



UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

**"MIGRACIÓN DE REDES DE DATOS CON NORMAS
ETHERNET, CABLEADO ESTRUCTURADO Y
COMUNICACIONES WIRELESS"**

T E S I S

Que para obtener el título de

INGENIERO EN COMPUTACIÓN

Presentan

Gabriela Maldonado García

Luis Octavio Rivera Valderrama



Director de Tesis: Ing. Noé Cruz Marín

Ciudad Universitaria, D.F., 2006



Universidad Nacional
Autónoma de México

Dirección General de Bibliotecas de la UNAM

Biblioteca Central



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

AGRADECIMIENTOS

Agradezco a mis Padres Victor y Guillermina por todo el apoyo brindado incondicionalmente desde siempre. Con este trabajo les expreso que gracias a ustedes puedo terminar esta etapa de la vida.

Agradezco a mis Hermanos Victor y Vero por ser parte de este apoyo recibido y por toda la ayuda que recibí de ustedes.

Agradezco a mi Familia por brindarnos su ayuda en épocas difíciles y por convivir excelentes momentos.

Agradezco a todos mis Compañeros y Amigos que he ido conociendo a través de mi vida; siento no poder mencionarlos a todos por temor de olvidar a alguno.

Agradezco a la UNAM, a la Facultad de Ingeniería y a mis Profesores por todos los conocimientos brindados para poder desarrollarme profesionalmente.

Y por último, pero no menos importante, agradezco a Dios por permitirme llegar a este momento importante y poder compartirlo con todos mis seres queridos.

Luis Octavio

AGRADECIMIENTOS

A la vida.

A mi familia, por ser la fuente de motivación e inspiración, por el apoyo incondicional durante toda mi vida, y más aún, por ser mi familia.

A mis profesores por hacer de estas instalaciones la segunda mejor casa, por guiarme con ahínco en la búsqueda e inquietud de retos constantes.

A la Facultad de Ingeniería por la formación gloriosa bajo su manto energético que a ella singulariza.

A la UNAM por proveerme de valiosos conocimientos para cumplir con el compromiso moral y social ante mi país.

Gabriela Maldonado García

DEDICATORIA

El presente trabajo lo dedico a mis padres, pues con su fortaleza, tenacidad y perseverancia aunadas a la confianza que han depositado en cada una de mis decisiones, han sido siempre sumamente importantes en mi vida. En particular, doy gracias a la madre más mala del mundo: mi madre. A ella, por ser una persona completa, un gran ejemplo a seguir.

Asimismo, a mis hermanos, a cada uno de ellos que han sido una luz en mi vida. Cada uno, elemento esencial de este gran equipo.

Por último, y con igual importancia, a mis amigas y amigos por ser camaradas de esta fase. Gracias por apoyar y avivar mis acciones en el continuo ascenso de esta cúspide.

Gabriela Maldonado García

ÍNDICE

I. INTRODUCCIÓN	i
I.I ¿Qué es el Sistema de Universidad Abierta-UNAM?	ii
Funcionamiento de la modalidad de Educación a Distancia	iii
Características de la Educación en Línea	iv
I.II División de Universidad Abierta de la Facultad de Derecho en la actualidad	v
Necesidades de la DUAD	v
Uso de la Tecnología en la Educación a Distancia	v
I.III Objetivo y alcances	vi
1. CONCEPTOS BÁSICOS	1
1.1. Red de datos	2
Definición de red de datos	2
1.1.1. Redes alámbricas	3
LAN	3
MAN	3
WAN	3
1.1.2. Redes inalámbricas	4
W-PAN	4
W-LAN	4
W-WAN	5
1.1.3. Topología	5
Bus	6
Anillo	7
Estrella	7
Árbol	8
1.1.4. Medios de transmisión guiados	8
Coaxial delgado	9
Coaxial grueso	9
Par trenzado	10
Fibra óptica (FDDI)	12

1.1.5.	Medios de transmisión no guiados	14
	Infrarrojos	14
	Radio frecuencia	15
	Microondas	16
1.2.	Modelo OSI	16
1.2.1.	Antecedentes	17
1.2.2.	¿Qué es el modelo OSI?	17
1.2.3.	Capas del modelo OSI	18
1.3.	Modelo TCP/IP	20
1.3.1.	¿Qué es el modelo TCP/IP?	20
1.3.2.	Capas del modelo TCP/IP	21
1.4.	Protocolos	23
1.4.1.	Protocolo TCP	23
1.4.2.	Protocolo IP	24
1.4.3.	Protocolo X.25	24
1.4.4.	Protocolo IPX/SPX	25
1.5.	Estándares	26
1.5.1.	IEEE	26
	802.3	26
	802.11	32
1.5.2.	FDDI	34
1.5.3.	ATM	36
1.5.4.	Frame relay	38
1.6.	Dispositivos activos usados en la red	39
1.6.1.	Repetidor	39
1.6.2.	Hub	39
1.6.3.	Bridge	39
1.6.4.	Switch	40
1.6.5.	Router	40
1.6.6.	Gateway	41

1.7.	Diseño de redes de datos	41
1.7.1.	Diseño de redes de cómputo	42
	Consideraciones técnicas	42
	Diseño de interconexión entre topologías	43
	Evaluación de servicio de distribución	45
	Evaluación de servicio de acceso local	45
1.7.2.	Identificación y selección de los dispositivos de red	46
1.8.	Sistemas operativos de red para servidor y clientes	48
	Sistemas operativos para clientes	48
	Sistemas operativos para servidor de archivos	55
	Sistemas operativos para servidor de web y base de datos	56
1.9.	Políticas de red	57
1.10.	Herramientas de mantenimiento y monitoreo de una red de datos	65
2.	CABLEADO ESTRUCTURADO	67
2.1.	Historia del cableado estructurado	68
2.1.1.	Definición del cableado estructurado	68
2.1.2.	Diferencias entre el cableado estructurado y no estructurado	68
2.2.	Estándares en los sistemas de cableado estructurado	70
2.2.1.	ANSI/TIA/EIA 568-A estándar de cableado de telecomunicaciones en edificios comerciales	71
2.2.2.	ANSI/TIA/EIA 569 Estándar para ductos y espacios de telecomunicaciones en edificios comerciales	81
2.2.3.	EIA/TIA 570 Estándar de alambrado de telecomunicaciones residencial y comercial pequeño	91
2.2.4.	EIA/TIA 606 Estándar de administración para infraestructura de telecomunicaciones en edificios comerciales	93
2.2.5.	EIA/TIA 607 Requerimientos de puesta a tierra para telecomunicaciones	99
2.3.	Consideraciones de diseño	103
2.4.	Elección de elementos activos	104
2.5.	Documentación de la red	107

3.	REDES INALÁMBRICAS	109
3.1.	Introducción	110
3.2.	Topologías WLAN	112
3.3.	Control de acceso al medio	116
3.4.	Especificación del medio	117
3.5.	Sistemas de redes infrarrojas	118
3.6.	Sistema de radiofrecuencia	119
3.7.	Estándar 802.11	120
3.7.1.	802.11a	121
3.7.2.	802.11b	121
3.7.3.	802.11g	122
4.	CASO: DIVISIÓN DE UNIVERSIDAD ABIERTA DE LA FACULTAD DE DERECHO (DUAD)	123
4.1.	Introducción	124
4.2.	BackBone de la UNAM	124
4.2.1.	Red de cómputo actual del edificio de la DUAD	128
4.3.	Metodologías de análisis	130
4.3.1.	Metodología utilizada por DGSCA	130
4.3.2.	Metodología propuesta	131
4.4.	Estado de la red de cómputo de la DUAD	134
4.4.1.	Equipo de cómputo actual	135
4.4.2.	Equipo de red actual	136
4.4.3.	Topología utilizada actualmente	137
4.4.4.	Estadísticas del funcionamiento de la red de datos	139
Análisis del tráfico que circula por la red	139	
Monitoreo de la red	142	
4.4.5.	Deficiencias encontradas	142
4.5.	Propuesta para la red de datos de la DUAD	143
4.5.1.	Necesidades del usuario	144
4.5.2.	Diseño y planeación de la migración de la red	144
4.5.3.	Áreas, edificios y pisos de la Facultad de Derecho y de la División de Universidad Abierta de la Facultad de Derecho	151
4.5.4.	Especificaciones de los elementos activos	153

4.5.5. Especificaciones de los elementos pasivos	154
4.5.6. Especificaciones del cableado	155
4.5.7. Especificación de los puntos de acceso	157
4.5.8. Servidores de red	159
4.5.9. Sistemas operativos de red para servidor y clientes	161
4.6. Análisis de la propuesta	163
4.7. Análisis de costos	167
4.8. Relación costo beneficio	168
4.9. Propuesta de las políticas de administración de la red de datos para la División de Universidad Abierta de la Facultad de Derecho	169
CONCLUSIONES	175
ANEXOS	178
Anexo A	179
Anexo B	182
Anexo C	183
GLOSARIO	184
BIBLIOGRAFIA Y MESOGRAFÍA	195

I. Introducción

El incesante esfuerzo de la sociedad por encontrar nuevas formas educativas que satisfagan las exigencias sociales, científicas y tecnológicas del momento actual y del futuro en el nivel universitario, ha venido desarrollando, entre otros, los sistemas de educación abierta y a distancia, modelos que se complementan y entrecruzan. Esta alternativa en la enseñanza superior representa una importante innovación en el proceso de enseñanza – aprendizaje.

Es aquí en donde el hombre encuentra su derecho a programar su tiempo en función de sus intereses, participar activamente en su formación, auto instruirse, y responsabilizarse de su aprendizaje.

En febrero de 1975 tuvo sus comienzos la División de Universidad Abierta de la Facultad de Derecho (DUAD) como una alternativa académica para formar profesionales de la ciencia jurídica y extender la educación universitaria a más amplios sectores de la población. Así como, desahogar la alta demanda que siempre ha tenido la carrera de Licenciado en Derecho.

Establecida oficialmente en el año de 1975 con fundamento en el Estatuto del Sistema de Universidad Abierta, aprobado en sesión del Consejo Universitario del 25 de febrero de 1972, la División de Universidad Abierta de la Facultad de Derecho en la UNAM, abrió sus puertas para atender las demandas de la población que por sus características, no podía aspirar a tener una carrera profesional basada en los sistemas tradicionales de estudio.

I.I ¿Qué es el Sistema de Universidad Abierta-UNAM?

El 25 de febrero de 1972, durante el período del entonces Rector de la Universidad Nacional Autónoma de México, Dr. Pablo González Casanova, mediante la aprobación del Consejo Universitario, surge el Sistema de Universidad Abierta (SUA). La idea que lo ha sustentado desde entonces es, la de crear núcleos de enseñanza superior en los recintos universitarios y en los centros de producción, además de ampliar las oportunidades de estudios a los trabajadores que dispongan de tiempo suficiente para efectuar las actividades académicas exigidas en los planes de estudio de las carreras ofrecidas.

El SUA se caracteriza por concebirse como un planteamiento de impartición de enseñanza que permita entender la educación desde una perspectiva más flexible, con el propósito de alcanzar un proceso de intercomunicación donde el contenido no se transmite sino se genera.

La Coordinación de Universidad Abierta y Educación a Distancia es la entidad universitaria encargada de fortalecer el desarrollo de la Educación Abierta, Continua y a Distancia de la Universidad Nacional Autónoma de México.

Su objetivo fundamental consiste en extender la educación dentro y fuera de la UNAM.

Sus programas estratégicos son:

- Uso de medios y tecnologías para la Educación Abierta y a Distancia.
- Fortalecimiento y expansión de la Educación Abierta y a Distancia.
- Universidad en línea.
- Educación Continua a Distancia.
- Recursos humanos para la Educación a Distancia.
- Calidad de la educación.

La Dirección de Sistema Universidad Abierta, la Dirección de Educación Continua y la Dirección de Educación a Distancia, cada una de ellas cuenta con programas específicos que interactúan entre sí en la combinación de metodologías educativas y recursos tecnológicos para ofrecer diversas oportunidades de educación universitaria. Estas diversas modalidades educativas son flexibles, dinámicas y basadas en la calidad académica, y responden a las circunstancias personales de los estudiantes y sus necesidades particulares de aprendizaje.

¿ Funcionamiento de la modalidad de Educación a Distancia

Conscientes de la necesidad de estar al día en las innovaciones tecnológicas que permitan la difusión de clases y tutorías en redes de cómputo, para generar un sistema más eficiente de educación abierta y a distancia, se hizo necesaria la incorporación de las nuevas Tecnologías de la Información y la Comunicación (TIC's), con fines educativos y formativos. Lo que llevó a crear el modelo pedagógico de la modalidad educativa: educación a distancia.

La educación a distancia es una alternativa para los alumnos inscritos en el sistema abierto e incorpora medios tecnológicos que facilitan funciones de aprendizaje como: leer, compartir, observar, simular, discutir, etcétera.

La educación a distancia es un sistema de impartición de formación a distancia, apoyado en las TIC's (tecnología, redes de telecomunicaciones, videoconferencias, TV digital, materiales multimedia), que combinan distintos elementos pedagógicos: la instrucción directa clásica (presencial o de autoestudio), las prácticas, los contactos en tiempo real (presenciales, videoconferencia o chats) y los contactos diferidos (tutores, foros de debate, correo electrónico).¹

Una novedad que las Tecnologías de la Información y la Comunicación han aportado a la educación a distancia clásica son los conceptos de formación sincrónica y asíncrona. Tradicionalmente la educación a distancia ha sido asincrónica, es decir, el formador y los alumnos aprenden en lugares distintos y en tiempos diferentes. Una novedad que han introducido las TIC's ha sido la posibilidad de desarrollar una formación sincrónica, en la que formadores y alumnos se escuchan, se leen y/o se ven en el mismo momento independientemente de que se encuentren en espacios físicos diferentes.

La Educación a Distancia considera innovadores modelos educativos en donde la educación será entendida como un programa sin límite de edad ni espacio. Mediante programas flexibles de enseñanza pretende fortalecer la educación superior en el país para promover el desarrollo de la educación no presencial.

¹ <http://prometeo.us.es/idea/mie/pub/marcelo/Formando%20Teleformadores.pdf>. Pag 1.

¿ Características de la Educación en Línea

A lo largo del planeta, las Instituciones privadas y públicas han enfocado sus esfuerzos hacia la educación a distancia, en donde, sin que el alumno asista a un salón y con base en los principios bajo los que funciona el Sistema Abierto, tomen asesorías, realicen consultas, compartan discusiones y debates sobre diversos tópicos, por medio de los cuartos de conversación (chatrooms), programas de mensajería instantánea, foros y grupos de discusión, audio y videoconferencia, mencionados sólo por destacar algunos.

De ahí que se considere la importancia de reforzar al Sistema Abierto con la educación en línea, primero, como un soporte para fortalecer la enseñanza de la División y después, como la opción de Sistema de Educación a Distancia, para que junto con el Sistema Abierto y el Sistema Tradicional capten la gran demanda que la carrera ha tenido históricamente.

La educación en línea se trata de una modalidad de formación que permite utilizar las potencialidades de la red para acercar la formación a sus posibles usuarios.

La educación en línea es un ambiente creado en Web en el que los estudiantes y educadores pueden llevar a cabo tareas de aprendizaje. No es solo un mecanismo para distribuir la información a los estudiantes; también supone tareas relacionadas con la comunicación, evaluación de los alumnos y la gestión de la clase. Algunas de las características más importantes de la formación a través del Internet son:

- Interactiva.
- Multimedia.
- Sistema abierto.
- Búsqueda on-line.
- Independencia de espacio, tiempo y dispositivo.
- Publicación electrónica.
- Comunicación intercultural.
- Multiplicidad de expertos.
- El alumno controla su aprendizaje.
- Facilidad de desarrollo y mantenimiento de cursos.
- Autonomía.

Los formadores proporcionan apoyo, retroalimentación y orientación vía comunicación sincrónica y asincrónica, lo que la hace ser interactiva.

I.II División de Universidad Abierta de la Facultad de Derecho en la actualidad

El funcionamiento de la DUAD se caracteriza por la proposición de innovaciones pedagógicas para la enseñanza y aprendizaje del Derecho, de manera que sus egresados como litigantes, juristas, legisladores, jueces, docentes o investigadores sean capaces de perfeccionarse y actualizarse constantemente en beneficio de la sociedad.

Actualmente, únicamente se da la modalidad de educación abierta, existen asesorías grupales los días sábados, para que el alumno pueda contar con un tutor que cubra la labor de orientación y guía que se requiere para aprovechar la información adquirida.

¶ Necesidades de la DUAD

En la actualidad, la DUAD se ha visto en la necesidad de diversificar la oferta educativa a través de la educación a distancia y virtual, mediante la gestión, coordinación y colaboración con organismos para ofrecer programas flexibles que no requieran la presencia en tiempo ni espacio y permita atender a la población demandante en distintas regiones de la entidad. Sus objetivos son formar equipos interdisciplinarios que puedan diseñar y producir programas académicos de calidad y que sean alternativa de educación flexible, innovadora, creativa, orientada a la construcción de nuevos ambientes de aprendizaje apoyado en una infraestructura física y tecnológica que permita la incorporación de nuevas Tecnologías de la Información y Comunicación.

Para alcanzar sus objetivos, la DUAD reconoce la importancia de la tecnología de las redes de datos, y la necesidad de construir soporte académico y tecnológico para educar a un número mayor de personas, educar con mejor y mayor eficacia y con menor cantidad de recursos.

La DUAD pretende incorporar en los ambientes de aprendizaje y áreas de trabajo, el desempeño de colaboración en redes de información y de comunicación, ya que la tecnología no es sólo una herramienta sino se integra como componente para la educación.

¶ Uso de las tecnologías en la Educación a Distancia

Las Tecnologías de la Información y la Comunicación utilizadas como apoyo o soporte para el desarrollo de actividades educativas, como: redes de computadoras, sistemas automatizados de información, audio, video digital, multimedia, etc., tienen como objetivo, proporcionar a la comunidad de Educación a Distancia servicios de cómputo y

comunicaciones cuyas características permitan definir, apoyar y enriquecer los modelos y planes académicos.

Algunas de las tecnologías y servicios que apoyan al funcionamiento de la Educación a Distancia son: videoconferencia, audio y video digital, internet, portal de servicios educativos, software educativo, audio y video por demanda, transmisión en línea, correo electrónico, foros de discusión, chat, etcétera.

I.III Objetivos y alcances

Con la presente tesis se pretende alcanzar los siguientes objetivos:

1. Rediseñar la red de datos de la División de Universidad Abierta de la Facultad de Derecho de la UNAM para satisfacer las necesidades tecnológicas de comunicaciones presentes y futuras considerando las tecnologías de alta velocidad que se están implantando en la actualidad.
2. Eliminar los problemas que se presentan actualmente al analizar el funcionamiento actual de la red de datos de la DUAD.
3. Proponer políticas de administración para la red de datos de la DUAD para un mejor manejo de los recursos de la misma, y cumpla con los lineamientos de la DGSCA.

Con el cumplimiento de los objetivos antes mencionados, se espera que el rediseño de la red de datos funcione correctamente por lo menos 5 años después de su implantación. Además de la disposición de la información y los recursos, así como, un ordenado crecimiento de dicha red y el uso adecuado de los recursos por parte de los usuarios.

Con la consecución del rediseño de la red de datos de la DUAD, se fortalece el proyecto del nuevo backbone de Red UNAM para robustecer la red de la Universidad con infraestructura de punta y asegurar su integración a la nueva red de Internet 2 nacional e internacional. Esta actualización contempla tecnología de vanguardia en materia de telecomunicaciones garantizando una red suficientemente robusta que proporcione mayor velocidad y calidad de transmisión, mayor flexibilidad e incremente la accesibilidad de la información, actual y de futuro próximo, a todo el personal que compone dicha Institución.

Capítulo 1

Conceptos Básicos

Las redes constituyen sistemas coherentes de interconexión de dispositivos independientes que trabajan en conjunto y permiten compartir información y recursos. Las redes deben cumplir una serie de estándares nacionales e internacionales para su implementación. Deben ser capaces de evolucionar de acuerdo a las necesidades cambiantes del sistema integrado de comunicación; por lo cual, es importante la consideración de la tecnología que conforma una red.

1.1. Red de datos

En la actualidad la red de datos en una organización es una inversión a largo plazo que asegura el acceso a la información de cualquier índole, interna o externa, que si bien, es su segundo activo más importante.

Definición de red de datos

Las redes de datos son un conjunto de computadoras, equipos de comunicaciones y otros dispositivos que se pueden comunicar entre sí a través de un medio en particular. Un sistema constituido por una unidad de control y muchos esclavos no es una red.

Objetivos de una red:

- Comunicar.
- Reducir costos.
- Aumentar la disponibilidad de la información.
- Ahorrar tiempo.
- Compartir recursos:
 - Físicos. Impresora, plotters, módem, etcétera.
 - Lógicos. Programas, datos, información, etcétera.

Las redes podemos clasificarlas de acuerdo a su tecnología de transmisión.

- Redes de Difusión (Broadcasting)

Existe un sólo canal o medio de comunicación que es compartido por todos los dispositivos de la red. Es decir, que se envía un paquete a todos los destinos colocando un código especial en el campo de dirección; cuando se transmite un paquete con este código, cada maquina en la red lo recibe y lo procesa.

- **Redes de Punto-a-Punto**

Consiste en múltiples conexiones entre pares individuales de máquinas. Para poder enviar un paquete de origen a destino, éste debe visitar primero una o más máquinas intermedias; para ello los algoritmos de ruteo desempeñan un papel muy importante en las redes punto-a-punto.

1.1.1. Redes alámbricas

Las redes alámbricas utilizan como medio de transmisión diferentes tipos de cables (cobre o fibra óptica) ya sea para comunicarse a otras redes o para unir sus nodos.

De acuerdo a su alcance se clasifican de la siguiente forma:

- **LAN (Local Area Network)**

Una red de área local LAN puede definirse como un sistema de comunicaciones que proporciona interconexión a una variedad de dispositivos en un área restringida (recinto, campus, etc.) y que no utilizan medios de telecomunicaciones externos. Se caracterizan por tres factores: extensión (de unos cuantos metros hasta algunos kilómetros), su tecnología de transmisión (cable de par trenzado UTP o coaxial, fibra óptica, portadoras con infrarrojo o láser, radio y microondas en frecuencias no comerciales) y su topología (anillo, bus, estrella, árbol e híbridas).

- **MAN (Metropolitan Area Network)**

Las redes MAN pueden ser vistas como una red LAN en cuanto a topología y medios de transmisión; pero de mayor alcance y normalmente se basan en una tecnología similar un poco más robusta.

Este tipo de redes MAN llegan a tener un alcance que va desde los 10 Km hasta abarcar una ciudad. En general cualquier red de datos, voz o video con una extensión de una a varias decenas de kilómetros puede ser considerada una MAN.

- **WAN (Wide Area Network)**

Una red WAN es una red de comunicación de datos que tiene una cobertura geográfica relativamente grande y suele utilizar las instalaciones de transmisión que ofrecen las compañías portadoras de servicios como son las telefónicas. A la infraestructura que une los

nodos de usuarios se le llama subred y abarca diversos equipos de red (llamados routers o ruteadores) y líneas de comunicación que unen las diversas redes. Sus alcances van desde a nivel país hasta continentes

1.1.2. Redes Inalámbricas

Las redes inalámbricas nos brindan la posibilidad de conectarnos a una red pública o privada sin el uso de cables. Nos ofrece la posibilidad de navegar por Internet, conectarse a la red privada de su empresa o consultar su correo personal desde aeropuertos, hoteles, o incluso mientras se está sentado en la playa o al volante de su coche. Las redes inalámbricas proporcionan a los usuarios finales la posibilidad de trabajar desde casi cualquier parte y a cualquier hora.

Las redes inalámbricas pueden dividirse en tres categorías: redes de área personal (PAN), redes de área local (LAN) y redes de área amplia (WAN).

- **W-PAN** (Wireless - Personal Area Network): Blue tooth

La tecnología Bluetooth se utiliza en el entorno de red de área personal en muchos tipos de dispositivos, desde PDA a automóviles.

Bluetooth permite la comunicación en todas direcciones a una velocidad de 1 Mbps con un alcance de 9.14 m. Esta tecnología es muy usada para compartir archivos y periféricos y comunicarse entre dispositivos que utilicen la misma tecnología¹ (figura 1.1).

- **W-LAN** (Wireless – Local Area Network)

El espacio para de la red inalámbrica LAN se mide por decenas de metros y abarca cualquier entorno en recintos, como edificios de oficinas, escuelas, aeropuertos, hoteles o cualquier espacio público. La opción tecnológica es la LAN de tecnología inalámbrica 802.11b de IEEE; pero 802.11a tiene una buena posición y la 802.11g también es un excelente estándar (figura 1.1).

¹ Introducción a IBM ThinkVantage Technologies, Soluciones IBM Wireless seguras.

- **W-WAN** (Wireless – Wide Area Network)

El espacio de la red inalámbrica WAN se mide por kilómetros y funciona casi en cualquier parte. La conectividad es a través de un teléfono móvil o una PC Card de un ordenador. W-WAN tiene la capacidad de proporcionar velocidades de hasta 144 Kbps (figura 1.1).

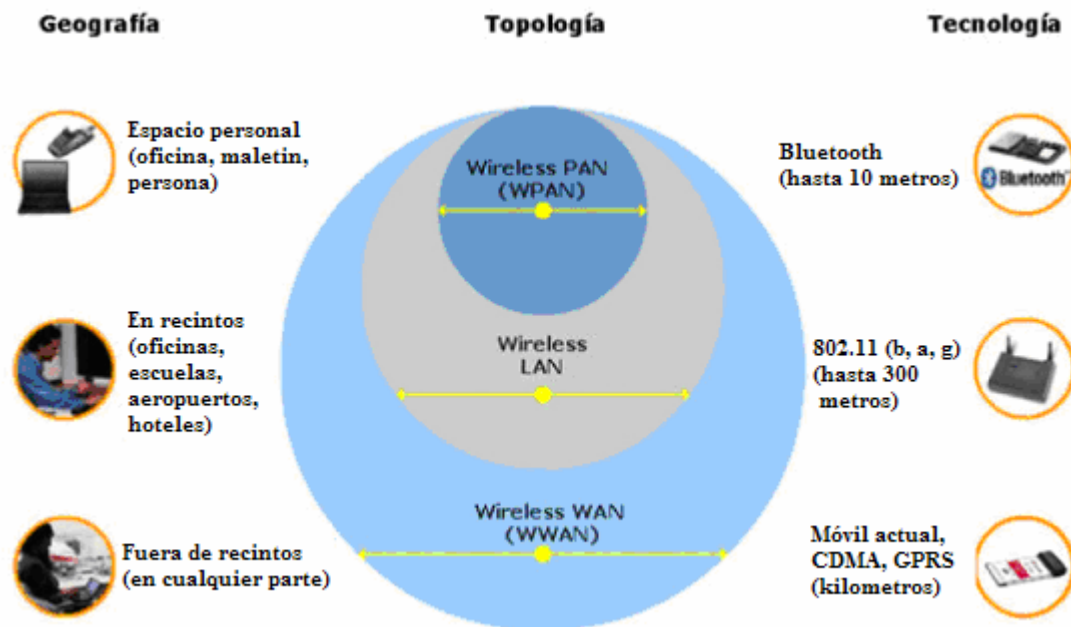


Figura 1.1 Redes Inalámbricas

1.1.3. Topología

La topología de una red es la forma en que se constituye físicamente la red, es decir la distribución del cable que interconecta los diferentes ordenadores. A la hora de instalar una red es importante seleccionar la topología más adecuada a las necesidades existentes. Para esto hay que tener en cuenta los siguientes factores:

- La distribución de los equipos a interconectar.
- La inversión que se quiere hacer.
- El costo del mantenimiento y la actualización de la red.
- La confiabilidad de la red.
- La tecnología a utilizar.

A continuación se explicarán las topologías típicas.

Topología en BUS

La topología en BUS, consta de un único cable que se extiende de una computadora a la siguiente en forma de serie. Los extremos del cable se terminan con una resistencia denominada terminador, que además de indicar que no existen más computadoras en el extremo, permite cerrar el BUS.

Sus ventajas son las siguientes:

- Fácil instalación y mantenimiento.
- Es económico.
- No existen elementos centrales de los que dependa toda la red, cuyo fallo dejaría inoperativas a todas las demás computadoras.
- Es una tecnología bien conocida.

Sus desventajas son las siguientes:

- Si se rompe el cable en algún punto, la red queda inoperativa por completo.
- Baja confiabilidad de en la operación.

Cuando se decide instalar una red de este tipo en un edificio con varias plantas, lo que se hace es instalar una red por cada planta de dicho edificio y después unir las todas a través de un bus troncal (figura 1.2).

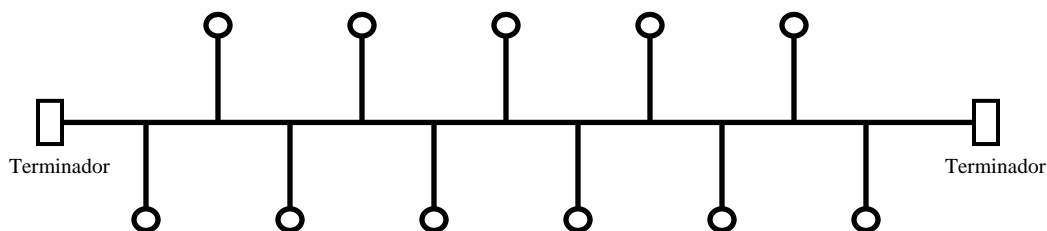


Figura 1.2 Topología en BUS

Topología en Anillo

Una topología de anillo se compone de un sólo anillo cerrado formado por nodos y enlaces, en el que cada nodo está conectado solamente con los dos nodos contiguos. Es una topología implementada por IBM (figura 1.3).

Sus principales inconvenientes de esta topología son:

- Si se rompe el cable que forma el anillo se paraliza toda la red.
- Es difícil de instalar.
- Es de baja confiabilidad.

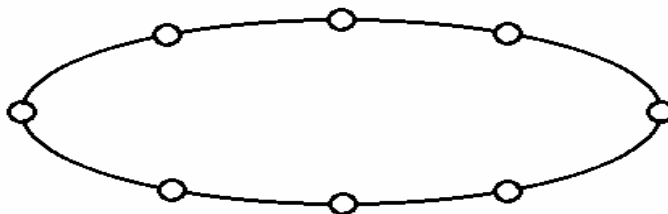


Figura 1.3 Topología en Anillo

Topología en Estrella

La topología en estrella tiene un nodo central desde el que se irradian todos los enlaces hacia los demás nodos. Por el nodo central, generalmente ocupado por un hub, pasa toda la información que circula por la red. La ventaja principal es que permite que todos los nodos se comuniquen entre sí de manera conveniente (figura 1.4).

La desventaja principal es que si el nodo central falla, toda la red se desconecta. Sus principales características se enlistan a continuación:

- Es la más usada.
- Todas las computadoras están conectadas a un concentrador formando una estrella física.
- Si se requiere establecer comunicación entre dos computadoras, la información transferida de uno hacia el otro debe pasar por el punto central.
- Al romperse la comunicación en un nodo, solo ese nodo se ve afectado.
- Es la más recomendada por su fiabilidad.

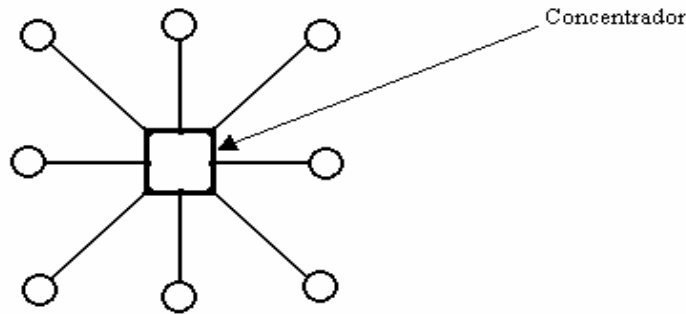


Figura 1.4 Topología en Estrella

Topología en Árbol

La topología en árbol es muy similar a la de bus; sin embargo, se permiten ramificaciones a partir de un punto llamado raíz, aunque no se permiten bucles (figura 1.5).

Los inconvenientes de esta topología son: ya que los datos son recibidos por todas las estaciones, hay que dotar a la red de un mecanismo para saber hacia que destinatario van los datos. Además, ya que todas las estaciones pueden transmitir a la vez, hay que implementar un mecanismo que evite que unos datos interfieran con otros.

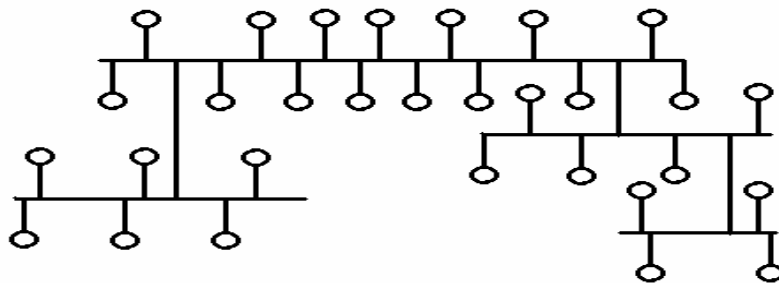


Figura 1.5 Topología en árbol

1.1.4. Medios de transmisión guiados

Los medios de transmisión más utilizados en las redes de comunicaciones de datos son el cable coaxial grueso y delgado, par trenzado y fibra óptica. Estos medios de transmisión son llamados guiados.

Cable Coaxial Delgado



Figura 1.6 Cable Coaxial Delgado

Consiste en un cable conductor interno cilíndrico separado de otro cable conductor externo por anillos aislantes o por un aislante macizo. Esto se recubre por otra capa aislante que es la funda del cable (figura 1.6).

De acuerdo a la IEEE se le conoce como 10BASE-2 y también se le conoce como:

- RG-58 /U (centro de alambre).
- RG-58 /AU (centro de cable).
- RG-58 /CU (aplicación militar).

Las características del cable son:

- Impedancia de 50 Ω .
- Longitud máxima: 185 m.
- Longitud mínima: 0.5 m.
- Diámetro de cable: ¼ pulgada.
- Velocidad de transmisión: 10 Mbps.
- Número máximo de nodos por segmento: 30 nodos.
- La conexión se realiza por medio de "T's" y "BNC's".

Cable coaxial Grueso



Figura 1.7 Cable coaxial grueso

Este cable es de misma forma que el cable coaxial delgado ya que contiene en el centro el cable conductor rodeado por un aislante y una malla conductora y cubierto finalmente por un aislante, con la diferencia de que es más grueso (figura 1.7).

De acuerdo a la IEEE se le conoce como 10BASE-5 ó como RG-8.

Características del cable son:

- Impedancia de: 50 Ω .
- Generalmente el color del cable es amarillo o naranja.
- Longitud máxima: 500 m.
- Longitud mínima: 2.5 m ó múltiplos.
- Diámetro de cable: ½ pulgada.
- Velocidad de transmisión: 10 Mbps.
- Número máximo de nodos por segmento: 100 nodos.
- La conexión se realiza a través de transceivers tipo vampiro.
- Este tipo de cable es más caro que el cable coaxial delgado.

Cable Par Trenzado



Figura 1.8 Cable Par Trenzado

Este medio es de los más usados y consiste en un par de cables aislados y trenzados entre sí, para cada enlace de comunicación. Debido a que puede haber acoples entre pares, estos se trenzan con pasos diferentes. La utilización del trenzado ayuda a disminuir la interferencia electromagnética.

Con estos cables se pueden transmitir señales analógicas o digitales; aunque su distancia máxima de transmisión es de 100 m y para alargar esa distancia se hace uso de repetidores. Su impedancia es de 100 ohms. Se usa para su conexión un concentrador y sus conectores son RJ-45.

Es un medio muy susceptible al ruido y a interferencias. Para evitar estos problemas se suele trenzar el cable con distintos pasos de torsión y se suele recubrir con una malla externa para evitar interferencias ya sean externas o entre los otros pares que se encuentran a su alrededor (figura 1.8).

Este tipo de transmisión esta dividido en categorías por la EIA/TIA:

- Categoría 1. Un par de hilo telefónico trenzado de calidad de voz no adecuado para la transmisión de datos. Su velocidad es inferior a 1 Mbps.
- Categoría 2. Esta categoría está constituida de 2 pares de cables de par trenzado sin apantallar. Su velocidad es de hasta 4 Mbps.
- Categoría 3. Esta categoría cuenta con 4 pares de cables de par trenzado. Su velocidad de transmisión es hasta de 4 Mbps. Con este tipo de cables se pueden implementar redes Ethernet 10BASE-T.
- Categoría 4. También cuenta con 4 pares de cables de par trenzado. Y su velocidad de transmisión llega hasta 16 Mbps.
- Categoría 5. También contiene 4 pares de cables de par trenzado. Y su velocidad es de hasta 100 Mbps.
- Categoría 5e. Cuenta con 4 pares de cables de par trenzado. Las velocidades que puede soportar son de 100 Mbps y de 1000 Mbps.
- Categoría 6. Su velocidad es hasta de 1000 Mbps.

Dentro de los cables de par trenzado se encuentran los siguientes tipos:

Cable UTP



Figura 1.9 Cable UTP

Los avances logrados respecto a los cables UTP permiten transportar datos hasta velocidades de 1 Gbps, lo que hace posible utilizar cables menos costosos y voluminosos en las aplicaciones, en lugar de los que antes se consideraban específicos para otros tipos de medios, por ejemplo, la fibra óptica (figura 1.9).

Cable FTP



Figura 1.10 Cable FTP

Los cables apantallados con lámina, también denominados FTP, están formados por cuatro pares trenzados con una manga de lámina completa. Los cables FTP son un poco más voluminosos que los UTP, aunque tienen una resistencia mayor a la interferencia externa que los cables UTP (figura 1.10).

Cable STP

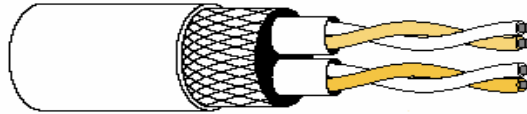


Figura 1.11 Cable STP

Los cables blindados, también denominados STP, cuentan con una estructura muy costosa que ocupa mucho espacio, formada por pares trenzados, blindados en forma individual y con un blindaje completo adicional. Estos cables son bastante resistentes, son más caros y ocupan mucho más espacio que los cables sin blindaje.

Tanto los cables blindados como los apantallados tienen mangas de metal que deben conectarse muy bien a tierra. Lo anterior es para eliminar el efecto de la interferencia electromagnética en las señales que transportan los conductores (figura 1.11).

Fibra Óptica

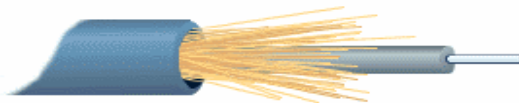


Figura 1.12 Fibra Óptica

La fibra óptica se trata de un medio muy flexible y muy fino que conduce señales a través de ondas de luz.

Su forma es cilíndrica con tres secciones radiales: núcleo, revestimiento y cubierta (figura 1.12). El núcleo está formado por una o varias fibras muy finas de cristal o plástico. Cada fibra está rodeada por su propio revestimiento que es un cristal o plástico con diferentes propiedades ópticas distintas a las del núcleo. Alrededor de todo esto está la cubierta que se encarga de aislar el contenido de aplastamientos, abrasiones, humedad, etcétera.

Es un medio muy apropiado para largas distancias e incluso últimamente para redes de tipo LAN.

Sus principales ventajas frente a cables coaxiales y pares trenzados son:

- Permite un mayor ancho de banda.
- Es totalmente dieléctrica.
- Menor tamaño y peso.
- Menor atenuación.
- Aislamiento Electromagnético.
- Mayor separación entre repetidores.
- Es segura y difícil de robar su señal.
- Su rango de frecuencias es todo el espectro visible y parte del infrarrojo.

El método de transmisión es el siguiente: Los rayos de Luz inciden con una gama de ángulos diferentes posibles en el núcleo del cable, entonces sólo una gama de ángulos conseguirán reflejarse en la capa que recubre el núcleo. Son precisamente esos rayos que inciden en un cierto rango de ángulos los que irán rebotando a lo largo del cable hasta llegar a su destino. A este tipo de propagación se le llama Multimodo. Si se reduce el radio del núcleo de tal forma que sólo sea posible la transmisión de un rayo, el rayo axial (central), entonces, este método de transmisión se le llama Monomodo (figura 1.13).

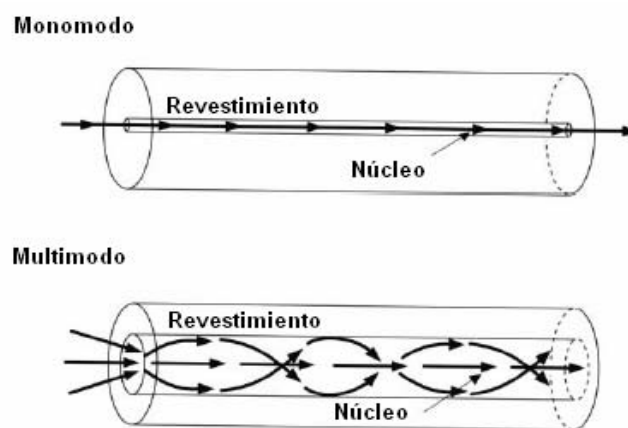


Figura 1.13 Monomodo y Multimodo

Hay un tercer modo de transmisión que es un paso intermedio entre los dos mencionados anteriormente y que consiste en cambiar el índice de refracción del núcleo. A este modo se le llama Multimodo de índice gradual (figura 1.13).

Los emisores de luz utilizados son: LED (de bajo costo, con utilización en un amplio rango de temperaturas y con larga vida media) e ILD (más caro, más eficaz y permite una mayor velocidad de transmisión).

Clasificaciones de la fibra óptica	
Por materiales dieléctricos	Fibra óptica de silicio
	Fibra óptica de vidrio multicompuesto
	Fibra óptica plástica
Por modo de propagación	Fibra óptica monomodo (SM)
	Fibra óptica multimodo (MM)
Por distribución del índice de refracción	Fibra óptica de índice escalonado (SI)
	Fibra óptica de índice gradual (GI)

Tabla 1.14 Clasificación de la fibra óptica

La función básica de los conectores de la fibra óptica es alinear adecuadamente dos fibras ópticas con el fin de transferir potencia de una a otra. Es por eso que deben de estar bien hechos para evitar pérdida de información. La clasificación de la fibra óptica se indica en la tabla 1.14.

Medios de transmisión no guiados

Las redes inalámbricas facilitan la conexión de las computadoras a la red. Las ventajas de usar medios inalámbricos son el poder tener movilidad y permanecer siempre conectado; evita la instalación de cables, canaletas, rosetas, etc., lo cual reduce el costo de la red.

Algunos de los medios de transmisión de redes inalámbricas son:

Infrarrojos (IrDA)

Las ondas infrarrojas son utilizadas para la comunicación entre equipos a corta distancia, no atraviesan los objetos sólidos, no es necesario tramitar una licencia del gobierno para operar un sistema infrarrojo y su transmisión debe de ser de línea directa, es decir, no debe haber objetos que se interpongan en la línea de transmisión del emisor y receptor.

Sus ventajas principales son:

- Los emisores y receptores son muy simples y baratos.
- No tienen interferencia con otros dispositivos.
- Son muy útiles para redes pequeñas.

Sus desventajas principales son:

- Poco ancho de banda.
- Necesidad de comunicación “visual”.
- Es de corto alcance.

Radio Frecuencia

Las ondas de radio pueden penetrar sin problemas edificios, viajar grandes distancias y además, son fáciles de generar. Son las más usadas en la comunicación tanto en interiores como en exteriores. Las ondas de radio son omnidireccionales, es decir, que viajan en todas direcciones desde el emisor, por lo cual el transmisor y receptor no tienen que ser alineados.

Las radio frecuencias dependen demasiado de su frecuencia en que trabajen. Si las ondas de radio son enviadas a baja frecuencia no tienen problema en atravesar los obstáculos; sin embargo, la potencia de la señal se ve disminuida conforme se aleja de la fuente. A altas frecuencias las ondas de radio tienden a viajar en línea recta y a rebotar en los obstáculos lo cual dificulta su recepción; además de que también son absorbidas por la lluvia y están sujetas a la interferencia por los motores, equipos eléctricos y campos magnéticos. Debido a que pueden viajar grandes distancias, los gobiernos legislan el uso de radiotransmisores.

Ventajas

- No existe conexión física.
- Multidireccional.
- Antenas pequeñas para cortas distancias.
- TX satelital para distancias grandes.

Desventajas

- Requiere permisos o licencias de uso de Radio Frecuencia.
- Más caro que el enlace de cobre o de fibra óptica.
- Costo alto de manutención.

Microondas

Las señales de microondas están por encima de una frecuencia de 100 Mhz, viajan en línea recta en un haz concentrado usando antenas parabólicas para una mejor comunicación. Dichas antenas deben de estar bien alineadas entre sí. Se requiere una línea de visión directa y para grandes distancias es necesario colocar repetidoras entre las antenas. Este tipo de señales son muy utilizadas para la comunicación telefónica, telefonía celular y distribución de señales de televisión.

Ventajas

- Utiliza frecuencias más altas que las ondas de radio.
- Es muy utilizada por las compañías de telecomunicaciones.
- Pueden utilizarse los satélites como repetidores para aumentar el alcance de la señal.

Desventajas

- Se debe tener una ruta visible y sin obstáculos.
- Es más caro que las redes de cobre o fibra óptica.
- El costo por mantenimiento es alto.

1.2 Modelo OSI

Los sistemas abiertos surgen de la necesidad de un sistema operativo estándar mundial que pudiera ofrecer la interoperabilidad entre ordenadores de cualquier fabricante, la portabilidad de software en distinto hardware, la compatibilidad entre distintas versiones de sistemas operativos y la escalabilidad del software en diferentes plataformas de hardware.

1.2.1 Antecedentes

En un inicio cuando aparecieron las primeras redes de datos, la conexión entre ellas era sencilla si el fabricante era el mismo, el inconveniente era cuando se pretendía conectar esas redes con otras de diferente fabricante era imposible. Así que la necesidad de conectar esas redes por parte de los dueños, y aunado al interés de ampliar mercado por parte de los fabricantes dio pauta a la creación de acuerdos entre los diferentes fabricantes en cuanto al hardware y el software, para lograr una comunicación entre sus dispositivos. Sin embargo, no todos los fabricantes accedieron a modificar sus tecnologías por lo que fue necesario crear organismos que dirigieran a nivel internacional el proceso de estandarización para interfaces y protocolos, uno de esos organismos reconocidos internacionalmente es la Organización Internacional para Estandarizaciones (ISO, “International Standard Organization”).

Fue hasta 1984, cuando la ISO publicó un modelo de referencia de Interconexión de Sistemas Abiertos (OSI, “Open Systems Interconnection”) que establece una arquitectura de comunicación. Dicha arquitectura forma un marco de normalización para establecer la comunicación entre dos dispositivos.

1.2.2 ¿Qué es el modelo OSI?

Es un modelo de referencia para la Interconexión de Sistemas Abiertos, refiriéndose a este tipo de sistemas como aquellos que no pertenecen a un mismo fabricante.

Este modelo de estandarización de arquitecturas hace posible la comunicación entre diferentes computadoras. Está organizado jerárquicamente por siete capas que son autocontenidas, ya que desempeñan funciones únicamente asignadas a cada capa. La capa inferior proporciona servicios a la capa inmediata superior y no tiene acceso a la información de ésta; sin embargo, la capa superior si puede acceder a la información contenida en la capa inferior. Cada capa tiene comunicación con tres capas: la capa inmediata superior, la capa inmediata inferior y la capa paritaria en el ordenador destino en la transmisión de información. Todas las capas utilizan información de control para establecer comunicación con el ordenador receptor.

El modelo OSI permite hacer comparaciones entre diferentes tecnologías sin hacer la implementación de una en específico, permitiendo la compatibilidad en hardware y software de dichas tecnologías; estandariza la manera en que se transmite información de un ordenador a otro.

La siguiente figura (figura 1.15), muestra la jerarquía de las capas del modelo OSI, de las cuales, las cuatro primeras desempeñan funciones de comunicación y las tres restantes de proceso.

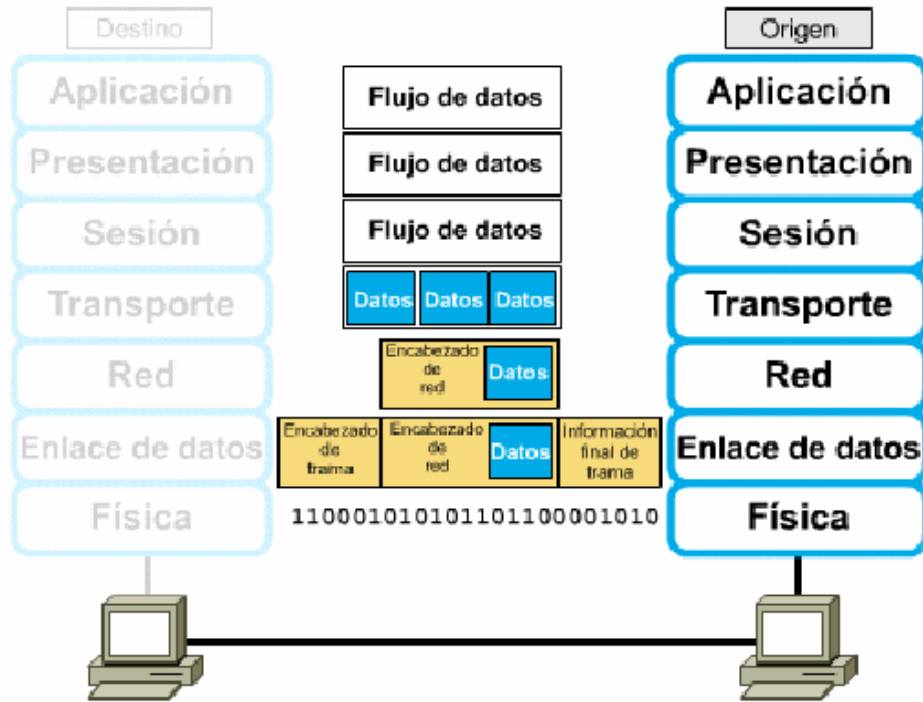


Figura 1.15 Modelo OSI

1.2.3 Capas del modelo OSI

Cada capa del modelo OSI realiza funciones independientes de las demás capas y el intercambio de la información siempre es entre capas del mismo nivel.

A continuación se describe cada una de ellas.

1. Capa física

Esta capa determina la manera en que se transmite físicamente la información entre dos ordenadores. Establece las características mecánicas, eléctricas, funcionales y de procedimiento para activar, mantener y desactivar conexiones entre dos extremos conectados por un medio físico. Especifica las características físicas de los conectores, así como, los niveles de tensión, velocidad de transmisión, etcétera.

2. Capa de enlace

Se encarga de proporcionar un medio confiable para la transmisión de datos entre dos puntos que comparten un medio de comunicación. Esta capa se encarga de controlar el flujo de datos, así como, la detección de errores, recuperación de la trama cuando se identifica un error y la retransmisión de la misma. En esta capa se define el formato del frame y se especifica la secuencia de los mismos, así como, las técnicas de acceso al medio.

Realiza direccionamiento físico entre dispositivos con base en la dirección MAC (Media Access Control, Control de Acceso al Medio) de cada uno de ellos.

3. Capa de red

Esta capa utiliza direccionamiento lógico para la identificación de un host destino en la transmisión de datos y en la red de datos. Especifica mecanismos de enrutamiento para transportar información entre cualesquiera dos puntos de una red. Así entonces, desempeña funciones de control de flujo, de segmentación, de secuenciación, de encaminamiento y de retransmisión.

4. Capa de transporte

La capa de transporte asegura una transmisión fiable y que la información llegue a su destino. Se encarga del control de flujo en la transmisión de datos, de la retransmisión de información y del multiplexaje; así como, de la detección y corrección de errores.

5. Capa de sesión

Se encarga de establecer, liberar y sincronizar la conexión de sesión entre entidades de presentación, así como, permitirles a éstas la organización y sincronización del diálogo entre ellas para el intercambio de datos.

6. Capa de presentación

Esta capa permite la representación de la información que transmiten dos entidades de aplicación que puede ser la compresión de datos o criptografía. A la capa de presentación le atañe la sintaxis pero no la semántica utilizada entre entidades de aplicación.

7. Capa de aplicación

Esta capa se encarga de la interfaz de las aplicaciones con los usuarios finales. Es el único medio para que el proceso de aplicación acceda al entorno de OSI, ya que es la capa de nivel más alto y no existe alguna superior a ella. Dentro de las funciones de esta capa se encuentra la transferencia de archivos, el software de terminales virtuales, el correo electrónico, la búsqueda en directorios entre otros recursos de uso general y especial, y todos aquellos que no han sido realizados por capas inferiores como las funciones realizadas por programas o seres humanos.

1.3 Modelo TCP/IP

Fue desarrollado y utilizado por primera vez en una red de investigación de conmutación de paquetes llamada ARPANET, patrocinada por la Agencia de Proyectos de Investigación Avanzada para la Defensa (DARPA, “Defense Advanced Research Projects Agency”) del Departamento de Defensa (DoD) de los Estados Unidos.

Debido al retraso de la entrega completa del modelo OSI, el DoD se vio obligado a utilizar el modelo TCP/IP que ya estaba listo para usarse, lo que dio pauta a los fabricantes a desarrollar productos basados en este modelo, el cual es ahora la base para el desarrollo de nuevos protocolos y el estándar de Internet.

1.3.1 ¿Qué es el modelo TCP/IP?

La arquitectura TCP/IP, Protocolo de Control de Transmisión (TCP, “Transmission Control Protocol”) /Protocolo de Internet (IP, “Internet Protocol “), es un conjunto de protocolos publicados como estándares de Internet por el IAB (Internet Activities Board) que es el departamento de la Sociedad de Internet (ISOC, “Internet Society”) encargado de la evolución y desarrollo técnico del Internet, así como, la evolución del TCP/IP y diversas investigaciones.

Ya que primero se utilizó y después se estandarizó, no se reconoce como un modelo de referencia, como es el caso del OSI, sino que se hace referencia a él como “conjunto de protocolos TCP/IP”.

Tiene como objetivos interconectar diferentes redes y que la comunicación no se pierda si un tramo en la subred falla, así como, soportar diferentes tipos de servicios. En cada capa se utiliza información de control para la transferencia de datos.

Otra característica de este conjunto es que permite conectar máquinas de diferentes tipos y con diferentes sistemas operativos en redes LAN y WAN.

1.3.2 Capas del modelo TCP/IP

Dado que no existe un modelo oficial de referencia TCP/IP todas las funciones involucradas en el sistema de comunicación se pueden clasificar en cuatro capas, ya que este modelo no es general y no hace una clara diferencia entre servicio, interfaz y protocolo, se dice en ocasiones que este modelo esta compuesto por cuatro o cinco capas.

Las cuatro capas a las que se hace referencia se mencionan a continuación:

- Capa de aplicación.
- Capa de transporte.
- Capa Internet.
- Capa de acceso a red.

La figura mostrada (figura 1.16) intenta describir la correspondencia funcional de las capas de la arquitectura TCP/IP con la OSI, ya que es difícil representar la jerarquía de los protocolos de la primera mediante un modelo de capas.

Modelo de referencia OSI

Aplicación
Presentación
Sesión
Transporte
Red
Enlace de datos
Física

Modelo TCP/IP

Aplicación
Transporte
Internet
Acceso a red

Figura 1.16 Comparación de los modelos OSI y TCP/IP

1. Capa de acceso a red

Esta capa corresponde a la capa física y de enlace del modelo OSI. Se encarga de colocar la información en el medio de comunicación y señala las características físicas del medio de transmisión como la velocidad de los datos, la naturaleza de las señales entre otras, aunque no incorpora las funciones de control de flujo y errores. Es responsable de llevar y recibir datos de la red.

2. Capa de Internet

Esta capa se encarga de transportar la información, a través de la red de datos, para ello utiliza el direccionamiento lógico, encaminamiento y empaquetamiento de los datos, así como, la dirección lógica de los dispositivos. En esta capa se distinguen cuatro protocolos: IP, ARP, ICMP, IGMP.

El Protocolo de Internet (IP) se destaca por ser el formato y protocolo oficial de esta capa, ya que provee el ruteo y control de la congestión sin asegurar la entrega de los datos, ya que es no orientado a la conexión lo que lo hace un protocolo no confiable. El Protocolo de Resolución de Direcciones (ARP) le permite identificar la dirección física del dispositivo correspondiente a una dirección lógica. El Protocolo de Control de Mensajes Internet (ICMP) se encarga de diagnosticar y reportar errores aunados a datagramas, también controla los mensajes. El Protocolo de Administración de Grupo de Internet (IGMP) permite enviar mensajes a grupos de host en una red.

3. Capa de transporte

Esta capa permite la conexión entre dos hosts, asegurando la transmisión entre ellos. Utiliza dos protocolos que funcionan de extremo a extremo, es decir, desde el emisor hasta el receptor: TCP y UDP.

El Protocolo de Control de Transmisión (TCP) está orientado a conexión lo que lo hace ser confiable y asegura la entrega integral de los datos, además permite a los hosts tener varias conexiones simultáneas. Este protocolo maneja el control de flujo. El Protocolo de Datagrama de Usuario (UDP) es un protocolo no confiable, ya que no es orientado a conexión, su principal uso es cuando la entrega de los datos requerida sea más rápida que precisa.

4. Capa de aplicación

Es la capa más alta de la arquitectura TCP/IP y es la interfaz para la comunicación con el usuario y el acceso de los procesos a la red, aquí se llevan a cabo las aplicaciones del usuario. Contiene todos los protocolos de alto nivel. Esta capa agrupa características de las tres capas superiores del modelo OSI, en ella se encuentran protocolos como HTTP para recuperar paginas de la Web, SMTP que es el Protocolo de Transferencia de Correo Sencillo que implementa la entrega de mensajes, FTP para la transferencia de archivos, Telnet que permite una terminal virtual remotamente, entre otros.

1.4 Protocolos

Para que dos máquinas se comuniquen es importante que haya un mutuo acuerdo para establecer una comunicación, entonces, al conjunto de normas que deben seguir dos hosts para establecer una comunicación desde que se inicia, se mantiene y se termina se le llama protocolo.

Los protocolos de red más utilizados se mencionan a continuación.

1.4.1 Protocolo TCP

Este protocolo es utilizado en la capa de transporte de la arquitectura TCP/IP, es orientado a conexión por lo cual es confiable. Se encarga del control de errores, del control del flujo, asegura que los paquetes sean entregados correctamente y que se ensamblen ordenadamente de acuerdo al orden en que se enviaron. Este protocolo por ser orientado a conexión consta de tres fases:

- Establecimiento de la conexión.
- Transferencia de los datos.
- Liberación de la conexión.

Establecimiento de la conexión. Se refiere al mutuo acuerdo que debe haber entre los dos extremos de la transmisión, es decir, estén listos para iniciarla.

Transferencia de los datos. Dado que la transmisión es fiable, permite la recuperación de datos ante la pérdida y la duplicación, o sean erróneos dichos datos. La entrega de los datos

lo hace agregando un número de secuencia y un código de control a la cabecera del segmento.

Liberación de la conexión. Si ya no hay más datos que transmitir se libera el medio en dicha dirección. Dado que la conexión esta determinada por los puertos origen y destino permite las múltiples conexiones a un puerto dado, cada una con diferentes puertos.

1.4.2 Protocolo IP

Es un protocolo de la capa de Internet no orientado a conexión, ya que no hace una conexión con el destinatario antes de la transferencia de datos por lo que no es fiable, y no garantiza la integridad de los datos que transmite ni que estos lleguen a su destino.

Puede realizar tareas como la fragmentación y el reensamblado de los datagramas, así como, la elección de la trayectoria a seguir por estos al ser enviados. Otra de las tareas es el encaminamiento, esto lo hace mediante el uso del encabezado IP que añade al datagrama en el encapsulamiento.

1.4.3 Protocolo X.25

La ITU-T antes CCITT estableció un conjunto de protocolos para las capas 1, 2 y 3 del modelo OSI denominados X.25, la capa 3 se suele llamar X.25 PLP (Packet Layer Protocol).

X.25 utiliza una terminología en la que hace referencia a la maquina del usuario, como equipo terminal de datos (DTE, “Data Terminal Equipment”), y el equipo terminal del circuito de datos (DCE, “Data Circuit Equipment”) lo referencía como el nodo local. Entonces, X.25 define el formato y el significado de la información intercambiada entre DTE y DCE en las tres primeras capas.

Para la capa uno referencia los estándares X.21 y X.21 bits que definen interfaces digitales y analógicas respectivamente.

En la segunda capa utiliza los protocolos LAP (Protocolo de Acceso al Enlace) y LAPB (Protocolo Equilibrado de Acceso al Enlace) para asegurar una comunicación confiable a través del enlace físico entre DTE y DCE.

En la tercer capa utiliza dos formas de conexiones entre pares de DTE’s: circuitos virtuales y circuitos virtuales permanentes, el primero se crea cuando un nodo envía un paquete a la red pidiendo llamar a un nodo remoto, consiste en establecer-usar-liberar la conexión; el

segundo es como una línea alquilada siempre disponible y cualquier DTE puede comenzar a transmitir sin que se establezca previamente una conexión.

En general, es un protocolo utilizado en redes públicas de transmisión de datos. Funciona por conmutación de paquetes, es decir, la información se particiona en bloques, de longitud determinada por la red en que viajan, del paquete original que contienen la dirección origen y la dirección destino por lo que asegura la entrega del mismo, sin riesgo a perderse aunque viajen por diferentes trayectorias.

Las principales características de este protocolo se mencionan a continuación:

- Orientado a conexión.
- Fiable.
- Multiplexación.

Es un protocolo fiable ya que no duplica ni pierde el paquete transmitido y es entregado en forma ordenada.

1.4.4 Protocolo IPX/SPX

Los protocolos IPX/SPX (Internetwork Packet Exchange/Sequential Packet Exchange) fueron desarrollados por Novell a principios de los años ochenta basándose en los protocolos del Sistema de Red Xerox (XNS, “Xerox Network System”). El sistema de redes NetWare de Novell es previo al ISO por lo que no se basa en él. Utiliza estos protocolos como interfaz entre su sistema operativo de red y las distintas arquitecturas de red. Es similar a la arquitectura TCP/IP.

- **Intercambio de Paquetes de Internet (IPX)**

Es un protocolo de la capa de red que transmite los datos en datagramas, no es confiable y es un protocolo no orientado a conexión por lo que los datos pueden no llegar en secuencia, funcionalmente es similar al protocolo IP de la arquitectura TCP/IP. Este protocolo encapsula los datos de capas superiores en datagramas en los cuales incluye la dirección del emisor y la del destino. Otra función que realiza es el encaminamiento de la información hacia la misma red u otras redes basándose en tablas de enrutamiento.

- **Intercambio de Paquetes Secuencial (SPX)**

Este protocolo funciona a nivel de la capa de transporte y es orientado a conexión. Utiliza un mecanismo de secuenciación por lo que puede pedir la retransmisión en caso de que los paquetes no lleguen.

1.5 Estándares

Los estándares como evaluadores de las acciones y de la eficacia de la organización, son maneras fáciles, confiables y aceptadas para la implantación de una red. Existen diversos tipos de estándares.

1.5.1. IEEE

De los estándares de la IEEE los que más usaremos para nuestro proyecto se mencionan a continuación.

IEEE 802.3

Las especificaciones de la IEEE para Ethernet es la 802.3, en ella se definen:

- Características mecánicas y eléctricas de la conexión de un equipo a la red.
- La gestión lógica de las tramas.
- El control de acceso a la red.

La técnica CSMA/CD, normalizada por la ISO, actualmente es la técnica de acceso aleatorio más utilizada. Consiste en escuchar la red (a través de la NIC) no sólo antes de una emisión, sino durante la transmisión: en un dispositivo preparado para transmitir, si detecta un canal libre, transmite y continua atento al canal. Si se produce una colisión aborta tan pronto como es posible su transmisión y envía señales especiales, bits de atasco con el fin de que todos los dispositivos se enteren de la colisión. Posteriormente, intentará de nuevo su emisión siguiendo un algoritmo que estará presente en la cadena.

Dentro de la norma 802.3 hay otras normas que definen las condiciones de uso de la técnica de acceso CSMA/CD (Carrier Sense Multiple Access/Collision Detection). Las diferencias

entre las normas provienen del cableado utilizado, y por lo tanto, de las velocidades que se puedan alcanzar y las longitudes máximas sin usar repetidor.

Estas normas se describen a continuación.

Ethernet

Las redes Ethernet originales trabajan a 10 Mbps y toman su notación de los identificadores del estándar IEEE. En 10BASE-T por ejemplo, El número 10 indica la velocidad de la red, BASE indica el tipo de operación para este caso opera en banda base; es decir, la señal no está modulada. El último parámetro señala la distancia máxima de acuerdo al medio utilizado.

10BASE-5. También conocida como Thicknet, usa una topología física en BUS. La velocidad de esta red es de 10 Mbps con una conexión en banda base, y alcanza una longitud máxima de 500 m. El cable que utiliza es de tipo coaxial conocido como RG-8 de 50 ohm, de ½ pulgada; generalmente el cable es de color amarillo o naranja. La conexión se realiza entre transceivers tipo “vampiro”, cada estación debe de estar a una distancia mínima de 2.5 m o múltiplos; además cada estación esta unida al cable mediante un tranceptor denominado MAU (Medium Attachment Unit) y un cable de derivación, el cual no debe de exceder los 50 metros. Permite un número máximo de 100 nodos por segmento, se pueden usar repetidores para unir segmentos o alargar las distancias de comunicación.

10BASE-2. Se le conoce como ethernet de cable fino, usa una topología lógica en BUS. La velocidad de la red es de 10 Mbps en banda base y alcanza una longitud máxima de 185 m. El tipo de cable que utiliza es coaxial conocido como RG-58 de 50 ohm, de ¼ de pulgada. La conexión se realiza por medio de “T’s” y BNC. La longitud mínima entre estaciones es de 0.5 m. El número máximo de nodos por segmento es de 30 nodos. También se pueden usar repetidores para alargar distancias o unir segmentos.

10BASE-T. Se le conoce como Twisted-Pair Ethernet, usa una topología física en estrella. Se puede utilizar un hub como concentrador de usuarios. Permite una distancia máxima del concentrador al usuario de 100 m. La conexión en árbol elimina el problema del bus coaxial, ya que una falla interrumpe la conexión en serie.

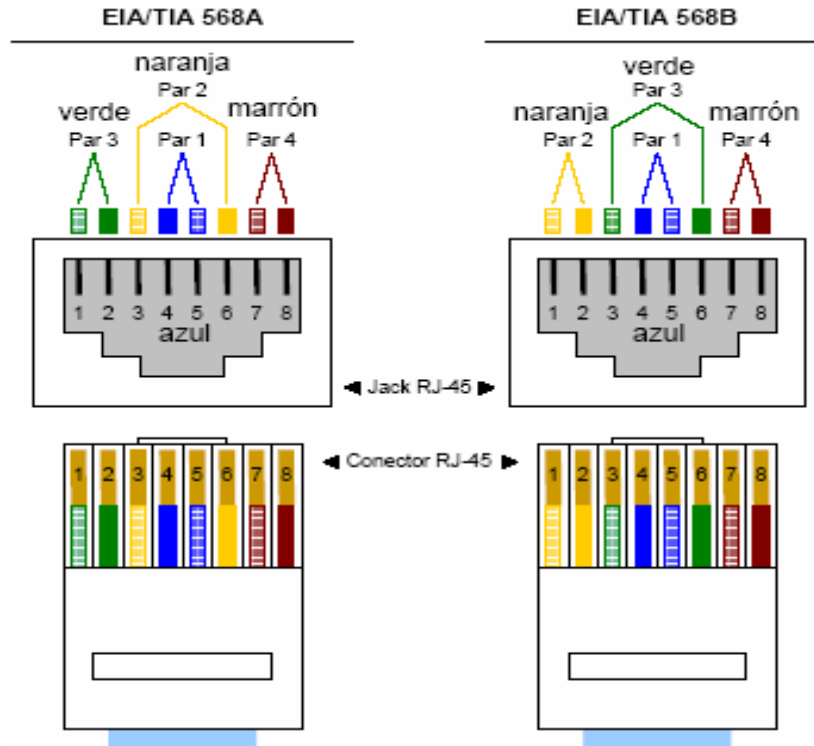


Figura 1.17 Conector RJ-45 de 8 hilos

El cable utilizado es par trenzado de 8 hilos, de categoría 3 ó superior, tiene una impedancia de 100 ohms. Usa el conector RJ-45. La forma en que pueden ser acomodados los hilos del cable UTP son 3 y estas depende de la utilidad (figura 1.17). A continuación se describe su conexión.

T568 A. Es usado para conectar del concentrador a la PC, el orden de los colores de los hilos en el conector RJ-45 (tabla 1.18) es el siguiente:

Pin	Hilo asignado
1	Blanco-Verde
2	Verde
3	Blanco-Naranja
4	Azul
5	Blanco-Azul
6	Naranja
7	Blanco-Café
8	Café

Tabla 1.18 Orden de los hilos en el conector RJ-45 T568 A

T568 B. Es usado para conectar del concentrador a la PC, el orden de los colores de los hilos en el conector RJ-45 (tabla 1.19) es el siguiente:

Pin	Hilo asignado
1	Blanco-Naranja
2	Naranja
3	Blanco-Verde
4	Azul
5	Blanco-Azul
6	Verde
7	Blanco-Café
8	Café

Figura 1.19 Orden de los hilos en el conector RJ-45 T568 B

Conexión Cruzada o Croosover. Este tipo de cable es usado para conectar dos PC's en red o conectar dos hub o switches en "Cascadeo".

A continuación (tabla 1.20) se especifica el cable para una conexión Gigabit.

Extremo izquierdo del cable	Extremo derecho del cable
Blanco-Naranja	Blanco- Verde
Naranja	Verde
Blanco-Verde	Blanco-Naranja
Azul	Blanco-Café
Blanco-Azul	Café
Verde	Naranja
Blanco-Café	Azul
Café	Blanco-Azul

Tabla 1.20 Cable Croosover

10BASE-F. Es una red que usa como medio de transmisión fibra óptica, mediante la cual se envían pulsos de luz en vez de señales eléctricas. Este tipo de redes es de las más seguras en cuanto a interferencia de campos electromagnéticos. Operan a una velocidad de 10 Mbps. La distancia máxima de operación es de 1 Km de hub a Nodo y de 2 Km de hub a hub. Los tipos de conectores son ST, SC, SMA y FC.

En resumen en cuanto a Ethernet (tabla 1.21) tenemos lo siguiente:

Nombre	Cable	Distancia entre segmentos	Nodos por segmentos
10BASE-5	Coaxial Grueso	500 m	100
10BASE-2	Coaxial Delgado	185 m	30
10BASE-T	Par Trenzado	100 m	1024
10BASE-F	Fibra Óptica	1000 m	1024

Tabla 1.21 Ethernet

Fast Ethernet

Las redes Fast Ethernet comparadas contra las redes Ethernet, su velocidad es 10 veces mayor que las redes Ethernet. Las redes Fast Ethernet se conectan a 100 Mbps lo que reduce el tiempo de transmisión considerablemente. Además, permite la conexión de dos hub entre la ruta de comunicación de dos nodos, y la conexión de 7 switches entre la ruta de dicha comunicación de dos nodos.

100BASE-TX. Es compatible con 10BASE-T. Dispone de una velocidad de 100 Mbps, la impedancia del cable es de 100 ohms. Utiliza cable de par trenzado de categoría 5 o superior; trabaja con dos pares de hilos, un par para transmitir datos y un par para recibirlos. El conector utilizado es RJ-45. La distancia máxima entre el nodo y el hub es de 100 m.

100BASE-FX. Utiliza fibra óptica de 62.5/125 μm . Emplea 2 hilos, uno lo utiliza para la transmisión y el otro para detección de colisiones y recepción. Los conectores que utiliza son de tipo SC o ST. La distancia máxima entre el hub y el nodo es de 2000 m en modo Full Duplex y 412 m en modo Half Duplex.

Las características más importantes de Fast Ethernet (tabla 1.22) son las siguientes:

Nombre	Cable	Distancia máxima entre segmentos	Ventajas
100BASE-TX	Par Trenzado	100 m	Full Duplex a 100 Mbps
100BASE-FX	Fibra Óptica	412 m	Half Duplex a 100 Mbps
		2000 m	Full Duplex a 100 Mbps

Tabla 1.22 Fast Ethernet

Gigabit Ethernet

Gigabit Ethernet es una opción conveniente para la migración de redes LAN de alta velocidad, sigue utilizando el protocolo de acceso al medio CSMA/CD. La velocidad a la que operan estas redes es de 1000 Gbps. Sólo permite utilizar un hub para unir dos segmentos.

1000BASE-T: El diseño de 1000BASE-T permite trabajar con Gigabit Ethernet sobre cable de cobre de categoría 5/5e ó superior, el medio de cableado más común actualmente. Esto permite que redes de Fast Ethernet se puedan fácilmente actualizar a redes Gigabit Ethernet sin que sea tan costoso. Usa cable par trenzado de categoría 5 o superior, con una impedancia de 100 ohm. Su distancia máxima del concentrador al nodo es de 100 m. Utiliza los cuatro pares del cable para la transmisión de datos.

1000BASE-CX: Este diseño trabaja con cable twinax, blindado, con una impedancia de 150 ohms. La distancia máxima del nodo al concentrador es de 25 m. Sus conectores son el RJ-45/DB-9.

1000BASE-SX: Utiliza cable de fibra óptica multimodo de 50/125 μm y de 62.5/125 μm ; de las cuales la distancia máxima entre el nodo y el concentrador son de 220 m y 550 m. Utilizan un led de radiación de longitud de onda corta (800 nm).

1000BASE-LX: Utiliza cable de fibra óptica multimodo de 50/125 μm y de 62.5/125 μm con una distancia máxima entre el nodo y el concentrador es de 550m. También utiliza una fibra óptica monomodo con la cual puede alcanzar una distancia del nodo al concentrador de 5 Km. Utiliza para la fibra multimodo un led de longitud de onda larga (1300 nm); y para la fibra monomodo utiliza diodos láser operando a 1300 nm.

En resumen las características de Gigabit Ethernet (tabla 1.23) son:

	1000BASE-T	1000BASE-CX	1000BASE-SX	1000BASE-LX
Medios de transmisión	4 Pares UTP5	STP	Par Fibra 850 nm	Par Fibra 1300 nm
Conectores	RJ45	DB9/RJ45 Shielded	SC	SC
Longitud máxima de segmento	100 m	25 m	220 m – 62,5 550 m – 50	550 m– MMF 5 Km – SMF

Tabla 1.23 Gigabit Ethernet

IEEE 802.11

IEEE ha utilizado la nomenclatura 802.11 para denominar a los estándares de comunicación inalámbrica de área local. Los dos estándares que se utilizan actualmente para las redes inalámbricas son 802.11b y 802.11a; el 802.11g.

802.11b: fue el primer estándar dominante de comunicación inalámbrica usado para la comunicación en hogares y oficinas. Además utiliza tecnología de frecuencia de radio.

A continuación se mencionan sus características:

- Soporta puntos de acceso y conexiones de punto a punto.
- El ancho de banda que maneja es de hasta 11 Mbps.
- Tiene un alcance de 91.44 m dependiendo del entorno.
- Funciona en el espectro de 2.4 Ghz, por lo que no es necesario tramitar licencia para su uso.
- Utiliza productos Wi-Fi, para garantizar la interoperabilidad entre diferentes fabricantes.

802.11a: Este estándar se introdujo después del estándar 802.11b, con un ancho de banda cinco veces mayor pero de menor cobertura. Se está haciendo cada vez más conocido y es posible que reemplace a algunas WLAN 802.11b, debido a que es más rápido y soporta a más usuarios.

Algunas de sus características son:

- Su ancho de banda es de 54 Mbps.
- Su alcance es de 24.38 m dependiendo del entorno.
- Funciona en la banda UNII¹ de 5 Ghz con ocho canales sin superposición.

¹ Unlicensed National Information Infrastructure; banda de frecuencia de radio que no necesita una licencia para utilizar equipos en el rango de frecuencia especificados.

- Utiliza multiplexación por división de frecuencia ortogonal, Orthogonal Frequency Division Multiplexing (OFDM)².
- Utiliza productos con certificado Wi-Fi para la interoperabilidad entre diferentes proveedores.
- En áreas más grandes requiere de más puntos de acceso que 802.11b, debido a las limitaciones en cuanto a distancia.

802.11g: es la ruta de actualización desde 802.11b, debido a que proporciona un ancho de banda cinco veces mayor y ofrece la compatibilidad con 802.11b.

El IEEE aprobó oficialmente la especificación 802.11g en el verano del 2003.

Algunas de sus características son:

- El ancho de banda es hasta de 54 Mbps.
- su alcance es de 91.44 m dependiendo del entorno.
- Opera en el espectro de frecuencia de 2.4 Ghz en la banda ISM en tres canales sin superposición.
- Utiliza multiplexación por división de frecuencia ortogonal (OFDM).
- Funcionará con puntos de acceso o en una red de punto a punto.

Los dispositivos 802.11b como 802.11g son compatibles y pueden interoperar con el mismo rango de distancia, dado que ambos utilizan el mismo espectro de 2.4 Ghz. Aunque 802.11g proporciona ocho velocidades de datos (6, 9, 12, 18, 24, 36, 48 y 54 Mbps), la velocidad máxima de datos en la práctica está entre 18 y 22 Mbps.

Como 802.11b utiliza DSSS y 802.11g utiliza OFDM, para lograr la interoperabilidad son necesarios mecanismos de ingeniería. En un entorno mixto de 802.11b/g, los clientes de g tendrán un rendimiento inferior al de los clientes de sólo el entorno g (incluso si los clientes de b no están enviando tráfico); a cualquier distancia dada se observa una reducción del rendimiento de entre el 10% y el 20%.

Un entorno todo de 802.11g proporciona el mejor rendimiento.

² Orthogonal Frequency Division Multiplexing (OFDM): es un método para la transmisión de grandes cantidades de datos digitales a través de una onda de radio. OFDM divide la señal de radio en varias subseñales más pequeñas que, luego, se transmiten simultáneamente al receptor a diferentes frecuencias.

A continuación (tabla 1.24) se presenta una tabla comparando las características de los tres estándares: 802.11b, 802.11a y 802.11g.

Cuestión principal	802.11b	802.11a	802.11g
Rendimiento y ancho de banda compartido	11 Mbps por usuario; tres canales por punto de acceso	54 Mbps por usuario; once canales por punto de acceso	54 Mbps por usuario; tres canales por punto de acceso
Distancia de la señal	Hasta 91,44 m en oficinas típicas; hasta 300 m en espacios abiertos	Hasta 25 m en oficinas típicas; hasta 75 m en espacios abiertos	Igual que 802.11b
Compatibilidad	Funciona con dispositivos 802.11b y 802.11g	Sólo funciona con dispositivos 802.11a	Funciona con dispositivos 802.11b y 802.11g
Infraestructura inalámbrica existente en oficinas o lugares públicos	En toda la oficina; lugares amplios	Algunas partes de la oficina; no en lugares públicos	Áreas limitadas de la oficina; no en lugares públicos
Interferencia de otros dispositivos que comparten el mismo espectro	Sí; el espectro de 2,4 Ghz es susceptible a interferencias de teléfonos, microondas, Bluetooth	No; 802.11a utiliza espectro de 5,2 Ghz "limpio"	Sí; el espectro de 2,4 Ghz es susceptible a interferencias de teléfonos,

Tabla 1.24 Estándares del 802.11

En todos los estándares 802.11 la velocidad se reduce conforme aumenta la distancia desde un punto de acceso.

1.5.2 FDDI

El estándar de interfaz de datos distribuidos (FDDI, "Fiber Distributed Data Interface") lo desarrolló el comité de estándares acreditado X3T9.5 que está reconocido por el Instituto Americano Nacional de Estándares (ANSI). Fue diseñado para satisfacer las necesidades de transmisión de redes de alta velocidad y su conexión entre ellas. Entre los tipos de redes se encuentran: las redes locales especializadas, son usadas para interconectar ordenadores mainframe y grandes dispositivos de almacenamiento de datos; las redes profesionales de alta velocidad conocidas así por la carga de imágenes y gráficos que soportan; y las redes troncales usadas para conectar redes de área local de muy baja capacidad.

Las principales características son las siguientes:

- Usa la fibra óptica como medio.
- Velocidad de transmisión de hasta 100 Mbps.
- Utiliza el método de paso de testigo como método de acceso.
- Proporciona mayor velocidad de transmisión que otros medios de comunicación.
- Es inmune a interferencias electromagnéticas.
- Proporciona mayor seguridad que otros medios.
- Mayor cobertura que otros medios.
- Proporciona mayor fiabilidad.

El estándar FDDI especifica un doble anillo de fibra óptica que permite redundancia evitando la pérdida de la información si falla la red. La longitud máxima del anillo es de 200 km o de 100 km si es doble. FDDI puede conectar hasta 500 nodos y la longitud máxima de las fibras es de 200 km, siendo la distancia entre nodos no mayor de 2 km con fibra multimodo, con fibra monomodo es no mayor de 20 km.

FDDI define una serie de protocolos que abarcan las capas uno y dos del modelo OSI.

La capa física está dividida en un subnivel dependiente del medio (PMD) y un protocolo del nivel físico (PHY). El primero define las características del medio de transmisión, tales como los enlaces de FO, niveles de potencia, tasas de error, componentes ópticos y conectores. El protocolo de esta capa define los algoritmos de codificación y decodificación, la temporización de las señales, así como otras funciones.

La capa de enlace queda dividida en un subnivel de control de acceso al medio (MAC) y un subnivel de control del enlace lógico (LLC). LLC está definido por el estándar IEEE 802.2 independientemente de FDDI. El MAC define la forma en la que se accede al medio, incluyendo la especificación del formato de las tramas, la manipulación del testigo (token), el direccionamiento, los algoritmos para calcular los valores CRC (*cyclic redundancy check*) y los mecanismos de recuperación de errores.

De forma adicional, FDDI define la capa de la estación de gestión (SMT) donde se especifica la configuración de la estación FDDI, la configuración y las características del control del anillo que incluye la inserción y extracción de estaciones, inicialización, aislamiento de los fallos y recuperación, programación y recopilación de estadísticas.

1.5.3 ATM

El Modo de Transferencia Asíncrona (ATM, “Asynchronous Transfer Mode”) es una tecnología de conmutación establecida por el ITU-T en 1988 como tecnología de conmutación de la red ISDN en banda ancha.

Esta tecnología es utilizada en redes LAN, MAN, y WAN y proporciona un ancho de banda que soporta la transmisión de datos, voz y video sobre el mismo medio físico.

Como protocolo se clasifica de transporte de alta velocidad, que es implementado en redes que demandan grandes anchos de banda. Es capaz de ofrecer servicios de hasta 155 Mbps.

ATM puede ser considerado como una tecnología de conmutación de paquetes de alta velocidad con las siguientes características:

- Los paquetes son de tamaño constante (53 bytes).
- Es una tecnología orientada a la conexión.
- No tienen mecanismos para el control de errores o control de flujo.

ATM como tecnología está compuesta por nodos de conmutación, elementos de transmisión y equipos terminales de usuarios. Los nodos son capaces de encaminar la información empaquetada en celdas a través de unos caminos conocidos como Conexiones de Canal Virtual.

El ATM como modelo se divide en tres niveles que ocupan la primer capa y parte de la segunda capa del modelo OSI.

1. Nivel de adaptación ATM (AAL)

Se encarga de las relaciones con el mundo externo. Acepta todo tipo de información heterogénea y la segmenta en paquetes de 48 bytes a la velocidad que fue generada por los usuarios. Sólo se encuentra en los puntos terminales de la red.

Su misión es la de aceptar la información adaptando los niveles superiores de comunicación no ATM a los formatos ATM.

Las funciones del nivel AAL son las siguientes:

- Adaptación a la velocidad de los usuarios.
- Segmentación de los datos en celdas de 48 bytes (sin cabecera ATM).
- Detección de celdas erróneas y perdidas.
- Mantenimiento del sincronismo entre terminales.

El Nivel de Adaptación ATM adapta cada tráfico a su velocidad inicial, segmenta o reensambla la información en celdas de 48 bytes, detecta celdas erróneas o perdidas, y mantiene el sincronismo entre los usuarios conectados.

2. Nivel Modo de Transferencia Asíncrona (ATM)

Este nivel es encargado de construir las cabeceras de las celdas ATM, responsable del routing y el multiplexado de las celdas a través de los Canales y Rutas Virtuales. También se encarga del control del flujo de datos y la detección de errores ocurridos en la cabecera aunque no en los datos.

3. Nivel físico (PL)

Es el nivel inferior encargado de controlar las señales físicas, ya sean ópticas o eléctricas, e independizarlas de los niveles superiores de protocolo adaptándolas al medio de transmisión y codificación utilizado. Puede soportar diversas configuraciones punto-a-punto y punto-multipunto. En una red ATM se distinguen dos tipos de nodos: los terminales que proporcionan los puntos de acceso a los usuarios finales y los nodos de conmutación responsables dentro de la red del routing de las celdas.

El nivel físico realiza dos funciones fundamentales: el transporte de celdas válidas y la entrega de la información de sincronismo.

ATM significa integración dada su alta escalabilidad, debido a que puede ser implementada tanto en WANs grandes o en el bus interno de un PC. ATM puede adaptar, debido a las funcionalidades proporcionadas por su AAL, cualquier tipo de tráfico permitiendo la reserva de recursos.

1.5.4 Frame Relay

Frame Relay (FR) fue diseñado originalmente como un protocolo para ser utilizado sobre interfaces RDSI; sin embargo, es utilizado en una gran variedad de redes públicas y privadas que no siguen estándares RDSI.

Frame Relay o retransmisión de tramas como también se le conoce, surgió por hacer más rápida y efectiva la interconexión entre redes LANs e incrementar la velocidad de transmisión de X.25. Se limita a eliminar parte de la carga de protocolo y funciones de X.25 incrementando su velocidad.

Frame Relay está más orientado a un flujo continuo de datos y facilita la consecución de mejores rendimientos y mayor eficiencia. Es un protocolo utilizado en la interfaz entre los dispositivos de usuario (routers, bridges, hosts) y equipos de red (nodos de conmutación) y posibilita la transmisión de los datos aplicando técnicas de conmutación.

Sus principales características se mencionan a continuación:

- Es un estándar.
- Puede "empaquetar" tramas de datos de cualquier protocolo de longitud variable.
- Frame Relay puede ser implementado en software por lo que reduce costos.
- La trama contiene así al identificador de conexión, y es transmitida a través de los nodos de la red en lugar de realizar una "conmutación de paquetes".
- Está orientado a conexión por lo que todas las tramas siguen la misma ruta a través de la red, basadas en un identificador de conexión.

Sin embargo, Frame Relay sólo ha sido definido para velocidades de hasta 1.544 Mbps en T1 o 2.048 Mbps en E1. Considerando que es orientado a conexión puede incrementarse el tiempo de retardo de extremo a extremo ya que es susceptible a perder la información si el enlace falla, ya que deberá realizarse nuevamente la conexión pero por una ruta diferente.

1.6 Dispositivos activos usados en la red

Como ya hemos mencionado, la información es el gran centro vital de una organización. La manera y ubicación en que se almacenen y procesen esos datos son condiciones clave para asegurar su seguridad, integridad, confiabilidad y pronta disponibilidad. Como elemento principal para proteger nuestra red interna del exterior está el equipo activo clasificado de acuerdo a sus funciones.

1.6.1 Repetidor

Es un dispositivo de red que trabaja en la capa física del Modelo de Referencia OSI, su función principal es regenerar la señal transmitida eliminando el ruido y la retransmite sin hacer una interpretación de la misma, únicamente restaura la amplitud y la simetría de dicha señal.

No permite la transmisión simultánea ni el uso de protocolos diferentes ni distintas velocidades de transmisión. Es utilizado para aumentar la distancia a cubrir, así como, el número de nodos que forman la red de datos; también es usado para unir dos medios diferentes en la comunicación dentro de la red.

1.6.2 Hub

Este dispositivo de red trabaja en la capa uno al igual que el repetidor, se dice que el hub es un repetidor multipuerto. Permite compartir el mismo medio a todos los nodos conectados a él, por lo que deben competir por el medio para la transmisión de datos.

Cuando recibe información por un puerto, la retransmite a todos los demás puertos por lo que la eficiencia de la red y la velocidad de transmisión se ven afectadas debido a las colisiones a las que es propensa por el modo de operación del hub. Es por lo anterior que este dispositivo propaga colisiones a todos los nodos conectados a él creando así dominio de colisiones.

1.6.3 Bridge

Es un dispositivo de red que trabaja en la capa de enlace por lo cual tiene acceso a la dirección física (MAC, “Media Access Control”) del dispositivo. Es utilizado principalmente para segmentar una red de datos aislando el tráfico a cada segmento; puede comunicar redes de diferentes velocidades.

Cuando un frame llega al bridge (puente) puede discriminar o no la salida de dicho frame del segmento al que pertenece con base en la dirección física del dispositivo, así evita que la colisión se propague a diferentes segmentos de la red. Utiliza tablas de ruteo para limitar el tráfico a cada segmento, en la tabla guarda las direcciones físicas de cada host aprendido siempre y cuando no expiren las entradas después de algunos minutos, para esto deben seguir transmitiendo.

Dado que no realiza modificaciones en el campo de datos del formato frame es transparente a la capa 3.

El bridge retrasa la velocidad de conmutación más de 1000 microsegundos debido a que transmite el frame hasta que este llegue por completo.

1.6.4 Switch

El switch (conmutador) es un dispositivo activo de red que trabaja en la capa de enlace del modelo OSI, se dice que es un dispositivo inteligente ya que el paquete lo envía únicamente al host destinatario, y no a todos los host como lo hace el hub, utiliza para ello la dirección MAC.

Es una Matriz conmutada ya que permite la transmisión simultánea entre dos host, su función principal al igual que el puente es segmentar dominios de colisión, y debido a que utiliza ancho de banda dedicado para cada host conectado a cada uno de sus puertos limita el tráfico únicamente al segmento que pertenece el frame, aumentando así la velocidad de transmisión.

Se dice que el switch es un bridge multipuerto, la diferencia entre estos dispositivos es que el switch apenas reciba el encabezado del frame inicia la transmisión y no es necesario que reciba todo el frame para transmitirlo como lo hace el bridge.

1.6.5 Router

Es un dispositivo que trabaja sobre la capa de red del modelo OSI y capas inferiores, es utilizado para segmentar una red limitando el tráfico de broadcast, proporciona seguridad y control al dominio de broadcast ya que utiliza filtros de paquetes en ambiente LAN y WAN. Otra de sus funciones principales es soportar rutas redundantes en la red y soportar diferentes tecnologías de enlace de datos tales como: Ethernet, Fast Ethernet, Token Ring, FDI y ATM. El router también es usado como firewall.

Debido a que trabaja en la capa 3 tiene acceso a la dirección lógica de cada host por lo que utiliza algoritmos de enrutamiento para elegir la mejor trayectoria en la transmisión de un paquete.

Se basa en tablas de ruteo que pueden para la elección de dicha trayectoria considerando diversos factores como: el número de saltos, velocidad de la línea, retraso y condiciones de tráfico; la desventaja es que el procesado adicional de paquete por el router puede incrementar el tiempo de espera o reducir el desempeño del mismo al compararlo con un switch, pero a diferencia de este, el router puede distinguir entre diferentes protocolos de red.

Las tablas de ruteo pueden ser creadas estáticamente o dinámicamente, las primeras requieren que el administrador las cree manualmente y no se actualizan automáticamente cuando se producen cambios en la red como lo hacen las tablas dinámicas.

1.6.6 Gateway

Es un dispositivo llamado también pasarela, es utilizado para realizar la conversión de protocolos entre sistemas de comunicación incompatibles. Se dice que el gateway es un servidor que actúa como servidor único para el cliente representando otros servidores que no son capaces de comunicarse directamente con el cliente

Las pasarelas pueden ser de transporte que conectan dos redes en la capa de transporte, o de aplicación que conecta una aplicación dividida en dos partes a nivel de la capa de aplicación.

También existen las medias pasarelas, las cuales son utilizadas cuando dos WAN están unidas por una pasarela y cada una es operada por organizaciones diferentes, entonces cada media pasarela es operada y administrada por cada operador de la red y únicamente se usa un protocolo común a usar en la conexión que une a las medias pasarelas, dicho protocolo no debe favorecer a ninguna parte.

1.7. Diseño de redes de datos

Para llevar a cabo un proyecto es imprescindible la planeación. Y como parte fundamental en la correspondiente a un edificio de una organización, la consideración de la red de datos desde el inicio del proyecto fundamenta su diseño para satisfacer la seguridad y flexibilidad que debe poseer la infraestructura. De ésta manera asegura su crecimiento en el mercado.

1.7.1 Diseño de redes de cómputo

Consideraciones técnicas

Para tener un buen diseño de una red de datos debemos atender algunas consideraciones técnicas que incluyen varios aspectos de la red; como son:

- Escalabilidad. Aquí debemos considerar que tanto podrá crecer una red sin disminuir la velocidad de transmisión y sin tener que llegar a rediseñarla. Para eso siempre se debe tener pensado que una red puede crecer para que el cliente pueda incorporar a un futuro más computadoras.
- Disponibilidad. Las redes de datos tienen siempre periodos de disponibilidad, así como, de periodos no disponibles. En estos periodos cuando la red está disponible se refiere a cuanto tiempo estará en funcionamiento y los periodos no disponibles es cuando se reserva un tiempo para mantenimiento. Para todo esto se deben calcular los problemas que pueda ocasionar el que la red no este operando.
- Rendimiento de la red. Cuando se hace el estudio de la red se deben ver las características del equipo, así como, su rendimiento, las condiciones mínimas y máximas para su correcto funcionamiento, el ancho de banda utilizado, el tiempo de respuesta, etc. Todo esto nos servirá para detectar posibles fallas y las capacidades de la red.
- Seguridad. La seguridad en una red siempre es de gran importancia, debido a la cantidad de información que viaja a través de ella. Para ello se debe negar el acceso a usuarios no autorizados, se deben crear políticas de seguridad, así como, implementar Hardware y software que ayude a proteger la información.
- Administración. El poder administrar una red es la capacidad de monitorear, configurar y corregir los errores que presente, durante su uso.
- Flexibilidad. Es importante que a una red pueda incorporarse nuevas tecnologías o conectarse con dispositivos diseñados para esa tecnología.
- Relación costo-beneficio. Es importante tener en cuenta el no considerar equipo demasiado costoso o barato; sino considerar el equipo que realmente haga funcional la red. Y de la elección que se haga se le debe justificar al cliente para que se de cuenta del beneficio a recibir.

Diseño de la topología

La topología es un mapa en el que se indican segmentos, puntos de interconexión y grupos de usuarios. Con esta información se pueden definir capacidades de los dispositivos y enlaces pero no los dispositivos particulares.

Los diferentes tipos de diseños de topologías son:

- Spaghetti. Puede definirse como una anarquía; la interconexión entre nodos se hace sin orden o planeación. Normalmente esta tecnología es la consecuencia del crecimiento sin plantación de la red y tarde o temprano ocasiona serios problemas para administración de la red, plantación de enlaces, etc.
- Plana. Todos los dispositivos de conmutación tienen la misma funcionalidad; pero no contempla el crecimiento de la red. Comúnmente es utilizada para redes pequeñas pues es sencilla de diseñar y su escalabilidad es limitada (figura 1.25).



Figura 1.25 Topología Plana

- Jerárquica. Es un agrupamiento ordenado de nodos y enlaces. El tráfico con destinos comunes se va agrupando y fluye por enlaces principal es para llegar lo más cerca de su destino y ahí proceder a la desagrupación. Puede decirse que utiliza la filosofía de divide y vencerás (figura 1.26). Está compuesta por una estructura en capas donde cada una hace una función específica:
 - Red de acceso. Proporciona acceso a los usuarios finales.
 - Red de distribución. Es una especie de service access point. Ofrece los servicios de la capa de red a la capa de acceso definiendo las políticas necesarias (traducción de direcciones, políticas de seguridad, etcétera).
 - Red dorsal o núcleo. Conocido como backbone proporciona conectividad entre los sitios. Sus principales objetivos de diseño son la disponibilidad y el desempeño; por lo cual debe tener la capacidad de adaptarse a cambios rápidamente.



Figura 1.26 Topología Jerárquica

El diseño jerárquico permite reducir costos al utilizar equipo especializado en cada nivel; aísla los dominios de difusión, mejorando así el desempeño de los enrutadores y estaciones de trabajo; permite una mejor plantación de capacidad, y en consecuencia, un mayor escalamiento. Su estructura lógica de la red, permite una administración sencilla; también simplifica la evolución gradual de la red y permite aislar fallas en la red.

- Redundante. La redundancia va a evitar la falla de la red en un punto de acceso, duplicando la conectividad de la red. Para esto se debe elegir cuidadosamente el nivel de redundancia, pues tiene una incidencia directa en el costo y en la complejidad de la red. El duplicar componentes de una red para aumentar la redundancia, puede tener el efecto positivo de distribuir la carga aumentando así el desempeño de la red (figura 1.27).



Figura 1.27 Redundancia

Evaluación de servicios de distribución

La evaluación de servicios de distribución, describe las características que estos servicios soportan.

- Administración del ancho de banda del backbone. Configura el envío de mensajes, verifica los protocolos; lo cual permite obtener un rendimiento del ancho de banda a favor.
- Áreas y servicios de filtrado. Permiten o restringen el envío de información a ciertas direcciones de la red.
- Políticas basadas en distribución. Mantienen los diferentes requerimientos en cada departamento sin comprometer el rendimiento y la integridad de la información.
- Servicio de gateway. Los ruteadores permiten el intercambio de información entre dispositivos con diferentes características de direccionamiento.
- Redistribución de los protocolos de ruteo. El ruteador puede funcionar como un gateway para así poder rutear protocolos.
- Traducción de medios. Las técnicas de traducción de los medios de comunicación traducen los paquetes (frame) de un sistema de redes dentro de paquetes de otro sistema.

Evaluación de los servicios de acceso local

La evaluación de los servicios de acceso local menciona los siguientes servicios:

- Direccionamiento de red de valor agregado. Los ruteadores aseguran que cada protocolo que reciben es el protocolo específico de direccionamiento de ayuda.
- El direccionamiento de ayuda es un mecanismo para asistir el movimiento de tráfico específico a través de la red para que el tráfico pueda transitar de otro.
- Segmentación de la red. El segmentar una red es una regla fundamental para los ruteadores de acceso local; en realidad se implantan políticas particulares para limitar el tráfico innecesario.
- Capacidades de broadcast y multicast. La red debe tener la capacidad de controlar el tráfico de broadcast y multicast.
- Broadcast. Son mensajes que se difunden hacia todos los destinos de la red.

- Multicast. Son mensajes que se difunden a un conjunto específico en la red.
- Capacidades de cache local, nombrado y proxy. Estas tres capacidades del ruteador ayudan a reducir el tráfico en la red y promueve una eficiente operación.
- Soporte de servicio de nombre. Las aplicaciones, así como, servicios de conexión proporcionados sobre segmentos de redes; requieren de un método racional para traducir los nombres y direcciones. Para lo cual el ruteador debe soportar el servicio de nombres implementados para diferentes dispositivos de sistema final.
- Servicios de proxy. Son utilizados para cuando las redes no pueden participar en actividades de ruteo o no se puede instalar el software que conforma a los protocolos que generalmente se implementan para la resolución de direcciones.
- Cache de información en la red. Las caches locales previamente aprenden información acerca de la red, así que las nuevas solicitudes de información no necesitan ser transmitidas nuevamente.
- Seguridad de acceso al medio. Se debe mantener vigilancia continua en la red para evitar violaciones de seguridad y el acceso inapropiado de archivos, ya que toda la información está disponible para todos los usuarios de la red.
- Descubrimiento de rutas. Los ruteadores deben proporcionar la mejor ruta para la comunicación de una estación a un dispositivo externo de la red.

1.7.2. Identificación y selección de los dispositivos de red

Para obtener un mejor rendimiento de los dispositivos de red que se van a emplear, es necesario tener en consideración lo siguiente:

- Número de puertos.
- Capacidad y velocidad de procesamiento.
- Costo.
- Protocolos de administración.
- Facilidad de administración.
- Manuales, documentación y software.
- Garantía.
- Soporte técnico.

Los dispositivos básicos de una red se dividen en dos grupos:

- Hubs y Puentes. Estos dispositivos fueron de los primeros en incursionar en la tecnología de las redes de datos. Actualmente se han visto superados por las nuevas tecnologías.
- Switches y Ruteadores. Estos dispositivos debido a su tecnología y su diseño son los que actualmente están dominando en el mercado de las redes. Algunas de sus características de estos dispositivos son las siguientes:

Con el switch se puede acelerar la salida de los paquetes, reducir el tiempo de espera y bajar el costo por puerto. Un switch segmenta una red en pequeños dominios de colisiones, obteniendo un alto porcentaje de ancho de banda para cada estación final.

El ruteador simplemente está diseñado para segmentar la red, con idea de limitar tráfico y proporcionar seguridad, control y redundancia entre dominios. El ruteador es el responsable de crear y mantener tablas de ruteo para cada capa de protocolo de red, y además, permite seleccionar la mejor ruta de comunicación entre dos estaciones.

1.8 Sistemas operativos de red para servidor y clientes

Sistemas operativos para clientes

Actualmente existen varios sistemas para clientes, cada uno procede de diferentes compañías, a lo cual cada uno tiene diferentes características.

Ventajas y desventajas de los sistemas operativos de red para clientes

NOVELL NETWARE

Ventajas

- NDS (Servicio de Directorios de Red) ofrece un directorio global y escalable, que puede diseñarse para gestión centralizada o descentralizada.
- Excelente administración de redes en gran escala.
- Es un sistema operativo de red independiente del hardware.
- Ofrece el mejor sistema de impresión y archivos.
- Excelente nivel de seguridad.
- Soporta aplicaciones a través de Módulos cargables de NetWare (NLM).
- La gran infraestructura de Novell es capaz de dar soporte técnico y asistencia por mucho tiempo.
- Cuando se descubre un error en la versión reciente de NetWare, Novell hace públicas las posibles soluciones para usuarios nuevos y antiguos.
- Mientras más grande sea la red se reduce el costo.

Desventajas

- NDS es bastante complejo de instalar y administrar.
- NetWare está perdiendo mercado por la complejidad de NetWare 4.1 y NDS.
- La plataforma de NetWare está un tanto limitada al proveer otros servicios fuera de servidor de archivos e impresión.
- Servicios como FTP o HTTP requieren comprar software adicional de Novell.
- La actualización de una versión a otra es lenta y compleja.
- Puede ser caro para redes pequeñas.

WINDOWS NT SERVER

Ventajas

- Proporciona una plataforma de propósito general superior.
- Soporta múltiples procesadores.
- Excelente seguridad.
- Existe una gran variedad de aplicaciones diseñadas exclusivamente para NT, incluyendo freeware y shareware.
- Es fácil de instalar y manejar.
- Tiene una interfaz de usuario muy amigable.
- NT es GUI (Interfaz Gráfica de Usuario) y OS (Sistema Operativo) a la vez.
- NT tiene el respaldo de Microsoft, la compañía más poderosa en software del mundo.
- NT está a punto de incorporar soporte completo para UNIX.
- Tiene buen soporte técnico.
- NT es económico para entornos medianos.

Desventajas

- Es un poco lento como servidor de archivos e impresión.
- No soporta cotas de disco.
- Cuando se descubre un error en la versión reciente del sistema, Microsoft se espera al lanzamiento de la siguiente versión para solucionarlo.
- Presenta serias dificultades en entornos muy grandes.
- Mientras crece la infraestructura, el costo de NT sube.
- Necesita muchos recursos de cómputo para funcionar correctamente.

UNIX

Ventajas

- Sistema multiusuario real, puede correr cualquier aplicación en el servidor.
- Es escalable, con soporte para arquitectura de 64 bits.
- El costo de las diferentes variantes de Unix es muy reducido y algunas son gratis, como FreeBSD y Linux.
- Se pueden activar y desactivar drivers o dispositivos sin necesidad de reiniciar el sistema.
- UNIX puede trabajar con CLI (Command Line Interface).
- Los kernels de Unix se confeccionan según las necesidades.
- Los estándares son diferentes de los proveedores (POSIX).
- Ofrece la capacidad de realizar cómputo remotamente.
- Es la mejor solución para enormes bases de datos.

Desventajas

- La interfaz de usuario no es muy amistosa en algunas versiones.
- Requiere capacitación, ya que debido a su complejidad, no cualquiera puede usarlo.
- Padece de la falta de aplicaciones comerciales con nombres importantes.
- La efectividad como servidor de archivos e impresión no es tan eficiente como en otros sistemas operativos de red.
- Hay discrepancias entre los distintos diseñadores y vendedores de UNIX.

MACINTOSH

Ventajas

- Utiliza el microprocesador Power PC, que por su velocidad y eficiencia tiene un futuro promisorio.
- Ambiente de usuario amigable. Es el sistema operativo de red más sencillo de usar.
- Capacidades poderosas en el manejo y diseño de gráficos.
- Compatibilidad consigo mismo. Al comprar nuevo hardware o software, es mucho menos propenso a fallas de instalación.
- Seguridad para servidor de Internet.
- Características de Plug and Play.
- Longevidad. En Macintosh los cambios drásticos de arquitecturas que discontinúan aplicaciones, no se dan.
- Fácil manejo de red.

Desventajas

- Participación de mercado muy reducida.
- No es compatible con PC's y otras arquitecturas.
- No existen clones.
- Algunas veces hay problemas con la multitarea. Una aplicación puede impedir que otras funcionen.

WINDOWS 98 SE.

Ventajas

- Corre en microprocesadores Intel y compatibles.
- En la actualidad ya es obsoleto.
- Interfaz de usuario muy amigable.
- Características de Plug and Play.
- Soporte técnico por dondequiera.
- Compatible con NT hasta cierto punto.
- Muchas aplicaciones disponibles.
- Facilidad de conexión en red.

Desventajas

- El viejo MS-DOS todavía se encuentra detrás de Windows 98 se.
- Contiene algunos errores de fábrica.
- Limitaciones en nombres de archivo.
- Incompatibilidades en nombres de archivo con Windows 3.1
- Es más lento en ambientes multitarea que otros sistemas operativos de red (Macintosh).

WINDOWS 2000 Pro.

Ventajas

- Está construido sobre la sólida fiabilidad de la tecnología Windows NT, mucho más estable que Windows 95 o 98.
- Windows 2000 Professional es rápido que Windows 98. Con 64 MB de memoria, Windows 2000 se ejecuta un 25% más rápido que Windows 98. Y no se hace lento con cargas pesadas.

- Facilita la vida de los administradores. Varios asistentes y detectores de problema ayudan a los usuarios finales a ejecutar tareas rutinarias o difíciles, reduciendo el tiempo que los administradores deben pasar ayudándoles y reduciendo el número de llamadas a soporte técnico.
- Si Windows 2000 detecta un controlador diferente, advierte al usuario acerca del riesgo que está corriendo antes de instalarlo en su sistema.
- Windows 2000 reduce significativamente la cantidad de reinicializaciones al mejorar la forma de instalación del software y hardware.
- La manera en que se les asigna la memoria a las aplicaciones, incluye una protección integrada llamada **Protección Windows de Archivos**, que evita que los archivos del sistema, críticos para el sistema operativo, sean borrados o alterados por los usuarios o sus aplicaciones.

WINDOWS XP Pro

Ventajas

- En Windows XP Home Edition, Microsoft ha combinado las mejores características de sus sistemas operativos de consumo con la eficacia, seguridad y confiabilidad del motor de Windows 2000 para crear un sistema operativo más seguro y agradable de utilizar.
- Impide que las aplicaciones cambien accidentalmente los archivos importantes del sistema operativo. De esta manera, el sistema se protege de forma activa y automática.
- Analiza automáticamente cientos de diferentes medidas del sistema, por ejemplo, memoria, disco y rendimiento de la red.
- Ofrece información útil acerca del rendimiento del equipo y permite terminar programas inactivos.
- El Servidor de seguridad de conexión a Internet protege el equipo de intrusos mientras esté conectado a Internet.
- Cambio rápido de usuario le permitirá compartir un mismo equipo con familiares y amigos sin tener que cerrar las aplicaciones del otro usuario cada vez que necesite tener acceso a su propia cuenta.

- El Asistente para limpieza del escritorio comprueba periódicamente el escritorio y le ofrece la oportunidad de mover los accesos directos que no utilice.

LANTASTIC

Sistema operativo de LANs par a par para PCs de Artisoft, Inc., Tucson, AZ, que destaca por su facilidad de utilización. Soporta su propia topología de par trenzado a 2Mbits/seg así como otros adaptadores Ethernet, ARCNET y Token Ring. Artisoft también hace adaptadores Ethernet junto con placas de 2MBps. También se incluyen funciones e-mail (correo electrónico) y chat (charla). El envío de voz y las conversaciones son opcionales.

Ventajas

- Maneja niveles de seguridad muy buenos.
- Es económico.
- Soporta más de 500 usuarios.
- Fácil instalación y operación.
- Fácil interfaz con Microsoft y Novell.

Desventajas

- Se tiene que hacer un gasto extra para adquirirlo. (Windows 95 y Macintosh incluyen gratis software de red punto a punto).
- No existe soporte para LANtastic en todos lados.
- Participación de mercado reducida.

Sistemas operativos para servidor de archivos

Para el servidor de archivos se analizaron y compararon tres sistemas operativos basados en tecnología de Microsoft debido a que ya ha manejando (tabla 1.28).

Concepto	Windows NT Server 4.0	Windows 2000 Server	Windows Server 2003
Directorio Activo	No disponible	Incluido	Mejorado con renombrado de directorios, modo de aplicación de Directorio Activo y replicación más eficiente
Políticas de grupo	No disponible	Incluido	Mejorada con decenas de nuevas características
Consola de gestión de Políticas de grupo	No disponible	No disponible	Proporciona gestión de estaciones de trabajo basada en directorios, permitiendo cambios sobre múltiples usuarios / máquinas mediante una sola orden administrativa
Internet information Services 6.0	No disponible	No disponible	Mejoras significativas en la arquitectura realizadas para superar los requisitos de fiabilidad de los clientes
Recuperación Automática del Sistema (ASR)	No disponible	No disponible	ASR permite la restauración en un solo paso del sistema operativo, el estado del sistema y la configuración del hardware
Servicio Volume Shadow Copy	No disponible	No disponible	Permite a los usuarios recuperar versiones previas de archivos almacenados en unidades de red sin intervención administrativa
.NET Framework integrada	No disponible	Está disponible la descarga de algunos componentes*	Plataforma de aplicaciones completamente integrada
Servicios UDDI Empresariales	No disponible	No disponible	Ayuda a las empresas a organizar y catalogar los servicios Web
Re-autenticación wireless más rápida	No disponible	No disponible	Asegura una experiencia de usuario sin interrupciones
Gestor de Recursos del Sistema de Windows	No disponible	No disponible	Empleado para establecer las limitaciones de recursos asignadas a aplicaciones servidor
Gestiona tu servidor/ configura tu servidor	No disponible	Limitado a la configuración del servidor	Muestra tareas administrativas comunes, listas de comprobación y ayuda relevante para realizar estas tareas

Tabla 1.28 Comparación de sistemas operativos basados en tecnología de Microsoft

Servidor de Web y de Bases de Datos

Para este servidor se compararon dos sistemas operativos los cuales a continuación se muestran en la tabla 1.29.

Componente	Linux	Windows NT Server 4.0
Sistema Operativo	Gratis, o sobre \$49.95 para una distribución en CD-ROM	Versión para cinco usuarios \$809
10 Usuarios \$1129		
"Enterprise Edition" 25-Usuarios \$3,999		
Soporte técnico gratuito on-line	Sí, Linux Online o Redhat	No
Código fuente del kernel	Sí	No
Servidor Web	Apache Web Server	IIS
Servidor FTP	Sí	Sí
Servidor Telnet	Sí	No
Servidor SMTP/POP3	Sí	No
DNS	Sí	Sí
Sistemas de Ficheros de Red	NFS and SMB	Only SMB
Servidor X Window (Para ejecutar aplicaciones gráficas remotas)	Sí	No
Herramientas de Mantenimiento Remoto	Sí, todas	Solo "User Manager for Domains" y "Server Manager"
Servidor de News	Sí	No
Compiladores C and C++	Sí	No
Perl 5.0	Sí	No
Control de Revisiones	Sí	No
Number of file systems supported	32	3
Número de interfaces a escoger	4	1

Tabla 1.29 Comparación de sistemas operativos para servidores

1.9 Políticas de red

Para conectar una red de computadoras a Internet, es necesario saber que tipo de información y servicios se deben proteger. Las políticas de red son un conjunto de recursos destinados a lograr que la información de una organización sea confidencial, íntegra, consistente y disponible a sus usuarios, autenticados por mecanismos de control de acceso y sujetos a auditoria.

Las políticas de red no deben entorpecer las actividades de los usuarios; esto es, que los usuarios deben tener acceso a la información necesaria para desempeñar eficientemente su trabajo. Es decir, “Una política de seguridad en redes efectiva es algo que todos los usuarios y administradores de redes pueden aceptar y están dispuestos a aplicar”.

Política de seguridad del sitio

Una red puede tener varios sitios o áreas, y cada uno de estos contar con sus propias redes. Y si la red es grande probablemente cada uno de esos sitios tengan una administración diferente en cuanto a la seguridad, teniendo metas y objetivos diferentes a cada sitio.

En general, un sitio o área es cualquier parte de una organización que posee computadoras y recursos relacionados con redes. Algunos de estos recursos pueden ser:

- Estaciones de trabajo.
- Computadoras host y servidores.
- Dispositivos de interconexión: gateways, routers, switches, hubs, repetidores.
- Servidores de terminal.
- Software para conexión de red y de aplicaciones.
- Cables de red.
- La información de archivos y bases de datos.

La política de seguridad de sitio debe tomar en cuenta la protección de los recursos arriba mencionados. Debido a que el sitio esta conectado a otras redes, la política de seguridad del sitio debe considerar las necesidades y requerimientos de seguridad de todas las redes interconectadas.

Para proteger estos recursos se tienen las siguientes políticas:

- Mantener las computadoras alejadas del fuego, humo, polvo y temperaturas extremas.
- Colocar las computadoras fuera del alcance de rayos solares, vibraciones, insectos, ruido eléctrico (balastras, equipo industrial, etc.), agua, etc.
- Todos los servidores serán ubicados en lugares de acceso físico restringido y deberán contar para acceder a ellos puertas con chapas.
- El lugar donde se instalarán los servidores deberán contar con una instalación eléctrica adecuada, entre sus características con tierra física. Y dichos equipos deberán contar con NO-BREAKS.
- En los lugares donde se encuentren equipo de cómputo queda prohibido el consumo de bebidas y alimentos.
- El lugar donde se encuentre los servidores se mantendrán en condiciones de higiene.
- Deberá contarse con extintores (para material eléctrico y no eléctrico) en las salas de cómputo. El personal deberá estar capacitado en el uso de extintores.
- Las salas de cómputo deberán contar con una salida de emergencia.

Planteamiento de la política de seguridad

El especificar una política de seguridad de red significa elaborar procedimientos y planes que protejan los recursos de la red contra pérdida y daño. Para delimitar y concretar las políticas de seguridad podemos usar las siguientes preguntas:

- ¿Qué recursos se están tratando de proteger?
- ¿De quiénes se necesita proteger los recursos?
- ¿Qué tan posibles son las amenazas?
- ¿Qué tan importante es el recurso?
- ¿Qué medidas puede implementar para proteger sus bienes de forma económica y oportuna?
- Examine periódicamente su política de seguridad de red para ver si han cambiado los objetivos y las circunstancias de la red.

Se debe tener en cuenta que cuando se necesita proteger una red, el costo de protegerla debe ser menor que el de recuperación en caso de que se viera afectado por una amenaza de seguridad. Para hacer el análisis de seguridad debe participar la gente adecuada para definir grupos y niveles de acceso a los usuarios; así como, participar con estos grupos de gente para discutir y aceptar las políticas de seguridad.

Para reducir las amenazas de seguridad la mejor defensa es el conocimiento. A los usuarios se les debe dar a conocer el uso adecuado de los sistemas de cómputo y saber cómo protegerse a sí mismos de accesos no autorizados. Para ello se debe hacer ver a la gente involucrada, los peligros a los que se está expuesto en el ambiente de las redes de computadoras.

Análisis de riesgo

Cuando se crean las políticas de seguridad de red, no se debe perder de vista que es lo que se requiere asegurar y que el costo de asegurarlo no cueste más. Para determinar el análisis de riesgo es conveniente plantearse lo siguiente:

- Que se necesita proteger.
- De que se necesita proteger.
- Como protegerlo

La evaluación de una amenaza y los riesgos no deben ser una actividad de una sola vez; es decir que no deben realizarse una sola vez y ya; si no debe ser una actividad monitoreada y actualizada constantemente.

Identificación de recursos

Cuando se realice el análisis de riesgo ya se podrá identificar todos los recursos que corran el riesgo de sufrir una violación de seguridad. Los recursos como el hardware deben ser incluidos dentro del análisis de riesgo, sin olvidar incluir a los usuarios del sistema. Es importante que se incluyan todos los recursos de la red que puedan ser afectados por un problema de seguridad.

Los siguientes recursos son los que se recomiendan al calcular las amenazas a la seguridad general:

- Hardware. procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, servidores terminales, routers, switches.
- Software. programas fuente, programas objeto, utilerías, programas de diagnostico, sistemas operativos, programas de comunicaciones.
- Datos. durante la ejecución, almacenados en línea, archivados fuera de línea, respaldos, registros de auditoria, bases de datos, en transito a través de medios de comunicación.
- Personas. usuarios, personas necesarias para operar los sistemas.
- Documentación. sobre programas, hardware, sistemas, procedimientos administrativos locales.
- Suministros. papel, formularios, cintas, medios magnéticos y ópticos.

Identificación de las amenazas

Ahora que se han identificado los recursos que se necesitan proteger, se requiere identificar las amenazas a las que están expuestos. Pueden examinarse las amenazas para determinar que posibilidad de perdida existe. También se debe identificar de cuales amenazas se están tratando de proteger los recursos.

A continuación se describen algunas de las amenazas posibles:

Definición del acceso no autorizado. El acceso a los recursos de la red debe estar permitido sólo a los usuarios autorizados. Comúnmente conocido como acceso autorizado. El acceso no autorizado en general es el uso de cualquier recurso de la red sin el permiso previo.

Riesgo de revelación de información. La revelación de información, ya sea voluntaria o involuntaria, es también otro tipo de amenaza. Se le debe asignar el valor y la forma en que se debe tratar cada tipo de información.

Negación del servicio. Las redes de computadoras vinculan recursos valiosos, como computadoras y bases de datos, y proporcionan servicios de los cuales depende la organización. La mayoría de estos usuarios depende de estos servicios para realizar su

trabajo con eficacia. Si no están disponibles estos servicios, hay una pérdida correspondiente de productividad.

Identificación de quien está autorizado para usar los recursos de la red

Se debe hacer una lista de los usuarios que requieren acceso a los recursos de la red. Para esto no es necesario enumerar a cada uno de estos usuarios; la mayoría pueden dividirse en grupos y así asignarle derechos a grupos.

Identificación del uso adecuado de los recursos

Una vez que se han determinado los usuarios que están autorizados a los recursos de la red, se deben establecer los lineamientos del uso aceptable de dichos recursos. La restricción de los recursos debe ser acorde a las funciones que desempeñe el usuario y a sus requerimientos. Lo delicado es equilibrar el acceso restringido a los privilegios especiales para hacer más segura la red; es decir, se deben conceder solo los privilegios suficientes para realizar las tareas necesarias.

Para la identificación de los usuarios que van a tener acceso a la red; se les va a asignar una cuenta con su respectiva contraseña a los usuarios que pertenezcan a la DUAD o tengan autorización del jefe de la misma, esta cuenta y su contraseña son intransferibles.

En lo que respecta a las contraseñas esta es la única forma de autenticar al usuario, por lo que es la última defensa contra ataques. Para ello se tienen las siguientes políticas:

- El administrador de la red será el responsable de asignar las contraseñas.
- La longitud de una contraseña deberá siempre ser verificada de manera automática al ser construida por el administrador o el usuario. Todas las contraseñas deberán contar con al menos seis caracteres.
- Las contraseñas elegidas por los usuarios deben ser difíciles de adivinar. No deben ser utilizadas palabras que aparezcan en el diccionario, secuencias conocidas de caracteres, datos personales ni acrónimos.
- Está prohibido que los usuarios construyan contraseñas compuestas de algunos caracteres constantes y otros que cambien de manera predecible y sean fáciles de adivinar.

- Los usuarios no deben construir contraseñas idénticas o muy parecidas a contraseñas anteriores.
- La comunicación de la contraseña se realizará de manera personal y no se podrá informar a otra persona que no sea el interesado.
- No se podrán informar contraseñas por vía telefónica.
- Las contraseñas del administrador deberán cambiarse máximo cada seis meses.

A continuación se muestran algunos aspectos a considerar para la determinación de responsabilidades y derechos para usuarios así como para administradores.

Para los usuarios:

- Crear lineamientos que consideren el uso de los recursos de red, tales como que usuarios están restringidos y cuales son sus restricciones.
- Contemplar que constituye un abuso en términos de usar recursos de red y afectar el desempeño del sistema y de la red.
- No permitir que los usuarios puedan compartir sus contraseñas.
- Los Usuarios no podrán revelar su contraseña por ningún motivo ya que es la única manera de autenticación.
- Determinar que usuarios deben cambiar su contraseña y con que frecuencia, todo esto para aumentar la seguridad de algunos usuarios.
- Definir quien es el que deberá hacer el respaldo de los datos del usuario, el Administrador o el usuario mismo.
- Detallar las consecuencias para los usuarios que divulguen información confidencial del sistema.
- Avisar de estas políticas a todos los usuarios, así como las sanciones a las faltas de las políticas de seguridad.

Para los administradores

- El administrador puede revisar o leer los archivos de un usuario, si es que la seguridad de la red está en riesgo.
- Los administradores tienen derecho a examinar el tráfico de la red o de la estación de trabajo.
- El administrador podrá aplicar sanciones a los usuarios que pongan en riesgo la seguridad de la red.

Las políticas que especifican como deben los usuarios acceder al sistema, desde donde y de que manera deben autenticarse; son las siguientes:

- Todos los administradores que den un servicio de acceso remoto deberán contar con aplicaciones que permitan una comunicación segura y encriptada.
- Todos los usuarios deberán autenticarse con su cuenta y no podrán hacer uso de sesiones activas de otros usuarios.
- Todos los usuarios deberán acceder al sistema utilizando algún programa que permita una comunicación segura y encriptada.
- Está prohibido acceder al sistema con una cuenta diferente de la propia, aún con la autorización del dueño de dicha cuenta.
- El usuario tendrá el derecho a cambiar su contraseña.
- El usuario podrá utilizar los servicios de sesiones remotas si se brinda.

Plan de acción cuando es violada la política de seguridad

Cuando en nuestra red es violada la política de seguridad, la red esta expuesta a amenazas. Si no se ocurren cambios en la seguridad de la red, entonces debe modificarse la política de seguridad para eliminar aquellos elementos que no sean seguros.

Cuando una política de seguridad de una red es muy restrictiva, esta va a tender a ser violada; por lo cual la política de seguridad no debe ser muy restrictiva, ni muy abierta. Se debe hallar un equilibrio para que los usuarios no intenten violarla.

Respuesta a las violaciones de la política

El documento de política de seguridad debe obtener procedimientos para manejar cada tipo de incidente de violación; por ejemplo cuando un usuario viola la política de seguridad de la red local o la de una red remota; o en otro caso, si la seguridad de la red es violada por un usuario local o remoto “foráneo”. Debe llevarse un registro apropiado de tales violaciones, el cual se debe revisar con frecuencia para observar las tendencias y tal vez ajustar la política de seguridad para que dicha política tome en cuenta cualquier nuevo tipo de amenazas.

Identificación y prevención de problemas de seguridad

El objetivo de la política de seguridad es definir lo que se necesita proteger, pero no señala explícitamente como deberán protegerse los recursos y el enfoque general para manejar los problemas de seguridad. Además de establecer las políticas de seguridad, se deben identificar los puntos vulnerables, por ejemplo como los siguientes:

- Puntos de acceso. Los puntos de acceso son los puntos de entrada (también llamados de ingreso) para los usuarios no autorizados. Par evitar esto, es importante incluir dentro de la política de seguridad que esta prohibido realizar conexiones privadas a estaciones de trabajo dentro y fuera de la red de datos, sin permiso alguno.
- Sistemas mal configurados. Cuando un individuo llega a penetrar en la red, por lo general los blancos preferidos son los servidores; si estos servidores están mal configurados son responsables de numerosos problemas dentro de la red. Para esto es necesario entender el funcionamiento de los sistemas operativos y software correspondiente para entender como funciona el sistema y poder dar una mejor seguridad a la red.
- Problemas de software. Por lo general cuando aumenta la complejidad del software aumenta el número y la complejidad de los problemas de un sistema determinado. Las fallas de seguridad conocidas públicamente se vuelven métodos de acceso no autorizado. Si la implementación de un sistema es abierta y muy conocida (como Unís o Linux), el intruso puede usar los puntos débiles del código de software que se ejecuta en modo administrador para tener acceso privilegiado al sistema. El administrador debe estar consiente de los puntos débiles de sus sistemas operativos y tiene la responsabilidad de obtener las actualizaciones y de implementar las correcciones cuando se descubran problemas relacionados con estos.

- Amenazas internas. los usuarios internos tienen más acceso al software de la computadora y de la red que al hardware. Si un usuario decide perturbar la red, puede representar una considerable amenaza a la red. Para evitar estos problemas es necesario evitar el acceso a los servicios de telnet, rlogin y ftp, desde cuentas privilegiadas.
- Seguridad física. La computadora del usuario debe ser físicamente segura. Todos los equipos de suma importancia de funcionamiento a la red deben estar ubicados en un área físicamente segura.

1.10 Herramientas de mantenimiento y monitoreo de una red de datos

El monitoreo y mantenimiento de una red de datos es una actividad básica, ya que permite saber con anticipación sobre las posibles caídas del sistema, así como tiempos de respuesta, velocidad de transmisión de datos; entre otros datos de gran utilidad para la administración de la red.

Actualmente existen varias empresas que ofrecen productos que ayudan a la administración de la red de datos. A continuación mencionaremos algunas.

HP OpenView. Esta herramienta es una de las más utilizadas, ya que se asegura que más del 70% de los dispositivos de red de todo el mundo están administrados por HP OpenView. Algunos de los principales beneficios ofrecidos por este producto es la capacidad de monitorear y controlar el sitio WEB de las empresas, además de permitirles asegurar la calidad y administración de servicio, así como, la seguridad de transacciones electrónicas y su infraestructura analiza el tráfico de la red y aísla la fuente de problemas de la infraestructura y así, poder evitar que estos ocurran.

CA Unicenter. CA ya está preparada para la vigilancia de la red. Sus productos, Unicenter Wireless Network Management y Unicenter Mobile Device Management, facilitan la administración tanto de infraestructuras de redes inalámbricas como de dispositivos móviles. La solución de seguridad para redes inalámbricas Unicenter Wireless Network Management incluye el descubrimiento automático de puntos de acceso inalámbrico y dispositivos LAN, visualización avanzada en topología LAN inalámbrica, recolección de datos de configuración crítica, disponibilidad e información de rendimiento y detección integrada de intrusos.

Tivoli. Es un software de seguridad, gestión y almacenamiento. Tivoli es una marca de IBM Corporation desde su adquisición en 1996. Este software permite a las organizaciones:

- Reducir el coste total de propiedad y mejorar los niveles de servicio de su infraestructura de la red de datos.
- Mantener un entorno informático seguro y dinámico entre socios, proveedores, clientes y empleados.

El software de gestión de Tivoli es útil tanto a las empresas tradicionales como a los negocios e-business en todo el mundo para gestionar la seguridad, almacenamiento, rendimiento, disponibilidad, configuraciones y operaciones de su infraestructura de la red de datos.

Cheops. Este es un programa conocido como la navaja del ejercito suizo de Internet, y no es para menos, ya que es capaz de sacar el mapa de la red, dibujar los enlaces, detectar las máquinas y su sistema operativo automáticamente, detecta y monitoriza los servicios, escanea los puertos, accede a servicios y mucho mas.

Tkined. Es un editor de red que ofrece extensiones para crear un entorno de trabajo completo, integrando algunas herramientas para localizar redes IP, soporte para el proceso de instalación de la red o resolución de problemas en redes IP utilizando SNMP en combinación con otras utilidades estándar (por ejemplo, traceroute).

LanExplorer. Es una poderosa herramienta administrativa que permite monitoreo de redes, análisis de tráfico, análisis de protocolos y solución de problemas de redes y tráfico de Internet. Es capaz de capturar, mostrar, decodificar y filtrar; proporciona muy buena información para resolver problemas y detectar redes dañadas. Lanexplorer proporciona un análisis detallado de los paquetes que viajan a través de la red; con esta opción se puede analizar paquetes en forma Hexadecimal, ASCII y decodificar el formato de cualquier paquete capturado a través de la red.

Capítulo 2

Sistema de cableado estructurado

Las comunicaciones hoy en día son un recurso muy importante para las organizaciones en el campo competitivo. Dado que se requiere obtener la información lo más rápido posible y a menor costo, es importante contar con una infraestructura de redes que les permita incorporar nuevas tecnologías como: video de banda ancha, intranet, imágenes tridimensionales, programas multimedia, entre otras.

2.1 Historia del cableado estructurado

Antes de que el Sistema de Cableado Estructurado (SCE) se concibiera como norma, el único cable utilizado para el cableado de edificios era el cable telefónico instalado por las compañías que suministraban conmutadores y teléfonos. Debido a que estas redes de cables sólo manejaban comunicaciones de voz era necesario instalar un segundo sistema privado de cables, lo que demandaba personal capacitado para cada sistema de cableado.

Las redes privadas eran exclusivas de un fabricante en particular que realizaba la instalación de cables de acuerdo a sus necesidades; dado que no podía ser utilizado por otros fabricantes dificultaba al cliente el cambio de proveedor. Dicha incompatibilidad con el cableado obligaba al cliente a comprar al anterior o a cambiar nuevamente toda la red.

Las instalaciones se realizaban de acuerdo a las necesidades de incorporar nuevos equipamientos y la demanda de nuevos usuarios.

2.1.1 Definición del sistema de cableado estructurado

El cableado estructurado es la metodología, basada en estándares de planeación, diseño e instalación, de un sistema de cableado capaz de integrar servicios de voz, datos, video, tráfico de Internet, seguridad, así como, a los sistemas de control y automatización de un edificio bajo una plataforma abierta. Lo que permite que esos servicios estén disponibles desde y hacia cualquier roseta de la conexión, utilizando un medio de transmisión independiente de la aplicación y de tecnología abierta.

Debido a la serie de lineamientos en los que se basa el SCE, se permite la implementación de redes de voz y datos seguros y confiables basadas en estándares internacionales que facilitan la intercomunicación y garantizan calidad, seguridad, capacidad, compatibilidad y escalabilidad.

2.1.2 Diferencias entre el cableado estructurado y no estructurado

La disponibilidad de la información y el rápido acceso a la misma, así como el rendimiento de la red, dependen de la infraestructura tecnológica con que se cuente, como lo es: provisión de equipamiento, conectividad y servicios de comunicación, asistencia técnica y exploración tecnológica.

Así entonces, el cableado estructurado a diferencia del no estructurado permite contar con una red capaz de adaptarse al cambio y al crecimiento, facilitando la administración de la misma por medio de una presentación de cables de forma ordenada y sistemática.

Beneficios del sistema de cableado estructurado

- Maximizar la velocidad, confiabilidad, eficiencia y seguridad de la red.
- El cableado estructurado implementa generalmente topología estrella, lo que permite una mayor flexibilidad para mover a los usuarios de la red, así como, futuras incorporaciones de los mismos.
- Aprovechamiento de espacios en instalaciones.
- Minimiza el costo de los cambios implicados.
- Ahorro a largo plazo dentro del ciclo de vida del cableado. Las fallas de un cableado mal diseñado o mal implementado son costosas.
- Proporciona la posibilidad de utilizar la misma red para dar servicio a una gama de sistemas diferentes.
- Independencia de proveedores. Es un sistema de tecnología abierta que brinda a los usuarios la libertad de conectar equipos de diferentes proveedores.
- Disminución del tráfico de red.
- Oportuna asimilación y aprovechamiento de nuevas tecnologías de la información para enfrentar la creciente competitividad.
- Disminución de costos de mantenimiento.
- Disminución de los tiempos de respuesta para atender nuevas necesidades de servicios.
- Simplifica la resolución de problemas, la identificación y el aislamiento de la falla.
- Facilita la administración y seguimiento del sistema.

2.2 Estándares en los sistemas de cableado estructurado

Debido a la gran variedad de fabricantes y características de redes y equipo de redes, para conseguir que el cableado estructurado sirva para todas ellas, es necesario que exista una normativa en cuanto a lo que va a circular por la red, como lo va a hacer y lo que necesita para que esto ocurra. Es importante fijar los parámetros, que deben ser uniformes para todos, de tal manera que la forma en la que esté realizada la infraestructura no fije un modo de funcionamiento para cada una de ellas, y además, es preciso que todos los dispositivos (actuales y en desarrollo) se adapten a estas normas; es decir, elimina la necesidad de seguir las reglas de un proveedor en particular, concernientes a tipos de cable, conectores, distancias o topologías; permite instalar una sola vez el cableado, y después adaptarlo a cualquier aplicación, desde telefonía, hasta redes locales Ethernet o Token Ring, o para tecnologías emergentes.

Un grupo de organizaciones publicó conjuntamente estándares para la manufactura, instalación y rendimiento del equipo y sistemas de telecomunicaciones y eléctrico. El estándar de ANSI/TIA/EIA (Instituto Nacional de Estándares, Asociación de Industrias de Telecomunicaciones, Asociación de Industrias Electrónicas) precisa un sistema uniforme de telecomunicaciones para edificios comerciales, los requerimientos para el cable, hardware, equipo y diseño. El estándar de la ANSI/TIA/EIA menciona cinco principales estándares que predominan en el cableado de telecomunicaciones en edificios; y estos son:

- ANSI/TIA/EIA-568-A. Estándar de Cableado de Telecomunicaciones en Edificios Comerciales.
- ANSI/TIA/EIA-569. Estándar para Ductos y Espacios de Telecomunicaciones en Edificios Comerciales.
- ANSI/TIA/EIA-570. Estándar de Alambrado de Telecomunicaciones Residencial y Comercial Pequeño.
- ANSI/TIA/EIA-606. Estándar de Administración para Infraestructura de Telecomunicaciones en Edificios Comerciales.
- ANSI/TIA/EIA 607. Requerimientos de Puesta a Tierra para Telecomunicaciones.

2.2.1. ANSI/TIA/EIA-568-A: Estándar de Cableado de Telecomunicaciones en Edificios Comerciales

El estándar 568-A se describe como un sistema general de alambrado de telecomunicaciones para edificios comerciales que puede soportar un ambiente de múltiples productos y proveedores.

El propósito de este estándar es aprobar el diseño e instalación del cableado de telecomunicaciones contando con poca información acerca de los productos de telecomunicaciones que posteriormente se instalarán. La instalación de los sistemas de cableado durante el proceso de instalación y/o remodelación son representativamente más baratos e involucran menos interrupciones después de ocupado el inmueble.

Este estándar especifica:

- Requerimientos mínimos para cableado de telecomunicaciones dentro de un ambiente de oficina.
- Topología y distancias recomendadas.
- Parámetros de medios de comunicación que determinan el rendimiento.
- La vida productiva de los sistemas de telecomunicaciones por cable por más de 10 años (15 actualmente).

De acuerdo al estándar 568-A, un sistema de cableado estructurado se fundamenta en los siguientes seis subsistemas:

1. Subsistema Entrada del Edificio.
2. Subsistema Cuarto de Equipo.
3. Subsistema Cableado Horizontal.
4. Subsistema Cuarto de Telecomunicaciones.
5. Subsistema Cableado Vertical (Backbone).
6. Subsistema del Área de Trabajo.

Dichos subsistemas son mostrados en la figura 2.1.

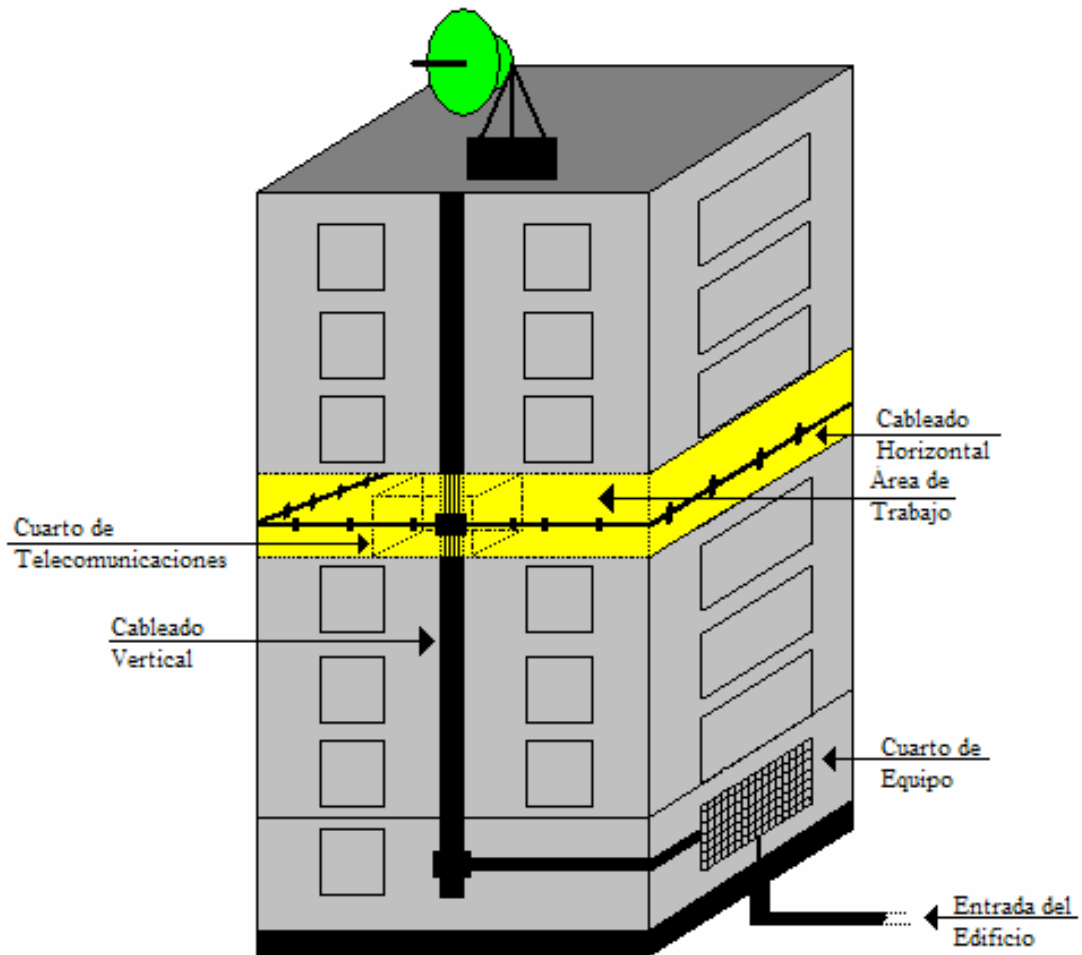


Figura 2.1 Cableado de Telecomunicaciones en Edificios Comerciales.

1 Subsistema Entrada del Edificio

El subsistema de entrada del edificio, se define como el lugar en el cual ingresan los servicios de telecomunicaciones al edificio y/o donde llegan las canalizaciones de interconexión con otros edificios de la misma agrupación.

Este subsistema puede contener las interfaces de acceso de la red pública, así como equipos de telecomunicaciones; además de que consiste en una entrada de servicios de telecomunicaciones al edificio, la cual incluye el punto de entrada a través de la pared del edificio y continuando al cuarto o área de entrada. Si existen enlaces privados entre edificios, la ruta del backbone que interconecta a los edificios pertenece a este subsistema de igual modo si el edificio cuenta con una comunicación a través de una antena (figura 2.2).

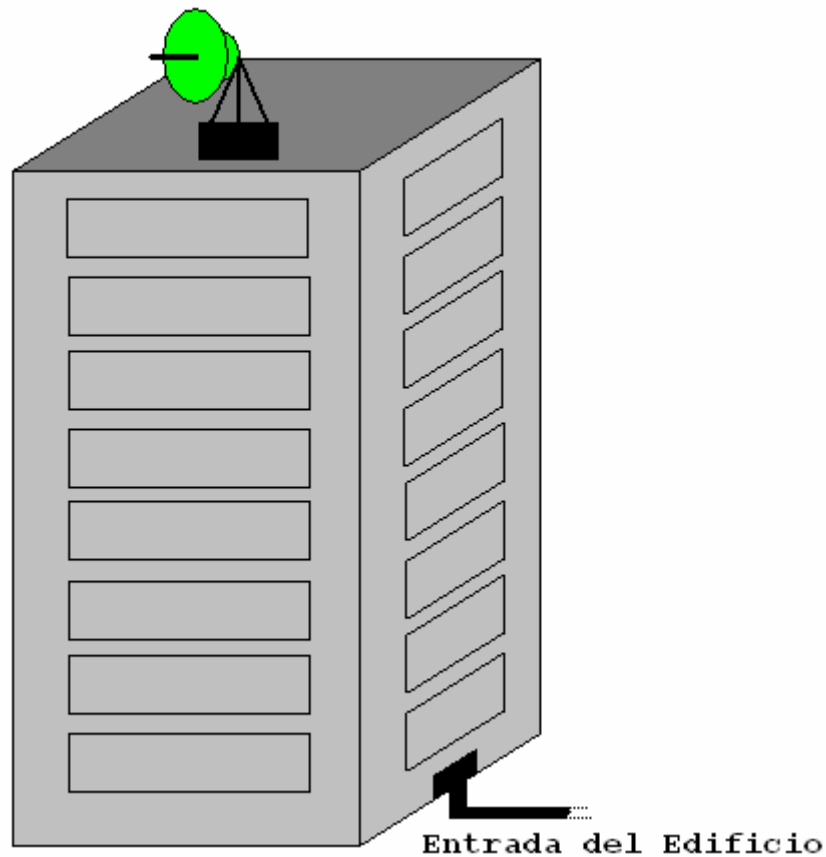


Figura 2.2 Subsistema Entrada del Edificio

2. Subsistema Cuarto de Equipo

El subsistema de cuarto de equipo se define como el cuarto donde se alojan los equipos de telecomunicaciones (PBX, Servidores, Switch, Router, etc.). En este cuarto solo se admiten equipos que van directamente relacionados con los sistemas de telecomunicaciones y sus elementos de soporte. Los cuartos de equipo se consideran distintos de los cuartos de telecomunicaciones por la naturaleza, costo, tamaño y/o complejidad del equipo que contienen. Los cuartos de equipo incluyen espacio de trabajo para personal de telecomunicaciones. Todo edificio debe contener un cuarto de telecomunicaciones o un cuarto de equipo (figura 2.3).

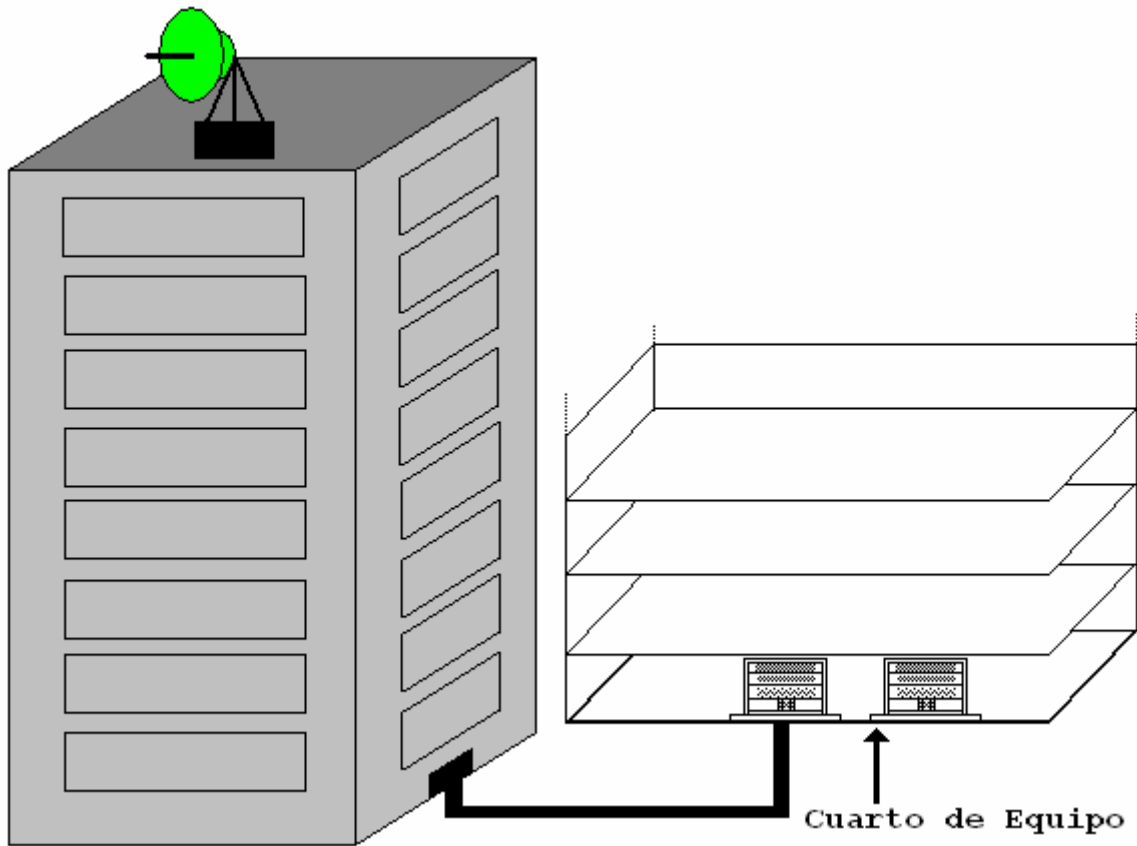


Figura 2.3 Subsistema Cuarto de Equipo

3. Subsistema Cableado Horizontal

El subsistema de cableado horizontal es la segmento del cableado que se extiende desde el área de trabajo hasta el cuarto de telecomunicaciones. El término “horizontal” se utiliza porque propiamente este cableado se desplaza de una manera horizontal en el edificio.

El cableado horizontal consta de los siguientes elementos básicos:

Cable horizontal y el hardware de conexión

El cable horizontal y el hardware de conexión proveen los medios para transportar señales de telecomunicaciones entre el área de trabajo y el cuarto de telecomunicaciones. Estos componentes son los "contenidos" de las rutas y espacios horizontales (figura 2.4).

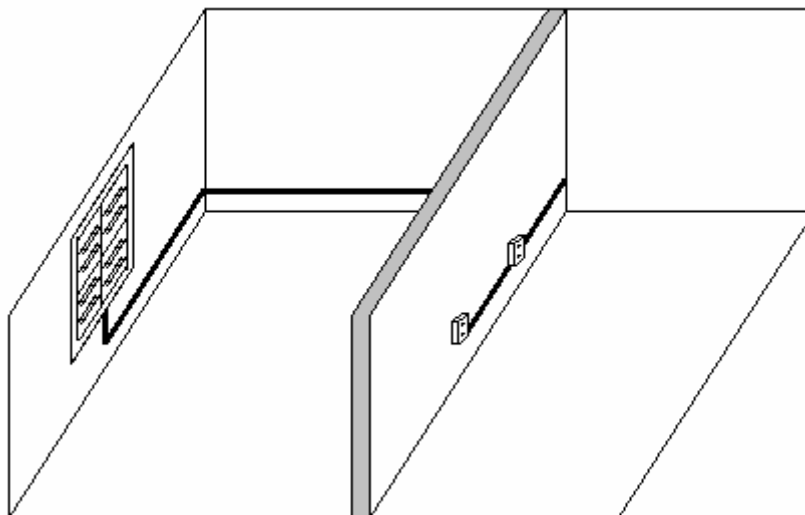


Figura 2.4 Subsistema Cableado Horizontal

El cableado horizontal incluye:

- Las salidas (cajas/placas/conectores) de telecomunicaciones en el área de trabajo.
- Cables y conectores de transición instalados entre las salidas del área de trabajo y el cuarto de telecomunicaciones.
- Paneles y cables utilizados para configurar las conexiones de cableado horizontal en el cuarto de telecomunicaciones.

Consideraciones para el cableado horizontal

- Distancias horizontales

La distancia horizontal máxima desde el área de trabajo de telecomunicaciones hasta el cuarto de telecomunicaciones es de 90 m independientemente del cable utilizado. Al establecer la distancia máxima se hace una previsión de 10 m Adicionales para la distancia combinada de cables de parcheo (3 m) y cables utilizados en la conexión de equipo en el área de trabajo y el cuarto de telecomunicaciones.

- Tipos de Cables

Existen tres tipos de cables que pueden ser usados en los sistemas de cableado horizontal:

- Cable UTP (Unshielded Twisted Pair).
- Cable STP (Shielded Twisted Pair).
- Fibra Óptica.

Para elegir adecuadamente el tipo de cable es necesario usar el mejor cable del mercado que permita la mayor velocidad de transmisión y que este calificado en un estándar, para garantizar el mejor desempeño de la red.

- Salidas de área de trabajo

Los ductos a las salidas del área de trabajo deben proporcionar la capacidad de manejar tres cables. Las salidas del área de trabajo deben contar con un mínimo de dos conectores; las salidas de área de trabajo deben contar con un mínimo de dos conectores, el cual al menos uno debe ser del tipo de RJ-45 bajo el código de colores de cableado T568-A ó T568-B la diferencia es que en el cableado T568-A tiene el par naranja terminado en los pines 3 y 6, el par verde terminado en los pares 1 y 2, el cableado T568-B sólo invierte la terminación del par naranja como se muestra a en la figura 2.5.

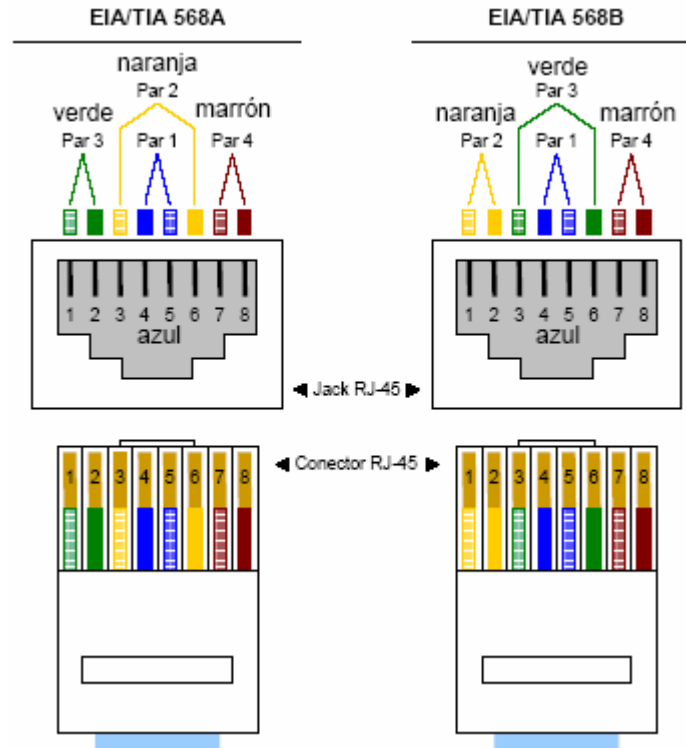


Figura 2.5 Código de colores de cableado T568-A Y T568-B

- Manejo del cable

El destrenzado de cables de pares individuales en los conectores y paneles de parcheo debe de ser menor a 1.25 cm para cables UTP categoría 5e.

El doblado del cable no debe de ser menor a cuatro veces el diámetro del cable. Para par trenzado de cuatro pares categoría 5e el radio mínimo de doblado es de 2.5 cm.

- Evitar Interferencia electromagnética

A la hora de establecer la ruta del cableado del cuarto de telecomunicaciones a los nodos es una consideración primordial evitar el paso del cable por los siguientes dispositivos, o al menos considerar las distancias sugeridas:

- Motores eléctricos grandes o transformadores (mínimo 1.2 m).
- Cables de corriente alterna:
- Mínimo 13 cm para cables con 2KVA o menos.

- Mínimo 30 cm para cables de 2KVA a 5KVA.
- Mínimo 91 cm para cables con más de 5KVA.
- Luces fluorescentes y balastos (mínimo 12 cm).
- El ducto debe de ir perpendicular a las luces fluorescentes y cables o ductos eléctricos.
- Intercomunicadores (mínimos 12 cm).
- Equipo de soldadura.
- Aires acondicionados, ventiladores, calentadores (mínimo 1.2 m).
- Otras fuentes de interferencia electromagnética y de radio frecuencia.

4. Subsistema Cuarto de Telecomunicaciones

El cuarto de telecomunicaciones es el área en un edificio utilizada para el uso exclusivo de equipo asociado con el sistema de cableado de telecomunicaciones. El espacio del cuarto de comunicaciones no debe ser compartido con instalaciones eléctricas que no sean de telecomunicaciones. El cuarto de telecomunicaciones debe ser capaz de hospedar equipo de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado. El diseño de cuartos de telecomunicaciones debe considerar, además de voz y datos, la incorporación de otros sistemas de información del edificio tales como televisión por cable (CATV), alarmas, seguridad, audio y otros sistemas de telecomunicaciones. Todo edificio debe contar con al menos un cuarto de telecomunicaciones o cuarto de equipo. No hay un límite máximo en la cantidad de cuartos de telecomunicaciones que pueda haber en un edificio.

Consideraciones de diseño

El diseño de un cuarto de telecomunicaciones depende de:

- El tamaño del edificio y del espacio para servir.
- Las necesidades de los ocupantes.
- los servicios de telecomunicaciones a usarse.

5. Subsistema Cableado Vertical (Backbone)

El propósito del cableado del backbone es proporcionar interconexiones entre cuartos de entrada de servicios del edificio, cuartos de equipo y cuartos de telecomunicaciones. El cableado del backbone incluye la conexión vertical entre pisos en edificios de varios pisos. El cableado del backbone incluye medios de transmisión (cable), puntos principales e intermedios de conexión cruzada y terminaciones mecánicas (figura 2.6).

El cableado vertical debe soportar todos los dispositivos que están dentro del rack y a menudo todas las impresoras, terminales y servidores de archivos de un piso en un edificio. Si más clientes o servidores son agregados a un piso, ellos compiten por el ancho de banda disponible en el cableado vertical. Sin embargo; existe una ventaja, y esta es la poca cantidad de canales verticales en un edificio y por ello se pueden usar equipos más costosos para proveer un mayor ancho de banda. Este es el área donde la fibra óptica se ha convertido en el medio más apropiado. El cableado vertical se presenta en varias topologías, pero la más usada es la topología en estrella.

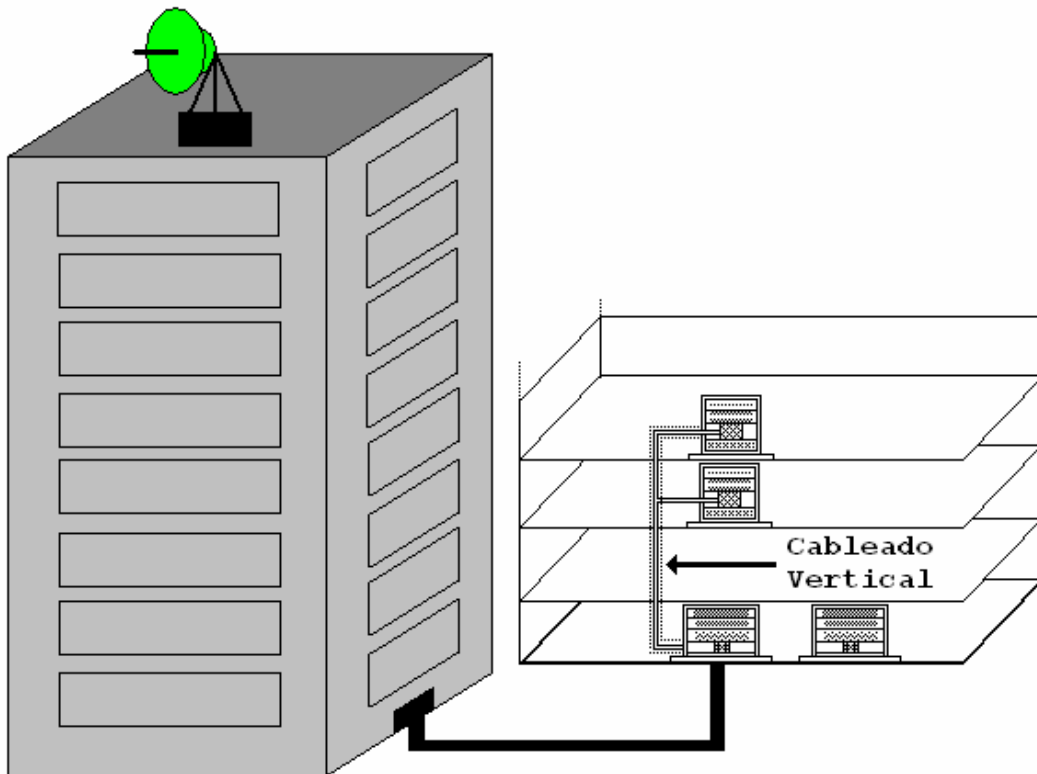


Figura 2.6 Subsistema Cableado Vertical (Backbone)

Consideraciones al instalar backbone:

1.- Cables reconocidos y distancias máximas

Cable	Distancia (m)	Aplicación
Cable UTP 100 Ω	800	Voz y Datos
Cable STP 150 Ω	90	Datos
Cable Múltimodo de fibra óptica de 62.5/125 μm	3000	Datos
Cable Monomodo de fibra óptica de 10/125 μm	2000	Datos

Tabla 2.7 Cables y distancias para cableado vertical

Las distancias del backbone, son dependientes de la aplicación. Las distancias máximas especificadas arriba son basadas en transmisión de voz para UTP y en transmisión de datos para STP y fibra óptica (tabla 2.7).

2.- Con cualquiera de los estándares existentes se puede construir un Backbone para el cableado vertical; pero deben tenerse en cuenta los siguientes factores:

- Flexibilidad con respecto a los servicios soportados.
- Vida útil requerida para el backbone.
- Tamaño del sitio y la población de usuarios.
- No se pueden colocar más de dos niveles jerárquicos de cross-connects.
- La longitud del patch-cord del cross-connect principal a intermedio no puede ser mayor a 20 m.
- El polo a tierra debe cumplir los requerimientos definidos en el estándar ANSI/TIA/EIA 607: requerimientos de puesta a tierra para telecomunicaciones.

6. Subsistema del Área de Trabajo

El área de trabajo comprende las inmediaciones físicas de trabajo habitual (mesa, silla, zona de movilidad, etc.) del o los usuarios. El punto que marca su comienzo en lo que se refiere a cableado es la roseta o punto de conexión (figura 2.8).

En el ambiente del área de trabajo se localizan diversos equipos activos del usuario tales como teléfonos, computadoras, telefax, terminales, etc. La naturaleza de los equipos activos

condicionan el tipo de los conectores existentes en las rosetas, mientras que el número de los mismos determina si la roseta es simple (de un conector), doble (de dos conectores), triple (de tres conectores), entre otros.

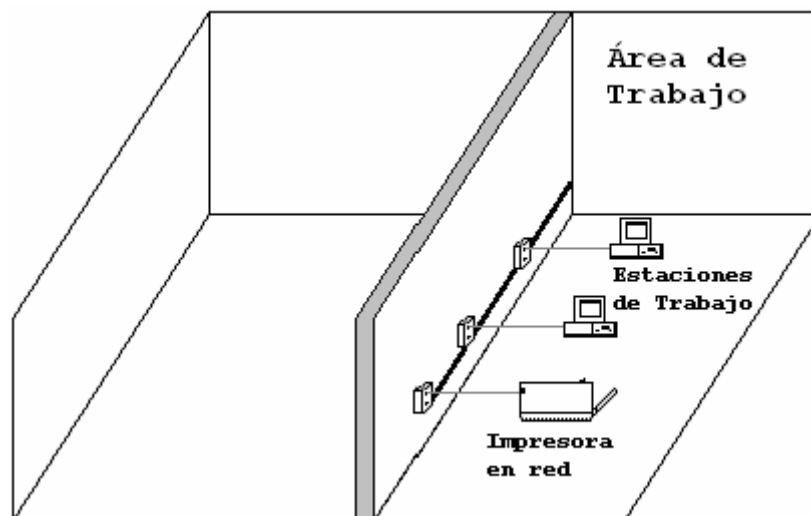


Figura 2.8 Subsistema del Área de Trabajo

2.2.2. ANSI/TIA/EIA-569: Estándar para Ductos y Espacios de Telecomunicaciones en Edificios Comerciales.

Este subsistema provee especificaciones para el diseño de los espacios planteados y de las canalizaciones para los componentes de los sistemas de cableado para edificios comerciales.

Este estándar tiene en cuenta tres conceptos fundamentales relacionados con telecomunicaciones y edificios:

- Los edificios son dinámicos. Durante la existencia de un edificio, las remodelaciones son comunes, y deben ser tomadas en cuenta desde el momento del diseño. Este estándar reconoce que el cambio ocurre y lo tiene en cuenta en sus recomendaciones para el diseño de las canalizaciones de telecomunicaciones.
- Los sistemas de telecomunicaciones son dinámicos. Durante la existencia de un edificio, las tecnologías y los equipos de telecomunicaciones pueden cambiar drásticamente. Este estándar reconoce este hecho siendo tan independiente como sea posible de proveedores y tecnologías de equipo.

- Telecomunicaciones es más que “voz y datos”. El concepto de Telecomunicaciones también incorpora otros sistemas tales como control ambiental, seguridad, audio, televisión, alarmas y sonido. De hecho, telecomunicaciones incorpora todos los sistemas de “bajo voltaje” que transportan información en los edificios.

Un buen diseño de un edificio debe soportar los requerimientos actuales y futuros de los sistemas de telecomunicaciones, para ello se debe incorporar durante la fase preliminar del diseño arquitectónico el diseño de las telecomunicaciones.

El estándar registra los siguientes seis componentes que mencionaremos.

1. Subsistema de Entrada del Edificio

Es el lugar por el cual ingresan los servicios de telecomunicaciones al edificio y/o donde llegan las canalizaciones de interconexión con otros edificios de la misma agrupación. Las instalaciones de entrada pueden incluir dispositivos de interfaz con las redes públicas prestadoras de servicios de telecomunicaciones, y también equipos de telecomunicaciones.

El estándar recomienda que la ubicación de las instalaciones de entrada sean lugares secos, cercanos a las canalizaciones del cableado vertical (backbone).

Localización del edificio: se debe tomar en cuenta la localización de otros servicios como agua, drenaje, gas, energía eléctrica, etc. para una buena selección de la instalación de entrada.

Vías de telecomunicaciones para la entrada de servicios: se debe proporcionar una ruta de transmisión para la entrada de servicios en el que los métodos para el abastecimiento son a través de vías aéreas o subterráneas.

Para los ductos subterráneos a la entrada de un edificio, es necesario utilizar un tubo conduit mínimo de cuatro pulgadas o ductos de PVC, ductos de plástico, tubo de acero galvanizado, etc. los cuales no deben tener una curvatura mayor a 90°. La pendiente no deberá ser mayor a 12° por cada 100 ft y se recomienda que el espacio del tubo no debe ser llenado por más del 40% de cables.

2. Subsistema Cuarto de Equipos

El subsistema de cuarto de equipos es un espacio destinado para la instalación de equipo sofisticado tal como: conmutadores telefónicos, conmutadores de datos de alta velocidad, conmutadores de video, entre otros, los cuales se emplean para proporcionar servicios a los usuarios de un edificio.

En el cuarto de equipos únicamente se deben albergar equipos, distribuidores de cableado y sistemas auxiliares de soporte para la operación de los equipos.

Para que un cuarto de equipo funcione adecuadamente, se deben tener en cuenta las siguientes consideraciones para el diseño:

Selección del sitio

Para la selección del cuarto de equipo se deben evitar sitios que estén limitados por componentes del edificio que restrinjan la expansión tales como: elevadores, escaleras, etc. El cuarto debe tener accesos amplios que permitan la entrada y salida de grandes equipos, y el acceso a este cuarto debe ser restringido.

La capacidad de resistencia del piso debe ser tal que la carga distribuida y concentrada de los equipos instalados. La carga que deben soportar es: distribuida deberá ser mayor que 12.0 KPa y la carga concentrada deberá ser mayor que 4.4 KN sobre el área de mayor tensión.

El cuarto de equipo no debe estar localizado debajo de niveles de agua a menos que las medidas preventivas hallan sido ya tomadas en contra de la infiltración de agua. Debe ser colocado un drenaje en el cuarto en caso de que existiera el ingreso de agua.

El cuarto de equipos debe tener un acceso directo al aire acondicionado y debe estar localizado lejos de fuentes de interferencias electromagnéticas, a una distancia la cual reduzca la interferencia. Se debe tener especial atención con transformadores eléctricos, motores, generadores, equipos de rayos x, radios o radares de transmisión. En la medida posible es deseable colocar el cuarto de equipos cerca de la ruta del backbone principal.

Tamaño

El cuarto de equipo debe ser dimensionado para satisfacer los requerimientos de espacio conocidos para la instalación de los equipos. Para definir el tamaño se debe tener en cuenta tanto los requerimientos actuales como los proyectos futuros. Cuando las especificaciones de tamaño de los equipos no son conocidas se deben tener en cuenta los siguientes puntos:

- Guía para voz y datos: el cuarto de equipos debe ser diseñado para un mínimo de 14m². basándose en el número de estaciones de trabajo. El tamaño del cuarto debe considerar aspectos de la tabla 2.9:

Número de estaciones de trabajo	Área en m ²
Hasta 100	14
Desde 101 hasta 400	37
Desde 401 hasta 800	74
Desde 801 hasta 1200	111

Tabla 2.9 Área del cuarto de equipo

- Guía para otros equipos: Los equipos de control ambiental, tales como los distribuidores de energía, aires acondicionados y UPS (Uninterruptible Power Suplí) hasta 100 KVA se deben instalar en el cuarto de equipos. Los equipos mayores a 100 KVA deben estar localizadas en cuartos separados.

Provisionamiento

La altura mínima de un cuarto de equipos debe ser de 2.44 m. El cuarto de equipo debe estar protegido de contaminación, la cual, pueda afectar la operación y al material de los equipos instalados.

El cuarto de equipos debe estar conectado a la ruta del backbone. En caso de que necesitarse detectores de humo, estos deben de estar dentro de su caja para evitar que se activen accidentalmente.

Equipos de calefacción, ventilación y aire acondicionado

El sistema de aire acondicionado debe estar diseñado para operar continuamente durante las 24 horas del día y los 365 días del año. Si el sistema del edificio no garantiza una operación continua, entonces una unidad independiente debe ser instalada para el cuarto de equipos.

La temperatura y la humedad en el interior del cuarto deben ser controlada para proporcionar rangos de operación continua de 18° C a 24° C con 30% a 55% de humedad. Dependiendo de las condiciones ambientales locales del sitio, se puede requerir que el sistema de aire acondicionado tenga la facilidad de humidificación y deshumidificación. La temperatura ambiente y la humedad deben ser medidas a una distancia de 1.5 metros sobre el nivel del piso y después de que los equipos estén en operación. Si se utilizan baterías para respaldo, se deben instalar equipos adecuados de ventilación.

Acabados e interiores

Las paredes, piso y techo del interior del cuarto de equipos deben estar sellados para reducir la acumulación del polvo. Los acabados deben ser en colores tenues para mejorar la iluminación en el interior del cuarto de equipos. Para el piso se deben seleccionar materiales con propiedades antiestáticas.

Iluminación

Las características de la iluminación deben ser las siguientes:

- Debe haber un interruptor dentro y cerca de la puerta.
- Evitar luz fluorescente (ruido electromagnético).
- La luz debe tener un mínimo de 50 candelas (540 lux)
- La ubicación de las fuentes de iluminación debe estar por encima de 2.6 m respecto del piso.

Energía

Se debe instalar un circuito separado para suplir de energía al cuarto de equipo y debe terminar en su propio panel eléctrico. La energía eléctrica que llegue al cuarto no se especifica ya que depende de los equipos instalados.

Puerta

La puerta de acceso debe tener como mínimo las siguientes medidas: 0.91 m de ancho y 2 m de altura, equipada con una cerradura de alta seguridad. Si se tiene contemplado para un futuro la instalación de equipo más grande, se recomienda utilizar una puerta del doble de 1.82 m de ancho por 2.28 m de altura.

Polo a tierra

Se debe instalar un conducto de 1½ desde el cuarto de equipos hasta el electrodo a tierra del edificio.

Extinguidores de fuego

Se deben mantener extinguidores de fuego portátiles y realizarles mantenimiento periódicamente. Estos deben ser instalados tan cerca y visiblemente a la puerta como sea posible.

3. Subsistema Cableado Horizontal

Rutas y espacios horizontales

Las rutas y espacios horizontales proporcionan los espacios, trayectorias y soporte para los cables de telecomunicaciones que van desde el distribuidor de cables de piso hasta las salidas o conectores de telecomunicaciones ubicadas en el área de trabajo.

El cableado horizontal consta de cable par trenzado de cobre, si se requiere un alto rendimiento se puede utilizar fibra óptica. El cableado horizontal debe emplear una topología de estrella. Cada punto terminal de conexión de datos y/o voz debe estar conectado al patch panel.

El término horizontal es utilizado debido a que típicamente este sistema de cableado se instala horizontalmente a través del piso o del techo del edificio. La canalización puede estar formada por varios componentes tales como escaleras portacables, ductos cuadrados embisagrados, tubería (conduit), ductos empotrados en piso y sistemas de canalización aparente.

El recorrido horizontal en el interior del edificio debe ser instalado en lugares secos que protejan a los cables de niveles de humedad que puedan dañarlos, lejos de interferencias electromagnéticas y se deben tener consideraciones estéticas. Esta canalización no debe localizarse en el interior de los cubos para los elevadores del edificio.

4. Subsistema Cuarto de Telecomunicaciones

El subsistema de cuarto de telecomunicaciones es un espacio dentro de un piso de oficinas, preferentemente con un sólo acceso, designado para albergar equipo, distribuidores de cableado y sistemas auxiliares requeridos para la operación de los equipos.

El cuarto de telecomunicaciones debe proporcionar todas las condiciones requeridas tales como espacio, alimentación eléctrica, control ambiental, entre otras, para la correcta operación de los equipos y componentes pasivos de la red instalados en su interior. Cada cuarto de telecomunicaciones debe tener acceso al subsistema de cableado vertical y al subsistema de cableado horizontal de las oficinas.

Consideraciones de diseño del subsistema del cuarto de telecomunicaciones

El diseño de un cuarto de telecomunicaciones depende de:

- El tamaño del edificio.
- El espacio de piso a servir.
- Las necesidades de los ocupantes.
- Los servicios de telecomunicaciones a utilizarse.

Altura

La altura mínima recomendada es de 2.6 m.

Ductos

El número y tamaño de los ductos utilizados para acceder al cuarto de telecomunicaciones varía con respecto a la cantidad de áreas de trabajo; sin embargo se recomienda por lo menos tres ductos de 10 cm (4 pulgadas aproximadamente) de diámetro para la distribución del cable del backbone.

Puertas

Las puertas de acceso deben de ser de apertura completa, con llave y de al menos 0.91 m de ancho y 2 m de alto. La puerta debe abrir hacia fuera (o lado a lado). Entre la puerta y el piso debe haber un mínimo de espacio de separación entre ellos, y no se debe tener postes centrales.

Polvo y electricidad estática

Se debe aplicar tratamiento especial en las paredes, pisos y techo para minimizar el polvo y la electricidad estática.

Control ambiental

En cuartos que no cuentan con equipo eléctrico la temperatura del cuarto de telecomunicaciones debe mantenerse las 24 horas del día y los 365 días del año entre 10 y 35 grados centígrados. La humedad relativa debe mantenerse menor a 85% y debe haber un cambio de aire por hora.

En cuartos que tienen equipo electrónico, la temperatura del cuarto de telecomunicaciones debe mantenerse las 24 horas del día y los 365 días del año entre 18 y 24 grados centígrados. La humedad relativa debe mantenerse entre 30% o 55% y debe haber un cambio de aire por hora.

Prevención de inundaciones

Los cuartos de telecomunicaciones deben estar libres de cualquier amenaza de inundación. No debe haber tubería de agua pasando por el cuarto de telecomunicaciones.

Pisos

Los pisos de los cuartos de telecomunicaciones deben soportar una carga de 2.4 KPa.

Iluminación

La iluminación debe estar a un mínimo de 2.6 m del piso terminado. Las paredes deben estar en un color claro para mejorar la iluminación. Se recomienda el uso de luces de emergencia.

Localización

Se recomienda instalar el cuarto de telecomunicaciones al centro del área que será cableada con el objeto de mantener la distancia horizontal del cable en un promedio de 46 m o menos con un máximo de 90 m.

Potencia

Debe haber suficientes contactos para abastecer los dispositivos a instalarse. El estándar establece que debe haber un mínimo de dos contactos dobles de 110 V corriente alterna de tres hilos. Deben ser circuitos separados de 15 a 20 amperes. Estos dos contactos estarán colocados a 1.8 m de distancia uno de otro. En muchos casos es deseable instalar un panel de control eléctrico dedicado al cuarto de telecomunicaciones. La alimentación específica de los dispositivos electrónicos se podrá hacer con UPS y regletas montadas en los andenes.

El cuarto de telecomunicaciones debe contar con una barra de puesta a tierra que a su vez debe estar conectada mediante un cable mínimo de 6 AWG al sistema puesta a tierra de telecomunicaciones según las especificaciones de ANSI/TIA/EIA 607: Requerimientos de Puesta a Tierra para Telecomunicaciones.

Seguridad

Le cuarto de telecomunicaciones se debe mantener con llave en todo momento y se debe asignar llave al personal encargado para que este disponible durante las horas de operación. Se recomienda que el cuarto de telecomunicaciones permanezca limpio y ordenado.

Requisitos de tamaño. Debe haber al menos un cuarto de telecomunicaciones por piso y por áreas que no excedan los 1000 m² y las instalaciones pequeñas pueden utilizar un sólo cuarto de telecomunicaciones si la distancia máxima no excede los 90 m (tabla 2.10).

Área a servir edificio normal	Dimensiones mínimas del cuarto de telecomunicaciones
500 m ² o menos	3.0 x 2.2 m
Mayor a 500 m ² , menor a 800 m ²	3.0 x 2.8 m
Mayor a 500 m ² , menor a 800 m ²	3.0 x 3.4 m
Área a servir edificio pequeño	Utilizar para el cuarto de telecomunicaciones
100 m ² o menos	Montante de pared o gabinete cerrado
Mayor a 100 m ² , menor a 800 m ²	Cuarto de 1.3 m x 1.3 m o closet angosto de 0.6 m x 2.6 m

Tabla 2.10 Área del cuarto de telecomunicaciones

Disposición de equipos

Los racks deben contar con al menos 82 cm de espacio de trabajo libre alrededor (al frente y detrás) de los equipos y paneles de telecomunicaciones. La distancia de 82 cm se debe medir a partir de la superficie más la salida del rack.

Debe haber por lo menos 1 metro de espacio libre para trabajar con partes expuestas sin aislamiento.

Todos los Racks y gabinetes deben cumplir con las especificaciones de ANSI/EIA. La tortillería debe ser métrica. Se recomienda dejar un espacio libre de 30 cm entre el rack y en las esquinas.

Paredes

Las paredes deben ser suficientemente rígidas para soportar equipo. Las paredes deben ser pintadas con pintura resistente al fuego, lavables y de color claro.

5. Subsistema Cableado Vertical (backbone)

El número de puntos de conexión en una instalación (un punto de conexión por área de trabajo) se determina en función de las superficies útiles o de los metros lineales de fachada, mediante la aplicación de la siguiente norma general; 1 punto de acceso por cada 8 a 10 metros cuadrados útiles o por cada 35 m de fachada. Este número se debe ajustar en función de las características específicas de la instalación, por ejemplo, los locales del tipo de salas de informática, salas de reuniones y laboratorios.

En el caso de que existiera telefonía e informática, se debe hacer un dimensionado de tres tomas por punto de conexión. Dicho dimensionado puede ajustarse en función de un análisis de necesidades concreto, pero no deberá en ningún caso ser inferior a dos tomas por punto de conexión del área de trabajo. Una de las tomas deberá estar soportado por pares trenzados no apantallados de cuatro pares y los otros por cualquiera de los métodos de cableado.

6. Subsistema del Área de Trabajo

Este estándar cubre aquellos aspectos de la estación de trabajo relacionados con salidas de telecomunicaciones.

La salida de telecomunicaciones es el lugar del punto de conexión entre el cable horizontal y los cables que conectan aparatos en el área de trabajo. Como son: computadoras, teléfonos, etcétera.

En la planificación se debe considerar instalar un mínimo de una salida por estación de trabajo y el espacio disponible para cada estación de trabajo debe de ser de 10 m² en promedio. Para áreas del edificio donde resulte difícil añadir en un futuro mas salidas de telecomunicaciones, en el diseño inicial se deben colocar un mínimo de dos salidas separadas para esa área, Dichas áreas tales áreas deberán ser colocadas de manera flexible para que permitan cambios en el área de trabajo.

Se deberá instalar una salida de energía cerca de cada salida de telecomunicaciones. Las salidas montadas en paredes son normalmente instaladas a la misma altura que la salida de energía.

2.2.3. ANSI/TIA/EIA-570: Estándar de Alambrado de Telecomunicaciones Residencial y Comercial Pequeño

El estándar ANSI/TIA/EIA-570 muestra la preparación de las residencias y comercios pequeños para incorporar servicios de telecomunicaciones más avanzados, para así poder incorporar nuevos servicios con el grado de cableado apropiado. El estándar ANSI/TIA/EIA-570 es considerado como un complemento del estándar ANSI/TIA/EIA-568-a (cableado de telecomunicaciones en edificios comerciales).

El estándar detalla el cableado de los sistemas considerando la conexión con uno o varios accesos de línea para varios tipos de equipos. Este estándar especifica un genérico funcional sistema de cableado para telecomunicaciones donde la construcción del edificio soporte multiproductos. La instalación del sistema de cableado debe ser durante la construcción del edificio puesto que el realizar esto permite que sea menos costoso después de que se ha ocupado el edificio.

Existen dos grados definidos de cableado de telecomunicaciones en predios residenciales. Estos grados se han establecido sobre la base de los servicios que se espera sean soportados dentro de cada unidad residencial y/o comercial pequeña y contribuir en la selección de la infraestructura del cableado.

El cableado de telecomunicaciones residencial de grado 1 proporciona un sistema de cableado genérico que satisface los requisitos mínimos para los servicios de telecomunicaciones, por ejemplo: teléfono, satélite, televisión por cable [CATV], servicios de datos. Dicho cable está compuesto de un cable de par trenzado de 4 pares y conectores asociados el cual cumple o excede los requisitos para la categoría 3 y un cableado coaxial de la serie 6 de 75 Ω .

El cableado de telecomunicaciones residencial de grado 2 proporciona un sistema de cableado genérico que cumple con los requisitos de los servicios de telecomunicaciones multimedia básicos y avanzados, actuales y en desarrollo. El cableado residencial de grado 2 está compuesto de un mínimo de dos cables de par trenzado de 4 pares y sus conectores asociados, el cual cumple o excede los requisitos del cableado de categoría 5 y dos cables coaxiales de la serie 6 de 75 Ω . Opcionalmente se puede aplicar cableado de fibra óptica de dos hilos. Se recomienda la instalación de cableado de categoría 5e en lugar del cableado de categoría 5.

De manera común, para ambos grados de cableado en predio residencial, es que tienen que colocarse en una topología de estrella que permite que el propietario pueda realizar cambios fácilmente en el cableado. Adicionalmente, la longitud de cada cable de salida no debe exceder los 90 m (295 pies). La longitud 90 m (295 pies) permite una longitud operacional de 100 m (328 pies) incluyendo cable de parcheo, cables de puente y cordones del equipo.

Las tablas siguientes (tabla 2.11 y tabla 2.12) muestran los cables y servicios para el estándar ANSI/TIA/EIA-570.

Servicio	Grado 1	Grado 2
Teléfono	√	√
Televisión	√	√
Datos	√	√
Multimedia		√

Tabla 2.11 Servicios para el estándar ANSI/TIA/EIA-570.

Cableado	Grado 1	Grado 2
UTP Categoría 3 (4-pares)	√ (se recomienda Categoría 5)	√
UTP Categoría 5 (4-pares)		(se recomienda Categoría 5e)
Coaxial de Serie 6 de 75 Ω	√	√
Fibra Óptica		√ (opcional)

Tabla 2.12 Cables para el estándar ANSI/TIA/EIA-570.

2.2.4. ANSI/TIA/EIA-606: Estándar de Administración para Infraestructura de Telecomunicaciones en Edificios Comerciales

El estándar ANSI/TIA/EIA-606, especifica los requerimientos de administración de la infraestructura ya sea un edificio nuevo, existente o renovado. La infraestructura de telecomunicaciones puede ser ideada como la conexión de varios componentes: espacio del equipo de comunicaciones, ruta del cable, sistema de tierra físico, cableado y la terminación al hardware; que provee el básico soporte de la distribución de toda la información dentro de un edificio. La administración de telecomunicaciones incluye la documentación de las cajas de conexión, conectores, terminación del hardware, conexión, tubo conduit, otro tipo de rutas del cable, closet de telecomunicaciones, puestas a tierra y otros espacios.

Este estándar establece un esquema de administración uniforme que sea independiente de las aplicaciones que se le den al sistema de cableado, las cuales pueden cambiar varias veces durante la existencia de un edificio. Este estándar facilita guías para dueños, usuarios finales, consultores, contratistas, diseñadores, instaladores y administradores de la infraestructura de telecomunicaciones y sistemas relacionados.

Los edificios modernos requieren una efectiva infraestructura de telecomunicaciones para soportar la variedad de servicios que dependen del transporte electrónico de la información. La administración incluye documentación básica, los planos actualizados, etiquetado y registro.

Los aspectos de administración que se deben de cumplir cuando se construye, instala o suministra una red son los siguientes:

- Identificar y etiquetar las canalizaciones, cableado de telecomunicaciones y sistema de tierra de acuerdo a lo que indica este estándar.
- Elaborar y entregar los registros de datos para cada uno de los elementos que conforman las canalizaciones, cableado de telecomunicaciones y sistemas de tierra.
- Elaborar los planos, dibujos de detalle, isométricos y diagramas de conexión de las canalizaciones, cableado de telecomunicaciones y sistema de tierra.

Conceptos de Administración

El típico sistema de administración incluye: registros, reportes, esquemas y registros de trabajo.

Identificadores

Se debe asignar un identificador a cada elemento de la infraestructura de telecomunicaciones para vincularlo a su correspondiente registro de datos. Los identificadores se deben checar en los elementos que son administrados.

Los identificadores utilizados para el acceso a los registros de datos de información del mismo tipo deben ser únicos. Se debe utilizar identificadores únicos para la identificación de los componentes de la infraestructura de telecomunicaciones. Por ejemplo: ningún identificador de cable debe ser idéntico a algún identificador de una canalización o espacio de telecomunicaciones.

Los identificadores pueden clasificarse como:

Identificadores de ruta

- CT Bandeja de entrada.
- CD Conducto.
- BCD Conducto de Backbone.

Las rutas deben ser etiquetadas en todos los puntos de terminación; en las localizaciones intermedias no es obligatorio, pero si es muy deseable.

Identificadores de espacio

- EF Infraestructura de entrada.
- ER Sala de equipos.
- IC Conexión cruzada intermedia.
- HH Orificio de acceso.
- S Empalme.

Todos los espacios deben ser rotulados. Se recomienda que las etiquetas se fijen en la entrada de cada espacio.

Identificadores de cable

- C Cable.
- CB Cable de backbone.
- F Fibra.

Los cables verticales y horizontales deben ser etiquetados en cada extremo; la rotulación en localizaciones intermedias no es obligatoria pero es útil. Es altamente recomendable que se usen etiquetas adhesivas en lugar de marcar directamente sobre el cable.

Identificadores de conexión a tierra

- BC Conductor unión.
- EC Conductor de equipo.
- GB Barra de distribución de tierra.
- TGB Barra de distribución de tierra de telecomunicaciones.
- TMGB Barra de distribución de tierra principal de telecomunicaciones.

Registro de Telecomunicaciones

Es un conjunto de información acerca de o relacionados con un elemento determinado de la canalización, espacio, cableado o sistema de tierra de telecomunicaciones.

Los registros de telecomunicaciones se clasifican de la siguiente forma:

- Registros de ruta.
- Registros de cable.
- Registros de espacio.
- Registros de conexión a tierra.
- Registros de posición de terminación.

Reportes opcionales. Pueden existir registros de otros dispositivos, como pueden ser: PBX, inventario de equipo (Teléfonos, PCs, software, LAN) e información de los usuarios (extensión, ubicación, etcétera).

Dibujos

Los dibujos deben contener los siguientes planos:

- Planos en planta a escala y los detalles suficientes para las trayectorias de las canalizaciones, indicando claramente cambios de dirección cajas de registro, pasos en muro, entre otros detalles de instalación.
- Ficha de canalizaciones y conductores.
- Planos en planta a escala de la distribución de trayectorias de canalizaciones visibles y subterráneas, barras del sistema de tierra de telecomunicaciones y distribuidores de cableado en el interior del cuarto de telecomunicaciones, sin que esto sea limitado.
- Planos de elevación y planta a escala, de la distribución de trayectorias de canalizaciones, barras del sistema de tierra de telecomunicaciones y distribuidores de cableado en el interior del cuarto de equipo.

- Planos de elevación y planta, a escala, de la distribución de trayectorias de canalizaciones, barras del sistema de tierra de telecomunicaciones y distribuidores de cableado en el interior del área o cuarto de telecomunicaciones.
- Diagrama unificado de la red de cableado estructurado de telecomunicaciones, indicando claramente la longitud y tipo de cable, entre otros datos.
- Planos de distribución de los accesorios de conexión o paneles de parcheo en los herrajes o gabinetes de los distribuidores de cableado.
- Planos de detalles de instalación de los elementos funcionales de la red.

En todos los planos e isométricos de las canalizaciones y espacios de telecomunicaciones, deben aparecer sus respectivos identificadores.

Orden de trabajo. Orden de trabajo que incluye espacios, rutas de los cables, sistema de tierra. La orden de trabajo debe listar las responsabilidades para cambios físicos, así como, la actualización de la documentación para futuros cambios.

Formatos de identificación. Un único código de identificación alfabética debe ser creado para cada lugar, ruta de cable, punto terminal. La sugerencia en este estándar se indica en la tabla 2.13.

Código	Descripción
BCxx	Unión del conductor
BCDxx	Canalización del backbone
Cxxx	Cable
CBxxx	Cable de backbone
CDxxx	Canalización
CTxxx	Cable de prueba
Ecxxx	Equipo conductor
Efxxx	Acceso a los recursos de comunicación
Erxxx	Cuarto de Equipo
Fxxx	Fibra
GBxxx	Barra conectada a tierra
GCxxx	Conductor conectado a tierra
Icxxx	Conexión de unión Intermedia
Jxxx	Jack
MCxxx	Conexión de unión principal
Sxxx	Empalme
Sexxx	Servicio de entrada
TCxxx	Cuarto de telecomunicaciones
TGBxxx	Conexión a tierra para telecomunicaciones
TMCB	Barra principal de conexión a tierra para Telecomunicaciones
Waxxx	Área de trabajo

Tabla 2.13 Formato de identificación

De Igual forma el escoger un formato debe ser considerado y proveer un único número de identificador para cada elemento del sistema. Este método permite por sí mismo organizar y actualizar los múltiples registros en uso logrando un programa de base de datos.

Por otra parte, dependiendo de la aplicación de los campos de terminación del ambiente en un punto de administración se asignan etiquetas insertables, con un código de colores para identificar los siguientes tipos de circuitos:

- Verde: lado del campo de la interfaz de la red, circuitos de la compañía de teléfono.
- Verde: lado del equipo de la interfaz de la red; troncales de la rama.
- Púrpura: terminación de equipos de comunicación.
- Amarillo: diversos hilos de equipo de comunicaciones, circuitos auxiliares.
- Blanco: cables de backbone ascendente.
- Azul: área de trabajo servida directamente desde la sala de equipo.

- Naranja: interfaz de red.
- Gris: cable de backbone de enlace a la sala de computadoras u otras salas de equipos.
- Marrón: cables del backbone del campus.
- Rojo: sistemas telefónicos con teclado.

2.2.5. ANSI/TIA/EIA 607: Requerimientos de Puesta a Tierra para Telecomunicaciones

Este estándar permite la planeación, diseño e instalación de sistemas de tierra para telecomunicaciones en un edificio con o sin conocimiento previo de sistemas de telecomunicaciones subsecuentemente instalados. Este estándar incluye también recomendaciones acerca de las tierras y los sistemas de tierra para las torres y las antenas.

El sistema de tierra está constituido por un conjunto de conductores interconectados entre sí y conectados a tierra mediante electrodos enterrados a cierta profundidad en el subsuelo. Los componentes principales que forman al sistema de tierras son los electrodos de puesta a tierra.

Características del diseño

Las varillas sólidas de cobre deben ser instaladas a una distancia lejana de la entrada del edificio, las varillas pueden ser de 1/4'' de delgada por 4'' de altura, por longitud variable; para el cuarto de equipo y el closet de telecomunicaciones con 2'' de altura es suficiente.

El equipo de telecomunicaciones, gabinetes, racks y los protectores de voltaje son típicamente aterrizados al sistema de tierra físico. Las varillas son conectadas por un backbone con aislamiento, cable de cobre sólido entre todos los closets y cuartos de equipos (mínimo 6 AWG ó 3 AWG como recomendado). El backbone es conectado a la varilla principal en la entrada del edificio y este va conectado a un sistema de tierra física del edificio, y una estructura de acero en cada piso. Relacionando el conductor de cable de color verde o con un etiquetado apropiado.

Un sistema de telecomunicaciones cuenta con un amplio número de equipos, que podemos clasificar de la siguiente forma:

- Fosa de cables. Es el área dentro de la instalación en la que entran los cables externos al edificio. Existen diferentes tipos de fosas de cables, dependiendo del tipo de cables que se instalen, estos pueden ser telefónicos, coaxial, UTP, fibra óptica, etcétera.
- Equipo de corriente directa. El equipo de corriente directa esta constituido de rectificadores, convertidores, baterías, distribuidores de corriente directa e inversores.
- Equipo de corriente alterna. Los equipos de corriente alterna que se manejan dentro de las instalaciones de telecomunicaciones son: subestaciones, transformadores, maquinas de emergencia, tableros de protección y distribución.
- Equipo de aire acondicionado. El equipo de cómputo, de conmutación y de transmisión deben trabajar bajo ciertas condiciones ambientales, por lo que el clima artificial es básico para el buen funcionamiento de los equipos.
- Equipo de transmisión. Los equipos de transmisión, pueden ser de microondas, radio, fibra óptica, etc, en algunos casos estos equipos pueden estar a la intemperie, expuestos al medio ambiente y por lo tanto más propensos a recibir descargas eléctricas.
- Equipos de conmutación. Este equipo es el de máxima impedancia dentro de una instalación de telecomunicaciones, ya que es el encargado de manejar el tráfico de llamadas.
- Equipo de cómputo. Debido a la alta relación entre las telecomunicaciones y la informática, en la actualidad es indispensable contar con salas de cómputo especiales para el control y supervisión de los equipos.

Las principales funciones que debe cumplir todo sistema de tierra son las siguientes:

- Proveer un medio seguro para proteger al personal y al equipo de los peligros de una descarga eléctrica bajo condiciones de falla.
- Proporcionar un circuito de mínima impedancia para la circulación de las corrientes de falla, debidas a condiciones anormales de operación.
- Evitar durante la circulación de estas corrientes a tierra, que se produzcan diferencias de potencial entre los diversos equipos de puesta a tierra.
- Evitar la inducción de ruido en los equipos de telecomunicaciones.

El sistema de puesta a tierra para una instalación de telecomunicaciones está constituido por cinco elementos principales que proveen la base para el diseño de la trayectoria de puesta a tierra a los equipos; los cuales se mencionan a continuación.

1. Sistema de electrodos de tierra o mallas de tierra

La malla de tierra está constituida por:

- La red o malla de conductores enterrados a una profundidad mínima de 0.6 m
- Conductores de puesta a tierra, a través de los cuales se realiza la conexión a tierra de las partes de la instalación o del equipo que requieran dicha conexión.

Es recomendado construir el sistema de electrodos de tierra con cable de cobre desnudo de calibre No. 1 AWG mínimo con electrodos de tierra (copperweld).

Todos los equipos dentro de un edificio de telecomunicaciones deben ser referidos a tierra por medio de este sistema; el cual permite el contacto con la tierra y provee un punto de potencial cero al equipo. Dado que este es el punto más débil en el sistema; es imperativa una baja resistencia entre el sistema y el subsuelo. Se recomienda mantener el sistema de tierra con una resistencia máxima de 5 Ω .

2. Barra principal de tierra

La barra principal de tierra (BPT) es el eje de la actividad del sistema del edificio. Es el punto general de la conexión para los elementos generadores de transitorios y de carga, lo mismo para las tierras de los equipos de las áreas aisladas y no aisladas.

La BPT se utiliza como una prolongación del sistema de electrodos de tierra del edificio. La BPT también sirve como el punto principal de conexión para el cableado vertical y el equipo localizado en la misma área del cuarto. El potencial de tierra, el cual se asume de cero volts, es establecido por el sistema de electrodos de tierra. Esta barra debe ser instalada en una zona de fácil acceso para que el personal capacitado pueda realizar mantenimiento.

3. Cable vertical

El cable vertical es un conductor que enlaza las barras de tierra del edificio de los diferentes pisos con la barra principal de tierra, distribuyendo la referencia de tierra. Básicamente, reduce o iguala las diferencias de potencias entre los sistemas de telecomunicaciones conectados a la barra de tierra. El cable vertical se conecta desde la barra principal de tierra, extendiéndose hacia todos los pisos y conectando las barras de tierra a cada uno de los niveles. Para ello se deben seguir las siguientes recomendaciones:

- Instalar en forma vertical un conductor continuo (sin empalmes) desde la barra principal de tierra hasta el último piso del edificio. Se recomienda un calibre mínimo de No. 6 AWG.
- Un cable vertical puede dar cobertura a los equipos que se encuentren dentro de un área de 30.5 m de radio.

Cuando existan varios cables verticales, éstos deben permanecer unidos cada tercer piso a través de un igualador horizontal del mismo calibre.

4. Barra de tierra

La función de las barras de tierra de piso (BT) es establecer el potencial de tierra en cada uno de los pisos de la central. Consiste en una barra de cobre pre-barrenada con perforaciones para conectores.

Dado que la barra de tierra de piso proporciona al mismo tiempo la referencia a tierra a los equipos, se debe establecer una localización conveniente de ésta, para lo cual se deben considerar los siguientes puntos:

- La máxima distancia del conductor, entre la BT y el equipo más lejano, no debe exceder a 6.1 m y no debe exceder el periodo de un cuadro superpuesto en un círculo de 30.5 m de radio desde la BT.
- Lo ideal para la instalación de BT en pisos con equipo es aproximadamente en el centro de área, lo cual proporcionará longitudes aproximadamente iguales de los cables igualadores horizontales. Cuando BPT no se pueda localizar en el centro, se recomienda localizar lo más cerca posible de los distribuidores principales, tableros de fusibles o interruptores, para proveer una trayectoria directa a tierra.

5. Ventana de tierra

Los modernos equipos de conmutación digital requieren de la incorporación del concepto de plano aislado, que consiste básicamente en la puesta a tierra a través de un punto denominado: Ventana de Tierra (VT). La ventana de tierra es una zona de transición tridimensional consistente en una esfera imaginaria con un radio de 91.5 cm, la cual es la interfase entre el plano integrado y el plano aislado de tierra, físicamente la VT está representada por varias barras de cobre interconectadas, denominada barra de ventana de tierra.

2.3 Consideraciones de diseño

Es importante considerar la capacidad necesaria de red, considerando los impredecibles y limitantes requerimientos de ancho de banda asociados a las tecnologías actuales, tales como: el acceso a internet, correo electrónico, el acceso en tiempo real a videos y demás medios audiovisuales, así como, la transferencia de archivos.

Es importante estimar la capacidad y planificación de la red. Algunos factores importantes por considerar al definirla son los siguientes:

- Área disponible para el tendido de los cables.
- Facilidad de instalación y cantidad de usuarios.
- Costo económico que genera tener una red.
- La flexibilidad a futuro crecimiento por un período extendido de tiempo.
- Ubicación de los usuarios y la distancia máxima entre ellos, así como, su rotación.
- Patrones de uso, incluyendo los tamaños combinados y la duración del tráfico pico respecto a todas las aplicaciones.
- Aumento previsto de la demanda de ancho de banda.
- La conectividad con los dispositivos y software actuales y futuros, así como, la carga de comunicaciones en ellos.
- Requerimientos establecidos por las normas, estándares, y la seguridad.
- Nivel de seguridad de la red.
- Topología de red a implementar y el tiempo de vida útil para dicha red.

2.4 Elección de elementos activos

Un elemento activo es aquel que requiere de corriente eléctrica para su funcionamiento.

Dentro de los equipos necesarios para la comunicación con el exterior de una red local se mencionan los siguientes.

- Tarjeta de red.
- Switch para la conexión de las computadoras.
- Ruteador que dirige el paquete de datos determinando la ruta hacia su destino.

Tarjeta de red

La tarjeta de red actúa como interfaz física o conexión entre la computadora y el cable de red. Se coloca en una ranura de expansión de cada ordenador de la red; dicha ranura puede ser de arquitectura de bus ISA, EISA, Micro Channel y PCI.

La tarjeta de red realiza las siguientes funciones:

- Prepara los datos de la computadora para su envío a la red.
- Envía dichos datos a la red. Indicando su dirección física para distinguirlos de las otras tarjetas de red. La dirección física es única, compuesta por 12 dígitos hexadecimales y es determinada por la IEEE.
- Controla el flujo de datos entre el ordenador y el sistema de cableado.
- Recibe los datos entrantes en serie del cable y los traduce en bytes en paralelo que el ordenador pueda comprender.

Antes de que la tarjeta emisora transmita información, es necesario que establezca parámetros con la tarjeta receptora de lo siguiente:

- El tamaño máximo de los paquetes de datos que se quiere enviar.
- El total de datos a ser enviados antes de la confirmación.
- El intervalo de tiempo entre cada envío de paquetes de datos.
- El tiempo de espera antes de que sea enviada la confirmación.

- Cuantos datos se puede almacenar en la memoria de cada tarjeta.
- La velocidad de transmisión de los datos.

Una vez establecida la comunicación y aceptados los parámetros se inicia la transmisión. Las tarjetas de red tienen opciones de configuración que deben ser establecidas para que funcionen correctamente:

- Interrupción.
- Dirección de entrada/salida.
- Dirección de memoria base.
- Conector.

1. Interrupción

Cuando la tarjeta de red envía una petición al ordenador utiliza una interrupción. Las peticiones de interrupción son señales electrónicas por las que los dispositivos pueden enviar peticiones de servicio al procesador del ordenador. Tienen asignados niveles de prioridad y es única para cada dispositivo. Es especificada cuando se configura el dispositivo.

2. Dirección de entrada/salida

Es el canal de comunicación entre la tarjeta de red y el procesador. Es única en formato hexadecimal para cada dispositivo de hardware y se especifica al configurarlo.

3. Dirección de memoria base

Identifica un lugar en la memoria del ordenador, la cual es usada por la tarjeta de red como un buffer para almacenar las tramas de datos entrantes y salientes. La dirección de memoria base para una tarjeta de red es a menudo D8000. Dicha dirección no debe ser usada por algún otro dispositivo.

4. Conector

Cada tarjeta de red puede tener varios conectores integrados como BNC, RJ45 ó AUI. El más habitual es el conector RJ45.

Así entonces, la selección de una tarjeta de red se basa en varios factores diferentes:

- El protocolo de enlace de datos utilizado por la red.
- La velocidad de transmisión de la red.
- El tipo de interfaz que conecta la tarjeta a la red.
- El tipo de bus en el que se instala la tarjeta.
- Los recursos de hardware requeridos por la tarjeta.
- La potencia eléctrica requerida por la tarjeta.
- El papel de la computadora que utiliza la tarjeta: servidor frente a estación de trabajo, computadoras domésticas frente a computadoras de empresa.
- La disponibilidad de controladores apropiados.

Switch

El switch segmenta dominios de colisión. Utiliza un ancho de banda dedicado para cada usuario con lo que logra limitar el tráfico al segmento de red al que pertenece el frame, y aumentar la velocidad de transmisión.

Los requisitos y la demanda de los usuarios determinan el tipo de switch a utilizar, como son: el ancho de banda requerido para cada usuario, el número de usuarios, el límite del tráfico de cada segmento y el tiempo de respuesta.

Router

El router se encarga de conectar dos redes independientes de diferente tecnología en el nivel de red del modelo OSI, así como, de transmitir información entre ellas. Es capaz de seleccionar, de manera inteligente, la ruta más eficiente hacia un destino específico. Dado que la tecnología utilizada en una LAN y una WAN son distintas, se hace necesario el uso del router para conectarlas.

Existe una jerarquía de routers, desde los ISP (Internet Service Provider) locales más pequeños hasta los proveedores regionales, que a su vez obtienen el servicio de los proveedores nacionales.

El tipo de router utilizado para una función específica determina su tamaño, coste y posibilidades.

2.5 Documentación de la red

La memoria técnica del SCE es de gran importancia para la operación y el mantenimiento de los sistemas de telecomunicaciones, así como el rastreo de fallas. Se debe establecer una nomenclatura de documentación para cada sistema de cableado.

La disponibilidad de dicha documentación actualizada, facilita la renovación de la misma debido a los cambios continuos, tales como la incorporación de nuevos servicios y equipos, la expansión de los existentes, etcétera.

Todos los elementos del SCE deberán estar documentados a simple vista como en su interior, como son: cables, rosetas, paneles de parcheo, armarios de telecomunicaciones entre otros.

La documentación deberá presentarse a través de: etiquetas, registros, reportes, planos, órdenes de trabajo.

La documentación técnica deberá contener cada uno de los siguientes puntos:

- Diagrama lógico de la red.
- Descripción de los elementos del cableado.
- Planos de la trayectoria del cableado y ubicación de los puntos de salida.
- Diagrama del sistema de parcheo, distribución de regletas y salidas.
- Documentación de la certificación de la red.

Los planos del cableado de todos los pisos deberán detallar:

- Ubicación de los gabinetes de telecomunicaciones.
- Ubicación de ductos a utilizar para cableado vertical.
- Disposición detallada de los puestos eléctricos en caso de ser requeridos.
- Ubicación de pisoductos si existen y pueden ser utilizados.
- Ubicación de las puestas a tierra.
- Deben incluir una referencia cruzada a las etiquetas físicas que lleve cada tendido de cables.

Debe indicarse que la Norma Nacional de Cableado Estructurado, NMX-I-NYCE-248-2005, fué publicada en marzo de 2005. Esta Norma Mexicana especifica un sistema de cableado estructurado genérico para telecomunicaciones en edificios comerciales que puede implementarse con productos de uno o varios fabricantes; así como, los requisitos de desempeño, distancias, configuraciones y topología del cableado estructurado genérico. Proporciona guías para la instalación, operación y verificación de cableados para tecnologías de la información. Esta Norma Mexicana especifica el cableado estructurado genérico en edificios, el cual puede comprender uno o varios edificios en un campus, abarcando el cableado balanceado y el cableado de fibra óptica.

Capítulo 3

Redes Inalámbricas

Las redes inalámbricas han surgido desde hace algunos años, como una solución a las redes locales que usan cables como medio de comunicación, con el fin de satisfacer la necesidad de movilidad de los usuarios y la cobertura de lugares difíciles de cablear y así, estar comunicado sin la necesidad de preocuparse por los cables.

3.1 Introducción

Actualmente las redes inalámbricas han aumentado su rendimiento y confiabilidad de transmisión de información, tomando así, gran auge en los medios de comunicación.

Existen diferentes tipos de tecnologías inalámbricas:

- Red de datos basada en tecnología celular. De la cual su mayor ventaja es su alcance.
- Tecnología Bluetooth. Proporciona comunicaciones inalámbricas de corto alcance entre dispositivos tales como: teléfonos móviles y asistentes digitales personales (PDA) a un precio muy bajo. Esta tecnología usa señales de radiofrecuencia que no están limitadas a transmisiones en la línea de visión.

La velocidad proporcionada por la tecnología Bluetooth es suficiente para tareas de red estándar, como son: acceso a archivos, impresoras y aplicaciones de servidor. Sin embargo, está lejos de emular las redes alámbricas.

La tecnología inalámbrica que está más cerca de emular las redes con medios alámbricos son las redes de área local inalámbricas (WLAN).

Al igual que cualquier otra red LAN, una red de área local inalámbrica debe cumplir con requisitos como: alta capacidad, cobertura de pequeñas distancias, conectividad y capacidad de difusión. Debe satisfacer necesidades tales como: rendimiento, conexión al núcleo de la LAN, área de servicio con una superficie típica por encima de 100 – 300 metros de diámetro, robustez en la transmisión y seguridad, así como, permitir el libre desplazamiento entre puntos de acceso conocido como acceso nómada.

Las principales aplicaciones de las WLAN son:

- Ampliación de redes LAN.
- Interconexión de edificios.
- Acceso nómada.
- Redes ad hoc.

Los componentes básicos de hardware que forman una red inalámbrica son: la tarjeta de interfase de red (NIC) y el punto de acceso (Access Point).

El punto de acceso inalámbrico es el equivalente a un hub. Es conectado al backbone de la LAN mediante un cable estandarizado ethernet. Se comunica con dispositivos inalámbricos mediante una antena. Mantiene la conexión de los usuarios alrededor de un área de cobertura, permitiendo o denegando el tráfico hacia ellos o procedente de los mismos.

Cuando se establece la comunicación entre un usuario y el punto de acceso, se ve afectada por los siguientes parámetros:

- La velocidad máxima del punto de acceso.
- La distancia entre el usuario y el punto de acceso. Si se aumenta la distancia disminuye la velocidad de transmisión y recepción.
- Elementos intermedios entre el usuario y el punto de acceso. Algunos de ellos son: paredes, campos electromagnéticos y eléctricos, entre otros elementos interpuestos entre ambos dispositivos. Estos elementos disminuyen la velocidad de transmisión.
- Saturación del espectro e interferencias. Conforme se aumente el número de usuarios inalámbricos en las cercanías, se aumentan las colisiones en las transmisiones, disminuyendo así la velocidad de la misma.

En la actualidad la capacidad de transmisión y recepción de los puntos de acceso puede incrementarse mediante el uso de antenas direccionales y omnidireccionales. Las primeras envían la información a una cierta área de cobertura y a un ángulo determinado, por lo cual el alcance es mayor. Sin embargo, fuera del área de cobertura no se puede establecer la comunicación. Las antenas omnidireccionales tienen un área de cobertura de 360 grados, aunque su alcance es menor pueden establecer la comunicación independientemente del punto en que se encuentre el dispositivo.

Al presente la mayoría de las WLANs usan la banda de frecuencia de 2.4 GHz; sin embargo, la banda de frecuencia de 5 GHz emerge rápidamente.

Una de las ventajas de las redes locales inalámbricas es que proporcionan todas las facilidades y beneficios que las redes LAN; pero sin la limitación del cable. Sin embargo, las redes inalámbricas deben enfrentarse a retos como la seguridad, la movilidad y la configuración.

3.2 Topologías WLAN

La movilidad es una parte integral del diseño de una red LAN inalámbrica, y el protocolo de red LAN inalámbrica debe asegurar la entrega de la información en el área en el que el medio puede funcionar.

El bloque constructivo fundamental de una WLAN es el conjunto de servicio básico (BSS, basic service set). Un BSS es un área geográfica en la que equipos inalámbricos se comunican ejecutando el mismo protocolo MAC y compitiendo para acceder al mismo medio compartido. El protocolo MAC puede ser completamente distribuido o controlado por el punto de acceso. El conjunto de servicios básicos también es conocido como una celda o célula. La configuración y el área del BSS dependen del tipo de medio inalámbrico que se use, y de la naturaleza del entorno en el que se esté utilizando, entre otras cosas. Los factores que pueden afectar las fronteras del BSS son: las condiciones ambientales, los elementos arquitectónicos entre muchos otros más. El equipo únicamente puede comunicarse con los demás equipos que se encuentran en el mismo BSS.

El proceso por el que los dispositivos entran en un BSS se llama asociación. Cada dispositivo inalámbrico tiene un alcance operativo que depende de su equipo, y a medida que dos dispositivos se aproximan uno al otro, el área de alcance que hay entre ellos se convierte en el BSS. El elemento que conecta varios conjuntos de servicios básicos se llama sistema de distribución (DS); es generalmente una LAN cableada. Los conjuntos de servicios básicos y el sistema de distribución que los conecta se llaman conjunto de servicios de ampliación (ESS). El conjunto de servicios de ampliación aparece en el nivel de control de enlace lógico (LLC) como una única LAN lógica. Se clasifican tres tipos de estaciones según la movilidad:

- Sin transición. Se le llama de transición a aquella que es estacionaria o se mueve solo en el rango de comunicaciones directas de las estaciones de comunicaciones de un único BSS.
- Transición BSS. Una estación de este tipo es aquella que se desplaza de un BSS a otro BSS dentro de un mismo ESS.
- Transición ESS. Es aquella que se define como una estación que se transfiere desde un BSS en un ESS a otro BSS perteneciente a otro ESS diferente. Este caso se acepta solo haciendo referencia a que la estación se puede desplazar. Sin embargo, es probable que se produzca una interrupción de servicio.

Hay dos tipos de topologías de redes inalámbricas, una es la topología de infraestructura, en la que las estaciones acceden a la red a través de uno o varios puntos de acceso; y la topología ad hoc, en la que las estaciones se comunican entre sí directamente. También son conocidas como administradas y no administradas, alojadas y par a par respectivamente.

Topología de infraestructura

En esta topología el conjunto de servicios básicos son más permanentes. Una red de infraestructura consta de al menos un punto de acceso inalámbrico, conectado a una red LAN fija mediante cable y sirve para encaminar las tramas hacia otras redes; aunque no impide que los dispositivos inalámbricos se comuniquen entre sí. El punto de acceso tiene relativamente un alcance operativo fijo, así que el dispositivo deberá estar dentro del área de cobertura para establecer la comunicación con la red fija.

El modo de operación de esta topología es de cliente/servidor. Ya que los dispositivos inalámbricos no pueden comunicarse directamente con los dispositivos pertenecientes a la red LAN fija, es necesario el controlador central entre ambas redes, es decir, el punto de acceso. El punto de acceso coordina la transmisión y recepción de los dispositivos inalámbricos dentro del área específica. Funciona como una extensión a una red LAN fija para permitir acceder a los recursos de la red a los dispositivos inalámbricos. La extensión y el número de dispositivos dependen del estándar de conexión inalámbrica que se utilice y del producto. En la figura 3.1 se muestra una red de topología de infraestructura.

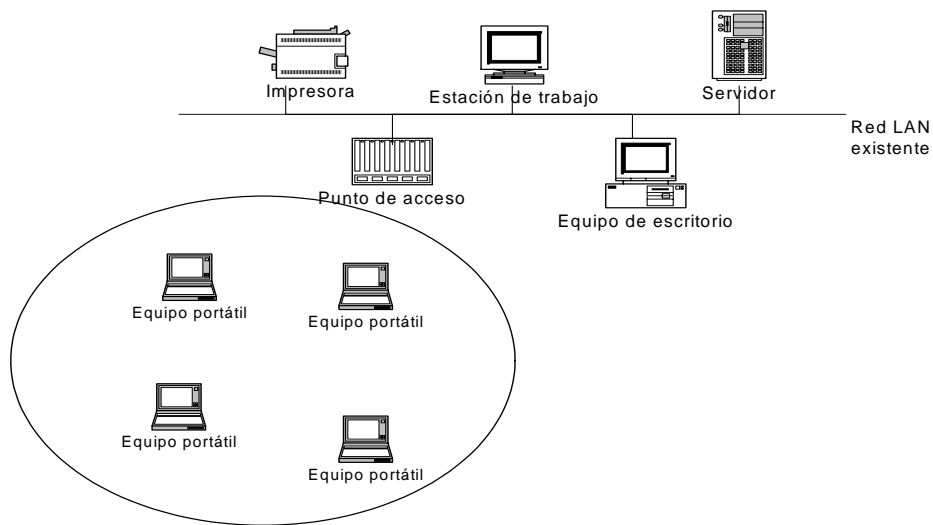


Figura 3.1 Topología de infraestructura

Una red de infraestructura puede tener cualquier número de puntos de acceso, y por consiguiente, cualquier número de conjuntos de servicios básicos.

Los conjuntos de servicios básicos conectados por un sistema de distribución pueden estar configurados físicamente de cualquier forma. Ya sea que se configuren para cubrir dos áreas remotas o una gran área de conectividad inalámbrica contigua.

- Funcionamiento de la modalidad de infraestructura

La estación primero debe identificar los puntos de acceso y las redes disponibles. Este proceso se realiza mediante el control de las tramas de señalización procedentes de los puntos de acceso que se anuncian a sí mismos o mediante el sondeo activo de una red específica con tramas de sondeo.

La estación elige una red entre las que están disponibles e inicia un proceso de autenticación con el punto de acceso; una vez que se han verificado mutuamente, comienza el proceso de asociación. Únicamente, después de que se haya finalizado la asociación, la estación puede transmitir o recibir tramas en la red.

La asociación permite que el punto de acceso y la estación intercambien información y datos de capacidad. La información obtenida por el punto de acceso respecto a la ubicación de la estación, la puede comunicar a los otros puntos de acceso.

En este tipo de topología, todo el tráfico de la red, procedente de las estaciones inalámbricas deben pasar por un punto de acceso para poder llegar a su destino en la red LAN con cable o inalámbricas. El punto de acceso es siempre el emisor o receptor en esta modalidad de red.

Este tipo de red inalámbrica utiliza el protocolo CSMA/CA que detecta las portadoras y evita las colisiones. Dos estaciones, aunque estén dentro del área de cobertura del punto de acceso, es posible que no se escuchen. Utiliza medidas especiales para evitar las colisiones; entre ellas se incluye un intercambio de tramas “petición para emitir” y “listo para emisor” y un vector de asignación que se mantiene en cada estación de la red. Así que, aunque una estación no pueda escuchar la transmisión de la otra estación, oirá la transmisión de “listo para emitir”, por lo que, evitará transmitir durante la transmisión de la otra estación evitando así, una colisión.

La señalización y el sondeo que se utilizan para buscar puntos de acceso, y un proceso de reasociación que permite a la estación asociarse a un punto de acceso diferente, proporcionan una transición fluida. La sincronización entre las estaciones de la red se controla mediante las tramas de señalización periódicas enviadas por el punto de acceso. La sincronización es necesaria por varias razones relacionadas con los protocolos y esquemas de modulación de las conexiones inalámbricas.

Topología ad hoc

El término de esta topología se debe a que una red de este tipo puede crearse sin una planificación previa, y existe sólo mientras los dispositivos necesitan comunicarse. A diferencia de la topología de infraestructura, no necesita un punto de acceso o controlador central (figura 3.2).

En la topología ad hoc todos los dispositivos de una red dentro de un BSS son móviles o portátiles. También es conocida como BSS independiente (IBSS). Este tipo de topología opera como una red de igual a igual o peer to peer.

A más dispersión geográfica de cada nodo más dispositivos pueden formar parte de la red, aunque algunos no lleguen a verse entre sí. Cada dispositivo se comunica directamente con los demás dispositivos de la red, en lugar de pasar por un controlador.

La red ad hoc no disfruta todavía de algunos avances como retransmitir tramas entre dos estaciones que no se oyen mutuamente.

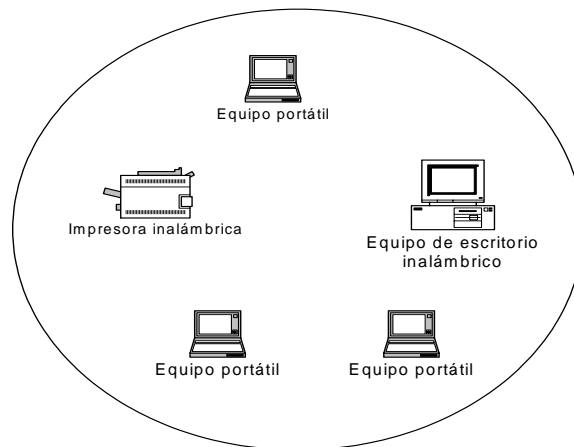


Figura 3.2 Topología ad hoc

3.3 Control de acceso al medio

En el estándar 802.11 se consideró dos tipos de proposiciones para el algoritmo MAC: protocolo de acceso distribuido y el protocolo de acceso centralizado. El primero, al igual que CSMA/CD, distribuye la decisión de transmitir entre todos los nodos usando un mecanismo de detección de portadora. El protocolo de acceso distribuido tiene sentido en las redes ad hoc donde las estaciones son paritarias. El protocolo de acceso centralizado es usual en las redes de topología de infraestructura, donde varias estaciones inalámbricas se comunican entre sí y están conectadas a un punto de acceso que se conecta a una LAN cableada.

El estándar final del 802.11 es un algoritmo MAC llamado MAC inalámbrico de principio distribuido (DFWMAC, Distributed Foundation Wireless MAC), que proporciona un mecanismo de control de acceso distribuido con un control centralizado opcional implementado sobre él. La subcapa inferior de la capa MAC es la función de coordinación distribuida (DCF). DCF utiliza un algoritmo de competición para proporcionar acceso a todo el tráfico. La función de coordinación puntual (PCF) es un algoritmo MAC centralizado utilizado para proporcionar un servicio sin competición. PCF se construye sobre DCF y utiliza las características de DCF para asegurar el acceso a los usuarios (figura 3.3).

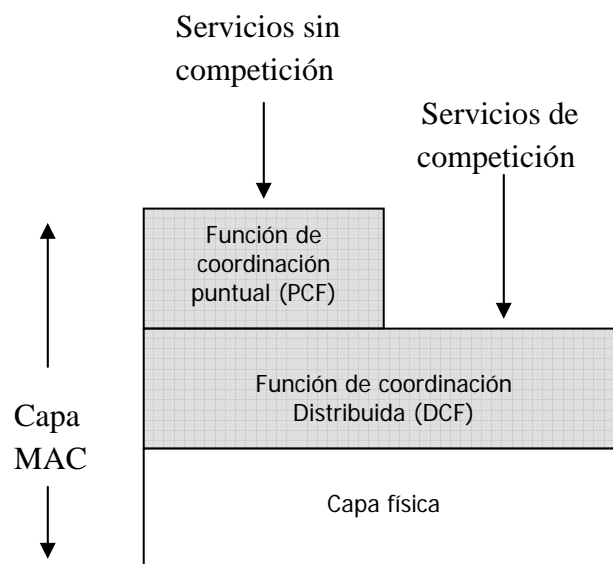


Figura 3.3 Arquitectura del protocolo IEEE 802.11

3.4 Especificación del medio

En la normalización 802.11 se definen tres medios físicos, los cuales se mencionan a continuación:

- Infrarrojos. Alcanzan una velocidad de transmisión de 1 y 2 Mbps y usan frecuencias en el intervalo 850 a 950 nanómetros.
- Espectro extendido de salto de frecuencia (FHSS).
- Espectro extendido de secuencia directa (DSSS).

Dos de ellos son medios que usan señales de radiofrecuencia y utilizan comunicación por espectro extendido, que es una forma de transmisión por radio. La tecnología de espectro extendido toma una señal de radio de banda estrecha existente y la divide en intervalos de frecuencias de diversas formas. El resultado es una señal que utiliza más ancho de banda, es más alta y más fácil de detectar por un receptor. Al mismo tiempo, la señal es difícil de interceptar, porque los intentos de localizarla explorando las bandas de frecuencia solo consiguen fragmentos aislados. También es difícil de interferir, porque sería necesario bloquear un intervalo más amplio de frecuencias para que la interferencia fuera eficaz.

Los medios de radiofrecuencia 802.11 funcionan en la banda de frecuencias de 2.4 GHz, ocupan 83 MHz de ancho de banda entre 2400 y 24835 Hz. Estas frecuencias no requieren licencias en la mayoría de los países, aunque existen diversas limitaciones en la intensidad de la señal, impuestas por los diferentes gobiernos.

La diferencia entre los diferentes tipos de comunicaciones del espectro extendido, radica en el método seguido en la distribución de las señales entre las frecuencias.

Por una parte, el espectro extendido de salto de frecuencia usa un código o algoritmo predeterminado para imponer cambios de frecuencia continuamente, en incrementos discretos sobre una amplia banda de frecuencias. La implementación FHSS del 802.11 exige 79 canales de 1 MHz, aunque pueden requerirse límites más pequeños. La velocidad de los cambios de frecuencia, que es el tiempo que la señal permanece en cada frecuencia antes de saltar a la siguiente, es independiente de la velocidad de bit de la transmisión de datos. Si la velocidad del salto de frecuencia es mayor que la velocidad de bit de la señal, la tecnología se llama sistema de salto rápido. Por el contrario, si la señal del salto de frecuencia es menor que la velocidad de bit, se llama un sistema de salto lento.

La implementación FHSS define una velocidad de 1 Mbps, con una velocidad opcional a 2 Mbps.

En las comunicaciones de espectro extendido de secuencia directa, la señal a transmitir se modula por medio de un código digital llamado chip o código por chip, que tiene una señal de bit más alta que la velocidad de la señal de datos. El código de chip convierte cada bit de la señal de datos en varios bits, que son los que se transmiten realmente. Cuanto más largo es el código de chip, más se aumenta el código de la señal de datos original. Dicho aumento hace más fácil para el receptor la recuperación de los datos transmitidos si algunos bits se corrompen. Conforme se aumenta la señal, disminuye el significado de cada bit. De igual manera que en el FHSS, un receptor que no tiene el código de chip usado por el emisor no puede interpretar la señal DSSS, y únicamente la ve como ruido. Solo DSSS soporta las velocidades de transmisión de 5.5 y de 11 Mbps del estándar 802.11b.

En las comunicaciones por infrarrojos, el rango de frecuencias que utilizan se encuentra por debajo del espectro de la luz visible. Una red de infrarrojos puede funcionar usando señales difusas o reflejadas. Sólo puede funcionar adecuadamente en un ambiente interior con superficies que proporcionen una adecuada difusión o reflexión de la señal. Soportan una velocidad de transmisión de 1 Mbps y una opcional de 2 Mbps.

3.5 Sistemas de redes infrarrojas

Los sistemas de comunicación por infrarrojos son útiles para las comunicaciones locales punto a punto, así como, para aplicaciones multipunto dentro de áreas de cobertura limitada, por ejemplo: habitación. Utilizan señales infrarrojas que se propagan en línea recta y pueden ser interrumpidas por cuerpos opacos. El rayo de luz infrarroja que utilizan para transportar los datos entre dispositivos, es susceptible a la luz desde fuentes como ventanas, por lo que requiere que las señales de transmisión sean de mayor potencia.

Ventajas

- Los emisores y receptores son muy simples y baratos.
- No interfieren con otros sistemas de radiofrecuencia.
- No es necesaria la obtención de una licencia administrativa para su uso.

Desventajas

- Poco ancho de banda.
- Necesidad de comunicación visual.
- Usualmente la comunicación se realiza entre dos interlocutores.
- No es capaz de atravesar muros.
- Limitado alcance de comunicación.

Ocupa un rango de frecuencias desde los 3×10^{11} hasta los 2×10^{14} Hz.

Hay cuatro tipos de redes infrarrojos:

- Redes en línea visual (Line-of-sight). En las cuales sólo es posible la transmisión si el emisor y el receptor se ven libremente sin obstáculos.
- Redes por dispersión de infrarrojos (Scatter). Este tipo emite transmisiones para que reboten en las paredes y techos y eventualmente contacten con el receptor.
- Redes por reflexión (Reflective). En este tipo, los transceptores ópticos situados cerca de los ordenadores, transmiten hacia un punto en común que redirige las transmisiones al ordenador apropiado.
- Telepunto óptico de banda ancha. Proporciona servicios de banda ancha. Es capaz de manejar requerimientos de alta calidad multimedia que puedan coincidir con los proporcionados por una red de cable.

3.6 Sistemas de radiofrecuencia

Es adecuada para las aplicaciones omnidireccionales. Por lo tanto, no necesitan antenas parabólicas ni que dichas antenas estén instaladas sobre una plataforma rígida para estar alineadas.

Ventajas

- Mayor área de cobertura.
- No necesita comunicación visual entre dispositivos.
- Mayor ancho de banda.

Desventajas

- Propenso a las interferencias electromagnéticas.
- Rango de frecuencias limitado.
- Se requiere licencia para su operación en algunos casos.

Existe otra desventaja en las transmisiones de radiofrecuencia: los países están tratando de ponerse de acuerdo en cuanto a las bandas que cada uno puede utilizar.

3.7 Estándar 802.11

Los estándares son desarrollados por organismos reconocidos internacionalmente, tal es el caso de la IEEE (Institute of Electrical and Electronics Engineers) y la ETSI (European Telecommunications Standards Institute). Una vez desarrollados se convierten en la base de los fabricantes para desarrollar sus productos.

Entre los principales estándares se encuentran:

- **IEEE 802.11.** El estándar original de WLANs que soporta velocidades entre 1 y 2 Mbps.
- **IEEE 802.11a.** Estándar de alta velocidad, soporta velocidades de hasta 54 Mbps en la banda de 5 GHz.
- **IEEE 802.11b.** Estándar dominante de WLAN (conocido también como Wi-Fi), que soporta velocidades de hasta 11 Mbps en la banda de 2.4 GHz.
- **IEEE 802.11g.** Estándar que trabaja de la misma forma que el 802.11a; pero es compatible con el 802.11b.

El gran éxito de las WLANs es debido a que utilizan frecuencias de uso libre, es decir no es necesario pedir autorización o permiso para utilizarlas, las normativas varían dependiendo del país. La desventaja de usar este tipo de bandas de frecuencias es que las comunicaciones son propensas a sufrir interferencias y errores de transmisión.

A continuación se indicaran las características principales de los estándares descritos en capítulos anteriores.

3.7.1 802.11a

- Funciona en 12 canales sobre 5 GHz, lo que reduce las interferencias.
- La transferencia de datos se realiza a velocidades hasta cinco veces superiores a la 802.11b mejorando la calidad de video streaming y pudiendo manejar ficheros con mucha mayor rapidez.
- No es compatible con la 802.11b, por lo que no pueden aprovecharse las inversiones ya realizadas.
- La modulación empleada es la OFDM.
- Velocidades de hasta 54 Mbps dentro de los estándares del IEEE y algunos fabricantes ofrecen velocidades de hasta 72 y 108 Mbps.
- Hasta 64 usuarios por Punto de Acceso (AP).

3.7.2 802.11b

- Líder para redes sin hilos
- Emplea la marca comercial Wi-Fi, que está avalada por la asociación WECA (Wireless Ethernet Compatibility Alliance).
- Velocidades de 11 Mbps estandarizada por el IEEE y algunos fabricantes ofrecen una velocidad de 22 Mbps.
- 32 usuarios por AP.
- Opera dentro de la frecuencia de los 2.4 GHz.
- Inicialmente empleaba FHSS; sin embargo, se ha impuesto DSSS.

3.7.3 802.11g

- Funciona sobre 3 canales de la banda 2.4 GHz.
- Ofrece una velocidad de 54 Mbps (similar a la 802.11a).
- Es más segura que la 802.11b.
- Es compatible con la 802.11b.
- Casi todos los fabricantes han anunciado equipos para este protocolo.
- Funciona dentro de la frecuencia de 2.4 GHz.
- La técnica de modulación empleada en esta tecnología es la DSSS (Direct Sequence Spread Spectrum).

Capítulo 4

CASO: División de Universidad Abierta de la Facultad de Derecho (DUAD).

La liberación del mercado de servicios de telecomunicaciones y las nuevas tecnologías, presentan una oferta cada vez más amplia de servicios de red como lo son: servicios de intranet y extranet, al igual que la conexión a Internet.

La presente propuesta tiene como finalidad el aprovechar al máximo la infraestructura a implementarse; de tal manera que se obtenga en máximo beneficio permitiendo el continuo crecimiento de la red y la incorporación a la misma.

4.1 Introducción

En este capítulo se hace un análisis de la situación actual de la Institución, se abarca un panorama general de la red de la UNAM y se estudia la red de datos del Sistema de Universidad Abierta de la Facultad de Derecho. Se hacen observaciones de diseño y desempeño de la red actual de la Dependencia. Se determina una metodología a emplear para obtener una solución del problema; de igual manera, se plantea una propuesta de red híbrida de datos que cumpla con las necesidades del usuario conforme a normas de Sistema de Cableado Estructurado. Se detallan las modificaciones a efectuarse y se dan a conocer los detalles del equipo a utilizar; así como, para robustecer el actual. Se proporcionan las medidas de seguridad que se deben tomar, tanto en la red LAN como en la inalámbrica.

Al final del capítulo, se proporcionan las opciones a elegir para dar una solución y se define la opción más viable, considerando la información presentada en los capítulos anteriores y basándonos en el análisis de costo beneficio correspondiente.

4.2 Backbone de la UNAM

La Universidad Nacional Autónoma de México inicia un proceso de renovación y crecimiento tecnológico en 1989. Creando así, la Dirección de Telecomunicaciones de la UNAM cuyo objetivo era, crear la Red Integral de Telecomunicaciones de la UNAM capaz de transmitir voz, datos, imágenes y posteriormente vídeo entre las dependencias universitarias, ubicadas desde Ensenada, B.C. hasta Puerto Morelos, Q. Roo.

Los objetivos principales de esta red son:

- Integrar a sus alumnos, desde el bachillerato hasta el posgrado, a la cultura informática, entendida ésta como la integración del cómputo y las telecomunicaciones.
- Incorporar la enseñanza de la informática a los planes formales de estudio de todas las disciplinas y actualizarla periódicamente.
- Proporcionar a su personal docente y de investigación todas las herramientas de tecnología informática para el desarrollo de sus actividades.
- Dotar a la institución de una moderna infraestructura de telecomunicaciones y cómputo.
- Utilizar esta herramienta como un factor de transformación profundo en su modelo de enseñanza aprendizaje.

En tanto se desarrollaba la primera etapa en 1989, se instala una red nacional privada satelital conformada por 7 estaciones terrenas para la transmisión de voz y datos. Paralelamente, se sustituye el sistema telefónico en el campus de Ciudad Universitaria por una red de conmutadores telefónicos digitales que, paulatinamente se incrementa para incorporar a los 7 campos de las Universidades Multidisciplinarias distribuidas en el área metropolitana.

En el campus de Ciudad Universitaria inicia un proceso acelerado de crecimiento en su Red de datos con una topología de anillo en el backbone de FDDI a 10 Mbps. En este momento, la UNAM es la primera Institución latinoamericana en conectarse a Internet y es el principal protagonista del Internet en México.

A finales de 1992, esta red contaba ya con 31 nodos de cómputo y telecomunicaciones enlazados a través de fibra óptica, vía satélite o vía microondas, y se destacaba la incorporación de la Ciudad de la Investigación en Cuernavaca, Mor. El servicio de Internet es uno de los recursos más utilizados por los investigadores de la UNAM. Internet se ofrece también a Universidades públicas y privadas en el D.F. y área metropolitana.

A finales de 1994, se incorpora la tercera red con el propósito de llevar educación a distancia a través de videoconferencia a la comunidad universitaria.

En junio de 1997 la infraestructura de telecomunicaciones tenía más de 15,000 computadores conectadas a la Red de datos, más de 10,000 líneas del sistema telefónico digital, 20 salas de videoconferencia y 5 enlaces internacionales con capacidad de transmisión de 10 Mbps a EEUU para la conexión a Internet. En esta fecha, el campo de Juriquilla, Qro., se integra a esta gran Red.

En agosto de 1997 la UNAM inicia operaciones con un backbone ATM que le permite consolidar con esta tecnología las redes de datos; sin embargo, es hasta 1999 cuando incorpora el tráfico de voz y videoconferencia en una plataforma multimedia. En esta fecha se coloca la Institución como una de las redes más modernas y más grandes en el ámbito académico en Latinoamérica, al contar con esta moderna tecnología y comparada incluso con redes de Universidades de Norteamérica (figura 4.1). Este esquema funcionó hasta el mes de agosto del 2002.

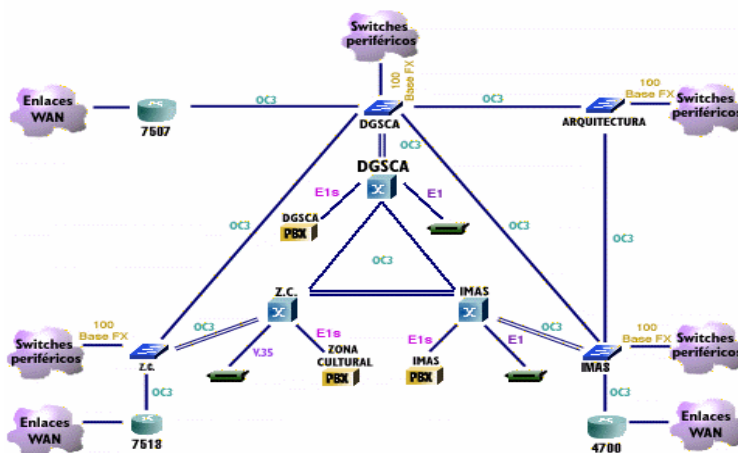


Figura 4.1 Topología del Backbone ATM-UNAM en 1997

El proceso de migración del backbone de la red UNAM con tecnología ATM a tecnología Gigabit se realizó desde finales del 2001 hasta, como ya se ha mencionado, el mes de agosto de 2002. Quedando así, la infraestructura suficiente para la implementación de aplicaciones que requieren mayor ancho de banda, al igual que una pérdida nula de paquetes, es decir, aplicaciones en tiempo real como lo son: voz sobre IP, video por H.323, transmisión multicast, telemedicina, educación a distancia, bibliotecas digitales. Además, de los servicios ya existentes: correo electrónico, transferencia de archivos, página Web, etcétera. Dicha infraestructura es compatible con Internet2 y permite la convergencia con la tecnología del protocolo IP; es una plataforma del protocolo IPv6, MPLS, y Calidad de Servicio (QoS).

A partir de ese año, 2002, el backbone de la UNAM utiliza tecnología Gigabit Ethernet entre los cuatro nodos principales: DGSCA, IIMAS, Arquitectura y Zona Cultural. Por medio de la redundancia entre dichos nodos asegura la disponibilidad de la Red UNAM. Figura 4.2., considerando aún los conmutadores ATM para tal objetivo (figura 4.2).

RedUNAM además de dar servicios a otras entidades universitarias, los ofrece también a más de 300 instituciones mexicanas, entre las cuales se pueden mencionar al Centro Nacional de Prevención de Desastres (CENAPRED), la Red Sismológica Nacional del Instituto de Geofísica de la UNAM, a los Institutos Nacionales de Cancerología, de Enfermedades Respiratorias, de Perinatología; a los Institutos Mexicanos de Psiquiatría, de la Propiedad Industrial; a las Universidades Autónomas de Campeche, Chapingo, Estado de México, Guerrero, Hidalgo y Querétaro; al Hospital General de Acapulco, Comisión Nacional de Electricidad y Comisión Nacional del Agua; además de universidades privadas como el ITAM, La Salle, la Anáhuac y la Panamericana, entre muchas otras. De igual forma, da servicio a un centro especializado de Supercómputo, cuenta con 31 nodos de cómputo y telecomunicaciones enlazados a través de fibra óptica, por vía satélite o por microondas, cuenta con una red satelital conformada por siete estaciones terrenas y con tres enlaces con una capacidad de transmisión de 34 Megabits por segundo cada uno de ellos para la conexión mundial a Internet vía Estados Unidos. Asimismo, tiene 34 enlaces nacionales y un backbone de Internet 2, atiende siete mil conexiones por línea conmutada, aloja 300 sitios de Internet, transporta diariamente alrededor de 100 mil correos electrónicos, registra 200 mil usuarios que consultan los servicios de información de la UNAM y tiene un total de 70 millones de consultas mensuales. Mantiene en operación alrededor de 15 mil líneas telefónicas a través de una red de telefonía integrada por 39 conmutadores digitales.

4.2.1 Red de cómputo actual del edificio de la DUAD

La División de Universidad Abierta de la Facultad de Derecho esta ubicado a un costado de la Torre de Humanidades, entre el edificio de Posgrado de Derecho y la Facultad de Economía (figura 4.4).

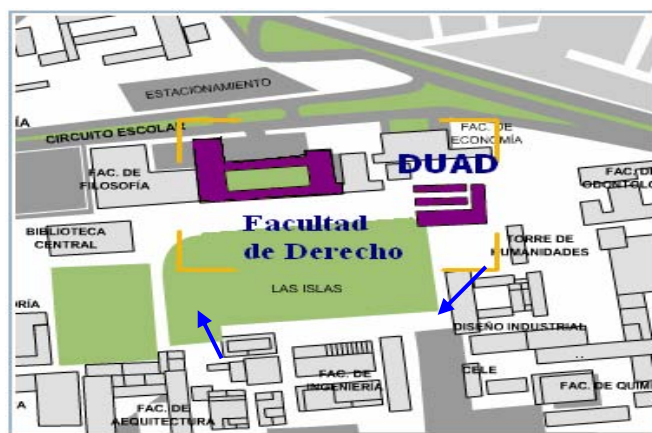


Figura 4.4 Plano de ubicación de la DUAD

El enlace llega del backbone de Red-UNAM a la DUAD mediante un enlace en fibra óptica multimodo a 10 Mbps proveniente del Lanplex 2500 de Laborales, el cual se comunica con IIMAS, que junto con DGSCA, Arquitectura y Zona Cultural conforman el backbone con tecnología Gigabit de la UNAM (figura 4.5).

Dicho Lanplex recibe en uno de sus slots el enlace a Gigabit proveniente del switch de capa 3 BigIron ubicado en IIMAS. Mantiene el enlace 10 FL con la DUAD y con el edificio principal de la Facultad de Derecho mediante el uso de dos de sus puertos para alimentar las redes de cómputo correspondientes.

En el backbone de Red UNAM se mantiene, además, de la comunicación a Gigabit de los dispositivos actuales, la conexión hacia los switches ATM como una doble redundancia y con esto mantener una alta disponibilidad de la Red UNAM.

Con la tecnología Gigabit Ethernet, la Red UNAM obtuvo mayor ancho de banda ya que, la tecnología ATM utilizada anteriormente utilizaba equipos Passport de Nortel Networks con tecnología ATM, los cuales se interconectaban mediante enlaces tipos OC-3 con un ancho de banda de 155 Mbps. Además, la anterior arquitectura utilizaba el protocolo LAN Emulation por medio de enlaces OC-3, que al ser sustituido por la tecnología Gigabit Ethernet se redujo el tiempo de retardo en la comunicación.

Cada uno de los Institutos, Facultades o dependencias son alimentados por segmentos de red Ethernet o Gigabit Ethernet conectados a switches con capacidades de enrutamiento, como el modelo Lanplex 2500 de capa 3 ubicado el Laborales.

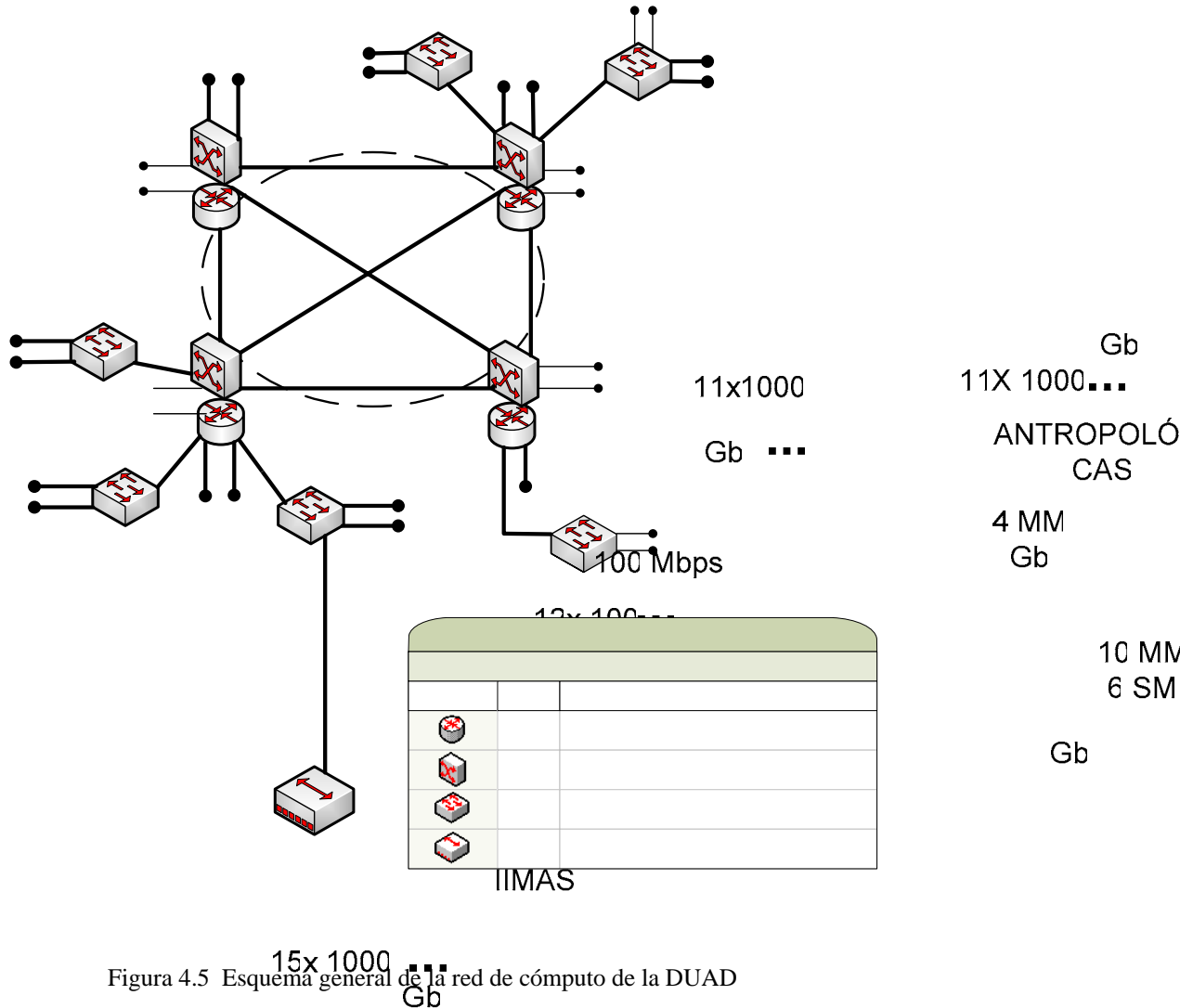


Figura 4.5 Esquema general de la red de cómputo de la DUAD

4.3 Metodologías de análisis

4.3.1 Metodología utilizada por DGSCA

La DGSCA es la entidad universitaria encargada de la operación de los sistemas centrales de cómputo académico y de las telecomunicaciones de la Institución. Y como tal, está dividida en diversas direcciones para llevar a cabo sus diferentes funciones.

La infraestructura de telecomunicaciones es supervisada por la Dirección de Telecomunicaciones con base en normas, lineamientos y políticas tanto técnicas como del uso de los servicios emitidos por la Dirección General de Servicios de Cómputo Académico.

La DGSCA estipula lineamientos para la actualización de redes de datos, en los cuales se menciona el contenido de la documentación de dicha red.

- Documentación
 1. Descripción
 - a. Objetivo. Se indica el objetivo de la actualización de la red de datos.
 - b. Alcance. Se describen los logros esperados con la implantación de la red.
 2. Planos o croquis con:
 - a. Número y tipo de servicio. Los servicios son etiquetados de acuerdo a su clasificación: de voz, datos u otro.
 - b. Ubicación de los cuartos de telecomunicaciones. Se especifica en el plano la ubicación física de los cuartos de telecomunicaciones.
 - c. Criterio de instalación de canalización. Se indica bajo que estándar se implemento la red de datos y el tipo de canalización.
 3. Catálogo de conceptos. Se especifica el significado de las etiquetas de los servicios.
 4. Especificaciones técnicas. Se indica las características propias de cada uno de los elementos de la red implantada.

La DGSCA estipula los requisitos mínimos para la elección de un Integrador de Sistemas de Transporte de Información (ISTI) para llevar a cabo la instalación de la red de datos. Un ISTI es una compañía que ha acreditado programas de capacitación, demostrando habilidad y profesionalismo en técnicas y tecnologías avanzadas en conectividad de aplicaciones, seguridad, control entre otras más. Un Integrador de Sistemas de Transporte de Información es una empresa legalmente constituida, actualizada en las tecnologías de vanguardia, y certifica la implementación de la infraestructura realizando diversas evaluaciones de cada uno de los servicios proporcionados. Además, propone diversas alternativas y se encarga de la implantación y certificación de la red a implantarse.

4.3.2 Metodología propuesta

Para desarrollar un proyecto es imprescindible contar con una logística que nos garantice resultados que cumplan con los objetivos, metas, y alcances planteados del proyecto. La planeación es fundamental en el desarrollo de proyectos y su importancia para alcanzar los resultados programados se fundamenta en una metodología estratégica adecuada a nuestras necesidades para alcanzar dicho estado deseado.

Las necesidades de comunicación se acrecientan día a día; sin embargo, la adquisición y actualización de la infraestructura tecnológica para satisfacer dichas necesidades requiere de la inversión de recursos de diversa índole sacrificando beneficios actuales. El ingeniero tiene con función satisfacer las necesidades humanas mediante la toma de decisiones efectivas y consistentes que minimicen los recursos a invertir y maximicen los beneficios; por lo que para el desarrollo del proyecto de la presente tesis se eligió la metodología propuesta por Edward V. Krick en su libro “Introducción a la ingeniería y al diseño de la ingeniería”. Dicha metodología se muestra en la figura 4.6.

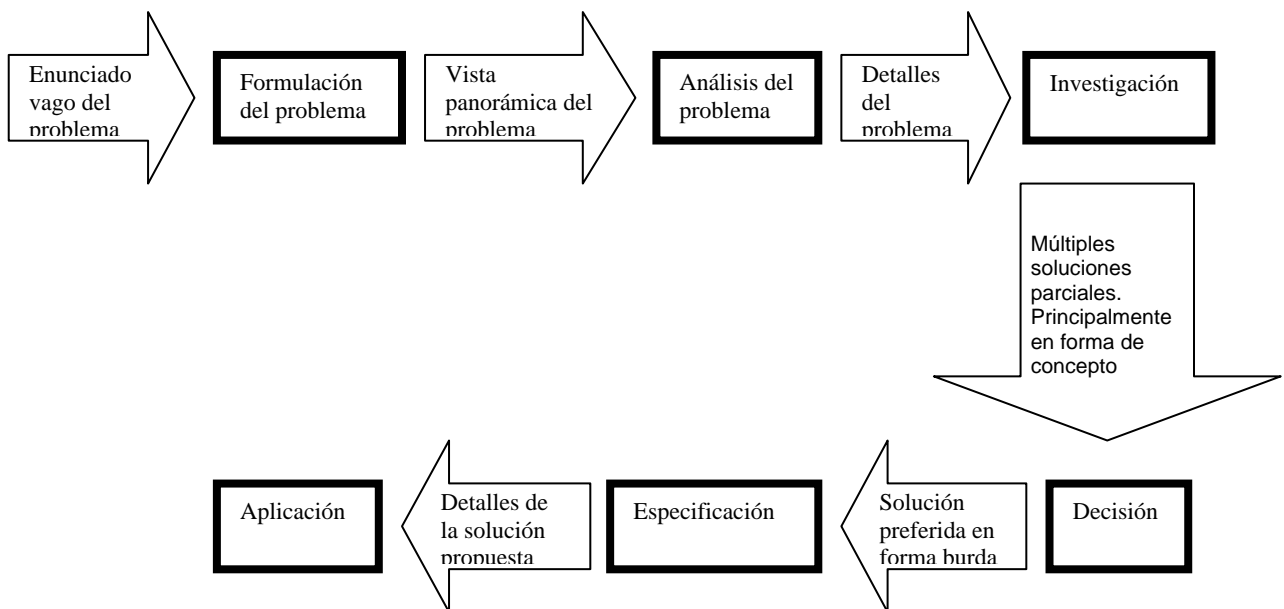


Figura 4.6 Metodología utilizada de Edward V. Krick

La decisión elegida se basa en que es un procedimiento general para resolver un problema de ingeniería. La aplicación de dicha metodología a nuestro proyecto se menciona a continuación.

1. **Formulación del Problema.** Actualmente la División de Universidad Abierta de la Facultad de Derecho de la UNAM se ve en la necesidad de tener un mayor número de máquinas conectadas entre sí; así como, una mayor velocidad de conexión debido a la incorporación futura de servicios que demandan un mayor ancho de banda tales como, educación a distancia y asesoría en línea.

En la actualidad la red de datos no proporciona la posibilidad de crecimiento de la misma, por lo que es imprescindible su migración a una red de datos que proporcione mayor velocidad de transmisión, mayor flexibilidad, y mayor accesibilidad a la información a todo el personal que compone dicha Institución Educativa, tanto el área de docentes así como el alumnado.

Actualmente no se cubren las necesidades de dicha institución como el servicio móvil, educación a distancia, y la posibilidad de aumentar el número de nodos en la red de datos. La educación a Distancia comprende asesoría en línea, foros de chat. Los servicios antes mencionados contribuyen a la formación académica de los alumnos.

2. **Análisis del problema.** La definición y estudio de las características cualitativas y cuantitativas del problema se realizan de manera detallada, lo que nos lleva a la descripción del estado actual de la red de cómputo de la DUAD. Tomando en cuenta la información arrojada de dicho análisis y con base en los objetivos planteados nos proporciona las diversas soluciones, que si bien, pueden funcionar para alcanzar las metas planteadas; pero no así con el objetivo y restricciones establecidas. Considerando lo anterior, sólo se discute en esta tesis aquella que cumple con las restricciones establecidas y garantiza satisfacer las necesidades del usuario.
3. **Planeación.** Es la etapa donde se consideran las distintas áreas que participan en el proyecto formando un equipo multidisciplinario. Cada área coordina su propia información y participa en conjunto con el equipo multidisciplinario para la toma de decisiones. Se planea el avance del proyecto con base en la calendarización de las actividades antecesoras de cada área.
4. **Evaluación.** Es en esta etapa cuando se realiza el análisis del costo del anteproyecto considerando los posibles candidatos a realizar el proyecto. Se analizan las ventajas y desventajas de acuerdo a las garantías proporcionadas por cada uno de los candidatos; al igual que las pertinentes a contar con la infraestructura tecnológica. Considerando lo anterior nos conduce a realizar el análisis de la propuesta, del costo de la misma y la relación costo beneficio de su implantación.
5. **Implantación.** Una vez que se a entregado el anteproyecto y elegido el responsable de realizar el proyecto, se deben realizar, en caso de existir, las correcciones pertinentes. En esta etapa se debe supervisar constantemente el avance del proyecto

con base en una memoria técnica diseñada con base en el anteproyecto donde se especifica el detalle de la solución elegida. Debe señalarse que se deberá contar con la memoria técnica y la documentación correspondiente al finalizar el proyecto.

4.4 Estado de la red de cómputo de la DUAD

La División de Universidad Abierta de la Facultad de Derecho cuenta con una red de datos no sistematizada ni en condiciones óptimas para proporcionar la posibilidad de crecimiento ni flexibilidad de la misma.

La falta de planeación de la red ha generado en ella un estado no estático, ya que existe una mezcla de estándares T568-A y T568-B sin establecer el uso único de uno de ellos.

La red de datos actualmente está implantada con una topología estrella 10BASE-T. Utiliza un hub a 10 Mbps con cable par trenzado sin blindar categoría 5 y 5e. Este tipo de cable empleado para la distribución de datos en la red es a 100 omhs y 24 AWG. Considerando que el cable categoría 5 no soporta la velocidad de operación de Gigabit se considera su sustitución por cable UTP categoría 6 en toda la Institución, para satisfacer las necesidades de comunicación de los usuarios.

Las tarjetas de red utilizadas actualmente para la comunicación son de tipo 3com 10/100. Tomando en cuenta que el hub opera a una velocidad de 10 Mbps, las tarjetas de red 3com poseen la característica de autonegociación para la detección de la velocidad de la red de datos. Es decir, a pesar de su capacidad de operación de 100 Mbps, al detectar dicha velocidad de la red va a operar a 10 Mbps.

En la DUAD no se cuenta con algún equipo activo de la capa 3 por lo que el ancho de banda no es administrado y tampoco aísla el tráfico de red del segmento. El ancho de banda de la red esta limitado por el hub a 10 Mbps por lo que la velocidad real de operación de cada host depende del número de equipos en operación. Aunado a lo anterior, cabe mencionar que el hub de la DUAD proporciona el servicio a otros dos edificios por medio de la conexión en “cascada” con sus respectivos hubs.

La distribución de los puntos no planeada y la demanda que crece continuamente han saturado la capacidad del equipo activo de la red. No existe ningún servicio que proporcione la movilidad de los usuarios.

4.4.1 Equipo de cómputo actual

La importancia de conocer el equipo de cómputo que reside en la actualidad, se fundamenta en presentar el ancho de bando demandado por las aplicaciones que puedan ser soportadas por los sistemas operativos correspondientes.

El equipo de cómputo con que cuenta actualmente la DUAD se describe en las tablas 4.7 y 4.8.

Equipo	Procesador	Disco duro	Memoria	Sistema Operativo	Área
Ordenador	Pentium 3/750 MHz	1 GB	32 MB	Windows XP Profesional	Jefatura
Ordenador	Pentium 2	10 GB	64 MB	Windows XP Home	Servicios Escolares
Ordenador	Pentium 3	20 GB	128 MB	Windows 2000 Profesional	Servicio Social
Ordenador	Pentium 3/750 MHz	40 GB	128 MB	Windows XP Profesional	Jefatura
Ordenador	Pentium 3/750 MHz	20 GB	128 MB	Windows XP Profesional	Coordinación Administrativa
Ordenador	Pentium 3/750 MHz	40 GB	128 MB	Windows XP Profesional	Pedagogía
Ordenador	Pentium 3/750 MHz	40 GB	128 MB	Windows XP Profesional	Centros Asociados
Ordenador		40 GB	128 MB	Windows XP Profesional	Coordinación Administrativa
Ordenador	Pentium 3 /750 MHz	40 GB	256 MB	Windows XP Profesional	Cómputo
Ordenador	Pentium 3/1.2 GHz	15 GB	64 MB	Windows XP Profesional	Apoyo a la titulación
Ordenador	Pentium 3/1.2 GHz	20 GB	128 MB	Windows XP Profesional	Jefatura
Ordenador	Pentium 3/1.2 GHz	30 GB	128 MB	Windows XP Profesional	Servicios Escolares
Ordenador	Pentium 3 / 1.2 GHz	40 GB	128 MB	Windows XP Profesional	Coordinación Académica
Ordenador	Pentium 4/1.8 GHz	40 GB	256 MB	Windows XP Profesional	Servicios Escolares
Ordenador	Pentium 4/1.8 GHz	40 GB	256 MB	Windows XP Profesional	Servicios Escolares
Ordenador	Pentium 4/1.8 GHz	40 GB	256 MB	Windows XP Profesional	Diseño
Ordenador	Pentium 4/1.8 GHz	40 GB	256 MB	Windows XP Profesional	Coordinación Administrativa
Ordenador	Pentium 4/1.8 GHz	40 GB	256 MB	Windows XP Profesional	Coordinación Administrativa
Ordenador	Pentium 4/1.8 GHz	40 GB	256 MB	Windows XP Profesional	Coordinación Administrativa
Ordenador	Pentium 4/1.8 GHz	80 GB	256 MB	Windows XP Profesional	Cómputo
Ordenador	Pentium 4 / 1.8 GHz	80 GB	512 MB	Windows XP Profesional	Proyectos Especiales
Ordenador	Pentium 4/2.6 GHz	40 GB	256 MB	Windows XP Profesional	Exámenes
Servidor	Pentium 4/2.6 GHz	40 GB	256 MB	Windows XP Profesional	Cómputo
Servidor	Pentium 4/2.6 GHz	40 GB	256 MB	Windows Advance 2000 Profesional	Cómputo
Ordenador	Pentium 4/2.8 GHz	40 GB	128 MB	Windows XP Profesional	Coordinación Administrativa
Ordenador	Pentium 4/2.8 GHz	40 GB	128 MB	Windows XP Profesional	Pedagogía
Servidor	Pentium4HT/3.2 GHz	160 GB	1 GB	Linux debian	Cómputo

Tabla 4.7 Equipo de cómputo de la DUAD

Equipo	Marca	Tipo	Área
Impresora	Hewlett Packard	LaserJet 4 Plus	Apoyo a la titulación
Impresora	Hewlett Packard	LaserJet 5P	Jefatura
Impresora	Hewlett Packard	LaserJet 5	Diseño
Impresora	Hewlett Packard	LaserJet 5 L	Coordinación Administrativa
Impresora	Startx	NX-1500	Cómputo
Impresora	Kyosera	Mita DP 1800	Proyectos Especiales
Impresora	Kyosera	Mita DP 1800	Exámenes
Impresora	Lexmark	E310	Servicios Escolares
Impresora	Lexmark	E321	Servicios Escolares
Impresora	Lexmark	E321	Servicios Escolares
Impresora	Lexmark	E321	Cómputo
Impresora	Hewlett Packard	920c	Coordinación Administrativa
Scanner	Hewlett Packard	ScanJet Iic	Coordinación Administrativa
Scanner	Hewlett Packard	3570	Diseño

Tabla 4.8 Dispositivos externos

4.4.2 Equipo de red actual

La red de datos de la DUAD cuenta con una acometida en fibra óptica de 8 hilos multimodo proveniente de uno de los puertos del equipo Lanplex 2500 de Laborales a una velocidad de 10 Mbps. La fibra óptica de tipo exterior FL llega al módulo interno, para fibra óptica, de un hub 3com de 24 puertos TELCO.

El hub 3com se conecta al panel de parcheo tipo regleta 110c para distribuir el cableado hasta el área de trabajo. A dicho panel de parcheo se conecta un transceiver de UTP a fibra óptica para dar servicio a la Secretaría Académica llegando la acometida a un hub Hewlett Packard de 24 puertos TELCO; el cual, remata los servicios a una regleta 110c de 24 puertos. El hub Hewlett Packard posee un puerto para cable coaxial, 2 puertos RJ45 para extensión de servicios, un interfaz serial para configuración del equipo mediante consola, y un módulo interno de fibra óptica al cual llega la acometida proveniente de la DUAD.

El hub de Secretaría Académica tiene a su vez conectados dos hubs más de 8 puertos 3com. Uno de los hubs proporciona el servicio de red a algunos hosts de la Secretaría Académica, y el resto de los hosts pertenecientes a la misma están conectados al hub Hewlett Packard, así como, los pertenecientes al área de trabajo de la Revista de la Facultad de Derecho. El otro hub de 8 puertos proporciona el servicio a la Secretaría de Planeación, la Asociación de Colegios de Profesores, y el Laboratorio de Enseñanza Práctica de Derecho.

El esquema de dichos equipos activos se muestra en la figura 4.9.

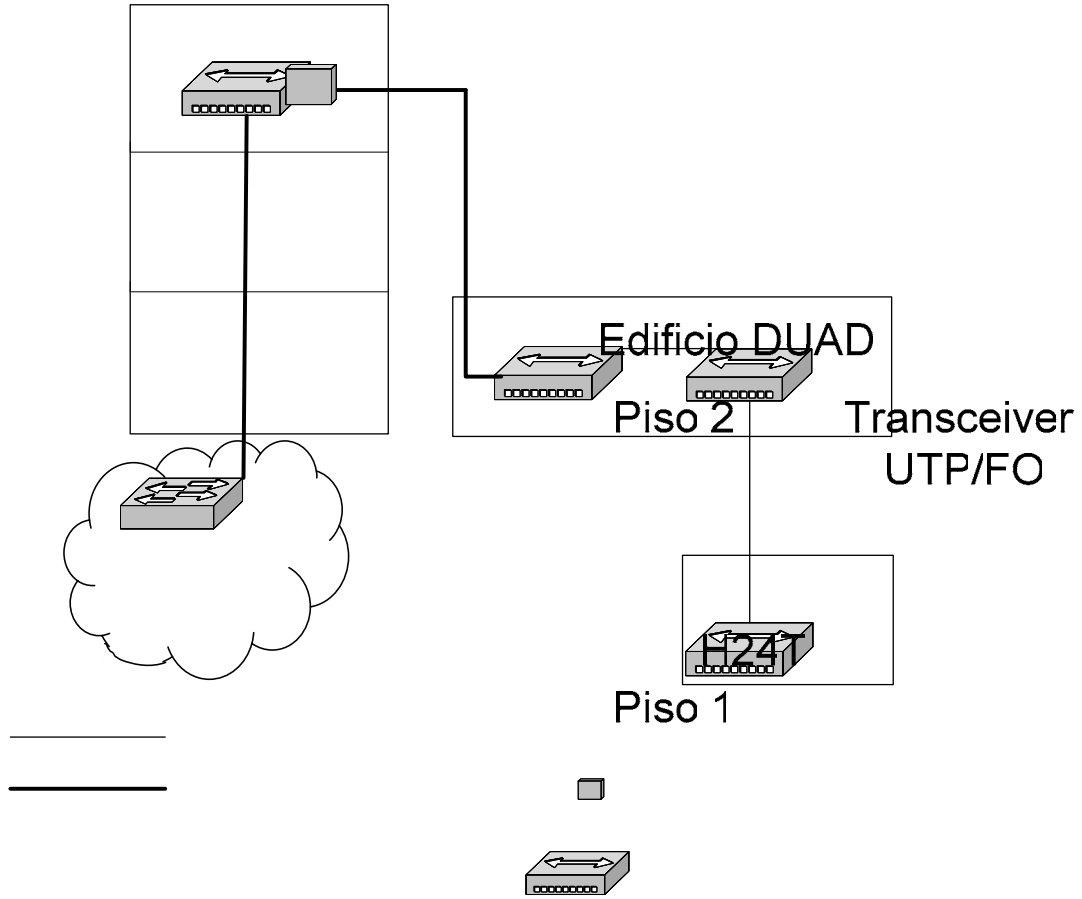


Figura 4.9 Equipo activo de la red actual de la DUAD y Dependencias adjuntas

Es importante considerar los equipos a los cuales se proporciona el servicio desde el hub de la dependencia para el análisis del tráfico en la red de datos.

4.4.3 Topología utilizada actualmente

La División de Universidad Abierta funciona con una topología física tipo estrella y lógica tipo bus Ethernet a 10 Mbps. La configuración física de estrella asigna a todos los host pertenecientes a la red su propio segmento físico de cable; sin embargo, la velocidad se reparte entre todos ellos debido al hub en que confluyen los mismos como punto central. Dado que este dispositivo activo no tiene ningún componente inteligente, ya que únicamente amplifica y repite la señal recibida en uno de sus puertos a todos los demás,

ocasiona el incremento del tráfico en la red y acrecenta el número de colisiones. El cable utilizado para la transferencia de datos es UTP categoría 5/5e a 100 ohms.

Cabe mencionar que las Secretarías y diversas áreas de trabajo a las que proporciona el servicio por medio del hub Hewlett Packard, utilizan una topología física tipo estrella 10BASE-T con cable UTP categoría 5e (figura 4.10).

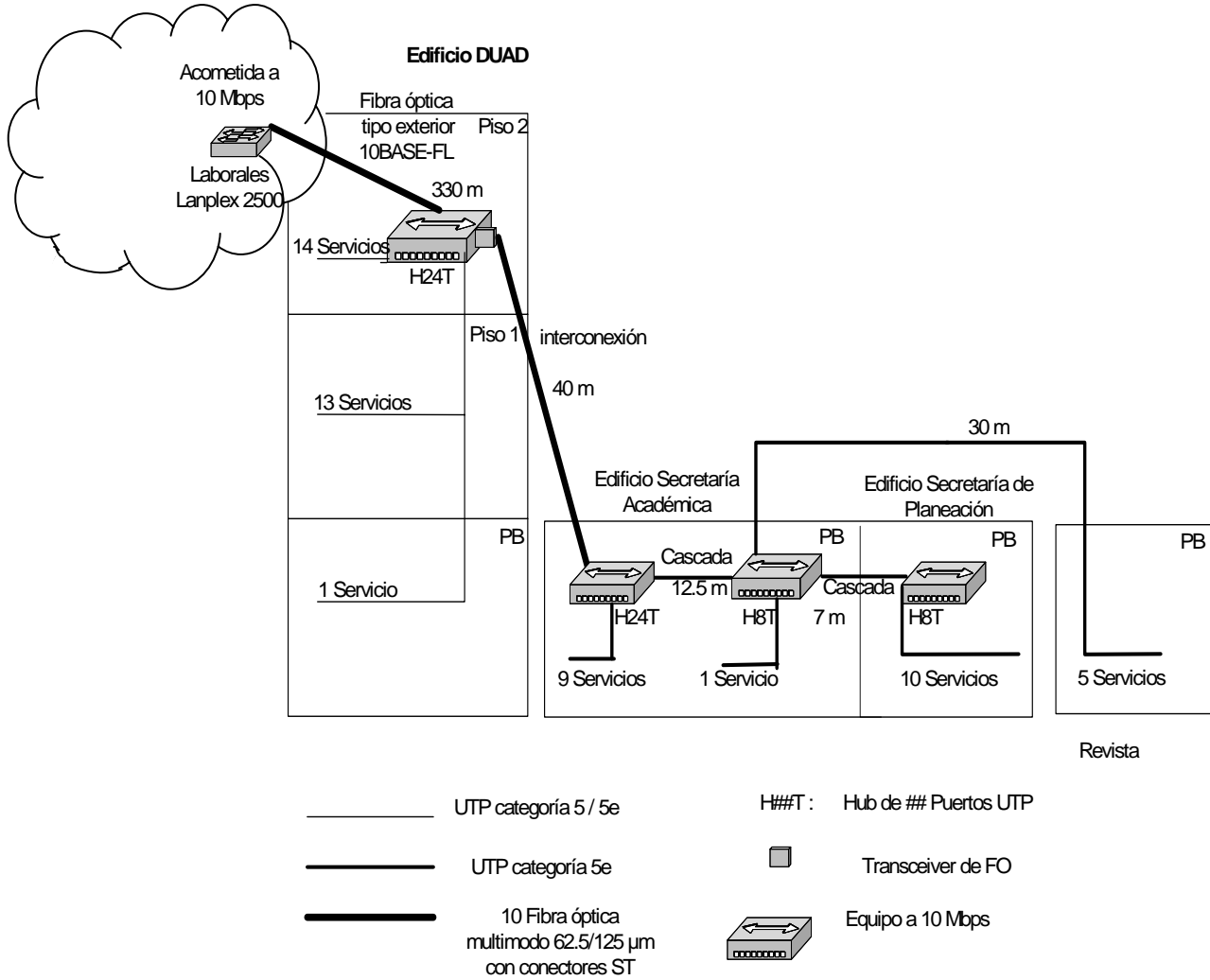


Figura 4.10 Red de cómputo actual de la DUAD y Dependencias adjuntas

En el diagrama anterior se muestra la red de datos de la DUAD. La acometida proveniente del Lanplex 2500 ubicado en el edificio de Laborales se conecta al hub de 24 puertos de la DUAD por medio del módulo interno de fibra óptica de dicho hub, a su vez, a este hub se encuentra conectado un transceiver de UTP a fibra óptica para proveer el servicio a la

Secretaría Académica. El hub de 24 puertos de la Secretaría Académica cuenta con un modulo interno de fibra óptica por el cual recibe el servicio, y mediante cable UTP se conecta en cascada con el hub de 8 puertos de la misma Dependencia. El servicio de la Secretaría de Planeación se provee mediante el cascadeo con cable UTP del hub de la Dependencia con la Secretaría Académica.

Ethernet utiliza CSMA/CD como método de arbitraje lo que conlleva a que ocurran múltiples colisiones. Para este tipo de red se estima un retardo de propagación de 51 microsegundos.

4.4.4 Estadísticas del funcionamiento de la red de datos

El análisis del comportamiento de la red de datos es imprescindible para conocer el estado operacional correspondiente y planear su migración, de ser necesario, antes de impactar a las aplicaciones que hacen uso de ella de manera negativa.

El crecimiento de la red y sus aplicaciones hacen más compleja su administración, de ahí la importancia de conocer el comportamiento de la red de datos para detectar y predecir su funcionamiento.

Análisis del tráfico que circula por la red

El dispositivo al que confluyen todos los segmentos de la red de datos es un hub a una velocidad de transmisión de 10 Mbps. Este dispositivo hace que se divida la velocidad de transmisión entre el número de hosts que concurren a él, es decir, se comparte el ancho de banda por lo que, de acuerdo al Manual de Referencia de Redes de Craig Zacker, cada host tiene asignado realmente 416.67 Kbps. Por lo que la velocidad de operación del host de la Secretaría Académica se reduce entonces, a 208.335 Kbps; considerando que el servicio es proporcionado por el host de la DUAD. Además, tomando en cuenta que a su vez, el host de dicha Secretaría tiene conectado en cascada el hub de la Secretaría de Planeación se reduce a la mitad su velocidad de operación en ésta última dependencia.

Cabe señalar que estamos hablando de kilobits por segundo no de kilobytes por segundo, así entonces, se tiene una velocidad media de 52 KBps, y 26 KBps para los hosts conectados al hub de la Secretaría Académica.

Ethernet trabaja en un modo duplex donde sólo una máquina a la vez puede transmitir información, por lo que se incrementa el número de colisiones en la red.

Las gráficas que muestran el comportamiento de la red se describen a continuación:

Equipo: Laborales en Edificio Posgrado Derecho
 Administrador: TAC-UNAM (+52)56 22 8527 email: tac@redes.unam.mx
 Interfaz: LANplex 2500, manuf: 3Com, Module 3, Ethernet Port 4
 Tipo: ethernetCsmacd (6)
 Velocidad: 10.0 Mbits/s

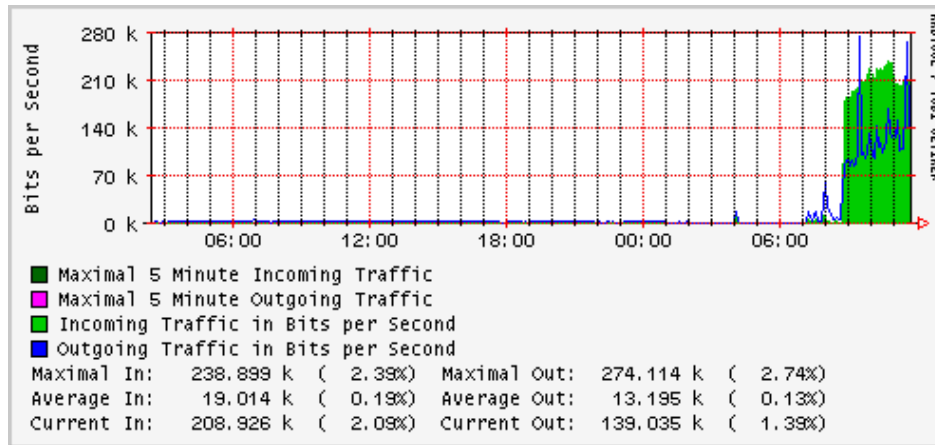


Figura 4.11 Gráfica diaria del tráfico de red

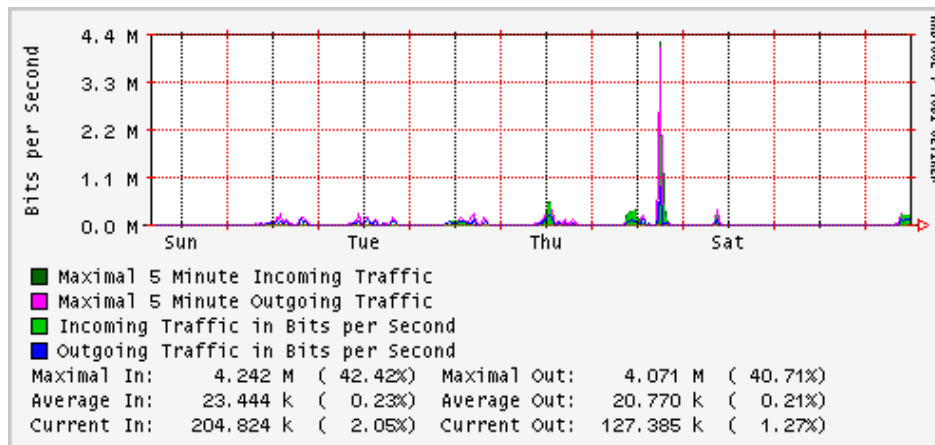


Figura 4.12 Gráfica semanal del tráfico de red

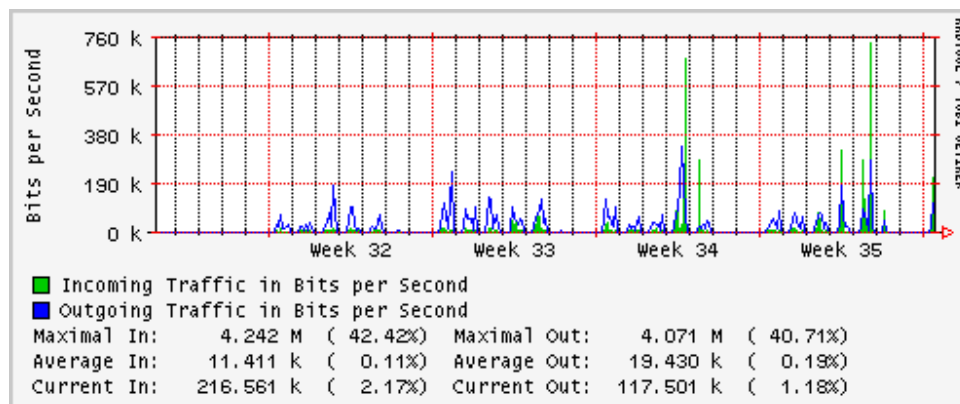


Figura 4.13 Gráfica mensual del tráfico de red

En las gráficas anteriores se observa que el tráfico en la red se mantiene constante la mayor parte del tiempo. Para la gráfica diaria (figura 4.11) es aleatoria la hora y día en que se incrementa dicho tráfico. En la gráfica semanal (figura 4.12) se observa que el día viernes es cuando se da un incremento; y finalmente, en la gráfica mensual (figura 4.13) los datos arrojados indican que en tiempo de reinscripciones es cuando se incrementa dicho tráfico.

Entre los parámetros más importantes para su administración se encuentran: el porcentaje del uso del ancho de banda, el procesamiento del uso del CPU y memoria, si existen errores de frames, colisiones, caracterización de tráfico.

Por la naturaleza del equipo activo con que cuenta la red, sabemos que las colisiones se dan muy a menudo. Dado que es un hub no se esperaría que el umbral fuese rebasado más de lo que muestran las gráficas.

Monitoreo de la red

En la gráfica de porcentaje de uso de red (figura 4.14), se observa que la red no rebasa el umbral del 30% ó 40% recomendado para el funcionamiento adecuado de una red Ethernet. Sin embargo, se observa que la red de datos se satura con las aplicaciones requeridas por la Institución; es decir, con aplicaciones de videoconferencia y transferencia de archivos de gran tamaño. Por lo que se corrobora la migración de la red a Gigabit, dado que la red actual de 10 Mbps es deficiente para la Educación a Distancia.

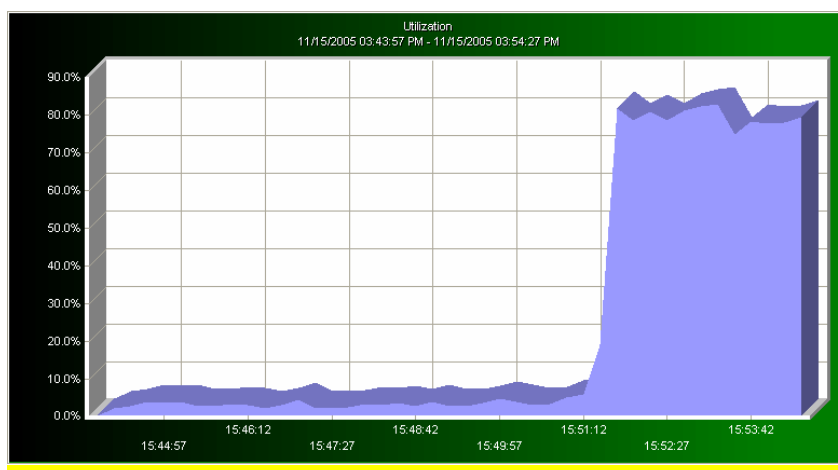


Figura 4.14 Gráfica de porcentaje de uso de la red

4.4.5 Deficiencias encontradas

La falta de planeación de la red aunado a los errores en su instalación provoca el bajo desempeño operacional de la misma. Las deficiencias encontradas en la red de datos de la DUAD se listan a continuación.

- La acometida que llega desde Laborales a la DUAD es mediante un condulet que no cumple en cuanto al radio de curvatura de la fibra óptica.
- La FO que conecta la Secretaría Académica con la DUAD es de tipo interior y no de tipo exterior.
- El gabinete de pared cerrado donde se encuentra el hub de la DUAD no permite la libertad de operación dentro del panel de parcheo tipo regleta 110c.
- No existe estándar alguno en el diseño de la red; sin embargo, se usa canaleta perimetral sin apearse a ninguna norma respecto a las distancias con las líneas de

corriente. Si bien, el cable UTP disminuye la interferencia electromagnética, debido a esta estrecha distancia ocasiona la disminución del rendimiento de la red.

- La red no estandariza el uso único del estándar T568-A o bien, T568-B.
- Los cables no están etiquetados.
- Cabe mencionar que en la instalación no se consideró el ángulo máximo permitido para cambiar de dirección en la instalación del cable.
- El equipo activo con que se cuenta es obsoleto hoy en día y no es administrable.
- No existen dominios de colisión lo que conlleva al aumento del tráfico en la red.
- La red no cuenta en la actualidad con la posibilidad de crecimiento, ya que ha llegado al máximo, e incluso rebasados, el número de los servicios proporcionado por el hub de la DUAD al igual que el perteneciente a la Secretaría de Planeación.
- El cascadeo de los hubs de las diversas secretarías a las cuales se les proporciona el servicio desde el hub de la DUAD, disminuye la velocidad de operación e incrementa el tráfico y número de colisiones en la red.
- Ya se ha mencionado que la red de datos no se apega a ningún estándar por lo que no se garantiza que los cables operen de acuerdo a parámetros de desempeño de normas y estándares.
- El ancho de banda demandado por las aplicaciones de los usuarios no es suficiente.
- La calidad de servicio es deficiente, como ya se ha mencionado en el capítulo 1 la funcionalidad del hub disminuye la eficiencia de la transmisión de datos.
- No existe políticas de administración y procedimientos para la red.

4.5 Propuesta para la red de datos de la DUAD

La instalación de una red implica la toma de decisiones sobre diferentes aspectos como son: técnicos, económicos, relevamiento del equipo con que se cuenta, lugar donde se va a realizar la instalación y tipo de cableado más adecuado, entre otros. Dicha instalación va a formar la infraestructura necesaria y, con base en ello, crear los mecanismos para proteger los recursos fundamentales para la organización: sus recursos humanos, la información y sus sistemas.

Considerando las tendencias de Red UNAM a la actualización de equipo de voz y de datos que soporte tecnologías emergentes VoIP y gigabit respectivamente, además de brindar servicios de acceso inalámbrico; es de suma importancia implantar la infraestructura tecnológica capaz de soportar dichas tecnologías para mantenerse a la vanguardia educacional.

La presente propuesta tiene como objetivo el diseño e implantación de la infraestructura física para una red de área local (LAN) e inalámbrica (Wireless) correspondiente a la División de Universidad Abierta de la Facultad de Derecho (DUAD) que comprende el cableado estructurado y el equipo activo.

4.5.1 Necesidades del usuario

La DUAD al igual que las Instituciones privadas ha enfocado sus esfuerzos hacia la educación a distancia; en donde, sin que el alumno asista a un salón y con base en los principios bajo los que funciona el Sistema Abierto, tome asesorías, realice consultas, comparta discusiones y debates sobre diversos tópicos por medio de los cuartos de conversación (chatroom), programas de mensajería instantánea, foros y grupos de discusión, audio y videoconferencia, mencionados sólo por destacar algunos.

De ahí que la DUAD considere la importancia de reforzar al Sistema Abierto con la educación en línea, primero como un soporte para fortalecer la enseñanza de la División y después como la opción de Sistema de Educación a Distancia; para que junto con el Sistema Abierto y el Sistema Tradicional capten la gran demanda que la carrera de Licenciado en Derecho ha tenido históricamente.

Surge así, la necesidad de migrar la red de datos de la DUAD para proporcionar la base tecnológica capaz de sustentar las tecnologías de información de comunicación para mantenerse a la vanguardia como Institución Educacional, y en la colaboración académica con Instituciones nacionales e internacionales. Además de garantizar la disponibilidad, accesibilidad, confiabilidad, confidencialidad e integridad de la información.

4.5.2 Diseño y planeación de la migración de la red

Conociendo las necesidades de la Institución y el estado actual de la red de datos se inicia el diseño de dicha red. La tecnología que se decidió utilizar por ser la más extensa, por su variedad de componentes y su flexibilidad en los precios es Gigabit Ethernet, considerando que es una tecnología que ha evolucionado a través del tiempo y está en continuo desarrollo. Aunado a su compatibilidad con las tecnologías precedentes que actualmente son utilizadas en gran número de organizaciones.

Para la implantación de la red LAN usaremos una topología tipo estrella física 1000BASE-T, debido a que la red que se va a implantar es entre edificios, la ubicación geográfica es la misma y los usuarios son menos de 1000. Se contempla la reconexión de la fibra óptica de la acometida proveniente de Red-UNAM a la DUAD, al igual que el cascadeo de dicho

switch con los pertenecientes a la Secretaría de Planeación y Secretaría Académica, y a la Revista de la Facultad.

El cable a utilizar será cable UTP categoría 6, ya que este tipo de cable brinda la oportunidad de soportar velocidades de 1000 Mbps y soporta aplicaciones a 1000 Mbps. Todos los componentes de red tales como conectores, cables, jacks y paneles de parcheo deben ser de la misma categoría (figura 4.15). Para terminar con el diseño de la red se debe incluir la documentación del trabajo, la cual, debe contener planos de la ubicación de los equipos y del cableado de red, y la memoria técnica de la misma. Debe documentarse la topología física y lógica del diseño de red.

En cuanto a los dispositivos para mejorar las capacidades de la red se agregan switches 10/100/1000 para reducir la congestión y el tamaño de los dominios de colisión.

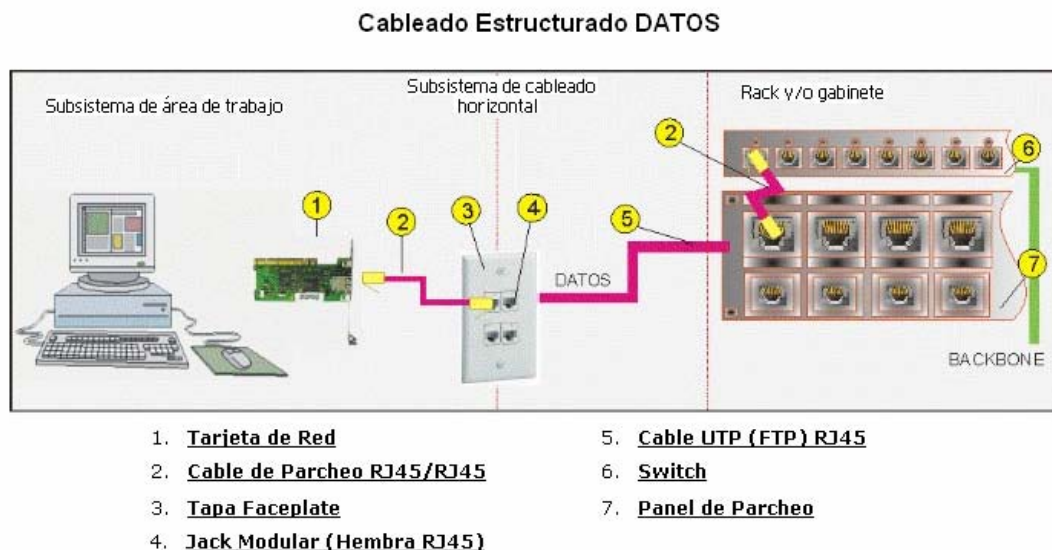


Figura. 4.15 Elementos de una red de datos

Para la parte de la red inalámbrica, ya que se tiene contemplado brindar este servicio a profesores y alumnos alrededor de las oficinas de la Institución, se colocarán dos access point de ondas de radio para brindar conexión inalámbrica fuera de dichas oficinas, refiérase al anexo A para notas técnicas. Estos access point estarán conectados a la red local mediante cable UTP (figura 4.16).

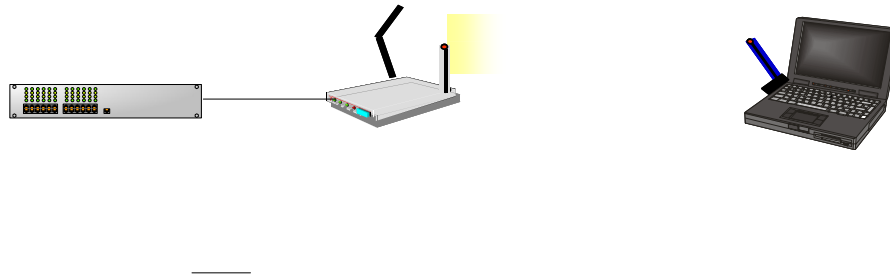


Figura. 4.16 red inalámbrica

El estándar a utilizar es el 802.11g debido a que puede soportar velocidades de hasta 54 Mbps y cuya distancia máxima de cobertura es de 300 m en lugares abiertos. Para incrementar la seguridad dentro de la red inalámbrica y prevenir intrusos, este estándar soporta WPA (Wi-Fi Protected Access), el cual es un protocolo que maneja una clave de red dinámica que cambia continuamente; hace uso del estándar de cifrado avanzado AES (Advanced Encryption Standard), maneja llaves de 128 bits.

Los equipos a utilizar en la propuesta para la red de datos de la DUAD se mencionan en la tabla 4.17.

Switch 10/100/1000

Access po

UTP Categoría 6

Área	Equipo	Descripción
------	--------	-------------

Piso 2 DUAD	Rack	Rack de 19" con panel de parcheo 16 y 48 puertos, barra de contactos con tierra física y organizadores horizontales y verticales.
	Pasivo	Cable y conectores diversos de categoría 6.
		F.O. MM 62.5/125 µm 100BASE-FX, 1000BASE-SX.
	Activo	Tarjeta de red 10/100/1000 Mbps.
		Switch 3com serie 5500G 10/100/1000 20 puertos, con módulo 100BASE-FX.
		Switch 3com serie 5500G 20 10/100/1000 4 SFP.
		Computadora personal. Refiérase a la tabla 4.7.
		Servidor de datos 1 Proliant ML150 G2 15900RU INTEL XEON X3.2-2MB/800MHZ 1 PROCESSOR 370/3380 G4 HP 2 Memorias RAM ML 150 GL 1024 MB 1 Discos Duros 72.8 GB 10K RPM 1 Tarjeta Raid 150G2 adapter PCI SCSI RAID CONTROLLER ACOM 78 1 Unidad óptica HP DVD+R/RW 16X HALF HEIGHT.
		Servidor Web. 1 Proliant ML150 G2 15900RU INTEL XEON X3.2-2MB/800MHZ 1 PROCESSOR 370/3380 G4 HP 2 Memorias RAM ML 150 GL 1024 MB 2 Discos Duros 72.8 GB 10K RPM 1 Tarjeta Raid 150G2 adapter PCI SCSI RAID CONTROLLER ACOM 78 1 Unidad óptica HP DVD+R/RW 16X HALF HEIGHT.
		Servidor de archivos. Pentium 4HT, 3.2 GHz, 1 GB RAM, 160 GB HD.
		Servidor de impresión. ImageRUNNER 2870 Canon con tarjeta de impresión en red.
RADIUS		Pentium 4HT 3.4 GHz, 80 GB, 1 GB RAM.
Fireware	Pentium 4HT 3.4 GHz, 80 GB, 1 GB RAM.	
Inalámbrico	Access Point 3com 8750 802.11a/g con 8 dbi de ganancia.	
Piso 1 DUAD	Rack	Rack de 19" con panel de parcheo 24 puertos, barra de contactos con tierra física y organizadores horizontales y verticales.
	Pasivo	Cable y conectores diversos de categoría 6.
		F.O. MM 62.5/125 µm 1000BASE-SX.
	Activo	Tarjeta de red 10/100/1000 Mbps.
		Switch 3com serie 5500G 20 10/100/1000 4 SFP.
Computadora personal. Refiérase a la tabla 4.7.		
Inalámbrico	Access Point 3com 8750 802.11a/g con 8 dbi de ganancia.	
PB DUAD	Pasivo	F.O. MM 62.5/125 µm 1000BASE-SX.
	Activo	Tarjeta de red 10/100/1000 Mbps.
		Computadora personal. Refiérase a la tabla 4.7.

Tabla 4.17 Equipos propuestos para la red de datos de la DUAD

Secretaría Académica	Rack	Rack de 19" con panel de parcheo 24 puertos, barra de contactos con tierra física y organizadores horizontales y verticales.
	Activo	Switch 3com serie 5500G 20 10/100/1000 4 SFP.
Revista de la Facultad de Derecho	Rack	Rack de 19" con panel de parcheo 24 puertos, barra de contactos con tierra física y organizadores horizontales y verticales.
	Activo	Switch 3com serie 5500G 20 10/100/1000 4 SFP.

Tabla 4.17 Equipos propuestos para la red de datos de la DUAD

La propuesta para la red de datos de la DUAD conforme a normas de Cableado Estructurado se muestra en la figura 4.18.

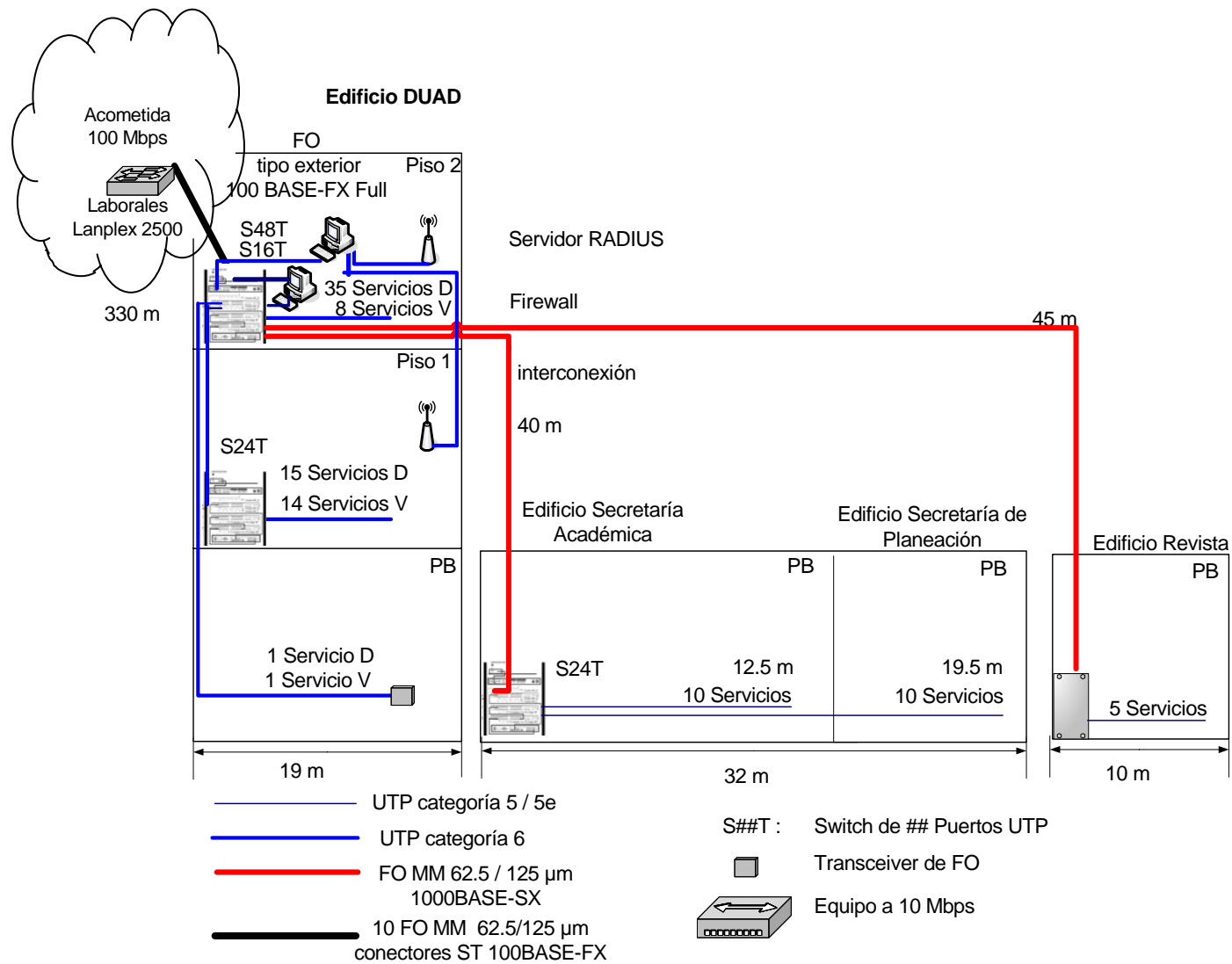


Figura 4.18 Propuesta de red de datos para la DUAD y las Dependencias adjuntas

La conectorización en el rack del piso 2 de la DUAD se muestra en la figura 4.19.

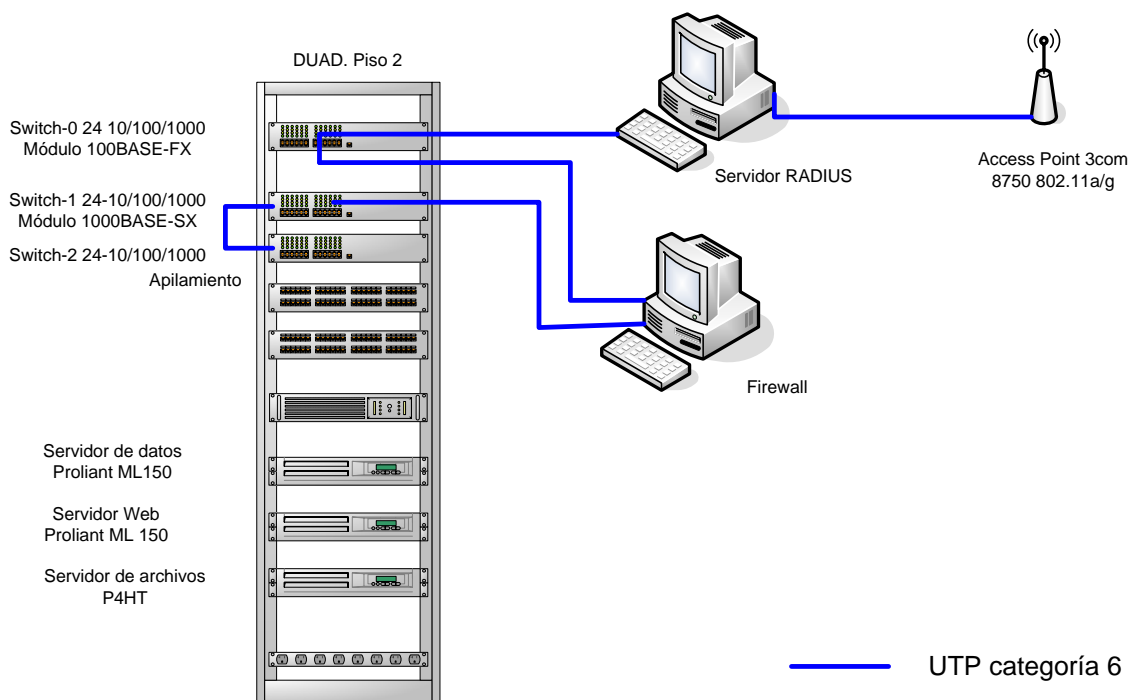


Figura 4.19 Conexión del rack del segundo piso de la DUAD

El switch 0 del segundo piso de la DUAD recibe la acometida proveniente de DGSCA-Laborales, como ya se comentó, a su vez, distribuye la señal a la red LAN e inalámbrica. El tráfico hacia la red Wireless se filtra a través del servidor Radius, y el correspondiente a la red LAN mediante el firewall. El switch 1 y 2 se apilan mediante cable UTP categoría 6.

El switch 3 del primer piso de la DUAD se apila al switch 2 mediante cable UTP categoría 6. El backbone distribuido de la DUAD está constituido por los switch correspondientes al primero y segundo piso; a su vez, hacia la planta baja de dicho edificio se forma un backbone colapsado con el switch 1, debido al único servicio de voz y datos requerido para dicha planta.

El switch de la Secretaría Académica al igual que el correspondiente a la Revista de la Facultad de Derecho, se cascadea al switch 1 mediante fibra óptica bajo el estándar 1000BASE-SX.

4.5.3 Áreas, edificios y pisos de la División de Universidad Abierta de la Facultad de Derecho

Como ya se ha mencionado, la red a implantarse es una red de área local especificada en el estándar del IEEE 802.3z, 1000BASE-T; la cual se refiere a una transmisión sobre cable UTP categoría 6, para nuestro caso práctico, a una velocidad de 1000 Mbps implantada sobre una topología tipo estrella física y bus lógica.

Es importante señalar que el equipo a seleccionar para la red debe soportar las tecnologías emergentes, como VozIP entre otras, conforme a los lineamientos emitidos por la DGSCA. Para cumplir con el objetivo de la presente propuesta se mencionan a continuación los componentes necesarios y la manera en que deben ser instalados cada uno de los bienes y servicios bajo estándares y conforme a los lineamientos de la DGSCA.

Para permitir la conexión de los equipos de cómputo localizados en las diversas áreas de trabajo a la red de la Institución, se instalarán 73 nodos de cableado estructurado mediante cable UTP, categoría 6, distribuidos en las diferentes áreas de trabajo de acuerdo a normas ISO/IEC 11801 y EIA/TIA-T568; al igual que los otros componentes requeridos para su instalación como lo son: rosetas de pared, jacks, organizadores y paneles de parcheo serán categoría 6. Los cordones de parcheo serán de fábrica.

Para la conexión a la Red-UNAM se considera la conectorización de la fibra óptica proveniente de Laborales a la Dependencia conforme el estándar 100BASE-FX.

El acceso de los usuarios fijos a la Red UNAM estará proporcionada por el equipo activo 3com de capa 3. El acceso de los usuarios móviles a la red de la UNAM se hace mediante la instalación del equipo activo inalámbrico de la marca 3com con 8 dbi de ganancia por lo que se asegura la cobertura de los 100 m debido a la construcción de los edificios.

Se ha citado anteriormente, la implantación de la red de cableado estructurado considera un total de 73 conexiones distribuidas en diferentes áreas de trabajo de la Dependencia, de las cuales 22 serán de voz.

El edificio de la DUAD está conformada por tres niveles de los cuales, en la planta baja únicamente existe un servicio de voz y uno de datos correspondientes a la librería de la Facultad. De los servicios de datos, se asignan 15 servicios para el primer nivel y el resto se instalarán en el segundo nivel. Se instalarán 14 y 8 servicios de voz para el primer y segundo nivel respectivamente.

En el primer nivel del edificio se ubican las siguientes áreas de trabajo: Coordinación Académica, Jefatura, Proyectos Especiales, Exámenes, Diseño, Pedagogía, y Centros Asociados (figura 4.20).

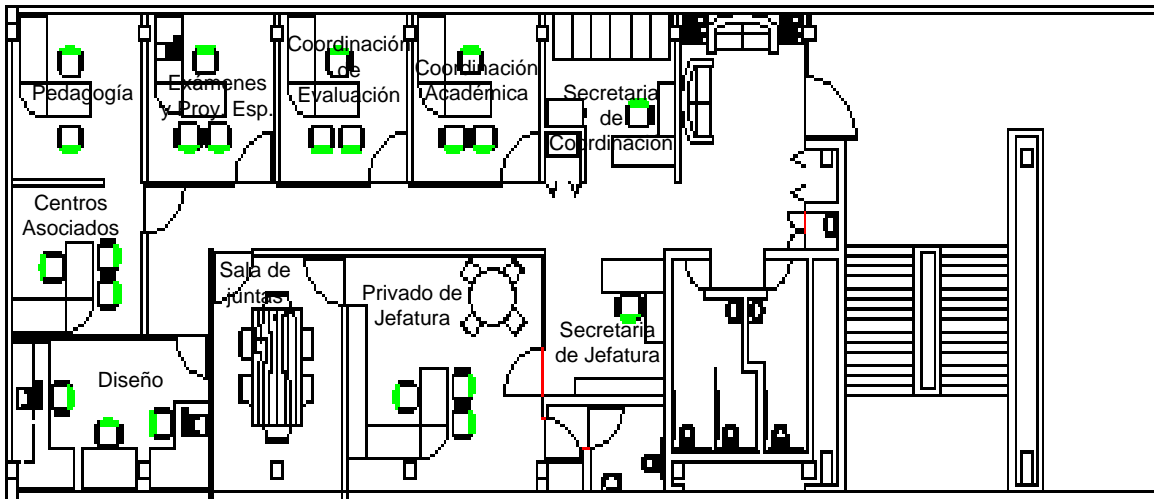


Figura 4.20 Primer nivel de la DUAD

En el segundo nivel se encuentran ubicadas las áreas: Cuarto de Equipo, Cómputo, Servicios Escolares y Servicio Social, Coordinación Institucional, y Coordinación Administrativa (figura 4.21).

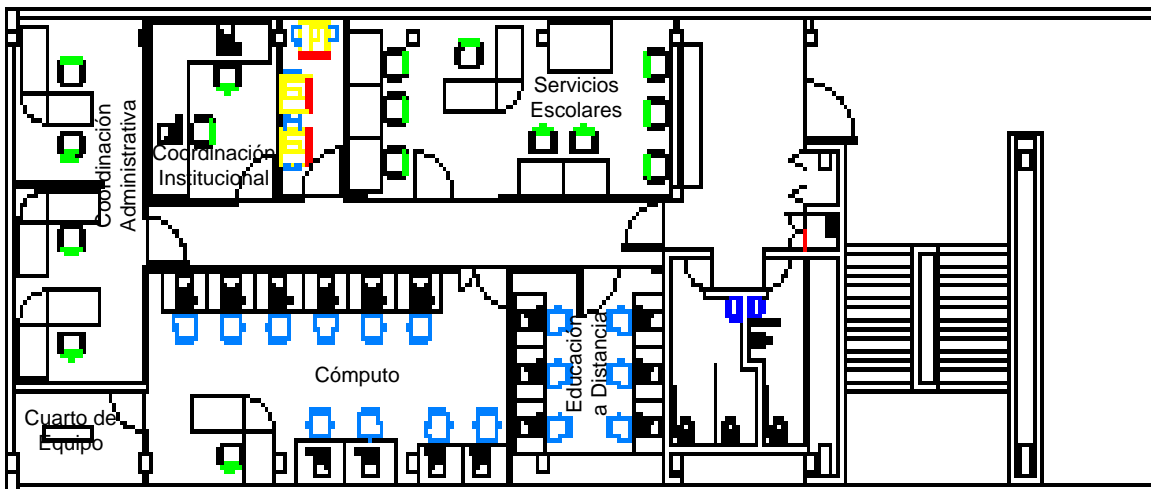


Figura 4.21 Segundo nivel de la DUAD

4.5.4 Especificaciones de los elementos activos

Los elementos activos son aquellos que cuentan con algún tipo de circuito electrónico, y por lo tanto, necesitan de alimentación electrónica.

Tarjeta de red. Este dispositivo soportar velocidades de 10, 100 y 1000 Mbps. Esta característica permite que la red ofrezca un servicio flexible a diferentes velocidades y minimiza costos; los cuales se generarían por el cambio de tarjetas a una velocidad específica. Para la implantación del presente proyecto utilizaremos tarjetas de red 3com 10/100/1000 con puerto RJ45 para cable UTP debido a su gran reconocimiento en el mercado. Cabe mencionar que por su característica de autonegociación se configura la NIC de forma transparente para adaptarse a la velocidad de conexión del switch: 10, 100 ó 1000 Mbps. La decisión se fundamenta en el prestigio de la marca en el mercado, lo que respalda su efectividad y garantiza su operabilidad.

Switch. Este dispositivo al igual que la tarjeta, es recomendable que tenga flexibilidad para soportar velocidades de 10, 100 y 1000 Mbps para facilitar la migración de la red y minimizar costos a futuro. Otro aspecto que hay que observar es si cuenta con módulos de expansión para poder implementar otros soportes de Gigabit como 1000BASE-SX y 1000BASE-LX en la misma plataforma. Además, es importante saber si tiene la capacidad de apilamiento con otro switch del mismo modelo para incrementar el número de nodos, y facilitar el funcionamiento de ambos como uno solo.

Para la implantación de la red local utilizaremos switches de la marca 3com. Para la acometida al edificio de la DUAD, switch DUAD 0, utilizaremos el switch de la serie 5500G 10/100/1000 de 20 puertos con un módulo 100BASE-FX. Para el edificio de la Revista de la Facultad, la Secretaría Académica, switch 1, 2 y 3 de la DUAD serán 3com serie 5500G de 20 puertos 10/100/1000 con 4 puertos a Gigabit basados en SFP. Lo anterior se basa en el número de servicios que soportan dichas áreas y aunado a que el ancho de banda será administrado desde el switch DUAD 1; en el caso de la acometida de la red, antes de distribuirse la señal en el switch DUAD 1 se filtra el tráfico mediante un firewall. La decisión se basa en el rendimiento, posibilidad de la administración de los dispositivos, gran disponibilidad en el mercado, la funcionalidad que ofrece sobre la capa 2 y 3 del modelo OSI, por mencionar algunas.

Access Point. Las características de este dispositivo son de suma importancia para los servicios requeridos por los usuarios. Es imprescindible considerar sus características que debe cumplir para ofrecer un servicio confiable y disponible. Este dispositivo debe permitir

a los usuarios conectarse con tarjetas de red inalámbricas bajo el estándar 802.11b y 802.11g a una velocidad de 54 Mbps.

Para la implantación de la red inalámbrica utilizaremos access points 8750 de la marca 3com. Este dispositivo soporta las frecuencias de 5 GHz y 2.4 GHz, lo que nos permite ampliar el número de usuarios.

La elección del dispositivo se fundamenta en sus funciones integradas de seguridad, manejabilidad, y confiabilidad. Aunado a la fácil administración y la disponibilidad de diversas tareas como autenticación y la encriptación, entre otras tantas, asegura la privacidad de las transmisiones en la red inalámbrica.

4.5.5 Especificaciones de los elementos pasivos

Los elementos pasivos son aquellos que no contienen ningún tipo de circuito electrónico para su funcionamiento.

Cable. Para la elección del cable es necesario tomar en cuenta las condiciones dónde se va a instalar, la humedad, fuentes electromagnéticas, etc; así como, las distancias que hay que cubrir, las velocidades de transmisión de datos y el ancho de banda que se va a necesitar. Con el cable de UTP se cubren estos requisitos. En nuestro caso práctico se utilizará cable UTP categoría 6, 24 AWG, ya que soporta velocidades de 1 Gbps, con un ancho de banda de 250 MHz.

Fibra óptica. En cuanto a la fibra óptica es recomendable usarla si se necesitan cubrir distancias mayores a 100 m. Considerando que la distancia es de 330 m del edificio DUAD a Laborales, se reconectorizará la actual fibra óptica utilizada. El tipo de fibra es multimodo 65/125 micras 100BASE-FX para laborales y 1000BASE-SX para las Dependencias adjuntas.

Cordones de parcheo. Éstos cordones deberán ser de fábrica con cables de 4 pares trenzados calibre 24 AWG, aislados, categoría 6, con 2 conectores tipo plug RJ-45 de 8 posiciones, uno a cada extremo, de alta calidad y longitud requerida de 2 y 3 m, con cable multifilar para mayor flexibilidad y con liberadores de tensión.

Rosetas. Actualmente existen varios tipos de rosetas con sus respectivos conectores, las cuales se deben seleccionar de acuerdo a los estándares señalados dentro de cableado estructurados y las más apropiadas para el lugar.

Tomas de telecomunicaciones. Conocidas como faceplates son utilizadas para conectores RJ-45 y cable UTP, ambos de categoría 6. Las tomas se componen de 2 y 4 espacios identificados por iconos correspondientes a los servicios de voz y datos.

Panel de parcheo. Este dispositivo de 19” de ancho es modular con capacidad de 16 y 24 puertos, con conectores RJ-45 categoría 6, compatible con el cable UTP categoría 6, y habrá tantos conectores como rosetas instaladas; es necesario prever la posible ampliación de nodos y tener disponibles conexiones libres para un crecimiento en equipos de red.

Conectores. Estos deben de cumplir la misma categoría del cable utilizado para garantizar el buen rendimiento de la red, se usarán conectores categoría 6 one click UTP, con un desempeño mayor a la frecuencia 250 MHz para el presente proyecto.

Canaletas. Estas van a contener y conducir los cables hasta nuestras conexiones y rosetas; por lo tanto, deben de ser fijadas a la pared y no deben de ser saturadas a más del 40% de su capacidad de cables para poder prever futuras ampliaciones de nodos.

Rack de telecomunicaciones. Este rack de 19” se empleará para soportar el equipo activo, los paneles de parcheo, barra de contactos y organizadores de cable horizontal y vertical.

4.5.6 Especificaciones del cableado

Las normas que se deben contemplar a la hora de trabajar con los cables son:

- Los cables no debes ser sometidos a estiramientos mayores a 10 Kg.
- Los cables no se deben doblarse en ángulos menores a 90°.
- Los cables deben ser etiquetados en cada uno de sus extremos.
- Los cables deben ser instalados de acuerdo a sus características de velocidad, distancia, interferencia, etcétera.
- Para el caso de cable UTP, manejar un solo tipo de código de colores (T568-A ó T568-B).
- La categoría del cable UTP debe soportar velocidades de Gigabits por segundo (Categoría 6 en la implantación de la presente propuesta).

Básicamente se deben de cumplir con las normas de cableado estructurado EIA/TIA 568-A y EIA/TIA 570.

La especificación del cableado contempla la descripción de la conectorización de los elementos requeridos para alcanzar el objetivo y las metas del presente proyecto.

A continuación mencionamos las especificaciones para su implantación.

- El cableado de la roseta de pared ubicada en el área de trabajo requerida hacia el panel de parcheo en el closet de comunicaciones se realiza con cable UTP categoría 6 y bajo el estándar T568-B.
- La longitud máxima del segmento del cableado horizontal de la roseta de pared, ubicada en el área de trabajo, hacia el panel de parcheo en el closet de telecomunicaciones será de 90 m.
- Todos los cables, de cableado horizontal y cordones de parcheo, deberán ser etiquetados de acuerdo a un código que debe indicar: el área a la que corresponden, el número de panel de parcheo o switch en que se rematan o toma de servicio, de colores para su fácil identificación del área correspondiente.
- La asignación de pines en las faceplates estará de acuerdo al estándar T568-B.
- En el rack de distribución se instalarán paneles de parcheo de 19” de ancho y en la cara frontal deberán ser colocadas las etiquetas de identificación.
- Los paneles de parcheo deberán considerar administradores horizontales y verticales de cables, guías y soporte de los cables de parcheo.
- Las conexiones o puentes entre los conectores de los servicios de datos se efectuarán con cordones de parcheo de fábrica.
- En el rack de distribución se instalará una barra de 6 multicontactos.
- Todos los componentes del Sistema de Cableado Estructurado: cable horizontal, faceplates, cordones de parcheo, sistema de distribución de bloques terminales, conectores tipo plugs RJ-45 y jacks RJ-45, deberán ser compatibles entre sí.
- Cuando se perforen las paredes o la estructura de la Dependencia, sus propiedades deberán ser suplidas.
- La canaleta perimetral deberá ser fijada cada 1.5 m aún cuando sea autoadherible.
- El número de cables conducidos por la canaleta no deberá rebasar el 40% de su capacidad.
- En el cuarto de equipo se deberá instalar el rack para soportar el equipo activo de comunicación, panel de parcheo, barra de contactos y los organizadores de cable horizontal y vertical.
- Deberá entregarse la memoria técnica de la red y deberá incluir: los planos de la red donde se indique la ubicación y tipo de los servicios, el esquemático del panel de parcheo, configuración de los equipos activos, diccionario de términos.

La memoria técnica deberá contener las pruebas de certificación del cableado mediante pruebas técnicas con instrumentos de medición.

4.5.7 Especificación de los puntos de acceso

Para la red inalámbrica se consideran dos puntos de acceso (PA) 802.11g debido a su capacidad de aplicar una modulación compatible con el estándar 802.11b. La velocidad máxima de transferencia del access point será 54 Mbps. Con base en la distancia de la estación al access point, las condiciones y parámetros que afectan a dicha comunicación, se establece un radio de cobertura de 100 m. Es importante señalar la disminución de la velocidad conforme se incrementa la distancia y los elementos entre ambos.

La topología para la red inalámbrica es de tipo infraestructura, debido a que el nodo central sirve para enlazar todos los nodos y para encaminar las tramas hacia una red convencional o hacia otras redes distintas. Todos los nodos deben estar dentro de la zona de cobertura del access point para establecer la comunicación.

Cada usuario puede conectarse a Internet a una velocidad razonable. Lo anterior es en teoría ya que el estándar 802.11g no dispone de QoS, es decir, la posibilidad de garantizar un ancho de banda determinado, por lo que no se puede garantizar que un usuario no absorba todo el ancho de banda dejando al resto de usuarios sin acceso o con mínimo ancho de banda. Para resolver este problema se instalará un software de gestión de comunicaciones: RADIUS. Este software administrará la red como si se tratase de un pequeño ISP.

Para definir el diseño de la red inalámbrica consideramos que las necesidades de movilidad están aunadas a la accesibilidad del Internet, sin tener recursos compartidos entre los participantes, y tomando en cuenta los puntos donde hay más concentración de máquinas a causa de las actividades académicas de la Institución, se decidió instalar un PA en el primer y segundo piso del edificio B del anexo de la Facultad de Derecho por ser el lugar más céntrico (figura 4.22). Debe mencionarse la importancia de la seguridad rigurosa que debe mantener la red inalámbrica para proteger la información de la Institución, que si bien, es el segundo activo más importante.

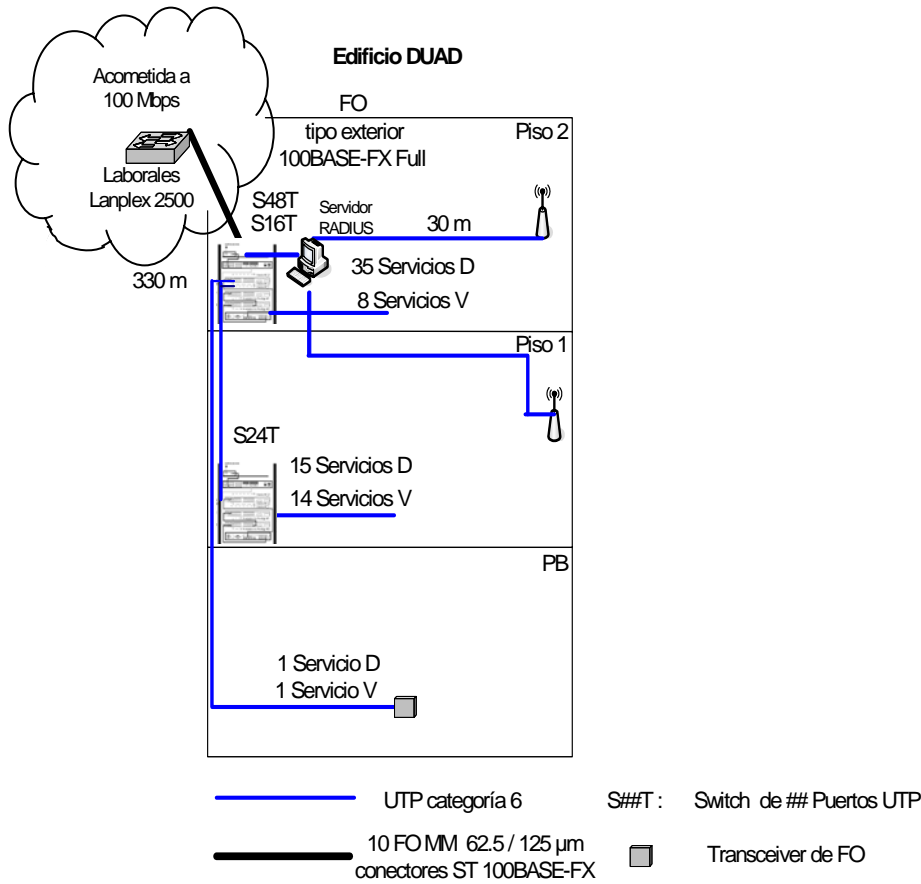


Figura 4.22 Red inalámbrica de la DUAD

La red inalámbrica de la DUAD sustentada por el servidor RADIUS, se conecta al switch 1 mediante cable UTP para aislar dominios de colisión y disminuir el tráfico en las distintas redes LAN. Mediante el firewall instalado entre el switch 0 y el switch 1 de la DUAD se aumenta la seguridad en la red LAN de la Dependencia antes mencionada.

La infraestructura básica de comunicaciones a implantarse es una red gigabit Ethernet a la que conectaremos PA 802.11g.

El firewall será el encargado de filtrar todo el tráfico de la red, permitiendo el acceso a los paquetes autorizados. Considerando que se utilizará Linux como sistema operativo, se recurrirá al uso de iptables para dicho fin, no sin dejar de mencionar su robustez, alto rendimiento y alta disponibilidad en el mercado.

La seguridad dentro de las comunicaciones es un aspecto crítico por lo que a continuación indicamos las buenas prácticas a implantarse para asegurar la transmisión confiable, íntegra y disponible de información.

Se mencionan las políticas de red para la red inalámbrica de la DUAD:

1. La red inalámbrica deberá tener activado el WPA con una clave de cifrado de longitud de más de 20 caracteres.
2. La red deberá mantener desactivado el DHCP, y la asignación de las direcciones IP se deberá asignar manualmente a las direcciones MAC conocidas con base al ACL.
3. Se deberá cambiar el SSID y modificar su intervalo de difusión.
4. Inhabilitar la emisión de broadcast del SSID.
5. Dado que la seguridad dentro de las comunicaciones inalámbricas es un aspecto crítico, se usará VPN.
6. Se usará un switch convencional con un punto de acceso. Se conectará al switch un ordenador que será el encargado de realizar la gestión de todo el sistema, y debe ser lo suficiente para instalar el software del servidor RADIUS.
7. Se deberá aislar la red inalámbrica de nuestra red convencional.
8. Se deberá instalar un firewall que filtre el tráfico entre los dos segmentos de red.

4.5.8 Servidores de red

Un servidor es una computadora normalmente de alta capacidad que proporciona diversos recursos a la red. Un servidor típico contiene varios discos duros, una unidad de respaldo en cinta y una unidad de CD-ROM. También permite a los empleados de una compañía compartir recursos como impresoras, máquinas de fax, módems, correo electrónico y conexiones a Internet. A menudo se utilizan servidores para almacenar información de bases de datos, archivos y copias de seguridad de archivos. Las computadoras conectadas al servidor se conocen como “clientes”.

A continuación presentaremos los servidores a utilizar.

Servidor de Archivos

Los servidores de archivos proporcionan y administran el acceso a archivos. Con el servidor de archivos se puede utilizar espacio del disco en este equipo para almacenar, administrar y compartir información, como archivos y aplicaciones de acceso a través de red.

Los servidores de red utilizan las asignaciones de disco en volúmenes con formato de sistema de archivos NTFS para supervisar y limitar la cantidad de espacio en disco disponible para los usuarios individuales. También puede especificar si desea registrar un suceso cuando un usuario supere el límite de espacio en disco especificado o cuando supere el nivel de advertencia de espacio en disco especificado (es decir, el punto en el que un usuario está próximo a su límite de cuota). Utilizan los servicios de Index Service para buscar información de forma rápida y segura, ya sea localmente o en la red.

Para este servidor de archivos proponemos un equipo con un procesador P4 a 3.2 GHz. tecnología HT, 1 GB de memoria RAM y 160 GB en disco duro. Dado que el número de usuarios no será mayor a 20 personas y el tipo de información que se va a almacenar es del tipo de archivos de Word, Excel, Access, documentos PDF's y archivos de multimedia en su mayoría.

Servidor de Impresión

El servidor de impresión es una computadora de aplicación específica que gestiona las impresoras y solicitudes de servicios de impresión; permite que múltiples usuarios compartan una impresora en red.

Para servidor de impresión se tienen dos propuestas:

La primera es colocar una computadora como servidor de impresión y mediante esta administrar y llevar el control de todas las impresiones de las diferentes áreas. El hacer esto conlleva a adquirir una computadora de buenas características para poder soportar la cantidad de trabajos enviados a imprimir.

La segunda es adquirir una impresora, la cual ya contiene un servidor de impresión integrado; esto ayuda a centralizar el trabajo de impresión por área y así llevar un mejor control de impresiones. Este servidor de impresión tiene la opción de consultar su estado

mediante el navegador de internet, también se puede restringir su uso, tiene las opciones de copiado y de escáner.

El modelo propuesto es el imageRUNNER 2870 de Canon, el cual cuenta con una memoria RAM Estándar de 256 MB y un Disco Duro 20 GB y soporta Windows 98 / Me / 2000 / XP / NT 4.0 / Server 2003 / Macintosh OS 8.0 ó posterior (PPD) Solaris 1.1x, 2.5x o posterior, Novell Netware v3.2, 4.1, 4.11, 4.2, 5, 5.1, 6, 6.5, (IPX/SPX), para mayor información de notas técnicas refiérase al anexo B.

Servidor de Bases de Datos

El servidor de bases de datos se basa en una estructura de datos integrada y centralizada, eliminando así, los problemas de redundancia. Este servidor, garantiza la integridad, seguridad, confidencialidad y disponibilidad de la información.

Para este servidor proponemos el modelo de Hewlett Packard ML150 G2 15900RU Intel Xeon X3.2-2MB con bus de 800 MHZ, con procesador 370/3380 G4, 2 GB de RAM, 72.8 GB HD 10K RPM, con tarjeta Raid 150G2 adapter PCI SCSI Raid Controller Acom 78, con unidad óptica HP DVD+R/RW 16X Half Height, para mayor información de notas técnicas refiérase al anexo C.

Servidor Web

El servidor web aloja páginas en formato HTML, imágenes, sonido, y más aún, aplicaciones tipo web. Debido a su gran concurrencia de usuarios, la disponibilidad, rapidez y confiabilidad con que se requiere la información solicitada, se propone para este servidor un modelo de Hewlett Packard ML150 G2 15900RU Intel Xeon X3.2-2MB con bus de 800 MHZ, con procesador 370/3380 G4, 2 GB de RAM, 145.6 GB HD 10K RPM, con tarjeta Raid 150G2 adapter PCI SCSI Raid Controller Acom 78, con unidad óptica HP DVD+R/RW 16X Half Height, para mayor información de notas técnicas refiérase al anexo C.

4.5.9 Sistemas operativos de red para servidor y clientes

Actualmente existen varios sistemas operativos de red, cada uno procede de diferentes compañías, a lo cual cada uno tiene diferentes características. Para decidir cuál de ellos es el que más conviene a las necesidades presentes y futuras del Sistema de Universidad Abierta de Derecho, se debe considerar cuál brinda mayor seguridad dentro de la red, la

cantidad de equipos a los que se les dará servicio, que sea capaz de soportar múltiples procesos, fácil de instalar y administrar, que sea económico.

Sistemas operativos para clientes

Para los usuarios de la red es necesario instalar un sistema operativo que sea sencillo de usar y amigable para el usuario; además, debe proporcionar seguridad tanto para el usuario como para el administrador de la red.

El sistema operativo de los clientes será XP y Windows 2000, según sea el caso, ya que la mayoría de los equipos ya cuenta con un sistema operativo basado en Windows; por ejemplo, Windows Me, Windows 2000 y Windows XP.

Sistemas operativos para servidor

El software de servidor de archivos permite a los usuarios en otras máquinas, y a los equipos clientes, poder compartir los datos y periféricos del servidor incluyendo impresoras, trazadores y directorios.

Así entonces, se seleccionará Windows 2003 Server, ya que muestra mayores ventajas a sus antecesores. La única desventaja que podemos observar es el precio.

Servidor Web y de Bases de Datos

Con base a la información de la tabla 1.28 y 1.9 del capítulo 1, decidimos seguir utilizando Linux como sistema operativo para el Servidor de Web y de Bases de Datos. Debido a su seguridad y su costo.

4.6 Análisis de la propuesta

Estudio de factibilidad para la red LAN

Factibilidad técnica. Los dispositivos físicos y lógicos están disponibles en el mercado y su reconocimiento como marcas competitivas respaldan su funcionamiento; debido a ello, el proyecto es técnicamente viable. Cabe aclarar que se cuenta con acceso a Internet mediante un ancho de banda actual de 10 Mbps proporcionada por la DGSCA mediante fibra óptica. El uso de la fibra óptica con base en el estándar 100BASE-FX asegura su vida por un largo tiempo.

Factibilidad económica. Es una cuestión de fundamental importancia que está directamente relacionada con el diseño elegido y responde a la relación costo – beneficio. Sin embargo, los productos seleccionados son de marcas reconocidas que garantizan su existencia en el mercado a largo plazo, por lo que no se corre el riesgo de volverse obsoleto a corto plazo y la reinversión en los mismos.

Factibilidad operacional. La administración e instalación de la red estará a cargo de ingenieros altamente capacitados para atender cualquier inconveniente técnico respecto de la misma que pudiera surgir. La certificación de la infraestructura a instalarse es emitida por el fabricante de los componentes del cableado estructurado, y proporciona la seguridad de su buen funcionamiento a largo plazo.

Cabe mencionarse que la red es escalable y flexible, por lo que garantiza su crecimiento y no es necesario rediseñarla para incorporar nuevas tecnologías.

La disponibilidad y rendimiento de la red se garantiza con la implantación de la infraestructura a gigabit. Se garantiza la seguridad y confiabilidad de la información que se transmite por la red, al igual que una fácil administración de la misma.

Enlace inalámbrico 802.11g

Ventajas. Los enlaces son proporcionados por la Universidad por lo que no se realiza pago alguno mensual por concepto de tráfico y/o derecho de línea. Proporciona a los usuarios la movilidad para acceder a diversas aplicaciones. El access point elegido permite la conexión con tarjetas inalámbricas 802.11b y 802.11g, y soporta frecuencias de 2.4 GHz y 5 GHz.

Desventajas. Posee solo dos nodos por lo que en el peor de los casos, si ambos dejan de funcionar, no hay forma de mantener la comunicación mientras se reestablece el enlace. Además de su alto costo de inversión inicial. La velocidad de transmisión es baja

comparada con la red tradicional, por lo que el uso de las aplicaciones está en función de dicha velocidad. La recepción de la señal está en función de las características de los edificios, lo que podría reducir el área de cobertura efectiva. La frecuencia del estándar 802.11g es usada por muchos dispositivos que usan frecuencia de radio, lo que conlleva a interferencias con la señal.

La propuesta que se consideró está basada en estándares, lineamientos, y avalada por la certificación al desempeño de la red de datos por un integrador externo. Cabe mencionar que el integrador de sistemas de transporte de información cuenta con todos los requisitos expuestos por la DGSCA. Sin embargo, se consideraron otras propuestas al plantear su diseño e implantación dentro de la UNAM. La comparativa entre las propuestas se describe a continuación.

a. Propuesta A

La instalación de una infraestructura que soporte 1000 Mbps bajo el estándar Gigabit Ethernet, ISO/IEC 11801 y EIA/TIA568A, con cable UTP categoría 5e. Instalación de ducto ahogado para los servicios al área de trabajo. Y de ser necesario, por la ausencia de tablaroca en los muros, el uso de canaleta perimetral. Certificación de la correcta operación de los elementos del cableado estructurado proporcionada por el fabricante por un periodo de 15 años, y garantía por un año de la instalación proporcionada por el Integrador de Sistemas de Transporte de Información.

Equipo activo para la red LAN. Switch 24 10/100/1000, 4 T/SFP LAN Base Image, Switch 48 10/100/1000T + 4 SFP Standard Image.

Equipo activo inalámbrico. Access point/Bridge/Router TRENDNet TEW-212APBO para exteriores con antena de 10 dbi, estándar 802.11b.

b. Propuesta B

La instalación de la infraestructura física a una velocidad de 1000 Mbps bajo el estándar Gigabit Ethernet, ISO/IEC 11801 y EIA/TIA568A, mediante canaleta perimetral con cable UTP categoría 5e. Esta oferta incluye la certificación de la correcta operación de los elementos del cableado estructurado proporcionada por el fabricante por un periodo de 15 años, y garantía por un año de la instalación proporcionada por el Integrador de Sistemas de Transporte de Información.

Equipo activo para la red LAN. Switch PowerConnect 5324, 24 Port 10/100/1000 y 4 puertos 1000, Switch PowerConnect 2724 de 24 puertos GigaBit, 2 GE/SFP, Switch PowerConnect 6024F de 24 puertos Gigabit FO, 8 puertos Gigabit UTP.

Equipo activo inalámbrico. Access point Dell FWAG114 NETGEAR, estándar 802.11a/g, 802.11b.

c. Propuesta C

La propuesta contempla la instalación de una infraestructura conforme al estándar Gigabit Ethernet, ISO/IEC 11801 y EIA/TIA568A, con cable UTP categoría 6, 24 AWG, mediante canaleta perimetral. Certificación de la correcta operación de los elementos del cableado estructurado proporcionada por el fabricante por un periodo de 15 años, y garantía por un año de la instalación proporcionada por el Integrador de Sistemas de Transporte de Información.

Equipo activo para la red LAN. Switch 3com serie 5500G 20 puertos 10/100/1000 con 4 puertos Gigabit basados en SFP, módulo 100BASE-FX y 100BASE-SX.

Equipo activo inalámbrico. Access point 3com 8750, estándar 802.11a/b/g con antena de 8 dbi de ganancia.

La comparación de las propuestas anteriormente mencionadas se indica en la tabla 4.23.

Equipo	Características	Propuesta A	Propuesta B	Propuesta C
LAN	Ventajas	-Velocidad 10/100/1000 -Administrable -Ruteo de capa 3 -Servicio QoS -Escalable	-Velocidad 10/100/1000 autonegociable -Administrable -Modulo opcional de expansión -4 puerto SFP incluidos -Servicio QoS -Conmutación en capa 2 y 3	-Velocidad 10/100/1000 -Módulo opcional de expansión -Administración del tráfico de red. -Apilable -Conmutación en capa 2 y 3 -Garantía y reconocido en el mercado. -Utiliza listas de acceso de IP. -Administrable -Soporta UTP categoría 6
LAN	Desventajas	-Costo elevado -No soporta UTP categoría 6	-No tiene un gran reconocimiento y confiabilidad ganada en el mercado comparada con otras marcas.	-Costo elevado
Wireless	Ventajas	-Cumple con el estándar 802.11b. -Encriptación WEP y listas de control de acceso. -Antena que proporciona una ganancia de 10 dbi. -Administrable -Trabaja como AP, AP Bridge, AP cliente, AP Router. -Soporta velocidades de 10/100. -Soporta frecuencias de 2.4GHz.	-Cumple con el estándar 802.11a/g -Soporta el estándar 802.11b -Soporta velocidades de 100 -Incluye un firewall. -Encriptación WEP. -Utiliza métodos de autenticación: AHP, HMAC-MD5-96, HMAC-SHA1-96.	-Cumple con el estándar 802.11a/g. -Soporta frecuencias de 5GHz y 2.4GHz. -Seguridad integrada -Capacidad de actualización. -Certificación Wi-Fi. -Soporta usuarios 802.11b/g. -Antena que proporciona una ganancia de 8 dbi. -Encriptación WEP, WPA AES -128 bits en sesiones inalámbricas -Soporta SNMP -Administrable -Autenticación con RADIUS -Soporta velocidades de 10/100 -Soporta hasta 253 usuarios simultáneos.
Wireless	Desventajas	-Costo elevado -Soporta cable UTP categoría 5 -Solo soporta el estándar 802.11b	-Aún está en lucha constante por el reconocimiento y confiabilidad en el mercado comparada con otras marcas.	-Costo elevado -Soporta cable UTP categoría 5

Tabla 4.23 Comparación de las diferentes propuestas

Cada una de las propuestas analizó diferentes recursos para satisfacer las necesidades a cubrir; sin embargo, debe indicarse que el fin es proveer a la Dependencia con la infraestructura a gigabit con tiempo de vida a largo plazo. En la tabla anterior se indica las ventajas de la marca 3com, en costo, características de los dispositivos. La operabilidad de los dispositivos está respaldada por el prestigio de la marca.

4.7 Análisis de costos

El costo de cada propuesta se indica en la tabla 4.24.

Equipo	Cantidad	Propuesta A	Cantidad	Propuesta B	Cantidad	Propuesta C
LAN						
Implantación de SCE	1	\$178,000	1	\$173,000.00	1	\$159,750.00
Switch 10/100/1000 48 puertos	1	\$82,988.1	0	-	0	-
Switch 10/100/1000 24 puertos	4	\$39,392.1	1 1 2 1 1	\$30,243.81 \$18,007.52 \$13,365.06 \$6,327.36 \$19,690.05	6	\$15,518.1
Switch 10/100/1000 16 puertos	0	-	0	-	0	-
Adaptadores diversos	1	\$2,595	0	-	1	\$65,850.72
Subtotal LAN		\$421,151.50		\$273,998.86		\$318,709.32
RADIUS	0	-	0	-	1	\$13,500.00
Fireware	0	-	0	-	1	\$13,500.00
Servidor de impresión	0	-	0	-	1	\$73,605.00
Servidor de base de datos	0	-	0	-	1	\$52,630.00
Servidor Web	0	-	0	-	1	\$59,005.00
Subtotal servidores y seguridad		0		0		\$212,240.00
Wireless						
Access Point	2	\$7,994.80	2	\$2,706.95	2	\$7,364.44
Subtotal		\$437,141.10		\$279,412.76		\$545,678.2
15 %IVA		\$65,571.17		\$41,911.95		\$81,851.73
Total MN		\$502,712.27		\$321,324.68		\$627,529.93

Tabla 4.24 Costos de las propuestas

El costo de la propuesta seleccionada, propuesta C, respalda la disponibilidad, confiabilidad e integridad de la información como el segundo activo de la Dependencia. Si bien, en la actualidad no es sólo una inversión de la tecnología a implantar, sino, una necesidad para persistir en el mercado tan competitivo en la actualidad. Dicha tecnología reduce a largo plazo el costo de adquirirla como una existencia de la Dependencia misma.

La tabla 4.21 muestra el costo para la propuesta óptima que rebasa a la propuesta B; sin embargo, en la tabla 4.20 se indican las características de los dispositivos que están por arriba de los demás.

Debe indicarse con gran persistencia, que el tiempo de vida de esta red esta estimada al menos, para 5 años en el equipo activo. La operabilidad de la red se garantiza con la certificación de la correcta operación de los elementos del cableado estructurado proporcionada por el fabricante por un periodo de 15 años, y garantía por un año de la instalación proporcionada por el Integrador de Sistemas de Transporte de Información.

4.8 Relación costo beneficio

El beneficio de la implantación de la red de datos de la DUAD se fundamenta en su correcto funcionamiento a largo plazo. La certificación y garantía de la instalación de la red que el Integrador de Tecnologías de Comunicación avala por 15 años, cumple con normas y estándares internacionales y mexicanas asegurando su operabilidad. Debe considerarse que la certificación es emitida por el fabricante.

El beneficio de la adquisición de la infraestructura física incurre en la escalabilidad de la tecnología física, la flexibilidad para posteriores incorporaciones o reubicación de componentes o tecnologías tales como voz sobre IP, la disponibilidad de la continua operación de la red, el rendimiento de la red que asegura el correcto funcionamiento de la misma, la seguridad de la información transmitida por la red, y la administración de la red que proporcione la facilidad de monitorear, configurar y corregir los errores que pudiesen presentarse durante su uso.

Así entonces, a pesar del coste de la propuesta C superior a la propuesta B, que podría considerarse como una buena elección, es imprescindible justificar la disponibilidad, confiabilidad e integridad de la información a largo plazo. Además, la marca de los dispositivos seleccionados es reconocida por su colaboración constante en el mercado y la calidad entregada de sus productos basados en la investigación e innovación de los mismos.

4.9 Propuesta de las políticas de administración de la red de datos para la División de Universidad Abierta de la Facultad de Derecho

Políticas de red

Las políticas de red a implementarse deben ser aceptadas por todos los usuarios y administradores de redes, es importante que ambos tipos de usuarios deban estar dispuestos a aplicarlas. Las políticas a utilizar son las recomendadas en el capítulo 1.

Política de seguridad del sitio

Dentro de la red se tienen contempladas varias áreas y para cada una de ellas se debe tener una administración de seguridad diferente. La red inalámbrica debe tener mayor seguridad para restringir el acceso a sólo personal autorizado.

La política de seguridad del sitio debe tomar en cuenta la protección de los recursos: estaciones de trabajo, computadoras host y servidores, dispositivos de interconexión: gateways, routers, switches, hubs, repetidores; servidores de terminal, software para conexión de red y de aplicaciones, cables de red, la información de archivos y bases de datos. Debido a que el sitio está conectado a otras redes, la política de seguridad del sitio debe considerar las necesidades y requerimientos de seguridad de todas las redes interconectadas respetando las políticas de Red UNAM.

Para proteger los recursos mencionados se tienen las siguientes políticas ya mencionadas en el capítulo 1; tales como, ubicar los servidores en lugares de acceso físico restringido libre de polvo, el servidor y los equipos de comunicaciones deben tener un no break, entre otros.

Planteamiento de la política de seguridad

Como ya se dio a conocer, el especificar una política de seguridad de red significa elaborar procedimientos y planes que protejan los recursos de la red contra pérdida y daño.

Cuando se necesita proteger una red, el costo de protegerla debe ser menor que el de recuperación en caso de que se viera afectado por una amenaza de seguridad. Para hacer el análisis de seguridad se deben discutir y aceptar las políticas de seguridad.

Para un mejor nivel de seguridad, a los usuarios se les debe dar a conocer el uso adecuado de los sistemas de cómputo, saber cómo protegerse a sí mismos de accesos no autorizados y explicar explícitamente las políticas de seguridad.

Se deben hacer inspecciones a las instalaciones de la red para la evaluación de amenazas y riesgos, con todo ello podemos saber en donde se necesita mayor o menor seguridad y con ello, tenerla actualizada.

Después de haber hecho inspecciones a la red ya se tendrá identificados todos los recursos con posibles riesgos de sufrir una violación de seguridad. Es necesario incluir todos los recursos de la red que puedan ser afectados por un problema de seguridad.

Los siguientes recursos son los que se recomiendan dentro de las políticas de red:

1. Hardware. Procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, servidores terminales, routers, switches.
2. Software. programas fuente, programas objeto, utilerías, programas de diagnostico, sistemas operativos, programas de comunicaciones.
3. Datos. Durante la ejecución, almacenados en línea, archivados fuera de línea, respaldos, registros de auditoria, bases de datos, en tránsito a través de medios de comunicación.
4. Personas. Usuarios, personas necesarias para operar los sistemas.
5. Documentación. De programas, hardware, sistemas, procedimientos administrativos locales.
6. Suministros. Papel, formularios, cintas, medios magnéticos y ópticos.

Ya que se identificaron los recursos a proteger hay que saber a que amenazas están vulnerables. Algunas de las amenazas a verificar son las siguientes:

- Acceso a los recursos de la red sin permiso alguno.
- No se debe revelar ningún tipo de información sin consentimiento de las autoridades pertinentes.
- Los servicios compartidos dentro de la red no deben ser modificados por usuarios sin autorización.
- Protección a los equipos de comunicación debido a los fallos eléctricos y acceso a personal no autorizado.

Las recomendaciones de las políticas de seguridad indican que se deben crear grupos de usuarios para dividir a los usuarios que requieran más permisos que otros usuarios dentro de los recursos de la red.

Una vez que se han determinado los usuarios que están autorizados a los recursos de la red, se deben establecer los lineamientos del uso aceptable de dichos recursos. La restricción de los recursos debe ser acorde a las funciones que desempeñe el usuario y a sus requerimientos. Lo delicado es equilibrar el acceso restringido a los privilegios especiales para hacer más segura la red; es decir, se deben conceder solo los privilegios suficientes para realizar las tareas necesarias.

Para identificar a los usuarios que van a tener acceso a la red; se les va a asignar una cuenta con su respectiva contraseña a los usuarios que pertenezcan a la DUAD o tengan autorización del jefe de la misma. Esta cuenta y su contraseña son intransferibles.

Para un buen uso de las contraseñas de red se tienen lo siguiente:

- El administrador de la red será el responsable de asignar las contraseñas.
- La longitud de una contraseña deberá siempre ser verificada de manera automática al ser construida por el administrador o el usuario. Todas las contraseñas deberán contar con al menos seis caracteres combinando letras y números.
- Las contraseñas elegidas por los usuarios deben ser difíciles de adivinar. No deben ser utilizadas palabras que aparezcan en el diccionario, secuencias conocidas de caracteres, datos personales ni acrónimos.
- Está prohibido que los usuarios construyan contraseñas compuestas de algunos caracteres constantes y otros que cambien de manera predecible y sean fáciles de adivinar.
- Los usuarios no deben construir contraseñas idénticas o muy parecidas a contraseñas anteriores.
- La comunicación de la contraseña se realizará de manera personal y no se podrá informar a otra persona que no sea el interesado.
- No se podrán informar contraseñas por vía telefónica.
- Las contraseñas del administrador deberán cambiarse máximo cada seis meses.

A continuación se muestran algunos aspectos a considerar para la determinación de responsabilidades y derechos para usuarios así como para administradores.

Para los usuarios:

- Crear lineamientos que consideren el uso de los recursos de red, tales como que usuarios están restringidos y cuales son sus restricciones.
- Contemplar que constituye un abuso en términos de usar recursos de red y afectar el desempeño del sistema y de la red.
- No permitir que los usuarios puedan compartir sus contraseñas.
- Los Usuarios no podrán revelar su contraseña por ningún motivo ya que es la única manera de autenticación.
- Determinar que usuarios deben cambiar su contraseña y con que frecuencia, todo esto para aumentar la seguridad de algunos usuarios.
- Definir quien es el que deberá hacer el respaldo de los datos del usuario, el Administrador o el usuario mismo.
- Detallar las consecuencias para los usuarios que divulguen información confidencial del sistema.
- Avisar de estas políticas a todos los usuarios, así como las sanciones a las faltas de las políticas de seguridad.

Para los administradores:

- El administrador puede revisar o leer los archivos de un usuario, si es que la seguridad de la red está en riesgo.
- Los administradores tienen derecho a examinar el tráfico de la red o de la estación de trabajo.
- El administrador podrá aplicar sanciones a los usuarios que pongan en riesgo la seguridad de la red.

Las políticas que especifican como deben los usuarios acceder al sistema, desde donde y de que manera deben autenticarse; son las siguientes:

- Todos lo administradores que den un servicio de acceso remoto deberán contar con aplicaciones que permitan una comunicación segura y encriptada.
- Todos los usuarios deberán autenticarse con su cuenta y no podrán hacer uso de sesiones activas de otros usuarios.

- Todos los usuarios deberán acceder al sistema utilizando algún programa que permita una comunicación segura y encriptada.
- Está prohibido acceder al sistema con una cuenta diferente de la propia, aún con la autorización del dueño de dicha cuenta.
- El usuario tendrá el derecho a cambiar su contraseña.
- El usuario podrá utilizar los servicios de sesiones remotas si se le brinda.

Plan de acción cuando es violada la política de seguridad

Dado que una red de datos siempre va a estar propensa a ataques, las políticas de seguridad nos permiten contemplar planes para cuando la seguridad es violada. Para poder hacer un buen plan de acción se deben tener procedimientos para poder manejar cada tipo de incidente de violación, ya sea si un usuario viola las políticas de seguridad de la red local o de una red remota; o en otro caso, si la seguridad de la red es vulnerada por un usuario local o remoto. Para identificar estos casos se debe llevar un registro apropiado de los ataques y revisarlo con frecuencia para revisar la tendencia y si es posible ajustar las políticas de seguridad para actualizar el plan y las medidas a seguir.

Identificación y prevención de problemas de seguridad

Para identificar los recursos y administrar la seguridad se tienen los siguientes recursos y las medidas de seguridad que trataron en el capítulo 1.

- Puntos de acceso. Los puntos de acceso son los puntos de entrada, también llamados de ingreso para los usuarios no autorizados. Para evitar esto, es importante incluir dentro de la política de seguridad que está prohibido realizar conexiones privadas a estaciones de trabajo dentro y fuera de la red de datos, sin permiso alguno.
- Sistemas mal configurados. Cuando un individuo llega a penetrar en la red, por lo general los blancos preferidos son los servidores; si estos servidores están mal configurados son responsables de numerosos problemas dentro de la red. Para esto es necesario entender el funcionamiento de los sistemas operativos y software correspondiente para entender como funciona el sistema y poder dar una mejor seguridad a la red.
- Problemas de software. Por lo general cuando aumenta la complejidad del software aumenta el número y la complejidad de los problemas de un sistema determinado. Las fallas de seguridad conocidas públicamente se vuelven métodos de acceso no autorizado. Si la implementación de un sistema es abierta y muy conocida como Unix o Linux, el intruso puede usar los puntos débiles del código de software que se

ejecuta en modo administrador para tener acceso privilegiado al sistema. El administrador debe estar consiente de los puntos débiles de sus sistemas operativos y tiene la responsabilidad de obtener las actualizaciones y de implementar las correcciones cuando se descubran problemas relacionados con estos.

- Amenazas internas. los usuarios internos tienen más acceso al software de la computadora y de la red que al hardware. Si un usuario decide perturbar la red, puede representar una considerable amenaza a la red. Para evitar estos problemas es necesario evitar el acceso a los servicios de telnet, rlogin y ftp, desde cuentas privilegiadas.
- Seguridad física. La computadora del usuario debe ser físicamente segura. Todos los equipos de suma importancia de funcionamiento a la red deben estar ubicados en un área físicamente segura.

CONCLUSIONES

La disponibilidad de la información es de suma importancia para las organizaciones, de cualquier índole, en el mercado tan competido. La confiabilidad e integridad de la información garantiza su valor como su segundo activo más importante para la Dependencia; de ahí, la importancia de contar con la infraestructura tecnológica para llevar a cabo las actividades propias de la Dependencia Educativa utilizando las tecnologías de información para mantenerse en la vanguardia de la educación.

Es de suma importancia la planeación de la red de datos a implantarse, ya que se reducen colisiones y tráfico en dicha red; al igual que limitaciones en el futuro crecimiento de la misma y escalabilidad de la tecnología.

Con la implantación del presente proyecto expuesto en esta tesis, se garantiza satisfacer los objetivos de rediseñar la red de datos de la DUAD mediante la implantación de tecnología de alta velocidad que asegura la capacidad de transferencia y confiabilidad de transmisión. Se sugiere equipo para robustecer los servidores actuales, con ello se aumenta la escalabilidad, el tiempo de respuesta, seguridad y disponibilidad de la información. Así entonces, se eliminan los problemas que se presentan en la actualidad en dicha red, lo cual fue planteado como un objetivo más.

Con el uso de switches en la DUAD y en las diferentes Dependencias se reducen las colisiones, se aumenta el performance de la red y la velocidad de transmisión para cada usuario con la asignación de su propio segmento. El switch propuesto puede también desempeñarse como conmutador de capa 3 y capa 2, así entonces, estamos separando dominios de colisión y disminuimos el tráfico en la red. Cabe señalarse que el equipo propuesto de la marca 3com, está preparado para la futura incorporación de tecnología para voz sobre IP, lo que repercute directamente en la disminución de los costos a largo plazo.

El punto de acceso propuesto para la red inalámbrica tiene además, entre sus múltiples características, la capacidad de segmentar dominios de colisión. Con esta segmentación aísla el tráfico de la red inalámbrica con el que genera la red local, logrando así, mayor seguridad a la información de la Dependencia requerida, dada la importancia de dicha información.

La infraestructura a implantarse es de categoría 6. Con ellos aseguramos su crecimiento a mediano y largo plazo. Es importante señalar que la categoría 6 del cableado garantiza la efectiva operabilidad de las aplicaciones de alta velocidad.

Es importante considerar de la misma categoría todos los componentes del cableado para evitar posibles fallas de acoplamiento de la señal, debido a las diferentes características de

desempeño que tienen las diferentes categorías; lo que conllevaría a afectar el preformance de la red. La flexibilidad de la red garantiza la fácil incorporación de nuevos servicios y nuevas tecnologías durante su vida útil de aproximadamente 15 años.

La presente propuesta se fundamenta en normas y estándares internacionales y nacionales, proporcionando estética en todo el cableado de la red. Debe mencionarse que la planeación de la red en conjunto con un grupo multidisciplinario formado por las diversas áreas que participan en el proyecto, ya sea remodelación o un edificio nuevo, asegura el cumplimiento de estándares correspondientes a cada una de ellas; para realizar el proyecto de manera ordenada y con una logística adecuada a las necesidades del proyecto.

El cumplimiento de los estándares y normas estipulados en el sistema de cableado estructurado garantiza la fácil administración de la red, basada en la identificación de cables y componentes que permitan su identificación, reubicación y sustitución de los elementos que conforman la red.

La red de datos sistematizada proporciona múltiples beneficios, y el costo de su implantación repercute directamente en la decisión de los directivos. La efectiva asignación de recursos, humanos o físicos, es una actividad que se debe llevar a cabo minimizando, en lo posible pero sin poner en riesgo, la operabilidad y disponibilidad de la red.

La administración de la red de datos es de suma importancia para el buen funcionamiento de dicha red. Con las políticas de seguridad expuestas en esta tesis, se cumple el objetivo de proponer políticas de administración para la red de datos de la DUAD para un mejor manejo de los recursos de la misma, por lo que, disminuyen las vulnerabilidades a los sistemas, aumenta la seguridad de la información y de los recursos utilizados. Aunado a lo anterior, los procedimientos son importantes para tomar acción cuando la información y recursos físicos están en riesgo de pérdida o daño. Cabe señalar que la seguridad está dirigida tanto a la física como a la lógica de los equipos.

ANEXOS

Anexo A

Puntos de Acceso (Access Point)

Especificaciones de producto

<p>Usuarios Soportados: Hasta 253 usuarios simultáneos</p> <p>Cumplimiento con estándares: Certificación Wi-Fi, IEEE 802.11a, IEEE 802.11g</p> <p>Velocidades de datos: 802.11a: 54, 48, 36, 24, 18, 12, 9, 6Mbps (hasta 108 Mbps en modalidad turbo) 802.11g: 54, 48, 36, 24, 18, 11, 9, 5.5, 2, 1 Mbps</p> <p>Banda de frecuencia: 802.11a: 5 GHz 802.11g: 2.4 GHz</p> <p>Medio inalámbrico: 802.11a: OFDM, 802.11g: OFDM y DSSS (con codificación Barker y CCK para compatibilidad con el estándar anterior 802.11b)</p> <p>Protocolo de Acceso de Medios: CSMA/CA</p> <p>Canales operativos: 802.11a: 36 - 64 (total de 8) 802.11g: 1 - 11 (EUA y Canadá), 1 - 13 (en todo el mundo; la disponibilidad del canal depende de regulaciones locales)</p> <p>Alcance operativo: 802.11a: hasta 50 metros (164 pies) de transmisión y recepción 802.11g: hasta 100 metros (328 pies) de transmisión y recepción</p> <p>Configuraciones de potencia de transmisión: 802.11a: 17 dBm en banda baja dependiendo de la velocidad en bits; 20dBm en banda media dependiendo de la velocidad en bits; 802.11g: 17 dBm dependiendo de la velocidad en bits</p> <p>Consumo: 2W de media, 11,2W máximo</p> <p>Sensibilidad de recepción: 802.11a: 6 Mbps: -84 dBm, +/- 2 dBm (dependiendo de la banda) 12 Mbps: -82 dBm 36 Mbps: -73 dBm 54 Mbps: -66 dBm 802.11g: 1 Mbps: -96 dBm 2 Mbps: -94 dBm 5.5 Mbps: -92 dBm 11 Mbps: -88 dBm 12 Mbps: -86 dBm 24 Mbps: -85 dBm 36 Mbps: -80 dBm 54 Mbps: -73 dBm</p> <p>Seguridad: Encriptación WEP de 40/64 y 128/154 bits; encriptación WPA AES de 256 bits, encriptación Dynamic Security Link de 128 bits; 802.11x con autenticación de servidor RADIUS; autenticación EAP-MD5, EAP-TLS, EAP-TTLS y PEAP; ESSID broadcast control, autenticación MAC local; listas de control de acceso a servidores, administración de Sesiones Dinámicas de Claves y TKIP, asignación dinámica VLAN, filtración cliente a cliente y uplink</p> <p>Rendimiento: Clear Channel Select, conexión automática a la red, cambios dinámicos de velocidad</p> <p>Gestión de red: Herramienta para "Site survey", Wireless Infrastructure Device Manager, Wireless LAN Discovery Tool, 3NS, SNMP</p> <p>Seguridad: IEC & EN 60950, UL / CSA 60950, NOM 019</p> <p>RF: FCC Parte 15.247, Parte 15.205, Parte15.209, y Parte 15.407, RSS-210, EN 300 328-2, EN 301 893, TELECOM RCR STD 33 & T66</p> <p>EMC : EN 301 489-17, EN 301 489-3</p> <p>Alcance de operación ambiental: Temperatura de operación: 0°C a 40°C (32°F a 105°F); Humedad: 5-95% no-condensación</p> <p>Antena: 802.11a: Antena integrada solamente; 802.11g: Opciones de antena externa disponibles, ver Lista de Opciones para mayores detalles</p> <p>Dimensiones: Alto: 32 cm (12.5 pulgadas) Ancho: 20 cm (8.1 pulgadas) Profundidad: 7 cm (2.8 pulgadas)</p> <p>Requisitos del sistema Para ejecutar las aplicaciones de administración, se necesita una computadora con CD-ROM que opere con Windows XP/2000/Me/98/95b+/NT 4.0+</p>

Características y ventajas

LAN inalámbrica de clase empresarial con protección a futuro para acceso a la red desde cualquier lugar. El 3Com Wireless 8750 Access Point crea una LAN inalámbrica de clase empresarial y alto rendimiento que soporta hasta 253 usuarios simultáneos. Su seguridad integrada, manejabilidad, capacidad de actualización y confiabilidad hacen que sea ideal para cualquier organización o institución que enfrente un aumento en sus necesidades de computación.

El 8750 Access Point se distribuye como punto de acceso bi-direccional 802.11a-802.11g de 54 Mbps, con soporte para transmisiones de radio de 5 GHz y 2.4 GHz para servirle a más clientes inalámbricos y a diferentes tipos de cliente dentro de la misma área de cobertura. La arquitectura dual de ranuras de radio provee flexibilidad de configuración y protección de inversiones. Sus funciones integradas de seguridad, manejabilidad y confiabilidad hacen que sea ideal para cualquier organización o institución que enfrente crecimiento en sus necesidades de computación móvil.

Para proteger comunicaciones y datos confidenciales en la LAN inalámbrica, el 8750 Access Point ofrece uno de los conjuntos de capacidades de autenticación y encriptación más avanzados y completos en el mercado, hoy en día.

Las herramientas de administración de red basadas en la Web hacen que la configuración y la administración remota de la red sean fáciles, mientras el soporte SNMP y el 3Com Network Supervisor integran a la LAN inalámbrica con su infraestructura por cables.

La certificación Wi-Fi asegura interoperabilidad con los productos certificados con Wi-Fi de otros fabricantes. Si el punto de acceso se utiliza con una antena externa, usted deberá comprar un cable de antena.

Para el máximo en eficiencia, usted deberá usar el cable de antena más corto posible. Los cables de antena inducen pérdidas de señal, lo cual limita el rendimiento y el alcance de la potencia irradiada del punto de acceso. De las opciones disponibles, recomendamos el Cable para Antena de 6 pies de 3Com (3CWE480).

- Se distribuye como punto de acceso bi-direccional 802.11a-802.11g para soportar a más clientes inalámbricos dentro de la misma área de cobertura
- Soporta hasta 253 usuarios simultáneos a velocidades de hasta 54 Mbps y distancias de hasta 100 metros (328 pies)
- Clear Channel Select escoge el canal menos traficado para brindar conexiones sin problemas
- La conexión automática a la red y los cambios dinámicos de velocidad hacen que las conexiones a la red estén continuamente disponibles modificando las velocidades de conexión automáticamente, a medida que las condiciones cambian y los usuarios móviles se desplazan a través del área de cobertura de la red
- A través de PoE el punto de acceso recibe corriente por medio de cables Ethernet existentes, resultando en instalaciones más simples y flexibles; no se requiere un suministro de potencia adicional
- Una antena de radio diversa provee rendimiento y cobertura excelentes en ambientes de altas trayectorias múltiples tales como oficinas, bodegas y otras instalaciones internas
- Las opciones de antenas externas extienden el alcance de la conexión inalámbrica 802.11g a hasta 305 metros (1,000 pies)
- Se distribuye como punto de acceso 802.11g 2.4 GHz de una sola modalidad de 54-Mbps con una ranura abierta de radio intercambiable.
- Soporta a usuarios inalámbricos 11g y 11b, preservando sus inversiones inalámbricas existentes

- La encriptación WEP de clave compartida de 40/64 bits y 128/54 bits, y la encriptación avanzada WPA AES de 256 bits asegura la privacidad de todas las transmisiones inalámbricas
- El enlace dinámico de seguridad automáticamente asigna claves de encriptación específicas para cada usuario de 128 bits en las sesiones inalámbricas
- La autenticación 802.11x del servidor RADIUS controla el acceso a la red inalámbrica y centraliza la autorización de los usuarios en toda la red
- La administración dinámica de claves de sesión y la asignación de claves dinámicas TKIP mejora la seguridad y simplifica las implementaciones
- Las listas de control de acceso de direcciones MAC controlan el acceso a los recursos de la red
- Las funciones de filtración "cliente a cliente" y filtración de uplinks dirigen las comunicaciones entre otros usuarios inalámbricos asociados a los puntos de acceso
- La asignación dinámica de VLAN, utilizada con autenticación RADIUS, les provee a los usuarios a una VLAN adecuada, protegiendo aún más el acceso a los recursos de la red
- El soporte para SNMP, 3Com Network Supervisor y otros software de gestión basados en estándares asegura una integración sin fisuras con su red de cable]
- Las herramientas Wireless Infrastructure Device Manager (Gerente Inalámbrico de Infraestructura de Dispositivos) y Wireless LAN Device Discovery (Descubrimiento de Dispositivos en LANs Inalámbricas) permiten configurar parámetros, ejecutar diagnósticos y supervisar el rendimiento desde cualquier punto en la red, usando un navegador Web
- Soporte para SNMP, 3Com Network Supervisor, HP OpenView y otros software de administración basados en estándares, aseguran una integración ininterrumpida con su red por cables
- El soporte de contabilidad RADIUS permite facturación por uso de hotspot u otro tipo de implementaciones comerciales
- La herramienta de detección de sitios funciona con PC Cards empresariales inalámbricas de 3Com para ayudarle a optimizar la localización y el número de puntos de acceso de su instalación

Anexo B

Servidor de impresión

IMAGERUNNER 2870



Copiadora de papel bond, acetatos y albanene en formato carta y legal Hasta Doble carta
Velocidad de 28 copias por minuto (tamaño carta)
Reduce y Amplifica con Zoom de 25 a 400 %
Tamaño máximo de copiado doble carta
Exposición Automática y Manual
100 Claves de acceso
Copiado ambos lados (DUPLEX))
2 Cassettes para 500 hojas c/u.
Compaginado electrónico
Pedestal
Opcionales: Tarjeta de Red, Tarjeta de Fax,
Finalizador/Engrapador
Doblador y Perforador. Alimentador gran capacidad, charolas para papel, RADF (alimentador Recirculante de originales),
Tarjetas de red, charola 2 vias copiado/impresión

Anexo C

Servidor de Bases de Datos y Web

Procesador, sistema operativo y memoria	
Procesador	Hasta 2 procesadores Intel® Xeon a 2.8 GHz, 3.0 GHz ó 3.2 GHz
Número de procesadores	se soportan 1 ó 2
Memoria caché	1 MB ó 2 MB de caché de segundo nivel (según modelo)
Chipset	Chipset Intel® E7320 con FSB a 800 MHz
Tipo de memoria	SDRAM DDR PC2700 a 333 MHz
Ranuras de memoria	4 ranuras
Ampliación de memoria	Máximo - 8 GB
Unidades internas	
Unidad de disco duro	Discos de 36.4GB, 72 GB ó 2x72 GB U320 SCSI 15K non-hot-plug pre-instalados sólo en modelos no hot-plug SCSI (según modelo)
Almacenamiento masivo interno	Controlador SATA RAID opcional de 880,8 GB (modelos SCSI) o 1,5 TB (6 x 250 GB) de 6 puertos (modelos SATA)
Compartimentos para unidades internas	6 discos duros SCSI de 1" (hot-plug o no hot-plug) ó 4 discos duros SATA hot-plug
CD-ROM/DVD	Unidad de CD-ROM IDE (ATAPI) 48x
Características del sistema	
Descripción del chasis	(5U) Torre; Existe un kit opcional para montaje en rack
Características de alimentación	Fuente de alimentación de 600 W no conectable en caliente
Puertos E/S externos	Paralelo - 1; Serie - 1; Dispositivo de puntero (ratón, PS2) - 1; Gráficos - 1; Teclado (PS2)- 1; USB - 2; Conector de red RJ-45 (Ethernet) - 1
Interface de red	Tarjeta de red Broadcom 5721 10/100/1000 PCI-Express (integrada) con WOL (Wake on LAN)
Ranura de expansión	(6) en total: (1) PCI-Express x4; (4) PCI-X 64 bits/66 MHz 3.3 V (3 disponibles); (1) PCI 32 bits/33 MHz 5,0 V
Sistemas operativos compatibles	Microsoft® Windows® 2000 Server; Microsoft® Windows® 2003 Server, Standard Edition; Microsoft® Windows® 2003 Server, Web Edition; Microsoft® Small Business Server 2003; Microsoft® Small Business Server 2003, Premium Edition; Novell NetWare 6.5; Novell NetWare SBS 6.5; Red Hat Enterprise Linux 3; Red Hat Enterprise Edition Linux 3 (64 bits); SuSE Linux Enterprise Server 9; SuSE Linux Enterprise Server 9 (64 bits); VMware Virtualization Software
Gestión de PCs	Tarjeta de gestión remota opcional HP ProLiant ML150 G2 Lights-Out 100
Gestión de la seguridad	Contraseña de encendido; Contraseña de configuración; Control de arranque desde disquetera.
Características del servicio y asistencia técnica	HP proporciona una garantía limitada de un año, incluida cobertura de disco duro, memoria y procesadores, plenamente respaldada por una red mundial de distribuidores y proveedores de servicios.
características que facilitan el servicio	Apertura de chasis y acceso a componentes sin necesidad de utilizar herramientas

GLOSARIO

ADSL: (asymmetric digital subscriber line) Línea Digital del Suscriptor Asimétrica. Una de las cuatro tecnologías DSL. ADSL entrega mayor ancho de banda hacia abajo (desde la oficina central al lugar del cliente) que hacia arriba (desde el lugar del cliente a la oficina central). Las tasas hacia abajo oscilan entre 1.5 a 9 Mbps, mientras que el ancho de banda hacia arriba oscila entre 16 a 640 kbps. Las transmisiones a través de ADSL funcionan a distancias de hasta 5.488 metros sobre un único par de cobre trenzado. Vea también DSL, HDSL, SDSL y VDSL.

AES: (Advanced Encryption Standard) Estándar de Encriptación Avanzado, también conocido como Rijndael, es un estándar de criptografía simétrica adoptada en 2000. Se emplea especialmente para almacenamiento seguro de datos.

Ancho de banda: Diferencia entre las frecuencias más altas y más bajas disponibles para las señales de red. Asimismo, la capacidad de rendimiento medida de un medio o protocolo de red determinado.

ANSI: (Instituto Nacional Americano de Normalización) Organización voluntaria compuesta por corporativas, organismos del gobierno y otros miembros que coordinan las actividades relacionadas con estándares, aprueban los estándares nacionales de los EE.UU. y desarrollan posiciones en nombre de los Estados Unidos ante organizaciones internacionales de estándares. ANSI ayuda a desarrollar estándares de los EE.UU. e internacionales en relación con, entre otras cosas, comunicaciones y networking. ANSI es miembro de la IEC (Comisión Electrotécnica Internacional), y la Organización Internacional para la Normalización.

ARP: (Protocolo de Resolución de Direcciones) Protocolo de Internet que se utiliza para asignar una dirección IP a una dirección MAC. Se define en RFC 826. Comparar con RARP.

ATM: (modo de transferencia asíncrona) Estándar internacional para relay de celdas en el que varios tipos de servicios (por ejemplo, transmisión de voz, vídeo o datos) se transmiten en celdas de longitud fija (53 bytes). Las celdas de longitud fija permiten que el procesamiento de las celdas se produzca en el hardware, reduciendo así los retardos de tránsito. ATM se encuentra diseñado para aprovechar los medios de transmisión de alta velocidad como E3, SONET y T3.

AUI: (interfaz de unidad de conexión) Interfaz IEEE 802.3 entre una MAU y una tarjeta de interfaz de red. El término AUI también puede hacer referencia al puerto del panel posterior al que se puede conectar un cable AUI, como los que pueden encontrarse en la tarjeta de acceso Ethernet del LightStream de Cisco. También denominado cable transceptor.

Backbone: Núcleo estructural de la red, que conecta todos los componentes de la red de manera que se pueda producir la comunicación.

Banda ancha: Técnica de transmisión de alta velocidad y alta capacidad que permite la transmisión integrada y simultánea de diferentes tipos de señales (voz, datos, imágenes, etcétera).

Bit: Dígito binario utilizado en el sistema numérico binario. Puede ser cero o uno. Ver también byte.

Broadcast: Paquete de datos enviado a todos los nodos de una red. Los broadcasts se identifican por una dirección broadcast. Comparar con multicast y unicast. Ver también dirección broadcast, dominio de broadcast y tormenta de broadcast.

Byte: Serie de dígitos binarios consecutivos que operan como una unidad (por ejemplo, un byte de 8 bits). Ver también bit.

CDDI: (Interfaz de datos distribuidos por cobre) Implementación de protocolos FDDI en cableado STP y UTP. CDDI transmite a distancias relativamente cortas (unos 100 metros), con velocidades de datos de 100 Mbps mediante una arquitectura de doble anillo para brindar redundancia. Se basa en el estándar dependiente del medio físico de par trenzado (TPPMD) de ANSI. Comparar con FDDI.

CIR: (velocidad de información suscrita) Velocidad en bits por segundo, a la que el switch Frame Relay acepta transferir datos.

CSMA/CD: (Acceso múltiple con detección de portadora y detección de colisiones) Mecanismo de acceso a medios dentro del cual los dispositivos que están listos para transmitir datos primero verifican el canal en busca de una portadora. El dispositivo puede transmitir si no se detecta ninguna portadora durante un período de tiempo determinado. Si dos dispositivos transmiten al mismo tiempo, se produce una colisión que es detectada por todos los dispositivos que colisionan. Esta colisión subsecuentemente demora las retransmisiones desde esos dispositivos durante un período de tiempo de duración aleatoria. El acceso CSMA/CD es utilizado por Ethernet e IEEE 802.3.

CSMA/CA: (Carrier Sense Multiple Access With Collision Avoidance) es un protocolo de control de redes utilizado para evitar colisiones entre los paquetes de datos (comúnmente en redes inalámbricas, ya que estas no cuenta con un modo práctico para transmitir y recibir simultáneamente). Es un método de acceso de red en el cual cada dispositivo señala su intento para transmitir antes de que lo haga realmente. Esto evita que otros dispositivos envíen la información, así evitando que las colisiones ocurran entre las señales a partir de dos o más dispositivos. De esta forma permite a un emisor transmitir en cualquier momento en que el medio no esté ocupado.

DARPA: (Agencia de Proyectos de Investigación Avanzada para la Defensa) Agencia gubernamental de los EE.UU. que financió la investigación y la experimentación con la Internet. Antiguamente denominada ARPA, volvió a utilizar ese nombre a partir de 1994.

DCE: (equipo de transmisión de datos) Dispositivo usado para convertir los datos del usuario del DTE en una forma aceptable para la instalación de servicios de WAN.

DFWMAC: (Distributed Foundation Wireless MAC) método de acceso al medio inalámbrico mediante el cual se escucha pero sin detección de colisión.

DHCP: Protocolo de configuración dinámica del Host. Protocolo que proporciona un mecanismo para asignar direcciones IP de forma dinámica, de modo que las direcciones se pueden reutilizar automáticamente cuando los hosts ya no las necesitan.

Dirección IP: Dirección de 32 bits asignada a los hosts mediante TCP/IP. Una dirección IP corresponde a una de cinco clases (A, B, C, D o E) y se escribe en forma de 4 octetos separados por puntos (formato decimal con punto). Cada dirección consta de un número de red, un número opcional de subred, y un número de host. Los números de red y de subred se utilizan conjuntamente para el enrutamiento, mientras que el número de host se utiliza para el direccionamiento a un host individual dentro de la red o de la subred. Se utiliza una máscara de subred para extraer la información de la red y de la subred de la dirección IP. También denominada dirección de Internet (dirección IP).

Dirección MAC:(Control de Acceso al Medio) Dirección de capa de enlace de datos estandarizada que se necesita para cada puerto o dispositivo que se conecta a una LAN. Otros dispositivos de la red usan estas direcciones para ubicar dispositivos específicos en la red y para crear y actualizar las tablas de enrutamiento y las estructuras de los datos. Las direcciones MAC tienen 6 bytes de largo, y son controladas por el IEEE. También se denominan direcciones de hardware, dirección de capa MAC o dirección física. Comparar con dirección de red.

DIC: (Control de Enlace de Datos de Alto Nivel) Protocolo síncrono de la capa de enlace de datos, orientado a bit, desarrollado por ISO. HDLC especifica un método de encapsulamiento de datos en enlaces síncronos seriales que utiliza caracteres de trama y sumas de comprobación

DNS: (Sistema de denominación de dominio) Sistema utilizado en Internet para convertir los nombres de los nodos de red en direcciones.

DSL: (Digital Subscriber Line) (Línea Digital del Suscriptor) Tecnología de red que permite conexiones de ancho de banda ancha sobre el cable de cobre a distancias limitadas. Hay cuatro tipos o sabores de DSL: ADSL, HDSL, SDSL y VDSL. Todas estas tecnologías funcionan a través de pares de módems, con un módem localizado en la oficina central y el otro en el lugar del cliente. Debido a que la mayoría de tecnologías DSL no utilizan todo el ancho de banda del par trenzado, queda espacio disponible para un canal de voz.

DSSS: (Direct Sequence Spread Spectrum) también conocido en comunicaciones móviles como DS-CDMA (acceso múltiple por división de código en secuencia directa), es uno de los métodos de modulación en espectro ensanchado para transmisión de señales digitales sobre ondas radiofónicas que más se utilizan. Tanto DSSS como FHSS están de nidos por la IEEE en el estándar 802.11 para redes de área local inalámbricas WLAN.

DTE: (equipo terminal de datos) Dispositivo en el extremo del usuario de una interfaz usuario a red que sirve como origen de datos, destino, o ambos. DTE se conecta a una red de datos a través de un dispositivo DCE (por ejemplo, un módem) y utiliza normalmente señales de sincronización generadas por el DCE. DTE incluye dispositivos tales como computadores, traductores de protocolo y multiplexores.

EIA: (Asociación de Industrias Electrónicas) Grupo que especifica los estándares de transmisiones eléctricas. EIA y TIA han desarrollado en conjunto numerosos estándares de comunicación de amplia difusión, como EIA/TIA-232 y EIA/TIA-449.

Ethernet : El método de conexión más común en las redes de área local, LANs. En el caso de Ethernet, todas las estaciones del segmento comparten el ancho de banda total, que es 10 megabits por segundo (Mbps), 100 Mbps para Fast Ethernet, o 1000 Mbps para Gigabit Ethernet.

Fast Ethernet : Cualquiera de varias especificaciones de Ethernet de 100-Mbps. Fast Ethernet ofrece un incremento de velocidad diez veces mayor que el de la especificación de Ethernet 10BASE-T, aunque preserva características tales como formato de trama, mecanismos MAC, y MTU. Estas similitudes permiten el uso de herramientas de administración de red y aplicaciones 10BASE-T existentes en redes Fast Ethernet. Se basa en una extensión de la especificación IEEE 802.3. Ver también Ethernet.

FDDI: (Interfaz de datos distribuida por fibra) Estándar de LAN, definido por ANSI X3T9.5, que especifica una red de transmisión de tokens de 100 Mbps que utiliza cable de fibra óptica, con distancias de transmisión de hasta 2 km. FDDI usa una arquitectura de anillo doble para brindar redundancia.

FDDI II : Estándar ANSI que mejora FDDI. FDDI II brinda transmisión isócrona para circuitos de datos no orientado a conexión y circuitos de voz y vídeo orientados a conexión.

FHSS: El espectro ensanchado por salto de frecuencia (del inglés frequency hopping) es una técnica de modulación en espectro ensanchado en el que la señal se emite sobre una serie de radiofrecuencias aparentemente aleatorias, saltando de frecuencia en frecuencia sincronamente con el transmisor. Los receptores no autorizados escucharán una señal ininteligible. Si se intentara interceptar la señal, sólo se conseguiría para unos pocos bits.

Firewall : Router o servidor de acceso, o varios routers o servidores de acceso, designados para funcionar como búfer entre redes de conexión pública y una red privada. Un router de firewall utiliza listas de acceso y otros métodos para garantizar la seguridad de la red privada.

Firmware : Instrucciones de software establecidas de forma permanente o semipermanente en la ROM.

Frame Relay : Protocolo conmutado de la capa de enlace de datos, de norma industrial, que administra varios circuitos virtuales utilizando un encapsulamiento HDLC entre dispositivos conectados. Frame Relay es más eficiente que X.25, el protocolo para el cual se considera por lo general un reemplazo.

FTP: (Protocolo de Transferencia de Archivos) Protocolo de aplicación, parte de la pila de protocolo TCP/IP, utilizado para transferir archivos entre nodos de red. FTP se define en la RFC 959.

GPRS: (Servicio general de paquetes por radio) General Package Radio Service. Servicio general de paquetes por radio que permite manejar datos sobre redes celulares de una manera más eficiente.

HDSL: (high-data-rate digital subscriber line) Línea Digital del Suscriptor de alta velocidad. Una de las cuatro tecnologías DSL. HDSL entrega 1.544 Mbps de ancho de banda hacia arriba (desde el lugar del cliente a la oficina central) y hacia abajo (desde la oficina central al lugar del cliente), sobre dos pares de cobre trenzados. Debido a que HDSL ofrece velocidad T1, las compañías telefónicas han estado utilizando HDSL para entregar acceso local para servicios T1 en la medida de lo posible. El funcionamiento de HDSL está limitado a un rango de distancia de hasta 3658,5 metros. Se utilizan repetidoras de señal para ampliar el servicio. HDSL requiere dos pares trenzados. Por esta razón es utilizado principalmente para conexiones de red PBX, sistemas de circuito de carrier digitales, POPs de intercambio, servidores de Internet y redes de datos privadas. Vea también DSL, ADSL, SDSL y VDSL.

Host : Computador en una red. Similar a nodo, salvo que el host normalmente implica un computador, mientras que nodo generalmente se aplica a cualquier sistema de red, incluyendo servidores y routers.

HTML: (Lenguaje de Etiquetas por Hipertexto) Formato simple de documentos en hipertexto que usa etiquetas para indicar cómo una aplicación de visualización, como por ejemplo un navegador de la Web, debe interpretar una parte determinada de un documento.

HTTP: (Protocolo de Transferencia de Hipertexto) Protocolo utilizado por los navegadores y servidores de la Web para transferir archivos, como archivos de texto y de gráficos.

Hub: Dispositivo de hardware o software que contiene múltiples módulos de red y equipos de red independientes pero conectados. Los hubs pueden ser activos (cuando repiten señales que se envían a través de ellos) o pasivos (cuando no repiten, sino que simplemente dividen las señales enviadas a través de ellos).

IAB: (Comité de Arquitectura de Internet) Comité de investigadores de internetwork de redes que discute temas relativos a la arquitectura de Internet. Responsables por designar una serie de grupos relacionados con Internet, como IANA, IESG e IRSG. El IAB es nombrado por los síndicos de la ISOC.

ICMP: (Protocolo de mensajes de control en Internet) Protocolo Internet de capa de red que informa errores y brinda información relativa al procesamiento de paquetes IP.

Internetwork : Industria dedicada a la conexión de redes entre sí. Este término se refiere a productos, procedimientos y tecnologías.

IP: (Protocolo Internet) Protocolo de capa de red de la pila TCP/IP que ofrece un servicio de internetwork de redes no orientado a conexión. El IP brinda funciones de direccionamiento, especificación del tipo de servicio, fragmentación y reensamblaje, y seguridad. Se define en RFC 791. IPv4 (Protocolo Internet versión 4) es un protocolo de conmutación no orientado a conexión de máximo esfuerzo.

IPv6: (IP versión 6) Reemplazo de la versión actual de IP (versión 4). IPv6 brinda soporte para identificación de flujo en el encabezado del paquete, que se puede usar para identificar flujos. Anteriormente denominado IPng (IP de próxima generación).

IPX: (Intercambio de Paquetes de Internetwork) Protocolo de capa de red de NetWare utilizado para transferir datos desde los servidores a las estaciones de trabajo.

IrDA: (Infrared Data Association) Organización fundada para crear las normas internacionales para el hardware y el software usados en enlaces de comunicación por rayos infrarrojos. La tecnología de rayos infrarrojos juega un importante papel en las comunicaciones inalámbricas.

ISDN: Integrated Services Digital Network: Integrated Services Digital Network: sistema para transmisión telefónica digital. Con una línea ISDN y un adaptador ISDN es posible navegar por la Web a una velocidad de 128 kbps, siempre que el ISP también tenga ISDN.

ISP: (Internet Service Provider) Proveedor de Servicios de Internet, empresa dedicada a conectar a Internet la línea telefónica de los usuarios, redes distintas e independientes, ambas.

ISO:(International Organization for Standarization) Organización internacional que establece normalizaciones en muchos campos de la técnica. Entre otras cosas, coordina los principales estándares de redes que se usan hoy en día.

ISOC: (Sociedad Internet) Organización internacional sin fines de lucro fundada en 1992, que coordina la evolución y el uso de la Internet. Además la ISOC delega facultades a otros grupos relacionados con la Internet, por ejemplo el IAB. La ISOC tiene su sede en Reston, Virginia, EE.UU.

ITU: (International Telecommunication Union)Organización internacional que desarrolla los estándares mundiales para las tecnologías de las telecomunicaciones.

LLC: (control de enlace lógico) La más alta de las dos subcapas de enlace de datos definidas por el IEEE. La subcapa LLC maneja el control de errores, control del flujo, entramado y direccionamiento de subcapa MAC. El protocolo LLC más generalizado es IEEE 802.2, que incluye variantes no orientado a conexión y orientadas a conexión.

MAC: (Control de Acceso al Medio) Parte de la capa de enlace de datos que incluye la dirección de 6 bytes (48 bits) del origen y del destino, y el método para obtener permiso para transmitir.

MAU: (unidad de conexión al medio) Dispositivo utilizado en redes Ethernet e IEEE 802.3 que proporciona una interfaz entre el puerto AUI de una estación y el medio común de Ethernet. La MAU, que puede ser incorporada a una estación, o puede ser un dispositivo separado, lleva a cabo funciones de la capa física, incluyendo la conversión de datos digitales de la interfaz Ethernet, la detección de colisiones, y la inyección de bits en la red. Denominada a veces unidad de acceso al medio, también abreviada como MAU.

MTU (unidad máxima de transmisión) : Tamaño máximo de paquete, en bytes, que puede manejar una interfaz en particular.

MultiCasting: Técnica de transmisión de datos a través de internet, en la que se envían paquetes desde un punto a varios simultáneamente.

NetBEUI: (Interfaz de Usuario NetBIOS Extendida) Versión mejorada del protocolo NetBIOS que usan los sistemas operativos de red (por ejemplo: LAN Manager, LAN Server, Windows for Workgroups y Windows NT). NetBEUI formaliza la trama de transporte y agrega funciones adicionales.

NetBIOS: (Sistema Básico de Entrada/Salida de Red) Interfaz de programación de aplicación que usan las aplicaciones de una LAN IBM para solicitar servicios a los procesos de red de nivel inferior. Estos servicios incluyen establecimiento y finalización de sesión, así como transferencia de información.

NetWare : Popular sistema operativo de red distribuido desarrollado por Novell. Proporciona acceso remoto transparente a archivos y varios otros servicios de red distribuidos.

NIC: (tarjeta de interfaz de red) Tarjeta que brinda capacidades de comunicación de red hacia y desde un computador. También denominada adaptador

NOS: (sistema operativo de red) Sistema operativo utilizado para hacer funcionar una red, como, por ejemplo, NetWare de Novell y Windows NT.

OFDM: (Orthogonal Frequency Division Multiplexing) Técnica de modulación FDM (empleada por el 802.11a wi-fi) para transmitir grandes cantidades de datos digitales a través de ondas de radio. OFDM divide la señal de radio en múltiples subseñales más pequeñas que luego serán transmitidas de manera simultánea en diferentes frecuencias al receptor. OFDM reduce la cantidad de ruido (crosstalk) en las transmisiones de señal.

FHSS: Frequency Hopping Spread Spectrum

OSI: (Modelo de referencia de internetwork de sistemas abiertos) Modelo de arquitectura de red desarrollado por ISO e UIT-T. El modelo está compuesto por siete capas, cada una de las cuales especifica funciones de red individuales, tales como el direccionamiento, el control de flujo, el control de errores, el encapsulamiento y la transferencia confiable de mensajes. La capa inferior (la capa física) es la más cercana a la tecnología de los medios. Las dos capas inferiores se implementan en el hardware y en el software, y las cinco capas superiores se implementan sólo en el software. La capa superior (la capa de aplicación) es la más cercana al usuario. El modelo de referencia OSI se usa a nivel mundial como método para la enseñanza y la comprensión de la funcionalidad de la red. Similar en algunos aspectos a SNA.

Paquete: Agrupación lógica de información que incluye un encabezado que contiene la información de control y (generalmente) los datos del usuario. Los paquetes se usan a menudo para referirse a las unidades de datos de capa de red. Los términos datagrama, trama, mensaje y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

PDN: (red de datos públicos) Red operada por el gobierno (como en el caso de Europa) o por entidades privadas para suministrar comunicaciones computacionales al público, generalmente cobrando una tarifa. Las PDN permiten que las pequeñas organizaciones creen una WAN sin los costos de equipamiento de los circuitos de larga distancia.

PHY: 1. Subcapa física. Una de las dos subcapas de la capa física de FDDI. 2. Capa física En ATM, la capa física se encarga de la transmisión de celdas a través de un medio físico que conecta dos dispositivos ATM.

PLP: (protocolo a nivel de paquete) Protocolo de capa de red en la pila de protocolo X.25. Algunas veces denominado X.25 Nivel 3 y protocolo X.25.

PPP: (Protocolo Punto a Punto) Sucesor del SLIP, un protocolo que suministra conexiones router a router y host a red a través de circuitos síncronos y asíncronos.

Protocolo: Descripción formal del formato de los mensajes y de las reglas que dos ordenadores deben seguir para intercambiar mensajes.

QoS: (calidad de servicio) Medida de desempeño de un sistema de transmisión que refleja su calidad de transmisión y disponibilidad de servicio.

RADIUS: (Remote Access Dial-In User Server). Es un protocolo de autenticación, autorización y accounting para aplicaciones de acceso a la red o movilidad IP.

RDSI: (Red digital de servicios integrados) Protocolo de comunicaciones que ofrecen las compañías telefónicas y que permite que las redes telefónicas transmitan datos, voz y tráfico de otros orígenes.

Router : Dispositivo de capa de red que usa una o más métricas para determinar cuál es la ruta óptima a través de la cual se debe enviar el tráfico de red. Los routers envían paquetes de una red a otra basándose en la información de capa. Denominado a veces gateway (aunque esta definición de gateway se está volviendo obsoleta).

Servidor: Nodo o programa de software que suministra servicios a los clientes.

SMTP: Simple Mail Transfer Protocol) protocolo simple de transferencia de correo electrónico. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras y/o distintos dispositivos (PDA's, Celulares, etc).

SNMP: (Protocolo simple de administración de redes) Protocolo de administración de redes utilizado casi con exclusividad en redes TCP/IP. El SNMP brinda una forma de monitorear y controlar los dispositivos de red y de administrar configuraciones, recolección de estadísticas, desempeño y seguridad.

SPX: (Intercambio de Paquete Secuenciado) Protocolo confiable, orientado a conexión, que complementa el servicio de datagramas suministrado por los protocolos de capa de red. Novell derivó este protocolo de transporte NetWare de uso común del SPP del conjunto de protocolos XNS.

SSID. Significa Service Set Identifier, y es una cadena de 32 caracteres máximo que identifica a cada red inalámbrica. Los TRs deben conocer el nombre de la red para poder unirse a ella.

Subred : 1. Red segmentada en una serie de redes más pequeñas. 2. En redes IP, una red que comparte una dirección de subred individual. Las subredes son redes segmentadas de forma arbitraria por el administrador de la red para suministrar una estructura de enrutamiento jerárquica, de varios niveles mientras protege a la subred de la complejidad de direccionamiento de las redes conectadas. A veces se denomina subnetwork. 3. En redes OSI, un conjunto de sistemas finales y sistemas intermedios bajo el control de un dominio administrativo exclusivo y que utiliza un protocolo de acceso de red exclusivo.

Switch : Dispositivo que conecta computadoras. El switch actúa de manera inteligente. Puede agregar ancho de banda, acelerar el tráfico de paquetes y reducir el tiempo de espera.

Los switches son más “inteligentes” que los “Hubs” y ofrecen un ancho de banda más dedicado para los usuarios o grupos de usuarios. Un switch envía los paquetes de datos solamente a la computadora correspondiente, con base en la información que cada paquete contiene. Para aislar la transmisión de una computadora a otra, los switches establecen una conexión temporal entre la fuente y el destino, y la conexión termina una vez que la conversación se termina.

TCP: (Protocolo de Control de Transmisión) Protocolo de capa de transporte orientado a conexión que provee una transmisión confiable de datos de dúplex completo. TCP es parte de la pila de protocolo TCP/IP.

TCP/IP: (Transmission Control Protocol/Internet Protocol): Conjunto de protocolos usados en Internet para soportar servicios tales como acceso remoto telnet, transferencia de ficheros FTP y correo electrónico SMTP.

Telnet: Protocolo de emulación de terminal estándar de la pila de protocolo TCP/IP. Telnet se usa para la conexión de terminales remotas, permitiendo que los usuarios se registren en sistemas remotos y utilicen los recursos como si estuvieran conectados a un sistema local.

UDP: (Protocolo de Datagrama de Usuario) Protocolo no orientado a conexión de la capa de transporte de la pila de protocolo TCP/IP. UDP es un protocolo simple que intercambia datagramas sin confirmación o garantía de entrega y que requiere que el procesamiento de errores y las retransmisiones sean manejados por otros protocolos.

VoIP (Voice over IP): (Voz sobre Protocolo de Internet (IP)) La habilidad para transportar voz telefónica normal sobre una red de datos basada en el protocolo de Internet, con la misma funcionalidad, confiabilidad y calidad de voz que ofrecen las empresas telefónicas tradicionales.

VPN: (Red Privada Virtual) Una Red Privada Virtual, o Virtual Private Network, VPN, permite establecer una conexión segura a través de una red pública, o Internet.

Una VPN permite que el tráfico IP viaje seguro a través de una red pública TCP/IP al encriptar el tráfico desde una red hasta la otra. Una VPN usa tunneling para encriptar toda la información en el nivel IP.

WAN: (Wide-Area Network) red que cubre un territorio amplio.

WiFi: (Wireless Fidelity) es el nombre comercial del 802.11b y el logo con que ya se están vendiendo dispositivos que usan esta tecnología.

WLAN: (Wireless Local Area Network) red inalámbrica de área local.

WPA: (Wi-Fi Protected Access) es un sistema para asegurar redes inalámbricas ya que cambia automáticamente, creado para corregir el sistema previo WEP (Wired Equivalent Privacy) Privacidad Equivalente a Cableado.

XNS: (Sistema de red de Xerox) Conjunto de protocolo originalmente diseñado por PARC. Muchas empresas de networking para PC tales como 3Com, Banyan, Novell y UB Networks utilizaron o actualmente utilizan una variante de XNS como protocolo de transporte primario.

X.25: Estándar UIT-T que define la manera en que las conexiones entre los DTE y DCE se mantienen para el acceso a la terminal remota y las comunicaciones en computadores en las redes de datos públicas. Frame Relay ha reemplazado en cierta medida a X.25.

BIBLIOGRAFÍA

MESOGRAFÍA

BIBLIOGRAFÍA

KRICK E. V., “Introducción a la Ingeniería y al Diseño en la Ingeniería”, Limusa, S.A. de C.V. 2002.

REID Neil y SEIDE Ron, “Manual de Redes Inalámbricas. 802.11 (Wi-Fi)”, McGraw-Hill Interamericana 2005.

SPURGEON Charles E., “Ethernet the Definitive Guide”, . O'Reilly, First Edition.

STALLINGS William, “Comunicaciones y Redes de Computadoras”, Prentice-Hall, Quinta Edición.

TANENBAUM Andrew S., “Redes de Computadoras”, Pearson Prentice-Hall, Tercera edición.

ZACKER Craig, “Redes: Manual de Referencia”, McGraw-Hill Interamericana 2002.

MESOGRAFÍA

<http://tejo.usal.es/~nines/d.alumnos/novell/web4.htm>

http://www.10gea.org/10GEA%20White%20Paper_0502.pdf

<http://www.10gea.org/Tech-whitepapers.htm>

http://www.cisco.com/application/pdf/en/us/guest/products/ps4076/c1161/ccmigration_09186a0080088a25.pdf

<http://www.signus-web.com/networkers/documentos.html>

<http://cisco.netacad.net>

<http://www.redaccionvirtual.com/redaccion/glosario>

<http://www.ciscopress.com/>

<http://www.cisco.com>

<http://www.netsumbler.com/>

www.experts-exchange.com/Networking/Microsoft_Network