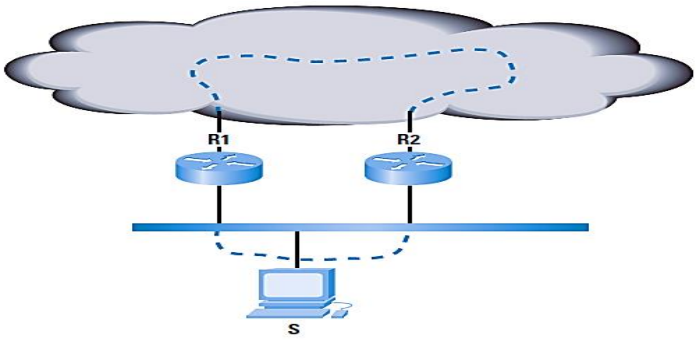
El concepto de LAN Virtual, Virtual LAN (VLAN), en Ethernet genera conjuntos de nodos finales que comparten la misma infraestructura (enlaces y puentes), de manera que los nodos

finales en el mismo conjunto puedan hablar entre ellos directamente (usando Ethernet), mientras que aquellos en VLANs diferentes han de comunicarse a través de un router. Los nodos IP, aunque en general no son conscientes de las etiquetas VLAN, perciben las diferentes VLANs como diferentes subredes IP.

Para ver la utilidad de VLAN en TRILL, sigamos el ejemplo de la siguiente ilustración 23. Si hay múltiples RBridges en un mismo enlace, junto con nodos finales, es importante que sólo uno de ellos encapsule un paquete de cierto nodo final. Como se muestra en la ilustración 23, si tanto R1 como R2 encapsularan un paquete unicast de S, se mandarían dos copias al destino. Sin embargo, si S estuviera mandando un paquete multidestino (ya sea multicast o con destino desconocido), entonces la copia que encapsulara R1 sería reenviada y recibida por R2, que la desencapsularía, y volvería a ser recibida por R1, que la encapsularía de nuevo y enviaría de nuevo a la red, creando un bucle. Este bucle además no se soluciona con el contador de saltos de TRILL, pues la cabecera se elimina y añade cada vez, ignorándose dicho campo. De este ejemplo en la figura, se ve que es importante que todos los RBridges conectados a un mismo enlace sepan sobre los otros, si no, puede haber problemas.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Ilustración 23- Enlace con múltiples RBridges conectados



http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_14-3/143_trill.html

. (Cisco Systems I. , TRILL, 2011)

2.3.8. Gateway Load Balancing Protocol

Para aumentar en las capacidades del Hot Standby Router Protocol (HSRP), Cisco desarrolló GLBP. GLBP proporciona automático, el Equilibrio de carga del gateway del primero-salto, que permite el USO de recursos más eficiente y los costos administrativos reducidos. Es una extensión del HSRP y especifica un protocolo que asigne dinámicamente la responsabilidad de una dirección IP virtual y distribuya las direcciones MAC virtuales múltiples a los miembros de un grupo GLBP.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Gateway virtual

Un miembro en un grupo puede estar en cualquiera de estos estados: activo, espera, o escuche. Los miembros de un grupo GLBP eligen un gateway para ser el gateway virtual activo (AVG) para ese grupo.

También elige a un miembro como gateway virtual espera (SVG). Si hay más de dos miembros, después los miembros que sigue habiendo están en el estado del escuchar.

Si un AVG falla, SVG asume la responsabilidad de la dirección IP virtual. Nuevo SVG entonces se elige de los gatewayes en el estado del escuchar. Si viene el AVG fallado o el nuevo miembro con un número más prioritario en línea, no se apropia por abandono. Usted puede configurar el Switches de modo que pueda apropiarse.

Promotor virtual

El AVG asigna las direcciones MAC virtuales a cada miembro en orden. Llaman el miembro el promotor Primary Virtual (PVF) o promotor virtual activo (AVF) si la dirección MAC es asignada directamente por el AVG. El mismo miembro es el promotor virtual secundario (SVF) para las direcciones MAC asignadas a otros

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

miembros. PVF está en el estado activo y el SVF es adentro escucha estado.

Limitación

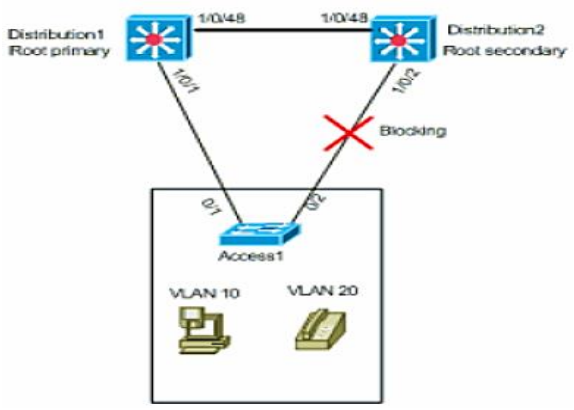
La expedición directa de Cisco (NSF) con el cambio stateful (SSO) tiene una restricción con GLBP. El SSO no está GLBP enterado, que significa que la información del estado GLBP no está mantenida entre el active y el motor del Supervisor en espera durante el funcionamiento normal. GLBP y el SSO pueden coexistir, pero ambas características trabajan independientemente. Trafique que confía en GLBP puede conmutar al recurso seguro GLBP en caso de intercambio del supervisor.

Aspecto del diseño

La implementación GLBP en los switches de Catalyst depende del diseño de red. Usted necesita considerar la topología del árbol de expansión para utilizar GLBP en su red. Usted puede utilizar esta Ilustración como un ejemplo:

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Ilustración 24- Aspectos Del Diseño



http://www.cisco.com/cisco/web/support/LA/102/1027/1027680_glbp-cat65k.html

En la ilustración 24, hay dos VLA N, 10 y 20, en todo el tres Switches. En esta red, Distribution1 es el Root Bridge para todos las VLA N y el resultado es el puerto 1/0/2 en Distribution 2 estará en el estado de bloqueo. En este escenario, GLBP no es conveniente de implementar. Porque usted tiene solamente una trayectoria de Access1 al switch de distribución, usted no puede alcanzar el Equilibrio de carga verdadero con GLBP.

Sin embargo, en este escenario, usted puede utilizar el Spanning Tree Protocol (STP) en vez de GLBP para cargar la balanza y usted puede utilizar el HSRP para la Redundancia. Usted debe considerar su topología de STP para decidir si utilizar GLBP o no. En tales configuraciones donde se requiere el atravesar árbol, la

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

solución es utilizar un STP mejorado, tal como Rápido PVST. Para habilitar el Rápido-PVST, utilice el comando del modo del árbol de expansión rápido-PVST en el Switches.

Éste es el STP que se recomienda para utilizar con GLBP. El Rápido PVST proporciona una época de la convergencia rápida, que permite que los links alcancen al estado de reenvío del atravesar-árbol antes de que el temporizador del control del valor por defecto GLBP mida el tiempo hacia fuera.

Si un STP se utiliza en un link a un router GLBP, el tiempo en espera GLBP debe ser mayor que el tiempo que toma para que el STP alcance al estado de reenvío. Las configuraciones del parámetro predeterminado alcanzan esto con el Rápido PVST, mientras que un tiempo en espera de más de 30 segundos se requiere si el STP se utiliza con sus configuraciones predeterminadas. (Cisco S. , 2015)

2.3.9. Definición de términos básicos

2.3.9.1. Alta Disponibilidad

Consiste en la capacidad del sistema para ofrecer un servicio activo durante un tanto por ciento de un tiempo determinado o a la capacidad de recuperación del mismo en caso de producirse un

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

fallo en la red. Cuando se habla de “caída del sistema” puede hacer referencia tanto a un equipo que ha dejado de funcionar, como un cable que ha sido cortado o desconectado; u otras situaciones que impliquen que la red deje de funcionar. En casos como estos, hace falta que el sistema detecte el fallo del mismo y que, además, reaccione de manera rápida y eficiente en la búsqueda de una solución a la caída.

2.3.9.2. Redundancia

La redundancia hace referencia a nodos completos que están replicados o componentes de éstos, así como caminos u otros elementos de la red que están repetidos y que una de sus funciones principales es ser utilizados en caso de que haya una caída del sistema.

2.3.9.3. Protocolo

Es un sistema de reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas para transmitir información por medio de cualquier tipo de variación de una magnitud física. Se trata de las reglas o el estándar que define a sintaxis, semántica y sincronización de la comunicación, así como también los posibles métodos de recuperación de errores.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Los protocolos pueden ser implementados por hardware, por software, o por una combinación de ambos.

2.3.9.4. Dirección IP

Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del modelo OSI. Dicho número no se ha de confundir con la dirección MAC, que es un identificador de 48 bits para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizado ni de la red.

2.3.9.5. ICMP

Es un protocolo que permite administrar información relacionada con errores de los equipos en red. Si se tienen en cuenta los escasos controles que lleva a cabo el protocolo IP, ICMP no permite corregir los errores sino que los notifica a los protocolos de capas cercanas. Por lo tanto, el protocolo ICMP es usado por todos los routers para indicar un error (llamado un problema de entrega).

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

2.3.9.6. Hot Standby

Es un método redundante en el que un sistema se ejecuta simultáneamente con un sistema primario idénticos. En caso de fallo del sistema primario, el sistema espera activa inmediatamente toma más, en sustitución del sistema primario. Sin embargo, los datos se reflejan todavía en tiempo real. Por lo tanto, ambos sistemas tienen datos idénticos.

2.3.9.7. Enrutador

Es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red). Un router es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

2.3.9.8. Dirección MAC

Es un identificador de 48 bits (6 bytes) que corresponde de forma única a una tarjeta o interfaz de red. Es individual, cada dispositivo tiene su propia dirección MAC determinada y configurada por el IEEE (**los últimos 24 bits**) y el fabricante (**los primeros 24 bits**) utilizando el OUI. La mayoría de los protocolos que trabajan en la capa 2 del modelo OSI usan una de las tres numeraciones

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

manejadas por el IEEE: **MAC-48, EUI-48, y EUI-64** las cuales han sido diseñadas para ser identificadores globalmente únicos. No todos los protocolos de comunicación usan direcciones MAC, y no todos los protocolos requieren identificadores globalmente únicos.

2.3.9.9. Jitter

Es la variación en el tiempo entre los paquetes que llegan, causados por la congestión de la red, la deriva de temporización, o cambios de ruta. Una memoria intermedia de fluctuación se puede utilizar para manejar la fluctuación de fase.

CAPITULO III MARCO METODOLÓGICO

3.1. Tipo y diseño de la investigación

3.1.1. Tipo de investigación:

Cuantitativo

3.1.2. Diseño de la investigación:

O1		**O3**
O2	**X**	**O4**

Dónde:

X: Protocolos de alta disponibilidad.

O1: Diagnosticar el estado actual de la disponibilidad de una red informática.

O2: Analizar los factores influyentes en la disponibilidad de una red informática.

O3: Implementar protocolos de comunicación para mejorar la disponibilidad de una red informática.

O4: Estimar los resultados que generara la implantación de protocolos de comunicación en la disponibilidad de una red informática.

.

3.2. Población y muestra:

3.2.1. Población:

Esta investigación tomara como población a la cantidad de data envía y recibida en la red local, es decir todo el tráfico IP.

Debido que se tiene acceso a toda la población no se utilizara una muestra, se tomara todo el tráfico IP.

3.3. Hipótesis

La implementación de protocolos de comunicación permitirá mejorar la disponibilidad de una red informática.

3.4. Variables

3.4.1. Variable independiente:

Protocolos de Comunicación.

3.4.2. Variable Dependiente:

La disponibilidad de una red informática.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

3.5. Operacionalización

Variable dependiente	Dimensiones	Indicadores	Técnicas e instrumentos de recolección de Datos
La disponibilidad de una red informática	Análisis de protocolos	-Tiempo caídas en la comunicación de una red informática. -tiempo reposición en la comunicación de una red informática. -Tiempo de detección de fallas en las comunicaciones de una red informática.	-Pruebas. -Recopilación de información. - Observación

3.6. Métodos, técnicas e instrumentos de recolección de datos

Entre las técnicas de recolección de datos en esta investigación son:

Pruebas

Se realizaran diferentes pruebas con los diferentes protocolos a analizar

Ficha de evaluación por juicio de expertos

Será evaluada la estructura de la investigación por expertos.

Recopilación de información

Se recopilara toda la data acerca de los diferentes protocolos a

analizar

Observación

Se observaran todos los eventos a lo largo de la investigación

3.6.1. Procedimiento para la recolección de datos

En la siguiente investigación se utilizaron las siguientes técnicas:

Recopilación de Información

Pre –procesamiento de la data

Software

3.6.2. Análisis estadístico e interpretación de datos

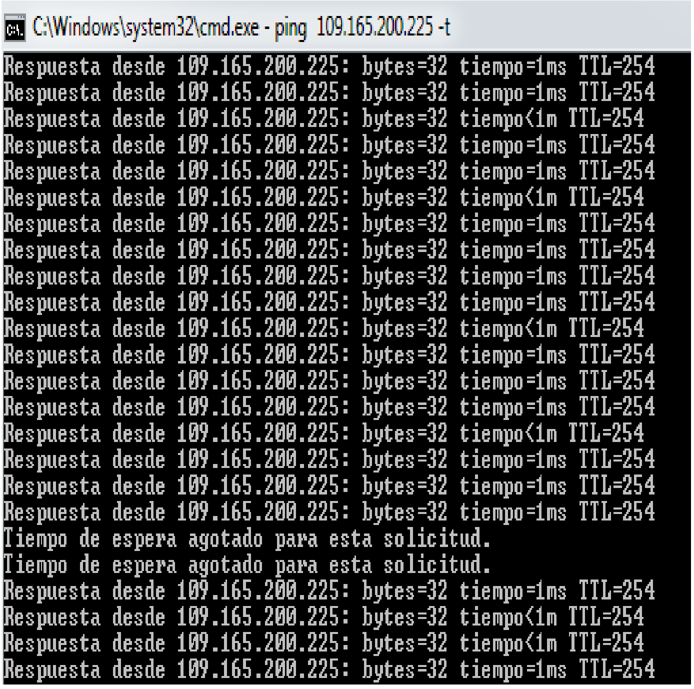
PING

El comando ping es un método muy común para la solución de problemas de la accesibilidad de los dispositivos. Utiliza una serie de mensajes de control de Internet Mensaje Protocol (ICMP) hecho para determinar:

- Si un host remoto está activo o inactivo.
- La ida y vuelta demora en la comunicación con el host.
- La pérdida de paquetes.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

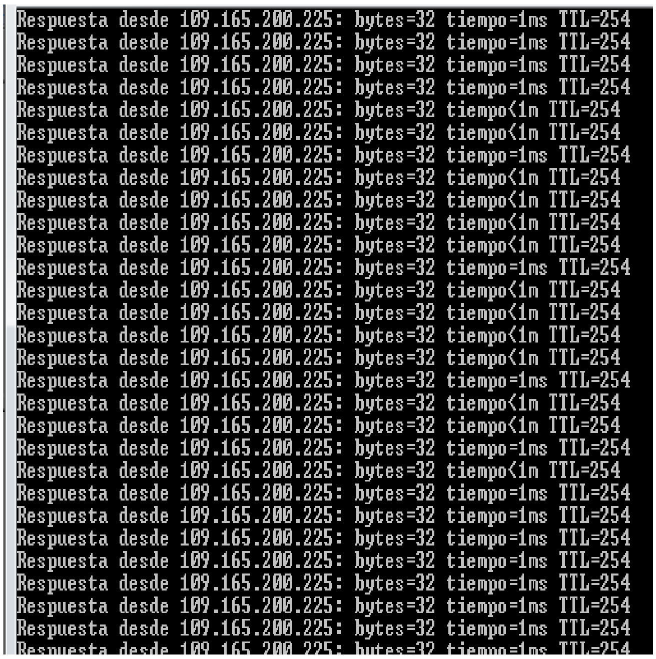
Ilustración 25- Caída de enlace-HSRP



```
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
```

Fuente: Elaboración Propia

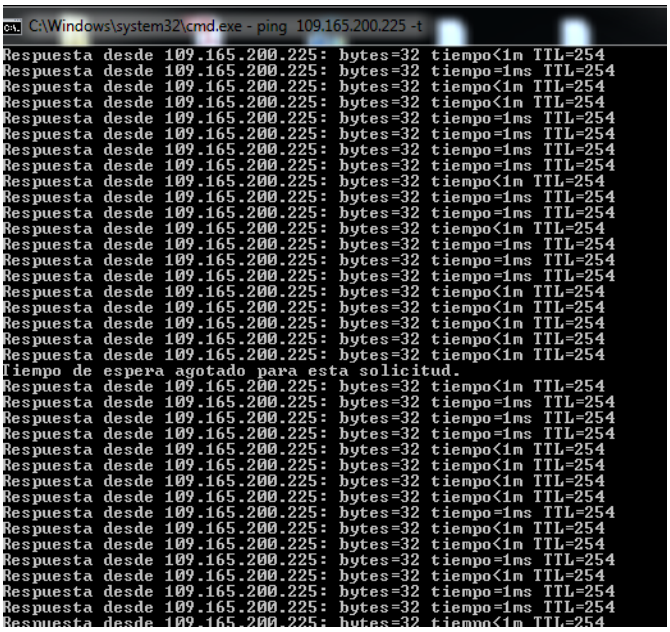
Ilustración 26- Caída de enlace-GLBP



```
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
```

Fuente: Elaboración Propia

Ilustración 27- Caída de enlace VRRP



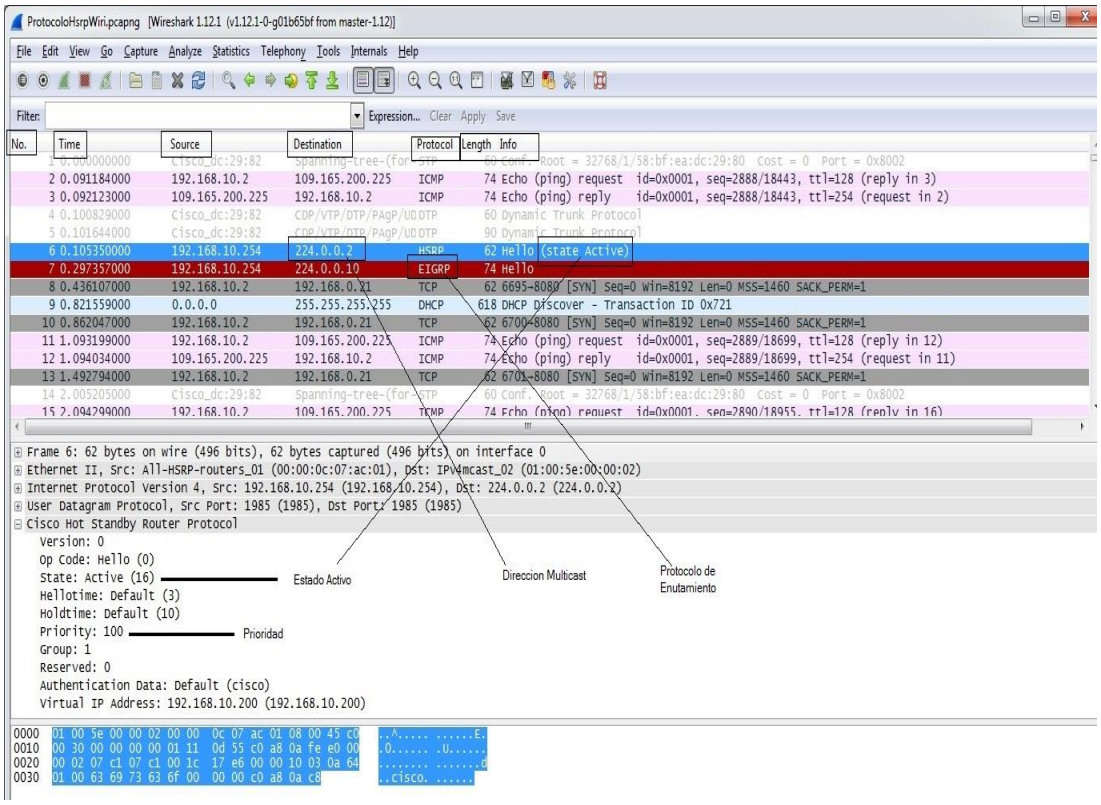
Fuente: Elaboración Propia

WIRESHARK

El wireshark es un analizador de protocolos utilizado para el análisis y solución de problemas en redes de comunicaciones para el desarrollo de software y protocolos.

Protocolo HSRP

Ilustración 28- Paquetes Capturados-HSRP



Fuente: Elaboración Propia

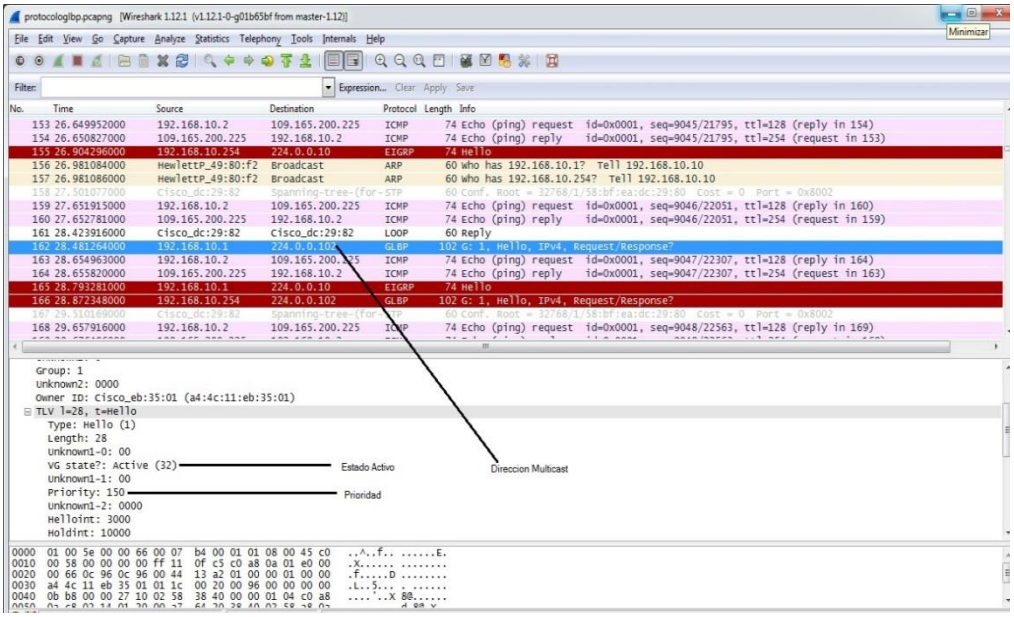
El programa wireshark Muestra la cabecera con el numero correlativo de los frame capturados, el tiempo en que los frame son capturados, origen, destino y la información de todos los protocolos involucrados en la captura, seguidamente nos muestra Ethernet II, la cabecera Ethernet que a su vez pertenece a la capa de enlace de datos.

Internet protocol II muestra los datos con la cabecera del datagrama IP, por lo tanto como en esta investigación se está

trabajando con los protocolos de alta disponibilidad se puede visualizar en la ilustración los protocolos TCP, protocolo de enrutamiento EIGRP, protocolo DHCP y el protocolo ICMP, la dirección multicast, el protocolo Cisco Hot Standby Protocol con prioridad 100 y su estado es Activo.

Protocolo GLBP

Ilustración 29- Paquetes Capturados-GLBP

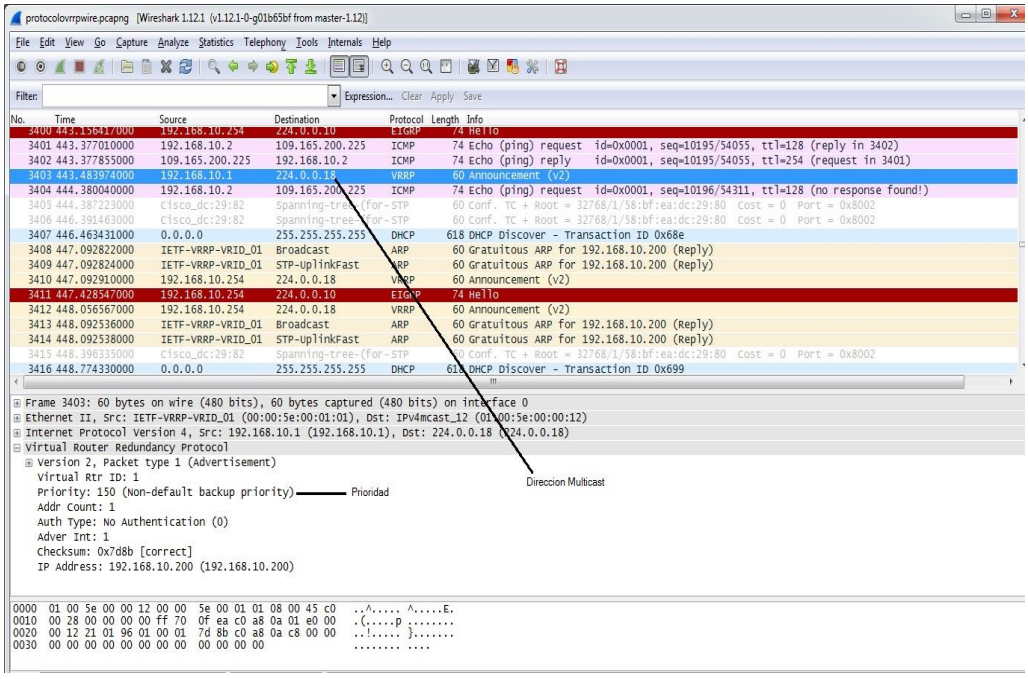


Fuente: Elaboración Propia

En la captura de paquetes muestra la misma información que la ilustración de captura de paquetes – HSRP se observa los mismo protocolos ICMP, protocolo de enrutamiento EIGRP, ICMPV6, ARP, dirección multicast y el protocolo Gateway Load Balancing Protocol y su estado es Activo.

Protocolo VRRP

Ilustración 30- Paquetes Capturados-VRRP



Fuente: Elaboración Propia

En la captura de paquetes muestra la misma información que la ilustración de captura de paquetes – HSRP se observa los mismo protocolos ICMP, protocolo de enrutamiento EIGRP, ICMPV6, ARP, dirección multicast y el protocolo Virtual Router Redundancy Protocolo.

3.6.3. Criterios éticos

Los criterios éticos que se respetan en el presente proyecto de tesis es el Código Deontológico del Colegio de Ingenieros del Perú en su Capítulo III "*Faltas Contra la Ética Profesional y*

Sanciones" y su Sub Capítulo II "*De la Relación con El Público"* en su Artículo 106 expresa:

- *Los ingenieros, al explicar su trabajo, méritos o emitir opiniones sobre temas de ingeniería, actuarán con seriedad y convicción, cuidando de no crear conflictos de intereses, esforzándose por ampliar el conocimiento del público a cerca de la ingeniería y de los servicios que presta a la sociedad.*

El presente proyecto de investigación expresara en la medida de lo posible lo más claro y conciso su contenido con el fin de generar un aporte a la disponibilidad de una red informática, para garantizar la disponibilidad de los servicios que brindan las diferentes empresas.

3.6.4. Criterios de rigor científico

Ilustración 31- Criterios de rigor científico

Criterios	Características éticas del criterio
Consentimiento informado	Los participantes deben estar de acuerdo con ser informantes y conocer sus derechos y responsabilidades.
Confidencialidad	Asegurar la protección de la identidad de las personas que participan como informantes de la investigación.
Manejo de riesgos	Este requisito tiene relación con los principios de no maleficencia y beneficencia establecidos para hacer investigación con seres humanos.
Observación participante	La incursión del investigador en el campo exige una responsabilidad ética por los efectos y las consecuencias que pueden derivarse de la interacción establecida con los sujetos participantes del estudio.
Entrevistas	Se trata de una interacción social donde no se deben provocar actitudes que condicionen las respuestas de los participantes.
Grabaciones de audio o video	Deben resguardarse en archivos confidenciales y el investigador necesita ser cauteloso anteponiendo la confidencialidad, el respeto y el anonimato de los participantes.

Fuente: http://www.scielo.org.co/pdf/aqui/v12n3/v12n3a06.pdf

CAPITULO VI: ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

4.1. Resultados en tablas y gráficos.

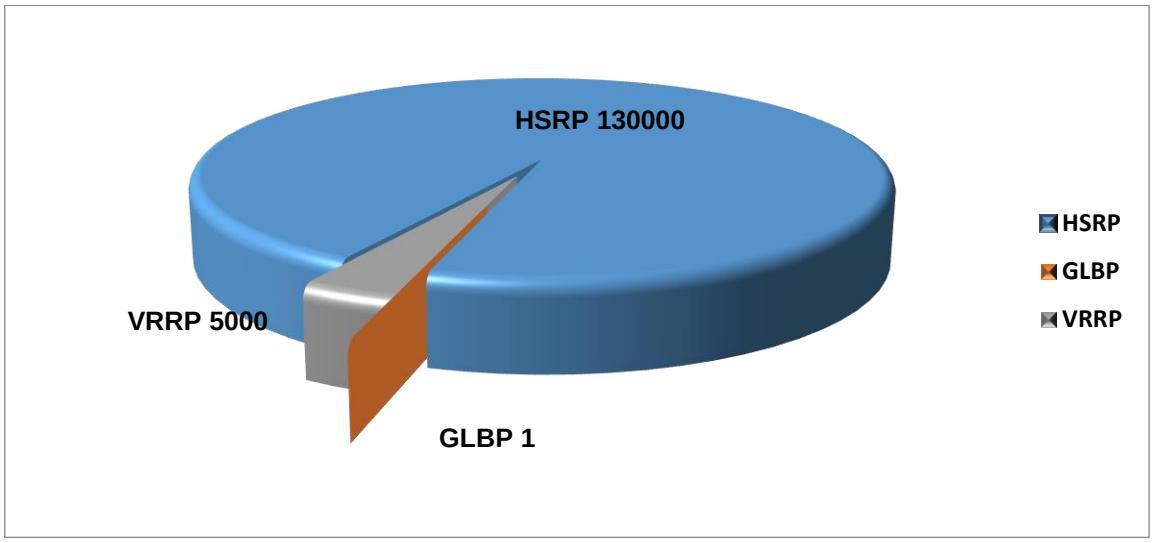
Tiempo de caídas en las comunicaciones de una red informática.

Tabla 1- Análisis de tiempo de caídas en las comunicaciones de una red informática

Protocolo	HSRP	GLBP	VRRP
Tiempo en ms	13000ms	1ms	5000ms

Fuente: Elaboración propia

Ilustración 32-Análisis de tiempo de caídas en las comunicaciones de una red informática



Fuente: Elaboración propia

En la ilustración 32 puede apreciarse el análisis de los tiempos en milisegundos que varían de protocolo en protocolo, obteniendo como resultado que el protocolo HSRP en cuanto a la caída de la comunicación de la red informática es de 13000 milisegundos, en el análisis del protocolo GLBP el resultado obtenido en la caída de la comunicación de la red informática es de 1 milisegundos, el protocolo VRRP con respecto al resultado obtenido durante la caída

de la comunicación es de 5000 milisegundos,

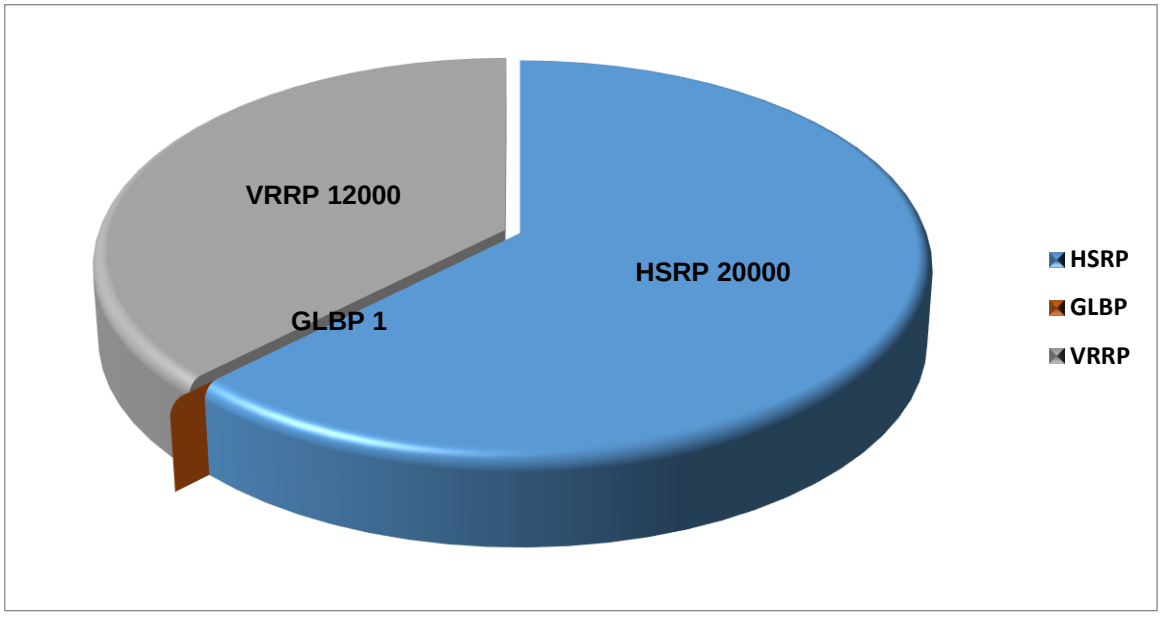
Tiempo de reposición en la comunicación de una red informática.

Tabla 2-Análisis de tiempo de reposición en la comunicación de una red informática

Protocolo	HSRP	GLBP	VRRP
Tiempo en ms	20000ms	1ms	12000ms

Fuente: Elaboración Propia

Ilustración 33-Análisis de tiempo de reposición en la comunicación de una red informática



Fuente: Elaboración Propia

En la ilustración 33 puede apreciarse que los tiempos en milisegundos varían de protocolo en protocolo, obteniendo como resultado que el protocolo HSRP en cuanto a la reposición de la comunicación es de 20000 milisegundos, el protocolo GLBP en el

análisis de la reposición de la comunicación es 1 milisegundos, con respecto al análisis del protocolo VRRP en cuanto a la reposición es 12000 milisegundos, de la red informática.

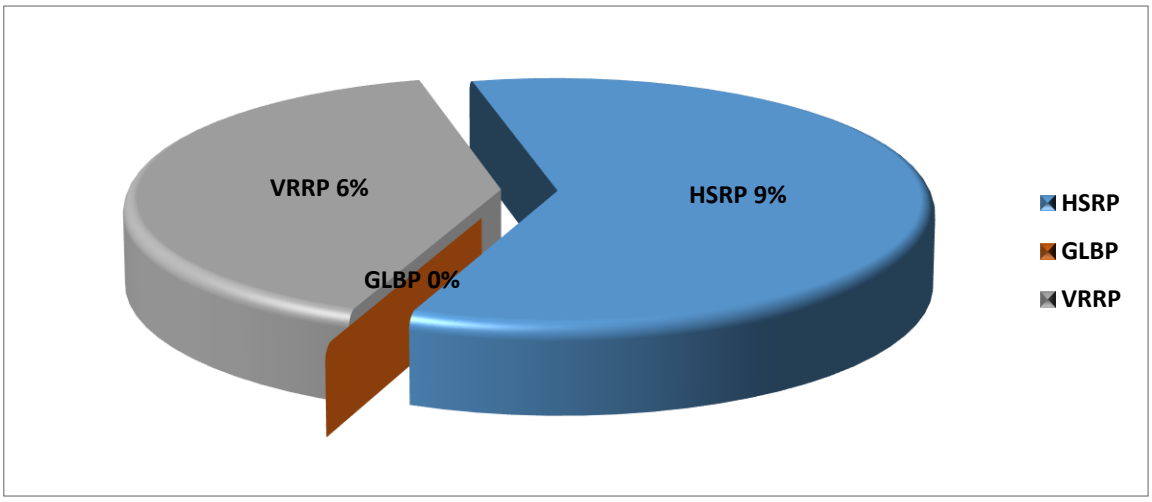
Cantidad de paquetes perdidos en las comunicaciones de la red informática

Tabla 3-Análisis Cantidad de paquetes perdidos en las comunicaciones de una red informática

CANTIDAD PAQUETES	HSRP	GLBP	VRRP
150	9%	0%	6%

Fuente: Elaboración Propia

Ilustración 34- Análisis Cantidad de paquetes perdidos en las comunicaciones de una red informática



Fuente: Elaboración Propia

En la ilustración 34 puede apreciarse que el porcentaje de los paquetes perdidos por protocolo son significativos, obteniendo como resultado que el protocolo HSRP en cuanto a la cantidad de

paquetes perdidos es de un 9%, el protocolo GLBP en cuanto al porcentaje de la cantidad de paquetes perdidos en las comunicaciones de la red informática es 0%, con respecto al protocolo VRRP el porcentaje de la cantidad de paquetes perdidos en las comunicaciones de la red informática es 6%.

4.2. Contrastación de Hipótesis

La contrastación de la hipótesis se realizó teniendo en cuenta los indicadores de la variable dependiente.

Formulación de Hipótesis

H_0 : Hipótesis Nula.

$$H_0: \quad \mu_{HSRP} - \mu_{GLBP} = 0$$

El tiempo de caída en la comunicación de la red informática utilizando el protocolo de alta disponibilidad HSRP es igual al tiempo de caída del protocolo GLBP.

H_A: Hipótesis Alterna.

$$H_A: \quad \mu_{HSRP} - \mu_{GLBP} > 0$$

El tiempo de caída en la comunicación de la red informática utilizando el protocolo de alta disponibilidad GLBP es menor al tiempo de caída del protocolo HSRP.

Protocolo	HSRP	GLBP
Tiempo en ms	13000ms	1ms

$$\mu_{HSRP} - \mu_{GLBP} > 0$$

13000ms - 1ms = 12999 ms

Decisión

$12999\ \text{ms} \in$ a la región crítica. Por tanto se rechaza la hipótesis nula y se acepta la hipótesis alterna.

Conclusión

Se estima que el tiempo de caída en la comunicación de la red informática utilizando el protocolo de alta disponibilidad GLBP es menor que el tiempo de caída del protocolo HSRP mejorando la disponibilidad de la red informática en un 99.99%.

Formulación de Hipótesis

H_0 : Hipótesis Nula.

$$H_0: \quad \mu_{\boldsymbol{VRRP}} - \mu_{GLBP} = 0$$

El tiempo de caídas en la comunicación de la red informática utilizando el protocolo de alta disponibilidad VRRP es igual al tiempo de caída del protocolo GLBP.

H_A: Hipótesis Alterna.

$$H_A: \quad \mu_{HSRP} - \mu_{GLBP} > 0$$

El tiempo de caída de la red informática utilizando el protocolo de

alta disponibilidad GLBP es menor al tiempo de caída del protocolo VRRP.

Protocolo	VRRP	GLBP
Tiempo en ms	5000ms	1ms

$$\mu_{\boldsymbol{VRRP}} - \mu_{\mathrm{GLBP}} > 0$$

5000ms - 1ms = 4999ms

Decisión

$4999\ \mathrm{ms}\ \in$ a la región crítica. Por tanto se rechaza la hipótesis nula y se acepta la hipótesis alterna.

Conclusión

Se estima que el tiempo de caída en la comunicación de la red informática utilizando el protocolo de alta disponibilidad GLBP es menor que el tiempo de caída de la comunicación del protocolo VRRP mejorando la disponibilidad de la red informática en un 99.99%.

4.3. Discusión de resultados

El análisis con cada uno de los protocolos de mi investigación he podido llegar que el protocolo GLBP es el más eficiente ya que este

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

protocolo tiene como principal funcionalidad el balanceo de carga, asimismo configurar el método Round Robin, El protocolo GLBP hace que los routers redundantes estén activos/activos mejorando la disponibilidad de la red informática, Esto corrobora las apreciaciones de (YEROVI & VALERIA, 2010) , quienes mencionan sus resultados en cuanto a los análisis de los protocolos utilizados en el diseño de redes campus, el protocolo GLBP del cual no pudieron obtener resultados en los tiempos de transmisión de archivos planos, 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 permitiendo el buen funcionamiento en la interconectividad y disponibilidad de la red campus,

Según (GALIANO, 2012) hace referencia de sus resultado El protocolo VRRP que es el que se implementó para proveer de alta disponibilidad a la red corporativa usa paquetes que se envían después de intervalos de tiempo determinados estos paquetes son bastante pequeños y el tiempo total que toma su análisis es despreciable por lo que el funcionamiento del sistema es bastante aceptable una de las características que se debe tomar en cuenta es que, en el caso de que exista un fallo del sistema primario el sistema secundario inunda la red con paquetes ARP, informando del fallo a

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

los distintos usuarios conectados, este intercambio de sistema toma tiempos menores a los 40 mili segundos, por lo que el índice de disponibilidad del sistema sería prácticamente del 100%, contrastando con mis resultados obtenidos que el protocolo VRRP en cuanto a la reposición y a las caídas de la comunicación de la red informática es de 5000 y 12000 milisegundos, esto conlleva a que el protocolo VRRP no es factible para su implementación en esta investigación, dando a lugar a que el protocolo GLBP es el más eficiente para la disponibilidad de una red informática

CAPITULO V: DESARROLLO DE PROPUESTA.

5.1 Reunir requisitos y expectativas

Ha sido el proceso destinado a recabar información para ayudar a

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

aclarar e identificar cualquier problema de la red actual.

Se formuló las siguientes preguntas al reunir la información:

a) Quienes son las personas que utilizan la red.
b) Datos críticos de la organización.
c) Que operaciones han sido declaradas críticas por la organización.
d) Protocolos permitidos en la red.
e) Cuantos hosts son soportados y cuáles son los tipos.
f) Quien es el responsable de las direcciones, la denominación, el diseño de topología y la configuración de las LAN.

a) Las personas que utilizan la red

Los beneficiados participaran de una comunicación rápida e integral lo que permitirá aumentar la eficiencia y efectividad de todos los trabajadores utilizando los servicios informáticos y facilitar el acceso a todos aquellos que querían conectarse, se lograra incrementar la movilidad y flexibilidad en sus coordinaciones reduciendo tiempo y problemas con la correcta y oportuna disponibilidad de la información.

b) Datos críticos de la organización

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Los datos críticos se encontraran en los servidores o aplicaciones que requieran de una atención rápida, reduciendo tiempo y los problemas venideros para las organizaciones.

c) Que operaciones han sido declaradas críticas por la organización

Los servicios informáticos que se brindaran a través de los diferentes servidores, porque se tendrá que brindar un servicio confiable y disponible las 24 horas del día.

d) Protocolos permitidos en la red

Los protocolos a usar son los siguientes:

Redes Inalámbricas

- IEEE 802.3
- DHCP
- WPS
- Authentication Method Exted Service Set ID (ESSID)
- Power over Ethernet

Telefonía IP

- IP
- Compresiones G.711 y G.729
- Session Initiation Protocol (SIP) puerto 5060

Red LAN

- Sistema de nombres de dominio (DNS): TCP/UDP 53.
- Protocolo de transferencia de hipertexto (HTTP), TCP 80.
- Protocolo simple de transferencia de correo (SMTP): TCP 25.
- Protocolo de oficina de correos (POP): UDP 110.
- Telnet: TCP 23.
- Protocolo de configuración dinámica de host (DHCP): UDP 67.
- Protocolo de transferencia de archivos (FTP): TCP 20 y 21.
- Protocolo de transferencia Datos SQL (TCP): TCP 1433.

e) Hosts Soportados

Son todos los host de la organización.

f) Responsable de las direcciones, la denominación, el diseño de topología y la configuración de las LAN

Son los administradores de la información y comunicación, el cual desempeña sus funciones en las diferentes organizaciones.

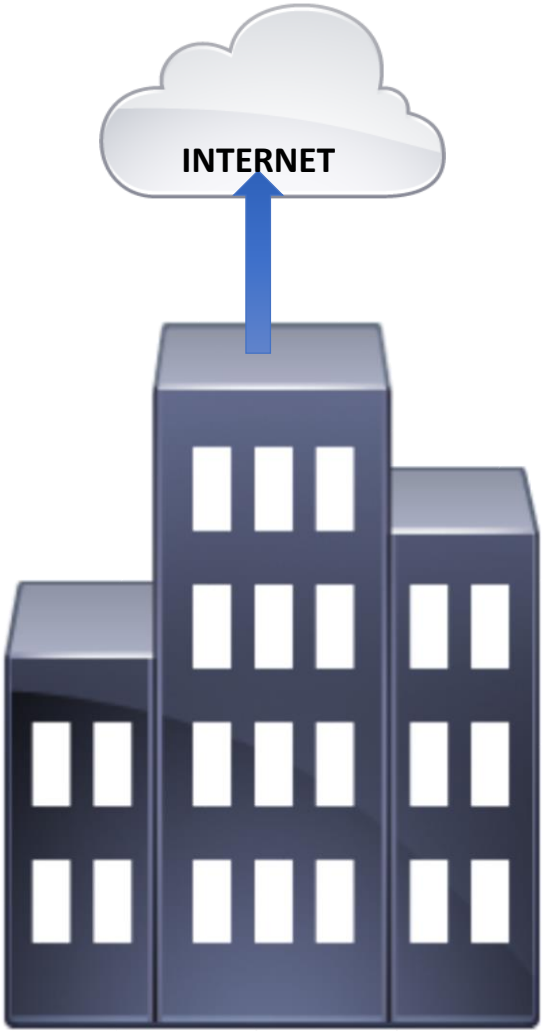
Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

5.2 Diseñar la estructura o topología de las Capas 1, 2 y 3 de la LAN.

5.2.1. Capa Física

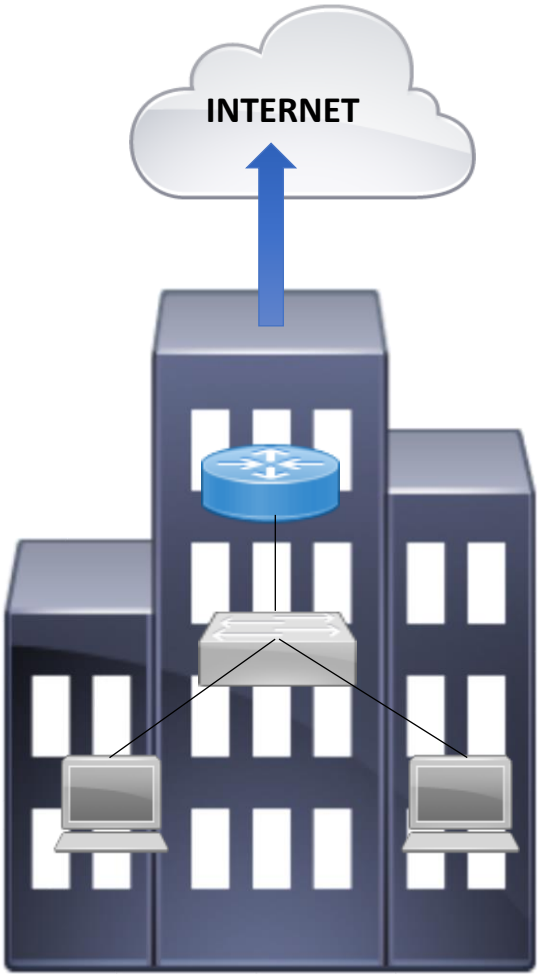
En la capa física se muestra el diseño de redes actuales y propuestas.

Ilustración 35- Ilustración Contextual de la Red



Fuente: Elaboración Propia

Ilustración 36- Ilustración Contextual de la Red



Fuente: Elaboración propia

5.2.2. Capa de enlace de datos

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Se sugiere un modelo jerárquico de capas (núcleo, distribución, acceso).

5.2.3. Capa de Red

Se realizó el direccionamiento IP. Según topología

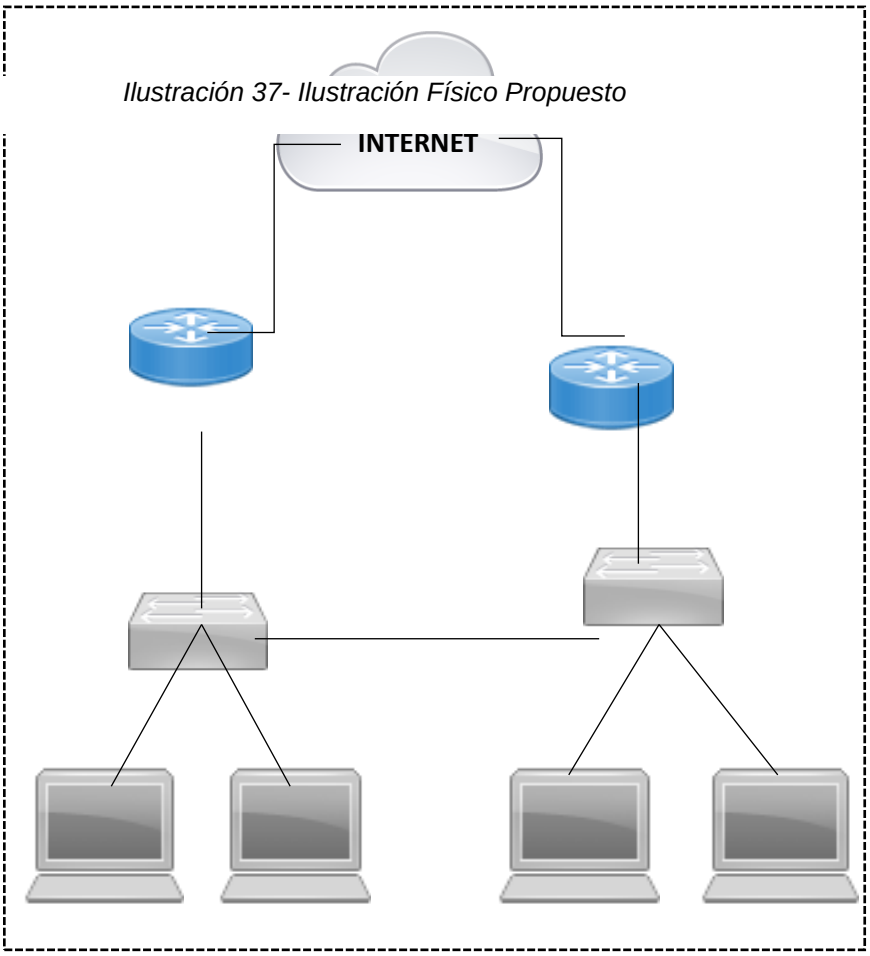
Tabla 4- Direccionamiento IP

Direccionamiento IP	Mascara	Default Gateway
10.1.1.0/30	255.255.255.252	----------
10.1.1.1/30	255.255.255.252	----------
10.1.1.2/30	255.255.255.252	----------
10.2.2.0/30	255.255.255.252	----------
10.2.2.1/30	255.255.255.252	----------
10.2.2.2/30	255.255.255.252	----------
192.168.10.0/24	255.255.255.0	----------
192.168.10.1/24	255.255.255.0	----------
192.168.10.254/24	255.255.255.0	----------
192.168.10.2/24	255.255.255.0	192.168.10.1
192.168.10.3/24	255.255.255.0	192.168.10.1
192.168.10.4/24	255.255.255.0	192.168.10.1
192.168.10.5/24	255.255.255.0	192.168.10.1
192.168.10.200	----------	----------

Fuente: Elaboración Propia

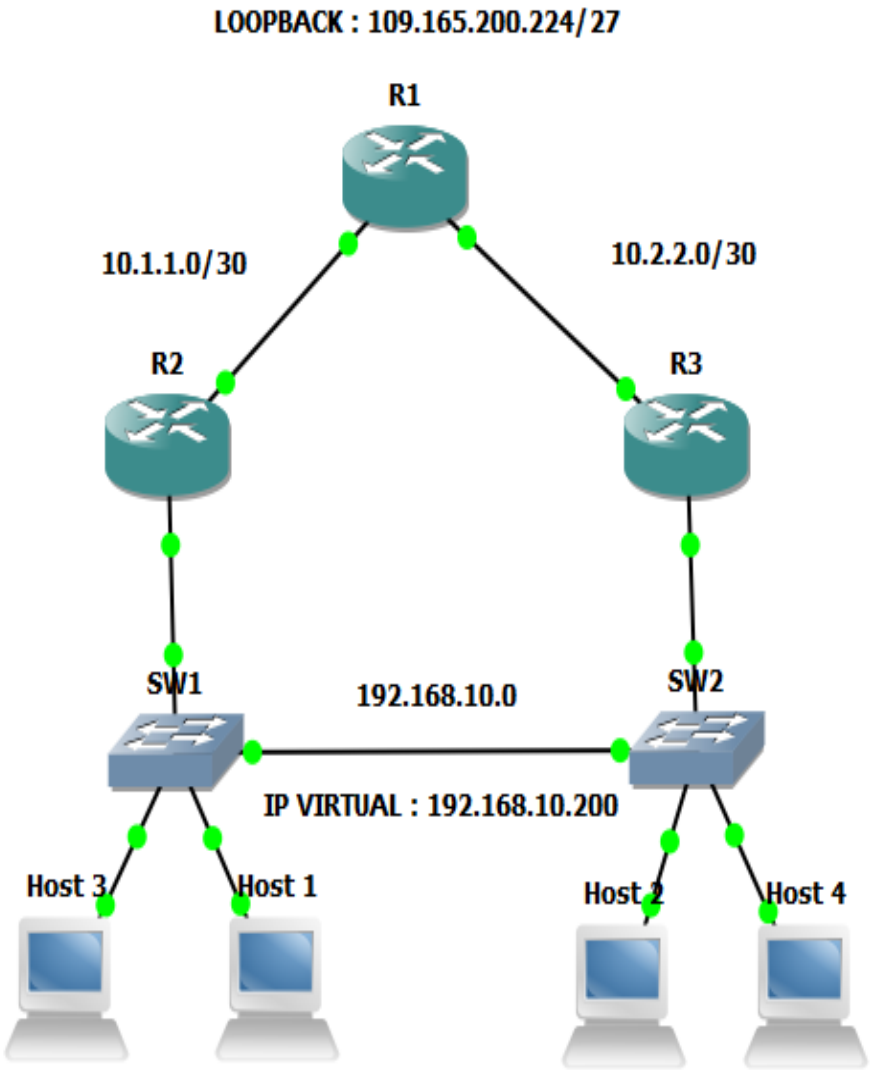
5.3. Diseñar la Físico y Lógico

Ilustración 37- Ilustración Físico Propuesto



Fuente: Elaboración propia

Ilustración 38- Topología de Red-Prototipo



Fuente: Elaboración propia

5.4. Implementación de los protocolos de alta disponibilidad - Prototipo

Ilustración 39- configuración con hyperterminal en equipo cisco Router 2901- protocolo HSRP

```
ce - HyperTerminal
Archivo  Edición  Ver  Llamar  Transferir  Ayuda
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 10.1.1.2 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.10.1 255.255.255.0
 standby 1 ip 192.168.10.200
 standby 1 priority 150
 standby 1 preempt
 duplex auto
 speed auto
!
!
router eigrp 10
 network 10.1.1.0 0.0.0.3
 network 192.168.10.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
logging trap debugging
 --More-- _
1:50:28 conectado  Autodetect.  9600 8-N-1  DESPLAZAR  MAY  NUM  Capturar  Imprimir
```

Fuente: Elaboración propia

Ilustración 40- Router R2 –State is Active

```
ce - HyperTerminal
Archivo  Edición  Ver  Llamar  Transferir  Ayuda
!
scheduler allocate 20000 1000
end

R2#show st
R2#show stan
R2#show standby
GigabitEthernet0/1 - Group 1
  State is Active
    23 state changes, last state change 00:30:38
  Virtual IP address is 192.168.10.200
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.648 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.10.254, priority 100 (expires in 9.760 sec)
  Priority 150 (configured 150)
  Group name is "hsrp-Gi0/1-1" (default)
R2#
Oct 16 11:08:11.067: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthe
rnet0/1, changed state to down
Oct 16 11:08:12.067: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state
 to down
Oct 16 11:08:12.067: %HSRP-5-STATECHANGE: GigabitEthernet0/1 Grp 1 state Active
-> Init
Oct 16 11:08:12.067: %DUAL-5-NBRCHANGE: EIGRP-IPv4 10: Neighbor 192.168.10.254 (
GigabitEthernet0/1) is down: interface down
Oct 16 11:08:17.067: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.10.10
 port 514 started - reconnection
R2#
R2#
```

Fuente: Elaboración propia

Ilustración 41- Verificando la conexión con mensajes de ICMP hacia la IP 109.165.200.225

```
^C
C:\Users\CesarCRXD>ping 109.165.200.225 -t

Haciendo ping a 109.165.200.225 con 32 bytes de datos:
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=22ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
```

Fuente: Elaboración propia

Ilustración 42- Caída de enlace-HSRP

```
C:\Windows\system32\cmd.exe - ping 109.165.200.225 -t
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=46ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo=1ms TTL=254
Respuesta desde 109.165.200.225: bytes=32 tiempo<1m TTL=254
```

Fuente: Elaboración propia

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Ilustración 43- Router R2 –Comando SHOW STANDBY- State Init

```
ce - HyperTerminal
Archivo  Edición  Ver  Llamar  Transferir  Ayuda

   Hello time 3 sec, hold time 10 sec
     Next hello sent in 1.648 secs
   Preemption enabled
   Active router is local
   Standby router is 192.168.10.254, priority 100 (expires in 9.760 sec)
   Priority 150 (configured 150)
   Group name is "hsrp-Gi0/1-1" (default)
R2#
Oct 16 11:08:11.067: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthe

rnet0/1, changed state to down
Oct 16 11:08:12.067: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state
 to down
Oct 16 11:08:12.067: %HSRP-5-STATECHANGE: GigabitEthernet0/1 Grp 1 state Active
-> Init
Oct 16 11:08:12.067: %DUAL-5-NBRCHANGE: EIGRP-IPv4 10: Neighbor 192.168.10.254 (
GigabitEthernet0/1) is down: interface down
Oct 16 11:08:17.067: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.10.10
 port 514 started - reconnection
R2#
R2#show standby
GigabitEthernet0/1 - Group 1
  State is Init (interface down)
    24 state changes, last state change 00:01:08
  Virtual IP address is 192.168.10.200
  Active virtual MAC address is unknown
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
  Preemption enabled
  Active router is unknown
  Standby router is unknown
  Priority 150 (configured 150)
  Group name is "hsrp-Gi0/1-1" (default)
R2#
```

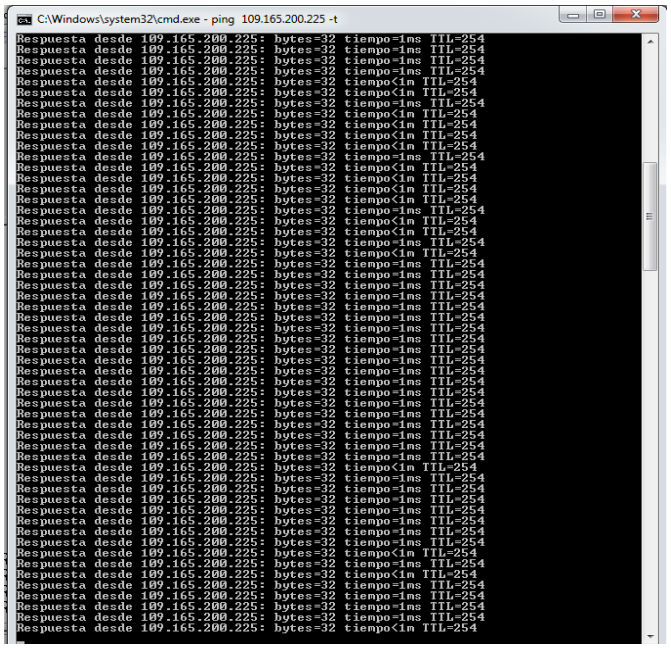
Fuente: Elaboración propia

Ilustración 44- Comando SHOW GLBP- State Active R2

```
ce - HyperTerminal
Archivo  Edición  Ver  Llamar  Transferir  Ayuda

R3(config)#
% Incomplete command.

R2(config)#
R2(config)#
R2(config)#
R2(config)#
R2(config)#do show glbp
GigabitEthernet0/1 - Group 1

  State is Active
    1 state change, last state change 00:03:57
  Virtual IP address is 192.168.10.200
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.088 secs
  Redirect time 600 sec, forwarder timeout 14400 sec
  Preemption enabled, min delay 0 sec
  Active is local
  Standby is 192.168.10.254, priority 100 (expires in 9.312 sec)
  Priority 150 (configured)
  Weighting 100 (default 100), thresholds: lower 1, upper 100
  Load balancing: round-robin
  Group members:
    a44c.11eb.3501 (192.168.10.1) local
    a493.4ccd.ce48 (192.168.10.254)
  There are 2 forwarders (1 active)
  Forwarder 1
    State is Active
      1 state change, last state change 00:03:45
    MAC address is 0007.b400.0101 (default)
    Owner ID is a44c.11eb.3501
    Redirection enabled
    Preemption enabled, min delay 30 sec
 --More--
```

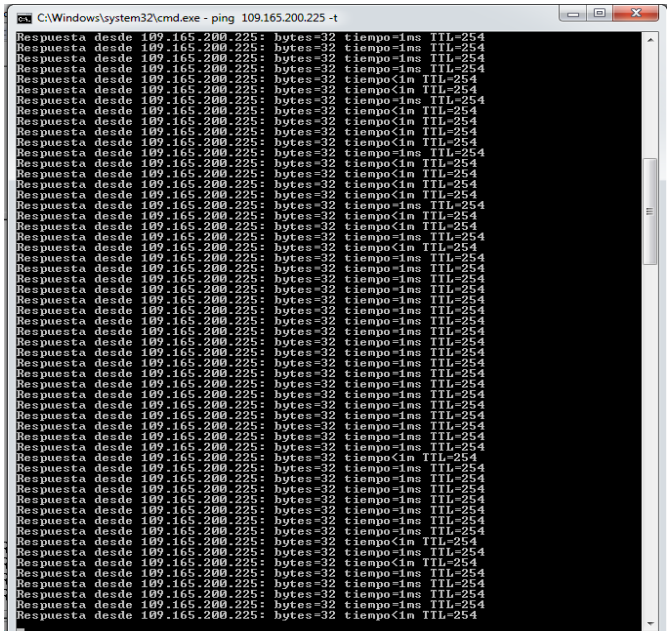
Fuente: Elaboración propia

Ilustración 45- Verificando la conexión con mensajes de ICMP hacia la IP 109.165.200.225-GLBP



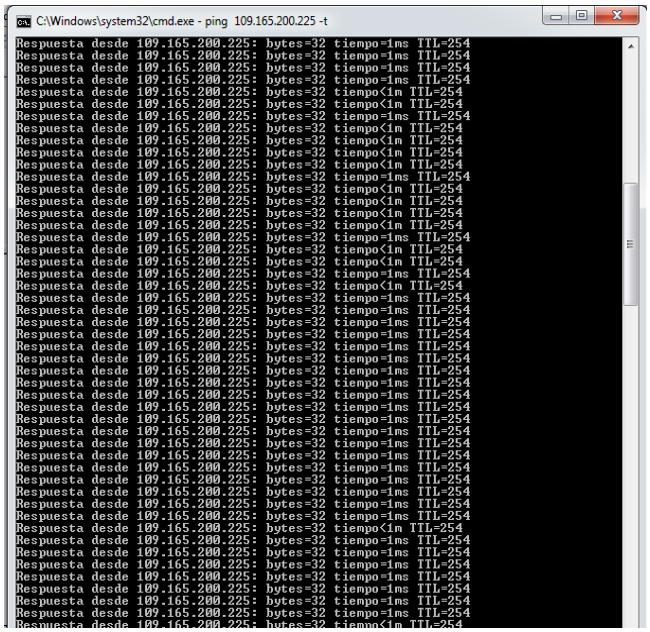
Fuente: Elaboración propia

Ilustración 46- Caída de enlace-GLBP



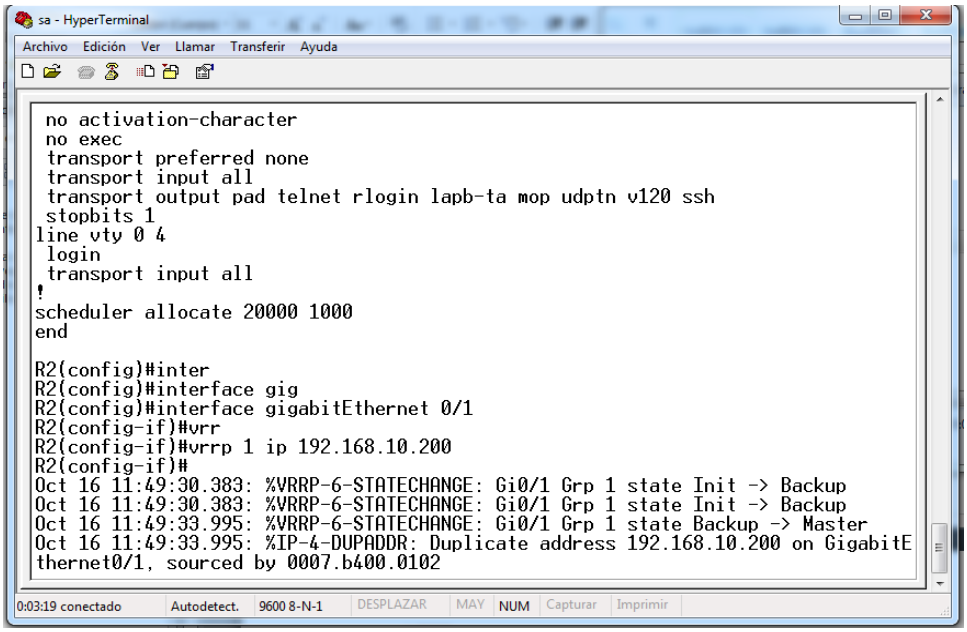
Fuente: Elaboración propia

Ilustración 47- Reposición de enlace-GLBP



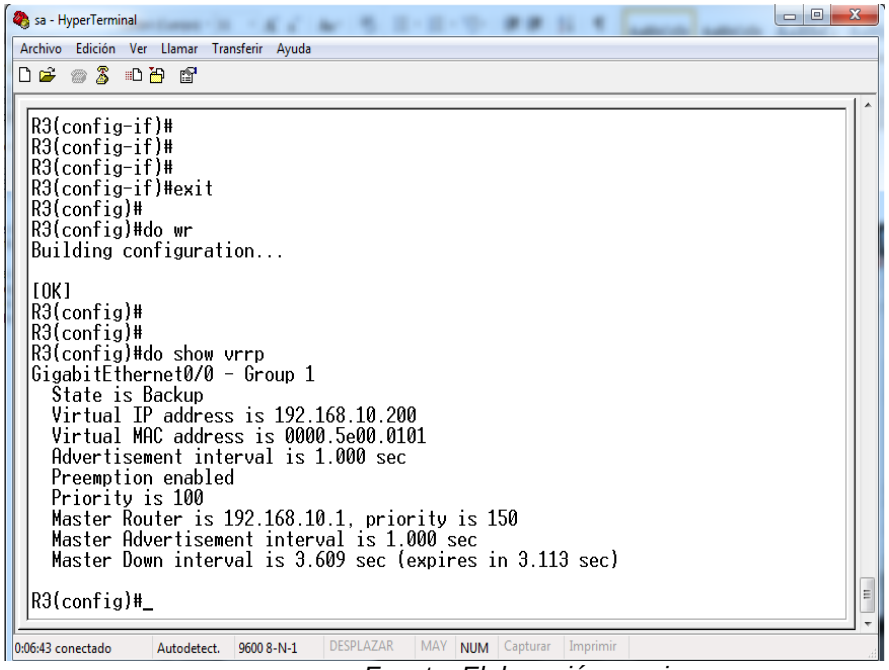
Fuente: Elaboración propia

Ilustración 48- configuración con hyperterminal en equipo cisco router 2901- protocolo VRRP



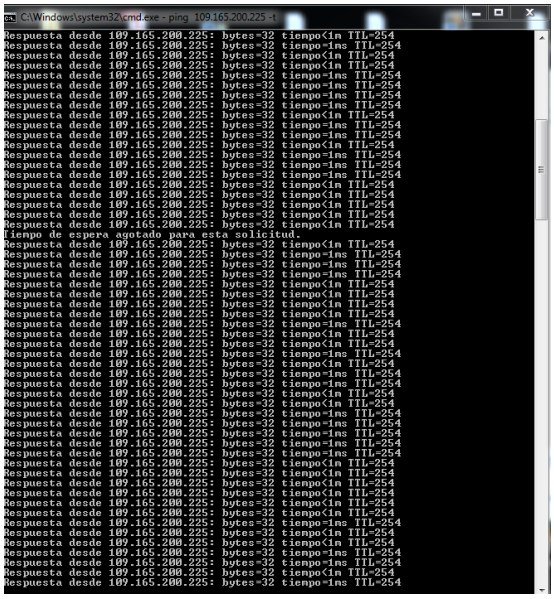
Fuente: Elaboración propia

Ilustración 49- Router R3- State is Backup



Fuente: Elaboración propia

Ilustración 50- Caída de enlace VRRP



Fuente: Elaboración propia

CAPITULO VI: CONCLUSIONES Y RECOMENDACIONES.

6.1 Conclusiones

A. Al Objetivo Específico 1: Diagnosticar el estado actual de la disponibilidad de una red informática.

Al finalizar la investigación se concluye con el análisis de cada uno de los protocolos, obteniendo como resultado que el protocolo HSRP en cuanto a la caída de la comunicación con un tiempo estimado de 13000 mili segundos, el tiempo en reposición de la comunicación es de 20000 mili segundos y la cantidad de paquetes perdidos es de un 9% como resultado del análisis, el protocolo HSRP no es factible para mejorar la disponibilidad de una red informática.

En cuanto al análisis del protocolo VRRP los resultados obtenidos en la caída de la comunicación con un tiempo estimado de 5000 milisegundos, el tiempo de reposición de la comunicación de 12000 milisegundos y la cantidad de paquetes perdidos es de un 6%, como resultado del análisis el protocolo VRRP no es factible para mejorar la disponibilidad de una red informática.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Lo cual nos lleva a la conclusión del análisis del protocolo GLBP durante los escenarios de pruebas obtenidos como resultados durante la caída de la comunicación con un tiempo estimado de 1 milisegundos, con un tiempo en la reposición de la comunicación de 1 milisegundos y el porcentaje de la cantidad de paquetes perdidos en las comunicaciones de la red informática es 0%, siendo el más eficiente mejorando la disponibilidad de la red informática.

(Ver anexo 1 – Instrumentos de recolección de datos. Resultados.)

B. Al Objetivo Especifico 2: Analizar los factores influyentes en la disponibilidad de una red informática.

En base al análisis de los datos recolectados se han identificado los siguientes factores influyentes:

- La efectividad del protocolo de alta disponibilidad.
- El nivel de eficiencia del protocolo para mejorar la disponibilidad de la red informática.

(Ver anexo 2 – Instrumentos de recolección de datos. Resultados.)

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

C. Implementar protocolos de comunicación para mejorar la disponibilidad de una red informática.

Al finalizar la investigación se implementó en una red local los protocolos de alta disponibilidad, basándose en el buen funcionamiento del protocolo GLBP y mejorando la disponibilidad de la red informática.

D. Estimar los resultados que generara la implantación de protocolos de comunicación en la disponibilidad de una red informática.

Luego de desarrollar la validación de la propuesta de la implementación de protocolos de alta disponibilidad, mediante el juicio de expertos, se concluye que este tiene una alta probabilidad de éxito, debido a que es considerado como adecuado y coherente en su estructura, está orientado al objetivo de la investigación, ha considerado todos los aspectos necesarios para resolver el problema, generará los resultados establecidos en la hipótesis y cada una de sus partes es considerada como buena o excelente. Toda la propuesta es considerada como buena, siendo la principal sugerencia la designación de recursos para su implementación.

(Ver anexo 2– Ficha de validación por juicio de experto)

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

6.2 Recomendaciones

Se recomienda tener en cuenta la importancia del protocolo GLBP protocolo que se puede implementar en equipos CISCO, tal como se demostró en esta investigación que generara muchos beneficios, garantizando la alta disponibilidad ya que es un protocolo que posee balanceo de carga y que permite el buen funcionamiento de las comunicaciones de una red informática.

Se recomienda tener en cuenta al momento de configurar el protocolo GLBP para la alta disponibilidad implementar el método de selección Round Robin.

Es recomendable evaluar de manera progresiva los resultados obtenidos en cuanto a la implementación del protocolo de alta disponibilidad, identificando los factores influyentes y estableciendo planes de mejora continua, permitiendo incrementar el grado de efectividad de la propuesta.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

REFERENCIAS:

METODOLOGÍA DEL DESARROLLO CON CISCO. (2014). Obtenido de http://metodologiaspararedes.blogspot.com/

AVAILABILITY, H. (2002). ALTA DISPONIBILIDAD EN DB. *http://www.cisco.com/c/en/us/support/docs/availability/high-availability/25562-ios-management.pdf*, 5.

BECERRA, M. G. (2012). Modelo administrativo para gestión de servidores Linux,. *M.Sc en informática Universidad Industrial de Santander*, 1-11.

Cecilia M. Lasserre, E. L. (2010). *SISTEMAS DE CÓMPUTO DE ALTAS PRESTACIONES CON ALTA DISPONIBILIDAD:EVALUACIÓN DE LA PERFORMANCE EN DIFERENTES CONFIGURACIONES.* ARGENTINA: http://hdl.handle.net/10915/19825.

CHIA-TAI TSAI, R.-H. J. (2010). *Optimal redundancy allocation for high availability routers.* Filipinas: INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS.

Cisco. (2013). Extending Switched Networks with Virtual LANs. *CCNA Self-Study (ICND Exam)*, 5.

Cisco Systems, I. (2010). *Configuring VRRP.* 170 West Tasman Drive, San Jose: Americas Headquarters:.

Cisco Systems, I. (2011). TRILL. *The Internet Protocol Journal*, 2-20.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Cisco Systems, I. (2012). *Configuring HSRP, VRRP, and GLBP.* 170 West Tasman Drive, San Jose.

Cisco Systems, I. (2013). *Escalamiento de redes.* San Jose EE.UU.

Cisco Systems, I. (2013). *Introducción a redes.* 170 West Tasman Drive, San Jose.

Cisco Systems, I. (2015). Virtual Switching Systems (VSS). *First Hop Redundancy Protocols Configuration Guide, Cisco IOS Release 15SY*.

Cisco, S. (2015). GLBP en el ejemplo de configuración de los Catalyst 6500 Switch. *Switches Cisco Catalyst de la serie 6500*, 1-4.

GALIANO, F. A. (2012). *SOLUCIÓN DE FIREWALL CON ALTA DISPONIBILIDAD PARA REDES CORPORATIVAS UTILIZANDO VYATTA CON VIRTUALIZACIÓN.* SANGOLQUÍ – ECUADOR.

González, F. G. (2013). *Diseño de una arquitectura escalable y de alta Disponibilidad para un Sistema middleware.* Madrid.

Guangping, X., Yong, M., Wenhui, M., Gang, W., & Xiaoguang. (and Parallel/Distributed Computing,). Model and Evaluation Of Redundant Data Organization For High Availity in Structured Overly Networks. *Software Engineering, Artificial Intelligences, Networking*, 447-452.

LEÓN FEIJOÓ, A. A. (2010). *DISEÑO DE ALTA DISPONIBILIDAD EN SERVIDORES SOLARIS 10 PARA APLICACIÓN EN EL CENTRO*

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

DE CÓMPUTO DE LA U.C.S.G. GUAYAQUIL – ECUADOR.

Luis Velasco, S. S. (2006). Alta disponibilidad en redes ASON/GMPLS. *Grupo de Comunicaciones Ópticas*, 1-9.

Moreno, J. C. (2015). *Sistemas web con alta Disponibilidad en cloud.* España, Madrid.

NATALI DEL ROCIO YEROVILLUAY, J. V. (2010). *ANALISIS DE PROTOCOLOS DE ALTA DISPONIBILIDAD DE GATEWAYS EN LA INTERCONECTIVIDAD LAN/WAN APLICADAS AL DISEÑO DE REDES DE CAMPUS.* RIOBAMBA, ECUADOR.

PALOMO, G. N. (2012). *ANÁLISIS Y DISEÑO DE UNA RED DE ALTA DISPONIBILIDAD PARA CENTRALES ASTERISK BASADA EN LA TECNOLOGÍA DUNDi.* RIOBAMBA – ECUADOR.

Research Scholar, J. U. (2011). High Availability Using Virtualization. *International Transactions in Applied Sciences*, 1-7.

Ulrik Franke, P. J. (2012). Availability of enterprise IT systems: an expert-based. *Software Qual J*, 3-5.

YEROVI, L. N., & VALERIA, F. O. (2010). *ANALISIS DE PROTOCOLOS DE ALATA DISPONIBILIDAD DE GATEWAYS EN LA INTERCONECTIVIDAD LAN/WAN APLICADAS AL DISEÑO DE REDES DE CAMPUS.* RIOBAMBA.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

ANEXOS

CONFIGURACION DEL PROTOCOLO HSRP

CONFIGURACION DE ROUTER R1

```
R1>enable
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ip add 10.1.1.1 255.255.255.252
R1(config-if)#no sh
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
R1(config-if)#exit
R1(config)#interface gigabitEthernet 1/0
R1(config-if)#ip add 10.2.2.1 255.255.255.252
R1(config-if)#no sh

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up

R1(config-if)#exit
R1(config)#
R1(config)#do wr
Building configuration...
[OK]
R1(config)#interface loopback 1
R1(config-if)#ip add 109.165.200.225 255.255.255.224
R1(config-if)#exit

%LINK-5-CHANGED: Interface Loopback1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1,
changed state to up

R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 1
%Default route without gateway, if not a point-to-point interface, may
```

```
impact performance

R1(config)#router eigrp 10
R1(config-router)#network 10.1.1.0 0.0.0.3
R1(config-router)#network 10.2.2.0 0.0.0.3
R1(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 10.1.1.2
(GigabitEthernet0/0) is up: new adjacency
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 10.2.2.2
(GigabitEthernet0/1) is up: new adjacency

R1(config-router)#redistribute static
R1(config-router)#exit
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*    0.0.0.0/0 is directly connected, Loopback1
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.1.1.0/30 is directly connected, GigabitEthernet0/0
L        10.1.1.1/32 is directly connected, GigabitEthernet0/0
C        10.2.2.0/30 is directly connected, GigabitEthernet1/0
L        10.2.2.1/32 is directly connected, GigabitEthernet1/0
      109.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        109.165.200.224/27 is directly connected, Loopback1
L        109.165.200.225/32 is directly connected, Loopback1
D     192.168.10.0/24 [90/3072] via 10.2.2.2, 00:03:27, GigabitEthernet1/0
                      [90/3072] via 10.1.1.2, 00:03:27, GigabitEthernet0/0
R1#


R1(config)#do wr
Building configuration...
[OK]
```

CONFIGURACION DE ROUTER R2

```
R2>enable
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#
R2(config)#interface gigabitEthernet 0/0
R2(config-if)#ip add 10.1.1.2 255.255.255.252
R2(config-if)#no sh

%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up

R2(config-if)#exit

R2(config)#interface gigabitEthernet 1/0
R2(config-if)#ip add 192.168.10.1 255.255.255.0
R2(config-if)#no sh
R2(config-if)#exit
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up

R2(config)#do wr
Building configuration...
[OK]
R2(config)#router eigrp 10
R2(config-router)#network 10.1.1.0 0.0.0.3
R2(config-router)#network 192.168.10.0
R2(config-router)#exit
R2(config)#do wr
Building configuration...
[OK]
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.10.254
(GigabitEthernet0/1) is up: new adjacency
```


Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up

%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 10.1.1.1
(GigabitEthernet0/0) is up: new adjacency

R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.1.1.1 to network 0.0.0.0

D*EX  0.0.0.0/0 [170/130816] via 10.1.1.1, 00:09:59, GigabitEthernet0/0
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.1.1.0/30 is directly connected, GigabitEthernet0/0
L        10.1.1.2/32 is directly connected, GigabitEthernet0/0
D        10.2.2.0/30
           [90/3072] via 192.168.10.254, 00:09:59, GigabitEthernet1/0
           [90/3072] via 10.1.1.1, 00:09:59, GigabitEthernet0/0
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet1/0
L        192.168.10.1/32 is directly connected, GigabitEthernet1/0
R2#


R2(config)#interface gigabitEthernet 1/0
R2(config-if)#standby 1 ip 192.168.10.200
R2(config-if)#standby 1 priority 150
R2(config-if)#standby 1 preempt delay minimum 5
R2(config)#do wr
Building configuration...
[OK]

%HSRP-6-STATECHANGE: GigabitEthernet0/1 Grp 1 state Speak ->
Standby

%HSRP-6-STATECHANGE: GigabitEthernet0/1 Grp 1 state Standby ->
Active
```

```
R2#show stan
R2#show standby
GigabitEthernet1/0 - Group 1 (version 2)
  State is Active
    2 state changes, last state change 01:49:12
  Virtual IP address is 192.168.10.200
  Active virtual MAC address is 0000.0c9f.f001
  Local virtual MAC address is 0000.0c9f.f001 (v2 default)
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 2.224 secs
  Preemption disabled
  Active router is local
  Standby router is 192.168.10.254, priority 100 (expires in 9.776 sec)
  Priority 150 (configured 150)
  Group name is "hsrp-Gi1/0-1" (default)
 %HSRP-6-STATECHANGE: GigabitEthernet0/1 Grp 1 state Active -> Init

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to down
```

CONFIGURACION ROUTER R3

```
R3>enable
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface gigabitEthernet 0/0
R3(config-if)#ip add 10.2.2.2 255.255.255.252
R3(config-if)#no sh
R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

R3(config-if)#exit
R3(config)#interface gigabitEthernet 1/0
R3(config-if)#ip add 192.168.10.254 255.255.255.0
R3(config-if)#no sh
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up

R3(config-if)#exit
```

```
R3(config)#
R3(config)#
R3(config)#do wr
Building configuration...
[OK]
R3(config)#router eigrp 10
R3(config-router)#network 10.2.2.0 0.0.0.3
R3(config-router)#network 192.168.10.0
R3(config-router)#exit
R3(config)#do wr
Building configuration...
[OK]
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.10.1
(GigabitEthernet0/1) is up: new adjacency

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up

%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 10.2.2.1
(GigabitEthernet0/0) is up: new adjacency
do
% Incomplete command.

R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.2.2.1 to network 0.0.0.0

D*EX  0.0.0.0/0 [170/130816] via 10.2.2.1, 01:52:18, GigabitEthernet0/0
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
D        10.1.1.0/30 [90/3072] via 192.168.10.1, 01:52:23,
GigabitEthernet1/0
                     [90/3072] via 10.2.2.1, 01:52:23, GigabitEthernet0/0
C        10.2.2.0/30 is directly connected, GigabitEthernet0/0
L        10.2.2.2/32 is directly connected, GigabitEthernet0/0
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet1/0
```

```
L       192.168.10.254/32 is directly connected, GigabitEthernet1/0


R3(config)#interface gigabitEthernet 1/0
R3(config-if)#standby 1 ip 192.168.10.200
R3(config-if)#exit
R3(config)#do wr
Building configuration...
[OK]
R3(config)#exit
R3#show standby
GigabitEthernet1/0 - Group 1 (version 2)
  State is Standby
    1 state change, last state change 01:52:16
  Virtual IP address is 192.168.10.200
  Active virtual MAC address is 0000.0c9f.f001
    Local virtual MAC address is 0000.0c9f.f001 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.400 secs
  Preemption disabled
  Active router is 192.168.10.1, priority 150 (expires in 10.272 sec)
    MAC address is ca03.0c5c.001c
  Standby router is local
  Priority 100 (default 100)
  Group name is "hsrp-Gi1/0-1" (default)
```

CONFIGURACION DEL PROTOCOLO GLBP

CONFIGURACION DE ROUTER R1

```
R1>enable
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ip add 10.1.1.1 255.255.255.252
R1(config-if)#no sh
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
R1(config-if)#exit
R1(config)#interface gigabitEthernet 1/0
```

```
R1(config-if)#ip add 10.2.2.1 255.255.255.252
R1(config-if)#no sh

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up

R1(config-if)#exit
R1(config)#
R1(config)#do wr
Building configuration...
[OK]
R1(config)#interface loopback 1
R1(config-if)#ip add 109.165.200.225 255.255.255.224
R1(config-if)#exit

%LINK-5-CHANGED: Interface Loopback1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1,
changed state to up

R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 1
%Default route without gateway, if not a point-to-point interface, may
impact performance

R1(config)#router eigrp 10
R1(config-router)#network 10.1.1.0 0.0.0.3
R1(config-router)#network 10.2.2.0 0.0.0.3
R1(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 10.1.1.2
(GigabitEthernet0/0) is up: new adjacency
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 10.2.2.2
(GigabitEthernet0/1) is up: new adjacency

R1(config-router)#redistribute static
R1(config-router)#exit
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
```

```
      o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
      + - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*    0.0.0.0/0 is directly connected, Loopback1
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.0/30 is directly connected, GigabitEthernet0/0
L       10.1.1.1/32 is directly connected, GigabitEthernet0/0
C       10.2.2.0/30 is directly connected, GigabitEthernet1/0
L       10.2.2.1/32 is directly connected, GigabitEthernet1/0
     109.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       109.165.200.224/27 is directly connected, Loopback1
L       109.165.200.225/32 is directly connected, Loopback1
D     192.168.10.0/24 [90/3072] via 10.2.2.2, 00:03:27, GigabitEthernet1/0
                      [90/3072] via 10.1.1.2, 00:03:27, GigabitEthernet0/0
R1#


R1(config)#do wr
Building configuration...
[OK]
```

CONFIGURACION DE ROUTER R2

```
R2>enable
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#
R2(config)#interface gigabitEthernet 0/0
R2(config-if)#ip add 10.1.1.2 255.255.255.252
R2(config-if)#no sh

%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up

R2(config-if)#exit

R2(config)#interface gigabitEthernet 1/0
```

```
R2(config-if)#ip add 192.168.10.1 255.255.255.0
R2(config-if)#no sh
R2(config-if)#exit
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up

R2(config)#do wr
Building configuration...
[OK]
R2(config)#router eigrp 10
R2(config-router)#network 10.1.1.0 0.0.0.3
R2(config-router)#network 192.168.10.0
R2(config-router)#exit
R2(config)#do wr
Building configuration...
[OK]
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.10.254
(GigabitEthernet0/1) is up: new adjacency

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up

%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 10.1.1.1
(GigabitEthernet0/0) is up: new adjacency

R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.1.1.1 to network 0.0.0.0

D*EX  0.0.0.0/0 [170/130816] via 10.1.1.1, 00:09:59, GigabitEthernet0/0
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.1.1.0/30 is directly connected, GigabitEthernet0/0
L        10.1.1.2/32 is directly connected, GigabitEthernet0/0
D        10.2.2.0/30
```

```
          [90/3072] via 192.168.10.254, 00:09:59, GigabitEthernet1/0
          [90/3072] via 10.1.1.1, 00:09:59, GigabitEthernet0/0
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet1/0
L       192.168.10.1/32 is directly connected, GigabitEthernet1/0
R2#


R2(config)#interface gigabitEthernet 1/0
R2(config-if)#glbp 1 ip 192.168.10.200
R2(config-if)#glbp 1 priority 150
R2(config-if)# glbp 1 preempt delay minimum 5
R2(config-if)#glbp 1 load-balancing round-robin
R2(config)#do wr
Building configuration...
[OK]

%HSRP-6-STATECHANGE: GigabitEthernet0/1 Grp 1 state Activo->
Standby

%HSRP-6-STATECHANGE: GigabitEthernet0/1 Grp 1 state Standby ->
Active

R2#show glbp
GigabitEthernet1/0 - Group 1
  State is Active
    1 state change, last state change 00:04:09
  Virtual IP address is 192.168.10.200
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.944 secs
  Redirect time 600 sec, forwarder timeout 14400 sec
  Preemption enabled, min delay 0 sec
  Active is local
  Standby is 192.168.10.254, priority 100 (expires in 7.840 sec)
  Priority 150 (configured)
  Weighting 100 (default 100), thresholds: lower 1, upper 100
  Load balancing: round-robin
  Group members:
    ca03.0c5c.001c (192.168.10.1) local
    ca04.182c.001c (192.168.10.254)
  There are 2 forwarders (1 active)
  Forwarder 1
    State is Active
      1 state change, last state change 00:03:58
```

```
    MAC address is 0007.b400.0101 (default)
    Owner ID is ca03.0c5c.001c
    Redirection enabled
    Preemption enabled, min delay 30 sec
    Active is local, weighting 100
  Forwarder 2
    State is Listen
    MAC address is 0007.b400.0102 (learnt)
    Owner ID is ca04.182c.001c
    Redirection enabled, 597.856 sec remaining (maximum 600 sec)
    Time to live: 14397.856 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 192.168.10.254 (primary), weighting 100 (expires in 8.704 sec)
```

CONFIGURACION ROUTER R3

```
R3>enable
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface gigabitEthernet 0/0
R3(config-if)#ip add 10.2.2.2 255.255.255.252
R3(config-if)#no sh
R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

R3(config-if)#exit
R3(config)#interface gigabitEthernet 1/0
R3(config-if)#ip add 192.168.10.254 255.255.255.0
R3(config-if)#no sh
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up

R3(config-if)#exit
R3(config)#
R3(config)#
R3(config)#do wr
Building configuration...
[OK]
R3(config)#router eigrp 10
R3(config-router)#network 10.2.2.0 0.0.0.3
R3(config-router)#network 192.168.10.0
R3(config-router)#exit
```

```
R3(config)#do wr
Building configuration...
[OK]
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.10.1
(GigabitEthernet0/1) is up: new adjacency

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up

%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 10.2.2.1
(GigabitEthernet0/0) is up: new adjacency
do
% Incomplete command.

R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.2.2.1 to network 0.0.0.0

D*EX  0.0.0.0/0 [170/130816] via 10.2.2.1, 01:52:18, GigabitEthernet0/0
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
D        10.1.1.0/30 [90/3072] via 192.168.10.1, 01:52:23,
GigabitEthernet1/0
                     [90/3072] via 10.2.2.1, 01:52:23, GigabitEthernet0/0
C        10.2.2.0/30 is directly connected, GigabitEthernet0/0
L        10.2.2.2/32 is directly connected, GigabitEthernet0/0
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet1/0
L        192.168.10.254/32 is directly connected, GigabitEthernet1/0


R3(config)#interface gigabitEthernet 1/0
R3(config-if)#glbp1 ip 192.168.10.200
R2(config-if)#glbp 1 load-balancing round-robin
R3(config-if)#exit
R3(config)#do wr
Building configuration...
```

```
[OK]
R3(config)#exit
R3#show glbp
GigabitEthernet1/0 - Group 1
  State is Standby
    1 state change, last state change 00:04:52
  Virtual IP address is 192.168.10.200
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.440 secs
  Redirect time 600 sec, forwarder timeout 14400 sec
  Preemption disabled
  Active is 192.168.10.1, priority 150 (expires in 8.704 sec)
  Standby is local
  Priority 100 (default)
  Weighting 100 (default 100), thresholds: lower 1, upper 100
  Load balancing: round-robin
  Group members:
    ca03.0c5c.001c (192.168.10.1)
    ca04.182c.001c (192.168.10.254) local
  There are 2 forwarders (1 active)
  Forwarder 1
    State is Listen
    MAC address is 0007.b400.0101 (learnt)
    Owner ID is ca03.0c5c.001c
    Time to live: 14398.688 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 192.168.10.1 (primary), weighting 100 (expires in 10.304 sec)
  Forwarder 2
    State is Active
      1 state change, last state change 00:04:49
    MAC address is 0007.b400.0102 (default)
    Owner ID is ca04.182c.001c
    Preemption enabled, min delay 30 sec
    Active is local, weighting 100
```

CONFIGURACION DEL PROTOCOLO VRRP

CONFIGURACION DE ROUTER R1

```
R1>enable
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ip add 10.1.1.1 255.255.255.252
R1(config-if)#no sh
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
R1(config-if)#exit
R1(config)#interface gigabitEthernet 1/0
R1(config-if)#ip add 10.2.2.1 255.255.255.252
R1(config-if)#no sh

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up

R1(config-if)#exit
R1(config)#
R1(config)#do wr
Building configuration...
[OK]
R1(config)#interface loopback 1
R1(config-if)#ip add 109.165.200.225 255.255.255.224
R1(config-if)#exit

%LINK-5-CHANGED: Interface Loopback1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1,
changed state to up

R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 1
%Default route without gateway, if not a point-to-point interface, may
impact performance

R1(config)#router eigrp 10
R1(config-router)#network 10.1.1.0 0.0.0.3
R1(config-router)#network 10.2.2.0 0.0.0.3
R1(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 10.1.1.2
(GigabitEthernet0/0) is up: new adjacency
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 10.2.2.2
(GigabitEthernet0/1) is up: new adjacency
```


Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

```
R1(config-router)#redistribute static
R1(config-router)#exit
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*    0.0.0.0/0 is directly connected, Loopback1
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.1.1.0/30 is directly connected, GigabitEthernet0/0
L        10.1.1.1/32 is directly connected, GigabitEthernet0/0
C        10.2.2.0/30 is directly connected, GigabitEthernet1/0
L        10.2.2.1/32 is directly connected, GigabitEthernet1/0
      109.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        109.165.200.224/27 is directly connected, Loopback1
L        109.165.200.225/32 is directly connected, Loopback1
D     192.168.10.0/24 [90/3072] via 10.2.2.2, 00:03:27, GigabitEthernet1/0
                      [90/3072] via 10.1.1.2, 00:03:27, GigabitEthernet0/0
R1#


R1(config)#do wr
Building configuration...
[OK]
```

CONFIGURACION DE ROUTER R2

```
R2>enable
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#
R2(config)#interface gigabitEthernet 0/0
R2(config-if)#ip add 10.1.1.2 255.255.255.252
R2(config-if)#no sh
```

```
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up

R2(config-if)#exit

R2(config)#interface gigabitEthernet 1/0
R2(config-if)#ip add 192.168.10.1 255.255.255.0
R2(config-if)#no sh
R2(config-if)#exit
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up

R2(config)#do wr
Building configuration...
[OK]
R2(config)#router eigrp 10
R2(config-router)#network 10.1.1.0 0.0.0.3
R2(config-router)#network 192.168.10.0
R2(config-router)#exit
R2(config)#do wr
Building configuration...
[OK]
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.10.254
(GigabitEthernet0/1) is up: new adjacency

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up

%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 10.1.1.1
(GigabitEthernet0/0) is up: new adjacency

R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override
```


Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

```
Gateway of last resort is 10.1.1.1 to network 0.0.0.0

D*EX  0.0.0.0/0 [170/130816] via 10.1.1.1, 00:09:59, GigabitEthernet0/0
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.1.1.0/30 is directly connected, GigabitEthernet0/0
L        10.1.1.2/32 is directly connected, GigabitEthernet0/0
D        10.2.2.0/30
          [90/3072] via 192.168.10.254, 00:09:59, GigabitEthernet1/0
          [90/3072] via 10.1.1.1, 00:09:59, GigabitEthernet0/0
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet1/0
L        192.168.10.1/32 is directly connected, GigabitEthernet1/0
R2#


R2(config)#interface gigabitEthernet 1/0
R2(config-if)#vrrp 1 ip 192.168.10.200
R2(config-if)#
*Jan 18 23:44:08.287: %VRRP-6-STATECHANGE: Gi1/0 Grp 1 state Init -
> Backup
*Jan 18 23:44:08.307: %VRRP-6-STATECHANGE: Gi1/0 Grp 1 state Init -
> Backup
R2(config-if)#vrrp 1 priority 150
*Jan 18 23:44:25.947: %VRRP-6-STATECHANGE: Gi1/0 Grp 1 state
Backup -> Master
R2(config-if)#vrrp 1 preempt delay minimum 5
R2(config-if)#exit
R2(config)#
R2(config)#do wr
Building configuration...
R2#show vrrp
GigabitEthernet1/0 - Group 1
  State is Master
  Virtual IP address is 192.168.10.200
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 150
  Master Router is 192.168.10.1 (local), priority is 150
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.414 sec
```

CONFIGURACION ROUTER R3

```
R3>enable
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface gigabitEthernet 0/0
R3(config-if)#ip add 10.2.2.2 255.255.255.252
R3(config-if)#no sh
R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

R3(config-if)#exit
R3(config)#interface gigabitEthernet 1/0
R3(config-if)#ip add 192.168.10.254 255.255.255.0
R3(config-if)#no sh
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up

R3(config-if)#exit
R3(config)#
R3(config)#
R3(config)#do wr
Building configuration...
[OK]
R3(config)#router eigrp 10
R3(config-router)#network 10.2.2.0 0.0.0.3
R3(config-router)#network 192.168.10.0
R3(config-router)#exit
R3(config)#do wr
Building configuration...
[OK]
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.10.1
(GigabitEthernet0/1) is up: new adjacency

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up

%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 10.2.2.1
(GigabitEthernet0/0) is up: new adjacency
do
% Incomplete command.

R3#show ip route
```


Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.2.2.1 to network 0.0.0.0

D*EX  0.0.0.0/0 [170/130816] via 10.2.2.1, 01:52:18, GigabitEthernet0/0
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
D        10.1.1.0/30 [90/3072] via 192.168.10.1, 01:52:23,
GigabitEthernet1/0
                     [90/3072] via 10.2.2.1, 01:52:23, GigabitEthernet0/0
C        10.2.2.0/30 is directly connected, GigabitEthernet0/0
L        10.2.2.2/32 is directly connected, GigabitEthernet0/0
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet1/0
L        192.168.10.254/32 is directly connected, GigabitEthernet1/0


R3(config)#interface gigabitEthernet 1/0
R3(config-if)#vrrp 1 ip 192.168.10.200
R3(config-if)#exit
R3(config)#do wr
Building configuration...
[OK]
R3(config)#exit
R3#show vrrp
GigabitEthernet1/0 - Group 1
  State is Backup
  Virtual IP address is 192.168.10.200
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 100
  Master Router is 192.168.10.1, priority is 150
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.609 sec (expires in 2.793 sec)
```


Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Instrumentos de recolección de datos

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

UNIVERSIDAD SEÑOR DE SIPAN

FACULTAD DE INGENIERIA, ARQUITECTURA Y URBANISMO

ESCUELA ACADEMICO PROFESIONAL DE INGENIERIA DE SISTEMAS

FICHA DE EVALUACIÓN POR JUICIO DE EXPERTO

INVESTIGACION

IMPLEMENTACIÓN DE PROTOCOLOS DE COMUNICACIÓN PARA MEJORAR LA DISPONIBILIDAD DE UNA RED INFORMATICA

AUTORES:

- Cesar Juniors Córdova Rengifo

DATOS INFORMATIVOS DEL EXPERTO:

NOMBRE: Alex Franklin Coronado Navarro

TÍTULO UNIVERSITARIO:

Ingeniero de Sistemas

POSTGRADO:

Magister en Educación

OTRA FORMACIÓN:

CCNA Security

OCUPACIÓN ACTUAL:

Administrador de la red Informática de la Universidad Señor de Sipán

FECHA DE LA ENTREVISTA:

18 de Setiembre de 2015

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Mensaje al especialista:

En la Universidad Señor de Sipán, km.5 Carretera a Pimentel, se está realizando una investigación dirigida a la IMPLEMENTACIÓN DE PROTOCOLOS DE COMUNICACIÓN PARA MEJORAR LA DISPONIBILIDAD DE UNA RED INFORMATICA. Por tal motivo, se requiere de su reconocida experiencia, para corroborar que la propuesta de esta investigación genera los resultados establecidos en la hipótesis. Su información será estrictamente confidencial. Se agradece por el tiempo invertido.

1. En la tabla siguiente, se propone una escala del 1 al 5, que va en orden ascendente del desconocimiento al conocimiento profundo. Marque con una "X" conforme considere su conocimiento sobre el tema de la tesis evaluada.

1	2	3	4	5
Ninguno	Poco	Regular	Alto	Muy alto X

2. Sírvase marcar con una "X" las fuentes que considere han influenciado en su conocimiento sobre el tema, en un grado alto, medio o bajo.

FUENTES DE ARGUMENTACIÓN	GRADO DE INFLUENCIA DE CADA UNA DE LAS FUENTES EN SUS CRITERIOS		
	A (ALTO)	M (MEDIO)	B (BAJO)
a) Análisis teóricos realizados. (AT)	X		
b) Experiencia como profesional. (EP)	X		
c) Trabajos estudiados de autores nacionales. (AN)	X		
d) Trabajos estudiados de autores extranjeros. (AE)	X		
e) Conocimientos personales sobre el estado del problema de investigación. (CP)	X		

ALEX FRANKLIN CORONADO NAVARRO
INGENIERO DE SISTEMAS
Reg. CIP. 171209

Firma del entrevistado

Estimado(a) experto(a):

Con el objetivo de corroborar que la hipótesis de esta investigación es correcta, se le solicita realizar la evaluación siguiente:

1. ¿Considera adecuada y coherente la estructura de la propuesta?

   Adecuada X Poco adecuada___ Inadecuada ___

2. ¿Considera que cada parte de la propuesta se orienta hacia el logro del objetivo planteado en la investigación?

   Totalmente X Un poco ___ Nada ___

3. ¿En la investigación se han considerado todos los aspectos necesarios para resolver el problema planteado?

   Todos X Algunos ___ Pocos ___ Ninguno ___

4. ¿Considera que la propuesta generará los resultados establecidos en la hipótesis?

   Totalmente X Un poco ___ Ninguno ___

5. ¿Cómo calificaría cada parte de la propuesta?

N	Aspecto/Dimensión/ Estrategia	Excelente	Buena	Regular	Inadecuada
1	Analisis de los protocolos				
2					
3					
4					
5					

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

6. ¿Cómo calificaría a toda la propuesta?

Excelente X Buena ___ Regular ___ Inadecuada ___

7. ¿Qué sugerencias le haría a los autores de la investigación para lograr los objetivos trazados en la investigación?

Implementar la presente investigación

ALEX FRANKLIN CORONADO NAVARRO
INGENIERO DE SISTEMAS
Reg. CIP. 171209

Firma del entrevistado

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

UNIVERSIDAD SEÑOR DE SIPAN

FACULTAD DE INGENIERIA, ARQUITECTURA Y URBANISMO

ESCUELA ACADEMICO PROFESIONAL DE INGENIERIA DE SISTEMAS

FICHA DE EVALUACIÓN POR JUICIO DE EXPERTO

INVESTIGACION

IMPLEMENTACIÓN DE PROTOCOLOS DE COMUNICACIÓN PARA MEJORAR LA DISPONIBILIDAD DE UNA RED INFORMATICA

AUTOR:

- Cesar Juniors Córdova Rengifo

DATOS INFORMATIVOS DEL EXPERTO:

NOMBRE: Julio Cesar Altamirano Távara

TÍTULO UNIVERSITARIO:

Ingeniero de Sistemas

OTRA FORMACIÓN:

CCNA

OCUPACIÓN ACTUAL:

Jefe de infraestructura informática de la Universidad Señor de Sipán

FECHA DE LA ENTREVISTA:

18 de Setiembre de 2015

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Mensaje al especialista:

En la Universidad Señor de Sipán, km.5 Carretera a Pimentel, se está realizando una investigación dirigida a la IMPLEMENTACIÓN DE PROTOCOLOS DE COMUNICACIÓN PARA MEJORAR LA DISPONIBILIDAD DE UNA RED INFORMATICA. Por tal motivo, se requiere de su reconocida experiencia, para corroborar que la propuesta de esta investigación genera los resultados establecidos en la hipótesis. Su información será estrictamente confidencial. Se agradece por el tiempo invertido.

1. En la tabla siguiente, se propone una escala del 1 al 5, que va en orden ascendente del desconocimiento al conocimiento profundo. Marque con una "X" conforme considere su conocimiento sobre el tema de la tesis evaluada.

1 Ninguno	2 Poco	3 Regular	4 Alto	5 X Muy alto

2. Sírvase marcar con una "X" las fuentes que considere han influenciado en su conocimiento sobre el tema, en un grado alto, medio o bajo.

FUENTES DE ARGUMENTACIÓN	GRADO DE INFLUENCIA DE CADA UNA DE LAS FUENTES EN SUS CRITERIOS		
	A (ALTO)	M (MEDIO)	B (BAJO)
a) Análisis teóricos realizados. (AT)	X		
b) Experiencia como profesional. (EP)	X		
c) Trabajos estudiados de autores nacionales. (AN)	X	X	
d) Trabajos estudiados de autores extranjeros. (AE)	X		
e) Conocimientos personales sobre el estado del problema de investigación. (CP)	X		

Firma del entrevistado

Estimado(a) experto(a):

Con el objetivo de corroborar que la hipótesis de esta investigación es correcta, se le solicita realizar la evaluación siguiente:

1. ¿Considera adecuada y coherente la estructura de la propuesta?
   Adecuada X Poco adecuada___ Inadecuada ___

2. ¿Considera que cada parte de la propuesta se orienta hacia el logro del objetivo planteado en la investigación?
   Totalmente X Un poco ___ Nada ___

3. ¿En la investigación se han considerado todos los aspectos necesarios para resolver el problema planteado?
   Todos X Algunos ___ Pocos ___ Ninguno ___

4. ¿Considera que la propuesta generará los resultados establecidos en la hipótesis?
   Totalmente X Un poco ___ Ninguno ___

5. ¿Cómo calificaría cada parte de la propuesta?

N	Aspecto/Dimensión/ Estrategia	Excelente	Buena	Regular	Inadecuada
1	Análisis de los protocolos	X			
2					
3					
4					
5					

6. ¿Cómo calificaría a toda la propuesta?

Excelente X Buena ___ Regular ___ Inadecuada ___

7. ¿Qué sugerencias le haría a los autores de la investigación para lograr los objetivos trazados en la investigación?

Implementación del proyecto planteado.

Firma del entrevistado

UNIVERSIDAD SEÑOR DE SIPAN

FACULTAD DE INGENIERIA, ARQUITECTURA Y URBANISMO

ESCUELA ACADEMICA PROFESIONAL DE INGENIERIA DE SISTEMAS

FICHA DE VALIDACION DE INSTRUMENTO DE RECOLECCION DE DATOS

DATOS PERSONALES DEL EXPERTO

APELLIDOS: CORONADO NAVARRO

NOMBRES: ALEX FRANKLIN

PROFESION: INGENIERO DE SISTEMAS

GRAFO ACADEMICO: MAGISTER

ACTIVIDAD LABORAL: ADMINISTRADOR DE RED

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

INDICACIONES AL EXPERTO

1. En la tabla siguiente, se propone una escala del 1 al 5, que va en orden ascendente del desconocimiento al conocimiento profundo. Marque con una "X" conforme considere su conocimiento sobre el tema de la tesis evaluada.

1 Ninguno	2 Poco	3 Regular	4 Alto	5 Muy alto

2. Sírvase marcar con una "X" las fuentes que considere han influenciado en su conocimiento sobre el tema, en un grado alto, medio o bajo.

FUENTES DE ARGUMENTACIÓN	GRADO DE INFLUENCIA DE CADA UNA DE LAS FUENTES EN SUS CRITERIOS		
	A (ALTO)	M (MEDIO)	B (BAJO)
a) Análisis teóricos realizados. (AT)	X		
b) Experiencia como profesional. (EP)	X		
c) Trabajos estudiados de autores nacionales. (AN)	X		
d) Trabajos estudiados de autores extranjeros. (AE)	X		
e) Conocimientos personales sobre el estado del problema de investigación. (CP)	X		

ALEX FRANKLIN CORONADO NAVARRO
INGENIERO DE SISTEMAS
Reg. CIP. 171209

Firma del entrevistado

Anexo: Hoja de vida.

Estimado(a) experto(a):

El instrumento de recolección de datos a validar es un hoja de análisis cuyo objetivo es recolectar información sobre los protocolos de alta disponibilidad :

1. ¿Considera pertinente la aplicación de este instrumento?
   Es pertinente X Poco pertinente___ no es pertinente ___

2. ¿Considera que el instrumento formula las preguntas suficientes para conocer los protocolos de alta disponibilidad?
   Suficientes X insuficiente ___

3. ¿considera que la preguntas estén adecuadamente formuladas de manera tal que el entrevistado no tenga dudas en la elección y/o de redacción de sus respuestas?
   Son adecuadas X poca adecuadas ___ inadecuadas ___

4. ¿Cómo calificaría cada parte de la propuesta?

Nº pregunta	Precisión			relevancia	
	Muy precisa	Poco precisa	Muy relevante	Poco relevante	irrelevante
1	X				
2	X				
3	X				
4	X				
5	X				

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

5. ¿Qué sugerencias haría Ud. Para mejorar el instrumento de recolección de datos?

Ninguna.

ALEX FRANKLIN CORONADO NAVARRO
INGENIERO DE SISTEMAS
Reg. CIP. 171209

Firma del entrevistado

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe