



**UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA DE INGENIERÍA EN TELEINFORMÁTICA**

**TRABAJO DE TITULACIÓN
PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIERO EN TELEINFORMÁTICA**

**ÁREA
TECNOLOGÍA DE LOS ORDENADORES**

**TEMA
“DISEÑO DE UNA RED LAN BASADA EN PROTOCOLOS DE
REDUNDANCIA DE PUERTAS DE ENLACE PARA
INFRAESTRUCTURA DE DATOS DE LA EMPRESA
SANFERSYSTEMS S.A”**

**AUTOR
VALENCIA CARPIO VÍCTOR ANDRÉS**

**DIRECTORA DEL TRABAJO
ING. COMP. CASTILLO LEÓN ROSA ELIZABETH, MG**

GUAYAQUIL, ABRIL 2022



ANEXO XI.- FICHA DE REGISTRO DE TRABAJO DE TITULACIÓN

FACULTAD DE INGENIERÍA INDUSTRIAL CARRERA INGENIERÍA EN TELEINFORMÁTICA



REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA		
FICHA DE REGISTRO DE TRABAJO DE TITULACIÓN		
TÍTULO Y SUBTÍTULO:	DISEÑO DE UNA RED LAN BASADA EN PROTOCOLOS DE REDUNDANCIA DE PUERTAS DE ENLACE PARA INFRAESTRUCTURA DE DATOS DE LA EMPRESA SANFERSYSTEMS S.A	
AUTOR(ES) (apellidos/nombres):	VALENCIA CARPIO VÍCTOR ANDRÉS	
REVISOR(ES)/TUTOR(ES) (apellidos/nombres):	ING. ARAUZ ARROYO OSWALDO ORLANDO, MG /ING. CASTILLO LEÓN ROSA ELIZABETH, MG	
INSTITUCIÓN:	UNIVERSIDAD DE GUAYAQUIL	
UNIDAD/FACULTAD:	FACULTAD DE INGENIERÍA INDUSTRIAL	
MAESTRÍA/ESPECIALIDAD:		
GRADO OBTENIDO:	INGENIERO EN TELEINFORMÁTICA	
FECHA DE PUBLICACIÓN:	21 DE ABRIL DEL 2022	No. DE PÁGINAS: 91
ÁREAS TEMÁTICAS:	TECNOLOGÍA DE LOS ORDENADORES	
PALABRAS CLAVES/ KEYWORDS:	REDUNDANCIA, RED, PROTOCOLO, DISEÑO, INFRAESTRUCTURA, ENLACE / REDUNDANCY, NETWORK, PROTOCOL, DESIGN, INFRASTRUCTURE, LINK.	

RESUMEN/ABSTRACT (150-200 palabras):

RESUMEN

En la actualidad la demanda de las redes corporativas da paso a que se apliquen diseños de red cada vez más sofisticados en base a los requerimientos de las organizaciones. En consideración a la problemática de red en la empresa SANFERSYSTEMS S.A, que cuenta con arquitectura plana y que presenta deficiencia en su comunicación, se propone diseñar y simular un esquema basado en protocolos de redundancia de puerta de enlace a fin de determinar que protocolo es el más adecuado para despliegues que sean tolerante a fallas. Para ello se realiza un análisis comparativo entre los diferentes mecanismos basado en características de funcionamiento, en donde VRRP debido a ser de fácil implementación y adaptabilidad, además de un menor costo fue elegido el protocolo a emplearse para la empresa SANFERSYSTEMS.A., de igual forma se elige el software

de simulación GNS3 por ser de mayor rendimiento en cuanto a adaptabilidad en entornos emulados de red. Los resultados obtenidos al hacer uso del protocolo VRRP indican una mejora en cuanto a tiempo de recuperación en caso de incidentes o fallas hacia Internet. En el que se concluye que con el mecanismo de redundancia de puertas de enlace se logra obtener mejoras en rendimiento, delay y latencia.

Palabras clave: Redundancia, red, protocolo, diseño, infraestructura, enlace.

ABSTRACT

Nowadays, the demand of corporate networks gives way to the application of increasingly sophisticated network designs based on the requirements of organizations. In consideration of the network problems in the SANFERSYSTEMS S.A. company, which has a flat architecture and a deficiency in its communication, it is proposed to design and simulate a scheme based on gateway redundancy protocols to determine which protocol is the most appropriate for deployments that are fault tolerant. For this purpose, a comparative analysis is made between the different mechanisms based on performance characteristics, where VRRP was chosen as the protocol to be used for SANFERSYSTEMS.A. due to its easy implementation and adaptability, as well as its lower cost. Likewise, the simulation software GNS3 was chosen for its higher performance in terms of adaptability in emulated network environments. The results obtained by using the VRRP protocol indicate an improvement in terms of recovery time in case of incidents or failures to the Internet. In which it is concluded that with the gateway redundancy mechanism, improvements in performance, delay and latency are achieved.

Keywords: Redundancy, network, protocol, design, infrastructure, link.

ADJUNTO PDF:	SI (X)	NO
CONTACTO CON AUTOR/ES:	Teléfono: 0998082616	E-mail: victorvalenciavavc@gmail.com victor.valenciac@ug.edu.ec
CONTACTO CON LA INSTITUCIÓN:	Nombre: Ing. Ramón Maquilón Nicola	
	Teléfono: 593-2658128	
	E-mail: direccionTi@ug.edu.ec	



**ANEXO XII.- DECLARACIÓN DE AUTORÍA Y DE
AUTORIZACIÓN DE LICENCIA GRATUITA
INTRANSFERIBLE Y NO EXCLUSIVA PARA EL USO NO COMERCIAL DE LA OBRA
CON FINES NO ACADÉMICOS**

**FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA**

LICENCIA GRATUITA INTRANSFERIBLE Y NO COMERCIAL DE LA OBRA CON
FINES NO ACADÉMICOS

Yo, **VALENCIA CARPIO VÍCTOR ANDRÉS**, con C.C. No. **092335535-8**, certifico que los contenidos desarrollados en este trabajo de titulación, cuyo título es **“DISEÑO DE UNA RED LAN BASADA EN PROTOCOLOS DE REDUNDANCIA DE PUERTAS DE ENLACE PARA INFRAESTRUCTURA DE DATOS DE LA EMPRESA SANFERSYSTEMS S.A”** son de mi absoluta propiedad y responsabilidad, en conformidad al Artículo 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN*, autorizo la utilización de una licencia gratuita intransferible, para el uso no comercial de la presente obra a favor de la Universidad de Guayaquil.

Victor Valencia C.

VALENCIA CARPIO VÍCTOR ANDRÉS
C.C. No. 092335535-8



ANEXO VII.- CERTIFICADO PORCENTAJE DE SIMILITUD

FACULTAD DE INGENIERÍA INDUSTRIAL CARRERA INGENIERÍA EN TELEINFORMÁTICA



Habiendo sido nombrado ING. COMP. CASTILLO LEÓN ROSA ELIZABETH, MG, tutor del trabajo de titulación certifico que el presente trabajo de titulación ha sido elaborado por VALENCIA CARPIO VÍCTOR ANDRÉS, con mi respectiva supervisión como requerimiento parcial para la obtención del título de INGENIERO EN TELEINFORMÁTICA.

Se informa que el trabajo de titulación: “DISEÑO DE UNA RED LAN BASADA EN PROTOCOLOS DE REDUNDANCIA DE PUERTAS DE ENLACE PARA INFRAESTRUCTURA DE DATOS DE LA EMPRESA SANFERSYSTEMS S.A.”, ha sido orientado durante todo el periodo de ejecución en el programa Antiplagio URKUND quedando el 0% de coincidencia.

The screenshot shows the URKUND interface with the following details:

- Document:** Valencia Carpio Victor Andres.docx (D129682778)
- Submitted:** 2022-03-07 13:38 (-05:00)
- Submitted by:** victor.valenciad@ug.edu.ec
- Receiver:** rosa.castillo@ug@analysis.orkund.com
- Message:** Tesis Victor Andres Valencia Carpio [Show full message](#)
- Similarity:** 0% of this approx. 25 pages long document consists of text present in 0 sources.
- Navigation:** Sources, Highlights, Login
- Table:**

Rank	Path/Filename
Alternative sources	
Sources not used	
- TEMA:** "DISEÑO DE UNA RED LAN BASADA EN PROTOCOLOS DE REDUNDANCIA DE PUERTAS DE ENLACE PARA INFRAESTRUCTURA DE DATOS DE LA EMPRESA SANFERSYSTEMS S.A."
- AUTOR:** VALENCIA CARPIO VICTOR ANDRÉS
- Introducción:** (text partially visible)

<https://secure.orkund.com/view/123746751-875616-750802>



Firmado electrónicamente por:
**ROSA
ELIZABETH
CASTILLO LEON**

ING. COMP. CASTILLO LEÓN ROSA ELIZABETH, MG.
DOCENTE TUTOR
C.C.: 0922372610
FECHA: 14 DE MARZO DE 2022



**ANEXO VI. - CERTIFICADO DEL DOCENTE-TUTOR DEL
TRABAJO DE TITULACIÓN
FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA**



Guayaquil, 14 de marzo del 2022,

Sra.

Ing. Annabelle Lizarzaburu Mora, MG.

Directora de Carrera Ingeniería en Teleinformática / Telemática

FACULTAD DE INGENIERÍA INDUSTRIAL DE LA UNIVERSIDAD DE GUAYAQUIL

Ciudad. -

De mis consideraciones:

Envío a Ud. el Informe correspondiente a la tutoría realizada al Trabajo de Titulación “DISEÑO DE UNA RED LAN BASADA EN PROTOCOLOS DE REDUNDANCIA DE PUERTAS DE ENLACE PARA INFRAESTRUCTURA DE DATOS DE LA EMPRESA SANFERSYSTEMS S.A.” del estudiante VALENCIA CARPIO VÍCTOR ANDRÉS indicando que ha cumplido con todos los parámetros establecidos en la normativa vigente:

- El trabajo es el resultado de una investigación.
- El estudiante demuestra conocimiento profesional integral.
- El trabajo presenta una propuesta en el área de conocimiento.
- El nivel de argumentación es coherente con el campo de conocimiento.

Adicionalmente, se adjunta el certificado de porcentaje de similitud y la valoración del trabajo de titulación con la respectiva calificación.

Dando por concluida esta tutoría de trabajo de titulación, **CERTIFICO**, para los fines pertinentes, que el estudiante está apto para continuar con el proceso de revisión final.

Atentamente,

 Fijado electrónicamente por:
**ROSA
ELIZABETH
CASTILLO LEON**

ING. COMP. CASTILLO LEÓN ROSA ELIZABETH, MG.

DOCENTE TUTOR

C.C.: 0922372610

FECHA: 14 DE MARZO DE 2022



**ANEXO VIII.- INFORME DEL DOCENTE REVISOR
FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA**



Guayaquil, 5 de abril del 2022

Sra.

Ing. Annabelle Lizarzaburu Mora, MG.

Director (a) de Carrera Ingeniería en Teleinformática / Telemática

FACULTAD DE INGENIERÍA INDUSTRIAL DE LA UNIVERSIDAD DE GUAYAQUIL

Ciudad. -

De mis consideraciones:

Envío a Ud. el informe correspondiente a la REVISIÓN FINAL del Trabajo de Titulación **“DISEÑO DE UNA RED LAN BASADA EN PROTOCOLOS DE REDUNDANCIA DE PUERTAS DE ENLACE PARA INFRAESTRUCTURA DE DATOS DE LA EMPRESA SANFERSYSTEMS S.A”** del estudiante **VALENCIA CARPIO VÍCTOR ANDRÉS**. Las gestiones realizadas me permiten indicar que el trabajo fue revisado considerando todos los parámetros establecidos en las normativas vigentes, en el cumplimiento de los siguientes aspectos:

Cumplimiento de requisitos de forma:

El título tiene un máximo de 23 palabras.

La memoria escrita se ajusta a la estructura establecida.

El documento se ajusta a las normas de escritura científica seleccionadas por la Facultad.

La investigación es pertinente con la línea y sublíneas de investigación de la carrera.

Los soportes teóricos son de máximo 5 años.

La propuesta presentada es pertinente.

Cumplimiento con el Reglamento de Régimen Académico:

El trabajo es el resultado de una investigación.

El estudiante demuestra conocimiento profesional integral.

El trabajo presenta una propuesta en el área de conocimiento.

El nivel de argumentación es coherente con el campo de conocimiento.

Adicionalmente, se indica que fue revisado, el certificado de porcentaje de similitud, la valoración del tutor, así como de las páginas preliminares solicitadas, lo cual indica el que el trabajo de investigación cumple con los requisitos exigidos.

Una vez concluida esta revisión, considero que el estudiante está apto para continuar el proceso de titulación. Particular que comunicamos a usted para los fines pertinentes.

Atentamente,



Firmado electrónicamente por:
**OSWALDO ORLANDO
ARAUZ ARROYO**

ING. ARAUZ ARROYO OSWALDO ORLANDO, MG.

C.C:001964749

FECHA: 05/04/2022

Dedicatoria

Dedico este proyecto de titulación primero a Dios por darme la fuerza, salud y sobre todo paciencia para culminar una de las más grandes, importante y demorada meta planteada en mi vida.

También dedico este logro a mi tiempo y a mi vida.

Una especial dedicatoria a mis dos madres Sra. Flérída Carpio y Sra. Shirley Carpio, a mi padre Julio Cesar Valencia.

Por ultimo y no menos importante dedico este logro a mi Kiki que me trasmitió toda su fuerza de voluntad para siempre seguir adelante.

Agradecimiento

Un particular agradecimiento a las siguientes personas:

Mis compañeros que se han vuelto mis colegas

A los docentes de la facultad que impartieron sus conocimientos conmigo, en especial a mi tutor, Ing. Castillo León Rosa Elizabeth y mi revisor Ing. Arauz Arroyo Oswaldo Orlando por su guía y paciencia para poder culminar este proyecto de titulación.

A Mi.

Declaración de autoría

“La responsabilidad del contenido de este Trabajo de Titulación, me corresponde exclusivamente; y el patrimonio Intelectual del mismo a la Facultad de Ingeniería Industrial de la Universidad de Guayaquil”

Valencia Carpio Víctor Andrés
C.C. 0923355358

Índice General

N°	Descripción	Pág.
	Introducción	1

Capítulo I

El Problema

N°	Descripción	Pág.
1.1	Formulación del problema	3
1.2	Sistematización del problema	3
1.3	Justificación e importancia	3
1.4	Objetivos de la investigación	4
1.4.1	Objetivo General	4
1.4.2	Objetivos específicos	4
1.5	Alcance	4
1.6	Delimitación del problema	4

Capítulo II

Marco Teórico

N°	Descripción	Pág.
2.1	Antecedentes de la Investigación	5
2.2	Fundamentación teórica	6
2.2.1	Protocolo de red	6
2.2.2	Sistema Autónomo (AS)	7
2.2.3	Enrutamiento	7
2.2.4	Protocolos de enrutamiento	7
2.2.5	Protocolo de enrutamiento	8
2.2.6	Enrutamiento Dinámico	9
2.2.7	Internal Gateway Protocol	11
2.2.8	Exterior Gateway Protocol	14
2.2.9	Distancia administrativa	15
2.2.10	Métricas de red	16
2.2.11	Protocolos de redundancia de Gateway	18

2.2.12	Protocolo VRRP (Virtual Router Redundancy Protocol)	22
2.2.13	Simulador GNS3	26
2.2.14	Wireshark	27
2.3	Marco conceptual	28
2.3.1	Red LAN	28
2.3.2	Red Wan	28
2.3.3	Router	28
2.3.4	Switch	28
2.3.5	Access Point	28
2.3.6	Round Robin	28
2.3.7	Load-Balancing	29
2.3.8	IP Hash	29
2.3.9	MAC	29
2.3.10	IP	29
2.4	Marco contextual	29
2.5	Marco legal	30

Capítulo III

Diseño de investigación

Nº	Descripción	Pág.
3.1	Metodología Bibliográfica	32
3.2	Deductiva	32
3.3	Exploratoria	32
3.4	Explicativa	32
3.5	Técnicas de recopilación de datos	32
3.5.1	La entrevista	33
3.5.2	Formato de preguntas para entrevista a especialista en conectividad de la empresa SANFERSYSTEMS S.A.	33
3.6	Elementos utilizados para el diseño de la propuesta	36
3.6.1	Comparativa de protocolos de redundancia de puerta en enlace	36
3.7	Compatibilidad de simuladores de red	37

3.8	Compatibilidad de simulador GNS3 con S.O.	38
3.9	Requisitos mínimos para uso de GNS3	39
3.10	Diseño de red actual SANFERSYSTEMS S.A.	39
3.11	Diseño propuesto	41
3.12	Esquema de red realizado en GNS3	42
3.13	Configuración de IPs en equipos finales	47
3.14	Configuración del switch core	48
3.15	Configuración de routers para redundancia de gateway	52
3.16	Configuración de VRRP en Routers para redundancia de Gateway	52
3.17	Evaluación del entorno simulado	56
3.18	Análisis de tráfico mediante Wireshark	59
3.19	Protocolo VRRP capturado en Wireshark	60
3.20	Protocolo ICMP capturado en Wireshark	61
3.21	Gráficas de flujo	62
3.22	Direcciones resueltas	63
3.23	Gráficas de entrada y salida de datos en Wireshark	64
3.24	Conclusiones	64
3.25	Recomendaciones	65
	Anexos	66
	Bibliografía	69

Índice de Tablas

Nº	Descripción	Pág.
1.	Comparativa de protocolos de redundancia de gateway	36
2.	¿Simuladores de red para entornos virtuales	38
3.	Compatibilidad de simulador en Sistemas Operativos	38
4.	Requerimientos mínimos para simulador de red GNS3	39

Índice de Figuras

Nº	Descripción	Pág.
1.	Ejemplo de un protocolo de red	6
2.	Sistema Autónomo (AS)	7
3.	Protocolo de enrutamiento	8
4.	Protocolo de enrutamiento estático	9
5.	Protocolo de enrutamiento dinámico	10
6.	Protocolos de vector distancia	12
7.	Protocolos de vector distancia	13
8.	Exterior Gateway Protocol	14
9.	Exterior Gateway Protocol	15
10.	Costos EIGRP	16
11.	Métricas de Red	17
12.	Métricas de Red	17
13.	Protocolo HSRP	19
14.	Roles HSRP	20
15.	Estados HSRP	21
16.	Protocolo VRRP	22
17.	Atributo VRRP	23
18.	Roles GLBP	24
19.	Características de GLBP	25
20.	Interfaz gráfica GNS3	26
21.	Interfaz Wireshark	27
22.	Topología Propuesta	40
23.	Funcionamiento de la red	42
24.	Asignación de IP	43
25.	Adaptador de red virtual	43
26.	CMD	44
27.	Ejecutable GNS3	44
28.	Creación del proyecto	45

29.	Escenario de pruebas	45
30.	Topología Base	46
31.	Funcionamiento de Equipos	47
32.	Configuración de IPs	47
33.	Creación de Vlans	48
34.	Validación de Vlans	48
35.	Asignación de puertos	49
36.	Visualización de puertos	49
37.	Configuración de SVI	50
38.	Direcciones IP	50
39.	Comando ip routing	50
40.	Conectividad	51
41.	Pruebas en el servidor	51
42.	Configuración de equipos	51
43.	Configuración Gateway	51
44.	Configuración de router	52
45.	Router master	53
46.	VRRP	53
47.	Comando show VRRP	53
48.	Configuración router backup	54
49.	Modo backup por el protocolo VRRP	54
50.	Validación de configuración	54
51.	Resumen de configuración	54
52.	Rutas de retorno	55
53.	Problemas de paquetes	55
54.	Activación de rutas	55
55.	Activación de rutas en router BK	55
56.	Trace a IP Virtual	56
57.	Ping al servidor	56
58.	Ping del lado del equipo 5.101	56

59.	Equipo Master	57
60.	Caida de paquetes	57
61.	Análisis de tráfico	59
62.	Puertas de enlace	60
63.	Campos del protocolo VRRP	61
64.	Protocolo ICMP capturado en Wireshark	62
65.	Gráfico de flujo	62
66.	Identificación de equipos	63
67.	Direcciones resueltas	63
68.	Gráficas de entrada y salida de datos en Wireshark	64

Índice de Anexos

Nº	Descripción	Pág.
1.	GNS3 instalado en VMWARE	67
2.	GNS3 funcionando	68



ANEXO XIII.- RESUMEN DEL TRABAJO DE TITULACION (ESPAÑOL)



FACULTAD DE INGENIERÍA INDUSTRIAL CARRERA INGENIERÍA EN TELEINFORMÁTICA

“DISEÑO DE UNA RED LAN BASADA EN PROTOCOLOS DE REDUNDANCIA DE
PUERTAS DE ENLACE PARA INFRAESTRUCTURA DE DATOS DE LA EMPRESA
SANFERSYSTEMS S.A”

Autor: Valencia Carpio Víctor Andrés

Tutor: Ing. Castillo León Rosa Elizabeth, Mg.

Resumen

En la actualidad la demanda de las redes corporativas da paso a que se apliquen diseños de red cada vez más sofisticados en base a los requerimientos de las organizaciones. En consideración a la problemática de red en la empresa SANFERSYSTEMS S.A, que cuenta con arquitectura plana y que presenta deficiencia en su comunicación, se propone diseñar y simular un esquema basado en protocolos de redundancia de puerta de enlace a fin de determinar que protocolo es el más adecuado para despliegues que sean tolerante a fallas. Para ello se realiza un análisis comparativo entre los diferentes mecanismos basado en características de funcionamiento, en donde VRRP debido a ser de fácil implementación y adaptabilidad, además de un menor costo fue elegido el protocolo a emplearse para la empresa SANFERSYSTEMS.A., de igual forma se elige el software de simulación GNS3 por ser de mayor rendimiento en cuanto a adaptabilidad en entornos emulados de red. Los resultados obtenidos al hacer uso del protocolo VRRP indican una mejora en cuanto a tiempo de recuperación en caso de incidentes o fallas hacia Internet. En el que se concluye que con el mecanismo de redundancia de puertas de enlace se logra obtener mejoras en rendimiento, delay e latencia.

Palabras Claves: Redundancia, red, protocolo, diseño, infraestructura, enlace.



ANEXO XIV.- RESUMEN DEL TRABAJO DE TITULACIÓN (INGLÉS)

FACULTAD DE INGENIERÍA INDUSTRIAL CARRERA INGENIERÍA EN TELEINFORMÁTICA



“DESIGN OF A LAN NETWORK BASED ON GATEWAY REDUNDANCY PROTOCOLS FOR DATA INFRASTRUCTURE OF THE COMPANY SANFERSYSTEMS S.A”

Author: Valencia Carpio Víctor Andrés

Advisor: Ing. Castillo León Rosa Elizabeth, MG.

Abstract

Nowadays, the demand of corporate networks gives way to the application of increasingly sophisticated network designs based on the requirements of organizations. In consideration of the network problems in the SANFERSYSTEMS S.A. company, which has a flat architecture and a deficiency in its communication, it is proposed to design and simulate a scheme based on gateway redundancy protocols to determine which protocol is the most appropriate for deployments that are fault tolerant. For this purpose, a comparative analysis is made between the different mechanisms based on performance characteristics, where VRRP was chosen as the protocol to be used for SANFERSYSTEMS.A. due to its easy implementation and adaptability, as well as its lower cost. Likewise, the simulation software GNS3 was chosen for its higher performance in terms of adaptability in emulated network environments. The results obtained by using the VRRP protocol indicate an improvement in terms of recovery time in case of incidents or failures to the Internet. In which it is concluded that with the gateway redundancy mechanism, improvements in performance, delay and latency are achieved.

Keywords: Redundancy, network, protocol, design, infrastructure, link.

Introducción

Hoy en día los entornos corporativos adquieren recursos que le permitan trabajar de forma más efectiva a la hora de procesar información a través de Internet, siendo este último el principal medio adquirido con el fin de no perder disponibilidad en la transmisión y recepción de datos externos.

Estos servicios por lo general son solicitados a los ISP o Carrier que en muchas ocasiones para facilidad brinda un mismo enlace de gestión. Muchas veces la falta de conocimiento o mala configuración de los sistemas de redundancia impiden que los servicios operen de forma correcta en el intercambio de información.

Estudios recientes por lo general indican que las empresas tienen mayor tiempo de operabilidad durante el día por lo que las redes deben estar operativas hacia Internet en todo momento.

Del mismo modo existen diferentes técnicas para permitir redundancia en puertas de enlace que son otorgadas o configuradas por los diferentes ISPs o administradores de la red, donde acorde a ciertos parámetros o métricas como delay, jitter, entre otros permiten definir cuál esquema y protocolo adecuado en escenarios de redundancia que garantiza disponibilidad a los problemas actuales que puede contar la entidad.

Por lo que en base a lo expuesto se pretende definir que protocolo puede trabajar en la empresa SANFERSYSTEMS S.A y obtener con ello mejoras en cuanto a enrutamiento y comunicación hacia Internet brindando excelencia en tiempos de respuesta y redundancia de enlaces.

Capítulo I

El Problema

Hoy en día las empresas constantemente buscan tener mejoras en cuanto a diseño o funcionalidades aplicados a nivel de redes LAN con el fin de optimizar los parámetros de QoS (Calidad de servicio) a nivel de capas inferiores como son la capa física y enlace de datos permitiendo así la mejora e incluso el aumento en los procesos de transmisión y recepción de información reduciendo drásticamente el delay, jitter o latencia que hacen que los servicios se vean afectados.

Debido a esto gran parte de las organizaciones se enfocan a tener una estructura confiable y que tenga tolerancia a falla en los modelos de dos capas constantemente aplicados en las organizaciones a nivel de pymes o LAN de campus, pero omiten los problemas de enrutamiento a nivel de equipamiento activo que permite la conexión hacia los servicios o URLs que existen en los que se conoce como Internet.

Este tipo de afectaciones produce que las empresas tengan problemas en cuanto a enrutamiento llegando muchas veces a no encontrar rutas hacia los servidores anunciados en Internet debido a fallas del equipo físico como hardware o problemas de software lo que produce pérdida en tiempo y dinero en las organizaciones.

Otro factor a tener en cuenta es que en muchas ocasiones por lo general las empresas optan por adquirir un segundo proveedor de servicio con el fin de solventar el problema de las caídas de red lo que podría ser una solución temporal, pero si no se tiene el correcto funcionamiento, donde además en muchas ocasiones la configuración demanda tiempo en cuestiones de reglas de firewall e incluso ajustes manuales a nivel de dominio o Neteo retrasando a la organización ya que siempre se debe de hacer los debidos cambios de forma manual cuando se requiera una puerta de enlace distinta a la previamente establecida. En las organizaciones donde el tiempo de caída en la red debe ser mínimo este tipo de práctica no es el más idóneo ya que no es transparente en cuanto a configuraciones provocando contrariedades en ajustes.

Actualmente la empresa SANFERSYSTEMS S.A cuenta con una red conformada con diferentes direccionamientos (Gateway), equipados para satisfacer la necesidad de los usuarios finales en el que por lo general los servicios deben ser constantes, pero al ser la red plana tiene

diferentes problemas a nivel de diseño además de problemas de reconfiguración en los enlaces lo que produce fallas a nivel de configuración donde para ello el encargado de sistemas debe realizar procesos manuales en cuanto a cambio de IP o direccionamiento en los switches de borde para obtener salida a Internet por un enlace secundario esto en la mayoría de las veces emana una cantidad de tiempo considerable para la operabilidad de los servicios que la empresa posee o necesita acceder.

1.1 Formulación del problema

Ante lo expuesto se pretende responder a la siguiente pregunta de investigación ¿Se puede diseñar una red LAN basada en protocolos de puerta de redundancia de enlace que permita mejoras de comunicación y tiempos cortos de respuesta hacia Internet?

1.2 Sistematización del problema

- ¿Cuál es el diseño actual de red que maneja la empresa SANFERSYSTEMS S.A.?
- ¿De qué manera se puede aplicar protocolos de redundancia de puerta de enlace en la red de datos que actualmente manejan?
- ¿Qué protocolo de puerta de enlace es el más idóneo para el diseño de red de la empresa SANFERSYSTEMS S.A.?
- ¿Cuáles son las consideraciones a tener en cuenta al momento de aplicar protocolos de redundancia de puertas de enlace?

1.3 Justificación e importancia

Actualmente las redes deben por lo general estar 100% operativas a la hora de requerir acceder a un recurso de la Extranet donde por lo general se busca que existan funciones que eviten fallos a nivel de servicios.

Para ello el nivel de interoperabilidad de los modelos de 2 capas debe ser más escalable a tal punto de poder tener una red funcional en cuanto a operaciones de servicios donde la redundancia es una de las técnicas que los administradores de infraestructura buscan obtener permitiendo así un diseño de red dinámico y escalable. Por lo que se busca analizar los diferentes protocolos de puerta de enlace que permitan reducir al mínimo las interrupciones de

los servicios así como la incorporación y optimización de rendimiento a nivel de un modelo colapsado permitiendo una mayor disponibilidad en cuanto a la red así como reducir los tiempos de configuración manuales evitando fallas a nivel de configuración de usuario planteando un diseño de una red LAN que permita contar con diferentes configuraciones a nivel de capa 2 y 3 con el fin de garantizar la confiabilidad e integridad de los datos y así evitar que los servicios en la empresa SANFERSYSTEMS sean ininterrumpidos.

1.4 Objetivos de la investigación

1.4.1 Objetivo General

Simular un diseño de red basado en protocolos de redundancia de puerta de enlace para la empresa SANFERSYSTEMS S.A

1.4.2 Objetivos específicos

- Identificar las diferentes tecnologías de redundancia de puertas de enlace (Gateway)
- Determinar los diferentes protocolos de puerta de enlace en base a métricas de rendimiento
- Diseñar una red basada en redundancia de puerta de enlace para la empresa SANFERSYSTEMS S.A.
- Evaluar el entorno de red simulado que muestre su desempeño en cuanto a mejoras de comunicación para la empresa SANFERSYSTEMS S.A.

1.5 Alcance

Diseñar una topología para la empresa SANFERSYSTEMS S.A. que cuente con redundancia de puerta de enlace a nivel de redes LAN consiguiendo una red escalable y tolerante a falla mejorando la comunicación a nivel de capas superiores

1.6 Delimitación del problema

El trabajo actual se encuentra delimitado en el área de las tecnologías de los ordenadores, en el que se diseña un modelo de red simulado basado en protocolos de redundancia de puertas de enlace con el fin de mejorar la infraestructura de datos actual de la empresa SANFERSYSTEMS S.A.

Capítulo II

Marco Teórico

2.1 Antecedentes de la Investigación

Hoy en día, gran parte de las organizaciones no tienen un control en cuanto al diseño o envío de tráfico hacia Internet muchas veces debido al tipo de infraestructura con la que cuentan e incluso el poco conocimiento por parte del personal encargado de la organización ocasionando que ciertos procesos se hagan mucho más lento existiendo problemas en cuanto a los servicios.

Asimismo, otro problema existente esta dado a los cambios que se producen en cuanto a fallas donde al no tener una correcta configuración pueden pasar horas para la corrección de la red. Cabe mencionar que gran parte de los procesos pueden llegar a ser optimizados logrando así la comunicación desde la capa inferior a la superior del modelo OSI teniendo como prioridad el jitter, delay o el throughput a nivel de calidad de servicio (QoS).

Por lo que, en la actualidad existen diferentes tecnologías que permiten reducir los problemas de red como jitter, latencia a través de técnicas como vlans, protocolos de árbol de expansión e incluso redundancia en la red LAN, donde Miranda (2012) en su trabajo de investigación realiza un análisis de los diversos protocolos de enrutamiento de redundancia de puertas de enlace con el fin de mostrar la disponibilidad en las redes LAN además de la eficiencia en cuanto a la mínima pérdida de paquetes que existe a la hora de realizar un diseño con alta disponibilidad para una infraestructura de red.

Del mismo modo, Espinoza (2018), en su tema de investigación indico de qué manera se puede establecer una comunicación efectiva con la capa de red haciendo uso de un esquema de redundante y tolerable a fallos aplicando procesos relacionados al load-balancing y a su vez la reducción de puntos críticos que comúnmente afectan a una red de datos.

Un punto para destacar es que en muchas ocasiones se desconoce el funcionamiento en la red de campus y con ello la interoperabilidad de los protocolos de puerta de enlace a la hora de ser implementados por lo que, Rocío (2010) en su estudio de investigación presenta un análisis que permita demostrar la alta disponibilidad a nivel de red Lan/Wan en redes de campus mediante tecnología Cisco adicional a la forma de cómo pueden ser implementados.

Los protocolos de redundancia no solo ayudan en la comunicación a nivel de red Wan sino también en redes LAN debido a que permite proporcionar una comunicación continua sin ver afectada la disponibilidad de una organización, además, de tener una percepción en cuanto a fallas y mediante su forma de operación permitir una comunicación constante hacia la red LAN a Internet y viceversa, (Jimenez, 2012).

A la hora de trabajar con protocolos de alta disponibilidad es recomendable tener una infraestructura de red segmentada con el fin de evitar pasar tráfico ajeno a la comunicación de Gateway permitiendo así que alguien de la red de usuarios capture el tráfico mediante un ataque de hombre en el medio (Man in the middle).

2.2 Fundamentación teórica

2.2.1 Protocolo de red

Se conoce como protocolo de red aquel conjunto de reglas o procedimientos utilizados para establecer una comunicación entre diferentes estaciones que se encuentran en una red de datos previamente configurada. Existe una gran cantidad de estos protocolos unos que otros con funcionalidades un poco diferentes los cuales por lo general tratan de establecer una comunicación entre sus diferentes capas y así realizar una comunicación sin problema, (Riffo, 2009),

2.2.1.1 Ventajas de los protocolos de red

- Interoperabilidad entre diferentes fabricantes
- Comunicación en medios heterogéneos
- Comunicación entre diferentes sistemas operativos en red
- Estándar para todos los equipos de red

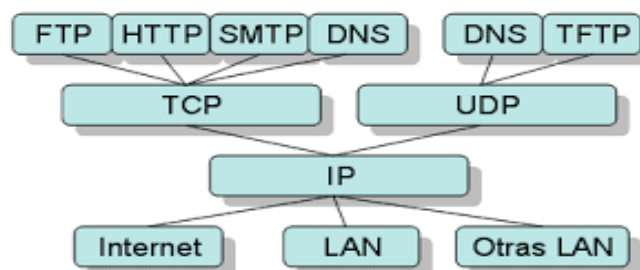


Figura 1. Ejemplo de un protocolo de red. Información tomada de <https://sites.google.com>. Elaborado por el autor

2.2.2 Sistema Autónomo (AS)

Los sistemas autónomos (AS) son un conjunto de IP que pertenecen a una política de ruteo que es definida por una entidad u organización, permitiendo que toda red que este dentro del AS pueda comunicarse.

Por lo general cada entidad cuenta con un ASN diferente es decir mantienen políticas de ruteo diferentes a otros donde de querer comunicarse con alguna otra entidad no será posible a menos que se utilicen protocolos de enrutamiento avanzado como BGP (Border Gateway Protocol), (Altamirano & Álvarez, 2016).

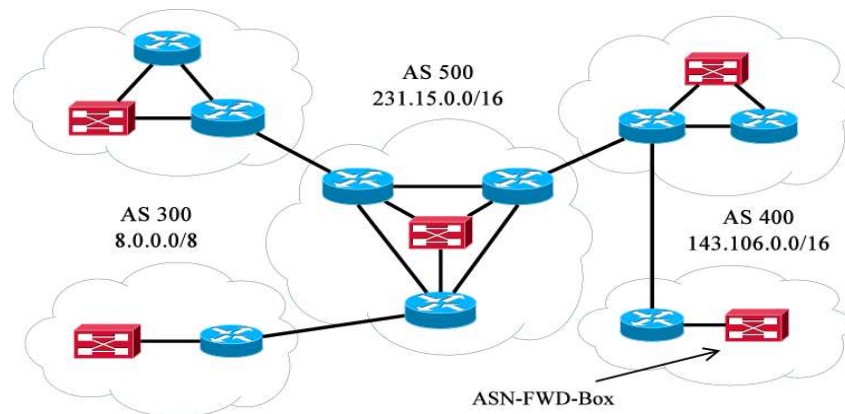


Figura 2. Sistema Autónomo (AS). Información tomada de <https://sites.google.com>. Elaborado por el autor

2.2.3 Enrutamiento

Se refiere al proceso que los routers elijen a través de diferentes rutas escogiendo aquella que mejor cumpla con los parámetros planteados en el que una vez definida permitirá enviar el tráfico que circula a través del equipo, en la actualidad existen diferentes protocolos o técnicas que permiten realizar el proceso mencionado tal como se menciona a continuación, (Barbecho, 2016).

2.2.4 Protocolos de enrutamiento

Rutas configuradas de forma manual o dinámica que permiten hacer que dispositivos de segmentos o lugares lejanos puedan comunicarse a través de un medio ya sea guiado o no guiado para ello es necesario un equipo que sea capaz de procesar la información y que interactúe con los demás sistemas autónomos en Internet o internos.

Un protocolo de enrutamiento este compuesto de varias características destacando entre ellas su forma en la que anuncia sus redes a los vecinos, así como las distancias administrativas que entre más baja mayor confiabilidad le da a la red. Así mismo los protocolos de routing se dividen en dos grandes grupos los cuales según el lugar de operación tienen mejoras uno de otro teniendo así:

- Protocolo de enrutamiento estático
- Protocolo de enrutamiento dinámico



Figura 3. Protocolo de enrutamiento. Información tomada de <https://sites.google.com>. Elaborado por el autor

2.2.5 Protocolo de enrutamiento

Un protocolo de enrutamiento estático son rutas definidas de forma manual por el administrador del sistema donde el mediante un esquema de red deberá enviar los datos a través del vecino o router de siguiente salto. Para ello previamente deberá definir la ruta en el equipo que desea enviar los datos algo a considerar del presente esquema es que en cada uno de los routers se debe crear las rutas respectivas haciendo una comunicación bidireccional caso contrario será imposible establecer el envío de datos entre los dispositivos, (Luje & Mosquera, 2011).

El enrutamiento estático es el primer protocolo de enrutamiento definido en las redes pero debido a que es un proceso manual pueden existir errores así como una alta demanda de tiempo en la configuración de los dispositivos por lo que no es aconsejable manejarlo en entornos donde existen muchos routers debido a su complejidad en cuanto a crecimiento se refiere.

2.2.5.1 Ventajas del protocolo de enrutamiento estático

- Redundante donde para ello si se realiza el proceso manual la red podrá operar sin ningún problema

- Confiable debido a que nadie más conoce la forma en como está elaborada la red aparte del administrador del sistema
- Segura debido a que al no ser dinámico se evita que exista actualizaciones evitando que un usuario no autorizado obtenga información en caso de realizar algún sniffer.

2.2.5.2 Desventaja del enrutamiento estático

- No es escalable donde de existir una ruta nueva a crear esta debe ser anunciada en cada uno de los routers o equipos por donde el tráfico atraviesa para llegar al destino.
- No es tolerante a fallas debido a que si se daña un enlace esta debe ser cambiada de forma manual siendo un proceso que consume demasiado tiempo.

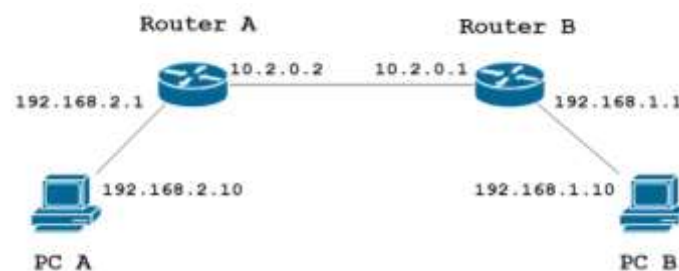


Figura 4. Protocolo de enrutamiento estático. Información tomada de <https://sites.google.com>.
Elaborado por el autor

2.2.6 Enrutamiento Dinámico

Se conoce como enrutamiento dinámico al proceso que uno o varios routers realizan para el reenvío de datos de una red a otra utilizando mecanismos avanzados de comunicación, todos estos procesos realizados permiten establecer caminos que sean óptimos donde mediante un esquema de ruta permitirá llegar a uno o varios destinos como tal.

Al hablar de enrutamiento dinámico se hace referencia a los datos que son asociados a la capa de red y que mediante un medio son retransmitidos de un extremo a otro, teniendo en cuenta el camino o método más rápido y que esté disponible. A diferencia del enrutamiento estático este tipo de enrutamiento es más fácil de administrar además de poder tener un envío y recepción de datos permitiendo mejoras en cuando a las actualizaciones de red de haber una o varias fallas en la red, (Espinosa & Moncayo, 2010).

Un factor muy importante del enrutamiento dinámico es la tolerancia a fallas que existe permitiendo tener un rápido cambio de topología buscando caminos alternos que tengan una

disponibilidad hacia equipos internos de una organización e incluso Internet, este proceso se conoce como tiempo de convergencia y siempre se da cuando ocurre cambios en las topologías.

Del mismo modo, otra característica importante por considerar es que este tipo de enrutamiento facilita al administrador de la red tener un proceso de implementación mucho más sencillo debido a la escalabilidad que poseen es decir permiten dar un crecimiento a la red donde con poca configuración es posible hacer que funcione.

- Los protocolos de enrutamiento dinámico son utilizados en varios escenarios de despliegue teniendo entre ellos:
- Las redes que cuentan con más de 2 routers es decir organizaciones o entidades
- En sitios donde existen cambios constantes en cuanto a rutas o enlaces que dinámicamente puedan ser organizados
- Esquemas de red que tengan proyección a crecimiento evitando configuraciones manuales a futuro
- Según el tipo de protocolo a utilizar puede llegar a tener mejoras en comunicación y tiempos acotados de respuesta en los envíos de mensaje de ida y vuelta conocidos estos últimos como RTT (Round Trip Time) es decir el delay promedio que se establece en una red a la hora de mandar un mensaje a la red destino.

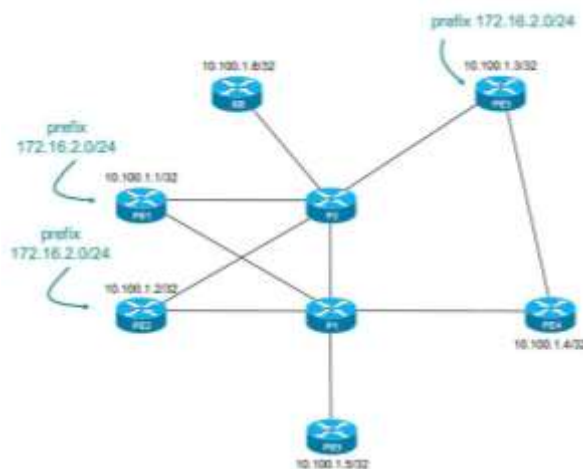


Figura 5. Protocolo de enrutamiento dinámico. Información tomada de <https://sites.google.com>. Elaborado por el autor

2.2.6.1 Ventajas de los protocolos de enrutamiento dinámico

- Tiempos de convergencia muy rápidos al existir un cambio en la red

- Aplicados en redes muy extensas o que cuenten con configuraciones complejas
- No se ven limitados por el tamaño de la red es decir pueden compartir rutas de forma eficiente
- Es tolerante a fallas permitiendo elegir rutas o caminos alternos hacia un destino

2.2.6.2 Desventajas de los protocolos de enrutamiento dinámico

- A diferencia del protocolo de enrutamiento estático consume mayores recursos en cuanto a RAM, CPU e incluso ancho de banda
- Son más inseguros debido a que propagan sus redes a sus vecinos donde con vectores de ataque como hombre en el medio se podría descubrir las redes alternas

Los protocolos de enrutamiento dinámico se dividen en dos grandes categorías conocidas como IGP (Internal Gateway Protocol) y EGP (Exterior Gateway Protocol) que son usados según su escenario de aplicación donde para mayor detalle se verá a continuación:

2.2.7 Internal Gateway Protocol

Se conoce como protocolos de puerta de enlace interior aquellos mecanismos que permiten establecer comunicación dentro de un sistema autónomo (ASN), es decir los protocolos de gateway interior tienen como funcionalidad permitir que todos los equipos ubicados dentro de una o varias organizaciones puedan comunicarse siempre y cuando pertenezcan al mismo grupo y su configuración no se vea afectada por otros sistemas que no pertenecen a sus tablas de rutas, (Vasquez, 2021).

IGP cuenta con dos clasificaciones en cuanto a protocolos de enrutamiento utilizados para comunicar redes que pertenezcan a un mismo grupo siendo ellos los protocolos de vector distancia y los de estado de enlace.

2.2.7.1 Protocolos de vector distancia

Los protocolos de vector distancia son aquellos que establecen el camino hacia un destino en función del conteo de saltos que tienen que dar para llegar a él es decir utilizan un mecanismo que permite establecer que rutas son las más optimas en función de la cantidad total de saltos que da en la red, (Zambrano, 2015).

Del mismo modo, los protocolos de vector distancia hacen uso del algoritmo de Bellman-Ford permitiendo tener una información completa de la red a través de sus vecinos que están directamente conectados y de haber un cambio en la topología puedan converger de manera muy rápida escogiendo rutas alternas para llegar al destino siempre y cuando las mismas sean validas y estén operativas, (Zambrano, 2015).

Los protocolos de vector distancia hacen uso de updates cada cierto tiempo indicando las rutas que cada vecino cuenta y con ello se pueda establecer los nuevos destinos en cada router por lo general según el protocolo aplicado puede demorar en el mayor de los casos hasta 120 segundos en transmitir toda la información de sus rutas a los demás vecinos llegando a ser un poco lento en cuanto a la forma de propagación. Por lo general este tipo de enrutamiento es utilizado en redes pequeñas que cuentan hasta con 15 saltos de destino permitiendo tener una visualización completa de la topología, un punto a mencionar es que si se tienen rutas con mayor cantidad a la mencionada de 15 automáticamente la red se considera inalcanzable.

Los protocolos que forman parte de la clasificación de vector distancia son:

- RIPv1 (Routing Information Protocol) en la actualidad obsoleto
- RIPv2 (Routing Information Protocol) successor de RIPv1
- IGRP (Interior Gateway Routing Protocol) en la actualidad obsoleto
- EIGRP (Enhanced Interior Gateway Routing Protocol) considerado protocolo híbrido

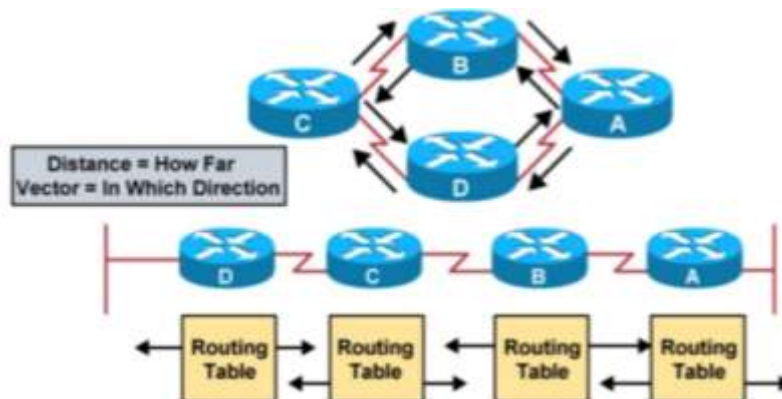


Figura 6. Protocolos de vector distancia. Información tomada de <https://sites.google.com>. Elaborado por el autor

2.2.7.2 Protocolos de estado de enlace

Los protocolos de estado de enlace a diferencia de los distance vector permiten tener una visibilidad completad de toda la red a través de los enlaces de comunicación que tienen hacia

sus vecinos los que incluye un mayor consumo de recursos, pero visualización general de cómo está compuesta la red, (Pérez, 2017).

Al igual que con los protocolos distance vector según el protocolo que se elija tendrá algunos beneficios frente a otro logrando de esta manera calcular el siguiente salto de la red.

Cada protocolo de estado de enlace calcula en cada uno de los routers cuales son los caminos más cortos para llegar a una red destino donde según la visibilidad de la topología se logra calcular la distancia que existe, (Cordova, 2010).

Otro punto por mencionar es que los protocolos de estado de enlace envían actualizaciones periódicas, pero solo cuando ocurren cambios en la topología esto permite reducir el uso excesivo de hardware.

De igual forma los protocolos de estado de enlace soportan el resumen de rutas, las redes con VLSM es decir que usen prefijos diferentes a los por defecto ejemplo /26 esto es conocido también como máscaras CIDR (Classless Inter Domain Routing).

A diferencia de los protocolos de vector distancia, solo existen 2 protocolos para estado de enlace siendo:

- IS-IS (Intermediate System to Intermediate System) cuenta con funciones parecidas a OSPF pero es muy poco usado debido a las funcionalidades que el protocolo Open Shortest Path First ofrece.
- OSPF (Open Shortest Path First) protocolo principal utilizados en las redes que usen protocolos de enrutamiento dinámico

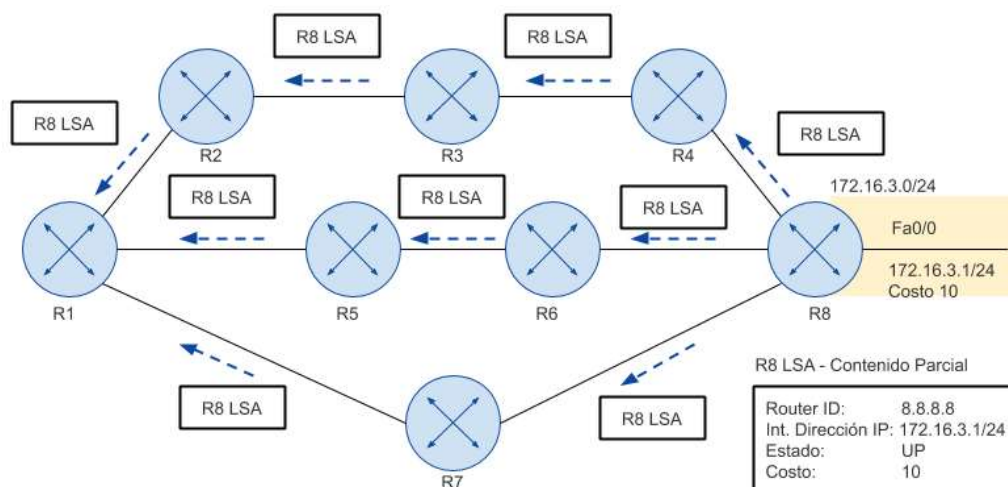


Figura 7. Protocolos de vector distancia. Información tomada de <https://sites.google.com>. Elaborado por el autor

2.2.8 Exterior Gateway Protocol

Se define como el protocolo estándar para la comunicación información que existe entre diferentes sistemas autónomos en internet a través del protocolo estándar BGP.

BGP ayuda con la retransmisión de información en las redes de diferentes entidades que tengan diferentes políticas de ruteo, (Riffo, 2009).

En la actualidad existen diferentes técnicas que permiten que BGP pueda realizar una retransmisión más rápidas hacia los equipos de borde de cada entidad siendo entre ellos MPLS el utilizado para la propagación de la red con BGP.

BGP posee información en enrutamiento manteniendo la base de datos de cada una de las redes destino permitiendo tener un completo gráfico de conectividad reduciendo los bucles de enrutamiento mediante correctas decisiones de directivas a nivel de sistemas autónomos.

En la actualidad existen múltiples variantes de BGP como MBGP (Multiprotocol Border Gateway Protocol) permitiendo diferentes atributos que pueden aportar información con mecanismos de IPv6 siendo esto más sencillo de implementar, (Cisco, 2020).

BGP trabaja sobre el protocolo TCP en el puerto 179 utilizado para establecer una comunicación al hacer uso de TCP se elimina la fragmentación, así como la confirmación, retransmisión y secuencia en updates.

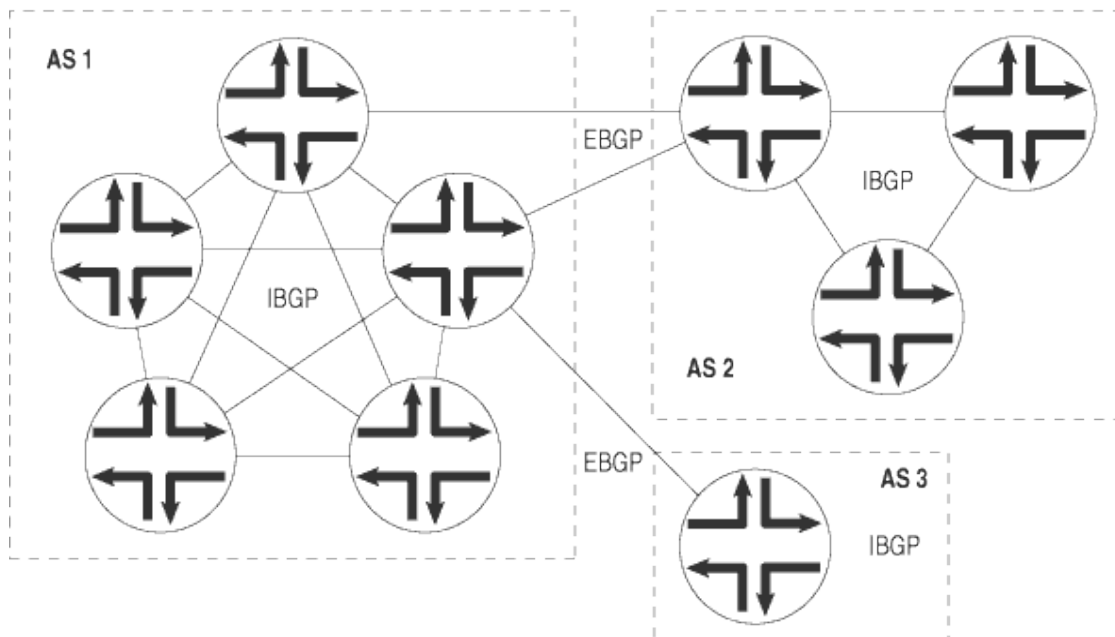


Figura 8. Exterior Gateway Protocol. Información tomada de <https://sites.google.com>. Elaborado por el autor

2.2.9 Distancia administrativa

Se conoce como distancia a la confiabilidad que existe en la red según el protocolo de enrutamiento a utilizarse, esto es debido a que cada protocolo cuenta con un valor numérico entero. La distancia administrativa indica que ruta es elegida para llegar a un destino entre los diferentes protocolos de red. Es importante mencionar que no solo los protocolos de enrutamiento cuentan con distancias administrativas sino también las interfaces locales que están conectadas de forma directa al equipo.

El protocolo con menor valor en distancia administrativa es el que pasará a formar parte de la tabla de ruteo del equipo y con ello se procederá al envío de la información es decir que la ruta elegida en la red.

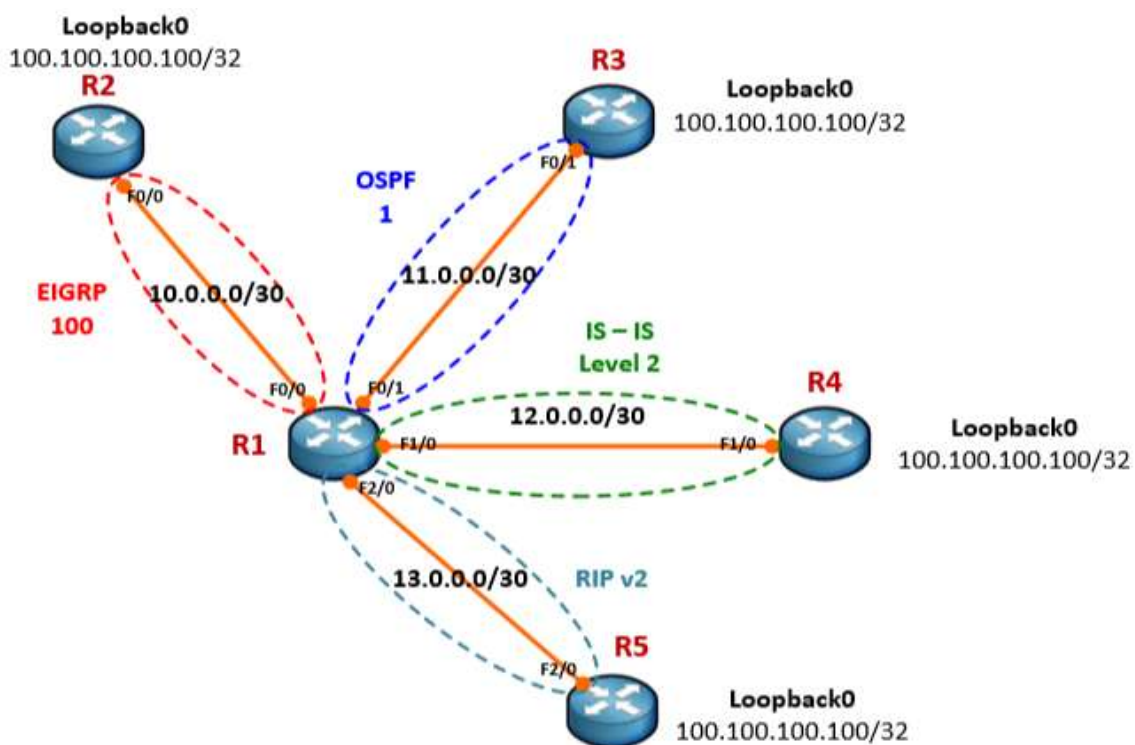


Figura 9. Exterior Gateway Protocol. Información tomada de <https://sites.google.com>. Elaborado por el autor

En la figura 9 se presenta una topología con varias redes entre ellos en el que se puede observar que cada router cuenta con protocolos de enrutamientos diferentes para su comunicación donde si se recapitula se mencionaba que aquel protocolo con la confiabilidad de la red de menor costo será aquel que forme parte de la tabla de enrutamiento global, para

ello es necesario hacer énfasis a sus valores de distancia administrativa según el fabricante de cada marca donde para este ejemplo se hace la comparativa con los valores definidos por cisco.

Origen de la ruta	Distancia administrativa
Conectada	0
Estática	1
Ruta resumizada EIGRP	5
BGP externo	20
EIGRP interno	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP externo	170
BGP interno	200

Figura 10. Costos EIGRP. Información tomada de <https://sites.google.com>. Elaborado por el autor

Como se puede observar en la figura 10, en cuestión de costo EIGRP es el protocolo que se podría estandarizar en la red y hacer que funcione solo con EIGRP esto es debido a su menor costo de distancia administrativa siendo el escenario ideal para aplicarse en la red.

2.2.10 Métricas de red

Otro valor que considerar es la métrica de red la cual hace referencia al valor o calculo que se usa para escoger porque destino debe viajar un paquete según el protocolo que se esté empleando, por ejemplo: si se usa RIPv2 se indicaba que trabajaba en base al conteo de saltos donde de haber 2 rutas para llegar al mismo destino el escogerá al que tenga menor saltos que realizar. Este proceso que se explicó como ejemplo es lo que se conoce como métrica a la facilidad de que un router tiene en elegir rutas diferentes que sean las más optimas cabe destacar que con RIP es el conteo de salto pero para protocolos de estado de enlace se hace función de otras características, (Alvarado, 2010).

Los protocolos de enrutamiento tienen definidas sus reglas o formas de establecer sus tablas de ruteo en el que cada algoritmo genera un valor totalmente distinto para cada ruta en la red. Para ello se procede a enumerar los protocolos de enrutamiento comúnmente más utilizados y con ello sus métricas de red.

- **RIP.** - Su métrica está basada al conteo de saltos donde por cada router atravesar se aumenta un valor de 1 en el contador, el total máximo para llegar a un destino es de 15 saltos superior a eso se considera métrica infinita, (Telecapp, 2022).

- **OSPF.** - Métrica basada en el ancho de banda que se utiliza al pasar por un enlace por lo general a los enlaces que son más rápidos se les define un costo más bajo con el fin de establecerlos como prioritarios en la red.
- **EIGRP.** - Cálculo de ancho de banda mediante valores de ancho de banda y delay así mismo puede incluirse la carga y la fiabilidad de la métrica en el cálculo.

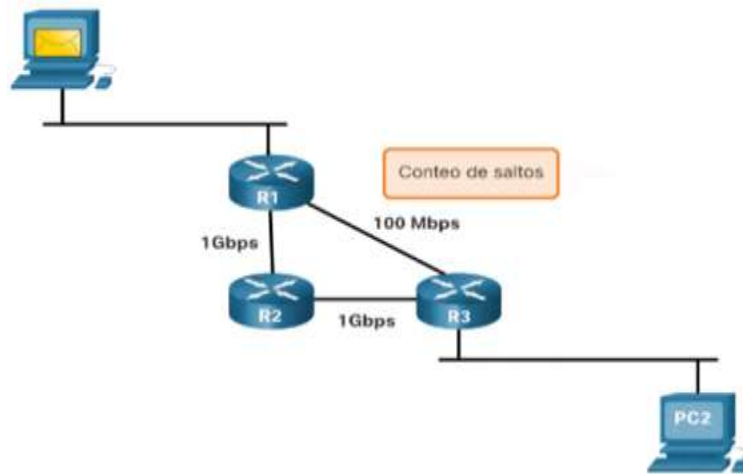


Figura 11. Métricas de Red. Información tomada de <https://sites.google.com>. Elaborado por el autor

Cuando se tiene métricas iguales en enlaces que van hacia un mismo destino se aplica lo que se conoce como balanceo de carga es decir que existen varias interfaces de salida que permiten llegar a un destino con el mismo costo por lo que los paquetes son enviados a través de los distintos enlaces hacia el destino, al hacer este proceso se logra tener una mejor efectividad y rendimiento en la red siempre que este correctamente configurado.

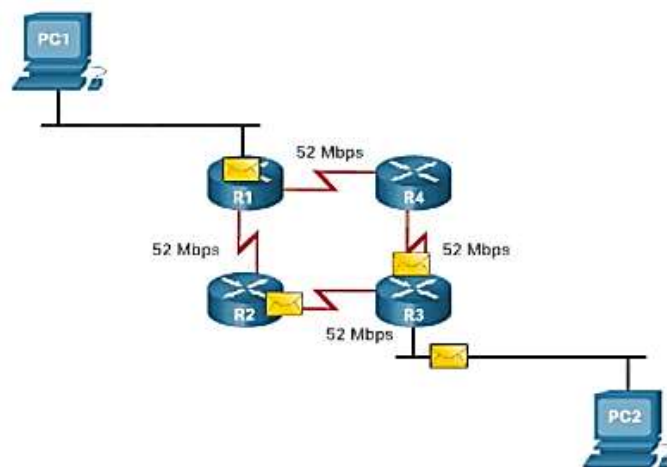


Figura 12. Métricas de Red. Información tomada de <https://sites.google.com>. Elaborado por el autor

2.2.11 Protocolos de redundancia de Gateway

Se conoce como protocolo de redundancia de Gateway aquel mecanismo que permite administrar dinámicamente el o los Gateway que se tengan para comunicación hacia servicios o redes externas conocidas como Internet, (Zambrano, 2015).

Para que los protocolos de redundancia de Gateway puedan trabajar de forma correcta es necesario tener direccionamiento IP y MAC de forma virtual con el fin de establecer un intercambio de mensajes de actualización o Hello a los equipos que forman parte de la IP o Gateway virtual. En la actualidad se utilizan diferentes técnicas no relacionadas con IP virtuales directamente, sino que hacen uso de diferentes soluciones llegando a tener una operabilidad lo más efectiva posible como puede ser:

- **ICMP Redirect:** Permite redirigir el tráfico generado por un Gateway a otro solo si el Gateway al que se le envían los datos a descubierto una mejor ruta para llegar al destino, este tipo de proceso no es óptimo debido a que si un Gateway cae no habrá esta comunicación.
- **Rutas estáticas:** Se establecen rutas por defectos a dos puertas de enlace con el fin de redistribuir el tráfico que vaya a viajar por esos enlaces el problema está en que no es un método escalable además de ser complejo de administrar.
- **Rutas dinámicas:** Se establece que los protocolos puedan aprender porque caminos deben enviar el tráfico al existir diferentes interfaces de salida es efectivo pero el consumo de recursos es elevado.
- **Protocolos dinámicos Gateway:** Son los más efectivos a la hora de administrar Gateway a través de diferentes métodos de administración de puertas de enlace como pueden ser HSRP, VRRP, GLBP.

2.2.11.1 Protocolo HSRP (*Hot Standby Router Protocol*)

El protocolo HSRP es propietario de Cisco que provee altos niveles de disponibilidad en puertas de enlace en el que es necesario al menos existan dos equipos de capa 3 que se encarguen de realizar el proceso de enrutamiento. Con este protocolo al haber dos equipos físicos lo que se procede a crear es un router virtual el cuál el que tendrá una dirección IP y MAC virtual que establecerá la comunicación con los equipos de capa 3 y la red, (Espinoza, 2018).

El protocolo HSRP (Hot Standby Router Protocol) hace que la dirección IPv4 o IPv6 a utilizarse se propague entre los grupos de routers que funcionan en la red local permitiendo que exista redundancias tolerables a fallos de red.

A la hora de configurar HSRP en un segmento de red, se puede proporcionar una MAC e IP que deben ser configuradas en el mismo grupo activo que se encarga de recibir y enrutar los paquetes que son enviados a la MAC virtual del grupo.

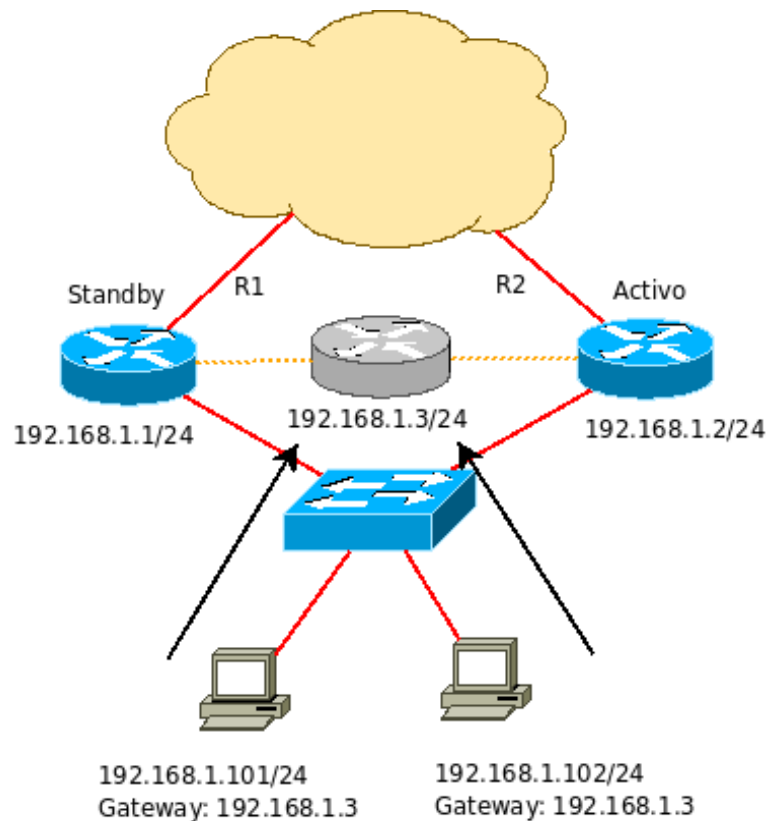


Figura 13. Protocolo HSRP. Información tomada de <https://sites.google.com>. Elaborado por el autor

2.2.11.2 Características de HSRP

- Protocolo creado por Cisco
- Se encarga de establecer una comunicación mediante una IP y dirección MAC Virtual para el grupo de routers conectados (Clúster)
- Se define un esquema de activo-pasivo siendo un router el encargado de enrutar tráfico y de fallar el pasivo realizará la misma función sin afectar a la red
- No se crea balanceo de tráfico a menos que se configure

Con el protocolo HSRP se pueden crear varios grupos que pueden segmentarse en base a la numeración que cada grupo recibe en donde para cada red existe un Gateway virtual que de querer comunicarse con la red deberá formar parte del mismo segmento IP, asimismo, se puede establecer funcionalidad de balanceo de carga en routers virtuales.

2.2.11.3 Roles de HSRP

Como se mencionó con anterioridad HSRP cuenta con 3 roles asignados a la hora de crear el clúster dividiéndose en: Router activo, router pasivo y router virtual.



Figura 14. Roles HSRP. Información tomada de <https://sites.google.com>. Elaborado por el autor

- **Router activo**
 - Equipo encargado de enrutar el tráfico que proviene de las diferentes redes siendo enviadas al equipo virtual.
 - Es el encargado de responder a los ARP request generado por los endpoint
- **Router virtual**
 - Encargado de responder al medio y establecer la comunicación entre los equipos finales y el equipo de capa 3.
 - Se requiere de una dirección IP y MAC para el grupo HSRP en el que estarán los equipos
 - La MAC por configurarse en HSRP contiene los bloques 00:00:0c:07:ac:xx donde XX hace referencia al número del grupo.
- **Router spare**
 - Equipo en espera responsable de sensor al equipo activo para validar su funcionamiento donde de presentar problemas el equipo en espera tomará el lugar del principal llegando a convertirse en el master, cabe mencionar que los mensajes utilizados para sensor el estado del equipo son de tipo Hello.

2.2.11.4 Estados HSRP

El protocolo HSRP cuenta con 6 tipos de estados utilizados para establecer el clúster virtual siendo estos:

- **Inicial:**
 - Estado por default del router antes de realizar el proceso de configuración
- **Aprender**
 - En esta fase el equipo desconoce la IP virtual
 - No se obtiene mensaje de tipo hello
 - No existe un proceso para realizar el proceso de activo o pasivo
 - Se encuentra a la espera de un mensaje por parte del equipo master
- **Escuchar**
 - Se tiene conocimiento de la IP virtual
 - No existe ninguna función en específico
- **Hablar**
 - Se conoce la IP virtual
 - Existen mensajes de tipo hello cada cierto tiempo
 - Busca participar en la elección del equipo activo o spare
- **Activo**
 - Encargado de procesar el enrutamiento de los paquetes



Figura 15. Estados HSRP. Información tomada de <https://sites.google.com>. Elaborado por el autor

2.2.12 Protocolo VRRP (Virtual Router Redundancy Protocol)

Protocolo definido en la RFC 3768, cuenta con funciones referentes a HSRP pero a diferencia de este último no es propietario es decir que puede ser utilizado por cualquier organización que desee establecer mecanismos de redundancia en Gateway.

VRRP soluciona diferentes problemas que existen a diferencia de otros mecanismos de redundancia en el que por lo general se caracteriza por trabajar con entornos configurados de manera estática, (Zambrano, 2015).

Se utiliza una IP virtual al igual que en HSRP y se define de manera automática una dirección MAC virtual para el clúster en el que funcionará el protocolo. Del mismo modo se elige un equipo que funciona como Master y todos los equipos operarán en modo Standby.

Cabe mencionar que el protocolo VRRP no establece mecanismos que permita balanceo de carga sobre múltiples puertas de enlace, por lo general el router VRRP controla las direcciones IP asignadas a través de un router virtual conocido como el router maestro el encargado de reenviar todos los datos a las direcciones IP que formen parte del clúster, (Patiño, 2015).

Cualquiera de las direcciones IP virtuales configuradas en los routers de la red LAN podrán ser utilizados como router de primer salto hacia los equipos finales ofreciendo una alta disponibilidad sin la necesidad de implementar ruteo dinámico o a través de un descubrimiento en cada endpoint que desee participar de la red, (Quiroz, Ramírez, & Rivera, 2013).

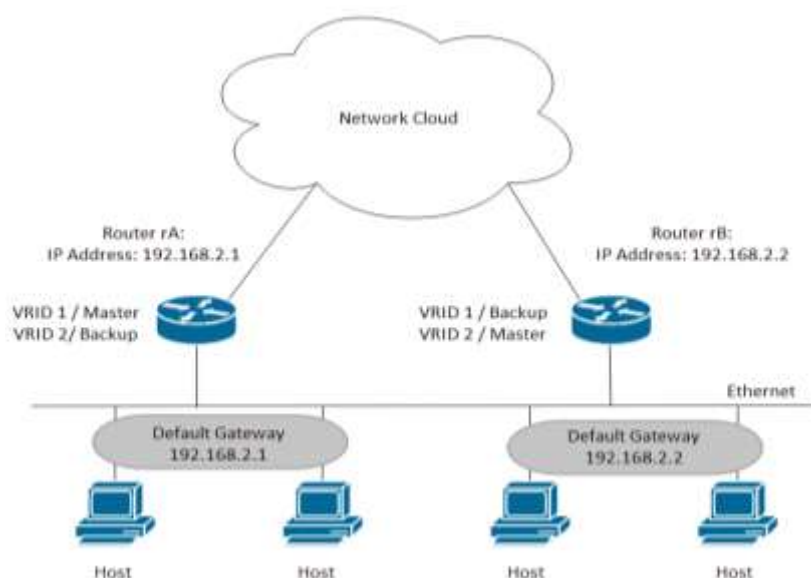


Figura 16. Protocolo VRRP. Información tomada de <https://sites.google.com>. Elaborado por el autor

2.2.12.1 Ámbitos de aplicación

El IETF en su RFC 2338 define cuales son las características, así como los objetivos de diseño de VRRP en la práctica en el que se menciona los estándares de mensajes utilizados, así como las reglas de procesamiento y el estado de cada máquina con el fin de garantizar la convergencia a través de un equipo máster o maestro.

El protocolo VRRP está diseñado a ser implementado en solo routers IPv4 a fin de solucionar diferentes problemas en cuanto a las peticiones ARP, los mensajes ICMP Redirect y los problemas de seguridad en red, (Patiño, 2015).

2.2.12.2 Atributos al configurar VRRP en enrutadores

- Se puede realizar la identificación del sistema
- Se establece un identificador de router dentro de la red LAN en la que este configurado
- Se obtiene una dirección IP principal encargada de enrutar el tráfico entre el origen y el destino, así como anunciar VRRP a través de mensajes hello.
- Creación de direcciones IPs virtuales
- Configuración de parámetros como prioridad, intervalos de anuncios, modo de aceptación y cambios.

Figura 17. Atributo VRRP. Información tomada de <https://sites.google.com>. Elaborado por el autor

2.2.12.3 Protocolo GLBP (Gateway Load Balancing Protocol)

El protocolo GLBP es un protocolo propietario de cisco el cual tiene como finalidad proveer redundancia de ruta a través de direcciones IP, con este mecanismo lo que se consigue es compartir el protocolo, así como las direcciones físicas (MAC) a su equipo de enrutamiento de capa 3, (Yerovi & Flores, 2010).

GLBP permite realizar una agrupación de equipos con el fin de poder distribuir la carga entre sus diferentes enlaces en el que siempre existe un equipo que funciones como el master y se encargue de tener el control automático, así como la definición de funciones de reenvío de tráfico.

A diferencia de HSRP y VRRP el protocolo de Gateway Load Balancing Protocol permite distribuir la carga entre los routers con el fin de proveer mejor protección a los datos que viajan y evitar que haya errores o fallos en el envío de paquetes por las interfaces de red, (Torres, 2016).

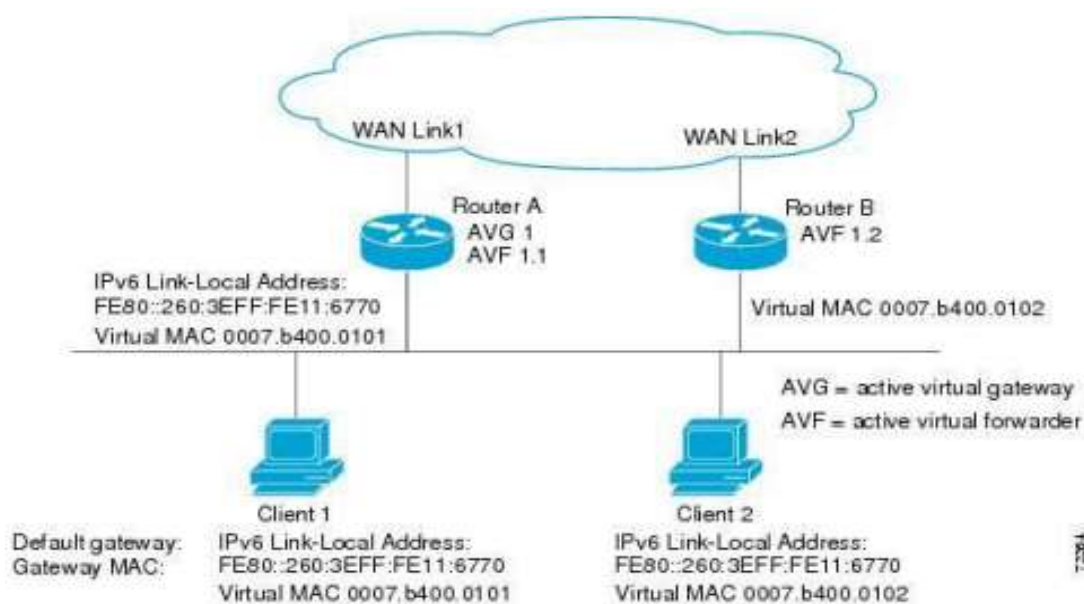


Figura 18. Roles GLBP. Información tomada de <https://sites.google.com>. Elaborado por el autor

2.2.14.4 Características de GLBP

- **Load-balancing.** - Hace referencia en como el tráfico de los clientes puede llegar a ser compartido sin problema con los equipos de capa 3, permitiendo realizar un equilibrio de carga eficiente entre los equipos que forman parte del grupo de GLBP

- **Múltiples routers virtuales.** - El protocolo GLBP es capaz de admitir un total de 1024 routers para que funciones de manera virtual en cada una de las interfaces físicas con las que cuenta el equipo, asimismo permite tener hasta un total de 4 routers virtuales por grupo
- **Preemption.** - Se logra que a través de este mecanismo se pueda tomar a los Gateway virtuales así como a los equipos en spare para el reenvío de los datos.
- **Autenticación.** - Es el tipo de cifrado aplicado para brindar seguridad a los mecanismos de red a través del uso de una clave secreta de tipo hash MD5 que se concatena al paquete de salida y que debe coincidir con el hash generado por el receptor, caso contrario el paquete procede a ser descartado. Dentro del formato de autenticación existen dos tipos a considerar:
 - **Autenticación de texto sin formato:** Se emplea un mecanismo de autenticación de texto simple para la comunicación
 - **Proceso sin autenticación:** No se requiere credenciales

GLBP como se mencionó proporciona protocolos de redundancia en el que puede aplicar mecanismos de balanceo de carga, mediante tres mecanismos comúnmente conocidos los cuales se detallan a continuación:



Figura 19. Características de GLBP. Información tomada de <https://sites.google.com>. Elaborado por el autor

- **Round Robin.** - El tráfico comienza se procesa según la cantidad de direcciones IP que se tengan enviando en forma secuencial las peticiones y puedan ser atendidas.

- **Ponderado.** - Trabaja en base a la prioridad de la información el cual es definido según el peso con el que venga una petición asociada a la dirección MAC.
- **Depende del host.** - Las direcciones Mac virtuales están atacadas al activo que hizo la petición es decir el equipo que hizo la petición siempre será su información procesada por el equipo con la dirección mac virtual que lo atendió.

2.2.13 Simulador GNS3

GNS3 es un simulador con entorno gráfico que permite diseñar redes básicas como complejas en el que se hace uso de iso de los diferentes fabricantes de productos de red en el mercado permitiendo establece una combinación de activos de red mediante máquinas virtuales y realizar los laboratorios lo más realistas posibles, (Figuerola, Díaz, & Gramajo, 2017).

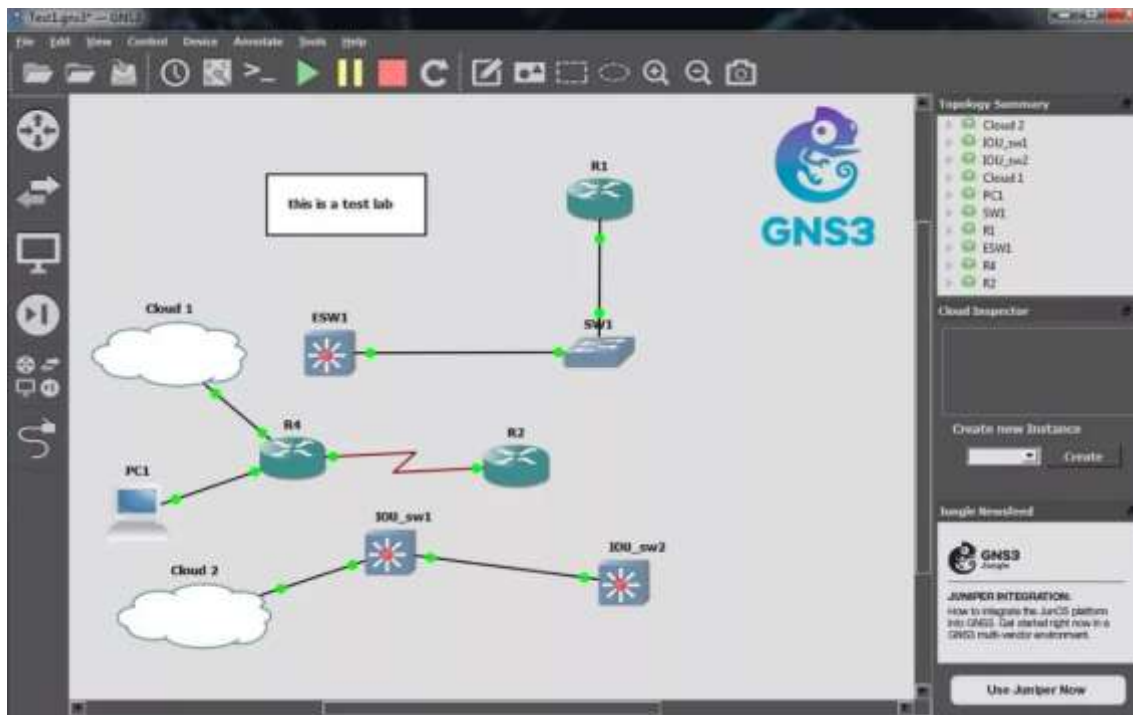


Figura 20. Interfaz gráfica GNS3. Información tomada por la Investigación Directa. Elaborado por Valencia Carpio Víctor Andrés.

Para que GNS3 pueda establecer las simulaciones en su entorno de red es necesario 3 componentes en su diseño.

- **Dynamips.** - Es un emulador de ios lo que permite a un usuario ejecutar imágenes ISO de diferentes fabricantes tales como Juniper, Cisco, Fortinet.

- **Dynagen.** - Está basado en texto y diseñado para los dynamips, es usado mediante un front end.
- **Qemu.** - Permite hacer uso de máquinas virtuales tales como VMware o VirtualBox y ejecutar entornos más reales pero se requiere de mayor cantidad de recursos del ordenador.

2.2.14 Wireshark

Analizador de protocolos utilizado para realizar un análisis de red en sus distintos protocolos y así encontrar falencias y solucionar problemas de red. Cuenta con un entorno gráfico siendo dinámico e interactivo. Además de contar con modo promiscuo de la red lo que permite poder escuchar todo el tráfico que existe en la red así como también se puede llegar a examinar datos de un archivo de captura, (Álava & Arcia, 2021).

Wireshark es un analizador de tráfico muy potente que muchas veces es utilizado para encontrar falencias y explotaras, posee herramientas de búsqueda avanzada además de presentar de manera gráfica los datos que pasan por una interfaz, el porcentaje de datos TCP o UDP, entre otros. También es conocida por ser una herramienta de software libre por lo que puede ser ejecutada en la mayoría de los sistemas operativos en la actualidad como puede ser Microsoft, MacOS e incluso en distribuciones de Linux como Solaris, FreeBSD así como Android.

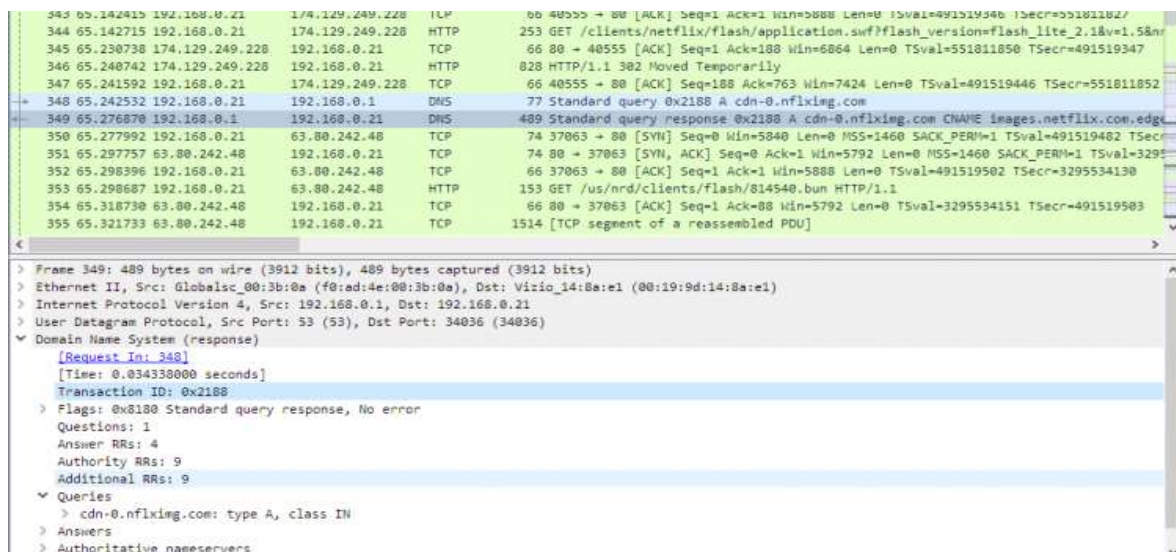


Figura 21. Interfaz Wireshark. Información tomada de <https://sites.google.com>. Elaborado por el autor

2.3 Marco conceptual

2.3.1 Red LAN

Conjunto de dispositivos interconectados entre sí por medio de equipos de comunicación con el fin de permitir el dialogo entre ellos, el cual varía en base a los tipos de consultas a realizarse, por lo general una red LAN en muchas ocasiones no excede los 250 dispositivos dentro de una organización y están situados en una misma organización

2.3.2 Red Wan

Permite la comunicación entre sitios que se encuentran relativamente alejados entre si a velocidades extremadamente altas según rutas definidas o incluso velocidad de navegación que se tenga por parte de una organización u hogar.

2.3.3 Router

Un enrutador o caminador de red permite la comunicación de dispositivos segmentados o ubicados en otros dominios de broadcast mediante su lógica de enrutamiento definida en su software.

2.3.4 Switch

Es un dispositivo de red que cuenta con una amplia cantidad de puertos con el fin de permitir tener varios componentes conectados y permitir el paso de la información desde un punto a otro.

2.3.5 Access Point

Dispositivo que permite mediante ondas electromagnéticas propagar diferentes SSIDs permitiendo que usuarios con equipos móviles puedan estar conectados constantemente mediante se desplacen de un punto a otro.

2.3.6 Round Robin

Algoritmo que permite establecer la distribución de los servicios dentro de un sistema de forma equitativa con el fin de usar todos los recursos de un equipo permitiendo mejor

rendimiento, para ello todo cada una de las tareas asignadas se hacen de forma ordenada y con la misma prioridad

2.3.7 Load-Balancing

Protocolo capaz de permitir la compartición de tráfico a través de dos o más equipos permitiendo mantener múltiples conexiones hacia diferentes servicios siendo Internet al que comúnmente es accedido a través de este método.

2.3.8 IP Hash

Proceso utilizado para establecer balanceo de carga en base a una dirección IP de origen y destino para cada uno de los paquetes que llegan a la red. Para el proceso es necesario aplicar un proceso XOR que permita definir la velocidad de enlace en cada una de las NIC y así establecer la cantidad de tráfico necesaria a pasar, por lo general es utilizado mucho en las etapas de virtualización

2.3.9 MAC

Dirección hexadecimal que identifica a un equipo físico por lo general las direcciones MAC se quedan en el chip de la memoria ROM esto con el fin de no se alteradas. Un punto importante por considerar es que todas las direcciones MAC son únicas en el mundo por lo que no habrá un equipo que use la misma dirección

2.3.10 IP

Se conoce como la identificación a nivel de capa 3 y es capaz de permitir que equipos puedan establecer una comunicación a través de diferentes métodos uno de ellos es la prueba de conectividad con el comando ping del protocolo ICMP.

2.4 Marco contextual

El estudio de investigación será realizado en la empresa SANFERSYSTEMS S.A ubicada en la ciudad de Guayaquil con la finalidad de analizar la situación de la red actual y proponer una red con protocolos de redundancia de puerta de enlace permitiendo así tener una disponibilidad constante hacia Internet al igual que tener una red tolerante a fallas.

SANFERSYSTEMS S.A. es una entidad dedicada a brindar soluciones en cuanto a diseño de páginas web, así como el asesoramiento y capacitación en lo que respecta a tecnología por lo que constantemente hace uso frecuente de aplicaciones o dominios exteriores que permitan desarrollar entornos eficientes.

Actualmente cuenta con dos proveedores de Internet con el fin de tener una operabilidad constante hacia peticiones externa donde un punto a mencionar es que no existe una correcta configuración de enlaces y solo uno de ellos funciona mientras que el otro solo estará operativo si y solo si el primero llegase a fallar, por ende, todo el proceso que realizarse es de forma manual además de que su red interna no cuenta con los criterios adecuados de segmentación en el que se busca diseñar una red capaz de usar un Gateway virtual que permita establecer una comunicación a la red interna mediante un clúster virtual en los equipos de red.

2.5 Marco legal

El presente trabajo de investigación hace énfasis a los reglamentos de la Ley Orgánica de Telecomunicaciones y la Ley Especial de Telecomunicaciones.

El artículo 6 referente a la Ley Especial de Telecomunicaciones menciona que, todo aquel medio o dispositivos que proporcionan capacidad completa para la comunicación entre usuarios ya sea mediante activos finales como ordenadores, teléfonos, entre otros son denominados servicios finales.

Por otra parte, el artículo 9 en su reforma de telecomunicaciones menciona que las redes se clasifican en dos grandes grupos los cuales son:

- Redes públicas de Telecomunicaciones anunciadas en Internet
- Redes privadas de Telecomunicaciones utilizadas en Pymes o redes SOHO

Es esencial que ambos grupos son divididos según las definiciones proporcionadas en la IETF en sus documentos de RFC en base a la norma 1918. Del mismo modo, el art. 13 referente a las redes privadas de telecomunicaciones menciona que se conoce como redes privadas aquellos grupos de red que son de uso exclusivo de una entidad u organización que tiene instalada soluciones que brinden accesibilidad a la información bajo su control en el que su operación debe ser auditada y aprobada por la Agencia de Regulación de Control de Telecomunicaciones.

Del mismo modo, el artículo 15 referente a la Ley especial de telecomunicaciones indica que únicamente las redes privadas pueden ser usadas para beneficios de usuarios finales y no puede ser sustentadas de ningún modo es decir es prohibido realizar la prestación de servicios a terceros usando segmentos privados. Debido a que las redes privadas no pueden intercomunicarse entre ellas.

Por otra parte el Artículo 76 referente a las técnicas necesarias para implementación de seguridad y solución o reducción de vulnerabilidades menciona que aquellos prestadores de servicios que otorguen segmentos de red propia o de un tercero deberán ajustar políticas adecuadas para Harden izar la seguridad en la red esto con el fin de no ser vulnerables a cualquier fallo de seguridad que pueda existir en Internet o de forma interna logrando así se garantice mejoras en cuanto a los riesgos existentes.

Capítulo III

Diseño de investigación

El presente trabajo de investigación está enfocado en el uso de diferentes técnicas de protocolos de redundancia de puerta de enlace que permitan determinar cuál es la más factible a ser desarrollado y con ello establecer las diferentes funcionalidades o mejoras en el estudio a tratar.

3.1 Metodología Bibliográfica

Utilizada con el fin de indagar en estudios previos en cuanto antecedentes a través de diferentes fuentes como libros, revistas, sitios, web, entre otros. Determinando de qué forma puede llevarse a cabo el diseño de redundancia de gateway para la empresa SANFERSYSTEMS S.A.

3.2 Deductiva

Busca determinar una conclusión referente al estudio realizado mediante el método deductivo con el fin de describir la acción del funcionamiento de un diseño o sistema.

3.3 Exploratoria

A través del método exploratorio se busca llevar a cabo el estudio de un tema en profundidad a punto de responder las dudas que existan, así como explorar el problema y el entorno en el que opera para posteriormente obtener una conclusión sobre el mismo.

3.4 Explicativa

Se conoce como método explicativo a todo aquel trabajo que tiene como finalidad determinar las causas de un determinado suceso o fenómeno para conocer los hechos que han pasado para que el fenómeno exista.

3.5 Técnicas de recopilación de datos

Son conocidas como el método que obtiene información sobre un estudio o trabajo en específico con el fin de establecer resultados que aporten a la investigación.

Por lo general se pueden definir mediante diferentes métodos de recopilación de datos como son: La entrevista o la encuesta.

3.5.1 La entrevista

Es la técnica utilizada para obtener información referente a un estudio, en el que se obtiene opiniones de manera abierta a alguien que tenga un alto conocimiento en la rama o tema a tratar. Logrando así tener una mejor idea e incluso una mejor gestión de análisis en cuanto a los protocolos de redundancia de enlace y su forma de operación.

De este modo se pretende hacer una serie de preguntas a un especialista en conectividad el que actualmente es colaborador de la empresa SANFERSYSTEMS S.A.

3.5.2 Formato de preguntas para entrevista a especialista en conectividad de la empresa SANFERSYSTEMS S.A.

1.- ¿Qué problema actualmente a nivel de red posee la empresa SANFERSYSTEMS S.A?

Respuesta: Se tiene problemas a nivel de vlans debido a que no están bien segmentadas, adicional a ello la mayor parte del tiempo existen inconvenientes con los diferentes enlaces de internet

Análisis: Cómo se puede observar actualmente la entidad cuenta con problemas a nivel de red siendo totalmente plana y expuesta a tormentas de broadcast e incluso loops de capa dos, además la administración de los enlaces no es automatizada lo que demanda tiempo en cuanto a cambio y operabilidad de los servicios que actualmente la empresa maneja.

2.- ¿Conoce usted el tipo de comunicación y los protocolos de enrutamiento utilizados en la red actual?

Respuesta: No se cuenta con protocolos de enrutamiento a nivel de red interna, en la parte externa se usa rutas estáticas para llegar a los diferentes servicios de forma manual.

Por otra parte, el tipo de comunicación utilizado es el TCP/IP.

Análisis: Debido a que la red actual no tiene un diseño jerárquico la empresa no maneja un esquema de enrutamiento, esto impide que no se aproveche de las características de los

equipos. Un punto importante por mencionar es que las rutas estáticas están configuradas para que funcionen de forma manual por lo que si falla un enlace se debe reconfigurar la ruta para tener salida con su enlace de backup.

3.- ¿Cuál es el ancho de banda actualmente otorgado por los diferentes proveedores de servicio

Respuesta: Cada proveedor ofrece 10Mbps de ancho de banda dedicado y simétrico.

Análisis: El ancho de banda proporcionado por los proveedores de servicio es actualmente suficiente para la cantidad de usuarios que laboran en la entidad, el ancho de banda otorgado es igual tanto en carga como descarga.

4.- ¿Cuáles son los servicios críticos que la empresa SANFERSYSTEMS S.A debe tener siempre operativos hacia la extranet?

Respuesta: Actualmente se cuenta con un sitio web creado en wordpress que debe siempre estar expuesto a internet con el fin de proporcionar información de los servicios que se ofrecen.

Análisis: El servicio que se maneja se considera altamente crítico debido a que es el que permite interactuar al usuario con las soluciones que la entidad brinda al público, por lo que debe operar 24/7 debido a la cantidad de peticiones o consultas que recibe a diario.

5.- ¿Qué métricas considera necesarias en cuanto a calidad de servicio se refiere para que la empresa SANFERSYSTEMS S.A opere sin problemas?

Respuesta: Jitter, Delay, Latencia

Análisis: Todos los servicios considerados como importantes por parte del especialista en redes son considerados a nivel de capa 1 y 2 del modelo OSI por lo que para tener mejoras es necesario realizar una reconfiguración en cuanto a diseño y conectividad del sitio.

6.- ¿Conoce usted sobre los protocolos de redundancia de puerta de enlace y su forma de operación?

Respuesta: Para ser sincero no tengo conocimiento al respecto

Análisis: Se observa que actualmente no existe conocimiento en cuanto a los protocolos de puerta de enlace lo que ha impedido que sean aplicados y así mejore la conectividad del servicio de la empresa SANFERSYSTEMS S.A.

7.- ¿Qué tan recomendable sería tener una red que permita operar con sus Gateway a internet en formato activo/pasivo?

Respuesta: Muy factible, debido a que se reduce de forma drástica los tiempos de configuración, además se tiene un mejor control según el mecanismo implementado.

Análisis: Se puede constatar que el personal técnico considera factible realizar cualquier proceso que permita tener a sus equipos operando todo el tiempo.

8.- ¿Cuántos proveedores de servicio de internet posee en su red?

Respuesta: Se tiene solo un proveedor de servicio que brinda acceso a Internet tanto vía cableada el cual llega por fibra y un enlace de respaldo mediante medio no guiado es decir un radioenlace

Análisis: Debido al servicio constante publicado en Internet así como las peticiones realizadas por los usuarios de manera de interna obliga, que se tenga dos enlaces de internet que actualmente trabajan de manera activo/pasivo pero de forma manual.

9.- ¿Posee algún tipo de configuración en cuanto a redundancia de Gateway se refiere?

Respuesta: Cómo indicaba anteriormente desconozco de este tipo de configuración

Análisis: La red actual no tiene mecanismos de redundancia aplicados debido al desconocimiento que el ingeniero en redes posee.

10.- ¿Cuál es el tiempo de inactividad que ocurre cuando existe un fallo de Gateway y se debe configurar la red para que funcione el enlace de respaldo o viceversa?

Respuesta: Aproximadamente de 1 a 2 minutos debido a los procesos que se realizan de configuración

Análisis: Los altos picos de respuesta a incidente son generados debido a que se debe realizar cambios manuales e incluso configuración de la ruta estática haciendo que a manera lógica se prolongue la convergencia y envío de datos además del alto tiempo que demanda la reconfiguración del servicio.

3.6 Elementos utilizados para el diseño de la propuesta

3.6.1 Comparativa de protocolos de redundancia de puerta en enlace

Para el trabajo de investigación actual será necesario definir el protocolo adecuado a la hora de realizar redundancia de Gateway logrando así mantener la disponibilidad de la información.

Otro punto por considerar al momento de realizar la comparativa es la compatibilidad que existe en cuanto a fabricantes permitiendo así tener una gestión accesible a la red, por lo que, a continuación, se presenta los datos a comparar:

Tabla 1. Comparativa de protocolos de redundancia de gateway

Característica	HSRPv2	VRRP	GLBP
Estándar/Propietario	Cisco	IETF	Cisco
IP Virtual	Si	Si	Si
Dirección MAC Virtual	0000.0c9f.fxxx	0000.5e00.01xx	0007.b4xx.xxyy
IP Destino	224.0.0.102	224.0.0.18	224.0.0.102
Puerto	UDP 1985	-	UDP 3222
ID de grupo	12 bits	8 bits	16 bits
Forma de operación	Activo/Pasivo	Master/Backup	1 AVG + 1 AVF
Load-balancing	No	No	Si
Mensajes Hello	3 seg	1 seg	3 seg
Autenticación	Si	IOS	Si
Soporta IPv6	Si	Si	Si
Latencia	Media	Baja	Baja

Información tomada de la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Como se observa en la tabla 1 existen 3 protocolos capaces de realizar la redundancia de Gateway en las redes LAN, permitiendo mantener una mayor disponibilidad y comunicación, aunque el protocolo GLBP sea el protocolo idóneo para diseño o implementación de redes al ser propietario se vuelve una solución sumamente cara debido a la adquisición del hardware necesario para el desarrollo del protocolo al igual que HSRP.

Por otra parte, VRRP es un protocolo estándar capaz de poder operar entre diferentes fabricantes lo que permite una interoperabilidad en las redes debido a que es protocolo abierto capaz de ser analizado e incluso mejorado como según sea necesario.

VRRP al ser un protocolo abierto tiene mayor facilidad en cuanto a su despliegue debido a que existen soluciones mucho más baratas que permiten levantar configuraciones para ser aplicados en escenarios como los antes descritos.

Otro punto para considerar es que las métricas evaluadas por el protocolo VRRP son mucho más eficiente, lo que le permite tener mejores tiempos de respuesta y comunicación con la red siendo entre ellos la latencia y el round trip time en el que por ser multifabricante VRRP ha conseguido ser el protocolo comúnmente implementado en las redes LAN.

Otras métricas para considerar por el cual VRRP fue escogido frente a los diferentes protocolos de puerta de enlace es que no cuentan con un puerto UDP en específico en el cual se transmite la comunicación siendo más fácil su uso por otra parte los tiempos de mensaje hello para informar a la topología de un cambio de la red le permite ser actualmente el protocolo más utilizado.

Cabe recalcar que con VRRP se logra que los equipos funcionen en base a grupos y con ello reducir de mejor manera la carga de tráfico enviada al equipo siendo factible su diseño.

Para el presente proyecto se tiene pensado hacer uso de VRRP para el diseño simulado de la empresa SANFERSYSTEMS S.A y comprobar su forma de operación y mejora frente al diseño actual.

3.7 Compatibilidad de simuladores de red

Se presenta los tipos de entornos utilizados para realizar laboratorios virtuales o diseños de red emulados que permitan comprobar la funcionalidad de la arquitectura y posteriormente ser implementado ahorrando tiempo y dinero.

Tabla 2. Simuladores de red para entornos virtuales

Característica	GNS3	EVE-NG	PNETLAB
Administración	Facil	Media	Facil
Implementación	Facil	Media	Media
Costo	Bajo	Bajo	Bajo
Recursos de hardware	Alta	Media	Baja
Documentación	Alta	Baja	Baa

Información tomada de la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

GNS3 a diferencia de los otros simuladores de red cuenta con mayores ventajas de uso permitiendo una interacción mucho más sencilla y directa. Su forma de instalación al ser es sencilla a diferencia que sus competidores.

3.8 Compatibilidad de simulador GNS3 con S.O.

A continuación, se presenta la compatibilidad que existe del simulador de red GNS3 con los sistemas operativos más utilizados en el mercado a fin de poder determinar cuál es el que mejor se adapta para la etapa de diseño.

Tabla 3.Compatibilidad de simulador en Sistemas Operativos

Característica	Windows	Ubuntu	MAC
Etapas de instalación	Fácil	Media	Fácil
Compatibilidad con SO	Alta	Alta	Alta
Aprendizaje	Fácil	Medio	Fácil
Documentación	Alta	Media	Baja
Licenciamiento	Free	Free	Free

Información tomada de la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

En cuanto a compatibilidad se refiere se puede constatar que el sistema operativo Windows cuenta con mayores ventajas frente a sus competidores esto debido a ser el sistema más utilizado en la actualidad por lo que la información referente a GNS3 para ser desplegado en Windows es muy amplia y sencilla de entender.

Otro punto para tener en cuenta es que al tener, gran parte de las personas desconocimiento de sistemas basados en el kernel de Linux ya sea Ubuntu, Debian, entre otros se considera compleja la instalación del software para muchos siento difícil a veces de entender debido a su arquitectura.

3.9 Requisitos mínimos para uso de GNS3

Para realizar el diseño de red en el simulador elegido previamente es necesario contar con una serie de requisitos en cuanto a hardware se refiere, permitiendo una mejor operabilidad de la solución presentada. Por lo que se describe a continuación los requerimientos mínimos a utilizar para el trabajo de investigación.

Tabla 4. Requerimientos mínimos para simulador de red GNS3

Característica	Descripción
Procesador	Con 4 o más núcleos lógicos a 2.0GHz
Virtualización	Función habilitada desde la BIOS
Memoria RAM	8Gb RAM
Disco Duro	50GB
Tarjeta Gráfica	Opcional

Información tomada de la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

3.10 Diseño de red actual SANFERSYSTEMS S.A.

SANFERSYSTEMS S.A posee un segmento de red 192.168.10.0/24 del cual 28 usuarios hacen uso de la red tanto wireless como cableada en el que para ello todas las conexiones wireless se realizan con un Access Point de marca TredNet funcionando en modo AP Bridge por lo que el direccionamiento que entrega a los dispositivos que se conectan a través de la red inalámbrica es igual que el segmento principal. Por otra parte el switch core posee actualmente 48 puertos que trabajan a velocidades de 10/100/1000Mbps permitiendo la conexión de los diferentes equipos y servicios de red tales como son el servidor de dominio, dns, dhcp, entre otros.

Al no haber vlans todos los equipos que se conectan al switch forma parte por defecto de la vlan 1 y a la hora de conectarse hacia Internet el switch core, cuenta con funciones de capa

3 (enrutamiento) que tiene conectado dos cables que van hacia los equipos del ISP, uno por cada tipo de conexión es decir fibra y radioenlace. El switch tiene solo una ruta estática que apunta hacia uno de los dos equipos que permiten la salida a Internet donde de haber problemas el equipo de core deberá ser configurado para que ahora apunte hacia el otro dispositivo disponible permitiendo el acceso a la extranet.

Cabe recalcar que a la hora de realizar la conexión hacia los dos equipos de borde el equipo de capa 3 tendrá que apuntar a redes que son totalmente diferentes ocasionando que la ruta sea configurada constantemente haya caídas de servicio.

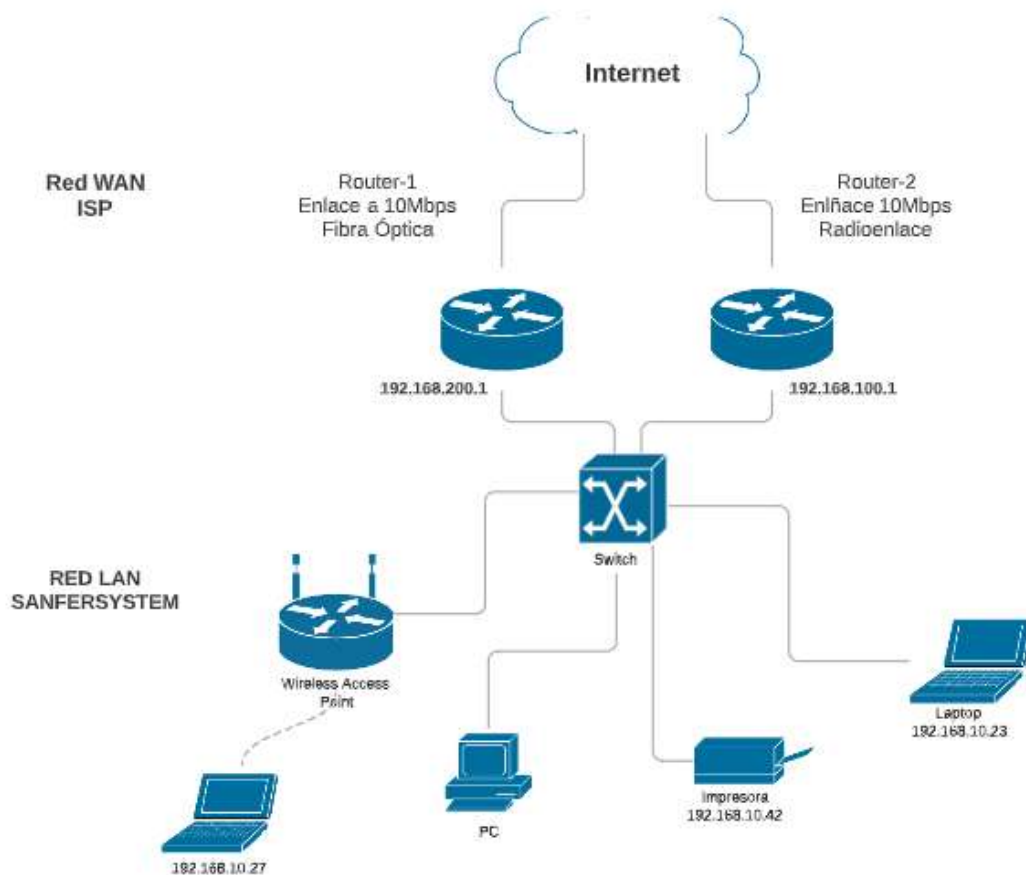


Figura 22. Topología Propuesta. Información tomada de <https://sites.google.com>. Elaborado por el autor

Como se puede observar en la figura 22 se presenta la topología actual de la empresa SANFERSYSTEMS S.A el cual por mayor entendimiento se ha omitido mayor cantidad de dispositivos a conectarse. En puntos anteriores se indicó que al ser una red totalmente plana existen problemas muy comunes siendo entre ellos:

- Bucles de enrutamiento a nivel de capa 2
- Tormentas de broadcast
- Inundación de puertos a través de ARP Poisoning
- Mayor RTT (Round Trip Tier) en cuando a paquetes ICMP
- Redundancia de gateway no existente con altos tiempos de respuesta en cuanto a configuración y cambio de enlaces

Debido a todos los problemas suscitados a continuación se plantea un esquema de red que permita que SANFERSYSTEMS S.A pueda operar de manera eficiente sin ver afectada a la disponibilidad de la información ya sea de manera interna o externa a la organización.

3.11 Diseño propuesto

Para el diseño propuesto se deberá considerar ciertos factores antes de realizar el despliegue teniendo entre ellos:

- Las redes van a segmentarse según el tipo de equipo a conectar y su uso ejemplo se crearán vlan para la red de servidores, vlans para la red inalámbrica, definidas de la siguiente manera:
 - Vlan 1.- Vlan por defecto sin direccionamiento IP
 - Vlan 5.- Será para la red inalámbrica con el segmento de red 192.168.5.0/24
 - Vlan 10.- Perteneciente a usuarios con red 192.168.10.0/24
 - Vlan 20.- Servidores con red 192.168.20.0/24
 - Vlan 40.- Para administración con segmento 192.168.40.0/24
- El switch core al contar con funciones de enrutamiento deberá ser capaz de crear SVI (Interfaces vlans) para segmentar la red actual
- El equipo de conmutación de capa 3 además deberá realizar funciones de ruteo permitiendo la comunicación entre vlans
- Solo habrá una ruta por defecto capaz de comunicar a la red interna hacia Internet, evitando la configuración manual de rutas estáticas a futuro
- A nivel de routers existirán equipos funcionando en modo Master/Backup
- Tanto el equipo master como el equipo backup deberán contar con una IP virtual que permitirá la comunicación con el switch core

- La red en la que se conectarán los equipos Master/Backup y switch core deberán ser del mismo segmento esto con el fin de que VRRP funcione de forma sin problema
- Se deberá crear rutas estáticas de retorno desde los routers del proveedor hacia el switch core con el fin de obtener respuestas caso contrario la red no funcionará.

Una vez explicado el funcionamiento de la red se procede a detallar el esquema planteado y con ello su tipo de conexión.

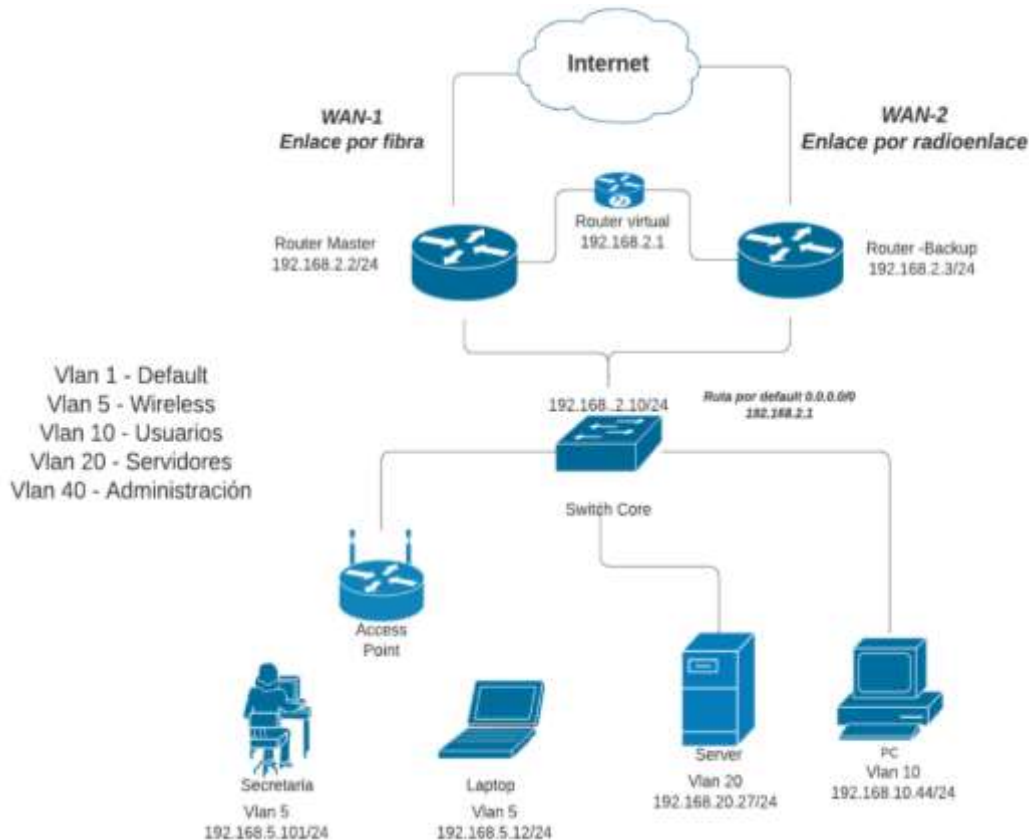


Figura 23. Funcionamiento de la red. Información tomada de <https://sites.google.com>. Elaborado por el autor

3.12 Esquema de red realizado en GNS3

Para la creación del entorno en GNS3 será necesario asignar la mayor cantidad de RAM posible con el fin de tener un control eficiente de la red, del mismo modo a la hora de realizar el esquema de red un punto a considerar es que GNS3 no permite hacer uso de redes inalámbricas ya que toma un adaptador virtual que esta concatenado a la interfaz física del equipo esto no afectará al trabajo de investigación debido a que se cumple con proporcionar redundancia de Gateway y en un entorno real la configuración de los Access Point es mínima.

Por lo que para el tema de wireless se colocará un switch adicional que haga de bridge con conexión física. Una vez claro el funcionamiento de GNS3 en el escenario propuesto se utilizará VMware a fin de virtualizar GNS3 y tome recursos físicos del equipo host permitiendo que el escenario propuesto sea lo más realista posible usando imágenes de equipos reales.

Para ello se deberá esperar que GNS3 cargue todos sus complementos dentro de VMware donde de hacerse de forma correcta proporcionará una IP para administración tal como se presenta a continuación:

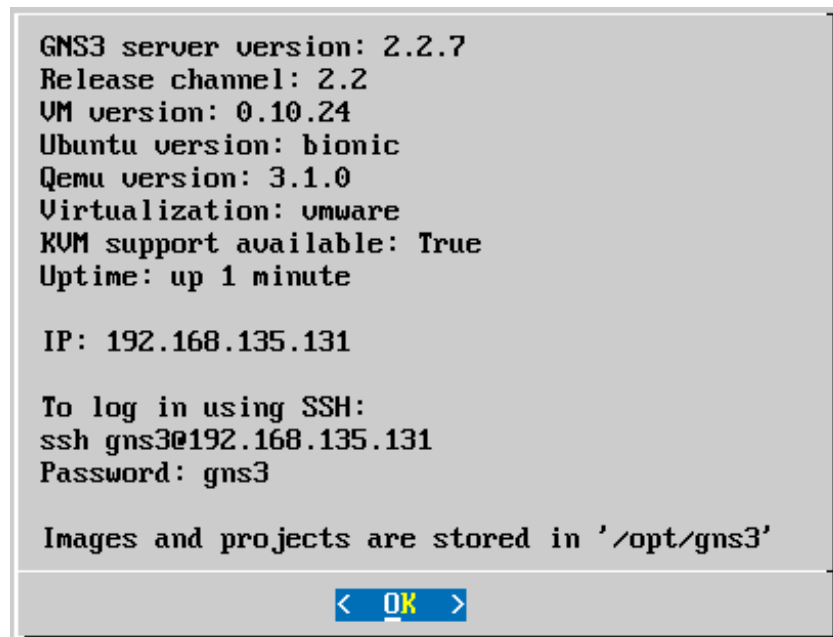


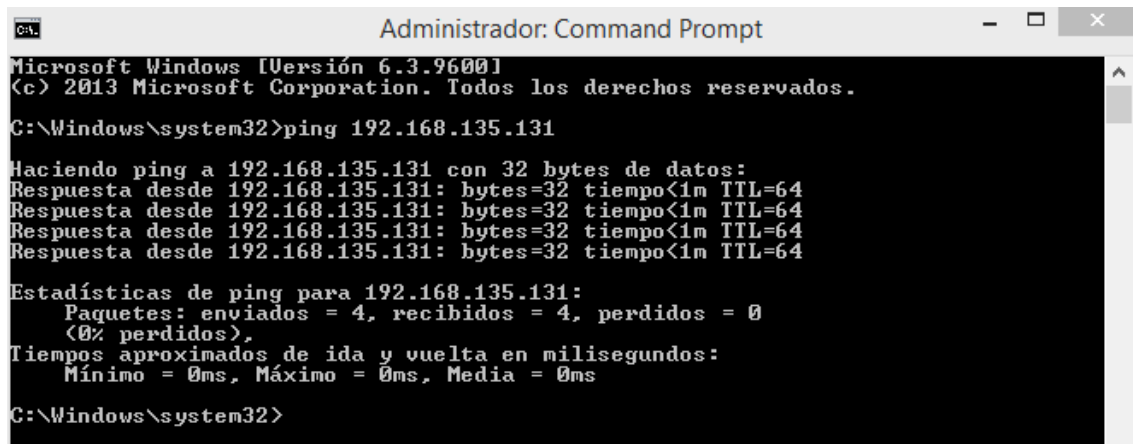
Figura 24. Asignación de IP. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

La IP que se le asigna a GNS3 es referente a un adaptador de red virtual que se crea a la hora de subir el ISO a VMware esto se puede observar con el comando `ncpa.cpl` desde el terminal mostrando los adaptadores de red.



Figura 25. Adaptador de red virtual. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Se deberá comprobar conectividad con la IP que GNS3 entrega a fin de poder ingresar al modo gráfico y replicar el escenario propuesto.



```

Administrador: Command Prompt
Microsoft Windows [Versión 6.3.9600]
(c) 2013 Microsoft Corporation. Todos los derechos reservados.
C:\Windows\system32>ping 192.168.135.131

Haciendo ping a 192.168.135.131 con 32 bytes de datos:
Respuesta desde 192.168.135.131: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.135.131: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.135.131: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.135.131: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.135.131:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Windows\system32>
  
```

Figura 26. CMD. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Una vez exitosa la conexión se podrá acceder al entorno de GNS3 desde su ejecutable.

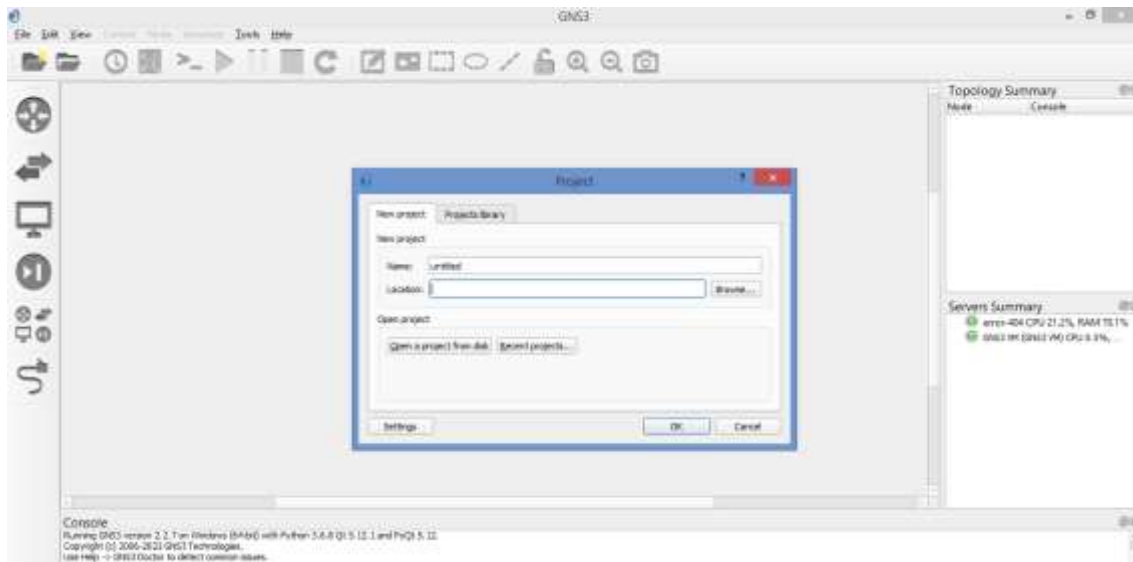


Figura 27. Ejecutable GNS3. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

El siguiente paso será crear un escenario o laboratorio totalmente nuevo que permita diseñar la topología de red antes mencionada para ello en New Project se deberá asignar un nombre al esquema a realizar y colocar la ruta donde se tiene pensado guardar y luego dar Ok o aceptar.

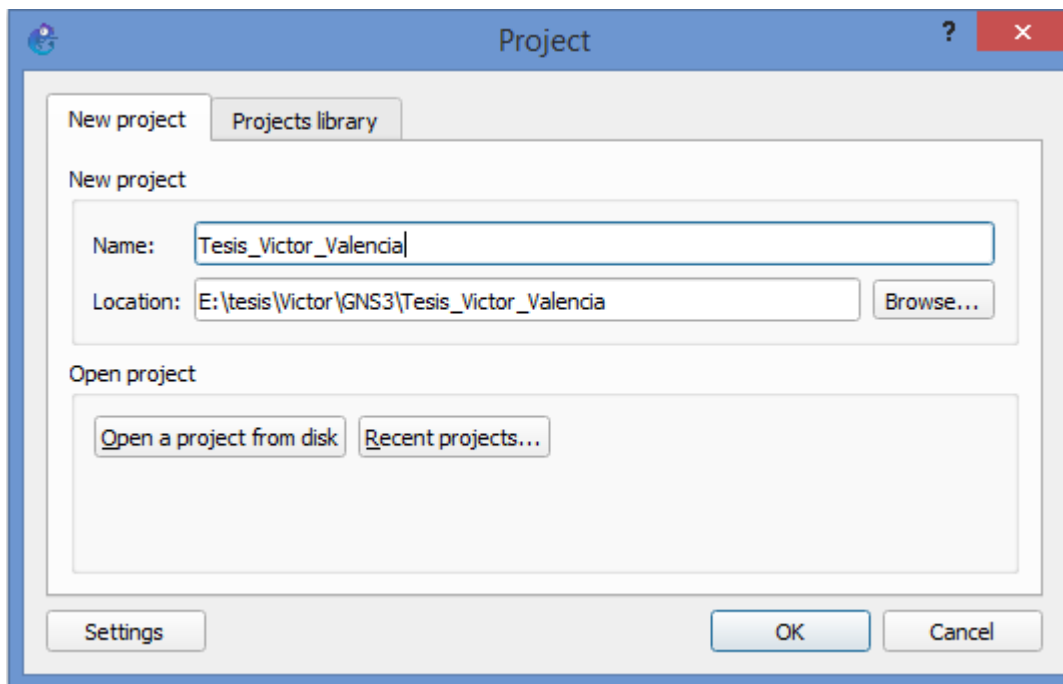


Figura 28. Creación del proyecto. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Una vez se haya creado el archivo se tendrá el escenario para realizar las pruebas respectivas que permitan validar el funcionamiento correcto del diseño propuesto.

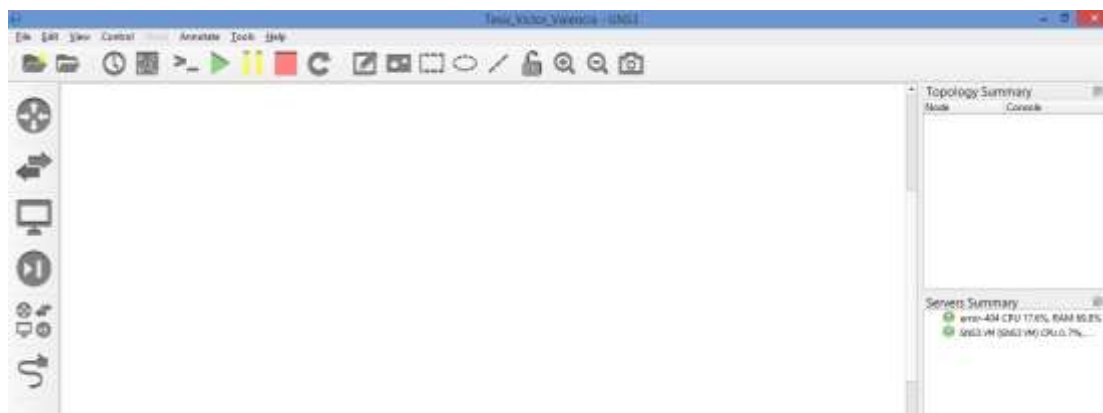


Figura 29. Escenario de pruebas. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Para realizar el diseño de red propuesto es necesario determinar las imágenes ISO a utilizar permitiendo usar el software de un equipo real de forma simulada logrando así tener un esquema lo más realista posible a tal punto de llevarlo a la práctica y funcione como muchas veces se hace.

Al realizar estos tipos de configuraciones en emuladores de red como GNS3 lo que se ahorra es una gran cantidad de dinero en cuanto a configuración en sitio e incluso reducción de adquisición de hardware donde ahora todo puede ser desplegado desde un equipo anfitrión o host de manera rápida y sencilla.

Para el escenario simulado se pretende hacer uso de los siguientes ISOs:

- Router 3745 permitiendo realizar todas las funciones de cualquier modelo de router en cisco ya que el sistema operativo es el mismo en cuanto a configuración.
- Un switch IOSv2 que en un entorno real es igual o funciona como cualquier switch cisco 2960 o 9200 e incluso 9300 de la familia Catalyst
- Equipos finales (Servidores, PC) ya sea emulados pero debido al alto consumo de ram se pretende hacer uso de equipos más simples pero con las funcionalidades necesarias para comprobar el funcionamiento de la red

Una vez claro los equipos a utilizar se procede a armar la topología en base al escenario propuesto en la sección anterior.

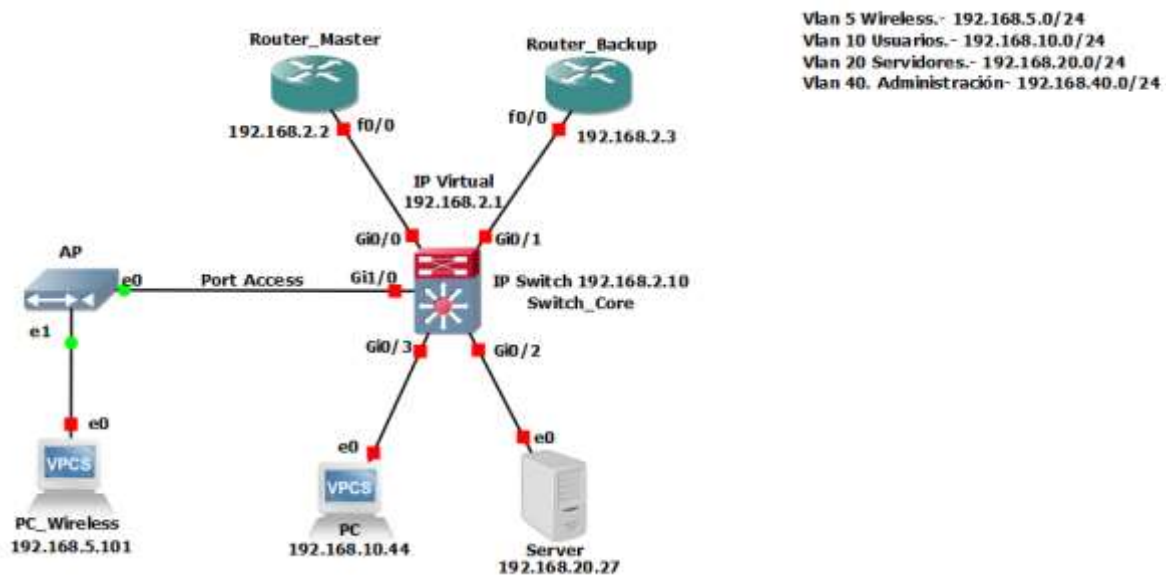


Figura 30. Topología Base. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Para proceder con la configuración es necesario que todos los equipos estén encendidos permitiendo tener una gestión en la configuración por lo que es necesario seleccionarlos y de manera general darles a todos up tal como se presenta a continuación:

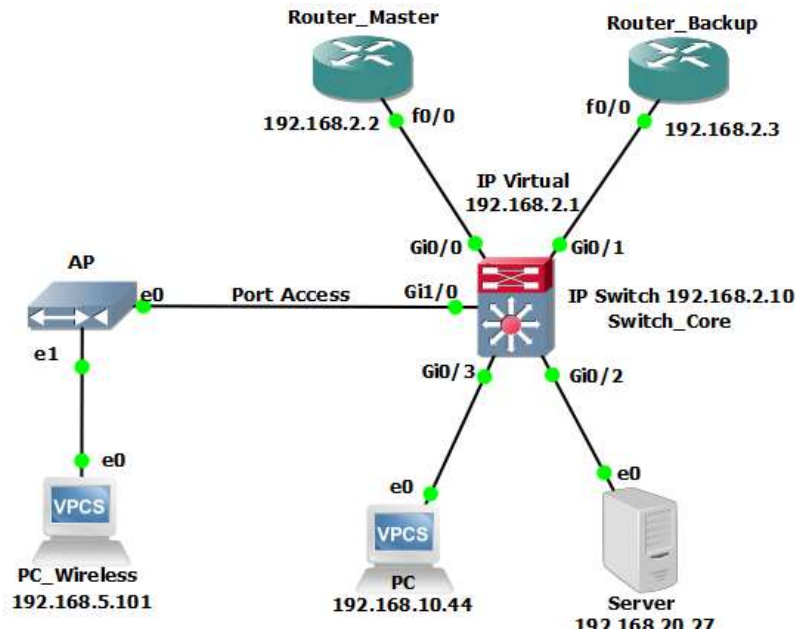


Figura 31. Funcionamiento de Equipos. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

3.13 Configuración de IPs en equipos finales

Para el proceso de configuración se procede en primer lugar a configurar cada uno de los equipos finales esto con el fin de tener una mejor gestión para ello solo se debe dar sobre el equipo doble clic y configurarlo según el segmento de red que corresponda para este caso se configurará para el PC.

```

PC
Welcome to Virtual PC Simulator, version 0.8.2
Dedicated to Belling.
Build time: Apr 18 2019 02:47:28
Copyright (c) 2007-2014, Paul Heng (mhreshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file.

PC> ip 192.168.10.44 255.255.255.0 192.168.10.1
Checking for duplicate address...
PC> 192.168.10.44 255.255.255.0 gateway 192.168.10.1
PC> save
Saving startup configuration to startup.vpc
Done
PC> show ip
NAME      : PC[1]
IP/PAUSE  : 192.168.10.44/34
GATEWAY   : 192.168.10.1
MAC       : 00:1B:7D:40:00:00
PORT      : 10011
HOST/PORT : 127.0.0.1:10011
CPU       : 1200
  
```

Figura 32. Configuración de IPs. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Cabe mencionar que el default Gateway o puerta de enlace de las diferentes vlans será la primera dirección útil de cada segmento asignado que posteriormente será configurado en el switch core. Otro punto que indicar es que el proceso para los demás equipos es repetitivo por lo que por razones obvias se omitirá el resto de las configuraciones realizadas en el demás host. Así mismo hay que indicar que el DNS será configurado a medida que se avance y se configure la salida a Internet.

3.14 Configuración del switch core

Para el proceso de switch se deberá realizar configuraciones adicionales que permitan una correcta configuración permitiendo así que en primer lugar la red no sea plana con las vlans creadas. Por lo que se procede a continuación a crear las diferentes vlans en el switch core a fin de segmentar el tráfico de la red para SANFERSYSTEMS S.A

```
Switch>ena
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 5
Switch(config-vlan)#name wireless
Switch(config-vlan)#vlan 10
Switch(config-vlan)#name usuarios
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name servicores
Switch(config-vlan)#vlan 40
Switch(config-vlan)#name administraciC3n
Switch(config-vlan)#name administracion
Switch(config-vlan)#
```

Figura 33. Creación de Vlans. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Para validar que las vlans han sido creadas de forma correcta en el equipo se utilizará el comando show vlan brief a fin de validar la configuración actual.

```
Switch(config)#do show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Gi0/0, Gi0/1, Gi0/2, Gi0/3
                    Gi1/0, Gi1/1, Gi1/2, Gi1/3
                    Gi2/0, Gi2/1, Gi2/2, Gi2/3
                    Gi3/0, Gi3/1, Gi3/2, Gi3/3
5    wireless              active
10   usuarios              active
20   servicores            active
40   administracion        active
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default       act/unsup
1005 trnet-default         act/unsup
Switch(config)#
```

Figura 34. Validación de Vlans. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Como siguiente punto es necesario asignar los puertos de los equipos finales a las diferentes vlans creadas a fin de tener correcta segmentación tal como se presenta a continuación.

```
Switch(config)#interface gi
Switch(config)#interface gigabitEthernet 1/0
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 5
Switch(config-if)#interface gi0/3
Switch(config-if)#swich mode acc
Switch(config-if)#switch mode acc
Switch(config-if)#switchport access vlan 10
Switch(config-if)#interface gi0/2
Switch(config-if)#switch mode acc
Switch(config-if)#switchport access vlan 20
Switch(config-if)#
```

Figura 35. Asignación de puertos. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

En la imagen se observa que en primer lugar se accede al puerto al que se quiere configurar y se aplican dos comandos el primero es el comando switchport mode access indicando que ese puerto ahora en adelante será solamente de acceso y el comando switchport access vlan x donde x significa la vlan a la que pertenecerá ese puerto de ahora en adelante.

Para mejor visualización se presenta el comando show vlan brief para ver los puertos asignados a las diferentes vlans.

```
Switch(config-if)#do show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Gi0/0, Gi0/1, Gi1/1, Gi1/2 Gi1/3, Gi2/0, Gi2/1, Gi2/2 Gi2/3, Gi3/0, Gi3/1, Gi3/2 Gi3/3
5	wireless	active	Gi1/0
10	usuarios	active	Gi0/3
20	servidores	active	Gi0/2
40	administracion	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

```
Switch(config-if)#
```

Figura 36. Visualización de puertos. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Otro punto importante es que ahora se debe configurar las SVI que funcionarán como default Gateway de los diferentes equipos previamente configurados para ello es necesario en cada interface vlan asignar la dirección IP que será la puerta de enlace de los dispositivos finales.

```
Switch(config-if)#ip address 192.168.5.1 255.255.255.0
Switch(config-if)#interface vlan 10
Switch(config-if)#
*Feb 17 08:33:29.766: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to down
Switch(config-if)#ip address 192.168.10.1 255.255.255.0
Switch(config-if)#interface vlan 20
Switch(config-if)#interface vlan 10
*Feb 17 08:33:47.853: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to down
Switch(config-if)#ip address 192.168.20.1 255.255.255.0
```

Figura 37. Configuración de SVI. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Para tener una mejor perspectiva de visualización se utilizará el comando show ip interface brief que detalla las direcciones IP configurada en cada una de las SVI mencionadas.

```
Switch(config-vlan)#do show ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 unassigned YES unset up up
GigabitEthernet0/1 unassigned YES unset up up
GigabitEthernet0/2 unassigned YES unset up up
GigabitEthernet0/3 unassigned YES unset up up
GigabitEthernet1/0 unassigned YES unset up up
GigabitEthernet1/1 unassigned YES unset down down
GigabitEthernet1/2 unassigned YES unset down down
GigabitEthernet1/3 unassigned YES unset down down
GigabitEthernet2/0 unassigned YES unset down down
GigabitEthernet2/1 unassigned YES unset down down
GigabitEthernet2/2 unassigned YES unset down down
GigabitEthernet2/3 unassigned YES unset down down
GigabitEthernet3/0 unassigned YES unset down down
GigabitEthernet3/1 unassigned YES unset down down
GigabitEthernet3/2 unassigned YES unset down down
GigabitEthernet3/3 unassigned YES unset down down
Vlan5 192.168.5.1 YES manual up up
Vlan10 192.168.10.1 YES manual up up
Vlan20 192.168.20.1 YES manual up up
Vlan40 192.168.40.1 YES manual down down
```

Figura 38. Direcciones IP. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Ahora para permitir que diferentes vlans se comuniquen a nivel de capa 3 en el switch es necesario habilitar el comando ip routing con ello equipos que se encuentren en vlans diferentes podrán verse entre sí.

```
Switch(config)#ip routing
Switch(config)#
```

Figura 39. Comando ip routing. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Ahora si comprobamos conectividad desde el PC hasta el servidor se debería tener comunicación entre ellos.

```
PC> ping 192.168.20.27
84 bytes from 192.168.20.27 icmp_seq=1 ttl=63 time=158.721 ms
84 bytes from 192.168.20.27 icmp_seq=2 ttl=63 time=37.061 ms
84 bytes from 192.168.20.27 icmp_seq=3 ttl=63 time=27.502 ms
84 bytes from 192.168.20.27 icmp_seq=4 ttl=63 time=35.324 ms
84 bytes from 192.168.20.27 icmp_seq=5 ttl=63 time=34.821 ms
```

Figura 40. Conectividad. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

De igual forma si probamos desde el servidor al equipo con la dirección ip 192.168.5.101

```
Server> ping 192.168.5.101
84 bytes from 192.168.5.101 icmp_seq=1 ttl=63 time=90.185 ms
84 bytes from 192.168.5.101 icmp_seq=2 ttl=63 time=15.623 ms
84 bytes from 192.168.5.101 icmp_seq=3 ttl=63 time=30.747 ms
84 bytes from 192.168.5.101 icmp_seq=4 ttl=63 time=23.863 ms
84 bytes from 192.168.5.101 icmp_seq=5 ttl=63 time=24.466 ms
```

Figura 41. Pruebas en el servidor. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Una vez configurado de forma correcta la red interna se deberá configurar la salida hacia los equipos proporcionados por el ISP en el que para ello se tendrá una nueva vlan que será la 100 y permitirá comunicar con los routers.

```
Switch(config-if)#vlan 100
Switch(config-vlan)#interface vlan 100
Switch(config-if)#ip add 192.168.2.10 255.255.255.0
Switch(config-if)#interface range gi0/0-1
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 100
Switch(config-if-range)#
```

Figura 42. Configuración de equipos. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Por último se deberá configurar el default Gateway para que todo tráfico desconocido vaya hacia la IP Virtual más adelante a configurarse del mismo modo definir a la IP virtual como la puerta de enlace de switch.

```
Switch(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.1
Switch(config)#ip default-gateway 192.168.2.1
```

Figura 43. Configuración Gateway. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

3.15 Configuración de routers para redundancia de gateway

Para el proceso de configuración de Gateway es necesario en cada router establecer una serie de parámetros o procesos que permitan identificar qué equipo funcionará como master y backup adicional a ello se deberá establecer una dirección IP que permita mantener la configuración con los equipos de la red interna.

Por lo que para ello se procederá a configurar el router uno y una vez realizado el proceso se repetirán los mismos pasos para el router 2 o el equipo de backup. Es necesario que el equipo a configurar cuente con un direccionamiento IP con el fin de poder enrutar hacia internet tal como se muestra a continuación

```
Router_Master(config)#interface fa0/0
Router_Master(config-if)#no shut
Router_Master(config-if)#
*Mar 1 00:14:42.459: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 00:14:43.459: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router_Master(config-if)#ip address 192.168.2.2 255.255.255.0
Router_Master(config-if)#
```

Figura 44. Configuración de router. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Como paso uno se procedió a encender la interfaz que se va a utilizar y que está conectada al switch core en este caso la interface Fa0/0 una vez realizado ese paso automáticamente la interfaz cambia de un modo disable o shutdown a un modo no shutdown o encendido en el que se indica que va a poder ser usada para enrutar tráfico entre diferentes equipos.

3.16 Configuración de VRRP en Routers para redundancia de Gateway

Para activar el protocolo VRRP y hacer que exista redundancia en Gateway es necesario realizar una serie de pasos previos los cuales fueron detallados a detalle en el capítulo 2 por lo que a continuación se procede a realizar los pasos necesarios para permitir una comunicación redundante entre diferentes Gateway permitiendo así que SANFERSYSTEMS S.A tenga mayor disponibilidad en su red además de un proceso automatizado en cuanto al cambio de puertas de enlace y no de forma manual como se ha venido hasta ahora realizando.

Paso 1.- Indicar la dirección IP y el grupo al que pertenecerá el VRRP

En este punto se busca determinar cuál es la dirección IP y el grupo al que el router pertenecerá y podrá realizar redundancia por lo que es necesario desde el IOS ejecutar los siguientes comandos:

- Vrrp number-priority ip x.x.x.x
 - Define al id de grupo que pertenecerá VRRP además de la dirección de IP virtual a utilizar que será la IP que permita salida a Internet a los equipos que deseen salir a Internet por medio de una ruta por defecto previamente configurada.

```
Router_Master(config-if)#vrrp 100 ip 192.168.2.1
Router_Master(config-if)#
*Mar 1 00:23:36.547: %VRRP-6-STATECHANGE: Fa0/0 Grp 100 state Init -> Backup
```

Figura 45. Router master. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Como se observa automáticamente VRRP le indica al router que función va a realizar donde de querer que sea el de mayor prioridad puede ser modificado mediante el comando

- Vrrp number-priority priority #

Se define en base a la prioridad si el equipo será master o backup

```
Router_Master(config-if)#vrrp 100 priority 200
```

Figura 46. VRRP. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Se puede visualizar con mayores detalles los ajustes generados mediante el comando show VRRP.

```
Router_Master#show vrrp
FastEthernet0/0 - Group 100
  State is Master
  Virtual IP address is 192.168.2.1
  Virtual MAC address is 0000.5e00.0164
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 200
  Master Router is 192.168.2.2 (local), priority is 200
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.218 sec
```

Figura 47. Comando show VRRP. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Como se observa en la gráfica se indica el estado del equipo el cual está definido como master, así mismo se identifica la IP Virtual que es la previamente asignada 192.168.2.1 así como la dirección MAC Virtual, por último se puede observar cual es la dirección IP que el equipo posee y su prioridad de 200.

El mismo proceso debe ser realizado en el otro equipo a fin de permitir una correcta configuración.

```
Router_Backup(config)#interface fa0/0
Router_Backup(config-if)#no shut
Router_Backup(config-if)#
*Mar 1 00:21:40.451: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 00:21:41.451: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router_Backup(config-if)#ip add 192.168.2.3 255.255.255.0
Router_Backup(config-if)#
```

Figura 48. Configuración router backup. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Visualización de la configuración del equipo en modo backup por el protocolo VRRP

```
Router_Backup(config-if)#vrrp 100 ip 192.168.2.1
Router_Backup(config-if)#
*Mar 1 00:22:26.223: %VRRP-6-STATECHANGE: Fa0/0 Grp 100 state Init -> Backup
Router_Backup(config-if)#vrrp 100 priority 100
Router_Backup(config-if)#
```

Figura 49. Modo backup por el protocolo VRRP. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Para mayor detalle se procede a ejecutar el comando show VRRP en el equipo de backup para ver de qué manera quedo configurado el equipo.

```
Router_Backup(config-if)#do show vrrp
FastEthernet0/0 - Group 100
  State is Backup
  Virtual IP address is 192.168.2.1
  Virtual MAC address is 0000.5e00.0164
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 100
  Master Router is 192.168.2.2, priority is 200
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.609 sec (expires in 2.481 sec)
```

Figura 50. Validación de configuración. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Un punto importante que mencionar es que se puede obtener un breve resumen de la configuración realizada permitiendo tener mejor noción de lo realizado a través del comando show VRRP brief.

```
Router_Master#show vrrp brief
Interface      Grp Pri Time  Own Pre State  Master addr  Group addr
Fa0/0          100 200 3218      Y Master 192.168.2.2 192.168.2.1
Router_Master#
```

Figura 51. Resumen de configuración. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Se indico anteriormente que al realizar este proceso es necesario tener rutas de retorno que vengán hacia la red interna debido a que si probamos la configuración como están ahora no funcionarán tal como se muestra a continuación:

```
PC> ping 192.168.2.1
192.168.2.1 icmp_seq=1 timeout
192.168.2.1 icmp_seq=2 timeout
```

Figura 52. Rutas de retorno. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Si se indaga un poco más en el problema se puede dar cuenta que está en que el switch de core no sabe cómo enviar los paquetes de regreso al host final ya que los routers no tienen rutas configuradas de forma estática siendo un gran problema.

```
PC> trace 192.168.2.1
trace to 192.168.2.1, 8 hops max, press Ctrl+C to stop
 1  192.168.10.1    22.449 ms  23.944 ms  20.541 ms
 2      * * *
 3      * * *
 4      * * *
```

Figura 53. Problemas de paquetes. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Para ello es necesario activar las rutas en ambos routers permitiendo así tener una respuesta de regreso tal como se presenta en la imagen que antecede:

```
Router_Master#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router_Master(config)#ip route 192.168.5.0 255.255.255.0 192.168.2.10
Router_Master(config)#ip route 192.168.10.0 255.255.255.0 192.168.2.10
Router_Master(config)#ip route 192.168.20.0 255.255.255.0 192.168.2.10
Router_Master(config)#ip route 192.168.40.0 255.255.255.0 192.168.2.10
Router_Master(config)#
```

Figura 54. Activación de rutas. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

El mismo proceso debe realizarse en el router de backup

```
Router_Backup(config)#ip route 192.168.5.0 255.255.255.0 192.168.2.10
Router_Backup(config)#ip route 192.168.10.0 255.255.255.0 192.168.2.10
Router_Backup(config)#ip route 192.168.20.0 255.255.255.0 192.168.2.10
Router_Backup(config)#ip route 192.168.40.0 255.255.255.0 192.168.2.10
Router_Backup(config)#
```

Figura 55. Activación de rutas en router BK. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Por lo que si se vuelve a realizar un ping o trace a la IP virtual configurada se obtiene que está funcionando sin problema.

```
PC> ping 192.168.2.1
84 bytes from 192.168.2.1 icmp_seq=1 ttl=254 time=29.527 ms
84 bytes from 192.168.2.1 icmp_seq=2 ttl=254 time=29.729 ms
84 bytes from 192.168.2.1 icmp_seq=3 ttl=254 time=30.620 ms
84 bytes from 192.168.2.1 icmp_seq=4 ttl=254 time=37.411 ms
84 bytes from 192.168.2.1 icmp_seq=5 ttl=254 time=22.300 ms
PC> █
```

Figura 56. Trace a IP Virtual. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Ping realizado desde el lado del servidor

```
ping 192.168.2.1
192.168.2.1 icmp_seq=1 timeout
84 bytes from 192.168.2.1 icmp_seq=2 ttl=254 time=28.910 ms
84 bytes from 192.168.2.1 icmp_seq=3 ttl=254 time=31.698 ms
84 bytes from 192.168.2.1 icmp_seq=4 ttl=254 time=48.580 ms
84 bytes from 192.168.2.1 icmp_seq=5 ttl=254 time=34.102 ms
█
```

Figura 57. Ping al servidor. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Ping del lado del equipo 5.101

```
PC_Wireless> ping 192.168.2.1
192.168.2.1 icmp_seq=1 timeout
84 bytes from 192.168.2.1 icmp_seq=2 ttl=254 time=29.516 ms
84 bytes from 192.168.2.1 icmp_seq=3 ttl=254 time=61.771 ms
84 bytes from 192.168.2.1 icmp_seq=4 ttl=254 time=64.218 ms
84 bytes from 192.168.2.1 icmp_seq=5 ttl=254 time=41.888 ms
PC_Wireless> █
```

Figura 58. Ping del lado del equipo 5.101. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

3.17 Evaluación del entorno simulado

Una vez levantado el protocolo VRRP en los equipos con su respectiva IP virtual es necesario comprobar que el esquema de alta disponibilidad en puertas de enlace funcione sin ningún inconveniente.

Para la comprobación del entorno simulado se optará por apagar el equipo Master a fin de comprobar que la comunicación sigue estando vigente y no haya afectaciones en la red de la

empresa SANFERSYSTEMS S.A a fin de validar los cambios automáticos en caso de fallo y con ello la operabilidad del protocolo VRRP propuesto para la entidad. A continuación se observa que el equipo considerado como Master es pausado para ver la respuesta de VRRP ante el equipo mencionado.

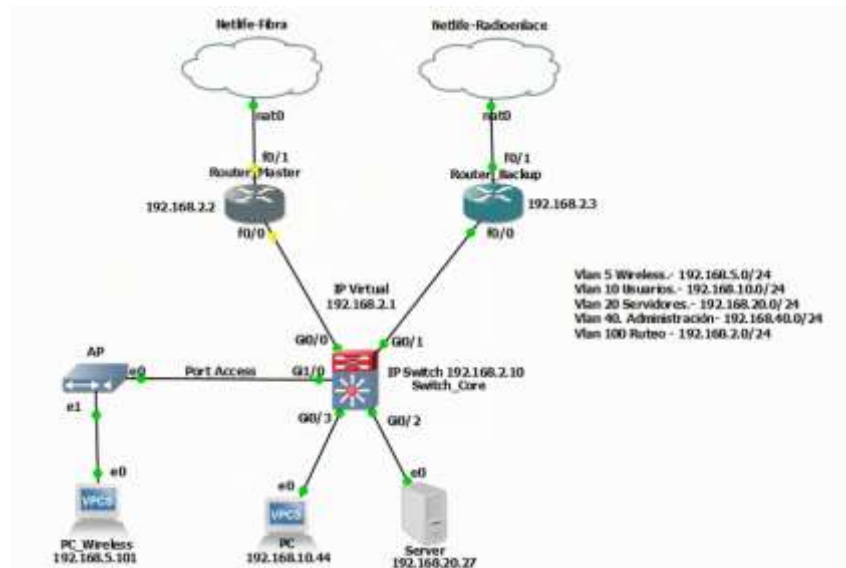


Figura 59. Equipo Master. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Esto ocasiona que por un segundo la red busque al equipo backup siempre y cuando exista y pasarle todos los roles que el equipo Master manejaba a fin de evitar fallas prolongadas para ello con el protocolo ICMP al recibir los Echo Reply se observa que existe una caída de paquetes mínima debido a que el equipo Master fallo pero se busca un reemplazo de forma inmediata sin necesidad de realizarlo de manera manual como se ejecutaba anteriormente en la empresa SANFERSYSTEMS S.A.

```
PC_Wireless> [5~
Bad command: "[5~". Use ? for help.

PC_Wireless> ping 192.168.2.1 -t
84 bytes from 192.168.2.1 icmp_seq=1 ttl=254 time=70.518 ms
84 bytes from 192.168.2.1 icmp_seq=2 ttl=254 time=42.339 ms
84 bytes from 192.168.2.1 icmp_seq=3 ttl=254 time=71.932 ms
84 bytes from 192.168.2.1 icmp_seq=4 ttl=254 time=25.142 ms
84 bytes from 192.168.2.1 icmp_seq=5 ttl=254 time=65.294 ms
84 bytes from 192.168.2.1 icmp_seq=6 ttl=254 time=26.854 ms
84 bytes from 192.168.2.1 icmp_seq=7 ttl=254 time=98.997 ms
84 bytes from 192.168.2.1 icmp_seq=8 ttl=254 time=50.725 ms
84 bytes from 192.168.2.1 icmp_seq=9 ttl=254 time=46.543 ms
84 bytes from 192.168.2.1 icmp_seq=10 ttl=254 time=63.088 ms
192.168.2.1 icmp_seq=11 timeout
192.168.2.1 icmp_seq=12 timeout
192.168.2.1 icmp_seq=13 timeout
84 bytes from 192.168.2.1 icmp_seq=14 ttl=254 time=83.870 ms
84 bytes from 192.168.2.1 icmp_seq=15 ttl=254 time=40.979 ms
```

Figura 60. Caída de paquetes. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

El resultado presentado permite determinar la rapidez con la que VRRP puede responder a incidentes permitiendo activar el equipo en Slave de forma casi inmediata siendo no detectado los usuarios.

Otro punto por considerar es que al equipo que actualmente tomo las funciones que el master tenía de forma interna el protocolo VRRP lo convierte en el equipo designado es decir será el Master hasta que un equipo con prioridad más alta sea ingresado en la red. Para ver los detalles indicados es necesario ejecutar un comando previamente ejecutado **show VRRP**.

```
Router_Backup(config)#do show vrrp
FastEthernet0/0 - Group 100
"Este es el slave"
  State is Master
  Virtual IP address is 192.168.2.1
  Virtual MAC address is 0000.5e00.0164
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 100
  Master Router is 192.168.2.3 (local), priority is 100
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.609 sec
Router_Backup(config)#
```

Al ejecutar el comando show VRRP se observa que los parámetros en cuanto al equipo Master local cambiaron siendo el equipo con la IP 192.168.2.3 el nuevo equipo con el Rol de Master por otra parte al haber una falla en algunos de estos equipos no significa que la IP virtual se vea afectada por lo que seguirá operando sin ningún problema y con ello establecerá la comunicación desde la red interna hacia Internet y viceversa.

Por otra parte al equipo Master al recuperarse automáticamente negociará con el equipo que es de backup o con prioridad más baja a fin de solicitar los roles que se le fueron asignados y con ello mantener la comunicación sin existir caídas del sistema y operando la red sin problemas.

Cabe recalcar que el proceso realizado se debe a los tiempos de hello time gestionados debido a cómo funciona VRRP de forma interna acorde a los definidos por la IEEE siendo una métrica determinante a la hora de transmitir roles entre equipos.

Es importante indicar que VRRP al hacer cambios de roles reduce considerablemente la latencia debido a que su cambio se da en menos de un segundo siendo factible para las comunicaciones que son altamente críticas.

3.18 Análisis de tráfico mediante Wireshark

Para el presente trabajo es necesario definir el tráfico que es generado por la red propuesta para la empresa SANFERSYSTEMS S.A por lo que es necesario hacer uso de Wireshark a fin de tener de forma más estructurada y clara los datos a fin de poder ser analizados y saber de qué manera operan en la red es decir de que punto inicien o terminen.

Como primer punto es necesario mencionar que Wireshark obtiene datos en tiempo real de la comunicación gestionada según los equipos que se estén comunicando en donde el siguiente escenario recopila información general de como un equipo el 192.168.5.101 envía solicitudes icmp al equipo master y en base a ello se procede analizar el total de datos recibidos así como los protocolos aplicados dentro de la red propuesta.

No.	Source	Time	Destination	Protocol	Length	Info
290	0c:d1:e6:9b:80:64	87.787153	Spanning-tree (for...	STP	68	IST. Root = 32768/100/0c:d1:e6:9b:80:64 Cost = 0 Port = 0x0001
291	192.168.2.2	88.331165	224.0.0.18	VRMP	60	Announcement (v2)
292	192.168.5.101	88.543313	192.168.2.1	ICMP	98	Echo (ping) request id=0x0e6d, seq=192/49152, ttl=63 (reply in 293)
293	192.168.2.1	88.547951	192.168.5.101	ICMP	98	Echo (ping) reply id=0x0e6d, seq=192/49152, ttl=255 (request in 292)
294	192.168.2.2	89.268786	224.0.0.18	VRMP	60	Announcement (v2)
295	192.168.5.101	89.681119	192.168.2.1	ICMP	98	Echo (ping) request id=0x0f6d, seq=193/49488, ttl=63 (reply in 296)
296	192.168.2.1	89.684499	192.168.5.101	ICMP	98	Echo (ping) reply id=0x0f6d, seq=193/49488, ttl=255 (request in 295)
297	192.168.2.2	90.256595	224.0.0.18	VRMP	60	Announcement (v2)
298	0c:d1:e6:9b:80:64	90.425335	Spanning-tree (for...	STP	68	IST. Root = 32768/100/0c:d1:e6:9b:80:64 Cost = 0 Port = 0x0001
299	192.168.5.101	90.649153	192.168.2.1	ICMP	98	Echo (ping) request id=0x106d, seq=194/49664, ttl=63 (reply in 300)
300	192.168.2.1	90.653082	192.168.5.101	ICMP	98	Echo (ping) reply id=0x106d, seq=194/49664, ttl=255 (request in 299)

▶ Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
 ▶ Ethernet II, Src: 0c:d1:e6:9b:80:64 (0c:d1:e6:9b:80:64), Dst: IETF-VRMP-VRID_64 (00:00:5e:00:01:64)
 ▶ Internet Protocol Version 4, Src: 192.168.5.101, Dst: 192.168.2.1
 ▶ Internet Control Message Protocol

Figura 61. Análisis de tráfico. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

El tráfico analizado en por Wireshark se da de diferentes formas teniendo entre ellas:

- El Source que corresponde a la dirección IP del equipo que ha realizado la comunicación
- Time el tiempo secuencial en el que se a estado realizando las peticiones por lo general no es una métrica importante
- Destination es decir el equipo que recibe la petición del source y así definir el tipo de comunicación que se está enviando entre los equipos
- El protocolo hace referencia al protocolo de comunicación o mecanismo establecido entre el emisor y receptor que define en la mayoría de las ocasiones que se está realizando.

- Info detalla a profundidad el tipo de mensaje enviado acorde al protocolo de comunicación utilizado en la red
- En la parte inferior se muestran las cabeceras utilizadas en base al protocolo TCP/IP en el que se define tanto las direcciones MAC, direccionamiento IP e incluso el protocolo aplicado.

Para determinar los protocolos que participan en la red de datos de SANFERSYSTEMS S.A se revisará a nivel de cabeceras a fin de identificar que es enviado y de qué manera a diferentes de la red anterior el escenario propuesto cumple con mayores características en cuanto a tiempos de respuesta, redundancia, escalabilidad permitiendo operar en un escenario más optimo, reduciendo las fallas producidas en los equipos.

3.19 Protocolo VRRP capturado en Wireshark

Como se mencionaba con WireShark se puede observar los protocolos que participan dentro de la comunicación de la red y con ello determinar la forma en la que operan donde a continuación se procede analizar los datos proporcionados y validar que se cumplan con los presentados a la hora de realizar la simulación.

Como se observa en la figura que antecede se observan 4 campos que son determinados por Wireshark en el que el campo Frame es como viaja la trama en cuestión de bits por algún medio ya sea cableado o guiado.

De la misma manera el entramado ethernet define un Frame que hace referencia a VRRP indicando que el protocolo es aplicado de forma correcta además de mencionar cuales son las tramas que participan de la comunicación siendo uno de ellos la dirección MAC definida por VRRP.

Por otra parte, en el campo Internet Protocol se define que dirección IP de origen y destino participa en la comunicación donde se puede observar la dirección IP 224.0.0.18 definida en el protocolo VRRP por la IEEE. Por último se observa el protocolo de puertas de enlace redundante siendo utilizado para la comunicación.

```

▶ Frame 407: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface -, id 0
▶ Ethernet II, Src: IETF-VRRP-VRID_64 (00:00:5e:00:01:64), Dst: IPv4mcast_12 (01:00:5e:00:00:12)
▶ Internet Protocol Version 4, Src: 192.168.2.2, Dst: 224.0.0.18
▶ Virtual Router Redundancy Protocol

```

Figura 62. Puertas de enlace. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

Para el protocolo VRRP se observan campos muy importantes a la hora de mantener la comunicación y Wireshark presenta teniendo entre ellos:

- Version 2: Por defecto activada en la comunicación del protocolo VRRP debido a su seguridad
- Virtual ID: Hace referencia al número de grupo creado y en el que están vinculados los equipos que formarán de VRRP
- Prioridad: Indica ID del equipo al que se le estableció la comunicación donde entre mayor sea la prioridad ese equipo es definido como Master
- Authentication Type para cifrar la comunicación a la hora de establecerse la comunicación entre el protocolo
- Checksum el comprobador de error de tramas donde de haber falla la descartará caso contrario permitirá el paso y envío hacia el equipo destino que está establecido en la comunicación.
- IP address hace referencia a la dirección IP Virtual usada por los routers que forman parte del VRRP a fin de tenerla como la principal para la transmisión de información

```
Virtual Router Redundancy Protocol
  ▸ Version 2, Packet type 1 (Advertisement)
    Virtual Rtr ID: 100
    Priority: 200 (Non-default backup priority)
    Addr Count: 1
    Auth Type: No Authentication (0)
    Adver Int: 1
    Checksum: 0x53ef [correct]
    [Checksum Status: Good]
    IP Address: 192.168.2.1
```

Figura 63. Campos del protocolo VRRP. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

3.20 Protocolo ICMP capturado en Wireshark

Así mismo es necesario mencionar que otro protocolo capturado para el proceso de comunicación de equipos es el ICMP encargado de enviar mensajes de tipo ping para validar que un equipo este operativo y funcionando.

Dentro de los parámetros capturados por Wireshark del protocolo ICMP se debe considerar los más importantes siendo ellos.

- Versión hace referencia si se está usando el protocolo versión 4 o 6
- Servicios diferenciados encargados de proporcionar calidad de servicio mediante 6 bits de DSCP y 2 de ECN basados en la colisión de datos
- Time to Live es el tiempo de vida que un paquete tiene para estar en la red y llegar a un destino en caso de llegar a cero se considera inalcanzable. Con TTL se evita los bucles de capa 3 en la red.
- El tipo de protocolo utilizado para este trabajo ICMP
- Header Checksum indica si la trama a tenido problemas en cuanto a interferencias o modificaciones

```
Internet Protocol Version 4, Src: 192.168.5.101, Dst: 192.168.2.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x6d61 (28001)
    ▸ Flags: 0x00
      ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 63
    Protocol: ICMP (1)
    Header Checksum: 0x8591 [validation disabled]
    [Header checksum status: Unverified]
```

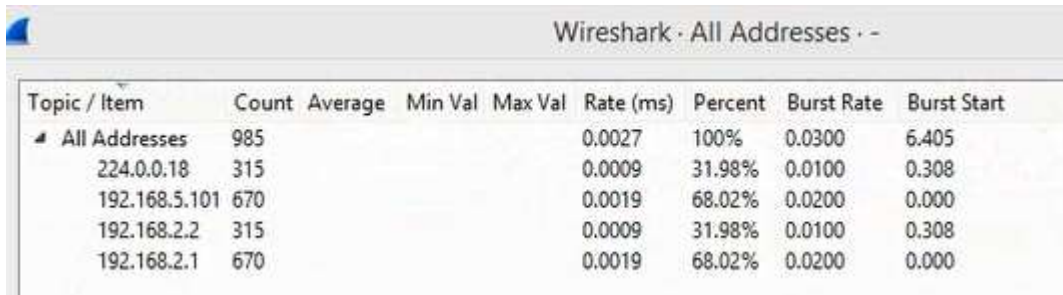
Figura 64. Protocolo ICMP capturado en Wireshark. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

3.21 Gráficas de flujo

Es necesario identificar de qué manera se establece el tráfico a la hora de realizar un ping hacia un punto específico por lo WireShark permite obtener el flujo de información en la red con el que se puede determinar de qué manera se está enviado los datos de forma más acertada, así mismo, definir los equipos que participan en la comunicación tanto en el origen como el destino.



Por otra parte en el escenario propuesto se puede identificar que equipos están participando de la comunicación así como un porcentaje total de participación teniendo mayor perspectiva de donde aplicar mayor hardenización o seguridad.

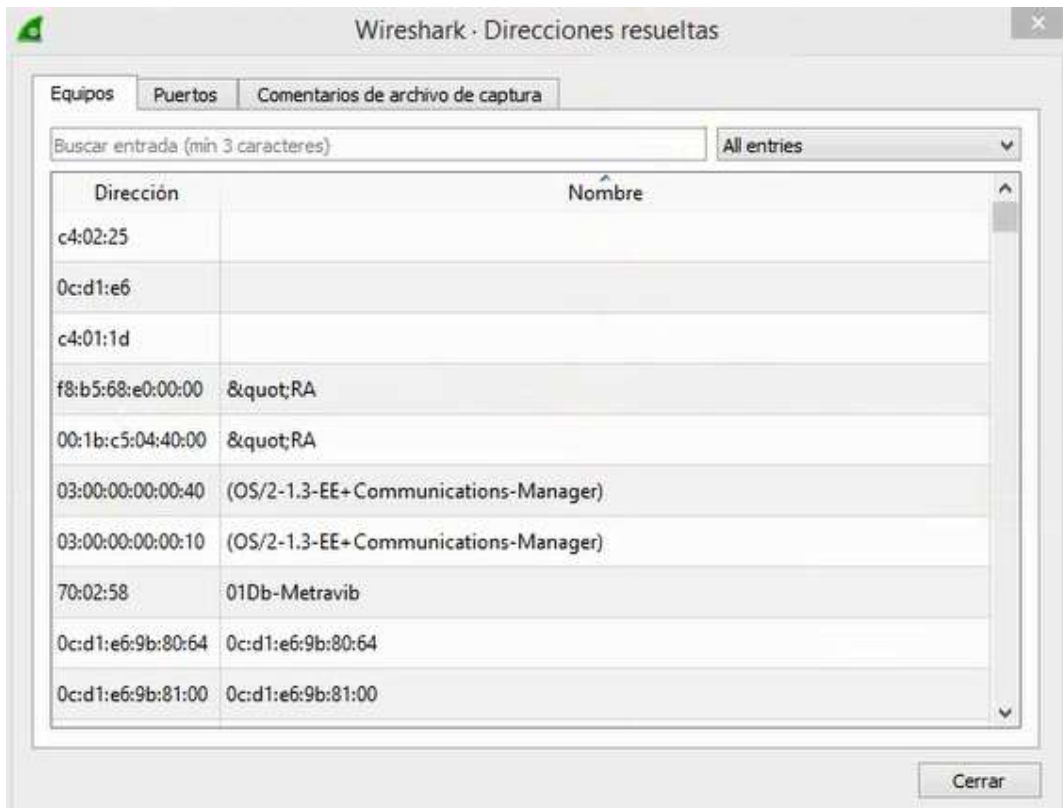


Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
All Addresses	985				0.0027	100%	0.0300	6.405
224.0.0.18	315				0.0009	31.98%	0.0100	0.308
192.168.5.101	670				0.0019	68.02%	0.0200	0.000
192.168.2.2	315				0.0009	31.98%	0.0100	0.308
192.168.2.1	670				0.0019	68.02%	0.0200	0.000

Figura 66. Identificación de equipos. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

3.22 Direcciones resueltas

Algo a mencionar es que al ejecutar es posible registrar todos los equipos que fueron procesados siendo separados por dirección del equipo y el nombre detectado.



Dirección	Nombre
c4:02:25	
0c:d1:e6	
c4:01:1d	
f8:b5:68:e0:00:00	"RA
00:1b:c5:04:40:00	"RA
03:00:00:00:00:40	(OS/2-1.3-EE+ Communications-Manager)
03:00:00:00:00:10	(OS/2-1.3-EE+ Communications-Manager)
70:02:58	01Db-Metravib
0c:d1:e6:9b:80:64	0c:d1:e6:9b:80:64
0c:d1:e6:9b:81:00	0c:d1:e6:9b:81:00

Figura 67. Direcciones resueltas. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

3.23 Gráficas de entrada y salida de datos en Wireshark

Por último, en el presente trabajo de investigación se puede visualizar el tráfico que ha sido enviado y analizado basado tanto en entrada y salida, cabe recalcar que el tráfico presentado va a variar acorde a que interfaces se está analizando es decir de manera separada o por un solo puerto que pase todos los datos.

Para el caso a presentarse el tráfico de entrada y salida tomado se basa a la conexión que existe entre el equipo master y el switch de capa 3 presentando el flujo de datos enviados en tiempo real que atraviesa la interface.

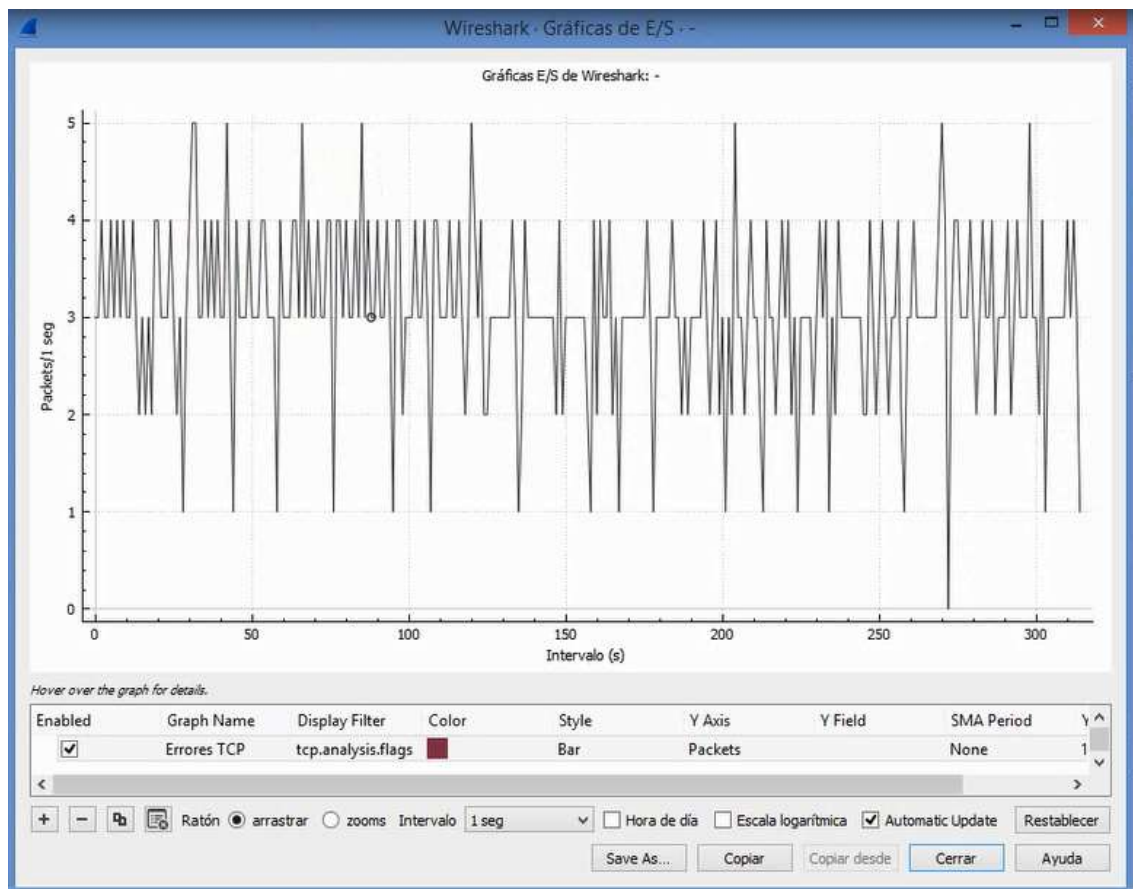


Figura 68. Gráficas de entrada y salida de datos en Wireshark. Información tomada por la investigación directa. Elaborado por Valencia Carpio Víctor Andrés

3.24 Conclusiones

- El protocolo VRRP demostró ser superior en cuanto a rendimiento y operabilidad con diferentes fabricantes siendo factible de implementar y gestionar

- Se determino que a través del protocolo VRRP se logra obtener mejoras en cuanto a rendimiento, delay, latencia e incluso despliegue
- VRRP a diferencia de los protocolos HSRP y GLBP permite desplegar un ambiente hasta de 8 equipos en un ID de grupo para formar master y esclavos logrando redundancia de red así como escalabilidad
- Los tiempos de respuestas proporcionados por el protocolo VRRP a la hora de haber afectaciones en algún equipo físico son casi inmediatos es decir no afecta a la gestión del servicio
- El analizador de tráfico Wireshark permitió identificar el tipo de tráfico que pasa por la red y determinar el flujo de datos
- Se comprobó que el simulador de red GNS3 es el más adecuado a la hora de realizar escenarios complejos que puedan ser replicados.

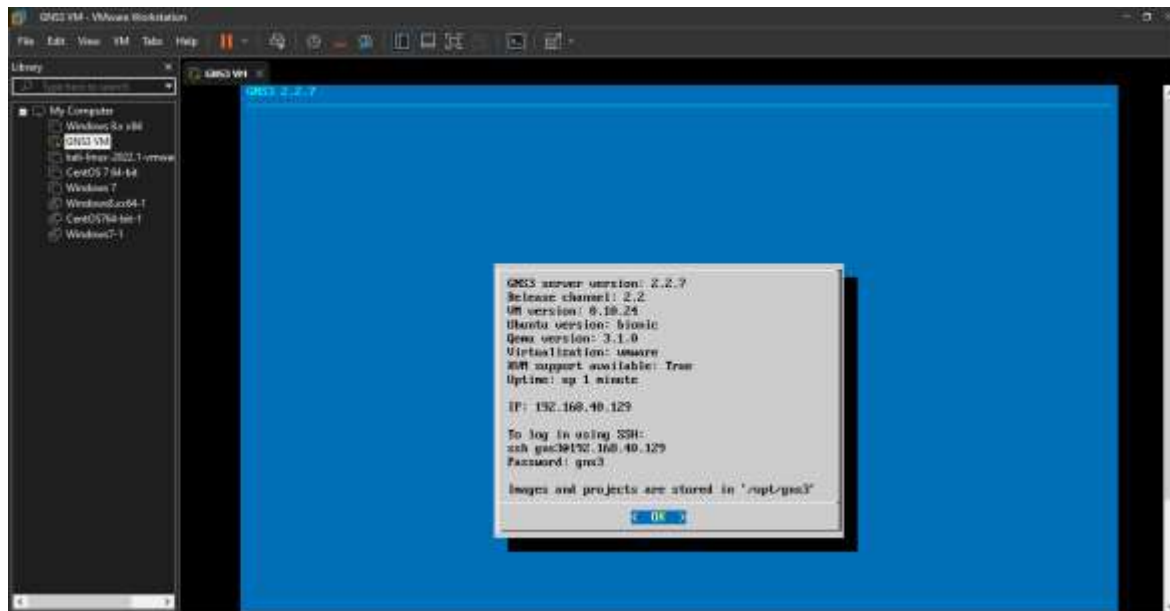
3.25 Recomendaciones

- Se recomienda colocar un equipo de borde NGFW después del switch para proporcionar un entorno de load-balancing y mejoras de seguridad
- Combinar el entorno de red con VRF (Virtual Routing Forward) a fin de segmentar la red de forma más eficiente
- Proporcionar un servidor DHCP a través de un Windows server y no por los equipos de red para mejor administración
- Usar un equipo que permita realizar la recopilación de logs y evaluar lo que sucede en la red en tiempo real.

ANEXOS

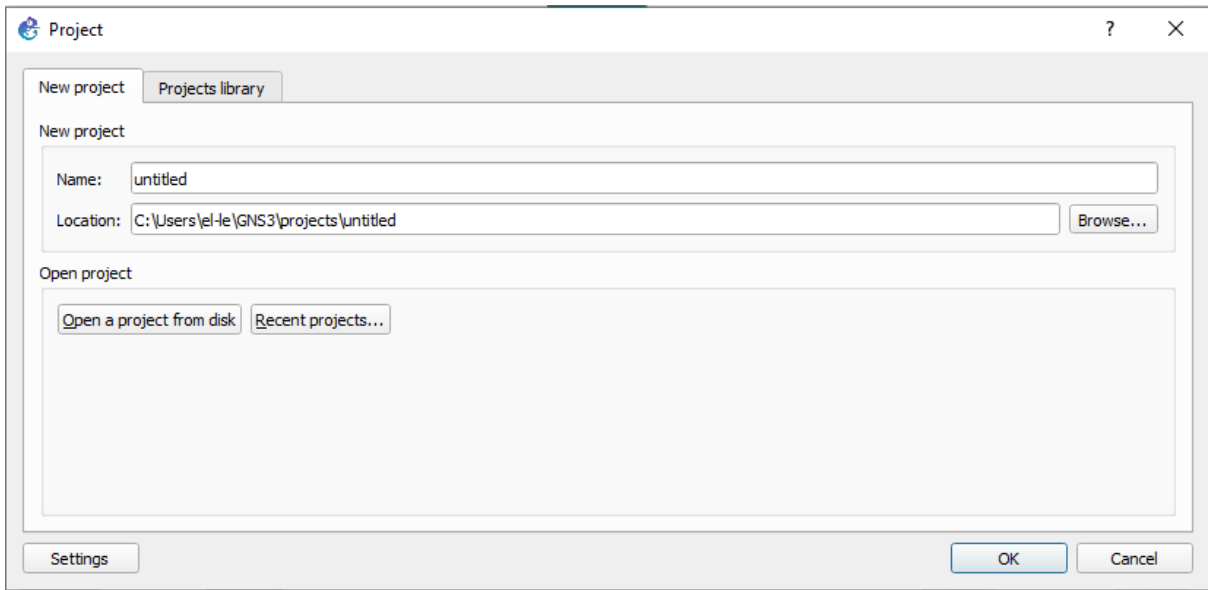
Anexo 1.

GNS3 instalado en VMWARE



Ruta: <https://docs.gns3.com/docs/getting-started/setup-wizard-gns3-vm/>

Anexo 2.
GNS3 funcionando



Bibliografía

- Álava, J. C., & Arcia, A. P. (2021). Análisis de tráfico de datos en la capa de enlace de redes LAN, para la detección de posibles ataques o intrusiones sobre tecnologías ethernet y wifi 802.11 en la carrera de ingeniería en sistemas computacionales de la Uni. de Manabí. *Universidad Estatal del Sur de Manabí*.
- Altamirano, D. O., & Álvarez, D. C. (2016). Estudio de la probabilidad de pérdida de carga y pérdida de carga horaria para sistemas autónomos y/o conectados a la red en Ecuador. *Universidad de Cuenca*.
- Alvarado, R. C. (2010). Documentación, implementación y elaboración de guías de laboratorio sobre protocolos de enrutamiento en la red: RIP, IS-IS, OSPF y BGP; basados en un software de simulación. *Universidad Pontificia Bolivariana*.
- Barbecho, P. B. (2016). Diseño y simulación de una topología y gestión de red basadas en túneles GRE y enrutamiento dinámica OSPF y EIGRP, caso de estudio grupo automotriz EIJURI. *Pontificia Universidad Católica Ecuador*.
- Cisco. (2020). *CCNA 200-301*. Estados Unidos.
- Cordova, C. R. (2010). Implementación de protocolos de comunicación para mejorar la disponibilidad de una red informática. *Universidad Señor de Spain*.
- Espinosa, E. C., & Moncayo, J. V. (2010). Análisis de los protocolos VRRP y CAP aplicado a la redundancia de gateway usando GNU/Linux para la empresa INFOQUALITY S.A. *Escuela Superior Politécnica de Chimborazo*.
- Espinoza, E. (2018). Desarrollo e implementación de un sistema de control de acceso a redes inalámbricas mediante Radius. *Universidad Nacional Mayor de San Marcos*.
- Figueroa, D., Díaz, F., & Gramajo, M. (2017). Estudio de la influencia de un entorno de simulación en la enseñanza de redes de computadoras en el nivel universitario. *Universidad de la Pata*.

- Jimenez, C. R. (2012). Implementación de un servidor radius para apoyar la seguridad en una red de telecomunicaciones. *Universidad Santo Toma*.
- Luje, L. Z., & Mosquera, H. G. (2011). Análisis de la metodología de integración de modelos de madurez de capacidades (CMMI) para el desarrollo de software. Caso práctico: Diseño e implementación de un sistema de fuerza de ventas de la empresa GATO SPORT importaciones de la ciudad de Quito. *Universidad Técnica de Cotopaxi*.
- Miranda, C. F., Villatoro, K. A., & Hernández, R. H. (2012). Implementación de un prototipo de red inalámbrica que permita elevar los niveles de seguridad a través de la autenticación de un servidor Radius para los usuarios que acceden a internet en el edificio Francisco Morazán de la UTEC. *Universidad Tecnológica de el Salvador*.
- Patiño, E. C. (2015). Reingeniería de la infraestructura de datos de la cooperativa de ahorro y crédito "San Antonio LTDA" y diseño de los enlaces inalámbricos a sus sucursales. *Universidad Técnica del Norte*.
- Pérez, C. S. (2017). Diseño e implementación de un enrutamiento redundante usando el protocolo Border Gateway Protocol (BGP) para la red de un proveedor de servicios de Internet en Bogotá. *Universidad Santo Tomás*.
- Quiroz, R. V., Ramírez, F. M., & Rivera, Y. G. (2013). Propuesta de prácticas de laboratorios de switching y routing para la carrera de ingeniería en telemática de UNAN - LEÓN. *Universidad Nacional Autónoma de Nicaragua UNAN - León*.
- Riffo, M. (2009). Vulnerabilidades de las redes TCP/IP y principales mecanismos de seguridad. *Universidad Austral de Chile*.
- Telecapp. (2022). *telecapp*.
- Torres, P. R. (2016). Diseño de una red privada virtual para la optimización de las comunicaciones en la empresa comunicaciones e informática SAC caso: redes de datos. *Universidad Inca Garcilaso de la Vega*.

- Vasquez, A. R. (2021). Diseño de una red de alto rendimiento aplicando el protocolo BGP o GLP con la funcionalidad de balanceo de carga transparente. *Universidad de Guayaquil*.
- Yerovi, N. L., & Flores, J. O. (2010). Análisis de los protocolos de la alta disponibilidad de gateways en la interconectividad LAN/WAN aplicadas al diseño de redes de campus. *Escuela Superior Politécnica de Chimborazo*.
- Zambrano, J. G. (2015). Estudio de una conexión de Internet aplicando un protocolo de alta disponibilidad para empresa grupo AGRIPRODUCT S.A. en la ciudad de Guayaquil. *Universidad de Guayaquil*.