

**PROPUESTA DE MIGRACION DE LA RED DE DATOS DE
LA UNIVERSIDAD DEL CAUCA HACIA LA TECNOLOGIA
IPv6 SOBRE REDES ETHERNET DE ALTA VELOCIDAD**

**VICTOR ALBERTO HERMIDA QUINTERO
WILLIAM JAMES RODRIGUEZ ORTIZ**

**UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELECOMUNICACIONES
POPAYÁN
2005**

**PROPUESTA DE MIGRACION DE LA RED DE DATOS DE LA
UNIVERSIDAD DEL CAUCA HACIA LA TECNOLOGIA IPv6 SOBRE
REDES ETHERNET DE ALTA VELOCIDAD**



**VICTOR ALBERTO HERMIDA QUINTERO
WILLIAM JAMES RODRIGUEZ ORTIZ**

**UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELECOMUNICACIONES
POPAYÁN
2005**

**PROPUESTA DE MIGRACION DE LA RED DE DATOS DE LA
UNIVERSIDAD DEL CAUCA HACIA LA TECNOLOGIA IPv6 SOBRE
REDES ETHERNET DE ALTA VELOCIDAD**



**VICTOR ALBERTO HERMIDA QUINTERO
WILLIAM JAMES RODRIGUEZ ORTIZ**

**Trabajo de grado presentado como requisito para optar al título de
Ingeniero en Electrónica y Telecomunicaciones**

Director: IE. Mag. FRANCISCO JAVIER TERÁN CUARÁN

**UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELECOMUNICACIONES
POPAYÁN
2005**

**PROPUESTA DE MIGRACION DE LA RED DE DATOS DE
LA UNIVERSIDAD DEL CAUCA HACIA LA TECNOLOGIA
IPv6 SOBRE REDES ETHERNET DE ALTA VELOCIDAD**

ANEXO A

**VICTOR ALBERTO HERMIDA QUINTERO
WILLIAM JAMES RODRIGUEZ ORTIZ**

**UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELECOMUNICACIONES
POPAYÁN
2005**

**PROPUESTA DE MIGRACION DE LA RED DE DATOS DE LA
UNIVERSIDAD DEL CAUCA HACIA LA TECNOLOGIA IPv6 SOBRE
REDES ETHERNET DE ALTA VELOCIDAD**

ANEXO A

PROTOCOLO IP VERSION 6



VICTOR ALBERTO HERMIDA QUINTERO

WILLIAM JAMES RODRIGUEZ ORTIZ

Director: IE. Mag. FRANCISCO JAVIER TERÁN CUARÁN

UNIVERSIDAD DEL CAUCA

FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

DEPARTAMENTO DE TELECOMUNICACIONES

POPAYÁN

2005

**PROPUESTA DE MIGRACION DE LA RED DE DATOS DE
LA UNIVERSIDAD DEL CAUCA HACIA LA TECNOLOGIA
IPv6 SOBRE REDES ETHERNET DE ALTA VELOCIDAD**

ANEXO B

**VICTOR ALBERTO HERMIDA QUINTERO
WILLIAM JAMES RODRIGUEZ ORTIZ**

**UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELECOMUNICACIONES
POPAYÁN
2005**

**PROPUESTA DE MIGRACION DE LA RED DE DATOS DE LA
UNIVERSIDAD DEL CAUCA HACIA LA TECNOLOGIA IPv6 SOBRE
REDES ETHERNET DE ALTA VELOCIDAD**

ANEXO B

JERARQUIA DIGITAL ETHERNET



**VICTOR ALBERTO HERMIDA QUINTERO
WILLIAM JAMES RODRIGUEZ ORTIZ**

Director: IE. Mag. FRANCISCO JAVIER TERÁN CUARÁN

**UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELECOMUNICACIONES
POPAYÁN
2005**

**PROPUESTA DE MIGRACION DE LA RED DE DATOS DE
LA UNIVERSIDAD DEL CAUCA HACIA LA TECNOLOGIA
IPv6 SOBRE REDES ETHERNET DE ALTA VELOCIDAD**

ANEXO C

**VICTOR ALBERTO HERMIDA QUINTERO
WILLIAM JAMES RODRIGUEZ ORTIZ**

**UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELECOMUNICACIONES
POPAYÁN
2005**

**PROPUESTA DE MIGRACION DE LA RED DE DATOS DE LA
UNIVERSIDAD DEL CAUCA HACIA LA TECNOLOGIA IPv6 SOBRE
REDES ETHERNET DE ALTA VELOCIDAD**

ANEXO C

**MEDIDAS DE DESEMPEÑO DE LA RED DE DATOS DE LA UNIVERSIDAD DEL
CAUCA**



**VICTOR ALBERTO HERMIDA QUINTERO
WILLIAM JAMES RODRIGUEZ ORTIZ**

Director: IE. Mag. FRANCISCO JAVIER TERÁN CUARÁN

**UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELECOMUNICACIONES
POPAYÁN
2005**

**PROPUESTA DE MIGRACION DE LA RED DE DATOS DE
LA UNIVERSIDAD DEL CAUCA HACIA LA TECNOLOGIA
IPv6 SOBRE REDES ETHERNET DE ALTA VELOCIDAD**

ANEXO D

**VICTOR ALBERTO HERMIDA QUINTERO
WILLIAM JAMES RODRIGUEZ ORTIZ**

**UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELECOMUNICACIONES
POPAYÁN
2005**

**PROPUESTA DE MIGRACION DE LA RED DE DATOS DE LA
UNIVERSIDAD DEL CAUCA HACIA LA TECNOLOGIA IPv6 SOBRE
REDES ETHERNET DE ALTA VELOCIDAD**

ANEXO D

ESPECIFICACIONES DE LOS DISPOSITIVOS DE INTERNETWORKING



**VICTOR ALBERTO HERMIDA QUINTERO
WILLIAM JAMES RODRIGUEZ ORTIZ**

Director: IE. Mag. FRANCISCO JAVIER TERÁN CUARÁN

**UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELECOMUNICACIONES
POPAYÁN
2005**

**PROPUESTA DE MIGRACION DE LA RED DE DATOS DE
LA UNIVERSIDAD DEL CAUCA HACIA LA TECNOLOGIA
IPv6 SOBRE REDES ETHERNET DE ALTA VELOCIDAD**

ANEXO E

**VICTOR ALBERTO HERMIDA QUINTERO
WILLIAM JAMES RODRIGUEZ ORTIZ**

**UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELECOMUNICACIONES
POPAYÁN
2005**

**PROPUESTA DE MIGRACION DE LA RED DE DATOS DE LA
UNIVERSIDAD DEL CAUCA HACIA LA TECNOLOGIA IPv6 SOBRE
REDES ETHERNET DE ALTA VELOCIDAD**

ANEXO E

**ESTUDIO FINANCIERO DE LAS PROPUESTAS DE DISEÑO PARA LA RED DE
DATOS DE LA UNIVERSIDAD DEL CAUCA**



**VICTOR ALBERTO HERMIDA QUINTERO
WILLIAM JAMES RODRIGUEZ ORTIZ**

Director: IE. Mag. FRANCISCO JAVIER TERÁN CUARÁN

**UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELECOMUNICACIONES
POPAYÁN**

2005

INTRODUCCION

La Red de Datos de la Universidad del Cauca actualmente se ve enfrentada al manejo de grandes volúmenes de información los cuales producen un efecto indeseable como son los “cuellos de botella”. La cantidad de usuarios del sistema y el uso que le dan ha crecido sustancialmente, la congestión de tráfico se está notando, lo que requiere ampliar sus capacidades.

Han surgido nuevas tecnologías y aplicaciones que requieren mayor rendimiento del sistema; un ejemplo de esto son los diversos Sistemas de Información con los que cuenta la Universidad del Cauca, entre los cuales se pueden nombrar los siguientes : Sistema de Información Administrativo que presta los servicios de pago de nómina, servicio financiero (contabilidad, presupuestos, tesorería), servicio de admisiones y pago de derechos financieros; Sistema de Información de la Vicerrectoría de investigaciones que maneja todo lo relacionado con los proyectos de investigación; Sistema de Información de la Biblioteca que presta los servicios de consulta y gestión de la misma; y actualmente se está implantando el Sistema de Información Académico el cual permite realizar todas las actividades de registro y control académico de toda la comunidad universitaria. El uso de estos Sistemas de Información representa una carga adicional para la red porque se incrementa el tráfico que circula por ella, por lo tanto se debe brindar una mayor seguridad para garantizar la integridad de los datos y confiabilidad de la información.

Además con el futuro cambio de Internet del protocolo IPv4 al protocolo IPv6, se hace necesario establecer un modelo para la evolución de la Red de Datos de la Universidad del Cauca hacia este protocolo soportado sobre tecnologías de transmisión de alta velocidad.

Con la aparición de las nuevas tecnologías Ethernet de alta velocidad e IPv6, existe la posibilidad de que la comunidad universitaria se pueda beneficiar de nuevas aplicaciones que en la actualidad no se pueden implantar con la potencia deseada, debido esencialmente a los grandes requerimientos de ancho de banda. Dentro de estas aplicaciones se encuentran las siguientes: Tele-educación, Tele-medicina, Videoconferencia, Acceso a Internet de banda ancha, Voz sobre IP o aplicaciones relacionadas con el almacenamiento tales como backup de datos, recuperación de desastres o almacenamiento bajo demanda; entre otros.

La migración de la Red de Datos le permitirá a la Universidad del Cauca acercarse a la comunidad universitaria con nuevos servicios que se añadan y complementen a los que ya se vienen prestando en la actualidad y en especial la participación directa en el

6Bone de Internet. Además con este proceso de migración se logrará la implantación de una red emblemática que sitúe a la Institución a la cabeza de la sociedad de la información y también servirá como modelo de referencia para proyectos similares que se realicen en la región o el país.

Este proyecto busca el fortalecimiento de la Red de Datos de la Universidad del Cauca con infraestructura de punta estableciendo una red suficientemente robusta para las aplicaciones actuales y de futuro próximo, preparándola para el advenimiento de la nueva red de Internet2. Esta actualización contempla tecnología de vanguardia en materia de telecomunicaciones, para darle mayor calidad de transmisión a las aplicaciones de los usuarios, seguridad, etc.

Para este fin, el documento se ha estructurado de la siguiente manera: En el primer capítulo se realiza un estudio de la infraestructura actual de la Red de Datos de la Universidad del Cauca, describiendo detalladamente la distribución física de los equipos de red y host's, cableado estructurado, funcionamiento lógico y servicios soportados. En el segundo capítulo se describen las reglas de configuración Ethernet y Fast-Ethernet para redes LAN, y se realiza el estudio de las técnicas empleadas para llevar a cabo un análisis de desempeño adecuado. En el tercer capítulo se realiza un estudio del funcionamiento de la Red de Datos de la Universidad del Cauca con las tecnologías existentes en donde se evalúa su comportamiento teniendo en cuenta las especificaciones técnicas requeridas. En el cuarto capítulo se exponen los fundamentos de las nuevas tecnologías que serán utilizadas en el proceso de migración de la Red de Datos de la Universidad del Cauca como son Gigabit Ethernet, 10 Gigabit Ethernet, e IPv6. En el quinto capítulo se realizan las diferentes opciones de diseño para la nueva arquitectura de la Red de Datos de la Universidad del Cauca, para lo cual inicialmente se presentan las consideraciones que se deben tener en cuenta para la migración de la red, se expone la metodología de diseño que se utiliza en dicho proceso y se especifican las características técnicas que deben reunir los dispositivos de internetworking para la realización de un diseño óptimo. Finalmente, en el capítulo 6 se exponen las consideraciones que se deben tener en cuenta para la migración hacia IPv6, los beneficios que se pueden obtener y la propuesta de implementación del nuevo protocolo de Internet para la Red de Datos de la Universidad del Cauca.

TABLA DE CONTENIDO

INTRODUCCION.

1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.....	1
1.1 DESCRIPCIÓN FÍSICA.....	1
1.1.1 CABLEADO DEL SECTOR DE INGENIERÍAS.....	4
1.1.2 CABLEADO DEL SECTOR DE MEDICINA.....	6
1.1.3 CABLEADO DEL SECTOR DE EDUCACIÓN.....	7
1.1.4 CABLEADO DEL SECTOR DE EL CARMEN.....	8
1.1.5 CABLEADO DEL SECTOR DE SANTO DOMINGO	10
1.1.6 CABLEADO DEL SECTOR DEL VRI.....	11
1.1.7 CABLEADO DEL SECTOR DE LAS GUACAS.....	12
1.2 DESCRIPCIÓN DEL FUNCIONAMIENTO LÓGICO.....	13
1.2.1 SECTOR DE INGENIERÍAS.....	16
1.2.2 SECTOR DE MEDICINA.....	25
1.2.3 SECTOR DE EDUCACIÓN.....	27
1.2.4 SECTOR DE EL CARMEN.....	31
1.2.5 SECTOR DE SANTO DOMINGO.....	36
1.2.6 SECTOR DEL VRI.....	39
1.2.7 SECTOR DE LAS GUACAS.....	41
1.3 DIRECCIONAMIENTO IP (SUBREDES).....	43
1.4 SERVIDORES Y SERVICIOS SOPORTADOS.....	44
2. NORMAS DE CONFIGURACION Y DESEMPEÑO DE REDES LAN ETHERNET.....	47
2.1 REGLAS DE CONFIGURACIÓN.....	47
2.1.1 MEDIOS DE COMUNICACIÓN.....	47
2.1.1.1 PAR TRENZADO.....	48
2.1.1.2 FIBRA ÓPTICA.....	49
2.1.2 REGLAS DE CONFIGURACIÓN PARA ETHERNET Y FAST-ETHERNET.....	52
2.1.2.1 CONFIGURACIÓN DE UNA ETHERNET A 10 MBPS.....	52
2.1.2.2 CONFIGURACIÓN DE UNA ETHERNET A 100 MBPS.....	55
2.2 NIVELES DE DESEMPEÑO.....	56
2.2.1 EVALUACIÓN DEL COMPORTAMIENTO DE LA RED.....	57
2.2.1.1 IDENTIFICACIÓN DEL SERVICIO CLAVE.....	58
2.2.1.2 DETERMINACIÓN DE LOS ELEMENTOS DEL SERVICIO.....	58

2.2.1.3	ESTABLECIMIENTO DE LAS MEDIDAS A TOMAR.....	58
2.2.1.4	CONOCIMIENTO DE LOS LÍMITES DE DESEMPEÑO.....	60
2.2.1.5	CONTROL DE LA RED.....	62
2.2.2	REQUERIMIENTOS DE LAS NUEVAS APLICACIONES.....	62

3.	ANALISIS DEL DESEMPEÑO DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.....	63
3.1	ANALISIS DE LA INFRAESTRUCTURA FISICA.....	63
3.2	ANALISIS DE DESEMPEÑO.....	64
3.2.1	ANALISIS DEL ACCESO A INTERNET.....	68
3.2.1.1	ENRUTADOR TELECOM: ROUTER CISCO 1700.....	68
3.2.1.2	ENRUTADOR EMTEL: ROUTER CISCO 3600.....	69
3.2.2	CONCLUSIONES DEL ACCESO A INTERNET.....	70
3.2.3	ANALISIS DEL ACCESO REMOTO (RAS).....	71
3.2.4	CONCLUSIONES DEL ACCESO REMOTO (RAS).....	72
3.2.5	ANALISIS DEL BACKBONE.....	73
3.2.6	CONCLUSIONES GENERALES DEL BACKBONE.....	80
3.2.7	ANALISIS DE LOS SEGMENTOS DEL SECTOR DE INGENIERIAS.....	82
3.2.8	ANALISIS DE LOS SEGMENTOS DEL SECTOR DE EDUCACION.....	85
3.2.9	ANALISIS DE LOS SEGMENTOS DEL SECTOR DEL CARMEN.....	88
3.2.10	ANALISIS DE LOS SEGMENTOS DEL SECTOR DE SANTO DOMINGO.....	90
3.2.11	ANALISIS DE LOS SEGMENTOS DEL SECTOR DEL VRI.....	93
3.2.12	ANALISIS DE LOS SEGMENTOS DEL SECTOR DE MEDICINA.....	95
3.2.13	CONCLUSIONES GENERALES DE LOS SEGMENTOS.....	97
3.2.14	ANALISIS DE LOS SERVIDORES DEL SECTOR DE EDUCACION (SISTEMAS DE INFORMACION).....	98
3.2.15	CONCLUSIONES GENERALES DE LOS SERVIDORES DEL SECTOR DE EDUCACION.....	99
3.2.16	ANALISIS DE LOS SERVIDORES DEL SECTOR DEL IPET (SERVICIOS DE LA RED TCP/IP).....	100
3.2.17	CONCLUSIONES GENERALES DE LOS SERVIDORES DEL SECTOR DEL IPET.....	101
3.2.18	ANALISIS DE BROADCAST Y MULTICAST.....	101

4. ESPECIFICACIONES TECNICAS DE LAS TECNOLOGIAS	
ETHERNET DE ALTA VELOCIDAD E IPv6.....	105
4.1 ESPECIFICACIONES DEL ESTANDAR GIGABIT ETHERNET	105
4.1.1 ARQUITECTURA DE GIGABIT ETHERNET	105
4.1.2 CAPA DE ACCESO AL MEDIO.....	107
4.1.2.1 NIVEL MAC.....	107
4.1.2.2 NIVEL DE ENLACE LÓGICO.....	108
4.1.3 CAPA FÍSICA.....	108
4.2 ESPECIFICACIONES DEL ESTANDAR 10 GIGABIT ETHERNET..	109
4.2.1 ARQUITECTURA DE 10 GIGABIT ETHERNET	109
4.2.2 CAPA DE ACCESO AL MEDIO.....	110
4.2.2.1 NIVEL MAC.....	110
4.2.2.2 NIVEL DE ENLACE LOGICO.....	110
4.2.3 CAPA FISICA.....	110
4.2.3.1 NECESIDAD DE UNA FIBRA DE NUEVA GENERACIÓN...	111
4.2.3.2 10 GIGABIT ETHERNET SOBRE CABLEADO DE COBRE..	112
4.2.4 10 GIGABIT ETHERNET EN REDES DE AREA LOCAL.....	112
4.3 ESPECIFICACIONES DEL PROTOCOLO IPV6.....	114
4.3.1 FORMATO DE TRAMA IPV6.....	114
4.3.2 DIRECCIONAMIENTO.....	117
4.3.2.1 TIPOS DE DIRECCIONES EN IPV6.....	117
4.3.2.2 DIRECCIONES UNICAST.....	117
4.3.2.3 DIRECCIONES ANYCAST.....	120
4.3.2.4 DIRECCIONES MULTICAST.....	120
4.3.3 PROTOCOLO ICMPV6.....	121
4.3.4 PROTOCOLO NEIGHBOR DISCOVERY (ND).....	123
4.3.5 AUTOCONFIGURACIÓN DE DIRECCIONES.....	125
4.3.6 DESCUBRIMIENTO DEL MTU.....	127
4.3.7 TRANSICION DE IPv4 HACIA IPv6.....	127
4.3.8 MECANISMOS DE TRANSICION DE IPv4 A IPv6.....	128
4.3.8.1 TÉCNICAS DE DOBLE PILA (DUAL STACK).....	128
4.3.8.2 TÉCNICAS DE TUNNELING.....	129
4.3.8.3 TÉCNICAS DE TRADUCCIÓN.....	131
5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.....	133
5.1 CONSIDERACIONES PARA LA MIGRACION HACIA GIGABIT ETHERNET.....	133
5.1.1 ETHERNET: LA TECNOLOGIA DE RED DOMINANTE.....	134
5.1.2 RAZONES QUE IMPULSAN EL CRECIMIENTO DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.....	135

5.1.3	GIGABIT ETHERNET: LA ALTERNATIVA PARA LANs E INTRANETS.....	137
5.2	CONSIDERACIONES PARA LA MIGRACION HACIA 10 GIGABIT ETHERNET.....	139
5.3	MODELO DE DISEÑO JERÁRQUICO.....	141
5.3.1	FUNCIÓN DEL NIVEL CORE.....	142
5.3.2	FUNCIÓN DEL NIVEL DE DISTRIBUCION.....	142
5.3.3	FUNCIÓN DEL NIVEL DE ACCESO.....	143
5.4	AGREGACION DE ENLACES.....	144
5.5	ESPECIFICACIONES DE LOS DISPOSITIVOS DE INTERNETWORKING.....	145
5.5.1	SWITCHES DE NIVEL DE ACCESO.....	145
5.5.1.1	CALIDAD DE SERVICIO (QOS).....	145
5.5.1.2	SEGURIDAD.....	145
5.5.1.3	GESTIÓN.....	146
5.5.1.4	DESEMPEÑO Y DISPONIBILIDAD.....	146
5.5.2	SWITCHES DE DISTRIBUCION.....	147
5.5.2.1	CALIDAD DE SERVICIO (QOS).....	147
5.5.2.2	SEGURIDAD.....	147
5.5.2.3	GESTIÓN.....	148
5.5.2.4	DESEMPEÑO Y DISPONIBILIDAD.....	148
5.5.2.5	DESEMPEÑO DE ROUTING.....	149
5.5.3	SWITCHES DE CORE.....	149
5.5.3.1	CALIDAD DE SERVICIO (QOS).....	149
5.5.3.2	SEGURIDAD.....	149
5.5.3.3	GESTIÓN.....	150
5.5.3.4	DESEMPEÑO Y DISPONIBILIDAD.....	150
5.5.3.5	DESEMPEÑO DE ROUTING.....	151
5.6	PROPUESTAS DE DISEÑO PARA LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.....	151
5.6.1	PROPUESTA DE DISEÑO CON LOS PRODUCTOS CISCO.....	152
5.6.1.1	DESCRIPCION GENERAL DE LOS PRODUCTOS CISCO....	152
5.6.1.2	PROPUESTAS DE DISEÑO PARA EL BACKBONE CON TECNOLOGIA GIGABIT ETHERNET.....	155
5.6.1.3	PROPUESTA DE DISEÑO PARA EL SECTOR DE INGENIERIAS.....	167
5.6.1.4	PROPUESTA DE DISEÑO PARA EL SECTOR DE INGENIERIAS (IPET Y FISICA).....	171
5.6.1.5	PROPUESTA DE DISEÑO PARA EL SECTOR DE EDUCACION.....	173
5.6.1.6	PROPUESTA DE DISEÑO PARA EL SECTOR DEL CARMEN.....	176

5.6.1.7	PROPUESTA DE DISEÑO PARA EL SECTOR DE SANTO DOMINGO.....	179
5.6.1.8	PROPUESTA DE DISEÑO PARA EL SECTOR DEL VRI.....	183
5.6.1.9	PROPUESTA DE DISEÑO PARA EL SECTOR DE MEDICINA.....	185
5.6.1.10	PROPUESTA DE DISEÑO PARA EL BACKBONE CON TECNOLOGIA 10 GIGABIT ETHERNET.....	187
5.6.2	PROPUESTA DE DISEÑO CON LOS PRODUCTOS ALCATEL...	191
5.6.2.1	DESCRIPCION GENERAL DE LOS PRODUCTOS ALCATEL.....	191
5.6.2.2	EQUIVALENCIA ENTRE LOS PRODUCTOS DE ALCATEL Y CISCO.....	195
5.7	FASES DE MIGRACION HACIA GIGABIT ETHERNET.....	195
5.7.1	FASE No. 1: ACTUALIZACIÓN DE ENLACES SWITCH A SWITCH (BACKBONE).....	196
5.7.2	FASE No. 2: ACTUALIZACIÓN DE ENLACES SWITCH A SERVIDOR.....	198
5.7.3	FASE No. 3: ACTUALIZACIÓN DE SEGMENTOS ETHERNET Y FAST ETHERNET.....	199
5.7.4	FASE No. 4: ACTUALIZACIÓN DE GRUPOS DE TRABAJO DE ALTO DESEMPEÑO.....	200
5.8	FASES DE MIGRACION HACIA 10 GIGABIT ETHERNET.....	201
5.8.1	FASE No. 1: ACTUALIZACIÓN DE ENLACES SWITCH A SWITCH (BACKBONE).....	202
5.8.2	FASE No. 2: ACTUALIZACIÓN DE ENLACES SWITCH A SERVIDOR.....	202

6. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA IPv6 SOBRE ETHERNET DE ALTA VELOCIDAD.....204

6.1	CONSIDERACIONES PARA LA MIGRACION HACIA IPv6.....	204
6.1.1	RETOS DE LA MIGRACION HACIA IPV6.....	204
6.1.2	NECESIDAD DE MIGRACION HACIA IPv6 Y APOYO DE LA INDUSTRIA.....	205
6.1.3	BENEFICIOS DE LA MIGRACION HACIA IPv6.....	206
6.2	TRANSMISION DE PAQUETES IPV6 SOBRE REDES ETHERNET.....	207
6.2.1	UNIDAD DE TRANSMISIÓN MÁXIMA.....	208
6.2.2	FORMATO DE LA TRAMA.....	208
6.2.3	AUTOCONFIGURACIÓN STATELESS.....	209
6.2.3.1	IDENTIFICADORES DE INTERFAZ DE IPv6.....	209
6.2.3.2	MAPEO DE DIRECCIONES UNICAST.....	213
6.2.3.3	MAPEO DE DIRECCIONES MULTICAST.....	214

6.3	PROPUESTA DE IMPLEMENTACION DE IPv6 PARA LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.....	215
6.3.1	ARQUITECTURA DE LA NUEVA RED.....	215
6.3.1.1	RED PARALELA IPv6.....	215
6.3.1.2	RED CON PILA DUAL DE PROTOCOLOS.....	216
6.3.1.3	SELECCIÓN DE LA ARQUITECTURA DE RED.....	217
6.3.2	PLAN DE NUMERACION.....	217
6.3.2.1	ESTRUCTURA DE DIRECCIONAMIENTO IPv6 DE MULTIPLES NIVELES.....	219
6.3.2.2	ESTRUCTURA DE DIRECCIONAMIENTO IPv6 DE UN UNICO NIVEL.....	219
6.3.3	CONEXIÓN CON EL 6BONE.....	220
6.3.3.1	SELECCIÓN DEL ROUTER DE FRONTERA.....	221
6.3.3.2	CONEXIÓN DEL ROUTER DE FRONTERA AL 6BONE.....	221
6.3.4	TOPOLOGIA FINAL DE LA ARQUITECTURA DE LA RED IPv6.....	221
6.3.5	PROTOCOLOS DE NIVEL SUPERIOR.....	223
6.4	CONFIGURACION DE LOS HOSTS PARA HABILITAR EL SOPORTE IPv6.....	226
6.4.1	CONFIGURACION DE EQUIPOS CON SISTEMAS OPERATIVOS WINDOWS.....	226
6.4.1.1	CONFIGURACION DEL PROTOCOLO IPv6 EN WINDOWS 2000.....	226
6.4.1.2	CONFIGURACION DEL PROTOCOLO IPv6 EN WINDOWS XP.....	228
6.4.1.3	CONFIGURACION DEL PROTOCOLO IPv6 EN WINDOWS 2003 SERVER.....	228
6.4.1.4	ASIGNACION DE DIRECCIONES IPv6 A UNA INTERFAZ DE RED.....	229
6.4.1.5	PRUEBA DE CONECTIVIDAD IPv6.....	231
6.4.2	CONFIGURACION DE EQUIPOS CON SISTEMAS OPERATIVOS LINUX (RED HAT Y FEDORA).....	231
6.4.2.1	CONFIGURACION DEL PROTOCOLO IPv6 EN RED HAT.....	231
6.4.2.2	CONFIGURACION DEL PROTOCOLO IPv6 EN FEDORA.....	234
6.5	FASES DE MIGRACION HACIA IPv6.....	234
6.5.1	FASE No. 1: ACTUALIZACIÓN DE LAS APLICACIONES PARA QUE SEAN INDEPENDIENTES DEL PROTOCOLO IPv6 O IPv4.....	235
6.5.2	FASE No. 2: ACTUALIZACIÓN DE LA INFRAESTRUCTURA DNS.....	235
6.5.3	FASE No. 3: ACTUALIZACIÓN DE HOSTS A NODOS IPv6/IPv4.....	235
6.5.4	FASE No. 4: ACTUALIZACIÓN DE LA INFRAESTRUCTURA DE ROUTING.....	236

6.5.5 FASE No. 5: CONVERSION DE NODOS IPv6/IPv4 A NODOS IPv6
SOLAMENTE.....236

CONCLUSIONES Y RECOMENDACIONES.....238

GLOSARIO.....240

LISTA DE ACRÓNIMOS.....248

BIBLIOGRAFIA.....252

LISTA DE TABLAS Y FIGURAS

Tabla 1. 1. Resumen Puntos de Red del Sector de Ingenierías.....	5
Tabla 1. 2. Resumen Puntos de Red del Sector de Medicina.....	6
Tabla 1. 3. Resumen Puntos de Red del Sector de Educación.....	7
Tabla 1. 4. Resumen Puntos de Red del Sector de El Carmen.....	9
Tabla 1. 5. Resumen Puntos de Red del Sector de Artes.....	9
Tabla 1. 6. Resumen Puntos de Red del Sector Archivo Histórico.....	9
Tabla 1. 7. Resumen Puntos de Red del Sector Casa Caldas.....	9
Tabla 1. 8. Resumen Puntos de Red del Sector de Santo Domingo.....	10
Tabla 1. 9. Resumen Puntos de Red del Sector de la Vicerrectoría de Investigaciones (VRI).....	11
Tabla 1. 10. Resumen Puntos de Red del Sector de Las Guacas.....	12
Tabla 1. 11. Resumen Puntos de Red Totales.....	13
Tabla 1. 12. Distribución de Hosts del Sector de Ingenierías.....	25
Tabla 1. 13. Distribución de Hosts del Sector de Medicina.....	27
Tabla 1. 14. Distribución de Hosts del Sector de Educación.....	31
Tabla 1. 15. Distribución de Hosts del Sector de El Carmen.....	36
Tabla 1. 16. Distribución de Hosts del Sector de Santo Domingo.....	38
Tabla 1. 17. Distribución de Hosts del Sector de la Vicerrectoría de Investigaciones (VRI).....	40
Tabla 1. 18. Distribución de Hosts del Sector de las Guacas.....	42
Tabla 1. 19. Resumen Distribución de Hosts de la Red total.....	42
Tabla 1. 20 Subredes IP Existentes.....	43
Tabla 2. 1. Características de los cables según su categoría.....	49
Tabla 2. 2. Atenuación (en dB/100 m) de distintos tipos de cables a diferentes frecuencias.....	49
Tabla 2. 3. Atenuación de diferentes tipos de fibra en las diversas ventanas.....	51
Tabla 2. 4. Distancias soportadas para Ethernet y Fast-Ethernet.....	51
Tabla 2. 5. Valores de retardo del viaje de ida y vuelta en tiempos de bit.....	54
Tabla 2. 6. Encogimiento del espaciamiento entre tramas en tiempos de bit.....	55
Tabla 2. 7. Modelo 1 – Máximo dominio de colisión Fast-Ethernet en metros.....	55
Tabla 2. 8. Retardo de los componentes del sistema 100BaseT.....	56
Tabla 3. 1. Umbrales de las medidas.....	68
Tabla 3. 2. Estadísticas del Enlace Switch Accelar 1200 – Router Cisco 3600.....	73
Tabla 3. 3. Tendencias de Protocolos del Enlace Switch Accelar – Router Cisco 3600.....	73
Tabla 3. 4. Niveles de Broadcast y Multicast de la Red de Datos de la Universidad del Cauca.....	102

Tabla 3. 5. Protocolos generadores de Broadcast y Multicast.....	102
Tabla 4. 1. Rangos de operación para 10GBASE-S.....	110
Tabla 4. 2. Distancias de la fibra utilizada en 10 Gigabit Ethernet.....	112
Tabla 4. 3. Tipos de mensajes ICMPv6.....	123
Tabla 5. 1. Configuraciones de la serie Cisco 4500.....	154
Tabla 5. 2. Equivalencia entre los equipos de Alcatel y Cisco.....	195
Tabla 6. 1. Direccionamiento IPv6 de múltiples niveles.....	219
Tabla 6. 2. Direccionamiento IPv6 de un único nivel.....	220
Figura 1. 1. Cableado de la Red de Datos de la Universidad del Cauca.....	3
Figura 1. 2. Cableado Estructurado del Sector de Ingenierías.....	4
Figura 1. 3. Cableado Estructurado del Sector de Medicina.....	6
Figura 1. 4. Cableado Estructurado del Sector de Educación.....	7
Figura 1. 5. Cableado Estructurado del Sector de El Carmen.....	8
Figura 1. 6. Cableado Estructurado del Sector de Santo Domingo.....	10
Figura 1. 7. Cableado Estructurado del Sector de la Vicerrectoría de Investigaciones (VRI).....	11
Figura 1. 8. Cableado Estructurado del Sector de Las Guacas.....	12
Figura 1. 9. Descripción General del Funcionamiento Lógico de la Red de Datos....	15
Figura 1. 10 Convenciones.....	16
Figura 1. 11. Funcionamiento del Sector de Ingenierías.....	17
Figura 1. 12. Funcionamiento de los Centros de Cableado 1, 13 y 15 del Sector de Ingenierías.....	18
Figura 1. 13. Funcionamiento de los Centros de Cableado 2, 11 y 12 del Sector de Ingenierías.....	19
Figura 1. 14. Funcionamiento de los Centros de Cableado 4, 5, 6, y 14 del Sector de Ingenierías.....	20
Figura 1. 15. Funcionamiento de los Centros de Cableado 7, 8 y 16 del Sector de Ingenierías.....	21
Figura 1. 16. Funcionamiento de los Centros de Cableado 9 y 10 del Sector de Ingenierías.....	22
Figura 1. 17. Funcionamiento del Centro de Cableado 3 del Sector de Ingenierías....	22
Figura 1. 18. Funcionamiento del Sector de Medicina.....	25
Figura 1. 19. Funcionamiento de los Centros de Cableado 1, 2, y 3 del Sector de Medicina.....	26
Figura 1. 20. Funcionamiento del Sector de Educación.....	27
Figura 1. 21. Funcionamiento del Centro de Cableado 1 del Sector de Educación....	28
Figura 1. 22. Funcionamiento de los Centros de Cableado 2A, 2B, 3 y 5 del Sector de Educación.....	29
Figura 1. 23. Funcionamiento del Centro de Cableado 4 del Sector de Educación...30	

Figura 1. 24. Funcionamiento del Sector de El Carmen.....	32
Figura 1. 25. Funcionamiento de los Centros de Cableado 1, 2, 3, 4, y 5 del Sector de El Carmen.....	33
Figura 1. 26. Funcionamiento de los Centros de Cableado de Artes, Archivo Histórico y Casa Caldas del Sector de El Carmen.....	34
Figura 1. 27. Funcionamiento del Sector de Santo Domingo.....	36
Figura 1. 28. Funcionamiento de los Centros de Cableado 1,2, 3, 4, 5, y 6 del Sector de Santo Domingo.....	37
Figura 1. 29. Funcionamiento del Sector de la Vicerrectoría de Investigaciones (VRI).....	39
Figura 1. 30. Funcionamiento de los Centros de Cableado 1, 2, 3 y 4 del Sector del VRI.....	39
Figura 1. 31. Funcionamiento del Sector de Las Guacas.....	41
Figura 1. 32. Funcionamiento de los Centros de Cableado 1 y 2 del sector de las Guacas.....	41
Figura 2. 1. Modelo de red para cálculo del retardo del viaje de ida y vuelta.....	53
Figura 2. 2. Modelo de red para cálculo del encogimiento del espaciamiento entre tramas.....	54
Figura 3. 1. Niveles de tráfico del acceso a Internet a través del canal de TELECOM.....	68
Figura 3. 2. Niveles de tráfico del acceso a Internet a través del canal 1 de EMTEL.....	69
Figura 3. 3. Niveles de tráfico del acceso a Internet a través del canal 2 de EMTEL.....	70
Figura 3. 4. Niveles de utilización del RAS durante un año.....	71
Figura 3. 5. Niveles de utilización del RAS durante una semana.....	72
Figura 3. 6. Niveles de utilización del RAS durante un día.....	72
Figura 3. 7 Eventos generados en el enlace SWITCH ACCELAR 1200 - ROUTER CISCO 3600.....	74
Figura 3. 8. Eventos generados en el enlace SWITCH ACCELAR 1200 - ROUTER CISCO 1700.....	75
Figura 3. 9. Eventos generados en el enlace IPET - INGENIERIAS.....	76
Figura 3. 10. Eventos generados en el enlace IPET - EDUCACION.....	77
Figura 3. 11. Eventos generados en el enlace IPET - EL CARMEN.....	77
Figura 3. 12. Eventos generados en el enlace IPET - SANTO DOMINGO.....	78
Figura 3. 13. Eventos generados en el enlace VRI - EL CARMEN.....	79
Figura 3. 14. Eventos generados en el enlace IPET – MEDICINA.....	79
Figura 3. 15. Niveles de utilización del segmento INGCC1SW1-INGCC3HUB3.....	83
Figura 3. 16. Niveles de utilización del segmento INGCC1SW1-INGCC2HUB1.....	84
Figura 3. 17. Niveles de utilización del segmento EDUCC1SW1-EDUCC1SW3.....	86
Figura 3. 18. Eventos generados en el segmento EDUCC1SW1-EDUCC1SW3.....	87
Figura 3. 19. Porcentaje de Utilización del segmento EDUCC1SW2 - EDUCC5HUB1.....	88

Figura 3. 20. Niveles de utilización del segmento VRICC1SW1- VRICC1HUB3....	94
Figura 3. 21. Porcentaje de Utilización del segmento VRICC1SW1 - VRICC1HUB2.....	95
Figura 3. 22. Porcentaje de Utilización del segmento MEDCC1SW1 – MEDCC2HUB1.....	96
Figura 4. 1. Especificación de capas de Gigabit Ethernet.....	106
Figura 4. 2. Elementos funcionales de Gigabit Ethernet.....	107
Figura 4. 3. Elementos funcionales de 10GBE.....	109
Figura 4. 4. Uso de 10 Gigabit Ethernet en ambientes LAN expandidos.....	113
Figura 4. 5. Formato de cabecera IPv4.....	114
Figura 4. 6. Formato de cabecera IPv6.....	116
Figura 4. 7. Dirección unicast global agregable.....	118
Figura 4. 8. Dirección local de enlace.....	119
Figura 4. 9. Dirección local de sitio.....	119
Figura 4. 10. Formato de la dirección Subnet Router Anycast.....	120
Figura 4. 11. Formato de una dirección multicast.....	121
Figura 4. 12. Formato de los mensajes ICMPv6.....	122
Figura 4. 13. Dual Stack, protocolos IPv4 e IPv6.....	129
Figura 4. 14. Tunneling IPv6 sobre IPv4.....	130
Figura 4. 15. Formato de la dirección 6to4.....	130
Figura 4. 16. Formato de una dirección ISATAP.....	131
Figura 4. 17. Funcionamiento de un NAPT.....	132
Figura 5. 1. Modelo de Diseño de red jerárquico.....	142
Figura 5. 2. Opción de diseño No. 1 para el backbone con tecnología Gigabit Ethernet y nodo de acceso WAN en el IPET.....	160
Figura 5. 3. Opción de diseño No. 2 para el backbone con tecnología Gigabit Ethernet y nodo de acceso WAN en el IPET.....	161
Figura 5. 4. Opción de diseño No. 1 para el backbone con tecnología Gigabit Ethernet y nodo de acceso WAN en El Carmen.....	164
Figura 5. 5. Opción de diseño No. 2 para el backbone con tecnología Gigabit Ethernet y nodo de acceso WAN en El Carmen.....	165
Figura 5. 6. Opción de diseño No. 1 Para el Sector de Ingenierías.....	169
Figura 5. 7. Opción de diseño No. 2 Para el Sector de Ingenierías.....	170
Figura 5. 8. Opción de diseño para el sector de ingenierías (IPET y FISICA).....	172
Figura 5. 9. Opción de diseño No. 1 para el Sector de Educación.....	174
Figura 5. 10. Opción de diseño No. 2 para el Sector de Educación.....	175
Figura 5. 11. Opción de diseño No. 1 para el Sector de El Carmen.....	177
Figura 5. 12. Opción de diseño No. 2 para el Sector de El Carmen.....	178
Figura 5. 13. Opción de diseño No. 1 para el Sector de Santo Domingo.....	181
Figura 5. 14. Opción de diseño No. 2 para el Sector de Santo Domingo.....	182
Figura 5. 15. Opción de diseño No. 1 para el Sector del VRI.....	184

Figura 5. 16. Opción de diseño No. 2 para el Sector del VRI.....	184
Figura 5. 17. Opción de diseño No. 1 para el Sector de Medicina.....	186
Figura 5. 18. Opción de diseño No. 2 para el Sector de Medicina.....	186
Figura 5. 19. Opción de diseño No. 1 para el backbone con tecnología 10 Gigabit Ethernet.....	189
Figura 5. 20. Opción de diseño No. 2 para el backbone con tecnología 10 Gigabit Ethernet.....	190
Figura 5. 21. Enlace switch a switch – antes de la actualización.....	197
Figura 5. 22. Enlace switch a switch – después de la actualización.....	197
Figura 5. 23. Enlace switch a servidor – antes de la actualización.....	198
Figura 5. 24. Enlace switch a servidor – después de la actualización.....	199
Figura 5. 25. Segmentos Fast Ethernet – antes de la actualización.....	200
Figura 5. 26. Segmentos Fast Ethernet – después de la actualización.....	200
Figura 5. 27. Conexiones a grupos de trabajo de alto desempeño – antes de la actualización.....	201
Figura 5. 28. Conexiones a grupos de trabajo de alto desempeño – después de la actualización.....	201
Figura 6. 1. Formato de la trama Ethernet.....	208
Figura 6. 2. Dirección IEEE 802 de 48 bits.....	209
Figura 6. 3. Dirección EUI-64.....	210
Figura 6. 4. Conversión de una dirección IEEE 802 en una dirección EUI-64.....	211
Figura 6. 5. Conversión de una dirección EUI-64 unicast administrada universalmente en un identificador de interfaz de IPv6.....	211
Figura 6. 6. Conversión de una dirección IEEE 802 unicast administrada universalmente en identificador de interfaz de IPv6.....	212
Figura 6. 7. Dirección de nivel de enlace IPv6.....	213
Figura 6. 8. Asignación de una dirección multicast IPv6 a una dirección MAC multicast Ethernet.....	214
Figura 6. 9. Ejemplo de Red paralela IPv6.....	216
Figura 6. 10. Ejemplo de Red con Pila Dual.....	217
Figura 6. 11. Estructura de direccionamiento IPv6 para UniCauca.....	218
Figura 6. 12. Topología de túneles estáticos entre los sitios UniCauca IPv6 y UNAM IPv6.....	220
Figura 6. 13. Topología final de la arquitectura de red IPv6.....	222

1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

En este capítulo se presenta de manera detallada la infraestructura actual de la Red de Datos de la Universidad del Cauca, describiendo la estructura física y el funcionamiento lógico de ésta, además de los servicios soportados.

1.1 DESCRIPCIÓN FÍSICA.

La Red de Datos de la Universidad del Cauca tiene una estructura física la cual se basa en un campus universitario dividido por sectores:

- Sector de Ingenierías
- Sector de Medicina
- Sector de Educación
- Sector de El Carmen
- Sector de Santo Domingo
- Sector de Vicerrectoría de Investigaciones
- Sector de Las Guacas
- Sector de Santander de Quilichao

En cada sector se encuentran uno o más edificios, los cuales se conectan entre sí por un backbone de fibra óptica multimodo, el cual posee físicamente una topología de doble estrella, que tienen como centro de esas estrellas los edificios del Instituto de Postgrados (IPET) y El Carmen, como se muestra en la Figura 1.1. Además existen otros sectores tales como Alfonso López y Consultorio jurídico en los cuales la densidad de equipos es muy baja.

La conexión con el sector de Santander de Quilichao se realiza a través de la Red Metropolitana de Emtel, conectándose a la Red Nacional de Fibra Óptica para llegar hasta el nodo ubicado en la ciudad de Cali. Desde este nodo se realiza una conexión por medio de un radio-enlace hacia la sede ubicada en Santander de Quilichao.

Actualmente, el acceso WAN o acceso a Internet se realiza a través de los proveedores de servicio de Internet *Telecom* y *Emtel*. La conexión con Telecom se realiza a través de un Modem HDSL a 2 Mbps; la conexión con Emtel se realiza por Fibra Óptica a través de su Red Metropolitana a 4 Mbps.

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

El acceso remoto o acceso telefónico se realiza por medio de un enlace primario (PRI – Primary Rate Interface) de la Red Digital de Servicios Integrados (Integrated Service Digital Network – ISDN) para 30 canales (los cuales permiten una velocidad máxima de 56 Kbps si el usuario se conecta a través de una línea telefónica analógica; 64 Kbps cuando el usuario tiene el servicio ISDN; y 128 Kbps cuando tiene el servicio ISDN y utiliza los 2 canales B); enlace provisto por la empresa Emtel.

La infraestructura física dentro de cada sector del campus universitario y específicamente dentro de cada edificio posee un cableado estructurado certificado utilizando par trenzado no-apantallado (Unshielded Twisted Pair - UTP) Categoría 5 o superior, teniendo por lo menos un centro de cableado (o rack) en cada edificio y sus respectivos puntos de red que se extienden hasta los puestos de trabajo dentro de ese edificio. En grandes edificios donde las limitaciones de distancia del Cableado Estructurado no permiten que un solo centro de cableado recoja todos los puntos de red, se tienen centros de cableado secundarios que recogen esos puntos de red distantes; y que a su vez se conectan al centro de cableado principal (generalmente conocido como centro de cableado 1, CC1) a través de un número de cables UTP, número determinado por el tamaño en puntos de red de los centros de cableado secundarios.

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

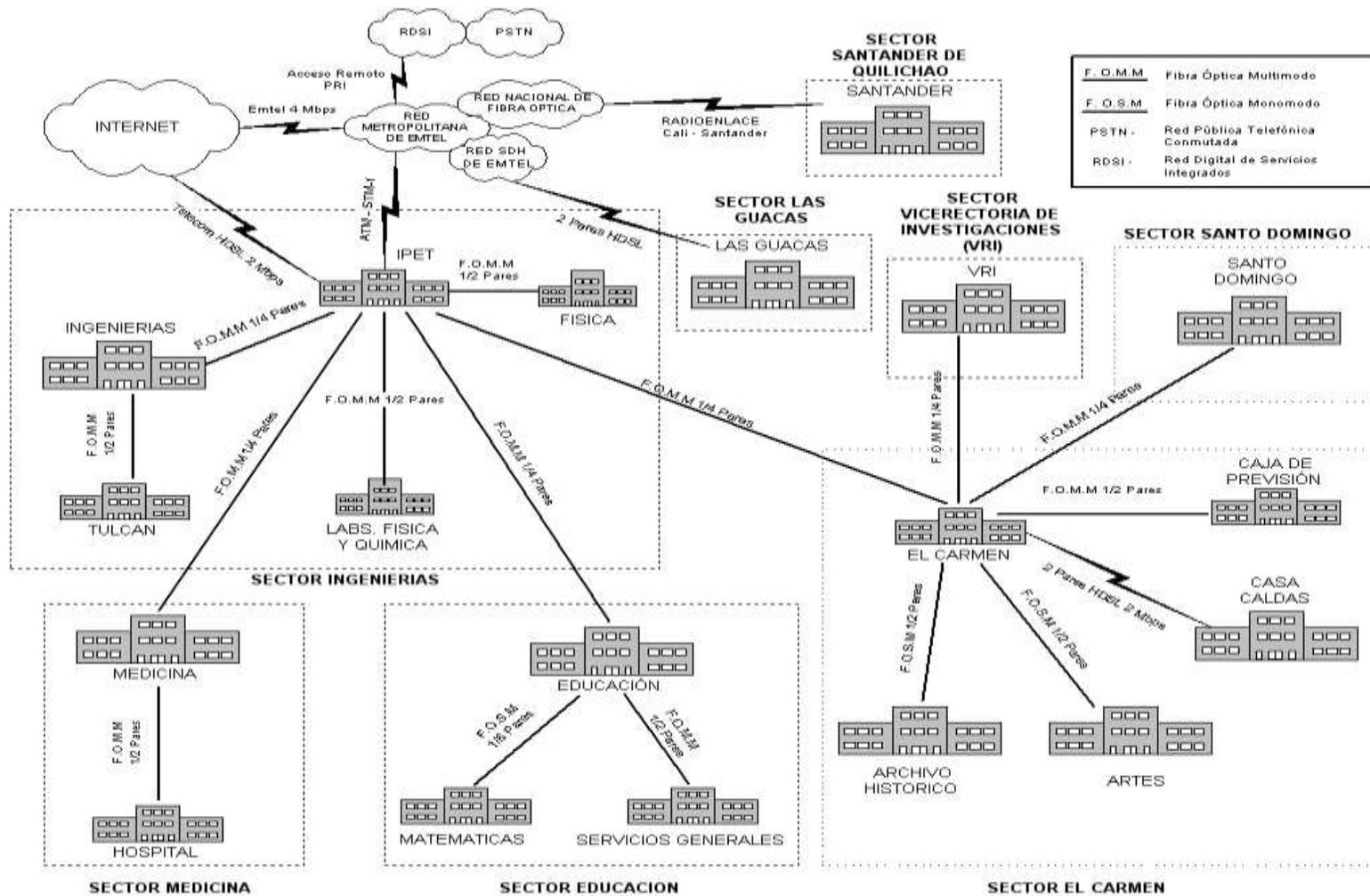


Figura 1. 1. Cableado de la Red de Datos de la Universidad del Cauca.

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

1.1.1 CABLEADO DEL SECTOR DE INGENIERÍAS.

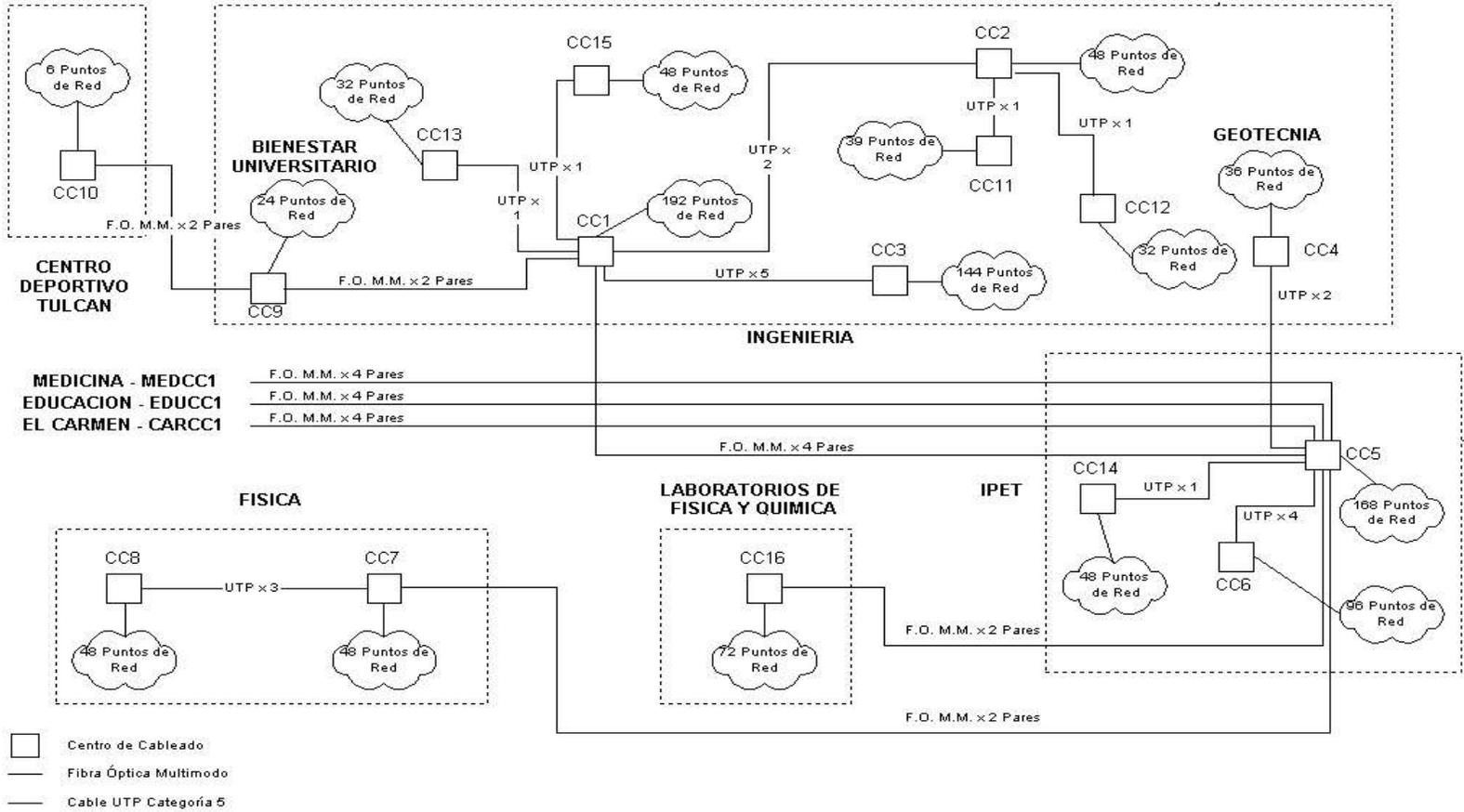


Figura 1. 2. Cableado Estructurado del Sector de Ingenierías.

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

La Tabla 1.1 resume la cantidad de puntos de red del Sector de Ingenierías.

CENTRO DE CABLEADO	NÚMERO DE PUNTOS DE RED	UBICACIÓN FÍSICA
CC1	192	Edificio Ingenierías - Oficina 425
CC2	48	Edificio Ingenierías - Decanatura Ingeniería Electrónica
CC3	144	Edificio Ingenierías - Salón Modelo de Transmisión
CC4	36	Edificio Ingenierías - Geotecnia
CC5	168	Edificio IPET - Administración Red de Datos
CC6	96	Edificio IPET - Salón 105
CC7	48	Edificio Física – Sala de Sistemas Ing. Física
CC8	48	Edificio Física – Departamento de Física
CC9	24	Bienestar Universitario - Enfermería
CC10	6	Centro Deportivo Universitario Tulcán
CC11	39	Edificio Ingenierías - Sala I de Informática
CC12	32	Edificio Ingenierías - Sala II de Informática
CC13	32	Edificio Ingenierías - Sala de Automática
CC14	48	Edificio IPET - Help Desk
CC15	48	Edificio Ingenierías
CC16	72	Edificio Laboratorios Física y Química
PUNTOS DE RED TOTALES	1081	

Tabla 1. 1. Resumen Puntos de Red del Sector de Ingenierías.

1.1.2 CABLEADO DEL SECTOR DE MEDICINA.

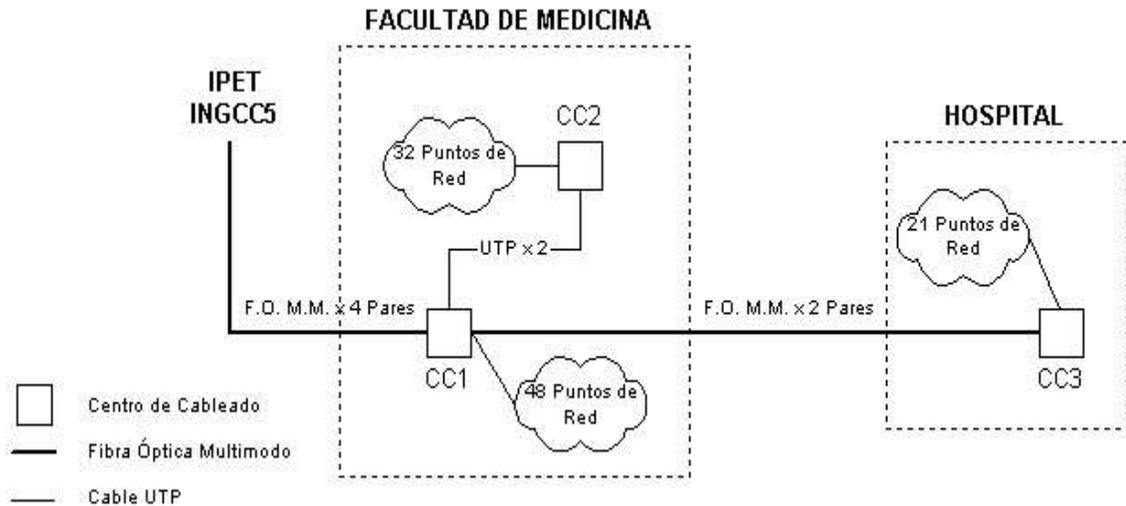


Figura 1. 3. Cableado Estructurado del Sector de Medicina.

La Tabla 1.2 resume la cantidad de puntos de red del Sector de Medicina.

CENTRO DE CABLEADO	NÚMERO DE PUNTOS DE RED	UBICACIÓN FÍSICA
CC1	48	Facultad de Medicina - Biblioteca
CC2	32	Facultad de Medicina - Tercer Piso
CC3	21	Hospital Universitario San José – Tercer Piso
PUNTOS DE RED TOTALES	101	

Tabla 1. 2. Resumen Puntos de Red del Sector de Medicina.

1.1.3 CABLEADO DEL SECTOR DE EDUCACIÓN.

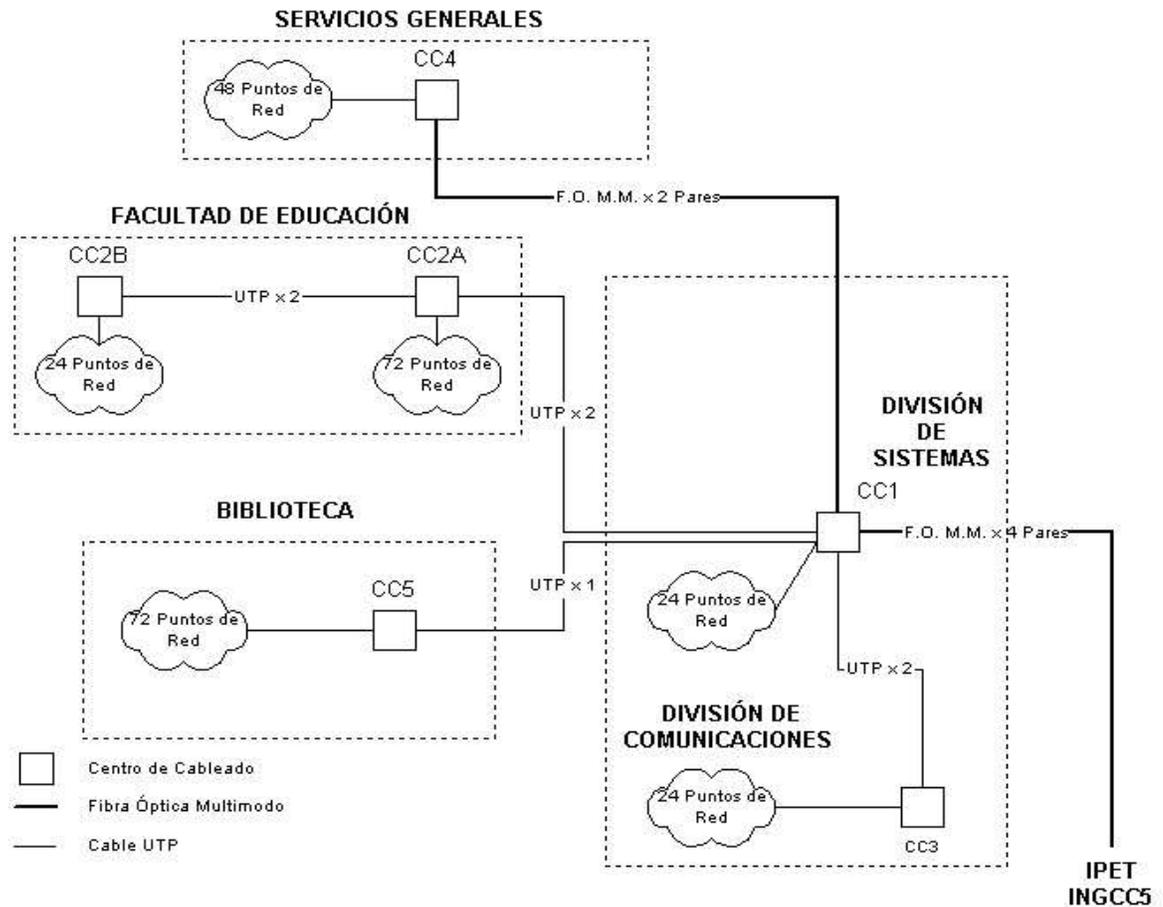


Figura 1. 4. Cableado Estructurado del Sector de Educación.

CENTRO DE CABLEADO	NÚMERO DE PUNTOS DE RED	UBICACIÓN FÍSICA
CC1	24	División de Sistemas
CC2A	72	Edificio Facultad de Educación
CC2B	24	Edificio Facultad de Educación
CC3	24	División de Comunicaciones
CC4	48	Edificio Servicios Generales
CC5	72	Biblioteca
PUNTOS DE RED TOTALES	264	

Tabla 1. 3. Resumen Puntos de Red del Sector de Educación.

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

1.1.4 CABLEADO DEL SECTOR DE EL CARMEN.

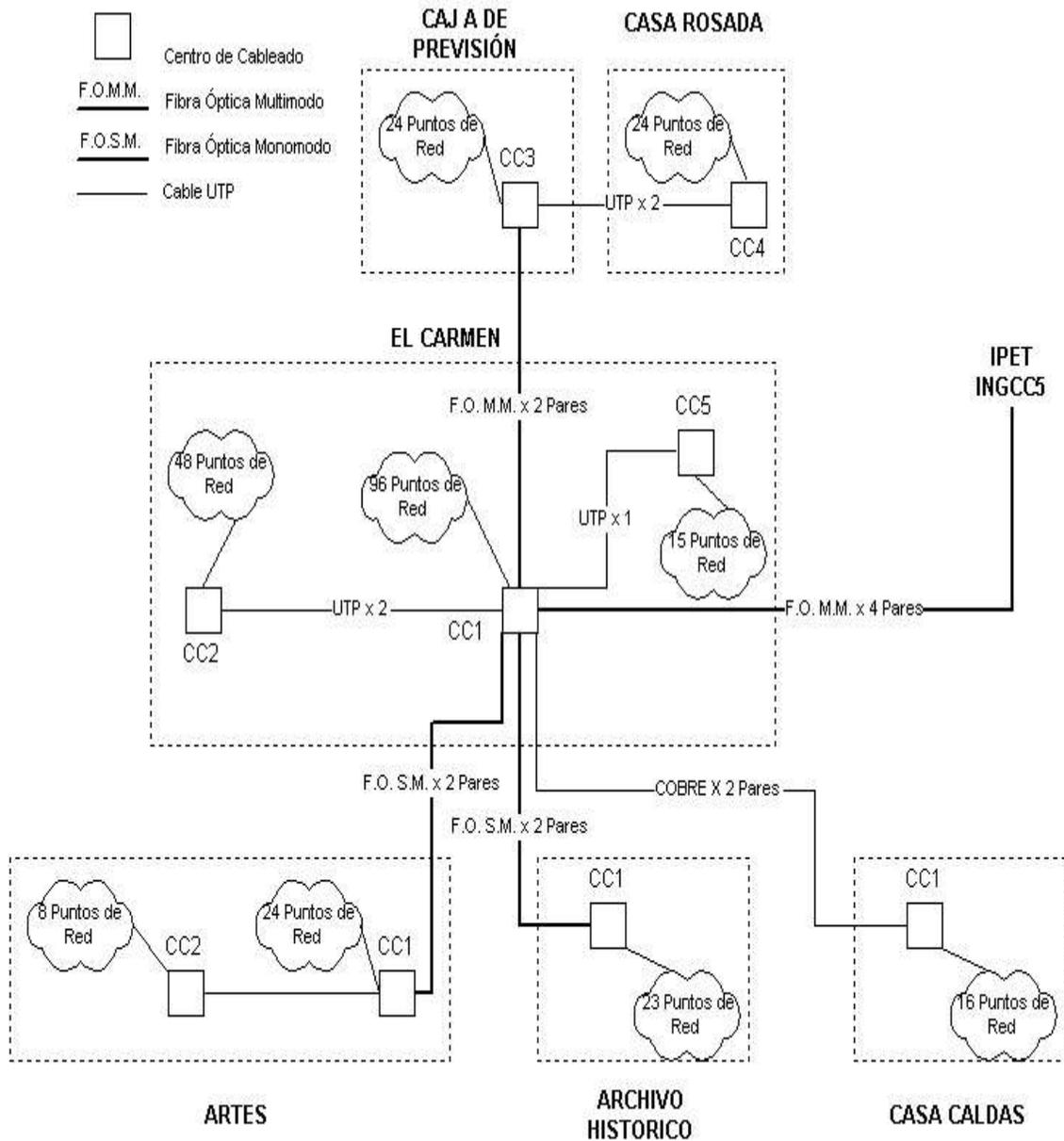


Figura 1. 5. Cableado Estructurado del Sector de El Carmen.

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

CENTRO DE CABLEADO	NÚMERO DE PUNTOS DE RED	UBICACIÓN FÍSICA
CC1	96	Edificio El Carmen
CC2	48	Edificio El Carmen - Oficina 112
CC3	24	Caja de Previsión de la Universidad
CC4	24	Casa Rosada
CC5	15	Edificio El Carmen - Biblioteca
PUNTOS DE RED TOTALES	207	

Tabla 1. 4. Resumen Puntos de Red del Sector de El Carmen.

CENTRO DE CABLEADO	NÚMERO DE PUNTOS DE RED	UBICACIÓN FÍSICA
CC1	24	Edificio Artes - Sala de diseño
CC2	8	Edificio Artes - Sala de informática
PUNTOS DE RED TOTALES	32	

Tabla 1. 5. Resumen Puntos de Red del Sector de Artes.

CENTRO DE CABLEADO	NÚMERO DE PUNTOS DE RED	UBICACIÓN FÍSICA
CC1	24	Edificio Archivo Histórico
PUNTOS DE RED TOTALES	24	

Tabla 1. 6. Resumen Puntos de Red del Sector Archivo Histórico.

CENTRO DE CABLEADO	NÚMERO DE PUNTOS DE RED	UBICACIÓN FÍSICA
CC1	16	Edificio Casa Caldas

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

PUNTOS DE RED TOTALES	16	
------------------------------	-----------	--

Tabla 1. 7. Resumen Puntos de Red del Sector Casa Caldas.

1.1.5 CABLEADO DEL SECTOR DE SANTO DOMINGO.

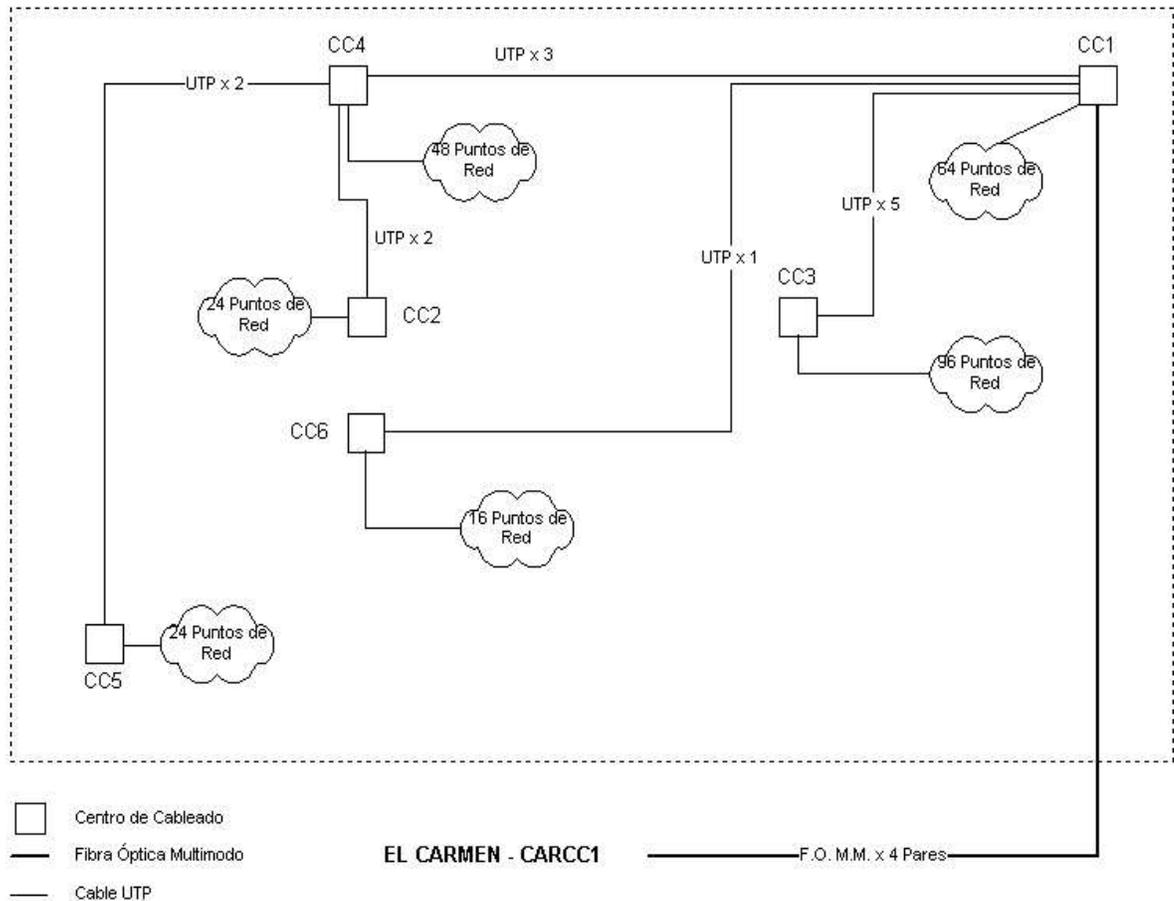


Figura 1. 6. Cableado Estructurado del Sector de Santo Domingo.

CENTRO DE CABLEADO	NÚMERO DE PUNTOS DE RED	UBICACIÓN FÍSICA
CC1	64	Conmutador
CC2	24	Sala de Computo 2
CC3	96	Oficina Personal

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

CC4	48	Sala de Computo 1
CC5	24	Sala de Profesores
CC6	16	Sala de Informática
PUNTOS DE RED TOTALES	272	

Tabla 1. 8. Resumen Puntos de Red del Sector de Santo Domingo.

1.1.6 CABLEADO DEL SECTOR DE VICERRECTORÍA DE INVESTIGACIONES.

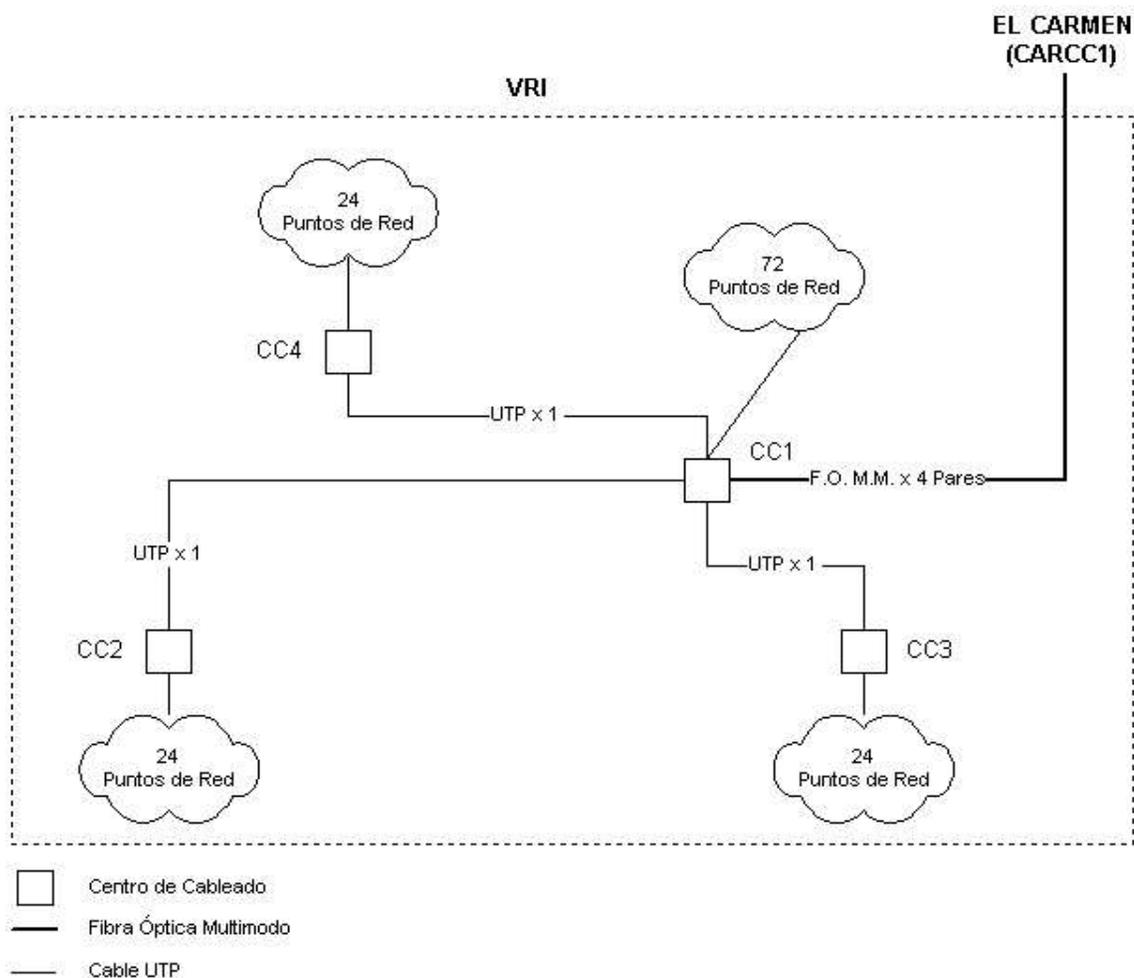


Figura 1. 7. Cableado Estructurado del Sector de la Vicerrectoría de Investigaciones (VRI).

CENTRO DE CABLEADO	NÚMERO DE PUNTOS DE RED	UBICACIÓN FÍSICA
--------------------	-------------------------	------------------

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

CC1	72	Oficina 204
CC2	24	Oficina 212
CC3	24	Oficina 208
CC4	24	Oficina 310
PUNTOS DE RED TOTALES	144	

Tabla 1. 9. Resumen Puntos de Red del Sector de la Vicerrectoría de Investigaciones (VRI).

1.1.7 CABLEADO DEL SECTOR DE LAS GUACAS.

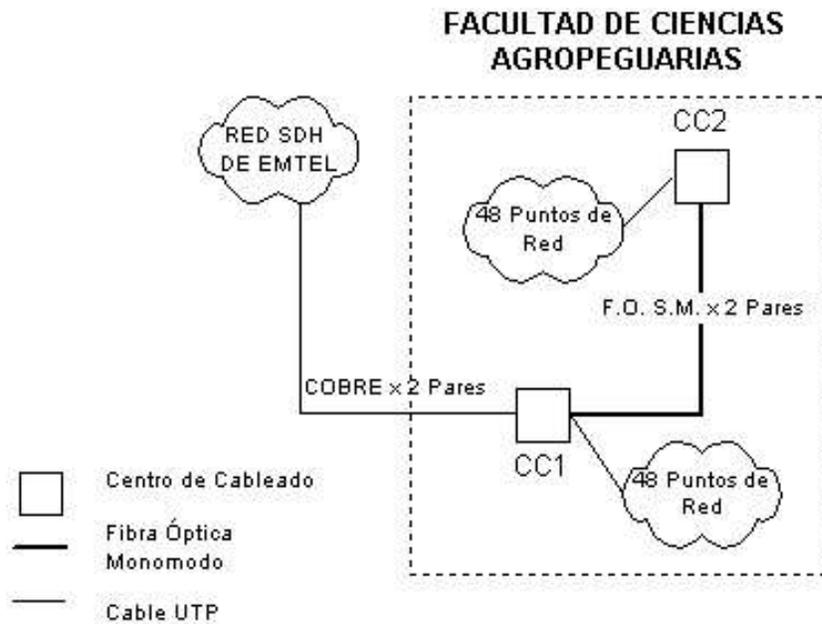


Figura 1. 8. Cableado Estructurado del Sector de Las Guacas

CENTRO DE CABLEADO	NÚMERO DE PUNTOS DE RED	UBICACIÓN FÍSICA
CC1	48	Sala de Profesores
CC2	48	Sala de Informática
PUNTOS DE RED TOTALES	96	

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

Tabla 1. 10. Resumen Puntos de Red del Sector de Las Guacas

Tomando las anteriores tablas se puede obtener la cantidad de puntos de red por sectores, como se muestra en la siguiente tabla resumen.

SECTOR	NÚMERO DE PUNTOS DE RED
Ingenierías	1081
Medicina	101
Educación	264
El Carmen	207
Artes	32
Archivo Histórico	24
Casa Caldas	16
Santo Domingo	272
VRI	144
Las Guacas	96
PUNTOS DE RED TOTALES	2237

Tabla 1. 11. Resumen Puntos de Red Totales.

1.2 DESCRIPCIÓN DEL FUNCIONAMIENTO LÓGICO.

La Red de Datos de la Universidad del Cauca es una red de área local (LAN) que utiliza la tecnología que se describe en el estándar 802.3 de la IEEE, en el cual se habla de una red LAN que tiene un método de acceso al medio denominado Acceso Múltiple por Detección de Portadora con Detección de Colisión (Carrier Sense Multiple Access/Collision Detection - CSMA/CD). De manera esquemática el procedimiento seguido por las estaciones que siguen esta técnica es el siguiente: Antes de transmitir, una estación monitoriza el medio para escuchar si alguna otra

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

estación está transmitiendo. Si se detecta una transmisión, la estación espera un tiempo aleatorio antes de volver a intentar la transmisión, escuchando de nuevo el medio en primer lugar. Si no detecta ninguna transmisión sobre el medio físico, la estación comienza su transmisión. Durante la transmisión de una trama la estación monitoriza el medio continuamente y si no detecta la transmisión de ninguna otra estación, continúa su transmisión hasta completar la trama. Una vez que se completa la transmisión de la trama, la estación espera un intervalo de 9,6 ms (intervalo entre tramas) antes de volver a efectuar ninguna transmisión. Este intervalo se aprovecha para una comprobación.

IEEE 802.3 permite un funcionamiento a 10 Mbps sobre diferentes medios físicos (coaxial, par trenzado, fibra óptica), sin embargo el estándar ha evolucionado permitiendo alcanzar velocidades de 100, 1000 y 10000 Mbps, oficialmente conocidos como IEEE 802.3u, IEEE 802.3z, e IEEE 802.3ae comúnmente llamados Fast-Ethernet, Gigabit-Ethernet y 10 Gigabit-Ethernet respectivamente. Con el desarrollo posterior de los switches nivel 2 (conmutadores) la tecnología IEEE 802.3 basada en CSMA/CD (conocida también como Ethernet compartida) ha superado una de sus limitaciones, al permitir la incorporación de mayores cantidades de hosts a la red sin disminuir su nivel de desempeño, objetivo que se alcanza segmentando la red al tener un segmento diferente en cada uno de los puertos del switch, lo que da origen a la tecnología conocida como Ethernet conmutada.

Para su funcionamiento la Red de Datos cuenta con un backbone en fibra óptica, el cual a pesar de poseer físicamente una topología de doble estrella, lógicamente tiene una topología de una sola estrella centrada en el IPET como se muestra en la Figura 1.8. Aunque físicamente Santo Domingo se conecta al Carmen, lógicamente tiene una conexión directa al IPET ya que se ha “puenteado” la fibra óptica en El Carmen evitando la conmutación de datos en ese punto.

El backbone funciona implementando Fast-Ethernet en forma conmutada a nivel 2, entregando una velocidad de 100 Mbps en cada uno de los enlaces. En cada edificio existe por lo menos un switch Ethernet conectado a dicho backbone a través de su puerto de alta velocidad. Este switch a su vez permite la conexión de la red de acceso constituida por los diferentes hubs Ethernet (los que implementan Ethernet compartido) repartidos entre los centros de cableado principal y secundarios y conectados utilizando el cableado estructurado existente basado en UTP Categoría 5.

El acceso a Internet a través de Telecom utiliza la tecnología HDSL (High-rate Digital Subscriber Line) y se conecta mediante dos pares de cobre dedicados a una velocidad de 2 Mbps; el acceso a Internet a través de Emtel se realiza utilizando Fibra

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

Óptica mediante su Red Metropolitana que funciona con la tecnología ATM conectándose a una velocidad de 4 Mbps.

Para el acceso telefónico se tiene un servidor de acceso remoto (Remote Access Server - RAS) Lucent Max 6000 que atiende un enlace PRI ISDN con 30 canales, contratado con Emtel, y que permite que los usuarios se conecten a una velocidad máxima de 56 Kbps si lo hacen a través de una línea telefónica analógica, o hasta 64 Kbps cuando tienen el servicio ISDN, o hasta 128 Kbps cuando tienen ISDN y utilizan los dos canales B.

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

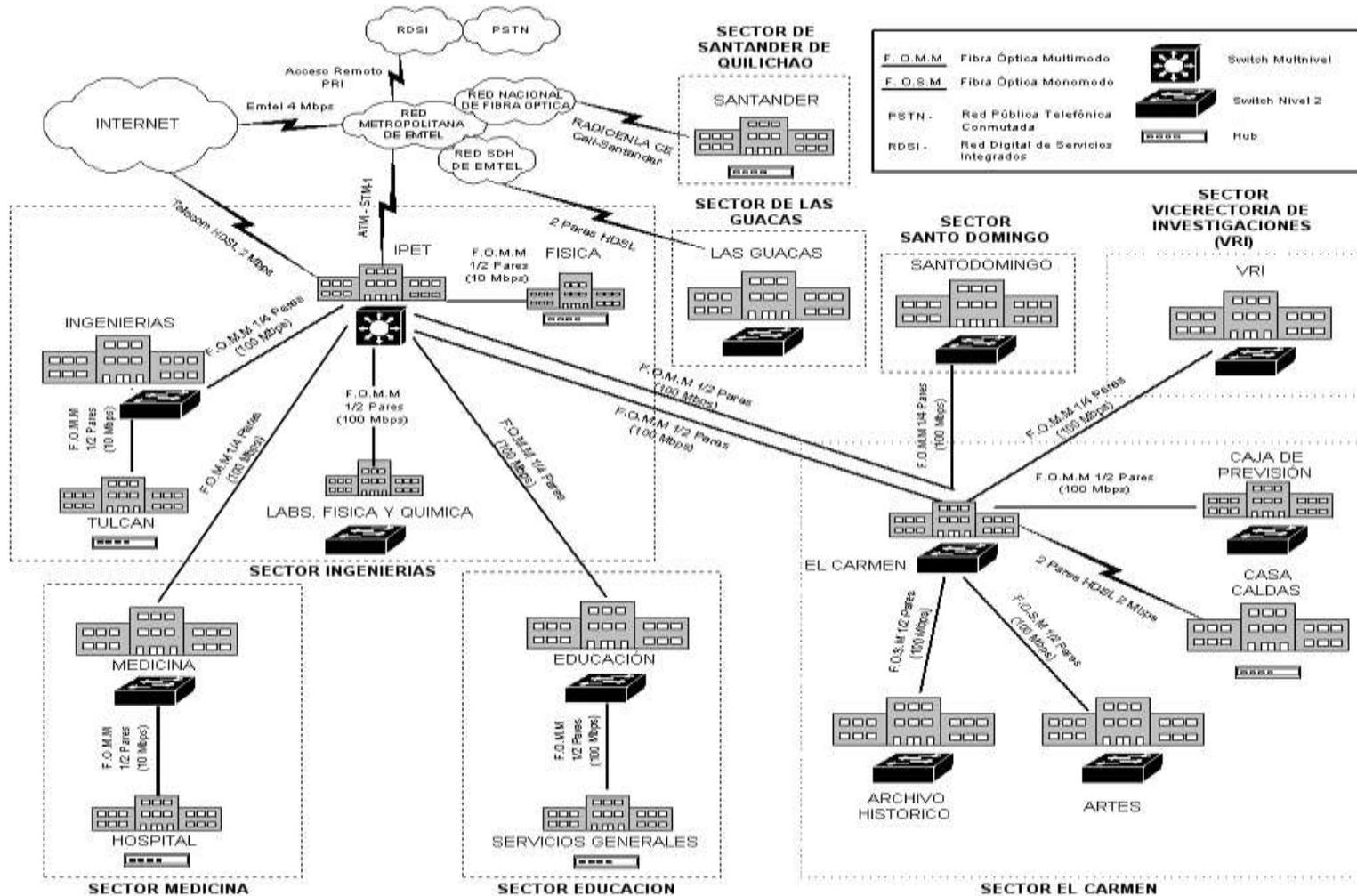


Figura 1. 9. Descripción General del Funcionamiento Lógico de la Red de Datos.

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

En las secciones subsiguientes se realizará una descripción detallada del funcionamiento de cada uno de los sectores. En ellos, los equipos de red son identificados de acuerdo al siguiente código: Sector de la Red – Número de Centro de Cableado – Tipo de Equipo de Red y Número, así por ejemplo un switch en el centro de cableado 4 del Sector de Ingenierías llevará el código IINGCC4SW1, o el cuarto hub del centro de cableado 3 de Santo Domingo será reconocido con base al código STOCC3HUB4. Además se utilizarán las siguientes convenciones.

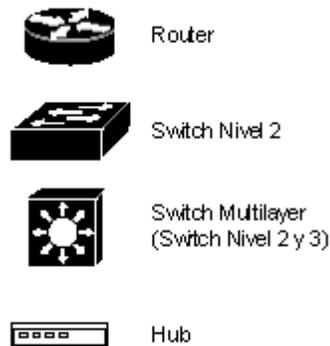


Figura 1. 10 Convenciones

1.2.1 SECTOR DE INGENIERÍAS.

El funcionamiento general del Sector de Ingenierías se muestra en la Figura 1.10. Las nubes de hubs que ahí se indican son detalladas en las figuras subsiguientes.

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

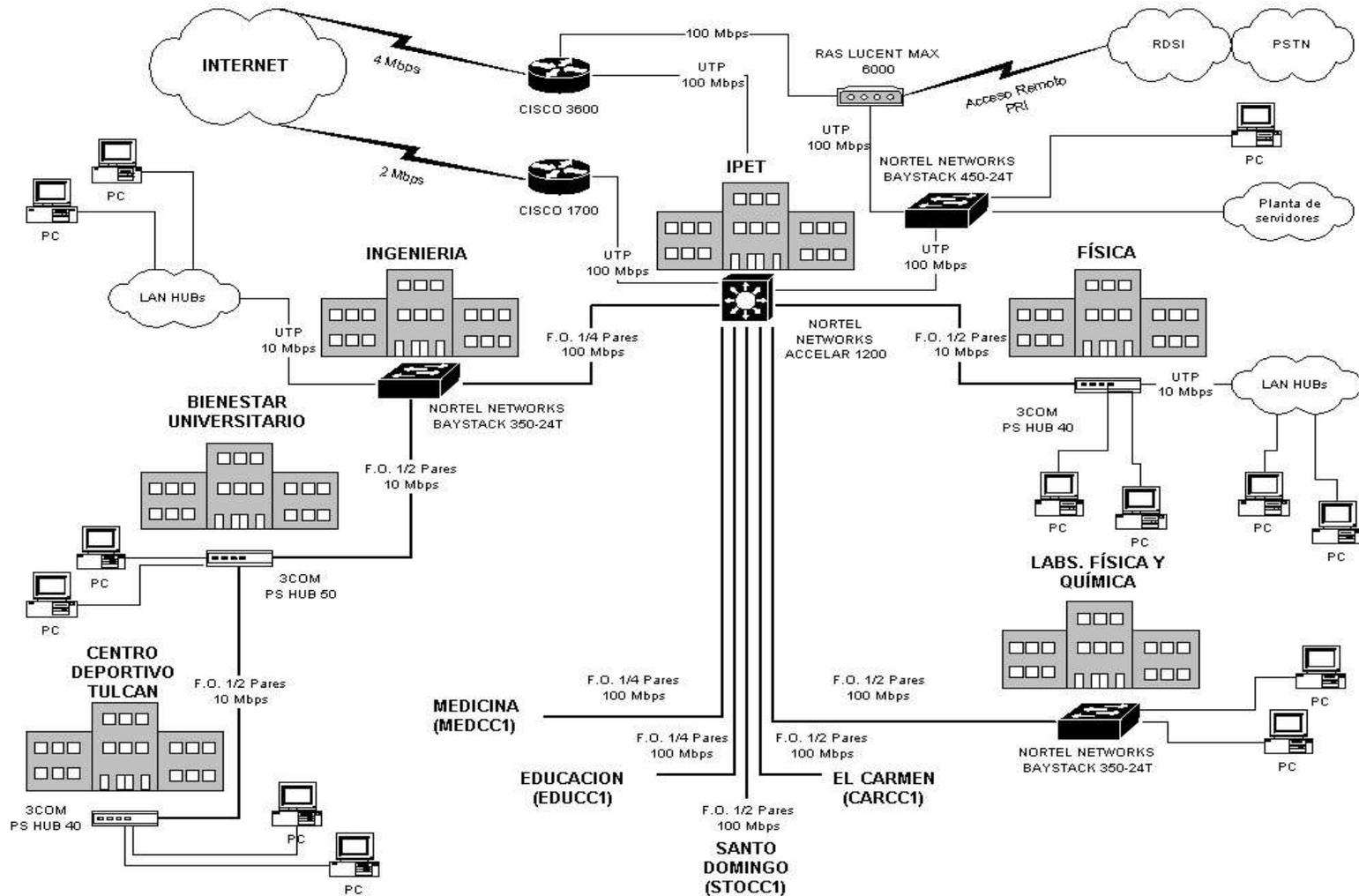


Figura 1. 11. Funcionamiento del Sector de Ingenierías.

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

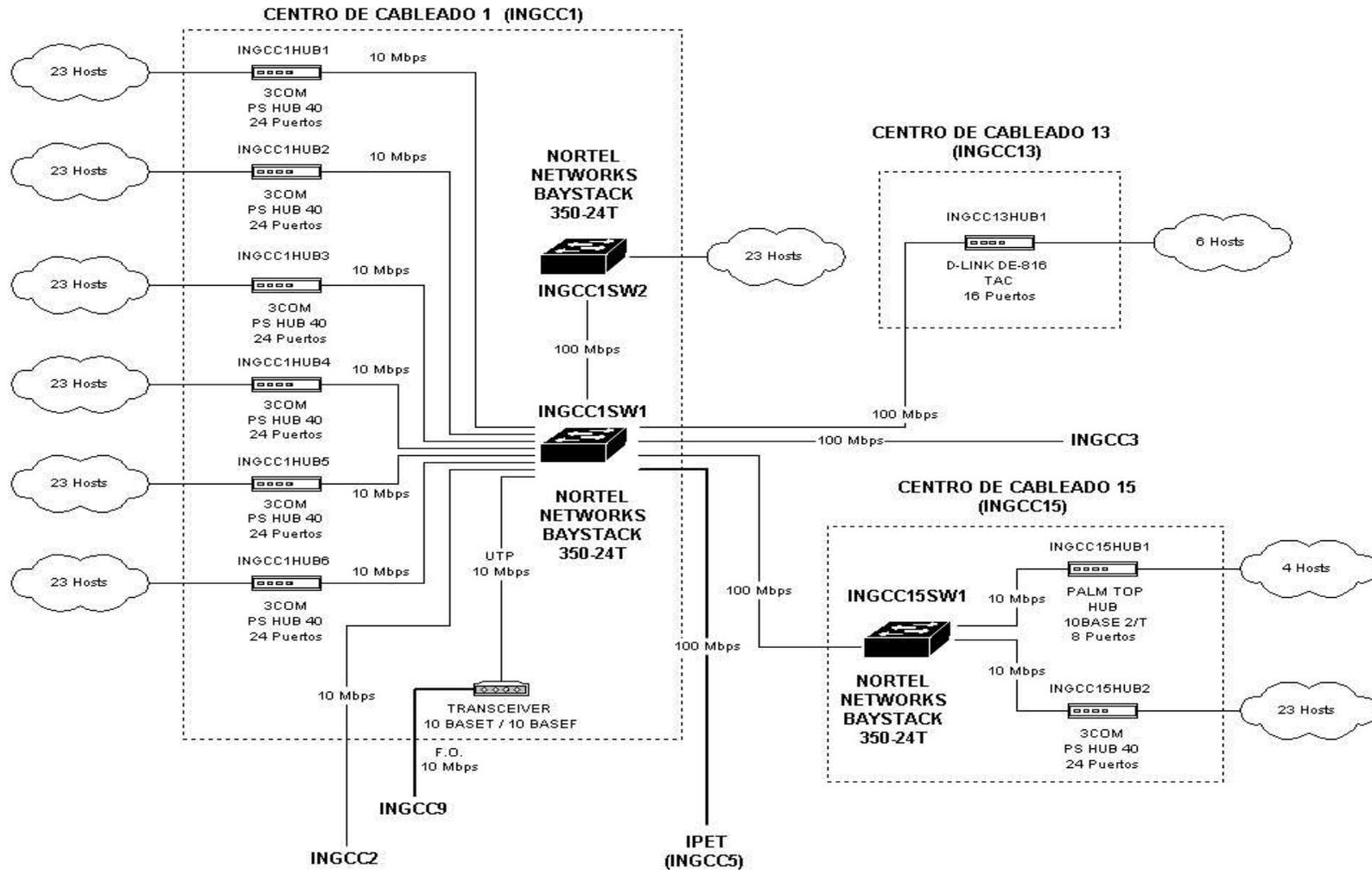


Figura 1. 12. Funcionamiento de los Centros de Cableado 1, 13 y 15 del Sector de Ingenierías.

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

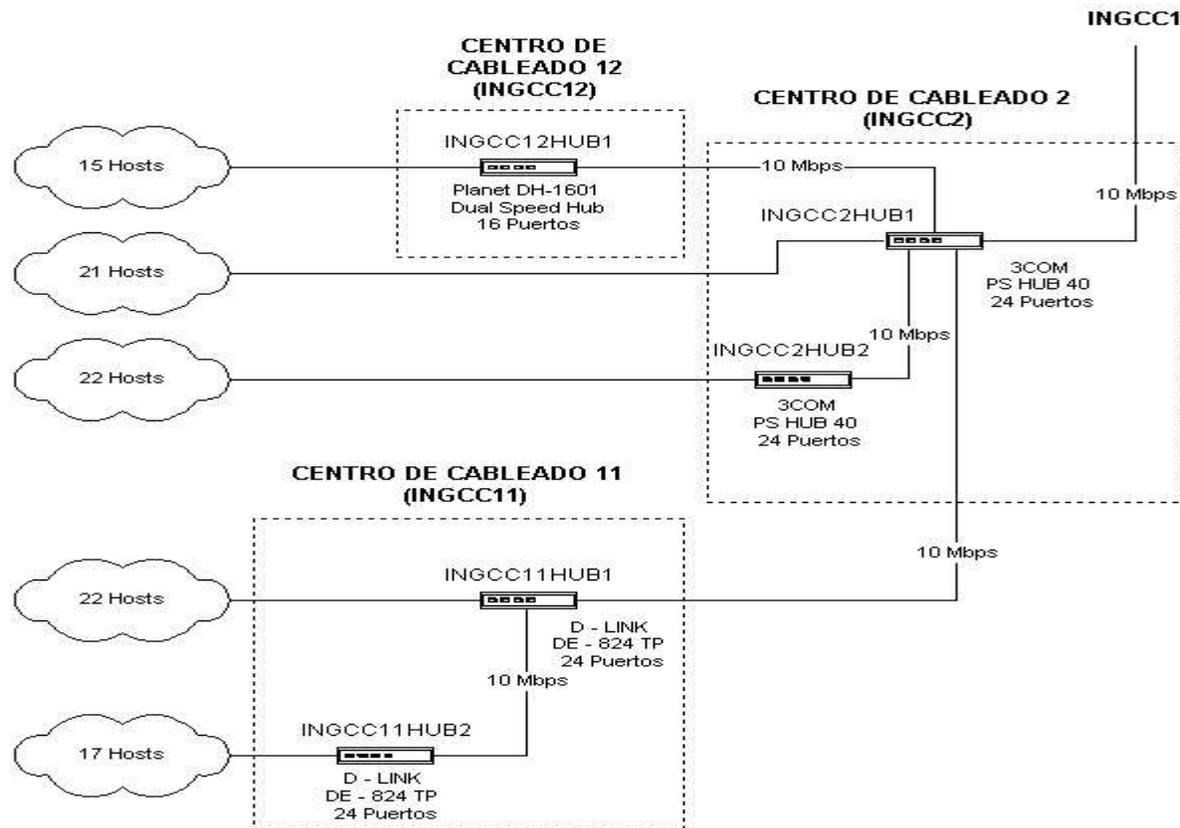


Figura 1. 13. Funcionamiento de los Centros de Cableado 2, 11 y 12 del Sector de Ingenierías.

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

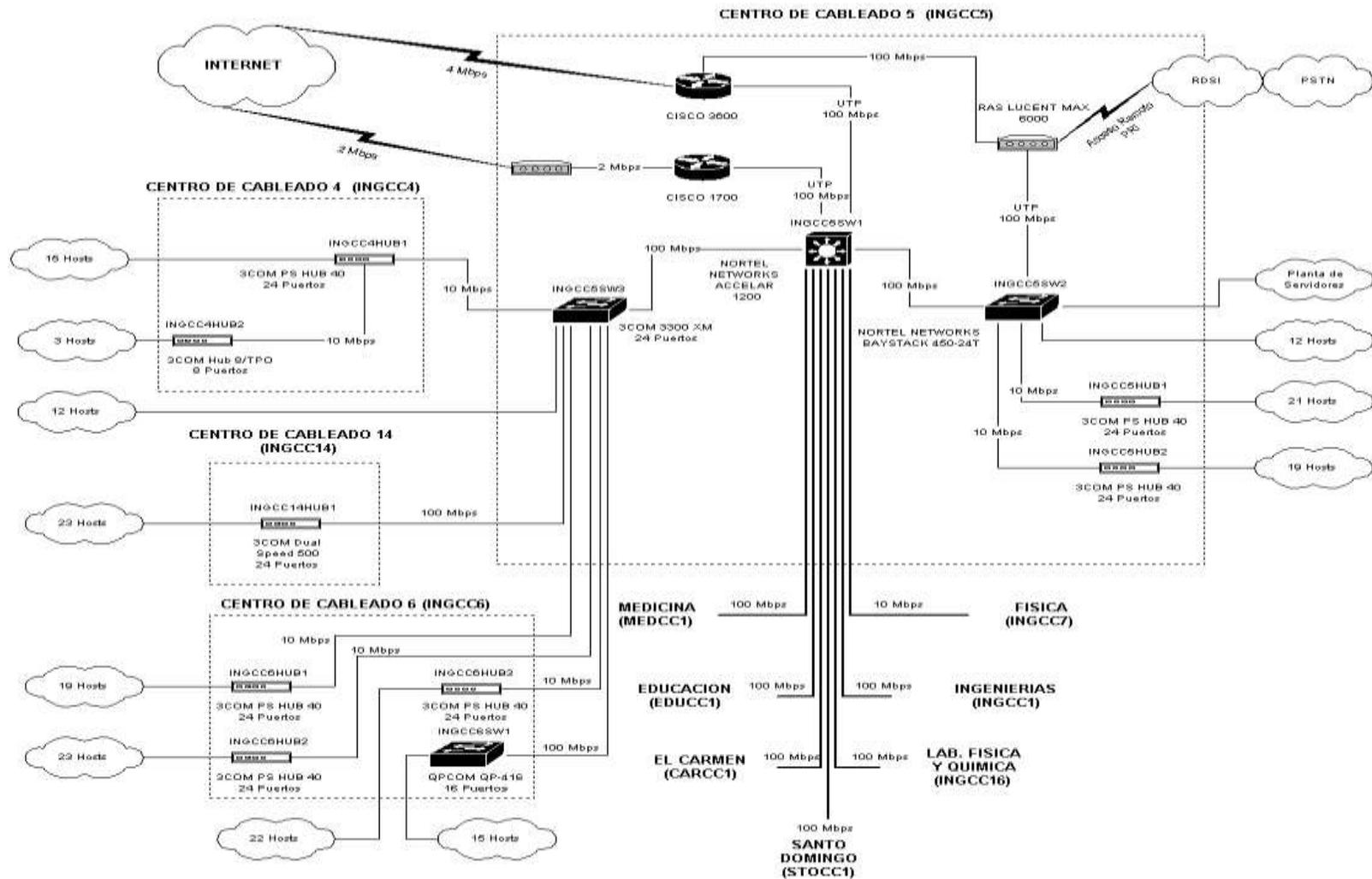


Figura 1. 14. Funcionamiento de los Centros de Cableado 4, 5, 6, y 14 del Sector de Ingenierías.

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

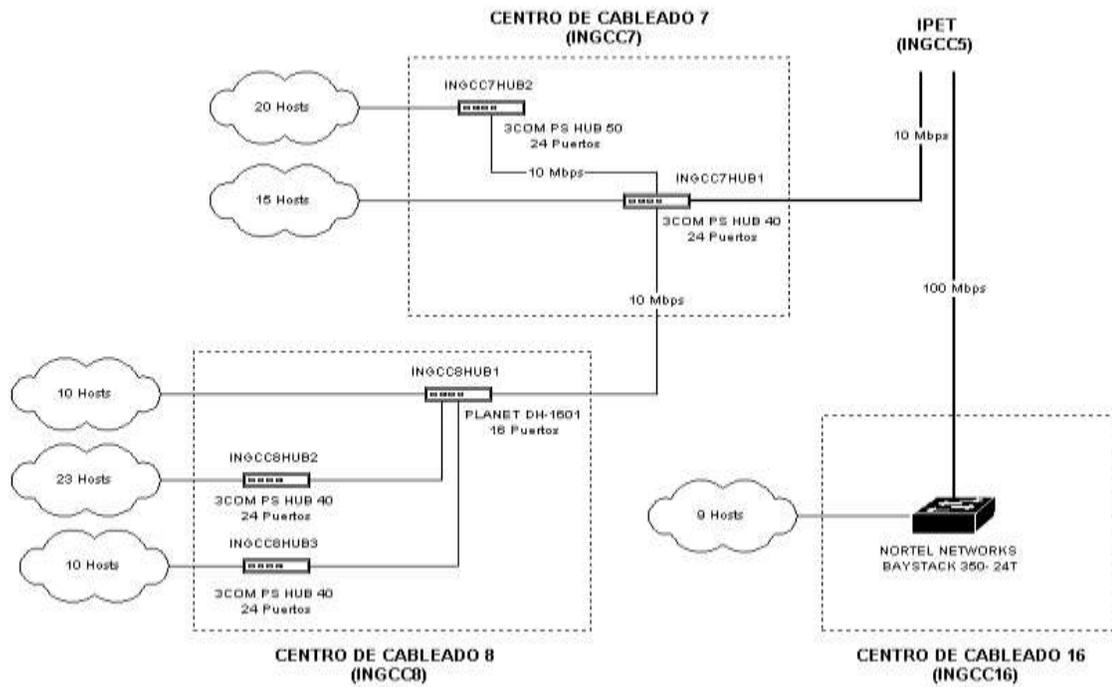


Figura 1. 15. Funcionamiento de los Centros de Cableado 7, 8 y 16 del Sector de Ingenierías.

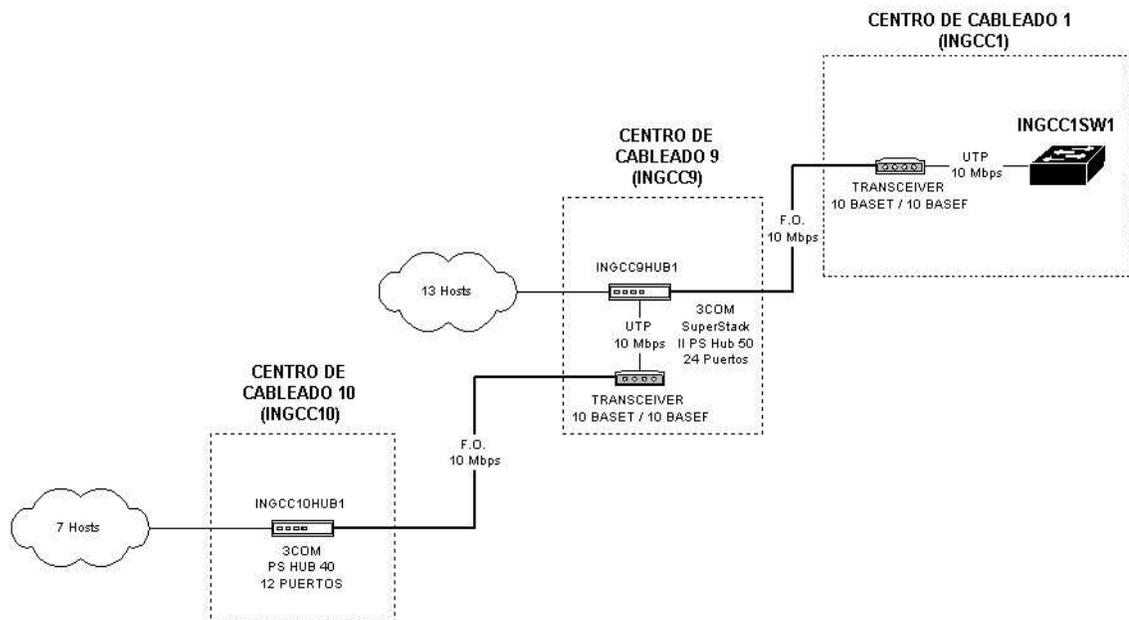


Figura 1. 16. Funcionamiento de los Centros de Cableado 9 y 10 del Sector de Ingenierías.

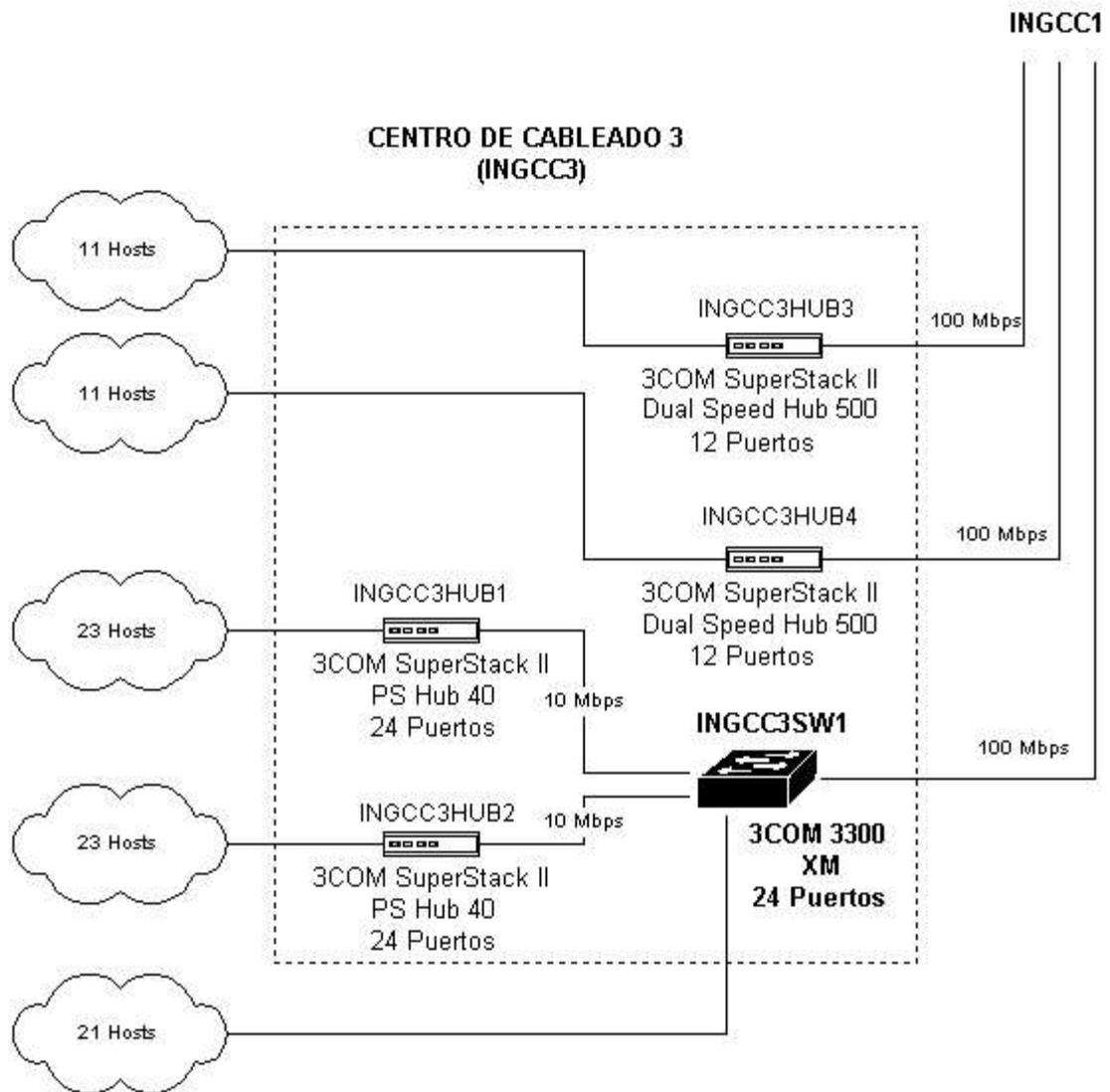


Figura 1. 17. Funcionamiento del Centro de Cableado 3 del Sector de Ingenierías.

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

La Tabla 1.12 resume la distribución de las estaciones de trabajo en los diferentes centros de cableado.

CENTRO CABLEADO	DE	EQUIPOS ACTIVOS	PUERTOS	HOSTS	TOTAL PUERTOS	TOTAL HOSTS
CC1						
		Sw 2	24	23		
		Hub 1	24	23		
		Hub 2	24	23		
		Hub 3	24	23		
		Hub 4	24	23		
		Hub 5	24	23		
		Hub 6	24	23		
TOTAL CC1					168	161
CC2						
		Hub 1	24	21		
		Hub 2	24	22		
TOTAL CC2					48	43
CC3						
		Sw 1	24	21		
		Hub 1	24	23		
		Hub 2	24	23		
		Hub 3	12	11		
		Hub 4	12	11		
TOTAL CC3					96	89
CC4						
		Hub 1	24	15		
		Hub 2	8	3		
TOTAL CC4					32	18
CC5						
		Sw 2	24	12		
		Sw 3	24	12		
		Hub 1	24	21		

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

	Hub 2	24	19		
TOTAL CC5				96	64
CC6					
	Sw 1	16	15		
	Hub 1	24	19		
	Hub 2	24	23		
	Hub 3	24	22		
TOTAL CC6				88	79
CC7					
	Hub 1	24	15		
	Hub 2	24	20		
TOTAL CC7				48	35
CC8					
	Hub 1	16	10		
	Hub 2	24	23		
	Hub 3	24	10		
TOTAL CC8				64	43
CC9					
	Hub 1	24	13		
TOTAL CC9				24	13
CC10					
	Hub 1	12	7		
TOTAL CC10				12	7
CC11					
	HUB1	24	22		
	HUB2	24	17		
TOTAL CC11				48	39
CC12					
	Hub 1	16	15		
TOTAL CC12				16	15

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

CC13					
	Hub 1	16	6		
TOTAL CC13				16	6
CC14					
	Hub 1	24	23		
TOTAL CC14				23	23
CC15					
	Sw 1	24	21		
	Hub 1	8	4		
	Hub 2	24	23		
TOTAL CC15				56	48
CC16					
	Sw 1	24	9		
TOTAL CC16				24	9
TOTALES DEL SECTOR				859	692

Tabla 1. 12. Distribución de Hosts del Sector de Ingenierías.

1.2.2 SECTOR DE MEDICINA.

El funcionamiento general del Sector de Medicina se muestra en la Figura 1.18. Las nubes de hubs que ahí se indican son detalladas en la Figura 1.19.

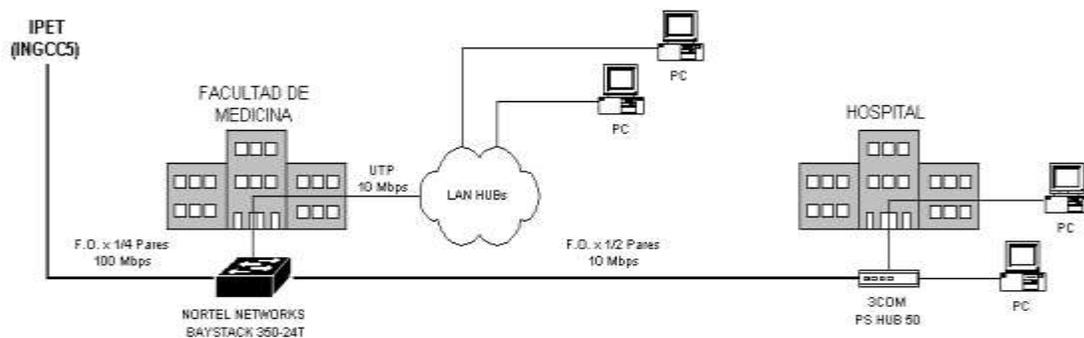


Figura 1. 18. Funcionamiento del Sector de Medicina.

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

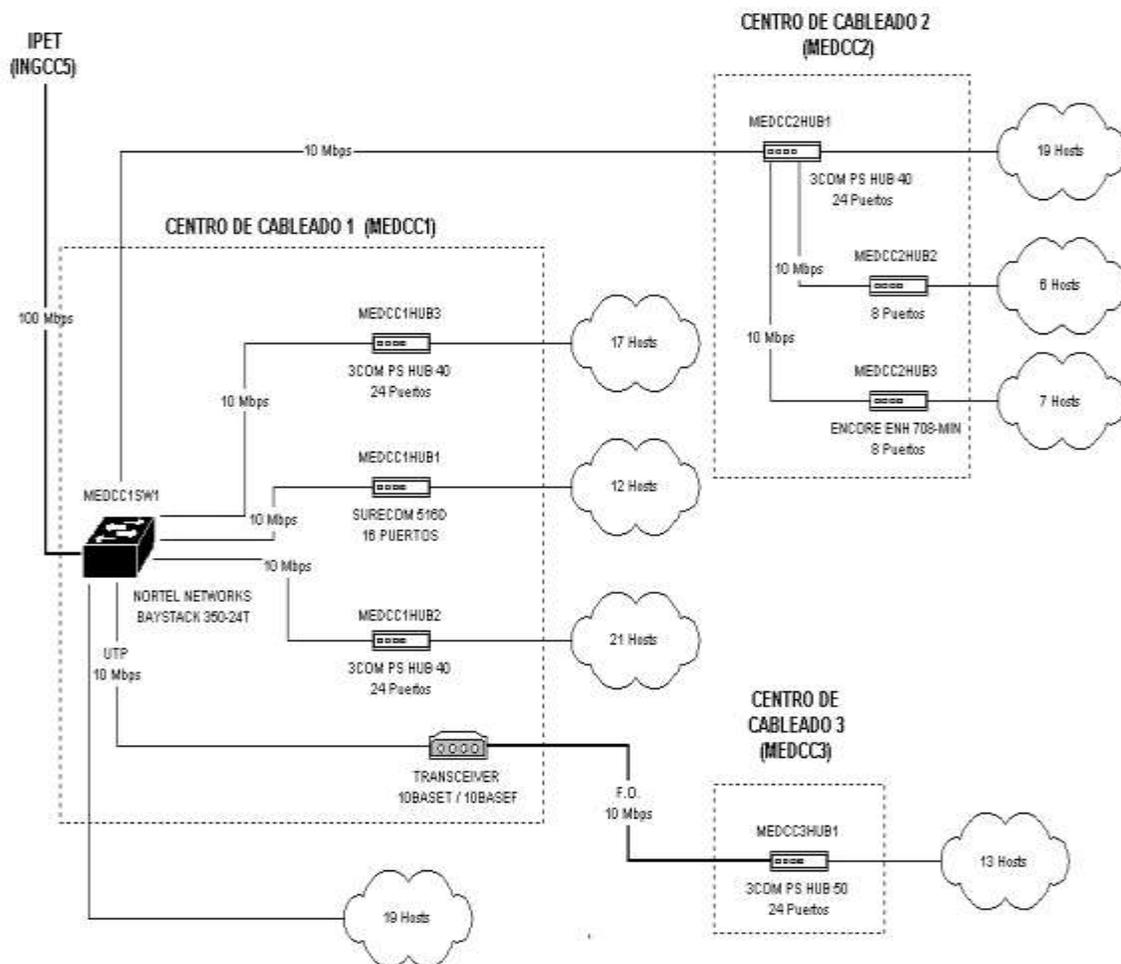


Figura 1. 19. Funcionamiento de los Centros de Cableado 1, 2, y 3 del Sector de Medicina.

La Tabla 1.13 resume la distribución de las estaciones de trabajo en los diferentes centros de cableado.

CENTRO CABLEADO	DE	HUBS	PUERTOS	HOSTS	TOTAL PUERTOS	TOTAL HOSTS
CC1		Sw 1	24	19		
		Hub 1	16	12		
		Hub 2	24	21		
		Hub 3	24	17		
TOTAL CC1					88	69

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

CC2					
	Hub 1	24	19		
	Hub 2	8	6		
	Hub 3	8	7		
TOTAL CC2				40	32
CC3					
	Hub 1	24	13		
TOTAL CC3				24	13
TOTALES DEL SECTOR				152	114

Tabla 1. 13. Distribución de Hosts del Sector de Medicina.

1.2.3 SECTOR DE EDUCACIÓN.

El funcionamiento general del Sector de Educación se muestra en la Figura 1.20. Las nubes de hubs que ahí se indican son detalladas en las figuras subsiguientes.

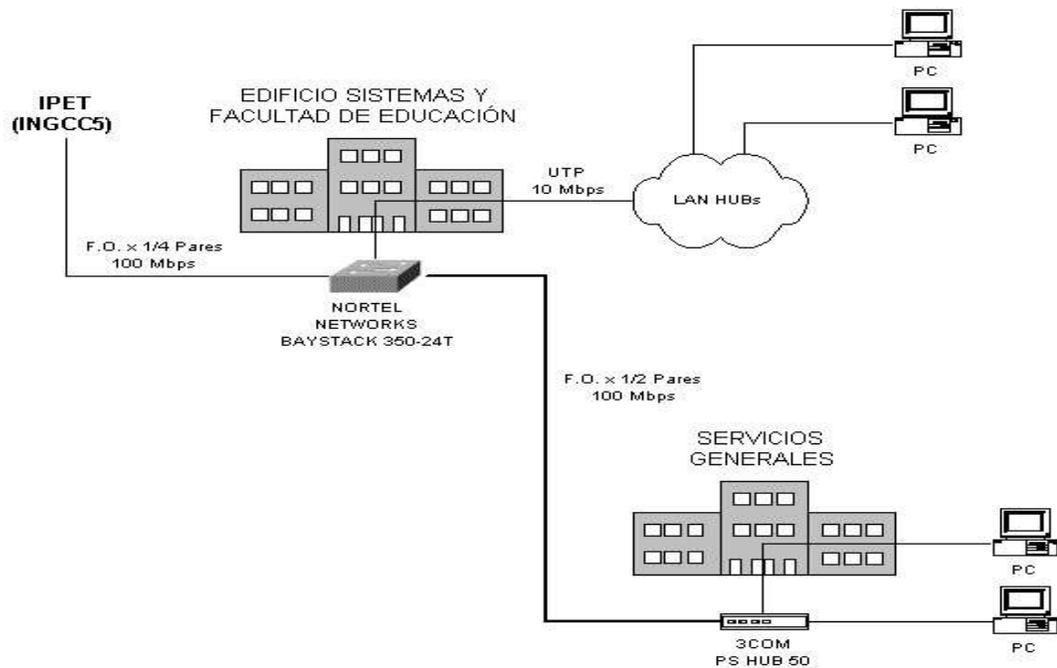


Figura 1. 20. Funcionamiento del Sector de Educación.

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

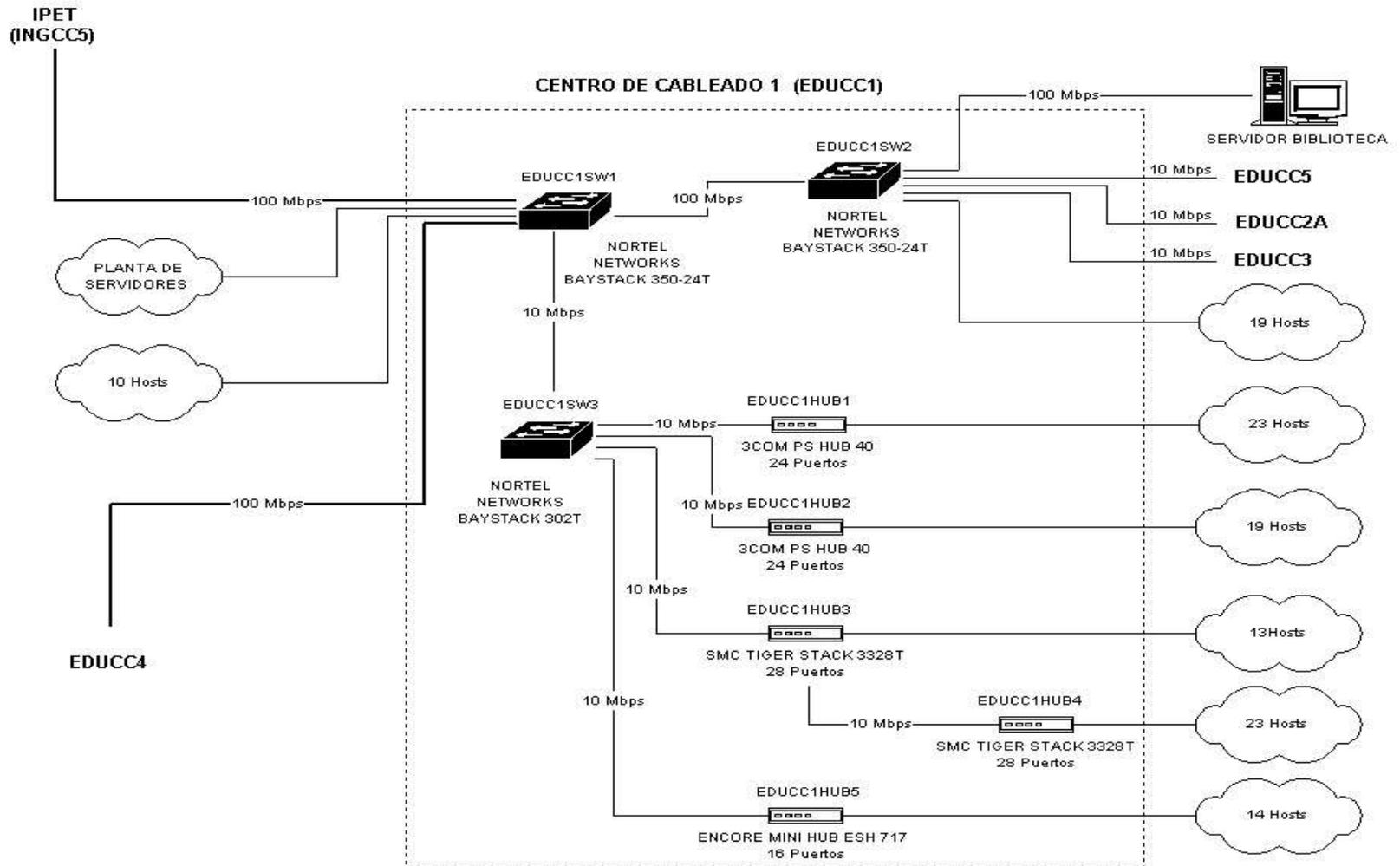


Figura 1. 21. Funcionamiento del Centro de Cableado 1 del Sector de Educación.

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

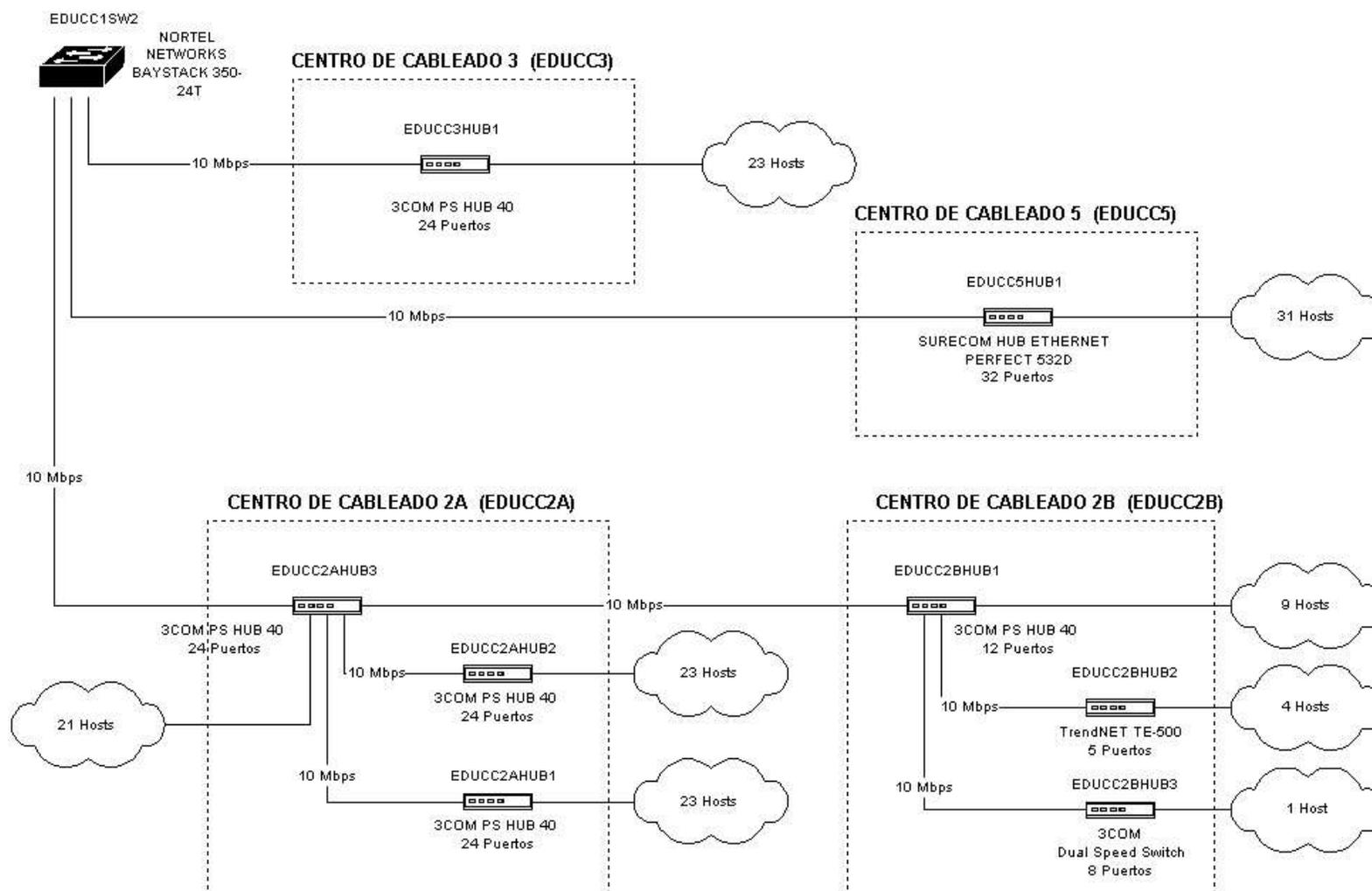


Figura 1. 22. Funcionamiento de los Centros de Cableado 2A, 2B, 3 y 5 del Sector de Educación.

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

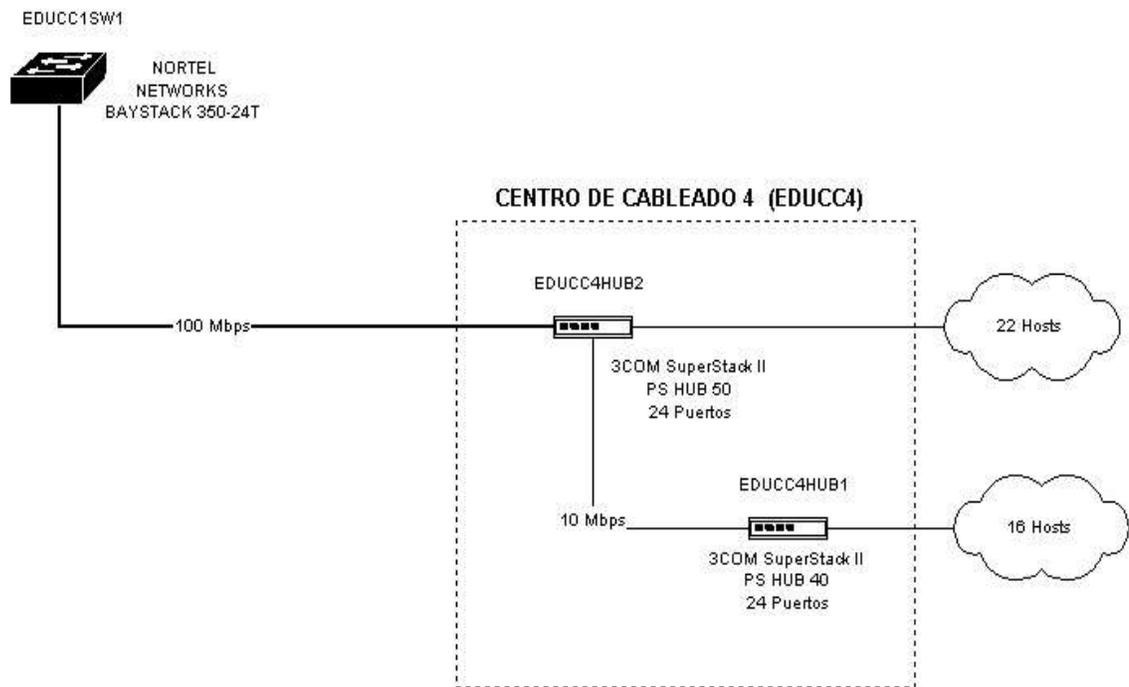


Figura 1. 23. Funcionamiento del Centro de Cableado 4 del Sector de Educación.

La Tabla 1.14 resume la distribución de las estaciones de trabajo en los diferentes centros de cableado.

CENTRO CABLEADO	DE	HUBS	PUERTOS	HOSTS	TOTAL PUERTOS	TOTAL HOSTS
CC1						
		Sw 1	24	16		
		Sw 2	24	20		
		Sw 3	8	0		
		Hub 1	24	23		
		Hub 2	24	19		
		Hub 3	28	13		
		Hub 4	28	23		
		Hub 5	16	14		
TOTAL CC1					176	128
CC2A						
		Hub 1	24	23		
		Hub 2	24	23		

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

	Hub 3	24	21		
TOTAL CC2A				72	67
CC2B					
	Hub 1	12	9		
	Hub 2	5	4		
	Hub 3	8	1		
TOTAL CC2B				25	14
CC3					
	Hub 1	24	23		
TOTAL CC3				24	23
CC4					
	Hub 1	24	16		
	Hub 2	24	22		
TOTAL CC4				48	38
CC5					
	Hub 1	32	31		
TOTAL CC5				32	31
TOTALES DEL SECTOR				377	301

Tabla 1. 14. Distribución de Hosts del Sector de Educación.

1.2.4 SECTOR DE EL CARMEN.

El funcionamiento general del Sector del Carmen se muestra en la Figura 1.24. Las nubes de hubs que ahí se indican son detalladas en las figuras subsiguientes.

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

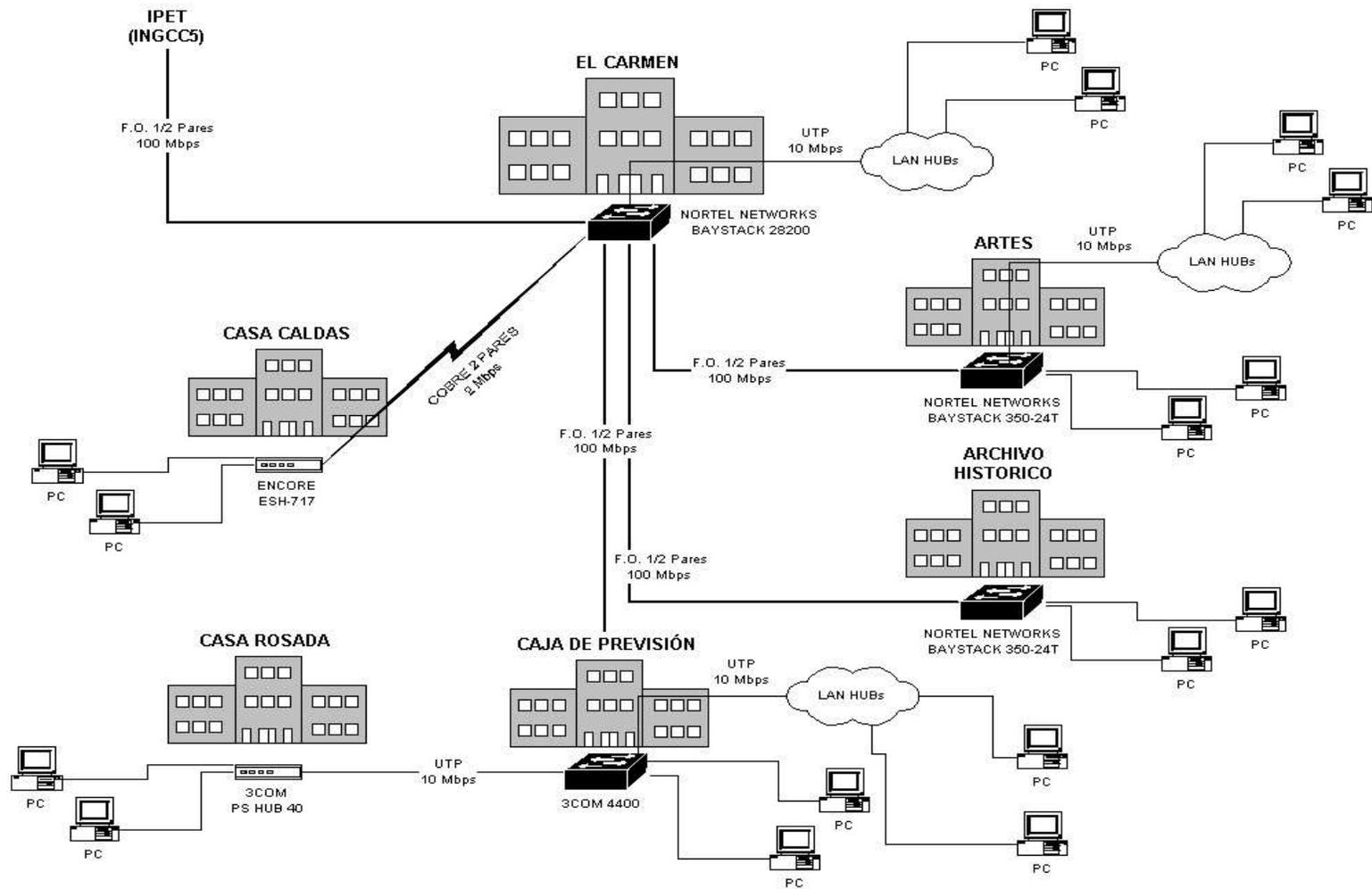


Figura 1. 24. Funcionamiento del Sector de El Carmen.

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

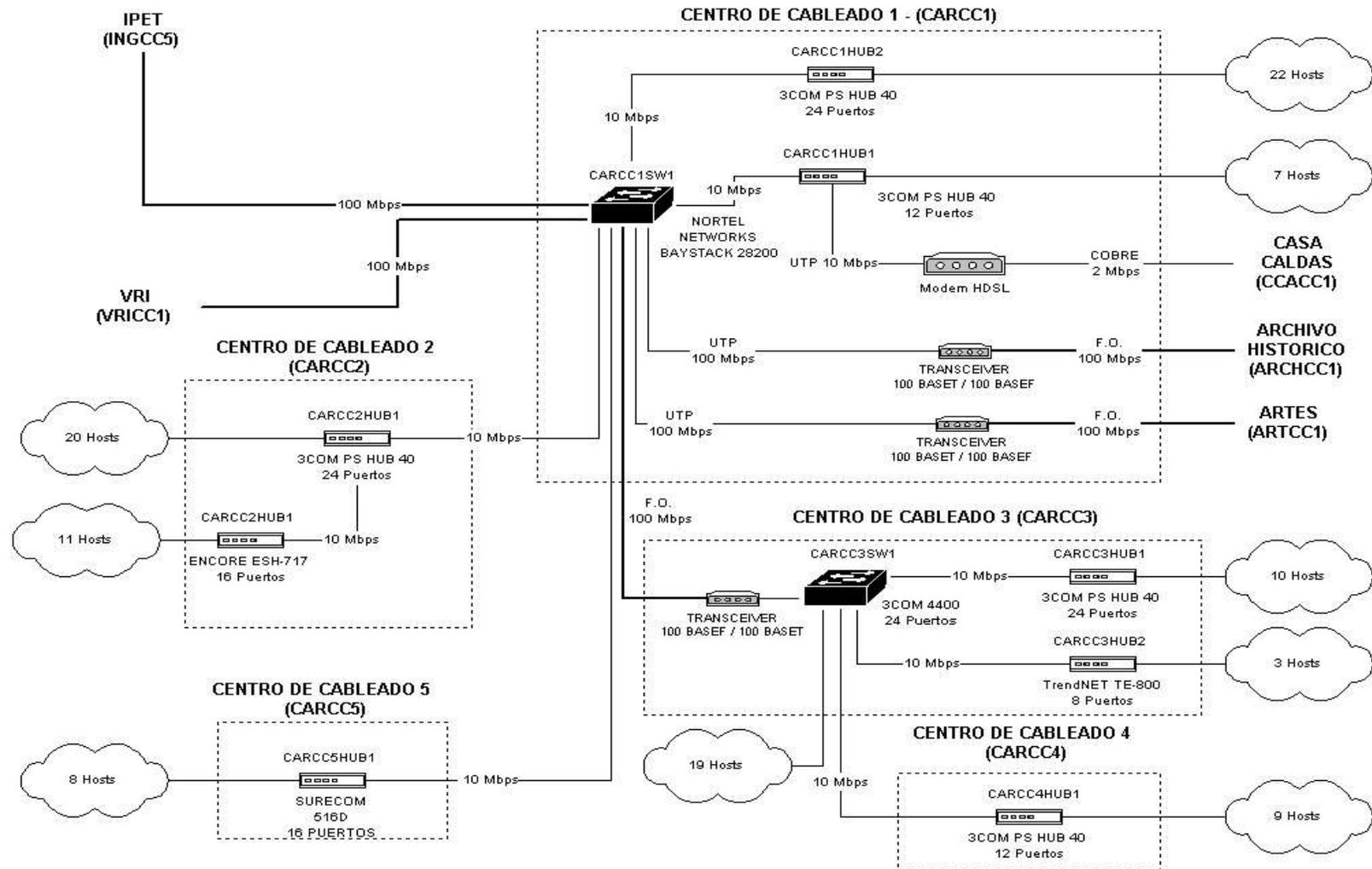


Figura 1. 25. Funcionamiento de los Centros de Cableado 1, 2, 3, 4, y 5 del Sector de El Carmen.

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

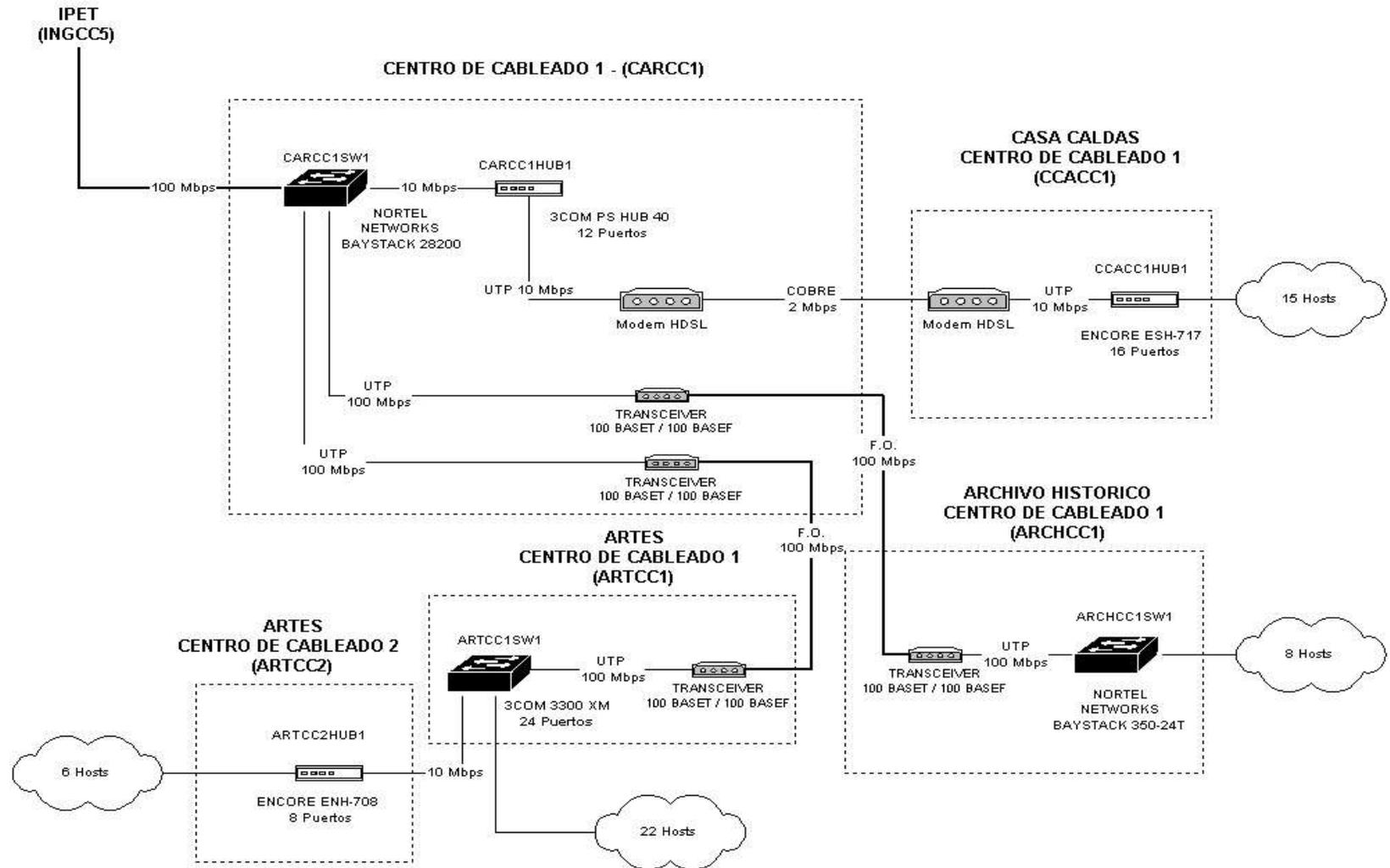


Figura 1. 26. Funcionamiento de los Centros de Cableado de Artes, Archivo Histórico y Casa Caldas del Sector de El Carmen.

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

La Tabla 1.15 resume la distribución de las estaciones de trabajo en los diferentes centros de cableado.

CENTRO CABLEADO	DE	HUBS	PUERTOS	HOSTS	TOTAL PUERTOS	TOTAL HOSTS
CC1						
	Sw 1		10	0		
	Hub 1		12	7		
	Hub 2		24	22		
TOTAL CC1					46	29
CC2						
	Hub 1		24	20		
	Hub 2		16	11		
TOTAL CC2					40	31
CC3						
	Sw 1		24	19		
	Hub 1		24	10		
	Hub 2		8	3		
TOTAL CC3					56	32
CC4						
	Hub 1		12	9		
TOTAL CC4					12	9
CC5						
	Hub 1		16	8		
TOTAL CC5					16	8
ARTES CC1						
	Sw 1		24	22		
TOTAL ARTES CC1					24	22
ARTES CC2						
	Hub 1		8	6		
TOTAL ARTES CC2					8	6
ARCHIVO HISTORICO CC1						
	Sw 1		24	8		
TOTAL ARCHIVO HISTORICO CC1					24	8

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

CASACALDAS CC1					
	Hub 1	16	15		
TOTAL CASA CALDAS CC1				16	15
TOTALES DEL SECTOR				242	160

Tabla 1. 15. Distribución de Hosts del Sector de El Carmen.

1.2.5 SECTOR DE SANTO DOMINGO.

El funcionamiento general del Sector de Santo Domingo se muestra en la Figura 1.27. Las nubes de hubs que ahí se indican son detalladas en la Figura 1.28.

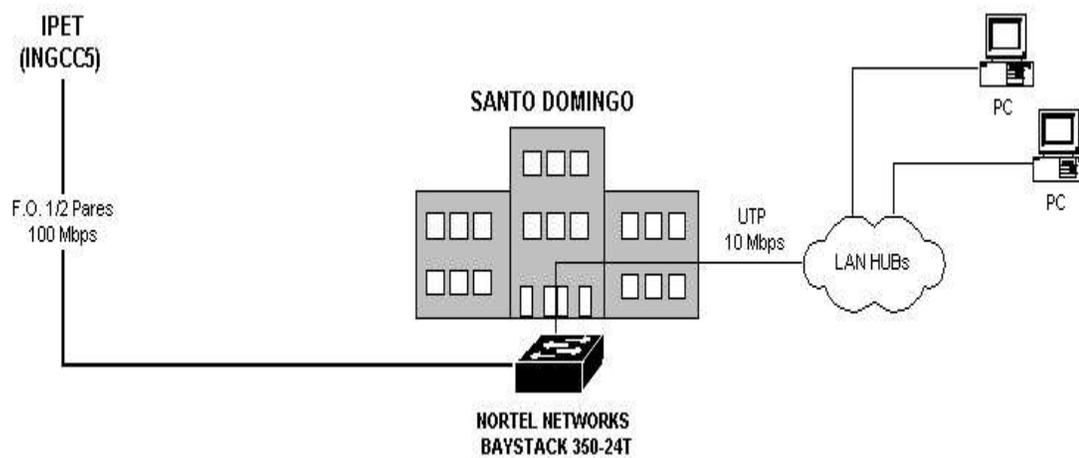


Figura 1. 27. Funcionamiento del Sector de Santo Domingo.

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

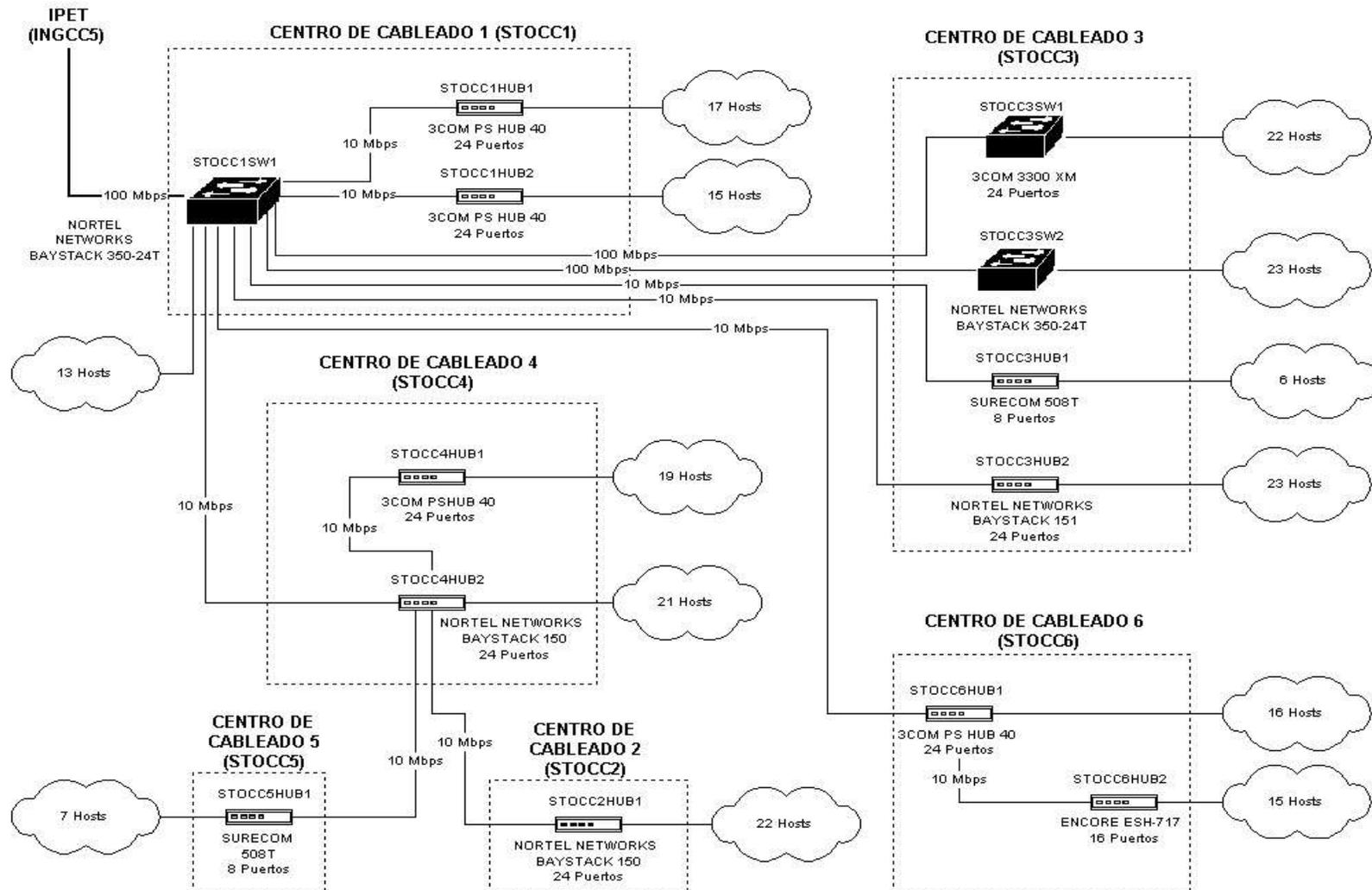


Figura 1. 28. Funcionamiento de los Centros de Cableado 1,2, 3, 4, 5, y 6 del Sector de Santo Domingo.

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

La Tabla 1.16 resume la distribución de las estaciones de trabajo en los diferentes centros de cableado.

CENTRO CABLEADO	DE	HUBS	PUERTOS	HOSTS	TOTAL PUERTOS	TOTAL HOSTS
CC1						
		Sw 1	24	13		
		Hub 1	24	17		
		Hub 2	24	15		
TOTAL CC1					72	45
CC2						
		Hub 1	24	22		
TOTAL CC2					24	22
CC3						
		Sw 1	24	22		
		Sw 2	24	23		
		Hub 1	8	6		
		Hub 2	24	23		
TOTAL CC3					80	74
CC4						
		Hub 1	24	19		
		Hub 2	24	21		
TOTAL CC4					48	40
CC5						
		Hub 1	8	7		
TOTAL CC5					8	7
CC6						
		Hub 1	24	16		
		Hub 2	16	15		
TOTAL CC6					40	31
TOTALES DEL SECTOR					272	219

Tabla 1. 16. Distribución de Hosts del Sector de Santo Domingo.

1.2.6 SECTOR DE VICERRECTORÍA DE INVESTIGACIONES (VRI).

El funcionamiento general del Sector del VRI se muestra en la Figura 1.29. Las nubes de hubs que ahí se indican son detalladas en la Figura 1.30.

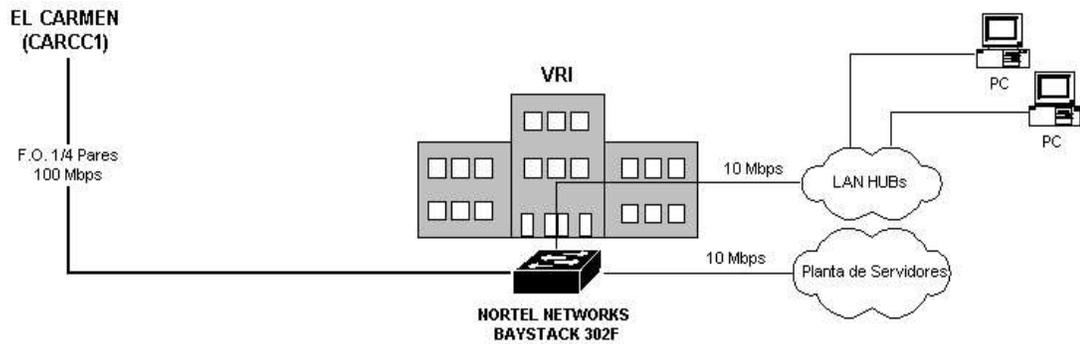


Figura 1. 29. Funcionamiento del Sector de la Vicerrectoría de Investigaciones (VRI).

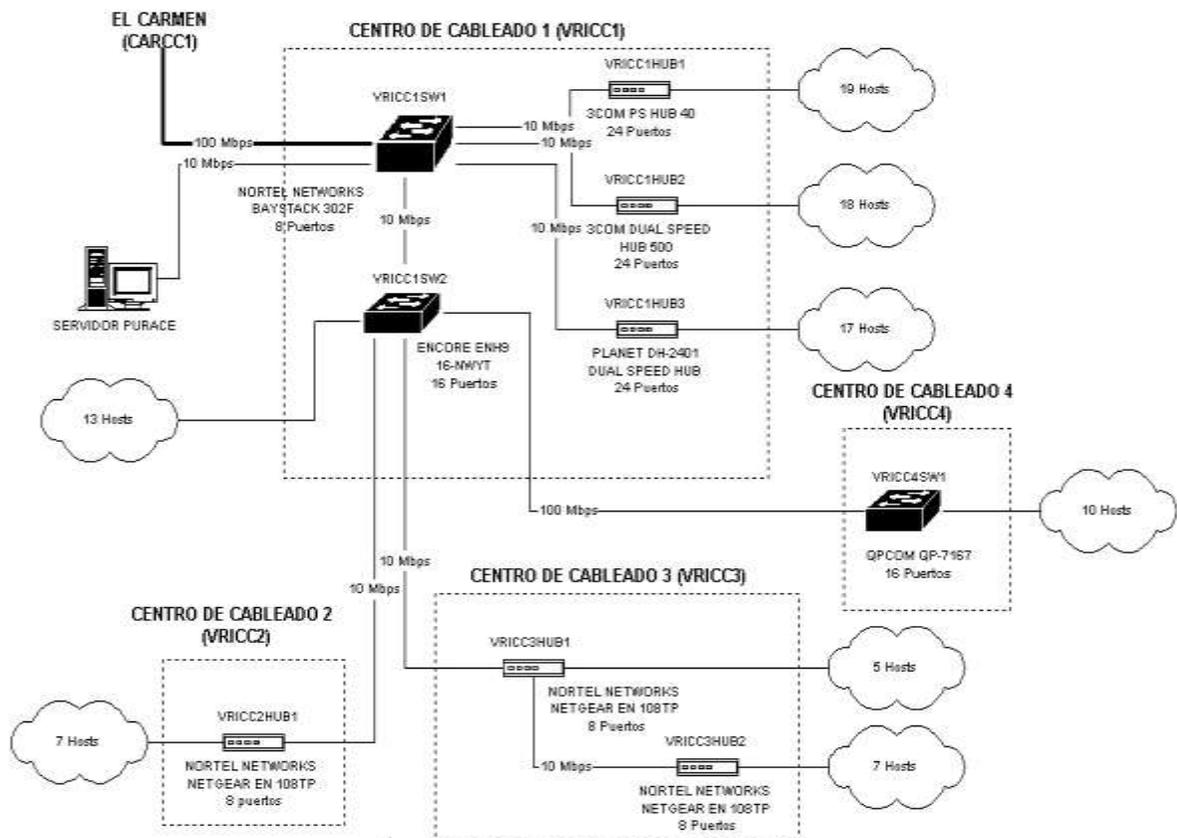


Figura 1. 30. Funcionamiento de los Centros de Cableado 1, 2, 3 y 4 del Sector del VRI.

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

La Tabla 1.17 resume la distribución de las estaciones de trabajo en los diferentes centros de cableado.

CENTRO CABLEADO	DE	HUBS	PUERTOS	HOSTS	TOTAL PUERTOS	TOTAL HOSTS
CC1						
	Sw 1		8	1		
	Sw 2		16	13		
	Hub 1		24	19		
	Hub 2		24	18		
	Hub 3		24	17		
TOTAL CC1					96	68
CC2						
	Hub 1		8	7		
TOTAL CC2					8	7
CC3						
	Hub 1		8	5		
	Hub 2		8	7		
TOTAL CC3					16	12
CC4						
	Sw 1		16	10		
TOTAL CC4					16	10
TOTALES DEL SECTOR					136	97

Tabla 1. 17. Distribución de Hosts del Sector de la Vicerrectoría de Investigaciones (VRI).

1.2.7 SECTOR DE LAS GUACAS.

El funcionamiento general del Sector de Las Guacas se muestra en la Figura 1.31. Las nubes de hubs que ahí se indican son detalladas en la Figura 1.32.

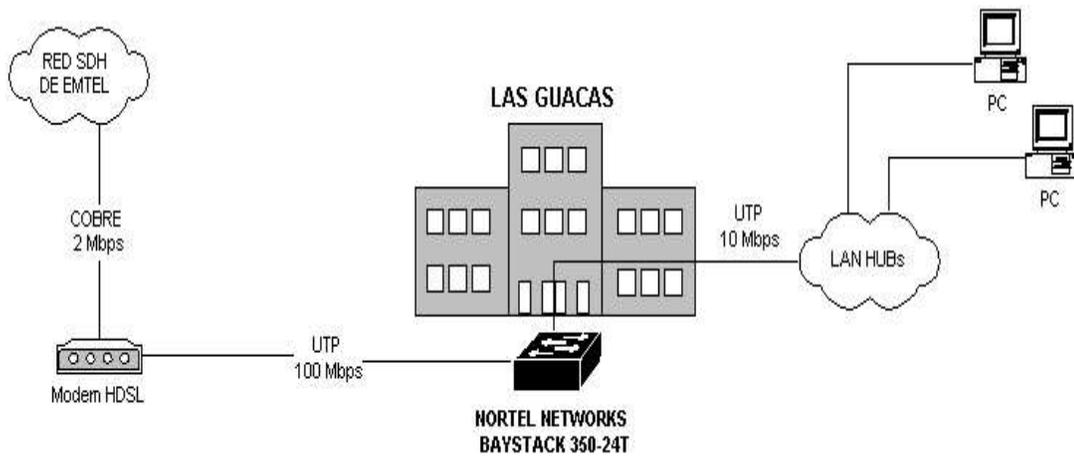


Figura 1. 31. Funcionamiento del Sector de Las Guacas

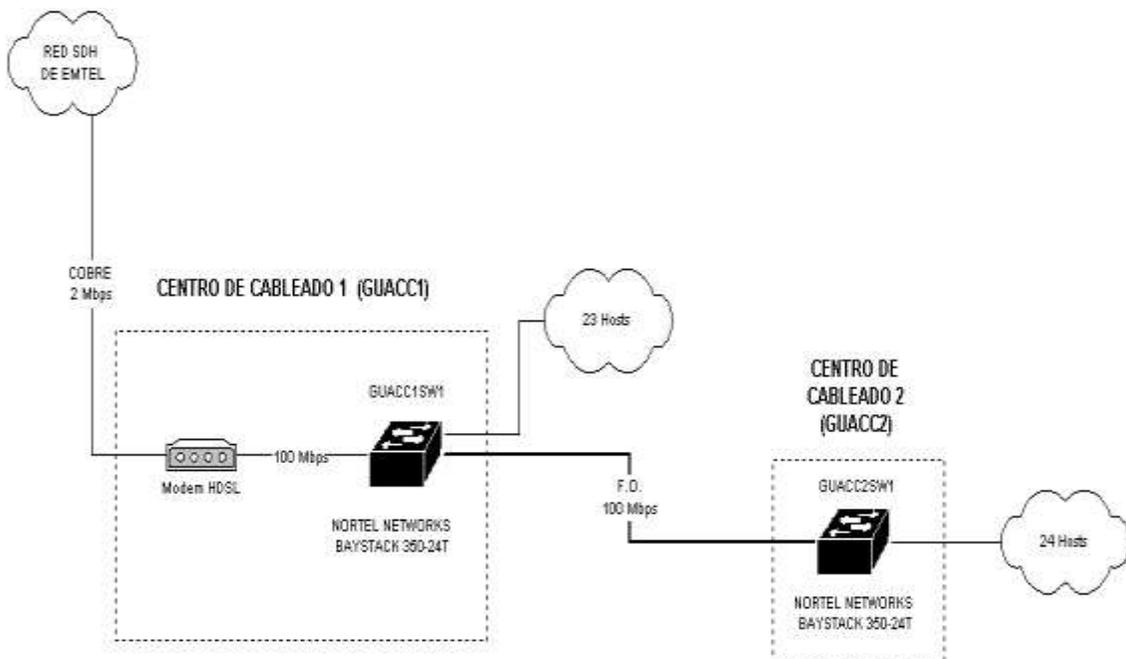


Figura 1. 32. Funcionamiento de los Centros de Cableado 1 y 2 del sector de las Guacas

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

La Tabla 1.18 resume la distribución de las estaciones de trabajo en los diferentes centros de cableado.

CENTRO CABLEADO	DE	HUBS	PUERTOS	HOSTS	TOTAL PUERTOS	TOTAL HOSTS
CC1						
	Sw 1		24	23		
TOTAL CC1					24	23
CC2						
	Sw 1		24	24		
TOTAL CC2					24	24
TOTALES DEL SECTOR					48	47

Tabla 1. 18. Distribución de Hosts del Sector de las Guacas.

Con base en las tablas anteriores se obtiene la Tabla 1.19, donde se resume la distribución de los hosts en los diferentes sectores de la Red.

SECTOR	TOTAL PUERTOS	TOTAL HOSTS
Ingenierías	859	692
Medicina	152	114
Educación	377	301
El Carmen	242	160
Santo Domingo	272	219
VRI	136	97
Las Guacas	48	47
TOTAL	2086	1630

Tabla 1. 19. Resumen Distribución de Hosts de la Red total.

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

1.3 DIRECCIONAMIENTO IP (SUBREDES).

Las direcciones IP de Red y sus correspondientes Máscaras entregadas a la Universidad del Cauca para su Red de Datos interna por parte de los Proveedores del Servicio de Comunicaciones a Internet son:

- **TELECOM:** 200.21.83.128 y 200.21.83.64 con mascara de subred 255.255.255.192
- **EMTEL:** 208.195.214.0 con mascara de subred 255.255.255.0

Debido al número limitado de direcciones IP públicas, y para obtener un mejor desempeño, ésta se ha dividido en subredes de la siguiente forma.

SECTOR	SUBRED
Santo Domingo	172.16.10.0
Artes	172.16.20.0
El Carmen	172.16.30.0
Ingenierías	172.16.40.0
Medicina	172.16.50.0
VRI	172.16.60.0
Laboratorios Física y Química	172.16.70.0
Casa Rosada – Casa Caldas	172.16.80.0
Caja de Previsión	172.16.90.0
Archivo Histórico	172.16.100.0
Educación	172.16.110.0
Servicios Generales	172.16.120.0
Ingenierías – IPET	172.16.130.0
Educación - Sistemas	172.16.140.0
CDU	172.16.150.0
Ciencias Agropecuarias	172.16.160.0
Hospital	172.16.170.0
Santander de Quilichao	172.16.213.0
Equipos de Red (Switches y Hubs)	10.1.13.0

Tabla 1. 20 Subredes IP Existentes.

1.4 SERVIDORES Y SERVICIOS SOPORTADOS.

SERVIDOR ACUARIO: El portal Web de La Universidad del Cauca y sitios como el del Grupo GNU/Linux, seminarios, eventos, departamentos y afines se encuentran alojados en Acuario. Este es el servidor principal de Hosting de Unicauca, que lo hace uno de los servidores de la institución con mayor presencia en Internet. Soporta sitios que utilizan php para brindar contenido dinámico y bases de datos en mysql.

SERVIDOR AFRODITA: Podría decirse que *Afrodita* es uno de los equipos con alta prioridad dentro de la Universidad. Su principal función es la de servidor de correo para estudiantes de Pregrado, Postgrado y Egresados de la Universidad del Cauca. *Afrodita* también es el servidor secundario de nombres externo, contiene una réplica de todas las zonas que se encuentran en el servidor maestro *Atenea*

SERVIDOR ARGES: Es el equipo servidor donde se encuentra la implementación Firewall para la Intranet de la Universidad del Cauca y donde se configura el servicio de NAT por demanda. El firewall es un servicio que utiliza la Red de Datos como herramienta complementaria para administrar la asignación de direcciones IP publicas al interior de la Universidad. Adicionalmente el Firewall se utiliza como primera línea de seguridad por la posibilidad que tiene de bloquear puertos y direcciones IP riesgosos. Por su parte, el servicio de NAT por demanda permite la conexión a nivel de red de un computador en la intranet de la Universidad con Internet

SERVIDOR ATENEA: Es uno de los equipos más importantes que tiene la Institución. En *Atenea* se alojan las cuentas de correo electrónico y archivos de docentes, las dependencias, eventos, grupos académicos y de investigación, funcionarios y pensionados. *Atenea* funciona como el servidor maestro de nombres externo, contiene las zonas de unicauca.edu.co y ucauca.edu.co con registros de direcciones IPs públicas, las zonas de resolución inversa para las redes de Telecom y Emtel, y las zonas para los proyectos EHAS, Tampu, Redpacífico y Visioncauca. *Atenea* también es el servidor de Radius, a través del cual se autentican los usuarios de acceso telefónico.

SERVIDOR CERES: Es el equipo donde se encuentra el MRTG que toma información sobre el tráfico de los enlaces de Telecom y Emtel, el ancho de banda consumido por los usuarios que acceden vía telefónica a través del RAS e información sobre el tráfico en los proxies Hiperion y Temis. Mediante Ceres también se presta alojamiento de sitios con la plataforma de Java (JSP, Servlets) y bases de datos en mysql, como el portal del Museo de Historia Natural.

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

SERVIDOR HADES: Es el servidor DNS Interno primario y aparte de esto es servidor de alojamiento de aplicaciones Web basadas en Tecnologías Microsoft como asp. Este servidor es muy importante ya que resuelve peticiones de nombres de dominio de casi todos los computadores de la Universidad.

SERVIDOR URANO: Es el equipo destinado a cumplir las funciones de DNS externo y servidor de RADIUS.

SERVIDOR HIPERION: Es uno de los servidores que soportan el acceso de la Intranet de Unicauca a Internet mediante Proxy Web, con una configuración especial para brindar Alta-Disponibilidad. Para la prestación de este servicio, son necesarias las aplicaciones squid, heartbeat y monit.

SERVIDOR JUNO: Es uno de los servidores menos conocidos y más importantes de la Universidad del Cauca: es el servidor de directorio. Juno es el soporte para servicios tan importantes como el correo electrónico. En el se almacenan datos personales de la comunidad Universitaria, como números telefónicos, nombres, ocupaciones, contraseñas que sirvan como soporte para validar a los usuarios frente a sus servidores de correo e información acerca del servicio de acceso telefónico de los usuarios. Juno es un servidor que no es conocido ni accedido directa o indirectamente por usuarios normales, pero guarda información muy importante. Es un servidor que debe caracterizarse por su estabilidad y su buen tiempo de respuesta.

SERVIDOR ODIN: Es el servidor FTP Institucional de la Universidad del Cauca. En el se almacenan muchos archivos que la comunidad Universitaria necesita obtener de forma fácil y rápida desde muchos computadores, entre otros archivos, aquí se encuentran actualizaciones de seguridad de algunos programas, instaladores de diferentes sistemas operativos, herramientas de ofimática, herramientas de desarrollo, comunicados a la opinión pública, etcétera.

SERVIDOR PERSEO: Es el servidor donde se encuentra implementado el servicio de DNS Interno Secundario para la Intranet de la Universidad del Cauca. Por la importancia del servicio de DNS, la Universidad del Cauca cuenta con dos servidores, uno primario y uno secundario, para prestar este servicio.

SERVIDOR TEMIS: Es uno de los servidores que soporta el servicio de Acceso a Internet de Alta Disponibilidad desde la Intranet de la Universidad del Cauca. La prestación de este servicio a los usuarios de la intranet de la Universidad del Cauca requiere de la instalación y configuración de los siguientes servicios: squid, heartbeat y monit.

SERVIDOR JANO: Es uno de los servidores que sirve como base de datos de la información de los docentes del Departamento de Telemática de la Facultad de

CAPITULO 1. ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

Ingeniería Electrónica y Telecomunicaciones, y de la información de sus proyectos de investigación.

SERVIDOR PURACE: Este servidor esta ubicado en la Vicerrectoría de Investigaciones y soporta los servicios Proxy y DNS. También alberga las páginas Web del VRI.

SERVIDOR BIBLIO: Este servidor esta ubicado en la Biblioteca en el Sector de Educación y presta los servicios de consulta y gestión de la misma.

SERVIDOR DE ACCESO REMOTO: El equipo Lucent Technologies Max 6000 presta el servicio de acceso remoto y es conocido dentro del ámbito Universitario como Acceso Telefónico.

SERVIDOR EOWIN: Este servidor está ubicado en el Sector de Educación en el área de sistemas y soporta las aplicaciones del Sistema de Información Financiero, el cual maneja los servicios de pago de nómina, servicio financiero (contabilidad, presupuestos, tesorería), pago de derechos financieros, entre otros.

SERVIDOR GALADRIEL: Este servidor está ubicado en el Sector de Educación en el área de sistemas y soporta las aplicaciones del Sistema de Información de Recursos Físicos, el cual principalmente lleva el control de todos los bienes físicos que posee la Universidad del Cauca.

SERVIDOR ARWEN: Este servidor está ubicado en el Sector de Educación en el área de sistemas y soporta las aplicaciones del Sistema de Información de Recursos Humanos, el cual maneja los procesos de nómina, contratación, puestos de trabajo, certificados, cesantías, entre otros.

SERVIDOR TESEO: Este servidor aloja las bases de datos Oracle de los Sistemas de Información de Recursos Físicos y Humanos. Se encuentra ubicado en el Sector de Educación en el área de sistemas.

SERVIDOR GANDALF: Este servidor aloja las bases de datos Oracle del Sistema de Información Financiero. Se encuentra ubicado en el Sector de Educación en el área de sistemas.

SERVIDOR SOCRATES: Este servidor soporta el Sistema de Información Académico el cual permite realizar todas las actividades de registro y control académico de toda la comunidad universitaria.

2. NORMAS DE CONFIGURACION Y DESEMPEÑO DE REDES LAN ETHERNET.

En éste capitulo se presentan los conceptos teóricos utilizados para realizar el análisis de desempeño de la Red de Datos de la Universidad del Cauca. Se describen las reglas de configuración Ethernet y Fast-Ethernet para redes LAN, y se realiza el estudio de las técnicas empleadas para poder llevar a cabo un análisis de desempeño adecuado.

2.1 REGLAS DE CONFIGURACIÓN.

La Red de Datos de la Universidad del Cauca es una red LAN que utiliza tecnología Ethernet y Fast-Ethernet para su funcionamiento, y se basa en el empleo del cableado estructurado lo que la hace un sistema de comunicaciones confiable. Las tecnologías son descritas por la IEEE en su estándar 802.3, en el cual se especifican los parámetros del hardware de los equipos, las tarjetas de red y cables a utilizar, junto con las reglas de configuración para los diferentes medios de transmisión y su combinación, y el cableado estructurado se especifica en el estándar ANSI/TIA/EIA-568-A, que constituye una filosofía de diseño capaz de permitir un fácil uso, expansión y mantenimiento de las redes, integrando todos los servicios de comunicaciones, y cubriendo con sus elementos constitutivos las necesidades de las aplicaciones existentes. Para comenzar se verán los medios de comunicación que emplean las tecnologías arriba mencionadas, y de esa forma tener una mejor comprensión de la reglamentación a ser descrita.

2.1.1 MEDIOS DE COMUNICACIÓN.

La evolución de las redes de comunicaciones ha llevado a la especificación de varios estándares de cableado capaces de soportar el volumen de información y la versatilidad física que la dinámica actual requiere. Las tecnologías Ethernet y Fast-Ethernet han visto evolucionar los diferentes medios de comunicación que las soportan, siendo dos los más utilizados en la actualidad: el estándar de cable par trenzado y la fibra óptica.

El funcionamiento del sistema de cableado deberá ser considerado no sólo cuando se están apoyando las necesidades actuales sino también cuando se anticipan las necesidades del mañana. Hacer esto permitirá la migración a aplicaciones de redes más rápidas sin necesidad de incurrir en costosas actualizaciones de dicho sistema.

CAPITULO 2. NORMAS DE CONFIGURACION Y DESEMPEÑO DE REDES LAN ETHERNET.

Las características de producto y de funcionamiento particulares de las opciones de sistemas de cableado son las siguientes.

2.1.1.1 PAR TRENZADO.

Actualmente casi todo el cable de cobre utilizado en redes Ethernet es el de pares trenzados sin apantallar (UTP), raramente se emplea cable de par trenzado apantallado (STP). Esto se debe en parte a la mejora de las virtudes del cable UTP, que ha alcanzado rendimientos que antes sólo eran alcanzables sobre medios apantallados y sobre todo a su bajo costo que permite un cableado integrado de voz y datos. Un cable UTP típicamente lleva 4 u 8 hilos que normalmente están doblados dos a dos formando una doble (o cuádruple) hélice, por lo que se le suele denominar cable de pares trenzados (twisted pair). Esto se hace para minimizar la interferencia eléctrica que pueden recibir de fuentes próximas, como por ejemplo los pares vecinos, y la que pueden emitir al exterior. Los cables pueden o no estar apantallados, característica que diferencia a dos tipos de par trenzado, el más habitual en redes locales no lleva apantallamiento de ningún tipo más allá del que proporciona el hecho de tener los pares trenzados; este se conoce como cable UTP (Unshielded Twisted Pair). Existe también cable en el que los pares llevan una pantalla de hilos de cobre formando una malla, llamado STP (Shielded Twisted Pair); este cable es bastante voluminoso debido a la pantalla, lo cual encarece su precio y su costo de instalación. El ancho de banda de estos cables depende de múltiples factores: el grosor del cable, la distancia, el tipo de aislamiento, la densidad de vueltas o grado de trenzado, etc. Y pueden llegar a transmitir con capacidades del orden de Mbps a varios kilómetros. La regla más importante y conocida de este tipo de cableado, aplicable a Ethernet y Fast-Ethernet, determina que la distancia máxima permisible con par trenzado a la que un host puede estar de un hub o switch es de 100 m.

Existen varios tipos de cables de pares trenzados que difieren fundamentalmente en la frecuencia máxima a la que pueden trabajar, que a su vez, viene determinada principalmente por la densidad de vueltas y por el tipo de material aislante que recubre los pares. Estos tipos se conocen como categorías y son las siguientes:

Categoría	Frecuencia Máxima (MHz)	Usos	Vueltas / metro
1	No se especifica	Telefonía, datos a corta distancia y baja velocidad	0
2	1	LANs de baja velocidad (1 Mbps)	0
3	16	LANs hasta 10 Mbps	10 – 16
4	20	LANs hasta 16 Mbps	16 – 26

CAPITULO 2. NORMAS DE CONFIGURACION Y DESEMPEÑO DE REDES LAN ETHERNET.

5	100	LANs hasta 1000,Mbps, ATM a 155 Mbps	26 – 33
6	250	LANs hasta 1000 Mbps, ATM a 622 Mbps	
7	600	LANs hasta 1000 Mbps, ATM a 622 Mbps	

Tabla 2. 1. Características de los cables según su categoría

Para el cable par trenzado apantallado (STP) con impedancia de 150 Ω , se tiene que todos los componentes son probados para un funcionamiento eléctrico de hasta 300 MHz, y gracias a que posee un ancho de banda de 600 MHz este tipo de cable puede acomodar aplicaciones multimediales y aplicaciones con tasas mayores a 100Mbps.

La característica principal de un cable desde el punto de vista de transmisión de datos es su atenuación. La atenuación se produce por la pérdida de energía radiada al ambiente, y en la medida en que el cable esté más apantallado menor será ésta; el cable UTP de categoría más alta tiene menor atenuación, ya que el mayor número de vueltas le da un mayor apantallamiento, y es todavía menor en el cable STP. Por otro lado la atenuación depende de la frecuencia de la señal transmitida, a mayor frecuencia mayor atenuación cualquiera que sea el tipo de cable.

Frecuencia (MHz)	UTP Categoría 3	UTP Categoría 5	STP
1	2.6	2	1.1
4	5.6	4.1	2.2
16	13.1	8.2	4.4
25		10.4	6.2
100		22	12.3
300			21.4

Tabla 2. 2. Atenuación (en dB/100 m) de distintos tipos de cables a diferentes frecuencias.

2.1.1.2 FIBRA ÓPTICA.

La fibra óptica es el elemento que ha causado el elevado desarrollo de las comunicaciones telemáticas en los últimos años, su capacidad de transportar grandes cantidades de tráfico a grandes distancias, la convierten en el medio de transmisión

más popular. Existen dos sistemas de transmisión de datos por fibras ópticas: los que utilizan LEDs (Light-Emitting Diodes) y los que utilizan diodos láser. En los sistemas que utilizan LEDs la transmisión de un pulso de luz (equivalente a un bit) genera múltiples rayos, pues se trata de luz normal no coherente; y se dice que cada uno de estos rayos tiene un modo. La fibra utilizada con esta clase de emisores se la denomina fibra multimodo y sus dimensiones típicas son de 50/100 y 62,5/125 micras (significando que el diámetro de la fibra interior es de 62.5 micras y el de la fibra exterior es de 125 micras). Los diodos láser emiten luz coherente, por lo que hay un único rayo al utilizar este tipo de emisor, la fibra utilizada con él se comporta como una guía-de-onda; la luz se propaga a través de ella sin dispersión; y es denominada fibra monomodo, estas se utilizan para transmitir a grandes velocidades y a grandes distancias. Su fibra interior (la que transmite la luz) es de un diámetro muy pequeño, de 8 a 10 micras (del mismo orden de magnitud que la longitud de onda de la luz que transmite); una fibra monomodo típica es la de 8,1/125 micras.

Para la transmisión de luz por fibras ópticas se utilizan tres rangos de frecuencias, aquellos en que las fibras muestran menor absorción. Son bandas situadas alrededor de 0,85, 1,30 y 1,55 micras, y se encuentran por lo tanto en la zona infrarroja del espectro (recordando que la parte visible esta entre 0,4 y 0,7 micras); se conocen como primera, segunda y tercera ventana, respectivamente. La primera ventana tiene mayor atenuación y es poco utilizada. La segunda ventana, que tiene una anchura de 18 THz (1 TeraHertzio = 1000 GHz) es la que más se utiliza. La tercera ventana tiene una anchura de 12,5 THz y es la que presenta menor atenuación, ésta se utiliza con fibra monomodo cuando se quiere cubrir una gran distancia sin repetidores.

Cuando se transmite un pulso por una fibra multimodo los rayos se reflejan múltiples veces antes de llegar a su destino, con ángulos diversos lo cual hace que la longitud del trayecto recorrido por los rayos que forman el pulso no sea exactamente igual para todos ellos; esto produce un ensanchamiento del pulso recibido, conocido como dispersión, que limita la velocidad de transferencia, ya que el emisor no puede enviar los pulsos con la rapidez que en un principio podría; la dispersión es función de dos factores: el ancho de banda y la longitud de la fibra, y se calcula como el producto de ambas magnitudes, así por ejemplo una fibra de 2 Km que transmita a 155 Mbps (equivalente a 155 MHz) tendrá una dispersión de 310 MHz Km. Con los elementos de transmisión actuales la dispersión máxima tolerable para la fibra multimodo es de 500 MHz Km; por ejemplo, si se transmite a 622 Mbps (que es la velocidad máxima empleada con este tipo de fibras) la distancia máxima que puede alcanzarse viene limitada a 800 metros por el efecto de dispersión. A 155 Mbps esta distancia es de 3,2 Km, y a 100 Mbps de 5 Km. Como la fibra monomodo no presenta dispersión, es fácil comprender que ésta siempre sea utilizada para cubrir grandes distancias.

A menudo los fabricantes dan cifras orientativas del alcance de sus equipos, como por ejemplo que la distancia máxima en fibra multimodo es de 2 Km o en monomodo de

CAPITULO 2. NORMAS DE CONFIGURACION Y DESEMPEÑO DE REDES LAN ETHERNET.

15 a 30 Km. Estos valores suelen no dar problemas, pero en casos que haya muchos conectores o empalmes, o que se quiera superar las distancias que da el fabricante, se debe de tener en cuenta que no se supere la atenuación máxima recomendable de la fibra que se está utilizando.

Tipo de fibra	Diámetro del núcleo (µm)	Diámetro de la funda (µm)	Atenuación (dB/Km)		
			850 nm	1300 nm	1500 nm
Monomodo	5	85 ó 125	2.3		
Monomodo	8.1	125		0.5	0.25
Multimodo	50	125	2.4	0.6	0.5
Multimodo	62.5	125	3	0.7	0.3
Multimodo	100	140	3.5	1.5	0.9

Tabla 2. 3. Atenuación de diferentes tipos de fibra en las diversas ventanas.

Habiendo conocido los distintos medios de transmisión, ahora se puede entender la forma como está compuesta la infraestructura que la Red de Datos de la Universidad del Cauca tiene desplegada actualmente: Sistema de cableado estructurado en cobre UTP Categoría 5/5e/6 en su red de acceso, fibra óptica multimodo de 62,5/125 µm en su red backbone y fibra óptica monomodo de 9/125 µm en los edificios de Artes, Archivo Histórico y Matematicas.

Las distancias soportadas para Ethernet y Fast-Ethernet por los varios medios de comunicación que estas tecnologías utilizan se muestran en la siguiente tabla.

	Ethernet 10BASE-T	Ethernet 10BASE-FL	Ethernet 100BASE-TX	Ethernet 100BASE-FX
Tasa de datos	10 Mbps	10 Mbps	100 Mbps	100 Mbps
UTP Cat5	100 m	-	100 m	-
STP / Coaxial	500 m	-	100 m	-
Fibra Multimodo	-	2 Km	-	412 m (operando Half-Duplex) 2 Km (operando Full-Duplex)
Fibra Monomodo	-	25 Km	-	20 Km

Tabla 2. 4. Distancias soportadas para Ethernet y Fast-Ethernet.

2.1.2 REGLAS DE CONFIGURACIÓN PARA ETHERNET Y FAST-ETHERNET.

El estándar IEEE 802.3 establece dos formas de verificar que una determinada topología Ethernet es válida. La primera, denominada Modelo 1, corresponde a un conjunto de reglas relacionadas con la distancia máxima y el número máximo de repetidores que puede haber entre dos estaciones. Cumpliendo esas reglas el usuario se asegura de que su red no excede los valores máximos en el tiempo de ida y vuelta. Ahora bien, el Modelo 1 adopta una actitud conservadora y presupone las longitudes máximas en el enlace del usuario final. Si éste no está utilizando la longitud máxima es posible aumentar la distancia en los enlaces intermedios. En este caso hay que verificar la topología siguiendo el Modelo 2, que consiste en realizar cálculos detallados del retardo para cada componente y para cada tramo de cable en cada trayecto. Una topología en principio inaceptable según el Modelo 1 puede resultar válida aplicando las reglas del Modelo 2.

2.1.2.1 CONFIGURACIÓN DE UNA ETHERNET A 10 MBPS.

El primer modelo de configuración recogido en el estándar 802.3 corresponde a una serie de reglas de configuración multisegmento para una red compuesta por varios segmentos Ethernet a 10 Mbps.

- Se requieren repetidores para todas las conexiones entre segmentos.
- Las MAU que son parte de los repetidores deben ser tenidas en cuenta a la hora de calcular el número máximo de MAUs en un segmento.
- El camino de transmisión entre dos DTEs puede constar de 5 segmentos, cuatro repetidores, dos MAUs y dos AUIs.
- Los cables AUI para 10Base-FP y 10Base-FL no excederán de los 25 metros.
- Cuando un camino de transmisión consta de cuatro repetidores y cinco segmentos, hasta tres de estos pueden ser mixtos y los restantes deben ser segmentos de enlaces entre repetidores. Cuando existen cinco segmentos, cada segmento de enlace de fibra óptica (FOIRL, 10Base-FB o 10Base-FL) no debe exceder de 500 metros y cada segmento 10Base-FP no debe exceder de los 300 metros.
- Cuando un camino consta de tres repetidores y cuatro segmentos se aplican las siguientes restricciones:
 - ✓ La longitud máxima permitida para segmentos de fibra entre repetidores (FOIRL, 10Base-FB o 10Base-FL) no debe exceder de 100 metros y los segmentos y cada segmento 10Base-FP no debe exceder de los 700 metros.
 - ✓ La longitud máxima para cualquier segmento de fibra entre repetidor y DTE no excederá de 400 metros para 10Base-FL, de 300 metros para 10Base-FP y de 400 metros para 10Base-FL.

CAPITULO 2. NORMAS DE CONFIGURACION Y DESEMPEÑO DE REDES LAN ETHERNET.

- ✓ No existe ninguna restricción al número de segmentos mixtos en este caso.

El segundo modelo proporciona una serie de elementos para la realización de cálculos que validen sistemas Ethernet complejos. Este modelo se basa en calcular el retraso en la ida y vuelta de la señal a partir de los retrasos que cada componente de un sistema Ethernet introduce (valores que aparecen detallados en el estándar).

El primer paso es identificar el peor camino posible (el de mayor retraso), que será el de segmentos más largos y con más repetidores entre dos estaciones. En caso de que no resulte evidente cuál es el peor de los caminos será preciso identificar todos los candidatos para aplicar los cálculos sobre todos ellos.

Una vez identificado el peor camino, debe modelarse el peor camino utilizando el modelo propuesto en el estándar, que incluye un segmento en los extremos derecho e izquierdo y tantos segmentos intermedios como sea preciso.

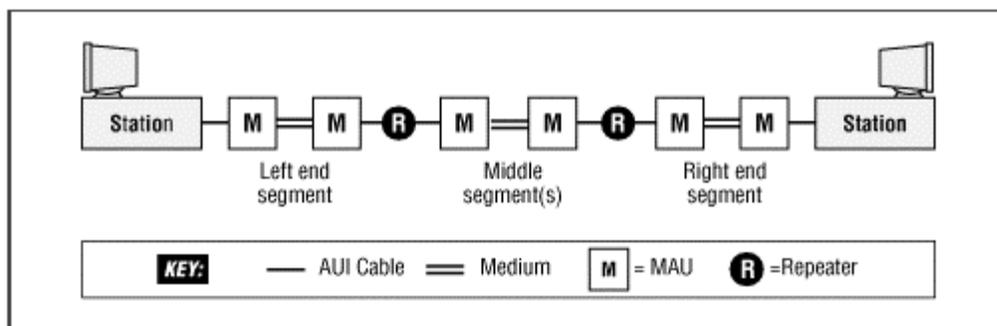


Figura 2. 1. Modelo de red para cálculo del retardo del viaje de ida y vuelta.

El siguiente paso es calcular el retraso total de la señal en el camino, o tiempo de ida y vuelta, sumando los retrasos introducidos por cada segmento.

La siguiente tabla recoge los retrasos (medidos en bits) introducidos por cada tipo de cable usado en Ethernet.

CAPITULO 2. NORMAS DE CONFIGURACION Y DESEMPEÑO DE REDES LAN ETHERNET.

Tipo de Segmento	Longitud Máxima (metros)	Extremo izquierdo		Segmento intermedio		Extremo derecho		Retraso ida y vuelta/ metro
		Base	Max	Base	Max	Base	Max	
10BASE5	500	11.75	55.05	46.5	89.8	169.5	212.8	0.0866
10BASE2	185	11.75	30.731	46.5	65.48	169.5	188.48	0.1026
FOIRL	1000	7.75	107.75	29	129	152	252	0.1
10BASE-T	100	15.25	26.55	42	53.3	165	176.3	0.113
10BASE-FL	2000	12.25	212.25	33.5	233.5	156.5	356.5	0.1
Excess AUI	48	0	4.88	0	4.88	0	4.88	0.1026

Tabla 2. 5. Valores de retardo del viaje de ida y vuelta en tiempos de bit.

El estándar recomienda que se añada 5 bits al tiempo total calculado y que el resultado sea menor o igual a 575 bits. Cuando el camino tiene extremos izquierdo y derecho de diferentes tipos de cable, es preciso realizar los cálculos dos veces con los extremos invertidos porque los resultados pueden diferir. Además del tiempo de ida y vuelta es preciso calcular cuanto se reduce el tiempo entre tramas (“interframe gap shrinkage”). Este tiempo permite la recuperación de las interfaces y otros componentes entre la transmisión de dos tramas y puede verse reducido como consecuencia de los retrasos introducidos por los segmentos en la transmisión. Un intervalo muy pequeño entre tramas puede hacer que las interfaces no se aseguren la capacidad de recepción de las interfaces con la posible pérdida de tramas.

El modelo propuesto en el estándar para estos cálculos es similar al anterior con la diferencia de que sólo incluye el segmento del extremo transmisor para los cálculos.

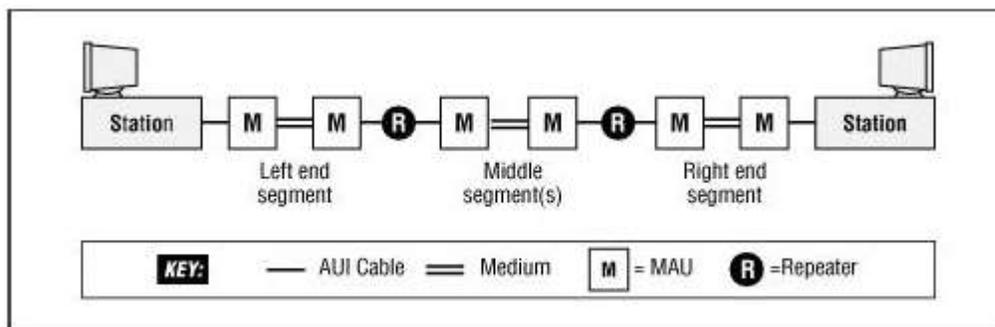


Figura 2. 2. Modelo de red para cálculo del encogimiento del espaciamiento entre tramas.

La siguiente tabla recoge los valores que deben usarse para el cálculo de encogimiento del intervalo entre tramas, cuyo valor deberá ser menor o igual que 49 bits.

CAPITULO 2. NORMAS DE CONFIGURACION Y DESEMPEÑO DE REDES LAN ETHERNET.

Tipo de Segmento	Extremo transmisor	Segmento medio
Coaxial	16	11
Segmento de enlace	10.5	8

Tabla 2. 6. Encogimiento del espaciamiento entre tramas en tiempos de bit.

2.1.2.2 CONFIGURACIÓN DE UNA ETHERNET A 100 MBPS.

Las reglas básicas del primer modelo para asegurar el funcionamiento de una red Ethernet multisegmento son las siguientes:

- Todos los segmentos de cobre deben tener una longitud menor o igual a 100 metros.
- Los segmentos de fibra deben tener una longitud menor o igual a 412 metros.
- Si se utilizan cables MII no deben exceder de 0,5 metros cada uno.

Con estas reglas en mente, la siguiente tabla recoge los diámetros máximos del dominio de colisión de segmentos utilizando repetidores Clase I y II (en Fast Ethernet existen dos tipos de repetidores, los de clase I que tienen un retardo de 1,4 ms, equivalente a 140 bits, y los de clase II que tienen un retardo de 0,92ms, equivalente a 92 bits). Este diámetro máximo del dominio de colisión es la mayor distancia que puede darse entre dos estaciones dentro de un dominio de colisión.

Tipo de repetidor	Todo Cobre	Todo Fibra	Mezcla de cobre y fibra (p.e. , T4 y FX)	Mezcla de cobre y fibra (TX y FX)
Segmento simple DTE-DTE	100	412	N/A	N/A
Un Repetidor de Clase I	200	272	231	260.8
Un Repetidor de Clase II	200	320	N/A	308.8
Dos Repetidores de Clase II	205	228	N/A	216.2

Tabla 2. 7. Modelo 1 – Máximo dominio de colisión Fast-Ethernet en metros.

El modelo 2 para Fast Ethernet resulta mucho más simple que el de Ethernet a 10 Mbps. Una vez calculado el peor camino posible, el siguiente paso es calcular el retraso total de ida y vuelta, sumando los retrasos de cada segmento individual y los retrasos introducidos por cada estación y repetidor. La siguiente tabla recoge los valores de los retrasos medidos en bits necesarios para realizar los cálculos.

CAPITULO 2. NORMAS DE CONFIGURACION Y DESEMPEÑO DE REDES LAN ETHERNET.

Componente	Retraso de ida y vuelta en bits por metro	Retraso de ida y vuelta máximo en bits
Dos DTEs TX/FX	N/A	100
Dos DTEs T4	N/A	138
Un DTE T4 y otro TX/FX	N/A	127
Cable de Categoría 3	1.14	114 (100 meters)
Cable de Categoría 4	1.14	114 (100 meters)
Cable de Categoría 5	1.112	111.2 (100 meters)
Cable STP	1.112	111.2 (100 meters)
Fibra Optica	1.0	412 (412 meters)
Repetidor de Clase I	N/A	140
Repetidor de Clase II con todos los puertos TX/FX	N/A	92
Repetidor de Clase II con algún puerto T4	N/A	67

Tabla 2. 8. Retardo de los componentes del sistema 100BaseT.

Para calcular el retraso se multiplica la longitud de los segmentos por el retraso por el valor de la tabla (si son de la longitud máxima se utiliza directamente el valor indicado en la misma). Se suma el retraso de las dos estaciones (DTEs) y el de los repetidores en el camino (los fabricantes de cables y dispositivos suelen proporcionar los valores de los retrasos de sus productos que pueden utilizarse en lugar de los de la tabla anterior, puesto que suelen ser retrasos inferiores a los recogidos en el estándar). Al resultado se le agregarán 4 bits de seguridad y el resultado debe ser menor de 512 bits.

Los retrasos de los segmentos dependen del tipo de segmento utilizado, y de la calidad del cable cuando este es de cobre. Los fabricantes suelen proporcionar un valor preciso de la velocidad de propagación de la señal por su cable o NVP (Nominal Velocity of Propagación).

2.2 NIVELES DE DESEMPEÑO.

El responsable de una red local tiene a menudo que plantearse la mejora de partes de la misma para evitar que los niveles de saturación produzcan una disminución en la calidad de servicio percibida por los usuarios. Por esta razón, las redes de datos deben tener una alta disponibilidad y confiabilidad en todos sus aspectos, para suplir las necesidades de las tareas que en ellas se soportan. Para mantenerse de esa forma, es necesario disponer de parámetros de medida objetivos y procesos de verificación de

funcionamiento que permitan comparar los niveles de calidad de servicio de acuerdo con criterios homogéneos para toda la red. Esto se debe hacer mediante un análisis de desempeño que permita ver la situación actual en la que se encuentra.

El análisis de desempeño es el estudio de la Red de Datos que permite encontrar las condiciones necesarias para su buen funcionamiento, eliminando las falencias que en ella se hallen, y que además permite la planeación de su estructuración física y lógica futura, para el soporte de los nuevos servicios a implementar. Existen dos formas de hacerlo; la primera esta basada en una técnica analítica de desempeño, y la segunda basada en un análisis práctico de desempeño. Debido a la validez de los resultados que presenta, la segunda forma de análisis es la escogida para desarrollar el estudio de la Red de Datos de la Universidad del Cauca, además se cuenta con las herramientas necesarias para hacerlo.

Este análisis se compone de dos partes, la primera es una evaluación del comportamiento de la red y la segunda es un estudio de los requerimientos de las nuevas aplicaciones por venir, para determinar su impacto.

2.2.1 EVALUACIÓN DEL COMPORTAMIENTO DE LA RED.

En esta primera parte se determina el desempeño de la red a través del estudio de las medidas que se tomen en el sistema, las tendencias de utilización de los protocolos presentes y la forma como opera cada uno de ellos. Las medidas se consiguen mediante el empleo de herramientas software, que brindan la oportunidad de trabajar con los datos reales que se manejan en la red. En el estudio de la Red de Datos de la Universidad del Cauca, las herramientas a utilizar son:

- Software Analizador de Protocolos “Agilent Advisor Software Edition”, que maneja las tecnologías Ethernet y Fast-Ethernet de redes LAN
- MRTG (Multi Router Traffic Graphic), que es una herramienta para monitorización de tráfico en tiempo real vía SNMP a través de una interfaz www.

Para un desarrollo ordenado y coherente del análisis, se deben considerar varios pasos, los cuales guiarán su realización y permitirán aprovechar al máximo las capacidades de la herramienta a emplear en la consecución de esta labor. Estos son:

- Identificación del servicio clave
- Determinación de los elementos del servicio
- Establecimiento de las medidas a tomar
- Conocimiento de los límites de desempeño
- Control de la red

El procedimiento que se presenta es el resultado de la compilación de varias técnicas usadas por los administradores de las redes LAN para conseguir una gestión de desempeño.

A continuación se describirá en que consiste cada paso de este procedimiento, y a la vez se indicará la forma como se aplican en la Red de Datos de la Universidad del Cauca.

2.2.1.1 IDENTIFICACIÓN DEL SERVICIO CLAVE

Aquí se tiene que identificar que es lo que se está tratando de gestionar, desde el punto de vista de los administradores de la red o del grupo que esté encargado de realizar el análisis. Para establecer cual es el servicio clave se debe preguntar, cuál es el servicio proporcionado a los clientes o usuarios por la parte de la red a la que se le está realizando el estudio. En el caso de la Red LAN Ethernet de la Universidad del Cauca, la definición que identifica su servicio clave, de acuerdo al propósito de este trabajo de grado, es: “La interconexión e interoperabilidad de la Red LAN, que incluye, los enlaces del backbone que interconectan switches y hubs, las conexiones de los servidores más importantes, los segmentos que componen la red de acceso local, los canales de acceso a Internet y el servicio de acceso remoto o telefónico”.

2.2.1.2 DETERMINACIÓN DE LOS ELEMENTOS DEL SERVICIO

Son los elementos individuales que se unen para proveer el servicio clave y son quienes afectan de manera conjunta el desempeño de la red. Mientras más clara haya sido la definición del servicio, la determinación de dichos elementos será más fácil.

Observando la definición del servicio clave hecha anteriormente para la Red de Datos de la Universidad del Cauca y considerando los objetivos del estudio que se está realizando en ella, los elementos del servicio en este caso son:

- El router, los switches, los hubs y los servidores
- Los enlaces del backbone que unen los switches
- Los segmentos de la red de acceso local
- Los enlaces de los servidores
- Los canales de acceso a Internet
- El enlace del servidor de acceso remoto (RAS)

2.2.1.3 ESTABLECIMIENTO DE LAS MEDIDAS A TOMAR

Habiendo identificado el servicio clave y determinado los elementos de este servicio, el siguiente paso es establecer las medidas que se requieren para describir el desempeño de la red y la forma como se van a conseguir.

Hay distintas clases de medidas para diferentes propósitos, por lo cual se debe tener una idea muy clara de lo que se quiere conseguir al elegir cada una de ellas. Existen cinco categorías de medidas basadas en la finalidad a la cual quieren servir, estas son:

1. **Servicios que proporciona la red.** En esta categoría se quiere estudiar el comportamiento del servicio o los servicios claves brindados por el sistema a sus usuarios, para esto, se utilizan las medidas que describen la calidad del servicio desde la perspectiva de un cliente de la red en términos de desempeño y disponibilidad. Dentro de las medidas apropiadas para ésta categoría están: el tiempo de respuesta del viaje de ida y vuelta de una señal, el porcentaje de disponibilidad durante un mes y el tiempo promedio para reparar un daño.
2. **Servicios que utiliza la red.** Aquí los administradores de la red requieren saber si sus proveedores de servicio están cumpliendo con el contrato de nivel de servicio estipulado anteriormente. Las medidas para este caso son las mismas que las de la primera categoría, solamente que aquí estas son específicas para la tecnología de transporte que se esté utilizando.
3. **Planeación de la capacidad.** Uno de los objetivos principales del análisis de desempeño es predecir los requerimientos de capacidad futura de la red a partir de las tendencias actuales de utilización. Las medidas esenciales en esta categoría son, el porcentaje de utilización (cuanto del ancho de banda disponible es usado) y la latencia (cuanto retardo es introducido en el transporte de datos a través de los elementos del servicio).
4. **Utilización de la red.** Una extensión de la planeación de la capacidad, es el análisis de cómo se hace la utilización de la red. Las tendencias de ésta utilización se reflejan en las medidas de los protocolos del nivel de red y del nivel de aplicación. Como un ejemplo, se podría rastrear el tráfico relacionado con HTML en los enlaces del backbone, para establecer si se despliegan o no servidores proxy en las diferentes partes de la red. Se debe tener en cuenta que la consecución de estas medidas se hace por medio de herramientas software que implican un costo adicional, pero que serán de beneficio para la administración del sistema.
5. **Salud de la red.** Por último en esta categoría se utilizan las medidas indicadoras de problemas, para estudiar las tendencias que ellas presentan y con ello solucionar el próximo inconveniente antes de que éste ocurra. La más común para la salud de la red es el número de errores asociados con un enlace particular o segmento LAN. Otras medidas de errores varían dependiendo de la tecnología que se este utilizando.

El presente estudio de la Red de Datos es realizado con el Software Analizador de Protocolos “Agilent Advisor Software Edition”, herramienta que permite tomar una gran variedad de medidas, entre las que se encuentran: número de hosts, número de conexiones, número de tramas, número de bytes y número de errores todas ellas por protocolo, número de nodos activos y muchas otras, pero de las cuales sólo son de interés y se han escogido para trabajar aquellas que ayudan a hacer una descripción objetiva del comportamiento de la Red. Estas son:

- Porcentaje de utilización
- Broadcast
- Multicast
- Eventos anormales
- Porcentaje de utilización por protocolos
- Porcentaje de utilización por protocolos del stack TCP/IP

Estas medidas se pueden situar dentro de las siguientes categorías: planeación de la capacidad, utilización y salud de la red. Los lugares claves donde se tomarán las medidas serán los elementos del servicio ya determinados: los enlaces del backbone, los principales servidores y los segmentos que constituyen la red de acceso.

Para observar el comportamiento de los canales de acceso a Internet y el servicio de acceso remoto RAS se utiliza la herramienta MRTG la cual permite conocer el ancho de banda utilizado y los periodos de tiempo de mayor utilización de los mismos.

2.2.1.4 CONOCIMIENTO DE LOS LÍMITES DE DESEMPEÑO

Son los valores individuales, ajustados a cierto nivel para cada medida, a los cuales se requiere estar consciente del comportamiento de la red, porque es cuando se pueden empezar a presentar cambios significativos en él. Usualmente se tienen dos límites para cada medida, uno para su valor promedio y el otro para su valor pico. Por lo general las herramientas de gestión poseen sus propios límites ya configurados por defecto, dependiendo de la tecnología que se este trabajando, y pueden ser una buena alternativa a utilizar cuando se vaya a empezar con un análisis y no se tenga mucha práctica con la herramienta, pero un administrador de red con experiencia variará los valores de los límites de acuerdo a sus necesidades.

Teniendo en cuenta las medidas que se escogieron para el estudio de la Red de Datos de la Universidad del Cauca, los límites para redes LAN Ethernet, de acuerdo al concepto de expertos y administradores de red, son:

- **Utilización.** En la práctica, Ethernet con su protocolo de acceso al medio CSMA/CD trabaja muy bien cuando la utilización se mantiene baja, pero su desempeño empeora exponencialmente cuando la utilización se incrementa.

Según Cisco, en el caso de una red local con decenas de estaciones por segmento se puede considerar que se da una carga excesiva en la red si se da alguna de las siguientes circunstancias:

- ✓ Se supera el 50% de ocupación durante 15 minutos, o
- ✓ Se supera el 20-30% durante una hora, o
- ✓ Se supera el 10-20% durante ocho horas.

En principio una red podría estar al 100% de ocupación durante cinco minutos, y eso no sería motivo para plantearse un aumento de capacidad. La razón es la siguiente: esa ocupación podría estar provocada por un usuario que transfiere un fichero grande (por ejemplo 400 Mbytes en una red de 10 Mbps). Si ese tipo de utilización es esporádico normalmente el tiempo de respuesta será aceptable, y si es frecuente provocará que se supere alguno de los umbrales antes mencionados.

Una posible excepción a la regla anterior serían las redes en las que se utilicen aplicaciones de tiempo real (videoconferencia o vídeo bajo demanda, por ejemplo). En este caso el criterio debería ser más exigente (por ejemplo 50% de ocupación durante 5 minutos) y aun así se pueden producir colapsos momentáneos. En realidad si se quiere utilizar este tipo de aplicaciones con garantías en una red Ethernet es preciso utilizar switches hasta el puesto del usuario final.

- **Broadcast.** La cantidad de tráfico de broadcast debe ser menor que 50 paquetes por segundo (pps).
- **Multicast.** La cantidad de tráfico de multicast debe ser menor que 40 paquetes por segundo (pps).

Otros parámetros a tener en cuenta en el análisis son los siguientes:

- La distribución de protocolos debe estar de acuerdo con los protocolos programados. Si se tiene una red TCP/IP cuyo principal uso es IP, y aparece IPX de Novell como el protocolo más usado, entonces esto indica que existen problemas de encapsulación o configuraciones inapropiadas.
- Los equipos con mayor consumo de ancho de banda (Top Talkers) deben ser usualmente los routers y los servidores. Cualquier otro dispositivo en la red con altos niveles de utilización debe ser analizado cuidadosamente.

- Un segmento Ethernet no debería contener más de 200 estaciones activas porque la demanda de la red será probablemente alta y los límites físicos de la red pueden ser fácilmente alcanzados.

2.2.1.5 CONTROL DE LA RED

Teniendo todos los elementos anteriores, se puede conseguir el desempeño de la red basándose en la comparación de las medidas obtenidas y los valores ideales de comportamiento del sistema, definiendo si éste es inferior a las expectativas o por el contrario cumple con los requerimientos de las aplicaciones y usuarios. El buen manejo de los resultados de este estudio proveerá el control de la red junto con la identificación y aislamiento de los problemas para su posterior solución.

2.2.2 REQUERIMIENTOS DE LAS NUEVAS APLICACIONES.

La función de ésta parte recae en la búsqueda de los requerimientos de las nuevas aplicaciones que se tienen pensadas implementar en un futuro, para considerar su impacto en el desempeño de la red y planear con anticipación los cambios a realizar, de esa forma cuando se empiecen a utilizar su introducción no sea traumática sino algo normal que se estaba esperando.

El impacto de las nuevas aplicaciones se puede anticipar con la ayuda de un proceso de cinco pasos:

1. Análisis de las transacciones. Se determina cuales son los diferentes tipos de interacciones de usuario realizadas con las aplicaciones existentes y la cantidad de tráfico de datos asociado a cada una de ellas.
2. Análisis de los usuarios. Se identifican cuales son las principales clases de usuario con su respectivo perfil de transacciones, además de la distribución o ubicación de cada una de las clases en la red.
3. Modelo de aplicación. Combina la información de cada uno de los pasos anteriores para establecer el perfil de cada enlace de la red con el nuevo tráfico adicional. Una manera de hacerlo y que puede resultar efectiva si no se tiene una red muy grande, es coger un diagrama de su infraestructura, unir los perfiles del nuevo tráfico de los varios usuarios e ir adicionándolos en forma de enlaces en la red.
4. Modelo del impacto en la red. Se consigue sobreponiendo el modelo de aplicación sobre el perfil de tráfico existente, para determinar los requerimientos de capacidad total de la red una vez las nuevas aplicaciones aparezcan.
5. Rediseño de la red. Aquí se determina donde es requerida la capacidad adicional o que cambios en el diseño de la red deben hacerse para el soporte de las nuevas aplicaciones.

3. ANALISIS DEL DESEMPEÑO DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

Tomando como referencia la infraestructura y funcionamiento de la Red de Datos detallada en el Capítulo 1, en conjunto con las reglas de configuración de la tecnología Ethernet y el método para medir su desempeño planteados en el Capítulo 2, a continuación se evalúa la topología física y se realiza el análisis del desempeño de la Red de Datos de la Universidad del Cauca. Para ello se empieza examinando su infraestructura y se verifica que cumpla con las normas del estándar IEEE 802.3. Finalmente, se realiza el análisis del desempeño de los segmentos y enlaces que conforman la Red, presentando los resultados de las medidas estipuladas anteriormente y profundizando en los problemas que con ellas se evidencian.

3.1 ANALISIS DE LA INFRAESTRUCTURA FISICA.

Con el levantamiento de la Red de Datos realizado en el Capítulo 1 de este documento, se pudo conocer la infraestructura física y el funcionamiento lógico de la misma. Por esta razón, la evaluación de la infraestructura de la Red se hace relativamente sencilla, analizando a cada uno de sus segmentos de acuerdo a las reglas de configuración Ethernet consignadas en el capítulo anterior, con el objetivo de obtener niveles de desempeño óptimos en cada uno de ellos. De esta forma se determina que:

- En general, las distancias máximas de los medios de comunicación utilizados, tanto en UTP como en fibra óptica, se mantienen por debajo de los límites establecidos en las reglas de configuración, porque han sido instalados bajo las exigencias del estándar de cableado estructurado.
- El segmento **STOCC1SW1 – STOCC6HUB1** ubicado en el sector de Santo Domingo excede la distancia máxima de 100 metros permitida por el estándar, lo cual afecta el desempeño del enlace.
- El segmento **STOCC1SW1 – STOCC4HUB2** ubicado también en el sector de Santo Domingo se encuentra al límite de la distancia máxima permitida lo cual puede ser inadecuado para su correcto funcionamiento.
- Los segmentos que presentan varios hubs en cascada, están bien configurados en cuanto al número de repetidores que les son permitido utilizar por las reglas de configuración. Lo que se verifica al observar los diagramas del Capítulo 1.

Esta evaluación permite concluir que la Red no presenta problemas de configuración en sus instalaciones de cableado, a excepción de los segmentos mencionados anteriormente.

3.2 ANALISIS DE DESEMPEÑO.

Continuando con el desarrollo del procedimiento del análisis, en ésta parte del documento se presentan las observaciones de los resultados de las medidas tomadas en cada uno de los elementos (enlaces del backbone, principales servidores, segmentos que constituyen la red de acceso, canales de acceso a Internet y RAS) del servicio clave que se está analizando: la interconexión e interoperabilidad de la Red LAN de la Universidad del Cauca, con el fin de detectar los problemas de la Red de Datos y buscar su pronta solución.

Las medidas se realizaron con el Software Analizador de Protocolos “Agilent Advisor Software Edition” y la herramienta de gestión MRTG. Las medidas se llevaron a cabo en horarios de oficina, de 8 a 12 a.m. y de 2 a 6 p.m. Se tomaron de tres a cuatro medidas para cada uno de los elementos del servicio, por periodos de una hora cada una de ellas.

A continuación se describirá cada una de las medidas establecidas previamente para una mejor comprensión de las mismas:

PORCENTAJE DE UTILIZACIÓN: Es una estadística muy importante, que indica cuanto del ancho de banda de la red (enlace o segmento) está siendo empleado. Esta medida se presenta como un porcentaje de la capacidad total del enlace o segmento que se está midiendo, en donde un alto porcentaje de utilización quiere decir que existen niveles excesivos de tráfico. Por ejemplo, si se mide el enlace en fibra óptica entre el IPET e Ingenierías (enlace a 100 Mbps Full-Duplex) y se encuentra un porcentaje de utilización del 5%, esto quiere decir que de los 200 Mbps (máxima tasa de línea para Fast-Ethernet Full-Duplex) de ancho de banda, se está transmitiendo 10 megabits de información cada segundo.

BROADCAST: Una trama de broadcast ocurre cuando una trama con la dirección de destino FF-FF-FF-FF-FF-FF es transmitida. Estas tramas son comúnmente usadas, por lo cual se debe esperar moderadas cantidades de ellas en un segundo. Su importancia se debe a que cada equipo en la red debe gastar tiempo al recibirlas y procesarlas, con lo que sí se presentan ráfagas de estas tramas, se podría causar grandes problemas para algunos equipos de la red.

Esta medida es presentada como un porcentaje del total de tramas. Una alta proporción de tramas de broadcast es común en redes con baja utilización porque ellas representan operaciones de segundo plano que ocurren independientemente del tráfico de usuario, en ésta situación el broadcast sería quien generaría la mayoría de tráfico existente. Pero si la utilización de la red es alta y el broadcast también lo es, una investigación del origen de estas tramas debe realizarse con el fin de reducirlas.

MULTICAST: Una trama multicast ocurre cuando una trama es recibida con una dirección de destino de un grupo. Estas direcciones tienen el bit menos significativo del byte más significativo fijado en 1. En Ethernet, éstas comprenden cualquier dirección donde el primer byte de la dirección es un número impar, por ejemplo 01-XX-XX-XX-XX-XX. Su importancia se debe a que, como el broadcast, las tramas de multicast representan tiempo de procesamiento para todos los equipos que sean miembros del grupo. Estas tramas son comunes en muchas redes, pero ocurren en menor frecuencia que el broadcast.

Esta medida es presentada como un porcentaje del total de tramas. Este porcentaje varía ampliamente entre las redes, por ejemplo, en las aplicaciones de red más nuevas se usa el multicasting para reducir la carga en la red cuando se transmite la misma información a muchos lugares, caso en el cual, un porcentaje alto será normal. Por el incremento en la carga de procesamiento que el multicast ocasiona en los equipos receptores, un alto nivel requiere de una investigación sobre las aplicaciones que lo genera, con el fin de confirmar su configuración eficiente.

EVENTOS ANORMALES: Los eventos anormales de la Red causan un decremento en la salud de la Red. Estos eventos son reportados por el analizador de protocolos como *Advertencia y Alertas*. Un evento de Advertencia significa que existe un posible error en la red y un evento de Alerta indica que realmente hay problemas en la red y requieren atención inmediata. En el análisis se tendrán en cuenta los eventos anormales detectados a nivel de RED y TRANSPORTE, entre los cuales se tienen:

- **IP Zero Time To Live:** Este mensaje es considerado como un evento de Alerta, el cual es generado cuando es detectada una trama con un valor en el campo TTL menor o igual a 1. Un valor en el campo TTL menor o igual a 1, significa que el destino del paquete debería estar en la red. Si el destino no está presente en ésta red, el paquete es descartado.
- **IP Duplicate Address:** Este mensaje es considerado como un evento de Alerta, y se genera cuando dos direcciones físicas MAC comparten erróneamente la misma dirección lógica IP.

- **TCP Low Window:** Este mensaje es considerado como un evento de Advertencia. Este evento ocurre cuando el tamaño de la ventana enviado por el receptor en el segmento TCP es igual a 0 y se mantiene así por más de 5 segundos.
- **TCP Excessive Retransmission:** Este mensaje es considerado como un evento de Advertencia. Este evento es generado si se cumple cualquiera de las siguientes condiciones:
 - ✓ Se han retransmitido más de 3 tramas TCP consecutivamente.
 - ✓ Se han transmitido menos de 10 tramas en una conexión, de las cuales:
 - Se han realizado 2 retransmisiones TCP de un total de 3 o 4 tramas transmitidas.
 - Se han realizado 3 retransmisiones TCP de un total de 5, 6 o 7 tramas transmitidas.
 - Se han realizado 4 retransmisiones TCP de un total de 8 o 9 tramas transmitidas.

Otros eventos anormales que se tendrán en cuenta en el análisis son los detectados por el analizador en las conexiones realizadas con bases de datos Oracle; lo cual es importante ya que los sistemas de información de la Universidad del Cauca utilizan este tipo de plataforma. Entre estos eventos se tiene:

- **Oracle TNS Slow Server Response:** Este mensaje es considerado como un evento de Advertencia, el cual es causado por una trama de respuesta tardía enviada por un servidor. Si el tiempo entre un requerimiento del cliente y la respuesta del servidor es mayor que el umbral (por defecto 150 ms), la respuesta del servidor es considerada tardía.
- **Oracle TNS Marker:** Este mensaje es considerado como un mensaje de Advertencia. Este mensaje es desplegado cuando se detecta una trama de tipo Marker/Attention. Esta trama es un requerimiento de interrupción la cual cierra y resetea la conexión. Este tipo de mensajes son utilizados por los clientes para decirle al servidor que pare de enviar datos, debido a que el cliente no tiene suficiente memoria para procesar los datos a la velocidad que están siendo enviados por el servidor.

PORCENTAJE DE UTILIZACIÓN POR PROTOCOLOS: Indica que stack de protocolos (TCP/IP, Novell, NetBEUI, AppleTalk, IPv6, otros) están siendo utilizados por los equipos dentro del segmento que se está midiendo, y la proporción de utilización de cada uno de ellos. Para esta medida se tienen en cuenta dos aspectos, la cantidad de tramas generadas por los protocolos del stack y los bytes

enviados por cada protocolo durante el tiempo de medición. Cada una de estas medidas es presentada como un porcentaje de la utilización, es decir del total de bytes y del total de tramas transmitidas.

PORCENTAJE DE UTILIZACIÓN POR PROTOCOLOS DEL STACK TCP/IP: Indica que protocolos del Stack TCP/IP (HTTP, FTP, Telnet, SNMP, SMTP, etc.) están siendo usados por los equipos dentro del segmento que se está midiendo, y la proporción de utilización de cada uno de ellos. Aquí se tienen en cuenta dos aspectos, al igual que en la medida anterior, la cantidad de tramas generadas por el protocolo y los bytes enviados por cada protocolo durante el tiempo de medición, aspectos que son presentados como un porcentaje del total de tráfico TCP/IP, es decir del total de tramas y bytes TCP/IP.

Cada una de las medidas se expondrá en tablas¹ presentando los siguientes campos: valor promedio, valor máximo y valor umbral, los cuales se interpretan de la siguiente manera:

El valor promedio de la medida de Utilización se obtiene al promediar todas las muestras tomadas (muestreo cada 10 segundos) durante el periodo de medición; el resultado no es exacto ya que se fundamenta en muestras. Para las medidas de broadcast y multicast, el valor promedio se consigue con base en la totalidad de las tramas en cuestión con respecto al total de tramas que se transmitieron durante el periodo de medición.

Los valores máximos se refieren a los picos de la medida. Por ejemplo un máximo de 45% en la utilización de un segmento, indica que la utilización del segmento alcanzó ese porcentaje de la capacidad durante un momento cualquiera de la medición. En cambio, un valor máximo de las medidas de broadcast o multicast, se refieren a un pico en el porcentaje de tramas del tipo en cuestión con respecto al total de tramas.

El valor umbral indica cuantas veces se excede el umbral de una medida determinada, durante el periodo de medición; los umbrales de las medidas se muestran en la Tabla 3.1. Por ejemplo, un valor de umbral de 100 para la medida de Utilización indica que la utilización sobrepasó el 40% de la capacidad del canal 100 veces durante el periodo de medición.

¹ Las tablas del estudio realizado para cada uno de los segmentos y enlaces se exponen en el anexo C. Como ejemplo se presenta la tabla del enlace Switch Accelar 1200 - Cisco 3600 en la sección 3.2.5.1.

MEDIDA	UMBRAL
Utilización	40%
Broadcast	50 paquetes por segundo. (50 pps)
Multicast	40 paquetes por segundo. (40 pps)

Tabla 3. 1. Umbrales de las medidas.

A continuación se presentan los principales resultados de las mediciones, organizados según la ubicación de los sitios dentro de la estructura de la Red donde se realizó la medida.

3.2.1 ANALISIS DEL ACCESO A INTERNET

El análisis del acceso a Internet se realiza teniendo en cuenta las gráficas del MRTG que se encuentran alojadas en el servidor CERES, las cuales se actualizan constantemente.

3.2.1.1 ENRUTADOR TELECOM: ROUTER CISCO 1700

El canal tiene un ancho de banda de 2 Mbps. En la siguiente gráfica se observa el comportamiento del tráfico durante el último año.

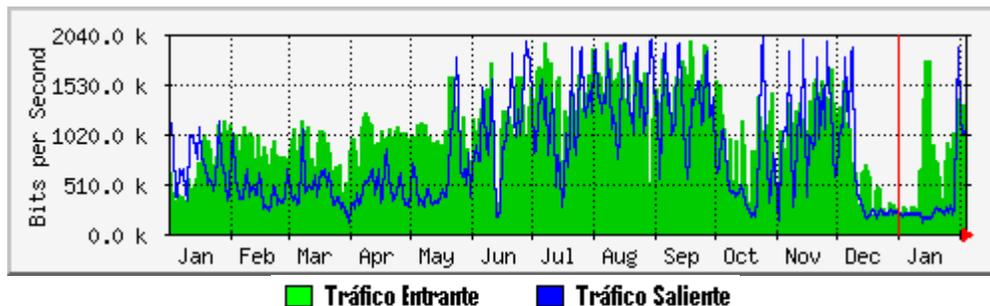


Figura 3. 1. Niveles de tráfico del acceso a Internet a través del canal de TELECOM

- La cantidad promedio de tráfico entrante es 1030.2 Kbps lo que representa el 50.3% de utilización del canal.
- La cantidad promedio de tráfico saliente es 794.2 Kbps lo que representa el 38.8% de utilización del canal.
- El valor máximo de tráfico entrante que se presenta en el periodo de medición es 1982.1 Kbps, lo que significa que en un instante específico el canal tiene un nivel de utilización del 96.8%.

- El valor máximo de tráfico saliente que se presenta en el periodo de medición es 2003.1 Kbps, lo que significa que en un instante específico el canal tiene un nivel de utilización del 97.8%.
- En general, teniendo en cuenta el tráfico entrante y saliente, el canal presenta un nivel de utilización promedio del 89.1% de su capacidad total.

3.2.1.2 ENRUTADOR EMTTEL: ROUTER CISCO 3600

El enlace tiene un ancho de banda de 4 Mbps, distribuidos en dos canales de 2 Mbps cada uno. En las figuras 3.2 y 3.3 se observa el comportamiento del tráfico a partir del mes de octubre del 2004, fecha en la que comenzó a funcionar el enlace.

CANAL No. 1

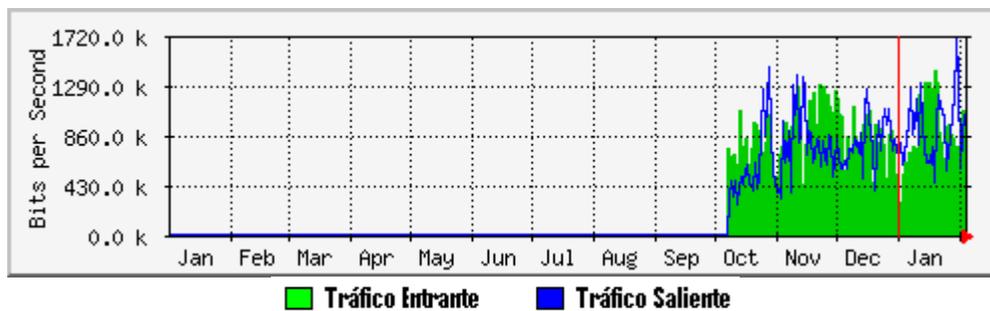


Figura 3. 2. Niveles de tráfico del acceso a Internet a través del canal 1 de EMTTEL

- La cantidad promedio de tráfico entrante es 829.6 Kbps lo que representa el 40.5% de utilización del canal.
- La cantidad promedio de tráfico saliente es 803.5 Kbps lo que representa el 39.2% de utilización del canal.
- El valor máximo de tráfico entrante que se presenta en el periodo de medición es 1442.9 Kbps, lo que significa que en un instante específico el canal tiene un nivel de utilización del 70.5%.
- El valor máximo de tráfico saliente que se presenta en el periodo de medición es 1705.8 Kbps, lo que significa que en un instante específico el canal tiene un nivel de utilización del 83.3%.
- Teniendo en cuenta el tráfico entrante y saliente, el canal presenta un nivel de utilización promedio del 79.7% de su capacidad total.

CANAL No. 2

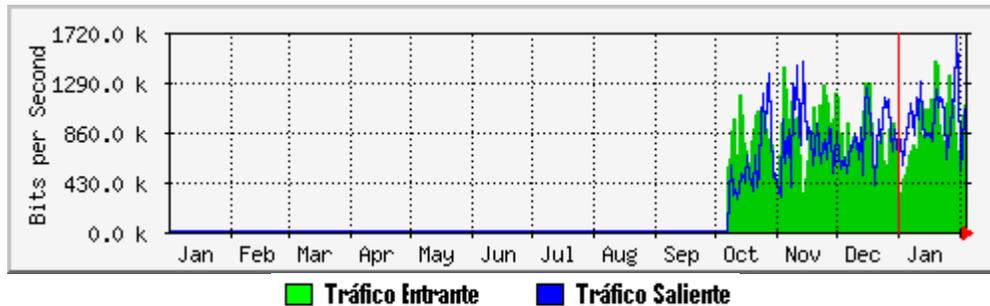


Figura 3. 3. Niveles de tráfico del acceso a Internet a través del canal 2 de EMTel

- La cantidad promedio de tráfico entrante es 824.3 Kbps lo que representa el 40.2% de utilización del canal.
- La cantidad promedio de tráfico saliente es 817 Kbps lo que representa el 39.9% de utilización del canal.
- El valor máximo de tráfico entrante que se presenta en el periodo de medición es 1493.1 Kbps, lo que significa que en un instante específico el canal tiene un nivel de utilización del 72.9%.
- El valor máximo de tráfico saliente que se presenta en el periodo de medición es 1710.4 Kbps, lo que significa que en un instante específico el canal tiene un nivel de utilización del 83.5%.
- Teniendo en cuenta el tráfico entrante y saliente, el canal presenta un nivel de utilización promedio del 80.1% de su capacidad total.

3.2.2 CONCLUSIONES DEL ACCESO A INTERNET

- Los niveles de utilización de los canales de acceso a los proveedores de Internet (Telecom y Emtel) son muy altos, alcanzando en promedio el 85% de la capacidad de los canales, lo cual indica que hay problemas de congestión.
- El canal de acceso a Telecom es el más congestionado ya que los valores promedio y pico del tráfico de este enlace son superiores a los presentados en los canales de acceso de Emtel.
- Los valores máximos del tráfico saliente son siempre superiores a los valores máximos del tráfico entrante.
- Los dos canales de acceso a Internet a través de Emtel presentan los mismos niveles de utilización, lo que indica que la carga de tráfico se distribuye equitativamente a través de estos dos canales.

3.2.3 ANALISIS DEL ACCESO REMOTO (RAS)

El acceso remoto o acceso telefónico se hace por medio de una enlace primario RDSI para 30 canales (los cuales permiten una velocidad máxima de 56 Kbps si el usuario se conecta a través de una line telefónica analógica; 64 Kbps cuando el usuario tiene el servicio RDSI; y 128 Kbps cuando tiene el servicio RDSI y utiliza los dos canales B); enlace provisto por la empresa Emtel. En la figura 3.4 se observa el comportamiento del tráfico del RAS durante el último año.

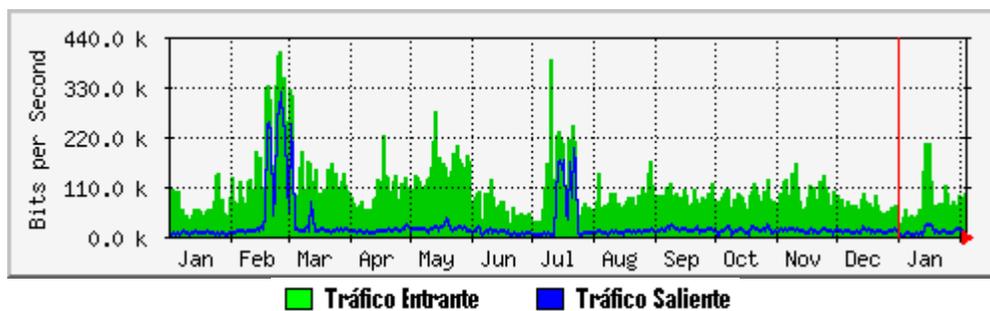


Figura 3. 4. Niveles de utilización del RAS durante un año

- La cantidad promedio de tráfico entrante es 103 Kbps lo que representa el 5.03% de utilización del enlace primario.
- La cantidad promedio de tráfico saliente es 24.7 Kbps lo que representa el 1.21% de utilización del enlace primario.
- El valor máximo de tráfico entrante que se presenta en el periodo de medición es 413.2 Kbps, lo que significa que en un instante específico el enlace primario tiene un nivel de utilización del 20.18%.
- El valor máximo de tráfico saliente que se presenta en el periodo de medición es 320.3 Kbps, lo que significa que en un instante específico el canal tiene un nivel de utilización del 15.64%.

En la figura 3.5 y 3.6 se observa el comportamiento del tráfico del RAS durante una semana y durante un día respectivamente.

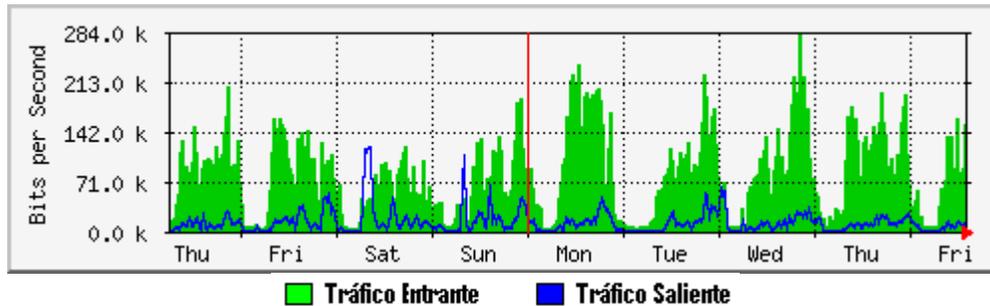


Figura 3. 5. Niveles de utilización del RAS durante una semana

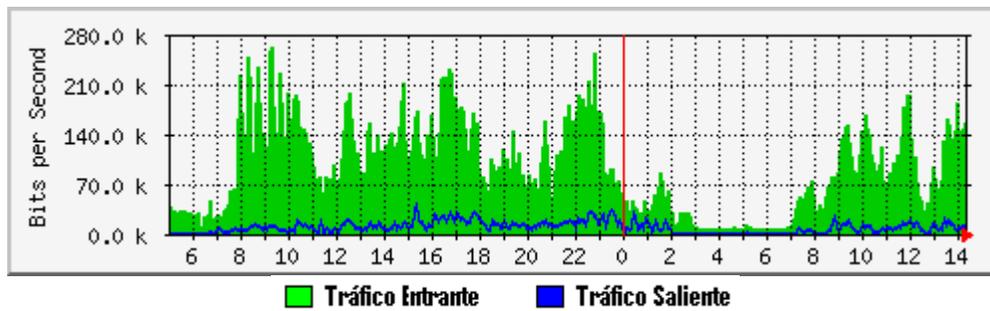


Figura 3. 6. Niveles de utilización del RAS durante un día

3.2.4 CONCLUSIONES DEL ACCESO REMOTO (RAS)

- El nivel de utilización promedio del RAS es 6.24%.
- Durante el último año, los meses que presentan mayores niveles de utilización son Febrero y Julio. Esto es debido a que en estos periodos se llevan a cabo los procesos de admisión de la Universidad del Cauca.
- Como se puede observar en la figura 3.5, los días que presentan mayores niveles de utilización son LUNES y MIÉRCOLES. Por el contrario, los fines de semana son los días de menor utilización.
- En la figura 3.6. se puede apreciar que el tráfico es relativamente constante durante la mayor parte del día, pero entre las 2:00 a.m. y las 7:00 am. los niveles de tráfico son casi nulos.

3.2.5 ANALISIS DEL BACKBONE

Todos los enlaces del backbone funcionan a 100 Mbps en modo Full Duplex.

CAPITULO 3. ANALISIS DEL DESEMPEÑO DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

3.2.5.1 ENLACE SWITCH ACCELAR 1200 – ROUTER CISCO 3600 (INGCC5SW1 – CISCO 3600)

NOMBRE DE LA ESTADÍSTICA	PROMEDIO	MÁXIMO	UMBRAL
Utilización (% de la Capacidad).	2,18	3,62	0
Broadcast (% de Tramas).	6,94	78,63	-
Multicast (% de Tramas).	0,43	10,15	-

Tabla 3. 2. Estadísticas del Enlace Switch Accelar 1200 – Router Cisco 3600.

STACK DE PROTOCOLOS / PROTOCOLO	TRAMAS (%)	BYTES (%)
TCP/IP	99,2736	99,8429
TCP/UDP USER PORTS --	46,5301	51,0828
WWW 80	37,8974	37,7363
SMTP 25	1,3714	4,2296
TCP - Port 22	0,7638	1,3556
DNS 53	3,4940	0,9656
ICMP1	3,5037	0,8474
NETBIOS 137	2,5582	0,6564
HA - CLUSTER 694	0,9224	0,3451
FTP 20	0,5252	0,2674
SNMP 161	0,9727	0,1881
IMAPS 993	0,1909	0,0428
IPP 631	0,1070	0,0265
RIP 520	0,0958	0,0216
HTTPS 443	0,0905	0,0216
TFTP 69	0,0147	0,0180
LOC-SRV 135	0,0568	0,0081
IP-Type 41	0,0327	0,0076
MICROSOFT - DS 445	0,0273	0,0035
IGMP2	0,0190	0,0024
BOOTP 67	0,0018	0,0010
TCPMUX 1	0,0012	0,0002
NAMESERVER 42	0,0014	0,0002
NTP 123	0,0009	0,0002
SYSTAT 11	0,0007	0,0001
RPC 111	0,0006	0,0001
Novell	0,3002	0,0690
NetBEUI	0,1511	0,0478
Other	0,2741	0,0402
IPv6	0,0007	0,0001
AppleTalk	0,0002	0,0000

Tabla 3. 3. Tendencias de Protocolos del Enlace Switch Accelar – Router Cisco 3600.

- Las utilizaciones promedio y pico son del 2.18% y 3.62% respectivamente.
- Las tramas de broadcast representan el 6.94% del total de tramas del enlace.²
- Las tramas de multicast representan el 0.43% del total de tramas del enlace.
- El protocolo TCP/UDP USER PORTS³ es el principal consumidor de ancho de banda con el 51.08% del total del tráfico TCP/IP y es generado en su mayoría por usuarios que utilizan direcciones públicas asignadas por Emtel.
- El protocolo WWW 80 es el segundo protocolo más utilizado con un porcentaje del 37.74%, seguido por el protocolo SMTP 25 con el 4.23% y TCP Puerto 22⁴ con el 1.36%.
- El enlace presenta una gran cantidad de eventos de Advertencia “TCP Low Window” y “TCP Excessive Retransmission”. La mayoría de estos mensajes se presentan en las conexiones que el Servidor de Proxy TEMIS establece con servidores externos.
- La siguiente gráfica ilustra los eventos mencionados anteriormente. La escala superior indica el estado de salud de la red. (En presencia de mensajes de Advertencia y Alertas, el estado de salud de la red puede disminuir desde el 100% hasta el 0%, dependiendo de la cantidad de eventos generados). La escala inferior indica el nivel de utilización de la red debido al tráfico IP generado.

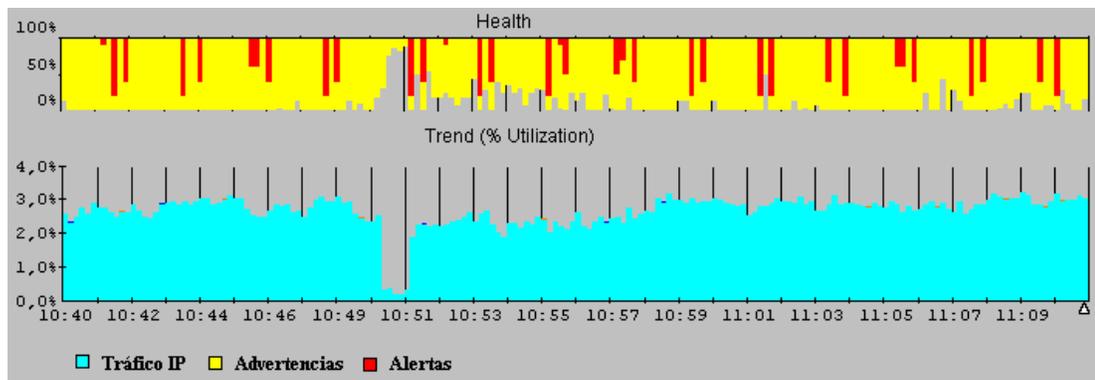


Figura 3. 7 Eventos generados en el enlace SWITCH ACCELAR 1200 - ROUTER CISCO 3600

² Los porcentajes de Broadcast y Multicast representan la proporción del impacto de este tipo de tráfico en el segmento o enlace en comparación con el Unicast.

³ El protocolo TCP/UDP USER PORTS representa el tráfico de las aplicaciones que utilizan los puertos mayores a 1000; entre estos se encuentra el puerto 3128 (Proxy 3128) mediante el cual se tiene configurado el servicio de Proxy para el acceso a Internet.

⁴ El protocolo TCP Puerto 22 (SSH Remote Login Protocol) se utiliza para realizar conexiones seguras de correo electrónico y transferencia de archivos

3.2.5.2 ENLACE SWITCH ACCELAR 1200 – ROUTER CISCO 1700 (INGCC5SW1 – CISCO 1700)

- Las utilizaciones promedio y pico son del 1.00% y 3.43% respectivamente.
- Las tramas de broadcast constituyen el 14.21% del total de tramas del enlace.
- Las tramas de multicast constituyen el 0.28% del total de tramas del enlace.
- El protocolo WWW 80 es el principal consumidor de ancho de banda con el 85.43% del total del tráfico TCP/IP.
- El protocolo TCP/UDP USER PORTS es el segundo protocolo más utilizado con un porcentaje del 5.30% y es originado por usuarios con direcciones IP privadas que acceden a Internet a través del Proxy,
- El protocolo NETBIOS 137⁵ es el tercer protocolo más utilizado con un porcentaje del 4.17% y DNS 53 con el 2.61%.
- El enlace presenta eventos de Advertencia “TCP Low Window” y “TCP Excessive Retransmission”, aunque en menor proporción que el enlace anterior. La mayoría de estos mensajes se presentan en las conexiones que el Servidor de Proxy HIPERION establece con servidores externos.

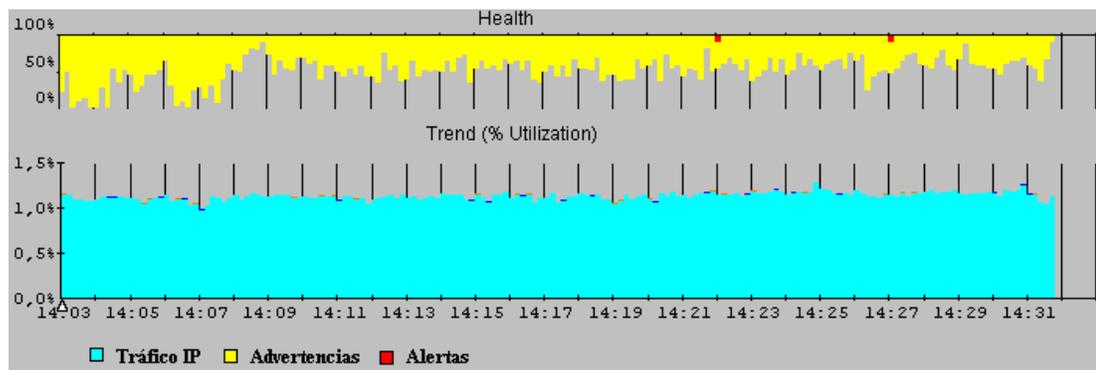


Figura 3. 8. Eventos generados en el enlace SWITCH ACCELAR 1200 - ROUTER CISCO 1700

3.2.5.3 ENLACE IPET - INGENIERIAS (INGCC5SW1 – INGCC1SW1)

- Las utilizaciones promedio y pico son del 1.05% y 13.29% respectivamente.
- Las tramas de broadcast representan el 11.11% del total de tramas del enlace.
- Las tramas de multicast representan el 0.84% del total de tramas del enlace.
- El protocolo PROXY 3128 es el principal consumidor de ancho de banda con el 53.77% del total del tráfico TCP/IP.

⁵ Este protocolo es utilizado para soportar la red Microsoft y la comunicación entre aplicaciones tipo Windows.

- El protocolo MICROSOFT-DS 445⁶ es el segundo protocolo más utilizado con un porcentaje del 21.59%, seguido por NETRJS3 73⁷ con el 15.43%, SSH 22 con el 3.90% y NETBIOS 137 con 2.82%.
- El enlace presenta eventos “TCP Excessive Retransmission”, que en su mayoría tienen su origen en las conexiones realizadas entre los proxies y algunos clientes del sector.
- Los eventos de Alerta observados en el enlace son debido a la presencia de mensajes “Zero Time To Live”.

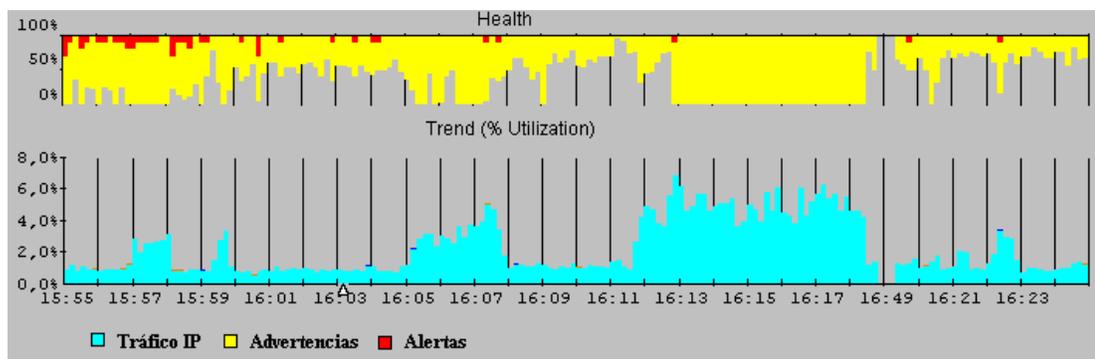


Figura 3. 9. Eventos generados en el enlace IPET - INGENIERIAS

3.2.5.4 ENLACE IPET - EDUCACION (INGCC5SW1 – EDUCC1SW1)

- Las utilizaciones promedio y pico son del 0.98% y 6.63% respectivamente.
- Las tramas de broadcast constituyen el 12.04% del total de tramas del enlace.
- Las tramas de multicast constituyen el 0.89% del total de tramas del enlace.
- El protocolo PROXY 3128 es el principal consumidor de ancho de banda con el 51.82% del total del tráfico TCP/IP.
- El protocolo MICROSOFT-DS 445 es el segundo protocolo más utilizado con un porcentaje del 31.49%, seguido por NETBIOS 137 con el 7.50%, ICMP 1 con el 1.03% y TCP Oracle TNS⁸ con 1.01%.
- El enlace presenta eventos “TCP Excessive Retransmission”, que generalmente tienen su origen en las conexiones realizadas entre los proxies y algunos clientes del sector.

⁶ El protocolo Microsoft-ds es usado para compartir recursos y archivos SMB (Server Message Block) en Windows 2000 y XP a través de la red.

⁷ Remote Job Service

⁸ Este protocolo es utilizado por las aplicaciones de bases de datos Oracle.

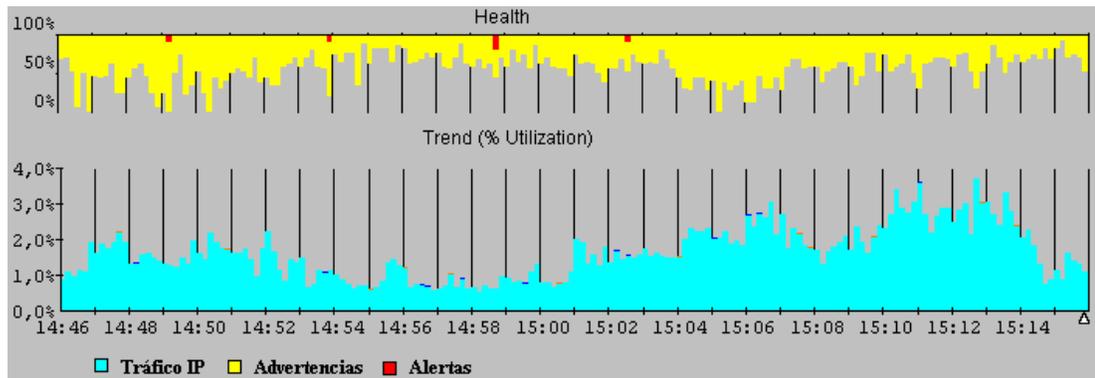


Figura 3. 10. Eventos generados en el enlace IPET - EDUCACION

3.2.5.5 ENLACE IPET – EL CARMEN (INGCC5SW1 – CARCC1SW1)

- Las utilizaciones promedio y pico son del 0.35% y 6.39% respectivamente.
- El 30.18% del total de tramas del enlace son tramas de broadcast.
- El 2.25% del total de tramas del enlace son tramas de multicast.
- El protocolo PROXY 3128 es el principal consumidor de ancho de banda con el 55.48% del total del tráfico TCP/IP.
- El protocolo NETBIOS 137 es el segundo protocolo más utilizado con un porcentaje del 20.25%, seguido por POP3 110 con el 14.80%, HA-CLUSTER 694⁹ con el 2.68% y DNS 53 con 2.23%.
- El estado del enlace es bueno y presenta muy pocos problemas a nivel de los protocolos IP y TCP.

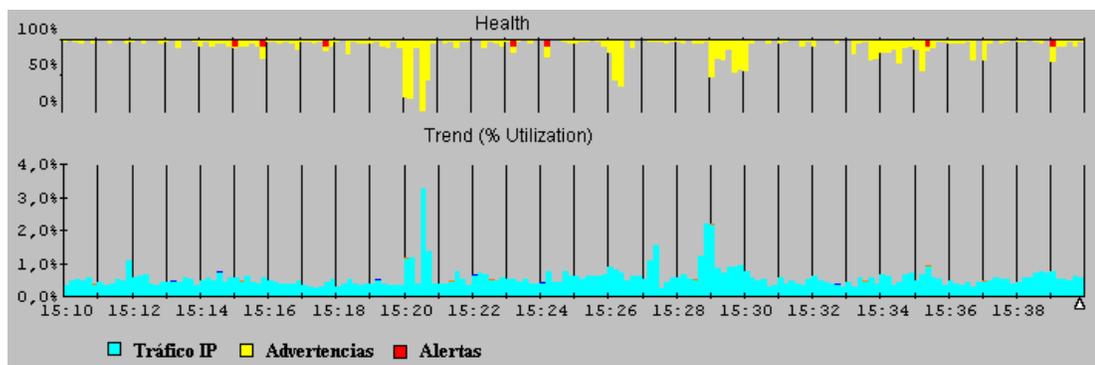


Figura 3. 11. Eventos generados en el enlace IPET - EL CARMEN

⁹ El protocolo HA-CLUSTER 694 es utilizado para clustering de alta disponibilidad, es decir, tener redundancia en los servidores para crear un sistema de respaldo, que monitoree constantemente la acción de un servidor primario de forma automática, y que al mismo tiempo este activo y monitoreando el comportamiento de los demás nodos que conforman dicha LAN.

3.2.5.6 ENLACE IPET – SANTO DOMINGO (INGCC5SW1 – STOCC1SW1)

- Las utilizaciones promedio y pico son del 0.72% y 6.17% respectivamente.
- Las tramas de broadcast representan el 28.81% del total de tramas del enlace.
- Las tramas de multicast representan el 1.91% del total de tramas del enlace.
- El protocolo NETBIOS 137 es el principal consumidor de ancho de banda con el 41.25% del total del tráfico TCP/IP.
- El protocolo PROXY 3128 es el segundo protocolo más utilizado con un porcentaje del 24.37%, seguido por TCP Oracle TNS con el 17.72%, MICROSOFT-DS 445 con el 13.32% y HA-CLUSTER 694 con el 1.21%
- El enlace presenta eventos “TCP Excessive Retransmission” que tienen su origen en las conexiones de los proxies y el servidor de aplicaciones de finanzas EOWIN¹⁰ con algunos clientes de este sector. Además Se presentan una gran cantidad de eventos de Alerta debido a la presencia de mensajes “Zero Time To Live”.

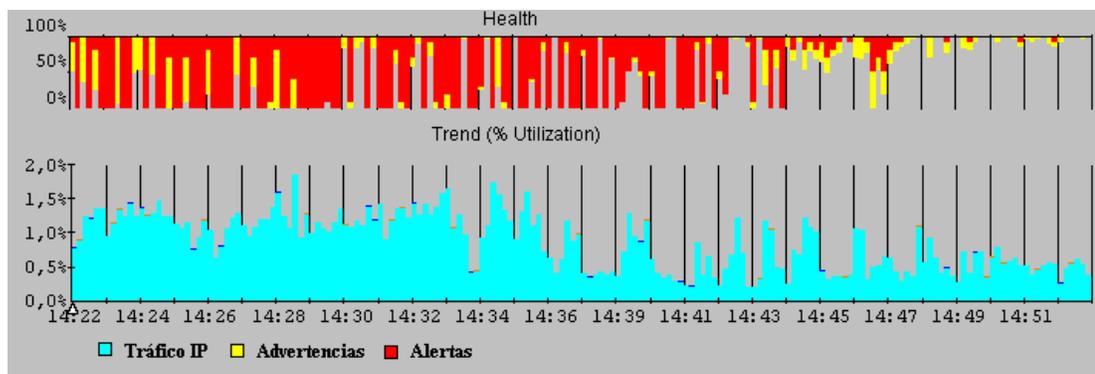


Figura 3. 12. Eventos generados en el enlace IPET - SANTO DOMINGO

3.2.5.7 ENLACE CARMEN – VRI (CARCC1SW1- VRICC1SW1)

- Las utilizaciones promedio y pico son de 0.15% y 3.92% respectivamente.
- Las tramas de broadcast representan el 52.46% del total de tramas del enlace.
- Las tramas de multicast representan el 3.65% del total de tramas del enlace.
- El protocolo de mayor utilización es PROXY 3128 con 40.10%, seguido por NETBIOS 137 con 30.76%, WWW 80 con 18.61%, HA-CLUSTER 694 con 5.30% y DNS 53 1.05%.
- Se observan una gran cantidad de eventos de Alerta debido a la presencia de mensajes “Zero Time To Live” y eventos de Advertencia “TCP Excessive Retransmission”.

¹⁰ El análisis de los eventos presentados entre el servidor EOWIN y sus clientes son analizados más adelante en la sección 3.2.15.

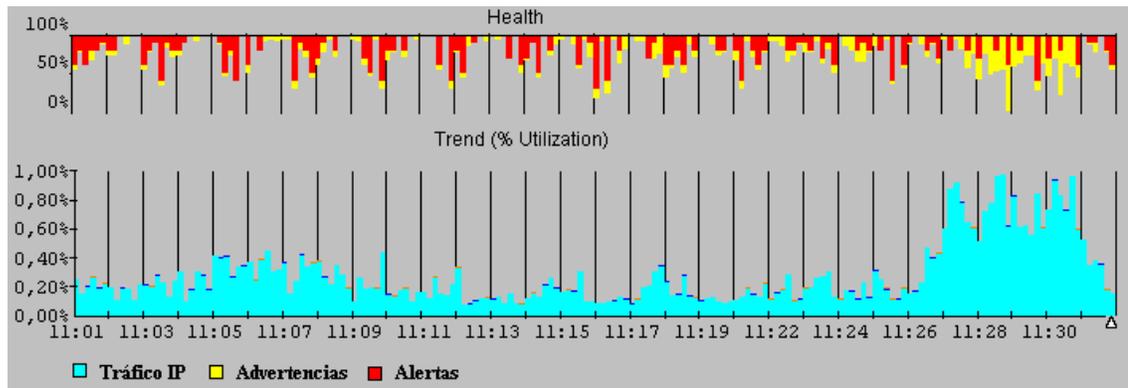


Figura 3. 13. Eventos generados en el enlace VRI - EL CARMEN

3.2.5.8 ENLACE IPET – MEDICINA (INGCC5SW1 – MEDCC1SW1)

- Las utilizaciones promedio y pico son del 0.31% y 4.53% respectivamente.
- Las tramas de broadcast representan el 58.07% del total de tramas del enlace.
- Las tramas de multicast representan el 3.09% del total de tramas del enlace.
- El protocolo PROXY 3128 es el principal consumidor de ancho de banda con el 40.82% del total del tráfico TCP/IP.
- El protocolo NETBIOS 137 es el segundo protocolo más utilizado con un porcentaje del 27.76%, seguido por MICROSOFT-DS 445 con el 20.36%, NETRJS 373 con el 4.54% y HA-CLUSTER 694 con el 3.33%.
- El estado del enlace es bueno y presenta muy pocos problemas a nivel de los protocolos IP y TCP.

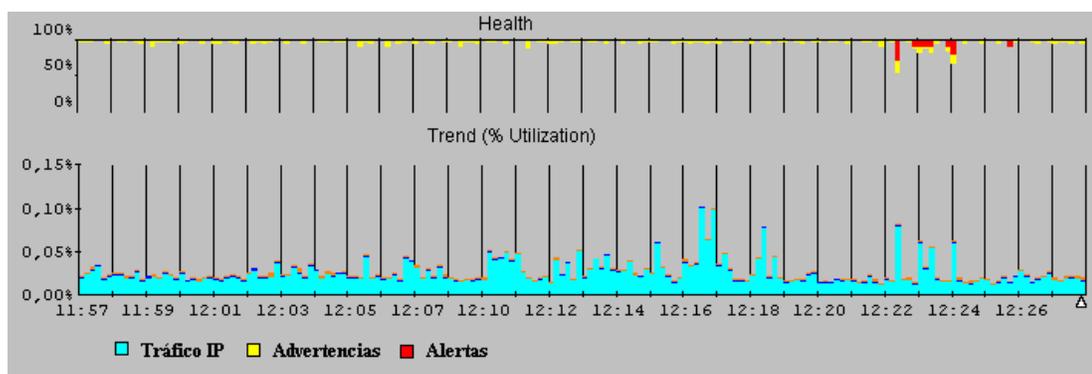


Figura 3. 14. Eventos generados en el enlace IPET – MEDICINA

3.2.6 CONCLUSIONES GENERALES DEL BACKBONE

- En general, la utilización del backbone de la Red de Datos está por debajo de los límites recomendados, dado que la utilización promedio de los enlaces no supera el 2.18% y los valores de máxima utilización son inferiores al 13.29%, por lo que su funcionamiento se puede considerar adecuado en cuanto a capacidad y congestión.
- El nivel de utilización promedio del enlace hacia el Router Cisco 3600 es aproximadamente el doble del enlace hacia el Router Cisco 1700. Aspecto justificado en que el ancho de banda del enlace WAN que se realiza con Emtel a través del Router Cisco 3600 es de 4 Mbps y el ancho de banda del enlace WAN que se realiza con TELECOM a través del Router Cisco 1700 es de 2 Mbps.
- Dentro de los sectores, el enlace IPET – INGENIERIAS es el más utilizado del backbone, no sólo debido a la alta densidad computacional del edificio de Ingenierías, sino quizá también al mayor uso de la Red por usuario con respecto a los demás edificios. En nivel de utilización le siguen de mayor a menor el enlace hacia Educación, Santo Domingo, El Carmen, Medicina y por último el enlace del Carmen hacia el VRI; lo cual concuerda con el orden de densidad computacional presentado en la Tabla 1.19.
- El stack de protocolos de mayor utilización en el backbone es TCP/IP, lo cual es lógico debido a la naturaleza misma de la Red, donde todos sus usuarios son reconocidos sobre la base de direcciones IP, y donde todos los servicios se fundamentan en la red TCP/IP. En nivel de utilización le siguen muy lejanamente los protocolos de Novell y posteriormente NetBEUI. En general en el backbone predomina TCP/IP con un 98.53% de utilización, seguido por Novell con un 0.72%, NetBEUI con un 0.43%, Otros¹¹ con un 0.32% y por último AppleTalk con un 0.014%.
- Los protocolos Novell, NetBEUI y AppleTalk, están presentes en la Red debido a que han sido habilitados cuando se realizó la configuración inicial de las conexiones de red de algunos equipos de la Universidad, o han sido habilitados por los mismos usuarios. En la actualidad estos protocolos no tienen ningún uso específico en la Red de Datos por lo cual este tipo de tráfico representa una carga adicional innecesaria.
- Del stack de protocolos TCP/IP, el protocolo PROXY 3128 es el de mayor utilización en todos los enlaces de los sectores del backbone, a excepción del enlace hacia el sector de Santo Domingo. En conjunto, el tráfico PROXY 3128 representa el 45.4% del tráfico total del stack de protocolos TCP/IP.
- El protocolo NETBIOS 137 se puede considerar como el segundo protocolo TCP/IP de mayor utilización en los enlaces del backbone, a excepción del

¹¹ Esto hace referencia a protocolos que no han sido reconocidos por el Analizador.

enlace hacia Santo Domingo en donde ocupa el primer lugar, y los enlaces hacia Educación e Ingenierías en donde ocupa el tercero y quinto lugar respectivamente. En general, el protocolo NETBIOS 137 representa el 21.83% de la utilización del stack de protocolos TCP/IP.

- El protocolo MICROSOFT-DS 445 se puede catalogar como el tercer protocolo TCP/IP de mayor utilización en los enlaces del backbone en conjunto. Este protocolo representa el 14.64% del total del tráfico TCP/IP.
- En los enlaces hacia Educación y Santo Domingo se destaca el protocolo TCP Oracle TNS. Esto debido a que los servidores de aplicaciones y bases de datos Oracle se encuentran ubicados en el sector de Educación y la mayoría de clientes que hacen uso de dichos servidores se encuentran ubicados en el sector de Santo Domingo.
- Otros protocolos TCP/IP presentes en la red con una proporción menor son: ICMP1, DNS 53, SMTP 25, POP3 110, FTP 20, SSH 22, NETRJS-3 73, HA-CLUSTER 694, TELNET 23, IGMP2 , BOOTP 67, SNMP 161, IMAPS 993, HTTPS 443, LDAP 389, LOC-SRV 135, entre otros.
- En los enlaces Switch Accelar 1200 – Router Cisco 1700 y Switch Accelar 1200 – Router Cisco 3600, el protocolo WWW 80 es generado principalmente por los servidores de Proxy HIPERION Y TEMIS, lo cual es lógico ya que los usuarios que tienen asignadas direcciones IP privadas acceden a Internet a través del servicio de Proxy.
- En el enlace Switch Accelar 1200 – Router Cisco 3600 existen algunos usuarios que tienen asignadas direcciones IP públicas que están utilizando aplicaciones que consumen un alto porcentaje del ancho de banda del enlace WAN con el proveedor de Internet Emtel, lo cual se evidencia con la alta utilización del protocolo TCP/UDP USER PORTS; por lo que es necesario que la administración de la Red de Datos identifique el tipo de aplicaciones que están siendo utilizadas y los usuarios que están haciendo uso de ellas.
- Los eventos “TCP Low Window” y “TCP Excessive Retransmission” presentes en los enlaces hacía los Routers Cisco 1700 y Cisco 3600 son generados principalmente por las conexiones establecidas entre los proxies y servidores externos. Dichos eventos indican una conexión lenta e ineficiente. Esto puede ser debido a que en determinados momentos los servidores de Proxy son sobrecargados y deben atender demasiadas sesiones lo que implica un alto consumo de recursos del sistema.
- El evento de Alerta “Zero Time To Live” que se presenta en los enlaces del IPET hacia los sectores de Ingenierías y Educación, y de El Carmen hacia el VRI son generados por la presencia de paquetes IP con un TTL bajo. Esto puede ser la causa de conexiones lentas debido a paquetes descartados, lo cual a su vez causan retransmisiones (eventos de Advertencia observados en gran cantidad).

- El evento de Alerta “IP Duplicate Address” aparece constantemente en la Red de Datos. Esto debido a que no se tiene un estricto control de la asignación de direcciones IP por parte de la administración de la Red o por errores en la configuración de los equipos¹².

3.2.7 ANALISIS DE LOS SEGMENTOS DEL SECTOR DE INGENIERIAS

3.2.7.1 INGCC1SW1-INGCC3SW1

- Las utilizaciones promedio y pico son del 1.38% y 14.68% respectivamente y están muy por debajo de los límites recomendados, lo cual no era lo esperado debido a la gran cantidad de equipos que contiene este segmento y a las aplicaciones que se manejan.
- Aunque la utilización es baja, los problemas de congestión se presentan muy a menudo en los segmentos INGCC3SW1-INGCC3HUB1 y INGCC3SW1-INGCC3HUB1 debido a que los hubs solo soportan tasas de 10 Mbps, lo que representa una velocidad muy baja considerando que los hubs se encuentran al limite de su capacidad y la demanda de los equipos es muy alta, ya que hacen parte de laboratorios de telemática.
- Los porcentajes promedios de broadcast y multicast combinados alcanzan el 20% del total de tramas del segmento.
- El protocolo PROXY 3128 es el principal consumidor de ancho de banda con 45.17% del total del tráfico TCP/IP.
- El protocolo NETBIOS 137 puede considerarse como el segundo en nivel de utilización ya que representa aproximadamente el 24.09%.
- El tercer protocolo en nivel de utilización es SSH 22 con 4.75%

3.2.7.2 INGCC1SW1-INGCC3HUB3

- La utilización promedio es del 0.41%, sin embargo muchas veces durante el periodo de medida la utilización sobrepasa valores del 25% y 30%, mostrando que se presentan instantes de alta utilización del segmento.
- La utilización máxima es del 40.52%, y a pesar de que el umbral es excedido una sola vez, no se puede catalogar como un evento aislado ya que se presentan muchos valores cercanos a él, además es significativamente alto si se considera que solamente hay 11 equipos en este segmento (figura 3.15).
- El porcentaje promedio de broadcast alcanza el 27.7% del total de tramas del segmento
- El porcentaje promedio de multicast es muy bajo y solo alcanza el 3.54% del total de tramas del segmento.

¹² En los archivos de las medidas realizadas con el Software Analizador de Protocolos se pueden detallar las direcciones IP duplicadas y las respectivas direcciones MAC en conflicto.

- El protocolo de mayor utilización es NETBIOS 137 con 22.5%, seguido por MICROSOFT-DS 445 con 12.98%, SSH 22 con 12.59%, FTP 20 con 11.37% y PROXY 3128 con 4.29%

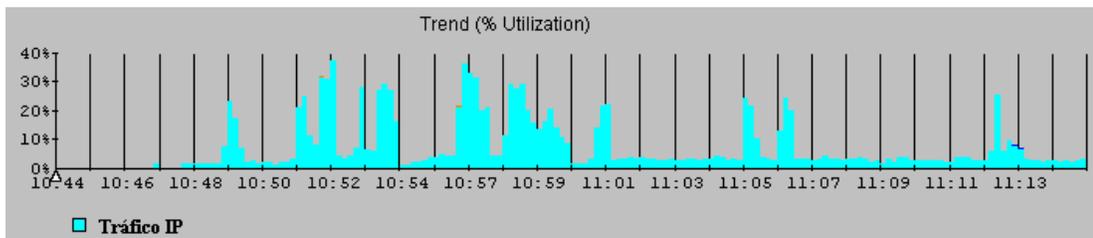


Figura 3. 15. Niveles de utilización del segmento INGCC1SW1-INGCC3HUB3

3.2.7.3 INGCC1SW1-INGCC3HUB4

- La utilización promedio alcanza un valor del 0.78%.
- La utilización máxima es del 38.43%, y a pesar de que el umbral no es excedido, no se puede catalogar como un evento aislado ya que se presentan muchos valores superiores al 20%, además es significativamente alto si se considera que solamente hay 11 equipos en este segmento.
- El porcentaje promedio de broadcast alcanza el 43.4% del total de tramas del segmento.
- El porcentaje promedio de multicast es muy bajo y solo alcanza el 4.71% del total de tramas del segmento.
- El protocolo de mayor utilización es NETBIOS 137 con 36.36%, seguido por MICROSOFT-DS 445 con 32.45%, PROXY 3128 con 18.17% y HA-CLUSTER 694 con 3.74%.

3.2.7.4 INGCC1SW1-INGCC2HUB1

- La utilización promedio alcanza un valor del 16.8% muy cercano al límite recomendado. Esto se debe a que el segmento no tiene una configuración óptima ya que todos los equipos y dispositivos de internetworking se conectan a través de un hub (INGCC2HUB1) al centro de cableado principal del sector de ingenierías (INGCC1SW1), situación no apropiada teniendo en cuenta la cantidad de hosts tan elevada que contiene cada centro de cableado.
- La utilización máxima alcanza un valor de 51.9%, el cual es un valor demasiado alto y preocupante si se tiene en cuenta que el valor máximo recomendado es excedido en varias ocasiones.
- Dentro de las medidas realizadas se observa que los periodos de tiempo de una hora más congestionados en el día alcanzan valores de utilización promedio de 32.4% en la mañana y 25.04% en la tarde. Estos valores

sobrepasan los rangos de desempeño establecidos para una red Ethernet (figura 3.16).

- Los niveles de broadcast son significativos teniendo en cuenta la alta utilización del segmento y la cantidad de ocasiones que se excede el umbral.
- Los niveles de multicast se mantienen bajos y por lo tanto no implica problemas.
- El protocolo PROXY 3128 tiene el mayor nivel de utilización con 40.99%, seguido por NETBIOS 137 con 27.99%, SSH 22 con 21.38% y DNS 53 con 6.24%.

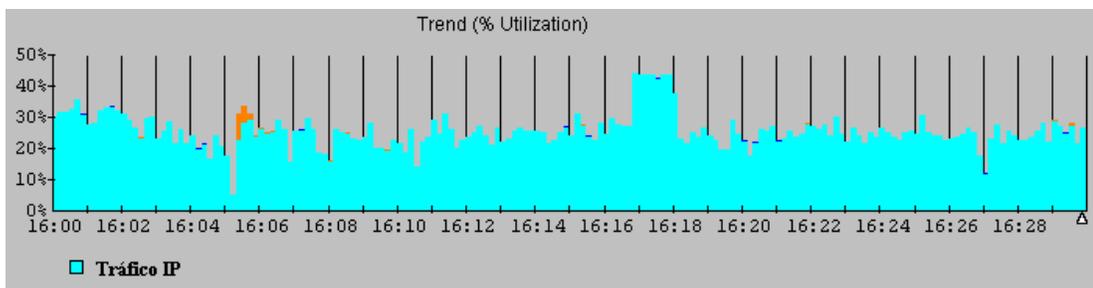


Figura 3. 16. Niveles de utilización del segmento INGCC1SW1-INGCC2HUB1

3.2.7.5 INGCC1SW1-INGCC9HUB1

- Las utilizaciones promedio y pico son del 0.44% y 9.24% respectivamente.
- La mayoría de tramas del segmento son de broadcast y multicast alcanzando un 94% del total de tramas, lo que es normal debido a la baja utilización del segmento.
- El protocolo de mayor utilización es NETBIOS 137 con 75.30%, seguido por HA-CLUSTER 694 con 11.27% y PROXY 3128 con 5.15%.

3.2.7.6 INGCC1SW1-INGCC13HUB1

- Las utilizaciones promedio y pico son del 0.04% y 4.35% respectivamente y están muy por debajo de los límites recomendados, por lo cual el segmento funciona adecuadamente. Esto debido a que el número de equipos que se encuentran conectados son solamente cinco y además posee una conexión Fast Ethernet.
- En el segmento hay cinco equipos conectados permanentemente, pero existe la posibilidad de que en un momento dado se conecten diez usuarios más (lo que supone un incremento en la utilización del segmento) los cuales no se encuentran conectados debido a políticas del departamento de Electrónica para el manejo de la sala de Automática.

- La presencia de altos valores de broadcast y multicast no indican congestión del segmento ya que se deben a la baja utilización del mismo.
- El protocolo de mayor utilización es NETBIOS 137 con 60.77%, seguido por PROXY 3128 con 23.52% y HA-CLUSTER 694 con 9.20%.

3.2.7.7 INGCC1SW1-INGCC15SW1

- Las utilizaciones promedio y pico son del 0.17% y 4.68% respectivamente.
- La presencia de altos valores de broadcast y multicast no indican congestión del segmento ya que se deben a la baja utilización del mismo.
- El protocolo de mayor utilización es NETBIOS 137 con 36.79%, seguido por PROXY 3128 con 33.25% y SSH 22 con 23.72%.

3.2.7.8 INGCC5SW1 – INGCC7HUB1

- Las utilizaciones promedio y pico son del 1.83% y del 19.00% respectivamente.
- Las tramas de broadcast representan el 46.51% del total de tramas del enlace.
- Las tramas de multicast representan el 4.46% del total de tramas del enlace.
- El protocolo PROXY 3128 es el principal consumidor de ancho de banda con el 56.45% del total del tráfico TCP/IP.
- El protocolo NETBIOS 137 es el segundo protocolo más utilizado con un porcentaje del 33.44%, seguido por HA-CLUSTER 694 con el 3.75%, DNS 53 con el 2.45% e ICMP1 con el 1.32%.

3.2.7.9 INGCC5SW1 – INGCC16HUB1

- Las utilizaciones promedio y pico son del 0.16% y del 4.56% respectivamente.
- Las tramas de broadcast representan el 44.29% del total de tramas del enlace.
- Las tramas de multicast representan el 4.11% del total de tramas del enlace.
- El protocolo PROXY 3128 es el principal consumidor de ancho de banda con el 62.81% del total del tráfico TCP/IP.
- El protocolo MICROSOFT-DS 445 es el segundo protocolo más utilizado con un porcentaje del 18.48%, seguido por NETBIOS 137 con el 12.92% y HA-CLUSTER 694 con el 2.07%.

3.2.8 ANALISIS DE LOS SEGMENTOS DEL SECTOR DE EDUCACION

3.2.8.1 EDUCC1SW2- EDUCC2AHUB3

- Las utilizaciones promedio y pico son del 0.41% y 18.61% respectivamente y están por debajo de los límites recomendados, a pesar de que la concentración de equipos es alta.

- Las tramas de broadcast representan el 82.04% del total de tramas del segmento.
- Las tramas de multicast representan el 6.13% del total de tramas del segmento.
- El protocolo de mayor utilización es NETBIOS 137 con 78.89%, seguido por HA-CLUSTER 694 con 8.94% y PROXY 3128 con 6.52%.

3.2.8.2 EDUCC1SW1- EDUCC1SW3

- La utilización promedio alcanza un valor del 4.27% y esta por debajo del límite recomendado.
- La utilización máxima alcanza un valor de 42.64%, y aunque el umbral es excedido en muy pocas ocasiones esto no se puede considerar como un hecho esporádico ya que se presentan niveles de utilización altos y constantes durante periodos de tiempo prolongados.
- Durante algunos periodos de tiempo se presentan niveles de utilización promedio superiores al 20% como se muestra en la figura 3.17, lo que indica que se presentan problemas de congestión. Esto puede ser debido a que el segmento esta configurado bajo la tecnología Ethernet compartida a 10 Mbps y el número de equipos interconectados es considerablemente alto.

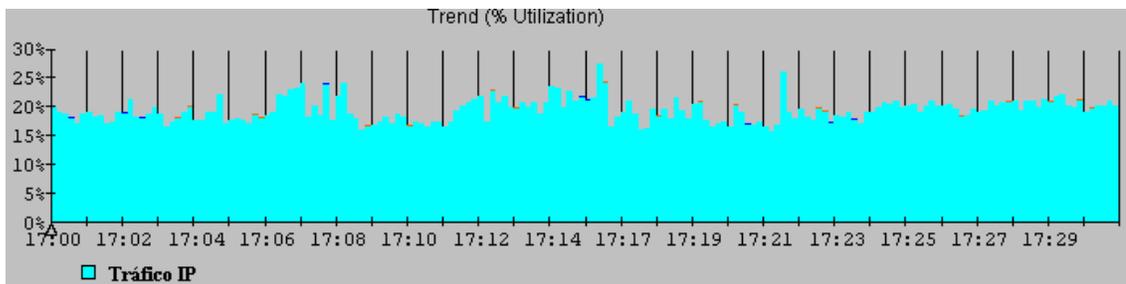


Figura 3. 17. Niveles de utilización del segmento EDUCC1SW1-EDUCC1SW3

- Las tramas de broadcast representan el 17.58% del total de tramas del segmento.
- Las tramas de multicast representan el 1.51% del total de tramas del segmento.
- El protocolo de mayor utilización es PROXY 3128 con 34.56%, seguido por X-WINDOWS 6000 con 32.71%, NETBIOS 137 con 23.88% y HA-CLUSTER 694 con 3.44%.
- Se presenta una gran cantidad de eventos de Advertencia “TCP Excessive Retransmission” detectados en las conexiones realizadas con equipos del segmento. Estos mensajes se presentan en su mayoría durante los periodos de

tiempo de alta utilización como se muestra en la figura 3.18. Esta situación se puede estar presentando por el bajo desempeño de los dispositivos del segmento lo que ocasiona que se estén descartando una gran cantidad de tramas. Además, este hecho puede afectar el desempeño general de la red.

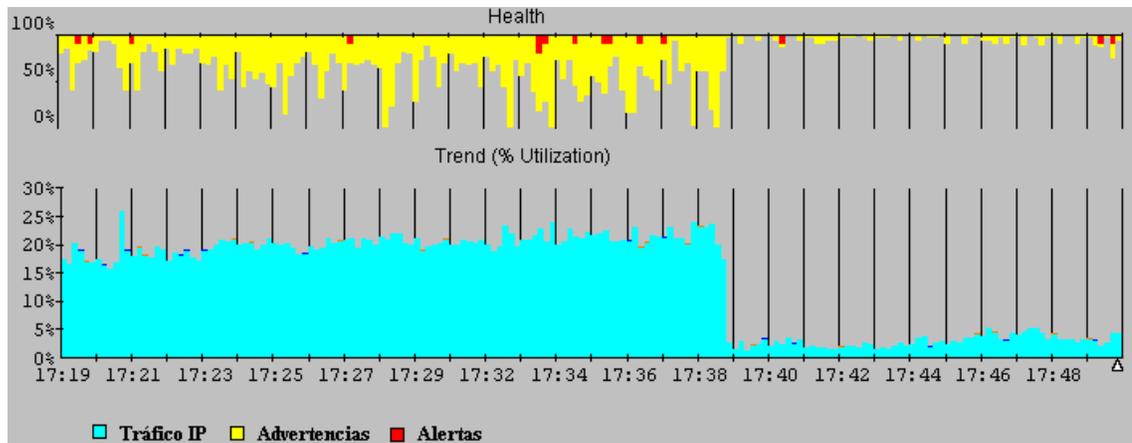


Figura 3. 18. Eventos generados en el segmento EDUCC1SW1-EDUCC1SW3

3.2.8.3 EDUCC1SW1- EDUCC1SW2

- Las utilizaciones promedio y pico son del 0.09% y 9.42% respectivamente.
- El enlace funciona adecuadamente, aunque se esperaban niveles de utilización más altos debido a que la concentración de equipos es alta.
- Las tramas de broadcast representan el 39.35% del total de tramas del segmento.
- Las tramas de multicast representan el 3.13% del total de tramas del segmento.
- El protocolo de mayor utilización es NETBIOS 137 con 57.43%, seguido por PROXY 3128 con 20.69%, MICROSOFT-DS 445 con 8.55%, HA-CLUSTER 694 con 5.23% y WWW 80 con 1.91%.

3.2.8.4 EDUCC1SW2- EDUCC3HUB1

- Las utilizaciones promedio y pico son del 0.47% y 6.77% respectivamente.
- Las tramas de broadcast representan el 83.86% del total de tramas del segmento.
- Las tramas de multicast representan el 7.94% del total de tramas del segmento.
- El protocolo de mayor utilización es NETBIOS 137 con 76.86%, seguido por HA-CLUSTER 694 con 10.00% y PROXY 3128 con 5.85%.

3.2.8.5 EDUCC1SW2- EDUCC5HUB1

- La utilización promedio alcanza un valor del 1.33% y esta por debajo del límite recomendado por lo que el enlace funciona correctamente.
- La utilización máxima alcanza un valor del 40.75% pero el umbral muestra que es excedido en una sola ocasión por lo que esto se puede considerar como un hecho aislado (figura 3.19).
- Las tramas de broadcast representan el 49.45% del total de tramas del segmento.
- Las tramas de multicast representan el 1.74% del total de tramas del segmento.
- El protocolo de mayor utilización es NETBIOS 137 con 71.32%, seguido por PROXY 3128 con 15.65%, HA-CLUSTER 694 con 5.28% y WWW 80 con 3.46%.

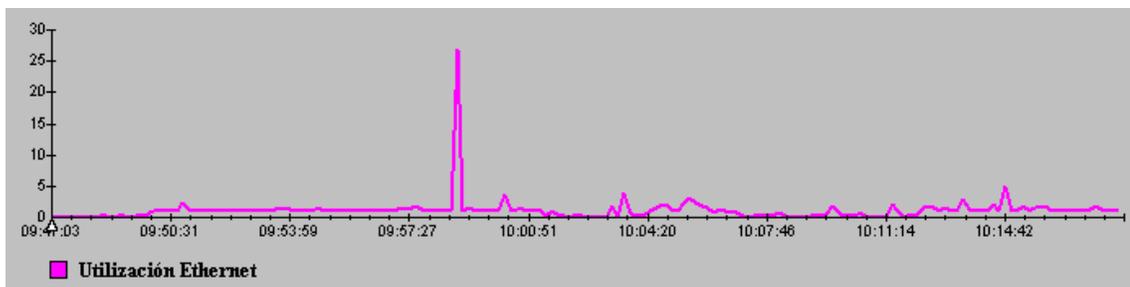


Figura 3. 19. Porcentaje de Utilización del segmento EDUCC1SW2 - EDUCC5HUB1

3.2.8.6 EDUCC1SW1- EDUCC4HUB2

- Las utilizaciones promedio y pico son del 0.07% y 3.54% respectivamente.
- Las tramas de broadcast representan el 76.14% del total de tramas del segmento.
- Las tramas de multicast representan el 3.70% del total de tramas del segmento.
- El protocolo de mayor utilización es NETBIOS 137 con 43.33%, seguido por PROXY 3128 con 35.97%, TCP Oracle TNS con 9.10%, MICROSOFT-DS 445 con 3.90% y HA-CLUSTER 694 con 3.72%.

3.2.9 ANALISIS DE LOS SEGMENTOS DEL SECTOR DEL CARMEN

3.2.9.1 CARCC1SW1- CARCC1HUB2

- Las utilizaciones promedio y pico son del 1.15% y 22.26% respectivamente.

- Las tramas de broadcast representan el 63.04% del total de tramas del segmento.
- Los niveles de multicast se mantienen bajos y por lo tanto no implica problemas.
- El protocolo de mayor utilización es NETBIOS 137 con 45.77%, seguido por PROXY 3128 con 43.45%, HA-CLUSTER 694 con 5.54% y MICROSOFT-DS 445 con 2.29%.

3.2.9.2 CARCC1SW1- CARCC1HUB1

- Las utilizaciones promedio y pico son del 0.77% y 12.44% respectivamente.
- Las tramas de broadcast representan el 71.98% del total de tramas del segmento.
- Los niveles de multicast se mantienen bajos y por lo tanto no implica problemas.
- El protocolo de mayor utilización es NETBIOS 137 con 53.29%, seguido por PROXY 3128 con 30.28% y HA-CLUSTER 694 con 9.43%.

3.2.9.3 CARCC1SW1- CARCC5HUB1

- Las utilizaciones promedio y pico son del 0.40% y 17.78% respectivamente.
- Las tramas de broadcast representan el 73.68% del total de tramas del segmento.
- Los niveles de multicast se mantienen bajos y por lo tanto no implica problemas.
- El protocolo de mayor utilización es NETBIOS 137 con 50.74%, seguido por PROXY 3128 con 31.06%, y HA-CLUSTER 694 con 8.17%.

3.2.9.4 CARCC1SW1- CARCC2HUB1

- Las utilizaciones promedio y pico son del 0.79% y 25.53% respectivamente.
- Las tramas de broadcast representan el 64.04% del total de tramas del segmento.
- Los niveles de multicast se mantienen bajos y por lo tanto no implica problemas.
- El protocolo de mayor utilización es NETBIOS 137 con 57.38%, seguido por PROXY 3128 con 24.43% y HA-CLUSTER 694 con 12.15%.

3.2.9.5 CARCC1SW1- CARCC3SW1

- Las utilizaciones promedio y pico son del 0.09% y 1.19% respectivamente.
- Las tramas de broadcast representan el 84.56% del total de tramas del segmento.

- Los niveles de multicast se mantienen bajos y por lo tanto no implica problemas.
- El protocolo de mayor utilización es NETBIOS 137 con 67.41%, seguido por HA-CLUSTER 694 con 11.53%, PROXY 3128 con 9.46%, SNMP 161 con 5.66% e IPP¹³ con 2.46%.

3.2.9.6 CARCC1SW1- ARTCC1SW1

- Las utilizaciones promedio y pico son de 0.14% y 2.96% respectivamente y están muy por debajo de los límites recomendados, lo que indica que no hay problemas de congestión.
- Las tramas de broadcast representan el 73.90% del total de tramas del segmento.
- Los niveles de multicast se mantienen bajos y por lo tanto no implica problemas.
- El protocolo de mayor utilización es NETBIOS 137 con 52.02%, seguido por PROXY 3128 con 35.02% y HA-CLUSTER 694 con 8.82%.

3.2.9.7 CARCC1SW1- ARCHCC1SW1

- Las utilizaciones promedio y pico son del 0.07% y 1.10% respectivamente.
- Las tramas de broadcast representan el 81.03% del total de tramas del segmento.
- Los niveles de multicast se mantienen bajos y por lo tanto no implica problemas.
- El protocolo de mayor utilización es NETBIOS 137 con 62.38%, seguido por PROXY 3128 con 19.61% y HA-CLUSTER 694 con 9.29%.

3.2.10 ANALISIS DE LOS SEGMENTOS DEL SECTOR DE SANTO DOMINGO

3.2.10.1 STOCC1SW1- STOCC3HUB1

- Las utilizaciones promedio y pico son del 0.53% y 13.18% respectivamente.
- Las tramas de broadcast representan el 72.71% del total de tramas del segmento.
- Los niveles de multicast se mantienen bajos y por lo tanto no implica problemas.
- El protocolo de mayor utilización es PROXY 3128 con 53.58%, seguido por NETBIOS 137 con 38.33% y HA-CLUSTER 694 con 4.80%.

¹³ Internet Printing Protocol

3.2.10.2 STOCC1SW1- STOCC3HUB2

- La utilización promedio alcanza un valor del 0.32% y esta muy por debajo del límite recomendado por lo que el segmento no presenta problemas de congestión.
- La utilización máxima alcanza un valor de 40.60%, pero esto se puede catalogar como un suceso esporádico ya que el umbral es excedido en muy pocas ocasiones.
- Las tramas de broadcast representan el 63.97% del total de tramas del segmento.
- Los niveles de multicast se mantienen bajos y por lo tanto no implica problemas.
- El protocolo de mayor utilización es NETBIOS 137 con 62.7%, seguido por TCP Oracle TNS con 19.27%, y PROXY 3128 con 12.65%.

3.2.10.3 STOCC1SW1- STOCC1HUB1

- La utilización promedio alcanza un valor del 1.05% y esta muy por debajo del límite recomendado por lo que el segmento presenta un buen desempeño.
- La utilización máxima alcanza un valor de 46.52%, y debido a que el umbral es excedido en muy pocas ocasiones esto se puede considerar como un hecho esporádico.
- Las tramas de broadcast representan el 79.87% del total de tramas del segmento.
- Los niveles de multicast se mantienen bajos y por lo tanto no implica problemas.
- El protocolo de mayor utilización es NETBIOS 137 con 83.63%, seguido por HA-CLUSTER 694 con 4.63%, y PROXY 3128 con 3.03%.

3.2.10.4 STOCC1SW1- STOCC1HUB2

- La utilización promedio alcanza un valor del 0.32% y esta muy por debajo del límite recomendado por lo que el segmento funciona adecuadamente.
- La utilización máxima alcanza un valor de 40.96%, y debido a que el umbral es excedido en muy pocas ocasiones esto se puede considerar como un hecho esporádico.
- Las tramas de broadcast representan el 80.29% del total de tramas del segmento.
- Los niveles de multicast se mantienen bajos y por lo tanto no implica problemas.
- El protocolo de mayor utilización es NETBIOS 137 con 77.16%, seguido por HA-CLUSTER 694 con 7.35%, MICROSOFT-DS 445 con 6.58% y PROXY 3128 con 4.10%.

3.2.10.5 STOCC1SW1- STOCC3SW1

- Las utilizaciones promedio y pico son del 0.05% y 11.88% respectivamente.
- Las tramas de broadcast representan el 47.11% del total de tramas del segmento.
- Los niveles de multicast se mantienen bajos y por lo tanto no implica problemas.
- El protocolo de mayor utilización es NETBIOS 137 con 54.84%, seguido por PROXY 3128 con 13.95%, TCP Oracle TNS con 13.64% y MICROSOFT-DS 445 con 7.9%.

3.2.10.6 STOCC1SW1- STOCC3SW2

- Las utilizaciones promedio y pico son del 0.21% y 3.36% respectivamente.
- Las tramas de broadcast representan el 57.02% del total de tramas del segmento.
- Los niveles de multicast se mantienen bajos y por lo tanto no implica problemas.
- El protocolo de mayor utilización es PROXY 3128 con 60.86%, seguido por NETBIOS 137 con 27.95%, HA-CLUSTER 694 con 3.70% y TCP Oracle TNS con 3.06%.

3.2.10.7 STOCC1SW1- STOCC4HUB2

- La utilización promedio alcanza un valor del 0.55% y esta muy por debajo del límite recomendado por lo que el segmento no presenta problemas de congestión. Además, este valor es muy bajo teniendo en cuenta que el segmento contiene una gran cantidad de equipos.
- La utilización máxima alcanza un valor de 36.98%, pero esto se puede catalogar como un suceso esporádico ya que su tiempo de duración es muy pequeño.
- Las tramas de broadcast representan el 51.91% del total de tramas del segmento.
- Los niveles de multicast se mantienen bajos y por lo tanto no implica problemas.
- El protocolo de mayor utilización es NETBIOS 137 con 71.14%, seguido por PROXY 3128 con 9.84%, SMTP 25 con 9.51%, y TCP Oracle TNS con 3.83%.

3.2.10.8 STOCC1SW1- STOCC6HUB1

- La utilización promedio alcanza un valor del 1.12% y esta muy por debajo del límite recomendado por lo que el segmento no presenta problemas de congestión.

- La utilización máxima alcanza un valor de 36.30%, pero esto se puede catalogar como un suceso esporádico ya que su tiempo de duración es muy pequeño.
- Las tramas de broadcast representan el 56.87% del total de tramas del segmento.
- Los niveles de multicast se mantienen bajos y por lo tanto no implica problemas.
- El protocolo de mayor utilización es PROXY 3128 con 53.63%, seguido por NETBIOS 137 con 32.59%, HA-CLUSTER 694 con 5.35% y SMTP 25 con 3.77%.

3.2.11 ANALISIS DE LOS SEGMENTOS DEL SECTOR DEL VRI

3.2.11.1 VRICC1SW1- SERVIDOR PURACE

- La utilización promedio alcanza un valor del 0.90% y esta por debajo del límite recomendado.
- La utilización máxima alcanza un valor de 21.55%, sin embargo es un nivel de utilización que solamente se presenta en un instante de la medida, por lo cual no representa ningún problema.
- El protocolo de mayor utilización es NETBIOS 137 con 44.34%, seguido por MICROSOFT-DS 445 con 27.17%, WWW 80 con 9.75%, HA-CLUSTER 694 con 7.21%, DNS 53 con 6.41% y PROXY 3128 con 2.25%.

3.2.11.2 VRICC1SW1- VRICC1SW2

- La utilización promedio alcanza un valor del 0.95% y esta por debajo del límite recomendado.
- La utilización máxima alcanza un valor de 34.60%, sin embargo es un nivel de utilización que solamente se presenta en un instante de la medida, por lo que se puede considerar como un hecho aislado.
- Las tramas de broadcast representan el 64.15% del total de tramas del segmento.
- Las tramas de multicast representan el 3.89% del total de tramas del segmento.
- El protocolo de mayor utilización es NETBIOS 137 con 43.04%, seguido por MICROSOFT-DS 445 con 32.56%, WWW 80 con 8.89%, HA-CLUSTER 694 con 5.66%, PROXY 3128 con 4.35% y DNS 53 con 3.15%.

3.2.11.3 VRICC1SW1- VRICC1HUB3

- La utilización promedio alcanza un valor del 0.80% y esta por debajo del límite recomendado.

- La utilización máxima alcanza un valor de 43,00%, y aunque el umbral es excedido en muy pocas ocasiones esto no se puede considerar como un hecho esporádico ya que se presentan niveles de utilización altos y constantes durante periodos de tiempo prolongados.
- Durante algunos periodos de tiempo se presentan niveles de utilización promedio superiores al 25% como se muestra en la figura 3.20, lo que indica que se presentan problemas de congestión. Esto puede ser debido a que el segmento esta configurado bajo la tecnología Ethernet compartida a 10 Mbps.
- Dentro de las medidas realizadas se puede observar que el periodo de tiempo de la hora más congestionada alcanza un valor de utilización promedio de 35.9%. Este valor sobrepasa los rangos de desempeño óptimos establecidos para una red Ethernet.

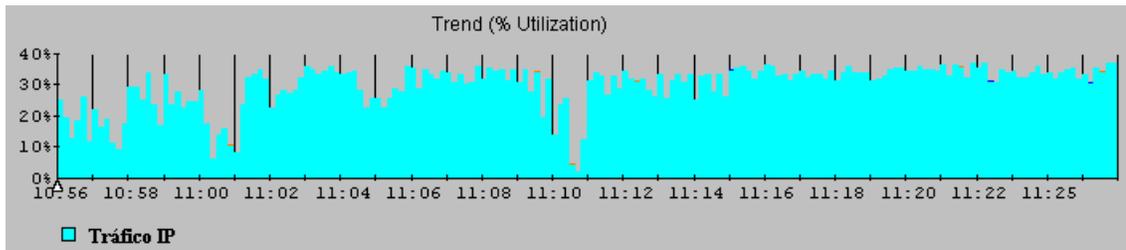


Figura 3. 20. Niveles de utilización del segmento VRICC1SW1- VRICC1HUB3

- Las tramas de broadcast representan el 50.30% del total de tramas del segmento.
- Las tramas de multicast representan el 1.12% del total de tramas del segmento.
- El protocolo de mayor utilización es NETBIOS 137 con 44.26%, seguido por MICROSOFT-DS 445 con 25.71%, PROXY 3128 con 21.16%, HA-CLUSTER 694 con 5.32% y DNS 53 con 1.38%.

3.2.11.4 VRICC1SW1- VRICC1HUB1

- Las utilizations promedio y pico son del 0.41% y 15.00% respectivamente.
- Las tramas de broadcast representan el 84.40% del total de tramas del segmento.
- Las tramas de multicast representan el 4.15% del total de tramas del segmento.
- El protocolo de mayor utilización es NETBIOS 137 con 66.95%, seguido por PROXY 3128 con 18.50% y HA-CLUSTER 694 con 9.61%.

3.2.11.5 VRICC1SW1- VRICC1HUB2

- La utilización promedio alcanza un valor del 1.00% y esta por debajo del límite recomendado.
- La utilización máxima alcanza un valor del 40,00%, sin embargo este suceso ocurre esporádicamente (figura 3.21) por lo cual no tiene ninguna incidencia en el desempeño del segmento
- Las tramas de broadcast representan el 45.77% del total de tramas del segmento.
- Las tramas de multicast representan el 2.18% del total de tramas del segmento.
- El protocolo de mayor utilización es NETBIOS 137 con 64.64%, seguido por HA-CLUSTER 694 con 21.94%, PROXY 3128 con 4.92% y DNS 53 con 4.56%.

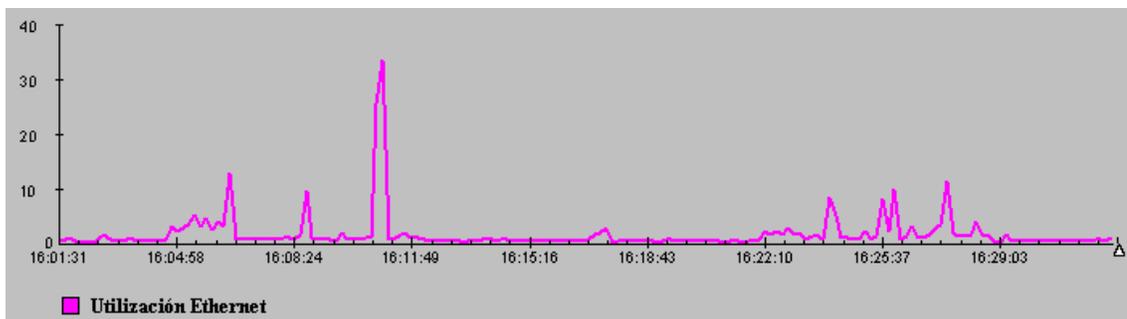


Figura 3. 21. Porcentaje de Utilización del segmento VRICC1SW1 - VRICC1HUB2

3.2.12 ANALISIS DE LOS SEGMENTOS DEL SECTOR DE MEDICINA

3.2.12.1 MEDCC1SW1- MEDCC1HUB1

- Las utilizations promedio y pico son del 0.25% y 8.74% respectivamente.
- Las tramas de broadcast representan el 87.91% del total de tramas del segmento.
- Los niveles de multicast se mantienen bajos y por lo tanto no implica problemas.
- El protocolo de mayor utilización es NETBIOS 137 con 66.15%, seguido por HA-CLUSTER 694 con 11.73%, PROXY 3128 con 11.58% y SMTP 25 con 2.79%.

3.2.12.2 MEDCC1SW1- MEDCC1HUB2

- Las utilizations promedio y pico son del 0.21% y 9.82% respectivamente.

- Las tramas de broadcast representan el 81.03% del total de tramas del segmento.
- Las tramas de multicast representan el 7.99% del total de tramas del segmento.
- El protocolo de mayor utilización es NETBIOS 137 con 66.63%, seguido por HA-CLUSTER 694 con 13.90% y PROXY 3128 con 10.26%.

3.2.12.3 MEDCC1SW1- MEDCC1HUB3

- Las utilizaciones promedio y pico son del 0.88% y 4.76% respectivamente.
- Las tramas de broadcast representan el 93.62% del total de tramas del segmento.
- Los niveles de multicast se mantienen bajos y por lo tanto no implica problemas.
- El protocolo de mayor utilización es NETBIOS 137 con 75.82%, seguido por HA-CLUSTER 694 con 12.66% y PROXY 3128 con 3.70%.

3.2.12.4 MEDCC1SW1- MEDCC2HUB1

- La utilización promedio alcanza un valor del 0.85% y esta muy por debajo del límite recomendado.
- La utilización máxima alcanza un valor de 20.23%, sin embargo este suceso ocurre esporádicamente (figura 3.22) por lo cual no tiene ninguna incidencia en el desempeño del segmento
- Las tramas de broadcast representan el 61.25% del total de tramas del segmento.
- Las tramas de multicast representan el 3.18% del total de tramas del segmento.
- El protocolo de mayor utilización es NETBIOS 137 con 64.10%, seguido por HA-CLUSTER 694 con 16.29% y PROXY 3128 con 10.34%.

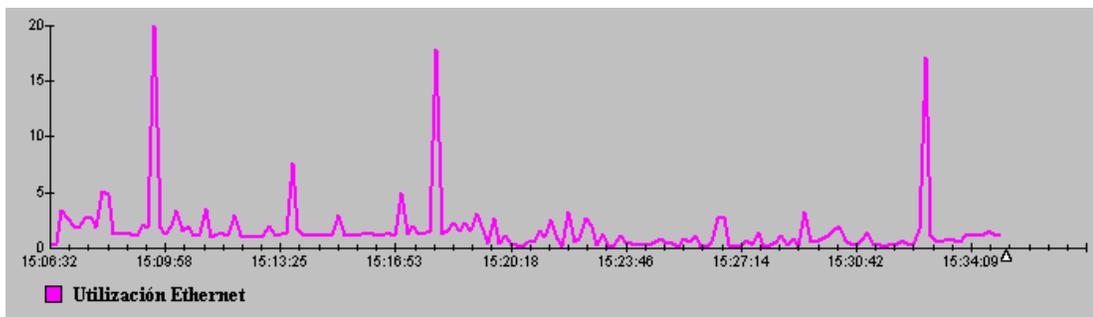


Figura 3. 22. Porcentaje de Utilización del segmento MEDCC1SW1 – MEDCC2HUB1

3.2.12.5 MEDCC1SW1- MEDCC3HUB1

- Las utilizaciones promedio y pico son del 0.31% y 15.08% respectivamente.
- Las tramas de broadcast representan el 52.40% del total de tramas del segmento.
- Los niveles de multicast están por debajo de los límites recomendados y por lo tanto no implica problemas.
- El protocolo de mayor utilización es NETBIOS 137 con 56.45%, seguido por PROXY 3128 con 25.11%, HA-CLUSTER 694 con 9.43% y SMTP 25 con 3.63%.

3.2.13 CONCLUSIONES GENERALES DE LOS SEGMENTOS

- En general, los segmentos presentan un desempeño adecuado y funcionan dentro de los límites recomendados por la IEEE para las tecnologías Ethernet y Fast Ethernet.
- Los segmentos que presentan un desempeño poco óptimo como consecuencia de sus altos niveles de utilización son los siguientes: **INGCC1SW1-INGCC3HUB3, INGCC1SW1 - INGCC3HUB4, INGCC1SW1-INGCC2HUB1, EDUCC1SW1 - EDUCC1SW3 y VRICC1SW1-VRICC1HUB3.**
- Los segmentos nombrados anteriormente deben ser atendidos con mayor prioridad durante el proceso de migración a realizarse en la Red de Datos.
- El segmento que presenta el desempeño más pobre es **INGCC1SW1-INGCC2HUB1** debido a que sobrepasa frecuentemente los límites recomendados por el estándar. Esto se debe a que el segmento no tiene una configuración óptima ya que todos los equipos y dispositivos de internetworking se conectan a través de un hub (INGCC2HUB1) al centro de cableado principal del sector de ingenierías (INGCC1SW1), situación no apropiada teniendo en cuenta la cantidad de hosts tan elevada que contiene cada centro de cableado.
- Algunos segmentos sobrepasan el valor máximo de utilización, sin embargo no presentan problemas de congestión ya que estos niveles alcanzados son esporádicos y los niveles de utilización promedio son relativamente bajos. Estos segmentos son los siguientes: **EDUCC1SW2 - EDUCC5HUB1, STOCC1SW1 - STOCC3HUB2, STOCC1SW1 - STOCC1HUB1, STOCC1SW1 - STOCC1HUB1, VRICC1SW1 - VRICC1HUB3, VRICC1SW1 - VRICC1HUB2.**
- Los protocolos TCP/IP son los mayores generadores de tráfico con un promedio mayor al 90% de la utilización total, seguido lejanamente por los protocolos Novell, NetBEUI, AppleTalk, IPv6 y otros.
- Dentro del stack de protocolos TCP/IP, los protocolos NETBIOS 137 y PROXY 3128 son los principales generadores de tráfico, seguidos por

protocolos tales como HA-CLUSTER 694, MICROSOFT-DS 445, SSH 22, FTP 20, SMTP 25, DNS 53, WWW 80, entre otros, aunque con niveles de utilización mínimos.

3.2.14 ANALISIS DE LOS SERVIDORES DEL SECTOR DE EDUCACION (SISTEMAS DE INFORMACION).

3.2.14.1 SERVIDOR DE RECURSOS FISICOS (GALADRIEL)

- Las utilizaciones promedio y pico son del 0.04% y 12.99% respectivamente.
- El protocolo de mayor utilización es NETBIOS 137 con 64.56%, seguido por MICROSOFT-DS 445 con 18.37%, TCP/UDP USER PORTS con 7.02% y HA-CLUSTER 694 con 6.59%.

3.2.14.2 SERVIDOR DE RECURSOS HUMANOS (ARWEN)

- Las utilizaciones promedio y pico son del 0.06% y 2.63% respectivamente.
- El protocolo de mayor utilización es TCP/UDP USER PORTS con 46.60%, seguido por NETBIOS 137 con 32.40%, MICROSOFT-DS 445 con 11.20%, TCP Oracle TNS con 4.62% y HA-CLUSTER 694 con 2.85%.

3.2.14.3 SERVIDOR DE FINANZAS (EOWIN)

- Las utilizaciones promedio y pico son del 0.05% y 11.86% respectivamente.
- El protocolo de mayor utilización es NETBIOS 137 con 87.62%, seguido por TCP/UDP USER PORTS con 8.49% y HA-CLUSTER 694 con 1.79%.

3.2.14.4 SERVIDOR DE BASE DE DATOS DE RECURSOS FISICOS Y HUMANOS (TESEO)

- Las utilizaciones promedio y pico son del 0.04% y 0.78% respectivamente.
- El protocolo de mayor utilización es TCP/UDP USER PORTS con 33.15%, seguido por TCP Oracle TNS con 31.32%, NETBIOS 137 con 28.37% y HA-CLUSTER 694 con 4.04%.

3.2.14.5 SERVIDOR DE BASE DE DATOS DE FINANZAS (GANDALF)

- Las utilizaciones promedio y pico son del 0.08% y 1.12% respectivamente.
- El protocolo de mayor utilización es TCP Oracle TNS con 48.89%, seguido por NETBIOS 137 con 35.37%, TCP/UDP USER PORTS con 10.39% y HA-CLUSTER 694 con 3.46%.

3.2.14.6 SERVIDOR DEL SISTEMA DE INFORMACION ACADEMICO (SOCRATES)

- Las utilizaciones promedio y pico son del 0.06% y 4.79% respectivamente.

- El protocolo de mayor utilización es TCP/UDP USER PORTS con 47.45%, seguido por NETBIOS 137 con 38.14%, HA-CLUSTER 694 con 5.87% y TCP Oracle TNS con 4.72%.

3.2.14.7 SERVIDOR DE LA BIBLIOTECA (BIBLIO)

- Las utilizaciones promedio y pico son de 0.05% y 8.01% respectivamente.
- El protocolo de mayor utilización es NETBIOS 137 con 56.02%, seguido por TCP/UDP USER PORTS con 18.11%, WWW 80 con 14.39% y HA-CLUSTER 694 con 7.18%.

3.2.15 CONCLUSIONES GENERALES DE LOS SERVIDORES DEL SECTOR DE EDUCACION.

- Ninguno de los enlaces a los servidores presenta problemas de congestión, por el contrario todos tienen niveles de utilización inferiores al 1%, y la utilización máxima está por debajo del 13% para todos los servidores.
- El servidor de Bases de Datos de Finanzas (GANDALF) presenta la mayor utilización promedio, seguido por ARWEN, SOCRATES, BIBLIO, EOWIN, GALADRIEL, y TESEO.
- Se observan mensajes “TCP Excessive Retransmission” los cuales son considerados como mensajes de Advertencia.
 - ✓ Cuando estos mensajes son enviados desde los servidores hacia los clientes significa que los clientes pueden ser sistemas con bajos recursos, por lo cual es aconsejable comprobar si el cliente está configurado óptimamente o si es necesario asignar más memoria para las conexiones de red.
 - ✓ Cuando estos mensajes están dirigidos hacia los servidores es necesario verificar si los servidores están siendo sobrecargados con demasiadas sesiones.
 - ✓ Si la red tiene dispositivos con bajo desempeño (switches, routers) estos pueden estar descartando tramas debido a su alta utilización.
 - ✓ El servidor de finanzas (EOWIN) es el que más genera este tipo de mensajes debido a las continuas retransmisiones que debe realizar hacia sus clientes, los cuales pertenecen en su mayoría al sector de Santo Domingo (subred 172.16.10.0)
 - ✓ Este tipo de mensajes también se encontraron en los demás servidores aunque en menor proporción, teniendo todos en común que la mayoría de estos mensajes estaban dirigidos hacia los clientes del sector de Santo Domingo.
 - ✓ Los servidores de finanzas (EOWIN) y recursos humanos (ARWEN) transmitieron un número considerable de mensajes hacia el servidor de

recursos físicos (GALADRIEL), lo cual puede indicar problemas de sobrecarga en este servidor.

- Se presentan mensajes de Oracle TNS (Transparent Network Substrate) en los enlaces a los servidores de Bases de Datos de Finanzas, Recursos Físicos y Humanos. Este mensaje identificado como SSR (Slow Server Response) indica respuesta lenta en dichos servidores.
 - ✓ Si el tiempo de respuesta es demasiado grande para un cliente en particular, se debe establecer una conexión dedicada para obtener un mejor desempeño.
 - ✓ Si el tiempo de respuesta es demasiado grande para un grupo de usuarios Oracle, se debe revisar el desempeño de los segmentos de red entre estos usuarios y el servidor.
 - ✓ Si el tiempo de respuesta es demasiado grande para un gran número de usuarios se debe considerar las siguientes opciones: Actualizar el hardware del servidor, distribuir las bases de datos entre múltiples servidores, incrementar el número de Listeners o incrementar el número de Dispatchers.
- También se presentan mensajes TNS MARKER, aunque con menor frecuencia, enviados desde los clientes hacia los servidores de Bases de Datos. Esto indica la presencia de clientes con sistemas bajos en recursos que necesitan más memoria, una tarjeta de red de más alto desempeño o un computador con mayor velocidad de procesamiento.

3.2.16 ANALISIS DE LOS SERVIDORES DEL SECTOR DEL IPET (SERVICIOS DE LA RED TCP/IP).

3.2.16.1 SERVIDORES HIPERION Y TEMIS (SERVIDORES DE PROXY)

- Las utilizaciones promedio y pico son de 0.7% y 7.69% respectivamente.
- El protocolo de mayor utilización es PROXY 3128 con 77.44%, seguido por WWW 80 con 15.46%, TCP/UDP USER PORTS con 7.09% e ICMP1 con 0.01%.

3.2.16.2 SERVIDOR ACUARIO

- Las utilizaciones promedio y pico son de 0.4% y 4.38% respectivamente.
- El protocolo de mayor utilización es MDBS_DAEMON 800 con 96.23%, seguido lejanamente por DNS 53 con 3.58% y SSH 22 con 0.54%.

3.2.16.3 SERVIDOR ATENEA

- Las utilizaciones promedio y pico son de 0.01% y 0.08% respectivamente.
- El protocolo de mayor utilización es SMTP 25 con 40.18%, seguido por DNS 53 con 28.75%, POP3 110 con 11.18%, ICMP 1 con 6.60%, SSH 22 con

5.11%, TCP/UDP USER PORTS con 4.74%, WWW 80 con 3.28%, e IMAP2 143 con 0.20%.

3.2.16.4 SERVIDOR AFRODITA

- Las utilizaciones promedio y pico son de 0.08% y 0.88% respectivamente.
- El protocolo de mayor utilización es LDAP 389 con 42.88%, seguido por SSH 22 con 23.33%, DNS 53 con 17.81%, SMTP 25 con 13.10%, e IMAP2 143 con 2.05%.

3.2.16.5 SERVIDOR JUNO

- Las utilizaciones promedio y pico son de 0.04% y 0.38% respectivamente.
- Por ser este el servidor de directorio, el protocolo de mayor utilización es LDAP 389 con aproximadamente un 99%.

3.2.16.6 SERVIDORES HADES Y PERSEO

- Las utilizaciones promedio y pico son de 0.03% y 0.35% respectivamente.
- El protocolo de mayor utilización es DNS 53 con 96.43%, seguido por NETBIOS 137 con 2.43%.

3.2.17 CONCLUSIONES GENERALES DE LOS SERVIDORES DEL SECTOR DEL IPET.

- Ninguno de los enlaces a los servidores presenta problemas de congestión, por el contrario todos tienen niveles de utilización inferiores al 1%, y la utilización máxima está por debajo del 8% para todos los servidores.
- El stack de protocolos más importante en cantidad de tráfico es TCP/IP, aspecto lógico porque se trata de enlaces de servidores con servicios TCP/IP. La distribución de los protocolos TCP/IP en los enlaces hacia los servidores esta de acuerdo a los servicios soportados por cada uno de ellos.
- La mayor utilización promedio entre los servidores la tienen los servidores de Proxy (HIPERION y TEMIS), seguido por ACUARIO, AFRODITA, JUNO, HADES, PERSEO y ATENEA.
- En los enlaces hacia los servidores no se presentan eventos de Alertas o Advertencias a excepción de los enlaces hacia los servidores de Proxy. Dichos eventos son “TCP Low Window” y “TCP Excessive Retransmission”.

3.2.18 ANALISIS DE BROADCAST Y MULTICAST.

Debido a que solo se tiene configurada una sola subred lógica IP, el tráfico de Broadcast y Multicast originado en cualquier sector se propaga por toda la red. Esto implica que al medir este tipo de tráfico en una subred se lo esta midiendo en toda la

CAPITULO 3. ANALISIS DEL DESEMPEÑO DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

Red. Por consiguiente, este tipo de tráfico se puede evaluar a partir de medidas realizadas en un enlace a 100 Mbps configurado en modo Full Duplex. A continuación se presenta el análisis de Broadcast y Multicast de la Red de Datos.

NOMBRE DE LA ESTADÍSTICA	PROMEDIO	MÁXIMO	UMBRAL
Broadcast (pps).	62	1553	437
Multicast (pps).	4	64	16

Tabla 3. 4. Niveles de Broadcast y Multicast de la Red de Datos de la Universidad del Cauca

STACK DE PROTOCOLOS / PROTOCOLO	TRAMAS (%)	BYTES (%)
TCP/IP	85,85%	79,65%
ARP/RARP	85,10%	69,43%
NETBIOS 137	11,54%	22,67%
HA - CLUSTER 694	2,48%	6,41%
RIP 520	0,61%	0,99%
IPP 631	0,24%	0,40%
BOOTP 67	0,02%	0,09%
NOVELL	9,38%	12,27%
NETBEUI	4,74%	8,05%
APPLETALK	0,03%	0,03%

Tabla 3. 5. Protocolos generadores de Broadcast y Multicast

De las tablas anteriores se puede deducir que:

- El valor promedio de tramas de broadcast por segundo es superior al límite recomendado (50 pps) para un nivel de desempeño adecuado de la Red, con lo cual se puede evidenciar que este tipo de tráfico esta afectando el funcionamiento de la Red en general.
- El valor del umbral de broadcast es excedido constantemente, alcanzando valores picos demasiado altos, lo cual indica que en repetidas ocasiones se presentan tormentas de broadcast que pueden llegar a afectar el normal desempeño de la Red.
- El valor promedio de tramas de multicast por segundo está por debajo del límite recomendado y el valor umbral indica que el límite es excedido muy pocas veces y solo es un hecho esporádico, por lo que se puede afirmar que este tipo de tráfico no representa ningún problema para la Red; sin embargo
- El mayor generador de este tipo de tráfico (broadcast y multicast) es el stack de protocolos TCP/IP con un 79.65%, seguido por Novell con un 12.27%, NetBEUI con un 8.05% y AppleTalk con un 0.03%.

- Del stack TCP/IP, el protocolo ARP/RARP es el mayor productor de tráfico de broadcast con un 69.43%, seguido por NETBIOS 137 con un 22.67% y HA-CLUSTER 694 con un 6.41%.
- El protocolo NETBIOS 137 que se transporta sobre IP genera niveles significativos de broadcast debido a la falta de una configuración adecuada de los clientes WINS para el soporte de la red Microsoft, lo que obliga al uso del broadcast para la resolución de nombres.
- Los protocolos TCP/IP generan principalmente unicast; en menor proporción le sigue el broadcast, mientras que el multicast producido es casi nulo.
- El protocolo RIP está generando el 0.99% del total del tráfico de broadcast. La presencia de éste protocolo se debe a que está habilitado en el router Cisco 1700 pero es totalmente innecesario ya que no presta ninguna funcionalidad dentro de la Red.
- La configuración de los protocolos Novell en la Red hace que la totalidad del tráfico IPX sea broadcast.
- La totalidad del tráfico generado por el protocolo AppleTalk es de broadcast.
- De los protocolos Novell, el protocolo Netbios Name 20 es el mayor generador de tráfico de broadcast con un 61%, seguido por Service ADV 0452 con un 22% y Routing 0453 con un 14%.
- El protocolo NetBEUI es uno de los principales generadores de tráfico multicast presente en la Red, seguido por IGMP2 pero con niveles de utilización muy bajos.
- El porcentaje de broadcast producido en la Red es mucho mayor que el multicast.

De acuerdo a lo anterior, se recomienda tomar las siguientes medidas, con el fin de mejorar el desempeño de la Red:

SUPRESIÓN DEL PROTOCOLO RIP.

El protocolo RIP no esta prestando ninguna funcionalidad debido a que en el interior de la Red no se realiza enrutamiento por lo que representa una carga adicional innecesaria. Se recomienda deshabilitar RIP en el router Cisco 1700 para evitar el tráfico de broadcast originado por éste protocolo.

SUPRESIÓN DEL STACK DE PROTOCOLOS DE NOVELL.

Los protocolos de Novell son innecesarios en la Red debido a que no existen servicios de carácter público basados en ellos (todos los servicios de la Red son TCP/IP) y necesidades concretas para su configuración

Con el objetivo de disminuir la carga de la Red (especialmente los niveles de tráfico broadcast, de los cuales los protocolos de Novell constituyen un porcentaje significativo) y en consecuencia mejorar el desempeño de la misma se debe

reconfigurar los hosts de la Red suprimiendo las interfaces IPX/SPX de todos los hosts de la Red (con excepción de usuarios exclusivos que las requieran).

SUPRESIÓN DEL PROTOCOLO NETBEUI.

El protocolo NetBEUI no es el elemento óptimo para el transporte del protocolo NetBIOS, necesario dentro de la Red para soportar la Red Microsoft y la comunicación de muchas aplicaciones tipo Windows, gracias a que existen otros protocolos que hacen un manejo más eficiente de los recursos. La razón de esto, es que NetBEUI es un protocolo para manejo en redes pequeñas (del orden de 25 hosts), que además consume mucho ancho de banda innecesario, basado totalmente en comunicaciones con tramas multicast, y no-enrutable. Es necesario entonces la supresión de NetBEUI de la configuración de red de todos los hosts de la Universidad. Para llevar esto a cabo, se necesita definir el protocolo, más eficiente, encargado de transportar a NetBIOS. Se tienen dos posibilidades: NetBIOS sobre IP o NetBIOS sobre IPX; consideradas porque a diferencia de NetBEUI no se basan en tramas multicast, son protocolos enrutables y el consumo de ancho de banda es eficiente. NetBIOS sobre IPX es descartado debido a que como se expuso en el párrafo anterior se eliminará el tráfico Novell, y porque NetBIOS sobre IP, configurado correctamente, es más eficiente que el primero. Esa configuración correcta de NetBIOS sobre IP ocurre cuando se configura un servidor WINS, ya que se elimina el broadcast de éste. Por lo tanto, se debe configurar en la Red por lo menos un servidor WINS en cada uno de los sectores y configurar adecuadamente los clientes WINS. De acuerdo a esto los hosts tienen que reconfigurarse para el transporte de NetBIOS sobre IP y el acceso a ese servidor WINS, eliminando NetBEUI.

4. ESPECIFICACIONES TECNICAS DE LAS TECNOLOGIAS ETHERNET DE ALTA VELOCIDAD E IPv6

En el presente capitulo se exponen los fundamentos de las nuevas tecnologías que serán utilizadas en el proceso de migración de la Red de Datos de la Universidad del Cauca como son Gigabit Ethernet, 10 Gigabit Ethernet, e IPv6.

4.1 ESPECIFICACIONES DEL ESTANDAR GIGABIT ETHERNET

4.1.1 ARQUITECTURA DE GIGABIT ETHERNET

El estándar Gigabit Ethernet¹, al igual que los otros estándares existentes de Ethernet, especifica el funcionamiento de las dos capas más bajas del modelo OSI. Estas capas son la capa física y la capa de enlace. Todos los estándares de Ethernet dividen la capa de enlace en dos subcapas: LLC (Link Layer Control) y MAC (Medium Access Control). Para mantener la compatibilidad con Ethernet y Fast Ethernet, la capa LLC no se modificó en el nuevo estándar, y a la capa MAC sólo se le hicieron pequeñas modificaciones que serán explicadas más adelante.

En vez de tratar de definir unos estándares desde cero para especificar la capa física, se utilizaron las dos capas inferiores del estándar ANSI X3T11 (Fibre Channel). Fibre Channel es un estándar que ya lleva varios años en vigencia, y se realizó con el objetivo de definir vías para comunicar datos a altas velocidades. Al principio se pensó sólo para fibra, pero luego se agregó la comunicación por cable de cobre.

¹ Para mayor información referirse al Anexo B.

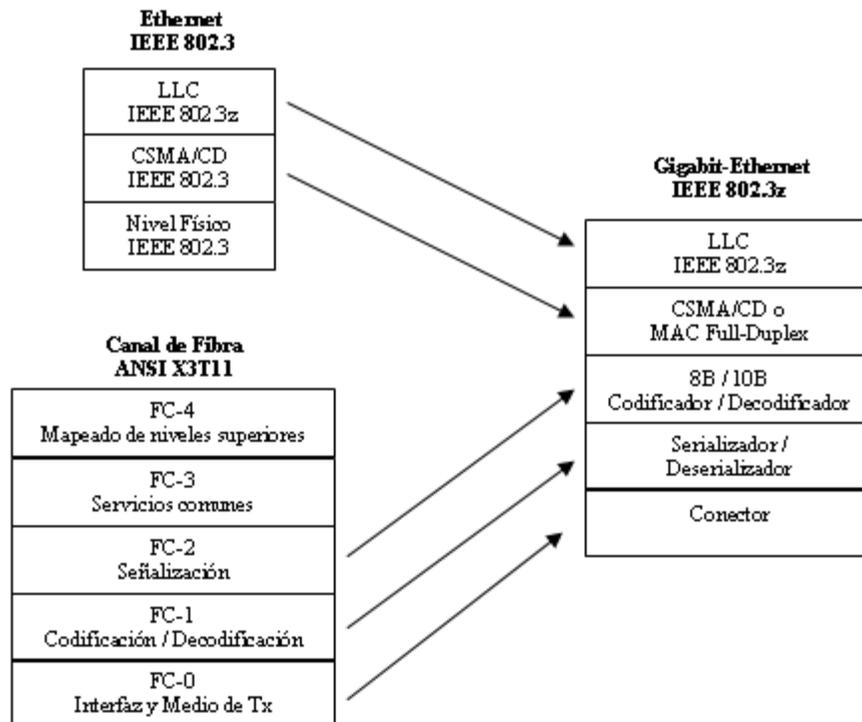


Figura 4. 1. Especificación de capas de Gigabit Ethernet

Como se puede observar en la Figura 4.1, Gigabit Ethernet usa el mismo LLC que Ethernet y el mismo MAC (con unos pequeños cambios), pero la capa física la toma de las dos capas más bajas de Fibre Channel. La capa FC-0 de Fibre Channel especifica todos los posibles tipos de conectores, aparatos y cables que se pueden utilizar para llegar a ciertas velocidades de transmisión. Es decir, FC-0 define todo lo relativo a la capa física.

La capa FC-1 de Fibre Channel, especifica la codificación/decodificación que se tiene que realizar para enviar de manera óptima los datos a través de cada tipo distinto de medio. En el caso de fibra óptica, se usa una codificación creada por IBM llamada 8b/10b. Esta codificación toma una secuencia de 8 bits y las transforma en secuencias de 10 bits, cada una de las cuales debe tener una de estas tres formas: 5 ceros y 5 unos, 4 ceros y 6 unos y 6 ceros y 4 unos. La idea es balancear el número de ceros y unos de manera de eliminar el componente DC. Adicionalmente, el esquema de codificación 8b/10b permite enviar un tipo especial de mensajes de control, que se utilizan para implementar varias opciones de Gigabit Ethernet, como Carrier Extension y Frame Bursting.

Por último, el Serializer/Deserializer es una capa que se agrega para poder serializar la información que llega y adaptarla al esquema de codificación. Por ejemplo para 8b/10b, el Serializer/Deserializer se encarga de juntar todos los bits que llegan en cadenas de 10bits y enviarlas al decodificador. En la figura 4.2 se ilustran los elementos funcionales de Gigabit Ethernet

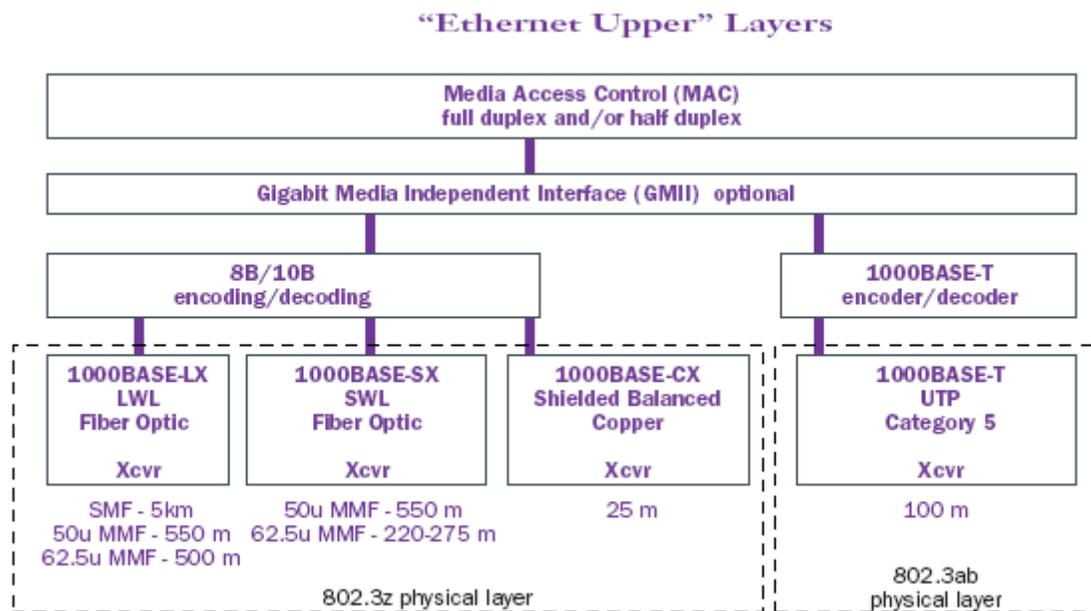


Figura 4. 2. Elementos funcionales de Gigabit Ethernet

4.1.2 CAPA DE ACCESO AL MEDIO

4.1.2.1 NIVEL MAC

Al igual que sus antecesores (Fast Ethernet y Ethernet), en Gigabit Ethernet la capa de control de acceso al medio es la encargada de construir la trama que luego va ser transmitida. Pero la velocidad en la que se transmite dicha trama trae complicaciones que a los otros estándares (en especial Fast Ethernet) no les era de suma importancia.

Las especificaciones a 1000 Mbps utilizan el mismo formato para las tramas y protocolo que el CSMA/CD usando las versiones de IEEE 802.3 a 10 Mbps y 100 Mbps. Se han introducido dos mejoras respecto al esquema CSMA/CD básico en lo que se refiere al funcionamiento de los concentradores:

- **Extensión de la portadora/Carrier Extension:** esta mejora consiste en añadir una serie de símbolos al final de la trama MAC de tal manera que el bloque resultante tenga una duración equivalente a 512 bytes (4096 bits), mucho mayor que los 64 bytes (512 bits) exigidos en el estándar a 10 y 100 Mbps.
- **Ráfagas de tramas/Frame bursting:** Esta funcionalidad permite que se transmitan de forma consecutiva varias tramas cortas (sin superar un límite) sin necesidad de dejar el control de CSMA/CD.

4.1.2.2 NIVEL DE ENLACE LÓGICO

Gigabit Ethernet adopta el formato de trama estándar de Ethernet, que mantiene compatibilidad con los productos base instalados de Ethernet y Fast Ethernet, y no requiere traducción de tramas.

El nivel LLC define servicios de acceso para protocolos que adoptan el Modelo OSI. Desafortunadamente, muchos protocolos no obedecen las reglas de estos niveles. Por lo tanto, se debe añadir información adicional al LLC para proveer la información relativa a estos protocolos. Los protocolos que entran en esta categoría incluyen IP e IPX.

4.1.3 CAPA FÍSICA

La especificación del IEEE 802.3 a 1Gbps define las siguientes alternativas:

- **1000BASE-SX:** esta opción, en la que se usan longitudes de onda pequeñas, proporciona enlaces duplex de 275 m usando fibras multimodo de 62,5 μm o hasta 550 m con fibras multimodo de 50 μm . Las longitudes de onda están en el intervalo comprendido entre 770 y 860 nm.
- **1000BASE-LX:** esta alternativa, en la que se utilizan longitudes de onda mayores, proporcionan enlaces duplex de 550 m con fibras multimodo de 62,5 μm o 50 μm , o de 5 Km con fibras monomodo de 10 μm . Las longitudes de onda están entre los 1270 y los 1355 nm.
- **1000BASE-CX:** esta opción, proporciona enlaces de 1 Gbps entre dispositivos localizados dentro de una habitación (o armario de conexiones) utilizando latiguillos de cobre (cables pares trenzados de menos de 25 m con un apantallamiento especial). Cada enlace consiste en dos pares trenzados apantallados, cada uno de los cuales se usa en un sentido.

- **1000BASE-T:** esta opción, utiliza cuatro pares no apantallados tipo 5 para conectar dispositivos separados hasta 100 m.

4.2 ESPECIFICACIONES DEL ESTANDAR 10 GIGABIT ETHERNET

4.2.1 ARQUITECTURA DE 10 GIGABIT ETHERNET

10 Gigabit Ethernet² define una familia de interfaz física LAN PHY que permite trabajar con tramas nativas Ethernet a una velocidad de 10 Gbps y que cubre las necesidades de los diferentes mercados.

La familia WAN PHY produce flujos de datos a una velocidad de 9.584640 Gbps dentro de una estructura de trama de compatibilidad SONET/SDH que le permite a Ethernet interoperar con las infraestructuras de transporte desplegadas en escenarios MAN/WAN que implementan normalmente puntos de conexión para agregar flujos OC192c/STM64c.

Las diferentes variantes de interfaces físicas definidas por el estándar IEEE 802.3ae que se muestran en la figura 4.3, cubren distintos escenarios de aplicación.



Figura 4. 3. Elementos funcionales de 10GBE

² Para mayor información referirse al Anexo B.

4.2.2 CAPA DE ACCESO AL MEDIO

4.2.2.1 NIVEL MAC

El nivel de control de acceso al medio de 10 Gigabit Ethernet es similar al nivel MAC de las tecnologías Ethernet anteriores. Este utiliza las mismas direcciones MAC y formato de trama, pero no soporta el modo de operación half duplex. Este nivel soporta una tasa de datos de 10 Gbps o menor, utilizando el mecanismo de pacing para adaptación de tasa y control de flujo.

4.2.2.2 NIVEL DE ENLACE LOGICO

Uno de los principales objetivos al desarrollar el estándar de 10 Gigabit Ethernet es utilizar el mismo formato de trama MAC especificado en los anteriores estándares Ethernet. Lo cual permite una integración natural entre 10 Gigabit Ethernet y las redes Ethernet existentes, sin necesidad de implementar funciones de fragmentación, reensamblaje o traducción de direcciones, obteniendo una conmutación más rápida. Ya que solo se opera en el modo full duplex, la distancia del enlace no es afectada por el tamaño de la trama MAC. El tamaño mínimo de la trama puede ser 64 octetos al igual que en los estándares anteriores de Ethernet. No se necesita la técnica de extensión de portadora.

4.2.3 CAPA FISICA

La especificación del IEEE 802.3 a 10Gbps define las siguientes alternativas:

- **10GBASE-SR Y 10GBASE-SW:** 10GBASE-SR y 10GBASE-SW están diseñados para utilizarse sobre fibras multimodo de longitud de onda corta (850 nm). Estos medios se usan para cubrir distancias de 2 a 300 metros, dependiendo de la calidad de la fibra multimodo. Se pueden lograr distancias mayores dependiendo de las cualidades del cable de fibra óptica empleado. 10GBASE-SR es utilizado sobre fibra oscura. 10GBASE-SW está diseñado para conectarse a equipos SONET, los cuales son utilizados típicamente para comunicaciones de datos a grandes distancias.

DESCRIPCION	Fibra de 62.5 μ m		Fibra de 50 μ m			Unidad
	850	850	850	850	850	
Longitud de Onda	850	850	850	850	850	nm
Ancho de Banda Modal	160	200	400	500	2000	Mhz*Km
Rango de Operación	2-26	2-33	2-66	2-82	2-300	m

Tabla 4. 1. Rangos de operación para 10GBASE-S

- **10GBASE-LR Y 10GBASE-LW:** 10GBASE-LR y 10GBASE-LW se utilizan sobre fibras monomodo de longitud de onda larga (1310 nm). Estos medios cubren distancias de 2 metros a 10 kilómetros, dependiendo del tipo y la calidad de la fibra se puede alcanzar distancias mayores. 10GBASE-LR es utilizado sobre fibra oscura, mientras 10GBASE-LW está diseñado para conectarse a equipos SONET.
- **10GBASE-ER Y 10GBASE-EW:** 10GBASE-ER y 10GBASE-EW se utilizan sobre fibras monomodo de longitud de onda larga (1550 nm). Estos medios cubren distancias de 2 metros hasta 40 kilómetros, dependiendo del tipo y la calidad de la fibra se puede alcanzar distancias mayores. 10GBASE-ER es utilizado sobre fibra oscura, mientras 10GBASE-EW está diseñado para conectarse a equipos SONET.
- **10GBASE-LX4:** 10GBASE-LX4 utiliza la tecnología de multiplexación por división de onda para enviar señales sobre cuatro longitudes de onda de luz transportadas en un par de cables de fibra óptica. El sistema 10GBASE-LX4 está diseñado para operar a 1310 nm en fibras oscuras monomodo o multimodo. Se pueden cubrir distancias de 2 hasta 300 metros con fibras multimodo o de 2 metros hasta 10 kilómetros sobre fibras monomodo, se pueden alcanzar distancias mayores dependiendo del tipo y calidad de la fibra.

4.2.3.1 NECESIDAD DE UNA FIBRA DE NUEVA GENERACIÓN

La interfaz de transmisión en primera ventana (850nm) es el más económico de todos, y de aplicación garantizada para distancias cortas.

El comité de estandarización encargado del estándar 10 Gigabit Ethernet creyó la necesidad de establecer dicho interfaz y previó en consecuencia una fibra multimodo capaz de transmitir 10 Gbps en una señal serie de primera ventana hasta 300 metros, algo que no cumplen ninguna de las fibras “tradicional” OM1 y OM2 del mercado.

Los cables de fibra que cumplen con dichas nuevas especificaciones se conocen como Cables de Fibra de Nueva Generación (NGMMOF en el acrónimo inglés) y se denominan OM3 según la nueva clasificación del estándar ISO 11801.

La fibra OM3 presenta un ancho de banda láser a 850 nm de 2000 MHz-km, a diferencia de las fibras OM1 y OM2, que sólo presentan ancho de banda en saturación (200 y 500 MHz-km respectivamente). Además, esta fibra cumple los requisitos de 10 Gigabit Ethernet, y es compatible con las aplicaciones ya existentes.

<i>VELOCIDAD</i>	<i>DISTANCIA</i>		
	300 m	500 m	2000 m
100 Mbps	OM1	OM1	OM1
1000 Mbps	OM1	OM2	OS1
10000 Mbps	OM3	OS1	OS1

Tabla 4. 2. Distancias de la fibra utilizada en 10 Gigabit Ethernet

OM1 y OM2 se refieren a las actuales 62.5/125 y 50/125, respectivamente
 OM3 es la nueva fibra optimizada para laser 50/125
 OS1 es el equivalente a la fibra monomodo G652

4.2.3.2 10 GIGABIT ETHERNET SOBRE CABLEADO DE COBRE

La IEEE 802.3 ha formado recientemente dos nuevos grupos de estudio para investigar sobre el cableado de cobre para 10 Gigabit Ethernet.

El grupo de estudio 10GBASE-CX4 esta desarrollando un estándar para transmitir y recibir señales XAUI mediante 4 pares de cable. Comúnmente referido como cable 4x InfiniBand. El objetivo del grupo de estudio es proveer un estándar para una solución a bajo costo inter-rack y rack a rack. Se espera que el desarrollo del estándar tome aproximadamente un año.

El grupo de estudio 10GBASE-T está desarrollando un estándar para la transmisión y recepción de 10 Gigabit Ethernet mediante cable de cobre UTP categoría 5 o mejor hasta 100 m. Se espera que este desarrollo tome más tiempo que el de 10GBASE-CX4, y se estima que se completará a finales del 2005 o inicios del 2006.

4.2.4 10 GIGABIT ETHERNET EN REDES DE AREA LOCAL

La tecnología Ethernet es ya la tecnología más desplegada por ambientes LAN de alto desempeño. Con la extensión de 10 Gigabit Ethernet dentro de la familia de tecnologías Ethernet, las LANs pueden proveer mejor soporte al creciente número de aplicaciones con gran requerimiento de ancho de banda y alcanzar grandes distancias. Similar al estándar Gigabit Ethernet, la tecnología 10 Gigabit Ethernet soporta la fibra monomodo y multimodo.

Con enlaces de hasta 40 km, 10 Gigabit Ethernet permite a las organizaciones que gestionen en sus propios ambientes LAN la habilidad para escoger estratégicamente la localización de sus centros de datos y granjas de servidores hasta 40 km lejos de sus campus. Esto los habilita para soportar múltiples localizaciones de campus con ese rango de 40 km (figura 4.4). Con centros de datos, aplicaciones switch a switch y

aplicaciones switch a servidor, pueden ser desplegadas sobre fibra multimodo para crear backbones 10 Gigabit Ethernet que soporte el continuo crecimiento de aplicaciones con gran requerimiento de ancho de banda.

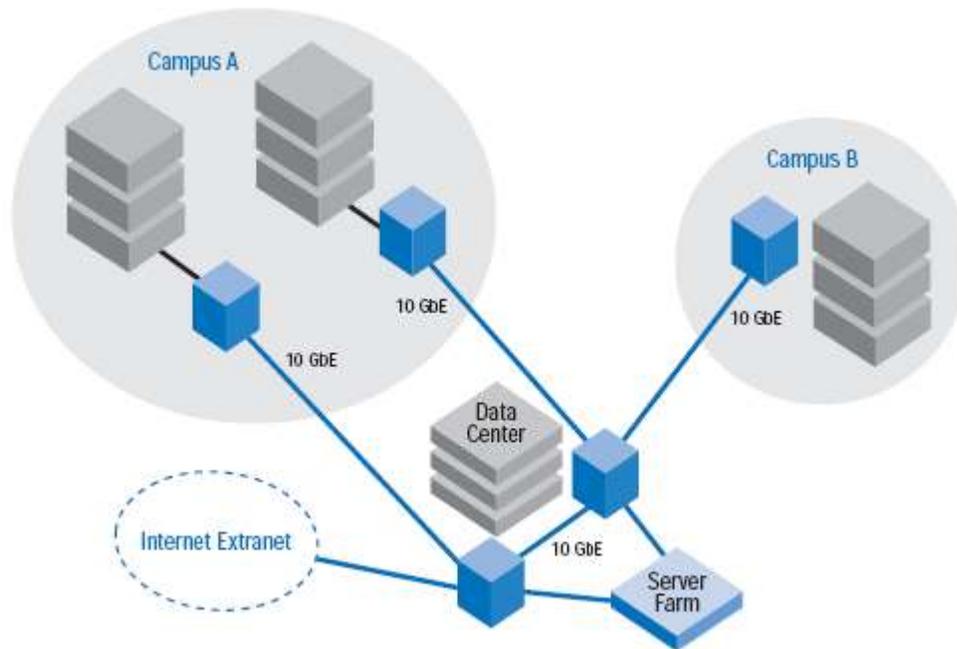


Figura 4. 4. Uso de 10 Gigabit Ethernet en ambientes LAN expandidos

Con backbones 10 Gigabit Ethernet, las organizaciones pueden fácilmente soportar conectividad Gigabit Ethernet en estaciones de trabajo y equipos de escritorio con el fin de brindar mayor capacidad de la red, habilitando una gran implementación de aplicaciones de gran ancho de banda, tales como video streaming, imágenes médicas, aplicaciones centralizadas y gráficos de alta resolución. 10 Gigabit Ethernet también mejora la latencia de la red, debido a la velocidad del enlace y amplio ancho de banda, para compensar la proliferación natural de datos en aplicaciones de la empresa.

El ancho de banda que los backbones 10 Gigabit Ethernet proveen también habilita la nueva generación de aplicaciones de red. Esto puede ayudar a realizar aplicaciones de telemedicina, teleeducación, videoconferencia digital, video bajo demanda, etc.

10 Gigabit Ethernet habilita a las empresas para reducir la congestión de la red, incrementa el uso de aplicaciones de intensivos anchos de banda, y hace más

estratégicas las decisiones acerca de la localización de sus dispositivos claves extendiendo su LAN hasta el límite de 40 km.

4.3 ESPECIFICACIONES DEL PROTOCOLO IPV6

Debido a la preocupación por el agotamiento inminente del conjunto actual de direcciones de Internet y el deseo de proporcionar funcionalidad adicional para dispositivos modernos, se llevó a cabo una actualización de la versión actual del Protocolo Internet (IP, *Internet Protocol*) denominada IPv4. La nueva versión, denominada IP versión 6 (IPv6), resuelve problemas de diseño no previstos en IPv4 y está preparada para llevar Internet al siglo XXI.

4.3.1 FORMATO DE TRAMA IPV6

En primer lugar, se realizará la descripción de la cabecera de un paquete IPv4:

bits:	4	8	16	20	32
Versión	Cabecera	TOS	Longitud Total		
Identificación			Indicador	Desplazamiento de fragmentación	
TTL	Protocolo		Checksum		
Dirección Fuente de 32 bits					
Dirección Destino de 32 bits					
Opciones					

Figura 4. 5. Formato de cabecera IPv4

Como se observa, la longitud mínima de la cabecera IPv4 es de 20 bytes (cada fila de la tabla supone 4 bytes). A ello hay que añadir las opciones, que dependen de cada caso. A continuación se definen cada uno de los campos:

- Versión : Versión (4 bits)
- Header : Cabecera (4 bits)
- TOS (Type Of Service) : Tipo de Servicio (1 byte)
- Total Length : Longitud Total (2 bytes)
- Identification : Identificación (2 bytes)
- Flag : Indicador (4 bits)
- Fragment Offset : Desplazamiento de Fragmentación (12 bits – 1.5 bytes)
- TTL (Time To Live) : Tiempo de Vida (1 byte)
- Protocol : Protocolo (1 byte)

- Checksum : Código de Verificación (2 bytes)
- 32 bit Source Address : Dirección Fuente de 32 bits (4 bytes)
- 32 bit Destination Address : Dirección Destino de 32 bits (4 bytes)

En la figura anterior, se han marcado, los campos que van a desaparecer en IPv6, y los que son modificados, según el siguiente esquema:

Campo modificado
Campo que desaparece

En el nuevo IP, se ha pasado de tener 12 campos, como en IPv4, a tan solo 8. El motivo fundamental por el que los campos son eliminados es la innecesaria redundancia. En IPv4 se facilita la misma información de varias formas. Un caso muy evidente es el checksum o verificación de la integridad de la cabecera, cuya función ya es realizada por otros mecanismos de encapsulado (IEEE 802 MAC, framing PPP, capa de adaptación ATM, etc.). El caso del campo de “Desplazamiento de Fragmentación”, es ligeramente diferente, dado que el mecanismo por el que se realiza la fragmentación de los paquetes se ha modificado totalmente en IPv6, lo que implica la total “inutilidad” de este campo. En IPv6 los enrutadores no fragmentan los paquetes, sino que de ser precisa, dicha fragmentación o desfragmentación se produce extremo a extremo.

Algunos de los campos han adoptado otras denominaciones:

- **Longitud total: longitud de carga útil (payload length).** Es, en definitiva, la longitud de los propios datos, y puede ser de más de 65.536 bytes. Tiene una longitud de 16 bits (2 bytes).
- **Protocolo: siguiente cabecera (next header).** Dado que en lugar de usar cabeceras de longitud variables se emplean sucesivas cabeceras encadenadas, desaparece el campo de opciones. En muchos casos ni siquiera es procesado por los enrutadores, sino tan sólo extremo a extremo. Tiene una longitud de 8 bits (1 byte).
- **Tiempo de vida: límite de saltos (Hop Limit).** Tiene una longitud de 8 bits (1 byte).

Los nuevos campos son:

- **Clase de Tráfico (Traffic Class):** también denominado Prioridad (Priority), o simplemente Clase (Class). Podría ser más o menos equivalente a TOS en IPv4. Tiene una longitud de 8 bits (1 byte).
- **Etiqueta de Flujo (Flow Label):** para permitir tráfico con requisitos de tiempo real. Tiene una longitud de 20 bits.

Estos dos campos, como se puede suponer, son los que permiten una de las características fundamentales e intrínsecas de IPv6: Calidad de Servicio (QoS), Clase de Servicio (CoS), y en definitiva un poderoso mecanismo de control de flujo, de asignación de prioridades diferenciadas según los tipos de servicios.

Por tanto, en el caso de un paquete IPv6, la cabecera tendría el siguiente formato:



Figura 4. 6. Formato de cabecera IPv6

El campo de versión, que es igual a 6, lógicamente, tiene una longitud de 4 bits.

La longitud de esta cabecera es de 40 bytes, el doble que en el caso de IPv4, pero con muchas ventajas, al haberse eliminado campos redundantes.

Además, la longitud fija de la cabecera implica una mayor facilidad para su procesamiento en routers y switches, incluso mediante hardware, lo que implica unas mayores prestaciones.

A este fin contribuye el hecho de que los campos están alineados a 64 bits, lo que permite que las nuevas generaciones de procesadores y microcontroladores, de 64 bits, puedan procesar mucho más eficazmente la cabecera IPv6.

El valor del campo “siguiente cabecera”³, indica cual es la siguiente cabecera y así sucesivamente. Las sucesivas cabeceras, no son examinadas en cada nodo de la ruta, sino sólo en el nodo o nodos destino finales. Hay una única excepción a esta regla: cuando el valor de este campo es cero, lo que indica opción de examinado y proceso “salto a salto” (hop-by-hop). Así se tiene, por citar algunos ejemplos, cabeceras con información de encaminado, fragmentación, opciones de destino, autenticación, encriptación, etc., que en cualquier caso, han de ser procesadas en el orden riguroso en que aparecen en el paquete.

La MTU (Unidad Máxima de Transmisión) debe de ser como mínimo, de 1.280 bytes, aunque se recomiendan tamaños superiores a 1.500 bytes. Los nodos descubren el valor MTU a través de la inspección de la ruta. Se prevé así una optimización de los paquetes y del número de cabeceras, dado el continuo crecimiento de los anchos de banda disponibles, así como del incremento del propio tráfico. Dado que IPv6 no realiza verificación de errores de la cabecera en tráfico UDP, se requiere el empleo del su propio mecanismo de checksum.

4.3.2 DIRECCIONAMIENTO

Una dirección IPv6 es de 128 bits, cuatro veces más larga que una IPv4. Una de las principales razones que han empujado a que se desarrollase una nueva versión del protocolo es el inminente agotamiento de las direcciones disponibles, debido al esquema de clases de direcciones del IPv4. En cambio, el IPv6 define un nuevo sistema orientado al eficaz enrutamiento en la red.

4.3.2.1 TIPOS DE DIRECCIONES EN IPV6

En IPv4 había tres tipos de direcciones: Unicast, Multicast y Broadcast. En IPv6 no hay el Broadcast, la difusión de paquetes a una red o subred, mal soportado por algunas topologías de redes físicas es reemplazado. Además se introduce el concepto de Anycast.

UNICAST

Como en IPv4, una dirección Unicast identifica únicamente a una interfaz de red. Los paquetes dirigidos a una dirección de Unicast sólo serán entregados a la interfaz indicada por esa dirección.

³ En el anexo A se presentan algunos ejemplos gráficos del uso de cabeceras de extensión.

MULTICAST

Como en IPv4, una dirección Multicast identifica únicamente a un conjunto de interfaces de red. Los paquetes dirigidos a una dirección de Multicast serán entregados a todas las interfaces que pertenecen a ese conjunto.

ANYCAST

Novedad del IPv6, una dirección Anycast identifica múltiples interfaces de red. Los paquetes dirigidos a una dirección de Anycast serán entregados a una de esas interfaces, generalmente la más próxima.

4.3.2.2 DIRECCIONES UNICAST

DIRECCIONES UNICAST GLOBALES AGREGABLES

Las direcciones Unicast Globales Agregables son identificadas por el prefijo 001. La dirección es dividida en cinco partes, para permitir una atribución jerárquica: el identificador de TLA (Top Level Aggregation) indica el nivel más alto de organización; el identificador NLA (Next Level Aggregation) el proveedor de servicios (ISP) o el punto de acceso; el identificador SLA (Site Level Aggregation) permite a los administradores de redes gestionar la estructura interna de la red de una organización. Además hay 8 bits reservados para un uso futuro.

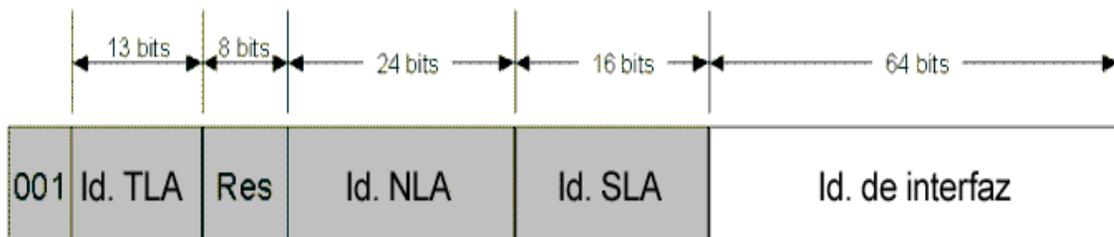


Figura 4. 7. Dirección unicast global agregable

DIRECCIONES LOCALES DE ENLACE Y DE SITIO

En IPv4 están asignadas unas clases de direcciones para uso local y privado, por ejemplo en las LANs. Los routers no pasan las direcciones privadas al exterior de la red local, es una tarea de los NATs traducir las direcciones privadas a direcciones válidas para Internet.

En IPv6 existen dos clases distintas de direcciones privadas: las locales de enlace y las locales de sitio, para uso a nivel de enlace directo o bien a nivel de sitio. Una dirección a nivel de enlace puede ser usada por un host que empieza el procedimiento de autoconfiguración, en redes sin routers y para el descubrimiento de vecinos. Por ejemplo se puede usar un conjunto de direcciones locales de enlace para conectar dos ordenadores entre ellos y una impresora de red, o bien para jugar en red entre dos

ordenadores en el mismo cuarto. Las direcciones locales de sitio pueden ser usadas dentro de un sitio, y también enrutadas dentro del sitio, pero nunca al exterior. El prefijo de las direcciones local de enlace y local de sitio es respectivamente FE80::/10 y FEC0::/10.

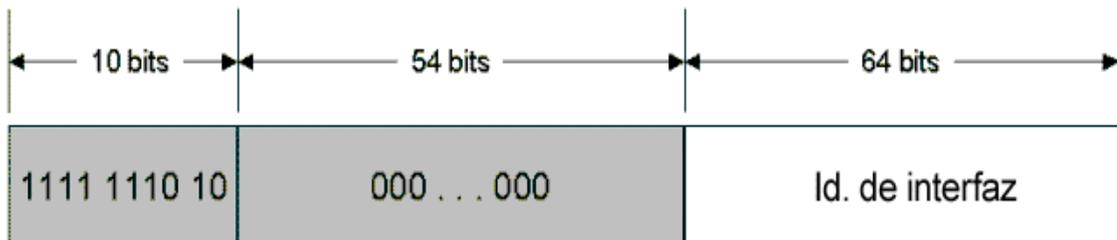


Figura 4. 8. Dirección local de enlace

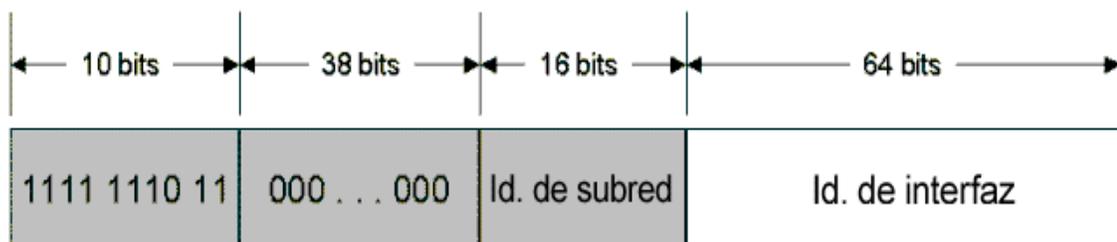


Figura 4. 9. Dirección local de sitio

DIRECCIONES ESPECIALES

La dirección no especificada tiene valor de 0:0:0:0:0:0:0 y es válida para dirección fuente de una interfaz que no tiene aún asignada una dirección. Nunca puede ser asignada como dirección estática o dinámica a un host y no puede ser la dirección destino de paquetes IPv6.

La dirección de bucle cerrado (loopback) es útil para hacer pruebas con la pila de protocolos TCP/IP y es indicada por 0:0:0:0:0:0:1 o bien ::1. Los paquetes enviados a esa dirección nunca salen a la red. Como la anterior, nunca puede ser asignada como dirección estática o dinámica a un host.

Además hay tres otras clases de direcciones IPv6, hechas para compatibilidad con IPv4 y para permitir la transición gradual a IPv6: las direcciones IPv6 con direcciones IPv4 en su interior (IPv4-compatible y IPv4-mapped), las direcciones 6to4 y las direcciones ISATAP. Son interfaces virtuales y a menudo se llaman pseudo-interfaces.

4.3.2.3 DIRECCIONES ANYCAST

Una dirección anycast se asigna a varias interfaces. La infraestructura de enrutamiento reenvía los paquetes dirigidos a una dirección de unicast a la interfaz más próxima a la que esté asignada la dirección anycast. Para facilitar la entrega, la infraestructura de enrutamiento debe conocer las interfaces a las que se asignan direcciones anycast y su "distancia" en términos de medida de enrutamiento. Actualmente, las direcciones anycast sólo se utilizan como direcciones de destino y se asignan únicamente a los enrutadores. Las direcciones anycast se asignan fuera del espacio de direcciones de unicast y el ámbito de una dirección anycast es el ámbito del tipo de dirección de unicast desde el que se asigna la dirección anycast.

La dirección anycast de Subred-Enrutador está predefinida y es necesaria. Se crea a partir del prefijo de subred para una interfaz dada. Para crear la dirección anycast de Subred-Enrutador, los bits del prefijo de subred quedan fijos en sus valores correspondientes y los bits restantes se establecen en 0. La figura 4.10 ilustra la dirección anycast de Subred-Enrutador.

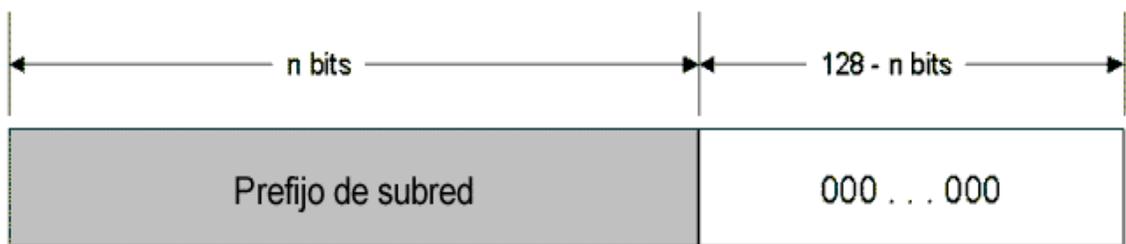


Figura 4. 10. Formato de la dirección Subnet Router Anycast

Todas las interfaces de enrutador conectadas a una subred se asignan a la dirección anycast de Subred-Enrutador de la subred. La dirección anycast de Subred-Enrutador se utiliza para la comunicación con uno o varios enrutadores conectados a una subred remota.

4.3.2.4 DIRECCIONES MULTICAST

Las direcciones Multicast tienen el prefijo de FF00::/8 e identifican un grupo de nodos. Un nodo puede pertenecer a uno o más grupos de multicast. En IPv6 las direcciones multicast se redefinen de acuerdo al siguiente esquema:

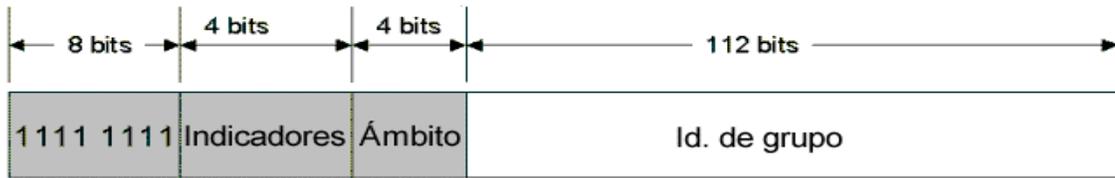


Figura 4. 11. Formato de una dirección multicast

El primer byte identifica la dirección de Multicast. De los siguientes 4 bits de Indicadores, los primeros tres no son usados y están reservados para uso futuro. El cuarto bit indica si puesto a uno si ésta es una dirección de multicast bien conocida⁴, o bien si es temporánea, si puesto a cero. Los 4 bits de Scope⁵ (ámbito) indican la visibilidad de la dirección:

DIRECCIONES SOLICITED-NODE MULTICAST

La dirección Solicited-Node Multicast es una dirección de multicast asociada a cualquier dirección de tipo Unicast o Anycast. Su utilidad es la de permitir el proceso de detección de direcciones duplicadas (DAD). La dirección Solicited-Node Multicast se construye a partir de los últimos 24 bits de la dirección de Unicast o de Anycast, y con el prefijo bien conocido FF02:0:0:0:0:1:FF00::/104.

Las direcciones posibles son 224, de FF02::1:FF00:0 hasta FF02::1:FFFF:FFFF. Por ejemplo, la dirección asociada a la de Unicast FE80::202:3FFF:FEBD:6008 es FF02::1:FFBD:6008.

4.3.3 PROTOCOLO ICMPV6

El protocolo de mensajes de control de Internet ICMP, descrito originalmente en el documento RFC 792 para IPv4, ha sido actualizado para permitir su uso bajo IPv6.

El protocolo resultante de dicha modificación es ICMPv6, y se le ha asignado un valor para el campo de “siguiente cabecera”, igual a 58. ICMPv6 es parte integral de IPv6 y debe ser totalmente incorporado a cualquier implementación de nodo IPv6.

ICMPv6 es empleado por IPv6 para reportar errores que se encuentran durante el procesamiento de los paquetes, así como para la realización de otras funciones relativas a la capa “Internet”, como diagnósticos (“ping”).

El formato genérico de los mensajes ICMPv6 es el siguiente:

⁴ Las direcciones multicast bien conocidas se especifican en el anexo A.

⁵ En el anexo A se especifican los valores definidos para este campo.

bits	8	16	32
Tipo	Código	Checksum	
Cuerpo del Mensaje			

Figura 4. 12. Formato de los mensajes ICMPv6

El campo “tipo” indica el tipo de mensaje, y su valor determina el formato del resto de la cabecera.

El campo “código” depende del tipo de mensaje, y se emplea para crear un nivel adicional de jerarquía para la clasificación del mensaje.

El checksum o código de redundancia nos permite detectar errores en el mensaje ICMPv6.

Los mensajes ICMPv6⁶ se agrupan en dos tipos o clases: mensajes de error y mensajes informativos. Los mensajes de error tienen cero en el bit de mayor peso del campo “tipo”, por lo que sus valores se sitúan entre 0 y 127.

Los valores de los mensajes informativos oscilan entre 128 y 255.

Los mensajes definidos por la especificación básica son los siguientes:

⁶ En el anexo A se describen de manera detallada los mensajes ICMPv6

Mensajes de error ICMPv6	
Tipo	Descripción y Códigos
1	Destino no alcanzable (Destination Unreachable)
	<small>Código</small> <small>Descripción</small>
	0 Sin ruta hacia el destino
	1 Comunicación prohibida administrativamente
	2 Sin asignar
	3 Dirección no alcanzable
	4 Puerto no alcanzable
2	Paquete demasiado grande (Packet Too Big)
3	Tiempo excedido (Time Exceeded)
	<small>Código</small> <small>Descripción</small>
	0 Límite de saltos excedido
	1 Tiempo de desfragmentación excedido
4	Problema de parámetros (Parameter Problem)
	<small>Código</small> <small>Descripción</small>
	0 Campo erróneo en cabecera
	1 Tipo de "cabecera siguiente" desconocida
	2 Opción IPv6 desconocida
Mensajes informativos ICMPv6	
Tipo	Descripción
128	Solicitud de eco (Echo Request)
129	Respuesta de eco (Echo Reply)

Tabla 4. 3. Tipos de mensajes ICMPv6

Por razones de seguridad, las cabeceras ICMPv6 pueden ser autenticadas y encriptadas, usando la cabecera correspondiente. El uso de este mecanismo permite, además, la prevención de ataques ICMP, como el conocido "Negación de servicio" (DoS Denial of Service Attack).

4.3.4 PROTOCOLO NEIGHBOR DISCOVERY (ND)

En IPv6, el protocolo equivalente, en cierto modo a ARP en IPv4, es el que se denomina "descubrimiento de vecindario". Sin embargo, incorpora también la funcionalidad de otros protocolos IPv4, como "ICMP Router Discovery" e "ICMP Redirect".

ND consiste en el mecanismo por el cual un nodo que se incorpora a una red, descubre la presencia de otros, en su mismo enlace, para determinar sus direcciones

en la capa de enlace, para localizar los routers, y para mantener la información de conectividad (“reachability”) acerca de las rutas a los “vecinos” activos.

El protocolo ND también se emplea para mantener limpios los “caches” donde se almacena la información relativa al contexto de la red a la que esta conectado un nodo (host o router), y por tanto para detectar cualquier cambio en la misma. Cuando un router, o una ruta hacia él, falla, el host buscará alternativas funcionales.

ND emplea los mensajes de ICMPv6, incluso a través de mecanismos de multicast en la capa de enlace, para algunos de sus servicios.

El protocolo ND es bastante completo y sofisticado, ya que es la base para permitir el mecanismo de autoconfiguración en IPv6.

Define, entre otros, mecanismos para: descubrir routers, prefijos y parámetros, autoconfiguración de direcciones, resolución de direcciones, determinación del siguiente salto, detección de nodos no alcanzables, detección de direcciones duplicadas o cambios, redirección, balanceo de carga entrante, direcciones anycast, y Anuncio de proxies.

ND define cinco tipos de paquetes ICMPv6⁷:

- **Solicitud de Router (Router solicitation):** Generado por una interfaz cuando es activada, para pedir a los routers que se “anuncien” inmediatamente. Tipo en paquete ICMPv6 = 133.
- **Anuncio de router (Router Advertisement):** Generado por los routers periódicamente (entre cada 4 y 1800 segundos) o como consecuencia de una “solicitud de router”, a través de multicast, para informar de su presencia así como de otros parámetros de enlace y de Internet, como prefijos (uno o varios), tiempos de vida, configuración de direcciones, limite de salto sugerido, etc. Es fundamental para permitir la reenumeración. Tipo en paquete ICMPv6 = 134.
- **Solicitud de vecino (Neighbor Solicitation):** Generado por los nodos para determinar la dirección en la capa de enlace de sus vecinos, o para verificar que el nodo vecino sigue activo (es alcanzable), así como para detectar las direcciones duplicadas. Tipo en paquete ICMPv6 = 135.

⁷ En el anexo A se detallan los tipos de paquetes ICMPv6 empleados por el protocolo ND.

- **Anuncio de vecino (Neighbor Advertisement):** Generado por los nodos como respuesta a la “solicitud de vecino”, o bien para indicar cambios de direcciones en la capa de enlace. Tipo en paquete ICMPv6 = 136.
- **Redirección (Redirect):** Generado por los routers para informar a los hosts de un salto mejor para llegar a un determinado destino. Equivalente, en parte a “ICMP redirect”. Tipo en paquete ICMPv6 = 137.

4.3.5 AUTOCONFIGURACIÓN DE DIRECCIONES

La autoconfiguración es el conjunto de pasos por los cuales un host decide como autoconfigurar sus interfaces en IPv6. Este mecanismo es el que permite afirmar que IPv6 es “Plug & Play”.

El proceso incluye la creación de una dirección de enlace local, verificación de que no esta duplicada en dicho enlace y determinación de la información que ha de ser autoconfigurada (direcciones y otra información).

Las direcciones pueden obtenerse de forma totalmente manual, mediante DHCPv6 (stateful o configuración predeterminada), o de forma automática (stateless o descubrimiento automático, sin intervención).

Este protocolo define el proceso de generar una dirección de enlace local, direcciones globales y locales de sitio, mediante el procedimiento automático (stateless). También define el mecanismo para detectar direcciones duplicadas.

La autoconfiguración “stateless” (sin intervención), no requiere ninguna configuración manual del host, configuración mínima (o ninguna) de routers, y no precisa servidores adicionales. Permite a un host generar su propia dirección mediante una combinación de información disponible localmente e información anunciada por los routers. Los routers anuncian los prefijos que identifican la subred (o subredes) asociadas con el enlace, mientras el host genera un “identificador de interfaz”, que identifica de forma única la interfaz en la subred. La dirección se compone por la combinación de ambos campos. En ausencia de router, el host solo puede generar la dirección de enlace local, aunque esto es suficiente para permitir la comunicación entre nodos conectados al mismo enlace.

En la autoconfiguración “stateful” (predeterminada), el host obtiene la dirección de la interfaz y/o la información y parámetros de configuración desde un servidor. Los servidores mantienen una base de datos con las direcciones que han sido asignadas a cada host.

Ambos tipos de autoconfiguración (stateless y stateful), se complementan. Un host puede usar autoconfiguración sin intervención (stateless), para generar su propia dirección, y obtener el resto de parámetros mediante autoconfiguración predeterminada (stateful).

El mecanismo de autoconfiguración “sin intervención” se emplea cuando no importa la dirección exacta que se asigna a un host, sino tan solo asegurarse que es única y correctamente enrutable.

El mecanismo de autoconfiguración predeterminada, por el contrario, nos asegura que cada host tiene una determinada dirección, asignada manualmente.

Cada dirección es cedida a una interfaz durante un tiempo predefinido (posiblemente infinito). Las direcciones tienen asociado un tiempo de vida, que indican durante cuanto tiempo esta vinculada dicha dirección a una determinada interfaz. Cuando el tiempo de vida expira, la vinculación se invalida y la dirección puede ser reasignada a otra interfaz en cualquier punto de Internet.

Para gestionar la expiración de los vínculos, una dirección pasa a través de dos fases diferentes mientras esta asignada a una interfaz. Inicialmente, una dirección es “preferred” (preferida), lo que significa que su uso es arbitrario y no está restringido. Posteriormente, la dirección es “deprecated” (desaprobada), en anticipación a que el vínculo con su interfaz actual va a ser anulado.

Mientras está en estado “desaprobado”, su uso es desaconsejado, aunque no prohibido. Cualquier nueva comunicación (por ejemplo, una nueva conexión TCP), debe usar una dirección “preferida”, siempre que sea posible.

Una dirección “desaprobada” debería ser usada tan solo por aquellas aplicaciones que ya la venían utilizando y a las que les es muy difícil cambiar a otra dirección sin interrupción del servicio.

Para asegurarse de que todas las direcciones configuradas son únicas, en un determinado enlace, los nodos ejecutan un algoritmo de detección de direcciones duplicadas, antes de asignarlas a una interfaz. Este algoritmo es ejecutado para todas las direcciones, independientemente de que hayan sido obtenidas mediante autoconfiguración stateless o stateful.

La autoconfiguración esta diseñada para hosts, no para routers, aunque ello no implica que parte de la configuración de los routers también pueda ser realizada automáticamente (generación de direcciones de enlace local). Además los routers también tienen que “aprobar” el algoritmo de detección de direcciones duplicadas.

4.3.6 DESCUBRIMIENTO DEL MTU

En la versión anterior del protocolo, los paquetes podían ser fragmentados por cualquier router. Si un router no podía enrutar un paquete porque era más largo que el MTU del siguiente enlace, lo fragmentaba, así que un mismo paquete podía ser fragmentado más de una vez a lo largo del camino.

En IPv6 sólo la fuente puede fragmentar los paquetes. Si un router no puede enrutar un paquete debido a su tamaño mayor que el MTU, lo rechaza y envía atrás a la fuente un mensaje de error ICMPv6 Packet Too Big, con el valor del MTU para aquel enlace.

El proceso de descubrimiento del MTU funciona así: el host supone que el MTU del camino es igual que el MTU del primer salto. Si el tamaño del paquete es demasiado grande para algún router a lo largo del camino, él envía un mensaje de error ICMP con el valor del MTU para aquel enlace. El host entonces reduce el valor del MTU hasta que no lleguen más mensajes de error. Desde luego, el MTU nunca será menor que el valor del mínimo MTU IPv6 de 1280 bytes. Como los caminos pueden cambiar en la red, de vez en cuando el host intentará aumentar el valor del MTU.

El proceso de descubrimiento del MTU considera también los destinos de multicast. Como no se pueden enviar distintos paquetes hacia cada uno de los participantes de un grupo, sino es tarea de los routers enrutar hacia cada uno de ellos, el host sólo envía un paquete, así que el tamaño debe ser el mínimo entre los permitidos para cada uno de los destinos.

Como no está obligatorio, no todos los host aplican el descubrimiento del MTU pero por supuesto reaccionan de manera adecuada a la llegada de mensajes de error Packet Too Big.

4.3.7 TRANSICION DE IPv4 HACIA IPv6

Los diseñadores de IPv6 reconocieron que la transición de IPv4 a IPv6 tomaría muchos años y que habría organizaciones o hosts dentro de organizaciones que continuarían su uso para siempre. A pesar que la migración es a largo plazo, existen ciertas consideraciones que permitirán la coexistencia de ambos protocolos.

Los diseñadores de IPv6 en la especificación original (RFC 1752) definieron los siguientes criterios de transición.

- Los hosts existentes con IPv4 podrán ser actualizados en cualquier momento, independientemente de la actualización de los otros hosts o enrutadores.

- Los nuevos hosts, utilizando sólo IPv6, pueden ser agregados en cualquier momento, sin dependencias de otros hosts u infraestructura de enrutamiento.
- Los hosts existentes con IPv4, con IPv6 instalado, pueden continuar utilizando direcciones IPv4 sin necesitar direcciones adicionales.
- Se requiere de una pequeña preparación ya sea para actualizar de IPv4 a IPv6 o para implementar nuevos nodos IPv6.

La inherente falta de dependencia entre los hosts de IPv4 e IPv6 y la infraestructura de enrutamiento IPv4 e IPv6, requiere de mecanismos que permitirán la coexistencia de los dos protocolos de manera transparente.

4.3.8 MECANISMOS DE TRANSICION DE IPv4 A IPv6

Es razonable pensar que IPv4 e IPv6 coexistirán por muchos años. Por eso se han previsto técnicas para permitir a los dos protocolos de convivir y a las empresas y organizaciones de actualizar sus equipos e infraestructuras poco a la vez. Hay tres principales categorías:

- Técnicas de doble pila (Dual Stack) que permiten a IPv4 e IPv6 coexistir en el mismo equipo o red.
- Técnicas de tunneling para enrutar tráfico IPv6 dentro de paquetes IPv4.
- Técnicas de traducción (NAT), para permitir a nodos IPv6 poderse comunicar con nodos IPv4.

4.3.8.1 TÉCNICAS DE DOBLE PILA (DUAL STACK)

La técnica de Dual Stack consiste en que un nodo tiene soporte completo para las dos implementaciones de IP. Cuando se trata de comunicar con nodos IPv4, el nodo se comporta como si fuese un nodo IPv4, mientras que con los nodos IPv6 se comporta como un nodo IPv6.

Los inconvenientes de esta técnica son que los nodos necesitan una completa actualización de software de red. La presencia de las dos pilas se traduce en un aumento de la carga para el procesador y una mayor ocupación de memoria: de hecho los routers y los hosts deben tener dos copias de las tablas de enrutamiento y de otros recursos asociados a los protocolos. Las aplicaciones deberán ser capaces de reconocer si el host está comunicando con otro host IPv6 o IPv4. A menudo habrá dos versiones de la misma aplicación, una por cada protocolo (p.ej. ping y ping6 bajo Windows). La ventaja es que cuando ya no sea necesario el IPv4, se podrá quitar o remover el modulo correspondiente del sistema operativo.

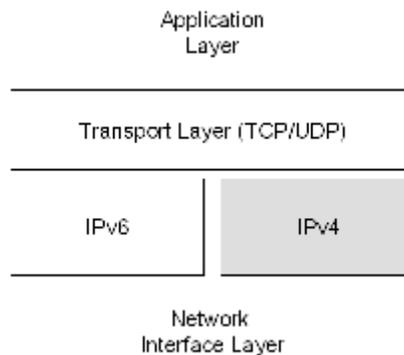


Figura 4. 13. Dual Stack, protocolos IPv4 e IPv6

4.3.8.2 TÉCNICAS DE TUNNELING

Las técnicas de tunneling consisten en que los paquetes IPv6 se encapsulan en paquetes IPv4 como si fueran de otro protocolo de nivel superior (por ejemplo TCP) y se enrutan en redes IPv4 a lo largo de un túnel, que tiene un extremo que se ocupa de encapsular y otro que saca el paquete IPv6 y lo enruta hacia su destino. Los túneles pueden ser configurados de manera manual o bien ser de tipo automático.

COMO FUNCIONA EL TUNNELING

Las fases de la encapsulación de paquetes IPv6 son las siguientes:

1. El router a la entrada del túnel decrementa el valor del campo Hop Limit del paquete IPv6 de una unidad y crea un paquete IPv4 con el valor 41 en el campo Protocol Type. La longitud del paquete es calculada sumando la longitud de la cabecera IPv6, las eventuales cabeceras adicionales y el contenido del paquete. Si es necesario el router fragmenta el paquete. El destino del nuevo paquete IPv4 es la salida del túnel.
2. El router a la salida del túnel recibe el paquete IPv4. Si es fragmentado, espera todos los fragmentos y los reúne. Luego saca el paquete IPv6 y lo encamina hacia su destino.

El túnel es considerado como un salto único. No hay manera para que un host IPv6 se entere de que el paquete ha sido encapsulado a lo largo de su camino por medio de herramientas como traceroute.

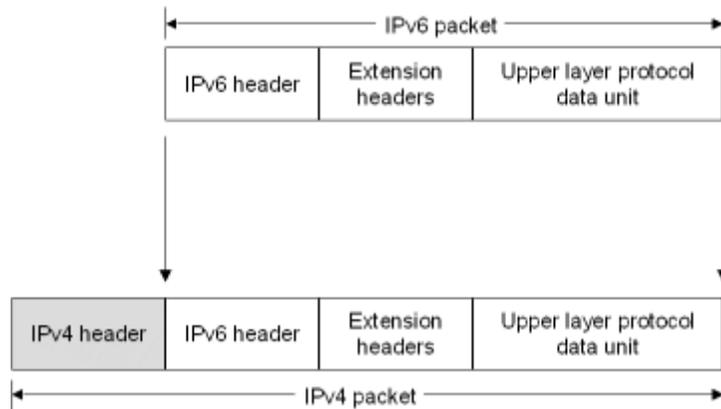


Figura 4. 14. Tunneling IPv6 sobre IPv4

TUNNELING MANUAL

El tunneling manual requiere configuración manual de los extremos del túnel. En este caso el extremo final del túnel es distinto del destino final del paquete, por lo que la dirección en el paquete IPv6 no proporciona la dirección IPv4 del extremo final del túnel. La dirección del extremo final del túnel debe ser determinada a través de información de configuración en el nodo que realiza el túnel.

TUNNELING AUTOMÁTICO

El tunneling automático permite a hosts IPv4/IPv6 comunicarse en una red IPv4, sin necesidad de configurar túneles, usando unas clases especiales de direcciones IPv6 que tienen dentro de sí una dirección IPv4 que es la de la entrada del túnel.

El RFC 3056 define un mecanismo para conectar redes IPv6 dentro de una infraestructura de red IPv4 llamada 6to4.



Figura 4. 15. Formato de la dirección 6to4

Este mecanismo se puede aplicar para comunicar redes IPv6 aisladas por medio de la red IPv4. El router extremo de la red IPv6 crea un túnel sobre IPv4 para alcanzar la otra red IPv6. Los extremos del túnel son identificados por el prefijo del sitio IPv6. Este prefijo consiste en 16 bits fijos que indican que se esta utilizando la técnica 6to4 más 32 bits que identifican al router externo del ‘sitio’.

Un efecto secundario de 6to4 es que deriva automáticamente un prefijo /48 de una dirección IPv4. De esta forma, los ‘sitios’ pueden empezar a utilizar IPv6 sin solicitar nuevo espacio de direccionamiento a la autoridad competente.

Otro estándar de reciente salida es el de ISATAP (Intra Site Automatic Tunnel Address Protocol) que permite a hosts IPv6 que están en una red local IPv4 de intercambiar tráfico IPv6 encapsulado en IPv4. La dirección ISATAP es compuesta por el prefijo asignado a la red, y por 64 bits formados por el OUI (Organization Unique Identifier) de IANA 0000 5EFE y los 32 bits de la dirección IPv4 del host.

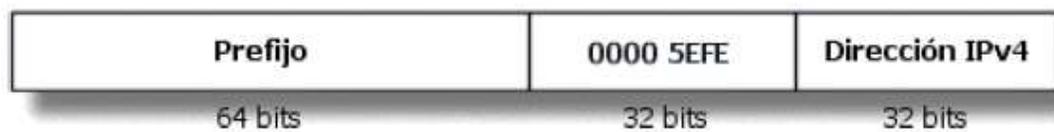


Figura 4. 16. Formato de una dirección ISATAP

Con ISATAP, los host pueden enviar tráfico IPv6 uno a otro sin necesidad de routers. Para alcanzar otros hosts IPv6 en Internet, un router se requiere un router ISATAP o bien un router 6to4.

4.3.8.3 TÉCNICAS DE TRADUCCIÓN

Las técnicas de traducción permiten, con unas limitaciones, a hosts IPv4 comunicarse con hosts IPv6. Básicamente se trata de instalar un NAT gateway que traduzca el tráfico IPv4 a IPv6 y viceversa, de manera transparente. El RFC 2765 define reglas para traducir los paquetes IP e ICMP.

El funcionamiento de un NAT (Network Address Translation) gateway es de asociar a cada uno de los hosts IPv6 una dirección de un conjunto a él asignado, por ejemplo 120.10.40/24 en notación CIDR. Los paquetes que llegan del host ABCD:EEFF::1234:5678 son traducidos a IPv4 con dirección fuente 120.10.40.10. Además si el NAT puede traducir números de puertos (NAPT) cambia el número del puerto de 3056 a 1025. El host IPv4 envía a su vez un paquete IPv4 al destino 120.10.40.10 (que en realidad no existe), y el NAPT se ocupa de construir un paquete IPv6 con la dirección destino del host IPv6. El NAPT tiene que memorizar las asociaciones hechas a lo largo de la sesión.

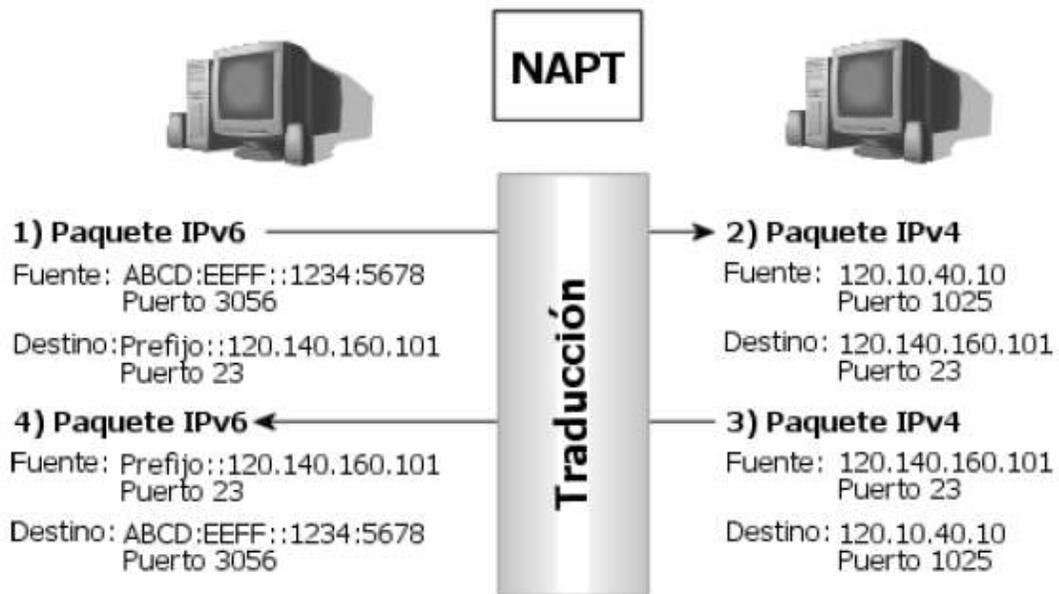


Figura 4. 17. Funcionamiento de un NAPT

Las limitaciones del NAT/NAPT son ya conocidas y son que los paquetes tienen que pasar siempre por el mismo sitio (el NAPT) porque sólo él tiene en memoria las asociaciones de direcciones. Además el proceso de traducción no tiene en cuenta las direcciones IP que están dentro del contenido de los paquetes, por ejemplo dentro de órdenes FTP, consultas DNS u otras aplicaciones de nivel superior. Por eso, es necesario añadir un servicio de ALG (Application Layer Gateway). Por último, el proceso de traducción no permite aprovechar las funciones avanzadas de IPv6 como por ejemplo las de seguridad.

5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD

En este capítulo se realizan las diferentes opciones de diseño para la nueva arquitectura de la Red de Datos de la Universidad del Cauca, para lo cual inicialmente se presentan las consideraciones que se deben tener en cuenta para la migración de la red, se expone la metodología de diseño que se utiliza en dicho proceso y se especifican las características técnicas que deben reunir los dispositivos de Internetworking para la realización de un diseño óptimo.

5.1 CONSIDERACIONES PARA LA MIGRACION HACIA GIGABIT ETHERNET

Las organizaciones modernas dependen de sus redes de área local (LANs) para proveer conectividad para un creciente número de aplicaciones informáticas críticas y complejas. El volumen de tráfico de la red incrementa, sin embargo, el ancho de banda ofrecido por una típica LAN Ethernet a 10/100 Mbps rápidamente se ha vuelto inadecuado para mantener un desempeño aceptable para un creciente número de ambientes informáticos de equipos cliente-servidor. Este embotellamiento de tráfico ha originado la necesidad de redes de más alta velocidad.

Entre las tecnologías LAN disponibles en la actualidad, Fast Ethernet se ha convertido en la opción principal. Fundamentada en la aceptación casi universal de 10BASE-T Ethernet, la tecnología Fast Ethernet provee una evolución flexible y no disruptora hacia desempeño 100 Mbps. Sin embargo, el creciente uso de conexiones Fast Ethernet hacia servidores y equipos de escritorio ha creado una clara necesidad para migrar hacia una tecnología de red de más alta velocidad a nivel del backbone y servidores. Idealmente, esta tecnología debería proveer un camino flexible de actualización, con un costo razonable y sin la necesidad de reentrenamiento.

La solución más apropiada es Gigabit Ethernet. Gigabit Ethernet provee 1 Gbps de ancho de banda para redes de campus con la simplicidad de Ethernet a más bajo costo que otras tecnologías de velocidad comparables. Esto ofrece un camino natural de actualización para las instalaciones Ethernet actuales, inversión de herramientas existentes y entrenamiento.

Las principales ventajas de Gigabit Ethernet es que emplea el mismo protocolo CSMA/CD, el mismo formato de trama y el mismo tamaño de trama de sus

predecesoras. Para la gran mayoría de los usuarios de red, esto significa que sus inversiones en redes existentes pueden ser extendidas a velocidades Gigabit a un costo inicial razonable sin la necesidad de volver a capacitar a sus usuarios y personal de soporte, y sin la necesidad de invertir en stack de protocolos adicionales o software intermedio. El resultado es el bajo costo de apropiamiento para los usuarios.

Por estos atributos, así como también el soporte para operación full-duplex, Gigabit Ethernet es una tecnología ideal para el backbone, para conexiones a servidores de alto desempeño y sirve como un camino de actualización para equipos de alta capacidad que requieren más ancho de banda que el que Fast ethernet puede ofrecer.

5.1.1 ETHERNET: LA TECNOLOGIA DE RED DOMINANTE

Más del 85% de todas las conexiones de red instaladas en la actualidad son Ethernet de acuerdo a IDC¹. Esto representado en 118 millones de PCs, servidores y estaciones de trabajos interconectados. Todos los sistemas operativos y aplicaciones son compatibles con Ethernet, como también los stacks de protocolos de nivel superior tales como Transmission Control Protocol/Internet Protocol (TCP/IP), IPv6, IPX, NetBEUI y DECnet.

1998 fue un año memorable para equipos de red Ethernet ya que la tecnología capturó el 86% del mercado. IDC proyectó que las ventas de tarjetas de interfaz de red Ethernet (NICs) excedería los 48 millones de unidades, y las ventas de hubs Ethernet excederían los 48 millones de puertos. En contraste, era esperado que las ventas de tarjetas de interfaz de red ATM, FDDI y Token Ring alcanzaran los 5 millones en 1998, o sea el 10% del total. Se estimaba que las ventas de los puertos de Hubs ATM, FDDI y Token Ring fueran de 4 millones, o sea el 7% del total. IDC proyectó que el dominio de Ethernet continuaría y efectivamente esto ha venido ocurriendo hasta la actualidad. Muchos factores han contribuido a hacer de Ethernet la tecnología de red más popular usada hoy en día.

- **Confiabilidad de la red:** Redes altamente confiables son críticas para el éxito de una empresa, de esta manera la facilidad de instalación y el soporte son consideraciones primarias en la escogencia de la tecnología de red. Desde la introducción en 1986 de Hubs 10BaseT, los sistemas de cableado estructurado han continuado su evolución y los hubs y switches han incrementado la confiabilidad. Hoy, las redes Ethernet están acercándose a los niveles de confiabilidad adecuados y son relativamente simples para entender y administrar.

¹ International Data Corporation

- **Disponibilidad de herramientas de gestión y localización de fallas:** Las herramientas de gestión para Ethernet, son posibles gracias a la adopción extendida de estándares de gestión incluyendo SNMP y sus sucesores, y permiten a un administrador observar el estado de todos los equipos y elementos de red, incluyendo elementos redundantes, desde una estación central. Las herramientas para localización de fallas abarcan un rango de capacidades, desde simples luces indicadores de estado del enlace hasta analizadores sofisticados de red. Como un resultado de la popularidad de Ethernet, un gran numero de personas han sido entrenadas en su instalación, mantenimiento y localización de fallas.
- **Escalabilidad:** El estándar Fast Ethernet, aprobado en 1995, estableció a Ethernet como una tecnología escalable. Ahora, con el desarrollo de Gigabit Ethernet y 10 Gigabit Ethernet se extiende la escalabilidad de Ethernet aún más. Ahora Ethernet escala desde 10 hasta 100, 1000 y 10000 Mbps.

5.1.2 RAZONES QUE IMPULSAN EL CRECIMIENTO DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA.

A medida que las aplicaciones de red existentes y nuevas evolucionan para incluir gráficos de alta resolución, video, sistemas de información y otros tipos de datos exigentes, la presión esta creciendo hacia los equipos de escritorio, los servidores, y los equipos de Internetworking para un incremento en el ancho de banda y mejoramiento de la seguridad. Muchas de estas aplicaciones requieren la transmisión de grandes archivos sobre la red.

A continuación se presentan los motivos más importantes que impulsan el crecimiento de la Red de Datos de la Universidad del Cauca:

- Los Sistemas de Información existentes en la Universidad del Cauca tales como Recursos Humanos, Físicos y Financieros requieren que se garantice la integridad de los datos y disponibilidad de la información, de tal manera que se pueda cumplir con las exigencias necesarias para brindar un servicio óptimo y confiable.
- Actualmente se encuentra en proceso de implementación el Sistema de Información Académico el cual por el momento solo maneja los procesos de admisión de los nuevos estudiantes. Se espera que un futuro cercano soporte en su totalidad los servicios de Registro y Control Académico de todos los estudiantes de la Universidad del Cauca. Cuando el Sistema de Información Académico este implementado completamente deberá estar en la capacidad de atender a 15.000 usuarios potenciales (estudiantes, profesores, funcionarios,

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

etc), los cuales pueden acceder a través de la Intranet o el servicio de acceso remoto. El número de usuarios que acceden simultáneamente a través de la Intranet podrán ser como máximo el total de equipos existentes en la Universidad (actualmente asciende a 1630 hosts aproximadamente). En este servicio también es indispensable garantizar la integridad y confiabilidad en el transporte y almacenamiento de la información.

- La Universidad del Cauca está empleando tecnologías de Internet para permitir a los usuarios de la red ir más allá del correo electrónico y acceso a datos críticos a través de la Web, abriendo la puerta a la nueva generación de aplicaciones multimedia cliente/servidor. Mientras que el tráfico de Internet esta actualmente compuesto primordialmente de texto, gráficos e imágenes, es esperado el crecimiento de aplicaciones de audio, video y voz en un futuro cercano por lo que sería necesario incluir más ancho de banda.
- Los servidores, sistemas de almacenamiento y sistemas de información de la Universidad del Cauca requieren realizar backup de datos. Tales backups necesitan una gran cantidad de ancho de banda durante una cantidad fija de tiempo (4 a 8 horas). El backup involucra gigabytes de datos distribuidos sobre varios servidores y sistemas de almacenamiento e información.
- Actualmente se adelantan con apoyo de la Vicerrectoría de Investigaciones un buen número de proyectos de alto impacto socio-económico para la región y el país, que se soportan en la Red de Datos, específicamente en Internet, como medio para su divulgación, trascendencia y crecimiento. Estos proyectos utilizan Sistemas de Información basados en la Web montados en servidores ubicados en el edificio del VRI; servidores que primordialmente deben ser accesible desde Internet con una alta disponibilidad y un tiempo de acceso razonable.
- Las herramientas de TELE-EDUCACION se presentan como una buena alternativa para el mejoramiento de los procesos educativos en la Universidad del Cauca, permitiendo la publicación basada en Web de las clases, material de apoyo y creación de espacios de interactividad con los diferentes docentes para la consulta y solución de inquietudes.
- La Universidad del Cauca tiene programas que pueden optar por participar en la compartición de equipos costosos y servicios médicos especializados por medio de la transmisión de imágenes médicas digitales de alta resolución.
- La Red de Datos de la Universidad del Cauca está en continuo crecimiento debido primordialmente a la construcción y ampliación de nuevas sedes, lo

que supone una extensión en su infraestructura física y un incremento en el tráfico que circula a través de ella.

Como estas aplicaciones proliferan y demandan grandes porciones de ancho de banda, y como el número total de usuarios de la red continúan creciendo, la Universidad del Cauca se ha visto en la necesidad de realizar un proceso de migración de su Red de Datos hacia una tecnología que pueda proporcionar mayores anchos de banda y mejores prestaciones.

5.1.3 GIGABIT ETHERNET: LA ALTERNATIVA PARA LANs E INTRANETS

El crecimiento acelerado de tráfico LAN esta impulsando la migración hacia redes de alta velocidad para resolver los requerimientos de ancho de banda. Aunque existen muchas alternativas en el mercado, Gigabit Ethernet reúne muchos criterios claves para ser escogida como una red de alta velocidad:

- Migración fácil y directa a niveles de desempeño más altos sin interrupción.
- Bajo costo de apropiamiento, incluyendo costo de adquisición y soporte.
- Capacidad para soportar nuevas aplicaciones y tipos de datos.
- Flexibilidad para el diseño de la red.

FÁCIL MIGRACIÓN A ALTO DESEMPEÑO

Una de las más importantes cuestiones que se deben tener en cuenta es como conseguir un ancho de banda más grande sin desestabilizar la red existente. Gigabit Ethernet sigue la misma forma, se adapta y funciona como sus antecesoras a 10 y 100 Mbps, permitiendo una migración directa e incremental a redes de más alta velocidad.

Todas las tecnologías Ethernet usan el mismo formato de trama IEEE 802.3, operación full duplex y métodos de control de flujo. En modo half duplex, Gigabit Ethernet emplea el mismo metodo de acceso CSMA/CD para resolver la disputa por el medio compartido. Además, Gigabit Ethernet usa los mismos objetos de gestión definidos por la IEEE 802.3. Gigabit Ethernet es Ethernet, solamente que más rápido.

BAJO COSTO DE APROPIAMIENTO

El costo de apropiamiento es un importante factor en la evaluación de cualquier tecnología de red. El costo global de apropiamiento incluye no solamente el precio de adquisición del equipo, sino también el costo de entrenamiento, mantenimiento y localización de fallas.

La competencia y las economías de escala han impulsado a que el precio de adquisición de productos Ethernet baje significativamente. Las conexiones Gigabit

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

Ethernet conmutadas son más bajas en costo que las interfaces ATM a 622 Mbps, debido a la relativa simplicidad de Ethernet y volúmenes de ventas más altos.

Debido a que la base instalada de usuarios es ya familiar con la tecnología Ethernet, herramientas de mantenimiento y localización de fallas, el costo de soporte asociado con Gigabit Ethernet será mucho más bajo que otras tecnologías. Gigabit Ethernet requiere solamente de entrenamiento de personal y adquisición de herramientas de mantenimiento y localización de fallas. Adicionalmente, el despliegue de Gigabit Ethernet es más rápido que otras tecnologías. Una vez actualizados con entrenamiento y herramientas necesarias, el personal de soporte de la red esta en capacidad de instalar confiadamente, arreglar fallas y dar soporte a instalaciones Gigabit Ethernet.

SOPORTE PARA NUEVAS APLICACIONES Y TIPOS DE DATOS

El surgimiento de aplicaciones de intranet presagia una migración hacia nuevos tipos de datos, incluyendo voz y video. En el pasado se pensaba que el video podría requerir una tecnología de red diferente diseñada específicamente para multimedia. Pero hoy es posible mezclar datos y video sobre Ethernet a través de una combinación de las siguientes características:

- Ancho de banda incrementado provisto por Fast Ethernet y Gigabit Ethernet, mejorado por LAN switching
- El surgimiento de nuevos protocolos, tal como el Protocolo de reserva de recursos (RSVP), que provee reservación de ancho de banda.
- El surgimiento de nuevos estándares tales como 802.1Q y 802.1p los cuales proveerán LAN virtuales (VLANs) e información de prioridad explícita para paquetes en la red.
- El extendido uso de comprensión de video avanzada tal como MPEG-2.

DISEÑO DE RED E INTERCONECTIVIDAD FLEXIBLE

En la actualidad existen una gran cantidad de opciones de interconectividad y diseños de redes. Ellas son combinación de redes enrutadas y conmutadas. Las redes Ethernet son compartidas (usando repetidores) y conmutadas dependiendo de los requerimientos de costo y ancho de banda. La opción de una red de alta velocidad, sin embargo, no debería restringir la opción de interconectividad o topología de red.

5.2 CONSIDERACIONES PARA LA MIGRACION HACIA 10 GIGABIT ETHERNET

En las redes de hoy, el incremento en el tráfico de las redes en el mundo esta impulsando a los proveedores de servicios y administradores de redes a considerar tecnologías de redes más rápidas para resolver la demanda en el incremento del ancho de banda. 10 Gigabit Ethernet tiene 10 veces mejor desempeño que la Gigabit Ethernet de hoy. Con la adición de 10 Gigabit Ethernet a la familia de la tecnología Ethernet, una LAN puede ahora soportar distancias más grandes y soportar incluso aplicaciones con grandes requerimientos de ancho de banda. 10 Gigabit Ethernet también reúne muchos criterios para ser una tecnología de muy buen rendimiento, eficiente y efectiva, la cual la hacen una opción natural para expandir, extender y actualizar las redes Ethernet existentes:

- Una infraestructura Ethernet existente es fácilmente interoperable con 10 Gigabit Ethernet. La nueva tecnología provee un bajo costo de apropiamiento incluyendo tanto costos de adquisición como de soporte, en contraste con otras tecnologías alternativas actuales.
- Es posible el uso de procesos, protocolos, y herramientas de gestión ya desplegados en la infraestructura de gestión, 10 Gigabit Ethernet maneja un conjunto conocido de herramientas de gestión y una base de experiencia común.
- Flexibilidad en el diseño de la red con conexiones a los servidores, switches y routers.
- Múltiples proveedores de productos basados en los estándares proveen interoperabilidad comprobada.

Como 10 Gigabit Ethernet entra al mercado y los proveedores de equipos entregan dispositivos de red 10 Gigabit Ethernet, el siguiente paso para las redes de empresa y proveedores de servicios es la combinación de ancho de banda multi-gigabit con servicios inteligentes, los cuales inducen a redes multi-gigabit, inteligentes y escalables con conexiones al backbone y los servidores al orden de los 10 Gbps. La convergencia de redes de voz y datos corriendo sobre Ethernet se ha vuelto una opción muy real. Y como TCP/IP incorpora características y servicios mejorados, tales como empaquetado de voz y video, 10 Gigabit Ethernet puede también acarrear estos servicios sin modificación.

El estándar 10 Gigabit Ethernet (IEEE 802.3ae) se diferencia de los estándares ethernet anteriores en que en la actualidad solamente funciona sobre fibra óptica y solamente opera en modo full-duplex (los protocolos para detección de colisiones son innecesarios). Ethernet puede ahora evolucionar a 10 Gigabits por segundo mientras

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

que mantiene las propiedades fundamentales de Ethernet, tales como formato de trama, y las capacidades actuales son fácilmente transferibles al nuevo estándar.

El estándar 10 Gigabit Ethernet no solo incrementa la velocidad de Ethernet a 10 Gbps, sino que también extiende su interconectividad y su distancia de operación hasta los 40 km. Al igual que Gigabit Ethernet, el estándar 10 Gigabit Ethernet (IEEE 802.3ae) soporta ambos tipos de medios de comunicación en fibra: Monomodo y Multimodo. Sin embargo, en 10 Gigabit Ethernet, la distancia para fibra monomodo se ha expandido desde 5 km en Gigabit Ethernet hasta 40 km en 10 Gigabit Ethernet. La ventaja de alcanzar nuevas distancias da a las organizaciones, quienes manejan sus propios ambientes LAN, la opción para extender sus centros de datos a una localización de hasta 40 km lejos de su campus. Esto también les permite soportar múltiples campus localizados dentro de la distancia de 40 km.

Como se ha visto en las versiones anteriores de Ethernet, el costo para las comunicaciones a 10 Gbps tiene la potencialidad para disminuir significativamente con el desarrollo de tecnologías basadas en 10 Gigabit Ethernet.

Con relación a los lasers para comunicaciones a 10 Gbps, la tecnología 10 Gigabit Ethernet, como fue definida en el IEEE 802.3ae, será capaz de usar optica a bajo costo, y lasers emisores de superficie de cavidad vertical (VCSEL), los cuales pueden bajar los costos de los dispositivos PMD.

Como se ha venido diciendo, las redes están sometidas a la presión de un elevado rendimiento. Además, los administradores de las mismas se enfrentan a la tarea de implementar innovaciones de redes con presupuestos restringidos.

La solución inteligente es preparar la red ahora para futuras innovaciones tecnológicas, con adaptadores preparados para Gigabit, conmutadores y enlaces ascendentes, y con la posterior incorporación de infraestructura Gigabit en fases incrementales hasta llegar a 10 Gigabit Ethernet en el backbone y los servidores más importantes. Existe gran variedad de productos de conectividad disponibles actualmente en el mercado que se pueden cambiar fácilmente de 100 Mbps o 1000 Mbps, al mismo tiempo que se despliegan Fast Ethernet y Gigabit Ethernet.

Aunque los mayores obstáculos en la Red de datos de la Universidad del Cauca para hacer llegar la tecnología Gigabit Ethernet hasta los computadores de los usuarios son de tipo económico, puede obtenerse un rendimiento aceptable utilizando esta tecnología en primera instancia en los servidores y el backbone, mientras se realiza un proceso de migración gradual dependiendo de las capacidades económicas de la Universidad del Cauca.

5.3 MODELO DE DISEÑO JERÁRQUICO

Los desarrollos tecnológicos y las siempre cambiantes realidades de las diferentes organizaciones se han convertido en agentes que han obligado a repensar la estructura de la red. El incremento en el número de usuarios y en el número de aplicaciones que utilizan la red ha incrementado el tráfico que circula a través de ella, y se espera que en el futuro alcance niveles mucho más altos, por lo que ha sido necesario concebir su estructura como una estructura jerárquica y modular, con diferentes requerimientos de capacidad y desempeño en cada nivel, entendiendo su diseño como un proceso.

Los modelos jerárquicos para el diseño de redes permiten diseñar redes en niveles. Para entender la importancia de la estratificación, se puede considerar el Modelo de Referencia de Sistemas de Interconexión Abierto (OSI), el cual es un modelo estratificado para el entendimiento e implementación de comunicaciones entre computadores. Por el uso de niveles, el modelo OSI simplifica la tarea requerida por dos computadores para comunicarse.

Los modelos jerárquicos para el diseño de redes también usan niveles para simplificar la tarea requerida por el Internetworking. Cada nivel puede ser enfocado en funciones específicas, permitiendo de esta manera escoger los sistemas y características correctos para el nivel.

Usar un diseño jerárquico puede facilitar cambios. La modularidad en el diseño de redes permite crear elementos de diseño que pueden ser reutilizados a medida que la red crece. Como cada elemento en el diseño de red requiere cambiar, el costo y la complejidad de hacer la actualización se reduce a un subconjunto pequeño de toda la red. En planos grandes, los cambios tienden a impactar un gran número de sistemas. El aislamiento de fallas es también facilitado por la estructura modular dentro de la red pequeña, fácil para entender los elementos. Los administradores de red pueden fácilmente entender los puntos de transición en la red, los cuales ayudan a identificar los puntos que están fallando.

Un diseño de red jerárquico incluye los siguientes tres niveles:

- El nivel del backbone (core) que provee el transporte óptimo entre sitios
- El nivel de Distribución que provee conectividad basado en políticas
- El nivel de Acceso Local que provee acceso a la red a los usuarios o grupos de trabajo

La figura 5.1 muestra una vista de alto nivel de varios aspectos de un diseño de red jerárquico. Un diseño de red jerárquico presenta tres niveles: Core (backbone), Distribución y Acceso. Con cada nivel se provee diferente funcionalidad.



Figura 5. 1. Modelo de Diseño de red jerarquico

5.3.1 FUNCIÓN DEL NIVEL CORE

El nivel Core es un backbone conmutando a alta velocidad y debe ser diseñado para conmutar paquetes tan rápido como sea posible. Este nivel de la red no debe realizar ninguna manipulación del paquete, como listas de acceso y filtros, eso disminuiría la velocidad de conmutación de los paquetes.

5.3.2 FUNCIÓN DEL NIVEL DE DISTRIBUCION

El nivel de distribución de la red es el punto demarcado entre el nivel de acceso y el nivel de core y ayuda a definir y diferenciar el core. El propósito de este nivel es proveer la definición del límite y es el área en el cual la manipulación de los paquetes puede tener lugar. En un ambiente de campus, el nivel de distribución puede incluir varias funciones, como las siguientes:

- Dirección o agregación de área
- Acceso a grupos de trabajo o Departamentales
- Definición de dominios de Broadcast/multicast
- Enrutamiento Virtual LAN (VLAN)
- Cualquier transición de los medios de comunicación que se necesite realizar
- Seguridad

El nivel de distribución puede ser resumido como el nivel que provee conectividad basado en políticas.

5.3.3 FUNCIÓN DEL NIVEL DE ACCESO

El nivel de acceso es el punto en el cual los usuarios finales locales están permitidos dentro de la red. Este nivel puede también usar listas de acceso o filtros para optimizar las necesidades de un grupo particular de usuarios. En un ambiente de Campus, el nivel de acceso puede incluir las siguientes funciones:

- Ancho de banda compartido
- Ancho de banda conmutado
- Filtrado a nivel MAC
- Microsegmentación

A veces se piensa equivocadamente que los tres niveles (core, distribución y acceso) deben existir en entidades físicas de forma clara y distinguible, pero esto no tiene que ser necesariamente así. Los niveles son definidos para ayudar a diseñar la red satisfactoriamente y representar la funcionalidad que debe existir en una red. Las aplicaciones de cada nivel pueden estar en distintos routers o switches, pueden estar representadas por un medio de comunicación físico, pueden estar combinados en un único dispositivo, o pueden ser omitidas del todo. La manera que los niveles son implementados depende de las necesidades de la red diseñada. Sin embargo, para que una red funcione óptimamente la jerarquía debe ser mantenida.

Se tiene entonces que la estructura de la red debe ser jerárquica. Teniendo en cuenta la convergencia (un componente que le agrega complejidad al diseño), las redes de hoy, más que redes de datos, son redes de información: flujos de información de datos, de voz y de video viajan a través de las redes modernas, los dispositivos de Internetworking deben estar en capacidad de reconocerlos y darles un tratamiento diferenciado, aspecto conocido como “calidad de servicio”. La red debe estar en capacidad de comprometerse a ofrecer servicios de diferente tipo, dependiendo de la clase de información que se quiera transferir a través de ella, los requerimientos de retraso en la transferencia, de variación del mismo y de capacidad de transmisión deben ser reconocidos y entendidos por los diferentes dispositivos que conforman la arquitectura de una red.

Todo esto conduce a pensar en la necesidad de contar con una metodología que permita abordar con éxito el proceso de diseño de una red. Existen razones de orden económico y tecnológico que lo justifican; por una parte, la red se ha convertido en un recurso estratégico para la universidad, muchos de sus procesos y aplicaciones corren sobre ella; por lo tanto, se imponen requerimientos de alto desempeño y de alta disponibilidad.

Por otra parte, la estructura de la red debe ser jerárquica, funcionalmente modular, con tecnologías de conmutación (*switching*) de diferente nivel y capacidad de transmisión variable en cada uno de sus niveles. La red debe adquirir el compromiso de ofrecer servicios diferenciados a aplicaciones y usuarios que necesitan transferir información de carácter multimedia a través de ella.

5.4 AGREGACION DE ENLACES

La agregación de enlaces es una técnica que permite utilizar varios enlaces Ethernet Full-dúplex para conectar dos equipos, realizando reparto del tráfico entre ellos. Actualmente esta funcionalidad, también denominada multiplexado inverso o etherchannel (nombre dado por Cisco), es ofrecida por diversos fabricantes.

En principio, según el estándar, si dos switches se unen por dos o más enlaces el protocolo Spanning Tree desactivaría todos menos uno (normalmente el de mayor velocidad), dejándolos preparados para entrar en funcionamiento en caso de fallo del primero por algún motivo. La agregación de enlaces requiere deshabilitar el Spanning Tree entre los enlaces que se agregan, para así poder repartir el tráfico entre ellos aumentando la capacidad.

El grupo de trabajo 802.3ad finalizó su trabajo en marzo del 2000, con un gran apoyo de la industria, interesada en poder utilizar masivamente las grandes capacidades de la fibra ya instalada. Desde hace varios años existen productos comerciales, lo que hace prever un rápido desarrollo e implantación de esta tecnología.

Actualmente existen en el mercado productos que permiten agregar hasta 32 enlaces Full-dúplex. Sin embargo, parece que cuatro es un límite razonable, ya que al aumentar el número de enlaces la eficiencia disminuye, y por otro lado debido al costo de las interfaces es aconsejable pasar a una velocidad superior en vez de agregar enlaces. Los enlaces pueden ser de 10, 100, 1000 o 10000 Mb/s, pero todos deben funcionar a la misma velocidad.

La agregación de enlaces requiere evidentemente el uso de múltiples cables, cosa que no siempre es posible, sobre todo si se trata de enlaces a gran distancia. En el caso de fibra óptica monomodo el problema puede resolverse mediante la técnica WDM (Wavelength Division Multiplexing) que consiste en multiplexar varias señales en una misma fibra utilizando longitudes de onda ligeramente distintas dentro de la misma ventana (equivalente a usar luz de diferentes 'colores'). Existen dispositivos comerciales que pueden utilizarse para multiplexar cuatro señales Gigabit Ethernet en una misma fibra, pudiendo así transmitir 4 Gb/s Full-dúplex por un solo par de fibras.

Con WDM también es posible multiplexar el canal de ida y el de vuelta en una misma fibra, con lo que es posible tener comunicación Full-dúplex por una sola fibra.

5.5 ESPECIFICACIONES DE LOS DISPOSITIVOS DE INTERNETWORKING

De acuerdo a la metodología de diseño tomada como referencia, a continuación se establecen las características técnicas que deben cumplir los dispositivos de Internetworking para cada uno de los niveles del modelo jerárquico.

5.5.1 SWITCHES DE NIVEL DE ACCESO

Estos dispositivos estarán ubicados en los centros de cableado que proveen conexión directa a los usuarios en los diferentes sectores de la Red de Datos de la Universidad del Cauca.

5.5.1.1 CALIDAD DE SERVICIO (QOS):

- Los switches deben soportar clasificación y marcado de flujo de paquetes basado en nivel 2,3 y 4.
 - En nivel 2 lo deben hacer basados en direcciones MAC origen y destino.
 - En nivel 3 lo deben hacer basados en direcciones IP origen y destino.
 - En nivel 4 lo deben hacer basados en puertos TCP origen y destino, puertos UDP origen y destino.
- Los switches deben hacer mapeo de niveles de QoS 802.1p a DSCP² y viceversa.
- A la entrada, los switches deben poder limitar flujos de entrada de datos a velocidades diferentes a 10/100/1000 Mbps.
- Para manejo de QoS a la salida del switch, cada puerto debe tener 4 colas para manejo de las prioridades DSCP y/o IEEE 802.1p.
- Soporte de Link Aggregation Control Protocol (LACP) y Port Aggregation Protocol (PAgP).

5.5.1.2 SEGURIDAD:

- Seguridad a nivel de puerto.
- Filtrado de flujos de tráfico entrantes al switch basado en información de nivel 2 (direcciones MAC origen y/o destino), información de nivel 3 (direcciones IP origen y/o destino) e información de nivel 4 (puertos TCP/UDP origen y/o destino).

² Differentiated service code point

- Los switches deben soportar el protocolo IEEE 802.1x para autenticación de usuarios conectados en la red. Sobre este estándar debe ofrecer ventajas adicionales como asignación dinámica de VLANs y/o asignación dinámica de listas de control de acceso (ACLs) por puerto-usuario.
- Debe permitir VLAN bajo el protocolo 802.1q. Para administración y configuración de VLANs en todo el dominio debe manejar VTP (VLAN Trunking Protocol).
- Debe tener seguridad de usuarios con login y password. Manejo de privilegios por diferentes usuarios. Debe poder autenticar estos usuarios en un servidor a través de protocolos tales como RADIUS (Remote Access Dial-In User Service), KERBEROS, otros.

5.5.1.3 GESTIÓN:

- Debe ser administrable vía web, consola, Telnet, SSH, SNMP v1/v2/v3.
- Para su administración, los switches deben permitir formar clusters administrativos, con la posibilidad de que estos equipos se encuentren geográficamente distribuidos en el mismo campus, no necesariamente todos en el mismo rack del centro de cableado.
- El switch debe soportar grupos RMON I y RMON II. Con esto se garantiza una herramienta de monitoreo en tiempo real e histórico del tipo de tráfico que cruza a través de la red.

5.5.1.4 DESEMPEÑO Y DISPONIBILIDAD:

- El desempeño debe ser mínimo de 6 Gbps y el procesamiento debe ser mínimo de 4 millones de paquetes por segundo (Mpps) para paquetes de 64 bytes.
- Puertos: 24 o 48 con Soporte de auto-negociación (half/full duplex) y auto-detección (10/100/1000 Mbps) en todos sus puertos
- Puertos de Uplink: 2 o 4 puertos Gigabit Ethernet Basados en GBIC o SFP. Debe soportar 1000 BaseT, 1000 Base SX y 1000 Base LX.
- Debe soportar el protocolo IEEE 802.1d (Spanning Tree Protocol). Debe tener mejoras como Uplinks fast para disminuir el tiempo de convergencia en caso de falla del enlace principal. También, debe soportar protocolos IEEE 802.1s (Multiple Spanning Tree) – IEEE 802.1w (Rapid Reconfiguration of Spanning Tree).
- Debe soportar IGMP v1/v2 e IGMP Snooping para manejo de sesiones multicast.
- Los switches de nivel de acceso deben permitir tener soluciones in-line power para la implementación de Telefonía IP. Se entiende por in-line power la capacidad de alimentar teléfonos IP directamente a través del cable de conexión UTP.

- Los switches de acceso deben permitir el balanceo de carga mediante el soporte de protocolos de capa 3 que ofrezcan redundancia, y garantizar de esta forma que en caso de ocurrir alguna falla en los enlaces de Uplink de un switch de capa 3, otro switch de capa 3 de la red pueda tomar el control del envío de tráfico, garantizando transparencia y alta disponibilidad para los usuarios/servicios conectados en cada VLAN y cada sub-red.
- Supresión y control de tormentas de broadcast y multicast por puerto
- Soporte IPv6

5.5.2 SWITCHES DE DISTRIBUCION

Estos dispositivos estarán ubicados en los nodos principales de cada sector de la red y proveen una conexión directa al backbone.

5.5.2.1 CALIDAD DE SERVICIO (QOS):

- EL switch debe soportar clasificación de tráfico IP, marcado de prioridad de paquetes tanto a nivel 2, 3 y 4; y su arquitectura interna debe garantizar prioridad a los paquetes marcados con prioridad alta.
- Para la clasificación de paquetes el switch debe soportar clasificación a nivel de puerto de entrada, según información de nivel 2, nivel 3 y/o nivel 4.
- Mapeo de información de QoS de nivel 2 a nivel 3 y viceversa, para garantizar el manejo de QoS extremo a extremo aún en ambientes donde los usuarios finales están conectados a switches de nivel 2.
- Para garantizar la entrega con prioridad de los paquetes marcados con prioridades altas, los puertos de salida deben soportar varias colas de salida, cada una soportando mecanismos para evitar congestión.
- Cada puerto del switch debe tener al menos 4 colas para manejo de las prioridades DSCP y/o IEEE 802.1p.
- Debe soportar algoritmos para dar prioridad en las colas de los puertos al tráfico sensible a la latencia.

5.5.2.2 SEGURIDAD:

- Seguridad a nivel de puerto.
- Filtrado de flujos de tráfico entrantes al switch basado en información de nivel 2 (direcciones MAC origen y/o destino), información de nivel 3 (direcciones IP origen y/o destino) e información de nivel 4 (puertos TCP/UDP origen y/o destino).
- Los switches deben soportar el protocolo IEEE 802.1x para autenticación de usuarios conectados en la red. Sobre este estándar debe ofrecer ventajas adicionales como asignación dinámica de VLANs y/o asignación dinámica de listas de control de acceso (ACLs) por puerto-usuario.

- Para el control de los usuarios que entran a configurar el switch, el equipo deberá soportar autenticación, autorización y contabilización en algún servidor basado en protocolos tales como RADIUS, KERBEROS, etc.
- Para manejo de seguridad, el equipo debe tener herramientas de seguridad para prevenir ataques de ARP Spoofing, ataques contra DHCP y otros.

5.5.2.3 GESTIÓN:

- Debe ser administrable vía web, consola, Telnet, SSH, SNMP v1/v2/v3.
- Para su administración, los switches deben permitir formar clusters administrativos, con la posibilidad de que estos equipos se encuentren geográficamente distribuidos en el mismo campus, no necesariamente todos en el mismo rack del centro de cableado.
- El switch debe soportar grupos RMON I y RMON II.
- Debe estar en capacidad de soportar mediante una herramienta HARDWARE o SOFTWARE la contabilidad de los flujos que pasan a través del equipo, y mediante esta herramienta poder conocer direcciones IP, puertos TCP-UDP, cantidad de bytes, interfaces usadas, etc.

5.5.2.4 DESEMPEÑO Y DISPONIBILIDAD:

- El desempeño debe ser mínimo de 24 Gbps y tener un Throughput Forwarding en capas 2, 3 y 4 mínimo de 17 millones de paquetes por segundo (Mpps) para paquetes de 64 bytes.
- Puertos: 24 o 48 con Soporte de auto-negociación (half/full duplex) y auto-detección (10/100/1000 Mbps) en todos sus puertos
- Soporte del estándar IEEE VLAN Trunking 802.1Q y del algoritmo Spanning Tree, por VLAN, para conectividad tolerante a fallos.
- Debe soportar IGMP v1/v2 e IGMP Snooping para manejo de sesiones multicast.
- Los equipos propuestos deben permitir redundancia a nivel 3 (definir una gateway virtual por defecto), para crear enlaces redundantes en la capa 3 y garantizar la confiabilidad de la solución
- Supresión y control de tormentas de broadcast y multicast por puerto
- El equipo debe soportar redundancia de fuente de poder.
- Soporte de Agregación de Ancho de Banda para las tecnologías Fast Ethernet y Gigabit Ethernet.
- Soporte IPv6
- El equipo debe estar en capacidad de soportar módulos 10 Gb Ethernet para aplicaciones futuras.

5.5.2.5 DESEMPEÑO DE ROUTING:

- El switch debe soportar Protocolos de enrutamiento avanzados para IPv4 e IPv6 tales como: Open Shortest Path First [OSPF], Border Gateway Protocol [BGP], Routing Information Protocol [RIP], protocolos y algoritmos necesarios para el diseño e implementación de redes LAN's altamente escalables y de óptimo desempeño.
- El switch debe tener funciones de Distance Vector Multicast Routing Protocol (DVMRP) tunneling, para IPv4 e IPv6.

5.5.3 SWITCHES DE CORE

Estos dispositivos estarán ubicados en el nodo principal de la Red de Datos de la Universidad del Cauca y proveerán la conexión hacia los proveedores de servicios de Internet (ISP's).

5.5.3.1 CALIDAD DE SERVICIO (QOS):

- EL switch debe soportar clasificación de tráfico IP, marcado de prioridad de paquetes tanto a nivel 2, 3 y 4; y su arquitectura interna debe garantizar prioridad a los paquetes marcados con prioridad alta.
- Para la clasificación de paquetes el switch debe soportar clasificación a nivel de puerto de entrada, según información de nivel 2, nivel 3 y/o nivel 4.
- Mapeo de información de QoS de nivel 2 a nivel 3 y viceversa, para garantizar el manejo de QoS extremo a extremo aún en ambientes donde los usuarios finales están conectados a switches de nivel 2.
- Para garantizar la entrega con prioridad de los paquetes marcados con prioridades altas, los puertos de salida deben soportar varias colas de salida, cada una soportando mecanismos para evitar congestión.
- Cada puerto del switch debe tener al menos 4 colas para manejo de las prioridades DSCP y/o IEEE 802.1p.
- Debe soportar algoritmos para dar prioridad en las colas de los puertos al tráfico sensible a la latencia.

5.5.3.2 SEGURIDAD:

- Seguridad a nivel de puerto.
- Filtrado de flujos de tráfico entrantes al switch basado en información de nivel 2 (direcciones MAC origen y/o destino), información de nivel 3 (direcciones IP origen y/o destino) e información de nivel 4 (puertos TCP/UDP origen y/o destino).
- Los switches deben soportar el protocolo IEEE 802.1x para autenticación de usuarios conectados en la red. Sobre este estándar debe ofrecer ventajas

adicionales como asignación dinámica de VLANs y/o asignación dinámica de listas de control de acceso (ACLs) por puerto-usuario.

- Para el control de los usuarios que entran a configurar el switch, el equipo deberá soportar autenticación, autorización y contabilización en algún servidor basado en protocolos tales como RADIUS, KERBEROS, etc.
- Para manejo de seguridad, el equipo debe tener herramientas de seguridad para prevenir ataques de ARP Spoofing, ataques contra DHCP y otros.

5.5.3.3 GESTIÓN:

- Debe ser administrable vía web, consola, Telnet, SSH, SNMP v1/v2/v3.
- Para su administración, los switches deben permitir formar clusters administrativos, con la posibilidad de que estos equipos se encuentren geográficamente distribuidos en el mismo campus, no necesariamente todos en el mismo rack del centro de cableado.
- El switch deberá soportar grupos RMON I y RMON II.
- Debe estar en capacidad de soportar mediante una herramienta HARDWARE o SOFTWARE la contabilidad de los flujos que pasan a través del equipo, y mediante esta herramienta poder conocer direcciones IP, puertos TCP-UDP, cantidad de bytes, interfaces usadas, etc.

5.5.3.4 DESEMPEÑO Y DISPONIBILIDAD:

- El desempeño debe ser mínimo de 64 Gbps y tener un Throughput Forwarding en capas 2, 3 y 4 mínimo de 48 millones de paquetes por segundo (Mpps) para paquetes de 64 bytes.
- Puertos: 24 o 48 con Soporte de auto-negociación (half/full duplex) y auto-detección (10/100/1000 Mbps) en todos sus puertos
- Soporte del estándar IEEE VLAN Trunking 802.1Q y del algoritmo Spanning Tree por VLAN, para conectividad tolerante a fallos.
- Debe soportar IGMP v1/v2 e IGMP Snooping para manejo de sesiones multicast.
- Supresión y control de tormentas de broadcast y multicast por puerto
- El equipo debe soportar redundancia de fuente de poder y de tarjeta supervisora, redundancia en backplane, relojes redundantes, soporte de enlaces redundantes.
- Las tarjetas de puertos, las tarjetas supervisoras, Switch Fabrics, ventiladores, fuentes de poder, deben ser “Hot Swappable”³.
- Soporte de Agregación de Ancho de Banda para las tecnologías Fast Ethernet y Gigabit Ethernet.

³ La posibilidad de realizar un cambio del equipo en caliente.

- El switch debe estar en la capacidad de soportar, mediante adición de módulos de software y/o hardware, sistemas de seguridad VPN IPSEC, IDS (Intrusión Detection Systems), Firewall de alta velocidad dedicado, soporte de características para manejo de aplicaciones emergentes como Telefonía IP e incluso conexión a redes WAN y MAN mediante protocolos como ATM, PPP, X.25 y Frame Relay.
- Soporte IPv6
- El equipo debe estar en capacidad de soportar módulos 10 Gb Ethernet.

5.5.3.5 DESEMPEÑO DE ROUTING:

- El switch debe soportar Protocolos de enrutamiento avanzados para IPv4 e IPv6 tales como: Open Shortest Path First [OSPF], Border Gateway Protocol [BGP], Routing Information Protocol [RIP], protocolos y algoritmos necesarios para el diseño e implementación de redes LAN's altamente escalables y de óptimo desempeño.
- El switch debe tener funciones de Distance Vector Multicast Routing Protocol (DVMRP) tunneling, para IPv4 e IPv6.

5.6 PROPUESTAS DE DISEÑO PARA LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA

De acuerdo al modelo de diseño jerárquico y a los requisitos mínimos que deben cumplir los dispositivos de Internetworking, se estudiaron diferentes productos existentes en el mercado de las empresas más reconocidas a nivel mundial. Los productos que cumplen con la totalidad de los requisitos y ofrecen ventajas adicionales son los de los fabricantes Cisco y Alcatel. Debido a esto las propuestas de diseño se realizan con las familias de equipos de estas organizaciones.

A continuación se presentan las propuestas de diseño para la Red de Datos de la Universidad del Cauca, describiendo la nueva topología de red. En primera instancia se realizará el diagrama de la infraestructura de red tomando como referencia los productos Cisco, posteriormente se realizará el diseño con los productos Alcatel para los cuales se mantendrá la misma topología de red y solo será necesario establecer la equivalencia de los equipos entre las dos organizaciones, teniendo en cuenta que los productos seleccionados cumplan con los requisitos establecidos anteriormente.

5.6.1 PROPUESTA DE DISEÑO CON LOS PRODUCTOS CISCO

5.6.1.1 DESCRIPCION GENERAL DE LOS PRODUCTOS CISCO

A continuación se describe de manera general los switches utilizados en el diseño⁴:

- **SWITCHES DE LA SERIE CISCO CATALYST 3750**

El switch Cisco Catalyst 3750 pertenece a una línea de switches de clase empresarial con soporte para configuraciones Gigabit Ethernet y Fast Ethernet y los estándares IEEE 802.3af y Cisco pre-estándar Power over Ethernet (PoE), los cuales ofrecen una alta disponibilidad, seguridad y calidad de servicio (QoS) para mejorar el funcionamiento de la red. El 3750 es un switch ideal para el nivel de acceso para pequeños centros de cableado o sucursales en los cuales se deseen prestar nuevos servicios de red tales como avanzada QoS, limitación de flujo, listas de control de acceso (ACLs), gestión de multicast, y alto desempeño de routing IP o desplegar nuevos productos y aplicaciones como teléfonos IP, puntos de acceso inalámbricos o video-vigilancia, todo esto manteniendo la simplicidad tradicional de las LANs conmutadas. Este switch trae incluido el software de gestión Cisco Cluster Management Suite (CMS) el cual permite realizar una gestión simple del switch y los servicios inteligentes de red.

CONFIGURACIONES

- ✓ **Cisco Catalyst 3750G-24TS:** 24 puertos Ethernet 10/100/1000 y 4 uplinks SFP
- ✓ **Cisco Catalyst 3750G-24T:** 24 puertos Ethernet 10/100/1000
- ✓ **Cisco Catalyst 3750G-12S:** 12 puertos Gigabit Ethernet SFP
- ✓ **Cisco Catalyst 3750-48TS:** 48 puertos Ethernet 10/100 y 4 uplinks SFP
- ✓ **Cisco Catalyst 3750-24TS:** 24 puertos Ethernet 10/100 y 2 uplinks Small Form-factor Pluggable (SFP)
- ✓ **Cisco Catalyst 3750-48PS:** 48 puertos Ethernet 10/100 y 4 uplinks SFP con soporte para IEEE 802.3af y Cisco pre-standard Power over Ethernet (PoE)
- ✓ **Cisco Catalyst 3750-24PS:** 24 puertos Ethernet 10/100 y 2 uplinks SFP con soporte para IEEE 802.3af and Cisco pre-standard Power over Ethernet (PoE)
- ✓ **Cisco Catalyst 3750G-16TD:** 16 puertos Ethernet Gigabit 10/100/1000 y 1 uplink 10Gigabit Ethernet XENPAK

⁴ Para mayor información sobre este tipo de switches referase al Anexo D.

La serie Cisco Catalyst 3750 esta disponible con la imagen Standard Multilayer Software Image (SMI) o Enhanced Multilayer Software Image (EMI). La SMI incluye las siguientes características: calidad de servicio (QoS) avanzada, listas de control de acceso (ACLs), y funcionalidades básicas de routing con soporte de routing estático y RIP. La EMI provee un rico conjunto de características de tipo empresarial que incluyen routing avanzado basado en unicast y multicast.

- **SWITCHES DE LA SERIE CISCO CATALYST 4500**

La serie Cisco Catalyst 4500 ofrece conmutación non-blocking de niveles 2 al 4 con elasticidad integrada, más allá del control mejorado de redes convergentes. Las redes convergentes de datos, voz y video con alta disponibilidad habilita la elasticidad de los negocios para empresa y usuarios ethernet desplegando aplicaciones de negocios basados en Internet.

La serie Cisco Catalyst 4500 incluye cuatro chasis Cisco Catalyst:

- ✓ **Cisco Catalyst 4510R (10 slots)**
- ✓ **Cisco Catalyst 4507R (7 slots)**
- ✓ **Cisco Catalyst 4506 (6 slots)**
- ✓ **Cisco Catalyst 4503 (3 slots)**

La elasticidad integrada mejorada ofrecida en la serie Cisco Catalyst 4500 incluye redundancia 1+1 del equipo supervisor (Cisco Catalyst 4507R/4510R), estandar IEEE 802.3af (Potencia sobre Ethernet), tolerancia ante fallos basada en software, y redundancia 1+1 de la fuente de poder. La elasticidad integrada tanto en hardware y software minimiza el tiempo de caída de la red, ayudando a asegurar la productividad y la rentabilidad de la empresa.

La serie Cisco Catalyst 4500 extiende el control al borde de la red con servicios de red inteligente, incluyendo calidad de servicio (QoS) sofisticado, rendimiento predecible, seguridad avanzada, gestión integral, y elasticidad integrada. Ofreciendo compatibilidad con todas las tarjetas de línea y equipos supervisores de la serie Cisco Catalyst 4500, se reduce el costo de apropiamiento minimizando gastos operacionales recurrentes, mejorando el retorno de la inversión.

CONFIGURACIONES

Cisco Catalyst 4500 Series Switching Módulos	Número de Interfaces Soportadas por Line Card	Cisco Catalyst 4503(No. Puertos)	Cisco Catalyst 4506(No. Puertos)	Cisco Catalyst 4507R(No. Puertos)	Cisco Catalyst 4510R(No. Puertos)
Switched 10/100 Fast Ethernet (RJ-45)	24, 32 o 48	96	240	240	384
Switched 10/100 Fast Ethernet (RJ-21)	48	96	240	240	384
Switched 100 Fast Ethernet (MT-RJ)	4, 24, o 48	96	240	240	384
Switched 1000 Gigabit Ethernet (fiber)	2, 6, 18, o 48	96	240	240	384
Switched 10/100/1000BASE-T Gigabit Ethernet	24 o 48	96	240	240	384

Tabla 5. 1. Configuraciones de la serie Cisco 4500

- **SWITCHES DE LA SERIE CISCO CATALYST 6500**

La serie Cisco Catalyst 6500 consiste en una serie de switches modulares multinivel que brindan seguridad y convergencia de servicios desde el nivel de acceso hasta el core y desde los centros de datos hasta el borde de la red. Presenta disponibilidad de puertos Ethernet desde 48 hasta 576 10/100/1000 Mbps y hasta 1152 10/100 Mbps, los cuales ofrecen un throughput de cientos de millones de paquetes por segundo (Mpps). Los switches de la serie Cisco Catalyst 6500 soportan múltiples enlaces Gigabit y 10 Gigabit por segundo y proveen un desempeño de conmutación multinivel inteligente y escalable tanto para redes empresariales como para proveedores de servicios.

Disponible en chasis de 3, 6, 9 y 13 slots, la serie Cisco Catalyst 6500 posee un rango incomparable de módulos de servicios integrados, incluyendo seguridad de red Multigigabit, telefonía, y módulos de análisis de red.

La serie Catalyst 6500 optimiza la utilización de la infraestructura de telecomunicaciones y maximiza el rendimiento de las inversiones ya que se adquiere una arquitectura de envío inteligente que soporta un rango inigualable de servicios

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

incluyendo la integración de datos y video, y la convergencia LAN/WAN/MAN con los siguientes beneficios adicionales:

- Máximo tiempo de actividad de la red para usuarios de mas alta productividad.
- Seguridad integral de la red usando tecnología Cisco Multigigabit probada.
- Protección de la inversión y ciclo de vida del producto larga soportando múltiples generaciones de interfaces y equipos para el envío de paquetes.
- Consistencia operacional permitiendo a los clientes estandarizar sobre una única plataforma que dirija todos los requerimientos de la red.
- Excelente integración de servicios soportando la convergencia de voz, video y datos sobre una única plataforma de gestión.

La serie Catalyst 6500 presenta el siguiente portafolio de productos:

- Equipo Supervisor 720
- Módulos de 2 puertos non-blocking y 4 puertos 10 Gigabit Ethernet
- Módulo de 48 puertos Ethernet 10/100/1000
- Módulo de 24 puertos Gigabit Ethernet para despliegue de centros de datos

5.6.1.2 PROPUESTAS DE DISEÑO PARA EL BACKBONE CON TECNOLOGIA GIGABIT ETHERNET

En las siguientes propuestas de diseño se plantea una topología de red con dos estrellas ubicadas en los sectores del IPET y El Carmen y con un backbone funcionando en el nivel 3 bajo la tecnología Gigabit Ethernet, con redes de acceso Ethernet conmutadas a 100 Mbps.

Para desplegar Gigabit Ethernet a través del backbone, es necesario cambiar la fibra multimodo 62.5/125 μm a fibra monomodo 9/125 μm en los enlaces donde la distancia supera los limites establecidos por el estándar para fibra multimodo. Dichos enlaces son los siguientes: IPET – MEDICINA, IPET – EDUCACION, IPET – SANTO DOMINGO, IPET – EL CARMEN, EL CARMEN – VRI.

Debido a que se debe cambiar la fibra multimodo que interconecta los sectores mencionados anteriormente, se propone realizar la adquisición de los pares de fibra monomodo necesarios para hacer una conexión directa entre los sectores de Santo Domingo y Educación, tal como se muestra en las opciones de diseño No. 2. Esto teniendo en cuenta que en el sector de Santo Domingo se encuentran ubicados la mayoría de clientes que hacen uso de los sistemas de información financiero, recursos humanos, recursos físicos y algunos usuarios del sistema de información académico. Todos los servidores de estos sistemas de información se encuentran ubicados en el

sector de Educación, por lo cual se requiere una comunicación eficiente y confiable entre los sectores de Santo Domingo y Educación. El tendido de la fibra entre Santo Domingo, Educación y el IPET se puede realizar utilizando los ductos existentes actualmente. Con el nuevo enlace entre Santo Domingo y Educación, los constantes flujos de tráfico existentes entre estos dos sectores mejorarían sus tiempos de retardo de transmisión, además de garantizar la disponibilidad de la comunicación y ofrecer redundancia.

En los enlaces del backbone se recomienda implementar la tecnología de *Agregación de Enlaces* o *Etherchannel* para incrementar el ancho de banda y obtener un mejor desempeño de la Red. En las opciones de diseño No. 1. se agregan solamente hasta dos enlaces debido a la cantidad limitada de interfaces de fibra disponibles en los equipos de la serie Cisco Catalyst 3750 utilizados en el nivel de distribución, obteniendo así una velocidad de 4 Gbps. En las opciones de diseño No. 2. se agregan hasta cuatro enlaces ya que esta es la cantidad máxima de agregaciones soportadas por los equipos propuestos, y además es un límite razonable para la implementación de esta tecnología. De ésta manera se obtiene así una velocidad de 8 Gbps a nivel de backbone.

Con relación a la infraestructura lógica general se recomienda que la Red funcione a nivel 3, ya que los dispositivos de Internetworking propuestos tienen el soporte necesario para operar como switches multinivel. Actualmente, a pesar de la gran extensión física de la Red y el considerable número de hosts conectados a ella, ésta posee una infraestructura soportada principalmente sólo por switches nivel 2, y con una sola subred lógica IP. Esta configuración no es adecuada ya que los niveles de broadcast son considerables y el aumento normal del tráfico con el tiempo debido a nuevos hosts y usuarios, nuevas aplicaciones y servicios, e incremento del uso de estos, conllevará una elevación de los niveles de broadcast y multicast. Para mantener los niveles de este tipo de tráfico dentro de los valores aceptables existen dos soluciones: la implementación de VLANs o subredes lógicas IP. Estas dos estrategias se encargan de subdividir una red lógicamente de tal manera que el broadcast y multicast no traspasen los límites de la subred o VLAN, impidiendo que éste se propague por toda la red. Es entonces necesario que la infraestructura de la Red implemente cualquiera de las dos estrategias mientras se sigue trabajando con el protocolo IPv4, ya que con IPv6 el tráfico de broadcast no se presenta.

Las VLANs son principalmente utilizadas con el objetivo de permitir la existencia de grupos de trabajo (llamados VLANs por esta tecnología) donde sus miembros puedan estar repartidos por toda la red; es decir si se tienen dos hosts en extremos distintos de una red pero pertenecientes a una misma VLAN, la comunicación se realizará a través de funciones de conmutación y no de enrutamiento como ocurriría en una red normal.

Las subredes lógicas IP, en cambio, se emplean fundamentalmente con el objetivo de reducir los dominios de broadcast y multicast. Esta estrategia ataca directamente el problema planteado por lo que es recomendable que la infraestructura de la Red maneje diferentes subredes lógicas IP.

La implementación de diferentes subredes IP puede ser desarrollada con switches multinivel. La topología de Red de dos estrellas sugiere la necesidad de tener al menos dos switches multinivel con una subred IP diferente para cada uno de los sectores, es decir, el tráfico broadcast y multicast estará confinado al sector donde se originó; un solo switch multinivel ubicado en el IPET implicaría un dominio de broadcast bastante grande formado por todos los hosts de los sectores del Centro, por lo cual no es recomendable. En las propuestas se plantea la posibilidad de tener varios switches multinivel ubicados en el nivel de distribución (centros de cableado CC1) de cada uno de los sectores de la Red con el objetivo de proporcionar un mejor desempeño creando dominios de broadcast aún más pequeños, habilitando las funcionalidades de nivel 3 que poseen los switches multinivel.

En el nivel de acceso a pesar de que los switches son multinivel, se recomienda que sean configurados para soportar solo conmutación de nivel 2, ya que si se quiere un funcionamiento a nivel 3 se deben adquirir nuevas licencias para soportar protocolos de enrutamiento avanzados lo cual implica unos costos muy altos y además es una capacidad que sobrepasa las necesidades actuales de la Red. Por lo tanto la infraestructura de red deberá tener switches multinivel que realicen conmutación a nivel 3 en los niveles de core y distribución, y el resto de la Red deberá seguir soportada por conmutación nivel 2, es decir en el nivel de acceso.

PROPUESTA No. 1: Nodo de Acceso WAN ubicado en el IPET

El acceso WAN o acceso a Internet se realiza a través del switch principal ubicado en el sector del IPET, tal como se hace actualmente.

Las razones para mantener esta configuración son las siguientes:

- Existe actualmente en el IPET un nodo de acceso a la Red Metropolitana Multiservicios de Emtel. La conexión se realiza por medio de 16 pares de Fibra Óptica Monomodo tendidos desde el Switch Central ATM ubicado en las instalaciones de Emtel-Centro hasta el IPET. Esta fibra es propiedad de Emtel.
- En el IPET se encuentran ubicados los principales servidores de la Red TCP/IP y ya se tiene instalada la infraestructura necesaria por lo que existe un entorno adecuado para el funcionamiento de los servidores.

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

- Como se analizó en el Capítulo 3, los sectores que generan el mayor tráfico debido a la alta utilización de Internet son Ingenierías y Educación. Por lo tanto, el mantener el nodo de acceso a Internet en el IPET disminuye los tiempos de retardo de transmisión hacia los clientes de dichos sectores.

Adicionalmente, se propone realizar una conexión directa entre los sectores del IPET y VRI, ya que en este último se llevan a cabo procesos de investigación y desarrollo que en un momento determinado pueden llegar a demandar recursos mayores de la Red. Esto aprovechando el hecho de que la fibra que comunica el sector del VRI con el sector de El Carmen debe ser cambiada, ya que no cumple con los requerimientos del estándar.

A continuación se presentan las opciones de diseño para el backbone, especificando los equipos seleccionados.

OPCION 1 (Figura 5.2):

NIVEL DE CORE:

- **Cisco Catalyst 4510R :**
 - ✓ 4 módulos Catalyst 4500 de 48 Puertos 10/100/1000 (RJ45)
 - ✓ Equipo supervisor V, Consola (RJ45)
 - ✓ 1 módulo de 6 puertos 1000BASE-LX (Fibra Monomodo)
 - ✓ 1 módulo de 6 puertos 1000BASE-SX (Fibra Multimodo)

NIVEL DE DISTRIBUCION:

- **Cisco Catalyst 3750G-24TS:** 24 puertos Ethernet 10/100/1000 y 4 uplinks SFP⁵ con Imagen mejorada.

OPCION 2 (Figura 5.3):

NIVEL DE CORE:

- **Cisco Catalyst 4510R :**
 - ✓ 4 módulos Catalyst 4500 de 48 Puertos 10/100/1000 (RJ45)
 - ✓ Equipo supervisor V, Consola (RJ45)
 - ✓ 1 módulo de 6 puertos 1000BASE-LX (Fibra Monomodo)
 - ✓ 1 módulo de 6 puertos 1000BASE-SX (Fibra Multimodo)

⁵ SFP - Small Form-Factor Pluggable: Es un dispositivo de entrada/salida que se conecta a slots o puertos Gigabit Ethernet. Está disponible para fibra óptica y cable UTP.

NIVEL DE DISTRIBUCION:

- **Cisco Catalyst 4510R**
- **Cisco Catalyst 4507R⁶**

⁶ Los módulos RJ45 y Fibra están especificados en las propuestas de diseño presentadas para cada sector.

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

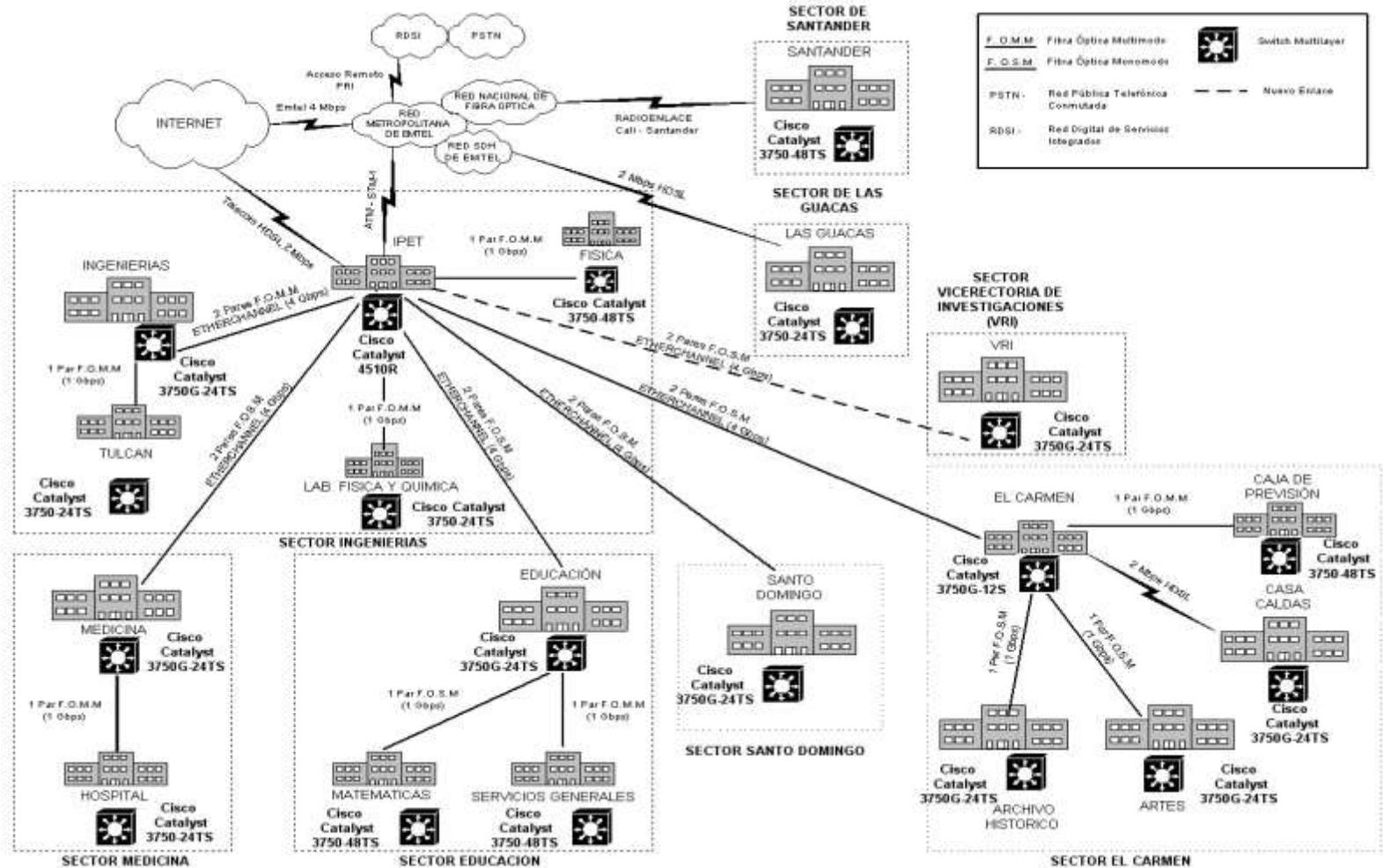


Figura 5. 2. Opción de diseño No. 1 para el backbone con tecnología Gigabit Ethernet y nodo de acceso WAN en el IPET

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

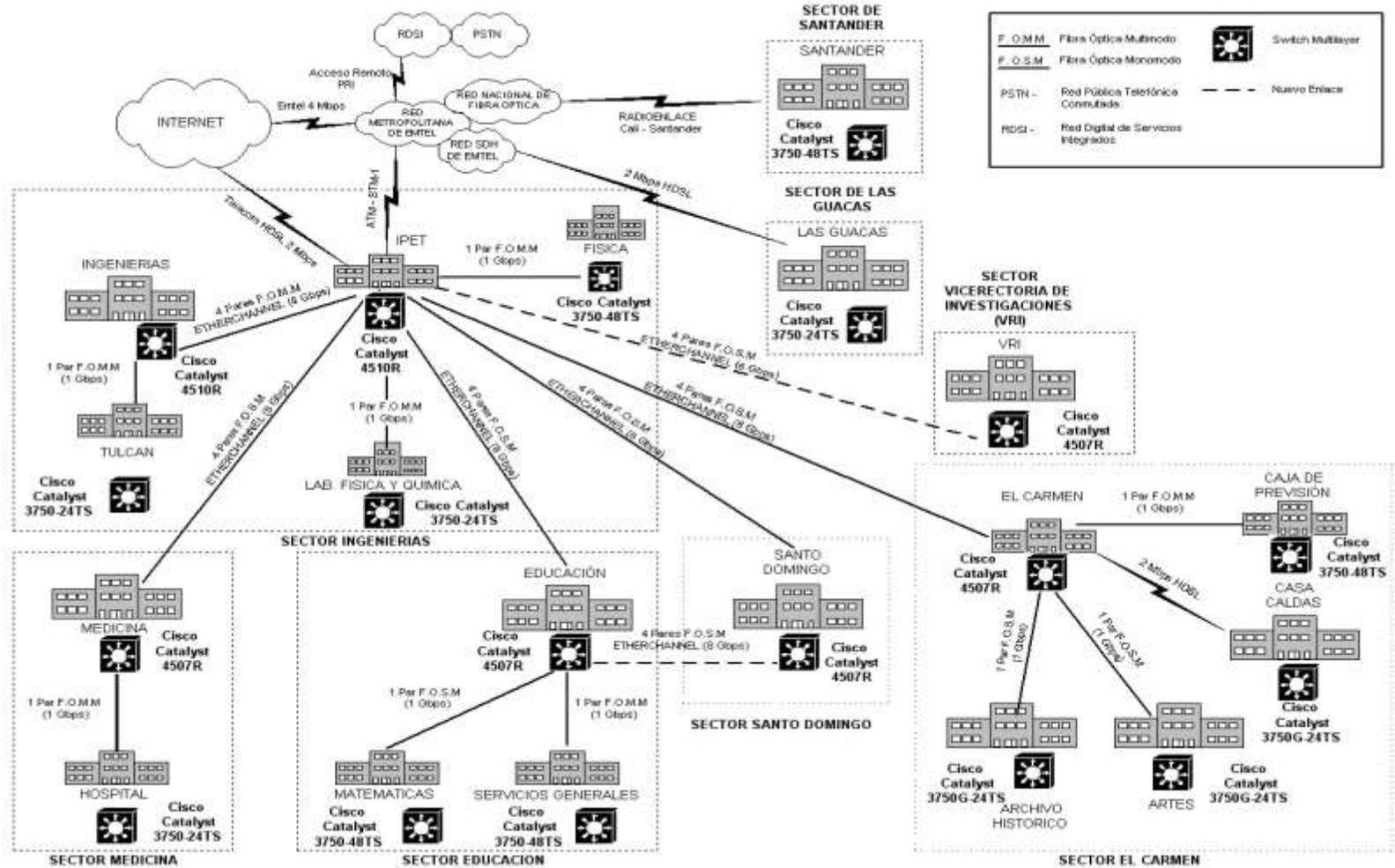


Figura 5. 3. Opción de diseño No. 2 para el backbone con tecnología Gigabit Ethernet y nodo de acceso WAN en el IPET

PROPUESTA No. 2: Nodo de Acceso WAN ubicado en El Carmen

El acceso WAN o acceso a Internet se realiza a través del switch principal ubicado en el sector de El Carmen.

Esta propuesta es justificable por las siguientes razones:

- La ubicación de El Carmen en el centro de la ciudad facilita la conexión con los nodos principales de los proveedores de servicios de Internet Emtel y Telecom. Esto teniendo en cuenta que las distancias son menores en comparación con las existentes entre el IPET y dichos proveedores.
- La comunicación con el ISP Telecom mejora ya que el trayecto de conexión mediante pares de cobre se reduce considerablemente. Actualmente, ésta conexión se realiza por dos pares de cobre dedicados propiedad de la Universidad del Cauca que se extienden desde el IPET hasta El Carmen, y dos pares de cobre dedicados propiedad de Telecom utilizados en el trayecto desde El Carmen hasta Telecom. Por consiguiente, al ubicar el nodo de acceso en El Carmen es innecesario el uso de los pares de cobre que interconectan el IPET con El Carmen.
- Gracias a la ubicación del nodo de acceso WAN en el Carmen, se facilita un posible proceso de actualización del medio físico para interconectarse con el ISP Telecom. Esta actualización comprende el cambio de cobre a fibra para realizar la interconexión entre la Universidad del Cauca y Telecom.

Algunas desventajas que se deben tener en cuenta son:

- Para la conexión con el ISP Emtel se debe realizar un nuevo tendido de fibra lo cual implica costos adicionales. Este hecho puede ser no considerado como una desventaja si el costo de instalación es asumido por Emtel.
- Es necesario la adecuación de nuevas instalaciones para adaptar un entorno de funcionamiento óptimo para los diferentes servidores y equipos principales de la Red (p.ej. switch de core).
- Los niveles de congestión en el enlace entre el IPET y El Carmen aumentan, ya que la cantidad de tráfico hacia Internet de los sectores de Ingenierías, Educación y Medicina es superior al tráfico generado en los sectores del Centro, lo cual implica que se incrementen los tiempos de retardo de transmisión del tráfico de Internet que circula por dicho enlace.

A continuación se presentan las opciones de diseño para el backbone especificando los equipos seleccionados.

OPCION 1 (Figura 5.4):

NIVEL DE CORE:

- **Cisco Catalyst 4510R :**
 - ✓ 1 módulo Catalyst 4500 de 48 Puertos 10/100/1000 (RJ45)
 - ✓ Equipo supervisor V, Consola (RJ45)
 - ✓ 1 módulo de 6 puertos 1000BASE-LX (Fibra Monomodo)
 - ✓ 1 módulo de 2 puertos 1000BASE-SX (Fibra Multimodo)

NIVEL DE DISTRIBUCION:

- **Cisco Catalyst 3750G-24TS:** 24 puertos Ethernet 10/100/1000 y 4 uplinks SFP con Imagen mejorada.
- **Cisco Catalyst 4510R**

OPCION 2 (Figura 5.5):

NIVEL DE CORE:

- **Cisco Catalyst 4510R :**
 - ✓ 1 módulo Catalyst 4500 de 48 Puertos 10/100/1000 (RJ45)
 - ✓ Equipo supervisor V, Consola (RJ45)
 - ✓ 1 módulo de 6 puertos 1000BASE-LX (Fibra Monomodo)
 - ✓ 1 módulo de 2 puertos 1000BASE-SX (Fibra Multimodo)

NIVEL DE DISTRIBUCION:

- **Cisco Catalyst 4510R**
- **Cisco Catalyst 4507R⁷**

⁷ Los módulos RJ45 y Fibra están especificados en las propuestas de diseño presentadas para cada sector.

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

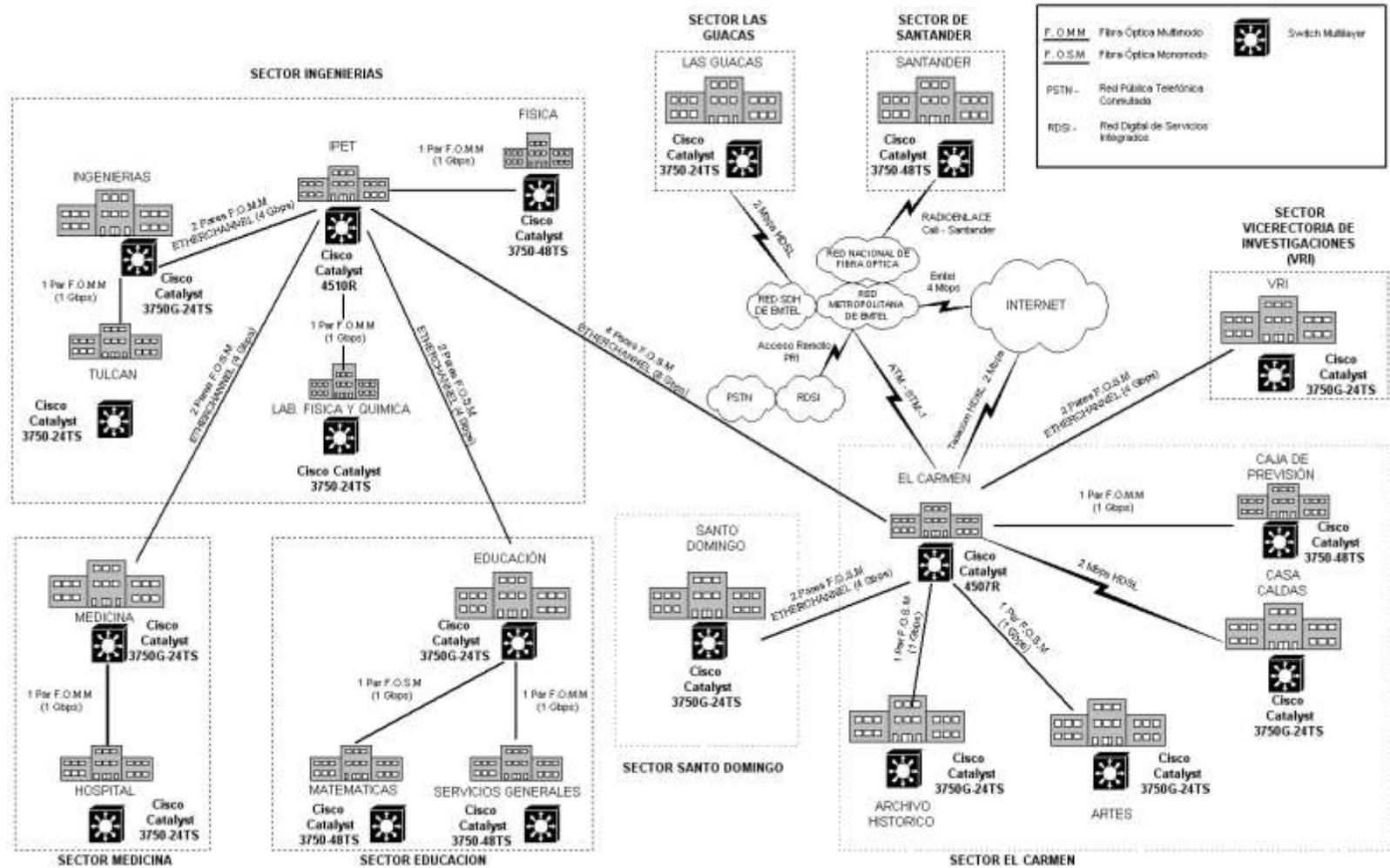


Figura 5. 4. Opción de diseño No. 1 para el backbone con tecnología Gigabit Ethernet y nodo de acceso WAN en El Carmen

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

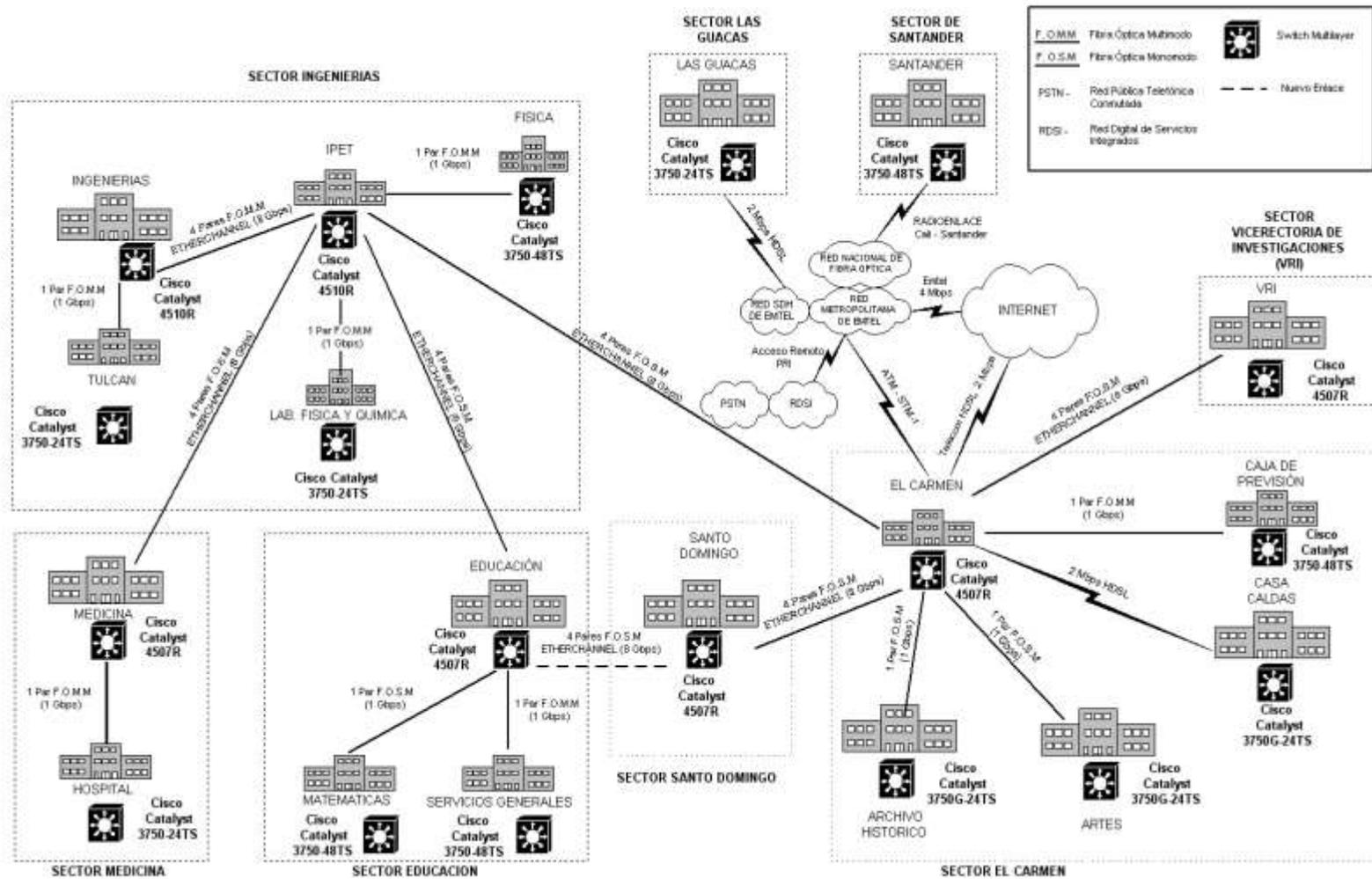


Figura 5. Opción de diseño No. 2 para el backbone con tecnología Gigabit Ethernet y nodo de acceso WAN en El Carmen

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

En las anteriores propuestas, se presentan dos opciones de diseño para cada una de ellas. En las opciones de diseño No. 1 se propone la utilización de switches de la serie Cisco Catalyst 4500 en el nivel de core y switches de la serie Cisco Catalyst 3750 en el nivel de distribución. En las opciones de diseño No. 2 se propone la utilización de switches de la serie Cisco Catalyst 4500 en el nivel de core y distribución.

Al implementar el nivel de distribución con equipos de la serie Cisco Catalyst 4500 se obtienen ventajas adicionales tales como:

- Mejor desempeño, mayores tasas de conmutación y enrutamiento.
- Funcionalidades de niveles 2, 3 y 4, características avanzadas de seguridad, calidad de servicio y gestión integral de la Red, entre otras.
- Estos switches permiten configurar mayores velocidades en el backbone mediante la agregación de un número mayor de enlaces, gracias a la disponibilidad de interfaces de fibra.
- Se puede implementar una conexión directa con fibra óptica entre los sectores de Santo Domingo y Educación ya que se puede disponer de un mayor conjunto de interfaces de fibra.
- Escalabilidad flexible hacia el despliegue de la tecnología 10 Gigabit Ethernet.

Teniendo en cuenta lo anterior, se puede afirmar que las opciones de diseño con switches de la serie Cisco Catalyst 4500 desde el punto de vista técnico es la mejor. Sin embargo, su implementación puede representar unos costos muy elevados para la Universidad del Cauca, por lo cual las opciones de diseño con switches de la serie Cisco Catalyst 3750 son una muy buena alternativa ya que estos equipos ofrecen las funcionalidades necesarias para dar respuesta a los requerimientos de la Red a un costo razonable y dentro de las capacidades económicas de la Universidad. Como factor en contra, la implementación con los switches de la serie Cisco Catalyst 3750 no ofrece un camino flexible para la futura migración hacia la tecnología 10 Gigabit Ethernet, por lo cual esta alternativa puede ser vista como un paso intermedio de la migración.

A continuación se presentan las propuestas de diseño para los diferentes sectores de la Red. En cada propuesta se plantean dos opciones de diseño, especificando los dispositivos de Internetworking que se utilizan tanto en el nivel de acceso como el nivel de distribución.

En general, para las diferentes opciones de diseño de cada uno de los sectores se mantiene la misma topología interna, salvo en el caso donde se indique lo contrario, con el objetivo de aprovechar la infraestructura física existente tanto de cableado

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

UTP como de fibra, teniendo en cuenta que la Red actual fue implementada bajo las normas del estándar IEEE 802.3.

En las diferentes opciones de diseño se plantea la posibilidad de utilizar switches multinivel en todos los centros de cableado del nivel de acceso, descartando el uso de hubs dentro de la Red. Esto justificado principalmente en que la diferencia del costo por puerto de los hubs frente a los switches ha disminuido notablemente en los últimos años. Además se puede obtener un mejor desempeño ya que el uso de switches permite suprimir totalmente el protocolo CSMA/CD y extender el funcionamiento en modod Full-duplex a toda la Red. Por estos motivos, hoy en día se considera que el diseño de una red Ethernet debe basarse normalmente en el uso de conmutación a nivel del usuario final, es decir, se recomienda la completa supresión de los hubs.

Las propuestas de diseño de los diferentes sectores de la Red se realizan tomando como referencia el nodo de acceso a internet ubicado en el IPET. Las propuestas también son validas en el caso de que el nodo de acceso a internet sea ubicado en El Carmen, ya que este cambio no afecta el nivel de acceso de cada uno de los sectores.

5.6.1.3 PROPUESTA DE DISEÑO PARA EL SECTOR DE INGENIERIAS

A continuación se presentan las opciones de diseño para este sector, especificando los equipos seleccionados.

OPCION 1 (Figura 5.6):

NIVEL DE DISTRIBUCION:

- **Cisco Catalyst 3750G-24TS:** 24 puertos Ethernet 10/100/1000 y 4 uplinks SFP con Imagen mejorada.

NIVEL DE ACCESO:

- **Cisco Catalyst 3750-48TS:** 48 puertos Ethernet 10/100 y 4 uplinks SFP con Imagen estándar.
- **Cisco Catalyst 3750-24TS:** 24 puertos Ethernet 10/100 y 2 uplinks SFP con Imagen estándar.

OPCION 2 (Figura 5.7):

NIVEL DE DISTRIBUCION:

- **Cisco Catalyst 4510R :**
 - ✓ 4 módulos Catalyst 4500 de 48 Puertos 10/100/1000 (RJ45)
 - ✓ Equipo supervisor V, Consola (RJ45)
 - ✓ 1 módulo de 6 puertos 1000BASE-SX (Fibra Multimodo)

NIVEL DE ACCESO:

- **Cisco Catalyst 3750-48TS:** 48 puertos Ethernet 10/100 y 4 uplinks SFP con Imagen estándar.
- **Cisco Catalyst 3750-24TS:** 24 puertos Ethernet 10/100 y 2 uplinks SFP con Imagen estándar.

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

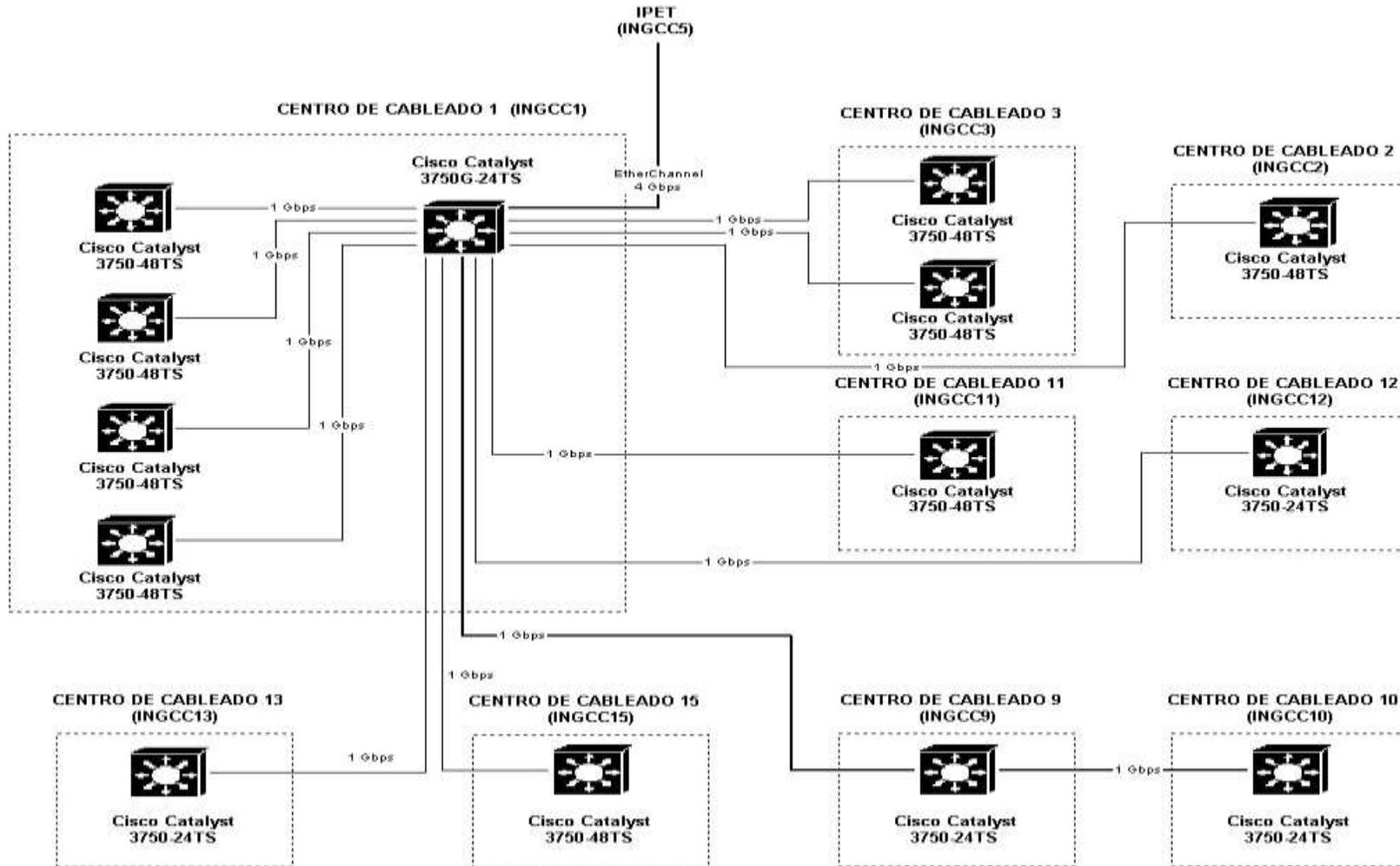


Figura 5. 6. Opción de diseño No. 1 Para el Sector de Ingenierias

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

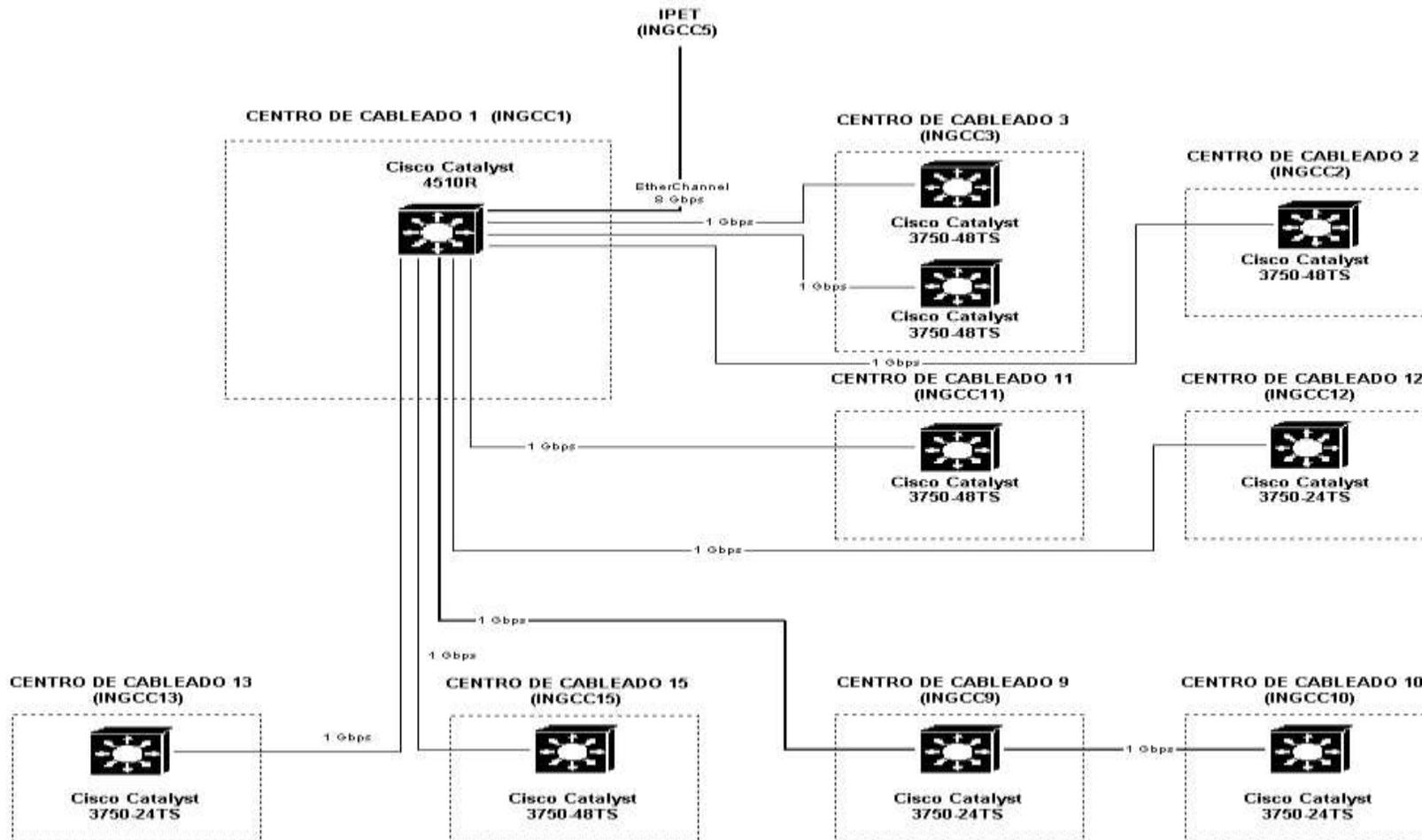


Figura 5. 7. Opción de diseño No. 2 Para el Sector de Ingenierías

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

5.6.1.4 PROPUESTA DE DISEÑO PARA EL SECTOR DE INGENIERIAS (IPET Y FISICA)

A continuación se presentan la opción de diseño para este sector, especificando los equipos seleccionados.

OPCION 1 (Figura 5.8):

NIVEL DE CORE:

- **Cisco Catalyst 4510R :**
 - ✓ 2 módulos Catalyst 4500 de 48 Puertos 10/100/1000 (RJ45)
 - ✓ Equipo supervisor V, Consola (RJ45)
 - ✓ 1 módulo de 18 puertos 1000BASE-LX (Fibra Monomodo)
 - ✓ 1 módulo de 6 puertos 1000BASE-LX (Fibra Monomodo)
 - ✓ 1 módulo de 6 puertos 1000BASE-SX (Fibra Multimodo)

NIVEL DE ACCESO:

- **Cisco Catalyst 3750-48TS:** 48 puertos Ethernet 10/100 y 4 uplinks SFP con Imagen estándar.
- **Cisco Catalyst 3750-24TS:** 24 puertos Ethernet 10/100 y 2 uplinks SFP con Imagen estándar.

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

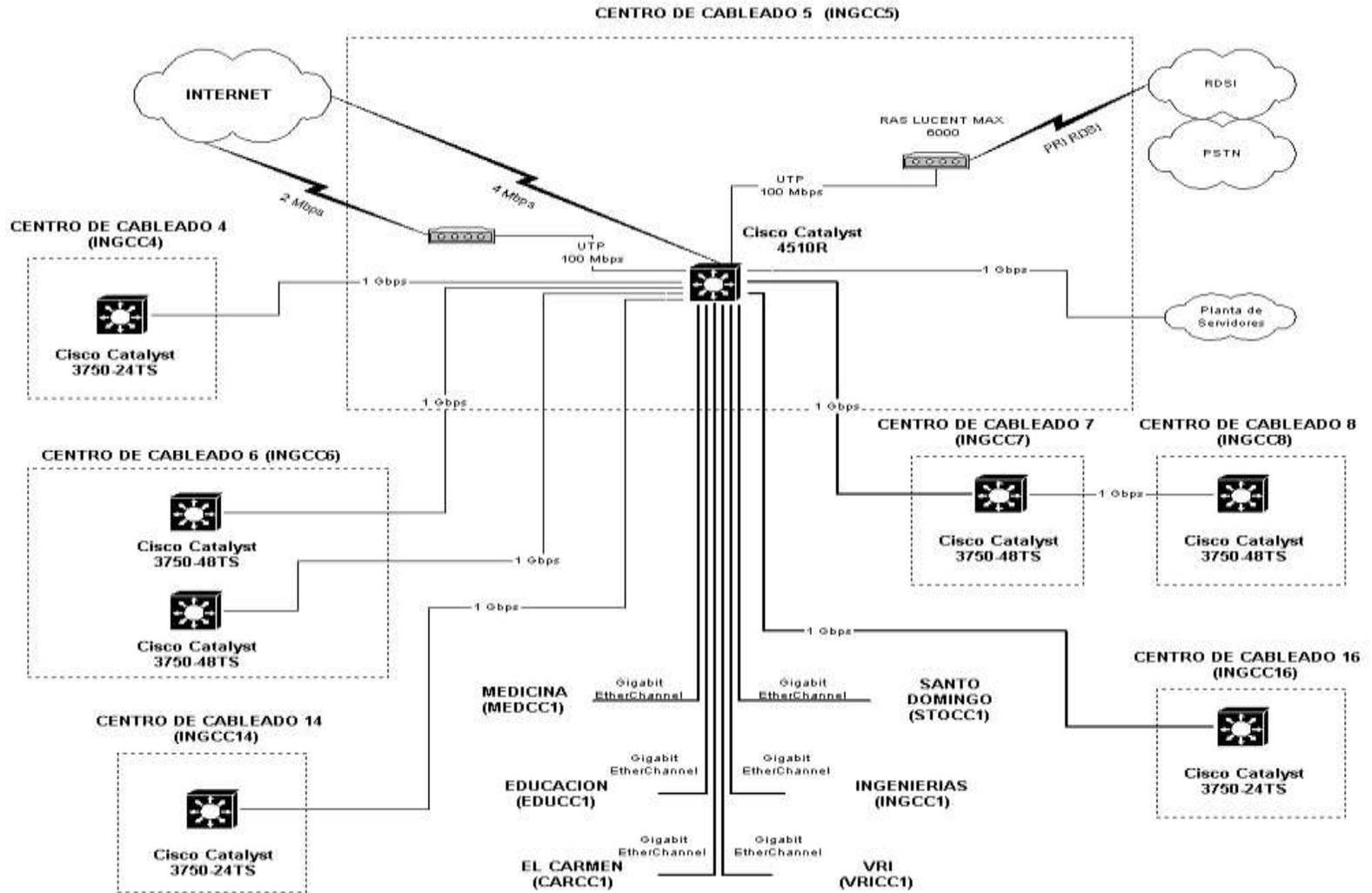


Figura 5. 8. Opción de diseño para el sector de ingenierias (IPET y FISICA)

5.6.1.5 PROPUESTA DE DISEÑO PARA EL SECTOR DE EDUCACION

A continuación se presentan las opciones de diseño para este sector, especificando los equipos seleccionados.

OPCION 1 (Figura 5.9):

NIVEL DE DISTRIBUCION:

- **Cisco Catalyst 3750G-24TS:** 24 puertos Ethernet 10/100/1000 y 4 uplinks SFP con Imagen Mejorada.

NIVEL DE ACCESO:

- **Cisco Catalyst 3750-48TS:** 48 puertos Ethernet 10/100 y 4 uplinks SFP con Imagen estándar.
- **Cisco Catalyst 3750-24TS:** 24 puertos Ethernet 10/100 y 2 uplinks SFP con Imagen estándar.

OPCION 2 (Figura 5.10):

NIVEL DE DISTRIBUCION:

- **Cisco Catalyst 4507R :**
 - ✓ 3 módulos Catalyst 4500 de 48 Puertos 10/100/1000 (RJ45)
 - ✓ Equipo supervisor V, Consola (RJ45)
 - ✓ 1 módulo de 6 puertos 1000BASE-LX (Fibra Monomodo)
 - ✓ 1 módulo de 2 puertos 1000BASE-SX (Fibra Multimodo)

NIVEL DE ACCESO:

- **Cisco Catalyst 3750-48TS:** 48 puertos Ethernet 10/100 y 4 uplinks SFP con Imagen estándar.
- **Cisco Catalyst 3750-24TS:** 24 puertos Ethernet 10/100 y 2 uplinks SFP con Imagen estándar.

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

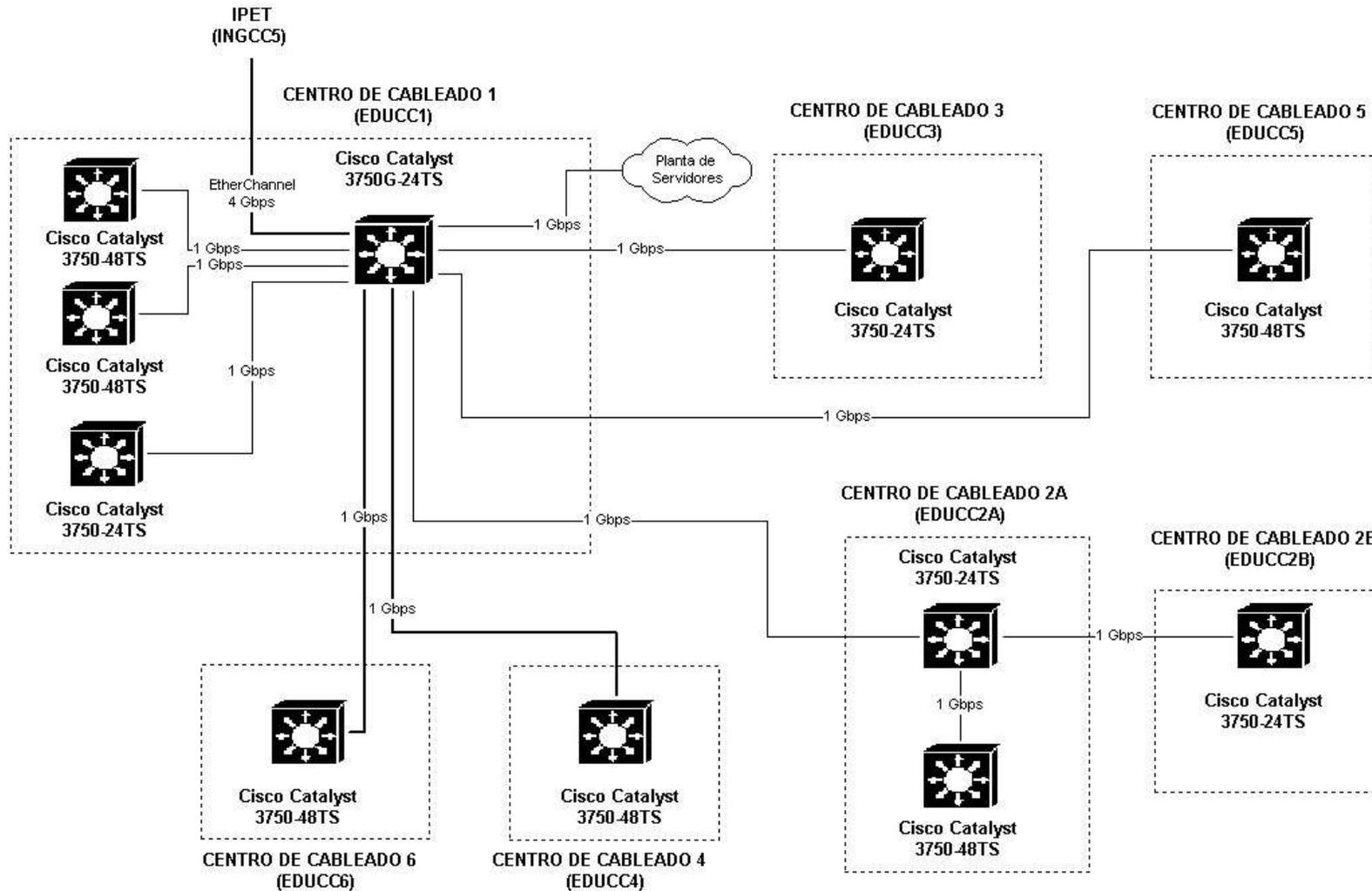


Figura 5. 9. Opción de diseño No. 1 para el Sector de Educación

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

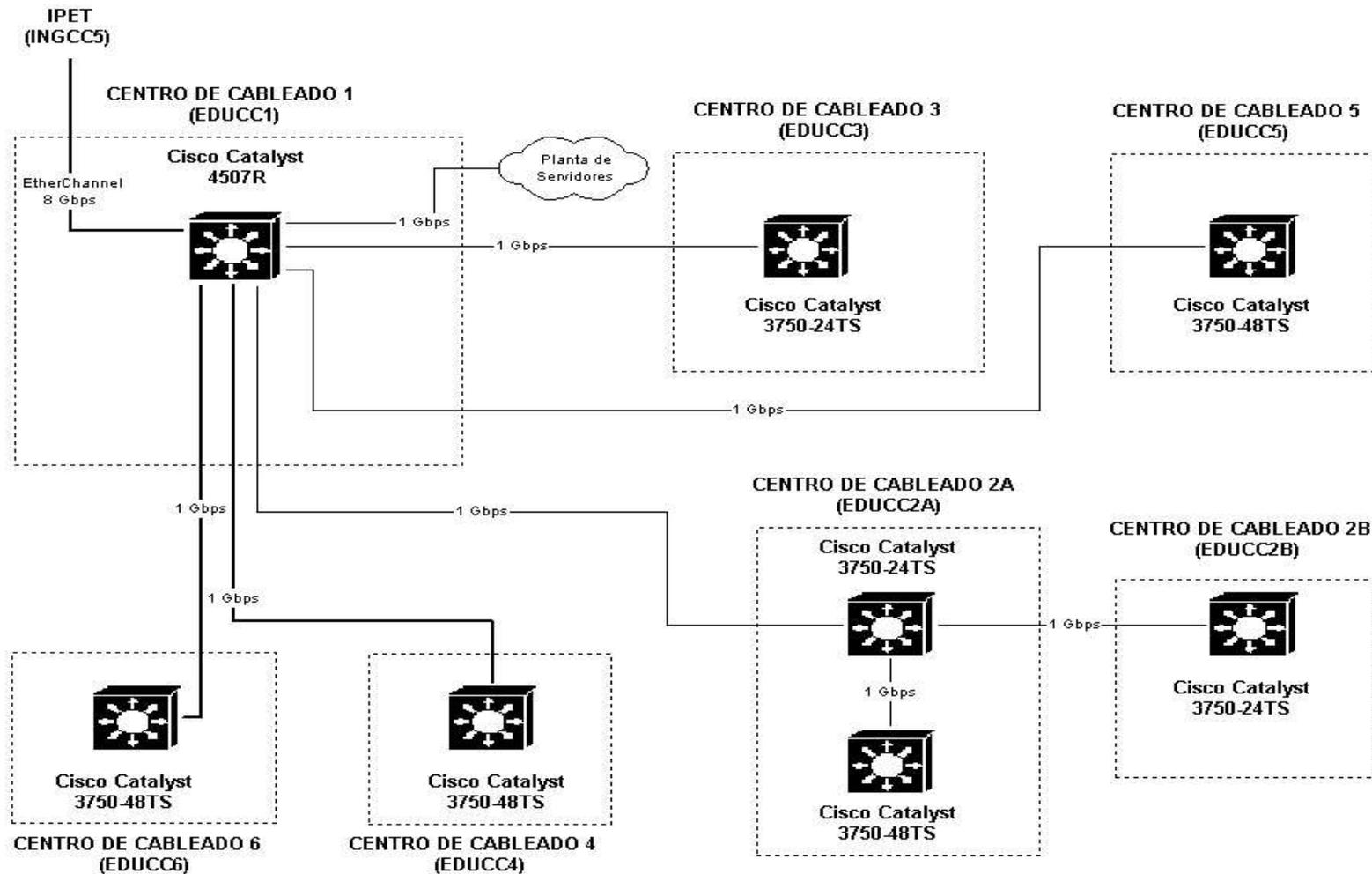


Figura 5. 10. Opción de diseño No. 2 para el Sector de Educación

5.6.1.6 PROPUESTA DE DISEÑO PARA EL SECTOR DEL CARMEN

A continuación se presentan las opciones de diseño para este sector, especificando los equipos seleccionados.

OPCION 1 (Figura 5.11):

NIVEL DE DISTRIBUCION:

- **Cisco Catalyst 3750G-12S:** 12 puertos Gigabit Ethernet SFP con Imagen Mejorada.

NIVEL DE ACCESO:

- **Cisco Catalyst 3750-48TS:** 48 puertos Ethernet 10/100 y 4 uplinks SFP con Imagen estándar.
- **Cisco Catalyst 3750-24TS:** 24 puertos Ethernet 10/100 y 2 uplinks SFP con Imagen estándar.

OPCION 2 (Figura 5.12):

NIVEL DE DISTRIBUCION:

- **Cisco Catalyst 4507R :**
 - ✓ 1 módulo Catalyst 4500 de 48 Puertos 10/100/1000 (RJ45)
 - ✓ Equipo supervisor V, Consola (RJ45)
 - ✓ 2 módulos de 6 puertos 1000BASE-LX (Fibra Monomodo)
 - ✓ 1 módulo de 2 puertos 1000BASE-SX (Fibra Multimodo)

NIVEL DE ACCESO:

- **Cisco Catalyst 3750-48TS:** 48 puertos Ethernet 10/100 y 4 uplinks SFP con Imagen estándar.
- **Cisco Catalyst 3750-24TS:** 24 puertos Ethernet 10/100 y 2 uplinks SFP con Imagen estándar.

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

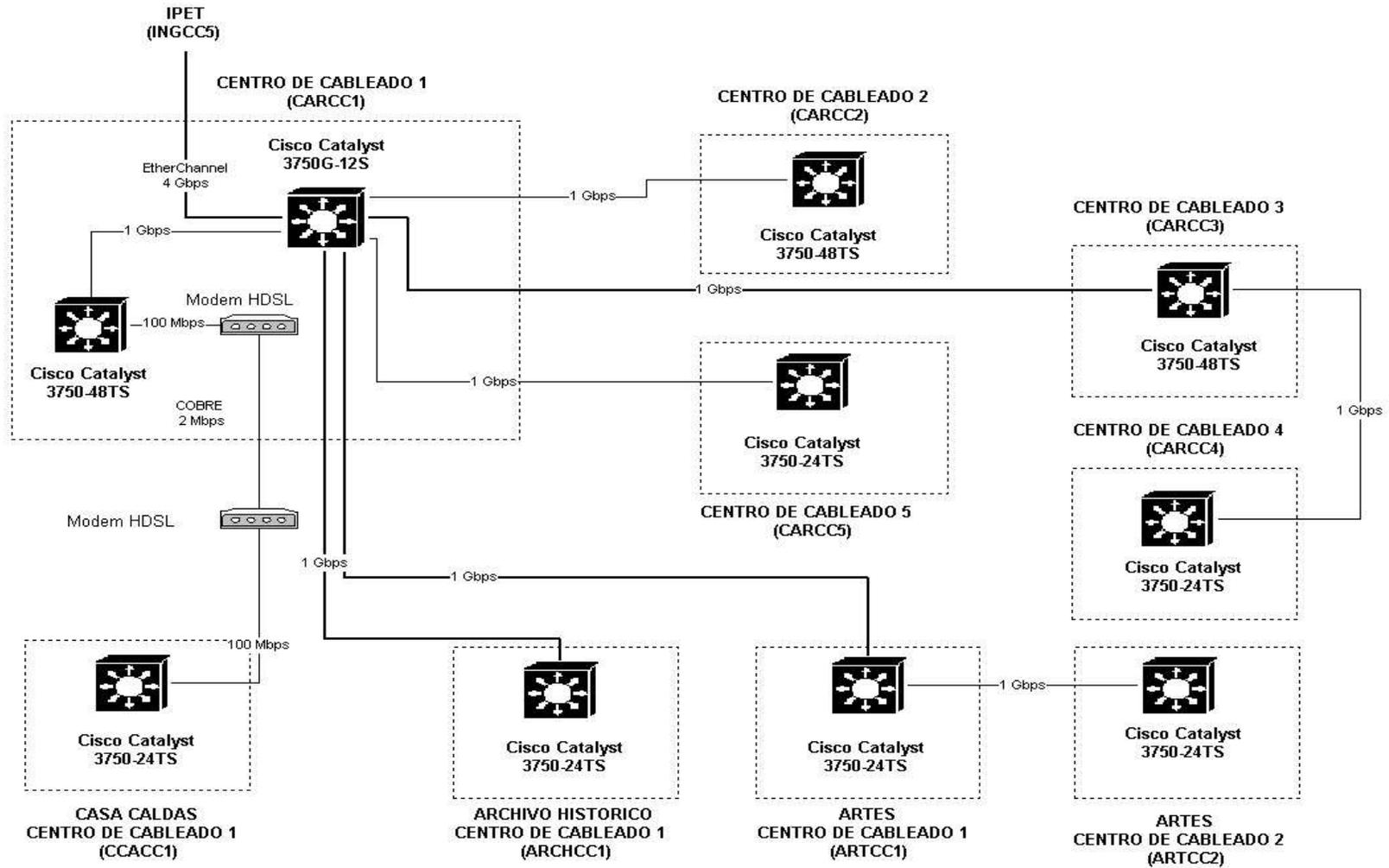


Figura 5. 11. Opción de diseño No. 1 para el Sector de El Carmen

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

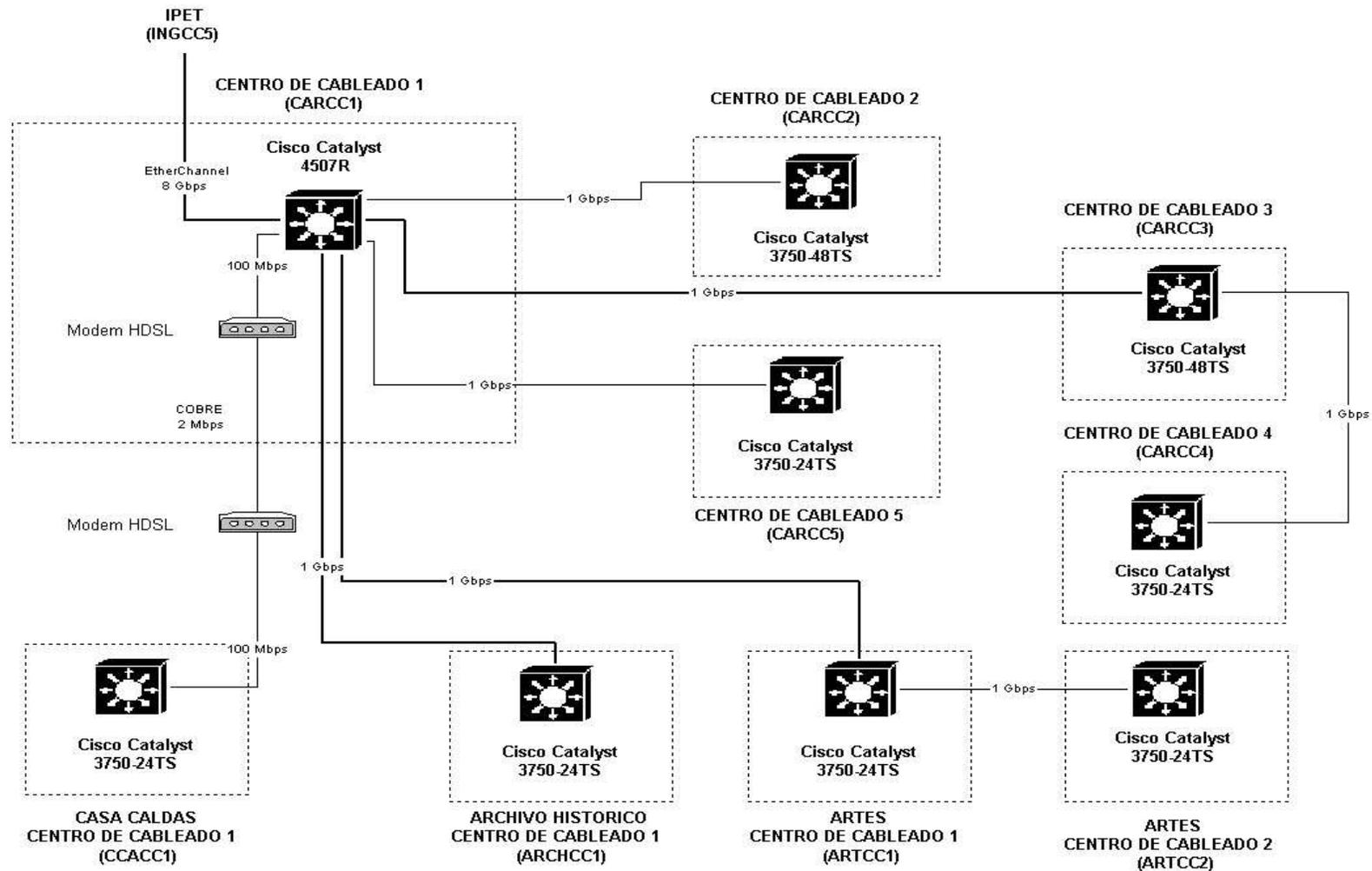


Figura 5. 12. Opción de diseño No. 2 para el Sector de El Carmen

5.6.1.7 PROPUESTA DE DISEÑO PARA EL SECTOR DE SANTO DOMINGO

De acuerdo al análisis de la infraestructura física y funcionamiento de la Red realizado en el Capítulo 3, se encontró que existen algunas configuraciones inadecuadas dentro de éste sector por lo cual se proponen los siguientes cambios a nivel de la topología:

- La conexión que existe actualmente entre CC6 y CC1 supera los límites de distancia permitidos por el estándar Ethernet para UTP, por lo que se recomienda que CC6 sea conectado a CC3.
- La conexión existente entre CC4 y CC1 abarca una distancia muy cercana al límite permitido por el estándar Ethernet para UTP lo cual puede originar inestabilidad del enlace, por lo que se recomienda que CC4 sea conectado a CC3.
- Se propone que los centros de cableado CC2 y CC5 sean conectados directamente a CC3 con el objetivo de lograr un mejor desempeño de la conexión.
- De acuerdo a los cambios propuestos anteriormente y teniendo en cuenta que en CC3 se tienen usuarios de los sistemas de información, se recomienda que el switch principal de éste centro de cableado sea un switch con puertos Gigabit y con características de alto desempeño.

A continuación se presentan las opciones de diseño para este sector, especificando los equipos seleccionados.

OPCION 1 (Figura 5.13):

NIVEL DE DISTRIBUCION:

- **Cisco Catalyst 3750G-24TS:** 24 puertos Ethernet 10/100/1000 y 4 uplinks SFP con Imagen Mejorada.

NIVEL DE ACCESO:

- **Cisco Catalyst 3750-48TS:** 48 puertos Ethernet 10/100 y 4 uplinks SFP con Imagen estándar.
- **Cisco Catalyst 3750-24TS:** 24 puertos Ethernet 10/100 y 2 uplinks SFP con Imagen estándar.

OPCION 2 (Figura 5.14):

NIVEL DE DISTRIBUCION:

- **Cisco Catalyst 4507R :**
 - ✓ 1 módulo Catalyst 4500 de 48 Puertos 10/100/1000 (RJ45)
 - ✓ Equipo supervisor V, Consola (RJ45)
 - ✓ 1 módulo de 6 puertos 1000BASE-LX (Fibra Monomodo)
- **Cisco Catalyst 3750G-24TS:** 24 puertos Ethernet 10/100/1000 y 4 uplinks SFP con Imagen Mejorada.

NIVEL DE ACCESO:

- **Cisco Catalyst 3750-48TS:** 48 puertos Ethernet 10/100 y 4 uplinks SFP con Imagen estándar.
- **Cisco Catalyst 3750-24TS:** 24 puertos Ethernet 10/100 y 2 uplinks SFP con Imagen estándar.

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

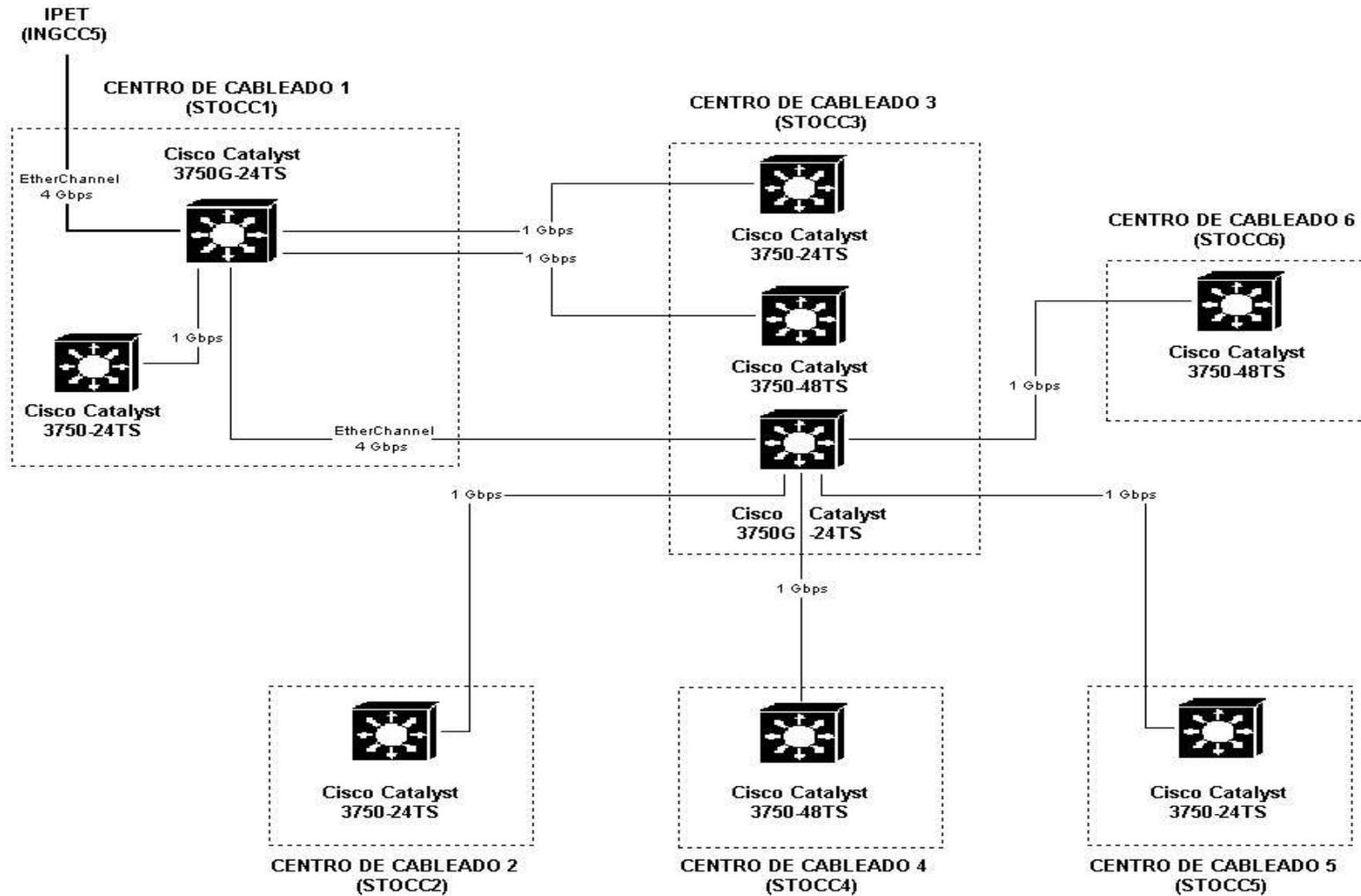


Figura 5. 13. Opción de diseño No. 1 para el Sector de Santo Domingo

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

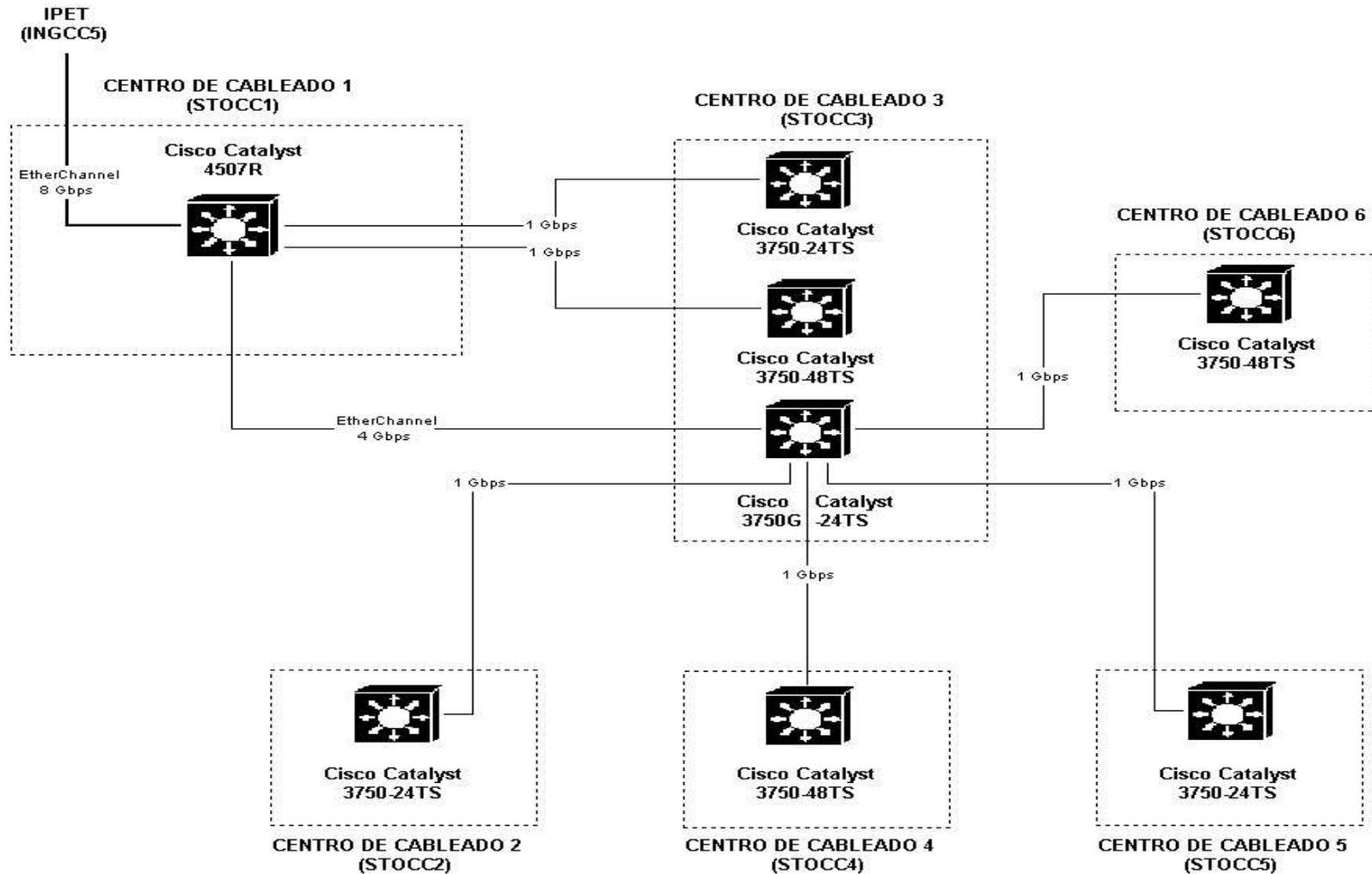


Figura 5. 14. Opción de diseño No. 2 para el Sector de Santo Domingo

5.6.1.8 PROPUESTA DE DISEÑO PARA EL SECTOR DEL VRI

A continuación se presentan las opciones de diseño para este sector, especificando los equipos seleccionados.

OPCION 1 (Figura 5.15):

NIVEL DE DISTRIBUCION:

- **Cisco Catalyst 3750G-24TS:** 24 puertos Ethernet 10/100/1000 y 4 uplinks SFP con Imagen Mejorada.

NIVEL DE ACCESO:

- **Cisco Catalyst 3750-48TS:** 48 puertos Ethernet 10/100 y 4 uplinks SFP con Imagen estándar.
- **Cisco Catalyst 3750-24TS:** 24 puertos Ethernet 10/100 y 2 uplinks SFP con Imagen estándar.

OPCION 2 (Figura 5.16):

NIVEL DE DISTRIBUCION:

- **Cisco Catalyst 4507R :**
 - ✓ 2 módulos Catalyst 4500 de 48 Puertos 10/100/1000 (RJ45)
 - ✓ Equipo supervisor V, Consola (RJ45)
 - ✓ 1 módulo de 6 puertos 1000BASE-LX (Fibra Monomodo)

NIVEL DE ACCESO:

- **Cisco Catalyst 3750-24TS:** 24 puertos Ethernet 10/100 y 2 uplinks SFP con Imagen estándar.

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

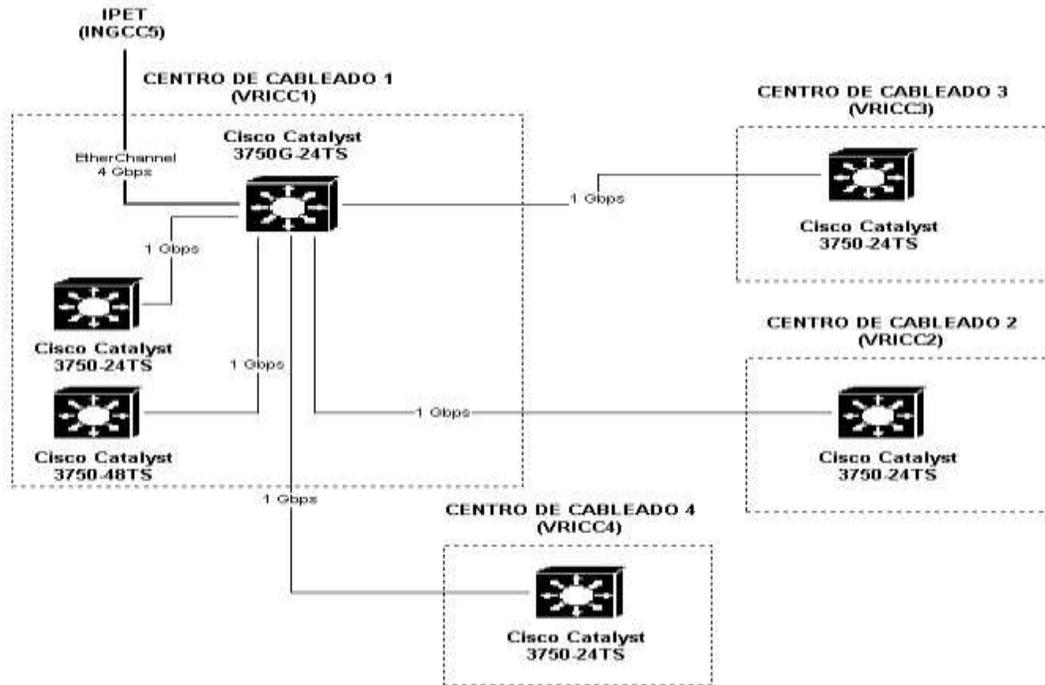


Figura 5. 15. Opción de diseño No. 1 para el Sector del VRI

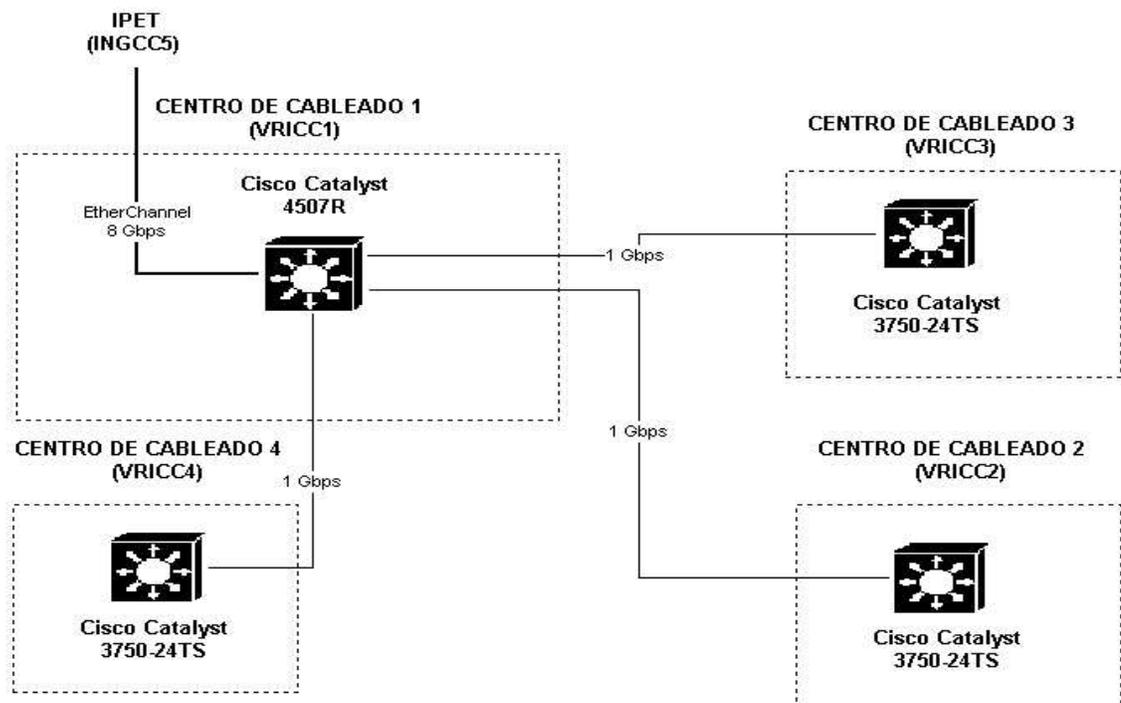


Figura 5. 16. Opción de diseño No. 2 para el Sector del VRI

5.6.1.9 PROPUESTA DE DISEÑO PARA EL SECTOR DE MEDICINA

A continuación se presentan las opciones de diseño para este sector, especificando los equipos seleccionados.

OPCION 1 (Figura 5.17):

NIVEL DE DISTRIBUCION:

- **Cisco Catalyst 3750G-24TS:** 24 puertos Ethernet 10/100/1000 y 4 uplinks SFP con Imagen Mejorada.

NIVEL DE ACCESO:

- **Cisco Catalyst 3750-48TS:** 48 puertos Ethernet 10/100 y 4 uplinks SFP con Imagen estándar.
- **Cisco Catalyst 3750-24TS:** 24 puertos Ethernet 10/100 y 2 uplinks SFP con Imagen estándar.

OPCION 2 (Figura 5.18):

NIVEL DE DISTRIBUCION:

- **Cisco Catalyst 4507R :**
 - ✓ 2 módulos Catalyst 4500 de 48 Puertos 10/100/1000 (RJ45)
 - ✓ Equipo supervisor V, Consola (RJ45)
 - ✓ 1 módulo de 2 puertos 1000BASE-LX (Fibra Monomodo)
 - ✓ 1 módulo de 2 puertos 1000BASE-SX (Fibra Multimodo)

NIVEL DE ACCESO:

- **Cisco Catalyst 3750-48TS:** 48 puertos Ethernet 10/100 y 4 uplinks SFP con Imagen estándar.
- **Cisco Catalyst 3750-24TS:** 24 puertos Ethernet 10/100 y 2 uplinks SFP con Imagen estándar.

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

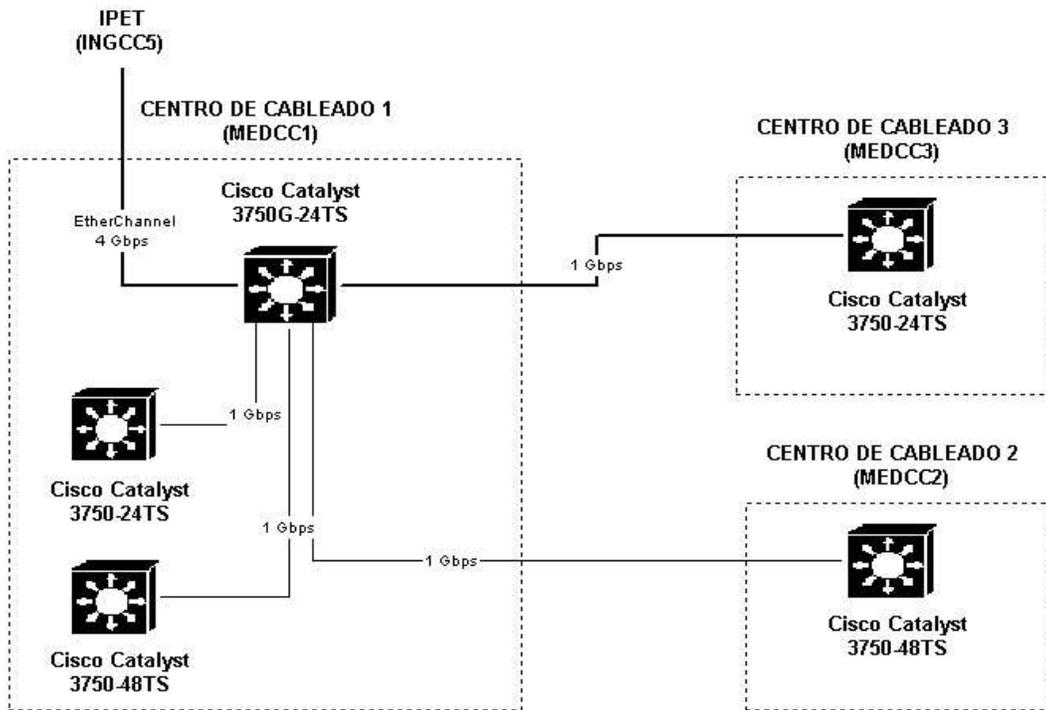


Figura 5.17. Opción de diseño No. 1 para el Sector de Medicina

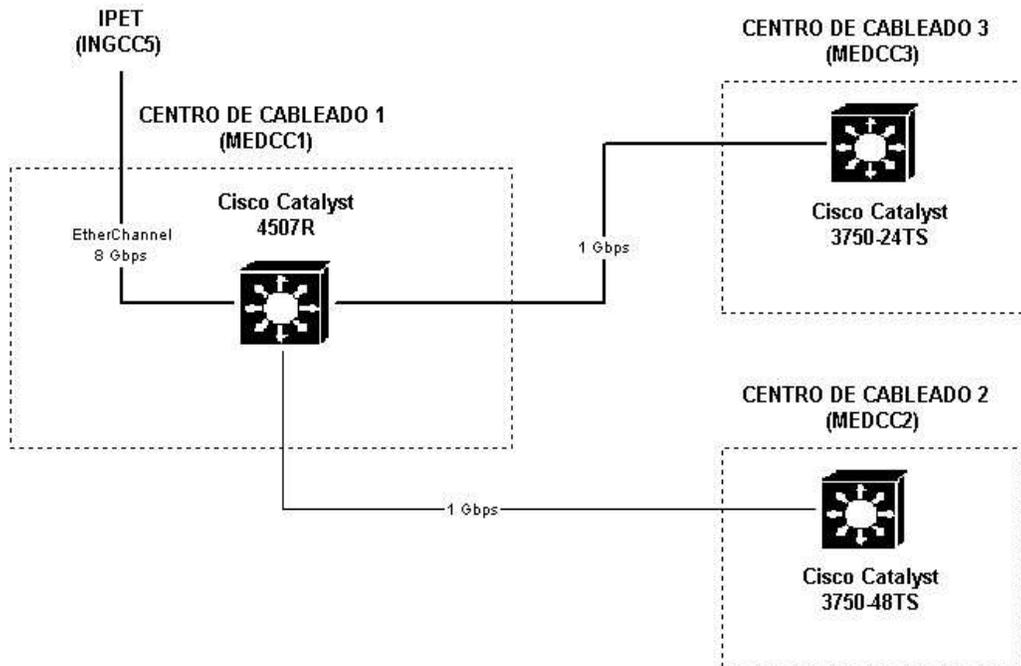


Figura 5.18. Opción de diseño No. 2 para el Sector de Medicina

5.6.1.10 PROPUESTA DE DISEÑO PARA EL BACKBONE CON TECNOLOGIA 10 GIGABIT ETHERNET

Para la posterior migración de Gigabit Ethernet hacia la tecnología 10 Gigabit Ethernet se presentan dos opciones de diseño teniendo en cuenta la ubicación del nodo de acceso a Internet. Para la implementación de estas opciones es necesario realizar los siguientes cambios a nivel del backbone:

- Debido a los requerimientos exigidos por el estándar 10 Gigabit Ethernet se debe cambiar la fibra multimodo que conecta los sectores del IPET e Ingenierías por una fibra monomodo.
- Es necesario cambiar el switch del nivel de core por un switch con soporte 10 GBE que brinde un mejor desempeño con tasas de conmutación y enrutamiento mas altas.
- Se deben actualizar los equipos supervisores de los switches de la serie Cisco Catalyst 4500 utilizados en el nivel de distribución, para adquirir el soporte 10 GBE.
- Si el nodo de acceso WAN es ubicado en El Carmen, se recomienda utilizar el switch de la serie Cisco Catalyst 6500 tanto en el sector de El Carmen como en el sector del IPET, ya que en éste último sector se reciben los sectores de Ingenierías, Medicina y Educación, los cuales se conectan a 10 Gbps, por lo cual es necesario un equipo de muy buen desempeño.
- En la opción de diseño No. 1 no se utiliza la agregación de enlaces para el backbone, sin embargo esta técnica se puede implementar en un futuro según las nuevas necesidades y requerimientos que se presenten en la Red.
- En la opción de diseño No. 2 se propone realizar agregación de enlaces entre los nodos del IPET y El Carmen, debido a que por la topología planteada, éste enlace puede presentar problemas de congestión.

A continuación se presentan las opciones de diseño para el backbone:

OPCION 1 (Figura 5.19):

NIVEL DE CORE:

- **Cisco Catalyst 6513R :**
 - ✓ 4 módulos Catalyst 6500 de 48 Puertos 10/100/1000 (RJ45)
 - ✓ Equipo supervisor 720
 - ✓ 1 módulo de 2 puertos 1000BASE-SX (Fibra Multimodo)
 - ✓ 2 módulos de 4 puertos 10GBASE-LR (Fibra Monomodo)

NIVEL DE DISTRIBUCION:

- **Cisco Catalyst 4510R⁸**
- **Cisco Catalyst 4507R**

OPCION 2 (Figura 5.20):

NIVEL DE CORE:

- **Cisco Catalyst 6513R :**
 - ✓ 1 módulo Catalyst 6500 de 48 Puertos 10/100/1000 (RJ45)
 - ✓ Equipo supervisor 720
 - ✓ 1 módulo de 2 puertos 1000BASE-SX (Fibra Multimodo)
 - ✓ 1 módulo de 2 puertos 1000BASE-LX (Fibra Monomodo)
 - ✓ 1 módulo de 4 puertos 10GBASE-LR (Fibra Monomodo)

NIVEL DE DISTRIBUCION:

- **Cisco Catalyst 6513R :**
 - ✓ 4 módulos Catalyst 6500 de 48 Puertos 10/100/1000 (RJ45)
 - ✓ Equipo supervisor 720
 - ✓ 1 módulo de 2 puertos 1000BASE-SX (Fibra Multimodo)
 - ✓ 2 módulos de 4 puertos 10GBASE-LR (Fibra Monomodo)
- **Cisco Catalyst 4510R⁹**
- **Cisco Catalyst 4507R**

⁸ Los módulos RJ45 están especificados en las propuestas de diseño presentadas para cada sector. Los módulos de fibra de los switches 4500 que se conectan al switch 6513R deben ser actualizados para soportar 10 GBE.

⁹ Los módulos RJ45 están especificados en las propuestas de diseño presentadas para cada sector.

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

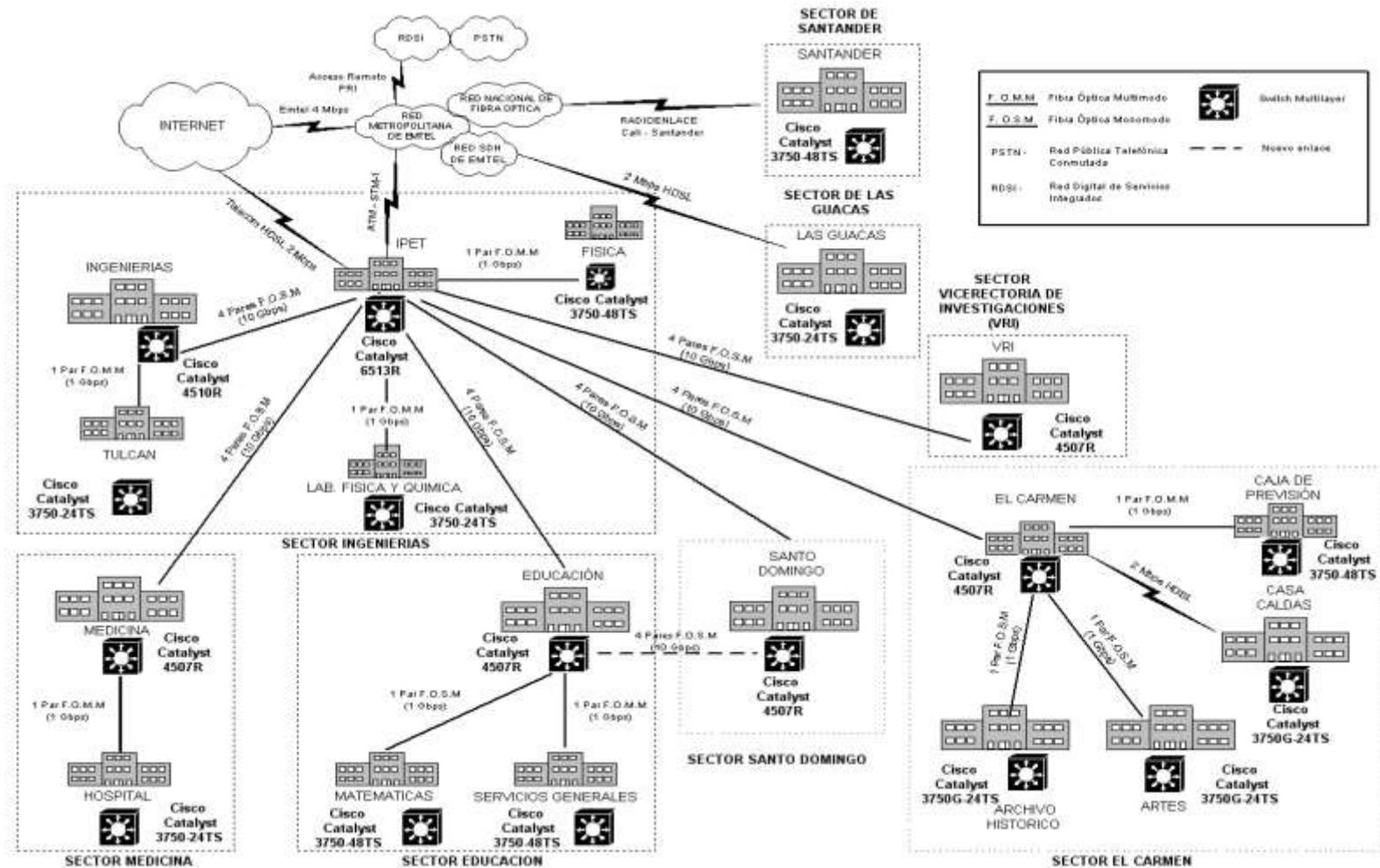


Figura 5. 19. Opción de diseño No. 1 para el backbone con tecnología 10 Gigabit Ethernet

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

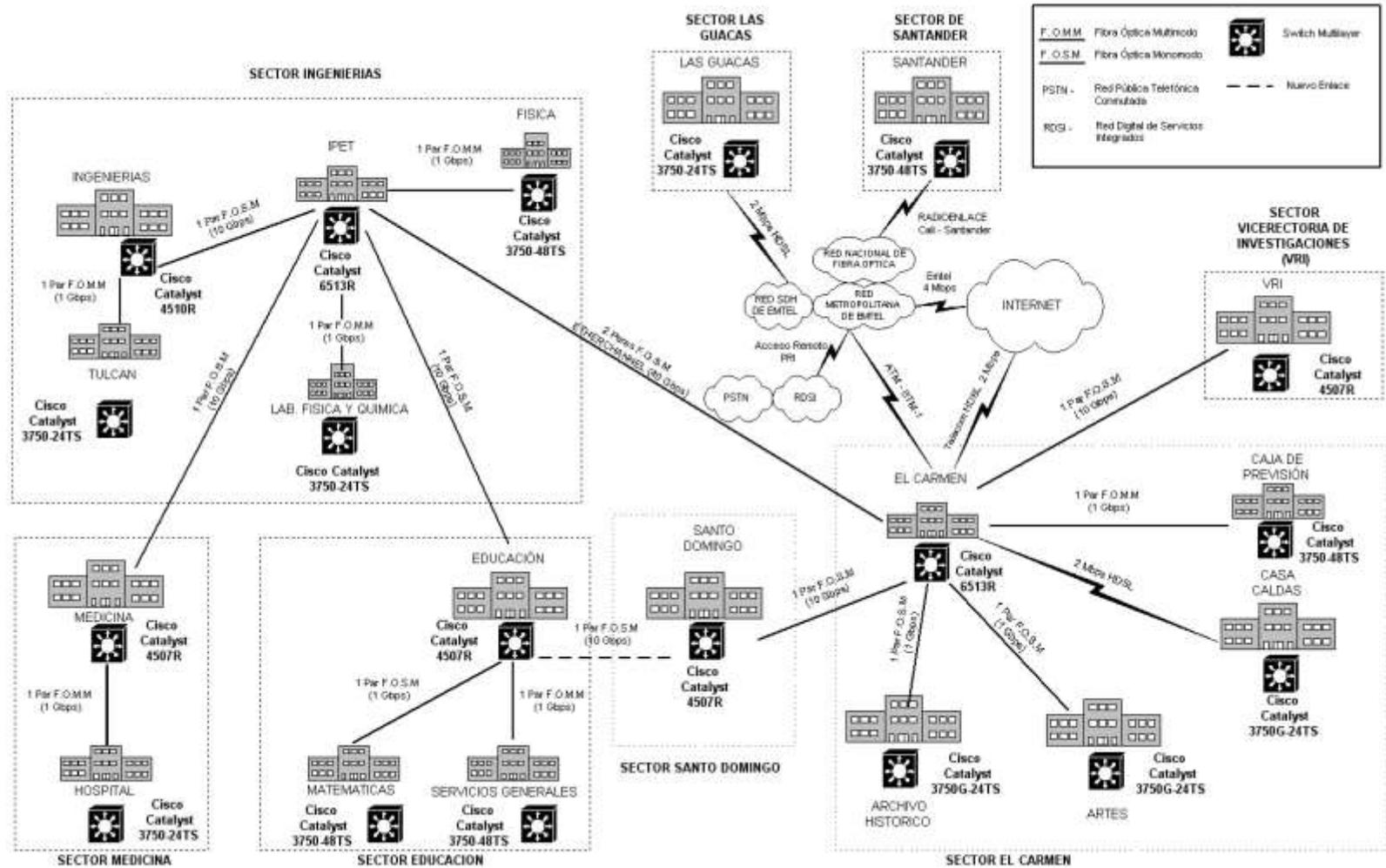


Figura 5. 20. Opción de diseño No. 2 para el backbone con tecnología 10 Gigabit Ethernet

5.6.2 PROPUESTA DE DISEÑO CON LOS PRODUCTOS ALCATEL

5.6.2.1 DESCRIPCION GENERAL DE LOS PRODUCTOS ALCATEL

A continuación se describe de manera general los switches Alcatel utilizados en el diseño¹⁰:

- **SWITCHES DE LA FAMILIA OMNISWITCH 6600.**

La familia de switches OmniSwitch 6600 son switches 10/100 Mbps de nivel 3 que proveen conmutación de nivel 2, routing de nivel 3 y servicios avanzados con alta disponibilidad para ambientes con comunicaciones IP y de misión crítica. Esta familia de switches ofrece características de alta disponibilidad, seguridad en la red, políticas de calidad de servicio y gestión simplificada, las cuales la convierten en una gran elección para las siguientes aplicaciones:

- ✓ Grupos de trabajo empresariales / centros de cableado LAN
- ✓ Sucursales
- ✓ Ambientes de convergencia de voz y datos
- ✓ Potencia sobre Ethernet
- ✓ Fibra 100BaseFx al escritorio

La familia OmniSwitch 6600 consiste de las series OmniSwitch 6600 y OmniSwitch 6602. El OmniSwitch 6600 provee 24/48 puertos con velocidades de 10/100 Mbps con dos slots de expansión para dos puertos opcionales Gigabit para módulos de stacking y/o uplinks Gigabit de fibra o cobre. Cuenta con un slot interno en la parte de atrás del chasis para conectar una fuente de poder de respaldo.

CONFIGURACIONES

El OmniSwitch 6600 posee las siguientes configuraciones:

- ✓ **OmniSwitch 6600-24** : 24 puertos RJ45 10/100
- ✓ **OmniSwitch 6600-48** : 48 puertos RJ45 10/100
- ✓ **OmniSwitch 6600-U24** : 24 puertos SFP base 100 Base FX
- ✓ **OmniSwitch 6600-P24** : 24 puertos RJ45 10/100 con soporte del estándar PoE (utiliza fuente de poder externa de respaldo)

La serie OS6602 está basado en el OS6600, pero viene con un nuevo diseño y una configuración fija que incluye dos puertos SFP para conectividad Gigabit y dos

¹⁰ Para mayor información sobre este tipo de switches referase al Anexo D.

puertos para establecer stacks. El OS6602 es completamente compatible con el OS6660 incluyendo un stack mixto de chasis virtual.

- ✓ **OmniSwitch 6602-24** : 24 puertos RJ45 10/100
- ✓ **OmniSwitch 6602-48** : 48 puertos RJ45 10/100

- **SWITCHES DE LA SERIE OMNISWITCH 6800.**

La familia Alcatel OmniSwitch 6800 son switches Ethernet avanzados, con soporte de stack, con configuración fija, y con tres velocidades (10/100/1000). Proveen altas tasas de conmutación de nivel 2 y enrutamiento de nivel 3 con servicios avanzados. El OS6800 incrementa el desempeño de la red mejorando el tiempo de respuesta de las aplicaciones, seguridad en la LAN, maximizando la capacidad y servicios de la red sobre el cableado de categoría 5/5e/6 existente. Con el soporte de tres velocidades, formación de grupos de puertos (4 puertos 10/100/1000 o mini-GBIC), módulos de 10 Gigabit Ethernet, las organizaciones puede proteger sus inversiones asegurando la posibilidad de llevar nuevos procesos de migración en un futuro.

Un diseño con tamaño compacto, chasis virtual, y conjunto amplio de características hacen del OS6800 perfecto para las siguientes aplicaciones:

- Grupos de trabajo y centros de cableado LAN
- Switches de nivel de distribución en redes de tres niveles
- Calidad de servicio (QoS) para aplicaciones de misión crítica
- Centros de datos y clusters de servidores

CONFIGURACIONES.

Los switches OS6800 ofrecidos actualmente son:

- **OmniSwitch 6800-24:** switch Gigabit Ethernet de nivel 3, configuración fija, con 20 puertos RJ45 10/100/1000, más dos puertos de stacking y grupos de cuatro puertos¹¹.
- **OmniSwitch 6800-48:** switch Gigabit Ethernet de nivel 3, configuración fija, con 44 puertos RJ45 10/100/1000, más dos puertos de stacking y grupos de cuatro puertos, con soporte de 10 Gigabit Ethernet.
- **OmniSwitch 6800-U24:** switch Gigabit Ethernet de nivel 3, configuración fija, con 20 puertos mini-GBIC (SFP), más grupos de cuatro puertos y soporte de 10 Gigabit Ethernet.

¹¹ Los grupos de puertos en todos los modelos consisten de cuatro puertos RJ45 10/100/1000 o cuatro puertos mini-GBIC.

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

Los modelos futuros pueden incluir switches de 24 y 48 puertos con soporte de los estándares potencia sobre Ethernet (PoE) y 10 Gbps.

El OS6800 utiliza un módulo externo para proporcionar soluciones con fuente de poder redundante.

La familia OmniSwitch 6800 es el switch Gigabit Ethernet de configuración fija más avanzado de Alcatel. El portafolio Alcatel de switches de configuración fija incluye las siguientes familias:

- Familia de switches OmniStack 6100: Nivel 2+ 10/100
- Familia de switches OmniStack 6300: Nivel 2+ 10/100/1,000
- Familia de switches OmniSwitch 6600: Nivel 3 10/100

Los switches Alcatel de configuración fija son parte de un gran portafolio que incluye los switches de core de las series OmniSwitch 7700, 7800 y 8800. Este portafolio ofrece una solución completa de core a acceso con una alta disponibilidad, desempeño inteligente, y seguridad mejorada en un paquete fácil de gestionar, flexible y escalable.

- **SWITCHES DE LA FAMILIA OMNISWITCH 7000.**

La familia Alcatel OmniSwitch 7000 esta constituida por los switches OmniSwitch 7000 y OmniSwitch 7800, esta familia de switches provee una plataforma de conmutación multinivel que proporciona una alta disponibilidad e inteligencia en la red. Estas nuevas plataformas hacen parte de la familia de productos de nueva generación OmniSwitch de Alcatel.

La familia Alcatel OmniSwitch 7000 entrega características de alta disponibilidad y desempeño con una gestión simplificada para un amplio rango de ambientes empresariales. Esta nueva plataforma de conmutación está optimizada para la integración de voz y datos proporcionando una capacidad Gigabit Ethernet non-blocking, seguridad multinivel, alta disponibilidad, conmutación inteligente y servicios de routing.

CONFIGURACIONES.

La familia de switches OmniSwitch 7000 tiene las siguientes configuraciones:

- ✓ **OmniSwitch 7700:** posee un chasis modular de 10 slots que soporta una capacidad de agregación de puertos de hasta 192 puertos Gigabit Ethernet full duplex.

- ✓ **OmniSwitch 7800:** posee un chasis modular de 18 slots que soporta una capacidad de agregación de puertos de hasta 348 puertos Gigabit Ethernet full duplex.

Estas plataformas han sido construidas para ambientes de convergencia de voz y datos y comunicaciones IP, ofreciendo características como avanzada calidad de servicio, distribución de potencia in line para teléfonos IP. Estos switches han sido diseñados para una operación continua, con dos slots dedicados al Modulo de Gestión del Chasis (CMM), ofreciendo una capacidad en el CMM de 64 Gbps en el OmniSwitch 7700 y 128 Gbps en el OmniSwitch 7800. Permiten la creación de configuraciones de redundancia con una amplia capacidad de interfaces Ethernet y densidad de puertos.

- **SWITCHES DE LA FAMILIA OMNISWITCH 8800.**

El OmniSwitch 8800 es un switch multinivel que provee las últimas soluciones para el desempeño y disponibilidad de las redes. El OmniSwitch 8800 forma parte de la plataforma de Alcatel de nueva generación, entregando las mejores características de funcionalidad con una densidad de puertos y throughput para comunicaciones IP sin precedentes, implementaciones de core, y ambientes de misión crítica. Posee una plataforma de alta densidad y capacidad soportando hasta 384 puertos de Gigabit Ethernet dentro de un rack de 40 pulgadas. El OmniSwitch 8800 proporciona conectividad 10 Gigabit Ethernet non-blocking, una alta disponibilidad, seguridad multinivel, y servicios de conmutación y routing inteligente.

El OmniSwitch 8800 provee numerosas características de conmutación a alta velocidad y conectividad entre edificios y campus. El OS 8800 está bien preparado para muchos ambientes, incluyendo los siguientes:

- Aplicaciones en el core y backbone de una organización
- Grandes centros de datos y granjas de servidores
- Alta densidad de agregación de puertos Gigabit Ethernet
- Ambientes MAN Gigabit Ethernet

El OmniSwitch 8800 comprende un chasis de 18 slots que soporta una capacidad de agregación de puertos de hasta 384 puertos Gigabit Ethernet full duplex. Diseñado para una operación continua sin interrupciones, posee dos slots dedicados para configuraciones redundantes de los Módulos de Gestión del Chasis (CMM), proporcionado una capacidad de 512 Gbps en el CMM. El OS 8800 fue diseñado para manejar altos requerimientos de tráfico y aplicaciones que demandan velocidades del orden de 10 Gigabit Ethernet, ofreciendo características como:

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

- Plataforma de conmutación de alta densidad y capacidad
- Servicios de conmutación y routing inteligente a alta velocidad
- Balanceo de carga
- Seguridad multinivel

5.6.2.2 EQUIVALENCIA ENTRE LOS PRODUCTOS DE ALCATEL Y CISCO

A continuación se describe la equivalencia entre los diferentes productos utilizados en el diseño. Esta equivalencia se realizó teniendo en cuenta parámetros tales como:

- Calidad de servicio (QoS)
- Seguridad
- Gestión
- Desempeño
- Disponibilidad
- Densidad de puertos

PRODUCTOS CISCO	PRODUCTOS ALCATEL
Catalyst 3750-24TS	OmniSwitch 6600-24
Catalyst 3750-48TS	OmniSwitch 6600-48
Catalyst 3750G-24TS	OmniSwitch 6800-24
Catalyst 3750G-12S	OmniSwitch 6800-24
Catalyst 4507R	OmniSwitch 7800 ¹²
Catalyst 4510R	OmniSwitch 7800
Catalyst 6513R	OmniSwitch 8800 ¹³

Tabla 5. 2. Equivalencia entre los equipos de Alcatel y Cisco

5.7 FASES DE MIGRACION HACIA GIGABIT ETHERNET

Puesto que Gigabit Ethernet es Ethernet, los tipos de productos Gigabit Ethernet son muy completos: Switches de nivel 2, switches de nivel 3 (o switches routing), switches multinivel, módulos uplink/downlink, Tarjetas de red o NICs Gigabit

¹² Para el OS 7800 se deben utilizar módulos de 2 puertos GBIC, módulos de 12 puertos MiniGBIC y módulos de 12 puertos 10/100/1000BaseT, de acuerdo a la densidad de puertos que se necesite en cada sector.

¹³ Para el OS 8800 se deben utilizar módulos de 1 puerto 10GBase-X, módulos de 8 o 24 puertos MiniGBIC y módulos de 8 y 24 puertos 10/100/1000BaseT, de acuerdo a la densidad de puertos que se necesite en cada sector.

Ethernet. Hay switches Ethernet con puertos Gigabit Ethernet puros con backplanes de alto desempeño, así como también dispositivos que combinan puertos Fast y Gigabit Ethernet. Los uplinks Gigabit Ethernet han aparecido como actualización modular de dispositivos Fast Ethernet de configuración fija o modular.

Las aplicaciones iniciales para Gigabit Ethernet son para campus o edificios con grandes requerimientos de ancho de banda entre routers, switches, hubs, y servidores.

En estas fases de migración, no se espera desplegar Gigabit Ethernet hasta el escritorio. En todos los escenarios, los sistemas operativos de red, aplicaciones y equipos de escritorio permanecen iguales.

El proceso de migración hacia Ethernet de alta velocidad es presentado en fases; y no como una planeación hecha año por año, con cronograma y con fechas de implementación definidas, por que todo esto depende de las posibilidades económicas y administrativas de la Universidad. Sin embargo, es muy importante indicar que la implementación de estas etapas de evolución debería llevarse a cabo en un periodo total de aproximadamente 3 años, al cabo del cual se deberá realizar un nuevo estudio de la Red. La razón primordial de esta limitación es que según recomendaciones se considera que las tecnologías cambian aproximadamente cada 3 años, surgiendo nuevas tecnologías que satisfagan de una mejor manera las necesidades contemporáneas de la Red con respecto a las tecnologías anteriores

A continuación se presentan las diferentes fases de evolución que puede adoptar la Universidad del Cauca para realizar un proceso de migración paulatino, teniendo en cuenta que se deben considerar además de factores técnicos aspectos económicos, que permitan implementar un proceso de migración óptimo.

5.7.1 FASE No. 1: ACTUALIZACIÓN DE ENLACES SWITCH A SWITCH (BACKBONE)

Un escenario muy completo de actualización es mejorar los enlaces 100 Mbps entre switches o repetidores Fast Ethernet hacia enlaces 1000 Mbps entre switches 10/100/1000. Tal aumento de ancho de banda en los enlaces switch a switch habilitarían los switches 10/100/1000 para soportar un gran numero de segmentos Fast Ethernet tanto compartidos como conmutados.

En esta fase se debe realizar la adquisición de nuevos equipos que soporten la tecnología Gigabit Ethernet para ser utilizados en el backbone, el cual comprende el switch principal del nivel de core ubicado en el IPET (INGCC5) y los equipos del nivel de distribución ubicados en los sectores de Ingenierías (INGCC1), Educación (EDUCC1), Medicina (MEDCC1), Santo Domingo (STOCC1), El Carmen (CARCC1) y Vicerrectoría de Investigaciones (VRICC1).

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

La figura 5.21 ilustra la red antes de la actualización, mientras que la figura 5.22 ilustra la red después de la actualización hacia Gigabit Ethernet.

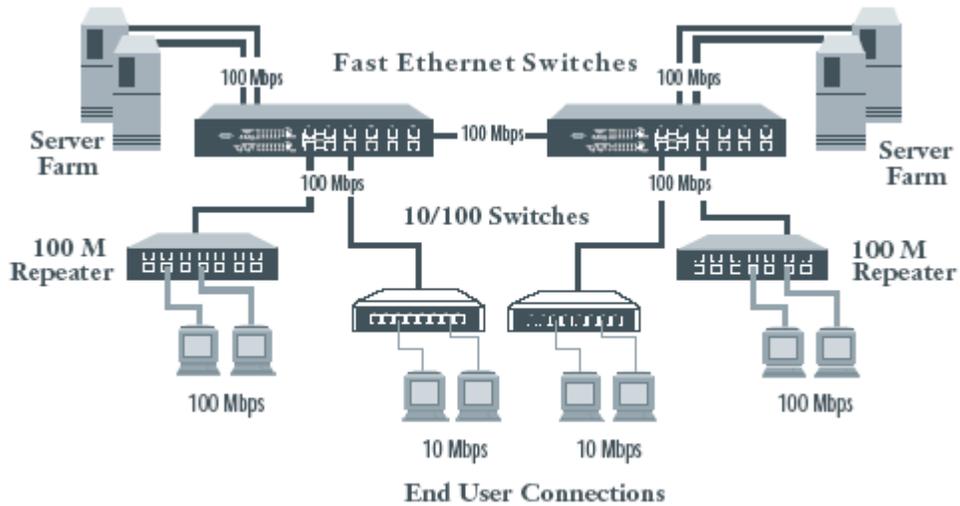


Figura 5. 21. Enlace switch a switch – antes de la actualización

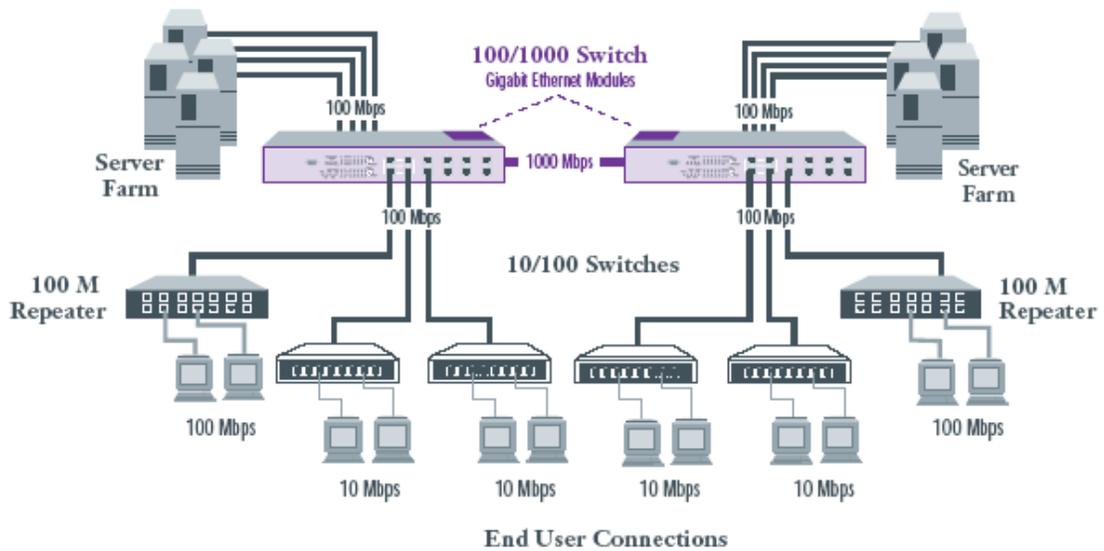


Figura 5. 22. Enlace switch a switch – después de la actualización

5.7.2 FASE No. 2: ACTUALIZACIÓN DE ENLACES SWITCH A SERVIDOR

El más simple escenario de actualización es migrar un switch Fast Ethernet hacia un switch Gigabit Ethernet para obtener altas velocidades, interconexión a 1000 Mbps hacia una granja de servidores de alto desempeño con NICs Gigabit Ethernet instaladas.

Por lo tanto, en esta fase se debe realizar la actualización de las tarjetas de red 10/100 Mbps hacia las tarjetas de red 10/100/1000 Mbps en todos los servidores de la Red de Datos. Debido a que estos servidores se encuentran conectados a los switches del nivel de core y de distribución, sería conveniente realizar esta etapa conjuntamente con la fase de actualización del backbone para lograr un mejor rendimiento y obtener mayores beneficios.

La figura 5.23 ilustra la red antes de la actualización, mientras que la figura 5.24 ilustra la red después de la actualización hacia Gigabit Ethernet.

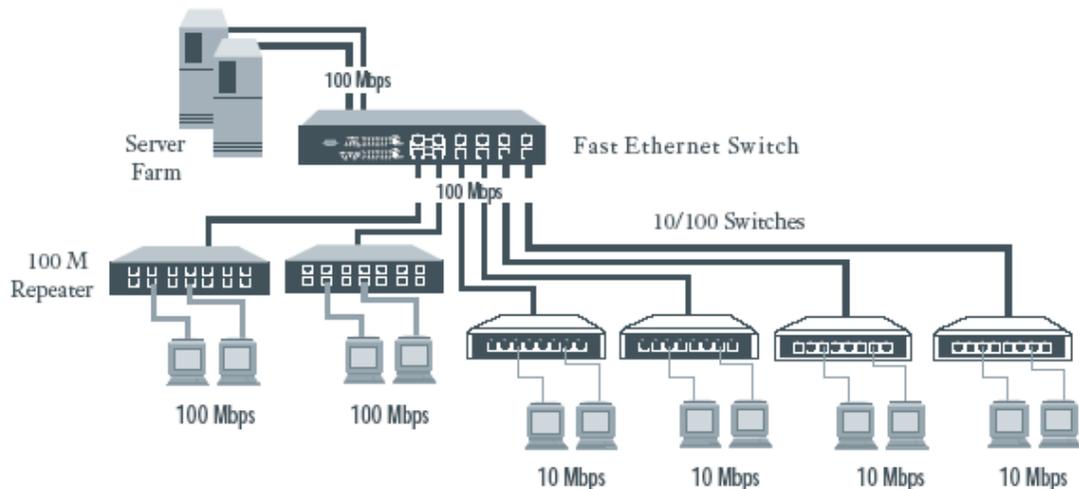


Figura 5. 23. Enlace switch a servidor – antes de la actualización

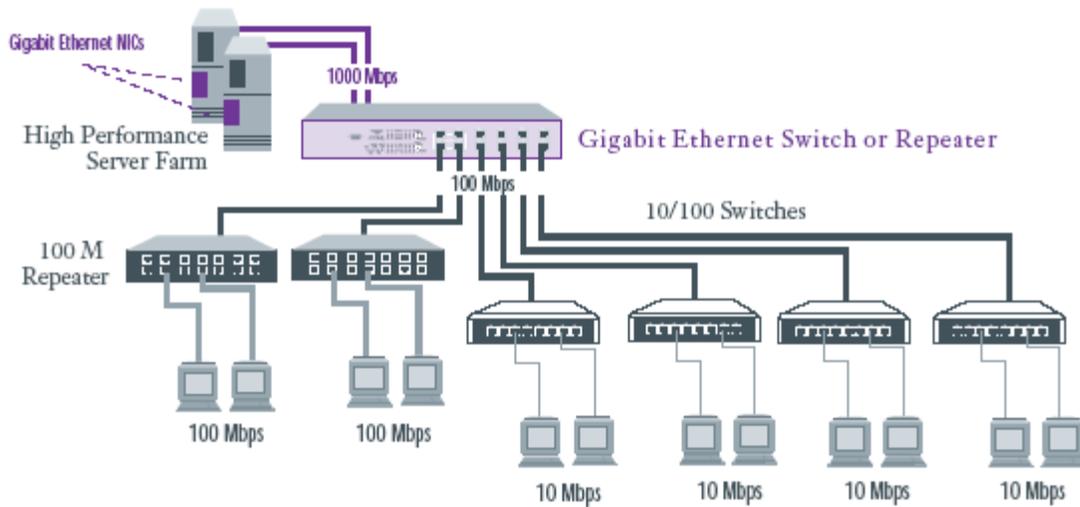


Figura 5. 24. Enlace switch a servidor – después de la actualización

5.7.3 FASE No. 3: ACTUALIZACIÓN DE SEGMENTOS ETHERNET Y FAST ETHERNET

Un switch del backbone Fast Ethernet que agrega múltiples switches 10/100 puede ser actualizado hacia un switch Gigabit Ethernet soportando múltiples switches 10/100/1000 así como también otros dispositivos tales como routers y hubs con interfaces Gigabit Ethernet y Uplinks. Una vez que el backbone es actualizado a un switch Gigabit Ethernet, los servidores de alto desempeño pueden ser conectados directamente al backbone con NICs Gigabit Ethernet, incrementando el rendimiento hacia los servidores para usuarios con aplicaciones que requieren gran ancho de banda. También, la red puede ahora soportar un gran número de segmentos, más ancho de banda por segmento, y por lo tanto un gran número de nodos por segmento.

En esta fase se debe realizar la adquisición de switches 10/100 Mbps con uplinks Gigabit Ethernet para ser desplegados en el nivel de acceso, teniendo en cuenta la demanda de ancho de banda de los segmentos que se evidenció en el análisis de desempeño realizado en el Capítulo 3.

La figura 5.25 ilustra la red antes de la actualización, mientras que la figura 5.26 ilustra la red después de la actualización hacia Gigabit Ethernet.

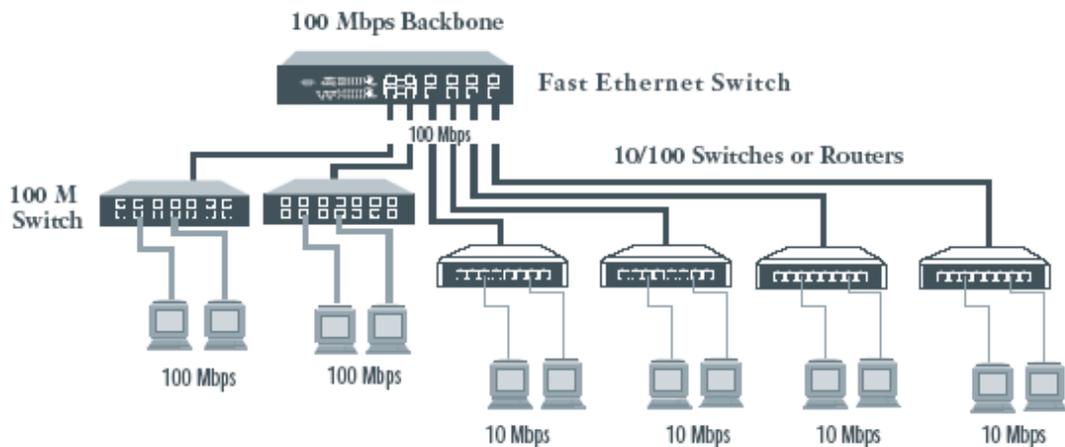


Figura 5. 25. Segmentos Fast Ethernet – antes de la actualización

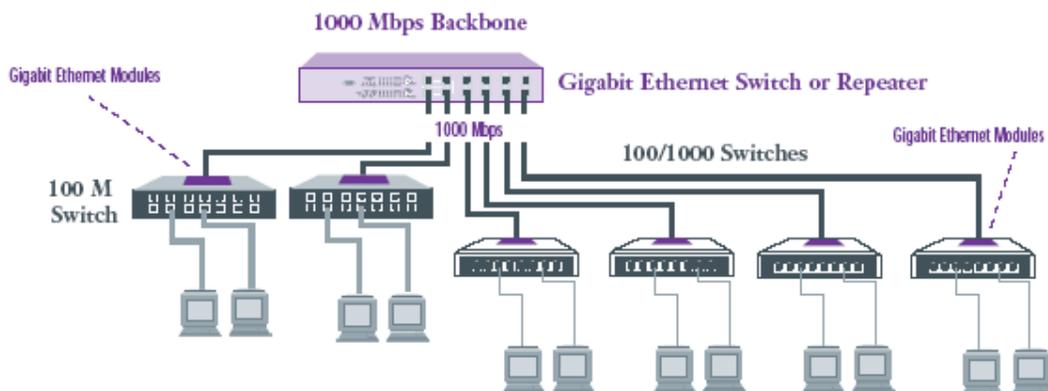


Figura 5. 26. Segmentos Fast Ethernet – después de la actualización

5.7.4 FASE No. 4: ACTUALIZACIÓN DE GRUPOS DE TRABAJO DE ALTO DESEMPEÑO

En las posteriores fases de la adopción de Gigabit Ethernet, Muchos de los equipos de escritorio conectados a Fast Ethernet, comienzan a sentir la necesidad de mayores anchos de banda; por lo tanto es necesario adquirir NICs Gigabit Ethernet que serán usadas para actualizar los computadores de escritorio de alto desempeño con conectividad Gigabit Ethernet. Los computadores de escritorio de alto desempeño son entonces conectados a switches Gigabit Ethernet.

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

Por lo tanto, cuando se lleve a cabo esta fase, se recomienda actualizar en primera medida los equipos utilizados por los grupos de investigación y los laboratorios y salas de informática que existen en la Universidad del Cauca.

La figura 5.27 ilustra la red antes de la actualización, mientras que la figura 5.28 ilustra la red después de la actualización hacia Gigabit Ethernet.

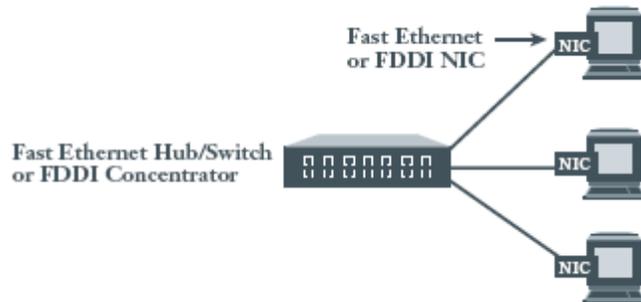


Figura 5. 27. Conexiones a grupos de trabajo de alto desempeño – antes de la actualización

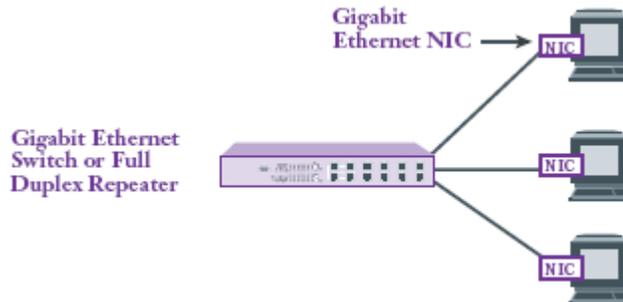


Figura 5. 28. Conexiones a grupos de trabajo de alto desempeño – después de la actualización

5.8 FASES DE MIGRACION HACIA 10 GIGABIT ETHERNET

Aunque el proceso de migración hacia 10 Gigabit Ethernet está proyectado a ejecutarse a largo plazo, es importante tenerlo presente hoy en día ya que la Universidad del Cauca debe proteger la inversión realizada en los diferentes dispositivos de Internetworking asegurando que los equipos Gigabit Ethernet que se adquieran en la actualidad sean escalables hacia la tecnología 10 Gigabit Ethernet en un futuro.

Se recomienda iniciar un proceso de migración hacia 10 Gigabit Ethernet cuando la última fase de la migración hacia Gigabit Ethernet, que contempla el acceso de los usuarios a la red a velocidades de 1 Gbps abarque un número considerable de equipos. En este caso la velocidad del backbone debe estar un factor por arriba de la velocidad de acceso a los usuarios, por lo que se espera que 10 GBE sea desplegado únicamente en los enlaces del backbone y en los enlaces hacia los servidores, con lo que sin duda alguna se conseguiría un desempeño óptimo.

A continuación se describen las fases que la Universidad del Cauca puede adoptar en el momento de realizar la migración hacia 10 GBE.

5.8.1 FASE No. 1: ACTUALIZACIÓN DE ENLACES SWITCH A SWITCH (BACKBONE)

En esta fase se debe realizar la adquisición de nuevos equipos que soporten la tecnología 10 Gigabit Ethernet para ser utilizados en el backbone, el cual comprende el switch principal del nivel de core ubicado en el IPET (INGCC5) y los equipos del nivel de distribución ubicados en los sectores de Ingenierías (INGCC1), Educación (EDUCC1), Medicina (MEDCC1), Santo Domingo (STOCC1), El Carmen (CARCC1) y Vicerrectoría de Investigaciones (VRICC1).

Para desplegar 10 Gigabit Ethernet a través del backbone, es necesario cambiar la fibra multimodo 62.5/125 μm a fibra multimodo optimizada para láser OM3 (en aquellos enlaces que no superan los 300m) o fibra monomodo 9/125 μm en los enlaces que aún no han sido actualizados.

De acuerdo a las propuestas de diseño planteadas en este Capítulo, para un posterior despliegue de 10 Gigabit Ethernet sería necesario implementar el backbone con equipos Cisco de la serie Catalyst 4500 o equipos Alcatel de la familia OmniSwitch 7000 en el nivel de distribución y equipos Cisco de la serie Catalyst 6500 o equipos Alcatel de la familia OmniSwitch 8800 para el nivel de core.

5.8.2 FASE No. 2: ACTUALIZACIÓN DE ENLACES SWITCH A SERVIDOR

En esta fase se debe realizar la actualización de las tarjetas de red 10/100/1000 Mbps hacia las tarjetas de red que soporten velocidades de 10 Gbps en todos los servidores de la Red de Datos. Esta fase se puede llegar a realizar utilizando el cableado de cobre existente, ya que actualmente existe un grupo de estudio formado por la IEEE conocido como 10GBASE-T que está desarrollando un estándar para la transmisión y recepción de 10 Gigabit Ethernet mediante cable de cobre UTP categoría 5 o mejor hasta 100 m. Se espera que este estándar este listo para cuando la Universidad del Cauca realice el proceso de migración hacia 10 GBE.

CAPITULO 5. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA REDES ETHERNET DE ALTA VELOCIDAD.

Debido a que estos servidores se encuentran conectados a los switches del nivel de core y de distribución, sería conveniente realizar esta etapa conjuntamente con la fase de actualización del backbone para lograr un mejor rendimiento y obtener mayores beneficios.

6. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA IPv6 SOBRE ETHERNET DE ALTA VELOCIDAD

La principal motivación que impulsa a la Universidad del Cauca a realizar un proceso de migración de su Red de Datos para implantar el nuevo protocolo IPv6 y las tecnologías de red Ethernet de alta velocidad, es la necesidad de manejar, experimentar y explorar tecnologías de última generación que permitan ofrecer nuevos y mejores servicios.

La migración de una tecnología a otra es justificable ya que dentro de la Universidad del Cauca hay proyectos, investigadores y recursos dedicados a la gestión de la tecnología, que de no actualizarse acabarían quedando ineludiblemente obsoletos.

Existen también fuerzas externas que empujan a intentar demostrar la viabilidad y la madurez de las nuevas tecnologías, las cuales se pueden ver como un factor a tener en cuenta para mejorar el rendimiento y la seguridad en las comunicaciones punto a punto.

Las ventajas que aportará el uso de las nuevas tecnologías en la Red de Datos de la Universidad del Cauca, a nivel de servicios y aplicaciones, previsiblemente irán más allá de los objetivos primarios, permitiendo obtener resultados que no podrían conseguirse de otro modo. El proceso de migración también permitirá evaluar los costes del cambio y ayudará a crear el conocimiento base a partir del cual se podrá desarrollar nuevos proyectos de implantación de estas tecnologías.

Durante la implantación de las nuevas tecnologías los sistemas deben ser afectados lo menos posible, con el fin de que la migración se pueda realizar de forma escalonada y según las necesidades que vayan surgiendo.

6.1 CONSIDERACIONES PARA LA MIGRACION HACIA IPv6

6.1.1 RETOS DE LA MIGRACION HACIA IPV6

En la actualidad Internet es básicamente una gran nube de IPv4. Cuando se empiece a implementar, existirán pequeñas islas de IPv6. Estas islas se comenzarán a hacer cada vez más grandes y la nube de IPv4 empezará a contraerse. Esto podría incrementar la migración o los problemas de coexistencia. Pero los desarrolladores están trabajando sobre este problema y han desarrollado aplicaciones que permitirán la coexistencia y

entender automáticamente cuando se está utilizando IPv4 o IPv6. Las aplicaciones tendrán implementadas pilas duales de IPv4 e IPv6 en la misma pila. Un host que soporte ambos protocolos puede comunicarse con nodos IPv4 o IPv6. Con una pila dual, las aplicaciones IPv4 funcionarán transparentemente con IPv6. Por ejemplo, si un servidor Web con IPv4 falla y el servidor de respaldo que utiliza IPv6 se encuentra en otra localidad, no habrá interrupción en el servicio.

La realidad es que las plataformas de administración de las redes de la actualidad no soportan IPv6. Los fabricantes de equipos podrán proveer funcionalidad libre, en forma de una actualización, asegurando que las versiones posteriores del software de administración de la red soportarán el nuevo esquema.

IPv6 es un estándar maduro y ha sido implementado exitosamente. Existen alrededor de 800 sitios en el mundo que corren IPv6 e interoperan con la nube de IPv4. La implementación comercial está empezando en Japón y la mayoría de los fabricantes de equipos han empezado a soportar el nuevo esquema. Esto es una buena señal para migrar pronto.

6.1.2 NECESIDAD DE MIGRACION HACIA IPv6 Y APOYO DE LA INDUSTRIA.

Internet continúa creciendo explosivamente, son cada vez más los dispositivos que se conectan a la red. La revolución inalámbrica es un hecho, y muchos dispositivos móviles están al acecho de ser parte de la superautopista de la información. Si un teléfono móvil estuviese enviando un correo electrónico y mientras está en movimiento se pierde la conexión, inmediatamente establece otra conexión para continuar enviando el mismo correo electrónico. El protocolo actual, el IPv4, no tiene la capacidad de soportar este tipo de movilidad. IPv6 tiene la capacidad de realizar esto transparentemente.

La red Internet está empezando a transportar tipos de datos que no fueron anticipados cuando fue diseñado en sus inicios. Hoy en día se conocen servicios como voz sobre IP, video bajo demanda, videoconferencia, datos en tiempo real, dispositivos controlados a control remoto y servicios de entretenimiento que jamás se hubiesen imaginado que se transportarán por la red. Algunos de estos servicios tales como los dispositivos controlados a control remoto, necesitan alta prioridad, asegurando que sus datos sean transmitidos sin retardo. Algunos de los servicios pueden soportar la pérdida de datos, mientras otros podrán requerir que cada bit llegue correctamente a su destino. Estos puntos son generalmente referidos como Calidad de Servicio (QoS).

El trabajo realizado en estándares y componentes relacionados a IPv6 tienen un gran avance y los fabricantes de equipos han acordado un número considerable de proyectos de prueba y desarrollo. La mayoría de los vendedores de equipos han

concertado agregar IPv6 a sus productos. Los fabricantes de equipos como DEC, Apple, Hewlett Packard, Novell, Microsoft, Compaq, 3Com, Cisco, Sun Microsystems, Nokia, Extreme Networks, entre muchos otros, están empezando a entregar computadores, servidores, routers, switches y otros dispositivos con IPv6. Muchas organizaciones están trabajando en manejadores de dispositivos (drivers) para el sistema operativo UNIX BSD, Linux, y otros. El servidor Windows 2003 de Microsoft contempla aplicaciones y componentes bajo IPv6; un navegador de Internet, un cliente FTP y un cliente Telnet. Fabricantes de software de red (Trumpet, Interpeak, Mentat,...) han desarrollado una gran variedad de soporte para IPv6 en aplicaciones de red y software de comunicaciones (FTP, navegador Mozilla, Apache Web server, Sendmail).

Otro gran esfuerzo es un prototipo de prueba de IPv6 puesto en operación llamado 6Bone, el cual enlaza más de 60 países en Norteamérica, Europa, Oceanía y Asia, incluyendo México, Cuba, Paraguay, Argentina, Colombia, Chile y Brasil.

6.1.3 BENEFICIOS DE LA MIGRACION HACIA IPv6

Muchas son las mejoras de IPv6 con respecto a IPv4, algunas de las ventajas y beneficios se listan a continuación:

- **Espacio de direcciones ampliado:** IPv6 incrementa el espacio de direcciones de 128 bits, contra 32 bits de IPv4. Esto supone un incremento de espacio de direcciones en un factor de 2^{96} . Un incremento en las direcciones permitirá que más de 340 sextillones de dispositivos tengan su propia dirección IP.
- **Soporte mejorado para extensiones y opciones:** Los cambios en la manera en que se codifican las opciones de la cabecera IP permiten un reenvío más eficiente, límites menos rigurosos y mayor flexibilidad para introducir nuevas opciones en el futuro. La implementación de extensiones de encabezado mejorará la forma en que los enrutadores procesan los paquetes.
- **Formato simplificado del encabezado:** El nuevo formato simplificado mejorará la eficiencia en el enrutamiento al procesarse más rápido.
- **Etiquetado del tráfico:** paquetes relacionados pueden ser tratados como flujos de tráfico, para lo cual, el nodo origen solicita tratamiento especial, como la calidad de servicio (QoS) no estándar o el servicio en tiempo real.
- **Autenticación y privacidad mejorada:** Medidas de seguridad son implementadas dentro del protocolo IPv6. Se especifican extensiones para utilizar autenticación, integridad de los datos y confidencialidad de los datos.

Con IPv4, el protocolo de seguridad IPSec es opcional. Con IPv6, IPSec es obligatorio. Por obligatorio se puede asumir que se puede asegurar la comunicación entre los dispositivos.

- **Autoconfiguración “plug and play”:** Autoconfiguración sin necesidad de servidores y facilidades de reconfiguración. Los dispositivos pueden configurar sus propias direcciones IPv6 basándose en la información que reciban del enrutador más próximo.
- **Mecanismos de movilidad más eficientes y robustos:** IP móvil soporta dispositivos móviles que cambian dinámicamente sus puntos de acceso a la red. Concretamente IPv6 permite a un host IPv6 dejar su subred de origen mientras mantiene transparentemente todas sus conexiones presentes y sigue siendo alcanzable por el resto de la red. Dado el auge de las redes inalámbricas tanto de telefonía celular como redes inalámbricas de área local (WLAN), la movilidad IP será un punto muy importante.
- **Aplicaciones en tiempo real:** IPv4 define una red pura orientada a datagramas y, como tal, no existe el concepto de reserva de recursos. Cada datagrama debe competir con los demás y el tiempo de tránsito en la red es muy variable y sujeto a congestión. Por ello, se necesita una extensión que posibilite el envío de tráfico de tiempo real, y así poder hacer frente a las nuevas demandas en este campo.
- **Tecnologías de ingeniería de tráfico:** IPv6 fue diseñado para permitir soporte a ingeniería de tráfico como diffserv o intserv (RSVP). Aunque no se tenga un estándar de ingeniería de tráfico, la especificación base de IPv6 tiene reservado un campo de 24 bits en la cabecera para esas tecnologías emergentes.
- **Multicast:** Multicast es obligatorio en IPv6, el cual era opcional en IPv4. Las especificaciones base de IPv6 por si mismas usan extensivamente multicast.

6.2 TRANSMISION DE PAQUETES IPV6 SOBRE REDES ETHERNET.

En esta parte del capítulo se especifica el formato de la trama para la transmisión de paquetes IPv6 y el método para formar direcciones IPv6 de enlace local y direcciones de autoconfiguración stateless sobre redes Ethernet.

También se especifica el contenido de la opción Dirección de la capa de Enlace Fuente/Destino utilizadas en los mensajes Solicitud de Router, Anuncio de Router, Solicitud de Vecino, Anuncio de Vecino y Redirección cuando estos son transmitidos sobre Ethernet.

6.2.1 UNIDAD DE TRANSMISIÓN MÁXIMA.

El tamaño de la MTU por defecto para los paquetes IPv6 sobre Ethernet es 1500 octetos. Este tamaño puede ser reducido por un mensaje de Anuncio de Router que contenga la opción MTU especificando una MTU menor, o por una configuración manual de cada nodo. Si una interfaz Ethernet recibe un mensaje de Anuncio de Router con la opción MTU especificando una MTU mayor que 1500, o mayor que el valor configurado manualmente, esa opción MTU puede ser registrada al sistema de gestión pero puede ser ignorada en otro caso.

6.2.2 FORMATO DE LA TRAMA.

Los paquetes IPv6 son transmitidos en tramas Ethernet estándares. La cabecera Ethernet contiene la dirección Ethernet de Fuente y Destino y el código de tipo Ethernet con el valor hexadecimal 86DD. El campo de datos contiene la cabecera IPv6 seguida por los propios datos, y probablemente de algunos octetos de relleno o alineación de tal forma que se alcance el tamaño mínimo de la trama Ethernet.

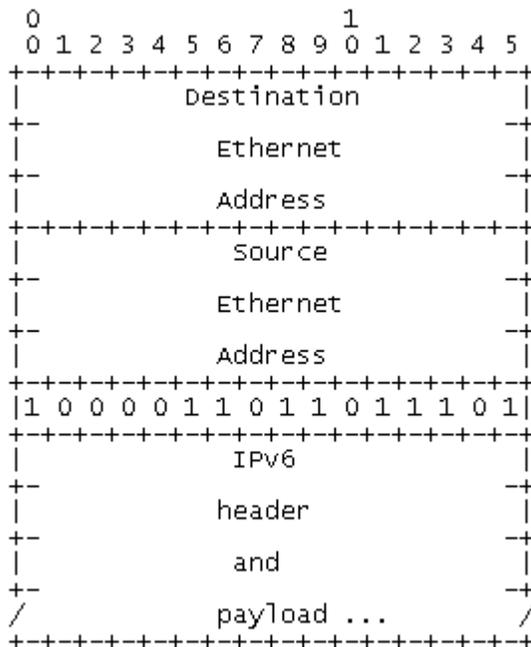


Figura 6. 1. Formato de la trama Ethernet

6.2.3 AUTOCONFIGURACIÓN STATELESS.

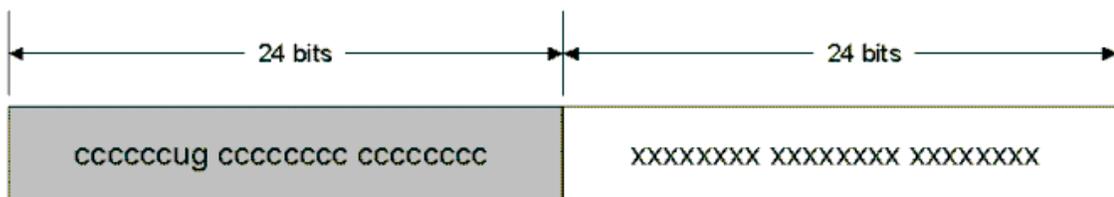
El Identificador de Interfaz, de una interfaz Ethernet, para la autoconfiguración stateless, se basa en el identificador EUI-64 derivado de la dirección MAC de 48 bits (IEEE 802).

6.2.3.1 IDENTIFICADORES DE INTERFAZ DE IPv6

Todas las direcciones que utilizan los prefijos comprendidos entre 001 y 111 deben utilizar también un identificador de interfaz de 64 bits que está derivado de la dirección EUI-64. La dirección EUI-64 de 64 bits fue definida por el Instituto de ingeniería eléctrica y electrónica (IEEE, *Institute of Electrical and Electronic Engineers*). Las direcciones EUI-64 se asignan a una tarjeta adaptadora de red o se derivan de direcciones IEEE 802.

DIRECCIONES IEEE 802

Los identificadores de interfaz tradicionales de los adaptadores de red utilizan una dirección de 48 bits denominada dirección IEEE 802. Consta de un Id. de compañía de 24 bits (también conocido como Id. del fabricante) y un Id. de extensión de 24 bits (también conocido como Id. de tarjeta). La combinación del Id. de compañía, que se asigna en exclusiva a cada fabricante de adaptadores de red, y el Id. de tarjeta, que se asigna en exclusiva a cada adaptador de red en el momento del montaje, genera una dirección exclusiva global de 48 bits. Esta dirección de 48 bits también se denomina dirección física, de hardware o de control de acceso a medios (MAC, *Media Access Control*). En la figura 6.2 se muestra la estructura de la dirección IEEE 802 de 48 bits.



Id. de organización administrado por IEEE Id. de extensión seleccionado por el fabricante

Figura 6. 2. Dirección IEEE 802 de 48 bits

Los bits definidos en la dirección IEEE 802 son:

Universal/Local (U/L): el bit situado junto al bit de orden inferior en el primer byte se utiliza para indicar si la dirección se administra universal o localmente. Si el bit U/L está establecido en el valor 0, IEEE ha administrado la dirección a través de la designación de un Id. de compañía. Si el bit U/L está establecido en el valor 1, la dirección se administra localmente. El administrador de la red ha suplantado la

CAPITULO 6. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA IPv6 SOBRE ETHERNET DE ALTA VELOCIDAD.

dirección del fabricante y ha especificado otra dirección. El bit U/L bit se designa mediante **u** en la figura 6.2.

Individual/Group (I/G) (Individual/Grupo): el bit de orden inferior del primer byte se utiliza para indicar si se trata de una dirección individual (unicast) o de grupo (multicast). Cuando está establecido en el valor 0, la dirección es unicast. Cuando está establecido en el valor 1, la dirección es multicast. El bit I/G se designa mediante **g** en la figura 6.2.

Para una dirección de adaptador de red 802.x típica, tanto el bit U/L como el bit I/G se establecen en el valor 0, que corresponde a una dirección MAC unicast administrada de forma universal.

IDENTIFICADORES DE INTERFAZ IEEE EUI-64

La dirección IEEE EUI-64 representa un nuevo estándar en el direccionamiento de interfaces de red. El Id. de la compañía también tiene 24 bits, pero el Id. de extensión es de 40 bits, lo que representa un espacio de direcciones mucho mayor para el fabricante de adaptadores de red. La dirección EUI-64 utiliza los bits U/L e I/G del mismo modo que la dirección IEEE 802. En la figura 6.3 se muestra la estructura de la dirección EUI-64.

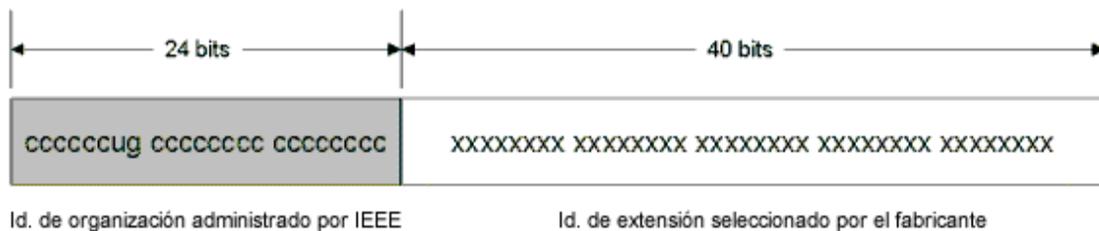


Figura 6. 3. Dirección EUI-64

ASIGNACION DE DIRECCIONES IEEE 802 A DIRECCIONES EUI-64

Para crear una dirección EUI-64 a partir de una dirección IEEE 802, los 16 bits de 11111111 11111110 (0xFFFE) se insertan en la dirección IEEE 802 entre el Id. de la compañía y el Id. de extensión, tal como se muestra en la figura 6.4.

CAPITULO 6. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA IPv6 SOBRE ETHERNET DE ALTA VELOCIDAD.

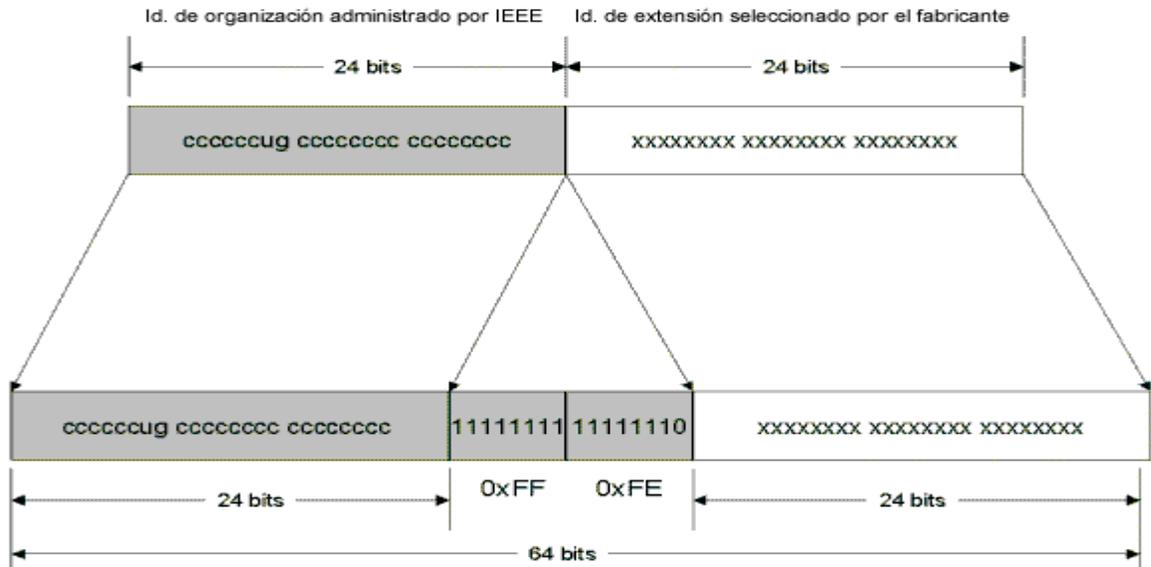


Figura 6. 4. Conversión de una dirección IEEE 802 en una dirección EUI-64

OBTENER IDENTIFICADORES DE INTERFAZ PARA DIRECCIONES IPV6

Para obtener el identificador de interfaz de 64 bits para direcciones unicast IPv6, el bit U/L de la dirección EUI-64 se complementa (si es 1, se establece en el valor 0 y si es 0, en el valor 1). En la figura 6.5 se muestra la conversión de una dirección EUI-64 unicast administrada universalmente.

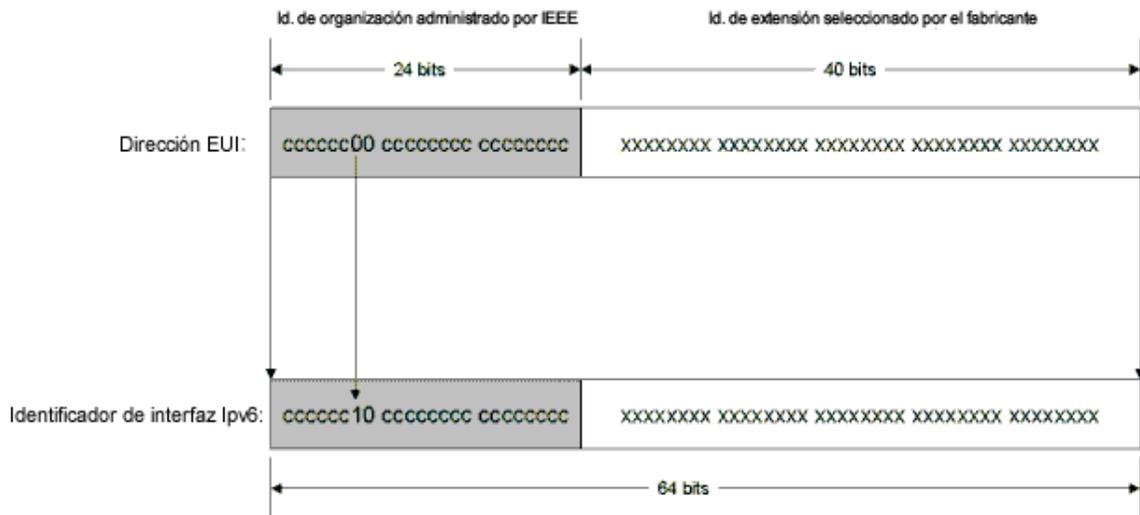


Figura 6. 5. Conversión de una dirección EUI-64 unicast administrada universalmente en un identificador de interfaz de IPv6

CAPITULO 6. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA IPv6 SOBRE ETHERNET DE ALTA VELOCIDAD.

Para obtener un identificador de interfaz de IPv6 a partir de una dirección IEEE 802, en primer lugar deberá asignar la dirección IEEE 802 a una dirección EUI-64 y, después, complementar el bit U/L. En la figura 6.6 se muestra el proceso de conversión de una dirección IEEE 802 unicast administrada universalmente.

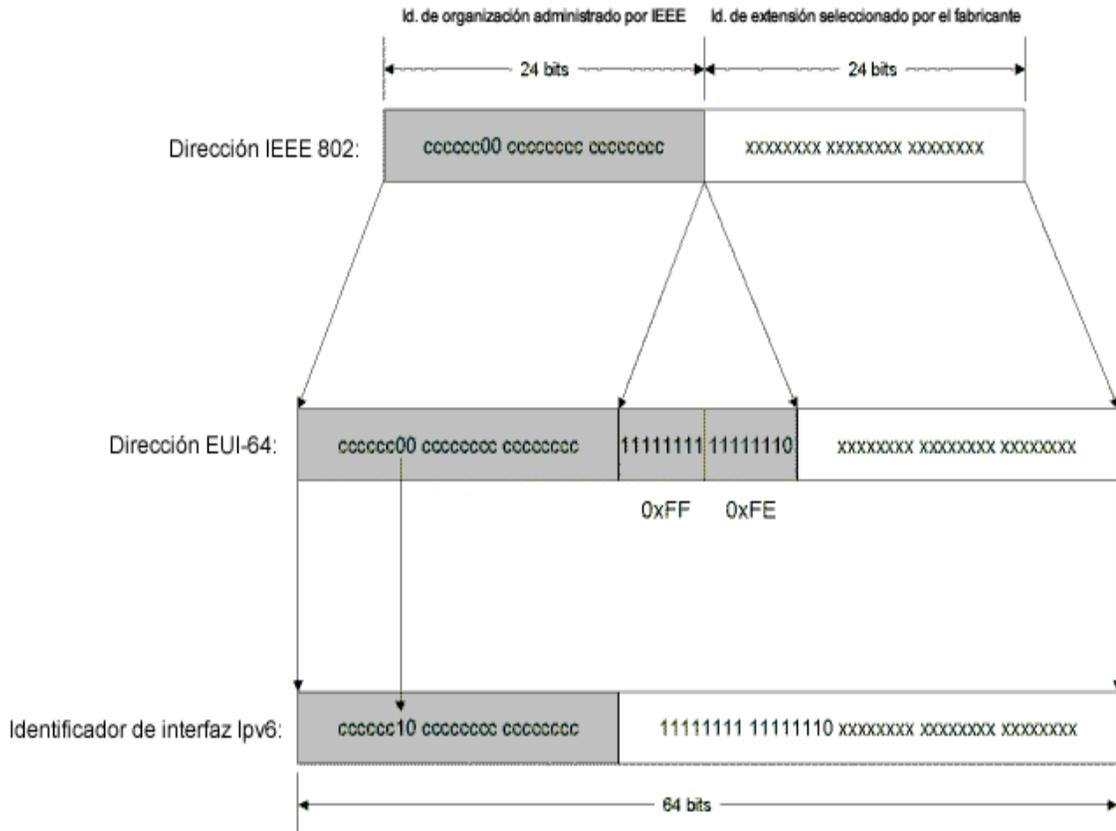


Figura 6. 6. Conversión de una dirección IEEE 802 unicast administrada universalmente en identificador de interfaz de IPv6

EJEMPLO DE CONVERSIÓN DE DIRECCIÓN IEEE 802

El Host A tiene la dirección MAC Ethernet 00-AA-00-3F-2A-1C. En primer lugar, se convierte al formato EUI-64 por la inserción de FF-FE entre el tercer y el cuarto bytes, lo que genera 00-AA-00-FF-FE-3F-2A-1C. A continuación, el bit U/L, que es el séptimo del primer byte, se complementa. El primer byte en forma binaria es 00000000. Cuando se complementa el séptimo bit, se convierte en 00000010 (0x02). El resultado final es 02-AA-00-FF-FE-3F-2A-1C que, cuando se convierte a la notación hexadecimal con puntos, pasa a ser el identificador de interfaz 2AA:FF:FE3F:2A1C. Como resultado, la dirección local de enlace que corresponde

CAPITULO 6. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA IPv6 SOBRE ETHERNET DE ALTA VELOCIDAD.

al adaptador de red con la dirección MAC 00-AA-00-3F-2A-1C es FE80::2AA:FF:FE3F:2A1C.

6.2.3.2 MAPEO DE DIRECCIONES UNICAST.

Las direcciones del nivel de enlace tienen el siguiente formato cuando el nivel de enlace es Ethernet.

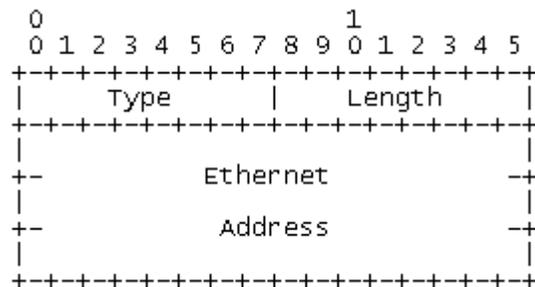


Figura 6. 7. Dirección de nivel de enlace IPv6

Los campos se describen a continuación:

- **Tipo:** 1 para la dirección de Nivel de Enlace de origen
2 para la dirección de Nivel de Enlace de destino
- **Longitud:** Longitud de la opción (incluyendo los campos tipo y longitud) en unidades de 8 bytes. Para Ethernet se fija en 1.
- **Dirección Ethernet:** los 48 bits de la dirección Ethernet 802.

La opción Dirección de Nivel de Enlace Origen contiene la dirección física del nodo que envía el paquete. Esta es utilizada en los paquetes Solicitud de Vecino, Solicitud de Router y Anuncio de Router.

La opción Dirección de Nivel de Enlace Destino contiene la dirección física del destino del paquete. Esta es utilizada en los paquetes de Anuncio de Vecino y Redirección.

Estas opciones deben ser ignoradas por otras opciones del protocolo ND.

6.2.3.3 MAPEO DE DIRECCIONES MULTICAST.

Cuando se envía paquetes multicast IPv6 a través de un enlace Ethernet, la dirección MAC de destino es 33-33-mm-mm-mm, donde mm-mm-mm-mm es una asignación directa de los últimos 32 bits de la dirección multicast IPv6, tal como se muestra en la figura 6.8.

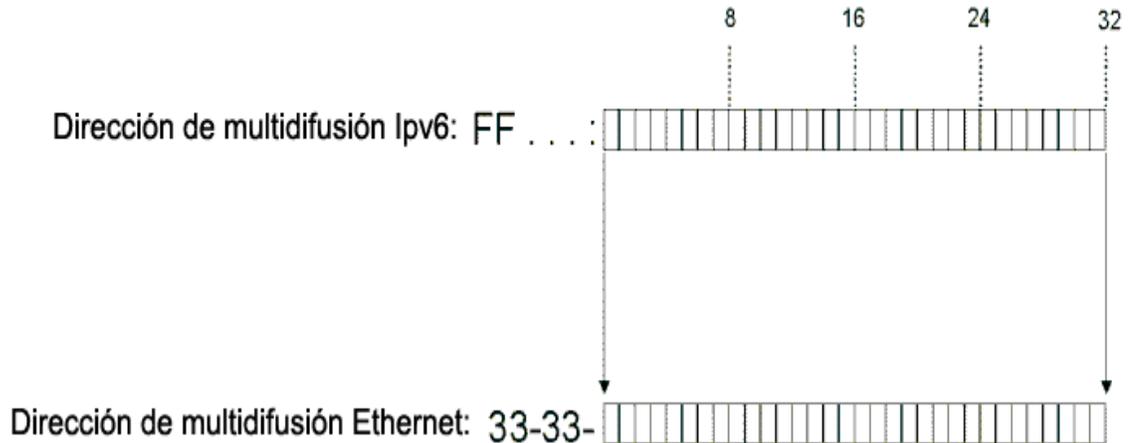


Figura 6. 8. Asignación de una dirección multicast IPv6 a una dirección MAC multicast Ethernet

Para recibir de un modo eficiente paquetes multicast IPv6 a través de un enlace Ethernet, los adaptadores de red Ethernet pueden almacenar otras direcciones MAC de interés en una tabla del adaptador de red. Si se recibe una trama Ethernet con una dirección MAC de interés, se pasa a las capas superiores para su procesamiento. Para todas las direcciones multicast que escucha el host, existe una entrada correspondiente en la tabla de direcciones MAC de interés.

Por ejemplo, un host con la dirección MAC Ethernet 00-AA-00-3F-2A-1C (dirección local de enlace FE80::2AA:FF:FE3F:2A1C) registra las siguientes direcciones MAC multicast con el adaptador Ethernet:

- La dirección 33-33-00-00-00-01, que corresponde a la dirección multicast de todos los nodos de ámbito local de enlace FF02::1.
- La dirección 33-33-FF-3F-2A-1C, que corresponde a la dirección de nodo solicitado FF02::1:FF3F:2A1C. Se debe recordar que la dirección de nodo solicitado se compone del prefijo FF02::1:FF00:0/104 y los últimos 24 bits de la dirección unicast IPv6.

Según sea necesario, se agregan o se quitan direcciones multicast adicionales de la tabla de direcciones de interés del adaptador de red Ethernet en el host que escucha.

6.3 PROPUESTA DE IMPLEMENTACION DE IPv6 PARA LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA

La migración hacia IPv6 debe verse como un proceso evolutivo que comenzará con la implantación del nuevo protocolo en la infraestructura de comunicaciones, para continuar luego con la modificación de aplicaciones, servicios y sistemas de gestión de la misma, acabando con la extensión del protocolo a la mayor parte de los dispositivos interconectados a la red de redes.

6.3.1 ARQUITECTURA DE LA NUEVA RED

Para introducir el nuevo protocolo de red se tiene que modificar la estructura y arquitectura de la infraestructura de comunicaciones. Esto realizándolo, tanto para el nivel de enlace, como para el nivel de red (niveles 2 y 3 del modelo de referencia OSI) y sin afectar a niveles superiores.

Una de las soluciones más deseables para el desarrollo de la nueva red IPv6, estriba en tener la posibilidad de acceder a los segmentos de red IPv6 desde cualquiera de los puntos de acceso de la red actual. Es así, porque hay que pensar que muchas estaciones de trabajo y sistemas de los que están funcionando en la red IPv4 tendrán que pasar a disponer de dirección IPv6, y por tanto, cuanto más sencillo sea acceder a la nueva red, menor será la inversión necesaria en coste y en tiempo.

Para ello, como la Red de la Universidad del Cauca está basada en tecnología Ethernet, caben dos soluciones técnicas:

1. **Red paralela IPv6:** La red IPv4 y la red IPv6 utilizan distintos segmentos de red. O lo que es lo mismo, la división de los dominios de broadcast (también llamados segmentos de red) mediante la técnica de etiquetado VLAN de las diferentes redes.
2. **Red de Pila Dual:** La red IPv4 y la red IPv6 conviven en los mismos segmentos de red. Lo que implica la compartición de la misma red física (y por tanto el mismo dominio de broadcast y la misma VLAN) entre todos los dispositivos de red, independientemente de que estén utilizando IPv4 o IPv6 a nivel de red.

6.3.1.1 RED PARALELA IPv6

Esta técnica consiste en separar los segmentos físicos de red por los que circularán los paquetes IPv6 de aquellos por los que circulan en la actualidad los paquetes IPv4. Esto implica que también los routers deben ser diferentes a los utilizados en la red IPv4, lo que, en general, supone un esfuerzo extra.

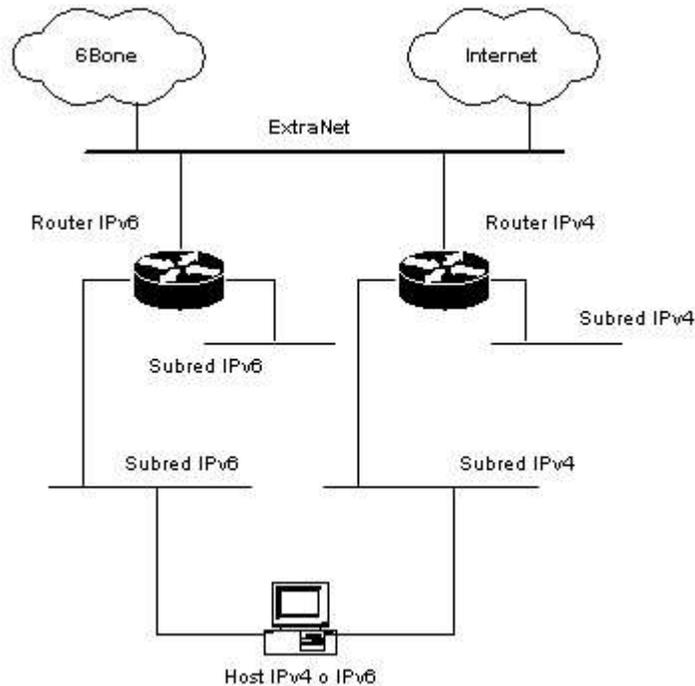


Figura 6. 9. Ejemplo de Red paralela IPv6

Esta solución es la más indicada en redes con altas exigencias de calidad y de estabilidad, ya que evita las posibles interferencias entre ambos protocolos de manera drástica. Hoy en día, gracias a la segmentación de redes Ethernet utilizando las técnicas de VLAN, la red paralela IPv6 puede no ser tan costosa en hardware, pero aún así, habría un alto coste de configuración, sobre todo si se considera necesario llevar las dos redes a los equipos finales de usuario.

6.3.1.2 RED CON PILA DUAL DE PROTOCOLOS

Esta técnica de la Pila Dual resulta ser la técnica más óptima de implementar, puesto que no requiere duplicar redes ni interfaces de red para que los sistemas accedan a IPv4 o IPv6. Sólo es necesario que los sistemas operativos de los equipos de escritorio y switches multinivel sean capaces de utilizar ambas pilas de protocolos en paralelo, distinguiendo el paquete en el momento de la recepción por medio de la cabecera de nivel de red y más concretamente a través del campo de versión de protocolo IP.

CAPITULO 6. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA IPv6 SOBRE ETHERNET DE ALTA VELOCIDAD.

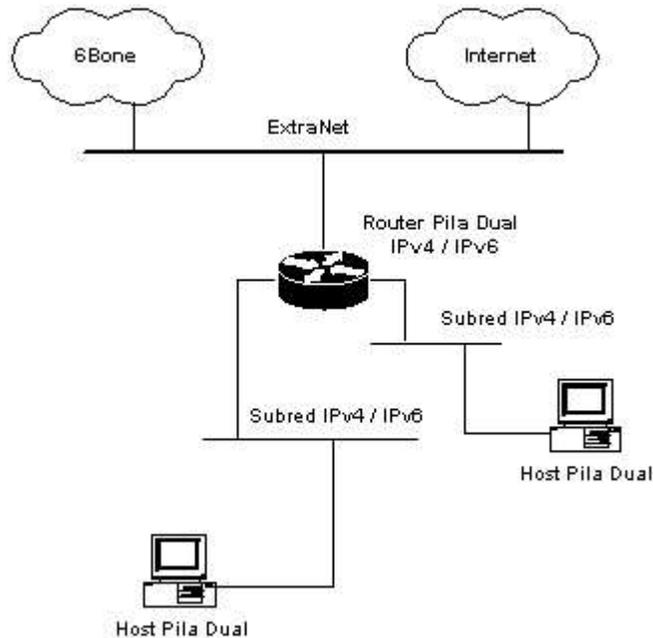


Figura 6. 10. Ejemplo de Red con Pila Dual

El problema principal de este método está en que ambas redes podrían llegar a interferir entre sí, sobre todo en los casos en que los recursos de red estén explotados al límite antes de introducir IPv6, o en los casos en que los switches multinivel implicados no tuviesen las capacidades necesarias para enrutar los paquetes de ambos niveles de red. Por lo tanto para tener un funcionamiento adecuado de la red al implementar el método de la Pila Dual es necesario contar con dispositivos de internetworking con un alto desempeño y altas tasas de conmutación multinivel.

6.3.1.3 SELECCIÓN DE LA ARQUITECTURA DE RED

La técnica de la Pila Dual se perfila como la solución técnica más sencilla de implementar para un entorno de Red como el de la Universidad del Cauca, en el que los potenciales usuarios de IPv6 pueden estar dispersos por todas las subredes del campus universitario.

También en el entorno de los servidores de red es la técnica más cómoda y sencilla de gestionar, puesto que permite reducir al máximo las tareas administrativas en la red y requiere una mínima inversión en hardware.

6.3.2 PLAN DE NUMERACION

La Red actual de la Universidad del Cauca tiene varios rangos de direcciones IPv4. En general, dispone de una parte de direccionamiento privado (direcciones IP que no

CAPITULO 6. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA IPv6 SOBRE ETHERNET DE ALTA VELOCIDAD.

se pueden enrutar hacia el exterior) y otra parte de direccionamiento público (direcciones IP que pueden salir al exterior y a las que se sabe cómo llegar desde el exterior).

El plan de numeración se encarga de realizar una asignación de direccionamiento nuevo a cada una de esas redes para así dotarlas de conectividad en IPv6. El plan de numeración también afectará a los routers que tendrán que anunciar los prefijos adecuados a cada red según la configuración especificada, así como configurar sus rutas para enrutar los paquetes en la intranet.

Conforme a lo especificado en el RFC 2471, “Plan de asignación de direcciones IPv6 para pruebas”, la UNAM por ser nodo del backbone del 6Bone ha distribuido su espacio de direcciones IPv6 a partir del prefijo tipo pTLA 3FFE:8070::/28 a comunidades autónomas en el mundo que utilizan la redUNAM IPv6 para pruebas, y dentro de este espacio ha asignado a UniCauca el bloque pNLA 3FFE:8070:1024::/48.

En la figura 6.11 se ilustra la estructura de las direcciones Globales Agregables asignadas a UniCauca.

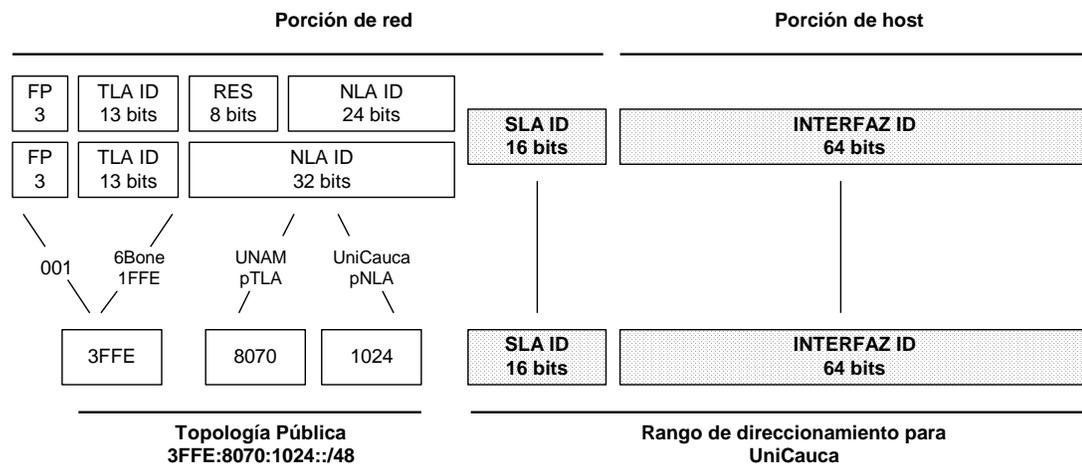


Figura 6. 11. Estructura de direccionamiento IPv6 para UniCauca

FP: 001; 3 bits

TLA ID: 1FFE (6bone); 13 bits

NLA ID: pTLA: 8070 (UNAM); 16 bits – pNLA:1024 (UniCauca); 16 bits

SLA ID: 16 bits

INT ID: 64 bits

CAPITULO 6. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA IPv6 SOBRE ETHERNET DE ALTA VELOCIDAD.

La Universidad del Cauca tiene capacidad para distribuir internamente diferentes rangos de direcciones IPv6 utilizando el campo SLA ID, el cual a su vez, al igual que se ha hecho con el campo NLA ID, se puede dividir en múltiples niveles.

6.3.2.1 ESTRUCTURA DE DIRECCIONAMIENTO IPv6 DE MULTIPLES NIVELES

En esta estructura de direccionamiento se asigna un prefijo /53 a cada sector y/o dependencia de la Universidad del Cauca. Por la tanto, se dispone de 2^5 o 32 subredes para sectores y/o dependencias (desde un /48 hasta un /53; 5 bits). De esta forma, cada sector o dependencia está en capacidad de direccionar y enrutar 2^{11} o 2048 sitios finales (desde un /53 hasta un /64; 11 bits). Cada sitio final está en la capacidad de asignar 2^{64} o 18,446,744,073,709,551,616 (1.84×10^{19}) direcciones IPv6 del tipo Global Agregable.

IPET	Subred 1	3FFE:8070:1024:1::/53
Ingenierías	Subred 2	3FFE:8070:1024:2::/53
Santo Domingo	Subred 3	3FFE:8070:1024:3::/53
El Carmen	Subred 4	3FFE:8070:1024:4::/53
Artes	Subred 5	3FFE:8070:1024:5::/53
Casa Rosada	Subred 6	3FFE:8070:1024:6::/53
Caja de Previsión	Subred 7	3FFE:8070:1024:7::/53
Archivo Histórico	Subred 8	3FFE:8070:1024:8::/53
Casa Caldas	Subred 9	3FFE:8070:1024:9::/53
VRI	Subred 10	3FFE:8070:1024:A::/53
Educación	Subred 11	3FFE:8070:1024:B::/53
Física y Química	Subred 12	3FFE:8070:1024:C::/53
CDU	Subred 13	3FFE:8070:1024:D::/53
Ciencias Agropecuarias	Subred 14	3FFE:8070:1024:E::/53
Medicina	Subred 15	3FFE:8070:1024:F::/53
Hospital	Subred 16	3FFE:8070:1024:10::/53
-----	-----	-----
Ultima Subred	Subred 31	3FFE:8070:1024:19::/53

Tabla 6. 1. Direccionamiento IPv6 de múltiples niveles

6.3.2.2 ESTRUCTURA DE DIRECCIONAMIENTO IPv6 DE UN UNICO NIVEL

En esta estructura de direccionamiento se asigna un prefijo /64 a la Universidad del Cauca. Se dispone así de 2^{16} o 65,536 subredes para UniCauca (desde un /48 hasta un /64; 16 bits). De esta forma, cada subred esta en capacidad de asignar 2^{64} o 18,446,744,073,709,551,616 (1.84×10^{19}) direcciones IPv6 del tipo Global Agregable.

CAPITULO 6. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA IPv6 SOBRE ETHERNET DE ALTA VELOCIDAD.

Subred 0	3FFE:8070:1024:0000::/64
Subred 1	3FFE:8070:1024:0001::/64
Subred 2	3FFE:8070:1024:0002::/64
-----	-----
Subred 65536	3FFE:8070:1024:FFFF::/64

Tabla 6. 2. Direccionamiento IPv6 de un único nivel

6.3.3 CONEXIÓN CON EL 6BONE

Actualmente, en el Laboratorio de Telecomunicaciones de la FIET se tiene habilitado el soporte para IPv6 a través de un nodo que funciona como enrutador y está conectado al 6bone, que es la red de pruebas para IPv6 que opera desde hace varios años, conectando redes IPv6, sobre el Internet IPv4 que se conoce, por lo cual se está en la capacidad de empezar a trabajar con esta tecnología desde ahora.

La inexistencia de una infraestructura de enrutamiento IPv6, hace que sea necesario el uso de túneles IPv6 en IPv4 para transportar paquetes IPv6 a través de topologías solo IPv4, utilizando para ello la infraestructura de enrutamiento IPv4. La colaboración de la UNAM, para el acceso al 6Bone de UniCauca, permite establecer un túnel IPv6 en IPv4 punto a punto entre estas dos instituciones.

Los túneles configurados son de sentido único, es decir, que para establecer una conexión Full-Duplex es necesario establecer túneles configurados en ambos sentidos. Por tal razón, la UNAM debe configurar un túnel simétrico al configurado por UniCauca.

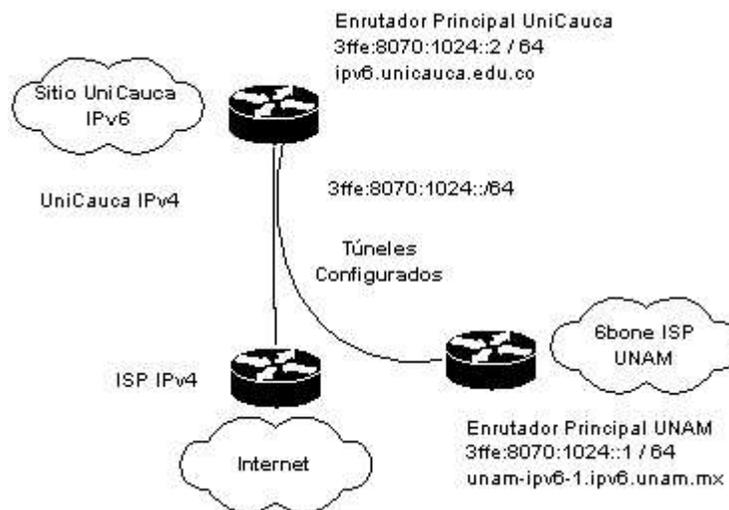


Figura 6. 12. Topología de túneles estáticos entre los sitios UniCauca IPv6 y UNAM IPv6

6.3.3.1 SELECCIÓN DEL ROUTER DE FRONTERA

Como se mencionó anteriormente, el router de frontera del sitio UniCauca IPv6 es un PC en el cual se tiene configurado un túnel IPv6 en IPv4 con la UNAM para realizar la conexión al 6Bone; sin embargo este nodo no posee las características adecuadas de desempeño y disponibilidad que se necesitarán cuando el protocolo IPv6 sea desplegado en toda la Red de la Universidad. Es por esto que se hace indispensable contar con un dispositivo de internetworking de alto rendimiento que permita la implementación de la Pila Dual de protocolos IP para manejar tanto IPv4 como IPv6.

En la actualidad muchas empresas dedicadas al desarrollo de dispositivos de internetworking como Cisco, Alcatel, entre otras ya cuentan con equipos que soportan los dos protocolos IPv6 e IPv4 y se pueden configurar para funcionar ya sea con un solo protocolo o con los dos (Pila Dual). Dentro de los equipos especificados en el Capítulo 5, los switches de Core propuestos cumplen con todos los requisitos necesarios para ser configurados en modo túnel y con la capacidad de brindar el soporte de la Pila Dual de protocolos IP. Dichos dispositivos son los siguientes:

- Cisco Catalyst 4500
- Cisco Catalyst 6500
- Alcatel OmniSwitch 7800
- Alcatel OmniSwitch 8800

6.3.3.2 CONEXIÓN DEL ROUTER DE FRONTERA AL 6BONE

Cuando se este listo para desplegar IPv6 en la Red de la Universidad, la conexión al “6bone ISP” será realizada a través de su ISP IPv4. Se configura el router de frontera para que se una al ISP IPv4 y para correr la pila dual con un túnel al “6bone ISP”. La dirección IPv4 del router de frontera cambiará según la dirección que el proveedor ISP IPv4 le asigne.

Usando la dirección IPv4 del “6bone ISP”, se configura el router de frontera para ejecutar la pila dual con un túnel que se conecta al 6bone.

6.3.4 TOPOLOGIA FINAL DE LA ARQUITECTURA DE LA RED IPv6

La topología final de la Intranet de la Universidad del Cauca se puede observar en la figura 6.13 donde se muestra la Red de Datos conectada al 6Bone utilizando un túnel manualmente configurado con la UNAM a través del proveedor de servicio de Internet IPv4. El router de frontera es el encargado de enrutar el tráfico IPv6 a través del túnel mencionado anteriormente.

CAPITULO 6. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA IPv6 SOBRE ETHERNET DE ALTA VELOCIDAD.

En la figura 6.13 también se pueden observar los siguientes elementos:

- **Switch Multinivel con Pila Dual:** En éste tipo de switches se puede habilitar el soporte tanto para IPv4 como para IPv6 y serán ubicados en los niveles de DISTRIBUCION y ACCESO.
- **Host IPv4:** Son equipos que no han sido actualizados o que no pueden ser actualizados ya que su S.O. no provee el soporte para IPv6.
- **Host IPv4 / IPv6:** Son equipos que tienen implementado la Pila Dual de protocolos.
- **Host IPv6:** Son equipos cuyo S.O. tiene la capacidad de soportar IPv6 nativo.

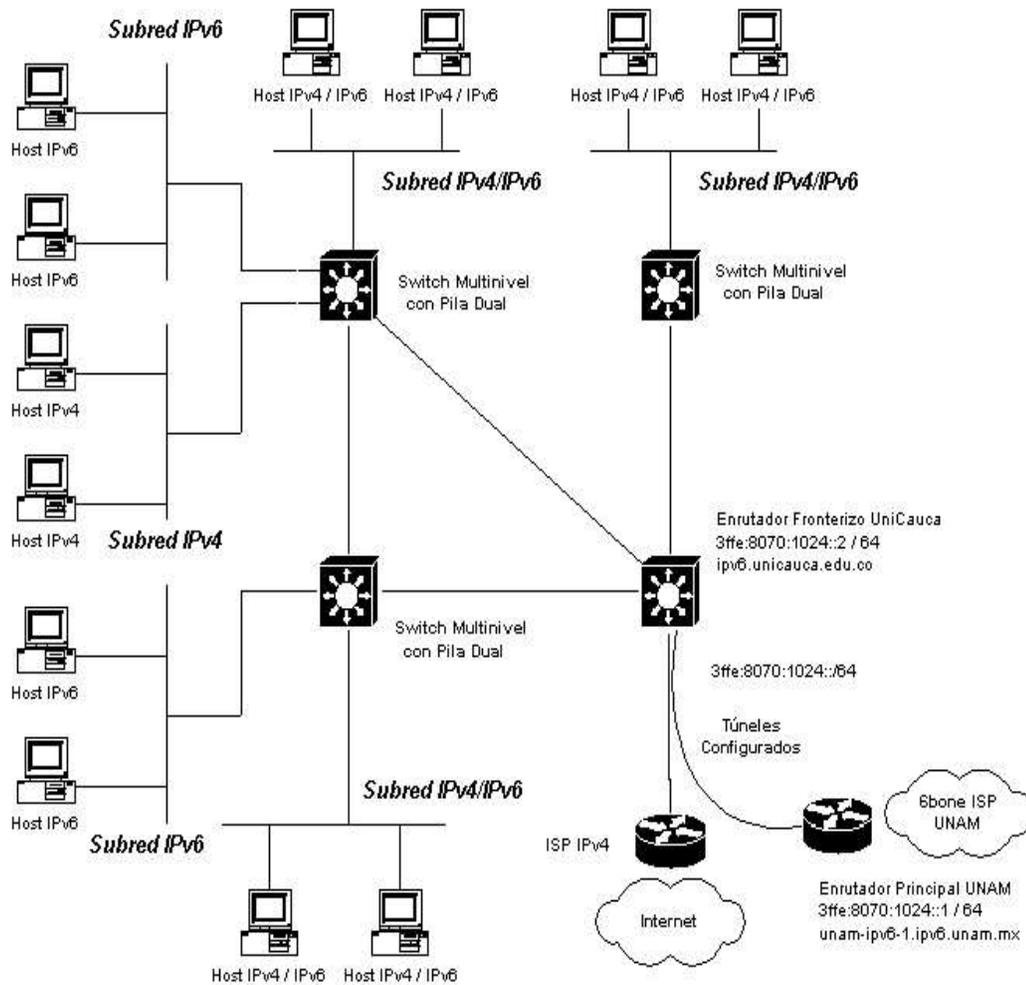


Figura 6. 13. Topología final de la arquitectura de red IPv6

6.3.5 PROTOCOLOS DE NIVEL SUPERIOR

Los cambios necesarios en los protocolos de nivel superior son poco relevantes, porque el servicio de datagramas es en sustancia idéntico, y sobre todo conciernen a las aplicaciones que usan directamente direcciones IP. Las aplicaciones deberán ser capaces de gestionar direcciones de 128 bits y aconsejablemente usar nombres DNS en vez de direcciones, para que el protocolo IP sea transparente, especialmente en previsión de una coexistencia por mucho tiempo de las versiones 4 y 6.

A continuación se tratarán los cambios que hay que considerar en TCP, UDP, DNS, Telnet y HTTP.

6.3.5.1 TCP/UDP

El protocolo IPv6 ya no implementa la gestión de errores, para reducir la carga de los routers. La gestión de errores es delegada a los protocolos de nivel de transporte, que poseen mecanismos de fiabilidad. Por eso los protocolos TCP y UDP calculan un checksum que incluye datos del paquete IP, como las direcciones fuente y destino. El RFC 2460 define el formato de la pseudocabecera a usarse con la nueva versión del protocolo. Además, con IPv6 el cálculo del checksum en el protocolo UDP es obligatorio y los datagramas que llevan el campo a cero deben ser rechazados y generar un error.

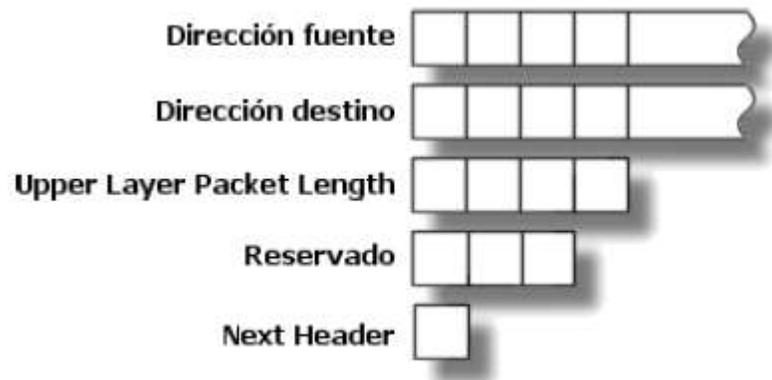


Figura 4. 1. Formato de la pseudocabecera

El campo de 4 bytes Upper Layer Packet Length (longitud paquete de nivel superior) indica la longitud del paquete TCP o UDP incluso la cabecera. El campo de tres bytes reservados es puesto a cero y el valor del campo Next Header se saca del paquete IP y es uno de los valores admitidos para la cabecera IPv6; en el caso del TCP es 6, y en el caso del UDP es 17.

6.3.5.2 DNS

Una infraestructura DNS será necesaria para la coexistencia exitosa de ambos protocolos, debido al prevaleciente uso de nombres en vez de números para referirse a los recursos de la red. Actualizar la infraestructura del DNS consiste en alimentar a los servidores DNS con registros para poder soportar resoluciones nombre a direcciones y direcciones a nombres IPv6. Después de que las direcciones son obtenidas a través de la consulta a un DNS, el nodo origen debe seleccionar que direcciones serán utilizadas para la comunicación.

En el RFC 1886 se describen varias mejoras realizadas en el Sistema de nombres de dominio (DNS) para IPv6, las cuales incluyen las novedades siguientes:

- Registro de recursos de direcciones de host (AAAA).
- Dominio IP6.INT para consultas inversas

REGISTRO DE RECURSOS DE DIRECCIONES DE HOST (AAAA)

Se utiliza un nuevo tipo de registro de recursos DNS, AAAA (denominado "cuatro as"), para resolver un nombre de dominio completo en una dirección IPv6. Es comparable al registro de recursos de direcciones de host (A) que se utiliza con IPv4. El tipo de registro de recursos se denomina AAAA (valor de tipo 28) porque las direcciones IPv6 de 128 bits son cuatro veces mayores que las direcciones IPv4 de 32 bits. A continuación, se muestra un ejemplo de un registro de recursos AAAA:

host1.unicauca.edu.co IN AAAA FEC0::2AA:FF:FE3F:2A1C

Un host debe especificar una consulta AAAA o una consulta general para un nombre de host específico para recibir datos de resolución de direcciones IPv6 en las secciones de respuesta de las consultas DNS.

EL DOMINIO IP6.INT

El dominio IP6.INT se ha creado para las consultas IPv6 inversas. Las consultas inversas, también denominadas consultas de puntero, determinan un nombre de host basado en la dirección IP. Para crear el espacio de nombres para las consultas inversas, cada dígito hexadecimal de la dirección IPv6 de 32 dígitos completamente expresada se convierte en un nivel independiente en el orden opuesto en la jerarquía de dominios inversa.

Por ejemplo, el nombre de dominio de búsqueda inversa para la dirección FEC0::2AA:FF:FE3F:2A1C (que de forma completa se expresa como FEC0:0000:0000:0000:02AA:00FF:FE3F:2A1C) es:

C.1.A.2.F.3.E.F.F.F.0.0.A.A.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.C.E.F.IP6.INT.

6.3.5.3 TELNET

Telnet es uno de los servicios más antiguos de Internet, y se utiliza para conectarse con un equipo remoto a través de la red, de forma que el ordenador cliente se comporta como un terminal conectado con el ordenador remoto. El Telnet usa el protocolo de transporte TCP, puerto 23, y no necesita ningún cambio para ser usado con el IPv6.

6.3.5.4 FTP

El protocolo FTP permite enviar ficheros entre dos máquinas conectadas por medio de la red.

Los servidores y los clientes deberán gestionar las direcciones IPv4/IPv6 y las consultas DNS de ambos tipos. Además, dado que en unas ordenes FTP, la PASV que permite al cliente y al servidor de cambiar sus papeles, y la PORT que indica el puerto a utilizar para la transferencia de datos, y permitir entonces transferir varios ficheros a la vez, incluyen en su sintaxis la dirección IPv4 del host, han sido definidas dos ordenes adicionales, EPSV y EPRT que permiten usar tanto las direcciones IPv4 como las IPv6.

6.3.5.5 HTTP

El protocolo HTTP es probablemente el servicio más popular de Internet, detrás del correo electrónico. Permite transmitir hipertextos, documentos que incluyen imágenes, sonidos y otros recursos multimediales. Los servidores como los clientes deberán gestionar correctamente respuestas de los servidores DNS IPv4/IPv6 para traducir las direcciones de las webs proporcionadas por el usuario.

Unas implementaciones permiten también de introducir direcciones IPv6 literales, de la forma `http://[4321::1:2:3:4:567:89ab]`

Las principales implementaciones comerciales tanto de servidores web (Apache, IIS, WebSphere), como de clientes (Internet Explorer, Mozilla, Safari) ya están listas para la nueva versión del protocolo.

6.3.5.6 GESTION DE RED

Las implementaciones actuales de Pila Dual proveen soluciones para la gestión de la Red permitiendo que aplicaciones tales como TFTP, Ping, Telnet, Traceroute se puedan correr sobre los protocolos IPv4 e IPv6.

La descarga y subida de archivos TFTP puede ser usada para salvar la configuración de los dispositivos de internetworking en un servidor TFTP IPv6.

El comando Ping puede aceptar como argumento una dirección de destino IPv6 o un nombre de host IPv6 y enviar un mensaje “ICMPv6 echo request” hacia el destino especificado. Los mensajes “ICMPv6 echo reply” enviados desde el destino son desplegados en consola.

Los servidores y clientes Telnet soportan conexiones IPv6 para poder usar Telnet para acceder a un dispositivo de internetworking o iniciar conexiones Telnet desde dicho dispositivo.

El comando Traceroute puede aceptar como argumento una dirección de destino IPv6 o un nombre de host IPv6 y generar tráfico IPv6 para reportar cada salto IPv6 realizado para alcanzar la dirección de destino.

La Gestión de Red IPv6 es soportada por una serie de RFC’s que especifican las MIB’s para el protocolo IPv6. Los dispositivos de internetworking propuestos en el diseño soportan dichas MIB’s, así como también SSH sobre IPv6 y SNMP sobre IPv6.

6.4 CONFIGURACION DE LOS HOSTS PARA HABILITAR EL SOPORTE IPv6

6.4.1 CONFIGURACION DE EQUIPOS CON SISTEMAS OPERATIVOS WINDOWS

En general, las plataformas de Microsoft disponen de un buen soporte para IPv6. A partir de las versiones de los sistemas operativos Windows XP y Windows 2003 Server el stack de protocolos IPv6 viene preinstalado y su configuración es muy sencilla.¹

6.4.1.1 CONFIGURACION DEL PROTOCOLO IPv6 EN WINDOWS 2000

El S.O. Windows 2000 no tiene preinstalado el stack de protocolos IPv6, así que es necesario habilitar el soporte IPv6 utilizando las extensiones “Microsoft IPv6 Technology Preview for Windows 2000”.

Para tener soporte IPv6 en Windows 2000 se recomienda hacer lo siguiente:

- Se puede utilizar la interfaz gráfica de Windows para verificar el S.O, su versión y el nivel de Service Pack (SP) instalado. Para esto, se selecciona

¹ En la página <http://www.microsoft.com/ipv6> de Microsoft, aparece todo el soporte de la empresa al protocolo IPv6 en sus sistemas operativos.

Propiedades dando click derecho en el icono “Mi PC” del Escritorio, y luego, en la pestaña **General** de las Propiedades del Sistema, se lee la información que se muestra debajo del ítem Sistema.

- Dependiendo del nivel de S.P instalado, se procede según corresponda: Windows 2000 con nivel de S.P 1, 2, 3 o 4.

INSTALACIÓN DEL SOPORTE IPv6 EN WINDOWS 2000

- Descargar el archivo *tpipv6-001205.exe* desde:
<http://msdn.microsoft.com/downloads/sdks/platform/download.asp>
- Ejecutar el archivo *tpipv6-001205.exe* y extraer su contenido en una carpeta local (Ejemplo: C:\IPv6TP).
- Ejecutar desde C:\IPv6TP, utilizando el interprete de comandos de Windows, el comando *setup.exe -x*. Después se debe extraer los archivos a una subcarpeta en la carpeta actual (Ejemplo: C:\IPv6TP\ipv6).
- Desde C:\IPv6TP\ipv6, se debe acceder al archivo *hotfix.inf* utilizando un editor de texto.
- En la sección [Versión] del archivo *hotfix.inf*, se debe modificar la línea NtServicePackVersion según corresponda y guardar los cambios:

	SP1	SP2	SP3	SP4
NtServicePackVersion	256	512	768	1024

- Desde C:\IPv6TP\ipv6, ejecutar el archivo *hotfix.exe*. Probablemente en este punto el S.O. se reinicie.

HABILITACIÓN DEL SOPORTE IPv6 EN WINDOWS 2000

- Desde el Escritorio, dando click derecho en el icono “Entorno de Red”, se selecciona **Propiedades**. Nuevamente dando click derecho sobre el dispositivo de red en el que se quiere habilitar IPv6, se da click en **Propiedades**.
- Haciendo click sobre **Instalar**, se selecciona **Protocolo** y **Agregar**. Ahora se selecciona “Microsoft IPv6 Protocol” y luego OK.
- Para probar que el stack de protocolos IPv6 ha sido instalado y habilitado correctamente, se ejecuta en una consola de Windows el comando *ipv6 if*, el cual muestra la configuración y las direcciones IPv6 autoconfiguradas para cada interfaz de red existente.

6.4.1.2 CONFIGURACION DEL PROTOCOLO IPv6 EN WINDOWS XP

En Windows XP con nivel S.P 1 o posterior, IPv6 ya está instalado, pero es preciso habilitarlo. Para ello es necesario ejecutar en la consola de Windows con privilegios de administrador, el siguiente comando:

```
prompt > ipv6 install
```

Aparecerá un mensaje indicando que se ha configurado correctamente.

También se puede utilizar la interfaz gráfica, seleccionando **Propiedades** sobre la interfaz LAN en la que se desea habilitar IPv6. A continuación se selecciona **Instalar – Protocolo – Ipv6**.

Para comprobar que ha sido correctamente instalado, se puede usar el siguiente comando:

```
prompt > ipv6 if
```

Se mostrará la configuración y las direcciones IPv6 adquiridas (auto-configuradas) para cada interfaz de red existente.

Windows XP incorpora la versión 6 del Internet Explorer, adaptada para navegar en webs IPv6 (e IPv4). Existen otros comandos como “tracert6”, “telnet6” y “ftp”.

6.4.1.3 CONFIGURACION DEL PROTOCOLO IPv6 EN WINDOWS 2003 SERVER

En Windows 2003 Server, IPv6 ya está instalado, pero es preciso habilitarlo. Para ello es necesario ejecutar en la consola de Windows con privilegios de administrador, el siguiente comando:

```
prompt > netsh interface ipv6 install
```

Aparecerá un mensaje indicando que se ha configurado correctamente.

También se puede utilizar la interfaz gráfica, seleccionando **Propiedades** sobre la interfaz LAN en la que se desea habilitar IPv6. A continuación se selecciona **instalar – protocolo – Ipv6**.

Para comprobar que ha sido correctamente instalado, se puede usar el siguiente comando:

CAPITULO 6. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA IPv6 SOBRE ETHERNET DE ALTA VELOCIDAD.

```
prompt > netsh interface ipv6 show address
```

Se mostrará la configuración y las direcciones IPv6 adquiridas (auto-configuradas) para cada interfaz de red existente.

Windows 2003 incorpora la versión 6 del Internet Explorer, adaptada para navegar en webs IPv6 (e IPv4). Algunos comandos como “tracert”, “telnet”, y “ftp”, han sido adaptados para utilizar IPv6 por defecto, salvo que se indique “-4” (para IPv4) o si no existe dirección IPv6 de destino (caso en el que se usa por defecto la IPv4 correspondiente).

6.4.1.4 ASIGNACION DE DIRECCIONES IPv6 A UNA INTERFAZ DE RED

Al ejecutar en la consola de Windows el comando *ipv6 if* se obtiene la siguiente información:

```
C:\>ipv6 if
Interface 5 (site 1): Conexión de Area local 2
cable unplugged
uses Neighbor Discovery
link-level address: 00-03-ce-89-2f-cb
  preferred address fe80::203:ceff:fe89:2fcb, infinite/infinite
  multicast address ff02::1, 1 refs, not reportable
  multicast address ff02::1:ff89:2fcb, 1 refs, last reporter
link MTU 1500 (true link MTU 1500)
current hop limit 128
reachable time 28500ms (base 30000ms)
retransmission interval 1000ms
DAD transmits 1

Interface 4 (site 1): Conexión de Area local
uses Neighbor Discovery
link-level address: 00-b0-d0-d9-9d-d7
  preferred address 3ffe:8070:1024:1:2b0:d0ff:fed9:9dd7, 2591998s/604798s (addrconf)
  preferred address fe80::2b0:d0ff:fed9:9dd7, infinite/infinite
  multicast address ff02::1, 1 refs, not reportable
  multicast address ff02::1:ffd9:9dd7, 2 refs, last reporter
link MTU 1500 (true link MTU 1500)
current hop limit 64
reachable time 23000ms (base 30000ms)
retransmission interval 1000ms
DAD transmits 1
```

CAPITULO 6. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA IPv6 SOBRE ETHERNET DE ALTA VELOCIDAD.

Interface 3 (site 1): 6-over-4 Virtual Interface
uses Neighbor Discovery
link-level address: 172.16.41.105
 preferred address fe80::ac10:2969, infinite/infinite
 multicast address ff02::1, 1 refs, not reportable
 multicast address ff02::1:ff10:2969, 1 refs, last reporter
link MTU 1280 (true link MTU 65515)
current hop limit 128
reachable time 17500ms (base 30000ms)
retransmission interval 1000ms
DAD transmits 1

Interface 2 (site 0): Tunnel Pseudo-Interface
does not use Neighbor Discovery
link-level address: 0.0.0.0
 preferred address ::172.16.41.105, infinite/infinite
link MTU 1280 (true link MTU 65515)
current hop limit 128
reachable time 0ms (base 0ms)
retransmission interval 0ms
DAD transmits 0

Interface 1 (site 0): Loopback Pseudo-Interface
does not use Neighbor Discovery
link-level address:
 preferred address ::1, infinite/infinite
link MTU 1500 (true link MTU 1500)
current hop limit 1
reachable time 0ms (base 0ms)
retransmission interval 0ms
DAD transmits 0

En las interfaces se pueden identificar los siguientes tipos de direcciones IPv6:

- **Dirección Unicast Global Agregable:** La interfaz 4 tiene asignada la dirección *3ffe:8070:1024:1:2b0:d0ff:fed9:9dd7*, la cual se forma a partir del prefijo *3ffe:8070:1024:1::/64* anunciado por el router del segmento y el Identificador de Interfaz. Para esta configuración se utiliza el mecanismo de autoconfiguración sin control de estado.
- **Dirección de Enlace Local:** Este tipo de direcciones son las que comienzan con el prefijo FE80/10. Para la interfaz 4 se tiene *fe80::2b0:d0ff:fed9:9dd7*, la cual es el resultado de concatenar el prefijo y el token que se obtiene al aplicar al Identificador de Interfaz (dirección Ethernet) de la tarjeta de red el formato EUI-64.

- **Direcciones de Multicast:** En las interfaces se configuran las siguientes direcciones de Multicast:
 - ✓ **ff02::1** - dirección multicast para todos los nodos del ámbito local de enlace
 - ✓ **ff02::1:ffd9:9dd7** – dirección de nodo solicitado para la interfaz 4, la cual se compone del prefijo **ff02::1:ff00:0/104** y los últimos 24 bits de la dirección unicast IPv6 (Para la interfaz 4 corresponde el valor **d9:9dd7**).

6.4.1.5 PRUEBA DE CONECTIVIDAD IPv6

Se puede comprobar la conectividad de los equipos con el 6Bone utilizando el comando **ping6**. A continuación se muestran dos ejemplos en donde se realiza un ping6 al enrutador de UniCauca y de la UNAM. También se puede observar los tiempos de respuesta empleado por cada paquete.

```
C:>ping6 3ffe:8070:1024::2 //ping6 al enrutador de UniCauca

Pinging 3ffe:8070:1024::2 with 32 bytes of data:

Reply from 3ffe:8070:1024::2: bytes=32 time<1ms

C:>ping6 3ffe:8070:1024::1 //ping6 al enrutador de la UNAM

Pinging 3ffe:8070:1024::1 with 32 bytes of data:

Reply from 3ffe:8070:1024::1: bytes=32 time=156ms
Reply from 3ffe:8070:1024::1: bytes=32 time=146ms
Reply from 3ffe:8070:1024::1: bytes=32 time=156ms
Reply from 3ffe:8070:1024::1: bytes=32 time=158ms
```

6.4.2 CONFIGURACION DE EQUIPOS CON SISTEMAS OPERATIVOS LINUX (RED HAT Y FEDORA)

6.4.2.1 CONFIGURACION DEL PROTOCOLO IPv6 EN RED HAT

SOPORTE IPv6 EN RH LINUX

Red Hat Linux soporta IPv6 a partir de su versión 7.1, y se implementa utilizando el módulo IPv6 que se incorpora de manera dinámica al kernel de Linux.

CAPITULO 6. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA IPv6 SOBRE ETHERNET DE ALTA VELOCIDAD.

Linux, implementa IPv6 como un módulo del kernel a partir de las versiones 2.2.x y 2.4.x, por que normalmente se instala el módulo IPv6 y se carga de manera automática durante el inicio del sistema.

Estos son los pasos que permiten habilitar el módulo IPv6 en RH Linux:

- **Examinar el soporte IPv6 en el kernel de Linux:** Para asegurarse que el kernel que se está corriendo soporte IPv6, se comprueba que exista la entrada `/proc/net/ipv6` en el sistema de archivos `/proc`.
- **Cargar el módulo IPv6 en el kernel de Linux:** En caso de que la entrada `/proc/net/ipv6` no exista, se carga el módulo IPv6 utilizando el comando `modprobe ipv6`. Si esto es exitoso, el módulo IPv6 será instalado en pantalla al ejecutar el comando `lsmod`.
- **Cargar el módulo IPv6 automáticamente:** Para esto se añade al archivo `/etc/modules.conf` o `/etc/conf.modules` las líneas:

```
alias net-pf-10 ipv6
alias sit0 ipv6
alias sit1 ipv6
alias tun6to4 ipv6
```

También es posible deshabilitar la carga automática del módulo usando la línea:

```
alias net-pf-10 off
```

CONFIGURACIÓN IPv6 DE RED EN RH LINUX

Una vez instaladas las aplicaciones y el soporte IPv6 en los hosts con sistema operativo RH Linux, se esta en capacidad de configurar interfaces de red y de interoperar directamente con nodos IPv6. Para esto se puede trabajar directamente sobre los scripts de red instalados en el sistema, los cuales proveen un control permanente de las interfaces de red a utilizar; de este modo, cuando RH Linux inicia, utiliza estos archivos para saber que interfaces utilizar automáticamente y como configurarlas para que operen correctamente.

A continuación se muestra el procedimiento para configurar los parámetros de red IPv6 en los equipos con S.O. RH Linux:

- Para cambiar el nombre a un PC se agrega en `/etc/sysconfig/network`, la línea:

```
HOSTNAME=nombre-del-equipo
```

CAPITULO 6. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA IPv6 SOBRE ETHERNET DE ALTA VELOCIDAD.

- El nombre del equipo puede verse en `/proc/sys/kernel/hostname`, o simplemente ejecutando el comando `hostname` sin ningún parámetro.
- Se deben añadir entradas en `/etc/hosts` para IPv6:

<code>::1</code>	<code>localhost</code>	<code>ip6-localhost</code>	<code>ip6-loopback</code>
<code>FE00::0</code>	<code>ip6-localnet</code>		
<code>FF00::0</code>	<code>ip6-mcastprefix</code>		
<code>FF02::1</code>	<code>ip6-allnodes</code>		
<code>FF02::2</code>	<code>ip6-allrouters</code>		
<code>FF02::3</code>	<code>ip6-allhosts</code>		

- Se debe comprobar que en `/etc/protocolos` aparezca:

<code>ipv6</code>	<code>41</code>	<code>IPv6</code>
<code>ipv6-route</code>	<code>43</code>	<code>IPv6-Route</code>
<code>ipv6-frag</code>	<code>44</code>	<code>IPv6-Frag</code>
<code>ipv6-crypt</code>	<code>50</code>	<code>IPv6-Crypt</code>
<code>ipv6-auth</code>	<code>51</code>	<code>IPv6-Auth</code>
<code>ipv6-icmp</code>	<code>58</code>	<code>IPv6-ICMP</code>
<code>ipv6-nonxt</code>	<code>59</code>	<code>IPv6-NoNxt</code>
<code>ipv6-opts</code>	<code>60</code>	<code>IPv6-Opts</code>

ASIGNACIÓN DE DIRECCIONES GLOBALES AGREGABLES A HOSTS

El mecanismo utilizado es el de autoconfiguración sin control de estado, el cual permite asignar una dirección Global Agregable en forma autónoma y automática, a partir del identificador de interfaz y del prefijo anunciado por el enrutador IPv6 del segmento de red. Para esto se trabaja directamente sobre los archivos de configuración de interfaz:

- El archivo `/etc/sysconfig/network` debe tener las siguientes entradas respecto a IPv6:

<code>NETWORKING_IPV6=yes</code> # NETWORKING_IPV6= <indicador>, donde <indicador> es uno de los siguientes valores: #yes: Habilita la inicialización Global de IPv6 #no: Deshabilita la inicialización Global de IPv6
<code>IPV6_AUTOCONF=yes</code> # IPV6_AUTOCONF = <indicador>, donde <indicador> es uno de los siguientes valores: #yes: Habilita la autoconfiguración de direcciones IPv6 #no: Deshabilita la autoconfiguración de direcciones IPv6

CAPITULO 6. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA IPv6 SOBRE ETHERNET DE ALTA VELOCIDAD.

```
IPV6FORWARDING=no
# IPV6FORWARDING = <indicador>, donde <indicador> es uno de los siguientes valores:
#yes: Habilita el reenvío de paquetes IPv6
#no:  Deshabilita el reenvío de paquetes IPv6

IPV6_AUTOTUNEL=no
# IPV6_AUTOTUNEL = <indicador>, donde <indicador> es uno de los siguientes valores:
#yes: Habilita la inicialización de túneles automáticos
#no:  Deshabilita la inicialización de túneles automáticos
```

- En el directorio `/etc/sysconfig/network-scripts/` se debe editar el archivo de configuración de interfaz apropiado (Ejemplo: `ifcfg-eth0`), y se agregan las siguientes entradas:

```
IPV6INIT=yes
# IPV6INIT = <indicador>, donde <indicador> es uno de los siguientes valores:
#yes: Habilita la inicialización de IPv6 en ésta interfaz
#no:  Deshabilita la inicialización de IPv6 en ésta interfaz

IPV6_ROUTER=no
# IPV6_ROUTER = <indicador>, donde <indicador> es uno de los siguientes valores:
#yes: Habilita el envío de Anuncios de enrutamiento en ésta interfaz
#no:  Deshabilita el envío de Anuncios de enrutamiento en ésta interfaz
```

- Se debe corroborar que los archivos de configuración de interfaz localizados en los directorios `/etc/sysconfig/network-scripts/` y `/etc/sysconfig/networking/devices/` tengan iguales entradas.
- Finalmente para trabajar con los nuevos parámetros de red configurados, se debe reiniciar el servicio de red ejecutando el comando `# service network restart`.

6.4.2.2 CONFIGURACION DEL PROTOCOLO IPv6 EN FEDORA

El procedimiento de configuración para habilitar el soporte IPv6 en FEDORA es similar al de RED HAT, por lo cual se deben seguir los mismos pasos.

6.5 FASES DE MIGRACION HACIA IPv6

La migración de IPv4 a IPv6 sin duda alguna será un proceso largo que involucra la actualización de aplicaciones, hosts, routers y la infraestructura DNS para brindar el soporte IPv6. Debido a que la migración puede durar varios años, los dispositivos de

CAPITULO 6. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA IPv6 SOBRE ETHERNET DE ALTA VELOCIDAD.

red IPv4/IPv6 deben ser capaces de coexistir con la infraestructura IPv4 actual tales como la Internet y las Intranets privadas.

A continuación se presentan las diferentes fases de evolución que puede adoptar la Universidad del Cauca como metodología general para migrar de IPv4 a IPv6 y de ésta manera realizar un proceso de migración paulatino.

6.5.1 FASE No. 1: ACTUALIZACIÓN DE LAS APLICACIONES PARA QUE SEAN INDEPENDIENTES DEL PROTOCOLO IPv6 O IPv4

En ésta primera fase, las aplicaciones deben ser cambiadas para usar nuevas API's (Application Programming Interfaces) de tal manera que la resolución de nombres, creación de sockets, y otras funciones sean independientes de la versión del protocolo IP que se este usando.

Actualmente en el mercado están disponibles aplicaciones con versiones que soportan el protocolo IPv6. La tarea principal de la administración de la Red de Datos será identificar dichas aplicaciones, su grado de funcionalidad y los requisitos de cada uno, además de sus parámetros de configuración.

6.5.2 FASE No. 2: ACTUALIZACIÓN DE LA INFRAESTRUCTURA DNS

En ésta fase, la infraestructura DNS debe ser actualizada para soportar los nuevos registros AAAA y los registros PTR en el dominio IP6.INT para las consultas IPv6 inversas.

Para realizar la actualización existe una herramienta llamada BIND (Berkeley Internet Name Domain) versión 9, la cual provee una implementación de los componentes principales del DNS para IPv6 tales como: DNS server, DNS resolver library, y herramientas de verificación.

6.5.3 FASE No. 3: ACTUALIZACIÓN DE HOSTS A NODOS IPv6/IPv4

En la fase número 3, los hosts deben ser actualizados para usar una capa IP Dual o Stack IP Dual. El soporte de resolución DNS también debe ser adicionado al proceso de consulta DNS que contiene tanto las direcciones IPv4 como IPv6.

Dado que la mayoría de los hosts de La Universidad del Cauca funcionan bajo la plataforma Windows, en ésta fase es necesario realizar los procedimientos de configuración detallados en la sección 6.4 de éste capítulo. A medida que La Universidad adquiera licencias para las nuevas versiones del sistema operativo Windows (Ejemplo: Windows 2003), su configuración será mucho más sencilla teniendo en cuenta que éstos ya brindarán el soporte necesario para el protocolo IPv6.

Para aquellos equipos que funcionan bajo la plataforma Linux, también será necesario realizar los procedimientos descritos en la sección 6.4, para poder proveer la conectividad IPv6 necesaria.

6.5.4 FASE No. 4: ACTUALIZACIÓN DE LA INFRAESTRUCTURA DE ROUTING

En esta fase, en primera instancia se realiza la actualización de los dispositivos de internetworking para proveer el soporte de la Pila Dual de protocolos. Para ello, se puede iniciar con la actualización de los dispositivos del nivel de CORE y posteriormente realizar la actualización de los dispositivos del nivel de DISTRIBUCION y ACCESO.

Finalmente, los routers y switches multinivel deben ser actualizados para soportar enrutamiento IPv6 nativo y protocolos de enrutamiento IPv6.

6.5.5 FASE No. 5: CONVERSION DE NODOS IPv6/IPv4 A NODOS IPv6 SOLAMENTE

Los nodos *IPv6/IPv4* pueden ser actualizados para ser nodos *IPv6-solamente*. Esto puede ser un objetivo a realizarse al largo plazo teniendo en cuenta que la actualización de los dispositivos de red *IPv4-solamente* a *IPv6-solamente* puede tomar varios años. Para aquellos nodos *IPv4-solamente* que no pueden ser actualizados a nodos *IPv6/IPv4* o *IPv6-solamente*, se pueden emplear técnicas de traducción como método apropiado para que los nodos *IPv4-solamente* puedan comunicarse con nodos *IPv6-solamente*.

La migración al nuevo protocolo en las redes actuales es un trabajo no exento de riesgos y costes. Algunos estarán ocultos hasta el momento de llevar a cabo la puesta en escena, pero la planificación y la discusión son las únicas herramientas que pueden ayudar a conseguir una migración lo más suave posible. Los riesgos están relacionados con la posible pérdida de eficiencia en las redes en las que se implante IPv6 en los períodos de transición, los costes dependerán de la densidad de cambios, la velocidad del despliegue y el esfuerzo (tanto económico como humano) que se vaya a dedicar a la tarea de migración.

Es más, se debe ser consciente que la migración a nivel de red y de servicios sólo será una parte de la migración a IPv6, puesto que si se quiere aprovechar las nuevas características del protocolo, se deben emplear nuevos esfuerzos en extender la red con aplicaciones que soporten calidad de servicio, sistemas preparados para la gestión de claves de seguridad y routers capaces de proveer entornos de movilidad a los usuarios, entre otras cosas.

CAPITULO 6. MIGRACION DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA HACIA IPv6 SOBRE ETHERNET DE ALTA VELOCIDAD.

También es importante remarcar que el éxito de la migración dependerá, además, en gran medida de la disponibilidad de software adecuado a la nueva tecnología, que no sólo permita estar a la altura del servicio proporcionado por la tecnología basada en IPv4, sino que permita sacar partido de sus características positivas y que permita obviar, en mayor o menor medida, sus posibles desventajas.

CONCLUSIONES Y RECOMENDACIONES

Con el desarrollo del presente trabajo de grado se puede concluir lo siguiente:

- Se puede asegurar que la Red de Datos de la Universidad del Cauca cuenta con una excelente infraestructura, ya que posee un importante número de equipos de red, servidores, estaciones de trabajo y un gran despliegue de cableado a lo largo del campus universitario. Sin embargo, el funcionamiento actual no es el más óptimo, debido principalmente a configuraciones inadecuadas y la falta de una arquitectura de gestión integral en la Red.
- Ethernet ha sido capaz de evolucionar desde 10 Mbps a 100, 1.000 y ahora 10.000 Mbps. Esta tecnología está presente en la inmensa mayoría de las redes corporativas de todo el mundo, y actualmente ofrece la velocidad, rendimiento y fiabilidad necesarios para soportar las nuevas necesidades de las empresas con el mejor costo total de propiedad. Todo esto hace pensar que, además del presente, Ethernet será también el futuro de las redes de alta velocidad.
- La migración de IPv4 hacia IPv6 permitirá que la Red de Datos de la Universidad del Cauca esté preparada para la nueva generación de Internet, con la cual se podrán obtener mayores beneficios, prestar nuevos y mejores servicios y superar muchas de las deficiencias del protocolo de Internet actual. Para ello es necesario aprovisionar y mejorar la Red con dispositivos, sistemas operativos y aplicaciones que estén realmente listos para cumplir las especificaciones de IPv6, sin que por ello dejen de ser válidos en IPv4.
- Para llevar a cabo la migración hacia IPv6 sobre Ethernet de alta velocidad es necesario establecer diferentes fases de implementación de acuerdo a las necesidades y capacidades económicas y administrativas de la Institución. Desplegar éstas tecnologías en una sola fase representaría un costo total muy alto que sobrepasa los recursos que la Universidad del Cauca puede destinar para la Red de Datos.

Para finalizar se recomienda:

- El mejoramiento en primera instancia de los segmentos en donde se detectaron niveles altos de congestión que sobrepasan constantemente los límites de desempeño recomendados para redes Ethernet.

- Buscar nuevas alternativas de conexión para los sectores de Las Guacas y Casa Caldas, con el fin de disponer de un enlace que sea propiedad de la Universidad del Cauca y poder alcanzar mayores velocidades de acceso teniendo en cuenta que toda la Red migrará hacia nuevas tecnologías de alta velocidad.
- La supresión de protocolos presentes en la Red tales como NetBEUI, Novell, AppleTalk y RIP, que no tienen una funcionalidad específica definida o que no están siendo utilizados, los cuales están generando tráfico innecesario que afecta el buen desempeño de la Red.
- Adquirir una solución propietaria para la migración de la Red de datos con el objetivo de poder aprovechar al máximo la capacidad de los dispositivos y obtener mayores beneficios. El adquirir equipos de un mismo fabricante permite mejorar el rendimiento y control de la Red ya que se pueden implementar técnicas como *configuración de equipos en stack, chasis virtual, etc.* y establecer un mecanismo de gestión integral por medio de herramientas propietarias ofrecidas por el mismo fabricante.
- Incrementar la capacidad de los canales de acceso WAN o acceso a Internet de acuerdo a las capacidades económicas de la Institución, debido a que con la migración de la Red de Datos se lograran mayores velocidades por lo que la demanda de ancho de banda de los canales aumentará. Esto teniendo que en cuenta que hoy en día los niveles de utilización de dichos canales son demasiado altos.

GLOSARIO

10BASE-T: Estándar IEEE 802.3, que especifica Ethernet sobre UTP.

10BASE-F: Estándar IEEE 802.3, que especifica Ethernet sobre fibra óptica.

100BASE-FX: Estándar IEEE 802.3u, que especifica Ethernet sobre fibra óptica a 100 Mbps.

100BASE-TX: Estándar IEEE 802.3u, que especifica Ethernet sobre UTP Categoría 5 y cableado Tipo 1 a 100 Mbps.

1000BASE-LX: Estándar IEEE 802.3z, que especifica Ethernet sobre fibra óptica para largas distancias a 1000 Mbps.

1000BASE-SX: Estándar IEEE 802.3z, que especifica Ethernet sobre fibra óptica para distancias cortas a 1000 Mbps.

1000BASE-T: Estándar IEEE 802.3z, que especifica Ethernet sobre UTP Categoría 5 y Categoría 5 mejorada a 1000 Mbps.

10GBASE-SR / 10GBASE-SW: Estándar IEEE 802.3ae, que especifica 10 Gigabit Ethernet sobre fibra óptica multimodo de onda corta (850 nm).

10GBASE-LR / 10GBASE-LW: Estándar IEEE 802.3ae, que especifica 10 Gigabit Ethernet sobre fibra óptica monomodo de onda larga (1310nm).

10GBASE-LR / 10GBASE-LW: Estándar IEEE 802.3ae, que especifica 10 Gigabit Ethernet sobre fibra óptica monomodo de onda larga (1550nm).

A

ANYCAST: identifica múltiples interfaces de red pertenecientes a diferentes nodos. Los paquetes dirigidos a una dirección de Anycast serán entregados a una de esas interfaces, generalmente la más próxima.

APPLETALK: protocolos de red desarrollados y comercializados por la corporación de computadores Apple utilizados para conectar ordenadores Macintosh en redes locales.

ARP (Protocolo de Resolución de Direcciones – Address Resolution Protocol): protocolo del conjunto TCP/IP que permite la resolución de direcciones IP a direcciones MAC para paquetes IP.

B

BACKBONE: conectividad LAN o WAN entre subredes a través de una red de alta velocidad. A menudo aplicado a una red de campus de gran velocidad, como ATM OC-12 o Gigabit Ethernet que interconecta redes de baja velocidad como ATM OC-3 o Fast-Ethernet.

BACKBONE COLAPSADO: Una arquitectura de red en la cual un router o switch proporciona un backbone de campus o edificio usando una topología de estrella.

BROADCAST: un paquete entregado a todas las estaciones de trabajo en una red. Existe en los niveles dos y tres.

C

CALIDAD DE SERVICIO . (Quality of Service – QoS): Capacidad de un equipo de red para proveer alguna garantía de desempeño como prioridad en la entrega de tráfico, velocidad, retardo o variación del retardo.

CONTROL DE ACCESO AL MEDIO (Medium Access Control - MAC): La manera en que las workstations LAN comparten el acceso al medio de transmisión. Entre los protocolos de nivel MAC se incluyen Ethernet, Token Ring, y FDDI.

CONTROL DE ENLACE LÓGICO (Logical Link Control - LLC): parte de la cabecera LLC/SNAP del IEEE usada para identificar el tipo de un paquete. La cabecera completa es de 8 octetos, de los cuales LLC ocupa los primeros tres.

D

DIRECCIÓN IPv4: Dirección de 32 bits asignada a la interfaz de un host o un enrutador que están dispuestos en la arquitectura de red de IPv4, escrita en formato decimal punteado.

DIRECCIÓN IPv6: Dirección de 128 bits asignada a las interfaces de un host o un enrutador que están dispuestos en la arquitectura de red de IPv6, escrita como 8 dígitos hexadecimales separados por : .

DIRECCIÓN MAC: Dirección del nivel 2 de un dispositivo LAN.

DOMINIO DE BROADCAST: Conjunto de estaciones terminales que reciben los mismos paquetes de broadcast.

E

E1: Sistema de transmisión digital a 2.048 Mbps utilizado en Europa.

ENCABEZAMIENTO: Porción adicionada al comienzo de un mensaje que contiene información esencial como la dirección de la fuente, dirección de destino e información de control.

ENRUTAMIENTO: El proceso de entregar un mensaje a través de una red o redes usando el camino mas apropiado.

ETHERNET: El protocolo de nivel dos mas comúnmente usado en las LAN. Ethernet es un estándar CSMA/CD a 10 Mbps originalmente desarrollado por Xerox

para correr sobre cableado coaxial grueso. Ha evolucionado y ahora se corre principalmente sobre cableado de par trenzado.

F

FAST ETHERNET: Una versión de Ethernet que opera a 100 Mbps.

FDDI: Una red de área local basada en un backbone de dos anillos en fibra óptica a 100 Mbps contrarotantes. Uno de los anillos se diseña normalmente como anillo primario; el otro es el anillo secundario.

FULL-DUPLEX: Transmisión bidireccional simultánea de información sobre un medio común.

FUERZA DE TAREAS EN INGENIERÍA DE INTERNET (Internet Engineering Task Force - IETF): Cuerpo de estandarización que soporta el desarrollo de nuevos protocolos para el Internet.

G

GIGABIT ETHERNET: Una variación de la Ethernet tradicional que opera sobre cable de fibra óptica multimodo, monomodo o par trenzado no apantallado a 1.000 Mbps.

H

HALF-DUPLEX: Transmisión bidireccional de información sobre un medio común, pero donde la información puede solamente viajar en una dirección en un momento dado.

HOST: Estación de comunicación terminal en una red. Estación de trabajo.

HUB: El centro de una red o sistema de cableado en topología de estrella. Típicamente usado en las redes Ethernet y Token Ring más primitivas. Un dispositivo conectado al un hub recibe todas las transmisiones de todos los otros dispositivos conectados a ese hub. Los hubs están ahora siendo remplazados en muchos casos por switches LAN.

I

INSTITUTO DE INGENIEROS ELÉCTRICOS Y ELECTRÓNICOS (Institute of Electrical and Electronic Engineers - IEEE): Un cuerpo de estandarización responsable de desarrollar muchos estándares usados en las LAN, incluyendo la serie 802.x.

IEEE 802.1p: Método de nivel 2 para la señalización de la prioridad en redes realizado a cada trama.

IEEE 802.1Q: Estándar que define cambios a las tramas Ethernet para permitirles llevar información VLAN.

INTERFAZ DE TASA BÁSICA (Basic Rate Interface - BRI): acceso básico ISDN que proporciona dos canales B (64 Kbps) y un canal D (16 Kbps) multiplexados a través de una línea telefónica.

INTERFAZ DE TASA PRIMARIA (Primary Rate Interface - PRI): acceso primario ISDN que proporciona 30 canales B y un canal D de 64 Kbps en Europa. En EE.UU. suele tener 23 canales tipo B y un canal D de 64Kbps.

INTERFAZ DE USUARIO MEJORADA NETBIOS (NetBIOS Extended User Interface - NetBEUI): es la implementación de Microsoft del estándar NetBIOS.

INTRANET: Red privada de una empresa basada en el modelo de Internet.

IPX/SPX (Internet Packet eXchange/Sequenced Packet eXchange): es el conjunto de protocolos de bajo nivel utilizados por el sistema operativo de red Netware de Novell. SPX actúa sobre IPX para asegurar la entrega de los datos.

M

MÁXIMA UNIDAD DE TRANSFERENCIA (Maximum Transfer Unit - MTU): Máximo tamaño de la unidad de transmisión que puede utilizarse en una red.

MULTICAST: Una forma de broadcast en la cual un paquete es entregado a un subconjunto predefinido de destinatarios. Una dirección de destino multicast específica es usada.

N

NETWARE: nombre de un sistema de red desarrollado y comercializado por Novell Incorporated.

NODO: es el punto en donde se producen dos o más conexiones en una red de comunicaciones. No se trata de un elemento estrictamente físico, sino de una unidad funcional que exige hardware y software. Un nodo puede incluir controladores de comunicaciones, clusters, servidores, repetidores, etc.

NOVELL: es una de las firmas de origen norteamericano más importantes en el ámbito de las redes de área local en todo el mundo y su producto estrella es Netware.

O

ORACLE: empresa especializada en la fabricación de programas de bases de datos en ordenadores.

OSPF (Open Shortest Path First): protocolo de enrutamiento enlace-estado no propietario utilizado por los enrutadores IP para determinar el camino óptimo a lo largo del cual transportar un paquete.

P

PING (Packet Internet Groper): es una herramienta de diagnóstico para verificar la conectividad entre dos computadores en una red. Envía paquetes ICMP con Respuesta de Eco a una dirección IP remota, observa las respuestas ICMP e indica el tiempo exacto que tardan los paquetes en ir y volver desde la máquina origen hasta la máquina destino.

PROXY: El mecanismo por medio del cual un sistema representa a otro sistema respondiendo a los requerimientos del protocolo.

PROTOCOLO INTERNET (IP): El protocolo de nivel 3 usado en el conjunto de protocolos TCP/IP que soporta el Internet y muchas redes privadas. IP proporciona un servicio de entrega de datagramas sin conexión para los protocolos del nivel de transporte como TCP y UDP.

PROTOCOLO DE CONFIGURACIÓN DINÁMICA DE HOST (Dynamic Host Configuration Protocol – DHCP): Protocolo para asignación dinámica de direcciones IP y la configuración automática TCP/IP que provee la asignación de direcciones dinámicas y estáticas.

PROTOCOLO DE INTERCAMBIO DE PAQUETES INTERNET (Internet Packet Exchange Protocol - IPX): Protocolo de nivel 3 usado en el conjunto de protocolos NetWare de Novell. IPX proporciona un servicio de entrega de datagramas para los protocolos del nivel de transporte como SPX y NCP.

PROTOCOLO SIMPLE DE GESTIÓN DE RED (Simple Network Management Protocol - SNMP): Protocolo diseñado para gestionar dispositivos de red. Con SNMP una estación de gestión puede configurar un dispositivo soportado; puede requerir que ese dispositivo envíe información estadística, de configuración o de estado y puede recibir alarmas no solicitadas de un dispositivo.

PROTOCOLO DE RESOLUCIÓN DE DIRECCIONES (Address Resolution Protocol – ARP): Protocolo TCP/IP usado para obtener la dirección física de un nodo cuando solamente su dirección IP lógica es conocida.

PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS (File Transfer Protocol – FTP): Protocolo de aplicación que es usado para transmitir archivos entre nodos de red.

PROTOCOLO DE MENSAJES DE CONTROL DE INTERNET (Internet Control Message Protocol – ICMP): Protocolo que provee un número de funciones de diagnóstico, incluyendo el envío de paquetes de error a hosts y mensajes ping.

PROTOCOLO DE MENSAJES DE CONTROL DE INTERNET VERSION 6 (Internet Control Message Protocol Versión 6– ICMPv6): Versión 6 del protocolo ICMP, para ser usado por IPv6.

PROTOCOLO DE GESTIÓN DE GRUPOS DE INTERNET (Internet Group Management Protocol – IGMP): Protocolo usado por hosts IP para reportar la membresía de grupos multicast a un router adyacente.

PROTOCOLO DE CAMINO MÁS CORTO DISPONIBLE PRIMERO (Open Shortest Path First – OSPF): Protocolo de enrutamiento de estado de enlace que determina el mejor camino para el enrutamiento del tráfico sobre una red TCP/IP.

PROTOCOLO DE RESOLUCIÓN DE DIRECCIONES INVERSA (Reverse Address Resolution Protocol - RARP): Protocolo que realiza lo opuesto de ARP, encontrando la dirección de nivel 3 que corresponde a la dirección de nivel 2.

PROTOCOLO DE INFORMACIÓN DE ENRUTAMIENTO (Routing Information Protocol - RIP): Protocolo de enrutamiento que determina el mejor camino para enrutar el tráfico sobre una red por medio del análisis del número de saltos

R

RED DE ÁREA LOCAL (Local Area Network - LAN): Red que interconecta todos los dispositivos informáticos localizados sobre un área geográficamente pequeña.

RED DE ÁREA LOCAL VIRTUAL (Virtual LAN - VLAN): Grupo de equipos independientes que se comunican como si estuvieran en el mismo segmento LAN físico, pero en realidad pueden estar localizados en cualquier parte de la red.

RED DE ÁREA METROPOLITANA (Metropolitan Area Network – MAN): Una red que geográficamente se extiende en un área mas grande que la LAN pero menos que la WAN.

RED DE ÁREA AMPLIA (WAN): Una red que cubre un área geográficamente mas grande en la cual los enlaces de telecomunicaciones normalmente son alquilados por los proveedores del servicio.

RED DE CAMPUS: Una red que cubre una sola ubicación comercial, tal como un edificio, un piso de un edificio, o todos los edificios en una gran red comercial, educacional, o otro campus.

RFC (Request For Comments): Documentos utilizados como medios primarios para comunicar información acerca de la Internet.

ROUTER: Un dispositivo de nivel 3 responsable de tomar decisiones con respecto a cual de todos los caminos seguirá el trafico de la red. Para hacer esto, usa un protocolo de enrutamiento para obtener información sobre la red, y los algoritmos para escoger la mejor ruta con base en varios criterios (conocidos como métricas de enrutamiento). Los routers interconectan las subredes.

S

SEGMENTO: Un trozo eléctricamente continuo de una LAN. Los segmentos pueden ser unidos usando hubs, switches, bridges, o routers.

SEGMENTACIÓN: Incrementar el ancho de banda disponible por dispositivo dividiendo la red con bridges, switches, o routers para disminuir el número de nodos en un segmento.

SERVICIOS DIFERENCIADOS (Differentiated Services. – DiffServ): El resultado de un grupo de trabajo del IETF que está definiendo un nuevo esquema de gestión de ancho de banda para redes IP, redefiniendo parte del byte Tipo de Servicio en cada encabezado de los paquetes IP, para marcar la prioridad o nivel de servicio que el paquete requiere.

SERVIDOR: computadora dedicada a gestionar el uso de la red por otras computadoras llamadas clientes. Contiene archivos y recursos que pueden ser accedidos desde otras terminales.

SISTEMA DE NOMBRES DE DOMINIO (Domain Name System – DNS): Sistemas de bases de datos distribuidas para la traducción de nombres de computadores Internet hacia direcciones IP.

SPANNING TREE: Protocolo definido en el estándar IEEE 802.1D que permite a una red tener una topología que contenga lazos lógicos. Opera en bridges y switches. Abre ciertos caminos para crear una topología de árbol, por lo tanto previene que los paquetes permanezcan indefinidamente en la red.

SUBRED: Una porción de la red en la cual todas las estaciones comparten una misma dirección de subred.

SWITCH: Dispositivo de nivel 2, encargado de la conmutación de tramas.

T

TARJETA DE INTERFAZ DE RED (NIC): Un módulo de conexión física que se coloca dentro de una workstation o servidor y proporciona la conexión a la red.

TCP/IP: Los múltiples protocolos que soportan el Internet y muchas redes privadas.

TELNET: protocolo que permite a los usuarios conectarse a una computadora remota en Internet. Ésta puede localizarse en una oficina próxima o en cualquier lugar del mundo.

TOPOLOGÍA: Puede ser o física o lógica. La primera describe las conexiones físicas de una red y el arreglo geométrico de los enlaces y nodos que componen la red. La segunda describe las posibles conexiones lógicas entre nodos, e indica que pares de nodos son capaces de comunicarse.

TORMENTA DE BROADCAST: Una condición de sobrecarga en una red creada por la difusión de un paquete incorrecto dentro de la red que causa que varios hosts respondan a la vez. Típicamente la respuesta contiene igualmente paquetes incorrectos, lo que causa que la tormenta crezca exponencialmente en severidad.

TRAMA: Una unidad de información en un protocolo de nivel dos. En las LAN, una trama es una unidad de nivel MAC que contiene información de control como una paquete de nivel 3 completo. Aunque el término paquete es a veces usado para

significar una trama, el termino trama nunca es usado para describir un paquete de nivel 3.

U

UNICAST: Una trama enviada de una estación a otra. Una trama unicast contiene la dirección MAC especifica de los dispositivos fuente y destino.

LISTA DE ACRÓNIMOS

- ACL:** Access Control Lists. Listas de control de acceso.
- ALG:** Application Layer Gateway. Nivel de aplicación de Gateway.
- ANSI:** American National Standards Institute. Instituto de estándares Nacionales Americanos.
- API:** Application Programming Interfaces.
- ARP:** Address Resolution Protocol. Protocolo de resolución de direcciones.
- ATM:** Asynchronous Transfer Mode. Modo de transferencia asíncrono.
- AUI:** Attachment Unit Interface.
- BIND:** Berkeley Internet Name Domain.
- BGP:** Border Gateway Protocol. Protocolo de Gateway de frontera.
- BootP:** Bootstrapp Protocol.
- CDU:** Centro Deportivo Universitario.
- CMS:** Cisco Cluster Management Suite.
- CRC:** Cyclical Redundancy Check. Chequeo de redundancia cíclica.
- CSMA/CD:** Carrier Sense Multiple Access/Collision Detection. Acceso múltiple con detección de Portadora y de colisión.
- DHCP:** Dynamic Host Configuration Protocol. Protocolo de configuración dinámica de hosts.
- DNS:** Domain Name System. Sistema de nombres de dominio.
- DSCP:** Differentiated Service Code Point.
- DVMRP:** Distance Vector Multicast Routing Protocol.
- EIA:** Electronic Industries Association. Asociación de Industrias Electrónicas.
- EMI:** Enhanced Multilayer Software Image. Imagen mejorada de software multinivel.
- ETD:** Equipo Terminal de Datos
- FDDI:** Fiber Distributed Data Interface. Interfaz de datos distribuidos por fibra.
- FO:** Fibra Óptica.
- FTP:** File Transfer Protocol. Protocolo de transferencia de archivos.
- GBIC:** Gigabit Interface Converter. Interfaz Gigabit.
- Gbps:** Gigabits per Second. Gigabits por segundo.
- GMI:** Gigabit Media Independent Interface. Interfaz Gigabit independiente del medio.

HDSL: High Rate Digital Subscriber Line.

HTTP: HyperText Transfer Protocol. Protocolo de Transferencia Hipertexto.

IANA: Internet Assigned Numbers Authority

ICMP: Internet Control Message Protocol. Protocolo de mensajes de control Internet.

IDC: Information Data Corporation.

IDS: Intrusión Detection Systems. Sistema de detección de intrusos.

IEEE: Institute of Electrical and Electronic Engineers. Instituto de Ingenieros Eléctricos y Electrónicos.

IETF: Internet Engineering Task Force. Fuerza de tareas en ingeniería de Internet.

IGMP: Internet Group Management Protocol. Protocolo de gestión de grupos Internet.

IP: Internet Protocol. Protocolo Internet.

IPv6: Internet Protocol Versión 6. La nueva versión de IP.

IPX: Internet Packet Exchange Protocol. Protocolo de intercambio de paquetes Internet

ISDN: Integrated Services Digital Network. Red digital de servicios integrados.

ISATAP: Intra Site Automatic Tunnel Address Protocol.

ISP: Internet Service Provider. Proveedor de servicio de Internet.

IPET: Instituto de Postgrados en Electrónica y Telecomunicaciones.

Kbps: Kilobits per second. Kilobits por segundo.

LACP: Link Aggregation Control Protocol.

LAN: Local Area Network. Red de área local.

LED: Light Emitting Diode. Diodo Emisor de Luz.

LLC: Link Layer Control. Control del nivel de enlace.

MAC: Medium Access Control. Control de acceso al medio.

MAN: Metropolitan Area Network. Red de área metropolitana.

MAU: Medium Attachment Unit. Interfaz unida el medio.

Mbps: Megabits per Second. Megabits por Segundo.

MDI: Medium Dependent Interface. Interfaz dependiente del medio.

MII: Media Independent Interface. Interfaz independiente del medio.

MRTG: Multi Router Traffic Graphic.

MTU: Unidad de transmisión máxima.

NAT: Network Address Translation. Traducción de direcciones de red.

ND: Neighbor Discovery. Descubrimiento de vecino.

NetBIOS: Network Basic Input/Output System. Sistema de entrada/salida básico de red.

NetBEUI: NetBIOS Extended User Interface. Interfaz de usuario extendida de NetBIOS.

NIC: Network Interface Card. Tarjeta de interfaz de red.

NLA: Next Level Aggregation. Siguiendo nivel de agregación.

NVP: Nominal Velocity of Propagation. Velocidad nominal de propagación

OSI: Open System Interconnection. Interconexión de sistemas abiertos.

OSPF: Open Shortest Path First.

OUI: Organization Unique Identifier. Identificador único de organizaciones.

PAgP: Port Aggregation Protocol. Protocolo de agregación de puertos.

PC: Personal Computer. Computador personal.

PMA: Physical Media Attachment. Unión de medio físico.

PMD: Physical Medium Dependent. Dependiente del medio físico.

PPS: Paquetes por segundo.

PoE: Power over Ethernet. Potencia sobre Ethernet.

POP3: Post Office Protocol-3. Protocolo de oficina postal versión 3.

PRI: Primary Rate Interface. Interfaz de tasa primaria.

PS Hub: Port Switch Hub. Hub con conmutación de puertos.

RADIUS: Remote Access Dial-In User Service.

RARP: Reverse Address Resolution Protocol. Protocolo de resolución de direcciones contrario.

RAS: Remote Access Server. Servidor de acceso remoto.

RDSI: Red Digital de Servicios Integrados.

RFC: Request For Comments. Solicitudes de Comentarios de Internet

RIP: Routing Information Protocol. Protocolo de información de enrutamiento.

RSVP: Protocolo de reserva de recursos

QoS: Quality of Service. Calidad del servicio.

SDH: Synchronous Digital Hierarchy. Jerarquía digital sincrónica.

SFP: Small Form-Factor Pluggable. Conector de tamaño reducido.

SLA: Site Level Aggregation. Nivel de agregación de sitio.

SMI: Standard Multilayer Software Image. Imagen estándar de software multinivel.

SMTP: Simple Mail Transfer Protocol. Protocolo de transferencia de correo simple.

SNMP: Simple Network Management Protocol. Protocolo simple de gestión de red.

SSL: Secure Socket Layer. Capa Nivel de Seguridad.

STP: Shielded Twisted Pair. Par Trenzado Apantallado.

TCP: Transfer Control Protocol. Protocolo de control de transferencia de datos.

TLA: Top Level Aggregation. Nivel de agregación superior.

TFTP: Trivial FTP. FTP trivial.

TNS: Transparent Network Substrate.

TTL: Time To Live. Tiempo de vida.

UDP: User Datagram Protocol. Protocolo de datagramas de usuario.

um: Micrometros.

UNAM: Universidad Autónoma de México.

UTP: Unshielded Twisted Pair. Par trenzado sin apantallar.

VLAN: Virtual LAN. LAN Virtual.

VoIP: Voz sobre IP.

VRI: Vicerrectoría de Investigaciones.

VTP: VLAN Trunking Protocol

XAUI: 10 Gigabit Attachment Unit Interface.

WAN: Wide Area Network. Red de área amplia.

WINS: Windows Internet Name System. Servicio de nombres de Internet de Windows.

WWW: World Wide Web. Red Mundial de Documentos HTML.

10GMII: 10 Gigabit Media Independent Interface. Interfaz 10 Gigabit independiente del medio.

BIBLIOGRAFIA

- 10 Gigabit Ethernet Alliance. “**10 Gigabit Ethernet: Technology Overview White Paper**”. Disponible online en <http://www.10gea.org>.
- 10 Gigabit Ethernet Alliance. “**10 Gigabit Ethernet: Interconnection with Wide Area Networks**”. Disponible online en <http://www.10gea.org>.
- 10 Gigabit Ethernet Alliance. “**Optical Fiber and 10 Gigabit Ethernet**”. Disponible online en <http://www.10gea.org>.
- Agilent Technologies. “**Internet Advisor WAN – Product Overview**”. Disponible online en <http://www.agilent.com/comms/onenetworks>.
- Agilent Technologies. “**Ethernet / Fast Ethernet Problems and Solutions**”. Disponible online en <http://www.agilent.com/comms/onenetworks>.
- Alcatel. “**Familia OmniSwitch 6600**”. Disponible online en <http://www.alcatel.com>.
- Alcatel. “**Familia OmniSwitch 6800**”. Disponible online en <http://www.alcatel.com>.
- Alcatel. “**Familia OmniSwitch 7000**”. Disponible online en <http://www.alcatel.com>.
- Alcatel. “**Familia OmniSwitch 8800**”. Disponible online en <http://www.alcatel.com>.
- Cisco Systems. “**Designing High Performance Campus Intranets**”. Disponible online en <http://www.cisco.com>.
- Cisco Systems. “**Designing Switched LAN Internetworks**”. Disponible online en <http://www.cisco.com>.
- Cisco Systems. “**Gigabit Networking Gigabit Ethernet Solutions**”. Disponible online en <http://www.cisco.com>.
- Cisco Systems. “**Internetworking Design Basics**”. Disponible online en <http://www.cisco.com>.

- Cisco Systems. “**LAN Switching**”. Disponible online en <http://www.cisco.com>.
- Cisco Systems. “**Serie Cisco Catalyst 3750**”. Disponible online en <http://www.cisco.com>.
- Cisco Systems. “**Serie Cisco Catalyst 4500**”. Disponible online en <http://www.cisco.com>.
- Cisco Systems. “**Serie Cisco Catalyst 6500**”. Disponible online en <http://www.cisco.com>.
- Gigabit Ethernet Alliance. “**Running 1000BASE-T: Gigabit Ethernet over Copper**”. Disponible online en <http://www.gigabit-ethernet.org>.
- Gigabit Ethernet Alliance. “**Gigabit Ethernet: Accelerating the standard for speed**”. Disponible online en <http://www.gigabit-ethernet.org>.
- Hewlett-Packard. “**HP Internet Advisor Getting Started**”. Disponible online en <http://www.hp.com>.
- IEEE. “**Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications**”. IEEE Std 802. 2000 Edition.
- Soporte IPv6 en Windows 2000. Disponible online en <http://msdn.microsoft.com/downloads/sdks/platform/download.asp>
- Spurgeon, Charles E. “**Ethernet: The Definitive Guide**”. O'Reilly and Associates. 2000.
- **Foro IPv6**: www.ipv6forum.com
- **6Bone**: www.6bone.net
- **IETF – The Internet Engineering Task Force Home Page**: www.ietf.org
- **RFC's**: www.ietf.org
- **Cisco Systems**: www.cisco.com

- **Alcatel:** www.alcatel.com
- CASAMACHIN FERNANDEZ, Victor Andres. ARGUMERO CORTES, Hernando. **“Estudio del equipo Internet Advisor WAN HP J2300D y Diseño de prácticas de laboratorio”**. Universidad del Cauca. 2002.
- PAZ CABRERA, Diego Alejandro. URBANO RAMOS, Liliana Andrea. **“Diseño e Implementación de un laboratorio Internet Desde la perspectiva de Enrutamiento, Seguridad y QoS”**. Universidad del Cauca. 2003.