RESUMEN

Capitulo 1: Describe los: Antecedentes, Estado del arte, Realidad Mundial, Realidad en el Ecuador, Descripción del problema y/o necesidad, Justificación del proyecto de tesis, Objetivos y Alcance del proyecto.

Capitulo 2: Conceptos relacionados con lo que es una Intranet y su relación con el sector educativo, como implementar un cableado estructurado, como trabajan las redes inalámbricas y que estándares se utilizaron en la investigación.

Capitulo 3: Recopilación y Análisis de los requerimientos, Diseño de la topología de la red, Documentación física y lógica de la implementación de la red y Descripción de equipos.

Capitulo 4: Implementación de un piloto con los servicios básicos de: DNS, Firewall, Proxy, Web, Correo Electrónico, DHCP y Autenticación.

Capitulo 5: Presupuesto considerando costos de cableado, equipos y costos de implementación.

Capitulo 6: Conclusiones relacionadas y recomendaciones que podrían servir de base para el desarrollo de otros trabajos relacionados.

INDICE

FACULTAD DE INGENIERIA

MAESTRIA EN TELEMATICA

TESIS DE GRADO

TEMA:

"Diseño de la Intranet para el Instituto Tecnológico Fiscomisional Juan XXIII del Cantón Yantzaza Provincia de Zamora Chinchipe."

DIRECTOR:
Ing. Raúl Ortiz Gaona

AUTOR:
Ing. Freddy Patricio Ajila Zaquinaula

CUENCA-ECUADOR
2010

CERTIFICACION

Certifico que el presente trabajo de tesis fue desarrollado por el ingeniero Freddy Patricio Ajila Z. bajo mi dirección.

_____

Ing. Raúl Ortiz

DEDICATORIA:

Dedico este trabajo a DIOS mi creador, a mis padres, esposa y de manera especial a mi nenita Jhaely Ajila que le da sentido a mi vida.

AGRADECIMIENTO:

A la Universidad de Cuenca, Universidad de Loja y en especial al Ing. Raúl Ortiz por su acertada y desinteresada dirección en el desarrollo de este trabajo.

CAPITULO 1

INTRODUCCION

1.1 Antecedentes

El Instituto Tecnológico Fiscomisional "Juan XXIII" Se encuentra ubicado en el centro del cantón Yantzaza y su estructura física está constituida por cuatro bloques de dos pisos distribuidos en un área aproximada de 40.000 metros cuadrados donde funciona la educación pre básico, básico, secundario y superior con la especialidad de Tecnología en Informática.

Su estructura administrativa está constituida por la rectora y vicerrectora que se encargan del nivel secundario y superior, una directora encargada del nivel de pre básica y básica, el área administrativa que lo conforman diez miembros, el área docente conformada por 40 profesores distribuidos en todos los niveles y los aproximadamente mil alumnos distribuidos en los 4 niveles.

Su misión es la de formar personas en los ámbitos: espiritual, intelectual, afectivo, motriz y científico; para enfrentar los retos de la vida de manera responsable y ser parte del desarrollo social, cultural, político y económico del país.

Entre uno de los objetivos específicos que se ha planteado la Institución es el de crear una biblioteca virtual

La meta institucional según consta en el plan estratégico a la largo plazo es la de mejorar la infraestructura física del plantel y a mediano plazo es el fomentar la investigación a nivel de profesores y estudiantes mediante el uso de las TICs (Tecnologías de la Información y comunicaciones).

Por esta razón el Instituto Tecnológico Fiscomisional "Juan XXIII" ha tomado la iniciativa de integrarse al avance tecnológico haciendo que la educación mejore cada vez más en este cantón y provincia. Actualmente existe una red de datos

domestica para dar el servicio de INTERNET a docentes, empleados y alumnos. En toda la institución existen cuarenta computadoras distribuidas entre las oficinas y centro de cómputo.

El proveedor da el servicio de Internet para 10 computadoras las mismas que están distribuidas de la siguiente manera: ocho computadoras en el área administrativa al servicio de los empleados y dos computadores en la sala de profesores está al servicio de los cuarenta docentes. Los estudiantes del nivel secundario y superior tienen acceso al centro de cómputo equipado con 10 computadoras de acuerdo al horario. Cabe señalar que este centro de computo está conectado a Internet por medio de un enlace satelital que fue financiado para un año por medio del proyecto “Plan Amanecer” de la Conferencia Episcopal Ecuatoriana.

1.2 Estado del arte

Un 84% de los centros educativos españoles ha participado en proyectos de innovación y mejora en los últimos cuatro años por lo cual se puede decir que hay un interés notable por integrar las TIC en las actividades pedagógicas. Muchos centros de Educación Primaria y de Educación Secundaria han participado en programas de innovación y mejora de infraestructura física, equipos informáticos y equipos de comunicaciones, pero para en el acceso a contenidos digitales o la integración de las TIC a la vida diaria de los centros educativos no se dado en igual medida. Lo anteriormente mencionado ocurre también en otros continentes.

En nuestro país Ecuador la mayoría de instituciones educativas de nivel secundario también han participado en proyectos de mejora e innovación de equipos informáticos a tal punto que un gran número de centros educativos primarios y secundarios de las provincias orientales alejadas de la capital

tienen un promedio de 10 computadoras al servicio de estudiantes y profesores.

Pero el acceso al Internet por medio de una red local a nivel nacional pocos centros educativos lo tienen y peor aún poco o nada han hecho por incursionar hacia las TIC.

1.3 Descripción del problema y/o necesidad

Para brindar el servicio de Internet a empleados, docentes y alumnos el Instituto cuenta un servidor proxy configurado en Linux Centos versión 5.0 como puerta de enlace para el acceso al Internet con un ancho de banda de 128 Kbps compartidos con otros usuarios externos a la institución lo cual hace que se cree un cuello de botella desde el proxy hasta el proveedor obteniendo un servicio lento y costoso. Este servidor proxy está instalado en un PC normal con las siguientes características técnicas básicas: Procesador Pentium II de 1.8 GHz, 2GB de memoria RAM, disco duro de 80 GB y una tarjeta de red de 10/100 Mbps, el mismo que fue configurado por el proveedor para controlar los diez equipos que tienen acceso al Internet.

Esta red es también utilizada por el personal administrativo para llevar el control de matrículas, control de notas y control de asistencias.

Este proyecto surge de la necesidad que tiene el instituto de incursionar hacia las tecnologías de información y comunicaciones (TICs) que consta en el plan estratégico institucional y por lo tanto se cuenta el aval de la rectora del instituto para el desarrollo de este proyecto.

a) Problemas a ser resueltos

- La limitación de acceso al Internet de profesores y alumnos por la falta de diseño de una red inalámbrica que les permita conectarse desde cualquier lugar del campus institucional.

- Con el diseño de la Intranet y su posterior implantación se migraría de la red domestica a una infraestructura sólida de telecomunicaciones.

b) Necesidades a Satisfacer

- Tener a futuro los servicios de telecomunicaciones necesarios para fomentar la investigación tanto de docentes como de alumnos y garantizar a la comunidad del cantón y provincia una mejor educación integral de acorde a los avances tecnológicos actuales.

- Tener a futuro una biblioteca virtual que dé el servicio a los alumnos, docentes de la institución y comunidad en general.

1.4 Justificación del proyecto de tesis

Para realizar un buen diseño de la intranet e implantar un piloto con los servicios básicos de: Internet, Autenticación de Usuarios, Correo Electrónico y Servicio Web es necesario tener conocimientos amplios y actuales de algunos campos de la telemática.

Por otro lado para cumplir con la meta institucional anteriormente mencionada, mejorar el nivel académico y garantizar una educación de calidad que vaya en beneficio de la comunidad del cantón y provincia, es necesario realizar el diseño de la intranet y su posterior implantación para que brinde los servicios básicos anteriormente citados y sobre todo por medio del Servicio Web permitir a los padres de familia y en especial a los que viven en el extranjero poder

conocer el rendimiento académico de sus hijos y comunicarse por este mismo medio con las autoridades de la Institución educativa.

1.5 Objetivos

1.5.1 Objetivo General

Diseñar una intranet con los servicios de Internet, Correo electrónico y Web para el Instituto Tecnológico Fisco misional "Juan XXIII" del cantón Yantzaza provincia de Zamora Chinchipe.

1.5.2 Objetivos Específicos

- Diseñar la red física.
- Diseñar la configuración del servidor Proxy y Firewall
- Diseñar la configuración del servidor de autenticación de usuarios RADIUS
- Diseñar la configuración del servidor de DHCP
- Diseñar la configuración del servidor de DNS
- Diseñar la configuración del servidor de Correo Electrónico
- Diseñar la configuración del Servidor Web
- Realizar un análisis económico de la implementación del proyecto
- Implementar un prototipo del proyecto

1.6 Alcance del proyecto

- Configurar el servidor Proxy y Firewall que permita el acceso al Internet
- Configurar el servidor de autenticación de usuarios para el acceso al Internet
- Configurar el servidor de Correo Electrónico con algunas cuentas de usuarios para pruebas

- Configurar el Servidor Web para subir el prototipo de pagina web institucional
- Obtener un dominio institucional " www.juanxxiii.edu.ec" y configurar el servidor DNS para que resuelva este dominio.
- Configurar el servidor de DHCP que permita a los usuarios inalámbricos obtener una dirección IP automática para conectarse al Internet desde cualquier punto del campus académico.
- Realizar las pruebas de consistencia de todos estos servicios.
- Realizar el diseño de la red planificado para cinco años.

CAPITULO 2

MARCO TEORICO

2.1 Intranet

2.1.1 Definición

La Intranet no es más que la red local configurada con el protocolo estándar de Internet, el TCP/IP y con sus servicios fundamentales instalados: WWW, FTP y correo electrónico. Una Intranet es como una pequeña Internet, con la gestión de información y herramientas de acceso del World Wide Web juntos en una organización. Las aplicaciones que se usan en una Intranet, como el correo electrónico y los navegadores Web también se pueden usar en Internet. Se puede elegir conectar la Intranet a Internet, o se puede decidir mantener la Intranet local y no conectarla jamás a Internet.

2.1.2 Beneficios de una Intranet

En la actualidad cada vez es más importante para las pequeñas y medianas empresas la implementación de sus redes corporativas, ya que sin duda estas ofrecen una gran cantidad de beneficios entre los cuales se pueden citar:

Acceso a información actualizada.- Las personas que utilicen la Intranet tienen acceso a la información más actual, ya que generalmente la información se encuentra almacenada en uno o varios servidores (y no en forma distribuida, en la cual es difícil ubicar la última versión consistente de algún archivo), por lo que los cambios realizados en la información son actualizados para todos los "clientes" (dentro del modelo cliente servidor en el cual basa su funcionamiento las Intranets).

Escalabilidad.- Una Intranet bien diseñada permite irse acoplando a las necesidades de la empresa, es decir que se puede ir acoplando a los cambios y el crecimiento de la organización.

Ahorro.- Las Intranets constituyen en gran medida una reducción de los costos al incluir varios servicios en una única infraestructura, en la cual el costo de la comunicación se reduce notablemente en comparación con el esquema tradicional.

Acceso.- Las personas autorizadas pueden acceder a la información independientemente de su ubicación, ya que se pueden conectar mediante cualquier computador con salida al Internet.

Fácil localización y confidencialidad.- El uso de los navegadores Web facilita en gran medida la localización de documentos, permitiendo a su vez tener un control acerca del acceso a ellos. Además con la implementación de enlaces vinculados se puede acceder de forma directa a la información y/o páginas de interés fácilmente.

2.1.3 Componentes de una Intranet

Como todo sistema de información la intranet de una organización se compone de varios elementos íntimamente relacionados entre sí. Desde luego, no puede olvidar que la tecnología no es el componente más importante: es solo el soporte para que las personas desarrollen las actividades que tienen encomendadas y alcancen los objetivos previstos.

1. Información: el núcleo duro de la intranet es la información y documentación que genera la organización ya que es necesaria para su funcionamiento diario, para crear la memoria corporativa y para el desarrollo de la empresa.

2. Soporte Tecnológico: la intranet es productiva si se tiene acceso rápido y directo a la información. Cuanto más sencillo sea su diseño es mejor. Es muy importante también el soporte técnico que se le de a la intranet.

3. Servidores: en algún lugar estarán los servidores de información, que principalmente serán web, de correo y de aplicaciones brindando los servicios necesarios.

4. Seguridad: Lo normal es que los miembros de la empresa tengan acceso integrado tanto a intranet como a Internet. La protección de esta doble vía es para prevenir tanto acceso como salidas no autorizadas, esto se logra instalando un firewall o un "muro de fuego" que impide entrar y vigila las salidas.

A continuación se presenta un cuadro con algunos de los elementos de hardware y software que conforman una Intranet y se describen algunas alternativas que se pueden tomar en consideración:

Componentes	Opciones en el mercado
Navegadores Web	Netscape Navigator, Mozilla FIRE Fox, Internet Explorer
Maquinas Clientes	IBM, MAC, Compaq, etc.
Protocolo de red	TCP/IP
Sistemas operativos de Servidores	Unix, Solaris, Windows Server 2003, Aix, etc.
Hardware para servidores	SUN, DELL, IBM, HP, etc.
Topología de red física	Estrella, bus, anillo, etc.

Tabla 1. Componentes de una Intranet.

2.1.4 Servicios de una Intranet

Podemos clasificar los servicios de la Intranet en dos tipos:

Servicios de usuario que suministran recursos y aplicaciones al usuario final, los servicios de red que permiten interconectar la intranet.

Servicios de Usuario.

Facilidad de crear, compartir y administrar la información.

La intranet facilita la ubicación y administración de contenidos, asegurando que todo aquel que cuente con derechos de acceso estará en posesión de la información más reciente. Pueden crearse documentos HTML usando intuitivas interfaces, hiperenlaces multimedia (imágenes, videos y sonidos) y objetos incrustados que permiten integrar y personalizar contenidos en línea enriquecidos e interactivos.

Navegación.

La intranet permite la búsqueda de cualquier recurso o información que se encuentre en la red. Por medio de los Links es posible tener acceso a toda la información que esté expuesta en el sitio web.

Comunicación.

El control de acceso y la seguridad permiten que el correo electrónico sea privado, así como la autentificación de acceso a Internet. Los usuarios pueden examinar direcciones de correo electrónico y números de teléfono usando una sencilla interfaz de agenda de direcciones.

Acceso a bases de datos y aplicaciones.

El acceso a bases de datos y aplicaciones ya existentes se realiza fácilmente con una interfaz amigable al usuario. Las aplicaciones pueden estar asociadas con el contenido y pueden desplegarse de forma transparente tanto en Internet como en la intranet. El acceso a las bases de datos y aplicaciones en un entorno web se considera como un servicio más de la Intranet.

Servicios de Red.

Directorio.

Los servicios de directorio gestionan la información permitiendo a ciertos usuarios administrar su propia información depositando, modificando o eliminando su información. En el ámbito académico los usuarios que suelen tener estos privilegios son los docentes y los estudiantes en cambio tienen solo acceso a esta información.

Seguridad

Los servicios de seguridad de la intranet ofrecen métodos para proteger la información y los recursos contra los usuarios no autorizados. Aplicaciones, páginas Web, directorios y bases de datos están sujetos a un control de acceso, que se gestiona de forma centralizada.

Administración.

Permite administrar los servidores se lo podría realizar en forma local o desde cualquier punto de la intranet o Internet usando un protocolo de conexión

remota. De igual manera la administración de contenido del sitio web es posible realizarlo de manera local o también de forma remota.

2.1.5 Direccionamiento IP

Las direcciones IP permiten identificar de manera única a cada computador o a cualquier dispositivo fuente o destino de los datos que atraviesan una red IP.

Estas direcciones pueden ser asignadas de forma estática o dinámica de acuerdo a las características del equipo, por ejemplo la dirección IP de un servidor de impresión se recomienda ser configurada como estática con el fin de no perder valioso tiempo en procesamiento y búsqueda del equipo.

Las direcciones IP son una combinación de un número entero de 32 bits que permiten identificar tanto el equipo como la red a la que pertenece. A fin de lograr este propósito toda dirección IP tiene asociada una máscara de subred, la cual tiene 32 bits de longitud. Para facilitar su representación las direcciones IP se simbolizan en notación decimal punto (desde 0 a 255), divididos en 4 octetos, como se muestra en el ejemplo:

Figura 1. Ejemplo de notación IP.

Inicialmente en la Internet se trabajaba con un esquema preconcebido basado en clases, que permitían asignar direcciones IP a las organizaciones pequeñas, medianas y grandes, de acuerdo al número de host que soportaban, como se muestra a continuación en el siguiente cuadro:

Clases de Direcciones IP					
Clase	Rango del 1er octeto (decimal)	Bit del primer octeto (bits de color verde no cambian)	Partes de Red (N) y Host (H) de la dirección	Máscara de subred por defecto	Número de posibles Hosts por red
A	1-126	00000000 – 01111111	N.H.H.H	255.0.0.0	2^{7} o 128 redes y 2^(24-2) 16777214 hosts por red
B	128-191	10000000 – 10111111	N.N.H.H	255.255.0.0	2^{14} o 16384 redes y $2^{(16-2)}$ 65534 hosts por red
C	192-223	11000000 – 11011111	N.N.N.H	255.255.255.0	2^{21} o 2097150 redes y $2^{(8-2)}$ 254 hosts por red
D	224-239	11100000 – 11101111	Multicast		
E	240-247	11110000 – 11111111	Experimental		

Tabla 2. Clases de direcciones IP

Sin embargo con el auge del Internet de las direcciones IP disponibles comenzaron a quedarse cortas para la expectativa de demanda a nivel mundial, por tal razón en la actualidad se han desarrollado metodologías que permiten a los diseñadores de red utilizar el concepto de direcciones IP públicas y privadas.

Direcciones IP Públicas: Son las direcciones IP válidas reconocidas en la Internet para el intercambio de información y sirven para identificar a un equipo en particular y pueda ser visto por otro conectado a Internet.

Direcciones IP Privadas: Se utilizan para la identificación de los equipos dentro de la red interna de la organización. Los computadores con una dirección privada requieren de un servidor Proxy para conectarse a Internet, que realiza las funciones de NAT (Network Address Traslation) que permite la traducción de dirección privada a pública y viceversa. El rango de direcciones IP privadas son:

• 10.0.0.0 – 10.255.255.255 (10.0.0.0 /8)

• 172.16.0.0 – 172.31.255.255 (172.16.0.0 /12)
• 192.168.0.0 – 192.168.255.255 (192.168.0.0 /16)

2.1.6 Medidas de seguridad

Las medidas básicas de seguridad se incluyen en los firewalls y en la identificación de usuarios. El diseño del sistema de seguridad de información en las redes corporativas se basa en la aplicación de reglas a nivel firewalls.

2.1.7 Intranet Educativa

Los centros educativos disponen de intranet, pero no se suele aprovechar todo su potencial educativo. Un componente esencial en la intranet será la instalación de un ordenador servidor, que será mantenido por el administrador de la red. Los beneficios principales de una intranet educativa son los siguientes:

1. Capacidad de compartir recursos (impresoras, escáner…) y la posibilidad de conexión a Internet.

2. Alojamiento de páginas web, tanto la del centro educativo como de estudiantes o profesores, que pueden consultarse con los navegadores desde cualquier PC de la Intranet o desde cualquier PC externo conectado a Internet.

3. Servicios de almacenamiento de información (Servicios de directorios). Espacios de disco virtual a los que se puede acceder para guardar y recuperar información desde los PCs del centro educativo y también desde cualquier equipo externo conectado a Internet.

4. Servicio de e-mail, que puede incluir diversas funcionalidades (buzón de correo electrónico y servicio de web mail)

6. Promocionar la institución manteniendo información actualizada y de interés para la comunidad local y sociedad en general. Actuar como fuente de información de otras entidades educativas o privadas.

2.1.8 Arquitectura básica para una Intranet Educativa

El esquema básico de una Intranet para el sector educativo puede verse como indica la siguiente figura:

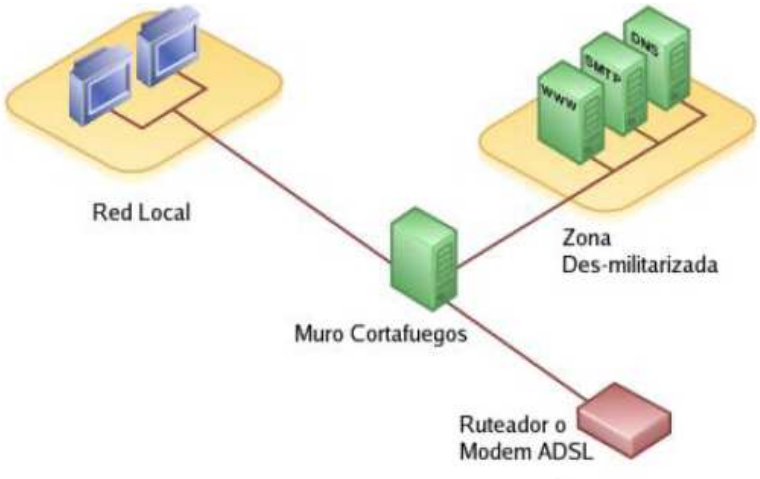


Figura 2. Arquitectura básica para una intranet educativa

Este esquema es recomendable ya que la mayoría de instituciones académicas cuentan con un sistema académico y una base de datos que no sería prudente que este expuesta directamente a los usuarios externos de Internet. Según el gráfico al tener una zona desmilitarizada donde se encuentran los servidores como www, Correo y DNS se fortalece la seguridad de la red local ya que los usuarios de Internet solo tendrían acceso a los servicios que ofrece la zona desmilitarizada (DMZ).

2.2 Cableado Estructurado

2.2.1 Cableado Horizontal

El sistema de cableado horizontal se extiende desde el área de trabajo hasta el cuarto de equipos, puede tener una longitud máxima de 90 metros y consta de los siguientes elementos: el cableado horizontal, los puntos de conexión al sistema en el área de trabajo, las terminaciones del cable tanto en el Jack como en el patch panel y las interconexiones horizontales desde las salidas del patch panel hacia los equipos de interconexión en el cuarto de equipos.

Existen tres tipos de medios de transmisión permitidos para la implementación del cableado horizontal:

- Cable UTP 100-ohm, 4-pares
- Cable STP 150-ohm, 2-pares
- Fibra óptica multimodal 62.5/125-µm, 2 fibras

Se recomienda construir ductería especial para el cableado horizontal o en su defecto la utilización de canaleta decorativa para proteger este subsistema.

2.2.2 Cableado Vertical

El subsistema de cableado vertical o backbone se encarga de la interconexión entre los racks de telecomunicaciones. Este subsistema incluye: cableado vertical, que básicamente son conexiones entre pisos de un mismo edificio o entre edificios, las interconexiones principales e intermedias. El siguiente cuadro muestra los tipos de medios de transmisión utilizados para el cableado vertical:

Tipo de Cable	Distancias máximas
100 ohm UTP (24 or 22 AWG)	800 metros (Voz)
150 ohm STP	90 metros (Datos)
Fibra Multimodo 62.5/125 µm	2000 metros
Fibra Multimodo 62.5/125 µm	3000 metros

Tabla 3. Tipos de conductores utilizados en el cableado vertical

2.2.3 Cuarto de Equipos

El cuarto de equipos es un área centralizada dentro del edificio de uso específico para equipos de telecomunicaciones (central telefónica, servidores, etc.), similar al cuarto de telecomunicaciones, difiere de éste en cuanto al costo, tamaño, propósito y/o complejidad de los equipos que contienen.

2.2.4 Cuarto de Telecomunicaciones

El cuarto de telecomunicaciones es un área exclusiva dentro del edificio que alberga equipos asociados con el sistema de cableado estructurado de telecomunicaciones, incluyendo las terminaciones mecánicas de cable y cableado de interconexión asociado al cableado horizontal y vertical.

2.2.5 Área de trabajo

El área de trabajo comprende desde la toma de telecomunicaciones al final del sistema de cableado horizontal hasta las estaciones de trabajo o equipos de red.

Los componentes del área de trabajo pueden ser equipos como: computadoras, teléfonos, impresoras, entre otros.

2.2.6 Estandarización del cableado estructurado

A continuación se muestra un cuadro con los diferentes estándares que son recomendados para la correcta implementación del cableado estructurado:

Estandar	Descripción
ANSI/TIA/EIA 568 B	Cableado de Telecomuniciones en Edificios Comerciales. Se encuentra dividido en tres partes: ANSI/TIA/EIA 568 B.1.- Requisitos Generales. ANSI/TIA/EIA 568 B.2.- Componentes para Cableado de UTP de 100 ohm. ANSI/TIA/EIA 568 B.3.- Norma para Componentes de cableado con Fibra Optica
ANSI/TIA/EIA 568 A	Rutas y espacios de telecomunicaciones en edificios comerciales

Tabla 4. Estándares ANSI/TIA/EIA recomendados para del cableado estructurado

Estándares EIA/TIA 568

La Asociación de la Industria de las Telecomunicaciones (TIA) y la Asociación de Industrias de Electrónica (EIA) son asociaciones industriales que desarrollan y publican una serie de estándares sobre el cableado estructurado para voz y datos para las redes LAN. Esta norma rige la instalación de Cableado de Telecomunicaciones en Edificios Comerciales.

EIA/TIA especifica el uso de un conector RJ-45 para cables UTP. Las letras RJ significan “registered jack”, y el número 45 se refiere a una secuencia específica de cableado. El conector transparente RJ-45 muestra ocho hilos de distintos colores. Cuatro de estos hilos conducen el voltaje y se consideran “tip” (punta) (T1 a T4). Los otros cuatro hilos están conectados a tierra y se llaman “ring” (anillo) (R1 a R4). Tip y ring son términos que surgieron a comienzos de

la era de la telefonía. Hoy, estos términos se refieren al hilo positivo y negativo de un par. Los hilos del primer par de un cable o conector se llaman T1 y R1. El segundo par son T2 y R2, y así sucesivamente.

Para que la electricidad fluya entre el conector y el jack, el orden de los hilos debe seguir el código de colores T568A, o T568B recomendado en los estándares EIA/TIA-568-B.1.

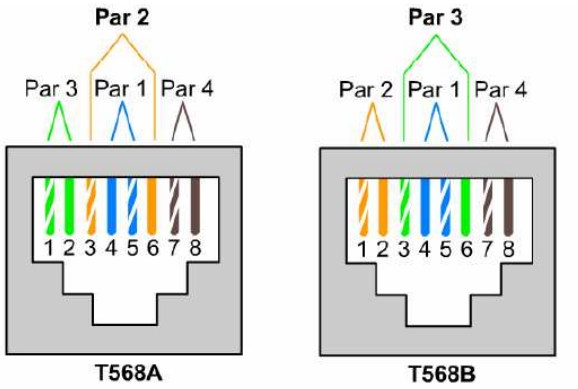


Figura 3. Configuración de pines en conectores RJ45 según la norma 568A/B.

Si los dos conectores de un cable RJ-45 se colocan uno al lado del otro, con la misma orientación, podrán verse en cada uno los hilos de color. Si el orden de los hilos de color es el mismo en cada extremo, entonces el cable es de conexión directa, como se observa en la siguiente Figura:

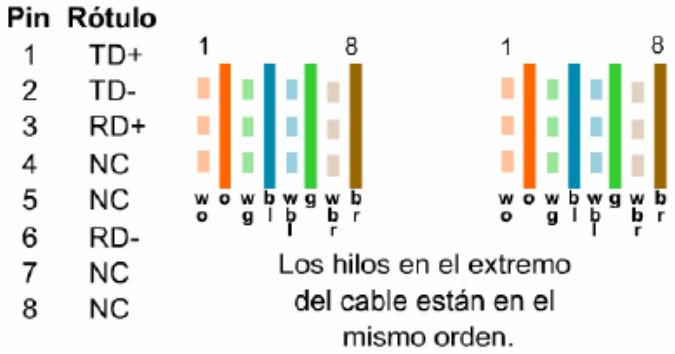


Figura 4. Conexión directa de pines en conectores RJ45

En un cable de conexión cruzada, los conectores RJ-45 de ambos extremos muestran que algunos hilos de un extremo del cable están cruzados a un pin diferente en el otro extremo del cable. En la siguiente figura se muestra que los pins 1 y 2 de un conector se conectan respectivamente a los pins 3 y 6 de otro.

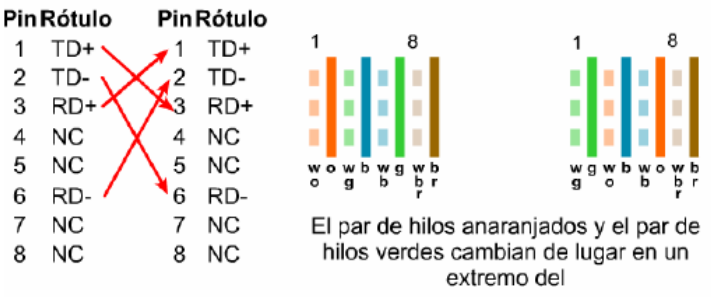


Figura 5. Conexión cruzada de pines en conectores RJ45

ANSI/TIA/EIA 568 B.1

Este estándar detalla la información necesaria para el planeamiento, instalación y verificación de cableado estructurado para edificios comerciales estableciendo sus parámetros de calidad.

ANSI/TIA/EIA 568 B.2

Estándar que especifica los requisitos mínimos para los componentes reconocidos de cable UTP balanceado de 100 ohm, usados en el cableado de telecomunicaciones en edificios comerciales. Estos componentes pueden ser: cable, conectores, hardware de conexión, cordones y jumpers. Se incluyen en el estándar los requisitos de los parámetros de transmisión de componentes y de los equipos de pruebas usados para la verificación del cableado instalado.

Las categorías de cables UTP reconocidas por el estándar son:

Categoría	Descripción
Categoría 5:	Hasta 100 Mbps, Se utiliza en las comunicaciones de tipo LAN. La atenuación de este cable depende de la velocidad
Categoría 5e:	Cable UTP de 100 ohm y sus accesorios de conexión. Ancho de banda hasta 200 MHz. Se especifica para esta categoría parámetros de conexión más exigentes que el de categoría 5.
Categoría 6:	Cable UTP de 100 ohm y sus accesorios de conexión. Ancho de banda hasta 200 MHz. Se especifica para esta categoría parámetros de transmisión de hasta los 250 MHz. Alcanza velocidades de 1 Gbps.

Tabla 5. Categorías cable UTP reconocidos por la norma ANSI/EIA/TIA 568 B

2.3 Redes de Información

Las redes informáticas son un conjunto de computadoras y dispositivos asociados configurados para compartir recursos informáticos con la ayuda de interfaces especiales, protocolos y dispositivos de hardware. La finalidad de una red es conservar los recursos y permitir la comunicación y la distribución electrónica de datos.

Las redes informáticas se clasifican de acuerdo a la tecnología de transmisión utilizada y de acuerdo a la cobertura o alcance geográfico.

Desde el punto de vista de la tecnología de transmisión se tiene la siguiente clasificación:

- Redes de Difusión.- Tienen un solo canal de comunicación compartido por todos los equipos de la red.
- Redes punto a punto.- Consiste en muchas conexiones entre pares individuales de maquinas, por lo tanto la información viaje desde su origen al destino pasando por una o más máquinas intermedias.

Desde el punto de vista de la cobertura se pueden clasificar de acuerdo al siguiente cuadro:

Red	Alcance geográfico	Descripción
Red de área local (LAN)	10 m – 1 Km	Soporte de hasta 1000 nodos Topología bien definida
Red de área metropolitana (MAN)	1 Km – 10 Km	De 100 a 1000 nodos Cobertura a nivel de ciudad Topología irregular Enrutamiento dinámico
Red de área extensa (WAN)	10 Km – 10000 Km	Entre 1000 – 1 millón de nodos Conecta redes entre países, regiones y continentes Topología irregular Enrutamiento dinámico
Internet	Red de alcance a nivel mundial	100 millones de nodos

Tabla 6. Clasificación de las Redes de Información

2.3.1 Redes LAN

Las redes LAN permiten la conectividad de equipos computacionales dentro de una área limitada físicamente a un piso, un edificio o a un entorno de pocos kilómetros. Los medios de transmisión que utiliza pueden ser cable UTP, Coaxial o fibra óptica, que les permite operar a velocidades entre 10, 100 y

hasta 1000 Mbps. Las tecnologías utilizadas para la implementación de este tipo de redes se han desarrollado a fin de ofrecer hoy en día poco retardo y bajo tasa de errores.

Dentro de los estándares para la implementación de redes LAN el más utilizado en es el estándar 802.3 o mejor conocido como Ethernet.

Estándar Ethernet

Ethernet ha sido la tecnología LAN de mayor éxito, en gran medida, debido a la simplicidad de su implementación frente a otras tecnologías y a su flexibilidad, ya que ha evolucionado para satisfacer las necesidades de las redes informáticas. Ethernet nació como la idea de utilizar un medio de transmisión compartido denominado bus, que permita la comunicación entre todos los dispositivos conectados a él, más sin embargo el bajo rendimiento y alta tasa de colisiones obligaron a que los diseñadores de esta tecnología involucren el concepto de la topología tipo estrella, en la cada estación es conectada directamente a dispositivo central, el que se encarga de realizar el proceso de comunicación de los mensajes, bien sea en modo de difusión, en el que la transmisión de la información se retransmite hacia todos los demás dispositivos conectados al nodo
central; o mediante un dispositivo de conmutación de tramas, que básicamente almacena las tramas en un buffer interno, analiza la dirección destino y retransmite la información solo por el enlace de salida hacia el destino.

Estándar Fast Ethernet

Su objetivo principal es incrementar la velocidad de 10Base-T (10 Mbps), conservando el sistema de cableado, el método MAC y los formatos de trama. Fast Ethernet trabaja con cable UTP o fibra óptica. Existe también como opción

el par trenzado apantallado STP. A continuación se presenta un cuadro que ilustra las principales características de las diferentes variantes de tecnologías Fast Ethernet:

	100Base TX	100Base – T4	100Base - FX
Longitud de segmento máxima	100 m	100 m	412 m
Tipo de cable	UTP cat 5 STP, a dos pares de hilos	UTP cat3, a 4 pares de hilos	Fibra multimodo 62,5/125 µm
Tipo de conector	RJ-45	RJ-45	SC, MIC o ST

Tabla 7. Características principales de 100BaseTX, 100Base-T4 y 100Base-FX.

2.3.2 Redes LAN Inalámbricas (WLAN)

Este tipo de redes basan su funcionamiento en Wi-Fi (Wireless-Fidelity) que corresponde al estándar 802.11 de la IEEE. Las WLANs permiten extender el alcance de las redes LAN hacia lugares en los cuales se dificulta en gran medida el acceso mediante el cableado estructurado, permitiendo además la movilidad de los usuarios y traslado de los equipos de la red.

Este tipo de redes realizan el proceso de comunicación utilizando un medio de transmisión no guiado como el espectro radioeléctrico mediante el uso de antenas que emiten ondas electromagnéticas.

Estándares IEEE 802.11

Los esquemas de transmisión en el estándar 802.11 que son: Infrarrojos y Radio Frecuencia utilizando dos técnicas de espectro extendido, que pueden

ser de secuencia directa DSSS: Direct Sequence Spread Spectrum, o de salto de frecuencia FHSS: Frecuency Hopping Spread Spectrum (ver Apéndice 1).

El estándar original fue creado en el año de 1997 y soportaba velocidades de hasta 2 Mbps en la banda de frecuencia de 2.4 GHz, con el impacto positivo de esta nueva tecnología en el mercado, los fabricantes desarrollaron productos que funcionaban a mejores velocidades, por lo que la IEEE (ver Apéndice 1) realizó una revisión de este estándar, y en octubre de 1999 publicaron los estándares 802.11ª y 802.11b.

El estándar IEEE 802.11b trabaja en la banda de frecuencia 2.4 GHz, utiliza DSSS (Espectro expandido por secuencia directa) como técnica de espectro expandido, y alcanza velocidades de hasta 11 Mbps, mientras que IEEE 802.11ª soporta velocidades hasta de 54 Mbps, trabaja en la frecuencia de 5 GHz y emplea como esquema de transmisión OFDM (Orthogonal Frequency Division Multiplexing) (ver Apéndice 1).

Al trabajar en frecuencias diferentes estos dos estándares son incompatibles entre sí, por lo cual IEEE tomó las mejores características de cada uno de éstos para desarrollar el estándar 802.11g.

El estándar IEEE 802.11g en la actualidad es el más utilizado, trabaja en la banda de los 2.4 GHz, por lo que es compatible con 802.11b, al igual que 802.11ª emplea OFDM como esquema de transmisión y alcanza velocidades de hasta 54 Mbps.

2.4 Metodología de diseño

La metodología que a continuación se describe es el “metodología de diseño de redes CISCO ”, se escogió este método por las siguientes razones:

- Es el más conocido y utilizado en la actualidad
- Las universidades y centros particulares tienen academias Cisco que permiten realizar especializaciones en este campo.
- Es aplicado a pequeñas, medianas y grandes redes de datos y telecomunicaciones
- Como ingeniero en Informática es mucho más sencillo entender este método porque tiene similitud con el diseño de sistemas, donde en resumen se parte de una recopilación de requerimientos, se analizan los requerimientos y se diseña el sistema, este último paso sería equivalente al diseño de la red.

Usando este método y para realizar un diseño efectivo de la red LAN y que satisfaga las necesidades de los usuarios se debe diseñar e implementar siguiendo una serie de pasos sistemáticos que incluyen lo siguiente:

1. Recolectar los requerimientos y expectativas de los usuarios.
2. Analizar los requerimientos
3. Diseñar la estructura de las capas 1, 2 y 3 de la red LAN (Topología de la red)
4. Documentación de la implementación física y lógica de la red.

2.4.1 Recopilación de requerimientos y expectativas de los usuarios

El primer paso en el diseño de una red debe ser la recopilación de información confiable de la estructura organizacional de la empresa. Esta información debe incluir tanto la historia de la empresa como su estado actual y su proyección futura, sus políticas de operación y sus procedimientos de administración. Esta información debe ser brindada por las personas que utilizan la red o la van a utilizar ya que son ellas las que saben realmente sus necesidades reales. Este

es un punto clave en el desarrollo del diseño y uno de los más difíciles de obtener.

Para empezar es bueno tener un perfil técnico de las personas que utilizarán la red, es decir que tipos de conocimientos tienen ellos.

- ¿Qué usuarios van a utilizar la red? (Serán administradores, contadores, programadores etc.)
- ¿Cuáles son sus habilidades respecto a computadoras y sus aplicaciones? (saben manejar computadoras, se encuentran actualizados en sus programas y aplicaciones).

Al lograr contestar estas preguntas se tendrá una idea de cuánto entrenamiento habrá que dar a los nuevos usuarios y que tanto soporte y mantenimiento requerirá la red. La idea de esta etapa en el diseño de la red es identificar los posibles problemas desde el inicio.

También se debe determinar si existen políticas de la empresa en el lugar o departamento.

- ¿Existen o existirán operaciones críticas?
- ¿Qué tipos de protocolos son permitidos en la red?
- ¿Solo ciertas máquinas tendrán servicio?

En estos aspectos hay que tener en cuenta que información crítica u operaciones críticas son las claves de los negocios y el acceso a ellas es importante en el desarrollo de los mismos.

Luego se debería determinar quien tiene la autoridad de direccionar, nombrar, diseñar topologías y configuraciones. Ya que muchas veces una compañía tiene un departamento de administración informática.

También se debe tomar en cuenta que los recursos de una empresa afectarán dramáticamente la implementación de una red. Estos recursos pueden ser:

- Hardware y Software
- Recurso Humano

En cuanto al Hardware y software se debe preguntar lo siguiente:

- ¿Debe ser identificada cualquier necesidad de Hardware y Software actuales y futuras?
- ¿Cómo se encuentran compartidos los recursos?
- ¿Qué tipo de recursos tiene disponible la organización?

Respondiendo cada una de estas preguntas ayudaran al diseñador a estimar los costos y desarrollar un presupuesto para la nueva red. Si se está mejorando, perfeccionando o ampliando una red actual se debe tener muy en cuenta los rendimientos de esa red de manera que sean compatibles con la ampliación, mejora o perfeccionamiento.

2.4.2 Análisis de Requerimientos

El siguiente paso en el diseño de una red es analizar los requerimientos de la red y de los usuarios obtenidos en el paso anterior. Los requerimientos de los usuarios de una red suelen variar constantemente. Por ejemplo a medida que más aplicaciones de voz y video basadas en red aumentan se necesita un mayor ancho de banda.

Por lo tanto se debe evaluar los requerimientos de los usuarios, ya que una red que no brinde información pronta y confiable a sus usuarios es de poca utilidad. Por lo tanto debe tomarse el tiempo para asegurar que los requerimientos de información de la organización y sus empleados concuerden.

Se debe llevar a cabo un análisis detallado de las necesidades actuales y de los objetivos técnicos de la organización. Para lograrlo se necesita responder preguntas como las siguientes:

- ¿Qué aplicaciones serán implementadas?
- ¿Qué nuevas redes serán acezadas?
- ¿Qué nivel de confiabilidad debe tener red?
- ¿Cuáles serían usuarios finales de la red?

Disponibilidad y tráfico de red

La disponibilidad de la red mide su utilidad, muchas cosas pueden afectar la disponibilidad incluyendo las siguientes:

En este punto se analiza la utilidad de la red tomando en cuenta aspectos como:

- Rendimiento de procesamiento
- Tiempo de respuesta

Los clientes tienen una definición diferente de la disponibilidad. Por ejemplo la mayoría quisiera poder transmitir voz y video sin problemas, pero esto significaría más recursos económicos. Una de las tareas del diseñador es buscar proveer la mejor disponibilidad con el menor costo.
Se debe determinar el tráfico de la red antes de diseñar la arquitectura y adquirir el hardware. Por lo tanto se necesita estimar el tamaño de los archivos en bytes por segundo que necesitan ser transmitidos por la red.

Requerimientos finales de la red

Una vez analizados los requerimientos iníciales es necesario definir la lista de requerimientos finales que deberá satisfacer la red de datos.

2.4.3 Diseño de la topología de red (Capa 1, 2 y 3)

Una vez claros los requerimientos de la red, el siguiente paso es decidir una topología de red general que los requerimientos del usuario. El modelo propuesto aquí es el de la topología de estrella extendida. Es preciso notar que esta topología utiliza la lógica Ethernet 802.3 (relaciona los medios cableados con sus velocidades de transmisión), y la técnica CSMA/CD (Acceso Múltiple Sensible a la Portadora con Detección de Colisiones). Estas topología es la más estable y dominante en la Industria.

Figura 6 Topología en estrella extendida

Diseño de la Capa 1

La capa física controla la forma en la que la información es transmitida desde el nodo fuente al nodo destino, por lo tanto el tipo de medio y la topología que se elija son muy importantes para determinar cuanta información y a qué velocidad puede viajar por la red.

Cableado

El cableado físico es uno de los componentes más importantes a considerar cuando diseñamos una red. Se toma en cuenta el tipo de cable que se va a usar y toda la estructura del cableado. Usualmente se utiliza UTP categoría 5 o fibra óptica junto con todos los estándares EIA/TIA 568 que son para el tendido y conexiones de medio físico.

La mayor parte de los problemas de la red suelen darse en la capa 1. Ya sea que se esté diseñando una nueva red o actualizando una ya existente es mejor utilizar fibra óptica o UTP categoría 6 en el cableado vertical y UTP categoría 5 en el cableado horizontal.

La norma estándar EIA/TIA 568 específica que cualquier equipo conectado a la red debe estar enlazado a la localización central con cableado horizontal y a una distancia máxima de 100 metros usando el cable UTP categoría 5 como muestra la siguiente figura:

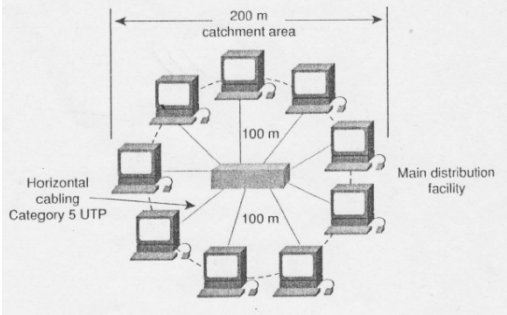


Figura 7. Cableado Horizontal

Característica	10 Base T	10 Base FL	100 Base TX	100 Base FX
Índice de Transferencia	10 Mbps	10 Mbps	100 Mbps	100 Mbps
Método de Señalización	Banda Base	Banda Base	Banda Base	Banda Base
Tipo de Medio	Categoría 5	Fibra óptica	Categoría 5	Fibra Multimodo
Longitud Máxima	100 metros	2000 metros	100 metros	400 metros

Tabla 7. Características de cable

Topología de estrella extendida

Cuando los nodos de una red están distantes que superan los 100 metros se debe tener varios armarios de distribución de cableado y así crear varias áreas de captación. Estos armarios se llaman centros de distribución intermedia y se les conoce por sus siglas en ingles (IDF).

El estándar EIA/TIA 568-A especifica que los IDF, deben estar conectados con el armario de cableado principal (conocido por sus siglas en ingles MDF), mediante cableado vertical que generalmente es fibra óptica para cubrir distancias mayores a 100 metros o UTP categoría 6 para distancias menores. A continuación se presenta un esquema de cableado vertical

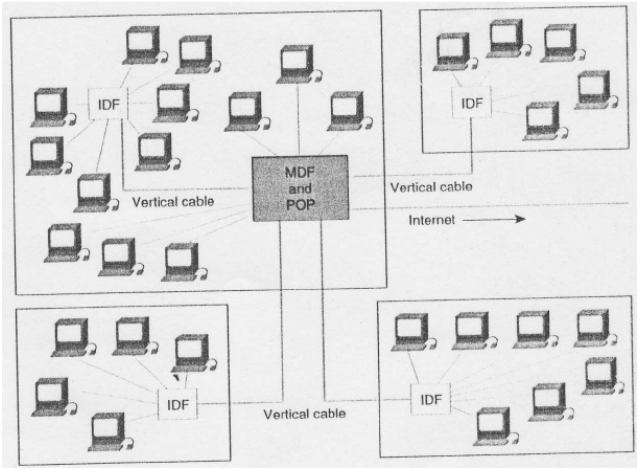


Figura 8. Cableado Vertical

Para conectar los IDFs con el MDF se utiliza el estándar Fast Ethernet que para cable UTP es 100 Base TX y para fibra óptica es 100 Base FX.

Diagrama lógico de la red

El diagrama lógico es el modelo de la topología de la red sin detalles de la ruta del cableado. Este diagrama es una visión instantánea de la red LAN y es útil para la solución de problemas y expansión en el futuro. Los elementos de este diagrama incluyen:

- La ubicación exacta de los armarios IDF e MDF.

- El tipo y la cantidad de cableado usado para la interconexión de los IDFs con el MDF, junto con la cantidad de cables de redundancia disponibles para aumentar el ancho de banda entre los armarios de cableado.

A continuación se presenta un diagrama lógico general de una red.

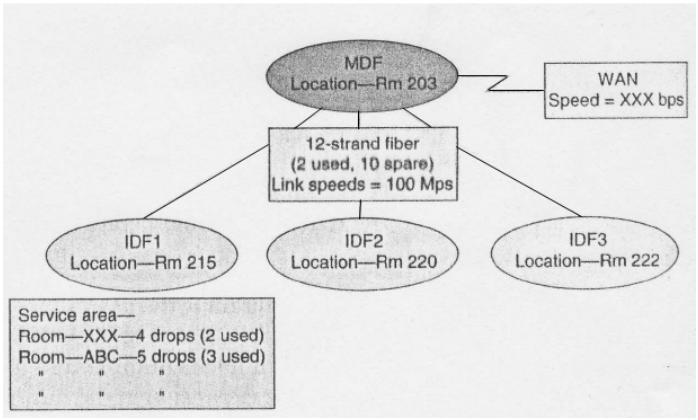
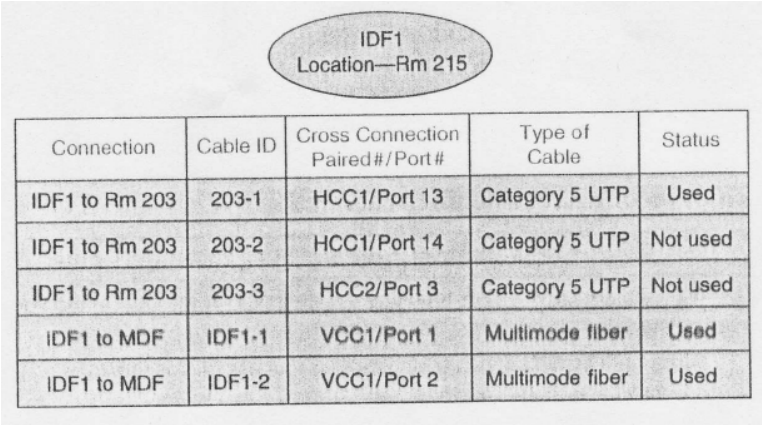


Figura 9. Diagrama lógico de la red

- La documentación detallada de todos los tendidos de cable, con los números de identificación y a que puerto del patch panel van. Se debe indicar también si es horizontal cruzado o vertical cruzado ya que esto nos ayudaría a verificar la continuidad de los cables y facilitar las tareas de mantenimiento de la red.



Connection	Cable ID	Cross Connection Paired#/Port#	Type of Cable	Status
IDF1 to Rm 203	203-1	HCC1/Port 13	Category 5 UTP	Used
IDF1 to Rm 203	203-2	HCC1/Port 14	Category 5 UTP	Not used
IDF1 to Rm 203	203-3	HCC2/Port 3	Category 5 UTP	Not used
IDF1 to MDF	IDF1-1	VCC1/Port 1	Multimode fiber	Used
IDF1 to MDF	IDF1-2	VCC1/Port 2	Multimode fiber	Used

Tabla 8. Documentación del cableado.

Diseño de la Capa 2

El propósito de los dispositivos de capa 2 es proporcionar el control de flujo, detección y corrección de errores para reducir la congestión en la red. Los dos dispositivos más comunes de capa 2 son los Hubs y switchs que determinan el tamaño de los dominios de colisión. Mediante el uso de switchs se puede micro segmentar la red, eliminando así las colisiones y reducir el tamaño de los dominios de colisión.

La distribución de switchs entre los los IDFs y MDF permite distribuir mejor el tráfico pesado usando generalmente la fibra óptica como medio de conexión, mientras que las conexiones desde los IDFs hasta los hosts no requieren mucha capacidad y por lo tanto se podría usar el cable UTP cat 5, considerando que no debe ser mayor a 100 metros para garantizar índices de tranasferencia de 10 o 100 Mbps. Los switchs asimétricos que permiten tener puertos de distintas velocidades en un mismo switch, por tanto la tarea siguiente en el diseño será determinar la cantidad exacta de puertos de 10 y 100 Mbps necesarios entre centros de distribución principal e intermedia.

Incremento de ancho de banda a nivel de capa 2.

Una parte fundamental del diseño de redes es considerar que la red crecerá y posiblemente a un 100% de su capacidad. Esto quiere decir que debemos dimensionar la red al doble para que quede prevista toda la infraestructura necesaria para ese incremento a “n” años según las especificaciones del usuario.

A nivel de capa 2 este incremento implicará en que los tendidos verticales que no están usados deberán conectarse a puertos no usados del switch, por lo tanto hay que considerar que el switch debe tener puertos libres o la posibilidad de instalarle módulos de expansión con ese tipo de puertos (tomar en cuenta esto al momento de escoger un modelo de switch).

Diseño de la Capa 3

Conocida como la capa de red, los dispositivos como los routers se usan en esta capa. Estos segmentos de capa 3 se comunican por medio del direccionamiento IP. Los routers también permiten la conectividad con la red de área extensa WAN como lo es el Internet.

El router determina el flujo de tráfico entre los segmentos de red física manejados por direccionamiento IP, este dispositivo es uno de los más poderosos en las topologías de red. A continuación se representa esta estructura a través de la siguiente figura:

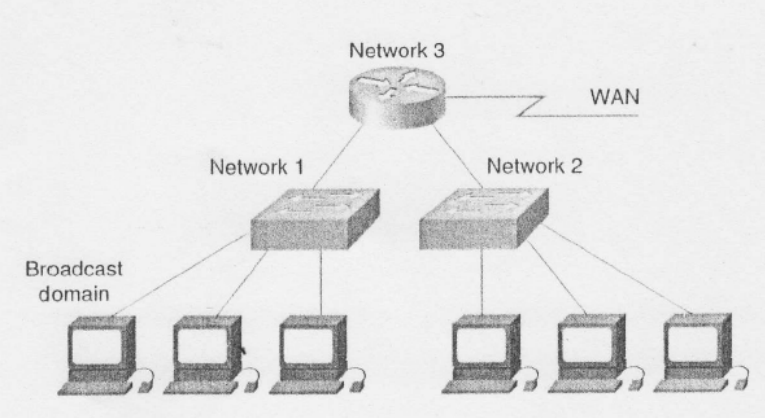


Figura 10. Segmentación de red a nivel de capa 3

Un ruteador se encarga del reenvió de paquetes según la dirección IP, pero no del reenvió de paquetes ARP (Protocolo de resolución de direcciones). Ósea se convierte en el punto de entrada y salida de un dominio de difusión para que los paquetes no se dirijan a otro segmento de red.

Por tal razón primero se debe identificar cuáles son los segmentos de red y que direccionamiento IP utilizarían cada uno de estos segmentos de red.

Como se observa en la siguiente figura un router crea un esquema de direcciones de los segmentos de red para no crear cuellos de botella con direcciones desconocidas como ocurriría con los Switches y Hubs.

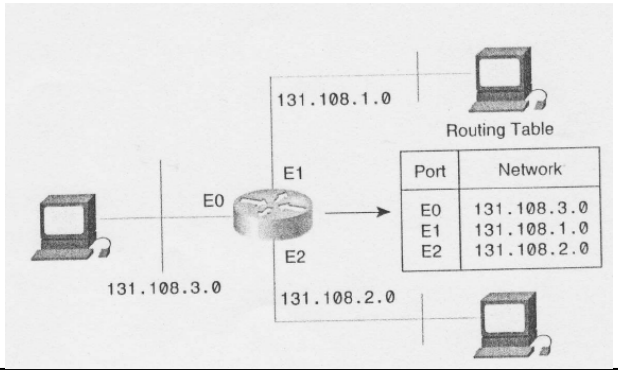


Figura 11. Ejemplo de una red escalable

Los routers brindan escalabilidad porque ellos pueden servir como firewalls para filtrar difusiones, además por su función de capa de red los routers pueden proveer una gran escalabilidad al dividir redes en subredes.

2.4.4 Documentación de la implementación lógica de la red.

Se debe desarrollar el esquema de direccionamiento IP para la red tomando en cuenta los dispositivos que formarán parte de la red como si indica en la siguiente tabla:

Direcciones lógicas	Unidades de red físicas
x.x.x.1 hasta x.x.x.10	Router, LAN, and WAN ports
x.x.x.11 hasta x.x.x.20	LAN switches
x.x.x.21 hasta x.x.x.30	Servidores de la empresa
x.x.x.31 hasta x.x.x.80	Servidores de grupos de trabajo
x.x.x.81 hasta x.x.x.254	Equipos

Tabla 9. Direccionamiento lógico de la red

CAPITULO 3

DISEÑO DE LA INTRANET

3.1 Recopilación de requerimientos

Historia

Esta institución fue creada el 10 de diciembre de 1971 con el nivel primario solo para mujeres con un total de 300 alumnas, en noviembre de 1983 se crea el nivel secundario como particular con el apoyo del estado, en noviembre de 1989 se crea el post bachillerato con la carrera de Técnico en computación y en el año 2003 es ascendido a nivel superior con las carreras de Análisis de Sistemas, Administración Turística y Hotelera sirviendo principalmente al cantón de Yantzaza y parroquias cercanas. Su infraestructura física ha crecido conforme se han ido creando los distintos niveles de estudio.

Desde su creación hasta la actualidad se encuentra ubicado en la Calle Jorge Mosquera entre Luis Bastidas y Armando Areas.

Desde hace unos diez años atrás su estructura física está formada por dos bloques de de dos pisos donde funcionan las oficinas administrativas, el nivel de bachillerato con la especialidades de Químico Biológicas, Físico Matemáticas e Informática y el nivel superior con la especialidad de Tecnología en Informática. Adjuntos están otros dos bloques de tres pisos donde funciona el nivel básico.

Desde hace unos 12 años atrás cuenta con las siguientes áreas para su desempeño diario:

Área directiva
Área administrativa
Área de servicios
Área Docente

Área Dicente

Situación Actual

Usuarios actuales de la red

La red de datos actualmente la usa el área administrativa de la siguiente manera:

- Rectorado, Vicerrectorado, Orientación y colecturía utilizan la red solo para conexión a Internet.
- Secretaría, Inspección y Dirección de la escuela utilizan la red para conectarse al sistema académico que está instalado en el equipo de secretaría y para la conexión a Internet.

A continuación se presenta un esquema de la estructura actual de la red:

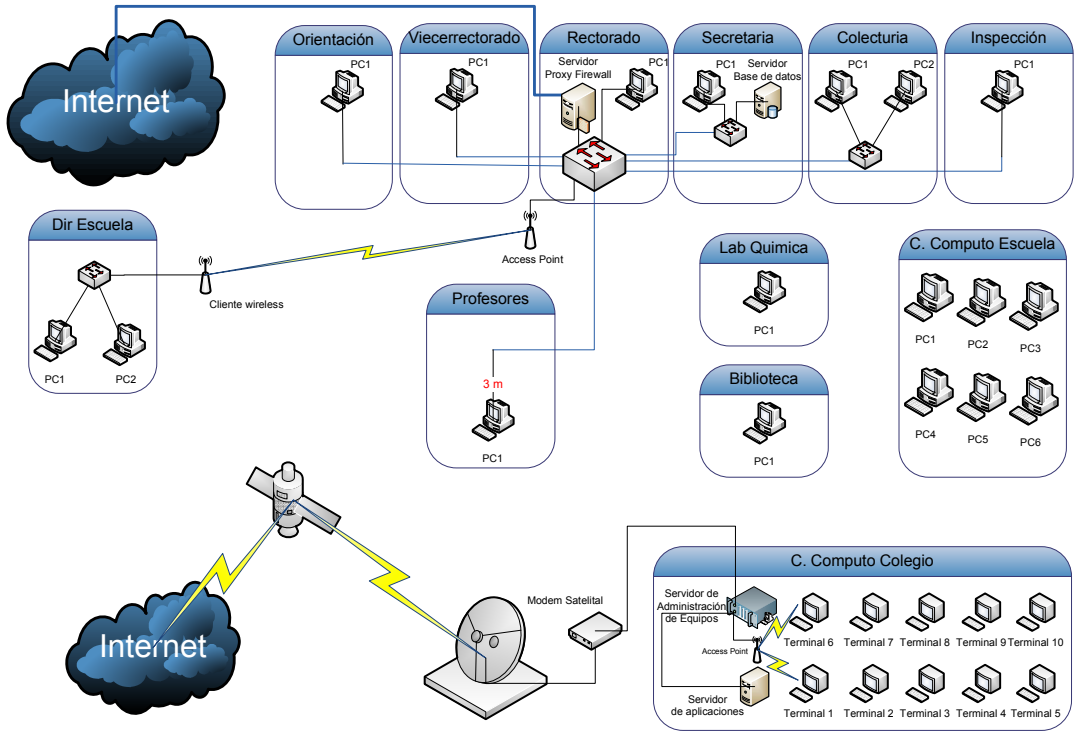


Figura 12. Situación actual de la red del I.S.T.F. “Juan XXIII”

Habilidades de los usuarios en el manejo de equipos y aplicaciones

En cuanto al manejo de equipos de cómputo existe un nivel aceptable por parte del área directiva, administrativa y docente gracias a los cursos de capacitación dictados por el área de docencia informática. Del área estudiantil un 50 % del total de alumnos tienen un conocimiento aceptable en el manejo del computador y son los alumnos del nivel de bachillerato y superior por el limitado número de equipos en el centro de cómputo.

Respecto del manejo del sistema académico en red, la Secretaría, Inspección y Dirección están familiarizados unos tres años atrás.

Todos los usuarios administrativos que disponen del servicio de Internet desde hace un año y medio atrás se encuentran ya familiarizados. Respecto de la demás áreas existe un nivel aceptable en el uso de este servicio.

Proyección Futura

La proyección futura de la institución es la siguiente:

- Dentro del área administrativa se incrementaran 4 personas para: auxiliar secretaría, auxiliar de inspección, un coordinador y una secretaria para el nivel superior y todos deberán contar con una estación de trabajo.
- Dentro del área docente se incrementaran aproximadamente diez personas como personal contratado.
- Los centros de cómputo del nivel básico y bachillerado deberán ser reequipados para poder operar con 18 PCs cada uno.
- El número de estudiantes se mantendrá porque no hay más espacio físico donde pueda ampliarse el Instituto.
- Contar con una biblioteca virtual.
- Publicar un portal web institucional para promocionar el instituto y realizar consultas al sistema académico. Estos servicios serían implementados cuando se tenga el apoyo económico de algún organismo público o privado, ya que es necesario primero tener implantado una buena infraestructura de telecomunicaciones para poder ofrecer este y otros tipos de servicios a nivel de Internet.

Políticas y procedimientos administrativos

Operaciones e información Crítica.

La única información que podría considerase crítica es la base de datos del sistema académico a la cual tienen acceso vía red local únicamente tres personas y la información fluye entre el servidor y los tres equipos clientes. Esta base de datos es actualizada diariamente por el departamento de inspección para el ingreso de asistencias de los estudiantes del nivel de bachillerato. De igual manera es actualizada trimestralmente para el ingreso de las notas de los estudiantes del nivel básico y bachillerato. Las notas de los estudiantes del nivel superior son ingresadas dos veces por ciclo. Por último esta base de datos es actualizada cada año académico para matriculas.

La base de datos es respaldada semanalmente en el mismo equipo de secretaría y en un disco duro externo.

Respecto de la información que tiene cada uno de los equipos del área administrativa no es crítica ya que son archivos que contienen formatos para el trabajo de rutina.

Protocolos permitidos en la red actual

Para los dos servicios que brinda la red actual como son datos e Internet se usan los protocolos TCP (protocolo de control de transmisión) e IP (protocolo de Internet).
Se deberán utilizar los protocolos necesarios para implementar la Intranet con los servicios de: Internet, Web, Correo Electrónico, DNS y DHCP.

Usuarios que serán permitidos en la Intranet

Posteriormente se verán beneficiadas por los servicios que brinde la Intranet las áreas directiva, docente y dicente con la excepción del área de servicios. Cabe señalar que el área dicente osea los estudiantes tendrán el servicio de

Internet en sus horas de practica en el centro de computo y en cualquier otro momento de manera inalámbrica. El servicio de correo electrónico será utilizado únicamente por el área administrativa cuando implante el prototipo por cuestiones de tiempo, pero en lo posterior todas la áreas se verán beneficiadas de este servicio.

Personal Técnico Operativo.

La institución cuenta con un operador de cómputo que es el encargado del mantenimiento de los equipos de cómputo y de la red. Deberá ser esta misma persona quien deba apoyar en el desarrollo de proyecto. Los usuarios administrativos deberán colaborar en el análisis y pruebas del prototipo.

Hardware y software actual y futuro.

Respecto del hardware:

Existen 9 computadores dentro del área administrativa. Un centro de computo con 1 servidor y 10 clientes que está conectado a Internet por medio de un enlace satelital. Este centro de cómputo está al servicio del nivel de bachillerato y superior. Y un segundo centro de cómputo con 6 PCs para el nivel básico sin conexión a Internet.

Todos los equipos de computo tienen características técnicas básicas como: Procesadores Pentium IV y Dual Core, Memoria promedio de 512 MB, discos duros promedio de 80 GB y puertos de red de 10/100 Mbps. Cada oficina cuenta con una impresora y los equipos de red que existen son:

- Un switch TRENDnet TE100-S24 10/100 Mbps
- 2 switch D-Link 10/100 Fast Ethernet modelo Des-100 8D.

- 2 Access Point D-Link de 108 Mbps en 2.4 GHz.

Respecto del software:

Existe el sistema académico y la base de datos instalado en el computador de secretaría que por medio de la red local brinda las siguientes funciones:

- Secretaria: matriculas, registro de notas, consultas
- Inspección: registro de asistencias
- Dirección de la escuela: matriculas, registro de notas, consultas

El software o programas que utilizan todos equipos de la institución son los siguientes:

Sistema Operativo: Windows (sin licencia).
Antivirus: Nod32 (sin licencia).
Software de Oficina: Microsoft Office (sin licencia).

Recursos compartidos.

Cada oficina maneja sus propios archivos con formatos personalizados para el trabajo rutinario y por lo tanto no son compartidos en la red. De igual manera no se comparten recursos de hardware ya que cada oficina cuenta con una impresora pero posteriormente para economizar recursos de impresión y si existe el presupuesto necesario será instalada una copiadora en red que de el servicio a toda el área administrativa.

3.2 Análisis de requerimientos

Una vez recopilados los requerimientos iníciales de la red se procedió a realizar un análisis detallado para obtener un catálogo de requerimientos reales de la red que satisfaga las necesidades de los usuarios y sirva de base para el diseño.

Aplicaciones que se implementarán

Analizados los requerimientos se puedo definir que las aplicaciones se ejecutarán en la Intranet como se indica a continuación.

- El sistema académico y su base de datos debe ser migrado al cuarto de equipos donde se encuentren los demás servidores y los equipos principales de la Intranet. El sistema seguirá ejecutándose como cliente-servidor a nivel local bajo la nueva red. Cabe señalar que los equipos que tengan acceso a este sistema también se podrán utilizar los demás servicios de la Intranet bajo esta misma red. Los equipos que tienen acceso a este sistema son: Secretaría, Inspección y Dirección de la Escuela.
- El correo electrónico deberá ejecutarse tanto a nivel local como a nivel de Internet.
- El servicio web también deberá ejecutarse a nivel local e Internet.
- Posteriormente deberán poderse ejecutar otros servicios como FTP, directorios, biblioteca virtual y video conferencia.

Nuevas redes de acceso

La única nueva red de acceso será Internet y posteriormente por medio del servicio web institucional se deberá crear vínculos que permitan un acceso fácil y rápido hacia sitios de interés para la institución.

Nivel de confiabilidad de la Intranet

La Intranet deberá garantizar que la base de datos del sistema académico deberá ser accesada solo a nivel local y por los usuarios autorizados. En un futuro la Intranet deberá permitir hacer consultas vía Web, que internamente serán administradas en forma local.

Identificación de los usuarios finales de la Intranet

Los usuarios de la nueva red se componen de personal administrativo, docente y estudiantes, tal y como se describe a continuación:

Tipo de Usuario	Cantidad
Directivos	2
Administrativos	7
Docentes Educación Básica	23
Docentes de Nivel Medio	25
Docentes de Nivel Superior	5
Estudiantes Nivel Básico	440
Estudiantes Nivel Medio	560
Estudiantes Nivel Superior	10
TOTAL	1072

Tabla 10. Usuarios de la red.

Cabe señalar que de todos estos usuarios, solo el total de usuarios directivos y administrativos deberán tener acceso a todos los servicios de la Intranet, en cambio los demás usuarios, solo un pequeño porcentaje tendrá acceso a Internet, pero no al servicio de correo electrónico por cuestiones de tiempo, posteriormente deberán ser beneficiados también de este servicio después de la implantación del prototipo.

Estimación del tráfico que generaría la Intranet

Para estimar el tráfico que puede generar la red se tomo en cuenta dos aspectos:

- El tráfico generado a nivel local
- El tráfico generado a nivel de Internet

Trafico de la red local (Sistema Académico)

Registro de asistencias: este tráfico es generado por el equipo ubicado en inspección durante una hora diaria. El análisis es el siguiente:

Tamaño aproximado de los registros de datos: 13 KB = 0.10 Mbits
Velocidad promedio del canal de transmisión: 100 Mbps
Aplicamos una regla de tres simple:
100 Mbits – 100 % del canal
0.10 Mbits – X

X = (0.10 Mb * 100 %) / 100 Mbits
X = 0.1 %
El volumen de datos a transmitir no ocuparía ni el 1% de la capacidad del canal durante una hora diaria.

Registro de Notas: Esta operación se la realiza en el equipo ubicado en secretaria cada trimestre durante una semana. El análisis es el siguiente:
Tamaño aproximado de los registros de datos: 15 KB = 0.12 Mbits
Velocidad promedio del canal de transmisión: 100 Mbps

100Mb – 100 % del canal
0.12 Mbits – X
X = (0.12 Mb * 100 %) / 100 Mbits
X = 0.1 %

En este caso también las transacciones no ocuparían ni el 1% de la capacidad del canal durante una semana en el trimestre.

Generación de reportes: Esta operación se realiza también en el equipo de secretaría y el análisis es el siguiente:

Tamaño aproximado de los registros de datos: 25 KB = 0.20 Mbits
Velocidad promedio del canal de transmisión: 100 Mbps

100 Mbits – 100 % del canal
0.20 Mb – X
X = (0.20 Mb * 100 %) / 100 Mb
X = 0.2 %

La interpretación sería que esta operación tampoco ocuparía ni el 1% del canal.

Matriculas: Esta operación se realiza una vez al año, 8 horas diarias durante una semana en cuatro equipos trabajando casi simultáneamente. El análisis sería el siguiente:

Tamaño aproximado de los registros de datos: 30 KB = 0.24 Mbits * 4 Equipos = 0.98 Mbits
Velocidad promedio del canal de transmisión: 100 Mbps
100 Mbits – 100 % del canal
0.98 Mbits – X
X = (0.98 Mb * 100 %) / 100 Mbits
X = 1 %

La interpretación sería que esta operación ocuparía el 1% del canal durante el día y por el lapso una semana.

Actualmente no se comparten archivos en red ni dispositivos, pero si lo hubiese en el futuro el ancho de banda de la red local aun sigue siendo eficiente.

Tráfico de Internet

Los cálculos para el dimensionamiento de la salida hacia Internet son referenciales, cuando se implemente este proyecto se deberá probar los enlaces con las especificaciones de este estudio y tomar decisiones para quedarse con las capacidades sugeridas o modificarlas.

Área	# Personas	Acceso a Internet	# de personas con acceso a Internet
Directiva	2	Si	2
Administrativa	7	Si	4
Docente	53	Si (Inalámbrico)	5
Estudiantes de los 3 niveles	1010	Si (Inalámbrico)	6
Total	**1072**		**17**

Tabla 11. Usuarios con acceso a Internet

En la institución se tiene un aproximado de 17 usuarios simultáneos que utilizan tanto la red local como el acceso a Internet; las principales aplicaciones que le dan a este servicio son:

- Navegar por sitios web
- Mensajería Instantánea
- Correo Electrónico
- Descarga de Archivos

Tráfico de Navegar por sitios web:

$$C\ usuario\ pag\ web = Tpagina \times t\ carga$$

$$C\ usuario\ pag\ web = 384 \frac{KB}{página} \times \frac{1\ página}{15\ segundos} \times \frac{8\ bits}{1\ \text{Byte}} = 204{,}8\ \text{Kbps}$$

$$C\ Navegar = \#\ usuarios \times I\ simultaneidad \times C\ usuario\ pag\ web$$

$$C\ Navegar = 17 \times 0.12 \times 204{,}8\ Kbps = 417.79\ \text{Kbps}$$

Se asume: que una página web promedio actualmente tiene 384 KB según Google, el tiempo de carga se asume de 15 segundos que sería razonable y se considera un índice de simultaneidad del 12% de los usuarios cargan una página web simultáneamente. Con estos datos el cálculo nos dice que serían necesarios 417,79 Kbps para navegación.

Tráfico de Mensajería Instantánea

CIM: Capacidad de mensajería instantánea

$$C\ IM = \#\ Usuarios \times C\ IM\ usuario$$

$$\text{C IM} = 17 \times 2\ \text{Kbps} = 34\ \text{Kbps}$$

Se dimensiona que la capacidad de transmisión para mensajería Instantánea por usuario CIM es igual a 2 Kbps como promedio.

Se asume que todos los usuarios conectados a Internet utilizan algún programa de mensajería instantánea para comunicación interna o externa. El cálculo nos dice que serían necesarios 34 Kbps para mensajería instantánea.

Tráfico de Correo Electrónico

$$C\ usuario\ email = Temail \times t\ descarga$$

$$C\ usuario\ email = 30\frac{KB}{email} \times \frac{1\ email}{5\ segundos} \times \frac{8\ bits}{1\ \text{Byte}} = 48\ \text{Kbps}$$

$$C\ Email = \#\ usuarios \times I\ simultaneidad \times C\ usuario\ email$$

$$C\ Email = 17 \times 0.1 \times 48\ Kbps = 81.60\ \text{Kbps}$$

Se asume que cada correo electrónico promedio tiene 30 KB y un índice de simultaneidad del 10%. El cálculo nos dice que serían necesarios 81.60 Kbps para el servicio de correo electrónico.

Descarga de archivos.

$$C\ usuario\ descarga\ archivo = Tarchivo \times t\ descarga$$

$$C\ usuario\ descarga\ archivo = 300\frac{KB}{\text{archivo}} \times \frac{1\ archivo}{60\ segundos} \times \frac{8\ bits}{1\ \text{Byte}} = 40\ \text{Kbps}$$

$$C\ Descargar = \#\ usuarios \times I\ simultaneidad \times C\ usuario\ descarga\ archivo$$

$$C\ Descargar = 17 \times 0.1 \times 40\ Kbps = 68\ \text{Kbps}$$

Se asume: que un archivo de 300 KB se descargue en 60 segundos. El cálculo nos dice que serían necesarios 68 Kbps para descargar archivos.

Capacidad Total.

$$C\ Total = C\ Navegar + C\ IM + C\ Email + C\ Descargar$$

$$C\ Total = 417.79 + 34 + 81.6 + 68 = = 601.39\ \text{Kbps}$$

El cálculo total nos indica que se necesitaría un canal de 601 Kbps para dar el servicio de Internet a 17 usuarios.

Disponibilidad de la Intranet

Una vez analizado el tráfico que generaría la red es necesario dimensionar la velocidad de procesamiento y el tiempo de respuesta de los servidores que brindarán los servicios de Internet, Web y correo. Por lo tanto se definió que estos equipos deber estar dotados de las características técnicas ideales para que garanticen un buen tiempo de respuesta sobre todo a los usuarios internos,

ya que los externos dependen también del ancho de banda para la conexión a Internet. Se debe tomar en cuenta también que la disponibilidad de la Intranet dependerá mucho de la energía eléctrica y por lo tanto se debe considerar en un futuro cercano la adquisición de un Backup de energía eléctrica para garantizar el funcionamiento de estos equipos cuando existan problemas de energía.

Requerimientos finales que deberá satisfacer la Intranet

- Se deberá ejecutar el sistema académico en tres equipos a nivel de red local, posteriormente la red deberá soportar consultas web a nivel de Internet.
- La red loca LAN debe estar segmentada en dos subredes. La subred LAN 1 que integrará todas las áreas de usuarios (Administrativos, Docentes, Alumnos, Inalámbricos, sistema académico) y la subred LAN 2 que integrarán los servidores para los servicios de: Firewall, DNS, Web y Correo Electrónico.
- Los usuarios de la LAN 1 podrán hacer peticiones a los servidores de la LAN 2 y tener Acceso al Internet.
- Los usuarios externos de Internet podrán hacer peticiones a los servidores ubicados en la LAN 2 considerada como una zona desmilitarizada (DMZ), pero no de deberán tener acceso a la LAN 1.
- Los usuarios de la red LAN 1 deberán autenticarse para conectarse al Internet y para el servicio de correo electrónico.
- El acceso al Internet por parte de los usuarios de las diferentes áreas deberá ser en unos casos con acceso limitado a servicios o contenido Web y en otros casos con acceso ilimitado, con el fin de administrar de la mejor manera los 256 Kbps de ancho de banda que actualmente posee la institución.
- El administrador de la red será el encargado de realizar configuraciones posteriores.
- Utilizar cableado estructurado según la norma vigente.
- Cableado horizontal mínimo UTP cat 5. Cableado de backbone mínimo UTP cat 6.

- Tecnología de conexión horizontal mínima 100BaseTX Fast Ethernet Full Duplex.
- Tecnología de conexión vertical 1000BaseT Gigabit Ethernet.
- Switchs de 10/100/1000 Mbps de acuerdo al diseño.
- Wifi 802.11g con seguridad WEP para red local inalámbrica.
- Crear rutas de redireccionamiento para la DMZ en el router y listas de control de acceso de usuarios para la conexión a Internet.
- Ubicar los centros de distribución secundaria en oficinas y pasillos. Ubicar el centro de distribución principal en la sala de equipos..
- El enlace WAN para Internet con el ISP debe ser mínimo de 256 Kbps.
- Direccionamiento privado de clase C 192.168.0.0 Ipv4 con división en subredes.
- Pool de direcciones IP públicas para salida a Internet y servicios.
- Asignación de direcciones IP por protocolo de configuración dinámico DHCP para los usuarios inalámbricos.
- La red deberá soportar servicios posteriores como FTP y Video Conferencia.

3.3 Diseño de la topología de red

3.3.1 Diseño de la capa 1

Cableado a utilizar

Se utilizará cable UTP categoría 5 para el cableado horizontal y UTP categoría 6 para el cableado vertical ya que estos dos tipos de cable cumplen con la norma EIA/TIA 568 y su capacidad de transmisión satisface los requerimientos de la red.

Topología de red a utilizar

Para el diseño de la red se usará la *topología en estrella extendida* ya que la red contará con más de un armario de distribución secundaria (IDF) para poder

crear varias áreas de captación. Para las conexiones de cable se utilizará el estándar EIA/TIA 568-B.

Se utilizará el estándar Fast Ethernet que alcanza 100BaseTX sobre el cable de cobre par trenzado para conectar los clientes con los switchs y Gigabit Ethernet para enlazar los IDFs con el MDF a una velocidad de 1000 Mbps.

Diagrama lógico de la red

El esquema que se propone para la intranet está compuesto por la integración de tres partes, un enlace que conecta con el proveedor de servicios de internet (ISP), una red LAN para la sala de servidores y los equipos instalados dentro del edificio y una red inalámbrica que permitirá el acceso a internet y a otros servicios a los estudiantes y profesores. A continuación se muestra el diseño lógico de la red:

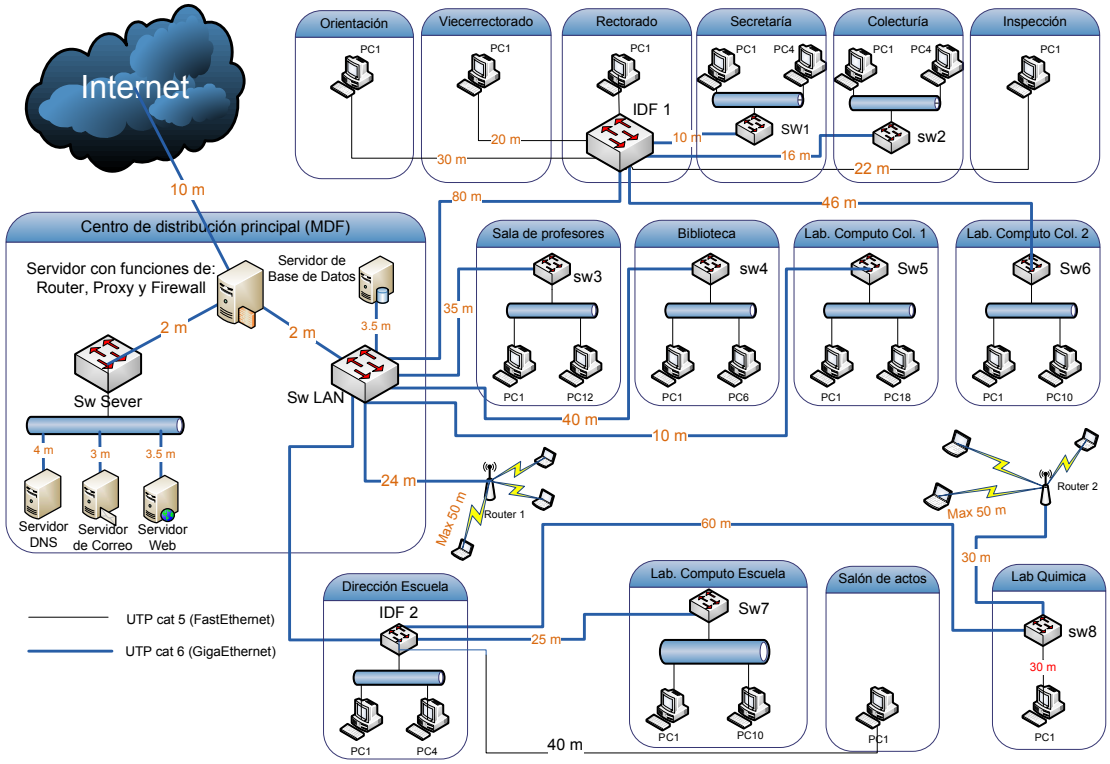


Figura 13. Diagrama lógico de la red

En la figura anterior las líneas color negro representan el cableado horizontal que será implementado con cable de cobre UTP cat. 5 Fast Ethernet y las líneas de color azul representan el cableado vertical se deberá ser implementado con el cable de cobre UTP cat. 6 Gigabit Ethernet.

Una vez definido el diagrama lógico de la red detallaremos donde se encuentran ubicados los armarios de distribución secundarios y principales (IDFs y MDFs), los cables que se usaran. Identificamos también la numeración del cableado, los puertos al que se conectarán y si se trata de una conexión cruzada horizontal o vertical. Esto se encuentra representado en la siguiente tabla.

Conexión	Ubicación	Id. De Cable	Conexión/Puerto origen	Tipo de Cable	Estado
Servidor Proxy a Internet	ETH 0	V1	RC/Puerto 1	UTP cat 6	Ocupado
Sw LAN a Servidor Proxy	ETH 1	V2	RC/Puerto 1	UTP cat 6	Ocupado
Sw Server a Servidor Proxy	ETH 2	V3	RC/Puerto 1	UTP cat 6	Ocupado
Sw LAN a IDF1	Rectorado	V4	RC/Puerto 2	UTP cat 6	Ocupado
Sw LAN a IDF2	Dir Escuela	V5	RC/Puerto 3	UTP cat 6	Ocupado
Sw LAN a Sw3	Sala Profes	V6	RC/Puerto 4	UTP cat 6	Ocupado
Sw LAN a Sw4	Biblioteca	V7	RC/Puerto 5	UTP cat 6	Ocupado
Sw LAN a Sw5	Lab. Computo Col 1.	V8	RC/Puerto 6	UTP cat 6	Ocupado
Sw LAN a Router 1	Patio Colegio	V9	RC/Puerto 7	UTP cat 6	Ocupado
IDF 1 a Sw1	Secretaría	V10	RC/Puerto 2	UTP cat 6	Ocupado
IDF 1 a Sw6	Lab. Computo Col 2.	V11	RC/Puerto 3	UTP cat 6	Ocupado
IDF 2 a Sw 8	Lab. Quimica	V12	RC/Puerto 2	UTP cat 6	Ocupado
IDF 2 a Sw7	Lab Computo Escuela	V13	RC/Puerto 3	UTP cat 6	Ocupado
Sw8 a Router2	Gradas Escuela	V14	RC/Puerto 2	UTP cat 6	Ocupado

Sw LAN a Servidor Datos	Cuarto de Equipos	H1	RC/Puerto 8	UTP cat 6	Ocupado
Sw Server a Servidor Web	Cuarto de Equipos	H2	RC/Puerto 2	UTP cat 6	Ocupado
Sw Server a Servidor Correo	Cuarto de Equipos	H3	RC/Puerto 3	UTP cat 6	Ocupado
Sw Server a Servidor DNS	Cuarto de Equipos	H4	RC/Puerto 4	UTP cat 6	Ocupado
IDF 1 a PC1	Orientación	H5	RC/Puerto 3	UTP cat 5	Ocupado
IDF 1 a PC1	Vicerrectorado	H6	RC/Puerto 4	UTP cat 5	Ocupado
IDF 1 a PC1	Rectorado	H7	RC/Puerto 5	UTP cat 5	Ocupado
IDF 1 a PC1	Inspección	H8	RC/Puerto 6	UTP cat 5	Ocupado
IDF 2 a PC1	Salón Actos	H9	RC/Puerto 4	UTP cat 5	Ocupado

Tabla 12. Documentación detallada del diseño lógico de la red

3.3.2 Diseño de la capa 2

A continuación se establece como estarán conectados los switchs que permitirían micro segmentar la red para reducir el tamaño de los dominios de colisión en la Intranet.

- En cada uno de los segmentos de red de las diferentes oficinas, donde haya más de un equipo se deberán colocar un switch para reducir al máximo los dominios de colisión. Como indica la figura 8, se deberán colocar 8 switchs que alcancen velocidades de hasta 100 Mbps.

- Para la distribución inalámbrica se deberán colocar dos ruteadores inalámbricos con el fin de cubrir todo el campus académico y también reducir los dominios de colisión de tal manera que los problemas de congestión se resuelvan dentro de estos segmentos de red inalámbrica y no se propaguen en toda la red.
- El MDF estará compuesto por dos switch Gigabit Ethernet para conectar los servidores y los IDFs
- Los dos IDFs deberán ser switchs Gigabit.

Incremento de ancho de banda

No será necesario tener conexiones verticales de Backup ya según el análisis de tráfico en el capitulo anterior los usuarios actuales no ocuparían ni el 1% de la capacidad del canal, sí consideramos que la red creciera al 100% de su capacidad de igual manera la conexión vertical diseñada soportaría este tráfico sin problemas.

Los switchs se deberán implementar como indica en el siguiente diagrama:

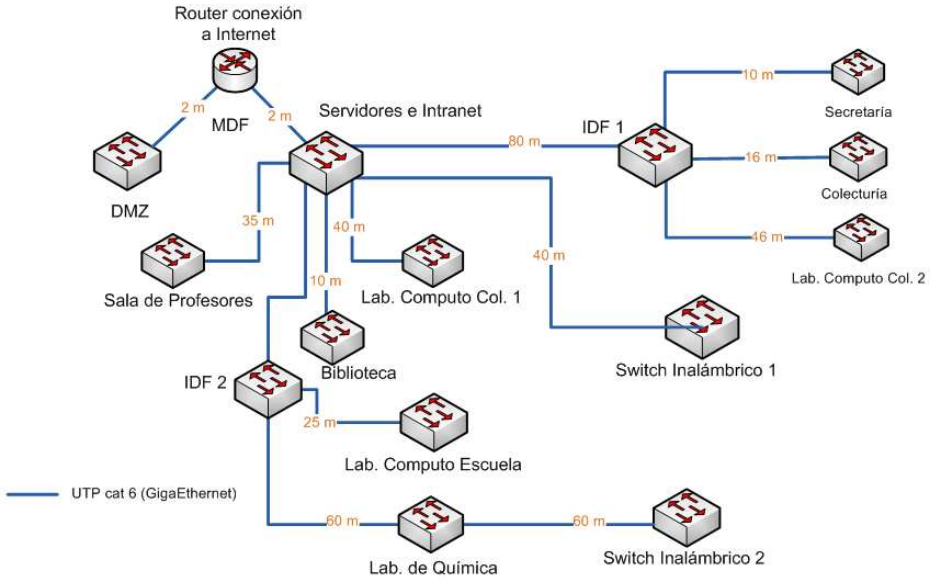


Figura 14. Estructura de los conmutadores de la red

3.3.3 Diseño de la Capa 3

El router que dará la cara al Internet se implementará en un computador con el sistema operativo Linux y con tres interfaces de red.

La red estará dividida en cuatro segmentos de red lógicos y el direccionamiento IP deberá estar como se indica el siguiente esquema:

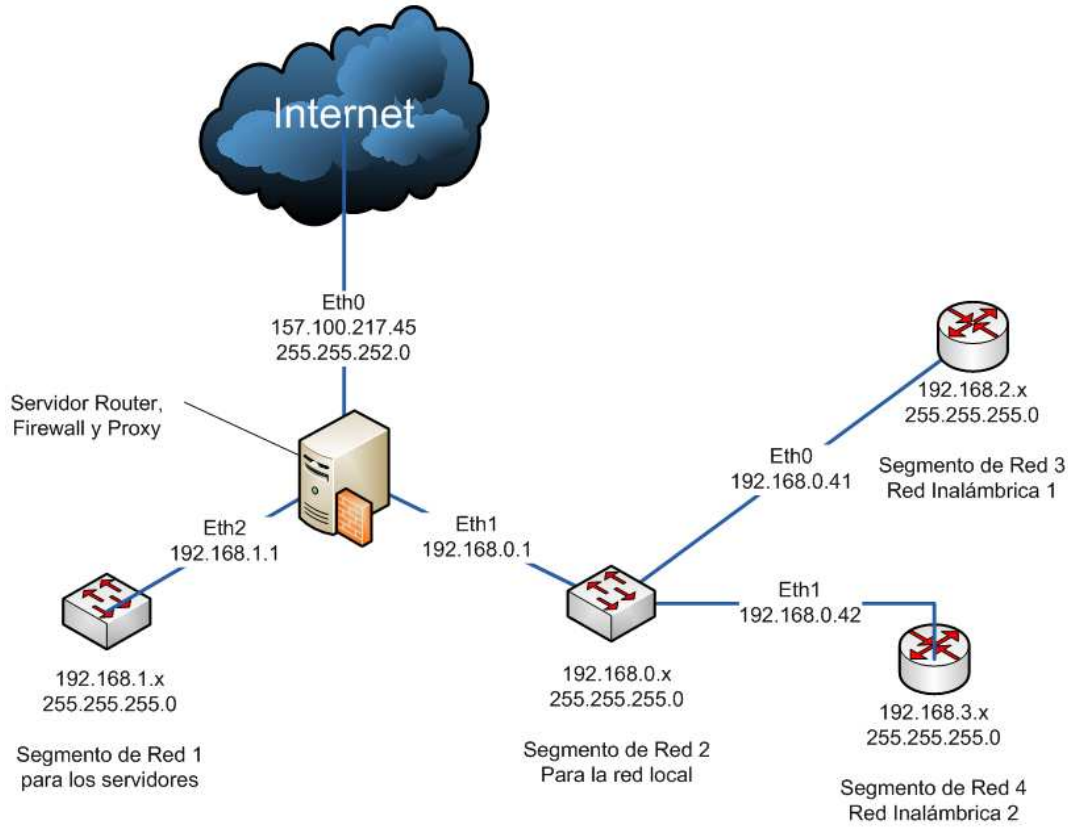


Figura 15. Estructura de los segmentos de la red

3.3.4 Documentación de la implementación lógica de la red

Una vez identificados los segmentos de red se documento el direccionamiento IP que cada uno de los equipos de los diferentes segmentos de red debe tener cuando se implemente la Intranet, como se indica en la siguiente tabla:

Red de Servidores				
Equipo	**IP**	**Mascara**	**Puerta Enlace**	**Estado**
Eth2 del Servidor Router/Proxy/ Firewall	192.168.1.1	255.255.255.0	Ninguna	Asignado
Servidor Web	192.168.1.3	255.255.255.0	192.168.1.1	Asignado
Servidor Correo	192.168.1.4	255.255.255.0	192.168.1.1	Asignado
Servidor DNS	192.168.1.5	255.255.255.0	192.168.1.1	Asignado
Otros Servidores	.1.6 - .1.254	255.255.255.0	192.168.1.1	Libres
Red Local				
Equipos	**IP**	**Mascara**	**Puerta Enlace**	**Estado**
Eth1 del Servidor Proxy y Firewall	192.168.0.1	255.255.255.0	Ninguna	Asignado
Administrador red	192.168.0.2	255.255.255.0	192.168.0.1	Asignado
Servidor de Datos	192.168.0.3	255.255.255.0	192.168.0.1	Asignado
	192.168.0.4 …. 192.168.0.10	255.255.255.0	192.168.0.1	Libres
Rectorado	192.168.0.11 ….. 192.168.0.13	255.255.255.0 255.255.255.0	192.168.0.1 192.168.0.1	Asignado Libres

Vicerrectorado	192.168.0.14 …… 192.168.0.16	255.255.255.0 255.255.255.0	192.168.0.1 192.168.0.1	Asignado Libres
Inspección	192.168.0.17 …. 192.168.0.19	255.255.255.0 255.255.255.0	192.168.0.1 192.168.0.1	Asignado Libres
Secretaria	192.168.0.20 …. 192.168.0.22	255.255.255.0 255.255.255.0	192.168.0.1 192.168.0.1	Asignado Libres
Colecturía	192.168.0.23 192.168.0.24 …… 192.168.0.26	255.255.255.0 255.255.255.0 255.255.255.0	192.168.0.1 192.168.0.1 192.168.0.1	Asignado Asignado Libres
Orientación	192.168.0.27 …. 192.168.0.29	255.255.255.0 255.255.255.0	192.168.0.1 192.168.0.1	Asignado Libres
Dirección Escuela	192.168.0.30 192.168.0.31 192.168.0.32	255.255.255.0 255.255.255.0 255.255.255.0	192.168.0.1 192.168.0.1 192.168.0.1	Asignado Asignado Libre
Otros Departamentos	192.168.0.33 …….. 192.168.0.39	255.255.255.0 255.255.255.0	192.168.0.1 192.168.0.1	Lab Química Libres
Profesores	192.168.0.40 …….. 192.168.0.79	255.255.255.0 255.255.255.0	192.168.0.1 192.168.0.1	Lab Química Libres
Lab Colegio	192.168.0.80 ……. 192.168.0.139	255.255.255.0 255.255.255.0	192.168.0.1 192.168.0.1	Libres
Lab Escuela	192.168.0.140 ……... 192.168.0.169	255.255.255.0 255.255.255.0	192.168.0.1 192.168.0.1	Libres
Reservado	192.168.0.170 ……..	255.255.255.0	192.168.0.1	Libres

	192.168.0.239	255.255.255.0	192.168.0.1	
Router1 Inalámbrico Router2 Inalámbrico	192.168.0.240 192.168.0.241 192.168.0.242 …… 192.168.0.254	255.255.255.0 255.255.255.0 255.255.255.0	192.168.0.1 192.168.0.1 192.168.0.1	Asignado Asignado Libres

Tabla 13. Esquema de direccionamiento IP de toda la red

3.4 Descripción de equipos

Servidor Router, Proxy y Firewall

Este equipo será implementado mediante software libre en un PC para que realice las funciones de ruteador, proxy y firewall. Las características técnicas básicas con las que deberá contar este equipo son las siguientes:

- Procesador core I3 de 3.2 Ghz
- Memoria RAM de 8 GB
- Disco duro de 160 GB
- Tres tarjetas de red Giga bit Ethernet

Aunque la Institución no cuenta con este equipo actualmente se podría usar uno de los equipos actuales que esté disponible y que cuente con características básicas como: un procesador Pentium IV de 2.0 Ghz con 2 GB de memoria RAM y un disco duro de 80 GB.

Routers para la red Inalámbrica.

Serán dos equipos que deberán atender todo el tráfico generado por los usuarios inalámbricos y deberán cumplir con las siguientes características técnicas básicas:

1. Tecnología Wi-Fi
2. Norma IEEE 802.11g Wireless LAN
3. Un puerto WAN de 10/100 Mbps Fast Ethernet
4. Un puerto LAN 10/100 Mbps Fast Ethernet
5. 3 antenas desmontables de 2dBi
6. Soporte dirección IP estática, DHCP Cliente.
7. Protección de Acceso Wi-Fi
8. Calidad de Servicio (QoS)
9. Alimentación por Ethernet (PoE)
10. Temperatura de funcionamiento de 0℃ a 50 ℃
11. Garantía dos años

Como estos equipos no tiene actualmente la Institución se recomienda la marca D-Link ya que son compatibles con el switch principal o MDF y más baratos que otras marcas.

Switch principal para la red local

Este switch es el encargado de atender el tráfico generado por la red local como se indica en el diseño para ello este equipo deberá cumplir con las siguientes características:

1. Norma IEEE 802.3 ab

2. 24 puertos Ethernet 10Base-T, Ethernet 100Base-TX, Ethernet 1000Base-T.
3. Velocidad de transferencia de 1 Gbps
4. Calidad de Servicio (QoS) para garantizar que aplicaciones en tiempo real como las de vídeo y audio tengan prioridad en el futuro
5. Temperatura de funcionamiento de 0℃ a 50 ℃
6. Garantía dos años

Se recomienda utilizar el switch 3COM® BASELINE SWITCH 2824 que actualmente tiene la institución ya que cumple con las características antes mencionadas.

Switch para la red de servidores

Este equipo como lo indica el diseño soportará el trafico generado por los servidores para atender solicitudes de la red interna y externa. Las características técnicas que debería cumplir son las siguientes:

1. Norma IEEE 802.3 ab
2. 8 puertos Ethernet 10Base-T, Ethernet 100Base-TX, Ethernet 1000Base-T.
3. Velocidad de transferencia de 1 Gbps
4. Calidad de Servicio (QoS) para garantizar que aplicaciones en tiempo real como las de vídeo y audio tengan prioridad en el futuro
5. Temperatura de funcionamiento de 0℃ a 50 ℃
6. Garantía dos años

Switch para el IDF1

Este switch se encuentra en la oficina de rectorado y es el encargado de atender el tráfico generado por los puntos de red enlazados al mismo como se

indica en el diseño para ello este equipo deberá cumplir con las siguientes características:

1. Norma IEEE 802.3 ab
2. 16 puertos Ethernet 10Base-T, Ethernet 100Base-TX, Ethernet 1000Base-T.
3. Velocidad de transferencia de 1 Gbps
4. Calidad de Servicio (QoS) para garantizar que aplicaciones en tiempo real como las de vídeo y audio tengan prioridad en el futuro
5. Temperatura de funcionamiento de 0℃ a 50 ℃
6. Garantía dos años

Switch para el IDF2

Este switch se encuentra en la oficina de la dirección de la escuela y es el encargado de atender el tráfico generado por los puntos de red enlazados al mismo como se indica en el diseño para ello este equipo deberá cumplir con características técnicas similares al IDF1.

Switches para las oficinas

Estos switches serán utilizados en la biblioteca, sala de profesores y laboratorio de química. Deberán cumplir con los siguientes requerimientos técnicos:

1. 8 puertos Ethernet 10Base-T, Ethernet 100Base-TX.
2. Velocidad de transferencia de 1/100 Mbps.
3. Calidad de Servicio (QoS) para garantizan que aplicaciones en tiempo real como las de vídeo y audio tengan prioridad en el futuro.
4. Temperatura de funcionamiento de 0℃ a 50 ℃
5. Garantía tres años.

CAPITULO 4

IMPLEMENTACION DEL PILOTO

4.1 Software a utilizar

Linux

Linux es un sistema operativo de libre distribución lo que significa que el usuario tiene la libertad de redistribuir y modificar a de acuerdo a necesidades específicas, siempre que se incluya el código fuente, como lo indica la Licencia Pública General dispuesta por la Fundación de equipamiento lógico libre. Esto también incluye el derecho a poder instalar el núcleo de GNU/Linux en cualquier número de ordenadores o equipos de cómputo que el usuario desee.

Es también de la mejor alternativa de siglo XXI para los usuarios que no solo desean libertad, sino que también desean un sistema operativo estable, robusto y confiable. Es un sistema operativo idóneo para utilizar en Redes.

Con Linux se pueden implementar varios servidores pero los principales y comunes son:

- Servidor Web
- Servidor de correo
- Servidor Firewall
- Servidor DNS
- Servidor DHCP
- Servidor LDAP
- Servidor Radius
- Servidor de archivos
- Servidor de aplicaciones
- Servidor de impresiones y más

Actualmente las distribuciones más utilizadas son las siguientes:

- Linux Ubuntu
- Linux CentOs
- Linux Fedora
- Linux Red Hat Enterprise

Con la descripción anterior se definió que el software a utilizar para la configuración de los servidores sería el Sistema Operativo Linux con la distribución Linux CentOs 2.6 ya que a nivel empresarial es el más recomendado.

4.2 Instalación del Cableado

Según el diseño una parte de la red local ya estaba implantada pero para implementar el piloto de la intranet fue necesario utilizar implementar la red de datos para los servidores y la red inalámbrica. Para ello se utilizó cable UTP categoría 6 de acuerdo al diseño.

4.3 Instalación de Equipos de Conmutación

En el cuarto de equipos se colocó un switch Gigabit que une toda la red local e inalámbrica y un switch de 10/100 Mbps para la red de servidores ya que aún no se dispone de otro switch Gigabit. De acuerdo a la descripción de equipos los switchs para el IDF1 e IDF2 son Gigabit pero por cuestiones económicas se seguirá utilizando switchs de 10/100 Mbps. El resto de switches de la red local que está funcionando tienen una velocidad de transmisión de 10/100 Mbps.

4.4 Configuración de Routers

Router Principal

El router principal que va conectado a la red externa WAN del ISP fue configurado en un PC con características técnicas de acuerdo a las sugerencias como constan en el punto 3.5 (Descripción de equipos). Para configurar que este equipo actué como ruteador fue necesario seguir los siguientes pasos:

1. Creamos el directorio **juanxxiii** en la siguiente ruta: mk /etc/squid/juanxxiii
2. Creamos el directorio **firewall** en la siguiente ruta: mk /etc/squid/juanxxiii/firewall
3. Creamos el archivo ejecutable llamado **reglas** en la siguiente ruta: **vi /etc/squid/juanxxiii/firewall/reglas**
4. Editamos este archivo creado agregándole esta línea para activar el reenvió de paquetes y que el equipo actué como ruteador.
   Echo "1" >> /proc/sys/net/ipv4/ip_forward
5. Presionamos la tecla ESC más la tecla Dos puntos y digitamos **wq** para salir grabando.
6. Ejecutamos este archivo para que se active el servicio desde la línea de comandos digitando **./reglas**
7. Editamos el archivo **rc.local** en la siguiente ruta **vi /etc/rc.local** y le agregamos la siguiente línea para que cuando arranque el equipo se ejecute automáticamente el archivo **reglas** que contiene la configuración del reenvió de paquetes.
   /etc/squid/juanxxiii/firewall/reglas
8. Presionamos la tecla ESC más la tecla Dos puntos y digitamos **wq** para salir grabando.

Configuración de Interfaces de red del Router Principal

En el PC que actúa como router principal se configuraron tres interfaces de red. La Eth0 para conectarse con el ISP, la Eth1 para enlazar el segmento de la red local y la Eth2 para el segmento de la red de servidores. Los detalles de esta configuración están en el Anexo 2.

Routers para la red Inalámbrica

Se utilizaron dos routers inalámbricos que cumplen con las características establecidas en el punto 3.5 (Descripción de equipos). El router que según el diseño lógico se llama Router 1 está ubicado en el bloque de aulas del colegio para cubrir una zona abierta de aproximadamente 15 metros a la redonda y se encuentra configurado como indica el Anexo 3.

El Router 2 está ubicado en el bloque de aulas de la Escuela para cubrir esa zona de aproximadamente 15 metros a la redonda y la configuración de igual forma se encuentra en el Anexo 3.

4.5 Configuración de Servidores

4.5.1 Servidor DNS

Este servidor es aquel que resolverá el nombre de dominio www.juanxxiii.edu.ec con la dirección IP pública 157.100.217.45 de tal manera que nuestro sitio web sea accesado a nivel mundial con este nombre de dominio. Para realizar esto usaremos el DNS de Linux conocido como BIND (Berkeley Internet Name Server). La configuración detallada ver en el Anexo 4.

4.5.2 Servidor firewall

Este servicio fue implementado con Linux en el mismo PC que actúa como Router. Se encarga del filtrado y enrutamiento de paquetes hacia la red local o DMZ, pero también se encargará de enmascarar la red local para la salida al Internet. La configuración es por medio de IP Tables ya que esta herramienta que nos permite configurar las reglas del sistema de filtrado de paquetes del kernel de Linux. Para configurar este servidor primero establecemos las políticas de seguridad del Firewall:

- Los clientes de la red local podrán conectarse a los servicios Web (APACHE) y Correo Electrónico (SENDMAIL) que se encuentran en la DMZ,
- Desde Internet se permitirá conectarse a los servicios Web (APACHE) y Correo Electrónico (SENDMAIL) que se encuentran en DMZ.

La configuración detallada de este servidor está en el Anexo 5.

4.5.3 Servidor proxy

La configuración de este servidor se lo realizó en el mismo equipo que actúa como Router y Firewall. El servicio que se configuro en Linux es **squid.** Se encarga de las conexiones a Internet permitiendo que ciertos usuarios tengan acceso a todos los servicios y contenido web, mientras que otros usuarios tendrán acceso restringido. Para esto se crearon listas de control de acceso por Ips, una lista de extensiones de archivos no deseados y una lista con palabras relacionadas con contenido web no deseado como playboy, etc. Luego se combinaron estas listas en la configuración del servidor proxy para restringir o dar acceso total a los usuarios. Para ver con detalle esta configuración ver el Anexo 6.

4.5.4 Servidor web

Configuramos este servidor por medio del servicio **Apache** que nos proporciona Linux. En este servidor se hospedó un piloto del sitio web de la institución con el fin de probar el funcionamiento del servidor web. La configuración básica se describe a continuación:

Instalamos el servicio httpd básico

yum –y install httpd

Como Apache es un servicio que solo necesita instalarse e iniciar. No requiere modificaciones adicionales para su funcionamiento básico.
Añadimos el servicio a los servicios que inician junto con el arranque del sistema
chkconfig httpdon

Por último iniciamos el servicio por primera vez
service httpd start

Cuando necesitemos reiniciar el servicio por algún motivo se debe considerar que se interrumpirán todas las conexiones establecidas en ese momento.
Service httpd restart

Cuando el servicio ya está trabajando, también se puede utilizar reload con el fin de que Apache vuelva a leer y cargue la configuración sin interrumpir el servicio y por lo tanto las conexiones establecidas.
Service httpd reload

Para detener el servicio, solo se necesitamos utilizar:
service httpd stop

4.5.5 Servidor de correo electrónico

Este servidor se configuro en el mismo equipo que actúa como servidor web. Con Linux se configuró el servicio de **SendMail** agregándole los parámetros necesarios para poder enviar y recibir correo interno y externo. Para ver con mayor detalle la configuración de este servidor vea el Anexo 7.

4.5.6 Servidor DHCP

Este servidor DHCP está configurado a nivel de hardware en los routers 1 y 2 que sirven para la conexión inalámbrica en todo el campus académico como se indica en el Anexo 3 (Configuración de routers inalámbricos), ya que los usuarios que se conecten a estos routers obtendrán automáticamente un dirección IP del rango definido en la configuración de la interfaz LAN de estos routers. No se configuró un servidor DHCP en Linux porque el acceso a Internet de todos los usuarios de la red local está controlado por medio de las direcciones IP estáticas que usan las listas de control de acceso configuradas en el servidor proxy.

4.5.7 Servidor de Autenticación

Debido a que son pocos los equipos usados para la conexión a Internet en las áreas administrativa, docente, estudiantil e inalámbrica se vio conveniente crear claves particulares para los usuarios administrativos, una sola clave para el área estudiantil y una clave para los usuarios inalámbricos. En el caso de los usuarios administrativos podrán accesar al Internet en cualquier momento desde sus equipos de escritorio, los estudiantes podrán usar este servicio únicamente en las horas clase de computación que son 2 horas a la semana, los docentes y los usuarios inalámbricos podrán hacer uso del servicio en forma inalámbrica con las computadoras personales. Esto fue conveniente

también porque el ancho de banda actual es de 256 Kbps necesario para el número de equipos actuales con conexiones no simultáneas. Por estas razones se vio que no sería conveniente utilizar un servidor de autenticación con base de datos como LDAP con MySql sino mas bien utilizar el módulo **ncsa_auth**, de la NCSA (National Center for Supercomputing Applications), y que ya viene incluido como parte del paquete principal de Squid en la mayoría de las distribuciones actuales. Este módulo provee una autenticación muy sencilla a través de un fichero de texto simple cuyas claves de acceso fueron creadas con htpasswd.

Para el servicio de correo electrónico como son pocos usuarios y claves que se debían crear para el funcionamiento del piloto se lo realizó con el mismo servidor de correo SendMail.

Posteriormente cuando se incremente el ancho de banda y los equipos en los centros de cómputo, biblioteca y sala de profesores entonces podremos migrar a un servidor de autenticación con base de datos para crear usuarios y claves particulares sobre todo para el servicio de correo electrónico.

Para ver los detalles de la configuración de la autenticación a través del módulo NCSA ver el Anexo 8.

4.6 Plan de Pruebas

4.6.1 Pruebas de Conexión

Para probar la conectividad entre los diferentes equipos de la red se lo realizó por software usando el protocolo ICMP (Protocolo de Mensajes de Control de Internet) mediante el comando ping bajo el sistema operativo Linux ya que nos permite localizar a un host y nos da un tiempo promedio en la que responde el

host buscado con lo cual podemos saber cuál es el estado de la conexión. Los resultados obtenidos se indican en la siguiente tabla.

Equipo Origen	Equipo Destino	Tiempo de Respuesta promedio
Servidor Proxy	Orientación	0.214 ms
	Vicerrectorado	0.215 ms
	Rectorado	0.215 ms
	Secretaría	0.215 ms
	Colecturía	0.215 ms
	Inspección	0.215 ms
	Dirección de la Escuela	0.213 ms
	Laboratorio de Química	0.215 ms
	Servidor Web y Correo	0.10 ms
	Servidor DNS	0.10 ms

Tabla 14. Pruebas de Conexión con el comando ping

Cabe señalar que el cableado de la red actual cuenta con un 75 % de la instalación respecto del diseño de red propuesto por ello solo las pruebas de conexión se hicieron solo con algunas oficinas. Los tiempos de respuesta obtenidos fueron excelentes respecto de los 200 ms que es lo recomendable para una conexión estable sobre el cable UTP categoría 5. Además soporta hasta 100 Mbps que es sobredimensionado para atender a los servicios de la Intranet, con lo cual se concluye que el medio físico de transmisión utilizado es ideal para satisfacer los requerimientos de la red.

Según la estimación de tráfico descrita en el capítulo 3 “Diseño de capa 1” se necesitarían 601 Kbps para que los 17 usuarios tengan los servicios de web, mensajería instantánea, correo electrónico y descarga de archivos con una conexión promedio de 35 Kbps individual.

Para la conexión externa (Internet) se realizaron las pruebas con los 9 usuarios utilizando diferentes servicios de Internet y se obtuvo un tráfico promedio generado de aproximadamente 250 Kbps. Si multiplicamos este tráfico por 2 obtendríamos que 500 Kbps generarían los 17 usuarios actualmente, pero todos conectados.

Si suponemos un crecimiento del 100 % de usuarios cada año entonces significa que se necesitaría 1000 Kbps para el segundo año y 2.5 Mbps para el quinto año atendiendo a un total de 85 usuarios.

El cable utilizado en la conexión a Internet soporta hasta 1000 Mbps lo que significa que quedaría probado que el medio de transmisión utilizado es el adecuado para soportar el tráfico más exigente que podría generar la Intranet en 5 años, pero a mayor tráfico exigente se genera un mayor gasto económico para la Institución.

4.6.2 Pruebas de funcionamiento de los servidores

Servidor DNS

Para probar que el servidor DNS resuelve el nombre de dominio www.juanxxiii.edu.ec se realizó desde una red externa al instituto utilizando el comando ping y desde Internet utilizando WebSitePulse que es un servidor de monitoreo se servicios web.

Comando ping

Hacemos ping al dominio desde una ventana de comandos y debería entregarnos la IP pública con la que se registró el dominio en el NIC.

C:\>ping juanxxiii.edu.ec

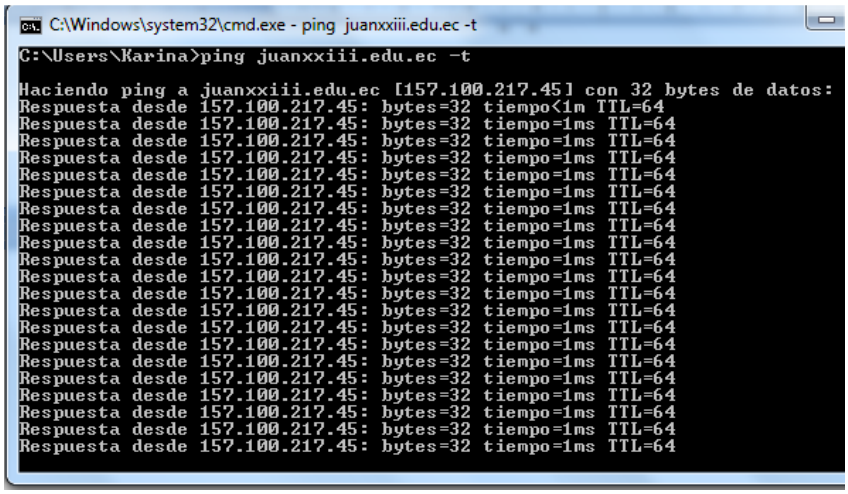


Figura 16. Comando ping aplicado al servidor DNS

WebSitePulse

En este servidor colocamos el nombre de dominio www.juanxxiii.edu.ec y nos devuelve la dirección IP pública.

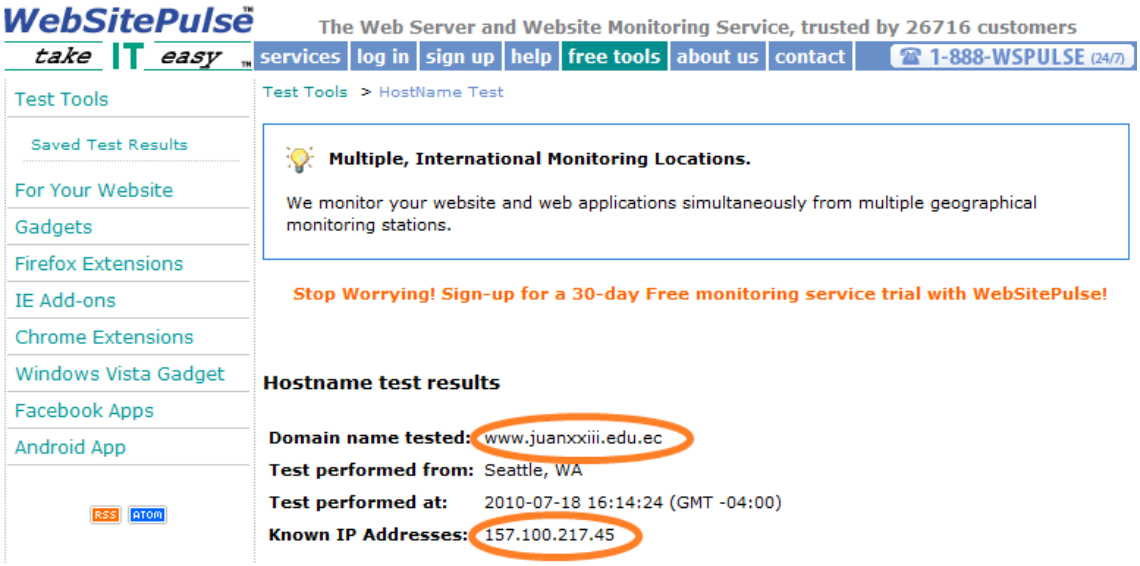


Figura 17. Prueba del servidor DNS con WebSitePulse

Servidor firewall

El servidor firewall tiene dos funciones

1. Dejar que los usuarios de la red local tengan acceso al Internet y hacia la DMZ
2. Dejar que los usuarios externos tengan acceso solo a los servicios de la DMZ como por ejemplo Web.

Para probar el primer punto se hicieron conexiones a Internet desde la red local y no se tuvo ningún inconveniente, luego se probo abriendo la pagina de prueba que se encuentra en el servidor web de la DMZ y también se obtuvo un resultado positivo, al tener estos dos accesos significa que el firewall está permitiendo estos accesos a los usuarios de la red local caso contrario de debería emitir un mensaje como este “The domain name does not exist”.

Para el segundo punto se probó desde una red externa abriendo la pagina web de prueba que se encuentra en el servidor web de la DMZ y se obtuvo la siguiente respuesta del servidor “Servidor Web del JuanXXIII 07/12/2010 este

sitio está en construcción. Gracias por su comprensión". Lo que significa que el firewall permitió el acceso externo a la DMZ caso contrario le debería salir un mensaje de error como el anterior.

Servidor Proxy

La función de este servidor es la de permitir el acceso a servicios y contenido web ilimitado o controlado. Para probar ingresamos como usuarios inalámbricos y digitamos la dirección www.youtube.com en un navegador y el servidor proxy no rechazó la conexión ya que se trata de un usuario limitado como se indica en la siguiente figura:

Figura 18. Prueba del servidor Proxy

Servidor Web

La función de este servidor es la de entregar la pagina web de prueba al usuario ya sea este interno o externo. Cuando realizamos las pruebas del firewall y este permitió que el servidor web presente la pagina de prueba al los

dos tipos de usuarios quedo implícitamente también comprobado que el servidor web está funcionando.

Servidor de correo electrónico

Se configuró el servidor de correo con una pocas cuentas para los usuarios administrativos, se probó primero a nivel local y fue posible realizar el envió y recepción de correo con el cliente de correo Outlook de Microsoft. Después se hicieron ciertos ajustes para realizar esto a nivel de red externa y los resultados fueron positivos porque IP pública ya estaba registrada y los ajustes solo eran a nivel de re direccionamiento en el firewall.

Servidor DHCP

Este servicio fue implementado a nivel de hardware en los routers para los usuarios inalámbricos. Para probar tomamos una PC portátil y nos conectamos al enlace inalámbrico del colegio llamado “Juan XXIII Data Center”, luego desde una consola utilizamos el comando ipconfig para verificar la IP asignada automáticamente a nuestra PC por DHCP como indica la siguiente figura:

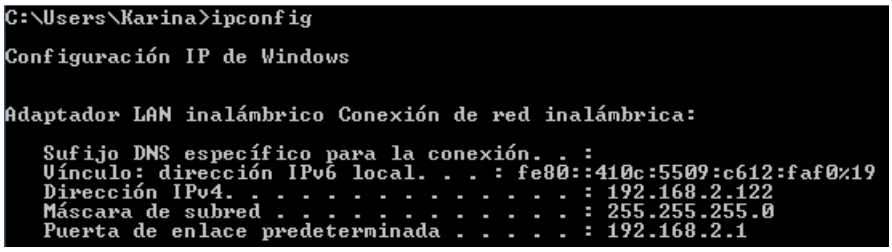


Figura 19. Prueba del servidor DHCP

Como vemos en la figura nos asigno la IP: 192.168.2.122 porque el rango de direcciones IP que maneja va desde la 192.168.2.100 hasta la 192.168.2.25 para 25 equipos.

Servidor de Autenticación

La función de este servicio esta implementada en squid.conf, quien maneja un módulo de autenticación y consiste en solicitar un nombre de usuario y contraseña al momento de abrir un navegador para permitirle el acceso si se trata de un usuario valido como indica la siguiente figura:

Figura 20. Prueba del servidor de Autenticación

4.7 Resultado de pruebas

Como podemos apreciar tanto las pruebas de conexión a nivel de cableado como las pruebas a los servidores fueron exitosas por lo tanto podemos decir que el diseño de la Intranet satisface los requerimientos actuales y podrá satisfacer los requerimientos futuros a cinco años siempre y cuando se implemente la Intranet con el diseño lógico y los equipos recomendados.

CAPITULO 5

PRESUPUESTO

5.1 Costos de cableado

Actualmente la institución cuenta con una red de datos y parte del cableado será utilizado para reducir gastos, por lo tanto en este presupuesto se hace constar solamente el resto de material que se va a utilizar como se detalla a continuación:

DETALLE	UNIDADES	PRECIO UNIT	VALOR
UTP cat 6 x 190 metros	190	0,45	85,5
UTP cat 5 x 250 metros	250	0,35	87,5
Canaleta PVC blanca de pared 60 unidades	145	1,5	217,5
Patch Panel de 24 puertos para RJ-45	3	55	165
Armario Rack de 19"	3	60	180
Conectores RJ 45	150	0,25	37,5
Cajas de conexiones de pared RJ-45	50	6	300
		SUBTOTAL	**1073**

Tabla 15. Costo de cableado

5.2 Costos de equipos

De igual manera se utilizarán los equipos de telecomunicaciones como switches y Access Point que tiene la institución.

DETALLE	UNIDADES	PRECIO UNIT	VALOR
Switches de 8 puertos 10/100 Mbps	3	40	120
Switch de 8 puertos Giga bit	2	90	180
Switch de 16 puertos Giga bit	2	250	500
Dos Routers Inalambricos	2	100	200

PC (Core I5 de 3.2 GHZ, 8 GB RAM, 160 GB)	4	600	2400
Trajetas de red Gigabit Ethernet	3	25	75
		SUBTOTAL	**3475**

Tabla 16. Costo de los equipos

5.3 Costos de Implementación

El costo de implementación incluiría la implementación del cableado y la configuración de los equipos pero por tratarse de un proyecto académico no le hemos incluido un valor porque el tesista debería encargarse de la implementación y además debería hacerlo como parte de su trabajo ya que pertenece a la Institución.

5.4 Costos Operativos

Los costos operativos son valores estimados por el registro de dominio y el pago del servicio de Internet. Estos valores se representan en el siguiente cuadro.

DETALLE	UNIDADES	PRECIO UNIT	VALOR
Registro de dominio para cinco años	5	50	250
Servicio de Internet primer año (256 Kbps)	12	200	2400
Servicio de Internet segundo año (512 Kbps)	12	290	3480
Servicio de Internet tercer año (512 Kbps)	12	290	3480
Servicio de Internet cuarto año (1 Mbps)	12	500	6000
Servicio de Internet quinto año (1 Mbps)	12	500	6000
		TOTAL	**21610**

Tabla 17. Costos operativos

Cabe señalar que el costo por el servicio de Internet no será tomado en cuenta para el presupuesto total ya que este valor actualmente es financiado con fondos de autogestión y no representan una nueva inversión para la institución, pero el costo por el registro de dominio para los cinco años si se tomará en cuenta por tratarse de un nuevo valor.

5.5 Presupuesto Total

DETALLE	UNIDADES	PRECIO UNIT	VALOR
Costo del cableado	1	1073	1073
Costo de equipos	1	3475	3475
Costos de Implementación	1	0	0
Costos Operativos	1	250	250
		SUBTOTAL	**4798**
Imprevistos 5%			**239,9**
TOTAL GENERAL			**5037,9**

Tabla 18. Costo Total

Cabe mencionar que por tratarse de un proyecto académico la inversión que se realice no generará réditos económicos y será verá recompensada con el beneficio social que brindará a la comunidad educativa y sociedad en general. Es por esta razón que en el presupuesto solo consta el valor total de la inversión y no un análisis económico para saber en qué tiempo se recuperaría la inversión y que utilidades generaría durante los cinco años.

CAPITULO 6

CONCLUSIONES Y RECOMENDACIONES

1.1 Conclusiones

- Diseñar una red es un gran desafío, el proceso no solo consiste en conectar computadoras. Una red depende de muchas características que la hagan fiable, manejable y escalable. Para lograr estos objetivos los requerimientos deben estar bien definidos.
- La implementación de un piloto es muy importante para poner a prueba el diseño de la red.
- Los gastos que ocasiona la implementación de una Intranet, se justifican ampliamente con los servicios y el beneficio social que brinda a la institución y comunidad en general.
- Los puntos de acceso inalámbrico al Internet desde cualquier parte del campus proveen de una gran comodidad a la mayoría de los usuarios de la red.
- Tras el estudio realizado, se puede garantizar que la solución adoptada ha sido la mejor entre las muchas posibilidades que nos brindan las redes de hoy en dia. Es decir, utilizando los conocimientos de las tecnologías de la información y comunicación (TIC) se ha desarrollado la solución óptima, adecuada a los requerimientos que garantice la funcionalidad, escalabilidad, adaptabilidad y manejabilidad de la Intranet.
- Como valor agregado la Intranet se convertirá, sin necesidad de costo adicional, en una plataforma válida para proporcionar a la institución conexión hacia el mundo exterior y mejor sus relaciones académicas con instituciones educativas que son exitosas en el área de educación virtual.
- En un futuro muy cercano, la Intranet va a ser un recurso indispensable para casi cualquier institución educativa; porque surgirán nuevos métodos de enseñanza académica y este es el medio tecnológico ideal para acortar distancias, tiempo y ahorrar dinero.

- Dentro del ambiente académico una Intranet es un elemento estratégico que brinda ventaja competitiva frente a otras instituciones, debido principalmente a que la tendencia educativa que apunta hacia las TICs.

1.2 Recomendaciones

- Se recomienda la creación de una área de soporte y telecomunicaciones para la administración y mantenimiento de la Intranet cuando esta sea implementada completamente.
- Dar capacitación a todo el personal para de esta manera motivarlos a utilizar los nuevos servicios de telecomunicaciones implementados en el piloto ya que cuando exista el recurso económico necesario y se implante la Intranet los usuarios ya estarán familiarizados con estos servicios.
- Se debe estudiar con detenimiento y mucho cuidado la ubicación de los puntos de acceso inalámbrico, estos deben ser instalados estratégicamente de tal forma que provean una excelente cobertura.
- Con la implantación de la Intranet se podrá agregar nuevos servicios como FTP, Video Conferencia, Elearning, entre otros que vayan en beneficio de la comunidad educativa y social del cantón y provincia.
- Se recomienda que los directivos agiliten las gestiones necesarias para conseguir el financiamiento que permita implantar todo el diseño de la Intranet en el menor tiempo posible.
- A pesar de los estándares que regulan los equipos de comunicaciones es mejor utilizar equipos de un solo fabricante, esto permite un mejor desempeño y estabilidad a la red.

BIBLIOGRAFIA

[1] Andrew S. Tanenbaum. "Redes de Computadoras", Ed. Prentice Hall, Tercera Edicion; México 2003.

[2] Tim Evans, "Construya su propia Intranet", Ed. Prentice Halls Hispanoamericana, S.A., México, 1997.

[3] William Satallings, "Wirelless Communications and Networking", Ed. Prentice Halls, 2002.

[4] Santiago Fraguas Berasain. "Diseño de seguridad en redes". PEARSON EDUCACION, S.A., Madrid, 2003.

[5] Douglas E. Comer, "Redes Globales de información con Internet y TCP/IP", principios básicos, protocolos y Arquitectura. Ed. Prentice-Hall, Tercera Edición; Mexico 1996.

[6] Joyanes Aguilar, "Historia de la Sociedad de la Información. Hacia la sociedad del Conocimiento" en R-evolución tecnológica. U. de Alicante: Alicante, 2003

DIRECCIONES URL CONSULTADAS

[7] Soluciones CISCO para educación superior
http://www.cisco.com/web/strategy/education/higher_education.html

[8] Pautas para el caso de estudio: CCNA 1
http://www.palomatica.info/ruben/CCNA1/APUNTES/CASOESTUDIO.pdf

[9] Principios básicos de conmutación y enrutamiento intermedio v3.1:CCNA3
http://www.scribd.com/doc/2196562/CCNA34

[10] Joel Barrios Dueñas, "Manual de Implementación de Servidores con GNU/Linux", Edición Agosto del 2009.
http://www.alcancelibre.org/staticpages/index.php/manuales-indice

[11] Arquitecturas de redes con firewall
http://www.pello.info/filez/firewall/iptables.html

[13] Estandares TIA/EIA-568

http://es.wikipedia.org/wiki/TIA-568B

[14] Normas IEEE 802.11
http://es.wikipedia.org/wiki/IEEE_802.11#802.11b

ANEXOS

Anexo 1. Aval de la Rectora del Instituto para la presentación del proyecto de tesis

REPÚBLICA DEL ECUADOR
INSTITUTO SUPERIOR TECNOLOGICO FISCOMISIONAL
"JUAN XXIII"
Yantzaza – Zamora Chinchipe
Telf: 2300151

Yantzaza, 12 de Septiembre del 2009
Hna. Lic. Rosa Alegría Sivisapa
RECTORA DEL INSTITUTO SUPERIOR TECNOLÓGICO FISCOMISIONAL JUAN XXIII

CERTIFICA:

Que Dentro del contexto del plan estratégico institucional del año 2009 consta como uno de los objetivos específicos la creación de una biblioteca virtual y de igual manera como una de las metas institucional a mediado plazo es la de fomentar la investigación a nivel de profesores y estudiantes mediante el uso de las TIC (Tecnologías de la Información y comunicaciones).

Por esta razón y conociendo el tema de tesis **DISEÑO DE LA INTRANET PARA EL INSTITUTO TECNOLÓGICO FISCOMISIONAL "JUAN XXIII" DEL CANTON YANTZAZA PROVINCIA DE ZAMORA CHINCHIPE** planteada por el ingeniero Freddy Ajila miembro de nuestro centro educativo me comprometo en brindar todo el apoyo necesario para que el desarrollo de este proyecto de tesis llegue a una culminación exitosa, consiente de la innovación y adelanto nuestro centro educativo, mejor servicio a la comunidad cantón y provincia de Zamora Chinchipe.

Atentamente.

Hna. Lic. Rosa Alegría Sivisapa

INSTITUTO SUPERIOR TECNOLOGICO FISCOMISIONAL
"JUAN XXIII"
RECTORADO
Yantzaza - Zamora Chinchipe - Ecuador

Anexo 2. Configuración del las interfaces de red Eth0, Eth1 y Eth2 del Servidor Router, Firewall y Proxy

Configuración de la Interfaz Eth0:

Esta interfaz o tarjeta de red permitirá la conexión con la red del ISP y por lo tanto se deberá configurar con la dirección IP pública 157.100.217.45 y como puerta de enlace la IP 157.100.217.33 ya que esta información es otorgada por el ISP. Cabe señalar que esta IP pública con el dominio www.juanxxiii.edu.ec ya fue previamente registra en el NIC[1] de Ecuador.

Datos para la Configuración:

IP: 157.100.217.45

Mascara de red: 255.255.255.224

Puerta de enlace: 157.100.217.45

Desde la línea de comandos realizamos lo siguiente:

1. Editamos el fichero de configuración digitando **vi /etc/sysconfig/network-scripts/ifcfg-eth0**
2. Presionamos las teclas **ESC+i** para modificar las líneas que están pintadas con negrita.
   DEVICE=eth0
   BOOTPROTO=none
   BROADCAST=157.100.217.63

[1] NIC Ecuador: Es el organismo oficial de nuestro país donde se debe registrar la IP pública junto con el nombre de dominio de la entidad. La dirección web es http://www.nic.ec

HWADDR=00:21:91:8A:EE:FC # Dirección MAC

IPADDR= 157.100.217.45 # Ip de la interfaz de red

NETMASK= 255.255.255.224 # Máscara de red

NETWORK= 157.100.217.32 # Red en la que se encuentra

ONBOOT=yes # Arranque automático al inicio del sistema

GATEWAY= 157.100.217.33 # Puerta de enlace

TYPE=Ethernet

3. Presionamos las teclas ESC más la tecla Dos puntos y digitamos **wq** para salir grabando.
4. Reiniciamos el servicio de red digitando **service network restart**
5. Esto no es necesario en este punto pero podemos aprovechar para editar el nombre del equipo digitando **vi /etc/sysconfig/network** y cambiamos la línea que está con negrita.

   NETWORKING=yes

   HOSTNAME=proxi.juanxxiii.edu.ec
6. Presionamos las teclas **ESC:** y digitamos **wq** para salir grabando.
7. Presionamos las teclas **ESC:** y digitamos **wq** para salir grabando.

Configuración de la Interfaz Eth1:

Esta interfaz de red permitirá la conexión con la red local LAN de los usuarios por lo tanto tendrá una dirección IP privada de clase C.

Datos para la Configuración:

IP: 192.168.0.1

Mascara de red: 255.255.255.0

Desde la línea de comandos realizamos lo siguiente:

1. Editamos el fichero de configuración digitando **vi /etc/sysconfig/network-scripts/ifcfg-eth1**
2. Presionamos las teclas **ESC+i** para modificar las líneas que están pintadas con negrita.

   DEVICE=eth1
   BOOTPROTO=none
   BROADCAST=192.168.0.255
   HWADDR=00:21:91:8A:EE:FC # Dirección MAC
   IPADDR= 192.168.0.1 # Ip de la interfaz de red
   NETMASK= 255.255.255.0 # Máscara de red
   NETWORK= 192.168.0.0 # Red en la que se encuentra
   ONBOOT=yes # Arranque automático al inicio del sistema
   TYPE=Ethernet
   PEERDNS=yes
   USERCTL=no
3. Presionamos las teclas ESC más la tecla Dos puntos y digitamos **wq** para salir grabando.
4. Reiniciamos el servicio de red digitando **service network restart**

Configuración de la Interfaz Eth2:

Esta interfaz de red permitirá la conexión con los servidores que se encuentran en la DMZ. La dirección IP será privada de clase C.

1. Editamos el fichero de configuración digitando **vi /etc/sysconfig/network-scripts/ifcfg-eth2**
2. Presionamos las teclas **ESC+i** para modificar las líneas que están pintadas con negrita.

   DEVICE=eth2
   BOOTPROTO=none
   BROADCAST=192.168.0.255

HWADDR=00:21:91:8A:EE:FC # Dirección MAC

IPADDR= 192.168.1.1 # Ip de la interfaz de red

NETMASK= 255.255.255.0 # Máscara de red

NETWORK= 192.168.1.0 # Red en la que se encuentra

ONBOOT=yes # Arranque automático al inicio del sistema

TYPE=Ethernet

PEERDNS=yes

USERCTL=no

3. Presionamos las teclas ESC más la tecla Dos puntos y digitamos **wq** para salir grabando.
4. Reiniciamos el servicio de red digitando **service network restart**

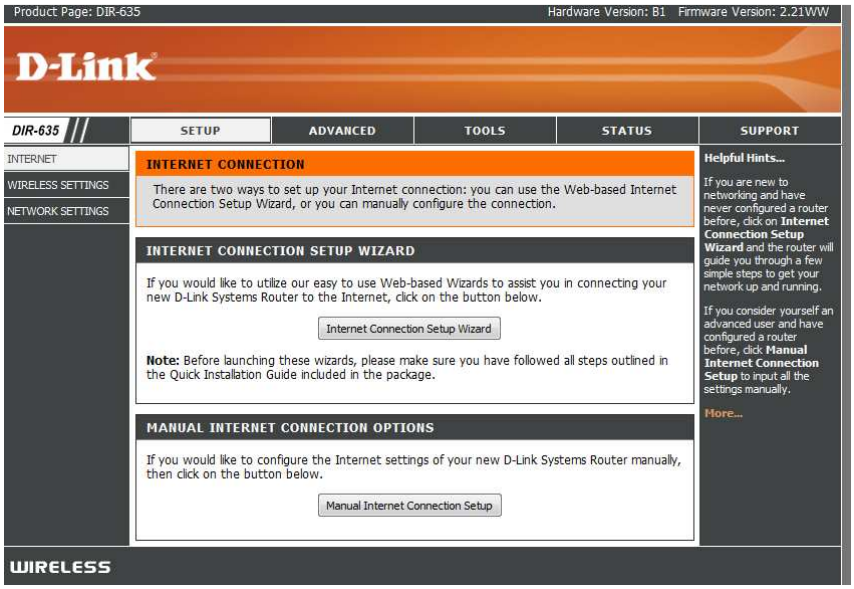
Anexo 3. Configuración de los routers inalámbricos.

Router 1

Este equipo es de Marca D-Link modelo RANGEBOOSTER N 650 ROUTER, que además de cumplir con las características técnicas indicadas en la sección 3.5 es compatible para audio y video streaming. Su configuración es la siguiente:

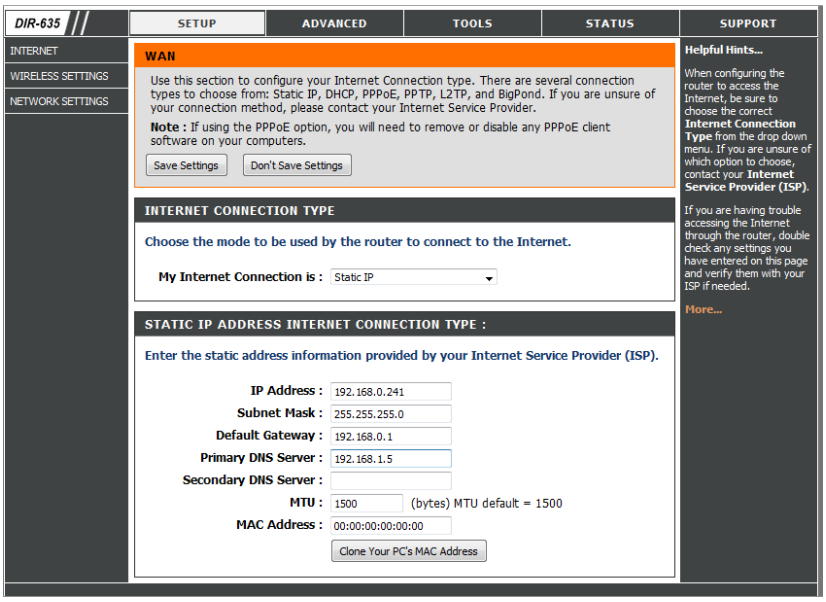
1. Abrimos un navegador como Internet Explorer y digitamos la dirección IP que traen de fabrica en el URL del navegador, la IP nos indica el manual por ejemplo: http://192.168.0.1 y luego digitamos el usuario y la clave que viene de fabrica y también está en el manual por ejemplo. User: admin y Password: vacio

   Cuando logramos ingresar escogemos el menú SETUP como indica la figura:



2. Escogemos la opción INTERNET y presionamos el botón Manual Internet Connection Setup como indica la figura anterior.

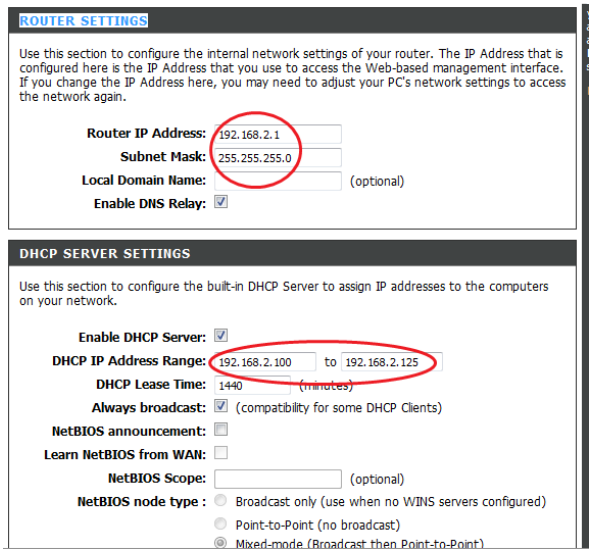
3. Ingresamos la dirección IP de acuerdo a la planificación de la Tabla 12. (Esquema de direccionamiento IP) que en este caso es la 192.168.0.240, la máscara de red 255.255.255.0, la puerta de enlace 192.168.0.1 que es la dirección IP de la Interfaz Eth 1 del PC que actúa como Router principal y la dirección IP del DNS local que es la 192.168.1.5. en la siguiente figura indicamos este proceso.



4. Presionamos el botón Save Settings para guardar la configuración y esperamos que se reinicie el router.

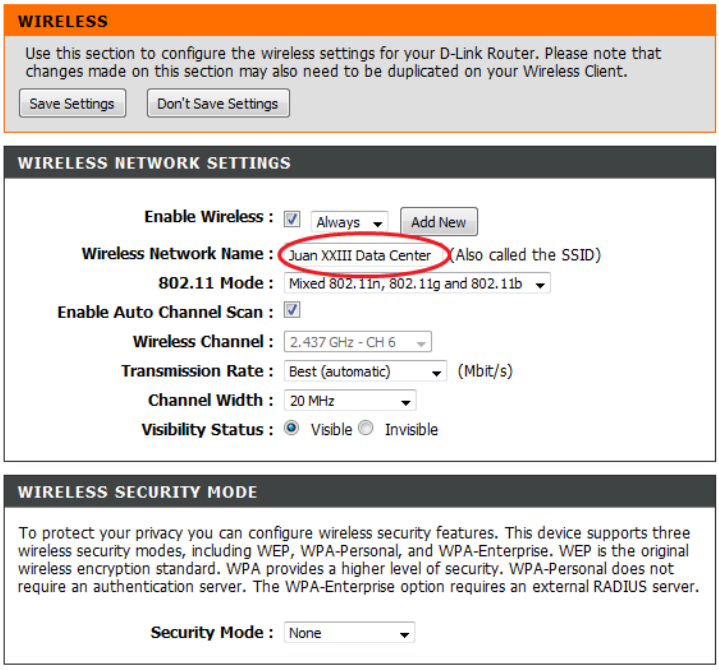
5. Escogemos la opción NETWORK SETTINGS y configuramos la sección ROUTER SETTINGS poniendo la dirección IP que identifica la red inalámbrica. Luego escogemos la opción DHCP SERVER SETTINGS y le ponemos un rango de direcciones IP de la misma red inalámbrica para que

los usuarios inalámbricos obtengan una dirección IP automática como indica la siguiente figura:



6. Presionamos el botón Save Settings para guardar la configuración y esperamos que se reinicie el router.

7. Escogemos la opción WIRELESS SETTINGS y presionamos el botón Manual Wireless Network Setup para configurar el nombre de la conexión inalámbrica que es lo que ven los usuarios al momento de conectarse. En nuestro caso el nombre es **Juan XXIII Data Center** como indica la figura:



8. Presionamos el botón Save Settings para guardar la configuración y esperamos que se reinicie el router.

Router 2

Este router es de la misma marca y modelo que el anterior por lo tanto solo debemos cambiar la información de configuración y seguir los pasos anteriores de la siguiente manera:

En el paso 3 solo cambiamos la dirección IP por la 192.168.0.241.
En el paso 5 cambiamos la dirección IP inalámbrica por 192.168.3.1 y el rango de direcciones IP para los usuarios inalámbricos que es desde la 192.168.3.100 hasta la 192.168.3.125 que servirían para 25 usuarios.

Por último en el paso 7 cambiamos el nombre de la conexión inalámbrica por **Juan XXIII Escuela.**

Anexo 4. Configuración del Servidor de nombres de dominio DNS

Información Previa.

Dominio a resolver: www.juanxxiii.edu.ec
Nombre del servidor DNS: dns1.juanxxiii.edu.ec
Cta de correo del administrador responsable de la zona: bacan2010@hotmail.com
Servidor de correo MX:
IP del dominio: 157.100.217.45
Subdominios e IPs asociadas: www (192.168.1.3), mail (192.168.1.3), ns (192.168.1.5)

Instalación de paquetes

Instalamos los paquetes necesarios desde la línea de comandos
yum -y install bind bind-chroot bind-utils caching-nameserver

Configuraciones previas que debe tener el DNS

Configuramos el fichero /etc/hosts. A este fichero deberemos agregar el nombre del equipo que desempeñara la función de servidor DNS así como la dirección IP asignada a este equipo, al final este fichero deberá verse así.

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1      localhost.localdomain localhost
192.168.1.5  dns1.juanxxiii.edu.ec  dns1
```

Editamos el fichero /etc/sysconfig/network. Este fichero debe quedar así:

```
NETWORKING=yes
```

NETWORKING_IPV6=no

HOSTNAME=dns1.juanxxiii.edu.ec

Ficheros de configuración del servidor DNS

Creamos los archivos de zona

touch /var/named/chroot/var/named/juanxxiii.edu.ec.zone
touch /var/named/chroot/var/named/157.100.217.in-addr.arpa.zone

Editamos el archivo vim /var/named/chroot/var/named/juanxxiii.edu.ec.zone y le añadimos el siguiente contenido:

```
$TTL    86400
@       IN      SOA     dns1.juanxxiii.edu.ec.  root.juanxxiii.edu.ec. (
                        2010052908 ;numero de serie
                        28800 ; tiempo de refrescamiento
                        7200 ; tiempo entre reintentos de consulta
                        604800 ; tiempo tras el cual expira la zona
                        86400 ; tiempo total de vida
                        )
juanxxiii.edu.ec.       IN      NS      dns1
juanxxiii.edu.ec.       IN      A       157.100.217.45
juanxxiii.edu.ec.       IN      MX      0       mail.juanxxiii.edu.ec.
www                     IN      A       157.100.217.45
dns1                    IN      A       157.100.217.45
mail                    IN      A       157.100.217.45
~
```

Editamos el archivo vim /var/named/chroot/var/named/217.100.157.in-addr.arpa.zone y le añadimos el siguiente contenido.

```
root@dns1:/var/named/chroot/var/named
$TTL    86400
@       IN      SOA     dns1.juanxxiii.edu.ec. root.juanxxiii.edu.ec. (
                        2010052909 ; Numero de Serie
                        28800 ; Tiempo de Refresco
                        7200 ; Tiempo de Reintentos
                        604800 ; Expiracion
                        86400 ; Tiempo Total de Vida
                        )
@       IN      NS      dns1.juanxxiii.edu.ec.
45      IN      PTR     juanxxiii.edu.ec.
45      IN      PTR     dns1.juanxxiii.edu.ec.
45      IN      PTR     www.juanxxiii.edu.ec.
45      IN      PTR     mail.juanxxiii.edu.ec.
~
~
```

Creamos y configuramos el fichero "named.conf" que a su vez llama a los archivos de zona.

touch /var/named/chroot/etc/named.conf
Editamos el archivo vim /var/named/chroot/etc/named.conf y le agregamos el siguiente contenido

```
// caching-nameserver package upgrade.
//
options {
        listen-on port 53 { 127.0.0.1;192.168.1.5;192.168.0.1; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";

};

include "/etc/rndc.key";
zone "juanxxiii.edu.ec." {
type master;
file "juanxxiii.edu.ec.zone";
allow-update { none; };
};

zone "217.100.157.in-addr.arpa" {
type master;
file "217.100.157.in-addr.arpa.zone";
allow-update { none; };
};
```

Reiniciamos el servicio

service named restart

Probamos que el DNS funcione

Digitamos host juanxxiii.edu.ec 157.100.217.45 y debería respondernos así

```
[root@dns1 named]# host juanxxiii.edu.ec 157.100.217.45
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:

juanxxiii.edu.ec has address 157.100.217.45
juanxxiii.edu.ec mail is handled by 0 mail.juanxxiii.edu.ec.
[root@dns1 named]#
```

Anexo 5. Configuración del Servidor Firewall

Editamos el archivo ejecutable “reglas” que fue creado cuando configuramos el Router para agregarle las reglas de nuestro firewall.

Vi /etc/squid/juanxxiii/firewall/reglas

Y le añadimos las siguientes líneas:

```
#Creamos las siguientes variables
IPTABLES=/sbin/iptables
LAN1=192.168.0.0/255.255.255.0
LAN2=192.168.1.0/255.255.255.0

#Limpiamos reglas de iptables en todas las tablas
$IPTABLES –F          #Para liberar o limpiar cadenas
$IPTABLES –X          #Para borrar cadenas que han sido creadas
$IPTABLES –Z          #Para poner en ceros los contadores de bytes y de
paquetes
$IPTABLES -t nat –F  #Para borrar antiguas reglas

#Establecemos políticas por defecto y aceptamos todo
$IPTABLES -P INPUT ACCEPT         #Aceptamos  que entren paquetes a
nuestro firewall
$IPTABLES -P OUTPUT ACCEPT      #Aceptamos que salgan paquetes de
nuestro firewall
$IPTABLES -P FORWARD ACCEPT  #Enrutamos los paquetes por medio
del firewall a otra maquina


#Hacemos enmascaramiento de la red local y DMZ
#Que todos los paquetes que provengan de la red local y se dirijan al
Internet salgan por la Eth0 enmascarados con la IP pública
$IPTABLES -t nat -A POSTROUTING -s $LAN1 -o eth0 -j MASQUERADE
# Que todos los paquetes que provengan de la DMZ y se dirijan al Internet
salgan por la Eth0 enmascarados con la IP pública
$IPTABLES -t nat -A POSTROUTING -s $LAN2 -o eth0 -j MASQUERADE

# Aceptamos y redireccionamos peticiones hacia el DNS
iptables -A INPUT -i eth0 -p TCP --dport 53 -m state --state NEW -j
ACCEPT
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 53 -j DNAT --to
192.168.1.5:53
iptables -t nat -A PREROUTING -i eth0 -p udp --dport 53 -j DNAT --to
192.168.1.5:53
```

```
# Redireccionamos peticiones de correo entrante al servicdor de correo con
IMAP
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 25 -j DNAT --to
192.168.1.3:25

# Redireccionamos peticiones de correo entrante al servicdor de correo con
POP
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 110 -j DNAT --to
192.168.1.3:110

#Redirecionamos peticiones web desde cualquiera de las tres interfaces al
servidor web
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to
192.168.1.3:80
iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j DNAT --to
192.168.1.3:80
iptables -t nat -A PREROUTING -i eth2 -p tcp --dport 80 -j DNAT --to
192.168.1.3:80

#Aceptamos todas las conexiones al puerto 22/ssh  por la interfaz Eth0
para la conexión remota
$IPTABLES -A INPUT -p tcp -i eth0 --dport 22 -j ACCEPT

#Negamos conexiones al puerto 1863 para Messenger
$IPTABLES -A FORWARD -s $LAN -d 0/0 -p tcp --dport 1863 -j DROP
$IPTABLES -t nat -A PREROUTING -i eth1 -p tcp --dport 1863 -j
REDIRECT --to-port 8080
$IPTABLES -t nat -A PREROUTING -i eth1 -p tcp --dport 1863 -j
REDIRECT --to-port 8080
```

Guardamos los cambios con las teclas **Esc:** y digitamos **wq** para salir grabando.

Ejecutamos este script llamado “reglas” para actualizar el iptables desde la línea de comandos

```
./reglas
```

Anexo 6. Configuración del Servidor Proxy

Configuración de fichero squid.conf:

En este archivo se configuraron los parámetros básicos del servidor proxy, se crearon las listas de control de acceso lógicas, y las reglas de control de acceso al Internet.

Editamos el fichero squid.conf y agregamos lo siguiente:

Vi /etc/squid/squid.conf

Indicamos que el proxy escuchará peticiones en el puerto 3128.

http_port 3128

Asignamos 128 MB para cache de contenido en memoria RAM

cache_mem 128 MB

Asignamos 15 GB para cache de contenido en disco

cache_dir ufs /var/spool/squid 15000 16 256

Creamos las listas de control de acceso lógicas

```
#Listadas de Control de Acceso personalizadas
#
#Control de acceso a mesenger
acl messenger req_mime_type -i ^application/x-msn-messenger$
acl messenger req_mime_type -i ^application/pkix-crl$
acl msn_url url_regex -i gateway.dll
acl msn_port port 1863
acl msn_method method POST
#
#Listas de acceso de toda la institución
acl servidores src "/etc/squid/juanxxiii/listas/servidores"
acl adminred src "/etc/squid/juanxxiii/listas/adminred"
acl privilegiados src "/etc/squid/juanxxiii/listas/privilegiados"
acl rectores src "/etc/squid/juanxxiii/listas/rectores"
acl administra src "/etc/squid/juanxxiii/listas/administrativos"
acl profesores src "/etc/squid/juanxxiii/listas/profesores"
acl reservados src "/etc/squid/juanxxiii/listas/reservados"
acl wireless src "/etc/squid/juanxxiii/listas/wireless"
```

```
acl estudiantes src "/etc/squid/juanxxiii/listas/estudiantes"
#
#Control de acceso a sitios denegados y archivos denegados
acl sitiosdenegados url_regex
"/etc/squid/juanxxiii/restricciones/sitiosdenegados"
acl archivosnegados urlpath_regex
"/etc/squid/juanxxiii/restricciones/archivosnegados"
#
#Fin de las listas de control de acceso personalizadas
```

Como siguiente paso creamos las reglas de control de acceso para las listas anteriores

```
#Reglas de control de acceso Personalizadas
#
http_access allow rectores
http_access allow privilegiados
http_access deny messenger
http_access deny msn_method msn_url
http_access deny msn_port
http_access deny CONNECT msn_port
http_access allow servidores
http_access allow adminred
http_access allow administra passwd !sitiosdenegados !archivosnegados
http_access allow estudiantes passwd !sitiosdenegados
!archivosnegados
http_access allow wireless passwd !sitiosdenegados !archivosnegados
http_access allow passwd profesores passwd !sitiosdenegados
!archivosnegados
http_access allow reservados !sitiosdenegados !archivosnegados
http_access deny all
#
#Fin de Reglas de control de acceso Personalisadas
```

Guardamos los cambios con **Esc:** y digitamos **wq** para salir grabando

Creamos los ficheros de las listas de control de acceso anteriores

Creamos el fichero servidores y lo editamos

vim /etc/squid/juanxxiii/listas/servidores

#Direcciones IP para los servidores de la Zona Desmilitarizada
192.168.1.1 #Interfaz Eth1 del proxy
192.168.1.2 #Servidor de datos
192.168.1.3 #Servidor Web y correo
#192.168.1.4 #libre
192.168.1.5 #Servidor DNS

Pulsamos **ESC:** y digitamos **wq** para salir grabando

Creamos el fichero adminred y lo editamos

vim /etc/squid/juanxxiii/listas/adminred

#Direcciones IP para los administradores de la red
#Administrador de la red
192.168.0.2
#Soporte técnico de la red
192.168.0.4
#Libres
#192.168.0.5
#192.168.0.6
#192.168.0.7
#192.168.0.8
#192.168.0.9
#192.168.0.10

Pulsamos **ESC:** y digitamos **wq** para salir grabando

Creamos el fichero privilegiados y lo editamos

vim /etc/squid/juanxxiii/listas/privilegiados

#Direcciones IP de los usuarios que tienen acceso total y sin claves
#secretaria
192.168.0.20
#Colector
192.168.0.23
#Contador
192.168.0.24

Pulsamos **ESC:** y digitamos **wq** para salir grabando

Creamos el fichero rectores y lo editamos

vim /etc/squid/juanxxiii/listas/rectores

#Direcciones IP del área Directiva

#Rectorado
192.168.0.11
#192.168.0.12
#192.168.0.13
#Vicerrectorado
192.168.0.14
#192.168.0.15
#192.168.0.16
#Dirección de la Escuela
192.168.0.30
192.168.0.31
#192.168.0.32

Pulsamos **ESC:** y digitamos **wq** para salir grabando

Creamos el fichero administrativos y lo editamos

vim /etc/squid/juanxxiii/listas/administrativos

#Direcciones IP para el área Administrativa
#Inspección
192.168.0.17
#192.168.0.18
#192.168.0.19
#192.168.0.21
#192.168.0.22
#Libres para Colecturía
#192.168.0.25
#192.168.0.26
#Orientación
192.168.0.27
#192.168.0.28
#192.168.0.29
#Otros Departamentos
192.168.0.33 #Laboratorio de Química
#192.168.0.34
#192.168.0.35
#192.168.0.36
#192.168.0.37
#192.168.0.38
#192.168.0.39

Pulsamos **ESC:** y digitamos **wq** para salir grabando

Creamos el fichero profesores y lo editamos

vim /etc/squid/juanxxiii/listas/profesores

#Direcciones IP para el área Docente
#Desde
192.168.0.40
#hasta
#192.168.0.79

Pulsamos **ESC:** y digitamos **wq** para salir grabando

Creamos el fichero reservados y lo editamos

vim /etc/squid/juanxxiii/listas/reservados

Pulsamos **ESC:** y digitamos **wq** para salir grabando

Creamos el fichero reservados y lo editamos

vim /etc/squid/juanxxiii/listas/reservados

#Direcciones IP Reservadas para el crecimiento de la Intranet
#Desde
192.168.0.170
#Hasta
#192.168.0.239

Pulsamos **ESC:** y digitamos **wq** para salir grabando

Creamos el fichero wireless y lo editamos

vim /etc/squid/juanxxiii/listas/wireless

#Direcciones IP para los accesos de la red Inalámbrica
#Router 1
192.168.0.240
#Router 2
192.168.0.241
#Acces Point
192.168.0.242
#hasta
#192.168.0.245
#Acces Clientes
192.168.0.246
#hasta
#192.168.0.254

Pulsamos **ESC:** y digitamos **wq** para salir grabando

Creamos el fichero estudiantes y lo editamos

vim /etc/squid/juanxxiii/listas/estudiantes

#Direcciones IP para los laboratorios del Colegio y Escuela
#Laboratorio del Colegio
#Desde
192.168.0.80
#hasta
#192.168.0.139
#Laboratorio de la Escuela
#Desde
#192.168.0.140
#Hasta
#192.168.0.169

Pulsamos **ESC:** y digitamos **wq** para salir grabando

Creamos el fichero sitiosdenegados y lo editamos

vim /etc/squid/juanxxiii/listas/sitiosdenegados

#Sitios denegados
youtube.com
msn.com
hi5.com
www.mp3.com
www.mp4.com
www.porno.com
www.porta.net
playboy
entre otros

Pulsamos **ESC:** y digitamos **wq** para salir grabando

Creamos el fichero archivos negados y lo editamos

vim /etc/squid/juanxxiii/listas/archivosnegados

\.mp3
\.avi
\.mpeg
\.mp4
\.exe
\.pif
\.mpg
\.mpeg

\.mov
\.zip
\.sys
\.pif
\.lnk
\.ace
\.pps
\.bat
\.mbd
\.wav
\.wmv
\.wma
\.vob

Pulsamos **ESC:** y digitamos **wq** para salir grabando

Una vez configurado **squid.conf** y creadas todas las listas de control de acceso reiniciamos el servicio y listo

service squid restart

Anexo 7. Configuración del Servidor de Correo Electrónico

En la distribución CentOS 4 o White Box Enterprise Linux 4, el paquete imap es reemplazado por el paquete dovecot. De tal modo que se ejecuta lo siguiente.

```
yum -y install sendmail sendmail-cf dovecot m4 make cyrus-sasl cyrus-
sasl-md5 cyrussasl-plain
```

Creamos las cuentas de usuario y asignamos las claves de acceso

```
useradd -s /sbin/nologin fpajila
```

Autenticamos SNMP a través de los protocolos IMAP y POP3

```
passwd fpajila
```

Asignamos la clave de acceso para autenticar SMTP a través de métodos cifrados (CRAM-MD5 y DIGEST-MD5) en sistemas con versión de Sendmail compilada contra SASL-2

```
saslpasswd2 fpajila
```

Luego asignamos la misma clave para autenticar SMTP a través de métodos cifrados (CRAM-MD5 y DIGEST-MD5) en sistemas con versión de Sendmail compilada contra SASL-1

```
saslpasswd fpajila
```

Para la autenticación con SMTP usando cualquier mecanismo se requiere iniciar y activar el servicio de saslauthd:

```
chkconfig saslauthd on
service saslauthd start
```

Editamos el siguiente archivo para establecer los dominios a administrar

```
vi /etc/mail/relay-domains
juanxxiii.edu.ec
mail.juanxxiii.edu.ec
```

Guardamos con wq y salimos

Establecer dominios permitidos para poder enviar correo:

vi /etc/mail/relay-domains
juanxxiii.edu.ec
mail.juanxxiii.edu.ec

Guardamos con **wq** y salimos

Editamos el siguiente archivo para definir el control de acceso

vi /etc/mail/access
192.168.1.4 RELAY #Agregamos esta línea con la dir IP del servidor

Editamos este archivo sendmail.mc para definir las funciones:

vi /etc/mail/sendmail.mc

De manera predefinida Sendmail escucha peticiones a través IPv4 (127.0.0.1) y no a través de otros dispositivos de red y para poder recibir correo desde Internet o la LAN modificamos esta línea:

DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dnl
y le dejamos así:

DAEMON_OPTIONS(`Port=smtp, Name=MTA')dnl

Segundo se recomienda desactivar FEATURE(`accept_unresolvable_domains')dnl con el fin de impedir aceptar correo de dominios inexistentes (generalmente utilizado para el envió de correo masivo no solicitado o Spam), y para ello lo comentamos poniendo dnl al inicio así:

dnl FEATURE(`accept_unresolvable_domains')dnl

Tercero habilitar las siguientes líneas y adaptar valores para definir la máscara que utilizara el servidor:

MASQUERADE_AS(`juanxxiii.edu.ec')dnl
FEATURE(masquerade_envelope)dnl

```
FEATURE(masquerade_entire_domain)dnl
```

Cuarto agregamos al final un parámetro que defina que juanxxiii.edu.ec se trata de un dominio local.

```
Cwjuanxxiii.edu.ec
```

Al final guardamos el archivo presionando **Esc:** y digitando **wq**.

Luego como el paquete imap es reemplazado por dovecot, el cual funciona como otros servicios. Se debe modificar el fichero /etc/dovecot.conf y habilitar los servicios de imap y/o pop3 así:

```
vi /etc/dovecot.conf #Editamos este archivo
protocols = imap pop3
```

Guardamos el archivo presionando **Esc:** y digitando **wq**.

Después agregamos este servicio al arranque del sistema y lo iniciamos

```
chkconfig dovecot on
service dovecot start
```

Para finalizar reiniciamos el servicio de Sendmail

```
service sendmail restart
```

y probamos el servidor enviando o recibiendo mensajes con cualquier cliente estándar de correo electrónico con soporte para POP3/IMAP/SMTP con soporte para autenticar a través de SMTP utilizando los métodos DIGEST-MD5 o CRAM-MD5.

Anexo 8. Configuración de la autenticación con el módulo NSCA de Squid.

Creamos el fichero “passwordsquid” en la siguiente ruta:

```
touch /etc/squid/juanxxiii/claves/passwordsquid
```

Para administrar estas claves desde el servidor web este fichero debe hacerse leíble y escribible solo para el usuario squid.

```
chmod 600 /etc/squid/claves
chown squid:squid /etc/squid/claves
```

Creamos las cuentas necesarias con htpasswd que viene incluida con httpd.

```
htpasswd /etc/squid/juanxxiii/claves/passwordsquid secretaria
```

Lo anterior solicitara teclear una nueva clave de acceso para el usuario secretaria y confirmar tecleando está de nuevo. Debemos repetir esto con el resto de las cuentas que requiera dar de alta. Estas cuentas son exclusivas solo para acceso al proxy.

Configuramos los Parámetros necesarios en /etc/squid/squid.conf

Indicamos a squid que programa de autenticación se utilizará, para ello ubicamos la siguiente línea y le indicamos en que fichero se encuentran almacenadas las claves.

```
auth_param basic program /usr/lib/squid/ncsa_auth
/etc/squid/juanxxiii/claves/passwordsquid
```

Definimos la lista de control de acceso denominada passwd la cual se configurará para utilizar obligatoriamente la autenticación para poder acceder a Squid.

```
acl passwd proxy_auth REQUIRED
```

Luego en las reglas de control de acceso ya definidas anteriormente le agregamos el nombre del la acl para que ese usuario o grupo de usuarios se conecten con la clave de acceso. Por ejemplo todos los usuarios inalámbricos deben logearse.

```
http_access allow wireless passwd
```

Reiniciamos el servicio de squid y listo

```
service squid restart
```

APENDICES

Apéndice 1. Glosario de ttérminos técnicos

CSMA/CD

Acceso Múltiple por Detección de Portadora con Detección de Colisiones"), es una técnica usada en redes Ethernet para mejorar sus prestaciones.

DMZ

En seguridad informática, una zona desmilitarizada o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa -- los equipos (hosts) en la DMZ no pueden conectar con la red interna.

Direct Sequence Spread Spectrum

El espectro ensanchado por secuencia directa también conocido en comunicaciones móviles como DS-CDMA, es uno de los métodos de modulación en espectro ensanchado para transmisión de señales digitales sobre ondas radiofónicas que más se utilizan.

EIA/TIA 568-A

TIA/EIA-568-B tres estándares que tratan el cableado comercial para productos y servicios de telecomunicaciones. Los tres estándares oficiales: ANSI/TIA/EIA-568-B.1-2001, -B.2-2001 y -B.3-2001.

Formación On line (E-Learning).

El e-learning es educación a través de correo electrónico o a distancia en el que se integra el uso de las tecnologías de la información y otros elementos pedagógicos (didácticos) para la formación, capacitación y enseñanza de los usuarios o estudiantes en línea.

FTP.

FTP (sigla en inglés de File Transfer Protocol) en informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor.

Full dúplex

La mayoría de los sistemas y redes de comunicaciones modernos funcionan en modo dúplex permitiendo canales de envío y recepción simultáneos.

Half dúplex

Half-duplex o semidúplex, significa que el método o protocolo de envío de información es bidireccional pero no simultáneo.

ICMP

Protocolo de Mensajes de Control y Error de Internet, este protocolo solamente lo utilizamos cuando hacemos envío de paquetes de un máquina a otra, en resumen es un ping.

IDF

Instalación de distribución intermedia. Recinto de comunicación secundaria para un edificio que usa una topología de red en estrella. El IDF depende del MDF.

IEEE

Corresponde a las siglas de (Institute of Electrical and Electronics Engineers), esuna asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas.

Infrarrojos

La radiación infrarroja, radiación térmica o radiación IR es un tipo de radiación electromagnética de mayor longitud de onda que la luz visible, pero menor que la de las microondas.

Iptables

El componente más popular construido sobre Netfilter es iptables, una herramientas de cortafuegos que permite no solamente filtrar paquetes, sino también realizar traducción de direcciones de red (NAT) para IPv4 o mantener registros de log.

MDF

Instalación principal de distribución principal. Recinto de comunicación primaria de un edificio. El Punto central de una topología de networking en estrella donde están ubicados los paneles de conexión, el hub y el router.

PoE

La alimentación a través de Ethernet (Power over Ethernet, PoE) es una tecnología que incorpora alimentación eléctrica a una infraestructura LAN estándar. Permite que la alimentación eléctrica se suministre al dispositivo de red como, por ejemplo, un teléfono IP o una cámara de red, usando el mismo cable que se utiliza para una conexión de red.

Radio Frecuencia.

El término radiofrecuencia, también denominado espectro de radiofrecuencia o RF, se aplica a la porción menos energética del espectro electromagnético, situada entre unos 3 Hz y unos 300 GHz.

TCP/IP.

Hace referencia a los dos protocolos más importantes que la componen: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP), que fueron los dos primeros en definirse, y que son los más utilizados de la familia.

Transmisión en banda base

En Telecomunicaciones, el término banda base se refiere a la banda de frecuencias producida por un transductor, tal como un micrófono, un

manipulador telegráfico u otro dispositivo generador de señales que no es necesario adaptarlo al medio por el que se va a trasmitir.

UDP

Protocolo de Datagrama de Usuario, sirve para el envía de datagrama pero debe existir una conexión establecida.

Wi-Fi

Es una marca de la Wi-Fi Alliance, la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11 relacionados a redes inalámbricas de área local.

WEP

Es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite.

WPA

WPA adopta la autenticación de usuarios mediante el uso de un servidor, donde se almacenan las credenciales y contraseñas de los usuarios de la red.

WWW.

World Wide Web, cuya traducción podría ser Red Global Mundial es un sistema de documentos de hipertexto o hipermedios enlazados y accesibles a través de Internet

INDICE DE FIGURAS

INDICE DE TABLAS