ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN SISTEMAS

"ANÁLISIS DEL PROTOCOLO DIFFSERV APLICADO A LA PROVISIÓN DE QOS EN EL TRÁFICO DE VIDEOLLAMADAS SOBRE REDES INALÁMBRICAS CON EQUIPOS CISCO Y LINUX"

TESIS DE GRADO

Previo a la obtención del título de:

INGENIERA EN SISTEMAS INFORMÁTICOS

Presentado por:

XIMENA ALEXANDRA QUINTANA LÓPEZ

LIGIA ELENA CASTELO TUMAILLE

Riobamba – Ecuador
2012

Queremos agradecer a nuestro Director de Tesis, Ing. Alberto Arellano y al Ing. Danilo Pastor, por el tiempo brindado a este tema de investigación además porque sus conocimientos y orientaciones han constituido un gran apoyo y guía durante el periodo de tiempo que ha durado el desarrollo de ésta tesis.

A los dos ángeles de mi vida, a mi abuelita Zoila y a la memoria de mi abuelito Arturo quiero dedicar todo el sacrificio de este trabajo de investigación, por ser los dos mi ejemplo de valentía, capacidad, generosidad y amor.

A mis padres Bolívar y Nancy por su amor, apoyo y comprensión pero sobre todo por enseñarme lo que significa la perseverancia y constancia y haber permanecido a mi lado inamovibles siendo el motor que ha impulsado alcanzar esta meta.

A mi hermana Lorena y a mis sobrinos Anthony y Antonella por su inmenso amor y por ser las tres más grandes bendiciones de mi vida.

A mi familia y amigos por haber sido un apoyo constate durante toda mi vida

Ximena Alexandra

La tesis la dedico a Dios por haberme guiado por el camino correcto y haberme bendecido para culminar esta etapa de mi vida y a toda mi familia especialmente a mis padres y hermano que siempre confiaron en mí pese a las dificultades y me dieron el apoyo incondicional para alcanzar todas mis metas.

A Silvia y Aida por bendecirme desde el cielo y no abandonarme ni un solo instante de mi vida.

A Carlitos y Tiffany quienes a su corta edad siempre me llenaron amor, bendiciones y alegrías.

Ligia Elena

FIRMAS DE RESPONSABLES Y NOTAS

	FIRMA	**FECHA**
Ing. Iván Menes **DECANO FACULTAD** **INFORMÁTICA** **Y ELECTRÓNICA**	_____	_____
Ing. Raúl Rosero **DIRECTOR DE LA ESCUELA** **DE INGENIERÍA EN SISTEMAS**	_____	_____
Ing. Alberto Arellano **DIRECTOR DE TESIS**	_____	_____
Ing. Danilo Pastor **MIEMBRO DEL TRIBUNAL**	_____	_____
Tlgo. Carlos Rodríguez **DIRECTOR CENTRO DE** **DOCUMENTACIÓN**	_____	_____

“Nosotras, Ximena Alexandra Quintana López y Ligia Elena Castelo Tumaille somos las responsables de las ideas, doctrinas y resultados expuestos en esta Tesis de Grado y el patrimonio intelectual de la misma pertenecen a la ESCUELA SUPERIOR POLITÉCNICA DE CHMBORAZO**”.**

_____

Ximena Alexandra Quintana López

_____

Ligia Elena Castelo Tumaille

ÍNDICE GENERAL

PORTADA

AGRADECIMIENTO

DEDICATORIA

FIRMAS RESPONSABLES

RESPONSABILIDAD DEL AUTOR

ÍNDICE GENERAL

ÍNDICE ABREVIATURAS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

CAPÍTULO I

1. MARCO REFERENCIAL....18

1.1. ANTECEDENTES....18
1.2. JUSTIFICACIÓN DEL PROYECTO DE TESIS....20
1.2.1 JUSTIFICACIÓN TEÓRICA....20
1.2.2 JUSTIFICACIÓN PRÁCTICA....21
1.3. OBJETIVOS....25
1.3.1 Objetivo General....25
1.3.2 Objetivo Específicos....25
1.4. HIPOTESIS....26

CAPÍTULO II

2. REDES INALAMBRICAS....27

2.1. INTRODUCCIÓN A REDES INALÁMBRICAS....27
2.1.1. ¿Qué es una Red Inalámbrica?....27
2.1.2. Ventajas de las Redes Inalámbricas....27
2.1.3. Desventajas de las Redes Inalámbricas....29
2.1.4. WLAN (Wireless Local Área Network, Redes de Área Local Inalámbrica)....30
2.1.5. Estándares de las Redes Inalámbricas....30
2.1.6. QoS (Quality of Service, Calidad de Servicio)....35
2.1.7. Parámetros de rendimiento....36
2.1.7.1. Retardo....36
2.1.7.2. Jitter....37
2.1.7.3. Pérdida de Paquetes....38
2.1.7.4. Ancho de banda....38
2.1.8. AP (Access Point, Punto de Acceso)....39
2.1.9. AP (Access Point, Punto de Acceso)....40

2.1.10. WLAN Controller *42*
2.2. PROTOCOLO DIFFSERV 43
2.2.1. Introducción al Protocolo Diffserv *43*
2.2.2. Modelo de la arquitectura Differentiated Services *44*
2.2.2.1. Dominio de los Servicios Diferenciados (Dominio DS) 44
2.2.2.1.1. Nodos DS de frontera e interiores 46
2.2.2.1.2. Nodos de Ingreso y Egreso 47
2.2.2.2. Región de servicios Diferenciados (Región DS) 47
2.2.2.3. Clasificación y Acondicionamiento del tráfico en un dominio DS 48
2.2.2.3.1. Clasificadores 49
2.2.2.3.2. Perfiles de Tráfico 49
2.2.2.3.3. Acondicionador de Tráfico 49
2.2.2.3.3.1. Medidior 50
2.2.2.3.3.2. Marcador 50
2.2.2.3.3.3. Conformador 50
2.2.2.3.3.4. Despachador 50
2.2.2.3.4. Ubicación de los acondicionadores de tráfico o clasificadores MF 51
2.2.2.3.4.1. Dentro del dominio origen 51
2.2.2.3.4.2. En la Frontera de un Dominio DS 52
2.2.2.3.4.3. Dominios que no soportan Diffserv 52
2.2.2.3.4.4. En nodos DS interiores 52
2.2.3. Definición del campo Differentiated Services (DIFFSERV) *53*
2.2.3.1. Comportamiento por salto (Per-Hop-Behavior, PHB) 55
2.2.3.1.1. PHB por Defecto (Default PHB) 57
2.2.3.1.2. Selector de Clase PHB (Class Selector PHB) 58
2.2.3.1.3. PHB Tránsito Expedito (Expedited forwarding) 58
2.2.3.1.3.1. Descripción del PHB Tránsito Expedido 60
2.2.3.1.3.2. Mecanismos de ejemplo para implementar el PHB Tránsito Expedito 61
2.2.3.1.3.3. Consideraciones de Seguridad 61
2.2.3.1.4. PHB Tránsito Asegurado (Assured Forwarding) 62
2.2.3.1.4.1. Acciones de Condicionamiento de Tráfico 63
2.2.3.1.4.2. Comportamiento de colas y descarte de paquetes 63
2.2.3.1.4.3. Algoritmo RED 64
2.2.3.1.4.4. Consideraciones de Seguridad 66
2.3. EL PROTOCOLO DIFFSERV BAJO EL SISTEMA OPERATIVO LINUX 67
2.3.1. INTRODUCCIÓN *67*
2.3.2. Flujo de tráfico en el sistema operativo Linux *68*
2.3.2.1. Mecanismos de interconexión del sistema operativo linux 69
2.3.2.2. Control de tráfico en el sistema operativo Linux 70
2.3.2.2.1. Elementos del control del tráfico en sistema operativo Linux 74
2.3.2.2.1.1. Conformado (Shaping) 74
2.3.2.2.1.2. Calendarizador (Scheduling) 75
2.3.2.2.1.3. Clasificador (Classifying) 75
2.3.2.2.1.4. Políticas (Policing) 75
2.3.2.2.1.5. Descartador (Dropping) 75
2.3.2.2.1.6. Marcador (Marking) 76

CAPÍTULO III

3. IMPLEMENTACIÓN DE LOS PROTOTIPOS DE PRUEBA 77

3.1. INTRODUCCIÓN 77
3.1.1. Características de los equipos *77*
3.2. ESTRUCTURA DE LA WLAN 81
3.2.1. Configuración de QoS en los Equipos Cisco *82*
3.2.1.1. Guias de Implementación 82
3.2.2. Configuración de QoS en los Equipos Linux *89*
3.2.2.1. Guias de Implementación 100

INSTALAR VSFTPD EN CENTOS.....145

CAPÍTULO IV

4. ANÁLISIS Y EVALUACIÓN FINAL DE RESULTADOS.....152

4.1. MARCO METODOLÓGICO.....152
4.1.1. Diseño de la investigación.....152
4.1.2. Métodos, Técnicas e Instrumentos.....153
4.1.3. Instrumentos:.....155
4.1.4. Validación de los instrumentos.....155
4.1.5. Procesamiento de la información.....155
4.1.6. Planteamiento de la Hipótesis.....157
4.1.7. Determinación de las variables.....157
4.1.8. Operacionalización Conceptual de las Variables.....158
4.1.9. Operacionalización Metodológica de las Variables.....158
4.1.10. Población y Muestra.....159
4.2. ANÁLISIS, COMPARACIÓN E INTERPRETACIÓN DE RESULTADOS.....159
4.2.1. Determinación de parámetros de comparación.....159
4.2.2. Resultados.....160
4.2.3. Comprobación de la Hipótesis de la investigación realizada.....197

CONCLUSIONES

RECOMENDACIONES

RESUMEN

SUMMARY

GLOSARIO

ANEXOS

BIBLIOGRAFÍA

ÍNDICE DE ABREVIATURAS

AF: Assured Forwarding,

AP: Access Point, Punto de Acceso

ASCII: American Standard Code for Information Interchange, Código Estándar Estadounidense para el Intercambio de Información

BA: Behavior Agregate, Comportamiento Agregado

BSS:,Conjunto de servicio básico, Basic Service Set

BSSID: Basic Service Set Identifier, Identificador de Servicio Básico

CBQ: Class Based Queue, Cola basada en Clase

CCK: Complementary Code Keying, Código de llaves complementario

CSMA/CA: Carrier Sense Multiple Access/Collision Detect, Múltiple acceso por detección de portadora evitando colisiones

DIFFSERV: Differentiated Services, Servicios Diferenciados

DSCP: Differentiated Services Code Point, Punto de Código de Servicio Diferenciado

DNS: *Domain Name System,* Sistema de Nombres de Dominio

ESS: *Extended Service Set, Conjunto de servicio extendido*

ESSID: Service Set Identifier Extended, Identificador del conjunto de servicio extendido

HCCA: Controlled Channel Access, Canal de Acceso Controlado

IEEE: Institute of Electrical and Electronics Engineers, Instituto de Ingenieros Eléctricos Electrónicos

LAN: Local Área Network, Red de área local

MTU: Maximum Transfer Unit , Unidad, Máxima de Transferencia

NIC: Network Interface Card, Tarjeta de interfaz de red

OFDM: Orthogonal Frecuency Division Multiplexing, División de Frecuencias ortogonales Multiplexadas

PBCC: Packet Binary Convolution Coding, Codificación convolucional binaria en paquetes

PHB: Per hop behavior, Comportamiento por salto

QoS: Quality of Service, Calidad de Servicio

RADIUS: Remote Authentication Dial-In User Server, Acceso telefónico de autenticación remota del servidor del usuario

SLA: Service Level Agreement, Acuerdo de Nivel de Servicio

TCP: *Transmission Control Protocol*, Protocolo de Control de Transmisión

UDP: User Datagram Protocol, Protocolo de datagramas de usuario

ToS: Type of Service, Tipo de Servicio

UNII: Unlicensed National Information Infrastructure, Infraestructura de Información Nacional sin licencia

WECA: Wireless Ethernet Compatibility Alliance, Alianza de Compatibilidad Ethernet Inalámbrica

WDS: Wireless Distribution System, Sistema de Distribución Inalámbrico

WLAN: Wireless Local Área Network, Red de área local inalámbrica

WPA: Wifi Protect Access, Acceso Wi-Fi protegido

ÍNDICE DE FIGURAS

FIGURA I.01 ESCENARIO DE PRUEBAS 1(CISCO) 22
FIGURA I.02 ESCENARIO DE PRUEBAS 2(LINUX) 23
FIGURA II.03 CONJUNTO DE SERVICIOS BÁSICO (BSS) 40
FIGURA II.04 CONJUNTO DE SERVICIO EXTENDIDO (ESS) 41
FIGURA II.05 CONJUNTO DE SERVICIO BÁSICO INDEPENDIENTE O IBSS 42
FIGURA II.06 TARJETA WLAN CONTROLLER (NME-AIR-WLC8-K9) 42
FIGURA II.07 DOMINIO DIFFSERV 45
FIGURA II.08 DIFFSERV – SERVICE LEVEL AGREEMENT 45
FIGURA II.09 ARQUITECTURA DE NODOS DS INTERIORES 46
FIGURA II.10 REGIÓN DIFFSERV 48
FIGURA II.11 VISTA LÓGICA DE UN CLASIFICADOR Y UN ACONDICIONADOR DE PAQUETES 48
FIGURA II.12 CAMPO TOS DE IPV4 53
FIGURA II.13 CAMPO TC DE IPV4 53
FIGURA II.14 CAMPO DS 54
FIGURA II.15 IMPLEMENTACIÓN DEL EF PHB CON EL PHB POR DEFECTO 59
FIGURA II.16 MODELADO Y DESCARTE DE PAQUETES 60
FIGURA II.17 ALGORITMO RED 65
FIGURA II.18 SERVICIO OLÍMPICO 65
FIGURA II.19 DIAGRAMA DE BLOQUES DE INTERCONEXIÓN ENTRE EL SISTEMA OPERATIVO LINUX Y LA RED FÍSICA 68
FIGURA II.20 DIAGRAMA DE BLOQUES DE UN COMPUTADOR CON DOS TARJETAS DE RED 69
FIGURA II.21 PROCESO DE INGRESO Y SALIDA DE PAQUETES EN LA RED 69
FIGURA II.22 PROCESAMIENTO DE DATOS DE RED 71
FIGURA II.23 RUTA DE LOS PAQUETES A TRAVÉS DE LINUX 71
FIGURA II.24 DISCIPLINA DE COLA SIMPLE SIN CLASES 72
FIGURA II.25 DISCIPLINA DE COLA SIMPLE CON MÚLTIPLES CLASES 72
FIGURA II.26 RELACIÓN DE LOS ELEMENTOS DE LA ARQUITECTURA DIFFSERV CON EL CONTROL DE TRÁFICO DEL KERNEL DE SISTEMA OPERATIVO LINUX 74
FIGURA III.27 PLACA FRONTAL DEL MÓDULO DE RED DE CISCO WIRELESS LAN CONTROLLER 83
FIGURA III.28 PING DEL ROUTER A LA ADMINISTRACIÓN WLCM 88
FIGURA III.29 PING A LA DIRECCIÓN CONFIGURADA 89
FIGURA III.30 FIRMWARE DD-WRT 91
FIGURA III.31 EXTRACCIÓN DEL ARCHIVO 91
FIGURA III.32 INGRESO DE IP DEL ROUTER Y PASSWORD 92
FIGURA III.33 INGRESO DE CONTRASEÑA 92
FIGURA III.34 INGRESO AL MÓDULO DE ADMINISTRACIÓN 92
FIGURA III.35 ACTIVACIÓN DE "FACTORY DEFAULTS". 93
FIGURA III.36 GUARDAR CAMBIOS 93
FIGURA III.37 INGRESO AL ROUTER CON EXPLORADOR DE INTERNET 94
FIGURA III.38 INTERFACE WEB DEL ROUTER 94
FIGURA III.39 MÓDULO DE ADMINISTRACIÓN 95
FIGURA III.40 INGRESO A SUB-PESTAÑA "FIRMWARE UPGRADE". 95
FIGURA III.41 MENSAJE DE ADVERTENCIA 95
FIGURA III.42 PROCESO DE FLASHEO 96
FIGURA III.43 MÓDULO QOS 97
FIGURA III.44 ASIGNACIÓN DE PRIORIDADES A LOS SERVICIOS 97
FIGURA III.45 CLASIFICACIÓN DE TRÁFICO 98
FIGURA III.46 ASIGNACIÓN DE PUERTOS AL SERVICIO 99
FIGURA III.47 ASIGNACIÓN DE PRIORIDAD SEGÚN LA MÁSCARA 99
FIGURA III.48 ASIGNACIÓN DE PRIORIDAD SEGÚN LA DIRECCIÓN MAC 100
FIGURA III.49 CCONFIGURACIÓN DE RED SERVIDOR ELASTIX 100
FIGURA III.50 ARRANQUE DE LA INSTALACIÓN DE ELASTIX 101

FIGURA III.51 CARGA DE ARCHIVOS 102
FIGURA III.52 CONFIGURACIÓN DEL IDIOMA 102
FIGURA III.53 OPCIONES DE ALMACENAMIENTO DE DISCO DURO 102
FIGURA III.54 DISTRIBUCIÓN DEL ESPACIO DEL DISCO DURO 103
FIGURA III.55 CONFIGURACIÓN DE LA TARJETA DE RED 103
FIGURA III.56 OPCIONES DE CONFIGURACIÓN PARA IPV6 103
FIGURA III.57 CONFIGURACIÓN ZONA HORARIA 104
FIGURA III.58 CONFIGURACIÓN DE CONTRASEÑA PARA ELASTIX 104
FIGURA III.59 DEPENDENCIAS DE ELASTIX 104
FIGURA III.60 PROCESO DE INSTALACIÓN ELASTIX 105
FIGURA III.61 FINALIZACIÓN DEL PROCESO DE INSTALACIÓN DE ELASTIX 105
FIGURA III.62 COMPROBACIÓN DEL FUNCIONAMIENTO CORRECTO ELASTIX 105
FIGURA III.63 INGRESO DEL PASSWORD PARA MYSQL 106
FIGURA III.64 CONFIRMACIÓN DEL PASSWORD 106
FIGURA III.65 INGRESO SERVIDOR ELASTIX 106
FIGURA III.66 INGRESO AL SERVIDOR ELASTIX A TRAVÉS DEL NAVEGADOR WEB 107
FIGURA III.67 CONFIGURACIÓN PBX 108
FIGURA III.68 CREACIÓN DE UNA NUEVA EXTENSIÓN 109
FIGURA III.69 APLICACIÓN X-LITE 110
FIGURA III.70 CONFIGURACIÓN CUENTA SIP 110
FIGURA III.71 AGREGAR CUENTAS SIP 111
FIGURA III.72 PROPIEDADES CUENTA SIP 112
FIGURA III.73 CUENTA SIP REGISTRADA 112
FIGURA III.74 USUARIO REGISTRADO 113
FIGURA IIII.75 RECURSOS DEL SISTEMA 114
FIGURA III.76 ESTADÍSTICAS DE LLAMADAS 114
FIGURA III.77 DISCO DURO 115
FIGURA III.78 PARÁMETROS DE RED 115
FIGURA III.79 LISTADO DE INTERFACES ETHERNET 116
FIGURA III.80 CONFIGURACIÓN INTERFACES DE RED 117
FIGURA III.81 CONFIGURACIÓN DEL IDIOMA 119
FIGURA III.82 CONFIGURACIÓN DE FECHA Y HORA 119
FIGURA III.83 SELECCIÓN DE TEMA 120
FIGURA III.84 SELECCIÓN DE CONFIGURACIONES A RESPALDAR 120
FIGURA III.85 PROCESO DE RESPALDO DE CONFIGURACIÓN 121
FIGURA III.86 LISTADO DE TARJETAS DISPONIBLES 122
FIGURA III.87 INGRESO DE COMANDOS DE ASTERISK A SER EJECUTADOS 123
FIGURA III.88 MONITOREO DE CANALES Y TERMINALES 123
FIGURA III.89 LISTADO DE LLAMADAS GRABADAS 124
FIGURA III.90 SELECCIÓN DE ARCHIVOS PARA EDITAR SU CONFIGURACIÓN 125
FIGURA III.91 EDICIÓN DE UN ARCHIVO DE CONFIGURACIÓN 125
FIGURA III.92 ACCESO AL TERMINAL SERVIDOR WEB 126
FIGURA III.93 INSTALACIÓN DE PAQUETES SERVIDOR WEB 127
FIGURA III.94 INGRESO AL NAVEGADOR CON HTTP://LOCALHOST 128
FIGURA III.95 CARGA DE SCRIPTS EN PHP 129
FIGURA III.96 INGRESO DE NOMBRE DE HOST, DIRECCIÓN IP Y PUERTA DE ENLACE 130
FIGURA III.97 CONFIGURACIÓN PREVIA A LA INSTALACIÓN DE PAQUETES 131
FIGURA III.98 SELECCIÓN DE PAQUETES A INSTALAR 131
FIGURA III.99 BÚSQUEDA DE DEPENDENCIAS 132
FIGURA III.100 PROCESO DE INSTALACIÓN CORREO ELECTRÓNICO 132
FIGURA III.101 FINALIZACIÓN DE LA INSTALACIÓN 133
FIGURA III.102 CONFIGURACIÓN DEL FIREWALL 133
FIGURA III.103 ELECCIÓN DEL NIVEL DE SEGURIDAD 134
FIGURA III.104 MENÚ PRINCIPAL DE ZIMBRA COLLABORATION SUITE 141

FIGURA III.105 CONFIGURACIÓN DE CONTRASEÑA 141
FIGURA III.106 INGRESO A LA INTERFAZ WEB CON HTTPS://MAIL.GEEKDEPT.COM:7071/ZIMBRAADMIN/ 142
FIGURA III.107 NAVEGACIÓN INTERFAZ WEB 143
FIGURA III.108 CREACIÓN DE DOMINIOS 143
FIGURA III.109 CREACIÓN CUENTA DE CORREO ELECTRÓNICO 144
FIGURA III.110 INTERFAZ DE USUARIO 144
FIGURA III.111 INICIO DE SESIÓN CUENTA DE CORREO ELECTRÓNICO 145
FIGURA III.112 INICIO DE SESIÓN 147
FIGURA III.113 INICIO DE SESIÓN CUENTA DE CORREO ELECTRÓNICO 148
FIGURA III.114 PERMISOS DE UN DIRECTORIO REMOTO 755 149
FIGURA III.115 PERMISOS DE UN DIRECTORIO REMOTO 644 149
FIGURA III.116 PERMISOS DE UN DIRECTORIO REMOTO 777 150
FIGURA III.117 PERMISOS DE UN DIRECTORIO REMOTO 777 150
FIGURA III.118 APLICACIÓN DE FILTROS A LOS ARCHIVOS 151
FIGURA IV.119 VIDEO LLAMADAS VOIP REALIZADAS 160
FIGURA IV.120 ANCHO DE BANDA DEL VIDEO LLAMADA. 161
FIGURA IV.121 RTP STREAMS. 161
FIGURA IV.122 ANÁLISIS DEL RTP STREAMS 162
FIGURA IV.123 VIDEO LLAMADAS VOIP REALIZADAS 162
FIGURA IV.124 ANCHO DE BANDA DEL VIDEO LLAMADA. 163
FIGURA IV.125 RTP STREAMS. 163
FIGURA IV.126 ANÁLISIS DEL RTP STREAMS 164
FIGURA IV.127 VIDEO LLAMADAS VOIP REALIZADAS 164
FIGURA IV.128 ANCHO DE BANDA DEL VIDEO LLAMADA. 164
FIGURA IV.129 RTP STREAMS. 165
FIGURA IV.130 ANÁLISIS DEL RTP STREAMS 165
FIGURA IV.131 VIDEO LLAMADAS VOIP REALIZADAS 166
FIGURA IV.132 ANCHO DE BANDA DEL VIDEO LLAMADA. 166
FIGURA IV.133 RTP STREAMS 166
FIGURA IV.134 ANÁLISIS DEL RTP STREAMS 167
FIGURA IV.135 VIDEO LLAMADAS VOIP REALIZADAS 167
FIGURA IV.136 ANCHO DE BANDA DEL VIDEO LLAMADA. 167
FIGURA IV.137 RTP STREAMS. 168
FIGURA IV.138 ANÁLISIS DEL RTP STREAMS 168
FIGURA IV.139 VIDEO LLAMADAS VOIP REALIZADAS 169
FIGURA IV.140 ANCHO DE BANDA DEL VIDEO LLAMADA. 169
FIGURA IV.141 RTP STREAMS. 169
FIGURA IV.142 ANÁLISIS DEL RTP STREAMS 170
FIGURA IV.143 VIDEO LLAMADAS VOIP REALIZADAS 170
FIGURA IV.144 ANCHO DE BANDA DEL VIDEO LLAMADA. 170
FIGURA IV.145 RTP STREAMS. 171
FIGURA IV.146 ANÁLISIS DEL RTP STREAMS 171
FIGURA IV.147 VIDEO LLAMADAS VOIP REALIZADAS 172
FIGURA IV.148 ANCHO DE BANDA DEL VIDEO LLAMADA. 172
FIGURA IV.149 RTP STREAMS. 172
FIGURA IV.150 ANÁLISIS DEL RTP STREAMS 173
FIGURA IV.151 VIDEO LLAMADAS VOIP REALIZADAS 173
FIGURA IV.152 ANCHO DE BANDA DEL VIDEO LLAMADA. 173
FIGURA IV.153 RTP STREAMS 174
FIGURA IV.154 ANÁLISIS DEL RTP STREAMS 174
FIGURA IV.155 VIDEO LLAMADAS VOIP REALIZADAS 174
FIGURA IV.156 ANCHO DE BANDA DEL VIDEO LLAMADA. 175
FIGURA IV.157 RTP STREAMS. 175
FIGURA IV.158 ANÁLISIS DEL RTP STREAMS 175

FIGURA IV.159 VIDEO LLAMADAS VOIP REALIZADAS 176
FIGURA IV.160 ANCHO DE BANDA DEL VIDEO LLAMADA. 176
FIGURA IV.161 RTP STREAMS. 176
FIGURA IV.162 ANÁLISIS DEL RTP STREAMS 177
FIGURA IV.163 VIDEO LLAMADAS VOIP REALIZADAS 177
FIGURA IV.164 ANCHO DE BANDA DEL VIDEO LLAMADA. 177
FIGURA IV.165 RTP STREAMS 178
FIGURA IV.166 ANÁLISIS DEL RTP STREAMS 178
FIGURA IV.167 VIDEO LLAMADAS VOIP REALIZADAS 178
FIGURA IV.168 ANCHO DE BANDA DEL VIDEO LLAMADA. 179
FIGURA IV.169 RTP STREAMS 179
FIGURA IV.170 ANÁLISIS DEL RTP STREAMS 179
FIGURA IV.171 VIDEO LLAMADAS VOIP REALIZADAS 180
FIGURA IV.172 ANCHO DE BANDA DEL VIDEO LLAMADA. 180
FIGURA IV.173 RTP STREAMS 180
FIGURA IV.174 ANÁLISIS DEL RTP STREAMS 181
FIGURA IV.175 RENDIMIENTO DE LOS SUBESCENARIOS POR LA ACCIÓN DEL JITTER. 184
FIGURA IV.176 RENDIMIENTO CUANTIFICADO DE LOS SUBESCENARIOS POR LA ACCIÓN DEL JITTER. 185
FIGURA IV.177 RENDIMIENTO DE LOS SUBESCENARIOS POR LA ACCIÓN DE LA LATENCIA. 188
FIGURA IV.178 RENDIMIENTO CUANTIFICADO DE LOS SUBESCENARIOS POR LA ACCIÓN DE LA LATENCIA. 189
FIGURA IV.179 RENDIMIENTO DE LOS SUBESCENARIOS POR LA ACCIÓN DEL % DE LA PÉRDIDA DE PAQUETES 192
FIGURA IV.180 RENDIMIENTO CUANTIFICADO DE LOS SUBESCENARIOS POR LA ACCIÓN DEL % DE LA PÉRDIDA DE PAQUETES 193
FIGURA IV.181 RENDIMIENTO CUANTIFICADO DE LOS SUBESCENARIOS POR LA ACCIÓN DE TODOS LOS PARÁMETROS 196
FIGURA IV.182 COMPROBACIÓN DE LA HIPÓTESIS SEGÚN LA GRÁFICA CHI CUADRADO 204

ÍNDICE DE TABLAS

TABLA II.I ESTÁNDAR IEEE 802.11A 31
TABLA II.II. ESTÁNDAR IEEE 802.11 B 32
TABLA II.III. ESTÁNDAR IEEE 802.11G 34
TABLA II.IV. POOL DE CÓDIGOS DSCP 54
TABLA II.V. CÓDIGOS DSCP 55
TABLA II.VI. CÓDIGOS PARA EL SELECTOR DE CLASE 58
TABLA II.VII. CÓDIGOS DS RECOMENDADOS PARA AS PHB 66
TABLA II.VIII. COMPONENTES DEL CONTROL DEL TRÁFICO EN SISTEMA OPERATIVO LINUX 76
TABLA III.IX. ROUTER CISCO 2811 78
TABLA III.X. TARJETA WLAN CONTROLLER NME-AIR-WLC8-K9 78
TABLA III.XI. SWITCH 79
TABLA III.XII. CISCO AIRONET 1300 79
TABLA III.XIII. ROUTER LINKSYS 80
TABLA III.XIV. PORTÁTILES 81
TABLA III.XV. DD-WRT 90
TABLA III.XVI. PORCENTAJES DE ANCHO DE BANDA 98
TABLA III.XVII. GRUPOS DE USUARIOS 117
TABLA IV.XVIII. OPERACIONALIZACIÓN CONCEPTUAL DE VARIABLES 158
TABLA IV.XIX. OPERACIONALIZACIÓN METODOLÓGICA DE VARIABLES 158
TABLA IV.XX. CLASIFICACIÓN DE QOS SUBJETIVA PARA VOIP 181
TABLA IV.XXI. EQUIVALENCIA DE LOS DENOMINADORES EN FUNCIÓN AL RENDIMIENTO DE LAS VIDEOLLAMADAS 182
TABLA IV.XXII. JITTER DE LOS SUBESCENARIOS SIN QOS – CON QOS 182
TABLA IV.XXIII. DENOMINADORES Y EQUIVALENCIAS EN FUNCIÓN DEL JITTER EN LOS SUBESCENARIOS SIN QOS–CON QOS 183
TABLA IV.XXIV. LATENCIA EN LOS SUBESCENARIOS SIN QOS – CON QOS 186
TABLA IV.XXV. DENOMINADORES Y EQUIVALENCIAS EN FUNCIÓN DE LA LATENCIA EN LOS SUBESCENARIOS SIN QOS–CON QOS 187
TABLA IV.XXVI. PÉRDIDA DE PAQUETES EN LOS SUBESCENARIOS SIN QOS – CON QOS 190
TABLA IV.XXVII. DENOMINADORES Y EQUIVALENCIAS EN FUNCIÓN DEL % PÉRDIDA DE PAQUETES EN LOS SUBESCENARIOS SIN QOS–CON QOS 191
TABLA IV.XXVIII. VALORACIÓN TOTAL DEL RENDIMIENTO EN FUNCIÓN DE LOS PARÁMETROS SIN QOS–CON QOS 194
TABLA IV.XIX. MEDIDA DE LOS INDICADORES EN FUNCIÓN DE SU EQUIVALENCIA 197
TABLA IV.XXX. RANGO DE ESTABLECIMIENTO DE MEJORA 198
TABLA IV.XXXI. VALORACIÓN TOTAL 199
TABLA IV.XXXII. TABLA DE CONTINGENCIA CON LAS FRECUENCIAS OBSERVADAS 200
TABLA IV.XXXIII. TABLA DE FRECUENCIAS ESPERADAS 201
TABLA IV.XXXIV. CÁLCULO DE X^2 202

INTRODUCCIÓN

En la presente tesis se presentan los resultados obtenidos tras una investigación realizada con el objetivo de determinar si la implementación de QoS en los escenarios planteados garantiza que las videollamadas se transmitan con mayor rendimiento.

La implementación de los diferentes escenarios se realizara utilizando equipos Cisco los cuales contemplan el uso de la tarjeta WLAN Controller para de esta manera alcanzar el objetivo deseado, así como el uso de equipos que cubran las necesidades requeridas para el escenario Linux, a través de la utilización de todos estos equipos nos permitiremos definir sus características además de sus ventajas, desventajas, etc...

En cuanto a la implementación de QoS lo aplicaremos a través del protocolo Diffserv el cual se adapta a las necesidades requeridas. Más adelante realizaremos la comprobación de la hipótesis planteada basándonos en los resultados que se obtendrán en el transcurso de la implementación de los escenarios.

El desarrollo de la tesis contempla cuatro capítulos los mismos que engloban información referente al tema de investigación. El capítulo I Marco Referencial contiene los Antecedentes, Justificación, Objetivos e Hipótesis los mismos que se cumplirán en la finalización de la tesis. Además se describen los escenarios propuestos para la realización de las diferentes pruebas. El capítulo II Marco Teórico se describe detenidamente a las redes WLAN, su estructura y funcionamiento así como el protocolo de estudio y su comportamiento bajo el sistema operativo Linux.

Posteriormente en el capítulo III se implementarán los escenarios para realizar todas las pruebas que permitirán obtener los resultados, valiéndonos de la herramienta Wireshark para analizar el tráfico de la red.

En el Capítulo IV se expone el proceso Metodológico de la investigación, el análisis de resultados y la Comprobación de la Hipótesis.

CAPÍTULO I

1. MARCO REFERENCIAL

1.1. ANTECEDENTES

En la actualidad el progresivo aparecimiento de nuevas tendencias y tecnologías como las redes inalámbricas, han permitido un gran desarrollo de las telecomunicaciones además han aportado características como movilidad, comodidad y flexibilidad las mismas que no son ofrecidas por las tecnologías de acceso; exige a los proveedores se adapten a los nuevos requerimientos a la hora de integrar voz, video y datos sobre esta infraestructura de red.

Es indudable el desarrollo en las telecomunicaciones gracias a la utilización de las redes inalámbricas sin embargo aún no existe la característica de Calidad de Servicio (QoS) para las aplicaciones relacionadas con información multimedia, como son la video-conferencia, audio-conferencia, o sistemas cooperativos en las redes inalámbricas usuales, y como consecuencia de esto no se puede asegurar una comunicación satisfactoria para el usuario final.

Se hace necesario el estudio del comportamiento de una plataforma inalámbrica según los parámetros más importantes que determinan la Calidad de Servicio, obteniéndose las características de desempeño y capacidad de la red. Las redes inalámbricas permiten que los dispositivos remotos se conecten sin dificultad, ya se encuentren a unos metros de distancia como a varios kilómetros.

Particularmente las redes inalámbricas ha forjado la imperiosa necesidad de dar un trato diferente al tráfico de voz, video y datos a través de la aplicación de métodos que aseguren una calidad en el servicio (QoS).
En particular el desarrollo de las videollamadas, que consiste en una comunicación simultánea bidireccional de audio y vídeo, se ve limitado ya que las redes fueron desarrolladas para manejar tráfico de datos en los que todos los flujos de la red tienen igual prioridad de transmisión. Así, cuando la demanda del tráfico excede el ancho de banda disponible la tasa de transmisión efectiva de los flujos se reduce de manera similar. Cuando se produce un retardo de un segundo en la transmisión de datos realmente no es percibido por el usuario a diferencia de un pequeño aumento en la latencia o reducción del desempeño puede inferir en la comunicación en una videollamada o en la pérdida de datos.

En Linux la manera de ofrecer QoS se hace a través de su Kernel, y el procedimiento inicia cuando los paquetes llegan al demultiplexor el cual se encarga de enviar el paquete a la capa superior en la pila de protocolos, siempre y cuando detecte que los paquetes son destinados al nodo local, en caso contrario el paquete se envía al bloque de reenvío, el cual también puede recibir paquetes de la capa superior, los paquetes que son reenviados son encolados en un dispositivo de colas, la cola es seleccionada por el control de tráfico (tc) basándose en los requerimientos de QoS.

La Arquitectura de Servicios Diferenciados (Diffserv) está basado en un modelo simple de tratamiento del tráfico, utilizado para grandes redes enrutadas. La sofisticada clasificación, marcado de los paquetes, política y operaciones de acondicionamiento necesitan sólo ser implementadas en los elementos de frontera de la red. El marcado de paquetes se realiza mediante la asignación de un código específico (DSCP – Diffserv Code Point), que es todo lo que se necesita para identificar a cada clase de tráfico.
Nuestro estudio está basado en la aplicación de Diffserv, que es uno de los principales métodos por agregación de tráfico y que lo único que hace es agrupar varios flujos de tráfico en diferentes clases que reciben distinto tratamiento por parte de los routers y en la asignación de prioridades. Los routers de borde son los encargados de marcar los paquetes que entran a la red.

1.2. JUSTIFICACIÓN DEL PROYECTO DE TESIS

1.2.1 JUSTIFICACIÓN TEÓRICA

Hasta hace poco el término QoS no era importante en la mayoría de los sistemas que suelen garantizar la llegada de todos los paquetes, pero no dan ninguna mesura respecto al límite de su llegada al destino. Para el tráfico en tiempo real, es trascendental que los datos lleguen a su destino en un tiempo determinado, ya que no cumplir con este último significará que la aplicación se detendría por falta de datos, lo cual sería inadmisible.
El mecanismo para soportar este tipo de tráfico es crear diferentes protocolos y estrategias para el trabajo de los diferentes recursos de la red, proporcionando así un "servicio" de redes mejorado para los diversos tipos de aplicaciones en los extremos de la red y garantizando la compatibilidad de las distintas técnicas a causa de la heterogeneidad de las redes.
En resumen, QoS, significa disponibilidad de la red y eficiencia en la transmisión, que ayuda a mejorar el servicio a los usuarios de la red. Los mecanismos de QoS funcionan al establecer preferencias en la asignación de este recurso en favor de cierto tráfico.

La utilización de DiffServ como QoS de extremo a extremo nos ayuda a reducir la carga de los dispositivos de red y escala fácilmente cuando la red crece, permite a los clientes guardar un Nivel 3 ToS existente de esquema de prioridad que debe estar en uso, permite a los clientes mezclar dispositivos compliant de DiffServ con equipos existentes que soportan ToS y alivia los cuellos de botella a través de una gestión eficiente de los recursos actuales de la red.

Uno de los puntos fuertes de Sistema Operativo Linux, es su gran capacidad de llevar a cabo tareas de conectividad de red, incluso con recursos modestos en hardware puede ser un hábil servidor de red y convivir con cualquier configuración que ya tengamos funcionando en nuestra red. Entre los beneficios para los cuales se puede utilizar el Sistema Operativo Linux se encuentran el servicio de almacenamiento de datos, servicio de acceso a Internet como servidor web, mail, FTP, etc.

Algunas de las ventajas que tiene la utilización de puntos de acceso implementados con herramientas de software libre son las siguientes:

- Se deja abierta la posibilidad de implementar nuevas tecnologías para redes WLAN.
- Se puede realizar adecuaciones a requerimientos específicos.
- Puede usarse equipo no muy poderoso en cuanto a hardware.
- Flexibilidad de configuración.

Son esas razones por las que el presente trabajo realiza la implementación en puntos de acceso basadas en GNU/Linux.

El elemento principal de implementación del presente trabajo son los puntos de acceso. Puntos de acceso que operan sobre computadoras con un sistema operativo GNU/Linux. A las cuales, se les instalaron tarjetas inalámbricas que soportan distintos modos de operación, entre ellos el modo punto de acceso.

1.2.2 JUSTIFICACIÓN PRÁCTICA

Actualmente existen ya trabajos de investigación que abarca QoS en sistemas multimediales pero no bajo el estudio del protocolo DiffServ y tampoco bajo escenarios con el sistema operativo Linux.

ESCENARIO PROPUESTO

El escenario propuesto contará con la presencia de equipos CISCO para cubrir las necesidades de sus elementos hardware.

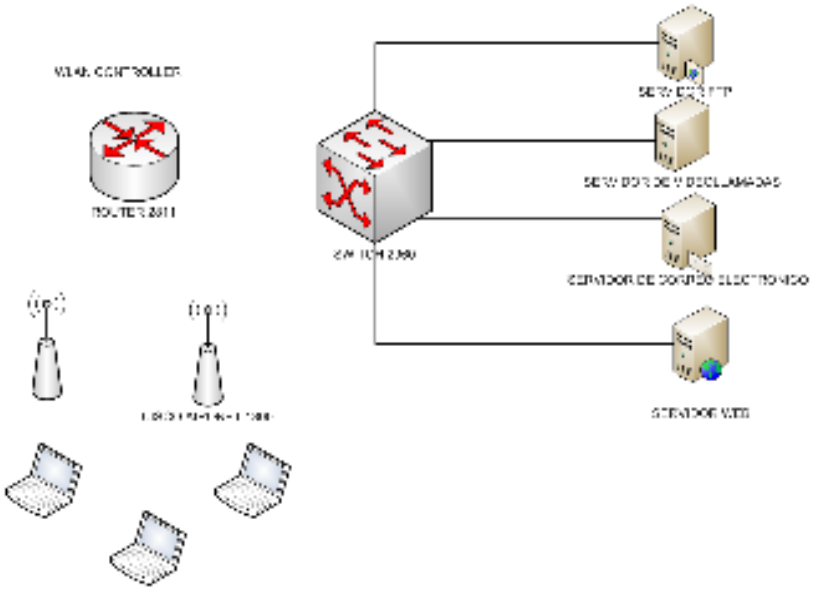

FIGURA I.01 Escenario de Pruebas 1(CISCO)

✓ Elementos Hardware

El escenario para la prueba está conformado por:

- Portátiles
- Cisco Aironet 1300
- Router 2811 con WLAN CONTROLLER
- Switch Cisco 2960
- Servidor FTP (Vsftpd)
- Servidor de Videollamadas (Elastix)
- Servidor de Correo Electrónico (Zimbra)
- Servidor Web (Apache)

✓ Elementos Software

- Vsftpd
- Elastix v2.0

- Zimbra v7.0
- Apache v2.2.19
- Wireshark v1.4.3
- X-lite v2.24
- Skype v5.3

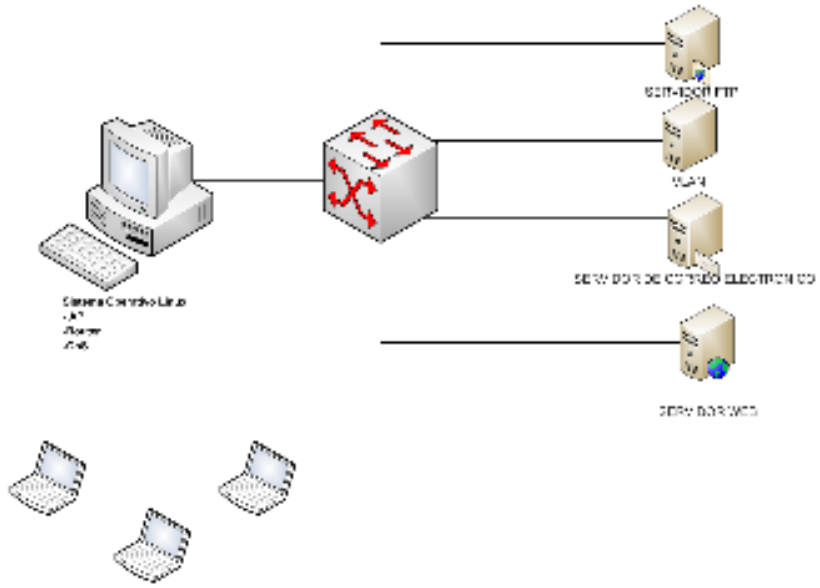

FIGURA II.02 Escenario de Pruebas 2(LINUX)

✓ Elementos Hardware

El escenario para la prueba está conformado por:

- Portátiles
- Una Computadora con el sistema operativo GNU/Linux. La distribución Centos.
- El paquete wireless-tools.
- Una tarjeta de red inalámbrica con chip Atheros.
- El controlador MadWifi para la tarjeta inalámbrica.
- Switch
- Servidor FTP (Vsftpd)

- Servidor de Videollamadas (Elastix)
- Servidor de Correo Electrónico (Zimbra)
- Servidor Web (Apache)

✓ Elementos Software

- Vsftpd
- Elastix v2.0
- Zimbra v7.0
- Apache v2.2.19
- Wireshark v1.4.3
- X-lite
- Skype v5.3

Vsftpd (Very Secure FTP Daemon): es un equipamiento lógico utilizado para implementar servidores de archivos a través del protocolo FTP. Se distingue principalmente porque sus valores predeterminados son muy seguros y por su sencillez en la configuración, comparado con otras alternativas como ProFTPD y Wu-ftpd. Actualmente se presume que vsftpd es quizá el servidor FTP más seguro del mundo

Elastix: es una distribución libre de Servidor de Comunicaciones unificadas que integra en un solo paquete: VoIP PBX, Fax, Mensajería Instantánea, Correo electrónico, Colaboración. Iimplementa gran parte de su funcionalidad sobre 4 programas de software muy importantes como son Asterisk, Hylafax, Openfire y Postfix. Estos brindan las funciones de PBX, Fax, Mensajería Instantánea y Correo electrónico respectivamente.

Zimbra: La Suite de Colaboración Zimbra es un programa colaborativo creado por Zimbra Inc., fue adquirida por Yahoo! Inc. en Septiembre de 2007, haciendo un acuerdo de mantener sus estándares de Software Abierto. Posee tanto el componente de servidor como su respectivo cliente. Existen varias versiones de Zimbra disponibles: una versión soportada por la comunidad de Software Abierto (Open Source), y otras con parte del código cerrado y soportado comercialmente que contiene algunas mejoras. Al igual que el programa

de correo electrónico Exchange, de Microsoft, Zimbra permite a los empleados de oficina enviar, recibir, guardar y buscar los miles de mensajes procesados cada día.

Apache: El servidor Apache es un servidor web HTTP de código abierto para plataformas Unix (BSD, GNU/Linux, etc.), Microsoft Windows, Macintosh y otras. Apache presenta entre otras características altamente configurables, bases de datos de autenticación y negociado de contenido, pero fue criticado por la falta de una interfaz gráfica que ayude en su configuración.

Wireshark (Ethereal Network Protocol Analyzer): Es un software de libre distribución, de código abierto, realizado bajo licencia GNU. Antes conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica para educación. Cuenta con todas las características estándar de un analizador de protocolos.

X-lite: Es una práctica aplicación de las denominadas softphone, es decir, que permite realizar llamadas desde el ordenador entre todos los usuarios de Internet, a nivel mundial. Como usuario de X-Lite solamente se tiene que registrar y se le asignará un número IP (VoIP) propio, para así hacer llamadas a cualquier número que pertenezca a la red softphone.

1.3. OBJETIVOS

1.3.1 Objetivo General

- ✓ Analizar el protocolo Diffserv aplicado a la provisión de QoS en el tráfico de videollamadas sobre redes inalámbricas con equipos Cisco y Linux.

1.3.2 Objetivo Específicos

- ✓ Analizar el protocolo Diffserv, su arquitectura y elementos principales.
- ✓ Implementar dos prototipos de prueba para estudiar el comportamiento del protocolo mencionado con equipos Cisco y Linux.
- ✓ Evaluar los parámetros de rendimiento de las videollamadas en los escenarios propuestos.

- ✓ Proponer una guía de implementación de servicio QoS en redes inalámbricas de los dos escenarios planteados"

1.4. HIPOTESIS

"La administración de QoS en las redes inalámbricas, garantizará que las videollamadas logren transmitirse con mayor rendimiento"

CAPÍTULO II

2. REDES INALAMBRICAS

2.1. Introducción a Redes Inalámbricas

2.1.1. ¿Qué es una Red Inalámbrica?

Una red inalámbrica es, una red en la que dos o más terminales (por ejemplo, ordenadores portátiles, agendas electrónicas, etc.) se pueden comunicar sin la necesidad de una conexión por cable. Con las redes inalámbricas, un usuario puede mantenerse conectado cuando se desplaza dentro de una determinada área geográfica. Por esta razón, a veces se utiliza el término "movilidad" cuando se trata este tema.

Las redes inalámbricas se basan en un enlace que utiliza ondas electromagnéticas (radio e infrarrojo) en lugar de cableado estándar.

Las redes inalámbricas permiten que los dispositivos remotos se conecten sin dificultad, ya se encuentren a unos metros de distancia como a varios kilómetros. Asimismo, la instalación de estas redes no requiere de ningún cambio significativo en la infraestructura existente como pasa con las redes cableadas. Tampoco hay necesidad de agujerear las paredes para pasar cables ni de instalar portacables o conectores. Esto ha hecho que el uso de esta tecnología se extienda con rapidez.

2.1.2. Ventajas de las Redes Inalámbricas

Las principales ventajas que ofrecen las redes inalámbricas son las siguientes:

Movilidad. La libertad de movimientos es uno de los beneficios más evidentes de las redes inalámbricas. Un ordenador o cualquier otro dispositivo (por ejemplo, una PDA o una webcam) pueden situarse en cualquier punto dentro del área de cobertura de la red sin tener que depender de que si es posible o no hacer llegar un cable hasta este sitio. Ya no es necesario estar atado a un cable para navegar en Internet, imprimir un documento o acceder a los recursos.

Desplazamiento. Con una computadora portátil o PDA no solo se puede acceder a Internet o a cualquier otro recurso de la red local desde cualquier parte de la oficina o de la casa, sino que nos podemos desplazar sin perder la comunicación. Esto no solo da cierta comodidad, sino que facilita el trabajo en determinadas tareas, como, por ejemplo, la de aquellos empleados cuyo trabajo les lleva a moverse por todo el edificio. **Flexibilidad.** Las redes inalámbricas no solo nos permiten estar conectados mientras nos desplazamos por una computadora portátil, sino que también nos permite colocar una computadora de sobremesa en cualquier lugar sin tener que hacer el más mínimo cambio de configuración de la red.

Las redes inalámbricas nos permiten llegar a donde el cable no puede así como evitar colocar peligrosos cables por el suelo. Resulta también especialmente indicado para aquellos lugares en los que se necesitan accesos esporádicos. Las redes inalámbricas suponen una alternativa mucho más viable que las redes cableadas.

Ahorro de costes. Diseñar o instalar una red cableada puede llegar a alcanzar un alto coste, no solamente económico, sino en tiempo y molestias. En entornos domésticos y en determinados entornos empresariales donde no se dispone de una red cableada porque su instalación presenta problemas, la instalación de una red inalámbrica permite ahorrar costes al permitir compartir recursos: acceso a Internet, impresoras, etc. **Escalabilidad.** Se le llama escalabilidad a la facilidad de expandir la red después de su instalación inicial. Conectar una nueva computadora cuando se dispone de una red inalámbrica es algo tan sencillo como instalarle una tarjeta y listo. Con las redes cableadas esto mismo requiere instalar un nuevo cableado o lo que es peor, esperar hasta que el nuevo cableado quede instalado.

2.1.3. Desventajas de las Redes Inalámbricas

Menor ancho de banda. Las redes de cable actuales trabajan a 100 Mbps, mientras que las redes inalámbricas Wi-Fi lo hacen a 11 Mbps Es cierto que existen estándares que alcanzan los 54 Mbps y soluciones propietarias que llegan a 100 Mbps, pero estos estándares están en los comienzos de su comercialización y tiene un precio superior al de los actuales equipos Wi-Fi.

Mayor inversión inicial. Para la mayoría de las configuraciones de la red local, el coste de los equipos de red inalámbricos es superior al de los equipos de red cableada.

Seguridad. Las redes inalámbricas tienen la particularidad de no necesitar un medio físico para funcionar. Esto fundamentalmente es una ventaja, pero se convierte en una desventaja cuando se piensa que cualquier persona con una computadora portátil solo necesita estar dentro del área de cobertura de la red para poder intentar acceder a ella. Como el área de cobertura no está definida por paredes o por ningún otro medio físico, a los posibles intrusos no les hace falta estar dentro de un edificio o estar conectado a un cable. Además, el sistema de seguridad que incorporan las redes Wi-Fi no es de lo más fiables. A pesar de esto también es cierto que ofrece una seguridad válida para la inmensa mayoría de las aplicaciones y que ya hay disponible un nuevo sistema de seguridad (WPA) que hace a Wi-Fi mucho más confiable.

Interferencias. Las redes inalámbricas funcionan utilizando el medio radio electrónico en la banda de 2,4 GAZ. Esta banda de frecuencias no requiere de licencia administrativa para ser utilizada por lo que muchos equipos del mercado, como teléfonos inalámbricos, microondas, etc., utilizan esta misma banda de frecuencias. Además, todas las redes Wi-Fi funcionan en la misma banda de frecuencias incluida la de los vecinos. Este hecho hace que no se tenga la garantía de nuestro entorno radioelectrónico este completamente limpio para que nuestra red inalámbrica funcione a su más alto rendimiento. Cuanto mayor sea las interferencias producidas por otros equipos, menor será el rendimiento de nuestra red. No obstante, el hecho de tener probabilidades de sufrir interferencias no quiere decir que se tengan. La mayoría de las redes inalámbricas funcionan perfectamente sin mayores problemas en este sentido.

Incertidumbre tecnológica. La tecnología que actualmente se está instalando y que ha adquirido una mayor popularidad es la conocida como Wi-Fi (IEEE 802.11B). Sin embargo, ya existen tecnologías que ofrecen una

mayor velocidad de transmisión y unos mayores niveles de seguridad, es posible que, cuando se popularice esta nueva tecnología, se deje de comenzar la actual o, simplemente se deje de prestar tanto apoyo a la actual. Lo cierto es que las leyes del mercado vienen también marcadas por las necesidades del cliente y, aunque existe una incógnita, los fabricantes no querrán perder el tirón que ha supuesto Wi-Fi y harán todo lo posible para que los nuevos dispositivos sean compatibles con los actuales.

2.1.4. WLAN (Wireless Local Área Network, Redes de Área Local Inalámbrica)

Una red de área local inalámbrica, también conocida como WLAN (*wireless local area network*), es un sistema de comunicación de datos inalámbrico flexible, muy utilizado como alternativa a las redes de área local cableadas o como extensión de estas. Utiliza tecnologías de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas. Estas redes van adquiriendo importancia en muchos campos, como almacenes o para manufactura, en los que se transmite la información en tiempo real a una terminal central. También son muy populares en los hogares para compartir el acceso a Internet entre varias computadoras.

WiFi Alliance

Wi-Fi es un sistema de envío de datos sobre redes computacionales, que utiliza ondas de radio en lugar de cables, además es una marca de la Wi-Fi Alliance (anteriormente la WECA: Wireless Ethernet Compatibility Alliance), la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11

La WECA tiene como misión certificar la interoperatividad y compatibilidad entre diferentes fabricantes de productos wireless bajo el estándar IEEE802.11. La WECA tiene por finalidad impulsar el desarrollo a nivel mundial de la tecnología de LAN inalámbrica bajo el estándar IEEE 802.11.

2.1.5. Estándares de las Redes Inalámbricas

IEEE 802.11

El IEEE 802.11fue publicada en el año 1997, tenía velocidades de transmisión teóricas de 1 hasta 2 Mbps que se transmiten por señales infrarrojas (IR) y trabajaba en la banda de frecuencia de 2,4 GHz. En la actualidad no se fabrican productos sobre este estándar. El término IEEE 802.11 se utiliza también para referirse a este protocolo al que ahora se conoce como "802.11legacy."

El estándar original también define el protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones) como método de acceso. Una parte importante de la velocidad de transmisión teórica se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas. Estas y otras debilidades fueron corregidas en el estándar 802.11b, que fue el primero de esta familia en alcanzar amplia aceptación entre los consumidores.

IEEE 802.11a

El estándar IEEE 802.11a se aplica a la banda de UNII (Unlicensed National Information Infrastructure) de los 5GHz. El estándar usa el método OFDM (división de frecuencias ortogonales multiplexadas) para la transmisión de datos hasta 54Mbps. Su mayor inconveniente es la no compatibilidad con los estándares de 2,4GHz. Por lo demás su operación es muy parecida al estándar 802.11g.

Cubre entre 30 y 300 metros si no hay muros y obstáculos.

A continuación se presenta una tabla resumen

TABLA II.I. Estándar IEEE 802.11a

Rango de frecuencias:	De 5,15 a 5,25 GHz (50mW) De 5,25 a 5,35 GHz (250mW) De 5,725 a 5,825 GHz (1W)
Acceso:	Orthogonal Frecuency Division Multiplexing (OFDM)
Velocidad:	Hasta 54 Mbps

TABLA II.I Estándar IEEE 802.11a(Continuación)

Compatibilidad:	**No compatible con los sistemas 802.11b, 802.11, HiperLAN2, Infrarrojos (IR) ni con HomeRF**
Distancia:	De 30 a 300 metros.
Aplicación	Todo tipo de red de datos Ethernet

IEEE 802.11b

Esta extensión del estándar 802.11, definido en 1.999, permite velocidades de 5,5 y 11Mbps en el espectro de los 2,4GHz. Esta extensión es totalmente compatible con el estándar original de 1 y 2 Mbps (sólo con los sistemas DSSS, no con los FHSS o sistemas infrarrojos) pero incluye una nueva técnica de modulación llamada Complementary Code Keying (CCK), que permite el incremento de velocidad. El estándar 802.11b define una única técnica de modulación para las velocidades superiores - CCK - al contrario que el estándar original 802.11 que permitía tres técnicas diferentes (DSSS, FHSS e infrarrojos). De este modo, al existir una única técnica de modulación, cualquier equipo de cualquier fabricante podrá conectar con cualquier otro equipo si ambos cumplen con la especificación 802.11b. Esta ventaja se ve reforzada por la creación de la organización llamada WECA (Wireless Ethernet Compatibility Alliance), una organización que dispone de un laboratorio de pruebas para comprobar equipos 802.11b. Cada equipo certificado por la WECA recibe el logo de compatibilidad WI-FI que asegura su compatibilidad con el resto de equipos certificados.

A continuación se presenta una tabla resumen del estándar IEEE 802.11b

TABLA II.II Estándar IEEE 802.11 b

Rango de frecuencias:	**De 2.4 a 2.4835 GHz**
Acceso:	Direct Sequence Spread Spectrum (DSSS) usando Complementary Code Keying (CCK)
Velocidad:	Hasta 11 Mbps
Compatibilidad:	Compatible con sistemas 802.11 DSSS de 1 y 2 Mbps No compatible con los sistemas 802.11 FHSS, Infrarrojos (IR) ni con HomeRF
Distancia:	Depende de la instalación y de los obstáculos, 300m típicos

TABLA II.II Estándar IEEE 802.11 b (Continuación)

Aplicación	**Todo tipo de red de datos Ethernet**

IEEE 802.11 e

Con el estándar 802.11e, la tecnología IEEE 802.11 soporta tráfico en tiempo real en todo tipo de entornos y situaciones. Las aplicaciones en tiempo real son ahora una realidad por las garantías de Calidad de Servicio (QoS) proporcionado por el 802.11e. El objetivo del nuevo estándar 802.11e es introducir nuevos mecanismos a nivel de capa MAC para soportar los servicios que requieren garantías de Calidad de Servicio. Para cumplir con su objetivo IEEE 802.11e introduce un nuevo elemento llamado Hybrid Coordination Function (HCF) con dos tipos de acceso:

(EDCA) Enhanced Distributed Channel Access, y (HCCA) Controller Channel Access.

En este nuevo estándar se definen cuatro categorías de acceso al medio (Ordenadas de menos a más prioritarias).

- Background (AC_BK)
- Best Effort (AC_BE)
- Video (AC_VI)
- Voice (AC_VO)

IEEE 802.11 g

El estándar IEEE 802.11g ofrece 54Mbps en la banda de 2,4GHz. Dicho con otras palabras, asegura la compatibilidad con los equipos Wi-Fi preexistentes. Para aquellas personas que dispongan de dispositivos inalámbricos de tipo Wi-Fi, 802.11g proporciona una forma sencilla de migración a alta velocidad, extendiendo el período de vida de los dispositivos de 11Mbps. El estándar 802.11g se publicó como borrador en Noviembre de 2001 con los siguientes elementos obligatorios y opcionales:

1. El método OFDM (Orthogonal Frecuancy Division Multiplexing) es obligatorio y es lo que permite velocidades superiores en la banda de los 2,4GHz.

2. Los sistemas deben ser totalmente compatibles con las tecnologías anteriores de 2,4GHz Wi-Fi (802.11b). Por lo que el uso del método CCK (Complementary Code Keying) también será obligatorio para asegurar dicha compatibilidad.
3. El borrador del estándar marca como opcional el uso del método PBCC (Packet Binary Convolution Coding) y el OFDM/CCK simultáneo.

A continuación se presenta una tabla resumen del estándar IEEE 802.11g

TABLA II.III Estándar IEEE 802.11g

Rango de Frecuencias	**De 2.4 a 2.4835 GHz**
Acceso:	Obligatoriamente complementary Code Keying (CCK) y Orthogonal Frecuency Division Multiplexing (OFDM), opcionalmente puede incluir Packet Binary Convolution Coding (PBCC) y CCK/OFDM
Velocidad:	Hasta 54 Mbps
Compatibilidad:	Compatible con sistemas 802.11b de 11Mbps y 5,5 Mbps. Compatible con sistemas DSSS de 1 y 2 Mbps. No compatible con los sistemas 802.11 FHSS, Infrarrojos (IR) ni con HomeRF
Distancia:	Depende de la instalación y de los obstáculos, 300m típicos
Aplicación:	Todo tipo de red de datos Ethernet

IEEE 802.11 n

Su velocidad real de transmisión podría llegar a los 600 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y unas 40 veces más rápida que una red bajo el estándar 802.11b. También se espera que el alcance de operación de las redes sea mayor con este nuevo estándar gracias a la tecnología MIMO

Múltiple Input – Multiple Output, que permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas. A diferencia de las otras versiones de Wi-Fi, 802.11n puede trabajar en dos bandas de frecuencias: 2,4 GHz (la que emplean 802.11b y 802.11g) y 5 GHz (la que usa 802.11a). Gracias a ello, 802.11n es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi. Además, es útil que trabaje en la banda de 5 GHz, ya que está menos congestionada y en 802.11n permite alcanzar un mayor rendimiento.

El estándar 802.11n fue ratificado por la organización IEEE el 11 de septiembre de 2009 con una velocidad de 600 Mbps en capa física.

2.1.6. QoS (Quality of Service, Calidad de Servicio)

QoS (Quality of Service o Calidad de Servicio) es un conjunto de protocolos y tecnologías que garantizan la entrega de datos a través de la red en un momento dado. De este modo, nos aseguramos que las aplicaciones que requieran un tiempo de latencia bajo o un mayor consumo de ancho de banda, realmente dispongan de los recursos suficientes cuando los soliciten. Por ello, uno de las principales metas de QoS es la priorización. Esto es, el dar más relevancia a unas conexiones frente a otras.

Algunos de los beneficios que podemos obtener al implantar QoS en nuestro sistema son:

- **Control sobre los recursos:** podemos limitar el ancho de banda consumido por transferencias de FTP y dar más prioridad a un servidor de bases de datos al que acceden múltiples clientes.
- **Uso más eficiente de los recursos de red:** al poder establecer prioridades dependiendo del tipo de servicio, umbrales de tasas de transferencia...
- **Menor latencia:** en aplicaciones de tráfico interactivo como SSH, telnet... que requieren un tiempo de respuesta corto.

2.1.7. Parámetros de rendimiento

2.1.7.1. Retardo

El retardo conocido también como latencia se define técnicamente como el tiempo que tarda un paquete en llegar desde la fuente al destino.

CAUSAS:

No es un problema específico de las redes no orientadas a conexión y por tanto de las videoconferencias. Es un problema general de las redes de telecomunicación. Por ejemplo, la latencia en los enlaces via satelite es muy elevada por las distancias que debe recorrer la información.

Las comunicaciones en tiempo real y full-dúplex son sensibles a este efecto. Es el problema de "pisarnos". Al igual que el jitter, es un problema frecuente en enlaces lentos o congestionados.

VALORES RECOMENDADOS:

La latencia o retardo entre el punto inicial y final de la comunicación debiera ser inferior a 150 ms**.** El oído humano es capaz de detectar latencias de unos 250 ms, 200 ms en el caso de personas bastante sensibles. Si se supera ese umbral la comunicación se vuelve molesta.

POSIBLES SOLUCIONES:

No hay una solución que se pueda implementar de manera sencilla. Muchas veces depende de los equipos por los que pasan los paquetes, es decir, de la red misma. Se puede intentar reservar un ancho de banda de origen a destino **o** señalizar los paquetes con valores de TOS para intentar que los equipos sepan que se trata de tráfico en tiempo real y lo traten con mayor prioridad pero actualmente no suelen ser medidas muy eficaces ya que no disponemos del control de la red.

Si el problema de la latencia está en nuestra propia red interna podemos aumentar el ancho de banda o velocidad del enlace o priorizar esos paquetes dentro de nuestra red.

2.1.7.2. Jitter

El jitter se define técnicamente como la variación en el tiempo en la llegada de los paquetes, causada por la congestión de la red, pérdida de sincronización o por las diferentes rutas seguidas por los paquetes para llegar al destino.

Las comunicaciones en tiempo real (como VoIP) son especialmente sensibles a este efecto. En general, es un problema frecuente en enlaces lentos o congestionados. Al incrementar mecanismos de QoS (calidad del servicio) como prioridad en las colas, reserva de ancho de banda o enlaces de mayor velocidad (100Mb Ethernet, E3/T3, SDH) se reduce los problemas del jitter aunque en el futuro seguirá siendo un problema por bastante tiempo.

CAUSAS:

El jitter es un efecto de las redes de datos no orientadas a conexión y basadas en conmutación de paquetes. Como la información se discretiza en paquetes cada uno de los paquetes puede seguir una ruta distinta para llegar al destino.

VALORES RECOMENDADOS:

El jitter entre el punto inicial y final de la comunicación debiera ser inferior a 100 ms. Si el valor es menor a 100 ms el jitter puede ser compensado de manera apropiada. En caso contrario deberá ser minimizado.

POSIBLES SOLUCIONES:

La solución más ampliamente adoptada es la utilización del jitter buffer. El jitter buffer consiste básicamente en asignar una pequeña cola o almacén para ir recibiendo los paquetes y sirviéndolos con un pequeño retraso. Si algún paquete no está en el buffer (se perdió o no ha llegado todavía) cuando sea necesario se descarta. Normalmente en los teléfonos IP (hardware y software) se pueden modificar los buffers. Un aumento del buffer implica menos perdida de paquetes pero más retraso. Una disminución implica menos retardo pero más pérdida de paquetes.

2.1.7.3. Pérdida de Paquetes

CAUSAS:

Las comunicaciones en tiempo real están basadas en el protocolo UDP. Este protocolo no está orientado a conexión y si se produce una pérdida de paquetes no se reenvían. Además la perdida de paquetes también se produce por descartes de paquetes que no llegan a tiempo al receptor.

Sin embargo la voz es bastante predictiva y si se pierden paquetes aislados se puede recomponer la voz de una manera bastante óptima. El problema es mayor cuando se producen pérdidas de paquetes en ráfagas.

VALORES RECOMENDADOS:

La pérdida de paquetes máxima admitida para que no se degrade la comunicación deber ser **inferior al 1%.** Pero es bastante dependiente del códec que se utiliza. Cuanto mayor sea la compresión del códec más pernicioso es el efecto de la pérdida de paquetes. Una pérdida del 1% degrada más la comunicación si se usa el códec G.729 en vez del G.711.

POSIBLES SOLUCIONES:

Para evitar la pérdida de paquetes una técnica muy eficaz en redes con congestión o de baja velocidad es no transmitir los silencios. Gran parte de las conversaciones están llenas de momentos de silencio. Si solo transmitimos cuando haya información audible liberamos bastante los enlaces y evitamos fenómenos de congestión.

2.1.7.4. Ancho de banda

Una medida de la capacidad de transmisión de datos, expresada generalmente en Kilobits por segundo (Kbps) o en Megabits por segundo (Mbps). Indica la capacidad máxima teórica de una conexión, pero esta capacidad teórica se ve disminuida por factores negativos tales como el retardo de transmisión, que pueden causar un deterioro en la calidad.

2.1.8. AP (Access Point, Punto de Acceso)

Un Access Point significa punto de acceso. Se trata de un dispositivo utilizado en redes inalámbricas de área local (WLAN - *Wireless Local Area Network*), una red local inalámbrica es aquella que cuenta con una interconexión de computadoras relativamente cercanas, sin necesidad de cables, estas redes funcionan a base de ondas de radio específicas. El Access Point entonces se encarga de ser una puerta de entrada a la red inalámbrica en un lugar específico y para una cobertura de radio determinada, para cualquier dispositivo que solicite acceder, siempre y cuando esté configurado y tenga los permisos necesarios.

Características de los Access point:

- Permiten la conexión de dispositivos inalámbricos a la WLAN, como: teléfonos celulares modernos, Netbook, Laptop, PDA, Notebook e inclusive otros Access Point para ampliar las redes.
- También cuentan con soporte para redes basadas en alambre (LAN - Local Area Network), que tienen un puerto RJ45 que permite interconectarse con Switch inalámbrico y formar grandes redes entre dispositivos convencionales e inalámbricos.
- La tecnología de comunicación con que cuentan es a base de ondas de radio, capaces de traspasar muros, sin embargo entre cada obstáculo esta señal pierde fuerza y se reduce su cobertura.
- El Access Point puede tener otros servicios integrados como expansor de rango y ampliar la cobertura de la red.
- Cuentan con un alcance máximo de cobertura, esto dependiendo el modelo, siendo la unidad de medida el radio de alcance que puede estar desde 30 metros (m) hasta más de 100 m.
- Cuentan con una antena externa para la correcta emisión y recepción de ondas, así por ende, una correcta transmisión de la información.

2.1.9. AP (Access Point, Punto de Acceso)

Los modos de funcionamiento definidos por el estándar 802.11 se listan a continuación:

Modo de infraestructura:

En el modo de infraestructura, cada estación informática se conecta a un punto de acceso a través de un enlace inalámbrico. La configuración formada por el punto de acceso y las estaciones ubicadas dentro del área de cobertura se llama conjunto de servicio básico o BSS. Estos forman una célula. Cada BSS se identifica a través de un BSSID (identificador de BSS) que es un identificador de 6 bytes (48 bits). En el modo infraestructura el BSSID corresponde al punto de acceso de la dirección MAC.

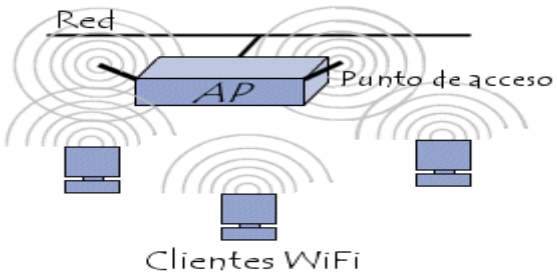

FIGURA III.03 Conjunto de servicios básico (BSS)

Es posible vincular varios puntos de acceso juntos (o con más exactitud, varios BSS) con una conexión llamada sistema de distribución (o SD) para formar un conjunto de servicio extendido o ESS. El sistema de distribución también puede ser una red conectada, un cable entre dos puntos de acceso o incluso una red inalámbrica.

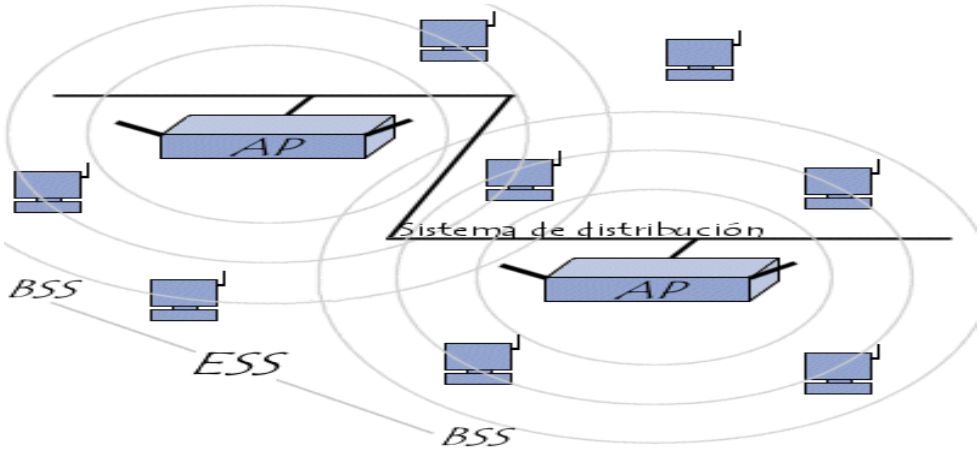

FIGURA IVI.04 Conjunto de servicio extendido (ESS)

Un ESS se identifica a través de un **ESSID** (identificador del conjunto de servicio extendido), que es un identificador de 32 caracteres en formato ASCII que actúa como su nombre en la red. El ESSID, a menudo abreviado **SSID**, muestra el nombre de la red y de alguna manera representa una medida de seguridad de primer nivel ya que una estación debe saber el **SSID** para conectarse a la red extendida.

Cuando un usuario itinerante va desde un BSS a otro mientras se mueve dentro del ESS, el adaptador de la red inalámbrica de su equipo puede cambiarse de punto de acceso, según la calidad de la señal que reciba desde distintos puntos de acceso. Los puntos de acceso se comunican entre sí a través de un sistema de distribución con el fin de intercambiar información sobre las estaciones y, si es necesario, para transmitir datos desde estaciones móviles. Esta característica que permite a las estaciones moverse "de forma transparente" de un punto de acceso al otro se denomina itinerancia.

Modo ad hoc

En el modo ad hoc los equipos clientes inalámbricos se conectan entre sí para formar una red punto a punto, es decir, una red en la que cada equipo actúa como cliente y como punto de acceso simultáneamente.

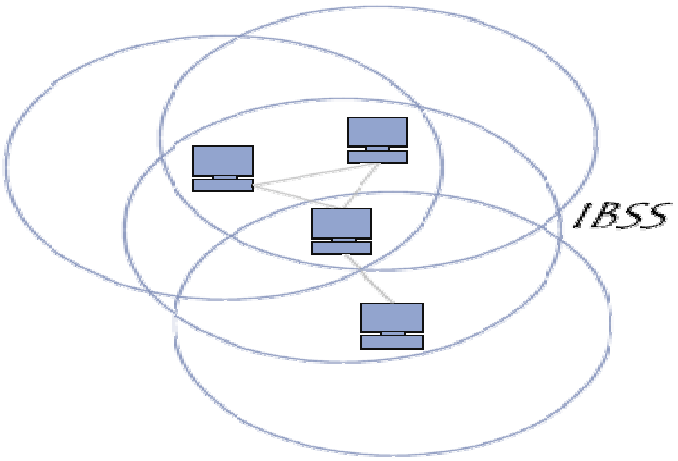

FIGURA II.05 Conjunto de servicio básico independiente o IBSS

La configuración que forman las estaciones se llama conjunto de servicio básico independiente o IBSS.

Un IBSS es una red inalámbrica que tiene al menos dos estaciones y no usa ningún punto de acceso. Por eso, el IBSS crea una red temporal que le permite a la gente que esté en la misma sala intercambiar datos. Se identifica a través de un SSID de la misma manera en que lo hace un ESS en el modo infraestructura.

En una red ad hoc, el rango del *BSS independiente* está determinado por el rango de cada estación. Esto significa que si dos estaciones de la red están fuera del rango de la otra, no podrán comunicarse, ni siquiera cuando puedan "ver" otras estaciones. A diferencia del modo infraestructura, el modo ad hoc no tiene un sistema de distribución que pueda enviar tramas de datos desde una estación a la otra. Entonces, por definición, un IBSS es una red inalámbrica restringida.

2.1.10. WLAN Controller

FIGURA VI.06 Tarjeta WLAN Controller (NME-AIR-WLC8-K9)

Cisco Wireless LAN Controller, proporciona soluciones de red inalámbricas 802.11 a las pequeñas y medianas empresas (Pymes) y clientes empresariales de sucursales. Como un componente de la Cisco Unified Wireless Network, Cisco WLCM provee a los administradores de red la visibilidad y control necesarios para gestionar con eficacia y seguridad redes LAN inalámbricas y servicios de movilidad, tales como mayor seguridad, voz, acceso de invitado, y servicios de localización. La tarjeta Wireless LAN Controller maneja hasta 8 puntos de acceso ligeros.

2.2. PROTOCOLO DIFFSERV

2.2.1. Introducción al Protocolo Diffserv

En los últimos años, han surgido diferentes mecanismos para brindar al usuario redes de Calidad de Servicio (QoS), siendo su principal objetivo proporcionar un "servicio" de redes reformado para las aplicaciones en los extremos de la red.

Los administradores agregan continuamente nuevos recursos para tratar de responder a la creciente demanda de aplicaciones multimedia y/o de tiempo real. Los mecanismos de QoS proporcionan un conjunto de herramientas que el administrador de redes puede utilizar para administrar el uso de recursos de red de una forma controlada y eficaz.

Las redes están construidas mediante la unión de dispositivos de red, tales como conmutadores y ruteadores. Estos dispositivos intercambian el tráfico entre ellos mediante interfaces, la capacidad de una interfaz para enviar tráfico constituye un recurso de red fundamental. Los mecanismos de QoS funcionan al establecer preferencias en la asignación de este recurso en favor de cierto tráfico. Nuestra investigación se basa en la aplicación Diffserv, que constituye un método por agregación de tráfico a través de la agrupación de varios flujos de tráfico en diferentes clases.

2.2.2. Modelo de la arquitectura Differentiated Services

En la Arquitectura de Servicios Diferenciados la sofisticada clasificación, marcado de los paquetes, política y operaciones de acondicionamiento son implementados en los componentes de frontera de la red. En cuanto al marcado de paquetes este se lo hace mediante la asignación de un código específico DSCP, para identificar a cada clase de tráfico.

La clase de tráfico es la agregación de todos los flujos bajo el mismo criterio de clasificación. El DSCP indica un comportamiento específico que un paquete debe de recibir en cada enrutador. La diferenciación de servicios se logra mediante la definición de comportamientos específicos para cada clase de tráfico entre dispositivos de interconexión, hecho conocido como PHB (Per Hop Behavior).

A través de esta arquitectura se logra mayor escalabilidad al implementar funciones de clasificación y condicionamiento sólo en los nodos del borde de la red, y aplicando conductas por salto a los agregados del tráfico (BA) que han sido apropiadamente marcados usando el campo DS en las cabeceras de IPv4 o IPv6.

Esta arquitectura sólo provee servicio diferenciado en una dirección del flujo de tráfico y es por ende asimétrica, ya que quien nos brinda el Servicio Diferenciado es el ISP.

2.2.2.1. Dominio de los Servicios Diferenciados (Dominio DS)

Un dominio DS es un conjunto de nodos DS que operan con una política de aprovisionamiento de servicios común y con un conjunto de grupos PHB implementados en cada nodo. Está formado por nodos DS de frontera que clasifican y posiblemente condicionen el tráfico entrante para asegurarse que los paquetes que transitan al dominio estén apropiadamente marcados para seleccionar un PHB de los grupos implementados dentro del dominio. Los nodos seleccionan el comportamiento de envío basándose en su código DS, y lo hacen asociando éste valor a unos de los PHB soportados. Los servicios proporcionados a través de un domino DS, se definen en un acuerdo de nivel de servicio (SLA). La inclusión de nodos que no soportan Diffserv dentro de un dominio DS puede resultar en un desempeño impredecible y puede impedir la habilidad de satisfacer el acuerdo del nivel de servicio (SLA).

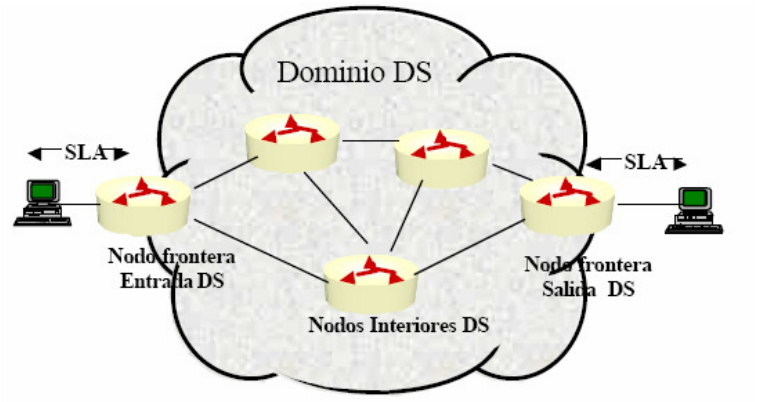

FIGURA VI.07 Dominio Diffserv

Un dominio DS consiste en general de una o más redes bajo la misma administración. Un Acuerdo de Nivel de Servicio (Service Level Agreement, SLA), es un contrato de servicios entre un proveedor de servicios y su cliente, el cual define las responsabilidades del proveedor en términos del nivel de funcionamiento de la red (rendimiento, tasa de pérdidas, retrasos, variaciones) y la disponibilidad temporal, el método de medida, las consecuencias cuando los niveles de servicio no se consiguen o si los niveles de tráfico definidos son superados por el cliente, así como el precio de todos estos servicios.

Evidentemente, y suele ser lo más común, el SLA puede incluir reglas de condicionamiento del tráfico.

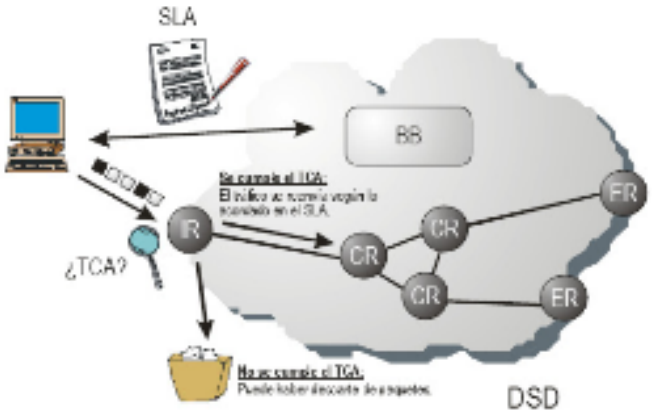

FIGURA VII.08 Diffserv – Service Level Agreement

2.2.2.1.1. Nodos DS de frontera e interiores

Los nodos DS de frontera interconectan el dominio DS con otros dominios que pueden o no soportar Diffserv. Los nodos interiores solo conectan con otros nodos interiores o de frontera dentro del mismo dominio DS.

Ambos tipos de nodos deben ser capaces de aplicar el PHB apropiado a los paquetes basándose en el código DS, sino, puede resultar en un comportamiento impredecible.

Los nodos DS de frontera puede que sean requeridos para desempeñar funciones de acondicionamiento de tráfico tal como se define en un Acuerdo de Acondicionamiento de Tráfico (TCA) entre su dominio DS y el dominio contiguo al cual conectan.

Los nodos DS interiores deben poder desempeñar otras funciones tales como el re-marcado de códigos DS y funciones más complejas de clasificación y acondicionamiento de tráfico que son análogas a las de los nodos DS de frontera.

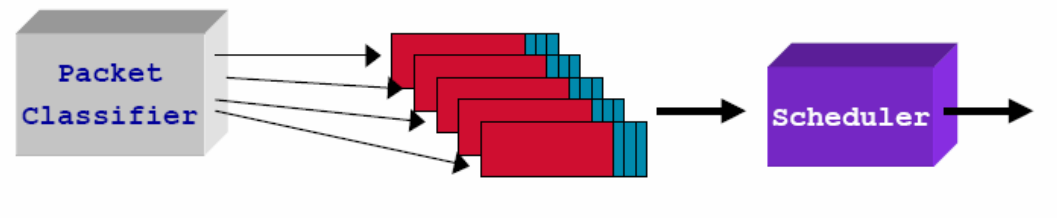

FIGURA VIII.09 Arquitectura de nodos DS Interiores

La clasificación de los paquetes se realiza de dos maneras dependiendo del tipo de cliente que esté conectado a los nodos de frontera. Cuando el cliente es una red de una organización, la clasificación o determinación de que PHB se le debe aplicar al paquete dentro de la red, se realiza tomando en cuenta los siguientes seis campos del paquete IP:

- ✓ Dirección IP de la fuente.
- ✓ Dirección IP del destino.
- ✓ Protocolo de transporte (TCP/UDP)
- ✓ Campo DiffServ (DS) en el paquete de llegada.

- ✓ Puerto del origen en el encabezado de TCP.
- ✓ Puerto destino en el encabezado de TCP.

Las reglas que mapean un paquete a un PHB determinado se llaman Reglas de Clasificación (classification rules). Las reglas de clasificación no necesariamente tienen que especificar los 6 campos. La regla puede ser una combinación de dos o más campos como por ejemplo, el protocolo de transporte y la dirección del puerto destino.

2.2.2.1.2. Nodos de Ingreso y Egreso

Los nodos de frontera actúan tanto como nodos DS de ingreso y egreso para el tráfico de distintas direcciones. Un nodo DS de ingreso es responsable por asegurar que el tráfico entrante al dominio DS cumpla con el Acuerdo de Acondicionamiento de Tráfico (TCA) entre éste y el dominio contiguo al cual está conectado el nodo de ingreso. Un nodo DS de egreso puede desempeñar funciones de acondicionamiento de tráfico para reenviarlo al siguiente dominio directamente conectado, dependiendo de los detalles del TCA entre los dos dominios.

2.2.2.2. Región de servicios Diferenciados (Región DS)

Una Región de Servicios Diferenciados es un conjunto de uno o más dominios DS contiguos. Las Regiones DS son capaces de soportar diferentes servicios a lo largo de una ruta la cual atraviesa los dominios dentro de la región. El dominio DS en una región DS, puede soportar diferentes grupos de PHB internamente. Sin embargo, para permitir servicios que se expanden a través de los dominios, los dominios DS contiguos deben cada uno establecer un Acuerdo de Nivel de Servicio (SLA), entre ellos que define (explicita ó implícitamente) cierta TCA, para especificar cómo el transito del tráfico de un dominio DS a otro es condicionado en la frontera entre los dos dominios DS. Es posible que algunos dominios dentro de una región puedan adoptar una política de provisión de servicios común y soportar un conjunto de grupos de PHB similares y de esta manera eliminar la necesidad de acondicionar el tráfico entre los dominios.

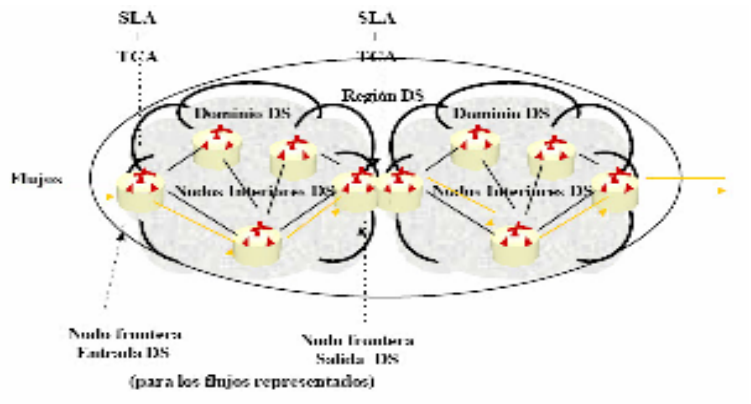

FIGURA II.10 Región Diffserv

2.2.2.3. Clasificación y Acondicionamiento del tráfico en un dominio DS

Los SLA pueden especificar la clasificación de paquetes y las reglas de remarcado y también pueden especificar los perfiles de tráfico y acciones para las cadenas de tráfico los cuales están dentro o fuera del perfil (in-out profile). El TCA entre los dominios proviene de éste SLA.

La política de clasificación de paquetes identifica el subconjunto de tráfico que puede llegar a recibir un servicio diferenciado, al ser condicionado y/o mapeado a uno o más comportamientos agregados dentro del dominio DS.

FIGURA IX.11 Vista lógica de un Clasificador y un Acondicionador de paquetes

El condicionamiento de tráfico desempeña la medición, conformación, política y/o remarcado, para asegurarse que el tráfico entrante al dominio DS respeta las reglas especificadas en el TCA, en concordancia con las políticas de provisión de servicios del dominio. El alcance del acondicionamiento de tráfico requerido depende del servicio específico ofrecido.

2.2.2.3.1. Clasificadores

Los clasificadores de paquetes seleccionan paquetes en una cadena de tráfico basándose en el contenido de alguna porción de la cabecera del paquete.

Se definen dos tipos de clasificadores.

- ✓ El Clasificador BA (Behavior Agregate), clasifica los paquetes basándose únicamente en el código DS.
- ✓ El MF (Multi-Archivo), clasifica a los paquetes basándose en el valor de uno o más campos de la cabecera del paquete, como puede ser la dirección origen, la dirección destino, número de puertos de origen y de destino e incluso el campo DS.

Los clasificadores son usados para distinguir los paquetes y hacer que coincidan con una regla específica y enrutarlos hacia un elemento acondicionador de tráfico para de esta manera darle un procesamiento adicional. Además los clasificadores deben estar configurados de acuerdo al TCA.

2.2.2.3.2. Perfiles de Tráfico

Especifica las propiedades temporales de una corriente de tráfico seleccionada por el clasificador. Provee de reglas para determinar si un paquete está dentro o fuera del perfil.

Diferentes acciones de condicionamiento pueden ser aplicadas a los paquetes dentro y fuera del perfil. Los paquetes dentro del perfil pueden ser mandados sin ningún otro procesamiento o marcado o remarcado. Los paquetes fuera de perfil pueden ser encolados hasta que estén dentro del perfil (conformados), desechados (política) o remarcados con un código nuevo (re-marcado).

Hay que hacer notar que el perfil de tráfico es un componente opcional de un TCA.

2.2.2.3.3. Acondicionador de Tráfico

Puede contener los siguientes elementos: medidor, marcador, conformador y despachador. Una cadena de tráfico es seleccionada por un clasificador. Un medidor es usado para medir la corriente de tráfico en base a

un perfil de tráfico. El estado del medidor respecto a un paquete en particular puede ser usado para afectar el marcado, despacho, o acción de conformación.

Cuando los paquetes salen del acondicionador de tráfico de un nodo DS frontera, el código DS de cada paquete debe setearse a un valor apropiado, según los requerimientos especificados por el usuario para ese tipo de tráfico.

2.2.2.3.3.1. Medidor

Miden las propiedades temporales de la cadena de paquetes seleccionada por el clasificador en base a un perfil de tráfico especificado en el TCA. Pasa información de estado a otras funciones de condicionamiento para tomar cierta acción para cada paquete tanto dentro como fuera del perfil.

2.2.2.3.3.2. Marcador

Setean el campo DS con un código particular, agregando el paquete marcado a un Behavior Agregate (BA). Puede que marque todos los paquetes que son dirigidos a él con un código particular o puede estar configurado para marcar un paquete a un código de un grupo de códigos usados para seleccionar un PHB en un grupo PHB. Cuando el marcador cambia el código en un paquete, se dice que ha "remarcado" el paquete.

2.2.2.3.3.3. Conformador

Retardan uno o todos los paquetes de una cadena de tráfico de manera de que la cadena cumpla con el perfil de tráfico estipulado. Usualmente tiene un buffer de tamaño finito y los paquetes pueden ser descartados si no hay suficiente espacio de buffer para aguantar a los paquetes retrasados.

2.2.2.3.3.4. Despachador

Descarta algunos o todos los paquetes en una cadena de tráfico, de manera que cumpla con el perfil de tráfico estipulado. Este proceso es conocido como "política". Un Despachador puede ser implementado como un

caso especial de un Conformador, si ponemos el tamaño del buffer del conformador igual a 0 paquetes, lo que quiere decir que no se almacenará ningún paquete, pues todos los paquetes que se conformen se enviarán inmediatamente.

2.2.2.3.4. Ubicación de los acondicionadores de tráfico o clasificadores MF

Los acondicionadores de tráfico están usualmente localizados dentro de los nodos DS de frontera de ingreso y egreso, pero pueden ser ubicados en los nodos dentro de un dominio DS o dentro de un dominio que no sea Diffserv.

2.2.2.3.4.1. Dentro del dominio origen

Se lo define como el dominio que contiene el nodo que origina el tráfico que recibe un servicio particular. El tráfico originado del dominio fuente a través de una frontera puede ser marcado por las fuentes de tráfico directamente o por medio de nodos intermediarios antes de que dejen el domino origen. Esto se conoce como "pre-marcado".

Por ejemplo, supongamos una compañía que tiene la política de que los paquetes de video, deben tener prioridad alta. El usuario puede marcar el campo DS de todos los paquetes de salida con un código DS que indique ese grado de prioridad alto, o alternativamente, el ruteador del primer salto, que está directamente conectado al host que genera estos paquetes, puede clasificar el tráfico y marcar los paquetes de video con el código DS correcto.

Hay ciertas ventajas en el hecho de marcar paquetes cerca del origen de tráfico. Primero, el origen del tráfico puede más fácilmente tomar en cuenta las preferencias de las aplicaciones en el momento de decidir qué paquetes deben recibir mejor tratamiento de envío. Además, la clasificación de paquetes es más simple, antes que el tráfico haya sido agregado a otros paquetes provenientes de otras fuentes, ya que el número de reglas de clasificación que deben ser aplicadas dentro de un nodo único es reducido.

El nodo frontera del dominio origen debe también monitorear la concordancia con el TCA, así como vigilar el conformado o re-marcado de paquetes según sea necesario.

2.2.2.3.4.2. En la Frontera de un Dominio DS

El tráfico puede ser clasificado, marcado y en otros casos condicionados en cualquiera de los enlaces de frontera entre dos dominios DS.

El Acuerdo de Nivel de Servicio (SLA), entre dominios, debe especificar cuál de ellos, tiene la responsabilidad de mapear el tráfico a agregados de comportamiento (BA) y acondicionar esos agregados en concordancia con el apropiado TCA.

Sin embargo, un nodo de ingreso debe asumir que el tráfico entrante puede no concordar con el TCA y debe estar preparado para reforzar el TCA de acuerdo a la política local.

Cuando los paquetes son pre-marcados y condicionados en un dominio superior, una clasificación y condicionamiento menores deben ser soportados en el dominio DS inferior.

Si un nodo de ingreso está conectado a un dominio superior que no soporta Diffserv (DS), el nodo de ingreso DS debe poder cumplir con todas las funciones de condicionamiento de tráfico necesarias para que el tráfico entrante al dominio superior pueda ser manejado adecuadamente.

2.2.2.3.4.3. Dominios que no soportan Diffserv

El tráfico de origen o los nodos intermedios en un Dominio que no soporta Diffserv, pueden emplear acondicionadores de tráfico para pre-marcar los paquetes antes de que estos alcancen el ingreso del siguiente dominio DS.

2.2.2.3.4.4. En nodos DS interiores

Aunque la arquitectura básica asume que la clasificación compleja y las funciones de acondicionamiento de tráfico están ubicadas únicamente en los nodos DS de frontera en el ingreso y egreso de la red, el desempeño de estas funciones en el interior de la red no está prohibido.

2.2.3. Definición del campo Differentiated Services (DIFFSERV)

Un campo de cabecera, llamado DS, es definido para los Servicios Diferenciados, el cual sustituye las definiciones existentes del octeto tipo de servicio (ToS) de IP versión 4 (IPv4) y del octeto Clase de Tráfico de IP versión 6 (IPv6), como se muestra en las FIGURAS II.11 y II.12

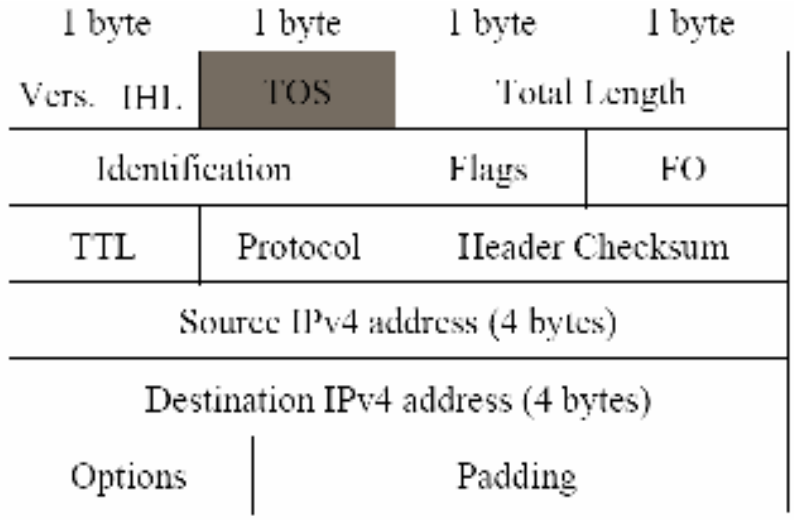

FIGURA X.12 Campo ToS de IPv4

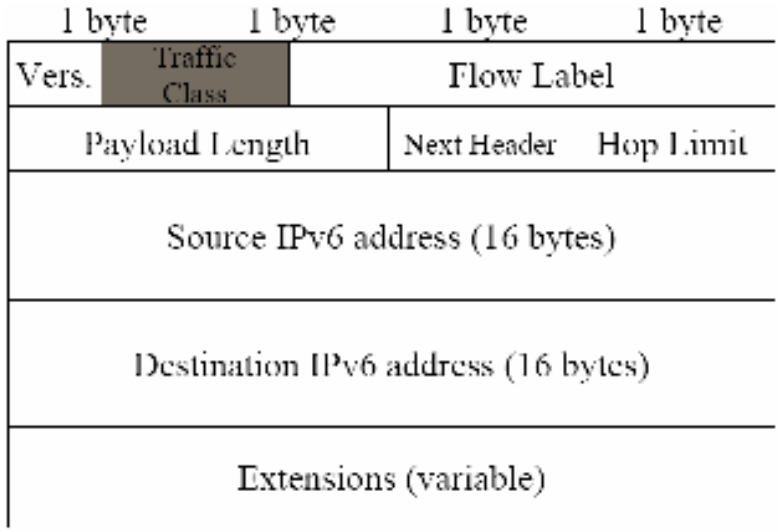

FIGURA XI.13 Campo TC de IPv4

Seis bits del campo DS se usan como un *codepoint* (DSCP) para seleccionar el PHB (Per Hop Behavior) en cada interfaz. Un campo actualmente no usado de 2 bits (CU) está reservado. El valor de CU es ignorado por los nodos que implementan Diffserv, cuando se determina el PHB que se aplicará a cada paquete.

La estructura del campo DS se indica a continuación:

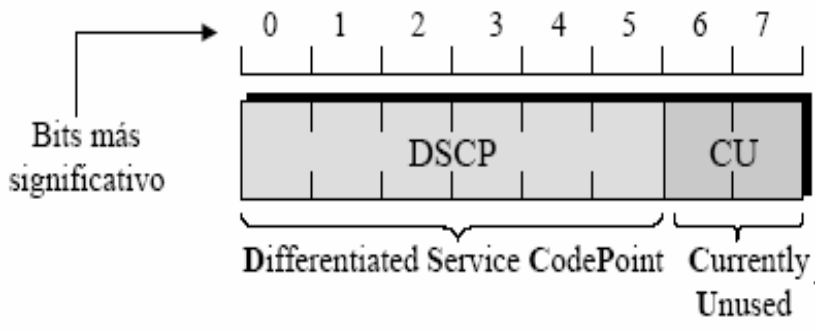

FIGURA XII.14 Campo DS

El campo DSCP dentro del campo DS es capaz de tener hasta 64 valores distintos. Estas 64 combinaciones están divididas en tres pools para propósitos de asignación y administración:

- ✓ Un pool de 32 códigos estandarizados (Pool 1).
- ✓ Un pool de 16 códigos (Pool 2), a ser utilizados para uso experimental o local (EXP/LU).
- ✓ Un pool de 16 códigos (Pool 3), los cuales inicialmente están disponibles para uso experimental o uso local, pero que pueden ser preferentemente utilizados para estandarización en caso de que el Pool 1 se use en su totalidad.

Los pools están definidos en la TABLA II.IV:

TABLA II.IV. Pool de Códigos DSCP

Pool	Código	Utilización
1	xxxxx0	Estandarizado
2	xxxx11	EXP/LU
3	xxxx01	EXP/LU (*)

La TABLA II.05, muestra las 64 combinaciones que puede tener el DSCP del campo DS: Cada código DSCP mapea un PHB determinado.

TABLA II.V. Códigos DSCP

DSCP	PHB	DSCP	PHB	DSCP	PHB	DSCP	PHB
000 000	CS0 (DB)	010 000	CS2	100 000	CS4	110 000	CS6
000 001	EXP/LU	010 001	EXP/LU	100 001	EXP/LU	110 001	EXP/LU
000 010	-	010 010	AF21	100 010	AF41	110 010	-
000 011	EXP/LU	010 011	EXP/LU	100 011	EXP/LU	110 011	EXP/LU
000 100	-	010 100	AF22	100 100	AF42	110 100	-
000 101	EXP/LU	010 101	EXP/LU	100 101	EXP/LU	110 101	EXP/LU
000 110	-	010 110	AF23	100 110	AF43	110 110	-
000 111	EXP/LU	010 111	EXP/LU	100 111	EXP/LU	110 111	EXP/LU
001 000	CS1	011 000	CS3	101 000	CS5	111 000	CS7
001 001	EXP/LU	011 001	EXP/LU	101 001	EXP/LU	111 001	EXP/LU
001 010	AF11	011 010	AF31	101 010	-	111 010	-
001 011	EXP/LU	011 011	EXP/LU	101 011	EXP/LU	111 011	EXP/LU
001 100	AF12	011 100	AF32	101 100	-	111 100	-
001 101	EXP/LU	011 101	EXP/LU	101 101	EXP/LU	111 101	EXP/LU
001 110	AF13	011 110	AF33	101 110	EF	111 110	-
001 111	EXP/LU	011 111	EXP/LU	101 111	EXP/LU	111 111	EXP/LU

2.2.3.1. Comportamiento por salto (Per-Hop-Behavior, PHB)

Un Comportamiento por salto (Per-Hop Behavior, PHB), es una descripción observada externamente del comportamiento de envío de un nodo DS, aplicada a un Comportamiento Agregado (Behavior Agregate) DS en particular.

Algunas distinciones de comportamiento son útiles cuando se observa que múltiples agregados de tráfico compiten por: recursos de buffer y ancho de banda en un nodo. El PHB es el medio por el cual un nodo asigna recursos a los agregados de comportamiento.

El ejemplo más simple de un PHB es uno que garantiza una mínima asignación de ancho de banda de un porcentaje X%, del enlace a un BA (sobre un intervalo razonable de tiempo). Este PHB puede ser medido en

forma justa y simple, bajo una variedad de condiciones de competencia de tráfico. Un PHB ligeramente más complicado sería garantizar una asignación de ancho de banda, de cualquier exceso de capacidad del enlace, con un reparto proporcional justo.

Los PHBs, pueden ser especificados en términos de su prioridad de recursos comparada con otros PHBs, o en términos de sus características relativas de tráfico observable.

Estos PHBs pueden ser usados como bloques de construcción para asignar recursos y deben ser especificados como un grupo (grupo PHB) para lograr consistencia. Un PHB único, definido aparte, es un caso especial de un grupo PHB.

Los PHBs son implementados en nodos por medio de algunos mecanismos de manejo de buffer y despacho de paquetes. Son definidos en términos de las características de comportamiento relacionadas a las políticas de aprovisionamiento de servicios, y no en términos de mecanismos de implementación particulares.

Es probable que más de un grupo PHB sea implementado en un nodo y sea utilizado dentro de un dominio.

Un PHB es seleccionado en un nodo por medio del mapeado del código DS en un paquete recibido. Los PHBs estándares tienen un código recomendado. Sin embargo, el espacio total de código es más largo (contiene 8 bits) que el espacio disponible (DSCP ocupa 6 bits) para los códigos recomendados para los PHBs estándar, y el campo DS deja provisiones para mapeos configurables localmente.

Todos los códigos deben ser mapeados a algún PHB, y en ausencia de alguna política local, los códigos que no están mapeados a un PHB estándar, deben ser mapeados a un PHB por defecto.

Los PHBs que se pueden utilizar son los siguientes:

- ✓ Comportamiento por omisión (Default Behavior)
- ✓ Selector de clase
- ✓ Tránsito expedito (Expedited forwarding)
- ✓ Tránsito asegurado (Assured forwarding)

Se definen dos PHB estandarizados (Tránsito expedito y Tránsito asegurado), uno por defecto (Default Behavior) y un PHB selector de clase.

2.2.3.1.1. PHB por Defecto (Default PHB)

Todos los nodos que implementen Diffserv deben tener disponible un PHB por "Defecto". Este es el comportamiento común que tienen los ruteadores existentes y que se trata del comportamiento de mejor esfuerzo. Cuando un paquete que ingresa al nodo no está marcado con un DSCP, lo que quiere decir que no pertenece a un PHB, se asume que estos paquetes pertenecen a este grupo.
Estos paquetes pueden ser enviados dentro de la red sin estar sujetos a una regla en particular y la red enviara la mayor cantidad de estos paquetes a la mayor brevedad posible, sujetos a otras políticas de recursos.

La implementación correcta de este PHB debería ser una disciplina de encolamiento, que envíe los paquetes marcados con este comportamiento, a la interfaz de salida cuando la misma no tenga que satisfacer los requerimientos de ningún otro PHB, es decir que estarían en al final del proceso de envío por la interfaz de salida. Una política razonable, a tener en cuenta, es que estos grupos no deben esperar indefinidamente para su reenvío, esto se puede lograr mediante un mecanismo en cada nodo que reserve un mínimo de recursos (buffer, ancho de banda, etc.) para este tipo de tráfico, o sea para este tipo de agregados de tráfico por defecto. Todo esto permite que los nodos que no soportan la implementación de Diffserv, puedan seguir funcionando dentro de la red como lo hacen hasta hoy.

El código DSCP recomendado para el PHB por Defecto es el siguiente, 000000, y este valor es mapeado a su PHB correspondiente. Este código es compatible con el valor existente en la práctica en los nodos que no implementan Diffserv. Si un DSCP no está mapeado a un PHB estandarizado o de uso local, este debe ser mapeado al PHB por Defecto. Un paquete inicialmente marcado con el DSCP para PHB por Defecto puede ser re-marcado con otro DSCP en la frontera entre dominios DS así que este será reenviado un diferente PHB dentro del dominio, posiblemente sujeto a algunas negociaciones entre los dominios contiguos.

2.2.3.1.2. Selector de Clase PHB (Class Selector PHB)

Este comportamiento define hasta ocho clases distintas en la red. El formato del código toma en cuenta los primeros 3 bits del campo DS, XXX000. Los tres primero bits representan un número del 0 al 7.

El número de menor valor representa una prioridad menor (es decir, los tres primeros bits son cero, el cual corresponde al PHB por Defecto o de mejor esfuerzo) mientras que un número mayor representa una prioridad mayor. No es necesario que un nodo (puede ser un nodo interno) soporte las ocho clases. Puede agrupar las clases para soportar por ejemplo 2 prioridades.

Los códigos con número 1 al 3 pueden representar una prioridad baja, mientras que los códigos con los números del 4 al 7 representan una prioridad alta. De esta forma, el nodo sigue siendo compatible con la especificación DiffServ, aún sin tener ocho clases definidas.

TABLA II.VI. Códigos para el selector de clase

Clase	Código	Clase	Código
0	000 000	4	100 000
1	001 000	5	101 000
2	010 000	6	110 000
3	011 000	7	111 000

2.2.3.1.3. PHB Tránsito Expedito (Expedited forwarding)

Como ya se mencionó, los nodos de red que implementan Servicios Diferenciados, usan un código en la cabecera IP para seleccionar un PHB, el cual le da un tratamiento de envío específico para los paquetes. El PHB Tránsito Expedito (EF PHB) puede ser usado para construir un servicio punto a punto de bajas pérdidas, baja latencia, bajo jitter (colas muy pequeñas) y ancho de banda asegurado, a través de dominios DS, por ello suele recibir el nombre de “Servicio Premium”.

Este servicio aparece en los puntos finales como una conexión punto a punto o como una “línea virtual alquilada”.

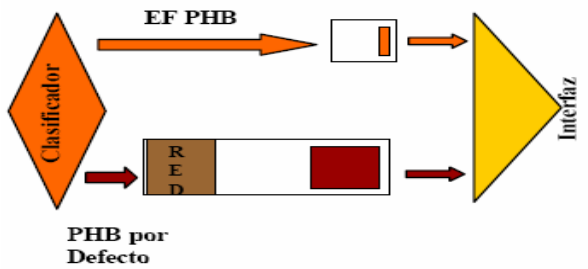

FIGURA XIII.15 Implementación del EF PHB con el PHB por defecto

Pérdidas, latencia y jitter son todos debidos al encolamiento que el tráfico experimenta mientras transita la red. Por lo tanto, el proveer bajas pérdidas, latencia y jitter para algunos agregados de tráfico, significa asegurarse que el agregado no vea ninguna, o por lo menos una pequeña cola, tal como se indica en GRÁFICO II.15.

Las colas se incrementan cuando la tasa o velocidad del tráfico entrante excede la tasa de salida en algún nodo. Así un servicio que asegura la no existencia de colas para algunos agregados, es equivalente a limitar la velocidad, tal que en cada nodo de tránsito en la red, la máxima velocidad de arribo de un agregado de tráfico sea menor que la velocidad mínima de salida del agregado de tráfico.

Crear un servicio como éste consta de dos partes:

1. Configurar los nodos de forma que el agregado de tráfico tenga una velocidad de salida mínima *bien definida*. (*bien definida* significa independiente del estado dinámico del nodo. En particular, independiente de la intensidad de otro tráfico en el nodo).

2. Acondicionar el agregado de tal manera que su tasa de llegada en cualquier nodo sea siempre menor que la tasa de salida mínima configurada para ése nodo.

El PHB Tránsito Expedito provee la primera parte para este servicio, mientras que los acondicionadores de tráfico en las fronteras de la red proveen la segunda parte.

Este PHB no es parte imperativa en la arquitectura Diffserv, lo que quiere decir que un nodo no necesita implementar el PHB Tránsito Expedito para ser considerado como un nodo que cumple con Diffserv. Otros

PHBs y grupos PHB pueden ser de utilizados, en el mismo nodo DS o dominio, con el PHB Tránsito Expedito.

2.2.3.1.3.1. Descripción del PHB Tránsito Expedido

El PHB Tránsito Expedito, es definido como un tratamiento de envío para un agregado de tráfico Diffserv particular, donde la tasa de salida de los paquetes del agregado de cualquier nodo Diffserv debe ser igual o exceder una velocidad ya especificada.

El tráfico con Tránsito Expedito debe recibir esta velocidad independiente de la intensidad de cualquier otro tráfico que intente transitar el nodo. Esta velocidad debe promediar al menos la velocidad configurada cuando se mide en cualquier intervalo de tiempo o ser mayor al tiempo que toma enviar un paquete MTU (Unidad Máxima de Transferencia) al enlace de salida a la velocidad configurada, esto significa que si tenemos una serie de paquetes del mismo tamaño que llegan a un nodo, éstos saldrán del nodo con la misma velocidad de entrada. La idea es reducir el exceso de retardo y jitter en lo posible.

La FIGURA II.16 nos muestra el principio de operación del EF PHB.

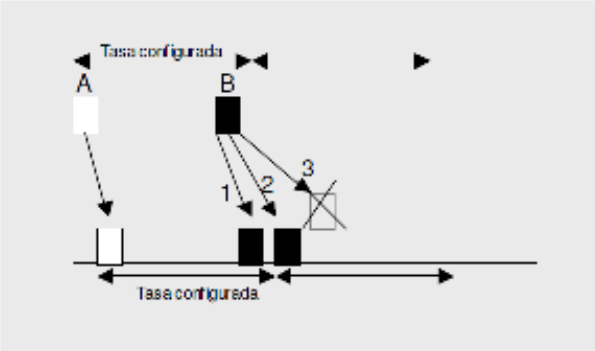

FIGURA XIV.16 Modelado y descarte de paquetes

Cuando el paquete llega antes de su tiempo programado de llegado, existen tres opciones en los nodos de ingreso e internos para su tratamiento:

1. Reenviar el paquete inmediatamente
2. Reenviar el paquete en el tiempo configurado
3. Descartar el paquete

Las opciones que toman los nodos de acceso e internos son diferentes: los nodos de acceso por lo general tomaran las opciones 2 y 3 para evitar que la fuente se apropie de un mayor ancho de banda del que se tiene configurado. Para los nodos internos, es altamente recomendada la opción 1, ya que la aplicación de la opción dos podría provocar retardos acumulados.

El DSCP 101110 es el recomendado para este PHB.

Los paquetes marcados con un EF PHB, pueden ser remarcados en el borde de un dominio DS solo con otro DSCP que satisfaga el EF PHB.

2.2.3.1.3.2. Mecanismos de ejemplo para implementar el PHB Tránsito Expedito

Varios mecanismos de despacho de cola pueden ser empleados para entregar el tipo de comportamiento descrito anteriormente, y así implementar el EF PHB.

Entre los cuales tenemos:

- ✓ Una cola con prioridad simple, la cual dará el comportamiento apropiado siempre y cuando no halla una cola con prioridad más alta, que pueda apropiarse del EF por más de un tiempo de paquete, a la tasa configurada.
- ✓ Planificador CBQ (Class Based Queue), que dé la prioridad al tráfico EF, hasta la velocidad ya establecida.

2.2.3.1.3.3. Consideraciones de Seguridad

Para protegerse de ataques de rechazos de servicios, la frontera de un dominio DS, debe estrictamente aplicar la política a todos los paquetes marcados EF, de manera que asegure, la tasa negociada con los dominios de frontera superiores.(Esta tasa debe ser menor o igual que la tasa de EF PHB configurada). Los paquetes en exceso de la tasa negociada deben ser descartados.

Si dos dominios adyacentes no han negociado una tasa EF, el domino inferior debe usar una tasa igual a 0, o sea descartar todos los paquetes marcados como EF.

Como el Servicio Premium punto a punto, descrito en el punto 1.2.3.1.3, construido a partir del EF PHB, requiere que el dominio superior establezca y aplique una política sobre el tráfico EF marcado, para conocer la tasa negociada con el dominio inferior, la política del domino inferior nunca debe dejar paquetes desechados. Así, cuando el dominio inferior descarte paquetes EF, estos descartes deben ser anotados como posibles violaciones de seguridad o serias desconfiguraciones.

2.2.3.1.4. PHB Tránsito Asegurado (Assured Forwarding)

El grupo PHB Tránsito Asegurado (AF PHB), provee el envío de paquetes IP en N clases AF independientes. Dentro de cada clase AF, a un paquete IP se le asigna uno de M diferentes niveles de *precedencia de descarte*. Un paquete IP que pertenece a una clase AF *i*, y tiene una precedencia de descarte *j* es marcado con un código AFij, donde 1<= i <= N y 1<= j <= M. En la actualidad existen cuatro clases (N = 4) con tres niveles de precedencia de descarte en cada clase (M = 3).

Un nodo DS debe implementar todas las cuatro clases AF. Los paquetes dentro

de una clase AF deben ser enviados independientemente de los paquetes que pertenecen a otra clase AF.

Un nodo DS debe configurarse con un mínimo de recursos, espacio en el buffer y ancho de banda, a cada clase AF implementada en el nodo.

Una clase AF también puede ser configurada para recibir más recursos de envío cuando los recursos exceden los requeridos por otras clases AF o de otros grupos PHB.

Dentro de una clase AF, un nodo DS no debe enviar un paquete IP que tiene un valor de precedencia de descarte menor (p) que un paquete que tiene una precedencia de descarte mayor (q). Esto se puede lograr sin necesidad de descartar los paquetes ya encolados.

Dentro de cada clase AF, un nodo DS debe aceptar los tres códigos de precedencias de descarte y estos deben proporcionar al menos dos niveles diferentes de probabilidad de pérdida. En algunas redes, particularmente en

redes empresariales, donde la congestión trasciende rara vez o en periodos muy cortos, puede ser razonable implementar solo dos niveles de probabilidad de pérdida en los nodos DS. Mientras que esto puede ser suficiente para algunas redes, tres niveles de probabilidad de pérdida deben ser soportados por los nodos DS dentro de un dominio DS donde la congestión es algo común.

Si un nodo DS solo implementa dos niveles de probabilidad de pérdida de paquetes para una clase AF x, el código AFx1 debe proporcionar la probabilidad de pérdida más baja y el código AFx2 y AFx3 deben proporcionar las probabilidades más altas de pérdida de paquetes.

Un nodo DS no debe reordenar los paquetes AF de un mismo flujo cuando estos pertenecen a la misma clase AF sin tener en cuenta su precedencia de descarte.

No hay requerimientos cuantificables de medir el tiempo de retardo o las variaciones de retardo, asociado con el envío de paquetes AF.

El grupo AF PHB puede ser usado para implementar el servicio extremo a extremo y domain edge – a – domain edge.

2.2.3.1.4.1. Acciones de Condicionamiento de Tráfico

En la frontera de un dominio DS se puede controlar la cantidad de tráfico de cada clase AF que entra o sale del dominio con varios niveles de precedencia de descarte. El control de tráfico puede implicar conformado, descarte, aumento o disminución de la precedencia de descarte y reasignación de paquetes a otras clases AF. Sin embargo no se debe realizar ninguna acción que implique el reordenamiento de paquetes de un mismo microflujo.

2.2.3.1.4.2. Comportamiento de colas y descarte de paquetes

La implementación del AF PHB debe minimizar la congestión de larga duración dentro de cada clase AF, y a la vez permitir las congestiones de corta duración causadas por las ráfagas de tráfico. Esto requiere de un algoritmo de administración de cola activa.

Un ejemplo de esta clase de algoritmo es el Descarte Temprano Aleatorio (Random Early Drop - RED).

La implementación de AF debe detectar y responder a las congestiones de larga duración en cada clase AF mediante el descarte de paquetes, mientras que el manejo de las congestiones de corta duración se maneja mediante el encolamiento de paquetes. Esto implica la presencia de funciones de filtrado que monitoree el nivel de congestión instantánea.

El algoritmo de descarte de paquetes debe tratar todos los paquetes dentro de una sola clase y nivel de prioridad idéntico. Esto implica que para un nivel de congestión dado, la tasa de descarte de los paquetes de un microflujo en particular que se encuentren dentro de un nivel de prioridad será proporcional al porcentaje de flujo del monto total del tráfico que atraviesa ese nivel de prioridad.

La notificación de congestión regresa a los nodos finales, y así el nivel de paquetes descartados de cada precedencia de descarte en relación a la congestión debe ser gradual y no abrupto para permitir a todo el sistema llegar a un punto estable de operación. Una forma de hacer esto es usando el algoritmo Random Early Drop (RED).

RED se basa en el descarte aleatorio de paquetes tras la detección temprana de la congestión, una vez superado un umbral del tamaño medio de la cola, el cual será explicado a continuación.

2.2.3.1.4.3. Algoritmo RED

A la llegada de un paquete se estima el tamaño medio de la cola de salida Q, como se indica en la FIGURA II.17:

- ✓ Si Q < umbral_min Funcionamiento normal: Almacenamiento del paquete.
- ✓ Si umbral_min < Q < umbral_max _ Evitar congestión: El paquete se descarta con prob. creciente linealmente con:

  Q: Pdrop=Pmax*(Q – umbral_min) / (umbral_max – umbral_min)
- ✓ Si Q > umbral_max _ Congestión: Se descarta el paquete.

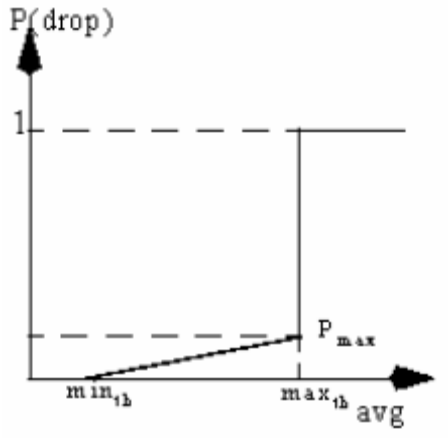

FIGURA XV.17 Algoritmo RED

El PHB Assured Forwarding (AF) PHB define un método por el cual los BAs pueden darse con diferentes garantías de envío hacia delante.

Por ejemplo, el tráfico de red puede clasificarse por ejemplo en un servicio denominado Servicio Olímpico, como se muestra en la FIGURA II.18, y que consta de las siguientes clases:

- ✓ Oro: El tráfico de esta categoría dispone del 50 % del ancho de banda.
- ✓ Plata: reserva el 30% del ancho de banda.
- ✓ Bronce: con el 20% del ancho de banda.

ORO→AF3j PLATA→AF2j BRONCE→AF1j

FIGURA XVI.18 Servicio Olímpico

Además, este PHB define cuatro clases: AF1, AF2, AF3, y AF4. A cada clase se le asigna una cantidad específica del espacio del buffer y ancho de banda de la interfaz, de acuerdo con la política establecida. En cada clase AF, se pueden especificar tres valores de precedencia: 1, 2 y 3.

Con lo cual los códigos DSCP recomendadas para uso general de las clases AFij, donde i corresponde a la clase y j corresponde a la precedencia, están dados a continuación:

AF11 = 001010 AF12 = 001100 AF13 = 001110

AF21 = 010010 AF22 = 010100 AF23 = 010110

AF31 = 011010 AF32 = 011100 AF33 = 011110

AF41 = 100010 AF42 = 100100 AF43 = 100110

Es importante señalar que no es necesario implementar los tres niveles de descarte. Si el operador de la red, no espera que existan muchas condiciones de congestión, el número de niveles de descarte se puede compactar a dos.

La TABLA II.VII, resume los valores DSCP recomendados para el PHB AF.

TABLA II.VII. Códigos DS recomendados para AS PHB

	Clase 1	**Clase 2**	**Clase 3**	**Clase 4**
Baja probabilidad de descarte	001010	010010	011010	100010
Media probabilidad de descarte	001100	010100	011100	100100
Alta probabilidad de descarte	001110	010110	011110	100110

2.2.3.1.4.4. Consideraciones de Seguridad

Para lograr protegerse a sí mismo de ataques de negación del servicio, el proveedor del dominio DS debe limitar el tráfico entrante al dominio a los perfiles subscritos. También, para poder proteger el enlace del consumidor de los ataques de negación de servicio en el dominio DS el proveedor del dominio DS debe permitir a los consumidores especificar como los recursos del enlace son ubicados en los paquetes AF. Sí el servicio ofrecido requiere que el tráfico marcado con un DSCP AF este limitado por algunos atributos tales como direcciones de origen y destino, es responsabilidad del nodo de ingreso a la red verificar la validez de dichos atributos.

2.3. EL PROTOCOLO DIFFSERV BAJO EL SISTEMA OPERATIVO LINUX

2.3.1. INTRODUCCIÓN

Sin duda una de las mayores ventajas del Sistema Operativo Linux es la facilidad de conectividad convirtiéndose en un buen servidor de red y coexistir con todas las configuraciones que ya tengamos trabajando dentro de nuestra red.

El entorno nativo de red del Sistema Operativo Linux, es el TCP/IP, por lo que la navegación en Internet y en general en redes basadas en esta familia de protocolos será muy fácil. El Sistema Operativo Linux puede actuar tanto de simple cliente hasta como una potente estación de trabajo a un bajo costo.

A nivel físico, el Sistema Operativo Linux puede conectarse con otros Sistemas Operativos Linux o con cualquier otro sistema, usando para ello cualquier interfaz física: cableado serie, paralelo, módems, tarjetas RDSI, Frame Relay, Ethernet o Token Ring, etc.

En cuanto a protocolos de red, ya hemos dicho que su entorno es TCP/IP, pero puede acceder a redes basadas en IPX (Novell), Apple Talk (Macintosh) SMB (Red LanManager para conectar con Windows para trabajo en grupo).

TCP/IP es un conjunto de protocolos, que permite a sistemas de todo el mundo comunicarse en una única red conocida como Internet. Con el Sistema Operativo Linux, TCP/IP y una conexión a la red, puede comunicarse con usuarios y computadores por toda la Internet, mediante correo electrónico, noticias (USENET news), transferencias de ficheros con FTP y mucho más.

Actualmente hay muchos Sistemas Operativos Linux, tanto clientes como servidores, que se encuentran conectados a Internet.

La mayoría de las redes TCP/IP usan Ethernet para la transmisión de datos. El Sistema Operativo Linux, da soporte a muchas tarjetas de red Ethernet e interfaces para computadores personales.

Pero dado que no todo el mundo tiene una conexión Ethernet en casa, el Sistema Operativo Linux también proporciona SLIP (Serial Line Internet Protocol), el cual permite conectarse a Internet a través de un modem.

Para poder usar SLIP, necesitará tener acceso a un servidor de SLIP, o sea un computador conectado a la red que permite el acceso de entrada por teléfono.

Muchas empresas y universidades tienen servidores SLIP disponibles. De hecho, si su Sistema Operativo Linux dispone de conexión Ethernet y de modem, puede configurarlo como servidor de SLIP para otros usuarios.

Servicios de almacenamiento de datos, servicio de impresoras y acceso a Internet, como servidor Web, mail y FTP, etc son algunos de los servicios para utilizar Linux.

Para entender como el Sistema Operativo Linux puede ayudarnos en nuestro intento de construir una arquitectura de Servicios Diferenciados, es muy importante primero entender como el Sistema Operativo Linux procesa los paquetes.

2.3.2. Flujo de tráfico en el sistema operativo Linux

En el Sistema Operativo Linux cada tarjeta de Red (NIC: Network Interface Card), es manejada por un Driver de Red, el cual controla el hardware. El driver de Red actúa como un mecanismo de intercambio de paquetes entre el código de interconexión del Sistema Operativo Linux y la red física.

FIGURA XVII.19 Diagrama de Bloques de interconexión entre el Sistema Operativo Linux y la red física

En este diagrama, el código de interconexión Sistema Operativo Linux puede pedir al driver de Red enviar paquetes a la red física, y viceversa. Esto nos interesa porque el Sistema Operativo Linux, se puede usar como un ruteador para re-enviar paquetes desde una interfaz a otra en el mismo computador, para lo cual se requiere de 2 NICs.

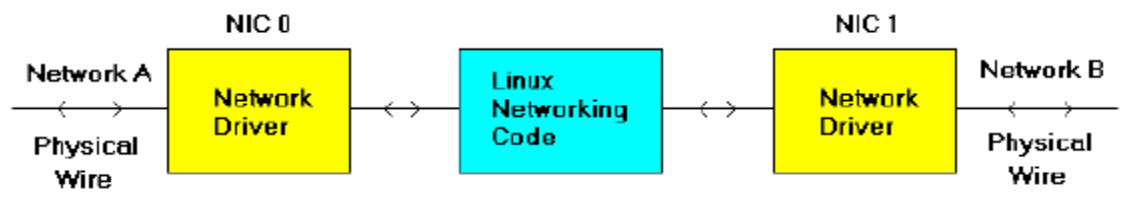

FIGURA XVIII.20 Diagrama de Bloques de un Computador con dos tarjetas de Red

Como vemos los paquetes pueden entrar desde la red física A a la NIC 0, el driver de Red de la NIC 0, le entrega los paquetes recibidos al código de Interconexión del Sistema Operativo Linux, en donde se solicita al driver de Red de la NIC 1 que re-envié los paquetes a la red física B o viceversa.

2.3.2.1. Mecanismos de interconexión del sistema operativo Linux

El de multiplexor de entrada examina los paquetes que ingresan para determinar si los paquetes están destinados para el nodo local, si es así estos son enviados a la siguiente capa más alta para procesamiento adicional, si no es así este envía los paquetes al bloque de re-envío.

El bloque de re-envío, el cual también puede recibir paquetes generados localmente desde la capa superior, busca en la tabla de ruteo y determina el siguiente salto para el paquete. Después de esto, encola el paquete para ser transmitido a la interfaz de salida. En este punto, el control de tráfico en Linux entra en juego.

El control de tráfico del Sistema Operativo Linux, puede ser usado para construir una combinación compleja de disciplinas de cola, clases y filtros que controlan los paquetes que son enviados en la interfaz de salida.

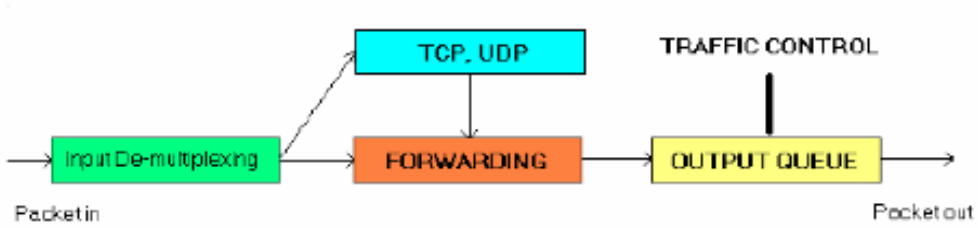

FIGURA XIX.21 Proceso de ingreso y salida de paquetes en la Red

El momento de utilizar el Sistema Operativo Linux como un ruteador, no interesa el procesamiento local de paquetes ya que no se aceptarán paquetes y no se van a generar paquetes de forma local, en este caso el Sistema Operativo Linux solo será un ruteador, el cual solo re-envía los paquetes o quizá los descarta.

2.3.2.2. Control de tráfico en el sistema operativo Linux

El proceso que sigue el núcleo del sistema operativo, para procesar los datos recibidos desde la red y generar nuevos datos para enviar a la red, se muestra en la FIGURA II.22, ahí podemos observar de manera aproximada que los paquetes que llegan a la interfaz de entrada son puestos para verificar que cumplan con las políticas.

Mediante la política se descartan los paquetes indeseables. Después los paquetes que cumplen las políticas son directamente enviados a la red o pasan a las capas superiores según la pila del protocolo para procesarlas. Estas capas superiores pueden también generar datos propios y pasarlos a las capas inferiores para las tareas de encapsulación, ruteo y eventualmente transmisión.

El *re-envío* implica la selección de la interfaz de salida, la selección del próximo salto, encapsulación, etc. una vez que todo esto se ha hecho, los paquetes son encolados en su respectiva interfaz de salida. Este es el segundo punto en donde el Control de Tráfico del Sistema Operativo Linux entra en acción.

El Control de Tráfico en el Sistema Operativo Linux puede, entre otras cosas, decidir si los paquetes son encolados ó si estos son desechados, un ejemplo de ello sería si la cola ha alcanzado una longitud límite, o si el tráfico excede una velocidad límite.

También puede decidir en qué orden se envían los paquetes, esto es útil para dar prioridad a ciertos flujos de datos, además puede retardar el envío de paquetes, etc. Una vez que el Control de Tráfico ha liberado un paquete para su envío el driver del dispositivo lo toma y lo envía a la red.

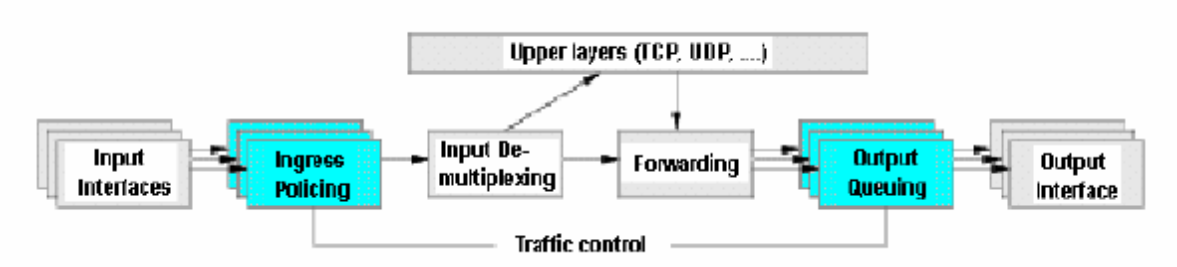

FIGURA XX.22 Procesamiento de datos de red

Como ya hemos dicho en el caso de que se use el Sistema Operativo Linux, solo como ruteador, la ruta de los paquetes será tal como se indica en la FIGURA II.23

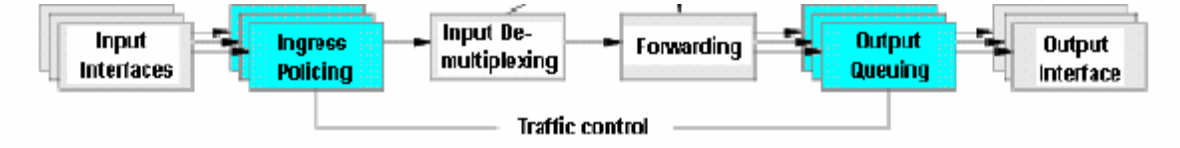

FIGURA XXI.23 Ruta de los paquetes a través de Linux

Como observamos, en los bloques celestes es en donde se ejerce el control sobre nuestros paquetes. Estos bloques son llamados *El código de control de tráfico del kernel del Sistema Operativo Linux*. Las políticas de entrada serán el primer punto de control; aquí se descartan los paquetes indeseables. El segundo punto será la cola de salida, aquí los paquetes son encolados y luego descartados, retrasados o priorizados de acuerdo a la regla que esté implementada.

El código de control de tráfico en el kernel del Sistema Operativo Linux, consiste en los siguientes componentes principales:

- ✓ Disciplinas de cola (queueing disciplines)
- ✓ Clases (dentro de una disciplina de cola)
- ✓ Filtros (filters)
- ✓ Vigilancia (policing y los conceptos relacionados)

Cada dispositivo de red tiene una disciplina de cola asociada a él, que controla como son tratados los paquetes encolados en ese dispositivo, tal como se indica en el GRÁFICO 3.6

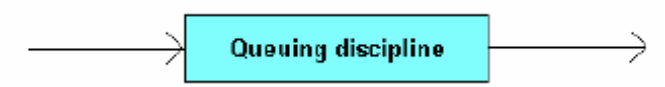

FIGURA XXII.24 Disciplina de cola simple sin clases

La disciplina de cola, a groso modo, describe la forma en que van a ser tratados los paquetes de datos dentro del buffer de la tarjeta de red.

Las disciplinas más elaboradas pueden utilizar filtros para distinguir entre diferentes clases de paquetes y procesar cada clase de una manera específica, por ejemplo, dando prioridad a una clase por encima de las otras.

La FIGURA II.25 muestra un ejemplo de esa disciplina de cola. Puede verse que varios filtros mapean a la misma clase.

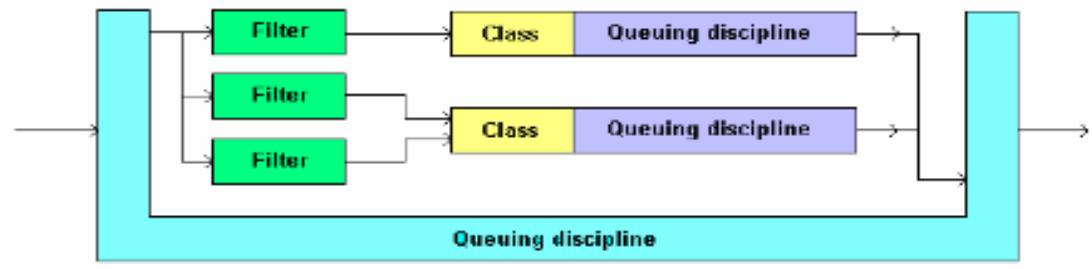

FIGURA XXIII.25 Disciplina de cola simple con múltiples clases

Las disciplinas de cola y las clases, están íntimamente relacionadas de la siguiente manera: la presencia de clases y sus semánticas son propiedades fundamentales de la disciplina de cola. En contraste con eso, los filtros pueden ser combinados arbitrariamente con disciplinas de cola y clases, sin importar si la disciplina de cola tiene clases o no.

Pero la flexibilidad no termina aún, las clases normalmente no almacenan sus paquetes ellas mismas, utilizan otra disciplina de cola para que se encargue de eso. Esa disciplina de cola puede ser elegida arbitrariamente de un conjunto de disciplinas de cola variadas y esas disciplinas pueden tener clases, y esas clases pueden utilizar disciplinas de colas y así sucesivamente, todo esto depende de los requerimientos que tenga la red.

Los paquetes son encolados de la siguiente manera: cuando se llama a la función de encolar, de una disciplina de cola, esta ejecuta los filtros, uno tras de otro hasta que, en alguno de ellos encuentre una coincidencia. Luego encola el paquete en la clase correspondiente, lo cual generalmente significa llamar a la función encolar de la disciplina de cola que está dentro de esa clase. Los paquetes que no coinciden con alguno de los filtros generalmente son asignados a una clase por defecto.

Típicamente, cada clase posee o es dueña de una cola, pero en principio también es posible que varias clases compartan la misma cola o que se utilice una sola cola para todas las clases de una disciplina de cola. Sin embargo es importante aclarar que los paquetes no cargan una identificación explícita de a que clase han sido asignados, por tanto las disciplinas de cola que cambian la información por clase, cuando desencolan los paquetes, pueden no trabajar correctamente si las colas “interiores” son compartidas, a menos que tengan la capacidad de repetir la clasificación del desencolado al encolado, que lleva a cabo en su interior, de alguna manera.

Usualmente cuando se encolan los paquetes, el flujo correspondiente puede ser vigilado, por ejemplo descartando paquetes que exceden cierta velocidad.

En la FIGURA II.26, se muestra como los elementos del control de Tráfico del Sistema Operativo Linux, se relacionan con la Arquitectura de Diffserv. Se puede notar que las clases pueden jugar dos roles, porque determinan el resultado final de una clasificación y también pueden ser parte de un mecanismo que implementa algún comportamiento de encolado o scheduling.

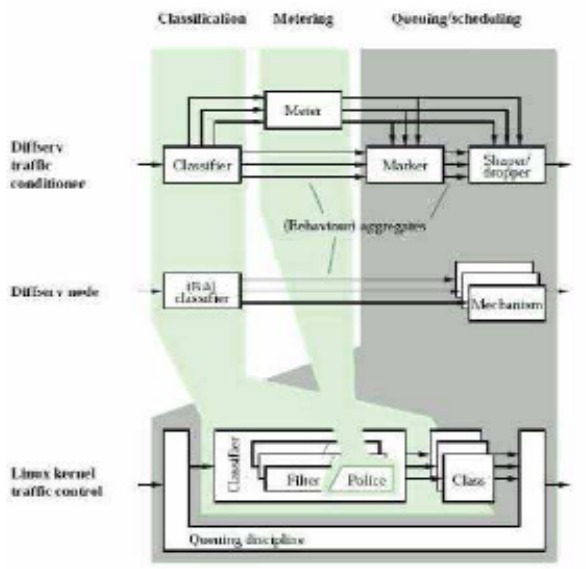

FIGURA XXIV.26 Relación de los elementos de la Arquitectura Diffserv con el Control de Tráfico del Kernel de Sistema Operativo Linux

2.3.2.2.1. Elementos del control del tráfico en sistema operativo Linux

2.3.2.2.1.1. Conformado (Shaping)

Un "shaper" o conformador retarda los paquetes para satisfacer una velocidad estipulada. Se utilizan para limitar el tráfico, de manera que no supere una velocidad, generalmente para suavizar el tráfico de ráfagas. Utilizan mecanismos de token bucket, el cual consiste en un algoritmo de regulación de tráfico, cuyo comportamiento se basa en el envío de testigos (tokes), a través del bucket (balde).

El bucket (balde) contiene testigos (tokens), que son generados a una tasa de *p* testigos por segundos, hasta un máximo de *C* testigos, de forma que cada testigo da derecho a transmitir un paquete. Así, este algoritmo permite ahorrar testigos cuando no hay datos que transmitir, para luego enviar ráfagas de al menos C paquetes.

2.3.2.2.1.2. Calendarizador (Scheduling)

Un "scheduler" o calendarizador ordena o desordena los paquetes antes de ser desencolados. Scheduling es el mecanismo por el cual los paquetes son ordenados o desordenados entre la entrada y la salida de una cola. Los mecanismos de scheduling, tratan de compensar varias condiciones de red. Un algoritmo del tipo "Encolado Justo" (Fair queuing - SFQ) intenta prevenir que un solo flujo se apodere del uso de la red. Un algoritmo tipo Round Robin (WRR), le da a cada flujo un turno para salida de la cola.

2.3.2.2.1.3. Clasificador (Classifying)

Los clasificadores ordenan o separan el tráfico entre colas. Clasificación es el mecanismo por el cual los paquetes son separados para tener diferente tratamiento, posiblemente diferente colas de salida.

En el Sistema Operativo Linux, el modelo permite que, un paquete fluya a través de una serie de clasificadores dentro de una estructura de control de tráfico y que sea clasificado de acuerdo a las políticas.

2.3.2.2.1.4. Políticas (Policing)

Los "policers" miden y limitan el tráfico en una cola en particular. Policing o políticas, como un elemento del control de tráfico, es simplemente un mecanismo por el cual el tráfico es limitado. Una política aceptará tráfico a una determinada velocidad, y luego realizará alguna acción si el tráfico excede la velocidad fijada. Una de las opciones puede ser que el tráfico sea descartado o puede ser reclasificado.

Una política es una pregunta tipo si/no acerca de qué hacer con el tráfico que ingresa en una cola. Si bien una política utiliza mecanismos de token bucket no tiene la capacidad de retardar el tráfico como un "shaper".

2.3.2.2.1.5. Descartador (Dropping)

Descarta un paquete, un flujo o una clasificación.

2.3.2.2.1.6. Marcador (Marking)

Es el mecanismo por el cual un paquete es alterado o marcado. No confundir con el marcado provisto por *fwmark* (marca de Firewall en Sistema Operativo Linux).

Los mecanismos de marcado del control de tráfico instalan una marca en el paquete mismo, la cual es usada y respetada por otros ruteadores dentro de un mismo dominio administrativo (DiffServ).

TABLA II.VIII. Componentes del Control del Tráfico en Sistema Operativo Linux

Elemento Tradicional	Componentes de Linux
Shaping	Una class ofrece capacidades de shaping.
Qdisc	Una qdisc (queue discipline) es un scheduler
Classifying	El objeto filter realiza la clasificación utilizando un objeto classifier. En Linux los classifiers no pueden existir fuera de los filter.
Policing	u-n policer solo existe como parte de un filter.
Dropping	Para hacer drop del tráfico se requiere un filter con un policer que utilice “drop” como acción.
Marking	Se utiliza dsmarkqdisc

CAPÍTULO III

3. IMPLEMENTACIÓN DE LOS PROTOTIPOS DE PRUEBA

3.1. INTRODUCCIÓN

El presente capítulo describe la implementación de los diferentes prototipos de prueba antes mencionados para lo cual empezaremos detallando las características de cada uno de los equipos planteados para de esta manera cubrir las necesidades y el buen funcionamiento de los escenarios Cisco y Linux.

En el transcurso de dicha implementación se presentará detalladamente todas las configuraciones necesarias desarrolladas en los equipos para posteriormente realizar las pruebas y obtener datos acordes a los parámetros de evaluación (jitter, retardo, pérdida de paquetes y ancho de banda).

3.1.1. Características de los equipos

A continuación detallaremos los equipos utilizados para la implementación del Escenario Cisco así como los equipos empleados para el Escenario Linux.

Escenario Cisco:

TABLA III.IX. Router Cisco 2811

Datos del producto	
Descripción del producto	CISCO 2811 Integrated Services Router – Encaminador - sobremesa
Tipo de dispositivo	Encaminador
Protocolos	
Protocolo de interconexión de datos	Ethernet, Fast Ethernet
Red/Protocolo de transporte	IPSec
Protocolo de gestión remota	SNMP3
Memoria	
Memoria Flash	64 MB
Memoria Interna	256 MB
Dimensiones	
Dimensiones	438.2 x 416.6 x 44.5 mm
Transferencia de datos	
Tasa de transferencia de datos (máx.)	0.1 Gbit/s
Velocidad de transferencia de datos	100 Mbits/s

TABLA III.X. Tarjeta WLAN Controller NME-AIR-WLC8-K9

Datos del producto	
Descripción del producto	Cisco Wireless LAN Controller Module - Adaptador de administración remota
Tipo de dispositivo	Adaptador de administración remota
Factor de forma	Módulo de inserción
Ethernet LAN (RJ-45) cantidad de puertos	1
Interfaz (bus)	NME
Dimensiones (An x P)	3,9 cm x 18 cm x 18.3 cm
Cumplimiento de normas	IEEE 802.1x, X.509, IEEE 802.11i
Diseñado para	Cisco 2811, 2811 de 2 pares, 2.811 de 4 pares, 2811 V3PN, 2821, 2821 de 4 pares, 2821 V3PN, 2851, 2851 V3PN, 3700, 3725, 3735, 3745, 3825, 3825 V3PN, 3845, 3845 V3PN

TABLA III.XI. Switch

Detalles técnicos	
Características técnicas	VLAN, auto MDI/MDI-X, IGMP
Conectividad	
Cantidad de puertos	24
Tecnología de cableado	10Base-T/100Base-TX/1000Base-T
Tecnología de conectividad	Con cables
Ranuras de expansión	2 (2) x SFP (mini-GBIC)
Puertos de entrada y salida (E/S)	2x host - 10Base-T/100Base-TX/1000Base-T - RJ-45
Dimensiones	
Factor de forma	1U
Dimensiones (Ancho x Profundidad x Altura)	445 x 236 x 44 mm
Protocolos	
Protocolos de gestión	SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP
Protocolo de conmutación	Ethernet
Protocolo de trasmisión de datos	Ethernet, Fast Ethernet
Red	
DHCP, cliente	✔
DHCP, servidor	✔
Transmisión de datos	
Tasa de transferencia (máx)	0.1 Gbit/s
Full dúplex	✔
Aprobaciones reguladoras	
Cumplimiento de estándares del mercado	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3ah
Características de manejo	
Tipo de interruptor	Administrado
Calidad de servicio (QoS) soporte	✔

Fuente: http://www.intelcompras.com/cisco-switch-cisco-catalyst-2960-puertos-10100-lite-p-49592.html

TABLA III.XII. Cisco Aironet 1300

Datos de los Productos	
Tipo de dispositivo	Punto de acceso inalámbrico
Tipo incluido	Externo
Dimensiones (Ancho x Profundidad x Altura)	20.3 cm x 20.6 cm x 7.9 cm
Conexión de redes	

TABLA III.XII. Cisco Aironet 1300 (Continuación)

Protocolo de interconexión de datos	**IEEE 802.11b, IEEE 802.11g**
Protocolo de gestión remota	SNMP 1, SNMP 2, Telnet, HTTP
Velocidad de transferencia de datos	54 Mbps
Banda de frecuencia	2,4 GHz
Número de canales seleccionables	11
Características	Soporte DHCP, soporte VLAN, activable, Quality of Service (QoS)
Método de autentificación	RADIUS
Cumplimiento de normas	IEEE 802.11b, IEEE 802.11g, IEEE 802.11x
Expansión / Conectividad	
Interfaces	1 x antena – RP-TNC| 1x red – Ethernet 10Base-T/100Base-TX_RJ45| 1X red-consola

Escenario Linux:

TABLA III.XIII. Router Linksys

Detalle del producto	
Marca	Linksys
Modelo	WRT310N
Puertos	4 10/100 RJ-45 Ports
Estándares	IEEE 802.3 10BASE-T, EEE 802.3 10BaseT ETHERNET
Protocolos	CSMA/CD, Star, DHCP, PPPoE

TABLA III.1. Portátiles

Características equipo	
Edición de Windows	Windows 7 Home Premium
Sistema	
Modelo	VAIO Computer
Procesador	Intel(R) Core(TM) i5-2430M CPU 2,40 GHz
Memoria instalada (RAM)	8,00 GB
Tipo de sistema	Sistema operativo de 64 bits

3.2. Estructura de la WLAN

La WLAN está formada a través de la conexión de un Router Cisco 2811 el cual tiene incorporado una tarjeta WLAN Controller y estos a su vez se conecta a un Switch Cisco 2960 el mismo que dispone de una conexión hacia otros servidores (Servidor de correo electrónico, Servidor FTP, Servidor Web, Servidor de Videollamadas).

Además la red cuenta con equipos Aironet Cisco 1300, estos dispositivos permiten la conexión inalámbrica entre los equipos mencionados. A través de esta conexión es posible que los clientes se comuniquen de manera inalámbrica y se haga posible la videollamada.

En cuanto al escenario Linux, la red consta de un router Cisco Linksys el cual está conectado a un Servidor Elastix (Central Telefónica), a través de los cuales los clientes debidamente registrados tienen acceso a videollamadas (Softphone X-Lite).

Adicionalmente por motivos de captura y análisis de datos se dispone de otros Servidores como son:

- Servidor de Correo Electrónico
- Servidor Web
- Servidor FTP

A través de su funcionamiento se aumentará el tráfico a las videollamadas las cuales serán debidamente analizadas con la herramienta Wireshark que es un capturador/analizador de paquetes de red el mismo que permite ver, aun nivel bajo y detallado, qué está pasando en la red.

3.2.1. Configuración de QoS en los Equipos Cisco

Observación: El Escenario con equipos Cisco no pudo ser concluido ya que la tarjeta Wireless Lan Controller si bien existe la misma, no se encuentra en buenas condiciones por lo que se hace imposible concluir la investigación en dichos equipos en la Figura III.28 y III.29 está demostrado y debidamente expuesta la nulidad de la tarjeta PERO realizaremos la demostración de la hipótesis apoyándonos totalmente en el escenario con equipos Linux el mismo que fue concluido satisfactoriamente en su totalidad.

3.2.1.1. Guías de Implementación

Configuración del módulo de red inalámbrica de Cisco controlador en un Router Cisco

La Cisco LAN inalámbrica (WLAN) y el módulo de controlador de red (WLCM) están diseñados para ofrecer soluciones de redes inalámbricas para Cisco serie 2800 y Cisco serie 3800, Routers de Servicios Integrados (ISR) y Cisco Serie 3700.

El sistema operativo de Cisco WLCM permite gestionar desde 8 a 12 puntos de acceso WLAN (APS) y simplifica la implementación y administración de redes LAN inalámbricas. El sistema operativo administra todos los datos de cliente, las comunicaciones y las funciones de administración del sistema, realiza la gestión de las funciones de los recursos de radio (RRM), gestiona todo el sistema de políticas de movilidad que utilizan el sistema operativo de seguridad (OSS), y coordina todas las funciones de seguridad utilizando el marco de OSS. El WLCM Cisco trabaja en conjunto con Cisco Aironet puntos de acceso ligeros de Cisco Wireless Control (WCS), y el aparato inalámbrico de Cisco Ubicación (WLA) para apoyar a los datos inalámbricos, voz y aplicaciones de video.

Requisitos previos para la configuración de la WLCM de Cisco en un Router Cisco

El sistema operativo Cisco WLCM debe ser compatible con la versión del software Cisco IOS y el conjunto de características del Router.

Para ver la versión del Cisco IOS en el router y para ver la versión del sistema operativo en el WLCM se utiliza los siguientes comandos:

- Para ver la versión del software Cisco IOS y el conjunto de funciones, se digita el comando "show versión" en el modo privilegiado en el router.
- Para ver la versión del sistema operativo Cisco WLCM, se digita el comando show sysinfo.

Información acerca de la WLCM de Cisco en un router Cisco

El WLCM Cisco es compatible con las plataformas de routers siguientes:

- Cisco 3725 y los routers 3745
- Routers Cisco 2811, 2821 y 2851 de Servicios Integrados
- Router Cisco 3825 y 3845 de Servicios Integrados

Cisco WLCMs se suministran con un gestor de arranque y una tarjeta de 512 MB de memoria CompactFlash.

La tarjeta de memoria Compactflash contiene un gestor de arranque, el kernel de Linux, Cisco WLCM, el archivo ejecutable de los puntos de acceso, el software de actualización, y la configuración de Cisco WLCM.

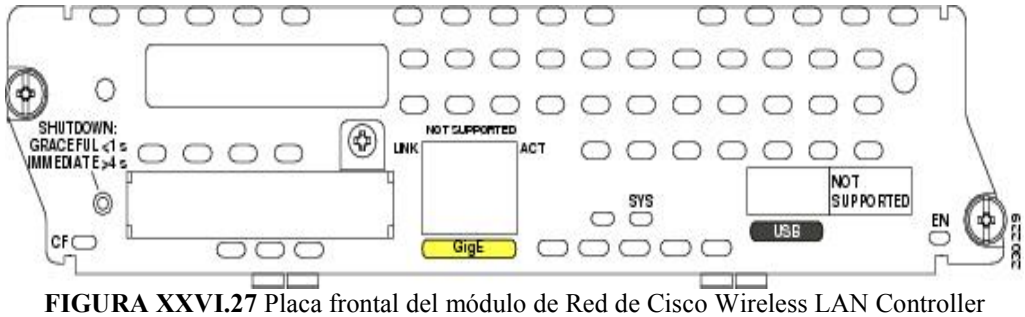

FIGURA XXVI.27 Placa frontal del módulo de Red de Cisco Wireless LAN Controller

Interfaces del sistema operativo del usuario

El WLCM Cisco y sus puntos de acceso asociados de Cisco pueden ser administrados por las siguientes interfaces:

Interfaz de línea de comandos (CLI) –El CLI es una herramienta completa, pero simple basada en texto, con estructura de árbol de interfaz que permite que hasta cinco usuarios con capacidad Telnet y emuladores de

terminal manejen simultáneamente todos los aspectos de la Cisco WLCM y a los puntos de acceso Cisco. Nos permite configurar de manera local o remota, supervisar y controlar cada WLCM de Cisco.

Cisco WLCM interfaz web, la interfaz de usuario de la web se construye en cada Cisco WLC. La interfaz de usuario de la web permite hasta cinco usuarios navegar al mismo tiempo, configurar los parámetros, y controlar el estado operativo de Cisco Wireless LAN Controller y los puntos de acceso asociados.

Debido a que la interfaz de usuario de la web funciona con una WLC a la vez, la interfaz de usuario de la web es especialmente útil cuando se desea configurar o monitorear un solo Cisco Wireless LAN Controller y sus puntos de acceso asociados que admiten el Protocolo ligero de punto de acceso (LWAPP) . La interfaz web es compatible con Internet Explorer, versión 6.0 Standard Edition y Enterprise Edition (SP1) o posterior.

Cisco WCS: Es una aplicación de software basada en navegador que ofrece la capacidad de administrar varias implementaciones del controlador a través de una única interfaz. El WCS Cisco se ejecuta en Windows 2000, Windows 2003 y Red Hat Enterprise Linux ES servidores.

El WCS Cisco incluye la misma configuración, monitoreo del desempeño, seguridad, gestión de fallos, y las opciones de contabilidad que se utilizan en el nivel de Cisco Wireless LAN Controller, pero añade una vista gráfica de varios controladores y puntos de acceso controlado.

Configuración de la WLCM

Acceso a la CLI a través de una conexión de consola o Telnet

Antes de poder acceder a la CLI de Cisco WLCM, primero se utilizó uno de estos métodos para establecer una conexión desde el router de acogida:

Conectar a la consola del router mediante Telnet o SSH, y abrir una sesión con el módulo con el comando:

service- module integrated –service-engine *slot/unit sesión*

El router debe tener conectividad de red con el Telnet o SSH permitido a los clientes. Después de conectar a través de la CLI, a través de una sesión Telnet, o por medio de una sesión SSH, el usuario aparece en la estación de administración.

El WLCM Cisco (NME-AIR-WLC8-K9 y NME-AIR-WLC12-K9) admite el comando **integrated-service-engine slot/sport** en la interfaz en modo de configuración mientras que El WLCM Cisco (NME-AIR-WLC8-K9 y NME-AIR-WLC12 K9) admite el comando **wlan-controller slot/port**

El software ajusta automáticamente el valor de puerto a puerto 1. Por lo tanto, no hay necesidad de configurar manualmente el puerto.

Configuración del Router Cisco en el WLCM

A continuación presentaremos una guía de cómo realizar la configuración inicial del router con un WLCM instalado de igual manera la configuración inicial de la WLCM:

Router# enable

Router# configure terminal

Router(config)# interface integrated-service-engine 1/0

Router(config-if)# ip address 192.0.2.254 255.255.255.0

Router(config-if)# no shutdown

Router(config-if)# end

Router# service-module integrated-service-engine 1/0 session

Al ejecutar el asistente de Configuración

Cuando arranca el controlador con los valores de fábrica, el script de inicio ejecuta el asistente de configuración, que le pide el instalador para la configuración inicial.

Después de la interfaz de Cisco WLCM se ha configurado y que haya arrancado la imagen WLCM, usted puede alternar entre el router y el módulo presionando **Control-Shift-6** , seguido de **x**

Welcome to the Cisco Wizard Configuration Tool

Use the '-' character to backup

WLCM:# **anyname**

Enter Administrative User Name (24 characters max): **anyname**

Enter Administrative Password (24 characters max): *****

Management Interface IP Address: **192.168.2.2**

Management Interface Netmask: **255.255.255.0**

Management Interface Default Router: **192.168.2.1**

Management Interface VLAN Identifier (0 = untagged): **0**

Management Interface Port Num [1]: **1**

Management Interface DHCP Server IP Address: **192.168.2.2**

AP Manager Interface IP Address: **192.168.2.3**

AP-Manager is on Management subnet, using same values

AP Manager Interface DHCP Server (192.0.2.24): **192.168.2.2**

Virtual Gateway IP Address: **1.1.1.1**

Mobility/RF Group Name: **anyname-mg**

Network Name (SSID): **wlan-15**

Allow Static IP Addresses [YES][no]: **no**

Configure a RADIUS Server now? [YES][no]: **no**

Warning! The default WLAN security policy requires a RADIUS server.

Please see documentation for more details.

Enter Country Code (enter 'help' for a list of countries) [US]: **EC**

Enable 802.11b Network [YES][no]: **yes**

Enable 802.11a Network [YES][no]: **yes**

Enable 802.11g Network [YES][no]: **yes**

Enable Auto-RF [YES][no]:

Configure an NTP server now? [YES][no]: **yes**

Enter the NTP server's IP address: 192.0.2.24

Enter a polling interval between 3600 and 604800 secs: 3600

Configuration correct? If yes, system will save it and reset. [yes][no]: **yes**

Configuration saved!

Resetting system with new configuration...

User:

Configure a NTP server now? [YES][no]: **no**

User: **tesis2**

Password: *********

(WLCM)

Configuración de la interface de administración de la WLCM y la interface de administración AP

Se puede crear cualquier número de interfaces lógicas estáticas o dinámicas en la WLCM Cisco, configurados como interfaces VLAN etiquetadas o interfaces sin etiquetar. Por defecto, dos interfaces estáticas sin etiquetar se asignan (*interfaz de gestión* y de *interfaz de gestión AP*) y se utiliza para la gestión y la comunicación con los puntos de acceso. Debido a estas interfaces no tienen etiqueta, que debe ser asignado a la misma subred que se utiliza para configurar la interfaz de WLCM en el router.

WLCM> configure interface address management 192.168.2.2 255.255.255.0 192.168.2.1

WLCM> configure interface address ap-manager 192.168.2.3 255.255.255.0 192.168.2.1

La última dirección (192.168.2.1) es la dirección por defecto del Gateway para esas interfaces y la dirección IP de la interface del WLCM en el router.

Se envía un ping del router a la interface de administración del WLCM

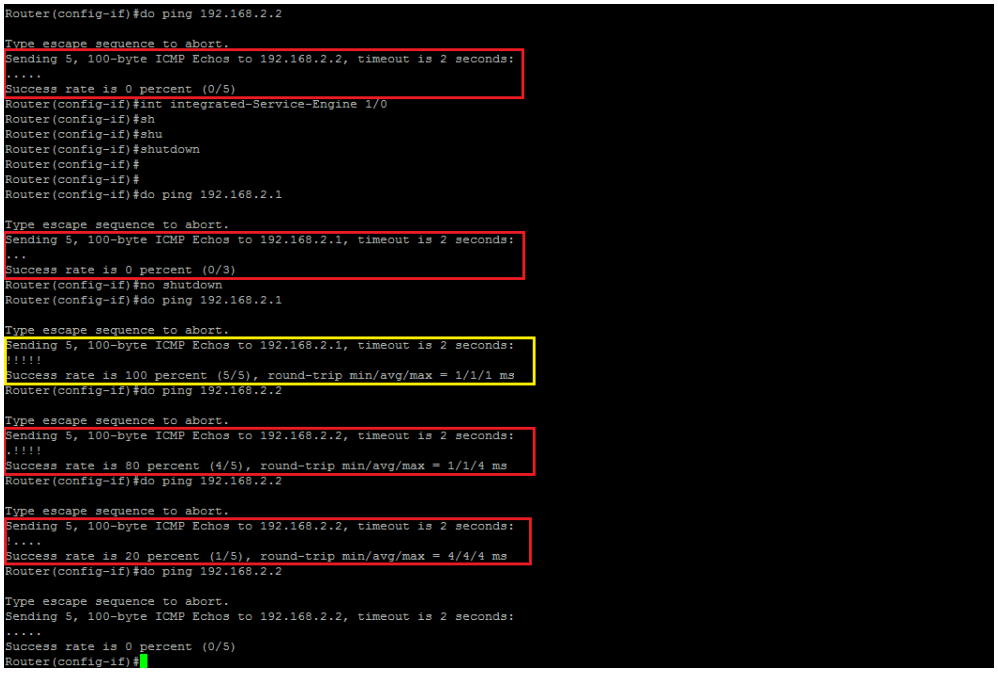

FIGURA XXVI.28 Ping del Router a la administración WLCM

Segundo Experimento

WLCM> configure interface address management 192.168.100.2 255.255.255.0 192.168.100.1

WLCM> configure interface address ap-manager 192.168.100.3 255.255.255.0 192.168.100.1

La última dirección IP (192.168.100.1) es la dirección IP por defecto-puerta de entrada para las interfaces y la dirección IP de la interfaz WLCM en el router.

Enviar un ping desde el router a la dirección de gestión que fue configurada en este segundo experimento.

Router:# ping 192.168.100.2

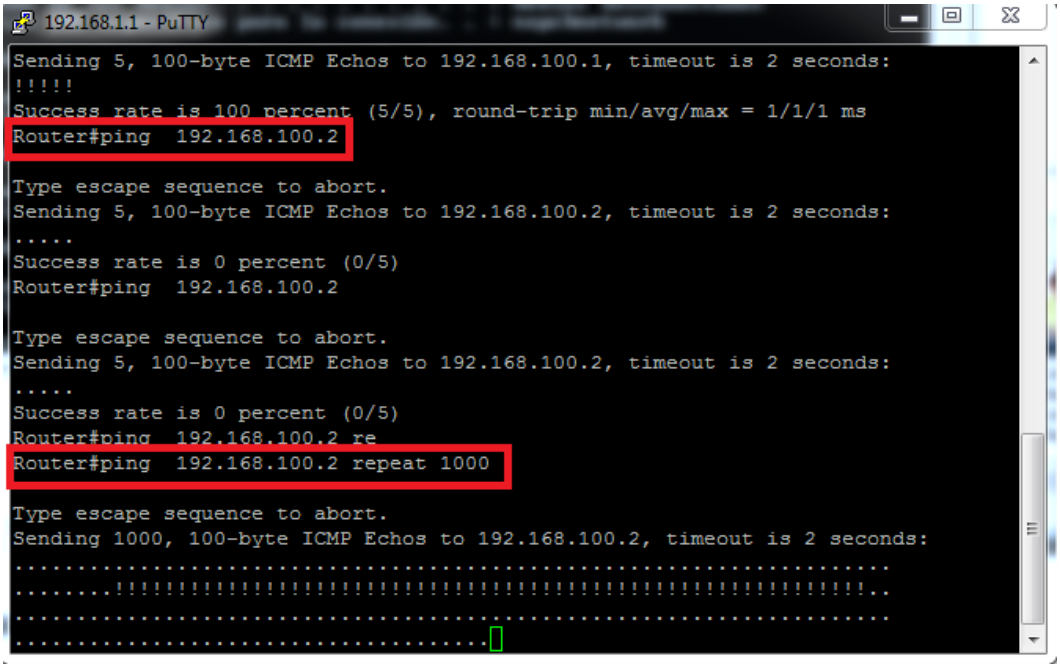

FIGURA XXVII.29 Ping a la dirección configurada

Como anexo encontraremos las configuraciones realizadas que fueron respaldadas con la idea de poder restaurarla, exactamente tal cual estaba al momento de la creación del backup. El procedimiento de restauración asume que la configuración será colocada en el mismo router, donde fue creado originalmente el backup, y también creará configuraciones dañadas parcialmente si el hardware ha sido cambiado.

La configuración puede ser exportada total o parcialmente en la pantalla de consola o en un archivo de texto (script), el cual puede ser descargado desde el router usando el protocolo FTP.

3.2.2. Configuración de QoS en los Equipos Linux

CONFIGURACIÓN DEL ROUTER

DD-WRT

Es un firmware libre para diversos routers inalámbricos o WIFI, es muy común observarlo en equipos Linksys WRT54G (incluyendo los modelos WRT54GL, WRT54GS y WRT54G2). Ejecuta un reducido sistema operativo basado en Linux. Está licenciado bajo la GNU General Public License versión 2.

DD-WRT es mantenido por BrainSlayer en dd-wrt.com. Las versiones hasta la v22 estaban basadas en el firmware Alchemy de Sveasoft, que a su vez estaba basado en el firmware original de Linksys. Desde la v23 en adelante están basadas en OpenWrt, que empezó siendo un firmware basado en el de Linksys pero más tarde cambió a su propio framework. Todos los firmwares están basados en Linux. DD-WRT, OpenWrt y Alchemy también incluyen otros proyectos de código abierto.

Aparte de otras características que no se encuentran en el firmware original de Linksys, DD-WRT incluye el demonio de la red de juego Kai, IPv6, Sistema de Distribución Inalámbrico (WDS), RADIUS, controles avanzados de calidad de servicio (QoS) para la asignación de ancho de banda y control de potencia (con un ajuste posible de hasta 251mW, mucho mayor que la potencia por defecto del router).

TABLA III.XV. DD-WRT

DD-WRT	
Desarrollador	BrainSlayer www.dd-wrt.com
INFORMACIÓN GENERAL	
Última versión estable	v24 SP1 26/07/2008
Género	SO para router
Sistema operativo	Linux
Licencia	GPL

Proceso de Flasheo

- Bajar el firmware DD-WRT de la sección descargas de DD-WRT

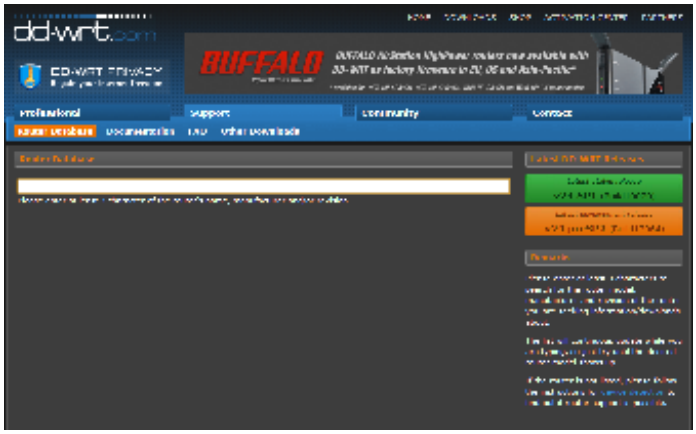

FIGURA XXVIII.30 Firmware DD-WRT

- Extraer el archivo. Una vez bajado y extraído desde el archivo zip, deberás ver algo como esto:

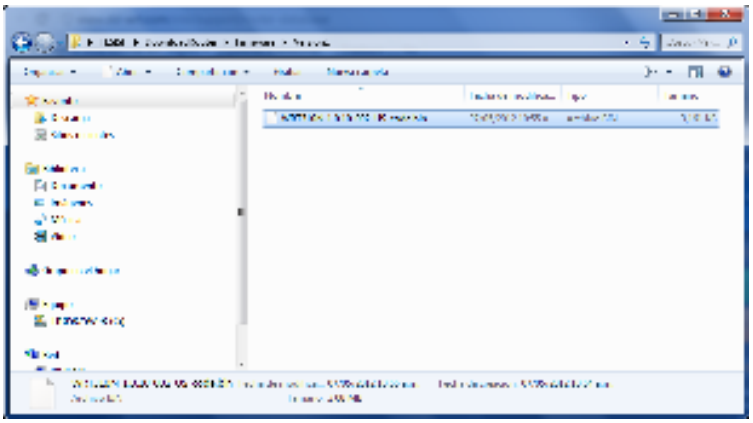

FIGURA XXIX.31 Extracción del archivo

Resetea vía Interfaz Web

Desde un PC conectado a uno de los 4 puertos LAN en el router abre un explorador de internet y pon la IP del router (La IP por defecto es 192.168.1.1).

FIGURA III.32 Ingreso de IP del router y Password

- A continuación se deberá ingresar por usuario y contraseña. El usuario no es requerido, ingresa la contraseña (la contraseña por defecto es *admin*) y deberás estar en la interface web.

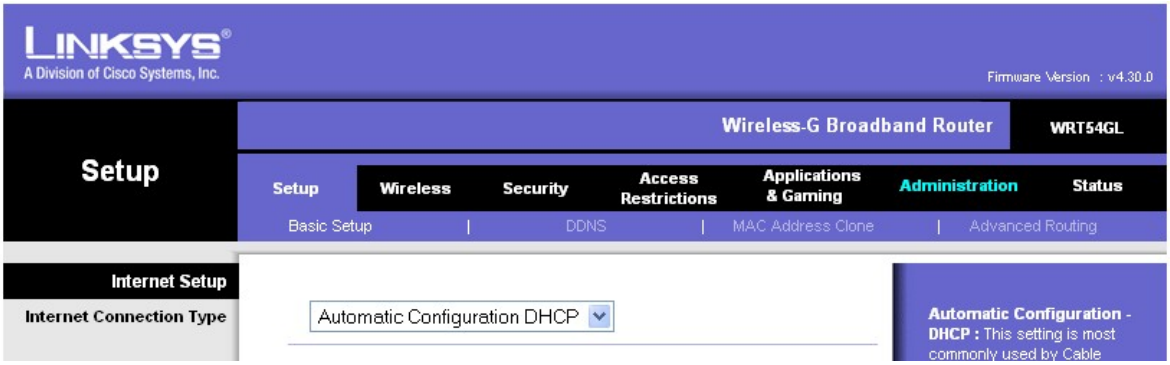

FIGURA XXX.33 Ingreso de Contraseña

- Has click en la pestaña "Administration".

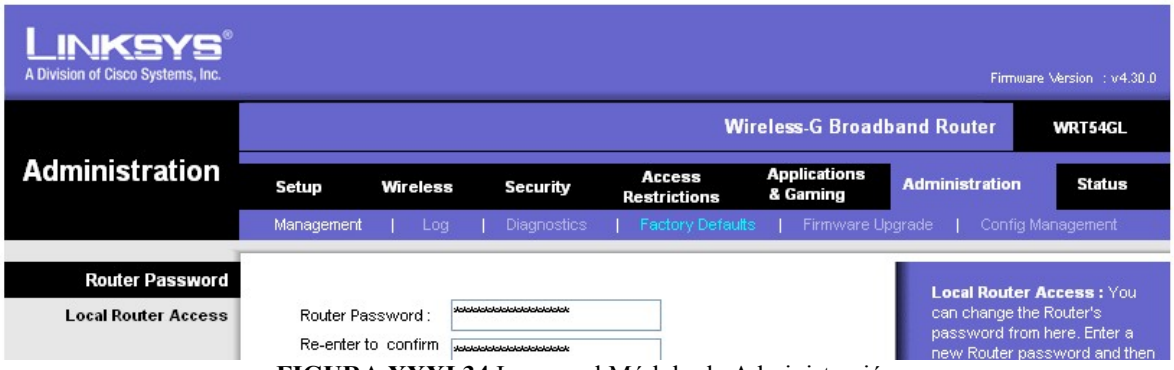

FIGURA XXXI.34 Ingreso al Módulo de Administración

- Has click en la sub-pestaña "Factory Defaults".
- Selecciona "Yes".

FIGURA III.35 Activación de "Factory Defaults".

- Has click en el botón "Save Settings".
- Aparecerá una advertencia, has click en "aceptar".

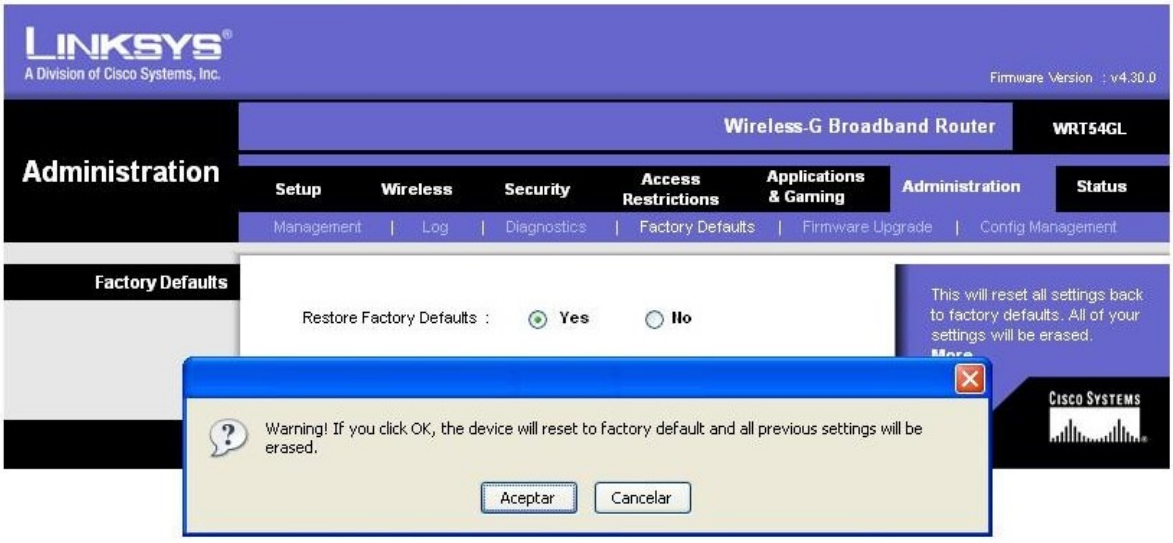

FIGURA XXXII.36 Guardar cambios

1) Actualizar Firmware

- Desde un PC conectado a uno de los 4 puertos LAN del router abre un explorador de internet y anda a IP 192.168.1.1.

FIGURA XXXIII.37 Ingreso al Router con Explorador de Internet

- Se te preguntará un nombre de usuario y contraseña. Deja el usuario en blanco y entra la contraseña *admin*. Ahora deberás estar en la interface web del router.

FIGURA XXXIV.38 Interface web del Router

Has click en la pestaña "Administration"

FIGURA XXXV.39 Módulo de Administración

- Has click en la sub-pestaña "Firmware Upgrade".

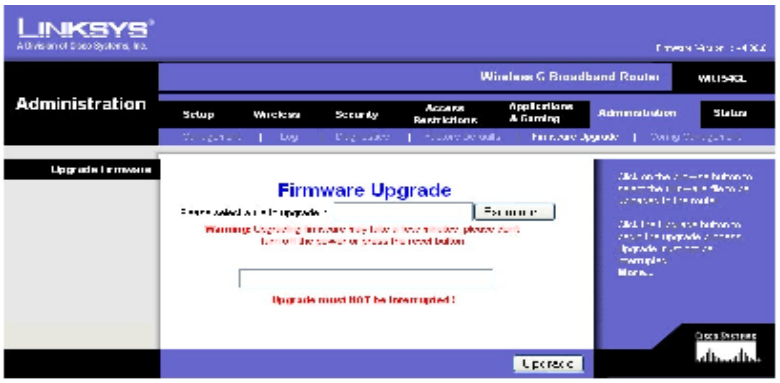

FIGURA III.40 Ingreso a sub-pestaña "Firmware Upgrade".

- Has click en el botón "Explorar" (o "Examinar...") y selecciona el archivo que nos descargamos de la base de datos de la página principal de DD-WRT que descomprimimos.
- Has click en el botón "Upgrade".

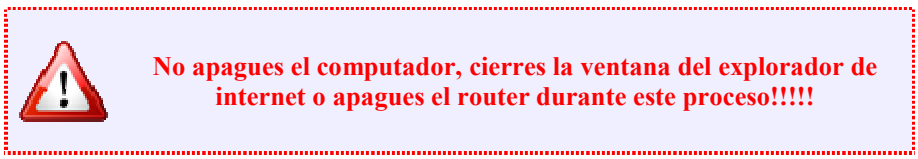

FIGURA XXXVI.41 Mensaje de advertencia

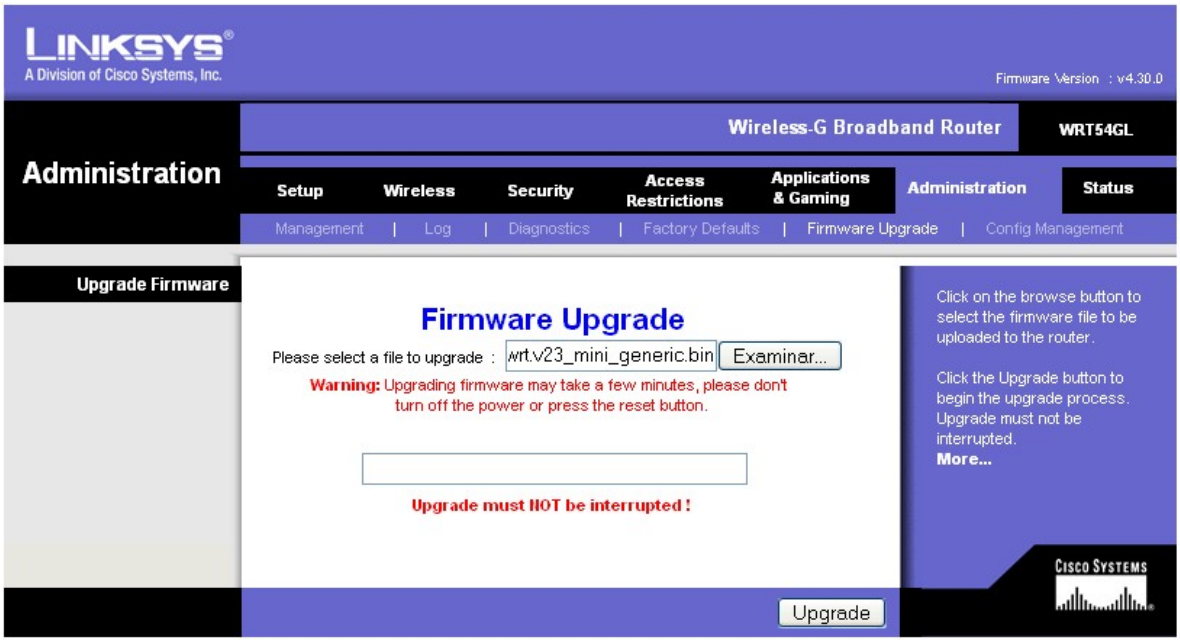

FIGURA XXXVII.42 Proceso de Flasheo

- El router tomará unos minutos para subir el archivo, flashear el firmware y resetearse.
- Si fue flasheado satisfactoriamente estarás ahora en la interfaz web de DD-WRT y el nombre del router será DD-WRT

SERVICIO DE CALIDAD

Configuración de QoS

FIGURA XXXVIII.43 Módulo QoS

Prioridad según los Servicios

Nos permite controlar la velocidad de datos con respecto a la aplicación que está consumiendo el ancho de banda. Los servicios se definen mediante puertos. Podemos favorecer ciertos servicios dando prioridad a los que usen ciertos puertos.

FIGURA XXXIX.44 Asignación de Prioridades a los Servicios

Diffserv

Clasificar el tráfico en pocas clases

• Clasifican los ingress routers (complejidad en la frontera) con un codepoint en la cabecera IP

• DiffServ mapea en cada nodo el codepoint en el paquete a un PHB en concreto

• PHB = Per Hop Behavior

– El tratamiento que se le da al paquete en cuestión de scheduling y gestión de cola en ese nodo

– El mapeo codepoint ↔ PHB debe ser configurable

Implementando Servicios usando DiffServ

Los routers de Entrada al dominio DiffServ deben tener un clasificador, que clasifica el tráfico entrante, un gestor que controle ancho de banda y prioridades, y un sistema de colas dependiendo de la clasificación del tráfico. Todo el tráfico dentro del dominio se gestiona de acuerdo a la clasificación que de él se hace en los routers de entrada.

En la VoIP se da prioridad tanto a los paquetes de señalización (los que nos ayudan a establecer la llamada, a colgar, etc..) como a los datos (la conversación digitalizada).

DD-WRT nos permite clasificar el tráfico en cinco clases, cada una de ellas determina el flujo de líneas de transmisión en condiciones de transmisión en tiempo real.

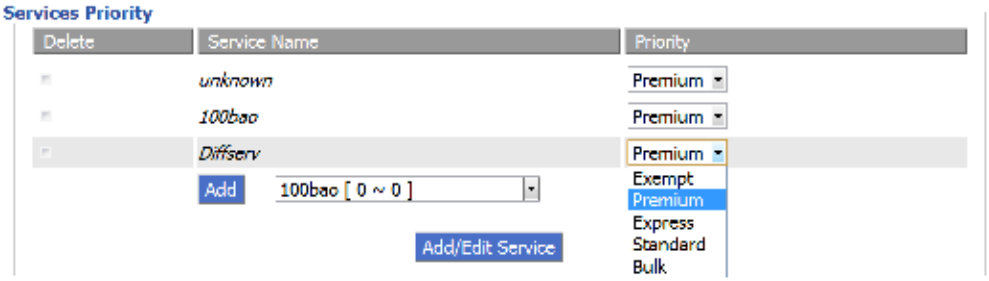

FIGURA XLIII.45 Clasificación de Tráfico

- **Exempt**. Esta clasificación está exenta de someterse a las reglas de la Calidad de Servicio.
- **Premium**. es la Elite. Solo es tráfico más importante debe tener esta clasificación. Idealmente sólo el tráfico VoIP. Si metemos demasiados servicios, al final no estaremos diferenciando. .
- **Express**. Es un nivel bueno, entre Premium y Standard.
- **Standard**. Es el que se usa por defecto. Los servicios que no tengan definida una regla de calidad de Servicio serán tratados como si se hubieran marcado con prioridad Standard..
- **Bulk**. Conviene clasificar así el tráfico de baja prioridad, como por ejemplo el P2P. Solo se le asigna ancho de banda cuando no hay tráfico con otras clasificaciones.

Ancho de banda es asignado sobre la base de los siguientes porcentajes de la subida y bajada para cada clase:

TABLA III.XVI. Porcentajes de ancho de banda

Porcentajes de ancho de banda

CLASE	PORCENTAJES DEL ANCHO DE BANDA
Exempt	-----
Premium	75% A 100%
Express	15% A 100%
Standard	10% A 100%
Bulk	1,5% A 100%

Los puertos UDP asignados son 16384 – 16482.

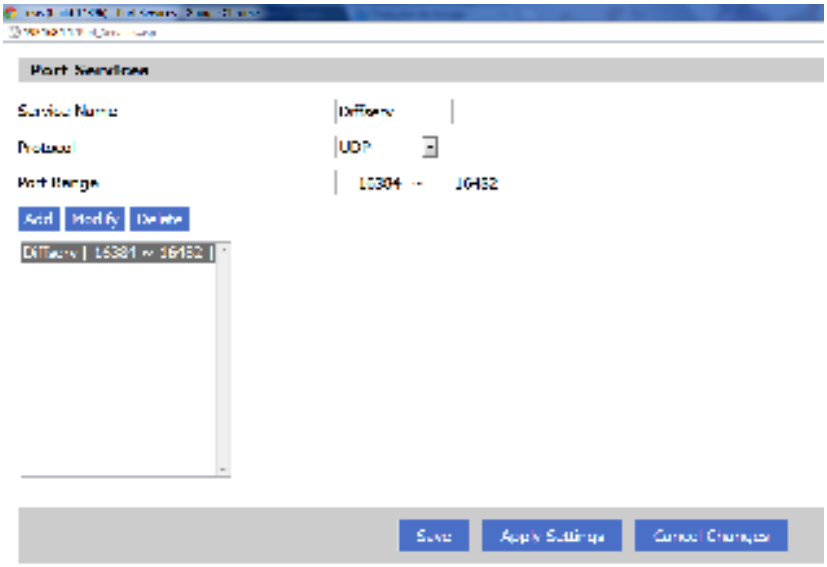

FIGURA XLI.46 Asignación de Puertos al Servicio

Prioridad según la Máscara

Nos permite especificar la prioridad para todo el tráfico de una dirección IP o rango de IP.

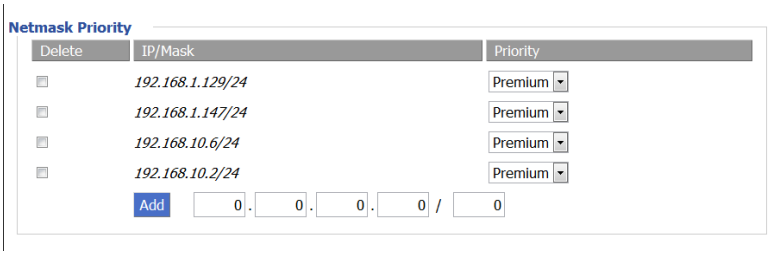

FIGURA XLII.47 Asignación de prioridad según la máscara

Prioridad según la dirección Mac:

En este módulo de la configuración del router podemos especificar la prioridad para todo el tráfico desde un dispositivo en su red, dando al dispositivo un nombre de dispositivo, especificando prioridades y entrando en su dirección MAC. El efecto es el mismo que el de dar prioridad a la Dirección IP, pero en ciertos casos, cuando se usan IPs dinámicas es más sencillo de implementar.

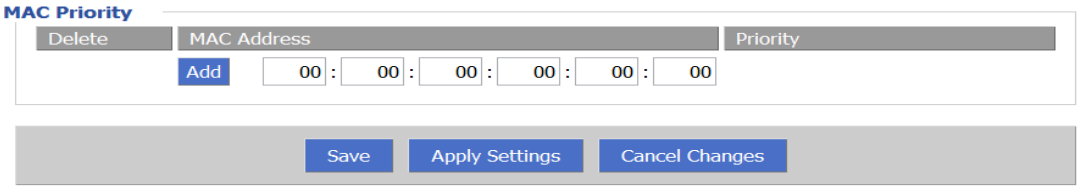

FIGURA XLIII.48 Asignación de prioridad según la dirección MAC

3.2.2.1. Guías de Implementación

A continuación presentamos la configuración realizada en cada uno de los servidores para el escenario Linux:

SERVIDOR DE VIDEOLLAMADAS (ELASTIX)

Elastix implementa gran parte de su funcionalidad sobre cuatro programas de software muy importantes como son Asterisk, Hylafax, Openfire y Postfix. Estos brindan las funciones de PBX, Fax, Mensajería Instantánea y Correo electrónico respectivamente. Elastix corre sobre Centos como sistema operativo y actualmente su versión más estable es Elastix 2.2

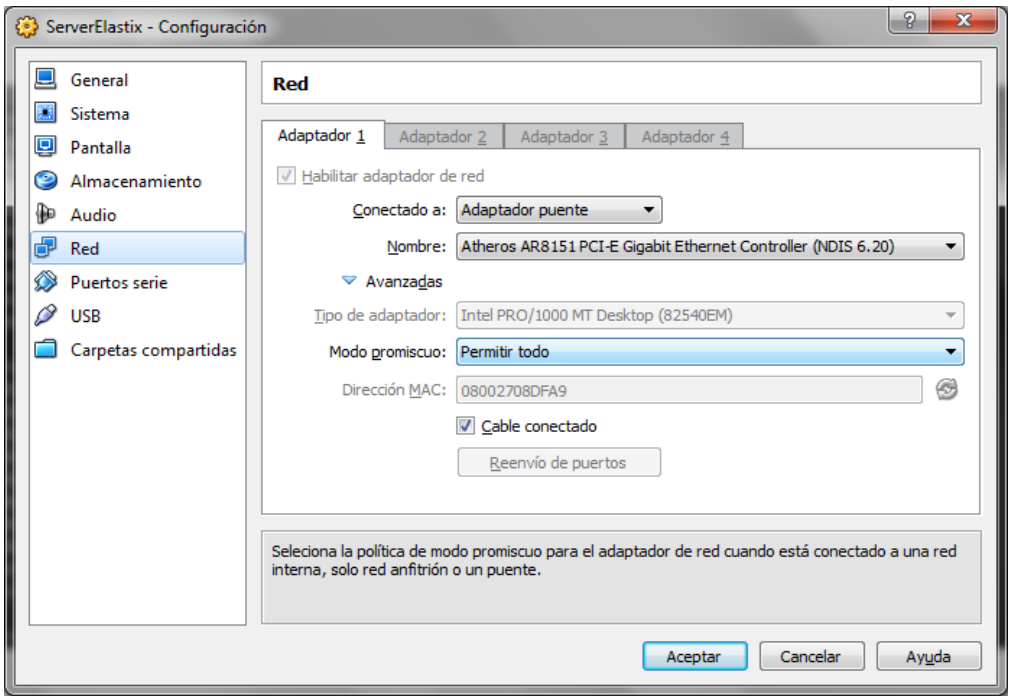

FIGURA XLIVII.49 Cconfiguración de red Servidor Elastix

Instalaremos Elastix 2.3.0 en una máquina Virtual, accediendo a este por web desde una maquina real.

Como trabajamos con la máquina virtual Oracle VM VirtualBox es recomendable que cuando se crea la maquina Linux con distribución Centos cambiamos la red de Nat por Adaptador puente. La ram puede ser según ser igual o mayor de 365mb y el almacenamiento puede ser de 8gb para la práctica.

Elastix se distribuye como un archivo ISO que puede ser quemado a un CD desde cualquier software de grabación de CDs.

Esta versión puede ser descargada desde http://www.elastix.org o directamente desde el sitio de descargas del proyecto: http://sourceforge.net/projects/elastix/

Instalación de Elastix

Al iniciar nos presentara esta pantalla donde le daremos Enter.

FIGURA III.50 Arranque de la instalación de Elastix

Esperamos que cargue y lea sus archivos.

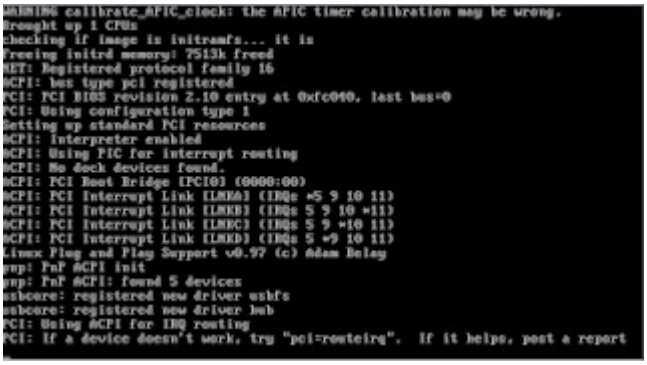

FIGURA XLV.51 Carga de archivos

Escogemos el idioma.

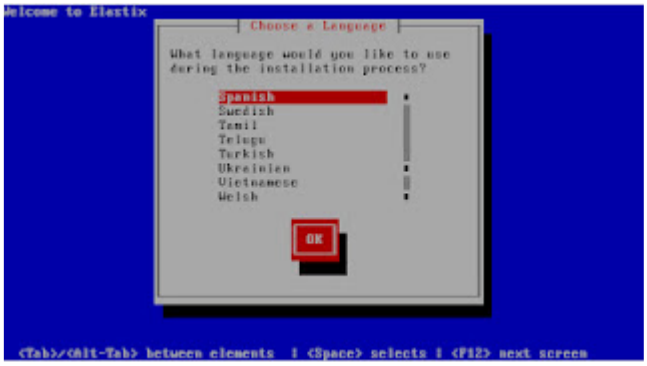

FIGURA XLVI.52 Configuración del idioma

Opciones para el diseño del almacenamiento del disco duro del elastix.

FIGURA XLVII.53 Opciones de almacenamiento de disco duro

Nos muestra como quedo el diseño y distribución del espacio del disco duro.

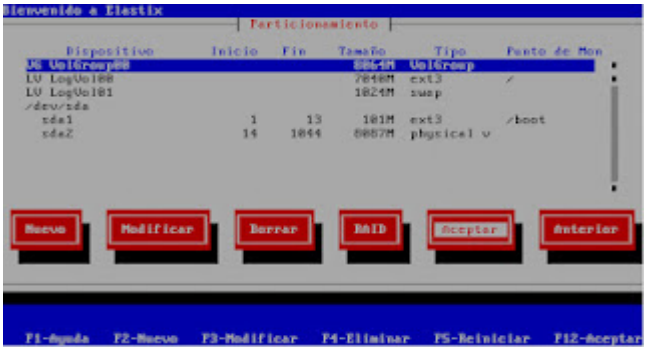

FIGURA XLVIIIII.54 Distribución del espacio del disco duro

Configuramos la Tarjeta de Red activando con la tecla espacio el soporte IPV4, también se puede el soporte IPV6 pero en este caso no lo utilizaremos.

FIGURA III.55 Configuración de la Tarjeta de Red

La configuración IPV6 si queremos Dinámica dhcp o estática, según sea nuestra topología de red.

FIGURA XLIX.56 Opciones de configuración para IPV6

Buscamos la Zona Horaria de nuestro País.

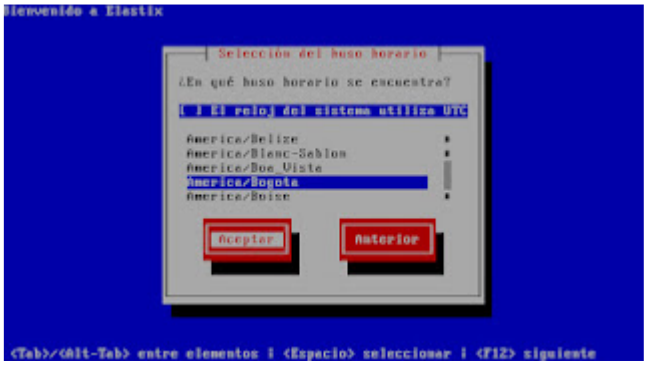

FIGURA L.57 Configuración Zona Horaria

Contraseña de root o admin para cuando vamos a acceder a elastix. En este caso utilizamos login: root y contraseña: elastix

FIGURA LI.58 Configuración de contraseña para Elastix

Esperamos las dependencias.

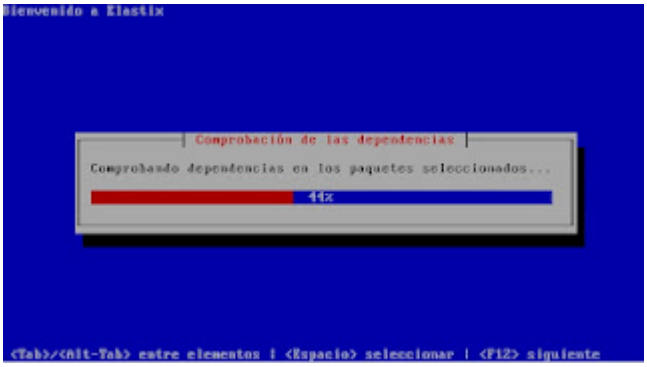

FIGURA LII.59 Dependencias de Elastix

Esperamos la instalación.

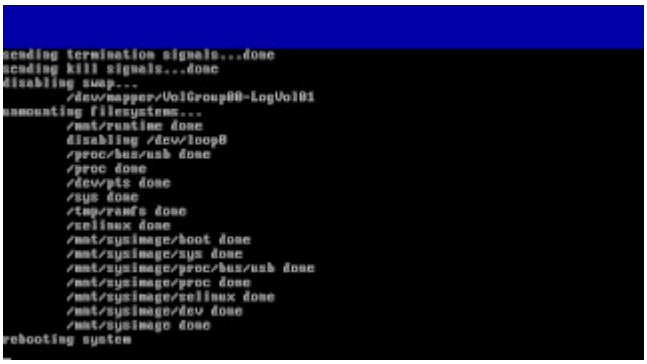

FIGURA III.60 Proceso de instalación Elastix

Está finalizando, se puede decir que el 1er paso de 2 de instalación y automáticamente nuestra maquina se reiniciara

FIGURA LIII.61 Finalización del proceso de instalación de Elastix

Cuando reinicia la maquina empieza a comprobar que todo esté funcionando bien.

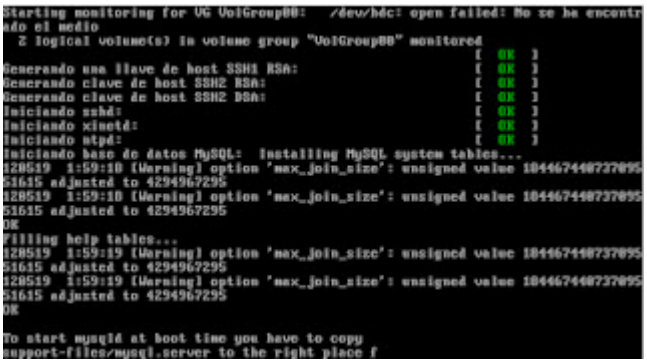

FIGURA LIV.62 Comprobación del funcionamiento correcto Elastix

Pedirá password para MYSQL, que es un paquete muy importante para elastix.

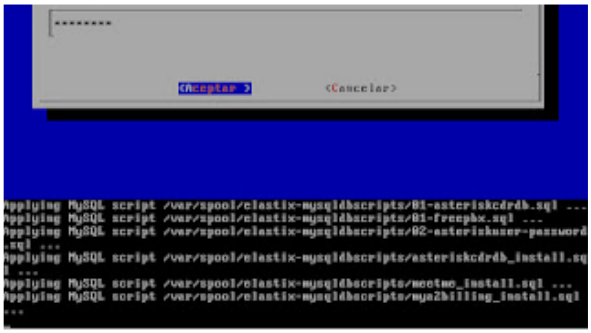

FIGURA LV.63 Ingreso del Password para MYSQL

Nos pide repetirla para confirmar que sea la misma.

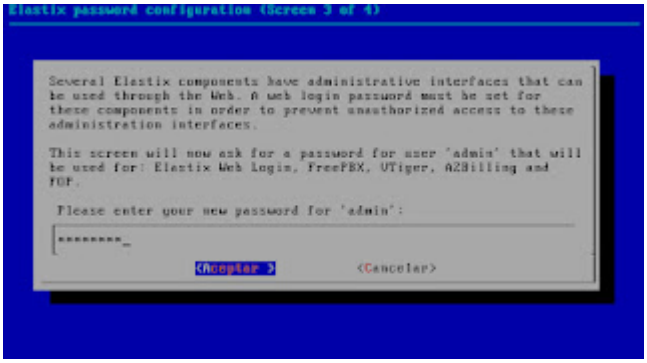

FIGURA LVI.64 Confirmación del Password

Ahora ya termina y nos tendremos que loguear como Root y la contraseña que previamente le configuramos al principio de la instalación.

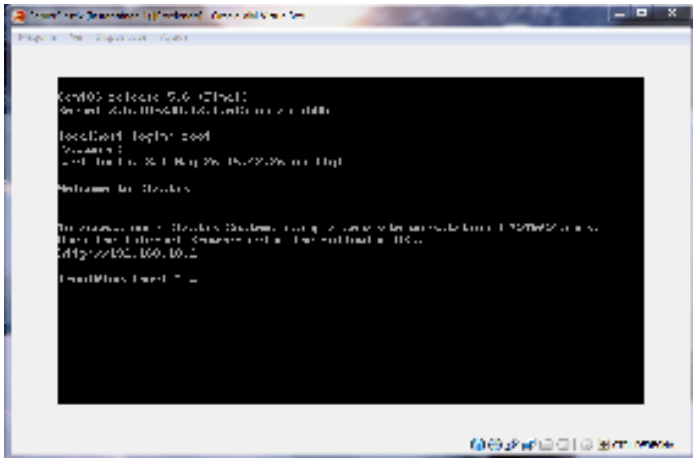

FIGURA LVIIII.65 Ingreso Servidor Elastix

Ya que la máquina de Elastix no presentara interfaz gráfica sino que será como cualquier terminal Linux (centos). Y ese será su estado normal y podemos probar que si está corriendo el servicio.

Ahora necesitamos saber la IP de nuestro servidor para poder acceder por la web, en este caso asignamos una dirección estática para el servidor. 192.168.10.2

Ahora desde un Navegador web de cualquier una máquina que este dentro de la misma red del servidor que instalamos, escribimos la IP que tiene el servidor de Elastix.

Aquí nos loguearemos con el administrador: **admin** y la contraseña es la que configuramos en el servidor.

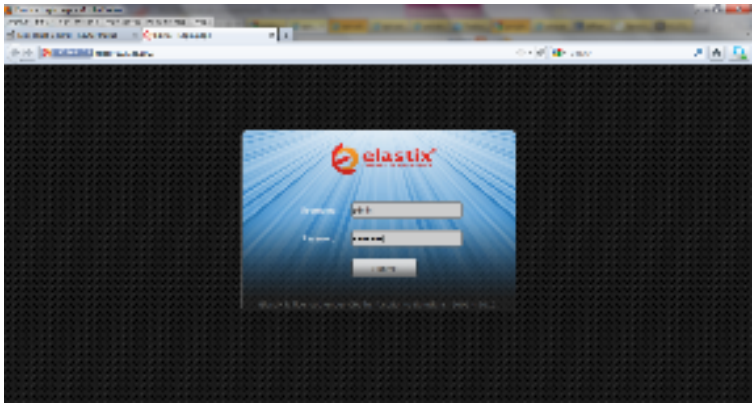

FIGURA LVIII.66 Ingreso al Servidor Elastix a través del Navegador Web

Listo todo ha ido muy bien y ahora podremos configurar nuestro servidor VOIP Elastix.

Siempre que queramos acceder a Elastix, Primero debemos poner a correr el servidor y fijarse en su IP después ir a un navegador de una máquina que esté en su misma red y escribiremos la IP del servidor.

Interfaz de Administración WEB

Configuración

a) Parámetros de Red

Diríjase a la sección Red.

b) Configuración de hardware telefónico

Diríjase a la sección Detalle de Puertos.

c) Creación de nueva extensión

Esta sección está dirigida a los handsets, softphones, sistemas paginadores, o cualquier cosa que pueda ser considerada como una "extensión".

Definir y corregir extensiones es probablemente la tarea más común realizada por un administrador de PBX, y como tal, se encontrará muy al corriente de esta página. Hay actualmente cuatro tipos de dispositivos soportados - el SIP, IAX2, ZAP y "Custom".

Para crear una "Nueva extensión" ingrese al Menú "PBX", por defecto se accede a la sección "Configuración PBX", en esta sección escogemos del panel izquierdo la opción "Extensiones". Ahora podremos crear una nueva extensión.

Primero escoja el dispositivo de entre las opciones disponibles:

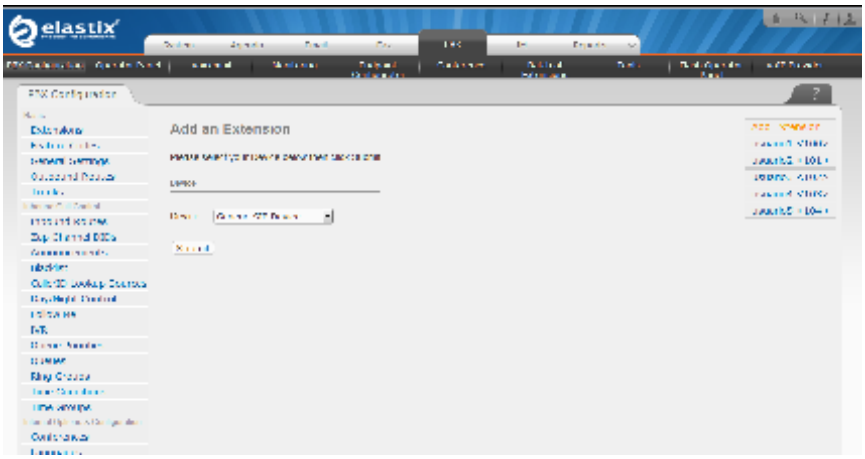

FIGURA LIX.67 Configuración PBX

Una vez haya escogido el dispositivo correcto de click en Ingresar.

Nota: Ahora se procede a ingresar los campos necesarios (obligatorios) para crear una nueva extensión.

Proceda a ingresar los datos correspondientes:

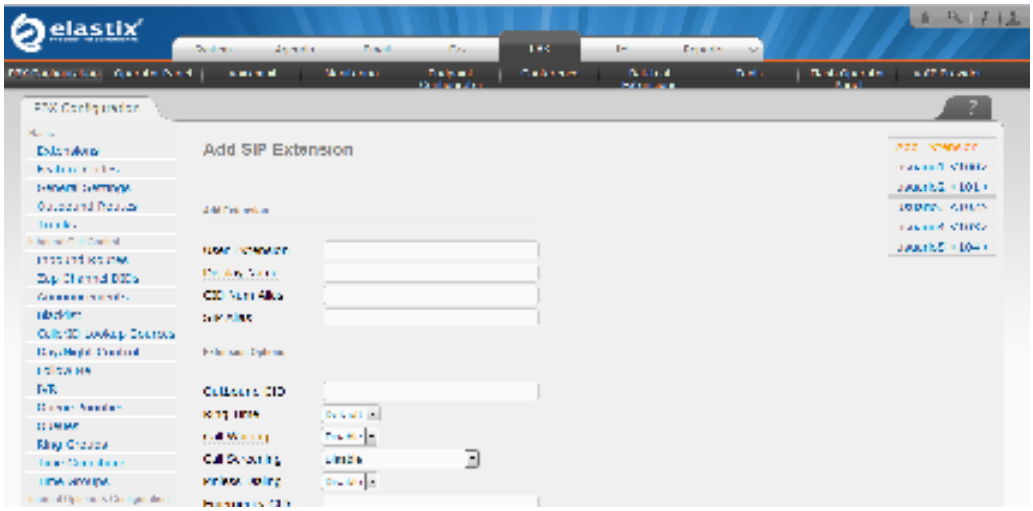

FIGURA LX.68 Creación de una nueva extensión

Extensión del Usuario: Debe ser único. Éste es el número que se puede marcar de cualquier otra extensión, o directamente del recepcionista Digital si está permitido.

Puede ser cualquier longitud, pero convencionalmente se utiliza una extensión de tres o cuatro cifras.

• Display Name : Es el nombre del Caller ID, para llamadas de este usuario serán fijadas con su nombre. Sólo debe ingresar el nombre no la extensión.

• Secret : Ésta es la contraseña usada por el dispositivo de la telefonía para autenticar al servidor de Asterisk. Esto es configurado generalmente por el administrador antes de dar el teléfono al usuario, y generalmente no se requiere que lo conozca el usuario.

Si el usuario está utilizando un soft-phone, entonces necesitarán saber esta contraseña para configurar su software.

d) Configuración de teléfono softphone

Un softphone es un software o programa de aplicación que permiten hacer llamadas desde una computadora, ya sea a otros softphones o a teléfonos convencionales, usando la tecnología VoIP. Pueden funcionar bajo el estándar SIP o H.323 o cualquier otro.

Podemos distinguir dos tipos de softphones, entre los cuales podemos mencionar:

• Propietarios; tal como Skype,

• De uso libre; al como el X-Lite, SJPhone, Wengophone classic, SipXphone, Linphone, etc.

Configuración del X-Lite

A continuación se describen los pasos a seguir:

1. Abra la aplicación X-Lite y se mostrara el teléfono.

FIGURA LXIII.69 Aplicación X-Lite

2. Posicione el cursor sobre el softphone y haga clic derecho. Se desplegara un menú, en el cual seleccionara "Sip Account Settings (configuraciones cuentas SIP).

FIGURA LXII.70 Configuración cuenta SIP

Le aparecerá una ventana en blanco donde podrá colocar sus cuentas SIP. Presione el botón Add. (Agregar) que aparece a mano derecha.

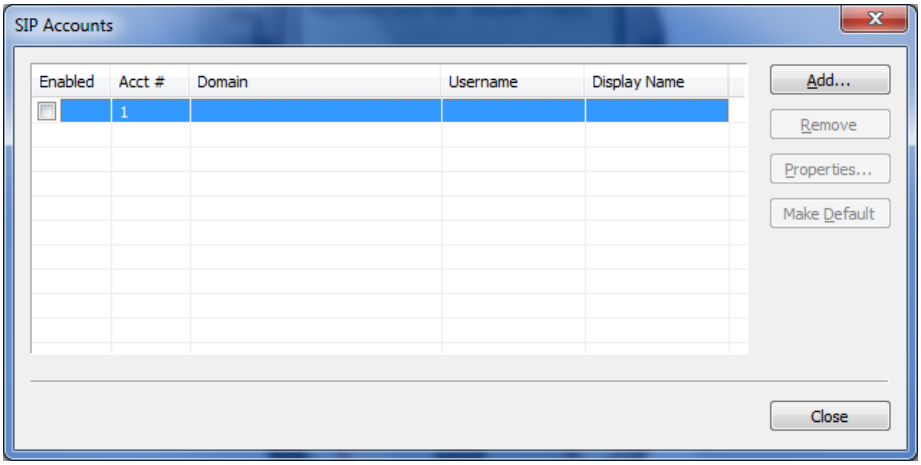

FIGURA LXIII.71 Agregar cuentas SIP

3. Se abrirá una nueva ventana en la cual aparecen cinco cuadros de texto que se deben completar, a saber:

• Display name: Es información que aparece en la pantalla del teléfono. Escribirá su nombre.

• User name: Es el número de identificación asignado en el plan de numeración de la PBX IP.

• Password: Escribir la contraseña asignada.

• Authorization user name: Se coloca el mismo número de identificación del pal de numeración (user name) para que la comunicación pueda ser registrada correctamente.

• Domain: Se escribe el dominio o proxi para conectarse en este caso a la PBX IP. Escribir 192.168.10.2

Después de haber ingresado la información necesaria haga clic en “aceptar”.

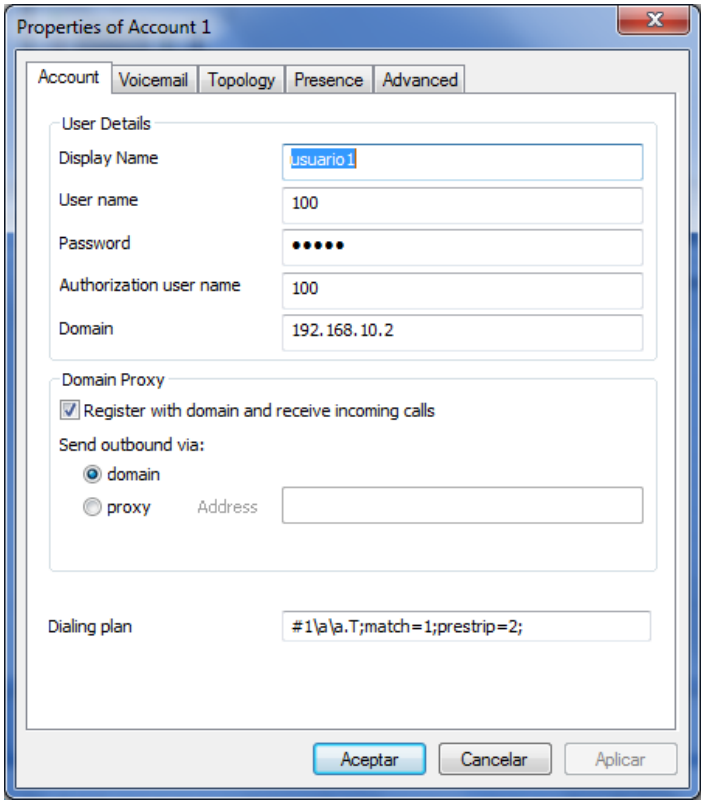

FIGURA LXIV.72 Propiedades cuenta SIP

Ahora se mostrará la ventana "SIP Account" pero con su cuenta registrada. Cierre la ventana.

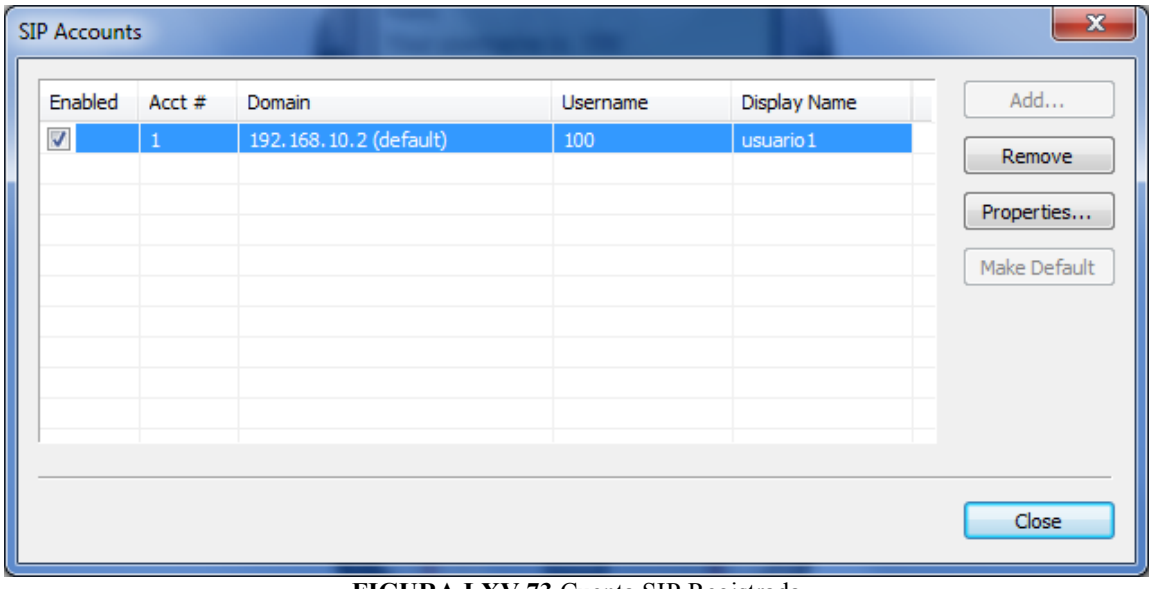

FIGURA LXV.73 Cuenta SIP Registrada

5. Volverá a ver el X-Lite registrándose la PBX IP, después de unos segundos aparecerá en la pantalla del softphone X-lite YOUR USER NAME: 100

FIGURA LXVI.74 Usuario registrado

6. Proceda a realizar una llamada a algún otro usuario registrado.

Si se recibe un mensaje de error se debe verificar la conexión y verificar la configuración de la cuenta.

MENÚ SISTEMA CENTRAL ELASTIX

1 Información del Sistema

La opción "Información del Sistema" del Menú "Sistema" del Elastix nos permite monitorear los recursos físicos del servidor.

Dentro de esta opción tenemos dos secciones:

Recursos del Sistema

"Recursos del Sistema" nos muestra valores del uso actual tanto de la memoria como del procesador.

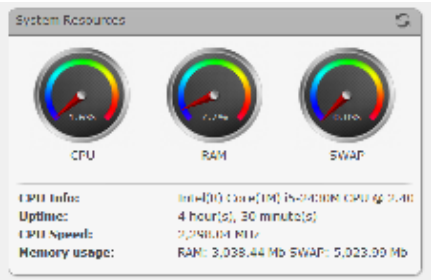

FIGURA LXVII.75 Recursos del Sistema

CPU: Datos acerca de marca, modelo y velocidad del Procesador

Tiempo de funcionamiento: Tiempo desde el último reinicio del servidor

CPU usado: Porcentaje de uso de la capacidad del procesador

Memoria utilizada Porcentaje de memoria RAM utilizada

También se muestra un gráfico con las estadísticas de llamadas simultáneas, porcentaje de uso de procesador y porcentaje de uso de memoria RAM.

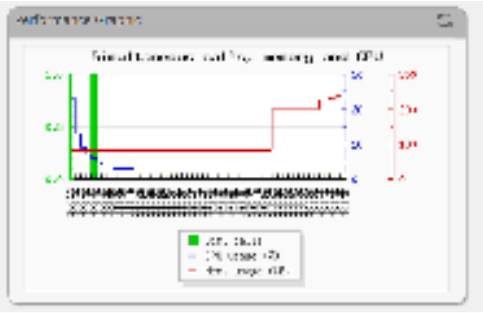

FIGURA LXVIII.76 Estadísticas de llamadas

Discos Duros

Esta sección muestra un resumen de la utilización de los medios de almacenamiento disponibles en el servidor.

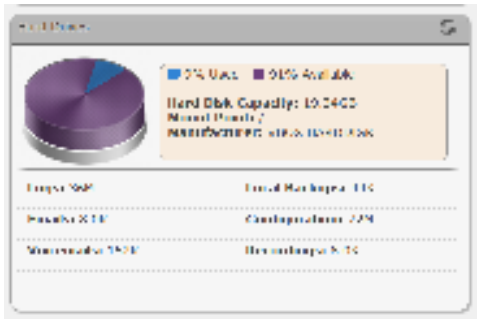

FIGURA LXIX.77 Disco Duro

Red

La opción "Red" del Menú "Sistema" del Elastix nos permite visualizar y configurar los parámetros de red del servidor. Dentro de esta opción tenemos dos secciones:

Parámetros de Red

FIGURA LXX.78 Parámetros de red

Corresponde a los parámetros de red generales del servidor:

Host Nombre del Servidor (ejm): localhost.localdomain

Puerta de Enlace: Dirección IP de la Puerta de Enlace

DNS Primario: Dirección IP del Servidor de Resolución de Nombres (DNS) Primario

DNS Secundario: Dirección IP del Servidor de Resolución de Nombres (DNS) Secundario o Alternativo

Para cambiar cualquiera de estos parámetros, debe dar click en el botón “Editar Parámetros de Red”.

Lista de Interfaces Ethernet

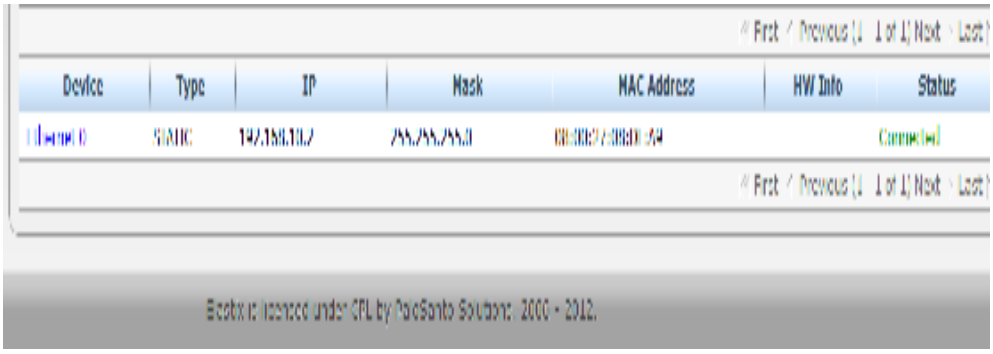

FIGURA LXXI.79 Listado de Interfaces Ethernet

Muestra un listado de las interfaces de red disponible en el servidor, con los siguientes datos:

Dispositivo: Nombre que el Sistema Operativo le asigna a la Interfaz

Tipo: El tipo de dirección IP que tiene la Interfaz, puede ser STATIC como es nuestro caso cuando la dirección IP es fija o DHCP cuando la dirección IP se la obtiene automáticamente al iniciar el equipo. Para utilizar la segunda opción, debe existir un servidor DHCP en su red.

IP: Dirección IP asignada a la Interfaz

Máscara: Máscara de Red asignada a la Interfaz

Dirección MAC: Dirección Física de la Interfaz de red

HW Info: Información adicional sobre la Interfaz de red

Estado: Muestra el estado físico de la Interfaz, si se encuentra conectada o no.

Para cambiar los parámetros de alguna de las Interfaces, debe dar click en el nombre del dispositivo (Dispositivo). Los únicos valores que puede cambiar son: Tipo, IP y Máscara

FIGURA LXXII.80 Configuración Interfaces de Red

Administrar Usuarios

Usuarios

La opción "Usuarios" nos permite crear y modificar los usuarios que tendrán acceso a la interfaz Web de Elastix. Existen 3 tipos o grupos de usuarios que son:

1. Administrador

2. Operador

3. Usuario de teléfono

Cada uno de estos grupos representa distintos niveles de acceso a la interfaz Web de Elastix. Estos niveles significan a qué conjunto de menús tendrá acceso cada tipo de usuarios. Los distintos permisos de acceso a los menús se ilustran mejor en la siguiente tabla:

TABLA III.XVII. 2 Grupos de Usuarios

Menú	Administrador	Operador	Usuario de teléfono
Menú Sistema			
Información del Sistema	Sí	Sí	No
Configuración PBX	Sí	No	No
Red	Sí	No	No
Administración de Usuarios	Sí	No	No
Apagar	Sí	No	No
Operator Panel			
Flash Operator Panel	Sí	Sí	No

Tabla III.XVII. Grupos de Usuarios (Continuación)

Correos de Voz			
Asterisk Recording Interface	Sí	Sí	Sí
Fax			
Listado de Fax Virtual	Sí	Sí	No
Nuevo Fax Virtual	Sí	No	No
Reportes			
Reporte CDR	Sí	Sí	No
Uso de Canales	Sí	Sí	No
Facturación			
Tarifas	Sí	No	No
Reporte de Facturación	Sí	No	No
Distribución de Destinos	Sí	No	No
Configuración de Troncales	Sí	No	No
Extras			
SugarCRM	Sí	Sí	Sí
Calling Cards	Sí	Sí	Sí
Descargas			
Softphones	Sí	Sí	Sí
Utilidades de Fax	Sí	Sí	Sí

• Permisos de Grupo

La opción "Permisos de Grupo" nos permite determinar cuáles serán los menús a los que tendrán acceso cada grupo de usuarios.

El listado muestra los nombres de los menús del Elastix, deberá seleccionar aquellos a los que el grupo seleccionado tendrá permisos de acceso y luego dar click en el botón "Aplicar".

4 Idioma

La opción "Idioma" del Menú "Sistema" del Elastix nos permite configurar el idioma para la interfaz Web de Elastix.

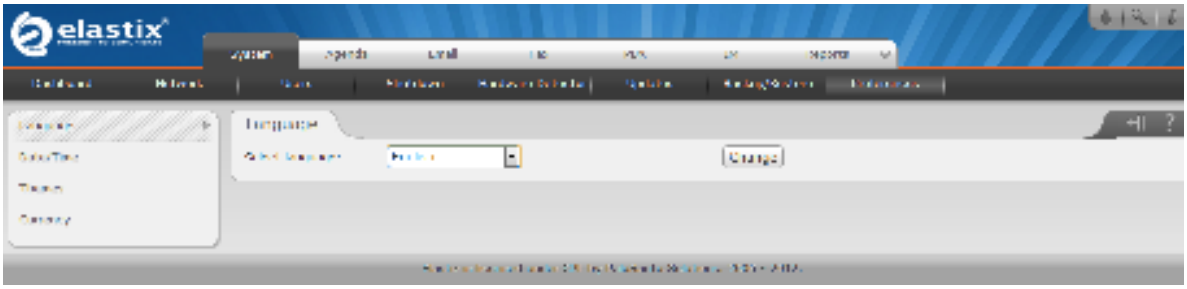

FIGURA LXXIII.81 Configuración del Idioma

Seleccione el idioma de la lista disponible y de click en el botón “Cambiar”.

Configuración de Fecha y Hora

La opción “Configuración de Fecha y Hora” del Menú “Sistema” del Elastix nos permite configurar la Fecha, Hora y Zona para la interfaz Web de Elastix.

FIGURA LXXIV.82 Configuración de Fecha y Hora

Seleccione la nueva fecha, hora y zona de ubicación y de click en el botón “Aplicar Cambios”.

Temas

La opción “Temas” del Menú “Sistema” del Elastix nos permite escoger un tema para la Interfaz Web del Elastix.

FIGURA LXXV.83 Selección de Tema

Para cambiar el tema escoge una de las opciones disponibles y da click sobre el botón “Cambiar”.

Cargar Menú

La opción “Cargar Menú” de “Sistema” del Elastix nos permite subir un módulo para el Elastix.

Para subir el nuevo módulo de click en el botón “Examinar”, seleccione el archivo y finalmente de click en el botón “Guardar”.

Respaldar

La opción “Respaldar” del Menú “Sistema” del Elastix nos permite escoger las configuraciones que deseamos respaldar del Elastix.

FIGURA LXXVI.84 Selección de configuraciones a respaldar

Para hacer un Respaldo de las configuraciones del Elastix selecciona de entre las opciones disponibles, y da click sobre el botón “Procesar”.

Restaurar

La opción “Restaurar” del Menú “Sistema” del Elastix nos permite escoger las configuraciones que deseamos recuperar del Elastix, a partir de un “Respaldo” realizado anteriormente.

Para recuperar las configuraciones del Elastix selecciona de entre las opciones disponibles, ingresa la ruta del archivo de respaldo y da click sobre el botón “Procesar”.

Apagar

Esta opción permite apagar o reiniciar la central telefónica. Al elegir cualquiera de las dos alternativas se le pedirá que confirme la opción que desea ejecutar.

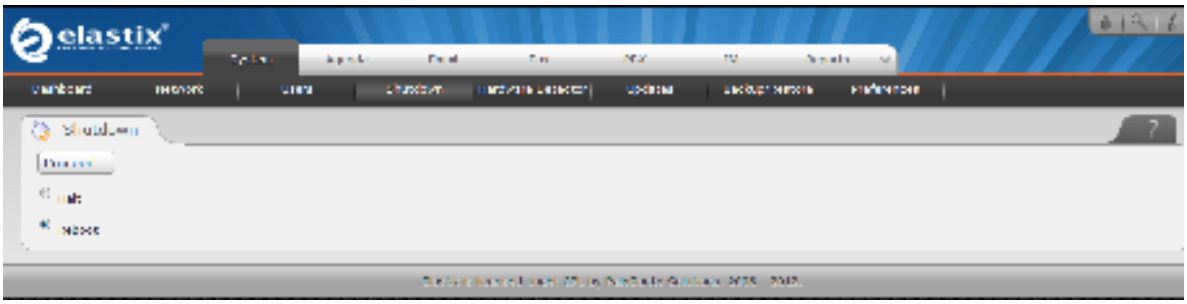

FIGURA III.85 Proceso de respaldo de configuración

Detalle de Puertos

La opción “Detalles de Puertos” del Menú “Sistema” del Elastix nos permite detectar el hardware telefónico disponible en nuestra máquina, es decir las tarjetas de telefonía instaladas.

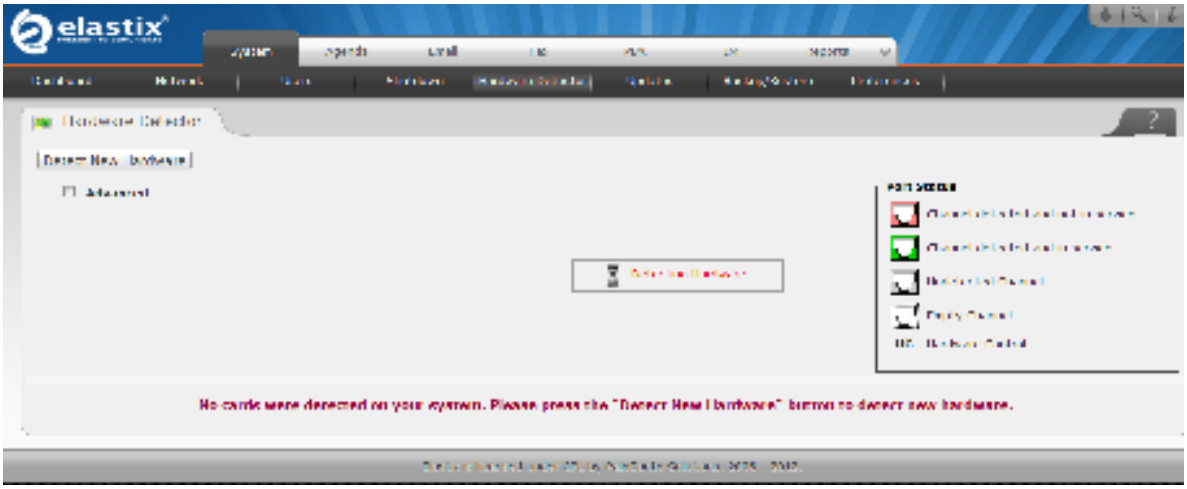

FIGURA LXXVII.86 Listado de tarjetas disponibles

El listado que usted verá al ingresar a esta sección serán todas las tarjetas ya instaladas y que se encuentran funcionando, además podrá ver los puertos aún disponibles (sin usar) para nuevas tarjetas telefónicas.

Para detectar nuevo hardware telefónico de click en el botón “Detectar Hardware”, a continuación se listarán todas las tarjetas disponibles inclusive las “NUEVAS TARJETAS INSTALADAS RECIENTEMENTE”.

MENÚ PBX

1 Configuración PBX

La opción “Configuración PBX” del Menú “PBX” nos permite realizar la configuración del Elastix.

En la parte izquierda podremos observar las distintas opciones de configuración que tenemos.

Elastix hace uso del software libre FreePBX como herramienta para administración de asterisk, para mayor información refiérase a la siguiente dirección:

http://www.freepbx.org/support/documentation/module-documentation

2 Asterisk-Cli

La opción “Asterisk-Cli” del Menú “PBX” del Elastix nos permite ingresar comandos de Asterisk y ejecutarlos.

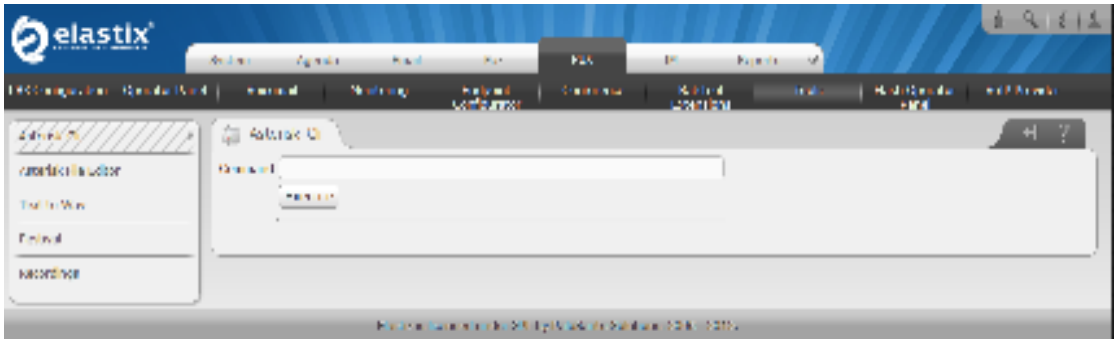

FIGURA LXXVIII.87 Ingreso de comandos de Asterisk a ser ejecutados

Para ejecutar un comando, ingrese el mismo en Command y de click sobre el botón “Execute”.

Ejemplo:

* show channels

Muestra cualquier canal que esté en uso en ese momento.

Flash Operator Panel

El “Flash Operator Panel” del Menú “PBX” del Elastix es un manejador en flash de extensiones en Asterisk para monitorear los canales y terminales que se producen en un servidor con Asterisk.

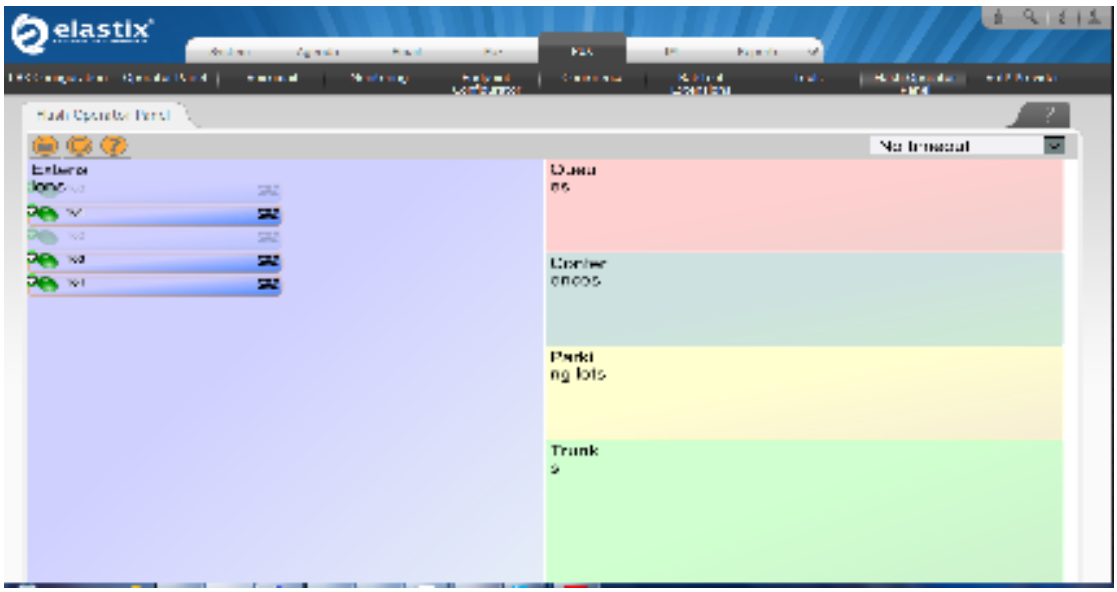

FIGURA LXXIX.88 Monitoreo de canales y terminales

Correo de voz

La opción “Correos de Voz” del Menú “PBX” del Elastix nos permite visualizar un listado con el detalle de los correos de voz para la extensión de un usuario conectado.

El reporte cambiará dependiendo de los valores de filtrado:

Fecha Inicio Fecha a partir de la cual se seleccionarán los correos de voz.

Fecha Fin Fecha hasta la cual se seleccionarán los correos de voz.

Monitoreo

La opción “Monitoreo” del Menú “PBX” del Elastix nos permite visualizar un listado con el detalle de las llamadas grabadas automáticamente o manualmente, para la extensión de un usuario conectado.

FIGURA LXXX.89 Listado de llamadas grabadas

El reporte cambiará dependiendo de los valores de filtrado:

Fecha Inicio: Fecha a partir de la cual se seleccionarán las llamadas.

Fecha Fin: Fecha hasta la cual se seleccionarán las llamadas.

Además podemos escuchar las llamadas al dar click en la opción “Listen” para cada llamada, o podemos descargar un archivo de audio con extensión wav de la llamada seleccionada.

Editor de Archivo

La opción “File Editor” del Menú “PBX” del Elastix nos permite editar los archivos de configuración del Elastix.

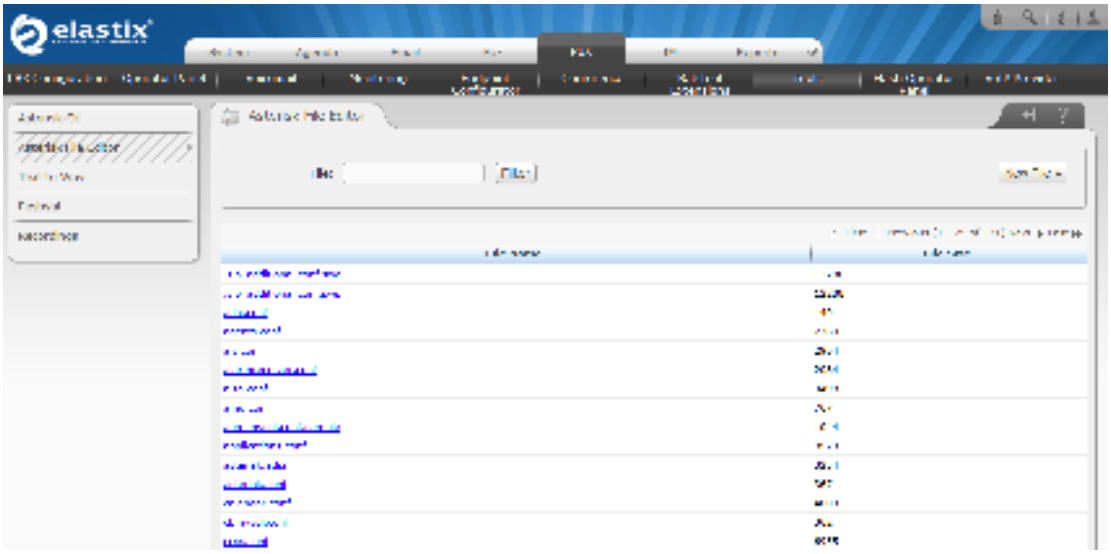

FIGURA III.90 Selección de archivos para editar su configuración

Para editar un archivo da click sobre el mismo, se mostrará el archivo a editar:

Proceda a editar el archivo de configuración, una vez realizado esto da click en el botón “Guardar” para guardar la nueva configuración. Para regresar sin guardar los cambios, da click sobre el botón “Atrás”.

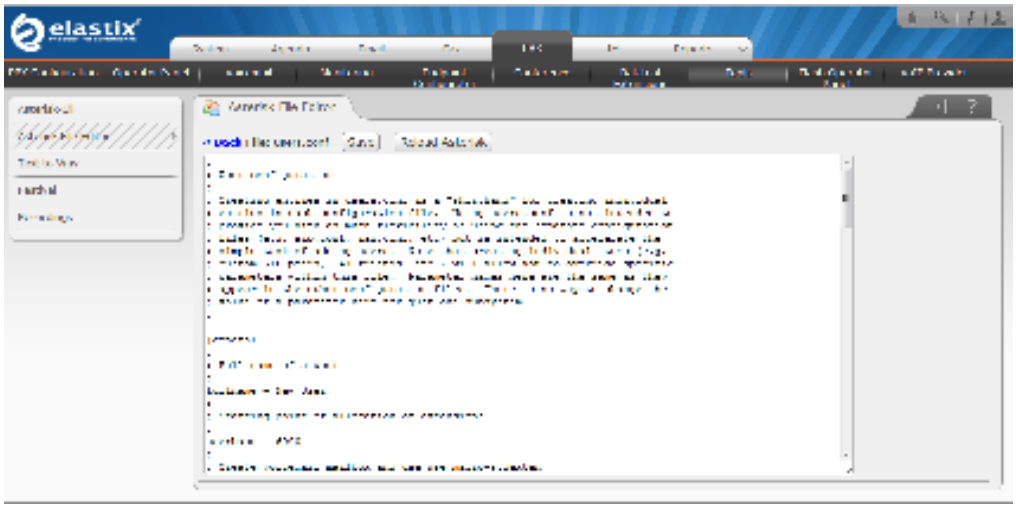

FIGURA LXXXI.91 Edición de un archivo de configuración

Configuración Avanzada

LLAMADAS CON VIDEO

Esta es una tarea fácil debido a que Elastix tiene los codecs de video incluidos. Apenas tienes que fijar un par de cosas en tu configuración del SIP para conseguir tus funcionamientos de video llamadas.

En la parte de abajo del archivo sip.conf (Sección "general") añade las siguientes líneas:

videosupport=yes

maxcallbitrate=384

allow=h261

allow=h263

allow=h263p

allow=h264

Recarga tu configuración de Elastix. Para recargar, por favor ejecute el siguiente comando desde CLI.

CLI> reload

SERVIDOR WEB

Lo primero que haremos será arrancar el sistema y accederemos con la **cuenta de root** que es a la que indicamos una contraseña durante la instalación. Por tanto accederemos con el nombre de usuario root y la contraseña elegida en la instalación. Una vez que hayamos accedido con dicha cuenta iremos a **Aplicaciones**, **Accesorios**, **Terminal** y nos saldrá algo como esto:

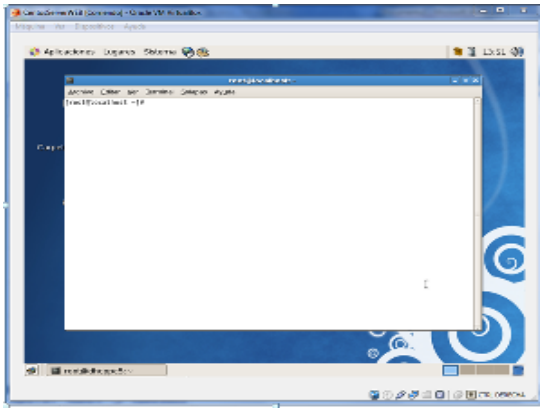

FIGURA LXXXII.92 Acceso al terminal Servidor Web

INSTALANDO APACHE Y PHP

Volvemos a abrir nuestro terminal pero en este caso vamos a hacer uso del comando **YUM** el cual nos servirá para instalar aquello que es necesario para nuestro servidor web.

1 yum install -y httpd php php-mysql mod_perl mod_python mod_ssl

Para que entendamos un poco los comandos el -y nos servirá para que nos responda a si a todas las preguntas que puedan surgir durante la instalación. Una breve descripción sobre los paquetes que vamos a instalar podría ser esta:

- **httpd**: el servidor web apache
- **php**:el paquete encargado de hacer funcionar php
- **php-mysql**: paquete necesario para poder hacer conexiones entre mysql y php
- **mod_perl**: modulo opcional que permite correr el intérprete de perl
- **mod_phyton**: modulo opcional que permite correr scripts escritos en phyton
- **mod_ssl**: permite la utilización de certificados de seguridad SSL

Cuando se termine la instalación saldrá lo que se ha instalado y que paquetes se han instalado al ser dependientes de los otros.

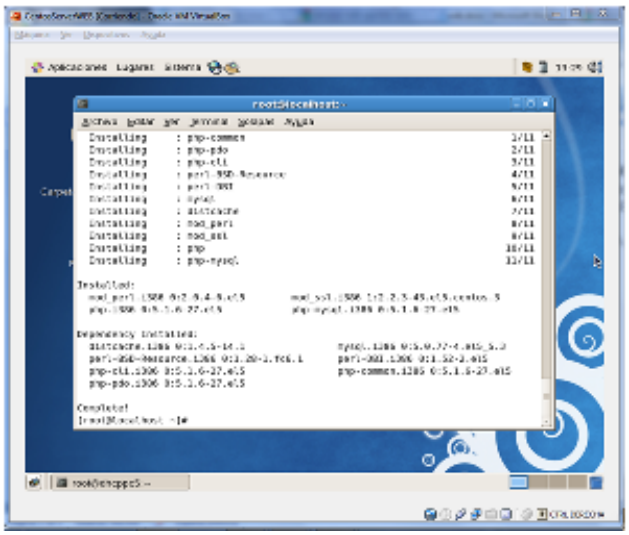

FIGURA LXXXIII.93 Instalación de Paquetes Servidor Web

Una vez realizado esto vamos a configurar nuestro sistema para que inicie **Apache** automáticamente para ello escribimos lo siguiente:

```
1 chkconfig --level 345 httpd on
```

Esto hará que se inicie automáticamente en los **runlevel 3,4 y 5** los únicos que vamos a necesitar.

Ahora vamos a reiniciar la máquina para ver si se ha guardado correctamente el inicio automático. Si es así una vez reiniciado entramos en el navegador y ponemos **http://localhost** y nos debería salir la siguiente pantalla:

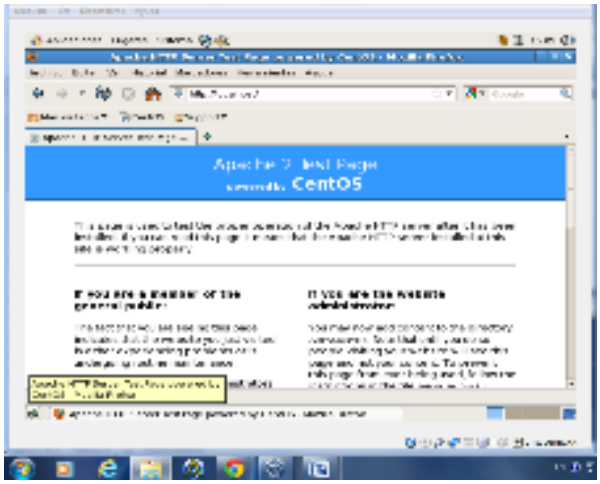

FIGURA LXXXIVII.94 Ingreso al navegador con http://localhost

Para poder cargar nuestros propios scripts en **PHP** volvemos al terminal y tecleamos lo siguiente:

```
1 vi /var/www/html/phpinfo.php
```

Y dentro de este archivo daremos a la **i** para empezar a insertar texto y pondremos lo siguiente:

```
1 <?php

2

3 phpinfo();

4

5 ?>
```

Para guardar daremos a **ESC** y luego **!wq:** y a **Intro**

Ahora si vamos a http://localhost/phpinfo.php veremos un phpinfo de nuestro sistema similar a este:

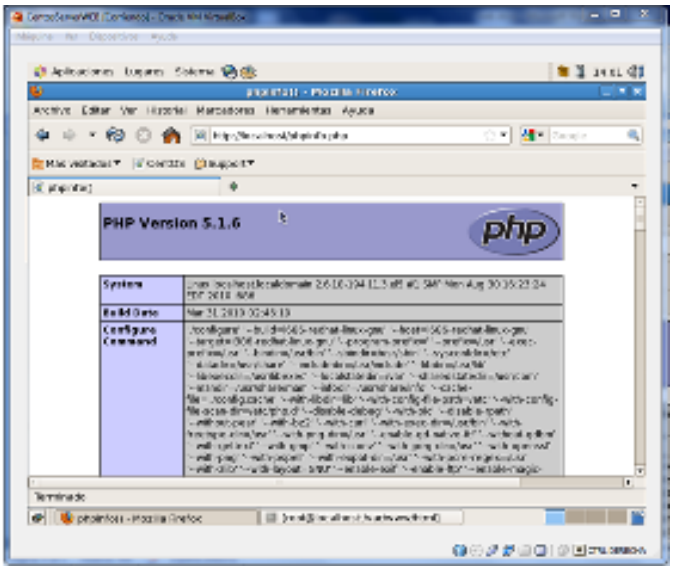

FIGURA LXXXV.95 Carga de scripts en PHP

SERVIDOR DE CORREO ELECRÓNICO

Instalación y Configuración de Zimbra en Centos.

Esta guía cubre la instalación de Centos, las dependencias de ZCS y la configuración de un DNS dividido cuando se trabaja detrás de un firewall.

Requisitos

Para instalar este sistema se necesita lo siguiente:

En este tutorial utilizo el nombre de host mail.geekdept.com con la dirección IP de 192.168.0.45 y una puerta de enlace 192.168.0.1.

Tomaremos en cuenta solo una parte de la instalación de Centos ya que no se puede ejecutar un servidor de correo electrónico mediante DHCP.

Los Dispositivos de red nos permite ingresar la información de dirección IP para la red. Utilizando el botón de edición introducimos la información adecuada para la red.

FIGURA LXXXVI.96 Ingreso de nombre de host, dirección IP y puerta de enlace

Ahora es el momento de elegir los paquetes a instalar. Desactive todas las casillas en el panel superior y marque la casilla de los paquetes de CentOS adicionales en el panel inferior.

Haga clic en el botón de radio para personalizar ahora y haga clic en Siguiente

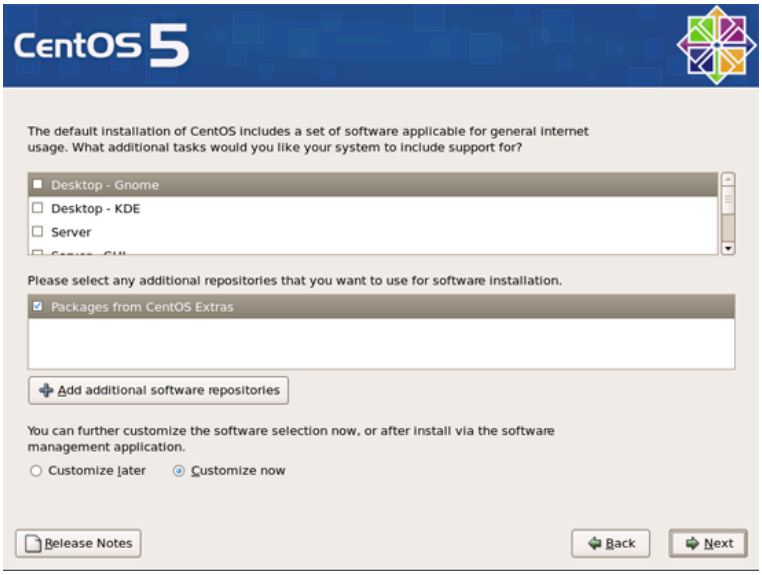

FIGURA LXXXVII.97 Configuración previa a la instalación de paquetes

Una ventana pop-up verificar la información de su dirección IP. La siguiente pantalla te permite elegir los paquetes para su instalación.

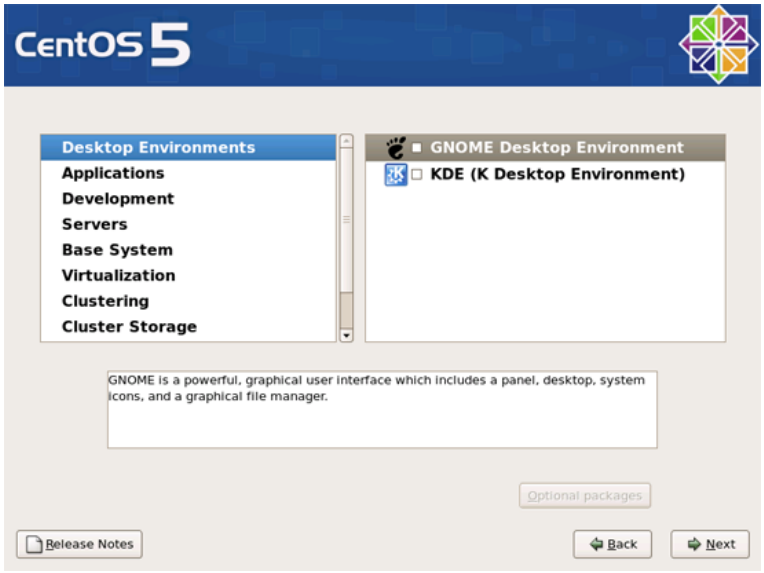

FIGURA LXXXVIII.98 Selección de paquetes a instalar

Una vez que haya seleccionado los paquetes haga clic en Siguiente y buscará las dependencias.

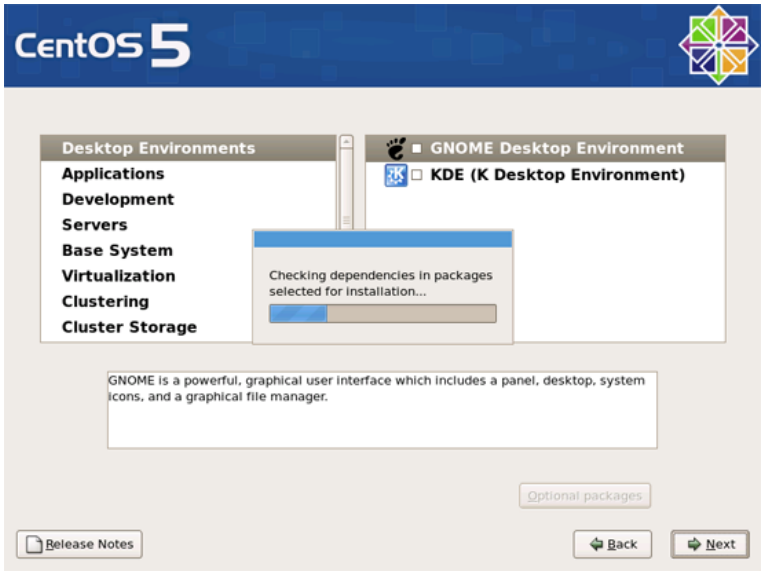

FIGURA LXXXIX.99 Búsqueda de dependencias

La instalación sólo toma unos pocos minutos porque estamos instalando el mínimo.

FIGURA III.100 Proceso de instalación Correo Electrónico

Haga clic en Reiniciar una vez que la instalación haya finalizado.

FIGURA XC.101 Finalización de la instalación

Una vez que se reinicia el sistema le presenta la pantalla firstboot. Esta característica es muy útil porque permite hacer cambios en el firewall. Con el teclado elegir Firewall, pulsamos el tabulador para ir hasta el botón Ejecutar herramienta y pulsamos enter.

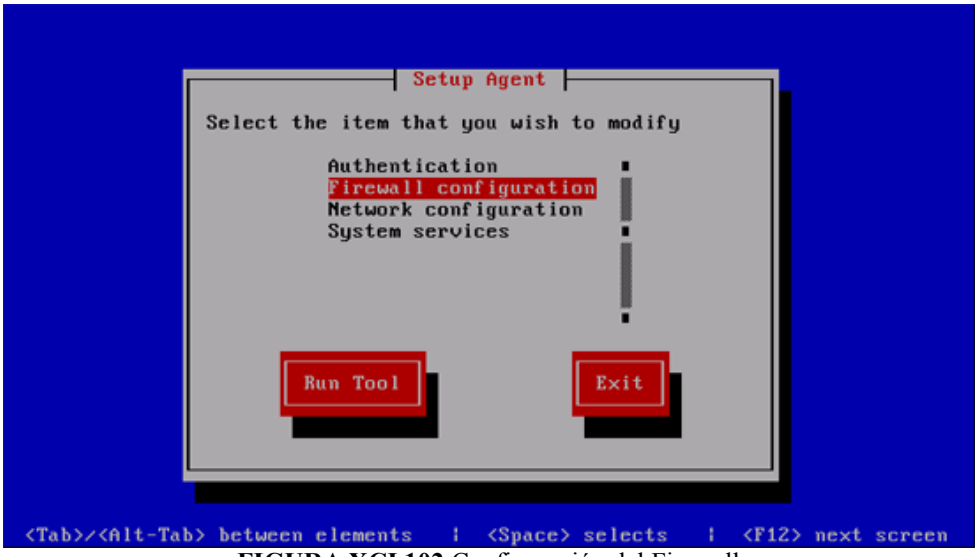

FIGURA XCI.102 Configuración del Firewall

Para elegir el nivel de seguridad desactivado seleccionamos Desactivado y clic en Aceptar.

FIGURA XCII.103 Elección del nivel de Seguridad

Ahora están de vuelta en la primera pantalla de arranque principal. Utilizamos la tecla Tab para avanzar al botón Exit.

El último paso es para apagar algunos de los servicios que interfieran con ZCS.

chkconfig *sendmail* *off*

chkconfig *ip6tables* *off*

chkconfig iptables off

Necesitamos un paquete antes de que podamos continuar:

yum install libtool-ltdl

Esto completa la instalación de la base de Centos. A continuación vamos a configurar el DNS dividido que es esencial para ZCS.

Instalación de un DNS dividido

```
yum install bind bind-chroot bind-libs bind-utils
```

Creamos el directorio / var / named / chroot / etc / named.conf:

```
vim /var/named/chroot/etc/named.conf
```

```
options {
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
forwarders { 192.168.0.10 ; };
};
include "/etc/rndc.key";
// We are the master server for mail.geekdept.com
zone "mail.geekdept.com" {
    type master;
    file "db.mail.geekdept.com";
};
```

La dirección IP debe ser la dirección IP de su servidor DNS. Ahora es necesario crear el archivo / var / named / chroot / var / named / db.mail.geekdept.com

vim /var/named/chroot/var/named/db.mail.geekdept.com

```
;       Addresses and other host information.
;
@       IN      SOA     mail.geekdept.com. hostmaster.mail.geekdept.com. (
                        10118      ; Serial
                        43200      ; Refresh
                        3600       ; Retry
                        3600000    ; Expire
                        2592000 )  ; Minimum
;       Define the nameservers and the mail servers
            IN      NS      192.168.0.45
            IN      A       192.168.0.45
            IN      MX      10 mail.geekdept.com.
```

Cambie su resolv.conf para utilizar la dirección IP de su servidor de correo, ya que es el DNS primario.

vim /etc/resolv.conf

```
search geekdept.com
nameserver 192.168.0.45
```

Inicie el llamado del servidor

/etc/init.d/named start

Habilitar el inicio automático de la llamada al servidor.

```
chkconfig named on
```

Para comprobar que se está funcionando se hace lo siguiente:

```
nslookup mail.geekdept.com
```

Debe devolver algo similar a esto:

```
Server:         192.168.0.45
Address:        192.168.0.45#53
Name:   mail.geekdept.com
Address: 192.168.0.45
```

Tenga en cuenta que la dirección IP devuelta es la misma que la máquina local. Eso significa que la instalación ha sido exitosa.

Ahora podemos pasar a la instalación de ZCS.

Instalación de Zimbra Collaboration Suite

Es necesario descargar desde el sitio Web ZCS Zimbra.

```
cd /tmp wget http://files.zimbra.com/downloads/5.0.2_GA/zcs-5.0.2_GA_1975.RHEL5.20080130221917.tgz
```

A continuación procedemos a descomprimir, cambiar al directorio del instalador y ejecutar el instalador.

```
tar xvzf zcs-5.0.2_GA_1975.RHEL5.20080130221917.tgz
cd zcs-5.0.2_GA_1975.RHEL5.20080130221917
./install.sh
```

El resultado debe ser algo así como:

Checking for existing installation...

zimbra-ldap...NOT FOUND

zimbra-logger...NOT FOUND

zimbra-mta...NOT FOUND

zimbra-snmp...NOT FOUND

zimbra-store...NOT FOUND

zimbra-apache...NOT FOUND

zimbra-spell...NOT FOUND

zimbra-proxy...NOT FOUND

zimbra-archiving...NOT FOUND

zimbra-cluster...NOT FOUND

zimbra-core...NOT FOUND

Leemos el acuerdo de licencia y pulsamos enter.

La salida debería ser similar a:

Checking for prerequisites...

NPTL...FOUND

sudo...FOUND sudo-1.6.7p12-10

libidn...FOUND libidn-0.6.5-1.1

fetchmail...FOUND fetchmail-6.3.6-1.1

gmp...FOUND gmp-4.1.4-10

compat-libstdc++-296...FOUND compat-libstdc++-296-2.96-138

compat-libstdc++-33...FOUND compat-libstdc++-33-3.2.3-61

libtool-ltdl...FOUND libtool-ltdl-1.5.22-6.1

/usr/lib/libstdc++.so.6...FOUND

Prerequisite check complete.

Checking for standard system perl...

perl-5.8.8...FOUND start system perl-5.8.8

Checking for installable packages

Found zimbra-core

Found zimbra-ldap

Found zimbra-logger

Found zimbra-mta

Found zimbra-snmp

Found zimbra-store

Found zimbra-apache

Found zimbra-spell

Found zimbra-proxy

Luego tenemos que seleccionar los paquetes a instalar. Los valores predeterminados se enumeran entre paréntesis por lo que sólo puede pulsar Enter para cada pregunta.

Install zimbra-ldap [Y]

Install zimbra-logger [Y]

Install zimbra-mta [Y]

Install zimbra-snmp [Y]

Install zimbra-store [Y]

Install zimbra-apache [Y]

Install zimbra-spell [Y]

Install zimbra-proxy [N]

Usted verá una advertencia como esta en la que indica que la instalación de paquetes se la realizará en una plataforma diferente de la plataforma para el que fueron construidos y que esto puede o no puede trabajar y si desea realizar la instalación de todos modos,

You appear to be installing packages on a platform different

than the platform for which they were built

This platform is CentOS5

Packages found: zimbra-core-5.0.2_GA_1975.RHEL5-20080130221917.i386.rpm

This may or may not work

Install anyway? [N] Y

The system will be modified. Continue? [N] Y

Una vez que la instalación haya finalizado se le presenta el menú principal. Se parece a esto:

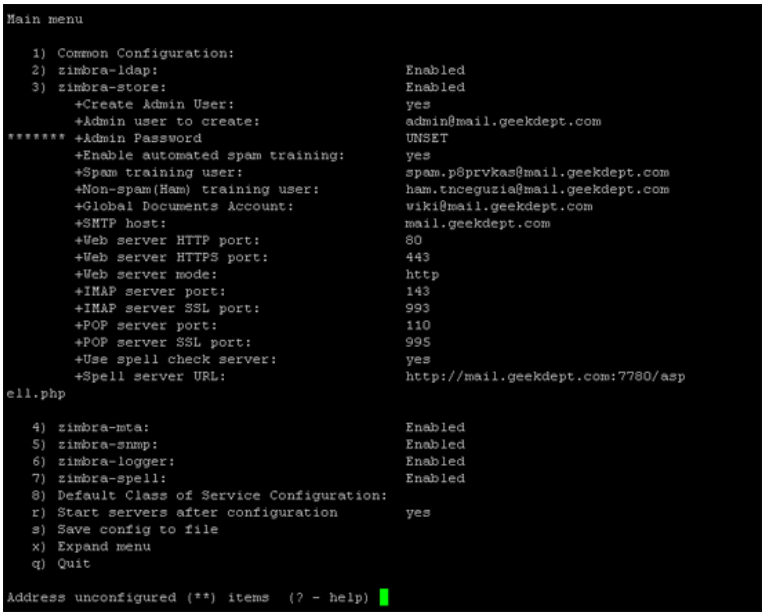

FIGURA XCIII.104 Menú principal de Zimbra Collaboration Suite

Tenga en cuenta los asteriscos al lado de la contraseña del administrador. Es necesario configurar la contraseña del administrador antes de completar la instalación. Para ello introduzca 3 en el indicador y pulse enter. El menú cambia a:

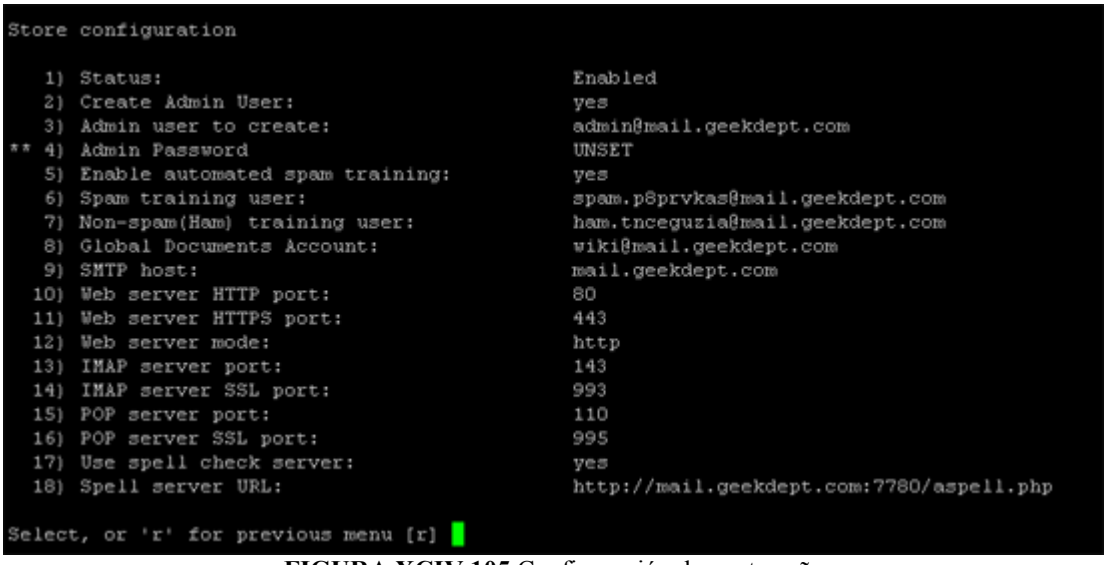

FIGURA XCIV.105 Configuración de contraseña

Ahora que usted elija 4. Se le pedirá que cambie la contraseña. Después de cambiar la contraseña pulse r, que le llevará de nuevo al menú anterior. Introduzca una en el indicador para guardar la configuración. La instalación se completará y estará listo para acceder a la interfaz Web de administración.

Interfaz Web de administración de ZCS.

Administración de sesión

Puede acceder a la interfaz web de administración, vaya a https://you.domain.com:7071 en el caso de nuestro servidor será: https://mail.geekdept.com:7071/zimbraAdmin/

Nota: La interfaz web se accede a través de SSL. Asegúrese de poner https de lo contrario no podrá acceder al sitio.

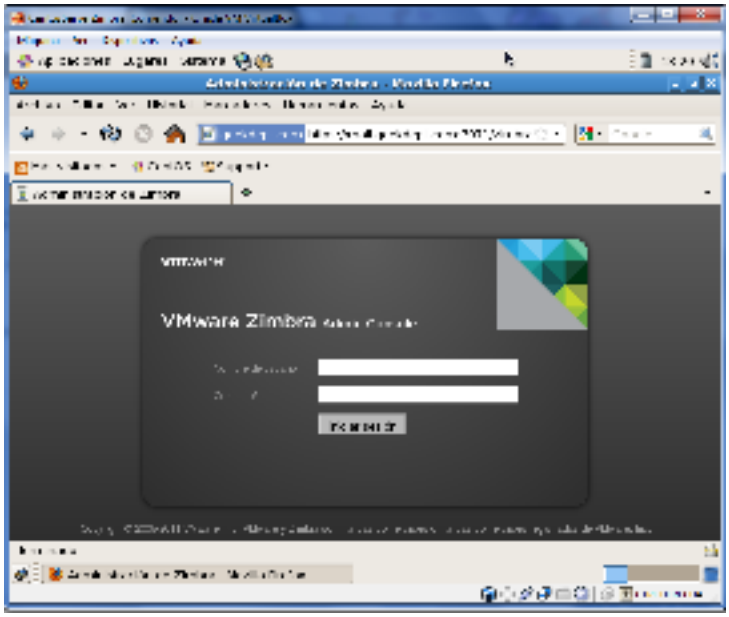

FIGURA XCV.106 Ingreso a la interfaz web con https://mail.geekdept.com:7071/zimbraAdmin/

La interfaz web es bastante fácil de navegar.

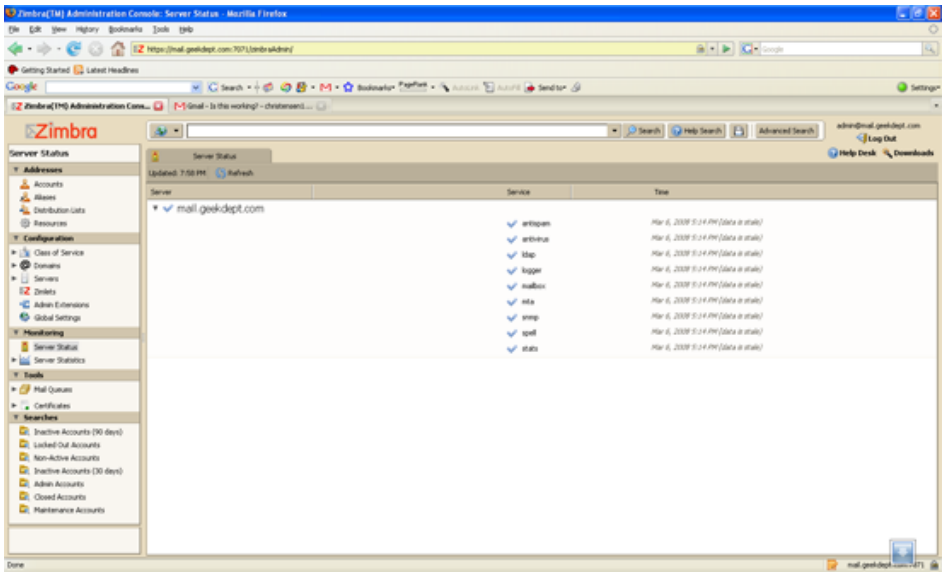

FIGURA XCVI.107 Navegación interfaz web

El mejor lugar para comenzar es con los dominios. En este momento lo más probable es tener un dominio como mail.geekdept.com. Se hace clic en los dominios.

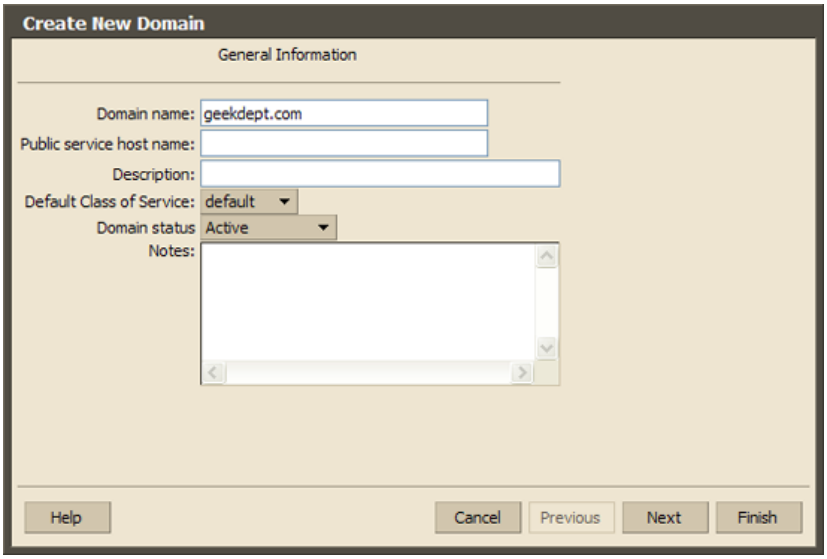

FIGURA XCVII.108 Creación de dominios

Después de haber agregado su dominio usted está probablemente va a querer agregar una cuenta de correo electrónico. Haga clic sobre las cuentas y añadir a su cuenta en primer lugar.

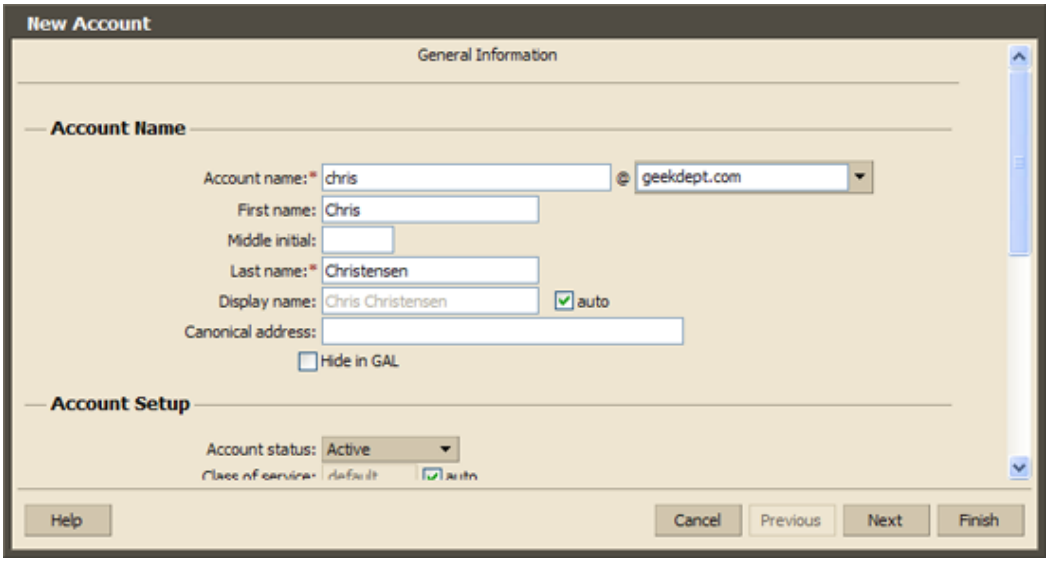

FIGURA XCVIII.109 Creación cuenta de Correo Electrónico

.

El Usuario Login

Ahora que tiene una configuración de la cuenta de correo electrónico se puede acceder a la interfaz de usuario. Dirija su navegador a http://your.domain.com.

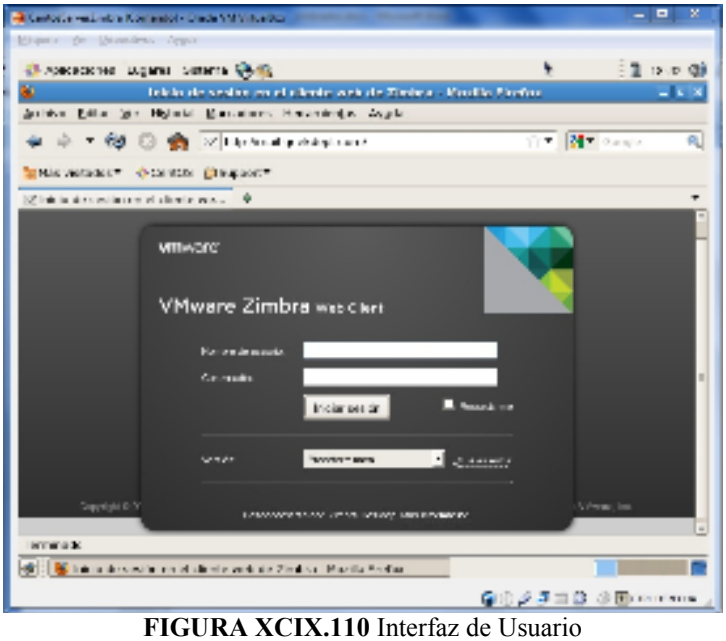

FIGURA XCIX.110 Interfaz de Usuario

Inicia sesión con tu dirección de correo electrónico completa y la contraseña que ha establecido para ello.

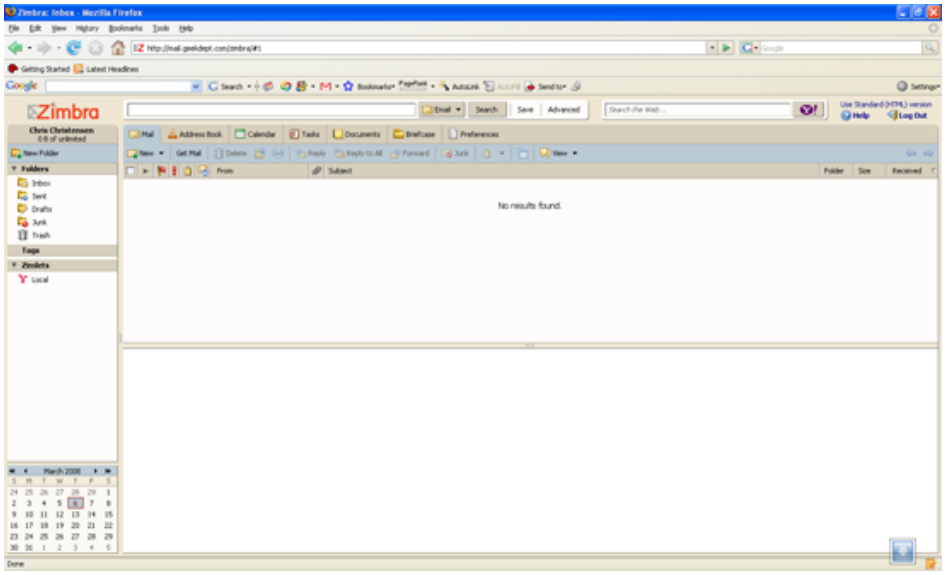

FIGURA C.111 Inicio de sesión cuenta de correo electrónico

Enviar algunos correos electrónicos de prueba para otra cuenta de correo electrónico para verificar que funciona correctamente.

Instalar Vsftpd en Centos

Si realizamos una instalación desde cero de un servidor con Linux y en muchas ocasiones, necesitaremos tener activado y configurado el FTP. Existen muchos servidores FTP. A continuación se instaló Very Secure FTP Daemon (VSFTPD).

Para hacerlo existen varias maneras. La más fácil es la siguiente:

Utilizaremos Yum para hacer la instalación utilizando:

```
yum install vsftpd
```

Ahora tenemos que hacer que se inicie como servicio cada vez que reiniciemos:

```
chkconfig vsftpd on
```

Reiniciamos el servicio:

```
/etc/init.d/vsftpd restart
```

Ya lo tenemos instalado, pero no hay ningún usuario que pueda utilizarlo. Tenemos que crear un usuario en nuestro FTP:

```
useradd NOMBRE DE USUARIO
```

Ahora tenemos que poner una clave a este usuario que hemos creado. Lo haremos escribiendo:

```
passwd NOMBRE DE USUARIO
```

Ahora podemos realizar una prueba y comprobar que todo está correcto.

Quizás queramos cambiar el home a este usuario que hemos creado, para ello utilizaremos lo siguiente:

```
usermod -d /ruta/a/nueva/carpeta/ NOMBRE DE USUARIO
```

Iniciar, detener, y reiniciar el servicio vsftpd.

Para iniciar por primera vez el servicio vsftpd, ejecute el siguiente mandato:

service vsftpd start

Para reiniciar el servicio vsftpd, o bien hacer que los cambios hechos a la configuración surtan efecto, ejecute el siguiente mandato:

service vsftpd restart

Para detener el servicio vsftpd, ejecute el siguiente mandato:

service vsftpd stop

Agregar el servicio vsftpd al arranque del sistema.

Para hacer que el servicio de vsftpd esté activo con el siguiente inicio del sistema, en todos los niveles de ejecución (2, 3, 4, y 5), se utiliza lo siguiente:

chkconfig vsftpd on

Inicio gFTP

Sólo nos queda teclear en una terminal o en un lanzador el comando gftp, y el programa aparecerá en la pantalla, si queremos usar el modo texto tendremos que teclear en una terminal: gftp-text.

Posteriormente a la conexión misma del Servidor con el cliente se procedió a realizar la transferencia de archivos de la siguiente manera.

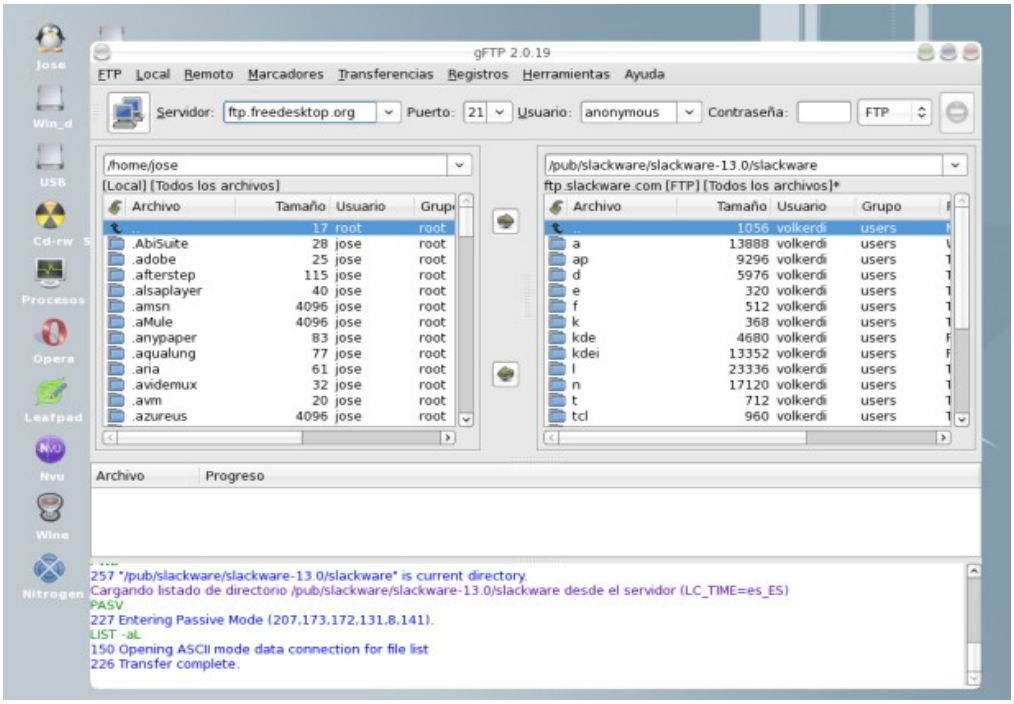

FIGURA CI.112 Inicio de sesión

Para cada uno de los archivos se muestra sus respectivas propiedades que a continuación se muestra

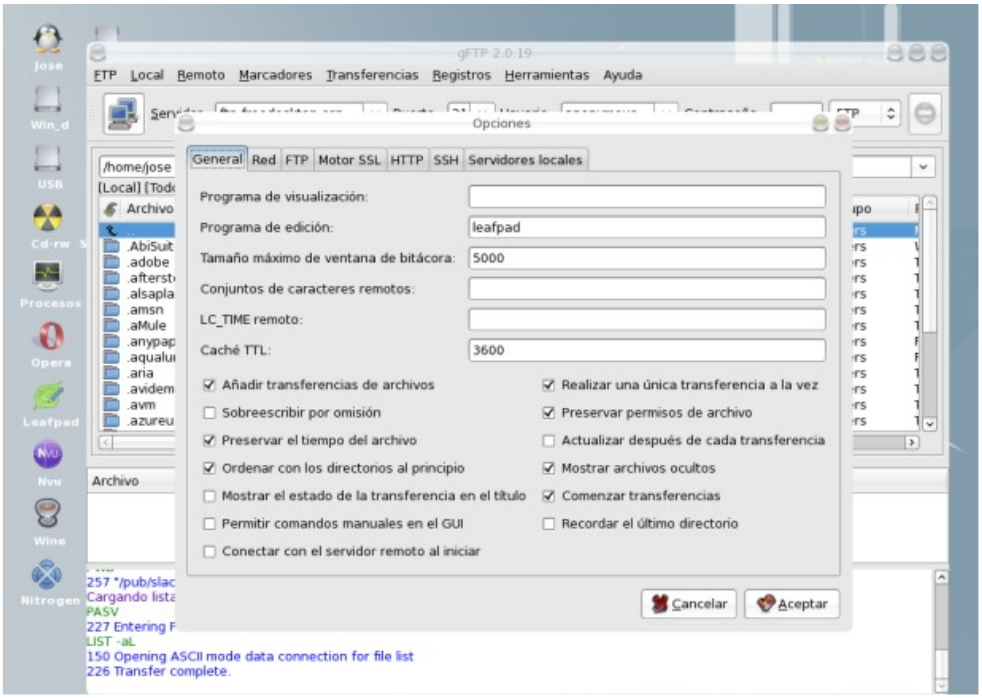

FIGURA CII.113 Inicio de sesión cuenta de correo electrónico

Normalmente los permisos de un directorio remoto suelen estar establecidos en 755 (lectura y ejecución para todos y escritura para el dueño) y para los archivos, 644 (lectura para todos y escritura para el dueño). A continuación se muestra la ventana de diálogo de asignación de permisos más comunes cuando trabajamos con un directorio remoto del que somos propietarios. Esta ventana de diálogo se abre al seleccionar un directorio o archivo y al desplegar el menú con el clic derecho del ratón y seleccionar **Permisos**

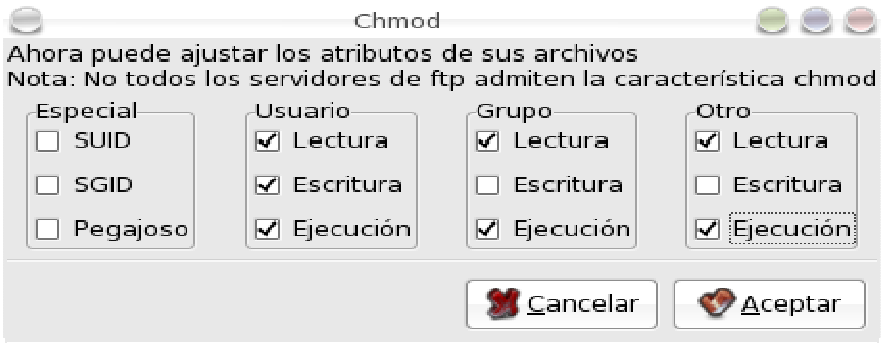

FIGURA CIII.114 Permisos de un directorio remoto 755

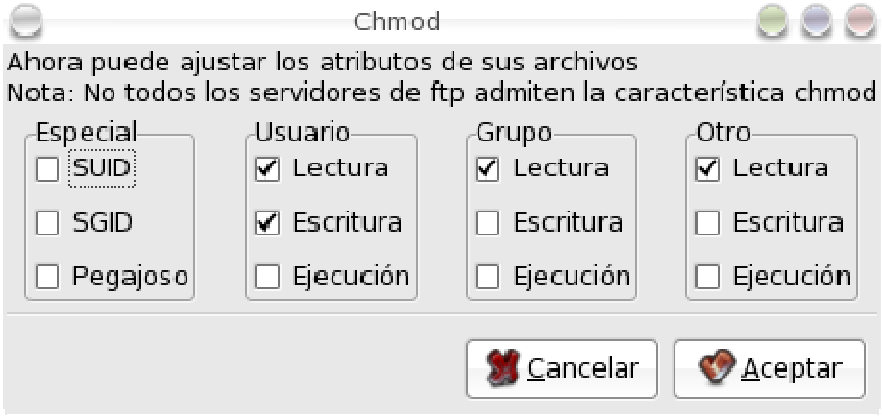

FIGURA CIV.115 Permisos de un directorio remoto 644

El 777 se suele utilizar en galerías de imágenes como las de Coppermine para permitir que todos los usuarios autorizados puedan escribir en el directorio de las imágenes de la galería.

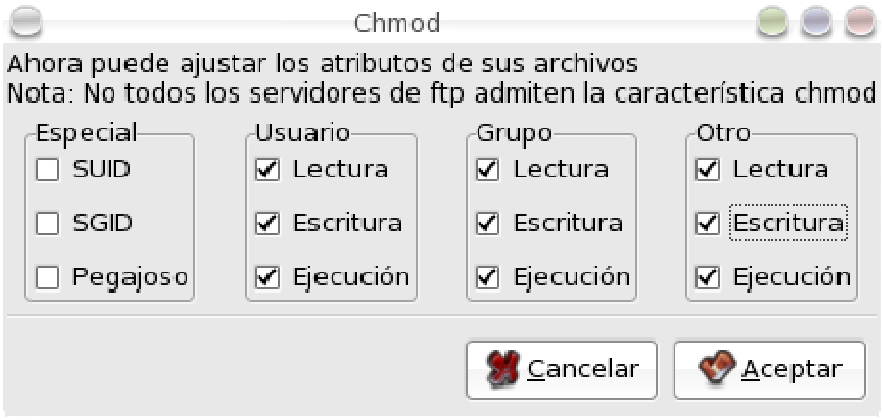

FIGURA CV.116 Permisos de un directorio remoto 777

El 444 es recomendable usarlo para aquellos archivos de configuración críticos que se suelen editar de forma manual para evitar un borrado accidental de éstos, tener en cuenta que al establecer los permisos en sólo lectura, no podremos borrar el archivo o directorio en cuestión hasta que no los volvamos a cambiar y le volvamos a asignar permisos de escritura.

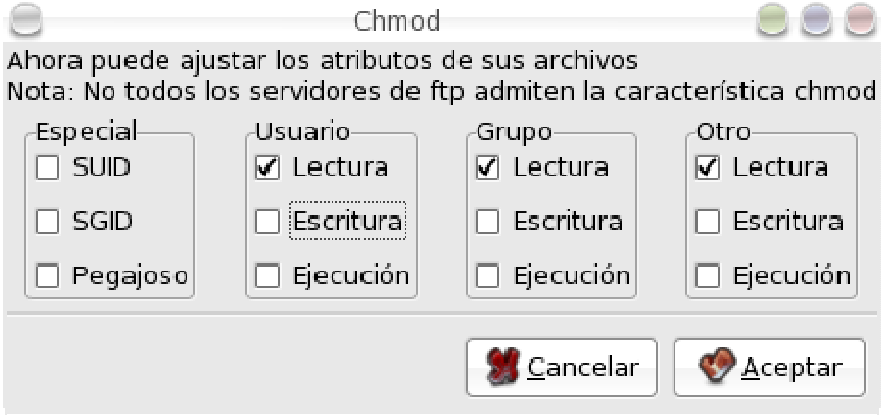

FIGURA CVI.117 Permisos de un directorio remoto 777

Y por último cabe recalcar la posibilidad de aplicar filtros a la hora de trabajar con los archivos, esto es muy sencillo y basta seleccionar en el menú que desplegamos con el clic derecho del ratón, la entrada **Cambiar filtro**, y añadir al comodín la extensión o palabra clave oportuna que haga referencia a un determinado grupo de archivos, también se debe dejar el comodín como estaba cuando finalice este proceso, ya que de lo

contrario no saldría ningún archivo o directorio en la ventana del árbol de directorios en la que estemos trabajando excepto los coincidentes con el filtro utilizado. Lo ideal sería que los archivos coincidentes con el filtro aparecieran seleccionados y el resto no desapareciera visualmente como sucede con el sistema de filtrado que utiliza **gFTP.**

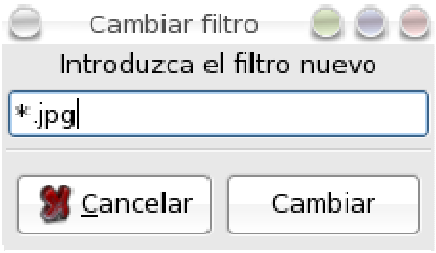

FIGURA CVII.118 Aplicación de filtros a los archivos

CAPÍTULO IV

4. ANÁLISIS Y EVALUACIÓN FINAL DE RESULTADOS

4.1. Marco Metodológico

QoS o Calidad de Servicio son las tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado generalmente se aplica a nivel de la capa 3-4. Es de trascendental importancia para las aplicaciones de tiempo real como la transmisión de vídeo y voz (Videollamada), video streaming, radio por Internet, etc.

El entorno inalámbrico es muy hostil para medidas de Calidad de Servicio debido a su variabilidad con el tiempo, ya que puede mostrar una calidad nula en un cierto instante de tiempo. Esto implica que satisfacer la QoS resulta imposible para el 100% de los casos, lo que representa un serio desafío para la implementación de restricciones de máximo retardo y máxima varianza en el retardo (jitter) en sistemas inalámbricos.

Las gráficas obtenidas y expuestas en el presente capitulo se benefician de una completa validez al mismo tiempo que representan resultados formales pues fueron obtenidos de escenarios reales.

4.1.1. Diseño de la investigación

La presente investigación se enmarca dentro de un estudio **Cuasi-Experimental**, ya que se trabaja en escenarios y subescenarios ya definidos con videollamadas las últimas si tomadas al azar dentro de un conjuntos numeroso de pruebas y además se manipula una variable independiente. Su validez se alcanzará a

medida que se demuestre el nivel de rendimiento en las videollamadas sobre redes inalámbricas, después de haber aplicado el protocolo Diffserv para la Provisión de QoS luego de ejecutado el análisis comparativo.

4.1.2. Métodos, Técnicas e Instrumentos

Métodos.-

Para este proyecto se utilizarán los siguientes métodos de investigación para conseguir los resultados de los objetivos planteados:

Método Científico: El método científico normalmente se divide en pasos, esto ayuda a poner al método dentro de contexto. Podríamos decir que una investigación y, como consecuencia, un conocimiento, se considera científica cuando es posible presentar los hechos en forma de enunciados, hipótesis, conceptos, teorías explicativas y, a partir de estas, poder deducir unas consecuencias cuyo grado de comprobación lógica o empírica nos permiten consolidar o reformular las teorías de las que se parte.

Utilizaremos este método como soporte ya que las ideas, conceptos, y teorías expuestas en este anteproyecto de tesis son verificables como válidas, además que servirá para recopilar la información necesaria para descubrir el aumento de rendimiento en las aplicaciones de tiempo real en cada uno de los escenarios y por ende de subescenarios a ser implementados.

- Se plantea la investigación en base al rendimiento obtenidos de las videollamadas en dos ámbitos diferentes que son el ámbito con Calidad de Servicio y el ámbito sin calidad de Servicio.
- Se trazan los objetivos de la investigación.
- Se justifican los motivos por los cuales se propone realizar la siguiente investigación.
- Se elabora un marco teórico que ayude a realizar un análisis del protocolo Diffserv aplicado a la provisión de QoS en el tráfico de videollamadas.
- Se plantea una hipótesis la cual es una posible respuesta al problema planteado y posee una íntima relación entre el problema y el objetivo.
- Se propone la operacionalización de las variables en base a la hipótesis planteada.

- Se realiza la recolección de datos, a través de diferentes pruebas y se analiza el rendimiento de las videollamadas en cada uno de los ámbitos establecidos.
- Se realiza la prueba de la hipótesis con los resultados obtenidos.
- Se elabora las conclusiones y recomendaciones, producto de la investigación realizada.

Método Analítico – Sintético: Este método, como lo dice su nombre, es el análisis que se realizará de los aspectos delimitados de la presente investigación que permitirá conocer, comprender y estudiar el objeto de estudio en partes y del todo investigado en sus diferentes componentes para el planteamiento de la metodología propuesto por los autores. El método analítico como su nombre lo indica abarca el análisis, esto es la separación de un tono en sus partes o en sus elementos constitutivos. Se apoya en que para conocer un fenómeno es necesario descomponerlo en sus partes. En cuanto al método Sintético Implica la síntesis esto es, unión de elementos para formar un todo. Este método Analítico-Sintético es aplicado en la sistematización de la bibliografía, que será analizada para entenderla y describirla.

Método Comparativo: Es necesario apoyarnos en un método comparativo ya que la base de nuestra investigación es comparar el rendimiento de las videollamadas realizadas en ámbitos con provisión de calidad de servicio y sin provisión de calidad de servicio en los diferentes escenarios y subescenarios.

Técnicas: Entre las técnicas a utilizarse están:

Observación

Investigación Bibliográfica

Análisis

Investigación Bibliográfica

Razonamiento

Pruebas

4.1.3. Instrumentos:

De acuerdo a la naturaleza de la investigación, los instrumentos más apropiados para la recolección de los datos fueron las guías, papers, información bibliográfica, con esto se pudo establecer los parámetros de comparación para realizar el estudio que dará como resultado el ámbito (con QoS o sin QoS) más adecuado para la realización de las aplicaciones en tiempo real específicamente de las videollamadas.

4.1.4. Validación de los instrumentos

La validez de los instrumentos depende del grado en que se mide el rendimiento de las variables que intervienen en la investigación. De tal forma que para determinar la validez de los instrumentos se basó en la forma como lo hacen las revistas especializadas al realizar comparaciones de todo tipo utilizando para esto observaciones directas y comparaciones entre los resultados obtenidos a través del analizador de protocolos.

4.1.5. Procesamiento de la información

Para realizar el estudio comparativo, se tomó en consideración ciertos parámetros (indicadores), que nos permitirán evaluar la calidad de las videollamadas durante su ejecución.

Los parámetros han sido tomados de revistas especializadas, estudios de tesis, foros de internet, entre otros y estos son: Jitter, Latencia y Pérdida de paquetes.

Los índices concernientes a cada parámetro han sido evaluados cuantitativamente y expuestos en tablas individuales realizadas por parámetro, luego de esto se realizará una tabla de resumen a la cual se le asignará pesos, mediante una escala de valoración cualitativa para escoger la tecnología adecuada que se utilizará para el desarrollo del ambiente de pruebas.

En lo referente a dicho ambiente de pruebas, se validará la variable dependiente mediante cada uno de sus indicadores todo esto asociado al valor obtenido en los índices, para esto se utilizará el analizador de protocolos con el que se podrá obtener información del desempeño en los dos ámbitos de pruebas.

Se instaló el software de Elastix en un equipo de cómputo, el cual funciona como un servidor PBX, a este se tiene acceso por medio de un servidor Web contenido en el software, en Elastix se configuraron cinco extensiones de VoIP y para de esta forma poder establecer la comunicación punto a punto.
Una vez dadas de altas las extensiones en Elastix, procedimos a configurar los softphones (X-Lite) en dos laptops diferentes.

Ya que los softphones quedaron correctamente instalados y dados de alta en nuestra PBX, posteriormente procedimos a realizar distintas pruebas de videollamadas de aproximadamente 900 segundos en rangos de 180 segundos cada una, al mismo tiempo en dos Laptop.

Durante la duración de la llamada, esta fue monitoreada por medio de Wireshark. Del total de los resultados del monitoreo de las llamadas solo se presentan algunas pruebas.

Escenarios

Para realizar un acertado análisis del rendimiento en las video-llamadas se implementó dos escenarios con equipos Cisco y Linux respectivamente.

Observación: El Escenario con equipos Cisco no pudo ser concluido ya que la tarjeta Wireless Lan Controller si bien existe la misma, no se encuentra en buenas condiciones por lo que se hace imposible concluir la investigación en dichos equipos en la Figura III.28 y III.29 está demostrado y debidamente expuesta la nulidad de la tarjeta PERO realizaremos la demostración de la hipótesis apoyándonos totalmente en el escenario con equipos Linux el mismo que fue concluido satisfactoriamente en su totalidad.

Para las pruebas realizadas se decidió presentar en el escenario antes propuesto subescenarios a través de los cuales se proporcionan diferentes niveles de congestión para el router, todo esto debido a que en casos de extrema congestión, los routers comienzan a “rechazar” paquetes, disminuyendo de esta forma el rendimiento del sistema, de esta manera lograremos un mejor análisis comparativo al momento de tabular y analizar los datos en los escenarios sin – con calidad de servicio.

Subescenarios

- Videollamadas sin Señal de Video
- Videollamadas con Señal de Video
- Videollamadas – Servidor de Correo Electrónico
- Videollamadas – Servidor Web
- Videollamadas – Servidor FTP
- Videollamadas – Servidor FTP – Servidor Web
- Videollamadas –Servidor FTP – Servidor Web – Servidor de Correo Electrónico

Después de haber realizado la implementación y las diferentes pruebas en los subescenarios se pudo realizar el análisis comparativo entre cada uno de los ámbitos establecidos con ayuda de los diferentes parámetros o indicadores planteados en la operacionalización de las variables.

4.1.6. Planteamiento de la Hipótesis

"LA ADMINISTRACIÓN DE QOS EN LAS REDES INALÁMBRICAS, GARANTIZARÁ QUE LAS VIDEOLLAMADAS LOGREN TRANSMITIRSE CON MAYOR RENDIMIENTO"

4.1.7. Determinación de las variables

De acuerdo a la hipótesis se han identificado dos variables:

Variable Independiente:

QoS

Variable Dependiente:

Garantizará que las videollamadas logren transmitirse con mayor rendimiento

4.1.8. Operacionalización Conceptual de las Variables

TABLA IV.3. Operacionalización Conceptual de variables

Variable	Tipo	Definición
Administración de QoS en Redes Inalámbricas	Independiente	Es un conjunto de estándares y mecanismos que aseguran la calidad en la transmisión de los datos. Indudablemente la implantación de redes inalámbricas han modificación las formas de comunicación en el mundo; por lo tanto hoy en día es fundamental, para cualquier compañía, un medio que facilite dicha comunicación.
Rendimiento en la transmisión de Videollamadas	Dependiente	Se refiere a la cuantificación del resultado con que se realiza la videollamada. Depende principalmente de los parámetros tales como el jitter, la latencia y la pérdida de paquetes es decir el nivel de calidad o aceptabilidad de la aplicación en tiempo real.

4.1.9. Operacionalización Metodológica de las Variables

TABLA IV.4XIX. Operacionalización Metodológica de variables

Variables	Indicadores	Índices	Técnica	Fuente de Información
Rendimiento en la transmisión de videollamadas	Jitter Latencia	Subescenario1 Subescenario2 Subescenario3 Subescenario4 Subescenario5	Observación Pruebas Análisis	Analizador de Protocolos (Wireshark) Referencia Bibliográficas

TABLA IV.XIX. Operacionalización Metodológica de variables (Continuación)

	Pérdida de Paquetes	Subescenario6 Subescenario7		
Administración de QoS en Redes Inalámbricas	Sistema Operativo Tráfico		-Observación -Investigación Bibliográfica -Razonamiento - Análisis	Papers Internet Referencia Bibliográficas Proyectos Similares Recopilación de información.

4.1.10. Población y Muestra

La población es el conjunto de todas las pruebas de videollamadas realizadas en cada uno de los subescenarios ya establecidos anteriormente. En la presente investigación las videollamadas fueron realizadas en un ámbito proveído de calidad de servicio y un segundo ámbito sin provisión de Calidad de Servicio.

De esta población se seleccionó una muestra no probabilística, ésta es una red inalámbrica de prueba, que se construyó para tomar los datos necesarios para el desarrollo de este proyecto.

4.2. ANÁLISIS, COMPARACIÓN E INTERPRETACIÓN DE RESULTADOS

4.2.1. Determinación de parámetros de comparación

Para realizar el estudio comparativo del rendimiento de las videollamadas sin QoS y con QoS, se tomó en consideración ciertos parámetros, que nos permitirán evaluar el rendimiento de cada uno de los ámbitos seleccionados como son el ámbito en el que se ha proveído Calidad de Servicio y el ámbito en el que no se ha proveído Calidad de Servicio.

Los parámetros han sido tomados de los datos que nos proporciona el Wireshark que es el analizador de protocolos que hemos seleccionado y son:

Jitter

El jitter se define técnicamente como la variación en el tiempo en la llegada de los paquetes, causada por la congestión de la red, pérdida de sincronización o por las diferentes rutas seguidas por los paquetes para llegar al destino. Las comunicaciones en tiempo real (como VoIP) son especialmente sensibles a este efecto. En general, es un problema frecuente en enlaces lentos o congestionados.

Latencia

La latencia conocida también como retardo se define técnicamente como el tiempo que tarda un paquete en llegar desde la fuente al destino.

Pérdida de Paquetes

Las comunicaciones en tiempo real están basadas en el protocolo UDP. Este protocolo no está orientado a conexión y si se produce una pérdida de paquetes no se reenvían. Además la perdida de paquetes también se produce por descartes de paquetes que no llegan a tiempo al receptor. Sin embargo la voz es bastante predictiva y si se pierden paquetes aislados se puede recomponer la voz de una manera bastante óptima. El problema es mayor cuando se producen pérdidas de paquetes en ráfagas.

4.2.2. Resultados

Sin Implementar Calidad de Servicio

Subescenario N°1 Videollamada sin Señal de Video

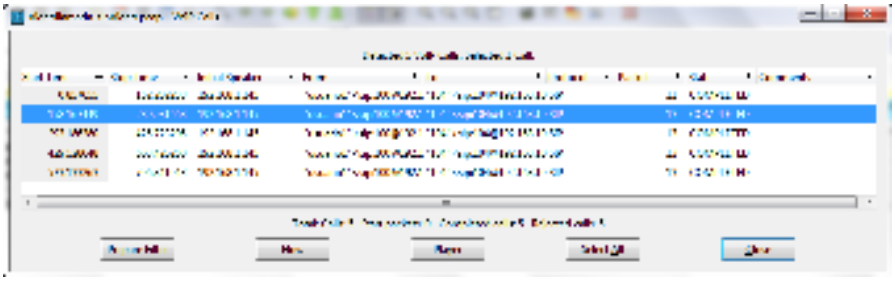

FIGURA CVIII.119 Video llamadas VoIP realizadas

Acceda al menú Statistics -> IO Graphs, lo que permitirá representar gráficamente el consumo de ancho de banda de la captura del tráfico.

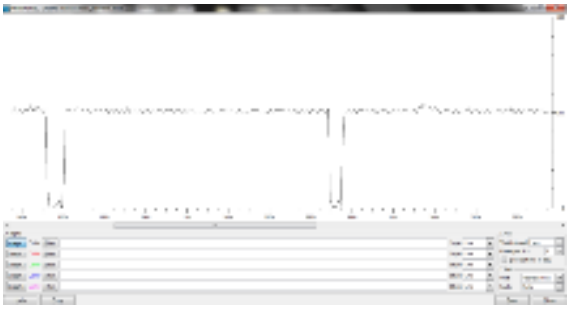

FIGURA CIX.120 Ancho de Banda del video llamada.

El programa wireshark tiene varias herramientas para el análisis de voz sobre IP en la cual se utilizara la opción RTP y la opción VoIPCalls que se encuentran el menú Telephony. En RTP se da clic en Show ALL Streams, donde se muestra todo los stream que existieron en la captura.

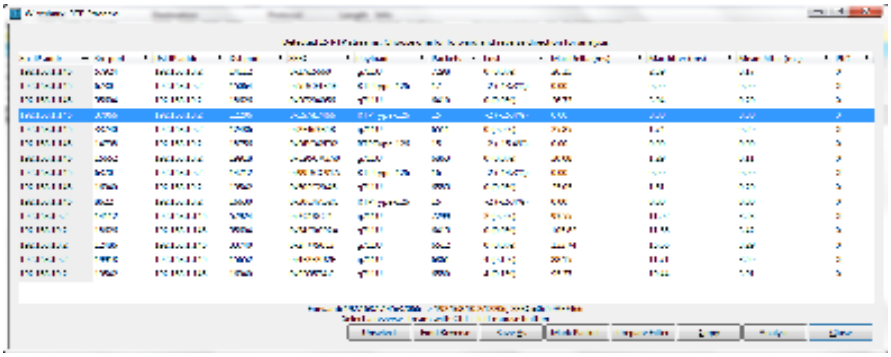

FIGURA CXV.121 RTP Streams.

A través de esta pantalla se podrá realizar un mejor análisis del tráfico, visualizando el porcentaje de paquetes perdidos (Lost %), máx jitter [ms] y max retardo [ms] (Max Delta).

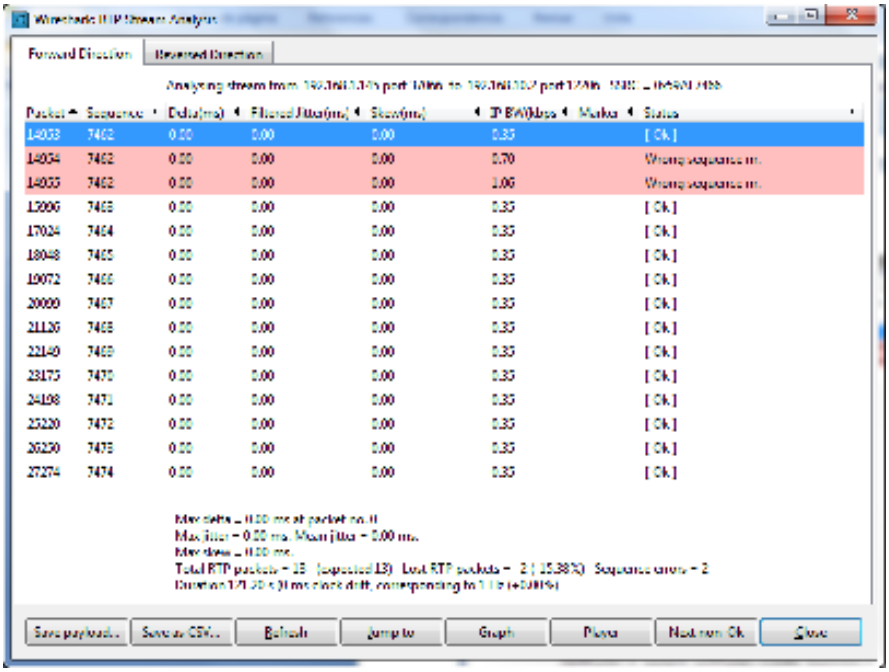

FIGURA CXI.122 Análisis del RTP Streams

Subescenario N°2 Videollamada con Señal de Video

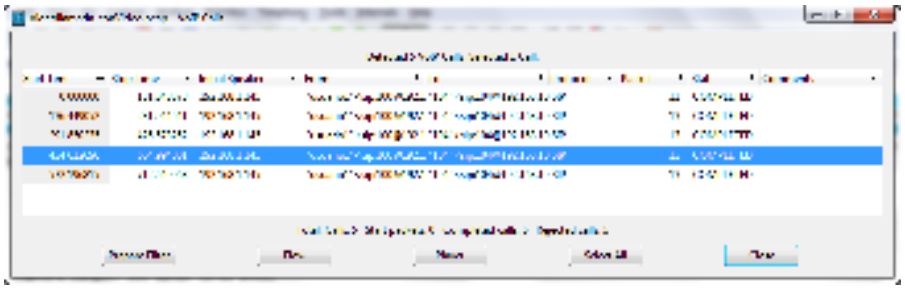

FIGURA CXII.123 Video llamadas VoIP realizadas

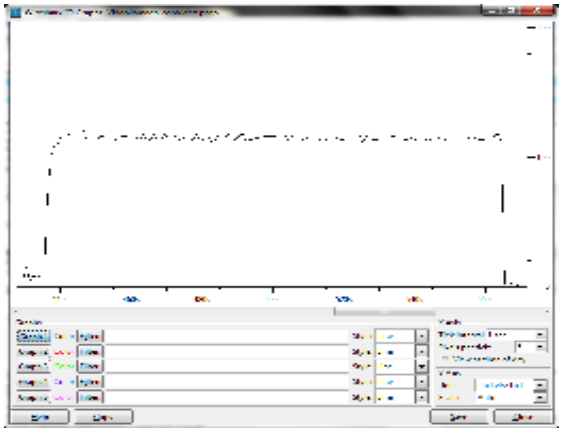

FIGURA CXIII.124 Ancho de Banda del video llamada.

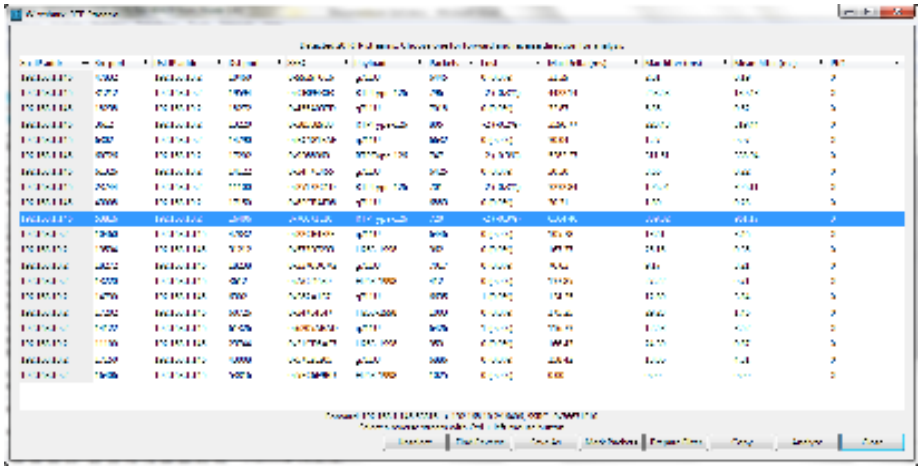

FIGURA CXIV.125 RTP Streams.

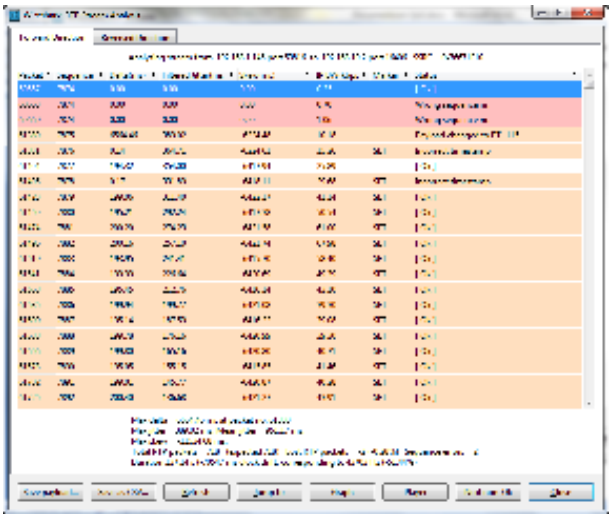

FIGURA CXV.126 Análisis del RTP Streams

Subescenario N°3 Videollamada – Servidor de Correo Electrónico

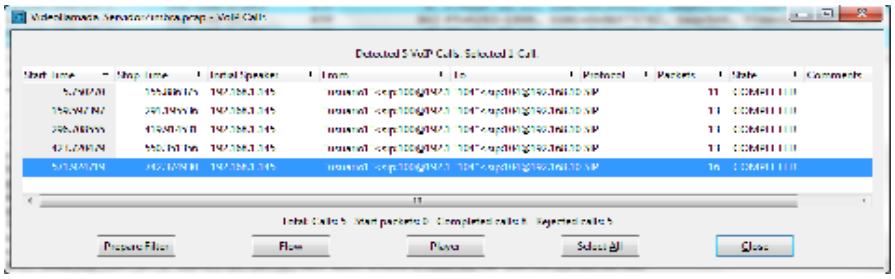

FIGURA CXVI.127 Video llamadas VoIP realizadas

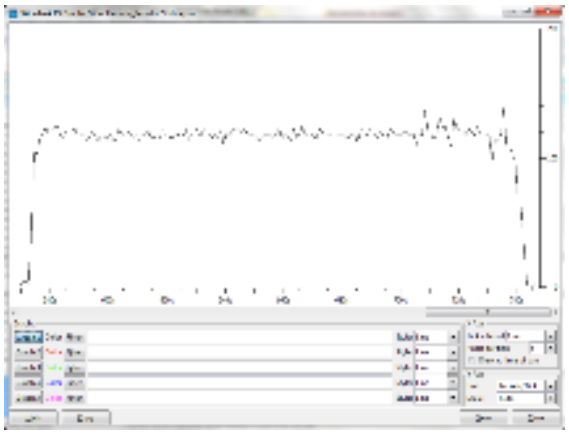

FIGURA CXVII.128 Ancho de Banda del video llamada.

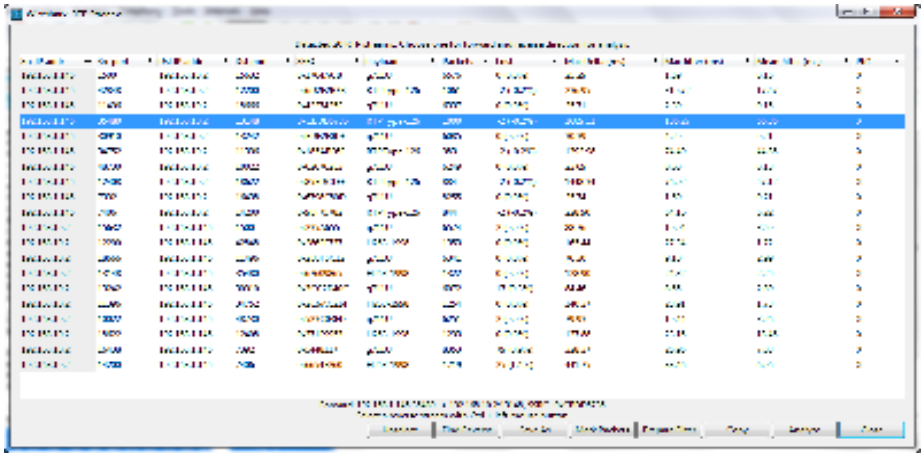

FIGURA CXVIII.129 RTP Streams.

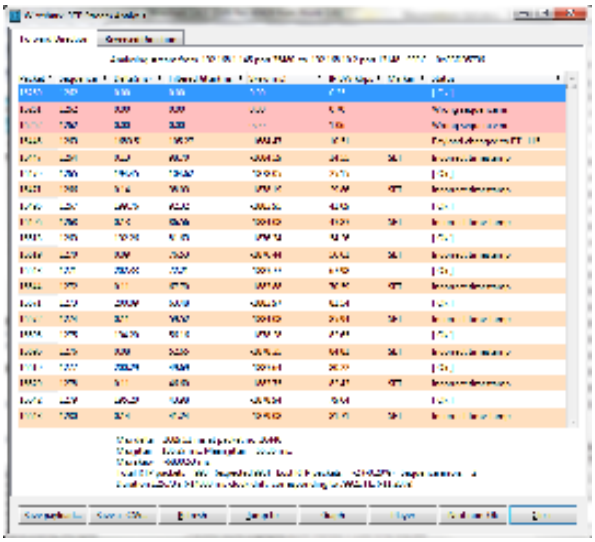

FIGURA CXIX.130 Análisis del RTP Streams

Subescenario N°4 Videollamada – Servidor Web

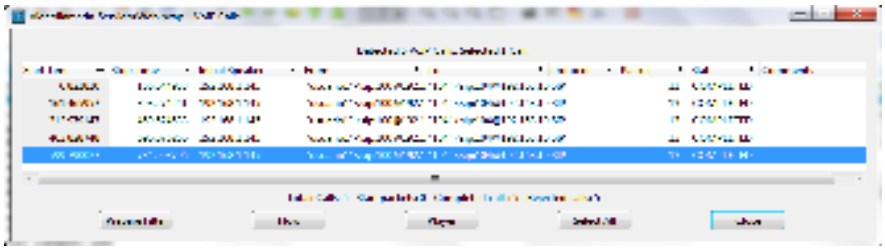

FIGURA CXXV.131 Video llamadas VoIP realizadas

FIGURA CXXI.132 Ancho de Banda del video llamada.

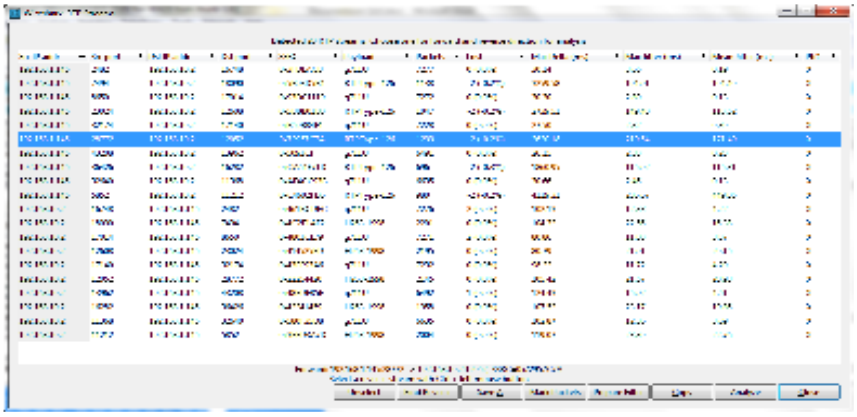

FIGURA CXXII.133 RTP Streams

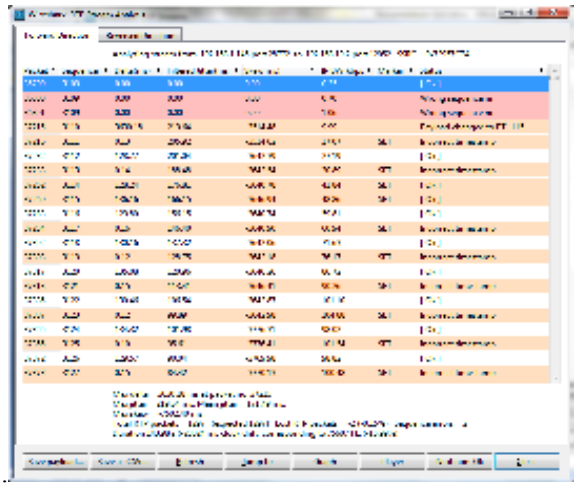

FIGURA CXXIII.134 Análisis del RTP Streams

Subescenario N°5 Videollamada – Servidor FTP

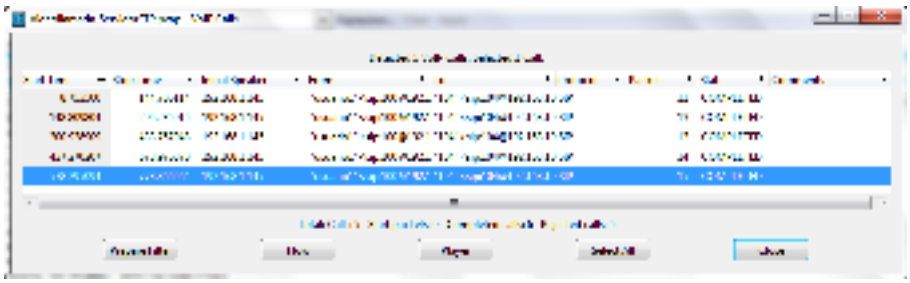

FIGURA CXXIV.135 Video llamadas VoIP realizadas

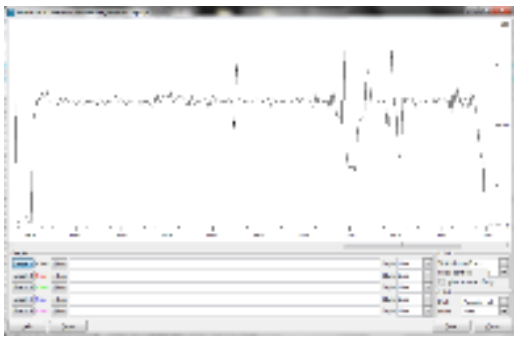

FIGURA CXXV.136 Ancho de Banda del video llamada.

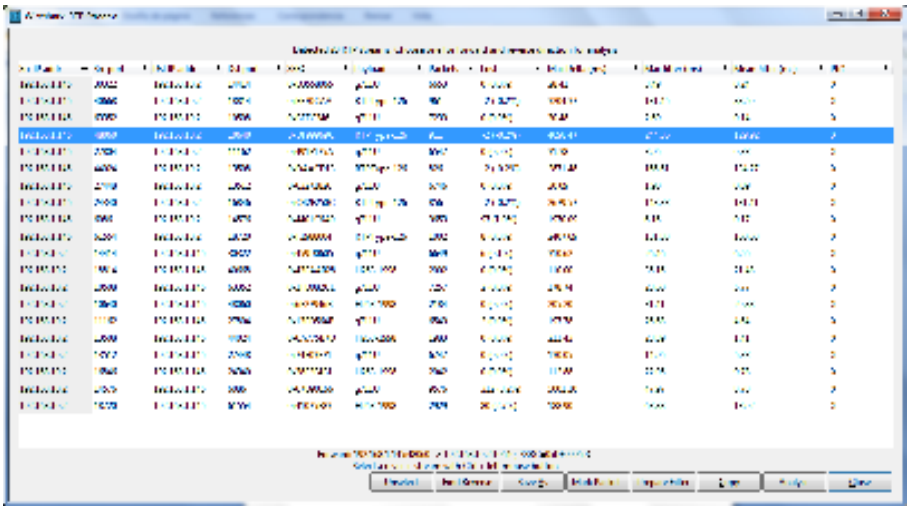

FIGURA CXXVI.137 RTP Streams.

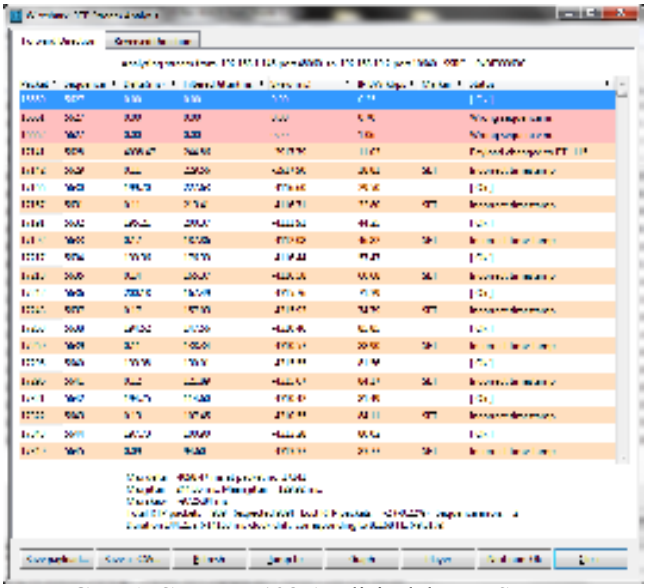

FIGURA CXXVII.138 Análisis del RTP Streams

Subescenario N°6 Videollamada – Servidor FTP – Servidor Web

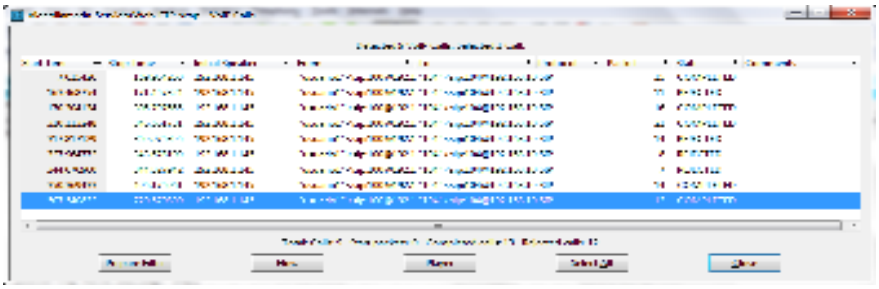

FIGURA CXXVIII.139 Video llamadas VoIP realizadas

FIGURA CXXIX.140 Ancho de Banda del video llamada.

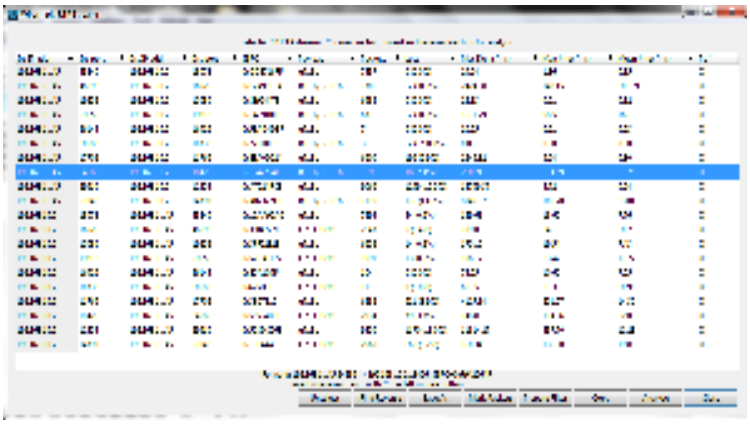

FIGURA CXXX.141 RTP Streams.

FIGURA CXXXI.142 Análisis del RTP Streams

Subescenario N°7 Videollamada – Servidor FTP – Servidor Web – Servidor de Correo Electrónico

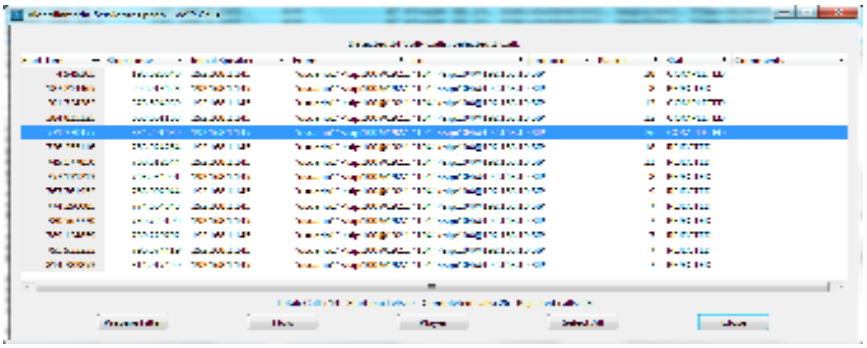

FIGURA CXXXII.143 Video llamadas VoIP realizadas

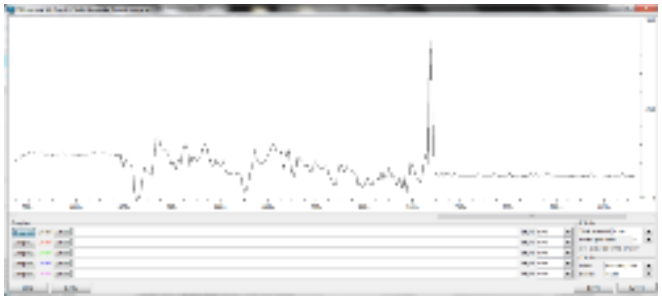

FIGURA CXXXIII.144 Ancho de Banda del video llamada.

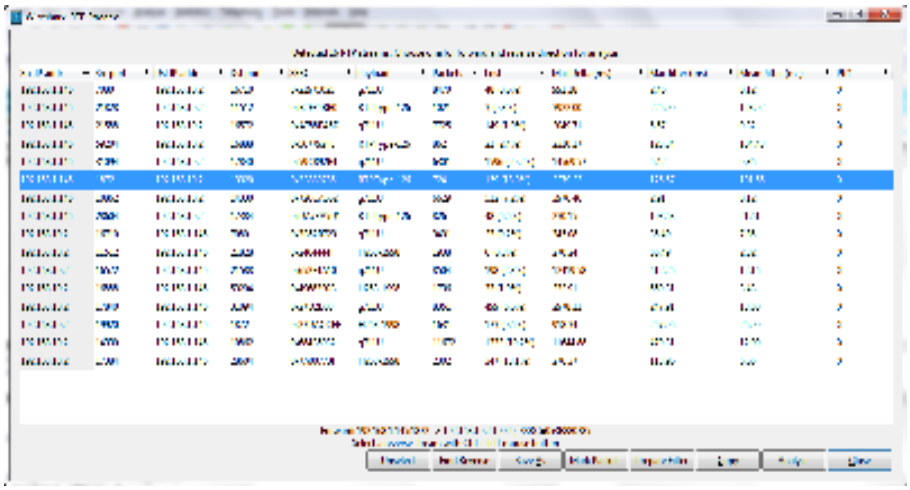

FIGURA CXXXIV.145 RTP Streams.

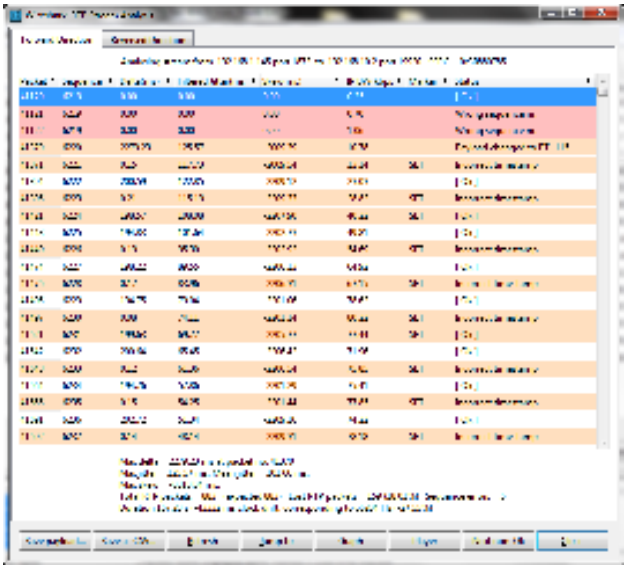

FIGURA CXXXV.146 Análisis del RTP Streams

Subescenario N°1 Videollamada sin Señal de Video

FIGURA CXXXVI.147 Video llamadas VoIP realizadas

FIGURA CXXXVII.148 Ancho de Banda del video llamada.

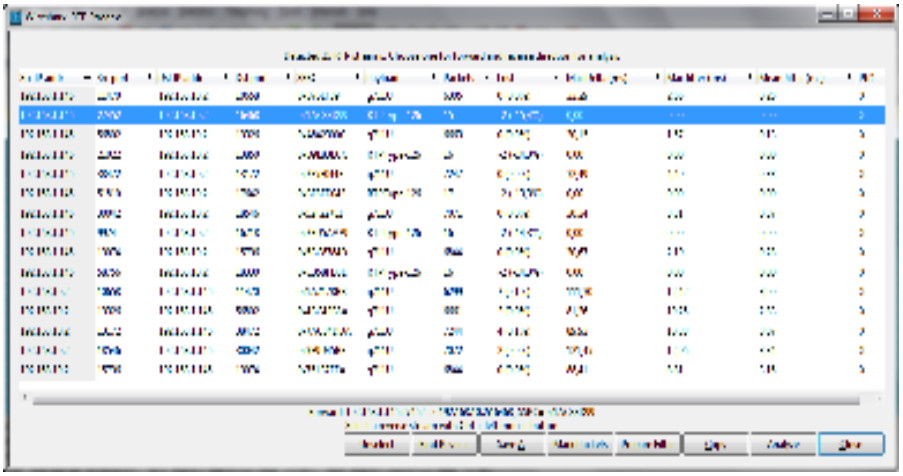

FIGURA CXXXVIII.149 RTP Streams.

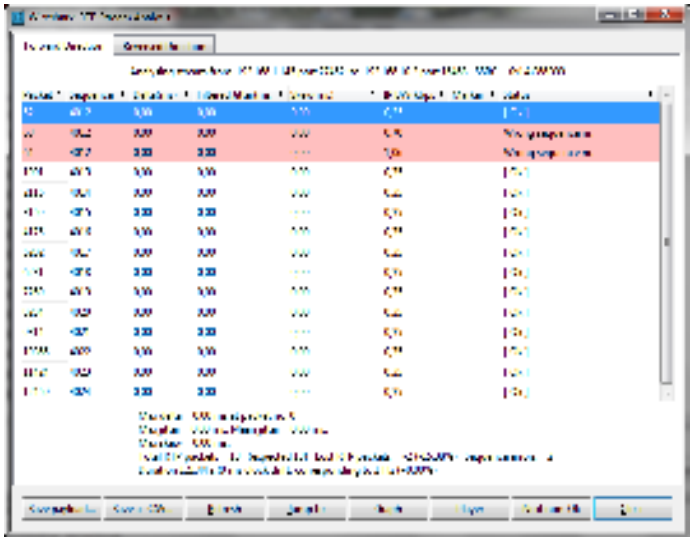

FIGURA CXXXIX.150 Análisis del RTP Streams

Subescenario N°2 Videollamada con Señal de Video

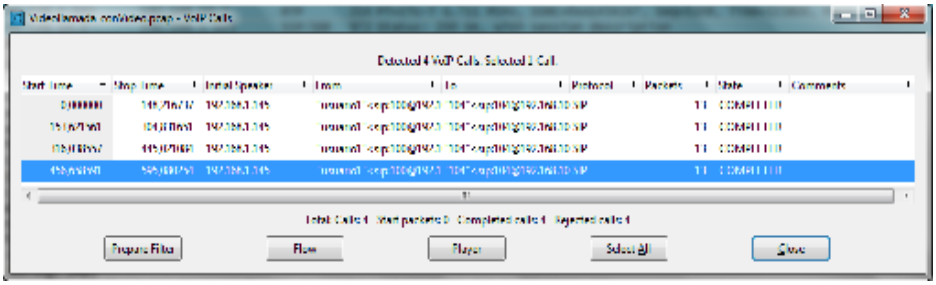

FIGURA CXL.151 Video llamadas VoIP realizadas

FIGURA CXLI.152 Ancho de Banda del video llamada.

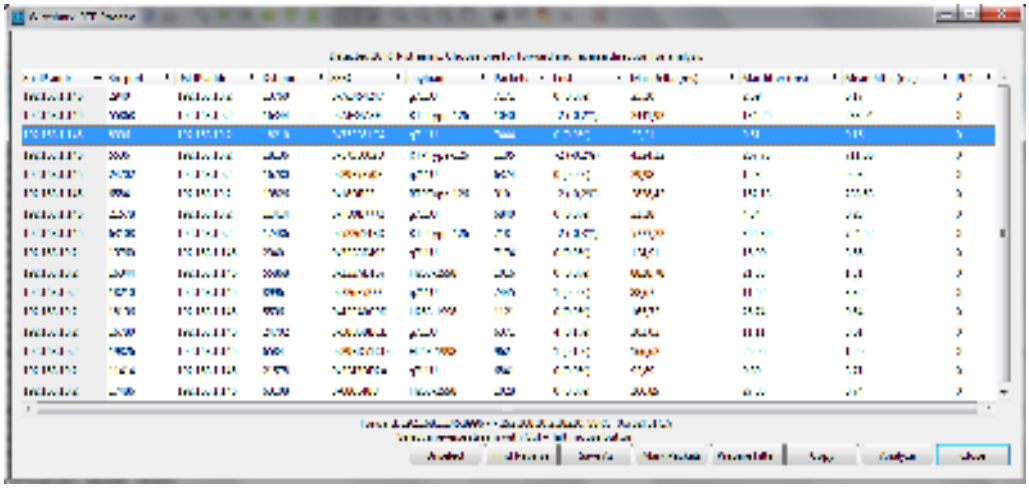

FIGURA CXLII.153 RTP Streams

.

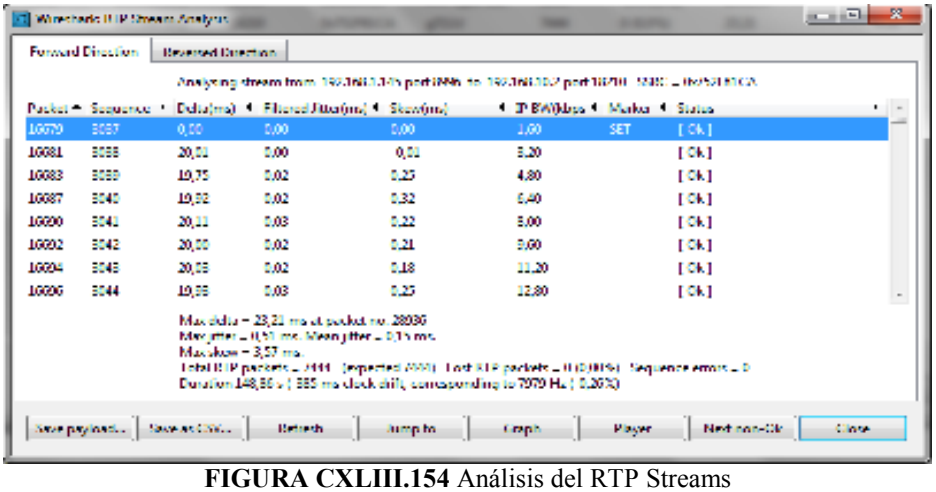

FIGURA CXLIII.154 Análisis del RTP Streams

Subescenario N°3 Videollamada – Servidor de Correo Electrónico

FIGURA CXLIV.155 Video llamadas VoIP realizadas

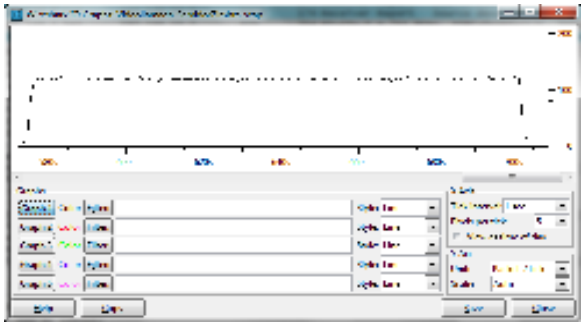

FIGURA CXLV.156 Ancho de Banda del video llamada.

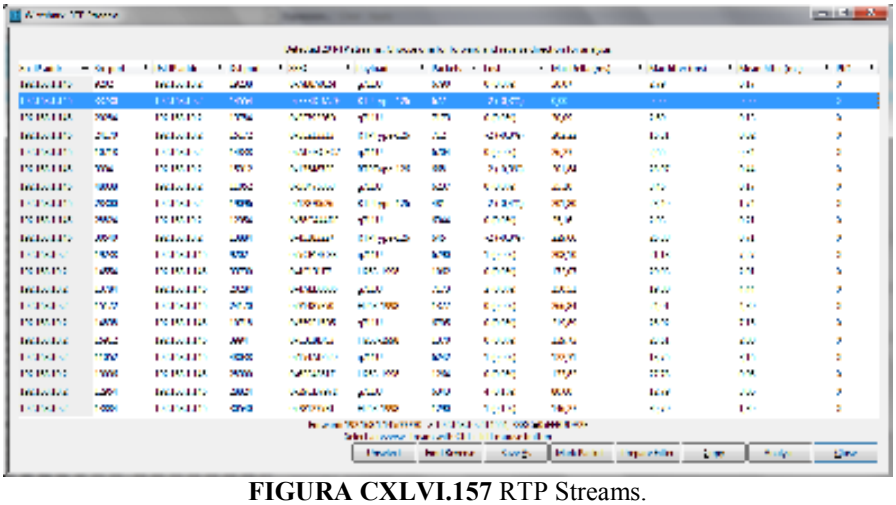

FIGURA CXLVI.157 RTP Streams.

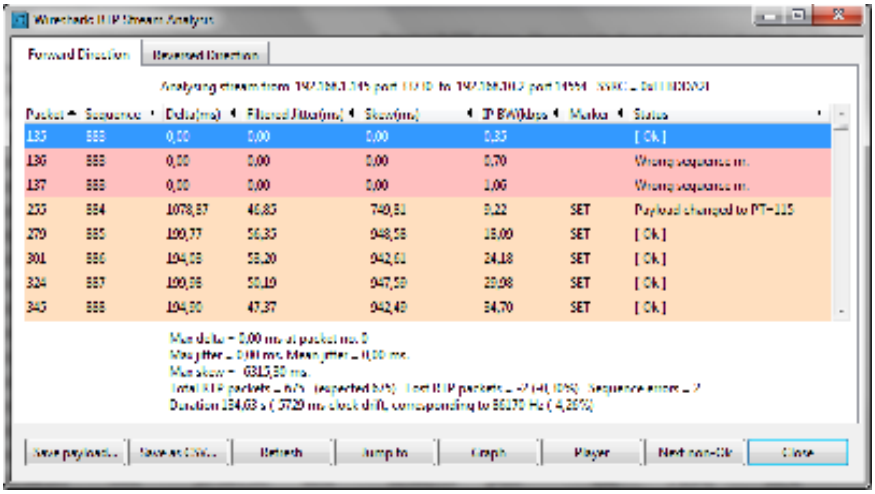

FIGURA CXLVII.158 Análisis del RTP Streams

Subescenario N°4 Videollamada – Servidor Web

FIGURA CXLVIIIV.159 Video llamadas VoIP realizadas

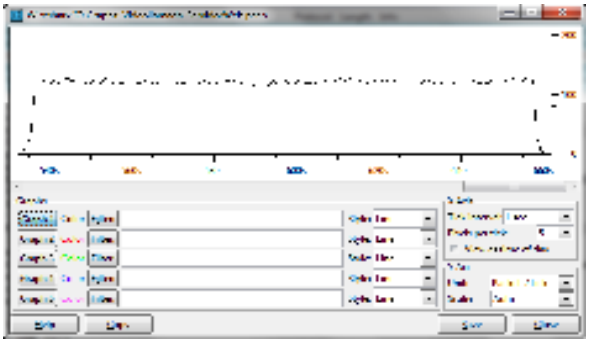

FIGURA CXLIX.160 Ancho de Banda del video llamada.

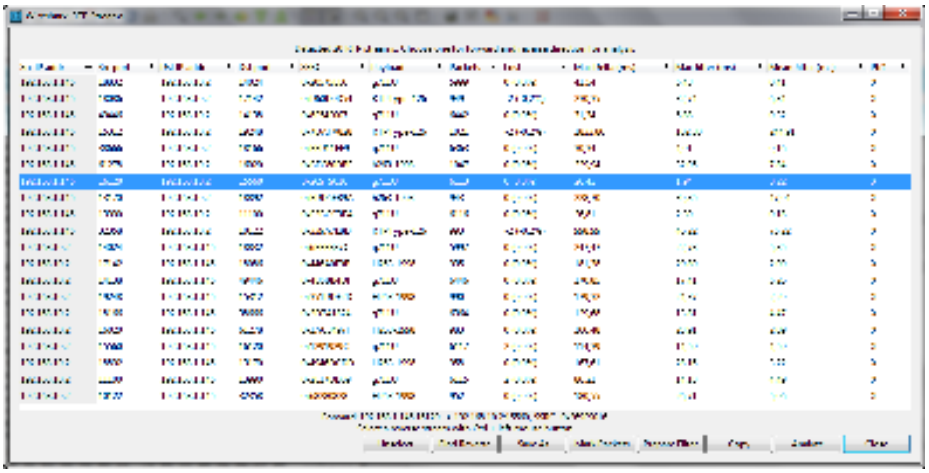

FIGURA CL.161 RTP Streams.

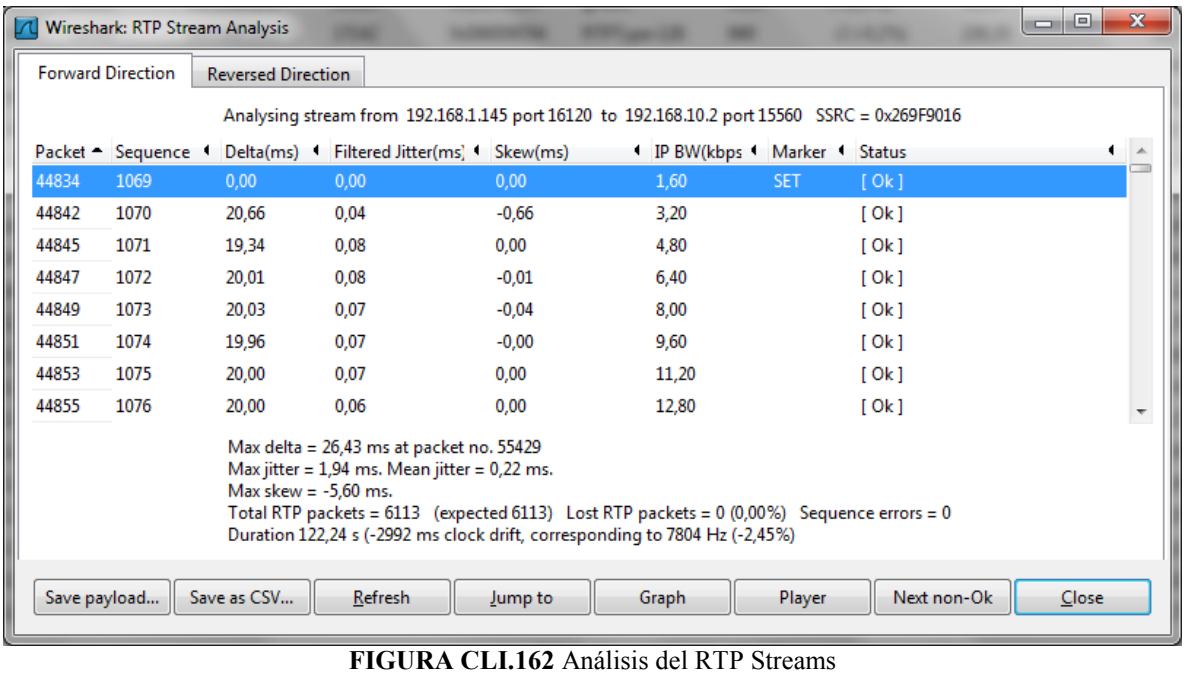

FIGURA CLI.162 Análisis del RTP Streams

Subescenario N°5 Videollamada – Servidor FTP

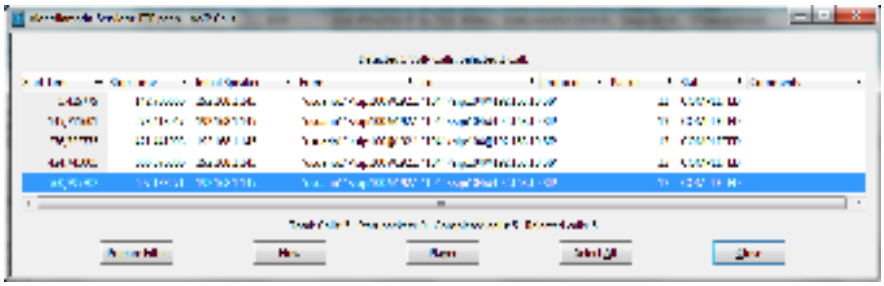

FIGURA CLII.163 Video llamadas VoIP realizadas

FIGURA CLIII.164 Ancho de Banda del video llamada.

FIGURA CLIV.165 RTP Streams

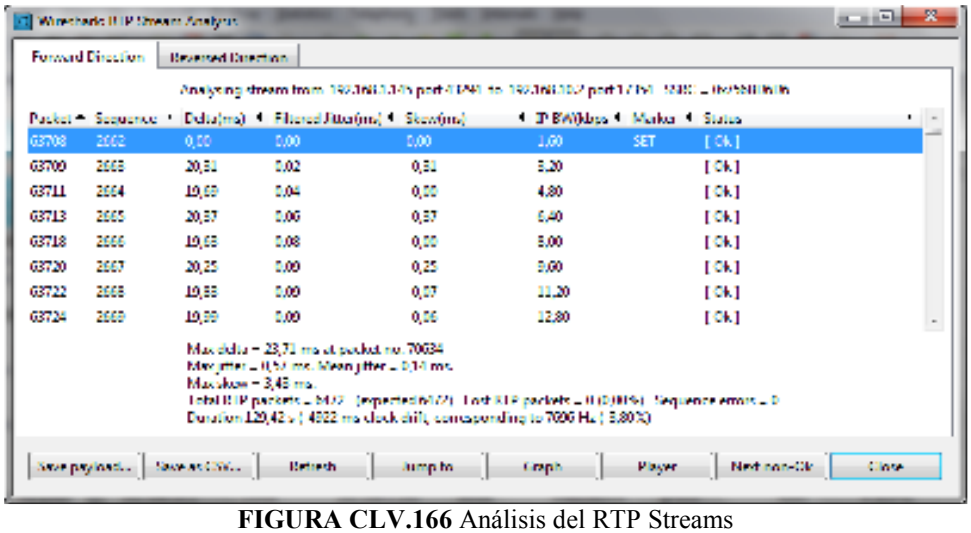

FIGURA CLV.166 Análisis del RTP Streams

Subescenario N°6 Videollamada – Servidor FTP – Servidor Web

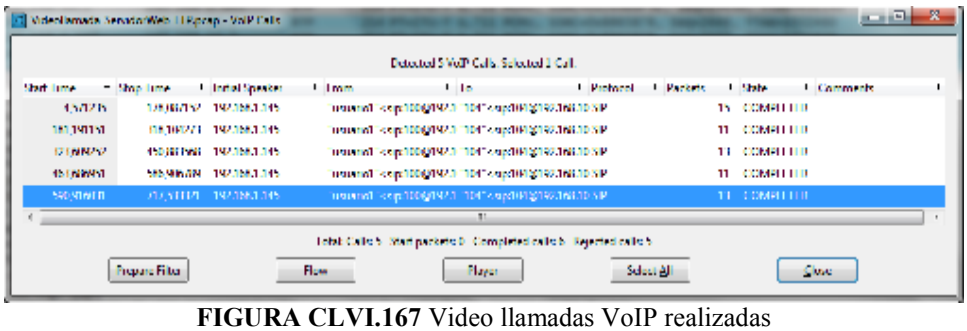

FIGURA CLVI.167 Video llamadas VoIP realizadas

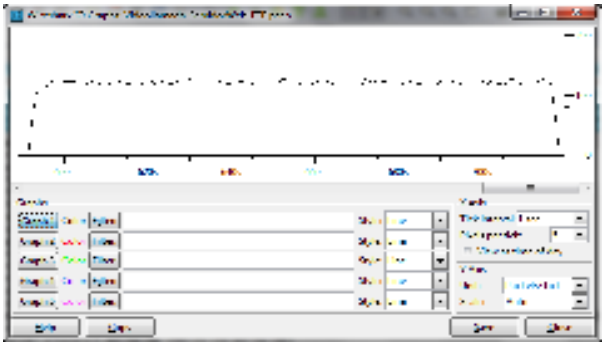

FIGURA CLVII.168 Ancho de Banda del video llamada.

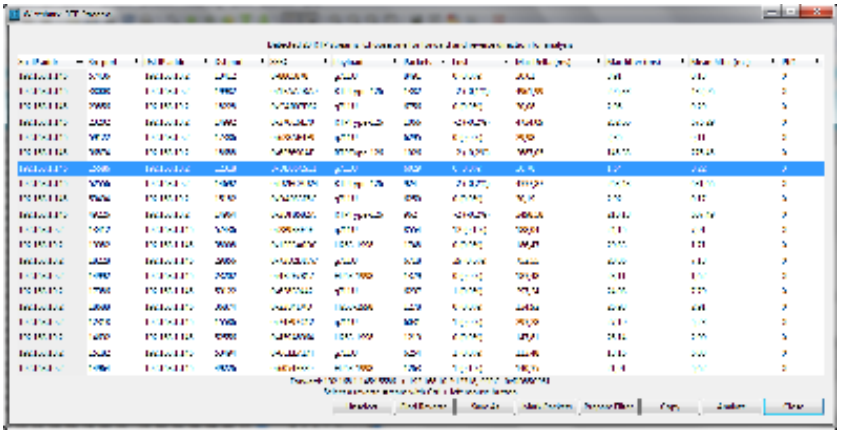

FIGURA CLVIII.169 RTP Streams

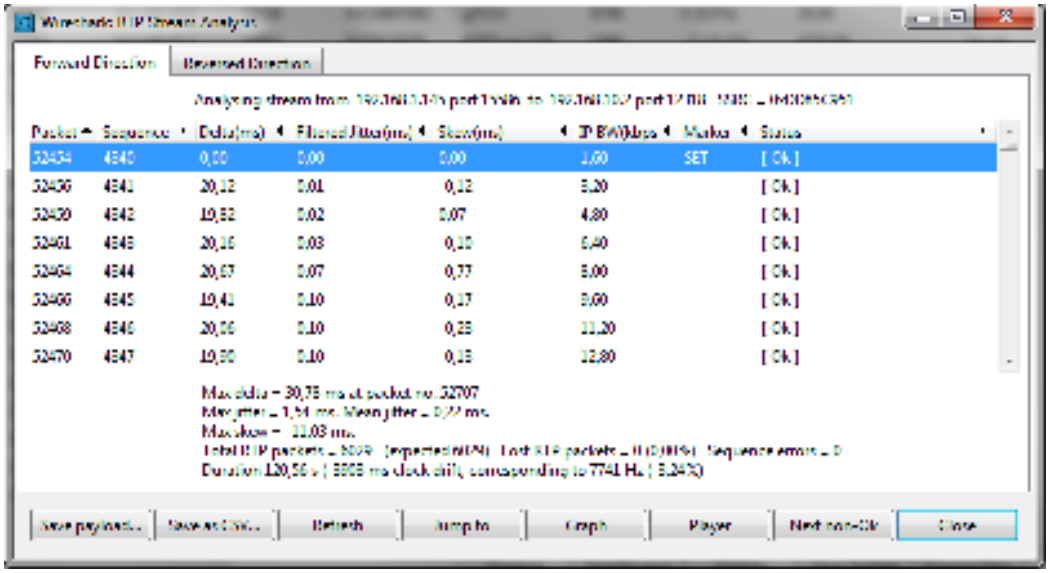

FIGURA CLIX.170 Análisis del RTP Streams

Subescenario N°7 Videollamada – Servidor FTP – Servidor Web – Servidor de Correo Electrónico

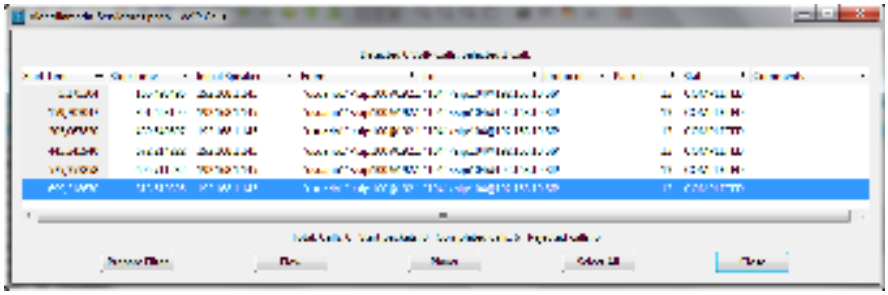

FIGURA CLX.171 Video llamadas VoIP realizadas

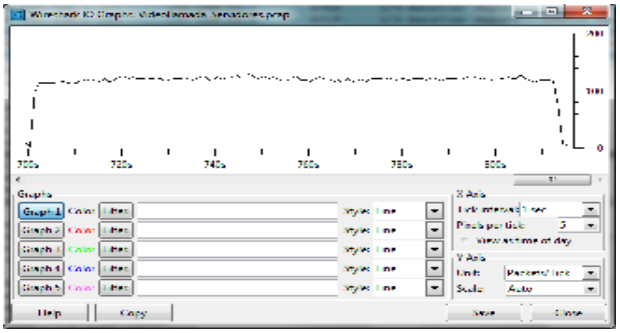

FIGURA CLXI.172 Ancho de Banda del video llamada.

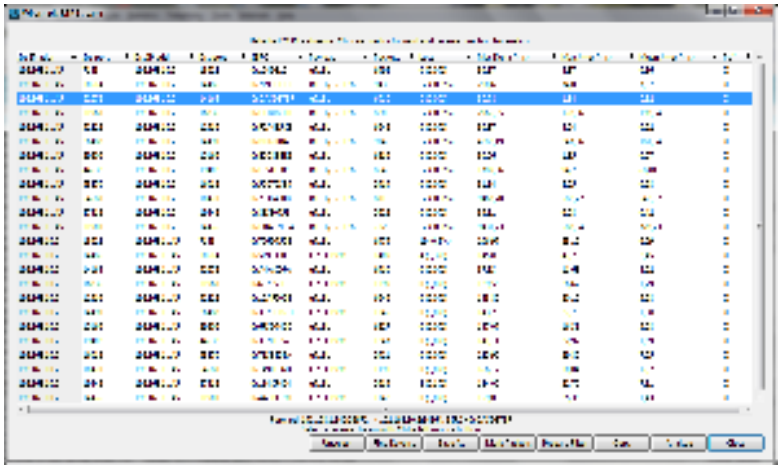

FIGURA CLXII.173 RTP Streams

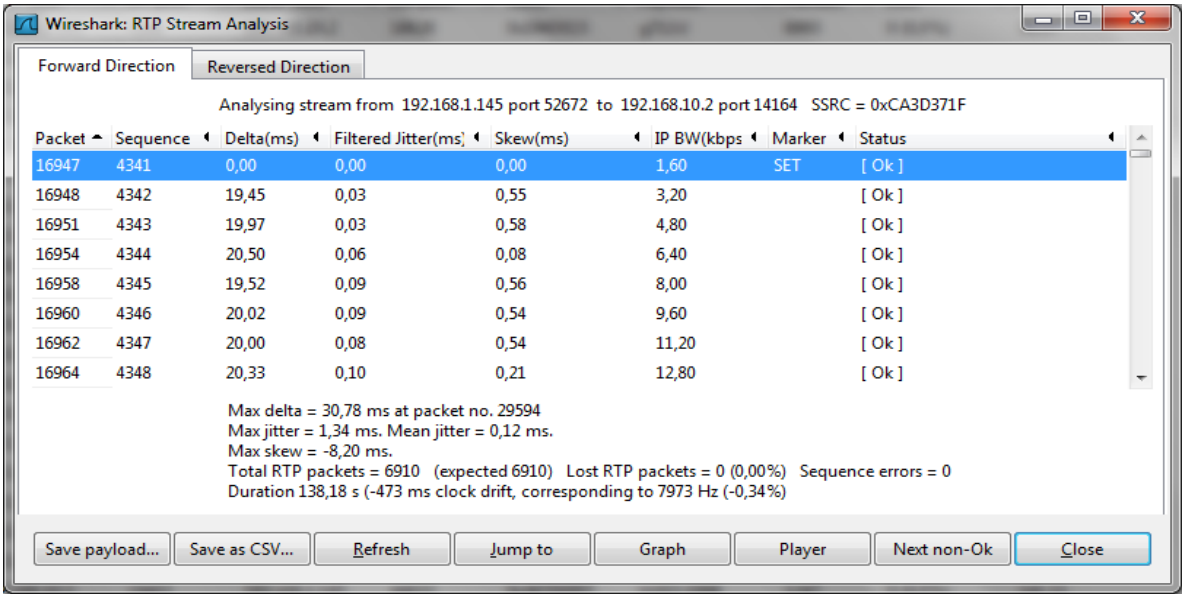

FIGURA CLXIII.174 Análisis del RTP Streams

Para establecer una clasificación subjetiva para la VoIP de los indicadores se estableció un rango de calidad en el mismo que se ubican los resultados obtenidos por el analizador de protocolos Wireshark de acuerdo a la calidad de transmisión de la videollamada.

TABLA IV.XX. Clasificación de QoS Subjetiva para VoIP

CLASIFICACIÓN DE QoS Subjetiva para VoIP				
Parámetro	**Excelente**	**Bueno**	**Regular**	**Pobre**
Jitter[ms]	$t < 10$	$10 \leq t < 200$	$200 \leq t < 300$	$t \geq 300$
Latencia[ms]	$t \leq 30$	$30 < t < 2000$	$2000 \leq t < 4000$	$t \geq 4000$
% Pérdida Paquetes	$p = 0$	$0 < p \leq 3$	$3 < p \leq 15$	$p > 15$

Para cuantificar a cada uno de los parámetros se utilizó la sumatoria de los valores de los índices obtenidos en los 7 subescenarios correspondientes a cada parámetro o indicador.

Para la cuantificación de cada índice se basó en una escala de cuatro niveles de acuerdo a la calidad de transmisión de la videollamada en cada ámbito planteado.

TABLA IV.5. Equivalencia de los Denominadores en función al rendimiento de las Videollamadas

Denominadores	Equivalencia
Excelente	4
Bueno	3
Regular	2
Pobre	1

Parámetro N° 1 Jitter [ms]

TABLA IV.6 Jitter de los Subescenarios Sin QoS – Con QoS

	Sin QoS	**Con QoS**
Videollamada sin Señal de Video	2,89	0
Videollamada con Señal de Video	389,02	0,51
Videollamada – Servidor de Correo Electrónico	105,27	0
Videollamada – Servidor Web	219,64	1,94
Videollamada – Servidor FTP	244,86	0,57
Videollamada – Servidor FTP – Servidor Web	214,59	1,54

TABLA IV.XXII. Jitter de los Subescenarios Sin QoS – Con QoS (Continuación)

Videollamada – Servidor FTP – Servidor	**125,57**	**1,34**

Web – Servidor de Correo Electrónico		

TABLA IV.XXIII. Denominadores y Equivalencias en función del Jitter en los Subescenarios Sin QoS–Con QoS

	Sin QoS		**Con QoS**	
Videollamada sin Señal de Video	Excelente	4	Excelente	4
Videollamada con Señal de Video	Pobre	1	Excelente	4
Videollamada – Servidor de Correo Electrónico	Bueno	3	Excelente	4
Videollamada – Servidor Web	Regular	2	Excelente	4
Videollamada – Servidor FTP	Regular	2	Excelente	4
Videollamada – Servidor FTP – Servidor Web	Regular	2	Excelente	4
Videollamada – Servidor FTP – Servidor Web – Servidor de Correo Electrónico	Bueno	3	Excelente	4
		17		28

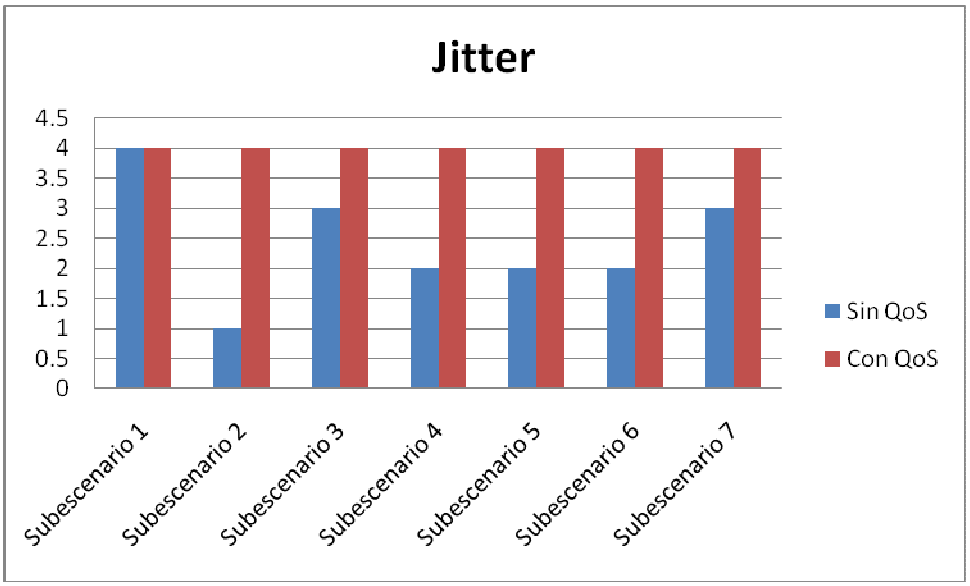

FIGURA CLXIV.175 Rendimiento de los Subescenarios por la acción del Jitter.

Interpretación

En la figura antes expuesta es fácil observar que el nivel de rendimiento en cada uno de los subescenarios es mayor en el ámbito en que se implementó Calidad de Servicio. Esto quiere decir que la calidad de servicio disminuye considerablemente la acción del jitter permitiendo de esta manera aumentar la aceptabilidad y por ende la calidad de la videollamada.

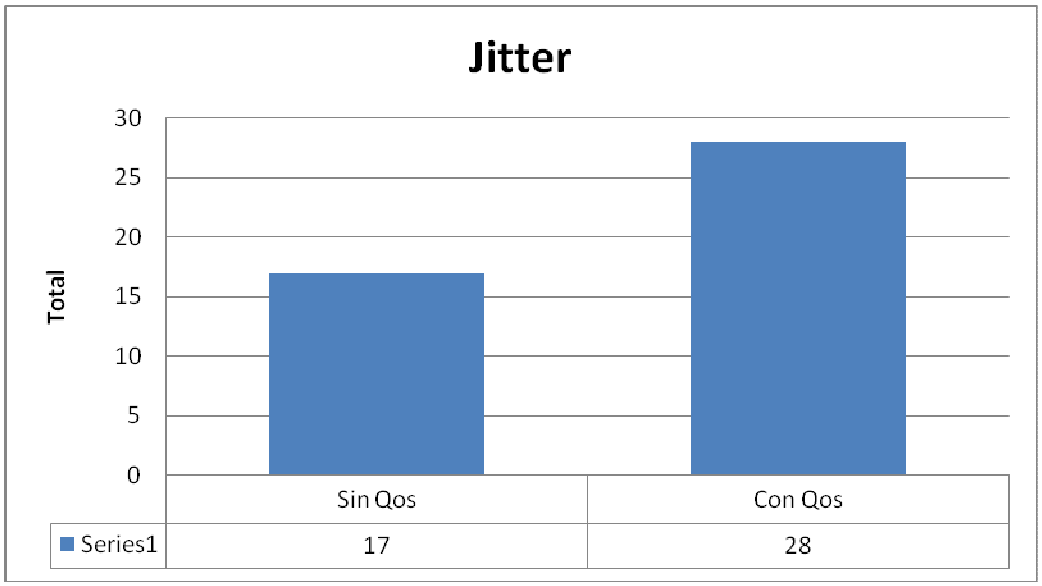

FIGURA CLXV.176 Rendimiento Cuantificado de los Subescenarios por la acción del Jitter.

Interpretación

Después de numerosas pruebas de videollamadas y una cuidadosa asignación de valores según los denominadores establecidos podemos claramente establecer que a pesar de la variación en el tiempo en la llegada de los paquetes (Jitter) producido en las diferentes videollamadas ejecutadas existe un mayor rendimiento en los subescenarios en los que ha sido implementado Calidad de Servicio que en los subescenarios en los que no se ha establecido Calidad de Servicio, cabe recalcar que los datos fueron obtenidos de una videollamada especifica escogida de manera aleatoria entre las heterogéneas videollamadas que fueron realizadas ya que el conjunto de pruebas fueron realizadas en subescenarios de diferente hostilidad a fin de apreciar de mejor manera la gestión de la Calidad de Servicio.

Parámetro N° 2 Latencia

TABLA IV.XXIV. Latencia en los Subescenarios Sin QoS – Con QoS

	Sin QoS [ms]	**Con QoS[ms]**
Videollamada sin Señal de Video	0	0
Videollamada con Señal de Video	389,02	23,21
Videollamada – Servidor de Correo Electrónico	1689,51	0
Videollamada – Servidor Web	3630,18	26,43
Videollamada – Servidor FTP	4098,47	23,71
Videollamada – Servidor FTP – Servidor Web	230,71	30,78
Videollamada – Servidor FTP – Servidor Web – Servidor de Correo Electrónico	2279,23	30,78

TABLA IV.XXV. Denominadores y Equivalencias en función de la Latencia en los Subescenarios Sin QoS– Con QoS

	Sin QoS		**Con QoS**	
Videollamada sin Señal de Video	Excelente	4	Excelente	4
Videollamada con Señal de Video	Bueno	3	Bueno	3
Videollamada – Servidor de Correo Electrónico	Bueno	3	Excelente	4
Videollamada – Servidor Web	Regular	2	Excelente	4
Videollamada – Servidor FTP	Pobre	1	Excelente	4
Videollamada – Servidor FTP – Servidor Web	Bueno	3	Bueno	3
Videollamada – Servidor FTP – Servidor Web – Servidor de Correo Electrónico	Regular	2	Bueno	3
		18		25

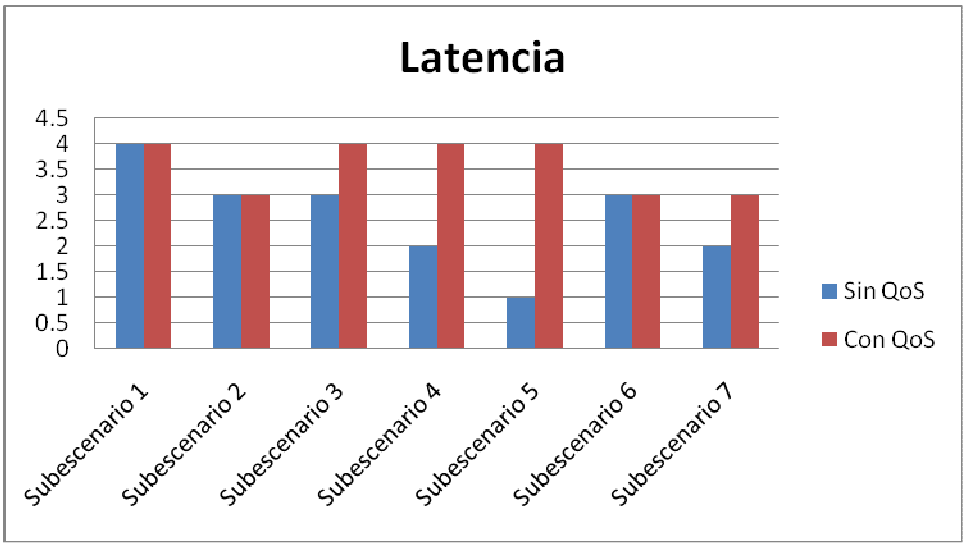

FIGURA CLXVI.177 Rendimiento de los Subescenarios por la acción de la Latencia.

Interpretación

Es posible analizar fácilmente a través de la observación de la figura anterior que el nivel de rendimiento de las videollamadas en cada uno de los subescenarios en los que fueron realizados las pruebas es mayor cuando al ámbito se le implemento Calidad de Servicio. Esto quiere decir que la calidad de servicio disminuye ampliamente el tiempo que tarda un paquete en llegar desde la fuente al destino conocido este fenómeno como Latencia permitiendo aumentar la calidad de la videollamada.

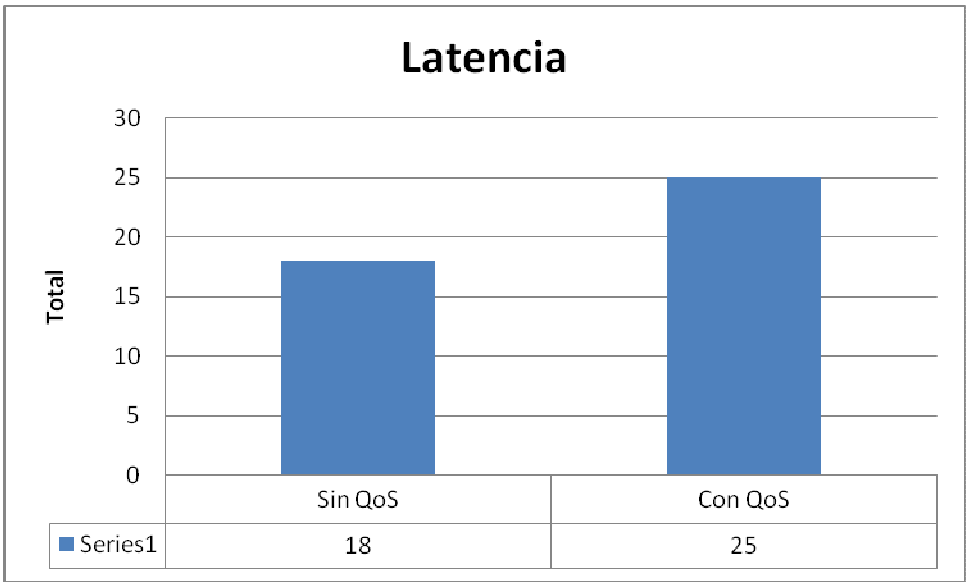

FIGURA CLXVII.178 Rendimiento Cuantificado de los Subescenarios por la acción de la Latencia.

Interpretación

Después de numerosas pruebas de videollamadas y una cuidadosa asignación de valores según los denominadores establecidos podemos claramente establecer que a pesar del tiempo que tarda un paquete en llegar desde la fuente al destino (latencia) producido en las diferentes videollamadas ejecutadas existe un mayor rendimiento en los subescenarios en los que ha sido implementado Calidad de Servicio que en los subescenarios en los que no se ha establecido Calidad de Servicio, cabe recalcar que los datos fueron obtenidos de una videollamada especifica escogida de manera aleatoria entre las heterogéneas videollamadas que fueron realizadas ya que el conjunto de pruebas fueron realizadas en subescenarios de diferente hostilidad a fin de apreciar de mejor manera la gestión de la Calidad de Servicio.

Parámetro N°3 % Pérdida de Paquetes

TABLA IV.XXVI. Pérdida de Paquetes en los Subescenarios Sin QoS – Con QoS

	Sin QoS	**Con QoS**
Videollamada sin Señal de Video	-15,38%	-15,38%
Videollamada con Señal de Video	-0,28%	0%
Videollamada – Servidor de Correo Electrónico	-0,20%	-0,30%
Videollamada – Servidor Web	-0,15%	0%
Videollamada – Servidor FTP	-0,20%	0%
Videollamada – Servidor FTP – Servidor Web	2,38%	0%
Videollamada – Servidor FTP – Servidor Web – Servidor de Correo Electrónico	18,01%	0%

Observación: Los resultados obtenidos en las tablas IV.XXII, IV.XXIV, IV.XXVI están respaldados por las Figuras IV.122, IV.126, IV.130, IV.134, IV.138, IV.142, IV.146, IV.150, IV.154, IV.158, IV.162, IV.166, IV.170, IV.174

TABLA IV.XXVII. Denominadores y Equivalencias en función del % Pérdida de Paquetes en los Subescenarios Sin QoS–Con QoS

	Sin QoS		**Con QoS**	
Videollamada sin Señal de Video	N/A	-	N/A	-
Videollamada con Señal de Video	N/A	-	Excelente	-
Videollamada – Servidor de Correo Electrónico	N/A	-	N/A	-
Videollamada – Servidor Web	N/A	-	Excelente	4
Videollamada – Servidor FTP	N/A	-	Excelente	4
Videollamada – Servidor FTP – Servidor Web	Bueno	3	Excelente	4
Videollamada – Servidor FTP – Servidor Web – Servidor de Correo Electrónico	Pobre	1	Excelente	4
		4		16

Observación: Los resultados obtenidos en las tablas IV.XXIII, IV.XXV, IV.XXVII están realizadas en base a la Tabla de Equivalencia IV.XXI.

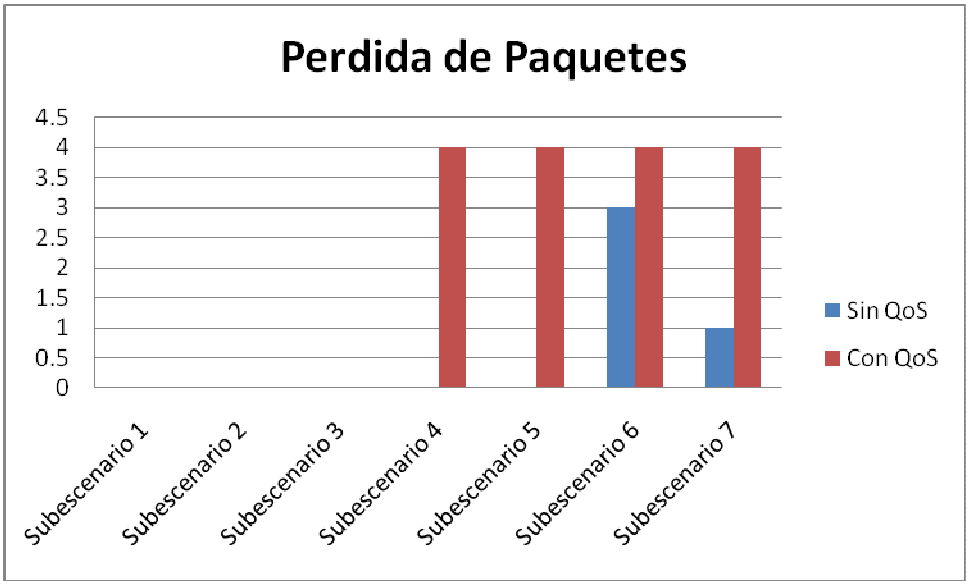

FIGURA CLXVIII.179 Rendimiento de los Subescenarios por la acción del % de la pérdida de Paquetes

Interpretación

A través de la figura anterior se observa que el rendimiento de las videollamadas realizadas en el ámbito en el que fue implementado calidad de servicio es superior al rendimiento de las llamadas realizadas en el ámbito en el que no fue implementado calidad de servicio. Esto se debe a que la acción de la Calidad de servicio disminuyo la pérdida de paquetes efectuada durante la realización de la videollamada.

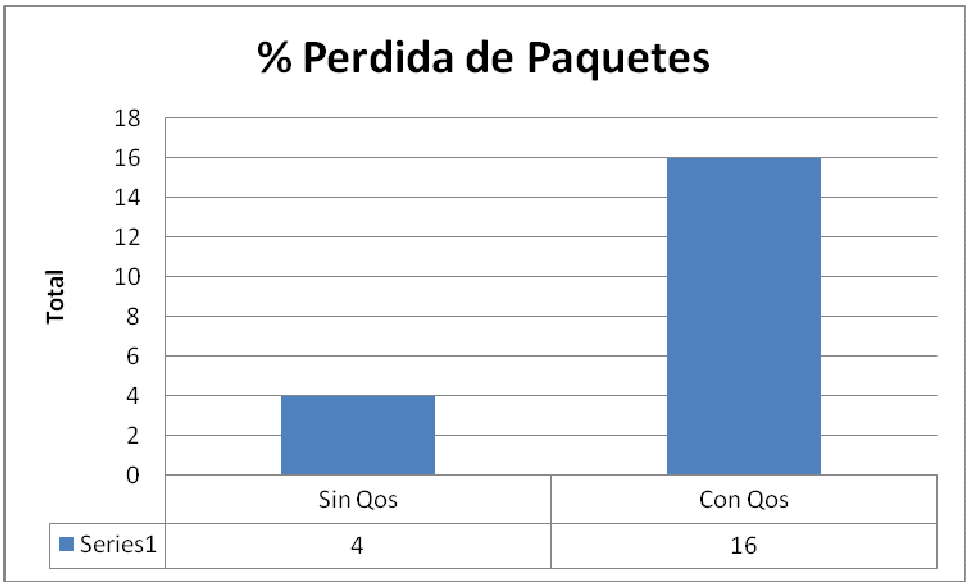

FIGURA CLXIX.180 Rendimiento Cuantificado de los Subescenarios por la acción del % de la pérdida de Paquetes

Interpretación

Después de numerosas pruebas de videollamadas y una cuidadosa asignación de valores según los denominadores establecidos y tomando en cuenta que las comunicaciones en tiempo real están basadas en el protocolo UDP podemos claramente establecer que a pesar de las comunicaciones en tiempo real están basadas en el protocolo UDP y este protocolo no está orientado a conexión y si se produce una pérdida de paquetes no se reenvían sin embargo la voz es bastante predictiva y si se pierden paquetes aislados se puede recomponer la voz de una manera bastante óptima existe un mayor rendimiento en los subescenarios en los que ha sido implementado Calidad de Servicio que en los subescenarios en los que no se ha establecido Calidad de Servicio, cabe recalcar que los datos fueron obtenidos de una videollamada especifica escogida de manera aleatoria entre las heterogéneas videollamadas que fueron realizadas ya que el conjunto de pruebas fueron realizadas en subescenarios de diferente hostilidad a fin de apreciar de mejor manera la gestión de la Calidad de Servicio

TABLA IV.XXVIII. Valoración Total del Rendimiento en función de los parámetros Sin QoS–Con QoS

PARÁMETROS	SUBESCENARIOS	SIN QoS	CON QoS
		Equivalencia según los Denominadores	
INDICADOR N° 1 **JITTER**	**Videollamada sin Señal de Video**	4	4
	Videollamada con Señal de Video	1	4
	Videollamada – Servidor de Correo Electrónico	3	4
	Videollamada – Servidor Web	2	4
	Videollamada – Servidor FTP	2	4
	Videollamada – Servidor FTP – Servidor Web	2	4
	Videollamada – Servidor FTP – Servidor Web – Servidor de Correo Electrónico	3	4
	Videollamada sin Señal de Video	4	4
	Videollamada con Señal de Video	3	3
	Videollamada – Servidor de Correo Electrónico	3	4

Tabla IV.XXVIII. Valoración Total del Rendimiento en función de los parámetros Sin QoS-Con QoS (Continuación)

	Videollamada – Servidor de Correo Electrónico	**-**	**-**
INDICADOR N° 2 **LATENCIA**	**Videollamada – Servidor FTP**	1	4
	Videollamada – Servidor FTP – Servidor Web	3	3
	Videollamada – Servidor FTP – Servidor Web – Servidor de Correo Electrónico	2	3
INDICADOR N° 3 PÉRDIDA DE PAQUETES	**Videollamada sin Señal de Video**	-	-
	Videollamada con Señal de Video	-	-
	Videollamada – Servidor de Correo Electrónico	-	-
	Videollamada – Servidor Web	-	4
	Videollamada – Servidor FTP	-	4
	Videollamada – Servidor FTP – Servidor Web	3	4
	Videollamada – Servidor FTP – Servidor Web – Servidor de Correo Electrónico	1	4
TOTAL		39	69

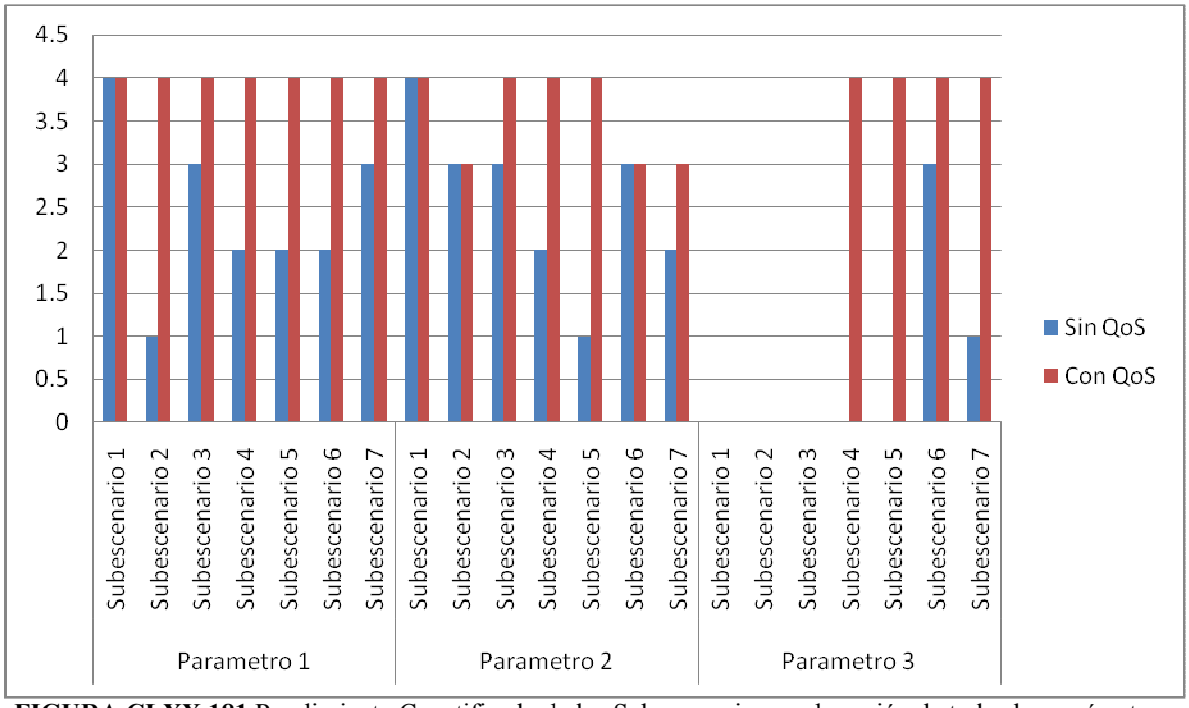

FIGURA CLXX.181 Rendimiento Cuantificado de los Subescenarios por la acción de todos los parámetros

Interpretación

En la presente investigación el rendimiento establecido en las videollamadas fue cuantificado en función de parámetros como el jitter, la latencia y la pérdida de paquetes. Esta claramente expresada en la Figura que en los subescenarios en los que fue implementado Calidad de Servicio gozan de un mayor rendimiento en la transmisión de las aplicaciones en tiempo real que las realizadas en los subescenarios en los que no fue implementado Calidad de Servicio.

Haciendo un resumen a través de la sumatoria de los valores obtenidos en las pruebas en cada Subescenario de los indicadores Jitter, Latencia y pérdida de paquetes obtuvimos 39 puntos (17 + 18 + 4) para el ámbito sin QoS mientras que para el ámbito con QoS obtuvimos un total de 69 puntos (28 + 25 + 16) concluyendo que para el Escenarios con Calidad de servicio el rendimiento mejoro en 30 puntos.

4.2.3. Comprobación de la Hipótesis de la investigación realizada

Estadístico x^2 Chi Cuadrado

La prueba x^2 es considerada como una prueba no paramétrica que mide la discrepancia entre una distribución observada y otra teórica. También es utilizada para probar probar la independencia de dos variables entre sí, mediante la presentación de los datos en tablas de contingencia.

Se dará a la variable independiente ***X*** los siguientes valores:

X = Administración Trabajo Colaborativo

X_1 = Administración sin QoS

X_2 = Administración con QoS

Los mismos que se aplicarán a la muestra en estudio con el fin de determinar su impacto en la variable dependiente ***Y*** **(**Rendimiento en la transmisión de Videollamadas).

Los resultados que se presentan a continuación constituye la media obtenida de cada uno de los indicadores basados en la equivalencia asignada a los denominadores (Tabla IV.XXI).

TABLA IV.XXIX. Medida de los Indicadores en función de su equivalencia

Ámbitos\Indicadores	Sin QoS	Con QoS
Jitter	2.4	4
Latencia	1.1	3.5
Pérdida de Paquetes	0.6	2.3

Establecemos un nuevo rango que revele cuando cada uno de los indicadores muestra o no una mejora, de acuerdo a la equivalencia de los denominadores (Tabla IV.42) rango que utilizaremos para realizar la **"Matriz de Contingencia"**

TABLA IV.XXX Rango de Establecimiento de Mejora

	Mejora	**No Mejora**
Rango	4 ≥ Equivalencia > 2	2 ≥ Equivalencia ≥ 0

La tabla de contingencia creada para el cálculo de la ji cuadrada, contiene las dos variables en estudio: Administración con QoS y Administración sin QoS, cada una en función a la equivalencia de los tres indicadores que nos permitirán evaluar el rendimiento de las videollamadas.

TABLA IV.XXXI. Valoración Total

		ADMINISTRACIÓN SIN QOS	ADMINISTRACIÓN CON QOS	TOTAL
Hi **LA ADMINISTRACIÓN DE QOS EN LAS REDES INALÁMBRICAS, GARANTIZARÁ QUE LAS VIDEOLLAMADAS LOGREN TRANSMITIRSE CON MAYOR RENDIMIENTO**	Jitter	2.4	4	6.4
	Latencia	0	3.5	3.5
	Pérdida de Paquetes	0	2.3	2.3
Ho **LA ADMINISTRACIÓN DE QOS EN LAS REDES INALÁMBRICAS, GARANTIZARÁ QUE LAS VIDEOLLAMADAS LOGREN TRANSMITIRSE CON MENOR RENDIMIENTO**	Jitter	0	0	0
	Latencia	1.1	0	1.1
	Pérdida de Paquetes	0.6	0	0.6
	Total	4.1	9.8	13.9

Para la prueba de la hipótesis planteada se utilizó la prueba chi cuadrado o χ^2 , que es una prueba que como indicamos anteriormente nos permitirá medir la relación entre la variable dependiente e independiente. Además se consideró la hipótesis nula Ho y la hipótesis de investigación Hi.

Planteamiento de la Hipótesis

Hi: LA ADMINISTRACIÓN DE QOS EN LAS REDES INALÁMBRICAS, GARANTIZARÁ QUE LAS VIDEOLLAMADAS LOGREN TRANSMITIRSE CON MAYOR RENDIMIENTO

Ho: "LA ADMINISTRACIÓN DE QOS EN LAS REDES INALÁMBRICAS, GARANTIZARÁ QUE LAS VIDEOLLAMADAS LOGREN TRANSMITIRSE CON MAYOR RENDIMIENTO"

TABLA IV.XXXII Tabla de Contingencia con las Frecuencias observadas

	Administración Sin QoS	**Administración Con QoS**	**Total**
Hi: La administración de QoS en las redes inalámbricas, garantizará que las videollamadas logren transmitirse con mayor rendimiento	2.4	9.8	12.2
Ho: La administración de QoS en las redes inalámbricas, garantizará que las videollamadas logren transmitirse con menor rendimiento	1.7	0	1.7
	4.1	**9.8**	**13.9**

La Tabla IV.32 contiene las frecuencias esperadas, la cual constituye los valores que esperaríamos encontrar si las variables no estuvieran relacionadas. La ji cuadrada partirá del supuesto de "no relación entre las variables" y se evaluará si es cierto o no, analizando si sus frecuencias observadas son diferentes de lo que pudiera esperarse en caso de ausencia de correlación.

La frecuencia esperada de cada celda, se calcula mediante la siguiente fórmula aplicada a la tabla de frecuencias observadas.

$$fe = \frac{(total\_de\_fila)(total\_de\_columna)}{N}$$

Donde ***N*** es el número total de frecuencias observadas

Frecuencias **Esperadas**

$$fe = \frac{(12.2)(4.1)}{13.9} = 3.6 \qquad fe = \frac{(12.2)(9.8)}{13.9} = 8.60$$

$$fe = \frac{(1.7)(4.1)}{13.9} = 0.50 \qquad fe = \frac{(1.7)(9.8)}{13.9} = 1.2$$

TABLA IV.XXXIII. Tabla de frecuencias esperadas

	Administración Sin QoS	**Administración Con QoS**	**Total**
Hi: La administración de QoS en las redes inalámbricas, garantizará que las videollamadas logren transmitirse con mayor rendimiento	3.6	8.6	12.2
Ho: La administración de QoS en las redes inalámbricas, garantizará que las videollamadas logren transmitirse con menor rendimiento	0.50	1.2	1.7
	4.1	**9.8**	**13.9**

Una vez obtenidas las frecuencias esperadas, se aplica la siguiente fórmula de ji cuadrada:

$$\chi^2 = \sum \frac{(O-E)^2}{E}$$

Dónde:

O es la frecuencia observada en cada celda

E es la frecuencia esperada en cada celda

En la Tabla IV.34 se calcula el valor de $\chi 2$

TABLA IV.XXXIV. Cálculo de χ^2

CELDA	O	E	0-E	$(O-E)^2$	$(O-E)^2/E$
Mejora/ Administración con QoS	2.4	3.6	-1.2	1.44	0.4
Mejora/Administración sin QoS	9.8	8.6	1.2	1.44	0.17
No Mejora/ Administración con QoS	1.7	0.5	1.2	1.44	2.88
No Mejora/Administración sin QoS	0	1.2	-1.2	1.44	1.2
				X^2	4.65

INTERPRETACIÓN: Para saber si el valor de χ^2 es o no significativo, se debe determinar los grados de libertad mediante la siguiente fórmula:

$$Gl = (r-1)(c-1)$$

Dónde:

r es el número de filas de la tabla de contingencia

c es el número de columnas de la tabla de contingencia

Por lo tanto:

$$Gl = (2-1)(2-1) = 1$$

De la tabla de distribución del $\chi 2$ que se encuentra en el Anexo y eligiendo como nivel de confianza $\alpha = 0,05$ se obtiene que $\chi 2 = 3,841$. El valor de $\chi 2$ calculado en esta investigación es de 4,65 que es mayor al de la tabla de distribución, por lo que $\chi 2$ resulta significativa y se acepta la hipótesis de investigación.

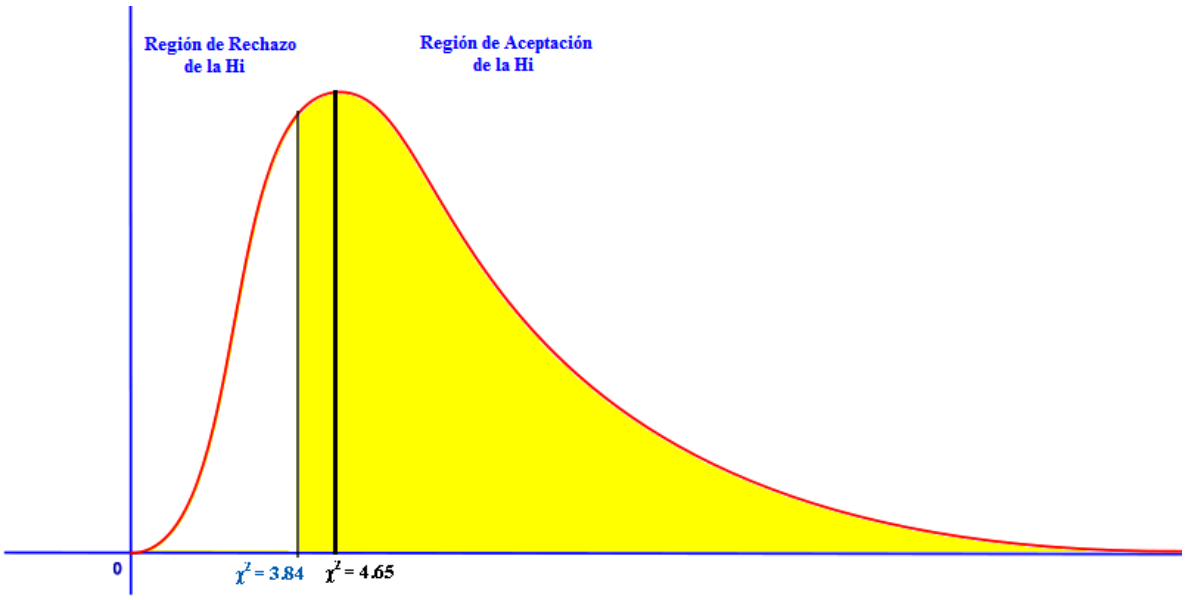

FIGURA CLXXI.182 Comprobación de la hipótesis según la gráfica Chi Cuadrado

4.65 < 3.84, **esto es Falso por lo tanto:** Se RECHAZA LA HIPÓTESIS NULA Ho Y SE ACEPTA LA HIPÓTESIS DE INVESTIGACIÓN Hi

CONCLUSIONES

1. A través de las pruebas se analizó el jitter producido para cada Subescenario en los dos ámbitos definidos y se ha llegado a la conclusión de que precisamente existe una disminución del Jitter en el ámbito provisto de QoS siendo el resultado para este fue de 17 puntos mientras que para el ámbito sin QoS se obtuvo 28 puntos recalcando que estos son los valores obtenidos después de asignadas las equivalencias a los denominadores de rendimiento.

2. En cuanto a la latencia se observa que existe una tendencia hacia la disminución en el ámbito provisto de Calidad de Servicio alcanzando 18 puntos mientras que en el otro ámbito se obtuvo 25 puntos.

3. Se demuestra la mejora en la pérdida de paquetes cuando se implementa la calidad de servicio, puesto que en las pruebas con QoS se alcanzo un valor de 4 puntos bastante inferior con respecto al ámbito sin QoS en los que la pérdida de paquetes alcanzó 16 puntos.

4. La aplicación del protocolo Diffserv resulta suficiente para la provisión de garantías QoS ya que evita que la red llegue a una situación de sobreutilización de sus recursos, provocando forzosamente congestión debido a que dicho protocolo realiza la diferenciación y priorización del trafico además que optimiza el manejo y el control de uso de los recursos de la red y esto se ha comprobado a través del análisis de los parámetros que aseguran la QoS dando como resultado mejoras evidentes.

5. Las políticas de calidad de Servicio se realizan a través del módulo de QoS del router. Para la priorización de tráfico se realizo configuraciones en dicho módulo logrando así comprobar la aplicación de QoS para este tipo de redes que no es solamente limitación sino es un intento de emplear los recursos existentes racionalmente.

6. A través de la utilización del software wireshark se pudo monitorear el comportamiento del tráfico en la red y de esta manera se permitió analizar los diferentes parámetros que determinan el rendimiento tales como jitter, latencia y pérdida de paquetes.

7. El Sistema operativo Linux se logró una reducción de costos y acceso a servicios indispensables para datos y comunicaciones. Además permitió el flasheo del router que fue una alternativa útil a la hora de implementar calidad de servicio debido a la fácil configuración y administración de los recursos de la red para la aplicación de QoS.

RECOMENDACIONES

1. La incorporación de mecanismos de Calidad de Servicio a través del protocolo Diffserv promete grandes ventajas no solo para el proveedor servicios sino para el usuario final. Se recomienda a los proveedores optimizar la utilización de los recursos de la red mediante la diferenciación del tráfico y aplicaciones ya que el usuario final concebirá mejores características de rendimiento de la red y un alto grado de satisfacción.

2. Para la aplicación del protocolo Diffserv se recomienda realizar un análisis del tráfico de la red para asignar prioridades en forma adecuada y de esta manera hacer prevalecer los recursos para la transmisión del tráfico.

3. Se debe realizar una correcta valoración de los dispositivos y software necesario para la implementación de los escenarios de prueba, ya que de ellos dependerá la fiabilidad de los resultados obtenidos en los estudios.

4. Para la captura del tráfico de la red, es necesario utilizar un analizador de protocolos que cumpla con las exigencias de análisis que son indispensables para un conseguir una captura real del trafico que se está generando en la red.

5. Los desarrollos que han alcanzado los grupos de código abierto posibilitaran que en el futuro empresas pequeñas y medianas puedan acceder a soluciones de calidad, flexibles, seguras y económicas por lo mismo se recomienda, si es posible, la utilización de alternativas que se basen en el Sistema operativo Linux.

RESUMEN

El análisis del protocolo Diffserv aplicado a la provisión de QoS en el tráfico de vídeollamadas sobre redes inalámbricas en equipos Cisco y Linux.

El método científico se utilizó en esta investigación para presentar hechos en forma de teorías y fue necesario contar con un método comparativo para permitir a los investigadores establecer la comparación del rendimiento de las videollamadas con los equipos antes mencionados.

Se plantaron escenarios de pruebas con equipos Cisco y Linux. El primer escenario, no pudo cumplirse debido a que la tarjeta Wireless Lan controller no se encuentra en buenas condiciones, en consecuencia, la investigación de este escenario no fue posible llevar a cabo. Sin embargo, la confirmación de la hipótesis fue apoyada totalmente por el escenario con equipos Linux.

Se implementaron sub-escenarios para proporcionar distintos niveles de congestión del router, de esta manera lograr un mejor análisis comparativo de la calidad de las videollamadas. Se ha comprobado que el rendimiento mejoró en 30 puntos en el ámbito en que se aplico Calidad de Servicio.

Una guía metodológica se desarrolló con el fin de proporcionar una ayuda didáctica basada en la implementación del escenario antes mencionado, que presentó los siguientes contenidos: Instalación, Configuración del servidor y la configuración del protocolo de Diffserv. Por medio de la utilización adecuada de ésta guía, los usuarios pueden ser capaces de utilizar y armar una red, sirviendo de esta manera de capacitación práctica.

Se puede concluir que las videollamadas tuvieron un mayor rendimiento en el ámbito en el que aplicamos Calidad de servicio a través del protocolo Diffserv después de haber realizado la comparación del rendimiento entre los ámbitos con y sin calidad de servicio, se estableció que la meta fue alcanzada, apoyándonos en indicadores como el jitter, latencia, pérdida de paquetes.

QoS a través del protocolo Diffserv promete grandes ventajas, por lo que se recomienda a los proveedores optimizar la utilización de los recursos de red mediante la diferenciación del tráfico y aplicaciones.

SUMMARY

Diffserv Protocol Analysis applied in quality service (QoS) provision for video-calls traffic concerning Cisco wireless network and Linux equipment.

The purpose of this research was to present facts in a theoretical mode about Cisco Wireless Network an Linux equipment. The scientific method was used in this investigation for which was necessary to rely on a comparative method for allowing the researches establish comparison on the aforementioned equipment and video-call perfomance.

Several testing scenarios about Cisco and Linux equipment were posed. The former, the Cisco one, could not be completed as the Wireless Lan Controller card has a miss match functioning ; consequently, such a scenario research was not possible to conduct. However, the hypothesis confirmation was totally supported by the latter, the Linux equipment scenario.

As a result, certain sub-scenarios were implemented for providing distinct router congestion levels; this way, reaching better comparative analyses on video-call quality was possible. It was proven that its QoS performance bettered 30 points respect to its environment.

A Methodological guide was developed in order to provide didactic help based on the aforementioned scenario implementation which presented the following contents: Installation, Server Configuration and Diffserv protocol configuration. By means of adequate guide utilization, users may be able to use and build network, so that they may help all users in a more practical training.

It can be concluded that video-calls had greater performance respect to the environment on which the researchers applied quality service (QoS) through Diffserv protocol. After having developed performance comparison between environments with and without QoS; it was established that the goal was reached by relying on jitter, latency, and package loss indicators.

QoS through Diffserv Protocol incorporation foresees great advantages; for that reason, it is recommended that providers optimize network utilization and resources by means of traffic segmentation and application.

GLOSARIO

ANÁLISIS: Estudio, mediante técnicas informáticas, de los límites, características y posibles soluciones de un problema al que se aplica un tratamiento por ordenador.

JITTER: El jitter se define técnicamente como la variación en el tiempo en la llegada de los paquetes, causada por la congestión de la red, pérdida de sincronización o por las diferentes rutas seguidas por los paquetes para llegar al destino.

DHCP: (Protocolo dinámico de la configuración del anfitrión) – Protocolo que deja un dispositivo en una red local, conocida como DHCP. Asigna direcciones temporales del IP a los otros dispositivos de la red, típicamente computadoras

Explorador: Es un programa de uso que proporciona una manera de mirar y de obrar recíprocamente con toda la información sobre el World Wide Web.

FTP: (File Transfer Protocol) Protocolo estándar para enviar archivos entre las computadoras sobre una red de TCP/IP y el Internet.

Hardware: Aspecto físico de computadoras de telecomunicaciones y de otros dispositivos de la tecnología de información.

HTTP: (Hypertext Transfer Protocol) protocolo de transferencia de hipertexto) es el protocolo usado en cada transacción de la World Wide Web.

IEEE: (INSTITUTO de los ingenieros electrónicos eléctricos)- Instituto dependiente que desarrolla estándares de establecimiento de una red.

IP: (Internet Protocol) Protocolo que envía datos sobre una red.

IP ADDRESS: Dirección que identifica a una computadora o un dispositivo en una red.

IP ADDRESS ESTÁTICO: Dirección fija asignada a una computadora o a un dispositivo que está conectado a una red.

LATENCIA: La latencia conocida también como retardo se define técnicamente como el tiempo que tarda un paquete en llegar desde la fuente al destino.

MAC: (Media Access control) Dirección única que un fabricante asigna a cada dispositivo del establecimiento de una red.

Paquete: Cada uno de los bloques en que se divide la información que se envía a través de una red en el nivel de red del modelo OSI. Por debajo de este nivel el paquete adquiere el nombre de trama de red.

Pérdida de Paquetes: Si una cola alcanza su longitud máxima, se pueden producir pérdidas de paquetes. Cuando sucede, los protocolos orientados a la conexión disminuyen la velocidad de transmisión para dar servicio a los paquetes de la cola y permitir que ésta se vacié.

RED: Varias computadoras o dispositivos conectados con el fin de compartir, almacenar, y/o transmitir datos entre los usuarios.

RTP: Es un protocolo de nivel de sesión utilizado para la transmisión de información en tiempo real.

SERVIDOR: Cualquier computadora que su función en una red sea la de proporcionar el acceso de los usuarios a los archivos, a la impresión, a comunicaciones y a otros servicios.

SUBNET MASK: Es un código de la dirección que determina el tamaño de la red.

ToS: (Type of Service): campo de ocho bits de la cabecera de IP. Lo utilizan IP Precedence, Differentiated Services Code Pont y ToS.

UDP: (User Datagram Protocol) Protocolo abierto, no orientado a la conexión y por lo que no establece un diálogo previo entre las dos partes, ni tampoco mecanismos de detección de errores. Generalmente se emplea un lugar del TCP, cuando no se necesitan fuertes controles en la comunicación de los datos. Brinda mayor velocidad y menos complejidad.

ANEXOS

ANEXO 1

CONFIGURACION DEL ROUTER

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
!
dot11 syslog
ip source-route
!
!
ip cef
!
ip dhcp pool redswitch
   network 192.168.1.0 255.255.255.0
   default-router 192.168.1.1
no ipv6 cef

multilink bundle-name authenticated
voice-card 0
username admin privilege 15 secret 5 $1$2ADU$R0Dcxzpkh/yYixWoQYJCa.
archive
log config
  hidekeys
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.2
 encapsulation dot1Q 2
 ip address 192.168.2.1 255.255.255.0
!
interface FastEthernet0/1.3
 encapsulation dot1Q 3
```

```
 ip address 192.168.3.1 255.255.255.0
!
interface FastEthernet0/1.4
 encapsulation dot1Q 4
 ip address 192.168.4.1 255.255.255.0
!
interface FastEthernet0/1.5
 encapsulation dot1Q 5
 ip address 192.168.5.1 255.255.255.0
!
interface Integrated-Service-Engine1/0
 ip address 192.168.100.1 255.255.255.0
 no keepalive
!
ip forward-protocol nd
no ip http server
no ip http secure-server
control-plane
voice-port 0/1/0
voice-port 0/1/1
mgcp fax t38 ecm
gatekeeper
 shutdown
line con 0
logging synchronous
line aux 0
line 66
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
line vty 0 4
 login local
!
scheduler allocate 20000 1000
end
```

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
```

```
no aaa new-model
!
dot11 syslog
ip source-route
!
!
ip cef
!
ip dhcp pool redswitch
   network 192.168.1.0 255.255.255.0
   default-router 192.168.1.1
!
!
no ipv6 cef
!
multilink bundle-name authenticated
voice-card 0
username admin privilege 15 secret 5 $1$2ADU$R0Dcxzpkh/yYixWoQYJCa.
archive
 log config
  hidekeys
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.2
 encapsulation dot1Q 2
 ip address 192.168.2.1 255.255.255.0
!
interface FastEthernet0/1.3
 encapsulation dot1Q 3
 ip address 192.168.3.1 255.255.255.0
!
interface FastEthernet0/1.4
 encapsulation dot1Q 4
 ip address 192.168.4.1 255.255.255.0
!
interface FastEthernet0/1.5
 encapsulation dot1Q 5
 ip address 192.168.5.1 255.255.255.0
!
interface Integrated-Service-Engine1/0
 ip address 192.168.100.1 255.255.255.0
 no keepalive
!
ip forward-protocol nd
no ip http server
no ip http secure-server
```

```
control-plane
voice-port 0/1/0
voice-port 0/1/1
mgcp fax t38 ecm
gatekeeper
 shutdown
line con 0
 logging synchronous
line aux 0
line 66
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
line vty 0 4
 login local
!
scheduler allocate 20000 1000
end
```

ANEXO 2

CONFIGURACION DE LA WLC

802.11a cac video tspec-inactivity-timeout ignore

802.11a cac voice stream-size 84000 max-streams 2

802.11b cac voice tspec-inactivity-timeout ignore

802.11b cac video tspec-inactivity-timeout ignore

802.11b cac voice stream-size 84000 max-streams 2

aaa auth mgmt local radius

Location Summary

Algorithm used: Average
Client
RSSI expiry timeout: 5 sec
Half life: 0 sec
Notify Threshold: 0 db
Calibr
ating Client
RSSI expiry timeout: 5 sec
Half life: 0 sec
Rogue AP
RSSI expiry timeout: 5 sec
Half life: 0 sec
Notify Threshold: 0 db
RFID Tag
RSSI expiry timeout: 5 sec
Half life: 0 sec
Notify Threshold: 0 db

location rssi-half-life tags 0

location rssi-half-life client 0

location rssi-half-life rogue-aps 0

location expiry tags 5

location expiry client 5

location expiry calibrating-client 5

location expiry rogue-aps 5

Cisco Public Safety is not allowed to set in this domain

ap syslog host global 255.255.255.255

cdp disable

country EC

local-auth method fast server-key 736563726574

interface address ap-manager 192.168.100.3 255.255.255.0 192.168.100.1

interface address management 192.168.100.2 255.255.255.0 192.168.100.1

interface address virtual 1.1.1.1

interface dhcp ap-manager primary 192.168.100.2

interface dhcp management primary 192.168.100.2

interface port ap-manager 1

interface port management 1

load-balancing window 5

mesh security eap

mgmtuser add admin **** read-write

mobility group domain tesis

mobility dscp 0

network multicast mode multicast 0.0.0.0

network ap-priority disabled

network otap-mode disable

network rf-network-name tesis

radius fallback-test mode off

radius fallback-test username cisco-probe

radius fallback-test interval 300

rogue ap ssid alarm

rogue ap valid-client alarm

rogue adhoc enable

rogue adhoc alert

rogue ap rldp disable

snmp version v2c enable

snmp version v3 enable

sysname Cisco_cc:bc:a0

wlan create 1 Tesis2 Tesis2

wlan nac disable 1

wlan session-timeout 1 1800

wlan wmm allow 1

wlan security wpa akm ft reassociation-time 20 1

wlan security wpa akm ft over-the-air enable 1

wlan security wpa akm ft over-the-ds enable 1

wlan enable 1

ANEXO 3

Distribución Chi Cuadrado X^2

P = Probabilidad de encontrar un valor mayor o igual que el chi cuadrado tabulado, ν = Grados de Libertad

ν/p	0,001	0,0025	0,005	0,01	0,025	0,05	0,1	0,15	0,2	0,25	0,3	0,35	0,4	0,45	0,5
1	10,8274	9,1404	7,8794	6,6349	5,0239	3,8415	2,7055	2,0722	1,6424	1,3233	1,0742	0,8735	0,7083	0,5707	0,4549
2	13,8150	11,9827	10,5965	9,2104	7,3778	5,9915	4,6052	3,7942	3,2189	2,7726	2,4079	2,0996	1,8326	1,5970	1,3863
3	16,2660	14,3202	12,8381	11,3449	9,3484	7,8147	6,2514	5,3170	4,6416	4,1083	3,6649	3,2831	2,9462	2,6430	2,3660
4	18,4662	16,4238	14,8602	13,2767	11,1433	9,4877	7,7794	6,7449	5,9886	5,3853	4,8784	4,4377	4,0446	3,6871	3,3567
5	20,5147	18,3854	16,7496	15,0863	12,8325	11,0705	9,2363	8,1152	7,2893	6,6257	6,0644	5,5731	5,1319	4,7278	4,3515
6	22,4575	20,2491	18,5475	16,8119	14,4494	12,5916	10,6446	9,4461	8,5581	7,8408	7,2311	6,6948	6,2108	5,7652	5,3481
7	24,3213	22,0402	20,2777	18,4753	16,0128	14,0671	12,0170	10,7479	9,8032	9,0371	8,3834	7,8061	7,2832	6,8000	6,3458
8	26,1239	23,7742	21,9549	20,0902	17,5345	15,5073	13,3616	12,0271	11,0301	10,2189	9,5245	8,9094	8,3505	7,8325	7,3441
9	27,8767	25,4625	23,5893	21,6660	19,0228	16,9190	14,6837	13,2880	12,2421	11,3887	10,6564	10,0060	9,4136	8,8632	8,3428
10	29,5879	27,1119	25,1881	23,2093	20,4832	18,3070	15,9872	14,5339	13,4420	12,5489	11,7807	11,0971	10,4732	9,8922	9,3418
11	31,2635	28,7291	26,7569	24,7250	21,9200	19,6752	17,2750	15,7671	14,6314	13,7007	12,8987	12,1836	11,5298	10,9199	10,3410
12	32,9092	30,3182	28,2997	26,2170	23,3367	21,0261	18,5493	16,9893	15,8120	14,8454	14,0111	13,2661	12,5838	11,9463	11,3403
13	34,5274	31,8830	29,8193	27,6882	24,7356	22,3620	19,8119	18,2020	16,9848	15,9839	15,1187	14,3451	13,6356	12,9717	12,3398
14	36,1239	33,4262	31,3194	29,1412	26,1189	23,6848	21,0641	19,4062	18,1508	17,1169	16,2221	15,4209	14,6853	13,9961	13,3393
15	37,6978	34,9494	32,8015	30,5780	27,4884	24,9958	22,3071	20,6030	19,3107	18,2451	17,3217	16,4940	15,7332	15,0197	14,3389
16	39,2518	36,4555	34,2671	31,9999	28,8453	26,2962	23,5418	21,7931	20,4651	19,3689	18,4179	17,5646	16,7795	16,0425	15,3385
17	40,7911	37,9462	35,7184	33,4087	30,1910	27,5871	24,7690	22,9770	21,6146	20,4887	19,5110	18,6330	17,8244	17,0646	16,3382
18	42,3119	39,4220	37,1564	34,8052	31,5264	28,8693	25,9894	24,1555	22,7595	21,6049	20,6014	19,6993	18,8679	18,0860	17,3379
19	43,8194	40,8847	38,5821	36,1908	32,8523	30,1435	27,2036	25,3289	23,9004	22,7178	21,6891	20,7638	19,9102	19,1069	18,3376
20	45,3142	42,3358	39,9969	37,5663	34,1696	31,4104	28,4120	26,4976	25,0375	23,8277	22,7745	21,8265	20,9514	20,1272	19,3374
21	46,7963	43,7749	41,4009	38,9322	35,4789	32,6706	29,6151	27,6620	26,1711	24,9348	23,8578	22,8876	21,9915	21,1470	20,3372
22	48,2676	45,2041	42,7957	40,2894	36,7807	33,9245	30,8133	28,8224	27,3015	26,0393	24,9390	23,9473	23,0307	22,1663	21,3370
23	49,7276	46,6231	44,1814	41,6383	38,0756	35,1725	32,0069	29,9792	28,4288	27,1413	26,0184	25,0055	24,0689	23,1852	22,3369
24	51,1790	48,0336	45,5584	42,9798	39,3641	36,4150	33,1962	31,1325	29,5533	28,2412	27,0960	26,0625	25,1064	24,2037	23,3367
25	52,6187	49,4351	46,9280	44,3140	40,6465	37,6525	34,3816	32,2825	30,6752	29,3388	28,1719	27,1183	26,1430	25,2218	24,3366
26	54,0511	50,8291	48,2898	45,6416	41,9231	38,8851	35,5632	33,4295	31,7946	30,4346	29,2463	28,1730	27,1789	26,2395	25,3365
27	55,4751	52,2152	49,6450	46,9628	43,1945	40,1133	36,7412	34,5736	32,9117	31,5284	30,3193	29,2266	28,2141	27,2569	26,3363
28	56,8918	53,5939	50,9936	48,2782	44,4608	41,3372	37,9159	35,7150	34,0266	32,6205	31,3909	30,2791	29,2486	28,2740	27,3362
29	58,3006	54,9662	52,3355	49,5878	45,7223	42,5569	39,0875	36,8538	35,1394	33,7109	32,4612	31,3308	30,2825	29,2908	28,3361

BIBLIOGRAFIA

1. KOUCHERYAVY, Y.. Traffic and QoS Management in Wirelless Multimedia Networks.., New York – Estados Unidos ., Springer., Pp. 20-26

2. REID, R., Manual de Redes Inalámbricas., New York – Estados Unidos., McGraw-Hill., 2008., Pp. 143-145

BIBLIOGRAFIA INTERNET

3. CALIDAD DE SERVICIO

http://es.wikipedia.org/wiki/Calidad_de_servicio#QoS_en_escenarios_inal.C3.A1mbricos
2011-04-11

4. DUALIDAD Y CALIDAD DE SERVICIO EN REDES INALÁMBRICAS.

http://www.cybertesis.uchile.cl/tesis/uchile/2010/cf-troncoso_cs/pdfAmont/cf-troncoso_cs.pdf
2011-05-01

5. REDES INALÁMBRICAS

http://www.monografias.com/trabajos12/reina/reina.shtml#in
2011-05-03

6. PROTOCOLOS DE CALIDAD DE SERVICIO – QOS

http://es.scribd.com/doc/49332259/Protocolos-QoS-v4-0.
2011-05-05

7. **INTRODUCCIÓN A PUNTO DE CÓDIGO DE SERVICIOS DIFERENCIADOS (DSCP, DIFFERENTIATED SERVICES CODE POINT)**
http://technet.microsoft.com/es-es/library/cc787218(v=ws.10)
2011-06-02

8. **CALIDAD DE SERVICIOS EN REDES**
http://www.monografias.com/trabajos82/calidad-servicios-redes-ip/calidad-servicios-redes-ip2.shtml
2011-08-15

9. **ANÁLISIS DE TRÁFICO**
http://dspace.ups.edu.ec/bitstream/123456789/32/9/Capitulo3.pdf
2011-08-29

10. **DIFFSERV: SERVICIOS DIFERENCIADOS**
http://iie.fing.edu.uy/ense/asign/perfredes/trabajos/trabajos_2003/diffserv/Trabajo%20Final.pdf
2011-09-11

11. **EL PROTOCOLO DIFFSERV**
http://dspace.epn.edu.ec/bitstream/15000/8685/9/T10471CAP2.pdf
2011-10-01

12. **EL PROTOCOLO DIFFSERV BAJO EL SISTEMA OPERATIVO LINUX**
http://dspace.epn.edu.ec/bitstream/15000/8685/4/T10471CAP3.pdf
2011-10-13

13. **ESTUDIO DE DIFFERENTIATED SERVICES (DIFFSERV) USANDO EL SISTEMA OPERATIVO ABIERTO (LINUX) PARA LA PROVISIÓN DE CALIDAD DE SERVICIO EN REDES CON VOIP AUTOR**
http://bibdigital.epn.edu.ec/bitstream/15000/261/1/CD-0683.pdf

2011-10-15

14. FACTORES QUE AFECTAN LA CALIDAD DE SERVICIO

http://www.voipers.net/2007/01/factores-que-afectan-la-calidad-de-la.html

2011-10-20

15. CAUSAS, SOLUCIONES Y VALORES RECOMENDADOS.

http://www.VoIPforo.com/QoS/QoS_Jitter.php

2011-11-09

16. DD-WRT

http://es.wikipedia.org/wiki/DD-WRT

2012-03-30

17. MEJORA TU ROUTER LINKSYS WRT310N CON DD-WRT

http://www.taringa.net/posts/info/9704858/Mejora-tu-Router-Linksys-WRT310N-con-DD-wrt.html

2012-03-05

18. WIRESHARK

http://es.scribd.com/doc/25350978/Manual-Rapido-de-WireShark

2012-03-20

19. CONFIGURING THE CISCO WIRELESS CONTROLLER NETWORK MODULE ON A CISCO ROUTER, CISCO IOS RELEASE 12.4(15)T

http://www.cisco.com/en/US/docs/ios/12_4t/12_4t15/rockynm.html#wp2023946

2012-04-02

20. ANÁLISIS DE LA CALIDAD EXPERIMENTADA EN APLICACIONES DE VOZ SOBRE IP DE LIBRE DISTRIBUCIÓN

http://repositorio.bib.upct.es/dspace/bitstream/10317/719/1/pfc2756.pdf

2012-04-16