



UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS

COMPUTACIONALES

TÍTULO:

“Análisis de los protocolos de Alta disponibilidad de Gateways en la interconectividad LAN/WAN aplicadas al diseño de la red del MAGAP Cotopaxi”

Tesis de Grado presentado previo a la obtención del título de Ingeniero en informática y sistemas Computacionales

AUTORES:

CARLOS DAVID AGUILAR CEVALLOS

EDGAR PATRICIO VELOSO CANCHIG

DIRECTOR DE TESIS:

ING. JAIME MESIAS CAJAS.

LATACUNGA - ECUADOR

Enero – 2012

AUTORIA

Por medio del presente, nosotros: **Carlos David Aguilar Cevallos** y **Veloso Canchig Edgar Patricio** declaramos que la investigación aquí realizada es de nuestra autoría: que no ha sido previamente presentado, y que hemos consultado todo lo que en este tomo está incluido.

.....
Carlos David Aguilar Cevallos

.....
Edgar Patricio Veloso Canchig

CERTIFICACIÓN

HONORABLE CONSEJO ACADÉMICO DE LA UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI.

De mi consideración.

Cumpliendo con lo estipulado en el capítulo IV, (art. 9 literal f), del reglamento del curso profesional de la Universidad Técnica de Cotopaxi, informo que los postulantes: Carlos David Aguilar Cevallos y Edgar Patricio Veloso Canchig, ha desarrollado su tesis de grado de acuerdo al planteamiento formulado en el plan de tesis con el tema: “Análisis de los protocolos de Alta disponibilidad de Gateways en la interconectividad LAN/WAN aplicadas al diseño de la red del MAGAP Cotopaxi”, cumpliendo con los objetivos planteados.

En virtud de lo antes expuesto, considero que la presente tesis se encuentra habilitada para presentarse al acto de la defensa de tesis.

Latacunga, 23 de Enero del 2012

Atentamente,

Ing. Jaime Mesías Cajas

DIRECTOR DE TESIS

AGRADECIMIENTO

Primero y antes que nada, dar gracias a Dios, por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante todo el periodo de estudio.

A mis padres y mis hermanos quienes me brindaron su apoyo moral y económico durante toda mi formación profesional, a mi hermano Fabian por sus palabras de aliento y su ayuda ya que también han formado parte de mi alegría y mi vida.

Un agradecimiento especial a la Universidad Técnica de Cotopaxi por haberme permitido adquirir conocimientos mediante sus docentes y ahora llegar a ser un gran profesional.

A mi director de tesis Ing. Jaime Cajas por la excelente orientación en la realización del presente trabajo.

A los Directivos del Magap Cotopaxi por habernos permitido realizar nuestro proyecto de tesis y poder culminarlo con gran éxito.

Edgar Veloso

Dedicatoria

A Dios quien fue el creador de todas las cosas, el que me ha dado fortaleza para continuar cuando a punto de caer he estado; por ello, con toda la humildad que de mi corazón puede emanar se lo dedico.

A mi hija Alejandra, que es el regalo más hermoso que Dios me pudo dar, ya que ella ha sido la fuente de inspiración e impulso en mi vida para alcanzar mis metas.

De igual forma, a mis Padres, a quien les debo toda mi vida, les agradezco el cariño y su comprensión, a ustedes quienes han sabido formarme con buenos sentimientos, hábitos y valores, lo cual me ha ayudado a salir adelante buscando siempre el mejor camino.

A mis hermanos Fabián, Cristina y Alex por su apoyo, amor y comprensión durante toda mi vida los quiero mucho.

Edgar Veloso

AGRADECIMIENTO

Para la realización de esta Tesis fue necesario el apoyo de personas muy importantes en mi vida y a quienes quiero agradecer.

En primer lugar a mis padres Carlos Alberto y Rosa Elena por brindarme su amor incondicional, comprensión, respaldo, confianza, apoyo moral y económico durante mi formación profesional, a mi hermano Renán Eduardo quien ha estado junto a mí en todo momento y a mi novia María Belén por amor, comprensión y sus palabras de aliento en momentos difíciles.

Un agradecimiento especial a la Universidad Técnica de Cotopaxi por abrirme las puertas del conocimiento a través de sus docentes y haberme formado académicamente para hoy poder ser un gran profesional.

A mi director de tesis Ing. Jaime Cajas por la excelente orientación en la realización del presente trabajo.

A todos los funcionarios del MAGAP Cotopaxi por la apertura y todo el apoyo brindado para la culminación de este trabajo.

Carlos David Aguilar.

DEDICATORIA

El presente proyecto de Tesis quiero dedicar a toda mi familia en especial a mis padres Carlos Alberto y Rosa Elena por su amor, cariño, comprensión y confianza que siempre depositaron sobre mí, a mi hermano Renán Eduardo por todo el apoyo que me brindaron durante toda mi vida, ellos quienes han estado en los buenos y malos momentos.

A mi novia María Belén quien me ha brindado su amor, cariño, comprensión y apoyo incondicional.

Carlos David Aguilar.

ÍNDICE GENERAL

PORTADA

PÁGINA DE AUTORÍA

CERTIFICACIÓN DEL DIRECTOR DE TESIS

CERTIFICACIÓN DEL DIRECTOR DE SERVICIOS INFORMÁTICOS

AGRADECIMIENTOS

DEDICATORIAS

CAPÍTULO I

FUNDAMENTO TEÓRICO SOBRE USO DE HERRAMIENTAS PARA OBTENER LOS RECURSOS MEDIDOS

1.1	INTERNET	5
1.1.1	Antecedentes	6
1.1.2	Definición	9
1.1.3	Importancia	11
1.2.	Routers	11
1.2.1	Definición	12
1.2.2	Importancia	13
1.2.3	Características	15
1.3	SWITCH	18
1.3.1	Definición	18
1.3.2	Importancia	19

1.3.3	Características	20
1.4	ENRUTAMIENTO	25
1.4.1	Definición	25
1.4.2.	Importancia	26
1.4.3	Características	31
1.5.	PROTOCOLO DE TRANSMISION	31
1.5.1	Definición	31

CAPÍTULO II

TRABAJO DE CAMPO

EL MINISTERIO DE AGRICULTURA GANADERIA ACUACULTURA Y PESCA DE COTOPAXI

2.1.	Diseño de la investigación	36
2.2.	MAGAP Cotopaxi	38
2.3.	Entrevistas realizadas a los directivos y empleados del MAGAP Cotopaxi	40
2.3.1.	Entrevista realizada al Director del MAGAP Cotopaxi	41
2.3.2	Entrevista realizada al encargado del Área de Comunicaciones y Sistemas	41
2.3.3	Encuesta a los empleados del MAGAP Cotopaxi	44
2.4	Comprobación de la Hipótesis	55

CAPÍTULO III

PROPUESTA

ANÁLISIS DE LOS PROTOCOLOS DE ALTA DISPONIBILIDAD DE GATEWAYS EN LA INTERCONECTIVIDAD LAN/WAN APLICADAS AL DISEÑO DE LA RED DEL MAGAP COTOPAXI

3.2.	Presentación	56
3.3.	Objetivos	58
3.3.1.	Objetivo General	58
3.3.2.	Objetivos Específicos	58
3.4.	Análisis de la situación actual del Router Cisco	58
3.5.	Protocolos de autenticación	59
3.6.	Análisis de los protocolos de configuración de equipos CISCO	60
3.6.1.	Protocolos HSPR	60
3.6.2.	Funcionalidad del protocolo HSPR en el MAGAP a nivel nacional	61
3.6.3.	Configuraciones	62
3.6.4	Aplicación del GLBP para el router del MAGAP Cotopaxi	64
3.6.5	Funcionamiento e identificación del proceso operativo	65
3.7.	Redes de Campus	71
3.8.	Implementación de los protocolos basados en cisco en el MAGAP de la provincia de Cotopaxi	73
3.9.	TRACERT	76
3.10	FILEZILLA	79
3.11	WIRESHARK	82
3.12	Procesamiento de Información	85

3.13	Retardos de Transmisión	86
3.14	Análisis estadístico de la red LAN/WAN	87
3.15	Tablas de análisis para el cálculo de envío/recepción de paquetes	88

CONCLUSIONES Y RECOMENDACIONES

	Conclusiones	90
	Recomendaciones	92
	Glosario de Términos y Siglas	93
	BIBLIOGRAFÍA	123

ANEXOS

RESUMEN

Las comunicaciones y las seguridades de la información y las telecomunicaciones hoy en día es la base primordial en toda institución pública o privada y más aún al tratarse de organismos gubernamentales ya que son las generadoras de recursos y las que promueven el desarrollo a las ciudades del país.

El Ministerio de Agricultura, ganadería, acuacultura y pesca es una institución que se encuentra a la vanguardia tecnológica ya que sus empleados y usuarios así lo demanda, prueba de esto ha sido que en la matriz(Quito) y en las provincias se encuentran equipados con computadores de última generación y con paquetes actualizados a la realidad nacional y mundial, prueba de esto es además que en la actualidad se encuentran equipadas las comunicaciones con equipos CISCO que son los que llevan la vanguardia tecnológica a nivel mundial.

El MAGAP para una buena atención a todos sus empleados y los usuarios de estos servicios a creído conveniente centralizar todas las comunicaciones en la ciudad de Quito y de aquí proveer todos sus servicios hacia las provincias de manera particular a Cotopaxi siendo esta una de las más necesitadas de recursos tecnológicos ya que cuenta con uno de los mayores números de usuarios por ser de las provincias ganaderas más grandes del país.

El enrutamiento se lo hace desde Quito hacia las provincias permitiendo de esta manera garantizar todas las comunicaciones y la fidelidad de la información toda vez que estas viajan encriptados mediante VPN's(Redes Privadas Virtuales), lo que hace que el personal que labora en la ciudad de Latacunga tenga preocupación alguna por la integridad de la información.

ABSTRACT

Today, Communications, information security and telecommunications is the primary basis in all public or private institution and even more when dealing with government institutions because they are generated resources and promoting the development of the cities.

The Agriculture, aquaculture and fisheries Ministry is an institution that it finds in vanguard of technology because its employees and users it demands, this test has been in the main institutions (Quito) and the provinces are equipped with computers and packages updated to national and global reality, Today they are fitted out with communications equipment that are CISCO that they have technology in worldwide.

The MAGAP to take care of all employees and users of these services they had believed centralize all communications in Quito city and provide all services to the Cotopaxi province because it needs technological resources so that it has the largest number of users and for being the largest livestock in the country.

The routing does from Quito to the provinces allowing thus to ensure all communications and accurate information whenever they travel encrypted VPN's ways (Virtual Private Networks), which makes the staff that works in Latacunga city they have any concern for the integrity of the information.

INTRODUCCION

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

Las instituciones cada vez más buscan un tiempo de actividad de 24 horas al día y siete días por semana para sus redes de informáticas. Lograr el 100% de tiempo de actividad tal vez es imposible., pero asegurar un tiempo de actividad de 99.99% es uno de los objetivos que toda empresa o institución se plantea.

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

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

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

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

Las redes requieren un nivel de disponibilidad cada vez más elevado, y en lo posible descartar completamente la posibilidad de interrupciones de servicio. Es por esto que la redundancia en el Gateway es una herramienta vital, toda vez que la puerta de enlace del router es la que definirá las seguridades y los anchos de banda de la institución.

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

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

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

En la parte práctica de la investigación se configurara cada uno de los protocolos de alta disponibilidad como son el GLBP, HSRP y VRRP en redes de campus en los equipos CISCO a fin de verificar físicamente como funcionan cada uno de ellos y así determinar cuál está libre .

En base a lo expuesto se tiene que la investigación comprende 3 secciones o capítulos claramente detallados para un mejor entendimiento y fácil acceso a esta fuente de consulta.

La investigación para un mejor entendimiento se detalla utilizando herramientas de última generación y que se basó completamente en el material que provee la academia CISCO NETWORKING la misma que en la actualidad son los que llevan la vanguardia tecnológica a nivel mundial en comunicaciones tanto de redes LAN como de las WAN.

En el primero se detalla de forma clara todos los conceptos y la teoría que se pone en práctica en los capítulos siguientes, tomando en cuenta siempre que los temas tengan que ver directamente con el desarrollo de la investigación propuesta.

En el segundo capítulo se hace un estudio de campo aplicando técnicas de investigación como son la entrevista y las encuestas para obtener los criterios tanto del director del MAGAP Cotopaxi, personal de Sistemas y finalmente de forma general de los empleados para posicionarse sobre el trabajo que se va a realizar.

En el tercer capítulo se realiza el estudio del funcionamiento previo a la investigación luego se diseña la estrategia a seguir para poder cumplir con los objetivos planteados dentro de la institución.

Por último se obtuvieron las conclusiones y recomendaciones sobre la investigación para poder generar sugerencias a los empleados y directivos del MAGAP Cotopaxi.

CAPITULO I

1 FUNDAMENTO TEÓRICO SOBRE USO DE HERRAMIENTAS PARA OBTENER LOS RECURSOS MEDIDOS.

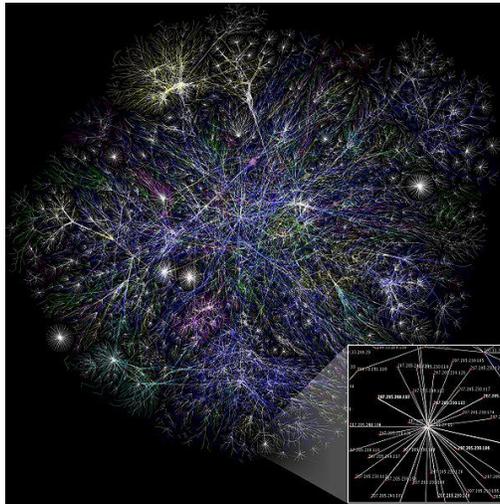
1.1 INTERNET

Internet es un conjunto descentralizado de [redes de comunicación](#) interconectadas que utilizan la familia de [protocolos TCP/IP](#), garantizando que las redes físicas [heterogéneas](#) que la componen funcionen como una red lógica única, de alcance mundial. Sus orígenes se remontan a [1969](#), cuando se estableció la primera conexión de computadoras, conocida como [ARPANET](#), entre tres universidades en [California](#) y una en [Utah, Estados Unidos](#).

Uno de los servicios que más éxito ha tenido en Internet ha sido la [World Wide Web](#) (WWW, o "la Web"), hasta tal punto que es habitual la confusión entre ambos términos. La WWW es un conjunto de protocolos que permite, de forma sencilla, la consulta remota de archivos de [hipertexto](#). Ésta fue un desarrollo posterior ([1990](#)) y utiliza Internet como [medio de transmisión](#).

Existen, por tanto, muchos otros servicios y protocolos en Internet, aparte de la Web: el envío de [correo electrónico](#) ([SMTP](#)), la transmisión de archivos ([FTP](#) y [P2P](#)), las [conversaciones en línea](#) ([IRC](#)), la [mensajería instantánea](#) y presencia, la transmisión de contenido y comunicación multimedia -[telefonía](#) ([VoIP](#)), [televisión](#) ([IPTV](#))-, los [boletines electrónicos](#) ([NNTP](#)), el [acceso remoto](#) a otros dispositivos ([SSH](#) y [Telnet](#)) o los [juegos en línea](#).

Grafico 1.1.: El Internet



Fuente: http://es.wikipedia.org/wiki/Archivo:Internet_map_1024.jpg

1.1.1 Antecedentes

Sus orígenes se remontan a la década de 1960, dentro de [ARPA](#) (hoy DARPA), como respuesta a la necesidad de esta organización de buscar mejores maneras de usar los computadores de ese entonces, pero enfrentados al problema de que los principales investigadores y laboratorios deseaban tener sus propios computadores, lo que no sólo era más costoso, sino que provocaba una duplicación de esfuerzos y recursos.⁵ Así nace ARPANet (Advanced Research Projects Agency Network o Red de la Agencia para los Proyectos de Investigación Avanzada de los Estados Unidos), que nos legó el trazado de una red inicial de comunicaciones de alta velocidad a la cual fueron integrándose otras instituciones gubernamentales y redes académicas durante los años 70.

Investigadores, científicos, profesores y estudiantes se beneficiaron de la comunicación con otras instituciones y colegas en su rama, así como de la posibilidad de consultar la información disponible en otros centros académicos y de investigación. De igual manera, disfrutaron de la nueva habilidad para publicar y hacer disponible a otros la información generada en sus actividades.

En el mes de julio de [1961](#) [Leonard Kleinrock](#) publicó desde el MIT el primer documento sobre la teoría de conmutación de paquetes. Kleinrock convenció a [Lawrence Roberts](#) de la factibilidad teórica de las comunicaciones vía paquetes en lugar de circuitos, lo cual resultó ser un gran avance en el camino hacia el trabajo informático en red. El otro paso fundamental fue hacer dialogar a los ordenadores entre sí. Para explorar este terreno, en [1965](#), Roberts conectó una computadora TX2 en Massachusetts con un Q-32 en California a través de una línea telefónica conmutada de baja velocidad, creando así la primera (aunque reducida) red de computadoras de área amplia jamás construida.

- [1969](#): La primera red interconectada nace el [21 de noviembre](#) de [1969](#), cuando se crea el primer enlace entre las universidades de UCLA y Stanford por medio de la línea telefónica conmutada, y gracias a los trabajos y estudios anteriores de varios científicos y organizaciones desde [1959](#) (ver: [Arpanet](#)). El [mito](#) de que ARPANET, la primera red, se construyó simplemente para sobrevivir a ataques nucleares sigue siendo muy popular. Sin embargo, este no fue el único motivo. Si bien es cierto que ARPANET fue diseñada para sobrevivir a fallos en la red, la verdadera razón para ello era que los nodos de conmutación eran poco fiables, tal y como se atestigua en la siguiente cita:

A raíz de un estudio de RAND, se extendió el falso rumor de que ARPANET fue diseñada para resistir un ataque nuclear. Esto nunca fue cierto, solamente un estudio de RAND, no relacionado con ARPANET, consideraba la guerra nuclear en la transmisión segura de comunicaciones de voz. Sin embargo, trabajos posteriores enfatizaron la robustez y capacidad de supervivencia de grandes porciones de las redes subyacentes. ([Internet Society](#), A Brief History of the Internet)

- [1972](#): Se realizó la Primera demostración pública de [ARPANET](#), una nueva red de comunicaciones financiada por la [DARPA](#) que funcionaba de forma distribuida sobre la [red telefónica conmutada](#). El éxito de ésta nueva arquitectura sirvió para que, en [1973](#), la [DARPA](#) iniciara un programa de investigación sobre posibles técnicas para interconectar redes (orientadas al tráfico de paquetes) de distintas clases. Para este fin, desarrollaron nuevos [protocolos de comunicaciones](#) que

permitiesen este intercambio de información de forma "transparente" para las computadoras conectadas. De la filosofía del proyecto surgió el nombre de "Internet", que se aplicó al sistema de redes interconectadas mediante los protocolos [TCP e IP](#).

- [1983](#): El [1 de enero](#), ARPANET cambió el protocolo [NCP](#) por TCP/IP. Ese mismo año, se creó el [IAB](#) con el fin de estandarizar el protocolo TCP/IP y de proporcionar recursos de investigación a Internet. Por otra parte, se centró la función de asignación de identificadores en la [IANA](#) que, más tarde, delegó parte de sus funciones en el [Internet registry](#) que, a su vez, proporciona servicios a los [DNS](#).
- [1986](#): La [NSF](#) comenzó el desarrollo de [NSFNET](#) que se convirtió en la principal [Red en árbol](#) de Internet, complementada después con las redes NSINET y ESNET, todas ellas en Estados Unidos. Paralelamente, otras redes troncales en [Europa](#), tanto públicas como comerciales, junto con las americanas formaban el esqueleto básico ("backbone") de Internet.
- [1989](#): Con la integración de los protocolos [OSI](#) en la arquitectura de Internet, se inició la tendencia actual de permitir no sólo la interconexión de redes de estructuras dispares, sino también la de facilitar el uso de distintos protocolos de comunicaciones.

En 1990 el [CERN](#) crea el código HTML y con él el primer cliente World Wide Web. En la imagen el código HTML con sintaxis coloreada.

En el [CERN](#) de [Ginebra](#), un grupo de físicos encabezado por [Tim Berners-Lee](#) creó el lenguaje [HTML](#), basado en el [SGML](#). En [1990](#) el mismo equipo construyó el primer cliente [Web](#), llamado WorldWideWeb (WWW), y el primer servidor web.

A inicios de los 90, con la introducción de nuevas facilidades de interconexión y herramientas gráficas simples para el uso de la red, se inició el auge que actualmente le

conocemos al Internet. Este crecimiento masivo trajo consigo el surgimiento de un nuevo perfil de usuarios, en su mayoría de personas comunes no ligadas a los sectores académicos, científicos y gubernamentales.

Esto ponía en cuestionamiento la subvención del gobierno estadounidense al sostenimiento y la administración de la red, así como la prohibición existente al uso comercial del Internet. Los hechos se sucedieron rápidamente y para 1993 ya se había levantado la prohibición al uso comercial del Internet y definido la transición hacia un modelo de administración no gubernamental que permitiese, a su vez, la integración de redes y proveedores de acceso privados.

- [2006](#): El [3 de enero](#), Internet alcanzó los mil cien millones de usuarios. Se prevé que en diez años, la cantidad de navegantes de la Red aumentará a 2.000 millones.

El resultado de todo esto es lo que experimentamos hoy en día: la transformación de lo que fue una enorme red de comunicaciones para uso gubernamental, planificada y construida con fondos estatales, que ha evolucionado en una miríada de redes privadas interconectadas entre sí. Actualmente la red experimenta cada día la integración de nuevas redes y usuarios, extendiendo su amplitud y dominio, al tiempo que surgen nuevos mercados, tecnologías, instituciones y empresas que aprovechan este nuevo medio, cuyo potencial apenas se comienza a descubrir.

1.1.2 Definición

Internet tiene un impacto profundo en el [mundo laboral](#), el [ocio](#) y el [conocimiento](#) a nivel mundial. Gracias a la web, millones de personas tienen acceso fácil e inmediato a una cantidad extensa y diversa de [información](#) en línea. Un ejemplo de esto es el desarrollo y la distribución de colaboración del software de Free/Libre/Open-Source (SEDA) por ejemplo GNU, Linux, Mozilla y OpenOffice.org.

Comparado a las [enciclopedias](#) y a las [bibliotecas](#) tradicionales, la web ha permitido una descentralización repentina y extrema de la información y de los datos. Algunas compañías e individuos han adoptado el uso de los *weblogs*, que se utilizan en gran parte como diarios actualizables. Algunas organizaciones comerciales animan a su personal para incorporar sus áreas de especialización en sus sitios, con la esperanza de que impresionen a los visitantes con conocimiento experto e información libre.

Internet ha llegado a gran parte de los hogares y de las empresas de los países ricos. En este aspecto se ha abierto una [brecha digital](#) con los países pobres, en los cuales la penetración de Internet y las nuevas tecnologías es muy limitada para las personas.

No obstante, en el transcurso del tiempo se ha venido extendiendo el acceso a Internet en casi todas las regiones del mundo, de modo que es relativamente sencillo encontrar por lo menos 2 computadoras conectadas en regiones remotas.

Desde una perspectiva cultural del conocimiento, Internet ha sido una ventaja y una responsabilidad. Para la gente que está interesada en otras culturas, la red de redes proporciona una cantidad significativa de información y de una interactividad que sería inasequible de otra manera.

Internet entró como una herramienta de globalización, poniendo fin al aislamiento de culturas. Debido a su rápida masificación e incorporación en la vida del ser humano, el espacio virtual es actualizado constantemente de información, fidedigna o irrelevante.

1.1.3 Importancia

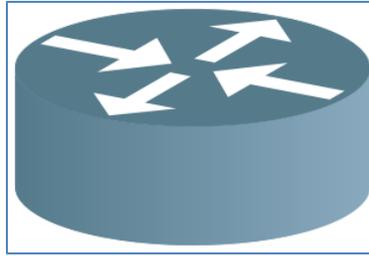
Inicialmente el Internet tenía un objetivo claro. Se navegaba en Internet para algo muy concreto: búsquedas de información, generalmente. Ahora quizás también, pero sin duda

algún hoy es más probable perderse en la red, debido al inmenso abanico de posibilidades que brinda. Hoy en día, la sensación que produce Internet es un ruido, una serie de interferencias, una explosión de ideas distintas, de personas diferentes, de pensamientos distintos de tantas posibilidades que, en ocasiones, puede resultar excesivo. El crecimiento o más bien la incorporación de tantas personas a la red hace que las calles de lo que en principio era una pequeña ciudad llamada Internet se conviertan en todo un planeta extremadamente conectado entre sí entre todos sus miembros. El hecho de que Internet haya aumentado tanto implica una mayor cantidad de relaciones virtuales entre personas. Es posible concluir que cuando una persona tenga una necesidad de conocimiento no escrito en libros, puede recurrir a una fuente más acorde a su necesidad. Como ahora esta fuente es posible en Internet. Como toda gran revolución, Internet augura una nueva era de diferentes métodos de resolución de problemas creados a partir de soluciones anteriores. Algunos sienten que Internet produce la sensación que todos han sentido sin duda alguna vez; produce la esperanza que es necesaria cuando se quiere conseguir algo. Es un despertar de intenciones que jamás antes la tecnología había logrado en la población mundial. Para algunos usuarios Internet genera una sensación de cercanía, empatía, comprensión y, a la vez, de confusión, discusión, lucha y conflictos que los mismos usuarios consideran la vida misma.

1.2 ROUTERS

Un router [anglicismo](#), también conocido como encaminador, enrutador, direccionador o ruteador es un dispositivo de [hardware](#) usado para la [interconexión](#) de [redes informáticas](#) que permite asegurar el direccionamiento de [paquetes de datos](#) entre ellas o determinar la mejor ruta que deben tomar. Opera en la [capa tres](#) del [modelo OSI](#).

Grafico 1.2.: Representación de un Router



Fuente: Ayuda del paquete Microsoft Visio 2007

1.2.1 Definición

Router es un término inglés que puede traducirse como enrutador, ruteador o direccionador. Se trata de un dispositivo de hardware que se utiliza para interconectar computadoras que operan en nivel de red.

El router se encarga de determinar qué ruta debe seguir un paquete de datos dentro de una red informática. Puede utilizarse en la interconexión de computadoras, en la conexión entre las computadoras e Internet o en el interior de los proveedores de servicios de Internet.

Los routers que se utilizan dentro de los hogares se conocen como SOHO (Small Office, Home Office). Estos dispositivos permiten que varias computadoras se conecten a un servicio de banda ancha a través de una red privada virtual segura. Técnicamente, los routers residenciales se encargan de traducir las direcciones de red en lugar de concretar el enrutamiento (no conecta a todos los ordenadores locales a red de forma directa, sino que hace que los distintos ordenadores funcionen como un solo equipo).

Dentro de las empresas, pueden encontrarse los routers de acceso (incluyendo los SOHO), los routers de distribución (suman tráfico a partir de otros enrutadores o de la obtención de los flujos de datos) y los routers de núcleo o core routers (que administran diversos niveles de routers).

Existen, por otra parte, los routers inalámbricos, que funcionan como una interfaz entre las redes fijas y las redes móviles (como WiFi, WiMAX y otras). Los routers inalámbricos

comparten los mismos principios que los routers tradicionales, aunque admiten la conexión sin cables a la red en cuestión

Grafico 1.3.: Router



Fuente: <http://es.wikipedia.org/wiki/Archivo:router1122.jpg>

1.2.2 Importancia

Los encaminadores pueden proporcionar [conectividad](#) dentro de las empresas, entre las empresas e [Internet](#), y en el interior de proveedores de servicios de Internet ([ISP](#)). Los encaminadores más grandes (por ejemplo, el [Alcatel-Lucent 7750 SR](#)) interconectan ISPs, se suelen llamar metro encaminador, o pueden ser utilizados en grandes redes de empresas.

Conectividad Small Office, Home Office (SOHO)

Los encaminadores se utilizan con frecuencia en los hogares para conectar a un servicio de banda ancha, tales como IP sobre [cable](#) o [ADSL](#). Un encaminador usado en una casa puede permitir la conectividad a una empresa a través de una [red privada virtual](#) segura.

Si bien funcionalmente similares a los encaminadores, los encaminadores residenciales usan [traducción de dirección de red](#) en lugar de enrutamiento.

En lugar de conectar ordenadores locales a la red directamente, un encaminador residencial debe hacer que los ordenadores locales parezcan ser un solo equipo.

Encaminador de empresa

En las empresas se pueden encontrar encaminadores de todos los tamaños. Si bien los más poderosos tienden a ser encontrados en ISPs, instalaciones académicas y de investigación, pero también en grandes empresas.

El modelo de tres capas es de uso común, no todos de ellos necesitan estar presentes en otras redes más pequeñas.

Los encaminadores de acceso, incluyendo SOHO, se encuentran en sitios de clientes como sucursales que no necesitan de enrutamiento jerárquico de los propios. Normalmente, son optimizados para un bajo costo.

Los encaminadores de distribución agregan tráfico desde encaminadores de acceso múltiple, ya sea en el mismo lugar, o de la obtención de los flujos de datos procedentes de múltiples sitios a la ubicación de una importante empresa. Los encaminadores de distribución son a menudo responsables de la aplicación de la calidad del servicio a través de una WAN, por lo que deben tener una memoria considerable, múltiples interfaces WAN, y transformación sustancial de inteligencia.

También pueden proporcionar conectividad a los grupos de servidores o redes externas. En la última solicitud, el sistema de funcionamiento del encaminador debe ser cuidadoso como parte de la seguridad de la arquitectura global. Separado del encaminador puede estar un [cortafuegos](#) o [VPN](#) concentrador, o el encaminador puede incluir estas y otras funciones de seguridad. Cuando una empresa se basa principalmente en un campus, podría no haber una clara distribución de nivel, que no sea tal vez el acceso fuera del campus.

En tales casos, los encaminadores de acceso, conectados a una [red de área local](#) (LAN), se interconectan a través del Core routers.

En las empresas, el core routers puede proporcionar una "columna vertebral" interconectando la distribución de los niveles de los encaminadores de múltiples edificios de un campus, o a las grandes empresas locales. Tienden a ser optimizados para ancho de banda alto.

Cuando una empresa está ampliamente distribuida sin ubicación central, la función del core router puede ser asumido por el servicio de [WAN](#) al que se suscribe la empresa, y la distribución de encaminadores se convierte en el nivel más alto.

Los encaminadores de borde enlazan [sistemas autónomos](#) con las redes troncales de Internet u otros sistemas autónomos, tienen que estar preparados para manejar el protocolo [BGP](#) y si quieren recibir las rutas BGP, deben poseer una gran cantidad de memoria.

1.2.3 Características

El enrutador ADSL es un dispositivo que permite conectar al mismo uno o varios equipos o incluso una o varias [redes de área local](#).

Realmente se trata de varios componentes en uno. Realiza las funciones de:

- [Puerta de enlace](#), ya que proporciona salida hacia el exterior a una red local.
- [Enrutador](#): cuando le llega un paquete procedente de Internet, lo dirige hacia la interfaz destino por el camino correspondiente, es decir, es capaz de encaminar paquetes IP, evitando que el paquete se pierda o sea manipulado por terceros.
- [Módem ADSL](#): modula las señales enviadas desde la red local para que puedan transmitirse por la línea ADSL y demodula las señales recibidas por ésta para que los equipos de la LAN puedan interpretarlos. De hecho, existen configuraciones formadas por un módem ADSL y un router que hacen la misma función que un router ADSL.
- [Punto de acceso inalámbrico](#): algunos enrutadores ADSL permiten la comunicación vía Wireless (sin cables) con los equipos de la red local.

Como se puede ver, los avances tecnológicos han conseguido introducir la funcionalidad de cuatro equipos en uno sólo

El cable telefónico de par de cobre que tenemos todos en casa se diseñó inicialmente para la transmisión de voz. Al comienzo de la era de las comunicaciones digitales se comenzó a utilizar para la transmisión de datos. El sistema era fácil: los "ceros" (determinando ausencia de tensión eléctrica por un periodo de tiempo determinado) y los "unos" (que no dejan de ser más que un impulso de tensión de unos 5 voltios durante idéntico tiempo determinado, y por tanto presencia de dicha tensión por igual periodo) de que estaban compuestas las señales digitales que genera el ordenador no podían circular por el cable telefónico. Para poder hacerlo se "modulaban", es decir, se convertían en un sonido que sí puede transmitirse. Las señales que se recibían lo hacían en forma de sonido que, a su vez, eran demoduladas y convertidas de nuevo en señales eléctricas ("unos" y "ceros"). Esto lo hacía un módem (modulador - demodulador). Es como si silbáramos con dos notas distintas (una para los "unos" y otra para los "ceros") por el teléfono. Todo el ancho de banda que admite el cable es empleado por la transmisión de datos. Este tipo de tecnología se denomina analógica.

Posteriormente se crea la tecnología [RDSI](#) que hizo posible que por los cables de teléfono pudiesen circular los "unos" y "ceros" puros, sin modular, como impulsos eléctricos que son. Ésta es la única tecnología de transmisión de datos verdaderamente digital. Esta tecnología presenta, sin embargo, un inconveniente, que se considera insalvable: las características electrónicas del famoso cable telefónico impide que se puedan transmitir datos en forma digital a una velocidad superior a 56 kbps. Para aumentar la velocidad se emplean varias líneas telefónicas. Se puede hablar y enviar datos por una línea básica porque está compuesta por dos líneas individuales, una de voz y otra de datos.

Surge entonces ADSL. En contra de lo que se cree, no es una tecnología digital, sino tan analógica como el antiguo módem de 56 Kbps, lo que sucede es que el tipo de señal analógica se la "interpreta" como digital por las variaciones que posee; en realidad si la señal fuera realmente digital la misma no podría alcanzar ni los 100 metros y se caería, sabiendo no obstante que las líneas ADSL superan los 5 kilómetros. La diferencia estriba en un elemento definitivo: el oído humano, el mismo no es capaz de oír todo el rango de frecuencias que produce la voz (el mismo principio empleado para poder comprimir música). De este modo, se aplica un [filtro sofométrico](#) que deja pasar sólo el rango de

frecuencias audibles y descarta las restantes, tanto por encima como por debajo de este rango. Es la función que desempeña el microfiltro que se pone en los teléfonos en una línea ADSL. En este espacio que queda libre se colocan diversas frecuencias portadoras moduladas con datos igual que hacía el módem. El aumento en la velocidad del ADSL viene dado porque, según va aumentando el nivel tecnológico, es posible meter más frecuencias portadoras en esos espacios libres, pues los filtros que separan unas portadoras de otras son cada vez más selectivos.

El router ADSL proporciona acceso a Internet a través de una línea ADSL, por lo que la interfaz que comunica con el exterior debe adaptarse a este medio. Por ello, este dispositivo lleva una interfaz [RJ11](#) para conectar el cable telefónico. Existen routers que disponen de dos conexiones RJ11 para poder transmitir sobre dos líneas y así duplicar la [capacidad de transmisión](#). Además, debe de estar provisto de un [modulador](#) para adecuar las señales de datos a las frecuencias en las que trabaja la tecnología ADSL y de un [demodulador](#) para poder interpretar las señales que le llegan desde el exterior

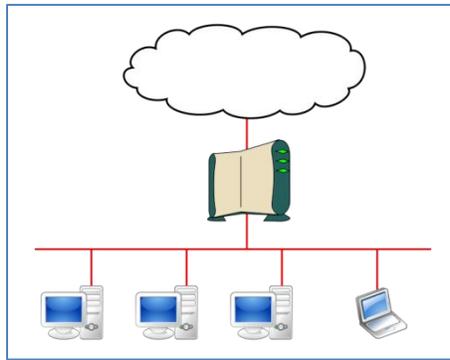
Por el otro lado está el conjunto de equipos o la red de área local a la cual se quiere dar conexión a Internet. En esta parte hay más posibilidades para realizar la comunicación. Las más comunes son [Ethernet](#) y [Wireless](#), incluso hay dispositivos que proporcionan ambas a la vez.

Para el primer caso, el router ADSL debe tener una o varias interfaces Ethernet. A cada una de estas interfaces se pueden conectar los equipos directamente o bien subredes comunicadas por medio de un concentrador ([hub](#)) o un conmutador ([switch](#)).

Para el caso de una interfaz Wireless, la comunicación se realiza sin cables. Simplemente hay que ubicar el equipo que se quiere conectar a Internet con una interfaz de estas características en una zona que tenga cobertura.

Otra interfaz que pueden ofrecer los enrutadores ADSL es por puerto [USB](#)

Grafico 1.4: [Enrutar el internet a una red LAN](#)



Fuente: http://es.wikipedia.org/wiki/Archivo:Internet_map_345.jpg

1.3 SWITCH

1.3.1 Definición

Un conmutador o el concentrador de conmutación es un [dispositivo de red informática](#) que conecta [segmentos de red](#) .

El término se refiere comúnmente a una multi-puerto de [puente de red](#) que los procesos y datos de rutas en la [capa de enlace de datos](#) (capa 2) del [modelo OSI](#) . Interruptores que, además, procesar los datos en la [capa de red](#) (Capa 3) y por encima se refieren a menudo como conmutadores de nivel 3 o [switches multicapa](#).

La primera [Ethernet](#) switch fue introducido por [Kalpana](#) en 1990.

El conmutador de red juega un papel integral en la mayoría de los modernos [Ethernet redes de área local](#) (LAN). De medio a gran tamaño de las LAN contienen un número de vinculados [logrado](#) interruptores. [pequeña oficina / oficina en casa](#) (SOHO), las aplicaciones suelen utilizar un solo interruptor, o para todo uso [de dispositivos convergentes](#) , como una [pasarela residencial](#) para el acceso de pequeñas oficinas / hogar [de](#)

[banda ancha](#) los servicios como DSL o Internet por cable . En la mayoría de estos casos, el dispositivo del usuario final contiene un [enrutador](#) y los componentes que interactúan con la tecnología de banda ancha física particular. Dispositivos para el usuario también puede incluir una interfaz de teléfono para VoIP.

Un conmutador Ethernet opera en la capa de enlace de datos del [modelo OSI](#) para crear nuestro propio [dominio de colisión](#) para cada puerto de switch. Con 4 ordenadores (por ejemplo, A, B, C y D) el 4 puertos de switch, A y B pueden transferir datos de ida y vuelta, mientras que C y D también lo hacen al mismo tiempo, y las dos conversaciones no se interfieren entre sí. En el caso de un hub, todos ellos a compartir el ancho de banda y se ejecutan en half duplex , lo que resulta en las colisiones, que a su vez requeriría retransmisiones. El uso de un switch se denomina [microsegmentación](#). Esto permite que los ordenadores tengan el ancho de banda dedicado en una conexión punto a punto a la red y por lo tanto, para ejecutar en full duplex sin colisiones.

1.3.2 Importancia

Interruptores pueden operar en una o más capas del modelo OSI, incluyendo [el enlace de datos](#) y [red](#) . Un dispositivo que funciona de forma simultánea en más de una de estas capas se conoce como un [interruptor de múltiples capas](#) .

En los aparatos destinados a uso comercial, interfaces integradas o modulares que permiten conectar diferentes tipos de redes, incluyendo [Ethernet](#) , [Fibre Channel](#) , [ATM](#) , [la UIT-T G.hn](#) y 802,11 . Esta conectividad puede ser en cualquiera de las capas mencionadas. Mientras que la funcionalidad de nivel 2 es adecuada para el ancho de banda de desplazamiento dentro de una tecnología, tecnologías de interconexión tales como [Ethernet](#) y [Token Ring](#) es más fácil en la capa 3.

Dispositivos que se interconectan en la capa 3 son llamados tradicionalmente [los routers](#) , por lo que "Layer-3 interruptores" también puede ser considerada como (relativamente primitivas) routers.

En algunos proveedores de servicios y otros ambientes donde hay una necesidad de una gran cantidad de análisis de rendimiento de la red y de seguridad, interruptores pueden estar conectados entre los routers WAN como los lugares para los módulos de análisis. Algunos vendedores proporcionan [firewall](#), de la red de detección de intrusos, y los módulos de análisis de rendimiento que se puede conectar a los puertos del switch. Algunas de estas funciones pueden estar en los módulos de combinación.

En otros casos, el interruptor se utiliza para crear una imagen de espejo de los datos que se pueden ir a un dispositivo externo. Como la mayoría de la duplicación de puertos switch proporciona sólo una secuencia en espejo, concentradores de red puede ser útil para avivar a los datos de varios analizadores de sólo lectura, tales como [sistemas de detección de intrusos](#) y sniffers

1.3.3 Características

Mientras que los interruptores pueden aprender acerca de topologías en muchas capas, y hacia adelante en una o más capas, que tienden a tener características comunes. Que no sea para aplicaciones de alto rendimiento, modernos interruptores comercial interfaces de Ethernet sobre todo, que puede tener de entrada diferentes y anchos de banda de salida de 10, 100, 1.000 o 10.000 [megabits por segundo](#) .

En cualquier capa, un interruptor moderno puede llevar a cabo [la alimentación por Ethernet](#) (PoE), lo que evita la necesidad de que los dispositivos conectados, tales como un [teléfono VoIP](#) o [punto de acceso inalámbrico](#) , para tener una fuente de alimentación independiente. Puesto que los conmutadores pueden tener circuitos redundantes de alimentación conectado a [sistemas de alimentación ininterrumpida](#) , el dispositivo conectado puede seguir funcionando incluso cuando la energía falla normal de oficina.

Un [concentrador de red](#) , o un repetidor, es un dispositivo de red simple. Centros no consiguen ninguno de los de tráfico que llega a través de ellos. Cualquier paquete que entre un [puerto](#) se transmite o se "repite" en todos los puertos, excepto para el puerto de entrada.

Dado que cada paquete se repite en cada puerto, paquetes [colisiones](#) afectan a toda la red, lo que limita su capacidad.

Hay aplicaciones especializadas en un centro puede ser útil, como la copia de tráfico de redes de sensores múltiples. Switches de gama alta tienen una característica que hace la misma cosa llamada [duplicación de puertos](#) .

Por la década de 2000, hubo una pequeña diferencia económica entre un concentrador y un conmutador de gama baja.

Un [puente de red](#) , que opera en la capa de enlace de datos, puede interconectar un número reducido de dispositivos en el hogar o la oficina. Este es un caso trivial de transición, en el que el puente aprende la [dirección MAC](#) de cada dispositivo conectado.

Puentes de un solo también puede proporcionar un rendimiento extremadamente alto en aplicaciones especializadas, tales como [redes de área de almacenamiento](#) .

Puentes clásicos también pueden interconectar mediante un [protocolo de árbol de expansión](#) que desactiva los enlaces para que la red resultante de área local es un [árbol](#) sin bucles. A diferencia de los routers, que abarcan puentes árbol debe tener topologías con sólo un camino activo entre dos puntos. La mayor [IEEE 802.1D](#) Spanning Tree Protocol podría ser muy lento, con el desvío de parar durante 30 segundos, mientras que el árbol de expansión que reconverger. Un [protocolo Rapid Spanning Tree](#) se introdujo como IEEE [802.1w](#) , pero la última edición del [IEEE 802.1D](#) adopta las extensiones 802.1w como el estándar de base.

El IETF está especificando el [TRILL](#) protocolo, que es la aplicación de la tecnología de enrutamiento de estado de enlace al capa-2 problema puente. Dispositivos que implementan TRILL, llamados [RBridges](#) , combinan las mejores características de ambos routers y puentes.

Mientras que el "switch de capa 2" sigue siendo más de un término de marketing que un término técnico, de los productos que se presentó como "switches" tendían a utilizar [microsegmentación](#) y [duplex](#) para evitar colisiones entre los dispositivos conectados a

Ethernet. Mediante el uso de un interno [plano de reenvío](#) mucho más rápido que cualquier interfaz, dan la impresión de rutas simultáneas entre varios dispositivos.

Una vez que un puente se entera de la topología a través de un protocolo spanning tree, envía tramas de datos de capa de enlace con una capa de 2 método de reenvío. Hay cuatro métodos de reenvío de un puente puede utilizar, de los cuales el segundo cuarto a través del método fueron el rendimiento cada vez mayor cuando se utilizan métodos de "cambiar" los productos con la misma entrada y salida de ancho de banda del puerto:

[Almacenar y enviar](#) : El interruptor de buffers y verifica cada cuadro antes de enviarlo.

[Corte a través de](#) : El interruptor sólo lee hasta la dirección de hardware del marco antes de comenzar a avanzar. De corte a través de los interruptores tienen que recurrir a almacenar y reenviar si el puerto de salida está ocupada en el momento en que el paquete llega. No hay ninguna comprobación de errores con este método.

[Fragmento libre](#) : Un método que intenta mantener los beneficios de almacenar y hacia adelante y cortar. Fragmento libre comprueba los primeros 64 [bytes](#) de la [trama](#) , donde [abordar](#) se almacena la información. De acuerdo a las especificaciones de Ethernet, las colisiones se detectan durante los primeros 64 bytes de la trama, por lo que las tramas que están en un error debido a una colisión, no será enviado. De esta manera el marco siempre llegará a su destino. Comprobación de errores de los datos reales en el paquete se deja para el último dispositivo.

[Adaptación de conmutación](#) : Un método de selección automática entre los otros tres modos.

Si bien existen aplicaciones especializadas, tales como redes de área de almacenamiento, donde la entrada y las interfaces de salida son los mismo ancho de banda, esto es raramente el caso, en general, aplicaciones LAN. En redes de área local, un interruptor utilizado para el acceso del usuario final por lo general se concentra menor ancho de banda (por ejemplo, 10/100 Mbit / s) en un mayor ancho de banda (al menos 1 Gbit / s). Por otra parte, un

interruptor que permite el acceso a los puertos de servidor por lo general se conecta a ellos en un ancho de banda mucho mayor que la utilizada por los dispositivos de usuario final.

Nivel 3

Dentro de los límites de la capa física Ethernet, un conmutador de capa 3 puede llevar a cabo todas o algunas de las funciones normalmente desempeñadas por un [enrutador](#) . La capa-3 más común es la conciencia de la capacidad [de multidifusión IP](#) a través de [IGMP](#) . Con esta toma de conciencia, un cambio de capa-3 puede aumentar la eficiencia mediante la entrega de tráfico de un grupo multicast sólo a los puertos en el dispositivo conectado ha señalado que quiere escuchar a ese grupo.

Nivel 4

Aunque el significado exacto del término de capa-4 switch es vendedor-dependiente, que casi siempre comienza con una capacidad de [traducción de direcciones de red](#) , pero luego agrega algún tipo de [distribución de la carga](#) basado en [TCP](#) sesiones.

El dispositivo puede incluir un stateful [firewall](#) , una [VPN](#) concentrador, o ser un [IPSec](#) gateway de seguridad.

Nivel 7

Capa 7 switches pueden distribuir las cargas sobre la base de [URL](#) o de alguna instalación específica técnica para reconocer el nivel de aplicación de las transacciones. Un interruptor de nivel 7 puede incluir un [caché web](#) y participar en una [red de distribución de contenido](#)

SWITCH DE BORDE O ACCESS

Estos switches son donde se conecta los equipos finales, su propósito es garantizar el acceso a equipos de red(workstation y servers)

SWITCH DISTRIBUCION

Son usados para segmentar grupos de trabajo, las políticas de conectividad están configuradas en esta capa.

SWITCH CORE.

Estos switches te proveen de alta velocidad hacia tu backbone o puerto WAN estos switches deben manejar los paquetes tan rápido como sea posible, son como el cerebro de tu red switchada, recuerda que el core es crítico para la conectividad, esta capa maneja alto nivel de disponibilidad y debe adaptarse a los cambios que sufra tu red de manera inmediata

1.4 ENRUTAMIENTO

1.4.1 Definición

El enrutamiento es el proceso de selección de rutas en una red a lo largo de la que enviar tráfico de red. Enrutamiento se realiza para muchos tipos de redes, incluyendo la [red telefónica](#) ([conmutación de circuitos](#)), [las redes de datos](#) (como el [Internet](#)), y [las redes de transporte](#) . Este artículo se ocupa principalmente de enrutamiento en redes de datos electrónica con [la conmutación de paquetes](#) de tecnología.

En las redes de conmutación de paquetes, enrutamiento ordena [el reenvío de paquetes](#) , el tránsito de los paquetes direccionará desde su origen hasta su destino final a través de intermediarios [nodos](#) , por lo general los dispositivos de hardware llamados [enrutadores](#) , [puentes](#) , [pasarelas](#) , [firewalls](#) o [switches](#) . De propósito general [computadoras](#) también puede reenviar los paquetes y realizar el enrutamiento, aunque no son de hardware

especializado y puede sufrir de un rendimiento limitado. El proceso de enrutamiento generalmente dirige el reenvío en la base de [las tablas de enrutamiento](#) que mantienen un registro de las rutas a destinos de red diferentes. Por lo tanto, la construcción de tablas de enrutamiento, que se celebran en el router de [la memoria](#) , es muy importante para el enrutamiento eficiente. La mayoría de los algoritmos de enrutamiento utilizan sólo una ruta de red a la vez, sino [múltiple de enrutamiento de](#) las técnicas de permitir el uso de vías alternativas múltiples.

De enrutamiento, en un sentido más estricto del término, es a menudo contrasta con [puente](#) en su suposición de que [las direcciones de red](#) están estructurados y que las direcciones similares implican la proximidad de la red. Puesto que las direcciones estructuradas permiten una entrada de la tabla de enrutamiento para representar el camino a un grupo de dispositivos, estructura de direccionamiento (routing, en el sentido estricto) supera estructuras de direccionamiento (puente) en redes de gran tamaño, y se ha convertido en la principal forma de abordar a través de Internet, a pesar de puente sigue siendo ampliamente utilizado en entornos localizados

1.4.2 Importancia

En una práctica conocida como [enrutamiento estático](#) (o no-adaptación de enrutamiento), redes pequeñas puede utilizar configurar manualmente las tablas de enrutamiento. Las grandes redes tienen complejas [topologías](#) que pueden cambiar rápidamente, por lo que la construcción manual de las tablas de enrutamiento inviable. Sin embargo, la mayoría de la red telefónica pública conmutada (PSTN) utiliza pre-computadas las tablas de enrutamiento, con rutas de alternativa en caso de la ruta más directa se bloquea (ver [ruta en el PSTN](#)). [Encaminamiento adaptativo](#) , o de enrutamiento dinámico, los intentos de resolver este problema la construcción de tablas de enrutamiento de forma automática, basándose en la información realizadas por [los protocolos de enrutamiento](#) , y permitiendo que la red de actuar casi de forma autónoma para evitar fallos en la red y los bloqueos.

Ejemplos de algoritmos de encaminamiento adaptativo-son el protocolo de información de enrutamiento ([RIP](#)) y el protocolo abierto la ruta más corta primero (OSPF). Encaminamiento adaptativo domina el Internet. Sin embargo, la configuración de los protocolos de enrutamiento requiere a menudo un toque experto,. La tecnología de red no se ha desarrollado hasta el punto de la automatización completa de enrutamiento ^{[[cita requerida](#)]}

[[editar](#)] algoritmos de vector de distancia

Artículo principal: [vector distancia del protocolo de enrutamiento](#)

Vector Distancia algoritmos utilizar el algoritmo de Bellman-Ford algoritmo. Este enfoque asigna un número, el costo, a cada uno de los enlaces entre cada nodo de la red. Nodos envían información desde el punto A al punto B a través de la trayectoria que se traduce en el menor costo total (es decir, la suma de los costos de los enlaces entre los nodos usados).

El algoritmo funciona de una manera muy simple. Cuando un nodo inicia por primera vez, sólo se sabe de sus vecinos inmediatos, y los costos directos involucrados en llegar a ellos. (Esta información, la lista de destinos, el costo total para cada uno, y el siguiente salto para enviar los datos para llegar allí, hacen que la tabla de enrutamiento, o una mesa de distancia.) Cada nodo, de forma regular, envía a cada vecino su propia idea actual del costo total para llegar a todos los destinos que conoce. El nodo vecino (s) examinar esta información, y compararlo con lo que ya "saben", lo que representa una mejora respecto a lo que ya tienen, se insertan en su propia tabla de enrutamiento (s). Con el tiempo, todos los nodos de la red a descubrir la mejor próximo salto para todos los destinos, y el mejor costo total.

Cuando uno de los nodos implicados se cae, los nodos que lo utilizó como su próximo salto para determinados destinos, descartar las entradas, y crear nuevas rutas, información de la tabla. A continuación, pasar esta información a todos los nodos adyacentes, que luego repita el proceso. Eventualmente, todos los nodos de la red reciben la información

actualizada, a continuación, descubrirá nuevos caminos a todos los destinos que todavía puede "llegar".

Algoritmos de estado de enlace

Al aplicar los algoritmos de estado de enlace, cada nodo utiliza como datos fundamentales de una [mapa](#) de la red en forma de un [gráfico](#) . Para producir este, cada nodo de las inundaciones en toda la red con información sobre lo que los otros nodos que pueden conectarse, y cada nodo de manera independiente reúne esta información en un mapa. El uso de este mapa, cada router de manera independiente determina la ruta de menor costo de sí mismo a todos los demás nodos utilizando un estándar de [los caminos más cortos](#) algoritmo como [el algoritmo de Dijkstra](#) . El resultado es un [árbol](#) con raíz en el nodo actual de tal manera que el camino a través del árbol desde la raíz a cualquier otro nodo es el camino de menor coste para ese nodo. Este árbol se sirve para construir la tabla de enrutamiento, que especifica el mejor próximo salto para llegar desde el nodo actual a cualquier otro nodo.

Enlace optimizada Estado algoritmo de encaminamiento

Un algoritmo de enrutamiento de estado de enlace optimizado para móviles ad-hoc es la Optimización de estado de enlace de Routing Protocol (OLSR). ^[1] OLSR es proactivo, sino que utiliza Hola y topología de mensajes de control (TC) para descubrir y difundir la información de estado de enlace a través de la móviles ad-hoc . Utilizando mensajes de saludo, cada nodo descubre dos-hop información del vecino y elige a un conjunto de [relevadores multipunto](#) (MPR). MPR OLSR distinguir de otros protocolos de enrutamiento de estado de enlace.

Protocolo de vector de ruta

Vector de distancia y de estado del vínculo de enrutamiento son protocolos de enrutamiento dentro del dominio. Se utilizan dentro de un [sistema autónomo](#) , pero no entre sistemas autónomos. Estos dos protocolos de enrutamiento se intratable en redes grandes y no se puede utilizar en [Inter-dominio](#) de enrutamiento. De enrutamiento vector distancia está sujeta a la inestabilidad si hay más de varios saltos en el dominio. Estado de los vínculos de enrutamiento necesita gran cantidad de recursos para el cálculo de las tablas de enrutamiento. También crea el tráfico pesado debido a las inundaciones.

Camino de enrutamiento por vector se utiliza para la inter-dominio de enrutamiento. Es similar a la de enrutamiento de vector de distancia. En ruta de enrutamiento de vector asumimos que hay un nodo (puede haber muchos) en cada sistema autónomo que actúa en nombre del sistema autónomo completo. Este nodo se denomina nodo altavoz. El nodo de altavoz crea una tabla de enrutamiento y anuncia que a los ganglios vecinos altavoz en la vecina sistemas autónomos. La idea es la misma de enrutamiento de vector de distancia, salvo que los nodos único orador en cada sistema autónomo pueden comunicarse entre sí.

El nodo de altavoz anuncia que el camino no, la métrica de los nodos, en su sistema autónomo o en otros sistemas autónomos. Camino de enrutamiento por vector se discute en el RFC 1322 , la ruta de enrutamiento vector algoritmo es algo similar al algoritmo de vector de distancia en el sentido de que cada router de borde de publicidad de los destinos que puede llegar a su router vecino. Sin embargo, en lugar de redes de publicidad en términos de un destino y la distancia a ese destino, las redes se anuncian como las direcciones de destino y las descripciones de camino para llegar a esos destinos. Una ruta se define como un enlace entre un destino y los atributos de la ruta a ese destino, de ahí el nombre, la ruta de enrutamiento por vector, en donde los routers reciben un vector que contiene las rutas a un conjunto de destinos. El camino, expresado en términos de los dominios (o confederaciones) atravesado hasta ahora, se realiza en un atributo de ruta especial que graba la secuencia de los dominios de enrutamiento a través del cual la información de accesibilidad ha pasado.

Comparación de algoritmos de encaminamiento

Vector-distancia Los protocolos de enrutamiento son simples y eficientes en las redes de pequeñas y requieren poca o ninguna, de gestión. Sin embargo, la tradicional distancia-vector algoritmos pobres [convergencia](#) propiedades debido al problema de la cuenta hasta el infinito .

Esto ha llevado al desarrollo de algoritmos más complejos pero más escalable para su uso en grandes redes. Interior de enrutamiento utiliza sobre todo [del estado de enlace los protocolos de enrutamiento](#) como OSPF y [IS-IS](#) .

Un desarrollo más reciente es el de los bucles de vector de distancia protocolos (por ejemplo, EIGRP). Sin bucles de vector de distancia protocolos son tan robustos y manejables como ingenua distancia-vector protocolos, pero no contar hasta el infinito, y tienen buenas peor de los casos [los tiempos de convergencia](#) .

Selección de Ruta

Selección de la ruta consiste en aplicar una [métrica de enrutamiento](#) de rutas múltiples, a fin de seleccionar (o predecir) la mejor ruta.

En el caso de redes de ordenadores, la métrica se calcula mediante un algoritmo de enrutamiento, y puede cubrir la información, tales como [ancho de banda](#) , [retardo en la red](#) , [el número de saltos](#) , coste de la ruta, carga, MTU coste, fiabilidad, y la comunicación (véase, por ejemplo esta encuesta para obtener una lista de las propuestas de las métricas de enrutamiento). La tabla de enrutamiento sólo almacena las mejores rutas posibles, mientras que del estado de enlace o bases de datos topológicos pueden almacenar toda la información también.

Debido a que una métrica de enrutamiento es específica para un determinado protocolo de enrutamiento multiprotocolo routers deben utilizar algunos heurísticos externos con el fin de seleccionar entre las rutas aprendidas de diferentes protocolos de enrutamiento. Cisco routers 's, por ejemplo, atribuir un valor conocido como la [distancia administrativa](#) de cada ruta, donde los pequeños distancias administrativas indican las rutas aprendidas de un protocolo supuestamente más fiables.

Un administrador de red local, en casos especiales, puede configurar las rutas de acogida específicos para una determinada máquina, que proporciona más control sobre el uso de la red, permite realizar pruebas y una mayor seguridad en general. Esto puede ser útil cuando sea necesario para depurar las conexiones de red o las tablas de enrutamiento

1.4.3 Características

Esquemas de encaminamiento difieren en su semántica de entrega:

- [Unicast](#) envía un mensaje a un nodo específico único;
- Difusión entrega un mensaje a todos los nodos de la red;
- Multicast envía un mensaje a un grupo de nodos que han expresado interés en recibir el mensaje;
- Anycast entrega un mensaje a cualquiera a uno de un grupo de nodos, por lo general más cercana la una a la fuente.
- Geocast entrega un mensaje a un área geográfica

Unicast es la forma dominante de la entrega de mensajes a través de Internet, y este artículo se centra en los algoritmos de enrutamiento de unidifusión

1.5 PROTOCOLOS DE TRANSMISION

1.5.1 Definición

Un **protocolo de enrutamiento** es un [protocolo](#) que especifica cómo [los routers](#) se comunican entre otra información, la difusión que les permite seleccionar las rutas entre dos [nodos](#) en una [red informática](#) , la elección de la ruta se realiza por [algoritmos de encaminamiento](#) . Cada router tiene un conocimiento a priori sólo de las redes conectadas directamente a ella. Un protocolo de enrutamiento de la información en primer lugar entre los vecinos inmediatos, y luego en toda la red de acciones. De esta manera, los routers de tener conocimiento de la topología de la red. Para una discusión de los conceptos detrás de los protocolos de enrutamiento, consulte: [Enrutamiento](#) .

El término **protocolo de enrutamiento** puede referirse específicamente a una operación en tres capas del [modelo OSI](#) , que de igual forma difunde información de topología entre los routers.

Aunque hay muchos tipos de protocolos de enrutamiento, tres clases principales son de uso generalizado en [IP](#) de redes:

- [Puerta de entrada de enrutamiento interior](#) a través de [protocolos de enrutamiento de estado de enlace](#) , como [OSPF](#) e [IS-IS](#)
- [Puerta de entrada de enrutamiento interior](#) por [vector de camino](#) o [de vector de distancia](#) protocolos, como [RIP](#) , [IGRP](#) y [EIGRP](#)
- [Exterior Gateway Routing](#) . [BGP](#) v4 es el protocolo de enrutamiento utilizado por el público en [Internet](#) .

Muchos protocolos de enrutamiento se definen en los documentos llamados [RFC](#).

Las características específicas de protocolos de enrutamiento incluyen

- La manera en que o bien prevenir los bucles de enrutamiento de la formación o rotura de los mismos por si lo hacen
- La manera en que seleccionan las rutas preferidas, con información sobre los costos hop

- El tiempo que tardan en [convergencia](#)
- Lo bien que [escala](#) hasta

Un protocolo enrutado se pueden dirigir por un router, es decir, que puede ser transmitido de un router a otro. Un protocolo de enrutamiento envía y recibe paquetes que contienen la información de enrutamiento y de otros routers.

En algunos casos, los protocolos de enrutamiento pueden ejecutar más de protocolos de enrutamiento, por ejemplo, [BGP](#) corre sobre [TCP](#) que se ejecuta a través de IP, se tenga cuidado en la aplicación de estos sistemas no crear una dependencia circular entre la ruta y protocolos de enrutamiento. Que un protocolo de enrutamiento se ejecuta sobre el mecanismo de transporte en particular no significa que el protocolo de enrutamiento de capa (N +1) si el mecanismo de transporte de la capa (N). Los protocolos de enrutamiento, de acuerdo con el marco de enrutamiento OSI, son protocolos de la capa de gestión de la capa de red, independientemente de su mecanismo de transporte:

- [IS-IS](#) se ejecuta sobre la capa de enlace de datos
- [OSPF](#) , [IGRP](#) y [EIGRP](#) se ejecutan directamente sobre IP, OSPF y EIGRP tienen su propio mecanismo de transmisión confiable, mientras que IGRP supone un transporte poco fiable
- [RIP](#) se ejecuta sobre [UDP](#)
- [BGP](#) corre sobre [TCP](#)

Interior Gateway Protocols (IGP) el intercambio de información de enrutamiento dentro de un mismo [dominio de enrutamiento](#) . Un determinado [sistema autónomo](#) ^[5] puede contener múltiples dominios de enrutamiento, o un conjunto de dominios de enrutamiento se pueden coordinar sin un sistema de Internet que participan autónoma. Los ejemplos más comunes incluyen:

- [IGRP](#) (Interior Gateway Routing Protocol)
- [EIGRP](#) (Enhanced Interior Gateway Routing Protocol)
- [OSPF](#) (Open Shortest Path First)
- [RIP](#) (Protocolo de Información de Enrutamiento)

- [IS-IS](#) (Sistema Intermedio a Sistema Intermedio)

Tenga en cuenta que IGRP, un protocolo de enrutamiento propietario de Cisco, ya no es compatible. EIGRP IGRP acepta comandos de configuración, pero la parte interna de IGRP y EIGRP son completamente diferentes.

Enrutamiento estático

Enrutamiento estático es una [comunicación de datos](#) concepto que describe una forma de configurar [la selección de rutas](#) de [los enrutadores](#) en [las redes de computadoras](#) . Es el tipo de [ruta](#) se caracteriza por la ausencia de comunicación entre los routers con respecto a la actual [topología](#) de la [red](#) . ^[1] Esto se logra agregando manualmente las [rutas](#) a la tabla de enrutamiento. Lo contrario de enrutamiento estático es [el enrutamiento dinámico](#) , a veces también se conoce como adaptación de enrutamiento.

En estos sistemas, las rutas a través de una red de datos se describen en rutas fijas (estática). Estas rutas suelen ser introducido en el router por el administrador del sistema. Toda una red se puede configurar mediante rutas estáticas, pero este tipo de configuración no es tolerante a fallos. Cuando hay un cambio en la red o se produce un fallo entre dos nodos estáticamente definido, el tráfico no será desviado. Esto significa que cualquier cosa que quiera tomar una ruta de afectados tendrán que esperar a que el hecho de no ser reparado o la ruta estática que se actualizará por el administrador antes de reiniciar su viaje. La mayoría de las solicitudes será el tiempo de espera (en última instancia, en su defecto) antes de que estas reparaciones se pueden hacer. Hay, sin embargo, ocasiones en las rutas estáticas se puede mejorar el rendimiento de una red. Algunos de estos incluyen [las redes de talón](#) y [las rutas por defecto](#)

Encaminamiento adaptativo

Encaminamiento adaptativo describe la capacidad de un sistema, a través de las rutas que se caracterizan por su destino, para modificar la ruta que toma la ruta a través del sistema en respuesta a un cambio en las condiciones. ^[1] La adaptación está destinada a permitir las rutas hasta posible para conservar su validez (es decir, tienen destinos que se puede llegar), en respuesta a los cambios.

Las personas que usan un sistema de transporte puede mostrar encaminamiento adaptativo. Por ejemplo, si una estación de ferrocarril local está cerrado, la gente puede bajarse de un tren en una estación diferente y utilice otro método, como un autobús, para llegar a su destino. Otro ejemplo de adaptación de enrutamiento puede ser visto dentro de [los mercados financieros](#) . Por ejemplo, ASOR o Router adaptable Orden Inteligente (desarrollado por [Quod financieros](#)), toma decisiones de enrutamiento de forma dinámica y basada en los acontecimientos del mercado en tiempo real.

El término es comúnmente utilizado en redes de datos para describir la capacidad de una red de 'recorrido por "daños, tales como la pérdida de un nodo o una conexión entre los nodos, en tanto que otras opciones de ruta están disponibles. Hay varios protocolos utilizados para lograr esto:

- [RIP](#)
- OSPF
- [IS-IS](#)
- IGRP / EIGRP

Sistemas que no implementan la adaptación de enrutamiento se describen como el uso de [enrutamiento estático](#) , donde las rutas a través de una red se describen por rutas fijas (estática). A cambio, como la pérdida de un nodo, o la pérdida de una conexión entre los nodos, no se compensa. Esto significa que cualquier cosa que quiera tomar una ruta de afectados tendrán que esperar a que el hecho de no ser reparado antes de reiniciar su viaje, o tendrá que dejar de llegar a su destino y abandonar el viaje

CAPITULO II

TRABAJO DE CAMPO

1. EL MINISTERIO DE AGRICULTURA GANADERIA, ACUACULTURA Y PESCA DE COTOPAXI.

1.1. Diseño de la investigación

El tipo de investigación aplicada para este trabajo, está basada en la investigación cuasi experimental ya que los ambientes de pruebas y la información a transmitir en estos no serán tomados al azar, sino que están previamente establecidos en ambientes de prueba.

Para este proyecto se utilizarán los siguientes métodos de investigación.

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

Las siguientes consideraciones fueron tomadas en cuenta para realizar esta investigación:

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

- Se plantean los objetivos de la investigación que permitirán resolver el problema de la falta de una metodología para determinar el protocolo que brindará mayor disponibilidad y menor porcentaje de pérdida de datos en los ambientes cisco y Linux planteados anteriormente.
- Se justifica los motivos por los cuales se propone realizar la presente investigación.
- Se elabora un marco teórico que permita tener una visión general para la realización del trabajo.
- Se plantea una hipótesis la cual es una posible respuesta al problema planteado.
- Se propone la operacionalización de las variables en base a la hipótesis planteada.
- Se realiza la recolección de datos de los índices e indicadores respectivos mediante las estadísticas de las interfaces de los equipos terminales.
- Se verifica la hipótesis con los resultados obtenidos.
- Se deducen las conclusiones y recomendaciones después de realizada la investigación.

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

Además se utilizará las técnicas que se detallan a continuación:

- Revisión Bibliográfica
- Pruebas
- Lluvia de ideas

- Recopilación de información.
- Y como fuentes de verificación se utilizarán:
- Información Bibliográfica y Linkográfica
- Transmisión de archivos
- Estadísticas de las Interfaces de los equipos clientes
- Simulación de los ambientes de prueba
- Analizador de tráfico
- Razonamiento

1.2. MAGAP Cotopaxi

La industria, agricultura, ganadería, el comercio y el transporte son los pilares que sustentan el desarrollo económico de Cotopaxi. Se suman la construcción, la floricultura, la artesanía y otras actividades que en 2007 generaron USD 991 millones según al Banco Central del Ecuador (BCE).

La industria es una de las principales generadoras de mano de obra y riqueza. Según Alberto Salvador, presidente de la Cámara de Industrias de Cotopaxi, este sector hace dos años obtuvo ingresos por USD 377 millones. El gremio tiene registradas a 37 empresas, pero Salvador indica que otras 30 firmas no están afiliadas.

Las industrias de Cotopaxi se dedican a la fabricación de productos de aluminio, acero, papel, harina, embutidos, curtiembre, cemento, generación eléctrica... También esta la agroindustria y lácteos.

Este desarrollo ocurrió, dice Salvador, porque en la década de 1970 hubo una política de descentralización de la producción a escala nacional. Se establecieron incentivos para que implantar industrias en otras provincias que no sean Guayas y Pichincha. Cotopaxi resultó favorecida.

Hoy la expectativa a corto o mediano plazo es mejorar la oferta industrial con la ampliación del aeropuerto internacional de carga y de pasajeros de Latacunga. Por ello, las cámaras de la producción plantearon al Gobierno que analice la posibilidad de que en el aeropuerto se establezca una zona franca. Esto ayudará al desarrollo de artesanías. El objetivo es exportar.

La agricultura y la ganadería generaron en 2007, USD 206 millones. Augusto Durán, técnico del Ministerio de Agricultura (Magap), asegura que en Cotopaxi existen 217 246 ovinos y 198 387 bovinos. La producción lechera es de 526 939 litros diarios que se comercializan en industrias locales y de otras provincias.

Además, cuenta con 29 497 ha de cultivos de plátano, café, cacao, caña de azúcar y cítricos en los cantones La Maná y Pangua. A esto se suma 52 230 ha de fréjol, arveja, maíz, papas, yuca y brócoli. “El 60% de la población se dedica a la agricultura”.

Asimismo, el actual Consejo Provincial puso en marcha el Plan de Desarrollo Provincial 2015 que tiene como ejes de desarrollo el fomento a la agricultura, vialidad, productividad y saneamiento ambiental.

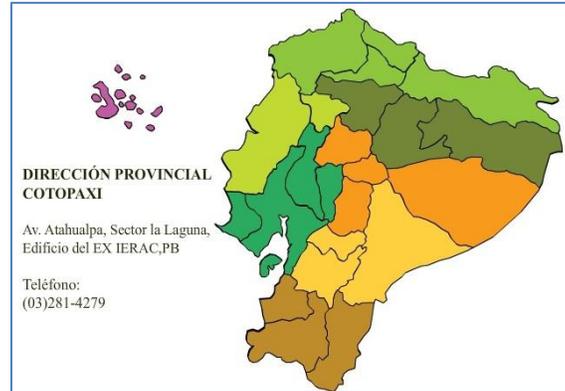
En cuanto a la actividad comercial, Iván Delgado, presidente de la Cámara de Comercio de Latacunga, detalla que la institución tiene 1 000 afiliados. El 60% son dueños de gasolineras, tiendas, panaderías, bares, hoteles, almacenes de electrodomésticos... Además hay 28 locales artesanales, 94 compañías y cooperativas de transporte y 21 avícolas. Todas generan el 55% de mano de obra directa e indirecta. En 2007, este sector obtuvo ingresos por USD 117 millones según el BCE.

En la Cámara de la Pequeña Industria están 1 000 socios. La mayoría se dedica a la fabricación de bloques, confección de ropa, lácteos, alimentos, turismo, servicios.

Otra actividad que sobresale es la producción de flores y brócoli. Oswaldo Coronel, gerente de la empresa Loco Farms, calcula que en Cotopaxi hay 700 ha de flores y 300 de brócoli para la exportación.

La siembra flores da empleo a 12 000 personas. El 80% es mano de obra directa y el resto indirecto. Cotopaxi aporta con el 25% de la producción nacional de flores.

Grafico 2.1.: Ubicación del MAGAP en Cotopaxi



1.3. Entrevistas realizadas a los directivos y empleados del MAGAP Cotopaxi.

En la actualidad las instituciones públicas se encuentran en un proceso de renovación profesional, personal y tecnológica por lo que se hace necesario estar acorde a los últimos avances, el MAGAP al ser un importante ministerio dentro de este aparato gubernamental ha sido blanco de críticas al estar un tanto quedado en el continuo devenir tecnológico.

Al ser decretado el estado de emergencia en el año 2009 por parte del gobierno de la revolución ciudadana se puso en marcha un proceso de actualización de quipos y personal que administre de mejor manera los recursos tanto en la matriz (Ciudad de Quito) como en todas las sucursales (provincias), lo que ha hecho que todos tengan que arrimar el hombro para poder estar acorde con todo lo solicitado desde la presidencia de la república y por los asesores del área de Informática y comunicaciones.

Con esta introducción que fue base de la entrevista con el señor. Ing. Segundo Chicaiza Director provincial del MAGAP en la ciudad de Latacunga provincia de Cotopaxi, se quiso poner en práctica lo manifestado configurado un equipo adquirido hace ya algún tiempo por

las oficinas de Cotopaxi y que se encontraba mal utilizado al ser ocupado como un simple switch sin administración o como simplemente un hub ya que la función de este era de repartir señal a todas las dependencias del MAGAP Cotopaxi únicamente.

1.3.1. Entrevista realizada al Director Provincial del MAGAP Cotopaxi

El Magap desde el año 2009 se encuentra en un franco procesos de actualización y automatización de sus procesos no solamente tecnológicos, ya que el gobierno nacional está comprometido en brindar un mejor nivel de vida a todos los habitantes de nuestro país.

Es necesario mencionar que el MAGAP siempre ha sido una institución que abierto sus puertas a todos los estudiantes y profesionales que deseen emprender acciones y proyectos que vayan en beneficio propio de ellos sus instituciones y empresas pero que siempre sean un aporte al país en su conjunto y que aporten para conseguir el buen vivir en esta tierra fértil y productiva llamada Ecuador.

En el ámbito tecnológico se debe manifestar que se cuenta con equipos de última generación bajo la administración de personas altamente capacidades que pueden brindar un soporte a los múltiples problemas que se puedan presentar, además que la institución está en capacidad de poder adquirir lo que sea necesario siempre y cuando vaya en beneficio de todos los empleados y supervisores que trabajan en las oficinas y que sirven para poder brindar un buen servicio a los usuarios de todos los servicios del ministerio en su sede de la ciudad de Latacunga.

1.3.2. Entrevista realizada al encargado del Área de Comunicaciones y Sistemas

Para la elaboración de un tema de investigación es necesario contar con la predisposición a la trabajo de todas las partes en el caso del MAGAP se está en capacidad de ofrecer todos los materiales como son los routers y los switch para que se pueda elaborar un análisis minucioso de todas las partes que componen una red WAN institucional siempre y cuando

se pueda precautelar toda la información del Ministerio esto porque siempre se puede ser flanco de intrusos o de instrucciones maliciosas que puedan afectar el normal funcionamiento de los equipos y de los sistemas.

Para la investigación de igual manera se considera indispensable el uso de los protocolos de alta disponibilidad ya que típicamente existe un tiempo de inactividad que es perjudicial para la operación del sistema y usualmente no puede ser evitado con la configuración de los sistemas actuales. Eventos que generan tiempos de inactividad quizás incluyen parches al software del sistema que requieran un rearranque o cambios en la configuración del sistema que toman efecto después de un rearranque. En general el tiempo de inactividad planificado es usualmente el resultado de un evento lógico o de gestión iniciado.

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

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

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

- 99,9% = 43.8 minutos/mes u 8,76 horas/año ("tres nueves")

- 99,99% = 4.38 minutos/mes o 52.6 minutos/año ("cuatro nueves")
- 99,999% = 0.44 minutos/mes o 5.26 minutos/año ("cinco nueves")

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

De la misma manera se debe mencionar algunas de las características de las configuraciones debe tener y que van a estar a consideración de la investigación esto con el fin de sacarle provecho a los equipos y precautelar toda la información que se genera tanto en Quito como en Latacunga.

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

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

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

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

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

1.3.3. Encuesta a los empleados del MAGAP Cotopaxi

La encuesta a los empleados se realiza de acuerdo a las actividades que éstos realizan dentro de la institución, este dato se obtuvo de la información recopilada permitirá conocer la disposición de productos para los clientes ante la propuesta de la red WAN.

ANALISIS E INTERPRETACION DE RESULTADOS

Pregunta

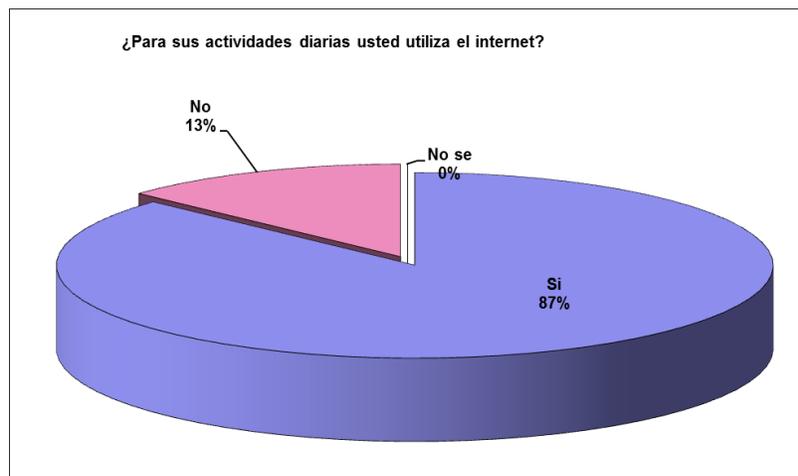
1.- ¿Para sus actividades diarias usted utiliza el internet?

Resultados

MINISTERIO DE AGRICULTURA GANADERIA ACUACULTURA Y PESCA			
PREGUNTA	Si	No	No se
¿Para sus actividades diarias usted utiliza el internet?	20	3	0

Interpretación de resultados

Grafico 2.2.: Resultados de las encuestas



Fuente: Los Investigadores

Análisis

El personal que labora en el MAGAP Cotopaxi considera importante contar con el servicio del internet para sus actividades profesionales ya que directamente tiene que ver con la información que se genera a través de este medio de comunicación, pero en algunos casos

puntuales como son los técnicos no requieren de esto ya que se desempeñan en el campo o en vistas técnicas en lugares que son fuera de las oficinas del MAGAP Cotopaxi.

Pregunta

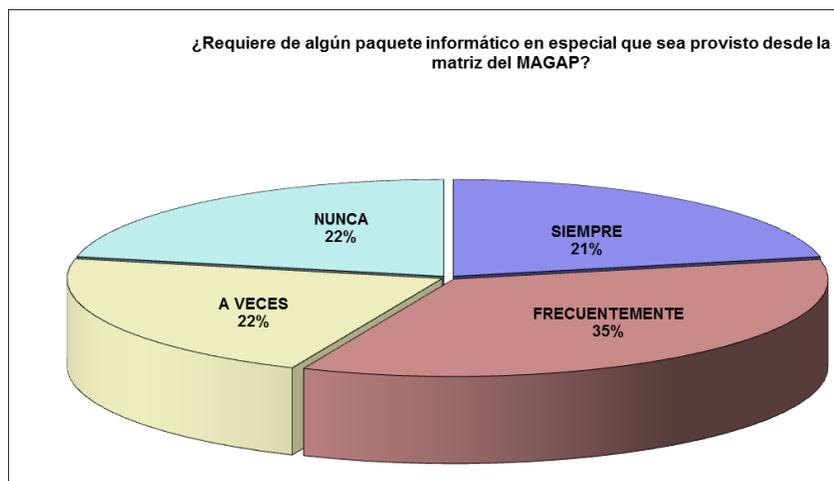
2.- ¿Requiere de algún paquete informático en especial que sea provisto desde la matriz del MAGAP?

Resultados

MINISTERIO DE AGRICULTURA GANADERIA ACUACULTURA Y PESCA				
PREGUNTA	SIEMPRE	FRECUENTEMENTE	A VECES	NUNCA
¿Requiere de algún paquete informático en especial que sea provisto desde la matriz del MAGAP?	5	8	5	5

Interpretación de resultados

Grafico 2.3.: Resultados de las encuestas



Fuente: Los investigadores

Análisis

Cuando se pregunta sobre las actividades que realizan los usuarios de los puntos de red institucional resultado que todos realizan funciones independientes y que en muchos casos no se requería de tener interconexión con Quito para poder desarrollar sus actividades profesionales, por lo que es importante que la navegación por el internet se controlado por

medio de un proxy para poder asegurar que los funcionarios desarrollen sus actividades que vayan en beneficio de la institución

Pregunta

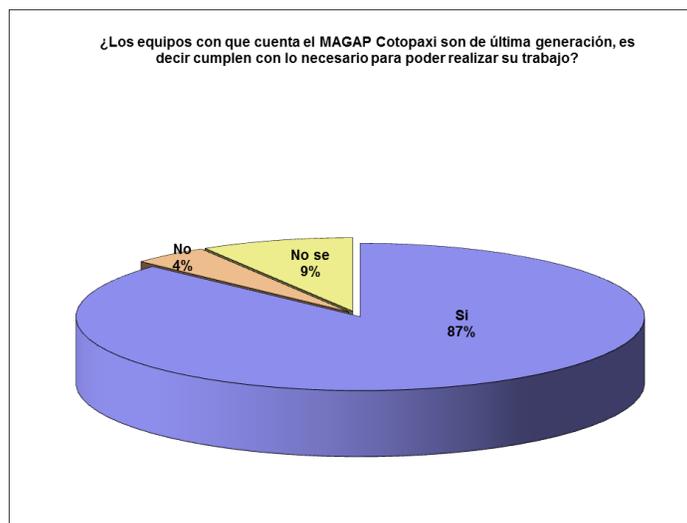
3.- ¿Los equipos con que cuenta el MAGAP Cotopaxi son de última generación, es decir cumplen con lo necesario para poder realizar su trabajo?

Resultados

MINISTERIO DE AGRICULTURA GANADERIA ACUACULTURA Y PESCA			
PREGUNTA	Si	No	No se
¿Los equipos con que cuenta el MAGAP Cotopaxi son de última generación, es decir cumplen con lo necesario para poder realizar su trabajo?	20	1	2

Interpretación de resultados

Grafico 2.4.: Resultados de las encuestas



Fuente: Los investigadores

Análisis

Un alto porcentaje considera que los equipos con los que cuenta la institución son de última generación pero sin embargo en un porcentaje más bien bajo han considerado que se puede mejorar el desempeño de sus actividades con equipos de mejores prestaciones tecnológicas.

Pregunta

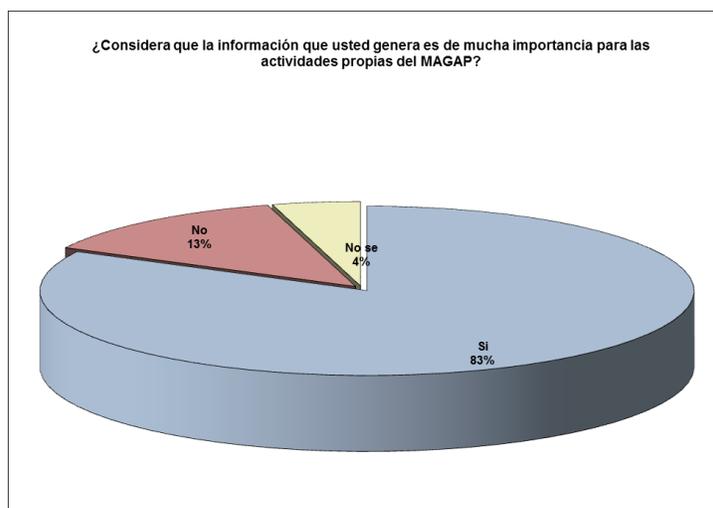
4.- ¿Considera que la información que usted genera es de mucha importancia para las actividades propias del MAGAP?

Resultados

MINISTERIO DE AGRICULTURA GANADERIA ACUACULTURA Y PESCA			
PREGUNTA	Si	No	No se
¿Considera que la información que usted genera es de mucha importancia para las actividades propias del MAGAP?	19	3	1

Interpretación de resultados

Grafico 2.5.: Resultados de las encuestas



Fuente: Los investigadores

Análisis

Cuando se pregunta si la información que se genera por cada uno de los empleados es de importancia para las actividades del MAGAP en un alto porcentaje mencionaron que es de vital importancia pero algunas personas están conscientes que la información generada se la

puede llevar de maneras alternativas y que no necesariamente son de vital importancia para el normal desarrollo de las actividades del ministerio.

Pregunta

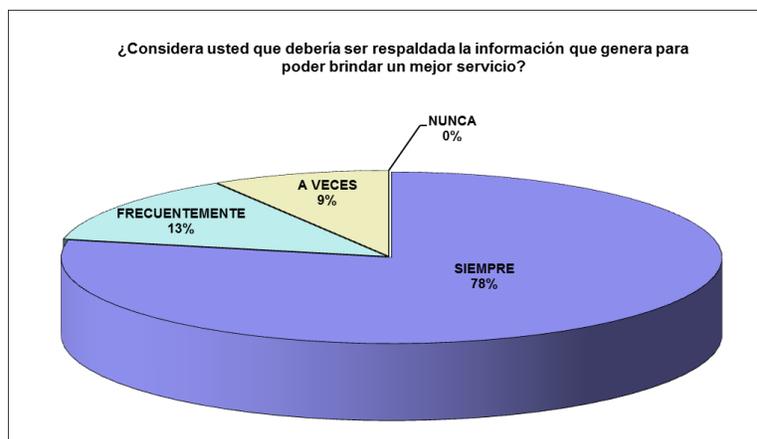
5.- ¿Considera usted que debería ser respaldada la información que genera para poder brindar un mejor servicio?

Resultados

MINISTERIO DE AGRICULTURA GANADERIA ACUACULTURA Y PESCA				
PREGUNTA	SIEMPRE	FRECUENTEMENTE	A VECES	NUNCA
¿Considera usted que debería ser respaldada la información que genera para poder brindar un mejor servicio?	18	3	2	0

Interpretación de resultados

Grafico 2.6.: Resultados de las encuestas



Fuente: Los investigadores

Análisis

Lo que si concuerdan todos es que la información debe ser respaldada para precautelar sus actividades lo que no se tiene claro es con que intervalos de tiempo se lo debe realizar, ya que estas actividades se las debe realizar con mucha frecuencia para algunos de los usuarios que tengan información que puede afectar al normal desempeño del ministerio en la sede de Latacunga.

Pregunta

6.- ¿Cuentan con adecuado soporte para sus actividades diarias en el área tecnológica, es decir su apoyo en el lugar de trabajo es el adecuado para su asesoría?

Resultados

MINISTERIO DE AGRICULTURA GANADERIA ACUACULTURA Y PESCA			
PREGUNTA	Si	No	No se
¿Cuentan con adecuado soporte para sus actividades diarias en el área tecnológica, es decir su apoyo en el lugar de trabajo es el adecuado para su asesoría?	22	1	0

Interpretación de resultados

Grafico 2.7.: Resultados de las encuestas



Fuente: Los investigadores

Análisis

Hoy en día todas las empresas e instituciones necesitan de un adecuado soporte para mejorar sus procesos pero siempre hace falta una adecuada capacitación para que se puedan defender los usuarios de forma adecuada, fue casi total la aceptación al desenvolvimiento de la persona que maneja las tecnologías en la institución.

Pregunta

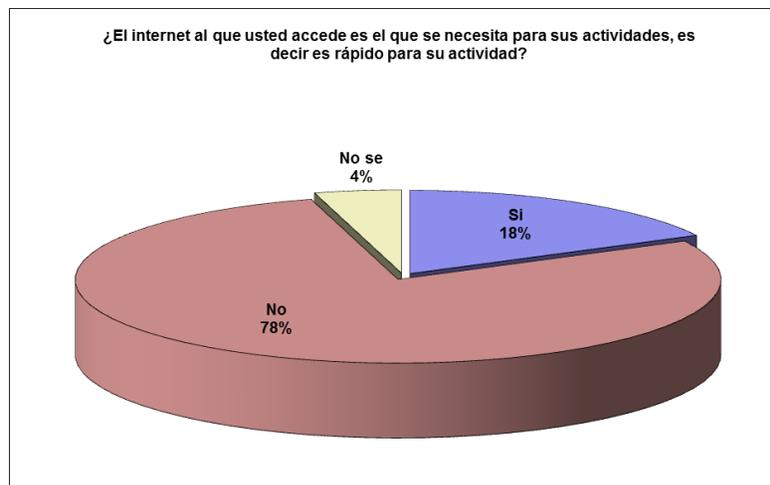
7.- ¿El internet al que usted accede es el que se necesita para sus actividades, es decir es rápido para su actividad?

Resultados

MINISTERIO DE AGRICULTURA GANADERIA ACUACULTURA Y PESCA			
PREGUNTA	Si	No	No se
¿El internet al que usted accede es el que se necesita para sus actividades, es decir es rápido para su actividad?	4	18	1

Interpretación de resultados

Grafico 2.8.: Resultados de las encuestas



Fuente: Los investigadores

Análisis

En la actualidad se dispone de conexiones por lo que se garantiza una buena comunicación por lo que casi es imperceptible el servicio de CNT pero por el ancho de banda que se asignara desde Quito todos los procesos y funciones deberían mejorar ostensiblemente

Pregunta

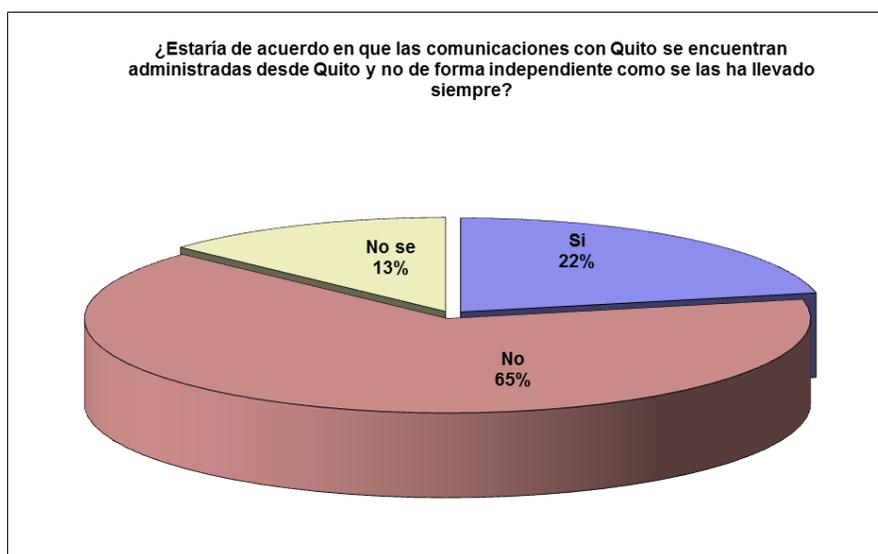
8.- ¿Estaría de acuerdo en que las comunicaciones con Quito se encuentran administradas desde Quito y no de forma independiente como se las ha llevado siempre?

Resultados

MINISTERIO DE AGRICULTURA GANADERIA ACUACULTURA Y PESCA			
PREGUNTA	Si	No	No se
¿Estaría de acuerdo en que las comunicaciones con Quito se encuentran administradas desde Quito y no de forma independiente como se las ha llevado siempre?	5	15	3

Interpretación de resultados

Grafico 2.9.: Resultados de las encuestas



Fuente: Los investigadores

Análisis

Esta pregunta genera mucha resistencia ya que se piensa que puede haber mayor control a las actividades que se realizan en las computadoras pero lo que se quiere es únicamente brindar un mejor ancho de banda y fidelidad en la información que se genera en Latacunga y se almacena en Quito.

Pregunta

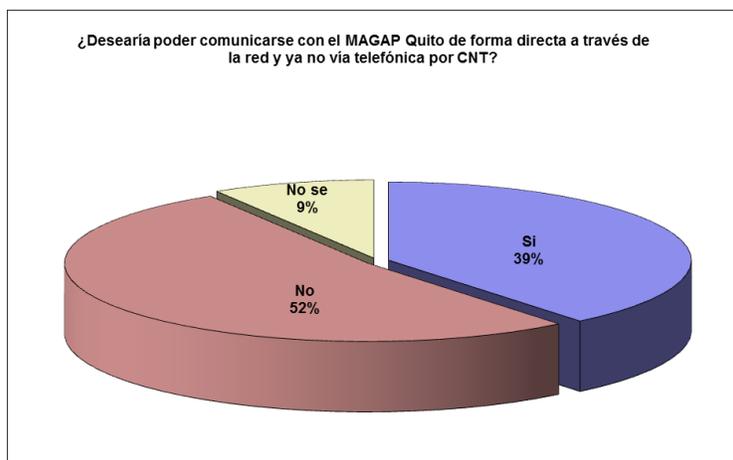
9.- ¿Desearía poder comunicarse con el MAGAP Quito de forma directa a través de la red y ya no vía telefónica por CNT?

Resultados

MINISTERIO DE AGRICULTURA GANADERIA ACUACULTURA Y PESCA			
PREGUNTA	Si	No	No se
¿Desearía poder comunicarse con el MAGAP Quito de forma directa a través de la red y ya no vía telefónica por CNT?	9	12	2

Interpretación de resultados

Grafico 2.10.: Resultados de las encuestas



Fuente: Los investigadores

Análisis

Una de las ventajas que se tiene de interconectar las dos ciudades es que se tiene la alternativa de poder utilizar las líneas telefónicas como extensiones entre todas las ciudades que se encuentren conectadas con esto existe alguna manera de ahorro económico, y que puede ser aprovechado en la misma área pero para otras funciones.

Pregunta

10.- ¿Con la información centralizada usted se sentiría más respaldada en sus actividades diarias?

Resultados

MINISTERIO DE AGRICULTURA GANADERIA ACUACULTURA Y PESCA			
PREGUNTA	Si	No	No se
¿Con la información centralizada usted se sentiría más respaldada en sus actividades diarias?	5	15	3

Interpretación de resultados

Grafico 2.11.: Resultados de las encuestas



Fuente: Los investigadores

Análisis

La centralización siempre deja una gran tela de dudas ya que se cree como en la pregunta 8 de que habrá un gran control y la mayoría concuerda es que la tendencia es descentralizar todo en el país y que no se entiende porque solo este ministerio se encuentra en estos

procesos si son de los más trabajadores y que no están de acuerdo con la decisión tomada unilateralmente.

1.4. Comprobación de la Hipótesis

Para el proyecto de grado se había planteado como hipótesis:

“Analizar los protocolos de Alta disponibilidad de Gateways en la interconectividad LAN/WAN aplicada al diseño de la red del MAGAP Cotopaxi”.

Los protocolos de alta disponibilidad permiten administrar dinámicamente la redundancia en el gateway. Todos ellos se centran en la utilización de una dirección IP y una MAC virtuales que definen un "gateway virtual" el que está disponible al intercambio de mensajes de hello entre los diferentes dispositivos adheridos al mismo gateway virtual.

CAPITULO III

PROPUESTA

1.5. TEMA

ANALISIS DE LOS PROTOCOLOS DE ALTA DISPONIBILIDAD DE GATEWAYS EN LA INTERCONECTIVIDAD LAN/WAN APLICADAS AL DISEÑO DE LA RED DEL MAGAP COTOPAXI.

1.6. Presentación

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

Los routers maestros tienen una prioridad de 255 y los de respaldo entre 1 y 254.

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

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

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

Esto redirige los paquetes del maestro caído al router maestro actual. En los casos en los que los routers de respaldo tengan toda la misma prioridad, el router de respaldo con la dirección IP más alta se convierte en el router maestro.

Todos los routers físicos que actúan como router virtual tienen que estar a un salto entre ellos. La comunicación dentro del router virtual se realiza periódicamente.

Este periodo puede ajustarse cambiando el intervalo de anuncio. Cuanto más corto sea el tiempo de agujero negro será más pequeño a cambio de un aumento del tráfico de red.

La seguridad se realiza respondiendo únicamente a los paquetes de primer salto, aunque se ofrecen otros mecanismos para su refuerzo, en particular para ataques locales.

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

1.7. Objetivos

1.7.1. Objetivo General

Analizar los protocolos de Alta disponibilidad en Gateways para la interconectividad LAN/WAN aplicadas al diseño de la red del Ministerio de Agricultura Acuicultura y Pesca (MAGAP) Cotopaxi.

1.7.2. Objetivos Específicos

- ✓ Analizar el fundamento teórico del tema de investigación para entender, conocer y disponer toda la información de forma clara, precisa facilitando el desarrollo de un trabajo acorde al planteamiento realizado.
- ✓ Recopilar toda la información acerca del tema para interpretar la situación actual de la institución y de qué forma actuar frente a los resultados hallados.
- ✓ Incorporar un análisis en los routers del MAGAP Cotopaxi para precautelar la información que transmite desde y hacia la matriz.

1.8. Análisis de la situación actual del Router Cisco.

La funcionalidad del router es aplicable a una amplia gama de entornos de interconexión que pueden emplear diferentes políticas de seguridad. El protocolo debe exigir un mínimo

de configuración y sobrecarga en el funcionamiento inseguro, prever la autenticación fuerte cuando el aumento de la seguridad es necesario, y permitirá la integración de los nuevos mecanismos de seguridad sin romper la operación compatible.

Mas sin embargo en la actualidad el MAGAP tiene el Router sin funcionalidad alguna para lo que fue adquirido ya que en la actualidad solamente interconecta la red LAN del ministerio

1.9. Protocolos de autenticación

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

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

Grafico 3.1: Tabla de configuraciones par protocolo VRRP

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Auth Type				Adver Int								Checksum											
IP Address (1)																							
:																							
:																							
:																							
IP Address (n)																							
Authentication Data (1)																							

Fuente: Cisco Academy

En la figura anterior se puede observar la representación gráfica del protocolo VRRP que es el que administra los ruteadores y que se pueden definir de la siguiente manera:

- **Versión.-** Especifica la versión del protocolo VRRP de este paquete.
- **Tipo.-** Identifica el tipo de paquete VRRP, el único tipo de paquete definido en la versión del protocolo es ADVERTISEMENT, un paquete con protocolo desconocido debe ser rechazado.
- **ID Router Virtual.-** identifica el router virtual, este paquete está informando el estado para: Item de configuración en el rango 1-255(decimal). No hay por defecto
- **Prioridad.-** especifica la prioridad de envío del router VRRP para el router virtual. Los valores más altos iguales a la prioridad más alta. Este campo es un entero sin signo de 8 bits.
- **Descripción de campos Ip**
- **Dirección Origen.-** La primera dirección Ip del paquete de direcciones está siendo enviada por Normas Hidden.
- **Dirección Destino.-** La dirección IP multicast asignado por IANA para VRRP es 224.0.0.18. Este es un enlace local de alcance a la dirección multicast. El router no debe reenviar un datagrama con esta dirección destino independientemente de su TTL.
- **TTL.-** deberá ser fijado en 255. Si un router VRRP recibe un paquete con el TTL diferente a 255, debe descartar el paquete.
- **Protocolo.-** El número de protocolo Ip asignado por la IANA para VRRP es el 112(decimal).

1.10. Análisis de los protocolos de configuración de equipos CISCO

1.10.1. Protocolos HSRP

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

1.10.2. Funcionamiento del Protocolo HSRP en el MAGAP a nivel nacional

La mecánica es similar a la de los protocolos VRRP y CARP.

Supongamos que disponemos de una red que cuenta con dos routers redundantes, RouterA (Quito) y RouterBv(Latacunga). Dichos routers pueden estar en dos posibles estados diferentes: maestro (Quito) y respaldo (Latacunga). Ambos routers intercambian mensajes, concretamente del tipo HSRP hello, que le permiten a cada uno conocer el estado del otro. Estos mensajes utilizan la dirección multicast 224.0.0.2 y el puerto UDP 1985.

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

Elección del Router "maestro"

Para determinar cuál es el router maestro se establece una prioridad en cada router. La prioridad por defecto es 100. El router de mayor prioridad es el que se establecerá como activo. Hay que tener presente que HSRP no se limita a 2 routers, sino que soporta grupos

de routers que trabajen en conjunto de modo que se dispondría de múltiples routers actuando como respaldo en situación de espera.

1.10.3. Configuraciones

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

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

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

Grafico 3.2: Tabla de configuraciones par protocolo HSRP

MAC header				IP header				UDP packet				HSRP packet			
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
Version								Opcode							
Holdtime								Priority							
Authentication Data															
-															
Virtual IP Address															
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
State								Hellotime							
Group								reserved							
Authentication Data															
-															
Virtual IP Address															

Fuente: Cisco Academy

Descripción de campos

- **Versión** (8 bits): Número de versión HSRP
- **Código operación** (8 bits): Operación que se llevará a cabo.

Grafico 3.3: Descripción de configuraciones routers cisco

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

Fuente: Cisco Academy

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

Grafico 3.4: Descripción de configuraciones routers cisco

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

Fuente: Cisco Academy

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

- **Holdtime** (8 bits) Defecto = 10 segundos. Contiene la cantidad de tiempo que el actual Hello debe ser considerado válido. El tiempo se da en segundos. Si un router envía un mensaje Hello, a continuación, los receptores deberían considerar la validez en el tiempo Holdtime. El Holdtime debe ser de al menos tres veces el valor del Hellotime.
- **Prioridad** (8 bits) Este campo se utiliza para elegir a los routers activos y reservas. Al comparar las prioridades de los dos routers, gana el router con la prioridad más alta. En el caso de empate gana el de la dirección IP más grande.
- **Grupo** (8 bits) Este campo identifica el grupo de espera. Para Token Ring, los valores entre 0 y 2 inclusive son válidos. Para otros valores medios de comunicación entre 0 y 255 inclusive son válidos.
- **Reservados** (8 bits)
- **Datos de autenticación** (64 bits) Este campo contiene una contraseña de 8 caracteres reutilizados. Si no hay datos de autenticación se configura, el valor predeterminado recomendado es de 0x63 0x69 0x73 0x63 0x6F 0x00 0x00 0x00.
- **Dirección IP virtual** (32 bits) La dirección IP virtual utilizada por este grupo. Si la dirección IP virtual no está configurada en un router, entonces puede ser adquirida en el mensaje Hello desde el router activo. La dirección sólo se debe aprender si no se ha configurado la dirección y el mensaje Hello esta autenticado.

1.10.4. Aplicación del GLBP para el router del MAGAP Cotopaxi

Dentro de las configuraciones debemos tomar en cuenta los siguientes ítems de configuración para poder precautelar la información y la integridad de la información.

- **Active virtual gateway (AVG):** Los miembros de un grupo GLBP eligen un gateway para ser el AVG para aquel grupo. Otros miembros de grupo proporcionan el backup para el AVG si el AVG se vuelve no disponible.
- El AVG asigna una dirección MAC virtual a cada miembro del grupo.
- **Active virtual forwarder (AVF):** Cada gateway asume la responsabilidad para expedir (forwarding) paquetes enviados a la dirección de MAC virtual asignada por el AVG. Estos gateways son conocidos como AVFs por su dirección MAC virtual.
- **Comunicación:** Los miembros GLBP se comunican entre sí usando mensajes hello enviados cada 3 segundos a la dirección multicast 224.0.0.102, el Protocolo de Datagrama de Usuario (User datagram protocol: UDP) puerto 3222.

1.10.5. Funcionamiento e identificación del proceso de operación

GLBP permite la selección automática y el empleo simultáneo de todos los gateways disponibles en el grupo. Los miembros de un grupo GLBP eligen un gateway para ser el AVG para aquel grupo. Otros miembros del grupo proporcionan backup para el AVG si este se vuelve no disponible (unavailable).

El AVG asigna una dirección MAC virtual a cada miembro del grupo GLBP.

Todos los routers se vuelven AVFs para tramas dirigidas a aquella dirección MAC virtual. Como los clientes envían peticiones (requests) Address resolution Protocol (ARP) para la dirección del default gateway, el AVG envía estas direcciones MAC virtuales en las respuestas de ARP. Un grupo GLBP puede tener hasta cuatro miembros de grupo GLBP soporta los siguientes modos operacionales para el balanceo de tráfico de carga a través de múltiples routers que revisan la misma dirección IP de default gateway:

- **Algoritmo de balanceo de carga ponderado (Weighted load-balancing algorithm):** La cantidad de carga dirigida a un router es dependiente del valor ponderado anunciado por aquel router.
- **Algoritmo balanceo de carga de host dependiente (Host-dependent load-balancing algorithm):** Un host es garantizado para usar la misma dirección MAC virtual mientras aquella dirección MAC virtual está participando en el grupo GLBP.
- **Algoritmo balanceo de carga round-robin (Round-robin loadbalancing algorithm):** Como los clientes envían peticiones de ARP para resolver la dirección MAC de default gateway, la respuesta a cada cliente contiene la dirección MAC del próximo router posible en modo Roundrobin.
- Todas las direcciones MAC de los routers toman turnos siendo incluidos en respuestas de resolución de dirección para la dirección IP del default gateway.
- GLBP automáticamente maneja la asignación de dirección de MAC virtual, determina quien maneja el forwarding, y asegura que cada estación tiene una ruta de forwarding para fallas de gateways o interfaces rastreadas. Si ocurren fallas, el ratio de balanceo de carga es ajustado entre los AVFs restante para que los recursos sean usados del modo más eficiente.

Grafico 3.5: Descripción de configuraciones routers cisco

VIRTUAL IP				MAC ADDRESS				OWNER ID				GLBP PACKET			
------------	--	--	--	-------------	--	--	--	----------	--	--	--	-------------	--	--	--

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
<u>Holdtime</u>								<u>Priority</u>							
<u>Forwarder preempt</u>								<u>Load Balancing</u>							
Authentication Data															
.															
.															
Virtual IP Address															
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
<u>Hello time</u>								<u>Weighting</u>							
<u>State</u>								<u>Group</u>							
Authentication Data															
.															
.															
Virtual IP Address															

Fuente: Cisco Academy

Virtual Asignación de direcciones MAC

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

Virtual Gateway de redundancia

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

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

Prioridad de Gateway

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

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

Gateway de ponderación y de seguimiento

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

La ponderación de grupo GLBP puede ser ajustado automáticamente por el seguimiento del estado de una interfaz en el router. Si una interfaz de seguimiento se baja, la ponderación del grupo GLBP se reduce en un valor determinado.

Diferentes interfaces pueden ser rastreados para disminuir la ponderación GLBP por cantidades variables

Estándar de VRRP

Virtual Router Redundancy Protocol (VRRP) es un protocolo de redundancia no propietario definido en el RFC 2338 en Abril de 1998 y luego modificado en el RFC 3768 de Abril del 2004, diseñado para aumentar la disponibilidad de la puerta de enlace por defecto dando servicio a máquinas en la misma subred. El aumento de fiabilidad se consigue mediante el anuncio de un router virtual como una puerta de enlace por defecto en lugar de un router físico. Dos o más routers físicos se configuran representando al router virtual, con sólo uno de ellos realizando realmente el enrutamiento. Si el router físico actual que está realizando el enrutamiento falla, el otro router físico negocia para sustituirlo. Se denomina router maestro al router físico que realiza realmente el enrutamiento y routers de respaldo a los que están en espera de que el maestro falle.

Ámbito de Aplicación

En el RFC 2338 se describe las características, objetivos de diseño, y la teoría de operación de VRRP. Los formatos de mensaje, el protocolo de reglas de procesamiento y la máquina de estado para garantizar que se presenta la convergencia a un solo Router Virtual Maestro. Por último, las cuestiones operativas relacionadas con la asignación de direcciones MAC, el manejo de peticiones ARP, la generación de mensajes ICMP redirect, y los problemas de seguridad están dirigidas.

Este protocolo está diseñado para ser utilizado solamente con routers IPv4. Una especificación separada se producirá si se decide que una funcionalidad similar es deseable en un entorno IPv6.

Cambios del RFC 2338 en el 3768

Se han eliminado los métodos de autenticación de VRRP. Los cambios incluyen:

- Se ha quitado los valores de contraseña y la autenticación basada en IPSEC.
- Los campos y los valores se conservan para mantener la compatibilidad hacia atrás con la RFC 2338.
- Eliminada la sección sobre la seguridad extensibles
- Actualización de la seguridad considerando la sección para eliminar la discusión de distintos métodos de autenticación y añadir un nuevo texto que explica la motivación para el cambio y la descripción de las vulnerabilidades.

Estándar de HSRP

Hot Standby Router Protocol está definido en el estándar RFC 2281, un conjunto de routers trabajan en conjunto para presentar la ilusión de un único router virtual para los host de la LAN. Este conjunto se conoce como un HSRP o un grupo de espera. Un solo router electo del grupo es el encargado de transmitir los paquetes que los host envían al router virtual. Este router es conocido como el router activo. Otro router es elegido como el router de espera. En el caso de que el router activo falla, el que está en modo en espera asume las funciones de reenvío de paquetes del router activo. Aunque un número arbitrario de routers pueden funcionar HSRP, sólo el router activo envía los paquetes al router virtual.

Para minimizar el tráfico de red, sólo los routers activos y los routers de espera envían mensajes periódicos HSRP, una vez que el protocolo ha completado el proceso de elección. Si el router activo falla, el router standby asume el router activo. Si el router no espera o se convierte en el router activo, otro router es elegido como el router de espera.

En una LAN en particular, varios grupos de reserva pueden coexistir y superponerse.

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

Si se utilizan varios grupos en una sola LAN, la división de la carga se puede lograr mediante la distribución de los host de los diferentes grupos de reserva.

El resto de esta especificación describe el funcionamiento de un grupo de espera único. En el caso de varios grupos, cada grupo funciona de manera independiente de otros grupos de la LAN y de acuerdo con esta especificación. Tenga en cuenta que los routers individuales pueden participar en varios grupos. En este caso, el router mantiene el estado independiente y contadores de tiempo para cada grupo.

Condiciones de uso

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

Ámbito de aplicación

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

1.11. Redes de Campus

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

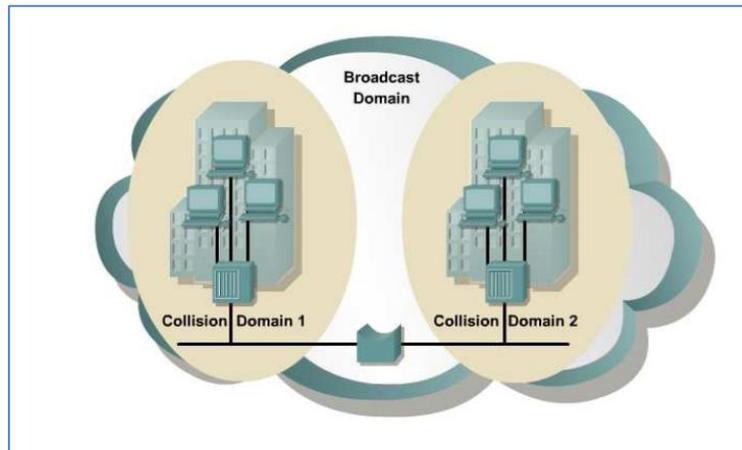
El área CAN (la Red de Área de Campus) es indudablemente más grande que una red del área local pero sigue siendo más pequeña una red del área amplia. Estas redes están diseñadas para un lugar en particular que incide el nivel más alto. Por ejemplo, varios laboratorios, oficinas múltiples en los edificios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

Las tradicionales redes de campus

En los primeros días de la creación de redes, principalmente las universidades de investigación y los militares experimentaron las redes informáticas. El término red del campus deriva de las redes construidas en los campus universitarios. Hoy en día, el término se utiliza más ampliamente para incluir redes que se extienden de las empresas "campus". El tamaño del Campus es un factor importante en el diseño de la red. Un campus grande tiene varios o muchos edificios localizados, un campus mediano es uno o algunos edificios co-localizados, mientras que un pequeño campus tiene un solo edificio.

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

Grafico 3.6: Redes de Campus

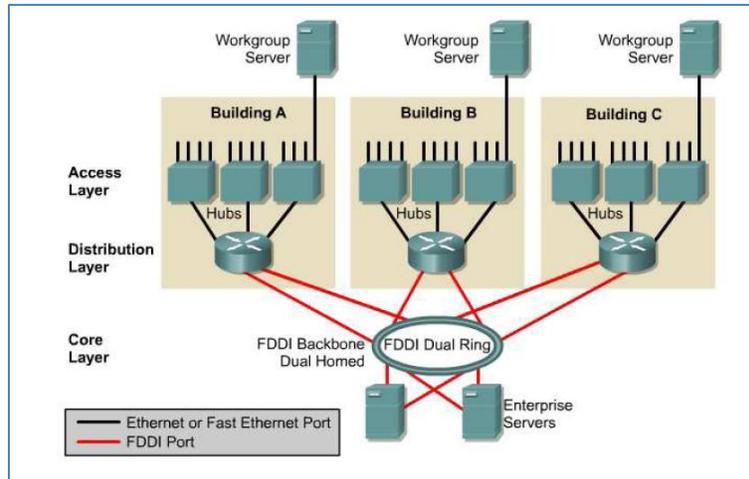


Fuente: Diseño de redes con equipo de Cisco Academy

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

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

Grafico 3.7: Descripción de configuraciones routers cisco



Fuente: Configuraciones en redes múltiples

1.12. Implementación de los protocolos basados en CISCO en el MAGAP de la provincia de Cotopaxi

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

Protocolo HSRP

Grafico 3.8: Ping a la dirección IP publica otorgada por CNT

```
C:\WINDOWS\system32\cmd.exe
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 14ms, Máximo = 20ms, Media = 18ms
Control-C
^C
C:\Documents and Settings\Usercisco>ping -t 172.168.1.5
Haciendo ping a 172.168.1.5 con 32 bytes de datos:
Respuesta desde 172.168.1.5: bytes=32 tiempo=16ms TTL=126
Respuesta desde 172.168.1.5: bytes=32 tiempo=15ms TTL=126
Respuesta desde 172.168.1.5: bytes=32 tiempo=15ms TTL=126
Respuesta desde 172.168.1.5: bytes=32 tiempo=15ms TTL=126
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 172.168.1.5: bytes=32 tiempo=20ms TTL=126
Estadísticas de ping para 172.168.1.5:
Paquetes: enviados = 13, recibidos = 11, perdidos = 2
(15% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 15ms, Máximo = 20ms, Media = 18ms
Control-C
^C
C:\Documents and Settings\Usercisco>
C:\Documents and Settings\Usercisco>
```

Fuente: Los Investigadores - CNT

Protocolo GLBP

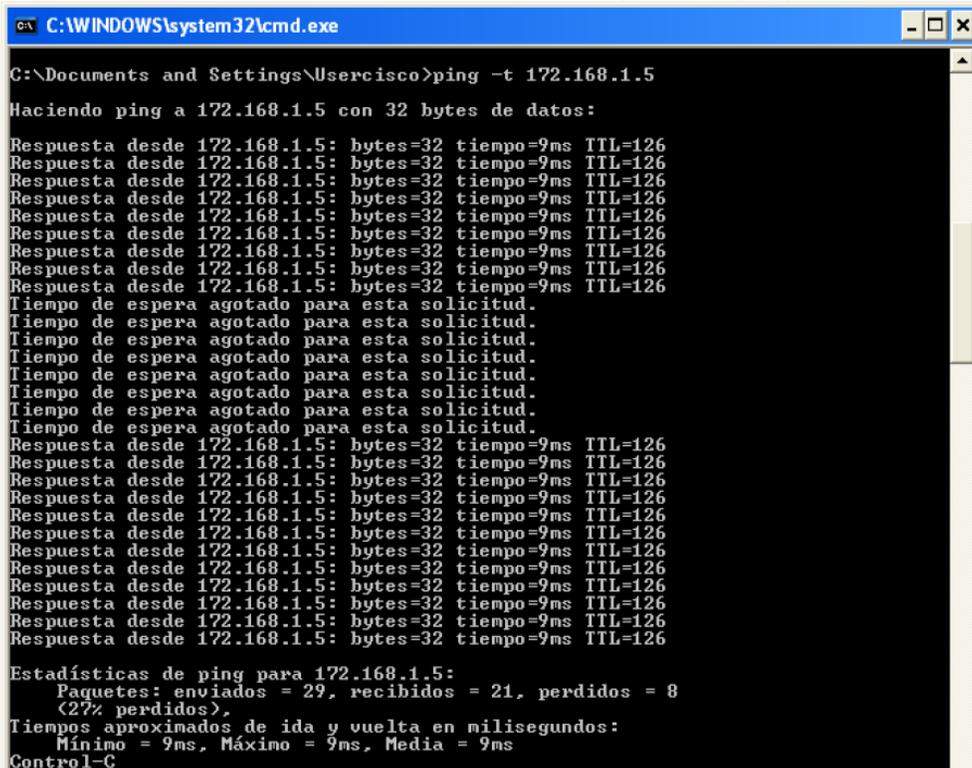
Grafico 3.9: Ping a la dirección IP publica otorgada por CNT(fidelidad probada)

```
C:\WINDOWS\system32\cmd.exe
3 ^C
C:\Documents and Settings\Usercisco>ping -t 172.168.1.5
Haciendo ping a 172.168.1.5 con 32 bytes de datos:
Respuesta desde 172.168.1.5: bytes=32 tiempo=20ms TTL=126
Tiempo de espera agotado para esta solicitud.
Respuesta desde 172.168.1.5: bytes=32 tiempo=20ms TTL=126
Estadísticas de ping para 172.168.1.5:
Paquetes: enviados = 33, recibidos = 32, perdidos = 1
(3% perdidos),
```

Fuente: Los Investigadores - CNT

Protocolo VRRP

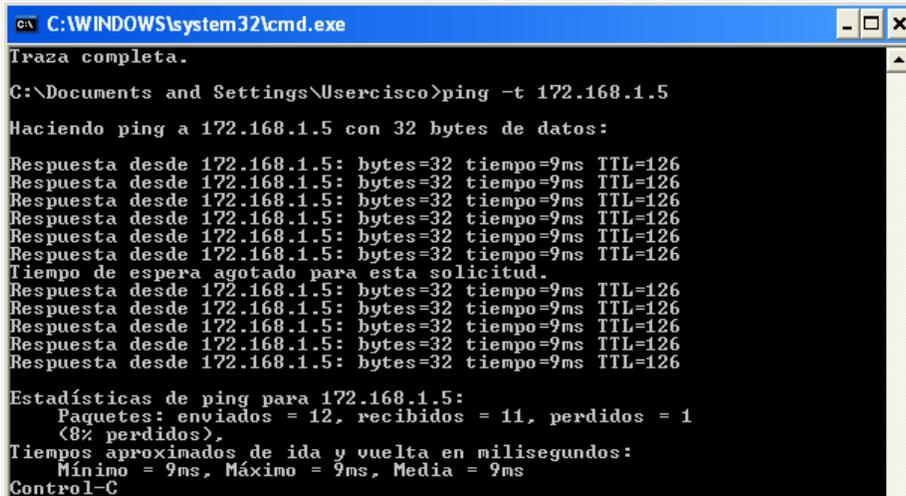
Grafico 3.10: Pruebas de conexión a la dirección IP publica otorgada por CNT



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Usercisco>ping -t 172.168.1.5
Haciendo ping a 172.168.1.5 con 32 bytes de datos:
Respuesta desde 172.168.1.5: bytes=32 tiempo=9ms TTL=126
Tiempo de espera agotado para esta solicitud.
Respuesta desde 172.168.1.5: bytes=32 tiempo=9ms TTL=126
Estadísticas de ping para 172.168.1.5:
    Paquetes: enviados = 29, recibidos = 21, perdidos = 8
    (27% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 9ms, Máximo = 9ms, Media = 9ms
Control-C
```

Fuente: Los Investigadores - CNT

Grafico 3.11: Pruebas de conexión a la dirección IP publica otorgada por CNT (fidelidad probada)



```
C:\WINDOWS\system32\cmd.exe
Traza completa.
C:\Documents and Settings\Usercisco>ping -t 172.168.1.5
Haciendo ping a 172.168.1.5 con 32 bytes de datos:
Respuesta desde 172.168.1.5: bytes=32 tiempo=9ms TTL=126
Tiempo de espera agotado para esta solicitud.
Respuesta desde 172.168.1.5: bytes=32 tiempo=9ms TTL=126
Estadísticas de ping para 172.168.1.5:
    Paquetes: enviados = 12, recibidos = 11, perdidos = 1
    (8% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 9ms, Máximo = 9ms, Media = 9ms
Control-C
```

Fuente: Los Investigadores - CNT

Grafico 3.12: Pruebas de conexión a la dirección IP publica reducción de tiempos

```
C:\Windows\system32\cmd.exe
C:\Users\SID>ping -t 192.168.1.5
Haciendo ping a 192.168.1.5 con 32 bytes de datos:
Respuesta desde 192.168.1.5: bytes=32 tiempo<1m TTL=126
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 192.168.1.5: bytes=32 tiempo<1m TTL=126
Estadísticas de ping para 192.168.1.5:
  Paquetes: enviados = 12, recibidos = 10, perdidos = 2
  (16% perdidos).
  Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
Control-C
^C
C:\Users\SID>
```

Fuente: Los Investigadores - CNT

Gráfico 3.13: Pruebas de conexión a la dirección IP pública reducción de tiempos (fidelidad probada)

```
C:\Windows\system32\cmd.exe
Control-C
^C
C:\Users\SID>ping -t 192.168.1.5
Haciendo ping a 192.168.1.5 con 32 bytes de datos:
Respuesta desde 192.168.1.5: bytes=32 tiempo=2ms TTL=126
Respuesta desde 192.168.1.5: bytes=32 tiempo<1m TTL=126
Respuesta desde 192.168.1.5: bytes=32 tiempo=17ms TTL=126
Respuesta desde 192.168.1.5: bytes=32 tiempo=1ms TTL=126
Respuesta desde 192.168.1.5: bytes=32 tiempo=2ms TTL=126
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 192.168.1.5: bytes=32 tiempo=3ms TTL=126
Respuesta desde 192.168.1.5: bytes=32 tiempo=3ms TTL=126
Respuesta desde 192.168.1.5: bytes=32 tiempo<1m TTL=126
Respuesta desde 192.168.1.5: bytes=32 tiempo=5ms TTL=126
Respuesta desde 192.168.1.5: bytes=32 tiempo<1m TTL=126
Estadísticas de ping para 192.168.1.5:
  Paquetes: enviados = 13, recibidos = 10, perdidos = 3
  (23% perdidos).
  Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 17ms, Media = 3ms
Control-C
```

Fuente: Los Investigadores - CNT

1.13. TRACERT

La segunda herramienta utilizada para el monitoreo, es mediante el comando **tracert dirección ip**, comando ampliamente utilizado para medir el tiempo que tarda un paquete en llegar desde un host (punto de red) a otro, el mismo que nos que permitirá detallar los nodos por los que pasa el paquete de datos antes de llegar a los recursos del servidor.

Grafico 3.14: Trazas desde la red LAN hacia la IP publica

```
C:\WINDOWS\system32\cmd.exe
Control-C
^C
C:\Documents and Settings\Usercisco>
C:\Documents and Settings\Usercisco>TRACERT 172.168.1.5
Traza a 172.168.1.5 sobre caminos de 30 saltos como máximo.

 1  <1 ms  <1 ms  <1 ms  192.168.4.2
 2  17 ms  16 ms  16 ms  172.168.50.2
 3  22 ms  21 ms  21 ms  172.168.1.5

Traza completa.
C:\Documents and Settings\Usercisco>
```

Fuente: Los Investigadores - CNT

Grafico 3.15: Traza del servidor Latacunga a la IP publica

```
C:\WINDOWS\system32\cmd.exe
Control-C
^C
C:\Documents and Settings\Usercisco>
C:\Documents and Settings\Usercisco>TRACERT 172.168.1.5
Traza a 172.168.1.5 sobre caminos de 30 saltos como máximo.

 1  <1 ms  <1 ms  <1 ms  192.168.4.1
 2  <1 ms  <1 ms  <1 ms  192.168.4.2
 3  17 ms  16 ms  16 ms  172.168.50.2
 4  22 ms  21 ms  21 ms  172.168.1.5

Traza completa.
C:\Documents and Settings\Usercisco>
```

Fuente: Los Investigadores - CNT

Protocolo HSRP

Grafico 3.16: Traza del cliente Latacunga a la IP publica

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Usercisco>tracert 172.168.1.5
Traza a 172.168.1.5 sobre caminos de 30 saltos como máximo.

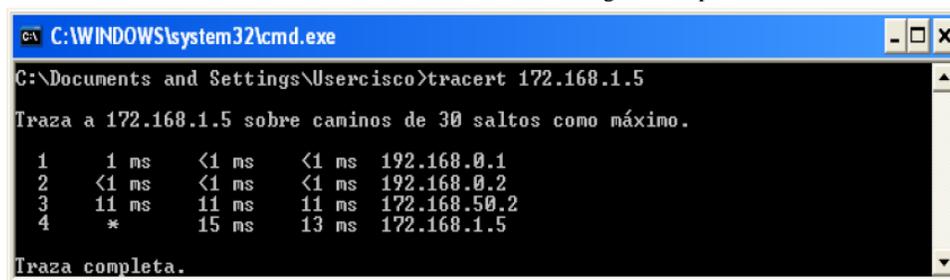
 1  <1 ms  <1 ms  <1 ms  192.168.0.2
 2  11 ms  11 ms  11 ms  172.168.50.2
 3  *      15 ms  13 ms  172.168.1.5

Traza completa.
```

Fuente: Los Investigadores - CNT

Protocolo GLBP

Grafico 3.17: Traza del servidor Latacunga a la IP publica



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Usercisco>tracert 172.168.1.5
Traza a 172.168.1.5 sobre caminos de 30 saltos como máximo.

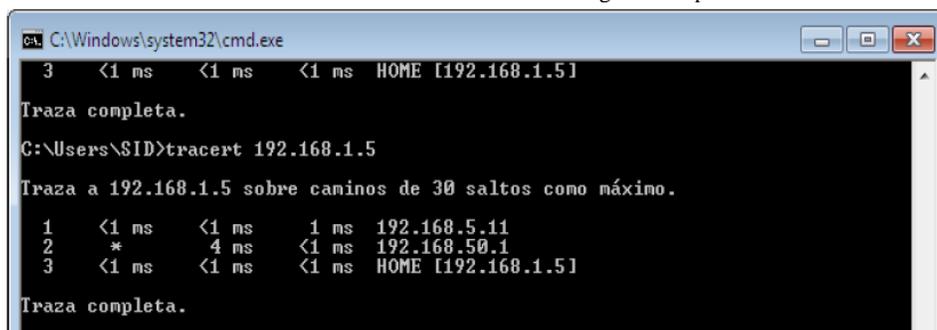
 1      1 ms    <1 ms    <1 ms    192.168.0.1
 2      <1 ms   <1 ms    <1 ms    192.168.0.2
 3     11 ms   11 ms   11 ms   172.168.50.2
 4      *     15 ms   13 ms   172.168.1.5

Traza completa.
```

Fuente: Los Investigadores - CNT

Protocolo VRRP

Grafico 3.18: Traza del servidor Latacunga a la IP publica



```
C:\Windows\system32\cmd.exe
3      <1 ms   <1 ms   <1 ms   HOME [192.168.1.5]

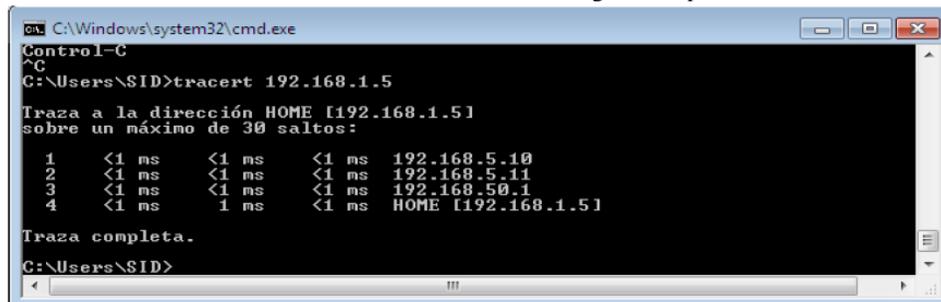
Traza completa.
C:\Users\SID>tracert 192.168.1.5
Traza a 192.168.1.5 sobre caminos de 30 saltos como máximo.

 1      <1 ms   <1 ms    1 ms    192.168.5.11
 2      *      4 ms    <1 ms   192.168.50.1
 3      <1 ms   <1 ms   <1 ms   HOME [192.168.1.5]

Traza completa.
```

Fuente: Los Investigadores - CNT

Grafico 3.19: Traza del cliente Latacunga a la IP publica



```
C:\Windows\system32\cmd.exe
Control-C
^C
C:\Users\SID>tracert 192.168.1.5
Traza a la dirección HOME [192.168.1.5]
sobre un máximo de 30 saltos:

 1      <1 ms   <1 ms   <1 ms   192.168.5.10
 2      <1 ms   <1 ms   <1 ms   192.168.5.11
 3      <1 ms   <1 ms   <1 ms   192.168.50.1
 4      <1 ms    1 ms    <1 ms   HOME [192.168.1.5]

Traza completa.
C:\Users\SID>
```

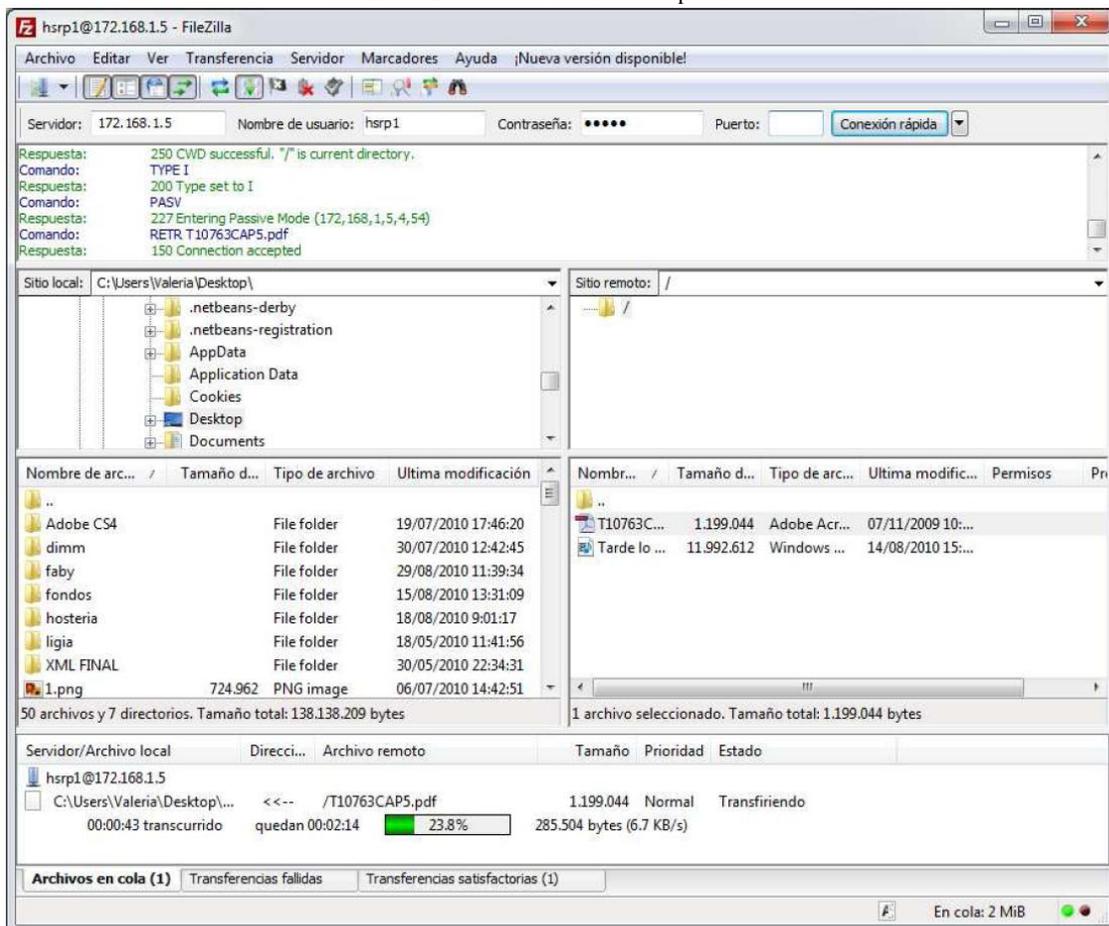
Fuente: Los Investigadores - CNT

1.14. FILEZILLA

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

Protocolo HSRP

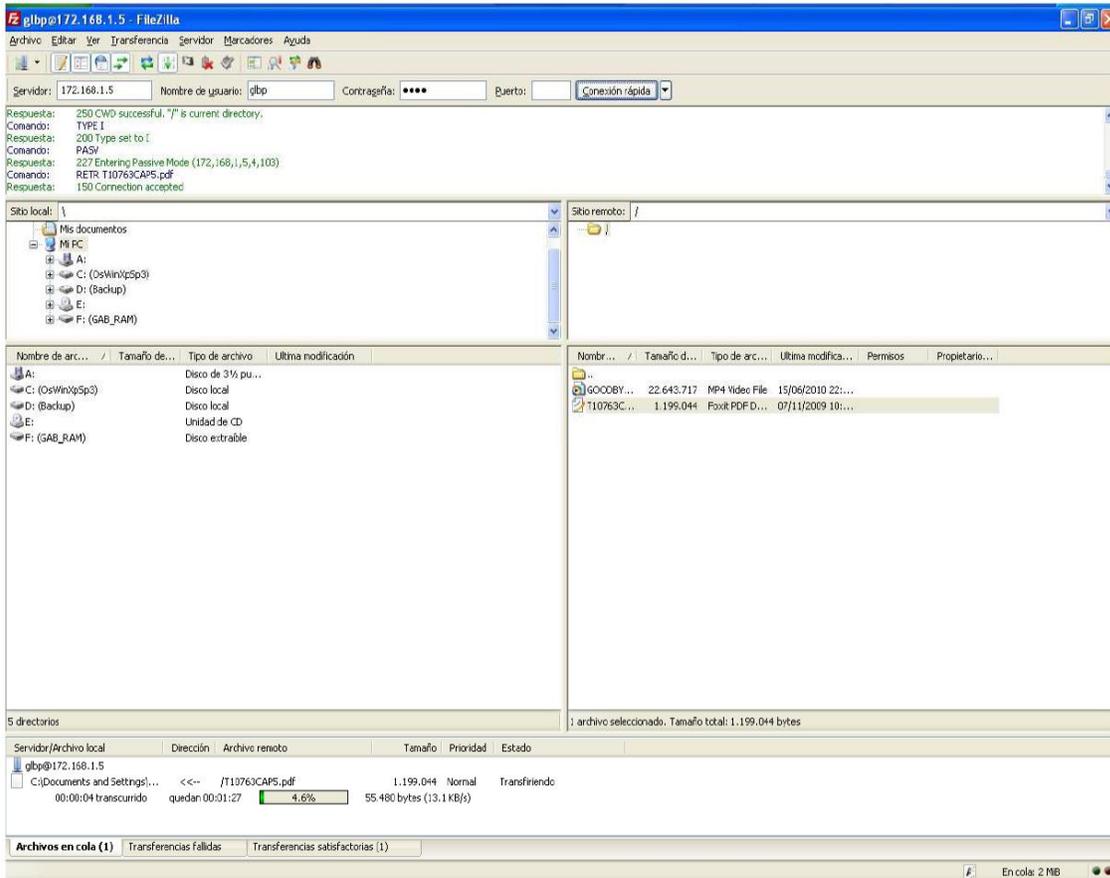
Grafico 3.20: Pruebas de envío/recepción de archivos



Fuente: Los Investigadores

Protocolo GLBP

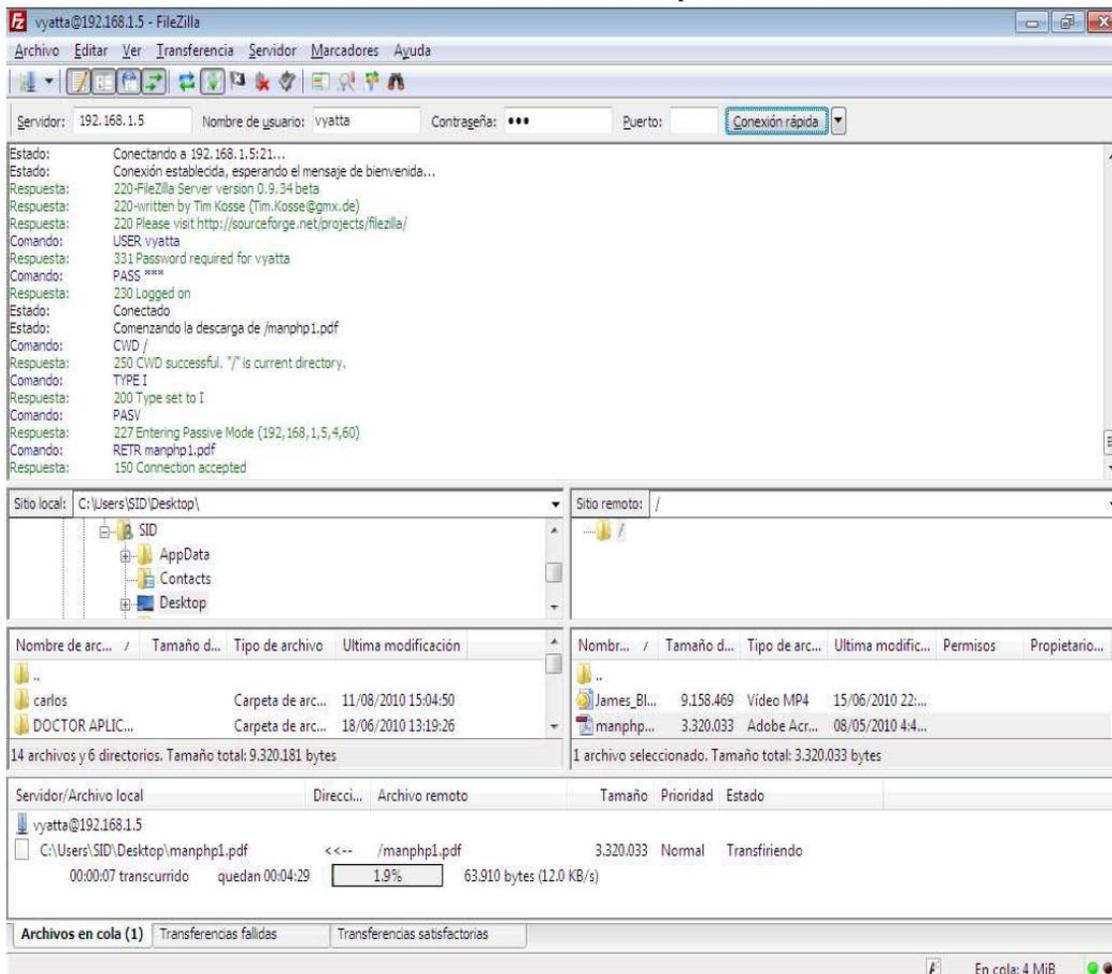
Grafico 3.21: Pruebas de envío/recepción de archivos



Fuente: Los Investigadores

Protocolo VRRP

Grafico 3.22: Pruebas de envío/recepción de archivos



Fuente: Los Investigadores

1.15. WIRESHARK

La cuarta herramienta utilizada para el monitoreo, es WireShark un analizador de protocolos utilizado para el análisis y solución de problemas en redes de comunicaciones para desarrollo de software y protocolos, la misma que nos permitirá determinar el equipo master y el equipo backup de cada uno de los protocolos, así como su dirección multicast.

Protocolo HSRP

Gráfico 3.23: Propiedades de ruteo mediante Wireshark

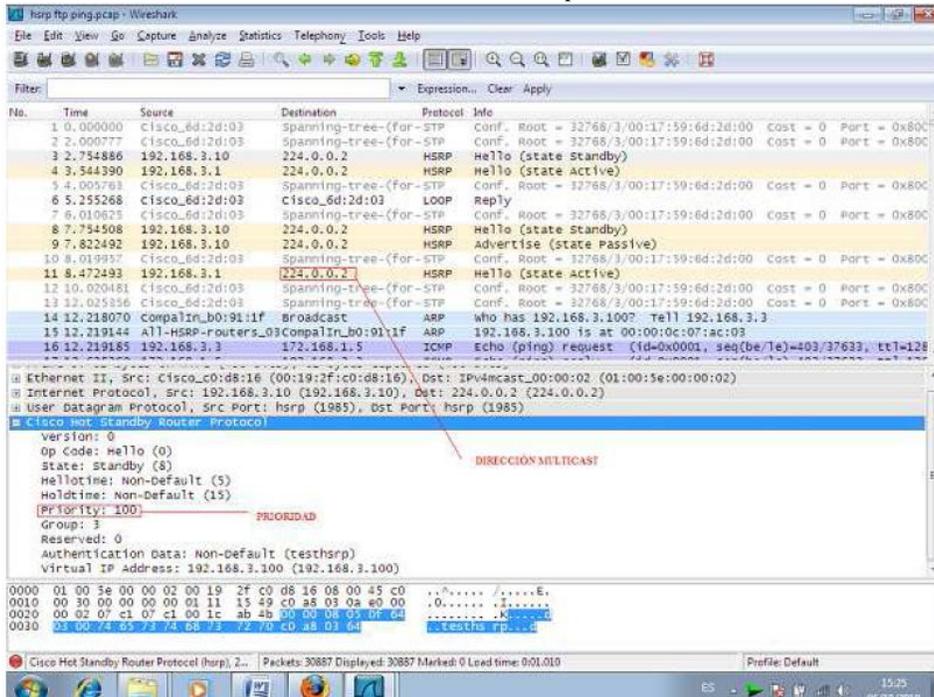
The screenshot shows the Wireshark interface with a packet list and a detailed view of a Cisco Hot Standby Router Protocol (HSRP) packet. The packet list shows several HSRP packets, with the selected packet having a priority of 110 and a virtual IP address of 192.168.3.100. The detailed view shows the following fields:

- Version: 0
- Op code: Hello (0)
- State: Active (16)
- Hello time: Non-Default (5)
- Hold time: Non-Default (15)
- Priority: 110
- Group: 3
- Reserved: 0
- Authentication Data: Non-Default (testhsrp)
- Virtual IP Address: 192.168.3.100 (192.168.3.100)

Red annotations in the image point to the 'Priority: 110' field, labeled 'PRIORIDAD', and the 'Virtual IP Address' field, labeled 'DIRECCION MULTICAST'.

Fuente: Los Investigadores

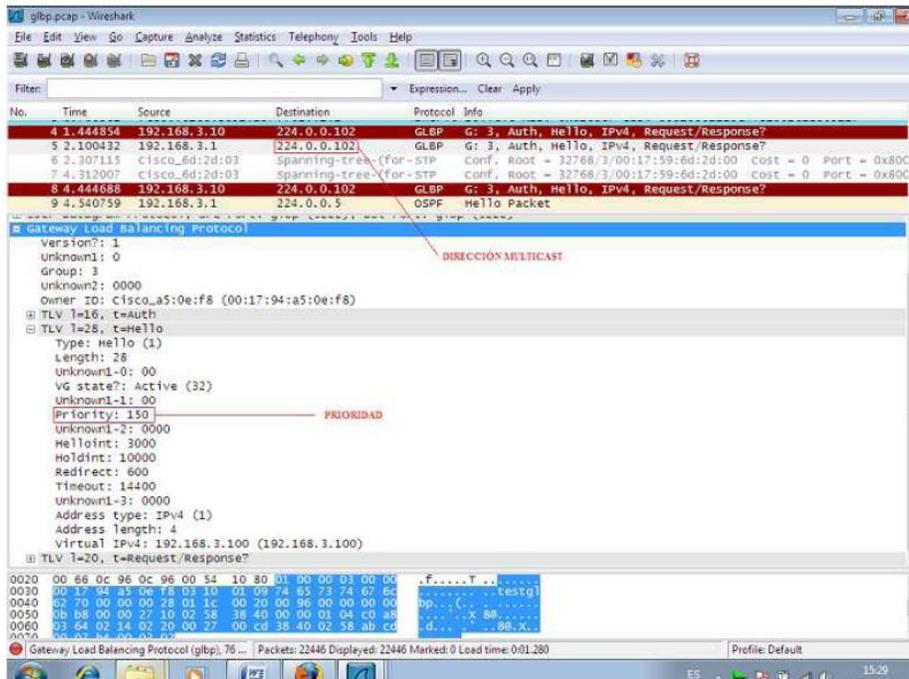
Grafico 3.24: Pruebas de envío/recepción de archivos



Fuente: Los Investigadores

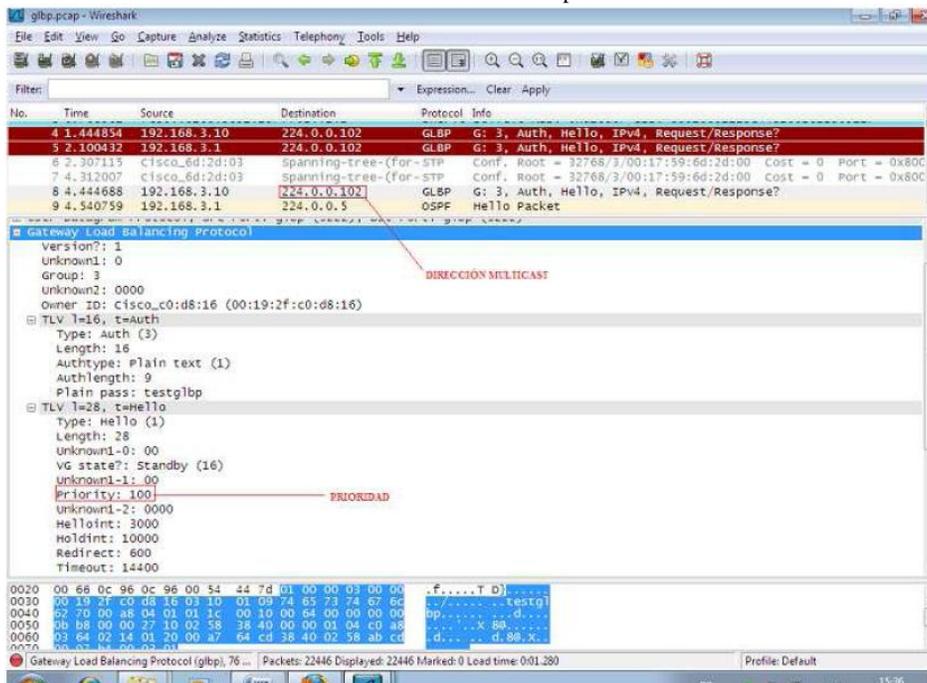
Protocolo GLBP

Grafico 3.25: Pruebas de envío/recepción de archivos



Fuente: Los Investigadores

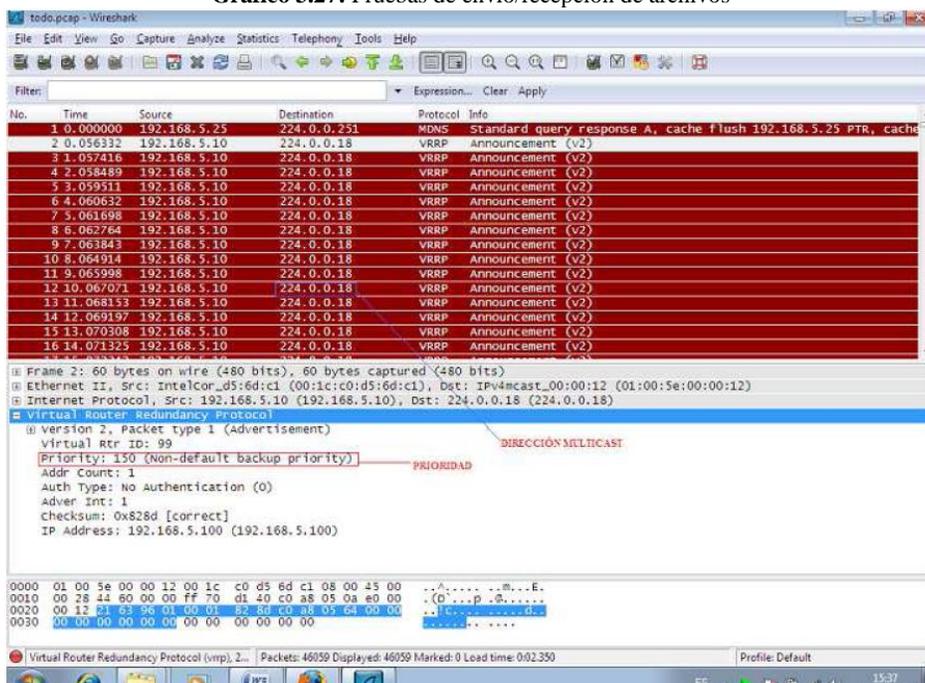
Grafico 3.26: Pruebas de envío/recepción de archivos



Fuente: Los Investigadores

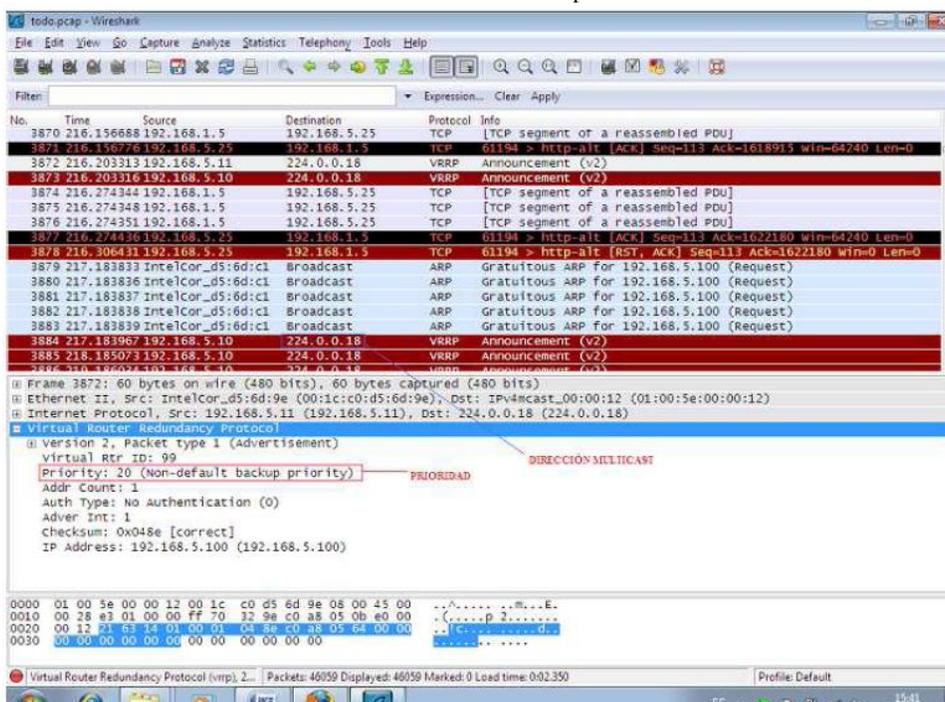
Protocolo VRRP

Grafico 3.27: Pruebas de envío/recepción de archivos



Fuente: Los Investigadores

Grafico 3.28: Pruebas de envío/recepción de archivos



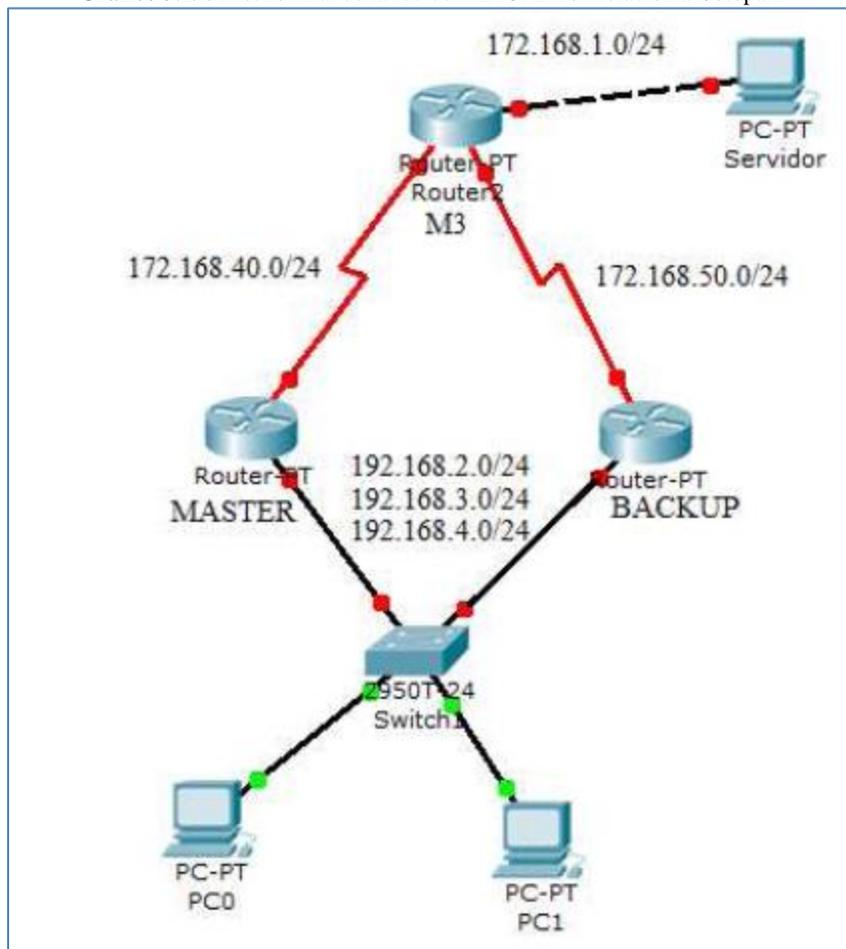
Fuente: Los Investigadores

1.16. Procesamiento de Información

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

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

Grafico 3.29: Diseño final de la red del MAGAP con relación a Cotopaxi



Fuente: Los Investigadores

Para la transmisión de archivos planos se utilizó el servicio FTP. Una vez realizadas las respectivas configuraciones de interfaces y ruteo, se procedió a instalar el software FileZilla Server en el computador que trabajó como Servidor Ftp y en cada cliente se ejecutó el FileZilla Client el cual permite copiar archivos de cualquier tipo, disponibles del servidor, los clientes se conectaran al servidor FTP con un ancho de banda de 5 Mbps que es la asignación para la ciudad de Latacunga por el número de usuarios.

1.17. Retardos de Transmisión

Los resultados obtenidos se muestran en la siguiente tabla la cual demuestra como fueron realizadas en base a la red LAN de Latacunga y la WAN entre Quito y Latacunga.

Tabla 3.1: Retardos en las comunicaciones MAGAP

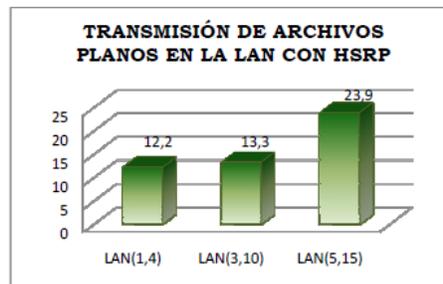
CLIENTES	RETARDOS DE TRANSMISIÓN (ms)				\bar{x}
	LAN(1,4)	LAN(3,10)	LAN(5,15)	WAN(1,4)	
PC2	LAN(1,4)	13,9	9,3	12,6	11,9
	LAN(3,10)	13,5	12,8	14,5	13,6
	LAN(5,15)	24,6	25,2	23,1	24,3
	WAN(1,4)	8,4	9,3	7,5	8,4
	WAN(3,10)	8,8	8,7	8,5	8,7
	WAN(5,15)	9,3	8,6	8,9	8,9
PC3	LAN(1,4)	14,2	9,8	13,7	12,6
	LAN(3,10)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

Fuente: Los Investigadores

1.18. Análisis estadístico de la red LAN/WAN

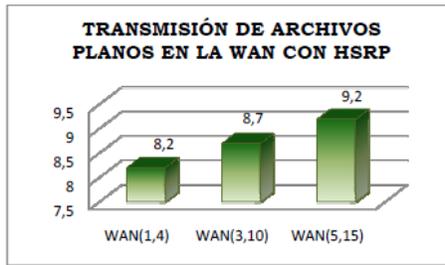
En base al cuadro anterior podemos desarrollar un análisis estadístico de los resultados de las mediciones que se hicieron en base al diseño de la red LAN y WAN del ministerio.

Grafico 3.30: Estadísticas de retardos



Fuente: Los Investigadores

Gráfico 3.31: Estadísticas de Retardos



Fuente: Los Investigadores

1.19. Tabla de análisis para el cálculo de envío y recepción de paquetes

Protocolo HSRP

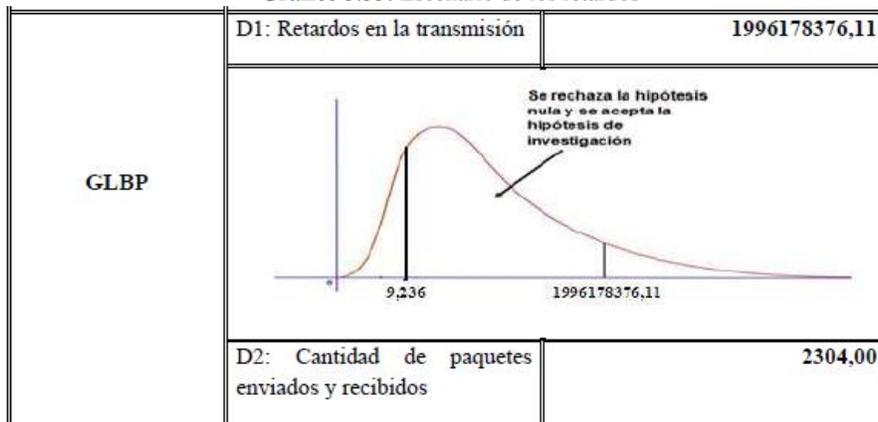
Gráfico 3.32: Escenario de los retardos

ESCENARIO	INDICADOR	χ^2
HSRP	D1: Retardo en la Transmisión	25452064,32
	D2: Cantidad de paquetes enviados y recibidos	3553,00

Fuente: Los Investigadores

Protocolo GLBP

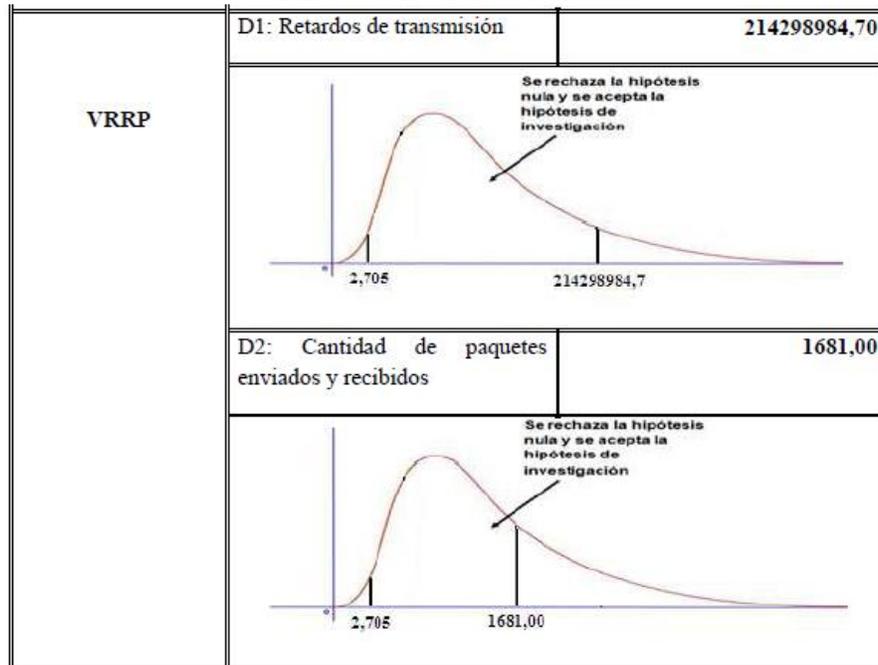
Gráfico 3.33: Escenario de los retardos



Fuente: Los Investigadores

Protocolo GLBP

Gráfico 3.34: Escenario de los retardos



Fuente: Los Investigadores

