UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE CUENCA

CARRERA DE INGENIERÍA DE SISTEMAS

Tesis previa a la obtención del Título de:
Ingeniero de Sistemas

TEMA:

"Propuesta de un Plan de Implementación para la migración a IPV6 en la red de la Universidad Politécnica Salesiana Sede-Cuenca"

AUTOR:

Dennys Xavier Landy Rivera.

DIRECTOR:

Wilson Quintuña.

Cuenca, 2013

DECLARACIÓN DE RESPONSABILIDAD

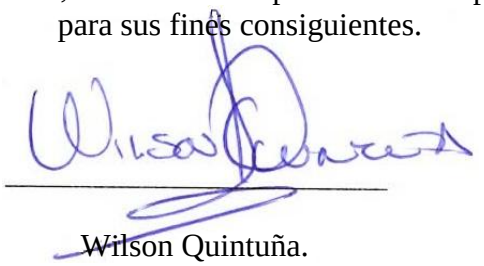
Los conceptos desarrollados, análisis realizados y las conclusiones del presente trabajo, son de exclusiva responsabilidad del autor, y autorizo a la Universidad Politécnica Salesiana el uso de la misma con fines académicos.

Cuenca, Abril del 2013

Dennys Xavier Landy Rivera

CERTIFICO

Que luego de haber revisado cuidadosamente tanto el trabajo práctico como el teórico ha sido aceptado esta investigación, autorizando su presentación al portador, para sus fines consiguientes.



Wilson Quintuña.
DIRECTOR DE TESIS

DEDICATORIA

El presente trabajo va dedicado primeramente a Dios quien me dio la fe, la fortaleza, la salud y la esperanza para terminar mis estudios. Luego a mis padres, porque creyeron en mí y porque me sacaron adelante, dándome ejemplos dignos de superación y entrega, porque en gran parte gracias a ellos, hoy puedo ver alcanzada mi meta, ya que siempre estuvieron impulsándome en los momentos más difíciles de mi carrera, y porque el orgullo que sienten por mí, fue lo que me hizo salir adelante.

Para todos mis primos, tíos, abuelitos, amigos y todos los docentes de la Universidad quienes fueron mi apoyo y estuvieron en las buenas y en las malas conmigo, va dedicado de corazón a cada una de ellos por sus consejos y confianza que me han brindado por lo que he podido culminar mi carrera. Gracias por haber fomentado en mí el deseo de superación y el anhelo de triunfo en la vida.

AGRADECIMIENTOS

Agradezco primeramente a DIOS, que día a día a pesar de las difíciles pruebas que nos pone en la vida siempre nos protege, ayuda, y nos guía por un buen camino.

Un agradecimiento especial a mis padres que siempre han sido la motivación principal, que me han apoyado incondicionalmente y han puesto la confianza para seguir adelante en cada jornada de mi vida.

A todos mis familiares en especial a mis primos: Jhoana, Juan Pablo y Victor Hugo que de alguna u otra manera contribuyeron para poder culminar mi trabajo de investigación lo cual me servirá para el porvenir de mi futuro profesional.

A todos mis amigos y compañeros del colegio: Rubén Jara, Jorge Cuzco, Victor Suquinagua, Carlos Guillermo, Wilmer Orellana, Diego Guillermo, Lorena Padilla, Verónica Sarmiento, Gabriela Ávila, Verónica Chacón, Alex Ortega, Carlos Diez, Johnny Alvear, Román Cárdenas, Darwin Cajilima, Emanuel Zeas, Diego Castro, Dario Bermeo, Carlos Reyes, Gino Mejía, Galo Yupangui, Wilmer León y Manuel Reinoso por estar siempre apoyándome para que culmine mi proyecto de tesis.

Para mis grandes compañeros de la Universidad que me han ayudado en todo momento y con los que he compartido momentos inolvidables: Juan Rodríguez, Isaías Erraez, Fredy Chablay, Cristian Mora, Denys Sigüenza, Jorge Jimenez, Stalin Ruilova, Adrián López, Tatiana Carrasco, Valeria Cuji, Tania Patiño, Johanna León, Pilar García, Daniel Borja, Patricio Cuenca, Lenin Andrade, Milton Asmal, Pablo Narea, Wilson Guiñanzaca, Pablo Guillermo, Edison Peña, Saúl Mora, Daniel Jiménez, Santiago Zea, Andrés Tacuri, Bernardo Cuzco, Diego Duque, Fabián Parra, Carlos Illescas, Pedro Urgilés, Sebastián Cáceres, Pablo Arévalo y Wilian Padilla.

Un sincero agradecimiento a la Universidad Politécnica Salesiana en especial a la Facultad de Ingenierías y cada una de los docentes de la carrera: Ing. Diego Quinde, Ing. Byron Carrión, Ing. Vladimir Robles, Ing. Bertha Tacuri, Ing. Álvaro Mejía, Ing. Rodolfo Bojorque, Ing. Paola Ingavelez, Ing. Miguel Zúñiga, Ing. Mauricio Ortiz, Ing. Eduardo Pinos, quienes con su amplia experiencia, se ingeniaron la forma de inculcar los conocimientos que hoy tenemos.

Finalmente quiero agradecer a los Ing. Patricio Jimenez, Cesar Calle y Fredy Pinos quienes me han brindado su ayuda y sus conocimientos para poder alcanzar mis objetivos y de manera muy especial a mi director de tesis, Wilson Quintuña, quien me ha dado todo el apoyo y me ha guiado en todo el proceso de desarrollo de este proyecto de tesis.

INDICE DE CONTENIDOS

INDICE DE CONTENIDOS	7
INDICE DE FIGURAS	11
INDICE DE TABLAS	12
SIMBOLOGIA	14
INTRODUCCION	15
CAPITULO I. ASPECTOS FUNDAMENTALES	18
1.1 ANTECEDENTES	18
1.2 SITUACIÓN ACTUAL DE LA RED DE LA UNIVERSIDAD POLITÉCNICA SALESIANA	18
1.3 JUSTIFICACIÓN	19
1.4 OBJETIVOS	19
CAPITULO II. MARCO TEÓRICO	20
2.1 CABECERA DE IPV6	20
2.2 DESCRIPCION DE IPV6	22
2.2.1 Resolución de Nombres de IPV6	23
2.2.1.1 Tipos de registro	24
2.2.2 Protocolos Principales de IPV6	25
2.2.2.1 Protocolo ICMPv6	25
2.2.2.2 Descubrimiento de escucha de multidifusión (MLD)	25
2.2.2.3 Descubrimiento de vecinos (ND)	26
2.2.3 Protocolos de enrutamiento	27
2.2.3.1 RIPng para IPV6	27
2.2.3.2 OSPF v3 para IPV6	28
2.2.3.3 BGP-4	29
2.2.4 Direccionamiento IPV6	29
2.2.4.1 Direcciones Unicast	30
2.2.4.2 Direcciones Anycast	32
2.2.4.3 Direcciones Multicast	32
2.2.5 Representación de direcciones IPV6	32
2.2.5.1 Prefijos IPV6	33
2.2.6 Enrutamiento IPV6	34
2.2.6.1 Tablas de enrutamiento IPV6	34
2.3 VENTAJAS Y DESVENTAJAS DE IPV6	35
2.3.1 Ventajas del Protocolo IPV6	35
2.3.2 Desventajas del Protocolo IPV6	36
2.4 MECANISMOS DE TRANSICIÓN IPV4-IPV6	37
2.4.1 Dual Stack(Doble Pila)	38

2.4.2 Tipo Túnel 38
2.4.2.1 Túneles Manuales 39
2.4.2.2 Túneles Automáticos 39
2.4.2.2.1 Túnel 6to4 40
2.4.2.2.2 Túnel 6over4 41
2.4.2.2.3 ISATAP 42
2.4.3 De Traducción 42
CAPITULO III. LEVANTAMIENTO DE INFORMACIÓN IPV4 DE LA UNIVERSIDAD POLITÉCNICA SALESIANA SEDE-CUENCA 43
3.1 IDENTIFICACION DE LA RED 43
3.2 TRAFICO DE RED 46
3.3 DISTRIBUCION DEL CABLEADO 49
3.3.1 CABLEADO HORIZONTAL 50
3.3.1.1 IDF’s 50
3.3.1.2 Área de Trabajo 53
3.3.2 CABLEADO VERTICAL 55
3.3.2.1 MDF 55
3.4 LEVANTAMIENTO Y OBTENCIÓN DEL DIAGRAMA LOGICO 60
3.4.1 Diseño de la Topología de red 60
3.4.2 Diseño de las VLANS 62
3.4.2.1 Reglas de Conectividad entre VLANS 63
3.4.3 Distribución de las Direcciones IPV4 64
3.4.4 Distribución de las Direcciones IP para cada VLAN 66
3.4.5 Elaboración de las tablas de enrutamiento 68
3.4.6 Servicios de la Intranet 68
3.5 LEVANTAMIENTO Y OBTENCION DEL DIAGRAMA FISICO 71
3.5.1 Características de los Equipos de Red 72
3.5.1.1 Servidores 73
3.5.1.2 PC’s 74
3.5.1.3 Firewall 74
3.5.1.4 Router 75
3.5.1.5 Switch 75
3.5.1.6 Teléfonos IP 76
CAPITULO IV. DISEÑÓ DE LA SOLUCION IPV6 PARA LA UNIVERSIDAD POLITECNICA SALESIANA SEDE CUENCA 78
4.1 Metodología de Implementación de la red IPV6 78
4.2 Conexión a Internet mediante IPV6 79
4.2.1 Selección de un proveedor de servicios 79
4.3 Protocolos de enrutamiento 81
4.3.1Configuración del protocolo OSPF en IPV6 81

4.3.2 Configuración del protocolo RIP en IPV6 82
4.3.3 Configuración de rutas estáticas en IPV6 83
4.4 Escenarios de Transición a IPV6 83
4.4.1 Primer Escenario: Mantener IPv4 al mundo y tener IPv6 en la red local 83
4.4.1.1 Comandos de Configuración del Primer Escenario 84
4.4.2 Segundo Escenario: Tener IPV6 en el mundo y tener IPV6 en la red local 86
4.4.2.1 Comandos de Configuración del Segundo Escenario 87
4.5 DISEÑO DEL DIAGRAMA LÓGICO 90
4.5.1 Diseño de la Topología de red IPV6 90
4.5.2 Diseño de las VLANS en IPV6 91
4.5.2.1 Configuración de VLANS usando IPV6 91
4.5.3 Reglas de conectividad entre VLANS para IPV6 92
4.5.4 Direccionamiento IPv6 en la red de la UPS Sede-Cuenca 92
4.5.4.1 Distribución de direcciones IPV6 para cada VLAN 93
4.5.4.2 Elaboración de las tablas de enrutamiento sobre IPV6 95
4.5.5 Servicios de la Intranet sobre IPV6 97
4.5.5.1 Configuración de un Servidor Web 97
4.5.5.2 Configuración del correo electrónico Zimbra 99
4.5.6 Evaluación del Diagrama Lógico 100
4.6 DISEÑO DEL DIAGRAMA FISICO 100
4.6.1 Evaluación del Diagrama Físico 100
4.6.1.1 Hardware 101
4.6.1.2 Software 101
CAPITULO V. DESARROLLO DEL PLAN DE IMPLEMENTACIÓN 103
5.1 Consideraciones Generales 103
5.2 Perspectiva general de la metodología 104
5.2.1 Fase 1. Situación actual 104
5.2.2 Fase 2. Modelo de Negocios/Organización 106
5.2.3 Fase 3. Modelo de Tecnologías de la Información 108
5.2.4 Fase 4. Modelo de planeación 110
5.2.4.1 Aspectos Generales 110
5.2.4.2 Prioridades de Implementación 111
5.2.4.3 Plan de Implementación 113
5.2.4.4 Impacto en la Implementación de IPV6 117
5.2.4.5 Costos de Implementación 118
5.2.4.5.1 Costos de Software 118
5.2.4.5.2 Costos de Hardware 120
5.2.4.5.3 Costos de RRHH 120
5.2.4.5.4 Costos de Capacitación 120
5.2.4.6 Formas de pago y financiación 121

5.2.4.7 Riesgos del proyecto 122
5.2.4.8 Plan de contingencia 122
5.2.4.9 Riesgos de no implementar IPV6 123
CONCLUSIONES 125
RECOMENDACIONES 128
GLOSARIO 129
REFERENCIAS 140
ANEXOS 158

INDICE DE FIGURAS

Figura 1 CAP II. Campos del encabezado de paquetes IPV6 20
Figura 2 CAP II. Formato de la cabecera del protocolo IPv4 22
Figura 3 CAP II. Formato de la cabecera del protocolo IPv6 22
Figura 4 CAP II. Formato de un mensaje ICMPV6 25
Figura 5 CAP II. Protocolos de enrutamiento 27
Figura 6 CAP II. Partes de una dirección Local de enlace 30
Figura 7 CAP II. Partes de una dirección Local de sitio 31
Figura 8 CAP II. Partes de una dirección Global 31
Figura 9 CAP III. Topología referencial de la UPS Sede-Cuenca 43
Figura 10 CAP III. Función de los Servidores 45
Figura 11 CAP III. Interfaz gráfica del Software TracePlus/Ethernet v 5.51.00 48
Figura 12 CAP III. Topología en estrella extendida 61
Figura 15 CAP III. Diagrama Físico de la UPS Sede-Cueca 71
Figura 16 CAP IV. Mecanismo de Transición Dual Stack 79
Figura 17 CAP IV. Mantener IPV4 al mundo y tener IPV6 en la red local 84
Figura 18 CAP IV. Tener IPV6 en el mundo y tener IPV6 en la red local 87
Figura 19 CAP V. Cantidad de host en Internet 104
Figura 20 CAP V. Desarrollo de sistemas con IPV6 habilitado por defecto 109
Figura 21 CAP V. Vulnerabilidad de IPV6 a lo largo del tiempo 124

INDICE DE TABLAS

Tabla 1 CAP II. Sitio web asociado a diferentes tipos de registros 24
Tabla 2 CAP II. Registro PRT 24
Tabla 3 CAP III. Edificios de la UPS Sede-Cuenca 49
Tabla 4 CAP III. Distribución de los tipos de racks y gabinetes 52
Tabla 5 CAP III. Características de los racks abiertos 52
Tabla 6 CAP III. Características de los racks cerrados 52
Tabla 7 CAP III. Características de los gabinetes 53
Tabla 8 CAP III. Características del Patch Panel 53
Tabla 9 CAP III. Características del Cable UTP CAT.6 54
Tabla 10 CAP III. Características del Patch Cord 54
Tabla 11 CAP III. Características de los Racks para servidores 57
Tabla 12 CAP III. Características de los Racks de Datos 58
Tabla 13 CAP III. Nombre de las VLANS configuradas en el Packet Tracer 62
Tabla 14 CAP III. Reglas de Acceso entre VLANS 63
Tabla 15 CAP III. Clase de Direcciones IPv4 y Número de host 64
Tabla 16 CAP III. Requerimientos de hosts y porcentaje de crecimiento futuro 65
Tabla 17 CAP III. Direcciones IPv4 para cada subred 66
Tabla 18 CAP III. Datos principales de la Configuración de VLANS 67
Tabla 19 CAP III. Tabla de enrutamiento del Router Principal 68
Tabla 20 CAP III. Tabla de enrutamiento del Router Firewall 68
Tabla 21 CAP III. Características de los Servidores 73
Tabla 22 CAP III. Aplicaciones Instaladas en los Servidores 73
Tabla 23 CAP III. Características de las PC's de los Laboratorios 74
Tabla 24 CAP III. Características de las PC's del Área Administrativa 74
Tabla 25 CAP III. Características del Firewall 74
Tabla 26 CAP III. Características del Router 75
Tabla 27 CAP III. Características del Switch CISCO 75
Tabla 28 CAP III. Características del Switch 3COM 76
Tabla 29 CAP III. Teléfono IP CISCO 7911G 76
Tabla 30 CAP III. Teléfono IP CISCO 7912G 77
Tabla 31 CAP III. Teléfono IP CISCO 7941G 77
Tabla 32 CAP IV. Número de Direcciones IPV6 disponibles 93
Tabla 33 CAP IV. Configuración de VLANS sobre IPV6 94
Tabla 34 CAP IV. Escenario1 Tabla de enrutamiento del Router Principal 95
Tabla 35 CAP IV. Escenario1 Tabla de enrutamiento de Router-Firewall 95
Tabla 36 CAP IV. Escenario2 Tabla de enrutamiento del Router Principal 96
Tabla 37 CAP IV. Escenario2 Tabla de enrutamiento del Router Firewall 97
Tabla 38 CAP IV. Evaluación del Diagrama Lógico 100
Tabla 39 CAP IV. Análisis de los Equipos 101
Tabla 40 CAP IV. Análisis del S.O de los Servidores 102
Tabla 41 CAP IV. Análisis del S.O de los PC's 102
Tabla 42 CAP V. Aplicaciones de uso común con soporte para IPV6 110
Tabla 43 CAP V. Análisis de los costos del Software 119

Tabla 44 CAP V. Análisis de los costos de Capacitación 120
Tabla 45 CAP V. Riesgos del Proyecto 122
Tabla 46 CAP V. Plan de Contingencia 123

SIMBOLOGIA

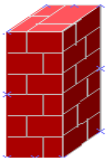
A continuación se presenta una descripción acerca de la simbología utilizada en los diagramas presentados en este proyecto de tesis:

Router

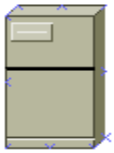
Access Point

Switch

Teléfono IP



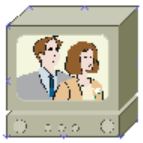
Firewall



Servidor

PC de escritorio

Portátil



TV

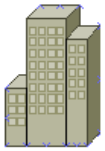
Nube

Medios LAN

Medios WAN

Medios inalámbricos

Universidad



Edificio UPS

Casa

[1]

[1] Cisco Systems, Inc., Simbología obtenida del Software Día Versión 0.96.1, 2012.

INTRODUCCION

En la actualidad se ha podido observar que las tecnologías de información y comunicaciones (TIC) se han convertido en parte fundamental de nuestras vidas.

Durante los últimos años se ha venido desarrollando diferentes tecnologías y servicios que nos permiten comunicarnos con las personas alrededor del mundo.

Con el pasar del tiempo los medios de comunicación tradicionales que causaron una gran aceptación hace algunos años atrás como la televisión, telefonía y mensajería convergen hacia una única red de comunicaciones conocida como internet.

El internet es la red de computadoras más grande de todo el mundo, de las que forman parte miles de redes que se encuentran distribuidas en todo el planeta, con un gran número de usuarios que participan en esta red. En un principio la conexión solo era posible entre dos computadoras usando una línea telefónica o comunicación por un puerto serie o paralelo, pero debido al crecimiento de la red este sistema quedo obsoleto.

En 1984 el Organismo Internacional para la Estandarización (ISO) realizó varias investigaciones de modelos de conexión de red (DECnet, SNA, TCP/IP) con el fin de solucionar los problemas de incompatibilidad con las redes antiguas de las empresas, dando origen al modelo de referencia de Interconexión de Sistemas Abiertos (OSI).

Luego de solucionar los problemas de incompatibilidad de redes el internet ha tenido un enorme crecimiento que ha evolucionado desde una red simple que conecta computadores a una plataforma que otorga diversos servicios de última tecnología.

Debido a este crecimiento se ha descubierto las debilidades del protocolo IPV4 como una forma de interconectar un reducido número de redes sin imaginar que se llegaría a alcanzar una red de millones de usuarios.

Durante la década de los 90 se ha desarrollado el protocolo IPV6 con el fin de sustituir y solucionar los problemas fundamentales de IPv4. Una de las ventajas más importantes de IPV6 es el gran número de direcciones disponibles que facilitan la implementación de modelos de seguridad y calidad de servicio dentro de las empresas.

A partir del 6 de Junio del 2012 ha iniciado el despliegue oficial del nuevo protocolo de direcciones IP en Internet, el cual permitirá el crecimiento y evitará el colapso de direcciones con el agotamiento del protocolo anterior IPV4.

Por el momento las empresas y las organizaciones no admitirán ningún cambio debido a que deberán convivir con el protocolo actual, ya que es un tema que en principio afectará a los más grandes proveedores de servicios y organismos que trabajan en la red.

El método tradicional mediante el cual las empresas, universidades y otros organismos han adoptado para la implementación de IPv6 es el Dual Stack, debido a que se puede aplicar en diferentes puntos de la red como en equipos clientes, servidores y routers. Este método permite ejecutar los protocolos IPV4 e IPV6 de manera simultánea en los nodos de una red, donde cada nodo tiene asignada direcciones IPV4 e IPV6.

El principal objetivo de este proyecto de tesis es realizar un estudio para la migración a IPV6 en la red de la UPS Sede-Cuenca. El presente trabajo pretende realizar un análisis de los mecanismos y requerimientos necesarios para llevar a cabo el proceso de migración en donde se deberá tomar en cuenta los conceptos y fundamentos de IPV6 con el fin de poder desarrollar un plan para la migración.

Los resultados de este proyecto constituyen el primer paso para una futura migración a IPV6 en todos los servicios que ofrece la red de la UPS Sede-Cuenca.

En el Capítulo 1, se presenta los objetivos principales de este proyecto además se realiza un análisis de la situación actual de la red de la UPS Sede-Cuenca.

En el Capítulo 2, se presenta un estudio completo acerca de las características de IPV6 como sus protocolos principales, direccionamiento, mecanismos de transición, ventajas y desventajas, etc.

En el Capítulo 3, se presenta el levantamiento de información IPV4 de la red de la UPS Sede-Cuenca en donde se realiza la identificación de la red, la distribución del cableado (horizontal y vertical) y la obtención del diagrama lógico y físico.

En el Capítulo 4, se presenta el diseño de la solución IPV6 para la red de la UPS Sede-Cuenca en donde se define la metodología de implementación, los protocolos de enrutamiento, los escenarios de transición, etc.

En el Capítulo 5, se presenta el desarrollo del plan de implementación basado en el Plan Estratégico de Tecnologías de la Información (PETI) que está compuesta por 15 módulos constituidos en 4 fases.

Finalmente se presentan las conclusiones y recomendaciones extraídas del proyecto, además se incluye un glosario de términos y los anexos con características importantes de los equipos y configuraciones de IPV6.

CAPITULO I

ASPECTOS FUNDAMENTALES

1.1 ANTECEDENTES

En la actualidad la Universidad Politécnica Salesiana, cuenta con una red basada en IPV4 cuya versión se utiliza desde 1981. Esta versión utiliza un direccionamiento de 32 bits, en la que cada dirección está formada por cuatro grupos binarios de 8 bits, dando como resultado un total de 4.294.967.296 direcciones máximas disponibles.

El crecimiento exponencial de Internet y la cantidad de dispositivos móviles que utilizan el protocolo TCP/IP como las cámaras IP, teléfonos móviles, PDA'S, está llevando hacia el agotamiento de las direcciones IPv4.

La entrega de los últimos bloques de direcciones IPV4 realizada por la IANA ha despertado a nivel mundial un amplio interés por el tema, debido a esto se ha determinado que la Universidad Politécnica Salesiana necesita realizar un amplio estudio para la migración al nuevo protocolo IPV6, por lo cual es necesario llevar a cabo un plan de análisis con el fin de conocer las características y las ventajas sobre este tema.

1.2 SITUACION ACTUAL DE LA RED DE LA UNIVERSIDAD POLITÉCNICA SALESIANA

En la actualidad la Universidad Politécnica Salesiana se encuentra formada por 3 sedes ubicadas en las ciudades principales del Ecuador como son Quito, Guayaquil y Cuenca. La red general de la Universidad Politécnica Salesiana se encuentra formada por 3 redes LAN una para cada sede, la interconexión entre estas redes se realiza a través de un Router ubicado en el Centro de Distribución Principal del Cableado (MDF) de cada una de las sedes.

En nuestro caso se llevará a cabo un análisis referencial de la topología de red, la distribución del cableado y los equipos con el fin de llevar a cabo un plan para la migración a IPv6 de la red LAN de la Universidad Politécnica Salesiana Sede-Cuenca.[2]

1.3 JUSTIFICACIÓN

Debido a la gran demanda de direcciones IP, el agotamiento de las direcciones IPV4 disponibles, tablas de enrutamiento de gran tamaño y la falta de funcionalidad para dar seguridad, eficiencia y calidad de servicio en la red, las Universidades a nivel mundial, al ser núcleo de investigación e implementación de nuevas tecnologías y al estar en la dinámica del cambio y análisis tecnológico, deben ser una de las pioneras en la migración al nuevo direccionamiento IP a nivel mundial.

Mediante el plan de implementación hacia el nuevo protocolo IP se podrá realizar un análisis sobre la estructura de la cabecera IPV6, conocer su direccionamiento y el impacto que produciría la implementación del protocolo IPV6 en la red de la Universidad Politécnica Salesiana.

1.4 OBJETIVOS

GENERAL:

Proponer la elaboración de un Plan de Implementación para la migración a IPV6 en la red de la Universidad Politécnica Salesiana Sede-Cuenca.

ESPECÍFICOS:

- Analizar la situación actual del cableado estructurado en la red de la UPS Sede-Cuenca.
- Investigar los diferentes mecanismos de transición para la migración a IPV6.
- Desarrollar un análisis de ventajas y desventajas de la migración.
- Presentar el diseño de la solución de IPV6.
- Desarrollar el Plan de Implementación para la migración de IPV4-IPV6.

[2] P. Jimenez, entrevista personal, 19 de Septiembre del 2011.

CAPITULO II

MARCO TEÓRICO

2.1 CABECERA DE IPV6

El origen de IPv6 comenzó en 1991, cuando la IETF (Internet Engineering Task Force) - empezó a estudiar el problema de expandir el número de direcciones de Internet realizando un cambio en la cabecera del protocolo lo que significaba una nueva versión de IP.

El protocolo IPv6 es un protocolo que permite aumentar el tamaño de direcciones IP de 32 a 128 bits, es decir 2^128 posibles direcciones. Este aumento en el espacio de direcciones no sólo proporciona mayor número de hosts, sino una jerarquía de direcciones mayor.

La cabecera IPv6 elimina o hace opcionales varios de los campos de la cabecera IPv4, con el fin de obtener una cabecera de tamaño fijo, más simple y reduciendo el tiempo de procesamiento de los paquetes.[3]

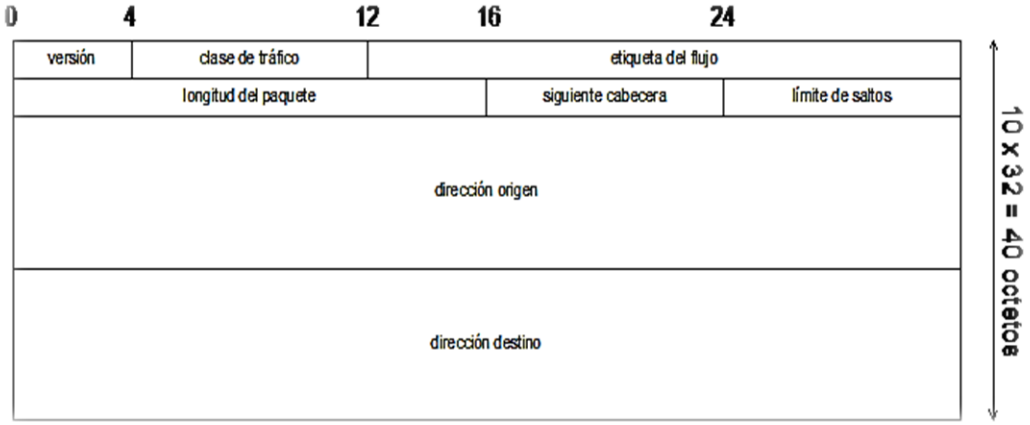


Figura 1 CAP II. Campos del encabezado de paquetes IPV6

Fuente: Ramón, M. (2001), Cabecera de IPV6, Obtenida el 20 de Julio del 2011, de http://www.ramonmillan.com/tutoriales/ipv6_parte1.php#cabeceraipv6

[3] RAMOS, I. (2011), "IPV4-IPV6", Obtenida el 06 de Abril del 2011, de http://es.scribd.com/doc/52418918/IPV4-IPV6.

"La cabecera básica de IPv6, tiene una longitud fija de 40 octetos y está compuesta de los siguientes campos:

***Versión (4 bits):** es el número de versión de IP, es decir 6.*

***Clase de tráfico (8 bits):** el valor de este campo especifica la clase de tráfico. Los valores de 0 - 7 están definidos para el tráfico de datos con control de la congestión, y de 8-15 para tráfico de vídeo y audio sin control de congestión.*

***Etiqueta del flujo (20 bits):** el estándar IPv6 define un flujo como una secuencia de paquetes enviados desde un origen específico a un destino. Un flujo se identifica únicamente por la combinación de una dirección fuente y una etiqueta de 20bits. De este modo, la fuente asigna la misma etiqueta a todos los paquetes que forman parte del mismo flujo.*

***Longitud del paquete (16 bits):** especifica el tamaño total del paquete, incluyendo la cabecera y los datos, en bytes. Es necesario porque también hay campos opcionales en la cabecera.*

***Siguiente cabecera (8 bits):** indica el tipo de cabecera que sigue a la cabecera fija de IPv6, por ejemplo, una cabecera TCP/UDP, ICMPv6 o una cabecera IPv6 opcional.*

***Límite de saltos (8 bits):** es el número de saltos máximo que le quedan al paquete. El límite de saltos es establecido a un valor máximo por el origen y reducido en 1 cada vez que un nodo encamina el paquete. Si el límite de saltos es reducido y toma el valor 0, el paquete es descartado.*

***Dirección origen (128 bits):** es la dirección del origen del paquete.*

***Dirección destino (128 bits):** es la dirección del destino del paquete."*[4]

[4] MILLÁN, R. (2001), El Protocolo IPV6, Obtenida el 25 de Julio del 2011, de http://www.ramonmillan.com/tutoriales/ipv6_parte1.php.

A continuación en la Figura 2 y 3, podemos observar como se ha reducido el tamaño de los 12 campos de la cabecera del protocolo IPv4 a 8 campos en IPv6.

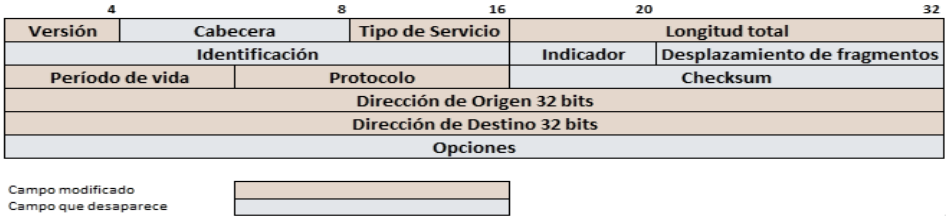


Figura 2 CAP II. Formato de la cabecera del protocolo IPv4

Fuente: El Autor

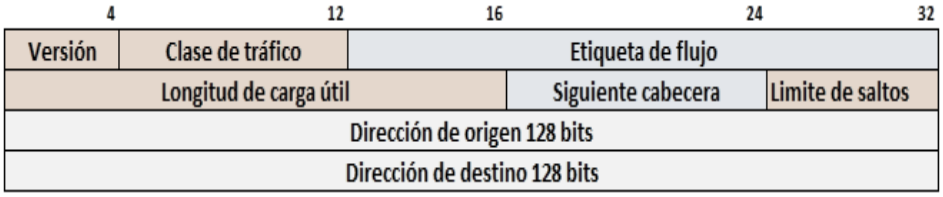


Figura 3 CAP II. Formato de la cabecera del protocolo IPv6

Fuente: El Autor

El motivo fundamental por el cual estos campos (tipo de servicio, indicadores, identificación y control de errores) son eliminados es la innecesaria redundancia, en IPv4 se está facilitando la misma información de diversas formas, como es el caso del campo de control de errores.

En la Figura 3 podemos ver que el campo de desplazamiento de fragmentación de IPv4 ha sido eliminado, porque los paquetes ya no son fragmentados en los nodos intermedios, en IPv6 es un proceso que se produce extremo a extremo. El único campo realmente nuevo en la cabecera del protocolo IPv6 es la etiqueta de flujo.[5]

2.2 DESCRIPCION DE IPV6

IPv6 es la nueva versión del protocolo IP que ha sido diseñado por el IETF[6] para reemplazar en forma gradual a la versión actual de IPv4.

[5] MILLÁN, Ramón, Art. Cit. p.20.
[6] IETF (Internet Engineering Task Force): Grupo Especial sobre Ingeniería de Internet.

(Ramírez y Cervantes, 2005)[7] nos presentan algunas de las características más importantes sobre IPV6:

- Ofrece un mayor espacio de direcciones. El tamaño de las direcciones IP cambian de 32 bits a 128 bits, con el fin de soportar mayores niveles de jerarquía de direccionamiento.
- Simplificación del formato de la cabecera IPv4 debido a que algunos campos se quitan o se hacen opcionales.
- Permite obtener paquetes IP eficientes y extensibles.
- Posibilidad de paquetes con una carga útil (datos) de más de 65.355 bytes.
- Calidad de servicio (QoS) y clase de servicio (CoS).
- Seguridad en el núcleo del protocolo (IPsec).
- Capacidad de etiquetas de flujo que pueden ser usadas por un nodo origen para etiquetar paquetes pertenecientes a un flujo de tráfico particular.

2.2.1 Resolución de Nombres de IPV6[8]

El Sistema de Nombres de Dominio (DNS) no puede ser fácilmente extendido para dar un soporte eficiente a las direcciones IPV6 debido a que las aplicaciones luego de ser consultadas retornan solamente direcciones IPV4 de 32 bits.
Para dar un soporte adecuado a las direcciones IPV6 se debe definir lo siguiente:

- Un nuevo tipo de registro con el fin de relacionar un nombre de dominio con una dirección IPv6.
- Un nuevo dominio con el fin de brindar un soporte hacia las búsquedas basadas en la dirección IPV6.

[7] RAMIREZ, Sergio, y CERVANTES, María, (2005), "Introducción a IPV6", Obtenida el 26 de Julio del 2011, de http://www.rau.edu.uy/ipv6/queesipv6.htm#01
[8] Thomson, S. y Huitema, C. (1995), Extensiones al DNS para dar soporte a IPV6, Obtenida el 01 de Agosto del 2011, de http://www.rfc-es.org/rfc/rfc1886-es.txt

La definición de un nuevo tipo de registro permite almacenar la dirección IPV6 de un host. En algunos casos un host tiene varias direcciones IPV6 por lo cual deberá tener más de un registro similar.

2.2.1.1 Tipos de registro

Existe un nuevo tipo de registro de recurso "AAAA" cuya función es almacenar una sola dirección IPV6, su equivalente en IPV4 es el registro "A".

A continuación presentamos un ejemplo de un sitio web con los dos tipos de registros:

Tabla 1 CAP II. Sitio web asociado a diferentes tipos de registros

Tipo de Registro	Formato
A	www.ups.edu.ec A 200.0.32.2
AAAA	www.ups.edu.ec AAAA 3FFE:YYYY:C18:1::2

Fuente: Cisco Systems, Inc., *CISCO IOS IPV6 Configuration Guide*, (2008), USA: Autor.

Ahora podemos decir que el proceso de resolución inversa del nombre de dominio IPV6 utiliza el tipo de registro de recurso "PTR" cuyo equivalente en IPV4 es el mismo.

Una dirección IPv6 se representa por una secuencia de nibbles separados por puntos con el sufijo ".IP6.INT". La secuencia de nibbles se codifican en orden inverso es decir primero el nibble de menor orden, seguido por el siguiente nibble de menor orden, etc.

Finalmente cada nibble se representa por un dígito hexadecimal, a continuación tenemos un ejemplo:

Tabla 2 CAP II. Registro PTR

Tipo de Registro	Formato
PTR	2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.1.c.0. y.y.y.y.e.f.f.3.ip6.int PTR www.ups.edu.ec

Fuente: Cisco Systems, Inc., *CISCO IOS IPV6 Configuration Guide*, (2008), USA: Autor.

2.2.2 Protocolos Principales de IPV6

2.2.2.1 Protocolo ICMPv6[9]

El protocolo ICMPv6 es utilizado por los nodos IPV6 con el fin de informar sobre los errores encontrados durante el procesamiento de los paquetes y para realizar otras funciones relativas a la capa de internet como son los diagnósticos (“ping”).

Los mensajes ICMPV6 se dividen en dos tipos:

1. **Mensajes de error:** se identifican con un 0 en su campo “Tipo de mensaje” y sus valores van desde 0 a 127.
2. **Mensajes informativos:** sus valores están entre 128 y 255.

“Mediante ICMPv6, los hosts y los enrutadores que se comunican mediante IPv6 pueden informar sobre los errores que se presentan y enviar mensajes de eco simples.”[10]

A continuación podemos observar el formato de un mensaje ICMPV6:

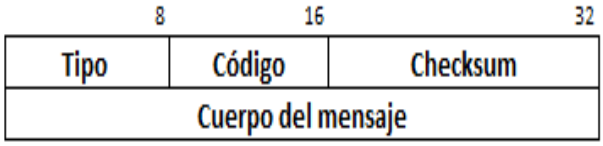


Figura 4 CAP II. Formato de un mensaje ICMPV6

Fuente: El Autor

2.2.2.2 Descubrimiento de escucha de multidifusión (MLD)

Como su nombre lo indica la multidifusión consiste en enviar una serie de mensajes ICMPV6 a un solo destino pero el procesamiento se produce en múltiples host.

[9] S. Deering, (1998), ICMPv6 para IPV6, Obtenida el 11 de Agosto del 2011, de http://www.ietf.org/rfc/rfc2463.txt

[10] MICROSOFT, (n.d), Protocolo de mensajes de control de Internet para IPV6 (ICMPV6), Obtenida el 11 de Agosto del 2011, de http://technet.microsoft.com/es-es/library/cc757063%28WS.10%29.aspx

De acuerdo al concepto citado en el párrafo anterior podemos decir lo siguiente:

- El conjunto de host que atienden en una sola dirección de multidifusión se conoce como grupo de multidifusión.
- Los grupos de multidifusión son dinámicos.
- Un host puede unirse a un grupo de multidifusión mediante él envió de mensajes.
- Un host puede enviar tráfico a diferentes direcciones de grupo.

El objetivo de los mensajes MDL es poder intercambiar información acerca del estado entre los enrutadores IPV6 y los miembros de cada uno de los grupos de multidifusión.

2.2.2.3 Descubrimiento de vecinos (ND)

El protocolo de Descubrimiento de vecinos puede ser utilizado por un host, router o nodo y ofrece diferentes funciones:

En un host:

- Permite descubrir enrutadores vecinos.
- Permite descubrir direcciones y otros parámetros de configuración.

En un router:

- Permite notificar su presencia mediante diferentes parámetros de configuración de host.
- Permite notificar a los host sobre la mejor dirección del siguiente salto.

En los nodos:

- Permite resolver la dirección IPV6 de un nodo vecino.
- Permite determinar si se pueden enviar y recibir paquetes IPV6 de un vecino.

2.2.3 Protocolos de enrutamiento:

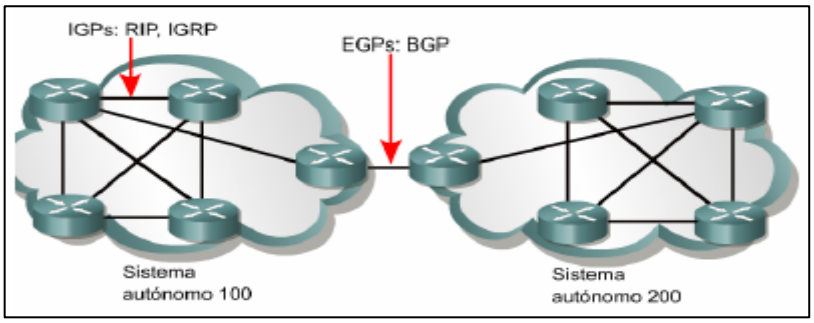


Figura 5 CAP II. Protocolos de enrutamiento

Fuente: Staky, *CCNA 1 and 2 Versión 3.1 Curriculum en formato pdf*, (n.d), p. 218.

En la actualidad IPV6 adopta los mismos protocolos de enrutamiento que se utilizan en las redes IPV4 a continuación presentamos los siguientes:

1. IGP: Protocolo de enrutamiento de Gateway Interior.
Ejemplos: RIPng, OSPFv3.

2. EGP: Protocolo de enrutamiento de Gateway Exterior.
Ejemplo: BGP.

2.2.3.1 RIPng para IPV6[11]

Este protocolo está diseñado para que los routers puedan intercambiar información de rutas a través de una red basada en IPV6.

RIPng es un protocolo de enrutamiento vector-distancia cuya finalidad es determinar mediante la métrica la dirección y la ruta más óptima de forma automática.

[11] G. Malkin, y R Minnear, (1997), RIPng for IPv6, Obtenida el 12 de Agosto del 2011, de http://www.ietf.org/rfc/rfc2080.txt

Cada router que implementa RIPng tiene una tabla de enrutamiento el cual posee una entrada para cada destino que se quiere alcanzar en todo el sistema de funcionamiento RIPng.

Cada entrada de la tabla de enrutamiento contiene la siguiente información:

- El prefijo IPV6 de destino.
- Una métrica que representa el número de saltos desde el router al destino.
- La dirección IPV6 del siguiente router y la ruta hacia el destino.
- Una bandera para indicar el cambio de ruta.
- Varios contadores asociados con la ruta.

2.2.3.2 OSPFv3 para IPV6

OSPF es un protocolo de enrutamiento de estado de enlace desarrollado por la IETF en 1988, cuya función es responder rápidamente las actualizaciones o cambios que se producen en la red.

Este tipo de protocolo permite enviar actualizaciones periódicas por rangos más prolongados por ejemplo de 20 minutos.

Los algoritmos de estado de enlace utilizan sus bases de datos para crear entradas de tablas de enrutamiento que prefieran la ruta más corta. [12]

A continuación presentamos una comparación acerca de las características de OSPFv3 y OSPFv2:

- *"OSPFv3 se amplia de OSPFv2 con el fin de proporcionar soporte para el enrutamiento IPV6.*
- *OSPFv3 permite obtener un mayor tamaño de direcciones IPV6.*
- *Para el proceso de enrutamiento se debe activar la configuración de OSPFv3 sobre una interfaz asociada.*

[12] Staky, *CCNA 1 and 2 Versión 3.1 Curriculum en formato pdf,* (n.d), p.219.

- *En OSPFv3 cada interfaz debe ser activada utilizando comandos sobre el modo de configuración de la interfaz.*

- *En IPV6 los usuarios pueden configurar varias direcciones sobre una interfaz. En OSPFv3 se incluyen todas las direcciones en una interfaz por defecto.*

- *A diferencia de OSPFv2 se puede ejecutar varias instancias de OSPFv3 en un solo enlace.”*[13]

2.2.3.3 BGP-4

La función de este protocolo es intercambiar información de enrutamiento entre sistemas autónomos de tal forma que garantiza la elección de una ruta libre de loops.

A continuación veremos algunas de las características de este protocolo:

- BGP es uno de los principales protocolos de publicación de rutas más utilizados por las compañías e ISP’s en Internet.

- BGP toma decisiones de enrutamiento basadas en las políticas o reglas de una red.

- La relación entre routers BGP se mantiene con el envio de paquetes cada 60 segundos.

2.2.4 Direccionamiento IPV6

Las direcciones pasan de los 32 a 128 bits, es decir de 2^32 direcciones (4.294.967.296) a 2^128 direcciones (3.402823669 e38). Durante las investigaciones realizadas acerca del direccionamiento en IPV6, Ramos (2011, p.13) afirma que existen tres tipos de direcciones:

[13] Cisco Systems, Inc. (2003-211), Implementing OSPF for IPV6, Obtenida el 23 de Agosto, de http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-ospf.html#wp1069815.

2.2.4.1 Direcciones Unicast o unidifusión

Este tipo de direcciones permite identificar una sola interfaz, es decir cuando un paquete es enviado a una dirección *unicast* este será entregado solo a la interfaz identificada con dicha dirección.

A continuación se describe los tipos de direcciones Unicast:

1. Local de enlace

Este tipo de direcciones permite identificar interfaces en un mismo enlace de red local. Se utiliza en los procesos de descubrimiento de vecinos y siempre se configura de forma automática.

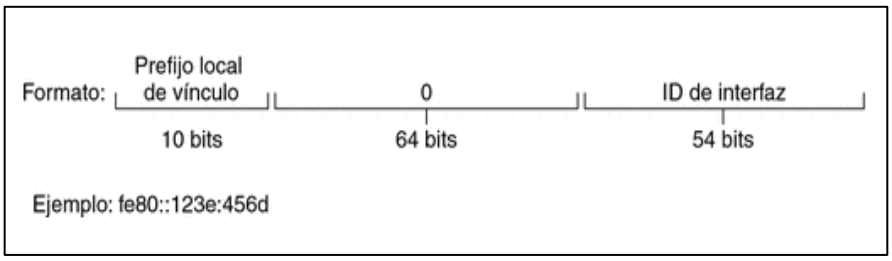


Figura 6 CAP II. Partes de una dirección Local de enlace

Fuente: ORACLE, (2010), Capitulo 3. Introducción a IPV6, Obtenida el 23 de Agosto, de http://docs.oracle.com/cd/E19957-01/820-2981/ipv6-overview-7/index.html

Como podemos observar en el ejemplo de la Figura 6 las direcciones Locales de enlace siempre comienzan por fe80.

- **Prefijo local de vínculo:** representa fe80::ID_Interfaz /10
- **ID_Interfaz:** dirección hexadecimal de la interfaz, que en general se deriva de la dirección MAC DE 48 bits.

2. Local de sitio

Este tipo de direcciones permite identificar interfaces en un mismo sitio. El ámbito de una dirección local de sitio es el mismo sitio (conjunto de redes de la organización).

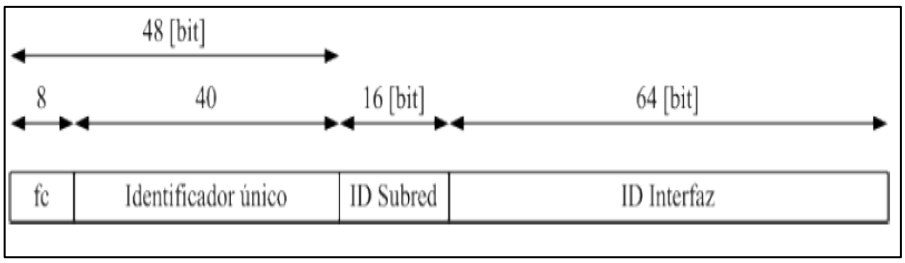


Figura 7 CAP II. Partes de una dirección Local de sitio

Fuente: Felipe Jara, (2009), Estudio e Implementación de una red IPV6 en la UTFSM, p.20

Como podemos observar en la Figura 7, los primeros 48 bits siempre son fijos y comienzan por fe::/48.

Luego del identificador único se presenta el identificador de subred de 16 bits con el cual se puede crear subredes dentro de una empresa.

Finalmente se encuentra el campo ID Interfaz de 64 bits el cual nos permite identificar una interfaz específica de una subred.

3. Global: este tipo de direcciones permite identificar interfaces en el internet cuyo equivalente son las direcciones públicas en IPV4.

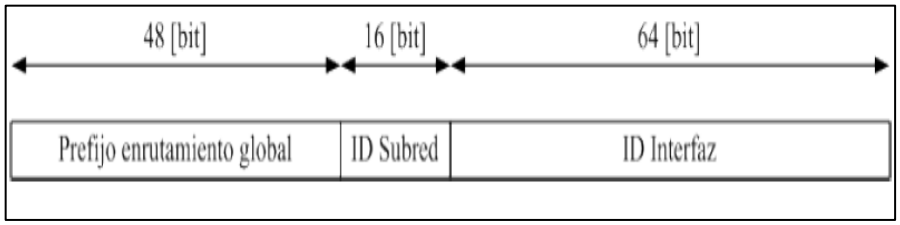


Figura 8 CAP II. Partes de una dirección Global

Fuente: Felipe Jara, (2009), Estudio e Implementación de una red IPV6 en la UTFSM, p.21

Como podemos observar en la Figura 8, el prefijo de enrutamiento global permite identificar un sitio conectado a internet, a continuación tenemos el ID de Subred que permite identificar una subred dentro de un sitio y finalmente el ID de Interfaz que permite identificar una interfaz de un determinado nodo.

2.2.4.2 Direcciones Anycast

Este tipo de direcciones permiten identificar un grupo de interfaces, es decir cuando un paquete es enviado a una dirección *anycast* este será entregado a cualquiera de las interfaces identificadas con dicha dirección.

2.2.4.3 Direcciones Multicast

Este tipo de direcciones permiten identificar un grupo de interfaces, es decir cuando un paquete es enviado a una dirección *multicast* este será entregado a todas las interfaces identificadas por dicha dirección.

2.2.5 Representación de direcciones IPv6

Una dirección IPV6 tiene un tamaño de 128 bits y se divide en 8 campos de 16 bits, en donde cada bloque se convierte a un número hexadecimal de 4 dígitos separado por un signo de dos puntos.

Ejemplo:

21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A

A continuación presentamos las formas de representar una dirección IPV6:

- Se puede eliminar los ceros iniciales de cada bloque de 16 bits, pero cada bloque debe tener al menos un dígito.

Por ejemplo: 21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A
Se puede representar como: 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A

- Cuando una dirección contiene varios grupos de ceros se puede reemplazar por el símbolo "::".

Por ejemplo: FE1A:4CB9:001B:0000:0000:12D0:005B:06B0
Se puede representar como: FE1A:4CB9:1B::12D0:5B:6B0

Nota: La compresión de ceros se puede utilizar una sola vez en una dirección dada.

- Cuando existe un escenario con nodos IPV4- IPV6 la dirección queda de la siguiente forma:

Ejemplo: 0000:0000:0000:0000:0000:0000:192.168.10.1

- Donde los ceros representan valores hexadecimales de 16 bits cada una.
- Los últimos bytes representan valores decimales de 8 bits cada una.

La dirección IP descrita en la parte superior se puede representar como:
::1928.168.10.1

2.2.5.1 Prefijos IPV6

Un prefijo es una parte de la dirección que indica los bits que tienen valores fijos o los bits del identificador de red.

Un prefijo de dirección IPV6 se representa como: ***dirección IPv6/longitud de prefijo.***

Ejemplo: 21DA:D3:0:2F3B::/64

2.2.6 Enrutamiento IPV6

Según Microsoft el enrutamiento es la parte de IPv6 que proporciona capacidades de reenvío entre hosts que se encuentran en segmentos independientes que pertenecen a una red mayor basada en IPv6.

A continuación se describen el proceso de enrutamiento en IPV6:

> *"El proceso de enrutamiento se da sobre el nivel IPv6, en donde los servicios de transporte del host de origen pasan los datos en forma de segmentos TCP o mensajes UDP al nivel IPv6. El nivel IPv6 crea los paquetes con la información de las direcciones de origen y destino, que se utiliza para enrutar los datos a través de la red. Finalmente el nivel IPv6 pasa los paquetes al nivel inferior del vínculo, donde los paquetes IPv6 se convierten en tramas para su transmisión a través de los medios específicos de una red física, este proceso se produce en el orden inverso en el host de destino."* [14]

2.2.6.1 Tablas de Enrutamiento IPV6

Las tablas de enrutamiento en IPV6 se utilizan para mantener información, con el fin de poder establecer una comunicación con redes y host remotos.

El procedimiento es el siguiente:

"Antes de enviar un paquete IPv6, el equipo inserta la dirección IPv6 de origen y la dirección IPv6 de destino (para el destinatario) en el encabezado IPv6. Luego el equipo examina la dirección IPv6 de destino, la compara con una tabla de enrutamiento IPv6 mantenida localmente y realiza la acción adecuada.

El equipo realiza una de las tres acciones siguientes:

- *Pasa el paquete a un nivel de protocolo superior a IPv6 en el host local.*
- *Reenvía el paquete a través de una de las interfaces de red conectadas.*
- *Descarta el paquete.*

Finalmente IPv6 busca en la tabla de enrutamiento la ruta más similar a la dirección IPv6 de destino. "[17]

[14] MICROSOFT, (n.d), Enrutamiento IPV6, Obtenida el 24 de Agosto del 2011, de http://technet.microsoft.com/es-es/library/cc758763%28v=ws.10%29

Según las investigaciones realizadas una tabla de enrutamiento en IPV6 esta formada por las siguientes entradas:

- *Prefijo de dirección*
- *Interfaz a través de la cual se envían los paquetes.*
- *Dirección del siguiente salto.*
- *Valor de preferencia: que se utiliza para seleccionar entre varias rutas que tengan el mismo prefijo.*
- *Duración de la ruta.*
- *Especificación cuando una ruta está publicada.*
- *Especificación de caducidad de la ruta.*
- *Tipo de ruta*.

2.3 VENTAJAS Y DESVENTAJAS DE IPV6

2.3.1 Ventajas del Protocolo IPv6

Según el Autor Iván Ramos (2011, p.10) las desventajas del protocolo IPV6 son las siguientes:

- Permite obtener direcciones más largas debido a que el tamaño de una dirección cambia de 32 a 128 bits, con un espacio disponible tan grande que no puede llegar a agotarse en un futuro previsible.

- Contiene un formato de cabecera flexible, es decir que utiliza un nuevo formato de datagrama que a diferencia de IPv4 utiliza un formato con un número fijo de octetos, IPv6 utiliza un conjunto opcional de cabeceras.

- Permite la fragmentación end-to-end, es decir que a todos los enrutadores se les elimina la función de fragmentar los paquetes que llegan debido al MTU.

- Permite un soporte para la reserva de recursos debido a que IPv6 reemplaza la especificación del tipo de recursos de IPv4 utilizando un mecanismo que permite la reserva de los recursos de red. Este mecanismo tiene la capacidad de soportar aplicaciones de video en tiempo real, cuyo requerimiento es garantizar el ancho de banda.

- Permite la provisión de extensiones al protocolo, debido a que se produce un desplazamiento de un protocolo a otro permitiendo características adicionales. Este tipo de capacidad de extensión permite que el protocolo se adapte a los cambios en el hardware de la red o las nuevas aplicaciones.

- Permite un número de saltos, es decir cuando se cambia el tiempo de vida de un paquete IPv4 por el número de saltos en IPv6 se garantiza que el paquete no será eliminado sin que tenga la opción de llegar hasta el nodo de destino.

2.3.2 Desventajas del Protocolo IPv6

Ramos (2011, p.10) afirma que los principales problemas que se presentan en IPV6 son los siguientes:

- El restablecimiento de la comunicación cuando un enlace se cae entre un par en enrutadores, de esta forma se afectan los siguientes factores:

  - El Tamaño de los fragmentos de acuerdo al mínimo MRU.
  - El Ancho de banda específico para esa comunicación.
  - El Retardo aceptable en la transmisión.

- La transición de IPv4 a IPv6 debido a la tecnología actual y a la gran cantidad de nodos con soporte IPv4 que existen en el mundo.

- La tecnología de enrutamiento exige que se utilicen buenas estrategias, debido a que no se podría eliminar en un solo día toda la cantidad de enrutadores que funcionan con IPv4. Además se deben crear nodos que soporten tanto IPv4 como IPv6 hasta cuando todos los nodos puedan llegar a comunicarse con la misma versión de IP.

2.4 MECANISMOS DE TRANSICIÓN IPV4-IPV6

El proceso de transición de IPv4 a IPv6 no se podrá realizar de un día para el otro ya que las dos versiones de IP deberán convivir durante algunos años. Es decir que el protocolo IPv6 puede ser implementado como una actualización de software en los nodos IPv4 actuales, para ello se establece un período de transición con el fin de minimizar los costes de los nuevos equipos y proteger las inversiones realizadas en las empresas tecnológicas.

Es muy complejo saber cuándo las operadoras en Internet podrán migrar a la tecnología IPv6 debido a que en la actualidad la mayoría de las operadoras utilizan nodos IPv4 y con esta situación resulta difícil lograr una mayor motivación para el cambio.

Las características de configuración hacen que las redes IPv6 sean más fáciles de configurar y mantener, todo esto puede resultar novedoso para las operadoras debido a que pueden realizar un despliegue de infraestructura muy rápido.

Además es muy importante tomar en cuenta que para facilitar la migración las aplicaciones IPv4 existentes deben ser capaces de operar con las aplicaciones IPv6 por ejemplo los navegadores de internet deben funcionar utilizando tanto IPv4 como IPv6.

Los mecanismos de transición se clasifican en 3 grupos importantes que son:

- Dual Stack (Doble Pila)
- Túneles
- Traducción

2.4.1 Dual Stack (Doble Pila)[15]

Este es uno de los métodos más utilizados en los procesos de transición, debido a que utiliza un nodo de doble pila IPv6/IPv4, que puede llegar a comunicarse tanto como un nodo IPv4 ó como un nodo IPv6, para lograr este proceso cada nodo IPv6/IPv4 debe tener configurado los dos tipos de direcciones.

La implementación del método Dual Stack permite activar o desactivar una de las pilas, por este motivo un nodo puede tener 3 modos de funcionamiento:

- Cuando la pila IPV4 esta activada y la pila IPV6 desactivada, se comporta como un solo nodo IPV4.
- Cuando la pila IPV6 esta activada y la pila IPV4 desactivada, se comporta como un solo nodo IPV6.
- Cuando se habilitan las pilas IPV4 e IPV6, el nodo puede utilizar los dos protocolos.

Un nodo IPv4/IPv6 utiliza una dirección para cada versión de protocolo.

Es muy importante mencionar que IPv4 utiliza mecanismos de configuración para direcciones IPV4 (configuración estática o DHCP) e IPv6 utiliza mecanismos de configuración para direcciones IPV6 (configuración estática o automática).

El DNS es utilizado por las dos versiones de protocolos para resolver los nombres y direcciones IP. Un nodo IPv6/IPv4 necesita una resolución DNS capaz de resolver los dos tipos de registros de direcciones DNS.

2.4.2 Tipo Túnel

Este método permite transmitir paquetes IPv6 por medio de una infraestructura IPv4, es decir se encapsula el contenido del paquete IPv6 en un paquete IPv4.

[15]HAGEN, Silvia, (n.d), IPV6 Essentials, Obtenida el 25 de Agosto del 2011, de http://es.scribd.com/doc/91049687/169/Configured-Tunneling-RFC-2893.

Ramón Millán (2001, parte II) afirma que el nodo IPv6 que hace frontera con el túnel, toma el paquete IPv6, y lo pone en el campo de datos de un paquete IPv4. Este paquete IPv4 tiene como dirección de destino el nodo IPv6 en la parte final del túnel y es enviado al primer nodo IPv4 que conforma el túnel. Los nodos IPv4 del túnel encaminan el paquete, sin tener constancia de que el paquete IPv4 que están manejando contiene un paquete IPv6. Finalmente cuando el paquete llega al extremo receptor IPv6 del túnel, este determina que el paquete IPv4 contiene un paquete IPv6 que debe ser extraído.

Los mecanismos de transición tipo túnel se dividen en 2 grupos:

2.4.2.1 Túneles manuales

Un paquete IPv6 es encapsulado en un paquete IPv4 para ser encaminado sobre una infraestructura de enrutamiento IPv4, estos son los túneles punto a punto que necesitan ser configurados manualmente.

2.4.2.2 Túneles automáticos

Los nodos IPv6 pueden utilizar diferentes tipos de direcciones compatibles con IPv4, IPv6 ó 6to4, el túnel automático es un túnel dinámico de paquetes IPv6 sobre una infraestructura de enrutamiento IPv4. La configuración de los túneles entre routers y host se pueden realizar de diferentes formas:

1. Router a Router: utiliza un mecanismo de túnel automático en donde los routers IPv6/IPv4 que están separados por una infraestructura IPv4 pueden encapsular paquetes IPv6 entre ellos mismos.

2. Host a Router: utiliza un mecanismo de túnel automático en donde un host IPv6/IPv4 puede encapsular paquetes IPv6 a un router intermedio IPv6/IPv4 que es accesible mediante una infraestructura de ruteo IPv4.

3. Host a Host: utiliza un mecanismo de túnel manual en donde los host IPv6/IPv4 que están interconectados por una infraestructura IPv4 pueden encapsular paquetes IPv6 entre ellos mismos.

4. Router a Host: utiliza un mecanismo de túnel manual en donde los routers IPv6/IPv4 pueden encapsular paquetes IPv6 a su destino final.

A continuación se describe las tecnologías de túnel automático:

2.4.2.2.1 Túnel 6to4

Este método 6to4 especifica un mecanismo para que los sitios de IPv6 puedan comunicarse entre sí a través de la red IPv4 sin la necesidad de establecer una configuración explícita del túnel.

La red de área amplia IPv4 es tratada como una capa de enlace punto a punto de unidifusión en donde los dominios de IPv6 se comunican a través de los routers 6to4 conocidos como puertas de enlace 6to4. Esto se realiza como un mecanismo de transición utilizado durante el período de coexistencia de IPv4 e IPv6.

"El método 6to4 utiliza el prefijo de dirección global:

2002:*WWXX*:*YYZZ*::/48

WWXX*:*YYZZ se refiere a la parte correspondiente al ID de agregación del siguiente nivel de una dirección global y la representación, en formato hexadecimal separado por dos puntos, de una dirección IPv4 pública **(*w.x.y.z*)** asignada al sitio o host. "[16]

[16] MICROSOFT, (n.d), ¿Cuál es la diferencia entre 6to4 e ISATAP? , Obtenida el 25 de Agosto del 2011, de http://www.microsoft.com/spain/windowsserver2003/technologies/ipv6/ipv6faq.mspx .

La dirección 6to4 completa de un host 6to4 sería la siguiente:

2002:WWXX:YYZZ:[SLAID]:[IdDeInterfaz].

2.4.2.2.2 Túnel 6over4

Ahuatzin Sánchez (2005, CAP II, p.72) sostiene que este método es una tecnología de túneles automáticos que provee conectividad "unicast" y "multicast" IPv6 entre nodos a través de una intranet IPv4.

Según la investigación realizada por Ahuatzin Sánchez se ha liberado las siguientes características sobre los túneles 6over4.

El túnel 6over4 maneja la infraestructura IPv4 como una asociación simple con capacidades "multicast", esto significa que el proceso de descubrimiento de vecinos como la resolución de direcciones y descubrimiento de ruteadores, trabaja como un enlace físico con capacidades "multicast" que deberán ser habilitados en IPv4.

Para facilitar las comunicaciones "multicast" IPv6 es una infraestructura IPv4 con "multicast" habilitado, se define el siguiente mapeo para traducir una dirección IPv6 "multicast" en una dirección IPv4 "multicast".

Ejemplos de mapeo de direcciones ""multicast" IPv6:

- FF02::1 (dirección "multicast" o de enlace local en equipos) se mapea a 239.192.0.1.

- FF02::2 (dirección "multicast" o de enlace local en enrutadores) se mapea a 239.192.0.2.

- FF02::1:FF28:9C5A (dirección "multicast" de un nodo solicitado de ejemplo) se mapea a 239.192.156.90.

2.4.2.2.3 ISATAP

Peralta (2002, p.32) sostiene que este método permite crear túneles IPv4/IPv6 automáticamente dentro de un sitio IPv4, tiene algunas ventajas respecto a 6over4, debido a que no necesita multicast IPv4 y soluciona los problemas que se dan cuando una organización no tiene toda su red en un mismo lugar, como la baja escalabilidad en la agregación.

2.4.3 De Traducción

"Este método de traducción permite un enrutamiento transparente de la comunicación entre nodos que sólo poseen soporte a una versión del protocolo IP, o que utilizan Doble Pila. Además pueden operar de diversas formas o en capas distintas, traduciendo cabeceras IPv4 en cabeceras IPv6 y viceversa, realizando conversiones de direcciones, o actuando en el intercambio del tráfico TCP a UDP."[17]

[17] UNTEC, (n.d), Mecanismo de transición IPV4/IPV6, Obtenida el 26 de Agosto del 2011, de http://www.ipv6.cl/noticia/mecanismos-de-transicion-ipv4ipv6

CAPITULO III

LEVANTAMIENTO DE INFORMACIÓN IPV4 DE LA UNIVERSIDAD POLITÉCNICA SALESIANA SEDE-CUENCA

3.1 IDENTIFICACIÓN DE LA RED

La red de datos de la Universidad Politécnica Salesiana se compone de la interconexión del campus universitario de la Sede-Cuenca con los campus de la Sede Quito y la Sede Guayaquil.

En la Figura 9 se presenta la topología simplificada de la red referencial de la Universidad Politécnica Salesiana Sede-Cuenca.

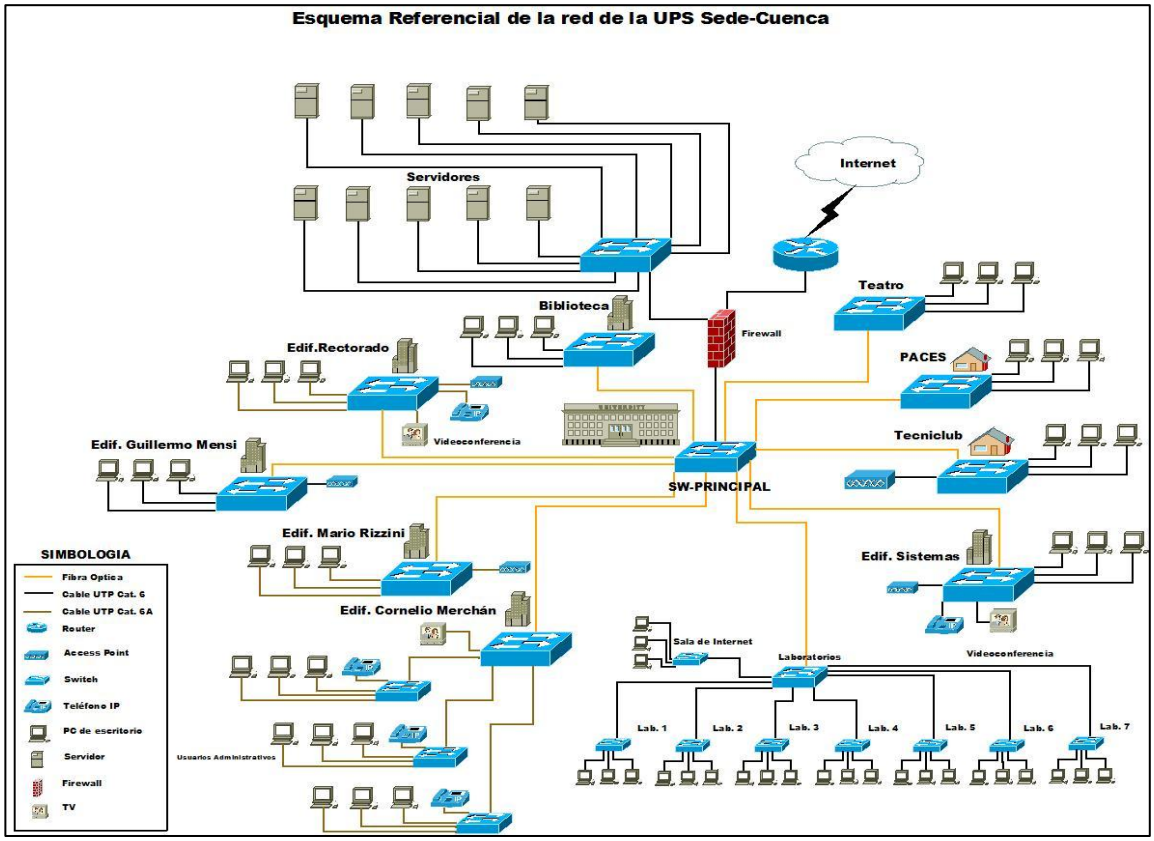


Figura 9 CAP III. Topología referencial de la UPS Sede-Cuenca

Fuente: P. Jimenez, entrevista personal, 26 de Septiembre del 2011

La red del campus universitario de la Sede-Cuenca posee un enlace a Internet otorgado por el ISP Telconet cuya velocidad es de 46 Mbps, además se compone de un "Backbone" de fibra óptica que permite la comunicación hacia los edificios internos del campus como son el Edificio del Rectorado, Edificio Guillermo Mensi, Edificio Mario Rizzini, Edificio Cornelio Merchán, etc.

La red principal permite la comunicación desde el Switch Principal hacia cada uno de los edificios y cuenta con enlaces de fibra óptica de 1Gbps.

La red secundaria permite la comunicación desde los Switches de cada uno de los edificios hacia los usuarios finales utilizando enlaces de cable UTP CAT 6A en los edificios Cornelio Merchán, Mario Rizzini y el Rectorado y enlaces de cable UTP CAT 6 en los edificios Guillermo Mensi, Sistemas, Biblioteca, Tecniclub, Teatro y PACES.

El router principal cuya función es ayudar a direccionar mensajes mientras viajan a través de una red se encuentra instalado en el Edificio de Sistemas.

Los switches cuya función es interconectar dos o más segmentos de red se encuentran instalados en todos los edificios estableciendo una conexión con un Switch Principal ubicado en el Edificio de Sistemas. De esta forma los equipos conforman el núcleo principal de la red, y permiten manejar toda la configuración de las VLANS y el enrutamiento de la red.

La mayoría de los switches que forman la red principal cuentan con 48 puertos para la interconexión de los usuarios y son de marca CISCO a excepción del switch de los Laboratorios cuya marca es 3Com.

El servicio de videoconferencia permite transmitir las imágenes de video a través de la red IP y se encuentra instalado en el Edificio Cornelio Merchán, Sistemas y Rectorado.

Los servidores cuya función es proporcionar diferentes servicios a los clientes se encuentran ubicados en el Edificio de Sistemas. A continuación se detalla las funciones de estos servidores dentro de la red de la UPS Sede-Cuenca:

Servidor	Función
Web	Permite almacenar documentos HTML, imágenes, archivos de texto y material Web con el fin de distribuir este contenido hacia los clientes de la red.
Proxy	Permite administrar el acceso a Internet en una red LAN permitiendo o negando el ingreso a diferentes sitios web.
Archivos	Permite un almacenamiento centralizado de un determinado número de archivos como una especie de biblioteca en donde cada usuario busca el archivo que necesita.
Antivirus	Permite el filtrado de correo electrónico entrante y saliente, bloquea páginas web de direcciones desconocidas, permite la protección Anti Spam, etc.
Desarrollo	Permite utilizar un archivo para simular un almacén de datos y administrar las cuentas de usuario.
Biblioteca	Permite visualizar y almacenar toda la información de las revistas, libros, tesis, etc.
Aplicaciones	Permite el procesamiento de datos de una aplicación a las computadoras cliente, además disminuye la complejidad del desarrollo de aplicaciones debido a que las aplicaciones no necesitan ser programadas, en su lugar son ensambladas desde bloques provistos por el servidor de aplicación.
Base de Datos	Proporciona servicios de base de datos a otros programas u computadoras definido por el modelo cliente-servidor.
Correo Electrónico	Permite almacenar, enviar, recibir y realizar otras operaciones relacionadas con el email para los clientes de la red.
Desarrollo de B.D	Permite crear y gestionar la Base de Datos.

Figura 10 CAP III. Función de los Servidores

Fuente: WIKIPEDIA, (n.d), Servidor, Obtenida el 14 de Noviembre de 2012, de http://es.wikipedia.org/wiki/Servidor

La estructura de red actual de la Universidad Politécnica Salesiana en el protocolo IPv4 ha mantenido un funcionamiento adecuado pese a ciertos problemas en el consumo de ancho de banda y recursos.

Debido a que IPv6 es un protocolo de capa 3 su uso es eficiente para todos los dispositivos de capa 2, por este motivo se procederá a realizar un análisis considerando todos los equipos de la red actual de la UPS Sede-Cuenca descritos en la Figura 9.

El objetivo de este análisis es mantener el mismo diseño de red referencial IPv4 de la UPS Sede-Cuenca para la migración a IPv6 con el fin de permitir la conexión de la red LAN de la Universidad hacia el Internet. De esta forma cada uno de los departamentos, laboratorios y auditorios de la institución podrán contar con acceso IPv6 al Internet a través del "backbone" de fibra óptica.

Mediante el análisis realizado en este proyecto estaremos dando el primer paso hacia una futura migración total de la red general de la Universidad que incluye las sedes Quito, Guayaquil y Cuenca.

3.2 TRÁFICO DE RED

"El análisis del Tráfico de Red de área local consiste en medir la cantidad de información promedio que se transfiere a través del canal de comunicación y la velocidad de transferencia."[18]

Uno de los problemas principales en una red con IPV4 es el Broadcast el cual se extiende en toda la red y produce un consumo innecesario de ancho de banda y recursos. Por este motivo es necesario realizar un análisis del tráfico de red para saber en que estado se encuentran los paquetes de datos.

En la actualidad existen varias herramientas para el análisis y monitoreo de redes, el cual nos permiten observar las siguientes características:[19]

[18] VACA, Carina, L, (n.d), Análisis de Tráfico de una red local universitaria, Obtenida el 27 de Septiembre del 2011, de http://www.slideshare.net/calu1212/anlisis-de-trfico-de-una-red-local-universitaria

[19] INTEGRACION DE SISTEMAS, (n.d), Análisis y Monitoreo de Redes, Obtenida el 27 de Septiembre del 2011, de http://www.integracion-de-sistemas.com/analisis-y-monitoreo-de-redes/index.html#Que_es_posible_observar

Control de desempeño:

- Determinar las tendencias de la red, y pronosticar la necesidad de aumentar la capacidad de los equipos.
- Obtener mayor eficiencia de la red sin la necesidad de aumentar el ancho de banda.

Control de múltiples instalaciones:

- Administrar y controlar redes remotas.
- Obtener reportes desde múltiples consolas acerca del estado de la red.
- Monitorear múltiples redes simultáneamente desde una consola.

Control de solución de problemas:

- Resolver los problemas que se presentan tanto en las redes locales y remotas.
- Administrar la configuración de dispositivos locales y remotos.

Control de Información:

- Permite visualizar y almacenar datos de la red para manejar reportes y tendencias.
- Analizar el tráfico de la red a través del tiempo.
- Generar reportes con el fin de justificar las necesidades de actualización de la red.

Para poder realizar el análisis del tráfico de red se utilizó una versión demo del software TracePlus/Ethernet versión 5.51.00 el cual permite controlar y administrar una red local.

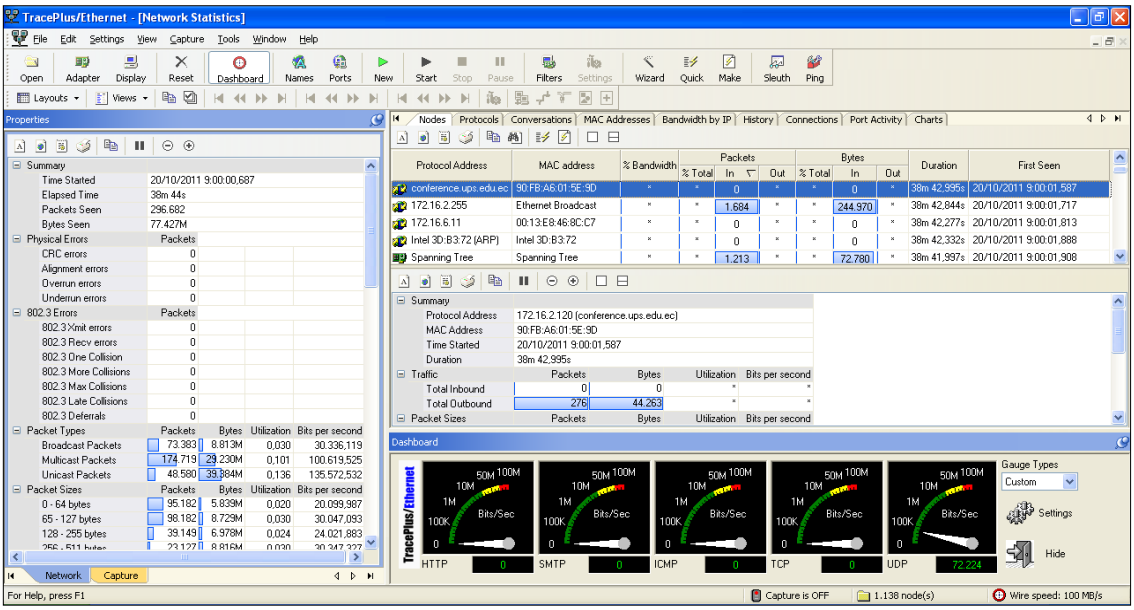


Figura 11 CAP III. Interfaz gráfica del Software TracePlus/Ethernet v 5.51.00

Fuente: El Autor

TracePlus/Ethernet permite crear un informe basado en el tráfico que genera cada una de las máquinas que se encuentran en red. Este informe describe en forma detallada todas las transferencias de datos, los protocolos utilizados, los paquetes enviados y recibidos, el comportamiento del protocolo IP, etc.

Una de las características más importantes de TracePlus/Ethernet es el de sugerir acciones que en muchos casos son indispensables para mejorar el rendimiento de la conexión local. Según los resultados obtenidos, nos ayuda a establecer permisos de acceso anteriormente denegados, limitar el intercambio de datos y solucionar errores que afecten a la red.

Para medir el desempeño de la red referencial de la UPS Sede-Cuenca se analizaron los siguientes parámetros:

- Análisis de paquetes Bits/Segundo
- Análisis del Porcentaje de Ancho de Banda
- Análisis de los Protocolos principales

El monitoreo fue realizado desde un computador dedicado que se encuentra conectado a un Switch Secundario ubicado en el Edif. Sistemas y este a su vez se encuentra conectado directamente con el Switch Principal de la Universidad (Ver Fig. 9), de esta manera se alcanzó a analizar todo el tráfico de la red LAN, durante un período efectivo de 5 días en un horario comprendido desde las 9:00am hasta las 9:45am en donde existe una mayor transmisión de datos debido a que los estudiantes finalizan sus dos primeras horas de clases y pasan directamente al laboratorio de internet para realizar sus investigaciones.

El Análisis completo con la descripción de los Gráficos del programa TracePlus/Ethernet y los resultados obtenidos se encuentran en el Anexo 1.

3.3 DISTRIBUCIÓN DEL CABLEADO

El objetivo principal de este análisis es determinar la situación actual de la red IPv4, conocer los tipos de medios, la ubicación y las características de los equipos, de esta manera se podrá verificar si la UPS Sede-Cuenca cuenta con las instalaciones adecuadas y los equipos necesarios para poder llevar a cabo el proceso de migración hacia el protocolo IPv6.

La red principal de datos de la UPS Sede Cuenca se encuentra ubicada en el Campus El Vecino **(**Calle Vieja 12-30 y Elia Liut**)**, en donde se tiene una infraestructura compuesta de los siguientes edificios:

Tabla 3 CAP III. Edificios de la UPS Sede-Cuenca

N^0	**Nombre del Edificio**
1	Edificio Rectorado
2	Edificio Guillermo Mensi
3	Edificio Mario Rizzini
4	Edificio Cornelio Merchán
5	Edificio de Sistemas
6	Biblioteca
7	Tecniclub
8	PACES

Fuente: El Autor

En cada uno de los edificios se encuentra ubicado un Switch el cual permite la interconexión entre los equipos de red.

El cableado para las aéreas de trabajo está distribuido por medio de canaletas decorativas marca DEXSON (60x40), que se encuentran fijadas sobre la pared con el objetivo de separar el cableado de datos del cableado eléctrico AC.

3.3.1 CABLEADO HORIZONTAL

El cableado horizontal del campus universitario de la Sede Cuenca se extiende desde los IDF's hacia los equipos del Área de trabajo.

A continuación se describen las características principales de los IDF's y las Áreas de Trabajo:

3.3.1.1 IDF's

Ubicación

Los IDF's se encuentran ubicados en cada uno de los Edificios que forman parte de la infraestructura de red de la UPS Sede-Cuenca. En cada cuarto de los IDF's se encuentran 48 puntos para la transmisión de datos y 24 puntos para la transmisión de voz, a excepción de los cuartos para el Tecniclub y PACES en donde se tienen 20 puntos para la transmisión de datos y 10 puntos para la transmisión de voz respectivamente.

Dimensiones

Cada uno de los IDF's tiene las siguientes dimensiones: 2 mts de largo x 2,5 mts de ancho dando un área total de 5 m^2.

Temperatura y humedad

- Temperatura ambiental promedio de 15^{o} C.
- Humedad relativa de 40-70 %.

Instalaciones eléctricas

- 4 tomacorrientes distribuidos de forma proporcional.
- 1 lámpara incandescente en cada IDF.

Paredes y pisos

- El acabado del piso es de baldosa el cual permite proteger los equipos del polvo y la electricidad estática.
- Las paredes son de cemento cubiertas con una capa de pintura antiflama con el fin de evitar posibles incendios.

Componentes de un IDF:

Dentro de un IDF podemos encontrar los siguientes elementos:

1. Racks abiertos o cerrados.
2. Gabinetes.
3. Patch panel.

A continuación se presenta la Distribución de los tipos de racks y gabinetes que se encuentran instalados dentro de los IDF's de la UPS Sede-Cuenca:

Tabla 4 CAP III. Distribución de los tipos de racks y gabinetes

N°	Tipos de racks y gabinetes	Edificios de la UPS Sede-Cuenca
1	Racks abiertos	Edificio Guillermo Mensi. Edificio Mario Rizzini. Edificio de Sistemas. Biblioteca.
2	Racks cerrados	Edificio Cornelio Merchán Edificio Rectorado.
3	Gabinetes	Tecniclub, PACES.

Fuente: Jimenez, entrevista personal, 03 de Octubre del 2011

Características Principales:

1. Racks

Tabla 5 CAP III. Características de los racks abiertos

Especificaciones técnicas	Materiales
Marca: Quest. **Altura útil:** 24 RU. **Alto:** 121.9cm. **Ancho:** 51.6cm. **Profundidad:** 35.5 cm. **Capacidad:** 250 kg.	**Base perforada:** Aluminio 6063. **Estructura:** Aluminio 6063. **Acabados:** Pintura electrostática. **Tornillos:** 3/8" x 1" UNTF. **Empaque:** Caja en cartón corrugado

Fuente: QUEST, (n.d), Infraestructura para Telecomunicaciones, Obtenida el 04 de Octubre del 2011, de http://issuu.com/daga_sa/docs/quest?mode=embed&showFlipBtn=false

Tabla 6 CAP III. Características de los racks cerrados

Especificaciones técnicas
Marca: Quest **Altura útil:** 28 RU. **Alto:** 142.5cm. **Ancho:** 58cm. **Profundidad:** 61cm. **Profundidad útil:** 53 cm. **Capacidad:** 325 kg.

Fuente: QUEST, (n.d), Infraestructura para Telecomunicaciones, Obtenida el 04 de Octubre del 2011, de http://issuu.com/daga_sa/docs/quest?mode=embed&showFlipBtn=false

2. Gabinetes:

Tabla 7 CAP III. Características de los gabinetes

Especificaciones técnicas
Marca: Quest. **Altura útil:** 15 RU. **Alto:** 85.7 cm. **Ancho:** 58 cm. **Profundidad:** 81cm. **Profundidad útil:** 73 cm. **Capacidad:** 240 kg.

Fuente: QUEST, (n.d), Infraestructura para Telecomunicaciones, Obtenida el 04 de Octubre del 2011, de http://issuu.com/daga_sa/docs/quest?mode=embed&showFlipBtn=false

3. Patch panel:

Tabla 8 CAP III. Características del Patch Panel

Especificaciones técnicas
Marca: Panduit. **Numero de módulos de espacio:** 24. **Numero de puertos:** 24. **Numero de espacios para rack:** 1 **Nivel de rendimiento:** Categoría 6. **Terminación:** RJ 45 Categoría 6.

Fuente: PANDUIT, (n.d), Products for you demanding requirements, Obtenida el 04 de Octubre del 2011, de http://www.panduit.com/Products/ProductOverviews/index.htm

3.3.1.2 Área de Trabajo

El cableado en las áreas de trabajo se desarrolla desde la terminación del cableado horizontal en la salida de información de los IDF's hasta el equipo en el cual se está corriendo una aplicación de base de datos, video, control, etc.

A continuación se presenta las características principales de los medios y demás elementos de un área de trabajo:

1. Cable UTP

Tabla 9 CAP III. Características del Cable UTP CAT.6

UTP CAT. 6	DESCRIPCION
Características	Tipo de aislamiento: Polietileno. Para conexiones y aplicaciones IP. Conductor de cobre sólido de 0.57 mm. Diámetro exterior 6.1 mm. Impedancia: 100 Ω.
Aplicaciones	1.2 Gbps ATM, 622 Mbps ATM, 100 Base T, 100 Mbps TP-PMD, 100 BASE VG ANYLAN, 1000 Base T, Video digital, Video Banda Base y Banda Ancha.
Normas Aplicables	ANSI/TIA/EIA 568B.2-1, ANSI/ICEA S-102-700, ISO/IEC 11801 (2a edición, clase E), NEMA WC66, EN 50173-1, UL, NMX-I-248-NYCE-2005.

Fuente: 3M, (n.d), Categoría 6, Obtenida el 05 de Octubre del 2011, de http://mws9.3m.com/mws/mediawebserver.dyn?yyyyyygeqJMySazyLazyyZhCg37YYYYX-

2. Patch Cord

Tabla 10 CAP III. Características del Patch Cord

Especificaciones técnicas
Conductor: 7 hilos de cobre de Ø0.20 mm. **Aislamiento:** polietileno altamente resistente **Diámetro del conductor en el aislamiento:** 0.98±0.05 mm **Cantidad de pares:** 4 **Colores de los pares trenzados:** azul-blanco/azul, naranja-blanco/naranja, verde-blanco/verde, marrón-blanco/marrón **Forro:** PVC Ø6.2±0.2 mm

Fuente: ICONO SISTEMAS, (n.d), Patch Cords, Obtenida el 05 de Octubre del 2011, de http://www.iconosistemas.com.ec/index.php?page=shop.product_details&flypage=flypage_lite_pdf.tpl&product_id=105&category_id=28&option=com_virtuemart&Itemid=150&vmcchk=1&Itemid=150

3. Conectores

Tipo: Clavija RJ-45 de par trenzado, Cat. 6.

Resistencia por aislamiento: > 10 M Ω.

Frecuencia: 100-250 Mhz.

4. Paneles frontales

Material: ABS UL 94V-0.
Medidas: 70x115mm.

3.3.2 CABLEADO VERTICAL

El cableado vertical de la red de la UPS Sede-Cuenca se desarrolla desde el Switch principal ubicado en el MDF del Edificio de Sistemas hacia cada uno de los Switches de los IDF's ubicados en los diferentes edificios de la UPS, a una distancia aproximada de 250 metros.

3.3.2.1 MDF

Ubicación

El MDF de la UPS Sede Cuenca se encuentra en el tercer piso del Edificio de Sistemas, y posee una conexión a tierra ubicado en el primer piso del mismo edificio.

Dimensiones

El cuarto tiene las siguientes dimensiones: 6 mts de largo x 4 mts de ancho dando un área total de 24 m^2.

Temperatura y humedad

- La temperatura aproximada del cuarto varía entre 18 - 22^oC y es controlada por medio de un sistema de climatización.
- La humedad relativa es del 50%.

Instalaciones eléctricas

- 10 tomacorrientes distribuidos de forma proporcional.
- 4 lámparas incandescentes.

Acceso a la habitación y equipos

El ingreso a la habitación se realiza a través de una puerta blindada de acero (2 mts de largo x 1,50 mts de ancho) la misma que cuenta con un sistema de control de acceso cuya finalidad es evitar el ingreso del personal no autorizado.

Acceso y mantenimiento del cableado

El tendido del cableado horizontal se encuentra por debajo del piso y está conectado a un punto central en el MDF el cual permite formar la topología en estrella.

Paredes y pisos

- El acabado del piso y el techo es de un material acrílico el cual permite una facilidad de instalación, acceso y mantenimiento del cableado.
- Las paredes son de cemento cubiertas con una capa de pintura antiflama con el fin de evitar posibles incendios.

Sistema principal de tierra

El cuarto para las conexiones a tierra se encuentra ubicado en el primer piso del Edificio de Sistemas, el mismo que está compuesto por un cable tipo Calibre que recorre las instalaciones desde el tercero hasta el primer piso del edificio.

El objetivo principal de la conexión a tierra es evitar que las partes metálicas de un equipo se carguen con voltajes peligrosos producto de una descarga eléctrica o una falla del cableado dentro del equipo.

Finalmente podemos decir que uno de los aspectos más importantes de un sistema con conexión a tierra es proteger la integridad de los técnicos encargados de dar el mantenimiento de la red.

A continuación se describe las características principales de los racks para servidores y datos que se encuentran ubicados dentro del Centro de Distribución principal de Cableado de la UPS Sede-Cuenca:

1. Racks de Servidores

Tabla 11 CAP III. Características de los Racks para servidores

Especificaciones técnicas	Materiales
Marca: Quest **SKU:** RP-4623. **Norma:** EIA-310D-IEC. **Formato:** 19" **Altura Útil:** 45 RU. **Altura:** 213.36 cm. **Ancho:** 51.56 cm. **Profundidad:** 81.28 cm. **Capacidad de Carga:** 771.11 kg.	**Base Perforada:** HOT ROLLED en espesor de 1/8" **Laterales Ajustables:** Acero laminado en frío, Calibre 14 **Parales:** HOT ROLLED en espesor de 1/8". **Acabados:** Pintura Electrostática. **Tornillos:** 3/8" x 1" UNTF. **Empaque:** Caja en Cartón Corrugado.

Fuente: QUEST, (n.d), Infraestructura para telecomunicaciones, Obtenida el 06 de Octubre del 2011, de http://issuu.com/daga_sa/docs/quest?mode=embed&showFlipBtn=false

2. Racks de Datos

Tabla 12 CAP III. Características de los Racks de Datos

Especificaciones técnicas	Materiales
Marca: Quest. **SKU:** RP-4621. **Formato:** 19" **Altura Útil:** 45 RU. **Altura:** 213.36 cm. **Ancho:** 51.56 cm. **Profundidad:** 35.56 cm. **Capacidad de Carga:** 430.91 Kg.	**Base Perforada:** HOT ROLLED en espesor de 1/8". **Laterales Ajustables:** Acero laminado en frío, Calibre 14. **Parales:** HOT ROLLED en espesor de 1/8". **Acabados:** Pintura Electrostática. **Tornillos:** 3/8" x 1" UNTF. **Empaque:** Caja en Cartón Corrugado.

Fuente: QUEST, (n.d), Infraestructura para telecomunicaciones, Obtenida el 06 de Octubre del 2011, de http://issuu.com/daga_sa/docs/quest?mode=embed&showFlipBtn=false

- **Fibra Óptica**

Tipo: Multimodo.

Numero de fibras: 8

Compatibilidad: 1GbE 50/125µm.

- **Conectores:**

Tipo: Multimodo

Tamaño de las fibras: 900 µm.

Compatibilidad: 1 GbE 50/125µm

Acceso y Mantenimiento de la Fibra Óptica

El acceso a los cables de fibra óptica para el mantenimiento se realiza directamente sobre los racks de datos, y por medio de ductos y pozos de revisión el cual permite la interconexión del cableado desde el IDF hacia el MDF.

La distribución actual del cableado de la red de la Universidad Politécnica Salesiana Sede-Cuenca se encuentra establecida de manera correcta debido a las características mencionadas en la Sección 3.3. Distribución del Cableado.

Según el análisis realizado se ha podido determinar que el cableado estructurado de la Universidad presenta los siguientes beneficios:

- Confiabilidad en la red

La red actual de la Universidad es capaz de cumplir todos los propósitos para lo cual ha sido diseñada.

- Capacidad de crecimiento

El diseño de la topología de red tiene la capacidad de permitir el aumento de nuevos sectores de red.

- Fácil administración.

La ubicación estratégica de los equipos de red permite detectar fácilmente los errores y corregirlos de forma inmediata.

- Mayor Seguridad.

El acceso al MDF y los IDF's se encuentra establecido por altas normas de seguridad.

Por todo esto podemos decir que la distribución del cableado se encuentra lista para llevar a cabo el proceso de migración a IPv6.

3.4 LEVANTAMIENTO Y OBTENCIÓN DEL DIAGRAMA LÓGICO

El diagrama lógico de red de la UPS Sede-Cuenca muestra las partes principales de los equipos de sistemas de redes y como están interconectados.

El diagrama lógico incluye los siguientes componentes:

- Routers.
- Switches.
- Firewalls.
- Servidores.
- Access Point.
- Estaciones de trabajo.

Cada uno de los servidores y servicios se incluyen en el diagrama lógico debido a que su ubicación puede afectar los patrones del tráfico, el uso del ancho de banda y la seguridad.

3.4.1 Diseño de la Topología de red

Una topología de red define la estructura de una red. Una parte de la definición topológica es la topología física que se refiere a la disposición real de los cables o medios. La otra parte es la topología lógica que define la forma en que los host acceden a los medios para enviar datos.[20]

Los factores más importantes que de deben tomar en cuenta en el momento de seleccionar una topología de red son los siguientes:

- El tráfico de red.
- La capacidad de crecimiento.

[20] Staky, *CCNA 1 and 2 Versión 3.1 Curriculum en formato pdf,* (n.d), p. 31

- La distribución de los equipos a interconectar.
- El tipo de aplicaciones que se va a ejecutar.
- La inversión que se pretende realizar.
- El costo para las actualizaciones y mantenimiento de la red.

La red del campus universitario de la Sede Cuenca posee una topología en estrella extendida que conecta estrellas individuales entre si mediante la conexión de switches a través de dos enlaces punto a punto, uno para transmisión y otro para recepción de los datos.

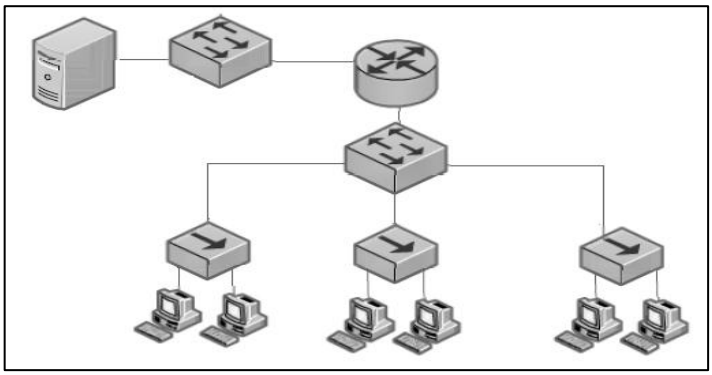


Figura 12 CAP III. Topología en estrella extendida

Fuente: El Autor

La topología en estrella es una de las ventajas que posee la red de la UPS Sede-Cuenca debido a que si se desconecta o se rompe el cable de red solo esa computadora se verá afectada, mientras que el resto de la red mantendrá su comunicación de forma normal.

El diseño de la topología de red de la UPS Sede-Cuenca se ha desarrollado en el Software Cisco Packet Tracer versión 5.3.2.0027 cuya función es el aprendizaje y la simulación de redes de forma interactiva.

Además el Packet Tracer nos permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales.

El diseño de la topología de red de la UPS Sede Cuenca en el Packet Tracer versión 5.3.2.0027 se encuentra en el Anexo 2.

3.4.2 Diseño de las VLANS

El diseño de las VLANS dentro de la red de la Universidad Politécnica Salesiana Sede-Cuenca se utiliza con el fin de obtener los siguientes beneficios:

- Uso eficiente del ancho de banda.
- Facilidad en la administración de la red.
- Mayor seguridad en el acceso a los dominios lógicos.

Para mantener la información entre cada dependencia y obtener mayores beneficios dentro de la red de la UPS Sede-Cuenca se ha diseñado un total de 32 VLANS distribuidas de la siguiente manera:

Tabla 13 CAP III. Nombre de las VLANS configuradas en el Packet Tracer

# VLAN	Nombre de la VLAN	# VLAN	Nombre de la VLAN
1	Biblioteca	**18**	EgresadosGraduados
2	EdifRectorado	**19**	PastoralUPS
3	EdifGuillermoMensi	**20**	EdifMarioRizzini
4	Estudiantes	**21**	LabInternet
5	CarrerasUPS	**22**	Laboratorio1
6	ConsejoAcadémico	**23**	Laboratorio2
7	ConsejoAdminEconomico	**24**	Laboratorio3
8	SecretariaGeneral	**25**	Laboratorio4
9	SecretariasTécnicas	**26**	Laboratorio5
10	ContabilidadGeneral	**27**	Laboratorio6
11	BienestarEstudiantil	**28**	Laboratorio7
12	UnidadPostgrados	**29**	EdifSistemas
13	UnidadPlanifEvaluación	**30**	Tecniclub
14	UnidadVinColectividad	**31**	PACES
15	UnidadInvestigación	**32**	Teatro
16	GestTalentoHumano	**33**	Wireless
17	AreasConocimiento	**34**	TeléfonosIP

Fuente: El Autor

3.4.2.1 Reglas de conectividad entre VLANS

Las reglas de conectividad entre VLANS se han diseñado con el fin de permitir el acceso a departamentos que manejan la misma información y en otros casos negar el acceso a departamentos que manejan otro tipo de información.

A continuación se presenta un resumen en donde podemos observar las reglas de acceso a cada una de las VLANS configuradas en el diagrama de red de la UPS Sede-Cuenca:

Tabla 14 CAP III. Reglas de Acceso entre VLANS

# /Nombre de la VLAN	Acceso VLAN	# /Nombre de la VLAN	Acceso VLAN
1. Biblioteca	17	18. EgresadosGraduados	-
2. EdifRectorado	-	19. PastoralUPS	31
3. EdifGuillermoMensi	20	20. EdifMarioRizzini	3
4. Estudiantes	5,6	21. LabInternet	-
5. CarrerasUPS	4,6	22.Laboratorio1	23,24,25,26,27,28
6. ConsejoAcadémico	5,7	23. Laboratorio2	22,24,25,26,27,28
7. ConsejoAdminEconomico	6	24. Laboratorio3	22,23,25,26,27,28
8. SecretariaGeneral	9	25. Laboratorio4	22,23,24,26,27,28
9. SecretariasTécnicas	8	26. Laboratorio5	22,23,24,25,27,28
10. ContabilidadGeneral	-	27. Laboratorio6	22,23,24,25,26,28
11. BienestarEstudiantil	-	28. Laboratorio7	22,23,24,25,26,27
12. UnidadPostgrados	13,14,15	29. EdifSistemas	-
13. UnidadPlanifEvaluación	12,14,15	30. Tecniclub	-
14. UnidadVinColectividad	12,13,15	31. PACES	19
15. UnidadInvestigación	12,13,14	32. Teatro	-
16. GestTalentoHumano	-	33. Wireless	-
17. AreasConocimiento	-	34. TeléfonosIP	-

Fuente: El Autor

En esta tabla se ha podido observar varias VLANS independientes (manejan información única) representadas por el símbolo “-”.

También es importante mencionar que todos los laboratorios manejan el mismo tipo de información por esta razón es necesario permitir el acceso entre cada uno de ellos.

Debido a que el diseño de las VLANS nos permite aumentar la seguridad y administrar el flujo de datos entre los componentes de aplicación, se ha desarrollado la simulación de todas las reglas de conectividad descritas en la Tabla 14, utilizando el Packet Tracer versión 5.3.2.0027 cuyo diagrama se puede observar en el Anexo 3.

3.4.3 Distribución de las Direcciones IPv4

Una dirección IP permite identificar una computadora conectada a una red, mientras que una red de datos permite la comunicación entre los dispositivos de usuario final y los dispositivos de red.

Por lo general la red de una empresa tiene una dirección IP el cual debe ser calculado de acuerdo al requerimiento de host y el porcentaje de crecimiento futuro de la red.
Para la elaboración de este proyecto tomaremos como base una dirección IP privada de clase B: 172.20.0.0/16.

Dirección IP en formato decimal: 172.20.0.0
Dirección IP en formato binario: 10101100.00010100.00000000.00000000
Mascara de red: 255.255.0.0

Se ha tomado como base esta dirección IP debido a que el número total de host de toda la red incluyendo el porcentaje de crecimiento futuro que es de 875 host.

En la Tabla 15 podemos observar el número de host que posee cada dirección IPv4 y realizar una comparación con el número total de host de nuestro requerimiento:

Tabla 15 CAP III. Clase de Direcciones IPv4 y Número de host

Clase	Dirección IP	# de host	Resultado
A	10.0.0.0/8	16777214	Mayor desperdicio de direcciones IP.
B	172.16.0.0/16	65534	Si me alcanza.
C	192.168.0.0/24	254	No me alcanza.

Fuente: El Autor

A continuación se describe el requerimiento de host y el porcentaje de crecimiento futuro para cada Switch en la red de la UPS Sede-Cuenca:

Tabla 16 CAP III. Requerimientos de hosts y porcentaje de crecimiento futuro

Switch	# de host	% de crecimiento futuro (30%)	Total
Biblioteca	48	14,4	62
Edif. Rectorado	48	14,4	62
Edif. Guillermo Mensi	48	14,4	62
	48(SW 1)	14,4	62
Edif. Cornelio Merchán	48(SW 2)	14,4	62
	48(SW 3)	14,4	62
Edif. Mario Rizzini	48	14,4	62
Edif. Sistemas	48	14,4	62
Teatro	48	14,4	62
	30(SW Internet)	9	39
	22(SW Lab1)	6,6	29
	22(SW Lab2)	6,6	29
Laboratorios	22(SW Lab3)	6,6	29
	22(SW Lab4)	6,6	29
	22(SW Lab5)	6,6	29
	22(SW Lab6)	6,6	29
	22(SW Lab7)	6,6	29
Tecniclub	24	7,2	31
PACES	24	7,2	31
Servidores	10	3	13
Requerimiento total:			**875**

Fuente: P. Jimenez, entrevista personal, 10 de Octubre del 2011

De acuerdo a la tabla anterior podemos observar que la red de la UPS Sede Cuenca necesita 20 subredes para cubrir los requerimientos de cada uno de los Switch que se encuentran ubicados en los edificios de la institución.

De acuerdo a estos requerimientos se decidió tomar la dirección IP 172.20.0.0/16 luego se procedió a realizar los cálculos utilizando el subneteo con VLSM, el cual permite evitar el desperdicio de direcciones IP obteniendo un mejor aprovechamiento y optimización del uso de direcciones. En la Tabla 17, podemos observar la descripción de los Switches y las direcciones IPV4 que se utilizan para cada subred:

Tabla 17 CAP III. Direcciones IPv4 para cada subred.

# de Subred	Switch	Dirección de subred	Mascara de subred
1	Biblioteca	172.20.0.0	255.255.255.192
2	Edif. Rectorado	172.20.0.64	255.255.255.192
3	Edif. Guillermo Mensi	172.20.0.128	255.255.255.192
4	Edif. Cornelio Merchán SW 1	172.20.0.192	255.255.255.192
5	Edif. Cornelio Merchán SW 2	172.20.1.0	255.255.255.192
6	Edif. Cornelio Merchán SW 3	172.20.1.64	255.255.255.192
7	Edif. Mario Rizzini	172.20.1.128	255.255.255.192
8	Edif. Sistemas	172.20.1.192	255.255.255.192
9	Teatro	172.20.2.0	255.255.255.192
10	Internet	172.20.2.64	255.255.255.192
11	Tecniclub	172.20.2.128	255.255.255.192
12	PACES	172.20.2.192	255.255.255.192
13	Laboratorio 1	172.20.3.0	255.255.255.224
14	Laboratorio 2	172.20.3.32	255.255.255.224
15	Laboratorio 3	172.20.3.64	255.255.255.224
16	Laboratorio 4	172.20.3.96	255.255.255.224
17	Laboratorio 5	172.20.3.128	255.255.255.224
18	Laboratorio 6	172.20.3.160	255.255.255.224
19	Laboratorio 7	172.20.3.192	255.255.255.224
20	Servidores	172.20.3.224	255.255.255.240

Fuente: El Autor

La distribución de las direcciones IPV4 para cada subred se describe en el Anexo 4.

3.4.4 Distribución de las direcciones IP para cada VLAN

Proceso de Configuración Inter-VLAN

Paso 1: Configuración de los puertos del Switch Principal en modo trunk.

Paso 2: Configuración de VTP.

Paso 3: Creación de VLANS en el Switch Principal.

Paso 4: Asignación de los puertos con su respectiva VLAN en cada Switch.

Paso 5: Configuración del Router-PT Firewall:

- Dentro de la interfaz Fa0/0 se crearon 32 sub-interfaces con encapsulación 802.1Q.
- Finalmente se asignó una dirección IP para cada sub-interfaz dependiendo de la VLAN a la que pertenece.

A continuación se presentan los datos del proceso de configuración Inter-VLAN en el Switch Principal y en el Router-PT Firewall:

Tabla 18 CAP III. Datos principales de la Configuración de VLANS

Switch Principal		**Router Firewall**	
# VLAN	Nombre de VLAN	Sub-interfaz	Dirección Sub-interfaz
10	Biblioteca	fa 0/0.10	172.20.0.1/26
20	EdifRectorado	fa 0/0.20	172.20.0.65/26
30	EdifGuillermoMensi	fa 0/0.30	172.20.0.129/26
40	Estudiantes	fa 0/0.40	* 172.20.0.193/26
41	CarrerasUPS	fa 0/0.41	172.20.0.205/26
42	ConsejoAcadémico	fa 0/0.42	172.20.0.217/26
43	ConsejoAdminEconómico	fa 0/0.43	172.20.0.229/26
44	SecretariaGeneral	fa 0/0.44	172.20.0.241/26
45	SecretariasTécnicas	fa 0/0.45	* 172.20.1.1/26
46	ContabilidadGeneral	fa 0/0.46	172.2.1.13/26
47	BienestarEstudiantil	fa 0/0.47	172.20.1.25/26
48	UnidadPostgrados	fa 0/0.48	172.20.1.37/26
49	UnidadPlanifEvaluación	fa 0/0.49	172.20.1.49/26
50	UnidadVinColectividad	fa 0/0.50	* 172.20.1.65/26
51	UnidadInvestigación	fa 0/0.51	172.20.1.75/26
52	GestTalentoHumano	fa 0/0.52	172.20.1.85/26
53	AreasConocimiento	fa 0/0.53	172.20.1.95/26
54	EgresadosGraduados	fa 0/0.54	172.20.1.105/26
55	PastoralUPS	fa 0/0.55	172.20.1.115/26
60	EdifMarioRizzini	fa 0/0.60	172.20.1.129/26
70	LabInternet	fa 0/0.70	172.20.2.65/26
71	Laboratorio1	fa 0/0.71	172.20.3.1/27
72	Laboratorio2	fa 0/0.72	172.20.3.33/27
73	Laboratorio3	fa 0/0.73	172.20.3.65/27
74	Laboratorio4	fa 0/0.74	172.20.3.97/27
75	Laboratorio5	fa 0/0.75	172.20.3.129/27
76	Laboratorio6	fa 0/0.76	172.20.3.161/27
77	Laboratorio7	fa 0/0.77	172.20.3.193/27
80	EdifSistemas	fa 0/0.80	172.20.1.193/26
90	Tecniclub	fa 0/0.90	172.20.2.129/26
100	PACES	fa 0/0.100	172.20.2.193/26
110	Teatro	fa 0/0.110	172.20.2.1/26
120	Wireless	fa 0/0.120	172.20.4.1/27
130	TeléfonosIP	fa 0/0.130	172.20.5.1/27

Fuente: El Autor

3.4.5 Elaboración de las tablas de enrutamiento

En el diagrama de red de la UPS Sede-Cuenca se ha configurado el enrutamiento estático, de esta manera el administrador de la red configura manualmente la información acerca de las redes remotas en el Router.

La información de las tablas de enrutamiento del Router Principal y el Router Firewall se describe a continuación:

Tabla 19 CAP III. Tabla de enrutamiento del Router Principal

Dirección IP destino	Interfaz de salida	Dirección IP del próximo salto
172.20.0.0/16	Serial 3/0	200.0.0.1/30

Fuente: El Autor

Tabla 20 CAP III. Tabla de enrutamiento del Router Firewall

Dirección IP destino	Interfaz de salida	Dirección IP del próximo salto
129.0.0.0/30	Serial 2/0	200.0.0.2/30
200.0.0.0	Serial 2/0	200.0.0.2/30

Fuente: El Autor

3.4.6 Servicios de la Intranet

La red interna de la UPS Sede Cuenca se encuentra diseñada con el fin de permitir y negar el acceso a determinados usuarios de la Universidad.

Dentro de la red interna se instalan los servidores Web, cuyo acceso se realiza mediante la tecnología de los navegadores web con el fin de obtener información relevante para los usuarios como por ejemplo consultas de los datos financieros, consulta de notas, record académico, etc.

A continuación se detalla cada uno de los servicios que ofrece la red interna de la UPS Sede Cuenca:

1. PORTAL WEB:

Ambientes virtuales para el aprendizaje:

Los docentes y los estudiantes de la UPS Sede Cuenca tienen la opción de ingresar a los Ambientes virtuales para el aprendizaje cuya plataforma se encuentran divida en diferentes modalidades:

- Modalidad presencial.
- Modalidad a distancia.
- Modalidad virtual.

Consultas Académicas:

Los estudiantes pueden realizar las siguientes consultas académicas:

- Datos de los estudiantes.
- Calificaciones académicas
- Horario de clases
- Malla curricular
- Materias pendientes
- Registro académico
- Materias fuera de malla
- Materias paracadémicas
- Pagos pendientes
- Estado de cuenta
- Evaluación docente

Productos Microsoft

Los estudiantes tienen la posibilidad de descargarse una serie de productos Microsoft.

- Microsoft Windows 8.
- Microsoft Office 2007.
- Microsoft SQL Server 2008.

Ficha socioeconómica

En esta sección los estudiantes tienen la capacidad de llenar un formulario con sus datos personales, académicos, domicilio, grupo familiar, situación habitacional y datos económicos con el objetivo de obtener una pensión diferenciada en el costo total de la matrícula.

2. SISTEMAS INTERNOS:

La UPS Sede Cuenca ofrece los siguientes sistemas internos:

Sistema Académico:

Este sistema se utiliza para que los docentes puedan ingresar las notas en el sistema, y al mismo tiempo permitir a los estudiantes revisar sus calificaciones.

Sistema Financiero:

Este sistema se utiliza para que los estudiantes puedan realizar el cobro de los siguientes derechos:

- Derecho de matrícula.
- Derecho de examen global.
- Derecho de denuncia de tesis, etc.

Sistema de RRHH:

El sistema de RRHH se utiliza para registrar el ingreso y la salida del personal administrativo y docente de la UPS Sede Cuenca.

Sistema CERS:

El Sistema de Crédito Educativo con responsabilidad social (CERS) se basa en el análisis, situación socioeconómica del estudiante, y se aplica el valor de los créditos académicos.

3.5 LEVANTAMIENTO Y OBTENCIÓN DEL DIAGRAMA FÍSICO

El diagrama físico de red de la UPS Sede Cuenca presenta una topología en estrella extendida. El punto central de esta topología de red se encuentra en el MDF que se encuentra ubicado en el tercer piso del Edificio de Sistemas. A continuación se presenta el Diagrama físico de red de la UPS Sede Cuenca:

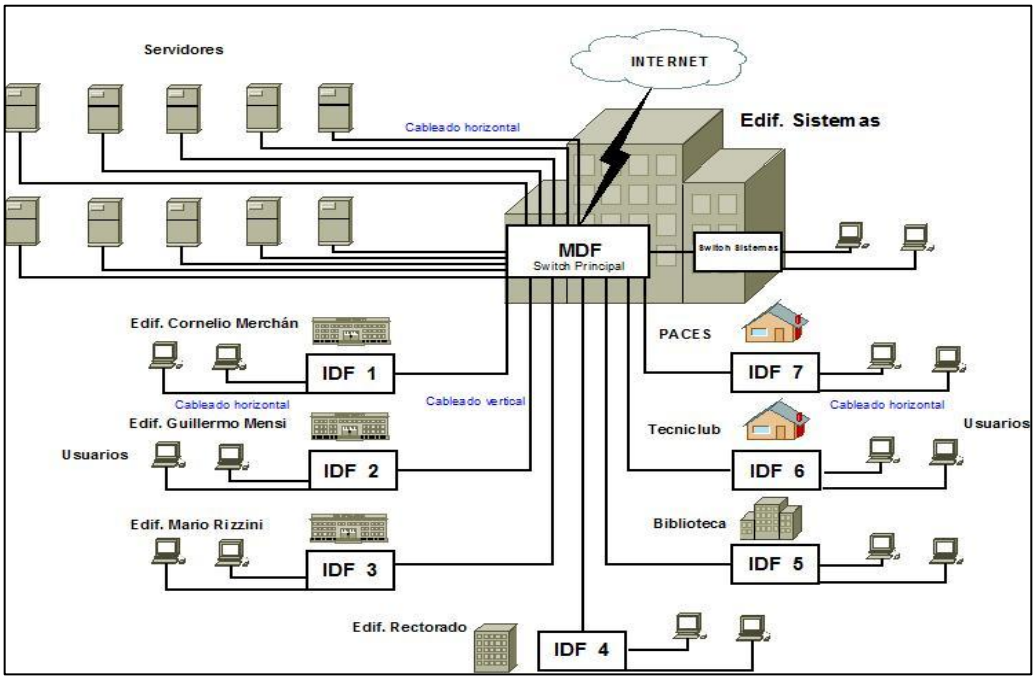


Figura 15 CAP III. Diagrama Físico de la UPS Sede-Cuenca
Fuente: P. Jimenez, entrevista personal, 24 de Octubre del 2011

En el gráfico podemos observar la ubicación del MDF y la distribución de cada uno de los IDF'S en los diferentes edificios de la UPS Sede Cuenca.

Las estaciones de trabajo se distribuyen a lo largo y ancho de cada una de las oficinas, cada una de ellas tiene una tarjeta de red el cual le permite conectarse a la red para el intercambio de archivos, enviar mensajes por correo electrónico, etc.

Los switches CISCO 3560 (capa 2) que se encuentran ubicados en los IDF'S de cada uno de los edificios se conectan por enlaces de fibra óptica multimodo a otro switch inteligente (capa 3) que se encuentra ubicado en su respectivo rack de datos dentro del MDF.

Mediante uno de los puertos del switch inteligente se realiza la conexión al firewall, el cual permite proteger la red interna de los intrusos y finalmente desde los puertos del firewall se realiza la conexión al Router con el fin de permitir la conexión con la red externa (WAN).

3.5.1 Características de los Equipos de Red

A continuación se describe las características principales de cada uno de los equipos que forman parte de la red de la UPS Sede Cuenca:

3.5.1.1 Servidores

Tabla 21 CAP III. Características de los Servidores

Característica	Descripción
Marca	IBM
Modelo	System X3200 M3
Procesador	Intel Xeon X3430 (2.4 Ghz/L3 8MB/1333 Mhz)
Memoria	8 GB DDR3 1333 Mhz capacidad máxima 48 GB
Tarjeta de video	ATI ES1000 (RN50)
Tarjeta de red	2 x Gigabit Ethernet.
Puertos	**Posterior:** Seriales: 2, Paralelo: 1, RJ-45: 1, DB-15: 1, USB: 4. **Frontal:** USB: 2
Disco duro:	100 GB
Sistema Operativo:	CentOS 6.2 excepto para el Servidor de Base de Datos cuyo S.O es Unix.

Fuente: P. Jimenez, entrevista personal, 25 de Octubre del 2011

Tabla 22 CAP III. Aplicaciones Instaladas en los Servidores

Nombre del Servidor	Servicios
Web	Paginas web, Liferay.
Proxy	DNS, DHCP, Squid.
Archivos	Almacenamiento de archivos.
Antivirus	Filtrado de correo electrónico, Bloqueo de páginas web y protección Anti Spam.
Desarrollo	Oracle Forms.
Biblioteca	Sitio Web de Ficheros
Aplicaciones	Oracle Forms.
Base de Datos	Oracle
Correo electrónico	Zimbra
Desarrollo de B.D	Oracle

Fuente: P. Jimenez, entrevista personal, 25 de Octubre del 2011

3.5.1.2 PC'S

Tabla 23 CAP III. Características de las PC's de los Laboratorios

Característica	Descripción
Procesador	Intel Core 2 Duo
Memoria RAM DDR3	4 GB
Velocidad	2.5 GHZ
Disco duro	100 GB
Sistema Operativo	Windows XP
Tarjeta de red	10/100 Mbps

Fuente: El Autor

Tabla 24 CAP III. Características de las PC's del Área Administrativa

Característica	Descripción
Procesador	Intel Core i3, i5,i7
Memoria RAM DDR3	4 GB
Velocidad	2.5 GHZ
Disco duro	100 GB
Sistema Operativo	Windows XP, Windows 7
Tarjeta de red	10/100 Mbps

Fuente: El Autor

3.5.1.3 Firewall

Tabla 25 CAP III. Características del Firewall

Característica	Descripción
Marca	CISCO
Modelo	ASA 5510
Número de Usuarios	Ilimitado
Máximo rendimiento(Mbps)	300
Número máximo de conexiones	50000
Número máximo de conexiones/segundo	6000
Paquetes/segundo(64bytes)	190000
Seguridad en la capa de aplicación	Si
Puertos integrados	5-10/100
Número máximo de VLANS	50 (trunk activado)

Fuente: ROUTER- SWITCH, (n.d), CISCO Firewalls Security, Obtenida el 26 de Octubre del 2011, de http://www.router-switch.com/asa5510-bun-k9-p-610.html

3.5.1.4 Router

Tabla 26 CAP III. Características del Router

Característica	Descripción
Marca	CISCO.
Modelo	2851.
Dimensiones	43.8 cm x 41.7 cm x 8.9 cm.
Peso	11,4 kg.
Memoria DRAM	512 MB (instalado) / 1 GB (max) – SDRAM
Memoria Flash	128 MB (instalado) / 256 MB (max).
Protocolo de enlace de datos	Ethernet, Fast Ethernet, Gigabit Ethernet.
Protocolo de transporte	IPSec.
Protocolo de administración remota	SNMP 3.
Estándares	IEEE 802.3af.
Voltaje	AC 120/230 V (50/60 Hz).

Fuente: ROUTER-SWITCH, (n.d), CISCO Routers, Obtenida el 27 de Octubre del 2011, http://www.router-switch.com/cisco2851-p-182.html

3.5.1.5 Switch

Tabla 27 CAP III. Características del Switch CISCO

Característica	Descripción
Modelo	3560
Número de puertos	48 x 10/100 + 4 x SFP
Protocolo de enrutamiento	RIP-1, RIP-2, HSRP, Enrutamiento estático
Protocolo de administración remota	SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, TFTP, SSH-2
Algoritmo de encriptación	SSL
Estándares	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1
Memoria flash	32 MB
Interfaces	48 x 10Base-T/100Base-TX - RJ-45 1 x console - RJ-45 – management 4 x SFP (mini-GBIC)
Voltaje	AC 120/230 V (50/60 Hz)
Dimensiones	44.3cm x 29.5cm x 4.4 cm
Peso	4,6 kg
Software	Cisco IOS IP Base

Fuente: ROUTER-SWITCH, (n.d), CISCO Switches, Obtenida el 27 de Octubre del 2011, de http://www.router-switch.com/ws-c3560v2-48ts-s-p-468.html

Tabla 28 CAP III. Características del Switch 3COM

Característica	Descripción
Modelo	SuperStack 3 Baseline 10/100 de 24 puertos.
Puertos	24 puertos 10 BASE-T/100BASE-TX con auto-detección y auto-configuración MDI/MDIX
Interfaces	RJ-45
Direcciones MAC que soporta:	4,000
Estándar	IEEE 802.1p
Alto	4.36 cm (1.7 pulgadas)
Ancho	44 cm (17.3 pulgadas)
Profundidad	23.5 cm (9.3 pulgadas)
Peso	3 kg

Fuente: PCEL, (n.d), Switches y Hubs para Empresas, Obtenida el 27 de Octubre del 2011, de http://www.pcel.com/mp/30559.html

3.5.1.6 Teléfonos IP

Tabla 29 CAP III. Teléfono IP CISCO 7911G

Característica	Descripción
Tipo de producto	Teléfono VoIP
Protocolos VoIP	SCCP
Códecs de voz	G.729a, G.729ab, G.711u, G.711ª
Visualizador:	Pantalla de cristal líquido – monocromo
Cantidad de puertos de red	2 x Ethernet 10/100Base-TX
Software compatible	Cisco CallManager
Calidad del servicio	IEEE 802.1Q (VLAN), IEEE 802.1p
Asignación de dirección IP	DHCP
Seguridad	AES de 128 bits
Propiedades de voz	Detección de actividad de voz (VAD)
Normas	CE, VCCI Class BITE, CISPR 24, EN 60950, EN 61000-3-2, EN55022, IEC 60950, EN 61000-3-3, EN55024, UL 60950, EN50082-1, CSA 22.2 No. 60950, ICES-003 Class B, EN 61000-6-1, FCC Part 15 B, FCC Part 68
Dimensiones	17.6 cm x15.2 cm x 20.3 cm
Peso	0.9 kg

Fuente: MERCADO ACTUAL, (n.d), Teléfonos IP, Obtenida el 28 de Octubre del 2011, de http://encuentraprecios.mercadoactual.es/mactual/fichaProd?productCode=121219

Tabla 30 CAP III. Teléfono IP CISCO 7912G

Característica	Descripción
Tipo de producto	Teléfono VoIP
Protocolos VoIP	SCCP,SIP
Códecs de voz	G.711, G.729
Visualizador:	Pantalla de cristal líquido – monocromo
Cantidad de puertos de red	2 x Ethernet 10Base-T/100Base-TX
Software compatible	Cisco CallManager 3.3
Calidad del servicio	IEEE 802.1Q (VLAN)
Asignación de dirección IP	DHCP
Protocolos de red	TFTP, Cisco Discovery Protocol (CDP)
Propiedades de voz	Generación de ruido confortable (CNG), detección de actividad de voz (VAD)
Normas	UL, VCCI, CISPR 22 Class B, EN 60950, EN 61000-3-2, EN50082, EN55022, ICES-003, IEC 60950, EN 61000-3-3, CSA 22.2 No. 950
Dimensiones	17.6 cm x 15.2 cm x 20.3 cm
Peso	0.9 kg

Fuente: HARDWARE.COM, (n.d), Cisco IP Phone 7912G, Obtenida el 28 de Octubre del 2011, de http://es.hardware.com/tienda/cisco/CP-7912G-CH1

Tabla 31 CAP III. Teléfono IP CISCO 7941G

Característica	Descripción
Tipo de producto	Teléfono VoIP
Protocolos VoIP	SCCP
Códecs de voz	G.729a, G.711u
Visualizador:	Pantalla de cristal líquido – monocromo
Cantidad de puertos de red	2 x Ethernet 10Base-T/100Base-TX/1000Base-T
Software compatible	Cisco CallManager
Calidad del servicio	IEEE 802.1Q (VLAN)
Asignación de dirección IP	DHCP
Protocolos de red	TFTP
Propiedades de voz	Detección de actividad de voz (VAD)
Normas	CISPR 22 Class B, EN 60950, EN 61000-3-2, EN55022, IEC 60950, EN 61000-3-3, EN55024, UL 60950, EN50082-1, CSA 22.2 No. 60950, ICES-003 Class B, IC CS-03, AS/NZ 3548 Class B, FCC Part 15 B, AS/NZS 60950-1, FCC Part 68
Dimensiones	27 cm x 15.2 cm x 20.3 cm
Peso	1.6 kg

Fuente: HARDWARE.COM, (n.d), Cisco IP Phone 7941G-GE, Obtenida el 28 de Octubre del 2011, de http://es.hardware.com/tienda/cisco/CP-7941G-GE

CAPITULO IV

DISEÑO DE LA SOLUCIÓN IPV6 PARA LA UNIVERSIDAD POLITECNICA SALESIANA SEDE CUENCA

4.1 Metodología de implementación de la red IPV6

El objetivo de este trabajo es realizar una simulación de la red actual de la UPS Sede-Cuenca en el Packet Tracer versión 5.3.2.0027 utilizando el mecanismo de transición Dual Stack.

El uso del método Dual Stack permite que los host y routers estén equipados con una pila para cada protocolo con el objetivo de tener la capacidad para enviar y recibir los dos tipos de paquetes que son IPV4 e IPV6.

De esta manera cuando se establezca una comunicación con un nodo IPV6, este nodo (IPV6/IPV4) actuará como un solo nodo IPV6, mientras que en la comunicación con un nodo IPV4 se comportará como un solo nodo IPV4.

Cada nodo IPV6/IPV4 se configura con dos direcciones IP, utilizando diferentes mecanismos por ejemplo para IPV4 el mecanismo DHCP (obtiene una dirección IPV4), y para IPV6 el mecanismo DHCPv6 (obtiene una dirección IPV6).

El método de transición Dual Stack nos permite facilitar la gestión de la implementación de IPv6, debido a que se maneja de forma gradual es decir se puede ir configurando pequeñas secciones del entorno de red. Si en el futuro desaparece el protocolo IPV4, lo único que se tendría que hacer es deshabilitar la pila IPV4 de cada nodo.

Finalmente podemos decir que el método de transición nos permite reducir el impacto sobre el costo, tiempo y funcionalidad de las aplicaciones.

A continuación se describe un esquema acerca del mecanismo de transición Dual Stack:

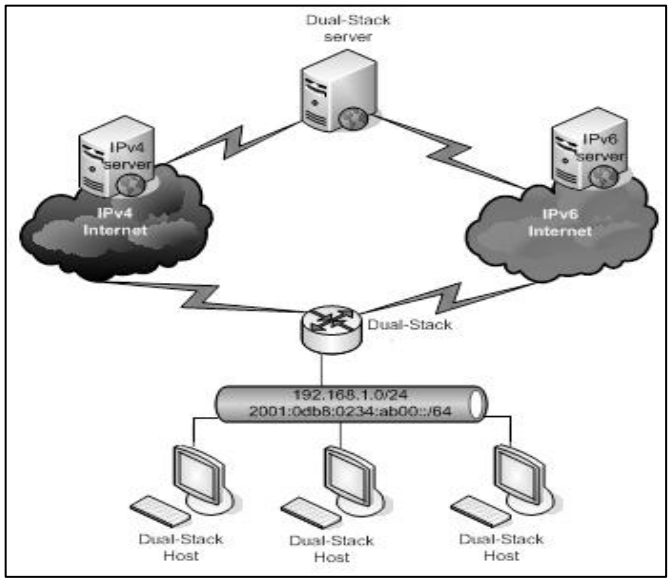


Figura 16 CAP IV. Mecanismo de Transición Dual Stack

Fuente: MDNX, (n.d), IPV4 to IPV6, Obtenida el 07 de Noviembre del 2011, de http://www.mdnx.com/news-events/ipv6-ipv4/

4.2 Conexión a Internet mediante IPV6

4.2.1 Selección de un proveedor de servicios

En la actualidad la red de la UPS Sede-Cuenca posee un enlace a internet mediante IPV4, otorgada por el ISP Telconet.

Telconet es una de las empresas más importantes del Ecuador que se caracteriza por ofrecer los siguientes servicios:

- Conexión permanente al Internet.
- Transmisión de datos.
- Comunicaciones unificadas.
- Tránsito al backbone de internet.
- Seguridad lógica.

De acuerdo a las investigaciones realizadas TELCONET es una de las redes del país que maneja IPV6, su implementación se basa en lo siguiente:

- Definición del modelo 6VPE.
- Habilitación de routers.
- Creación de un esquema de direccionamiento
- Laboratorio y pruebas.
- Liberación del producto.

Las ciudades y Universidades que actualmente soportan IPV6 en el Ecuador son las siguientes:

Guayaquil (ESPOL), Quito (EPN), Milagro (UNEMI), Ambato (UTA), Riobamba (UTN), Cuenca (UC), Guaranda (UEB), Loja (UTPL).

Movistar una de las empresas de telefonía móvil en el Ecuador afirmó que ya está utilizando la nueva versión del protocolo IP, según Guillermo Miño experto en el área tecnológica de Movistar afirmó su trabajo con IPV6 desde el mes de Marzo además señaló que la nueva tecnología se entrega a los clientes corporativos y en el 2013 se estaría brindando el soporte hacia los clientes individuales.[21]

El gerente de telecomunicaciones de ETAPA EP, Juan Córdova, afirmó que la mayoría del equipamiento de la empresa está listo para la migración a IPV6. [22]

Por otro lado el 35% de los módems que se encuentran instalados en los hogares no tienen capacidad para soportar la nueva versión del protocolo IP.

En la actualidad ETAPA EP, se encuentra realizando una consultoría internacional con el fin de realizar un estudio para la migración de IPV4 a IPV6. De esta manera podemos determinar que la empresa no ofrece soluciones como ISP con soporte para IPV6.

[21] EL TELÉGRAFO, (2012), La migración a IPV6 tomará cinco años, Obtenida el 04 de Julio del 2012, http://telegrafo.com.ec/index.php?option=com_zoo&task=item&item_id=39168&Itemid=112
[22] EL MERCURIO, (2012), Internet tendrá cambios por aumentos de cibernautas, Obtenida el 04 de Julio del 2012, http://www.elmercurio.com.ec/hemeroteca-virtual?noticia=333479

Debido a las características antes mencionadas podemos determinar que TELCONET es una de las empresas que ofrece la más amplia red de fibra óptica cuya extensión consta de 17000 km permitiendo interconectar redes de datos geográficamente distantes con la mayor garantía sobre las rutas físicas completamente independientes.

De acuerdo a las investigaciones realizadas en la empresa TELCONET se ha llegado a determinar que en la ciudad de Quito ya se está ofreciendo un soporte sobre IPV6, pero en la ciudad de Cuenca todavía se está estableciendo los cambios necesarios para brindar un soporte sobre IPV6 a corto plazo.

Por esta razón la UPS Sede-Cuenca debe mantenerse con el mismo ISP hasta el momento en el cual la empresa TELCONET esté lista para brindar los servicios y poder establecer una conexión hacia el internet sobre el protocolo IPV6.

4.3 Protocolos de enrutamiento

Según las características presentadas en la Sección 2.2.2 del Capítulo III, se ha tomado en consideración el protocolo OSFP debido a que es uno de los protocolos de enrutamiento interior más implementados para redes corporativas medianas y grandes.
A continuación presentamos un resumen de las características más importantes por las cuales se ha tomado en cuenta el protocolo OSPF para la migración a IPv6:

- Respuesta rápida y sin bucles ante cambios.
- Seguridad ante los cambios.
- Balanceo de carga en múltiples caminos.
- Escalabilidad en el crecimiento de rutas externas.

4.3.1 Configuración del protocolo OSPF en IPV6

1. Asignación de nombres al router

Router> enable
Router# configure terminal
Router(config)# hostname <nombre_del_router>

2. **Configuración del enrutamiento de paquetes IPV6**

Router(config)# ipv6 unicast-routing

3. Configuración de IPV6 en la interfaz FastEthernet de un router

Router(config)# interface fastEthernet 0/0
Router(config-if)# ipv6 enable
Router(config-if)# ipv6 address <Dirección_IPv6>/<Longitud_del_prefijo>
Router(config-if)# exit

4. Habilitar OSF dentro de un router:

Router(config)# interface fastEthernet 0/0
Router(config-if)# ipv6 ospf 1 area 0

5. Comando para verificar las configuraciones

Router# show ipv6 route ospf

4.3.2 Configuración del protocolo RIP en IPV6

1. Habilitar rip dentro de un router

Router# configure terminal
Router(config)# ipv6 router rip <numero_de_proceso>

2. Habilitar rip dentro de la interfaz de un router

Router(config)# interface fastEthernet 0/0
Router(config-if)# ipv6 rip <numero_de_proceso> enable

3. Comando para verificar las configuraciones del protocolo rip

Router# show ipv6 route rip

4.3.3 Configuración de rutas estáticas en IPV6

1. Habilitar rutas estáticas dentro de un router

Router# configure terminal
Router(config)# ipv6 route <prefijo_IPv6>/<longitud_del_prefijo> <interfaz_o_gateway>

En el caso de querer usar un gateway por defecto:

prefijo_IPv6/longitud_del_prefijo= :: /0

2. Comando para verificar la lista de todas las rutas estáticas

Router# show ipv6 route static

4.4 Escenarios de Transición a IPV6

El proceso de transición de IPv4 a IPv6 no es una tarea fácil, por este motivo se debe mantener una comunicación entre la versión actual y el protocolo IPv6, ya que tarde o temprano se deberá llevar a cabo un cambio completo de IPv4 a IPv6 sin la necesidad de afectar los servicios y aplicaciones de la red actual de la UPS Sede-Cuenca.

El objetivo de la transición no es remplazar los servicios IPv4 existentes, lo único que se trata de hacer es buscar diferentes escenarios para la migración ya que las instituciones modernas como la UPS necesitan implementar lo último en tecnología con el fin de obtener mecanismos estables para que se puedan transmitir los datos y demás aplicaciones tanto en IPv4 como en IPv6.

A continuación presentamos una descripción de los escenarios para la migración a IPv6 en la red de la UPS Sede-Cuenca:

4.4.1 Primer Escenario: Mantener IPv4 al mundo y tener IPv6 en la red local.

El esquema que se propone permite activar la configuración IPv6 por medio de DHCP en todos los equipos de red que se encuentran conectados al Switch principal y al Switch servidores hasta la conexión con el Firewall.

Dentro del Firewall CISCO ASA 5510 se establece la configuración del mecanismo de transición Dual Stack para permitir la comunicación de la red local de IPv6 a IPv4, además se debe realizar la configuración de NAT para permitir la traducción de las direcciones IPv4/IPv6.

A continuación se presenta el diagrama del Primer Escenario para la migración a IPv6:

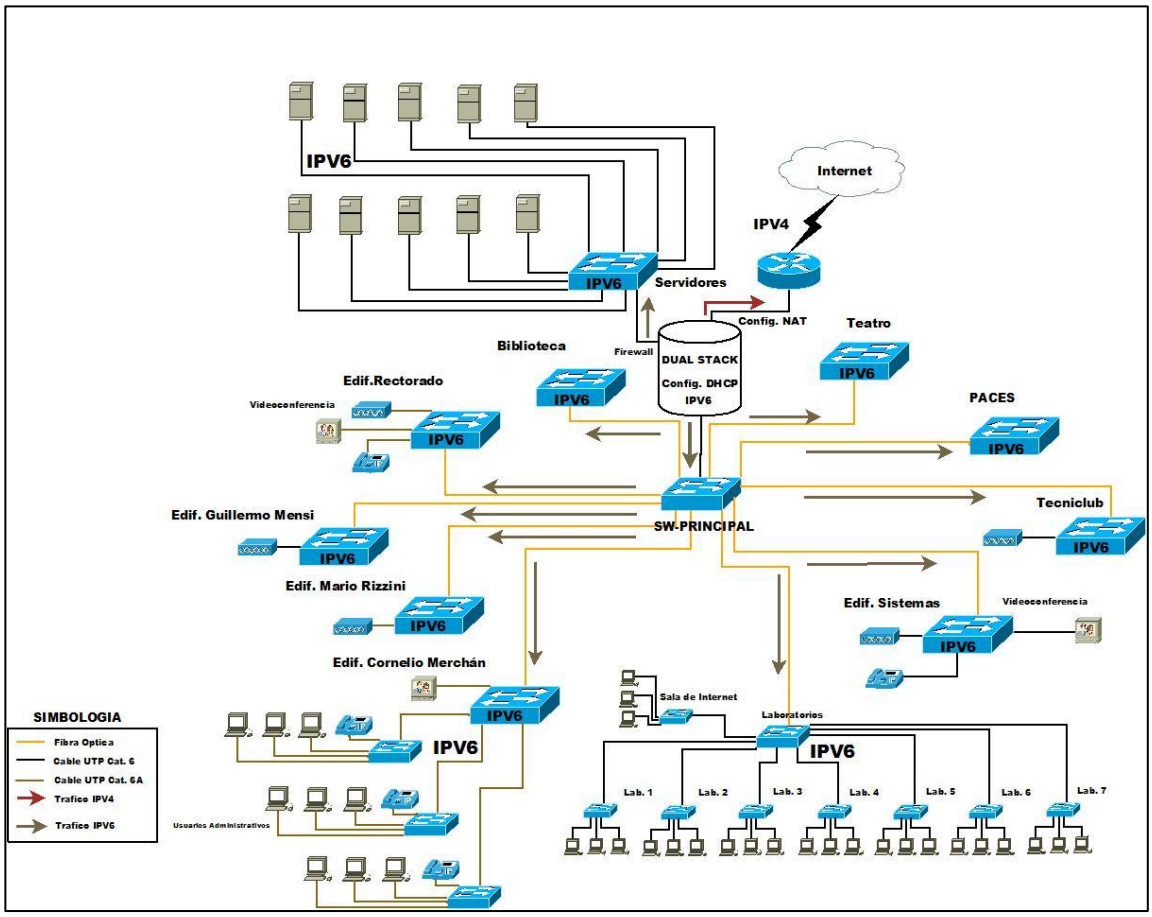


Figura 17 CAP IV. Mantener IPv4 al mundo y tener IPv6 en la red local

Fuente: El Autor

4.4.1.1 Comandos de Configuración del Primer Escenario

Para cada interfaz del Router Firewall y el Router Principal añadimos una dirección IPV4 e IPV6 de la siguiente manera:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ipv6 unicast-routing
Router(config)# interface fastEthernet 0/0
Router(config-if)#ipv6 enable
Router(config-if)#ip address 172.20.2.225 255.255.255.240
Router(config-if)#ipv6 address 2001:db8:2f:35::1/64
Router(config-if)#no shut
```

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface serial 0/1/0
Router(config-if)#ipv6 enable
Router(config-if)#ip address 200.0.0.1 255.255.255.252
Router(config-if)#ipv6 address 2001:db8:2f:40::1/64
Router(config-if)#clock rate 64000
Router(config-if)#no shut
```

Configuración de rutas estáticas en el Router Firewall de la siguiente manera:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 129.0.0.0 255.255.255.252 serial 0/1/0
Router(config)#ip route 200.0.0.0 255.255.255.252 serial 0/1/0
Router(config)#ipv6 route 2001:db8:2f:50::/64 serial 0/1/0
Router(config)#ipv6 route 2001:db8:4::/64 serial 0/1/0
Router(config)#ipv6 route 2001:db8:5::/64 serial 0/1/0
Router(config)#
```

Configuración de rutas estáticas en el Router Principal de la siguiente manera:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 172.20.3.224 255.255.255.240 serial 0/1/0
Router(config)#ip route 200.0.0.0 255.255.255.252 serial 0/1/0
Router(config)#ipv6 route 2001:db8:2f:35::/64 serial 0/1/0
Router(config)#ipv6 route 2001:db8:2f:1::/64 serial 0/1/0
Router(config)#ipv6 route 2001:db85:1::/64 serial 0/1/0
Router(config)#ipv6 route 2001:db85:2::/64 serial 0/1/0
Router(config)#ipv6 route 2001:db85:3::/64 serial 0/1/0
Router(config)#
```

Ejemplos de Configuración de ACLS en el Router Firewall:

```
Router(config)#ipv6 access-list Biblioteca
Router(config-ipv6-acl)# permit ipv6 any 2001:DB8:2F:17::/64
Router(config-ipv6-acl)# permit ipv6 any 2001:DB8:2F:50::/64
Router(config-ipv6-acl)# permit ipv6 any 2001:DB8:2F:35::/64
Router(config-ipv6-acl)# permit ipv6 any 2001:DB8:2F:40::/64

Router(config-ipv6-acl)#exit
Router(config)#interface fastEthernet 0/1.10
Router(config-subif)#ipv6 traffic-filter Biblioteca in
Router(config-subif)#exit

Router(config)#ipv6 access-list EdifRectorado
Router(config-ipv6-acl)#permit ipv6 any 2001:db8:2f:50::/64
Router(config-ipv6-acl)#permit ipv6 any 2001:db8:2f:40::/64
Router(config-ipv6-acl)#permit ipv6 any 2001:db8:2f:35::/64
Router(config-ipv6-acl)#exit
Router(config)#interface fastEthernet 0/1.20
Router(config-subif)#ipv6 traffic-filter EdifRectorado in
Router(config-subif)#exit

Router(config)#ipv6 access-list EdifGuillermoMensi
Router(config-ipv6-acl)#permit ipv6 any 2001:db8:2f:50::/64
Router(config-ipv6-acl)#permit ipv6 any 2001:db8:2f:40::/64
Router(config-ipv6-acl)#permit ipv6 any 2001:db8:2f:35::/64
Router(config-ipv6-acl)#permit ipv6 any 2001:db8:2f:20::/64
Router(config-ipv6-acl)#exit

Router(config)#interface fastEthernet 0/1.30
Router(config-subif)#ipv6 traffic-filter EdifGuillermoMensi in
Router(config-subif)#exit
```

4.4.2 Segundo Escenario: Tener IPv6 en el mundo y tener IPv6 en la red local

El esquema que se propone es similar al primer escenario en donde tenemos que activar la configuración IPv6 por medio de DHCP en todos los equipos de red que se encuentran conectados al Switch principal y al Switch servidores hasta la conexión con el Firewall.

En este escenario estamos asumiendo que el mundo ya se encuentra funcionando completamente en IPv6, debido a esto para acceder al Internet desde nuestra red local,

lo único que tenemos que hacer es configurar el Firewall utilizando un direccionamiento estático para IPv6.

A continuación se presenta el diagrama del Segundo Escenario para la migración a IPv6:

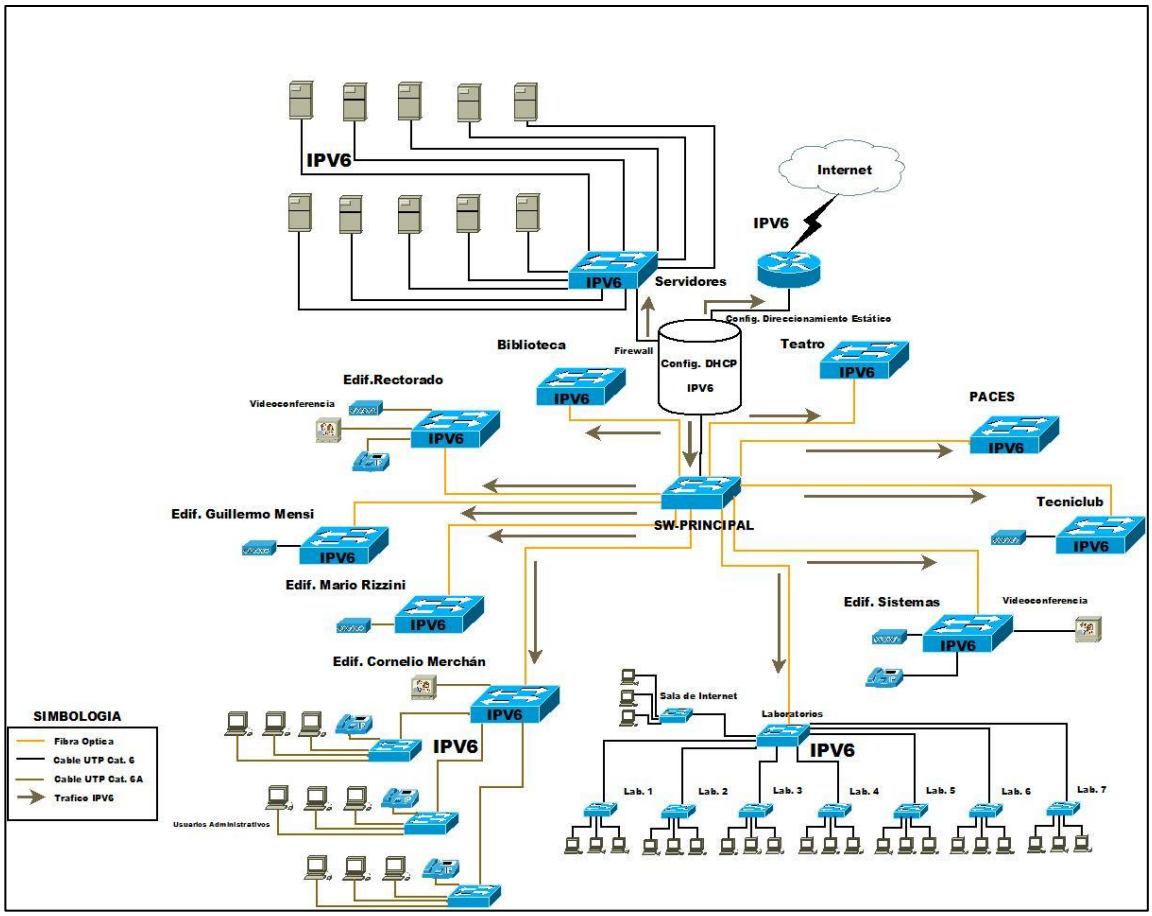


Figura 18 CAP IV. Tener IPv6 en el mundo y tener IPv6 en la red local
Fuente: El Autor.

4.4.2.1 Comandos de Configuración del Segundo Escenario

En este escenario para cada interfaz del Router Firewall y el Router Principal se debe configurar una dirección IPV6.

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)#ipv6 unicast-routing
Router(config)# interface fastEthernet 0/0
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 address 2001:db8:2f:35::1/64
Router(config-if)#no shut

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface serial 0/1/0
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 address 2001:db8:2f:40::1/64
Router(config-if)#clock rate 64000
Router(config-if)#no shut
```

Configuración de rutas estáticas en el Router Firewall de la siguiente manera:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ipv6 route 2001:db8:2f:50::/64 serial 0/1/0
Router(config)#ipv6 route 2001:db8:4::/64 serial 0/1/0
Router(config)#ipv6 route 2001:db8:5::/64 serial 0/1/0
Router(config)#
```

Configuración de rutas estáticas en el Router Principal de la siguiente manera:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ipv6 route 2001:db85:1::/64 serial 0/1/0
Router(config)#ipv6 route 2001:db85:2::/64 serial 0/1/0
Router(config)#ipv6 route 2001:db85:3::/64 serial 0/1/0

Router(config)#ipv6 route 2001:db8:2f:1::/64 serial 0/1/0
Router(config)#ipv6 route 2001:db8:2f:2::/64 serial 0/1/0
Router(config)#ipv6 route 2001:db8:2f:3::/64 serial 0/1/0
Router(config)#ipv6 route 2001:db8:2f:4::/64 serial 0/1/0
Router(config)#ipv6 route 2001:db8:2f:5::/64 serial 0/1/0
!
!
!
Router(config)#ipv6 route 2001:db8:2f:34::/64 serial 0/1/0

Router(config)#
```

Ejemplos de Configuración de ACLS en el Router Firewall:

En este caso la configuración es la misma que se utilizó en el Escenario 1:

Ejemplo:

```
Router(config)#ipv6 access-list Biblioteca
Router(config-ipv6-acl)# permit ipv6 any 2001:DB8:2F:17::/64
Router(config-ipv6-acl)# permit ipv6 any 2001:DB8:2F:50::/64
Router(config-ipv6-acl)# permit ipv6 any 2001:DB8:2F:35::/64
Router(config-ipv6-acl)# permit ipv6 any 2001:DB8:2F:40::/64

Router(config-ipv6-acl)#exit
Router(config)#interface fastEthernet 0/1.10
Router(config-subif)#ipv6 traffic-filter Biblioteca in
Router(config-subif)#exit
```

Resultados de la Configuración del Escenario 1 y Escenario 2:

Protocolo DHCP:

Debido a que no se puede asignar un rango automático de direcciones IPV6 para cada subinterfaz del router (es decir una subred para cada vlan) se estableció la configuración de cada una de las máquinas de los usuarios añadiendo una dirección estática debido a que el Packet Tracer no soporta todos los comandos de configuración.

A continuación se presenta un ejemplo para establecer la configuración del protocolo DHCP según el libro Cisco IOS IPv6 Configuration Guide:

En este caso se ha tomado como referencia la Configuración de DHCP para la Biblioteca y el EdifRectorado:

```
ipv6 unicast-routing
ipv6 cef
ipv6 dhcp pool Biblioteca
prefix-delegation 2001:DB8:2f:1::/64 00030001C402068F0000
prefix-delegation pool Biblioteca
dns-server 2001:DB8:2f:35::10
domain-name cisco.com
```

```
ipv6 dhcp pool EdifRectorado
prefix-delegation 2001:DB8:2:2::/64 00030001C402068F0000
prefix-delegation pool EdifRectorado
dns-server 2001:DB8:2f:35::1
domain-name cisco.com

ipv6 multicast-routing

interface FastEthernet0/0
 no ip address
 speed 100
 full-duplex

interface FastEthernet0/0.10
encapsulation dot1Q 10
ipv6 address 2001:DB8:2f:1::1/64
ipv6 enable
ipv6 dhcp server Biblioteca

interface FastEthernet0/0.20
encapsulation dot1Q 20
ipv6 address 2001:DB8:2f:2::1/64
ipv6 enable
ipv6 dhcp server EdifRectorado
```

Teléfonos IP

El Packet Tracer no soporta la configuración de los Teléfonos IP sobre el protocolo IPV6 debido a esto en el Escenario 1 se mantiene la representación de cada uno de los teléfonos IP ya que se está trabajando con IPV4/IPV6, pero en el Escenario 2 se ha eliminado todos los Teléfonos IP debido a que se está trabajando en un escenario en donde todo funciona sobre IPV6.

4.5 DISEÑO DEL DIAGRAMA LÓGICO

4.5.1 Diseño de la topología de red IPv6

Según los criterios expuestos en la Sección 3.6.1 se ha podido determinar que la mayoría de equipos son de marca CISCO y todos soportan IPv6. Uno de los puntos más importantes es que la UPS Sede-Cuenca tiene varios técnicos que manejan y brindan un soporte adecuado en los equipos CISCO.

La topología de red se mantiene, el objetivo de este análisis es utilizar el simulador de red Packet Tracer con el fin de probar las configuraciones de cada uno de los equipos antes de su implementación.

4.5.2 Diseño de las VLANS en IPv6

Las consideraciones que se aplican para configurar una VLAN en IPV6 son las mismas que se aplican en IPV4.

Utilizando el mecanismo de transición Dual Stack, las configuraciones tanto de IPV4 como IPV6 atraviesan la misma VLAN de esta manera el uso de IPV6 en las VLANS de datos y voz son fácilmente soportadas.

El diseño de las VLANS para la red de la UPS Sede-Cuenca usando IPV6 se mantiene con las mismas características descritas en la Sección 3.4.2.

4.5.2.1 Configuración de VLANS usando IPV6

Ejemplo de Creación de sub-interfaces en el router:

Router# configure terminal
Router(config)# interface fastEthernet 0/1.10
Router(config-subif)# description VLAN Biblioteca
Router(config-subif)# encapsulation dot1Q 10
Router(config-subif)# ipv6 addess 2001:db8:2f:2::1/64

Ejemplo de Creación de VLANS en el Switch

Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name Biblioteca
Switch(config-vlan)# exit

Ejemplo de configuración de los puertos de cada Interfaz del Switch:

Switch# configure terminal
Switch(config)# interface fa0/1
*Switch(config-if)# **switchport mode trunk***
Switch(config-if)# exit

Switch# configure terminal
Switch(config)# interface fa0/2
*Switch(config-if)# **switchport mode access***
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit

4.5.3 Reglas de conectividad entre VLANS para IPV6

Las reglas de conectividad entre VLANS descritas en la Sección 3.4.2.1 se mantienen con el fin de proporcionar mayor seguridad en el acceso hacia departamentos que manejan la misma información.

Sintaxis para configurar ACLS en IPV6

Switch# configure terminal
*Switch(config)# ipv6 **access-list** access-list-name*
*Switch(config-ipv6-acl)# **deny** | **permit** protocol*
{source-ipv6-prefix/prefix-length | **any** | **host** *source-ipv6-address}*
[operator [*port-number]]*
{destination-ipv6-prefix/ prefix-length | **any** | **host** *destination-ipv6-address}*
[operator [*port-number]]*
*[*dscp *value*] [fragments] [log] [log-input] [sequence *value*] [time-range *name]*

Ejemplo:

Switch# configure terminal
Switch(config)# ipv6 access-list Biblioteca
Switch(config-ipv6-acl)# permit tcp host 2001:DB8:0:1::2 host 2001:DB8::1
Switch(config-ipv6-acl)# deny ipv6 any any log

4.5.4 Direccionamiento IPv6 en la red de la UPS Sede-Cuenca

Para la elaboración del diagrama de red de la UPS Sede-Cuenca se ha tomado como base la siguiente dirección IPV6:

Dirección IPV6 en formato hexadecimal: 2001:0db8:002f:0000:0000:0000:0000:0000

Máscara de red:/64

Esta dirección IPV6 se puede representar de la siguiente manera: 2001:db8:2f:0::/64

Según las características mencionadas en la Sección 3.4.3 el requerimiento de host para toda la red de la UPS Sede-Cuenca incluido el porcentaje de crecimiento futuro es de 875 host.

A continuación se presenta la siguiente tabla según el número total de direcciones IPV6 disponibles.

Tabla 32CAP IV. Número de Direcciones IPV6 disponibles

Direcciones IPV6 por cada m^2	6.67126144781401e+23
Direcciones IPV6 por cada habitante	60,000 millones de billones
Direcciones IPV6 por subred en la UPS	18.446.744.073.709.551.616

Fuente: El Autor

Para la configuración de las direcciones IPV6 de cada equipo se utilizó el mecanismo de autoconfiguración por DHCP existente en IPV6 a excepción de los equipos de red como switch, router, firewall en donde se realizó la asignación de direcciones IPV6 de forma manual para simplificar su configuración y administración.

4.5.4.1 Distribución de direcciones IPV6 para cada VLAN

Según las características descritas en la Sección 3.4.4 la distribución de las direcciones IPV6 para cada VLAN quedaría de la siguiente manera:

Tabla 33 CAP IV. Configuración de VLANS sobre IPV6

Switch Principal		**Router Firewall**	
# VLAN	Nombre de VLAN	Sub-interfaz	Dirección IPV6
10	Biblioteca	Fa 0/1.10	2001:db8:2f:1:1/64
20	EdifRectorado	Fa 0/1.20	2001:db8:2f:2:1/64
30	EdifGuillermoMensi	Fa 0/1.30	2001:db8:2f:3:1/64
40	Estudiantes	Fa 0/1.40	2001:db8:2f:4:1/64
41	CarrerasUPS	Fa 0/1.41	2001:db8:2f:5:1/64
42	ConsejoAcadémico	Fa 0/1.42	2001:db8:2f:6:1/64
43	ConsejoAdminEconómico	Fa 0/1.43	2001:db8:2f:7:1/64
44	SecretariaGeneral	Fa 0/1.44	2001:db8:2f:8:1/64
45	SecretariasTécnicas	Fa 0/1.45	2001:db8:2f:9:1/64
46	ContabilidadGeneral	Fa 0/1.46	2001:db8:2f:10:1/64
47	BienestarEstudiantil	Fa 0/1.47	2001:db8:2f:11:1/64
48	UnidadPostgrados	Fa 0/1.48	2001:db8:2f:12:1/64
49	UnidadPlanifEvaluación	Fa 0/1.49	2001:db8:2f:13:1/64
50	UnidadVinColectividad	Fa 0/1.50	2001:db8:2f:14:1/64
51	UnidadInvestigacion	Fa 0/1.51	2001:db8:2f:15:1/64
52	GestTalentoHumano	Fa 0/1.52	2001:db8:2f:16:1/64
53	AreasConocimiento	Fa 0/1.53	2001:db8:2f:17:1/64
54	EgresadosGraduados	Fa 0/1.54	2001:db8:2f:18:1/64
55	PastoralUPS	Fa 0/1.55	2001:db8:2f:19:1/64
60	EdifMarioRizzini	Fa 0/1.60	2001:db8:2f:20:1/64
70	LabInternet	Fa 0/1.70	2001:db8:2f:21:1/64
71	Laboratorio1	Fa 0/1.71	2001:db8:2f:22:1/64
72	Laboratorio2	Fa 0/1.72	2001:db8:2f:23:1/64
73	Laboratorio3	Fa 0/1.73	2001:db8:2f:24:1/64
74	Laboratorio4	Fa 0/1.74	2001:db8:2f:25:1/64
75	Laboratorio5	Fa 0/1.75	2001:db8:2f:26:1/64
76	Laboratorio6	Fa 0/1.76	2001:db8:2f:27:1/64
77	Laboratorio7	Fa 0/1.77	2001:db8:2f:28:1/64
80	EdifSistemas	Fa 0/1.80	2001:db8:2f:29:1/64
90	Tecniclub	Fa 0/1.90	2001:db8:2f:30:1/64
100	PACES	Fa 0/1.100	2001:db8:2f:31:1/64
110	Teatro	Fa 0/1.110	2001:db8:2f:32:1/64
120	Wireless	Fa 0/1.120	2001:db8:2f:33:1/64
130	TelefonosIP	Fa 0/1.130	2001:db8:2f:34:1/64

Fuente: El Autor

4.5.4.2 Elaboración de las tablas de enrutamiento sobre IPV6

La información de las tablas de enrutamiento del router principal y el router firewall de cada uno de los escenarios propuestos en este proyecto de tesis sobre IPV6 se describen a continuación:

Tabla 34 CAP IV. Escenario 1 Tabla de enrutamiento del Router Principal

Dirección IP destino	Interfaz de salida	Next Hop IP
172.20.3.224/28	Serial 0/1/0	
200.0.0.0/30	Serial 0/1/0	
2001:db8:1::/64	Serial 0/1/0	
2001:db8:1::/64	Serial 0/1/0	
2001:db8:3::/64	Serial 0/1/0	
2001:db8:2f:1::/64	Serial 0/1/0	
2001:db8:2f:35::/64	Serial 0/1/0	

Fuente: El Autor

Tabla 35 CAP IV. Escenario 1 Tabla de enrutamiento del Router Firewall

Dirección IP destino	Interfaz de salida	Next Hop IP
129.0.0.0/30	Serial 0/1/0	
200.0.0.0/30	Serial 0/1/0	
2001:db8:4::/64	Serial 0/1/0	
2001:db8:5::/64	Serial 0/1/0	
2001:db8:2f:50::/64	Serial 0/1/0	

Fuente: El Autor

Tabla 36 CAP IV. Escenario 2 Tabla de enrutamiento del Router Principal

Dirección IP destino	Interfaz de salida	Next Hop IP
2001:db8:1::/64	Serial 0/1/0	
2001:db8:2::/64	Serial 0/1/0	
2001:db8:3::/64	Serial 0/1/0	
2001:db8:2f:1::64	Serial 0/1/0	
2001:db8:2f:2::64	Serial 0/1/0	
2001:db8:2f:3::64	Serial 0/1/0	
2001:db8:2f:4::64	Serial 0/1/0	
2001:db8:2f:5::64	Serial 0/1/0	
2001:db8:2f:6::64	Serial 0/1/0	
2001:db8:2f:7::64	Serial 0/1/0	
2001:db8:2f:8::64	Serial 0/1/0	
2001:db8:2f:9::64	Serial 0/1/0	
2001:db8:2f:10::64	Serial 0/1/0	
2001:db8:2f:11::64	Serial 0/1/0	
2001:db8:2f:12::64	Serial 0/1/0	
2001:db8:2f:13::64	Serial 0/1/0	
2001:db8:2f:14::64	Serial 0/1/0	
2001:db8:2f:15::64	Serial 0/1/0	
2001:db8:2f:16::64	Serial 0/1/0	
2001:db8:2f:17::64	Serial 0/1/0	
2001:db8:2f:18::64	Serial 0/1/0	
2001:db8:2f:19::64	Serial 0/1/0	
2001:db8:2f:21::64	Serial 0/1/0	
2001:db8:2f:22::64	Serial 0/1/0	
2001:db8:2f:23::64	Serial 0/1/0	
2001:db8:2f:24::64	Serial 0/1/0	
2001:db8:2f:25::64	Serial 0/1/0	
2001:db8:2f:26::64	Serial 0/1/0	
2001:db8:2f:27::64	Serial 0/1/0	
2001:db8:2f:28::64	Serial 0/1/0	
2001:db8:2f:29::64	Serial 0/1/0	
2001:db8:2f:30::64	Serial 0/1/0	
2001:db8:2f:31::64	Serial 0/1/0	
2001:db8:2f:32::64	Serial 0/1/0	
2001:db8:2f:33::64	Serial 0/1/0	
2001:db8:2f:34::64	Serial 0/1/0	
2001:db8:2f:35::64	Serial 0/1/0	

Fuente: El Autor

Tabla 37 CAP IV. Escenario 2 Tabla de enrutamiento del Router Firewall

Dirección IP destino	Interfaz de salida	Next Hop IP
2001:db8:4::/64	Serial 0/1/0	
2001:db8:5::/64	Serial 0/1/0	
2001:db8:2f:50::/64	Serial 0/1/0	

Fuente: El Autor

4.5.5 Servicios de la Intranet sobre IPV6

Los servidores instalados en la red de la UPS Sede-Cuenca brindan diferentes servicios a usuarios como profesores, alumnos y personal administrativo entre ellos se encuentran las consultas de los datos financieros, consulta de notas, record académico, transferencia de archivos, correo electrónico, etc.

La mayoría de estos servicios tienen soporte para IPV6 debido a que se encuentra instalado sobre el S.O CentOS y Unix que ofrece muchas facilidades para la implementación, lo único que se tiene que modificar son los archivos de configuración.

4.5.5.1 Configuración de un Servidor Web

La configuración de un servidor web en IPV6 se realiza de la siguiente manera:

El servidor web debe tener una dirección IPV6 que debe ser registrada en el DNS utilizando los registros AAAA, además se debe realizar la configuración para que escuche direcciones IPV6.

La UPS Sede-Cuenca utiliza la plataforma web corporativa Liferay la cual permite desarrollar soluciones empresariales con resultados inmediatos y valor a largo plazo.

Liferay se diferencia de otras soluciones por su equilibrio óptimo entre funcionalidad práctica, usabilidad, e innovación técnica. A continuación se describe algunas de sus características:

- Facilita el diseño de interfaces de usuario.
- Personalización de usuarios.
- Framework de integración de aplicaciones.
- Soporte de campos personalizados.
- Integración de motores de reglas.
- Plataforma SOA.
- Auditoria y monitorización de rendimiento.

La plataforma Liferay se ejecuta por encima de Apache Tomcat e incluye una API agradable la cual permite agregar fácilmente componentes que no forman parte del núcleo.

Dentro del Apache web Server existe un archivo de configuración llamado "***httpd.conf***" que utiliza un Listen para configurar la dirección y el puerto de escucha del servidor web.

La dirección IPV6 debe ser ingresada dentro de los corchetes de la siguiente manera:

 # cat httpd.conf
Listen [2001:db8:2f:0::25]

De la misma forma la asignación del host virtual sobre IPV6 debe estar ingresada dentro de los corchetes de la siguiente manera:

 # cat httpd.conf
NameVirualHost 172.20.0.30
NameVirualHost [2001:db8:2f:0::30]

Si el nombre de dominio ups.edu.ec se resuelve como una dirección IPV6, hay la posibilidad de configurar el JVM para preferir una pila IPV4 sobre IPV6 de la siguiente manera:

-Djava.net.preferIPv4Stack=true

4.5.5.2 Configuración del correo electrónico Zimbra

Debido a que el protocolo IPV4 todavía se está usando, es necesario convivir con la existencia de un entorno mixto IPV4/IPV6 para luego pasar hacia un entorno único sobre IPV6.

Zimbra permite trabajar con IPV6 desde la versión 7.0 de forma limitada por lo que requiere una configuración especial. En la actualidad solo algunos servicios soportan IPV6 en la Suite de Zimbra por lo que se debe realizar lo siguiente:

Se debe instalar un nodo especial que permita el acceso al internet con IVP6, en donde se deberá instalar los paquetes *zimbra-proxy* y *zimbra-mta*. Este nodo deberá tener una dirección localhost sobre IPV4 definido como 127.0.0.1, y de manera adicional una dirección IP definida sobre un host IPV6.

Este nodo puede tener habilitado IPV4 para una interfaz pública o también se lo puede ejecutar sobre un modo mixto. Una vez instalado este nodo se lo puede configurar de la siguiente manera:

ipv6 - Only IPv6 address for the host
both - Use both IPv4 and IPv6 addresses for the host

Este nodo se puede controlar a través de la clave de configuración del servidor ***zimbraIPMode*** que puede tener un valor de operación de IPV4/IPV6 ó solamente sobre IPV6.

El rango de direcciones para el servidor deberá ser añadido dentro de las configuraciones de ***zimbraMtaMyNetwork*** vía zmprov.

Ejemplo:

zmprov ms edge.example.com zimbraMtaMyNetworks
"127.0.0.0/8 [::1]/128 x.x.x.x/x [xxxx:xxxx:xxxx::x]/x"

4.5.6 Evaluación del Diagrama Lógico

A continuación se describe una tabla con todos los puntos analizados en esta Sección con el fin de poder determinar las acciones que se deben realizar para poder establecer el proceso de migración hacia IPv6.

Tabla 38 CAP IV. Evaluación del Diagrama Lógico

Tema	Acción a realizar
Diseño de la topología de red	La topología de red se mantiene, lo único que cambia es la configuración de los equipos utilizando la nueva versión IPv6. Ver Sección 4.5.1
Diseño de las VLANS	El diseño de las VLANS se mantiene, lo único que cambia es la configuración de las VLANS utilizando IPv6. Ver Sección 4.5.2 y 4.5.2.1
Distribución de las direcciones IP.	La distribución de las direcciones cambia de IPv4 a IPv6. Ver Sección 4.5.4
Distribución de las direcciones IP para cada VLAN.	La distribución de las direcciones IPv4 para cada VLAN cambia de IPv4 a IPv6. Ver Sección 4.5.4.1
Elaboración de las tablas de enrutamiento.	La elaboración de las tablas de enrutamiento cambia de IPv4 a IPv6. Ver Sección 4.5.4.2
Servicios de la Intranet	Los Servicios de la Intranet se mantienen, lo único que se debe realizar es la actualización y configuración de las aplicaciones para que soporten IPv6. Ver Sección 4.5.5

Fuente: El Autor

4.6 DISEÑO DEL DIAGRAMA FISICO

4.6.1 Evaluación del Diagrama Físico

El diagrama físico de red de la UPS Sede Cuenca se mantiene debido al análisis realizado en esta sección donde se ha podido observar que la ubicación del MDF y la distribución de cada uno de los IDF'S se encuentran establecidos de forma correcta debido a las altas normas de seguridad y calidad que tiene la Universidad.

A continuación se realiza un análisis para evaluar el hardware y software de todos los equipos que forman parte de la red de la UPS Sede-Cuenca:

4.6.1.1 Hardware

El proceso de migración de la red de la Universidad requiere que todos sus equipos cuenten con soporte para IPv6. A continuación se presenta un resumen de los resultados obtenidos al analizar cada uno de los equipos de red de la UPS Sede-Cuenca:

Tabla 39 CAP IV. Análisis de los Equipos

Equipo de red	Marca/Modelo	Soporta IPv6	Acción a realizar
Servidores	IBM/ System X3200 M3	Si	Verificar que se encuentre instalado las actualizaciones recientes del S.O para la activación de IPv6.
PC's		Si	Verificar que se encuentre instalado las actualizaciones recientes del S.O para la activación de IPv6.
Firewall	CISCO ASA 5510	Si	Descargar actualizaciones del SO.
Router	CISCO 2851	Si	Descargar actualizaciones del SO.
Switch	CISCO 3560	Si	Descargar actualizaciones del SO.
	3COM SuperStack 3 Baseline 10/100	Si	Descargar actualizaciones del SO.
Teléfonos IP	CISCO 7911G	Si	Descargar actualizaciones del SO.
	CISCO 7912G	Si	Descargar actualizaciones del SO.
	CISCO 7941G	Si	Descargar actualizaciones del SO.

Fuente: El Autor

4.6.1.2 Software

La mayor parte de los Sistemas Operativos cuentan con soporte para IPv6 debido a que se encuentra activado por defecto, en algunos casos se requiere activar el soporte para IPv6 utilizando diferentes comandos, a continuación se describe una lista de los Sistemas Operativos instalados en los equipos de la UPS Sede Cuenca:

Tabla 40 CAP IV. Análisis del S.O de los Servidores

Servidor	S.O Instalado	Soporta IPv6	Acción a realizar
Web	CentOS 6.2	Si	Cargar el módulo IPv6 del sistema operativo en el caso de ser necesario.
Proxy			
Archivos			
Antivirus			
Desarrollo			
Biblioteca			
Aplicaciones			
Correo electrónico			
Desarrollo de B.D			
Base de datos	Unix	Si	Cargar el módulo IPv6 del sistema operativo en el caso de ser necesario

Fuente: El Autor

Tabla 41 CAP IV. Análisis del S.O de los PC's

Tipos de usuarios	S.O Instalado	Soporta IPv6	Acción a realizar
Administrativos	Windows 7	Si	Activar soporte para IPv6.
Estudiantes	Windows XP(SP 2)	Si	Activar soporte para IPv6.

Fuente: El Autor

CAPITULO V

DESARROLLO DEL PLAN DE IMPLEMENTACIÓN

5.1 Consideraciones Generales

Con el fin de facilitar el proceso de transición entre las dos versiones de IP se ha venido desarrollando una serie de técnicas, que permiten mantener toda la base de redes instaladas sobre IPV4 compatibles con IPV6, de esta manera se podrá mantener la coexistencia entre los dos protocolos con el objetivo de alcanzar el éxito en la transición a IPV6.

Todas las técnicas de transición analizadas en ente proyecto tienen características específicas y se pueden aplicar de manera individual o junto con otras técnicas para acomodarse a las necesidades de diferentes empresas, de esta forma una migración a IPV6 se lo puede realizar paso a paso, iniciando desde un computador hacia toda una red corporativa.

Debido a que el período de coexistencia entre los dos protocolos puede durar por un largo período de tiempo, la implementación de un método que permita la interoperabilidad entre el protocolo IPV4 e IPV6 nos será de gran ayuda, de esta manera se podrá garantizar una migración segura hacia el nuevo protocolo mediante el empleo de pruebas que permitan conocer las ventajas que nos ofrecen los mecanismo de transición.

En la primera fase de implementación sobre la red de la Universidad Politécnica Salesiana Sede-Cuenca, no es recomendable tener nodos que trabajen solamente con la versión IPV6, debido a que muchos servicios y aplicaciones de red continúan trabajando solamente sobre IPV4, por este motivo se ha visto necesario implementar el método Dual Stack.

5.2 Perspectiva general de la Metodología

A continuación se describe la metodología de planeación estratégica de tecnologías de la información (PETI) que está compuesta por las siguientes 4 fases:

5.2.1 Fase 1: Situación Actual

Durante la última década de avance de IPV6, se ha podido determinar que el desarrollo de Internet es cada día más grande mostrando una taza de crecimiento acelerada cuyo número de host conectados a Internet pasó de 30000000 a 732000000 en la actualidad, mientras tanto día a día aumenta el número de usuarios y dispositivos conectados a la redes de computadoras.

Los resultados del crecimiento de Internet lo podemos observar en la Figura.19

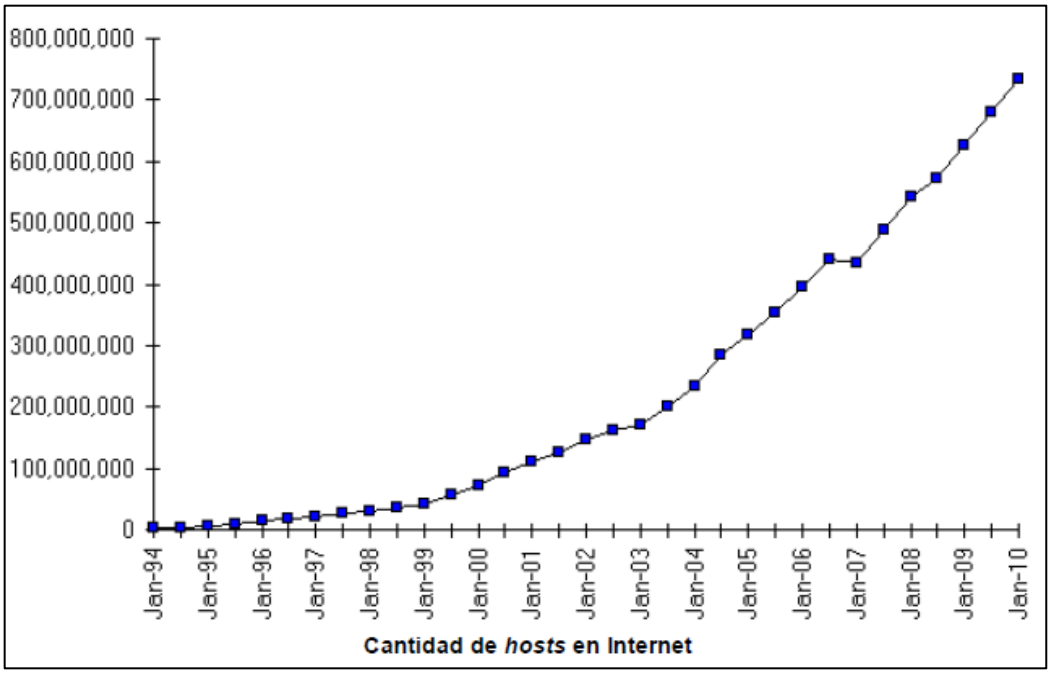


Figura 19 CAP V. Cantidad de host en Internet

Fuente: Rodrigo dos Santos, Antonio M. Moreiras, Eduardo Ascenço Reis, Ailton Soares da Rocha, (2010), Curso IPV6 Básico,

El desarrollo de Internet se puede observar a través de diversos factores y numerosas investigaciones que han demostrado que en el mundo existen alrededor de 1.733.993.741 usuarios de Internet (25,6% de la población mundial), lo cual permite determinar que en los últimos 9 años se ha dado un crecimiento de 380,3%. Si la tasa de crecimiento se mantiene, podemos determinar que dentro de 2 años existirán 200 millones de usuarios.

"Según datos del MINTEL (Ministerio de Telecomunicaciones) y el INEC (Instituto Nacional de Estadísticas y Censos) se ha determinado que en Ecuador existe una aplicación total de Internet que representa el 36,77 % es decir alrededor de 5,5 millones de usuarios a nivel nacional.

De acuerdo a los datos se ha podido determinar que el acceso al internet ha aumentado 7 veces más en relación al año 2006, debido a que 25 de cada 100 hogares ecuatorianos cuentan con una computadora de escritorio y 10 poseen un equipo portátil."[23]

A continuación se presentan los pasos para determinar la situación actual de la red de la UPS Sede-Cuenca:

Paso 1. Identificación del alcance competitivo de la organización:

La UPS Sede-Cuenca como institución educativa se encuentra entre una de las mejores universidades de la ciudad de Cuenca debido a su infraestructura y al avance tecnológico de sus laboratorios, razón por la cual es necesario desarrollar un plan para la migración hacia el nuevo protocolo IP con el objetivo de actualizar la red de la institución y estar al día con las nuevas tecnologías de internet.

Paso 2. Evaluación de las condiciones actuales de la institución:

Durante el desarrollo del Capítulo III, se ha realizado un análisis profundo acerca de las condiciones actuales de la red de la universidad, en donde se ha determinado que la UPS Sede-Cuenca cuenta con una red LAN que proporciona servicio a todos los usuarios del campus universitario, la infraestructura actual de la universidad esta diseñada bajo el

[23] ANDES, (2012), 5,5 millones de personas tienen acceso a internet en Ecuador, Obtenida el 13 de Agosto del 2012, de http://andes.info.ec/2009-2011.php/?p=141153

protocolo IPV4, debido a esto se presentan desempeños no deseados que afectan directamente sobre los servicios que se desean ofrecer.

5.2.2 Fase 2: Modelo de Negocios/Organización

Establecer una estrategia de migración es un proceso complicado por lo que primero se debería realizar la configuración del Gateway principal con el fin de permitir a la institución continuar con sus labores diarias, mientras se levanta la nueva infraestructura de red y se realiza los cambios en las aplicaciones para que funcionen con IPV6.

En la actualidad los dispositivos Gateway pueden operar en ambientes mixtos IPV4/IPV6, de esta manera la universidad tiene la facilidad de realizar pruebas, mover y migrar su infraestructura existente a un paso controlado administrado.

De manera general el Gateway se encuentra instalado entre los dispositivos clientes y servidores con el fin de proporcionar diferentes aplicaciones. En este caso los dispositivos pueden proveer funciones de virtualización y alta disponibilidad haciendo que los servidores físicos utilicen direcciones IP privadas como si fuera una entidad virtual con una sola dirección IP virtual. Mediante este método tenemos la oportunidad de migrar los clientes o servidores a redes IPV6 sin la necesidad de cambiar todo en un solo paso.

Stonesoft expone una serie de sugerencias que se deberían tomar en cuenta para establecer el proceso de migración de una forma segura y rentable:

1. La actualización de la red existente: consiste en eliminar las características antiguas de la red y actualizarla hasta que quede como nueva, esta actualización consiste en asegurar cada aspecto de la red que pueda estar efectivamente sin clasificar hasta el siguiente nivel de tal manera que quede activo a lo largo de ese nivel.

2. Planificación de una introducción progresiva: consiste el realizar una planificación a largo plazo para migrar a IPV6, de esta manera se podrá obtener un tiempo suficiente para asegurar el correcto funcionamiento del protocolo con el mecanismo de transición

actual sobre la infraestructura IPV4, además nos permite tener controlado el presupuesto de la institución.

3. Implementación del método Dual- Stack: este método nos permite obtener una serie de beneficios, además requiere las actualizaciones del router para alcanzar una serie de demandas en lo que se refiere a memoria y potencia con el fin de soportar el funcionamiento simultaneo de IPV4/IPV6.

4. Actualización y adopción de un firewall certificado.

5. Mantener IPV6 disponible cuando realmente este siendo usado.

6. Evitar los ataques de usuarios maliciosos que se están infiltrando en el protocolo IPV6

7. Revisión de fragmentos de tráfico de túnel antes de permitir tanto la salida y la entrada del sistema.

8. Autenticación de usuarios mediante el uso de un proxy HTTP/HTTPS con el fin de permitir a los usuarios el acceso a Internet.

9. Manejar la sintaxis IPV6 con el fin de permitir el manejo de comandos para establecer medidas de seguridad o configuración de los equipos.

Fernando Egido, director general de Broca de España, recomienda realizar la migración a IPV6 mediante los siguientes pasos:

> ***1. Prepararse sin agobiarse:***
>
> *La transición a IPV6 no debe ser un proceso alarmante, lo importante es preparase de forma progresiva, analizar el estado de los equipos y evaluar el impacto que tendrá la implantación del nuevo protocolo dentro de la institución.*

2. Revisión de la infraestructura de red:

En este apartado tenemos que revisar que servicios y aplicaciones no están actualizados para funcionar con IPV6, de esta manera se podrá realizar un análisis y una clasificación de los más importantes.

3. Diseñar un cronograma de trabajo:

Debido a que cada día aumenta el número de usuarios de internet, se debe establecer un calendario con todas las actividades necesarias para llevar a cabo el proceso de migración a IPV6 y de esta manera tratar de cumplir y ajustarse a él.

4. No tratar de solucionarlo todo a la vez:

Tratar de identificar las soluciones adecuadas que permitan facilitar la transición sin la necesidad de recurrir a actualizaciones costosas y de alto riesgo que en muchos casos implica una sustitución completa de toda la infraestructura de red.

5. El diseño de la red debe satisfacer las necesidades de la institución a corto, medio y largo plazo:

Este paso consiste en elaborar un plan de migración por etapas con el fin de reducir el impacto en las actividades de la institución y evitar la compra de equipos que no sean compatibles con IPV6.

6. Las soluciones intermedias pueden generar un retorno de la inversión a largo plazo:

La tecnología de transición Dual Stack, permite gestionar los flujos de tráfico IPV6, en cambio las nuevas soluciones permiten ejecutar IPV6 e IPV4 sin ningún impacto notable. [24]

5.2.3 Fase 3: Modelo de Tecnologías de la Información

En el capítulo IV se ha podido realizar un estudio completo para evaluar las características del hardware y software que forman parte de la infraestructura de la red interna de la UPS Sede-Cuenca, con la finalidad de determinar si soporta la versión del nuevo protocolo de red IPV6.

[24] EGIDO, Fernando, (2011), Migrar a IPV6 en seis pasos, Obtenida el 15 de Agosto del 2012, de http://www.idg.es/computerworld/Migrar-a-IPv6-en-seis-pasos/seccion-tecnologia/articulo-203281

En la Figura 20, podemos observar un listado de sistemas operativos, equipos de red que soportan IPV6 y vienen con el protocolo habilitado por defecto.

Fecha	Productos	Soporte para IPv6	IPv6 habilitado
1996	OpenBSD / NetBSD / FreeBSD	Sí	Sí
	Linux Kernel 2.1.6	Sí	No
1997	AIX 4.2	Sí	No
2000	Windows 95/98/ME/NT 3.5/NT 4.0	Sí (paquetes adicionales)	No
	Windows 2000	Sí	No
	Solaris 2.8	Sí	Sí
2001	Cisco IOS (12.x y superior)	Sí	No
2002	Juniper (5.1 y superior)	Sí	La mayoría
	IBM z/OS	Sí	Sí
	Apple OS/10.3	Sí	Sí
	Windows XP	Sí	No
	Linux Kernel 2.4	Sí	No
	AIX 6	Sí	Sí
	IBM AS/400	Sí	Sí
2006	Routers Linksys (Mindspring)	Sí	No
	Teléfonos celulares (varios)	Sí	Sí
	Solaris 2.10	Sí	Sí
	Linux Kernel 2.6	Sí	Sí

Figura 20 CAP V. Desarrollo de sistemas con IPV6 habilitado por defecto

Fuente: Rodrigo dos Santos, Antonio M. Moreiras, Eduardo Ascenço Reis, Ailton Soares da Rocha, (2010), Curso IPV6 Básico.

A continuación se presenta un listado de las aplicaciones de uso común que soportan IPV6 dentro de la red interna de la UPS Sede-Cuenca.

Tabla 42 CAP V. Aplicaciones de uso común con soporte para IPV6

Aplicación	Soporte IPV6
Winamp	Desde la versión 5.34
Mozilla Firefox	Desde la versión 2.0
Mozilla Thunderbird	Desde la versión 2.0.0.4
Internet Explorer	Desde la versión 4.01
Microsoft Outlook	Desde la versión 2003
Windows Mail	Soporta el uso directo de direcciones IPV6
VLC media Player	Desde la versión 0.8.6
Windows Media Player	Desde la versión 9.0

Fuente: El Autor

5.2.4 Fase 4: Modelo de Planeación

5.2.4.1 Aspectos Generales

Para establecer el proceso de migración de la red de la UPS Sede-Cuenca hacia el protocolo IPV6 se plantea dos posibles escenarios:

1. Mover los clientes hacia IPV6 mientras se mantienen los servidores en IPV4.
Este escenario requiere que todos los clientes sean capaces de agregarse a la red vía caminos o túneles IPV6 permitidos.

2. Migrar los servidores a IPV6 y dejar los clientes en un entorno con IPV4.
En algunos casos es más fácil comenzar a migrar los servidores (aplicaciones) en lugar de los clientes, estos se debe a que los servidores a menudo están bajo el control de la institución mientras que los clientes no lo están.

Si la institución decide migrar primero sus servidores, el dispositivo Gateway que se encuentra entre los servidores y los clientes deben agregar una red capaz de soportar

IPV6. De esta manera se tendrá una red IPV4 sobre el lado del cliente del dispositivo y los dos protocolos IPV4/IPV6 sobre los servidores.

Una vez configurada la red IPV6, los servidores podrán moverse sobre la red IPV4, debido a que los clientes en un futuro se cambiarán a IPV6 es importante que la institución asegure que toda su infraestructura y aplicaciones puedan ser capaces de soportar IPV6.

5.2.4.2 Prioridades de Implementación

La institución debe realizar inversiones e implementaciones esenciales para obtener grandes beneficios, a continuación se presenta unos de los temas más importantes para llevar a cabo el proceso de migración de manera correcta:

Seguridad

Es un tema muy importante cuyo objetivo es interconectar redes de investigación académicas, el protocolo IPV4 no presentaba ninguna preocupación respecto al tema de seguridad. En la actualidad el crecimiento de Internet para las instituciones y usuarios exige mayores niveles de seguridad por ejemplo la encriptación de datos, identificación de usuarios de esta manera se hace necesario agregar nuevos mecanismos de seguridad para el manejo del nuevo protocolo.

La implementación de IPV6 requiere tomar en cuenta aspectos de seguridad, que todavía no alcanzan una buena experiencia en su administración. A pesar que IPV6 tiene mas de 10 años, las mejores prácticas continúan siendo tomadas de IPV4 por lo que en algunos casos no siempre funcionan de manera correcta.

El protocolo IPV6 se desarrolló pensando en la seguridad de la red por lo que permite implementar las siguientes herramientas de seguridad:

- *IPSec.*
- *Secure Neighbor Discovery (SEND).*
- *Estructura de las direcciones.*
- *Cryptographically Generated Address (CGA).*
- *Extensiones de privacidad.*
- *Unique Local Addresses (ULA).*

Para establecer estas herramientas de seguridad es necesario:

- Obtener equipos certificados.
- Educación y capacitación del personal.
- Actualizar las herramientas y procesos de seguridad.
- Buscar auditores y equipos de prueba que conozcan IPV6.
- Desarrollar prácticas de programación adecuadas para IPV6.
- Preocuparse por la seguridad y considerar la seguridad de los equipos desde el inicio.

Implementación del protocolo IPSec:

El protocolo IPSec se puede utilizar de dos formas diferentes:

1. Modo transparente: se mantiene el encabezado del paquete IP original, para que la comunicación sea segura se requiere un soporte IPSec en los dos extremos, además permite proteger solo los protocolos de las capas superiores debido a que el encabezado de seguridad aparece de forma inmediata después del encabezado IP y antes de los encabezados de los protocolos de las capas superiores.

2. Modo túnel: en este modo se codifica y se crea un nuevo encabezado que hace posible la comunicación entre el dispositivo emisor y el dispositivo receptor (del túnel). Este modo se implementa en dispositivos propios (por ejemplo, concentradores VPN) de esta manera la comunicación IPSec se realiza encapsulando todos los paquetes IP de los

respectivos extremos. Además este método protege todo el paquete IP, encapsulándolo dentro de otro paquete IP y dejando visible solo el encabezado IP externo.

5.2.4.3 Plan de Implementación

La adopción del protocolo IPV6 genera una serie de preguntas que se describen a continuación:

- ¿IPv6 es realmente necesario?
- ¿Cuándo será necesario tener IPv6?
- ¿Cuál es el costo de implementación?
- ¿Cómo planificar para esta transición?
- ¿Hay alternativas viables al uso de IPv6?
- ¿Cómo aprovechar las nuevas funcionalidades de IPv6?
- ¿La transición se debe realizar de forma inmediata o gradualmente?
- ¿Cómo hacer para que las aplicaciones y servicios sean compatibles con el nuevo protocolo?

Dentro del Plan de Implementación se debe establecer un cronograma con la finalidad de describir con mayor detalle cada uno de los pasos presentados en el Plan de Implementación de acuerdo a un orden cronológico en base a las prioridades.

El cronograma del Plan de Implementación permite establecer una relación entre las actividades y el tiempo de duración de cada una de ellas, para ello se utiliza el software Microsoft Project 2010.

El software Microsoft Project 2010 permite organizar, almacenar y visualizar de mejor manera toda la planificación de un proyecto. En el Anexo 5 podemos observar con mayor detalle el cronograma del Plan de Implementación para la migración hacia IPV6 en la red de la UPS Sede-Cuenca.

A continuación se expone los puntos más importantes dentro del cronograma del Plan de Implementación:

1. Capacitación del personal técnico

Debido a que el protocolo IPV6 es un tema nuevo es necesario que tanto los técnicos como los administradores de red busquen adquirir conocimientos sobre esta nueva tecnología mediante cursos, libros, sitios web, documentos técnicos, eventos, etc.

2. Adopción de una dirección IPV6

En la Sección 4.5.4 se ha establecido una dirección IPV6 base, el cual deberá ser otorgado por el ISP con la finalidad de establecer la configuración de toda la red de la UPS Sede-Cuenca.

3. Plan de asignación de direcciones IPV6

En este paso tenemos que identificar los nodos principales y dispositivos que forman parte de la red de la UPS Sede-Cuenca, con el fin de establecer una dirección IPV6 para cada nodo.

A continuación se describen los nodos principales de la red que se esta analizando:

- Router
- Firewall
- Switch Principal
- Switch Servidores
- Switch Biblioteca
- Switch Edificio Rectorado
- Switch Edificio Guillermo Mensi
- Switch Edificio Mario Rizzini

- Switch Edificio Cornelio Merchán
- Switch Laboratorios
- Switch Edificio Sistemas
- Switch Tecniclub
- Switch PACES
- Switch Teatro

4. Obtener herramientas para el manejo y monitoreo de la red.

Hace mucho tiempo atrás no se disponía de las herramientas necesarias para el manejo y monitoreo de la red por lo que era necesario contratar una empresa especializada para llevar a cabo estas acciones con unos costos muy elevados.

La mayoría de los programas para el manejo y monitoreo de la s redes se basan en el protocolo SNMP, el cual utiliza estaciones de administración que permiten monitorear y manejar dispositivos que contienen un agente SNMP y se encuentran conectador a una red IP.

En la actualidad existen diferentes aplicaciones de software libre muy interesantes para monitorear redes y servidores en IPV6:

- *Zenoss*
- *Munin*
- *Zabbix*
- *Cacti*
- *Nagios*

5. Actualización de los nodos para que funcionen con IPV4/IPV6.

En este paso tenemos que llevar a cabo el proceso de actualización del IOS en cada uno de los equipos CISCO (routers, firewalls, switches, access point, teléfonos IP, etc.) con el fin de que puedan soportar el protocolo IPV6.

6. Seleccionar un protocolo de enrutamiento adecuado para IPV6 y establecer políticas de enrutamiento.

El protocolo de enrutamiento se debe seleccionar de acuerdo a las necesidades de la red, de acuerdo al estudio realizado en la Sección 4.3 se ha seleccionado el protocolo OSPF y se ha establecido el enrutamiento de rutas estáticas.

7. Implementación de un mecanismo de transición.

En la Sección 4.1 se ha realizado un estudio acerca del mecanismo de transición Dual Stack el cual deberá ser implementado en el router principal de la red de la UPS Sede-Cuenca.

8. Habilitar los servicios IPV6 necesarios (DNS, QoS, etc.).

Se debe establecer la configuración de todos los servicios de la red interna con la finalidad de que permitan el soporte para el protocolo IPV6, la mayoría de estos servicios se encuentran instalados en los servidores descritos en la Tabla 22 CAP III.

9. Habilitar IPV6 en los equipos del usuario.

Para evitar inconvenientes y reducir el tiempo en configurar direcciones IPV6 fijas se puede utilizar la asignación de direcciones IPV6 mediante DHCPv6 para esto se deberá realizar lo siguiente:

1. Habilitar la configuración de DHCPv6 en el router principal.
2. Establecer un cronograma para habilitar DHCPv6 por departamentos.
3. Habilitar DHCPv6 en cada una de las máquinas de los usuarios de acuerdo al cronograma establecido para cada departamento de la universidad.

10. Capacitación de los usuarios de la red.

Una vez configurada la red sobre IPV6, los técnicos y administradores de la red deberán establecer cronogramas para dictar cursos de capacitación a todos los usuarios de la red incluyendo a los estudiantes y profesores.
Los cursos deberán ser dictados en diferentes fechas de acuerdo a las necesidades de cada departamento o área funcional de la institución.

Ejemplo:

Semana 1. Curso de capacitación para el área de Sistemas
Semana 2. Curso de capacitación para el área Administrativa.
Semana 3. Curso de capacitación para el área de RRHH.
Semana 4. Curso de capacitación para el área Financiera.

5.2.4.4 Impacto en la Implementación de IPV6

El protocolo IPV4 e IPV6 son protocolos que actúan sobre la capa de red y esta es la única que se ve afectada por la implementación de IPV6 sin necesidad de modificar el resto de capas.

A continuación se describe una serie de consideraciones para reducir el impacto en la implementación de IPV6:

- Minimizar los costos de implementación.
- La adopción de IPV6 debe realizarse de manera gradual.
- Los equipos deben soportar las funcionalidades de los dos protocolos.
- Debe existir un período de coexistencia entre los protocolos IPV4 e IPV6.
- En las redes con Dual Stack las configuraciones deben ser duplicadas por ejemplo el DNS, Firewall y los protocolos de enrutamiento.

Es muy importante que la red de la universidad este preparada para utilizar el nuevo protocolo, mientras mas pronto se llegue a entender el tema y se realice una planificación adecuada, menor serán los gastos del proceso.

5.2.4.5 Costos de implementación

Dentro del proceso de transición uno de los temas fundamentales son los costos de implementación debido a que en la inversión que se realiza se requiere la obtención de bienes y servicios que van a formar parte de la infraestructura actual o de una nueva.

> *Según Gartnet estima que el costo de convertir el entorno de una empresa de TI de IPV4 a IPV6 ronda el 6% del presupuesto anual total del departamento de TI de la empresa. Los costos fijos luego de realizada la conversión ascenderán aproximadamente el 1% del presupuesto de TI en los años siguientes, en comparación a los costos incurridos por la empresa si se hubiera mantenido la versión IPV4.*
>
> *El costo de establecer una presencia IPv6 en internet es más económico, alrededor de unos USD 500.000 para una puerta de enlace a internet típica, con costos fijos de aproximadamente un 10% de este monto.*[25]

Por otro lado nuestro análisis consiste en evaluar los siguientes elementos:

- *Software*
- *Hardware*
- *RRHH*
- *Capacitación*

5.2.4.5.1 Costos de Software:

A continuación se presenta un detalle de las especificaciones y costos aproximados de los principales Sistemas Operativos y Aplicaciones instalados tanto en los servidores como en las máquinas de los usuarios.

[25] VERISIGN, (2011-2012), Lanzamiento mundial de IPV6, Obtenida el 20 de Agosto del 2012, de http://www.verisigninc.com/es_LA/why-verisign/innovation-initiatives/ipv6/index.xhtml

Tabla 43 CAP V. Análisis de los costos del Software

Software	Observaciones	Costo
CentOS 6.2	Este S.O de Software Libre soporta IPV6 y se encuentra instalado en los servidores, lo único que se debe realizar es descargar las actualizaciones buscando en Internet y almacenarlos en medios magnéticos como CD'S o DVD.	$20,00
Unix	Este grupo de S.O de Software Libre soporta IPV6 y se encuentra instalado en el servidor de B.D, lo único que se debe realizar es descargar las actualizaciones buscando en Internet y almacenarlos en medios magnéticos como CD'S o DVD.	$20,00
Windows 7	Este S.O de Microsoft soporta IPV6 y se encuentra instalado en las máquinas de los usuarios de la red, lo único que se debe hacer es activar el protocolo IPV6. La activación no tiene costo.	$0,00
Windows XP	Este S.O de Microsoft soporta IPV6 y se encuentra instalado en las máquinas antiguas de la institución, lo único que se debe hacer es activar el protocolo IPV6 y en caso de ser necesario descargar las actualizaciones buscando en internet.	$10,00
Squid	Es una aplicación de Software Libre que implementa un servidor proxy, lo único que se debe hacer es activar el soporte para IPV6 buscando información en Internet.	$10,00
Zimbra	Aplicación de correo electrónico que se encuentra instalado sobre un servidor, lo único que tenemos que hacer es configurar el soporte para IPV6, buscando información en el Internet	$10,00
Liferay	Lo único que se necesita es configurar el soporte para IPV6 buscando información en el Internet.	$10,00
Oracle	Lo único que se necesita es configurar el soporte para IPV6 buscando información en el Internet.	$10,00
Oracle Forms	Lo único que se necesita es configurar el soporte para IPV6 buscando información en el Internet.	$10,00
Total:		$100,00

Fuente: El Autor

5.2.4.5.2 Costos de Hardware:

En la Tabla 39 del Capítulo IV se ha determinado que los equipos de red de la UPS Sede-Cuenca soportan IPV6 por lo tanto no es necesario realizar la compra de nuevos equipos, lo único que se necesita es realizar la configuración y actualización del IOS para cada equipo.

5.2.4.5.3 Costos de RRHH:

Uno de los puntos importantes para establecer la migración hacia el protocolo IPV6 es los costos del personal cuya mano de obra no será incluida para la implementación física y lógica del protocolo IPV6, debido a que la UPS Sede Cuenca cuenta con el personal calificado en el área de redes para realizar estas actividades bajo la dirección del jefe del área de sistemas para presentar calidad en los procesos de implementación.

5.2.4.5.4 Costos de Capacitación:

Otro de los aspectos importantes para llevar a cabo el proceso de migración hacia IPV6 en la red de la UPS Sede-Cuenca son las pruebas de funcionamiento y la capacitación del personal técnico y usuarios.

Tabla 44 CAP V. Análisis de los costos de Capacitación

Descripción	Unidad	Cantidad	Costo por unidad	Valor
Pruebas de funcionamiento	horas	200	$20,00	$ 4000
Capacitación personal técnico para el manejo de IPV6.	horas	40	$50,00	$ 2000
Capacitación de los usuarios para el manejo de IPV6.	horas	80	$20,00	$ 1600
Total:				$ 7600

Fuente: El Autor

Inversión Final

Es muy importante considerar un porcentaje adicional del 20% para los gastos de imprevistos debido a que en algunos casos puede ser necesario la contratación de un técnico externo para el asesoramiento en algunas configuraciones y procesos complejos, además se debe tomar en cuenta que los costos de software y capacitación son valores aproximados y en cualquier momento puede ser necesario una modificación al momento de realizar el proceso de transición hacia IVP6.

Costos de Software	$	100,00
Costos de Hardware	$	0,00
Costos de RRHH	$	0,00
Costos de Capacitación	$	7600,00
Imprevistos (20%)	$	1540,00
Total:	$	9240,00

5.2.4.6 Formas de pago y financiación

Es muy importante establecer una inversión al contado a medida que se va realizando la implementación de las diferentes partes del proyecto. De esta forma se podrá ahorrar en los intereses que pueden ocasionar los diferentes tipos de financiación disponibles en el mercado.

Una inversión al contado requiere desembolsar una gran cantidad de dinero, pero de esta manera la institución controla de una mejor manera el flujo de caja por lo que no cuenta con la posibilidad de realizar créditos.

5.2.4.7 Riesgos del proyecto

Durante el desarrollo del proyecto es posible que exista una serie de factores que ponen en riesgo el proceso de migración hacia el protocolo IPV6, a continuación se presenta una tabla con los riesgos más importantes:

Tabla 45 CAP V. Riesgos del Proyecto

N°	Descripción
1	Pérdida de información.
2	Daños físicos en los equipos.
3	No disponibilidad de repuestos.
4	Incompatibilidad de hardware.
5	Inestabilidad de las aplicaciones.
6	Problemas de funcionamiento del S.O.
7	Falta de pago en los servicios de Internet.
8	Cortes de luz inesperados no superados.
9	Incompatibilidad de aplicaciones con el S.O.
10	Falta de compromiso por parte del personal técnico.
11	Fallas de instalación y conexión de los equipos de red.
12	Falta de tiempo de adaptación al nuevo protocolo IPV6.
13	Falta de capacitación al personal técnico de la UPS Sede-Cuenca.

Fuente: El Autor

5.2.4.8 Plan de contingencia

El plan de contingencia permite prevenir los riesgos con la finalidad de garantizar el perfecto funcionamiento de un proyecto, asegurando un servicio continuo con una calidad adecuada.

A continuación se presenta una tabla con las acciones que se deben realizar para prevenir los riesgos descritos en la Tabla 45 CAP V.

Tabla 46 CAP V. Plan de Contingencia

N°	Acciones
1	Respaldo de toda la información en dispositivos de almacenamiento extraíbles como discos duros, pendrive, cd's, etc.
2	Revisión de manuales para el uso de los equipos.
3	Mantenimiento y revisión continúa de los equipos.
4	Utilizar la documentación para el manejo de los equipos.
5	Revisar las configuraciones y establecer pruebas de funcionamiento.
6	Descargar todas las actualizaciones y complementos para el manejo del Sistema Operativo.
7	Elaborar un plan de presupuestos para el manejo y pago de los servicios principales dentro del área de Sistemas.
8	Revisión continua y mantenimiento del generador eléctrico.
9	Revisión y configuración del código de las aplicaciones.
10	Establecer un cronograma de trabajo para distribuir las actividades a cada miembro del personal técnico.
11	Revisiones periódicas de las conexiones y mantenimiento de los equipos de red.
12	Establecer un cronograma en el cual se debe dedicar por un largo período a la capacitación del personal técnico.
13	Tomar evaluaciones al personal técnico con el fin de determinar los conceptos que no están claros y dedicar un tiempo extra para reforzar los conocimientos.

Fuente: El Autor

5.2.4.9 Riesgos de no implementar IPV6

El uso de IPV6 en las empresas aumenta de forma progresiva, por lo tanto la no implementación de IPV6 puede producir lo siguiente:

1. Aumentar el uso técnicas como NAT.
2. Impedir el surgimiento de nuevas redes.
3. Dificultar el surgimiento de nuevas aplicaciones.
4. Reducir el proceso de inclusión digital reduciendo el número de nuevos usuarios.
5. El costo de no implementar IPv6 puede ser mayor que el costo de implementarlo.

En la actualidad el uso de IPV6 no es muy representativo, pero su adopción en las redes va en aumento, por este motivo es imposible postergar la implementación de IPV6 ya que puede generar diferentes desventajas para el desarrollo de Internet.

Todos los días tenemos nuevas redes gracias a la expansión de las empresas y al surgimiento de nuevos negocios, el crecimiento de las redes 3G y el uso del Internet en dispositivos electrónicos son ejemplos de aplicaciones que contribuyen al crecimiento de la red.

Un aspecto muy importante que vale la pena mencionar es la vulnerabilidad que ha tenido el protocolo IPV6 a lo largo de estos años, según la Figura 21 CAP V. podemos observar que a medida que aumenta el uso de IPV6, aumenta curva de vulnerabilidad.

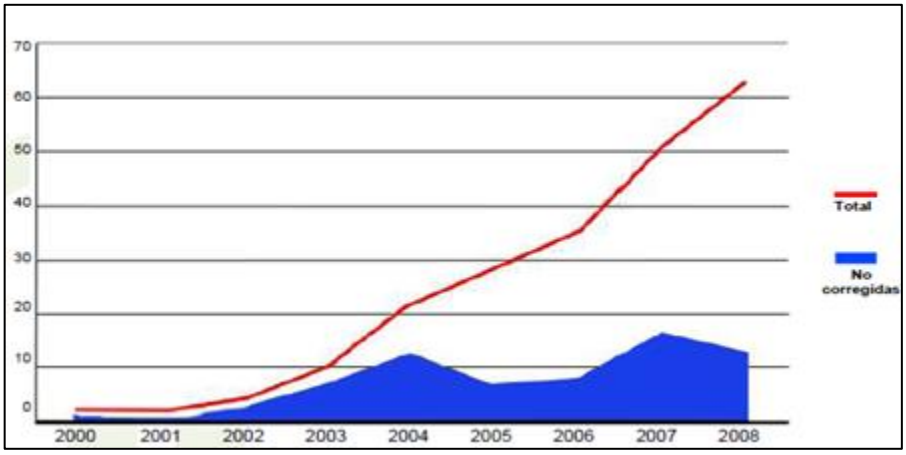


Figura 21 CAP V. Vulnerabilidad de IPV6 a lo largo del tiempo

Fuente: Rodrigo dos Santos, Antonio M. Moreiras, Eduardo Ascenço Reis, Ailton Soares da Rocha, Curso (2010), IPV6 Básico.

CONCLUSIONES

- Durante el desarrollo de este proyecto de tesis se ha logrado analizar, diseñar y realizar un plan de implementación para la migración a IPV6 tomando como información referencial la red de la UPS Sede-Cuenca, de esta manera se ha logrado realizar la simulación de toda la red de la universidad mediante el software Packet Tracer, para esto se ha utilizado el mecanismo de traducción Dual Stack, el cual permite conectar las distintas unidades administrativas, los departamentos y laboratorios al internet mediante el protocolo IPV6, sin la necesidad de utilizar mecanismos de transición complejos.

- El proceso de migración hacia IPV6 si es posible dentro de la red de la UPS Sede-Cuenca, debido a que se ha logrado analizar las características de los equipos de red llegando a determinar que todos poseen soporte para IPV6, lo único que se debe realizar son las configuraciones y actualización del software.

- El espacio de direccionamiento en IPV6 tiene mayor capacidad debido a que aumentó de 32 a 128 bits, de esta manera se puede obtener niveles más específicos de agregación de direcciones, identificar una mayor cantidad de dispositivos en la red, implementar mecanismos de autoconfiguración, etc.

- La cabecera de IPV6 tiene un nuevo formato debido a que se eliminaron algunos campos del encabezado IPV4 con la finalidad de reducir el costo de procesamiento de los paquetes en los routers.

- El diseño de red base de la UPS Sede-Cuenca cuenta con varias VLANS el cual nos permite crear grupos de trabajo diferentes, de esta manera se trata de mejorar la seguridad y administración entre los diferentes grupos estableciendo reglas de conectividad.

- La migración hacia IPV6 se debe realizar de manera gradual, por este motivo es necesario establecer un periodo de transición y coexistencia entre los dos protocolos con el fin de reducir el impacto sobre el funcionamiento de la red.

- El protocolo IPV6 especifica encabezados de extensión capaces de suministrar mecanismos de autenticación y garantizar la integridad y confidencialidad de los datos dentro de una red.

- El protocolo DHCPv6 utiliza el protocolo UDP para el intercambio de mensajes, además permite suministrar direcciones IPV6 y diferentes parámetros en la red por ejemplo: direcciones de servidores DNS, NTP, SIP, etc.

- El protocolo IPV6 fue diseñado con la finalidad de proporcionar aspectos relevantes como la escalabilidad en la red, seguridad, configuración y administración de redes, Soporte para QoS, movilidad, políticas de enrutamiento, etc.

- El primer escenario descrito en este proyecto nos permite visualizar la solución para lograr que la red de la UPS Sede-Cuenca pueda manejar el protocolo IPV4/IPV6 mediante el mecanismo de transición Dual Stack, de esta manera se permite la coexistencia entre los dos protocolos.

- Mediante el desarrollo del plan de implementación se ha determinado que uno de los aspectos más importantes dentro de la red de la UPS Sede-Cuenca es la implementación de niveles de seguridad, además se ha logrado establecer una serie de pasos para poder llevar a cabo el proceso de migración, de la misma manera se ha realizado un análisis completo sobre los costos de implementación, riesgos del proyecto y planes de contingencia.

- El método Dual Stack requiere habilitar el protocolo OSPFv2 para realizar el enrutamiento IPV4 y OSPFv3 para el enrutamiento en IPV6.

- La implementación del protocolo IPV6 en la red de la UPS Sede-Cuenca es un tema de gran relevancia para el futuro de la institución. Debido a que la Universidad de Cuenca ya cuenta con una red funcionando sobre IPV6 es necesario que nuestra institución comience a trabajar en el desarrollo de este proyecto con la finalidad de estar al día con la tecnología actual.

- Para la implementación del mecanismo de transición Dual Stack es necesario habilitar el servicio DNS con la finalidad de resolver nombre y direcciones para los dos protocolos, en el caso de IPV6 es necesario responder a consultas de registros tipo AAAA (Quad - A).

- Para obtener mayor seguridad entre los diferentes departamentos que tiene la red de la UPS Sede-Cuenca se ha creado un total de 34 VLANS sobre la red IPV6.

- Durante los próximos años IPV6 tomará mayor relevancia en Internet, de esta manera este proyecto permite a la red de la UPS Sede-Cuenca estar preparada para las futuras necesidades de los usuarios sobre redes IPV6.

RECOMENDACIONES

- En la fase inicial de implementación no se recomienda configurar todos los nodos con soporte para IPV6, debido a que muchos servicios y dispositivos de red continúan trabajando sobre IPV4, por este motivo es necesario implementar el método de transición Dual Stack.

- En la Figura 21. Se ha podido observar que a medida que pasa el tiempo existen problemas y vulnerabilidades importantes en las redes IPV6. Los ataques que se presentan hacen necesario tomar las debidas precauciones cuando se implementan redes IPV6 a gran escala.

- La parte teórica del protocolo IPV6 requiere una gran cantidad de conocimientos, por este motivo el personal técnico de la UPS Sede-Cuenca deberá tomarse el tiempo necesario para capacitarse y hacer un estudio completo de esta manera se puede tener un alto nivel de comprensión al momento de desarrollar las soluciones para IPV6.

- Con el fin de obtener los mejores resultados antes del proceso de migración se debe diseñar un plan de implementación en donde se considere varios aspectos relevantes como el tamaño de la red, diseño de la topología de red, distribución de las direcciones IP, metodóloga de implementación, protocolos de enrutamiento, etc.

- Se debe tomar en cuenta que en este proyecto no se considera el análisis de los dispositivos inalámbricos, debido a esto se recomienda revisar el soporte IPV6 en los equipos de red WIFI existentes y evaluar las alternativas para otorgar direcciones IPV6 de forma conjunta con las direcciones IPV4. Debido al gran número de estudiantes que utilizan la red WIFI dentro de la universidad es necesario realizar investigaciones para aplicar conceptos de seguridad dentro de una red inalámbrica.

GLOSARIO

6VPE: IPv6 VPN provider edge (6VPE) over MPLS.

A

AAAA: *Address*, registro que se utiliza en IPv6 para traducir nombres de hosts a direcciones IPv6.

AES 128: *Advanced Encryption Standard*, esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos.

ANSI: *American National Standards Institute* (Instituto Nacional Estadounidense de Estándares) es una organización sin fines de lucro que supervisa el desarrollo de estándares para productos, servicios, procesos y sistemas en los Estados Unidos

ARP: *Address Resolution Protocol*, (Protocolo de Resolución de Direcciones) es un protocolo de la capa de enlace de datos responsable de encontrar la dirección MAC que corresponde a una determinada dirección IP.

B

Backbone: es una parte de la infraestructura de red informática que interconecta varios pedazos de red, proporcionando un camino para el intercambio de información entre las diferentes redes de área local o subredes.

BGP-4: *Border Gateway Protocol*, (Protocolo de Gateway Fronterizo) es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos.

Bit: *Binary digit*, (Dígito Binario) es un dígito del sistema de numeración binario.

Broadcast: transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea.

C

CDP: *Cisco Discovery Protocol*, (Protocolo de descubrimiento de Cisco) es un protocolo de red propietario de nivel 2, desarrollado por Cisco Systems y usado en la mayoría de sus equipos.

CE: *Conformité Européenne*, (Conformidad Europea) esta marca indica la conformidad con las directivas de la Comunidad Europea.

CISCO IOS: *Internetwork Operating System*, es el software utilizado en la gran mayoría de routers y switches de Cisco Systems.

CISPR 22, 24: *Comité International Spécial des Perturbations Radioélectriques*, (Comité Internacional Especial de Perturbaciones Radioeléctricas) es una organización de normalización en el campo de las interferencias electromagnéticas para dispositivos eléctricos y electrónicos.

CNG: *Comfort Noise Generation*, Generación de ruido confortable.

CoS: *Class Of Service*, (Clase de servicio) es un esquema de clasificación que agrupa los tráficos que tienen requerimientos similares con el fin de diferenciar los tipos de tráficos y poder priorizarlos.

D

DHCP: *Dynamic Host Configuration Protocol*, (Protocolo de Configuración Dinámica de Host) es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente.

DNS: *Domain Name System*, (Sistema de Nombres de Dominio) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada.

DRAM: *Dynamic Random Access Memory*, es un tipo de memoria dinámica de acceso aleatorio que se usa principalmente en los módulos de memoria RAM y en otros dispositivos, como memoria principal del sistema.

E

EGP: *Exterior Gateway Protocol*, (Protocolo de Gateway Exterior) es un protocolo estándar usado para intercambiar información de enrutamiento entre sistemas autónomos.

F

Firewall: (ó Cortafuegos), es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

FTP: *File Transfer Protocol*, (Protocolo de Transferencia de Archivos) es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP, basado en la arquitectura cliente-servidor.

G

GbE: *Gigabit Ethernet*, es un término que describe diversas tecnologías para la transmisión de tramas Ethernet a una velocidad de un Gigabit por Segundo (1.000.000.000 bits por segundo).

H

HTML: *HyperText Markup Language*, (Lenguaje de Marcado de Hipertexto), hace referencia al lenguaje de marcado predominante para la elaboración de páginas web que se utiliza para describir y traducir la estructura y la información en forma de texto.

HSRP: *Hot Standby Router Protocol*, es un protocolo propiedad de CISCO que permite el despliegue de routers redundantes tolerantes a fallos en una red.

HTTP: *Hypertext Transfer Protocol*, (Protocolo de Transferencia de Hipertexto) es el protocolo usado en cada transacción de la World Wide Web.

I

IANA: *Internet Assigned Numbers Authority*, es la entidad que supervisa la asignación global de direcciones IP.

ICEA: *Insulated Cable Engineers Association*, organización dedicada a las normas de cable en desarrollo para la energía eléctrica, control, y las industrias de telecomunicaciones.

ICMPv6: *Internet Control Message Protocol for IPv6*, (Protocolo de Mensajes de Control de Internet para IPV6) este protocolo es una nueva versión de ICMP y es una parte importante de la arquitectura IPv6 que debe estar completamente soportada por todas las implementaciones y nodos IPv6.

IDF: Centro Intermedio de Distribución del Cableado.

IEC: *International Electrotechnical Commission*, (Comisión Electrotécnica Internacional) es una organización de normalización en los campos eléctrico, electrónico y tecnologías relacionadas.

IEEE 802.1Q: *Institute of Electrical and Electronics Engineers*, el protocolo IEEE 802.1Q es un proyecto del grupo de trabajo 802 de la IEEE, cuyo objetivo es desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas.

IETF: *Internet Engineering Task Force*, (Grupo Especial sobre Ingeniería de Internet) es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad, etc.

IGP: *Interior Gateway Protocol*, (Protocolo de Gateway Interno) hace referencia a los protocolos usados dentro de un sistema autónomo.

IPsec: *Internet Protocol Security,* es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet, autenticando o cifrando cada paquete IP en un flujo de datos.

ISATAP: *Intra-Site Automatic Tunnel Addressing Protocol,* es un mecanismo de transición de IPv6, para transmitir paquetes de IPv6 entre nodos con doble pila (Dual-Stack) sobre redes IPv4.

ISO: (Organización Internacional de Normalización), es un organismo encargado de promover el desarrollo de normas internacionales de fabricación (tanto de productos como de servicios), comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica.

ISP: *Internet Service Provider*, (Proveedor de servicios de Internet), es una empresa que brinda conexión a Internet a sus clientes.

J

JVM: *Java Virtual Machine,* (Máquina Virtual Java) es una máquina virtual de proceso nativo, que se ejecuta sobre una plataforma específica, capaz de interpretar y ejecutar instrucciones expresadas en un código binario especial, generado por el compilador del lenguaje Java.

L

LAN: *Local Área Network,* (Red de área local) es la interconexión de una o varias computadoras y periféricos.

Liferay: es un portal de gestión de contenidos de código abierto escrito en Java.

M

MDF: Centro de Distribución Principal del Cableado.

MLD: *Multicast Listener Discovery,* (Descubrimiento de escucha de multidifusión) es un componente del Protocolo de Internet versión 6 (IPv6) utilizado por los routers IPv6 para el descubrimiento de multidifusión en un enlace de conexión directa.

MRU: *Maximum Receive Unit,* (Unidad Máxima de Recepción), es la unidad que indica el tamaño máximo (en octetos) del campo de datos de una trama (en el nivel de enlace) que un determinado host es capaz de recibir en una red.

MTU: *Máximum Transfer Unit,* (Unidad Máxima de Transferencia) es un término de redes de computadoras que expresa el tamaño en bytes de la unidad de datos más grande que puede enviarse usando un protocolo de comunicaciones.

Multicast: (Multidifusión), es el envío de la información en una red a múltiples destinos simultáneamente.

N

ND: *Neighbor Discovery,* (Descubrimiento de Vecinos) es un conjunto de mensajes y procesos que determinan las relaciones entre nodos vecinos.

NEMA: *National Electrical Manufacturers Association,* (Asociación Nacional de Fabricantes Eléctricos) es una asociación industrial estadounidense, responsable de numerosos estándares industriales comunes usados en el campo de la electricidad.

Nibble: conjunto de cuatro dígitos binarios (bits).

NNTP: *Network News Transport Protocol*, (Protocolo para la Transferencia de Noticias en Red) es un protocolo inicialmente creado para la lectura y publicación de artículos de noticias en red.

O

OSPF v3: *Open Shortest Path First*, es un protocolo de enrutamiento creado para soportar direccionamiento IPV6.

P

PDA: *Personal Digital Assistant*, (Asistente Digital Personal) es un organizador de bolsillo o una computadora de mano originalmente diseñada como agenda electrónica (calendario, lista de contactos, bloc de notas y recordatorios) con un sistema de reconocimiento de escritura.

POP: *Post Office Protocol*, (Protocolo de la Oficina de Correo) es un protocolo utilizado por clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto.

PRT: funciona a la inversa del registro A, traduciendo IP's en nombres de dominio.

PVC: *Poly Vinyl Chloride,* (Poli Cloruro de Vinilo) es un polímero termoplástico que se presenta como un material blanco que comienza a reblandecer alrededor de los 80 °C y se descompone sobre los 140 °C.

Q

QoS: *Quality of Service*, (Calidad de Servicio) son las tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado.

R

Rack: permiten organizar los equipos informáticos y de redes, consiste en un armazón metálico que cuenta con guías horizontales donde se pueden apoyar los equipos.

RAM: *Random Access Memory,* (Memoria de Acceso Aleatorio) se utiliza como memoria de trabajo para el sistema operativo, los programas y la mayoría del software.

RIP: *Routing Information Protocol*, (Protocolo de Información de Enrutamiento) es un protocolo de puerta de enlace interna o IGP, utilizado por los routers para intercambiar información acerca de redes IP.

RIPng: *Routing Information Protocol Next Generation*, (Protocolo de Información de Enrutamiento de la siguiente generación) se refiere al protocolo RIP de la siguiente generación que tiene soporte para IPv6.

RMON: *Remote Network Monitoring,* desarrollado por la IETF para apoyar el monitoreo y análisis de protocolos de redes LAN.

S

SCCP: *Skinny Client Control Protocol,* es un protocolo propietario de control de terminal desarrollado originariamente por Selsius Corporation.

SIP: *Session Initiation Protocol,* (Protocolo de Inicio de Sesiones) es un protocolo desarrollado con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia.

SMTP: *Simple Mail Transfer Protocol,* (Protocolo Simple de Transferencia de Correo) es un protocolo de la capa de aplicación basado en textos utilizados para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA's, teléfonos móviles, etc.).

SNMP 3: *Simple Network Management Protocol,* (Protocolo Simple de Administración de Red) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.

SNMP Traps: *Simple Network Management Protocol Traps,* (Protocolo Simple de Administración de Red por Trampas) permite a un agente notificar a la estación de gestión de eventos significativos por medio de un mensaje de SNMP no solicitado.

SOA: *Service Oriented Architecture,* (Arquitectura Orientada a Servicios de Cliente) es un concepto de arquitectura de software que define la utilización de servicios para dar soporte a los requisitos del negocio.

SQL Server: es un sistema para la gestión de bases de datos producido por Microsoft basado en el modelo relacional.

SQUID: es un popular programa de software libre que implementa un servidor Proxy y un dominio para caché de páginas web, publicado bajo licencia GPL.

T

TCP/IP: (Protocolo de control de transmisión/Protocolo de Internet), es un conjunto de protocolos de red en los que se basa Internet y que permiten la transmisión de datos entre computadoras.

TFTP: *Trivial File Transfer Protocol*, (Protocolo de Transferencia de Archivos Trivial) es un protocolo de transferencia muy simple semejante a una versión básica de FTP que se utiliza para transferir pequeños archivos entre ordenadores dentro de una red.

TIA/EIA-568-B: tres estándares que tratan el cableado comercial para productos y servicios de telecomunicaciones.

U

UDP: *User Datagram Protocol*, es un protocolo del nivel de transporte basado en el intercambio de datagramas.

UL: *Underwrites Laboratories*, es una importante compañía global de las ciencias de seguridad que certifica, valida, prueba, inspecciona, asesora y capacita para una gama de diversos actores incluyendo fabricantes, diseñadores de políticas, reguladores, empresas de servicios, consumidores y profesionales del entorno.

Unicast: es el envío de información desde un único emisor a un único receptor.

UTP CAT 6: *Unshielded Twisted Pair Cat 6,* (Par Trenzado no Blindado Categoria 6) es un tipo de cable de par trenzado que no se encuentra blindado y que se utiliza

principalmente para comunicaciones, la categoría 6 posee características y especificaciones para la diafonía y ruido.

V

VAD: *Voice Activity Detection,* (Detección de Actividad de Voz) es una técnica utilizada en el procesamiento de voz en el que se detecta la presencia o ausencia del habla humana.

VCCI: *Voluntary Control Council for Interference by Information Technology Equipment,* (Consejo de Control Voluntario de Interferencias) es el organismo regulador de las emisiones electromagnéticas.

VLAN: (Red de Área Local Virtual) es un método de crear redes lógicamente independientes dentro de una misma red física.

VLSM: *Variable Length Subnet Mask,* (Máscaras de Subred de Tamaño Variable) permite evitar el agotamiento de direcciones IP, la división en subredes, el enrutamiento de Inter dominio CIDR, NAT y las direcciones IP privadas.

VoIP: *Voice over IP,* (Voz sobre el Protocolo de Internet) es un grupo de recursos que hacen posible que la señal de voz viaje a través del Internet mediante el protocolo IP.

VTP: *VLAN Trunking Protocol*, es un protocolo de mensajes de nivel 2 usado para configurar y administrar VLAN's en equipos Cisco.

W

WAN: *Wide Área Network,* (Red de Área Amplia) es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km, proporcionando servicio a un país o un continente.

REFERENCIAS

Tesis:

BARRERA, Jessica y GUERRA, Edgar, *Implementación de Tunneling entre redes IPV4 e IPV6 para la empresa "Netxperts Consulting S.A*", Escuela Politécnica del Ejército, Sangolqui, Junio 2005.

CARRERA, Miguel, *Análisis de las Técnicas de convivencia entre IPV4 e IPV6 y su implementación en los servicios: Web, Mail, FTP, Proxy, DNS y DHCP de la Intranet de la ESPOCH,* Escuela Superior Politécnica del Chimborazo, s/f.

DUQUE, Silvia y VALLEJO, Davis, *Mecanismos de transición de IPV4 a IPV6*, Universidad Técnica del Norte, s/f.

JARA, Felipe, Estudio e Implementación de una red IPV6 en la UTFSM, Universidad Técnica Federico Santa María, Valparaíso, 2009.

MORALES, Marco y TAIPE, Fabián, *Análisis y Diseño de una Infraestructura de redes basado en VLAN's para la Comandancia del Ejército,* Escuela Politécnica Nacional, Quito, Enero 2006.

NUÑEZ, David, *Estudio para la migración de IPV4 a IPV6 para la empresa proveedora de Internet Milltec S.A*, Escuela Politécnica Nacional, Quito, Agosto del 2009.

ORTEGA, Julissa y REINOSO, Diego, *Análisis y Diseño del enlace de datos IPV6 para el Ministerio de Desarrollo y Vivienda – MIDUVI*, Escuela Politécnica Nacional, Quito Diciembre del 2006.

ORTEGA, Hugo, *Análisis e Implementación de un Sistema Video Streaming en Redes Dual Stack IPV4/IPV6*, Pontificia Universidad Católica del Perú, Lima, 2010.

RIOS, René y FERMIN, José, *Análisis de Tráfico de una red local Universitaria*, Universidad Rafael Belloso Chacín, 2009

ROBERT, Reina, PELÁEZ, Gerado y GURRIS Luis, *Metodología de Implementación de Ipv6 en La Red de La Universidad de Oriente*, Universidad de Oriente, s/f.

RODRIGUEZ, Mirella y ZAMBRANO, Marilú, *Análisis y diseño de una reingeniería organizativa de la red del campus de la Universidad Técnica de Manabí mediante la utilización de IPV6 y su Implementación en la Facultad de ciencias Informáticas en el Laboratorio de Redes*, Universidad Técnica de Manabí, Portoviejo, 2010.

RUIZ, Oscar, *Plan Estratégico de Tecnología Informática para una empresa del sector Alimentos*, Universidad Pontificia Bolivariana, Medellín, 2012.

UBIDIA, Anibal, *Análisis Diseño e Implementación de una Intranet IPV6 y QoS*, Escuela Politécnica del Ejército, Sangolquí, 24 de Mayo del 2007.

VASQUEZ, Jenny, *Análisis de las funcionalidades de los protocolos de seguridad IPSEC, IKE, ISAKMP, sobre IPV6 e Implementación en una red prototipo bajo infraestructura CISCO*, Universidad Politécnica Salesiana, Quito, Abril 2009.

VERA, Ghislayne, *Diseño de la transición de direcciones IPv4 a IPv6 en la Extensión Universitaria de Zamora*, Universidad Técnica Particular de Loja, Zamora, 2009.

Libros y Manuales:

6SOS, *El protocolo IPV6*, Enero 2004.

Guía para la incorporación de IPV6 como requisito de compra pública, Instituto Nacional de Tecnologías de la Comunicación S.A, España, Enero 2012.

Plan Estratégico de Tecnología de Información, UNMSM, s/f.

ALMEIDA, Jenny y otros, *Protocolos de enrutamiento para IPV6*, 2005.

ALVARADO, Luis, *Proyecto de Cableado Estructurado y Diseño de red Bankcolombie*, Corporación Universitaria Remington, Medellín, 2007.

CICILEO, Guillermo, IPV6 para todos, Internet Society, Buenos Aires, 2009.

CISCO, *Deploying IPv6 in Branch Networks*, s/f.

CISCO, *Cisco IOS IPv6 Configuration Guide*, 2008

CISCO, *CCNA 1 and 2 Versión 3.1 Curriculum en formato pdf*, s/f.

CISCO, *CCNA Exploration 4.0 Conceptos y protocolos de enrutamiento* (Manual de prácticas de laboratorio para el instructor), s/f.

DOOLEY, Kevin y BROWN, Ian, *CISCO IOS Cookbook 2nd Edition*, O'REILLY.

DOS SANTOS, Rodrigo, y otros, *Curso IPV6 básico*, Núcleo de Información y Coordinación, Sao Paulo, 2010.

HAGEN, Silvia, *IPV6 Essentials*, O'REILLY.

KLEIN, Joel, *IPV6 Security Are you ready?*, 2009, p.3.

LOPEZ, Martín, *Técnicas de comunicación IPV6 en redes IPV4*, Benemérita Universidad Autónoma de Puebla, Puebla, Diciembre 2003.

PERALTA, Luis, *IPV6*, Febrero 2012.

RAMOS, Iván, *IPV4 IPV6*, Universidad Nacional Experimental Politécnica de la Fuerza Armada, Guacara - Venezuela, Abril 2011.

SALVUCCI, Gustavo y VIRUES, Luis, *Diseño de una red LAN*, Argentina, 2003.

SEPULVEDA, Francisco, *Tecnología de Stack Doble IPV4-IPV6*, s/f.

Páginas web:

CHAPTER 37 Configuring IPV6 ACLs, s/f, http://www.cisco.com/en/US/docs/switches/metro/me3400/software/release/12.2_50_se/configuration/guide/swv6acl.pdf.

CHAPTER 38 Configuring IPV6 ACLs, s/f, http://www.cisco.com/en/US/docs/switches/lan/catalyst3750x_3560x/software/release/12.2_55_se/configuration/guide/swv6acl.pdf

CHAPTER 13 Configuring VLAN ACLs, s/f http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_1/nx-os/security/configuration/guide/sec_vlanacls.pdf

CCNA Security, 2009, http://es.scribd.com/doc/65202776/CCNA-Security-Espanol

Características de IPV6, 2011, http://www.redesymas.org/2011/06/caracteristicas-principales-de-ipv6.html

Configuración Routing / resumen comandos, s/f, http://www.6deploy.org/workshops/20100927_bogota_colombia/DIA3-3-routing-Help_Commands_Cisco.pdf

Curso Cableado Estructurado, Universidad del Azuay, Junio 2006, http://www.slideshare.net/jorge_613/cableado-estructurado-5142635

Ejercicio de Subneteo con VLSM de una Red Clase B - Calcular Máscara Variable, 2009, http://www.garciagaston.com.ar/verpost.php?id_noticia=193

IPv6 Access Lists on IOS, Junio 2010, http://packetlife.net/blog/2010/jun/30/ipv6-access-lists-acl-ios/

Las empresas no están listas para IPV6, s/f, http://www.ipv6.mx/index.php/informacion/noticias/1-latest-news/106-enterprisenotreadyipv6

Listas de Control de Acceso VLAN, s/f, http://es.scribd.com/doc/58116973/12/Listas-de-Control-de-Acceso-VLAN.

Migramos la red a IPv6, s/f, http://quepagina.es/internet/migramos-la-red-a-ipv6.html

Normas y Estándares para la Administración Pública Conectividad, s/f, http://www.optic.gob.do/LinkClick.aspx?fileticket=jv0etBu0H08%3D&tabid=88&mid=1060

Preguntas Frecuentes, IPV6 Chile, s/f, http://www.ipv6.cl/pequena-oficina/preguntas-frecuentes.

Que es una Red Backbone, s/f, http://wifiw.com/1625/que-es-una-red-backbone.html#ixzz1ZpJf3p1e

Uso de IPV6 situación actual y perspectivas del futuro, Internet Society, s/f, http://www.internetsociety.org/sites/default/files/ipv6-way-forward-es.pdf.

Router Cisco: Configuración básica, s/f, http://es.kioskea.net/faq/2759-router-cisco-configuracion-basica

Tutorial Subneteo VLSM / CIDR - Máscara de Subred de Longitud Variable, 2009, http://www.garciagaston.com.ar/verpost.php?id_noticia=189

AGUILERA, Rubén, *Trabajando con los Web Services de Liferay*, 2010, http://www.adictosaltrabajo.com/tutoriales/tutoriales.php?pagina=LiferayWebServices

AHUATZIN, Gerardo, *Desarrollo de un esquema de traducción de direcciones IPV6-IPV4-IPV6,* s/f, http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/ahuatzin_s_gl/capitulo3.pdf

CASTRO, Gabriel, *Introducción de IPV6 en Telecom Argentina,* 2010, http://lacnic.net/documentos/presentaciones/lacnicxiv/TelecomArgentinaIPv6.pdf

CEDIA, *Curso IPV6,* Enero 2010, http://dspace.cedia.org.ec/bitstream/123456789/44/2/cedia%20ipv6%20curso.pdf

CISCO, *CCNA Security 1.0 Implementación de seguridad en redes*, s/f, http://es.scribd.com/doc/34759326/Ccna-Security-Iins

CISCO, *Deploying IPv6 in Campus Networks*, Febrero 2012, http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/CampIPv6.html#wp390438.

CISCO, *Adding an IPv6 Access List*, s/f, http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/acl_ipv6.html#wpxref69804.

CISCO, *Configuring IPv6 ACLs*, s/f, http://www.cisco.com/en/US/docs/switches/blades/3110/software/release/12.2_40_ex2/configuration/guide/swv6acl.html

CISCO, Configuring Voice VLAN, s/f, http://www.cisco.com/en/US/docs/switches/lan/catalyst3550/software/release/12.1_19_ea1/configuration/guide/swvoip.html

CISCO, *CHAPTER 14 Configuring Voice VLAN*, s/f, http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_40_se/configuration/guide/swvoip.pdf

CISCO, *CCNA ICND2 Guía Oficial para el examen de Certificación Segunda edición*, España, 2008, http://es.scribd.com/doc/79514092/17/Creacion-de-VLANs-y-asignacion-de-VLANs-de-acceso-a-una-interfaz.

CISCO, *Cisco Self-Study: Implementing Cisco IPv6 Networks (IPV6)*, 2003, http://www.ciscopress.com/articles/article.asp?p=31948&seqNum=4

CISCO, *DHCPv6 Using the Prefix Delegation Feature Configuration Example*, 2011, http://www.cisco.com/en/US/tech/tk872/technologies_configuration_example09186a0080b8a116.shtml

CISCO, *Implementing Traffic Filters and Firewalls for IPv6 Security*, 2011, http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-sec_trfltr_fw.html#wp1073622.

CISCO, *Implementing IPv6: Addressing, Routing, and Dual Stacking*, 2011, https://learningnetwork.cisco.com/thread/31918

CISCO*, IPv6 NAT-PT*, 2011, https://supportforums.cisco.com/thread/2092027

CISCO, *IPv6 IPv4 Network Interconnection NAT-PT*, 2011, https://supportforums.cisco.com/thread/2131296

CISCO, *Understanding Simple Network Management Protocol (SNMP) Traps*, 10 de Octubre de 2006, http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094aa5.shtml

CONAWAY, Aaron, *Some Exercises with IPv6 ACLs*, Abril 2011, http://aconaway.com/2011/04/15/some-exercises-with-ipv6-acls/.

COMPUTER NETWORKING*, How to configure routing with IPv6 step by step guides*, 2011,http://computernetworkingnotes.com/ipv6-features-concepts-and-configurations/routing-with-ipv6.html

COMPUTER WORLD, *Como migrar a IPV6*, 2011, http://www.networkworld.es/Como-migrar-a-IPv6/seccion-atualidad/noticia-111664

EGIDO, Fernando, *Como realizar la migración a IPV6 en seis sencillos pasos*, s/f, http://www.muycomputerpro.com/2011/04/26/migracion-ipv6-seis-pasos/

ECURED, *Calidad de servicio*, 12 de septiembre de 2012, http://www.ecured.cu/index.php/Calidad_de_servicio.

GAGLIANO, Roque, *Planificando IPV6*, s/f, http://lacnic.net/documentos/lacnicxii/presentaciones/Planificacion.pdf

GARCIA, Daniel, *Comandos CISCO CCNA Exploration*, Abril 2011, http://dani.albatalia.com/code/cisco/comandos_cisco_ccna_exploration.pdf

GROSSETETE, Patrick, *Cisco IOS IPv6 Access Control Lists*, 2001, http://www.ipv6-tf.com.pt/documentos/geral/cisco/ipv6_Acls_Abr2003.pdf

GUERRERO, Alejandro, *Tutorial Voz IP Packet Tracer*, Julio 2011, http://www.wcruzy.pe/ri/ptvozip.pdf

ICA, *Insulated Cable Engineers Association*, n.d, http://icea.net/.

JIMENEZ, Jaime y otros, *Framework para el desarrollo del encaminamiento interdominio con QoS basado en PCE sobre MPLS*, Octubre 2008, http://es.scribd.com/doc/89531987/34/Soporte-a-las-clases-de-servicio-CoS

LACNIC, *FAQ sobre IPV6*, s/f, http://portalipv6.lacnic.net/es/ipv6/novedades/preguntas-frecuentes-faq

LACNIC, *IPV6 en el Ambiente Académico*, s/f, http://portalipv6.lacnic.net/es/ipv6/ipv6-en/ambiente-acad-mico-0

LIFERAY, *Funcionalidades de portal*, s/f, http://www.liferay.com/es/products/liferay-portal/features/portal

MARCHAND, William, *Listas de Control de Acceso*, UPLA, s/f, http://es.scribd.com/doc/57583218/Listas-de-Control-de-Acceso-y-Vlan-cap-Upla-2009.

MICROSOFT, *Descubrimiento de Vecinos (ND)*, n.d, http://technet.microsoft.com/es-es/library/cc778019%28v=ws.10%29.

MILLAN, Ramón, *El protocolo IPV6*, 2001, http://www.ramonmillan.com/tutoriales/ipv6_parte1.php

MILLAN, Ramón, *SNMPv3 (Simple Network Management Protocol versión 3)*, 2003, http://www.ramonmillan.com/tutoriales/snmpv3.php

ORACLE, *Capítulo 3 Introducción a IPv6* (Descripción general), s/f, http://docs.oracle.com/cd/E19957-01/820-2981/ipv6-overview-7/index.html

ORELLANA G, Vega L., QUINTANA L., & VIRULA E., *Cableado estructurado*, 01 de enero de 2011, UMG Jutiapa, http://es.scribd.com/doc/77556662/34/I-D-F-CENTRO-INTERMEDIO-DE-DISTRIBUCION-DE-CABLEADO

PALET, Jordi, *Manual para la transición de IPV4 a IPV6*, 2011, http://www.baquia.com/posts/2011-03-21-manual-para-la-transicion-de-ipv4-a-ipv6

RAMIREZ, Sergio, *Introducción al IPV6*, 2005, http://www.rau.edu.uy/ipv6/queesipv6.htm

SANCHEZ, Carlos, *Monitoreo de Redes y Servidores*, 2011, http://cezequiel.wordpress.com/2012/03/11/monitoreo-de-redes-y-servidores/

SANTAMARIA, Pilar*, "Si una empresa no migra a IPV6 su web no podrá estar accesible, 2012"*, s/f, http://www.muycomputerpro.com/2012/06/05/santamaria-cisco-empresa-migra-ipv6-web-accesible/

SKIBBZ, *Configure a static IPV6 address on a network*, 2012, http://skibbz.com/step-by-step-guide-on-how-to-configure-a-static-ipv6-address-on-a-network-device-interface-and-implementation-of-ospf-routing-protocol/

STEPHANY, Erika y ORTEGA, Franco, *Soluciones Perimetrales Plan de Seguridad de la Información solución de aceleración y filtrado Web (Proxy) en Zentyal*, 2011, http://es.scribd.com/doc/61205578/4/DIAGRAMA-LOGICO-DE-RED

STONESOFT, *Diez consejos para implementar IPV6 de forma segura*, s/f, http://www.muycomputerpro.com/2012/07/03/consejos-implementar-ipv6-segura/

VERISIGN, *Lanzamiento mundial del IPv6*, s/f, http://www.verisigninc.com/es_LA/why-verisign/innovation-initiatives/ipv6/index.xhtml

VMWARE Zimbra, *Configuring ZCS to work in an IPv6 environment*, s/f, http://wiki.zimbra.com/wiki/Configuring_for_IP_V6

Wikipedia:

Wikipedia, Advanced Encryption Standard, 15 de agosto de 2012, http://es.wikipedia.org/wiki/Advanced_Encryption_Standard.

Wikipedia, Domain Name System, 11 de septiembre de 2012, http://es.wikipedia.org/wiki/Domain_Name_System.

Wikipedia, Bit, 11 de septiembre de 2012, http://es.wikipedia.org/wiki/Bit.

Wikipedia, Border Gateway Protocol, 09 de agosto de 2012, http://es.wikipedia.org/wiki/Border_Gateway_Protocol.

Wikipedia, CISPR, 17 de junio de 2011, http://es.wikipedia.org/wiki/CISPR.

Wikipedia, Cisco Discovery Protocol, 16 de mayo de 2012, http://es.wikipedia.org/wiki/Cisco_Discovery_Protocol

Wikipedia, Cisco IOS, 24 de julio de 2012, http://es.wikipedia.org/wiki/Cisco_IOS.

Wikipedia, Marca CE, 05 de septiembre de 2012, http://es.wikipedia.org/wiki/Marca_CE.

Wikipedia, Domain Name System, 11 de septiembre de 2012, http://es.wikipedia.org/wiki/Domain_Name_System.

Wikipedia, Dynamic Host Configuration Protocol, 19 de agosto de 2012, http://es.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol.

Wikipedia, DRAM, 9 de septiembre del 2012, http://es.wikipedia.org/wiki/DRAM.

Wikipedia, Exterior Gateway Protocol, 02 de agosto de 2012, http://es.wikipedia.org/wiki/Exterior_Gateway_Protocol.

Wikipedia, Cortafuegos (informática), 05 de septiembre de 2012, http://es.wikipedia.org/wiki/Cortafuegos_%28inform%C3%A1tica%29.

Wikipedia, HTLM, 11 de septiembre de 2012, http://es.wikipedia.org/wiki/HTML.

Wikipedia, HSRP, 06 de junio de 2011, http://es.wikipedia.org/wiki/HSRP.

Wikipedia, Internet Assigned Numbers Authority, 5 de septiembre de 2012, http://es.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority.

Wikipedia, Open Shortest Path First, 16 de mayo de 2012, http://es.wikipedia.org/wiki/Open_Shortest_Path_First

Wikipedia, Internet Engineering Task Force, 27 de agosto de 2012, http://es.wikipedia.org/wiki/Internet_Engineering_Task_Force

Wikipedia, ICMPV6, 8 de enero de 2012, http://es.wikipedia.org/wiki/ICMPv6.

Wikipedia, IPsec, 12 de junio de 2012, http://es.wikipedia.org/wiki/IPsec.

Wikipedia, Interior Gateway Protocol, 2 de agosto de 2012, http://es.wikipedia.org/wiki/Interior_Gateway_Protocol

Wikipedia, ISATAP, 11 de agosto de 2012, http://es.wikipedia.org/wiki/ISATAP.

Wikipedia, Proveedor de servicios de Internet, 5 de septiembre de 2012, http://es.wikipedia.org/wiki/Proveedor_de_servicios_de_Internet

Wikipedia, IEEE 802.1Q, 31 de julio de 2012, http://es.wikipedia.org/wiki/IEEE_802.1Q

Wikipedia, Máquina virtual Java, 9 de septiembre de 2012, http://es.wikipedia.org/wiki/M%C3%A1quina_virtual_Java

Wikipedia, Red de área local, 12 de septiembre de 2012, http://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local

Wikipedia, Liferay, 31 de agosto de 2012, http://es.wikipedia.org/wiki/Liferay.

Wikipedia, Multicast Listener Discovery, 31 de agosto de 2012, http://en.wikipedia.org/wiki/Multicast_Listener_Discovery.

Wikipedia, Unidad máxima de transferencia, 30 de julio de 2012, http://es.wikipedia.org/wiki/Unidad_m%C3%A1xima_de_transferencia.

Wikipedia, Maximum Receive Unit, 19 de julio de 2012, http://es.wikipedia.org/wiki/Maximum_Receive_Unit.

Wikipedia, Nibble, 10 de julio de 2012, http://es.wikipedia.org/wiki/Nibble.

Wikipedia, Neighbor Discovery, 17 de agosto de 2012, http://es.wikipedia.org/wiki/Neighbor_Discovery

Wikipedia, Open Shortest Path First, 16 de mayo de 2012, http://es.wikipedia.org/wiki/Open_Shortest_Path_First.

Wikipedia, PDA, 5 de septiembre de 2012, http://es.wikipedia.org/wiki/PDA.

Wikipedia, Domain Name System, 11 de septiembre de 2012, http://es.wikipedia.org/wiki/Domain_Name_System.

Wikipedia, Calidad de Servicio, 13 de julio de 2012, http://es.wikipedia.org/wiki/Calidad_de_servicio.

Wikipedia, Routing Information Protocol, 1 de septiembre de 2012, http://es.wikipedia.org/wiki/Routing_Information_Protocol#RIPng.

Wikipedia, Memoria de acceso aleatorio, 06 de septiembre de 2012, http://es.wikipedia.org/wiki/Memoria_de_acceso_aleatorio.

Wikipedia, RMON, 13 de agosto de 2012, http://en.wikipedia.org/wiki/RMON.

Wikipedia, Squid (programa), 04 de agosto de 2012, http://es.wikipedia.org/wiki/Squid_%28programa%29.

Wikipedia, Skinny Client Control Protocol, 28 de julio de 2012, http://es.wikipedia.org/wiki/Skinny_Client_Control_Protocol.

Wikipedia, Simple Network Management Protocol, 02 de septiembre del 2012, http://es.wikipedia.org/wiki/Simple_Network_Management_Protocol.

Wikipedia, Session Initiation Protocol, 31 de julio de 2012, http://es.wikipedia.org/wiki/Session_Initiation_Protocol.

Wikipedia, Familia de protocolos de Internet, 3 de septiembre del 2012, http://es.wikipedia.org/wiki/Familia_de_protocolos_de_Internet.

Wikipedia, TFTP, 06 de diciembre de 2012, http://es.wikipedia.org/wiki/TFTP.

Wikipedia, User Datagram Protocol, 2 de septiembre de 2012, http://es.wikipedia.org/wiki/User_Datagram_Protocol.

Wikipedia, Unshielded twisted pair, 12 de agosto de 2012, http://es.wikipedia.org/wiki/Unshielded_twisted_pair.

Wikipedia, UL (Safety Organization), 11 de septiembre de 2012, http://en.wikipedia.org/wiki/UL_%28safety_organization%29.

Wikipedia, VLAN Trunking Protocol, 26 de julio de 2012, http://es.wikipedia.org/wiki/VLAN_Trunking_Protocol.

Wikipedia, Máscaras de subred de tamaño variable, 23 junio de 2012, http://es.wikipedia.org/wiki/M%C3%A1scaras_de_subred_de_tama%C3%B1o_variable

Wikipedia, VCCI, 10 de mayo de 2012, http://es.wikipedia.org/wiki/VCCI.

Wikipedia, VLAN, 30 agosto de 2012, http://es.wikipedia.org/wiki/VLAN.

Wikipedia, Voice activity detection, 13 de agosto de 2012, http://en.wikipedia.org/wiki/Voice_activity_detection.

Wikipedia, Voz sobre Protocolo de Internet, 2 de septiembre de 2012, http://es.wikipedia.org/wiki/Voz_sobre_Protocolo_de_Internet.

Wikipedia, Red de área amplia, 4 de septiembre de 2012, http://es.wikipedia.org/wiki/Red_de_%C3%A1rea_amplia.

Wikipedia, Instituto Nacional Estadounidense de Estándares, 16 de agosto de 2012, http://es.wikipedia.org/wiki/Instituto_Nacional_Estadounidense_de_Est%C3%A1ndares

Wikipedia, Address Resolution Protocol, 2 de septiembre de 2012, http://es.wikipedia.org/wiki/Address_Resolution_Protocol.

Wikipedia, File Transfer Protocol, 6 de septiembre de2012, http://es.wikipedia.org/wiki/File_Transfer_Protocol.

Wikipedia, Gigabit Ethernet, 22 de agosto de 2012, http://en.wikipedia.org/wiki/Gigabit_Ethernet.

Wikipedia, Hypertext Transfer Protocol, 12 de septiembre de 2012, http://es.wikipedia.org/wiki/Hypertext_Transfer_Protocol.

Wikipedia, Comisión Electrotécnica Internacional, 20 de mayo de 2012, http://es.wikipedia.org/wiki/Comisi%C3%B3n_Electrot%C3%A9cnica_Internacional.

Wikipedia, Organización Internacional de Normalización, 4 de septiembre de 2012, http://es.wikipedia.org/wiki/Organizaci%C3%B3n_Internacional_de_Normalizaci%C3%B3n.

Wikipedia, Multidifusión, 5 de septiembre de 2012, http://es.wikipedia.org/wiki/Multidifusi%C3%B3n.

Wikipedia, National Electrical Manufacturers Association, 3 de septiembre de 2012, http://es.wikipedia.org/wiki/National_Electrical_Manufacturers_Association.

Wikipedia, Network News Transport Protocol, 2 de septiembre de 2012, http://es.wikipedia.org/wiki/Network_News_Transport_Protocol.

Wikipedia, Policloruro de vinilo, 12 de julio de 2012, http://es.wikipedia.org/wiki/Policloruro_de_vinilo.

Wikipedia, Post Office Protocol, 6 de julio de 2012, http://es.wikipedia.org/wiki/Post_Office_Protocol.

Wikipedia, Arquitectura orientada a servicios, 12 de septiembre de 2012, http://es.wikipedia.org/wiki/Arquitectura_orientada_a_servicios.

Wikipedia, Simple Mail Transfer Protocol, 2 de septiembre de 2012, http://es.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol.

Wikipedia, Microsoft SQL Server, 05 de septiembre de 2012, http://es.wikipedia.org/wiki/Microsoft_SQL_Server.

Wikipedia, TIA-568B, 07 de mayo de 2012, http://es.wikipedia.org/wiki/TIA-568B.

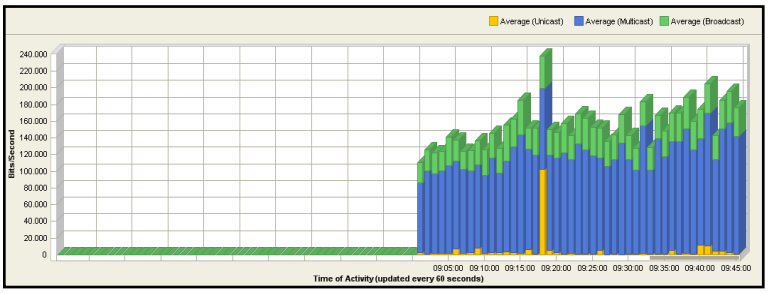
Wikipedia, Unicast, 25 de julio de 2012, http://es.wikipedia.org/wiki/Unicast.

ANEXOS

ANEXO 1. ANÁLISIS TRAFICO DE RED

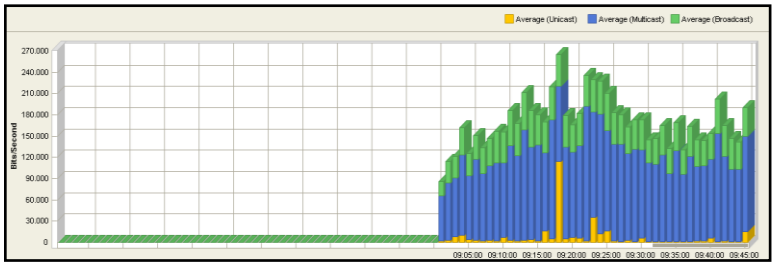
1. Análisis de paquetes Bits/Segundo

DIA 1



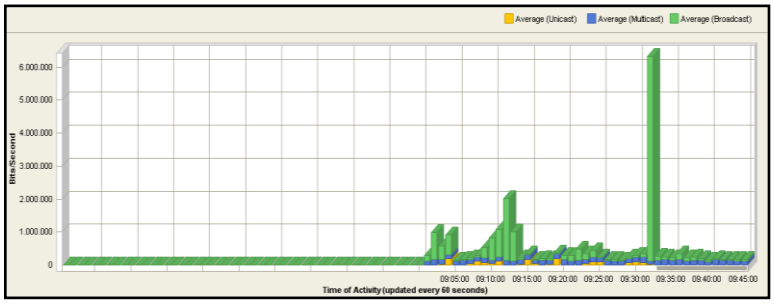
En el Gráfico 1, podemos observar que en el transcurso del tiempo los paquetes broadcast poseen una mayor transmisión (valor máximo de 240.000 bits/segundo) con respecto a los paquetes multicast sobre la red de la UPS Sede-Cuenca.

DIA 2



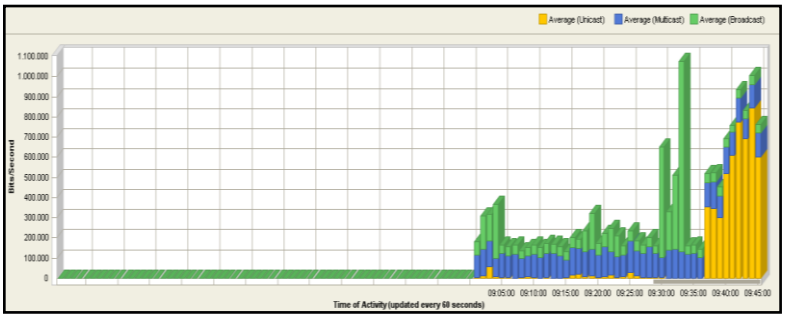
En el Gráfico 2, podemos observar que los paquetes broadcast poseen una mayor transmisión (valor máximo 270.000 bits/segundo) con respecto a los paquetes multicast sobre la red de la UPS Sede-Cuenca.

DIA 3



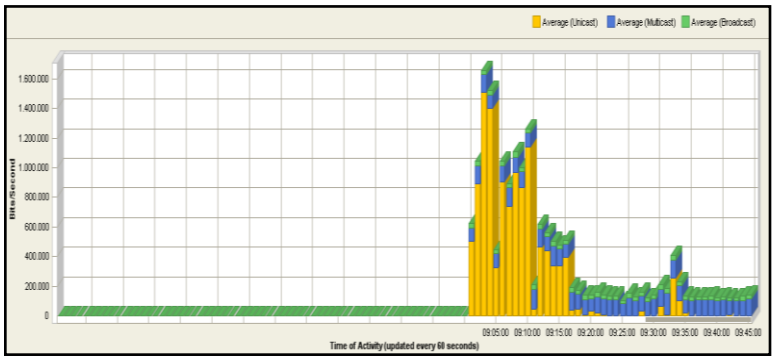
En el Gráfico 3, podemos observar que en el transcurso de las 9:05 y 9:30 los paquetes de broadcast ofrecen diferentes valores (1000.000-2000.000 bits/segundo) pero cabe destacar que en el rango de tiempo comprendido entre las 9:30 y 9:35 los paquetes broadcast alcanzan un valor mayor a los 6000.000 bits/segundo.

DIA 4



En la Gráfico 4, podemos observar que los paquetes broadcast alcanzan valores que van desde los 100.000 – 1100.000 bits/segundo, también se ha podido observar que en el rango de tiempo comprendido entre las 9:35 – 9:45 los paquetes unicast alcanzan valores mayores que van desde los 300.000 – 800.000 bits/segundo.

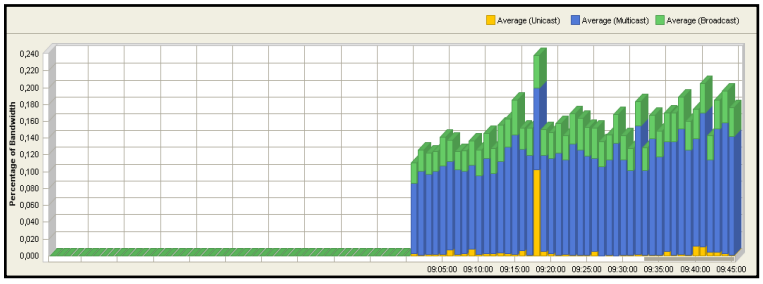
DIA 5



En la Gráfico 5, podemos observar que los paquetes broadcast alcanzan un valor máximo de 1600.000 bits/segundo, de igual manera los paquetes multicast presentan un valor similar al anterior, pero cabe destacar que en el rango de tiempo comprendido entre las 9:00 y 9:15 los paquetes unicast alcanzan diferentes valores que van desde 0 – 1400.000 bits/segundo.

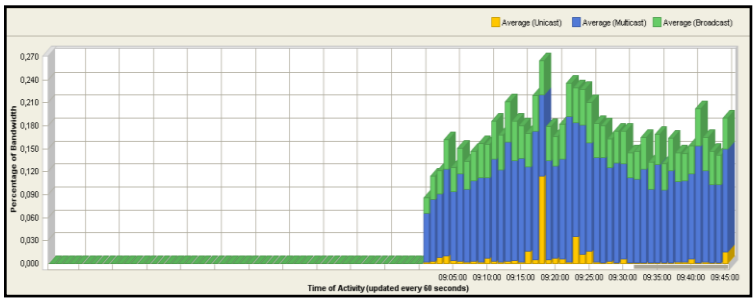
2. Análisis del Porcentaje de Ancho de Banda

DIA 1



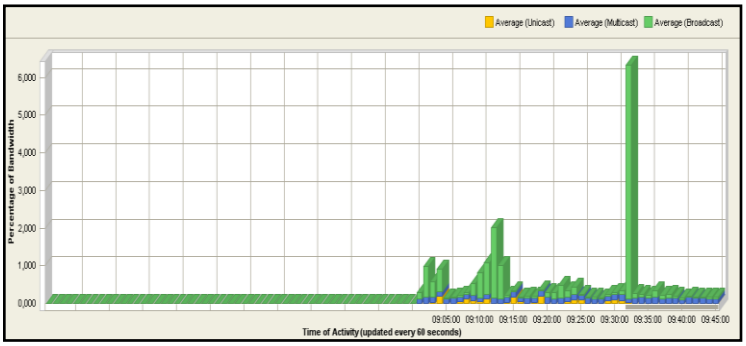
En este gráfico podemos observar que los paquetes de broadcast alcanzan la mayor utilización promedio de ancho de bando con un valor máximo de 0,240%, seguido por los paquetes multicast cuyo valor máximo es de 0,180%

DIA 2



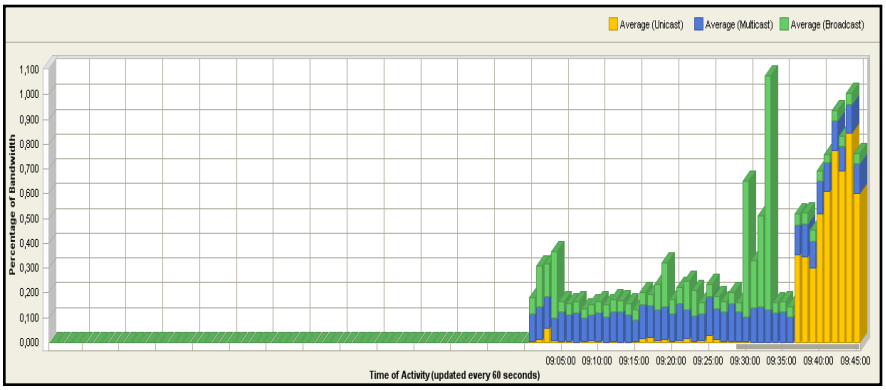
En este gráfico podemos observar que los paquetes de broadcast tienen diferentes valores que va desde el 0,060% - 0,240%, mientras que los paquetes multicast tienen valores que van desde 0,055% - 0,210% de utilización promedio del ancho de banda.

DIA 3



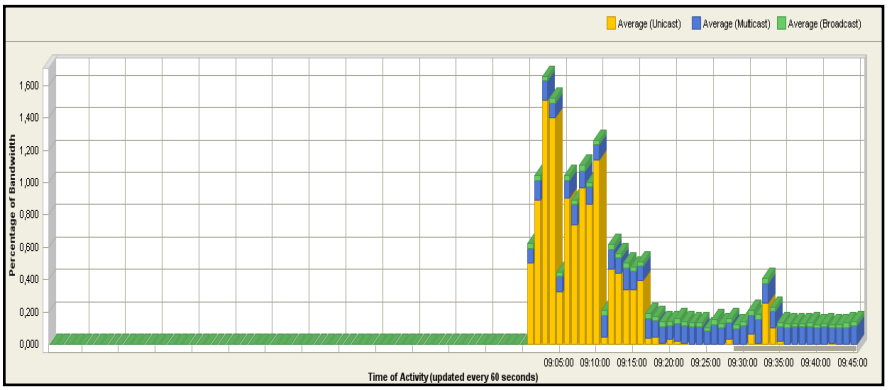
En este gráfico podemos observar una gran diferencia con respecto a los anteriores, debido a que los paquetes broadcast alcanzan valores que van desde 0,100% hasta un valor máximo de 6,00% (alcanzado a las 9:32 min.), mientras tanto los paquetes multicast no sobrepasan el 0,500% de utilización promedio del ancho de banda.

DIA 4



En este gráfico podemos observar que los paquetes broadcast alcanzan un valor máximo de 1,050%, los paquetes multicast un valor máximo de 0,900% mientras q los paquetes unicast alcanzan valores altos que van desde 0,200% - 0,800% (de 9:35 – 9:45 min.).

DIA 5



En este gráfico podemos observar que los paquetes Broadcast alcanza un valor máximo de 1,500%, los paquetes multicast de 1,600%, mientras tanto los paquetes unicast sobresalen durante el rango de tiempo comprendido entre las 9:00 – 9:15 min., alcanzando un valor máximo de 1,400% de utilización promedio del ancho de banda.

3. Análisis de los Protocolos dentro de la red de la UPS Sede-Cuenca

DIA 1

Gráfico 1.

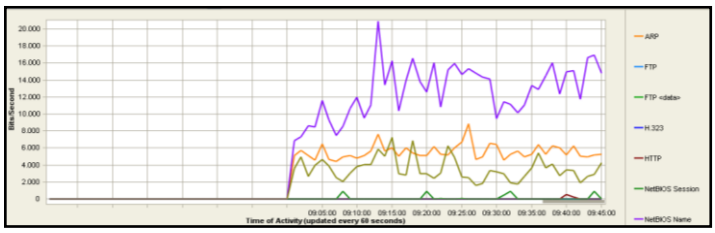
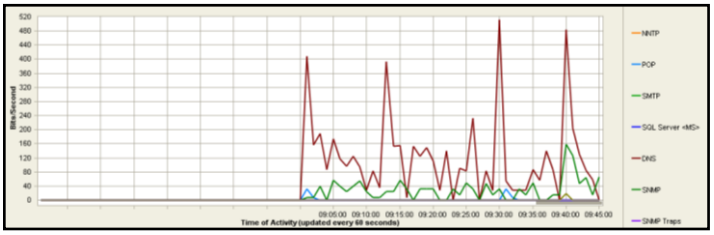


Gráfico 2.



Resultados Obtenidos con los 3 Protocolos más importantes del Gráfico 1:

Orden	Valor máximo	Protocolo
1	20000 bits/seg.	NetBIOS Name
2	8900 bits/seg.	ARP
3	7000 bits/seg.	NetBIOS Session

Resultados Obtenidos con los 3 Protocolos más importantes del Gráfico 2:

Orden	Valor máximo	Protocolo
1	510 bits/seg.	DNS
2	160 bits/seg.	SNMP
3	30 bits/seg.	POP

DIA 2

Gráfico 3.

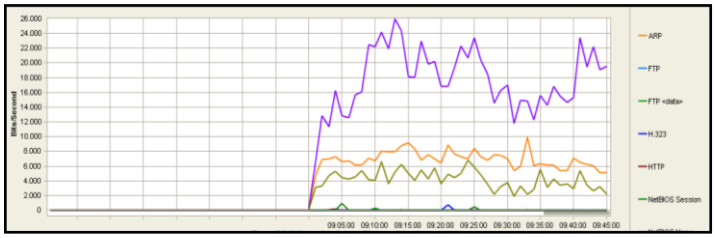
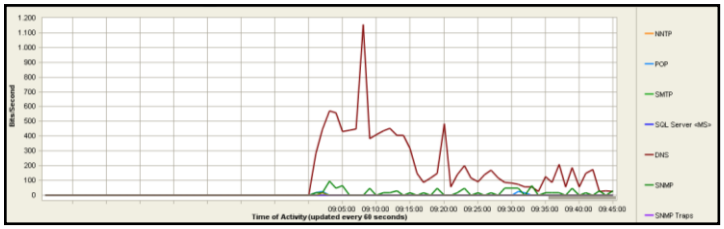


Gráfico 4.



Resultados Obtenidos con los 3 Protocolos más importantes del Gráfico 3:

Orden	Valor máximo	Protocolo
1	26000 bits/seg.	NetBIOS Name
2	10000 bits/seg.	ARP
3	6800 bits/seg.	NetBIOS Session

Resultados Obtenidos con los 3 Protocolos más importantes del Gráfico 4:

Orden	Valor máximo	Protocolo
1	1150 bits/seg.	DNS
2	100 bits/seg.	SNMP
3	50 bits/seg.	POP

DIA 3

Grafico 5.

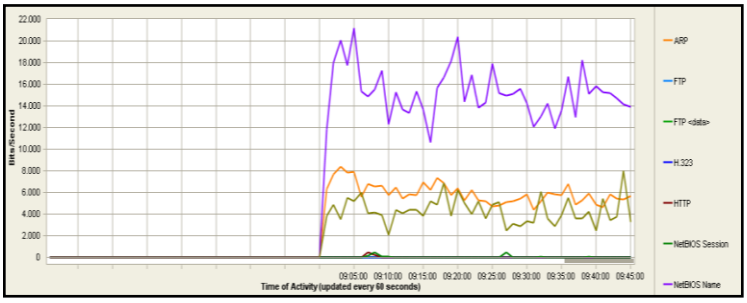
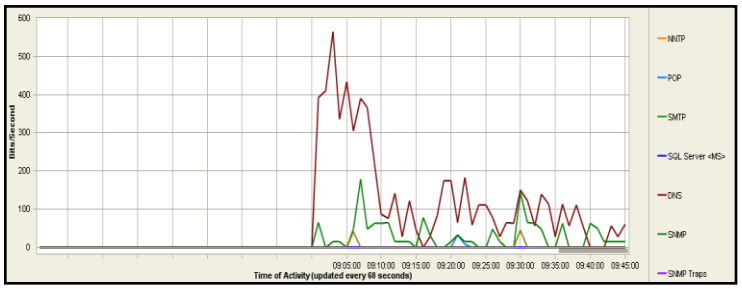


Gráfico 6.



Resultados Obtenidos con los 3 Protocolos más importantes del Gráfico 5:

Orden	Valor máximo	Protocolo
1	21000 bits/seg.	NetBIOS Name
2	8100 bits/seg.	ARP
3	8000 bits/seg.	NetBIOS Session

Resultados Obtenidos con los 3 Protocolos más importantes del Gráfico 6:

Orden	Valor máximo	Protocolo
1	560 bits/seg.	DNS
2	180 bits/seg.	SNMP
3	30 bits/seg.	POP

DIA 4

Grafico 7.

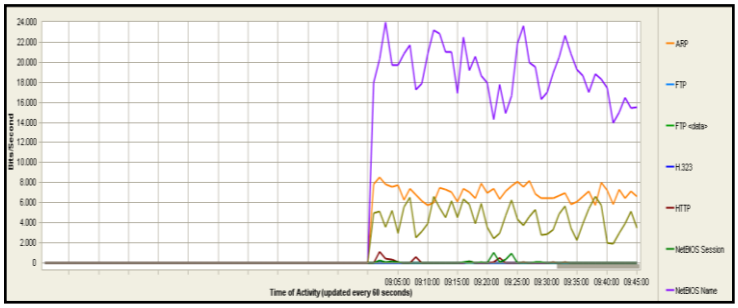
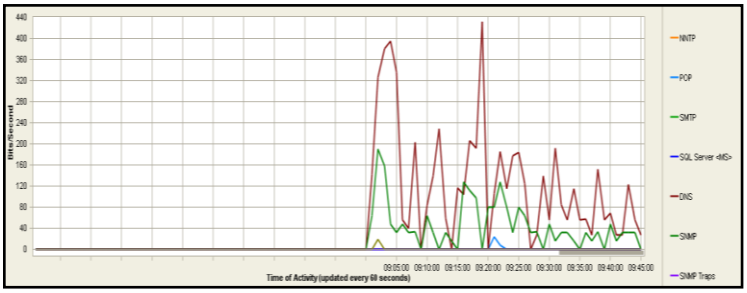


Gráfico 8.



Resultados Obtenidos con los 3 Protocolos más importantes del Gráfico 7:

Orden	Valor máximo	Protocolo
1	24000 bits/seg.	NetBIOS Name
2	8500 bits/seg.	ARP
3	6900 bits/seg.	NetBIOS Session

Resultados Obtenidos con los 3 Protocolos más importantes del Gráfico 8:

Orden	Valor máximo	Protocolo
1	430 bits/seg.	DNS
2	190 bits/seg.	SNMP
3	25 bits/seg.	POP

DIA 5

Gráfico 9.

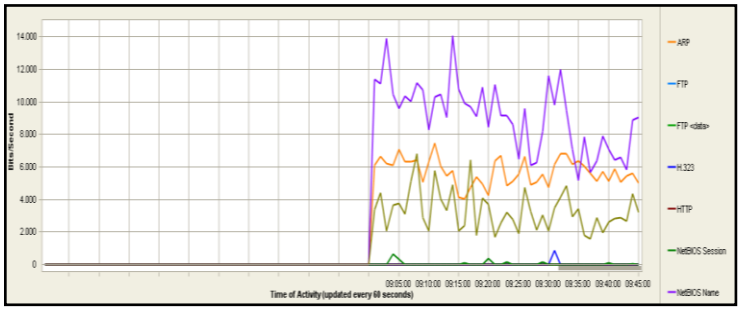
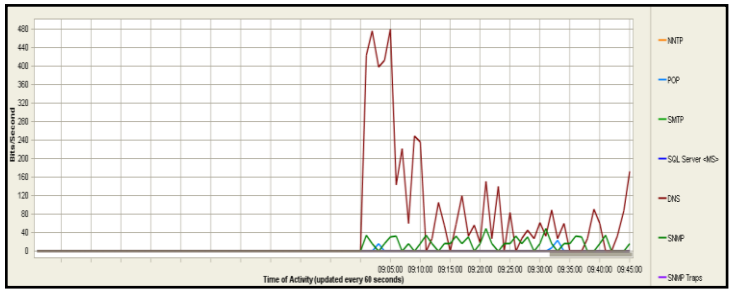


Gráfico 10.



Resultados Obtenidos con los 3 Protocolos más importantes del Gráfico 9:

Orden	Valor máximo	Protocolo
1	14000 bits/seg.	NetBIOS Name
2	7500 bits/seg.	ARP
3	6900 bits/seg.	NetBIOS Session

Resultados Obtenidos con los 3 Protocolos más importantes del Gráfico 10:

Orden	Valor máximo	Protocolo
1	480 bits/seg.	DNS
2	50 bits/seg.	SNMP
3	30 bits/seg.	POP

RESULTADOS FINALES

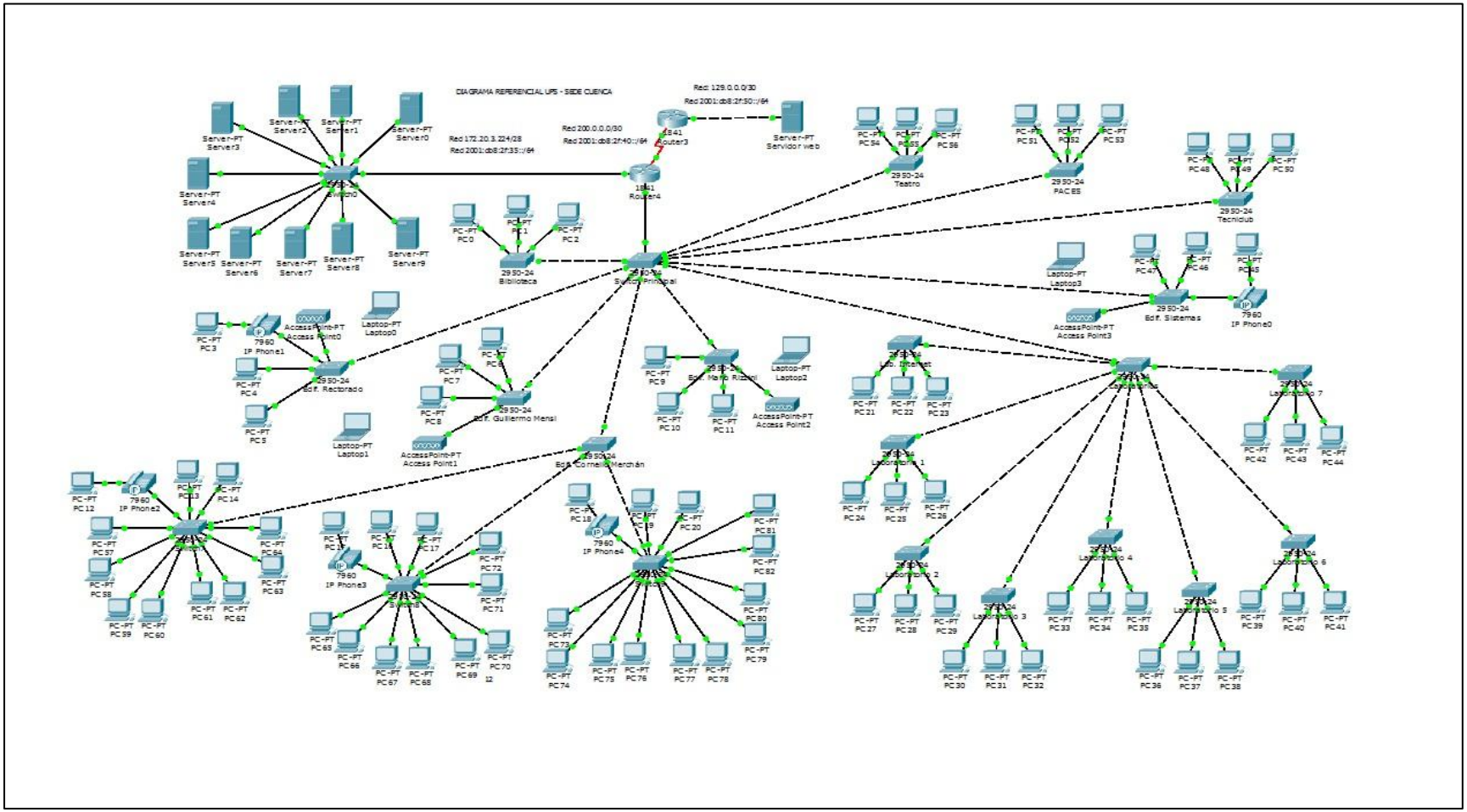
Tabla 1.

Orden	Valor máx. Promedio 5 días	Protocolo	Análisis del Protocolo
1	21000 bits/seg.	NetBIOS Name	Se ha podido observar que la mayor parte del tiempo se utiliza el Servicio NetBIOS Name cuya función es el registro de nombres y resolución de un equipo. NetBIOS Name no soporta IPV6. La principal desventaja de NetBIOS es la vulnerabilidad, además realiza un broadcast en la red para compartir su información, consumiendo recursos.
2	8600 bits/seg.	ARP	ARP es el protocolo de la capa de enlace de datos que ocupa el segundo lugar dentro del análisis de la red de la UPS Sede-Cuenca, su función es encontrar la dirección MAC que corresponde a una determinada dirección IP.
3	7120 bits/seg.	NetBIOS Session	NetBIOS Session permite que 2 equipos establezcan una conexión para dar paso a una “conversación”.

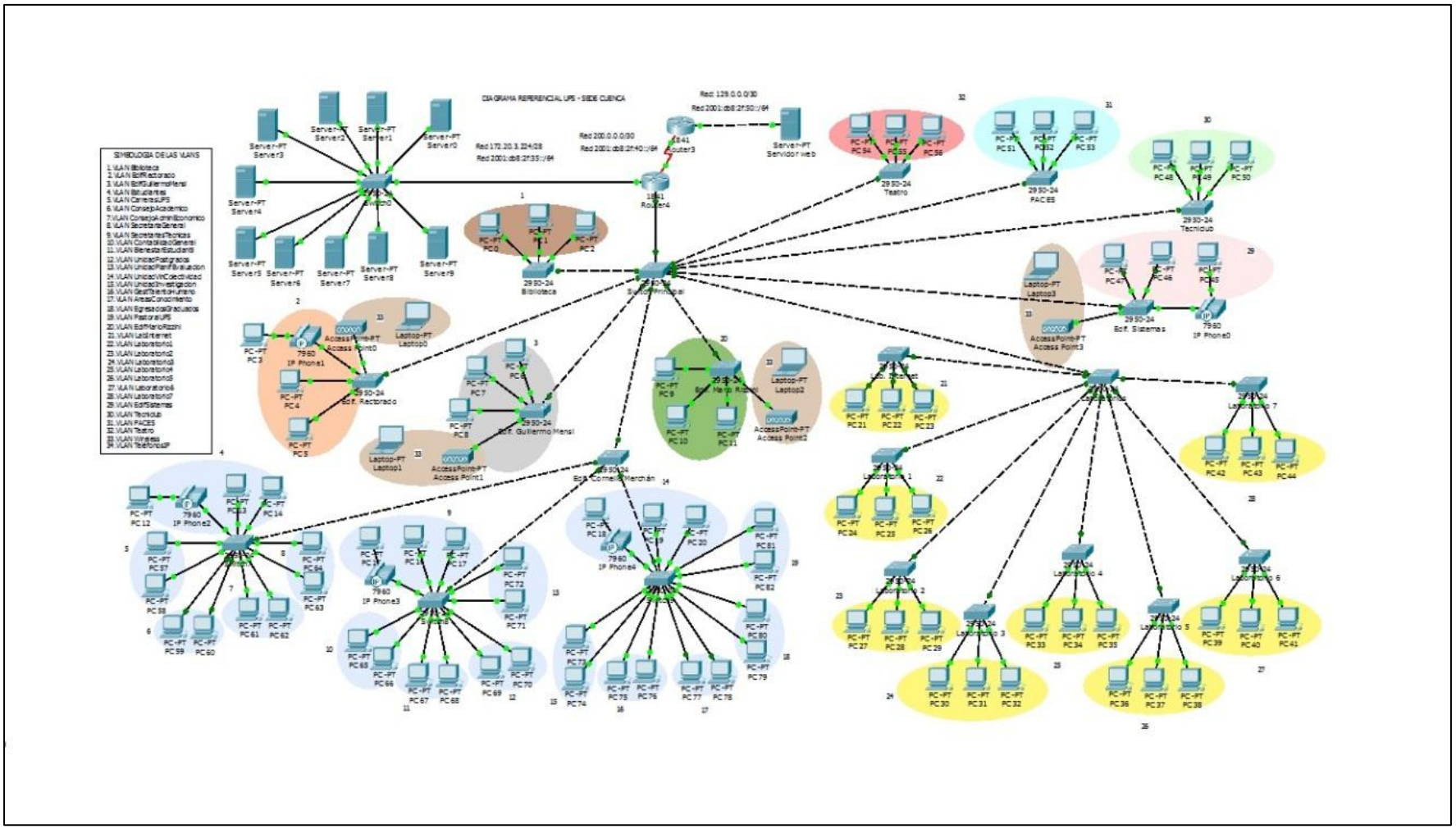
Tabla 2.

Orden	Valor máx. Promedio 5 días	Protocolo	Análisis del Protocolo
1	626 bits/seg.	DNS	Otro de los protocolos con mayor utilización durante el período de tiempo comprendido entre las 9:00 – 9:45am (cambio de la 1era hora) es el protocolo DNS cuya función es la resolución de nombres para redes TCP/IP, eso significa que la mayor parte de los usuarios están utilizando un nombre descriptivo dentro de una aplicación o navegando en internet.
2	136 bits/seg.	SNMP	El protocolo SNMP es un protocolo de la capa de aplicación que utiliza el segundo lugar cuya función es facilitar el intercambio de información de administración entre dispositivos de red.
3	33 bits/seg.	POP	El protocolo POP es un protocolo a nivel de aplicación, cuya función es obtener los mensajes de correo electrónico almacenados en un servidor remoto, eso significa que la mayoría de usuarios revisan sus correos electrónicos de tal forma que se conectan a los servidores que almacenan los e-mails y reciben sus mensajes a la computadora cliente.

ANEXO 2. DISEÑO DE LA TOPOLOGÍA DE RED DE LA UPS SEDE CUENCA EN EL PACKET TRACER VERSIÓN 5.3.2.0027



ANEXO 3. DIAGRAMA DE VLANS DESARROLLADO EN EL PACKET TRACER VERSIÓN 5.3.2.0027



ANEXO 4. DISTRIBUCIÓN DE DIRECCIONES PARA CADA SUBRED

1. Subred Biblioteca: 172.20.0.0/26

Dirección IP	Descripción
172.20.0.0	Dirección de red de la Biblioteca.
172.20.0.1	Dirección para el Gateway
172.20.0.2	Dirección de red de la PC0
172.20.0.3	Dirección de red de la PC1
172.20.0.4	Dirección de red de la PC2
172.20.0.5 - 172.20.0.50	Rango de direcciones IP para la red actual.
172.20.0.51 - 172.20.0.62	Rango de direcciones IP para un crecimiento futuro.
172.20.0.63	Dirección de broadcast.

2. Subred Edif. Rectorado: 172.20.0.64/26

Dirección IP	Descripción
172.20.0.64	Dirección de red del Edif. Rectorado.
172.20.0.65	Dirección para el Gateway
172.20.0.66	Dirección de red de la PC0
172.20.0.67	Dirección de red de la PC1
172.20.0.68	Dirección de red de la PC2
172.20.0.69 - 172.20.0.114	Rango de direcciones IP para la red actual.
172.20.0.115 - 172.20.0.126	Rango de direcciones IP para un crecimiento futuro.
172.20.0.127	Dirección de broadcast.

3. Subred Edif. Guillermo Mensi: 172.20.0.128/26

Dirección IP	Descripción
172.20.0.128	Dirección de red del Edif. Guillermo Mensi.
172.20.0.129	Dirección para el Gateway
172.20.0.130	Dirección de red de la PC0
172.20.0.131	Dirección de red de la PC1
172.20.0.132	Dirección de red de la PC2
172.20.0.133 - 172.20.0.177	Rango de direcciones IP para la red actual.
172.20.0.178 - 172.20.0.190	Rango de direcciones IP para un crecimiento futuro.
172.20.0.191	Dirección de broadcast.

4. Subred Edif. Cornelio Merchán SW 1: 172.20.0.192/26

Dirección IP	Descripción
172.20.0.192	Dirección de red del Edif. Cornelio Merchán SW1.
172.20.0.193	Dirección para el Gateway
172.20.0.194	Dirección de red de la PC0
172.20.0.195	Dirección de red de la PC1
172.20.0.196	Dirección de red de la PC2
172.20.0.197 - 172.20.0.241	Rango de direcciones IP para la red actual.
172.20.0.242 - 172.20.0.253	Rango de direcciones IP para un crecimiento futuro.
172.20.0.254	Dirección de broadcast.

5. Subred Edif. Cornelio Merchán SW 2: 172.20.1.0/26

Dirección IP	Descripción
172.20.1.0	Dirección de red del Edif. Cornelio Merchán SW2.
172.20.1.1	Dirección para el Gateway
172.20.1.2	Dirección de red de la PC0
172.20.1.3	Dirección de red de la PC1
172.20.1.4	Dirección de red de la PC2
172.20.1.5 - 172.20.1.49	Rango de direcciones IP para la red actual.
172.20.1.50 - 172.20.1.62	Rango de direcciones IP para un crecimiento futuro.
172.20.1.63	Dirección de broadcast.

6. Subred Edif. Cornelio Merchán SW 3: 172.20.1.64/26

Dirección IP	Descripción
172.20.1.64	Dirección de red del Edif. Cornelio Merchán SW3.
172.20.1.65	Dirección para el Gateway
172.20.1.66	Dirección de red de la PC0
172.20.1.67	Dirección de red de la PC1
172.20.1.68	Dirección de red de la PC2
172.20.1.69 - 172.20.1.114	Rango de direcciones IP para la red actual.
172.20.1.114 - 172.20.1.126	Rango de direcciones IP para un crecimiento futuro.
172.20.1.127	Dirección de broadcast.

7. Edif. Mario Rizzini: 172.20.1.128/26.

Dirección IP	Descripción
172.20.1.128	Dirección de red del Edif. Mario Rizzini.
172.20.1.129	Dirección para el Gateway
172.20.1.130	Dirección de red de la PC0
172.20.1.131	Dirección de red de la PC1
172.20.1.132	Dirección de red de la PC2
172.20.1.133 - 172.20.1.177	Rango de direcciones IP para la red actual.
172.20.1.178 - 172.20.1.190	Rango de direcciones IP para un crecimiento futuro.
172.20.1.191	Dirección de broadcast.

8. Edif. Sistemas: 172.20.1.192/26

Dirección IP	Descripción
172.20.1.192	Dirección de red del Edif. Sistemas.
172.20.1.193	Dirección para el Gateway
172.20.1.194	Dirección de red de la PC0
172.20.1.195	Dirección de red de la PC1
172.20.1.196	Dirección de red de la PC2
172.20.1.197 - 172.20.1.241	Rango de direcciones IP para la red actual.
172.20.1.241 - 172.20.1.253	Rango de direcciones IP para un crecimiento futuro.
172.20.1.254	Dirección de broadcast.

9. Teatro: 172.20.2.0/26

Dirección IP	Descripción
172.20.2.0	Dirección de red del Teatro.
172.20.2.1	Dirección para el Gateway
172.20.2.2	Dirección de red de la PC0
172.20.2.3	Dirección de red de la PC1
172.20.2.4	Dirección de red de la PC2
172.20.2.5 - 172.20.2.49	Rango de direcciones IP para la red actual.
172.20.2.50 - 172.20.2.62	Rango de direcciones IP para un crecimiento futuro.
172.20.2.63	Dirección de broadcast.

10. Internet: 172.20.2.64/26

Dirección IP	Descripción
172.20.2.64	Dirección de red del Internet.
172.20.2.65	Dirección para el Gateway
172.20.2.66	Dirección de red de la PC0
172.20.2.67	Dirección de red de la PC1
172.20.2.68	Dirección de red de la PC2
172.20.2.69 - 172.20.2.95	Rango de direcciones IP para la red actual.
172.20.2.96 - 172.20.2.105	Rango de direcciones IP para un crecimiento futuro.
172.20.2.106 - 172.20.2.127	Rango de direcciones IP libres.
172.20.2.128	Dirección de broadcast.

11. Tecniclub: 172.20.2.128/26

Dirección IP	Descripción
172.20.2.128	Dirección de red Tecniclub.
172.20.2.129	Dirección para el Gateway
172.20.2.130	Dirección de red de la PC0
172.20.2.131	Dirección de red de la PC1
172.20.2.132	Dirección de red de la PC2
172.20.2.133 - 172.20.2.154	Rango de direcciones IP para la red actual.
172.20.2.155 - 172.20.2.162	Rango de direcciones IP para un crecimiento futuro.
172.20.2.163 - 172.20.2.190	Rango de direcciones IP libres.
172.20.2.191	Dirección de broadcast.

12. PACES: 172.20.2.192/26

Dirección IP	Descripción
172.20.2.193	Dirección de red PACES.
172.20.2.194	Dirección para el Gateway
172.20.2.195	Dirección de red de la PC0
172.20.2.196	Dirección de red de la PC1
172.20.2.197	Dirección de red de la PC2
172.20.2.198 - 172.20.2.219	Rango de direcciones IP para la red actual.
172.20.2.220 - 172.20.2.227	Rango de direcciones IP para un crecimiento futuro.
172.20.2.228 - 172.20.2.253	Rango de direcciones IP libres.
172.20.2.254	Dirección de broadcast.

13. Laboratorio 1: 172.20.3.0/27

Dirección IP	Descripción
172.20.3.0	Dirección de red del Laboratorio 1
172.20.3.1	Dirección para el Gateway
172.20.3.2	Dirección de red de la PC0
172.20.3.3	Dirección de red de la PC1
172.20.3.4	Dirección de red de la PC2
172.20.3.5 - 172.20.3.23	Rango de direcciones IP para la red actual.
172.20.3.24 - 172.20.3.30	Rango de direcciones IP para un crecimiento futuro.
172.20.2.31	Dirección de broadcast.

14. Laboratorio 2: 172.20.3.32/27

Dirección IP	Descripción
172.20.3.32	Dirección de red del Laboratorio 2
172.20.3.33	Dirección para el Gateway
172.20.3.34	Dirección de red de la PC0
172.20.3.35	Dirección de red de la PC1
172.20.3.36	Dirección de red de la PC2
172.20.3.37 - 172.20.3.55	Rango de direcciones IP para la red actual.
172.20.3.55 - 172.20.3.62	Rango de direcciones IP para un crecimiento futuro.
172.20.2.63	Dirección de broadcast.

15. Laboratorio 3: 172.20.3.64/27

Dirección IP	Descripción
172.20.3.64	Dirección de red del Laboratorio 3
172.20.3.65	Dirección para el Gateway
172.20.3.66	Dirección de red de la PC0
172.20.3.67	Dirección de red de la PC1
172.20.3.68	Dirección de red de la PC2
172.20.3.69 - 172.20.3.87	Rango de direcciones IP para la red actual.
172.20.3.88 - 172.20.3.94	Rango de direcciones IP para un crecimiento futuro.
172.20.2.95	Dirección de broadcast.

16. Laboratorio 4: 172.20.3.96/27

Dirección IP	Descripción
172.20.3.96	Dirección de red del Laboratorio 4
172.20.3.97	Dirección para el Gateway
172.20.3.98	Dirección de red de la PC0
172.20.3.99	Dirección de red de la PC1
172.20.3.100	Dirección de red de la PC2
172.20.3.101 - 172.20.3.119	Rango de direcciones IP para la red actual.
172.20.3.120 - 172.20.3.126	Rango de direcciones IP para un crecimiento futuro.
172.20.2.127	Dirección de broadcast.

17. Laboratorio 5: 172.20.3.128/27

Dirección IP	Descripción
172.20.3.128	Dirección de red del Laboratorio 5
172.20.3.129	Dirección para el Gateway
172.20.3.130	Dirección de red de la PC0
172.20.3.131	Dirección de red de la PC1
172.20.3.132	Dirección de red de la PC2
172.20.3.133 - 172.20.3.151	Rango de direcciones IP para la red actual.
172.20.3.152 - 172.20.3.158	Rango de direcciones IP para un crecimiento futuro.
172.20.2.159	Dirección de broadcast.

18. Laboratorio 6: 172.20.3.160/27

Dirección IP	Descripción
172.20.3.160	Dirección de red del Laboratorio 6
172.20.3.161	Dirección para el Gateway
172.20.3.162	Dirección de red de la PC0
172.20.3.163	Dirección de red de la PC1
172.20.3.164	Dirección de red de la PC2
172.20.3.165 - 172.20.3.183	Rango de direcciones IP para la red actual.
172.20.3.184 - 172.20.3.190	Rango de direcciones IP para un crecimiento futuro.
172.20.2.191	Dirección de broadcast.

19. Laboratorio 7: 172.20.3.192/27

Dirección IP	Descripción
172.20.3.192	Dirección de red del Laboratorio 7
172.20.3.193	Dirección para el Gateway
172.20.3.194	Dirección de red de la PC0
172.20.3.195	Dirección de red de la PC1
172.20.3.196	Dirección de red de la PC2
172.20.3.197 - 172.20.3.215	Rango de direcciones IP para la red actual.
172.20.3.216 - 172.20.3.222	Rango de direcciones IP para un crecimiento futuro.
172.20.2.223	Dirección de broadcast.

20. Servidores: 172.20.3.224/28

Dirección IP	Descripción
172.20.3.224	Dirección de red de los Servidores
172.20.3.225	Dirección para el Gateway
172.20.3.226	Dirección de red de la PC0
172.20.3.227	Dirección de red de la PC1
172.20.3.228	Dirección de red de la PC2
172.20.3.229 - 172.20.3.235	Rango de direcciones IP para la red actual.
172.20.3.236 - 172.20.3.238	Rango de direcciones IP para un crecimiento futuro.
172.20.2.239	Dirección de broadcast.

ANEXO 5. CRONOGRAMA DE ACTIVIDADES PARA LA MIGRACIÓN A IPV6 EN LA RED DE LA UPS SEDE-CUENCA.

	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1						
2		**Plan de Implementación para la migración hacia IPV6 en la red de la UPS Sede Cuenca**	**200 días**	**lun 05/11/12**	**vie 09/08/13**	
3		**1. Capacitación del personal técnico**	**45 días**	**lun 05/11/12**	**vie 04/01/13**	
4		1.1 Detectar necesidades de la capacitación	2 días	lun 05/11/12	mar 06/11/12	
5		1.2 Identificar recursos para la capacitación	2 días	mié 07/11/12	jue 08/11/12	4
6		1.3 Integración de un plan de capacitación	2 días	vie 09/11/12	lun 12/11/12	5
7		**1.4 Elaboración de programas de capacitación**	**9 días**	**mar 13/11/12**	**vie 23/11/12**	**6**
8		Establecer los objetivos de la capacitación	2 días	mar 13/11/12	mié 14/11/12	
9		Establecer el contenido del programa para la capacticación	3 días	jue 15/11/12	lun 19/11/12	8
10		Establecer los principios de aprendizaje	2 días	mar 20/11/12	mié 21/11/12	9
11		Seleccionar herramientas de capacitación	1 día	jue 22/11/12	jue 22/11/12	10
12		Seleccionar las técnicas de capacitación	1 día	vie 23/11/12	vie 23/11/12	11
13		1.5 Evaluación, control y seguimiento de la capacitación	30 días	lun 26/11/12	vie 04/01/13	7
14		**2. Adopción de una dirección IPV6**	**6 días**	**lun 07/01/13**	**lun 14/01/13**	**3**
15		Establecer las necesidades de adoptar una dirección IPV6	1 día	lun 07/01/13	lun 07/01/13	
16		Elaboración de oficio para el ISP de la UPS Sede-Cuenca	1 día	mar 08/01/13	mar 08/01/13	15
17		Entrega del oficio en las oficinas del ISP	1 día	mié 09/01/13	mié 09/01/13	16
18		Recepción de la dirección IPV6 para la red de la UPS Sede-Cuenca	3 días	jue 10/01/13	lun 14/01/13	17
19		**3. Asignación de direcciones IPV6**	**5 días**	**mar 15/01/13**	**lun 21/01/13**	**14**
20		Identificar nodos principales en la red de la UPS Sede-Cuenca	2 días	mar 15/01/13	mié 16/01/13	
21		Elaboración de tablas y direcciones IPV6 para cada nodo principal	3 días	jue 17/01/13	lun 21/01/13	20
22		**4. Obtener herramientas de manejo y monitoreo de la red**	**5 días**	**mar 22/01/13**	**lun 28/01/13**	**19**
23		Descripción de necesidades de herramientas de monitoreo de la red	1 día	mar 22/01/13	mar 22/01/13	
24		Investigación sobre cada herramienta de monitoreo de red	2 días	mié 23/01/13	jue 24/01/13	23
25		Descarga de herramientas de software libre para monitoreo de la red	2 días	vie 25/01/13	lun 28/01/13	24
26		**5. Actualización de los nodos para que funcionen con IPV4/IPV6**	**41 días**	**mar 29/01/13**	**mar 26/03/13**	**22**
27		Descarga del IOS para cada uno de los equipos de red	5 días	mar 29/01/13	lun 04/02/13	
28		Actualización y pruebas de funcionamiento del Router principal	1 día	mar 05/02/13	mar 05/02/13	27
29		Actualización y pruebas de funcionamiento del Firewall	1 día	mié 06/02/13	mié 06/02/13	28
30		Actualización y pruebas de funcionamiento de los Access Point	2 días	jue 07/02/13	vie 08/02/13	29
31		Actualización y pruebas de funcionamiento de los Switchs	12 días	lun 11/02/13	mar 26/02/13	30
32		Actualización y pruebas de funcionamiento de los Teléfonos IP	20 días	mié 27/02/13	mar 26/03/13	31
33		**6. Selección de un protocolo de enrutamiento**	**2 días**	**mié 27/03/13**	**jue 28/03/13**	**26**
34		Investigación de protocolos que funcionan sobre IPV6	1 día	mié 27/03/13	mié 27/03/13	
35		Selección del protocolo con las mejores características	1 día	jue 28/03/13	jue 28/03/13	34
36		**7. Implementación de un mecanismo de transición**	**6 días**	**vie 29/03/13**	**vie 05/04/13**	**33**
37		Revisión de los mecanismos de transición	1 día	vie 29/03/13	vie 29/03/13	
38		Implementación del mecanismo de transición Dual-Stack	3 días	lun 01/04/13	mié 03/04/13	37
39		Pruebas de funcionamiento	2 días	jue 04/04/13	vie 05/04/13	38
40		**8. Habilitar los servicios IPV6 necesarios (DNS, QoS,etc)**	**30 días**	**lun 08/04/13**	**vie 17/05/13**	**36**
41		Configuración de los servicios que ofrece el Servidor web	3 días	lun 08/04/13	mié 10/04/13	
42		Configuración de los servicios que ofrece el Servidor proxy	3 días	jue 11/04/13	lun 15/04/13	41
43		Configuración de los servicios que ofrece el Servidor de archivos	3 días	mar 16/04/13	jue 18/04/13	42
44		Configuración de los servicios que ofrece el Servidor antivirus	3 días	vie 19/04/13	mar 23/04/13	43
45		Configuración de los servicios que ofrece el Servidor de desarrollo	3 días	mié 24/04/13	vie 26/04/13	44
46		Configuración de los servicios que ofrece el Servidor Biblioteca	3 días	lun 29/04/13	mié 01/05/13	45
47		Configuración de los servicios que ofrece el Servidor de aplicaciones	3 días	jue 02/05/13	lun 06/05/13	46
48		Configuración de los servicios que ofrece el Servidor de Base de datos	3 días	mar 07/05/13	jue 09/05/13	47
49		Configuración de los servicios que ofrece el Servidor de correo electrónico	3 días	vie 10/05/13	mar 14/05/13	48
50		Configuración de los servicios que ofrece el Servidor de Desarrollo de BD	3 días	mié 15/05/13	vie 17/05/13	49
51		**9. Habilitar IPV6 en los equipos de los usuarios**	**30 días**	**lun 20/05/13**	**vie 28/06/13**	**40**
52		Habilitar DHCP en el router principal	2 días	lun 20/05/13	mar 21/05/13	
53		Configuración y pruebas de funcionamiento en cada equipo de usuario	28 días	mié 22/05/13	vie 28/06/13	52
54		**10. Capacitación de los usuarios de la red**	**30 días**	**lun 01/07/13**	**vie 09/08/13**	**51**
55		Elaboración de cronogramas de capacitación según las áreas de trabajo	2 días	lun 01/07/13	mar 02/07/13	
56		Capacitación para el área de sistemas	5 días	mié 03/07/13	mar 09/07/13	55
57		Capacitación para el área administrativa	5 días	mié 10/07/13	mar 16/07/13	56
58		Capacitación para el área de RRHH	5 días	mié 17/07/13	mar 23/07/13	57
59		Capacitación para el área financiera	5 días	mié 24/07/13	mar 30/07/13	58
60		Capacitación para los docentes	4 días	mié 31/07/13	lun 05/08/13	59
61		Capacitación para los estudiantes	4 días	mar 06/08/13	vie 09/08/13	60