ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD.

UNIDAD DE GESTIÓN DE POSTGRADOS.

MAESTRÍA EN GESTIÓN DE REDES Y TELECOMUNICACIONES

IV PROMOCIÓN

TESIS DE GRADO MAESTRÍA EN GESTIÓN DE REDES Y TELECOMUNICACIONES.

TEMA: PROYECTO PARA LA REESTRUCTURACIÓN DE LA RED DE DATOS DE FUERZAS ARMADAS, ORIENTADA A LA CONVERGENCIA DE SERVICIOS, MEDIANTE UNA PLATAFORMA MPLS.

AUTOR: CRISTIAN MANRIQUE ARIAS ESPINOSA.

DIRECTOR: ING. MAURICIO CAMPAÑA. MSC.

SANGOLQUÍ, ABRIL 2014.

CERTIFICADO

ING. MAURICIO CAMPAÑA
ING. DANILO CORRAL.

CERTIFICAN

Que el trabajo titulado: "PROYECTO PARA LA REESTRUCTURACIÓN DE LA RED DE DATOS DE FUERZAS ARMADAS, ORIENTADA A LA CONVERGENCIA DE SERVICIOS, MEDIANTE UNA PLATAFORMA MPLS." realizado por CRISTIAN MANRIQUE ARIAS ESPINOSA, ha sido guiado y revisado periódicamente y cumple normas estatuarias establecidas por la ESPE, en el Reglamento de Estudiantes de la Universidad de Fuerzas Armadas ESPE.

ING. MAURICIO CAMPAÑA
DIRECTOR

ING. DANILO CORRAL
OPONENTE.

AUTORÍA DE RESPONSABILIDAD

CRISTIAN MANRIQUE ARIAS ESPINOSA

DECLARO QUE:

El proyecto de grado denominado: PROYECTO PARA LA REESTRUCTURACIÓN DE LA RED DE DATOS DE FUERZAS ARMADAS, ORIENTADA A LA CONVERGENCIA DE SERVICIOS, MEDIANTE UNA PLATAFORMA MPLS.", ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan el pie de las páginas correspondiente, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es mi autoría. En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

_____

CRISTIAN MANRIQUE ARIAS ESPINOSA

AUTORIZACIÓN:

Yo, CRISTIAN MANRIQUE ARIAS ESPINOSA

Autorizo a la Universidad de las Fuerzas Armadas ESPE, la publicación, en la biblioteca virtual de la Institución del trabajo "PROYECTO PARA LA REESTRUCTURACIÓN DE LA RED DE DATOS DE FUERZAS ARMADAS, ORIENTADA A LA CONVERGENCIA DE SERVICIOS, MEDIANTE UNA PLATAFORMA MPLS.", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

_____

CRISTIAN MANRIQUE ARIAS ESPINOSA

DEDICATORIA:

A mi dios por ser mi inspiración divida y permitirme siempre contar con él en todo momento, por darme la fortaleza, fé y la vida para alcanzar mis metas.

A mis padres por su apoyo permanente, sus consejos y por haberme inculcado siempre el deseo de superación en mi vida.

A mi esposa e hijos por su amor, su comprensión, su tiempo y su inspiración que me han permitido culminar con éxito este trabajo.

A toda mi familia por sus consejos y la confianza depositada en mí.

CRISTIAN ARIAS ESPINOSA

AGRADECIMIENTO:

A mi familia por su comprensión y el apoyo recibido en toda mi vida, gracias a uds, he logrado alcanzar mis objetivos, siempre se han constituido en mi inspiración por el amor y gratificación que representan en mi vida.

A la Fuerza Aérea Ecuatoriana, por ser la Institución que me ha permitido crecer como persona y profesional, gracias a esta noble Institución y las personas que lo conforman he podido superarme y hacia la cual entregaré mi conocimiento y esfuerzo para que siga siendo la gran Institución, ejemplo de nuestra nación.

A mis oficiales superiores, subalternos, compañeros militares, ingenieros y personal civil que trabajan en el Departamento de Telecomunicaciones por su confianza, su apoyo y colaboración para culminar con éxito este trabajo.

CRISTIAN ARIAS ESPINOSA

TABLA DE CONTENIDOS:

Contenido

CAPÍTULO 1 1
MARCO CONCEPTUAL. 1
1.1.-Método de diseño de la red. 1
1.1.1.- Criterio a considerar para ubicar los equipos en la red. 3
1.2.- Método de dimensionamiento de la red: 5
1.2.1.-Dimensionamiento con tolerancia a fallas con compartición de enlaces.- 5
1.3.- Tecnología MPLS: 7
1.3.1.- Elementos Básicos de MPLS: 7
1.3.2.- Características de MPLS: 12
1.3.3.- Funcionamiento de la tecnología MPLS: 13
1.4.- Facilidades de la tecnología MPLS: 18
1.4.1.- Virtual private Networks (VPNs) 18
1.4.2.- Ingeniería de Tráfico (TE): 37
1.4.3.- Calidad de Servicio (QoS): 45
1.5.- Conceptos de la Plataforma OPNET: 47
1.5.1.- Modelo de RED: 49
CAPÍTULO 2 54
SITUACIÓN ACTUAL. 54
2.1.-Introducciòn. 54
2.1.1.-Delimitaciòn. 56
2.1.2.-Definiciòn del problema. 56
2.1.3.-Justificaciòn. 58
2.1.4.-Determinación de objetivos. 59
2.2.-Anàlisis de los servicios habilitados en la red. 60
2.3-Análisis de los equipos instalados en la red: 62
2.4.-Determinación de canales E1´s asignados a la red: 67
2.4.1.-Backbone: 67
2.4.2.- Acceso.- Para el acceso de las unidades hacia el backbone se emplea los siguientes medios: 70

2.4.3.- Enlaces para servicios de voz: 72
2.5.-Determinación de configuraciones en la red: 76
2.6.-Análisis de anchos de banda en la red: 80
2.7.- Requerimientos de los usuarios y crecimiento a mediano plazo. 87
CAPÍTULO 3 92
DISEÑO DE LA RED. 92
3.1.- Topología de la red: 92
3.1.1.- Ubicación de equipos LER: 93
3.1.2.-Ubicación equipos LSR: 93
3.1.3.- Ubicación de equipos LSR y LER: 94
3.1.4.- Análisis de Topología: Nodos Anillo central: 95
3.1.5.- Análisis de Topología: Nodos Anillo Norte. 96
3.1.6.- Análisis de Topología: Nodos Anillo Sur: 97
3.2.- Dimensionamiento de la red: 99
3.3.- Determinación de los equipos de core, distribución y acceso: 101
3.3.1.- Equipos de core: 101
3.3.2.- Equipos de distribución: 102
3.3.3.- Equipos de acceso: 102
3.3.4.- Parámetros diferenciales de los equipos: 103
3.4.- Determinación de costos del equipo definido: 103
3.5.- Establecimiento de facilidades MPLS en la red: 104
3.5.1.- Protocolos a emplearse: 104
3.5.2.-Empleo MPLS en la red: 110
CAPÍTULO 4 120
MODELAMIENTO Y EVALUACIÓN DE LA PROPUESTA. 120
4.1.-Modelamiento de la solución en la plataforma OPNET. 120
4.1.1.- Configuración de Protocolos de enrutamiento: OSPF: 120
4.1.2.- Configuración de Protocolos de enrutamiento: IS-IS: 123
4.1.3.- Configuración del Protocolo LDP y MPLS: 125
4.1.4.- Configuración de VPN: 126
4.1.5.- Configuración del Protocolo MP-BGP y redistribución con OSPF: 127
4.1.6.- Configuración de distintas VPN´s con diferentes usuarios: 130

4.1.7.- Configuración de VPN´s complejas: 132
4.1.8.- Configuración de QoS MPLS: 136
4.1.9.- Configuración de Ingeniería de tráfico-túneles MPLS. 144
4.2.-Evaluación de tiempos de respuesta. 147
4.2.1.- Evaluación Escenario 1: OSPF 147
4.2.2.- Evaluación Escenario 2: IS-IS 154
4.2.3.- Evaluación Escenario 3: Configuración MP-BGP. 156
4.2.4.- Evaluación Escenario 4: Configuración VRF´s distintas para diferentes usuarios. 161
4.2.5.- Evaluación Escenario 5: Configuración VRF´s complejas. 166
4.2.6.- Evaluación Escenario 6: Configuración Qos. 167
4.2.7.- Evaluación Escenario 7: Configuración Policing. 171
4.2.8.- Evaluación Escenario 8: Configuración Ingeniería de Tráfico. 173
CAPÍTULO 5 177
DIRECTIVA PARA ADMINISTRACIÓN, USO E IMPLEMENTACIÓN DE SERVICIOS Y EQUIPOS EN LA RED. 177
5.1.-Políticas de administración. 177
5.2.-Políticas de uso en base a los servicios. 179
5.1.-Políticas de implementación de equipos en base a la tecnología MPLS. 180
CAPÍTULO 6 182
CONCLUSIONES Y RECOMENDACIONES. 182
6.1.- Conclusiones. 182
6.2.- Recomendaciones. 183
REFERENCIAS BIBLIOGRÁFICAS 185
ANEXO A “PROYECCIÓN DE REQUERIMIENTOS A MEDIANO PLAZO”. 186
ANEXO B “REQUERIMIENTOS DE USUARIOS” 194
ANEXO C “DISTANCIAS DE ENLACES” 200
ANEXO D “PROYECTO MPLS-SENPLADES” 202
ANEXO E “ESPECIFICACIONES TÉCNICAS” 218

LISTADO DE TABLAS:

Tabla No 1.- Costo ramal costa. 2
Tabla No 2.- Costo ramal sierra. 2
Tabla No 3.- Tipos de modelos OPNET..... 48
Tabla No 4.- Servicios Comando Conjunto..... 61
Tabla No 5.- Servicios Fuerza Terrestre..... 61
Tabla No 6.- Servicios Fuerza Naval. 62
Tabla No 7.- Servicios Fuerza Aérea. 62
Tabla No 8.- Equipos del Nodo Quito..... 64
Tabla No 9.- Equipos del Nodo Guayaquil 64
Tabla No 10.- Equipos del Nodo Coca..... 65
Tabla No 11.- Equipos del Nodo Machala 66
Tabla No 12.- Resumen equipos de la red de datos. 67
Tabla No 13.- Capacidades Anillo Central..... 67
Tabla No 14.- Capacidades Anillo este. 68
Tabla No 15.- Capacidades Anillo norte. 68
Tabla No 16.- Capacidades Anillo sur. 69
Tabla No 17.- Capacidad red nororiental-noroccidental..... 69
Tabla No 18.- Ubicación estaciones wimax. 70
Tabla No 19.- Ubicación estaciones satelitales. 71
Tabla No 20.- Centrales que dependen del Nodo Quito. 72
Tabla No 21.- Centrales que dependen del Nodo Guayaquil..... 72
Tabla No 22.- Centrales que dependen del Nodo Coca. 73
Tabla No 23.- Centrales que dependen del Nodo Machala..... 73
Tabla No 24.- E1´s asignados para datos. 74
Tabla No 25.- E1´s asignados para voz. 75
Tabla No 26.- E1´s asignados para videoconferencia de los Comandos Operacionales 76
Tabla No 27.- Configuraciones de Equipos del Nodo Quito 76
Tabla No 28.- Configuraciones de Equipos del Nodo Guayaquil..... 77
Tabla No 29.- Configuraciones de Equipos del Nodo Coca 78

Tabla No 30.- Configuraciones de Equipos del Nodo Machala 79
Tabla No 31.- Anchos de banda datos Anillo Central. 80
Tabla No 32.- Anchos de banda voz Anillo central. 81
Tabla No 33.- Anchos de banda Centrales telefónicas. 82
Tabla No 34.- Anchos de banda videoconferencia Anillo central. 83
Tabla No 35.- Anchos de banda datos Anillo norte. 83
Tabla No 36.- Anchos de banda voz Anillo norte. 83
Tabla No 37.- Anchos de banda datos Anillo oeste. 84
Tabla No 38.- Anchos de banda voz Anillo oeste. 85
Tabla No 39.- Anchos de banda datos Anillo sur. 86
Tabla No 40.- Anchos de banda voz Anillo sur. 86
Tabla No 41.- Anchos de banda proyectada Anillo central. 87
Tabla No 42.- Anchos de banda proyectada Anillo norte. 88
Tabla No 43.- Anchos de banda proyectada Anillo oeste. 88
Tabla No 44.- Anchos de banda proyectada Anillo sur. 89
Tabla No 45.- Resumen de capacidades por anillo. 89
Tabla No 46.- Requerimientos de las Fuerzas por unidades. 90
Tabla No 47.- Requerimientos en los anillos de las Fuerzas. 90
Tabla No 48.- Ubicación equipos LER. 93
Tabla No 49.- Ubicación equipos LSR. 93
Tabla No 50.- Costo Anillo Central. 95
Tabla No 51.- Costo Anillo Norte. 96
Tabla No 52.- Costo Anillo Sur. 97
Tabla No 53.- Capacidades de la red de datos a mediano plazo. 99
Tabla No 54.- Capacidades actuales de la red de transporte. 100
Tabla No 55.- Equipos de Core 101
Tabla No 56.- Equipos de distribución. 102
Tabla No 57.- Equipos de acceso. 102
Tabla No 58.- Parámetros diferenciales de los equipos: 103
Tabla No 59.- Costos de equipo definido: 104
Tabla No 60.- Nominativos VRF´s. 107

Tabla No 61.- RD de VRF´s: XX. 108
Tabla No 62.- RD de VRF´s: YYY 109
Tabla No 63.- IP ENTRE LSR-LSR Y LSR-LER: 112
Tabla No 64.- IP ENTRE LER-CE: 112
Tabla No 65.- IP LOOPBACK: 113
Tabla No 66.- QOS DSCP: 115
Tabla No 67.- RD y RT para diferentes servicios. 131
Tabla No 68.- Tráfico para QoS 168
Tabla No 69.- Tráfico Policing para QoS 172
Tabla No 70.- Tráfico Policing para QoS. 174

LISTADO DE FIGURAS:

Figura No 1: Anillo central SDH..... 2
Figura No 2: Capas de Interconectividad. 3
Figura No 3: Capa de acceso..... 4
Figura No 4: Capa de distribución. 4
Figura No 5: Capa de core..... 5
Figura No 6: Dimensión con tolerancia a fallas. 6
Figura No 7: MPLS en el modelo OSI. 7
Figura No 8: LSR y LER 8
Figura No 9: FEC con y sin agregación. 10
Figura No 10: LSP 11
Figura No 11: Pila de Etiquetas..... 12
Figura No 12: MPLS..... 14
Figura No 13: Intercambio de Etiquetas..... 16
Figura No 14.- Plano de control de envío..... 16
Figura No 15.- Operación MPLS. 17
Figura No 16.- VPWS..... 21
Figura No 17.-Trama Ethernet con paquete MPLS. 22
Figura No 18.- VPLS funcionamiento..... 24
Figura No 19.- Dirección VPNIPv4. 26
Figura No 20.-Establecimiento de los LSP´s e intercambio de rutas CE-PE..... 30
Figura No 21.-Tablas de forwarding MPLS. 31
Figura No 22.- Publicación de rutas por los PE´s. 33
Figura No 23.- Contenido de las VRF´s 34
Figura No 24.- Tablas de ruteo en los CE´s..... 35
Figura No 25.- Tráfico en VPN´s BGP/MPLS CON PHP. 37
Figura No 26.- Head end and tail end..... 41
Figura No 27.- Protección de enlace. 43
Figura No 28.- Protección de enlace 1:N- tráfico..... 44
Figura No 29.- Protección de enlace modo 1:1. 44

Figura No 30.- Establecimiento del túnel de protección. 45
Figura No 31.- Valores DSCP para AF 47
Figura No 32.- Simulador Opnet. 49
Figura No 33.- Creación de nuevo proyecto. 50
Figura No 34.- Escenario vacío Opnet. 50
Figura No 35.- Open Object Palette. 51
Figura No 36.- Node Models MPLS. 51
Figura No 37.-Edit Attributes. 52
Figura No 38.-Configuración de la simulación. 52
Figura No 39.-Vista de resultados. 53
Figura No 40.- Anillos del Sistema MODE. 55
Figura No 41.- Nodos de la Red de datos. 63
Figura No 42.- Equipos que se derivan del Nodo Quito. 63
Figura No 43.- Equipos que se derivan del Nodo Guayaquil. 64
Figura No 44.- Equipos que se derivan del nodo Coca. 65
Figura No 45.- Equipos que se derivan de la estación Lumbaqui conectada al Nodo Coca. 65
Figura No 46.- Equipos que se derivan del nodo Machala. 66
Figura No 47.- Configuración Backbone. 77
Figura No 48.- Configuración OSPF Nodo Quito. 77
Figura No 49.- Configuración OSPF Nodo Guayaquil. 78
Figura No 50.- Configuración OSPF Nodo Coca. 79
Figura No 51.- Configuración OSPF Nodo Machala. 79
Figura No 52.- NCOMPASS Y SOLARWINDS. 80
Figura No 53.- Red de transporte MODE. 92
Figura No 54.- Ubicación Equipos LSR y LER. 94
Figura No 55.- Topología Anillo central 95
Figura No 56.- Conexiones nodos Anillo Central. 96
Figura No 57.- Conexiones nodos Anillo Norte 97
Figura No 58.- Topología Anillo Norte. 97
Figura No 59.- Topología Anillo Sur. 98
Figura No 60.- Conexiones Backbone Red de datos. 98

Figura No 61.- Topología LSR y LER 99
Figura No 62.- Capacidades en los anillos de la red de transporte. 100
Figura No 63.- Campo NSAP. 105
Figura No 64.- VPN MPLS 107
Figura No 65.- Convergencia en caso de fallas 110
Figura No 66.- Capacidades de los enlaces. 111
Figura No 67.- Estructura ToS. 114
Figura No 68.- Opción Cisco. 120
Figura No 69.-Configuración interfaces. 121
Figura No 70.- Configuración protocolo OSPF. 122
Figura No 71.- Tráfico editado entre dos nodos. 122
Figura No 72.- Escenario 1: OSPF. 123
Figura No 73.- Configuración protocolo IS-IS. 124
Figura No 74.- Escenario 2: IS-IS. 124
Figura No 75.- Protocolo LDP. 125
Figura No 76.- Habilitación MPLS. 125
Figura No 77.- Configuración VPN. 126
Figura No 78.- Configuración VPN. 126
Figura No 79.- Habilitación IPv4 y VPNv4 127
Figura No 80.- Redistribución OSPF en BGP. 128
Figura No 81.- Redisribución BGP en OSPF 128
Figura No 82.- Configuración neighbor BGP. 129
Figura No 83.- Configuración Sistema Autónomo. 130
Figura No 84.- Escenario 3: Configuración MP-BGP. 130
Figura No 85.- VPN VOZFAE 131
Figura No 86.- Escenario 4: VRF´s distintas para diferentes usuarios 132
Figura No 87.- VRF´s con import y export. 133
Figura No 88.- Sub-interfaces lógicas entre CE´s y PE´s. 134
Figura No 89.- VLAN´s creadas en cada interface. 135
Figura No 90.- Procesos OSPF asociado a cada sub-inetrfaz. 135
Figura No 91.- Escenario 5: VRF´s complejas. 136

Figura No 92.- Clasificación de Clases QoS. 137
Figura No 93.- Configuración de marcaje QoS. 138
Figura No 94.- Configuración WFQ. 139
Figura No 95.- Asignación WFQ a la política de salida. 140
Figura No 96.- Asociación de la política a la interfaz. 141
Figura No 97.- Escenario 6 : QoS 141
Figura No 98.- Configuración policing. 142
Figura No 99.- Asociación policing a la política de entrada. 143
Figura No 100.- Escenario 7: Policing. 143
Figura No 101.- Configuración de FEC y Trunk para el túnel. 145
Figura No 102.- Rutas de los LSP´s creados. 146
Figura No 103.- Selección del LSP a utilizar para determinado FEC. 146
Figura No 104.- Escenario 8: Túnel LSP. 147
Figura No 105.- Generación de tráfico. 148
Figura No 106.- Configuración para visualizar resultados 149
Figura No 107.- Corrida de la simulación. 149
Figura No 108.- Visualización ping OSPF. 150
Figura No 109.- Visualización tráfico enviado vs recibido. 150
Figura No 110.- Tablas de Enrutamiento. 151
Figura No 111.- Ruta seleccionada por OSPF. 152
Figura No 112.- Caída del enlace LER-LU-LER-IG. 153
Figura No 113.- Tráfico re-enrutado OSPF. 153
Figura No 114.- Tráfico con fallas en dos enlaces. 154
Figura No 115.- Visualización ping IS-IS. 154
Figura No 116.- Ping IS-IS y OSPF. 155
Figura No 117.- Tabla de enrutamiento IS-IS. 155
Figura No 118.- Tráfico con fallas en dos enlaces. 156
Figura No 119.- Protocolos Configurados. 157
Figura No 120.- Visualización VPN. 157
Figura No 121.- Rutas prendidas de un CE. 158
Figura No 122.- Rutas aprendidas en la nube MPLS. 158

Figura No 123.- Tráfico entre CE´s. 159
Figura No 124.- Ping en routers MPLS. 159
Figura No 125.- Rutas de tráfico. 160
Figura No 126.- Tráfico re-enrutado 160
Figura No 127.- Diagrama de simulación. 161
Figura No 128.- Protocolos de simulación. 162
Figura No 129.- VRF´s distintas en la red. 162
Figura No 130.- Tabla de enrutamiento CE-LA. 163
Figura No 131.- Tablas de enrutamiento OPNET. 163
Figura No 132.- VRF´s creadas entre los LER´s. 164
Figura No 133.- Tráfico entre CE-COL y CE-LA. 164
Figura No 134.- Tráfico entre CE-CO y CE-UIO 165
Figura No 135.- Tráfico entre CE-LA y CE-UIO. 165
Figura No 136.- VRF´s con import y export. 166
Figura No 137.- Tráfico entre VRF´s compartidas. 166
Figura No 138.- VRF compartida. 167
Figura No 139.- Tráfico generado para video. 167
Figura No 140.- Tráfico recibido Simulación No 1. 168
Figura No 141.- Tráfico recibido Simulación No 2. 169
Figura No 142.- Tráfico recibido Simulación No 3. 169
Figura No 143.- Tráfico recibido Simulación No 4. 170
Figura No 144.- Ruta del tráfico con QoS. 171
Figura No 145.- Ruta con caída de enlace QoS. 171
Figura No 146.- Tráfico generado en la simulación Policing. 172
Figura No 147.- Tráfico recibido en la simulación Policing. 173
Figura No 148.- Tráfico en el túnel LER-LU-LER-MA 174
Figura No 149.- Ruta 1 del tráfico entre CE-LA y CE-COL por el LSP. 175
Figura No 150.- Tráfico en el túnel LER-LU-LER-MA 1. 175
Figura No 151.- Ruta 2 del tráfico entre CE-LA y CE-COL por el LSP. 176
Figura No 152.- Rutas que realiza cada LSP. 176

RESUMEN

El objetivo del presente trabajo es elaborar un proyecto para la reestructuración de la red de datos de Fuerzas Armadas con capacidad de soportar el crecimiento, integración y convergencia de los servicios mediante un análisis de la estructura actual de la red, canales asignados a cada servicio, equipos instalados, para dimensionar la nueva red con anchos de banda proyectados a mediano plazo en base a criterios de crecimiento anual de la red y requerimientos de los usuarios. Este diseño de topología de costo mínimo permitirá la implementación de equipos con tecnología MPLS y aprovechar sus funcionalidades en la integración de los servicios que soporta la red de datos de Fuerzas Armadas, siendo la solución simulada con el software OPNET

PALABRAS CLAVE: REESTRUCTURACIÓN, MPLS, OPNET, TOPOLOGÍA, SIMULACIÓN.

ABSTRACT

The aim of the present work is to elaborate a project for the restructuring of the network of information of Armed Forces with aptitude to support the growth, integration and convergence of the services by means of an analysis of the current structure of the network, channels assigned to every service, installed equipments, then to measure the new network with bandwidths projected to medium term on the basis of criteria of annual growth of the network and requirements of the users. This design with topology of minimal cost will allow the implementation of equipments with technology MPLS and to take advantage of his functionalities in the integration of the services that supports the network of information of Armed Forces, being the solution simulated with the software OPNET.

KEY WORDS: RESTRUCTURING, MPLS, OPNET, TOPOLOGY, SIMULATION.

CAPÍTULO 1
MARCO CONCEPTUAL.

1.1.-Método de diseño de la red.

En la actualidad existen diversos métodos para el diseño de una red, sin embargo para el presente proyecto se establecerá un modelo que se ajuste a la realidad de la red de datos de Fuerzas Armadas, considerando los anillos de transporte de la red MODE y que satisfaga los requerimientos presentes y futuros. Este método estará basado en las clases recibidas de planificación de redes en el transcurso de la maestría de Gestión de Redes y Telecomunicaciones.

Para conocer el modelo aplicable es necesario establecer el concepto de costo mínimo. Esto significa que el costo asociado a cada configuración de la red Cost(x) está dado por la suma de los costos de sus enlaces. Una manera de establecer el costo de un enlace es conociendo la distancia que cubre y el precio por unidad de distancia que implica la colocación de una tecnología específica (YOANDI, 2010).

$$Cost(x) = \sum_{i=1}^{n} dis\_unit_{i-j} * Cost(x_{i-j})$$

En donde:

n: representa el número de enlaces del nodo i a j.

dis_unit_{i-j}: representa la distancia del terminal i al j.

$Cost(x_{i-j})$: representa el costo del enlace entre el terminal i al j.

Para este caso práctico al ser una red de transporte basado en la tecnología SDH/PDH, el costo de cada enlace está relacionado directamente a la distancia del enlace; debido a que los enlaces se encuentran implementados y su costo no representa un parámetro mandatorio en el diseño, lo que significa que la ecuación para el cálculo del costo de un nodo a otro estará definida por la siguiente ecuación:

$$Cost(x) = \sum_{i=1}^{n} dis\_unit_{i-j}$$

Al estar configurada la red de transporte en anillos, el costo mínimo de un nodo a otro estará definido por la distancia mínima o de menor costo en cada uno de los ramales. Es decir el costo entre dos nodos se define mediante el siguiente ejemplo.

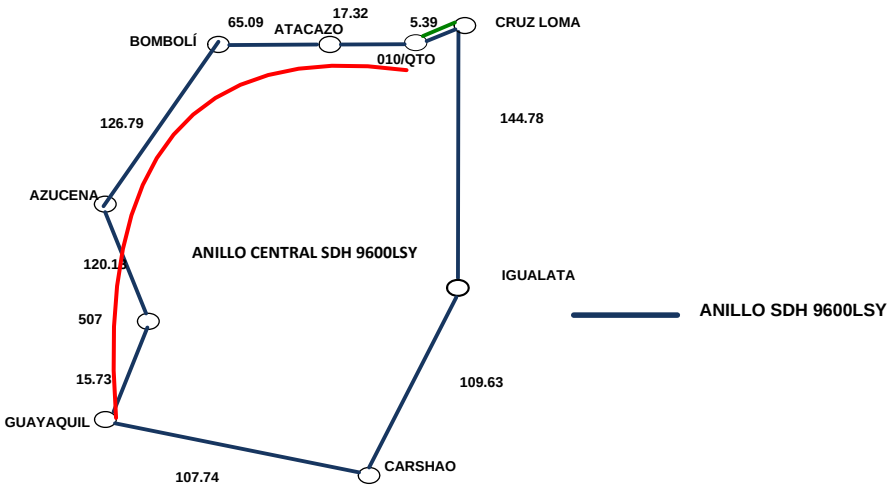


Figura No 1: Anillo central SDH.

Tabla No 1.- Costo ramal costa.

RAMAL COSTA: ENLACE	COSTO (DISTANCIA EN Km)
CRUZ LOMA- QUITO	5.39
QUITO-ATACAZO	17.32
ATACAZO-BOMBOLÍ	65.09
BOMBOLÍ-AZUCENA	126.79
AZUCENA-507	120.13
TOTAL	**334.72**

Tabla No 2.- Costo ramal sierra.

RAMAL SIERRA: ENLACE	COSTO (DISTANCIA)
CRUZ LOMA-IGUALATA	144.78

CONTINÚA →

IGUALATA-CARSHAO	109.63
CARSHAO-GUAYAQUIL	107.74
GUAYAQUIL-507	15.73
TOTAL	**377.88**

En referencia al ejemplo ilustrado en la Figura No 1, el ramal costa representa el de menor costo, por lo cual el camino para unir estos nodos es este ramal y su backup o respaldo, lo que más adelante se denominará diseño con tolerancia a fallas, será el ramal sierra.

Este modelo para establecer el diseño de la red, considerando los enlaces y el criterio de costo mínimo, se encuentra asociado al criterio empleado por el protocolo OSPF del algoritmo de Dijkstra, como el camino más corto entre dos puntos o nodos de una red (THOMAS). Para el caso puntual los nodos son Cruz Loma y 507 y los pesos entre cada terminal están representados por las distancias de los enlaces de la red de transporte SDH. Estas rutas para el posterior análisis de otros nodos, tendrán un costo de cero y podrán ser utilizadas como rutas de estos, analizados de par en par.

1.1.1.- Criterio a considerar para ubicar los equipos en la red.

El criterio se fundamentará en los conceptos de interconectividad, bajo una estructura de RED definida jerárquicamente como se observa en la Figura No. 2:

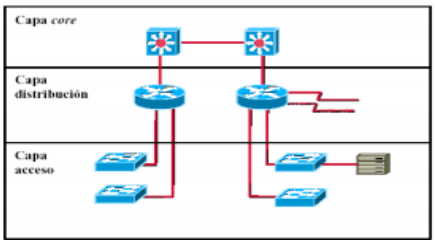


Figura No 2: Capas de Interconectividad.

La **capa de acceso** de RED es el punto en el cual los usuarios finales son conectados a la red. El tráfico hacia y desde los recursos locales está confinado entre los recursos, switches y usuarios finales como se representa en la Figura No. 3.

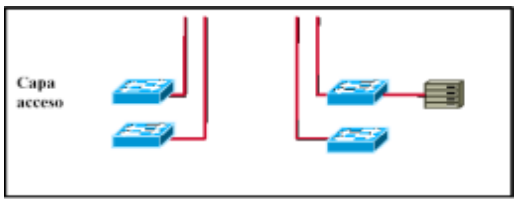


Figura No 3: Capa de acceso

La **capa de distribución** marca el punto entre la capa de acceso y el core, manipula paquetes mediante ruteo, filtrado y acceso WAN, como lo representa la Figura No. 4. La capa de distribución proporciona conectividad basada en políticas, porque determina como pueden acceder al core o al backbone. Determina el camino más rápido para una petición de usuario, una vez que la capa de distribución decide la trayectoria, se envía la petición a la capa core (CISCO).

Figura No 4: Capa de distribución.

En esta capa se considerará la distribución de la información, en base a las unidades que se conectan a determinado terminal. Por lo cual las características mínimas de estos equipos son:

- Acceso grupal o departamental.
- Enrutamiento de VLAN´s.
- Establecimiento de políticas.

La **capa core o backbone** tiene como función swtichear el tráfico rápidamente. El tráfico es por los servicios de usuarios (e-mail, acceso a internet, videoconferencia), los equipos de core se representan en la Figura No. 5.

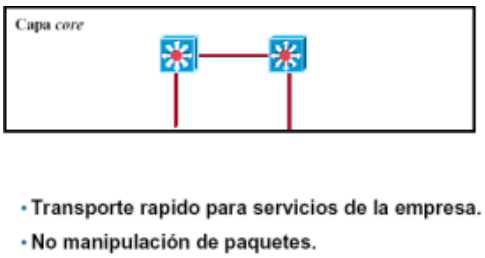


Figura No 5: Capa de core.

En esta capa al disponer en el sistema MODE una red de transporte en anillos, se considerará las uniones de los anillos que faciliten y permitan la conmutación por caminos principal y alterno. Por lo tanto entre las características mínimas que deben cumplir estos equipos son:

- Alta confiabilidad.
- Tolerancia a fallas.
- Redundancia.
- Transporte rápido.

1.2.- Método de dimensionamiento de la red:

1.2.1.-Dimensionamiento con tolerancia a fallas con compartición de enlaces.-

Este dimensionamiento consiste en el siguiente procedimiento:

1. Se selecciona dos nodos.
2. Se asigna un canal primario y un secundario.
3. El canal primario es el de menor costo y el secundario disjunto.
4. Se puede compartir los canales, si los primarios son disjuntos y los secundarios comparten la misma ruta (BEGHELLI).

Este método acoplado a la red MODE, considerando su estructura en anillos se realizará de la siguiente manera:

1. Se selecciona dos nodos en un anillo.
2. A cada nodo se le asignará un canal primario y secundario.
3. Al ser una red en anillo el canal primario se establecerá el de menor costo por un ramal y el secundario por el segundo ramal.
4. El canal primario y secundario entre los nodos tendrá la capacidad suficiente para soportar el tráfico que se desprende en los puntos de paso.
5. Para el dimensionamiento en el diseño se considerará el tráfico actual, lo requerido por las unidades y la proyección a mediano plazo.

A continuación se ilustra en el ejemplo de la Figura No. 6, el procedimiento entre los puntos Quito- Bombolí y Quito- Cruz Loma. Para el ejemplo los canales podrán compartir el medio en la ruta Igualata- Carshao, por lo tanto los canales secundarios compartidos, representan la redundancia o tolerancia a fallos.

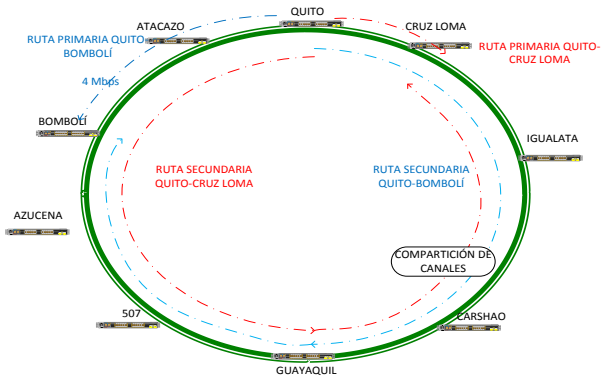


Figura No 6: Dimensión con tolerancia a fallas.

Mediante este método se dispondrá de la capacidad en los enlaces en las dos rutas, donde la conmutación de los paquetes lo realizarán los equipos activos en la red.

Para dimensionar las capacidades en los anillos, se empleará la siguiente fórmula de crecimiento de la red en base a las variables definidas a continuación:

$$Cf = Ci(1 + x)^n$$

Donde:
Cf = Capacidad estimada en n años
Ci = Capacidad inicial

x = Índice de crecimiento anual del servicio de Telecomunicaciones
n = Tiempo de proyección en años.

1.3.- Tecnología MPLS:

MPLS es una tecnología que combina las funciones de enrutamiento de capa 3 con las funciones de envío de capa 2 del modelo OSI, como se observa en la Figura No. 7, por esta razón se lo denomina Multiprotocolo ya que brinda la posibilidad de trabajar con cualquier tecnología de transporte y con aplicaciones que están sobre el nivel de red (DÍAZ). La Conmutación de etiquetas (Label Switching) permite identificar una clasificación de tráfico, encaminando a esta clasificación por un determinado camino virtual brindando QoS y otras ventajas que serán descritas a lo largo del presente capítulo.

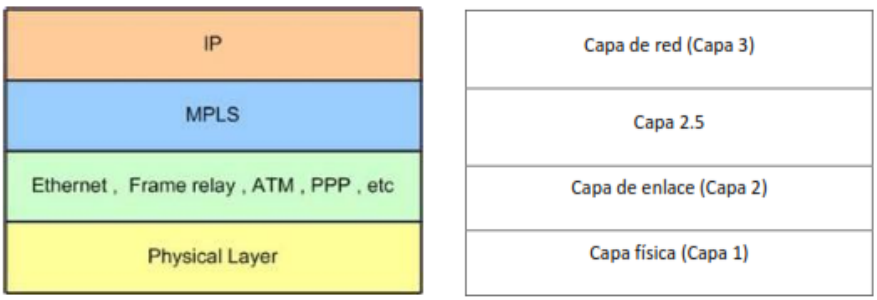


Figura No 7: MPLS en el modelo OSI.

1.3.1.- Elementos Básicos de MPLS:

Los elementos básicos en MPLS son los siguientes:

- LER, Label Edge Router (Ruteador Etiquetador de Borde)
- LSR, Label Switching Router (Ruteador de Conmutación de Etiquetas)
- FEC, Forward Equivalence Class (Clase Equivalente de Envío)
- LSP, Label Switched Path (Ruta Conmutada de Etiquetas)
- LDP, Label Distribution Protocol (Protocolo de Distribución de Etiquetas)

- **Label Edge Router (LER):**

Los LER se encuentran ubicados en el borde de la red MPLS y desempeñan las funciones de encaminamiento tanto para un dominio MPLS como para un dominio no MPLS (otras redes).

El propósito de un LER es el análisis y clasificación del paquete IP que entra a la red, a esta clasificación por conjuntos de paquetes se le denomina FEC. Una vez analizado el paquete IP se añade una cabecera MPLS y en uno de sus campos denominado Etiqueta se le asigna un valor de acuerdo a su clasificación FEC. Al salir del dominio MPLS el LER de salida es el que direcciona el paquete a la red de destino por enrutamiento convencional eliminando la cabecera MPLS.

- **Label Switching Router (LSR):**

El LSR realiza el encaminamiento basándose en la conmutación de etiquetas. Una vez que le llega un paquete a una de sus interfaces éste lee la etiqueta de entrada en la cabecera MPLS y busca en la tabla de conmutación la etiqueta y la interfaz de salida para designar la nueva etiqueta que indica el siguiente salto dentro del dominio y finalmente reenvía el paquete por el camino ya designado en el LER (según el FEC) como se observa en la Figura No. 8.

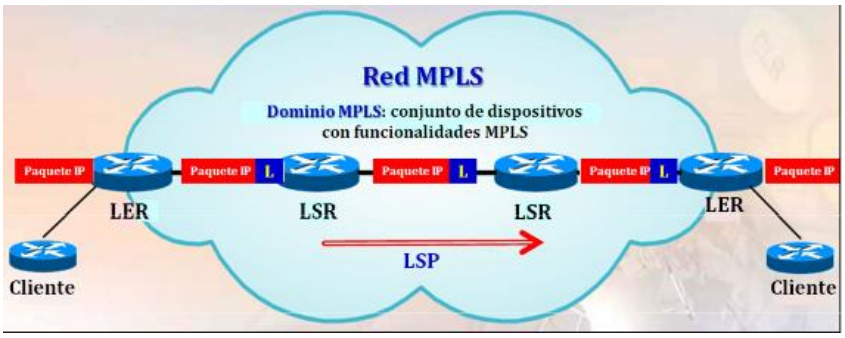


Figura No 8: LSR y LER

- **Forward Equivalence Class (FEC):**

El FEC es la agrupación de etiquetas que permite la asociación de un conjunto de paquetes sobre el mismo camino y con un destino común. Todos los paquetes de un mismo FEC se tratan de la misma forma hacia su destino, y cuantos más FECs se tenga, mejor se podrá diferenciar entre distintos tipos de flujos. Cada FEC tiene QoS debido a que se debe tratar a los paquetes que van por el mismo camino de diferente manera, dando prioridad según la necesidad de manera que se utilizan los recursos de la red óptimamente.

La etiqueta de un determinado paquete representa al FEC al cual pertenece. Los LSR de entrada, que son los que etiquetan a los paquetes, son los encargados de asociar al paquete a un FEC y se basan principalmente en los siguientes aspectos:

- Dirección IP de origen, destino o direcciones IP de la red.
- Número de puerto de origen o destino
- Campo protocolo de IP (TCP, UDP, ICMP, etc.)
- Valor del campo DSCP de DiffServ
- Etiqueta de flujo en IPv6

- **Agregación**

La Agregación es un mecanismo que permite agrupar varios FEC mediante la asignación de una sola etiqueta para todos, de esta manera se reduce el tiempo de envío de los FEC porque se elimina asociaciones etiqueta/FEC redundantes.

Puede ser posible la Agregación cuando a un LSR le llegan desde un mismo LER varios FEC con el mismo origen y destino dentro de la red MPLS asignados al mismo camino LSP, en la Figura No. 9 se representa los FEC con y sin agregación respectivamente.

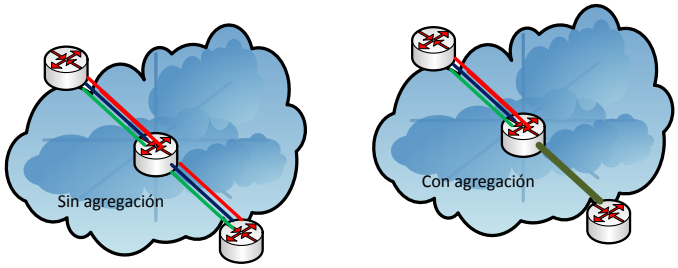


Figura No 9: FEC con y sin agregación.

- **Label Switched Path (LSP):**

El LSP es un camino virtual o una ruta de tráfico específica a través de la red MPLS que sigue un grupo de paquetes que pertenecen a un mismo FEC. Estos caminos son unidireccionales (simplex) y solo transmiten hacia un sentido de tráfico. Si se desea que la red sea dúplex, se deben establecer dos LSPs, uno para cada sentido. Los mensajes utilizados por los LSR son los siguientes:

- Descubrimiento: mediante mensajes *"hello"* de un LSR a otro LSR.
- Sesión: dos LSR establecen y mantienen la comunicación.
- Anuncio: para dar a conocer a otro LSR de las asociaciones FEC/Etiqueta.
- Notificación: información de eventos y errores

Las rutas LSP se forman desde el destino hacia el origen debido a que el LSR de origen genera las peticiones para crear un nuevo LSP mientras que el destino responde a estas solicitudes formándose de esta manera el LSP hasta el origen.
MPLS proporciona dos opciones para crear un LSP:

Encaminamiento salto a salto (*hop-by-hop routing*).- Cada LSR selecciona independientemente el próximo salto para un determinado FEC, para ello utiliza cualquier protocolo de routing disponible como OSPF, ATM PNNI (*Private Network-Node Interface*), etc.

Encaminamiento Explicito (explicit routing).- El LER de entrada determina la secuencia de saltos explícita desde la entrada hasta la salida (ER-LSP, Explicit

Routing LSP), utilizando los protocolos de señalización o de distribución de etiquetas (RSVP, LDP, etc). Esto facilita la ingeniería de tráfico y el poder tener servicios diferenciados usando políticas de tráfico o métodos de gestión de red como se muestra en la Figura No. 10.

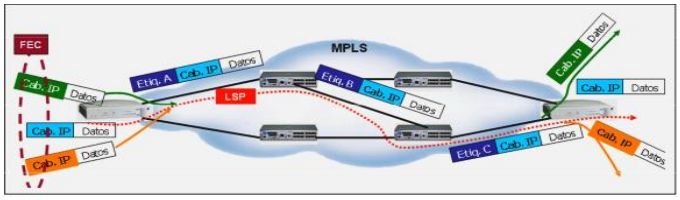


Figura No 10: LSP

- **Label Distribution Protocol (LDP):**

El LDP define los mecanismos para la distribución de etiquetas, permite a los LSR descubrirse e intercambiar información sobre las asociaciones FEC/Etiqueta que se han realizado y sobre todo para mantener la coherencia de las etiquetas utilizadas para los distintos tipos de tráfico que conmutan. Con este protocolo se evita que a un LSR le llegue tráfico con una etiqueta que no se encuentra en su tabla, con esto se asegura la rapidez en la conmutación de los LSR. La distribución de etiquetas usa uno de los siguientes métodos:

Downstream on-demand: Un LER/LSR informa a su vecino sobre que etiqueta debe usar para el envío del tráfico por una determinada interfaz, es decir que la distribución de etiquetas se realiza contraria al camino que sigue el tráfico.

Unsolicited downstream: Un LER/LSR informa de las asociaciones Etiqueta/FEC a sus vecinos que las almacenan en sus tablas sin haber solicitado la información, este mecanismo es más eficaz ya que así todos los vecinos LER/LSR mantienen las tablas actualizadas (del mismo LSP) y haciendo el proceso de conmutación de etiquetas mucho más rápido pero incrementando el tráfico de control.

- **Label Stack (Pila de Etiquetas)**

Una de las características del protocolo MPLS es que permite apilar diversas etiquetas unas sobre las otras. Esto se denomina "Pila de Etiquetas" y consigue anidar un LSP dentro de otro. El objetivo de esta técnica es el de crear túneles dentro de los otros LSPs, como se puede observar en la Figura No. 11.

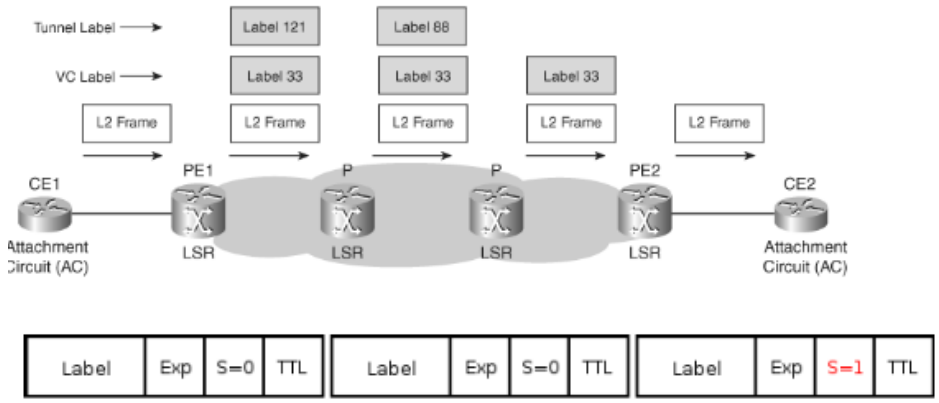


Figura No 11: Pila de Etiquetas.

Para conseguirlo, un LSR en vez de intercambiar las etiquetas lo que hace es añadir una etiqueta nueva encima de la pila. Las etiquetas se añaden siguiendo un sistema LIFO (Last-in, Fisrt-out) y no altera el funcionamiento de enrutado, simplemente el router lee la etiqueta más externa y actúa únicamente en función de ese valor.

1.3.2.- Características de MPLS:

A continuación se describen las características más importantes que destacan la tecnología MPLS en las redes de datos:

- Opera sobre cualquier tecnología de transporte a nivel físico o de enlace, facilitando la migración a las Redes de próxima Generación.
- MPLS es una tecnología que combina eficazmente las funciones de control de ruteo con la simplicidad y rapidez de la conmutación de nivel 2.

- La implementación de MPLS permite a una red ser más sencilla de operar, mayor escalabilidad e interoperabilidad debido al soporte de diversas tecnologías bajo una plataforma común que permite ofrecer variados servicios dependiendo de los requerimientos de los usuarios.
- Utiliza protocolos para el intercambio y distribución de etiquetas que permite la creación de caminos virtuales conocidos como LSP (Label Switched Path) que se crean dependiendo de la clasificación del flujo de tráfico que cursa la red.
- Al ser un estándar abierto, también para la distribución de etiquetas utiliza protocolos abiertos.
- MPLS permite aplicar técnicas de Ingeniería de Tráfico para encontrar la mejor ruta no necesariamente la más corta en algunos casos, pero que garantiza la llegada de los flujos de tráfico evitando cuellos de botella y caída de los enlaces, además de QoS, VPN´s, entre otras.
- Los paquetes enviados de los endpoints pueden tener diferentes FEC, por lo que las etiquetas serán diferentes y tendrá un PHB distinto en cada LSR, esto permite generar diferentes flujos en una misma red y la integración de servicios.

1.3.3.- Funcionamiento de la tecnología MPLS:

Una red MPLS, funciona básicamente cambiando las etiquetas de un paquete ya etiquetado, cada paquete de datos transforma su etiqueta o label durante la totalidad de la trayectoria. Gracias a que las etiquetas de tamaño fijo son insertadas en el encabezado del paquete, el switching se puede realizar a muy alta velocidad (URQUIZA, 2011).

- **Encabezado MPLS:**

En la Figura No. 12 se presentan los campos de la cabecera genérica MPLS que se asigna una vez a la entrada en el router LER.

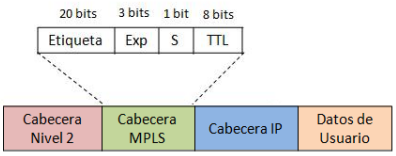


Figura No 12: MPLS.

Como se puede observar la cabecera está formado por 32 bits, distribuidos de la siguiente manera:

Etiqueta: identifica a que conjunto de FEC está asignado el paquete y mediante este campo los routers deciden por donde encaminar el paquete o que LSP debe seguir, es la etiqueta propiamente dicha compuesta de 20 bits.

Exp (Experimental): 3 bits, actualmente utilizado para el soporte de QoS.

S (Stack): 1 bit para apilar las etiquetas en forma jerárquica, si S vale 1 se trata de la última etiqueta en la pila (primera en ingresar a un dominio MPLS), caso contrario S vale 0. En caso de existir una sola etiqueta el valor de S es 1.

TTL (Time To Live): 8 bits que cumplen con una función similar a la del campo TTL de IPv4. Cuando a un paquete se le asigna la cabecera MPLS el campo TTL copia el valor TTL del paquete IP pero reducido en una unidad en el LER y por cada salto que realice en el dominio MPLS. Este mecanismo permite reducir la posibilidad de bucles en la red y de igual manera al salir de la red MPLS en el LER el campo TTL de la cabecera MPLS se traslada al campo TTL del paquete IP.

- **Descripción funcional:**

MPLS se basa fundamentalmente en la separación de dos funciones que a su vez están efectivamente coordinadas, conocidas como:

  - Plano de Control
  - Plano de Envío

Los routers o switches que soportan MPLS trabajan en estos dos planos, específicamente los LER al ser el borde del dominio MPLS cumplen con estas dos funciones de encaminamiento y de envío inicial de los paquetes asignando una cabecera MPLS mientras que los LSR solo se encargan de la conmutación de las etiquetas ignorando que es lo que hay tras de la cabecera MPLS, es decir la cabecera de red.

- **Plano de control:**

El Plano de Control utiliza los protocolos de enrutamiento ya sean de vector distancia o estado de enlace, para el intercambio de información dentro de la red MPLS, permitiendo la construcción y mantenimiento de las tablas de enrutamiento (RIB), que proporcionan las características de la topología, patrón de tráfico o detalles de los enlaces.

La difusión de las tablas de enrutamiento a los vecinos es muy importante porque establece los caminos virtuales LSP que los LER indican al inicio para la generación de las tablas de envío utilizando también la señalización que proveen los Protocolos de Distribución de Etiquetas RSVP, LDP o TDP (LIB) y posteriormente el intercambio de etiquetas (Plano de Envío). Entonces un LSR o LER tiene dos tablas, una dedicada a la información de enrutamiento y la segunda con la información a nivel local de las etiquetas conocida como **LIB**.

La construcción de estas tablas se basa en las operaciones que realizan las etiquetas y son las siguientes:

- PUSH: imposición de las etiquetas en un ruteador de ingreso LER.
- SWAP: la etiqueta es cambiada por otra dentro del mismo rango que identifica un FEC en los LSRs.
- POP: operación en la que se elimina la etiqueta en un LER al salir de la red MPLS.

- **Plano de envío:**

El Plano de Envío MPLS utiliza la información de las etiquetas para la conmutación local de las mismas y para el envío de los paquetes a sus vecinos dentro del dominio, es decir se encarga de las asignaciones y modificaciones de etiquetas (LFIB), rigiéndose a la información proporcionada por el Plano de Control.

El paquete conforme avanza dentro de la red MPLS adquiere una nueva etiqueta, el valor de esta etiqueta define el FEC (Forward Equivalence Class) asignado. En la Figura No. 13 se puede apreciar el intercambio de etiquetas de un paquete y en la Figura No. 14 el plano de control y envío.

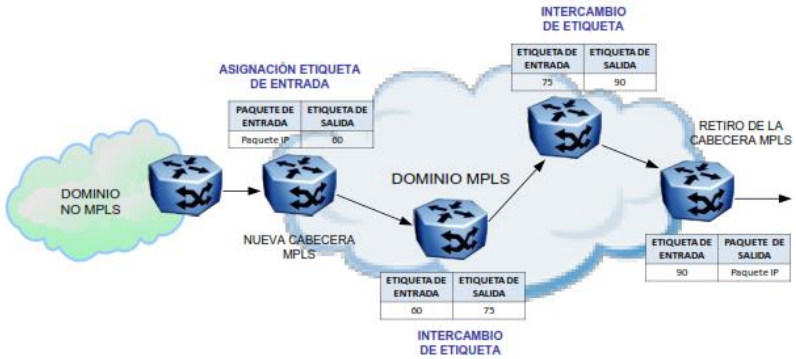


Figura No 13: Intercambio de Etiquetas.

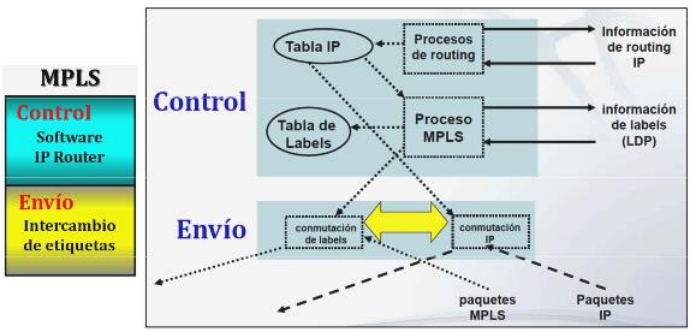


Figura No 14.- Plano de control y de envío.

- **Ejemplo de Operación:**

Se supone que el criterio para la asignación de un FEC será en función del prefijo IP destino, con el modo de distribución de etiquetas basado en downstream on

demand y el protocolo de señalización LDP. Según el ejemplo de la Figura No. 15, se analizará el camino de un paquete que ingresa por el LER1 destinado a una máquina detrás de LER4 (URQUIZA, 2011).

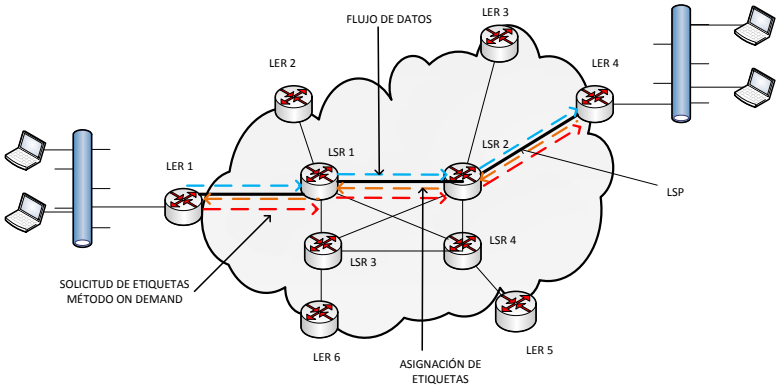


Figura No 15.- Operación MPLS.

1. LER1 no tienen etiquetas para el destino deseado, por lo que realiza una solicitud de label al LSR 1, que él sabe por el IGP que será el next hop para su destino. Esta solicitud se propagará por la red MPLS como lo indica el camino ascendente.

2. Cada LSR intermedio recibe una etiqueta desde su dowstream router comenzando desde LER 4 hasta LER 1 como lo indica el camino descendente de la figura.

3. Una vez que cada LSR tiene una etiqueta para dicho destino (FEC) en su LIB, queda establecido el LSP como lo indica el camino de la figura.

4. En la LIB se encontrará mapeado el puerto de entrada y la etiqueta de entrada con el puerto de salida y la etiqueta de salida.

5. Por último el LER 1 insertará una etiqueta al paquete y lo enviará al LSR 1. Cada LSR subsiguiente examina la etiqueta del paquete, la reemplaza por la etiqueta saliente y realiza el forwarding.

6. Cuando el paquete llega al LER 4, se le remueve la etiqueta porque el paquete está saliendo del dominio MPLS y es entregado al destino. El camino recorrido por el paquete se indica en la figura. Este procedimiento es conocido como penultimate Hop Popping (PHP).

1.4.- Facilidades de la tecnología MPLS:

Actualmente existen tres aplicaciones más comunes de MPLS, las cuales son:

- Redes privadas virtuales-Virtual private Networks (VPNs)
- Ingeniería de Tráfico- Traffic Engineering.
- Calidad de Servicio- Quality of service (QoS).

1.4.1.- Virtual private Networks (VPNs)

Una Red Privada Virtual es una red de información privada que utiliza una infraestructura de Telecomunicaciones y conecta a usuarios de forma remota hacia una red principal, siendo una solución ideal para las empresas, y su objetivo es brindar aplicaciones Intranet y Extranet integrando soluciones multimedia.

Entre las características más importantes de una VPN se destaca la seguridad ya que se crea un canal privado de comunicación entre dos puntos utilizando la infraestructura de Internet, la privacidad se mantiene a través de Protocolos de Túnel o de aislamiento, que aplican encapsulación o cifrado de datos.

Las VPNs tradicionales ya sean basadas en PVC (Circuitos Virtuales Permanentes) o túneles IP han sido de gran beneficio pero tienen ciertos inconvenientes que pueden ser resueltos con la utilización de MPLS.

Las IP VPN están basadas en Protocolos de Túnel como por ejemplo IPSec, la información se cifra y se encapsula en una nueva cabecera IP. La desventaja en este tipo de implementaciones se dan porque se ocultan las cabeceras de los paquetes

originales y las opciones de QoS son bastante limitadas ya que no se puede distinguir los flujos por aplicación, dificultando la asignación de los diferentes niveles de servicio.

En general los inconvenientes más comunes que tienen las VPN tradicionales son los siguientes:

- Se basan en conexiones punto a punto (PVC o túneles).
- La configuración de cada nodo de la VPN es manual y cada vez que se integra uno supone la reconfiguración de todos los anteriores.
- La Calidad de Servicio se ofrece hasta cierta parte, más no durante el transporte.
- El modelo topológico sobrepuesto a la red existente implica poca flexibilidad en la provisión y gestión del servicio.

Utilizando MPLS para implementar VPNs se eliminan los inconvenientes de las tecnologías anteriores. En primera instancia el modelo topológico que se crea no se sobrepone sino se acopla a la red del proveedor, esto elimina las conexiones extremo a extremo (túneles IP convencionales o circuitos virtuales) y los túneles se van creando con el intercambio de las etiquetas formándose así los LSP que vendrían a ser los "túneles MPLS".

Dentro de la red del proveedor las VPNs se forman mediante las rutas virtuales LSPs, similares a los túneles de las VPNs tradicionales pero con la diferencia de que la información se transporta por el mecanismo de intercambio de etiquetas obviando la información de enrutamiento lo que facilita aplicar técnicas de QoS que son propagadas hasta el destino, reservando ancho de banda, estableciendo Clases de Servicios y aplicando Ingeniería de Tráfico de esta manera optimizando los recursos de la red y cumpliendo los máximos requerimientos de disponibilidad y seguridad.

Las ventajas que se tiene con MPLS son:

- Se elimina la complejidad de los túneles y los PVCs.

- Para la implementación no es necesario realizar cambios en todos los puntos involucrados como ocurre con las VPNs tradicionales, al contrario, solo se configura a nivel del proveedor evitando tareas complejas y riesgosas.
- Las garantías de Calidad de Servicio se mantienen de extremo a extremo separando los flujos de tráfico por clases.
- Para aumentar la seguridad se pueden utilizar los protocolos de encriptación manejados también por las VPNs tradicionales como IPSec.
- Con la Ingeniería de Tráfico que ofrece MPLS se garantiza que en el servicio VPN no influyan parámetros que afecten la calidad de extremo a extremo.

- **VPN capa 2 punto a punto Virtual private Wire Service (VPWS):**

VPWS provee enlaces punto a punto entre sitios de clientes. El cliente percibe a cada VPWS como un enlace físico privado. De acuerdo con IEFT(Internet Engineering Task Force) RFC 3985(pseudo Wire Emulation Edge-to- Edge Architecture), pseudowire emulation edge-to-edge (PWE3) es un mecanismo que emula los atributos esenciales de servicios tales como ATM, Frame Relay o Ethernet en redes de paquetes. La idea básica es que se dispone una red de capa 3 sobre la cual el operador de servicios quiere transportar servicios de capa 2. En el caso de MPLS estos pseudowires (PW) son LSPs (URQUIZA, 2011).

- **VPWS Ethernet sobre IP/MPLS-Implementación:**

1. Se debe configurar los túneles (túnel LSP) para llegar del PE1 al PE2 y viceversa. Como los LSPs son unidireccionales se necesita un par. Para la señalización de estos túneles se puede emplear cualquier protocolo de distribución, comúnmente se utiliza LDP y cuando se requiere ingeniería de tráfico RSVP-TE. Una vez finalizada la señalización se obtiene las etiquetas externas o sea los túneles LSPs en ambas direcciones.

2. Una vez establecido un camino virtual bidireccional, se debe crear los Virtual Circuit LSPs (VC LSPs). Esto puede realizarse de manera estática o dinámica mediante la utilización de Targeted LDP. De esta forma a través de los

túneles ya establecidos se forman dos sesiones TLDP una de PE1 a PE2 y otra de forma inversa. Una vez ocurrido esto quedan intercambiadas las etiquetas internas o sea establecido los VC LSPs en ambas direcciones. Se debe tomar en cuenta que una vez establecidos los túneles (PE1-PE2 y pE2 y pE1) los mismos pueden ser usados por varios clientes, es decir transportar varios VC LSPs, como se observa en la Figura N o. 16.

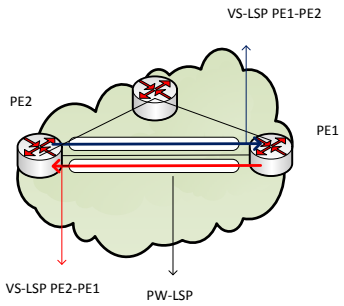


Figura No 16.- VPWS

- **Flujo de un paquete:**

A continuación se describe el flujo de paquetes una vez establecidos los túneles y los VC LSPs (URQUIZA, 2011):

1. Una trama Ethernet del cliente es switcheada o ruteada por un CE hasta un router PE (Provider Edge) también conocido como router de borde de etiqueta MPLS(MPLS Label Edge Router) o LER.

2. El router de borde determina a que VLAN pertenece la trama, fijándose en el encabezado 802.1q o determinándolo a partir del puerto de entrada.

3. Luego de que se determinó la validez del paquete, éste se mapea a una FEC definida para el usuario que determina como serán reenviados los paquetes. Mediante el FEC se determina el puerto de salida y dos etiquetas. La primera etiqueta del stack es la etiqueta de túnel y se utiliza para transportar la trama a través del backbone del proveedor. La segunda etiqueta del stack es la

etiqueta del VC y se utiliza por el router de egreso para determinar cómo procesar la trama.

4. Luego de agregar los dos encabezados MPLS (uno por cada etiqueta), la trama se encapsula según el formato correspondiente a la interfaz de salida, est6o se puede ver en la Figura No. 17.

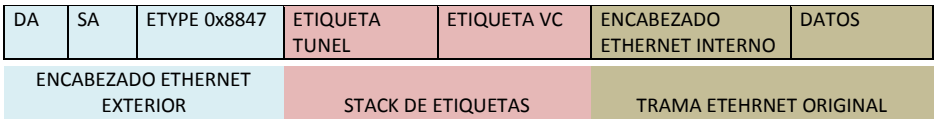


Figura No 17.-Trama Ethernet con paquete MPLS.

5. Los routers del backbone (LSRs), solo se fijan en la etiqueta de más arriba del stack para enviar la trama a través el dominio MPLS. La etiqueta de más arriba del stack en general se elimina en el penúltimo salto (PHP). Debido a la jerarquía de tunelización de MPLS, la etiqueta del VC no está visible hasta que la trama llega al LER de egreso.

6. El LER de egreso infiere cómo proceder según la etiqueta de VC y reenvía la trama por el puerto apropiado. Basado en la etiqueta de VC el LER de egreso determina el tipo de tráfico que se está transportando y cómo manejarlo. Para el caso de tráfico Ethernet, la etiqueta de VC puede ser usada para determinar la VLAN a la que pertenece y el puerto de salida. El LSP VC crea un túnel por cliente que aísla el tráfico entre un cliente y otro, ofreciendo el mismo nivel de seguridad que Frame Relay o ATM.

- **VPN capa 2 multipunto virtual private LAN service (VPLS).**

VPLS(Virtual private Lan Service), es una VPN de capa 2 multipunto que permite la interconexión de múltiples sitios en un mismo dominio de broadcast sobre una red IP/MPLS. Todos los sitios de clientes en una VPLS aparecen como pertenecientes a una misma LAN. Las VPLS brindan al usuario una interfaz Ethernet, simplificando la conexión LAN-WAN permitiendo el aprovisionamiento de servicio en forma más rápida y eficiente.

- **Funcionamiento:**

A.- fase de descubrimiento y señalización:

Se crea los LSPs externos (túneles) e internos (VC LSPs).

1. La red MPLS se encuentra funcionando y existe una malla de túneles entre los cuatro PE´s que la integran. Como los mismos son unidireccionales esto implica que existe señalizados 12 túneles.

2. Los PE´s: PE1, PE2 y PE3 participan de la VPLS por lo que s e establece una malla de PW entre ellos. Esto implica señalización de 6 VC LSP´s los cuales utilizarán los túneles previamente establecidos.

B.- Aprendizaje de direcciones MAC y envío de paquetes:

1. Una vez establecida la VPLS (todos los LSP´s externos e internos señalizados) se puede enviar el primer paquete y comenzar el proceso de aprendizaje de MAC´s (URQUIZA, 2011).

2. En la Figura No. 18, M1, M2, M3 y M4 son estaciones de trabajo que pertenecen a la VPLS en estudio.

3. Si M3 envía un paquete a PE2 con destino M1:

    a. PE2 recibe el paquete y aprende que la MAC correspondiente a M3 puede ser alcanzada en el puerto 1/1/2:0. De esta forma PE2 ingresa dicha información en la FIB correspondiente a la VPLS en cuestión.
    b. PE2 aún no sabe por dónde alcanzar la dirección MAC de M1, por lo que procede (al igual que un switch convencional) a realizar un "flooding" del paquete enviándolo por todas sus interfaces menos por donde lo recibió. De esta forma PE2 envía el paquete a PE1 con la

etiqueta asignada al PE2-1(VC LSP) a través del túnel MPLS exterior que une PE2 con PE1 y a PE3 con la etiqueta VC de PE2-3 (en el túnel correspondiente).

c. PE1 aprende de la etiqueta PE2-1 que la dirección MAC de M3 está detrás de PE2 y lo guarda en la FIB correspondiente a la VPLS.
d. PE3 aprende de la etiqueta de PE2-3 que la dirección MAC de M3 está detrás de PE2, y lo guarda en la FIB correspondiente a la VPLS.
e. PE1 saca la etiqueta de PE2-1, y como no sabe por dónde alcanzar dicha MAC inunda el paquete por los puertos 1/1/1:100 y 1/1/1:200. PE1 inunda el paquete a PE3 aplicando la regla de Split horizon (no enviar al que envío).
f. PE3 saca la etiqueta de PE2-3 y como no sabe por dónde alcanzar dicha MAC inunda el paquete por el puerto 1/1/2:0. PE3 no inunda el paquete a PE1 aplicando la regla de Split horizon.
g. Cuando M1 recibe el paquete de M3, responde con un paquete a M3.
h. PE1 recibe el paquete de M1 y aprende interfaz local 1/1/1:100 y guarda la correspondiente a la VPLS.
i. PE1 sabe que M3 puede ser alcanzado vía PE2 por lo que solo envía el paquete a PE2 utilizando la etiqueta de PE1-2.
j. PE2 recibe el paquete para M3 y como sabe que puede alcanzar a M3 por el puerto 1/1/2:0 lo envía.
k. M3 recibe el paquete.

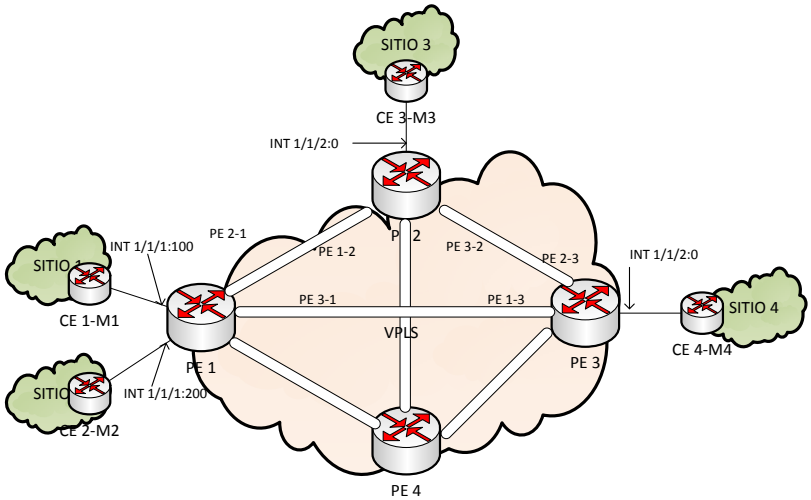


Figura No 18.- VPLS funcionamiento

- **VPN BGP/MPLS:**

Las VPNs de capa 3 basadas en el PE (borde de proveedor) conectan varios sitios, permitiéndoles hacer comunicaciones basadas en direcciones IP. Los routers PE son responsables del mantenimiento de contextos IP diferentes para cada VPN y del aislamiento del tráfico de distintas VPNs. En consecuencia, los dispositivos CE (borde de cliente) no requieren ningún cambio ni ninguna funcionalidad adicional para conectarse a una VPN en lugar de a una red privada clásica.

La solución de VPN de BGP/MPLS IP es el método más popular de VPN basada en PE. No sólo es el único adoptado como estándar propuesto por el IETF, sino que también está soportado por los principales fabricantes de routers.

Cada PE debe mantener una instancia de ruteo por cliente conectado (VRF-VPN Routing and forwarding) o sea aprender IP´s de los clientes.

- **Componentes:**

En el contexto de la RFC 2547 bis, una VPN es una colección de políticas que controlan la conectividad entre sitios. Un sitio de cliente se conecta a la red del proveedor de servicio por uno o más puertos, donde el proveedor de servicio asocia cada puerto con una tabla de ruteo de una VPN. En términos de la RFC2547 bis, a la tabla de ruteo de la VPN se le denomina VPN routing and forwarding (VRF). Para esto sus componentes son (URQUIZA, 2011):

CE: Equipo Customer Edge, provee al cliente acceso a la red del proveedor de servicios a través de uno o más provider edge (PE). El CE típicamente es un router que establece una adyacencia con el PE al cual se conecta y publica IP´s hacia el PE y aprende IP´s de los sitios remotos de la VPN a través del PE.

PE: Provider Edge Router, intercambian información de ruteo con los CE´s utilizando rutas estáticas, RIPv2, OSPF o EBGP. Si bien los PE´s mantienen información de ruteo de las VPN, solo se requiere que mantengan rutas de las VPN´s a las cuales está directamente conectado.

Cada PE mantiene una VRF por cada una de las VPN´s directamente conectadas. Una vez aprendidas las rutas de la VPN desde el CE, el PE intercambia información de ruteo con otros routers PE utilizando IBGP. Finalmente cuando se utiliza MPLS para enviar el tráfico de la VPN a través de la red del proveedor de servicio, el PE de ingreso funciona como el LSR de ingreso y el PE de egreso como el LSR de egreso.

P: Provide Routers, es cualquier router en la red del proveedor de servicio, que no se conecta a dispositivos CE.

- **Dirección VPN-IPv4:**

Si BGP convencional ve dos rutas distintas con un mismo prefijo IPv4 (cuando un mismo prefijo se asigna a dos sistemas en distintas VPN´s), trata los prefijos como equivalentes e instala una sola ruta al destino, quedando uno de ellos inaccesible.

Para evitar este problema se requiere un mecanismo que permite eliminar dicha ambigüedad RFC 2547 bis soluciona esto mediante la definición de direcciones VPNIPv4, como se muestra en la Figura No. 19.

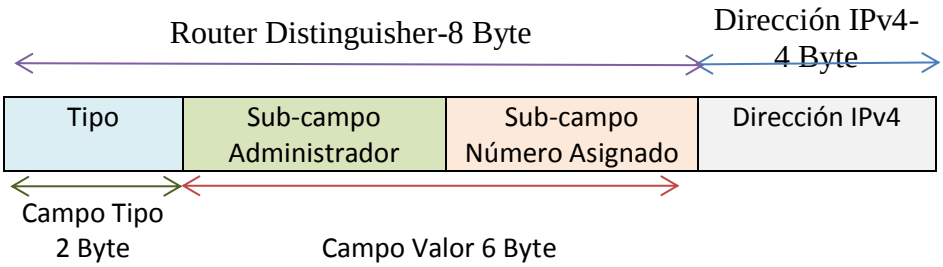


Figura No 19.- Dirección VPNIPv4.

En resumen los routers PE (Provider Edge) se conectan a los routers CE (Customer Edge) y distribuyen la información que contienen sobre las VPNs a otros routers PE a través del protocolo MP-BGP o Multiprotocolo BGP, en este intercambio de información el router PE agrega como prefijo a la dirección IPv4 una cantidad de 64 bits conocidos como **Route Distinguisher (RD)** lo que permite a la dirección IPv4 hacerla globalmente única (ruta privada) y resultando finalmente una

dirección de 96 bits denominada VPNv4. El campo RD se compone de (URQUIZA, 2011):

Un campo Tipo (2 Bytes): determina el tamaño de los sub-campos que componen el campo valor, así como el significado del campo Administrador. Actualmente hay tres valores definidos para el campo Tipo (Type): 0, 1 y 2.

- Para Tipo=0: El subcampo Administrador contiene 2 bytes y el sub-campo Número asignado contiene 4 bytes. El campo Administrador debe contener Número de Sistema Autónomo (ASN-Autonomous System Number) preferentemente público, no se recomienda el uso de un número del espacio privado. El sub-campo Número Asignado contiene un valor de un espacio de numeración administrado por el proveedor de servicio que brinda la solución (o sea un número cualquiera de 4 bytes a elección del proveedor de servicio).

- Para Tipo=1: El sub-campo Administrador contiene 4 bytes y el sub-campo Número Asignado contiene 2 bytes. El sub-campo Administrador contiene una dirección IPv4. El sub-campo Número Asignado contiene un valor de un espacio de numeración administrado por el proveedor de servicio que brinda la solución.

- Para tipo=2: El sub-campo Administrador contienen 4 bytes y el sub-campo Número Asignado contiene 2 bytes. El sub-campo Administrador contiene un número de sistema autónomo BGP-AS4. El sub-campo Número Asignado contienen un valor de un espacio de numeración administrador por el proveedor de servicio que brinda la solución.

- **Modo de operación:**

Antes de distribuir rutas locales a otros PE´s, el PE de ingreso adjunta el atributo RT (**Route Target**) a cada una de las rutas aprendidas de los sitios directamente conectados. El Route target adjunto a la ruta se basa en el valor de Export Target

Policy configurado en la VRF. Dicha funcionalidad brinda una gran flexibilidad a la solución.

El PE de ingreso puede configurarse para asignar un único RT a todas las rutas aprendidas de un sitio. El PE de ingreso puede configurarse para asignar un RT a un grupo de rutas y otro RT distinto a otro grupo de rutas aprendidas del mismo sitio.

Antes de instalar rutas remotas que fueron distribuidas por otros PE´s, cada VRF en un PE de egreso se configura con una política de importación de rutas (Import Target Policy). Un router PE puede solamente instalar una ruta VPN_IPv4 en una VRF si el RT transportado con la ruta coincide con alguna de las VRF Import Target.

Esta funcionalidad permite que un proveedor de servicios implemente para sus clientes un gran número de políticas de conectividad entre sitios. Mediante la configuración de políticas de Export Target y de Import Target, el proveedor puede construir diferentes tipos de topologías de VPN´s. El mecanismo utilizado para implementar las distintas topologías de VPN´s es aplicado por el proveedor de servicios y es transparente para el cliente.

Para que una nueva ruta sea aceptada el valor de su ruta objetivo de salida (exportación) debe de coincidir con el valor de entrada (importación) del dispositivo de entrada.

La operación con VPN MPLS MP-BGP tiene muchas ventajas sobre otros tipos de VPN como las VPN IPSEC en principio con una VPN MPLS MP-BGP el cliente que solicita la VPN tiene una topología de malla completa lo cual implica que todos los sitios tienen comunicación directa entre ellos, esto añade redundancia a la solución y también reduce puntos de fallos únicos de la red como ocurre en una topología hub. Otra ventaja muy importante es la capacidad de añadir QoS extremo a extremo en la VPN tomando en cuenta los enrutadores del SP, con otras VPN esto no es realizable ya que se crea un túnel sobre la red del SP sin la posibilidad de configurar los enrutadores del SP. Con VPN MPLS MP-BGP se tiene una plataforma

disponible para agregar multimedia a la red con servicios como video conferencias de una manera mucho más transparente que con otras VPN. Con una VPN MPLS MP-BGP se tiene una mayor escalabilidad que con cualquier otra VPN ya que se puede agregar un nuevo sitio que requiere configurar en su correspondiente PE (ICARAN).

- **Ejemplo de operación:**

Se asume la siguiente red MPLS para implementar VPN´s BGP/MPLS. Las políticas configuradas para conectividad entre sitios establecen que:

- Cualquier equipo del sitio 1 puede comunicarse con cualquier host del sitio 2.
- Cualquier equipo del sitio 3 puede comunicarse con cualquier host del sitio 4.

Se asume que se utiliza RSVP para establecer los LSP a través de la red MPLS, la figura muestra los túneles establecidos en ambas direcciones así como las etiquetas por cada uno de los routers. El router CE distribuye sus rutas IPv4 a su PE. Como se muestra la Figura No 20, hay varios mecanismos que pueden ser utilizados por el PE para aprender rutas del CE directamente conectado:

- Rutas estáticas, se configuran en el PE en forma estática las rutas alcanzables detrás del CE.
- Protocolo IGP(RIPv2, OSPF) con el CE.
- Estableciendo conexión EBGP con el CE.

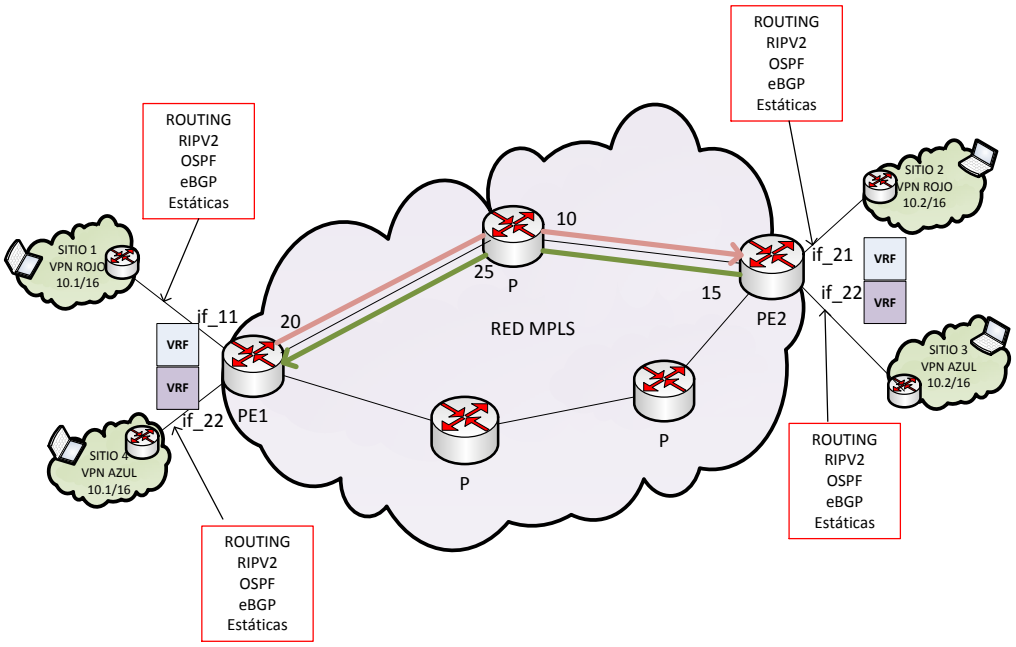


Figura No 20.-Establecimiento de los LSP´s e intercambio de rutas CE-PE

El PE realiza una serie de funciones durante el intercambio de información de ruteo con el CE:

- Crea y mantiene la VRF para cada sitio directamente conectado.
- Chequea que las rutas aprendidas del CE cumplan con las políticas de importación configurada y de ser así, las ingresa a la VRF como una ruta IPv4.
- Antes de programar la ruta, el PE le asigna una etiqueta.
- Si la ruta es aprendida por un enlace punto a punto, la etiqueta es asignada basada en la interfaz lógica de entrada. En caso de un enlace punto a punto, se le asigna la misma etiqueta a todas las rutas.
- Si las rutas son aprendidas en un medio compartido como Fast Ethernet, la etiqueta es asignada basada en el CE que advierte el prefijo. El caso de un medio compartido, todas las rutas de un CE son asignadas a una misma etiqueta.

Acciones realizadas por PE1:

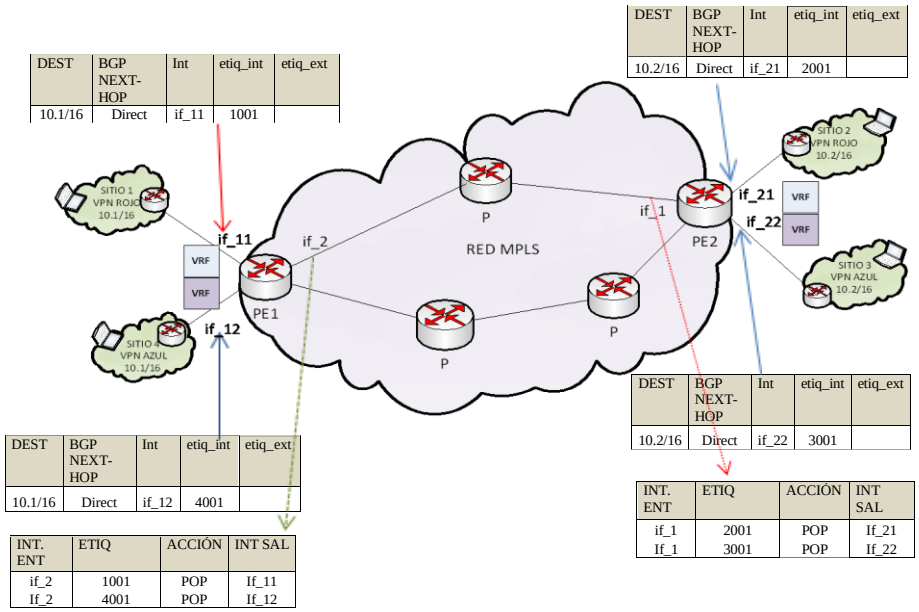


Figura No 21.-Tablas de forwarding MPLS.

Según se muestra en la Figura No 21, PE1 asigna la etiqueta 1001 a todas las rutas aprendidas del Sitio 1 y la etiqueta 4001 a las aprendidas del Sitio 4. El PE1 crea dos entradas en su tabla de forwarding MPLS de forma que cuando recibe un paquete de la red con la etiqueta 1001 o 4001, simplemente realiza un POP de dicha etiqueta y envía el paquete IPv4 directamente al CE del sitio 1 o al del sitio 4 basándose en dicha etiqueta.

De esta forma las VRF´s en PE1 contiene las rutas locales como se indica en la figura.

Acciones realizadas por PE2:

PE2 asigna la etiqueta 2001 a todas las rutas aprendidas del Sitio 2 y la etiqueta 3001 a las aprendidas del Sitio 3. El PE2 crea dos entradas en su tabla de forwarding MPLS de forma que cuando recibe un paquete de la red con la etiqueta 2001 o 3001, simplemente realiza un POP de dicha etiqueta y envía el paquete IPv4 directamente al CE del sitio 2 o al del sitio 3 basándose en dicha etiqueta.

De esta forma las VRF´s en PE2 contiene las rutas locales como se indica en la figura.

- **Distribución de rutas entre PE de ingreso y PE de egreso:**

1. El PE de ingreso utiliza el protocolo MP-IBGP para la distribución de las rutas recibidas de los sitios que tienen directamente conectados hacia el PE de egreso. Los routers PE´s deben mantener una malla de sesiones MP-IBGP entre todos los PE´s para asegurar que la información de ruteo pueda ser distribuida a todos.

2. Antes que el PE de ingreso distribuya las rutas locales de las VPN´s a sus pares MP-IBGP, convierte cada dirección IPv4 en una dirección VPN-IPv4 utilizando el RD configurado para VRF en cuestión. La publicación de cada ruta contiene la siguiente información:

- La dirección VPN-IPv4 para la ruta (ejemplo Figura No 22: RD_1:10.1/16, PE1 VPN roja).
- El next hop BGP que contiene la dirección de loopback del PE de ingreso. La dirección se codifica como una dirección VPN-IPv4 con RD=0 dado que MP-BGP requiere que el next hop sea un miembro de la misma familia de la ruta que se publica o sea una dirección VPN-IPv4.
- La etiqueta MPLS que fue asignada a la ruta por el PE de ingreso, cuando aprendió la ruta del CE directamente conectado (1001, PE1 VPN roja).
- Un atributo Route Target basado en la política de Export Target configurada localmente para la VRF en cuestión.

3. Cuando el PE de egreso recibe la dirección VPN-IPv4 de su par MP-IBGP, compara la ruta con todas las Import Target Policy (políticas de importación) que tiene localmente configuradas de todas las VPN´s que están directamente conectadas a dicho PE. Si la RT (Route Target) transportada con la ruta coincide con la Import target Policy de al menos una de las VRF´s, la ruta VPN-IPv4 se instala en la tabla VPN-IPv4 RIB(Routing Information Base). La VPN-IPv4 RIB es una gran tabla de

ruteo que contiene todas las rutas que cumplen con alguna política de Import Target configuradas en alguna VRF del PE. Esta tabla es la única que utiliza el RD para distinguir las rutas porque es la única que contienen todas las rutas de todas las VPN´s directamente conectadas al PE. Las rutas en esta tabla deben ser globalmente únicas porque si bien las direcciones IPv4 pueden repetirse, el RD asignado debe ser globalmente único.

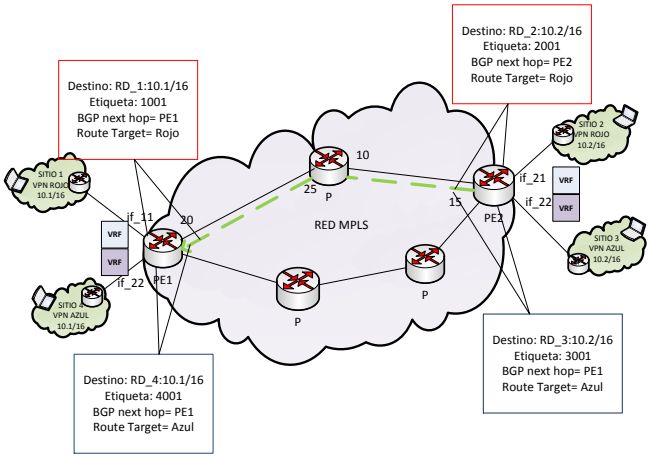


Figura No 22.- Publicación de rutas por los PE´s.

Publicación de rutas por el PE de ingreso:

Como se muestra en la Figura No 22, el PE1 publica las rutas a sus pares MP-IBGP, de igual manera lo realiza el PE2.

- **Instalación de las rutas por el PE de egreso:**

A continuación se describe como el PE de egreso aplica los filtros y luego instala las rutas remotas del PE de ingreso.

PE1 instala las rutas:

PE1 instala las rutas de su par PE2 en la VRF roja:

Destino= RD_2:10.2/16 (dirección VPN-IPv4)

Etiqueta=2001.

BGP Next Hop= PE2.

Route Target= Rojo.

PE1 instala las rutas de su par PE2 en la VRF Azul:

Destino= RD_3:10.2/16 (dirección VPN-IPv4)

Etiqueta=3001.

BGP Next Hop= PE2.

Route Target= Azul.

PE2 instala las rutas:

PE2 instala las rutas de su par PE1 en la VRF roja:

Destino= RD_1:10.1/16 (dirección VPN-IPv4)

Etiqueta=1001.

BGP Next Hop= PE1.

Route Target= Rojo.

PE2 instala las rutas de su par PE1 en la VRF Azul:

Destino= RD_4:10.1/16 (dirección VPN-IPv4)

Etiqueta=4001.

BGP Next Hop= PE1.

Route Target= Azul.

Una vez intercambiadas todas las rutas, el contenido de las VRF´s en los PE´s se muestra en la Figura No 23:

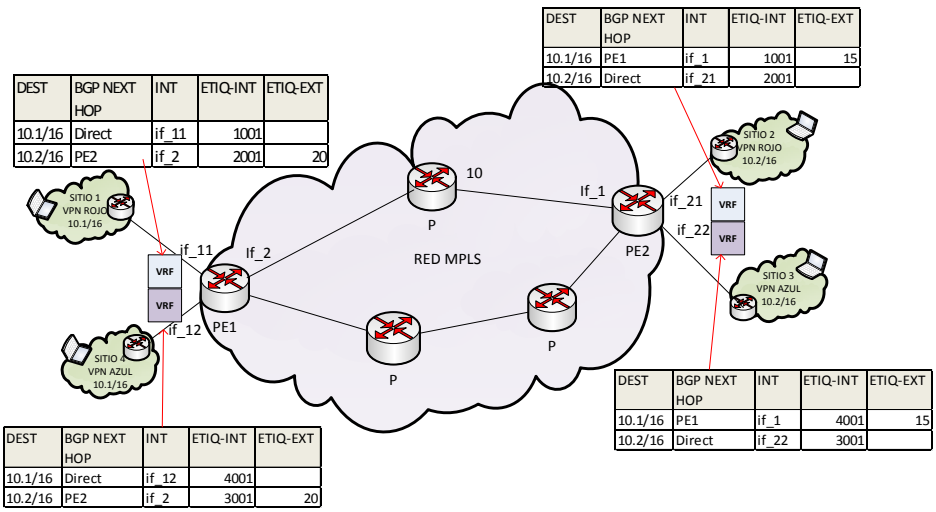


Figura No 23.- Contenido de las VRF´s

NOTA:

La etiqueta interna se intercambió utilizando MP-IBGP e identifica el CE por el cual se aprendieron las rutas.

La etiqueta externa es la que permite llegar de un par MP-IBGP a otro y se intercambió directamente mediante algún protocolo de distribución de etiquetas en este caso RSVP.

- **Distribución de rutas del PE de egreso al CE:**

Existen varios mecanismos para que el CE pueda aprender las rutas del PE, como se muestra en la Figura No. 24 y son:

- Corriendo un protocolo IGP (RIPv2, OSPF) con el PE.
- Estableciendo una conexión EBGP con el PE. El PE puede mediante el protocolo de ruteo distribuir al CE una ruta por defecto apuntando al PE.
- El CE puede ser configurado con una ruta estática por defecto apuntando al PE.

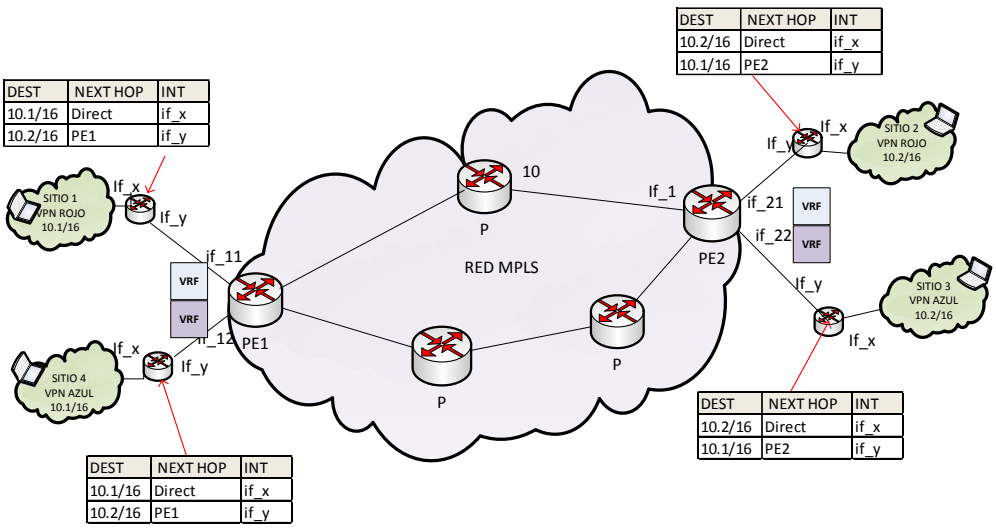


Figura No 24.- Tablas de ruteo en los CE´s.

- **Envío de tráfico de una VPN BGP/MPLS:**

A continuación se ejemplarizará un tráfico del Sitio 1 al Sitio 2 de la VRF Roja. Se supone que el equipo IPv4=10.1.5.6 del sitio 1 quiere transferir un paquete de datos del equipo con IPv4= 10.2.7.4. La Figura No 25 muestra el proceso seguido de dicho tráfico (URQUIZA, 2011):

1. El equipo con IP=10.1.5.6 envía un paquete con destino la IP=10.2.7.4.
2. El CE recibe dicho paquete y realiza una búsqueda en su tabla de ruteo IP (Figura No 24: Tablas de ruteo en los CE´s). De esta forma el CE1 envía un paquete IPv4 por su interfaz if_y al PE1.
3. PE1 recibe el paquete IP por su interfaz if_11, como todos los paquetes que llegan por esa interfaz pertenecen a la VRF Roja, busca en la tabla de forwarding correspondiente a dicha VRF (ver Figura No 22 contenido de las VRF´s). El PE1 agrega un encabezado MPLS y realiza un push de la etiqueta 2001 etiqueta interna (asignada por el PE2 para alcanzar el prefijo IP 10.2/16), luego haciendo uso del stack de etiquetas agrega un nuevo encabezado MPLS con una nueva etiqueta (etiqueta externa) haciendo un nuevo push con el valor de 20 subiendo así el tráfico al LSP que lleva de PE1 a PE2.
4. El paquete se envía al router IP de tránsito en el LSP de PE1 a PE2. El IP realiza el intercambio de etiquetas, cambiando la etiqueta externa 20 por la 10.
5. Cuando el PE2 recibe el paquete MPLS por su interfaz if_1, busca en su tabla de forwarding MPLS (Figura No 20: Tablas de forwarding MPLS). Como resultado de esa búsqueda, PE2 realiza el POP de las etiquetas y envía el paquete como un paquete IPv4 por su interfaz if_21 al CE2.
6. Cuando el paquete IPv4 arriba al CE2, dicho router busca en su tabla de ruteo IP y como resultado el paquete IP se va por su interfaz if_x a la máquina de destino IP=10.2.7.4.

7. Si se emplea PHP (penultimate Hop Popping) como se indica en la Figura No. 25, el rouer P, retitra la etiqueta externa (20) hace un POP y el PE2 solo retira la etiqueta interna (2001).

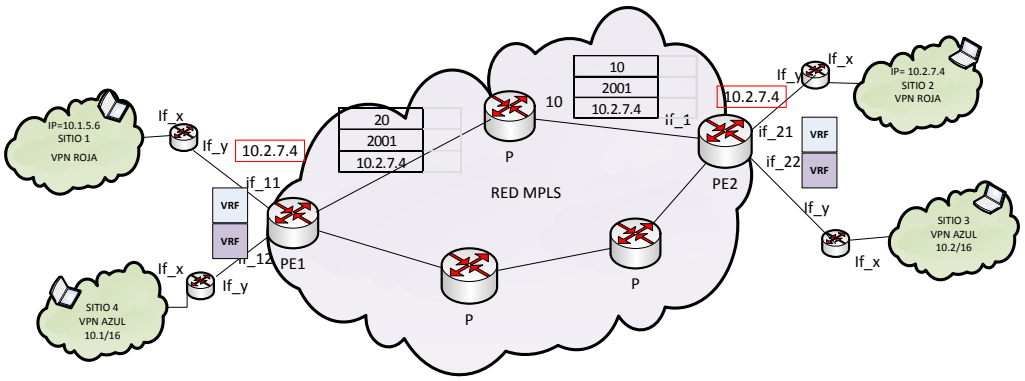


Figura No 25.- Tráfico en VPN´s BGP/MPLS CON PHP.

1.4.2.- Ingeniería de Tráfico (TE):

Es una facilidad que ofrece MPLS para adaptar los flujos de tráfico a los recursos físicos de la red, equilibrando de forma óptima la utilización de los mismos, de manera que no haya recursos utilizados excesivamente y otros no, con lo que se provocaría cuellos de botella y colapso de los enlaces.

Con la Ingeniería de Tráfico es factible desviar parte del tráfico cursante por otro camino alternativo menos congestionado aunque no sea la ruta más corta, teniendo el administrador de la red la posibilidad de:

1. Establecer rutas explícitas especificando el camino LSP exacto (cobre, fibra óptica, etc.)
2. Rutas restringidas para el caso de servicios especiales.
3. Calcular la ruta más eficiente en base a los requerimientos y restricciones.
4. Obtener informes estadísticos sobre el tráfico que cursa constituyendo una herramienta eficaz para el análisis de la distribución de los recursos de la red y para una planificación futura.

Existen dos aproximaciones: TE-RSVP y CR-LDP, ambas utilizan el encaminamiento explícito para crear los LSPs e introducen una sobrecarga de

información adicional al crear, mantener y destruir un LSP, pero ésta, es mínima comparada con la generada al procesar la cabecera IP.

- **TE-RSVP.**

TE-RSVP (Trafic Engneering – RSVP) es una extensión del protocolo RSVP.

RSVP: Es un protocolo de señalización que reserva la capacidad solicitada por un flujo en todos los routers del camino. Es un protocolo orientado a conexión, por lo que requiere guardar información de estado en todos los routers que conforman el trayecto.

Es un protocolo diseñado principalmente para tráfico multicast y aunque no es un protocolo de routing, utiliza los protocolos que sí lo son para su funcionamiento.

TE-RSVP es un protocolo de señalización *soft state* que utiliza UDP o datagramas IP para la comunicación entre LSR´s.

- **Creación de un ER-LSP:**

1. El LER de entrada quiere establecer un nuevo LSP hacia el LER de salida. Los parámetros de tráfico determinan por dónde debe pasar la ruta, así que el LER de entrada envía un mensaje PATH con la ruta explícita hacia el LER de salida y con los parámetros de tráfico que requiere la sesión.
2. Cada nodo de la ruta que recibe el mensaje determina si es la salida para ese LSP, si no lo es, sigue enviando el mensaje PATH eliminándose de la ruta. En cualquier caso cada LSR creará una nueva sesión.
3. Una vez llega al LER de salida, éste determina qué recursos ha de reservar y devuelve un mensaje RESV que distribuirá la etiqueta que ha elegido para ese LSP y contendrá los detalles de la reserva.
4. Los LSRs intermedios emparejan los mensajes PATH y RESV que han recibido según el identificador de LSP, reservan los recursos que indica RESV, asignan una etiqueta para el LSP, rellenan la tabla de envío y envían la nueva etiqueta en otro mensaje RESV.

5. El LER de entrada, cuando lo recibe, enviará un mensaje de confirmación RESVConf para indicar que se ha establecido el LSP.
6. Después de haberse establecido el LSP se enviarán mensajes periódicos para mantener el camino y las reservas.

- **CR-LDP.**

CR-LDP (Constraint-based LDP), a diferencia de TE-RSVP, no necesita de implementaciones adicionales ya que está basado en LDP y utiliza su misma estructura para los mensajes.

Es un protocolo *hard state* y utiliza sesiones TCP entre compañeros LSR.

- **Creación de un ER-LSP:**

1. El LER de entrada quiere establecer un nuevo LSP hacia el LER de salida. Los parámetros de tráfico determinan por dónde debe pasar la ruta, así que el LER de entrada reserva los recursos que necesita y envía un mensaje LABEL_REQUEST con la ruta explícita hacia el LER de salida y con los parámetros de tráfico que requiere la sesión.
2. Cada nodo de la ruta que recibe el mensaje reserva los recursos y determina si es la salida para ese LSP, si no lo es, sigue enviando el mensaje LABEL_REQUEST eliminándose de la ruta. Puede reducir la reserva si los parámetros de tráfico están marcados como negociables.
3. Una vez llega al LER de salida, éste realiza cualquier negociación final sobre los recursos y hace la reserva. Asigna una nueva etiqueta al nuevo LSP y la distribuye en un mensaje LABEL_MAPPING que contiene los parámetros de tráfico finales reservados para el LSP.
4. Los LSRs intermedios emparejan los mensajes LABEL_REQUEST y LABEL_MAPPING que han recibido según el identificador de LSP, asignan una etiqueta para el LSP, rellenan la tabla de envío y envían la nueva etiqueta en otro mensaje LABEL_MAPPING.
5. En cuanto llegue al LER de entrada se habrá establecido el LSP.

- **Comparación de Métodos:**

1. TE-RSVP es *soft state,* lo cual significa que la información es intercambiada cuando se establece el LSP, pero se deben enviar mensajes periódicos para notificar que la conexión todavía se requiere. Por el contrario, CR-LDP es *hard state*, es decir, toda la información se intercambia al iniciar la conexión y no se produce más información adicional hasta que el LSP se elimine.
2. El hecho que TE-RSVP sea *soft state* e introduzca una sobrecarga adicional hace que no sea escalable ya que esta sobrecarga crecerá proporcionalmente con el número de sesiones RSVP. Para evitar esto se intenta resumir la información y aprovechar un único mensaje para enviar varios mensajes de refresco.
3. CR-LDP utiliza conexiones TCP lo que hace que éstas sean más fiables y seguras, mientras que TE-RSVP utiliza UDP o datagramas IP para establecer las comunicaciones, lo que supone mayor vulnerabilidad aunque puede utilizar IPSec o algún otro esquema de encriptación.
4. Las conexiones TCP de CR-LDP permiten detectar un fallo mediante notificaciones propias de TCP. Esta notificación se procesa rápidamente así que las acciones oportunas sean iniciadas. Sin embargo, una conexión fallida en TE-RSVP será detectada cuando no se reciba un determinado mensaje de refresco y, dependiendo de cómo se haya configurado, detectar un fallo tardará segundos o minutos antes de que puedan iniciarse las acciones de recuperación.

   Ambos protocolos soportan re-encaminamiento (*re-routing*):

   - TE-RSVP puede crear una nueva ruta a partir de un salto diferente en un LSR, así, en el momento en que se detecte el fallo refrescará esta nueva ruta que pasará a ser operativa y, la antigua se eliminará cuando deje de recibir mensajes de refresco.
   - Otra alternativa que soportan ambos protocolos es crear una ruta completa alternativa mientras se usa la antigua, en el momento

que se produzca un fallo la nueva ruta será operativa y se eliminará la antigua.

- CR-LDP soporta que un LSP dé servicio a muchos *hosts* mediante la designación de FECs, mientras que RSVP sólo reserva ancho de banda a una única dirección IP (FERRER).

- **Detección de fallas:**

La habilidad para detectar la ocurrencia de una falla es una componente fundamental para brindar protección de tráfico. SDH brinda identificación de pérdida de conectividad a nivel hardware y cuando la detección de fallas no es provista a este nivel, la tarea puede ser realizada por alguna entidad superior en la red (URQUIZA, 2011).

- **Protección "end-to-end" o "Path protection"**

Este modelo establece dos LSP´s: uno primario, utilizado en operación normal y otro secundario para utilizarse en caso de falla del primario. Para disminuir el tiempo de respuesta ante una falla, el LSP secundario se pre señala quedando listo para cursar el tráfico, un mensaje de error de RSVP se propaga al head end LSR para enviar tráfico por el LSP secundario, como se observa en la Figura No. 26.

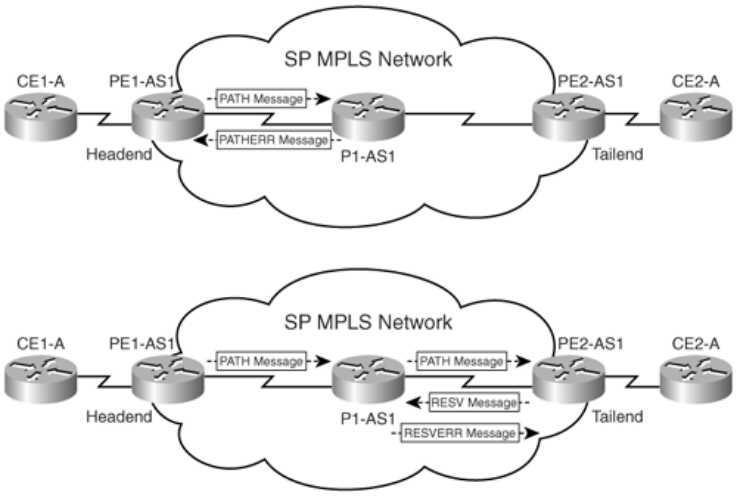


Figura No 26.- Head end and tail end.

Un problema con este tipo de respaldo, es que el mensaje de error llega al head end LSR, el tráfico continúa siendo enviado por el LSP primario por lo que los datos se siguen perdiendo.

- **Características de Path Protection:**

Control de flujo de tráfico luego de una falla: El uso de un camino secundario pre-señalizado es una herramienta muy potente porque permite un conocimiento exacto del camino que seguirá el tráfico luego de ocurrida una falla:

Diversidad de camino: El LSP primario y secundario deberán tomar caminos separados desde el origen hasta el destino.

Reserva doble de recursos: El LSP secundario usualmente se establece con la misma reserva de recursos que el primario, para así asegurar la misma calidad de servicio cuando el tráfico fluye por el camino secundario.

Protección innecesaria: Se protege todo el camino, no es posible aplicar este método en forma selectiva.

Tiempo de respuesta no determinístico: El retardo para pasar del LSP primario al secundario está determinado por el tiempo que tarda el mensaje error de RSVP en llegar al head end LSR.

- **Protección local Fast Reroute:**

Su objetivo es minimizar el tiempo durante el cual se pierde el tráfico. Para esto en lugar de implementar protección en el head end LSR (en el origen del túnel), se reenrutará el tráfico alrededor de la falla. La idea no es mantener el tráfico fluyendo a través del desvío hasta que el enlace se recupere, sino de cursar dicho tráfico hasta que el head end LSR mueva el LSP a un nuevo camino que no utilice el enlace que falló.

Los mecanismos para proveer FRR en redes MPLS fueron desarrollados por IETF y se documentan en la RFC 4090. Se clasifican basados en dos criterios:

  - El tipo de recurso que es protegido, un enlace o nodo.
  - El número de LSP´s protegidos por el túnel de protección 1:1 o 1: N.

- **Protección de enlace:**

Se refiere a la habilidad de proteger el tráfico que está siendo cursado por un LSP cuando un enlace a lo largo del LSP falla, estableciendo un túnel de respaldo en torno al enlace. El respaldo es denominado desvío en el caso 1:1 y bypass en el caso

1: N. En la Figura No 27, el nodo A donde el tráfico es desviado al túnel de respaldo se le denomina a punto local de reparación (PRL-Point of Local Repair) y el nodo B, donde el tráfico vuelve a tomar el camino original se le denomina punto de fusión (MP-Merge Point).

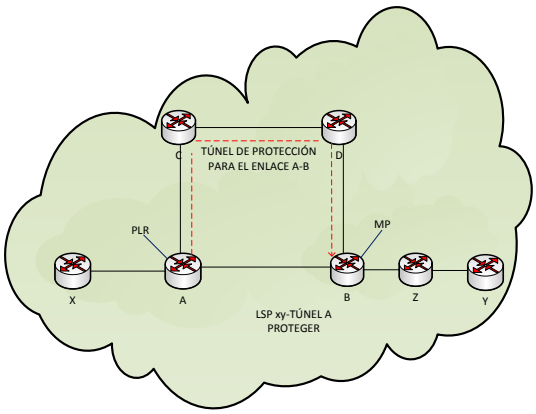


Figura No 27.- Protección de enlace.

Para informar al LSR A que el enlace a proteger será A-B, la configuración debe realizarse directamente en el router A que contiene el enlace. Mientras que a los efectos de informar del LSP a proteger, la configuración se realiza en el head end del túnel o sea el LSR X.

- **Respaldo 1: N:**

El tráfico llega por el túnel de respaldo con la misma etiqueta con la que llegaría si el mismo fuera enviado a través del túnel principal. La única diferencia desde el punto de vista del forwarding es que el tráfico llega al MP sobre una interfaz distinta. Para esto lo que necesita hacer es:

1. Poner en el PRL un segunda etiqueta (la del túnel de respaldo) encima de la etiqueta del túnel que se está protegiendo.
2. Realizar PHP para el túnel de respaldo antes del MP.

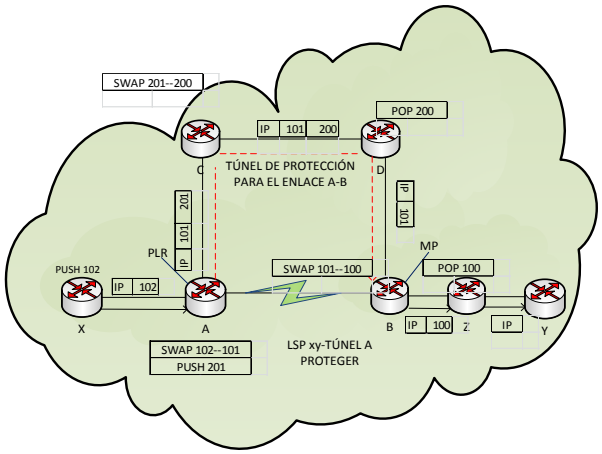


Figura No 28.- Protección de enlace 1:N- tráfico.

Este método permite que cualquier número de LSP´s atravesando el enlace A_B pueda ser protegido por el túnel de respaldo, lo cual le da a la herramienta buena escalabilidad, como se observa en la Figura No. 28.

- **Respaldo 1:1:**

El tráfico llega al MP con una etiqueta distinta al que utiliza el túnel principal, ver figura No. 29. De esta forma el MP debe mantener una entrada que asocia la etiqueta del túnel de respaldo con la del túnel principal. Por lo cual este modo requiere el ingreso de datos en la LIB del MP como del PRL.

Si un segundo LSP debe ser protegido, un nuevo túnel de respaldo debe establecerse y una nueva entrada de forwarding debe instalarse en el MP.

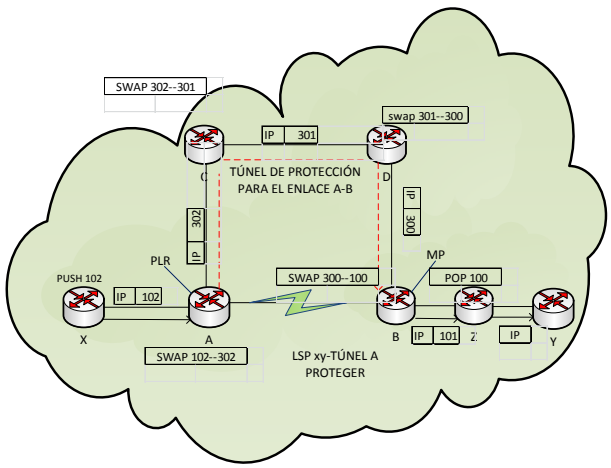


Figura No 29.- Protección de enlace modo 1:1.

- **Protección de nodos:**

En la figura No 30, se muestra el LSPxy, a lo largo del camino X-A-B-Z-Y. El LSPxy se protege contra una falla del nodo B con un túnel de respaldo que toma el camino A-C-D-Z el cual retorna el LSP xy en el nodo Z. Cuando B falla, el tráfico del LSPxy se desvía al túnel de respaldo en A y es entregado a Z, donde continúa su camino normal al destino Y.

Para esto A debe obtener dos datos:

La dirección del nodo Z, el tail end LSR del túnel de respaldo. Esta información se puede obtener del Record Route Object (RRO) de RSVP. Esta dirección se utiliza para alcanzar el MP (nodo Z).

La etiqueta que utiliza el LSP principal en el nodo Z.

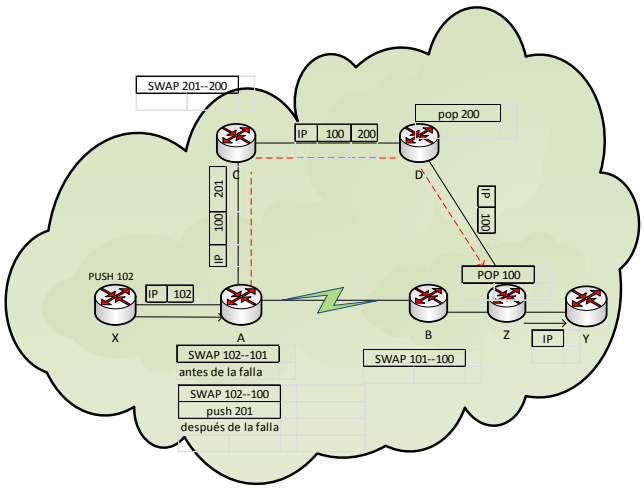


Figura No 30.- Establecimiento del túnel de protección.

1.4.3.- Calidad de Servicio (QoS):

En el área de QoS, el objetivo inicial de MPLS era el de brindar los mismos beneficios que IP, es decir soportar Differentiated Services (DiffServ).

Existen básicamente dos problemas para soportar DiffServ en MPLS. En primer lugar el campo DSCP que determina el nivel de QoS que se tiene que brindar a un paquete se encuentra en el encabezado IP, pero los LSRs solo examinan el header

MPLS para realizar el forwarding. Esto implica que para soportar DiffServ es necesario mapear el DSCP de cada paquete en el header MPLS. Esto lleva un segundo problema debido a que el campo EXP (Experimental Field), que podría ser utilizado para realizar el mapeo del DSCP en el header MPLS, tiene únicamente tres bits.

IETF propone RFC 3270 MPLS Support of Differentiated Services dos soluciones:

- **Exp-Inferred-PsC LSP(E-LSP):**

E-LSP determina el Per Hop Behavior (PHB) de un paquete únicamente con el campo EXP del encabezado MPLS, por lo que puede soportar hasta ocho PHB por cada LSP. El valor del campo EXP determina PHP Scheduling Class (PSC) (Tratamiento de queuing y scheduling que recibirá el paquete; así como el "drop precedence" (prioridad de dropeo) del paquete. El mapeo del valor del campo exp en PHB puede hacerse manualmente en cada LSR o mediante la utilización de extensiones a los protocolos de distribución de etiquetas LDP y RSVP definidas en el RFC 3270.

Se entiende por PHB al tratamiento de forwarding aplicado por un nodo que maneje Diffserv, a un conjunto de paquetes marcados con el mismo DSCP.

- **label- Only- Inferred- PSC LSP (L-LSP):**

L-LSP determina el PHB de un paquete a partir de la etiqueta y del campo EXP del encabezado MPLS. La etiqueta determina el PHB Scheduling Class (PSC) mientras que el campo EXP determina el "drop precedence". Esto implica que puedan ser soportados un número arbitrario de PHBs. En este modo se requiere la utilización de las extensiones para DiffServ realizadas a los protocolos LDP y RSVP, para poder mapear el PHB a una etiqueta determinada. Si bien este método permite la implementación de un número arbitrario de PHB, no todos los equipos soportan dicho modo por lo que es poco utilizado.

Existen cuatro estándares definidos para PHB que son:

Defautl PHB: RFC 2474, tiene un valor DSCP definido 000000, conocido como mejor esfuerzo.

Class- Selector PHB: RFC 2474, tiene siete valores DSCP desde 001000 a 111000 cada uno tiene mayor probabilidad de envío a tiempo que su predecesor.

Assured Forwarding PHP (AF): RFC 2597, ofrece distintos niveles de garantía de entrega o de calidad relativa para paquetes IP. Para esto define N clases, para cada clase se reserva recursos, de forma que los retardos y/o pérdidas de una clase sea siempre inferior a los de una clase de menor prioridad como se representa en la Figura No. 31. Dentro de cada clase los paquetes se pueden clasificar en M categorías de preferencia de descarte. Actualmente N= 4 y M=3 son definidos para uso general:

% de descarte	Clase 1	Clase 2	Clase 3	Clase 4
Bajo	AF11=001010	AF21=010010	AF31=011010	AF41=100010
Medio	AF12=001100	AF22=010100	AF32=011100	AF42=100100
Alto	AF13=001110	AF23=010110	AF33=011110	AF43=100110

Figura No 31.- Valores DSCP para AF

Expedited Forwarding PHB (EF): RFC 2598, tiene un valor DSCP 101110, que permite ofrecer un servicio punta a punta de bajas pérdidas, baja latencia, bajo jitter y ancho de banda asegurado, reservado únicamente para aplicaciones más críticas

1.5.- Conceptos de la Plataforma OPNET:

Modeler es un simulador basado en eventos orientado a la simulación de redes de telecomunicaciones creado por OPNET (Optimized Network Engineering Tools). Se lo puede definir como un simulador dinámico, porque la simulación evoluciona con el tiempo y discreto porque el comportamiento de los sistemas representados cambia únicamente en instantes concretos.

La herramienta Modeler es uno de los simuladores más avanzados en el campo de las redes de telecomunicaciones. La característica más relevante es que es un simulador orientado a objetos, lo que permite interactuar al usuario sin problemas y ofrece una gran facilidad de interpretación y creación de escenarios aparte de tener en cada objeto una serie de atributos configurables.

La herramienta diseñada por OPNET para el modelado y simulación está basada en la teoría de redes de colas mediante eventos discretos y dispone de multitud de librerías, lo que permite simular gran diversidad de redes donde intervenga un amplio número de protocolos y variables específicas que el usuario podrá modificar y estudiar. Número de paquetes perdidos, throughput, jitter, caída de enlaces y potencia de transmisión son algunos de los parámetros que se pueden controlar (RAFAEL).

El desarrollo de los modelos se realiza mediante la conexión de varios nodos, utilizando diferentes tipos de enlaces. Mediante OPNET MODELER, se deben especificar tres tipos de modelos, como se muestra en la tabla No. 3:

Tabla No 3.- Tipos de modelos OPNET

MODELO DE RED	**Redes y subredes**
MODELO DE NODOS	Nodos y estaciones
MODELO DE PROCESOS	Especifica la funcionalidad de cada nodo.

- **Teoría de colas:**

La teoría de colas es el estudio matemático del comportamiento de líneas de espera. Esta se presenta, cuando los "clientes" llegan a un "lugar" demandando un servicio a un "servidor", el cual tiene una cierta capacidad de atención. Si el servidor no está disponible inmediatamente, el cliente decide esperar entonces se forma la línea de espera. Una cola es una línea de espera y la teoría de colas es una

colección de modelos matemáticos que describen sistemas de línea de espera particulares.

Los modelos sirven para encontrar un buen compromiso entre costes del sistema y los tiempos promedio de la línea de espera para un sistema dado.

Características de las colas:

- Tiempo de llegada: El cual sigue una función exponencial, es aleatoria ya que varía con respecto al tiempo.
- Tiempo de servicio: Es el tiempo en que se demora la persona en el preciso momento que está siendo atendido.
- Tiempo en la cola: Tiempo en el que se demora la persona en ser atendido.
- Tiempo en un sistema: El tiempo total en que se demora una persona al entrar al sistema.
- Clientes: Número de clientes que se encuentran dentro del sistema.
- Servidores: Número de dispositivos que atenderán a los clientes.

1.5.1.- Modelo de RED:

Para el presente trabajo se empleará este tipo de modelo, para lo cual se describirá brevemente su funcionamiento (FIXGROUP, 2008):

a. Abrir el simulador:

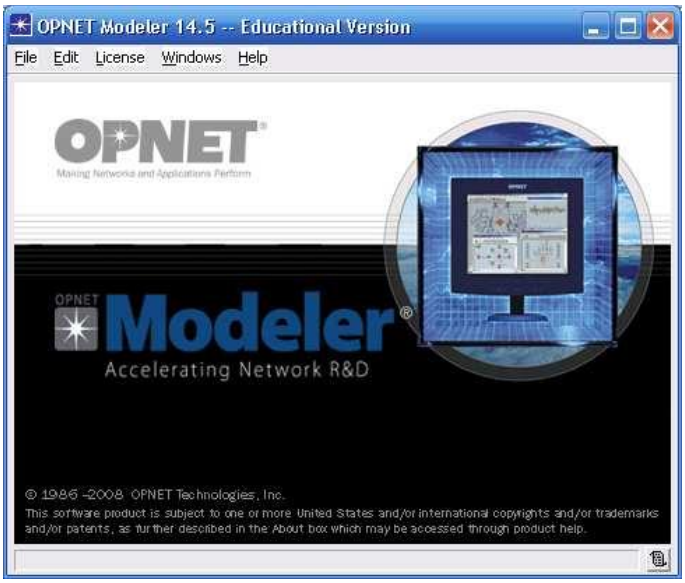


Figura No 32.- Simulador Opnet.

b. Crear un nuevo proyecto File-New-Project

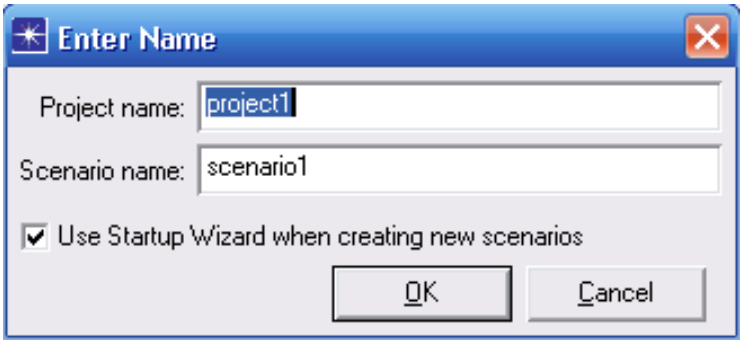


Figura No 33.- Creación de nuevo proyecto.

c. Elección del tipo de escenario.

Se escoge la primera opción create empty scenario.

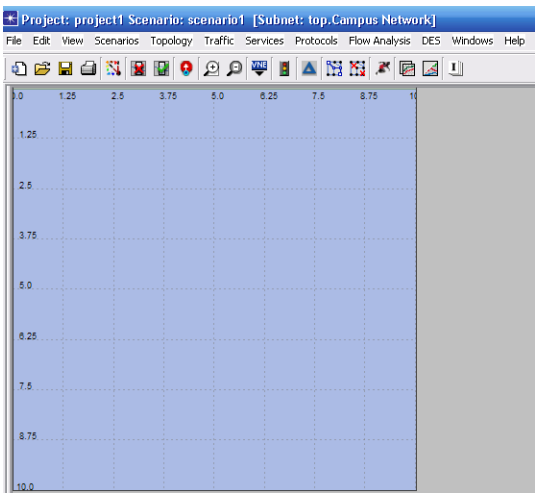


Figura No 34.- Escenario vacío Opnet.

d. Paleta de objetos:

Desde el menú topolgy-open object palette, se escoge los elementos que se desea integrar a la simulación: elementos activos y enlaces TDM e IP.

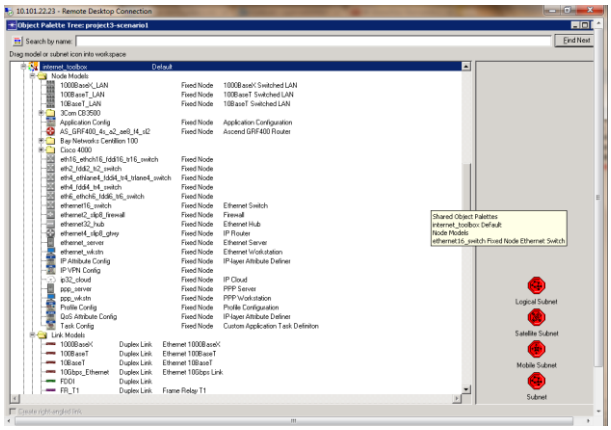


Figura No 35.- Open Object Palette.

Una parte importante en este procedimiento es la selección de Node Models, para seleccionar las aplicaciones o la forma de configurar la red o servicios. En este caso particular se seleccionará especialmente las facilidades de MPLS.

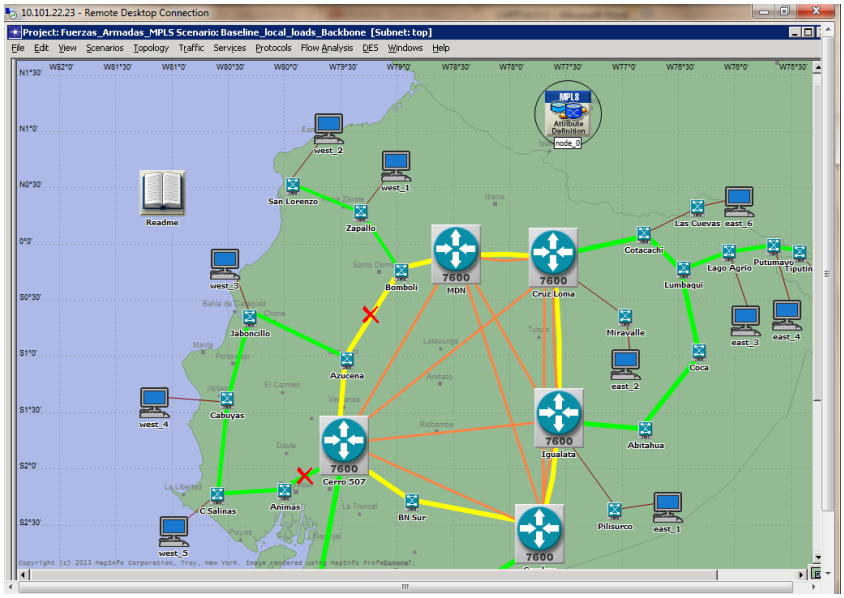


Figura No 36.- Node Models MPLS.

e. Atributos:

En el elemento seleccionado se coloca los atributos de ese elemento, mediante click derecho Edit Attributes, con esto se configura el elemento a la necesidad de la simulación.

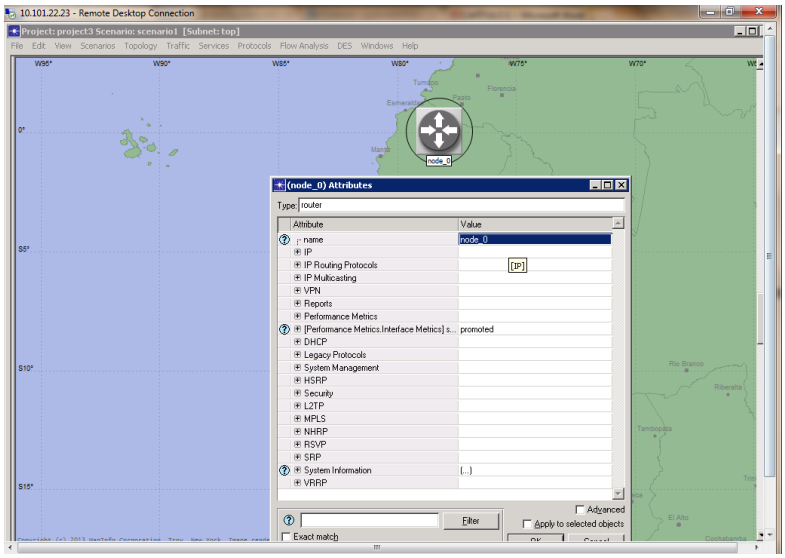


Figura No 37.-Edit Attributes.

Establecida la red y las funcionalidades sobre la cual operará, se establece la corrida de la simulación.

f. Configurar la simulación:

Para ello se accede a partir de la opción Configure/Run Discrete Event Simulation o a través del siguiente acceso directo:

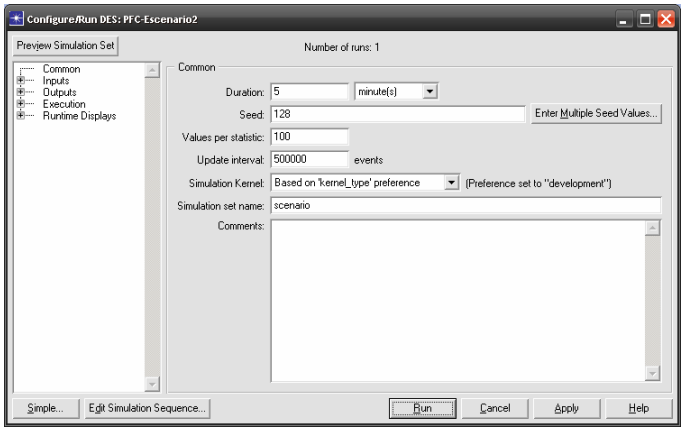


Figura No 38.-Configuración de la simulación.

En esta pantalla se puede establecer la duración de la simulación. Por lo general se pone un tiempo de simulación de 5 minutos ya que con esta duración los resultados ya muestran estadísticas fiables.

El número de eventos es el número de llegadas o salidas que se producen durante la simulación. Se establece que a mayor número de eventos, en iguales condiciones, la fiabilidad se ve incrementada.

g. Analizar los resultados:

Para analizar los resultados se va a la opción DES-Results-View Results o mediante el siguiente acceso directo:

Entre todos los resultados posibles a analizar en esta red de simulación, se pueden mostrar las gráficas del delay (retardo), jitter, tráfico recibido, tráfico enviado y throughput (rendimiento) en el enlace que une el último router con el destino. En el capítulo 4, se observarán algunos resultados obtenidos de la simulación de la propuesta para la red de datos de Fuerzas Armadas con tecnología MPLS.

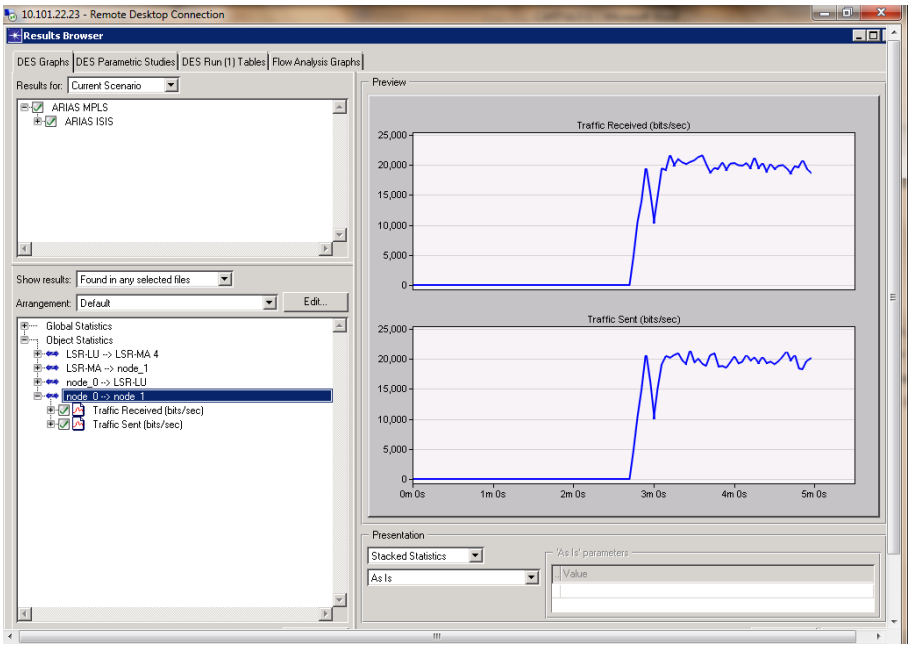


Figura No 39.-Vista de resultados.

CAPÍTULO 2
SITUACIÓN ACTUAL.

2.1.-Introducciòn.

La red MODE fue implementada en el año de 1995, mediante enlaces PDH, con capacidades de 32 E1´s[1], para servicios de voz TDM (Time Division Multiplexation). Con el avance de la tecnología y las aplicaciones en las diferentes unidades Militares se implementaron equipos activos para los aplicativos de datos, bajo un esquema general basado en la ubicación de las centrales telefónicas a nivel nacional.

Los aplicativos de las Fuerzas Armadas fueron implementados en base a requerimientos puntuales sin un dimensionamiento de uso, ni crecimiento, al igual que las aplicaciones de video conferencia. Estos servicios se han incrementado para todas las unidades militares a nivel nacional, por lo que el equipamiento actual instalado tiene una capacidad limitada, para conmutar los paquetes y proporcionar un servicio adecuado.

Las centrales telefónicas fueron implementadas en el mismo año que la red MODE, siendo necesario 1 E1 por central telefónica para un uso limitado de abonados por su tecnología TDM, en la actualidad estas centrales son híbridas, permitiendo su conexión mediante un puerto Ethernet y trasmitiendo su información en forma de paquetes, bajo la tecnología IP.

La red MODE, tiene su característica particular de tener acceso hacia lugares geográficos, en donde las operadoras telefónicas no proporcionan el servicio, por lo cual la comunicación de voz es transportada por esta red, siendo su único medio de comunicación. Adicionalmente, mediante conexiones VPN (Virtual Private Nerwok), permite el acceso a la red de las agregadurías militares ubicadas en diferentes ciudades del mundo.

[1] 32 canales de 64 Kbps

Se ha determinado además que la capacidad del backbone en sus anillos no es aprovechada en su totalidad, ya que por las características tecnológicas y de estructura de la red de datos, se asignan E1s completos para cada aplicación, siendo limitada la posibilidad de realizar una convergencia de servicios, optimización de los canales y la utilización adecuada de la red.

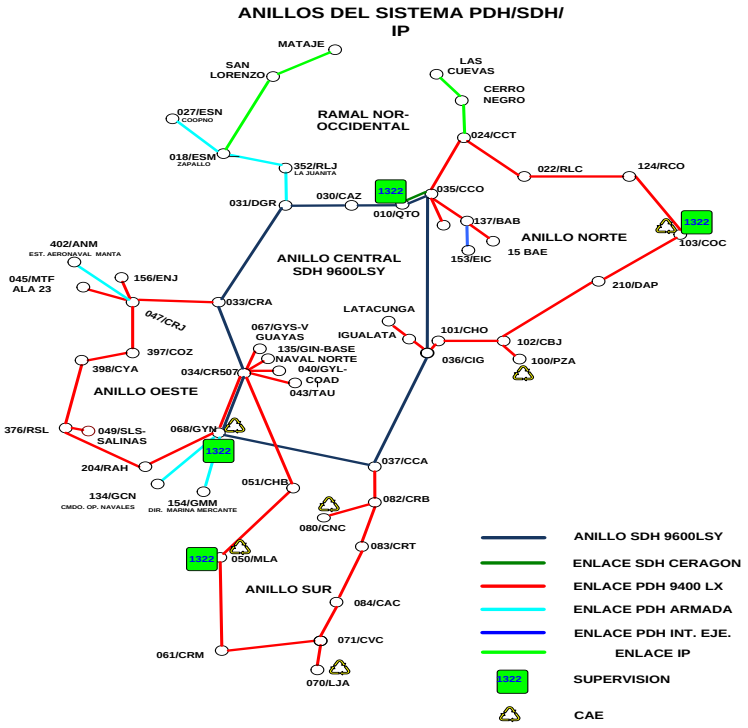


Figura No 40.- Anillos del Sistema MODE.

Como consecuencia de la falta de un diseño adecuado en la red, no se definieron políticas de su empleo, ni las consideraciones bajo las cuales deben ser implementados los servicios en cada una de las unidades militares, derivando de ello una red con servicios que no optimizan la capacidad existente para el transporte de los aplicativos, la topología de la Red MODE puede observarse en la Figura No. 40.

Con el surgimiento de MPLS en redes, nace como una idea de interés institucional de Fuerzas Armadas, la implementación de esta tecnología, que solucionaría un problema de comunicaciones, eje principal de las actividades militares, considerada además como una solución de diseño para operar sobre

cualquier tecnología, basadas en este caso particular de Fuerzas Armadas en infraestructuras PDH/SDH/SONET.

2.1.1.-Delimitaciòn.

En el presente proyecto, se determinará el estado de la red actual, partiendo de un análisis de los aplicativos que se trasportan, equipos instalados, tráfico existente en la red, consumos de ancho de banda y necesidades de los usuarios; para de esta manera definir su diseño mediante una topología y dimensionamiento de la red en base a criterios de costo mínimo con tolerancia a fallas a nivel nacional, considerando para ello los equipos adecuados basados en la tecnología MPLS.

Establecida la solución se realizará el proyecto en formato SEMPLADES y las bases técnicas de los equipos con sus respectivos costos para su posterior adquisición. Esta solución será modelada con la plataforma OPNET, que permitirá en base a tiempos de respuesta y funcionalidades de la tecnología, identificar las ventajas de la propuesta con la red actual. Finalmente se elaborará una directiva que definirá las políticas de administración, usos e implementaciones, considerando las bondades que proporciona la tecnología para cada uno de los servicios de la red de Fuerzas Armadas y que se constituirá en el direccionamiento para las Fuerzas y unidades militares que se integran a esta red.

2.1.2.-Definiciòn del problema.

El Comando Conjunto de las Fuerzas Armadas dispone de una Red de datos implementada bajo requerimientos puntuales de las unidades militares, sobre un backbone que fue diseñado y dimensionado para la transmisión de voz.

Con el avance de la tecnología, los servicios proporcionados a los usuarios de Fuerzas Armadas, se han desarrollado e incrementado mediante el transporte de paquetes bajo el protocolo IP, tal es el caso, que en la actualidad se dispone del servicio de videoconferencia y voz sobre IP; sea para usuarios locales como remotos.

Para cada servicio se establecieron canales individuales, es decir E1`s para datos, voz y videoconferencia, sobre equipos que fueron colocados sin un diseño adecuado que permita la escalabilidad y la optimización de la red, ocasionado a su vez, que la capacidad de transporte de la red MODE sea insuficiente para los requerimientos actuales de los usuarios; siendo la causa principal, la subutilización de estos canales para cada uno de los servicios establecidos.

Debido al incremento de usuarios y de servicios, la red de datos de Fuerzas Armadas tiende a saturarse. Adicionalmente, la capacidad limitada de sus equipos, no permite la convergencia y diferenciación de los servicios que permitan la optimización de los canales del backbone principal de la red MODE que mejoren la fluidez de las comunicaciones en Fuerzas Armadas.

En la actualidad no existen políticas establecidas para el empleo óptimo de la red de datos, definición de los equipos ideales para la ampliación de la misma y las condiciones bajo las cuales deben ser implementados los servicios y aplicaciones que transitan por la red.

Resumiendo los problemas que motivan el desarrollo del presente proyecto son los siguientes:

- Subutilización de E1s para los diferentes servicios implementados en cada una de las unidades militares de Fuerzas Armadas a nivel nacional.
- No existe la integración en la red de datos de las centrales telefónicas a nivel nacional con tecnología IP, así como la red de videoconferencia en alta definición para las unidades militares.
- Capacidad limitada de los equipos existentes, que no permiten aplicar QoS, balanceo de carga y funcionalidades que la tecnología actual proporciona para una red de datos, ocasionado retardo en los aplicativos especialmente en aquellos de tiempo real y que deben ser garantizados para las operaciones de Fuerzas Armadas a nivel nacional.
- Falta de una administración unificada de todo el equipamiento que maneja el protocolo IP, como lo es routers, switch, equipos de videoconferencia, centrales telefónicas, etc.

- Integración de las agregadurías militares con acceso al servicio de voz y aplicativos de Fuerzas Armadas, mediante la elaboración de VPN's, que los constituyen como abonados remotos de la red de datos.
- Falta de políticas de implementación de equipos y servicios que se transportan por la red de datos, que permitan el control y direccionamiento a las Fuerzas y unidades militares a nivel nacional.
- Carencia de un diseño estructurado de la red de datos de Fuerzas Armadas, en base a equipos y tecnología con capacidad de soportar el crecimiento, integración y convergencia de los servicios implementados.

2.1.3.-Justificaciòn.

La red de datos de Fuerzas Armadas en la actualidad se ha convertido en la base del transporte de la información en apoyo a las operaciones estratégicas, operacionales y tácticas de FF.AA. a nivel nacional, por lo cual el desarrollo del presente proyecto constituye uno de los ejes fundamentales y prioritarios en el Departamento de Operación y Mantenimiento de la Dirección de Tecnologías de la Información y Comunicaciones para el año 2014, el cual será fundamentado en un diseño óptimo bajo la tecnología MPLS, con capacidad de soportar el crecimiento, integración y convergencia de los servicios implementados.

Con este diseño se solventarán los problemas detallados anteriormente, ya que los principales servicios que proporciona la Red MODE, están transportados a través de equipos activos, que actualmente funcionan con una implementación bajo requerimientos puntuales, sin un estudio que defina la mejor ubicación de estos, topología y dimensionamiento y que permita explotar las ventaja de una tecnología adecuada para redes como lo es MPLS. Para lograr este propósito el autor del presente proyecto realizará el estudio de esta tecnología, ya que actualmente no existen profesionales con este nivel de conocimiento y que servirá de base para el aprendizaje de los técnicos operadores de la red de datos.

Para elaborar este diseño, el proyecto partirá de un análisis de la red, ya que al estar implementada mediante requerimientos puntuales, no existe un análisis de su

estado actual. Insumo necesario e importante al tratarse de una red que maneja información vital para las operaciones militares.

Definido el diseño de la red y al ser un proyecto para el Comando Conjunto de las FF.AA[2]., se elaborará el proyecto en formato SEMPLADES, así como las bases técnicas necesarias con su costo para la adquisición de los equipos. Para sustentar la propuesta se realizará el modelamiento en la plataforma OPNET, que permitirá en base a tiempos de respuesta realizar una evaluación de las ventajas del diseño propuesto a la red actual. Este trabajó será la base para justificar el proyecto a ser ejecutado por la Dirección de Tecnologías de la Información y Comunicaciones para el año 2014.

Para el gerenciamiento del diseño de la red propuesta, se elaborará una directiva para la administración, uso e implementación de servicios y equipos en la red de datos que gobiernen el desempeño técnico-operativo y administrativo de la red de datos. Esta directiva se constituirá en el direccionamiento para las Fuerzas y unidades militares, a fin de que se normalice las características mínimas y configuraciones que deben tener los equipos sobre todo al ser parte de la capa de acceso a la red de datos de FF.AA.

2.1.4.-Determinación de objetivos.

Objetivo General:

Elaborar un proyecto para la reestructuración de la red de datos de Fuerzas Armadas mediante un diseño topológico de costo mínimo, que permita la implementación de equipos con tecnología MPLS con capacidad de soportar el crecimiento, integración y convergencia de los servicios.

[2] Fuerzas Armadas.

Objetivos Específicos:

- Establecer la situación actual de la red de datos mediante un análisis de servicios, equipos, configuraciones, matriz de tráfico y configuraciones actuales, así como su crecimiento a mediano plazo.
- Determinar el marco conceptual que permita conocer los fundamentos para el diseño, topología y dimensionamiento de una red de datos, considerando la tecnología MPLS y el modelamiento de estas redes, mediante la investigación de textos, revistas y manuales técnicos.
- Diseñar la red de datos de Fuerzas Armadas mediante técnicas de costo mínimo, para proporcionar servicios convergentes sobre una plataforma MPLS.
- Evaluar la propuesta en base a tiempos de respuesta, fundamentado en el modelamiento mediante la plataforma OPNET, que permitan comparar la solución con la red de datos existente.
- Elaborar una directiva que permita establecer las políticas de administración, uso e implementación de servicios y equipos en la red de datos, considerando la tecnología MPLS.
- Establecer las conclusiones y recomendaciones de la investigación realizada del proyecto en base a la tecnología planteada para la reestructuración de la red de datos de FF.AA.

2.2.-Anàlisis de los servicios habilitados en la red.

Para el análisis de los servicios habilitados, se realizó las gestiones con las diferentes Fuerzas, quienes son las encargadas de elaborar y generar los diferentes aplicativos y servicios en cada unidad bajos su responsabilidad, pero todas dependen del sistema de Comunicaciones del Comando Conjunto de las Fuerzas Armadas, los servicios de detallan en las Tablas No. 4, 5,6,7.

a) Comando Conjunto:

Tabla No 4.- Servicios Comando Conjunto.

SERVICIOS	DETALLE
INTRANET DATOS	APLICATIVOS Fuerza Terrestre APLICATIVOS Fuerza Naval APLICATIVOS Fuerza Aérea C3I2. CORREO
OTROS SERVICIOS	VIDEOCONFERENCIA VoIP

b) Fuerza Terrestre:

Tabla No 5.- Servicios Fuerza Terrestre.

SERVICIOS	DETALLE
INTRANET DATOS	SISEG SIDDI CORREO INSTITUCIONAL SIBIE SILOG SIFIN SIGOB SIPER SISLOG SISLIN SICOS SIEDU SIACAD
OTROS SERVICIOS	VIDEOCONFERENCIA VoIP

c) Fuerza Naval:

Tabla No 6.- Servicios Fuerza Naval.

SERVICIOS	DETALLE
INTRANET DATOS	CORREO INSTITUCIONAL
	SIGMAP SISTEMA DE EVALUACIÓN DE PERSONAL
	SISLOG
	FINANCIERO
	ACTIVOS
	OPERACIONES
	APLICATIVOS WEB
OTROS SERVICIOS	VIDEOCONFERENCIA
	VoIP

d) Fuerza Aérea:

Tabla No 7.- Servicios Fuerza Aérea.

SERVICIOS	DETALLE
INTRANET DATOS	SISTEMA DE RECURSOS HUMANOS
	SISTEMA FINANCIERO
	CORREO INSTITUCIONAL
	SISTEMA DE MANTENIMIENTO
	OPERACIÓN VUELOS LOGÍSTICOS
	ABASTECIMIENTOS
	ROLES
	FINANCIERO
	ACTIVOS FIJOS
	EVALUACIÓN
	DEFENSA AÉREA
	OPERACIONES
OTROS SERVICIOS	VIDEOCONFERENCIA
	VoIP

2.3-Análisis de los equipos instalados en la red:

El análisis de los equipos instalados se realizará en base al levantamiento de la información existente en registros y sistemas de gestión, como lo es el sistema IMC

de 3COM y fundamentado en la ubicación de los nodos, estaciones repetidoras y terminales del sistema de comunicaciones MODE de FF.AA. los mismos que se observan en la Figura No. 41, de los cuales se derivan los equipos conectados por las unidades militares para sus servicios de voz, datos y videoconferencia:

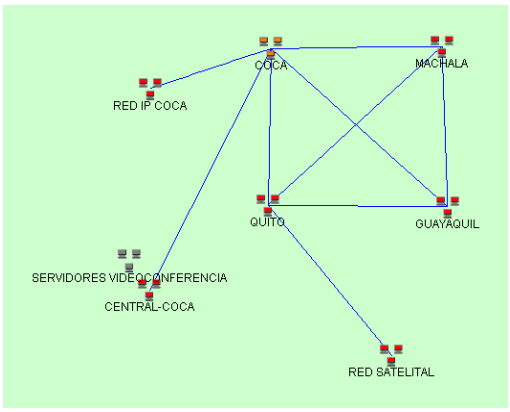


Figura No 41.- Nodos de la Red de datos.

Mediante el sistema de gestión se verificará los equipos conectados en la actual red, su marca, modelo, ubicación, así como las unidades que se conectan al mismo:

a) Nodo Quito:

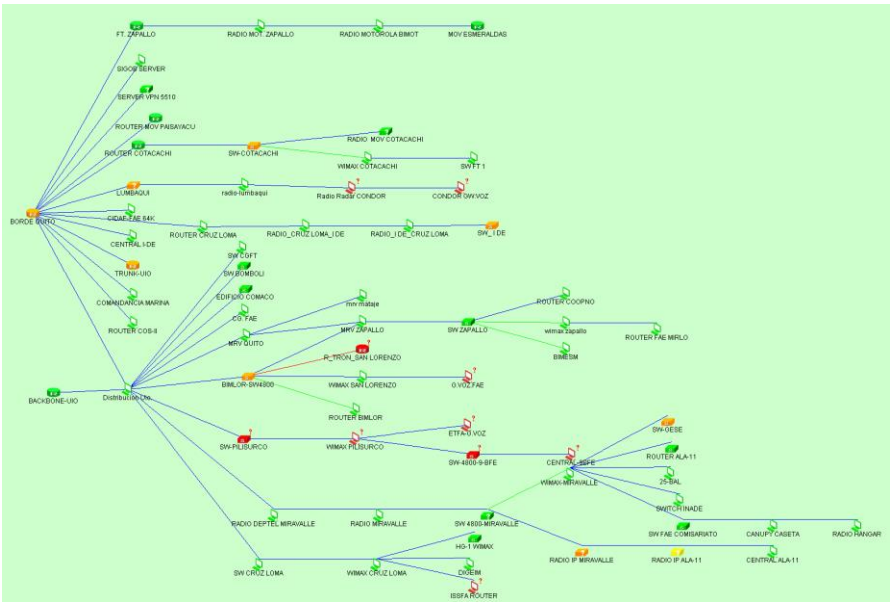


Figura No 42.- Equipos que se derivan del Nodo Quito.

En referencia a este análisis, ilustrado en la Figura No. 42, se tiene la tabla No. 9, que resumen los equipos que dependen del Comando Conjunto y del Nodo Quito:

Tabla No 8.- Equipos del Nodo Quito

Equipo	Nombre	Marca	Modelo	Ubicación
Router	UIO_BACKBONE	3COM	R6080	Comando Conjunto
Router	UIO_BORDE	3COM	R6040	Comando Conjunto
Switch	5500UIO	3COM	S5500G-EI24	Comando Conjunto
Router	R_COTACACHI	3COM	3Com R5232	Cotacachi
Router	ROUTER CRUZ LOMA	Cisco	Cisco 2801	Cruz Loma
Router	ZAPALLO	Cisco	Cisco 2811	Zapallo
Switch	SW_LUMBAQUI	Cisco	Cisco 3560	Lumbaqui
Switch	SW-MIRAVALLE	Cisco	Cisco 3560	Miravalle
Switch	BOMBOLI	3COM	3Com Switch 4500	Bombolí
Switch	MRV QUITO	MRV	9012-M	Zapallo
Switch	SW CRUZ LOMA	Cisco	Cisco 3560	Cruz Loma
Router	CCEE ATACAZO	Cisco	Cisco 2800	Atacazo
Switch	SW-PILISURCO	3COM	3Com Switch 4500	Pilisurco
Switch	BIMLOR-SW4800	3COM	Switch 4800G	San Lorenzo

Total: Router: 6 Switch: 8

a) Nodo Guayaquil:

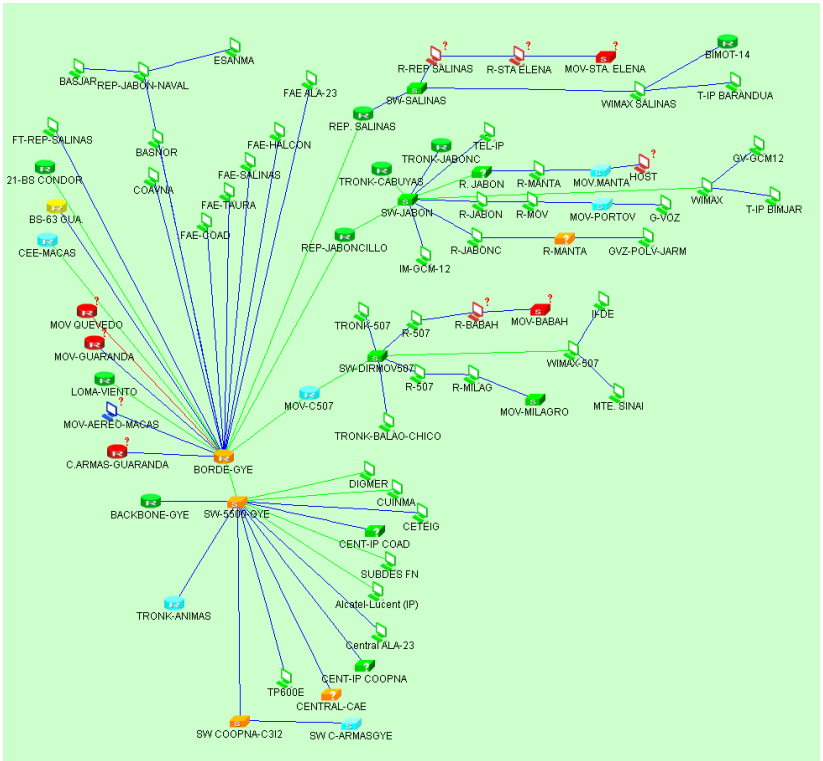


Figura No 43.- Equipos que se derivan del Nodo Guayaquil.

Los equipos que dependen del Nodo Guayaquil, mostrado en la Figura No. 43, se detallan en la Tabla No. 9.

Tabla No 9.- Equipos del Nodo Guayaquil

Equipo	Nombre	Marca	Modelo	Ubicación
Router	BACKBONE-GYE	3Com	3Com Router 6080	Guayaquil
Router	GYE_BORDE	3Com	3Com Router 6080	Guayaquil
Switch	5500G_GYE	3Com	3Com Switch 5500G	Guayaquil
Router	ROUTER-SALINAS	3Com	3Com R5232	Salinas
Switch	SW-CSALINAS	3Com	3Com S5500	Salinas
Router	TRONK-ANIMAS	Cisco	Cisco 2610	Änimas
Router	ROUTER_JABONCILLO	3Com	3Com R5232	Jaboncillo
Switch	SW_JABONCILLO	3Com	3Com S4500-26	Jaboncillo
Router	DIRMOV-C507	3Com	3Com R5232	Cerro 507
Switch	SW-DIRMOV-507	3Com	3Com S4500-26	Cerro 507

Total: Router: 6 Switch: 4

b) Nodo Coca

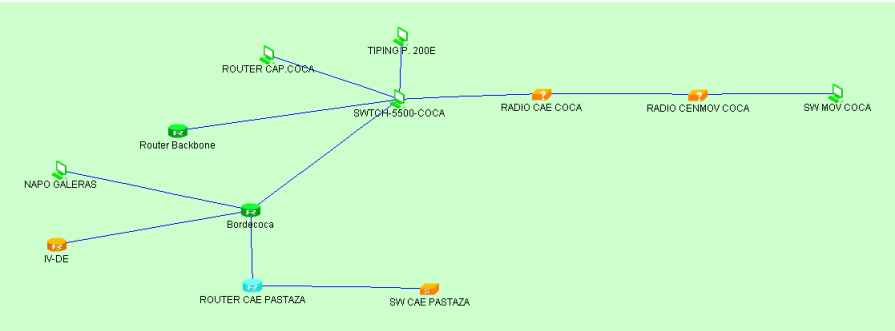


Figura No 44.- Equipos que se derivan del nodo Coca.

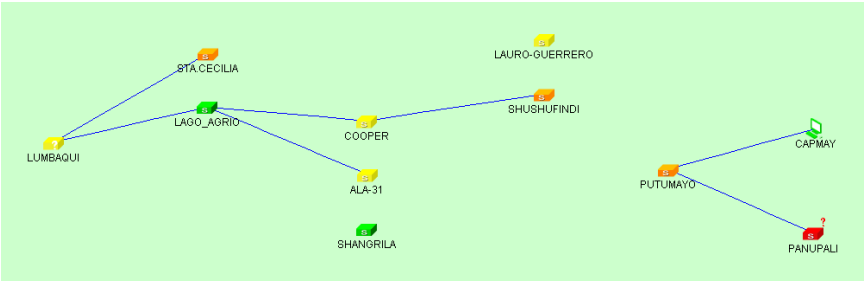


Figura No 45.- Equipos que se derivan de la estación Lumbaqui conectada al Nodo Coca.

Las Figuras No. 44 y 45 muestran los nodos que se desprenden de Nodo Coca y Estación Lumbaqui, el resumen de equipos se muestra en la Tabla No. 10.

Tabla No 10.- Equipos del Nodo Coca

Equipo	Nombre	Marca	Modelo	Ubicación
Router	COCA-BACKBONE	3 Com	3Com R6080	Coca
Router	BORDE_COCA	3 Com	3Com R6080	Coca

CONTINÚA ⟶

Switch	SWTCH-5500-COCA	3 Com	3 Com SE 5500	Coca
Switch	SW_LUMBAQUI	Cisco	Cisco C3560G	Lumbaqui
Switch	LAGO_AGRIO	3 Com	3Com S5500	Lago Agrio
Switch	STA.CECILIA	3 Com	3Com S5500	Santa Cecilia
Switch	COOPER	3 Com	3Com S5500	Cooper
Switch	SANSAHUARI	3 Com	3Com S5500	Sansahuari
Switch	PUTUMAYO	3 Com	3Com S5500	Putumayo
Switch	NUEVO PANUPALI	3 Com	3Com S5500	Nuevo Panupali
Switch	ZANCUDO	3 Com	3Com S5500	Zancudo
Switch	TIPUITINI	3 Com	3Com S5500	Tiputini
Switch	NUEVO ROCAFUERTE	3 Com	3Com S5500	Nuevo Rocafuerte
Router	RCAE_PZA	3 Com	3Com R5232	Pastaza
Switch	SWCAE_PZA	3 Com	3Com S4500-26	Pastaza

Total: Router: 3 Switch: 12

c) Nodo Machala

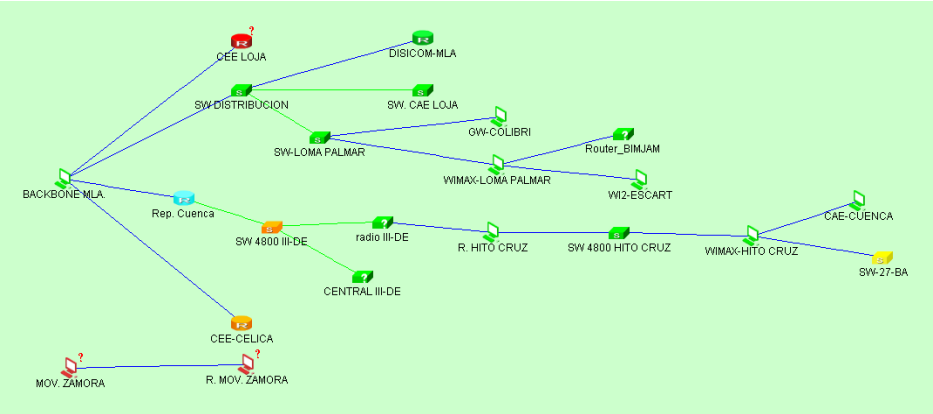


Figura No 46.- Equipos que se derivan del nodo Machala.

Las estaciones que dependen del Nodo Machala, representado en la Figura No. 46 se detallan en la Tabla No. 11.

Tabla No 11.- Equipos del Nodo Machala

Equipo	Nombre	Marca	Modelo	Ubicación
Router	BACKBONE MLA.	3 Com	3Com R6080	Machala
Switch	5500-EI-MLA	3 Com	3Com S5500G-24	Machala
Router	RT_CUENCA	3 Com	3Com R5232	Repetidora Cuenca
Switch	4800G_IIIDE	3 Com	3Com S4800G	Repetidora Cuenca
Switch	SW_HITOCRUZ	3 Com	3Com S4800G	Hito Cruz
Switch	SW_COLIBRI	3 Com	3Com S5500	Loma Palmar
Router	R-Loja	Cisco	Cisco 805	CAE Loja.

Total: Router: 3 Switch: 4

A continuación en la Tabla No 12, se detalla el resumen de los equipos de networking que se encuentran instalados y que dependen del Comando Conjunto, a través de los cuales se conectan los equipos de las unidades militares a nivel nacional para los diferentes servicios:

Tabla No 12.- Resumen equipos de la red de datos.

Nodo	Router	Switch
Quito	6	8
Guayaquil	6	4
Coca	3	12
Machala	3	4
Total	**14**	**27**

2.4.-Determinación de canales E1´s asignados a la red:

Antes de detallar los canales asignados para los diferentes servicios de la red de datos, se realizará una breve descripción de los medios de comunicación empleados en cada enlace a partir de los cuales se derivan los equipos de datos:

2.4.1.-Backbone:

El backbone se encuentra conformado por los anillos SDH, PDH y ramales con tecnología IP como se describen en las siguientes Tablas No. 13 a 17.

Tabla No 13.- Capacidades Anillo Central.

BACKBONE	TECNOLOGÍA	CAPACIDAD
QUITO - CRUZ LOMA	SDH	1 STM-1
CRUZ LOMA - IGUALATA	SDH	1 STM-1
IGUALATA – CARSHAO	SDH	1 STM-1
CARSHAO - BASE SUR	SDH	1 STM-1
BASE SUR - CERRO 507	SDH	1 STM-1
CERRO 507 – AZUCENA	SDH	1 STM-1
AZUCENA – BOMBOLI	SDH	1 STM-1
BOMBOLI – ATACAZO	SDH	1 STM-1
ATACAZO – QUITO	SDH	1 STM-1

CONTINÚA ⟶

TERMINALES	TECNOLOGÍA	CAPACIDAD
IGUALATA-PILISURCO	PDH	4 E1´s
CRUZ LOMA-I DE (CO-4)	PDH	16 E1´s
CRUZ LOMA-DIREL	PDH	16 E1´s
QUITO-MIRAVALLE	IP	100 MBPS

Tabla No 14.- Capacidades Anillo este.

BACKBONE	TECNOLOGÍA	CAPACIDAD
NODO GUAYAQUIL-ANIMAS	PDH	16 E1´s
ANIMAS-SALINAS	PDH	16 E1´s
SALINAS-CABUYAS	PDH	16 E1´s
CABULLAS-COROZO	PDH	16 E1´s
COROZO-JABONCILLO	PDH	16 E1´s
JABONCILLO-AZUCENA	PDH	16 E1´s
TERMINALES	**TECNOLOGÍA**	**CAPACIDAD**
CERRO 507-COAD	PDH	16 E1´s
CERRO 507-TAURA	PDH	4 E1´s
CERRO 507-V BI GUAYAS	PDH	4 E1´s
CERRO 507-BASNOR	PDH	4 E1´s
NODO GUAYAQUIL-COOPNA	PDH	4 E1´s
NODO GUAYAYQUIL-DIGMER	PDH	4 E1´s
SALINAS-BASALI	PDH	4 E1´s
JABONCILLO-ALA 23	PDH	4 E1´s
JABONCILLO-BASJAR	PDH	4 E1´s
JABONCILLO-ESTACIÓN AERONAVAL	PDH	4 E1´s

Tabla No 15.- Capacidades Anillo norte.

BACKBONE	TECNOLOGÍA	CAPACIDAD
CRUZ LOMA-COTACACHI	PDH	16 E1´s
COTACACHI-CAYAMBE	PDH	16 E1´s
CAYAMBE-LUMBAQUI	PDH	16 E1´s
LUMBAQUI-NODO COCA	PDH	16 E1´s
NODO COCA-NAPO GALERAS	PDH	16 E1´s
NAPO GALERAS-ABITAGUA	PDH	16 E1´s
ABITAGUA-TABLON	PDH	16 E1´s
TABLON-IGUALATA	PDH	16 E1´s
TERMINALES	**TECNOLOGÍA**	**CAPACIDAD**
ABITAGUA-PASTAZA	PDH	4 E1´s
LUMBAQUI-SANTA CECILIA	IP	10 MBPS

CONTINÚA ⟶

LUMBAQUI-LAGO AGRIO	IP	10 MBPS
LAGO AGRIO-ALA 31	IP	10 MBPS
LAGO AGRIO-FARFAN	IP	10 MBPS
FARFAN-LAUGO GUERRERO	IP	10 MBPS
LAGO AGRIO-COOPER	IP	10 MBPS
COOPER-SHUSHUFINDI	IP	10 MBPS

Tabla No 16.- Capacidades Anillo sur.

BACKBONE	**TECNOLOGÍA**	**CAPACIDAD**
CARSHAO-BUERAN	PDH	16 E1´s
BUERAN-TINAJILLAS	PDH	16 E1´s
TINAJILLAS-ACACANA	PDH	16 E1´S
ACACANA-VILLONACO	PDH	16 E1´S
VILLONACO-MOTILON	PDH	16 E1´S
MOTILON-NODO MACHALA	PDH	16 E1´S
NODO MACHALA-BALAO CHICO	PDH	16 E1´S
BALAO CHICO-CERRO 507	PDH	16 E1´S
TERMINALES	**TECNOLOGÍA**	**CAPACIDAD**
BUERAN-III DE	PDH	4 E1´s
VILLONACO-7 BI	PDH	4 E1´s

Tabla No 17.- Capacidad red nororiental-noroccidental.

RED NORORIENTAL	**TECNOLOGÍA**	**CAPACIDAD**
LUMBAQUI-LAGO AGRIO	IP	100 MBPS
COOPER-SANSAHUARI	IP	100 MBPS
SANSAHUARI-PUTUMAYO	IP	100 MBPS
PUTUMAYO-PANUPALI	IP	100 MBPS
PANUPALI-ZANCUDO	IP	100 MBPS
ZANCUDO-TIPUTINI	IP	100 MBPS
TIPUTINI-NUEVO ROCAFUERTE.	IP	100 MBPS
RED NOROCCIDENTAL	**TECNOLOGÍA**	**CAPACIDAD**
COTACACHI-LAS CUEVAS	IP	10 MBPS
LAS CUEVAS-CERRO NEGRO	IP	10 MBPS
SAN LORENZO- MATAJE	IP	10 MBPS
ZAPALLO-SAN LORENZO	IP	10 MBPS

2.4.2.- Acceso.- Para el acceso de las unidades hacia el backbone se emplea los siguientes medios:

- **Multiacceso:**

El Sistema de Transmisión Multiacceso, es el encargado de proporcionar el enlace de última milla, para proporcionar servicio de voz y datos de baja capacidad (128 kbps) a los usuarios (Unidades Militares). Estos terminales por su configuración se enlazan directamente a los nodos de Quito, Guayaquil, Coca y Machala, por lo cual el tráfico se suma a estos nodos y son muy pocas unidades que disponen todavía de este medio de comunicación.

- **Wimax:**

El Sistema de Transmisión Wimax, es el encargado de proporcionar la conectividad y enlace de última milla para dar servicio de voz y datos a los usuarios (Unidades Militares) a nivel nacional con una capacidad de 8 Mbps por terminal y está conformado por 2 Macro estaciones y 9 Micro estaciones de acuerdo al detalle que muestra la Tabla No. 18.

Tabla No 18.- Ubicación estaciones Wimax.

TIPO	UBICACIÓN
MACRO ESTACION	CRUZ LOMA
MACROESTACION	CERRO 507
MICROESTACION	MIRAVALLE
MICROESTACION	COTACACHI
MICROESTACION	SAN LORENZO
MICROESTACION	ZAPALLO
MICROESTACION	PILISURCO
MICROESTACION	HITO CRUZ
MICROESTACION	JABONCILLO
MICROESTACION	SALINAS
MICROESTACION	LOMA PALMAR

- **Satelital:**

El sistema satelital de Fuerzas Armadas dispone de un hub VSAT (Very Small Aperture Terminal) en banda KU[3], que proporciona servicios a unidades que por su ubicación geográfica no disponen de otro medio y por su capacidad de usuarios no

[3] Kurz-under banda, rango 12-18 Ghz.

requiere de mayor demanda como lo son los destacamentos militares y unidades de la región Insular, las cuales se integran a la red de datos del nodo Quito y los abanados telefónicos de la central del Nodo Quito. Están distribuidas como se indica en la Tabla No. 19.

Tabla No 19.- Ubicación estaciones satelitales.

ESTACIONES SATELITALES BANDA "Ku"			
ORD	**FUERZA**	**ESTACION**	
1	TERRESTRE	CHICAL	FIJA
2	TERRESTRE	TUFIÑO	FIJA
3	TERRESTRE	TOBAR DONOSO	FIJA
4	TERRESTRE	MALDONADO	FIJA
5	TERRESTRE	MONTALVO	FIJA
6	TERRESTRE	TAISHA	FIJA
7	TERRESTRE	LITA	MANPACK
8	TERRESTRE	QUITO PRUEBA	MANPACK
9	TERRESTRE	SANTA BARBARA	MANPACK
10	TERRESTRE	BS-55 PUTUMAYO	MAMPACK
11	TERRESTRE	CC-19 NAPO	MAMPACK
12	TERRESTRE	GFE 53 RAYO	VEHICULAR
13	TERRESTRE	BI-39 TULCAN	VEHICULAR
14	TERRESTRE	BS-56 TUNGURAHUA	VEHICULAR
15	NAVAL	BIMLOR	VEHICULAR
16	NAVAL	SANTA CRUZ	FIJA
17	NAVAL	SAN CRISTOBAL	FIJA
18	AEREA	BALTRA	FIJA
19	AEREA	COAD	FIJA
20	AEREA	ALA-21	FIJA
21	AEREA	RADAR COS-2	FIJA
22	AEREA	RADAR LUMBAQUI	FIJA
23	AEREA	MÓVIL	MANPACK

- **Enlaces IP:**

Este tipo de enlaces se encuentran implementados en determinadas unidades como los describe la Tabla No 17 y sus capacidades son de 10 y 100 MBPS, principalmente en la red nororiental y noroccidental. Además como lo describe la tabla antes mencionada existen unidades terminales que disponen de enlaces PDH para el acceso al backbone de la red.

2.4.3.- Enlaces para servicios de voz:

Las centrales telefónicas en su inicio trabajaban con TDM, pero con la modernización de las mismas en la actualidad la mayoría de ellas son híbridas. Estas centrales operan con le códec G729 y disponen de varios tipos de conexiones TDM, IP, cobre, fibra, que dependen de los siguientes nodos de las Tabla No. 20 a 23, en una configuración en estrella.

Tabla No 20.- Centrales que depende del Nodo Quito.

CENTRAL	NODO	ENLACE	MEDIO	OBSERVACIÓN
ALA 11	QUITO	ALA 11-MIRAVALLE	IP	
CO-1	QUITO	ATUNTAQUI-COTACACHI	WIMAX	
COOPNO	QUITO	COPPNO-ZAPALLO	WIMAX	
CGFAE	QUITO	CGFAE-QUITO	COBRE	
CGFN	QUITO	CGFN-QUITO	FIBRA	
CGFT	QUITO	CGFT-QUITO	FIBRA	
I DE (CO-4)	QUITO	I DE-QUITO	IP CONVERSORES PDH	DEBE INGRESAR A CRUZ LOMA
BACO	QUITO	LATACUNGA-QUITO	PDH	DEBE INGRESAR A PILISURCO
25 BAL	QUITO	PINTADO-CRUZ LOMA	WIMAX	
9 BFE	QUITO	LATACUNGA-PILISURCO	WIMAX	
PRESIDENCIA	QUITO	CENTRO QUITO-MIRAVALLE	WIMAX	
MIRLO	QUITO	ESMERALDAS-ZAPALLO	WIMAX	
HE-1	QUITO	CENTRO QUITO-CRUZ LOMA	WIMAX	
BAL 72	QUITO	PINTADO-CRUZ LOMA	WIMAX	
ISSFA	QUITO	NORTE QUITO-CRUZ LOMA	WIMAX	

Tabla No 21.- Centrales que depende del Nodo Guayaquil.

CENTRAL	NODO	ENLACE	MEDIO	OBSERVACIÓN
ALA 23	GUAYAQUIL	MANTA-GUAYAQUIL	IP CONVERSORES PDH	DEBE ENTRAR A JABONCILLO
COPNA (CO-2)	GUAYAQUIL	GUAYAQUIL-NODO GUAYAQUIL	IP CONVERSORES PDH	
COAD (CO-5)	GUAYAQUIL	GUAYAQUIL-NODO GUAYAQUIL	IP CONVERSORES PDH	DEBE ENTRAR A 507
ALA 21	GUAYAQUIL	TAURA-NODO GUAYAQUIL	PDH	
BASALI	GUAYAQUIL	SALINAS-NODO GUAYAQUIL	PDH	DEBE ENTRAR CERRO SALINAS
II DE	GUAYAQUIL	GUAYAQUIL-507	WIMAX	
GCM-12	GUAYAQUIL	PORTOVIEJO-	WIMAX	

CONTINÚA ⟶

		JABONCILLO	
DEPJAR	GUAYAQUIL	MANTA-JABONCILLO	WIMAX
TAURITAS	GUAYAQUIL	TAURITAS-507	WIMAX

Tabla No 22.- Centrales que depende del Nodo Coca.

CENTRAL	NODO	ENLACE	MEDIO	OBSERVACIÓN
NUEVO ROCAFUERTE	COCA	NUEVO ROCAFUERTE-LUMBAQUI	IP	
TIPUTINI	COCA	TIPUTINI-LUMBAQUI	IP	
ZANCUDO	COCA	ZANCUDO-LUMBAQUI	IP	
NUEVO PANUPALI	COCA	NUEVO PANUPALI-LUMBAQUI	IP	
LAURO GUERRERO	COCA	LAURO GUERRERO-LUMBAQUI	IP	
FARFÁN	COCA	FARFÁN-LUMBAQUI	IP	
SHANGRILA	COCA	SHANGRILA-LUMBAQUI	IP	
BS-56	COCA	SANTA CECILIA-LUMBAQUI	IP	
BS-55	COCA	PUTUMAYO-LUMBAQUI	IP	
GFE-53	COCA	LAGO AGRIO-LUMBAQUI	IP	
BALAG	COCA	LAGO AGRIO-LUMBAQUI	IP	
17 BS	COCA	PASTAZA-COCA	PDH	

Tabla No 23.- Centrales que depende del Nodo Machala.

CENTRAL	NODO	ENLACE	MEDIO	OBSERVACIÓN
MACHALA	MACHALA	MACHALA	FIBRA	
LOJA	MACHALA	LOJA-MACHALA	PDH	
COLIBRI	MACHALA	LOAM PALMAR-MACHALA	IP	

En base a los problemas que motivaron el desarrollo del presente proyecto, a continuación en las Tablas No. 24 y 25, se detallan los E1´s asignados a cada uno de los servicios que se transporta por la red de datos. En base a estos cuadros se puede apreciar la subutilización de E1s para los diferentes servicios implementados en cada una de las unidades militares de FF.AA. a nivel nacional, así como la falta de integración en la red de datos de las centrales telefónicas con tecnología IP, además de la red de videoconferencia en alta definición para las unidades militares.

Por todos estos servicios y al constituirse el sistema MODE, para el tráfico de voz TDM, no existen los equipos de networking con capacidad y características que permitan aplicar QoS, balanceo de carga y funcionalidades que la tecnología actual proporciona para una red de datos con integración de sus servicios:

a) Canales de datos:

Tabla No 24.- E1´s asignados para datos.

NODOS	**NODO QUITO**	CRUZ LOMA	MIRAVALLE	COTACACHI	ZAPALLO	BIMLOR	IGUALATA	LUMBAQUI	BOMBOLI	PILISURCO	ATACAZO	**NODO GUAYAOUIL**	REPETIDOR 507	COOPNA	JABONCILLO	REPETIDOR SALINAS	**NODO MACHALA**	TERMINAL CUENCA	COLIBRI	HITO CRUZ	TERMINAL LOJA	**NODO COCA**	PASTAZA
NODO QUITO	**-**	**8**	**40**	**4**	**4**	**2**	**2**	**6**	**2**	**-**	**2**	**20**	-	-	-	-	**6**	-	-	-	-	**6**	-
CRUZ LOMA	8	-	-	-	-	-	-	-	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-
MIRAVALLE	40	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
COTACACHI	4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
ZAPALLO	4	-	-	-	-	100	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
BIMLOR	-	-	-	-	100	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
IGUALATA	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
LUMBAQUI	6	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	6	-
BOMBOLI	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
PILISURCO	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
ATACAZO	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
NODO GUAYAQUIL	**20**	-	-	-	-	-	-	-	-	-	-	-	8	2	4	2	6	-	-	-	-	4	-
REPETIDOR 507	-	-	-	-	-	-	-	-	-	-	-	8	-	-	-	-	-	-	-	-	-	-	-
COOPNA	-	-	-	-	-	-	-	-	-	-	-	2	-	-	-	-	-	-	-	-	-	-	-
JABONCILLO	-	-	-	-	-	-	-	-	-	-	-	4	-	-	-	-	-	-	-	-	-	-	-
REPETIDOR SALINAS	-	-	-	-	-	-	-	-	-	-	-	2	-	-	-	-	-	-	-	-	-	-	-
NODO MACHALA	**6**	-	-	-	-	-	-	-	-	-	-	6	-	-	-	-	-	4	10	-	2	4	-
TERMINAL CUENCA	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	4	-	-	10	-	-	-
COLIBRI	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	10	-	-	-	-	-	-
HITO CRUZ	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0	10	-	-	-	-	-
TERMINAL LOJA	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2	-	-	-	-	-	-
NODO COCA	**6**	-	-	-	-	-	-	6	-	-	-	-	-	-	-	-	4	-	-	-	-	-	4
PASTAZA	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	4	-

b) Canales de voz:

Tabla No 25.- E1´s asignados para voz.

NODOS	NODO QTO	I-DE	BACO	COOPNO	DIREL	NODO GYE	5-BI	BASNOR	COAD	BASALI	TAURA	BASJAR	ESANMA	AVINAV	NODO MLA	TERMINAL CUENCA	TERMINAL LOJA	NODO COCA	PASTAZA
NODO QUITO	-	**2**	**2**	**2**	**2**	**10**	-	-	-	-	-	-	-	-	**2**	-	-	**2**	**0**
I-DE	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
BACO	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
COOPNO	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
DIREL	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
NODO GUAYAQUIL	**8**	-	-	-	-	-	2	4	2	6	4	2	2	2	2	-	-	2	-
5-BI	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
BASNOR	4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
COAD	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
BASALI	6	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
TAURA	4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
BASJAR	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
ESANMA	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
AVINAV	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
NODO MACHALA	**2**	-	-	-	-	2	-	-	-	-	-	-	-	-	-	2	2	2	-
TERMINAL CUENCA	**2**	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
TERMINAL LOJA	**2**	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
NODO COCA	**2**	-	-	-	-	-	-	-	-	-	-	-	-	-	2	-	-	-	2
PASTAZA	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	2	-

Nota: La central de Quito y Guayaquil, está integrada a la red de datos.

c) Canales de videoconferencia:

La responsabilidad del Comando Conjunto comprende a los Comandos Operacionales, como unidades operativas para la ejecución de las operaciones. Esto no significa que otras unidades no realizan videoconferencia, sino que lo hacen a través de la red de datos; sin embargo para los Comandos Operacionales se asignó E1´s independientes para de esta manera garantizar este servicio, como lo muestra la Tabla No. 26.

Tabla No 26.- E1´s asignados para videoconferencia de los Comandos Operacionales

NODOS	NODO QUITO	C3I2	CRUZ LOMA (CO 4)	COTACACHI (CO 1)	NODO GUAYAQUIL	COAD (CO 5)	COOPNA (CO 2)	DIRNEA	NODO MACHALA	III DE (CO 3)
NODO QUITO	**-**	**100**	**2**	**4**		-	-	-	-	-
C3I2	**100**	**-**	-	-	-	-	-	-	-	-
CO 4	2	-	-	-	-	-	-	-	-	-
COTACACHI (CO 1)	4	-	-	-	-	-	-	-	-	-
NODO GUAYAQUIL	-	-	-	-	-	2	2	2	-	-
COAD (CO 5)	-	-	-	-	2	-	-	-	-	-
COOPNA (CO 2)	-	-	-	-	2	-	-	-	-	-
DIRNEA	-	-	-	-	2	-	-	-	-	-
NODO MACHALA	-	-	-	-	-	-	-	-	-	2
III DE (CO 3)	-	-	-	-	-	-	-	-	2	-

Nota: El Comando Operacional No 1, transporta la videoconferencia por la red de datos, simplemente asignándole una VLAN distinta para este servicio.

2.5.-Determinación de configuraciones en la red:

El análisis de las configuraciones permitirá identificar la forma en la que se encuentran configurados los equipos, que como se había mencionado fueron instalados bajo requerimientos puntuales y necesidades de conectividad, para de esta manera facilitar el análisis que justifica el proyecto propuesto, esta información se resume en las Tablas No. 27 a 30 y Figuras No. 47 a 51.

Tabla No 27.- Configuraciones de Equipos del Nodo Quito

Equipo	Ubicación	Protocolo de enrutamiento	snmp	rip	bgp	static route
ROUTER	COMANDO CONJUNTO BACKBONE	OSPF AREA 0	si	no	no	Si
ROUTER	COMANDO CONJUNTO BORDE	OSPF AREA 0, 1,2,3,4	si	no	no	Si
SWITCH	COMANDO CONJUNTO	no	no	no	no	Si
ROUTER	COTACACHI	OSPF AREA 4	si	no	no	Si
ROUTER	CRUZ LOMA	OSPF AREA 1	no	no	no	Si
ROUTER	ZAPALLO	OSPF AREA 1	si	no	no	Si
SWITCH	LUMBAQUI	no	no	no	no	Si
SWITCH	MIRAVALLE	no	si	no	no	Si

CONTINÚA ⟶

SWITCH	BOMBOLÍ	no	si	no	no	Si
SWITCH	ZAPALLO	no	si	no	no	Si
SWITCH	CRUZ LOMA	no	si	no	no	Si
ROUTER	ATACAZO	OSPF AREA 4	si	no	no	Si
SWITCH	PILISURCO	no	si	no	no	Si
SWITCH	SAN LORENZO	no	si	no	no	Si

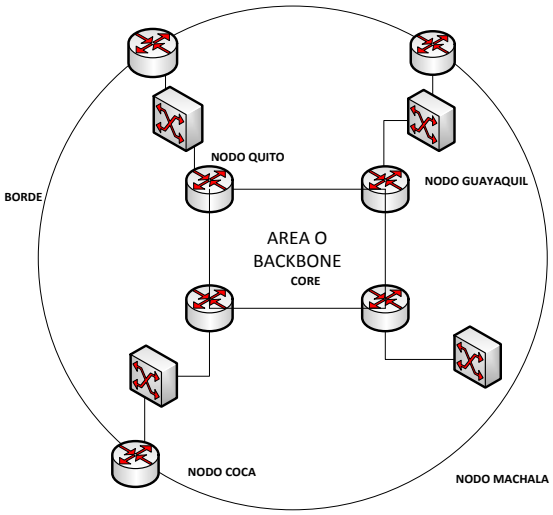


Figura No 47.- Configuración Backbone.

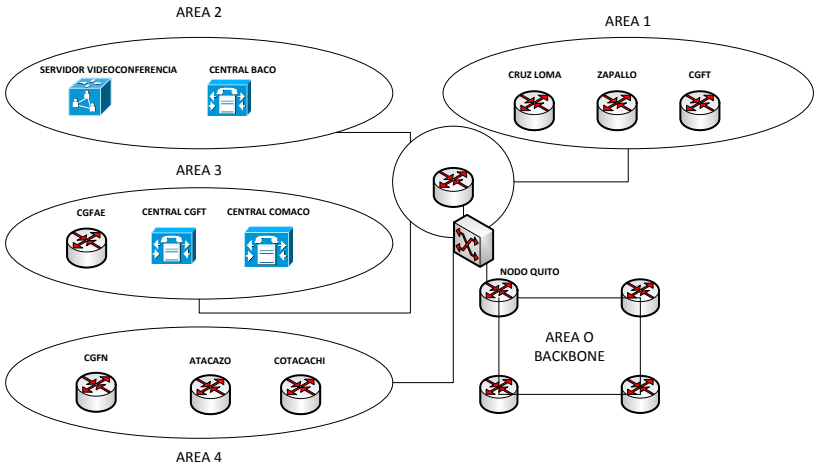


Figura No 48.- Configuración OSPF Nodo Quito.

Tabla No 28.- Configuraciones de Equipos del Nodo Guayaquil

Equipo	Ubicación	Protocolo de enrutamiento	snmp	rip	bgp	static route
ROUTER	GUAYAQUIL-BACKBONE	OSPF AREA 0	si	no	no	si
ROUTER	GUAYAQUIL-BORDE	OSPF AREA 0,	si	no	no	si

CONTINÚA ⟶

		5,9,10				
SWITCH	GUAYAQUIL	OSPF AREA 0, 5,9	si	no	no	si
ROUTER	SALINAS	OSPF AREA 9	si	no	no	no
SWITCH	SALINAS.	no	si	no	no	si
ROUTER	ANIMAS	OSPF AREA 10	si	no	no	si
ROUTER	JABONCILLO	OSPF ARAEA 5	si	no	no	Si
SWITCH	JABONCILLO	no	si	no	no	Si
ROUTER	CERRO 507	OSPF AREA 5	si	no	no	Si

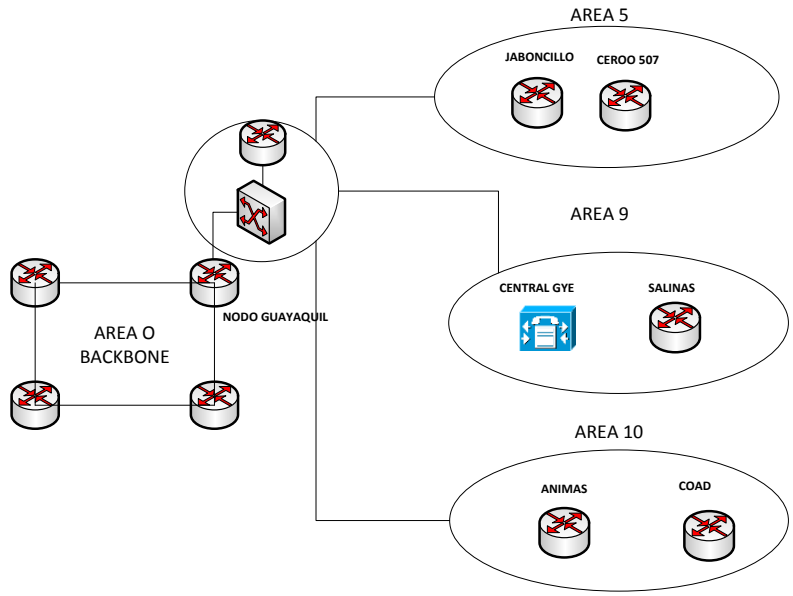


Figura No 49.- Configuración OSPF Nodo Guayaquil.

Tabla No 29.- Configuraciones de Equipos del Nodo Coca

Equipo	Ubicación	Protocolo de enrutamiento	SNMP	RIP	BGP	STATIC ROUTE
ROUTER	COCA-BACKBONE	OSPF AREA 0,1	si	no	no	Si
ROUTER	COCA-BORDE	OSPF AREA 0,1,7	si	no	no	Si
ROUTER	PASTAZA	OSPF AREA 7	si	no	no	Si
SWITCH	COCA	no	si	no	no	No
SWITCH	LUMBAQUI	no	si	no	no	No
SWITCH	LAGO AGRIO	no	si	no	no	No
SWITCH	SANTA CECILIA	no	si	no	no	No
SWITCH	COOPER	no	si	no	no	No
SWITCH	SANSAHUARI	no	si	no	no	No
SWITCH	PUTUMAYO	no	Si	no	no	No

CONTINÚA ⟶

SWITCH	NUEVO PANUPALI	no	Si	no	no	No
SWITCH	ZANCUDO	no	Si	no	no	no
SWITCH	TIPUTINI	no	Si	no	no	No
SWITCH	NUEVO ROCAFUERTE	no	Si	no	no	No

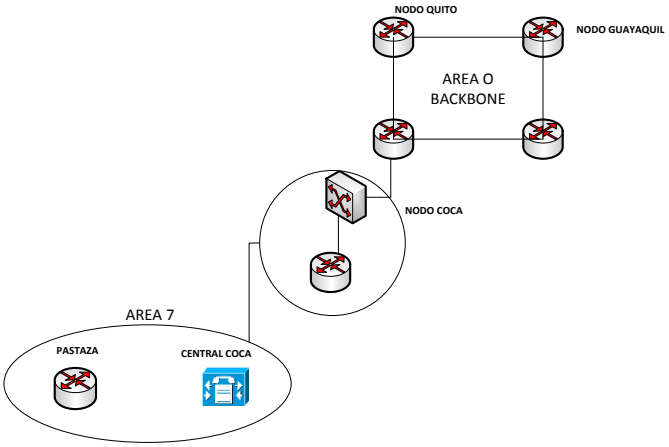


Figura No 50.- Configuración OSPF Nodo Coca.

Tabla No 30.- Configuraciones de Equipos del Nodo Machala

Equipo	Ubicación	Protocolo de enrutamiento	SNMP	RIP	BGP	STATIC ROUTE
ROUTER	MACHALA-BACKBONE	OSPF AREA 0,8,12	Si	no	no	si
SWITCH	MACHALA	no	Si	no	no	si
ROUTER	TERMINAL CUENCA	OSPF AREA 8	Si	no	no	si
SWITCH	HITO CRUZ	no	Si	no	no	si
SWITCH	COLIBRÍ	no	Si	no	no	si
ROUTER	TERMINAL LOJA	OSPF AREA 12	Si	no	no	si

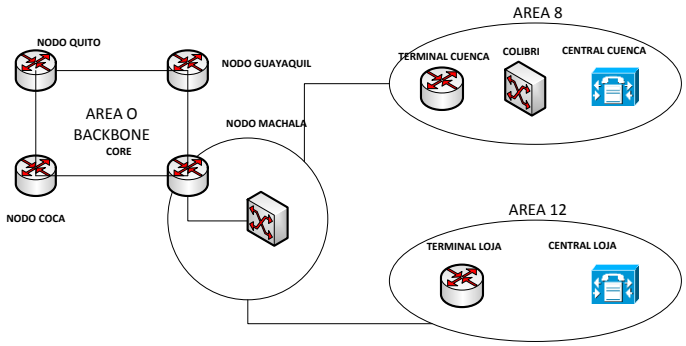


Figura No 51.- Configuración OSPF Nodo Machala.

Estas configuraciones permiten identificar que no existe organización en la habilitación del protocolo OSPF mediante las diferentes áreas, así como la creación

de rutas estáticas, que dificultan la administración y operación de la red de datos, constituyéndose en una de las deficiencias de la red actual.

2.6.-Análisis de anchos de banda en la red:

En referencia a los aplicativos descritos en la sección 1.4 y los E1´s asignados para los diferentes servicios habilitados, se procederá analizar los anchos de banda en los equipos de responsabilidad del Comando Conjunto y que serán tomados de referencia para el diseño de la topología en el presente trabajo. Para el respectivo análisis se empleará el software solarwinds y Opnet Ncompass y se muestra en la Figura No. 52 y detalla en las Tabla No. 31 a 40.

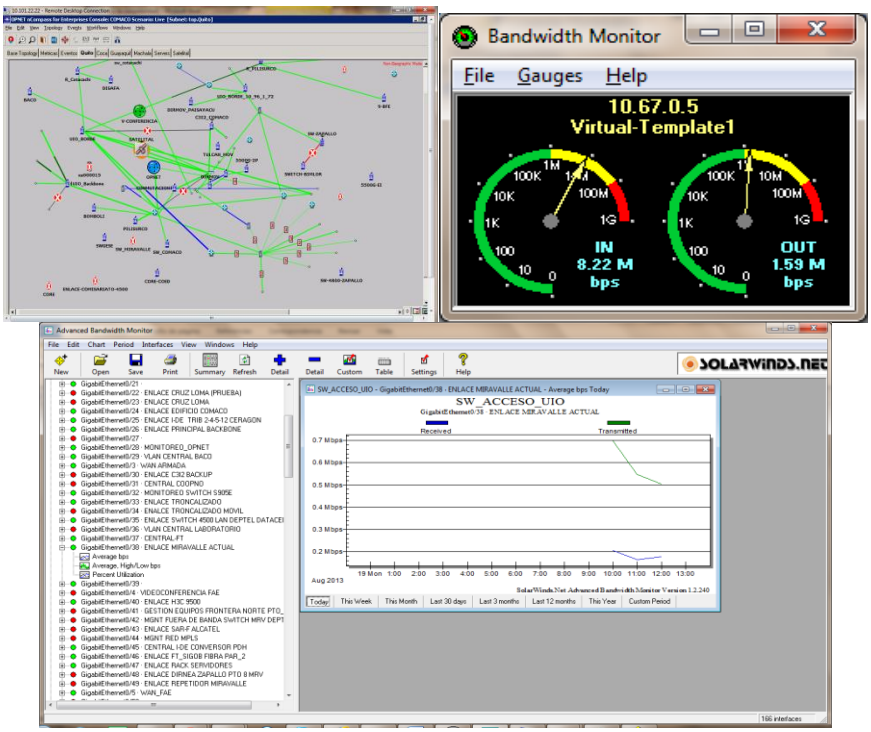


Figura No 52.- NCOMPASS Y SOLARWINDS.

ANILLO CENTRAL:

a) DATOS:

Tabla No 31.- Anchos de banda datos Anillo Central.

ORIGEN	DESTINO	SERVICIO	AB IN (Mbps)	AB OUT (Mbps)	AB asignado	TOTAL (Mbps)	CPU %
CRUZ LOMA	QUITO BORDE	DATOS	1.5	2.33	8 Mbps	3.83	20-30

CONTINÚA ⟶

COMACO8 BORDE	NODO QUITO BACKBONE	DATOS	19	18	100 Mbps	37	20-40
ATACAZO	QUITO BORDE	DATOS	0.202	0.060	2 Mbps	0.26	10-20
BOMBOLÍ	QUITO BORDE	DATOS	0.10	0.23	2 Mbps	0.33	15-30
ZAPALLO	QUITO BORDE	DATOS	0.458	1.55	4 Mbps	2.01	25-45
MIRAVALLE	QUITO BORDE	DATOS	1	0.50	40 Mbps	1.5	15-30
PILISURCO	QUITO BORDE	DATOS	0.40	0.89	2 Mbps	1.29	20-40
COTACACHI	QUITO BORDE	DATOS	0.15	0.20	4 Mbps	0.35	10-20
GUAYAQUIL	NODO QUITO BACKBONE	DATOS	7.67	6.59	20 Mbps	14.26	30.50
COCA	NODO QUITO BACKBONE	DATOS	0.50	3.00	4Mbps	3.50	25-45
MACHALA	NODO QUITO BACKBONE	DATOS	0.80	1.2	6 Mbps	2.00	10-30
CGFT	QUITO BORDE	DATOS	2.2	2.8	100 Mbps	5.00	20-35
CGFN	QUITO BORDE	DATOS	1.4	1.8	100 Mbps	3.2	20-30
CGFA	QUITO BORDE	DATOS	1.20	1.6 Mbps	100 Mbps	2.8	20-30
SATELITAL	QUITO BORDE	DATOS	3.00	0.80	6 Mbps	3.80	25-35

b) VOZ

Las centrales telefónicas disponen de una topología en estrella en base a sus cuatro nodos principales: Quito, Guayaquil, Coca y Machala. El ancho de banda que consumen se describe la Tabla No. 32.

Tabla No 32.- Anchos de banda voz Anillo central.

ORIGEN	DESTINO	TDM/IP	SERVICIO	AB IN (Mbps)	AB OUT (Mbps)	AB TOTAL (Mbps)
CENTRAL UIO	NODO UIO	IP 10.96.0.254 GEth0/35	VOZ	0.160	0.150	0.31

CONTINÚA →

CENTRAL I DE	NODO UIO	IP 10.96.0.254 GEth0/45	VOZ	0.160	0.150	0.31
CENTRAL FT	NODO UIO	IP 10.96.0.254 GEth0/37	VOZ	0.190	0.170	0.36
CENTRAL BACO	NODO UIO	IP 10.96.0.254 GEth0/29	VOZ	0.150	0.140	0.29

Como se observa el tráfico en cada central es similar ya que están instaladas en unidades militares con similares cantidades de usuarios y centrales de las mismas características. En base a estas mediciones se determina que el tráfico promedio en cada una de las centrales instaladas e integradas al nodo Quito está definido bajo el detalle que se muestra en la Tabla No. 33.

Tabla No 33.- Ancho de banda Centrales telefónicas.

CENTRAL	DESTINO	RUTA	AB total= suma in +out (Mbps)
NODO COMACO	QUITO	FIBRA: NODO QUITO-QUITO	0.36
CGFT	QUITO	FIBRA: CGFT-QUITO.	0.36
CGFA	QUITO	COBRE: CGFA-QUITO	0.36
CGFN	QUITO	FIBRA: CGFN-QUITO	0.36
MIDENA	QUITO	FIBRA: MIDENA-QUITO.	0.28
IDE	QUITO	PDH (1 E1) I DE-CRUZ LOMA-QUITO.	0.30
DIREL	QUITO	WIMAX IP: DIREL-CRUZ LOMA.	0.28
COLOG	QUITO	WIMAX IP: COLOG-MIRAVALLE.	0.28
ALA 11	QUITO	IP: ALA 11-MIRAVALLE.	0.30
FTC-1	QUITO	WIMAX IP: FTC-1-COTACACHI	0.32
COOPNO	QUITO	WIMAX IP: COOPNO-ZAPALLO	0.30
ALA 12	QUITO	PDH 1 E1: ALA 12-IGUALATA-PILISURCO-CRUZ LOMA-QUITO.	0.30
9 BFE	QUITO	WIMAX IP: BFE-IGUALATA-PILISURCO.	0.28
PRESIDENCIA	QUITO	WIMAX IP: PRESIDENCIA-CRUZ LOMA	0.24
MIRLO	QUITO	WIMAX IP: MIRLO-ZAPALLO.	0.24
ISSFA	QUITO	WIMAX IP: ISSFA-CRUZ LOMA	0.28
HE-1	QUITO	WIMAX IP: HE-1-CRUZ LOMA	0.24

Como se puede observar en las rutas, la conectividad no es la adecuada, siendo en muchos casos conectadas con E1´s directamente desde Quito.

c) VIDEOCONFERENCIA:

Tabla No 34.- Ancho de banda videoconferencia Anillo central.

ORIGEN	DESTINO	SERVICIO	AB IN (Mbps)	AB OUT (Mbps)	AB ASIGNADO (Mbps)
COMANDOS OPERACIONALES	COMACO	VIDEOCONFERENCIA	3.00	2.00	8.00
CO-1	COMACO	VIDEOCONFERENCIA	2.00	2.16	10

ANILLO NORTE:

a) DATOS:

Tabla No 35.- Anchos de banda datos Anillo norte.

ORIGEN	DESTINO	SERVICIO	AB IN (Mbps)	AB OUT (Mbps)	AB ASIGNADO (Mbps)	TOTAL (Mbps)	CPU %
COTACACHI	QUITO	DATOS	0.15	0.18	4.00	0.33	10-15
LUMBAQUI	QUITO	DATOS	1.50	1.10	8.00	2.60	15-20
IGUALATA	QUITO	DATOS	0.40	0.89	2.00	1.29	20-30
NAPO GALERAS	COCA	DATOS	0.15	0.13	2.00	0.28	10-20
PASTAZA	COCA	DATOS	0.17	0.15	2.00	0.32	10-20
LUMBAQUI	COCA	DATOS	0.60	7.00	8 Mbps	7.60	20-40

b) VOZ:

Tabla No 36.- Anchos de banda voz Anillo norte.

CENTRAL	DESTINO	RUTA	AB total= suma in +out (Mbps)
CENTRAL COCA	NODO COCA	IP:COCA	0.31
CENTRAL PASTAZA	NODO COCA	TDM (E1): PASTAZA-COCA	0.31
BALAG	NODO COCA	IP: LAGO AGRIO-LUMBAQUI	0.26
GFE-53	NODO COCA	IP: LAGO AGRIO-LUMBAQUI	0.26

CONTINÚA ⟶

BOES 54	NODO COCA	IP: COOPER	0.26
BS-55	NODO COCA	IP: PUTUMAYO	0.26
BS-56	NODO COCA	IP: SANTA CECILIA-LUMBAQUI	0.26
SHANGRILA	NODO COCA	IP: SHANGRILA-COCA	0.26
FARFAN	NODO COCA	IP: LAGO AGRIO	0.26
LAURO GUERRERO	NODO COCA	IP: LAURO GUERRERO-IP: FARFAN	0.26
NUEVO PANUPALI	NODO COCA	IP: NUEVO PANUPALI-PUTUMAYO	0.26
ZANCUDO	NODO COCA	IP: ZANCUDO-PANUPALI	0.26
TIPUTINI	NODO COCA	IP: TIPUTINI-ZANCUDO	0.26
NUEVO ROCAFUERTE	NODO COCA	IP: NUEVO ROCAFUERTE	0.26

ANILLO OESTE:

a) DATOS:

Tabla No 37.- Anchos de banda datos Anillo oeste.

ORIGEN	DESTINO	SERVICIO	AB IN (Mbps)	AB OUT (Mbps)	AB ASIGNADO	TOTAL (Mbps)	CPU %
507	GUAYAQUIL	DATOS	1.70	1.50	4.00	3.20	25-40
SALINAS	GUAYAQUIL	DATOS	0.30	2.00	4.00	2.30	20-30
JABONCILLO	GUAYAQUIL	DATOS	0.80	2.10	6.00	3.00	20-30
ÁNIMAS	GUAYAQUIL	DATOS	0.20	1.64	2.00	1.84	20-30
MANTA	GUAYAQUIL	DATOS	0.20	1.60	2.00	1.80	15-25
MACHALA	GUAYAQUIL	DATOS	0.18	0.20	2.00	0.38	15-20
COCA	GUAYAQUIL	DATOS	0.15	0.22	4.00	0.27	10-15

CONTINÚA →

COOPNA	GUAYAQUIL	DATOS	0.10	0.12	2.00	0.22	10-15
DIRNEA	GUAYAQUIL	DATOS	0.80	0.87	2.00	1.67	10-15
BASE NAVAL NORTE	507	DATOS	0.24	0.80	2.00	1.04	10-15
COAD	507	DATOS	2.3	0. 20	4.00	2.5	15-25
TAURA	507	DATOS	0. 20	0.14	2.00	0.34	10-15

b) VOZ:

Tabla No 38.- Anchos de banda voz Anillo oeste.

CENTRAL	DESTINO	RUTA	AB
MANTA	NODO GUAYAQUIL	PDH 1 E1: GUAYAQUIL-ÁNIMAS-SALINAS-JABONCILLO.	0.36
II DE	NODO GUAYAQUIL	WIMAX IP: 507-II DE	0.28
BASNOR	NODO GUAYAQUIL	PDH 1 E1: BASNOR-507-NODO GUAYAQUIL	0.28
COOPNA	NODO GUAYAQUIL	PDH 1 E1: COOPNA- NODO GUAYAQUIL	0.30
VI GUAYAS	NODO GUAYAQUIL	PSH 1 E1: VI GUAYAS- 507-NODO GUAYAQUIL.	0.24
CUINMA	NODO GUAYAQUIL	PDH 1 E1: CUINMA-NODO GUAYAQUIL	0.28
ESMA	NODO GUAYAQUIL	PDH 1 E1: SALINAS-NODO GUAYAQUIL.	0.24
COAD	NODO GUAYAQUIL	COAD- NODO GUAYAQUIL.	0.36
TAURA	NODO GUAYAQUIL	TAURA- NODO GUAYAQUIL.	0.36
CODESC	NODO GUAYAQUIL	FIBRA: CODESC-NODO GUAYAQUIL.	0.28
ESDESU	NODO GUAYAQUIL	FIBRA: ESDESU-NODO GUAYAQUIL	0.24
TAURITAS	NODO GUAYAQUIL	WIMAX IP: TAURITAS-507	0.20
GCM-12	NODO GUAYAQUIL	WIMAS IP: PORTOVIEJO-JABONCILLO	0.20

ANILLO SUR:

a) DATOS:

Tabla No 39.- Anchos de banda datos Anillo sur.

ORIGEN	DESTINO	SERVICIO	AB IN (Mbps)	AB OUT(Mbps)	AB ASIGNADO (Mbps)	AB TOTAL(Mbps)	CPU %
LOJA	MACHALA	DATOS	0.20	0.50	2.00	0.70	10-20
CUENCA	MACHALA	DATOS	0.40	3.34	4.00	3.74	20-40
GUAYAQUIL	MACHALA	DATOS	0.30	0.40	4.00	0.70	10-20
LOMA PALMAR	MACHALA	DATOS	0.50	0.20	10	0.70	10-15
COCA	MACHALA	DATOS	0.45	0.30	2.00	0.75	10-15
MACHALA	MACHALA	DATOS	0.80	1.00	100	1.80	10-15
HITO CRUZ	MACHALA	DATOS	0.30	0.40	10	0.70	10-15

b) VOZ:

Tabla No 40.- Anchos de banda voz Anillo sur.

CENTRAL	DESTINO	RUTA	AB
MACHALA	NODO MACHALA	MACHALA	0.36
III DE	NODO MACHALA	PDH 1 E1: MOTILON-VILLONACO-ACACANA-TINAJILLAS-BUERÁN-III DE	0.36
27 BAA	NODO MACHALA	IP: MOTILON-VILLONACO-ACACANA-TINAJILLAS-BUERÁN-III DE-HITO CRUZ- 27 BAA	0.24
7 BI LOJA	NODO MACHALA	PDH 1 E1: MOTILÓN-VILLONACO-7 BI	0.24
LOMA PALMAR	NODO MACHALA	MACHALA-LOMA PALMAR	0.22

2.7.- Requerimientos de los usuarios y crecimiento a mediano plazo.

En base a los consumos de anchos de banda para cada servicio según lo descrito en el capítulo 2.6; además de la proyección en base a la fórmula detallada en el capítulo 1.2 del Método de dimensionamiento de la red, la capacidad de transporte para los aplicativos por emplearse considerando un índice de crecimiento establecido en base al crecimiento del tráfico actual en relación a la capacidad asignada cuando se inició la red de datos con un valor promedio de crecimiento del 20% anual y considerando además, un incremento de AB entre 2 y 5 Mbps requerido para aplicaciones de videoconferencia con unidades que frecuentemente utilizan este servicio con las Comandancias de Fuerza y Comandos Operacionales. Estos anchos de banda se detallan en las Tablas No. 41 a 44 (ANEXO A "PROYECCIÓN A MEDIANO PLAZO"):

Anillo Central (NODO QUITO):

Tabla No 41.- Anchos de banda proyectada Anillo central.

ESTACIÓN	USUARIOS	SERVICIOS REQUERIDOS	AB actual (Mbps)	AB requerido a mediano plazo	índice de crecimiento anual	AB proyectado
QUITO	10 (COMANDANCIAS)	VOZ, DATOS, VIDEOCONFERENCIA	3.8	8.8	0.20	21.90
CRUZ LOMA	7 (CO-4)	VOZ, DATOS, VIDEOCONFERENCIA	3.83	5.83	0.20	14.51
IGUALATA - PILISURCO	5	VOZ, DATOS, VIDEOCONFERENCIA	1.29	1.29	0.20	3.21
ATACAZO	1	VOZ, DATOS, VIDEOCONFERENCIA	0.26	0.26	0.20	0.65
COTACACHI	2 (CO-1)	VOZ, DATOS, VIDEOCONFERENCIA	0.35	5.35	0.20	13.31
BOMBOLI	2	VOZ, DATOS, VIDEOCONFERENCIA	0.33	0.33	0.20	0.88
ZAPALLO	8	VOZ, DATOS, VIDEOCONFERENCIA, DEFENSA AÉREA.	2.01	4.01	0.20	9.98
MIRAVALLE	9	VOZ, DATOS, VIDEOCONFERENCIA.	1.5	1.5	0.20	3.73
SAN LORENZO	3	VOZ, DATOS, VIDEOCONFERENCIA.	0.45	2.45	0.20	6.10
QUITO	GUAYAQUIL	VOZ, DATOS, VIDEOCONFERENCIA, DEFENSA AÉREA	14.26	19.26	0.20	47.93
QUITO	COCA	VOZ, DATOS, VIDEOCONFERENCIA	2.71	7.71	0.20	19.18
QUITO	MACHALA	VOZ, DATOS, VIDEOCONFERENCIA, DEFENSA AÉREA	2	7	0.20	17.42
		TOTAL	32.79	63.79	0.20	158.73

Anillo Norte (NODO COCA):

Tabla No 42.- Anchos de banda proyectada Anillo norte.

ESTACIÓN	USUARIOS	SERVICIOS REQUERIDOS	AB actual (mbps).	AB requerido a mediano plazo	índice de crecimiento anual	AB proyectado
NODO COCA	5	VOZ, DATOS, VIDEOCONFERENCIA	2.6	7.6	0.20	18.91
LUMBAQUI	21	VOZ, DATOS, VIDEOCONFERENCIA, DEFENSA AÉREA.	7.6	12.6	0.20	31.35
COCA	GUAYAQUIL	VOZ, DATOS, VIDEOCONFERENCIA	0.27	5.27	0.20	13.11
COCA	QUITO	VOZ, DATOS, VIDEOCONFERENCIA	2.71	7.71	0.20	19.18
COCA	MACHALA	VOZ, DATOS, VIDEOCONFERENCIA	0.75	5.75	0.20	14.31
		TOTAL	13.93	38.93	0.20	96.87

Anillo Oeste (NODO GUAYAQUIL):

Tabla No 43.- Anchos de banda proyectada Anillo oeste.

ESTACIÓN	USUARIOS	SERVICIOS REQUERIDOS	AB actual (Mbps).	AB requerido a mediano plazo	índice de crecimiento anual	AB proyectado
507	31 (CO-5)	VOZ, DATOS, VIDEOCONFERENCIA, DEFENSA AÉREA.	3.2	10.2	0.20	25.38
SALINAS	5	VOZ, DATOS, VIDEOCONFERENCIA.	2.3	2.3	0.20	5.72
CAE-GYE	17 (CO-2)	VOZ, DATOS, VIDEOCONFERENCIA, DEFENSA AÉREA.	11.57	11.57	0.20	28.79
JABONCILLO	11	VOZ, DATOS, VIDEOCONFERENCIA.	3	3	0.20	7.46
GUAYAQUIL	QUITO	VOZ, DATOS, VIDEOCONFERENCIA	14.26	19.26	0.20	47.93
GUAYAQUIL	COCA	VOZ, DATOS, VIDEOCONFERENCIA	0.27	5.27	0.20	13.11
GUAYAQUIL	MACHALA	VOZ, DATOS, VIDEOCONFERENCIA	0.38	5.38	0.20	13.39
		TOTAL	34.98	56.98	0.20	141.78

Anillo Sur (NODO MACHALA):

Tabla No 44.- Anchos de banda proyectada Anillo sur.

ESTACIÓN	USUARIOS	SERVICIOS REQUERIDOS	AB actual (Mbps).	AB requerido a mediano plazo	índice de crecimiento anual	AB proyectado
LOMA PALMAR	5	VOZ, DATOS, VIDEOCONFERENCIA, DEFENSA AÉREA	0.7	2.7	0.15	6.72
CAE - MACHALA	4	VOZ, DATOS, VIDEOCONFERENCIA	1.8	6.8	0.15	16.92
HITO CRUZ	2	VOZ, DATOS, VIDEOCONFERENCIA	0.7	0.7	0.20	1.74
CUENCA-BUERAN	III-DE (CO-3)	VOZ, DATOS, VIDEOCONFERENCIA	3.74	8.74	0.20	21.75
MACHALA	GUAYAQUIL	VOZ, DATOS, VIDEOCONFERENCIA	0.38	0.38	0.20	0.95
MACHALA	COCA	VOZ, DATOS, VIDEOCONFERENCIA	0.75	5.75	0.20	14.31
MACHALA	QUITO	VOZ, DATOS, VIDEOCONFERENCIA	2	7	0.20	17.42
MACHALA	GUAYAQUIL	VOZ, DATOS, VIDEOCONFERENCIA	0.38	5.38	0.20	13.39
		TOTAL	10.07	37.07	0.20	92.24

En resumen las capacidades por utilizarse en los anillos se detallan en la Tabla No. 45.

Tabla No 45.- Resumen de capacidades por anillo.

ANILLO	CAPACIDAD
CENTRAL	158.73 MBPS
NORTE	96.87 MBPS
OESTE	141.78 MBPS
SUR	92.24 MBPS

Sin embargo de esto y en referencia al oficio No 13-DTIC-b-1512-ancho de banda, en el cual se solicitó los requerimientos de servicios para las unidades militares, las Fuerzas requieren la siguiente capacidad por unidad como lo muestra la Tabla no. 46.

Tabla No 46.- Requerimientos de las Fuerzas por unidades.

UNIDAD	CAPACIDAD REQUERIDA(MBPS)
COMANDO DE FUERZA	21 MBPS
COMANDO OPERACIONAL	17 MBPS
DIVISIÓN/BRIGADA/HOSPITAL	16 MBPS
BATALLÓN/BASE/ISSFA	9 MBPS
GRUPO/COS/DIRMOV/CEE	2.5 MBPS
COMPAÑÍA/CAPITANÍA/RETÉN	2 MBPS
DESTACAMENTO/BASE GUERRA ELECTRÓNICA, INTELIGENCIA.	1 MBPS

Este requerimiento se fundamente en los aspiraciones de cada unidad por efectuar sus proyectos que comprenden en sí en la transmisión de video en tiempo real para señales de radares, monitoreo de zonas vulnerables, aplicaciones médicas para hospitales y centros de salud militares, transmisión de video de los UAV´s y aplicativos propios de cada unidad. Las centrales telefónicas no incrementarían su uso en razón que no existiría o sería mínimo el incremento de usuarios en las unidades militares. Resumiendo lo descrito en el ANEXO B "REQUERIMIENTOS DE USUARIOS", se detalla la Tabla 47.

Tabla No 47.- Requerimientos en los anillos de las Fuerzas.

ANILLO	CAPACIDAD
CENTRAL	879.61 MBPS
NORTE	189.98 MBPS
OESTE	645.33 MBPS
SUR	182.35 MBPS

Esta proyección estaría sujeta a los desarrollos de los aplicativos por implementarse en base a los presupuestos asignados, que pueden o no ejecutarse dependiendo de las asignaciones económicas a cada Fuerza. En todo caso los equipos de datos deben tener la capacidad de soportar estas capacidades y superiores en el orden de los Gbps. Con lo descrito en el presente capítulo se puede verificar las siguientes observaciones:

- Existe variedad en las configuraciones, capacidades y marcas de los equipos instalados en la red.

- Existen enlaces saturados en su capacidad y muchos de ellos no representan una conectividad adecuada sino que salen directamente de los nodos Quito, Guayaquil, Machala y Coca.
- Los requerimientos de las unidades se ven reflejados en videoconferencias y aplicativos de datos considerados en las proyecciones a mediano plazo.
- No existe una integración de servicios, ni configuraciones con calidad de servicios que permitan diferenciarlos o priorizarlos.

CAPÍTULO 3
DISEÑO DE LA RED.

3.1.- Topología de la red:

En referencia a los parámetros establecidos en el capítulo 1 del diseño de la red y la topología de la red de transporte MODE indicada en la Figura No 53, se establecerá la ubicación de los equipos LSR y LER:

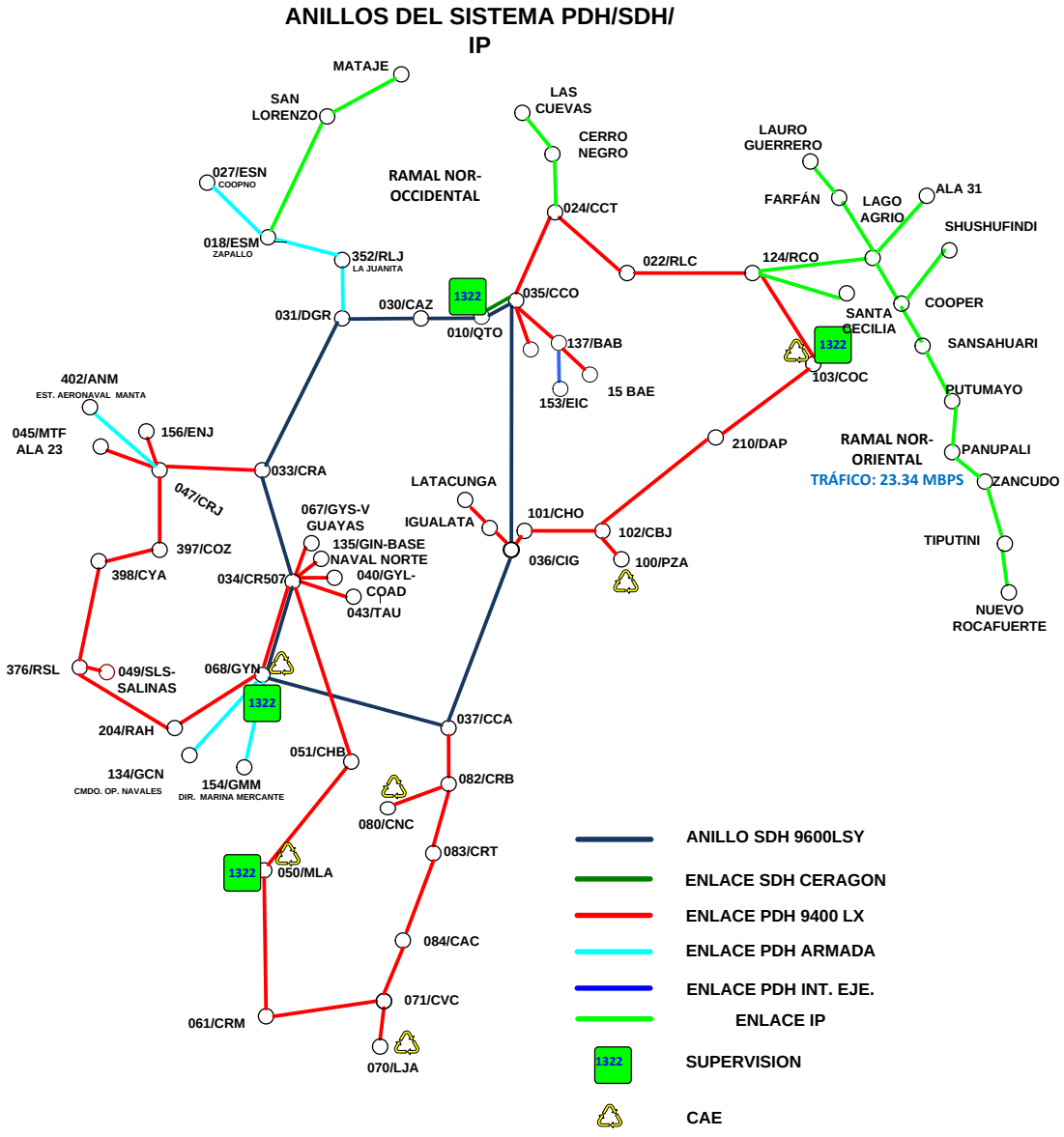


Figura No 53.- Red de transporte MODE.

3.1.1.- Ubicación de equipos LER:

Tabla No 48.- Ubicación equipos LER.

ORD	ANILLO	ESTACIÓN	NOMINATIVO	AB	USUARIOS	JUSTIFICACIÓN
1	CENTRAL	CRUZ LOMA	LER-CL	14.51	8	Tráfico, usuarios, CO-4
2	CENTRAL	QUITO	LER-QU	21.90	10	Tráfico, usuarios, Comandancias
3	CENTRAL	IGUALATA	LER-IG	3.21	5	Tráfico, usuarios
4	CENTRAL	ZAPALLO	LER-ZA	9.98	8	Tráfico, usuarios
5	OESTE	CERRO 507	LER-507	25.38	23	Tráfico, usuarios, CO-2, CO-5
6	OESTE	JABONCILLO	LER-JA	7.46	11	Tráfico, usuarios
7	OESTE	BASE SUR	LER-BS	28.79	17	Tráfico, usuarios
8	OESTE	SALINAS	LER-SA	5.72	5	Tráfico, usuarios
9	SUR	BUERAN	LER-BU	21.75	3	tráfico, usuarios, CO-3
10	SUR	MACHALA	LER-MA	16.92	9	Tráfico, usuarios.
11	NORTE	COTACACHI	LER-CO	13.31	3	Tráfico, usuarios, CO-1
12	NORTE	COCA	LER-CC	18.91	5	Tráfico, usuarios
13	NORTE	LUMBAQUI	LER-LU	31.35	21	Tráfico, usuarios.

Los equipos detallados en la Tabla No 48, se ubicarán en razón de la cantidad de usuarios que se derivan y la ubicación de los Comandos Operacionales, quienes ejecutan las operaciones militares.

3.1.2.-Ubicación equipos LSR:

Tabla No 49.- Ubicación equipos LSR.

ESTACIÓN/REPETIDORA	JUSTIFICACIÓN	NOMINATIVO
CRUZ LOMA	NODO QUITO, CO-4, CO-1 CONMUTACIÓN ANILLO CENTRAL-NORTE-RED NOROCCIDENTAL. REDUNDANCIA. TOLERANCIA A FALLAS.	LSR-CL
LUMBAQUI	NODO COCA CONMUTACIÓN ANILLO NORTE-RED NORORIENTAL. REDUNDANCIA. TOLERANCIA A FALLAS.	LSR-LU
CARSHAO	CO-3 CONMUTACIÓN ANILLO SUR-CENTRAL. REDUNDANCIA. TOLERANCIA A FALLAS.	LSR-CA

CONTINÚA ⟶

CERRO 507	NODO GUAYAQUIL, CO-2, CO-5 CONMUTACIÓN ANILLO OESTE-CENTRAL. REDUNDANCIA.	LSR-507
MACHALA	TOLERANCIA A FALLAS. NODO MACHALA. REDUNDANCIA.	
IGUALATA	TOLERANCIA A FALLAS. CONMUTACIÓN ANILLO NORTE-CENTRAL. REDUNDANCIA. TOLERANCIA A FALLAS.	LSR-MA LSR-IG

Los LSR descritos en la Tabla No 49, por su funcionalidad serán ubicados en los puntos en donde se unen los anillos de transporte y puedan proporcionar redundancia y tolerancia a fallas, que faciliten la conmutación de los paquetes.

3.1.3.- Ubicación de equipos LSR y LER:

En referencia a las Tablas No 48 y 49, los equipos LSR y LER estarán distribuidos como se indica en la Figura No 54:

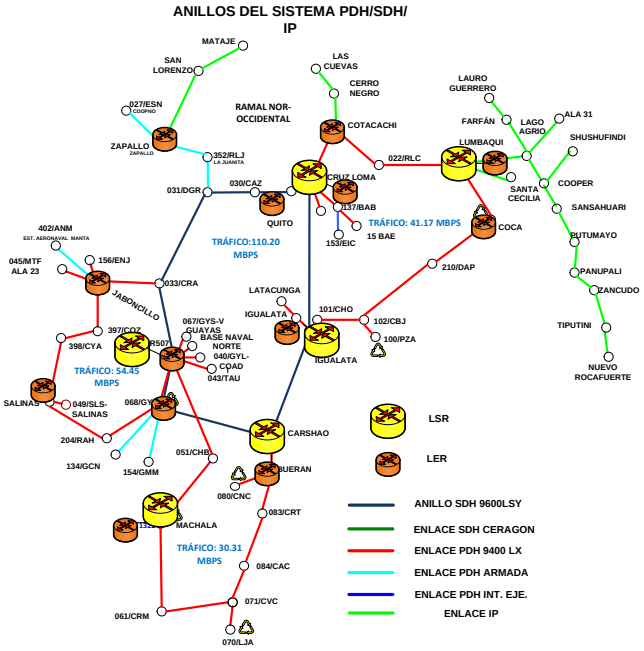


Figura No 54.- Ubicación Equipos LSR y LER.

Para la topología de la red se realizará en base al análisis de las distancias de los anillos de la red de transporte, que representará el costo del enlace, tal como fue descrito en el capítulo 1.1 Método de diseño de la red, basado en el algoritmo de

Dijkstra y el camino de costo mínimo. Por lo tanto los equipos de core estarán enlazados como se describe en las Tablas 50 a 52 y Figuras No 55 a 61 (ANEXO C "DISTANCIAS DE LOS ENLACES"):

3.1.4.- Análisis de Topología: Nodos Anillo central:

Tabla No 50.- Costo Anillo Central.

NODOS	ANILLO	COSTO RAMAL COSTA (KM)	COSTO RAMAL SIERRA (KM)
CRUZ LOMA-CERRO 507	CENTRAL	345,06	367,54

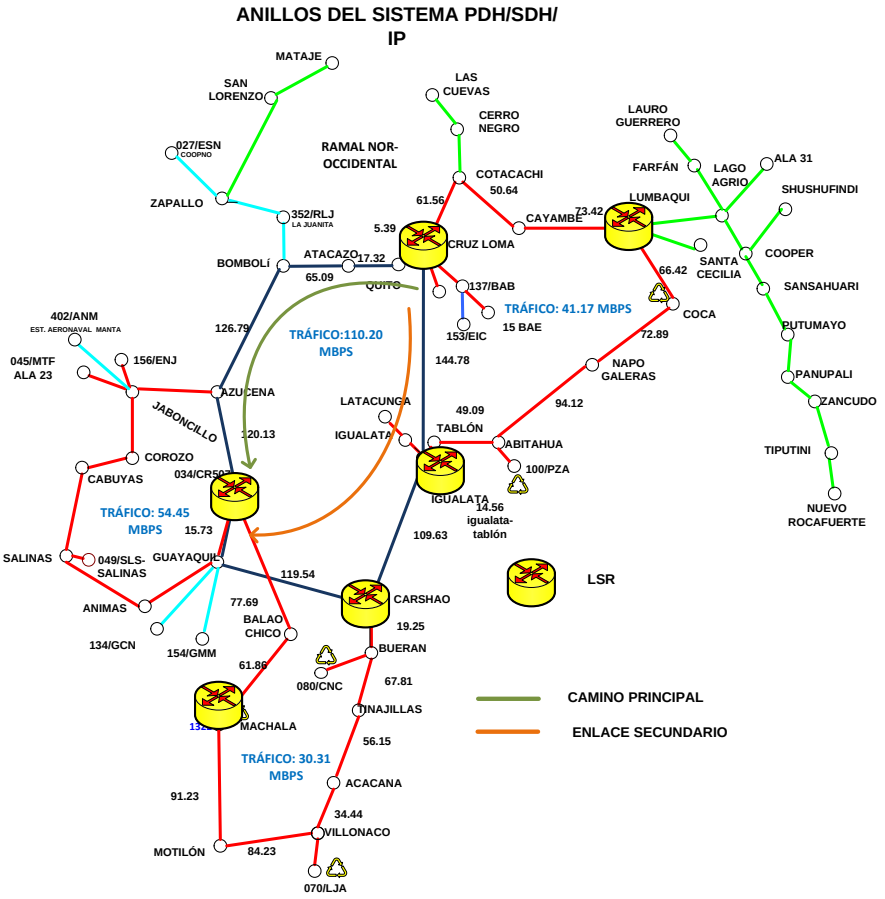


Figura No 55.- Topología Anillo central

En base a lo antes descrito se aprecia que en estas rutas existen conexiones con los siguientes nodos:

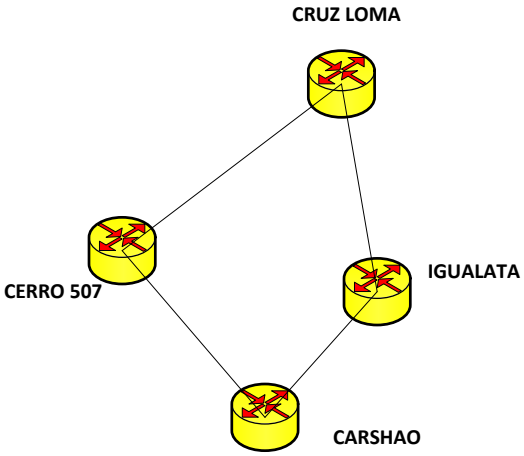


Figura No 56.- Conexiones nodos Anillo Central.

3.1.5.- Análisis de Topología: Nodos Anillo Norte.

Tabla No 51.- Costo Anillo Norte.

NODOS	ANILLO	COSTO POR IGUALATA (KM)	COSTO POR COTACACHI (KM)
CRUZ LOMA-LUMBAQUI	NORTE	282.52	185.62

En base a las distancias entre los enlaces del anillo norte, se puede observar que la distancia de costo mínimo es por la vía de Cotacachi, por lo cual los caminos y topología en este anillo estarían definidas en las Figura No 57 y 58, que formarían parte del backbone de la red de datos de FF.AA:

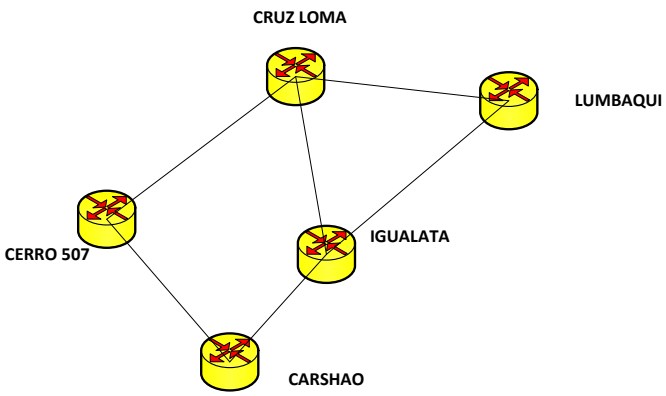


Figura No 57.- Conexiones nodos Anillo Norte

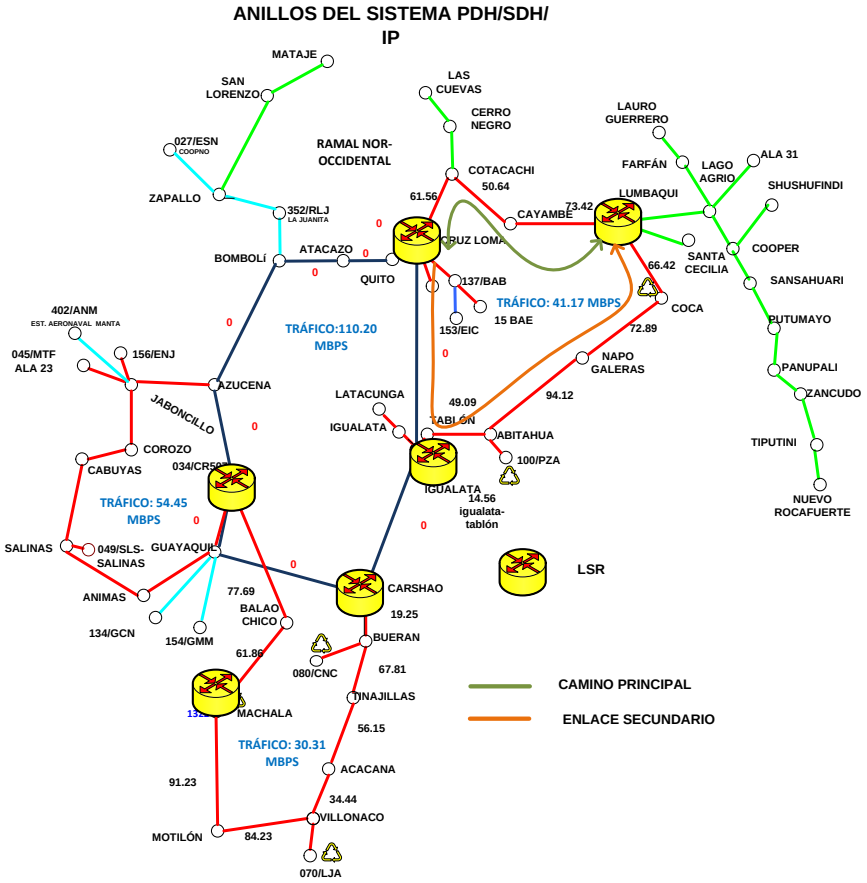


Figura No 58.- Topología Anillo Norte.

Como se puede observar los enlaces que pasan por las rutas definidas en el anillo central adquieren el valor de cero y pueden ser utilizadas como parte de los enlaces hacia los siguientes nodos.

3.1.6.- Análisis de Topología: Nodos Anillo Sur:

Tabla No 52.- Costo Anillo Sur.

NODOS	ANILLO	COSTO BALAO CHICO (KM)	COSTO POR MOTILÓN(KM)
MACHALA-507	SUR	139.55	353.11

Como se mencionó anteriormente las rutas seleccionadas forman parte del backbone de la red de datos y sus enlaces adquieren un costo con valor 0. Por lo cual

las rutas para este anillo y su topología se describen en la Tabla No 52 y Figura No 59:

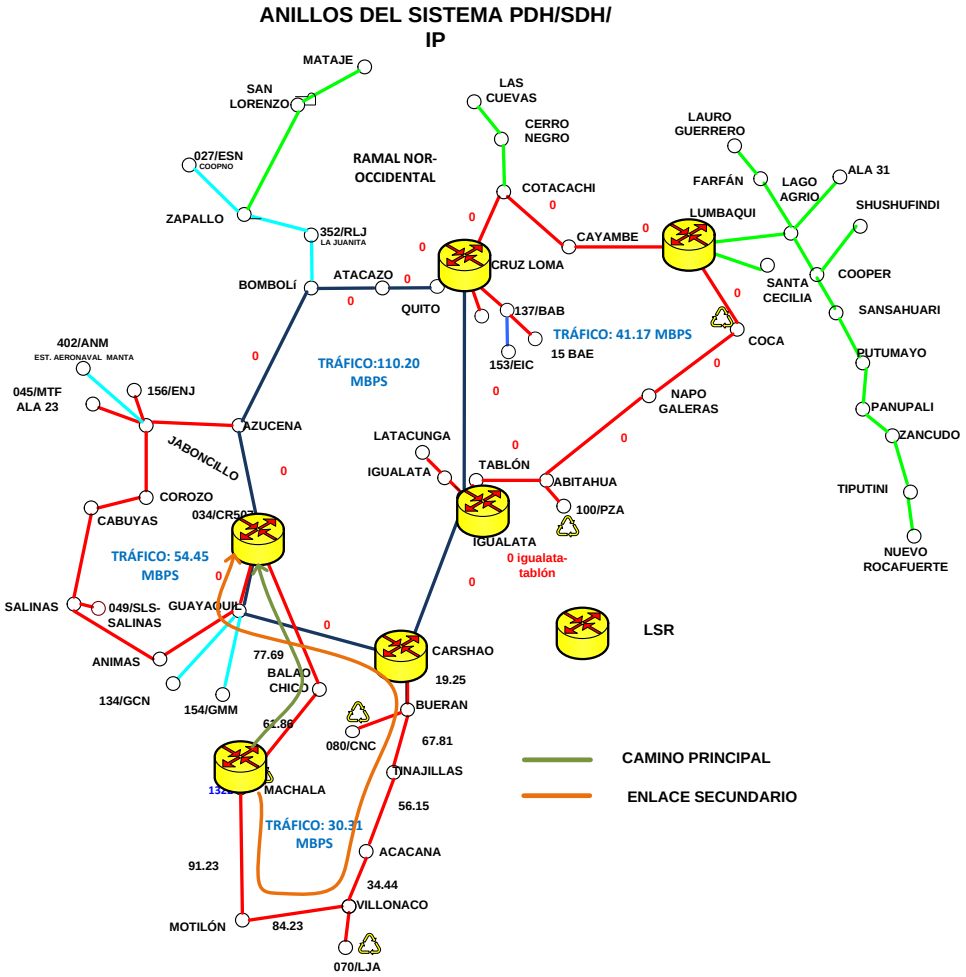


Figura No 59.- Topología Anillo Sur.

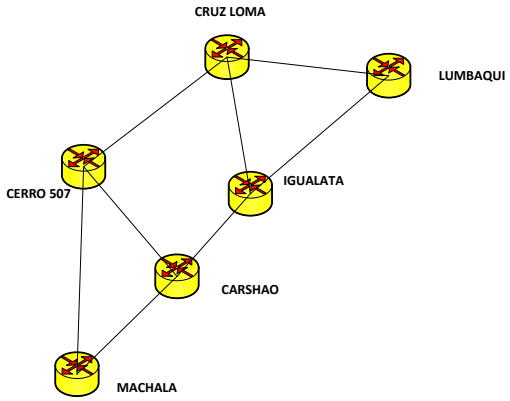


Figura No 60.- Conexiones Backbone Red de datos.

Como se puede observar en la Figura No 60, el anillo sur se conecta a los nodos cada uno con rutas diferentes, sustentando el concepto de topología con tolerancia a fallas, mediante caminos redundantes y de costo mínimo.

Para los equipos LER estarán conectados al nodo más cercano, como se demuestra en la Figura No 61:

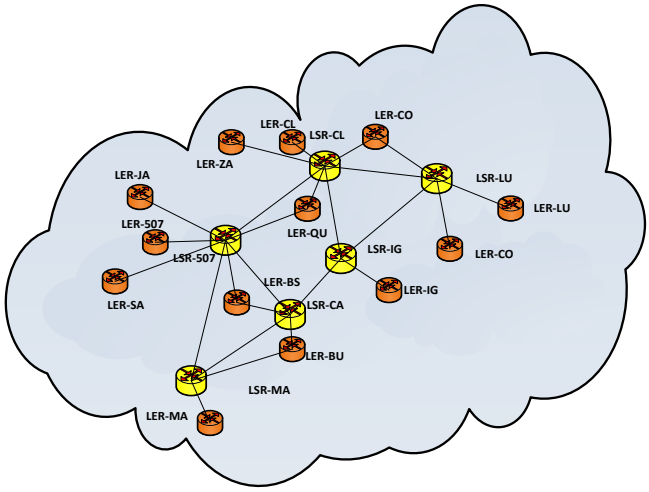


Figura No 61.- Topología LSR y LER

3.2.- Dimensionamiento de la red:

En base a lo analizado en el capítulo 2.7- Requerimientos de los usuarios y crecimiento a mediano plazo, se determina la capacidad de tráfico que deben soportar los anillos de la red de transporte para la red de datos con sus servicios de voz, videoconferencia y datos, resumidos la Tabla No 53:

Tabla No 53.- Capacidades de la red de datos a mediano plazo.

ANILLO	ANCHO DE BANDA CALCULADO	ANCHO DE BANDA REQUERIDO
CENTRAL	158.73 MBPS	879.61 MBPS
NORTE	96.87 MBPS	189.98 MBPS
SUR	141.78 MBPS	645.33 MBPS

CONTINÚA ⟶

OESTE	92.24 MBPS	182.35 MBPS

Estas capacidades comparadas con la capacidad actual del sistema MODE, establece que existen requerimientos que se deben efectuar en la red de transporte como lo demuestra la Tabla No 54:

Tabla No 54.- Capacidades actuales de la red de transporte.

ANILLO	ANCHO DE BANDA	CAPACIDAD ACTUAL	REQUERIMIENTO
CENTRAL	158.73 MBPS	2 STM1: 63 E1´S	SOPORTA EL REQUERIMIENTO A MEDIANO PLAZO.
NORTE	96.87 MBPS	16 E1´s	SE DEBE INCREMENTAR LA CAPACIDAD DE LOS ENLACES
SUR	141.78 MBPS	16 E1´s	SE DEBE INCREMENTAR LA CAPACIDAD DE LOS ENLACES
OESTE	92.24 MBPS	16 E1´s	SE DEBE INCREMENTAR LA CAPACIDAD DE LOS ENLACES.

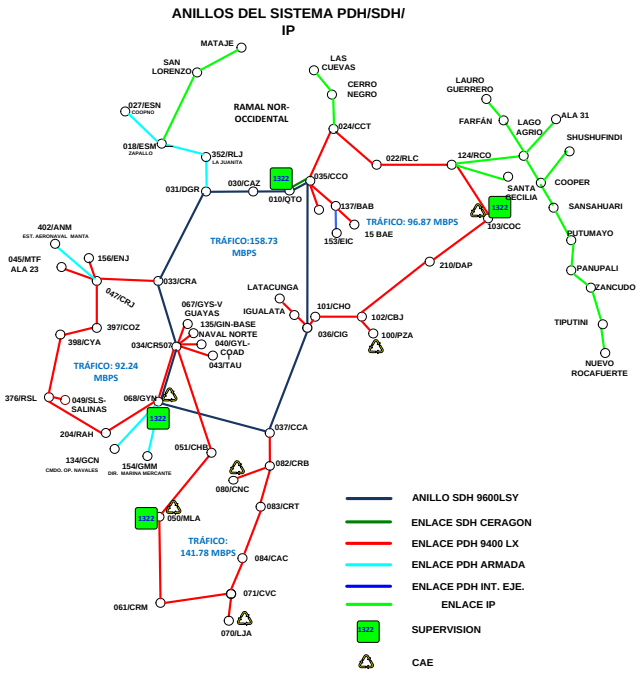


Figura No 62.- Capacidades en los anillos de la red de transporte.

3.3.- Determinación de los equipos de core, distribución y acceso:

3.3.1.- Equipos de core:

Entre las características mínimas que deben soportar estos equipos se detalla las siguientes:

- Soporte de MPLS y funcionalidad de VPN.
- Interfaces 100/1000 Ethernet y fibra óptica.
- Soporte de protocolos de capa 2 como VLAN Trunk Protocol (VTP), IEEE 802.1q.
- Soporte de protocolos de enrutamiento como OSPF, IS-IS, BGPv4 y soporte de IPv6.
- Deben soportar cualquier protocolo de señalización como RSVP o LDP.
- Alta disponibilidad.

Considerando estas características en la Tabla No 55, se realiza una comparación entre equipos de marcas conocidas para estas funcionalidades como lo son Cisco, Alcatel y HP:

Tabla No 55.- Equipos de Core

CARACTERÍSTICAS	CISCO ASR 9006	ALCATEL 7710 SR C-12.	HP HSR 6802
Soporte MPLS	SI,	SI	SI
Señalización MPLS	LDP, T-LDP, RSVP	LDP, T-LDP, RSVP	LDP, T-LDP, RSVP
MPLS/VPN	SI	SI	SI
QoS MPLS	SI	SI	SI
Protocolos de enrutamiento.	IS-IS, OSPF, BGP	IS-IS, OSPF, BGP	IS-IS, OSPF, BGP
Velocidad de backplane	3.5 TBPS	320 GBPS	1024 GBPS
Puertos	10/100/1000 base T, SPF	10/100/1000 base T, SPF	10/100/1000 base T.
Número de VRF	8000	1024	1024
Apilamiento MPLS.	SI	SI	SI
Voltajes de alimentación	220 Vac 60 HZ.	85-265 Vac.	100-220 Vac.

3.3.2.- Equipos de distribución:

Para estos equipos se detalla las siguientes características mínimas descritas en la Tabla No 56:

- Interfaces 100/1000 Ethernet y fibra óptica.
- Soportar MPLS, VRF(VPN Routing and Forwarding) y Qos y VRF.
- Protocolos de enrutamiento principalmente OSPF, IS-IS, BGP, IGMP.

Tabla No 56.- Equipos de distribución.

CARACTERÍSTICAS	CISCO ASR903	ALCATEL 7705 SAR-8	HP 6608
Soporte MPLS	SI	SI	SI
Señalización MPLS	LDP, RSVP	LDP, RSVP	LDP, RSVP
MPLS/VPN	SI	SI	SI
Puertos	10/100/1000 base T	10/100/1000 base T	10/100/1000 base T
Protocolos de enrutamiento.	IS-IS, OSPF, BGP	IS-IS,OSPF, BGP	IS-IS,OSPF, BGP
Realiza QoS	SI	SI	SI
VRF	2000	1024	1024
Voltajes de alimentación	110 ac	110 ac.	110 ac

3.3.3.- Equipos de acceso:

Tabla No 57.- Equipos de acceso.

CARACTERÍSTICAS	CISCO 2800	HP MSR 20-20
Puertos	3: 10/100/1000	2; 10/100
Protocolos de enrutamiento.	OSPF,BGP,IS-IS	OSPF,BGP,IS-IS
Realiza QoS	SI	SI
Voltajes de alimentación	110 ac.	110 ac
Rendimiento mínimo	50 Mbps	100 Mbps
Soporte tarjetas EHWIC	SI	SI

La Tabla No 57 describe las características mínimas de los equipos de acceso o equipos de usuario en las Unidades Militares de FF.AA.

3.3.4.- Parámetros diferenciales de los equipos:

Como se puede apreciar los equipos analizados trabajan con los protocolos mínimos requeridos, sin embargo Cisco posee ventajas en el manejo de capacidades y velocidades. Además de estas características técnicas, en la Tabla No 58 de describe parámetros que deben ser considerados al elegir un equipo y como son:

Tabla No 58.- Parámetros diferenciales de los equipos:

PARÁMETRO	CISCO	ALCATEL	HP
Proveedores certificados.	5	1	2
Soporte técnico.	Diverso algunos proveedores certificados	Limitado un solo proveedor.	Limitado con pocos proveedores certificados.
Redes instaladas con mpls en el país.	SI	NO	NO
Información tecnológica disponible.	Diversa	Limitada	Limitada
Experiencia de técnicos del CC.FF.AA en estas marcas.	Media	Nula	Baja
Experiencia de los técnicos del CC.FF.AA en la manipulación de quipos	Media	Nula	Baja

Como se puede observar en base a las características técnicas de los equipos y por los parámetros descritos en la Tabla No 58, los equipos adecuados para la implementación de la red de datos de Fuerzas Armadas por su capacidad y sus parámetros diferenciales, serán de marca Cisco.

3.4.- Determinación de costos del equipo definido:

En la Tabla No 59 se detallen los costos referenciales de los equipos seleccionados para la red de datos de FF.AA:

Tabla No 59.- Costos de equipo definido:

RED	EQUIPO	PRECIO (USD)	CANTIDAD	TOTAL
Core	ASR-9006	95000,00	6	570000,00
Distribución	ASR903	48000,00	13	624000,00
Acceso	CISCO 2800	6700,00	30	201000,00
Instalación	LOTE	300000,00	1	300000,00
Capacitación	LOTE	1110000	10	110000
Soporte Técnico	LOTE	20000	1	20000
TOTAL:				1825000,00

3.5.- Establecimiento de facilidades MPLS en la red:

En el presente capítulo se procederá a establecer los parámetros básicos para la simulación en la plataforma OPNET y las facilidades MPLS a ser utilizadas:

3.5.1.- Protocolos a emplearse:

- **IS-IS como protocolo de enrutamiento:**

IS-IS *(Intermediate System to Intermediate System*) es un protocolo ISO de encaminamiento jerárquico de pasarela interior o IGP (*Interior Gateway Protocol*), que usa el estado de enlace para encontrar el camino más corto mediante el algoritmo SPF (*Shortest Path First*). Este envía mensajes a todos los routers, con la finalidad de que cada router conozca por completo la topología del sistema autónomo, con la finalidad de que cada router decida la mejor ruta para el envió de la información. Al igual que OSPF, IS-IS utiliza el algoritmo Dijkstra (Shortest Path First –SPF) para el cálculo de rutas; pero mientras que OSPF suele emplearse como solución empresarial (aunque también en ISPs), IS-IS sólo suele verse en ISPs.

En IS-IS, la dirección de área y de host son asignados al router entero, mientras que en OSPF el direccionamiento es asignado al nivel de interfaz.

Para el funcionamiento de ISIS son necesarias las direcciones CLNS (incluso si el router solo está configurado con IP). Las direcciones CLNS que utilizan los routers se denominan NSAP (network service access points), con el siguiente formato:

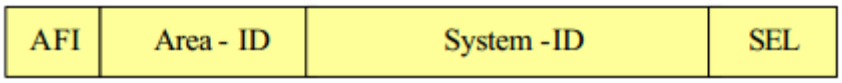


Figura No 63.- Campo NSAP.

El campo AFI (Authority Format Identifier), está determinado por organizaciones internacionales, pero se tiene un valor asignado para las redes privadas, 49 (SERVIN).

El valor del Area–ID es determinado por el administrador de la red y es definido en 4 valores hexadecimales. Este campo identifica el área de enrutamiento, para el diseño se empleará el valor de 0001.

El valor de System–ID es determinado igualmente por el administrador y no debe ser repetido, ya que identifica a cada IS como único dentro del área. Para nuestro caso se empleará la dirección loopback transformada en el Id de la siguiente manera:

- Ip loopback: 10.68.0.200
- Tres dígitos: 010.068.000.200
- Agrupación 4 dígitos: 0100.6800.0200.

El campo SEL (Selector) es para identificar si el equipo hará tareas de enrutamiento, para el caso adquirirá el valor de 00, ya que este identifica a los routers.

Existen tres tipos de routers en ISIS:

- Level 1 (L1): Solo identifica routers de la misma área.
- Level2 (L2): Pueden incluir vecinos en la misma área o diferente área, comprende el área de backbone.
- Both (L1/L2): puede incluir vecinos en cualquier área.

Para nuestro diseño se empleará el level 2 para todas las configuraciones y con mayor razón al considerar una misma área de backbone.

Este protocolo es seleccionado ante OSPF por las siguientes razones:

- Escalabilidad.
- Cada router es posicionado en una sola área.
- Los paquetes OSPF son encapsulados en el datagrama Ip, mientras ISIS son encapsulados directamente en el marco de la capa de enlace.
- Los grandes proveedores actualmente utilizan ISIS, como protocolo de enrutamiento.

- **Arquitectura VPN MPLS:**

MP-BGP como protocolo para el intercambio de VPN entre PE´s:

La RFC 2547 se conoce como VPNs MPLS MP-BGP porque MP-BGP se utiliza para el intercambio de la información de enrutamiento entre sitios remotos sobre la WAN y MPLS se utiliza para enviar tráfico de VPN como lo indica la Figura No 64. Para el diseño los clientes (Unidades Militares) están conectados a la red por una interfaz del PE, la cual está asociada a una tabla de enrutamiento.

El dispositivo cliente (CE) será un enrutador que establecerá la adyacencia con el PE directamente conectado. Después de establecer esta adyacencia el enrutador CE anuncia las rutas locales del sitio VPN y aprende rutas remotas desde el PE (ICARAN).

El enrutador de borde del proveedor (PE) intercambiará información de enrutamiento con el enrutador CE, para lo cual utilizará los protocolos empleados en las unidades militares que en su mayoría es OSPF.

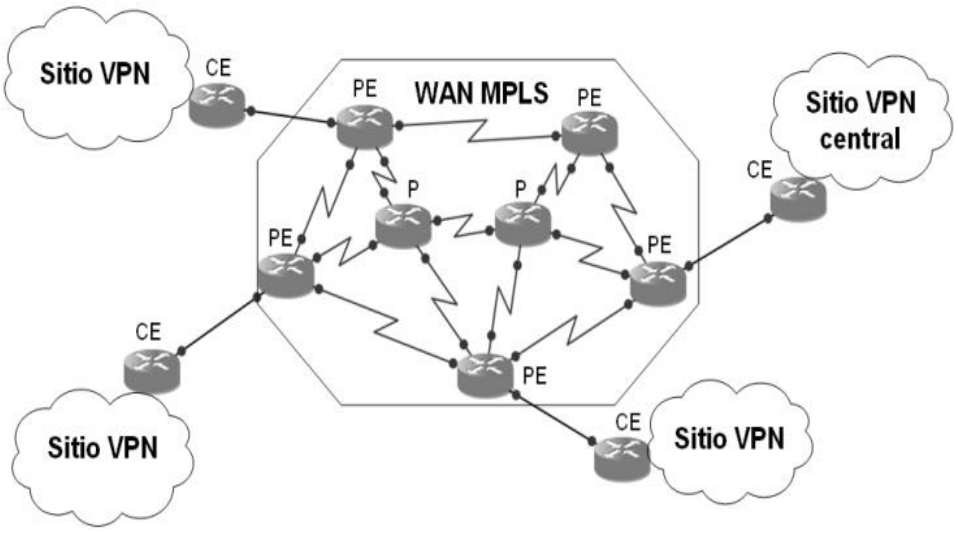


Figura No 64.- VPN MPLS

Por lo tanto el protocolo BGP es el responsable del transporte de las rutas del cliente entre los PE.

- **Establecimiento de VRF´s:**

Al utilizar VPN sobre la red MPLS nace el concepto de tablas de rutas virtuales o VRFs, que no es más que tener tablas de rutas independientes dentro del mismo router; esta información únicamente la conocerán los sitios que comparten la misma VPN, para la seguridad y privacidad de los datos.

Esta VRF, estará asociada a una interfaz o sub-interfaz de donde se conecta el usuario del COMACO, Fuerza Terrestre, Naval o Aérea, por lo cual la denominación de las VRF´s se describe en la Tabla No 60:

Tabla No 60.- Nominativos VRF´s.

APLICACIÓN	VRF
VIDEO:	VIDEOCOMACO
	VIDEOFT.
	VIDEOFN.
	VIDEOFAE

CONTINÚA ⟶

VOZ	VOZCOMACO
	VOZFT
	VOZFN
	VOZFAE
DATOS	DATOSCOMACO
	DATOSFT
	DATOSFN
	DATOSFAE

La Creación de las VRF´s, será responsabilidad del administrador de la red, pero se mantendrá el principio de anteponer el servicio y la Fuerza a la que pertenece la VRF. Dentro de cada VRF, se empleará el concepto de **Route Distinguisher (RD),** que permite a la dirección IPv4 hacerla globalmente única (ruta privada) y utilizará el formato AS:XXYYYY, donde AS indica el número de sistema autónomo de la red MPLS, que en este caso se define el 65100; los valores XX indican la Fuerza a la que corresponde la VRF y YYYY es un número consecutivo que en este caso se asignará al servicio proporcionado como lo describen las Tablas No 61 y 62 y también dependerá del administrador, quien deberá registrar y llevar un control de las VRF´s .

Tabla No 61.- RD de VRF´s: XX.

La asignación de los valores XX es la siguiente: VRF	**XX**
COMACO	10
EJERCITO	20
NAVAL	30
AEREA	40

Tabla No 62.- RD de VRF´s: YYYY

La asignación de los valores YYY es la siguiente: VRF	XX
VOZ	0001
VIDEO	0002
DATOS	0003

Si un cliente desea conversar con más de una VRF, se empleará el concepto de Router Targets (RT); los cuales permiten elegir que rutas se exportan a los vecinos y que rutas se añaden a la tabla VRF.

En el caso del servicio de voz, se empleará una sola VRF denominada VOZCOMACO, en razón que la comunicación de la telefonía es entre todas las unidades militares. Para el servicio de datos y videoconferencia cada Fuerza tiene sus servidores propios al igual que el Comando Conjunto, por tal motivo las VRF´s para estas aplicaciones serán propias de cada Fuerza, es decir existirán VRF´s: DATOSFAE, DATOSCOMACO, DATOSFT, DATOSFN, etc. En el caso que estas VRF´s por situaciones particulares, operacionales se deseen comunicar o compartir información se aplicará VRF´s complejas variando los RT en cada una de ellas, por lo cual se recomienda aplicar el siguiente concepto:

Ejemplo para la simulación:

Se desea compartir los datos de las VRF´s DATOSFAE y DATOSCOMACO, se empleará diferentes RD´s en cada VRF y el RT se asignará con la siguiente numeración, en este caso el valor XX será 50 y el valor YYY se ubicará con 0001 al import y 0002 al export, cuyos valores serán invertidos en el otro LER:

En LER-1: RT: 65100:500001 import y 65100:500002 export.

En LER-2: RT: 65100:500001 export y 65100:500002 import

3.5.2.-Empleo MPLS en la red:

- **Distribución de etiquetas:**

Para el diseño se empleará el protocolo LDP, para la distribución de etiquetas. Como se explicó el funcionamiento de la tecnología MPLS en el capítulo 2, los equipos LER son los responsables de manejar el tráfico entrante, realizando la función de etiquetar los paquetes (modo push) o retirar etiquetas (modo pop) y reenviando el paquete por la mejor ruta y los LSR serán los responsables de realiza el swap de etiquetas o intercambio de etiquetas; es decir, el únicamente revisa la etiqueta del paquete entrante y basada en su tabla de etiquetas de envió, realiza un intercambio de etiqueta y la envía por la interfaz basada en la IP de destino.

De la información contenida en las tablas FIB (Forwarding Information Base) y LFIB (Label Forwarding Information Base), se crea rutas LSP a través de los LSR, para que el paquete llegue a su destino. La tabla LIB (Label Information Base) es la que almacena todas las etiquetas que son asignadas por el LSR y estas son asociadas con las etiquetas que son enviadas por sus vecinos. Las etiquetas asignadas por el LSR tienen un significado local.

- **Convergencia en el caso de fallas:**

Para explicar la convergencia de fallas, se describe la Figura No 65 en donde los routers ya han levantado sesiones LDP con sus vecinos y con ellos se realizó el intercambio de etiquetas:

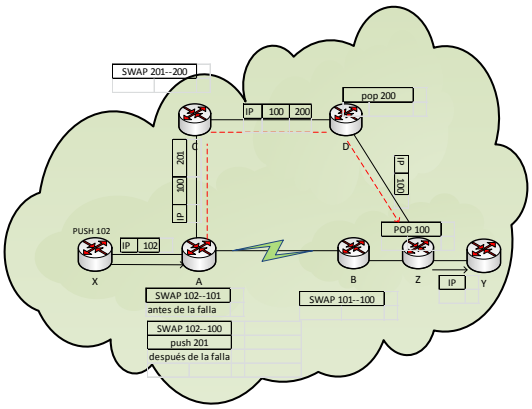


Figura No 65.- Convergencia en caso de fallas

El roter A, recibe un paquete del router X, queriendo alcanzar una ip del router Y, previamente el router A selecciona el LSP que se conecta con el router B. La ruta se dirige a través del router C, seleccionada previamente como ruta de respaldo. Este seré el concepto para el envió de la información en caso de fallas mediante la tecnología MPLS. Para la simulación se establecerá caídas de enlace para la convergencia en el caso de fallas y se verificará los caminos empelados para la transmisión de la información entre dos usuarios en la nube MPLS.

- **Capacidades en los enlaces:**

Las capacidades de los enlaces en base a las necesidades y capacidad propia de la red de transporte, considerando lo descrito en la Tabla No 45 del capítulo 2, serán las definidas en la Figura No 66:

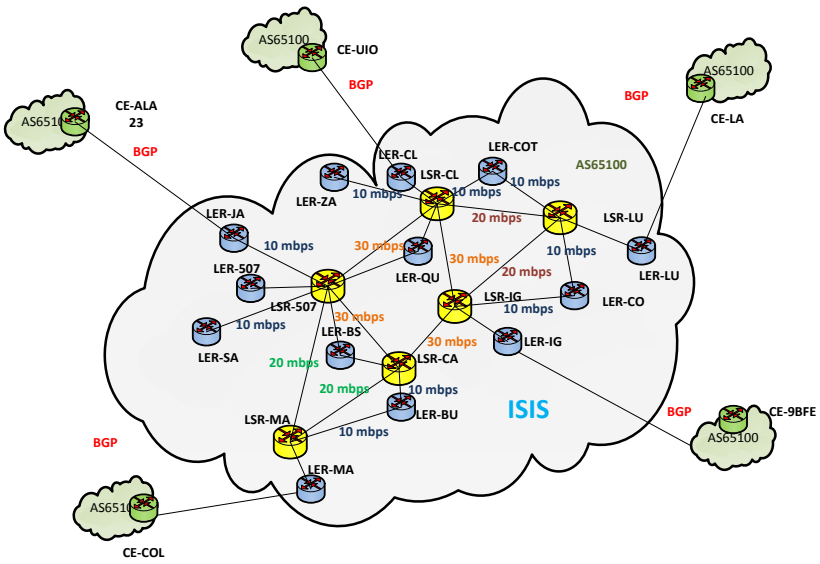


Figura No 66.- Capacidades de los enlaces.

Con estas capacidades se determina la necesidad a corto plazo, de elaborar un proyecto para ampliar la capacidad de los enlaces de la red de transporte a una tecnología de mayor capacidad que la actual PDH o SDH.

- **Direccionamiento:**

Para el direccionamiento se definirá de la siguiente manera:

a) ENTRE LSR-LSR Y LSR-LER:

RED: 10.68.0.0: Para cada enlace entre LSR-LSR y LSR-LER mascara con 30, como lo describe la Tabla No 63.

Ejemplo:

Tabla No 63.- IP ENTRE LSR-LSR Y LSR-LER:

ORD	ORIGEN	IP ORIGEN	DESTINO	IP DESTINO
1	LSR-CL	10.68.0.6	LSR-LU	10.68.0.5
2	LSR-CL	10.68.0.21	LSR-IG	10.68.0.22
3	LSR-CL	10.68.0.30	LSR-507	10.68.0.29
4	LSR-CL	10.68.0.17	LER-CL	10.68.0.18
5	LSR-LU	10.68.0.65	LER-LU	10.68.0.66
6	LSR-LU	10.68.0.14	LSR-IG	10.68.0.13
7	LSR-IG	10.68.0.37	LSR-CA	10.68.0.38
8	LSR-IG	10.68.0.25	LER-IG	10.68.0.26
9	LSR-CA	10.68.0.45	LSR-507	10.68.0.46
10	LSR-CA	10.68.0.57	LSR-MA	10.68.0.58
11	LSR-MA	10.68.0.69	LER-MA	10.68.0.70

b) ENTRE LER-CE:

RED: 10.67.0.0: Para cada enlace entre LER-CE mascara con 30 como lo describe la Tabla No 64:

Ejemplo:

Tabla No 64.- IP ENTRE LER-CE:

ORD	ORIGEN	IP ORIGEN	DESTINO	IP DESTINO
1	LER-CL	10.67.0.5	CE-UIO	10.67.0.6
2	LER-LU	10.67.0.13	CE-LA	10.67.0.14
3	LER-IG	10.67.0.9	CE-9BFE	10.67.0.10
4	LER-MA	10.67.0.17	CE-COL	10.67.0.18

Adicional como se empleará sub-interfaces para las VRF´s de los diferentes servicios estas serán designadas variando el segundo octeto de la dirección ip, es decir:

DATOS: 10.67.0.13

VOZ: 10.67.10.13

VIDEO: 10.67.20.13

Y las VLAN´s creadas entre los LER y CE serán igual designadas por servicios:

DATOS: VLAN 10

VOZ: VLAN 20

VIDEO: VLAN 30.

c) LOOPBACK:

Las direcciones loopback empezarán desde 10.68.254.1 máscara 32 como lo describe la Tabla No 65:

LSR: 10.68.254.1-10.68.254.50

LER: 10.68.254.51-10.68.254.150

CE: 10.68.254.151-10.68.254.251

Tabla No 65.- IP LOOPBACK:

ORD	NOMINATIVO	DIRECCIÓN
1	LSR-CL	10.68.254.1
2	LSR-507	10.68.254.2
3	LSR-MA	10.68.254.3

CONTINÚA ⟶

4	LSR-CA	10.68.254.4
5	LSR-IG	10.68.254.5
6	LSR-LU	10.68.254.6
7	LER-CL	10.68.254.52
8	LER-LU	10.68.254.53
9	LER-IG	10.68.254.54
10	LER-MA	10.68.254.55
11	CE-UIO	10.68.254.151
12	CE-LA	10.68.254.152
13	CE-9BFE	10.68.254.153
14	CE-COL	10.68.254.154

Este direccionamiento facilitará la administración de la red, por lo cual deberá llevarse en un registro asignada por el Comando Conjunto.

- **Calidad de Servicio:**

Dentro de la cabecera del paquete IP existe un campo denominado ToS (Type of Service), formado de 8 bits cuya función es indicar la importancia del paquete. En la siguiente figura se muestra la ubicación del campo ToS dentro de la cabecera IP.

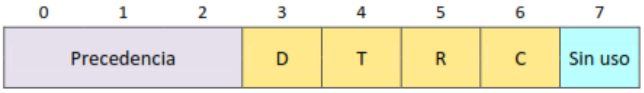


Figura No 67.- Estructura ToS.

Como se observa en la Figura No 67, los 3 primeros bits se denominan *"Precedencia"* usado para asignar un nivel de prioridad al datagrama IP. Se tendrían con estos tres bits ocho niveles, pero los dos valores máximos están reservados para la utilización interna de la red, teniendo disponible seis Clases de Servicios.

El campo ToS dentro del Modelo de Servicios Diferenciados se lo conoce también como campo DS (DiffServ). Dentro del campo DS los seis primeros bits se denominan DSCP (DiffServ Code Point) mientras que los dos últimos bits están reservados. Con los otros 6 bits restantes es posible obtener 64 combinaciones o posibles tipos de servicios.

Para el diseño se empleará la Tabla No 66 con las diferentes clases de servicio:

Tabla No 66.- QOS DSCP:

CLASE	DSCP (Binary)	DSCP (Decimal)	Ip precedence (PHP)	Per-Hop-Behavior	TOS
VOZ	101110	46	5	Expedited Forwarding (EF)	184
VIDEO	100010	34	4	AF41	136
DATOS CRÍTICOS	011010	30	3	AF31	104
DATOS NO CRÍTICOS	010010	18	2	AF21	72

El procedimiento para la calidad de servicios será el siguiente:

a. Clasificación y marcaje:

Para el ingreso del tráfico al LER:

1. Clasificación:

La clasificación será en base a las clases descritas en la Tabla No 66 y el marcado en referencia al valor de PHB:

Ejemplo:

Class-map match-any Clase-video-in

match dscp AF41

match vlan 30

match input-interface FastEthernet 3.3

2. Marcaje en la política de entrada:

Una vez que los paquetes están clasificados se someten a ciertas reglas que son especificadas dentro de una política a la entrada por el router.

Ejemplo:

Policy-map política-in

Class Clase-video-in

Set precedence 4

3. Asignación de la política a la interfaz de entrada:

Interface fastEthernet 3.3

Service-policy input política-in.

Para el egreso del tráfico del LER:

Ejemplo:

1. Clasificación:

Class-map match-any Clase-video-out.

Match precedence 4

2. Marcaje en la Política:

Policy-map política-out

Class Clase-video-out

Set mpls experimental topmost 4

Bandwidth percent 20

3. **Asignación de la política a la interfaz de salida:**

Interface fastEthernet 2

Service-policy output política-out.

Para el ingreso del tráfico al LSR:

1. **Clasificación:**

Ejemplo:

Class-map match-any Clase-video-in

match mpls experimental 4

2. **Creación de la política de entrada:**

Policy-map política-in

Class Clase-video-in

Set precedence 4

3. **Asignación de la política a la interfaz de entrada:**

Interface fastEthernet 4

Service-policy input política-in.

Para el egreso del tráfico del LSR:

Ejemplo:

1. **Clasificación:**

Class-map match-any Clase-video-out

Match precedence 4

2. Política:

Policy-map política-out

Class Clase-video-out

Set mpls experimental topmost 4

Bandwidth percent 20

3. Asignación de la política a la interfaz de salida:

Interface fastEthernet 2

Service-policy output política-out.

b. Manejo de la Congestión

Para el manejo de la congestión se garantiza en las políticas de salida un ancho de banda mínimo para cada servicio en la política de salida, en este caso como ejemplo para simulación está definido de la siguiente manera:

- Para el video un Bandwidth de 30, en porcentaje relacionado a la capacidad del enlace (CBWFQ[4]).
- Para la voz un Bandwidth de 20, con prioridad para este servicio (LLQ[5]).
- Para datos un bandwidth de 10, en porcentaje relacionado a la capacidad del enlace (CBWFQ).

c. Policing and shaping:

Para evitar la congestión se configurará policing y shaping bajo el siguiente concepto: para la voz se adicionará la política de policing a la entrada de la interfaz, a fin de descartar los paquetes que superen el 20 por ciento de ancho de banda:

Police percent 20

conform-action transmit

[4] CBWFQ: Class-based weighted fair queueing
[5] LLQ: Low-latency queuing

exceed-action drop

Para la aplicación de datos se aumentará la política de shaping a la salida de la interfaz, que permitirá el encolamiento de paquetes que serán transmitidos una vez que exista disponibilidad de ancho de banda:

Shape averange percent 10.

Este criterio se debe a su relación con los servicios en tiempo real, es decir para la voz en especial no sería de utilidad aplicar shaping ya que no es conveniente encolar los paquetes en este tipo de servicio, pero sí es válido para los datos.

- **Ingeniería de Tráfico:**

Con la finalidad de adaptar los flujos de tráfico a los enlaces físicos se empleará túneles mediante rutas explícitas, empleando el protocolo RSVP y se aplicará especialmente en aquellos nodos donde exista mayor concurrencia de usuarios, a fin de que el tráfico que salga de un equipo LER pueda adoptar diferentes rutas y evitar el congestionamiento y cuellos de botella.

Para la simulación se analizará la ruta que toma el tráfico de un usuario y se inducirá a que el mismo tráfico viaje por otra ruta, con esto se visualizará el funcionamiento del concepto de túneles MPLS.

CAPÍTULO 4
MODELAMIENTO Y EVALUACIÓN DE LA PROPUESTA.

4.1.-Modelamiento de la solución en la plataforma OPNET.

4.1.1.- Configuración de Protocolos de enrutamiento: OSPF:

Para crear los escenarios en OPNET, en la pantalla principal se ejecuta *File-New* y colocamos el nombre del proyecto y escenario a desarrollar. Mediante la opción *View-Zoom*, se puede elegir la zona en donde se va a desarrollar la simulación. Los equipos de networking son insertados mediante la opción *Topology-Object Palette* , en donde se presentará una variada gama de equipos y tecnologías a emplearse como lo muestra la Figura No 68, en este caso se buscará los equipos en la opción de Cisco:

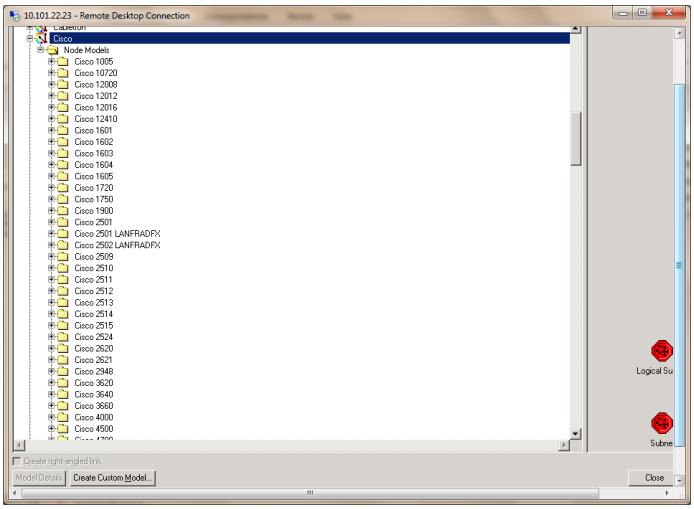


Figura No 68.- Opción Cisco.

Para la simulación planteada, el software no dispone de los equipos definidos en el capítulo 3, en razón que son los últimos equipos desarrollados por Cisco con tecnología MPLS para NGN. Sin embargo en este software existen equipos que dispone de esta tecnología pero de menor capacidad, por lo cual se empleará la serie 7600 para equipos tipo LSR, 7200 para equipos tipo LER y 2600 para los de tipo CE.

En razón de que es la primera vez que se emplea este software para la simulación de redes se realizará el modelamiento desde la configuración y empleo de protocolos

de enrutamiento con el algoritmo de Dijkstra como son OSPF y IS-IS. La primera estructura de modelamiento se presenta en la siguiente figura mediante la configuración del protocolo OSPF, para lo cual se configura cada equipo de la siguiente manera:

- En el router, mediante click derecho *Edit Atributtes-IP-Ip Rounting Parameters*, se configura la IP de cada interfaz con su respectiva máscara, así como la selección del protocolo OSPF como lo indica la Figura No 69. Este procedimiento se realiza en todas las interfaces y en la interfaz loopback de cada router con área 0:

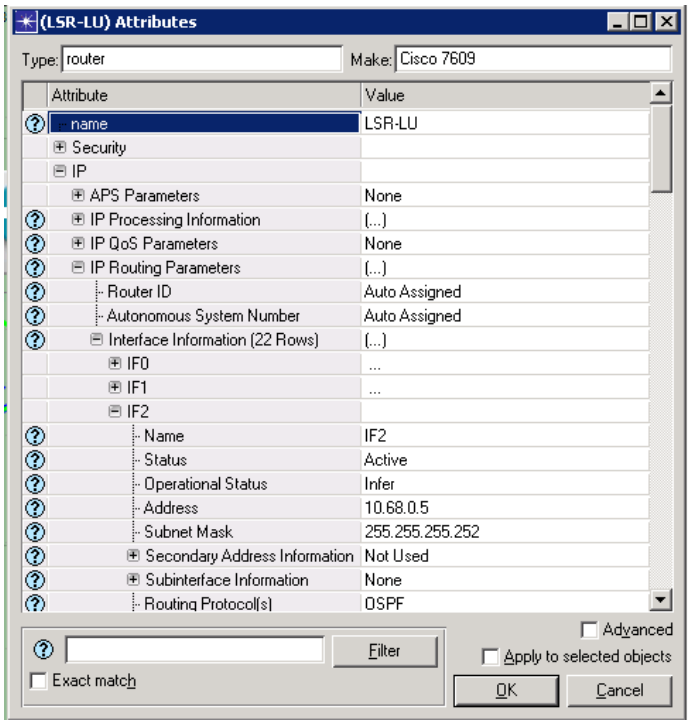


Figura No 69.-Configuración interfaces.

- Se habilita el protocolo en el router, mediante *IP Rounting Protocolos-OSPF*, señalando el número de proceso establecido y habilitando el proceso en cada interfaz del router, como lo presenta la Figura No 70:

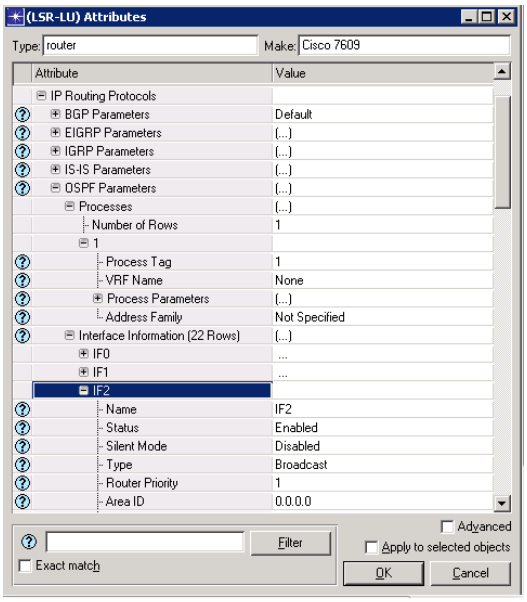


Figura No 70.- Configuración protocolo OSPF.

- Se genera tráfico entre los nodos deseados mediante *Object Palette* y se busca la opción *Demand Models* y encontraremos alternativas como *IP Ping Traffic Flow y IP Traffic Flow.*

- Para establecer el tráfico deseado se realiza un click derecho Edit Attributes en el *IP Traffic Flow* trazado entre dos nodos y en la opción Traffic seleccionamos un tráfico establecido en el software o editamos el tráfico bajo un requerimiento puntual señalado en la Figura No 71:

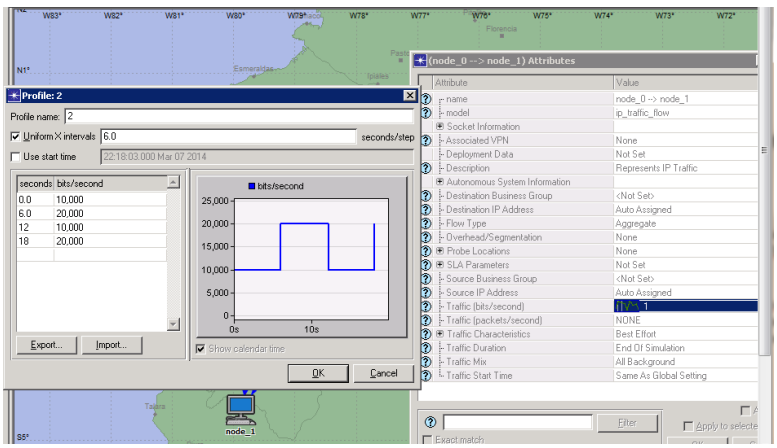


Figura No 71.- Tráfico editado entre dos nodos.

- Para visualizar el resultado de igual manera con click derecho en el tráfico trazado y la opción *Choose Individual DES statistics*, se selecciona *Traffic received y Traffic send* en bits/seg.

- Para simular y comprobar el funcionamiento de los protocolos de enrutamiento se agrega el icono *Failure Recovery* desde el Object Palette.

Existen dos formas de generar el tipo de tráfico: con los iconos Aplication Definition y Profile Definition, creados desde el Object Palette o mediante click derecho en el tráfico trazado entre los nodos y en la opción Edit Attributes-Traffic Characteristics, definiendo un tipo de servicio que será empleado especialmente en el escenario de calidad de servicio. A continuación en la Figura No 72 se presenta el primer escenario de simulación:

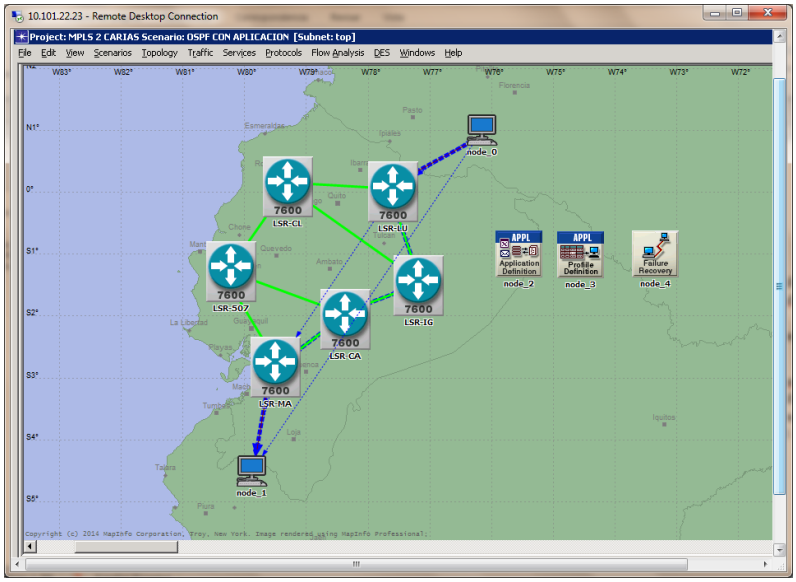


Figura No 72.- Escenario 1: OSPF.

4.1.2.- Configuración de Protocolos de enrutamiento: IS-IS:

- Para la configuración de IS-IS, se realiza el procedimiento similar a OSPF, pero en el router, mediante *IP Rounting Protocolos-IS-IS-Processe-Process Parameters-Network Entity Title*, se establece el campo NSAP descrito en el capítulo 3, con el system type level-2 como se indica en la Figura No 73:

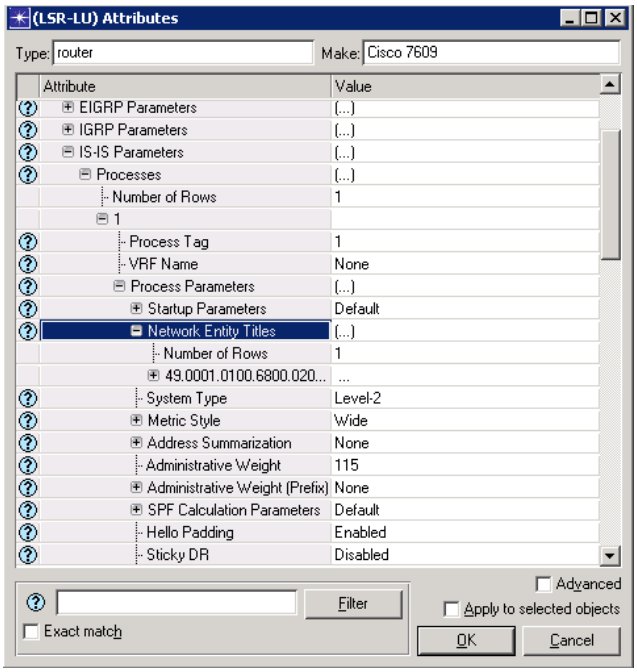


Figura No 73.- Configuración protocolo IS-IS.

- Igual que en OSPF, se habilita el protocolo en las interfaces físicas y en la loopback. El escenario IS-IS se presenta en la Figura No 74:

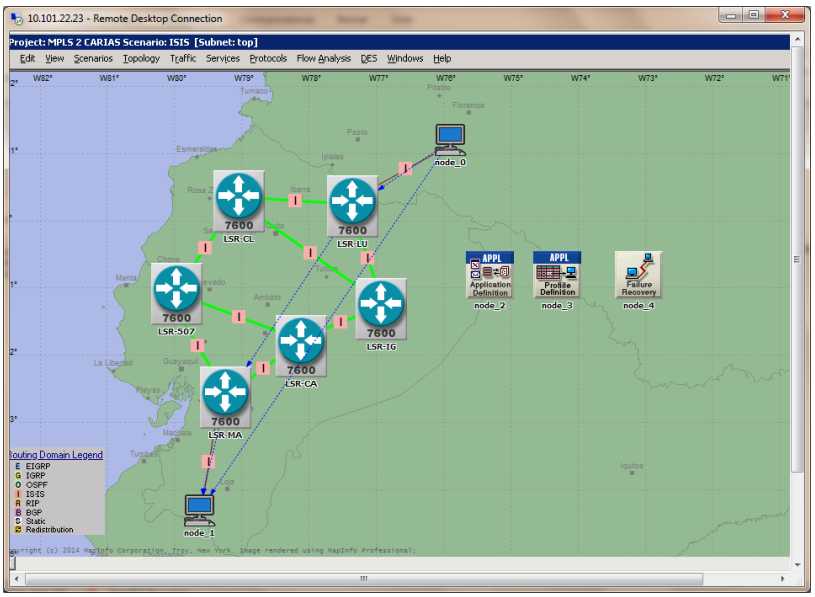


Figura No 74.- Escenario 2: IS-IS.

4.1.3.- Configuración del Protocolo LDP y MPLS:

Para habilitar el protocolo de distribución de etiquetas se realiza el siguiente procedimiento en cada router de la nube MPLS:

- Click derecho en cada router, *Edit Atributtes-MPLS-LDP Parameters*, se habilita el status Enable y en cada interfaz física y loopback que pertenece a la nube MPLS como lo indica la Figura No 75:

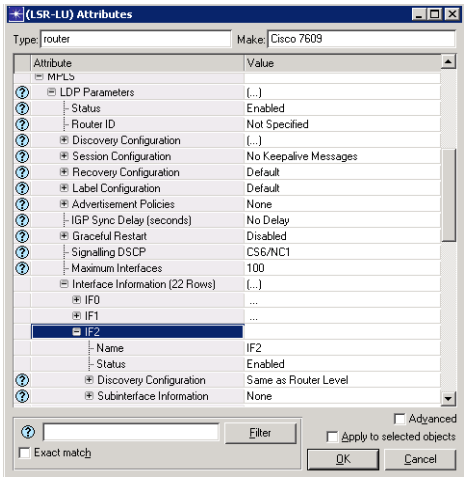


Figura No 75.- Protocolo LDP.

- Click derecho en cada router, *Edit Atributtes-MPLS-MPLS Parameters*, se habilita el status Enable y en cada interfaz que pertenece a la nube MPLS como lo muestra la Figura No 76:

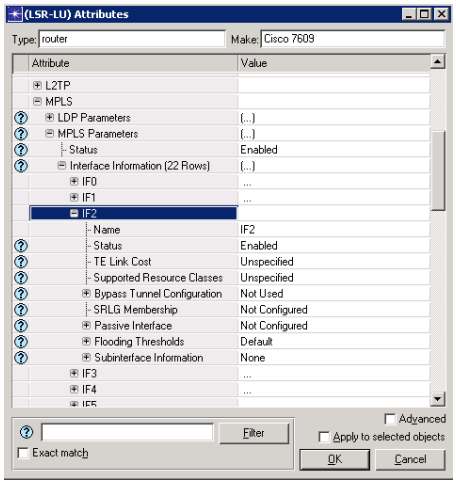


Figura No 76.- Habilitación MPLS.

4.1.4.- Configuración de VPN:

Para crear las VPN entre los routers tipo LER´s se realiza el siguiente procedimiento:

- Click derecho en los routers LER que se requiere formar la vpn, en la opción *VPN-Network Based-VRF instances-Number of rows-1*.
- Se coloca el nombre de la VRF, el Route Distinguisher y Route Target definido en el capítulo 3, en este caso para la voz de COMACO, que por ser un servicio compartido tendrá la característica de both configurada en las Figuras No 77 y 78:

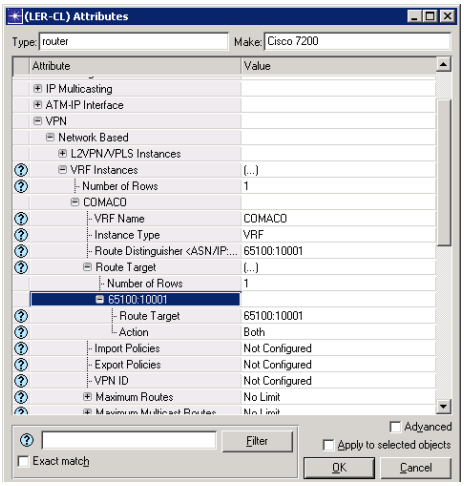


Figura No 77.- Configuración VPN.

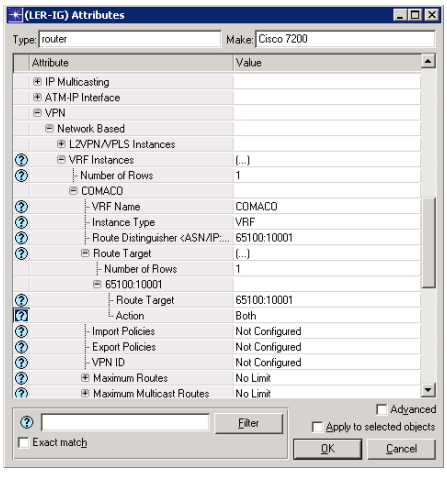


Figura No 78.- Configuración VPN.

4.1.5.- Configuración del Protocolo MP-BGP y redistribución con OSPF:

El protocolo IBGP, permite enviar tráfico entre sitios remotos, para lo cual empleará la redistribución de las rutas de los CE´s que operan con OSPF y se configurará de la siguiente manera:

- En cada router tipo LER o PE click derecho *Edit Atributtes-IP Routing Protocols-BGP Parameters-Status-Enable.*
- En Address Family Parameters, se habilita los parámetros IPv4 y VPNv4 asociada a la VRF creada como lo indica la Figura No 79:

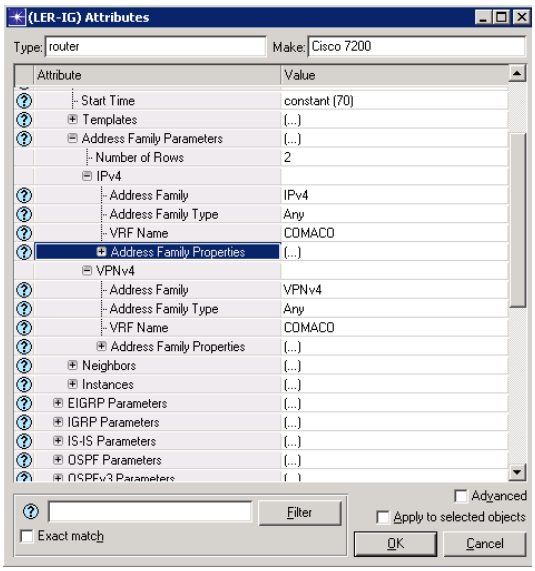


Figura No 79.- Habilitación IPv4 y VPNv4

- Una configuración importante es la distribución de las rutas de los CE´s, para lo cual se habilita la redistribución en BGP como lo muestra la Figura No 80. Para este caso los CE´s disponen de una configuración con protocolo OSPF, por lo cual la redistribución está configurada en: *BGP Parameters-Address Family Parameters- IPv4-Address Family Properties- Redistribución-Routing protocols-OSPF-Number Rows-1-Enable:*

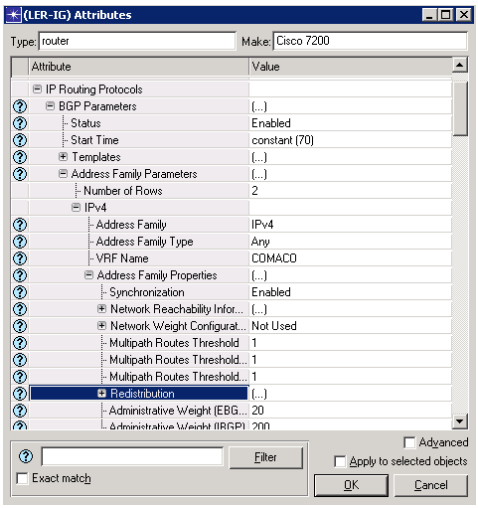


Figura No 80.- Redistribución OSPF en BGP.

- Como la distribución es OSPF sobre BGP, se debe habilitar en la opción IP *Routing Protocolos-OSPF Parameters-process Tag-1(*proceso OSPF configurado*)-VRF name-VOZCOMACO (*VRF creada*)* como indica la Figura No 81, la redistribución en *Process Parameters-Redistribution*, protocolo BGP:

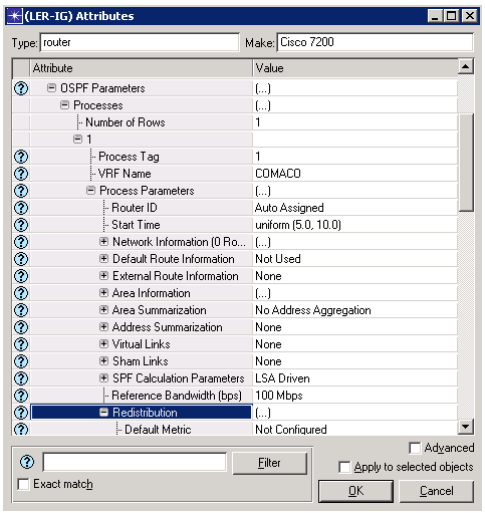


Figura No 81.- Redisribución BGP en OSPF

- Realizada la redistribución, en *BGP Parameters-neighbors*, añadimos la dirección loopback del vecino LER en el cual se crea la vpn. Para este caso en el LER-IG, se añade la IP de su vecino el LER-CL como lo demuestra la Figura No 82:

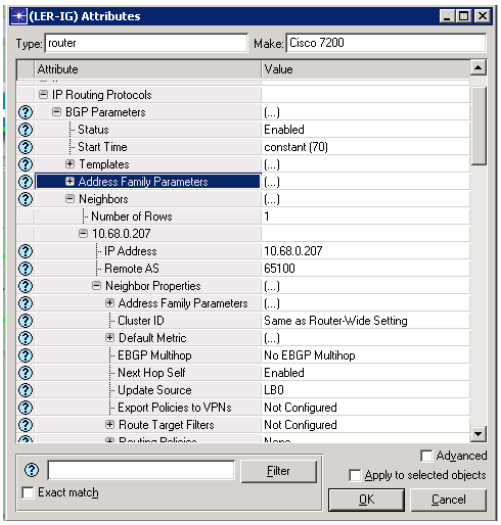


Figura No 82.- Configuración neighbor BGP.

- Los parámetros configurados en el vecino BGP son: *Next Hop Self*, para que el next hop sea el router local que será quien aprenda las rutas de su vecino BGP; *Update source-LBO*, ya que todas las actualizaciones será por la dirección loopback; *Send Community-Both,* para garantizar que los atributos de la comunidad sean enviado a su vecino *BGP*.

Para este escenario se debe recalcar que la configuración de la interfaz F3 del LER-IG, está configurada con OSPF, proceso 1, área 0 y es la interfaz conectada con el CE del usuario que maneja OSPF. La interfaz F2 del router LER-IG tiene como protocolo IS-IS y es parte de la nube MPLS, como lo señala la Figura No 84.

Con esta configuración se logra que el router LER, tenga conexión OSPF con el usuario y se cree la conexión MP-BGP con el LER vecino, para lo cual emplea el protocolo IS-IS para la distribución de etiquetas en la nube MPLS. Es importante mencionar que para este proceso se ha configurado como sistema autónomo el AS:65100, en *IP-Ip Routing Parameters-Autonomous System Number*, como lo señala la Figura No 83:

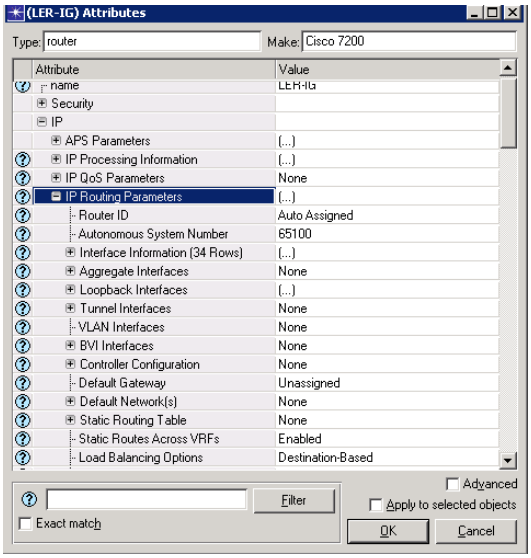


Figura No 83.- Configuración Sistema Autónomo.

A continuación en la Figura No 84, se presenta el escenario No 3.- MP-BGP:

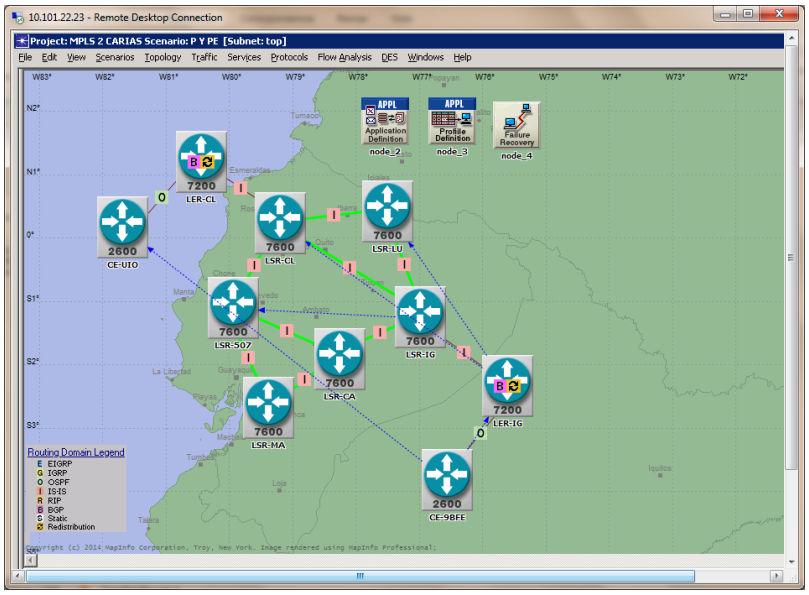


Figura No 84.- Escenario 3: Configuración MP-BGP.

4.1.6.- Configuración de distintas VPN´s con diferentes usuarios:

Para comprender el uso de las VPN´s y la configuración descrita en el capítulo 3 para el RD y RT, a continuación se realiza el escenario de la Figura No 86 con distintas VRF compartidas para diversos usuarios como lo señala la Tabla No 67 y Figura No 85:

Tabla No 67.- RD y RT para diferentes servicios.

LER	VRF´S	RD Y RT
LER-LU	DATOSFAE	RD Y RT: 65100:40003
	VOZCOMACO	RD Y RT: 65100:10001
	VIDEOFAE	RD Y RT: 65100: 40002
LER-MA	DATOSFAE	RD Y RT: 65100:40003
	VOZCOMACO	RD Y RT: 65100:10001
	VIDEOFAE	RD Y RT: 65100: 40002
LER-IG	VOZCOMACO	RD Y RT: 65100:10001
LER-CL	VOZCOMACO	RD Y RT: 65100:10001

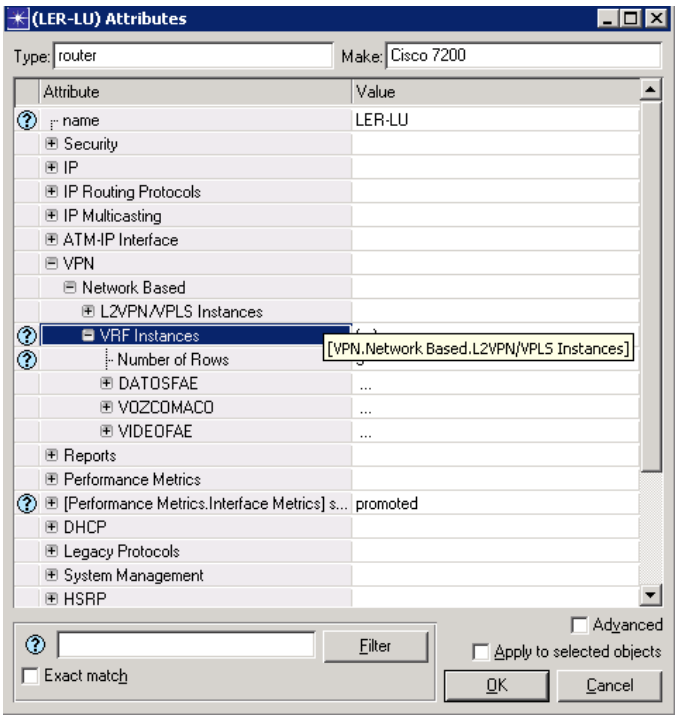


Figura No 85.- VPN VOZFAE

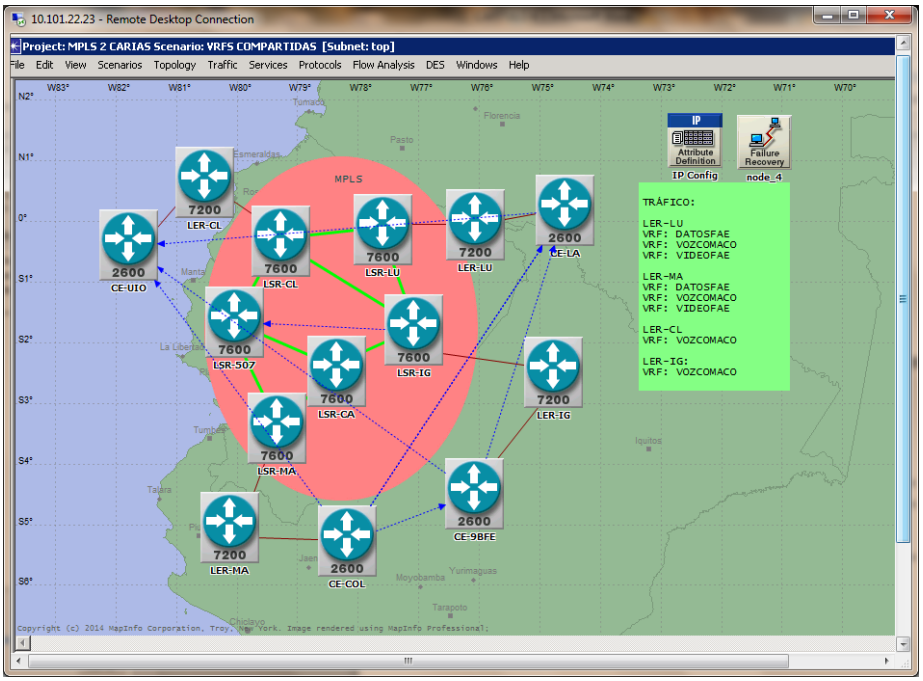


Figura No 86.- Escenario 4: VRF´s distintas para diferentes usuarios

4.1.7.- Configuración de VPN´s complejas:

Se denominarán VRF´s complejas, a los servicios que compartirá determinado usuario con otro usuario específico, sin que este servicio específico sea compartido con los otros usuarios, para lo cual se planteará el escenario descrito en la Figura No 91, mediante la siguiente configuración:

El LER-LU para el usuario de Lago Agrio que corresponde a la FAE, dispondrá de los siguientes servicios:

- VIDEOFAE
- DATOSFAE y
- VOZCOMACO.

El LER-MA para el usuario de Machala-Estación Radar Colibrí dispondrá de servicios como:

- VOZCOMACO
- VIDEOFAE y
- DATOSCOMACO.

Es decir la particularidad de este escenario es que los usuarios de FAE compartirán un servicio de diferente Fuerza, mediante DATOSCOMACO y DATOSFAE. Considerando que para las operaciones militares cierta información deberá ser compartida solo entre estos usuarios y no con los demás.

Los usuarios de Quito (UIO) y 9-BFE (Latacunga) compartirán el servicio de voz con los usuarios de Lago Agrio y Machala, pero no tendrán acceso a los demás servicios. Esto es alcanzado en base a lo descrito en el capítulo 3: "Establecimiento de VRF´s", es decir modificando el valor de RT con las propiedades de import y export. Para facilitar la administración de los servicios se ha creado VLAN´s entre los CE´s y PE´s:

- Con click derecho sobre cada router (LER-LU y LER-MA), Edit Atributtes-VPN, se crea las VPN´s descritas anteriormente. La particularidad es que para la compartición del servicio de DATOSCOMACO y DATOSFAE se configura dos RT´s: uno configurado como RT import en un router y en el otro export y otro RT como export en un router e import en el otro. De esta manera lo que el uno importe en este servicio será exportado por el otro y de manera inversa como lo detalla la Figura No 87:

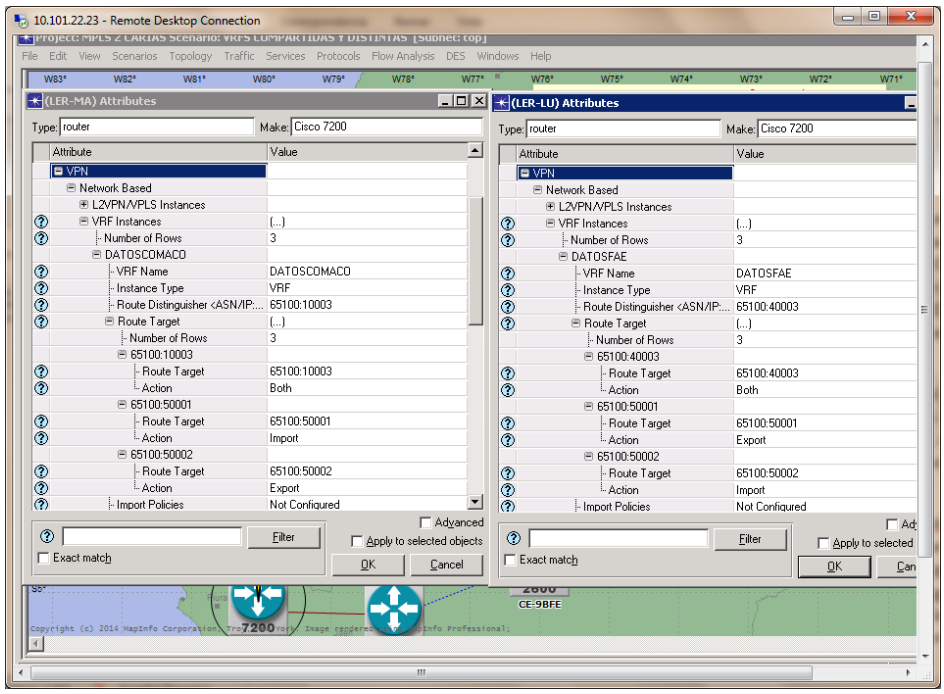


Figura No 87.- VRF´s con import y export.

- Los otros servicios (VOZCOMACO y VIDEOFAE) en el LER-LU y LER-MA, serán configurados como se detalló en el numeral 4.1.4: “Configuración de VPN´s”.

- Para los otros usuarios, es decir para UIO y 9 BFE, como es un servicio común de VOZCOMACO, se seguirá el procedimiento detallado en el numeral 4.1.4: “Configuración de VPN´s”.

- Las VLAN´s entre los CE´s y PE´s serán configuradas mediante sub-interfaces lógicas en cada interfaz física que conecta estos routers como lo describe las Figuras No 88 y 89:

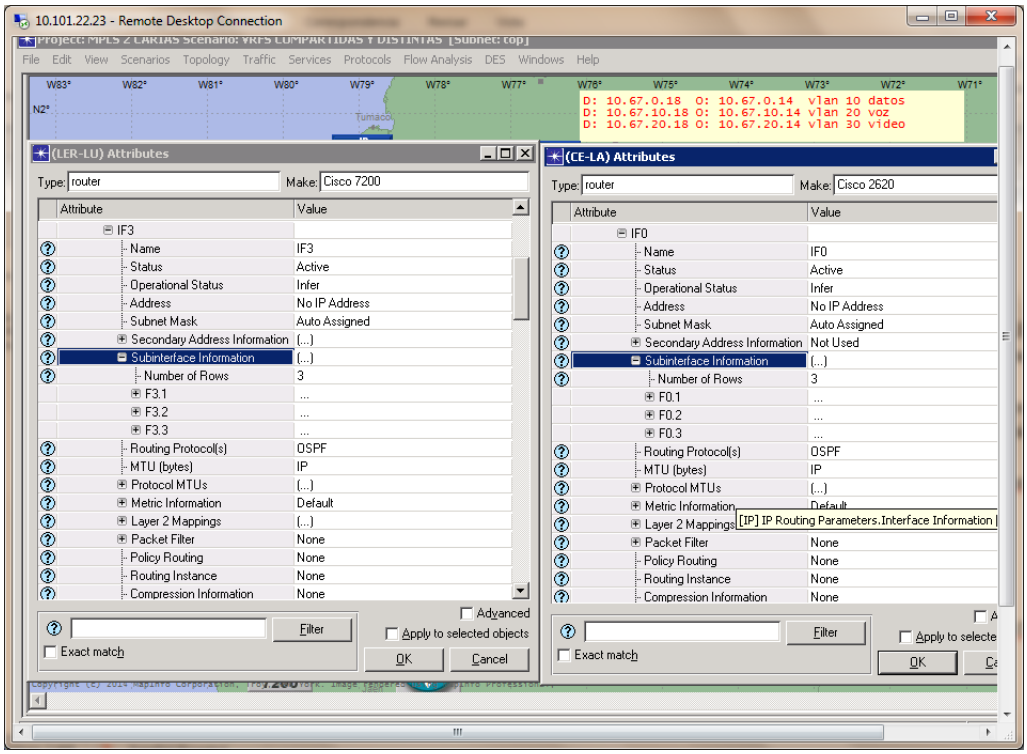


Figura No 88.- Sub-interfaces lógicas entre CE´s y PE´s.

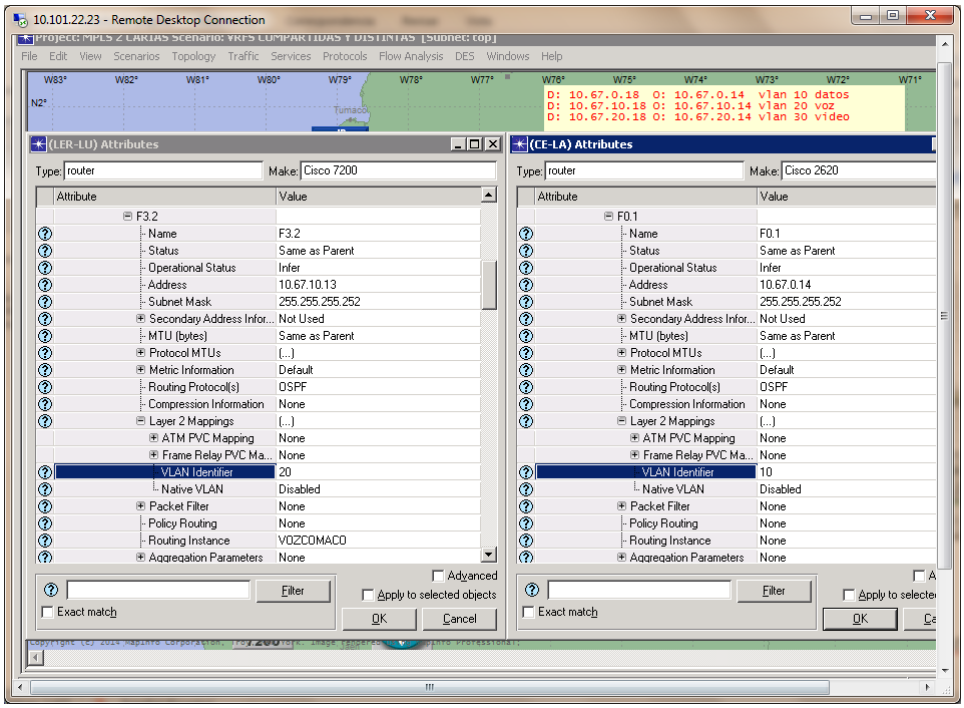


Figura No 89.- VLAN´s creadas en cada interface.

- Como cada direccionamiento de los servicios, le corresponderá una VRF en una sub-interfaz como lo indica la Figura No 90, se asociará estas a un proceso OSPF que será configurada en el LER y CE. Esto facilitará la verificación de cómo los routers aprenden las rutas de cada servicio:

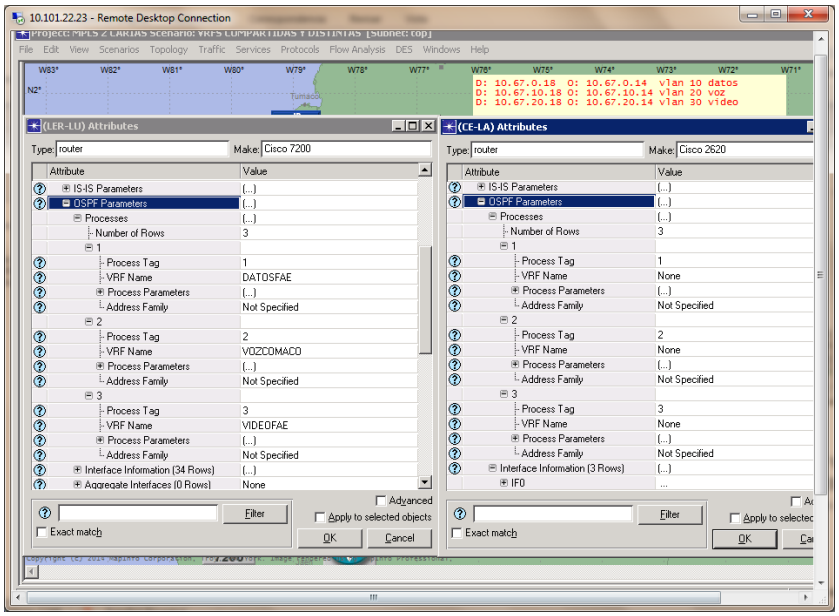


Figura No 90.- Procesos OSPF asociado a cada sub-inetrfaz.

Con este escenario se asocia una sub-interfaz con una VLAN para cada servicio según lo detallado en el capítulo 3: “Direccionamiento”. Con esta configuración se verificará lo descrito en la teoría para habilitación de VRF´s de distintos servicios modificando los RT´s.

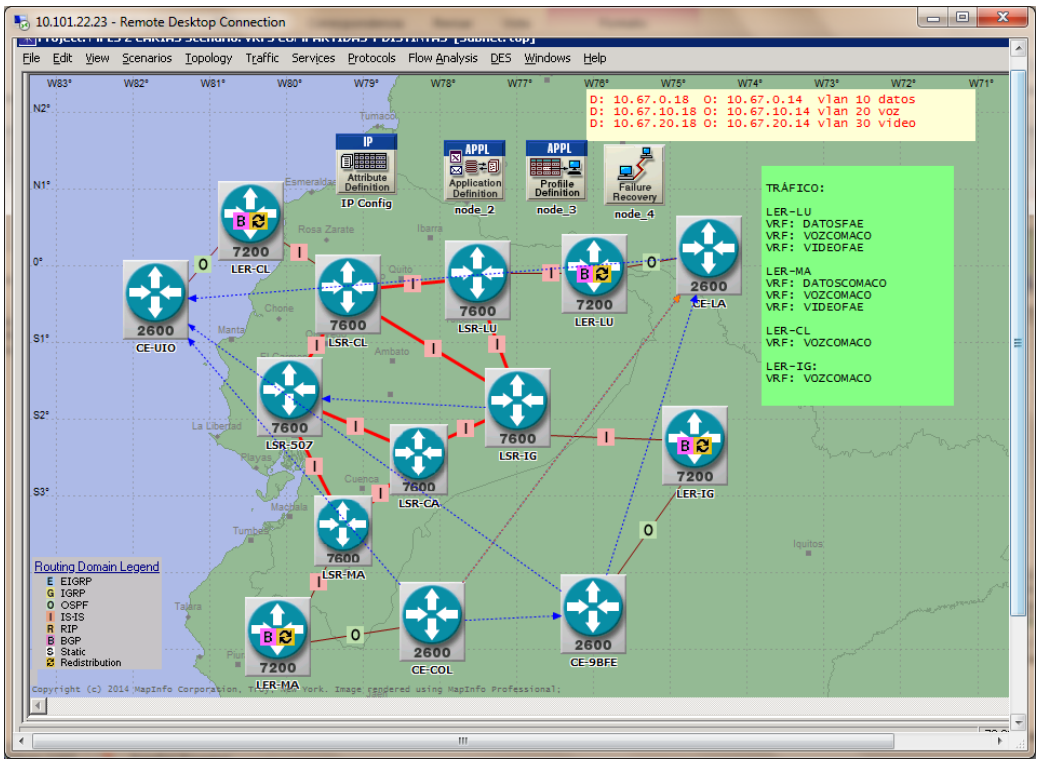


Figura No 91.- Escenario 5: VRF´s complejas.

4.1.8.- Configuración de QoS MPLS:

Para la implementación de la calidad de servicios se realizará la clasificación, el marcaje y la implementación de la política, en base a lo descrito en el capítulo 3, cuya configuración será la siguiente:

a) Clasificación y marcaje:

- Creación de las clases: click derecho sobre cada *LER-Ip-Ip Qos Parameters-Traffic Class-Number of Rows*. Se coloca el número de clases deseadas en este caso se creará las clases Clase-video-in y Clase-video-out en el router LER-LU, para el tráfico que ingresa del usuario CE-LA.

- En cada clase se crearán las condiciones de match del tráfico que ingresará a este router, por lo cual dentro de cada clase se creará en *Number of Rows*, en este caso 3 alternativas DSCP con un match value asignado en QoS de AF41, Vlan con un match value de 30 asignado a la vlan de video e incoming interface con un match value de F3.3 asignada a la subinterfaz de video como lo describe la Figura No 92.

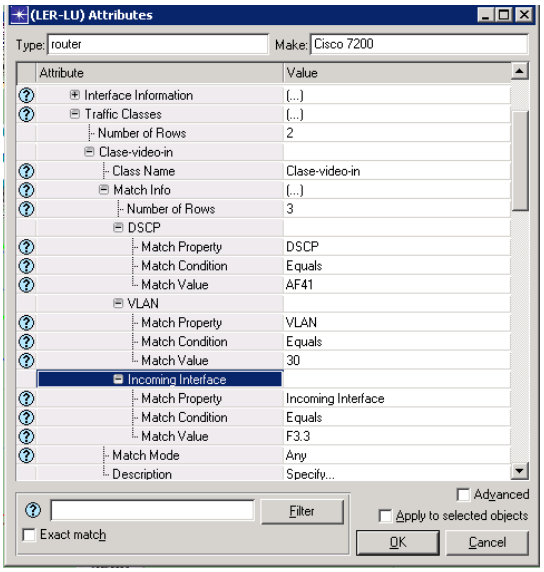


Figura No 92.- Clasificación de Clases QoS.

- Creada la clase se configurará la política de entrada, es decir el tipo de tratamiento que se realizará al tráfico ingresado bajo las condiciones descritas anteriormente. Para lo cual en *Ip Qos Parameters-Traffic Classes-Number of Rows*, se coloca el número de políticas que se desea crear.

- Una vez realizado el procedimiento anterior en *Policy Name*, se coloca el nombre de la política que está definido como política-in. En *Configuration-Number of Rows* se coloca el número de clases será asociada esta política, para esta simulación el *Class Name* será la Clase-video-in y en *Set Info*, se coloca el marcado que será establecido en esta política. En base a la tabla de QoS del capítulo 3, se establece como marcada *Precedence* con *Set value 4* como lo demuestra la Figura No 93.

- Para la política de salida se creará la *política-out* para la *Clase-video-out*, se establecerá en *Set Info*, el marcado *MPLS EXP-4*.

- Este procedimiento será realizado para las clases de entrada y salida, con la respectiva política en el LER y LSR como fue descrito en el capítulo 3 "Calidad de Servicio", quedando definido la clasificación y marcaje de QoS para los diferentes servicios que cursarán por la Red de datos de Fuerzas Armadas. Cabe recalcar que este marcaje está relacionado y fue definido en la Tabla No 66"QOS DSCP" del capítulo 3, en el cual se definió el diseño de la red y las facilidades MPLS que serán aplicadas en cada servicio. Sin embargo si se define otros servicio y/o aplicaciones, está tabla podría ser modificada por los administradores de la red.

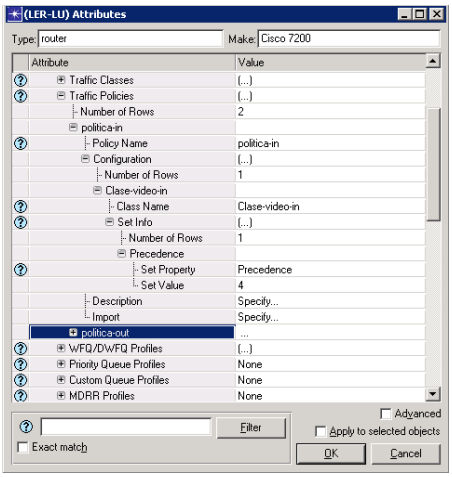


Figura No 93.- Configuración de marcaje QoS.

b) Manejo de Congestión:

Dentro de las políticas de QoS se establece el manejo de la congestión, asignando un determinado ancho de banda para cada servicio, en OPNET esto se configura de la siguiente manera:

- En *IP QoS Parameters-Traffic Policies-WFQ Profiles-Class-based- WFQ Profiles-Number of Rows,* se define el perfil de esta política para cada servicio como lo indica la Figura No 94. Para la simulación se establecerá:

Para el servicio de video:

Name: Bandwidth video

Badwidth Type: Relative

Badwidth value: 30

Para el servicio de voz:

Name: Priority voz

Badwidth Type: Relative

Badwidth value: 20

Priority: Enable.

Para el servicio de datos:

Name: Bandwidth datos

Badwidth Type: Relative

Badwidth value: 10

Priority: Enable.

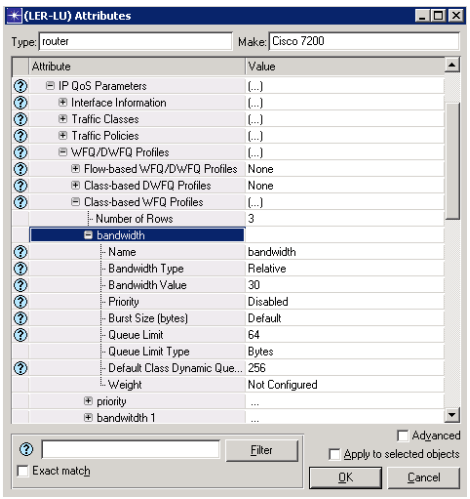


Figura No 94.- Configuración WFQ.

Esta configuración se asociará a la política de salida de cada servicio como lo muestra la Figura No 95, de la siguiente manera:

- En *IP QoS Parameters-Traffic Policies-politica-out* (política de salida creada)-*WFQ Profile-Set Property: WFQ profile (Class based)* y *Set Value* el nombre de la política creada en *WFQ Profiles-Class-based*, para el caso del video *bandwidth video:*

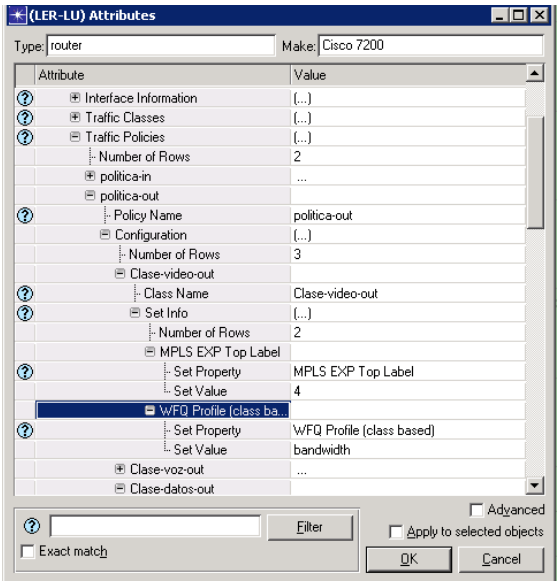


Figura No 95.- Asignación WFQ a la política de salida.

Por último cada política de entrada y salida será asociada a las interfaces de cada router, para el efecto se configura de la siguiente manera:

- El *IP-IP-QoS Parameters* en *Number of Rows* se agrega el número de interfaces de entrada y salida a las cuales se asociará las políticas, seleccionando en *Name* el nombre de la interfaz y en *Qos Scheme* en *Number of Rows* el número de políticas que serán asignadas, para el ejemplo *Type: Inbound Traffic Policy* y *Name: política-in* en la interfaz de entrada y *Type: Outbound Traffic Policy* y *Name: política-out* en la interfaz de salida. Lo descrito se ilustra e la Figura No 96.

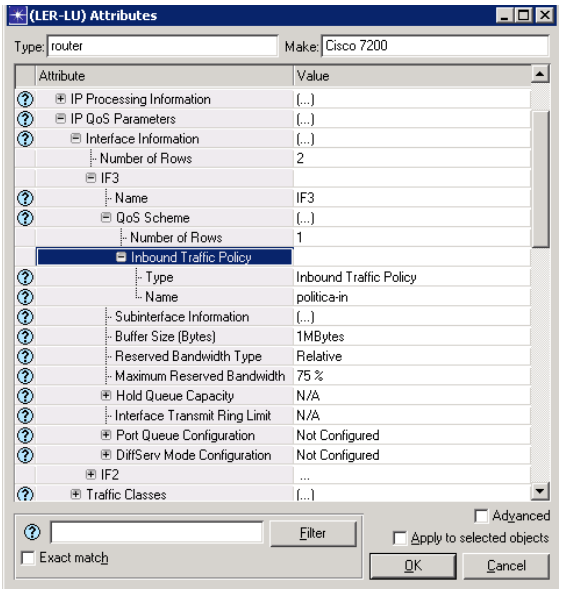


Figura No 96.- Asociación de la política a la interfaz.

Para la Calidad de servicios se establece el escenario descrito en la Figura No 97:

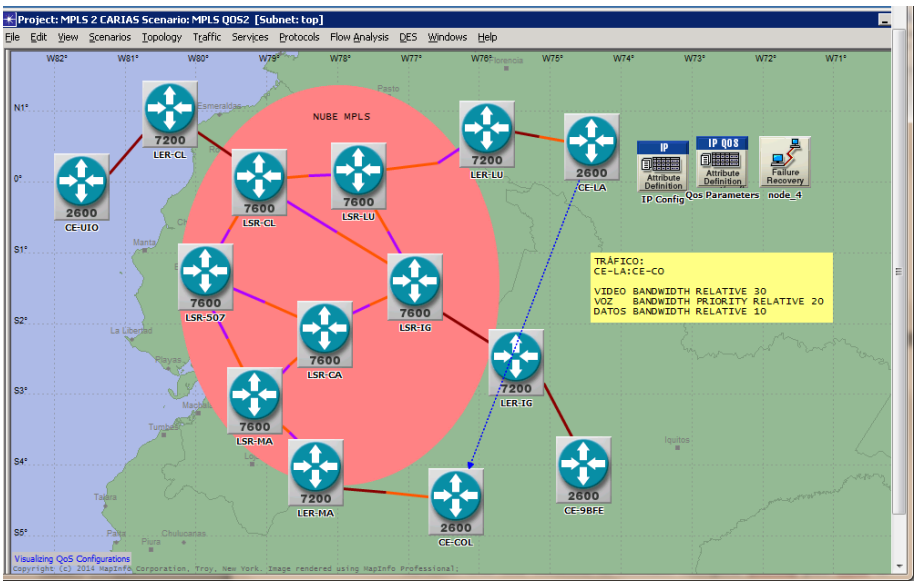


Figura No 97.- Escenario 6 : QoS

c) Configuración de policing

Como se puede apreciar en el escenario anterior, la Calidad de servicio está orientada a clasificar y marcar el tráfico garantizando un determinado ancho de banda para cada servicio con prioridad para el servicio de voz, es decir que, si existe mayor cantidad de tráfico en la voz tendrá prioridad sobre los otros servicios. Con esta condición es necesario configurar policing para evitar la congestión del canal.

Para la simulación y con el fin de comprobar la funcionalidad se presenta el escenario descrito en la Figura No 100. Esta política se aplicará al servicio de datos por ser el menor tráfico establecido y facilitará de mejor manera su visualización en los resultados, descartando los paquetes que exceda el ancho de banda para este servicio mediante la siguiente configuración:

- En *IP-IP QoS Parameters-Policer Profiles-Number of Rows* para definir el número de configuraciones para cada servicio que se definirán en policing. En este caso será para el servicio de datos por lo cual el *Number of Rows* será 1 y el Name el nombre del servicio al cual se aplicará la política, es decir el nombre *datos*.

- En *Policer Details* se agrega un *Number of Rows: 1* y en *Match Property* se establece el tipo de servicio al cual se aplicará la política es decir para datos DSCP con el Match value de AF31. En *Bandwith Type* se define como *Relative* para establecer el porcentaje de 5 % en *Average Rate*.

- En *Action Configuration* se define la acción para los paquetes que estén dentro del porcentaje definido mediante *Traffic type conform* y *Action Transmit* y para los paquetes que exceden el tráfico con *Traffic Type Exceed y Action Drop* como se observa en la Figura No 98.

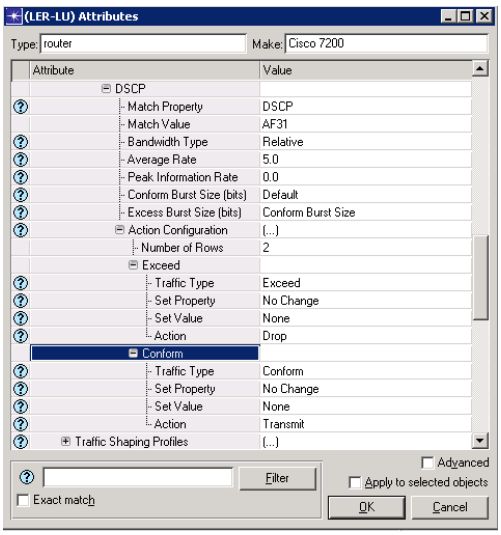


Figura No 98.- Configuración policing.

- Esta configuración es asignada a la política de entrada como se observa en la Figura No 99, ya que será en esta etapa en la cual se aplique policing, Entonces en *Ip-IP QoS Parameters- Traffic Policies* en *la política-in* de entrada definida anteriormente en la clase *Clase-datos-in*, se agrega en *Set Info- Set Property-Policer Profile* y en *Set value* el nombre que fue definido en policing para el servicio, es decir *datos*.

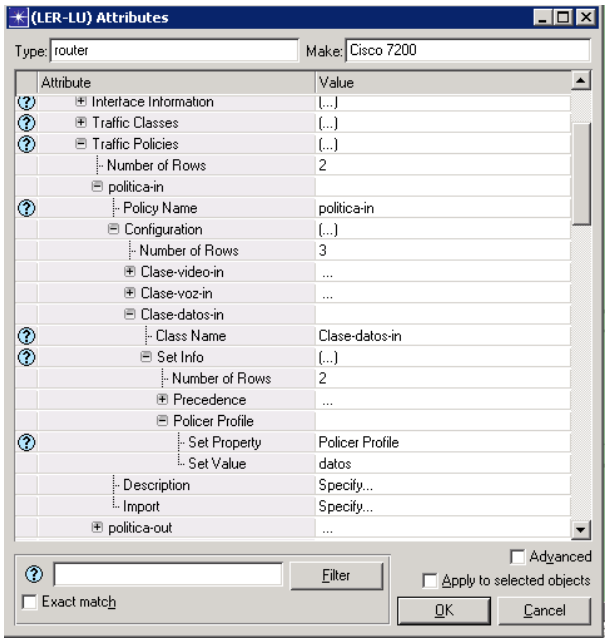


Figura No 99.- Asociación policing a la política de entrada.

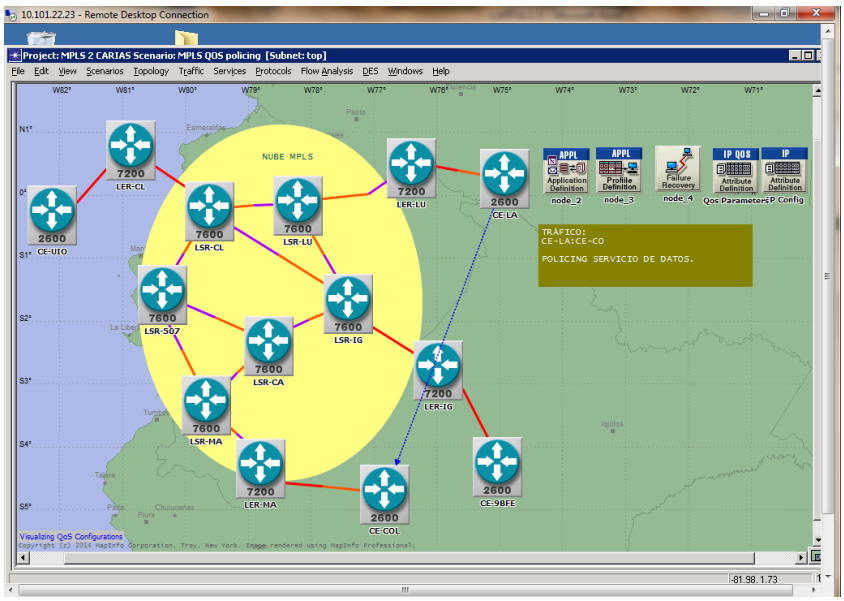


Figura No 100.- Escenario 7: Policing.

4.1.9.- Configuración de Ingeniería de tráfico-túneles MPLS.

Debido a las métricas establecidas en cada enlace y por el protocolo IS-IS que seleccionará el camino más corto para el envío del tráfico y considerando que existirán varios usuarios que se derivan de un LER, los cuales podrían enviar todo el tráfico por la misma ruta, se definirá túneles con rutas explícitas para el envío de la información.

A continuación se explicará la configuración en OPNET para crear túneles asociados a determinado tráfico que ingresa por una determina interfaz del router LER, que permitirá balancear el tráfico en la red de datos, evitando la saturación y congestión de la misma.

- En la opción *Topology* del menú en *Open Object Palette* se busca las facilidades MPLS y se agrega el icono *Attribute Definition MPLS*, que permitirá configurar los FEC´s que serán trasportados por el túnel y las características del *Traffic Trunk* para este túnel.

- Añadido el icono antes mencionado click derecho en *Attributes-FEC Specifications* establecemos las ip´s de la fuente y destino de la interfaz del LER que ingresa el tráfico del CE. En este caso es el LER-LU y el tráfico le corresponde al CE-LA.

- De igual manera en la misma opción se configura el *Traffic Trunk Profiles* con un nombre de trunk que será utilizado para enviar el tráfico en determinado túnel.

- El FEC, puede ser configurado por ip origen-destino, indicando el ToS o el puerto de origen y destino del tráfico a cursar por la red. Lo descrito se observa en la Figura No 101.

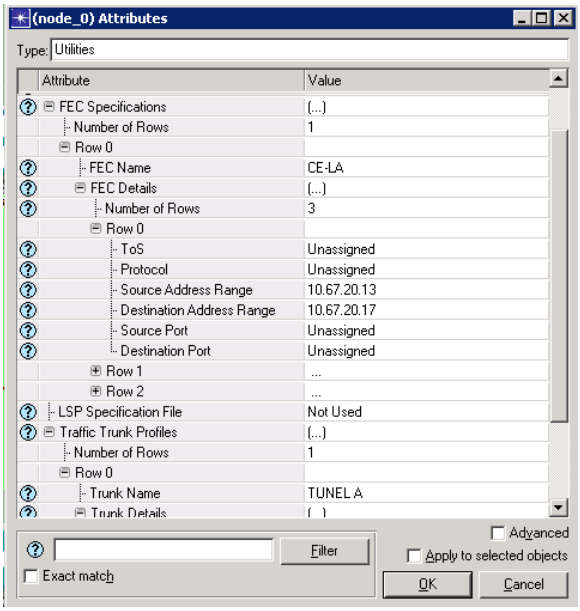


Figura No 101.- Configuración de FEC y Trunk para el túnel.

- Para establecer los caminos que seguirán los túneles creados, en la opción de Topology del menú principal en Open Object Palette, se busca la alternativa de un túnel MPLS Dynamic y se realiza el trazado por cada router que se desea sea la ruta del túnel creado. Para la simulación se define dos túneles como define el escenario de la Figura No 104, con los siguientes recorridos :

  1. LER-LU-LER-MA: LER-LU, LSR-LU, LSR-IG, LSR-CA-LSR-MA Y LER-MA
  2. LER-LU-LER MA 1: LER-LU, LSR-LU, LSR-CL, LSR-507, LSR MA Y LER-MA

- Para actualizar las rutas se selecciona en el menú principal *Protocols-MPLS-Update LSP Details.*

- En el router LER-LU, click derecho- *Edit Attributes-MPLS-MPLS Parameters* en *Explicit Routes*, verificamos las rutas de los LSP´s creados, como se observa en la Figura No 102.

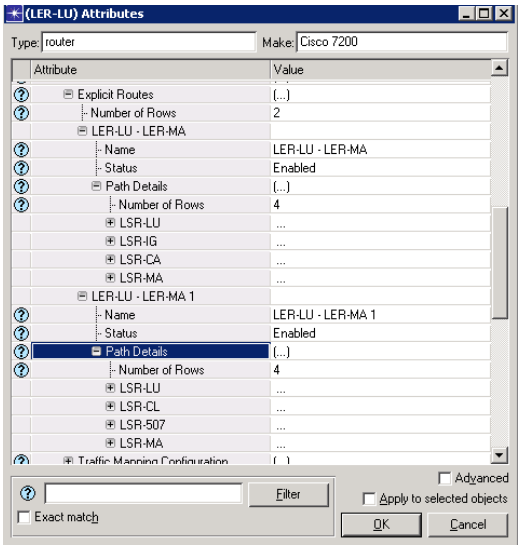


Figura No 102.- Rutas de los LSP´s creados.

- En el router LER-LU, click derecho- *Edit Attributes-MPLS-MPLS Parameters-Traffic Mapping Configuration*, se detalla las características para el LSP. Los parámetros definidos son: Interface In: 3 (interfaz del ingreso al LER-LU del tráfico del CE-LA), *FEC/destinations Prefix* (nombre del FEC creado en el icono *Attribute Definition MPLS, Traffic Trunk (* Nombre del Trunk creado en el icono *Attribute Definition MPLS y* se determina el LSP para este tráfico como lo demuestra la Figura No 103.

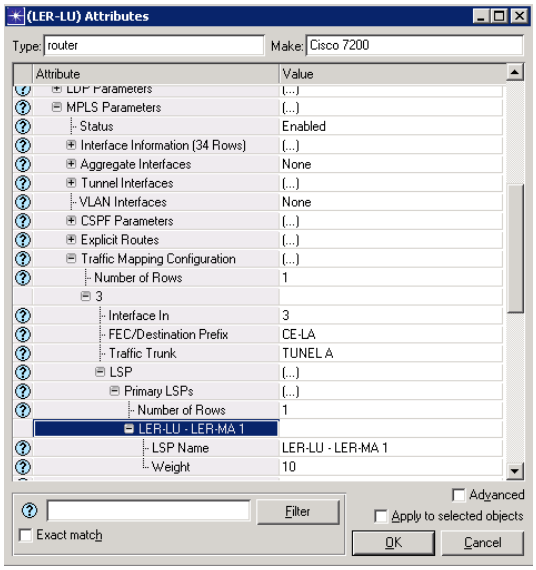


Figura No 103.- Selección del LSP a utilizar para determinado FEC.

Con esta configuración se enviará el tráfico por el LSP deseado y por las rutas definidas para este LSP.

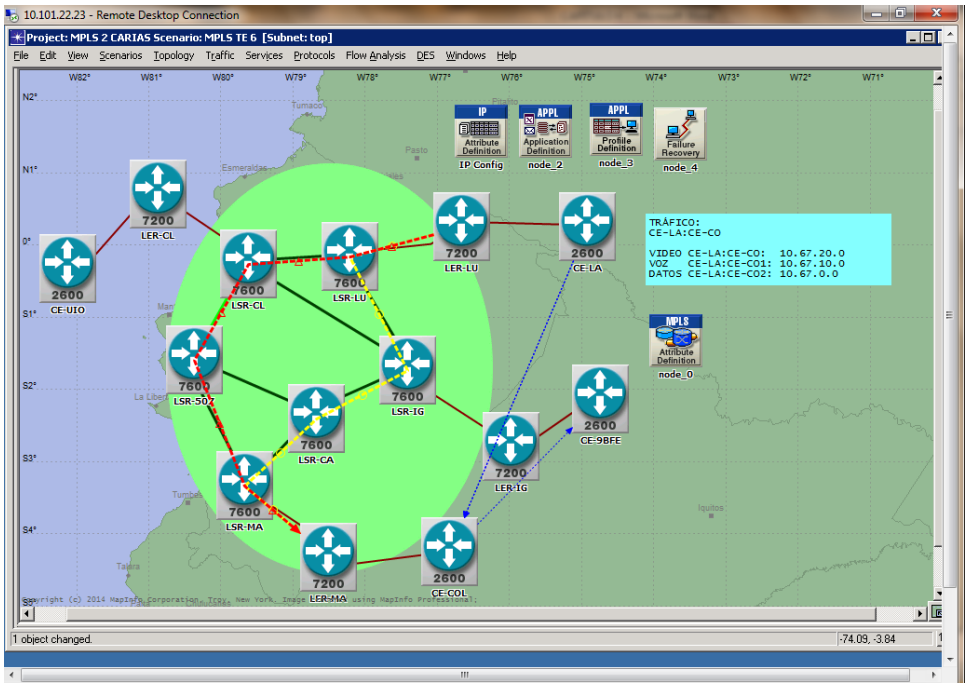


Figura No 104.- Escenario 8: Túnel LSP.

4.2.-Evaluación de tiempos de respuesta.

4.2.1.- Evaluación Escenario 1: OSPF

El primer escenario comprende la configuración del protocolo OSPF, en el cual se podrá verificar los siguientes parámetros característicos del protocolo del camino más corto:

a) Ping entre nodos:

- Para la demostración generaremos tráfico entre el nodo_o y nodo_1, mediante *Topology-Open object Palette-Demand Models-ip_traffic_flow* y se señalará la fuente y destino del tráfico.
- Trazado el tráfico con click derecho en *Edit Attributes-Traffic (bits/second)*, se establece el tráfico definiendo el tiempo y la cantidad de bits por segundo como lo indica la Figura No 105:

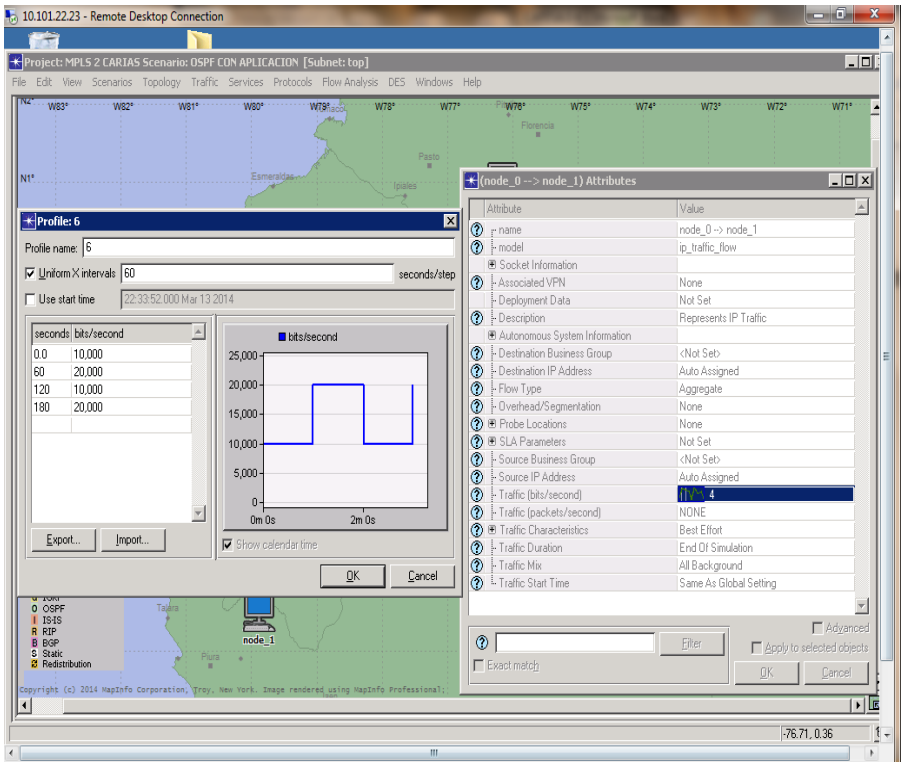


Figura No 105.- Generación de tráfico.

- De manera similar como se agregó el tráfico se traza un ping para analizar los tiempos de respuesta, es decir se crea un *ip_ping_traffic* entre los nodo: *nodo_0 y nodo_1*.
- Para configurar el tiempo de generación del ping en *Topology-Open Object Palette*, se agrega el icono *Ip Atributtes*. Para esta simulación se generará 100 segundos de tráfico ping.
- Para visualizar los resultados se realiza click derecho sobre el router o el tráfico generado y en la opción *Choose Individual DES Statistics*, se seleccionará la opción de *Traffic Received y Traffic Send* en bits/segundo.
- Para visualizar el resultado del ping en el escenario principal se realiza click derecho y con la misma opción *Choose Individual DES Statistics- Node Statistic- Ip- Ping Response Time (sec)* como lo indica la Figura No 106*:*

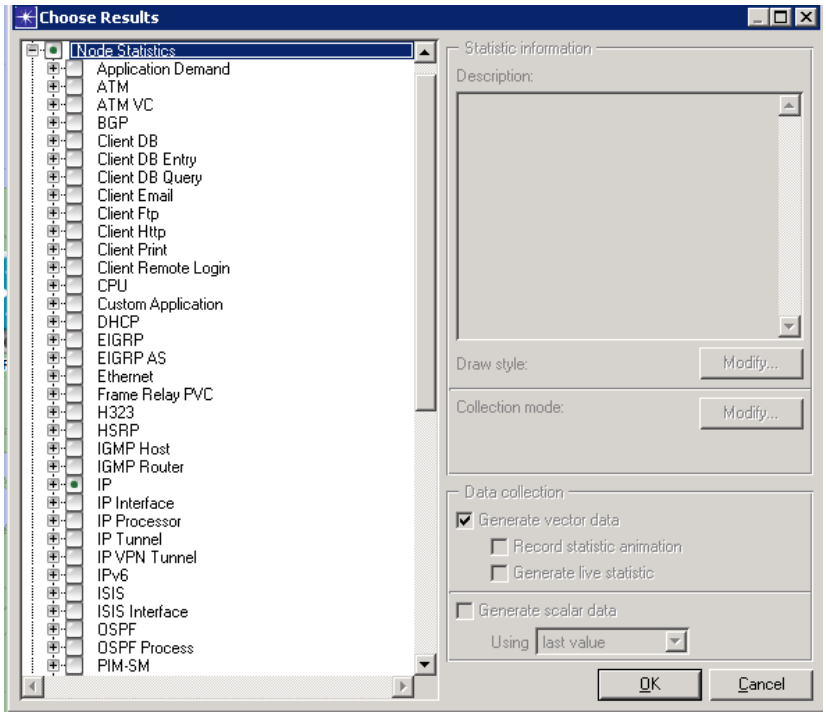


Figura No 106.- Configuración para visualizar resultados

- Para correr la simulación en el menú principal DES-Configure/Run Discret Event Simulation demostrada en la Figura No 107:

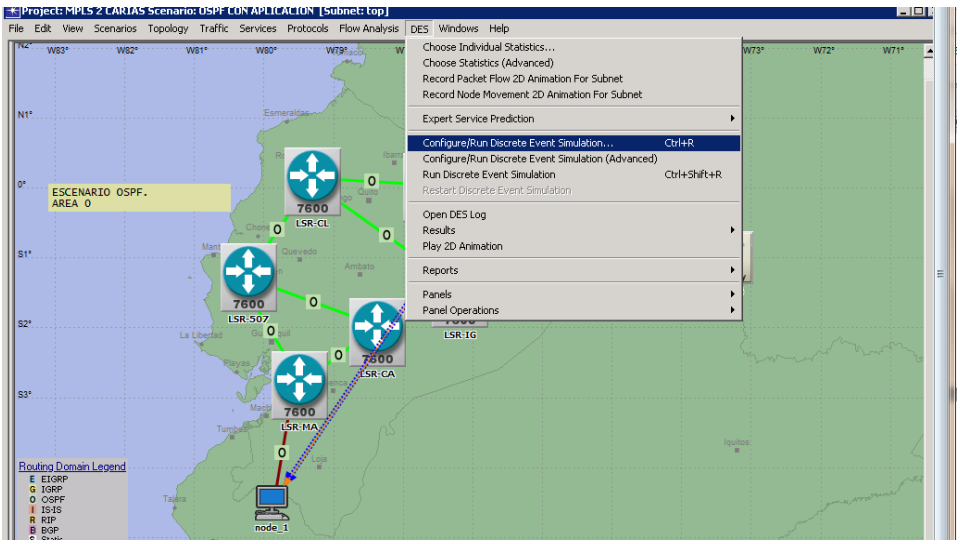


Figura No 107.- Corrida de la simulación.

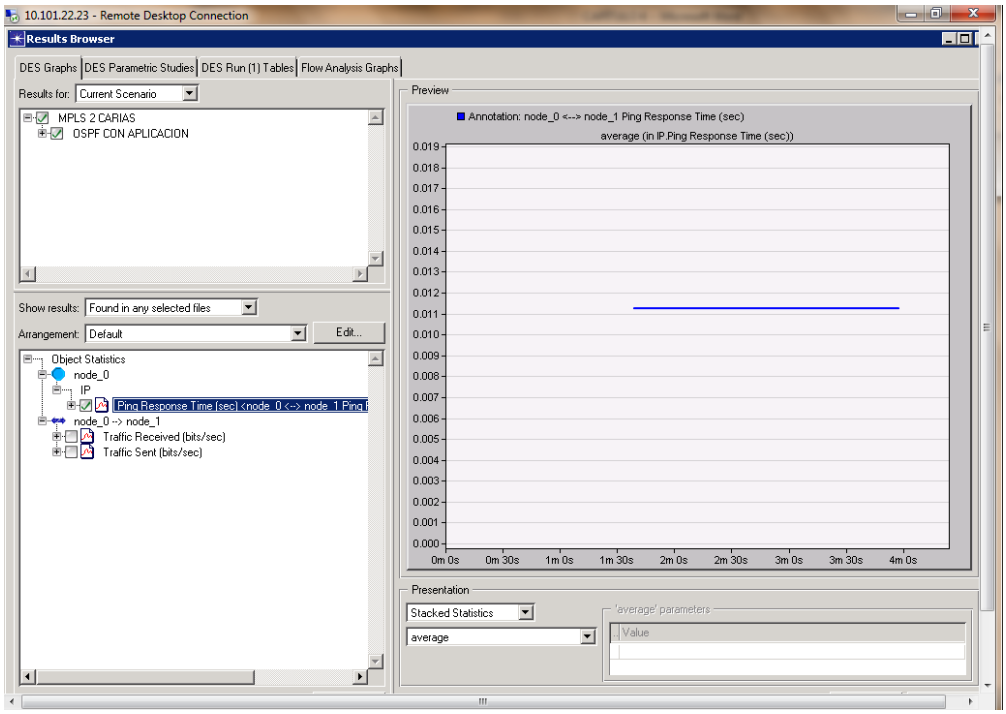


Figura No 108.- Visualización ping OSPF.

Como se puede observar en la Figura No 108, el tiempo de respuesta es de aproximadamente 11 ms y el tráfico enviado y recibido será el visualizado en la Figura No 109:

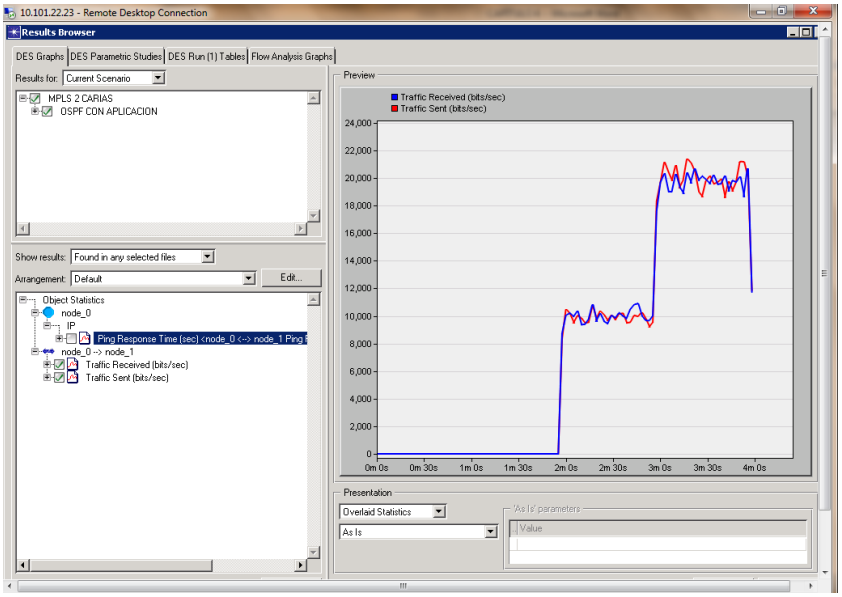


Figura No 109.- Visualización tráfico enviado vs recibido.

b) Tablas de enrutamiento:

- En la pantalla de Results Browser-Des Run (1) Tables indicada en la Figura No 110, se puede observar las tablas de enrutamiento aprendidas por cada equipo, el protocolo, la métrica establecida en este protocolo (110); así como el next hop en ip address o nodo y la interfaz por la cual aprende la ruta:

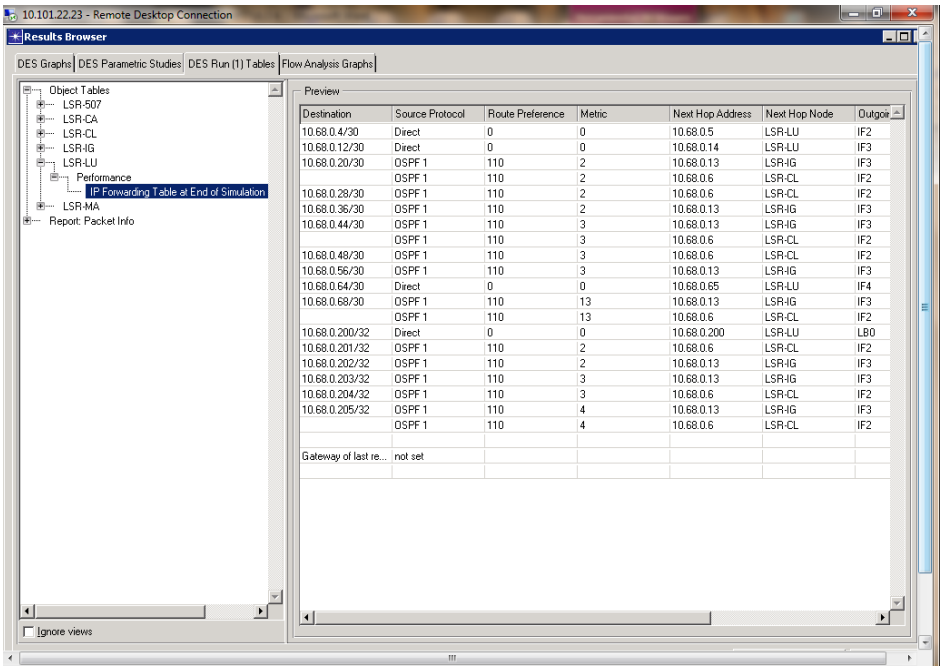


Figura No 110.- Tablas de Enrutamiento.

Es necesario considerar que lo importante en esta simulación es visualizar los resultados de los protocolos y facilidades de la tecnología que se aplica en cada simulación. Con esto se comprueba que mediante OSPF todos los routes aprenden las rutas de toda la red.

En el menú principal en *Protocols-Ip-Demands-Display Routes for Configured Demands*, se podrá visualizar el camino recorrido por el tráfico indicado en la Figura No 111:

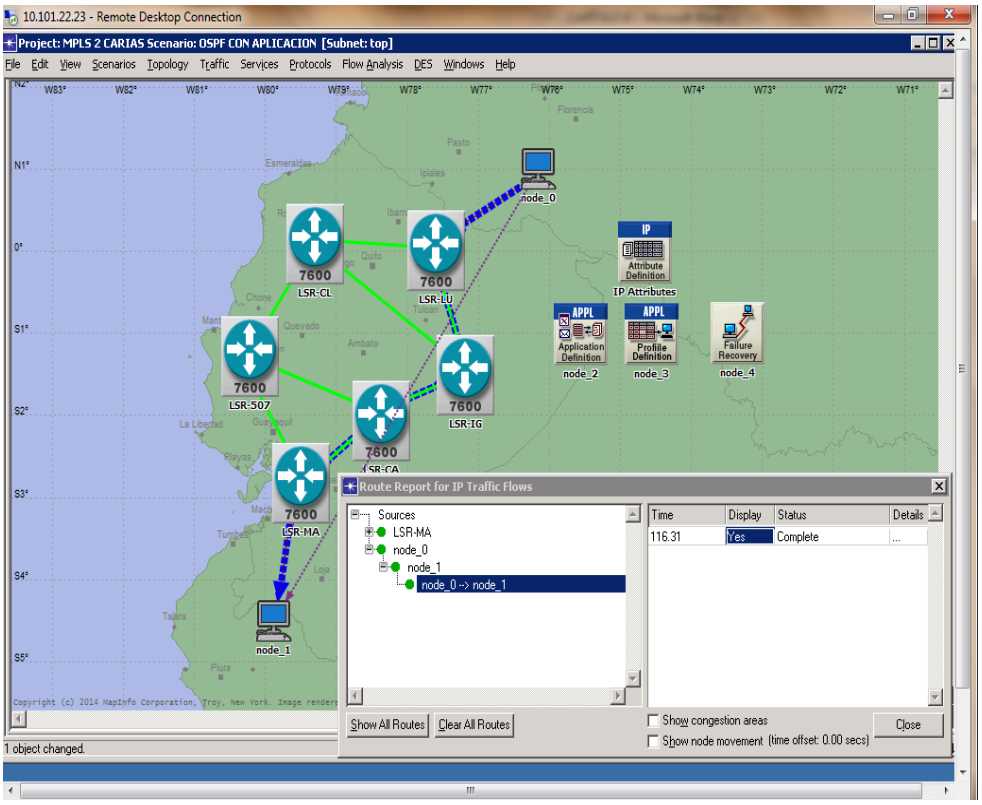


Figura No 111.- Ruta seleccionada por OSPF.

c) Re-enrutamiento en caso de fallas de enlace:

Los protocolos de estado de enlace como lo es OSPF en caso de fallas tomará otra ruta disponible para el envío de tráfico. Para visualizar este resultado se simularán caídas de enlace mediante la opción en *Topology-Open Object Palette-Failure Recovery*:

En la Figura No 111 se observó que la ruta seleccionada por el protocolo para el tráfico del node_o al node_1 es el LSR-LU, LSR-IG, LSR-CA y LSR-MA, por lo cual se cortará el enlace LSR-LU-LSR-IG indicado en la Figura No 112:

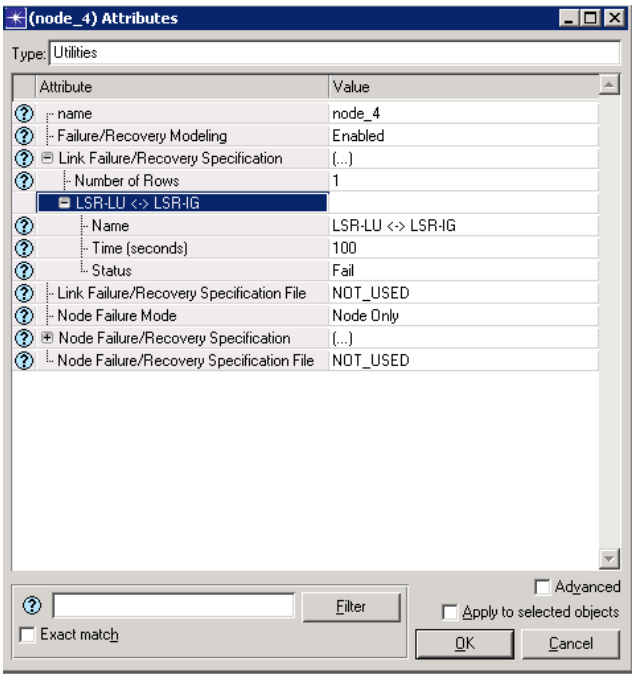


Figura No 112.- Caída del enlace LER-LU-LER-IG.

En la Figura No 113, se observará el trafico re-enrutado con la caída de enlace simulada:

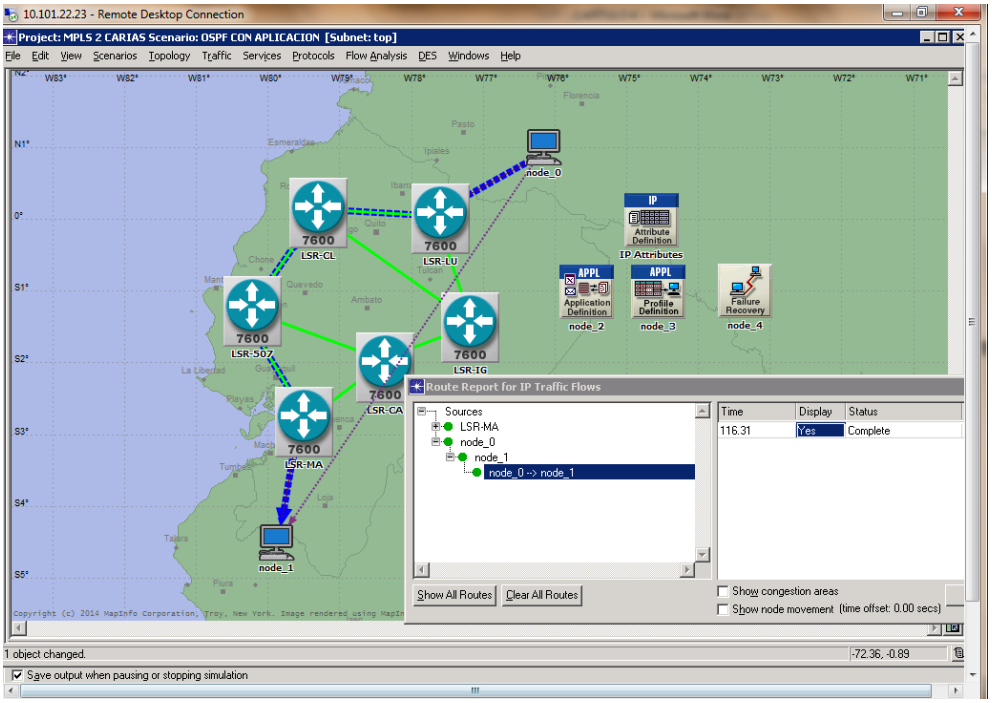


Figura No 113.- Tráfico re-enrutado OSPF.

A continuación se provocará fallas en los enlaces LSR-LU-LSR-IG y LSR-CL-LSR-507y en la Figura No 114 se apreciará el tráfico por las rutas con enlaces disponibles:

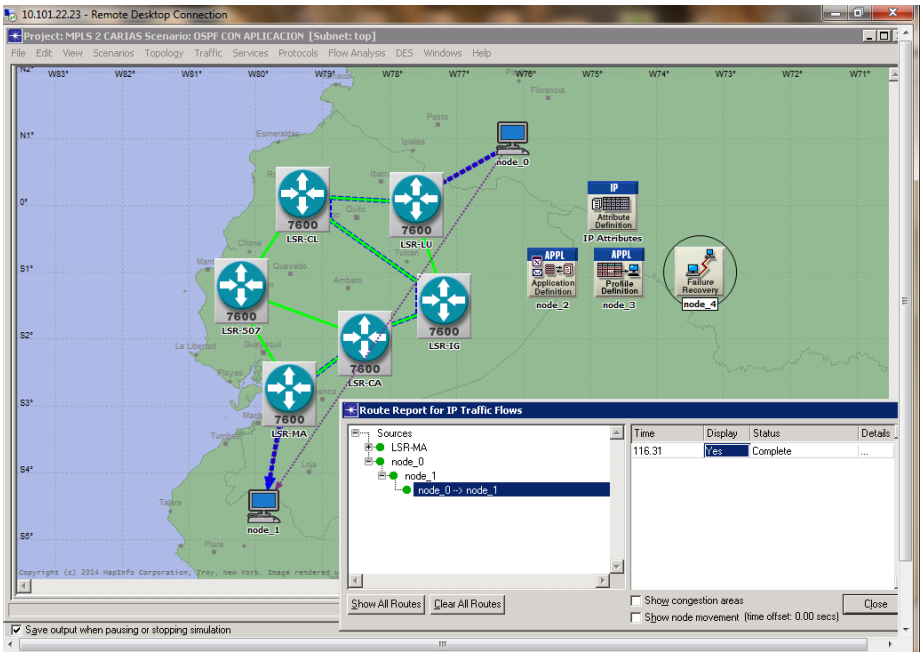


Figura No 114.- Tráfico con fallas en dos enlaces.

4.2.2.- Evaluación Escenario 2: IS-IS

a) Ping entre nodos

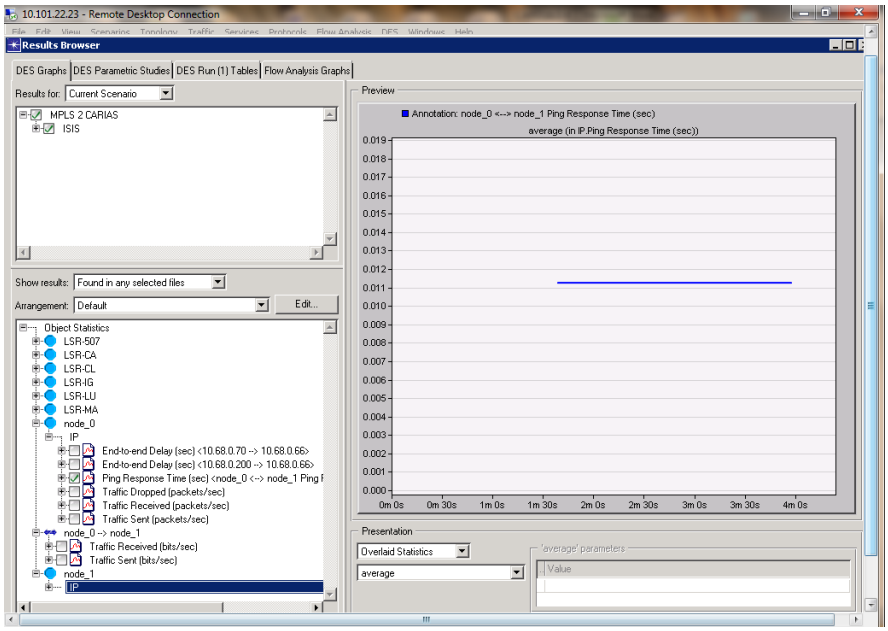


Figura No 115.- Visualización ping IS-IS.

Como se puede observar en la Figura No 115, el tiempo de respuesta con el protocolo ISIS, es de aproximadamente 11 ms.

Los tiempos de respuesta con OSPF y IS-IS son similares como se puede observar en la Figura No 116:

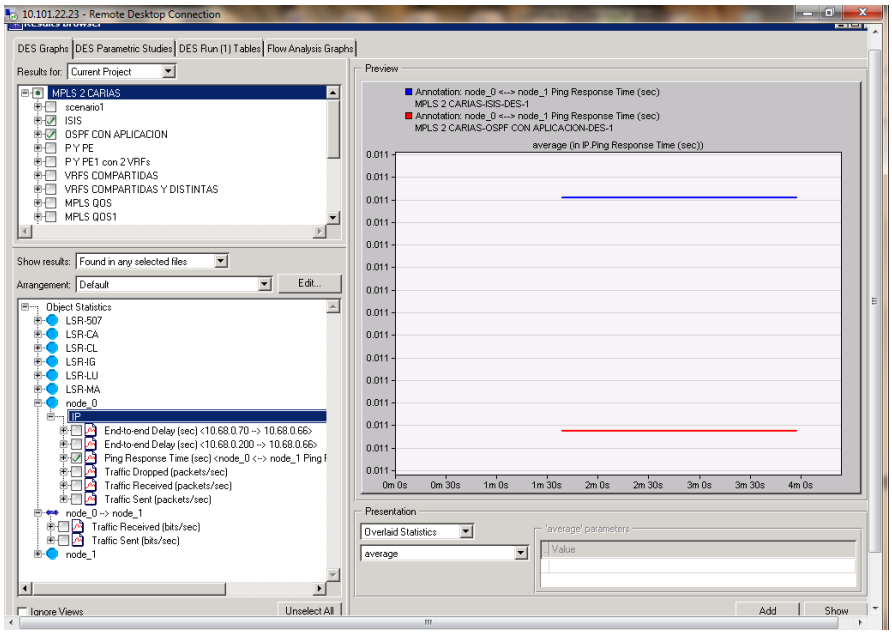


Figura No 116.- Ping IS-IS y OSPF.

b) Tablas de enrutamiento:

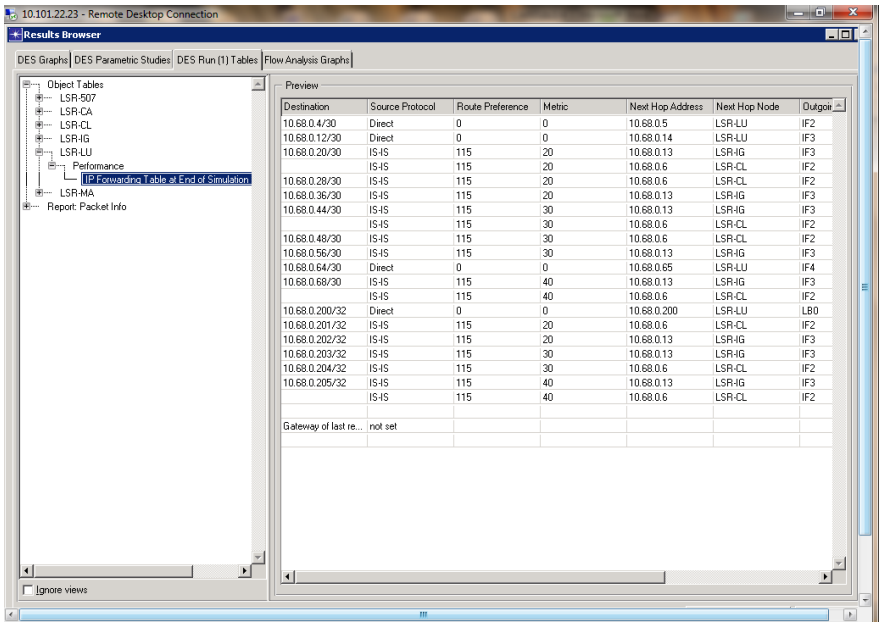


Figura No 117.- Tabla de enrutamiento IS-IS.

Como se observa en la Figura No 117, las tablas de enrutamiento aprendidas por cada equipo, el protocolo, la métrica establecida en este protocolo (115); así como el next hop en ip address o nodo y la interfaz por la cual aprende la ruta.

c) Re-enrutamiento en caso de fallas de enlace:

En la Figura No 118, se puede observar el tráfico con fallas provocadas en los enlaces: LSR-LU-LSR-CL y LSR-IG-LSR-CA:

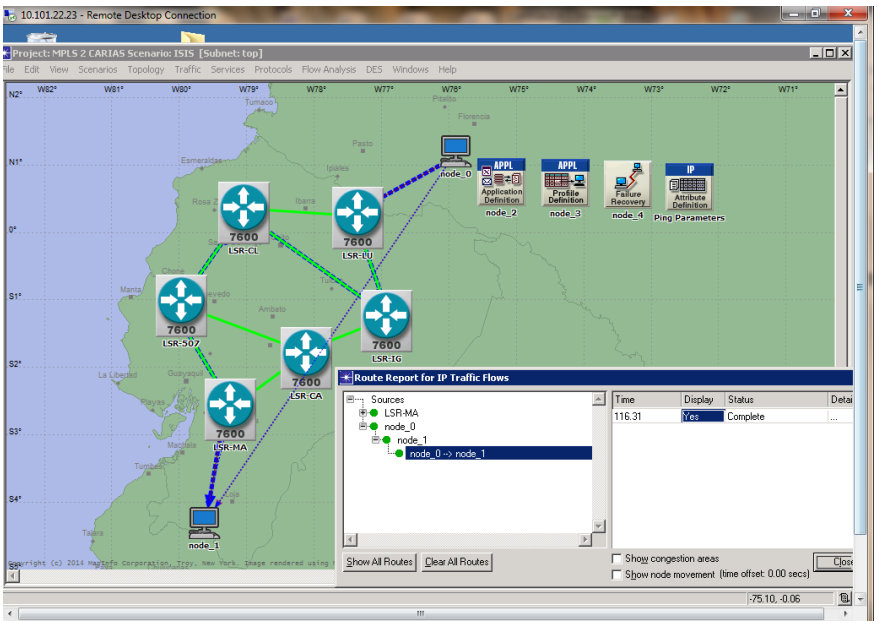


Figura No 118.- Tráfico con fallas en dos enlaces.

Con los escenarios 1 y 2, lo que se ha logrado es verificar la funcionalidad de los protocolos de estado de enlace.

4.2.3.- Evaluación Escenario 3: Configuración MP-BGP.

a) Visualización Protocolos configurados:

En la Figura No 119, se observa los protocolos configurados en los routers LSR, LER y CE con la distribución de BGP y OSPF.

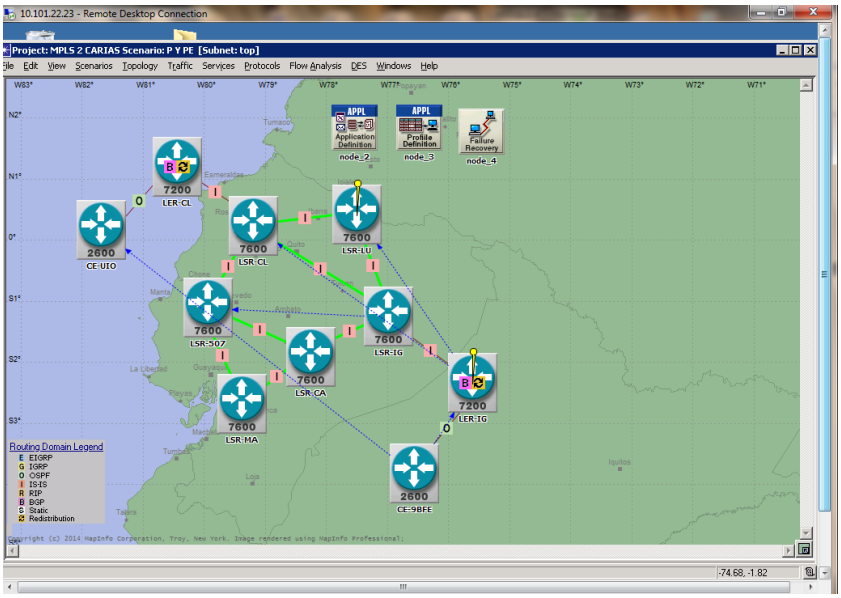


Figura No 119.- Protocolos Configurados.

A continuación en la Figura No 120, se verifica la VPN entre los routers LER´s:

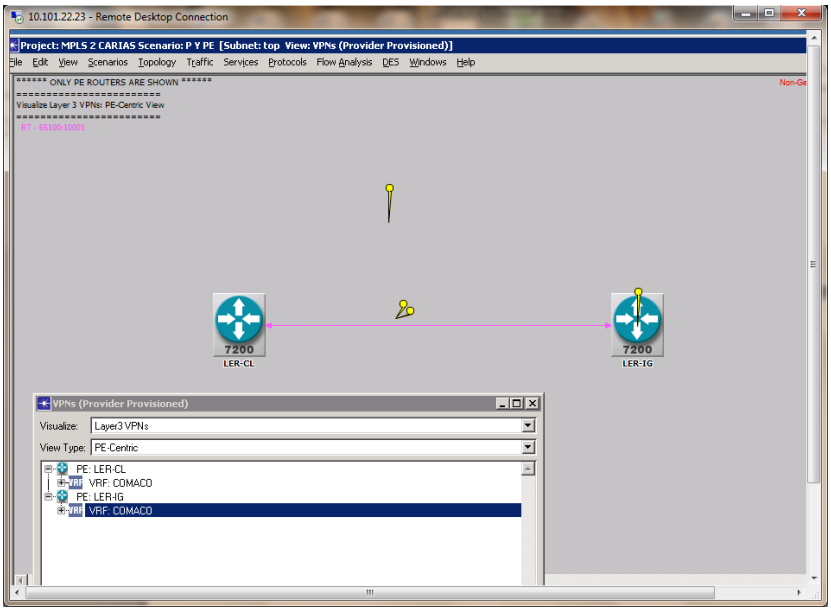


Figura No 120.- Visualización VPN.

b) Tablas de enrutamiento:

Mediante las tablas de enrutamiento se comprueba que las rutas aprendidas por los equipos de usuarios en base a la redistribución de BGP-OSPF y la VPN creada en los LER, solamente aprenden las rutas de su vecino VPN. En este caso el CE-9BFE aprende las rutas del CE-UIO como lo indica la Figura No 121:

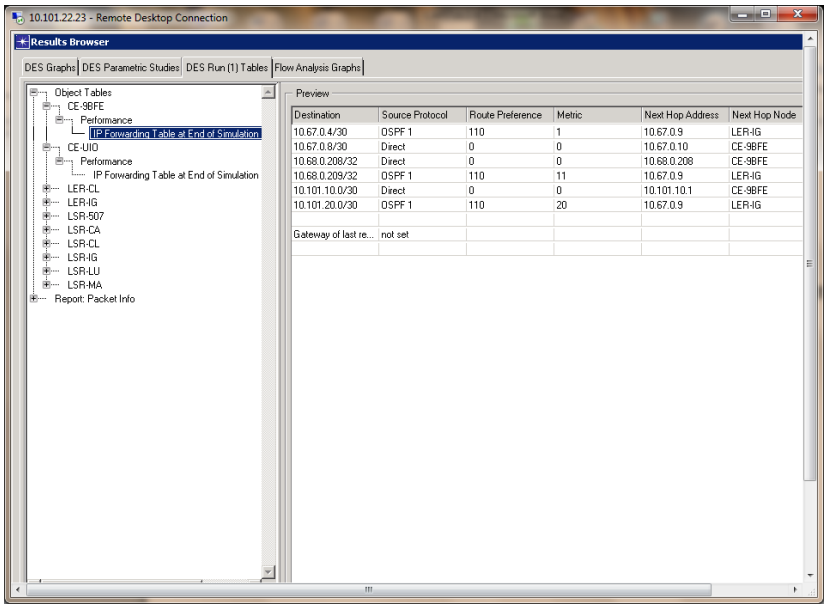
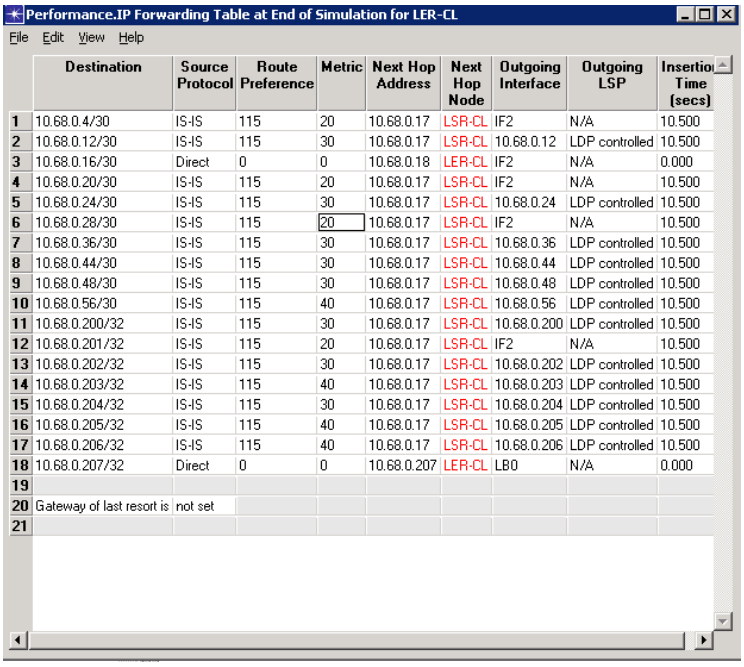


Figura No 121.- Rutas prendidas de un CE.

Los routers de la red MPLS aprenderán sus rutas mediante el protocolo IS-IS e indica que el protocolo LDP se encuentra configurado en estos routers, como lo señala la Figura No 122:



	Destination	Source Protocol	Route Preference	Metric	Next Hop Address	Next Hop Node	Outgoing Interface	Outgoing LSP	Insertion Time (secs)
1	10.68.0.4/30	IS-IS	115	20	10.68.0.17	LSR-CL	IF2	N/A	10.500
2	10.68.0.12/30	IS-IS	115	30	10.68.0.17	LSR-CL	10.68.0.12	LDP controlled	10.500
3	10.68.0.16/30	Direct	0	0	10.68.0.18	LER-CL	IF2	N/A	0.000
4	10.68.0.20/30	IS-IS	115	20	10.68.0.17	LSR-CL	IF2	N/A	10.500
5	10.68.0.24/30	IS-IS	115	30	10.68.0.17	LSR-CL	10.68.0.24	LDP controlled	10.500
6	10.68.0.28/30	IS-IS	115	20	10.68.0.17	LSR-CL	IF2	N/A	10.500
7	10.68.0.36/30	IS-IS	115	30	10.68.0.17	LSR-CL	10.68.0.36	LDP controlled	10.500
8	10.68.0.44/30	IS-IS	115	30	10.68.0.17	LSR-CL	10.68.0.44	LDP controlled	10.500
9	10.68.0.48/30	IS-IS	115	30	10.68.0.17	LSR-CL	10.68.0.48	LDP controlled	10.500
10	10.68.0.56/30	IS-IS	115	40	10.68.0.17	LSR-CL	10.68.0.56	LDP controlled	10.500
11	10.68.0.200/32	IS-IS	115	30	10.68.0.17	LSR-CL	10.68.0.200	LDP controlled	10.500
12	10.68.0.201/32	IS-IS	115	20	10.68.0.17	LSR-CL	IF2	N/A	10.500
13	10.68.0.202/32	IS-IS	115	30	10.68.0.17	LSR-CL	10.68.0.202	LDP controlled	10.500
14	10.68.0.203/32	IS-IS	115	40	10.68.0.17	LSR-CL	10.68.0.203	LDP controlled	10.500
15	10.68.0.204/32	IS-IS	115	30	10.68.0.17	LSR-CL	10.68.0.204	LDP controlled	10.500
16	10.68.0.205/32	IS-IS	115	40	10.68.0.17	LSR-CL	10.68.0.205	LDP controlled	10.500
17	10.68.0.206/32	IS-IS	115	40	10.68.0.17	LSR-CL	10.68.0.206	LDP controlled	10.500
18	10.68.0.207/32	Direct	0	0	10.68.0.207	LER-CL	LB0	N/A	0.000
19									
20	Gateway of last resort is	not set							
21									

Figura No 122.- Rutas aprendidas en la nube MPLS.

El tráfico recibido en un CE no presenta errores en la trasmisión como lo demuestra la Figura No 123:

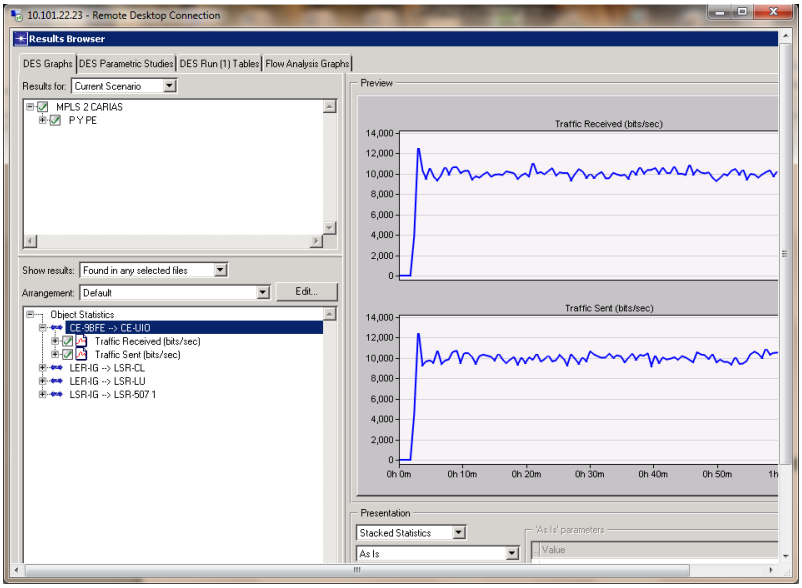


Figura No 123.- Tráfico entre CE´s.

c) Tiempo de respuesta:

Para guardar similitud y comparar con la configuración de OSPF y IS-IS se realiza un ping entre los routers LER-IG-LER-CL:

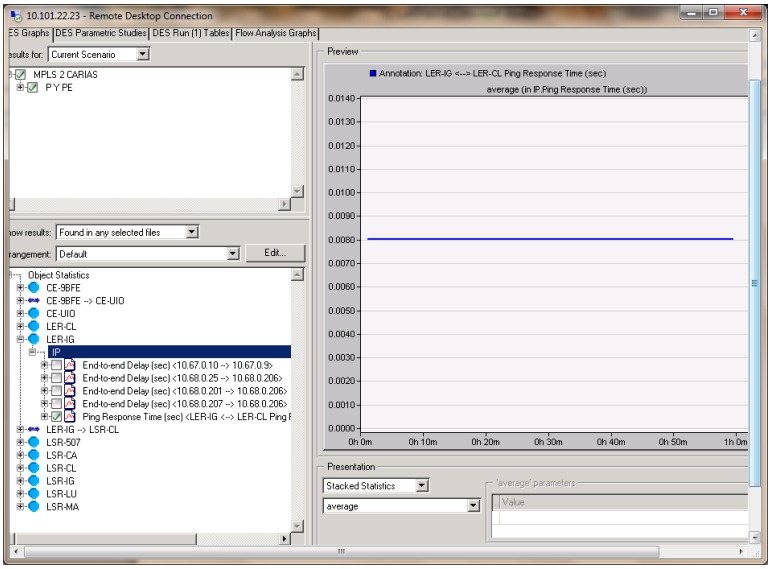


Figura No 124.- Ping en routers MPLS.

En la Figura No 124, se verifica que el tiempo de respuesta es de aproximadamente 8 ms.

d) Rutas del tráfico:

En la Figura No 125, se demuestra la ruta seleccionada para el envío de tráfico entre el CE-9BFE y CE-UIO.

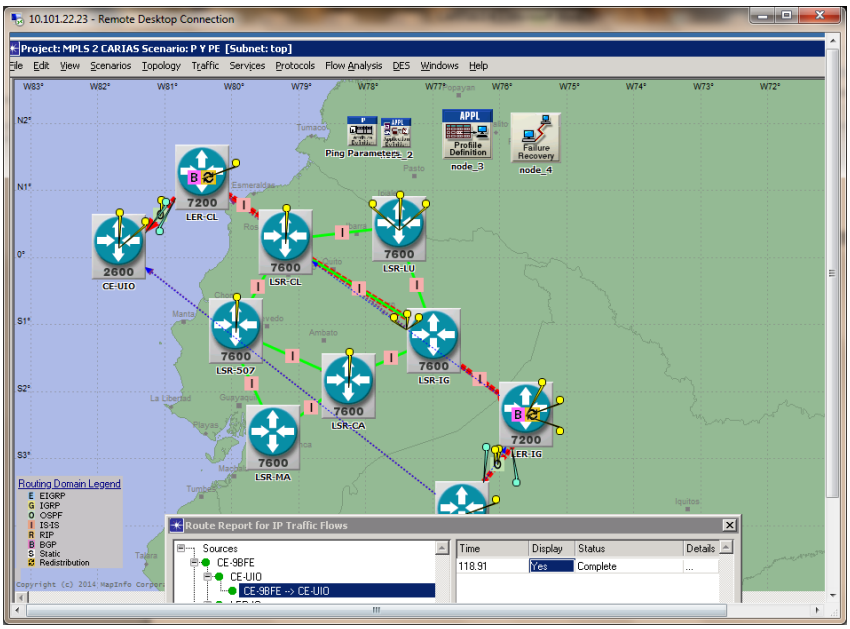


Figura No 125.- Rutas de tráfico.

- En la Figura No 126, se demuestra el tráfico entre los mismos CE´s, con fallas provocadas en el enlace LSR-IG-LSR-CL:

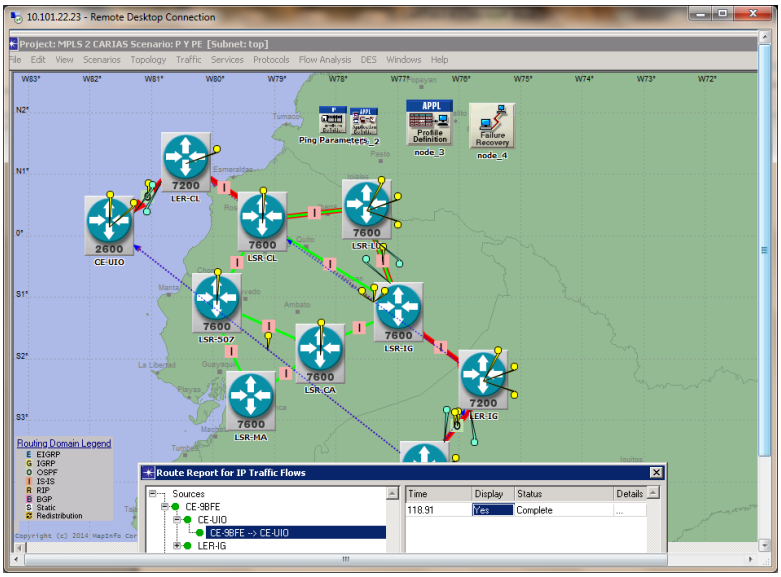


Figura No 126.- Tráfico re-enrutado

4.2.4.- Evaluación Escenario 4: Configuración VRF´s distintas para diferentes usuarios.

A continuación en la Figura No 127, se establece el diagrama de simulación, que permitirá verificar las VRF configuradas en la red con un RT y RD específico para la aplicación. En base a la Tabla No 67.- *RD y RT para diferentes servicios,* se comprueban las VRF´s en las cuales el servicio de VOZCOMACO lo comparte todos los LER´s y los servicios de DATOSFAE y VIDEOFAE lo comparte solamente el LER-LU para el usuario FAE en CE-LA y el LER-MA para el mismo usuario en el CE-MA

a) Diagrama de simulación:

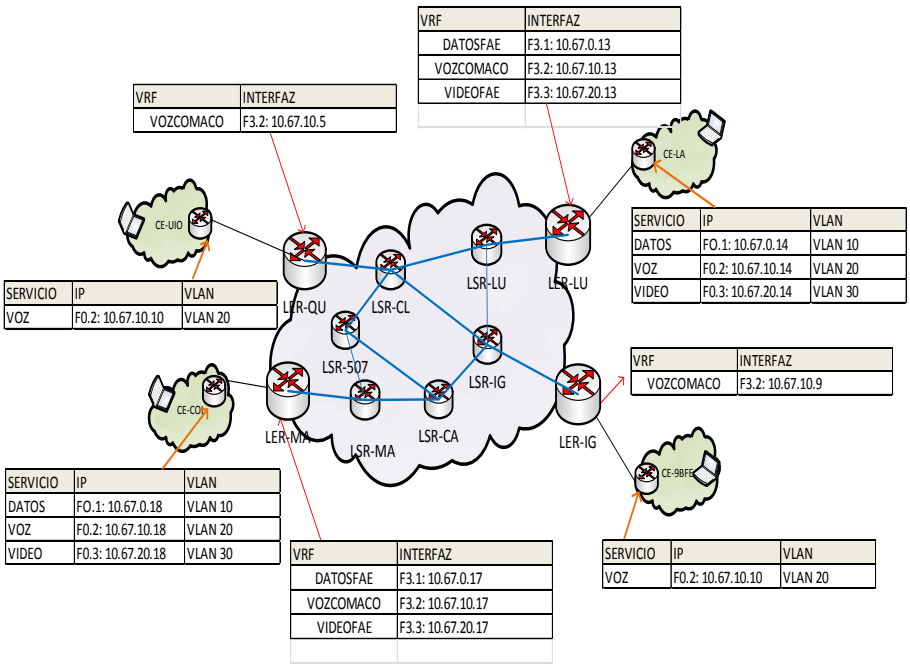


Figura No 127.- Diagrama de simulación.

b) Protocolos de simulación:

En la Figura No 128, se puede apreciar los protocolos configurados en la red MPLS con redistribución BGP-OSPF, así como el tráfico que se envía entre los diferentes usuaros:

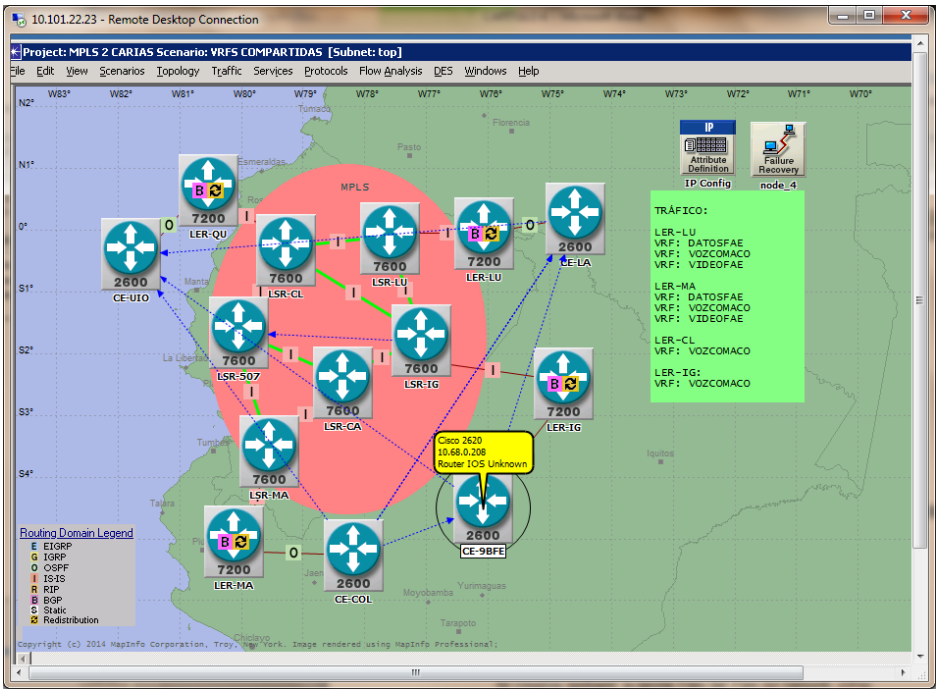


Figura No 128.- Protocolos de simulación.

c) VRF´s creadas:

En la Figura No 129, se visualiza las VRF´s creadas y las conexiones VPN´s entre los diferentes LER´s de los cuales se derivan los usuarios. Esto se obtiene en el software mediante la opción *View-Set View for Network- VPNs:*

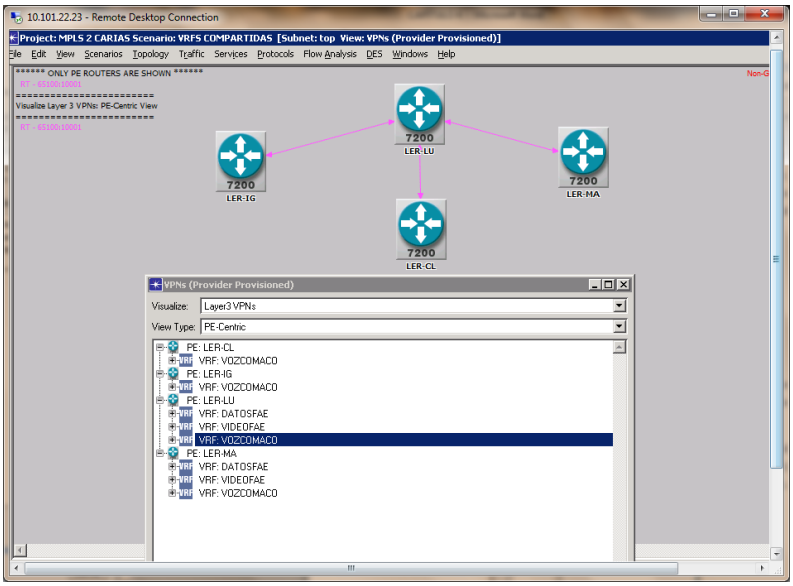


Figura No 129.- VRF´s distintas en la red.

d) Tablas de enrutamiento:

Con las Figuras No 130 y 131, se puede verificar las tablas de los equipos CE´s, los cuales solo aprenden las rutas de sus vecinos BGP, no todas las rutas de todos los equipos como ocurre en un enrutamiento puramente IP:

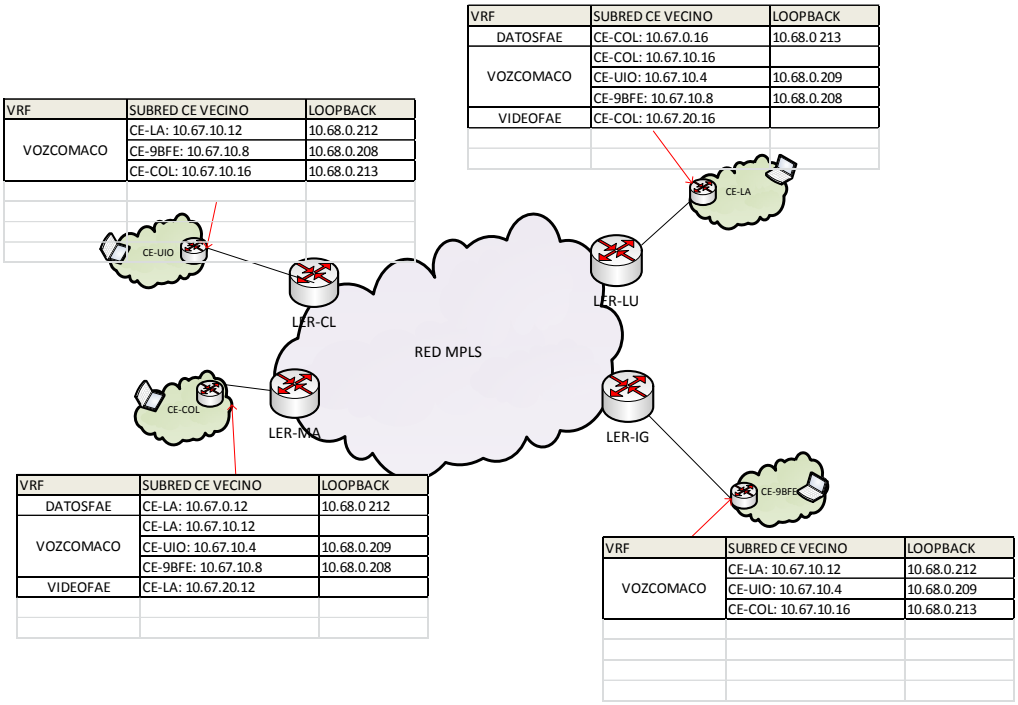


Figura No 130.- Tabla de enrutamiento CE-LA.

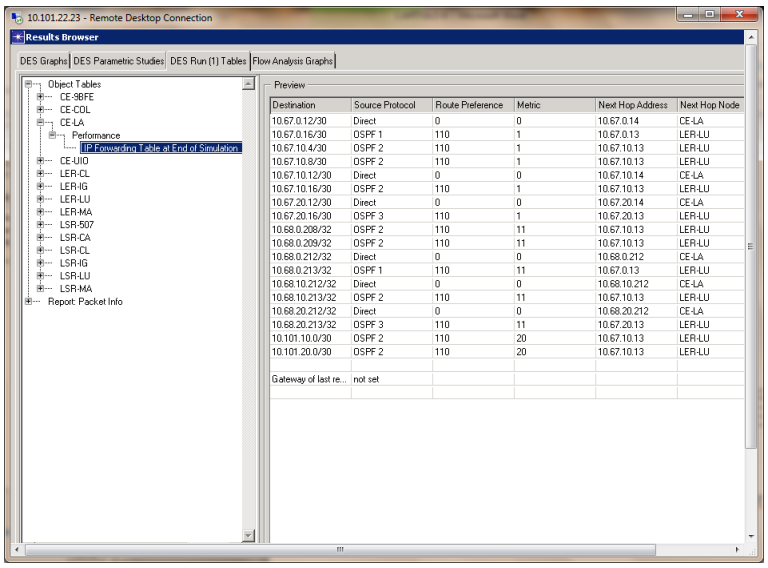


Figura No 131.- Tablas de enrutamiento OPNET.

d) VRF´s creadas entre los LER:

Para observar de mejor manera y aprovechando las características del software, en la Figura No 132 se observa de color rojo las VRF´s creadas en los diferentes LSR´s:

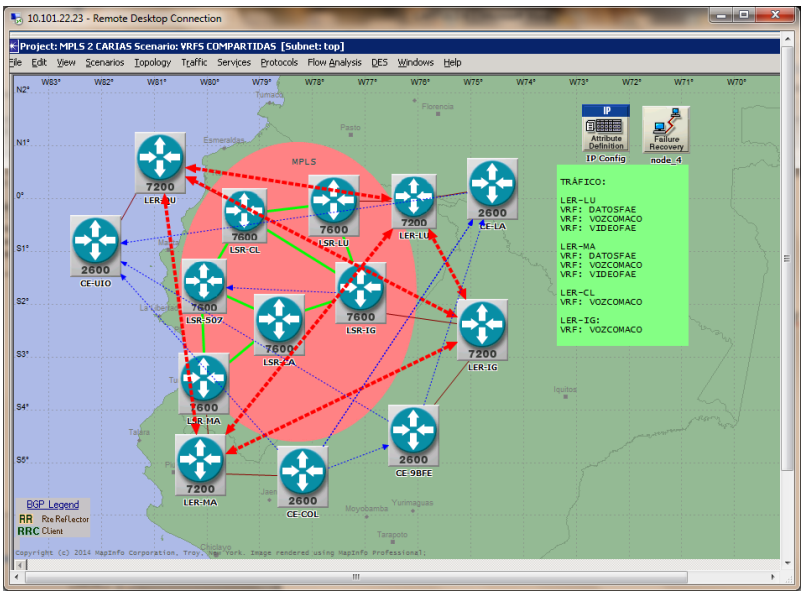


Figura No 132.- VRF´s creadas entre los LER´s.

e) Rutas del tráfico enviado:

En la Figura No 133, se puede observar la ruta por la cual se transporta el servicio simulado entre el CE-COL y CE-LA:

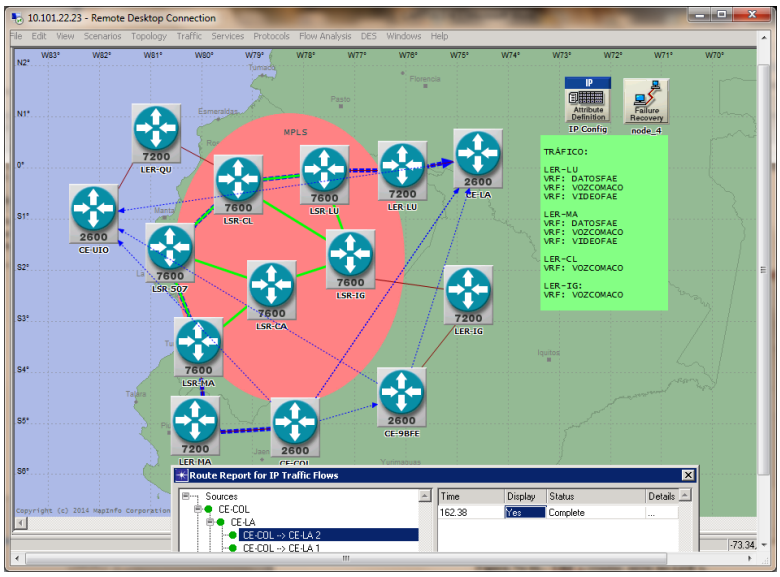


Figura No 133.- Tráfico entre CE-COL y CE-LA.

En la Figura No 134, se puede observar la ruta por la cual se transporta el servicio simulado entre el CE-CO y CE-UIO:

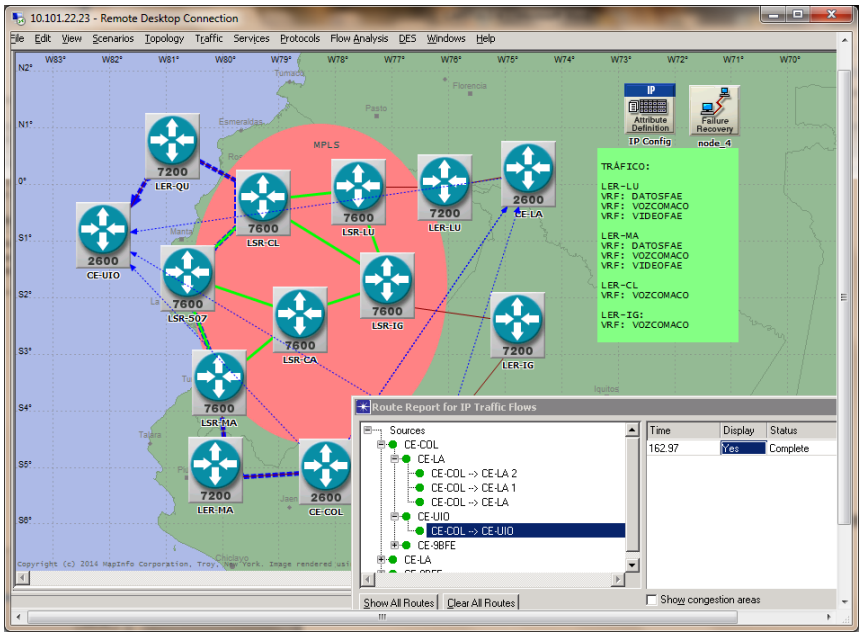


Figura No 134.- Tráfico entre CE-CO y CE-UIO

En la Figura No 135, se puede observar la ruta por la cual se transporta el servicio simulado entre el CE-LA y CE-UIO:

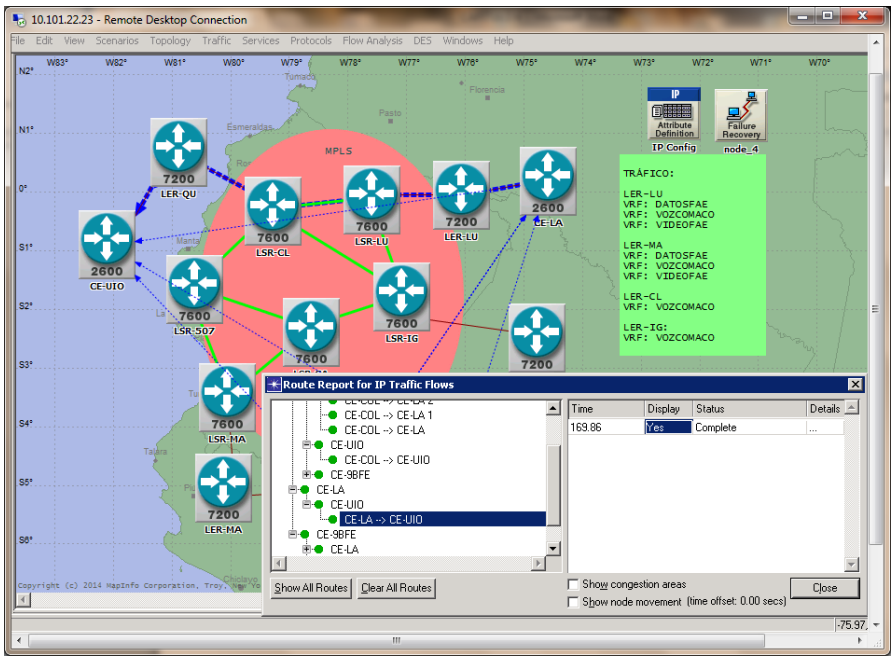


Figura No 135.- Tráfico entre CE-LA y CE-UIO.

4.2.5.- Evaluación Escenario 5: Configuración VRF´s complejas.

En la Figura No 136, se observa el escenario que tiene por objeto compartir la información de servicios entre DATOSFAE del CE-LA y DATOS COMACO del CE-COL que son usuarios de FAE, mediante la configuración del RT con import y export descritos en el capítulo 4.1.7:

a) Escenario de la simulación:

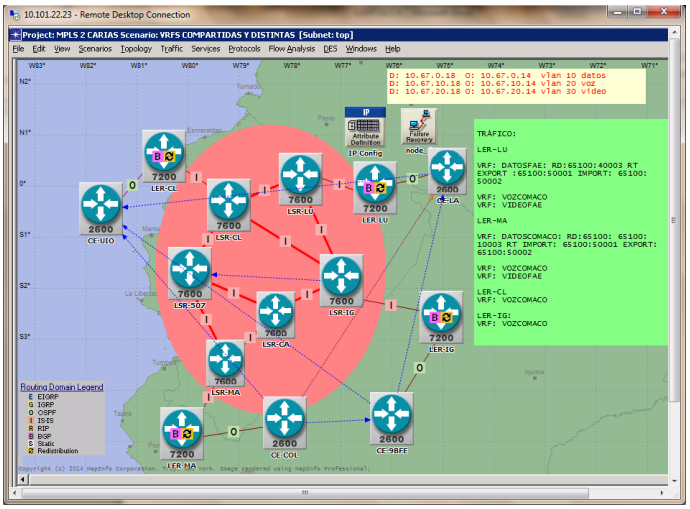


Figura No 136.- VRF´s con import y export.

b) Tráfico compartido entre las VRF´s:

En la Figura No 137, se observa que no existen errores en el tráfico de la VRF compleja entre los usuarios de FAE:

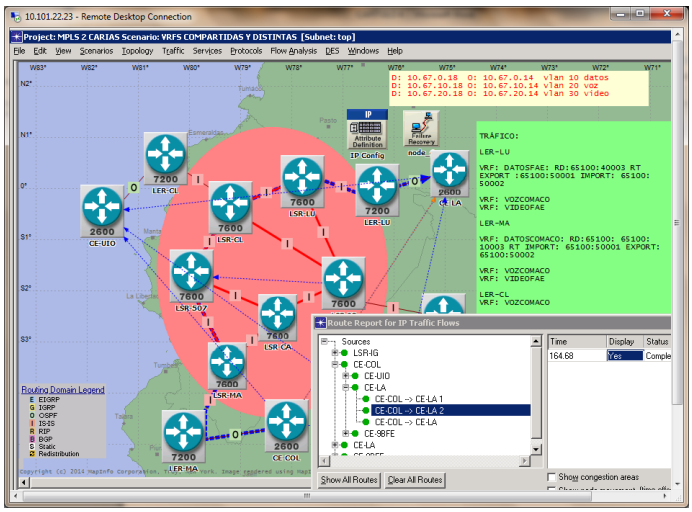


Figura No 137.- Tráfico entre VRF´s compartidas.

c) Comprobación de la VRF compartida:

En la Figura No 138, se observa de mejor manera que existe conectividad entre los usuarios que comparte la VRF compleja con servicios de DATOSFAE Y DATOSCOMACO:

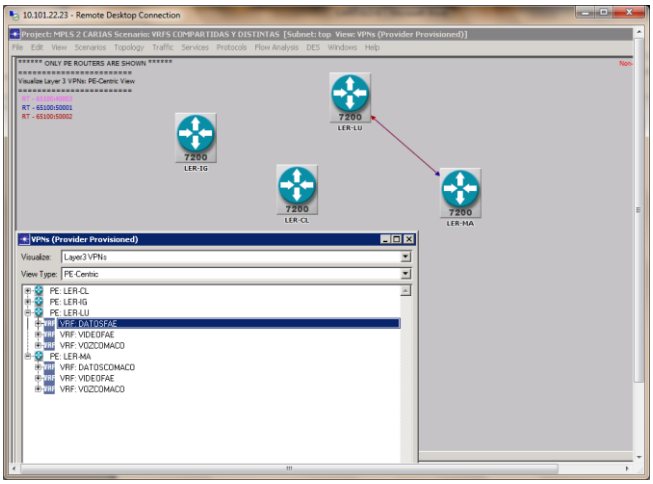


Figura No 138.- VRF compartida.

4.2.6.- Evaluación Escenario 6: Configuración Qos.

En base a lo descrito en el numeral 4.1.8 “Configuración QoS MPLS”, se ha realizado la clasificación y marcaje de los paquetes, con un aseguramiento de ancho de banda por servicio de video de 30 %, voz 20% y datos 10 %. para esto se simulará tráfico entre el CE-LA y CE-COL, para video, datos y voz como lo indica la Figura No 139:

a) Tráfico enviado desde el usuario CE-LA a CE-COL:

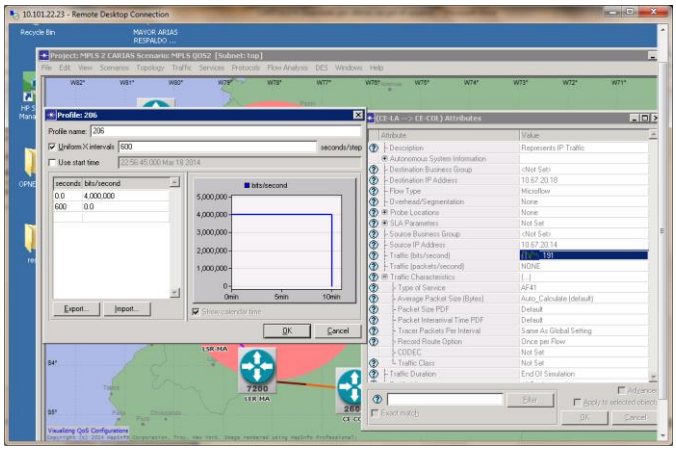


Figura No 139.- Tráfico generado para video.

Para las simulaciones se irá variando el tráfico del video hasta la saturación del canal para visualizar su comportamiento como lo describe la Tabla No 68:

Tabla No 68.- Tráfico para QoS

SIMULACIÓN	TRÁFICO		
SERVICIO	**VIDEO (CE-LA-CE-COL)**	**VOZ (CE-LA-CE-COL 2)**	**DATOS (CE-LA-CE- COL 1)**
SIMULACIÓN NO 1.-	3 Mbps	2 Mbps	1 Mbps
SIMULACIÓN NO 2.-	4 Mbps	2 Mbps	1 Mbps
SIMULACIÓN NO 3.-	4 Mbps	2 Mbps	3 Mbps
SIMULACIÓN NO 4.-	6 Mbps	3 Mbps	2 Mbps

b) Tráfico recibido en la simulación No 1.-

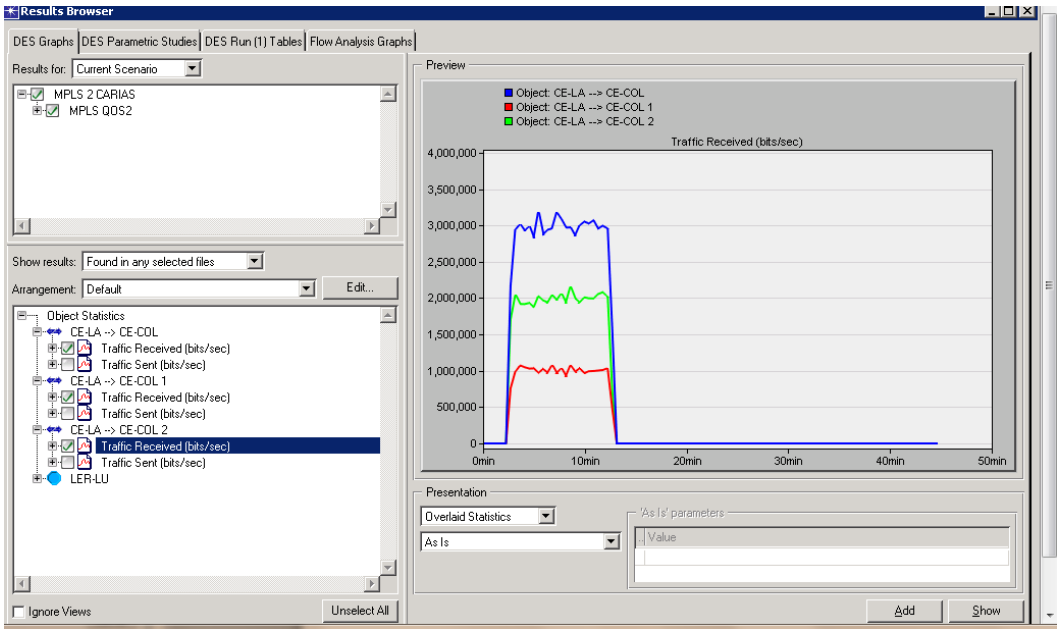


Figura No 140.- Tráfico recibido Simulación No 1.

Como se puede observar en la Figura No 140, no existe saturación y el tráfico enviado está en base a lo garantizado para cada servicio.

c) Tráfico recibido en la simulación No 2.-

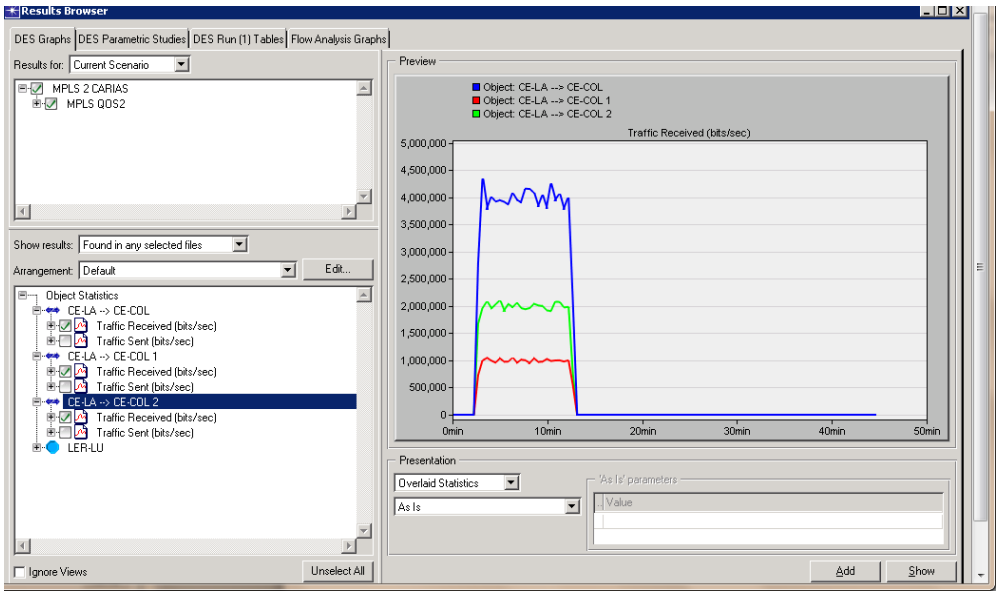


Figura No 141.- Tráfico recibido Simulación No 2.

Como lo demuestra la Figura No 141, al existir disponibilidad de ancho de banda, este es utilizado por el servicio de video al no existir saturación.

d) Tráfico recibido en l simulación No 3.-

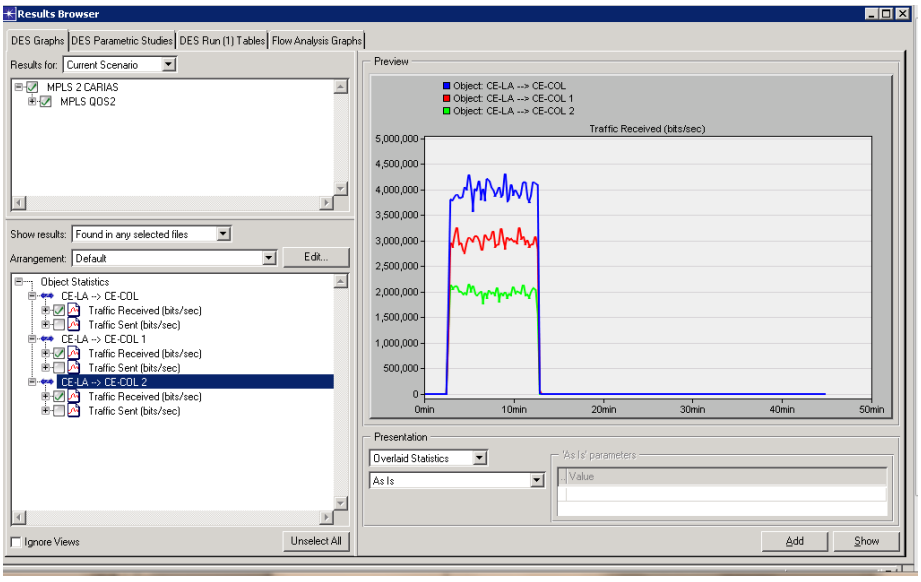


Figura No 142.- Tráfico recibido Simulación No 3.

El ancho de banda disponible es utilizado por los servicios que lo requieran, en este caso de datos y video sin existir saturación del canal como lo demuestra la Figura No 142.

e) Tráfico recibido en l simulación No 4.-

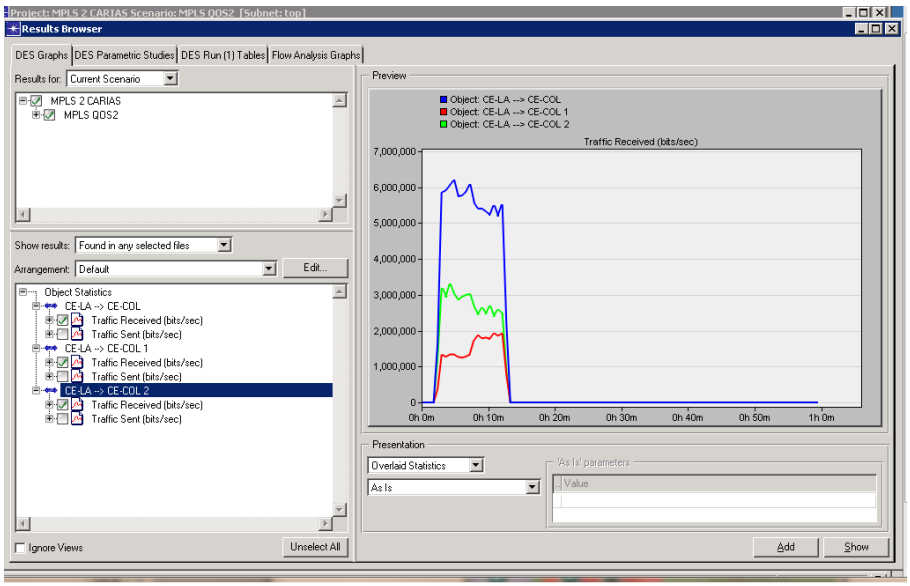


Figura No 143.- Tráfico recibido Simulación No 4.

En la Figura No 143 se observa que si el canal es saturado, la prioridad en el transporte del tráfico será la voz por la configuración de priority y la clase EF, luego el tráfico del video con la clase AF41 y finalmente los datos con la clase AF31. Es necesario recordar que el tráfico es compartido en el canal, sin embargo por la política establecida de garantizar el ancho de banda mínimo, se observa que en ningún momento los servicios transportan tráfico menor a lo garantizado, es decir para la voz el 20% equivalente a 2 Mbps, los datos 10% equivalente a 10 Mbps y el video con un 30% equivalente a 3 Mbps. A continuación en la Figura No 144 se demuestra la ruta empleada al transportar el tráfico.

f) Ruta del tráfico cursado:

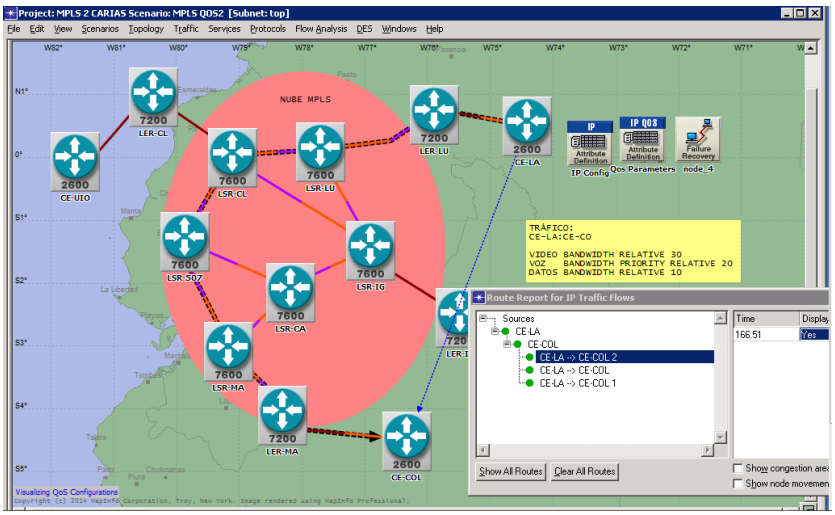


Figura No 144.- Ruta del tráfico con QoS.

f) Ruta de Tráfico con caída de enlace LSR-LU-LSR-CL:

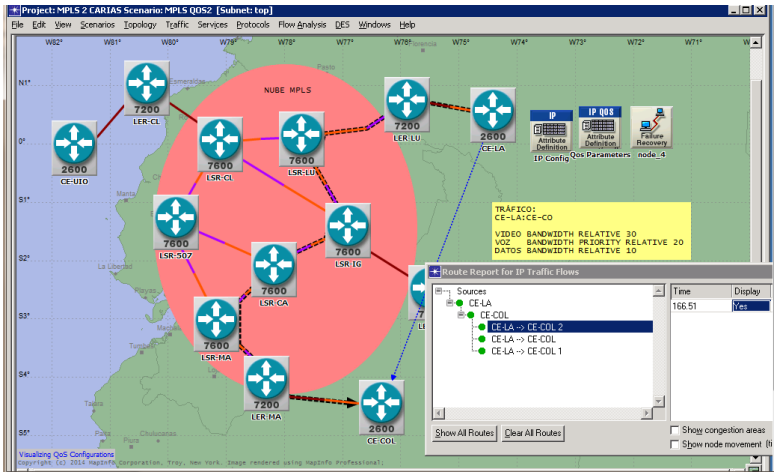


Figura No 145.- Ruta con caída de enlace QoS.

En la Figura No 145 se observa la ruta del tráfico con Qos y falla de enlaces LSR-LU y LSR-CL.

4.2.7.- Evaluación Escenario 7: Configuración Policing.

Para evitar la congestión en el canal y en base a los conceptos descritos en el capítulo 3 se aplicará la política de Policing. Para el caso de la simulación es aplicado al tráfico de datos, sin embargo en el capítulo 3 se determinó que esta política será aplicada al servicio de voz en la interfaz de ingreso al router LER, por ser una aplicación de tiempo real, en la cual no es conveniente que exista delay ni

encolamiento en la trasmisión de paquetes en la comunicación como lo realiza la política de shaping, ideal para aplicaciones de datos.

Es importante señalar que la simulación es para comprender las facilidades de la tecnología MPLS, las políticas aplicadas a cada servicio están escritas en el capítulo 3. El tráfico utilizado es descrito en la tabla No 69:

Tabla No 69.- Tráfico Policing para QoS

SIMULACIÓN	TRÁFICO		
SERVICIO	**VIDEO (CE-LA-CE-COL)**	**VOZ (CE-LA-CE-COL 2)**	**DATOS (CE-LA-CE- COL 1)**
SIMULACIÓN.	10 Mbps	4 Mbps	3 Mbps

a) Tráfico generado en la simulación:

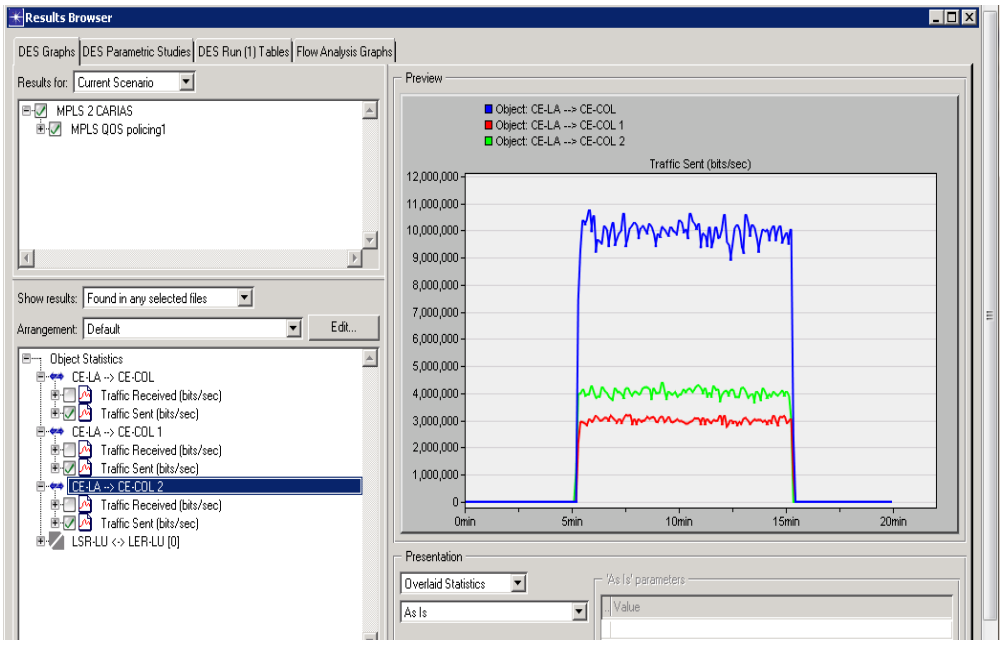


Figura No 146.- Tráfico generado en la simulación Policing.

b) Tráfico recibido en la simulación:

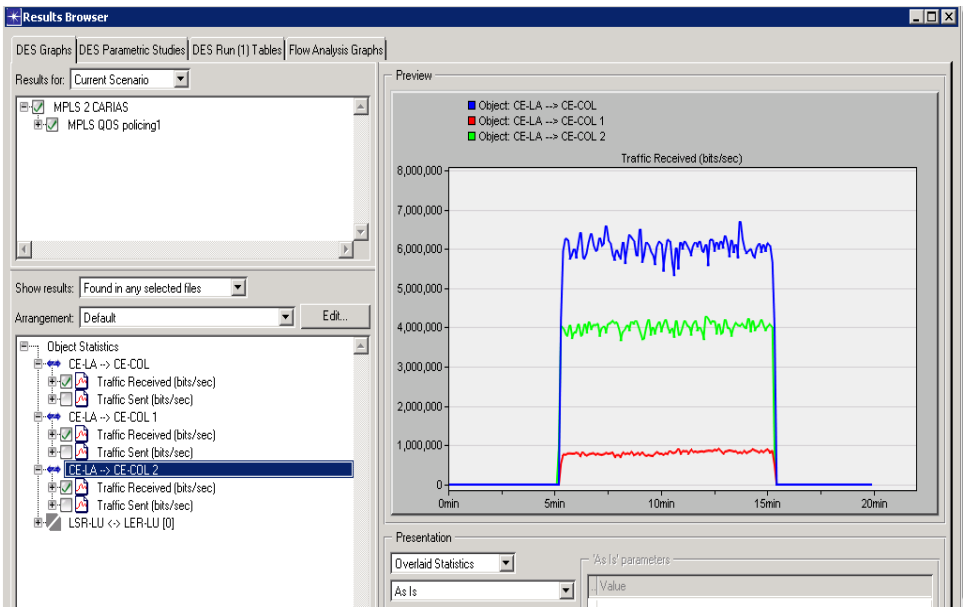


Figura No 147.- Tráfico recibido en la simulación Policing.

En base a las Figuras No 146 y 147, se analiza el resultado en el cual se puede apreciar que llega todo el tráfico de voz como prioridad; es decir los 4 Mbps llegan a su destino. Para el tráfico de datos se aplica la política de policing a 1 Mbps, verificándose que se limita a este ancho de banda cumpliendo el objetivo de la política. El resto de ancho de banda es empleado por el servicio de video. Come se describió en el capítulo 3, la política de policing sería aplicada a los servicios en tiempo real y la de shaping al servicio de datos, esto permitirá evitar la congestión en el canal.

4.2.8.- Evaluación Escenario 8: Configuración Ingeniería de Tráfico.

Para la evaluación de este escenario se supondrá que en cada LER existirá tráfico que ingrese de diferentes usuarios CE´s, por lo cual se puede crear túneles para cada usuario. Para comprobar el funcionamiento de un túnel según la configuración descrita en el presente capítulo, se creará dos túneles entre el LER-LU y LER-MA que permitirá visualizar como el tráfico descrito en la Tabla No 70 navega por cada uno de estos caminos:

Tabla No 70.- Tráfico Policing Túneles.

SIMULACIÓN	TRÁFICO			
SERVICIO	**VIDEO**	**VOZ**	**DATOS**	**TÚNEL**
SIMULACIÓN 1.-	5 Mbps	2 Mbps	500 Kbps	**LER-LU-LER-MA**
SIMULACIÓN 2.-	5 Mbps	2 Mbps	500 Kbps	**LER-LU-LER-MA1**

a) Simulación 1.- LER-LU-LER-MA

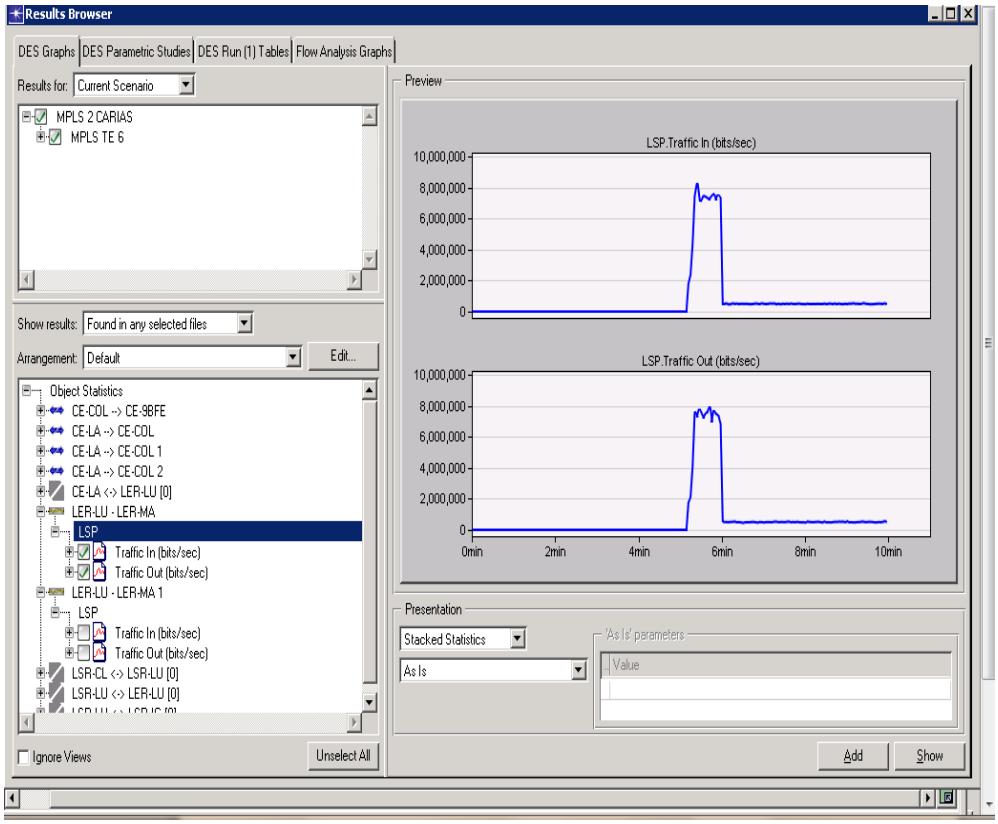


Figura No 148.- Tráfico en el túnel LER-LU-LER-MA

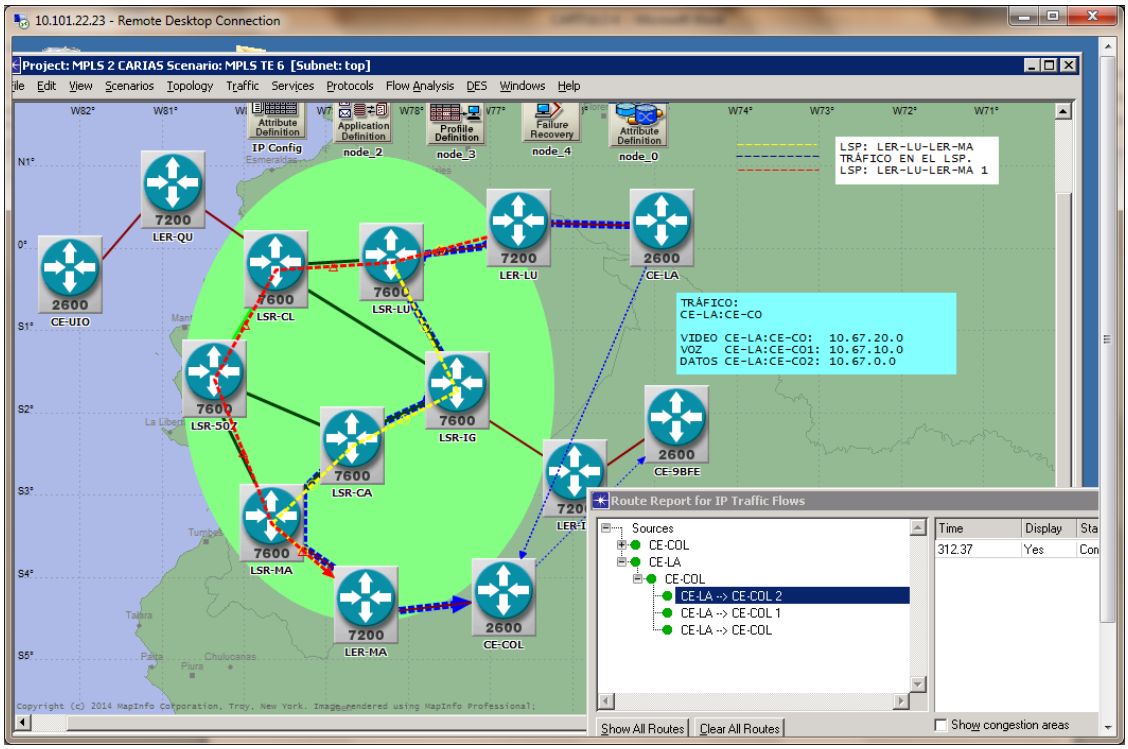


Figura No 149.- Ruta 1 del tráfico entre CE-LA y CE-COL por el LSP.

En las Figuras No 148 y 149, se puede observar que no existe errores en la transmisión del servicio, que el tráfico utiliza el túnel creado y la ruta que adquiere el tráfico que es la misma del túnel creado (LER-LU-LER-MA).

b) Simulación 1.- LER-LU-LER-MA 1

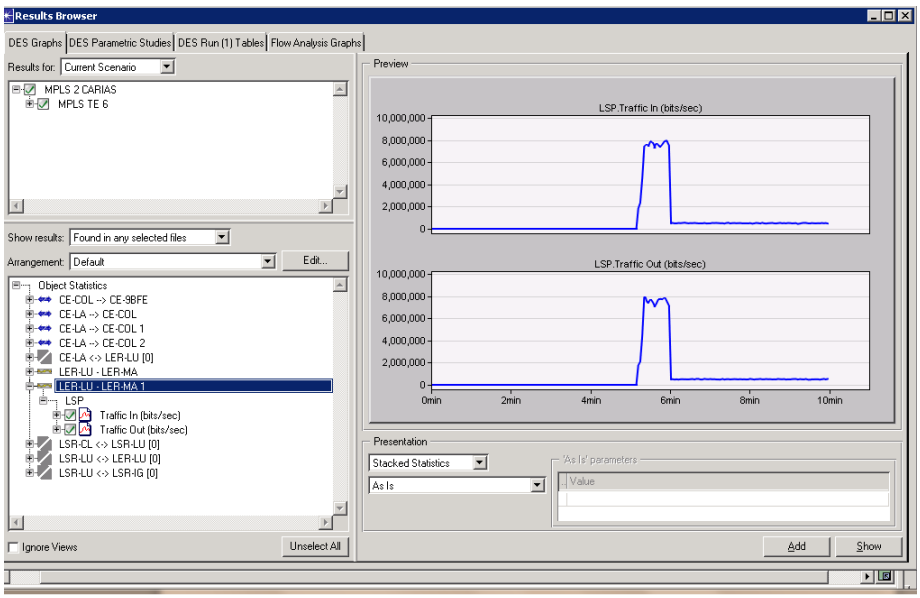


Figura No 150.- Tráfico en el túnel LER-LU-LER-MA 1.

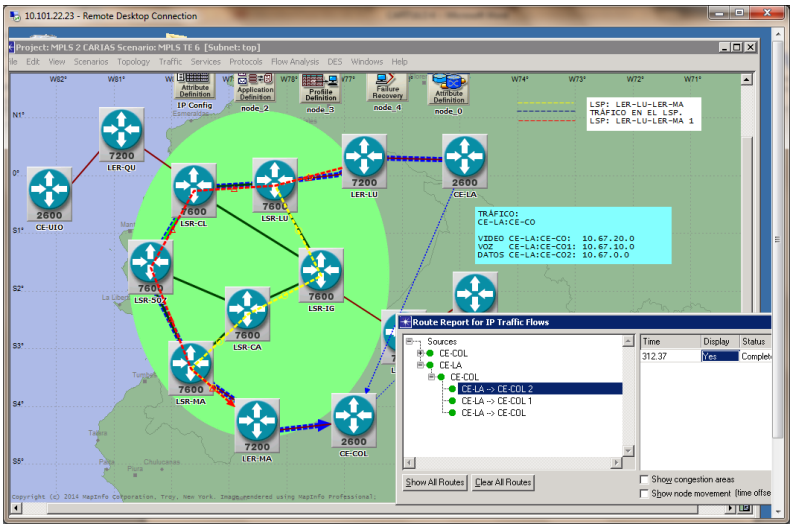


Figura No 151.- Ruta 2 del tráfico entre CE-LA y CE-COL por el LSP.

En las Figuras No 150 y 151, se puede observar que no existe errores en la transmisión del servicio, que el tráfico utiliza el túnel creado y la ruta que adquiere el tráfico que es la misma del túnel creado (LER-LU-LER-MA 1).

Con esta configuración se puede apreciar que el tráfico es enviado por donde se define las rutas en cada uno de los equipos. A continuación en la Figura No 152 se presenta las rutas definidas en cada LSP y que se pueden verificar visualmente en la simulación:

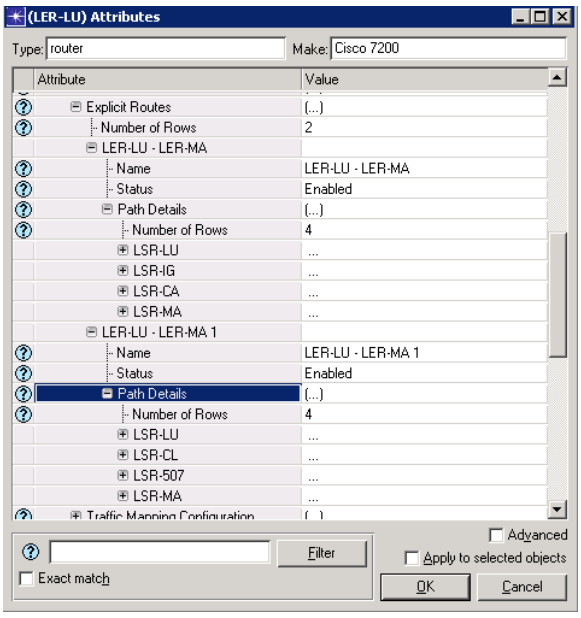


Figura No 152.- Rutas que realiza cada LSP.

CAPÍTULO 5
DIRECTIVA PARA ADMINISTRACIÓN, USO E IMPLEMENTACIÓN DE SERVICIOS Y EQUIPOS EN LA RED.

En el presente capítulo se establecerán los lineamientos generales por los cuales se realizará la administración, uso e implementación de servicios y equipos en la red, que servirán de base para la ejecución de proyecto en fuerzas armadas. comprendiendo la parte gerencial como tal y que regirá como política establecida en la red de datos.

5.1.-Políticas de administración.

- Establecer cuentas para los administradores de la red, destinando usuarios descentralizados y centralizados por responsabilidades en los diferentes Centros de Apoyo Electrónico (CAE´s) definidos en la Directiva AMSRET (Administración, mantenimiento y Seguridad de la Red Estratégica de Fuerzas Armadas). El CAE Quito tendrá la administración centralizada y nacional de la red, así como los LSR´s y LER´s de su región. Estas cuentas serán cambiadas de password cada seis (06) meses.
- Los accesos a la red y la integración de las unidades militares se realizará con autorización y coordinación con la Dirección de Tecnologías de la Información y comunicaciones del Comando Conjunto de las Fuerzas Armadas.
- Se llevará registros de las direcciones ip´s asignadas a cada Fuerza o unidad, así como las utilizadas en la red MPLS de Fuerzas Armadas.
- Se llevará registros de los servicios y anchos de banda asignados a cada unidad militar, los cuales permitirá establecer el crecimiento de la red de datos de Fuerzas Armadas.
- Se establecerá una bitácora de sucesos y soluciones que se presenten en la implementación de servicios o equipos a la red de datos.
- Se definirá un formato de ejecución de trabajos en base a los requerimientos de los usuarios, en donde se defina los protocolos empelados, su

direccionamiento, facilidades MPLS configuradas (calidad de servicio, túneles, VRF´s).

- Se dispondrá de manuales actualizados de configuraciones de los equipos en la red, así como un registro de estas configuraciones por equipo.
- Se realizará semestralmente un backup de las configuraciones de cada equipo de la red de datos
- Mensualmente se comprobará los tiempos de respuesta (ping) entre cada equipo de la red MPLS.
- Se analizará las rutas (trazas) empleadas por los equipos en cada servicio, a fin de establecer los caminos comúnmente empelados para el tráfico de la información, que facilitará a su vez la implementación de los túneles MPLS.
- Se elaborará un formato de satisfacción de los servicios implementados, los cuales deberán ser llenados semestralmente en cada unidad militar.
- Se implementarán equipos de seguridad en la red de datos, como lo son firewalls al ingreso de los equipos LSR´s de la red MPLS.
- Cada usuario de la red de datos (Unidades Militares), es el responsable de la administración de sus redes LAN, por lo cual se llevará un registro de personal responsable y forma de contacto para coordinaciones, siendo los únicos gestionadores de requerimientos las Direcciones de Comunicaciones e Informática de cada Fuerza.
- Los administradores de la red son los responsables del monitoreo, acceso y modificaciones en los equipos, el incumplimiento estará sujeto al reglamento de disciplina militar por el no cumplimiento de una disposición dependiendo de la falta cometida pudiendo establecer sanciones de afectación a la seguridad del Estado por el nivel de información que se transporta por la red.
- Todos los equipos instalados en la red de datos deberán ser debidamente etiquetados e ingresados a los activos del Comando Conjunto, cuya responsabilidad será en los administradores de la red.
- Los equipos instalados a nivel nacional deberán disponer de la seguridad física en el sitio, siendo la responsabilidad y custodia de cada unidad militar que proporciona la seguridad del sitio en base a la Directiva AMSRET.

- Se prohíbe la compartición de contraseñas ni la revelación de las mismas a otros usuarios.
- Elaborar y mantener actualizado el diagrama de red y diagramas de cada equipo detallando las conexiones físicas y puertos empleados.
- Se elaborará y mantendrá vigente un plan de mantenimiento preventivo en cada uno de los equipos en base a las responsabilidades de cada CAE, detallando los trabajos que se realizarán.
- Los cambios en la red deberán efectuarse de manera planificada evitando afectaciones al usuario e interrupciones en el servicio, previa autorización de la sección Servicios del Departamento de Telecomunicaciones.

5.2.-Políticas de uso en base a los servicios.

- Se prohíbe el uso de la red para otros fines que no sean los correspondientes al transporte de información empleada en apoyo a las operaciones y misiones militares.
- Los administradores de los servicios como telefonía, datos y video del Departamento de Telecomunicaciones del Comando Conjunto de las FF.AA, son los responsables de coordinar el acceso a la red de datos para la implementación de estos servicios.
- Se respetará las configuraciones en los equipos para cada servicio, en base a lo establecido, es decir el asignar una VRF para cada servicio.
- Los servicios en tiempo real deberán siempre tener prioridad en relación a otro tipo de servicio.
- Se respetará la forma de asignar el nombre a las VRF por el servicio implementado anteponiendo la palabra VRF al servicio.
- Se prohíbe la integración con otras redes de compañías públicas o privadas a la red de datos de Fuerzas Armadas.

5.1.-Políticas de implementación de equipos en base a la tecnología MPLS.

- Para la implementación de un equipo se realizará una planificación describiendo los responsables del trabajo, las características de configuración del equipo y su integración a la red de datos.
- En cada implementación se verificarán las rutas aprendidas por cada equipo y mediante comandos de verificación se establecerá mediante un check list las facilidades MPLS habilitadas y sus tiempos de respuesta para cada servicio.
- Se definirá como protocolos de la red MPLS a IS-IS como protocolo de enrutamiento, BGP para creación de VRF´s y LDP para el transporte de etiquetas MPLS.
- Se definirá una VRF para cada servicio entre LER´s, como VIDEOCOMACO y una número de vlan para cada uno de los mismos entre el LER y CE, por ejemplo vlan de datos No 10.
- Se establecerá en la red un único sistema autónomo para la red que fue definido como 65100.
- Para el protocolo IS-IS, el área identifier será 49.0001 y todos los equipos configurados en el mismo nivel level 2.
- Se definirá un rango de direccionamiento para las interfaces loopback, se recomienda el rango 10.68.254.0 /24, siendo las 30 primeras direcciones para los equipos LSR y la siguientes para los equipos LER´s.
- Se establecerá un direccionamiento para las interfaces de los equipos en la red 10.68.0.0 / 24, pudiendo los administrador varias la máscara en base al número de conexiones por equipo.
- Se establecerá un valor definido de RT y RD para cada VRF en base a la Fuerza y al servicio implementado, por ejemplo COMACO: 10 VOZ: 001, entonces RD: 10001
- Se implementarán los equipos con una configuración de calidad de servicio mediante la clasificación y marcaje de los paquetes, la asignación de anchos de banda para cada servicio y como políticas para evitar la congestión policing y shaping.

- Los túneles MPLS serán habilitados en base al análisis del tráfico, determinándose las rutas adecuadas que permitan efectuar un balanceo de carga o determinar la mejor ruta para un tráfico determinado.
- La implementación de equipos CE serán de responsabilidad de los usuarios, quienes deberán gestionar a la Dirección de Tecnologías de la Información y Comunicaciones del CC.FF.AA, las características mínimas que deben cumplir los equipos.
- Los equipos CE´s de los Comandos Operacionales dependerán directamente de la administración del Departamento de Telecomunicaciones por ser unidades dependientes directamente del Comando Conjunto de las FF.AA.
- Los E1´s del sistema PDH, serán multiplexados, para disponer de una capacidad superior y disponer directamente de la interfaz Ethernet.
- En el sistema SDH la capacidad será mapeada en los puertos ISA de interfaz Ethernet propia del sistema.

CAPÍTULO 6
CONCLUSIONES Y RECOMENDACIONES.

6.1.- *Conclusiones.*

- Mediante el desarrollo del presente proyecto, se estableció la situación actual de la Red de Datos de Fuerzas Armadas, mediante el análisis de servicios, equipos, configuraciones, matriz de tráfico y configuraciones actuales; así como la determinación del crecimiento de la red a mediano plazo.
- En base a la situación de la red, se determinó que la capacidad de la red de transporte es subutilizada al emplear E1's para cada uno de los servicios, lo que dificulta la integración de los servicios de voz, datos y videoconferencia.
- Se realizó el marco conceptual en base al estudio de la tecnología MPLS, su operación y funcionalidades; así como el empleo del software de simulación OPNET, que facilitaron el desarrollo del diseño y comprobación de resultados en relación a los conceptos establecidos.
- Se elaboró un diseño de red de datos con topología de costo mínimo, en base a la distancia entre los enlaces de los ramales de los anillos de transporte de la red Mode, permitiendo establecer una estructura jerárquica con equipos de networking distribuidos en capas de core, distribución y acceso.
- Se determinó la necesidad de incrementar la capacidad de transporte de la red Mode, considerando el crecimiento de los servicios en la red de datos a mediano plazo; así como la necesidad de multiplexar los canales E1´s para ser utilizados en la convergencia de servicios, evitándose la subutilización de estos canales.
- Se evaluó la propuesta establecida mediante el software de simulación OPNET, considerando las funcionalidades de la tecnología MPLS, analizándose tiempos de respuesta, configuraciones de protocolos LDP, IS-IS, BGP; así como la visualización y comprobación del empleo de las facilidades como VPN, QoS e ingeniería de tráfico que facilita y garantiza el tráfico de la información en la red.

- El simulador empleado en la plataforma OPNET, facilita la visualización de comportamiento de las facilidades MPLS configuradas en la red, sin embargo presenta ciertas dificultades al no disponer de material de consulta, poca información en la web, falta de manuales destinados para el efecto y caducidad de licencias para simular todas las facilidades de la tecnología MPLS.
- Las políticas para la administración, uso e implementación de la red permitirán definir los lineamientos generales a los cuales se sujetaran los administradores y usuarios, a fin de establecer un adecuado control y crecimiento de la red en base a los servicios implementados.
- Con el desarrollo de la presente tesis se ha cumplido los objetivos propuestos y se proporciona al personal técnico del Departamento de Telecomunicaciones del Comando Conjunto una guía para la implementación de la tecnología MPLS en la red; además del primer material didáctico y guía de configuración del software OPNET adquirido por esta Institución y que no se ha explotado en el simulación de redes y este tipo de tecnologías.

6.2.- Recomendaciones.

- Multiplexar los E1´s para optimizar la capacidad actual de la red de transporte PDH y emplear los puertos ISA del SDH, que permitirán emplear interfaces Ethernet.
- Elaborar un proyecto para la migración de los enlaces de transporte PDH/SHD a tecnología puramente IP que permita manejar mayores capacidades acorde a las requeridas y proyectadas por los usuarios para sus aplicaciones.
- Difundir el conocimiento de la tecnología MPLS y sus facilidades al personal técnico y de ingenieros del Departamento de Telecomunicaciones del CC.FF.AA, con miras a la futura implementación de esta tecnología en la red de datos de FF.AA.
- Profundizar el conocimiento de la tecnología MPLS, por sus facilidades y la mejor manera de explotarlas en la implementación de la red de datos de Fuerzas Armadas.

- Considerar el diseño desarrollado en el presente trabajo, para ser implementado en la red de datos de Fuerzas Armadas, por presentar una topología de costo mínimo y fundamentado en capas de core, distribución y acceso.
- Adquirir actualizaciones de las librerías del simulador OPNET modeler, ya que no dispone de equipos actuales desarrollados por los grandes fabricantes como cisco, que permita una simulación con los equipos propuestos; así como ciertas facilidades que la tecnología MPLS dispone.
- Difundir y emplear las políticas establecidas en el presente proyecto, que faciliten la coordinación e integración permanentemente con los usuarios y las proyecciones reales de sus aplicativos, que permita ir dimensionando la red de transporte y de datos en base a sus proyectos planteados.
- Gestionar los recursos para la implementación de esta tecnología en la red de datos, priorizando este proyecto en el PAI del Comando Conjunto.

REFERENCIAS BIBLIOGRÁFICAS

- BEGHELLI, A. (s.f.). Planificación de redes. *Módulo de Redes*. Ecuador.
- CISCO. (s.f.). *TOP/DOWN DESIGNER*. Obtenido de http://www.cisco.com/web/learning/le31/le46/cln/qlm/CCDA/design/top-down-approach-to-network-design-3/player.html
- DÍAZ, L. (s.f.). Tesis de Mestría. *MPLS en la red IPN*. México DF: ESIME-Zacatenco.
- FERRER, M. (s.f.). *Multiprotocolo label wsitching.*
- FIXGROUP. (2008). *Manual Introduction to Modeler.*
- ICARAN, J. (s.f.). *Estudio y Configuración de una VPN MPLS-BGP.* Madrid: USM.
- RAFAEL, J. (s.f.). *Modelamiento OPNET.* Universidad Politécnica de Valencia.
- SERVIN, A. (s.f.). *Propuesta de implementación del protocolo ISIS.* Obtenido de http://wgrouting.internet2.unam.mx/propuesta-isis.pdf
- THOMAS, R. (s.f.). *Planning Teelcommunication networks.*
- URQUIZA, L. (2011). *MPLS.* Quito: Escuela Politécnica Nacional CEC.
- YOANDI, G. (2010). Análisis, diseño y propuesta para un generador de topologías ip/mpls. *Tesis de mestría*. La Habana, Cuba: CUJAE.

ANEXO A "PROYECCIÓN DE REQUERIMIENTOS A MEDIANO PLAZO".

QUITO:

ESTACIÓN	USUARIOS	SERVICIOS REQUERIDOS	AB ACTUAL (MBPS)	AB REQUERIDO A MEDIANO PLAZO	INDICE DE CRECIMIENTO ANUAL	AB PROYECTADO
QUITO	COMACO	voz datos videoconferencia	3.8	8.8	0.2	21.90
	CGFT					
	CGFN					
	CGFA					
	SATELITAL					
	DRMOV					
	DIREL					
	COS II					
	I DE					
	MIDENA					
CRUZ LOMA	I-DE (CO-4)	voz datos videoconferencia	3.83	5.83	0.2	14.51
	HG-1					
	CETEL					
	FLOPEC					
	COLOG					
	COCOM					
	ISSFA					
	RADAR MONJAS					
PILISURCO	ESPE LAT.	voz datos videoconferencia	1.29	1.29	0.2	3.21
	CAL-9					
	DIREL LAT					
	BACO MISILES					
	9 BFE					
ATACAZO	CEE	voz, datos, videoconferencia	0.26	0.26	0.2	0.65
COTACACHI	CO-1		0.35	5.35	0.2	13.31

CONTINÚA ⟶

	DISAFA	voz, datos, videoconferencia				
BOMBOLI	INTELIGENCIA MANABÍ		0.33	0.33	0.2	0.82
	INTELIGENCIA SANTO DOMINGO	voz, datos, videoconferencia				
ZAPALLO	CEE. ESMERALDAS	voz datos videoconferencia	2.01	4.01	0.2	9.98
	BIMOT-13					
	BIMLOR					
	MATAJE					
	SISTEMA TRONCALIZADO					
	INT.COOPNO					
	BIMESM					
	DEFENSA AÉREA MIRLO					
MIRAVALLE	G.E.O	voz datos videoconferencia	1.5	1.5	0.2	3.73
	25-BAL					
	GESE					
	INADE					
	HAGAR PRESIDENCIAL					
	ESCOLTA PRESIDENCIAL					
	POLVORÍN CORAZÓN					
	ALA-11					
SAN LORENZO	TRONCALIZADO BIMLOR	voz datos videoconferencia	0.45	2.45	0.2	6.10
	FAE RADAR SAN LORENZO					
	INTELIGENCIA BIMLOR					

CONTINÚA ⟶

QUITO	GUAYAQUIL	voz, datos, videoconferencia, Defensa Aérea	14.26	19.26	0.2	47.93
QUITO	COCA	voz, datos, videoconferencia	2.71	7.71	0.2	19.18
QUITO	MACHALA	voz, datos, videoconferencia, Defensa Aérea	2	7	0.2	17.42
		TOTAL	32.79	63.79	0.2	158.73

GUAYAQUIL:

ESTACIÓN	USUARIOS	SERVICIOS REQUERIDOS	ANCHO DE BANDA ACTUAL	ANCHO DE BANDA REQUERIDO A MEDIANO PLAZO	INDICE DE CRECIMIENTO ANUAL	ANCHO DE BANDA PROYECTADO
507	II-DE	voz datos videoconferencia Defensa Aérea	3.2	10.2	0.2	25.38
	CAE-CEE WIMAX					
	TAURITAS					
	LAN BAL- 74					
	LAN COE-5 WIMAX					
	UHF AM/FM AEREO					
	AVINAV					
	TRONKALIZADO 507					
	TRONKALIZADO BALAO					
	E.I.A					
	CORGAL					
	CORIOS					
	COAD (CO-5)					
	LAN MTE-SINAI					

CONTINÚA ⟶

	SHILCA					
	SHIRY					
	TANATA					
	TANQUI					
	TRACAL					
	DIRVIV					
	FRAMOR					
	FRAPAL					
	CORESM					
	CORLOJ					
	LAMQUI					
	LAMUIL					
	LAMCUE					
	TAURA					
	DAC					
SALINAS	TRONKALIZADO SALINAS	voz	2.3	2.3	0.2	5.72
	PUNTA BARANDUA	datos videoconferencia				
	BIMOT-14					
	ESSUNA					
	ESMA					
CAE-GYE	QUEVEDO ARMAS	voz	11.57	11.57	0.2	28.79
	COOPNA (CO 2)	datos videoconferencia				
	CEE MACAS					
	21-BS CONDOR					
	JABONCILLO					
	GUALAQUIZA					
	WAN CERRO SALINAS					
	FAE COAD					
	FAE SALINAS					
	FAE TAURA					
	FAE MANTA					

CONTINÚA ⟶

	FM- SALINAS					
	COAVNA					
	FAE HALCON					
	ENLACE JABOMCILLO					
	BASNOR					
	INTELIGENCIA GUAYAS					
JABONCILLO	GCM-12	voz	3	3	0.2	7.46
	LAN GRUP TRABAJO MANABI	datos				
	TRONK. JABONCILLO	videoconferencia				
	INTELIGENCIA TNT. HUGO ORTIZ					
	TRONK. CABUYAS					
	ALERTA TEMPRANA FAE					
	INTELIGENCIA CAPMAN					
	INTELIGENCIA MANTA					
	WIMAX ALA 23					
	ESANMA					
	POLVORINES JARAMIJO					
GUAYAQUIL	QUITO	voz, datos, videoconferencia	14.26	19.26	0.2	47.93
GUAYAQUIL	MACHALA	voz, datos, videoconferencia	0.38	5.38	0.2	13.39
GUAYAQUIL	COCA	voz, datos, videoconferencia	0.27	5.27	0.2	13.11
		TOTAL	34.98	56.98	0.2	141.78

COCA:

ESTACIÓN	USUARIOS	SERVICIOS REQUERIDOS	AB ACTUAL (MBPS).	AB REQUERIDO A MEDIDANO PLAZO	INDICE DE CRECIMIENTO ANUAL	AB PROYECTADO
NODO COCA	19-BS (IV DE)	voz	2.6	7.6	0.2	18.91
	CAPORE	datos				
	CONTROL DE ARMAS	videoconferencia				
	ENLACE SHANGRILA					
	INTELIGENCIA					
LUMBAQUI	RADAR CÓNDOR	voz	7.6	12.6	0.2	31.35
	BAL IV-DE	datos				
	CAMPO BERMEJA G.E	videoconferencia				
	SISTEMA TIERRA AIRE (FAE)	Defensa Aérea				
	LAGO AGRIO-GFE-53					
	LAGO AGRIO-GRUPO VIAL AMAZÓNICO (CEE)					
	LAGO AGRIO-FAE LAGO AGRIO					
	CAPITANÍA FARFÁN					
	DESTACAMENTO LAURO GUERRERO					
	SANTA CECILIA-BS-56					
	SANTA CECILIA-INTELIGENCIA					
	SANTA CECILIA-F. REACCIÓN BS-56 (FAE)					
	DESTACAMENTO COOPER					
	DESTACAMENTO SANSAHUARI					

CONTINÚA ⟶

	SHUSHUFINDI-BOES-54 PUTUMAYO-BS-55 PUTUMAYO-CAPMAY DESTACAMENTO PANIPALI DESTACAMENTO ZANCUDO TIPUTINI-BS-57 DESTACAMENTO ROCAFUERTE					
COCA	GUAYAQUIL	voz, datos, videoconferencia	0.27	5.27	0.2	13.11
COCA	QUITO	voz, datos, videoconferencia	2.71	7.71	0.2	19.18
COCA	MACHALA	voz, datos, videoconferencia	0.75	5.75	0.2	14.31
		TOTAL	13.93	38.93	0.2	96.87

MACHALA:

ESTACIÓN	USUARIOS	SERVICIOS REQUERIDOS	AB ACTUAL(MBPS).	AB REQUERIDO A MEDIANO PLAZO	INDICE DE CRECIMIENTO ANUAL	AB PROYECTADO
LOMA PALMAR	BI-2 BI-3 ESCART RADAR COLIBRÍ BIMJAM	voz, datos, videoconferencia, Defensa Aérea	0.7	2.7	0.2	6.72
CAE - MACHALA	1-BI CONTROL DE ARMAS	voz, datos, videoconferencia	1.8	6.8	0.2	16.92

CONTINÚA ⟶

	INTELIGENCIA CAE-LOJA					
HITO CRUZ	CAE-CUENCA 27-BA	voz, datos, videoconferencia	0.7	0.7	0.2	1.74
CUENCA	III-DE (CO-3)	voz, datos, videoconferencia	3.74	8.74	0.2	21.75
MACHALA	GUAYAQUIL	voz, datos, videoconferencia	0.38	5.38	0.2	13.39
MACHALA	COCA	voz, datos, videoconferencia	0.75	5.75	0.2	14.31
MACHALA	QUITO	voz, datos, videoconferencia	2	7	0.2	17.42
		TOTAL	10.07	37.07	0.2	92.24

ANEXO B "REQUERIMIENTOS DE USUARIOS"

ANILLO CENTRAL:

ESTACIÓN	USUARIOS	SERVICIOS REQUERIDOS	AB ACTUAL (MBPS)	AB REQUERIDO A MEDIANO PLAZO	AB POR UNIDAD	TOTAL
QUITO	COMACO	voz	3.8	127.5	21	
	CGFT	datos			21	
	CGFN	videoconferencia			21	
	CGFA				21	
	SATELITAL				20	
	DIRMOV				2.5	
	DIREL				2.5	
	COS II				2.5	
	MIDENA				16	127.5
CRUZ LOMA	I-DE (CO-4)	voz	3.83	57.5	16	
	HG-1	datos			16	
	CETEL	videoconferencia			2	
	FLOPEC				1	
	COLOG				2	
	COCOM				9	
	ISSFA				9	
	RADAR MONJAS				2.5	57.5
PILISURCO	ESPE LAT.	voz	1.29	22	9	
	CAL-9	datos			2	
	DIREL LAT	videoconferencia			1	
	BACO MISILES				1	
	9 BFE				9	22
ATACAZO	CEE	voz, datos, videoconferencia	0.26	2.5	2.5	
COTACACHI	CO-1	voz, datos, videoconferencia	0.35	33	17	
	DISAFA				16	33
BOMBOLI	INTELIGENCIA MANABÍ	voz, datos, videoconferencia	0.33	2	1	
	INTELIGENCIA SANTO DOMINGO				1	2
ZAPALLO	CEE. ESMERALDAS	voz	2.01	4.01	2.5	
	BIMOT-13	datos			9	
	BIMLOR	videoconferencia			9	
	MATAJE				1	
	SISTEMA				1	

CONTINÚA ⟶

	TRONCALIZADO					
	INT.COOPNO				1	
	BIMESM				9	
	DEFENSA AÉREA MIRLO				2.5	35
MIRAVALLE	G.E.O	voz	1.5	43.5	2.5	
	25-BAL	datos			9	
	GESE	videoconferencia			1	
	INADE				9	
	HAGAR PRESIDENCIAL				2	
	ESCOLTA PRESIDENCIAL				2	
	POLVORÍN CORAZÓN				9	
	ALA-11				9	43.5
SAN LORENZO	FAE RADAR SAN LORENZO	voz, dtaos, videoconferencia	0.45	3.5	2.5	
	INTELIGENCIA BIMLOR				1	3.5
QUITO	GUAYAQUIL	voz, datos, videoconferencia, Defensa Aérea	14.26	442.8	si existe ese requerimiento, existiría un incremento de tráfico aproximado de 30 veces =442.8	
QUITO	COCA	voz, datos, videoconferencia	2.71	81.3		
QUITO	MACHALA	voz, datos, videoconferencia, Defensa Aérea	2	60		
		TOTAL	32.79	879.61		

ANILLO OESTE:

ESTACIÓN	USUARIOS	SERVICIOS REQUERIDOS	ANCHO DE BANDA ACTUAL.	ANCHO DE BANDA REQUERIDO A MEDIANO PLAZO	AB POR UNIDAD	TOTAL
507	II-DE	voz	3.2	88	16	
	CAE-CEE WIMAX	datos			1	
	TAURITAS	videoconferencia			1	
	LAN BAL- 74	Defensa Aérea			2	
	LAN COE-5 WIMAX				1	
	UHF AM/FM AEREO				1	
	AVINAV				9	

CONTINÚA ⟶

	TRONKALIZADO 507				1	
	TRONKALIZADO BALAO				1	
	E.I.A				9	
	CORGAL				1	
	CORIOS				1	
	COAD (CO-5)				17	
	LAN MTE-SINAI				2	
	SHILCA				1	
	SHIRY				1	
	TANATA				1	
	TANQUI				1	
	TRACAL				1	
	DIRVIV				1	
	FRAMOR				1	
	FRAPAL				1	
	CORESM				1	
	CORLOJ				1	
	CORORO				1	
	LAMQUI				1	
	LAMUIL				1	
	RENCHI				1	
	LAMCUE				1	
	TAURA				9	
	DAC				1	88
SALINAS	TRONKALIZADO SALINAS	voz	2.3	29	1	
	PUNTA BARANDUA	datos			1	
	BIMOT-14	videoconferencia			9	
	ESSUNA				9	
	ESMA				9	29
CAE-GYE	QUEVEDO ARMAS	voz	11.57	50.5	1	
	COOPNA (CO 2)	datos			17	
	CEE MACAS	videoconferencia			1	
	21-BS CONDOR				9	
	GUALAQUIZA				1	
	COAVNA				9	
	FAE HALCON				2.5	
	BASNOR				9	
	INTELIGENCIA GUAYAS				1	50.5
JABONCILLO	GCM-12	voz	3	15.5	2.5	
	LAN GRUP TRABAJO MANABI	datos			1	
	TRONK. JABONCILLO	videoconferencia			1	
	INTELIGENCIA TNT. HUGO ORTIZ				1	

CONTINÚA ⟶

	TRONK. CABUYAS				1	
	ALERTA TEMPRANA FAE				1	
	INTELIGENCIA CAPMAN				1	
	INTELIGENCIA MANTA				1	
	WIMAX ALA 23				2	
	ESANMA				2	
	POLVORINES JARAMIJO				2	15.5
GUAYAQUIL	QUITO	voz, datos, videoconferencia	14.26	442.8		
GUAYAQUIL	MACHALA	voz, datos, videoconferencia	0.38	17.1		
GUAYAQUIL	COCA	voz, datos, videoconferencia	0.27	2.43		
		TOTAL	20.07	645.33		

ANILLO NORTE:

ESTACIÓN	USUARIOS	SERVICIOS REQUERIDOS	AB ACTUAL (MBPS).	AB REQUERIDO A MEDIANO PLAZO	AB POR UNIDAD	TOTAL
NODO COCA	19-BS (IV DE)	voz	2.6	23	16	
	CAPORE	datos			2	
	CONTROL DE ARMAS	videoconferencia			2	
	ENLACE SHANGRILA				2	
	INTELIGENCIA				1	23
LUMBAQUI	RADAR CÓNDOR	voz	7.6	49.5	2.5	
	BAL IV-DE	datos			9	
	CAMPO BERMEJA G.E	videoconferencia			2	
	SISTEMA TIERRA AIRE (FAE)	Defensa Aérea			1	
	LAGO AGRIO-GFE-53				2.5	
	LAGO AGRIO-GRUPO VIAL AMAZÓNICO (CEE)				2.5	
	LAGO AGRIO-FAE LAGO AGRIO				2.5	
	CAPITANÍA FARFÁN				2	
	DESTACAMENTO LAURO GUERRERO				1	
	SANTA CECILIA-BS-56				9	

CONTINÚA ⟶

	SANTA CECILIA-INTELIGENCIA				1	
	SANTA CECILIA-F. REACCIÓN BS-56 (FAE)				1	
	DESTACAMENTO COOPER				1	
	DESTACAMENTO SANSAHUARI				1	
	SHUSHUFINDI-BOES-54				2.5	
	PUTUMAYO-BS-55				2.5	
	PUTUMAYO-CAPMAY				1	
	DESTACAMENTO PANIPALI				1	
	DESTACAMENTO ZANCUDO				1	
	TIPUTINI-BS-57				2.5	
	DESTACAMENTO ROCAFUERTE				1	49.5
COCA	GUAYAQUIL	voz, datos, videoconferencia	0.27	2.43	si existe ese requerimiento, el tráfico se incrementaría aproximado de 9 veces =2.43	
COCA	QUITO	voz, datos, videoconferencia	2.71	81.3		
COCA	MACHALA	voz, datos, videoconferencia	0.75	33.75		
		TOTAL	10.47	189.98		

ANILLO SUR:

ESTACIÓN	USUARIOS	SERVICIOS REQUERIDOS	AB ACTUAL(MBPS).	AB REQUERIDO A MEDIANO PLAZO	AB POR UNIDAD	TOTAL
LOMA PALMAR	BI-2	voz, datos, videoconferencia, Defensa Aérea	0.7	31.5	9	
	BI-3				9	
	ESCART				2	
	RADAR COLIBRÍ				2.5	
	BIMJAM				9	31.5
CAE – MACHALA	1-BI	voz, datos, videoconferencia	1.8	13	9	
	CONTROL DE ARMAS				2	
	INTELIGENCIA				1	
	CAE-LOJA				1	13
HITO CRUZ	CAE-CUENCA	voz, datos, videoconferencia	0.7	10	1	
	27-BA				9	10

CONTINÚA ⟶

CUENCA	III-DE (CO-3)	voz, datos, videoconferencia	3.74	17	17	17
MACHALA	GUAYAQUIL	voz, datos, videoconferencia	0.38	17.1	si existe ese requerimiento, existiría un incremento de tráfico aproximado de 45 veces =17.1	
MACHALA	COCA	voz, datos, videoconferencia	0.75	33.75		
MACHALA	QUITO	voz, datos, videoconferencia	2	60		
		TOTAL	10.07	182.35		

ANEXO C "DISTANCIAS DE ENLACES"

DISTANCIAS DE ENLACES SDH DEL ANILLO CENTRAL		
ORD.	ESTACION	DISTANCIA KM
ANILLO CENTRAL SDH		
1	QUITO - CRUZ LOMA	5.39
2	CRUZ LOMA - IGUALATA	144.78
3	IGUALATA - CARSHAO	109.63
4	CARSHAO - BASE SUR	119.54
5	BASE SUR - CERRO 507	15.73
6	CERRO 507 - AZUCENA	120.13
7	AZUCENA - BOMBOLI	126.79
8	BOMBOLI - ATACAZO	65.09
9	ATACAZO - QUITO	17.32
ENLACES PDH AWY		
	BOMBOLI - LA JUANITA	94.82
	LA JUANITA - ZAPALLO	47.52
	ZAPALLO - COOPNO	18.02

ORD.	ESTACION	DISTANCIA KM
ANILLO CENTRAL NORORIENTE		
1	CRUZ LOMA - COATACHI	61.56
2	COTACACHI - CAYAMBE	50.64
3	CAYAMBE - LUMBAQUI	73.42
4	LUMBAQUI - COCA	66.42
5	COCA - NAPO GALERAS	72.89
6	NAPO GALERAS - ABITAHUA	94.12
7	ABITAHUA - TABLON	44.09
8	TABLON - IGUALATA	14.56

ORD.	ESTACION	DISTANCIA KM
ANILLO CENTRAL OESTE		
1	AZUCENA - JABONCILLO	61.67
2	JABONCILLO - JARAMIJO	12.77
3	JABONCILLO - BASE MANTA	18.02
4	JABONCILLO - COROSO	49.27
5	COROSO - CABUYAS	28.52
6	CABUYAS - REP. SALINAS	74.76
7	REP. SALINAS - BASE SALINAS	0.83
8	REP. SALINAS - ANIMAS	66.42
9	ANIMAS - BASE SUR	66.94
10	BASE SUR - COOPNA	8.85

CONTINÚA ⟶

11	BASE SUR - DIRNEA	7.45
12	BASE SUR - CERRO 507	15.73
13	CERRO 507 - BASE GUAYAQUIL	11.18
14	CERRO 507 - BASE TAURA	37.06
15	CERRO 507 - GUANCAVILCA	7.31
16	CERRO 507 - NAVAL NORTE	11.93

ORD.	ESTACION	DISTANCIA KM
ANILLO CENTRAL SUR		
1	CARSHAO - BUERAN	19.25
2	BURAN - TERMINAL CUENCA	31.55
3	BUERAN - TINAJILLAS	67.81
4	TINAJILLAS - ACACANA	56.15
5	ACACANA - VILLONACO	34.44
6	VILLONACO - TERMINAL LOJA	6.74
7	VILLONACO - MOTILON	84.27
8	MOTILON - MACHALA	91.23
9	MACHALA - BALAO CHICO	61.86
10	BALAO - CERRO 507	77.69

ANEXO D "PROYECTO MPLS-SENPLADES"

COMANDO CONJUNTO DE LAS FUERZAS ARMADAS
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

1. DATOS GENERALES DEL PROYECTO

1.1. Nombre del PROYECTO.

IMPLEMENTAR UNA RED DE DATOS PARA FUERZAS ARMADAS ORIENTADA A LA CONVERGENCIA DE SERVICIOS MEDIANTE UNA PLATAFORMA MPLS.

1.2. Entidad Ejecutora.

Comando Conjunto de las Fuerzas Armadas.

1.3. Unidades Atendidas.

Nombre(s): Unidades Militares a nivel Comandos Operacionales, Brigadas y Batallones
Localización: Territorio Nacional
Provincia(s):
Cantón:
Parroquia:

1.4. Monto.

Primera fase: USD 1´500.000,00

1.5. Plazo de Ejecución.

120 días, a partir de la entrega del anticipo

1.6. Sector y tipo del PROYECTO.

Sector: 1.6.1 Justicia y Seguridad.

Tipo: 1.6.2 Asuntos Internos.

1.6.3 Asuntos del Exterior.

2. DIAGNÓSTICO

2.1.Descripción de la situación actual del área de intervención del proyecto.

La red de datos se implementó bajo requerimientos puntuales de usuarios mediante una topología sustentada en los nodos principales de las centrales telefónicas ubicadas en Quito, Guayaquil, Coca y Machala, a partir de las cuales se han agregado los usuarios dependientes por regiones de estos nodos como se demuestra en la siguiente figura:

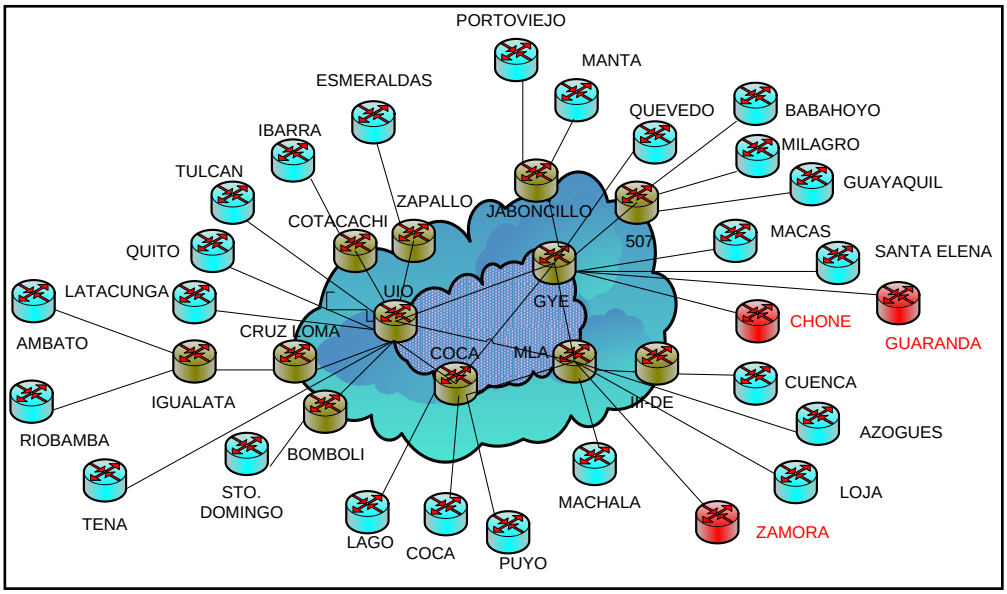


Figura No 1.- Estructura actual de la red de datos.

En base a los recursos de cada unidad se han implementado equipos de diferentes marcas que dificultan la administración y operación de la red de datos, siendo su capacidad física (puertos) y de procesamiento limitada a las aplicaciones que se están implementando en Fuerzas Armadas. Además de

existir capacidades E1´s de la red de transporte asignados a cada servicio, que ha ocasionado una subutilización de estos canales, que a su vez han impedido la convergencia de los servicios que al momento existen en la red.

El direccionamiento de la red, utiliza la clasificación de una red privada (10.0.0.0), las Fuerzas se reestructuraron para acoplarse al rango que les corresponde, de acuerdo a:

Rango	Fuerza Terrestre	Comando Conjunto	Fuerza Naval	Fuerza Aérea	Reserva
Desde	**10.0.0.0**	**10.64.0.0**	**10.128.0.0**	**10.160.0.0**	**10.192.0.0**
Hasta	**10.63.0.0**	**10.127.0.0**	**10.159.0.0**	**10.191.0.0**	**10.255.0.0**

2.2. Identificación, descripción y diagnóstico del problema

Resumiendo los problemas que motivan el desarrollo del presente proyecto son los siguientes:

- Subutilización de E1s para los diferentes servicios implementados en cada una de las unidades militares de Fuerzas Armadas a nivel nacional.
- No existe la integración en la red de datos de las centrales telefónicas a nivel nacional con tecnología Ip, así como la red de videoconferencia en alta definición para las unidades militares.
- Capacidad limitada de los equipos existentes, que no permiten aplicar QoS, balanceo de carga y funcionalidades que la tecnología actual proporciona para una red de datos, ocasionado retardo en los aplicativos especialmente en aquellos de tiempo real y que deben ser garantizados para las operaciones de Fuerzas Armadas a nivel nacional.
- Falta de una administración unificada del todo el equipamiento que maneja el protocolo Ip, como lo es routers, switch, equipos de videoconferencia, centrales telefónicas, etc.

- Integración de las agregadurías militares con acceso al servicio de voz y aplicativos de Fuerzas Armadas, mediante la elaboración de vpn's, que los constituyen como abonados remotos de la red de datos.
- Falta de políticas de implementación de equipos y servicios que se transportan por la red de datos, que permitan el control y direccionamiento a las Fuerzas y unidades militares a nivel nacional.
- Carencia de un diseño estructurado de la red de datos de Fuerzas Armadas, en base a equipos y tecnología con capacidad de soportar el crecimiento, integración y convergencia de los servicios implementados.

2.3. Línea Base del PROYECTO.

El presente proyecto tendrá su incidencia en la unidades militares a nivel nacional, las cuales transmiten la información de voz, datos y videoconferencia necesarias para el cumplimiento de las operaciones de Fuerzas Armadas en apoyo a las acciones del Estado, mediante canales E1´s asignados a cada servicio con equipos de networking de capacidades limitadas acorde al desarrollo de los aplicativos de Fuerzas Armadas. Para mejorar la red se implementarán equipos LSR, LER con tecnología MPLS y equipos de usuario que permitan el empleo de las funcionalidades como vpn´s, QoS e ingeniería de tráfico en cada uno de los servicios de la red de Fuerzas Armadas; que a su vez permitirá la integración y convergencia de estos servicios.

2.4. Análisis de Oferta y Demanda

Considerando los aplicativos de Fuerzas Armadas agrupados en voz, datos y videoconferencia, el crecimiento anual de la red desde su implementación y los requerimientos de las unidades se fundamenta en el siguiente cuadro:

UNIDAD	CAPACIDAD REQUERIDA(MBPS)
COMANDO DE FUERZA	21
COMANDO OPERACIONAL	17
DIVISIÓN/BRIGADA/HOSPITAL	16
BATALLÓN/BASE/ISSFA	9
GRUPO/COS/DIRMOV/CEE	2.5

CONTINÚA ⟶

COMPAÑÍA/CAPITANÍA/RETÉN	2
DESTACAMENTO/BASE GUERRA ELECTRÓNICA, INTELIGENCIA.	1

La Demanda de capacidad de la red de datos considerando la topología de anillos de la red de transporte PDH/SDH, será la descrita en el siguiente cuadro:

ANILLO	**CAPACIDAD**
CENTRAL	879.61 MBPS
NORTE	189.98 MBPS
OESTE	645.33 MBPS
SUR	182.35 MBPS

Sin embargo, el crecimiento de la red de datos se encuentra condicionado a la ejecución de los proyectos de las Fuerzas, existiendo aplicaciones de transmisión de aplicativos de tiempo real como el video, por lo cual la red deberá estar en capacidad de soportar transmisiones en el orden de Gbps.

Actualmente la red de datos no está en capacidad de ofertar la capacidad requerida, siendo las principales razones la subutilización de los canales E1´s asignados a cada servicio, la limitada capacidad de los equipos de networking implementados. En el mercado se han implementado en las redes de nueva generación equipos con tecnología MPLS, optimizando el desempeño de las redes, por lo cual las empresas han desarrollado equipos de gran capacidad y orientados a mejorar las funcionalidades de esta tecnología.

2.5. Identificación y Caracterización de la población objetivo

Con el desarrollo de la tecnología y sus aplicativos, se hace cada día imprescindible el disponer de información que facilite la toma de decisiones, especialmente en el ámbito militar cuyas misiones están orientadas al apoyo a las acciones del Estado. Las unidades que actúan en estas misiones se encuentran ubicadas en los niveles estratégico, operativo y táctico, siendo el ejecutor el Comando Conjunto, quien asume las decisiones directamente para

toda operación, razón por la cual se hace necesaria la disponibilidad de todos los aplicativos en todas las unidades y niveles antes mencionados.

Por lo tanto la población objetivo del proyecto estará conformada por todo el personal militar de las unidades en todos los niveles y a nivel nacional, que es ámbito de operación de Fuerzas Armadas.

3. OBJETIVOS DEL PROYECTO

3.1. Objetivo general y objetivos específicos

OBJETIVO GENERAL O PROPÓSITO

Reestructurar la red de datos de Fuerzas Armadas, mediante la implementación de equipos con tecnología MPLS, para proporcionar servicios de voz, datos y video a nivel nacional, con capacidad de soportar el crecimiento, integración y convergencia de los servicios.

OBJETIVOS ESPECIFICOS

- Implementar equipos con tecnología MPLS por capas o niveles de funcionamiento en core, distribución y acceso.

- Conocer el funcionamiento de la tecnología MPLS y sus bondades mediante una transferencia tecnológica al personal técnico del Departamento de Telecomunicaciones del CC.FF.AA.

- Migrar e integrar los servicios y aplicativos de Fuerzas Armadas en base a las funcionalidades de la tecnología MPLS.

- Implementar un sistema de gestión, que me permita monitorear y administrar todos los elementos que conforman la red MPLS.

3.2. Indicadores de resultado

- Se dispondrá de seis (6) equipos LSR que conformarán el Core de la red y se encargarán de conmutar las etiquetas.

- Se instalarán trece (13) equipos LER en la capa de Distribución, en los cuales se configurarán las facilidades que la tecnología proporciona.

- Se instalarán treinta (30) equipos CE en la capa de Acceso, en los cuales se integrarán los servicios de las unidades.

- Se dispondrá de diez (10) técnicos capacitados, para la operación, administración y mantenimiento de la red.

3.3. Matriz de Marco Lógico

Apéndice "A"

4. VIABILIDAD Y PLAN DE SOSTENIBILIDAD.

4.1. Viabilidad técnica.

Para determinar la viabilidad técnica se ha realizado un análisis de la tecnología y su implementación en el mercado, considerando que la red de Fuerzas Armadas es un red de similares características técnicas a una operadora privada con la particularidad en la seguridad, independencia y objetivos que van apegados a la misión de Fuerzas Armadas y su apoyo a las acciones del Estado.

Para la implementación de los equipos se considerará las facilidades de infraestructura pata la instalación de los equipos, en lo cual Fuerzas Armadas dispone de espacios en repetidoras y unidades militares ya que son sitios donde operan las estaciones de la red de transporte PDH/SDH. Los equipos serán instalados de acuerdo al siguiente detalle:

Equipos LSR:

Tabla No1.- Equipos LSR.

ESTACIÓN/REPETIDORA	NOMINATIVO
CRUZ LOMA	LSR-CL
LUMBAQUI	LSR-LU
CARSHAO	LSR-CA
CERRO 507	LSR-507
MACHALA	LSR-MA
IGUALATA	LSR-IG

Equipos LER:

Tabla No 2.- Equipos LER.-

ESTACIÓN	NOMINATIVO
CRUZ LOMA	LER-CL
QUITO	LER-QU
IGUALATA	LER-IG
ZAPALLO	LER-ZA
CERRO 507	LER-507
JABONCILLO	LER-JA
BASE SUR	LER-BS
SALINAS	LER-SA
BUERAN	LER-BU
MACHALA	LER-MA
COTACACHI	LER-CO
COCA	LER-CC
LUMBAQUI	LER-LU

Equipos CE:

Tabla No 3.- equipos CE.-

1	COMACO
2	CO-1
3	ALA 11
4	CGFA
5	CGFT
6	CGFN
7	BACO
8	9BFE
9	BIMLOS
10	MIRLO
11	CORAZÓN
12	BASE SUR
13	COOPNA

CONTINÚA ⟶

14 COOPNO
15 ALA 21
16 ALA 23
17 CO-2
18 CO-5
19 RADAR COLIBRÍ
20 CO-3
21 BINJAM
22 I-B1
23 19 BS
24 17 BS
25 GFE-53
26 RADAR LUMBAQUI
27 BS-55
28 BS-56
29 BS-57
30 BOES-54

El proyecto se realizará en base a etapas que permitirán asegurar la viabilidad técnica del proyecto:

- Situación Actual
- Requerimientos del Usuario
- Diseño de la Red MPLS
- Selección de Equipos y Servicios MPLS
- Simulación de la Topología y Servicios MPLS
- Elaboración de Documentos Precontractuales (Bases Técnicas Anexo "B")
- Implementación y Pruebas de la Red MPLS

4.2 VIABILIDAD ECONÓMICA Y FINANCIERA

4.2.1 Viabilidad Económica

Por razones económicas, el proyecto se lo implementará en tres (3) fases, comenzando en el año 2015, de la siguiente manera:

ITEM	DESCRIPCIÓN	CANTIDAD	OBJETIVOS
I-FASE	EQUIPOS CORE	6	1. IMPLEMENTAR LA NUBE MPLS EN LA RED.
	EQUIPOS DE DISTRIBUCIÓN	6	2. MIGRAR LOS COMANDOS OPERACIONALES COMO RESPONSABILIDAD DIRECTA DEL COMACO.
	EQUIPO USUARIO	5	3. INTEGRAR Y CONVERGER LOS SERVCIOS DE LOS COMANDOS

CONTINÚA ⟶

			OPERACIONALES.
	INSTALACIÓN Y CONFIGURACIÓN.	LOTE	
	CAPACITACIÓN	LOTE	
			USD 1´201500.00
II-FASE	EQUIPOS DE DISTRIBUCIÓN	7	1. COMPLETAR LA CAPA DE DISTRIBUCIÓN 3. COMPLETAR EQUIPO DE USUARIO DETALLADA EN EL NUMERAL 4.1
	EQUIPO USUARIO	25	
	INSTALACIÓN Y CONFIGURACIÓN	LOTE	
	SOPORTE TÉCNICO	LOTE	
	TOTAL		**USD 623500.00** **USD 1825000.00**

4.2.2. Supuestos utilizados

Para atender la demanda de comunicaciones de las Fuerzas, es necesario que la red de transporte incremente su capacidad de enlaces como base los siguientes valores:

ANILLO	**CAPACIDAD**
CENTRAL	879.61 MBPS
NORTE	189.98 MBPS
OESTE	645.33 MBPS
SUR	182.35 MBPS

4.2.3 Identificación, cuantificación y valoración de costos y beneficios.

El detalle del valor de USD 1´775000.000, para las dos fases del proyecto, corresponden al año 2015 y 2016, se presenta en el siguiente cuadro:

ITEM	**DESCRIPCIÓN**	**CANTIDAD**	**PRECIO UNITARIO USD**	**PRECIO TOTAL USD**
FASE I: EQUIPOS				
1	ROUTER MPLS LSR	6	95.000,00	570.000,00
2	ROUTER MPLS LER	6	48.000,00	288.000,00
3	ROUTER CE	5	6.700,00	33.500,00

CONTINÚA ⟶

INSTALACIÓN Y CONFIGURACIÓN: INCLUYE				
1	UPS	10	6.000,00	60.000,00
2	RACK	12	1.500,00	18.000,00
3	MULTIPLEXORES INVERSOS	20	1.000,00	20.000,00
4	INSTALACIÓN Y CONFIGURACIÓN	Lote	180.000,00	200.000,00
CAPACITACIÓN				
1	TRANSFERENCIA TECNOLÓGICA	Lote	110.000,00	110.000,00
FASE II: EQUIPOS				
1	ROUTER MPLS LER	7	48000,00	336000,00
2	ROUTER CE	25	6700,00	167500,00
3	INSTALACIÓN Y CONFIGURACIÓN	LOTE	100000,00	100000,00
4	SOPORTE TÉCNICO	LOTE	20000,00	20000,00
			SUB-TOTAL	1825000,00
			12% IVA	219000,00
			TOTAL USD	**2´044.000,00**

5.- PRESUPUESTO:

El proyecto estará financiado por el Ministerio de Defensa Nacional, como proyecto de inversión como componente del proyecto macro de Mando y Control en el fortalecimiento de las capacidades operativas de Fuerzas Armadas.

5. ESTRATEGIA DE EJECUCIÓN

5.1. Estructura Operativa

La Dirección de Tecnologías de la Información y Comunicaciones, a través del Departamento de Telecomunicaciones, serán los encargados de realizar el monitoreo y seguimiento de la ejecución.

A pesar de que la ejecución directa estará a cargo de la empresa que proveerá los equipos, los técnicos del Comando Conjunto participarán durante todo el proceso de instalación, configuración y puesta a punto de la red MPLS, para lo cual la capacitación será una actividad que se desarrolle al inicio de la contratación.

6.- ESTRATEGIA DE SEGUIMIENTO Y EVALUACIÓN

6.1. Monitoreo de la ejecución.

El Gerente técnico del contrato y una comisión encargada de la Entrega-Recepción, serán los responsables de realizar el seguimiento del cumplimiento del cronograma de actividades a realizarse durante toda la ejecución, comunicando a través de informes el avance y cumplimiento de las obligaciones, de conformidad a la oferta y a las especificaciones técnicas solicitadas en el contrato.

6.2. Evaluación de resultados e impactos

El departamento/sección de evaluación y control, es el organismo encargado de evaluar las metas alcanzadas en base a los indicadores descritos en la Matriz de Marco Lógico.

Cristian Arias.
MAYO. TÉC. AVC.
JEFE DE CONECTIVIDAD.

APÉNDICE "A"

MATRIZ DE MARCO LOGICO

CONCEPTO	INDICADORES	MEDIOS DE VERIFICACION	SUPUESTOS
FIN:			
Contribuir con el proceso de fortalecimiento de la capacidad operativa de Fuerzas Armadas.	Al finalizar el 2016, la Red de datos mejorará tecnológicamente en un 90%.	Reportes de gestión con disminución de problemas en la integración de servicios.	Asignación oportuna de los recursos y en la cantidad solicitada. Agilidad en el proceso de contratación en Bienes Estratégicos

PROPOSITO:			
Reestructurar la red de datos de Fuerzas Armadas, mediante la implementación de equipos con tecnología MPLS, para proporcionar servicios de voz, datos y video a nivel nacional, con capacidad de soportar el crecimiento, integración y convergencia de los servicios.	Al terminar la ejecución del proyecto los servicios y aplicaciones de las unidades de Fuerzas Armadas estarán integrados en una única plataforma de tecnología MPLS, siendo atendidos en un 80% de sus requerimientos de comunicaciones en voz, datos y video.	Informes de satisfacción de los servicios de comunicaciones por parte de las Unidades Militares.	Implementación paralela del incremento de capacidad en los anillos laterales de la red. Las unidades militares no consideradas en el proyecto se integrarán con equipos CE´s mediante proyectos de las Fuerzas Migración de las centrales telefónicas de todas las unidades a tecnología IP.
COMPONENTES:			
Implementación del CORE de la Red MPLS	Transcurridos 90 días del plazo del contrato, se contará con 6 equipos LSR en	Informe de ejecución y	Disponibilidad de capacidad en la

	la red.	cumplimiento de protocolos técnicos de recepción de equipos.	red de transporte PDH/SDH.
Instalación de la capa MPLS de Distribución	Al cabo de 120 días del contrato, se dispondrá de 13 equipos LER en los anillos y ramales de la red.	Pruebas en función de protocolos técnicos	Disponibilidad de capacidad en los ramales de la red.
Integración de equipos de usuario a la red	Al final del plazo de ejecución de 180 días, se migrará el servicio de datos, en las 30 unidades militares de Fuerzas Armadas.	Acta entrega-recepción parcial	Capacidad de los enlaces de última milla en las unidades militares.
Transferencia tecnológica por parte del fabricante	En un plazo de 60 días, se contará con 10 técnicos capacitados para que participen en la instalación, configuración y posteriormente en la gestión de la red MPLS.	Informe de cumplimiento de la capacitación y certificados correspondientes.	Contar con las autorizaciones respectivas para asistir al entrenamiento en fábrica.
ACTIVIDADES:			
Adquisición de ROUTER MPLS CORE LSR	570.000,00	GPR	
Adquisición de ROUTER MPLS EDGE LER	624.000,00	GPR	
Adquisición de ROUTER TIPO CE	201.000,00	GPR	

Instalación y Configuración	300.000,00	GPR	
Capacitación	110.000,00	GPR	
Soporte Técnico	20.000,00	GPR	
	TOTAL USD: 1´825.000,00		

ANEXO E "ESPECIFICACIONES TÉCNICAS"

ESPECIFICACIONES TÉCNICAS

ADQUIRIR E IMPLEMENTAR DE EQUIPOS CON TECNOLOGÍA MPLS, PARA PROPORCIONAR SERVICIOS DE VOZ, DATOS Y VIDEO A NIVEL NACIONAL, CON CAPACIDAD DE SOPORTAR EL CRECIMIENTO, INTEGRACIÓN Y CONVERGENCIA DE LOS SERVICIOS.

ROUTER MPLS LSR **CANTIDAD: 6**

DESCRIPCIÓN	CARACTERÍSTICAS
Marca	Especificar
Modelo	Especificar
Año de fabricación	Mínimo 2012 (presentar certificado)
Tipo de equipo	Router - ASR
Fiabilidad (reliability)	Carrier-class
Tecnología	MPLS
Sistema Operativo	Cisco IOS XR
Chassis	A instalarse en rack 19"
Número de Slots	Mínimo 6: ➢ 2 para instalar tarjetas de procesadores ➢ Slots restantes para tarjetas de línea
Interfaces Soportadas	E1, E3, STM-1, STM-4, STM-16, STM-64, 1GE, 10GE, 40GE, 100GE
Puertos de servicio requeridos	Mínimo 20:

	➢ 16 puertos 10/100/1000 base T (RJ-45) ➢ Puertos restantes SFP
Puertos de Gestión	Mínimo 4 puertos: ➢ 2 puertos 100/1000 ➢ 1 puerto de consola ➢ 1 puerto auxiliar
Memoria RAM	Mínimo 6 GB
Versión del software	Última versión liberada por el fabricante (Presentar certificado)
Temperatura de operación	5 ^{o}C a 40 ^{o}C o superior
Alimentación	220 Vac, 60 hz
Certificación Metro Ethernet Forum	El equipo debe contar con la certificación MEF 2.0 (Presentar certificado)
FUNCIONALIDADES	
Protocolos de enrutamiento	OSPF, BGP, IS-IS, RIPv2, RPL, HSRP, VRRP
MPLS	Mínimo: ➢ MPLS QoS ➢ MPLS VPN (L2VPN, L3VPN) ➢ MPLS TE (FRR , RSVP) ➢ Multisegment Pseudowire ➢ LDP, T-LDP ➢ 6Vpe
Ethernet	Ethernet Virtual Connections, Traducción Flexible de VLANs, Clasificación Flexible de VLANs, IEEE bridging, IEEE 802.1s MST
Calidad de servicio	WRED, CBWFQ, Priority Queuing, MQC, Políticas 2R3C, Calidad de Servicio Jerárquico de 4 niveles (H-QoS), Diffserv
Multicast	Mínimo: PIM-SM, PIM-SSM, Auto RP, Multiprotocol BGP, Multicast VPN, MSDP, IGMPv2 y v3
Administración	CLI, Telnet, SNMP, XML, SSH, FTP, TFTP, Syslog

OAM	IEEE 802.1ag CFM, IEEE 802.3ah Link OAM, MPLS OAM, LSP Ping, LSP Traceroute, ITU-T Y.1731, Virtual Circuit Connectivity Verification
Seguridad	ACL capa 2/capa 3, AAA, TACACS+, SSH, 802.1ad L2CP, MAC limiting por EVC o Bridge Domain, Storm-Control Blocking, Unknown Unicast Flood Blocking, DHCP snooping, Unicast Reverse Path Forwarding, Control-Plane security, Dynamic ARP inspection, IP Source Guard
Sincronismo	Sistemas de Referencia BITS, DTI, PTP o IEEE 1588-2008 mediante puerto dedicado, Interfaces ToD de 10MHz y 1-pps, SyncE
Multi Chasis	El equipo podrá: ➢ Funcionar en configuración Cluster con otro equipo similar ➢ Utilizar equipos remotos como tarjetas adicionales del equipo.
ESCALABILIDAD	
Número de Rutas	Mínimo: 4’000.000 (IPv4); 2’000.000 (IPv6)
Rutas Multicast	Mínimo 128.000
MAC Addresses	Mínimo 2’000.000
Pseudowires VPLS	Mínimo 128.000
Pseudowires VPWS	Mínimo 128.000
VPN capa 3 (VRF)	Mínimo 8.000
Número de Colas	Mínimo 256.000 por tarjeta
Número de Políticas	Mínimo 256.000 por tarjeta
Rendimiento Soportado	>= 3,5 Tbps
ALTA DISPONIBILIDAD	
Protocolos Soportados	MPLS TE-FRR, BFD, 802.3ad Link Aggregation

	Bundles, Non Stop Forwarding, Non Stop Routing, Multi Chassis LAG
Redundancia soportada	En procesamiento, para implementarse a corto plazo
Redundancia instalada	En alimentación y ventiladores
Soporte SMARTNET	8X5XNBD, para el chassis, tarjetas de procesamiento, tarjeta de línea y software

ROUTER MPLS LER CANTIDAD: 13

DESCRIPCIÓN	CARACTERÍSTICAS
Marca	Especificar
Modelo	Especificar
Año de fabricación	Mínimo 2012 (presentar certificado)
Tipo de equipo	Router - ASR
Fiabilidad (reliability)	Carrier-class
Tecnología	MPLS
Sistema Operativo	Cisco IOS XE
Chassis	A instalarse en rack 19”
Número de Slots	Mínimo: ➢ 6 para instalar interfaces ➢ 2 para instalar procesadores
Interfaces Soportadas	E1, STM-1, STM-4, 10/100/1000 RJ-45, Gigabit Ethernet Optico, 10 Gigabit Ethernet
Puertos requeridos	>= 16 puertos 10/100/1000 base T (RJ-45)
Puertos de Administración	10/100/1000 (RJ-45), Consola (RJ-45 / RS232 serial), Console – USB 2.0 type A

Memoria RAM	Mínimo 4GB
Versión del software	Última versión liberada por el fabricante (presentar certificado)
Temperatura de operación	0 ^{o}C a 40 ^{o}C o superior
Alimentación	115 Vac, 60 hz
FUNCIONALIDADES	
Características MPLS soportadas	➢ LDP ➢ EoMPLS ➢ MPLS VPN ➢ MPLS TE-FRR ➢ MPLS-TP ➢ VPLS ➢ VPWS ➢ CESoPSN Pseudowires ➢ SAToP Pseudowires ➢ Multisegment Pseudowires
Protocolos de enrutamiento	OSPF, BGP, IS-IS, VRRP, BFD, ECMP
Calidad de servicio	H-QoS, WRED, CBWFQ, CoS, Tos, MQC, DSCP, Classification using ACL, 2R3C, Priority Queueing, Eggress Shaping, Eggress Policing, RSVP, Call Admision Control.
Ethernet	Selective QinQ, IEEE 802.1s MST, VLAN Local Significance, Trunk EFP, 802.3ad/ 802.3ax LACP L2PT, Static Multicast MAC Address, Link Pass Through
Seguridad	ACL, AAA, TACACS+, SSH, DHCP snooping, Dynamic ARP Inspection, MAC Security, Unicast Reverse Path Forwarding, MAC Limiting per Bridge Domain.
Multicast	Mínimo: PIM-SM, PIM-SSM, PIMv2, IGMPv2, IGMPv3, IGMP Group Limiting

IPv6	Ipv4 and Ipv6 dual stacking, Ipv6 static routing OSPF for Ipv6, DHCPv6, 6PE, 6VPE
Administración	SNMP, CLI, Port level local SPAN, Network Virtualization
OAM	IEEE 802.1ag CFM, IEEE 802.3ah Link OAM, MPLS OAM, ITU-T Y.1731, E-LMI
Sincronismo	BITS, ToD, SyncE, IEEE 1588-2008
ESCALABILIDAD	
Rendimiento en paquetes por segundo	>=65 Mpps
Rendimiento en bits por segundo	Mínimo 55 Gbps
Direcciones Mac	Mínimo 256.000
Ethernet flow points	Mínimo 8.000
Interfaces L3	Mínimo 4.000
Número de rutas	Mínimo: 80.000 (IPv4); 40.000 (IPv6)
Rutas Multicast	Mínimo 8.000
Túneles EoMPLS por sistema	Mínimo 8.000
MPLS VPN	Mínimo 2.000
Etiquetas MPLS	Mínimo 32.000
VPLS	Mínimo 4.000
Gestión de colas	Mínimo 32.000
Contadores de cola (paquetes y bytes)	Mínimo 128.000
ALTA DISPONIBILIDAD	

Redundancia soportada	En procesamiento, para implementarse a corto plazo
Redundancia instalada	En alimentación
Soporte SMARTNET	8X5XNBD, para el chassis, tarjetas de procesamiento, tarjeta de interfaces y software

ROUTER TIPO CE **CANTIDAD: 30**

DESCRIPCIÓN	CARACTERISTICAS
Marca	Especificar
Modelo	Especificar
Tipo de equipo	Router – ISR G2
Sistema operativo	Cisco IOS
Chassis	A instalarse en rack 19”
Número de slots	Mínimo 4, para instalar tarjetas EHWIC
Puertos requeridos	Mínimo: ➢ Tres (3) puertos 10/100/1000 Base T (RJ-45) ➢ Dos (2) puertos USB ➢ Un puerto de Consola
Rendimiento en bits por segundo	Mínimo 50 Mbps
Memoria	Mínimo: ➢ RAM: 512 MB ➢ FLASH: 256 MB
Versión del software	Última versión liberada por el fabricante (presentar certificado)

Procesador	Multi-core
Protocolos de enrutamiento	OSPF, BGP, IS-IS, EIGRP, otros
Calidad de servicio QoS	ACL, LLQ, DSCP, CBWFQ, WRED, otros
Seguridad	ACL, NAT, AAA, Radius, PAP, CHAP, IPSec, SSL, L2TPv3, VPN
Redundancia	VRRP, otros
Multicast	PIM-SM, PIM-SSM, otros
Configuración	Telnet, Secure Shell o Rlogin, SNMP, SSH, RMON
Alimentación	115 Vac, 60 hz

INSTALACIÓN Y CONFIGURACIÓN: INCLUYE:

MULTIPLEXOR INVERSO CANTIDAD: 20

DESCRIPCIÓN	CARACTERISTICAS
Operación	Multiplexor de E1´s a Ethernet
Puertos E1´s	Mínimo 16 puertos G.703 BNC (75 ohmios)
Puerto Ethernet	Mínimo un puerto 10/100 base T (RJ 45), auto negociable
Puertos auxiliares	Mínimo un puerto 10 base T y RS-232 para gestión
Alimentación	115 Vac

RACK CERRADO

DESCRIPCIÓN	CARACTERISTICAS
Tipo	Gabinete metálico cerrado de 19”
Altura	42U (estándar)
Profundidad	La necesaria para instalar los equipos MPLS y CE.
Tipo de puerta	Puerta frontal con seguridad
Accesos laterales	Si
Tomas de alimentación	Mínimo 12 de 115 Vac
Ventiladores	Los necesarios para mantener refrigerado el interior a plena carga (en caso de utilizar todo el rack con equipos activos)
Accesorios que incluye:	Columna soportante de acero con anillos organizadores para patch cords y cables.

SISTEMA ININTERRUMPIDO DE ENERGÍA UPS CANTIDAD: 10

DESCRIPCIÓN	CARACTERISTICAS
Marca	Especificar
Modelo	Especificar
Potencia	6 KVA

Tecnología	Float charging
Tiempo de autonomía	Mínimo 60 minutos a media carga
Tipo de baterías	Libres de mantenimiento
Rango del Voltaje de Entrada	200-240 Vac (a 25%, 50%, 75% y 100% de carga)
Voltaje de salida nominal	220/240 Vac
Regulación del Voltaje de Salida	+/-2% en línea; +/-3% en modo batería
Protecciones	Sobrecarga, ruido, otros
Factor de Potencia de Entrada	≥ 0.99
Eficiencia	>90% (modo Online)
Puertos de comunicación	RS-232 y USB
Temperatura de operación	0 ^{o}C a 40 ^{o}C o superior

NOTA:	Se deberá adjuntar catálogos o data sheet de todos los equipos, para verificar el cumplimiento de los parámetros solicitados, para lo cual, se añadirá en la oferta una columna y en cada característica se indicara el número de la página donde se encontrará resaltada la información. Todas las funcionalidades solicitadas, deberán estar incluidas con su respectiva licencia.

OTROS

PRUEBAS DE FUNCIONALIDAD	Como parte de la recepción del objeto de contrato, se realizarán pruebas del correcto funcionamiento de los equipos y la verificación de las especificaciones solicitadas en los pliegos, las mismas que se efectuaran en el CAE-Quito. Al contratista se le proporcionará la topología con la que se probará las funcionalidades MPLS. La instalación será en sitio en base a lo establecido en el Anexo A, para lo cual la empresa asumirá todos los gastos de transporte, material de instalación (cables requeridos); así como el material eléctrico para la alimentación de los equipos adquiridos. Para compaginar la alimentación de los equipos ofertados (115 o 220 Vac), con la existente en las repetidoras de la red, es responsabilidad del oferente visitar los sitios para corroborar el tipo de energía requerida y que será la alimentación correcta que se oferte en cada equipo.
PLAZO DE ENTREGA	El plazo máximo para la entrega del objeto del contrato, será de noventa (120) días calendario, a partir de la entrega del anticipo.
FORMA DE PAGO	El pago se realizará de la siguiente manera: • 50% a la firma del contrato. • 50% con la firma del acta entrega-recepción
GARANTÍA TÉCNICA	Mínimo de dos años para todos los equipos ofertados.
PROVISIÓN DE REPUESTOS	Al menos por 5 años, periodo durante el cual, se deberá proveer soporte y repuestos para los equipos MPLS y CE.
CAPACITACIÓN	Para 10 técnicos del Departamento de Telecomunicaciones, mediante temario de un curso oficial en la tecnología MPLS

	vigente en los cursos regulares de la marca ofertada. Este curso y temario será aprobado por el Departamento de Telecomunicaciones previa ejecución del mismo.
SOPORTE TÉCNICO	De al menos 60 horas con técnico local certificado por la empresa en soluciones de networking, especialmente en la tecnología MPLS. Además de acceso on-line a soluciones de problemas actualizaciones en versiones de software por técnicos de fábrica durante un año desde la firma del acta de entrega-recepción.

REQUISITOS A CUMPLIR EL OFERENTE

Certificados a presentar con la oferta	1. Que los Routers MPLS y CE ofertados y que se instalarán como parte del contrato, serán producción mínimo año 2013 (Del Fabricante). 2. Que los modelos de los Routers MPLS y CE ofertados, no estén descontinuados y que tendrán vigencia en el mercado de al menos cinco (5) años, periodo en el cual existirá soporte y provisión de repuestos de manera ininterrumpida (Del Fabricante). 3. Certificación Metro Ethernet Forum de los equipos MPLS (Del Fabricante). 4. Que la versión del software de los equipos MPLS, sea la última liberada por el fabricante (Del Fabricante). 5. Que el oferente debe ser canal autorizado por el fabricante para manejar proyectos de la marca en territorio ecuatoriano (Del Fabricante) 6. Que el oferente cuente con especialización avanzada en Switching y Routing, además deberá adjuntar al menos una certificación CCIP de uno de los ingenieros asignados al proyecto (De la Empresa). 7. Que el oferente tenga experiencia en el manejo de

	proyectos con equipos MPLS en el país (De la Empresa). 8. De las inspecciones realizadas a los sitios, para verificar el tipo de alimentación que requieren los equipos ofertados (De la Empresa)

Cristian Arias.
MAYO. TÉC. AVC.
JEFE DE CONECTIVIDAD.