

INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA

UNIDAD CULHUACÁN

TESINA

Seminario de Titulación:
“Las tecnologías aplicadas en redes de computadoras”
DES/ESIME-CUL/5092005/10/2011

**Diseño de una red con infraestructura
económica para las nuevas tecnologías
y un mejor manejo de información**

Que como prueba escrita de su examen profesional para obtener el
Título de: Ingeniero en Comunicaciones y Electrónica.

Presentan:

Josué Jaime Rodríguez Grande
Oswaldo Calderón Vázquez
Lázaro Hernández Martínez



México D.F.

Enero 2012.

**INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD CULHUACAN
TESINA**

POR LA OPCIÓN DE	SEMINARIO DE TITULACIÓN DES/ESIME-CUL/5092005/10/11
QUE PARA OBTENER EL TÍTULO DE	INGENIERO EN COMUNICACIONES Y ELECTRÓNICA
PRESENTAN:	CALDERÓN VÁZQUEZ OSVALDO RODRÍGUEZ GRANDE JOSUE JAIME HERNÁNDEZ MARTÍNEZ LÁZARO

**DISEÑO DE UNA RED CON INFRAESTRUCTURA ECONÓMICA PARA LAS NUEVAS TECNOLOGÍAS
Y UN MEJOR MANEJO DE INFORMACIÓN**

IMPLEMENTAR EL DISEÑO E INFRAESTRUCTURA DE REDES DE VOIP Y DATOS PARA LA SECRETARÍA DE TURISMO DE LA DELEGACIÓN IZTACALCO, SE DECIDIÓ HACER ESTA IMPLEMENTACIÓN DE DISEÑO, SE PRETENDE DEMOSTRAR QUE AL REDISEÑAR Y ACTUALIZAR EQUIPOS SIMPLES SE PUEDE DAR UN SERVICIO DE CALIDAD Y SOBRE TODO DE A MUY BAJO COSTO POR LO QUE HAREMOS USO DE ALGUNOS EQUIPOS COMO ROUTER, SWITCHES, CABLEADO ESTRUCTURADO, TELÉFONOS IP'S Y SERVIDORES, SOFTWARE DE ADMINISTRACIÓN Y SEGURIDAD COMO SERIA EL ENDIAN, TODO ESTO PARA TENER UN MEJOR FUNCIONAMIENTO Y ADMINISTRACIÓN DE LA RED A BAJO COSTO.

CAPITULADO

INTRODUCCIÓN.

CAPÍTULO 1.- TIPOS DE REDES.
CAPÍTULO 2.- DISPOSITIVOS ETHERNET.
CAPÍTULO 3.- SISTEMAS DE CABLEADO ESTRUCTURADO.
CAPÍTULO 4.- TELEFONIA IP Y FIBRA ÓPTICA.
CAPÍTULO 5.- DISEÑO DE LA RED Y APLICACIÓN EN EL EDIFICIO DE GOBIERNO DE LA DELEGACIÓN IZTACALCO EN EL DEPARTAMENTO DE TURISMO.
CONCLUSIONES.
BIBLIOGRAFÍA.
GLOSARIO.

México D.F. 28 de Enero de 2011

M. en C. Diana Salomé Vázquez Estrada
Coordinador Académico del Seminario

M. en C. Antonio Romero Rojano
Jefe del Departamento de Ingeniería
en Comunicaciones y Electrónica

AGRADECIMIENTOS

A MIS PADRES: Ya que gracias a ellos y todos los sacrificios que han hecho por mi, he llegado hasta este punto en mi vida, ellos son los que me han forjado los cimientos de mi vida y son inspiración para seguir superando cualquier obstáculo, hoy como agradecimiento dedico este trabajo a ellos, sé que es poco lo que estoy brindando a comparación de lo que ellos me han dado.

Mil gracias por su apoyo.

A LOS PROFESORES: Que tuvieron que ver con el desempeño académico ya que son los que me han brindado un poco de sabiduría.

A TODOS: Los que estuvieron a mi lado en los momentos difíciles y demostraron su amistad.

GRACIAS

JOSUE.

Esta tesis, es un logro más en mi vida la cual solo no pudiese haber realizado, por tal motivo me gustaría agradecer esta tesis a las siguientes personas.

Primero y antes que nada, dar gracias a Dios, por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante toda mi vida y a través de mi carrera.

Agradecer hoy y siempre a mis hermanos, abuelos, tíos, primos a mis grandes amigos, y en especial a dos personas, a mi Padre Alejandro el cual quise y querré toda mi vida, fuiste mi inspiración y fortaleza, a mi madre Mariana la cual agradezco profundamente al apoyarme y luchar para sacar adelante mi carrera y hacer de mi una buena persona. Eres y serás la mejor madre.

Y por ultimo y no menos importantes a mis profesores, que sin su valiosa ayuda y enseñanza esto jamás hubiera sido posible concluir.

GRACIAS

OSVALDO.

A Dios creador del universo y dueño de mi vida que me permite construir otros mundos mentales posibles.

A mis padres, Maurilia Martínez Hernández y Camerino Hernández Morales, a pesar de la distancia siempre recibí el apoyo incondicional de ellos.

A mis hermanos por el apoyo que recibí de cada uno de ellos.

A Laura Azucena Montaña Torres por todo su cariño, amor y comprensión.

A mis maestros, M. en C. Diana Salomé Vázquez Estrada, Ing. Marcos Geraldo López Ixtla y a todos los demás maestros que tuvieron que ver en mi formación profesional.

MUCHAS GRACIAS.

LÁZARO.

ÍNDICE

INTRODUCCIÓN	1
CAPÍTULO I: TIPOS DE REDES	3
1.1 Clasificación de las redes	3
1.1.1 Subredes	3
1.1.2 Red LAN	3
1.1.3 Red WAN y redes globales	5
1.1.4 Red MAN	5
1.1.5 Red de CAMPUS	5
1.2 Modelo	5
1.3 Protocolo del modelo OSI	5
1.4 Topología de red basado en el modelo OSI	7
1.4.1 Topología de bus lineal	8
1.4.2 Topología en estrella	8
1.4.3 Anillo malla completa	10
CAPÍTULO II: DISPOSITIVOS ETHERNET.	11
2.1. Equipo centralizador de cableado (hubs)	11
2.2. Dispositivos de interconexión de redes. (bridges)	14
2.3. Elementos de interconectividad (switches)	16
2.4. Dispositivo de enlace entre redes (routers).	18
CAPÍTULO III: SISTEMAS DE CABLEADO ESTRUCTURADO.	22
3.1. Introducción	22
3.2. Tipos de cableado	24
3.2.1 Canalizaciones externas entre edificios	24
3.2.2. Canalizaciones subterráneas	25
3.3. Normatividad	25
3.3.1. Antecedentes normativos	25
3.3.2. Objetivos de TIA/EIA-568-b.	26
3.3.3. Cableado	26
3.4. Compatibilidad con versiones anteriores	28
3.4.1. Categoría de cableado	28

desde internet y desde la LAN permitir a la LAN.	71
5.6.3.3 Permitir a la WAN.	72
5.6.3.4 Acceso del servidor web al servidor SQL SERVER	72
5.7 Costos y beneficios de instalación	74
CONCLUSIÓN	76
BIBLIOGRAFÍA	77
PÁGINAS DE INTERNET	78
GLOSARIO DE TÉRMINOS Y ACRÓNIMOS	79

ÍNDICE DE FIGURAS

CAPÍTULO I

Figura 1.1 Muestra las capas del modelo OSI.	7
Figura 1.2. Muestra la topología de un bus lineal.	8
Figura 1.3 Muestra la topología estrella.	9
Figura 1.4 Muestra la topología malla completa.	10

CAPÍTULO II

Figura 2.1 Concentrador NETGEAR 10/100.	12
Figuras 2.2 a) Concentradores b) No Modulares.	14
Figura 2.3 switches.	15
Figura 2.4 Switch Advantek de NETWORK Vista lateral mostrando número de puertos RJ-45.	18
Figura 2.5 Conectividad entre Switches y sus terminales.	18
Figura 2.6 Conectividad entre Switches y sus terminales.	19

CAPÍTULO III

Tabla 3.1 Cableado RJ-45 (T568A/B).	27
Tabla 3.2 Cableado RJ-45 para TIA/EIA 568-B y TIA/EIA 568-A.	31

CAPÍTULO IV

Figura 4.1 Diagrama de conexión de telefonía VoIP.	33
Figura 4.2 Fibra multimodal.	40
Figura 4.3 Fibra multimodal con índice graduado.	40

CAPÍTULO V

Figura 5.1 Tomada desde las oficinas de la secretaria de turismo.	43
Figura 5.2 Tomada desde la parte de adentro de las instalaciones.	43
Figura 5.3 Equipo y cableado en techo.	44
Figura 5.4 Adentro de las instalaciones.	44
Figura 5.5 Dispositivo Huawei.	45
Figura 5.6 Dispositivo RouterNetgear N300.	45
Figura 5.7 Conmutador Avaya.	46

Figura 5.8 Teléfono digital Avaya.	46
Figura 5.9 Teléfono analógico Iusacell.	47
Figura 5.10 Servidores Poweredge 1900.	47
Figura 5.11 Servidores Poweredge 1900 por dentro.	47
Figura 5.12 Routers Cisco Systems 2600.	48
Figura 5.13 Switch Foundry FastIron edge4802.	48
Figura 5.14 Acces Point Wireless Linksys.	48
Figura 5.15 UPS.	49
Figura 5.16 El cableado que utilizaremos para montar la nueva infraestructura es RJ-45 y RJ-12 para voz.	49
Figura 5.17 Cable RJ-45 para datos.	50
Figura 5.18 RJ-12 cable para voz.	50
Figura 5.19 Cableado actual del rack y las escalerillas de la Secretaría de Turismo.	50
Figura 5.20 Primer diseño de la infraestructura.	51
Figura 5.21 Panorámica de las instalaciones con su respectivo diseño.	51
Figura 5.22 Equipo que tiene las oficinas y el diseño con el nuevo equipo.	52
Figura 5.23 Infraestructura vista desde la parte superior.	52
Figura 5.24 Validación acceso a Netgear.	53
Figura 5.25 Configuración básica.	54
Figura 5.26 Configuración de dirección IP.	54
Figura 5.27 Configuración de dirección del servidor.	55
Figura 5.28 Configuración dirección MAC.	55
Figura 5.29 Configuración inalámbrica.	55
Figura 5.30 Deshabilitamos la red inalámbrica.	56
Figura 5.31 Configuración LAN.	56
Figura 5.32 Configuración de DHCP.	57
Figura 5.33 Topología usando Endian Firewall.	58
Figura 5.34 Permiso de contenido.	60
Figura 5.35 Acceso a Endian Firewall.	60
Figura 5.36 Pantalla de Bienvenida Endian Firewall.	61
Figura 5.37 Pantalla de Bienvenida Endian Firewall	61

Figura 5.38 Aceptación de licencia.	62
Figura 5.39 Establecimiento de Backup.	62
Figura 5.40 Establecimiento user y password.	63
Figura 5.41 Tipo de Conexión.	64
Figura 5.42 Selección de las zonas de red.	64
Figura 5.43 Preferencias de red LAN VERDE.	65
Figura 5.44 Preferencias de red LAN NARANJA.	65
Figura 5.45 Preferencias de red LAN ROJO.	66
Figura 5.46 Configuración de DNS.	66
Figura 5.47 Pantalla de Guardar Cambios.	67
Figura 5.48 Establecimiento Configuración.	67
Figura 5.49 Alerta de Seguridad para el sitio Endian.	68
Figura 5.50 Requerimiento de contraseña para acceso.	68
Figura 5.51 Port forwarding / Destina.	69
Figura 5.52 Trafico de Firewall.	69
Figura 5.53 Port forwarding configuration.	70
Figura 5.54 Aplicación de cambios Port forwarding configuration.	71
Figura 5.55 Adición de reglas en Inter-Zonetraffic.	71
Figura 5.56 Configuración para permitir a la WAN.	72
Figura 5.57 Adición de reglas en Inter-Zonetraffic del servidor web al servido SQL server.	73
Figura 5.58 Paquete conexión 10	74
Tabla 5.1 Costos del proyecto	75

INTRODUCCIÓN

Las comunicaciones hoy en día representan más del 80% de las operaciones de una empresa, las crecientes necesidades de comunicación y actualización nos dan la base suficiente para encarar el diseño y construcción de la infraestructura necesaria para implementar una red de datos en una institución.

Con este proyecto pretendemos diseñar una red económica de infraestructura la cual nos sirva para modificar las redes que se han venido aplicando en nuestro país para modernizar las pequeñas y medianas empresas, además de crear una red más barata, poder otorgar medidas de seguridad más altas a bajos precios para una pronta actualización ya que en nuestro país urge actualizar las redes y modificarlas para las nuevas tecnologías.

Hemos observado que en las instituciones públicas aún se utiliza la telefonía analógica por lo tanto este servicio es muy costoso por lo que se propone realizar la actualización de redes telefónicas a través de telefonía fija de IP digital y analógica e Internet para reducir el costo a largo y corto plazo, y así reducir los problemas por mantenimiento.

Por ello se pretende demostrar que de llevar a cabo este proyecto en unas instalaciones pequeñas de gobierno como vendría siendo la Secretaria de Turismo de la delegación Iztacalco, se logre su mejor funcionamiento y eficiencia en los servicios que ofrecen para estar a la altura de grandes países en tecnología y comunicaciones a bajo costo además de actualizarlos.

CAPÍTULO I: TIPOS DE REDES.

1.1 CLASIFICACIÓN DE REDES.

Las redes de información se pueden clasificar según su extensión y su topología. Una red puede empezar siendo pequeña para crecer junto con la organización o institución. A continuación se presentan los distintos tipos de redes disponibles:

1.1.1 SUBREDES.

Un segmento de red suele ser definido por el "hardware" o una dirección de red específica. Por ejemplo, en el entorno "Novell NetWare", en un segmento de red se incluyen todas las estaciones de trabajo conectadas a una tarjeta de interfaz de red de un servidor y cada segmento tiene su propia dirección de red.

1.1.2 RED LAN.

Una LAN es un segmento de red que tiene conectadas estaciones de trabajo y servidores o un conjunto de segmentos de red interconectados, generalmente dentro de la misma zona. Por ejemplo un edificio.

Las redes LAN surgieron por la necesidad de compartir recursos entre las computadoras y los usuarios de las mismas, para hacer más eficiente, económico y administrable un sistema de cómputo, inicialmente se interconectaron de 4 a 5 computadoras utilizando un solo canal de transmisión

y recepción para todas las terminales. Las aplicaciones utilizadas eran no gráficas en D.O.S. (Disk Operative System, Sistema Operativo en Disco) y generalmente los archivos transmitidos eran texto en código ASCII. Las redes funcionaban bien con ésta poca demanda existente.

El problema se suscitó con la estructura del cableado, pues el uso de cable coaxial Ethernet o de un anillo Token Ring (Paso se Testigo), el añadir y mover usuarios se convirtió en una actividad de conexiones y empalmes defectuosos que ocasionaban problemas constantemente. Para dar solución se inventaron los concentradores que ofrecen al exterior una topología en forma de estrella manteniendo; ya sea el bus Ethernet o el anillo Token Ring en su interior. Esto dio solución a problemas ya que al añadir o mover usuarios consistía mover solo un cable y no todo un bus o un anillo, las aplicaciones se tornaron más complejas. Se integraron más usuarios y en consecuencia se demandaron más recursos de la red. El exceso de tráfico en un bus o en un anillo hizo a las redes muy lentas e ineficientes. La solución en parte, surgió con la invención de los bridges que permitieron dividir la red en segmentos al interconectarlos en la red con la siguiente división del tráfico.

Así surgió la necesidad de interconectar redes con diferentes topologías e identificarlas lógicamente para hacerlas administrables. Para resolver éstos problemas de conectividad surgieron ruteadores, que permiten dividir el tráfico, organizar segmentos lógicamente e interconectar redes de diferentes topologías.

Actualmente por la complejidad de las aplicaciones y los volúmenes de información que se transfieren de un punto a otro, han surgido tecnologías que ofrecen anchos de banda mayores y dedicados a cada usuario, denominados “connection oriented”, así como dispositivos que procesan el tráfico a mayor velocidad y eficiencia al internarse en el mundo del switcheo.

1.1.3 RED WAN Y REDES GLOBALES.

Las WAN (World Area Network, Red de Area Mundial) y redes globales se extienden sobrepasando las fronteras de las ciudades, pueblos o naciones. Los enlaces se realizan con instalaciones de telecomunicaciones públicas y privadas, además por microondas y satélites.

1.1.4 RED MAN.

Una red MAN “red de área metropolitana” es una red que se expande por pueblos o ciudades y se interconecta mediante diversas instalaciones públicas o privadas, como el sistema telefónico o los suplidores de sistemas de comunicación por microondas o medios ópticos.

1.1.5 RED DE CAMPUS.

Una red de campus se extiende a otros edificios dentro de un campus o área industrial. Los diversos segmentos o LAN (Local Area Network, Red de Area Local) de cada edificio suelen conectarse mediante cables de la red de soporte.

1.2 MODELO

Representa conceptos generales y guías de cómo se debe mover la información de un lugar a otro. Describe los servicios que deben ser proporcionados y que capa es responsable de hacerlo.

1.3 PROTOCOLO DEL MODELO OSI

Es un conjunto de reglas concernientes al hardware, procedimientos y estructuras de datos. Es el “plano” que siguen los desarrolladores para crear productos de hardware o software para que muevan información a través de una red o que provean servicios de red. Típicamente un protocolo trata con solo una capa del modelo.

A continuación se da una breve explicación de cada capa del modelo OSI para tener una mayor perspectiva de cuáles son las capas y cómo se relacionan.

1. **FÍSICO:** Se encarga de las características eléctricas, mecánicas, funcionales y de procedimiento que se requieren para mover los bits de datos entre cada extremo del enlace de la comunicación.
2. **ENLACE:** Asegura confiabilidad del medio de transmisión, ya que realiza la verificación de errores, retransmisión, control fuera del flujo y la secuenciación de las capacidades que se utilizan en la capa de red.
3. **RED:** Proporciona los medios para establecer, mantener y concluir las conexiones conmutadas entre los sistemas del usuario final. Por lo tanto, la capa de red es la más baja, que se ocupa de la transmisión de extremo a extremo.
4. **TRANSPORTE:** Ésta capa proporciona el control de extremo a extremo y el intercambio de información con el nivel que requiere el usuario. Representa el corazón de la jerarquía de los protocolos que permite realizar el transporte de los datos en forma segura y económica.
5. **SESIÓN:** Administra el diálogo entre las dos aplicaciones en cooperación mediante el suministro de los servicios que se necesitan para establecer la comunicación, flujo de datos y conclusión de la conexión.
6. **PRESENTACIÓN:** Permite a la capa de aplicación interpretar el significado de la información que se intercambia. Ésta realiza las conversiones de formato mediante las cuales se logra la comunicación de dispositivos.
7. **APLICACIÓN:** Se entiende directamente con el usuario final, al proporcionarle el servicio de información distribuida para soportar las aplicaciones y administrar las comunicaciones por parte de la capa de presentación.

Las 7 capas del modelo OSI

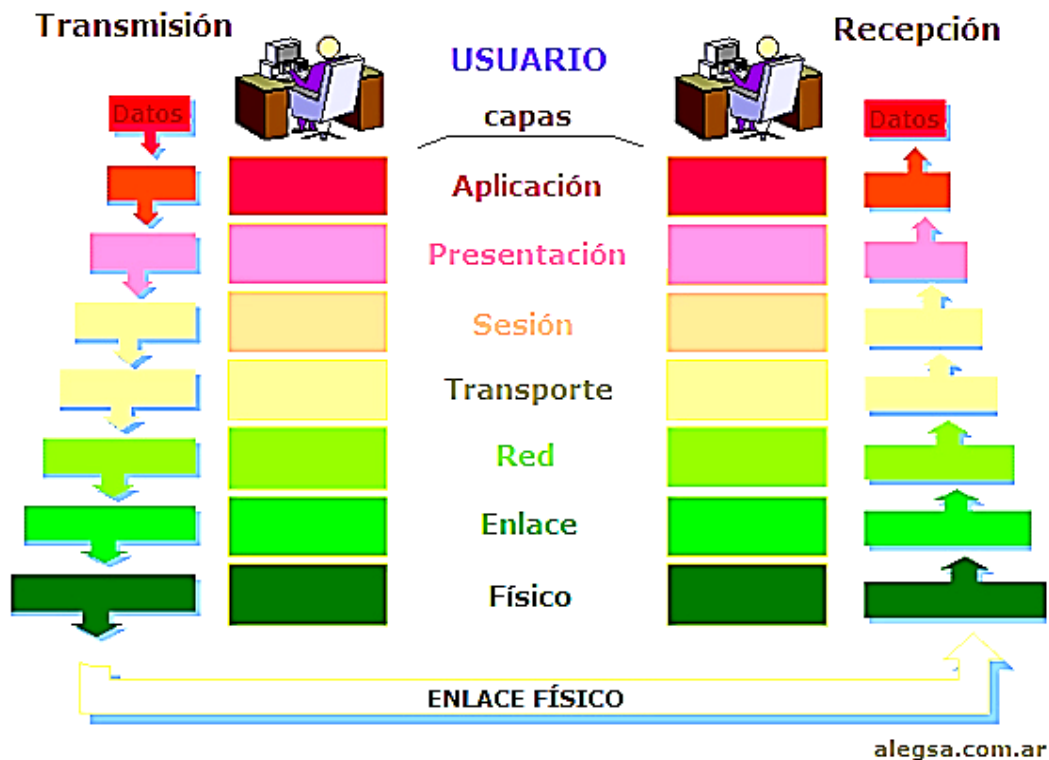


Figura 1.1 Muestra las capas del modelo OSI

1.4 TOPOLOGÍA DE RED BASADO EN EL MODELO OSI

Basándose en el modelo OSI nos situamos en el nivel de enlace de datos. Actualmente en el mundo de las redes hay numerosas topologías, entre las que destacan algunas que se han caracterizado por su rápida velocidad, flexibilidad y su tolerancia a fallas. De tal manera que las más usadas son:

- Bus lineal (Ethernet 10 MB).
- Estrella (Ethernet 10MB, Fast-Ethernet 100MB y Gigabit-Ethernet 1GB).
- Anillo Token Ring.
- Anillo Doble FDDI.

Se define un nodo como una computadora, no importa si es servidor de archivos o una estación de trabajo. Una topología define como los nodos se conectan entre sí.

1.4.1 TOPOLOGÍA DE BUS LINEAL.

Consiste de una Línea Troncal o Bus, a la que están conectadas todos los nodos. La señal viaja en ambas direcciones del cableado y es terminada en los extremos por una resistencia o terminador. Muchos nodos se pueden conectar al Bus y comenzar a comunicarse con los otros nodos en ese segmento de cable. Una ruptura en cualquier parte del cable causará que todo el segmento sea inoperable hasta que la ruptura se repare. Este tipo de topología es posible implementarla a través de cable coaxial. La velocidad de comunicación es de aproximadamente 10 Mbps.



Figura 1.2. Muestra la topología de un bus lineal

1.4.2 TOPOLOGÍA EN ESTRELLA

La topología en estrella es una topología de red muy común en las redes de computadoras. En su forma más simple, una topología en estrella consta de un Switch central, o Hub que actúa como un Router (Ruteador) para retransmitir los mensajes.

Consiste en un bus lineal que se encuentra de manera lógica dentro de un concentrador, al cual se conectan uno a uno los nodos formando una estrella. La principal ventaja de esta topología es la confiabilidad, si una estación falla o se desconecta, el concentrador restablece el Bus lineal, evitando así la caída

de la red. Este arreglo utiliza cable de par trenzado tipo UTP¹ o STP², para redes Ethernet a 100Mbps, dependiendo de la tecnología que maneje dicho dispositivo.

Cuando se aplica a redes basadas en Bus, este Hub central retransmite todas las transmisiones recibidas desde cualquier nodo periférico a todos los nodos periféricos de la red, a veces incluso al nodo original. Todos los nodos periféricos se pueden comunicar con los demás transmitiendo o recibiendo del nodo central solamente. Un fallo en la línea de conexión de cualquier nodo con el nodo central provocaría el aislamiento de ese nodo respecto a los demás, pero el resto de sistemas permanecería intacto.

Si el nodo central es pasivo, el nodo origen debe ser capaz de tolerar un eco de su transmisión. Una red en estrella activa tiene un nodo central activo que normalmente tiene los medios para prevenir problemas relacionados con el eco. Se utiliza sobre todo para redes locales. La mayoría de las redes de área local que tienen un Router, un Switch o un Hub siguen esta topología. El nodo central en estas sería el Hub, el Router o el Switch, por el que pasan todos los paquetes.



Figura 1.3 Muestra la topología estrella

¹Unshielded Twisted Par.

²Shielded Twisted Par.

1.4.3 ANILLO MALLA COMPLETA.

En una topología de malla completa, cada nodo se enlaza directamente con los demás nodos. Las ventajas son que, como nodo se conecta físicamente a los demás nodos, creando una conexión redundante, si algún enlace deja de funcionar la información puede circular a través de cualquier cantidad de enlaces hasta llegar a destino. Además, ésta topología permite que la información circule por varias rutas a través de la red. La desventaja física principal es que sólo funciona con una pequeña cantidad de nodos, ya que de lo contrario la cantidad de medios necesarios para los enlaces, y la cantidad de conexiones con los enlaces se torna abrumadora.



Figura 1.4 Muestra la topología malla completa

CAPÍTULO II: DISPOSITIVOS ETHERNET

2.1 EQUIPO CENTRALIZADOR DE CABLEADO (Hubs)

Un concentrador es un dispositivo que permite centralizar el cableado de una red. También conocido con el nombre de hub. Un concentrador funciona repitiendo cada paquete de datos en cada uno de los puertos con los que cuenta, excepto en el que ha recibido el paquete, de forma que todos los puntos tienen acceso a los datos. También se encarga de enviar una señal de choque a todos los puertos si detecta una colisión. Son la base para las redes de topología tipo estrella. Como alternativa existen los sistemas en los que los ordenadores están conectados en serie, es decir, a una línea que une varios o todos los ordenadores entre sí, antes de llegar al ordenador central. Llamado también repetidor multipuerto, existen 3 clases.

- Pasivo: No necesita energía eléctrica.
- Activo: Necesita alimentación.
- Inteligente: También llamados smarthubs son hubs activos que incluyen un microprocesador.

Dentro del modelo OSI el concentrador opera a nivel de la capa física, al igual que los repetidores, y puede ser implementado utilizando únicamente tecnología analógica. Simplemente une conexiones y no altera las tramas que le llegan.

Envía información a ordenadores que no están interesados. A este nivel sólo hay un destinatario de la información, pero para asegurarse de que la recibe el concentrador envía la información a todos los ordenadores que están conectados a él, así seguro que acierta. Este tráfico añadido genera más probabilidades de colisión. Una colisión se produce cuando un ordenador quiere enviar información y emite de forma simultánea con otro ordenador que hace lo mismo. Al chocar los dos mensajes se pierden y es necesario retransmitir. Además, a medida que añadimos ordenadores a la red también aumentan las probabilidades de colisión.



Figura 2.1 Concentrador NETGEAR 10/100

Funciona a la velocidad del dispositivo más lento de la red. Si observamos cómo funciona vemos que el concentrador no tiene capacidad de almacenar nada. Por lo tanto si un ordenador que emite a 100Mbps le transmitiera a otro de 10Mbps algo se perdería del mensaje. En el caso del ADSL los routers suelen funcionar a 10Mbps, si lo conectamos a nuestra red casera, toda la red funcionará a 10Mbps, aunque nuestras tarjetas sean 10/100Mbps.

Se considera un dispositivo simple debido a esto influye en dos características importantes. El precio es barato. Un concentrador casi no añade ningún retardo a los mensajes.

Los fueron muy populares hasta que se abarataron los switch que tienen una función similar pero proporcionan más seguridad contra programas como los sniffer. La disponibilidad de switches ethernet de bajo precio ha dejado

obsoletos, pero aún se pueden encontrar en instalaciones antiguas y en aplicaciones especializadas.

Las especificaciones del estándar IEEE 802.3 describen reglas para el número máximo de repetidores que se pueden encontrar entre dos nodos, éste es de cuatro; por otro lado el número máximo de segmentos de red entre dos nodos es de cinco, con una restricción adicional de que no más de tres de estos cinco segmentos pueden tener estaciones conectadas, los otros segmentos deben ser uniones entre concentradores las cuales solo conectan concentradores, éstas reglas se determinan mediante cálculos de longitudes máximas de cables y retardos en los concentradores.

Las redes que violan éstas reglas podrían seguir funcionando, pero están expuestas a fallas esporádicas o problemas frecuentes de naturaleza indeterminada. Además, el uso de repetidores simplemente extiende el tamaño de la red y a medida que va creciendo, el ancho de banda en la red podría llegar a ser un problema. En este caso, se pueden utilizar switches, bridges y routers para partir una red grande en muchos segmentos pequeños y más eficientes.

Existe en el mercado una gran cantidad de fabricantes que ofrecen concentradores inteligentes, básicamente se dividen en dos grupos: los “no modulares y los Modulares”. Los no modulares son utilizados para pequeños grupos de trabajo que pueden ser interconectados entre sí y que soportan un solo producto como Ethernet, Token ring, FDDI o ATM. Los Modulares son concentradores que permiten integrar en un solo chasis, varios métodos de acceso y múltiples protocolos como Ethernet, Token ring y FDDI; y que además permiten integrar dispositivos adicionales para dar interconectividad a la red y servicios adicionales como bridges, routers, switches, conexiones a host, servidores en el mismo chasis. Estos concentradores trabajan a través de módulos que cumplen una función específica.



Figuras 2.2 a) Concentradores No Modulares b) Concentrador Modular

2.2 DISPOSITIVOS DE INTERCONEXIÓN DE REDES. (Bridges)

Un puente o bridge es un dispositivo de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Éste interconecta dos segmentos de red (o divide una red en segmentos) haciendo el pasaje de datos de una red para otra, con base en la dirección física de destino de cada paquete. Son dispositivos que incrementan el desempeño de una red LAN, al filtrar frames entre segmentos de la red definidos con base en direcciones de hardware. Un bridge conecta dos segmentos de red como una sola red usando el mismo protocolo de establecimiento de red.

Si se tienen múltiples dispositivos conectados a una sola LAN de tal forma que por su número y por la demanda de servicios de la red impacten negativamente en su eficiencia, se necesita dividir la LAN en segmentos interconectados mediante los puentes.

Estos dispositivos usualmente interconectan medios iguales de acceso, es decir, Ethernet con Ethernet y Token ring con Token ring; pero por definición pueden conectar medios diferentes también. Sin embargo esto no es usual, ya que no representa una implementación sencilla.

En la capa de enlace de datos, las señales en el cable están organizadas en frames llamados Media Access Control (MAC). Los encabezados de los frames contienen información acerca de las direcciones de origen y destino del frame.

Los puentes tienen la capacidad de filtrar el tráfico entre segmentos LAN basándose en estas direcciones.

Funcionan a través de una tabla de direcciones MAC detectadas en cada segmento a que está conectado. Cuando detecta que un nodo de uno de los segmentos está intentando transmitir datos a un nodo del otro, el bridge copia la trama para la otra subred. Por utilizar este mecanismo de aprendizaje automático, los bridges no necesitan configuración manual.

La principal diferencia entre un bridge y un hub es que el segundo pasa cualquier trama con cualquier destino para todos los otros nodos conectados, en cambio el primero sólo pasa las tramas pertenecientes a cada segmento. Esta característica mejora el rendimiento de las redes al disminuir el tráfico inútil.

Cuando se diseña una LAN con puentes, una buena regla es seguir un tráfico 80/20, es decir 80% del tráfico debe ser local (en el segmento) y 20% debe pasar entre segmentos. Los puentes trabajan independientemente de las capas superiores a la capa de enlace de datos del modelo OSI. Esto significa que no importa qué tipo de protocolos sean utilizados en el área de datos del frame, ya que estos datos no afectan la forma en que los frames son filtrados. Para hacer el bridging o interconexión de más de 2 redes, se utilizan los switches.

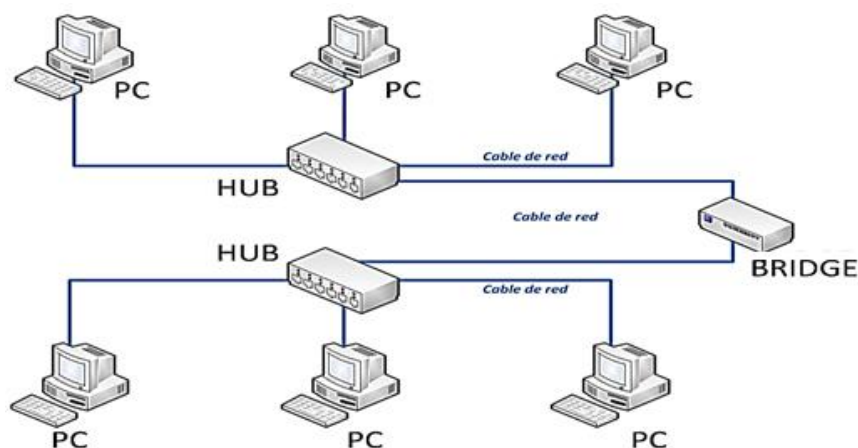


Figura 2.3 switches

2.3 ELEMENTOS DE INTERCONECTIVIDAD (Switches)

Un conmutador o switch es un dispositivo electrónico de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Un conmutador interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.

Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LANs.

Un switch local es un dispositivo inteligente que permite la interconexión de redes de uno o diferentes protocolos, dando capacidades de segmentación en las redes.

Los switch Ethernet tuvieron su desarrollo inicial en 1991, como una forma de segmentar y hacer más eficiente la comunicación entre diferentes segmentos de Ethernet en la búsqueda de mejorar la velocidad de filtrado y de aceptación, surgió la idea de que el tiempo requerido para determinar si un paquete debía ser filtrado o aceptado (“tiempo de Latencia”) se podría reducir si solo se examinara la información de direcciones contenida al inicio del frame Ethernet. Los dispositivos que empezaron a usar éste tipo de tecnología fueron llamados “cut-through”. Básicamente un switch es un Puente Multipuerto de alto desempeño, diseñado para incrementar el desempeño de una Red de Área local.

Los conmutadores poseen la capacidad de aprender y almacenar las direcciones de red de nivel 2 (direcciones MAC) de los dispositivos alcanzables a través de cada uno de sus puertos. Por ejemplo, un equipo conectado directamente a un puerto de un conmutador provoca que el conmutador almacene su dirección MAC. Esto permite que, a diferencia de los concentradores o hubs, la información dirigida a un dispositivo vaya desde el puerto origen al puerto destino. En el caso de conectar dos conmutadores o un

conmutador y un concentrador, cada conmutador aprenderá las direcciones MAC de los dispositivos accesibles por sus puertos, por tanto en el puerto de interconexión se almacenan las MAC de los dispositivos del otro conmutador.

Como anteriormente se comentaba, uno de los puntos críticos de estos equipos son los bucles (ciclos) que consisten en habilitar dos caminos diferentes para llegar de un equipo a otro a través de un conjunto de conmutadores. Los bucles se producen porque los conmutadores que detectan que un dispositivo es accesible a través de dos puertos emiten la trama por ambos. Al llegar esta trama al conmutador siguiente, este vuelve a enviar la trama por los puertos que permiten alcanzar el equipo. Este proceso provoca que cada trama se multiplique de forma exponencial, llegando a producir las denominadas inundaciones de la red, provocando en consecuencia el fallo o caída de las comunicaciones.

Los switch ofrecen los beneficios de los puentes, con mejores ventajas, los switches son más rápidos, incrementan la capacidad, permiten la segmentación, las conversaciones en paralelo y seleccionar el tipo de conexión hacia la LAN. Además desde que se implementaron en el Nivel 2 de la capa del modelo OSI, son más simples de administrar y de dar mantenimiento.

Aunque los conmutadores o switches son los elementos que fundamentalmente se encargan de encaminar las tramas de nivel 2 entre los diferentes puertos, existen los denominados conmutadores de nivel 3 o superior, que permiten crear en un mismo dispositivo múltiples redes de nivel 3 (Redes Virtuales o VLANs) y encaminar los paquetes (de nivel 3) entre las redes, realizando por tanto las funciones de encaminamiento o routing.

Actualmente los fabricantes de switches utilizan diversas técnicas de conmutación destacando las principales: Store and Forward, Cut-Through y Cell Backplane.



Figura 2.4 SwitchA dvantek de NETWORK. Vista lateral mostrando número de puertos RJ-45.

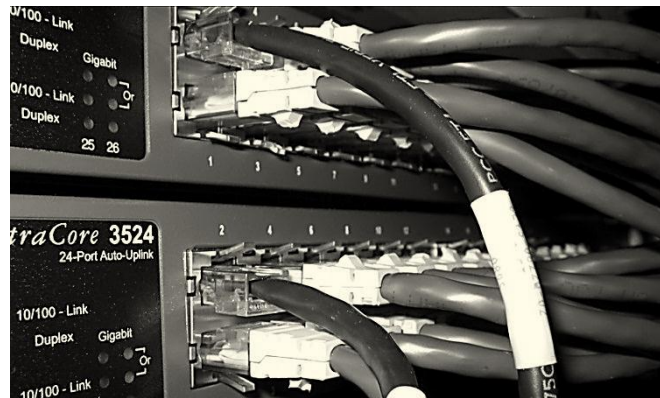


Figura 2.5 Conectividad entre Switches y sus terminales.

- Tipos de Conectividad de los Switches:
- 10BASE-T, 10BASE-F.
- 100BASE-T, 100 VG-AnyLAN.
- FDDI.
- Gigabit Ethernet.
- Usualmente una combinación de las tecnologías de 10 y 100Mbps, ATM y Gigabit Ethernet.

2.4 DISPOSITIVO DE ENLACE ENTRE REDES (Routers).

Los ruteadores alivian muchos los problemas de puenteo en las LANs, creando una red interna jerárquica dividida en subredes, donde cada una comprende un segmento de LAN comprimido o un grupo de segmentos puenteados. Actualmente, los Ruteadores empleados en ambientes LAN crean mucha latencia entre nodos de comunicación, teniendo un impacto negativo en los tiempos de respuesta. La latencia introducida por los ruteadores se deriva del hecho de que un ruteador envía tráfico entre subredes basándose en la tabla

de direcciones de red y que modifica el encabezado del paquete antes de que pueda ser enviado a su puerto de destino, ya que un router IP puede dividir una red en varias subredes de tal manera que sólo el tráfico destinado a ciertas direcciones IP pueda pasar entre los segmentos.

Los routers tienen acceso a la información de las tres capas inferiores del modelo OSI, es decir, a la capa Física, de Enlace de Datos y de Red. La información de la capa 3 generalmente incluye lo que se denomina un direccionamiento lógico de red. El direccionamiento físico no es asignado por el administrador de la red, mientras que el direccionamiento lógico si lo puede ser. Ésta es la diferencia básica entre un puente y un router.

Las direcciones físicas son asignadas por el fabricante del equipo (con excepción de los arreglos Arcnet), por lo que tienen una asociación más fuerte con un fabricante en particular que con el uso de las direcciones lógicas. El administrador puede usar los direccionamientos lógicos para asociar un grupo de equipos con alguna característica en común, como puede ser en un área departamental de un edificio. Éstas direcciones proporcionan la flexibilidad que un direccionamiento físico no tiene, sencillamente porque estos pueden ser agrupados jerárquicamente y cambiarse más fácilmente.

Los routers envían información a través de la parte interna de la red usando información de direcciones lógicas en lugar de físicas. Las subdivisiones de una red lógica a menudo son llamadas subredes (subnetworks o subnets). Una subred puede o no trazarse o mapearse directamente a un solo elemento físico.

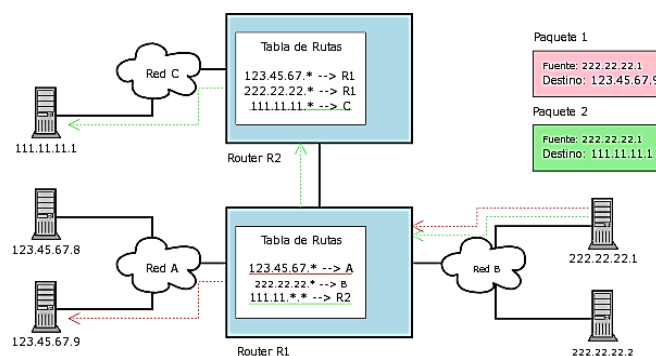


Figura 2.6 Conectividad entre Switches y sus terminales

En el ejemplo del diagrama, se muestran 3 redes IP interconectadas por 2 routers. La computadora con el IP 222.22.22.1 envía 2 paquetes, uno para la computadora 123.45.67.9 y otro para 111.11.11.1 A través de sus tablas de enrutamiento configurados previamente, los routers pasan los paquetes para la red o router con el rango de direcciones que corresponde al destino del paquete. Nótese que el contenido de las tablas de rutas está simplificado por motivos prácticos, en realidad se utilizan máscaras de red para definir las subredes interconectadas.

Los protocolos de enrutamiento son aquellos protocolos que utilizan los routers o encaminadores para comunicarse entre sí y compartir información que les permita tomar la decisión de cuál es la ruta más adecuada en cada momento para enviar un paquete. Los protocolos más usados son RIP (v1 y v2), OSPF (v1, v2 y v3), y BGP (v4), que se encargan de gestionar las rutas de una forma dinámica, aunque no es estrictamente necesario que un router haga uso de estos protocolos, pudiéndosele indicar de forma estática las rutas (camino a seguir) para las distintas subredes que estén conectadas al dispositivo.

Comúnmente los routers se implementan también como puertas de acceso a Internet (por ejemplo un router ADSL), usándose normalmente en casas y oficinas pequeñas. Es correcto utilizar el término router en este caso, ya que estos dispositivos unen dos redes (una red de área local con Internet).

Como resulta obvio, la función de los ruteadores es comúnmente más demandante de proceso que la de los puentes. Como resultado, sus velocidades de proceso no son tan altas. Por otra parte, son capaces de una selección de ruta mucho más sofisticada basada en estos protocolos de ruteo. La decisión de adquirir un puente o un ruteador depende de las necesidades de cada administrador de red y del ambiente de la misma.

Gracias a los protocolos de ruteo, los ruteadores son capaces de construir tablas con todas las rutas posibles, así como todas las direcciones de las redes que interconectan. Para intercambiar estas tablas los protocolos de ruteo pueden funcionar usando un algoritmo de vector o de estado de enlace.

Los protocolos de vector distancia, como IP-RIP o IPX-RIP, intercambian todas las tablas entre todos los ruteadores en una base temporal, típicamente cada 60 segundos. Forman la decisión de cual ruta tomar de acuerdo a aquella que represente el menor número de pasos intermedios por ruteadores o por el tiempo que toma un paquete en llegar a esa red (Hop Count o Tic Count). Los protocolos de estado del enlace como OSPF-IP o IPX-NLSP, intercambian sus tablas de ruteo solo cuando existe un cambio en la topología de la red, como puede ser la caída de un enlace o una nueva red que es conectada, reduciendo notoriamente el tráfico.

CAPÍTULO III: SISTEMAS DE CABLEADO ESTRUCTURADO.

3.1 INTRODUCCIÓN

A medida que las tecnologías de los sistemas informáticos comenzaron a madurar, más y más organizaciones y empresas comenzaron a requerir de estos sistemas, cada uno de los que requería de su tipo de cable, conectores, y prácticas de instalación. Los clientes comenzaron a quejarse, ya que con cada cambio tecnológico en sus sistemas de información también debían cambiar el cableado.

En 1985, la CCIA (Computer Communications Industry Association) solicitó a la EIA (Electronic Industries Alliance) realizar un estándar referente a los sistemas de cableado. En esa fecha se entendió que era necesario realizar un estándar que contemplara todos los requerimientos de cableado de los sistemas de comunicaciones, incluyendo voz y datos, para el área corporativa (empresarial) y residencial.

La EIA asignó la tarea de desarrollar estándares de cableado al comité "TR-41". El foco principal del comité al desarrollar estos estándares consistió en asegurarse de que eran independientes tanto de las tecnologías de los sistemas de comunicaciones como de los fabricantes.

Si se está considerando conectar equipos de cómputo y de comunicaciones a un sitio central desde el cual pueda administrarlos, enlazar sus centros de

comunicaciones dispersos en su área geográfica o suministrar servicios de alta velocidad a sus computadoras de escritorio, debe pensar en el diseño e implementación de infraestructuras de fibra y cableados que cumplirán con éxito todas sus demandas de voz, datos y video. Los sistemas de cableado estructurado constituyen una plataforma universal por donde se transmiten tanto voz como datos e imágenes y constituyen una herramienta imprescindible para la construcción de edificios modernos o la modernización de los ya construidos. Ofrece soluciones integrales a las necesidades en lo que respecta a la transmisión confiable de la información, por medios sólidos; de voz, datos e imagen. La instalación de cableado estructurado debe respetar las normas de construcción internacionales más exigentes para datos, voz y eléctricas tanto polarizadas como de servicios generales, para obtener así el mejor desempeño del sistema.

El cableado estructurado consiste en el tendido de cables en el interior de un edificio con el propósito de implantar una red de área local. Suele tratarse de cable de par trenzado de cobre, para redes de tipo IEEE 802.3. No obstante, también puede tratarse de fibra óptica o cable coaxial.

El tendido de cable para una red de área local tiene cierta complejidad cuando se trata de cubrir áreas extensas tales como un edificio de varias plantas. En este sentido hay que tener en cuenta las limitaciones de diseño que impone la tecnología de red de área local que se desea implantar:

- La segmentación del tráfico de red.
- La longitud máxima de cada segmento de red.
- La presencia de interferencias electromagnéticas.
- La necesidad de redes locales virtuales.

Salvando estas limitaciones, la idea del cableado estructurado es simple:

- Tender cables en cada planta del edificio.
- Interconectar los cables de cada planta.

3.2 TIPOS DE CABLEADO

CABLEADO HORIZONTAL O "DE PLANTA". En cada planta se instalan las rosetas (terminaciones de los cables) que sean necesarias en cada dependencia. De estas rosetas parten los cables que se tienden por el falso suelo (o por el falso techo) de la planta.

Todos los cables se concentran en el denominado armario de distribución de planta. Se trata de un bastidor donde se realizan las conexiones eléctricas (o "empalmes") de unos cables con otros. En algunos casos, según el diseño que requiera la red, puede tratarse de un elemento activo o pasivo de comunicaciones, es decir, un Hub o un Switch. En cualquier caso, este armario concentra todos los cables procedentes de una misma planta.

CABLEADO VERTICAL O "TRONCAL" (BACKBONE). Por último solamente nos queda interconectar todos los armarios de distribución de planta mediante otro conjunto de cables que deben atravesar verticalmente el edificio de planta a planta. Esto se hace a través de las canalizaciones existentes en el edificio. Si esto no es posible, es necesario habilitar nuevas canalizaciones, aprovechar aberturas existentes (huecos de ascensor o escaleras), o bien, utilizar la fachada del edificio (poco recomendable). Estos cables acaban en una sala donde, de hecho, se concentran todos los cables del edificio. Aquí se sitúa la electrónica de red y otras infraestructuras de telecomunicaciones, tales como pasarelas, puertas de enlace, cortafuegos, etc., así como el propio Centro de proceso de datos (si se aplica).

3.2.1 CANALIZACIONES EXTERNAS ENTRE EDIFICIOS

Las canalizaciones externas entre edificios son necesarias para interconectar "Instalaciones de Entrada" de varios edificios de una misma corporación, en ambientes del tipo "campus". La recomendación ANSI/TIA/EIA-569 admite, para estos casos, cuatro tipos de canalizaciones: Subterráneas, directamente enterradas, aéreas, y en túneles.

3.2.2 CANALIZACIONES SUBTERRÁNEAS

Las canalizaciones subterráneas consisten en un sistema de ductos y cámaras de inspección. Los ductos deben tener un diámetro mínimo de 100 mm (4 "). No se admiten más de dos quiebres de 90 grados.

3.3 NORMATIVIDAD

TIA/EIA-568-B tres estándares que tratan el cableado comercial para productos y servicios de telecomunicaciones. Los tres estándares tienen los siguientes títulos oficiales: ANSI/TIA/EIA-568-B.1-2001, -B.2-2001 y -B.3-2001. Los estándares TIA/EIA-568-B se publicaron por primera vez en 2001. Sustituyen al conjunto de estándares TIA/EIA-568-A que han quedado obsoletos.

Tal vez la característica más conocida del TIA/EIA-568-B.1-2001 sea la asignación de pares/pines en los cables de 8 hilos y 100 ohmios (Cable de par trenzado). Esta asignación se conoce como T568A y T568B, y a menudo es nombrada (erróneamente) como TIA/EIA-568A y TIA/EIA-568B.

3.3.1 ANTECEDENTES NORMATIVOS.

El estándar TIA/EIA-568-B se desarrolló gracias a la contribución de más de 60 organizaciones, incluyendo fabricantes, usuarios finales, y consultoras. Los trabajos para la estandarización comenzaron en 1985, cuando la Asociación para la Industria de las Comunicaciones y las Computadoras (CCIA) solicitó a la Alianza de Industrias de Electrónica (EIA), una organización de Normalización, que definiera un estándar para el cableado de sistemas de telecomunicaciones. EIA acordó el desarrollo de un conjunto de estándares, y se formó el comité TR-42, con nueve subcomités para desarrollar los trabajos de estandarización.

La primera revisión del estándar, TIA/EIA-568-A.1-1991, se emitió en 1991 y fue actualizada en 1995. La demanda comercial de sistemas de cableado aumentó fuertemente en aquel período, debido a la aparición de los ordenadores personales y las redes de comunicación de datos, y a los avances en estas tecnologías. El desarrollo de cables de pares cruzados de altas

prestaciones y la popularización de los cables de fibra óptica, conllevaron cambios importantes en el estándar, que fue sustituido por el actual conjunto de estándares TIA/EIA-568-B

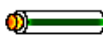

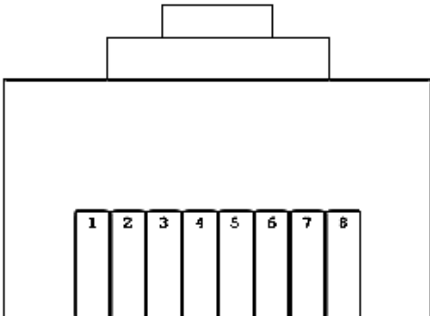











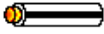

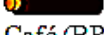
3.3.2 OBJETIVOS DE TIA/EIA-568-B.

La intención de estos estándares es proveer una serie de prácticas recomendadas para el diseño e instalación de sistemas de cableado que soporten una amplia variedad de los servicios existentes, y la posibilidad de soportar servicios futuros que sean diseñados considerando los estándares de cableado. El estándar pretende cubrir un rango de vida de más de diez años para los sistemas de cableado comercial. Este objetivo ha tenido éxito en su mayor parte, como se evidencia con la definición de cables de categoría 5 en 1991, un estándar de cable que satisface la mayoría de requerimientos para 1000BASE-T, emitido en 1999. Por tanto, podemos decir que el proceso de estandarización ha proporcionado al menos un período de nueve años (probablemente más) para el cableado de edificios.

3.3.3 CABLEADO

Respecto al estándar de conexión, los pines en un conector RJ45 modular están numerados del 1 al 10, siendo el pin 1 el del extremo izquierdo de conector, y el pin 10 el del extremo derecho. Los pines del conector hembra (jack S.) se numeran de la misma manera para que coincidan con ésta numeración, siendo el pin 1 el del extremo derecho y el pin 8 el del extremo izquierdo. La asignación de pares de cables son como sigue:

Tabla 3.1 Cableado RJ-45 (T568A/B)

Pin	Color T568A	Color T568B	Pines en conector macho (hembra invertidos)
1	 Blanco/Verde (W-G)	 Blanco/Naranja (W-O)	
2	 Verde (G)	 Naranja (O)	
3	 Blanco/Naranja (W-O)	 Blanco/Verde (W-G)	
4	 Azul (BL)	 Azul (BL)	
5	 Blanco/Azul (W-BL)	 Blanco/Azul (W-BL)	
6	 Naranja (O)	 Verde (G)	
7	 Blanco/Café (W-BR)	 Blanco/Café (W-BR)	
8	 Café (BR)	 Café (BR)	

Nótese que la única diferencia entre T568A y T568B es que los pares 2 y 3 (Naranja y Verde) están alternados. Ambos estándares conectan los cables "directamente", es decir, los pines 1 a 8 de cada extremo se conectan con los pines 1 a 8, respectivamente, en el otro. Asimismo, los mismos pares de cables están emparejados en ambos estándares: pines 1-2, 3- 6, 4-5 y 7-8. Y aunque muchos cables implementan pequeñas diferencias eléctricas entre cables, estos efectos son inapreciables, de manera que los cables que utilicen cualquier estándar son intercambiables.

3.4 COMPATIBILIDAD CON VERSIONES ANTERIORES

Debido a que el cable 1 se conecta con los pines centrales (4 y 5) del conector RJ-45 en ambos estándares T568A y T568B, ambos estándares son compatibles en la primera línea de conectores RJ-11, RJ-14, R-45, RJ-25 y RJ-61 que tienen el primer par en el centro de estos conectores.

Si la segunda línea de un conector RJ-14, RJ-25 o RJ-61 es usada, se conecta con el segundo par (naranja/blanco) de los conectores cableados a un T568A pero el par 3 (verde/blanco) en conectores cableados con el estándar T568B. Esto hace al estándar T568B potencialmente confuso en aplicaciones telefónicas.

3.4.1 CATEGORÍA DE CABLEADO.

Cable de Categoría 1 (Cat 1), también llamado cobre de grado de voz es un grado de cable UTP definido por el estándar TIA/EIA-568-B creado por la Electronic Industries Alliance (Alianza de Industrias Electrónicas o EIA) y la Telecommunications Industry Association (Asociación de la Industria de Telecomunicaciones o TIA). El Cable de Categoría 1 fue diseñado para comunicaciones telefónicas.

Cable de Categoría 2 (Cat 2), es un tipo de cable de par trenzado no protegido (unshielded) definido por el estándar TIA/EIA-568-B. Esta categoría de cable es capaz de transmitir datos hasta 4 Mbit/s. Generalmente ya dejó de ser usado.

Cable de Categoría 3 (Cat 3), es un cable de par trenzado diseñado para transportar fielmente data de hasta 10 Mbit/s, con un posible ancho de banda de 16 MHz. Es parte de una familia de estándares de cables de cobre definido en conjunto por la Electronic Industries Alliance y la Telecommunications Industry Association. La Categoría 3 fue un popular formato de cableado entre administrador de redes en los comienzos de los noventa, pero cayó en popularidad contra el similar pero superior estándar de Cable de Categoría 5.

Actualmente, la mayoría de cableados se encuentran hechos en Cat 5 o Cat 6, pero se mantiene el uso en sistemas de telefonía de 2 líneas, incluso a pesar de que Cat 5 o 6 facilitaría la migración a VOIP.

Cable de Categoría 4 (Cat 4), es una descripción no estandarizada de cable que consiste en 4 cables UTP con una velocidad de datos de 16 Mbit/s y una performance de hasta 20 MHz. Fue usado en redes Token Ring, 10BASE-T, 100BASE-T4, y ya ha dejado de estar en uso masivo. Fue rápidamente reemplazado el Cable de Categoría 5/5e, los cuales poseen 100 ± 15 Ohmios de impedancia.

Cable de Categoría 5 (Cat 5), es una de las cinco clases de cableado UTP que se describen en el estándar TIA/EIA-568-B. El cableado de categoría 5 se usa para ejecutar CDDI y puede transmitir datos a velocidades de hasta 100 Mbps.

Está diseñado para señales de alta integridad. Estos cables pueden ser blindados o sin blindar. Este tipo de cables se utiliza a menudo en redes de ordenadores como Ethernet, y también se usa para llevar muchas otras señales como servicios básicos de telefonía, Token Ring, y ATM.

Cable de Categoría 6 (Cat 6), (ANSI/TIA/EIA-568-B.2-1) es un estándar de cables para Gigabit Ethernet y otros protocolos de redes que es backward compatible (compatible con versiones anteriores) con los estándares de Categoría 5/5e y Categoría 3. La Categoría 6 posee características y especificaciones para crosstalk y ruido. El estándar de cable es utilizable para 10BASE-T, 100BASE-TX y 1000BASE-TX (Gigabit Ethernet). Provee performances de hasta 250 MHz. El cable contiene 4 pares de cable de cobre trenzado, al igual que estándares de cables de cobre anteriores. Aunque la Categoría 6 está a veces hecha con cable 23 gauge, esto no es un requerimiento; la especificación ANSI/TIA-568-B.2-1 aclara que el cable puede estar hecho entre calibre 22 y 24, mientras que el cable cumpla todos los estándares de pruebas indicados.

Cuando es usado como un patch cable, Cat-6 es normalmente terminado con fichas eléctricas RJ-45, a pesar de que algunas cables Cat-6 son incómodos









para ser terminados de tal manera sin piezas modulares especiales y esta práctica no cumple con el estándar. Si los componentes de los varios estándares de cables son mezclados entre sí, el desempeño de la señal quedará limitada a la menor categoría que todas las partes cumplan. Como todos los cables definidos por TIA/EIA-568-B, el largo máximo de un cable Cat-6 horizontal es de 90 metros (295 pies). Un canal completo (cable horizontal más cada final) está permitido a llegar a los 100 metros en extensión.

Los cables UTP Cat-6 comerciales para redes LAN, son eléctricamente construidos para exceder la recomendación del grupo de tareas de la IEEE, que está trabajando desde antes de 1997.





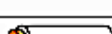



La TIA está trabajando para completar una nueva especificación que definirá estándares de performance mejorados para sistemas con cables cruzados sin protección (unshielded). La especificación ANSI/TIA/EIA-568-B.2-10 indica sistemas de cables llamados Categoría 6 Aumentada o mas frecuentemente "Categoría 6a", que operan a frecuencias de hasta 500 MHz (tanto para cables shielded como unshielded) y proveerán transferencias de hasta 10 GBit/s. La nueva especificación tiene límites en sistemas de cableado aliencrosstalk. Soporta una distancia máxima de 100 metros en un canal de 4 conectores.

Tabla 3.2 Cableado RJ-45 para TIA/EIA 568-B y TIA/EIA 568-A

RJ-45 Wiring (TIA/EIA-568-B T568A)

Pin	Par	Cable	Color
1	3	1	 blanco/verde
2	3	2	 verde
3	2	1	 blanco/naranja
4	1	2	 azul
5	1	1	 blanco/azul
6	2	2	 naranja
7	4	1	 blanco/marrón
8	4	2	 marrón

RJ-45 Wiring (TIA/EIA-568-A T568B)

Pin	Par	Cable	Color
1	2	1	 blanco/naranja
2	2	2	 naranja
3	3	1	 blanco/verde
4	1	2	 azul
5	1	1	 blanco/azul
6	3	2	 verde
7	4	1	 blanco/marrón
8	4	2	 marrón

El Cable de Categoría 7 (Cat 7), (ISO/IEC 11801:2002 categoría7/claseF), es un estándar de cable para Ethernet y otras tecnologías de interconexión que puede hacerse compatible hacia atrás con los tradicionales de Ethernet actuales Cable de Categoría 5 y Cable de Categoría 6. El Cat 7 posee especificaciones aún más estrictas para Crosstalk y ruido en el sistema que Cat 6. Para lograr esto, blindaje ha sido agregado para pares de cable individuales y para el cable entero.

El estándar Cat 7 fue creado para permitir 10 Gigabit Ethernet sobre 100 metros de cableado de cobre. El cable contiene, como los estándares anteriores, 4 pares cruzados de cobre. Cat 7 puede ser terminado tanto con un conector eléctrico GG-45 (compatible con RJ-45) como con un conector TERA. Cuando se combina con éstos, el Cat 7 puede transmitir frecuencias de hasta 600MHz

CAPÍTULO IV: TELEFONÍA IP Y FIBRA ÓPTICA.

4.1 INTRODUCCIÓN

La telefonía IP conjuga dos mundos históricamente separados: la transmisión de voz y la de datos. Se trata de transportar la voz, previamente convertida a datos, entre dos puntos distantes. Esto posibilitará utilizar las redes de datos para efectuar las llamadas telefónicas, y yendo un poco más allá, a desarrollar una única red que se encargue de usar todo tipo de comunicación, ya sea voz o de datos.

Es evidente que el hecho de tener una red en vez de dos, es beneficioso para cualquier operador que ofrezca ambos servicios.

4.2 ¿QUÉ ES VoIP (VOICEOVER INTERNET PROTOCOL)?

La VoIP proviene del inglés VoiceOver Internet Protocol, que significa "voz sobre un protocolo de internet". Básicamente VoIP es un método por el cual tomando señales de audio analógicas del tipo de las que se escuchan cuando uno habla por teléfono se las transforma en datos digitales que pueden ser transmitidos a través de internet hacia una dirección IP determinada.

4.2.1 ¿CÓMO FUNCIONA UNA COMUNICACIÓN TELEFONÍA IP?

Es una forma nueva de hacer y recibir llamadas telefónicas utilizando una conexión de Internet de banda ancha (broadband) en lugar de una línea

telefónica corriente. VoIP convierte su llamada telefónica (en realidad convierte la señal de voz de su teléfono) en una señal digital que viaja a través del Internet hasta llegar al teléfono de la persona que usted está llamando. Si usted llama a un número de teléfono fijo, la señal se reconvierte al llegar al receptor de la llamada.

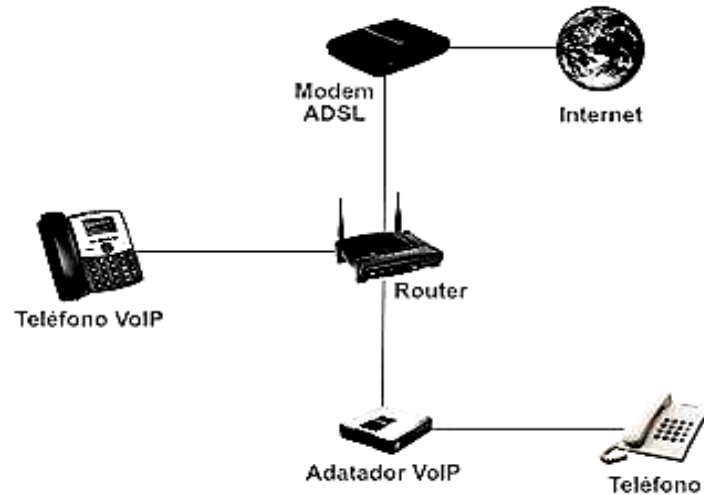


Figura 4.1 Diagrama de conexión de telefonía VoIP

La mayoría de los servicios de tecnología VoIP posibilita llamar a cualquier persona que tenga un número de teléfono, incluyendo números telefónicos locales, de larga distancia, celulares e internacionales. Otros servicios puede que le permitan llamar solamente a personas que tengan el mismo servicio. Además, la mayor parte de los servicios VoIP le permiten utilizar un aparato de teléfono común mediante el uso de un adaptador, pero otros servicios solamente funcionan en su computadora o mediante un aparato telefónico especial adaptado para la tecnología VoIP. Si usted se suscribe a un servicio VoIP que le permite hacer llamadas utilizando un teléfono con un adaptador, usted marca sus llamadas de la misma manera de siempre. En caso de que se suscriba a un servicio VoIP que funciona directamente desde su computadora, usted necesitará utilizar un software especial, un micrófono, parlantes y una tarjeta de sonido (soundcard). Si su servicio VoIP le asigna un número de teléfono común, podrá recibir llamadas de cualquier persona que lo llame desde un aparato telefónico común sin necesidad de ningún equipo especial.

4.2.2 ¿PORQUÉ LA TELEFONÍA IP ES MÁS BARATA?

Para explicar esto vamos a definir los gastos que implicaba una comunicación por conmutación de circuitos. A comienzos de la telefonía convencional, a mediados de 1960, cada llamada debía tener un cable dedicado yendo de una punta a la otra de la comunicación durante todo el tiempo que durara la misma. Entonces, si por ejemplo una persona ubicada en Argentina tuviera que realizar un llamado a otra persona en España los conmutadores de su operadora telefónica conectarían cables a lo largo de todo el recorrido para formar un camino entre los 2 extremos de la comunicación.

En este caso si la llamada durara 10 minutos se usarían esos cables conmutados que van a lo largo de todo el recorrido entre España y Argentina a lo largo de la duración de la conversación. Esto hacía que las comunicaciones a larga distancia fueran muy caras.

Hoy en día las comunicaciones telefónicas son mucho más eficientes por eso cuestan menos. Las voces son digitalizadas, y tu voz, puede viajar junto con muchas otras a través de un cable de fibra óptica por la mayoría del trayecto (sigue habiendo un pedazo de cable dedicado, que es el que va justo hacia tu casa). Esas llamadas son transmitidas a una calidad de 64kb por segundo (kbps) en cada dirección, por un total de transmisión de 128kb (64kb de ida y 64kb de vuelta). Como existen 8Kb en un KiloByte (KB), esto se transada en una transmisión de 16KB por cada segundo que el circuito está abierto, y 960KB cada minuto que está abierto. Entonces, en una comunicación de 10 minutos, el total transmitido sería de 9,600KB, lo que es prácticamente equivalente a 10 megas. Si observaras una conversación típica te darías cuenta fácilmente que mucha de esta información es malgastada.

4.3 FIBRA ÓPTICA

Las fibras ópticas son filamentos de vidrio de alta pureza extremadamente compactos: El grosor de una fibra es similar a la de un cabello humano. Fabricadas a alta temperatura con base en silicio, su proceso de elaboración es controlado por medio de computadoras, para permitir que el índice de

refracción de su núcleo, que es la guía de la onda luminosa, sea uniforme y evite las desviaciones, entre sus principales características se puede mencionar que son compactas, ligeras, con bajas pérdidas de señal, amplia capacidad de transmisión y un alto grado de confiabilidad debido a que son inmunes a las interferencias electromagnéticas de radio-frecuencia. Las fibras ópticas no conducen señales eléctricas por lo tanto son ideales para incorporarse en cables sin ningún componente conductor y pueden usarse en condiciones peligrosas de alta tensión. Tienen la capacidad de tolerar altas diferencias de potencial sin ningún circuito adicional de protección y no hay problemas debido a los cortos circuitos. Tienen un gran ancho de banda, que puede ser utilizado para incrementar la capacidad de transmisión con el fin de reducir el costo por canal; De esta forma es considerable el ahorro en volumen en relación con los cables de cobre. Con un cable de seis fibras se puede transportar la señal de más de cinco mil canales o líneas principales, mientras que se requiere de 10,000 pares de cable de cobre convencional para brindar servicio a ese mismo número de usuarios, con la desventaja que este último medio ocupa un gran espacio en los ductos y requiere de grandes volúmenes de material, lo que también eleva los costos. Comparado con el sistema convencional de cables de cobre donde la atenuación de sus señales (decremento o reducción de la onda o frecuencia) es de tal magnitud que requieren de repetidores cada dos kilómetros para regenerar la transmisión, en el sistema de fibra óptica se pueden instalar tramos de hasta 70 km. Sin que haya necesidad de recurrir a repetidores lo que también hace más económico y de fácil mantenimiento este material. Originalmente, la fibra óptica fue propuesta como medio de transmisión debido a su enorme ancho de banda; sin embargo, con el tiempo se ha planteado para un amplio rango de aplicaciones además de la telefonía, automatización industrial, computación, sistemas de televisión por cable y transmisión de información de imágenes astronómicas de alta resolución entre otros.

4.3.1 CONCEPTO DE TRANSMISIÓN.

En un sistema de transmisión por fibra óptica existe un transmisor que se encarga de transformar las ondas electromagnéticas en energía óptica o en

luminosa, por ello se le considera el componente activo de este proceso. Una vez que es transmitida la señal luminosa por las minúsculas fibras, en otro extremo del circuito se encuentra un tercer componente al que se le denomina detector óptico o receptor, cuya misión consiste en transformar la señal luminosa en energía electromagnética, similar a la señal original. El sistema básico de transmisión se compone en este orden, de señal de entrada, amplificador, fuente de luz, corrector óptico, línea de fibra óptica (primer tramo), empalme, línea de fibra óptica (segundo tramo), corrector óptico, receptor, amplificador y señal de salida.

En resumen, se puede decir que este proceso de comunicación, la fibra óptica funciona como medio de transportación de la señal luminosa, generado por el transmisor de LED'S (diodos emisores de luz) y láser.

Los diodos emisores de luz y los diodos láser son fuentes adecuadas para la transmisión mediante fibra óptica, debido a que su salida se puede controlar rápidamente por medio de una corriente de polarización. Además su pequeño tamaño, su luminosidad, longitud de onda y el bajo voltaje necesario para manejarlos son características atractivas.

4.3.2 SISTEMAS DE COMUNICACIÓN DE FIBRA ÓPTICA.

Los bloques principales de un enlace de comunicaciones de fibra óptica son:

- Transmisor
- Receptor
- Guía de fibra

El transmisor consiste de una interface analógica o digital, un conversor de voltaje a corriente, una fuente de luz y un adaptador de fuente de luz a fibra.

La guía de fibra es un vidrio ultra puro o un cable plástico.

El receptor incluye un dispositivo conector, un fotodetector, un conversor de corriente a voltaje un amplificador de voltaje y una interface analógica o digital.

En un transmisor de fibra óptica la fuente de luz se puede modular por una señal análoga o digital. Acoplando impedancias y limitando la amplitud de la señal o en pulsos digitales.

El convertor de voltaje a corriente sirve como interface eléctrica entre los circuitos de entrada y la fuente de luz. La fuente de luz puede ser un diodo emisor de luz LED o un diodo de inyección láser ILD, la cantidad de luz emitida es proporcional a la corriente de excitación, por lo tanto el convertor voltaje a corriente convierte el voltaje de la señal de entrada en una corriente que se usa para dirigir la fuente de luz. La conexión de esa fuente a la fibra es una interface mecánica cuya función es acoplar la fuente de luz al cable.

La fibra óptica consiste de un núcleo de fibra de vidrio o plástico, una cubierta y una capa protectora. El dispositivo de acoplamiento del receptor también es un acoplador mecánico.

El detector de luz generalmente es un diodo PIN o un APD (fotodiodo de avalancha).

Ambos convierten la energía de luz en corriente. En consecuencia, se requiere un convertor corriente a voltaje que transforme los cambios en la corriente del detector a cambios de voltaje en la señal de salida.

4.3.3 VENTAJAS DE LA FIBRA ÓPTICA.

Capacidad de transmisión: La idea de que la velocidad de transmisión depende principalmente del medio utilizado, se conservo hasta el advenimiento de las fibras ópticas, ya que ellas pueden transmitir a velocidades mucho más altas de lo que los emisores y transmisores actuales lo permiten, por lo tanto, son estos dos elementos los que limitan la velocidad de transmisión.

1. Mayor capacidad debido al ancho de banda mayor disponible en frecuencias ópticas.
2. Inmunidad a transmisiones cruzadas entre cables, causadas por inducción magnética.
3. Inmunidad a interferencia estática debida a las fuentes de ruido.
4. Resistencia a extremos ambientales. Son menos afectadas por líquidos corrosivos, gases y variaciones de temperatura.
5. La seguridad en cuanto a instalación y mantenimiento. Las fibras de vidrio y los plásticos no son conductores de electricidad, se pueden usar cerca de líquidos y gases volátiles.

4.3.4 UN EXCELENTE MEDIO PARA LAS COMUNICACIONES

En el último kilómetro es donde se presenta con mayor frecuencia problemas y daños en las comunicaciones de los clientes, pensando en esto empresas como la ETB crearon el proyecto de digitalización de la red de abonado en fibra óptica. La fibra es el soporte ideal por todas las ventajas que brinda, tales como:

1. Supresión de ruidos en las transmisiones.
2. Red redundante.
3. Conexión directa desde centrales hasta su empresa.
4. Alta confiabilidad y privacidad en sus comunicaciones telefónicas.
5. Posibilidad de daño casi nula.
6. Tiempos de respuesta mínimos en la reparación de daños.
7. Mayor número y rapidez en la solicitud y entrega de nuevos servicios.
8. Gran ancho de banda.

También la fibra óptica es una plataforma para la prestación de otros servicios, como:

1. Transmisión de datos de Alta Velocidad.
2. Enlaces E1 (2Mb/s) para conexión de PABX.

4.3.5 DESVENTAJAS

A pesar de las ventajas antes enumeradas, la fibra óptica presenta una serie de desventajas frente a otros medios de transmisión, siendo las más relevantes las siguientes:

- La alta fragilidad de las fibras.
- Necesidad de usar transmisores y receptores más caros.
- Los empalmes entre fibras son difíciles de realizar, especialmente en el campo, lo que dificulta las reparaciones en caso de ruptura del cable.
- No puede transmitir electricidad para alimentar repetidores intermedios.

- La necesidad de efectuar, en muchos casos, procesos de conversión eléctrica óptica.
- La fibra óptica convencional no puede transmitir potencias elevadas.
- No existen memorias ópticas

4.3.6 PARÁMETROS DE UNA FIBRA ÓPTICA.

Existen varios parámetros que caracterizan a una fibra óptica. Se habla de parámetros estructurales y de transmisión que establecen las condiciones en las que se puede realizar la transmisión de información.

Entre los parámetros estructurales se encuentra:

- El perfil de índice de refracción.
- El diámetro del núcleo.
- La apertura numérica.
- Longitud de onda de corte.

En cuanto a los parámetros de transmisión se tiene:

- Atenuación.
- Ancho de banda.
- Inmunidad a las Interferencias.

4.4 TIPOS BÁSICOS DE FIBRAS ÓPTICAS

- Multimodales
- Multimodales con índice graduado
- Monomodales

4.4.1 FIBRA MULTIMODAL

En este tipo de fibra viajan varios rayos ópticos reflejándose a diferentes ángulos como se muestra en la figura.

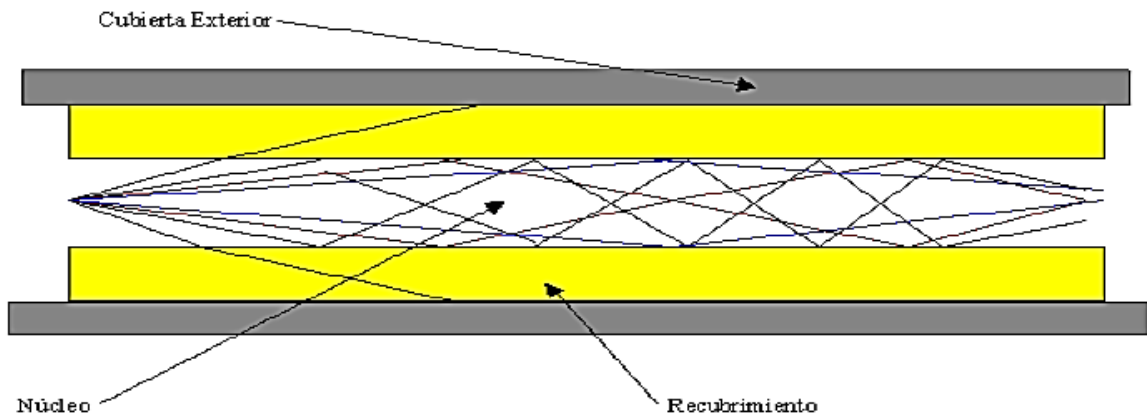


Figura 4.2 Fibra multimodal.

Los diferentes rayos ópticos recorren diferentes distancias y se desfasan al viajar dentro de la fibra. Por esta razón, la distancia a la que se puede transmitir esta limitada.

4.4.2 FIBRA MULTIMODAL CON ÍNDICE GRADUADO

En este tipo de fibra óptica el núcleo está hecho de varias capas concéntricas de material óptico con diferentes índices de refracción. La propagación de los rayos en este sigue un patrón similar mostrado en la figura.

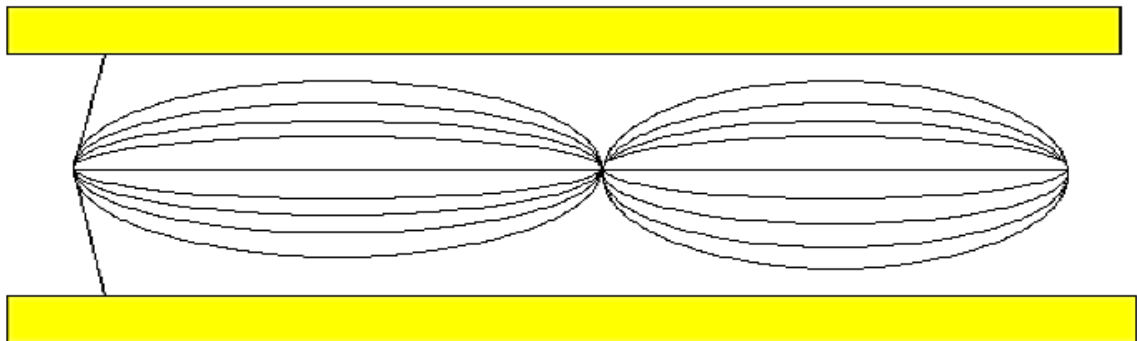


Figura 4.3 Fibra multimodal con índice graduado

En estas fibras el número de rayos ópticos diferentes que viajan es menor y, por lo tanto, sufren menos el severo problema de las multimodales.

4.4.3 FIBRA MONOMODAL

Esta fibra óptica es la de menor diámetro y solamente permite viajar al rayo óptico central. No sufre del efecto de las otras dos pero es más difícil de construir y manipular. Es también más costosa pero permite distancias de transmisión mayores.

La fibra óptica ha venido a revolucionar la comunicación de datos ya que tiene las siguientes ventajas:

- Gran ancho de banda (alrededor de 14Hz)
- Muy pequeña y ligera
- Muy baja atenuación
- Inmunidad al ruido electromagnético

Para transmitir señales por fibra óptica se utiliza modulación de amplitud sobre un rayo óptico, la ausencia de señal indica un cero y la presencia un uno. La transmisión de fibra óptica es unidireccional. Actualmente se utilizan velocidades de transmisión de 50, 100 y 200 Mbps, pero experimentalmente se han transmitido hasta Gbps sobre una distancia de 110 Kms.

CAPÍTULO V: DISEÑO DE LA RED Y APLICACIÓN EN EL EDIFICIO DE GOBIERNO DE LA DELEGACIÓN IZTACALCO EN EL DEPARTAMENTO DE TURISMO.

5.1 INTRODUCCIÓN.

El proyecto pretende actualizar las redes de nuestro país para tener un mejor servicio y acoplarnos a las nuevas tecnologías, ya que actualmente estamos atrasados en ese tema, por ejemplo en algunos edificios del gobierno se encuentran en pésimas condiciones lo que refiere a infraestructura de redes.

Como siempre se ha hablado de la ineficiencia de los sistemas de comunicación en las redes y de su seguridad en el gobierno, se propone modificar y rediseñar una infraestructura más estable y claro más confiable, a bajo precio y con excelentes resultados para un mejor servicio.

Para ello se propone hacer un pequeño prototipo que será evaluado y monitoreado como programa piloto en el edificio de la Delegación Iztacalco en el área de Turismo, que se eligió por sus instalaciones viejas, se pretende que de ser posible modificar esta pequeña instalación se logre implementar poco a poco en los demás departamentos.

5.2 FUNCIONAMIENTO Y OPERACIÓN.

Actualmente se puede observar a simple vista los diferentes edificios que rodean el Distrito Federal y Estado de México, podemos darnos cuenta de la calidad de las instalaciones existe carencia de recursos tanto eléctricos,

administrativos y por supuesto de comunicaciones por redes, por lo que se pretende hacer ver y concientizar a los directivos de la institución de Secretaría de Turismo de la delegación Iztacalco en modernizarse y poder hacer uso de las nuevas tecnologías para reducir gastos en las vías de comunicaciones haciendo esta área mas eficiente y menos costosa por lo que se considero modificar su equipo e infraestructura en su totalidad.

Nota: Actualmente la secretaría de turismo opera con el equipo más obsoleto y la infraestructura de más de 15 años.



Figura 5.1 Tomada desde las oficinas de la secretaria de turismo



Figura 5.2 Tomada desde la parte de adentro de las instalaciones.



Figura 5.3 Equipo y cableado en techo.



Figura 5.4 Adentro de las instalaciones.

5.3 MATERIAL Y DISPOSITIVOS

Para este diseño se pretende usar el servicio de internet y telefonía por medio de enlace lusacell el cual brinda ya algunos dispositivos los cuales son certificados y estandarizados con la más actual tecnología que soporta el servicio de Fibra Óptica que actualmente es lo más rápido que hay en el mercado. Se verifico la mejor opción para la necesidad del área y dentro de los paquetes que existen se seleccionó la llamada “Conexión 10” que brindaría velocidad de 20 Mb de bajada por 2 Mb de subida, conmutador AVAYA IP que brinda 30 extensiones telefónicas de las cuales habría 30 extensiones 20

analógicas y 10 digitales, a continuación se presenta el material usado para la red.

- DISPOSITIVO HUAWEI OT928 EN MODO BRIDGE.



Figura 5.5 Dispositivo Huawei

- DISPOSITIVO ROUTER NETGEAR N300



Router Netgear N300

Figura 5.6 Dispositivo Router Netgear N300

CONMUTADOR AVAYA IP

CARACTERÍSTICAS.

- Software de operadora
- Monitoreo de llamadas en tiempo real
- Distribución automática de llamadas
- Gestión de cambios vía remota
- Grabación de hasta 3 saludos empresariales.

- Personalización de la música de espera.
- Servicios de conferencia, buzón de voz y llamada en espera.



Figura 5.7 Conmutador Avaya

Se instalaran 14 Terminales Avaya con las siguientes características.

- Soporta 16 llamadas a la vez
- Display de 4 filas
- Conferencia de hasta 6 personas
- SpeakPhone
- Transferencia y retención de llamada



Figura 5.8 Teléfono digital Avaya

- Se instalaran 10 teléfonos analógicos con las siguientes características
- Teclas de memoria
- Speaker phone

- Llamada en espera, conferencia tripartita y transferencia de llamadas.



Figura 5.9 Teléfono analógico iusacell

Al igual que 2 servidores, uno principal para la operación diaria y uno como respaldo en caso de falla, estos 2 servidores serian Poweredge 1900, donde uno de ellos estaría en lo que sería el rack y el otro en un lugar seguro.

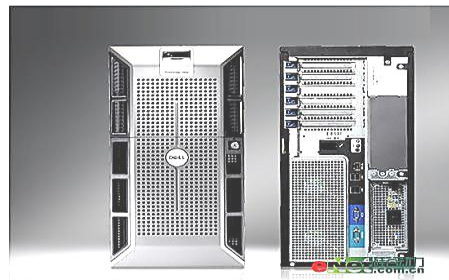


Figura 5.10 Servidores Poweredge 1900



Figura 5.11 Servidores Poweredge 1900 por dentro

Trabajaremos con 3 Pach Panel Avaya 1100 PSE para dividir los puertos y claro también poder definir la telefonía fija por IP. Como se muestra en la siguiente imagen.

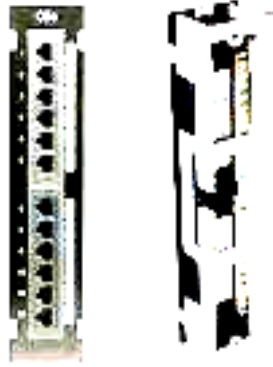


Figura 5.12 Routers Cisco Systems 2600

Manejaremos 1 switch capa 2 de 48 puertos marca Foundry FastIron edge4802 para un mejor soporte de puertos y distribución de privilegios:



Figura 5.13 Switch Foundry FastIron edge4802

También usaremos un Acces Point Wireless linksys



Figura 5.14 Acces Point Wireless linksys

El servicio de Internet y unos UPS para el respaldo de energía en caso de falla eléctrica para que no se desconfigure el equipo.



Figura 5.15 UPS

También utilizaremos uno o dos Racks para montar el equipo. Como éstos que ya se están empezando a montar gracias a nuestra propuesta.

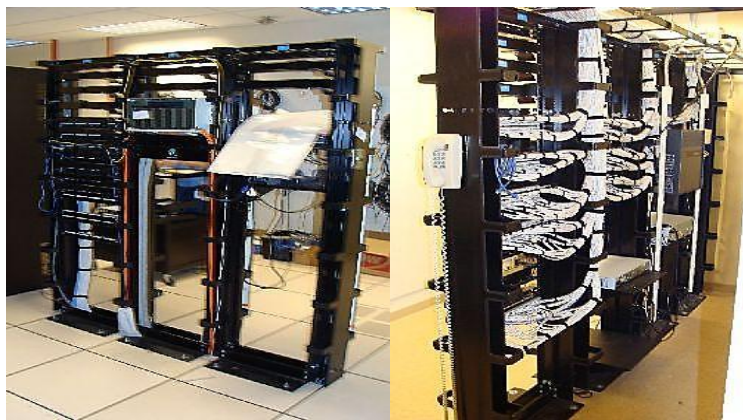


Figura 5.16 El cableado que utilizaremos para montar la nueva infraestructura es RJ-45 y RJ-12 para voz.

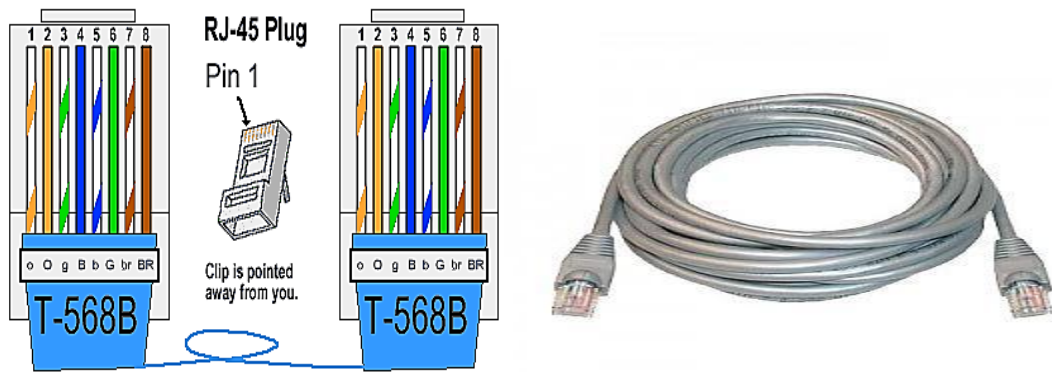


Figura 5.17 Cable RJ- 45 para datos

Digitrax Wiring Standards

Pin No	Colour	Function	Voltage
1	White	Rail Sync-B	7 vdc
2	Black	Ground	—
3	Red	Locolet	14.5 vdc
4	Green	Locolet	14.5 vdc
5	Yellow	Ground	—
6	Blue	Rail Sync-A	7 vdc

All components are RJ11 6-wire
Do not use RJ11 4-wire.

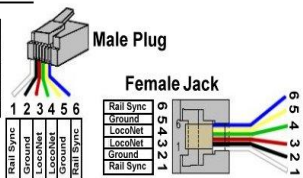


Figura 5.18 RJ-12 cable para voz.

Al reunir estos dispositivos realizamos una infraestructura utilizando una herramienta de diseño llamada sketchup 8 y haciendo una comparación de las fotos tomadas durante la estancia en secretaria de turismo podemos realizar dicha modificaciones como lo mostramos en los siguientes diseños.



Figura 5.19 Cableado actual del rack y las escalerillas de la Secretaria de Turismo.

5.4 DISEÑO DE LA INFRAESTRUCTURA.

Para el diseño de esta nueva infraestructura es poder crear la red más eficiente, barata y mejor utilizable, todo esto para tener un mejor servicio, reducir costos mensuales del uso de las vías de comunicación por lo cual se diseñó bajo el programa sketchup 8 la infraestructura del área de trabajo de las oficinas de la secretaria de turismo, basándonos en las fotos que pudimos tomar dentro de las instalaciones hicimos las siguientes comparativas.



Figura 5.20 Primer diseño de la infraestructura.

Como podemos observar se distribuye mejor el espacio y con más individualidad del personal además de que cada cubículo cuenta con una red de voz y datos, independiente para el uso exclusivo del personal además, se muestra mejor el diseño.

En la siguiente imagen mostramos una panorámica mejor del diseño.

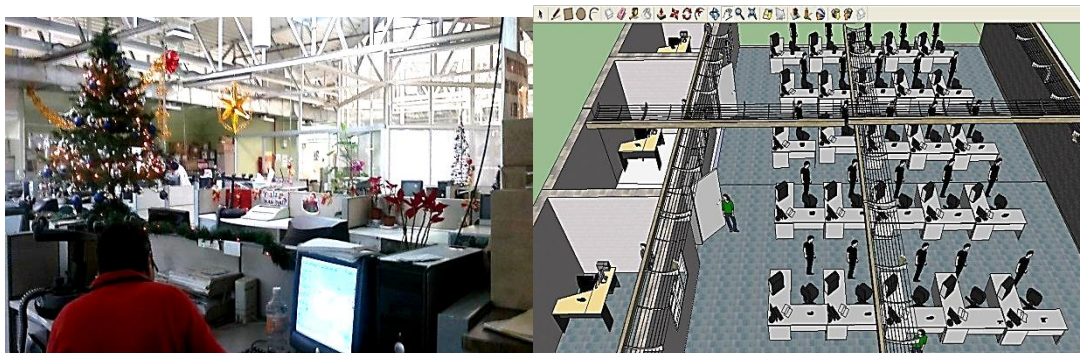


Figura 5.21 Panorámica de las instalaciones con su respectivo diseño.



Figura 5.22 Equipo que tiene las oficinas y el diseño con el nuevo equipo.

Como infraestructura quedaría así el diseño final.



Figura 5.23 Infraestructura vista desde la parte superior.

Muchos se preguntarán a que se debe esta propuesta de cambio de infraestructura, por lo cual decidimos rediseñar éstas oficinas porque durante una pequeña investigación encontramos que el gobierno en este caso la secretaria de turismo, pagaba aproximadamente 30 mil pesos al mes en el servicio de telecomunicaciones (Internet, telefonía móvil, telefonía fija y mantenimiento del equipo.) sabiendo que todo esto no le cuesta solo a gobierno si no a todos, puesto que todos pagamos esas rentas con nuestros impuestos por lo que una restructuración que ahorre dinero a corto y largo plazo nos beneficiaría a todos.

5.5 CONFIGURACIÓN DE NETGEAR N300

Netgear es la aplicación donde configuraremos las IP que tendrán servicio, ésta clase de aplicación es solo para el router que utilizaremos el N300.

A continuación configuraremos el router Netgear N300 paso a paso junto con su configuración inalámbrica donde estableceremos las IP's que se utilizaran, las máscaras de red y submáscaras aparte de la Mac address e ilustraremos casa paso, así que comenzaremos instalando la aplicación de Netgear N300 para poderla utilizar estos pasos gráficos viene adjuntos en el CD, que viene junto a la tesis por lo que se recomienda utilizar ambos materiales a la vez.

Como ya mencionamos una vez instalada la aplicación Netgear N300 procedemos a ingresar el usuario y el password para que nos dé acceso al router y a la configuración. En teoría utilizaremos el user "admin" y el password con el mismo nombre "password", como se muestra en la siguiente imagen:



Figura 5.24 Validación acceso a Netgear

Una vez puesto el usuario y el password correcto nos permitirá ingresar a la parte de configuración de netgear, dentro de la aplicación nos dirigimos a configuración básica en este paso igual nos vuelve a pedir el usuario y el

password lo volvemos a introducir, esto se debe a que el router tiene ciertos niveles de seguridad por eso nos estará pidiendo el password y el usuario, ya que nos permita ingresar procedemos a ponerla como se muestra en la imagen.

¿Necesita su conexión a Internet un nombre de usuario?

Sí

No

Nombre de la cuenta (si corresponde)

Nombre del dominio (si corresponde)

Figura 5.25 Configuración básica

Una vez hecho el paso anterior configuramos la parte de “Dirección IP de Internet” como se muestra en la siguiente imagen, esto sirve para establecer las direcciones IP’s y el tipo de clase de red LAN.

Dirección IP de Internet

Obtener dinámicamente del ISP

Utilizar una dirección IP estática

Dirección IP . . .

Máscara de subred IP . . .

Dirección IP de la puerta de enlace . . .

Figura 5.26 Configuración de dirección ip

Ya que hemos configurado la parte de IP procederemos a configurar la parte del dominio (DNS) como se muestra en la siguiente imagen:

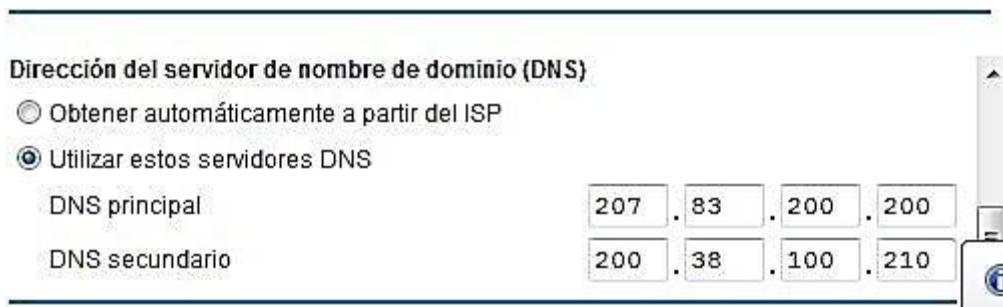


Figura 5.27 Configuración de dirección del servidor

Una vez hecho la configuración del DNS procedemos a realizar la parte de configuración de la dirección Mac con el Router esto por lo regular lo da por default en caso de que no, lo pondremos de manera manual como se muestra en la siguiente imagen:

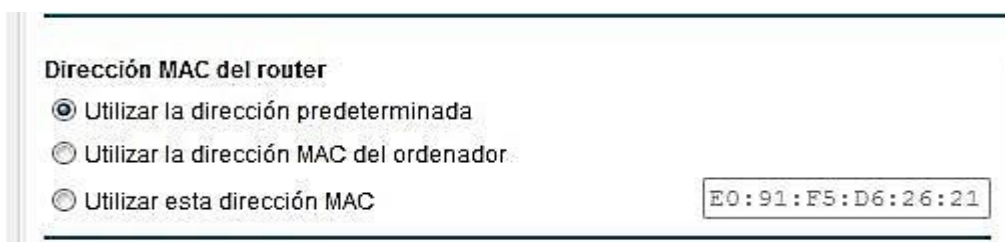


Figura 5.28 Configuración dirección MAC

Una vez configurado el Router procedemos a deshabilitar la parte de red Inalámbrica, para esto nos iremos a la parte izquierda de la aplicación y procedemos a entrar con un click.



Figura 5.29 Configuración inalámbrica

Una vez dentro, sólo procedemos a deshabilitar la red inalámbrica esto se hace en la parte de “Activar el aislamiento inalámbrico” tan solo dando un click o activando la casilla con el mismo nombre, después de esto solo activamos en la parte de seguridad la casilla “Ninguno” y listo esta deshabilitada la red inalámbrica esto se requiere por motivos de seguridad, para que personas externas no tengan acceso a la red y hagan un mal uso de ella. Debe quedar como en la siguiente imagen:

The screenshot shows a configuration page for wireless networking. Under the heading "Red inalámbrica", there are several settings: "Publicar SSID" is unchecked, "Activar el aislamiento inalámbrico" is checked, "Nombre (SSID)" is "NETGEAR", "Región" is "Norteamérica", "Canal" is "06", and "Modo" is "Hasta 300 Mbps". Below this, under "Opciones de seguridad", the "Ninguno" radio button is selected, while "WEP", "WPA-PSK [TKIP]", "WPA2-PSK [AES]", and "WPA-PSK [TKIP] + WPA2-PSK [AES]" are unselected.

Figura 5.30 Deshabilitamos la red inalámbrica

Cuando hayamos deshabilitado la parte de red inalámbrica procedemos a configurar la LAN para esto, solo damos las Ip's que se utilizarán como se muestra en la imagen:

The screenshot shows the "Configuración LAN" page. On the left is a navigation menu with "Configuración LAN" selected. The main area shows: "Nombre del dispositivo" as "WNR2000v2", "Configuración TCP/IP LAN" with "Dirección IP" set to 192.168.0.1 and "Máscara de subred IP" set to 255.255.255.0. "Dirección RIP" is set to "Ambas" and "Versión de RIP" is set to "Desactivado".

Figura 5.31 Configuración LAN

Por último damos click en la casilla "Utilizar el Router como servidor DHCP" y llenamos los últimos recuadros como se muestra en la imagen y damos en click en el rectángulo de aplicar y listo:

The screenshot shows a DHCP configuration interface. At the top, there is a checkbox labeled "Utilizar router como servidor DHCP" which is checked. Below this, there are two rows of IP address input fields. The first row is labeled "Dirección IP de inicio" and contains the values 192, 168, 0, and 2. The second row is labeled "Dirección IP de destino" and contains the values 192, 168, 0, and 254. Below these fields is a section titled "Reserva de emisión" which contains a table with three columns: "#", "Dirección IP", and "Nombre del dispositivo", and a fourth column labeled "Dirección MAC". Below the table are three buttons: "Añadir", "Editar", and "Eliminar". At the bottom of the interface are two buttons: "Aplicar" and "Cancelar".

Figura 5.32 Configuración de DHCP

5.6 ENDIAN FIREWALL

5.6.1 INTRODUCCIÓN

El software utilizado para la aplicación de Firewall es ENDIAN FIREWALL (EFW) el cual es un "llave en mano" de distribución de seguridad de Linux que convierte a cada sistema en un dispositivo de seguridad con todas las funciones de gestión unificada de amenazas (UTM) funcionalidad. El software ha sido diseñado con "pensando en el usuario" y es muy fácil de instalar, utilizar y gestionar, sin perder su flexibilidad.

Las características incluyen un firewall Stateful Packet Inspection, a nivel de aplicación proxy para varios protocolos (HTTP, FTP, POP3, SMTP) con soporte antivirus, antivirus y de filtrado de spam para el tráfico de correo electrónico (POP y SMTP), filtrado de contenido de tráfico de Internet. La página para poder descargar este software es:

<http://www.endian.com/en/community/download/>

5.6.2 IMPLEMENTACIÓN DE ENDIAN FIREWALL

Dentro de este proyecto se aplicara con la siguiente topología:

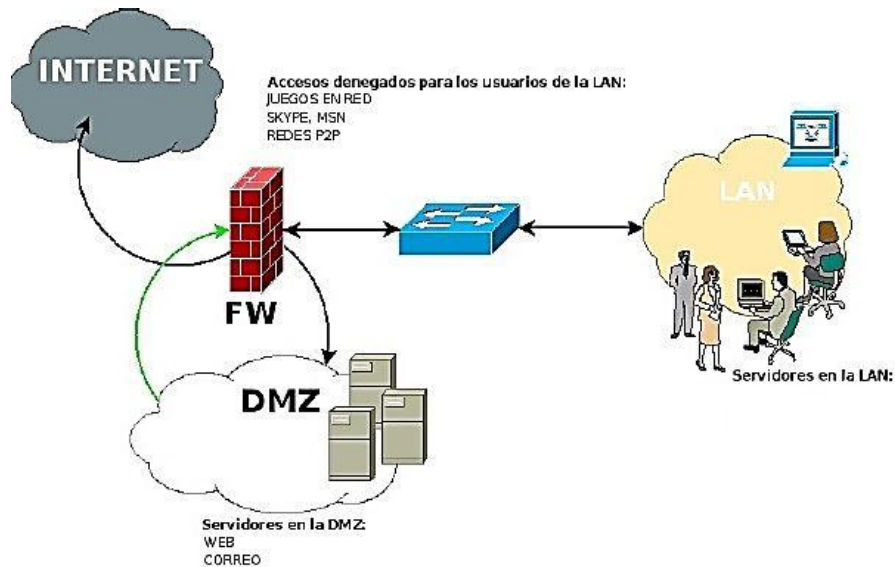


Figura 5.33 Topología usando Endian Firewall.

El proyecto contara con los siguientes requerimientos dentro del Firewall:

- Se otorgaran 2 tipos de permisos para los usuarios el primero tendrá privilegios para los jefes administrativos los cuales son 2 en esa área, los demás usuarios serán bloqueados de algunos servicios como son paginas de redes sociales, contenido sexual.
- Se podrá entrar a los servidores WEB y de CORREO desde Internet y desde la LAN, usando puertos seguros para descarga y envío de correos.
- El servidor WEB puede acceder solamente al servidor de la LAN.
- El servidor de Correo puede acceder únicamente al servidor de impresión de la LAN

- Dentro del área existen 3 personas las cuales tendrán acceso total a la red debido a que son directivos de esta área.

5.6.3 APLICACIÓN DEL SOFTWARE

Tenemos tres tarjetas de red en un PC el cual instalaremos la distribución de Linux Endian, Por otro lado tenemos nuestro Equipo el cual administraremos el Endian gráficamente y así podremos configurarlo más fácilmente para que nos opere como Firewall, cabe aclarar que este equipo debe estar conectado en la red LAN (VERDE) para poder tener acceso a la administración.

Cada una de las tarjetas están conectadas a una red diferente como se muestra a continuación:

Una de las interfaces está conectada con la WAN (ROJO (RED) - Internet), la cual posee la dirección IP 192.168.0.1 La Segunda interfaz está conectada a nuestra red Privada LAN (VERDE(GREEN))y posee la dirección 192.168.0.1 y la tercera interfaz está conectada a la DMZ (NARANJA (ORANGE) – Zona desmilitarizada), la cual posee la dirección IP 10.0.0.1 en la cual está el Servidor.

Como primer instancia Una vez hecha la instalación en el equipo se tiene que realizar la configuración desde otra PC.

Ahora abrimos el navegador desde una de las maquinas que formara parte de nuestra LAN y en la URL escribimos la dirección IP que ya hemos configurado con anterioridad en la instalación de nuestro Firewall. Endian en nuestro caso <https://192.168.0.10:10443> Esto significa que el Firewall nos esta exigiendo una conexión segura utilizando un certificado digital, para continuar damos clic en “Agregar una excepción”

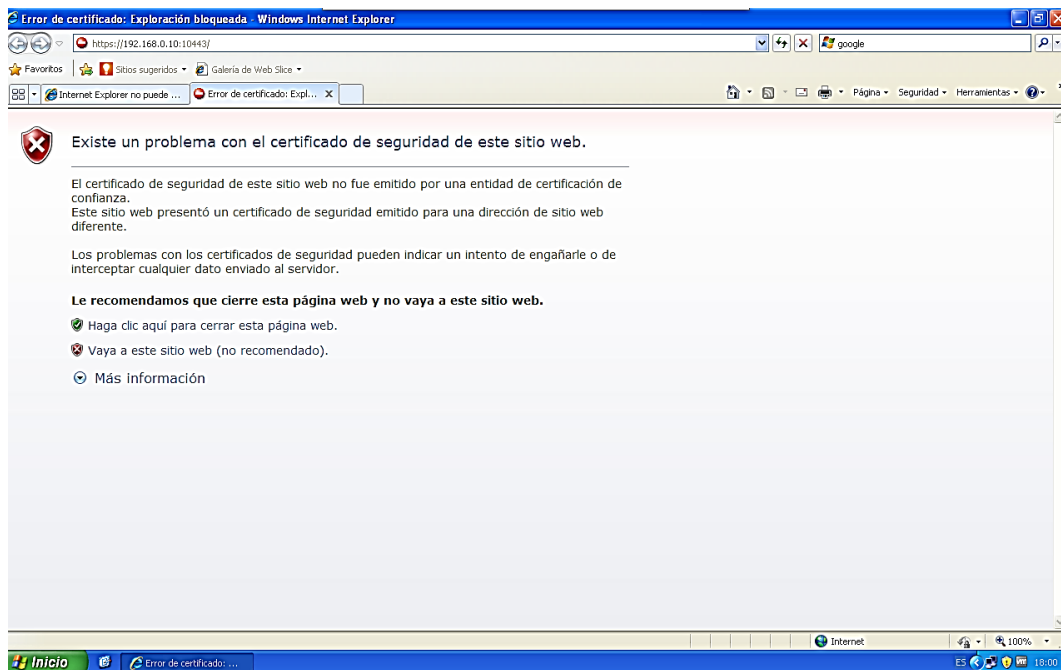


Figura 5.34 Permiso de contenido.

A continuación se obtiene certificado y después nos aparecerá usuario y contraseña.



Figura 5.35 Acceso a Endian Firewall.

Esta es la pantalla de bienvenida para la configuración de Endian Firewall. Para Continuar hacer click sobre el botón.



Figura 5.36 Pantalla de Bienvenida Endian Firewall.

A continuación se nos ofrece la posibilidad de cambiar el lenguaje con el que se configurará Endian Firewall. Seleccionaremos Aquí se nos muestra el acuerdo de licencia de uso de Endian Firewall.



Figura 5.37 Pantalla de Bienvenida Endian Firewall.

Desplazándonos hacia abajo en la página encontraremos el recuadro "ACCEPT License" al cual deberemos hacer click para aceptar la licencia y poder continuar la configuración del firewall.



Figura 5.38 Aceptación de licencia.

Tras haber aceptado la licencia de uso, el asistente de configuración del firewall nos muestra una pantalla en donde nos pregunta si queremos restablecer un backup o archivo de respaldo de la configuración. Puesto que esta instalación corresponderá a una instalación nueva, desde cero, le decimos que “No” queremos restablecer un backup. Le damos click en “>>>” para continuar con la configuración del firewall.



Figura 5.39 Establecimiento de Backup.

Antes de proceder con la configuración IP del Firewall, debemos establecer las contraseñas del administrador del sistema. Estas contraseñas permitirán el acceso a la configuración y visualización del estado del Firewall. Es importante que estas contraseñas sean “difíciles de adivinar por otras personas” y que además tengan al menos 8 caracteres (letras y/o números). Tanto la contraseña para “Admin” y para “root” pueden ser las mismas. Para configurar el firewall posteriormente será necesario acceder a él usando solo el usuario “Admin”.



Figura 5.40 Establecimiento user y password.

Ahora elegimos el tipo de conexión WAN (ROJO), en nuestro caso será un enlace Ethernet DHCP.

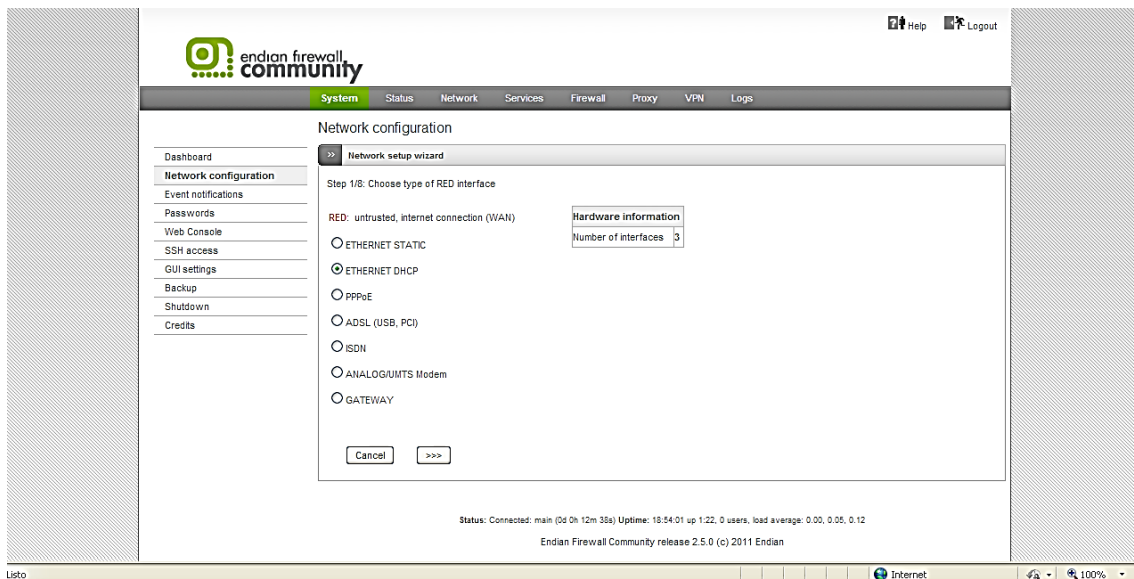


Figura 5.41 Tipo de Conexión.

Como Endian nos ha detectado 3 tarjetas de red, ahora nos pregunta para que utilizaremos la tarjeta de red que nos queda, en este caso la usaremos para un Zona Desmilitarizada DMZ (NARANJA).

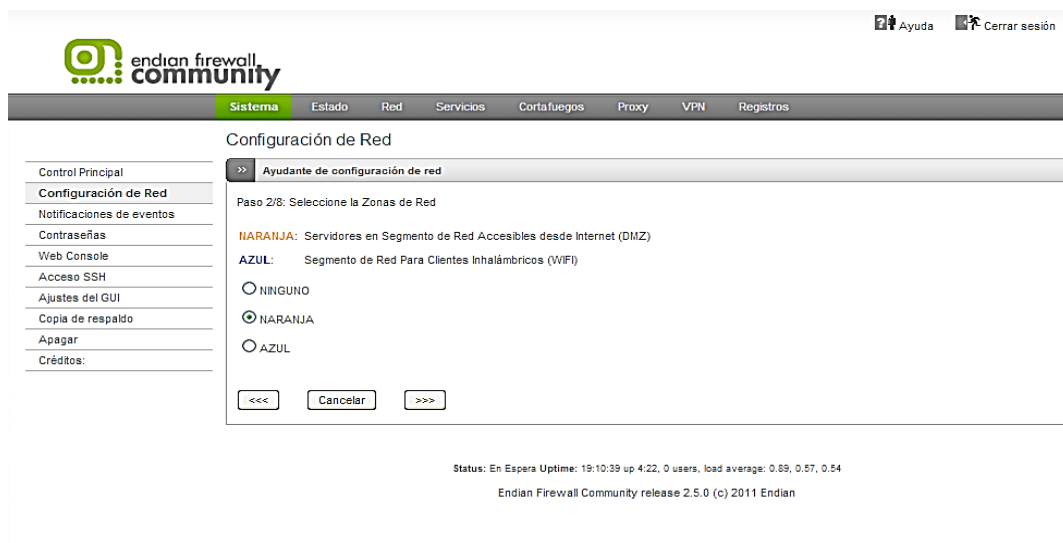


Figura 5.42 Selección de las zonas de red.

Aquí asignamos las direcciones IP de la red LAN (VERDE) y de la DMZ (NARANJA).

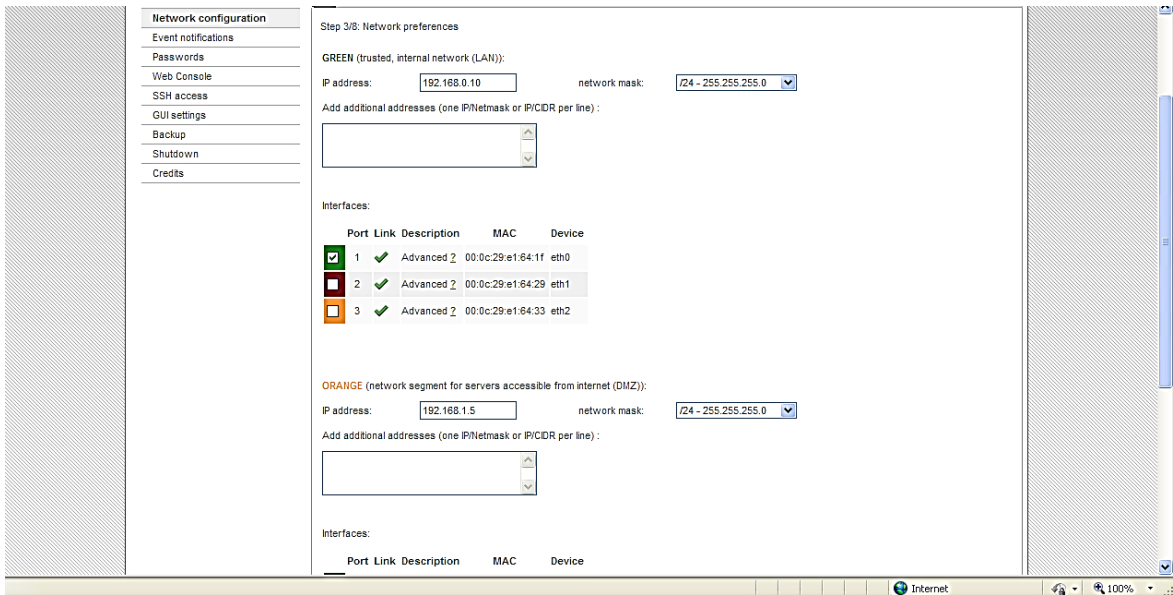


Figura 5.43 Preferencias de red LAN VERDE.

También le damos un nombre al equipo y un nombre de dominio.

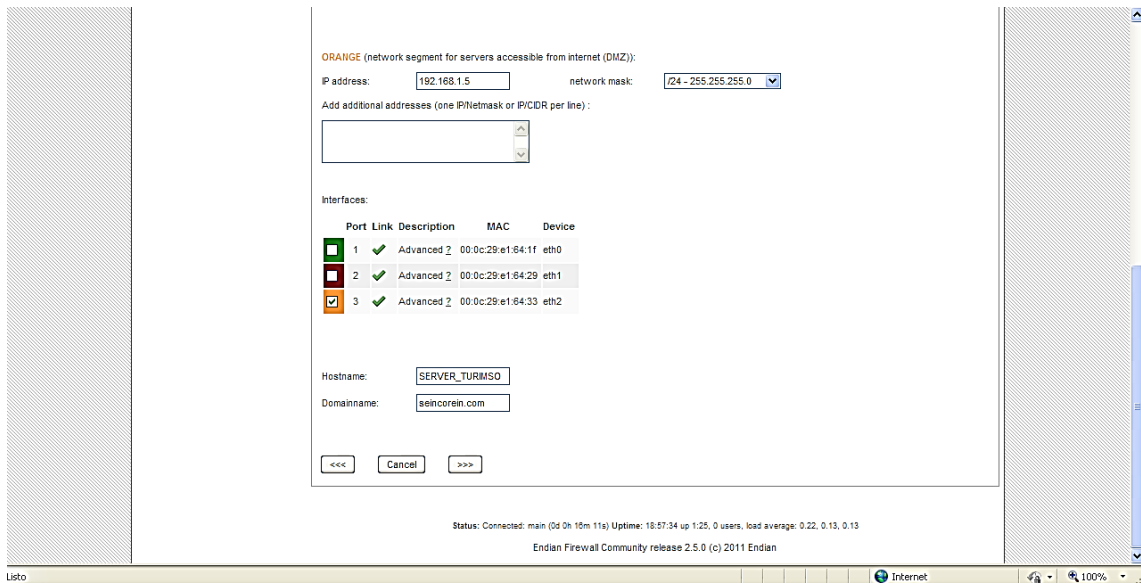


Figura 5.44 Preferencias de red LAN NARANJA.

Ahora pasamos a la configuración de la red WAN (ROJO), le damos la dirección IP y la puerta de enlace (es decir el próximo salto al cual hay que llegar después del Firewall).

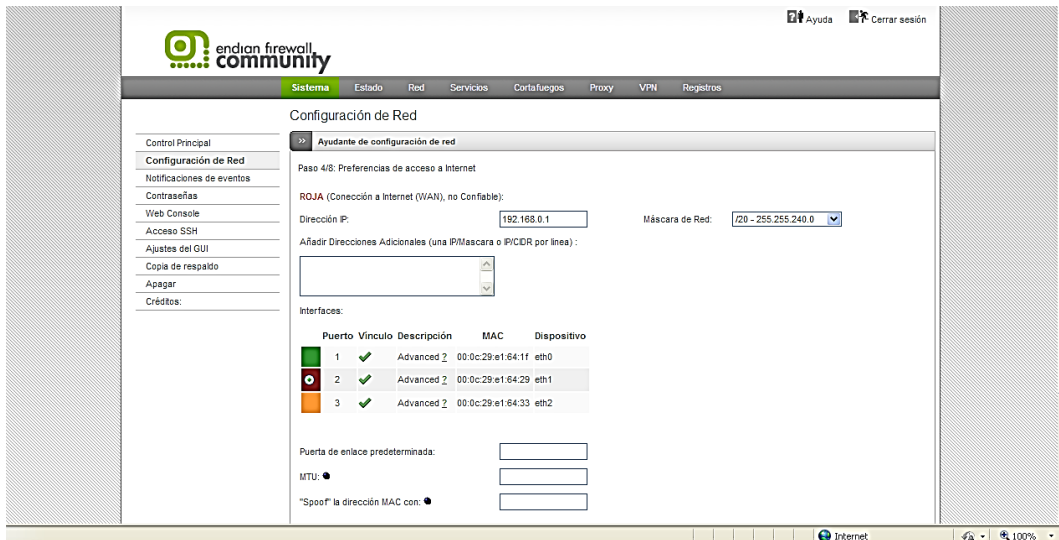


Figura 5.45 Preferencias de red LAN ROJO.

Aquí el asistente nos pregunta por las direcciones IP de los DNS a ser usados por el Firewall. En este caso usaremos las direcciones: 207.83.200.200 y 200.38.100.210 tal y como se muestra en la imagen. Hacemos click en >>> para continuar.

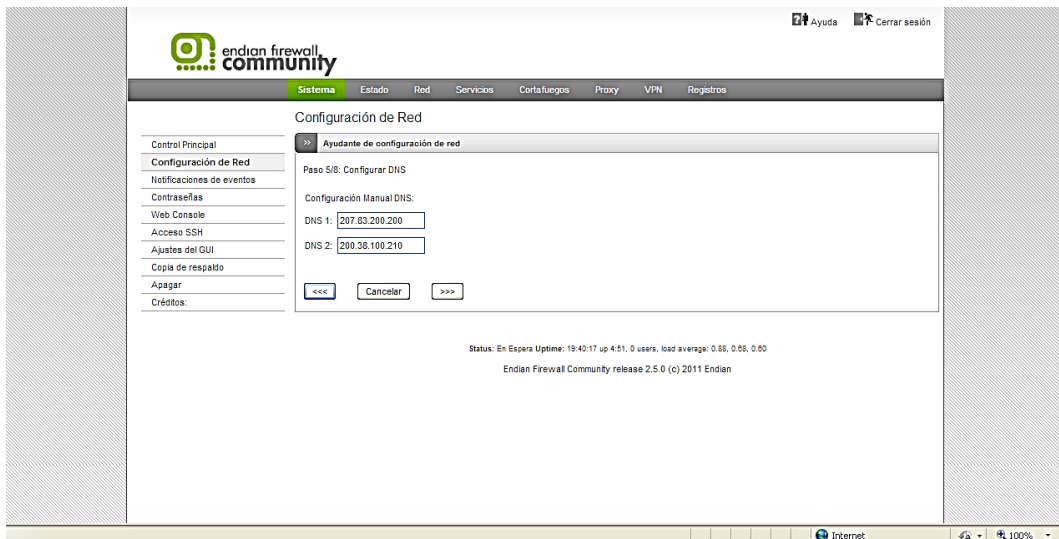


Figura 5.46 Configuración de DNS.

Ya en este paso estamos listos para aplicar y grabar los cambios y configuraciones hechas previamente en las pantallas anteriores. Hacemos click en "OK, Apply configuration" para aplicar la nueva configuración del Firewall.

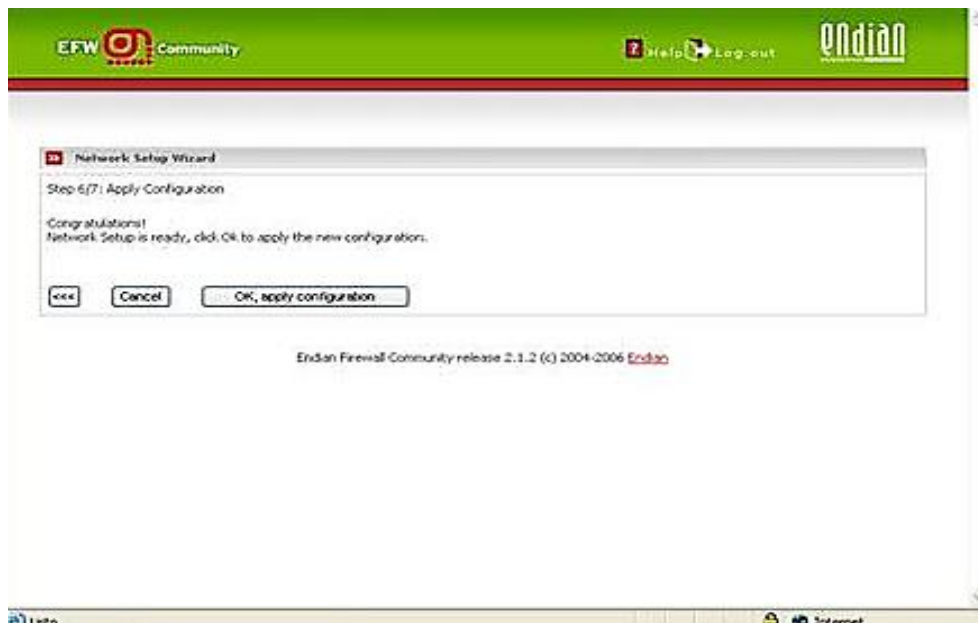


Figura 5.47 Pantalla de Guardar Cambios.

Tras haber aplicado la configuración el Firewall se reiniciara de manera automática. Esto tomara unos minutos, tiempo en el cual el firewall llevara a cabo todas las operaciones necesarias empezar a funcionar.

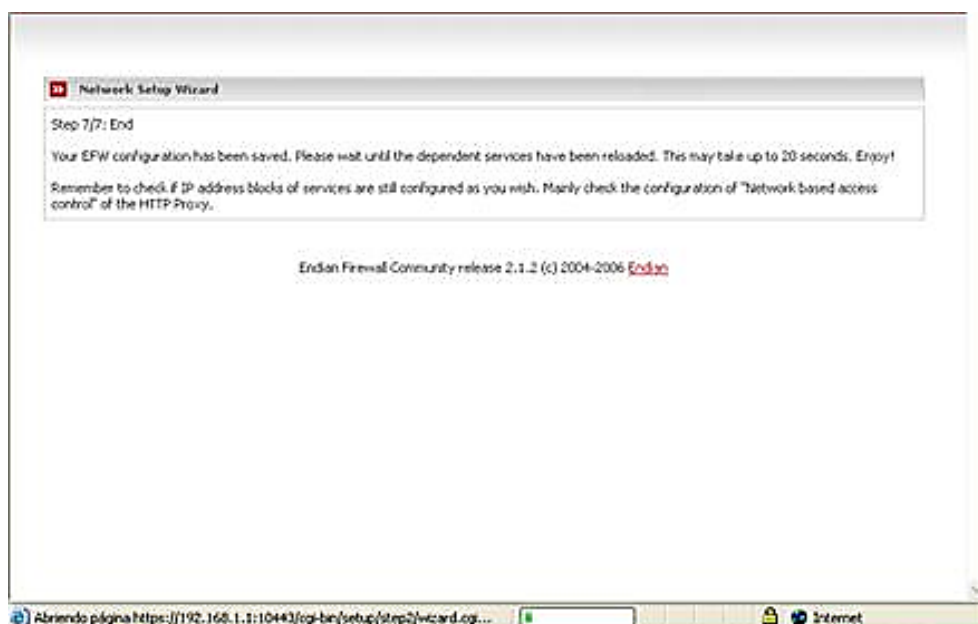


Figura 5.48 Establecimiento Configuración.

Tras la aplicación de la configuración del Firewall, después de unos segundos el navegador nos volverá a preguntar si es que queremos continuar con la carga o acceso a la página web de configuración y monitoreo del Firewall. Para

continuar hacemos click en "Sí". En caso que no se muestre nada o no pregunte nada ingresar a la página web de configuración y monitoreo del Firewall a través de su dirección: <https://192.168.0.10:10443>



Figura 5.49 Alerta de Seguridad para el sitio Endian.

Ingresamos el usuario **Admin** o la contraseña previamente establecida.

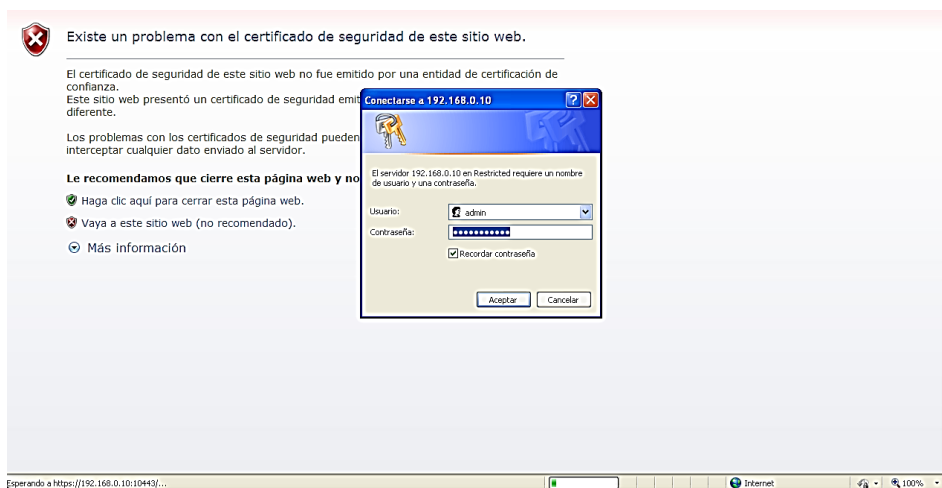


Figura 5.50 Requerimiento de contraseña para acceso.

El Endian trae NAT por defecto desde la LAN hacia la WAN y permite tráfico común como es http, DNS, FTP, etc. Para ver esto seguimos los siguientes pasos: NAT POR DEFECTO-ENDIAN Vamos a Firewall (Cortafuegos) reenvío de puertos /NAT fuente y damos click en mostrar las reglas del sistema, podremos ver la regla de NAT.

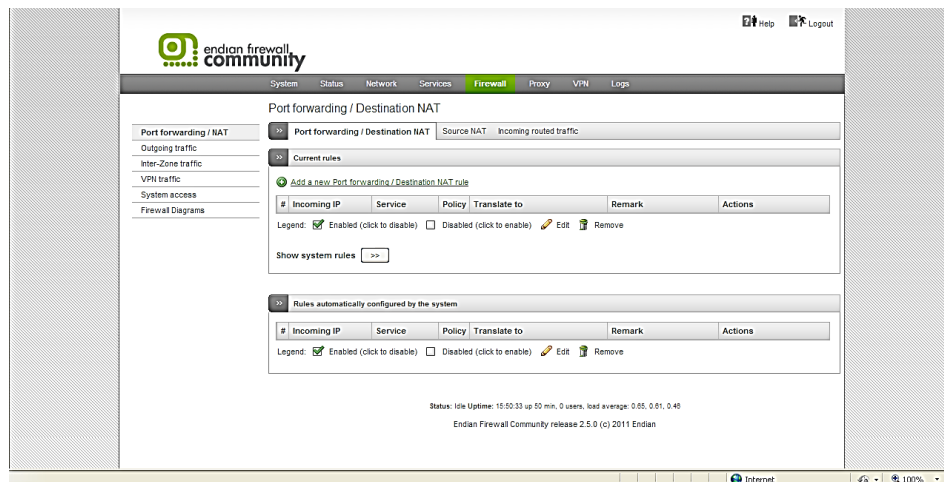


Figura 5.51 Port forwarding / Destina

Para ver el tráfico vamos a Firewall (Cortafuegos)- Outgoingtraffic.

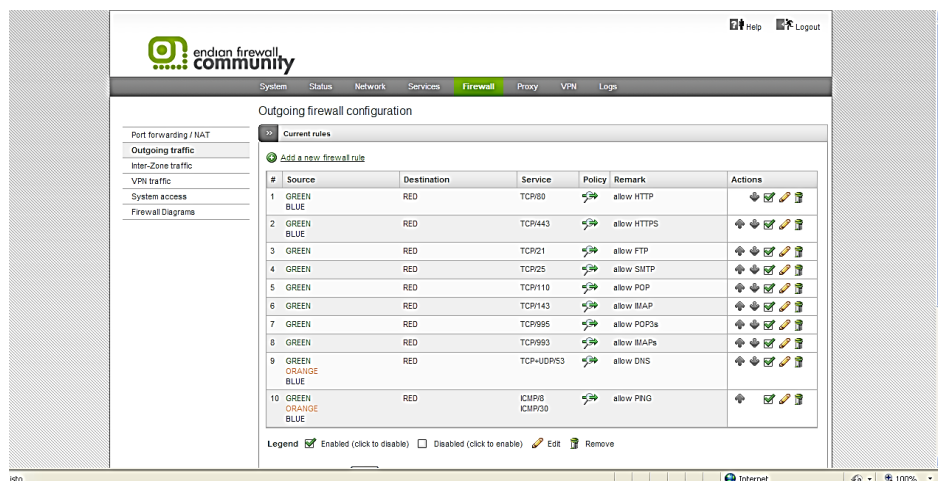


Figura 5.52 Tráfico de Firewall.

5.6.3.1 DEFINIR REGLAS ACCESO AL SERVIDOR POSTGRESQL DESDE INTERNET.

Vamos a Firewall, luego clic Port forwarding /NAT, damos clic en Add a new port forwarding rule, debemos llenar los espacios requeridos. En el espacio de Remark escribimos el nombre de la nueva regla, el puerto en el cual el firewall estará alerta para luego reenviar las peticiones, la dirección IP del servidor Postgre SQL y el puerto (por defecto es el 5432), habilitamos la regla clic Add.



Figura 5.53 Port forwarding configuration.

Ahora agregaremos los orígenes a los cuales se les permitirá el acceso al servidor de la LAN, para ello damos clic en el símbolo Add external access .Agregamos la dirección de red del origen. Clic en Add .No debemos olvidar aplicar los cambios. Clic en Apply.

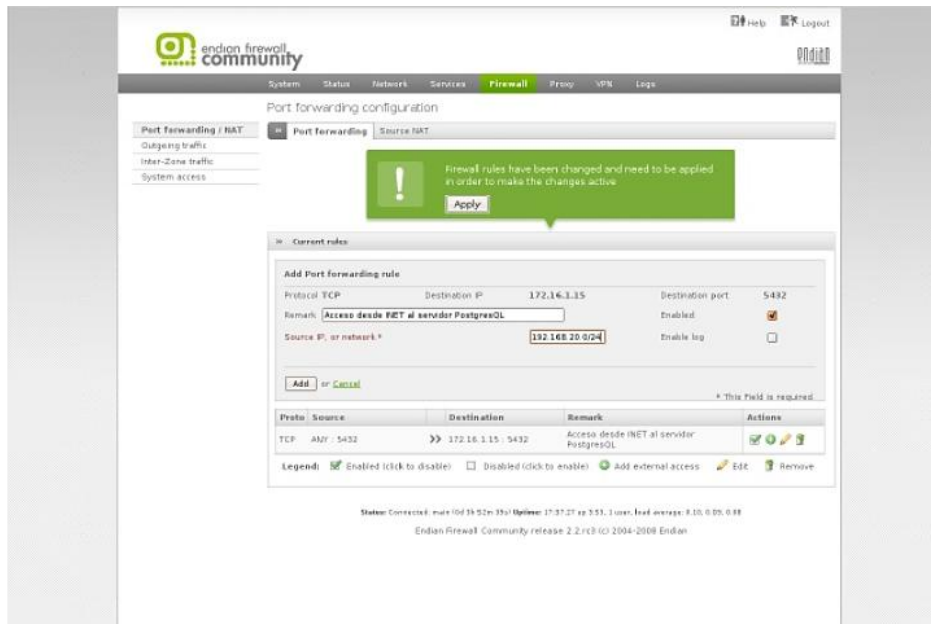


Figura 5.54 Aplicación de cambios Port forwarding configuration.

5.6.3.2 PERMITIR ACCESO A LOS SERVIDORES EN LA DMZ DESDE INTERNET Y DESDE LA LAN PERMITIR A LA LAN.

Después vamos a Firewall, Inter-Zone traffic y Add zone firewall rule. Elegimos la LAN (GREEN) como source y de destination la DMZ (ORANGE). Definimos los puertos 443, 995, 993 y 80, la acción a tomar será ACCEPT y la Agregamos (Add rule).

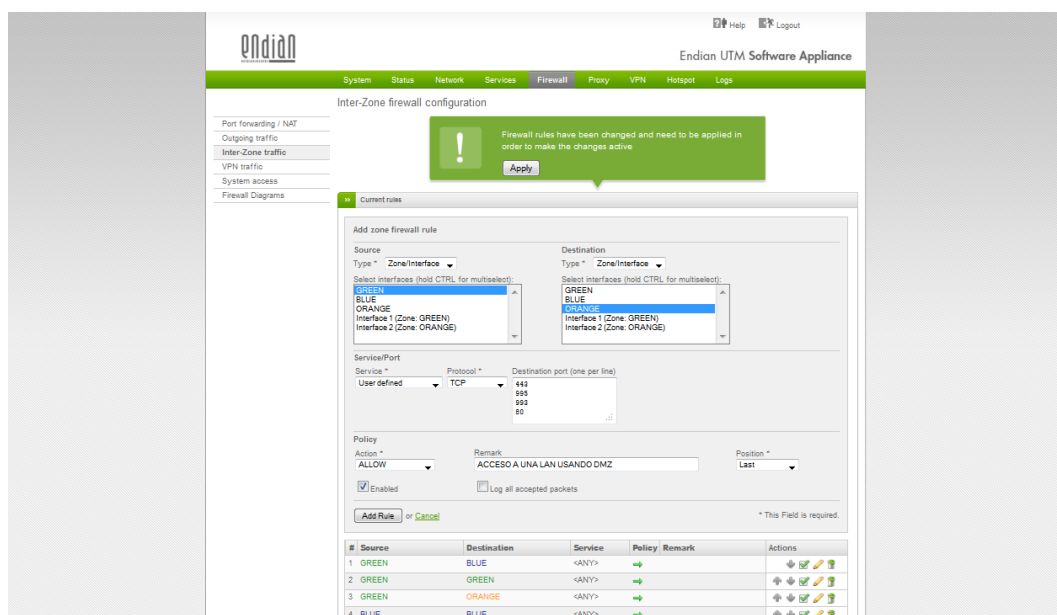


Figura 5.55 Adición de reglas en Inter-Zonetraffic.

5.6.3.3 PERMITIR A LA WAN.

Vamos a Firewall, Port forwarding/NAT y Add port forwarding rule. Elegimos el protocolo. La interfaz donde va escuchar el FW y el puerto. Definimos la dirección IP del servidor interno y el puerto. Una descripción, la habilitamos, ponemos el rango de IPS a las cuales se les dará permiso de acceder a este servicio. Click enAdd.

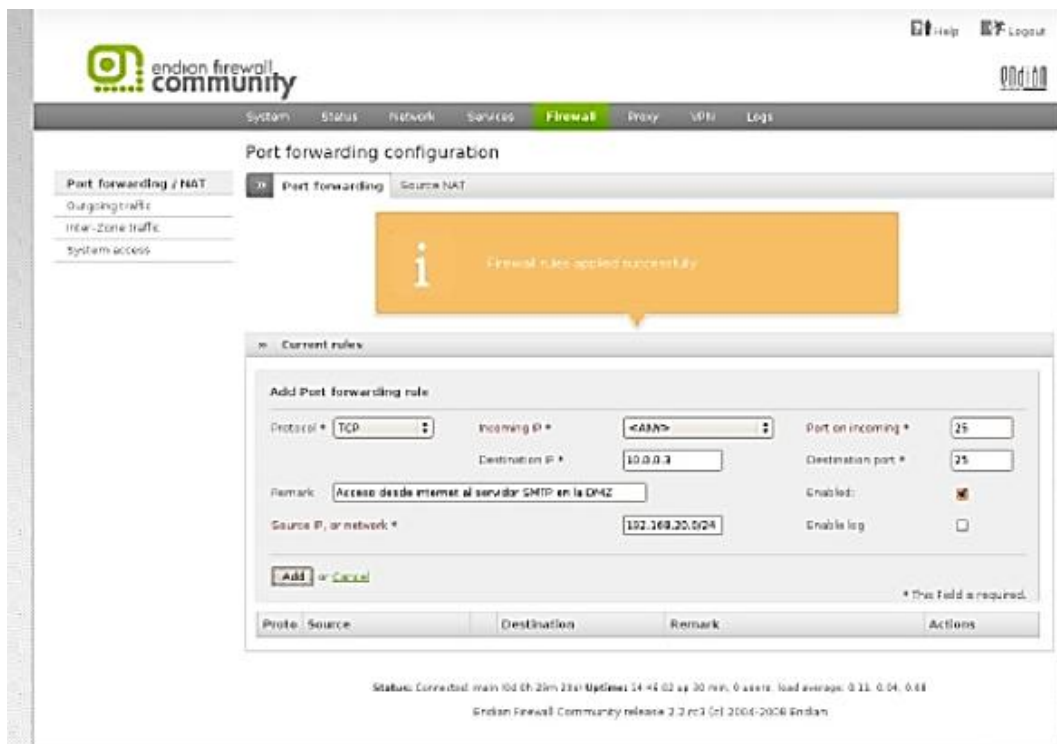


Figura 5.56 Configuración para permitir a la WAN.

5.6.3.4 ACCESO DEL SERVIDOR WEB AL SERVIDOR SQL SERVER

Para permitirle al servidor Web el acceso hacia el servidor SQL Server debemos crear una regla de inter-zona. Vamos a Firewall, Inter-Zonetraffic y Addzone firewall rule .En el campo Source escribimos la dirección IP del servidor Web, en Destination la dirección IP del servidor SQL Server, definimos el Puerto por el cual esta accedando nuestro servidor SQL Server (por defecto es 1433), en la parte de Action seráALLOW, le damos una descripción en el campo Remark, la habilitamos (Checkear Enabled) y damos clic en Add rule.



Figura 5.57 Adición de reglas en Inter-Zonetraffic del servidor web al servido SQL server.

5.7 COSTOS Y BENEFICIOS DE INSTALACIÓN.

•••••	Troncales	>>	10 troncales										
	DID'S	>>	30										
	Llamadas a números locales fijos	>>	5,000 llamadas										
	Larga distancia Nacional a números fijos (incluye 198 ciudades), EUA y Canadá	>>	2,000 minutos										
	Llamadas a Celular (044)	>>	700 minutos										
	Velocidad de INTERNET	>>	<table border="0"> <tr> <td>24 meses</td> <td>20 Mbps</td> <td>▼</td> <td>2 Mbps</td> <td>▲</td> </tr> <tr> <td>36 meses</td> <td>30 Mbps</td> <td>▼</td> <td>2 Mbps</td> <td>▲</td> </tr> </table>	24 meses	20 Mbps	▼	2 Mbps	▲	36 meses	30 Mbps	▼	2 Mbps	▲
24 meses	20 Mbps	▼	2 Mbps	▲									
36 meses	30 Mbps	▼	2 Mbps	▲									
	Precio	>>	<table border="0"> <tr> <td>24 meses</td> <td>36 meses</td> </tr> <tr> <td>\$ 11,900.00</td> <td>\$ 11,400.00</td> </tr> </table>	24 meses	36 meses	\$ 11,900.00	\$ 11,400.00						
24 meses	36 meses												
\$ 11,900.00	\$ 11,400.00												
Paquetes con CONMUTADOR integrado													
	Conmutador	>>	<table border="0"> <tr> <td>30 extensiones</td> </tr> <tr> <td>20 ext. analógicas</td> </tr> <tr> <td>10 ext. digitales</td> </tr> </table>	30 extensiones	20 ext. analógicas	10 ext. digitales							
30 extensiones													
20 ext. analógicas													
10 ext. digitales													
	Teléfonos incluidos en el paquete	>>	4 Analógicos, 2 Digitales										
	Precio	>>	<table border="0"> <tr> <td>24 meses</td> <td>36 meses</td> </tr> <tr> <td>\$ 14,500.00</td> <td>\$ 13,900.00</td> </tr> </table>	24 meses	36 meses	\$ 14,500.00	\$ 13,900.00						
24 meses	36 meses												
\$ 14,500.00	\$ 13,900.00												
AHORRA HASTA 40% VS LA COMPETENCIA													

- Tarifas adicionales
- Límites de responsabilidad
- Precios IVA incluido
- Servicio técnico incluido durante el plazo
- Políticas de usos justos
- No incluye costo de cableado
- Usos legales

Figura 5.58 Paquete Conexión 10

NOTA: Costo de instalación en plazo a 24 meses de \$35 000.00, con o sin conmutador; en plazo a 36 meses no hay cobro por instalación.

Tabla 5.1 Costos del Proyecto

DISPOSITIVO	CANTIDAD	PRECIO UNITARIO	MARCA	COSTO
Computadora	24	\$6,000.00	Dell	\$144,000.00
Conmutador	1	Incluido en paquete	Avaya	
Teléfono Analógico	4	Incluido en paquete		\$13,900.00 por 36 meses
Teléfono digital	2	Incluido en paquete		
Switch 48 puertos	1	\$7,000.00	Foundry fastIron edge4802	\$7,000.00
Cable UTP Cat. 6	410 mts	\$3.00 por metro		\$1,230.00
			Total + IVA	\$166,130.00

CONCLUSIÓN

Durante la creación y desarrollo de éste proyecto nos dimos cuenta que existen instituciones del gobierno y áreas atrasadas en cuanto a las tecnologías y comunicaciones, por ello se buscó hablar con el encargado del área de informática de la Delegación Iztacalco para poder recomendarle algunas cuestiones sobre la necesidad de actualizar la red e implementar algunos equipos de comunicaciones que existen en el área de dicha delegación, para la adaptación de las nuevas tecnologías y su optimización y un mejoramiento de servicios de comunicaciones vía red de voz y datos por fibra óptica, por lo que se pretendió cambiar los equipos obsoletos por unos nuevos y también considerando el cambio cableado, para que acorto y largo plazo se logre ahorrar una cantidad considerable de dinero en el pago de dichos servicios y mejorando la calidad de estos para estar a la altura mundial de nuevas tecnologías de comunicación.

Este proyecto se basó en la necesidad de modernizar esta área para la concientización de directivos y personal que labora en el área de informática de la Secretaria de Turismo, en actualizarse y poder considerar nuestras recomendaciones ya que son factibles y necesarias para el mejoramiento de tecnología de telecomunicaciones. El diseño que se logró implementar demuestra que la tecnología usada actualmente ya es obsoleta y por lo que la propuesta de esta innovación que se propone, tendría un tiempo de vida aproximado de 15 años o más de vida útil, considerando la tecnología que actualmente utiliza la Secretaria de Turismo, en un año se gastaría en mantenimiento de estos equipos obsoletos lo mismo que se invertiría en este proyecto que consta de diseño, implementación, seguridad y administración de los equipos en el área de turismo a un largo plazo y reduciendo considerablemente los costos de mantenimiento y renta del servicio.

BIBLIOGRAFÍA

STALLINGS WILLIAM, “Fundamentos de Seguridad en Redes”, 2ª Edición, Pearson Educación, 4004, pp. 432

FRED HALSALL, “Redes de Computadores e Internet”, 5a edición, Pearson Educación, 2006, pp. 856.

PÁGINAS DE INTERNET

- <http://www.iusacellenlace.com.mx/?menuId=negocios§ion=internet&item=caracteristicas>
- http://www.iusacellenlace.com.mx/?menuId=negocios§ion=paquetes&item=conexion_10
- <http://www.iusacellenlace.com.mx/?menuId=negocios§ion=voz>
- <http://www.monografias.com/trabajos14/tipos-redes/tipos-redes.shtml>
- <http://www.monografias.com/trabajos-pdf/fibra-optica-maravilla-moderna/fibra-optica-maravilla-moderna.pdf>

GLOSARIO DE TÉRMINOS Y ACRÓNIMOS

VoIP: Voz sobre Protocolo de Internet, también llamado Voz sobre IP, Voz IP, VoIP (Voiceover IP).

OSI: Modelo de Interconexión de Sistemas Abiertos (open system interconnection).

ISO: Organización Internacional para la Estandarización (International Organization for Standardization).

ANSI: (American National Standards Institute, Instituto Americano de Normas).

FIREWALL: (pared a prueba de fuego) Conjunto de programas de protección y dispositivos especiales que ponen barreras al acceso exterior a una determinada red privada.

NAT: (Network Address Translation - Traducción de Dirección de Red) es un mecanismo utilizado por enrutadores IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles.

DIRECCION IP: La dirección IP de una máquina conectada a Internet es un número que identifica unívocamente a esa máquina (es decir, tan sólo esa máquina tiene ese número). Las direcciones IP constan de cuatro números que van del 0 al 255, y que se representan por dígitos decimales separados por puntos, como 123.456.1.1

FTP: (File Transfer Protocol, Protocolo de Transferencia de Archivos) Es un servicio de Internet que permite transferir archivos (upload y download) entre computadoras conectadas a Internet.

GATEWAY: Dispositivo de comunicación entre dos o más redes locales (LANs) y remotas, usualmente capaz de convertir distintos protocolos, actuando de traductor para permitir la comunicación.

HOST: Actualmente, sinónimo de **SERVIDOR**, y también se le conoce a los servidores que albergan como "HOST" a una o varias Páginas, pudiendo tener estas un nombre de dominio distinto a la del HOST en que se encuentren.

HTML: (Hyper text Markup Language, Lenguaje de Marcado de Hipertextos) Lenguaje que define textos, subgrupo del SGML, destinado a simplificar la escritura de documentos estándar.

HTTP: (Hypertext Transfer Protocol, Protocolo de Transferencia de Hipertexto) Es el mecanismo de intercambio de información que constituye la base funcional de la World Wide Web.

IP: (Internet Protocol) Protocolo de Internet definido en el RFC 791.

CAN: Campus Area Network, Red de Area Campus. Una CAN es una colección de LANs dispersadas geográficamente dentro de un campus (universitario, oficinas de gobierno, maquilas o industrias) pertenecientes a una misma entidad en una área delimitada en kilómetros. Una CAN utiliza comúnmente tecnologías tales como FDDI y Gigabit Ethernet para conectividad a través de medios de comunicación tales como fibra óptica y espectro disperso.

LAN: (Local Area Network, redes de área local) son las redes que todos conocemos, es decir, aquellas que se utilizan en nuestra empresa. Son redes pequeñas, entendiendo como pequeñas las redes de una oficina, de un edificio. Debido a sus limitadas dimensiones, son redes muy rápidas en las cuales cada estación se puede comunicar con el resto.

WAN: (Wide Area Network, redes de área extensa) son redes punto a punto que interconectan países y continentes. Al tener que recorrer una gran distancia sus velocidades son menores que en las LAN aunque son capaces de transportar una mayor cantidad de datos. El alcance es una gran área geográfica, como por ejemplo: una ciudad o un continente.

MAN: (MetropolitanArea Network, redes de área metropolitana) comprenden una ubicación geográfica determinada "ciudad, municipio", y su distancia de cobertura es mayor de 4 Kmts.

SERVIDOR: En una estructura cliente-servidor, se llama servidor a un programa que ofrece una serie de servicios, a los cuales se suele acceder por medio de programas especiales llamados clientes.

TIA: Asociación de la Industria de Telecomunicaciones.

EIA: Asociación de la Industria Electrónica

BRIDGES: Son equipos que unen dos redes actuando sobre los protocolos de bajo nivel, en el nivel de control de acceso al medio. Solo el tráfico de una red que va dirigido a la otra atraviesa el dispositivo. Esto permite a los administradores dividir las redes en segmentos lógicos, descargando de tráfico las interconexiones. Los bridges producen las señales, con lo cual no se transmite ruido a través de ellos.

BROADCAST. La transmisión de un mensaje enviado por todas las estaciones de trabajo conectadas en una red, sin ser específica para una estación.

CABLEADO HORIZONTAL Y HARDWARE DE CONEXIÓN. Proporcionan 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.

CABLEADO HORIZONTAL. Incorpora el sistema de cableado que se extiende desde el área de trabajo de telecomunicaciones hasta el cuarto de telecomunicaciones.

CABLEADO VERTICAL (BACKBONE). El propósito es proporcionar interconexiones entre cuartos de entrada de servicios, cuartos de equipo y cuartos de telecomunicaciones. Incluye la conexión vertical entre pisos en edificios de varios pisos.

El cableado vertical incluye medios de transmisión (cable), puntos principales e intermedios de conexión cruzada y terminaciones mecánicas. El cableado vertebral se debe implementar en una topología de estrella (jerárquica). Puesta a tierra para telecomunicaciones: brinda una referencia a tierra de baja resistencia para el equipo de telecomunicaciones. Sirve para proteger el equipo y el personal.

ETHERNET. Esquema de red realizada por las empresas: Digital, Intel y Xerox, codificado como IEEE 802.3.

GATEWAY. Son equipos para interconectar redes con protocolos y arquitecturas completamente diferentes a todos los niveles de comunicación. La traducción de las unidades de información reduce mucho la velocidad de transmisión a través de estos equipos.

HOST. Son generalmente empleados para identificar un nodo o computadora en una red que puede ser usada interactivamente, es decir, se puede conectar y desconectar a ella.

HUBS. Son equipos que permiten estructurar el cableado de las redes. La variedad de tipos y características de estos equipos es muy grande. En un principio eran solo concentradores de cableado, pero cada vez disponen de mayor número de capacidad de la red, gestión remota, etc. La tendencia es a incorporar más funciones en el concentrador. Existen concentradores para todo tipo de medios físicos.

MÓDEM: Son equipos que permiten a las computadoras comunicarse entre sí a través de líneas telefónicas; modulación y demodulación de señales electrónicas que pueden ser procesadas por computadoras. Los módems pueden ser externos (un dispositivo de comunicación) o interno (dispositivo de comunicación interno o tarjeta de circuitos que se inserta en una de las ranuras de expansión de la computadora).

NIC/MAU. "Network Interface Card" (Tarjeta de interfaz de red) o "Medium Access Unit" (Medio de unidad de acceso). Cada computadora necesita el "hardware" para transmitir y recibir información. Es el dispositivo que conecta la computadora u otro equipo de red con el medio físico. La NIC es un tipo de tarjeta de expansión de la computadora y proporciona un puerto en la parte trasera de la PC al cual se conecta el cable de la red. Hoy en día cada vez son más los equipos que disponen de interfaz de red, principalmente Ethernet, incorporadas. A veces, es necesario, además de la tarjeta de red, un transceptor. Este es un dispositivo que se conecta al medio físico y a la tarjeta, bien porque no sea posible la conexión directa (10 base 5) o porque el medio sea distinto del que utiliza la tarjeta.

NODO. Es cualquier dispositivo "inteligente", físicamente conectado a la red. Para una LAN se considera como nodos los servidores de terminales, estaciones de trabajo, host y cualquier hardware conectado. Un nodo LAN puede ser cualquier dispositivo que tiene una dirección IP.

PROTOCOLO. Cualquier estándar de comunicaciones en una red. Existen protocolos para trasladar bits por medio del cable de red. Otros protocolos son clasificados en las capas más altas del modelo OSI.

REPETIDORES. Son equipos que actúan a nivel físico. Prolongan la longitud de la red uniendo dos segmentos y amplificando la señal, pero junto con ella amplifican también el ruido. La red sigue siendo una sola, con lo cual, siguen siendo válidas las limitaciones en cuanto al número de estaciones que pueden compartir el medio.

ROUTERS. Son equipos de interconexión de redes que actúan a nivel de los protocolos de red. Permite utilizar varios sistemas de interconexión mejorando el rendimiento de la transmisión entre redes. Su funcionamiento es más lento que los bridges pero su capacidad es mayor. Permiten, incluso, enlazar dos redes basadas en un protocolo, por medio de otra que utilice un protocolo diferente.

RUTAS Y ESPACIOS HORIZONTALES. Son utilizados para distribuir y soportar cable horizontal y conectar hardware entre la salida del área de trabajo y el cuarto de telecomunicaciones, son los "contenedores" del cableado horizontal.