PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIÓN

TRABAJO PREVIO LA OBTENCIÓN DEL TÍTULO DE:

MÁSTER EN REDES DE COMUNICACIONES

TÍTULO:

"DISEÑO Y SIMULACIÓN DE UNA TOPOLOGÍA Y GESTIÓN DE RED BASADAS EN TÚNELES GRE Y ENRUTAMIENTO DINÁMICO OSPF Y EIGRP, CASO DE ESTUDIO – GRUPO AUTOMOTRIZ ELJURI"

PABLO ANDRÉS BARBECHO BAUTISTA

Quito – octubre 2016

Tabla de contenido

Tabla de contenido i
Listado de Ilustraciones iii
Listado de Tablas v
Introducción vii
Justificación ix
Antecedentes x
Objetivo General: xii
Objetivos Específicos: xii
Capítulo 1 : SITUACIÓN ACTUAL – CASO DE ESTUDIO 1
1.1 Situación actual - Caso de Estudio Grupo Automotriz 1
1.1.1 Análisis de la infraestructura de red 4
1.2 NBAR Protocol Discovery 7
1.3 Descripción de los principales servicios de red - Caso de Estudio 9
1.3.1 Escenario de Simulación para análisis de tráfico 10
1.3.2 Análisis de Servicios de Red 10
Capítulo 2 : PROTOCOLOS DE TUNELIZACIÓN Y ENRUTAMIENTO DINÁMICO 23
2.1 Túnel GRE 23
2.1.1 Proceso de Encapsulación 26
2.2 Simulación y Comandos básicos 28
2.3 Análisis del proceso de encapsulación con Wireshark 39
2.4 MTU Unidad Máxima de Transferencia 40
2.5 Tipos de Enrutamientos Dinámicos y Route-Map [6] 42
2.5.1 Enrutamiento OSPF 44
2.5.2 Simulación OSPF 45
2.5.3 Redundancia de Enlaces 49
2.5.4 Función Route-Map Cisco 55
2.5.5 Simulación Route-Map 56
Capítulo 3 : DISEÑO Y SIMULACIÓN 62
3.1 Descripción del Diseño 62
3.1.1 Diseño del Diagrama físico y lógico 64
3.1.2 Segmentación de Red VLSM y Direccionamiento 68
3.1.3 Licenciamiento de los equipos (IOS) 73
3.2 Simulación del diseño en GNS3 74
3.2.1 Implementación del diseño para el cuarto de datos entorno GNS3 75
3.2.2 Implementación del diseño para la red a nivel nacional entorno GNS3 79
3.2.3 Configuración de calidad de servio QoS para VoIP 82
3.2.4 Identificación de Tráfico y requerimientos 84
3.2.5 Clasificación de Tráfico 84
3.2.6 Definición de Políticas por clase 85
3.3 Configuración QoS 86

3.3.1 Mapa de Clase 88
3.3.2 Mapa de Políticas 90
3.3.3 Política de Servicio 91

Capítulo 4 : PRUEBAS DEL SISTEMA 96
4.1 Software de monitoreo Cacti y Nagios 96
4.1.1 Implementación de Cacti 96
4.1.2 Implementación Nagios XI 101
4.2 Enrutamiento Dinámico / Tolerancia a Fallos 104
4.3 Balanceo de carga 109
4.4 Calidad de Servicio QoS para VoIP 111
4.5 Seguridad de la Infraestructura 117
4.5.1 Capa 1 118
4.5.2 Capa 2 119
4.5.3 Capa 3 120

Capítulo 5 : CONCLUSIONES Y RECOMENDACIONES 125
5.1 Conclusiones 125
5.2 Recomendaciones 128

BIBLIOGRAFÍA: 131

Listado de Ilustraciones

Ilustración 1-1 Esquema Físico de Enlaces Dedicados - Agencias Principales..... 2
Ilustración 1-2 Topología Física del Data Center 5
Ilustración 1-3 Entorno GNS3 8
Ilustración 1-4 Comandos activar NBAR en la interfaz FastEth0 8
Ilustración 1-5 Resultado de NBAR Protocol Discovery 9
Ilustración 1-6 Principales Servicios y Aplicaciones - Caso de Estudio 9
Ilustración 1-7 Entorno de Simulación 10
Ilustración 1-8 Sistema SIA Virtualinfo 11
Ilustración 1-9 Configuración de NBAR para implementación de QoS para protocolos dinámicos 12
Ilustración 1-10 Filtrado Tráfico http NBAR 12
Ilustración 1-11 Tráfico Medido - Acceso a Web Server Elastix 13
Ilustración 1-12 Consola de Emulación Sistema AS400 13
Ilustración 1-13 Características de conexión de la consola PC5250 14
Ilustración 1-14 Filtrado de Tráfico Telnet NBAR 15
Ilustración 1-15 Tráfico Medido – Conexión Telnet 15
Ilustración 1-16 Dominios de Correo 16
Ilustración 1-17 Consola de administración del servidor de Telefonía 17
Ilustración 1-18 Filtrado de Tráfico RTP NBAR 17
Ilustración 1-19 Simulación de 1 llamada con máquinas virtuales y GNS3..... 18
Ilustración 1-20 Tráfico Medido – Consumo de ancho de banda de 1 llamada usando el códec G.711 18
Ilustración 1-21 Cisco WebEx 19
Ilustración 1-22 Windows Conexión a Escritorio Remoto 20
Ilustración 1-23 Configuración Cliente Escritorio Remoto 20
Ilustración 1-24 Tráfico Medido – Servicio de Escritorio Remoto con alta calidad . 21
Ilustración 1-25 Tráfico Medido – Servicio de Escritorio Remoto con calidad media 21
Ilustración 2-1 Topología Túnel IP 23
Ilustración 2-2 Cabecera GRE 25
Ilustración 2-3 Formato Encapsulación IP 27
Ilustración 2-4 Formato de encapsulación GRE 28
Ilustración 2-5 Cisco 3745 IOS 29
Ilustración 2-6 RouterOS Mikrotik Image 29
Ilustración 2-7 Topología GNS3 para simulación de Túneles IP 30
Ilustración 2-8 Consola Winbox 31
Ilustración 2-9 Configuración de direccionamiento IP de los Host GNS3 32
Ilustración 2-10 Direccionamiento IP Mikrotik mediante Winbox 34
Ilustración 2-11 Ping CUE-UIO 37
Ilustración 2-12 Ping CUE-GYE 38
Ilustración 2-13 Ping GYE-UIO / Tracert GYE-UIO 38
Ilustración 2-14 Cabeceras Inner Outer GRE Wireshark 39
Ilustración 2-15 Cabecera GRE Wireshark 40
Ilustración 2-16 MTU Fragmentación 41

Ilustración 2-17 Protocolos de Enrutamiento Dinámico 43
Ilustración 2-18 Tabla de Enrutamiento Router Cisco R2 46
Ilustración 2-19 Tabla de enrutamiento Mikrotik / DAo - Dinamic Active Ospf 47
Ilustración 2-20 Tabla de Enrutamiento Cisco R1 48
Ilustración 2-21 Pruebas de conectividad entre Agencias 49
Ilustración 2-22 Enlace Redundante UIO-GYE 50
Ilustración 2-23 Tabla de Enrutamiento R1 51
Ilustración 2-24 Estado de las Interfaces R1 51
Ilustración 2-25 Tabla de enrutamiento R2 52
Ilustración 2-26 Estado de las Interfaces R2 52
Ilustración 2-27 Tabla de enrutamiento Mikrotik 52
Ilustración 2-28 Estado de las interfaces Mikrotik 53
Ilustración 2-29 Interfaz Tunnel2 down 53
Ilustración 2-30 Tabla de enrutamiento R1 con la interfaz Tunnel 2 deshabilitada 54
Ilustración 2-31 Redirección de tráfico 54
Ilustración 2-32 Tiempo de Recuperación 55
Ilustración 2-33 Topología de Simulación de Acceso a Internet GNS3 56
Ilustración 2-34 Redistribución de ruta por defecto OSPF R1 y Mikrotik 58
Ilustración 2-35 Resultado del Debug policy Match 59
Ilustración 2-36 Resultado debug policy rejected normal forwarding 60
Ilustración 3-1 Diseño Jerárquico Cisco 64
Ilustración 3-2 Diagrama Físico Cuarto de Datos 65
Ilustración 3-3 Diagrama Lógico Cuarto de Datos 66
Ilustración 3-4 Diagrama Físico de enlaces a nivel nacional 67
Ilustración 3-5 Diagrama Lógico – Simulación del Diseño 71
Ilustración 3-6 Características del Licenciamiento 73
Ilustración 3-7 Cisco 3560 Funcionalidades 74
Ilustración 3-8 Resumen del STP en R1 76
Ilustración 3-9 Resumen STP enlaces balanceados 77
Ilustración 3-10 Resumen STP e interfaces Port-channel Router R2 78
Ilustración 3-11 Topología de Simulación - Caso de Estudio 79
Ilustración 3-12 Resumen configuración R1 UIO 80
Ilustración 3-13 Resumen configuración R2 CUE 80
Ilustración 3-14 Resumen configuración Mikrotik GYE 80
Ilustración 3-15 Resumen configuración R5 81
Ilustración 3-16 Latencia de ICMPs a los diferentes Routers 82
Ilustración 3-17 Pasos para implementara QoS en una red Convergente 83
Ilustración 3-18 Clasificación de Tráfico - Caso de Estudio 85
Ilustración 3-19 Pasos para implementar QoS Método MQC 88
Ilustración 3-20 Tráfico de ingreso clasificado en Router R1 93
Ilustración 3-21 Tráfico de salida clasificado en router R1 93
Ilustración 4-1 Administración Web Cacti 97
Ilustración 4-2 Cacti Dispositivos 98
Ilustración 4-3 Cacti Configuración del Gráfico de Interfaces 99
Ilustración 4-4 Cacti Arbol de Monitoreo 99
Ilustración 4-5 Topología de Simulación Cacti 100
Ilustración 4-6 Cacti Arbol de Monitoreo - Caso de estudio 100

Ilustración 4-7 Cacti Plugin Monitor 101
Ilustración 4-8 Nagios XI 102
Ilustración 4-9 Interfaz Nagios XI 103
Ilustración 4-10 Nagios XI Interfaces Status 103
Ilustración 4-11 Tráfico NetFlow 105
Ilustración 4-12 Interfaz Túnel 1 Down 105
Ilustración 4-13 Monitor Túnel 1 R2 Cacti 106
Ilustración 4-14 Monitor Nagios Túnel 1 Alerta 106
Ilustración 4-15 Tabla de Enrutamiento Router R1 Quito 108
Ilustración 4-16 Ancho de banda Enlaces - Métrica OSPF 109
Ilustración 4-17 Tabla de Enrutamiento R1 - Balanceo de Carga 110
Ilustración 4-18 Class Maps - R5 112
Ilustración 4-19 Policy Map – R2 113
Ilustración 4-20 Llamada Softphone 113
Ilustración 4-21 Tráfico VoIP 80 kbps 114
Ilustración 4-22 Netflow Solarwinds 115
Ilustración 4-23 Policy Map Interface Input R2 116
Ilustración 4-24 Policy Map Interface Output R2 117
Ilustración 4-25 Huellas Digitales o Fingerprint EER=5% 119
Ilustración 4-26 VPN - Protocolos de Seguridad Capas de Red 121
Ilustración 4-27 Herramienta NMAP 121
Ilustración 4-28 John The Ripper - Ataques de Fuerza Bruta 122
Ilustración 4-29 NIKTO escáner de vulnerabilidades en Servidores Web 122
Ilustración 4-30 SQLmap - SQL injection 123

Listado de Tablas

Tabla 1-1 Agencias – Caso de Estudio 2
Tabla 1-2 Ancho de banda Agencias 4
Tabla 1-3 Equipos Data Center 5
Tabla 2-1 Direccionamiento IP para la Simulación de Túneles IP 30
Tabla 2-2 Configuraciones adicionales para enlace Redundante 50
Tabla 2-3 Distribución Internet 55
Tabla 3-1 Descripción de Equipos 64
Tabla 3-2 Segmentación de Red Centro de Datos 68
Tabla 3-3 Direccionamiento de red agencias a nivel nacional 70
Tabla 3-4 Direccionamiento Túneles 71
Tabla 3-5 Direccionamiento Routers a Nivel Nacional 72
Tabla 3-6 Configuración VTP 75
Tabla 3-7 Parámetro QoS 83
Tabla 3-8 Requerimientos Tráfico 84
Tabla 3-9 Requerimientos por Clase - Políticas 86
Tabla 3-10 Equivalencias PHB - IP Precedence 88
Tabla 3-11 Clasificación y Marcaje de Tráfico - Router R2 89

Tabla 3-12 Políticas 90
Tabla 3-13 Tabla Policy-Map 91
Tabla 3-14 Service Policy - Router R2 92
Tabla 4-1 Servicios Activos del Escenario 104
Tabla 4-2 Impacto en los servicios – Tiempo de convergencia OSPF / Keepalive Túneles GRE 108

Introducción

El presente trabajo monográfico, previo a la obtención del título de Máster en Redes de Comunicaciones, desarrolla un análisis, diseño y simulación técnicos para una futura implementación que facilite la administración y monitoreo de equipos de telecomunicaciones a nivel de capa 3.

Mediante el diseño y configuración de túneles GRE sobre enlaces de datos, y por medio de enrutamientos dinámicos, se pretende proporcionar autonomía en la administración de la red, eliminando la necesidad de solicitar la administración de los ISPs, y de esta manera ofrecer un determinado grado de servicio de telecomunicaciones, que incorpore confiabilidad en las conexiones, tolerancia a fallos, balanceo de carga, calidad de servicio VoIP y tiempos de respuesta óptimos que faciliten la administración local.

El proyecto monográfico tomará como referencia la infraestructura y topología de red de un grupo automotriz de la ciudad de Cuenca. El esquema de red del caso de estudio es de tipo estrella extendida y maneja 62 sucursales a nivel nacional y 2 agencias en Perú y Venezuela.

Debido a la falta de cobertura, temas económicos, o asuntos administrativos, los enlaces de datos e internet los brindan varios ISPs, Tv Cable, Punto Net, CNT y Telconet. Al tener varios proveedores, con distintas tecnologías en las redes de acceso y core, el departamento de Telecomunicaciones necesita una solución que disminuya al máximo la injerencia en las configuraciones de los enlaces por parte de los proveedores.

Eventos como, caídas de enlaces, creación de nuevas agencias, nuevos segmentos de red, solicitud de interconexión entre agencias, interconexión entre agencias con distintos ISPs, enrutamientos a internet, calidad de servicio QoS y seguridades en la

red, deben ser administrados netamente por el departamento de Telecomunicaciones de la empresa, eventos que al momento es administrado por los diferentes ISPs, generando problemas en tiempos de reacción y dependencia total de los ISPs.

Adicional, al implementar herramientas de monitoreo como CACTI y NAGIOS, se puede generar reportes, alertas, históricos de anchos de banda, estado de enlaces y verificar los servicios de los ISPs. Este compendio de información permitirá tomar acciones correctivas y decidir futuros cambios de proveedor o verificación de los SLAs ofrecidos. Estas herramientas de monitoreo se instalarán en un entorno virtual que permita el monitoreo y exploración de la topología del caso de estudio.

Para llevar a cabo el desarrollo práctico del proyecto de tesis (análisis, diseño y simulación), se toma como referencia y Caso de Estudio al Grupo Automotriz, sin embargo, la solución puede ser implementada en cualquier ambiente que posea una topología de red similar.

La primera parte del trabajo monográfico, expone un levantamiento de información de la infraestructura de red y análisis de la situación actual, así como un marco teórico de los protocolos de tunelización y protocolos de enrutamiento dinámico a implementar en la simulación. La segunda parte, desarrolla el diseño y simulación de la solución propuesta, basada en el software GNS3, el cual permite emular entornos CISCO IOS y máquinas virtuales.

Justificación

Desde finales del año 2014 y principios del 2016 en el Ecuador se ha venido desarrollando un proceso de actualización del marco regulatorio de las leyes. Dentro de estas reformas a la constitución, se incluyen reformas a las importaciones de vehículos terrestres, por parte del COMEX[1], en la resolución 049-2014 en el Artículo 1, en su Anexo 1 se deroga a la empresa de NEGOCIOS AUTOMOTRICES NEOHYUNDAI S.A., un cupo de importación de vehículos de hasta 5.014 vehículos.

Al ser la mencionada empresa la encargada de las importaciones del Grupo Automotriz, se ven afectados en gran medida los concesionarios Automotrices a nivel nacional. Dada esta situación, y proyectando un año de recesión económica para el país, es importante que los departamentos de TI de las empresas, encargados de las áreas tecnológicas y de comunicaciones, brinden soluciones que optimicen recursos humanos, económicos, y de infraestructura.

La implementación del presente trabajo monográfico optimiza la administración y los recursos de las comunicaciones, disminuyendo costos operativos, tiempos fuera de servicio y carga operativa para el departamento de TI. Garantiza además un determinado nivel de calidad en los servicios que fluyen a través de la infraestructura de red, en especial los servicios que funcionan en tiempo real (RTP) como la voz sobre IP.

El trabajo propone una infraestructura de red autónoma que optimice los recursos de telecomunicaciones, válido para implementaciones en entornos que posean recursos humanos limitados o recursos de capacitación media-baja.

Adicional al diseño de la infraestructura de comunicaciones, los reportes que proveen las herramientas de monitoreo, brindan a la gerencia datos válidos para toma de

decisiones, como cambios de proveedor por mal servicio (incumplimiento de SLA) u optimización de anchos de banda, según sean los requerimientos de cada sucursal.

Antecedentes

Se toma como caso de estudio al Grupo Automotriz de la ciudad de Cuenca. El Grupo contempla 62 agencias distribuidas para distintas marcas de vehículos con un centro de datos ubicado en la ciudad de Cuenca.

El centro de datos concentra los sistemas y accesos a internet a través de un equipo proxy. El data center es administrado por el departamento de TI del Grupo, el cuál incluye equipamiento de diferentes proveedores como CISCO, MIKROTIK y D-LINK.

Los switches de core y distribución son de marca CISCO Catalyst con licenciamiento IP Services y manejan los enrutamientos de las agencias, salida a internet, interconexión entre agencias, ACLs de seguridad para acceso a bases de datos y servidores WEB. Adicional, a estos equipos se conectan los diferentes proveedores, teniendo como red de acceso fibra óptica, par trenzado y enlaces de microonda, entregando un cable UTP para interconexión con la LAN.

Por otra parte, los switches de acceso son de marca CISCO y D-LINK, y manejan los accesos a las diferentes redes, por medio de VLANs creadas en los switches de distribución y aprendidas mediante VTP. Este equipamiento de acceso, maneja seguridades a nivel de puerto (Port Security) para la conexión de servidores y equipamiento de administración.

Las agencias de igual manera manejan equipamiento CISCO de gama baja small-business, en los cuales se mantienen las configuraciones de seguridad de puertos y segmentación de la red para las diferentes áreas de ventas, contabilidad,

administrativo, telefonía IP, clientes y red inalámbrica. Las agencias manejan una topología y equipamiento similar en todas las agencias, cambiando únicamente los segmentos de red y VLSM.

El manejo de rutas en el switch de core se configura de manera estática, lo cuál por la cantidad de servicios y agencias, resulta muy complejo, ya que se requiere personal altamente capacitado en la topología para realizar cambios, enrutamientos o subneteos para una nueva agencia o servicio. Adicional a este complejo panorama, se tienen varios proveedores que brindan los servicios de enlaces de datos dedicados y enlaces de internet. Al tratar de realizar enrutamientos de las agencias al centro de datos se tiene que solicitar al proveedor el enrutamiento de todos los segmentos de red según los servicios que requiera la agencia. De igual manera para interconectar dos o más agencias se requiere la intervención de los proveedores para que agreguen los segmentos de red en las tablas de enrutamientos de los equipos, siendo esto un proceso que implica demoras, carga administrativa y gastos de comunicación con los proveedores.

Objetivo General:

- Diseñar y simular una topología y gestión de red basadas en tuneles GRE y enrutamiento dinamico OSPF y EIGRP, caso de estudio – Grupo Automotriz.

Objetivos Específicos:

- Diseñar una topología de red que implemente Túneles GRE, eliminando la necesidad de soporte del ISP en capa 3.
- Simular en GNS3 el tunelizado GRE de los concentradores de Cuenca, Quito y Guayaquil y 62 agencias del caso de estudio – Grupo Automotriz Eljuri
- Simular en GNS3 la implementación del enrutamiento dinámico OSPF entre las agencias y concetradores del caso de estudio – Grupo Automotriz
- Simular en GNS3 la implementación del enrutamiento dinámico OSPF en los concentradores para redundancia de enlaces de datos.
- Simular en GNS3 calidad de servicio QoS para manejo de 5 canales de VoIP sobre los túneles GRE entre las agencias de Quito, Cuenca y Guayaquil.
- Implementar los sistemas de monitoreo Cacti y Nagios para administración y reportes de la topología de red propuesta.

Capítulo 1 : SITUACIÓN ACTUAL – CASO DE ESTUDIO

1.1 Situación actual - Caso de Estudio Grupo Automotriz

El presente trabajo monográfico toma como referencia y caso de estudio a la infraestructura de comunicaciones del Grupo Automotriz. En la Tabla I se especifican las principales empresas Automotrices del Grupo Eljuri que se tomarán en cuenta para el análisis de las comunicaciones. Cada empresa está estructurada con un determinado número de oficinas/agencias que requieren acceso a los diferentes sistemas y servicios de comunicaciones ubicados en el Data Center localizado en la ciudad de Cuenca en las instalaciones de la empresa Virtualinfo. Los diferentes sistemas y servicios se describen en el apartado "**Análisis de tráfico de los principales servicios de red".**

Cada empresa es administrada de manera autónoma. El manejo de las TICs se encuentra centralizado en la ciudad de Cuenca. El departamento de Telecomunicaciones se encarga de la administración de las comunicaciones de las diferentes agencias del grupo automotriz, esto incluye administración de la infraestructura del Data Center, enlaces de datos / internet, centralillas telefónicas de VoIP, mantenimiento de enrutadores, segmentación de redes, enrutamientos entre empresas y agencias, según sean los requerimientos.

De manera general los aspectos que se toman en cuenta para la administración de los enlaces de datos al momento son:

- Disponibilidad
- Escalabilidad
- Confiabilidad
- Costos
- Latencia o Delay
- Jitter

Empresa	Ciudad	Agencia
QUITO MOTORS - QM	QUITO	MATRIZ
	LATACUNGA	LAT
	RIOBAMBA	RIO
	AMBATO	AMB
	IBARRA	IBA
	SANTO DOMINGO	STO DOM
NEOAUTO - NA	QUITO	MATRIZ
	QUITO	SUR
	QUITO	SHIRIS
	QUITO	AMB
	QUITO	STO DOM
MERQUIAUTO - MQ	QUITO	MATRIZ
	LATACUNGA	LAT
	IBARRA	IBA
	RIOBAMBA	RIO
	TENA	TENA
	PUYO	PUYO
	QUEVEDO	QUE
LOGIMANTA - LM	MANTA	MATRIZ
	MANTA	ENSAMBLADORA
	MANTA	BODEGA
AUTOHYUN - AH	GUAYAQUIL	MATRIZ
	GUAYAQUIL	ECSY AUTO - EC
	GUAYAQUIL	LOCALIZA AEROPUERTO
	GUAYAQUIL	AMERICAS
CUENCA - DATA CENTER	CUENCA	MERQUIAUTO
	CUENCA	AUTOHYUN
	CUENCA	NEOAUTO
	CUENCA	QUITO MOTORS

Tabla 1-1 Agencias – Caso de Estudio

La *Ilustración 1-1* describe de manera general la situación actual de los enlaces de datos. Al tener una topología centralizada, donde los servicios y aplicaciones que utilizan las empresas del Grupo se encuentran concentradas en el Data Center en la ciudad de Cuenca *Ilustración 1-2*, los diferentes aplicativos y servicios utilizan los enlaces dedicados para su correcto funcionamiento.

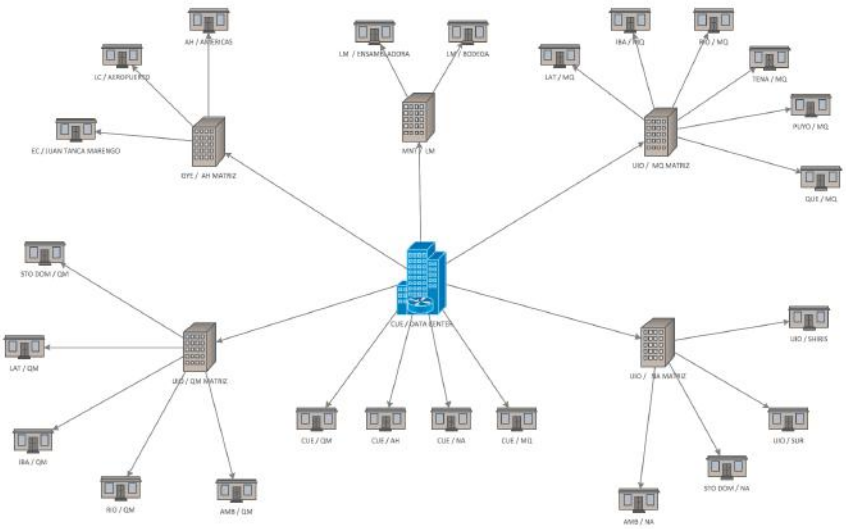


Ilustración 1-1 Esquema Físico de Enlaces Dedicados - Agencias Principales

Las agencias se encuentran distribuidas a nivel nacional e internacional, conectadas con enlaces de datos e internet dedicados, descritos en la *Tabla 1-2*. Actualmente las capacidades de los enlaces (ancho de banda) no tienen ningún sustento técnico y han ido creciendo de manera desordenada y sin mayor soporte de los proveedores del servicio. Este crecimiento desordenado y la implementación de nuevos aplicativos como la telefonía IP (VoIP) han deteriorado la calidad en las comunicaciones de las agencias. En algunos casos se tienen enlaces con capacidades sobre dimensionadas (enlaces subutilizados a un alto costo), y en otras agencias enlaces totalmente saturados (se requiere ampliación del ancho de banda).

Es por estos problemas que se vuelve imprescindible un análisis de tráfico de los principales servicios y aplicativos que permita optimizar las capacidades de los enlaces en función del consumo de ancho de banda que se pueda generar en cada punto. Adicional al análisis inicial, se requiere implementar un monitor de los enlaces para dar seguimiento a las capacidades en los enlaces dedicados.

El presente trabajo monográfico describe en el capítulo 4 la simulación de dos monitores de red muy utilizados en el medio como son CACTI y NAGIOS. Ésta simulación será meramente para análisis de las herramientas de monitoreo, ya que no se conectarán a la topología de la empresa.

Resulta imprescindible para el caso de estudio realizar mediciones de tráfico de los principales aplicativos y servicios de red. Con estas métricas se pretende estimar un tráfico de red por cada servicio que permita redimensionar los enlaces para las sucursales. Basado en las métricas a obtener, el dimensionamiento por agencia y los monitores de red se pretende brindar herramientas para un correcto control y seguimiento de las comunicaciones.

Las simulaciones propuestas brindarán la información suficiente determinar la factibilidad de la implementación de la topología de red propuesta y de las configuraciones de red en función de brindar un cierto nivel de servicio a los usuarios.

Este nivel de servicio está orientado a los aplicativos actuales y en especial para la telefonía IP y Video Conferencia que son servicios basados en RTP (Real Time Protocol) con requerimientos de baja latencia e inexistencia de jitter.

Empresa	Ciudad	Agencia	Ancho de Banda (Mbps)	Proveedor	Tipo
QUITO MOTORS - QM	QUITO	MATRIZ	10	Telconet	Interurbano
	LATACUNGA	LAT	5	Punto Net	Urbano
	RIOBAMBA	RIO	3	Punto Net	Urbano
	AMBATO	AMB	1	Tv Cable	Urbano
	IBARRA	IBA	1	Punto Net	Urbano
	SANTO DOMINGO	STO DOM	1	Tv Cable	Urbano
NEOAUTO - NA	QUITO	MATRIZ	5	Tv Cable	Interurbano
	QUITO	SUR	1	Punto Net	Urbano
	QUITO	SHIRIS	1	Punto Net	Urbano
	AMBATO	AMB	2	Telconet	Urbano
	SANTO DOMINGO	STO DOM	2	Tv Cable	Urbano
MERQUIAUTO - MQ	QUITO	MATRIZ	5	Telconet	Interurbano
	LATACUNGA	LAT	2	Punto Net	Urbano
	IBARRA	IBA	1	Punto Net	Urbano
	RIOBAMBA	RIO	1	Punto Net	Urbano
	TENA	TENA	1	Tv Cable	Interurbano
	PUYO	PUYO	1	Tv Cable	Interurbano
	QUEVEDO	QUE	1	Tv Cable	Interurbano
LOGIMANTA - LM	MANTA	MATRIZ	10	Punto Net	Interurbano
	MANTA	ENSAMBLADORA	5	Punto Net	Urbano
	MANTA	BODEGA	5	Punto Net	Urbano
AUTOHYUN - AH	GUAYAQUIL	MATRIZ	8	Tv Cable	Interurbano
	GUAYAQUIL	ECSY AUTO - EC	3	Tv Cable	Urbano
	GUAYAQUIL	LOCALIZA AEROPUERTO	2	Tv Cable	Urbano
	GUAYAQUIL	AMERICAS	4	Tv Cable	Urbano
CUENCA - DATA CENTER	CUENCA	MERQUIAUTO	2	Tv Cable	Urbano
	CUENCA	AUTOHYUN	2	Tv Cable	Urbano
	CUENCA	NEOAUTO	2	Tv Cable	Urbano
	CUENCA	QUITO MOTORS	2	Tv Cable	Urbano

Tabla 1-2 Ancho de banda Agencias

1.1.1 Análisis de la infraestructura de red

Para el análisis de la infraestructura actual se tomará encuenta equipos de core, distribución, acceso y equipos de frontera.

En la *Tabla 1-3* se detallan los modelos de los equipos y su función dentro de la topología de red actual dentro del Data Center.

Marca	Modelo	Descripción
Cisco	WS-C3560G-24TS-E	Core Data Center
Cisco	WS-C3550-24-EMI	Distribución
Cisco	WS-C3550-48-EMI	Acceso
Mikrotik	CCR1016-12G	Internet

Tabla 1-3 Equipos Data Center

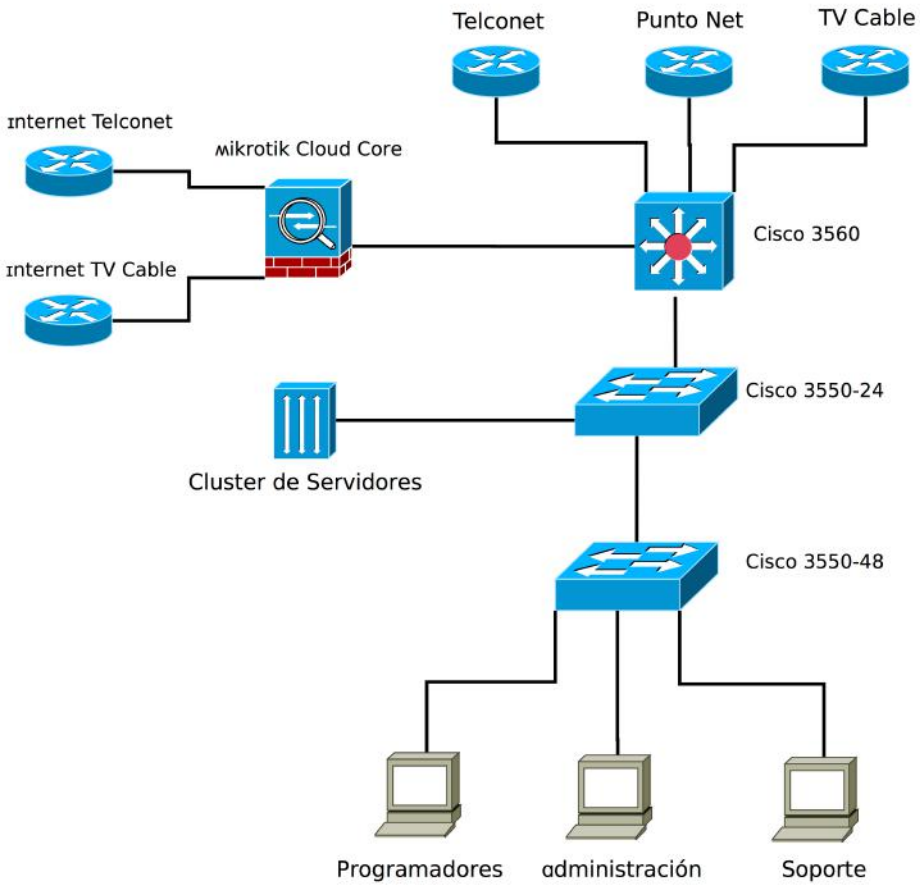


Ilustración 1-2 Topología Física del Data Center

La *Ilustración 1-2* muestra claramente la topología de red que maneja el Centro de Datos, basado en el modelo jerárquico de Cisco. Cada nivel jerárquico se encarga de un determinado grupo de servicios de red de manera que se balancea la carga entre los equipos.

Core: Al tratarse de una capa que requiere de grandes capacidades de procesamiento confiabilidad y baja latencia, se ha considerado el equipo mas actual con mejores características. En el próximo capítulo se analizará una actualización del equipo, ya que el equipo actual posee problemas de saturación y su capacidad de procesamiento resulta insuficiente.

El equipo que se encuentra en esta capa es el Cisco Catalyst WS-C3560G-24TS-E con una licencia IP Services. Entre las funciones actuales que maneja este dispositivo se encuentran:

- Enrutamiento Estático
- Enrutamiento dinámico RIPV2
- ACL (Listas de Control de Acceso)
- Port Trunking
- Acceso a la Intranet e Internet

Distribución: Esta capa se encuentra compuesta por el equipo Cisco Catalist WS-C3550-24-EMI. Este equipo es antiguo y se proyecta reubicarlo. Las principales funciones que funcionan en esta capa son:

- Enrutamiento Estático
- Enrutamiento dinámico RIPV2
- Ruteo InterVLAN
- Manejo de VLANs (VTP Server)
- Link Agreggation (Cluster de Servidores)
- Port Trunking

Acceso: Básicamente el equipo en esta capa administra los PC y dispositivos inalámbricos de la infraestructura de la empresa Virtualinfo. Esta capa esta compuesta por el equipo Cisco Catalyst WS-C3550-48-EMI.

- Manejo de VLANs (VTP Client)
- ACL (Listas de Control de Acceso)
- DHCP Server
- Link Agreggation (NAS)

Acceso a Internet: Para el acceso a internet se cuenta con un equipo Mikrotik CRR 1016-12G que realiza las funciones de:

- Firewall
- Portforwarding
- Traffic Control
- DMZ
- Acceso a Internet
- Load Balancing (Tv Cable, Telconet)

1.2 NBAR Protocol Discovery

De acuerdo a lo revisado en la asignatura Calidad de Servicio, el aplicativo NBAR (Network-Based Application Recognition) es una herramienta de clasificación que reconoce y clasifica una amplia variedad de protocolos y aplicaciones. Resulta una herramienta simple y poderosa que permite identificar y clasificar el trafico que cursa por una red. Permite la identificación de tráfico de capa 4-7. Además se puede añadir mas funcionalidades a la librería NBAR a través de los módulos PDLMs (Packet Description Language Modules).

Como introducción al análisis de los principales servicios de red del caso de estudio se plantea una topología de simulación *Ilustración 1-3* en el software GNS3 donde se configuró la herramienta NBAR para su análisis.

En la topología de simulación se incluyen dos equipos Windows y un equipo Elastix (Central de Telefonía IP) basado en Linux. Se realizan conexiones ssh, http, sip, escritorio remoto, ping, etc.

El resultado de NBAR *Ilustración 1-5* muestra el tráfico por protocolo, lo cuál ayuda a determinar la cantidad de tráfico que circula por la red y los principales servicios que se usan sobre ella.

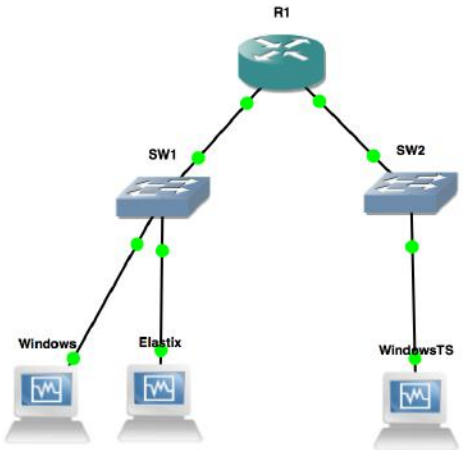


Ilustración 1-3 Entorno GNS3

NBAR se puede configurar de manera básica habilitando "nbar protocol discovery" en la interface o interfaces a monitorear. Para el caso de esta simulación se habilita en la interfaz FastEthernet 0/0.

```
TESIS#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
TESIS(config)#interface fastEthernet 0/0
TESIS(config-if)#ip nbar protocol-discovery
TESIS(config-if)#end
```

Ilustración 1-4 Comandos activar NBAR en la interfaz FastEth0

NBAR Protocol Discovery se utilizará en los próximos capítulos para identificar el tráfico y asociarlo a políticas para la implementación de calidad de servicio.

```
TESIS#show ip nbar protocol-discovery interface fastEthernet 0/0

 FastEthernet0/0
                              Input                     Output
                              -----                     ------
   Protocol                   Packet Count              Packet Count
                              Byte Count                Byte Count
                              5min Bit Rate (bps)       5min Bit Rate (bps)
                              5min Max Bit Rate (bps)   5min Max Bit Rate (bps)
   ------------------------   ------------------------  ------------------------
   secure-http                2356                      1528
                              2641726                   194887
                              0                         0
                              24000                     7000
   netbios                    296                       0
                              38852                     0
                              0                         0
                              4000                      0
   icmp                       3852                      4154
                              304992                    326136
                              1000                      1000
                              1000                      1000
   ssh                        888                       888
                              136701                    51652
                              1000                      0
                              1000                      1000
   dns                        602                       0
                              48408                     0
                              0                         0
                              0                         0
   sip                        22                        22
                              11198                     14872
```

Ilustración 1-5 Resultado de NBAR Protocol Discovery

1.3 Descripción de los principales servicios de red - Caso de Estudio

Se describen los principales servicios de red del caso de estudio, siendo estos, variados y con diferentes requerimientos de red. Esta amplia gama de servicios permite tener una clara idea del ancho de banda, manejo de tráfico, seguridades, enrutamientos y configuraciones de red en general que requieren los servicios y aplicaciones típicas dentro de un entorno empresarial de tamaño medio.

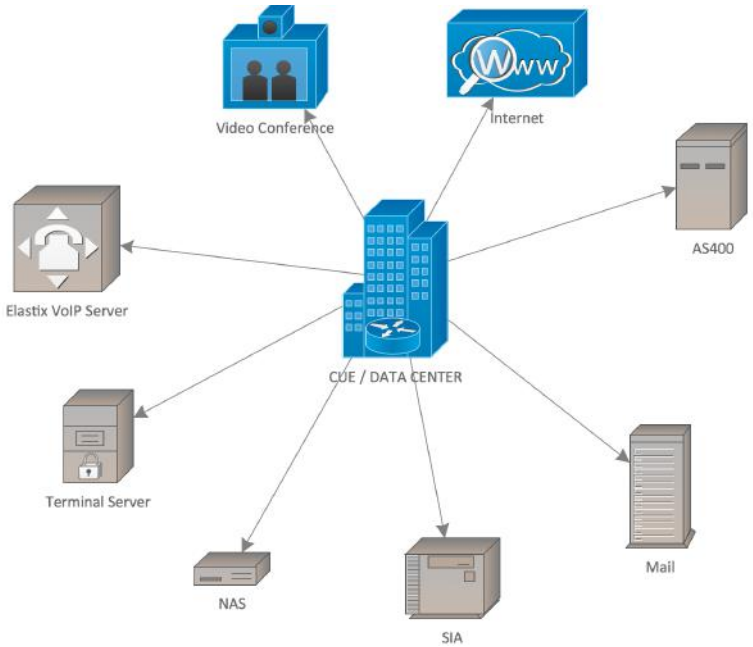


Ilustración 1-6 Principales Servicios y Aplicaciones - Caso de Estudio

1.3.1 Escenario de Simulación para análisis de tráfico

Para realizar las mediciones de tráfico de los diferentes servicios, se plantea el escenario de la *Ilustración 1-6*. La topología de red presenta tres hosts con diferentes sistemas operativos dos switches que simulan diferentes redes y un router para la el enrutamiento entre las redes. Para efectos de simulación los dispositivos se encuentran en dos redes 192.168.1.0/24, 192.168.2.0/24 y tienen habilitados un servicio a la vez para obtener mediciones de tráfico que luego se puedan usar para estimar el tráfico total por servicio y de esta manera calcular el tráfico general que requeriría una agencia de acuerdo a los servicios y número de usuarios que accedan a ellos.

Para el entorno de simulación se usa el software GNS3 (Equipos de Red Cisco) y VirtualBox (Máquinas Virtuales). En el capítulo 4 se revisará mas a fondo el uso del software GNS3 con configuraciones puntales para el caso de estudio.

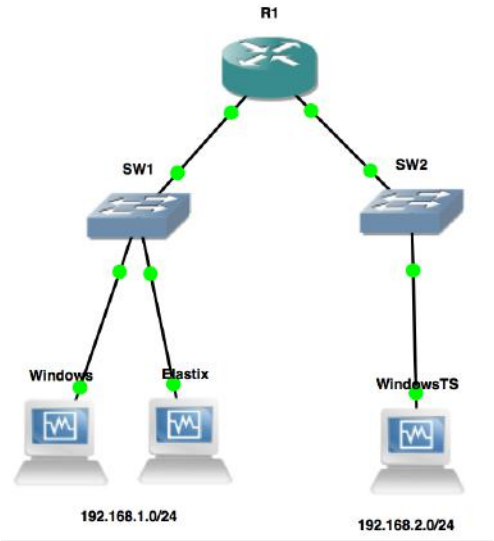


Ilustración 1-7 Entorno de Simulación

1.3.2 Análisis de Servicios de Red

a) Sistema SIA (Sistema Integrado Automotriz), servicio WEB

El Grupo Automotriz cuenta con un Sistema Integrado Automotriz, que entre otras funciones, ayuda con el ingreso de facturas de compra, control de inventario, ventas, manejo de bodegas, Kardex de repuestos, talleres, control de citas en los concesionarios automotrices, etc. El servicio es de acceso WEB, el servidor y bases de datos se encuentran localizados en las instalaciones del Data Center en Cuenca, de manera que el gran porcentaje del tráfico que se genera desde las agencias es hacia el centro de datos para el uso de este aplicativo.

El tráfico que se genera por este aplicativo se clasifica como de importancia alta y debe ser priorizado sobre otro tipo de tráfico WEB y peer to peer.

Ilustración 1-8 Sistema SIA Virtualinfo

Análisis de Tráfico

En la *Ilustración 1-8* se muestra cómo filtrar el tráfico http con NBAR. Este resultado corresponde al entorno de simulación, abriendo una página web del servidor de telefonía IP ubicado en la red 192.168.1.0/24 desde un host de la red 192.168.2.0/24 y pasando por el router TESIS en donde se encuentra habilitado el NBAR Protocol Discovery en ambas interfaces.

El resultado muestra el tráfico cursado por el router filtrado para el protocolo http. En los siguientes capítulos se utilizará este filtro y además un match *Ilustración 1-9* [1] que permite reconocer los paquetes http GET que contiene el URL especificado y de esta manera poder garantizar un determinado ancho de banda a este aplicativo. En el caso de estudio el *url-string* se reemplazaría con *sia.virtualinfo.com.ec.*

```
router(config-cmap)#
match protocol http url url-string
```

Ilustración 1-9 Configuración de NBAR para implementación de QoS para protocolos dinámicos

```
TESIS#sho ip nbar protocol-discovery protocol http
 FastEthernet0/0
                                Input                     Output
                                -----                     ------
   Protocol                     Packet Count              Packet Count
                                Byte Count                Byte Count
                                5min Bit Rate (bps)       5min Bit Rate (bps)
                                5min Max Bit Rate (bps)   5min Max Bit Rate (bps)
   ------------------------     ------------------------  ------------------------
   http                         2                         2
                                597                       414
                                0                         0
                                0                         0
   unknown                      3                         3
                                174                       174
                                0                         0
                                0                         0
   Total                        1931                      1730
                                1174589                   219312
                                19000                     2000
                                22000                     8000

 FastEthernet0/1
                                Input                     Output
                                -----                     ------
   Protocol                     Packet Count              Packet Count
                                Byte Count                Byte Count
                                5min Bit Rate (bps)       5min Bit Rate (bps)
                                5min Max Bit Rate (bps)   5min Max Bit Rate (bps)
   ------------------------     ------------------------  ------------------------
   http                         2                         2
                                414                       597
                                0                         0
                                0                         0
   unknown                      3                         3
                                174                       174
                                0                         0
                                0                         0
   Total                        1713                      1794
                                218566                    1163573
                                2000                      22000
                                9000                      22000
```

Ilustración 1-10 Filtrado Tráfico http NBAR

En la simulación también se incluye un monitoreo del consumo del ancho de banda en tiempo real, con la herramienta STG basada en el protocolo snmp. Para efectos de

[1] Ilustración tomada del Módulo de Calidad de Servicio Máster en Redes de Comunicaciones PUCE

simulación, el tráfico generado mostrado en la *Ilustración 1-11* hace referencia al acceso desde un host en la red 192.168.2.0/24 hacia el servidor WEB (Elastix) en la red 192.168.1.5/24. Previamente se habilitó el snmp-server y los traps en el router TESIS para poder monitorear la interfaz FastEthernet 0/1 con dirección 192.168.2.1. Se puede observar que el tráfico no es constante y depende de las consultas que se realizan al servidor web (Max. 738kbps).

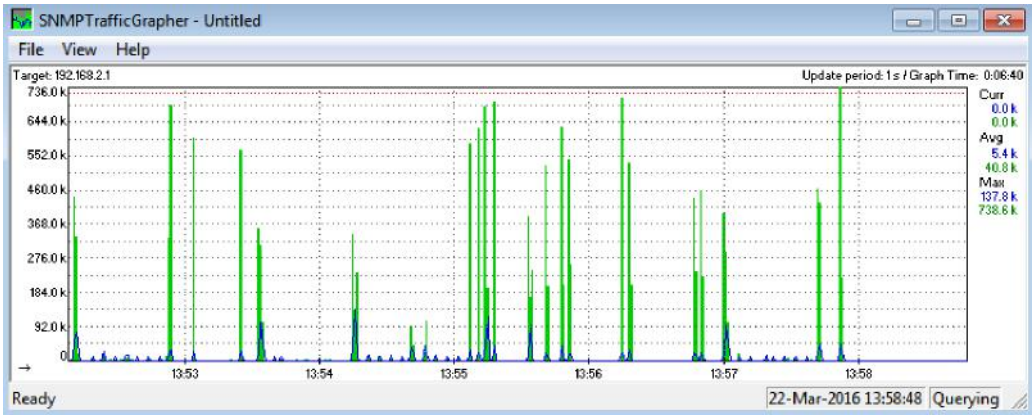


Ilustración 1-11 Tráfico Medido - Acceso a Web Server Elastix

b) Sistemas AS400

El sistema AS400 es un equipo de IBM de gama media-alta, para todo tipo de empresas. Concretamente en el caso de estudio este sistema se encuentra activo para consultas contables, ya que el Servicio de Rentas Internas requiere un resguardo de información de al menos 5 años.

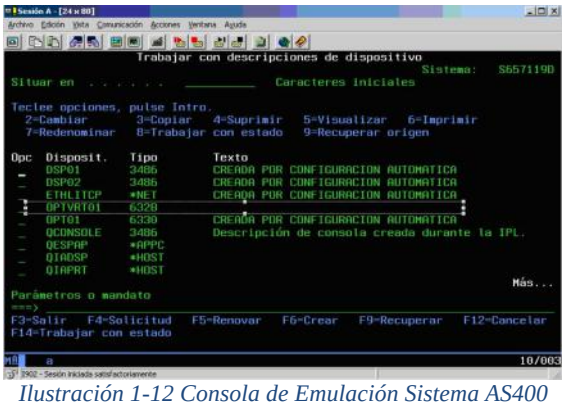


Ilustración 1-12 Consola de Emulación Sistema AS400

Análisis de Tráfico

De igual manera que el servicio SIA, el servidor AS400 se encuentra localizado en el data center en las instalaciones de Virtualinfo. Para conexiones remotas a este servicio desde las sucursales se cuenta con una consola de emulación PC5250 que utiliza el puerto 23 (Telnet-texto plano) y el puerto 992 en una capa de conexión segura SSL.

PC Function	Server Name	Port Non-SSL	Port SSL
Telnet (PC5250 Emulation)	telnet	23	992

Ilustración 1-13 Características de conexión de la consola PC5250

Básicamente se debería filtrar el protocolo de telnet para luego incorporar el control del consumo de recursos (ancho de banda) por parte de este servicio. En la *Ilustración 1-14* se muestra el resultado del filtrado por medio del NBAR Protocol Discovery. De igual manera que el protocolo HTTP, el protocolo TELNET deberá concatenarse con un match [2] para luego aplicarlo a una clase y política. Estas configuraciones se revisarán en detalle en el Capítulo 3.

[2] Descripción del uso de match en NBAR Cisco, http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/configuration/15-mt/qos-nbar-15-mt-book/nbar-cust-protcl.html

```
TESIS#sho ip nbar protocol-discovery protocol telnet

 FastEthernet0/0
                         Input                     Output
                         -----                     ------
   Protocol              Packet Count              Packet Count
                         Byte Count                Byte Count
                         5min Bit Rate (bps)       5min Bit Rate (bps)
                         5min Max Bit Rate (bps)   5min Max Bit Rate (bps)
   ----------------------- ------------------------ ------------------------
   telnet                284                       101
                         15764                     10238
                         0                         0
                         3000                      3000
   unknown               3                         3
                         174                       174
                         0                         0
                         0                         0
   Total                 7425                      6818
                         1591325                   601848
                         0                         0
                         27000                     13000
```

Ilustración 1-14 Filtrado de Tráfico Telnet NBAR

Al monitorear una conexión telnet activa, se observa que el tráfico alcanza picos de 12.7kbps. Este tipo de tráfico no representa gran consumo de ancho de banda pero puede significar un problema al tener varios usuarios simultáneos sobre una conexión dedicada.

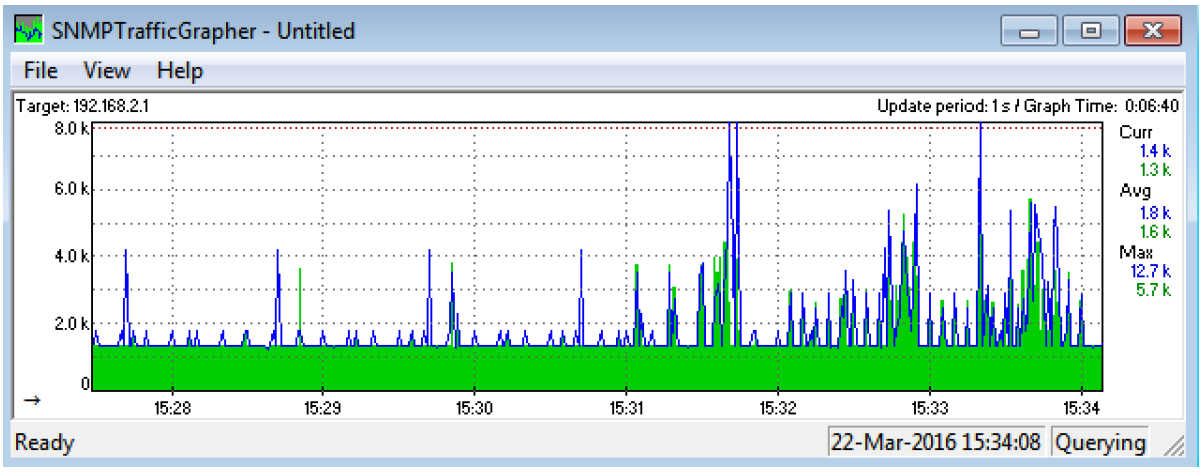


Ilustración 1-15 Tráfico Medido – Conexión Telnet

c) Servicio de Correo

Las diferentes empresas cuentan con dominios separados de correo. Estos dominios se encuentra alojados en un servidor de correo en el Data Center de la ciudad de Cuenca en las instalaciones de Virtualinfo.

- mail.virtualinfo.com.ec
- mail.logimanta.com.ec
- mail.neomotors.com.pe
- mail.merquiauto.com.ec
- mail.ecsyauto.com.ec
- mail.quitomotors.com.ec

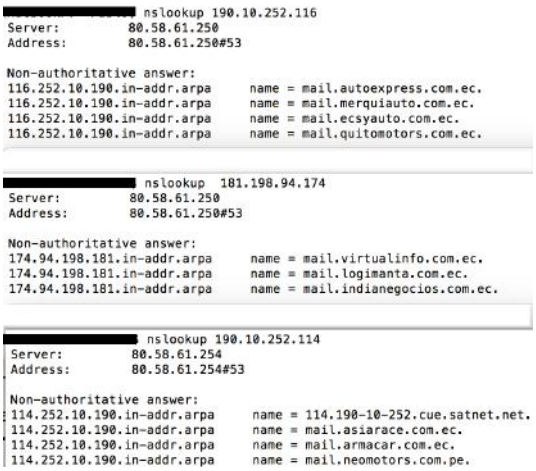


Ilustración 1-16 Dominios de Correo

El consumo de ancho de banda definido para correo no es crítico, ya que se trata de un tráfico tolerante a demoras, sin embargo se tomará en cuenta en el siguiente capítulo para el cálculo de presupuesto de capacidad por enlace.

d) Servidor de Telefonía Elastix VoIP

Cada empresa cuenta con un servicio de telefonía. Las diferentes agencias del caso de estudio se conectan a un servidor central de telefonía ubicado en el Data Center en la ciudad de Cuenca. Las líneas telefónicas externas de cada empresa (troncales) son líneas digitales IP contratadas con diferentes proveedores (TV CABLE, CNT y

ETAPA), y se conectan a la central telefónica Elastix *Ilustración 1-17* por medio de los enlaces dedicados.

Hay que tener en cuenta que cada troncal IP de telefonía maneja su respectivo segmento de red, que deberá ser enrutado y tener un correcto tratamiento de tráfico a través de los enlaces dedicados. Estas configuraciones se analizarán en los capítulos siguientes.

Ilustración 1-17 Consola de administración del servidor de Telefonía

Hay que tener en cuenta que para el filtrado de paquetes y posterior manejo para calidad de servicio tenemos que referirnos al protocolo RTP. Configuramos NBAR para obtener los paquetes que circulan por la red usando el protocolo RTP. Para efectos de simulación se tiene una llamada activa entre dos softphones.

```
TESIS#sho ip nbar protocol-discovery protocol rtp

 FastEthernet0/0
                          Input                     Output
                          -----                     ------
   Protocol               Packet Count              Packet Count
                          Byte Count                Byte Count
                          5min Bit Rate (bps)       5min Bit Rate (bps)
                          5min Max Bit Rate (bps)   5min Max Bit Rate (bps)
   ------------------------ ------------------------ ------------------------
   rtp                    6108                      0
                          1307112                   0
                          22000                     0
                          40000                     0
   unknown                1533                      2137
                          125769                    1349309
                          0                         18000
                          10000                     42000
   Total                  7692                      5214
                          1447172                   1573934
                          22000                     18000
                          51000                     55000
```

Ilustración 1-18 Filtrado de Tráfico RTP NBAR

Para la estimación de tráfico de una llamada de voz sobre la central de telefonía IP, se realizó la simulación utilizando las máquinas virtuales Windows y Elastix con la misma topología de la *Ilustración 1-7*. Se realizaron métricas para varios intentos de llamadas. La *Ilustración 1-19* muestra los softphones instalados en cada máquina de Windows y registrados en la central Elastix con una llamada en curso.

Ilustración 1-19 Simulación de 1 llamada con máquinas virtuales y GNS3

El tráfico medido muestra un consumo de 86kbps para una llamada establecida utilizando un códec G711 que muestrea a 8000 muestras por segundo y codifica en 8 bits, dando como resultado 64kbps. El exceso de carga viene definido por cabeceras extras para la comunicación.

Ilustración 1-20 Tráfico Medido – Consumo de ancho de banda de 1 llamada usando el códec G.711

e) Sevicio de Video Conferencia WebEx y mensajería instantánea Jabber

Las empresas cuentan con un servicio para video conferencias a través del aplicativo WebEx. El servicio de videoconferencia WebEx es un servicio de pago de Cisco, que permite realizar reuniones en línea dinámicas con herramientas de colaboración integradas. Los requerimientos de tráfico de red son básicamente internet.

Para el servicio de mensajería instantánea, las empresas utilizan un servidor con Jabber centralizado en Virtualinfo. Para la conexión y acceso a este servicio se usan los enlaces dedicados.

Ilustración 1-21 Cisco WebEx

f) Servicio de Escritorio Remoto TS (Terminal Server)

El servicio de Escritorio Remoto es utilizado de manera interna (intranet) y externa (Internet), por lo cuál el ancho de banda estimado se considerará para enlaces dedicados y para los enlaces de internet.

Análisis de Tráfico

De igual manera para analizar el tráfico del servicio utilizamos la topología de la *Ilustración 1-6*. Realizamos una conexión entre los equipos Windows ubicados en diferentes segmentos de red e interconectados por el router TESIS.

Se habilita el servicio de Escritorio Remoto y se realizan las mediciones en la interfaz del host “WindowsTS” para verificar el aumento en el consumo de red.

Ilustración 1-22 Windows Conexión a Escritorio Remoto

Cabe indicar que el consumo de red depende de la configuración del tamaño, resolución y rendimiento de la pantalla en el cliente de conexión a Escritorio Remoto.

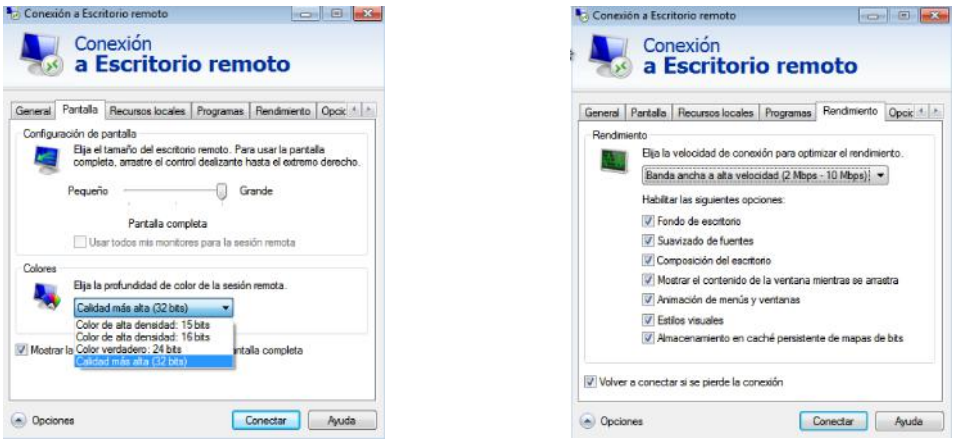


Ilustración 1-23 Configuración Cliente Escritorio Remoto

Al configurar el cliente de escritorio remoto en la calidad más alta y con todas las opciones habilitadas, obtenemos el consumo mostrado en la *Ilustración 1-24*. Se tiene un pico máximo de la tasa de datos de 1Mbps.

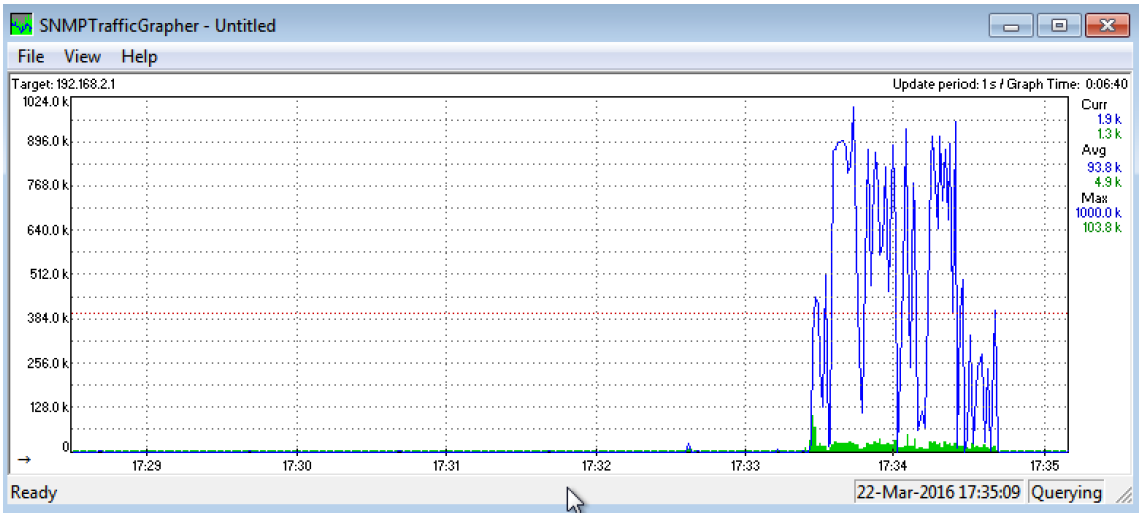


Ilustración 1-24 Tráfico Medido – Servicio de Escritorio Remoto con alta calidad

Configurando el cliente con una tasa de conexión media (Enlace de 2Mbps) y sin opciones como fondo de escritorio o animaciones, obtenemos una tasa de datos de 893kbps. Aunque la diferencia no es grande, en este caso se puede observar una menor densidad de tráfico.

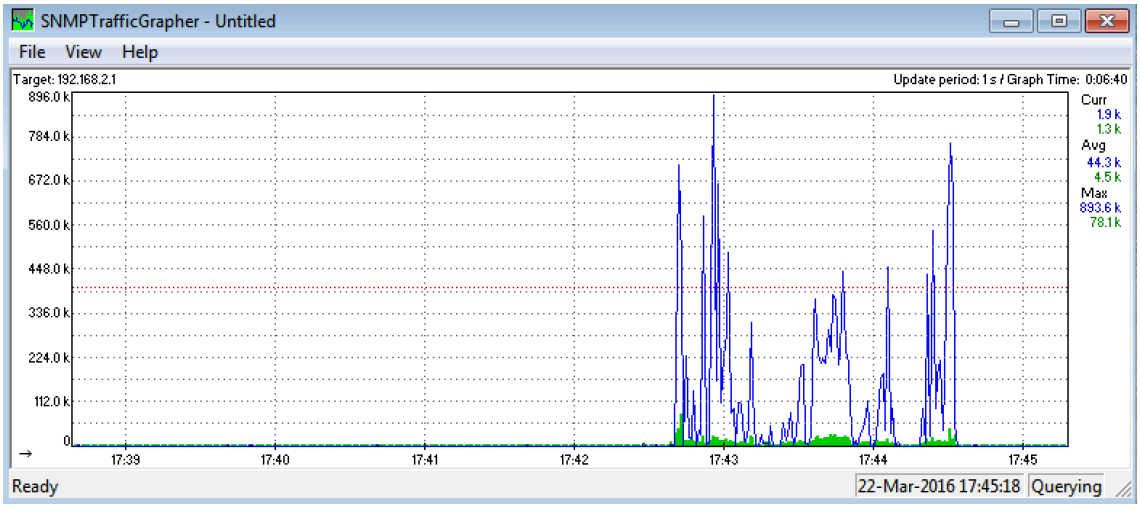


Ilustración 1-25 Tráfico Medido – Servicio de Escritorio Remoto con calidad media

Capítulo 2 : PROTOCOLOS DE TUNELIZACIÓN Y ENRUTAMIENTO DINÁMICO

2.1 Túnel GRE [2]

Los túneles se utilizan para el transporte de un protocolo de red sobre otro, por medio de la encapsulación de sus paquetes.

- Cuando el túnel se construye en la capa IP se denomina túnel IP.
- Pueden verse como rutas que eluden los mecanismos de encaminamiento convencionales.
- Las direcciones IP públicas "externas" del router identifican los "puntos finales" del túnel. En el caso de estudio, las direcciones IP públicas, hacen referencia a la red del proveedor.

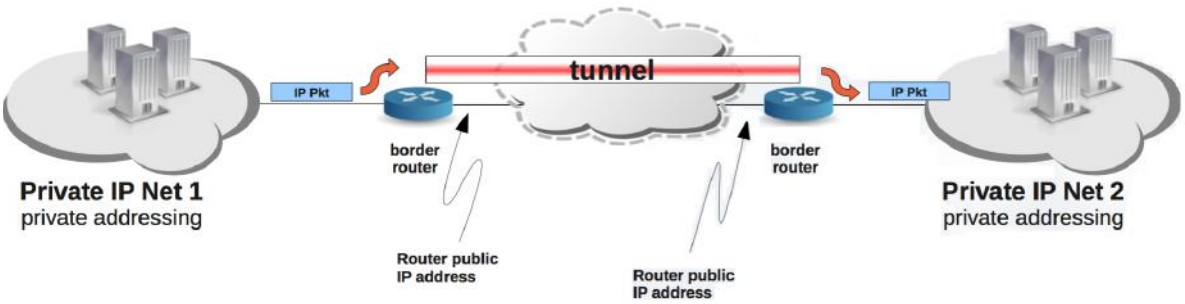


Ilustración 2-1 Topología Túnel IP

Cada paquete IP y su información de direccionamiento se encapsulan dentro de otro paquete, cuyo formato corresponde a la red externa del proveedor (red administrada por el proveedor). El destino, en el caso de estudio las agencias o sucursales, pueden ser alcanzadas de manera transparente y sin necesidad de que la fuente debe conocer la topología del proveedor o viceversa.

Se tienen varios tipos de túneles identificables por el nivel de la capa de red en la que se establece o por la tecnología sobre la que se implementan. Entre los mas conocidos están:

- L2TP (Protocolo de tunelización de Capa 2)
- MPLS (Multiprotocol Label Switching)
- GRE (Generic Routing Encapsulation)
- PPTP (Point-to-Point Tunneling Protocol)
- PPPoE (point-to-point protocol over Ethernet)
- PPPoA (point-to-point protocol over ATM)
- IPSec (Internet Protocol security)

En el presente caso de estudio se revisará una solución de conectividad con la implementación del protocolo de encapsulación GRE (Generic Routing Encapsulation), el cuál ofrece la posibilidad de trabajar como una overlay que soporta otros protocolos sobre GRE. Esta función permite implementar un protocolo de enrutamiento estático o dinámico independiente de la topología del proveedor.

GRE [9] es un protocolo originalmente desarrollado por Cisco Systems, pero que se ha llegado a convertir en un estándar. El protocolo se encuentra definido en los RFC 1701, 1702 y 2784. Es un protocolo de túnel, es decir, que permite transportar paquetes de una red a través de otra red diferente. La especificación RFC básicamente explica la estructura de la cabecera GRE, la cuál es de longitud variable (4 a 16 bytes) con campos opcionales.

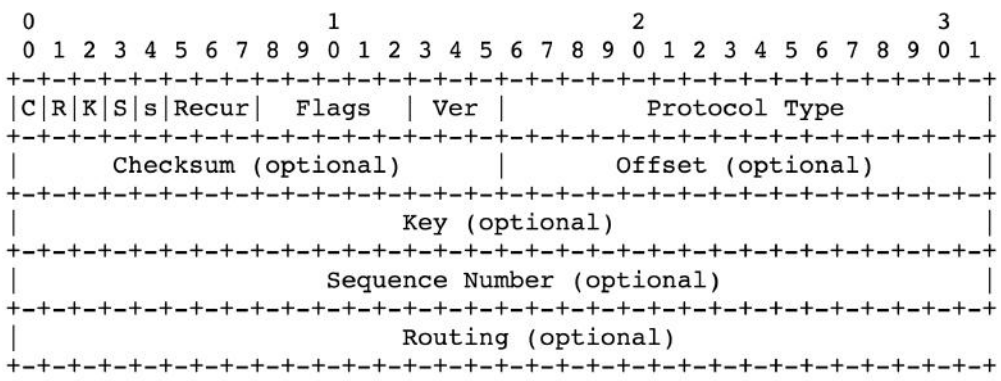


Ilustración 2-2 Cabecera GRE

- **C, presencia del campo de integridad de la trama o *Checksum*. 1 bit.** Si es 1 los campos Checksum y Offset están presentes.
- **R, presencia del campo de enrutamiento o *Routing*. 1 bit.** Si es 1 el campo routing tiene información válida y los campos Checksum y Offset están presentes.
- **K, presencia de clave o *Key*. 1 bit.** Si es 1 el campo Key existe y tiene información válida.
- **S, presencia del número de secuencia o campo *Sequence Number*. 1 bit.** Si es 1 el campo Sequence number existe y tiene información válida.
- **s, Campo Strict Source Route. 1 bit.** Este campo está definido en otros documentos. Se recomienda ponerlo a 1 sólo si toda la información de enrutamiento está formada por rutas estrictas.
- **Recur, campo *Recursion Control*. 3 bits.** Número de encapsulaciones recursivas permitidas. Por defecto 0.
- **Flags. 5 bits.** Reservado. Poner a 0.
- **Version. 3 bits.** Versión del protocolo GRE. Debe ser 0.
- **Protocol. 16 bits.** Indica el protocolo contenido en el paquete GRE. Para ello utiliza los mismo indicadores que Ethernet. Por ejemplo, si dentro del túnel GRE viaja un servicio MPLS, el valor de este campo sería 0x8847.
- **Checksum. 16 bits.** Opcional. Contiene la suma en complemento a 1 de los datos y la cabecera GRE.

- **Offset. 16 bits.** Opcional. Indica el primer octeto a examinar dentro del campo routing para conocer la entrada de enrutamiento activa.
- **Key. 32 bits.** Opcional. Contiene un número insertado por la parte encapsuladora del túnel que puede utilizarse en destino para propósitos de comprobación del remitente correcto.
- **Sequence Number. 32 bits.** Opcional. Contiene un número insertado por la parte encapsuladora del túnel que puede utilizarse en destino para controlar el orden de los paquetes.
- **Routing. Longitud variable.** Opcional. Este campo consiste en una lista de rutas.[3]

2.1.1 Proceso de Encapsulación

En el proceso de encapsulación IP, cada router de borde crea un pseudo-dispositivo de red que se encuentra asociado a la dirección IP externa (IP del proveedor). Cuando se envía un paquete a través de este pseudo-device, éste se encapsula en un paquete IP y se envía al router de borde remoto. Una vez el paquete es recibido a través del pseudo-device, se des encapsula y se trata como cualquier paquete IP de entrada. El pseudo-device solo acepta paquetes provenientes del border router remoto. La tabla de enrutamiento de los routers usan este pseudo-device de red para enrutar los paquetes de las redes remotas.

El paquete IP externo (Outer IP packet) tiene un formato similar al presentado en la *Ilustración 3*.

[3] RFC 1701 Generic Routing Encapsulation (GRE)[3]

Ilustración 2-3 Formato Encapsulación IP

Outer IP header (Cabecera IP Externa):

- Contiene la IP de origen y destino de los puntos origen y destino del túnel.
- Dentro del outer IP header en el campo IP protocol se define el tipo de protocolo de encapsulación usado. En nuestro caso el número de protocolo IPv4 para GRE es el **47**. [4]

Tunnel Header (Cabecera del Túnel):

- Dependiendo del tipo de encapsulación, se puede incluir una cabecera propia del protocolo de encapsulación para incluir parámetros propios de la encapsulación. GRE incorpora una cabecera en el proceso de encapsulación que incluye algunos campos opcionales detallados en la *Ilustración 2-2*.

[4] https://en.wikipedia.org/wiki/List_of_IP_protocol_numbers

Inner IP Header (Cabecera IP Interior):

- Contiene las direcciones IP origen e IP destino del paquete IP original. El Inner IP Header o cabecera interior IP, se encapsula como payload del paquete IP externo.

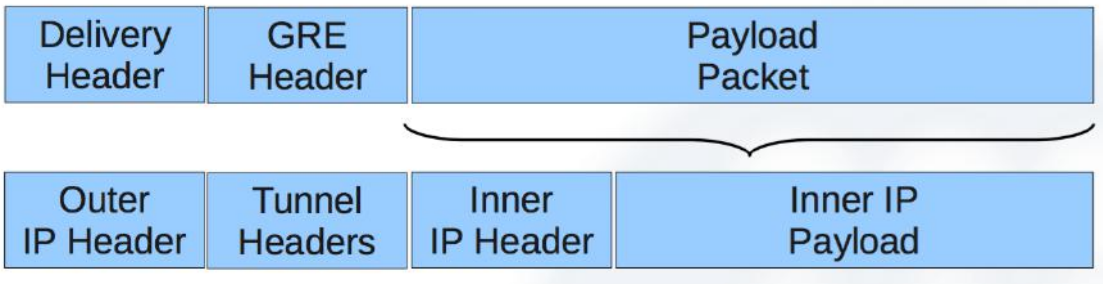


Ilustración 2-4 Formato de encapsulación GRE

2.2 Simulación y Comandos básicos

La simulación de los túneles GRE se realiza mediante el software GNS3 con la topología de la *Ilustración 2-5*. Para la simulación se toman en cuenta los comandos básicos para establecer un túnel GRE entre equipos CISCO y entre CISCO y MIKROTIK.

El software GNS3 nos permite la virtualización de una amplia gama de equipos. Para la presente simulación se han virtualizado los siguientes equipos:

- Cisco IOS c3745-advipservicesk9
- RouterOS Mikrotik image
- Windows 7

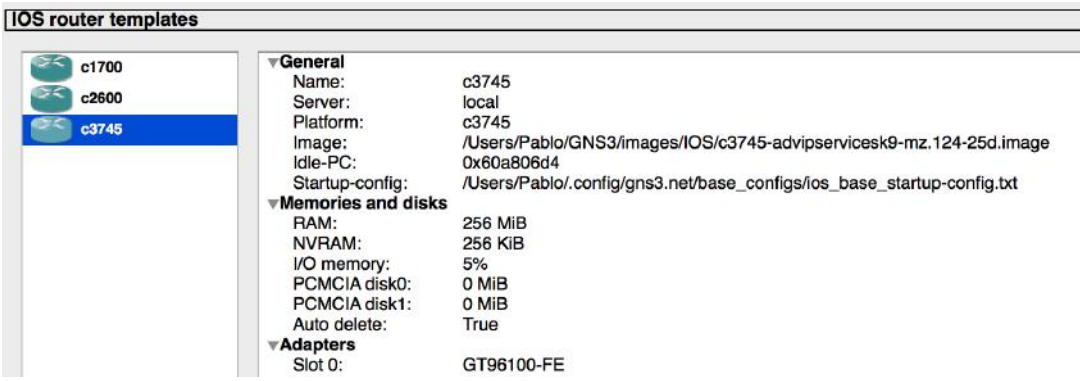


Ilustración 2-5 Cisco 3745 IOS

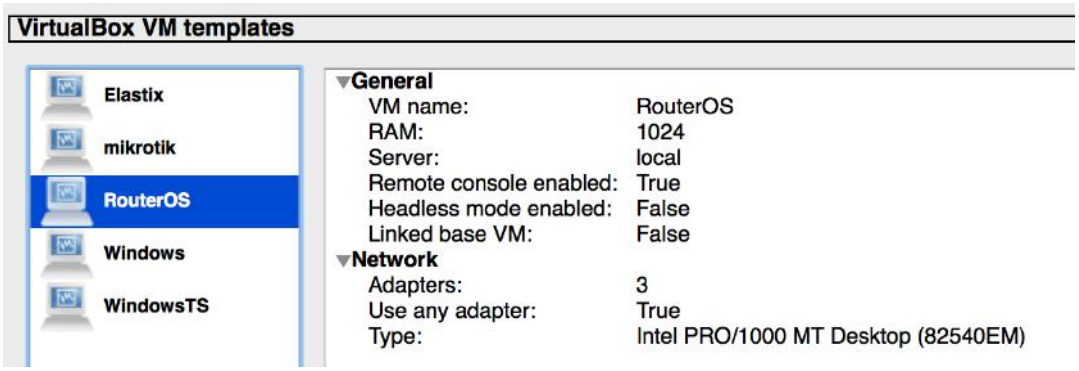


Ilustración 2-6 RouterOS Mikrotik Image

Estos equipos corresponden a una topología genérica del caso de estudio, ya que las agencias en gran parte cuentan con equipos mikrotik o equipos cisco de gama media, por lo cuál los túneles IP se establecerían entre estos equipos.

Como referencia para la simulación se toman en cuenta las principales agencias del caso de estudio como son Quito, Cuenca y Guayaquil. Se pretende establecer túneles IP entre las agencias de Guayaquil y Quito con el concentrador de Cuenca en donde se encuentra el Data Center con los diferentes aplicativos mencionados en el Capítulo 1. La *Tabla 2-1* describe el direccionamiento de los dispositivos utilizados en simulación.

Ubicación	Equipo	Red	Dirección IP	Máscara	Gateway
Cuenca	Host2	LAN	192.168.50.100	255.255.255.0	192.168.50.1
	R2	LAN	192.168.50.1	255.255.255.0	N/A
		WAN F0/1	172.16.1.1	255.255.255.252	N/A
		WAN F0/0	172.16.1.5	255.255.255.252	N/A
		TUNEL CUE-UIO	10.10.10.5	255.255.255.252	N/A
		TUNEL CUE-GYE	10.10.10.1	255.255.255.252	N/A
Quito	Host4	LAN	192.168.150.100	255.255.255.0	192.168.150.1
	R1	LAN	192.168.150.1	255.255.255.0	N/A
		WAN	172.16.1.6	255.255.255.252	N/A
		TUNEL UIO-CUE	10.10.10.6	255.255.255.252	N/A
Guayaquil	Windows	LAN	192.168.100.100	255.255.255.0	192.168.100.1
	Mikrotik	LAN	192.168.100.1	255.255.255.0	N/A
		WAN	172.16.1.2	255.255.255.252	N/A
		TUNEL GYE-CUE	10.10.10.2	255.255.255.252	N/A

Tabla 2-1 Direccionamiento IP para la Simulación de Túneles IP

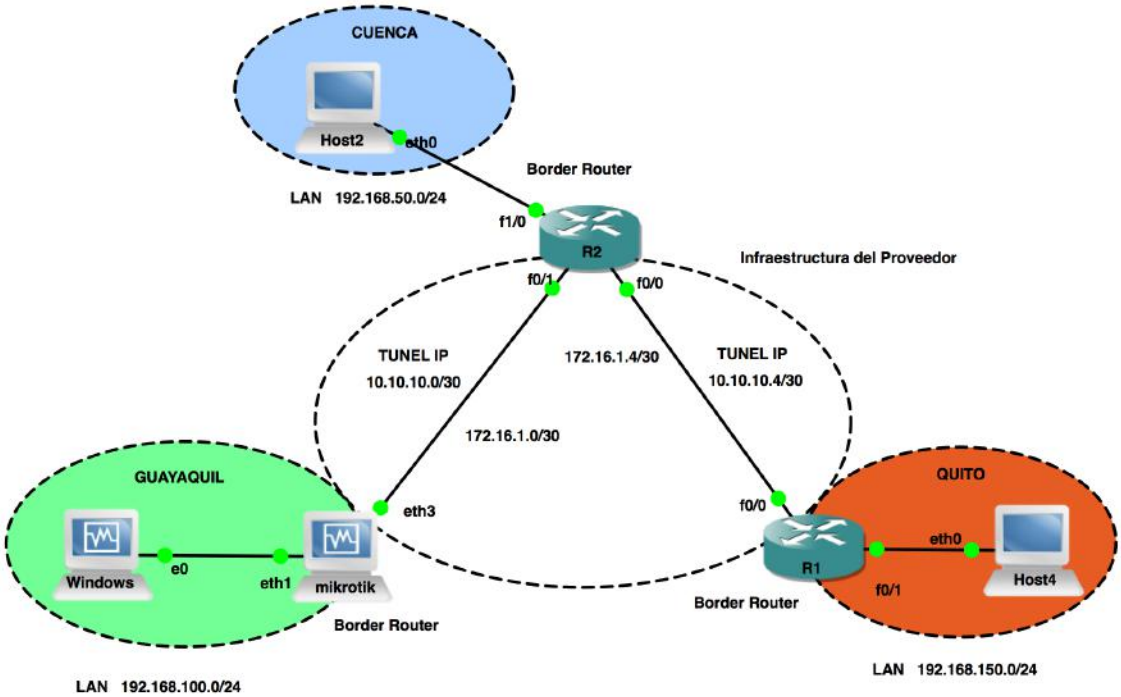


Ilustración 2-7 Topología GNS3 para simulación de Túneles IP

Para la administración del equipo mikrotik se utiliza la herramienta de conexión remota Winbox[5]. El acceso al Winbox se realiza desde el host Windows que se encuentra en la red LAN de la Agencia Guayaquil. Una vez levantados los túneles IP se podrán configurar políticas de acceso o ACL para administrar el router Mikrotik de manera remota desde la matriz en Virtualinfo Cuenca.

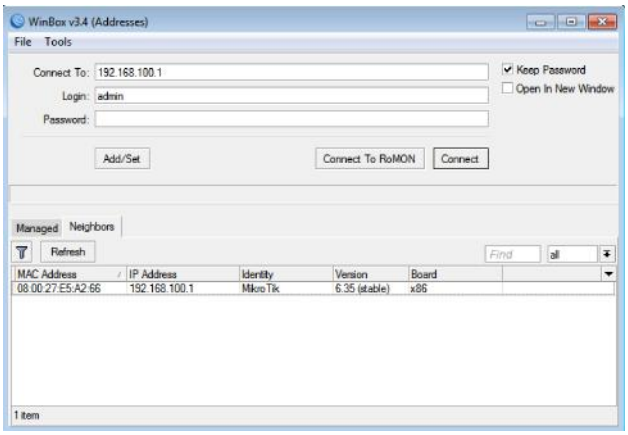


Ilustración 2-8 Consola Winbox

Para la administración de los routers Cisco, el entorno GNS3 brinda accesos por consola a cada equipo, por lo cuál se puede realizar la configuración directamente sobre el equipo o mediante conexión remota desde los host. De igual manera, una vez establecidos los túneles se pueden implementar políticas de acceso.

Se definen los siguientes pasos para la configuración inicial de Túneles GRE:

1. Configurar el direccionamiento IP de acuerdo a lo especificado en la *Tabla 2-1*.

En el entorno de simulación GNS3 la configuración del direccionamiento IP de los hosts nativos se realiza de acuerdo a la *Ilustración 2-9*.

[5] http://wiki.mikrotik.com/wiki/Manual:Winbox

Ilustración 2-9 Configuración de direccionamiento IP de los Host GNS3

R2

```
R2#conf term
R2(config)#interface FastEthernet 1/0
R2(config-if)#ip address 192.168.50.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#interface FastEthernet 0/1
R2(config-if)#ip address 172.16.1.1 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#interface FastEthernet 0/1
R2(config-if)#interface FastEthernet 0/0
R2(config-if)#ip address 172.16.1.5 255.255.255.252
R2(config-if)#no shutdown


R2#sho ip interface brief

Interface          IP-Address   OK? Method Status
Protocol
FastEthernet0/0     172.16.1.5     YES manual up      up
FastEthernet0/1     172.16.1.1     YES manual up      up
FastEthernet1/0     192.168.50.1  Y ES manual up      up
```

MIKROTIK

```
[admin@MikroTik] > ip address add
address=192.168.100.1/24 comment="LAN GYE"
interface=ether1 network=192.168.100.0

[admin@MikroTik] > ip address  add address=172.16.1.2/30
comment=WAN interface=ether3 network=172.16.1.0
```

```
[admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   ;;; LAN GYE
     192.168.100.1/24   192.168.100.0   ether1
 1   ;;; WAN
     172.16.1.2/30      172.16.1.0      ether3
```

Al igual que en los equipos Cisco, la configuración de los equipos Mikrotik se puede realizar mediante consola o de manera gráfica por medio de la consola Winbox. En la *Ilustración 2-9* se muestra la configuración del direccionamiento IP utilizando la consola Winbox. La consola gráfica es muy intuitiva pero poco práctica ya que requiere de mucho tiempo para realizar las configuraciones.

R1

```
R1#conf term
R1(config)#interface FastEthernet 0/1
R1(config-if)#ip address 192.168.150.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#interface FastEthernet 0/0
R1(config-if)#ip address 172.16.1.6 255.255.255.252
R1(config-if)#no shutdown

R1#sho ip interface brief

Interface      IP-Address     OK? Method Status
Protocol
FastEthernet0/0   172.16.1.6      YES manual up      up
FastEthernet0/1   192.168.150.1   YES manual up      up
```

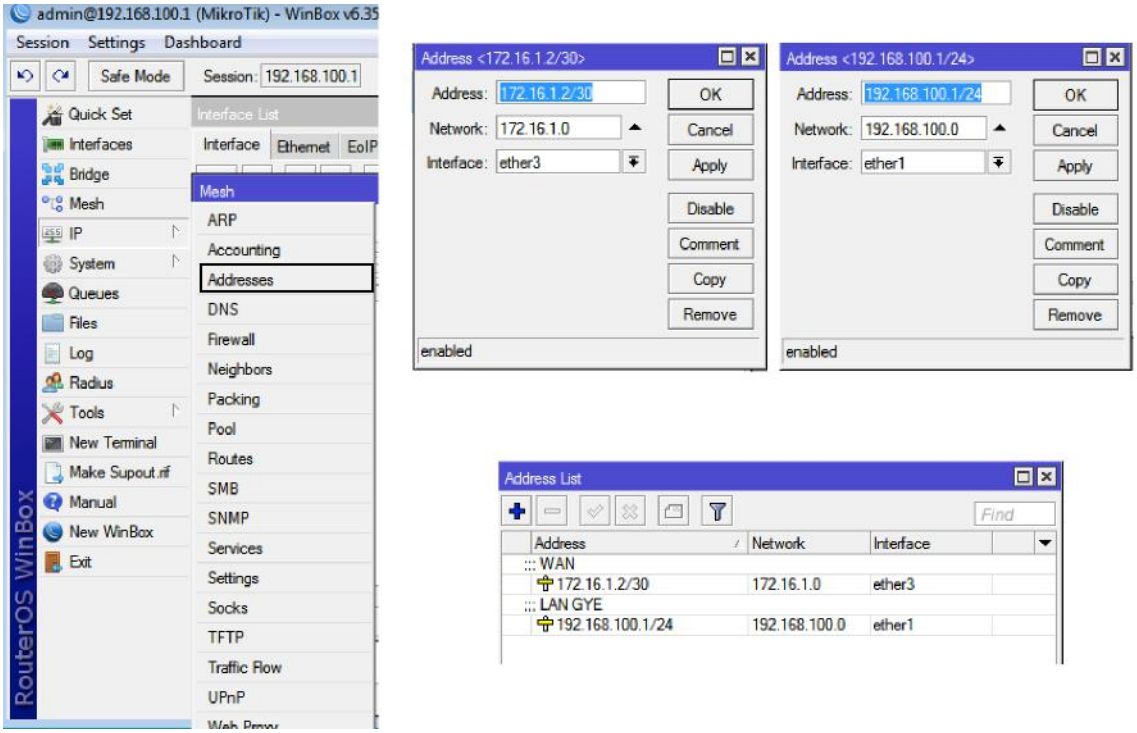


Ilustración 2-10 Direccionamiento IP Mikrotik mediante Winbox

2. Configurar los túneles entre los dispositivos Cisco y Mikrotik.

R2

TUNEL 1 CUE-GYE

```
R2#conf term
R2(config)#interface tunnel 1
R2(config-if)#description CUE-GYE
R2(config-if)#ip address 10.10.10.1 255.255.255.252
R2(config-if)#tunnel source fastEthernet 0/1
R2(config-if)#tunnel destination 172.16.1.2
R2(config-if)#tunnel mode gre ip
R2(config-if)#no shutdown
```

TUNEL 2 CUE-UIO

```
R2#conf term
R2(config)#interface tunnel 2
R2(config-if)#description CUE-UIO
R2(config-if)#ip address 10.10.10.5 255.255.255.252
R2(config-if)#tunnel source fastEthernet 0/0
R2(config-if)#tunnel destination 172.16.1.6
R2(config-if)#tunnel mode gre ip
```

```
R2(config-if)#no shutdown

R2#sho ip int brief
Interface       IP-Address    OK? Method Status    Protocol
FastEthernet0/0   172.16.1.5   YES manual up        up
FastEthernet0/1   172.16.1.1   YES manual up        up
FastEthernet1/0   192.168.50.1 YES manual up        up
Tunnel1           10.10.10.1   YES manual up        up
Tunnel2           10.10.10.5   YES manual up        up
```

MIKROTIK

TUNEL 1 GYE-CUE

```
[admin@MikroTik]>interface gre add local-address=172.16.1.2
name =tunnel1 remote-address = 172.16.1.1
[admin@MikroTik]>ip address add address=10.10.10.2/30
interface = tunnel1 network = 10.10.10.0
[admin@MikroTik]>interface gre comment tunnel1 GYE-CUE
```

R1

TUNEL 2 UIO-CUE

```
R1#conf term
R1(config)#interface tunnel 2
R1(config-if)#description UIO-CUE
R1(config-if)#ip address 10.10.10.6 255.255.255.252
R1(config-if)#tunnel source fastEthernet 0/0
R1(config-if)#tunnel destination 172.16.1.5
R1(config-if)#tunnel mode gre ip
R1(config-if)#no shutdown
```

3. Implentar un enrutamiento estático para alcanzar las redes privadas a través de las interfaces Tunel. En el *Tema 2.2 Tipos de Enrutamientos Dinámicos y Route Map* revisaremos las configuraciones del protocolo OSPF para facilitar la administración de rutas.

R2

Rutas para alcanzar las redes privadas de la agencia Quito y Guayaquil:

```
R2#conf term
R2(config)#ip route 192.168.150.0 255.255.255.0 10.10.10.6
R2(config)#ip route 192.168.100.0 255.255.255.0 10.10.10.2

R2#sho ip route

S    192.168.150.0/24 [1/0] via 10.10.10.6
     172.16.0.0/30 is subnetted, 2 subnets
C       172.16.1.4 is directly connected, FastEthernet0/0
C       172.16.1.0 is directly connected, FastEthernet0/1
     10.0.0.0/30 is subnetted, 2 subnets
C       10.10.10.0 is directly connected, Tunnel1
C       10.10.10.4 is directly connected, Tunnel2
C    192.168.50.0/24 is directly connected, FastEthernet1/0
S    192.168.100.0/24 [1/0] via 10.10.10.2
```

El Gateway para cada ruta es la dirección destino de las interfaces tunelizadas correspondientes.

MIKROTIK

Rutas para alcanzar las redes privadas de las agencias Cuenca y Quito

```
[admin@MikroTik]>ip route add distance=1 dst-address =
192.168.50.0/24 gateway = 10.10.10.1
```

[admin@MikroTik] > **ip route print**

Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme, B - blackhole, U - unreachable, P - prohibit

#	DST-ADDRESS	PREF-SRC	GATEWAY	DISTANCE
0 ADC	10.10.10.0/30	10.10.10.2	tunnel1	0
1 ADC	172.16.1.0/30	172.16.1.2	ether3	0
2 A S	192.168.50.0/24	10.10.10.1	1	

3 ADC 192.168.100.0/24 192.168.100.1 ether1 0

R1

Rutas para alcanzar las redes privadas de la agencia Cuenca y Guayaquil:

```
R1#conf term
R1(config)#ip route 192.168.50.0 255.255.255.0 10.10.10.5
R1(config)#ip route 192.168.100.0 255.255.255.0 10.10.10.5
R1#sho ip route

Gateway of last resort is not set

C    192.168.150.0/24 is directly connected, FastEthernet0/1
     172.16.0.0/30 is subnetted, 1 subnets
C       172.16.1.4 is directly connected, FastEthernet0/0
     10.0.0.0/30 is subnetted, 1 subnets
C       10.10.10.4 is directly connected, Tunnel2
S    192.168.50.0/24 [1/0] via 10.10.10.5
S    192.168.100.0/24 [1/0] via 10.10.10.5
```

4. Realizar pruebas de conectividad.

Para las pruebas de conectividad se ejecutarán pings desde cada red privada hacia las agencias destino.

Cuenca – Quito

Se realiza una traza desde CUE red 192.168.50.0/24 hacia UIO red 192.168.150.0/24

```
VPCS> ping 192.168.150.100
84 bytes from 192.168.150.100 icmp_seq=1 ttl=62 time=31.498 ms
84 bytes from 192.168.150.100 icmp_seq=2 ttl=62 time=33.275 ms
84 bytes from 192.168.150.100 icmp_seq=3 ttl=62 time=33.151 ms
84 bytes from 192.168.150.100 icmp_seq=4 ttl=62 time=27.917 ms
84 bytes from 192.168.150.100 icmp_seq=5 ttl=62 time=27.085 ms
```

Ilustración 2-11 Ping CUE-UIO

Cuenca – Guayaquil

Se realiza una traza desde CUE red 192.168.50.0/24 hacia GYE red 192.168.100.0/24.

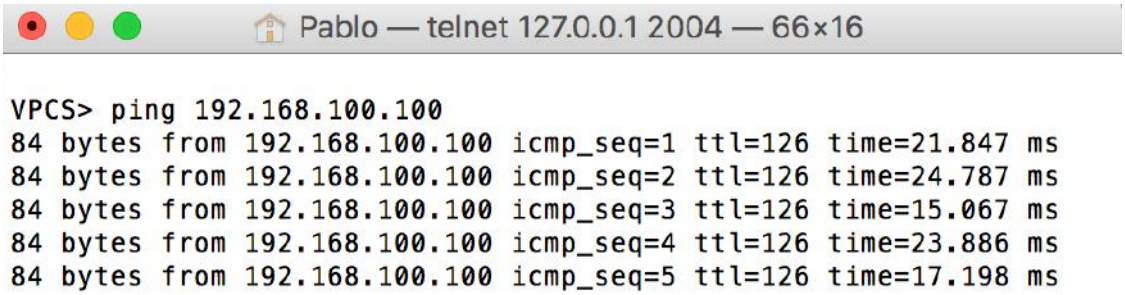


Ilustración 2-12 Ping CUE-GYE

Guayaquil – Quito

Se realiza un ping desde GYE red 192.168.100.0/24 hacia la red UIO 192.168.150.0/24. Adicional se realiza una traza hacia el destino y se verifica los saltos por los túneles IP configurados.

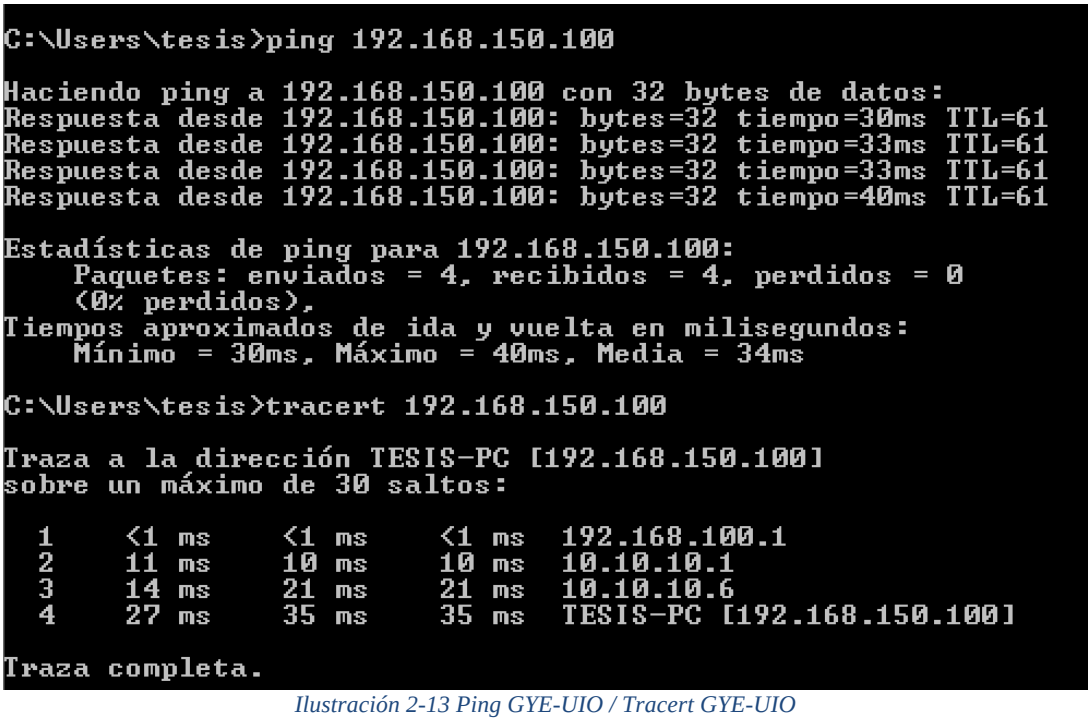


Ilustración 2-13 Ping GYE-UIO / Tracert GYE-UIO

2.3 Análisis del proceso de encapsulación con Wireshark

Mediante la interfaz del simulador GNS3 podemos analizar el tráfico de red que circula por los enlaces de la topología. Para efectos del análisis se monitorea el enlace entre la agencia Guayaquil y Cuenca. Se realiza un ping desde la agencia GYE red 192.168.100.0/24 hacia la agencia CUE red 192.168.50.0/24 y así generar tráfico para el análisis de los paquetes encapsulados

En la *Ilustración 2-14* se valida que el protocolo GRE se encuentra activo y se constata la estructura de los paquetes encapsulados, los cuales contiene las cabeceras Inner o internas del paquete original (Paquete IP, IP Origen: 192.168.100.100, IP Destino: 192.168.50.100) así como las cabeceras Outer o externas del paquete encapsulado (Paquete IP Encapsulado, IP Origen: 172.16.1.2, IP Destino: 172.16.1.1).

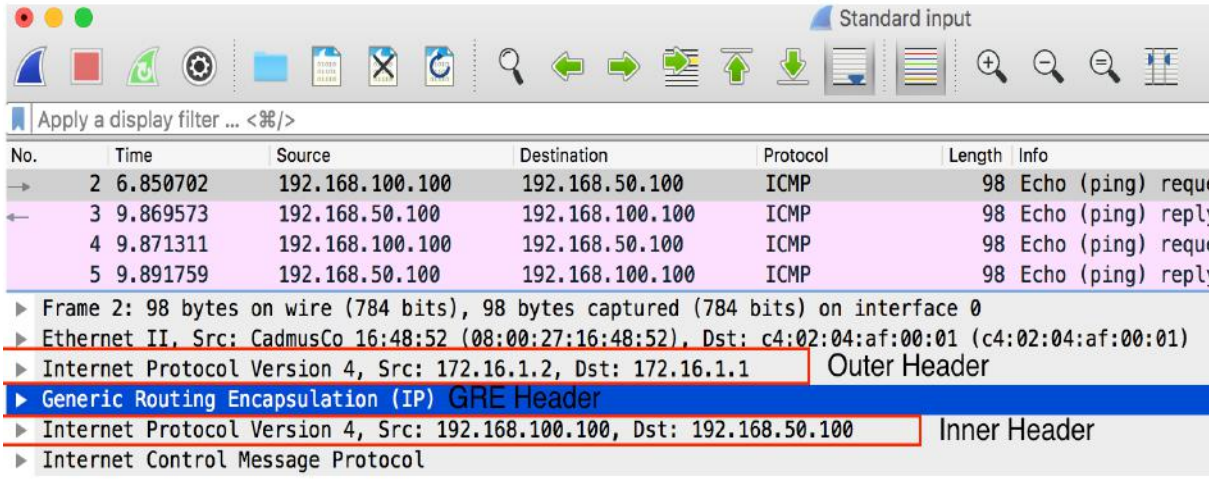


Ilustración 2-14 Cabeceras Inner Outer GRE Wireshark

En la *Ilustración 2-15* se verifica la cabecera del protocolo de encapsulación GRE referida en la *Ilustración 2-2* con cada uno de los campos correspondientes al protocolo. El tamaño del encabezado GRE es de 4 bytes.

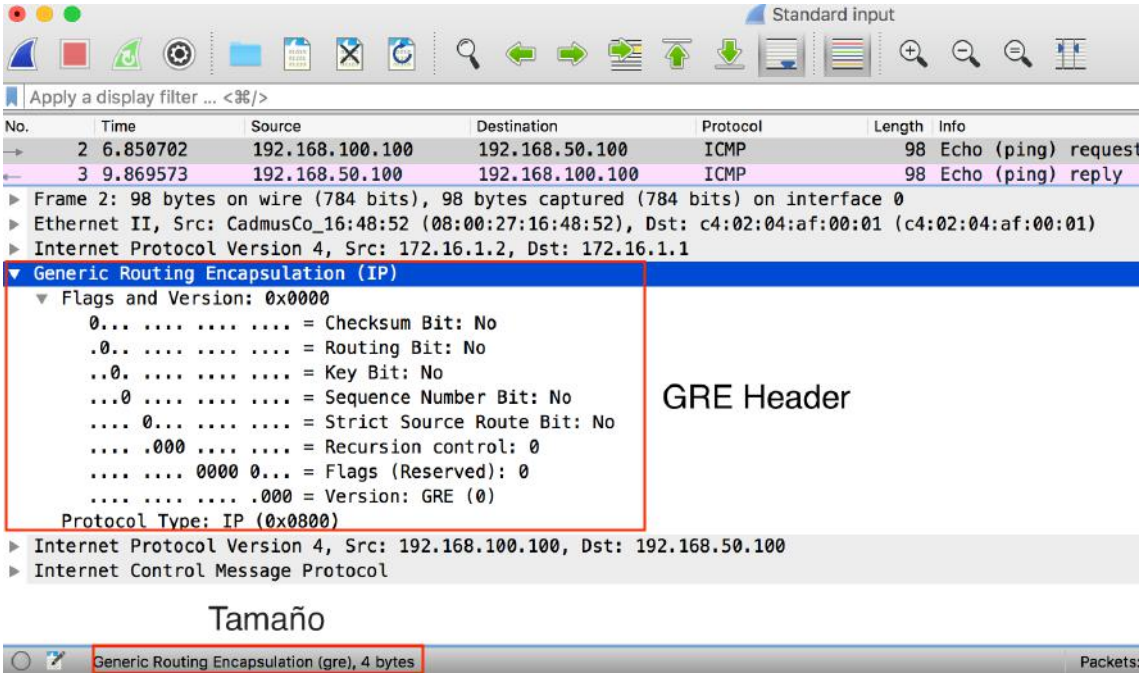


Ilustración 2-15 Cabecera GRE Wireshark

2.4 MTU Unidad Máxima de Transferencia

Otra parámetro muy importante que se debe tomar en cuenta al momento de realizar la tunelización es la Unidad Máxima de Transferencia o MTU. En nuestra simulación los datagramas deben pasar por varios enlaces, los cuales tienen cada uno su MTU definido, por lo cuál el MTU general para todo el path se define por el menor tamaño de unidad de transferencia máxima del path. Debido a ese parámetro para que un datagrama llegue sin fragmentarse al destino debe ser menor o igual que el menor MTU del path.

En el caso de TCP/UDP, el valor máximo de MTU viene definido por el MSS Maximum Segment Size, y toma su valor en función del tamaño máximo del datagrama. Para el caso del protocolo GRE que tiene una cabecera extra de 4 bytes, el tamaño del MTU viene definido por:

MTU = MSS + Cabeceras IP + Cabeceras TCP/UDP + Cabecera GRE

1500 = 1456 bytes + 20 bytes + 20 bytes + 4 bytes

El proceso de fragmentación incorpora carga innecesaria y hace mas pasada y lenta a la red, por lo cuál se tiene que considerar los MTU y MSS al momento de configurar el protocolo GRE para tunelización. En la Ilustración 2-16 se puede verificar el proceso de fragmentación al realizar un ping con una carga de 2000 bytes. Hay que tener en cuenta que cada paquete fragmentado deberá ser encapsulado lo que significa agregar cabeceras y por lo tanto carga innecesaria a la red.

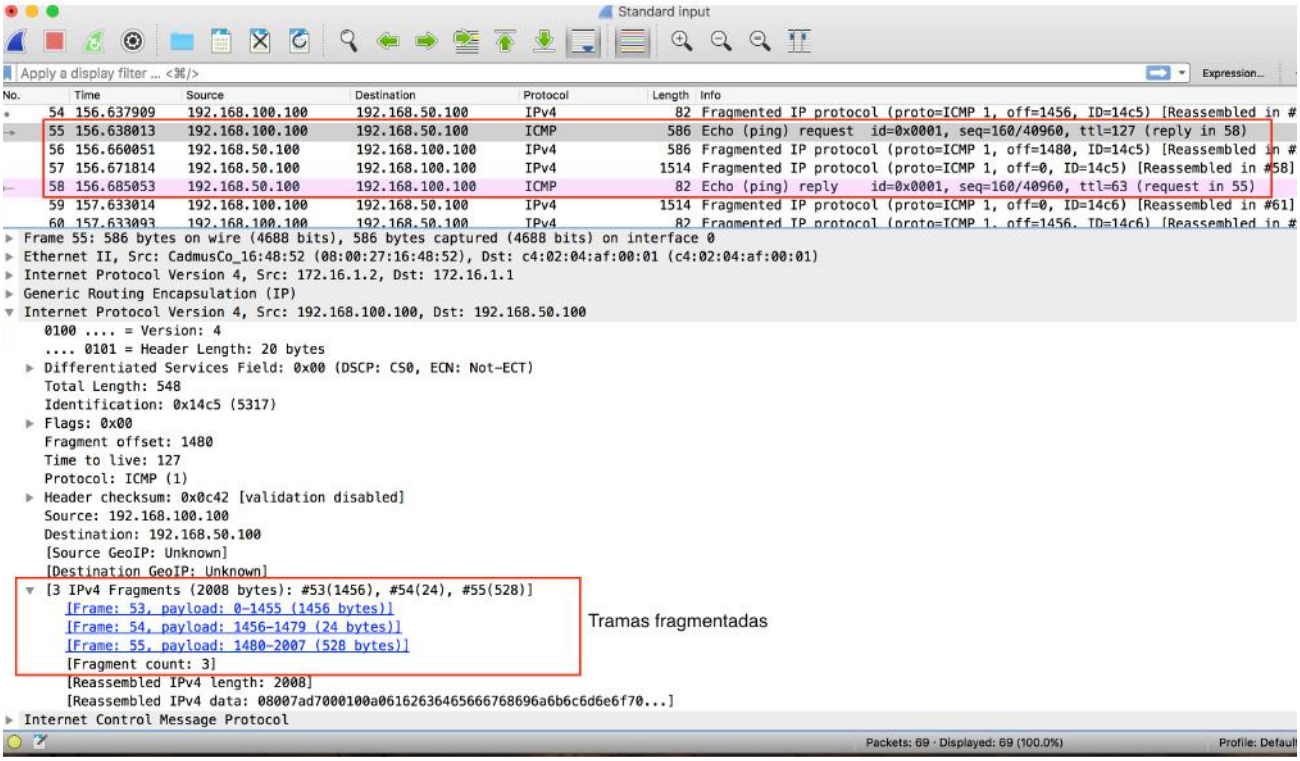


Ilustración 2-16 MTU Fragmentación

Para efectos de simulación se ajusta el el MTU a 1400 bytes y el MSS a 1356 bytes. Debido a que la mayoría de MTU en el path de transporte de los proveedores son de 1500 bytes y GRE agrega 4 bytes debido al proceso de encapsulación, se agrega un

margen de tolerancia que en un entorno práctico debería ser reajustado. Las configuraciones en el **R1** quedarían de la siguiente manera:

```
interface Tunnel1
 description CUE-GYE
 ip address 10.10.10.1 255.255.255.252
 ip mtu 1400
 ip tcp adjust-mss 1356
 tunnel source FastEthernet0/1
 tunnel destination 172.16.1.2
 tunnel path-mtu-discovery
```

El último comando path-mtu-discovery indicará a los hosts remotos el MTU que segmento del túnel de manera que no se envíen fragmentos superiores a este máximo y se evite la fragmentación de los paquetes. De igual manera se debe configurar el R2 y el router Mikrotik.

2.5 Tipos de Enrutamientos Dinámicos y Route-Map

En el apartado *2.2 Simulación y Comandos básicos* se realizó la implementación de los túneles GRE para funcionar como overlay de otros protocolos. En la simulación en GNS3 se configuró un enrutamiento estático para las agencias. En este apartado se revisarán los conceptos y configuraciones básicas para implementar protocolos de enrutamiento dinámico sobre la plataforma de tunelización.

La principales ventajas que tiene implementar protocolos de enrutamiento dinámico en una topología son:

- Comparten automáticamente la información acerca de las redes remotas.
- Determinan la mejor ruta para cada red y actualizan sus tablas de enrutamiento en base diferentes métricas.
- A diferencia de los protocolos de enrutamiento estático, los protocolos de enrutamiento dinámico requieren una menor carga administrativa y de control.

Desventajas de los protocolos de enrutamiento dinámico:

- Dedican parte de los recursos de los routers al funcionamiento del protocolo, lo cuál puede resultar contrapoducente en equipos sobrecargados o mal dimensionados.
- Requieren un poco más de conocimiento para su implementación

La *Ilustración 2-17* se muestra la clasificación de los enrutamientos dinámicos. Para el presente caso de estudio, se pretende implementar EIGRP [5] y OSPF. El primero basado en el vector distancia y el segundo en el estado de enlace.

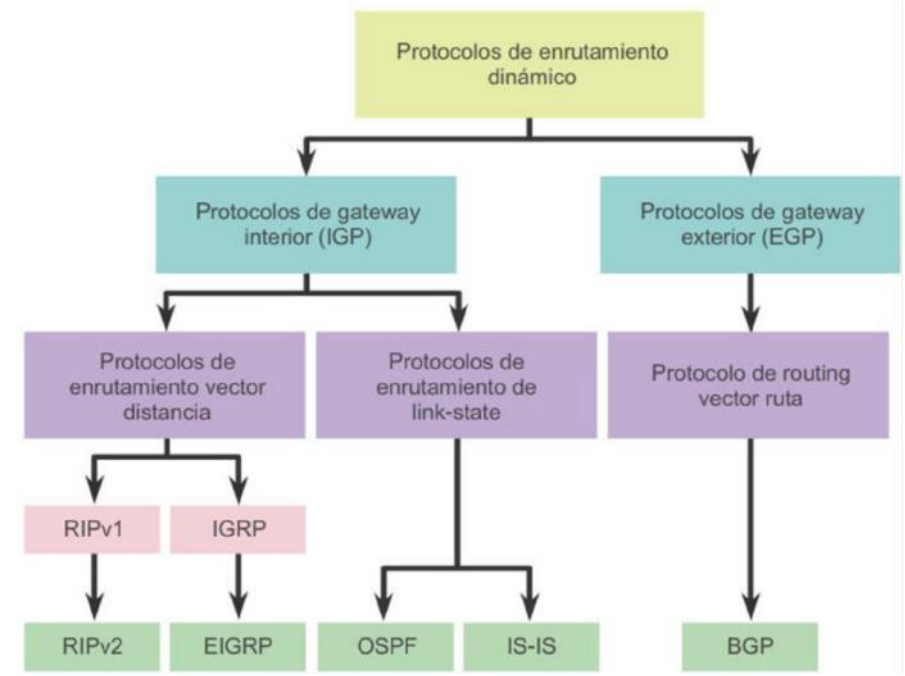


Ilustración 2-17 Protocolos de Enrutamiento Dinámico

2.5.1 Enrutamiento OSPF [4]

El protocolo OSPF (Open Shortest Path First) se encuentra definido en el RFC 2328 y OSPF V3 en el RFC 5340. Como observamos en la Ilustración 2-17, corresponde a un protocolo de gateway interior IGP y es usado para distribuir información de enrutamiento dentro de un mismo sistema autónomo. Este protocolo es utilizado en implementaciones de gran tamaño y que requieren escalabilidad, función que RIP en sus versiones no soporta (RIP tiene un limitante de 15 saltos). Adicional RIP converge de manera mas lenta que OSPF. Por estos motivos se a optado por OSPF con solución de protocolo de enrutamiento dinámico para el caso de estudio.

Algunas de las principales características de OSPF son[6]:

- **Sin clase:** fue concebido como un protocolo sin clase, de modo que admite VLSM y CIDR.
- **Eficaz:** los cambios de enrutamientos desencadenan actualizaciones de enrutamiento (no hay actualizaciones periódicas). Usa el algoritmo SPF para elegir la mejor ruta.
- **Convergencia rápida:** propaga rápidamente los cambios que se realizan a la red.
- **Escalable:** funciona bien en redes pequeñas y grandes. Se pueden agrupar los routers en áreas para admitir un sistema jerárquico.
- **Seguro:** admite la autenticación de síntesis del mensaje 5 (MD5). Cuando están habilitados, los routers OSPF solo aceptan actualizaciones de routing cifradas de peers con la misma contraseña compartida previamente.

[6] CCNA 2 Exploration v 4.0 Conceptos y protocolos de enrutamiento

Al ser OSPF un protocolo de estado de enlace, éste ofrece una descripción del estado de sus interfaces y de su relación con los routers vecinos. Dicha descripción de la interfaz incluye, la dirección IP de la interfaz, la máscara de red, el tipo de red a la que se conecta, los routers conectados a la red, entre otros parámetro que le ayudan a construir la topología de la red.

La métrica de una interfaz OSPF es el costo que se calcula en base al ancho de banda de la interfaz y es configurable por parte del usuario. El costo es inversamente proporcional al ancho de banda de dicha interfaz. Un mayor ancho de banda indica un menor costo.

COSTO = 10000 0000/banda de ancha en bps

Para efectos de la simulación de la topología del caso de estudio de deberá establecer un costo en base a los datos proporcionados el Capítulo 1.

2.5.2 Simulación OSPF

Para la configuración del protocolo OSPF, se modificarán los enrutamientos estáticos configurados previamente para las pruebas de Túneles GRE.

R2

```
R2#conf term
R2(config)#router ospf 1
R2(config-router)#network 192.168.50.0 0.0.0.255 area 0
R2(config-router)#network 10.10.10.0 0.0.0.3 area 0
R2(config-router)#network 10.10.10.4 0.0.0.3 area 0
R2(config-router)#
*Mar  1 00:08:46.351: %OSPF-5-ADJCHG: Process 1, Nbr
192.168.150.1 on Tunnel2 from LOADING to FULL, Loading Done
*Mar  1 00:25:52.679: %OSPF-5-ADJCHG: Process 1, Nbr
172.16.1.2 on Tunnel1 from LOADING to FULL, Loading Done
```

En la *Ilustración 2-18* se verifica la redistribución de rutas por medio del protocolo OSPF a través de los Túneles 1 y 2 . El router R2 recibe las redes privadas de las agencias UIO 192.168.150.0/24 y GYE 192.168.100.0/24.

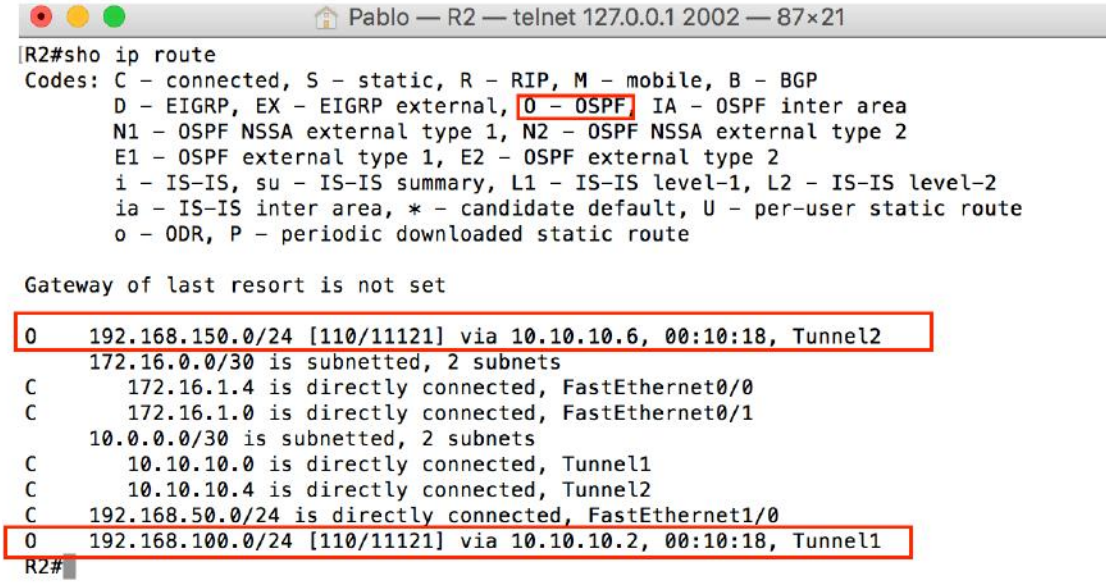


Ilustración 2-18 Tabla de Enrutamiento Router Cisco R2

Router MIKROTIK

[admin@MikroTik] > routing ospf area set [find default=yes] area-id=0.0.0.0 disabled=no instance=default name=0
[admin@MikroTik] > routing ospf network add area=0 disabled=no network=192.168.100.0/24
[admin@MikroTik] > routing ospf network add area=0 disabled=no network=10.10.10.0/30

En la *Ilustración 2-19* se verifica la redistribución de rutas por medio del protocolo OSPF a través del Túnel 1. El router Mikrotik recibe las redes privadas de las agencias CUE 192.168.50.0/24 y UIO 192.168.150.0/24.

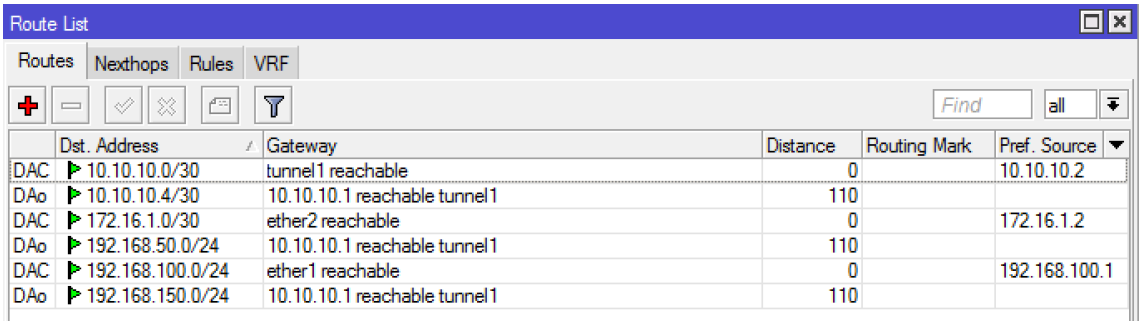


Ilustración 2-19 Tabla de enrutamiento Mikrotik / DAo - Dinamic Active Ospf

R1

```
R1#conf term
R1(config)#router ospf 1
R1(config-router)#network 192.168.150.0 0.0.0.255 area 0
R1(config-router)#network 10.10.10.4 0.0.0.3 area 0
R1(config-router)#
*Mar  1 00:09:34.227: %OSPF-5-ADJCHG: Process 1, Nbr
192.168.50.1 on Tunnel2 from LOADING to FULL, Loading Done
```

En la *Ilustración 2-20* se verifica la redistribución de rutas por medio del protocolo OSPF a través del Túnel 2. El router R1 recibe las redes privadas de las agencias CUE 192.168.50.0/24 y GYE 192.168.100.0/24.

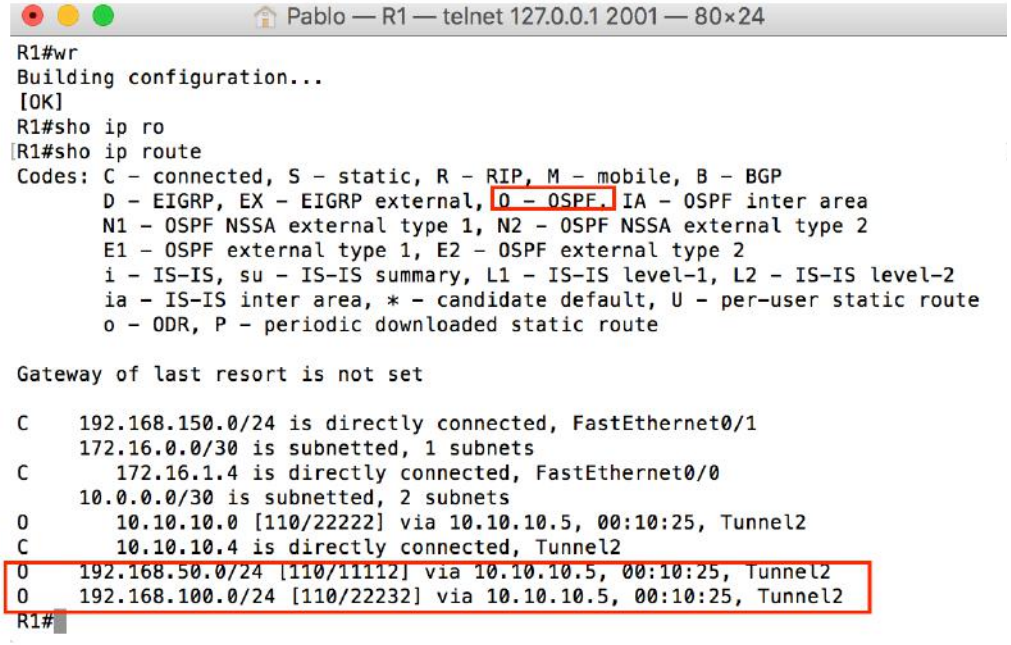


Ilustración 2-20 Tabla de Enrutamiento Cisco R1

Algunos comandos útiles para dar seguimiento a problemas o revisar configuraciones de OSPF son:

- show ip ospf neighbor
- show ip ospf neighbor detail
- show ip ospf interface
- show ip ospf database

2.5.2.1 Pruebas de Conectividad

Las pruebas de conectividad se muestran en la *Ilustración 2-21*, donde se verifica conectividad entre todas las agencias mediante el comando ping realizado desde las máquinas virtualizadas en el software GNS3.

Se verifica que existe conectividad entre todas las agencias y mediante un tracert desde la agencia GYE hacia la agencia UIO se constata el path de los paquetes, a través de los túneles.

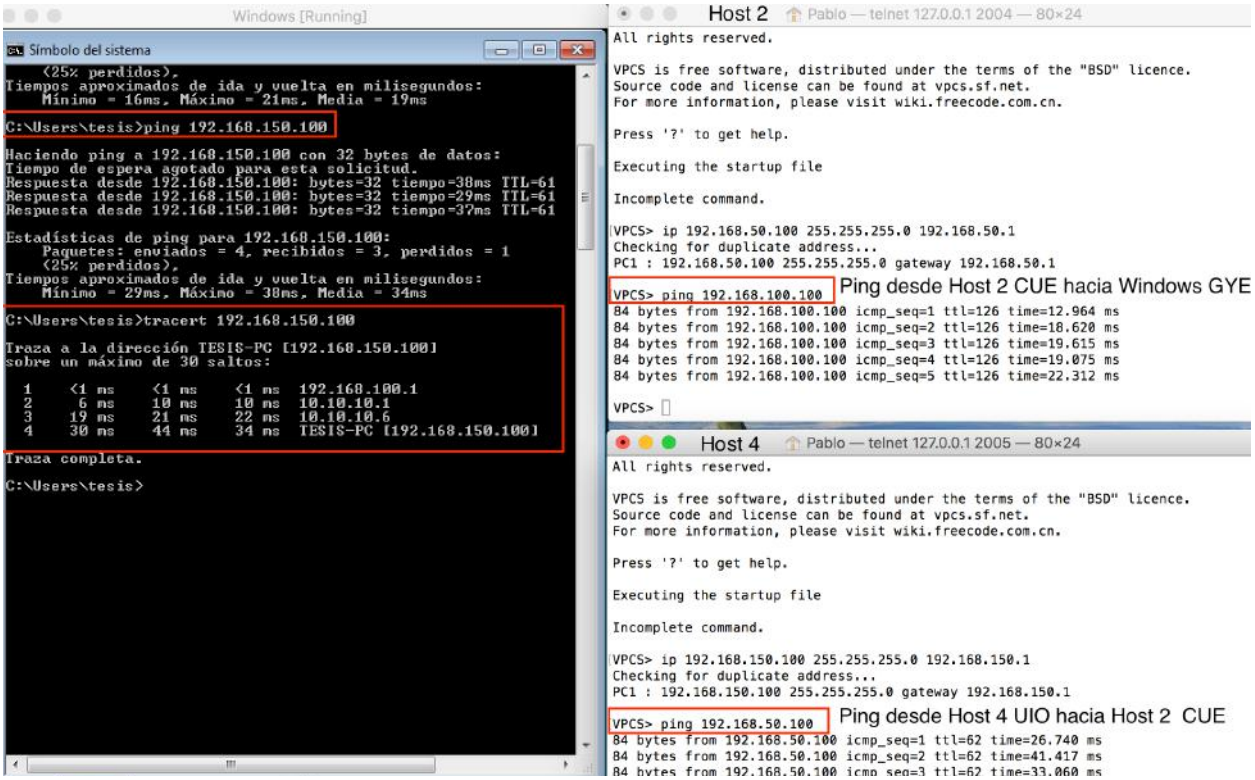


Ilustración 2-21 Pruebas de conectividad entre Agencias

2.5.3 Redundancia de Enlaces

Para mejorar el servicio de disponibilidad de la red, se plantea implementar enlaces redundantes entre las agencias de Quito – Guayaquil. Esto implica la contratación de un nuevo enlace de datos que brindará redundancia a la topología. La Ilustración 2-22 muestra la topología con el enlaces UIO-GYE redundante. En el próximo capítulo de analizará el proveedor y ancho de banda requerido para este nuevo enlace.

Para brindar la redundancia se requiere la implementación del protocolo de tunelización GRE en el nuevo enlace, así con el protocolo de enrutamiento dinámico OSPF de estado de enlace que actualizaría automáticamente cualquier cambio en la topología. La *Tabla 2-2* muestra las configuraciones adicionales a las ya realizadas.

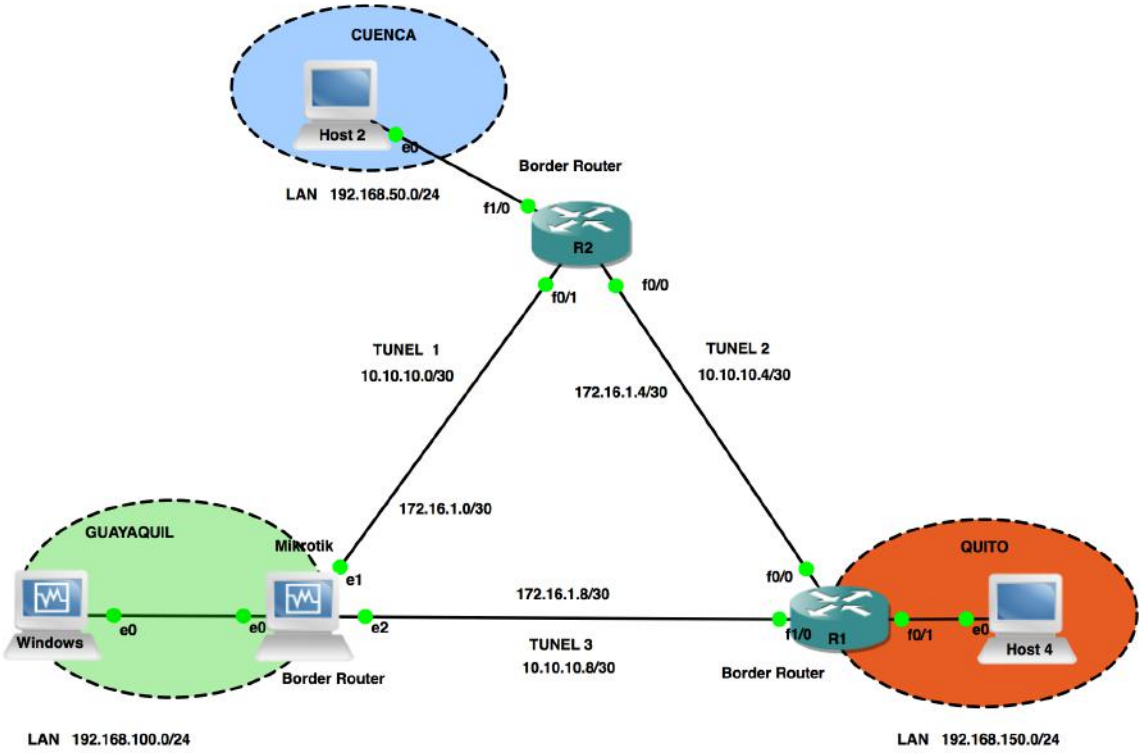


Ilustración 2-22 Enlace Redundante UIO-GYE

R1	MIKROTIK
TUNELl 3 UIO-GYE interface Tunnel3 description UIO-GYE ip address 10.10.10.10 255.255.255.252 ip mtu 1400 ip tcp adjust-mss 1356 keepalive 10 3 tunnel source FastEthernet1/0 tunnel destination 172.16.1.9 tunnel path-mtu-discovery	**TUNELl 3 GYE – UIO** interface gre add comment="TUNEL GYE-UIO" keepalive=10 local-address=172.16.1.9 mtu=1400 name=tunnel3 remote- address=172.16.1.10
OSPF router ospf 1 network 10.10.10.8 0.0.0.3 area 0	**OSPF** routing ospf network add area=0 network=10.10.10.8/30

Tabla 2-2 Configuraciones adicionales para enlace Redundante

2.5.3.1 Simulación Redundancia

Para simular la redundancia de la topología mediante el simulador GNS3 se dará de baja una de las interfaces tunelizadas de manera que el protocolo de enrutamiento dinámico OSPF realice la actualización de rutas en los equipos involucrados. Durante el cambio de estado de enlace de una de las interfaces de los túneles se mantendrá activo un ping para verificar el tiempo de respuesta del protocolo de enrutamiento.

La interfaz del Túnel 2 se dará de baja mientras se mantiene un ping entre la agencia UIO hacia la agencia CUE. Se analizan los estados de las tablas de enrutamiento e interfaces antes y después de dar de baja el enlace.

Estado de la tablas de enrutamiento e interfaces antes de dar de baja el enlace:

R1

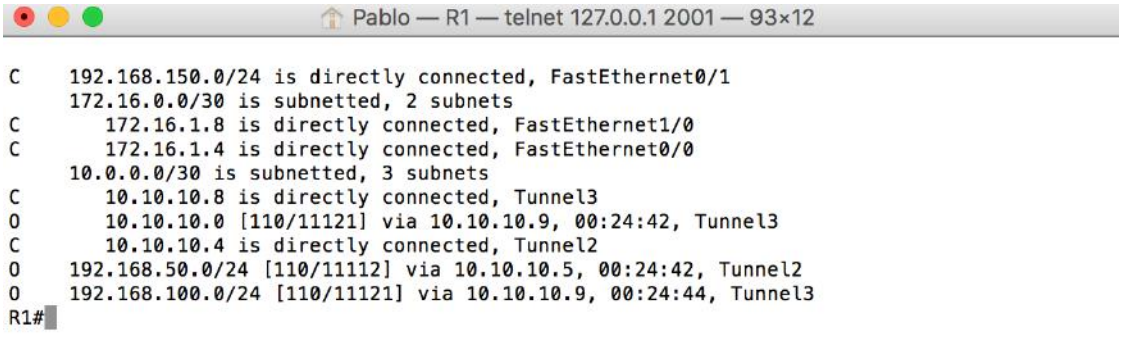


Ilustración 2-23 Tabla de Enrutamiento R1

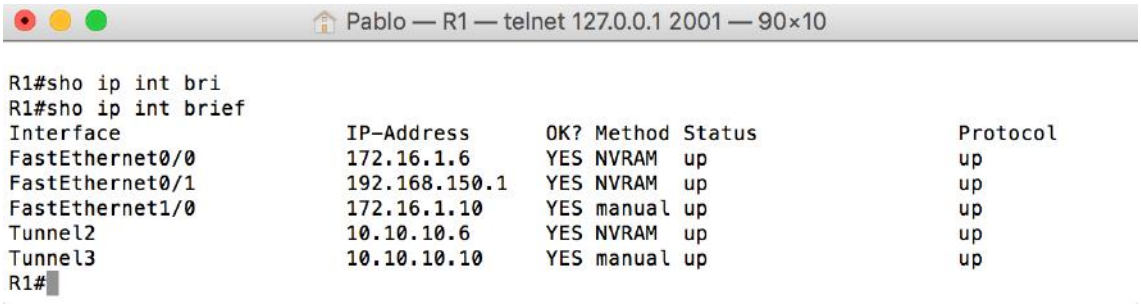


Ilustración 2-24 Estado de las Interfaces R1

R2

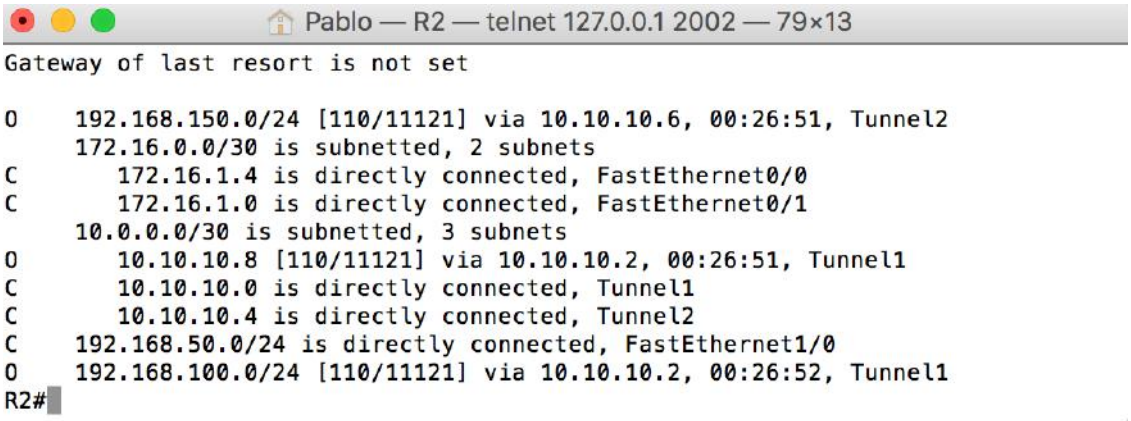


Ilustración 2-25 Tabla de enrutamiento R2

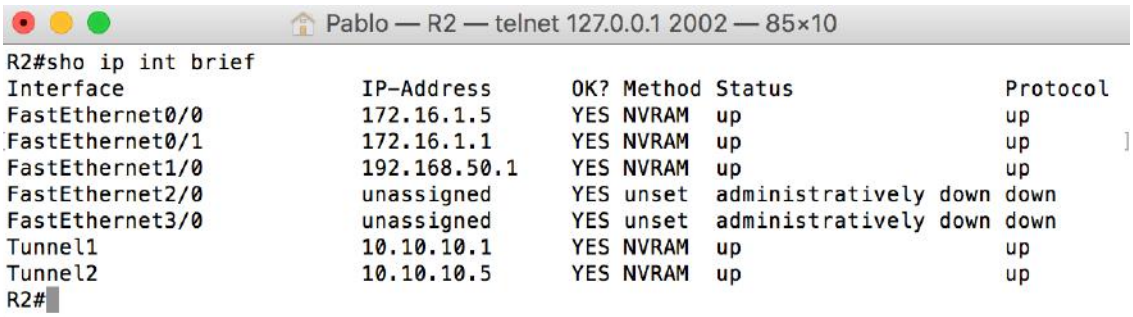


Ilustración 2-26 Estado de las Interfaces R2

MIKROTIK

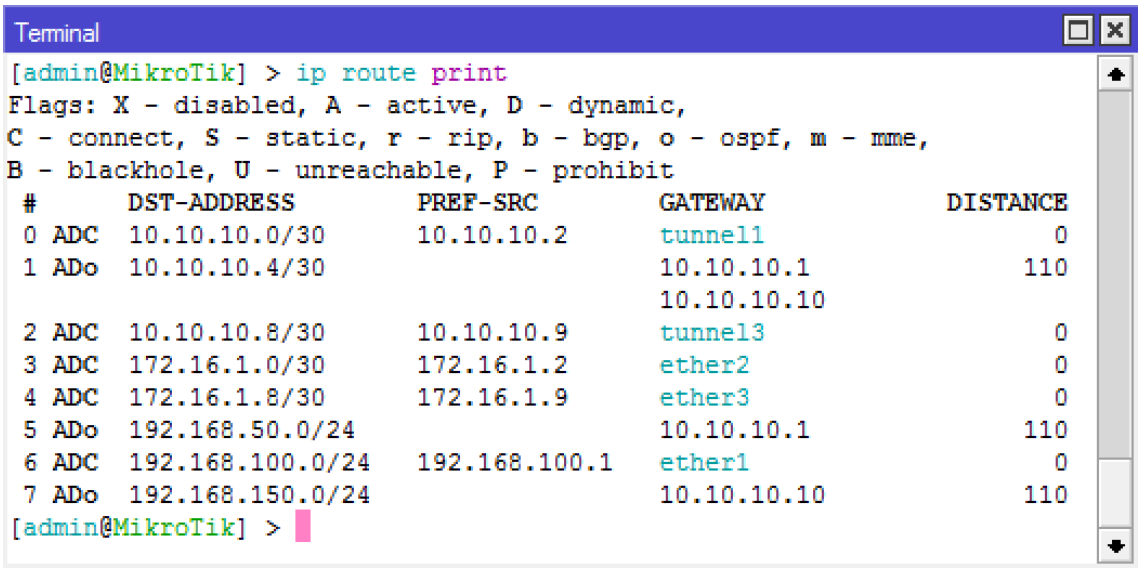


Ilustración 2-27 Tabla de enrutamiento Mikrotik

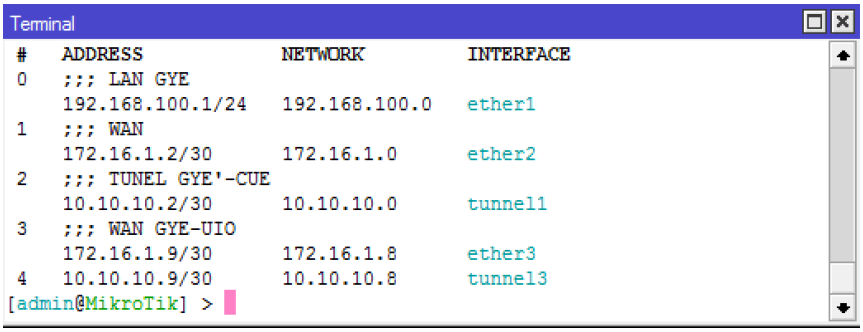


Ilustración 2-28 Estado de las interfaces Mikrotik

Se da baja la interfaz Túnel 2 entre las agencias UIO – CUE y se monitorea la recuperación de la conexión por medio del ping entre UIO – CUE *Ilustración 2-29*.

R1

```
R1#conf term
R1(config)#interface tunnel 2
R1(config-if)#shutdown
*Mar  1 00:57:53.567: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.50.1 on
Tunnel2 from FULL to DOWN, Neighbor Down: Interface down or detached
R1(config-if)#end
*Mar  1 00:57:55.563: %LINK-5-CHANGED: Interface Tunnel2, changed
state to administratively down
*Mar  1 00:57:56.563: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Tunnel2, changed state to down
R1(config-if)#end
```

Se verifica el estado de la interfaz Tunnel 2 como administrativamente abajo y las actualizaciones de la tabla de enrutamiento para alcanzar la red de la agencia CUE 192.168.50.0/24.

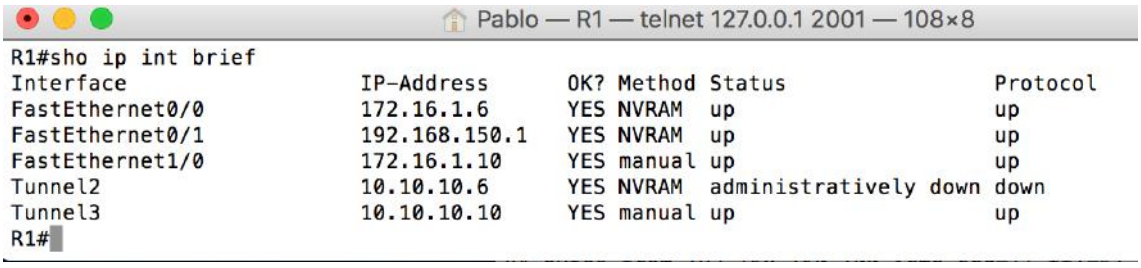


Ilustración 2-29 Interfaz Tunnel2 down

```
Pablo — R1 — telnet 127.0.0.1 2001 — 72×13

Gateway of last resort is not set

C    192.168.150.0/24 is directly connected, FastEthernet0/1
     172.16.0.0/30 is subnetted, 2 subnets
C       172.16.1.8 is directly connected, FastEthernet1/0
C       172.16.1.4 is directly connected, FastEthernet0/0
     10.0.0.0/30 is subnetted, 2 subnets
C       10.10.10.8 is directly connected, Tunnel3
O       10.10.10.0 [110/11121] via 10.10.10.9, 00:06:29, Tunnel3
O    192.168.50.0/24 [110/11122] via 10.10.10.9, 00:06:29, Tunnel3
O    192.168.100.0/24 [110/11121] via 10.10.10.9, 00:06:29, Tunnel3
R1#
```

Ilustración 2-30 Tabla de enrutamiento R1 con la interfaz Tunnel 2 deshabilitada

Se verifica que las rutas en el router R1 se han actualizado (*Ilustración 2-23*). Para alcanzar la red CUE 192.168.50.0/24 en esta nueva topología se re enruta el tráfico por la interfaz Tunnel 3. El efecto de los cambios se explica en la *Ilustración 2-31*.

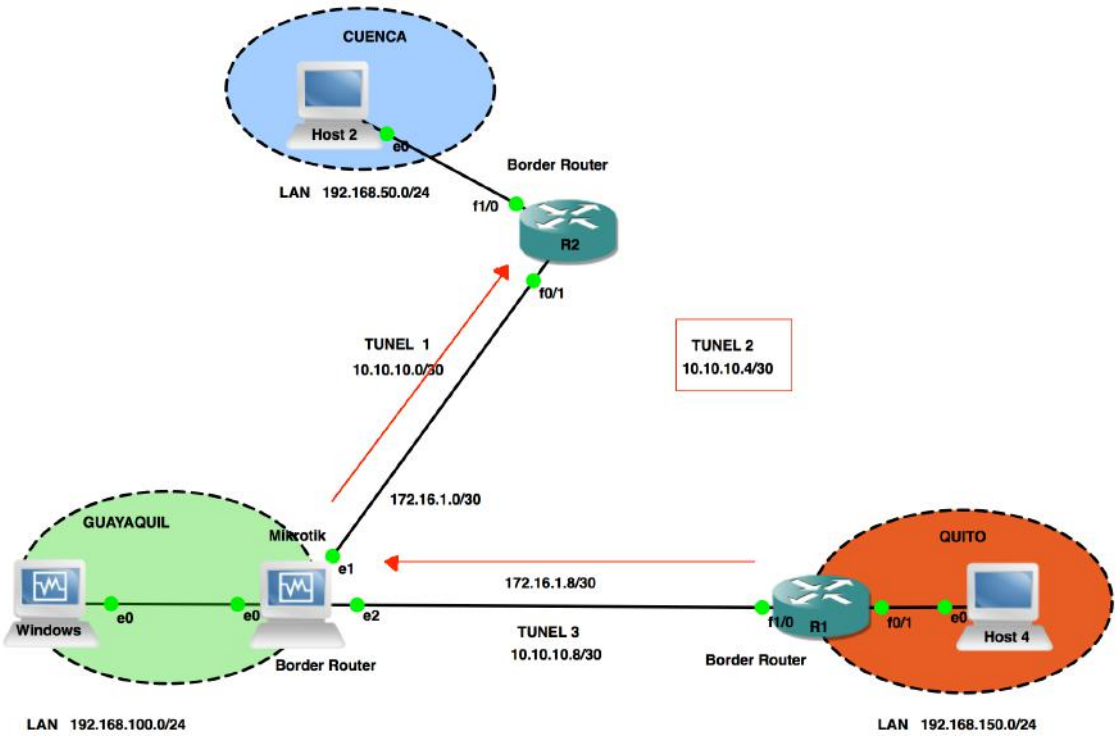


Ilustración 2-31 Redirección de tráfico

Se verifica en la *Ilustración 2-32* que en promedio se tiene una pérdida de 4 paquetes hasta que el protocolo de enrutamiento OSPF actualice cambios en la topología. Este tiempo de inactividad es aceptable para el tipo de transaccionalidad del caso de estudio.

Ilustración 2-32 Tiempo de Recuperación

2.5.4 Función Route-Map Cisco [6]

En el caso de estudio se presenta una topología con dos accesos a internet. Los proveedores de internet son TV Cable y Telconet, de acuerdo a lo especificado a la *Tabla 2-3*.

	Servicio de Internet
Telconet	10M 1:1
Tv Cable	15M 1:1

Tabla 2-3 Distribución Internet

Las políticas de acceso a internet al momento se manejan mediante un equipo Mikrotik Cloud Core 1016-12G, mediante el cuál se realiza un balanceo de carga.

Por temas administrativos y de pagos del gasto mensual por concepto de internet, se requiere que solo ciertas agencias tengan accesos a la salida de internet por el proveedor Telconet. Únicamente las agencias que paguen por el rubro de internet de Telconet serán quienes tengan acceso a este servicio.

Para solventar este requerimiento se plantea una configuración con una sola ruta por defecto hacia el proveedor de internet Tv Cable, por el cuál deben acceder la mayor parte de agencias al servicio de internet, y mediante la función Route-Map de Cisco mapeamos las rutas del resto de agencias hacia el enlace de Telconet.

La función Route-Map

2.5.5 Simulación Route-Map

Para la simulación del uso y configuración de la función Route-Map[9], se plantea el entorno GNS3 de la *Ilustración 2-33.*

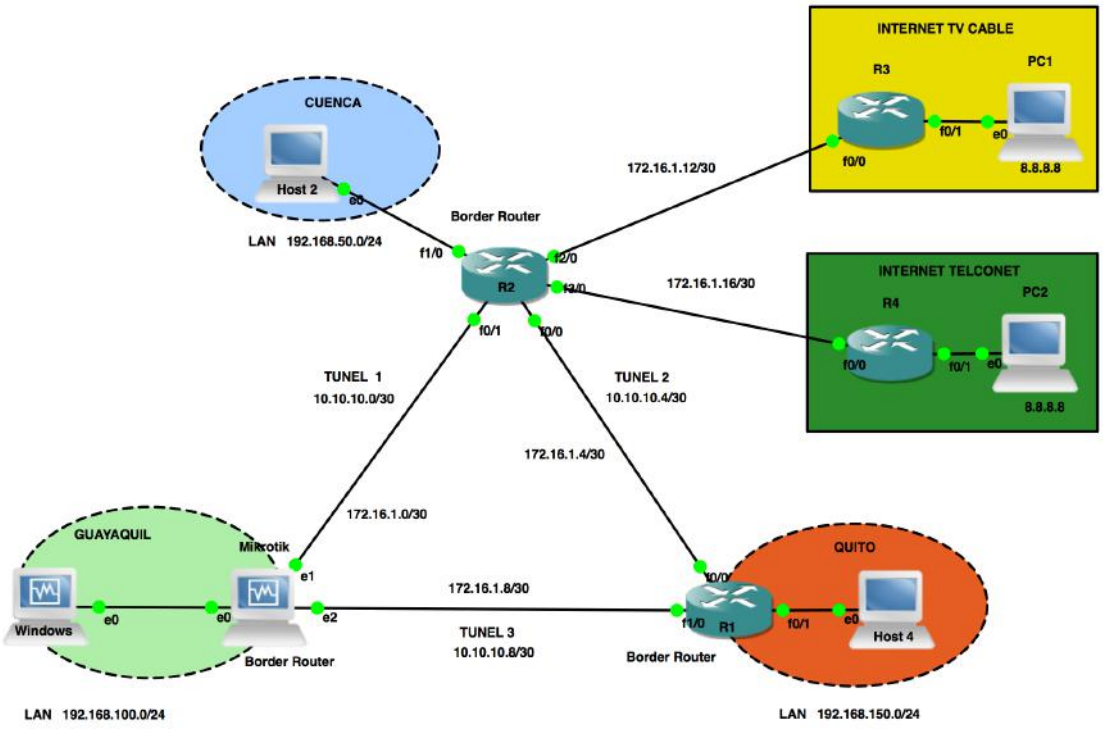


Ilustración 2-33 Topología de Simulación de Acceso a Internet GNS3

En la topología se agregan dos equipos R3 y R4 que corresponderían a los gateways de internet de los proveedores, por lo tanto no tenemos injerencia alguna sobre estos equipos. Las configuraciones se centran en el router R2, el cual requiere las siguientes configuraciones:

1. Configurar la conexión con los gateways

```
interface FastEthernet2/0
description INTERNET TVCABLE
ip address 172.16.1.13 255.255.255.252
interface FastEthernet3/0
description INTERNET TELCONET
ip address 172.16.1.17 255.255.255.252
```

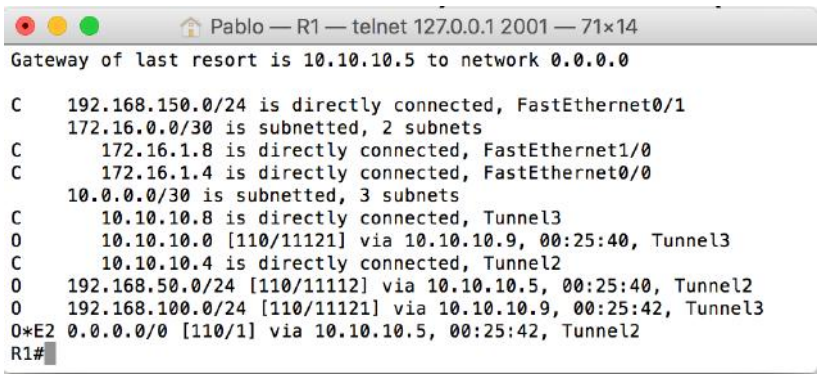
2. Configurar ruta por defecto hacia el gateway de internet de TV CABLE

```
ip route 0.0.0.0 0.0.0.0 172.16.1.14
```

3. Redistribuir la ruta por defecto por medio de OSPF

```
router ospf 1
default-information originate always
```

En la Ilustración 2-34 se verifica que la ruta por defecto se anuncia mediante OSPF en los routers remotos R1 y Mikrotik.



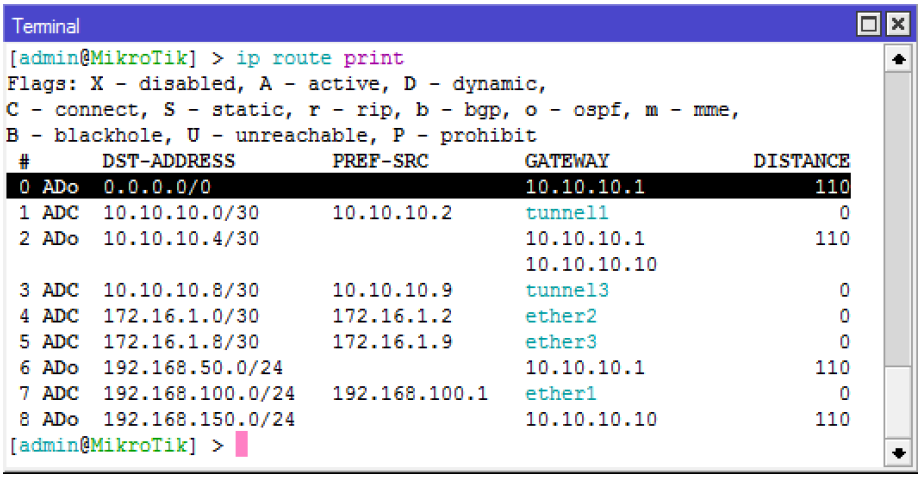


Ilustración 2-34 Redistribución de ruta por defecto OSPF R1 y Mikrotik

4. Configurar una lista de control de acceso que contenga las ip de las agencias que requieren salir por el enlace de Telconet. Para la simulación se toma a la red UIO 192.168.150.0/24 que deberá usa el enlace a internet de Telconet.

   access-list 10 permit 192.168.150.0 0.0.0.255

5. Configurar la política de route map "internet" basado en el ACL creada previamente y el match para la redirección, en este caso de la red de UIO por el l gateway de internet de Telconet 172.16.1.18.

   route-map internet permit 10
   match ip address 10
   set ip next-hop 172.16.1.18

6. Asignar la política a la interfaz del Tunel.

El túnel correspondiente es el túnel 2, sin embargo hay que tener en cuenta que si se cae el enlace entre UIO y CUE la conexión de la agencia UIO se reestablece por medio del túnel 1 entre GYE-UIO, por lo cuál la política se debe aplicara en ambas interfaces de los túneles 1 y 2 en el router R2.

```
interface Tunnel1
description CUE-GYE
ip policy route-map internet
interface Tunnel2
```

```
description CUE-UIO
ip policy route-map internet
```

Para el análisis del mapeo de rutas, habilitamos el debug de las políticas:

```
R2#debug ip policy
Policy routing debugging is on
```

Verificamos en la *Ilustración 2-35* que al realizar un ping a internet desde la agencia de UIO 192.168.150.0/24 se tienen coincidencias y se refleja en el debug las coincidencias de la política internet. Se comprueba el correcto funcionamiento del mapeo de rutas para direccionar el internet de la agencia de UIO por el enlace de Internet de Telconet.

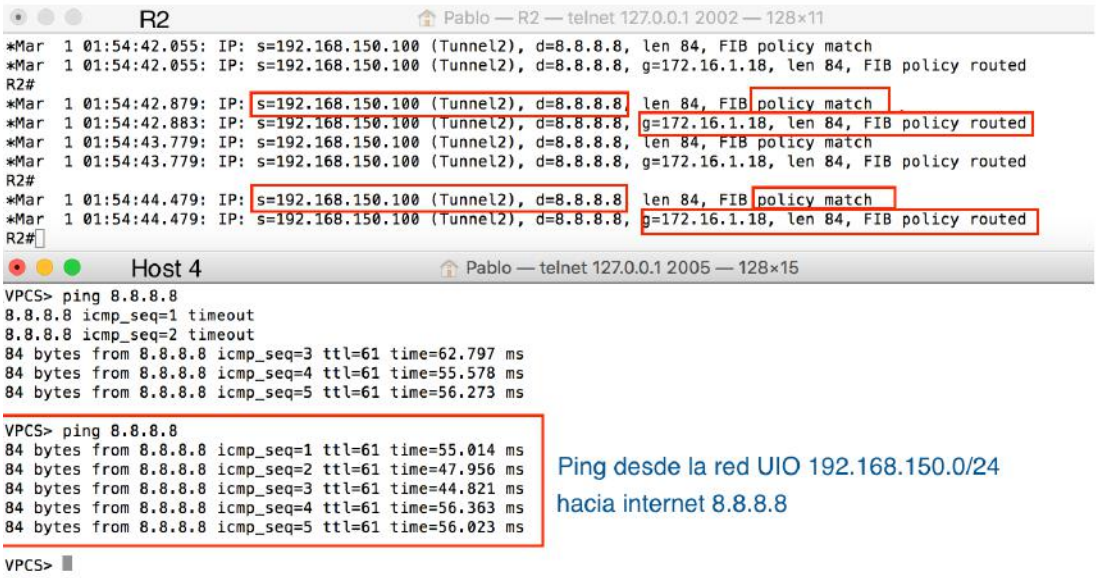


Ilustración 2-35 Resultado del Debug policy Match

Para el caso de otras agencias con direcciones origen diferentes a las del ACL, se verifica en la *Ilustración 2-36* que se en rutan mediante la tabla de ruteo del router R2, con ruta por defecto al Gateway de internet del proveedor Tv Cable.

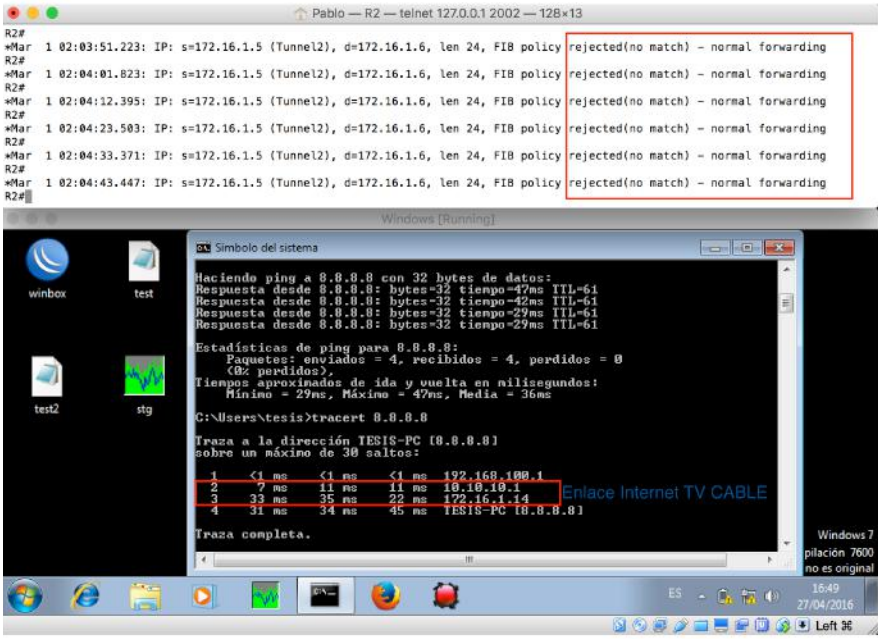


Ilustración 2-36 Resultado debug policy rejected normal forwarding

Capítulo 3 : DISEÑO Y SIMULACIÓN

3.1 Descripción del Diseño [8]

El diseño propuesto se basa en el modelo jerárquico de Cisco. El modelo implementa alta disponibilidad, balanceo de carga e implementación de seguridades en la capa física. El diseño propuesto se detalla en dos partes, para el cuarto de datos y para la red a nivel nacional.

Para el cuarto de datos en la ciudad de Cuenca se toman en cuenta las capas Core, Distribución y Acceso, mientras que para las agencias Quito y Guayaquil, se toman en cuenta las capas de Distribución y Acceso, con las variantes de ciertos servicios como el servicio de tunelización que se implementará en el capa de distribución.

Core: El equipo evaluado para este nivel es el Cisco Catalyst WS-C3560G-24TS-E con una licencia IP Services. Se selecciona este modelo debido al gran performance, capacidad de procesamiento (paquetes por segundo) y confiabilidad que brinda. En este nivel el equipo tendrá las siguientes funciones:

- Enrutamiento Estático
- Enrutamiento dinámico OSPF
- ACL (Listas de Control de Acceso)
- Link Aggregation
- Manejo de enlaces de datos
- Route Mapping
- Tunneling
- Port Trunking
- STP (Spanning Tree)

Distribución: Para este nivel se determina que el equipo Cisco Catalyst WS-C3650-24TS-E. Las características para seleccionar este dispositivo para la capa de

distribución son el alto performance que brinda el equipo y la capacidad de administrar en un futuro implementaciones de redes inalámbricas WLAN (Wireless Controller). El licenciamiento será IP Services. No se requiere soporte POE ni stack.

- Enrutamiento Estático
- Enrutamiento dinámico OSPF
- Manejo de VLANs (VTP Server)
- Link Agreggation
- Port Trunking
- DHCP Server
- ACL (Listas de Control de Acceso)
- STP (Spanning Tree)

Acceso: Se plantea para este nivel el equipo Catalyst 2960X-24PD-L, debido a sus características de crecimiento, ya que soporta hasta 8 dispositivos en stack, con un licenciamiento de fábrica LAN Base que resulta suficiente para las funciones que cumplirán estos equipos en la capa de acceso. Otra de las características importantes de este equipo es el soporte de POE, para servicios de alimentación de teléfonos y cámaras IP.

- Manejo de VLANs (VTP Client)
- ACL (Listas de Control de Acceso)
- Port Security
- Port Trunking
- QoS
- STP (Spanning Tree)

Marca	Modelo	Descripción
Cisco	WS-C3560G-24TS-E	Core Data Center
Cisco	WS-C3650-24TS-E	Distribución
Cisco	Catalyst 2960X-24PD-L	Acceso

Tabla 3-1 Descripción de Equipos

3.1.1 Diseño del Diagrama físico y lógico

Para dar una solución a los requerimientos de disponibilidad, escalabilidad, confiabilidad, optimización de recursos para el caso de estudio, se plantea re diseñar la red a nivel nacional. Esta diseño incluye la readecuación de la red de core, distribución y acceso del cuarto de datos. En la *Ilustración 3-2*, se muestra el diagrama físico correspondiente al diseño para el cuarto de datos. El diseño se basa en el modelo jerárquico de cisco [8]. La *Ilustración 3-3* detalla el diagrama lógico de los equipos que componen el diseño de la red para el cuarto de datos. La *Ilustración 3-4* muestra de manera general la topología física de la red a nivel nacional, mientras que la *Ilustración 3-5* detalla la topología lógica.

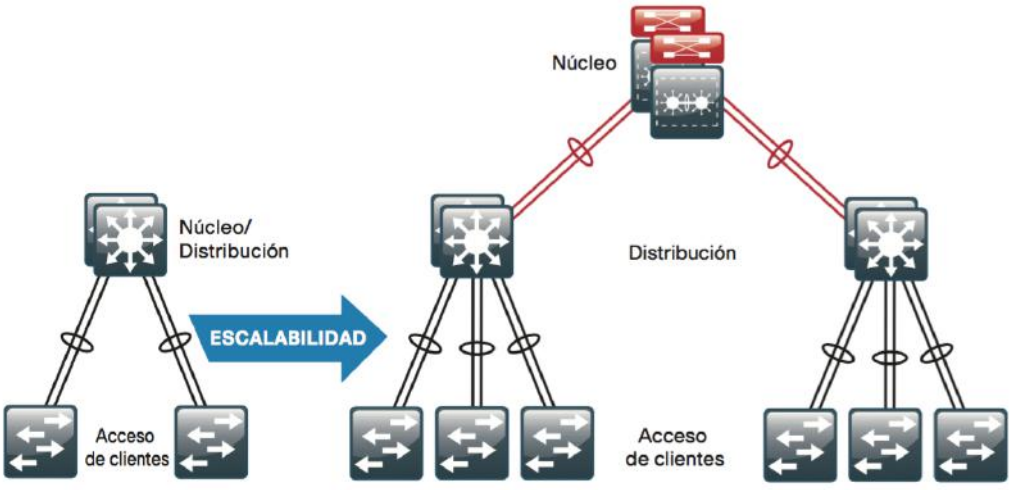


Ilustración 3-1 Diseño Jerárquico Cisco [7]

[7] Imagen tomada de http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-campus/index.html#~validate - último acceso 10 de junio 2016

Por otra parte la *Ilustración 3-3* describe el diagrama físico de la red a nivel nacional con las agencias en Quito, Guayaquil y Cuenca. De acuerdo a lo revisado en el capítulo anterior, se incorporan algunos servicios de red (tunneling, routing, etc) que funcionan como una red superpuesta que soportará los servicios brindados y permitirán implementar QoS en la topología del diseño.

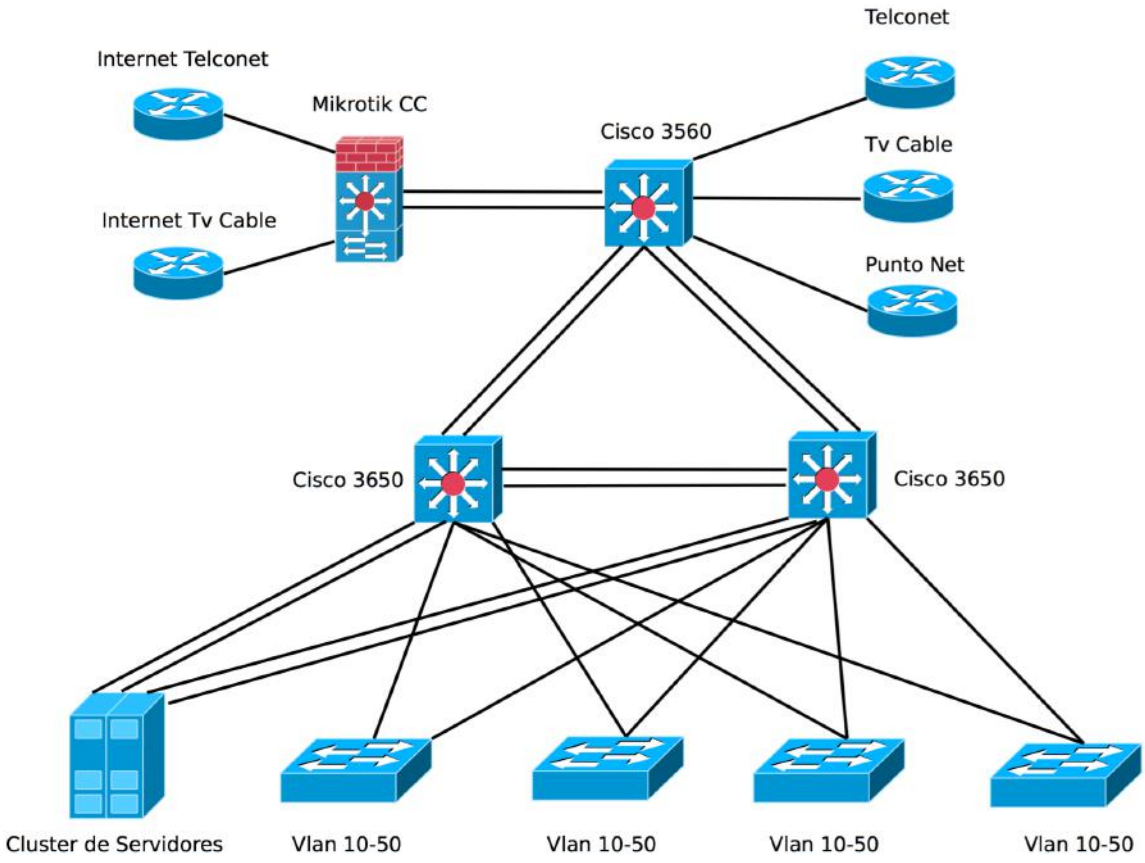


Ilustración 3-2 Diagrama Físico Cuarto de Datos

La *Ilustración 3-3* muestra el diagrama lógico de los equipos del cuarto de datos. El diagrama incluye interfaces y direccionamiento de las redes virtuales internas. No se toman en cuenta los equipos de proveedores ni el equipo Mikrotik administrador del internet. Estos equipos se incluirán mas adelante en el análisis a nivel nacional del diseño. Para efectos de simulación se incluyen dos máquinas para monitorizar el comportamiento de las configuraciones de capa 2. Se incluyen los equipos correspondientes indicados en la *Tabla 3-1* para cada nivel del modelo jerárquico.

La configuración del diseño de red planteado, requiere la implementación de ciertos protocolos de red que permiten brindar redundancia en los enlaces y equipos del data center. Estos protocolos se mencionarán en la simulación de la topología en el punto 3.3

Adicional a la redundancia, otro parámetro a tomar en cuenta, es la capacidad de cada enlace. El centro de datos concentra los servidores de bases de datos, correo, backups, etc. Estos servicios generan gran cantidad de tráfico y se ven afectados por enlaces saturados o de baja velocidad.

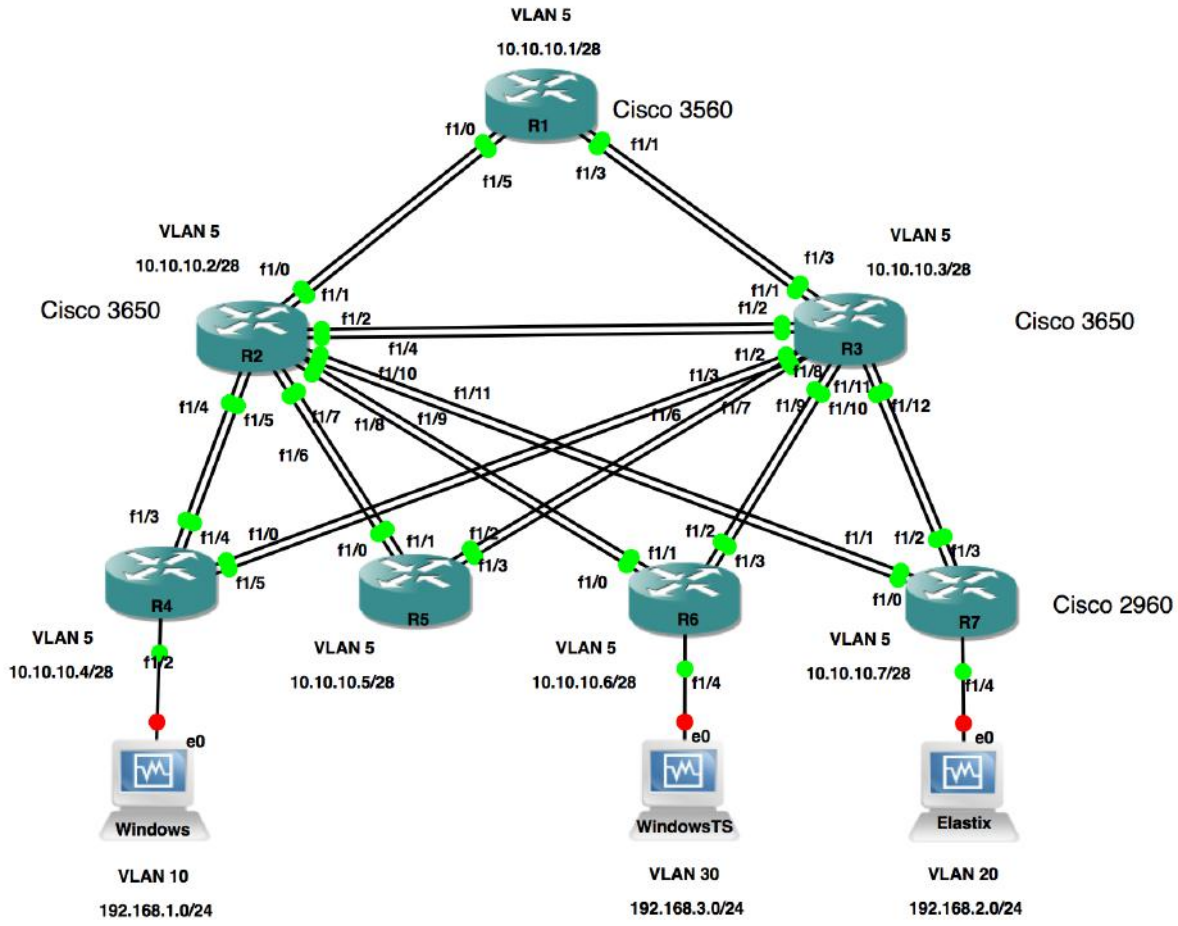


Ilustración 3-3 Diagrama Lógico Cuarto de Datos

Para solucionar el requerimiento de alta disponibilidad, el diseño plantea configurar dos equipos por cada nivel en el core y distribución. Uno actuará como equipo principal y el segundo como backup. Adicional el diseño contempla un balanceo de carga, de manera que todos los equipos se encuentren activos todo el tiempo, optimizando los recursos existentes. Para esto, el diseño plantea la configuración del protocolo RSTP (Rapid Spannig Tree Protocol). Como una primera etapa para el caso de estudio, se plantea implementar redundancia en el nivel de distribución, por lo cuál la simulación y los esquemas de las *Ilustraciones 3-2, y 3-3* hacen referencia únicamente a una redundancia en el nivel de distribución.

Para dar una solución al requerimiento de alto tráfico, a más de seleccionar equipos con altas prestaciones (procesamiento de paquetes), se plantea de igual manera como una primera etapa optimizar los recursos y configurar enlaces agregados (Link Aggregation) para aumentar las capacidades de los enlaces entre swiches del data center y los enlaces de las máquinas del cluster de servidores.

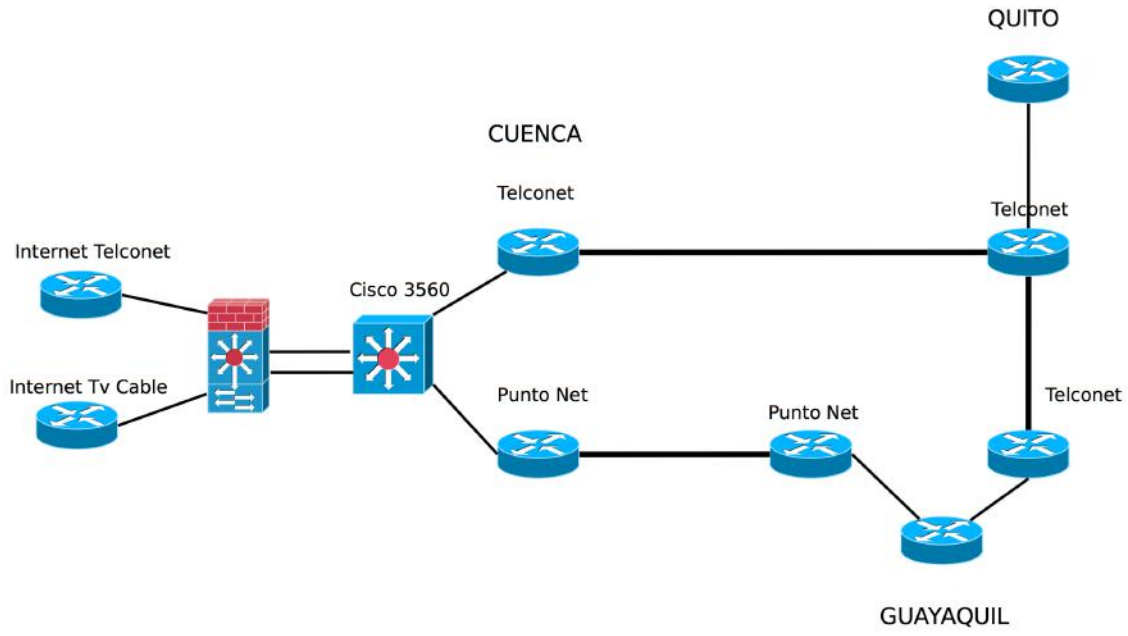


Ilustración 3-4 Diagrama Físico de enlaces a nivel nacional

3.1.2 Segmentación de Red VLSM y Direccionamiento

La *Tabla 3-2* describe el direccionamiento y las redes virtuales creadas para el manejo y diferenciación del tipo de tráfico. Cabe indicar que las redes virtuales han sido creadas para efectos de simulación. La cantidad de VLANs dependerá del número de servicios, seguridad, tipo de tráfico o departamentos que requiera la implementación. Para el caso de estudio se definen de manera general 6 redes virtuales con diferentes requerimientos y tipo de tráfico. Se excluye de las configuraciones parámetros de seguridad, únicamente se hace referencia, como ejemplo de configuración, a la seguridad implementada a nivel de interfaz de los switches de acceso de configuración fija (Port-Security [8]).

Equipo	Interfaz	Descripción	Dirección de Red	Dirección IP	Máscara
S1	VLAN 5	Administración	10.10.10.0/28	10.10.10.1	255.255.255.240
	VLAN 10	Telefonía	192.168.1.0/24	192.168.1.1	255255255.0
	VLAN 20	Video	192.168.2.0/24	192.168.2.1	255255255.0
	VLAN 30	Soporte	192.168.3.0/24	192.168.3.1	255255255.0
	VLAN 40	Internet	192.168.4.0/24	192.168.4.1	255255255.0
	VLAN 50	Servidores	192.168.5.0/24	192.168.5.1	255255255.0
S2	VLAN 5	Administración	10.10.10.0/28	10.10.10.2	255.255.255.240
S3	VLAN 5	Administración	10.10.10.0/28	10.10.10.3	255.255.255.240
S4	VLAN 5	Administración	10.10.10.0/28	10.10.10.4	255.255.255.240
S5	VLAN 5	Administración	10.10.10.0/28	10.10.10.5	255.255.255.240
S6	VLAN 5	Administración	10.10.10.0/28	10.10.10.6	255.255.255.240
S7	VLAN 5	Administración	10.10.10.0/28	10.10.10.7	255.255.255.240

Tabla 3-2 Segmentación de Red Centro de Datos

Para el direccionamiento de las agencias a nivel nacional se a tomado como referencia la ubicación de las agencias, implementando un esquema de

[8] Understanding Port Security - http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/port_sec.html#wp1061587 - último acceso 10 de junio 2016

direccionamiento por ciudad y/o sector del país. El plan de direccionamiento toma en cuenta un rengo de direcciones privadas 192.168.50.0-100.0 para agencias ubicadas en la cuidad de cuenca y alrededores, 192.168.100.0-150.0 para la parte norte del país, 192.168.150.0-200.0 para la ciudad de Guayaquil y alrededores, 192.168.200.0-250.0 para la ciudad de Manta y alrededores. La *Tabla 3-3* describe el direccionamiento de los equipos del backbone (Quito, Guayaquil y Cuenca), así como las agencias principales.

En la *Tabla 3-4* se detalla el direccionamiento lógico de la *Ilustración 3-4* que se utiliza para la simulación en GNS3. El diseño plantea la configuración de túneles entre las agencias para lograr un control independiente del proveedor, de acuerdo a lo revisado en las simulaciones del capítulo 2.

Para realizar la simulación de calidad de servicio, se incorporan nuevos elementos de direccionamiento como subredes virtuales VLANs para los diferentes aplicativos que utilizan las agencias; sin embargo, este direccionamiento extra no se contempla en la *Tabla 3-3*. Para la simulación del diseño propuesto, se toma como referencia el direccionamiento de las agencias mostrado en la *Tabla 3-3 y 3-4*.

Empresa	Ciudad	Agencia	Direcciones de Red	Host Disponibles	Máscara de Red	Gateway
QUITO MOTORS QM	QUITO	MATRIZ	192.168.100.0/24	254	255.255.255.0	192.168.100.1
	LATACUNGA	LAT	192.168.103.0/26	62	255.255.255.192	192168.103.1
	RIOBAMBA	RIO	192.168.103.64/26	62	255.255.255.192	192168.103.65
	AMBATO	AMB	192.168.103.128/26	62	255.255.255.192	192.168.103.129
	IBARRA	IBA	192.168.103.192/26	62	255.255.255.192	192.168.103.193
	SANTO DOMINGO	STO DOM	192.168.104.0/26	62	255.255.255.192	192168.104.1
NEOAUTO NA	QUITO	MATRIZ	192.168.101.0/25	126	255.255.255.128	192.168.101.1
	QUITO	SUR	192.168.101.128/26	62	255.255.255.192	192.168.101.129
	QUITO	SHIRIS	192.168.101.192/26	62	255.255.255.192	192.168.101.193
	QUITO	AMB	192.168.102.0/26	62	255.255.255.192	192.168.102.1
	QUITO	STO DOM	192.168.102.64/26	62	255.255.255.192	192.168.102.65
MERQUIAUTO MQ	QUITO	MATRIZ	192.168.102.128/25	126	255.255.255.128	192.168.102.129
	LATACUNGA	LAT	192.168.104.64/26	62	255.255.255.192	192168.104.65
	IBARRA	IBA	192.168.104.128/26	62	255.255.255.192	192.168.104.129
	RIOBAMBA	RIO	192.168.104.192/26	62	255.255.255.192	192.168.104.193
	TENA	TENA	192.168.105.0/26	62	255.255.255.192	192168.105.1
	PUYO	PUYO	192.168.105.64/26	62	255.255.255.192	192168.105.65
	QUEVEDO	QUE	192.168.105.128/26	62	255.255.255.192	192.168.105.129
LOGIMANTA LM	MANTA	MATRIZ	192.168.200.0/24	254	255.255.255.0	192.168.200.1
	MANTA	PATIOS	192.168.201.0/25	126	255.255.255.128	192.168.201.1
	MANTA	BODEGA	192.168.201.128/25	126	255.255.255.128	192.168.201.129
AUTOHYUNAH	GUAYAQUIL	MATRIZ	192.168.150.0/24	254	255.255.255.0	192.168.150.1
	GUAYAQUIL	ECSY AUTO	192.168.151.0/25	126	255.255.255.128	192.168.151.1
	GUAYAQUIL	LOCALIZA	192.168.151.128/25	62	255.255.255.192	192.168.151.129
	GUAYAQUIL	AMERICAS	192.168.151.192/25	62	255.255.255.192	192.168.151.193
CUENCA	CUENCA	MERQUIAUTO	192.168.50.128/26	62	255.255.255.192	192.168.50.129
	CUENCA	AUTOHYUN	192.168.50.192/26	62	255.255.255.192	192.168.50.193
	CUENCA	NEOAUTO	192.168.51.0/24	254	255255255.0	192.168.51.1
	CUENCA	QUITO MOTORS	192.168.50.0/25	126	255.255.255.128	192.168.50.1

Tabla 3-3 Direccionamiento de red agencias a nivel nacional

Interfaz	Descripción	Dirección de Red	Dirección Origen	Dirección Destino
Túnel 0	CUE-GYE	10.1.1.0/30	172.16.0.1	172.16.0.2
Túnel 1	CUE-UIO QM	10.1.1.4/30	172.16.0.5	172.16.0.6
Túnel 2	UIO-GYE AH	10.1.1.8/30	172.16.0.9	172.16.0.10
Túnel 3	CUE-GYE AMERICAS AH	10.1.1.12/30	172.16.0.1	172.16.0.22
Túnel 4	CUE-AMBATO QM	10.1.1.16/30	172.16.0.5	172.16.0.14
Túnel 5	CUE-RIO QM	10.1.1.20/30	172.16.0.5	172.16.0.18

Tabla 3-4 Direccionamiento Túneles

La *Tabla 3-4* detalla el direccionamiento de los túneles configurados para la simulación. Se incluye también las subredes del proveedor como referencia en las configuraciones. El direccionamiento se aplica a la topología de la *Ilustración 3-5* utilizada para la simulación.

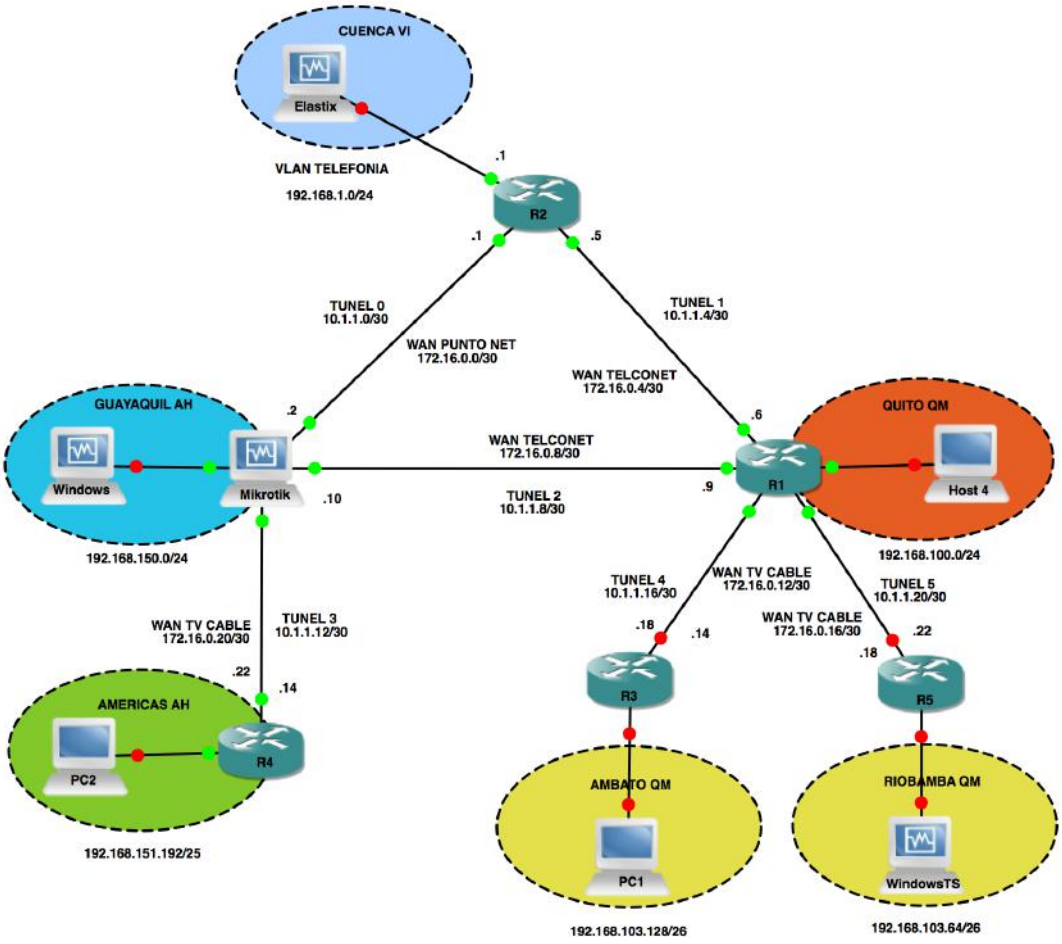


Ilustración 3-5 Diagrama Lógico – Simulación del Diseño

La *Tabla 3-5* muestra el direccionamiento de los routers de la topología de la *Ilustración 3-5* y especifica el direccionamiento por interfaz de cada equipo. En base a este direccionamiento se realiza la simulación del diseño propuesto.

Equipo	Interfaz	Red	Dirección IP	Máscara de Subred
R1	FastEthernet 0/0	172.16.0.4/30	172.16.0.6	255.255.255.252
	FastEthernet 0/1	192.168.100.0/24	192.168.100.1	255.255.255.252
	FastEthernet 1/0	172.16.0.8/30	172.16.0.9	255.255.255.252
	FastEthernet 2/0	172.16.0.12/30	172.16.0.13	255.255.255.252
	FastEthernet 3/0	172.16.0.16/30	172.16.0.17	255.255.255.252
	TUNEL 1	10.1.1.4/30	10.1.1.6	255.255.255.252
	TUNEL 2	10.1.1.8/30	10.1.1.9	255.255.255.252
R2	FastEthernet 0/0	172.16.0.4/30	172.16.0.5	255.255.255.252
	FastEthernet 0/1	192.168.1.0/24	192.168.1.1	255.255.255.252
	FastEthernet 1/0	172.16.0.8/30	172.16.0.9	255.255.255.252
	TUNEL 0	10.1.1.0/30	10.1.1.1	255.255.255.252
	TUNEL 1	10.1.1.4/30	10.1.1.5	255.255.255.252
	TUNEL 3	10.1.1.12/30	10.1.1.13	255.255.255.252
	TUNEL 4	10.1.1.16/30	10.1.1.17	255.255.255.252
	TUNEL 5	10.1.1.20/30	10.1.1.21	255.255.255.252
MIKROTIK	FastEthernet 0	192.168.150.0/24	192.168.150.1	255.255.255.252
	FastEthernet 1	172.16.0.0/30	172.16.0.2	255.255.255.252
	FastEthernet 2	172.16.0.8/30	172.16.0.10	255.255.255.252
	FastEthernet 3	172.16.0.20/30	172.16.0.21	255.255.255.252
	FastEthernet 3/0	172.16.0.16/30	172.16.0.17	255.255.255.252
	TUNEL 0	10.1.1.0/30	10.1.1.2	255.255.255.252
	TUNEL 2	10.1.1.8/30	10.1.1.10	255.255.255.252
R3	FastEthernet 1/0	172.16.0.12/30	172.16.0.14	255.255.255.252
	FastEthernet 0/1	192.168.103.128/26	192.168.103.129	255.255.255.192
	TUNEL 4	10.1.1.16/30	10.1.1.18	255.255.255.252
R4	FastEthernet 0/0	172.16.0.20/30	172.16.0.22	255.255.255.252
	FastEthernet 0/1	192.168.151.192/25	192.168.151.193	255.255.255.128
	TUNEL 3	10.1.1.12/30	10.1.1.14	255.255.255.252
R5	FastEthernet 1/0	172.16.0.16/30	172.16.0.18	255.255.255.252
	FastEthernet 2/0	192.168.103.64/26	192.168.103.65	255.255.255.192
	TUNEL 5	10.1.1.20/30	10.1.1.22	255.255.255.252

Tabla 3-5 Direccionamiento Routers a Nivel Nacional

3.1.3 Licenciamiento de los equipos (IOS)

Un aspecto importante a tener en cuenta en el diseño de los servicios de red, es la licencia que tendrán los routers o switches de la topología. Por ejemplo, en cisco los equipos viene con un Universal Cisco Software Image precargado *(Ilustración 3-6)* que contiene todas las características que podrán ejecutarse en el equipo. Las funcionalidades disponibles en un equipo están determinadas por la combinación de una o varias licencias instaladas en el mismo. La flash memory almacena un archivo con esta licencia y de esta manera se libera un set de funcionalidades en el equipo.

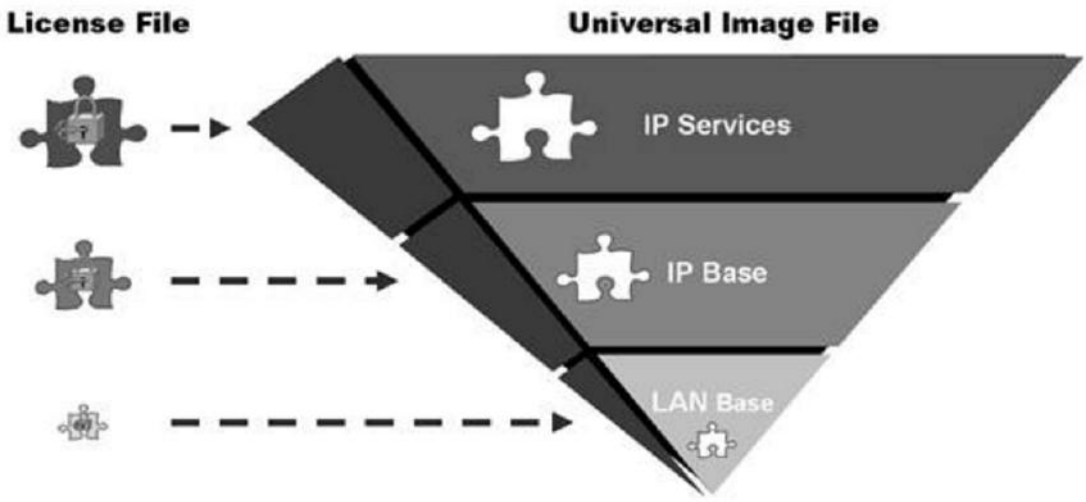


Ilustración 3-6 Características del Licenciamiento [9]

La *Ilustración 3-7* muestra algunas de las funcionalidades que se liberan en cada tipo de licenciamiento. Para el diseño del caso de estudio nos interesa el licenciamiento funciones IP Services, ya que incorpora las funcionalidades de OSPF y PBR que servirán para enrutamiento dinámico e implementación de calidad de servicio respectivamente.

[9] Imagen tomada de http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3560-x-series-switches/white_paper_c11-579326.html

Cada marca de equipos de comunicaciones implementa servicios de licenciamiento similares, por ejemplo en Mikrotik manejan un licenciamiento por niveles L4, L5 y L6. De igual manera los equipos vienen con el software RouterOS preinstalado, pero en función del licenciamiento que tenga el equipo, se liberan un set de funcionalidades diferentes.

Ya que el set de funcionalidades que se libera con un licenciamiento mas avanzado es mayor, el costo también es mayor y se vuelve un parámetro muy importante dentro del diseño de la red.

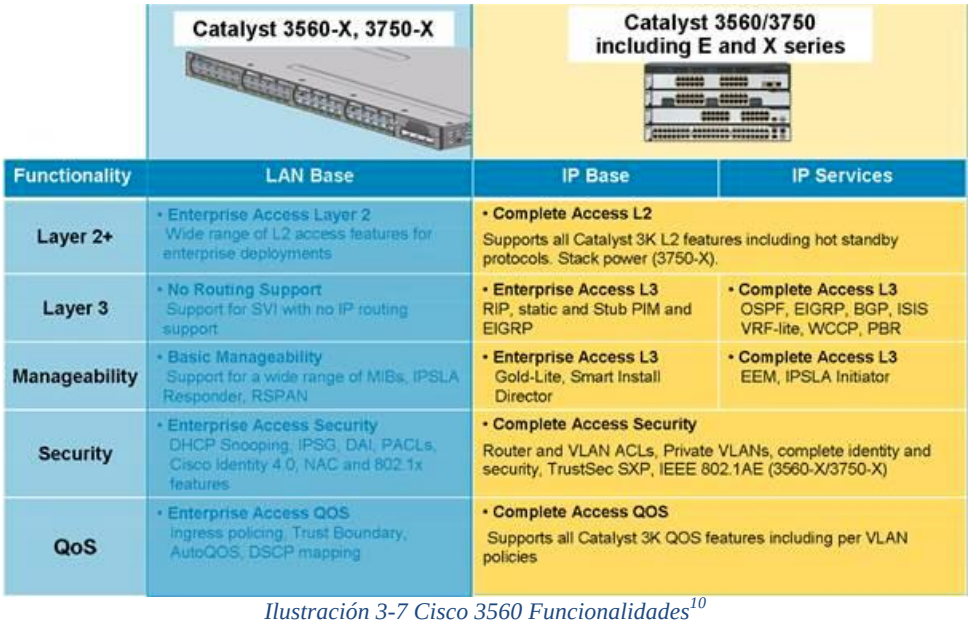


Ilustración 3-7 Cisco 3560 Funcionalidades[10]

3.2 Simulación del diseño en GNS3 [7]

En función de realizar la simulación se requiere prepara el escenario del diseño propuesto. Como se revisó en el capítulo 2 los enlaces a nivel nacional implementan OSPF y Túneles GRE entre el centro de datos y las agencias. La topología para la simulación es la detallada en el Ilustración 3-5 con el direccionamiento y

[10] Imagen tomada de http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3560-x-series-switches/white_paper_c11-579326.html

segmentación de red especificado en las Tablas 3-3, 3-4 y 3-5. Adicional a esta, se tiene la topología de la Ilustración 3-3 que corresponde al diseño para el centro de datos. Para efectos de simulación se incorporan 6 agencias correspondiendo 3 al backbone principal entre Quito, Guayaquil y Cuenca y 3 agencias distribuidas, 2 en Quito y 1 en Guayaquil. La simulación se compone de dos partes:

- Implementación del diseño para el cuarto de datos en el entorno GNS3 - *Ilustración 3-3*.
- Implementación del diseño para la red a nivel nacional en el entorno GNS3 – *Ilustración 3-5.*

3.2.1 Implementación del diseño para el cuarto de datos entorno GNS3

Para la implementación del diseño para el cuarto de datos, se requieren configuraciones en capa 2. De manera general se requieren redes virtuales para segmentar los servicios de red, eliminar broadcast innecesario, seguridad. Mediante el protocolo VTP (VLAN Trunk Protocol) se optimiza la **administración** de las redes virtuales, centralizando las configuraciones en el switch S1 correspondiente al equipo Cisco Catalyst 3560 del nivel de core. Este equipo se encarga del ruteo inter-vlans. La *Tabla 3-6* detalla las configuraciones necesarias en cada equipo para implementar el protocolo VTP. El diagrama lógico se detalla en la *Ilustración 3-3*.

Equipo	VTP Mode	Domain/Clave	VLAN Creadas	VLAN Aprendidas
S1	Server	Tesis	5,10,20,30,40,50	-
S2	Client	Tesis	-	5,10,20,30,40,50
S3	Client	Tesis	-	5,10,20,30,40,50
S4	Client	Tesis	-	5,10,20,30,40,50
S5	Client	Tesis	-	5,10,20,30,40,50
S6	Client	Tesis	-	5,10,20,30,40,50
S7	Client	Tesis	-	5,10,20,30,40,50

Tabla 3-6 Configuración VTP

Adicional a la configuración de las redes virtuales VLANs y a la mejora de la administración de las mismas con el protocolo VTP, se requiere configurar el protocolo RSTP (Rapid Spanning Tree Protocol) definido en el estándar IEEE Std 802.1w-2001. El principal objetivo de STP es evitar la creación de bucles en trayectos redundantes en la red. Al implementar STP sobre la topología redundante se evitan los bucles que resultan fatales para la red.

```
R1#show spanning-tree summary
Root bridge for: VLAN1, VLAN5, VLAN10, VLAN20, VLAN30, VLAN40, VLAN50.
PortFast BPDU Guard is disabled
UplinkFast is disabled
BackboneFast is disabled

Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- ---------- -------- ---------- ----------
VLAN1                0        0          0        2          2
VLAN5                0        0          0        2          2
VLAN10               0        0          0        2          2
VLAN20               0        0          0        2          2
VLAN30               0        0          0        2          2
VLAN40               0        0          0        2          2
VLAN50               0        0          0        2          2
-------------------- -------- ---------- -------- ---------- ----------
            7 VLANs  0        0          0        14         14
```

Ilustración 3-8 Resumen del STP en R1

De manera general los switches implementan automáticamente el protocolo STP. Para el caso de estudio, cisco implementa el protocolo STP por defecto. Se requiere cambiar de STP a RSTP para tener una rápida convergencia. Para implementar el balanceo de carga se debe modificar el STP de manera que todos los enlaces queden activos y balanceados en concordancia al tráfico que se maneja cada VLAN. La *Ilustración 3-8* muestra el estado inicial del switch R1 como root bridge para todas las VLANs configuradas, lo cual genera una única ruta activa, dejando el enlace entre R3-R2 bloqueado, desperdiciando recursos.

```
R1#sho spanning-tree summary
Root bridge for: VLAN1, VLAN5, VLAN50.
PortFast BPDU Guard is disabled
UplinkFast is disabled
BackboneFast is disabled

Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- ---------- -------- ---------- ----------
VLAN1                0        0          0        2          2
VLAN5                0        0          0        2          2
VLAN10               0        0          0        2          2
VLAN20               0        0          0        2          2
VLAN30               0        0          0        2          2
VLAN40               0        0          0        2          2
VLAN50               0        0          0        2          2
-------------------- -------- ---------- -------- ---------- ----------
            7 VLANs  0        0          0        14         14
```

```
R2#sho spanning-tree summary
Root bridge for: VLAN20, VLAN30.
PortFast BPDU Guard is disabled
UplinkFast is disabled
BackboneFast is disabled

Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- --------- -------- ---------- ----------
VLAN1                0        0         0        3          3
VLAN5                0        0         0        3          3
VLAN10               1        0         0        2          3
VLAN20               0        0         0        3          3
VLAN30               0        0         0        3          3
VLAN40               1        0         0        2          3
VLAN50               0        0         0        3          3
-------------------- -------- --------- -------- ---------- ----------
            7 VLANs  2        0         0        19         21

R3#show spanning-tree summary
Root bridge for: VLAN10, VLAN40.
PortFast BPDU Guard is disabled
UplinkFast is disabled
BackboneFast is disabled

Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- --------- -------- ---------- ----------
VLAN1                1        0         0        3          4
VLAN5                1        0         0        1          2
VLAN10               0        0         0        2          2
VLAN20               1        0         0        1          2
VLAN30               1        0         0        1          2
VLAN40               0        0         0        2          2
VLAN50               1        0         0        1          2
-------------------- -------- --------- -------- ---------- ----------
            7 VLANs  5        0         0        11         16
```

Ilustración 3-9 Resumen STP enlaces balanceados

La *Ilustración 3-9* muestra el resumen del STP luego de realizar el balanceo de carga en los enlaces. Se puede observar que los routers se distribuyen como root bridge de las diferentes VLANs, manteniendo activos todos los enlaces. El momento que falle algún equipo o interfaz física de un enlace, este se bloquea y el tráfico se direcciona por otro path que determina STP. Se provee **confiabilidad** en el diseño por medio de la redundancia a nivel de capa 2 en el centro de datos.

Para brindar **escalabilidad** en los enlaces del cuarto de datos el diseño propone implementar la agregación de enlaces basado en el protocolo LACP (Link Aggregation Control Protocol). Una de las formas de implementar la agregación de enlaces es por medio de la funcionalidad Port Channel que permite agrupar hasta 8 interfaces de manera lógica. Estas interfaces agrupadas lógicamente se ven como un puerto adicional del equipo con una capacidad aproximada a la suma de las capacidades de cada interfaz que compone el Port Channel. De esta manera se puede incrementar la capacidad en un enlace y la redundancia del mismo.

Esta nueva interfaz se mantendrá funcional mientras al menos una de las interfaces que la componen se mantenga activa. La capacidad será igual a la suma de los enlaces activos. Como se puede observar en la *Ilustración 3-2* cada enlace entre los switches de los niveles de core, distribución y acceso mantienen una configuración de link agregado que proporciona redundancia y cierta escalabilidad en capacidad.

Junto con la configuración del protocolo STP el diseño brinda redundancia y un alto grado de confiabilidad al contar con equipos y enlaces redundantes en el centro datos. La *Ilustración 3-10* muestra en resumen los protocolos STP y LACP activos, brindando la redundancia y capacidad deseadas. Se observa el protocolo Spannig Tree activo con los puertos Port-Channel 1, 2, 3 que corresponden a la agregación de enlaces. En el siguiente capítulo se analiza la capacidad resultante al tener varias interfaces agregadas.

```
VLAN10
  Spanning tree enabled protocol ieee
  Root ID     Priority    8192
              Address     c803.1597.0002
              Cost        12
              Port        122 (Port-channel3)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32768
              Address     c802.158c.0002
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface                                    Designated
Name                 Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
-------------------- ------- ---- ----- --- ----- -------------------- -------
Port-channel1        128.121  128    12 BLK    12 32768 c801.158a.0002 128.121
Port-channel3        128.122  128    12 FWD     0  8192 c803.1597.0002 128.122
Port-channel2        128.123  128    12 FWD    12 32768 c802.158c.0002 128.123
```

Ilustración 3-10 Resumen STP e interfaces Port-channel Router R2

3.2.2 Implementación del diseño para la red a nivel nacional entorno GNS3

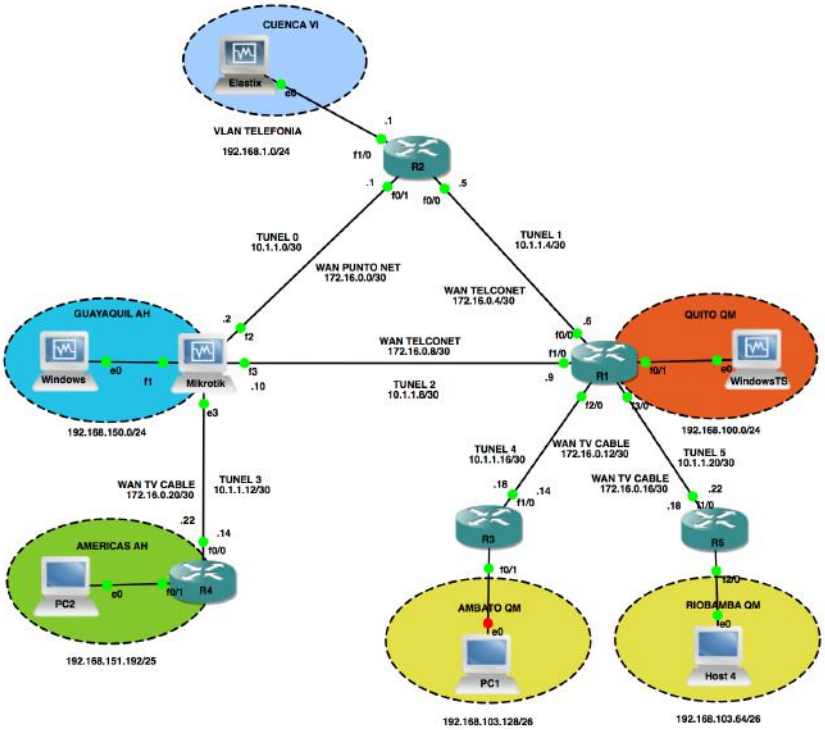


Ilustración 3-11 Topología de Simulación - Caso de Estudio

La *Ilustración 3-11* muestra la topología de red utilizada para la simulación del diseño de red a nivel nacional del caso de estudio. Para la implementación del diseño en el simulador GNS3 se requiere la configuración de los protocolos introducidos en el capítulo 2, OSPF, Túneles GRE y Route Map.

Una vez realizada la configuración de los Túneles GRE, se procede a la implementación del enrutamiento OSPF sobre los Túneles configurados. Cabe indicar que para efectos de simulación se utiliza un mismo equipo para las interfaces LAN (Agencias) y WAN (Proveedor). En un entorno práctico el proveedor instala su propio equipo y se encarga del enrutamiento entre las redes WAN de sus equipos instalados en las agencias. El enrutamiento entre las redes LAN de las agencias se realiza sobre los Túneles GRE con la redistribución de rutas automáticas por medio de OSPF, siendo configuraciones propias del departamento de Telecomunicaciones.

Como se muestra en las Ilustraciones 3-12,13,14 y 15, se encuentran configurados los Túneles GRE 1-5 y el protocolo OSPF esta re distribuyendo las rutas entre los equipos del backbone y agencias. Se presenta el resumen las configuraciones, siguiendo los pasos y comandos explicados en el Capítulo 2.

Route information

Name	sysName	sysContact	sysLocation	Comments
R1 [192.168.100.1]	R1			

Destination	Next Hop IP	ifDescr	Route Type	Method	Route Mask	Metric 1-4
10.1.1.0/30	10.1.1.10	Tunnel2	Indirect	OSPF	255.255.255.252	11121,-1,-1,-1
10.1.1.4/30	10.1.1.6	Tunnel1	Direct	Local	255.255.255.252	0,-1,-1,-1
10.1.1.8/30	10.1.1.9	Tunnel2	Direct	Local	255.255.255.252	0,-1,-1,-1
10.1.1.12/30	10.1.1.5	Tunnel1	Indirect	OSPF	255.255.255.252	22222,-1,-1,-1
10.1.1.16/30	10.1.1.5	Tunnel1	Indirect	OSPF	255.255.255.252	22222,-1,-1,-1
10.1.1.20/30	10.1.1.5	Tunnel1	Indirect	OSPF	255.255.255.252	22222,-1,-1,-1
172.16.0.0/30	10.1.1.5	Tunnel1	Indirect	OSPF	255.255.255.252	11121,-1,-1,-1
172.16.0.4/30	172.16.0.6	FastEthernet0/0	Direct	Local	255.255.255.252	0,-1,-1,-1
172.16.0.8/30	172.16.0.9	FastEthernet1/0	Direct	Local	255.255.255.252	0,-1,-1,-1
172.16.0.12/30	172.16.0.13	FastEthernet2/0	Direct	Local	255.255.255.252	0,-1,-1,-1
172.16.0.16/30	172.16.0.17	FastEthernet3/0	Direct	Local	255.255.255.252	0,-1,-1,-1
172.16.0.20/30	10.1.1.10	Tunnel2	Indirect	OSPF	255.255.255.252	11131,-1,-1,-1
192.168.1.0/24	10.1.1.5	Tunnel1	Indirect	OSPF	255.255.255.0	11112,-1,-1,-1
192.168.100.0/24	192.168.100.1	FastEthernet0/1	Direct	Local	255.255.255.0	0,-1,-1,-1
192.168.103.64/26	10.1.1.5	Tunnel1	Indirect	OSPF	255.255.255.192	22223,-1,-1,-1
192.168.103.128/26	10.1.1.5	Tunnel1	Indirect	OSPF	255.255.255.192	22232,-1,-1,-1
192.168.150.0/24	10.1.1.10	Tunnel2	Indirect	OSPF	255.255.255.0	11131,-1,-1,-1
192.168.151.128/25	10.1.1.5	Tunnel1	Indirect	OSPF	255.255.255.128	22232,-1,-1,-1

Ilustración 3-12 Resumen configuración R1 UIO

Route information

Name	sysName	sysContact	sysLocation	Comments
R2 [192.168.1.1]	R2			

Destination	Next Hop IP	ifDescr	Route Type	Method	Route Mask	Metric 1-4
10.1.1.0/30	10.1.1.1	Tunnel0	Direct	Local	255.255.255.252	0,-1,-1,-1
10.1.1.4/30	10.1.1.5	Tunnel1	Direct	Local	255.255.255.252	0,-1,-1,-1
10.1.1.8/30	10.1.1.2	Tunnel0	Indirect	OSPF	255.255.255.252	11121,-1,-1,-1
10.1.1.12/30	10.1.1.13	Tunnel3	Direct	Local	255.255.255.252	0,-1,-1,-1
10.1.1.16/30	10.1.1.17	Tunnel4	Direct	Local	255.255.255.252	0,-1,-1,-1
10.1.1.20/30	10.1.1.21	Tunnel5	Direct	Local	255.255.255.252	0,-1,-1,-1
172.16.0.0/30	172.16.0.1	FastEthernet0/1	Direct	Local	255.255.255.252	0,-1,-1,-1
172.16.0.4/30	172.16.0.5	FastEthernet0/0	Direct	Local	255.255.255.252	0,-1,-1,-1
172.16.0.8/30	10.1.1.2	Tunnel0	Indirect	OSPF	255.255.255.252	11131,-1,-1,-1
172.16.0.12/30	172.16.0.6		Indirect	Local	255.255.255.252	0,-1,-1,-1
172.16.0.16/30	172.16.0.6		Indirect	Local	255.255.255.252	0,-1,-1,-1
172.16.0.20/30	172.16.0.2		Indirect	Local	255.255.255.252	0,-1,-1,-1
192.168.1.0/24	192.168.1.1	FastEthernet1/0	Direct	Local	255.255.255.0	0,-1,-1,-1
192.168.100.0/24	10.1.1.6	Tunnel1	Indirect	OSPF	255.255.255.0	11121,-1,-1,-1
192.168.103.64/26	10.1.1.22	Tunnel5	Indirect	OSPF	255.255.255.192	11112,-1,-1,-1
192.168.103.128/26	10.1.1.18	Tunnel4	Indirect	OSPF	255.255.255.192	11121,-1,-1,-1
192.168.150.0/24	10.1.1.2	Tunnel0	Indirect	OSPF	255.255.255.0	11131,-1,-1,-1
192.168.151.128/25	10.1.1.14	Tunnel3	Indirect	OSPF	255.255.255.128	11121,-1,-1,-1

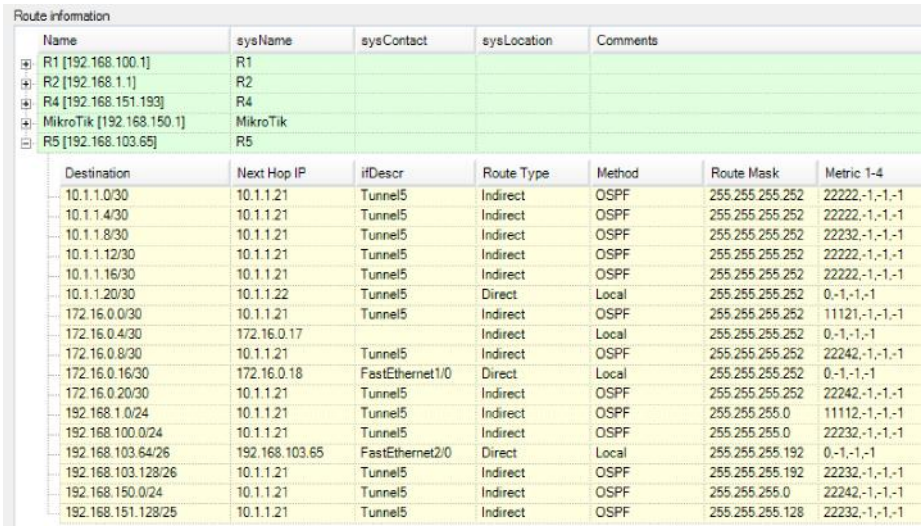
Ilustración 3-13 Resumen configuración R2 CUE

Route information

Name	sysName	sysContact	sysLocation	Comments
MikroTik [192.168.150.1]	MikroTik			

Destination	Next Hop IP	ifDescr	Route Type	Method	Route Mask	Metric 1-4
10.1.1.0/30	10.1.1.2	tunnel0	Direct	Other	255.255.255.252	0,-1,-1,-1
10.1.1.8/30	10.1.1.10	tunnel2	Direct	Other	255.255.255.252	0,-1,-1,-1
10.1.1.16/30	10.1.1.1	tunnel0	Indirect	OSPF	255.255.255.252	110,-1,-1,-1
172.16.0.0/30	172.16.0.2	ether2	Direct	Other	255.255.255.252	0,-1,-1,-1
172.16.0.20/30	172.16.0.21	ether4	Direct	Other	255.255.255.252	0,-1,-1,-1
192.168.100.0/24	10.1.1.9	tunnel2	Indirect	OSPF	255.255.255.0	110,-1,-1,-1
192.168.103.128/26	10.1.1.1	tunnel0	Indirect	OSPF	255.255.255.192	110,-1,-1,-1
192.168.151.128/25	10.1.1.1	tunnel0	Indirect	OSPF	255.255.255.128	110,-1,-1,-1

Ilustración 3-14 Resumen configuración Mikrotik GYE



Route information

Name	sysName	sysContact	sysLocation	Comments
R1 [192.168.100.1]	R1			
R2 [192.168.1.1]	R2			
R4 [192.168.151.193]	R4			
MikroTik [192.168.150.1]	MikroTik			
R5 [192.168.103.65]	R5			

Destination	Next Hop IP	ifDescr	Route Type	Method	Route Mask	Metric 1-4
10.1.1.0/30	10.1.1.21	Tunnel5	Indirect	OSPF	255.255.255.252	22222,-1,-1,-1
10.1.1.4/30	10.1.1.21	Tunnel5	Indirect	OSPF	255.255.255.252	22222,-1,-1,-1
10.1.1.8/30	10.1.1.21	Tunnel5	Indirect	OSPF	255.255.255.252	22232,-1,-1,-1
10.1.1.12/30	10.1.1.21	Tunnel5	Indirect	OSPF	255.255.255.252	22222,-1,-1,-1
10.1.1.16/30	10.1.1.21	Tunnel5	Indirect	OSPF	255.255.255.252	22222,-1,-1,-1
10.1.1.20/30	10.1.1.22	Tunnel5	Direct	Local	255.255.255.252	0,-1,-1,-1
172.16.0.0/30	10.1.1.21	Tunnel5	Indirect	OSPF	255.255.255.252	11121,-1,-1,-1
172.16.0.4/30	172.16.0.17		Indirect	Local	255.255.255.252	0,-1,-1,-1
172.16.0.8/30	10.1.1.21	Tunnel5	Indirect	OSPF	255.255.255.252	22242,-1,-1,-1
172.16.0.16/30	172.16.0.18	FastEthernet1/0	Direct	Local	255.255.255.252	0,-1,-1,-1
172.16.0.20/30	10.1.1.21	Tunnel5	Indirect	OSPF	255.255.255.252	22242,-1,-1,-1
192.168.1.0/24	10.1.1.21	Tunnel5	Indirect	OSPF	255.255.255.0	11112,-1,-1,-1
192.168.100.0/24	10.1.1.21	Tunnel5	Indirect	OSPF	255.255.255.0	22232,-1,-1,-1
192.168.103.64/26	192.168.103.65	FastEthernet2/0	Direct	Local	255.255.255.192	0,-1,-1,-1
192.168.103.128/26	10.1.1.21	Tunnel5	Indirect	OSPF	255.255.255.192	22232,-1,-1,-1
192.168.150.0/24	10.1.1.21	Tunnel5	Indirect	OSPF	255.255.255.0	22242,-1,-1,-1
192.168.151.128/25	10.1.1.21	Tunnel5	Indirect	OSPF	255.255.255.128	22232,-1,-1,-1

Ilustración 3-15 Resumen configuración R5

Las configuraciones se basan en el direccionamiento especificado en la *Tabla 3-5*. Se observa las rutas hacia las distintas agencias y equipos del backbone. Las rutas para alcanzar las redes LAN de las agencias utilizan los diferentes Túneles configurados y se describen como Route Type Indirect, mientras que las redes configuradas localmente se describen como Route Type Direct.

Se realiza pruebas básicas de conectividad entre los nodos. La *Ilustración 3-16* muestra el resultado de un ping realizado desde la agencia de QUITO QM desde la máquina virtual WindowsTS hacia los diferentes nodos del backbone y agencias. Se obtienen resultados de latencias comprendidas entre 10ms-90ms, correspondientes la mas baja al Gateway de la agencia R1 - 192.168.100.1 y la latencia más alta al equipo R5 – 192.168.103.65. A pesar de que la red aún no tienen ningún servicio funcionando, se obtienen elevadas latencias entre los nodos. Esto se debe a que el entorno de simulación tiene varias máquinas e imágenes IOS virtualizadas funcionando simultáneamente, requiriendo mucho procesador y memoria de la máquina base (MacbookPro 4Gb Ram Intel Core i5).

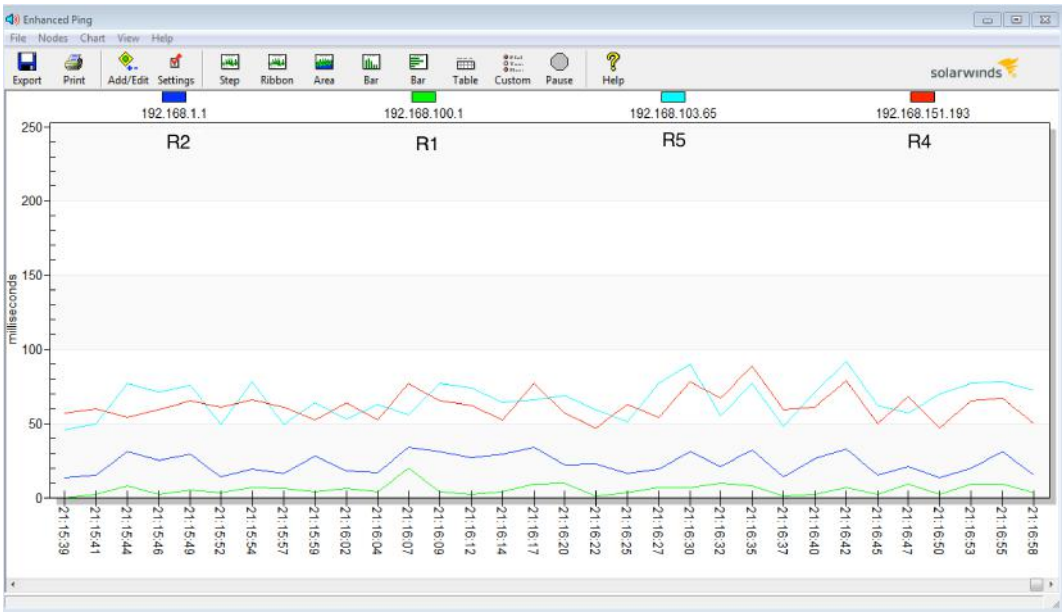


Ilustración 3-16 Latencia de ICMPs a los diferentes Routers

3.2.3 Configuración de calidad de servio QoS para VoIP

Para realizar la implementación de calidad de servicio en una red convergente (VoIP, Video y Datos) se deben tener en cuenta ciertos parámetros de la red que afectan el rendimiento de los aplicativos, principalmente de los servicios en tiempo real. Los parámetros a tener en cuenta para la implementación de QoS en el diseño de red propuesto son:

- **BW Disponible**: El Ancho de banda se comparte entre los aplicativos mencionados en el Capítulo 1.
- **End-to-End Delay**: Para realizar una conexión desde una agencia hacia el centro de datos en Cuenca, los paquetes deben atravesar varios routers y enlaces, lo cuál incoorpora retardos. Adicional a estos delays, el proceso de encapsulación incrementa los retardos end to end (Retardo por serialización).
- **Jitter**: VoIP sensible al retardo y a la variación del mismo → jitter.
- **Pérdida de Paquetes**: Los paquetes pueden ser descartados por enlaces congestionados. El caso de estudio presenta este problema, en videoconferencias la imagen se distorsiona, el audio se desfasa, en VoIP la

comunicación es entrecortada, en la tranferencia de archivos se tienen archivos corruptos.

Parámetros QoS						
Parámetro	**Solución**					
	Aumentar Ancho de Banda del enlace	Priorizar (Clasificar, marcar tráfico y mecanismos de encolamiento)	Compresión payload capa 2	Buffer De-Jitter	Incremento Buffer	Prevención de congestión
Ancho de Banda Disponible	✓	✓	✓			
Retardo End to End	✓	✓	✓			
Jitter				✓		
Pérdida de Paquetes	✓	✓			✓	✓

Tabla 3-7 Parámetro QoS

La *Tabla 3-7* muestra los diferentes parámetros a tener en cuenta para la implementación de QoS en el diseño propuesto, así como las posibles acciones a tomar para mitigar o eliminar los problemas que pueden producirse por bajo ancho de banda disponible, retardos o jitter y pérdida de paquetes.

Los pasos para implementar un control de asignación de recursos y una diferenciación de servicios son:

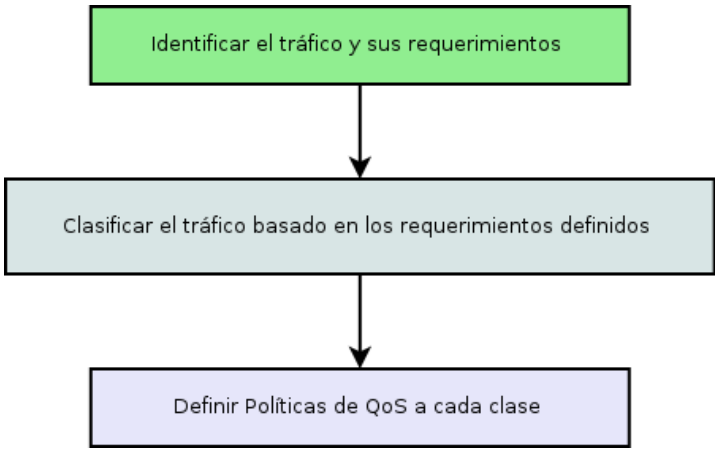


Ilustración 3-17 Pasos para implementara QoS en una red Convergente

3.2.4 Identificación de Tráfico y requerimientos

De acuerdo a lo revisado en el Capítulo 1, se resume en la *Tabla 3-5* el tráfico y requerimientos a tener en cuenta para la simulación de QoS para el caso de estudio.

	Tráfico	Requerimientos
VOZ	VoIP	84 Kbps x Llamada
APLICATIVOS	Escritorio Remoto (TS)	350 kbps x Sesión
	AS400	15 kpbs x Consola
	WEB	500 kbps - Promedio
	E-MAIL	150 kbps - Promedio
	TOTAL =	**955 kbps**

Tabla 3-8 Requerimientos Tráfico

El tráfico estimado se considera por usuario. Se debe extrapolar el tráfico necesario para los enlaces en función del número de usuarios en las agencias y servicios que ocupen cada uno. El peor escenario se deriva de una concurrencia total de usuarios y servicios de manera simultánea en cada agencia. Adicional a las mediciones presentadas, en una implementación práctica, se requiere analizar horas pico (utilización de CPU y del canal) y horas lentas o de congestión.

3.2.5 Clasificación de Tráfico

En base a la importancia de los aplicativos para la empresa, el modelo de negocio y objetivos, se clasifica el tráfico para luego definir políticas por clase.

En la *Ilustración 3-18* se definen 6 niveles de clasificación para el tráfico del caso de estudio. El primer nivel considera el tráfico de voz IP sensible a retardos y jitter, el cuál requiere una latencia mínima. En el segundo nivel se incorporan los aplicativos de la empresa con mayor importancia, siendo el Escritorio Remoto y el sistema AS400. En el tercer nivel se clasifican los protocolos de señalización de los servicios de voz SIP, y se agregan también la señalización de los servicios de red, tunelización

y enrutamiento dinámico, GRE y OSPF respectivamente. En el cuarto nivel se ubica el tráfico transaccional, como el que se genera en el aplicativo WEB de la compañía. Al igual que en el tercer nivel, el tráfico del cuarto nivel tiene una entrega garantizada. En los últimos niveles se coloca el tráfico menos susceptible a retardos y pérdida de paquetes como son el correo electrónico y el tráfico P2P y redes sociales.

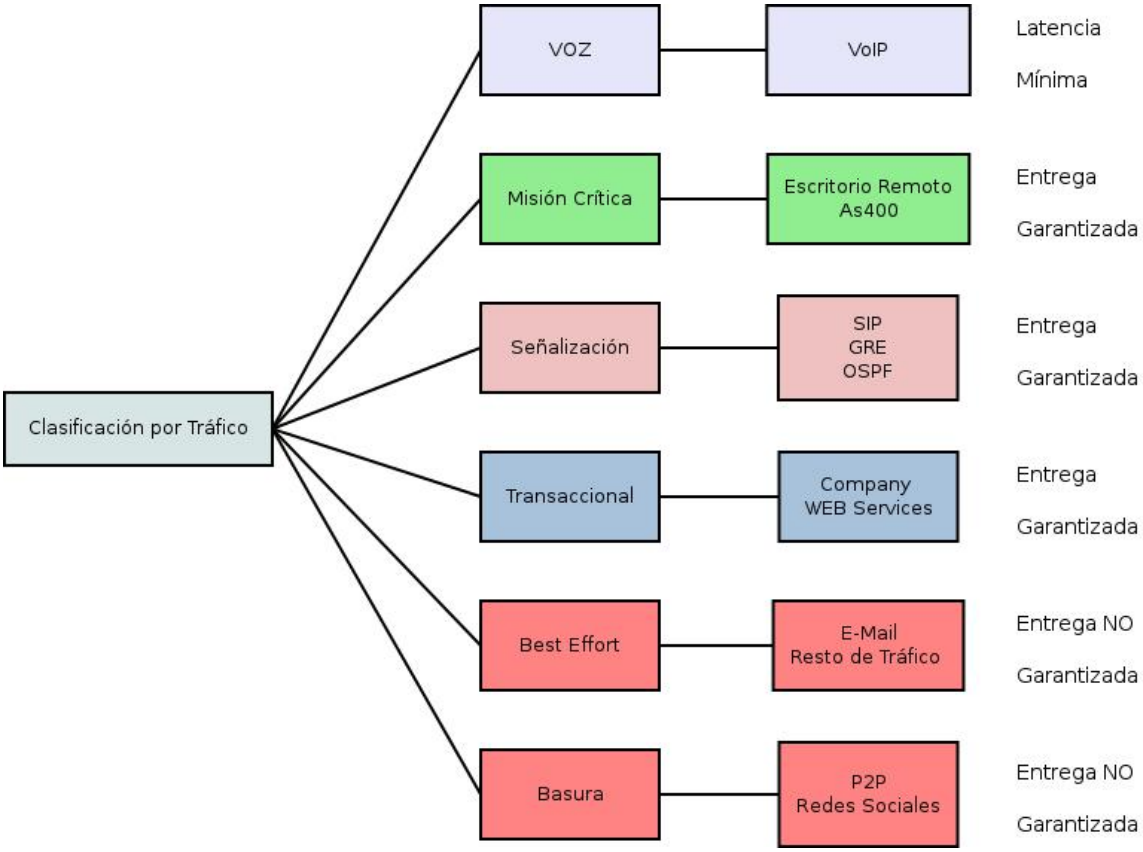


Ilustración 3-18 Clasificación de Tráfico - Caso de Estudio

3.2.6 Definición de Políticas por clase

En función de establecer las políticas por clase de tráfico, se deben definir los siguientes parámetros:

7. Establecer un límite máximo de ancho de banda para una clase
- Establecer un límite mínimo de ancho de banda garantizado para una clase

- Asignar un nivel de prioridad a cada clase
- Aplicar mecanismos de Control de Congestión (Queuing), Congestion Avoidance, y otras tecnologías avanzadas de QoS a una clase.

Clase	Tráfico	Max BW (kbps)	Min BW (kbps)	Prioridad
Voz	VoIP	1008	840	1
Misión Crítica	Escritorio Remoto/AS400	2100	1750	2
Señalización	SIP/GRE/OSPF	300	250	3
Transaccional	Web Services	1500	1200	4
Best Effort	email / Resto	1200	1000	5
Basura	P2P/Redes Sociales	700	500	6
Total =		6808	5540	

Tabla 3-9 Requerimientos por Clase - Políticas

De la *Tabla 3-9* se aproxima el ancho de banda para los enlaces troncales del backbone, a **6 Mbps**, donde:

8. El tráfico de voz tiene garantizado un 30% del total del ancho de banda.
9. El tráfico de Misión Crítica - Aplicativos, tiene garantizado un 20% del total del ancho de banda del enlace.
10. El tráfico de señalización tiene garantizado un 30% del total del ancho de banda.
11. El tráfico Transaccional, tiene garantizado un 20% del total del ancho de banda del enlace.
12. El tráfico best effort, tiene un 20% del total del ancho de banda del enlace, no garantizado.
13. El tráfico Basura, tiene un 20% del total del ancho de banda del enlace, no garantizado.

3.3 Configuración QoS

En función de configurar QoS aplicado al caso de estudio (simulación GNS3), se toman encuentra ciertas recomendaciones y directrices revisadas en la asignatura de Calidad de Servicio del Máster en Redes de Comunicaciones.

14. El Método más común para la clasificación y marcaje de paquetes es el uso de **class-maps** (**MQC –** Modular Qualify of Service Command Line Interface).
15. Class-maps pueden clasificar el tipo de aplicaciones usando **NBAR** (Network-Based Application Recognition) [12] como se revisó en el Capítulo 1.
16. La clasificación debe realizarce lo más cercano a la fuente de tráfico. Para el caso de estudio se realiza en switch de acceso.

Se elige el método MQC para la implementación de QoS en el entono de simulación sobre los métodos CLI (Command Line Interface), AutoQoS y SDM (Security Device Manager) QoS Wizard, ya que MQC se introduce para mejorar el método de CLI y permitir el uso de nuevas técnica de QoS. Algunas de las características de MQC son:

- La clasificación del tráfico y la definición de políticas de QoS son realizadas por separado, brindando una configuración modular.
- MQC es más eficiente y consume menos tiempo de procesamiento que CLI.
- Método uniforme a través de la mayoría de plataformas CISCO
- Las políticas son creadas y luego aplicadas a las interfaces, lo que permite el re uso de código.

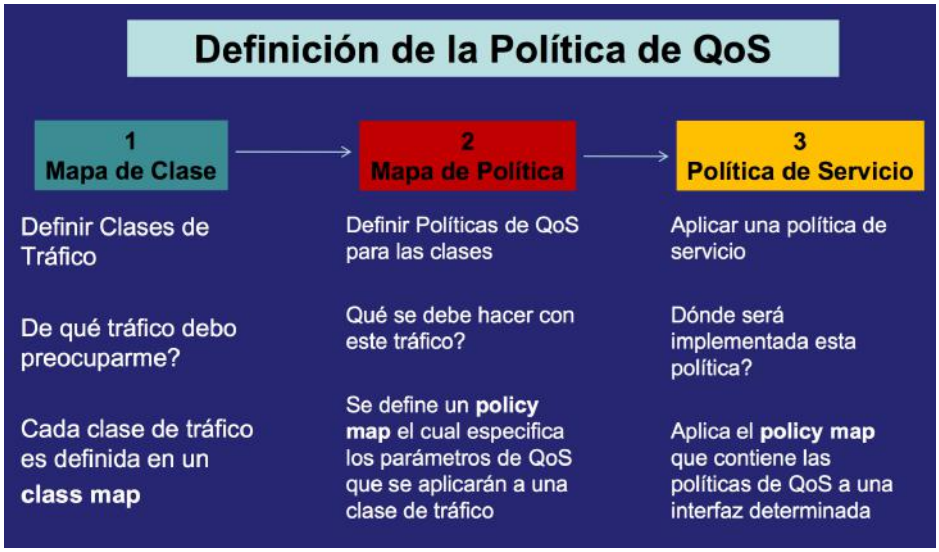


Ilustración 3-19 Pasos para implementar QoS Método MQC[11]

3.3.1 Mapa de Clase

La *Tabla 3-10* muestra las equivalencias de prioridades de PHB (Per hop Behaviour) e IPP (IP Precedence). En base a estos valores se realiza la clasificación y marcaje de los diferentes tipos de tráfico definidos para el caso de estudio.

Application	Layer 3 Classification			Layer 2 CoS
	IPP	PHB	DSCP	
Reserved	7	—	56–62	7
Reserved	6	—	48	6
Voice bearer	5	EF	46	5
Video-data traffic	4	AF41	34	4
Mission-critical data	3	AF31	26	3
Transactional data	2	AF2x	18, 20, 22	2
Scavenger	1	—	8	1
Bulk data	1	AF1x	10, 12, 14	1
Best-effort data	0	BE	0	0
Less-than-best-effort data	0	—	2, 4, 6	0

Tabla 3-10 Equivalencias PHB - IP Precedence[12]

[11] Imagen tomada de Asignatura QoS Máster en Redes de Comunicaciones Pontificie Universitaria Católica – "Métodos de Implementación QoS"

[12] Imagen tomada de Asignatura QoS Máster en Redes de Comunicaciones Pontificie Universitaria Católica – "Clasificación y Marcaje"

La *Tabla 3-11* muestra las configuraciones necesarias para el router R2 para la implementación de la clasificación y marcaje del tráfico definido en los class-maps, basados en protocolos conocidos de NBAR.

Clasificación y Marcaje de Tráfico - Router R2		
	Interface IN	**Interface OUT**
	F 1/0	**Tunnel0 / Tunnel1**
VOICE	class-map voice-in match protocol rtp audio	class-map voice-out match ip dscp ef
APLICACIONES	class-map match-any mission-critical-in match protocol xwindows match protocol telnet	class-map mission-critical-out match ip dscp af31
SIGNALING	class-map match-any signaling-in match protocol ospf match protocol gre match protocol snmp match protocol sip	class-map signaling-out match ip dscp af21
TRANSACCIONAL	class-map match-any transaccional-in match protocol http url www.virtualinfo.com.ec match protocol secure-http	class-map transaccional-out match ip dscp af22
BEST EFFORT	class-map match-any best-effort-in match protocol secure-ftp	class-map best-effort-out match ip dscp default
SCAVENGER / BASURA	class-map match-any basura-in match protocol gnutella match protocol kazaa2 match protocol fasttrack match protocol http url www.facebook.com match protocol http url www.youtube.com	class-map basura-out match ip precedence 0

Tabla 3-11 Clasificación y Marcaje de Tráfico - Router R2

3.3.2 Mapa de Políticas

Las políticas de tráfico determinan las características de QoS asociadas a una clase de tráfico anteriormente identificada usando **class maps**. Una política de tráfico contiene 3 elementos:

- Un nombre case-sensitive
- Una clase de tráfico
- La política de QoS asociada a una clase de tráfico

La *Tabla 3-12* resume las políticas definidas en el punto 3.2.3.3 Definición de políticas por clase. Como se observa el porcentaje de ancho de banda dinámico reservado se referencia a una conexión de 6 Mbps. Enlace estimado de acuerdo a las mediciones y consumo referido en el Capítulo 1.

Clase	Max BW (kbps)	Min BW (kbps)	Porcentaje Referenciado a un enlace de 6Mbps	Reservado (kbps)
Voz	1008	840	14%	840
Misión Crítica	2100	1750	29%	1740
Señalización	300	250	4%	240
Transaccional	1500	1200	20%	1200
Best Effort	1200	1000	17%	1020
Basura	700	500	8%	480
Enlace Troncal (kbps) =	**6000**		92%	

Tabla 3-12 Políticas

La *Tabla 3-13* muestra la configuración requerida en el Router R2 para implementar el policy-map QoS-Policy que incluye los class maps definidos en la *Tabla 3-11*. Es importante mencionar que tanto los class maps como el policy map son case sensitive, por lo tanto al configurar el policy map y llamar a los class maps de salida

(out) se tiene que ingresar el nombre configurado anteriormente. De igual manera al configurar las políticas de servicio en las interfaces respectivas, se deberá llamar a los policy maps con el nombre exacto.

Router R2	
F 1/0	**F 0/0, F/1**
policy-map class-mark class best-effort-in set ip dscp default class basura-in set ip precedence 0 class signaling-in set ip dscp af21 class transaccional-in set ip dscp af22 class voice-in set ip dscp ef class mission-critical-in set ip dscp af31	policy-map QoS-Policy class voice-out priority percent 14 class mission-critical-out bandwidth remaining percent 29 class signaling-out bandwidth remaining percent 4 class transaccional-out bandwidth remaining percent 20 class best-effort-out bandwidth remaining percent 17 class basura-out bandwidth remaining percent 8 class class-default fair-queue

Tabla 3-13 Tabla Policy-Map

Como se observa en la *Tabla 3-13*, el class class-default, contiene todo el tráfico no clasificado, y en este nivel se implementa un encolamiento de tipo fair-queue, que provee una división justa (*fair*) del ancho de banda de la interfaz entre todos los flujos activos restantes.

3.3.3 Política de Servicio

Debido a que la clasificación y marcado de tráfico debe configurarse en las interfaces Tunnel 0, Tunnel1 y Tunnel2 e interfaces de salida, se requiere adicionar una configuración jerárquica en las políticas del servicio. Esto se debe a que en interfaces lógicas de Cisco IOS, no es soportado un estado de congestión de manera inherente y no son compatibles con la aplicación directa de una política de servicio. Por este motivo, es necesario aplicar una política jerárquica de la siguiente manera:

Service Policy R2
policy-map parent class class-default shape average 6000000 service-policy qos-policy interface tunnel0 bandwidth 6000 service-policy output parent interface tunnel1 bandwidth 6000 service-policy output parent interface fast1/0 service-policy in class-mark

Tabla 3-14 Service Policy - Router R2

La *Tabla 3-14* muestra la configuración de las políticas de servicio en el router R2 aplicadas en las interfaces correspondientes a los túneles 0 y 1. Las políticas se aplican en modo out o de salida.

Cabe indicar que las configuraciones se especifican para el router R2, de igual manera se requieren configuraciones para todos los equipos del backbone. Para efectos de simulación se realizan las configuraciones en los routers R1-R6, pero como se indicó en las recomendaciones para la configuración de Calidad de Servicio, por escalabilidad el marcaje y clasificación de tráfico debe hacerse lo más cercano a la fuente de tráfico. Hay que tener en cuenta la frontera de confianza para esta implementación, que puede encontrase en:

- Dispositivos terminales (Teléfonos IP)
- En la capa de acceso (Switch de Acceso)
- En la capa de distribución (Switch de distribución)

La *Ilustración 3-20*, muestra los resultados del tráfico clasificado y marcado en la interfaz de ingreso fast0/1 del router R1.

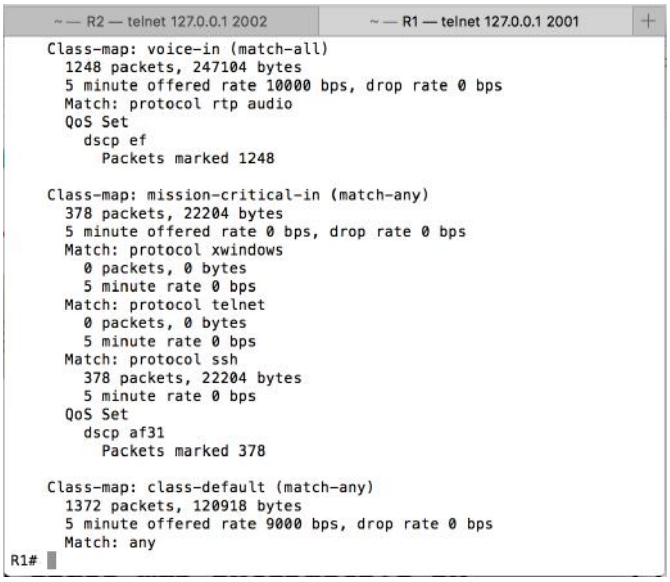


Ilustración 3-20 Tráfico de ingreso clasificado en Router R1

La *Ilustración 3-21*, muestra los resultados del tráfico clasificado y marcado en la interfaz de salida Tunnel1 del router R1.

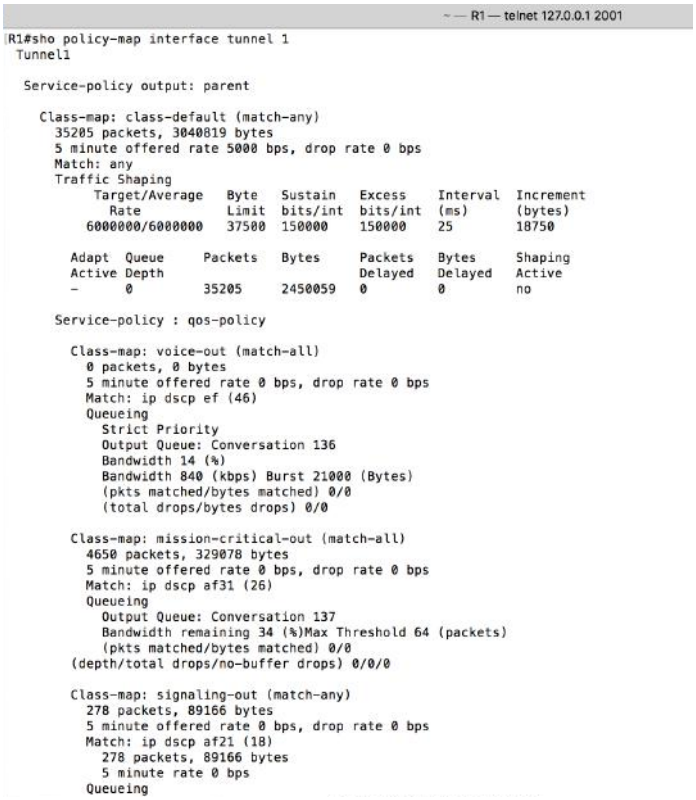


Ilustración 3-21 Tráfico de salida clasificado en router R1

El diseño propuesto contempla una primera etapa basada en los recursos disponibles y presupuesto del caso de estudio. En una segunda etapa se planta la implementación de un switch redundante en el nivel de core, lo cuál brindaría una confiabilidad comparable con un data center TIER 3. De igual manera en una segunda etapa se plantea el cambio a fibra óptica de los enlaces entre los switches y también entre el blade de servidores y los switches de distribución. Los switches propuestos en el diseño soportan puertos SFP de fibra para este cambio. En cuanto al blade, se requiere la compra de una tarjeta con soporte para puertos de fibra.

En el próximo Capítulo se analizan las configuraciones realizadas en los equipos realizando mediciones de tráfico y saturando los canales para ver el comportamiento de QoS en los enlaces congestionados. Las configuraciones buscan controlar el comportamiento de la red, de manera que ésta provea un servicio predecible (nivel de servicio) a las aplicaciones detalladas para el caso de estudio.

Capítulo 4 : PRUEBAS DEL SISTEMA

4.1 Software de monitoreo Cacti y Nagios

Para realizar el análisis del diseño propuesto, se plantea la implementación en el entorno de simulación de un sistema de monitoreo de enlaces y consumo de los diferentes canales. Se plantean las plataformas de monitoreo de Cacti y Nagios, siendo herramientas con versiones open source con grandes facilidades para monitoreo de TI.

La primera herramienta es Cacti que permite un monitoreo gráfico basado en almacenamiento de datos, mostrando estadísticas y estado de los enlaces. La captura de datos se hace a través de protocolo snmp y un poller configurable (5, 10, 30 minutos). La herramienta presenta templates para mostrar las gráficas de tráfico de manera web con una interfaz intuitiva y fácil de usar. Otro de los beneficios de la herramienta es su escalabilidad, que permite tener cientos de dispositivos en la consola de monitoreo.

La segunda herramienta que se analiza es Nagios. Este software tiene versiones de pago y open source. Se analizará la versión open source de Nagios Network Analizer. La herramienta provee estadísticas del banda, y herramientas de monitoreo de seguridades de la red y tráfico en general. El usuario puede configurar el monitoreo de información específica sobre IP únicas, puertos de origen, puertos de destino, o verificar si un equipo se encuentra infectado con malware y está saturando los enlaces.

4.1.1 Implementación de Cacti [13]

Para la simulación del caso de estudio se pretende virtualizar una máquina con un sistema operativo Linux y una distribución Centos 6.0 utilizando la herramienta virtualbox. Sobre esta máquina virtual se monta el monitor Cacti. Con ayuda del

GNS3 se configura la máquina virtual “Monitor_Cacti” en el entorno de simulación (Topología de Red).

El software Cacti se basa en un paquete open source que se puede instalar sobre una distribución de Linux o plataforma Windows. Requiere tener instalados los paquetes MySQL, PHP, RRDTool, net-snmp y Apache. Para la instalación de los paquetes iniciales se puede consultar la referencia.[13]

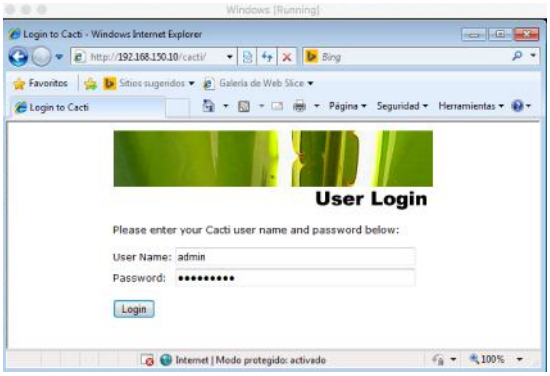


Ilustración 4-1 Administración Web Cacti

Una vez instalados los paquetes iniciales y configurado el usuario Cacti en la base de datos, se accede al servidor web con usuario y password admin, *Ilustración 4-1*. Se realizan las configuraciones iniciales:

- Crear los dispositivos (192.168.150.10/cacti → Managment → Devices)

De manera general las configuraciones para agregar un dispositivo al entorno de monitoreo Cacti, incluyen los siguientes parámetros:

  - Nombre del dispositivo
  - Host template (MIB Management Information Base), para el caso de estudio se selecciona el template “Cisco Router”.

[13] Instalación y configuración del software de monitoreo Cact
http://www.cacti.net/downloads/docs/html/unix_configure_cacti.html

- Versión snmp. Para la simulación se selecciona el protocolo snmp versión 2.

Una vez configurado el equipo, se indicará que la adyacencia a sido exitosa *Ilustración 4-2*. Claro está que los equipos deben tener activos el snmp en las interfaces a monitorear.

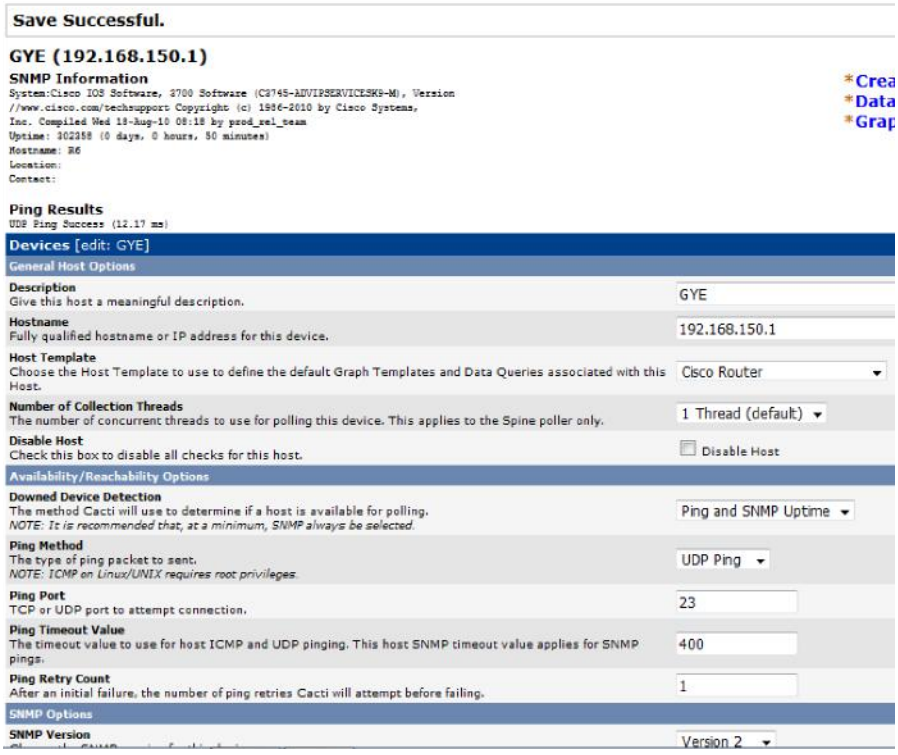


Ilustración 4-2 Cacti Dispositivos

- Crear los gráficos

Una vez agregado el dispositivo, se selecciona los gráficos de las interfaces que se desean monitorear. En este caso, como se trata de uno de los routers del backbone se agregarán todas las interfaces, incluidas las interfaces Túnel 0 y Túnel 2 correspondientes GYE – CUE y GYE –UIO respectivamente.

Ilustración 4-3 Cacti Configuración del Gráfico de Interfaces

- Crear el árbol de monitoreo (192.168.150.10/cacti → Managment→Graph Tree)

Una vez configuradas las interfaces a monitorear, se crea un nuevo árbol para organizar la topología. Para el caso de estudio se configura el backbone Quito, Guayaquil y Cuenca, y como ejemplo los dispositivos de las agencias Ambato, Riobamba y Guayaquil.

Ilustración 4-4 Cacti Arbol de Monitoreo

Las configuraciones anteriores, dispositivos, gráficos y árbol de monitoreo se deben repetir para cada equipo e interfaces a monitorear. Para el caso de estudio se agrega al monitoreo los equipos de backbone y las agencias mostradas en la *Ilustración 4-5*.

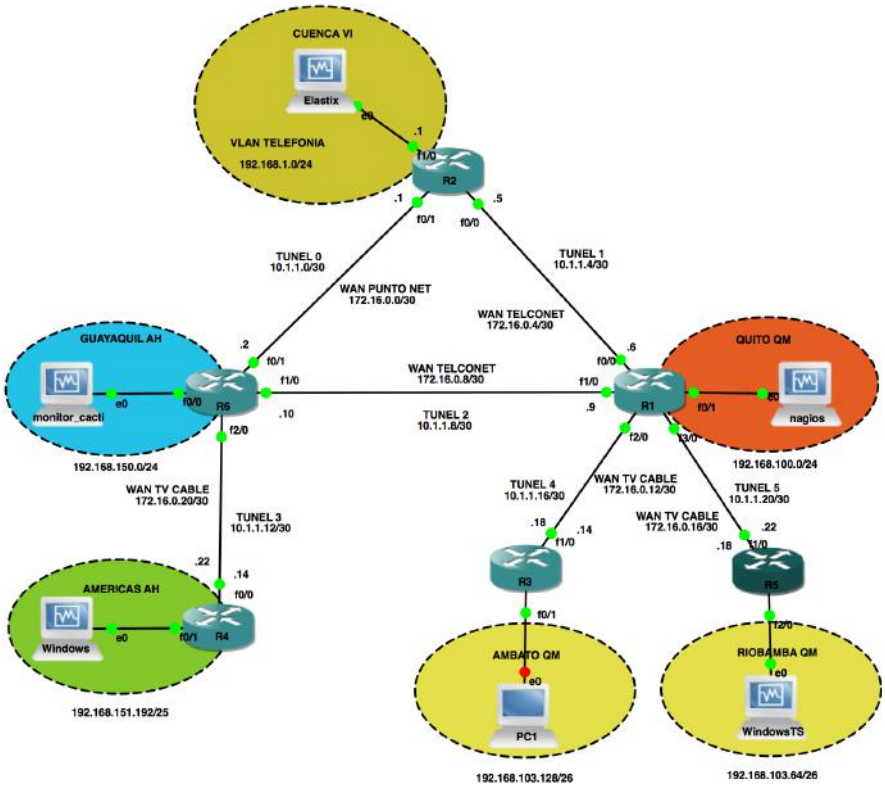


Ilustración 4-5 Topología de Simulación Cacti

En la *Ilustración 4-6* se observa el árbol de monitoreo con las estadísticas de tráfico de cada interfaz de los equipos configurados en el Cacti. Las interfaces que nos interesan para el análisis son las correspondientes a los túneles del backbone y agencias.

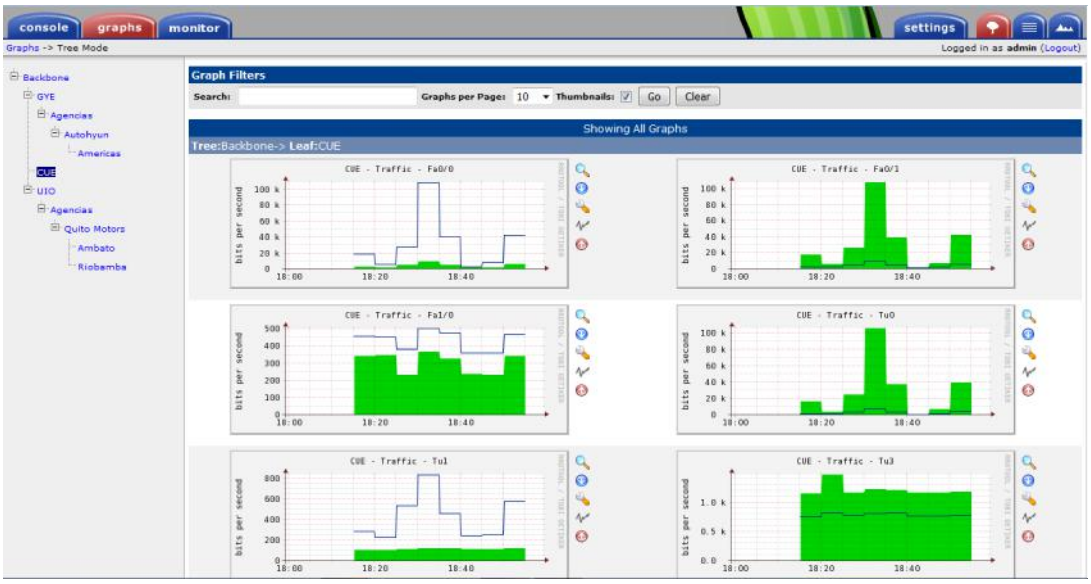


Ilustración 4-6 Cacti Arbol de Monitoreo - Caso de estudio

Para monitorear el estado de los enlaces se agrega el plugin monitor[14]. Una vez activo el plugin aparece una pestaña extra de “Monitor” en la cuál se observa el estado de los equipos con respecto al Cacti. En verde se encuentran los equipos activos y en rojo los inactivos o inalcanzables por el Cacti. Pulsando sobre cada equipo se muestra una estadística del estado del equipo.

Este plugin presenta datos muy útiles para una visión rápida del estado de la red. Entre los datos que proporciona esta herramienta está el estado del equipo (up/down), promedio de tiempo de ping (average time), promedio de disponibilidad (availability) y última caída. Estos datos permiten un monitoreo de primer nivel, no se requieren conocimiento avanzados de la topología de la red o de networking para verificar el estado en una agencia. Con respecto al caso de estudio, la facilidades que presenta Cacti van de acuerdo con los objetivos de la empresa, ya que no se requiere personal especializado para soporte de primer nivel.

Ilustración 4-7 Cacti Plugin Monitor

4.1.2 Implementación Nagios XI [14]

Nagios a diferencia de Cacti tiene una herramienta especializada en análisis de tráfico “Nagios Network Analyzer” en una versión de pago. Nagios ofrece también la versión Nagios XI para empresas con una interfaz de configuración mas amigable que Nagios Core y mejores herramientas que Nagios Network Analyzer. La herramienta cuenta con soporte únicamente para las distribuciones Centos 6 y 7. Para el caso de estudio se instalará el Nagios XI en un servidor virtualizado con sistema

[14] Documentación Cacti Plugins http://docs.cacti.net/plugins

operativo Centos 6.0. De igual manera que Cacti, la máquina virtual de "nagios_monitor" se agrega a la topología de red por medio de la plataforma GNS3.

Para su instalación básicamente se requieren descargar el paquete de instalación de Nagios XI sobre la plataforma Linux Centos con una instalación mínima[15]. Una vez descomprimido el paquete se auto configura el script de instalación y descarga las dependencias faltantes del Nagios XI.

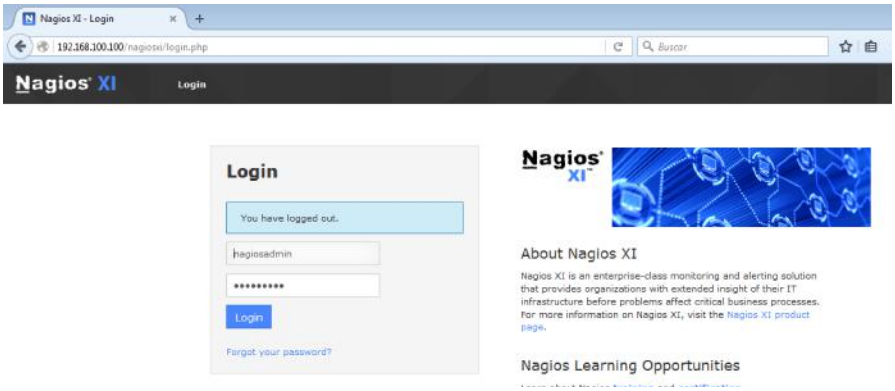


Ilustración 4-8 Nagios XI

Una vez configurado el equipo, se ingresa de manera web como se indica en la *Ilustración 4-8.* Los pasos para comenzar a monitorear los equipos con Nagios XI son los siguientes:

- Agregar hosts (Configure → Configuration Wizards → SNMP Network Monitor)

La topología propuesta, *Ilustración 4-5*, tiene activo el protocolo snmp en cada equipo. Nagios XI presenta una configuración amigable para agregar hosts por medio del protocolo snmp. Se activa el wizard para agregar los hosts. Se requieren las direcciones IP y nombre de la comunidad para el descubrimiento de los equipos.

[15] Documentación de Instalación Nagios XI https://library.nagios.com/library/products/nagiosxi/documentation/252-manual-installation-instructions-for-nagios-xi

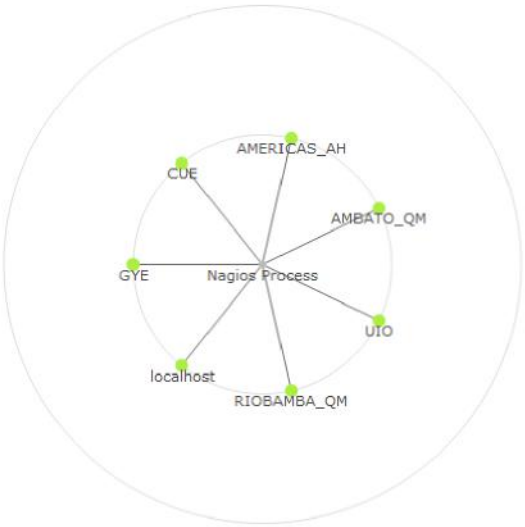


Ilustración 4-9 Interfaz Nagios XI

La *Ilustración 4-9* muestra los equipos activos en el Nagios XI[15]. Cabe indicar que el monitoreo a través del snmp incluye varios servicios como el uptime del equipo, consumo de las interfaces, monitoreo del estado de las interfaces, entre otros.

Host	Status	Duration	Attempt	Last Check	Status Information
AMBATO_QM	Up	30m 35s	1/2	2016-07-14 12:38:26	OK - 192.168.103.129: rta 409.559ms, lost 0%
AMERICAS_AH	Up	32m 31s	1/2	2016-07-14 12:38:21	OK - 192.168.151.193: rta 48.491ms, lost 0%
CUE	Up	36m 19s	1/2	2016-07-14 12:38:50	OK - 192.168.1.1: rta 28.751ms, lost 0%
GYE	Up	34m 35s	1/2	2016-07-14 12:38:24	OK - 192.168.150.1: rta 22.774ms, lost 0%
localhost	Up	17h 20m 38s	1/10	2016-07-14 12:37:26	OK - 127.0.0.1: rta 0.013ms, lost 0%
RIOBAMBA_QM	Up	28m 38s	1/2	2016-07-14 12:38:52	OK - 192.168.103.65: rta 65.673ms, lost 0%
UIO	Up	20m 13s	1/2	2016-07-14 12:37:57	OK - 192.168.100.1: rta 10.972ms, lost 0%

Ilustración 4-10 Nagios XI Interfaces Status

En la *Ilustración 4-10* se muestra el monitoreo del estado (up) de cada equipo de la topología. Adicional a este monitoreo, Nagios por medio de snmp proporciona el monitoreo del estado de cada interfaz de los routers. Esta herramienta se utilizará durante este capítulo para verificar las configuraciones, en especial la tolerancia a fallos y enrutamiento dinámico.

4.2 Enrutamiento Dinámico / Tolerancia a Fallos

Con ayuda de los monitores se verifica las configuraciones propuestas para la tolerancia a fallos y el enrutamiento dinámico. Se plantea el siguiente escenario 1 de pruebas:

Escenario 1: Mantener conexiones activas desde las sucursales hacia el data center en la ciudad de Cuenca. Se utilizan varios servicios del data center y servicios entre las agencias GYE – UIO. La *Tabla 4-1* muestra las conexiones que se mantienen activas. Se analiza el impacto sobre los servicios al simular la caída de uno de los enlaces del backbone. Enlace a verificar CUE - UIO.

Servicios	Client	Agencia	Servidor	Destino	ENLACE
SSH (AS400)	Windows TS	Riobamba QM	Elastix	Data Center	UIO-CUE
Telefonía IP (Elastix)	Windows/ WindowsTS	Riobamba QM/ Américas AH	Elastix	Data Center	UIO-CUE
Escritorio Remoto	Windows	Américas AH	WindowsTS	Ambato QM	UIO-GYE
FTP	Windows	Riobamba QM	WindowsTS	Américas AH	UIO-GYE
Ping	PC1	Ambato QM	Elastix	Data Center	UIO-CUE

Tabla 4-1 Servicios Activos del Escenario

Enlace CUE - UIO: Para simular la caída del enlace CUE – UIO se desactiva la interfaz WAN del equipo R2 ubicado en la ciudad de Cuenca.

Por medio de la herramienta SolarWinds - NetFlow RealTime, analizamos el tráfico que se encuentra activo en el Túnel 5 del router R2 de Cuenca. En la *Ilustración 4-11* observamos tráfico HTTPS, http, TELNET, SSH, SIP, ICMP, SNMP, entre otros. El tráfico descrito se encuentra utilizando el enlace CUE-UIO.

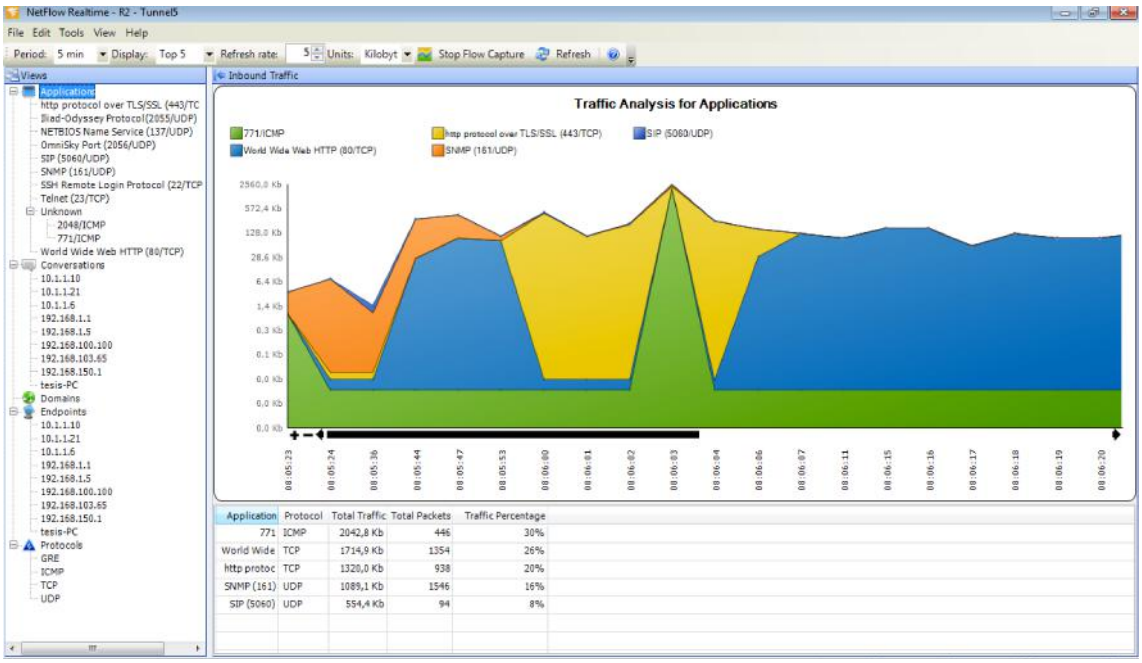


Ilustración 4-11 Tráfico NetFlow

Se procede a desactivar la interfaz WAN del Router R2 de la ciudad de Cuenca para simular la caída del enlace CUE – UIO, *Ilustración 4-12*. Se verifica que al bajar la interfaz WAN, la interfaz TUNEL 1 también se desactiva, ya que esta se configura en base a la interfaz WAN. El tiempo de reacción de la Interfaz TUNEL 1 depende el parámetro keepalive [3]. Al ser menor el tiempo del parámetro Keepalive el router actualiza mas rápido el estado de enlace del túnel, a costa de generas mas tráfico en el enlace. Los resultados mostrados en la *Tabla 4-2* tiene como referencia un valor de keepalive = 5.

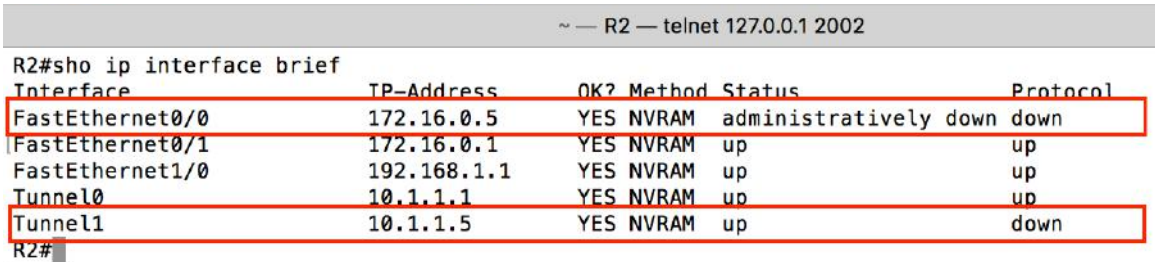


Ilustración 4-12 Interfaz Túnel 1 Down

El monitor Cacti, *Ilustración 4-13*, muestra que la interfaz túnel 1 del router R2 de Cuenca ya no genera tráfico desde las 20:35 minutos. Cacti por defecto no presenta alertas por la caída de la interfaz Túnel 1. Para activar las notificaciones y alertas se requiere la instalación de un plugin extra.

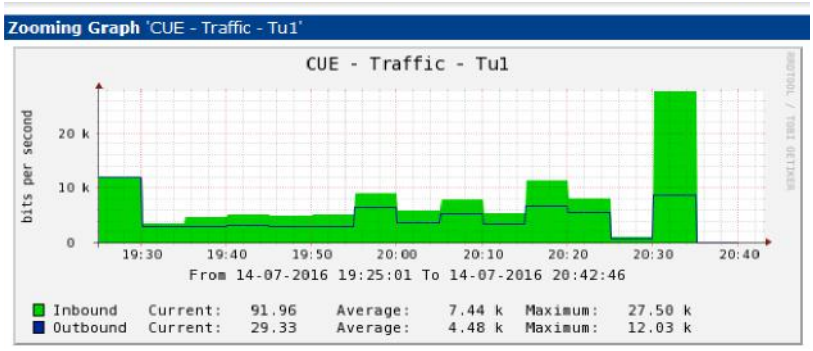


Ilustración 4-13 Monitor Túnel 1 R2 Cacti

Con el monitor Nagios se obtiene una mejor respuesta al incidente, ya que se emite una alerta crítica de interfaz caída. Nagios al igual que Cacti proporciona el tráfico promedio consumido por la interfaz, pero para pruebas fail-over, resulta mas efectivo el monitoreo por estado de enlace.

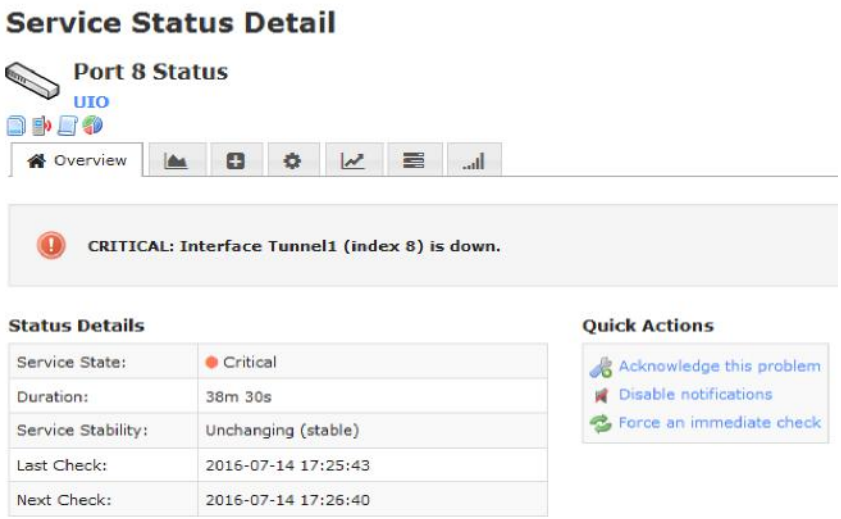


Ilustración 4-14 Monitor Nagios Túnel 1 Alerta

El monitor Nagios XI presenta una mejor interfaz de alertas comparado con el Cacti. Este último muestra el consumo de tráfico de las interfaces, pero por defecto no emite alertas ante la caída de alguna interfaz. El monitoreo de estado de enlace se puede implementar en Cacti, pero requiere la instalación de plugins extras.

Luego de la convergencia del enrutamiento dinámico OSPF, se constata que los servicios siguen activos, por el enlace UIO – GYE y GYE – CUE. La *Ilustración 4-15* muestra el cambio de ruta debido a la caída del enlace principal CUE-UIO. Al hacer una traza desde el host WindowsTS ubicado en la agencias Riobamba QM se observa la nueva ruta de los paquetes. En el idle state con el enlace CUE-UIO activo, se verifican 3 saltos que corresponden a R5 - R1 - R2, siendo Riobamba → Quito → Cuenca respectivamente, *Ilustración 4-15 1*. Al dar de baja la interfaz WAN, se observa en la *Ilustración 4-15 2* la nueva ruta de los paquetes, R5 – R1 – R6 – R2, siendo Riobamba → Guayaquil → Cuenca.

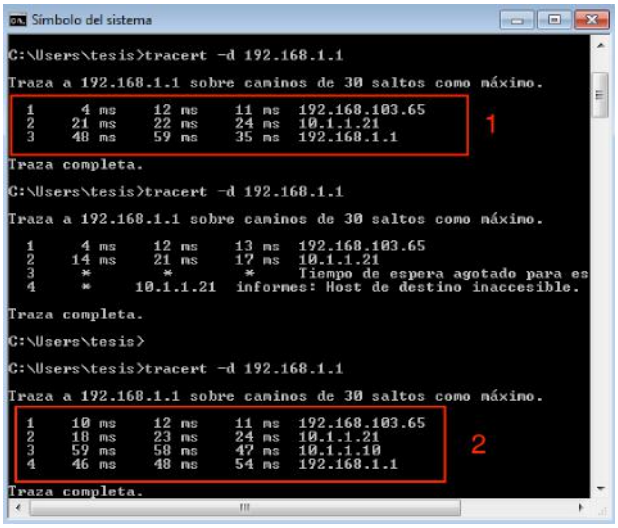


Ilustración 4-15 Traza - Tolerancia a Fallos/Enrutamiento Dinámico

De igual manera se verifica la tabla de enrutamiento del router R1, *Ilustración 4-16*. Se observa los cambios en el enrutamiento de la red 192.168.1.0/24 de la ciudad de Cuenca. Al no tener activo el Túnel 1 el tráfico con dirección a la red del data center de Cuenca 192.168.1.0/24 se re enruta el tráfico por el Túnel 2 hacia Guayaquil. A su vez el router R6 en Guayaquil enruta el tráfico a Cuenca por el Túnel 0.

Debido al tiempo de convergencia del protocolo OSPF y al parámetro de chequeo de estado de enlace keepalive de los túneles GRE, se obtiene un tiempo de caída de la red igual a **5 segundos**. Cabe indicar que este tiempo se calcula en base a la carga y la reacción de los equipos en el simulador GNS3. Con este tiempo de caída de la red, los servicios se ven afectados en cierta medida. La *Tabla 4-2* resume los efectos en algunos servicios.

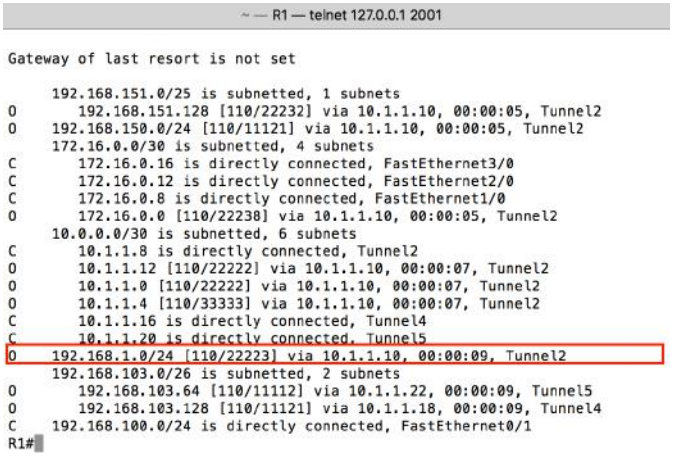


Ilustración 4-15 Tabla de Enrutamiento Router R1 Quito

Hay que tener en cuenta que los efectos mostrados en la *Tabla 4-2* se producen únicamente cuando existe una caída del enlace y se requiere una nueva convergencia de la topología de red. El tiempo de convergencia del backbone con OSPF es de 5 segundos. En promedio se obtiene como resultado un impacto MEDIO (Perceptible al usuario) en los aplicativos de la red.

Servicios	Delay	Status	Impacto
SSH (AS400)	5s	Continúa Activo	Nulo
Telefonía IP (Elastix)	5s	Llamada con voz entrecortada	Medio
Escritorio Remoto	5s	Pérdida de la conexión (reconexión automática)	Medio
FTP	5s	Pérdida de la conexión	Alto
Ping	5s	Pérdida de 7 paquetes	Medio

Tabla 4-2 Impacto en los servicios – Tiempo de convergencia OSPF / Keepalive Túneles GRE

La tolerancia a fallos se basa en el diseño del backbone, al tener una topología tipo anillo, el tráfico se puede re enrutar ante la caída de cualquier tramo que comprenda el anillo. Las agencias terminales conectadas a cada extremo del anillo, son re enrutadas automáticamente a través de protocolo OSPF. Como se revisó en el capítulo anterior, OSPF presenta un mejor rendimiento y tiempo de convergencia que RIPv2, sin embargo, el tiempo de actualización de las tablas de enrutamiento, sumado al tiempo del keepalive de los túneles GRE, tiene un impacto que resulta perceptible al usuario final.

4.3 Balanceo de carga

El balanceo de la carga en la topología del caso de estudio, se basa en la métricas de los enlaces. A diferencia de RIP, donde la métrica del enlace está determinada por el numero de saltos hasta llegar al destino, en OSPF, la métrica del enlace viene determinada por parámetros adicionales como el ancho de banda de los enlaces.

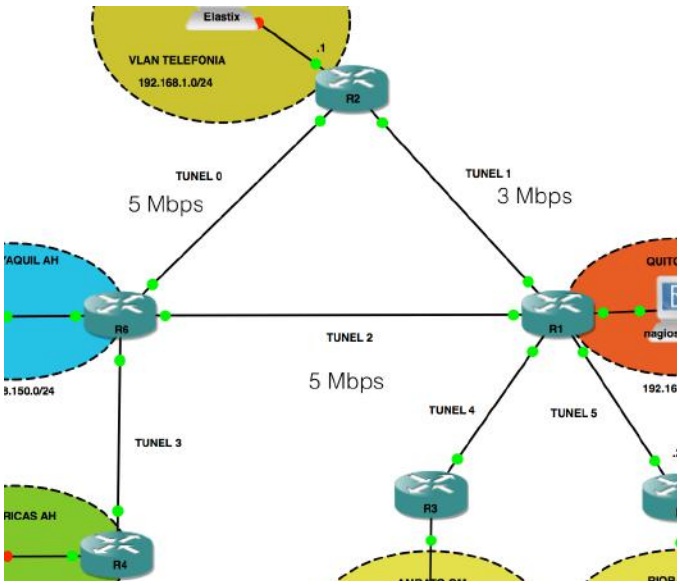


Ilustración 4-16 Ancho de banda Enlaces - Métrica OSPF

Como ejemplo la Ilustración 4-16 muestra un ancho de banda definido para cada enlace, lo cuál muestra que para ir de R1 a R2, la ruta mas corta en términos de ancho de banda, no corresponde al enlace directo entre los equipos, ya que este enlace es de 3 Mbps. La ruta más corta corresponde a R1 – R6 – R2, ya que estos enlaces tienen un ancho de banda de 5 Mbps. En el Capítulo 3 se determinó una ancho de banda superior a 6 Mbps para los enlaces troncales (backbone) del caso de estudio. Sin embargo en la práctica, por temas económicos o de factibilidad por para parte de los proveedores de enlaces, puede darse un caso similar al ejemplo, por lo cuál es importante tener en cuenta la las métricas que tienen los enlaces.

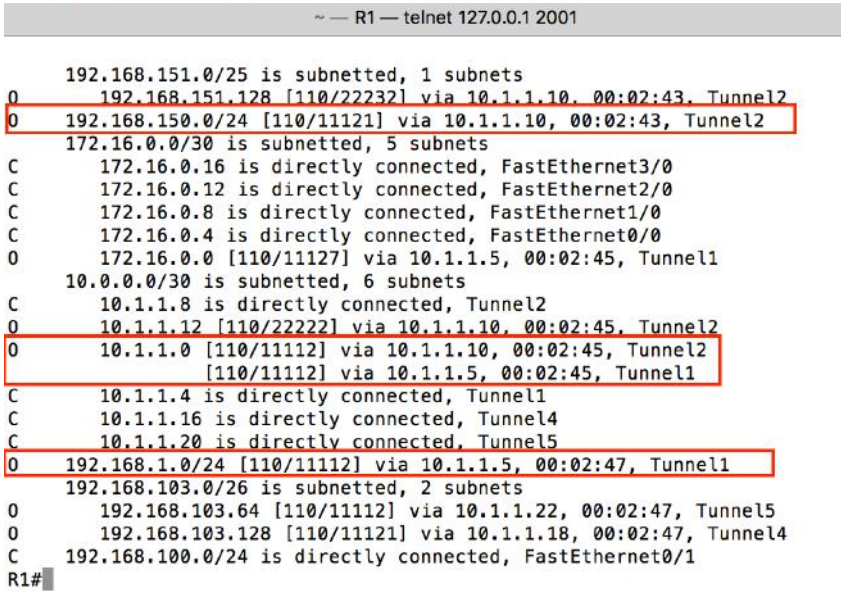


Ilustración 4-17 Tabla de Enrutamiento R1 - Balanceo de Carga

En la *Ilustración 4-17* se observa las rutas hacia la red 192.168.1.0/24 del data center en Cuenca, 192.168.150.0/24 Agencia Guayaquil y 10.1.1.0/30 Red del Túnel 3 enlace CUE-GYE. En el primer caso, la ruta hacia la red 192.168.1.0/24 tiene como siguiente salto la interfaz Túnel 1 correspondiente al enlace UIO – GYE, mientras que el Gateway a la red 192.168.150.0/24 de Guayaquil es la interfaz Túnel 2. Por otra parte, el siguiente salto para llegar a la red del Túnel 3 correspondiente al enlace CUE – GYE, presenta 2 gateways Túnel 1 y Túnel 2, esto debido a que los enlaces están debidamente balanceados con anchos de banda simétricos y por tanto las métricas de las rutas OSPF toman en cuenta la métrica de distancia al destino.

La topología de red propuesta, optimiza los recursos (enlaces), balanceando la carga entre los diferentes enlaces del anillo que componen el backbone.

4.4 Calidad de Servicio QoS para VoIP

Para el análisis de la simulación de QoS, se revisan las configuraciones del router R5 correspondiente a la agencia Riobamba QM. De manera general, las configuraciones de la topología siguen el mismo esquema de configuración en todos los routers. Se definen la clasificación, marcaje y políticas, comentadas en el Capítulo 3. La *Ilustración 4-18* muestra las clasificación de los paquetes o mapas de clase de entrada y salida. El mapa de política de entrada "QoS-in", define la marcación de los paquetes usando el campo dscp, para luego definir la política de servicio y aplicarlo a la interfaz correspondiente y habilitar el encolamiento CBWFQ. El mapa de política de Salida "QoS-out" define las políticas de control de ancho de banda.

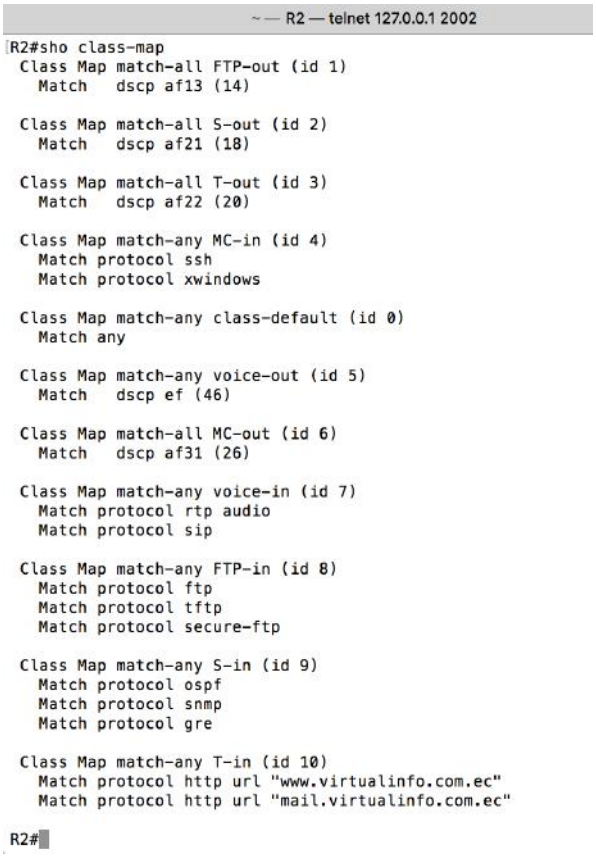


Ilustración 4-18 Class Maps - R5

Como se observa en la *Ilustración 4-18* la clasificación y filtrado de tráfico se basa en class-maps. Adicional al mapeo por clase, se puede utilizar ACLs. Para el caso de estudio se utilizan class-maps con la herramienta de cisco NBAR (**Network Based Application Recognition**).

La *Ilustración 4-19*, muestra los mapas de políticas configurados en el router R5, tanto de entrada como de salida, aplicados a las interfaces Fastethernet 2/0 y Fastethernet 1/0, respectivamente. En la política de salida, la configuración de la clase de voz incluye el comando “Priority percent”. Este comando, a más de garantizar un porcentaje del ancho de banda disponible, provee baja latencia propia para el tráfico de voz.

```
~ — R2 — telnet 127.0.0.1 2002
R2#sho policy-map
  Policy Map QoS-out
    Class voice-out
      Strict Priority
      Bandwidth 14 (%)
    Class MC-out
      Bandwidth remaining 29 (%) Max Threshold 64 (packets)
    Class S-out
      Bandwidth remaining 6 (%) Max Threshold 64 (packets)
    Class T-out
      Bandwidth remaining 20 (%) Max Threshold 64 (packets)
    Class FTP-out
      Bandwidth remaining 17 (%) Max Threshold 64 (packets)
    Class class-default
      Flow based Fair Queueing
      Bandwidth 0 (kbps) Max Threshold 64 (packets)
  Policy Map QoS-in
    Class voice-in
      set dscp ef
    Class MC-in
      set dscp af31
    Class S-in
      set dscp af21
    Class T-in
      set dscp af22
    Class FTP-in
      set dscp af13
R2#
```

Ilustración 4-19 Policy Map – R2

Para realizar las pruebas del sistema se propone el Escenario 2:

- **Escenario 2:** Se realiza una llamada desde el host WindowsTS Ext. 1004 hacia el host Windows Ext. 1003, *Ilustración 4-20*. Con ayuda del Cacti y su función de monitoreo en tiempo real se verifica la generación de tráfico en el router R5 de la agencia Riobamba QM.

Ilustración 4-20 Llamada Softphone

Se verifica el tráfico de VoIP en la interfaz Fastethernet 2/0 de R2 con un consumo promedio de 80kbps. El monitor muestra un promedio de los últimos 10 segundos, *Ilustración 4-21*.

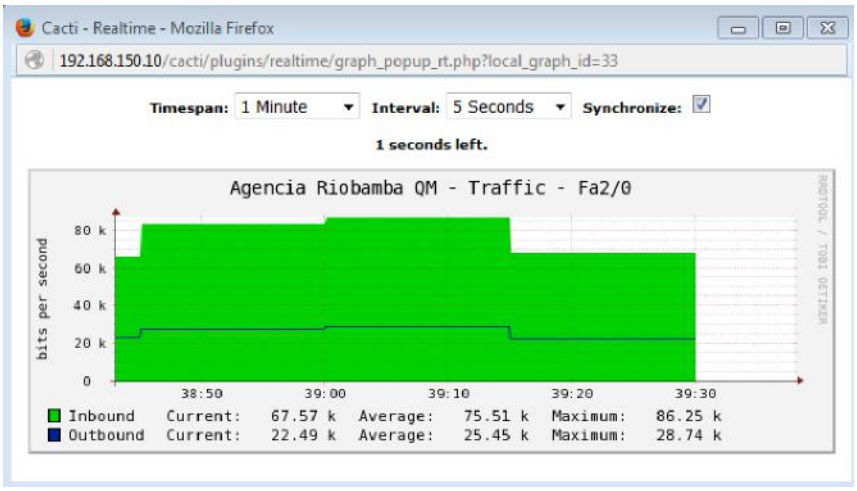


Ilustración 4-21 Tráfico VoIP 80 kbps

El monitor Nagios presenta una medición de tráfico similar, por lo cuál para las pruebas se puede utilizar cualquiera de las dos herramientas. Adicional se configura la herramienta de monitoreo Netflow de Solarwinds. Con esta última herramienta, se verifica el tráfico, por protocolo, constatando todo el tráfico generado en la simulación, para luego contrastar con la clasificación y marcaje de paquetes en los mapas de políticas de los routers. En a *Ilustración 4-22*, se observa el tráfico correspondiente a la interfaz Tunnel 1 del router R2, enlace Cuenca – Quito. Se tiene diferente tipos de tráfico como SSH, FTP, OmniSky (monitor), SIP, entre otros. Cabe indicar que el tráfico mostrado corresponde a un promedio de 5 minutos, por lo cuál se usa solo como referencia para verificar el tráfico circulando a través de la interfaz Tunnel 1 en un momento determinado.

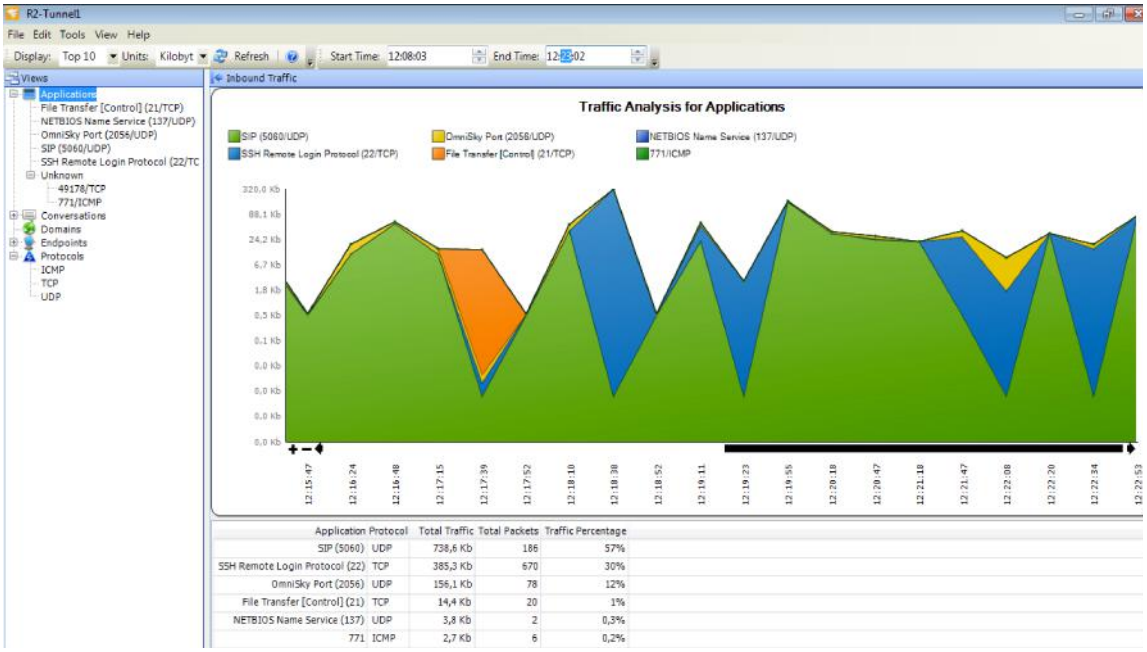


Ilustración 4-22 Netflow Solarwinds

Para el análisis se verifica el policy-map QoS-in aplicado a la interfaz Fa1/0 del router R2 (equipo más próximo a la fuente). En la *Ilustración 4-23*, se observa que los paquetes de voz son clasificados y marcados con un DSCP 46, correspondiente a un EF-express forwarding, de acuerdo a lo revisado en el *Capítulo 3*. Se verifica además la clasificación y marcaje de los paquetes:

- SIP, establecimiento y control de la llamada, class-map voice-in.
- RTP, transmisión de los paquetes de voz, class-map voice-in.
- SSH, simula la consola del AS400 - caso de estudio, class-map MC-in (Mission Critical-input).
- OSPF, GRE[16], SNMP, tráfico correspondiente al enrutamiento, tunelización y monitoreo, class-map S-in [17], (Signaling-input).
- URL, www.virtualinfo.com.ec/mail.virtualinfo.com.ec, correspondiente a páginas de uso interno del caso de estudio. Debido a que el entorno de simulación GNS3 no cuenta con salida a internet, no se verifica tráfico en este class-map T-in (Transactional-input).

- FTP, tráfico correspondiente a respado de archivos – caso de estudio. Class-map FTP-in.

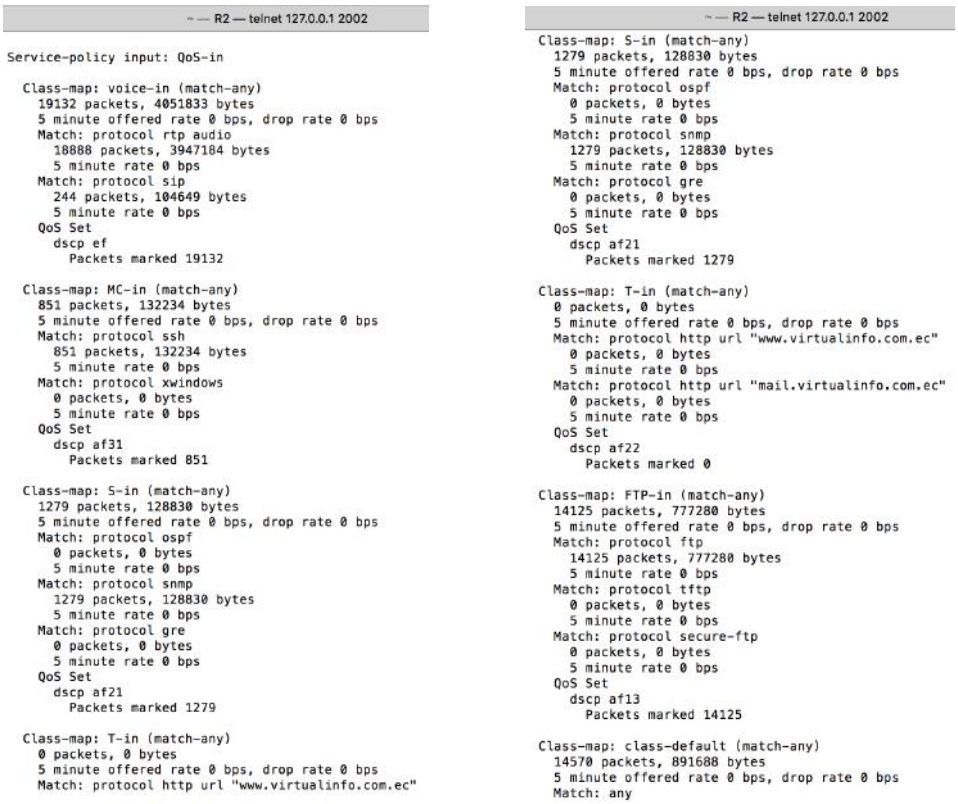


Ilustración 4-23 Policy Map Interface Input R2

De igual manera, se verifica el tráfico filtrado por el mapa de políticas de salida “QoS-out” aplicada a la interfaz Fastethernet 2/0 del Router R2. En esta instancia se aplica las políticas de control de ancho de banda y manejo de tráfico (baja latencia). La *Ilustración 4-24* muestra los paquetes filtrados en cada clase.

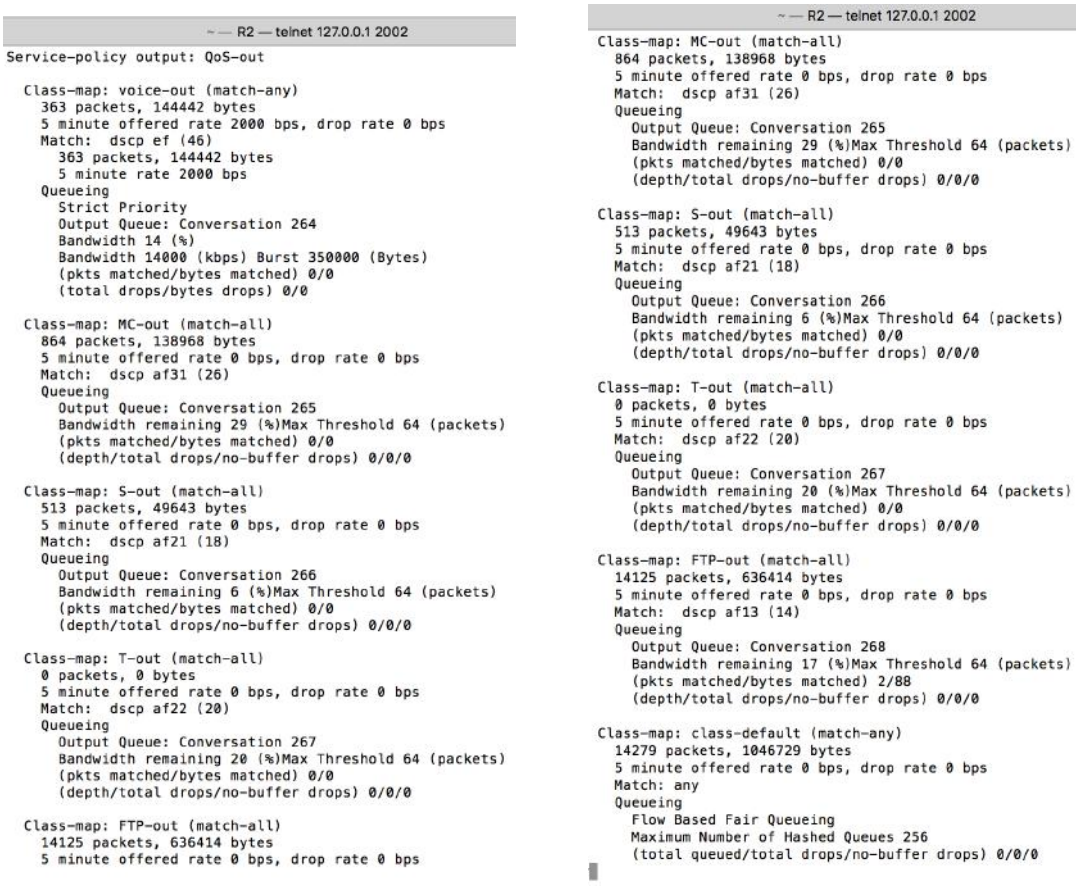


Ilustración 4-24 Policy Map Interface Output R2

Se verifica que el tráfico está siendo clasificado, marcado y filtrado, según las políticas establecidas en el Capítulo 3. Es importante configurar el ancho de banda contratado en la interfaz correspondiente, ya que las políticas de QoS se basan en este parámetro para la distribución del ancho de banda.

4.5 Seguridad de la Infraestructura

Al analizar las vulnerabilidades de red, se debe clasificar como un servicio a brindarse por el departamento de TI, cuyo objetivo debe ser garantizar el tratamiento y solución de vulnerabilidades de las infraestructuras de red y hasta cierto nivel de los aplicativos, con el fin de reducir al mínimo los niveles de riesgo.

Adicional a la seguridad de acceso al data center, considerado como seguridad física o de capa 1, se deben tomar encuenta las capas 2 y 3 de TCP/IP, para lo cuál se desarrollan ciertas recomendaciones de seguridad en la red. Se detallan también cirtas recomendaciones a nivel de capa 7 para un análisis rápido de vulnerabilidades en los aplicativos.

4.5.1 Capa 1

A nivel físico, se recomienda la instalación de controles de acceso al data center. Para el caso de estudio, el data center se ubica en la ciudad de Cuenca, en un edificio privado, pero con afluencia de personas, por lo cual es vulnerable a un ataque a nivel físico.

Actualmente el mercado presenta un gran numero de soluciones de controles de acceso. Para analizar cuál es recomendable o menos vulnerable, se toma encuentra los métodos de autenticación de los equipos. De manera general los equipos basan sus métodos de autenticación en:

- Algo que se conoce. Por ejemplo una clave, número ó palabras.
- Algo que se tiene. Por ejemplo una tarjeta de acceso.
- Algo que se es. Por ejemplo, hulla digital ó retina del ojo.

De estos 3 métodos de autenticación, el menos vulnerable es el “Algo que se es” aplicado en sistemas biométricos. Se consideran seguros a los sistemas biométricos por:

- Más seguros que claves, vulnerables a ataques. Por lo general las personas usan claves realacionadas con datos que pueden recordar, como fechas de nacimiento.

- Más seguros que tarjetas o tags de acceso. La mayoría de controles de acceso utilizan los tags Mifare Classic.[16]
- Sistemas biométricos difíciles de reemplazar o copiar. Autenticación por huellas dactilares, palma de la mano, iris del ojo, etc.

De entre los sistemas biométrico se recomienda el uso de un sistema biométrico lector de hullas digitales, costo – beneficio. El parámetro EER (Equal Error Rate), tasa de error y acierto se sitúa en un 5%. [17]

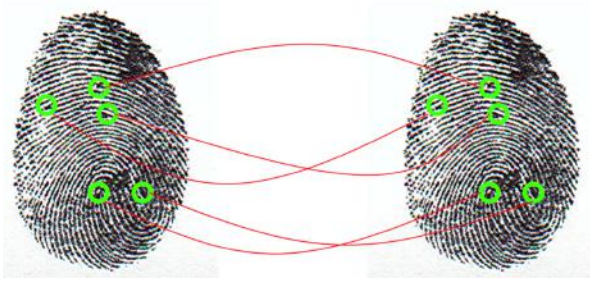


Ilustración 4-25 Huellas Digitales o Fingerprint EER=5%

4.5.2 Capa 2

A nivel de enlace de datos, se presentan ciertas vulnerabilidades localizadas principalmente en los switches de acceso y Access points. Los principales ataques que se presentan en este nivel son:

- Hombre en el medio – Men in the middle
- Espionaje de datos – Eavesdropping
- Falsificación de MAC address

[16] Ejemplo de Ataque a Mifare Classic - http://arxiv.org/abs/0803.2285
[17] ERR Tasa de error y acierto White Paper - http://www.aware.com/what-are-biometrics/

Para reducir el impacto de estos ataques, se plantean las siguientes recomendaciones.

- Configuración de portsecurity en las interfaces de los switchces de acceso. Esta configuración se basa en la MAC de los dispositivos que se conectarán en un determinado puerto del switch. No elimina totalmente los ataques, pero presenta una dificultad extra de acceso. Para el caso de estudio se recomienda en espacial la configiración de portsecurity en el switch de los servidores.

- Entre las recomendaciones de seguridad para la red Wifi, se especifica mantener actualizados los firmware de los access points, para evitar bugs propios de la casa fabricante. Adicional resulta imperativo migrar cualquier configuración con seguridad WEP a WAP2 con una contraseña cuyos caracteres no tengan relación alguna con datos de la empresa o personales. Un nivel de seguridad superior sugiera la implementación de autenticación por medio de un servidor RADIUS.
- Se recomienda el uso de la herramienta aircrak[18], para verificar la seguridad de los Access points. Esta herramienta se puede instalar como paquete unitario o pre instalada en la distribución de Kali Linux[19].

4.5.3 Capa 3

A nivel de red es importante tener encuentra los túneles públicos que se puedan configurar. En el caso de estudio, se plantea conexiones con otros países a través de internet, para lo cuál se recomienda el uso de VPN (virtual private networks) usando el protocolo IPsec, que a diferencia de otros protocolos punto a punto o punto multipunto, IPsec ofrece un mecanismo de autenticación y encriptación combinado. En el caso de estudio, los túneles GRE, al no ser de acceso público, basan su

[18] Herramienta de Monitoreo de seguridad Wifi - https://www.aircrack-ng.org/

[19] Herramienta de escaneo de vulnerabilidades https://www.kali.org/

seguridad en los mecanismos de capas inferiores, sin embargo existe la posibilidad de configurar GRE sobre IPsec para brindar seguridad a los túneles GRE.

Layer	Protocol
Transport	SSL/TLS
Network	IPSec
Link	L2TP ,PPTP (microsoft)

Ilustración 4-26 VPN - Protocolos de Seguridad Capas de Red

Una de las herramientas en capa 3 para verificar vulnetabilidades es nmap, que puede ser instalado como un paquete extra en las distribuciones linux y que viene por defecto en la distribución kali. Nmap o network mapper, permite descubrir hosts en la red y los puerto que estan escuchando en los equipos. Estos parámetros brindan información al atacante para establecer un plan de ataque basado en los servicios que están activos (Puertos por defecto).

```
~ — -bash
HP-desktop:~ Pablo$ nmap localhost

Starting Nmap 6.47 ( http://nmap.org ) at 2016-07-19 17:09 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00061s latency).
Not shown: 966 closed ports, 27 filtered ports
PORT     STATE SERVICE
631/tcp  open  ipp
2001/tcp open  dc
2002/tcp open  globe
2005/tcp open  deslogin
2006/tcp open  invokator
8000/tcp open  http-alt
9090/tcp open  zeus-admin

Nmap done: 1 IP address (1 host up) scanned in 5.92 seconds
```

Ilustración 4-27 Herramienta NMAP

Para el análisis de la capa de aplicación, se presentan muchas herramientas útiles como “John The Ripper” que facilita la exploración de contraseñas débiles en entornos como Elastix y sus contraseñas de las extensiones. Esta herramienta es utilizada para ataques de fuerza bruta a través de un diccionario de palabras para descifrar claves, sin embargo para es útil también para verificar seguridades de contraseñas de un entorno corporativo.

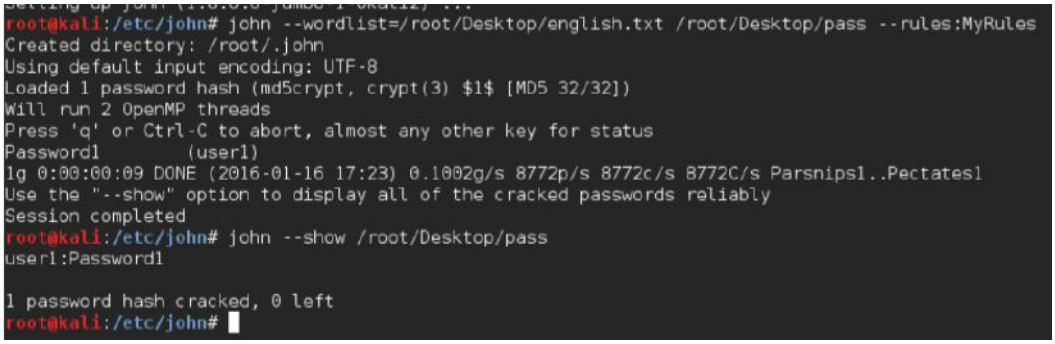


Ilustración 4-28 John The Ripper - Ataques de Fuerza Bruta

Otra de las herramientas para verificar las vulnerabilidades en la capa de aplicación es NIKTO, que se basa en vulnerabilidades bien conocidas y reportadas de servidores web. En el caso de estudio se cuenta con servidores Web para manejo de la página de talleres y correo corporativo. Está fuera del alcance de este trabajo monográfico el análisis de vulnerabilidades web.

Ilustración 4-29 NIKTO escáner de vulnerabilidades en Servidores Web

la Ilustración 4-30, muestra la herramienta sqlmap, que se usa para realizar ataques a bases de datos. En el caso de estudio, se puede usar la herramienta para realizar un hacking ético para verificar errores de configuración o vulnerabilidades existentes.

```
root@kali:~# sqlmap -u http://www.colinst.com/brief.php?id=61 -a
        _
 ___ ___| |_____ ___ ___  {1.0-stable}
|_ -| . | |     | .'| . |
|___|_  |_|_|_|_|__,|  _|
      |_|           |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not
responsible for any misuse or damage caused by this program

[*] starting at 02:29:02

[02:29:02] [INFO] resuming back-end DBMS 'mysql'
[02:29:02] [INFO] testing connection to the target URL
[02:29:03] [INFO] heuristics detected web page charset 'ISO-8859-2'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
       Type: boolean-based blind
       Title: AND boolean-based blind - WHERE or HAVING clause
       Payload: id=61 AND 9735=9735

       Type: error-based
       Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
clause
       Payload: id=61 AND (SELECT 7476 FROM(SELECT
COUNT(*),CONCAT(0x7170717a71,(SELECT
(ELT(7476=7476,1))),0x716a627a71,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)
```

Ilustración 4-30 SQLmap - SQL injection

Capítulo 5 : CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

El presente trabajo monográfico, brinda una amplia visión de los aspéctos técnicos del diseño una red LAN y WAN. Las configuraciones presentadas en el trabajo, se orientan a un caso de estudio, sin embargo el análisis es genérico, y explica de manera general las características del diseño. Luego de proponer el diseño para el caso de estudio se concluye:

- Se identifica los requerimientos para los diferentes tipos de tráfico como Voz IP Éste requiere baja latencia (< 120 ms) y control del jitter a diferencia del tráfico Web que tiene un comportamiento transaccional sin grandes requerimientos de latencia, pero sí de picos de ancho de banda. En base al análisis de los primeros capítulos, se propone el diseño de una topología de red para el caso de estudio “Grupo Automotriz”, el cuál contempa dos etapas, diseño de red para el cuarto de datos ubicado en la ciudad de Cuenca y diseño de red a nivel nacional.

- La configuración de los protocolos VTP, STP y LINK AGREGGATION, brindan al diseño confiabilidad, escalabilidad y disponibilidad. En el Capítulo 3 las configuraciones y simulaciones se aplican al cuarto de datos del caso de estudio.

- El diseño de la topología de red WAN incorpora las configuraciones necesarias para la implementación de túneles GRE. La propuesta toma encuentra párametros como la longitud del encabezado GRE (4 bytes) dentro del proceso de encapsulación, para tener un MTU consistente a lo largo de los diferentes enlaces y evitar la framentación de paquetes que incoorpora carga adicional a la red. Se desarrollan configurarciones paso a paso de los túneles GRE en equipos Cisco y Mikrotik, siendo estas las

principales marcas de los equipos con los que se cuenta en el caso de estudio.

- Para el diseño de la topología de red WAN a nivel nacional se incluye un direccionamiento lógico completo, que incluye la segmentación de red de las principale agencias del caso de estudio y el direccionamiento de las interfaces lógicas GRE e interfaces físicas de los equipos que componen el backbone de la red, Cuenca, Quito y Guayaquil, así como tres agencia de ejemplo para el caso de estudio.

- Una vez planteado el diseño y direccionamiento, el trabajo monográfico desarrola la simulación de la topología propuesta, inlcuyendo el enrutamiento dinámico. Se realiza un análisis previo de los IGP para la topología y se verifica la aplicabilidad de EIGRP y OSPF como protocolo de enrutamiento dinámico sobre tuneles GRE. Se concluye que OSPF presenta mejores características sobre EIGRP como su escalabilidad y tiempo de convergencia. Por otra parte EIGRP se determina factible para ser implementado como protocolo dinámico para conexión a internet.

- La implementación de OSPF sobre los túneles GRE en el backbone del diseño, cumple con el principal objetivo del caso de estudio, que determina eliminar la recurrente necesidad de soporte por parte del proveedor de los enlaces, al tener que administrar el enrutamiento de nuevas redes. Las interfaces lógicas GRE simulan una conexión directa entre los equipos del backbone, sobre la cual viajan los paquetes de convergencia del protocolo OSPF. Si una nueva agencia o subred se incoorpora al backbone, las tablas de enrutamiento se actualizan de manera automática sin necesidad de requerir configuraciones extras del proveedor.

- Otro de los beneficios que presenta el diseño de la topología en anillo con OSPF y tunelizado GRE, es la redundancia automática ante caída de enlces. Se analiza la tolerancia a fallos con ayuda del simulador GNS3. Se plantea

un escenario donde se simula la caída de un enlace del backbone. Se verifica que el tiempo de convergencia de OSPF sumado al tiempo de encapsulación de GRE, presentan un retardo de 5s antes de reestablecer las conexiones, produciendo pérdidas de paquetes perceptibles usuario. Luego del tiempo de convergencia, se recuperan las conexiones y se verifica el fail-over.

- Se implementa QoS basado en el concepto de Clases de Tráfico (Diferenciación del Tráfico por clases) y de PHB (per hop behavior). Se definen diferentes políticas para el manejo de tráfico de Voz, misión crítica, señalización, transaccional y el resto de tráfico con un encolamiento CBWFQ y FAIR-QUEUE respectivametne. La clasificación de tráfico basado en los mapas de clase utiliza la herramienta de cisco NBAR para la identificación de protocolos como FTP, SSH, OSPF, GRE, SNMP, entre otros. Para el caso de estudio se ve factible y escalable el uso de NBAR, ya que contiene los principales servicios usados en el Grupo Automotriz.

- Los monitores de red implementados en el entorno de simulación, permiten un ágil monitoreo con estadísticas de tráfico. A diferencia de Nagios, Cacti no implementa por defecto alarmas ante la caída de un enlace. Se requiere la instalación de un plugin extra para configurar alarmas en tiempo real y notificiaciones al correo.

- De los monitores analizados, Nagios presenta un entorno más amigable y estadísticas de nivel gerencial, lo cuál lo hace propicio para la implementación en un entorno real. Adicional Nagios implementa monitoreo por interfaz y no por equipo como lo hace Cacti por defecto. Este último presenta una herramienta de monitoreo en tiempo real, que a diferencia de Nagios, muestra el tráfico promedio con un tiempo configurable de mínimo 5 segundos.

5.2 Recomendaciones

Basado en el trabajo desarrollado y en los resultados obtenidos del simulador GNS3 se plantean las siguientes recomendaciones:

- En la etapa de diseño de una topología de red, se recomienda tener presente aspectos como la disponibilidad, escalabilidad del entorno, nivel de confiabilidad que brindará el esquema de red, costos de la solución, en redes convergentes es importante el parámetro de latencia o delay y el jitter. Todos estos parámetros influyen en un presupuesto de enlace y en un SLA que se brindará al usuario final.

- Para brindar tolerancia a fallos en un red LAN, se recomienda implementar enlaces redundantes entre switches e implementar el protocolo STP, para evitar bucles entre los equipos. De igual manera para brindar cierto grado de escalabilidad se recomienda la implementación del link agreggation a través de la configuración de interfaces portchannel. Para el caso de estudio, se recomienda en un futuro la implementación de enlaces de fibra óptica entre los switches de core y con el case del blade.

- Con respecto a la red WAN, para el caso de estudio, se recomienda tener al menos dos proveedores distintos que brinden el servicio en los enlaces del backbone. Esto con la finalidad de tener redundancia en la topología en anillo. Esta configuración en conjunto con el protocolo dinámico OSPF, brinda una estabilidad y un cierto grado de confiabilidad al diseño de red.

- Los túneles GRE proveeen autonomía del proveedor y un grado de seguridad de los datos que viajan a través del entorno de red del proveedor. Se recomienda una revisión futura para implementar la tunelización GRE sobre IPSec para garantizar la confidencialidad de los datos en la Intranet.

- Se recomienda implementar la redundancia, el enrutamiento dinámico y los monitores de red en conjunto para reducir la carga administrativa del departamento de TI.

- Para la implementación de calidad de servicio en cualquier topología de red, se recomienda aplicar la políticas lo más cerca de la fuente. Se deben definir de manera clara y consistente las políticas para el manejo de tráfico dentro de la empresa, en función de los objetivos del negocio. Para implementar las políticas de calidad de servicios, es importante seguir los pasos recomendados en el presente documento, mapa de clase, mapa de política y política de servicio. Se recomienda además, implementar no mas de 5 mapas de clases, ya que el procesamiento que requieren los equipos para clasificicar, marcar y filtrar los paquetes, podría afectar el rendimiento de la red. Adicional al tener demasiadas mapas de clases, se podrían generar inconsistencias en el manejo del tráfico.

- Se sugiere implementar el software de Monitoreo Nagios. A diferencia de Cacti, Nagios incorpora una reportería detallada. Para el caso de estudio, la reportería brinda las estadísticas necesarias para sugerir cambios y actualizaciones de los enlaces de datos. Una desventaja de Nagios es el tiempo promedio que ultiliza el software para presentar el tráfico (5 min). Se recomienda contrastar las estadísticas de Nagios con un monitoreo en tiempo que ofrece el STG através del protocolo snmp.

- Para cualquier modificación o futura implementación de red, se recomienda el uso del software GNS3 para realizar las pruebas y test necesarios antes de incluir el proceso en un entorno de produción.

- Dentro de un diseño de red, se recomienda tener encuenta aspectos de seguridad de todo el entorno de la infraestructura. Esto comprende un análisis de seguridad de todas las capas del model TCP/IP, desde la capa física hasta

la capa de aplicación con exploits de vulnerabilidades en busca de posibles huecos de seguridad. Se recomienda el uso de la distribución Kali Linux con el fin de realizar un análisis de seguridad del caso de estudio una vez implementado el diseño prupuesto en este trabajo monográfico.

BIBLIOGRAFÍA:

[1] COMEX, Resolución 049-2014, Anexo 1 del Artículo 1, enero 2015.

[2] Cisco, GRE Tunnel Keepalive, 64565, agosto 2005.

[3] RFC 1701, Generic Router Encapsulation (GRE), octubre 1994.

[4] Cisco ASA 5500 Series Configuration Guide using the CLI, Chapter 21 - Configuring OSPF, OL-18970-03, octubre 2013.

[5] Cisco IOS IP Configuration Guide, Release 12.2, Configuring EIGRP febrero 2014.

[6] Cisco ASA Services Module CLI Configuration Guide, Chapter 21 - Defining Route Map, noviembre 2013.

[7] Software de Simulación GNS3, Guia de Instalación, https://community.gns3.com/support/docs/quick-start-guide-for-windows-us, último acceso 19 de julio de 2015.

[8] Cisco Validated Desing, Campus LAN and Wireless LAN Design, Octubre 2105.

[9] Cisco Route-Maps for IP Routing Protocol Redistribution Configuration, 49111, agosto 2005.

[10] 802.1w-2001 - IEEE Standard for Local and Metropolitan Area Networks - Common Specification. Part 3: Media Access Control (MAC) Bridges - Amendment 2: Rapid Reconfiguration, 0-7381-2925-9, 2001.

[11] Ariganello Ariganello, Ernesto / Barrientos Sevilla, Enrique, Redes cisco: guía de estudio para la certificación ccnp routing y switching, 2015.

[12] Cisco IOS Quality of Service Solutions Configuration Guide, NBAR configuracion, enero 2014.

[13] Ian Berry, Tony Roman, Larry Adams, J.P. Pasnak, Jimmy Conner, Reinhard Scheck, Andreas Braun, The Cacti Manual, 2013.

[14] Nagios Guide, https://assets.nagios.com/downloads/nagios-network-analyzer/guides/nna-ag/#_ga=1.76550741.1730386738.1467728328 - último acceso 20 de julio 2016.

[15] Nagios Monitoring Routers and Switches, https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/monitoring-routers.html, último acceso 20 de julio 2016.

[16] Cisco Quality of Service Options on GRE Tunnel Interfaces, 10106, marzo 2015.

[17] Cisco IOS Quality of Service Solutions Configuration Guide, Chapter: Configuring Class-Based Shaping, enero 2014