ESCUELA SUPERIOR POLITECNICA DEL LITORAL

Escuela de Diseño y Comunicación Visual

TÓPICO DE GRADUACIÓN

Previo a la obtención del título de

Analista de Soporte de Microcomputadores

Tema:

Manual de Administración y Seguridades de Redes

Empresa:

Grupo Romero

Autores:

Ronny Luís Vargas León
Johan Javier Larrea Buenaño
Kléber Javier Montiel Criollo

DIRECTOR:

Lsi. José Luís Ramírez

Año 2007

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

ESCUELA DE DISEÑO Y COMUNICACIÓN VISUAL

TÓPICO DE GRADUACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

ANALISTA DE SOPORTE DE MICROCOMPUTADORES

TEMA:
MANUAL DE ADMINISTRACIÓN Y SEGURIDADES DE REDES

EMPRESA:
GRUPO ROMERO

AUTORES:
RONNY LUÍS VARGAS LEÓN
JOHAN JAVIER LARREA BUENAÑO
KLÉBER JAVIER MONTIEL CRIOLLO

DIRECTOR:
LSI. JOSÉ LUÍS RAMÍREZ

AÑO:
2007

AGRADECIMIENTOS

Agradecemos a todos los docentes los cuales han sido nuestra guía en este difícil camino al éxito profesional, en especial al analista José Luís Ramírez por su ayuda incondicional en este tópico de graduación. A nuestros amigos de la universidad y a todos aquellos que de alguna u otra manera nos han ayudado en este proyecto.

DEDICATORIA

Queremos dedicar este manual a Dios a quien le debemos todo nuestro esfuerzo y dedicación, también a nuestros padres por el sacrificio que han hecho por nosotros para poder culminar con éxito nuestra carrera, y a nuestras familias y amigos que nos ayudaron durante el tiempo que ha durado nuestro estudio.

DECLARACIÓN EXPRESA

La responsabilidad por los hechos, ideas y doctrinas expuestas en este proyecto de Graduación / Tesis de grado nos corresponden exclusivamente. Y el patrimonio intelectual de la misma EDCOM (**Escuela de Diseño y Comunicación Visual)** de la escuela Superior Politécnica del Litoral

(Reglamento de Exámenes y Títulos profesionales de la ESPOL)

FIRMA DEL DIRECTOR DE TÓPICO

LSI. JOSÉ LUIS RAMÍREZ
DIRECTOR DE TÓPICO

FIRMA DE LOS AUTORES DE TÓPICO

SR. RONNY LUÍS VARGAS LEÓN

SR. JOHAN JAVIER LARREA BUENAÑO

SR. KLÉBER JAVIER MONTIEL CRIOLLO

ÍNDICE DE CONTENIDO

CAPÍTULO 1 GENERALIDADES

CAPÍTULO 2 SITUACIÓN ACTUAL

CAPÍTULO 3 ROUTERS

CAPÍTULO 4 NORMAS

CAPÍTULO 5 SOLUCIÓN PROPUESTA

CAPÍTULO 6 SEGURIDADES

ÍNDICE DE TABLAS

CAPÍTULO 1 GENERALIDADES

CAPÍTULO 2 SITUACIÓN ACTUAL

CAPÍTULO 3 ROUTERS

CAPÍTULO 5 SOLUCIÓN PROPUESTA

CAPÍTULO 6 SEGURIDADES

ÍNDICE DE FIGURAS

CAPÍTULO 4 NORMAS

CAPÍTULO 6 SEGURIDADES

CAPÍTULO 1

GENERALIDADES

1.1. INTRODUCCIÓN

El presente documento contiene la Situación Actual y Solución Propuesta de acuerdo a la empresa en que basamos el estudio. Dispositivos de Conmutación y Enrutamiento, para que las personas se involucren en lo que es el campo de las Redes y poder aprender configuraciones sencillas.

1.2. OBJETIVO DEL MANUAL

El objetivo del manual es servir de guía, consulta y ayuda a los Administradores de Red, Jefes Networking, y a todos los relacionados en esta área.

1.3. ¿A QUIÉN VA DIRIGIDO ESTE MANUAL?

Este manual esta dirigido al Jefe de Sistemas, autoridades de la empresa grupo romero. Jefes de Networking, Administradores de Redes y usuarios finales relacionados con el área.

1.4. LO QUE SE DEBE CONOCER

En este manual se ha procurado utilizar un lenguaje flexible, con miras a que tanto usuarios expertos como novatos puedan ayudarse con las configuraciones descritas tanto como para Dispositivos de Conmutación y Enrutamiento, para interpretarlo de mejor manera se necesita tener conocimientos básicos de redes.

1.5. ORGANIZACIÓN DEL CONTENIDO DEL MANUAL

El manual se divide en 4 capítulos, cada uno de los capítulos contiene un propósito específico. El contenido de cada capitulo tiene un propósito diferente. Los mismos que explicamos a continuación.

1.6. ORGANIZACIÓN DE ESTE MANUAL

Este manual está organizado en seis partes principales:

Generalidades	
Capítulo 1	**Generalidades** Explica brevemente el contenido de este manual.
Capítulo 2	**Situación Actual** Se especifica el estado de la empresa en el aspecto de redes, los dispositivos que cuenta en la actualidad así como el resultado de los mismos con sus problemas.
Capítulo 3	**Solución Propuesta** Aquí se le ha dado dos soluciones enfocados en los problemas que se ha encontrado detallando los requerimientos en factibilidades técnicas, operativas y económicas.
Capítulo 4	**Normas** Se refiere a los dispositivos, medios y enlaces que se implementarán en la solución propuesta.
Capítulo 5	**Implementación de Seguridades** En este Capítulo se habla de los aspectos de seguridad que se implementarán en la Empresa.
Capítulo 6	**Configuración de routers** Este Capítulo trata de las configuraciones que se implementaran en los routers de conexión

Tabla 1.1 Generalidades

1.7. ACERCA DE ESTE MANUAL

Este manual contiene diversas ilustraciones e instrucciones que debe seguir un administrador de redes para poder configurar equipos de enrutamiento y conmutación así como un servidor con sus respectivos servicios.

CAPÍTULO 2

SITUACIÓN ACTUAL

2.1. HISTORIA DE LA COMPAÑÍA: GRUPO ROMERO

Es uno de los grupos más exitosos que desarrolla productos estratégicos en el mercado nacional brindando buenos proyectos

Esta conformada por las siguientes empresas:

- Promotora Inmobiliaria Urbanis S.A. URBANIS (Villa España)
- Servicios Audio Video S.A. SERUVI (Administradora del Centro Comercial Mall del Sur)
- PROMOUTLET S.A. (Administradora del Centro Comercial Duran Outlet)
- Sambocity S.A. (Promotora Y Constructora de Villas)

Promotora Inmobiliaria Urbanis S.A. PROURBANIS es una compañía cuya función principal es la promoción de proyectos inmobiliarios e intermediación de bienes inmuebles.
Se encuentra Ubicada en la Cooperativa Mucho Lote Primera Etapa (Villa España).
Durante 7 años, Nuestro equipo ha logrado reunir una vasta experiencia en proyectos, avalúos e intermediación, además de las numerosas obras realizadas, las que constituyen nuestra mejor carta de presentación.

2.1.1. MISIÓN:

La misión de **Urbanis S.A.** es la de satisfacer las necesidades inmobiliarias de personas y empresas, desarrollando proyectos de calidad, que brinden bienestar, paz y felicidad al cliente.

Ser líderes en la promoción, desarrollo, intermediación y administración de proyectos inmobiliarios en el Ecuador, contribuyendo al desarrollo del país, fortaleciendo nuestro patrimonio, y posicionando nuestra imagen como la de promotores visionarios y exitosos.
Administrar eficientemente sus recursos humanos, tecnológicos y financieros, para lograr una rentabilidad que retribuya equitativamente a sus accionistas y colaboradores, participando así en el desarrollo social y económico del Ecuador.

2.1.2. VISIÓN:

Ser una compañía institucionalizada y en constante búsqueda de la excelencia como promotor inmobiliario y en nuestra relación con nuestros accionistas, socios, clientes, colaboradores y proveedores. Ofreciendo estándares más altos de calidad en nuestros productos y servicios, e impactando positivamente en el desarrollo de las comunidades en que nos desenvolvemos

2.1.3. VALORES:

Competitividad: la mejor ventaja competitiva es aprender más rápido que los demás.

- Liderazgo: siempre adelante del pelotón.

- Calidad: siempre mejorando con sinceridad.
- Ética personal y profesional: el bien siempre triunfa a largo plazo. Ética: conjunto de normas internas que impide que perjudiquemos a nuestros semejantes.
- Rentabilidad: Sin ser el fin, es un medio imprescindible. Sin utilidades la empresa quiebra y perdemos la oportunidad de servir a la sociedad.
- Análisis del entorno: que desean nuestros huéspedes? Cómo los podemos atender mejor que la competencia?
- Talento humano: los grandes y pequeños cambios que han hecho crecer a la humanidad, nacen con un pensamiento, los pensamientos nacen en la mente humana.

2.2. DISEÑO E IMPLEMENTACIÓN DE LA EMPRESA:

2.2.1. DISEÑO FÍSICO:

Con el siguiente gráfico se detalla la infraestructura de red de Urbanis, se muestra claramente le ubicación de los componentes en juego:

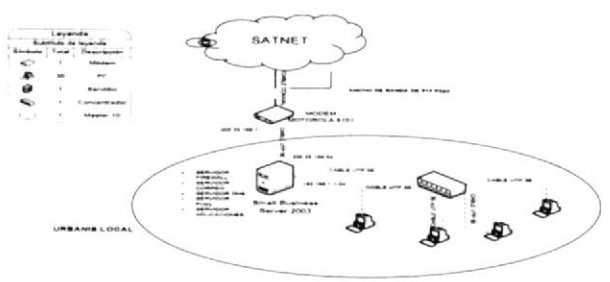


Figura 2.1.- Lan De Urbanis

Adicionalmente en el servidor se encuentra instalado Small Business Server 2003 con su respectivo Firewall (ISA Server 2004), dentro de este tenemos las bases de SQL del Sistema Comercial en las cuales se detalla:

- Módulo de Generación de Contratos
- Módulo de Facturación de Clientes y Otros
- Módulo de Cuentas por Cobrar de los Clientes
- Módulo de Inventario de las Villas
- Módulo de Escrituración

Adicionalmente hay un Sistemas Administrativo Financiero realizado en Cobol las cual contiene:

- Módulo de Contabilidad
- Módulo de Ingresos a Caja

2.2.2. SERVIDOR DE URBANIS

El Servidor Cuentan Con tres Tarjetas de red **10/100/1000 Mbps** y con las siguientes características:

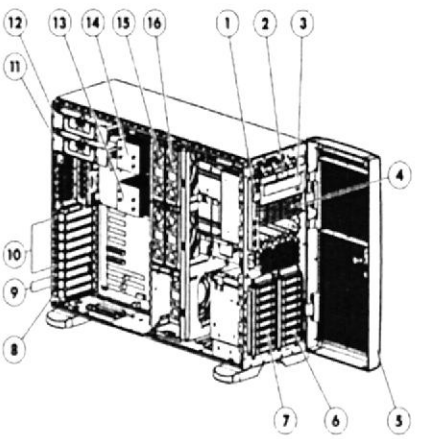
CANT	DESCRIPCIÓN	CARACTERÍSTICAS
1	 **HP ML 370 G5** Sistema operativo Windows 2003 Small Business Professional En este servidor se encuentran instalados los siguientes servicios: • Servidor DNS • Servidor de Correo • Firewall • Servidor de Datos • Servidor de Base de Datos	**Quad-Core** ML370T05 E5320 **Processor(s)** Quad-Core Intel Xeon Processor E5320 (1.86 GHz, 80 Watts, 1066 FSB) **HDD** HP 146GB 3G SAS 10K SFF SP HDD **Adicionales** HP 146GB 3G SAS 10K SFF SP HDD(2) **Cache Memory** 8MB (2 x 4MB) Level 2 cache - 5300 Sequence **Memory** 2 GB (2 x 1 GB); 1 memory card **Network Controller** Embedded NC373i Multifunction Gigabit Sever Adapters **Storage Controller** HP Smart Array P400/256MB Controller (RAID 0/1/1+0/5) **Hard Drive** None ship standard **Internal Storage** 1.168TB maximum **Optical Drive** 48x CD-ROM Drive (diskette optional) **Availability** Redundant Power/Fans Optional **Form Factor** Tower

Tabla 2 -1 Servidor De Urbanis

2.2.3. URBANIS 30 MÁQUINAS.

De las 30 estaciones de trabajo del edificio Urbanis, 6 equipos desktop marca (Dell), 2 equipos Portátiles marca (Dell) y 1 Portátil marca (HP), 10 equipos marca (xtratech) y 11 equipos Clones las cuales poseen las siguientes características:

MARCA	DESCRIPCIÓN	CARACTERÍSTICAS
DELL	Estaciones de trabajo	**Procesador: Pentium IV 3.2 GHZ** **Memoria: 512 MB** **Disco Duro: 160 GB**
DELL	Portátiles	**Procesador: Pentium IV 3.2 GHZ** **Memoria: 512 MB** **Disco Duro: 120**
HP	Portátil	**Procesador: Pentium IV 3.2 GHZ** **Memoria: 512 MB** **Disco Duro: 120 GB**
XTRATECH	Estaciones de trabajo	**Procesador: Pentium IV 2.8 GHZ** **Memoria: 512 MB** **Disco Duro: 80 GB**
CLON	Estaciones de Trabajo	**Procesador: Pentium IV 3.4 GHZ** **Memoria: 1 GB** **Disco Duro: 160 GB**

Tabla 2 -1 Máquinas Urbanis

- Planta baja, en este piso se encuentran instaladas 18 computadoras, en este piso se encuentra el Cuarto de Telecomunicaciones distribuidas por departamento de la siguiente manera

CANTIDAD	UBICACIÓN
10 Computadores	Departamento de Ventas
1 Computadora	Departamento de Caja
2 Computadores	Departamento de Sistemas
4 Computadores	Departamento de Operaciones
1 Computadora	Departamento de Cobranza

Tabla 2 -3 Máquinas Planta baja

- Planta Alta, en este piso se encuentran instaladas 12 computadoras por Departamento de la siguiente manera:

CANTIDAD	UBICACIÓN
3 Computadores	Departamento de Contabilidad
2 Computadora	Departamento Financiero
2 Computadores	Gerencia General
2 Computadores	Contraloría
1 Computadora	Administración General
1 Computadora	Gerencia de Comercialización
1 Computadora	Departamento de Planificación y Proyectos

Tabla 2 -4 Máquinas Planta Alta

2.2.4. TIPO DE CABLE USADO EN LA RED

CANTIDAD	DESCRIPCIÓN	FABRICANTE	UBICACIÓN	NOTAS
 500 METROS	CABLE AL GRANEL UTP CATG 5E	PANDUIT 1000ft Cat6 Gigabit Bulk Solid PVC Cable Blue	TODO CABLEADO HORIZONTAL	HACIA LAS ESTACIONES DE TRABAJOS
 300 METROS	CABLE AL GRANEL UTP CATG 5E	BELDEN DATA TWIST 350 AZUL	CAB HORIZONTAL	PARA LOS TELEFONOS

Tabla 2 -5 Tipo De Cable

2.3. MEDIOS DE COMUNICACIÓN

2.3.1. MEDIOS ALÁMBRICOS - URBANIS

Los medios alámbricos utilizados en el edificio de Urbanis son marca BELDEN distribuidos de la siguiente forma:

- Cable utp categoría 5e para las estaciones de trabajo y servidores a excepción de ciertos puntos antiguos con cable Cat 5e

2.3.2. MEDIOS INALÁMBRICOS - URBANIS

Los medios inalámbricos utilizados en el edificio Urbanis son los siguientes:

- Una antena de microondas a una frecuencia de 2.4 Ghz

La cual sirve como medio para comunicarse con la matriz Quito, utilizando la empresa porta que les hace de Carrier.

2.4. DISPOSITIVOS DE CONMUTACIÓN

2.4.1. MATRÍZ

Figura 2-1 Switch Matriz

CANT	UBICACIÓN	MARCA	MODELO	DESCRIPCIÓN
2	Planta Baja	D-LINK	**DES-1024D**	• Puertos: 24 puertos 10BASE-T/100BASE-TX con auto-detección y auto-configuración. • Interfaces para medios RJ 45 • Funciones de switching Ethernet: Velocidad total

Tabla 2-6 Características Del Switch mMatríz

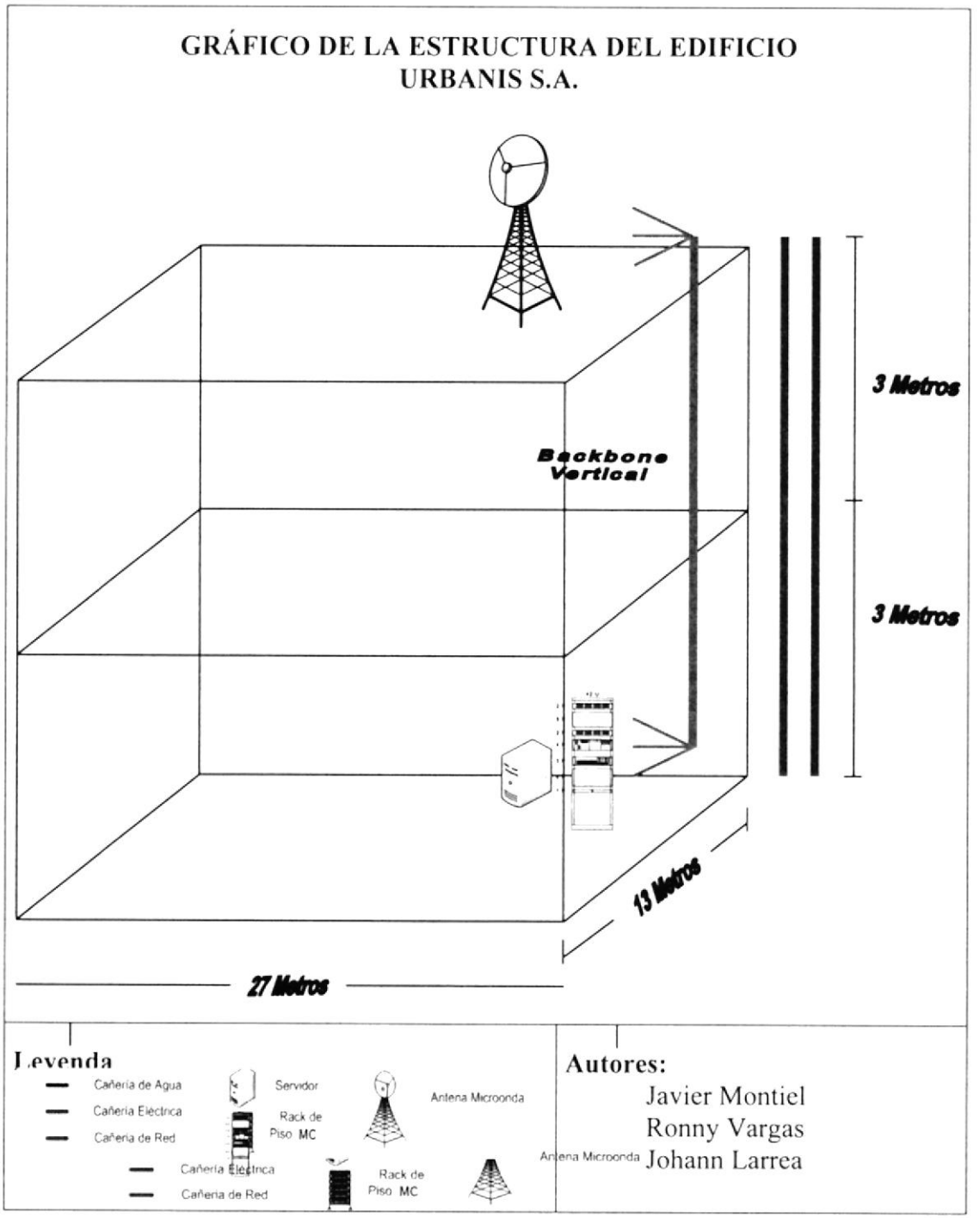


Figura 2-2 Estructura Del Edificio Urbanis

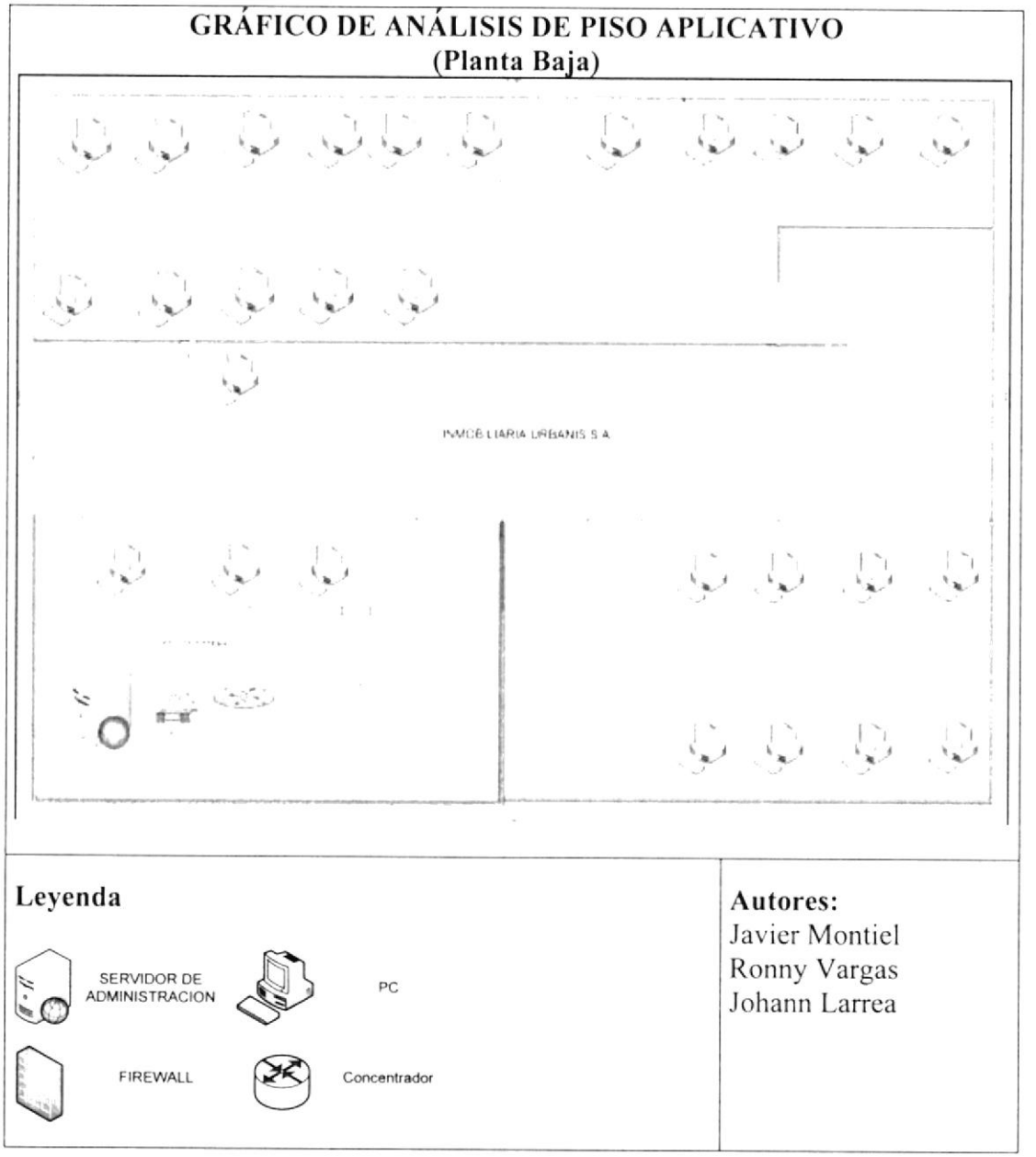
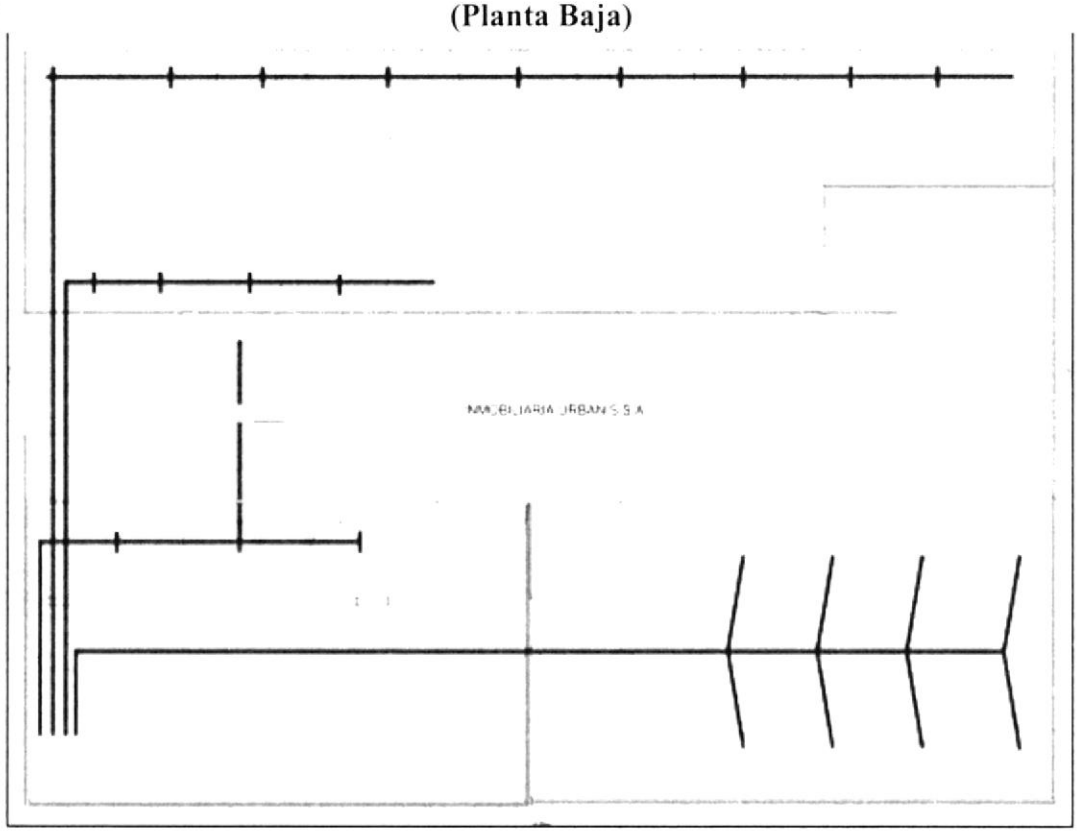


Figura 2-3 Análisis de piso aplicativo (Planta Baja)

GRÁFICO DE ANÁLISIS DE PISO LÓGICO
(Planta Baja)



Leyenda	**Autores:** Javier Montiel Ronny Vargas Johann Larrea

Figura 2-4 Análisis De Piso Lógico (Planta Baja)

2.5. MALL DEL SUR

El origen de esta compañía se remonta en el año 2003, tiempo durante el cual, esta empresa se dedica a la administración de la parte operativa y de control del Centro Comercial Mall del Sur, al igual que las demás entidades del Grupo Romero, cuenta con una estructura sólida a nivel organizacional que permite el manejo efectivo de los diferentes eventos y procesos que se suscitan dentro de dicho centro comercial.

La labor realizada hasta la actualidad ha sido recibida de manera satisfactoria por parte de los altos ejecutivos, motivo por el cual ha sido sujeta a muchos reconocimientos durante este lapso de tiempo de actividades.

2.5.1. VISIÓN:

Ser reconocido como el centro comercial de mayor prestigio en la zona sur de la ciudad de Guayaquil.

2.5.2. MISIÓN:

Dotar de instalaciones, que permitan que comerciantes nacionales e internacionales, puedan instalar sus negocios y ofrecer sus productos y servicios, bajo un marco de apego a las normas reglamentarias, que les aseguren a los comerciantes establecidos en el Centro Comercial poder disponer de bienes y servicios adecuados en lo que se refiere a administración, mantenimiento y publicidad necesarios para obtener un alto rendimiento de su actividad comercial. Constituirnos en una alternativa para la población del centro y sur de la ciudad, ya que pueden acceder a una serie de productos, de calidad y excelencia en el servicio, todo en un solo lugar.

2.6. DISEÑO E IMPLEMENTACIÓN DE LA EMPRESA:

2.6.1. DISEÑO FÍSICO:

Con el siguiente gráfico se detalla la infraestructura de red de la Administración del centro comercial Mall del Sur, se muestra claramente la ubicación de los componentes en juego:

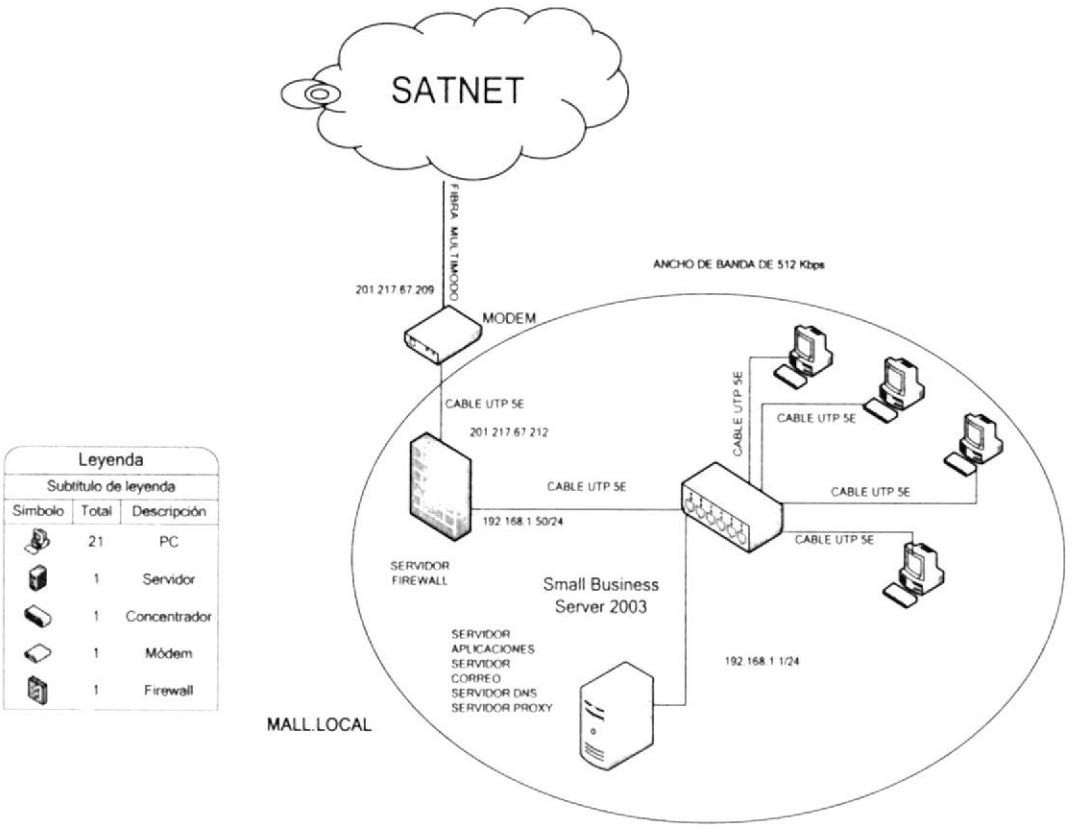


Figura 2.5.- Lan De Mall Del Sur

Adicionalmente en el servidor se encuentra instalado Small Business Server 2003, dentro de este tenemos las bases de SQL del Sistema Comercial en las cuales se detalla:

- Módulo de Generación de Contratos de Concesión
- Módulo de Facturación de Clientes u Otros (Valores mensuales de Concesión, Alícuotas, Reembolso de Gastos.
- Módulo de Cuentas por Cobrar y control de Cartera de los Clientes y locales
- Inventario y control de Los Locales del Centro Comercial

Adicionalmente hay un Sistemas Administrativo Financiero realizado en Cobol las cual contiene:

- Módulo de Contabilidad
- Módulo de Ingresos a Caja y Cierres de Caja
- Módulo de Nomina y Control de Roles de pagos

2.6.2. SERVIDOR DE MALL DEL SUR.

El Servidor cuentan con una Tarjetas de red **10/100/1000 Mbps** y con las siguientes características:

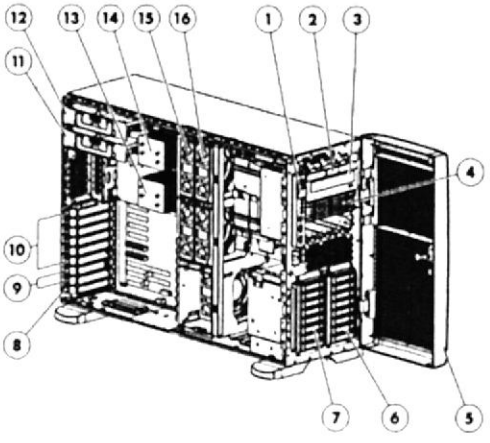
CANT	DESCRIPCIÓN	CARACTERÍSTICAS
1	 **HP ML 370 G5** Sistema operativo Windows 2003 Small Business STANDARD En este servidor se encuentran instalados los siguientes servicios: • Servidor DNS • Servidor de Correo • Servidor de Base de Datos 	**Quad-Core** ML370T05 E5320 **Processor(s)** Quad-Core Intel Xeon Processor E5320 (1.86 GHz, 80 Watts, 1066 FSB) **HDD** HP 146GB 3G SAS 10K SFF SP HDD **Adicionales** HP 146GB 3G SAS 10K SFF SP HDD(2) **Cache Memory** 8MB (2 x 4MB) Level 2 cache - 5300 Sequence **Memory** 2 GB (2 x 1 GB); 1 memory card **Network Controller** Embedded NC373i Multifunction Gigabit Sever Adapters **Storage Controller** HP Smart Array P400/256MB Controller (RAID 0/1/1+0/5) **Hard Drive** None ship standard **Internal Storage** 1.168TB máximum **Optical Drive** 48x CD-ROM Drive (diskette optional) **Availability** Redundant Power/Fans Optional **Form Factor** Tower
1	**FIREWALL** S.O. LINUX RED HAT 9.0	**Procesador: Pentium IV** 3.2 GHZ/800 MHZ **Memoria: 512 MB** 1 HDD de 120 GB

Tabla 2-7 Servidor Mall Del Sur

2.6.3. MALL DEL SUR. 21 MÁQUINAS

De las 18 estaciones de trabajo del edificio MALL DEL SUR, 5 equipos son marca (Dell), 2 equipos marca (HP), 10 son Clones y 1 equipo (COMPAQ) las cuales poseen las siguientes características:

- Planta Baja del Mall, se encuentran las Entidades Financieras, Comidas Rápidas, etc.

MARCA	DESCRIPCIÓN	CARACTERÍSTICAS
DELL	Estaciones de trabajo	**Procesador: Pentium IV 3.2 GHZ** **Memoria: 512 MB** **Disco Duro: 160 GB**
HP	Portátil	**Procesador: Pentium IV 3.2 GHZ** **Memoria:512 MB** **Disco Duro: 160 GB**
CLON	Estaciones de trabajo	**Procesador: Pentium IV 3.2 GHZ** **Memoria: 512 MB** **Disco Duro: 160 GB**
COMPAQ	Portátil	**Procesador: Pentium IV 3.2 GHZ** **Memoria: 512 MB** **Disco Duro: 160 GB**

Tablas 2-8 Máquinas Mall Del Sur

- En el segundo Nivel se encuentran las Oficinas Administrativas de Mall del Sur a la entrada de los baños principales de este Nivel, en la cual están instaladas 21 computadoras por departamento de la siguiente manera:

CANTIDAD	UBICACIÓN
1 Computadora	GERENCIA GENERAL
1 computadora	SUBGERENTE DE OPERACIONES
1 Computadora	MARKETING
1 Computadora	ASISTENTE DE OPERACIONES
1 Computadora	ASISTENTE DE MARKETING
1 Computadora	SISTEMAS

Tabla 2-9 Máquinas Mall Del Sur (Segundo Nivel)

CANTIDAD	UBICACIÓN
1 Computadora	ASISTENTE DE MARKETING
1 Computadora	CONTADOR
1 Computadora	ASISTENTE CONTABLE
1 Computadora	CAJA
1 Computadora	COBRANZA
1 Computadora	SUB GERENTE FINANCIERO
1 Computadora	CUARTO DE CAMARAS
1 Computadora	ASISTENTE DE MARKETING

Tabla 2-10 Computadoras Segundo Nivel

2.6.4. TIPO DE CABLE USADO EN LA RED

CANTIDAD	DESCRIPCIÓN	FABRICANTE	UBICACIÓN	NOTAS
 320 Mt	CABLE AL GRANEL UTP CAT. 6	PANDUIT 1000ft Cat6 Gigabit Bulk Solid PVC Cable Blue	TODO CABLEADO HORIZONTAL	HACIA LAS ESTACIONES DE TRABAJOS
 250 Mt	CABLE AL GRANEL UTP CAT. 5E	BELDEN DATA TWIST 350 AZUL	CAB HORIZONTAL	PARA LOS TELEFONOS

Tabla 2-11 Tipo De Cable Segundo Nivel

2.7. MEDIOS DE COMUNICACIÓN

2.7.1. MEDIOS ALAMBRICOS – MALL SUR

Los medios alambricos utilizados en el Centro Comercial de Guayaquil son marca BELDEN distribuidos de la siguiente forma:

- Cable utp categoría 6 para las estaciones de trabajo y servidores

2.7.2. MEDIOS INALÁMBRICOS - MALL SUR

Los medios inalámbricos utilizados en el edificio matriz Guayaquil son los siguientes:

- Un Router LINKSYS a una frecuencia de 2.4 Ghz Ubicado en le Departamento de Sistemas.

2.8. DISPOSITIVOS DE CONMUTACIÓN

2.8.1. MALL SUR

Figura 2-6 Switch Mall Del Sur

CANT	UBICACIÓN	MARCA	MODELO	DESCRIPCIÓN
2	SEGUNDO NIVEL	3COM	**4400**	• Puertos: 24 puertos 10BASE-T/100BASE-TX con auto-detección y auto-configuración. • Interfaces para medios RJ 45 • Funciones de switching Ethernet: Velocidad total

Tabla 2-12 Características De Switch Mall Del Sur

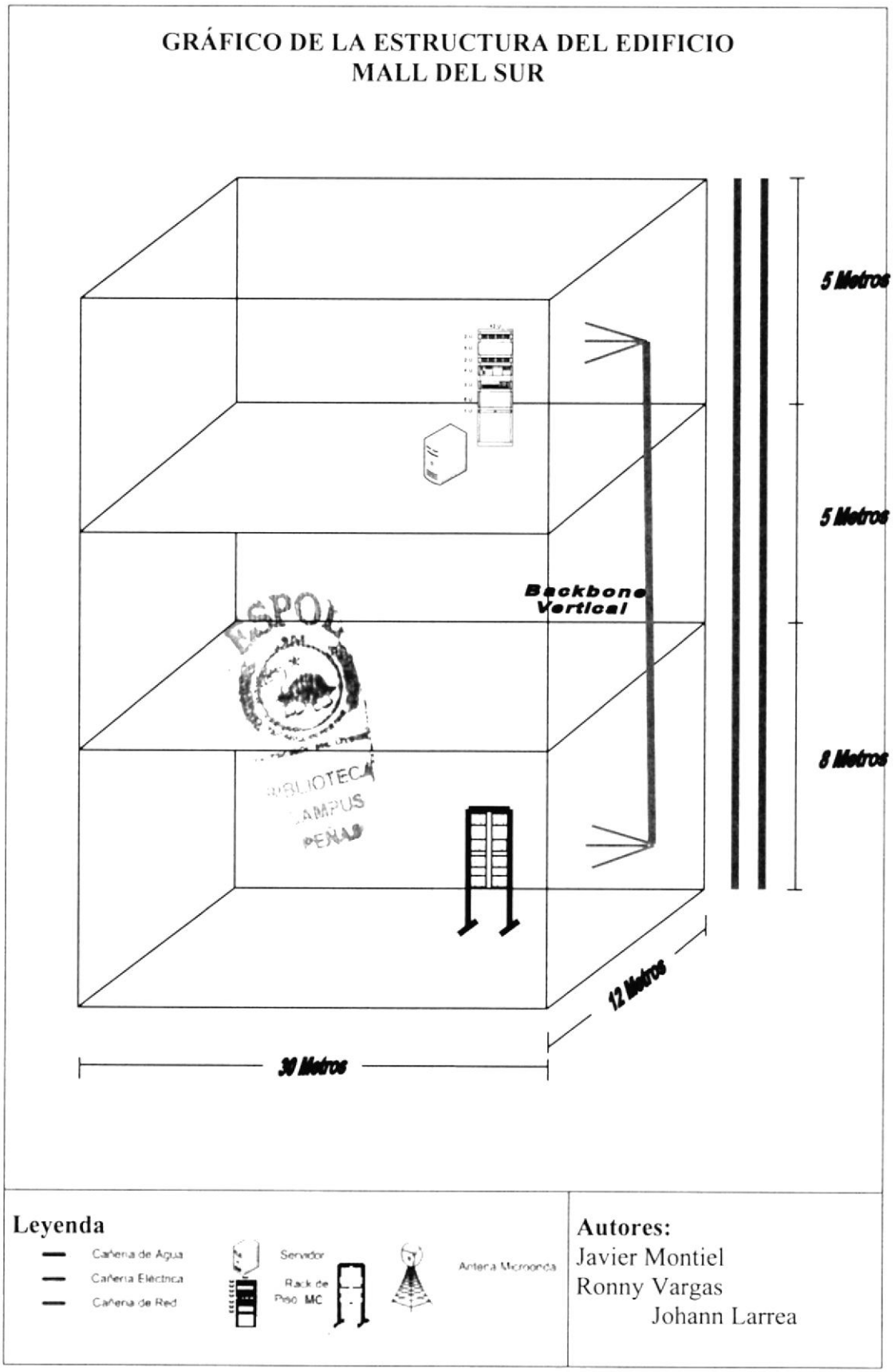


Figura 2-7 Estructura Mall del Sur

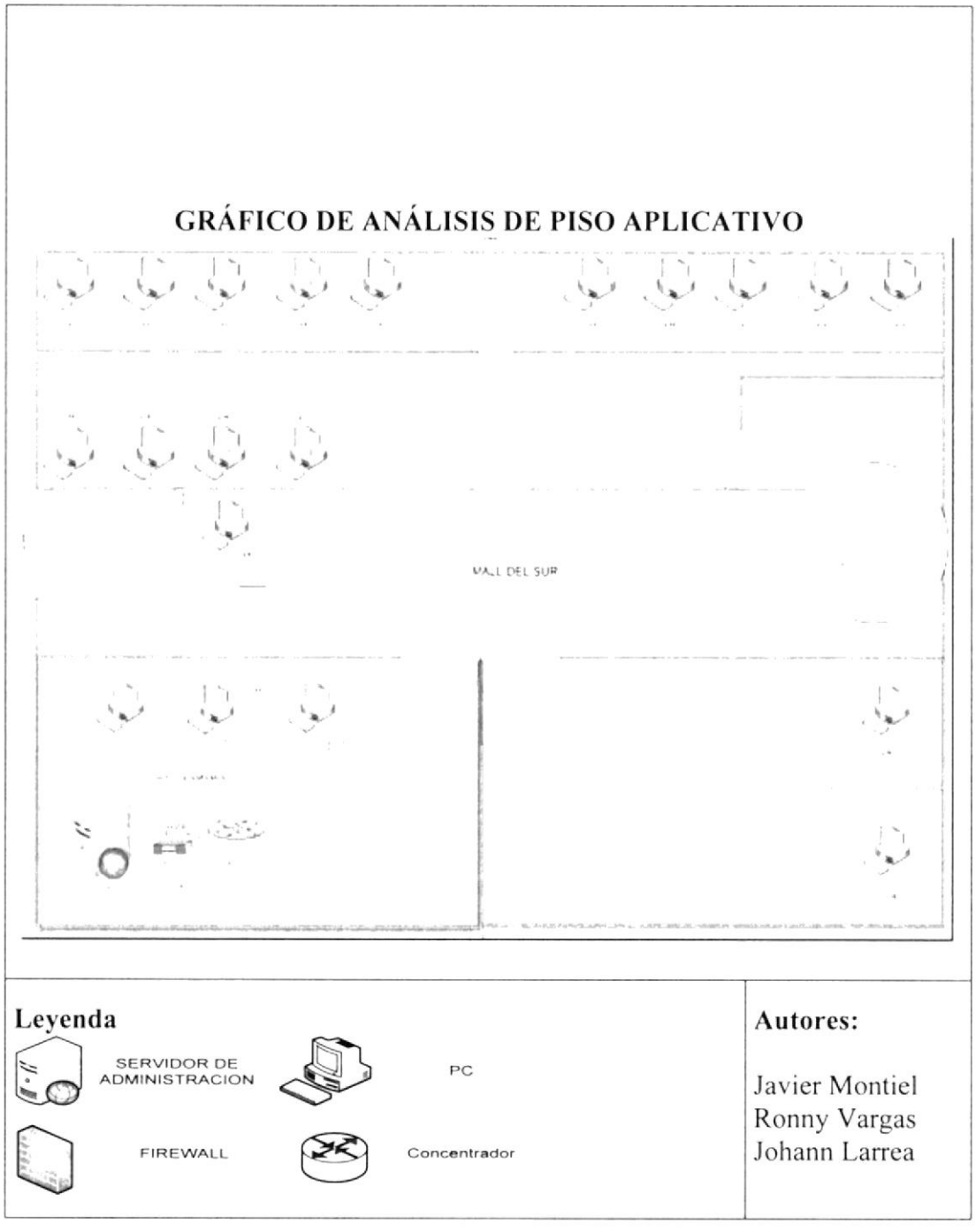


Figura 2-8 Análisis de piso Aplicativo Mall Del Sur

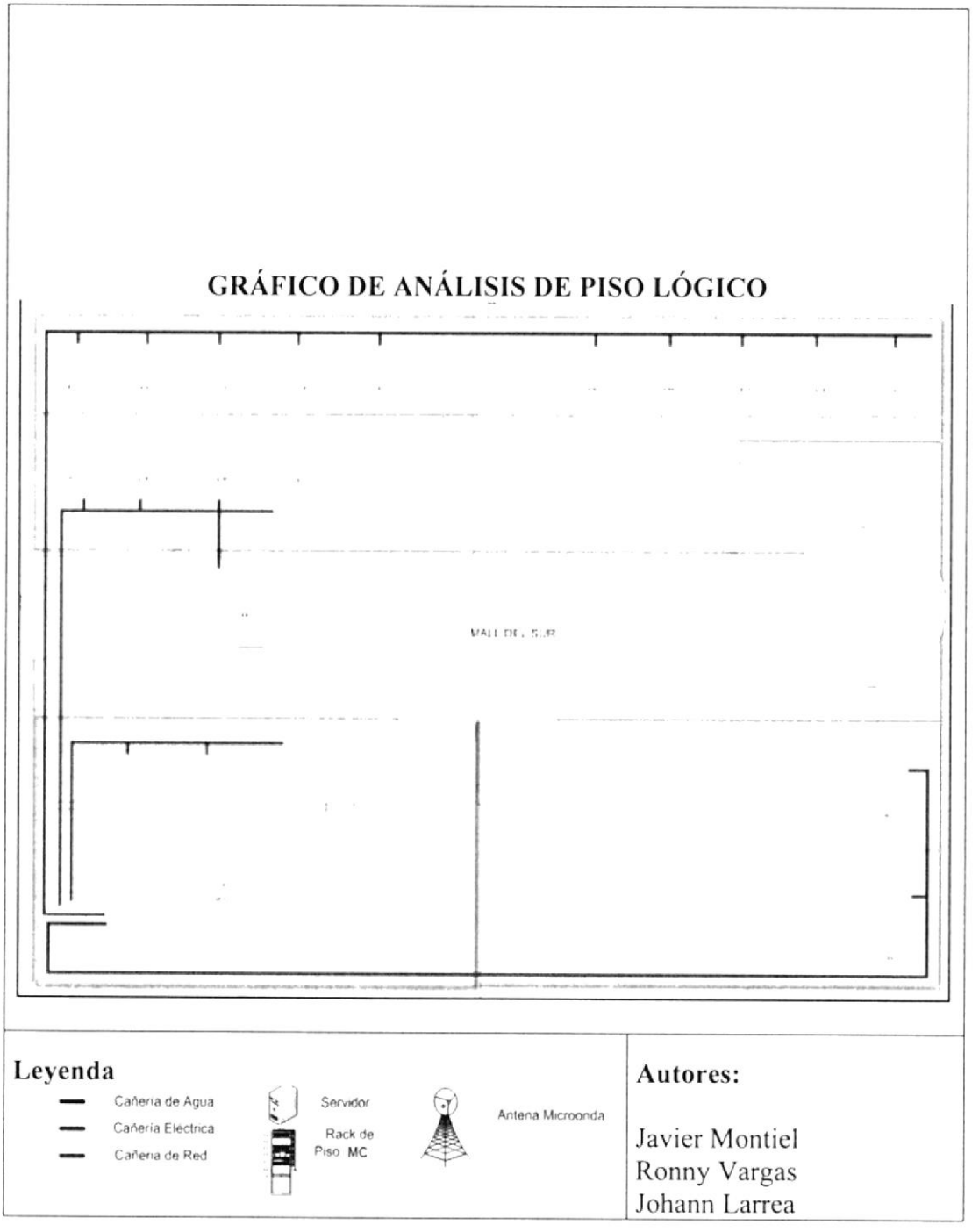


Figura 2-9 Análisis De Piso Lógico Mall Del Sur

2.9. DURAN OUTLET

2.9.1. VISIÓN:

Ser reconocido como el primero y mejor centro comercial de DURAN y acoger a todos los clientes de esta zona.

2.9.2. MISIÓN:

Dotar de instalaciones, que permitan que comerciantes nacionales e internacionales, puedan instalar sus negocios y ofrecer sus productos y servicios, bajo un marco de apego a las normas reglamentarias, que les aseguren a los comerciantes establecidos en el Centro Comercial poder disponer de bienes y servicios adecuados en lo que se refiere a administración, mantenimiento y publicidad necesarios para obtener un alto rendimiento de su actividad comercial. Constituirnos en una alternativa para la población de DURAN, ya que pueden acceder a una serie de productos, de calidad y excelencia en el servicio, todo en un solo lugar.

2.9.3. DISEÑO E IMPLEMENTACIÓN DE LA EMPRESA:

Diseño Físico:

Con el siguiente gráfico se detalla la infraestructura de red de Duran Outlet, se muestra claramente le ubicación de los componentes en juego:

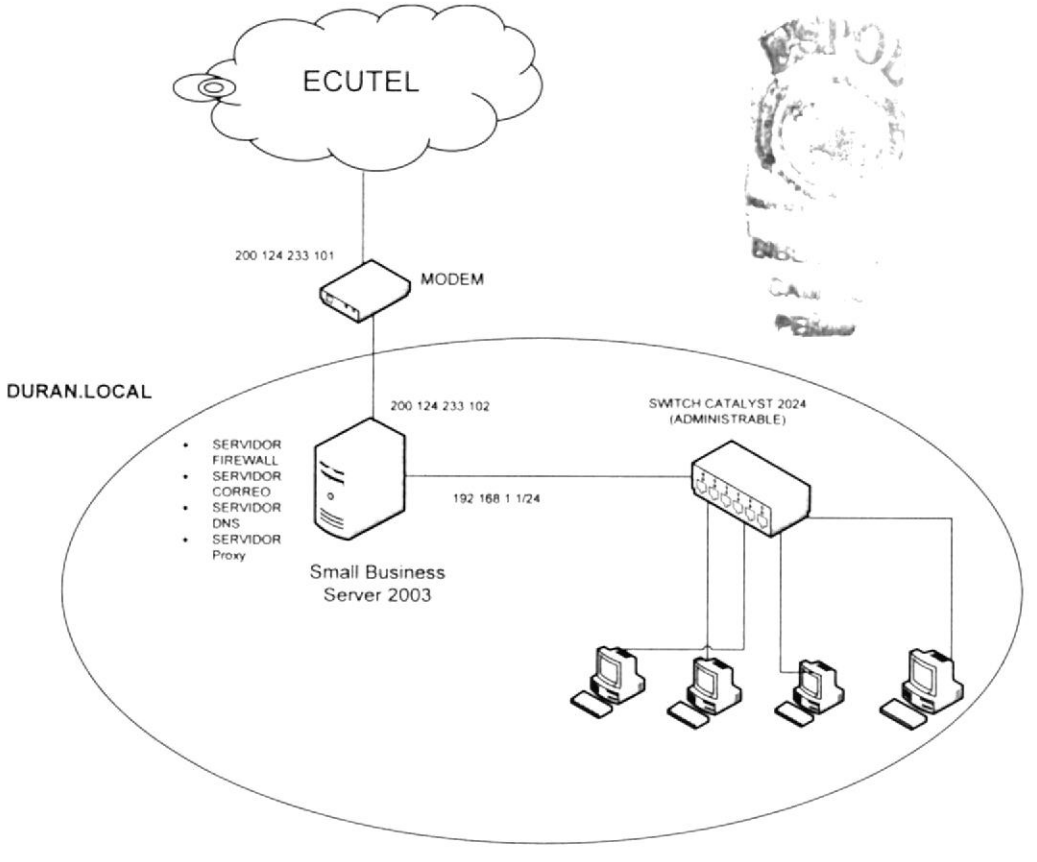


Figura 2.10.- Lan De Duran Outlet

2.9.4. SERVIDOR DE DURAN OUTLET

El Servidor Cuentan Con tres Tarjetas de red **10/100/1000 Mbps** y con las siguientes características:

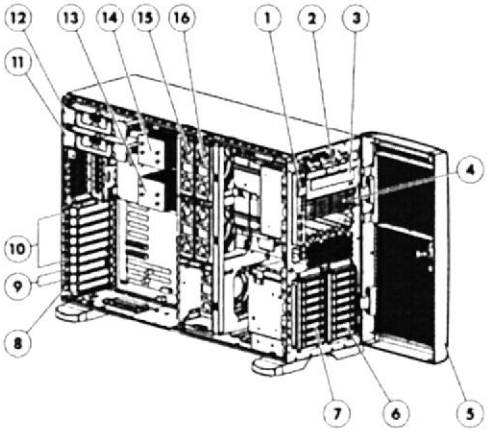
CANT	DESCRIPCIÓN	CARACTERÍSTICAS
1	 **HP ML 370 G3** Sistema operativo Windows 2003 Small Business Professional En este servidor se encuentran instalados los siguientes servicios: • Servidor DNS • Servidor de Correo • Firewall • Servidor de Base de Datos	**Quad-Core** ML370T05 E5320 **Processor(s)** Quad-Core Intel Xeon Processor E5320 (1.86 GHz, 80 Watts, 1066 FSB) **HDD** HP 80GB 3G SAS 10K SFF SP HDD **Adicionales** HP 80GB 3G SAS 10K SFF SP HDD(2) **Cache Memory** 8MB (2 x 4MB) Level 2 cache - 5300 Sequence **Memory** 2 GB (2 x 1 GB); 1 memory card **Network Controller** Embedded NC373i Multifunction Gigabit Sever Adapters **Hard Drive** None ship standard **Internal Storage** 1.168TB máximum **Optical Drive** 48x CD-ROM Drive (diskette optional) **Availability** Redundant Power/Fans Optional **Form Factor** Tower

Tabla 2-13 Servidor Duran Outlet

2.9.5. DURAN OUTLET 13 MÁQUINAS

MARCA	DESCRIPCIÓN	CARACTERÍSTICAS
DELL	Estaciones de trabajo	**Procesador: Pentium IV 3.2 GHZ** **Memoria: 512 MB** **Disco Duro: 160 GB**
HP	Portátil	**Procesador: Pentium IV 3.2 GHZ** **Memoria: 512 MB** **Disco Duro: 160 GB**
CLON	Estaciones de trabajo	**Procesador: Pentium IV 3.2 GHZ** **Memoria: 512 MB** **Disco Duro: 160 GB**
COMPAQ	Portátil	**Procesador: Pentium IV 3.2 GHZ** **Memoria: 512 MB** **Disco Duro: 160 GB**
TOSHIBA	Portátil	**Procesador: Pentium IV 3.2 GHZ** **Memoria: 512 MB** **Disco Duro:160 GB**

Tabla 2-14 Máquinas Duran Outlet

2.9.6. TIPO DE CABLE USADO EN LA RED

CANTIDAD	DESCRIPCIÓN	FABRICANTE	UBICACIÓN	NOTAS
 160 Mt	CABLE AL GRANEL UTP CAT. 6	1000ft Cat6 Gigabit Bulk Solid PVC Cable Blue	TODO CABLEADO ORIZONTAL	HACIA LAS ESTACIONES DE TRABAJOS
 250 Mt	CABLE AL GRANEL UTP CAT. 5E	BELDEN DATA TWIST 350 AZUL	CAB ORIZONTAL	PARA LOS TELEFONOS

Tabla 2-15 Tipo De Cable Duran

- En la Planta Baja se encuentran ubicadas las oficinas administrativas del Centro Comercial en la cual están instaladas 13 computadoras por departamento de la siguiente manera:

CANTIDAD	UBICACIÓN
1 computadora	SUBGERENTE DE OPERACIONES
1 Computadora	SUBGERENTE DE MARKETING
1 Computadora	SISTEMAS
1 Computadora	CONTADOR
1 Computadora	RECEPCION Y CAJA
1 Computadora	COBRANZA
1 Computadora	SUB GERENTE FINANCERO
1 Computadora	CUARTO DE CAMARAS
1 Computadora	CUARTO DE VIDEOS
1 Computadora	CUARTO DE CORREO
1 Computadora	MANTENIMIENTO
1 Computadora	SEGURIDAD
1 Computadora	LIMPIEZA

Tabla 2-16 Computadoras Planta Baja

2.10. MEDIOS DE COMUNICACIÓN

2.10.1. MEDIOS ALAMBRICOS – DURAN OUTLET

Los medios alambricos utilizados en el edificio matriz de Guayaquil son marca BELDEN distribuidos de la siguiente forma:

- Cable utp categoría 6 para las estaciones de trabajo y servidores
- Lo que es tendido de voz se utiliza Cable Utp Cat. 5e.

2.10.2. MEDIOS INALÁMBRICOS - DURAN OUTLET

Los medios inalámbricos utilizados en el C.C. Duran Outlet son los siguientes:

- Una Router Inalámbrico Linksys a una frecuencia de 2.4 GHz

2.11. DISPOSITIVOS DE CONMUTACION

2.11.1. DURAN OUTLET

Figura 2-11 Switch Duran Outlet

CANT	UBICACIÓN	MARCA	MODELO	DESCRIPCIÓN
2	SEGUNDO NIVEL	3COM	4400	Puertos: 24 puertos 10BASE-T/100BASE-TX con auto-detección y auto-configuración. Interfaces para medios RJ 45 Funciones de switching Ethernet: Velocidad total

Tabla 2-17 Características Switch Duran

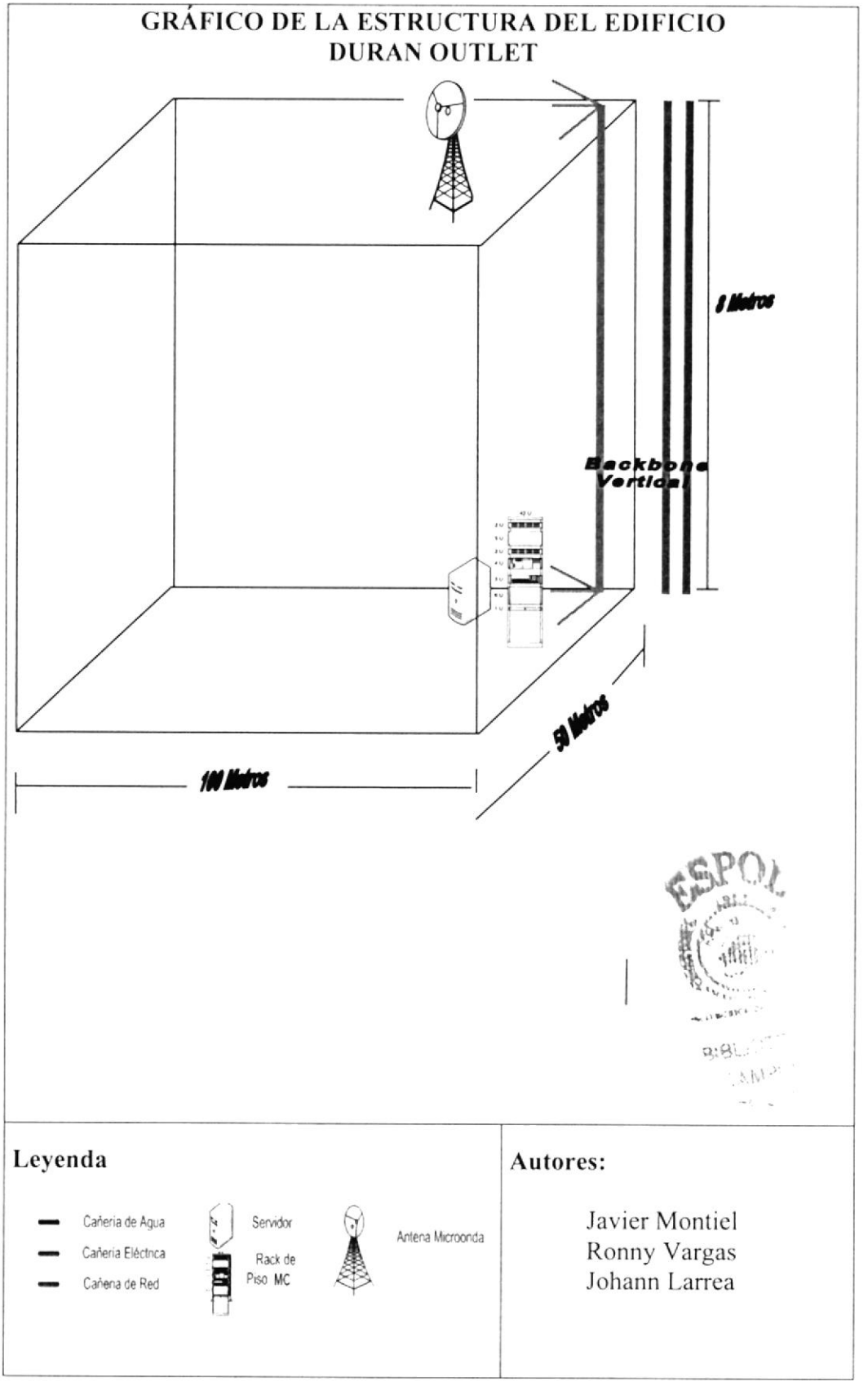


Figura 2-12 Edificio Duran Outlet

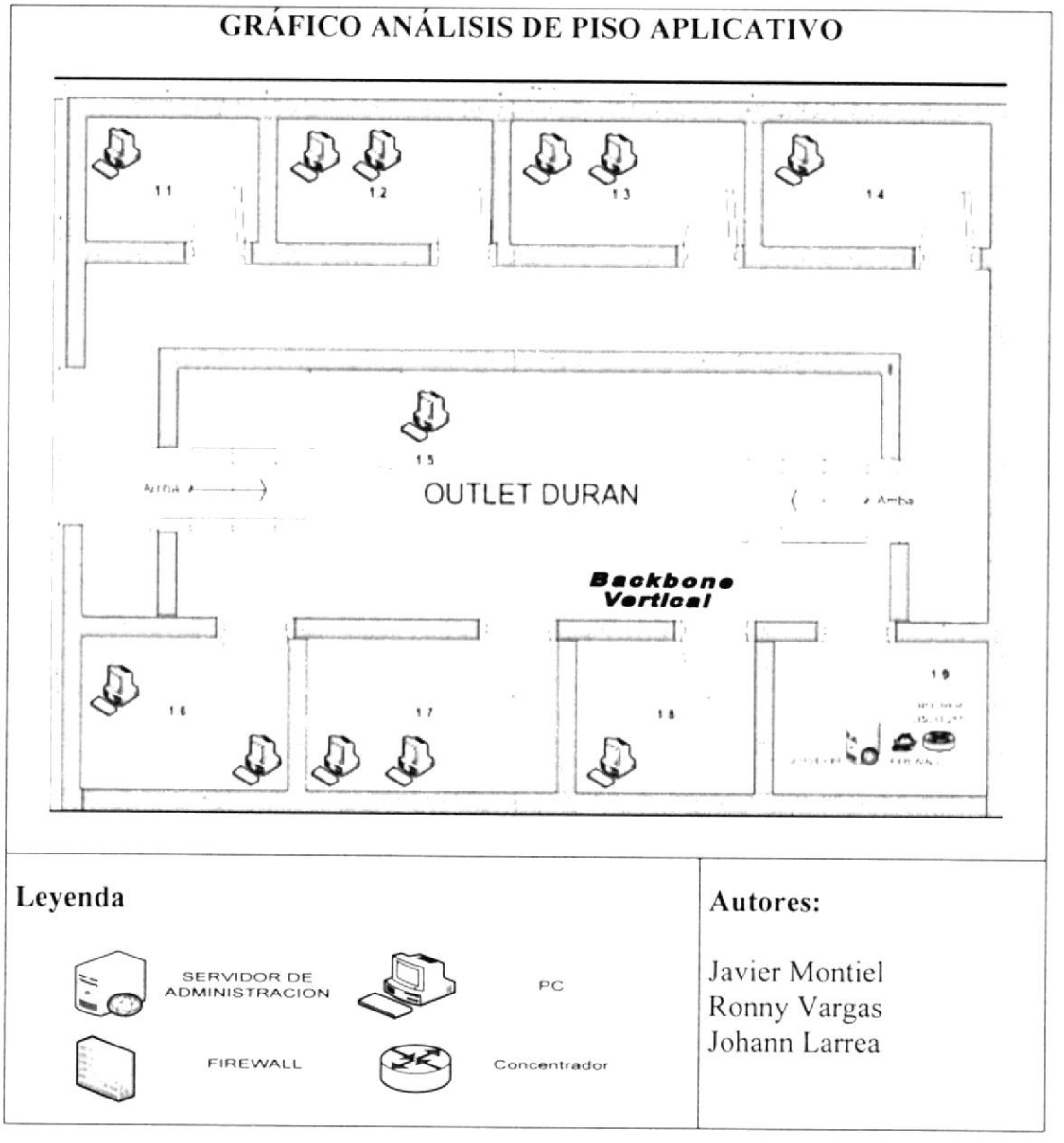


Figura 2-13 Análisis De Piso Aplicativo Duran

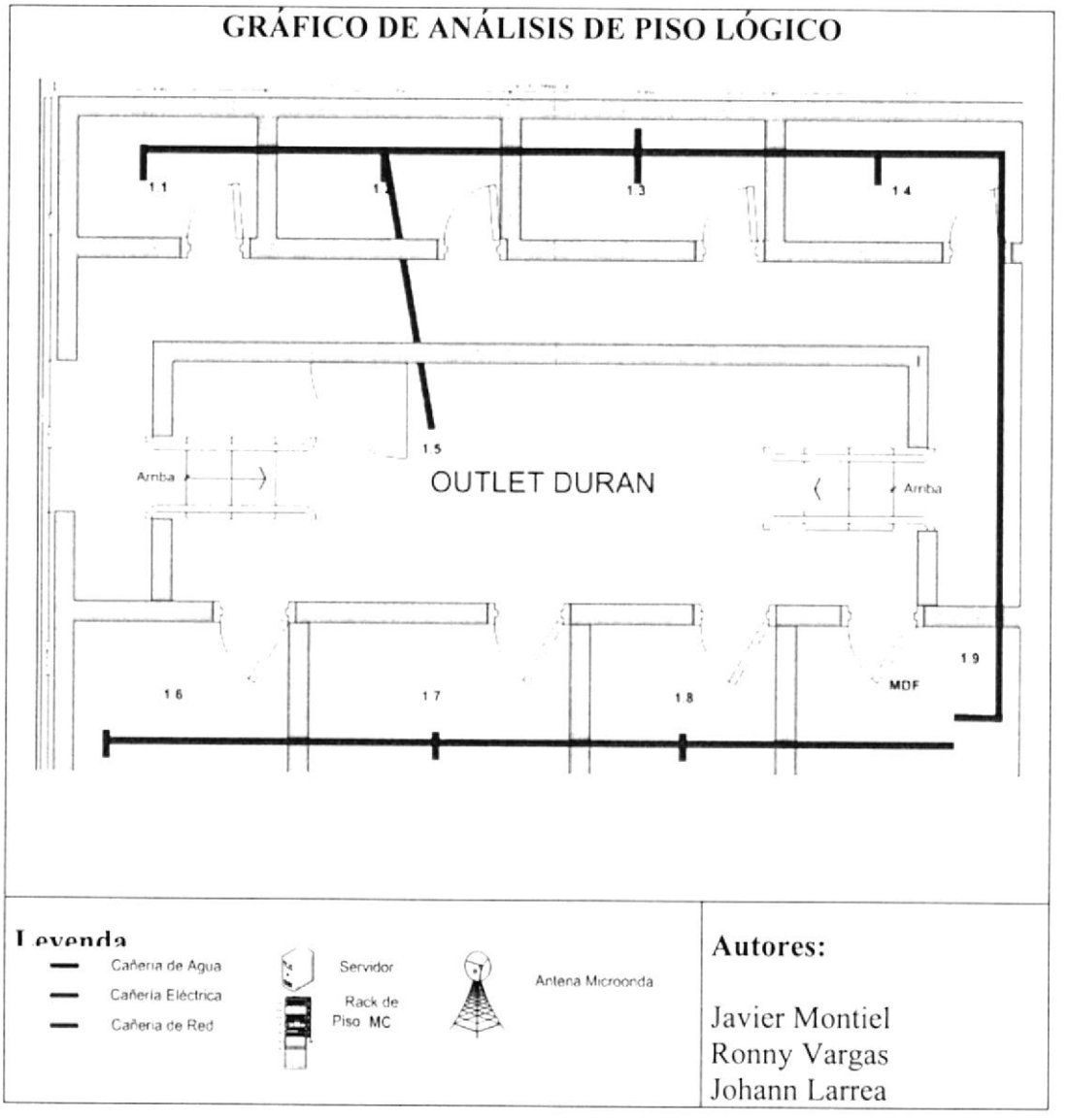


Figura 2-14 Análisis De Piso Lógico Duran

2.11.2. INFRAESTRUCTURA WAN

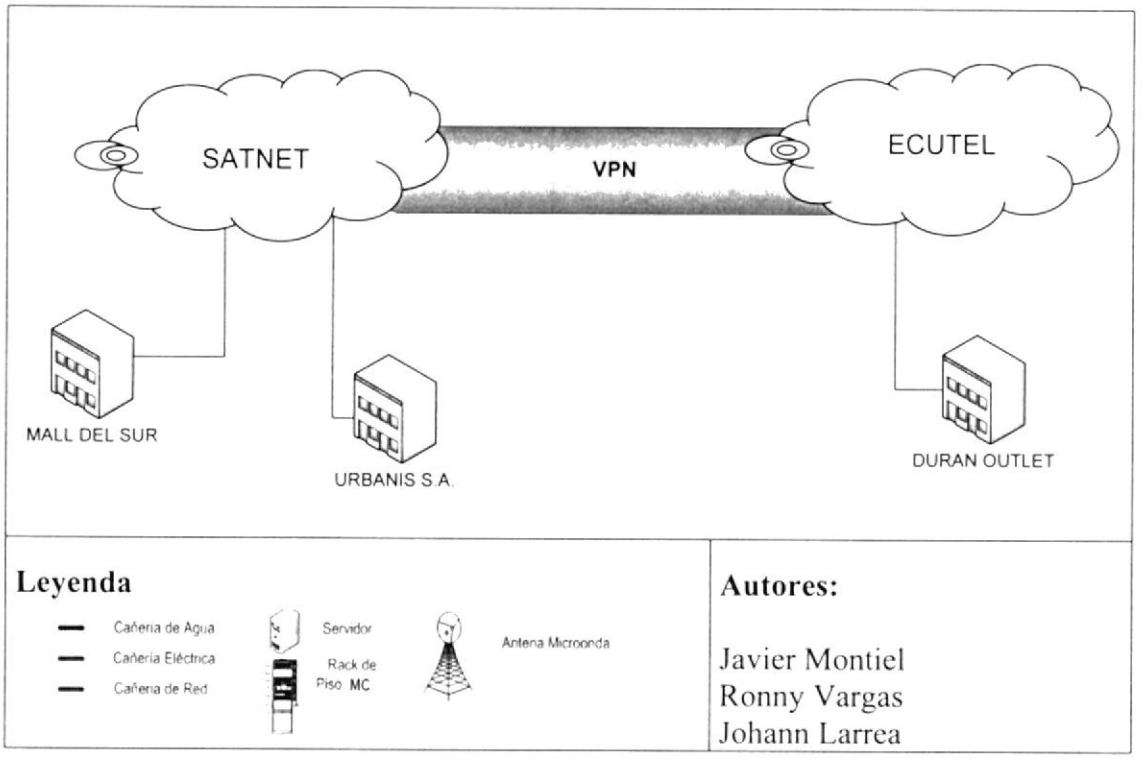


Figura 2-15 Infraestructura Wan A Nivel Medios De Comunicación

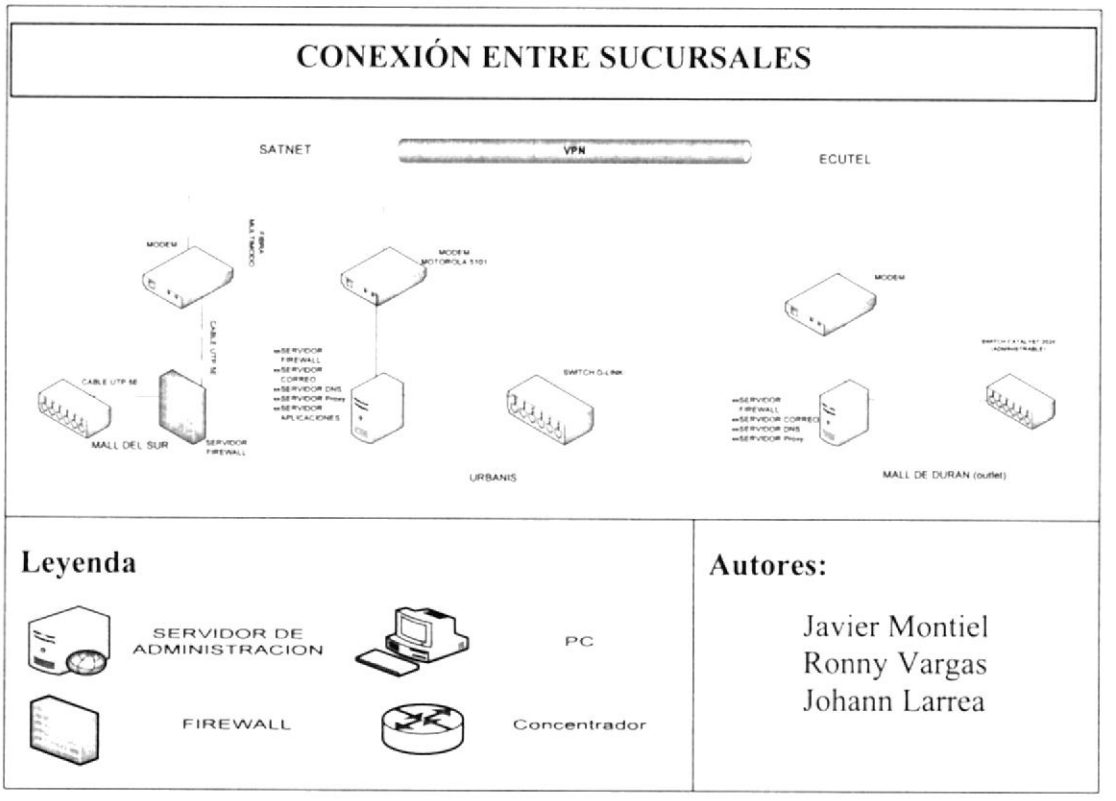


Figura 2-16 Conexión Entre Sucursales

2.11.3. ANCHO DE BANDA

URBANIS – MATRIZ

ANCHO DE BANDA	MEDIO
512 Mbps	Línea dedicada

Tabla 2-18 Ancho De Banda Matriz

2.11.4. MALL DEL SUR

ANCHO DE BANDA	MEDIO
512 Mbps	Línea dedicada

Tabla 2-19 Ancho De Banda Mall Del Sur

2.11.5. DURAN OUTLET

ANCHO DE BANDA	MEDIO
256 Mbps	Línea dedicada

Tabla 2-20 Ancho De Banda Duran Outlet

2.12. PROBLEMA - CAUSA – EFECTO

PROBLEMA	CAUSA	EFECTO
No poseen normas de cableado estructurado en la red Lan	▪ Falta de conocimiento por parte del departamento técnico. ▪ Descuido por parte de la empresa.(Directivos).	▪ Dificultad al momento de solucionar un problema en la red.(cables) ▪ No cuentan con protección ante siniestros.
Saturación en su red LAN	▪ No hay redes segmentadas. ▪ Mala administración por parte del encargado de la red	▪ Colisión al momento de acceder a los recursos de la red, forzando el reenvió de paquetes.
No existe un Respaldo para la comunicación WAN	• Falta de equipos de Respaldo para la comunicación WAN	• Si el ISP fallara no se podría realizar operaciones en Línea.
Existen Switch capa 2	• Factor económico	• Las IP son tomadas al azar no existe una Administración en lo que es la red
El rack de Matriz esta dentro del Dpto. Sistemas	• Por espacio Físico y Mala Planificación de la construcción	• No existe seguridad para los equipos que se encuentran en el rack.

Tabla 2-21 Problema Causa Efecto

2.13. PROBLEMA - SOLUCIÓN

PROBLEMA	SOLUCIÓN
No existe segmentación	Segmentar por departamentos los edificios de Matriz y sucursales.
No poseen normas de cableado estructurado en la red Lan	• Realizar un nuevo cableado estructurado conforme a las normas para categoría 6.
Saturación en su red LAN	▪ Segmentar las redes por área de trabajo. ▪ Verificar las cascadas de los switches e implementar políticas de administración de la red.
No existe un Respaldo para la comunicación WAN	Implementar una nueva infraestructura para respaldo
No existe ni un switch Administrable dentro de la Organización	Adquirir un Switch de capa 3 Administrable para poder organizar por IP los departamentos a segmentar.
El rack de Matriz esta dentro del Dpto. Sistemas	Creación de un cuarto independiente para el rack de Matriz.

Tabla 2-22 Problema Solución

CAPÍTULO 3

ROUTER

3.1. INTRODUCCIÓN A LOS ROUTERS

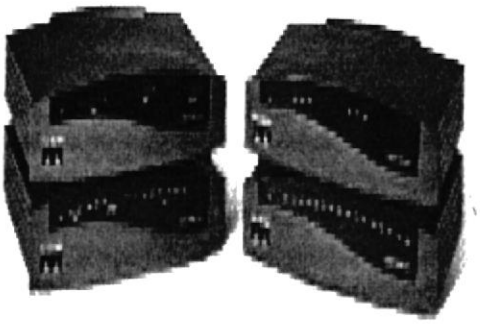


Figura 3-1 Routers

Un router trabaja mediante protocolos enrutamientos específicamente para nivel wan, a su vez es un dispositivo de hardware para interconexión de redes de las computadoras que opera en la capa tres (nivel de red) del modelo OSI.
El router se interconecta con diferentes segmentos de red, o algunas veces hasta redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red.

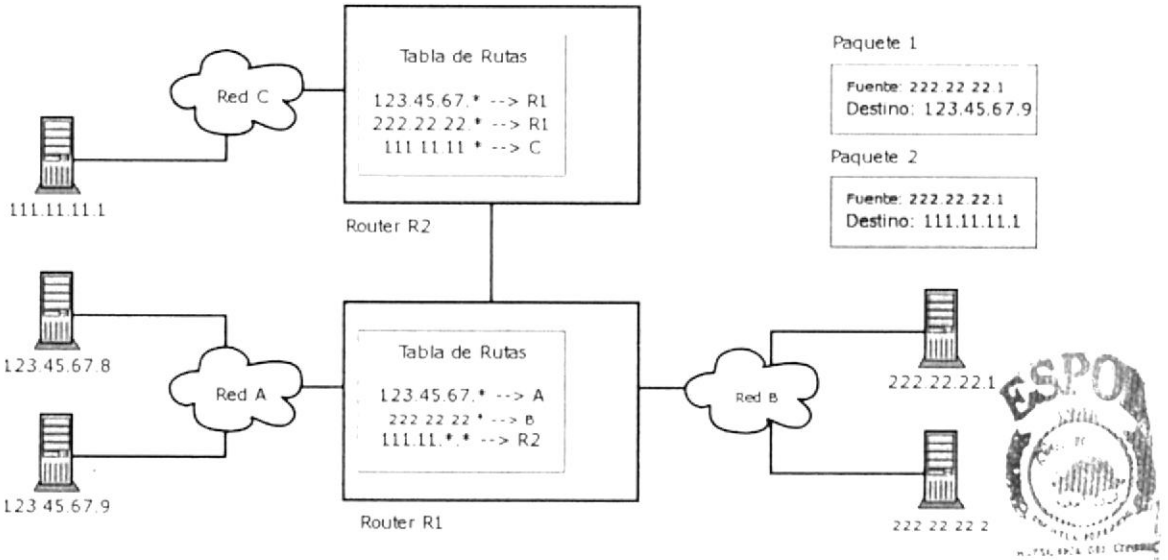


Figura 3-2 Conexiones De Segmentos De Red

El router toma decisiones basadas en diversos parámetros con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego redirige los paquetes hacia el segmento y el puerto de salida adecuados. Una de las más importantes es decidir la dirección de la red hacia la que va destinado el paquete (En el caso del protocolo IP esta sería la dirección IP). Otras decisiones son la carga de tráfico de red en las distintas interfaces de red del router y establecer la velocidad de cada uno de ellos, dependiendo del protocolo que se utilice

3.1.1. INTERFAZ DTE-DCE

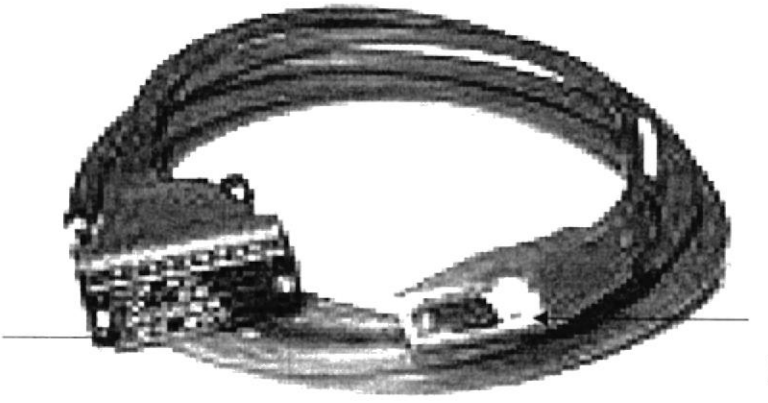


Figura 3-3 DCE - DTE

Para analizar las características del nivel físico del modelo OSI es indispensable considerar las características del canal de salida de datos del puerto de salida del equipo emisor de datos conocido normalmente como Equipo Terminal de Datos (DTE) y las del canal de entrada de datos del puerto de entrada de datos del equipo receptor de datos denominado normalmente Equipo de Terminación del Circuito de Datos (DCE). Este equipo puede incluso constituir el equipo de comunicación de datos o una parte de él.

3.2. COMPONENTES INTERNOS DEL ROUTER

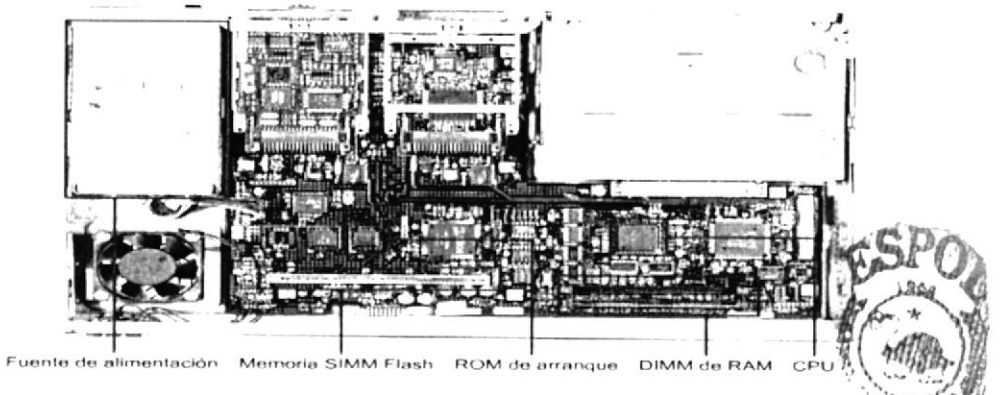


Figura 3-4 Componentes

El router internamente esta compuesto por partes que son:

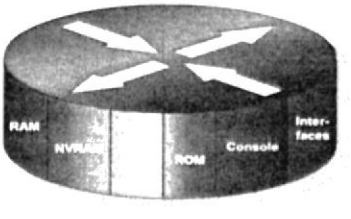


Figura 3-5 Símbolo

- RAM
- NVRAM
- FLASH
- ROM
- CONSOLA
- INTERFAZ

Memoria	Propósito
ROM	Guarda el ROM monitor, y la boot ROM
Memoria Flash	Guarda la Imagen del Sistema (Cisco IOS)
NVRAM	Guarda el archivo de configuración (starup-config)
RAM	Guarda la configuración en operación (running-config), tablas de ruteo, caches, queues, packets, etc.

Figura 3-6 Memoria

3.2.1. RAM

La memoria de acceso aleatorio (RAM) se usa para la información de las tablas de enrutamiento, el caché de conmutación rápida, la configuración actual y las colas de paquetes. En la mayoría de los routers, la RAM proporciona espacio de tiempo de ejecución para el software IOS de Cisco y sus subsistemas. El contenido de la RAM se pierde cuando se apaga la unidad. En general, la RAM es una memoria de acceso aleatorio dinámica (DRAM) y puede actualizarse agregando más Módulos de memoria en línea doble (DIMM).

3.2.2. NVRAM

La memoria de acceso aleatorio no volátil (NVRAM) se utiliza para guardar la configuración de inicio. En algunos dispositivos, la NVRAM se implementa utilizando distintas memorias de solo lectura programables, que se pueden borrar electrónicamente (EEPROM). En otros dispositivos, se implementa en el mismo dispositivo de memoria flash desde donde se cargó el código de arranque. En cualquiera de los casos, estos dispositivos retienen sus contenidos cuando se apaga la unidad.

3.2.3. FLASH

La memoria flash se utiliza para almacenar una imagen completa del software IOS de Cisco. Normalmente el router adquiere el IOS por defecto de la memoria flash. Estas imágenes pueden actualizarse cargando una nueva imagen en la memoria flash. El IOS puede estar comprimido o no. En la mayoría de los routers, una copia ejecutable del IOS se transfiere a la RAM durante el proceso de arranque. En otros routers, el IOS puede ejecutarse directamente desde la memoria flash. Agregando o reemplazando los Módulos de memoria en línea simples flash (SIMMs) o las tarjetas PCMCIA se puede actualizar la cantidad de memoria flash.
ROM

La memoria de solo lectura (ROM) se utiliza para almacenar de forma permanente el código de diagnóstico de inicio (Monitor de ROM). Las tareas principales de la ROM son el diagnóstico del hardware durante el arranque del router y la carga del software IOS de Cisco desde la memoria flash a la RAM. Algunos routers también tienen una versión más básica del IOS que puede usarse como fuente alternativa de arranque. Las memorias ROM no se pueden borrar. Sólo pueden actualizarse reemplazando los chips de ROM en los tomas.

3.2.4. CONSOLA

El puerto de consola proporciona es el acceso físico para la configuración inicial.

3.2.5. INTERFAZ

Las interfaces son las conexiones de los routers con el exterior. Los tres tipos de interfaces son la red de área local (LAN), la red de área amplia (WAN) y la Consola/AUX. Las interfaces LAN generalmente constan de uno de los distintos tipos de Ethernet o Token Ring. Estas interfaces tienen chips controladores que proporcionan la lógica necesaria para conectar el sistema a los medios. Las interfaces LAN pueden ser CONFIGURACIÓNes fijas o modulares.
Las interfaces WAN incluyen la Unidad de servicio de canal (CSU) integrada, la RDSI y la serial. Al igual que las interfaces LAN, las interfaces WAN también cuentan con chips controladores para las interfaces. Las interfaces WAN pueden ser de CONFIGURACIÓNes fijas o modulares.
Los puertos de Consola/AUX son puertos seriales que se utilizan principalmente para la configuración inicial del router. Estos puertos no son puertos de networking. Se usan para realizar sesiones terminales desde los puertos de comunicación del computador o a través de un módem.

3.3. CONEXIONES EXTERNAS DEL ROUTER

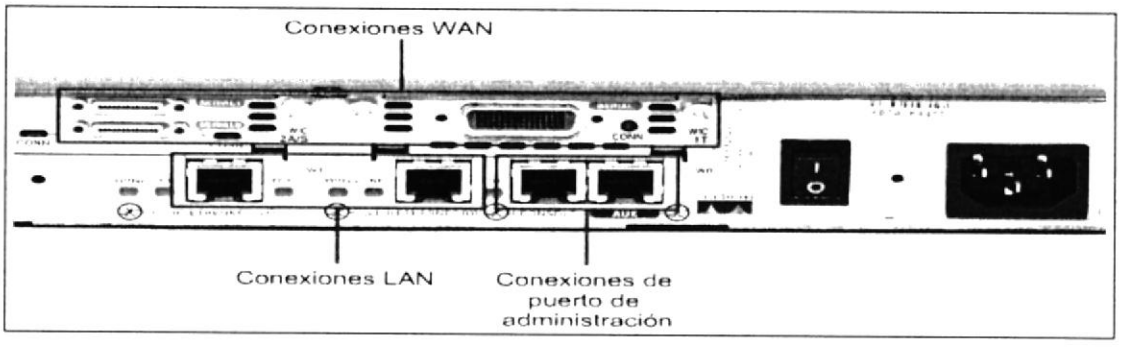


Figura 3-7 Partes Externas

El router externamente esta compuesto por:

- CONEXIÓN WAN
- CONEXIÓN LAN
- CONEXIONES DE PUERTOS ADMINISTRATIVOS

3.3.1. CONEXIÓN LAN

Esta conexión permite conectarse a una red cercana, es decir, a una red **LAN** mediante conexión ethernet.

3.3.2. CONEXIÓN WAN

Esta conexión permite estar comunicado a grandes distancia como proveedor de Internet (ISP); sucursales lejanos, es decir, mediante conexiones seriales

3.3.3. CONEXIONES DE PUERTOS ADMINISTRATIVOS

Esta conexión permite controlar todos los movimientos que se efectúa en un ruteador e incluso en esta conexión se lo utiliza para configurar los dispositivos mediante el conector de la consola.

3.4. VENTAS Y DESVENTAJAS DE UN ROUTERS

VENTAJA	DESVENTAJAS
❖ Segmentación eficiente de tráfico y broadcats. ❖ Manejo de protocolos de nivel 3. ❖ Interconexión de redes heterogéneas ❖ Dependiendo del protocolo de ruteo pueden manejar múltiples caminos para un mismo destino y balancear cargas de enlaces. ❖ Proveen escalabilidad para redes muy grandes.	❖ Complejos de operar. ❖ Utilizan protocolos complejos de implementar para los fabricantes de equipos. ❖ Lentos ❖ Caros

Tabla 3-1 Ventajas-Desventajas

3.5. FUNCIONES DE UN ROUTER

Las funciones primarias de un ruteador son:

- Segmentar la red dentro de dominios individuales de broadcast.
- Suministrar un envió inteligente de paquetes. Y Soportar rutas redundantes en la red.
- Aislar el tráfico de la red ayuda a diagnosticar problemas, puesto que cada puerto del ruteador es una subred separada, el tráfico de los broadcast no pasarán a través del ruteador.

3.6. BENEFICIOS DE UN ROUTER

Otros importantes beneficios del ruteador son:

- Proporcionar seguridad a través de filtros de paquetes, en ambiente LAN y WAN.
- Consolidar el legado de las redes de mainframe IBM, con redes basadas en PCs a través del uso de Data Link Switching (DLSw).
- Permitir diseñar redes jerárquicas, que delegan autoridad y puedan forzar el manejo local de regiones separadas de redes internas.
- Integrar diferentes tecnologías de enlace de datos, tales como Ethernet, FastEthernet, Token Ring, FDDI y ATM.

3.6.1. TECNOLOGÍA DE RUTEADOR

Un ruteador es un dispositivo general diseñado para segmentar la red, con la idea de limitar tráfico de broadcast y proporcionar seguridad, control y redundancia entre dominios individuales de broadcast, también puede dar servicio de firewall y un acceso económico a una WAN.

El ruteador opera en la capa 3 del modelo OSI y tiene más facilidades de software que un switch. Al funcionar en una capa mayor que la del switch, el ruteador distingue entre los diferentes protocolos de red, tales como IP, IPX, AppleTalk o DECnet. Esto le permite hacer una decisión más inteligente que al switch, al momento de reenviar los paquetes. El ruteador realiza dos funciones básicas:

1. El ruteador es responsable de crear y mantener tablas de ruteo para cada capa de protocolo de red, estas tablas son creadas ya sea estáticamente o dinámicamente. De esta área el ruteador extrae de la capa de red la dirección destino y realiza una decisión de envió basado sobre el contenido de la especificación del protocolo en la tabla de ruteo.

2. La inteligencia de un ruteador permite seleccionar la mejor ruta, basándose sobre diversos factores, más que por la dirección MAC destino. Estos factores pueden incluir la cuenta de saltos, velocidad de la línea, costo de transmisión, retrazo y condiciones de tráfico. La desventaja es que el proceso adicional de procesado de frames por un ruteador puede incrementar el tiempo de espera o reducir el desempeño del ruteador cuando se compara con una simple arquitectura de switch.

3.7. HYPERTERMINAL

La conexión **HYPERTERMINAL** se trata de la conexión del router al computador. Mediante sus conexiones:

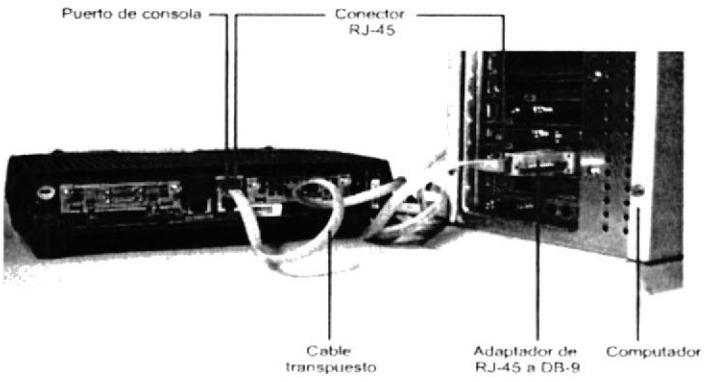


Figura 3-8 Conexión Hiperterminal

Conexión RJ-45 del punto de router desde la consola
Conexión DB-9 del punto de la computadora desde com 1 o com 2 depende del modelo; en este caso utiliza com 1

Figura 3-9 Cable RollOver

3.8. CONFIGURACIÓN DEL HYPERTERMINAL

Paso uno

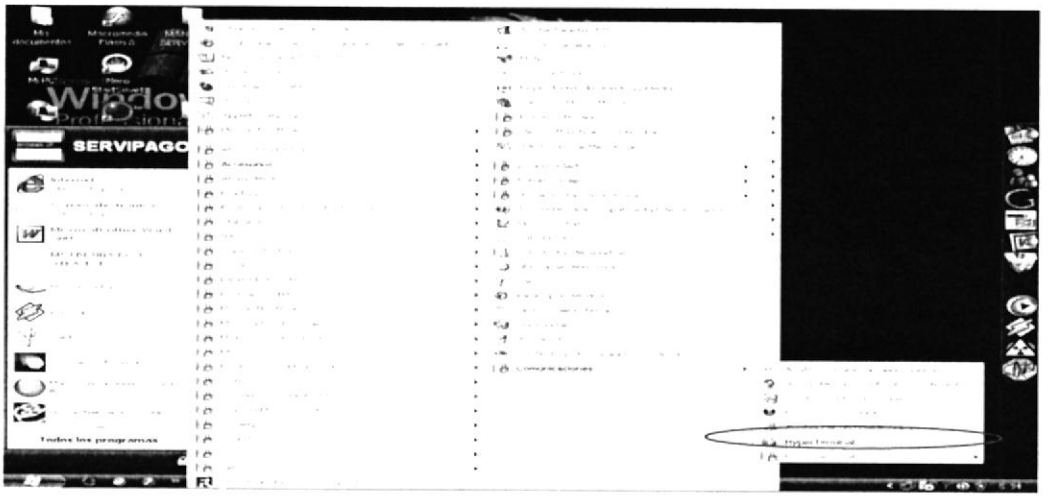


Figura 3-10 Configuración

Abrimos el Hyperterminal de la siguiente manera:

- Hacer clic en inicio
- Escoger la opción accesorios
- Luego hacer click en comunicación
- Por último dar click en Hyperterminal

Paso 2

Al abrir el hyperterminal, se darán las opciones de crear una nueva conexión, le ponemos un nombre que identifique la BBS, por ejemplo 'URBANIS' y se elige el icono que se guste.

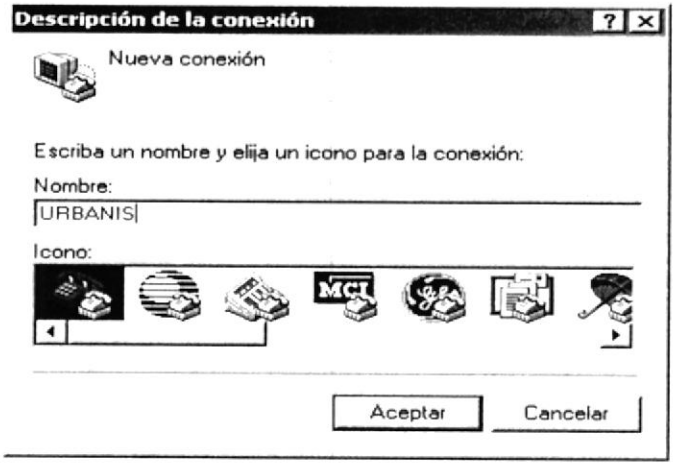


Figura 3-11 Nombre De La Conexión

Paso 3

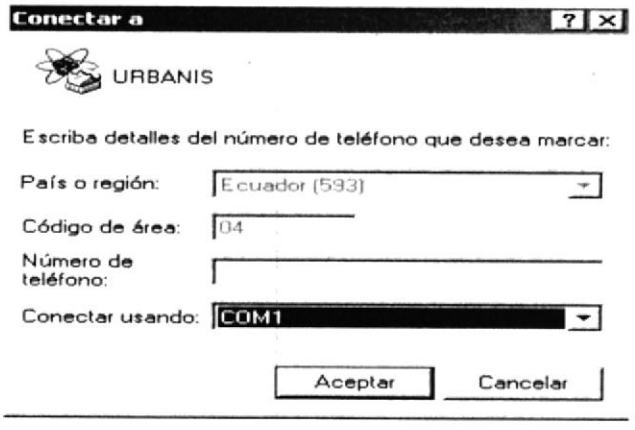


Figura 3-12 Puerto De Conexión

En esta pantalla se elige el puerto para conectar el router con el cable rollover, cabe indicar que puede conectarse mediante el com1, com2, com3 dependiendo el tipo de conexión que tenga la PC.

Paso 4

A continuación se debe configurar los bits.

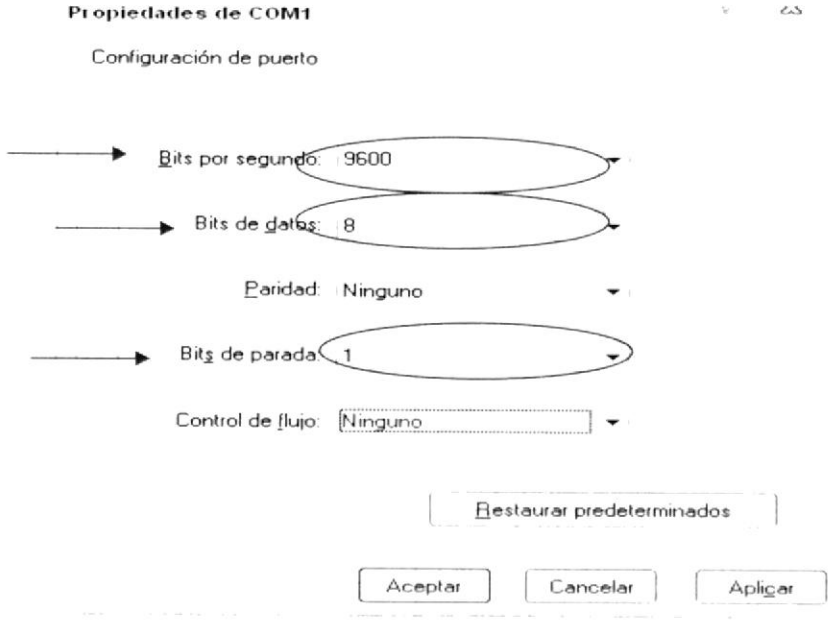


Figura 3-13 Configuración de los Bits

NOTA: Los bits son parámetros por defecto del puerto de consola

3.9. MODOS DE UN ROUTER

Al momento de ingresar a la consola de un router existen 3 tipos modos:

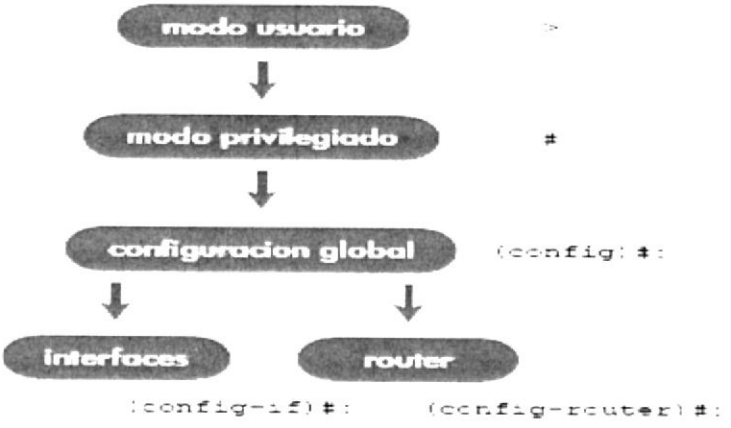


Figura 3-14 Gráfico De Los Modos

MODO	DETALLE
Modo usuario	El que solo puede visualizar pero no modificar nada
Modo privilegiado	El que puede modificar editar configurar un ruteador.
Modo Global	Se trata al ingresar a la configuración principal del router

Tabla 3-6 Modos Del Router

3.10. PROTOCOLOS DE ENRUTAMIENTOS

3.10.1. INTRODUCCIÓN

Un aspecto fundamental en las redes de conmutación de paquetes es el encaminamiento y los algoritmos que para él se emplean. A lo largo de las clases teóricas, se han diferenciado dos técnicas para los mismos (por vector distancia y por estado del enlace) y se han analizado dos de los posibles algoritmos de camino más corto. En este manual, observaremos cómo funcionan dos de los protocolos de enrutamiento que se utilizan en IP (R.I.P. y O.S.P.F.).

- El primero de ellos será un protocolo de vector distancia
- El segundo lo será de **estado del enlace**. Que no permitirá observar cómo se crean las tablas de rutas de los routers de la red, ni cuál es la información intercambiada entre los mismos, pero sí se podrá comprobar como es posible encaminar los paquetes en función de distintos criterios.

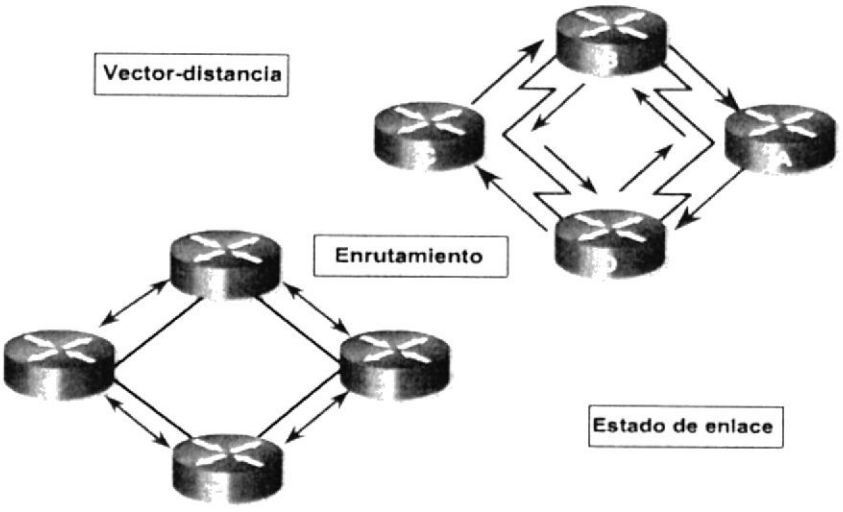


Figura 3-14 Gráfico De Los Modos

3.10.2. ENRUTAMIENTO DINÁMICO VS. ESTÁTICO

Básicamente existen dos maneras de enrrutar a otros hosts fuera del nodo local y son utilizando enrutamiento estático o enrutamiento dinámico.
Cada método tiene ventajas e inconvenientes, pero cuando una red crece finalmente el enrutamiento dinámico es la única manera factible de gestionar la red.

Por este motivo se plantea la necesidad de utilizar protocolos de enrutamiento dinámico en vez de usar rutas estáticas en *todos* los nodos.
Existen programas para llevar el enrutamiento dinámico en la mayoría de los sistemas operativos, por lo que no debe ser complicado instalarlos en un nodo. Para sistemas UNIX existe un programa, zebra, que puede gestionar los protocolos de enrutamiento estáticos mencionados en este documento. Además zebra es software gratuito con licencia GPL.
Hay que destacar que el uso de estos protocolos será transparente al usuario final y será exclusivamente un tema para los gestores de nodos en caso que el nodo conecte a otros.

Desde el punto de vista del cliente el enrutamiento será resuelto mediante la configuración DHCP automática cuando el cliente conecta al nodo.
Como no es obligatorio que un nodo conecta a otros, el uso de estos protocolos y el enrutamiento dinámico no es obligatorio. En algunos casos una ruta estática puede ser suficiente para realizar la conexión.

3.11. PROTOCOLOS RIP

3.11.1. INTRODUCCIÓN HISTÓRICA

Uno de los protocolos de routing más antiguos es el Routing Informacition Protocol o más comúnmente llamado RIP. Utiliza algoritmos de vector distancia para calcular sus rutas.
Este tipo de algoritmos para calcular rutas fueron utilizados durante décadas en sus distintas variantes. De hecho los algoritmos de vector distancia utilizados por RIP están basados en aquellos algoritmos utilizados por ARPANET en el año 1969.

Los protocolos vector distancia fueron descritos académicamente por: R.E. Bellman, L.R. Ford Jr y D.R. Fulkerson.

La primera organización que implementó un protocolo de vector distancia fue la compañía Xerox en su protocolo GIP (Gateway Information Protocol), este protocolo estaba incluido dentro de la arquitectura XNS (Xerox Network Systems). GIP se utilizaba para intercambiar información de routing entre redes o sistemas autónomos no adyacentes. Pero claro, Xerox había implementado su propio protocolo propietario.

Poco después la Universidad de California en Berkeley creo una variante llamada "routed", esta variante del GIP introdujo novedades como modificación del campo de direccionamiento, que se consiguió más flexible, también se añadió un temporizador que limitaba a 30 segundos el tiempo máximo de actualización, es decir, el tiempo máximo permitido sin saber la información de los vecinos, y por supuesto se integró dentro de UNIX, con lo cual pasó a ser abierto.

3.11.2. INTRODUCCIÓN TÉCNICA

RIP es un protocolo de routing de vector distancia muy extendido en todo el Mundo por su simplicidad en comparación a otros protocolos como podrían ser OSPF, IS-IS o BGP. RIP se trata de un protocolo abierto a diferencia de otros protocolos de routing como por ejemplo IGRP y EIGRP propietarios de Cisco Systems o VNN propietario de Lucent Technologies. RIP está basado en el algoritmo de Bellman Ford y busca su camino óptimo mediante el conteo de saltos, considerando que cada router atravesado para llegar a su destino es un salto. RIP, al contar únicamente saltos, como cualquier protocolo de vector distancia no tiene en cuenta datos tales como por ejemplo ancho de banda o congestión del enlace.

3.12. VERSIONES RIP

También existe un RIP para IPX; casualmente lleva el mismo acrónimo, pero no

RIPv1	✓ No soporta subredes ni CIDR. ✓ Tampoco incluye ningún mecanismo de autentificación de los mensajes. ✓ No se usa actualmente. ✓ Su especificación está recogida en el RFC 1058.

RIPv2	✓ Soporta subredes, CIDR y VLSM. ✓ Soporta autenticación utilizando uno de los siguientes mecanismos: o no autentificación o autentificación mediante contraseña o autentificación mediante contraseña codificada mediante MD5 (desarrollado por Ronald Rivest). ✓ Su especificación está recogida en el RFC 1723-2453.
RIPng	✓ RIP para IPv6. Su especificación está recogida en el RFC 2080

Tabla 3-3 Protocolo Rip

3.12.1. CARACTERÍSTICAS RIP

- ✓ RIP utiliza UDP para enviar sus mensajes y el puerto bien conocido 520.
- ✓ RIP calcula el camino más corto hacia la red de destino usando el algoritmo del vector de distancias. La distancia o métrica está determinada por el número de saltos de router hasta alcanzar la red de destino.
- ✓ RIP tiene una distancia administrativa de 120 (la distancia administrativa indica el grado de confiabilidad de un protocolo de enrutamiento, por ejemplo EIGRP tiene una distancia administrativa de 90, lo cual indica que a menor valor mejor es el protocolo utilizado)
- ✓ RIP no es capaz de detectar rutas circulares, por lo que necesita limitar el tamaño de la red a 15 saltos. Cuando la métrica de un destino alcanza el valor de 16, se considera como infinito y el destino es eliminado de la tabla (inalcanzable).

3.12.2. MÁSCARA DE RED DE RIP

La característica de máscara de red de *rip* está soportada para ambas versiones, la 1 y la 2.

3.12.3. VERSIÓN 1 DE RIP

Originalmente no contenía información de la máscara. En la versión 1 de RIP, las clases eran utilizadas originalmente para determinar el tamaño de la máscara. Las redes de Clase A utilizaban 8 bits para la máscara, las redes de Clase B utilizaban 16 bits para la máscara, mientras que las redes de Clase C utilizaban 24 bits para la máscara.

Actualmente, el método más utilizado para el tamaño de la máscara de un paquete consiste en asignar al paquete la máscara en base al interfaz que recibió el paquete.

3.12.4. VERSIÓN 2 DE RIP

Soporta la máscara de subred de tamaño variable (variable length subnet mask VLSM). Extendiendo la submáscara de red, la máscara puede ser dividida y puede rehusarse. Cada subred puede usarse para propósitos diferentes como grandes o medianas LANs y enlaces WAN. El demonio *ripd* de Quagga no soporta las máscaras no secuenciales, las cuales están incluidas en la especificación de RIP versión 2.
En caso de existir información similar con el mismo prefijo y métrica, la información antigua será eliminada. Rip actualmente no soporta rutas multipath con el mismo coste.

3.13. VENTAJAS Y DESVENTAJAS DE RIP

3.13.1. VENTAJAS

En comparación con otros protocolos de enrutamiento, RIP es más fácil de configurar. Además, es un protocolo abierto, soportado por muchos fabricantes.
Desventajas
Por otra parte, tiene la desventaja que, para determinar la mejor métrica, únicamente toma en cuenta el número de saltos (por cuántos routers o equipos similares pasa la información); no toma en cuenta otros criterios importantes, especialmente el ancho de banda. Esto puede causar ineficiencias, ya que puede preferir una ruta de bajo ancho de banda.

3.13.2. FUNCIONAMIENTO RIP

- ✓ RIP utiliza UDP para enviar sus mensajes y el puerto bien conocido 520.
- ✓ RIP calcula el camino más corto hacia la red de destino usando el algoritmo del vector de distancias. La distancia o métrica está determinada por el número de saltos de router hasta alcanzar la red de destino.
- ✓ RIP tiene una distancia administrativa de 120 (la distancia administrativa indica el grado de confiabilidad de un protocolo de enrutamiento, por ejemplo EIGRP tiene una distancia administrativa de 90, lo cual indica que a menor valor mejor es el protocolo utilizado)
- ✓ RIP no es capaz de detectar rutas circulares, por lo que necesita limitar el tamaño de la red a 15 saltos. Cuando la métrica de un destino alcanza el valor de 16, se considera como infinito y el destino es eliminado de la tabla (inalcanzable).
- ✓ La métrica de un destino se calcula como la métrica comunicada por un vecino más la distancia en alcanzar a ese vecino. Teniendo en cuenta el límite de 15 saltos mencionado anteriormente. Las métricas se actualizan sólo en el caso de que la métrica anunciada más el coste en alcanzar sea estrictamente menor a la almacenada. Sólo se actualizará a una métrica mayor si proviene del enrutador que anunció esa ruta.

3.13.3. INTRODUCCIÓN HISTÓRICA

En 1988, el grupo: Fuerza de Trabajo de Ingenieros de Internet (IETF) empezó a desarrollar un nuevo protocolo de enrutamiento que reemplazaría al protocolo RIP. Se desarrolló entonces el protocolo de pasarela interior Primero el camino abierto más corto (OSPF - Open Shortest Path Firsht). OSPF es un protocolo de encaminamiento para redes IP que se basa en las especificaciones de RFC descritas al final del documento. En la década de los 90 OSPF fue recomendado como un protocolo de encaminamiento estándar.

El protocolo OSPF propone el uso de rutas más cortas y accesibles mediante la construcción de un mapa de la red y mantenimiento de bases de datos con información sobre sistemas locales y vecinos, de esta manera es capaz de calcular la métrica para cada ruta, entonces se eligen las rutas de encaminamiento más cortas. En este proceso se calculan tanto las métricas de estado del enlace como de distancia, en el caso de RIP se calcula sólo la distancia y no el tráfico del enlace, por esta causa OSPF es un protocolo de encaminamiento diseñado para redes con crecimiento constante y capaz de manejar una tabla de encaminamiento distribuida y de rápida propagación, entre las características más resaltantes de OSPF están:

- ✓ Rápida detección de cambios en la topología y restablecimiento muy rápido de rutas sin bucles.
- ✓ Poca sobrecarga, usa actualizaciones que informan de los cambios de rutas.
- ✓ División de tráfico por varias rutas equivalentes.
- ✓ Encaminamiento según el tipo de servicio.
- ✓ Uso de multienvio en las redes de área local.
- ✓ Máscaras de subred y superred.
- ✓ Autentificación.

3.13.4. INTRODUCCIÓN TÉCNICA

OSPF (Open shortest path first, El camino más corto primero)

Es un protocolo de routing link-state no propietario, esto quiere decir principalmente dos cosas: Primero que es de libre uso y suele estar soportados por la mayoría de los equipos destinados a ofrecer servicios a la red y Segundo el ser un link-state quiere decir que a diferencia de RIP o IGRP que son Distance-vector, no mandan continuamente la tabla de rutas a sus vecinos sino que solo lo hacen cuando hay cambios en la topología de red, de esta forma se evita el consume de ancho de banda innecesario. En un cambio de topología OSPF envía el cambio inmediatamente de forma que la convergencia de la red es mas rápida que en los distance-vector donde depende de timers asignados, de forma que en un link-state el tiempo de convergencia puede ser de 4 o 5 segundos según la red en RIP puede se de 180 segundos.

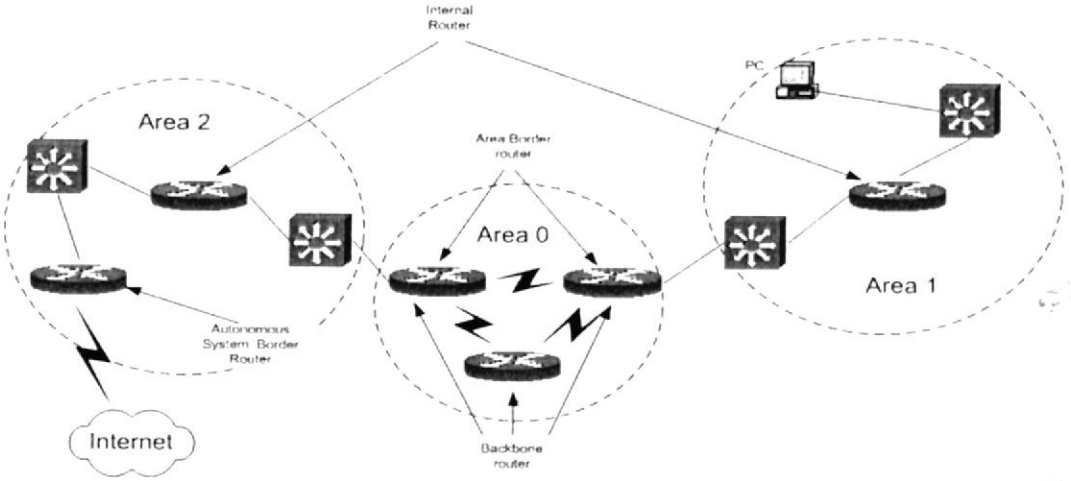


Figura 3-16 Protocolo OSPF

Los router que forman parte de la red con OSPF se les denomina según su situación y su función dentro de la red de la siguiente forma:

Internal router: Un router con todas las redes directamente conectadas a la misma área. Estos solo mantienen una copia del algoritmo de routing.

Área Border Router: ABRs es un router que une un área al área 0 comparte la información entre las dos áreas y gestiona que redes se tiene que compartir entre ellas.

Backbone Routers: Son los routers que pertenecen al área 0 y responsable de la propagación de las redes entre distintas áreas. Autonomous System Boundary Routers: Son routers conectados a otros AS o Internet. También suele ser el router que intercambia entre protocolos de routing IGP y EGP.

3.13.5. CARACTERÍSTICAS OSPF

- OSPF es un protocolo de encaminamiento interior, pero está diseñado para operar con un protocolo exterior adecuado, tal como BGP (Border Gateway Protocol).
- OSPF es complejo en comparación con RIP.
- Mucha de su complejidad tiene un sólo propósito: asegurar que las bases de datos topológicas son las mismas para todos los routers dentro de un área.
- Si los routers tuvieran bases de datos independientes, podrían tomar decisiones mutuamente conflictivas.
- OSPF se comunica por medio de IP (su número de protocolo es el 89).
- Es un protocolo de estado de enlace, primero el camino más corto.
- La especificación de OSPF hace uso de máquinas de estado para definir el comportamiento de los routers que siguen en el protocolo.
- Hay una máquina por componente y el estado de uno es independiente del resto.
- OSPF soporta rutas específicas de hosts, redes y subredes.

- El protocolo OSPF reconoce tres tipos de conexiones y redes:

3.13.6. CONEXIONES QUE SOPORTA OSPF

- Conexiones punto a punto entre dos ruteadores
- Redes multiacceso por difusión (la mayoría de las Lan)
- Redes multiacceso sin difusión (la mayoría en redes Wan)

Las redes multiacceso son todas aquellas que interconectan múltiples equipos donde cada uno es capaz de comunicarse con todos los otros equipos; la mayoría de las redes LAN y WAN tienen esta prioridad

3.13.7. VENTAJAS Y DESVENTAJAS DE OSPF

3.13.7.1. VENTAJAS

- Las rutas calculadas mediante OSPF nunca presentan bucles.
- OSPF puede escalar a interconexiones de redes mayores o mucho mayores.
- La reconfiguración correspondiente a los cambios de topología de la red es más rápida.
- Utilizan métricas de costos para seleccionar rutas a trabes de la red
- Utiliza actualizaciones generales por eventos e inundaciones LSA: (intercambia cambios en la red)
- Cada router tiene una topología de su propia red
- Cada router tiene una base de datos topológicos

3.13.7.2. DESVENTAJAS

- Este protocolo necesita un router que tenga más memoria y potencia de procesamiento
- Para reducir las bases de las políticas es necesario dividir la red en áreas (se necesita un Administrador capacitado)
- Al inicio del proceso se debe inundar la red con mensajes LSA, puede degradar la red

3.13.8. FUNCIONAMIENTO DE OSPF

1. Descubrir vecinos OSPF
2. Elegir el DR
3. Formar adyacencias
4. Sincronizar bases de datos

5. Calcular la tabla de encaminamiento
6. Anunciar los estados de enlaces

A continuación se describen cada uno de los seis pasos de funcionamiento del OSPF.

3.13.8.1. DESCUBRIMIENTO VECINO OSPF

Cuando los "routers" OSPF se activan, inician y mantienen relaciones con sus vecinos usando el protocolo Hello.
El protocolo además asegura que la comunicación entre vecinos sea bidireccional.
Los paquetes Hello se envían periódicamente al exterior por todas las interfaces de los "routers".
La comunicación bidireccional se indica si el propio "router" aparece en el paquete Hello
Del vecino.

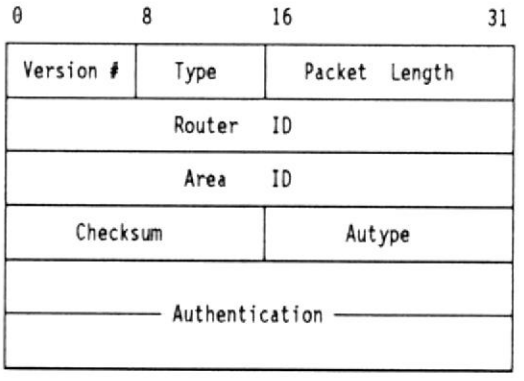


Figura 3-17. Cabecera OSPF

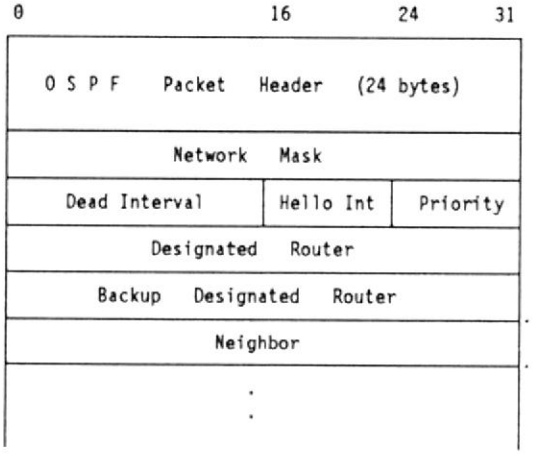


Figura 3-18. Cabecera OSPF

3.13.9. DETERMINANDO EL DR

Se usa el protocolo Hello. El "router" examina la lista de sus vecinos, desecha cualquiera que no tenga comunicación bidireccional o que tenga un RP de ver, y graba el DR, el BDR y la RP que ha declarado cada uno de ellos. El "router" se añade él mismo a la lista, usando el valor RP configurado para la interfaz cero (desconocido) para el DR y el BDR, en el caso de que este proceso esté en proceso de activaciones determina el BDR y el DR.

La intención del mecanismo es la siguiente:

- Que cuando un "router" se active, no debería usurpar la posición del BDR actual aunque tenga un RP superior.
- Que la promoción de un BDR a DR debería ser ordenada y requerir que el BDR acepte sus responsabilidades.
- El algoritmo no siempre da lugar a que el "router" de mayor prioridad sea el DR, ni tampoco que el segundo de mayor prioridad sea el DR.

3.13.10. RESPONSABILIDADES DEL DR:

El DR genera para la red los anuncios de los estados de los enlaces, que inundan el área y describen esta red a todos los "routers" de todas las redes del área.

El DR se hace adyacente a otros "routers" de la red.

El BDR se hace adyacente a todos los demás "routers" de la red. Esto asegura que cuando ocupe el puesto del DR lo pueda hacer rápidamente.

3.13.11. FORMANDO ADYACENCIAS

La siguiente decisión es si se debería formar una adyacencia con uno de sus vecinos: En redes multiacceso, todos los "routers" se hacen adyacentes al DR y la BDR.

En enlaces punto a punto (virtuales), cada "router" forma siempre una adyacencia con el "router" del otro extremo.
Si se toma la decisión de no formar una adyacencia, el estado de la comunicación con el vecino permanece en el estado "2-way".

Las adyacencias son estables usando paquetes DD ("Database Description").
Se emplea un procedimiento de sondeo-respuesta para describir la base de datos.

El "router" con mayor ID se convertirá en maestro, el otro en esclavo. Los paquetes DD enviados por el maestro (sondeos) serán reconocidos por los DDs del esclavo (respuestas). El paquete contiene números de secuencia para asegurar la correspondencia entre sondeos y respuestas. Este proceso se denomina DEP ("Database Exchange Process").

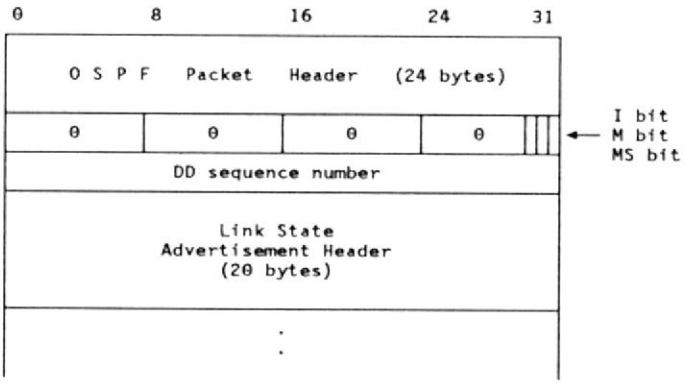
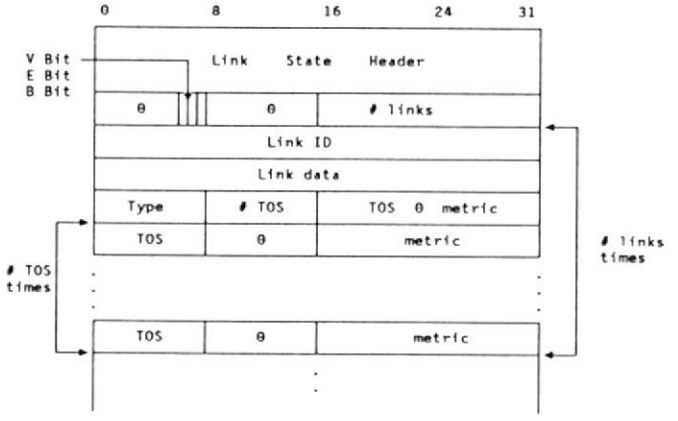


Figura 3-19. Paquete DD De OSPF

3.13.12. SINCRONIZACIÓN DE LAS BASES DE DATOS

Después de terminar el DEP ("Database Exchange Process"), cada "router" tiene una lista de aquellos anuncios para los que el vecino tiene más instancias actualizadas, que se solicitan por medio de paquetes LSR ("Link State Request"). La respuesta a un LSR es un LSU ("Link State Update") que contiene algunos o todos los anuncios solicitados. Si no se repite respuesta, se repite la solicitud.

NOTA: Los anuncios vienen en los siguientes cinco formatos



.Figura 3-20 (tipo 1) RLA ("Router Links Advertisement") de OSPF

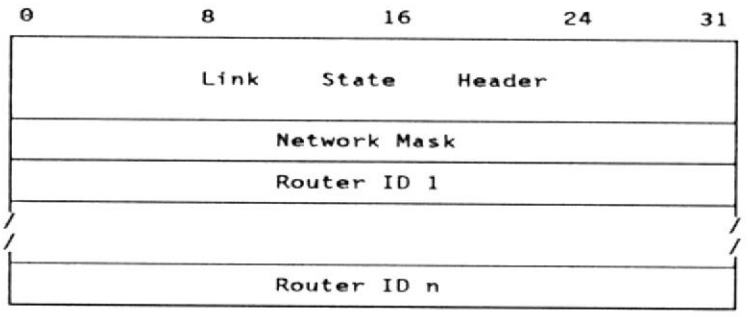


Figura 21. (Tipo 2) NLA ("Network Links Advertisement") de OSPF

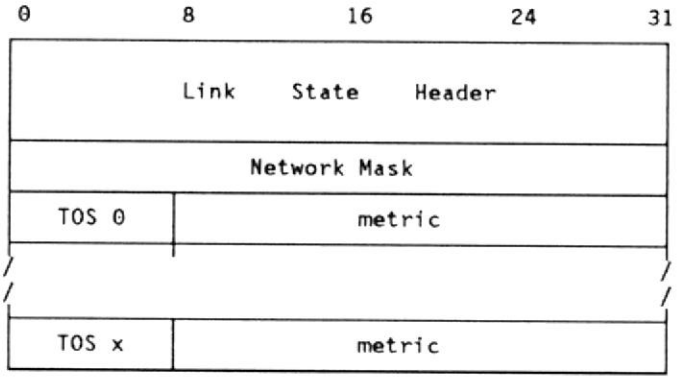


Figura 22. (Tipo 3 y 4) SLA ("Summary Links Advertisement") de OSPF

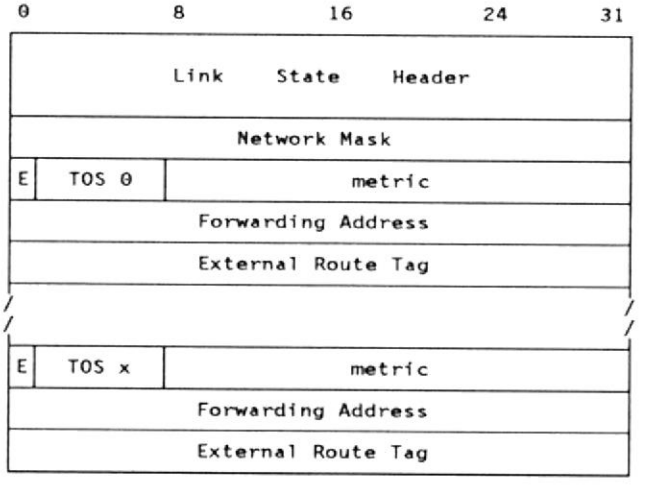


Figure 23. (Tipo 5) ELA ("External Links Advertisement") de OSPF

Cuando se han respondido los paquetes LSR, las bases de datos se sincronizan y los routers" se describen como totalmente adyacentes. La adyacencia se añade a los anuncio de los dos "routers" correspondientes.

3.14. CALCULANDO LA TABLA DE ENCAMINAMIENTO

Usando como entrada las bases de datos de estados de enlaces de las áreas con las que está conectado, el "router" ejecuta el algoritmo SPF para construir su tabla de encaminamiento. El cálculo consiste en los siguientes pasos:

- Las rutas intra-área se calculan construyendo el árbol mínimo para cada área conectada usando el mismo "router" como raíz del árbol. El "router" calcula además si el área puede actuar como área de tránsito para enlaces virtuales.
- Las rutas inter-área se calculan examinando los SLA. Para los ABR (que forman parte de la troncal) sólo se utilizan los anuncios correspondientes a la troncal.
- Si el "router" está conectado a una o más áreas de tránsito, el "router" sustituye las rutas que haya calculado por rutas que pasen por áreas de tránsito si estas son mejores.
- Las rutas externas se calculan examinado los anuncios externos del AS. Las localizaciones de los ASBR ya se conocen debido a que se determinan como cualquier otra ruta intra-área o inter-área.

3.14.1. ANUNCIANDO LOS ESTADOS DE LOS ENLACES

Un "router" anuncia periódicamente el estado de su enlace, por lo que la ausencia de un anuncio reciente indica a los vecinos del "router" que no está activo.

Todos los "routers" que hayan establecido comunicación bidireccional con un vecino ejecutan un contador de inactividad para detectar ese suceso.

La comunicación se debe establecer desde cero, incluyendo la resincronización de las bases de datos.
Un "router" también relanza sus anuncios cuando su estado cambia.

Un router puede lanzar diversos anuncios para cada área. Estos se propagan a través del área por el procedimiento de inundación. Cada "router" emite un RLA. Si el "router" es además el DR para una o más de las redes del área, originará NLAs para estas.

Los ABR generan una SLA para cada destino inter-área conocido. Los ASBR originan un ASL para cada destino externo conocido. Los destinos se anuncian uno cada vez de tal forma que el cambio de una sola ruta puede inundar la red sin tener que enviar el resto de las rutas. Durante el proceso de inundación, un solo LSU puede llevar muchos anuncios.

3.14.2. CONCLUSIONES DEL PROTOCOLÓ OSPF

OSPF es un protocolo de encaminamiento complejo. Los beneficios de esta complejidad (sobre RIP) son los siguientes:

- ✓ Debido a las bases de datos de estados de enlaces sincronizados, los "router" OSPF convergerán mucho más rápido que los "routers" RIP tras cambios de topología. Este efecto se hace más pronunciado al aumentar el tamaño del AS.
- ✓ Incluye encaminamiento TOS ("Type of Service") diseñado para calcular rutas separadas para cada tipo de servicio. Para cada destino, pueden existir múltiples rutas, cada una para uno o más TOSs
- ✓ Utiliza métricas ponderadas para distintas velocidades el enlace. Por ejemplo, un enlace T1 a 544 Mbps podría tener una métrica de 1 y un SLP a 9600 bps una de 10.
- ✓ Proporciona balanceamiento de la carga ya que una pasarela OSPF puede emplear varios caminos de igual coste mínimo. A cada ruta se le asocia una máscara de subred, permitiendo subnetting de longitud variable y supernetting. Todos los intercambios entre "routers" se pueden autentificar mediante el uso de passwords.
- ✓ OSPF soporta rutas específicas de hosts, redes y subredes.
- ✓ OSPF permite que las redes y los hosts contiguos se agrupen juntos en áreas dentro de un AS, simplificando la topología y reduciendo la cantidad de información de encaminamiento que se debe intercambiar. La topología de un área es desconocida para el resto de las áreas.
- ✓ Minimiza los broadcast permitiendo una topología de grafo más compleja en la que las redes multiacceso tienen un DR que es responsable de describir esa red a las demás redes del área. Permitiendo el intercambio de información de encaminamiento externa, es decir, información de encaminamiento obtenida de otro AS.
- ✓ Permite configurar el encaminamiento dentro del AS según una topología virtual más que sólo las conexiones físicas. Las áreas se pueden unir usando enlaces virtuales que crucen otras áreas sin requerir encaminamiento complicado.
- ✓ Permite el uso de enlaces punto a punto sin direcciones IP, lo que puede ahorrar recursos escasos en el espacio de direcciones IP.

3.15. SWITCHES

3.15.1. INTRODUCCIÓN

Un switch denominado en el idioma castellano se la llama tambien "conmutador"; es un dispositivo electrónico de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (Open Systems Interconection).

Un conmutador o swicht se 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.

Figura 3-24.Switch

3.15.2. TECNOLOGÍA DE SWITCH

Un switch es un dispositivo de proposito especial diseñado para resolver problemas de rendimiento en la red, debido a anchos de banda pequeños y embotellamientos. El switch puede agregar mayor ancho de banda, acelerar la salida de paquetes, reducir tiempo de espera y bajar el costo por puerto. Opera en la capa 2 del modelo OSI y reenvia los paquetes en base a la dirección MAC.

El switch segmenta económicamente la red dentro de pequeños dominios de colisiones,obteniendo un alto porcentaje de ancho de banda para cada estación final. No estan diseñados con el proposito principal de un control íntimo sobre la red o como la fuente última de seguridad, redundancia o manejo.

Al segmentar la red en pequeños dominios de colisión, reduce o casi elimina que cada estación compita por el medio, dando a cada una de ellas un ancho de banda comparativamente mayor.

3.15.3. QUE ES UNA SEGMENTACIÓN

La segmentación se trata de dividir un segmento de red en varias direcciones osea direcciones ip con la finalidad que estas ip sean utilizadas en varias máquinas que se encuentra conectadas en la red, esta dirección ip no se puede repetirse en la red ya que produce problemas de dirección de ip en la red.

NOTA: Las direcciones ip son direcciones que se la denomina direcciones lógicas

3.15.4. TIPOS DE SWICHT

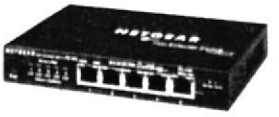
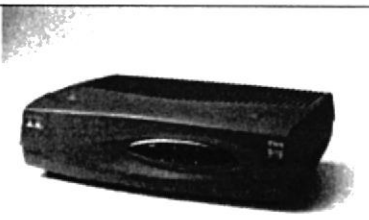
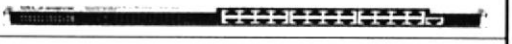
SWICHT	IMAGEN
✓ Switchs Netgear de 4 puertos	
✓ Linksys de 8 puertos	
✓ Cisco de 8 puertos	
✓ Linksys de 8 puertos	
✓ Linksys de 24 puertos.	
✓ Cisco de 48 puertos.	

Figura 3-25 Tipos De Switch

3.15.5. TIPOS DE CAPAS DE SWITCH

El SWITCH tiene a tomar distintas conexiones a medida que se plantean nuevos esquemas para mejorar el rendimiento de las redes de área local. Además los Switch pueden ser administrables y esclavos por lo tanto cada switch pueden ser diferentes tipos de capas conocidas que son:

- Switch capa 2.
- Switch capa 3.
- Switch capa 4.

3.15.5.1. SWITCH CAPA 2

Este es el tipo de switch de red de área local (LAN) más básico, el cual opera en la capa 2 del modelo OSI. Su antecesor es el bridge, por ello, muchas veces al switch se le

refiere como un bridge multipuerto, pero con un costo más bajo, con mayor rendimiento y mayor densidad por puerto.

El switch capa 2 hace sus decisiones de envío de datos en base a la dirección MAC destino contenida en cada frame. Estos, al igual que los bridges, segmentan la red en dominios de colisión, proporcionando un mayor ancho de banda por cada estación.

La configuración de los switches capa 2 y el soporte de múltiples protocolos es totalmente transparente a las estaciones terminales. Como igual es el soporte de las redes virtuales (VLAN´s), las cuales son una forma de segmentación que permite crear dominios de broadcasts formando así grupos de trabajo independientes de la ubicación física.

El uso de procesadores especializados (**ASIC: Application Specific Integrated Circuit**) incrementaron la velocidad de conmutación de los switches, en comparación con los bridges, porque pueden enviar los datos a todos los puertos de forma casi simultánea.
Estos switches siguen, principalmente, dos esquemas para envío de tráfico, los cuales son:

- **Cut-trough:** comienzan el proceso de envío antes de que el frame sea completamente recibido. En estos switches la latencia es baja porque sólo basta con leer la dirección MAC destino para comenzar a transferir el frame. La desventaja de este esquema, es que los frames corruptos (corruptos, enanos, con errores, etc.) son también enviados.
- **Store-and-forward:** lee y valida el paquete completo antes de iniciar el proceso de envío. Esto permite que el switch descarte paquetes corruptos y se puedan definir filtros de tráfico. La desventaja de este esquema es que la latencia se incrementa con el tamaño del paquete.

Algunos switches implementan otros esquemas (Fragment free) o esquemas híbridos en base a rendimiento y porcentaje de errores, pasando en un momento de modo Cut-trough al modo Store-and-forward y, viceversa.

3.15.5.2. SWITCH CAPA 3

Este tipo de switches integran routing y switching para producir altas velocidades (medidas en millones de paquetes por segundo). Esta es una tecnología nueva (Lippis, 1997) a los cuales los vendedores se refieren muchas veces como: Netflow, tag switching (Packet, 1998), Fast IP (3Com, 1997).

Este nuevo tipo de dispositivos es el resultado de un proceso de evolución natural de las redes de área local, ya que, combinan las funciones de los switches capa 2 con las capacidades de los routers (3Com, 1997).

Existen dos tipos de switches de capa 3:

- **Packet-by-packet (PPL3).**
- **Cut-trough (CTL3).**

En ambos tipos de switches, se examinan todos los paquetes y se envían a sus destinos.

La diferencia real entre ellos es el rendimiento. PPL3 enrruta todos los paquetes, en tanto que los switches CTL3 efectúan la entrega de paquetes de una forma un poco distinta, estos switches investigan el destino del primer paquete en una serie. Una vez que lo conoce, se establece una conexión y el flujo es conmutado en capa 2 (con el consiguiente, rendimiento del switching de capa 2) (Lippis, Jun1997).
Funciones:

- Procesamiento de rutas: esto incluye construcción y mantenimiento de la tabla de enrutamiento usando RIP y OSPF.
- Envío de paquetes: una vez que el camino es determinado, los paquetes son enviados a su dirección destino. El TTL (Time-To-Live) es decrementado, las direcciones MAC son resueltas y el checksum IP es calculado.
- Servicios especiales: traslación de paquetes, prioritización, autenticación, filtros

3.15.5.3. SWITCH CAPA 4

La información en los encabezados de los paquetes comúnmente incluyen direccionamiento de capa 2 y 3, tal como: tipo de protocolo de capa 3, TTL y checksum. Hay también información relevante a las capas superiores, como lo es el tipo de protocolo de capa 4 (UDP, TCP, entre otros.) y el número de puerto (valor numérico que identifica la sesión abierta en el host a la cual pertenece el paquete).
En el caso de los switches capa 3, éstos son switches capa 2 que utilizan la información del encabezado de capa 3. Lo mismo ocurre con los switches capa 4, son switches capa 3 que procesan el encabezado de la capa. También son conocidos como switches sin capa (Layerless switches).
La información del encabezado de capa 4 permite clasificar de acuerdo a secuencias de paquetes manejados por aplicación (denominados "flujos"). Ahora bien, dependiendo del diseño del switch, éste puede dar servicios o garantizar ancho de banda por "flujos". Algunos de los diseños de capa 4 son (Torrent, 1998)

3.15.6. CONSIDERACIONES ACERCA DE SWITCH

Los diseñadores y administradores de redes necesitan saber como y cuando usar las tecnologías de las que hemos hablado hasta ahora:

- ✓ Colocar los switches capa 3 en puntos de concentración de la red o como backbone colapsado para eliminar "cuellos de botella".
- ✓ Evitar enrrutar en los switches capa 2 ubicados en los extremos o fronteras de la red.
- ✓ Escoger switches capa 3 que tengan buffers con capacidad desde 50 hasta 100 paquetes por puerto y enviar millones de paquetes por segundo en la capa 3.
- ✓ Evitar retardos excesivos, limitando los dominios de colisión entre 10 y 20 usuarios.

Cuando se escogen switches capa 2 con soporte de VLAN se debe tomar en cuenta que la comunicación inter-vlan se hace usando un router y que, éste puede convertirse en un "cuello de botella" si la red es muy grande.

3.16. VLANS

3.16.1. INTRODUCCIÓN

La definición de VLANs se lleva a cabo en un único switch (servidor), La información sobre las VLANs se transmite mediante el backbone hacia los demás switches (clientes) usando el protocolo VTP (VLAN Trunk Protocol), si un switch se puede configurar para ignorar los mensajes VTP (modo transparente) , La configuración del switch sólo puede hacerse dentro de la VLAN de gestión (Management VLAN), por defecto, VLAN 1.

A su vez las vlan también se la utiliza para reducir los brodcast en la red y dividir la red por cada departamento.

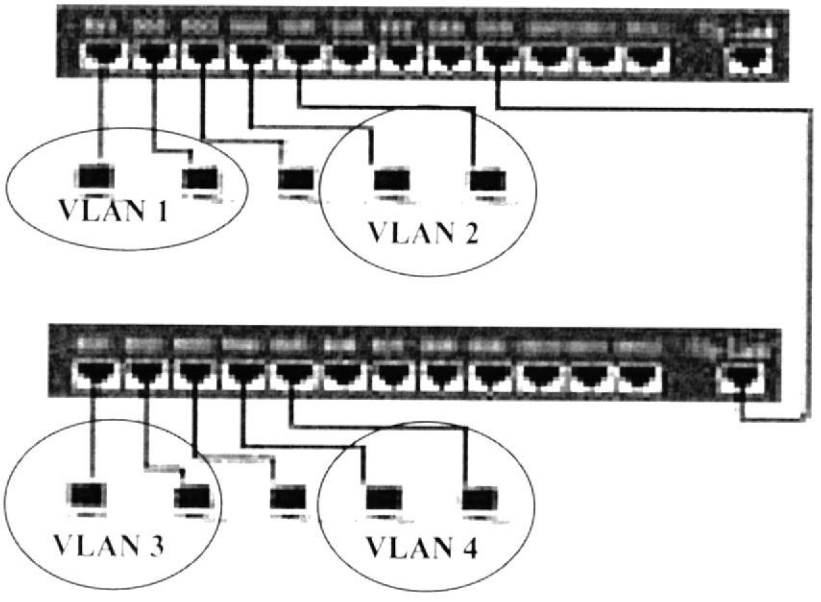


Figura 3-26 Comunicación Entre Vlans

3.16.2. SEGMENTACIÓN TRADICIONAL

Cada usuario se conecta al hub/switch más próximo físicamente

- ✓ La pertenencia de un usuario a una red u otra está limitada por el cableado físico
- ✓ Si un segmento emplea hubs para la interconexión, todos los usuarios pertenecen al mismo dominio de colisión (no así si se usan switches)
- ✓ Los dominios de broadcast están delimitados por el router

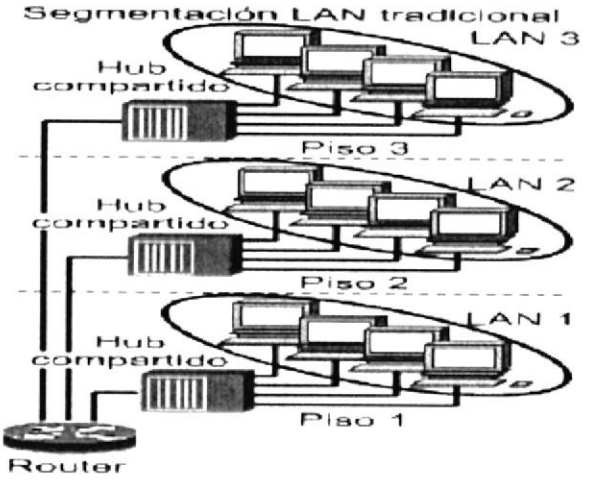


Figura 3-27. Segmentación Tradicional

3.16.3. SEGMENTACIÓN CON VLANS.

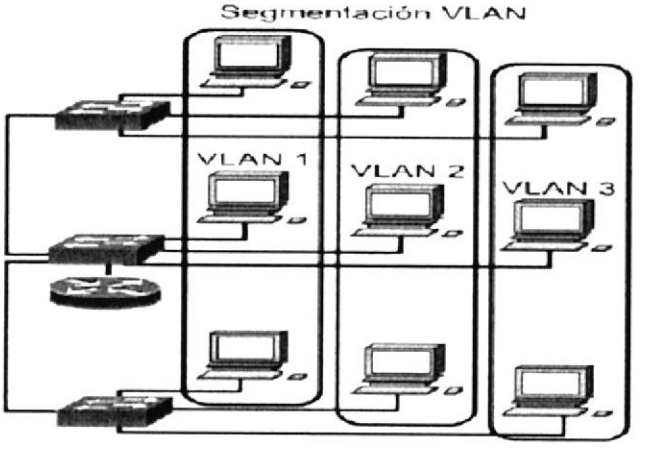


Figura 3-28. Segmentación Con Vlans

- Cada usuario se conecta al switch VLAN más próximo físicamente.

✓ Se definen varias VLANs en los switches.

✓ Los usuarios se agrupan en las VLANs, según criterio del administrador.

✓ La pertenencia de un usuario a una VLAN no depende del cableado físico.

✓ Cada VLAN es un dominio de broadcast.

✓ El router permite la comunicación entre VLANs.

3.16.4. ENCAPSULAMIENTO

El encapsulamiento es el proceso por el cual los datos que se deben enviar a través de una subred se deben colocar en paquetes que se puedan administrar mediante las vlans y rastrear. Las tres capas superiores del modelo OSI (aplicación, presentación y sesión). preparan que los datos llegena su destino.

3.16.5. CARACTERÍSTICAS DE LAS VLANS

- Crean una topología virtual independiente de la física
- Permiten agrupar a los usuarios en grupos de trabajo flexibles
- Funcionan en los niveles 2 y 3 de OSI
- La comunicación entre VLANs requiere enrutamiento de capa 3 (routers)
- Permiten controlar el tamaño de los dominios de broadcast
- Necesitan administración
- Pueden ayudar a aumentar la seguridad de la red

3.16.6. ASIGNACIÓN A VLANS

La asignación de usuarios a las VLANs definidas puede ser:

3.16.6.1. ESTÁTICA:

Cada puerto del switch es asignado a una VLAN. Por tanto, el usuario conectado a ese puerto pertenecerá a la VLAN.

- ✓ El administrador debe realizar la configuración VLAN manualmente
- ✓ Fácil de administrar
- ✓ Implementación más eficiente

3.16.6.2. DINÁMICA:

La pertenencia se determina en función de la dirección física (capa 2), dirección lógica (capa 3), tipo de protocolo, etc.

- ✓ Necesita de un servidor de configuración VLAN (que hay que mantener)
- ✓ Al conectar un usuario a un puerto, el switch consulta el servidor de configuración para determinar a qué VLAN pertenece
- ✓ No necesita administración al realizar desplazamientos de usuarios
- ✓ Seguridad: notificación cuando usuarios no autorizados acceden a la red

3.16.7. TIPOS DE VLANS

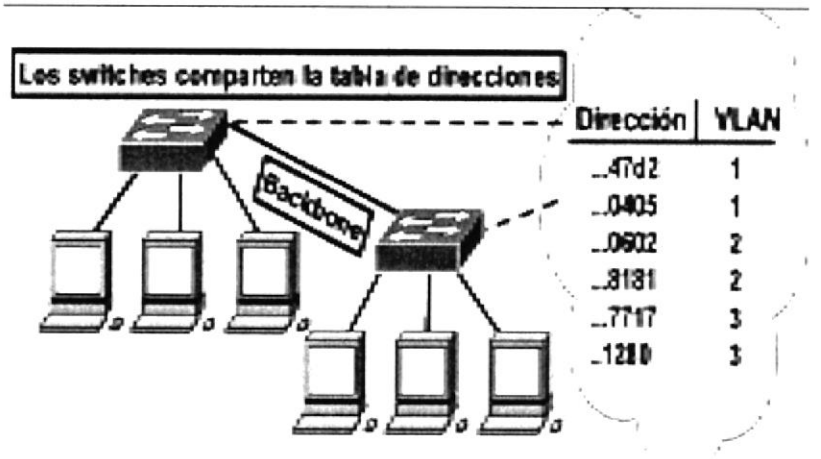


Figura 3-29.Vlan Entre Switches

3.16.8. VLAN ENTRE SWITCHES: FILTRADO

- ✓ Cada switch desarrolla una tabla de filtrado, que asocia cada dirección física con la VLAN a la que pertenece
- ✓ Los switches comparten las tablas a través del backbone
- ✓ Cuando una trama llega a un switch, éste puede determinar a qué VLAN pertenece empleando la tabla
- ✓ Esta técnica permite filtrar en función de cualquier parámetro de la trama (dirección física, lógica, ...)
- ✓ No es escalable; no se emplea actualmente

1.1. *VLAN ENTRE SWITCHES: ETIQUETADO*

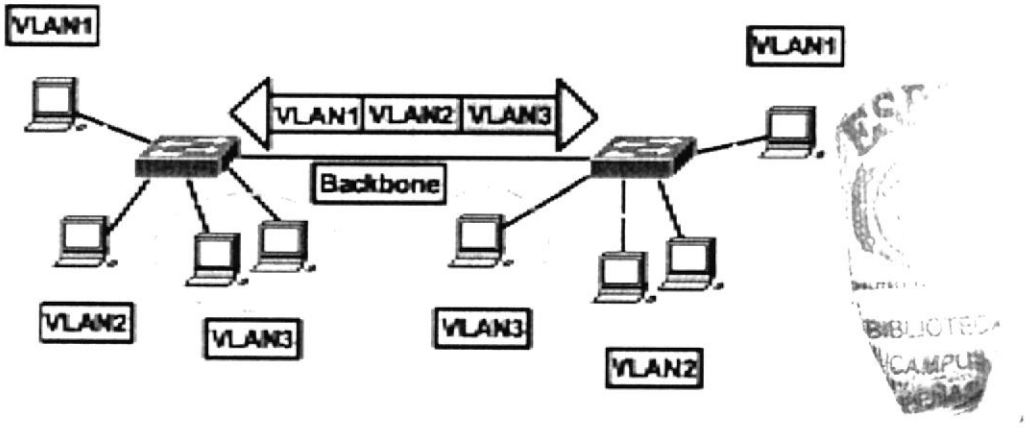


Figura 3-30.Vlan Entre Switches (Etiquetado)

- ✓ Cada VLAN tiene asociado un identificador
- ✓ Las tramas procedentes de los usuarios se etiquetan con el identificador correspondiente a la VLAN a la que pertenecen
- ✓ El etiquetado se lleva a cabo en el switch (capa 2 OSI)
- ✓ Las tramas etiquetadas atraviesan el backbone
- ✓ Cuando una trama etiquetada va a abandonar el backbone, el switch elimina el identificador
- ✓ Estándar IEEE 802.1Q

3.16.9. SEGURIDAD DE VLANS

- ✓ Un usuario sólo puede ver el tráfico broadcast de su VLAN.
- ✓ Un usuario no puede conectarse a la red sin la aprobación del administrador.
- ✓ Configuración de los switches: sólo desde la VLAN de gestión.
- ✓ Los routers pueden incorporar listas de control de acceso para filtrar el tráfico entre VLANs.

3.16.10. VENTAJAS DE LAS VLANS

- ✓ Permite reducir los broadcast.
- ✓ Brinda una mayor seguridad en la red LAN.
- ✓ Reduce congestionamiento en la red.
- ✓ Brinda estabilidad el usuario en el manejo de la red.
- ✓ Si un departamento genera un broadcast no le afectaría al resto de los departamentos.

3.17. DISTRIBUCIÓN DE LAS DIRECCIONES DE RED

Dentro de cada una de las Empresas

Cant. de direcciones de host requeridas	Dirección de red	Máscara de subred	Cantidad máxima de hosts posible	En uso (Sí / No)	Nombre de la red
30	192.168.1.32	255.255.255.240	62	Si	URBANIS
18	192.168.1.64	255.255.255.240	62	Si	MALL DEL SUR
13	192.168.1.96	255.255.255.240	62	Si	DURAN OUTLET

Tabla 3-4 Distribución De Las Direcciones

Ubicación: EDIFICIO URBANIS
Nombre del router: URBANIS

Tipo/# de Interfaz/ Sub-interfaz	Descripción objetivo	DCE/ DTE (si corresponde)	Vel. de reloj	Nombre de la red	# de la red	Dirección IP de la interfaz	Máscara de subred
1	URBANIS	DCE	56000	URBANIS	1	192.168.1.1	255.255.255.0
2	DURAN OUTLET	DTE		DURAN	2	192.168.1.2	255.255.255.0

Tabla 3-5 Distribución De Urbanis

Ubicación: EDIFICIO DURAN OUTLET
Nombre del router: DURAN

Tipo/# de Interfaz/ Sub-interfaz	Desc. y objetivo	DCE/ DTE (si corresponde)	Vel. de reloj	Nombre de la red	# de la red	Dirección IP de la interfaz	Máscara de subred
1	DURAN OUTLET	DCE	56000		1	192.168.1.9	255.255.255.0
2	MALL DEL SUR	DTE			2	192.168.1.10	255.255.255.0

Tabla 3-6 Distribución De Duran Outlet

Ubicación: EDIFICIO MALL DEL SUR
Nombre del router: SUR

Tipo/No. de Interfaz/ Sub-interfaz	Desc. y objetivo	DCE/ DTE (si corresponde)	Vel. de reloj	Nombre de la red	# de red	Dirección IP de la interfaz	Máscara de subred
1	MALL DEL SUR	DCE	56000		1	192.168.1.5	255.255.255.0
2	URBANIS	DTE			2	192.168.1.6	255.255.255.0

Tabla 3-7 Distribución De Mall Del Sur

Ubicación: EDIFICIO URBANIS
Nombre del Switch: URBA_1
Dirección IP del Switch: 192.168.1.16

Tipo/Puerto/ No. de Interfaz/ Sub-interfaz	Desc .y objetivo	Vel.	Duplex	Nombre de la red	No. de la red	Máscara de subred	VLAN	Tipo de puerto de Switch	Encapsulamiento (en caso de ser necesario)
1-8		10 MBS	FULL	VENTAS		240	10	ACCESS	
40-48		100 MBS	FULL	SISTEMAS		240	20	ACCESS	
64-96		100 MBS	FULL	OPERACIONES		240	30	ACCESS	
128-160 160-190		100 MBS	FULL	COBRANZA		240	40	ACCESS	

Tabla 3-8 Distribución De Edificio Urbanis

Para completar el diseño IP, asigne y tabule las direcciones de la PC/estación de trabajo y del servidor para cada LAN en cada ubicación.

Nombre de la LAN	Nombre de la PC o servidor	Dirección IP	Máscara de subred	Gateway	Servicios suministrados
VENTAS	VENT_1	192.168.1.26	255.255.255.240	192.168.1.17	
VENTAS	VENT_2	192.168.1.27	255.255.255.240	192.168.1.17	
VENTAS	VENT_3	192.168.1.28	255.255.255.240	192.168.1.17	
VENTAS	VENT_4	192.168.1.29	255.255.255.240	192.168.1.17	
VENTAS	VENT_5	192.168.1.30	255.255.255.240	192.168.1.17	
VENTAS	VENT_6	192.168.1.31	255.255.255.240	192.168.1.17	
VENTAS	VENT_7	192.168.1.34	255.255.255.240	192.168.1.17	
VENTAS	VENT_8	192.168.1.35	255.255.255.240	192.168.1.17	
VENTAS	VENT_9	192.168.1.36	255.255.255.240	192.168.1.17	
VENTAS	VENT_10	192.168.1.37	255.255.255.240	192.168.1.17	
OPERACIONES	OPER_1	192.168.1.42	255.255.255.240	192.168.1.25	
OPERACIONES	OPER_2	192.168.1.43	255.255.255.240	192.168.1.25	
OPERACIONES	OPER_3	192.168.1.44	255.255.255.240	192.168.1.25	
OPERACIONES	OPER_4	192.168.1.45	255.255.255.240	192.168.1.25	
SISTEMAS	SIST_1	192.168.1.44	255.255.255.240	192.168.1.33	
SISTEMAS	SIST_2	192.168.1.45	255.255.255.240	192.168.1.33	
COBRANZAS	COB_1	192.168.1.50	255.255.255.240	192.168.1.41	
COBRANZAS	COB_2	192.168.1.51	255.255.255.240	192.168.1.41	

Tabla 3-9 Diseño Ip

Se deben preparar tablas que documenten las asignaciones de puertos VLAN del Switch para el equipo de demostración disponible. Cualquier puerto que no haya sido asignado debe permanecer en la VLAN por defecto.
La tabla siguiente es un ejemplo de la documentación requerida por la empresa.

Nombre del Switch	Modelo	N° de puertos	ubicación	Dirección IP	Gateway	VLAN de administración
URBA_1	2950	48	Ventas	192.168.1.24	192.168.1.17	VLAN 1
URBA_1	2950	48	Operaciones	192.168.1.32	192.168.1.25	VLAN 2
URBA_1	2950	48	Sistema	192.168.1.40	192.168.1.33	VLAN 3
URBA_1	2950	48	cobranza	192.168.1.48	192.168.1.41	VLAN 4

Tabla 3-10 Documentación De La Empresa

Ubicación: EDIFICIO DURAN
Nombre del Switch: DUR_1
Dirección IP del Switch: 192.168.1.24

Tipo/Puerto/ No. de Interfaz/ Sub-interfaz	Desc.y objetivo	Vel.	Duplex	Nombre de la red	No.de la red	Máscara de subred	VLAN	Tipo de puerto de Switch	Encapsulamiento (en caso de ser necesario)
1-8		10 MBS	FULL	COBRANZA		240	10	ACCESS	
40-48		100 MBS	FULL	CONTABILIDAD		240	20	ACCESS	
64-96		100 MBS	FULL	ADMINISTRACION		240	30	ACCESS	
128-160 160-190		100 MBS	FULL	SISTEMAS		240	40	ACCESS	

Tabla 3-11 Edificio Duran

Para completar el diseño IP, asigne y tabule las direcciones de la PC/estación de trabajo y del servidor para cada LAN en cada ubicación.

Nombre de la LAN	Nombre de la PC o servidor	Dirección IP	Máscara de subred	Gateway	Servicios suministrados
COBRANZA	COB_1	192.168.1.57	255.255.255.40	192.168.1.25	
COBRANZA	COB_2	192.168.1.58	255.255.255.40	192.168.1.25	
COBRANZA	COB_3	192.168.1.59	255.255.255.40	192.168.1.25	
COBRANZA	COB_4	192.168.1.60	255.255.255.40	192.168.1.25	
COBRANZA	COB_5	192.168.1.61	255.255.255.40	192.168.1.25	
CONTABILIDAD	CONT_1	192.168.1.66	255.255.255.40	192.168.1.57	
CONTABILIDAD	CONT_2	192.168.1.67	255.255.255.40	192.168.1.57	
CONTABILIDAD	CONT_3	192.168.1.68	255.255.255.40	192.168.1.57	
CONTABILIDAD	CONT_4	192.168.1.69	255.255.255.40	192.168.1.57	
CONTABILIDAD	CONT_5	192.168.1.70	255.255.255.40	192.168.1.57	
CONTABILIDAD	CONT_6	192.168.1.71	255.255.255.40	192.168.1.57	
ADMINISTRACION	ADMI_1	192.168.1.74	255.255.255.40	192.168.1.65	
ADMINISTRACION	ADMI_2	192.168.1.75	255.255.255.40	192.168.1.65	
ADMINISTRACION	ADMI_3	192.168.1.76	255.255.255.40	192.168.1.65	
ADMINISTRACION	ADMI_4	192.168.1.77	255.255.255.40	192.168.1.65	
ADMINISTRACION	ADMI_5	192.168.1.78	255.255.255.40	192.168.1.65	
SISTEMAS	SIS_1	192.168.1.82	255.255.255.40	192.168.1.73	
SISTEMAS	SIS_2	192.168.1.83	255.255.255.40	192.168.1.73	
SISTEMAS	SIS_3	192.168.1.84	255.255.255.40	192.168.1.73	

SISTEMAS	SIS_4	192.168.1.85	255.255.255.40	192.168.1.73	
SISTEMAS	SIS_5	192.168.1.86	255.255.255.40	192.168.1.73	

Tabla 3-12 Diseño Ip

Se deben preparar tablas que documenten las asignaciones de puertos VLAN del Switch para el equipo de demostración disponible. Cualquier puerto que no haya sido asignado debe permanecer en la VLAN por defecto.
La tabla siguiente es un ejemplo de la documentación requerida por la empresa.

Nombre del Switch	Modelo	N° de puertos	ubicación	Dirección IP	Gateway	VLAN de administración
DUR_1	2950	24	Cobranza	192.168.1.56	192.168.1.25	VLAN 1
DUR_1	2950	24	Contabilidad	192.168.1.64	192.168.1.57	VLAN 2
DUR_1	2950	24	Administración	192.168.1.72	192.168.1.65	VLAN 3
DUR_1	2950	24	Sistemas	192.168.1.80	192.168.1.73	VLAN 4

Tabla 3-13 Documentación De la Empresa

Ubicación: EDIFICIO MALL DEL SUR
Nombre del Switch: SUR_1
Dirección IP del Switch: 192.168.1.32

Tipo/Puerto/ No. de Interfaz/ Sub-interfaz	Desc. y objetivo	Vel.	Dúplex	Nombre de la red	No.de la red	Máscara de subred	VLAN	Tipo de puerto de Switch	Encapsulamiento (en caso de ser necesario)
1-8		10 MBS	FULL	GERENCIA		240	10	ACCESS	
64-96		100 MBS	FULL	CONTABILIDAD		240	20	ACCESS	
128-160 160-190		100 MBS	FULL	SISTEMAS		240	30	ACCESS	

Tabla 3-14 Edificio Mall Del Sur

Para completar el diseño IP, asigne y tabule las direcciones de la PC/estación de trabajo y del servidor para cada LAN en cada ubicación.

Nombre de la LAN	Nombre de la PC o servidor	Dirección IP	Máscara de subred	Gateway	Servicios suministrados
GERENCIA	GER_1	192.168.1.90	255.255.255.240	192.168.1.32	
GERENCIA	GER_2	192.168.1.91	255.255.255.240	192.168.1.32	
GERENCIA	GER_3	192.168.1.92	255.255.255.240	192.168.1.32	
GERENCIA	GER_4	192.168.1.93	255.255.255.240	192.168.1.32	
GERENCIA	GER_5	192.168.1.94	255.255.255.240	192.168.1.32	
CONTABILIDAD	CONT_1	192.168.1.98	255.255.255.240	192.168.1.32	
CONTABILIDAD	CONT_2	192.168.1.99	255.255.255.240	192.168.1.32	
CONTABILIDAD	CONT_3	192.168.1.100	255.255.255.240	192.168.1.32	

CONTABILIDAD	CONT_4	192.168.1.101	255.255.255.240	192.168.1.32	
CONTABILIDAD	CONT_5	192.168.1.102	255.255.255.240	192.168.1.32	
CONTABILIDAD	CONT_6	192.168.1.103	255.255.255.240	192.168.1.32	
SISTEMAS	SIS_1	192.168.1.106	255.255.255.240	192.168.1.32	
SISTEMAS	SIS_2	192.168.107	255.255.255.240	192.168.1.32	

Tabla 3-15 Diseño Ip

Se deben preparar tablas que documenten las asignaciones de puertos VLAN del switch para el equipo de demostración disponible. Cualquier puerto que no haya sido asignado debe permanecer en la VLAN por defecto.
La tabla siguiente es un ejemplo de la documentación requerida por la empresa.

Nombre del Switch	Modelo	N° de puertos	ubicación	Dirección IP	Gateway	VLAN de administración
SUR_1	2950	48		192.168.1.88	192.168.1.33	VLAN 1
SUR_1	2950	48		192.168.1.96	192.168.1.89	VLAN 2
SUR_1	2950	48		192.168.1.104	192.168.1.97	VLAN 3

Tabla 3-16 documentación Requerida

3.18. CONFIGURACIÓN DE LOS ROUTER Y SWITCH

3.18.1. ASGNACION DE NOMBRE AL ROUTER

3.18.1.1. ROUTER URBANIS

Press Enter to Start

Router>
Router>enable
Router#configure terminal
Enter configuration commands , one per line. End with CNTL/Z
Router(config)#hostname URBANIS
URBANIS(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console
URBANIS#wr
Building configuration...
[OK

URBANIS#

3.18.1.2. ROUTER DURAN

Press Enter to Start

Router>
Router>enable
Router#configure terminal
Enter configuration commands , one per line. End with CNTL/Z
Router(config)#hostname DURAN
DURAN (config)#^Z
%SYS-5-CONFIG_I: Configured from console by console
DURAN #wr
Building configuration...
[OK

DURAN #

3.18.1.3. ROUTER SUR

Press Enter to Start

Router>
Router>enable
Router#configure terminal
Enter configuration commands , one per line. End with CNTL/Z
Router(config)#hostname SUR
SUR (config)#^Z
%SYS-5-CONFIG_I: Configured from console by console
SUR #wr

Building configuration...
[OK

SUR #

3.19. CONFIGURACIÓN DE LA INTERFAZ (S0/0 – S0/1)

NOTA: Antes de configurar las interfaces en cualquier router lo primero que debemos darnos cuenta con que nombre están asignado las seriales con el comando show protocols, y a su vez permiten ver si las seriales están baja o no

URBANIS#show protocols
Global values:
Internet Protocol routing is enabled
Serial0 is administratively down, line protocol is down
Serial1 is administratively down, line protocol is down
FastEthernet 0/0 is administratively down,line protocol is down
Brio is administratively down, line protocol is down
Brio:1 is administratively down, line protocol is down
Brio:2 is administratively down, line protocol is down

3.19.1. ROUTER URBANIS

3.19.1.1. CONFIGURACIÓN DE LA SERIAL 0 DEL ROUTER URBANIS

URBANIS#configure terminal
Enter configuration commands , one per line. End with CNTL/Z
URBANIS(config)#interface serial 0
URBANIS(config- if)#ip address 192.168.1.1 255.255.255.0
URBANIS(config- if)#clock rate 64000
URBANIS(config- if)#no shutdown
%LINK-3-UPDOWN:Interface serial1, changed stated to up
URBANIS(config- if)#^Z
%SYS-5-CONFIG_I: Configured from console by console

URBANIS#wr
Building configuration...
[OK]

3.19.1.2. CONFIGURACIÓN DE LA SERIAL 1 DEL ROUTER URBANIS

URBANIS#configure terminal
Enter configuration commands , one per line. End with CNTL/Z
URBANIS(config)#interface serial 1
URBANIS(config- if)#ip address 192.168.1.2 255.255.255.0
URBANIS(config- if)#no shutdown
%LINK-3-UPDOWN:Interface serial1, changed stated to up
URBANIS(config- if)#^Z

%SYS-5-CONFIG_I: Configured from console by console

URBANIS#wr
Building configuration...
[OK]

3.19.2. ROUTER DURAN

3.19.2.1. CONFIGURACIÓN DE LA SERIAL 0 DEL ROUTER DURAN

DURAN#configure terminal
Enter configuration commands , one per line. End with CNTL/Z
DURAN (config)#interface serial 0
DURAN (config- if)#ip address 192.168.1.9 255.255.255.0
DURAN(config- if)#clock rate 64000
DURAN (config- if)#no shutdown
%LINK-3-UPDOWN:Interface serial1, changed stated to up
DURAN (config- if)#^Z
%SYS-5-CONFIG_I: Configured from console by console

DURAN #wr
Building configuration...
[OK]

3.19.2.2. CONFIGURACIÓN DE LA SERIAL 1 DEL ROUTER DURAN

DURAN#configure terminal
Enter configuration commands , one per line. End with CNTL/Z
DURAN (config)#interface serial 1
DURAN (config- if)#ip address 192.168.1.10 255.255.255.0
DURAN (config- if)#no shutdown
%LINK-3-UPDOWN:Interface serial1, changed stated to up
DURAN (config- if)#^Z
%SYS-5-CONFIG_I: Configured from console by console

DURAN #wr
Building configuration...
[OK]

3.19.3. ROUTER SUR

3.19.3.1. CONFIGURACIÓN DE LA SERIAL 0 DEL ROUTER SUR

SUR#configure terminal
Enter configuration commands , one per line. End with CNTL/Z
SUR (config)#interface serial 0
SUR (config- if)#ip address 192.168.1.5 255.255.255.0
SUR(config- if)#clock rate 64000
SUR (config- if)#no shutdown
%LINK-3-UPDOWN:Interface serial1, changed stated to up

SUR (config- if)#^Z
%SYS-5-CONFIG_I: Configured from console by console
SUR #wr
Building configuration...
[OK]

3.19.3.2. CONFIGURACIÓN DE LA SERIAL 1 DEL ROUTER DURAN

DURAN#configure terminal
Enter configuration commands , one per line. End with CNTL/Z
DURAN (config)#interface serial 1
DURAN (config- if)#ip address 192.168.1.6 255.255.255.0
DURAN (config- if)#no shutdown
%LINK-3-UPDOWN:Interface serial1, changed stated to up
DURAN (config- if)#^Z
%SYS-5-CONFIG_I: Configured from console by console

DURAN #wr
Building configuration...
[OK]

3.20. VERIFICAR SI LAS DIRECCIONES SERIALES SE LEVANTAN CON ÉXITO.

3.20.1. ROUTER URBANIS

La dirección que se conecta con el router esta levantada (UP)

URBANIS#show protocols
Global values:
Internet protocol routing is enabled
Serial0 is up , line protocol is up
Internet address is 192.168.1.1 /24
Serial1 is up , line protocol is up
Internet address is 192.168.1.2 /24
FastEthernet0/0 is administratively down, line protocol is down
Brio is administratively down, line protocol is down
Brio:1 is administratively down, line protocol is down
Brio:2 is administratively down, line protocol is down

3.20.2. ROUTER DURAN

La dirección que se conecta con el router esta levantada (UP)

URBANIS#show protocols
Global values:
Internet protocol routing is enabled
Serial0 is up , line protocol is up
Internet address is 192.168.1.9 /24

Serial1 is up , line protocol is up
Internet address is 192.168.1.10/24
FastEthernet0/0 is administratively down, line protocol is down
Brio is administratively down, line protocol is down
Brio:1 is administratively down, line protocol is down
Brio:2 is administratively down, line protocol is down

3.20.3. ROUTER SUR

La dirección que se conecta con el router esta levantada (UP)

URBANIS#show protocols
Global values:
Internet protocol routing is enabled
Serial0 is up , line protocol is up
Internet address is 192.168.1.5 /24
Serial1 is up , line protocol is up
Internet address is 192.168.1.6 /24
FastEthernet0/0 is administratively down, line protocol is down
Brio is administratively down, line protocol is down
Brio:1 is administratively down, line protocol is down
Brio:2 is administratively down, line protocol is down

3.21. CONFIGURAR LA FAST ETHERNET

3.21.1. ROUTER URBANIS

URBANIS#
URBANIS#configure terminal
Enter configuration commands , one per line. End with CNTL/Z
URBANIS(config)#interface fastethernet 0/0
URBANIS(config- if)#ip address 192.168.1.16 255.255.255.0
URBANIS(config- if)#no shutdown
%LINK-3-UPDOWN:Interface fastethernet 0/0 changed stated to up
URBANIS(config- if)#^Z
%SYS-5-CONFIG_I: Configured from console by console

URBANIS#wr
Building configuration...
[OK]

3.21.2. ROUTER DURAN

DURAN#
DURAN #configure terminal
Enter configuration commands , one per line. End with CNTL/Z
DURAN (config)#interface fastethernet 0/0
DURAN(config- if)#ip address 192.168.16.24 255.255.255.0
DURAN (config- if)#no shutdown

%LINK-3-UPDOWN:Interface fastethernet 0/0 changed stated to up
DURAN (config- if)#^Z
%SYS-5-CONFIG_I: Configured from console by console

DURAN #wr
Building configuration...
[OK]

3.21.3. ROUTER SUR

SUR#
SUR #configure terminal
Enter configuration commands , one per line. End with CNTL/Z
SUR (config)#interface fastethernet 0/0
SUR (config- if)#ip address 192.168.1.32 255.255.255.0
SUR (config- if)#no shutdown
%LINK-3-UPDOWN:Interface fastethernet 0/0 changed stated to up
SUR (config- if)#^Z
%SYS-5-CONFIG_I: Configured from console by console

SUR #wr
Building configuration...
[OK]

3.22. VERIFICAR SI LAS DIRECCIONES FASTETHERNET SE LEVANTAN CON ÉXITO.

3.22.1. ROUTER URBANIS

La dirección 192.168.1.16 que pertenece a la fastethernet de URBANIS esta levantada (UP)

URBANIS#show protocols
Global values:
Internet protocol routing is enabled
Serial0 is up , line protocol is up
Internet address is 192.168.1.1/24
Serial1 is up , line protocol is up
Internet address is 192.168.1.2/24
FastEthernet0/0 is up, line protocol is up
Internet address is 192.168.1. 16/24

3.22.2. ROUTER DURAN

La dirección 192.168.1.24 que pertenece a la fastethernet de DURAN esta levantada (UP)

DURAN#show protocols

Global values:
Internet protocol routing is enabled
Serial0 is up, line protocol is up
Internet address is 192.168.1.9/24
Serial1 is up, line protocol is up
Internet address is 192.168.1.10/24
FastEthernet0/0 is up, line protocol is up
Internet address is 192.168.1.24/24

3.22.3. ROUTER SUR

La dirección 192.168.1.32 que pertenece a la fastethernet de SUR esta levantada (UP)

SUR#show protocols
Global values:
Internet protocol routing is enabled
Serial0 is up , line protocol is up
Internet address is 192.168.1.5/24
Serial1 is up , line protocol is up
Internet address is 192.168.1.6/24
FastEthernet0/0 is up, line protocol is up
Internet address is 192.168.1.32/24

3.23. CONFIGURAR TELNET

3.23.1. ROUTER URBANIS

URBANIS#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
URBANIS(config)#line console 0
URBANIS(config-line)#password
URBANIS(config-line)#login
URBANIS(config-line)#line vty 0 4
URBANIS(config-line)#password
URBANIS(config-line)#login
URBANIS(config-line)#exit
URBANIS(config)#enable password
URBANIS(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console

URBANIS#wr
Building configuration...
[OK]

3.23.2. ROUTER DURAN

URBANIS#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
DURAN(config)#line console 0

```
DURAN(config-line)#password
DURAN(config-line)#login
DURAN(config-line)#line vty 0 4
DURAN(config-line)#password
DURAN(config-line)#login
DURAN(config-line)#exit
DURAN(config)#enable password
DURAN(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console

DURAN#wr
Building configuration...
[OK]
```

3.23.3. ROUTER SUR

```
URBANIS#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
SUR(config)#line console 0
SUR(config-line)#password
SUR (config-line)#login
SUR (config-line)#line vty 0 4
SUR (config-line)#password
SUR (config-line)#login
SUR (config-line)#exit
SUR (config)#enable password
SUR (config)#^Z
%SYS-5-CONFIG_I: Configured from console by console

SUR #wr
Building configuration...
[OK]
```

3.24. CONFIGURACIÓN DE LOS PROTOCOLOS DE ENRUTAMIENTOS

NOTA: Los protocolos enrutamiento están ligados a nivel **WAN** en este caso solo va a usar el protocolo **OSPF:**

3.24.1. ROUTER URBANIS

```
URBANIS#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
URBANIS(config)#router ospf 1
URBANIS(config-router)#network  192.168.1.1   0.0.0.  area   0
URBANIS(config-router)#network  192.168.1.2   0.0.0.  area   0
URBANIS(config-router)#^Z
%SYS-5-CONFIG_I: Configured from console by console
```

```
URBANIS#wr
Building configuration...
[OK]
```

3.24.2. ROUTER DURAN

```
DURAN#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
DURAN(config)#router ospf 1
DURAN(config-router)#network    192.168.1.9    0.0.0.  area    0
DURAN(config-router)#network    192.168.1.10   0.0.0.  area    0
DURAN(config-router)#^Z
%SYS-5-CONFIG_I: Configured from console by console

DURAN#wr
Building configuration...
[OK]
```

3.24.3. ROUTER SUR

```
URBANIS#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
URBANIS(config)#router ospf 1
URBANIS(config-router)#network  192.168.1.5    0.0.0.  area    0
URBANIS(config-router)#network  192.168.1.6    0.0.0.  area    0
URBANIS(config-router)#^Z
%SYS-5-CONFIG_I: Configured from console by console

URBANIS#wr
Building configuration...
[OK]
```

3.25. PRUEBAS DE PING ENTRE SUCURSALES Y MATRIZ

NOTA: Una vez realizado las Configuraciones de los protocolos de enrutamiento comenzara las pruebas de ping, con la finalidad de saber si los dispositivos se comunican el uno con el otro.

3.25.1. ROUTER URBANIS

El router URBANIS hace ping a su propio serial 0 y i para ver si tiene conexión entre ello mismo.

```
URBANIS#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte  ICMP Echos To 192.168.1.1  timeout is 2 second:
!!!!!
```

Success rate is 100 percent (5/5), round-trip min/avg /max =1/2/4 ms
El router URBANIS hace ping a la IP que sale del serial 0 de su propio router
URBANIS#ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos To 192.168.1.2 timeout is 2 second:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg /max =1/2/4 ms
El router URBANIS hace ping a la IP que sale del serial 1 de su propio router
URBANIS#ping 192.168.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos To 192.168.1.10 timeout is 2 second:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg /max =1/2/4 ms
El router URBANIS hace ping a la IP que sale del serial 0 de su propio router
URBANIS#ping 192.168.1.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos To 192.168.1.5 timeout is 2 second:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg /max =1/2/4 ms
El router URBANIS hace ping a la IP que sale del serial 1 de su propio router

3.25.2. ROUTER DURAN

El router DURAN hace ping a su propio serial 0 y i para ver si tiene conexión entre ello mismo.

DURAN#ping 192.168.1.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos To 192.168.1.9 timeout is 2 second:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg /max =1/2/4 ms
El router DURAN hace ping a la IP que sale del serial 0 de su propio router

DURAN#ping 192.168.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos To 192.168.1.10 timeout is 2 second:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg /max =1/2/4 ms
El router DURAN hace ping a la IP que sale del serial 1 de su propio router
DURAN#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos To 192.168.1.1 timeout is 2 second:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg /max =1/2/4 ms
El router DURAN hace ping a la IP que sale del serial 0 de su propio router

DURAN#ping 192.168.1.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos To 192.168.1.6 timeout is 2 second:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg /max =1/2/4 ms
El router DURAN hace ping a la IP que sale del serial 1 de su propio router

3.25.3. ROUTER SUR

El router SUR hace ping a su propio serial 0 y i para ver si tiene conexión entre ello mismo.

SUR#ping 192.168.1.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos To 192.168.1.5 timeout is 2 second:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg /max =1/2/4 ms
El router SUR hace ping a la IP que sale del serial 0 de su propio router

SUR#ping 192.168.1.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos To 192.168.1.6 timeout is 2 second:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg /max =1/2/4 ms
El router SUR hace ping a la IP que sale del serial 1 de su propio router
SUR#ping 192.168.1.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos To 192.168.1.9 timeout is 2 second:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg /max =1/2/4 ms
El router SUR hace ping a la IP que sale del serial 0 de su propio router

SUR#ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos To 192.168.1.2 timeout is 2 second:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg /max =1/2/4 ms
El router SUR hace ping a la IP que sale del serial 1 de su propio router

3.26. CONFIGURACIÓN DE LAS VLANS

NOTA: Para comenzar a configurar las vlans primeramente tenemos que subnetiar bien ya que aquí tenemos que sacar las interfaz por lo tanto cada sub interfaz vendría hacer una vlan diferente.

3.26.1. CONFIGURACIÓN DE LAS VLANS DE URBANIS

3.26.1.1. SWITCH URBANIS

- **PRIMER PASO**

Crear las vlan en una base de datos donde se almacena las vlans en el Switch

```
URBA_1#vlan database
URBA_1(vlan)#vlan 10      name  ventas
URBA_1(vlan)#vlan 20      name  sistemas
URBA_1(vlan)#vlan 30      name  operaciones
URBA_1(vlan)#vlan 40      name  cobranza
APPLY completed.
Exiting...
URBA_1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

- **SEGUNDO PASO**

Verifica si las vlans fueron creadas con éxito haciendo un show vlan

```
URBA_1#show vlan
Vlan Name                              Status    Ports
---------------------------------------------------------------------------------------
-----------
1 defaul                               active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
10      ventas                         active

20      sistemas                       active

30      operaciones                    active

40      cobranza                       active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

- **TERCER PASO**

Una vez realizadas las vlan: asignaremos los puertos fastethernet e las vlans según sean asignados por el administrador

```
Urba_1#configure terminal
URBA_1(config)#interface fastethernet 0/2
```

```
URBA_1(config-if)#switchport  mode  trunk
URBA_1(config-if)#switchport  Access  vlan  10
URBA_1(config)#interface fastethernet 0/3
URBA_1(config-if)#switchport  mode  trunk
URBA_1(config-if)#switchport  Access  vlan  20
URBA_1(config)#interface fastethernet 0/4
URBA_1(config-if)#switchport  mode  trunk
URBA_1(config-if)#switchport  Access  vlan  30
URBA_1(config)#interface fastethernet 0/5
URBA_1(config-if)#switchport  mode  trunk
URBA_1(config-if)#switchport  Access  vlan  40
URBA_1(config-if)#^Z

URBA_1#copy running-config  startup-config
Building configuration...
[OK]
```

- **CUARTO PASO**

Verifica si los puertos fueron asignados en sus respectivas vlans

URBA_1#show vlan

Vlan Name	Status	Ports
1 defaul	active	Fa0/1, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12
10 ventas	active	Fa0/2
20 sistemas	active	Fa0/3
30 operaciones	active	Fa0/4
40 cobranza	active	Fa0/5
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

3.26.2. ROUTER URBANIS

NOTA:Una vez realizadas las vlans en el switch toca configurar las subinterfas en el router donde se especifica en el router cuales son las subinterfas y en que vlan son asignadas. En el puerto que viajan las vlan hacia al router es 802.1Q

- **Primer Paso**

  ✓ En el router tendremos que configurar las subinterfas con sus respectivas vlans; con la finalidad para que se puedan comunicarse una vlan con otra.

URBANIS#configure Terminal

```
URBANIS(config)#interface fastethernet 0/0.1
URBANIS(config-subif)#ip address  192.168.1.17  255.255.255.240
URBANIS(config-subif)#no shutdown
URBANIS(config-subif)#encasuplation dot1q  10
URBANIS(config-subif)#exit
URBANIS(config)#interface fastethernet 0/0.2
URBANIS(config-subif)#ip address  192.168.1.25  255.255.255.240
URBANIS(config-subif)#no shutdown
URBANIS(config-subif)#encasuplation dot1q  20
URBANIS(config-subif)#exit
URBANIS(config)#interface fastethernet 0/0.3
URBANIS(config-subif)#ip address  192.168.1.33  255.255.255.240
URBANIS(config-subif)#no shutdown
URBANIS(config-subif)#encasuplation dot1q  30
URBANIS(config-subif)#exit
URBANIS(config)#interface fastethernet 0/0.4
URBANIS(config-subif)#ip address  192.168.1.41  255.255.255.240
URBANIS(config-subif)#no shutdown
URBANIS(config-subif)#encasuplation dot1q  40
URBANIS(config-subif)#^Z
```

HOST

Una vez configurados los Switch y el router nos tocaran configurar las maquinas d cada usuario donde asignaremos la IP y el Gateway por donde pasara la comunicación

HOST DPTO. VENTAS

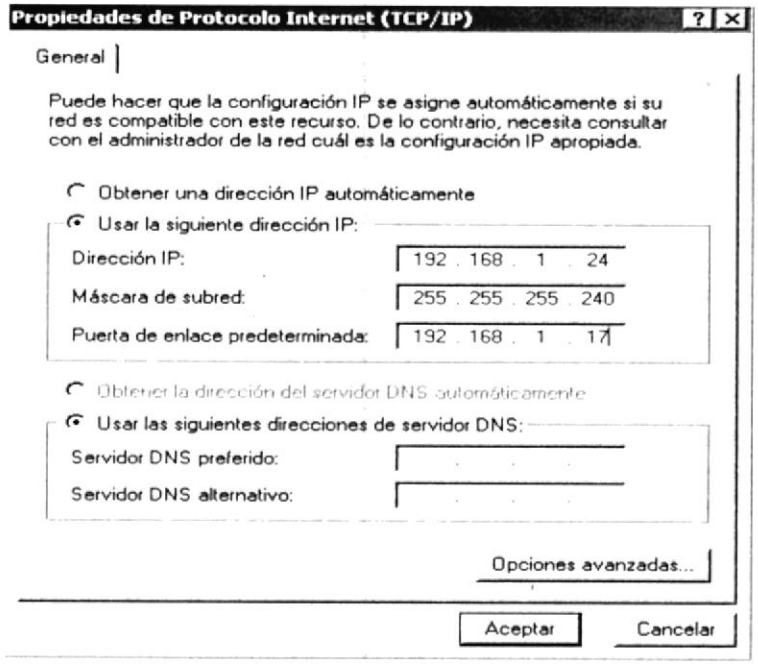


Figura 3-31.Ventas

HOST DPTO. OPERACIONES

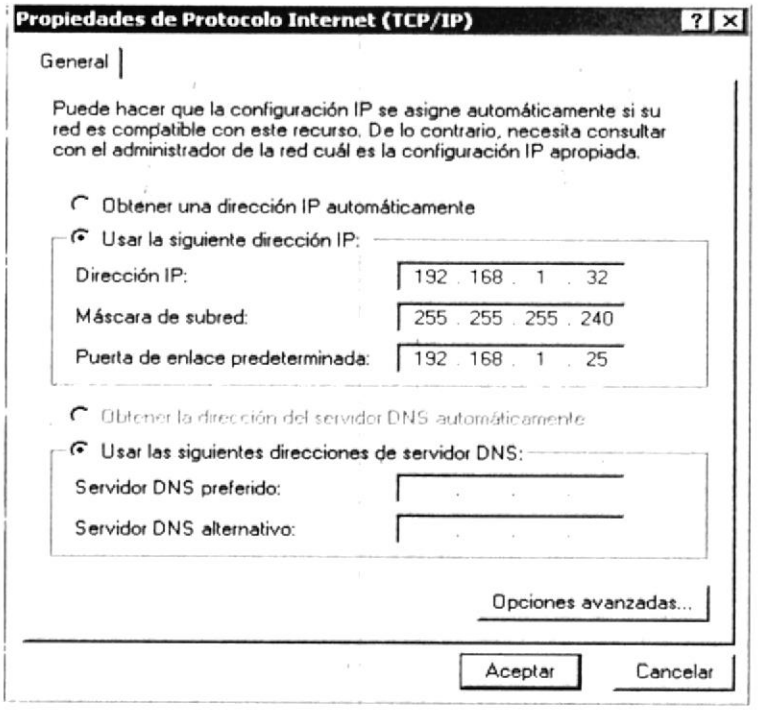


Figura 3-32.Operaciones

HOST DPTO. SISTEMAS

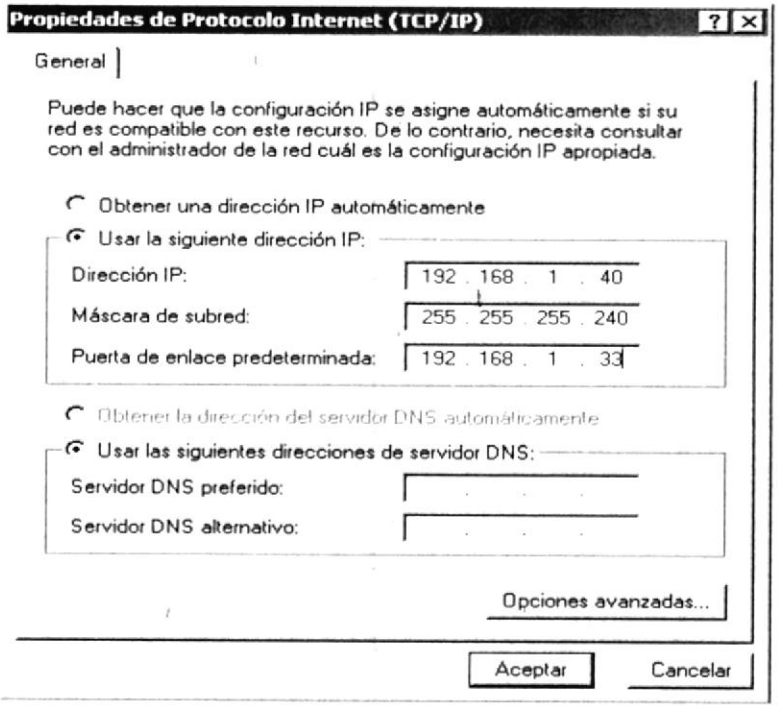


Figura 3-33.Sistemas

HOST DPTO. COBRANZA

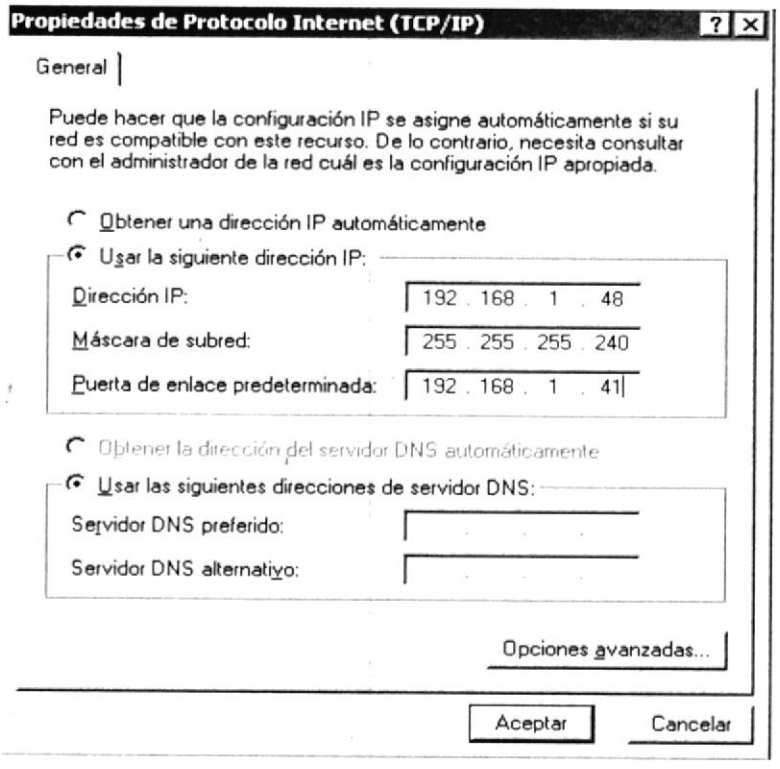


Figura 3-34.Cobranzas

3.27. CONFIGURACIÓN DE LAS VLANS DE DURAN

3.27.1. SWITCH DURAN

- **PRIMER PASO**

Crea las vlan en una base de datos donde se almacena las vlans en el Switch

```
DUR_1#vlan database
DUR_1 (vlan)#vlan  10    name  cobranza
DUR_1 (vlan)#vlan  20    name  contabilidad
DUR_1 (vlan)#vlan  30    name  administración
DUR_1 (vlan)#vlan  40    name  sistemas
APPLY completed.
Exiting...
DUR_1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

- **SEGUNDO PASO**

Verifica si las vlans fueron creadas con éxito haciendo un show vlan

```
DUR_1#show vlan
Vlan Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    defaul                            active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
10   cobranza                          active
20   contabilidad                      active
30   administración                    active
40   sistemas                          active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

- **TERCER PASO**

Una vez realizadas las vlan: asignaremos los puertos fastEthernet e las vlans según sean asignados por el administrador

```
DUR_1(config)#interface fastethernet 0/2
DUR_1 (config-if)#switchport mode trunk
DUR_1(config-if)#switchport Access vlan 10
DUR_1(config)#interface fastethernet 0/3
DUR_1(config-if)#switchport mode trunk
DUR_1 (config-if)#switchport Access vlan 20
DUR_1(config)#interface fastethernet 0/4
DUR_1(config-if)#switchport mode trunk
DUR_1(config-if)#switchport Access vlan 30
DUR_1(config)#interface fastethernet 0/5
DUR_1(config-if)#switchport mode trunk
DUR_1(config-if)#switchport Access vlan 40
DUR_1(config-if)#^Z

DUR_1#copy running-config startup-config
Building configuration...
[OK]
```

- **CUARTO PASO**

Verifica si los puertos fueron asignados en sus respectivas vlans

```
DUR_1#show vlan
Vlan Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
```

1	defaul	active	Fa0/1, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12
10	cobranza	active	Fa0/2
20	contabilidad	active	Fa0/3
30	administración	active	Fa0/4
40	sistemas	active	Fa0/5
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

3.27.2. ROUTER DURAN

NOTA: Una ves realisados las vlans en el switch nos tocara configurar las subinterfas en el router donde especifica en el router cuales seran las subinterfas y en que vlan seran asignadas. En el puerto que viajan las vlan hacia al router es **802.1Q**

- **Primer Paso**

  - ✓ En el router tendremos que configurar las subinterfas con sus respectivas vlans; con la finalidad para que se puedan comunicarse una vlan con otra.

```
DURAN#configure Terminal
DURAN (config)#interface fastethernet 0/0.1
DURAN(config-subif)#ip address  192.168.1.17  255.255.255.240
DURAN(config-subif)#no shutdown
DURAN(config-subif)#encasuplation dot1q  10
DURAN(config-subif)#exit
DURAN(config)#interface fastethernet 0/0.2
DURAN(config-subif)#ip address  192.168.1.25  255.255.255.240
DURAN(config-subif)#no shutdown
DURAN(config-subif)#encasuplation dot1q  20
DURAN(config-subif)#exit
DURAN(config)#interface fastethernet 0/0.3
DURAN(config-subif)#ip address  192.168.1.33  255.255.255.240
DURAN(config-subif)#no shutdown
DURAN(config-subif)#encasuplation dot1q  30
DURAN(config-subif)#exit
DURAN(config)#interface fastethernet 0/0.4
DURAN(config-subif)#ip address  192.168.1.41  255.255.255.240
DURAN(config-subif)#no shutdown
DURAN(config-subif)#encasuplation dot1q  40
DURAN(config-subif)#^Z
```

HOST

Una vez configurados los Switch y el router nos tocaran configurar las maquinas d cada usuario donde asignaremos la IP y el Gateway por donde pasara la comunicación

HOST DPTO. COBRANZA

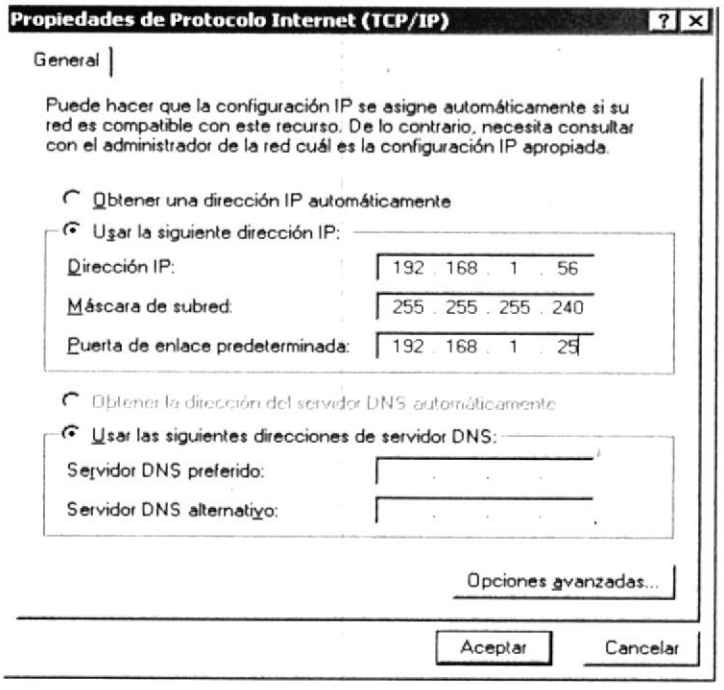


Figura 3-35.Cobranzas

HOST DPTO. CONTABILIDAD

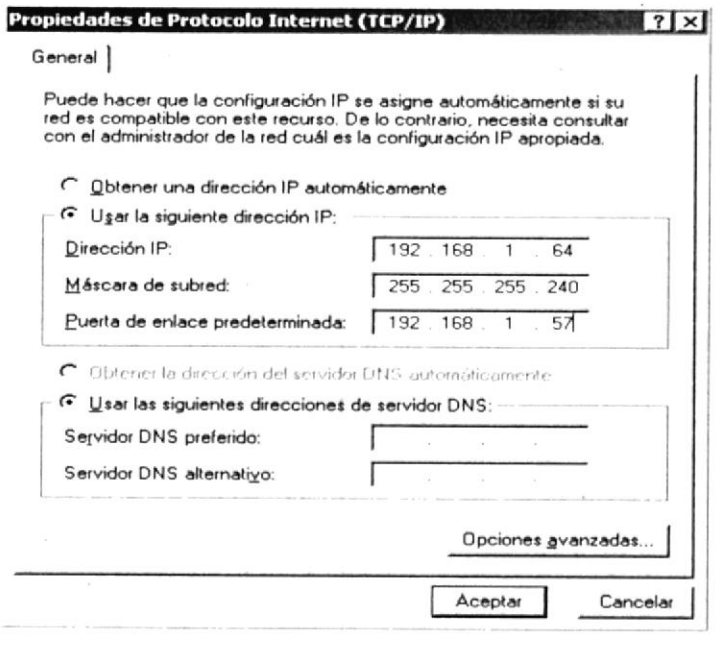


Figura 3-36.Cobranzas

HOST DPTO. ADMINISTRACION

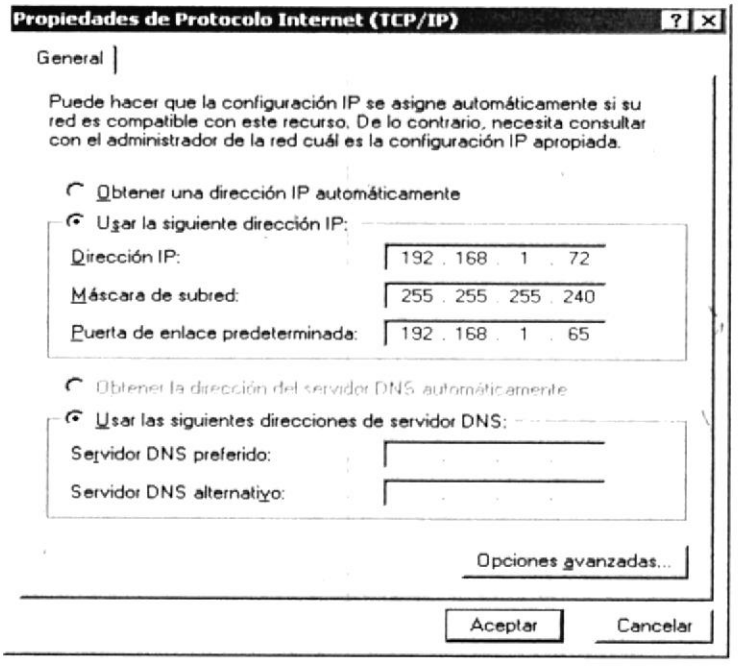
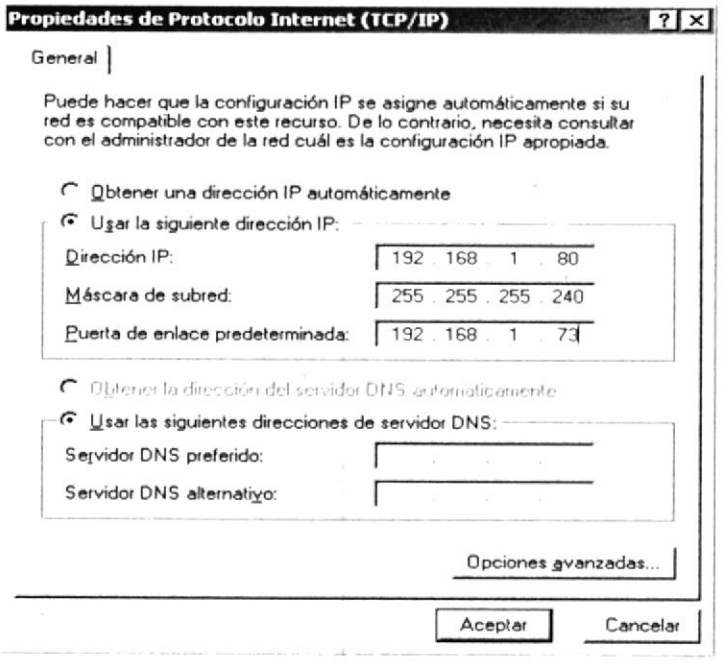


Figura 3-37.Administración

HOST DPTO. SISTEMA



3.27.3. SWITCH SUR

- **PRIMER PASO**

Crea las vlan en una base de datos donde se almacena las vlans en el Switch

SUR_1#vlan database

```
SUR_1(vlan)#vlan   10    name  gerencia
SUR_1(vlan)#vlan   20    name  contabilidad
SUR_1(vlan)#vlan   30    name  sistemas
APPLY completed.
Exiting...
SUR_1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

- **SEGUNDO PASO**

Verifica si las vlans fueron creadas con éxito haciendo un show vlan

```
SUR_1#show vlan
Vlan Name                              Status    Ports
---------------------------------------------------------------------------------------------
----------
1    defaul                            active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
10   gerencias                         active

20   contabilidad                      active

30   sistemas                          active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

- **TERCER PASO**

Una vez realizadas las vlan: asignaremos los puertos fastethernet e las vlans según sean asignados por el administrador

```
SUR_1#configure terminal
SUR_1(config)#interface fastethernet 0/2
SUR_1(config-if)#switchport mode trunk
SUR_1(config-if)#switchport Access vlan 10
SUR_1(config)#interface fastethernet 0/3
SUR_1(config-if)#switchport mode trunk
SUR_1(config-if)#switchport Access vlan 20
SUR_1(config)#interface fastethernet 0/4
SUR_1(config-if)#switchport mode trunk
SUR_1(config-if)#switchport Access vlan 30
SUR_1(config-if)#^Z
```

```
SUR_1#copy running-config  startup-config
```

Building configuration…
[OK]

- **CUARTO PASO**

Verifica si los puertos fueron asignados en sus respectivas vlans
SUR_1#show vlan

Vlan	Name	Status	Ports
1	defaul	active	Fa0/1, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/5 Fa0/12
10	gerencia	active	Fa0/2
20	contabilidad	active	Fa0/3
30	sistemas	active	Fa0/4
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

3.27.4. ROUTER SUR

NOTA: Una ves realisados las vlans en el switch nos tocara configurar las subinterfas en el router donde especifica en el router cuales seran las subinterfas y en que vlan seran asignadas. En el puerto que viajan las vlan hacia al router es **802.1Q**

- **Primer Paso**

  - ✓ En el router tendremos que configurar las subinterfas con sus respectivas vlans; con la finalidad para que se puedan comunicarse una vlan con otra.

```
SUR#configure Terminal
SUR(config)#interface fastethernet 0/0.1
SUR(config-subif)#ip address   192.168.1.17   255.255.255.240
SUR(config-subif)#no shutdown
SUR(config-subif)#encasuplation dot1q  10
SUR(config-subif)#exit
SUR(config)#interface fastethernet 0/0.2
SUR(config-subif)#ip address   192.168.1.25   255.255.255.240
SUR(config-subif)#no shutdown
SUR(config-subif)#encasuplation dot1q  20
SUR(config-subif)#exit
SUR(config)#interface fastethernet 0/0.3
SUR(config-subif)#ip address   192.168.1.33  255.255.255.240
```

```
SUR(config-subif)#no shutdown
SUR(config-subif)#encasuplation dot1q  30
SUR(config-subif)#exit
SUR(config)#interface fastethernet 0/0.4
SUR(config-subif)#ip address   192.168.1.41   255.255.255.240
SUR(config-subif)#no shutdown
SUR(config-subif)#encasuplation dot1q  40
SUR(config-subif)#^Z
```

HOST

Una vez configurados los Switch y el router nos tocaran configurar las maquinas d cada usuario donde asignaremos la IP y el Gateway por donde pasara la comunicación

HOST DPTO. GERENCIA

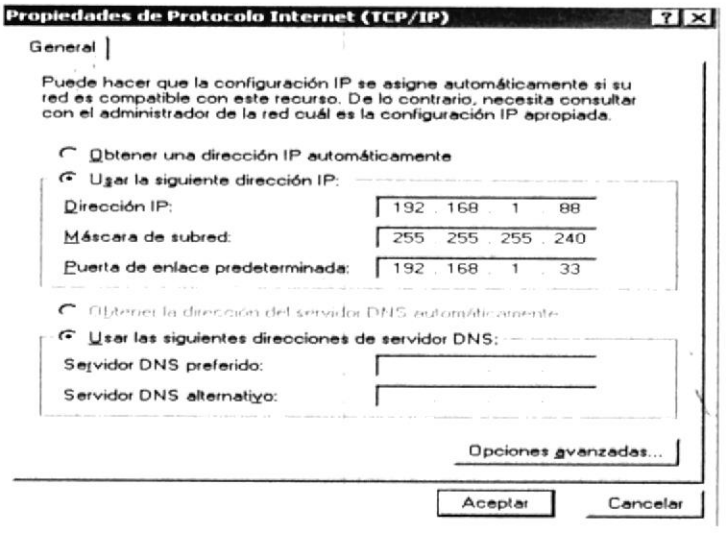


Figura 3-39.Gerencia

HOST DPTO. CONTABILIDAD

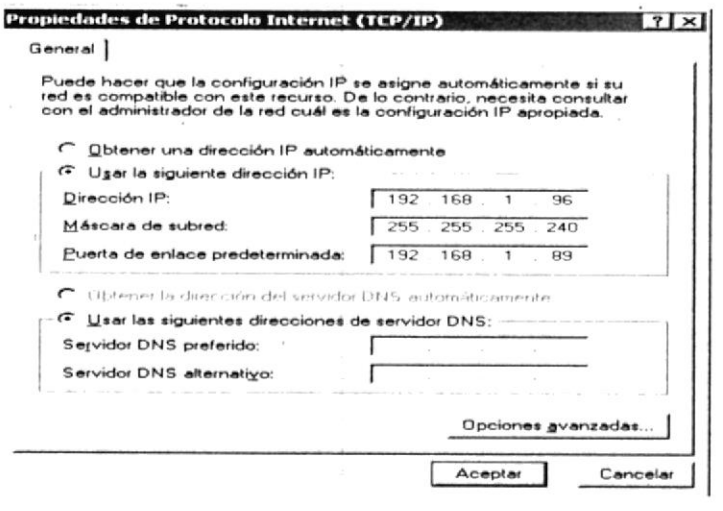


Figura 3-40.Gerencia

HOST DPTO. SISTEMAS

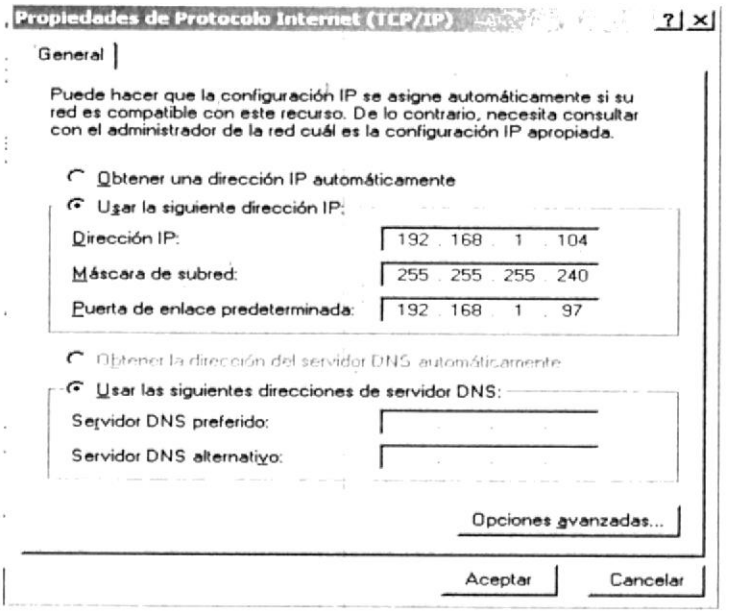


Figura 3-41.Sistemas

CAPÍTULO 4

NORMAS

4.1 NORMATIVAS DE CABLEADO ESTRUCTURADO

4.1.1 NORMAS PARA BACKBONE HORIZONTAL

4.1.1.1 NORMA 1 (CONSULTATIVA)

Cuando existe proximidad en las instalaciones de CE (Cableado estructurado) vs. Equipos eléctricos debe considerarse protección metálica.

4.1.1.2 NORMA 2 (OBLIGATORIA)

Todos los sistemas de cableado deben tener terminación a tierra.

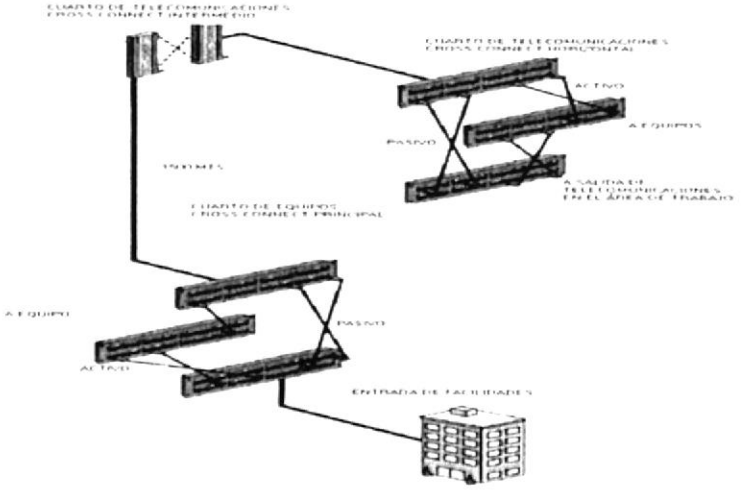


Figura 4-1 Norma 2

4.1.1.3 NORMA 3 (OBLIGATORIA)

Deberá mantenerse una separación mínima de 50 milímetros (5 cm.) entre el cableado par trenzado sin blindaje y los circuitos derivados menores a 3 KBA usados generalmente en toma eléctrica e interruptora de iluminación.

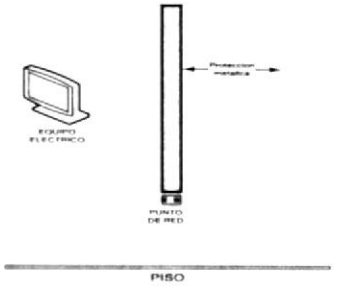


Figura 4-2 Norma 3

4.1.1.4 NORMA 4 (OBLIGATORIA)

Los circuitos de energía mayor o igual a 3 KBA y menor a 6 KBA deberá tener una separación mínima de 1.5 metros del cableado utp, 0.6 metros en cableado blindado y 3 metros en cross conect utp.

4.1.1.5 NORMA 5 (OBLIGATORIA)

Para sistemas eléctricos mayores o iguales a 6 KBA debe haber una separación mínima de 3 metros para cableado utp, 6 metros en cross conect utp y 1 metro en medios blindados.

4.1.1.6 NORMA 6 (CONSULTATIVA)

El Cableado horizontal deberá estar configurado como una topología estrella. La salida del distribuidor debe estar conectada a un cross conect en cada piso.

Figura 4-3 Norma 6

NORMA 7 (OBLIGATORIA)

Todo piso debe tener como mínimo un cuarto de comunicaciones

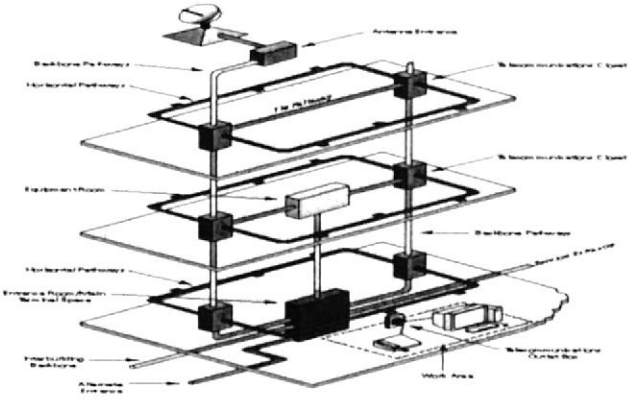


Figura 4-4 Norma 7

4.1.1.7 NORMA 8 (OBLIGATORIA)

Cada área de trabajo deberá ser atendida por un HC/FD localizado en el mismo piso o en un piso adyacente

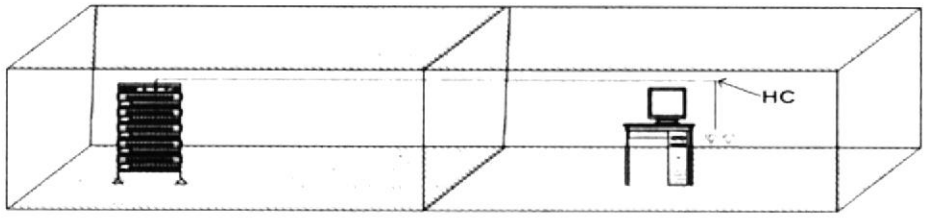


Figura 4-5 Norma 8

4.1.1.8 NORMA 9 (CONSULTATIVA)

El área que puede atenderse efectivamente por el cuarto de telecomunicaciones abarcará un área de 60 metros.

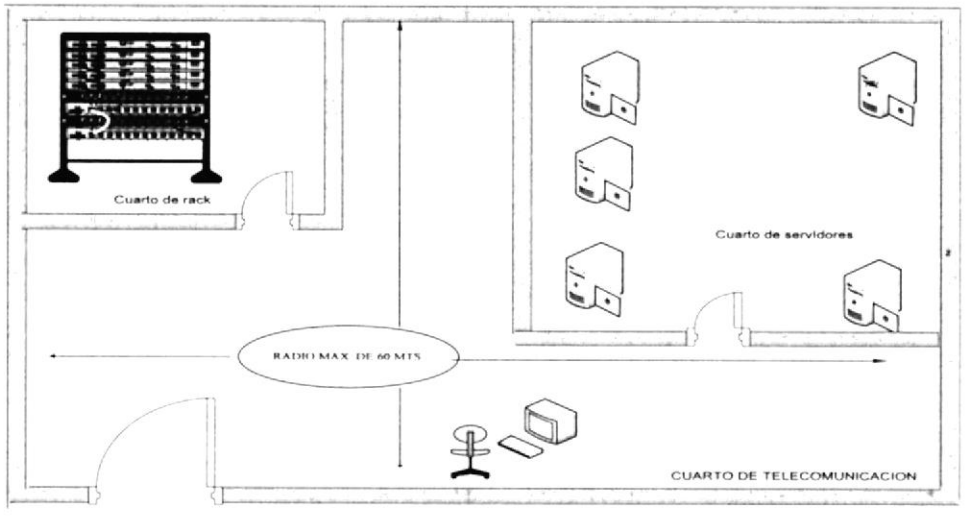


Figura 4-6 Norma 9

4.1.1.9 NORMA 10 (CONSULTATIVA)

No se usara cableado de bajo alfombra con producto Siemon

4.1.1.10 NORMA 11 (OBLIGATORIA)

No se permite el uso de derivaciones punteadas en el cableado horizontal

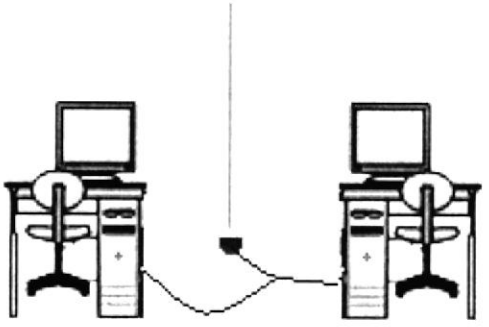


Figura 4-7 Norma 11

4.1.1.11 NORMA 12 (OBLIGATORIA)

No se recomienda más de 2 empalmes de fibra en el cableado horizontal.

4.1.1.12 NORMA 13 (OBLIGATORIA)

No se utilizara empalmes para par trenzado en el cableado

4.1.1.13 NORMA 14 (CONSULTATIVA)

No se recomienda más de 1 empalme de cable utp en el cableado horizontal

4.1.1.14 NORMA 15 (OBLIGATORIA)

La longitud del cable entre la salida de telecomunicaciones y la caja de terminaciones no excederá los 90 metros independiente del medio.

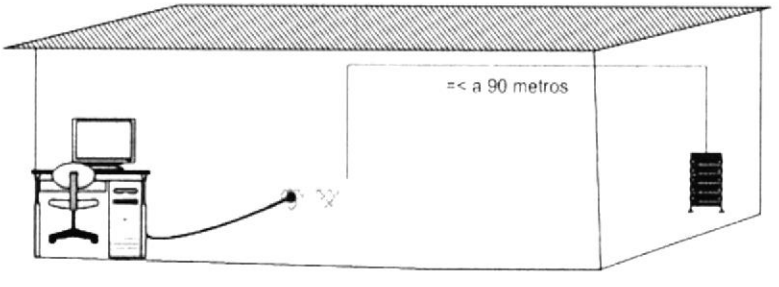


Figura 4-8 Norma 15

4.1.1.15 NORMA 16 (CONSULTATIVA)

Se recomienda un mínimo de 15 metros entre el distribuidor y la caja de terminación.

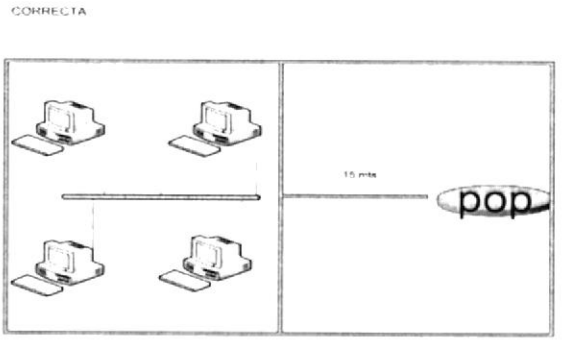


Figura 4-9 Norma 16

4.1.1.16 NORMA 17 (CONSULTATIVA)

La longitud individual o combinada de los patch cord no excederá los 5 metros ya sea en par trenzado o fibra.

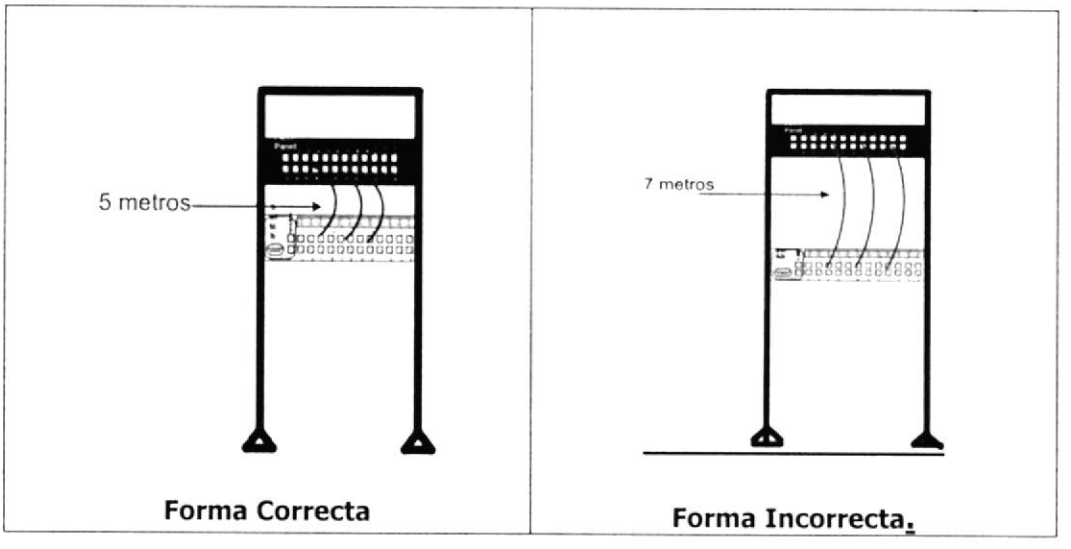


Figura 4-10 Norma 17

4.1.1.17 NORMA 18 (OBLIGATORIA)

La longitud del canal de cableado horizontal incluyendo los patch cord en ambos extremos y opcionalmente un patch cord no excederá los 100 metros independiente del medio.

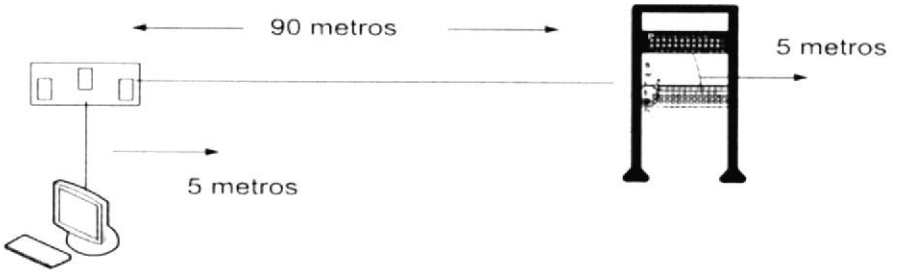


Figura 4-11 Norma 18

4.1.1.18 NORMA 19 (OBLIGATORIA)

Los soportes y canalizaciones de cableado se instalaran con medios estructuralmente independientes al techo falso y sus soportes.

4.1.1.19 NORMA 20 (OBLIGATORIA)

En áreas cubiertas por techos falsos/pisos falsos se usaran rutas definidas para el cable de telecomunicaciones.

4.1.1.20 NORMA 21 (OBLIGATORIA)

Deberá proveerse de un mínimo de 2 salidas (conectores) por cada área de trabajo individual.
La mínima categoría de cable requerido para datos es 6
La mínima categoría de cable requerido para voz es 5E

4.1.1.21 NORMA 22 (OBLIGATORIA)

La longitud del canal del cableado de fibra óptica multimodo no excederá los 300 metros cuando se usan interconexiones o empalmes en una topología de cableado centralizados de fibra óptica.

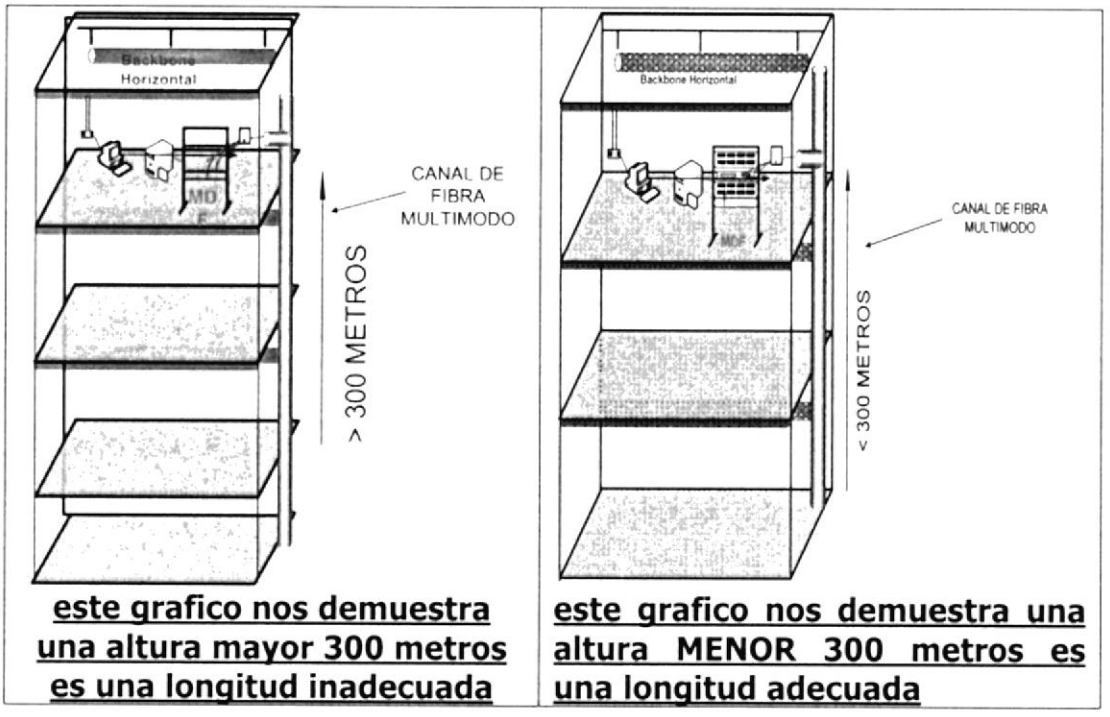


Figura 4-12 Norma 22

4.1.1.22 NORMA 23 (CONSULTATIVA)

Los cableados horizontales no se obstaculizaran por: calefacción, ventilación, aire acondicionado, distribución de energía eléctrica, estructura del edificio.

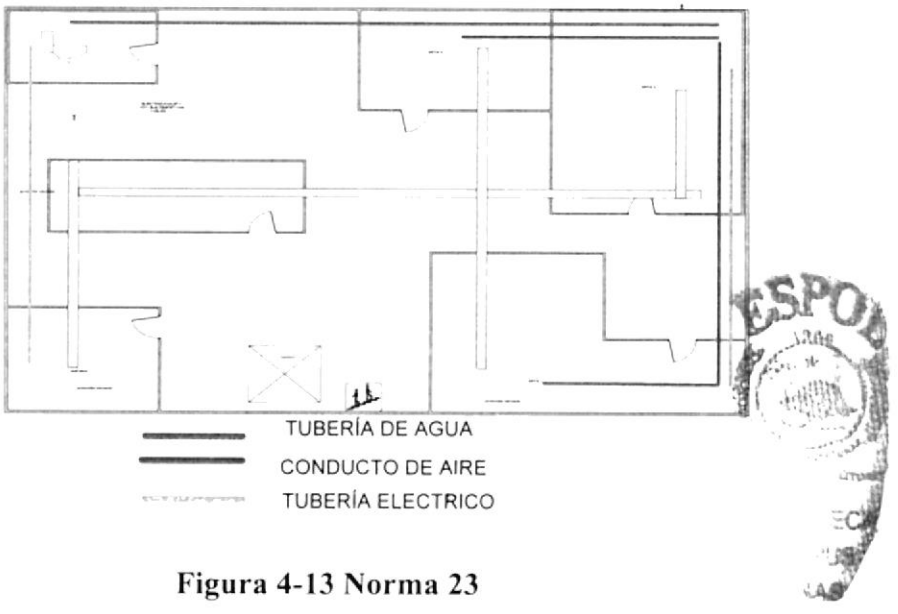


Figura 4-13 Norma 23

4.1.1.23 NORMA 24 (CONSULTATIVA)

Todas las canalizaciones utilizadas por el cableado de telecomunicaciones, estarán dedicadas a su uso exclusivo y no serán compartidas por otros servicios del edificio.

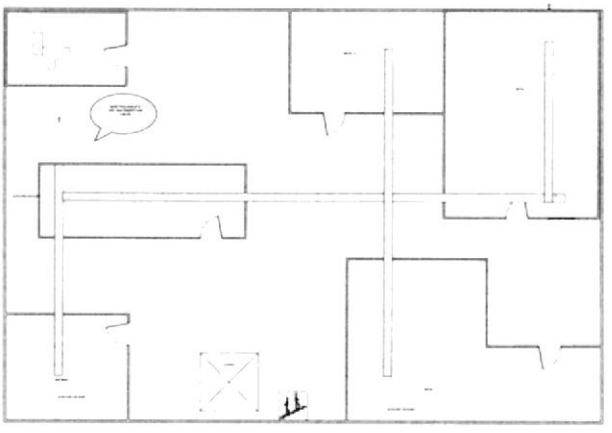


Figura 4-14 Norma 24

4.1.2 NORMAS PARA BACKBONE VERTICAL

4.1.2.1 NORMA 1 (OBLIGATORIA)

El backbone usará una topología estrella jerárquica

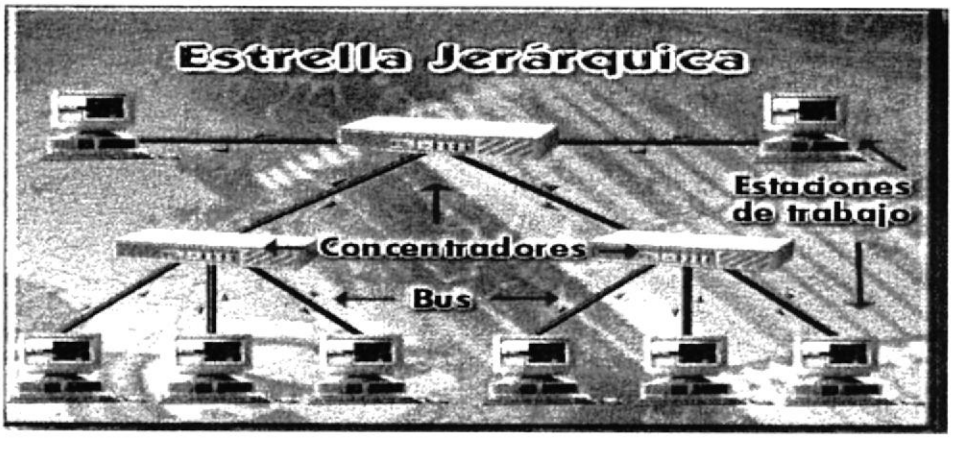


Figura 4-15 Norma 1

4.1.2.2 NORMA 2 (OBLIGATORIA)

No habrá más de 2 subsistemas en el backbone vertical.

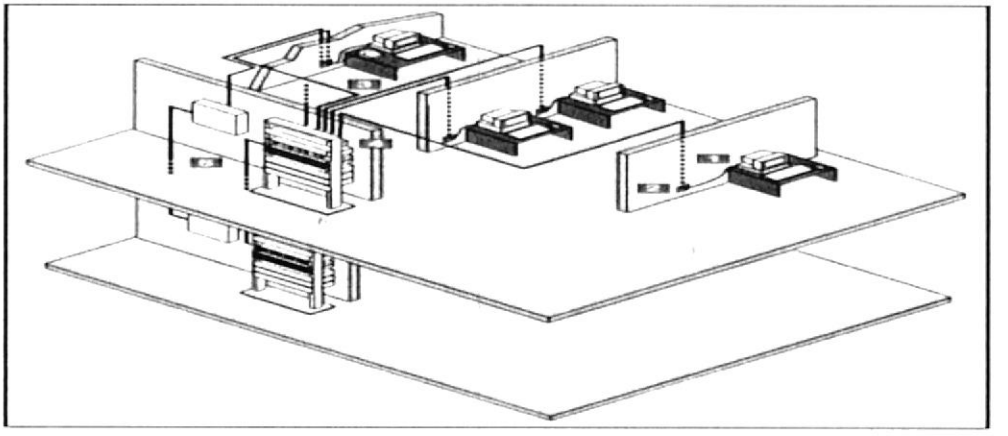


Figura 4-16 Norma 2

4.1.2.3 NORMA 3 (OBLIGATORIA)

No se permitirá el uso de derivaciones en el backbone.

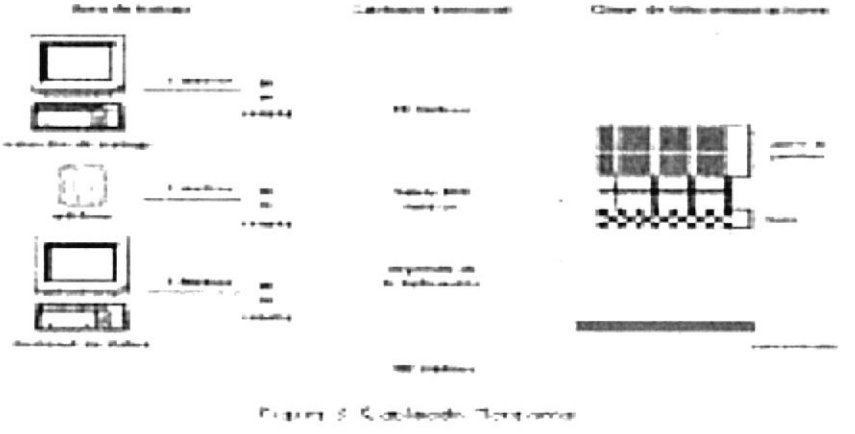


Figura 4-17 Norma 3

4.1.2.4 NORMA 4 (OBLIGATORIA)

Solo se permitirá un empalme en fibra óptica.

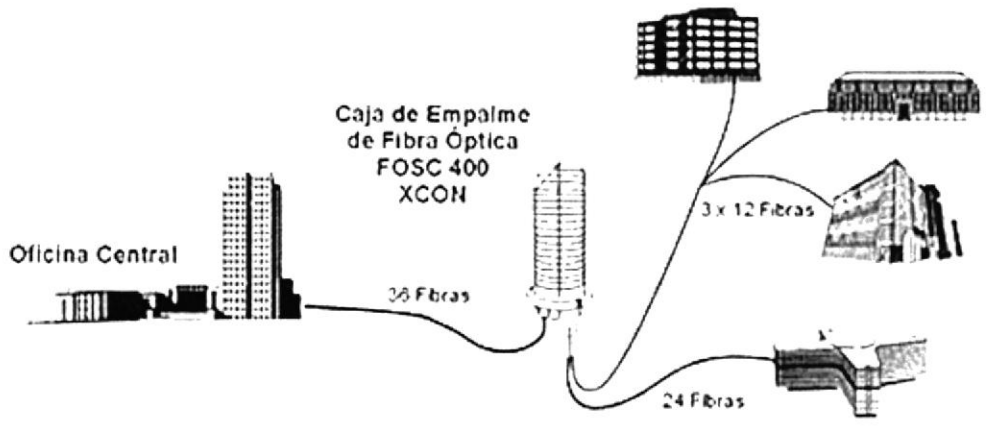


Figura 4-18 Norma 4

4.1.2.5 NORMA 5 (OBLIGATORIA)

No se usara empalmes en cables SCTP FTP y UTP.

4.1.2.6 NORMA 6 (OBLIGATORIA)

Los cables multipar en el backbone tienen como finalidad soportar aplicaciones de voz únicamente.

4.1.2.7 NORMA 7 (OBLIGATORIA)

Cada tendido de backbone mayor a 90 metros debe instalarse con fibra.

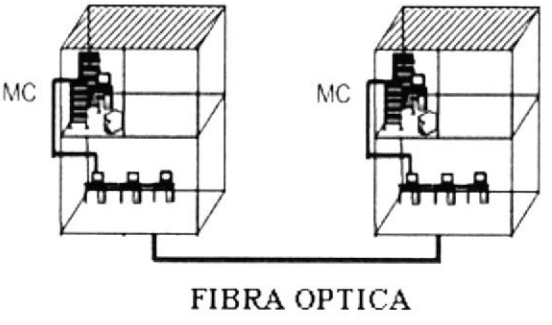


Figura 4-19 Norma 7

4.1.2.8 NORMA 8 (OBLIGATORIA)

Las canalizaciones de backbone deberán cumplir los reglamentos eléctricos y de construcción.

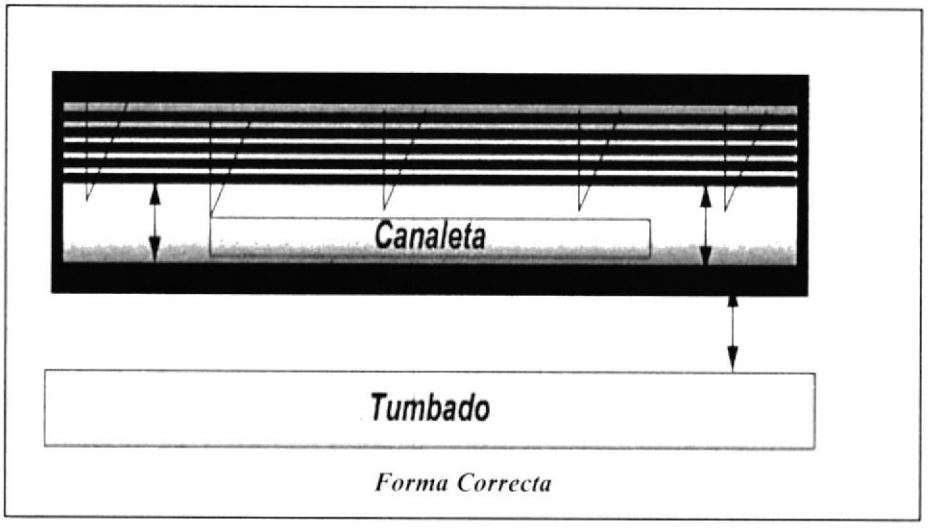


Figura 4-20 Norma 8

NORMA 9 (OBLIGATORIA)

Las canalizaciones del backbone deberán respetar el radio mínimo de curvatura dentro de las especificaciones del fabricante.

Figura 4-21 Norma 9

4.1.2.9 NORMA 10 (OBLIGATORIA)

Las canalizaciones del edificio se deben configurar como topología tipo estrella.

4.1.2.10 NORMA 11 (OBLIGATORIA)

Las canalizaciones no se usaran en ductos de ascensores.

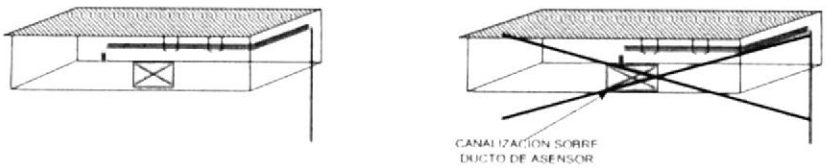
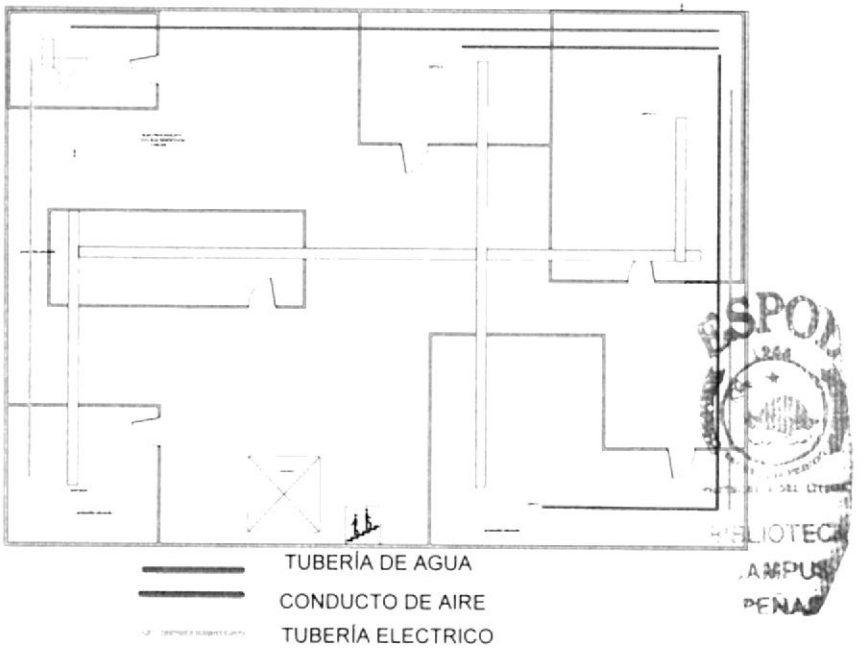


Figura 4-21 Norma 9

NORMA 12 (OBLIGATORIA)

Las canalizaciones deben ser apropiadas y no obstaculizaran su paso por ductos de calefacción, ventilación, aire acondicionado, distribución de energía o estructura de edificio.



Forma Correcta

Figura 4-22 Norma 12

4.1.2.11 NORMA 13 (CONSULTATIVA)

Para cable de backbone se recomienda un mínimo de 3 metros de reserva en cada extremo.

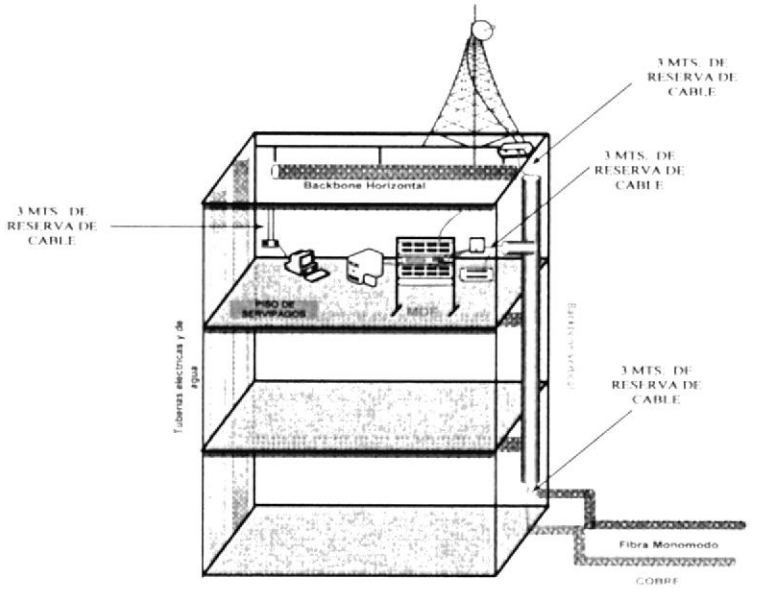


Figura 4-23 Norma 13

4.1.2.12 NORMA 14 (CONSULTATIVA)

Se recomienda como mínimo 2 hilos de fibra óptica para cada aplicación conocida durante su periodo de planificación y debe preverse un factor de crecimiento del 100 %

Voz	2	2 hilos para voz de datos
Video	2	Mínimo fibra de 12 hilos
Lan	2	Desde un mismo cable utp de 8 hilos sacar 2 conectores
Crecimiento	6	Cable utp <90mts; >90 fibra óptica
TOTAL	12	

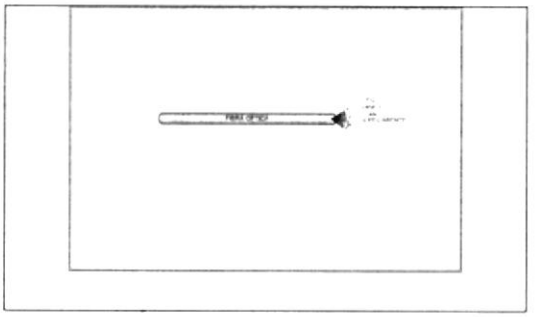


Figura 4-24 Norma 14

4.1.2.13 NORMA 15 (OBLIGATORIA)

Para la comunicación del backbone de campus debe instalarse fibra óptica para el soporte de aplicaciones de datos.

4.1.2.14 NORMAS PARA ÁREA DE TRABAJO

4.1.2.15 NORMA 1 (CONSULTATIVA)

El cable que corre entre el cuarto de telecomunicaciones y la salida de telecomunicaciones no estará expuesto en área de trabajo u otros espacios de acceso público.

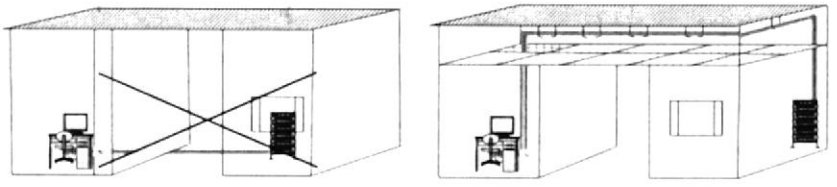


Figura 4-25 Norma 1

4.1.2.16 NORMA 2 (CONSULTATIVA)

Debe cumplir de manera obligatoria todos los reglamentos eléctricos y normas aplicables.

4.1.2.17 NORMA 3 (OBLIGATORIA)

Se usarán los medios apropiados para manejo, enrutado y eliminación de stress del cable tales como bandeja, amarras y los cinturones de cable.

4.1.2.18 NORMA 4 (OBLIGATORIA)

Las terminaciones fijas de cable de backbone y horizontales no se usarán para cambios rutinarios al sistema de cableado, para estos cambios se utilizarán cordones de parcheo y de equipos o sea Pacth Cord.

4.1.2.19 NORMA 5 (OBLIGATORIA)

El cuarto de telecomunicaciones estará dedicado a la función de telecomunicaciones. El acceso al cuarto de telecomunicaciones se restringirá al personal se servicio autorizado y no será compartido por servicios del edificio o se utilizaran para servicios de mantenimientos del edificio.

Figura 4-26 Norma 5

4.1.2.20 NORMA 6 (OBLIGATORIA)

Las cajas de gabinetes usados como espacio físico alternativo, cumplirán los requisitos de separación tendrán una puerta provista de cerradura y se montara en una ubicación fija.

Figura 4-27 Norma 6

4.1.2.21 NORMA 7 (CONSULTATIVA)

Se debe colocar tomas auxiliares cada 1.8 metros alrededor del perímetro del cuarto de telecomunicaciones.

4.1.2.22 NORMA 8 (OBLIGATORIA)

Las instalaciones de energía deben tener puestas y unidas a tierra.

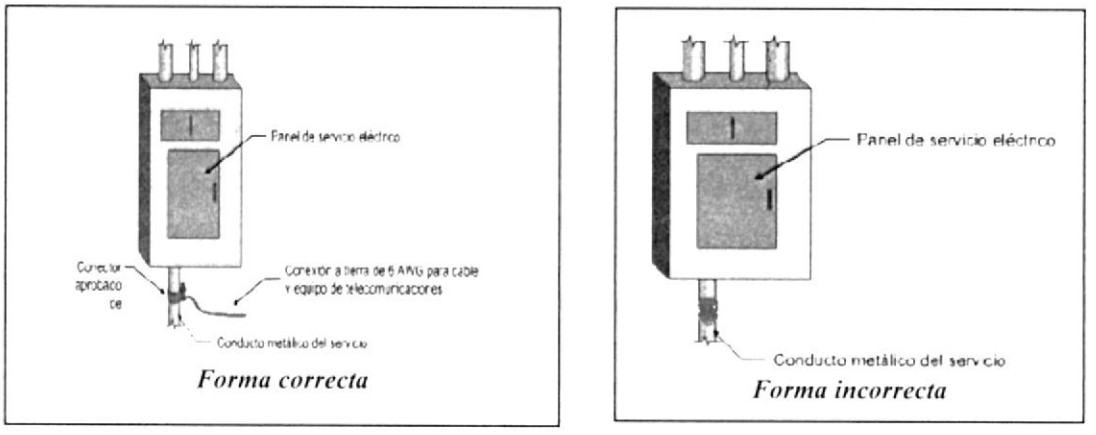


Figura 4-28 Norma 8

4.1.2.23 NORMA 9 (OBLIGATORIA)

Las acometidas (datos, voz, energía) deben estar en un área seca no expuesta a inundaciones.

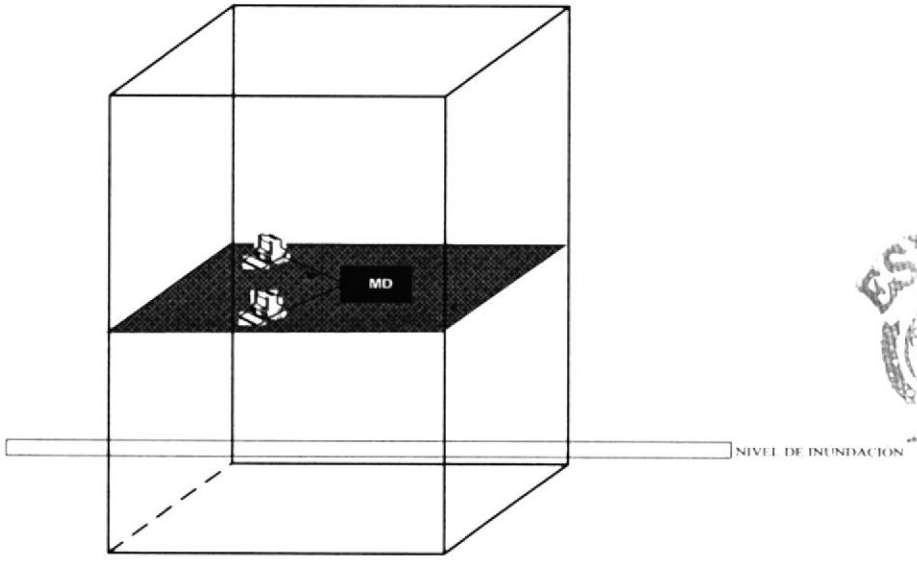


Figura 4-29 Norma 9

4.1.2.24 NORMA 10 (OBLIGATORIA)

El cableado a instalar debe estar rotulado y documentado que permita el código de colores en forma consistente como requisito de administración.

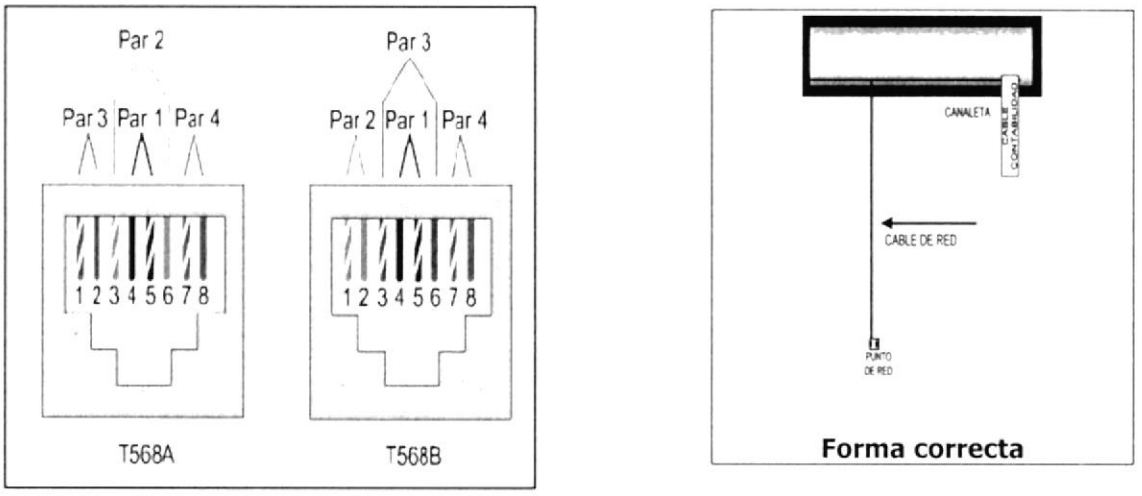


Figura 4-30 Norma 10

4.1.2.25 NORMA 11 (OBLIGATORIA)

La instalación de gabinetes y racks deben proporcionar separaciones que no sean menores a un metro donde el acceso para servicio sea requerido.

Figura 4-31 Norma 11

4.1.2.26 NORMA 12 (OBLIGATORIA)

Las canalizaciones tipo bandeja o canal no excederá una capacidad máxima del 50% de llenado y altura máxima interior de 150mm.

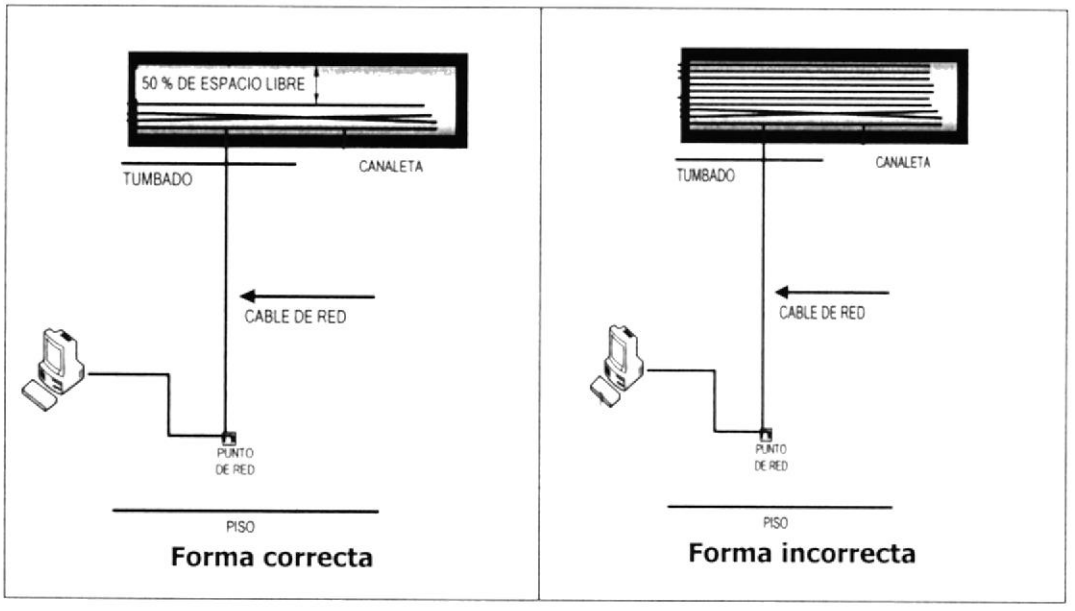


Figura 4-32 Norma 12

4.1.2.27 NORMA 13 (CONSULTATIVA)

Cuando se agrupen y amarren cables tengan cuidado que no queden sobre apretadas.

4.1.2.28 NORMA 14 (OBLIGATORIA)

Los cables del backbone horizontal y vertical deberán rotularse en cada extremo la etiqueta se marcará con su identificación dentro de los 30cm del extremo del cable.

Figura 4-33 Norma 14

4.1.2.29 NORMA 15 (OBLIGATORIA)

Los registros del cable deberán incluir al menos la siguiente información:

1. Identificador del cable
2. Tipo del cable
3. Pares o conductores dañados
4. referencias de registros de posiciones del hardware de conexión.
5. referencias de empalmes.

Descripción	Identificación
Cable n°7 Multimodo	FOM007
Cable N°5 de UTP cat. 5E	C5005

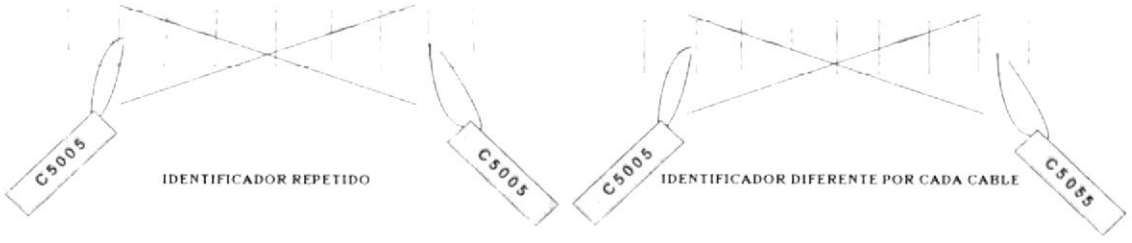


Figura 4-34 Norma 15

4.1.2.30 NORMA 16 (OBLIGATORIA)

- *HARDWARE DE CONEXIÓN*

A cada pieza y a cada hardware de conexión se le asignará un identificador único que será de referencia en sus registros respectivos.

4.1.2.31 NORMA 17 (OBLIGATORIA)

- *ROTULADO DE HARDWARE DE CONEXION*

Un identificador único deberá rotularse en la cubierta de cada pieza y de cada posición de hardware de conexión.

4.1.2.32 NORMA 18 (OBLIGATORIA)

- *REGISTRO DE HARDWARE DE CONEXION*

El registro del hardware de conexión deberá incluir al menos la siguiente información:

1. Identificador de la pieza/posición del hardware de conexión.
2. Tipo de la pieza/posición del hardware de conexión.
3. Posiciones dañadas.
4. referencias de registros de cable

4.1.2.33 NORMA 19 (OBLIGATORIA)

- *ROTULADO E IDENTIFICACION DE EMPALMES*

Un identificador único deberá asignarse y rotularse en cada empalme como referencia en sus registros.

4.1.2.34 NORMA 20 (OBLIGATORIA)

El registro de empalme debe tener:

1. Identificador de empalme.
2. Tipo de empalme.
3. Referencia de registro del cable.

4.1.2.35 NORMA 21 (OBLIGATORIA)

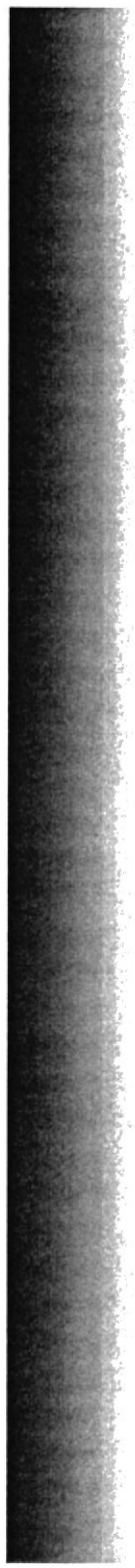
El integrador deberá conservar y guardar un archivo de diseño y planos de la infraestructura del sistema de cableado. Estos planos y dibujos deben tener lo siguiente:

1. Localización de las terminaciones de cableado horizontal.
2. Localización de las salidas de telecomunicaciones.
3. Localización de terminaciones de cables del backbone.
4. Localización de las canalizaciones.
5. Localización de los cuartos de telecomunicaciones.
6. Diagrama del backbone lógico.

4.1.2.36 NORMA 22 (OBLIGATORIA)

- *ORDENES DE TRABAJO*

Se deben mantener un archivo (Bitácora) y debe actualizarse para efectos de cambios y reparaciones.



CAPÍTULO 5

SOLUCIÓN PROPUESTA

5.1 PROBLEMA - CAUSA – EFECTO

PROBLEMA	CAUSA	EFECTO
No poseen normas de cableado estructurado en la red Lan	▪ Falta de conocimiento por parte del departamento técnico. ▪ Descuido por parte de la empresa.(Directivos).	▪ Dificultad al momento de solucionar un problema en la red.(cables) ▪ No cuentan con protección ante siniestros.
Saturación en su red LAN	▪ No hay redes segmentadas. ▪ Mala administración por parte del encargado de la red	▪ Colisión al momento de acceder a los recursos de la red, forzando el reenvió de paquetes.
No existe un Respaldo para la comunicación WAN	• Falta de equipos de Respaldo para la comunicación WAN	• Si el ISP fallara no se podría realizar operaciones en Línea.
Existen Switch capa 2	• Factor económico	• Las IP son tomadas al azar no existe una Administración en lo que es la red
El rack de Matriz esta dentro del Dpto. Sistemas	• Por espacio Físico y Mala Planificación de la construcción	• No existe seguridad para los equipos que se encuentran en el rack.

Tabla 5.1 Problema Causa Efecto

5.2 PROBLEMA – SOLUCIÓN

PROBLEMA	SOLUCIÓN	ALCANCE
No existe segmentación	▪ Segmentar por departamentos los edificios de Matriz y sucursales.	Poseer una buena segmentación para una buena administración de la red.
No poseen normas de cableado estructurado en la red Lan	Realizar un nuevo cableado estructurado conforme a las normas para categoría 6.	Para tener un cableado Estructurado catalizada y que cumpla con las normas de seguridades respectivas.
Saturación en su red LAN	▪ Segmentar las redes por área de trabajo. ▪ Verificar las cascadas de los switches e implementar políticas de administración de la red.	Estos nos dará un mejor control de la red por áreas y nos evitara saturación en el envió de información y a la vez pondremos las políticas de administración.
No existe un Respaldo para la comunicación WAN	▪ Implementar una nueva infraestructura para respaldo.	En caso de falla con la comunicación Wan tener un respaldo para estar siempre operativo.
No existe ni un switch Administrable dentro de la Organización	▪ Adquirir un Switch de capa 3 Administrable para poder organizar por IP los departamentos a segmentar.	Poseer equipos de última tecnología para así detectar las fallas en las estaciones de trabajo en el caso de presentarse.
El rack de Matriz esta dentro del Dpto. Sistemas	▪ Creación de un cuarto independiente para el rack de Matriz.	Tener un cuarto independiente para el rack ya que así protegeríamos de manera más segura el equipo.

Tabla 5.2 Problema Solución

5.3 ESTUDIO DE FACTIBILIDAD

5.3.1 ESTUDIO DE LA ALTERNATIVA "A"

Esta alternativa está orientada a mejorar los tiempos de respuestas en la red, brindar mayor ancho de banda; medios de respaldos para mantener una comunicación segura.

5.3.2 FACTIBILIDAD TÉCNICA

En esta factibilidad estamos detallando los dispositivo y equipos que se van adquirir para la empresa.

CANT	DESCRIPCIÓN	UBICACIÓN	EDIFICIO	GRÁFICO
1	Switch	Sistema	Urbanis	
1	Switch	Sistema	Mall del sur	
1	Switch	Sistema	Mall Outlet	
1	Firewall	sistemas	Urbanis	

Tabla 5.3 Factibilidad Técnica

5.3.3 FACTIBILIDAD ECONÓMICA

5.3.3.1 COSTOS EQUIPOS

En este cuadro se muestra los valores de cuanto van a costar los materiales que se adquirirán.

Costos de equipos			
Cant.	**Descripción**	**costo unitario**	**costo total**
1	SWITCH D-LINK DES-3526	$ 350	$ 350
1	FIREWALL D- LINK DFL - 800	$1859	$840
Total implemento			**$1190**

Tabla 5.4 Costos Equipos

5.3.3.2 COSTO DEL ENLACE

Costo del Enlace			
Tipo de Enlace	**distancia**	**costo mensual**	**costo total**
Ultima milla	10 km	1790.88	1958.88
Total			1958.88

Tabla 5.4 Costos Enlaces

5.3.4 FACTIBILIDAD OPERATIVA

FASES	CANTIDAD PERSONAL	SEMANAS	COSTOS POR PERSONAL SEMANAL	COSTO TOTAL	COSTO FASE
Fase de diseño de la red Wan	1 Ing. en telecomunicación	2 días	$ 40.33 por día	$ 80.66	
COSTO FASE					$ 80.66
Fase de implementación Wan	1 Adm. red	7 días	$ 30 por día	$ 210	
	1 Ing. en Telecomunicación	3 días	$40,33 por día	$ 120.99	
	2 Asistentes redes	7 días	$ 25 por día	$ 350	
COSTO FASE					$680.99
Fase de prueba Wan	1 Adm. red	1 semana 4 días	$30 por día	$ 330	
	1 Ing. en Telecomunicación	2 días	$40,33 por día	$ 80.66	
	2 Asistentes de Redes	1 semana 4 días	$25 por día	$ 550	
COSTO FASE					$ 960.66
Fase de documentación Wan	1 Adm. red	10 días	$ 30	$ 300	
	1 Ing. en Telecomunicación	2 días	$ 40,33	$ 80.66	
COSTO FASE					$ 380.66
TOTAL DEL COSTO OPERATIVO					$ 2102.97

Tabla 5.5 Factibilidad Operativa

5.3.5 DETALLE DE LA FASE DE ANÁLISIS LAN Y WAN

En la fase de análisis se detalla el estudio realizado de la empresa GRUPO ROMERO con el objetivo de verificar los problemas actuales que tienen la empresa tanto a nivel LAN como WAN, para darle solución a los problemas encontrados.
Las personas que intervienen en esta fase que durará 2 semanas serán un Ingeniero en Telecomunicación y un Administrador de Red.

FASES	SEMANA	TOTAL SEMANA
FASE DE ANÁLISIS DE LA RED LAN Y WAN		
1 Ing. en Telecomunicación	2 semanas	
1 Adm. de Red	2 semanas	
semana por fase		2 semanas
FASE DE DISEÑO DE LA RED WAN		
1 Adm. Red	2 semanas	
1 Ing. en Telecomunicación	1 semana	
1 Asistente de red	2 semanas	
semanas por fase		2 semana
FASE DE IMPLEMENTACIÓN WAN		
1 Adm. Red	2 semanas	
1 Ing. en Telecomunicación	3 días	
2 Asistentes de redes	1 semana 3 días	
semanas por fase		2 semanas
FASE DE LA PRUEBA DE LA RED WAN		
1 Adm. Red	1 semana 4 días	
2 Asistentes de redes	1 semana 2 días	
1 Ing. en Telecomunicación	2 días	
semanas por fase		1 semana 4 días
FASE DE DOCUMENTACIÓN WAN		
1 Adm. Redes	7 días	
1 Ing. en Telecomunicación	2 días	
semanas por fase		7 días
TOTAL DE SEMANAS		8 Semanas 5 días

Tabla 5.6 Fase De Análisis

5.3.6 COSTO TOTAL DE LA PROPUESTA

COSTO TOTAL FACTIBILIDAD ECONÓMICA	
Costo de Equipos	**1190**
Costo del enlace	**1958.88**
Costo Operativo	**2102.97**
SUB TOTAL DE LA PROPUESTA A	**$5,833.97**
Costo total de la factibilidad Económica	**$7889.13**

Tabla 5.7 Costo Total

5.3.7 VENTAJAS & BENEFICIO

5.3.7.1 VENTAJAS

- Los envíos de paquetes de datos sucursal y matriz serán más rápidos.
- Gracias a este proyecto Todas las sucursales no tendrán pérdidas de Enlaces.

5.3.7.2 BENEFICIO

- La empresa tendrá una imagen más eficaz y eficiente.
- Los clientes de Grupo Romero contarán con un servicio rápido y mejorado sin demora alguna.

5.3.8 FORMA DE PAGO

A continuación se detallará la forma de pago de la alternativa

Esta propuesta esta sujeto a los estudios realizados de la empresa de existir un cambio se le comunicará con anticipación, de aceptar este propuesta se deberá enviar.

60% de la aceptación de la propuesta (al inicio de la primera fase)

40% del costo total al finalizar el contrato

El cliente se compromete a proveer la instalación y dar las facilidades respectivas para realizar el trabajo en el tiempo estimado, caso contrario, el sueldo por los días adicionales del personal involucrado, será cancelado por parte de dicha empresa.

5.3.9 GARANTÍA

La garantía que ofrecemos será el soporte técnico que brindaremos, una vez terminado el proyecto que se realizará a la Empresa, nuestro tiempo de duración será por 3 meses sin costo alguno, durante los 3 meses si se llega a efectuar un problema ustedes podrán contar con nuestros técnicos directamente.

Pasado de los 3 meses se pierde la garantía, si ustedes desean podrán renovar un contrato de 3 meses o más, para que ustedes cuenten con nuestros servicios.

El valor por renovar el contrato tendrá un costo adicional.

Las garantías de equipos y dispositivos los brindarán los proveedores con los cuales estamos trabajando ().

CAPÍTULO 6

SEGURIDADES

6.1 QUE ES UN FIREWALL

Un firewall es un sistema que protege a un ordenador o a una red de ordenadores contra intrusiones provenientes de redes de terceros (generalmente desde Internet). Un sistema de firewall filtra paquetes de datos que se intercambian a través de Internet Por lo tanto, se trata de una pasarela de filtrado que comprende al menos las siguientes interfaces de red:

- ✓ una interfaz para la red protegida (red interna)
- ✓ una interfaz para la red externa.

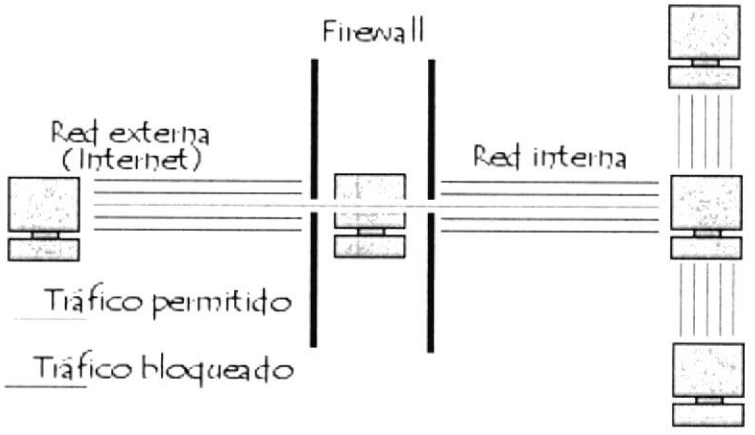


Figura 6-1 Esquema De Firewall

El sistema firewall es un sistema de software, a menudo sustentado por un hardware de red dedicada, que actúa como intermediario entre la red local (u ordenador local) y una o más redes externas. Un sistema de firewall puede instalarse en ordenadores que utilicen cualquier sistema siempre y cuando:

- ✓ La máquina tenga capacidad suficiente como para procesar el tráfico
- ✓ El sistema sea seguro.
- ✓ No se ejecute ningún otro servicio más que el servicio de filtrado de paquetes en el servidor

6.1.1 COMO FUNCIONA UN SISTEMA FIREWALL

Un sistema firewall contiene un conjunto de reglas predeterminadas que le permiten al sistema:

- ✓ Autorizar la conexión (permitir)
- ✓ Bloquear la conexión (denegar)
- ✓ Rechazar el pedido de conexión sin informar al que lo envió (negar)

Todas estas reglas implementan un método de filtrado que depende de la política de seguridad adoptada por la organización. Las políticas de seguridad se dividen generalmente en dos tipos que permiten:

- ✓ la autorización de sólo aquellas comunicaciones que se autorizaron explícitamente: Todo lo que no se ha autorizado explícitamente está prohibido"
- ✓ el rechazo de intercambios que fueron prohibidos explícitamente

El primer método es sin duda el más seguro. Sin embargo, impone una definición precisa y restrictiva de las necesidades de comunicación.

6.1.2 BENEFICIOS DE UN FIREWALL EN INTERNET

6.1.2.1 PRIMER PUNTO

Los firewalls en Internet administran los accesos posibles del Internet a la red privada. Sin un firewall, cada uno de los servidores propios del sistema se expone al ataque de otros servidores en el Internet. Esto significa que la seguridad en la red privada depende de la "Dureza" con que cada uno de los servidores cuenta y es únicamente seguro tanto como la seguridad en la fragilidad posible del sistema.

El firewall permite al administrador de la red definir un "choke point" (envudo), manteniendo al margen los usuarios no-autorizados (tal, como., hackers, crakers, vándalos, y espías) fuera de la red, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques posibles. Uno de los beneficios clave de un firewall en Internet es que ayuda a simplificar los trabajos de administración, una vez que se consolida la seguridad en el sistema firewall, es mejor que distribuirla en cada uno de los servidores que integran nuestra red privada.

Figura 6-2 Esquema Del Sistema Firewall (Internet)

El firewall ofrece un punto donde la seguridad puede ser monitoreada y si aparece alguna actividad sospechosa, este generara una alarma ante la posibilidad de que ocurra un ataque, o suceda algún problema en el transito de los datos. Esto se podrá notar al acceder la organización al Internet, la pregunta general es "si" pero "cuando" ocurrirá el ataque.

Esto es extremadamente importante para que el administrador audite y lleve una bitácora del tráfico significativo a través del firewall. También, si el administrador de la red toma el tiempo para responder una alarma y examina regularmente los registros de base.

Esto es innecesario para el firewall, desde que el administrador de red desconoce si ha sido exitosamente atacado.

- ✓ Concentra la seguridad Centraliza los accesos

- ✓ Genera alarmas de seguridad Traduce direcciones (NAT)
- ✓ Monitorea y registra el uso de Servicios de WWW y FTP.
- ✓ Internet.

6.1.2.2 SEGUNDO PUNTO

Con el paso de algunos años, el Internet ha experimentado una crisis en las direcciones, logrando que el direccionamiento IP sea menos generoso en los recursos que proporciona.

Por este medio se organizan las compañías conectadas al Internet, debido a esto hoy no es posible obtener suficientes registros de direcciones IP para responder a la población de usuarios en demanda de los servicios.

Un firewall es un lugar lógico para desplegar un Traductor de Direcciones de Red (NAT) esto puede ayudar aliviando el espacio de direccionamiento acortando y eliminando lo necesario para re-enumerar cuando la organización cambie del Proveedor de Servicios de Internet (ISPs).
Un firewall de Internet es el punto perfecto para auditar o registrar el uso del Internet.

Esto permite al administrador de red justificar el gasto que implica la conexión al Internet, localizando con precisión los cuellos de botella potenciales del ancho de banda, y promueve el método de cargo a los departamentos dentro del modelo de finanzas de la organización.

Un firewall de Internet ofrece un punto de reunión para la organización. Si una de sus metas es proporcionar y entregar servicios información a consumidores, el firewall de Internet es ideal para desplegar servidores WWW y FTP.
Finalmente, el firewall puede presentar los problemas que genera un punto de falla simple. Enfatizando si este punto de falla se presenta en la conexión al Internet, aun así la red interna de la organización puede seguir operando - únicamente el acceso al Internet esta perdido - .

La preocupación principal del administrador de red, son los múltiples accesos al Internet, que se pueden registrar con un monitor y un firewall en cada punto de acceso que posee la organización hacia el Internet. Estos dos puntos de acceso significan dos puntos potenciales de ataque a la red interna que tendrán que ser monitoreados regularmente.

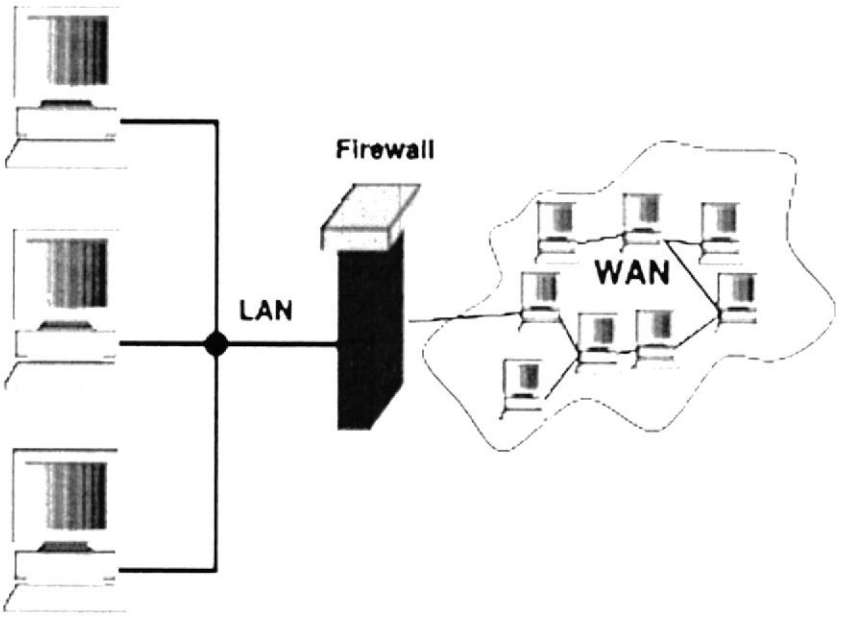


Figura 6-2 Esquema Del Sistema Firewall (Lan)

6.1.3 FILTRADOS DE FIREWALL

6.1.3.1 FILTRADO DE PAQUETES STATELESS

Un sistema de firewall opera según el principio del filtrado simple de paquetes, o filtrado de paquetes stateless. Analiza el encabezado de cada paquete de datos (data grama) que se ha intercambiado entre un ordenador de red interna y un ordenador externo.

Así, los paquetes de datos que se han intercambiado entre un ordenador con red externa y uno con red interna pasan por el firewall y contienen los siguientes encabezados, los cuales son analizados sistemáticamente por el firewall:

- ✓ La dirección IP del ordenador que envía los paquetes
- ✓ La dirección IP del ordenador que recibe los paquetes
- ✓ El tipo de paquete (TCP, UDP, etc.)
- ✓ El número de puerto (recordatorio: un puerto es un número asociado a un servicio o a una aplicación de red).

Las direcciones IP que los paquetes contienen permiten identificar el ordenador que envía los paquetes y el ordenador de destino, mientras que el tipo de paquete y el número de puerto indican el tipo de servicio que se utiliza.

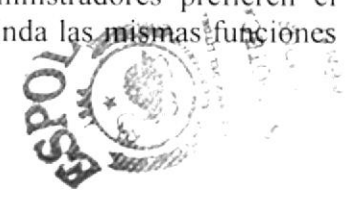
La siguiente tabla proporciona ejemplos de reglas del firewall:

Regla	Acción	IP fuente	IP destino	Protocolo	Puerto fuente	Puerto destino
1	Aceptar	192.168.10.20	194.154.192.3	TCP	cualquiera	25
2	Aceptar	cualquiera	192.168.10.3	TCP	cualquiera	80
3	Aceptar	192.168.10.0/24	cualquiera	TCP	cualquiera	80
4	Negar	cualquiera	cualquiera	cualquiera	cualquiera	cualquiera

Tabla 6-1 Reglas Del Firewall

Los puertos reconocidos (cuyos números van del 0 al 1023) están asociados con servicios ordinarios (por ejemplo, los puertos 25 y 110 están asociados con el correo electrónico y el puerto 80 con la Web). La mayoría de los dispositivos de firewall se configuran al menos para filtrar comunicaciones de acuerdo con el puerto que se usa. Normalmente, se recomienda bloquear todos los puertos que no son fundamentales (según la política de seguridad vigente).

Por ejemplo, el puerto 23 a menudo se bloquea en forma predeterminada mediante dispositivos de firewall, ya que corresponde al protocolo TELNET, el cual permite a una persona emular el acceso terminal a una máquina remota para ejecutar comandos a distancia. Los datos que se intercambian a través de TELNET no están codificados. Esto significa que es probable que un hacker observe la actividad de la red y robe cualquier contraseña que no esté codificada. Generalmente, los administradores prefieren el protocolo SSH, el cual tiene la reputación de ser seguro y brinda las mismas funciones que TELNET.



6.1.3.2 FILTRADO DINÁMICO

El Filtrado de paquetes Stateless sólo intenta examinar los paquetes IP independientemente, lo cual corresponde al nivel 3 del modelo OSI (Interconexión de sistemas abiertos). Sin embargo, la mayoría de las conexiones son admitidas por el protocolo TCP, el cual administra sesiones, para tener la seguridad de que todos los intercambios se lleven a cabo en forma correcta. Asimismo, muchos servicios (por ejemplo, FTP) inician una conexión en un puerto estático. Sin embargo, abren un puerto en forma dinámica (es decir, aleatoria) para establecer una sesión entre la máquina que actúa como servidor y la máquina cliente.

De esta manera, con un filtrado de paquetes stateless, es imposible prever cuáles puertos deberían autorizarse y cuáles deberían prohibirse Para solucionar este problema, el sistema de filtrado dinámico de paquetes se basa en la inspección de las capas 3 y 4 del modelo OSI, lo que permite controlar la totalidad de las transacciones entre el cliente y el servidor. El término que se usa para denominar este proceso es "inspección stateful" o "filtrado de paquetes stateful".

Un dispositivo de firewall con "inspección stateful" puede asegurar el control de los intercambios. Esto significa que toma en cuenta el estado de paquetes previos cuando se definen reglas de filtrado. De esta manera, desde el momento en que una máquina autorizada inicia una conexión con una máquina ubicada al otro lado del firewall, todos los paquetes que pasen por esta conexión serán aceptados implícitamente por el firewall.

El hecho de que el filtrado dinámico sea más efectivo que el filtrado básico de paquetes no implica que el primero protegerá el ordenador contra los hackers que se aprovechan de las vulnerabilidades de las aplicaciones. Aún así, estas vulnerabilidades representan la mayor parte de los riesgos de seguridad.

6.1.3.3 FILTRADO DE APLICACIONES

El filtrado de aplicaciones permite filtrar las comunicaciones de cada aplicación. El filtrado de aplicaciones opera en el nivel 7 (capa de aplicaciones) del modelo OSI, a diferencia del filtrado simple de paquetes (nivel 4). El filtrado de aplicaciones implica el conocimiento de los protocolos utilizados por cada aplicación.

Como su nombre lo indica, el filtrado de aplicaciones permite filtrar las comunicaciones de cada aplicación. El filtrado de aplicaciones implica el conocimiento de las aplicaciones en la red y un gran entendimiento de la forma en que en ésta se estructuran los datos intercambiados (puertos, etc.).

Un firewall que ejecuta un filtrado de aplicaciones se denomina generalmente "pasarela de aplicaciones" o ("proxy"), ya que actúa como relé entre dos redes mediante la intervención y la realización de una evaluación completa del contenido en los paquetes intercambiados. Por lo tanto, el proxy actúa como intermediario entre los ordenadores de la red interna y la red externa, y es el que recibe los ataques. Además, el filtrado de aplicaciones permite la destrucción de los encabezados que preceden los mensajes de aplicaciones, lo cual proporciona una mayor seguridad.

Este tipo de firewall es muy efectivo y, si se ejecuta correctamente, asegura una buena protección de la red. Por otra parte, el análisis detallado de los datos de la aplicación requiere una gran capacidad de procesamiento, lo que a menudo implica la ralentización de las comunicaciones, ya que cada paquete debe analizarse minuciosamente.

Además, el proxy debe interpretar una gran variedad de protocolos y conocer las vulnerabilidades relacionadas para ser efectivo.
Finalmente, un sistema como este podría tener vulnerabilidades debido a que interpreta pedidos que pasan a través de sus brechas. Por lo tanto, el firewall (dinámico o no) debería disociarse del proxy para reducir los riesgos de comprometer al sistema.

6.1.4 POLÍTICAS DEL FIREWALL.

Las posturas del sistema firewall describen la filosofía fundamental de la seguridad en la organización. Estas son dos posturas diametralmente opuestas que la política de un firewall de Internet puede tomar:

- ✓ "No todo lo específicamente permitido esta prohibido"
- ✓ "Ni todo lo específicamente prohibido esta permitido"

La primera postura asume que un firewall puede obstruir todo el tráfico y cada uno de los servicios o aplicaciones deseadas necesariamente para ser implementadas básicamente caso por caso.
Esta propuesta es recomendada únicamente a un limitado número de servicios soportados cuidadosamente seleccionados en un servidor. La desventaja es que el punto de vista de "seguridad" es más importante que - facilitar el uso - de los servicios y estas limitantes numeran las opciones disponibles para los usuarios de la comunidad. Esta

propuesta se basa en una filosofía conservadora donde se desconocen las causas acerca de los que tienen la habilidad para conocerlas.

La segunda postura asume que el firewall puede desplazar todo el tráfico y que cada servicio potencialmente peligroso necesitara ser aislado básicamente caso por caso. Esta propuesta crea ambientes más flexibles al disponer mas servicios para los usuarios de la comunidad. La desventaja de esta postura se basa en la importancia de "facilitar el uso" que la propia - seguridad - del sistema. También además, el administrador de la red esta en su lugar de incrementar la seguridad en el sistema conforme crece la red. Desigual a la primer propuesta, esta postura esta basada en la generalidad de conocer las causas acerca de los que no tienen la habilidad para conocerlas

6.1.5 POLÍTICA INTERNA DE LA SEGURIDAD

Tan discutidamente escuchada, un firewall de Internet no esta solo - es parte de la política de seguridad total en una organización -, la cual define todos los aspectos en competentes al perímetro de defensa. Para que esta sea exitosa, la organización debe de conocer que es lo se esta protegiendo. La política de seguridad se basara en una conducción cuidadosa analizando la seguridad, la asesoría en caso riesgo, y la situación del negocio. Si no se posee con la información detallada de la política a seguir, aun que sea un firewall cuidadosamente desarrollado y armado, estará exponiendo la red privada a un posible atentado.

6.1.6 LIMITACIONES DEL FIREWALL

Por supuesto que los sistemas firewall no brindan seguridad absoluta; todo lo contrario. Los firewalls sólo ofrecen protección en tanto todas las comunicaciones salientes pasen sistemáticamente a través de éstos y estén configuradas correctamente. Los accesos a la red externa que sortean el firewall también son puntos débiles en la seguridad. Claramente, éste es el caso de las conexiones que se realizan desde la red interna mediante un módem o cualquier otro medio de conexión que evite el firewall.
Asimismo, la adición de medios externos de almacenamiento a los ordenadores de sobremesa o portátiles de red interna puede dañar enormemente la política de seguridad general.
Para garantizar un nivel máximo de protección, debe ejecutarse un firewall en el ordenador y su registro de actividad debe controlarse para poder detectar intentos de intrusión o anomalías. Además, se recomienda controlar la seguridad (por ejemplo, inscribiéndose para recibir alertas de seguridad de CERT) a fin de modificar los parámetros del dispositivo de firewall en función de las alertas publicadas.
La instalación de un firewall debe llevarse a cabo de la mano de una política de Seguridad real

6.2 FIREWALL A USAR

El firewall que se usara es un firewall físico ya que este da una mejor seguridad en el tráfico de datos aquí indica el modelo y unas de sus características de firewall:

6.1.7 FIREWALL D- LINK DFL - 800

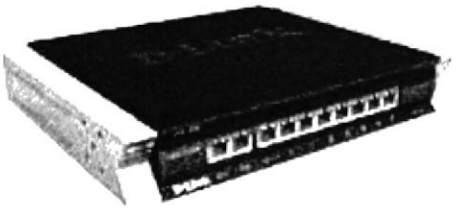


Figura 6-3 Firewalll Link

Este cuenta con 2 protocolos de interconexión que son:

- ✓ ethernet.
- ✓ fast ethernet.

Unas características de protección:

- ✓ Encaminamiento de los datos.
- ✓ Asistencia técnica VPN.
- ✓ Limitación del tráfico.

CAPÍTULO 7

GLOSARIO

GLOSARIO DE TÉRMINOS

A

Ancho de Banda: La diferencia entre las frecuencias más altas y más bajas disponibles para señales de red. El término también se usa para describir la capacidad de rendimiento medida de un medio o un protocolo de red específico.

Arp: Protocolo de resolución de direcciones. Protocolo Internet que se usa para asignar una dirección IP a una dirección MAC. Definido en la RFC 826. Comparar con RARP.

Asignación de direcciones: Técnica que permite que distintos protocolos interoperen traduciendo direcciones desde un formato a otro. Por ejemplo, al enrutar IP a través de una red Frame Relay, las direcciones IP se deben mapear a las direcciones Frame Relay de modo que los paquetes IP se puedan transmitir por la red. Ver también resolución de direcciones.

B

Banda Ancha: Sistema de transmisión que permite multiplexar múltiples señales independientes en un cable. En la terminología de telecomunicaciones, cualquier canal que tenga un ancho de banda mayor que el de un canal con calidad de voz (4 kHz). En terminología LAN, un cable coaxial en el que se usa la señalización analógica. Comparar con banda ancha.

Broadcast: Envío de información en cualquier formato a más de un lugar de destino

Banda Base: Característica de una tecnología de red en la que se usa sólo una frecuencia de portadora. Ethernet es un ejemplo de una red de banda base. También denominada banda estrecha. Ver la diferencia con banda ancha. Término utilizado en la WWW.

Bps: (Bits per Second). Medida que representa la rapidez con que los bits de datos se transmiten a través de un medio de comunicaciones. Por ejemplo: un módem de 28.8 Kbps es capaz de transferir 28.800 bits por segundo.

Bit: (Binary Digit ó Dígito Binario). Es un dígito en base 2, es decir, O ó l.Un bit es la unidad más pequeña de información que la computadora es capaz de manejar. El ancho de banda se suele medir en bits por segundo.

Byte: Unidad de medida de la cantidad de información en formato digital. Usualmente un byíe consiste de 8 bits. Un bit es un cero (0) o un uno (3). Esa secuencia de números (byte) puede simbolizar una letra o un espacio (un carácter). Un kilobyte (Kb) son 1024 bytes y un Megabyte (Mb) son 1024 Kilobytes.

Bloqueo: En un sistema de conmutación, una condición en el que no hay ninguna ruta disponible para completar un circuito. El término también se usa para describir una

situación en la que no se puede iniciar una actividad hasta que la otra no se haya completado.

C

Cable blindado: Cable que posee una capa de aislamiento blindado para reducir la interferencia electromagnética.

Cable coaxial: Cable compuesto por un conductor cilíndrico exterior hueco que rodea un conductor de alambre interno-único. En la actualidad se usan dos tipos de cable coaxial en la LAN: cable de 50 ohmios, que se usa para la señalización digital, y cable de 75 ohmios que se usa para señales analógicas y señalización digital de alta velocidad.

Cable de fibra óptica: Medio físico que puede conducir una transmisión de luz modulada. Si se compara con otros medios de transmisión, el cable de fibra óptica es más caro, sin embargo no es susceptible a la interferencia electromagnética y es capaz de brindar velocidades de datos más altas.

Cable neutro: Cable de circuito que se conecta a la conexión a tierra en la central de energía y en el transformador.

Cableado backbone: Cableado que proporciona interconexiones entre los armarios de cableado, entre los centros de cableado y el POP, y entre los edificios que forman parte de la misma LAN. Ver cableado vertical.

Cableado de Categoría 1: Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 1 se usa para comunicaciones telefónicas y no es adecuado para transmitir datos. Comparar con cableado de Categoría 2, cableado de Categoría 3, cableado de Categoría 4 y cableado de Categoría 5. Ver también EIA/TIA-568B y UTP.

Cableado de Categoría 2: Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 2 es capaz de transmitir datos a velocidades de hasta 4 Mbps. Comparar con cableado de Categoría 1, cableado de Categoría 3, cableado de Categoría 4 y cableado de Categoría 5. Ver también EIA/TIA-568By UTP.

Cableado de Categoría 3: Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 3 se usa en las redes 10BASE-T y puede transmitir datos a velocidades de hasta 10 Mbps. Comparar con cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 4 y cableado de Categoría 5. Ver también EIA/TIA-568B y UTP.

Cableado de Categoría 4: Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 4 se usa en redes Token Ring y puede transmitir datos a velocidades de hasta 16 Mbps. Comparar con cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 3 y cableado de Categoría 5. Ver también EIA/TIA-568B y UTP.

Cableado de Categoría 5: Una de las cinco clases de cableado UTP que se describen en el estándar EIA/TIA-568B. El cableado de Categoría 5 se usa para ejecutar CDDI y puede transmitir datos a velocidades de hasta 100 Mbps. Comparar con cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 3 y cableado de Categoría 4. Ver también EIA/TIA-568By UTP.

Caché: Subsistema especial de memoria en el que se almacenan los datos más utilizados para obtener acceso más rápido. Una memoria caché almacena el contenido de las ubicaciones RAM de acceso más frecuente y las direcciones donde estos datos se almacenan. Cuando el procesador hace referencia a una dirección de memoria, la caché comprueba si almacena dicha dirección. En caso afirmativo, los datos se devuelven al procesador. En caso negativo se produce un acceso normal a memoria. La caché es útil cuando los accesos a RAM son lentos respecto a la velocidad del microprocesador ya que es más rápida que la memoria RAM principal.

Canaleta decorativa: Tipo de canal montado en la pared que tiene una cubierta removible que se usa para admitir el cableado horizontal. La canaleta decorativa es lo suficientemente grande como para contener dos cables.

Canaleta: Un tipo de canal adosado a la pared que tiene una cubierta removible para dar apoyo al cableado horizontal. La canaleta es lo suficientemente grande como para contener varios cables.

Capa física: La Capa 1 del modelo de referencia OSI. La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales.

Capa de control de enlace de datos: La Capa 2 del modelo de arquitectura SNA. Tiene la responsabilidad de transmitir datos a través de un enlace físico determinado.

Capa de red: La Capa 3 del modelo de referencia OSI. Esta capa proporciona conectividad y selección de rutas entre dos sistemas finales.

Capa de transporte: La Capa 4 del modelo de referencia OSI. Esta capa es responsable de la comunicación confiable de red entre nodos finales. La capa de transporte suministra mecanismos para establecer, mantener y terminar los circuitos virtuales, detección y recuperación de errores de transporte y control del flujo de información

Capa de sesión: La Capa 5 del modelo de referencia OSI. Esta capa establece, administra y termina sesiones entre aplicaciones y administra el intercambio de datos entre entidades de capa de presentación.

Capa de servicios de presentación: La Capa 6 del modelo de arquitectura SNA. Esta capa suministra administración de recursos de red, servicios de presentación de sesión y algo de administración de aplicaciones. Corresponde aproximadamente a la capa de presentación del modelo OSI. Ver también capa de control de flujo de datos, capa de control de enlace de datos, capa de control de ruta, capa de control física, capa de servicios de transacción y capa de control de transmisión.

Capa de aplicación: La Capa 7 del modelo de referencia OSI. Esta capa suministra servicios a los procesos de aplicación (como, por ejemplo, correo electrónico, transferencia de archivos y emulación de Terminal) que están fuera del modelo OSI. La capa de aplicación identifica y establece la disponibilidad de los socios de comunicaciones deseados (y los recursos que se requieren para conectarse con ellos), sincroniza las aplicaciones cooperantes y establece acuerdos con respecto a los procedimientos para la recuperación de errores y el control de la integridad de los datos. Corresponde aproximadamente a la capa de servicios de transacción del modelo SNA. Ver también capa de enlace de datos, capa de red, capa física, capa de presentación, capa de sesión y capa de transporte.

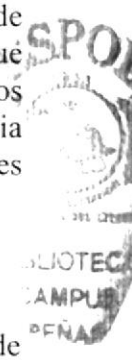
Cliente: Nodo que solicita servicios a un servidor.

Colisión: En Ethernet, el resultado de dos nodos que transmiten de forma simultánea. Las tramas de cada uno de los dispositivos chocan y resultan dañadas cuando se encuentran en el medio físico. Ver también dominio de colisión.

Cola: Generalmente, una lista ordenada de elementos que esperan ser procesados. En enrutamiento, un conjunto de paquetes que esperan ser enviados a través de una interfaz de router.

Conector RJ: Conector macho registrado. Conectores estándar que se usaban originalmente para conectar las líneas telefónicas. En la actualidad, los conectores RJ se usan para conexiones telefónicas y para conexiones 10-100-1000 BASE-T y otro tipo de conexiones de red. Los RJ-11, RJ-12 y RJ-45 son tipos populares de conectores RJ

Costo: Valor arbitrario, generalmente basado en el número de saltos, ancho de banda de los medios u otras medidas, que se asigna a través de un administrador de la red y que se usa para comparar varias rutas a través de un entorno de internetwork. Los protocolos de enrutamiento usan los valores de costo para determinar la ruta más favorable hacia un destino en particular: cuanto menor sea el costo, mejor será la ruta. A veces denominado costo de ruta.



Consola: DTE a través del cual se introducen los comandos en un host.

Correo electrónico: Aplicación de red utilizada ampliamente en la que los mensajes de correo se transmiten electrónicamente entre los usuarios finales a través de diversos tipos de redes usando diversos protocolos de red. A menudo denominado e-mail.

CSMA/CD: Acceso múltiple con detección de portadora y detección de colisiones. Mecanismo de acceso a los medios en que los dispositivos que están listos para transmitir datos verifican primero eí canaí en busca efe una portadora. Si no se detecta ninguna portadora durante un período de tiempo determinado, el dispositivo puede comenzar a transmitir. Si dos dispositivos transmiten al mismo tiempo, se produce una colisión que es detectada por todos los dispositivos que han tenido una colisión. Esta colisión retarda las transmisiones desde aquellos dispositivos durante un período de tiempo aleatorio. El acceso CSMA/CD se usa en Ethernet e IEEE 802.3.

Clic: Acción de presionar y soltar rápidamente el botón del mouse (ratón).

Cliente: Se dice que un programa es un "cliente" cuando sirve sólo para obtener información sobre un programa "servidor". Cada programa "cliente" está diseñado para

trabajar con uno ó más programas "servidores" específicos, y cada "servidor" requiere un tipo especial de "cliente". Un navegador es un programa "cliente".

Computador: Es un dispositivo electrónico compuesto básicamente de un procesador, memoria y dispositivos de entrada/salida (E/S). La característica principal del computador, respecto a otros dispositivos similares, como una calculadora, es que puede realizar tareas muy diversas, cargando distintos programas en la memoria para que los ejecute el procesador. Siempre se busca optimizar los procesos, ganar tiempo, hacerlo más fácil de usar y simplificar las tareas rutinarias.

Contraseña ó Password: Una clave generalmente contiene una combinación de números y letras que no tienen ninguna lógica. Es una medida de seguridad utilizada para restringir los inicios de sesión a las cuentas de usuario, así como el acceso a los Sistemas y recursos de la computadora.

CPU; (Centra] Processirjg Unit ó Unidad central de procesamiento). Es el dispositivo que contiene los circuitos lógicos que realizan las instrucciones de la computadora.

Cuadro de Diálogo: Ventana que aparece temporalmente para solicitar o suministrar información al usuario.

Cuadro de Texto: Parte de un cuadro de diálogo donde se escribe la información necesaria para ejecutar un comando. En el momento de abrir un cuadro de diálogo, el cuadro de texto puede estar en blanco o contener texto.

Cursor: Símbolo en pantalla que indica la posición activa, generalmente titilante. Muestra la posición en que aparecerá el próximo carácter a visualizar cuando se pulse uñatéela.

CSU: Unidad de servicio de canal. Dispositivo de interfaz digital que conecta el equipo del usuario final con el loop telefónico digital local. A menudo se denomina, de forma conjunta con DSU, como CSU/DSU.

D

Db: Decibelios

Dominio: En Internet, una parte del árbol de jerarquía de denominación que se refiere a las agrupaciones generales de redes basadas en el tipo de organización o geografía.

DCE: Equipo de comunicación de datos (expansión EIA) o equipo de terminación de circuito de datos (expansión ITU-T). El dispositivo y las conexiones de una red de comunicaciones que abarca el extremo de la red de la interfaz usuario a red. El DCE proporciona una conexión física con la red, envía tráfico y suministra una señal de temporización que se usa para sincronizar la transmisión de datos entre los dispositivos DCE y DTE. Los módems y las tarjetas de interfaz son ejemplos de DCE. Comparar con DTE.

Descifrado: La aplicación inversa de un algoritmo de cifrado a los datos cifrados, restaurando por lo tanto los datos a su estado original, no cifrado.
Dato: Son las señales individuales en bruto y sin ningún significado que manipulan las computadoras para producir información.

DTE: Equipo de terminal de datos. Dispositivo en el extremo del usuario de una interfaz usuario-red que actúa como origen de datos, destino de datos o ambas. El DTE se conecta a una red de datos a través de un dispositivo DCE (por ejemplo, un módem) y por lo general usa señales de temporización generadas por el DCE. El DTE incluye dispositivos como, por ejemplo, computadores, traductores de protocolo y multiplexores.

Directorio: En D.O.S., una lista de nombres de archivo que contiene toda la información de los archivos almacenados. A partir de Windows 95 este término se reemplazó por CARPETA.
Dirección: Existen tres tipos de dirección de uso común dentro de Internet: "Dirección de correo electrónico* (emáil address); "IP" y (direccion de Internet) y "dirección hardware".

Dirección del Protocolo de Internet (dirección IP): Dirección única que identifica a un equipo host en una red. Identifica a un equipo como una dirección de 32 bits que es única en una red con Protocolo de control de transmisión/Protocolo Internet (TCP/IP). Número único que consta de 4 partes separadas por puntos. Una dirección IP se suele representar en una flotación decimal con puntos que indica cada octeto (ocho bits o un byte) de una dirección IP como su valor decimal y separa cada octeto con un punto. Por ejemplo: 172.16.255.255.
Cada computadora conectada a Internet tiene un único número de IP. Si la máquina ni tiene un IP fijo, no está en realidad en Internet, sino que pide "prestado" un IP a un servidor cada vez que se conecta a la Red (usualmente vía módem).

Disco Rígido: Unidad de almacenamiento permanente de información. Éste es el que guarda la información cuando apagamos la computadora. Aquí se gtiardan la mayoría de los programas y el sistema operativo. Su capacidad de almacenamiento se mide en Megabytes (Mb) o Gigabytes (Gb), en donde 1024 Mb = 1Gb.

Disquete: Dispositivo que puede insertarse y extraerse en una unidad de disco.

DNS: (Domain Ñame System ó Sistema de Nombres de Dominio). El DNS es un servicio de búsqueda de datos de uso general, distribuido y multiplicado. Su utilidad principal es la búsqueda de direcciones IP de sistemas centrales ("hosts") basándose en los nombres de éstos. El estilo de los nombres de "hosts" utilizado actualmente en Internet es llamado "nombre de dominio". Algunos de los dominios más importantes son: .COM (comercial - empresas), .EDU (educación, centros docentes), .ORG (organización sin ánimo de lucro), . NET (operación de la red), .GOV (Gobierno USA) y .MIL (ejército USA). La mayoría de los países tienen un dominio propio. Por ejemplo, AR (Argentina) .PY (Paraguay), .US (Estados Unidos de América), .ES (España), ..AU (Australia), etc.

Dominio: (Domain Ñame). Nombre único que identifica a un sitio de Internet. Los nombres de dominio tienen 2 o más secciones, separadas por puntos. La sección de la izquierda es la más específica, y la de la derecha, la más general. Una computadora particular puede tener más de un nombre de dominio, pero un nombre de dominio se refiere únicamente a una PC.

Download ó descargar: En Internet es el proceso de transferir información desde un servidor de información a la propia PC.

Documentación: Manual escrito que detalla el manejo de un sistema o pieza de hardware.

Doble Clic: Acción de presionar y soltar rápidamente el botón del mouse (ratón) dos veces, sin desplazarlo. Esta acción sirve para ejecutar una determinada aplicación, como por ejemplo: inicializarla.

DSU: Unidad de servicio de datos. Dispositivo que se usa en la transmisión digital que adapta la interfaz física de un dispositivo DTE a una instalación de transmisión como, por ejemplo, TI y El.

DVD: (Digital Versatile Disc ó Disco Versátil Digital). Disco que sirve para almacenar más datos de contenido digital, como música o video, que un CD. Un DVD guarda un mínimo de 4.7 Gigabytes (el tamaño de una película de cine).

E

El: Estándar Europeo equivalente al americano TI. Los circuitos El y TI. Los dos usan canales de 64 Kbps, pero el TI tiene 24 mientras que el El tiene 32 canales.

EIA/TIA-568: Estándar que describe las características y aplicaciones para diversos grados de tendido de cableado UTP. Ver también cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 3, cableado de Categoría 4, cableado de Categoría 5 y UTP.

Encapsulamiento: El proceso por el cual se envuelven datos en un encabezado de protocolo en particular.

Emulación de terminal: Aplicación de red en la que un computador ejecuta software que la hace aparecer ante un host remoto como una terminal conectada directamente.

Enrutamiento: Proceso para encontrar una ruta hacia un host destino. El enrutamiento en redes de gran tamaño es muy complejo dada la gran cantidad de destinos intermedios potenciales que debe atravesar un paquete antes de llegar al host destino.

Ethernet: Especificación de LAN de banda base inventada por Xerox Corporation y desarrollada de forma conjunta por Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet usan CSMA/CD y se ejecutan a través de varios tipos de cable a 10 Mbps. Ethernet es similar al conjunto de estándares IEEE 802.3. Ver también IOBASE2, IOBASE5, IOBASE-F, IOBASE-T, lOBroad36 e IEEE 802.3.

Elemento de Pantalla: Partes que constituyen una ventana o cuadro de diálogo como por ejemplo: la barra de título, los botones de "Maximizar" y "Minimizar", los bordes de las ventanas y las barras de desplazamiento.

Escritorio: Fondo de la pantalla sobre la cual aparecen ventanas, iconos y cuadros de diálogo.

Estación de trabajo: Computador de gran potencia que cuenta con elevada capacidad gráfica y de cálculo. Llamadas así para distinguirlas de los que se conocen como servidores.

Expandir: Mostrar los niveles de directorio ocultos del árbol de directorios. Con el administrador de archivos es posible expandir un solo nivel de directorio, una rama del árbol de directorio o todas las ramas a la vez.

Explorador: Llamado también explorador Web. Interfaz cliente que permite al usuario ver documentos HTML en el World Wide Web, en otra red o en su propio equipo; seguir los hipervínculos y transferir archivos. Un ejemplo es Microsoft Internet Explorer.

Extensión: Está compuesto por un punto y un sufijo de hasta tres caracteres situados al final de un nombre de archivo. La extensión suele indicar el tipo de archivo o directorio.

F

Fibra monomodo: Cable de fibra óptica con un núcleo estrecho que permite que la luz entre sólo en un único ángulo. Dicho cableado tiene mayor ancho de banda que la fibra multimodo, pero requiere una fuente de luz con una anchura espectral más angosta (por ejemplo, un láser). También denominada fibra de modo único. Ver también fibra multimodo.

Fibra multimodo: Fibra óptica que permite la propagación de múltiples frecuencias de luz.

Firewall: Router o servidor de acceso, o varios routers o servidores de acceso, designados como un búfer entre cualquier red pública conectada y una red privada. El router firewall usa listas de acceso y otros métodos para garantizar la seguridad de la red privada.

Fluctuación de fase: Distorsión analógica de la línea de comunicación provocada por la variación de una señal de sus posiciones de temporización de referencia. La fluctuación de fase puede provocar la pérdida de datos, especialmente a altas velocidades.

Flujo de datos: Todos los datos que se transmiten a través de la línea de comunicaciones en una sola operación de lectura o escritura.
Frecuencia: Cantidad de ciclos, medidos en hercios, de una señal de corriente alterna por unidad de tiempo.

FTP: Protocolo de transferencia de archivos. Protocolo de aplicación, parte de la pila de protocolo TCP/IP, que se usa para transferir archivos entre nodos de la red. El FTP se define en la RFC 959.

Full dúplex: Capacidad de transmitir datos de forma simultánea entre una estación emisora y una estación receptora.

G

Gateway: En la comunidad IP, un término antiguo que se refiere a un dispositivo de enrutamiento. En la actualidad, el término router se usa para describir nodos que ejecutan esta función, y gateway se refiere a un dispositivo con fines especiales que ejecuta conversión de capa de aplicación de la información de una pila de protocolo a otra.
Gateway fronterizo: Router que se comunica con routers de otros sistemas autónomos.
Giga: Prefijo que indica un múltiplo de 1.000 millones, o sea 109. Cuando se emplea el sistema binario, como ocurre en informática, significa un múltiplo de 1.073.741.824.

Grupo de trabajo: Conjunto de estaciones de trabajo y servidores de una LAN que están diseñados para comunicarse e intercambiar datos entre sí.

H

Hardware: Son todos los componentes físicos que componen una PC.
Hercio: Unidad de medida de la frecuencia, abreviada como Hz. Un sinónimo sería ciclos por segundo.

Hexadecimal: Base 16. Representación numérica que usa los dígitos O a 9, con su significado habitual, y las letras A a la F para representar dígitos hexadecimales con valores de 10 a 15. El dígito ubicado más a la derecha cuenta unos, el siguiente cuenta múltiplos de 16, luego 16A2=256, etc.

Host: Sistema computacional ubicado en una red. Es similar al término nodo, salvo que el host generalmente implica un sistema computacional, mientras que el nodo generalmente se aplica a cualquier sistema conectado a la red, incluyendo servidores de acceso y routers.

HTML: (HyperText Markup Language). Lenguaje utilizado para crear los documentos de hipertexto que se emplean en la WWW. Los documentos HTML son simples archivos de texto que contienen instrucciones (llamadas tags) entendibles por el Navegador (Browser).

HTTP: (HyperText Transport Protocol). Protocolo utilizado para transferir archivos de hipertexto a través de Internet. Requiere de un programa "cliente" de HTTP en un extremo y un "servidor" de HTTP en el otro extremo. Es el protocolo más importante de la WWW.

Hub: Dispositivo de hardware o software que contiene módulos de red y equipo de internetwork múltiples, independientes pero conectados. Los hubs pueden ser activos (cuando repiten señales que se envían a través de ellos) o pasivos (cuando no repiten, sino que simplemente dividen, las señales que se envían a través de ellos).

I

IEEE: Instituto de ingenieros eléctricos y electrónicos. Organización profesional cuyas actividades incluyen el desarrollo de estándares de comunicaciones y de redes. Los estándares LAN del IEEE son los estándares de LAN predominantes en el mundo actual.

IEEE 802.1: Especificación del IEEE que describe un algoritmo que evita los loops de capa dos mediante la creación de un spanning tree. El algoritmo fue inventado por Digital Equipment Corporation. El algoritmo de Digital y el algoritmo IEEE 802.1 no son exactamente los mismos, ni tampoco son compatibles.

IEEE 802.12: Estándar LAN del IEEE que especifica la capa física y la subcapa MAC de la capa de enlace de datos. El IEEE 802.12 usa el esquema de acceso a los medios de prioridad de demanda a 100 Mbps a través de una diversidad de medios físicos. Ver también 100 VG-Any LAN.

IEEE 802.2: Protocolo LAN del IEEE que especifica una implementación de la subcapa LLC de la capa de enlace de datos. IEEE 802.2 administra errores, entramado,

control de flujo y la interfaz de servicio de la capa de red (Capa 3). Se usa en las LAN IEEE 802.3 e IEEE 802.5. Ver también IEEE 802.3 e IEEE 802.5.

IEEE 802.3: Protocolo LAN del IEEE que especifica una implementación de la capa física y la subcapa MAC de la capa de enlace de datos. IEEE 802.3 usa acceso CSMA/CD a diversas velocidades sobre diversos medios físicos. Las extensiones del estándar IEEE 802.3 especifican las implementaciones de Fast Ethernet. Las variantes físicas de la especificación IEEE 802.3 original incluyen IOBASE2, IOBASE5, 1 OBASE-F, 1 OBASE-T y 1 OBroad36. Las variantes físicas de Fast Ethernet incluyen 1 OOBASE-T, 1 OOBASE-T4y ¡ OOBASE-X.

Icono: Símbolo gráfico que aparece en la pantalla de una PC para representar determinada acción a realizar por el usuario, ejecutar un programa, leer una información, imprimir un texto, etc.

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

Impresora: Dispositivo de salida, cuya funcionalidad es transcribir/pasar un documento (imagen y/o texto) desde el ordenador (procesador de textos, bloc de notas, visor de imágenes, etc.) a un medio físico, generalmente papel, mediante el uso de cinta, cartuchos de tinta o también con tecnología láser.

Impresora de Inyección a tinta: Crean imágenes directamente sobre el papel al rociar tinta a través de una pequeñas boquillas, su calidad de impresión es bastante alta.

Impresora Predeterminada: Impresora que se utiliza si se elige el comando Imprimir, no habiendo especificado antes la impresora que se desea utilizar. Sólo puede haber una impresora predeterminada, que debe ser la que se utilice con mayor frecuencia.

Información: Es lo que se obtiene del procesamiento de datos, es el resultado final.

Informática cliente-servidor: Término que se usa para describir los sistemas de red informáticos distribuidos (de procesamiento) en los que las responsabilidades de transacción se dividen en dos partes: cliente (front end) y servidor (back end). Ambos términos (cliente y servidor) se pueden aplicar a los programas de software o a los dispositivos informáticos actuales.

Internetwork: Conjunto de redes interconectadas por routers y otros dispositivos que funcionan (generalmente) como una sola red.

IP: Protocolo Internet. Protocolo de capa de red en la pila TCP/IP que brinda un servicio de internetworking no orientado a conexión. El IP suministra características de direccionamiento, especificación de tipo de servicio, fragmentación y reensamblaje y seguridad. Documentado en la RFC 791.

IP access-group: Comando que enlaza una lista de acceso existente con una interfaz de salida.

IP host: Comando que se usa para crear una entrada estática que relaciona el nombre de host con la dirección del mismo en el archivo de configuración del router.

IP muiticast: Técnica de enrutamiento que permite que el tráfico IP se propague desde un origen hacia un número de destinos o desde varios orígenes hacia varios destinos. En lugar de enviar un paquete a cada destino, se envía un paquete a un grupo de multicast que se identifica mediante una sola dirección de grupo de destino IP.

IPX: Intercambio de paquetes de internetworking. Protocolo de capa de red (Capa 3) de NetWare que se usa para transferir datos desde servidores a estaciones de trabajo. El IPX es similar al IP y al XNS.

Interfaz: Una conexión e interacción entre hardware, software y usuario, es decir, como la plataforma o medio de comunicación entre usuario o programa.

Internet: Conjunto de redes conectadas entre sí, que utilizan el protocolo TCP/IP para comunicarse.

Intranet: Red privada dentro de una empresa que utiliza el mismo software y protocolos empleados en la Internet global, pero que sólo es de uso interno.
ISO: Organización Internacional de Normalización. Organización internacional que es responsable por una amplia gama de estándares, incluyendo aquellos relevantes para el networking. ISO desarrolló el modelo de referencia OSI, un modelo de referencia de networking sumamente popular.

J

Jumper: Término que se usa para los cables de interconexión que se encuentran en el armario de cableado.

K

Kbps: (Kilobits por segundo). Unidad de medida de la capacidad de transmisión de una línea de telecomunicación. Cada kilobit esta formado por mil bits.

Kilobyte: Es el equivalente a 1024 bytes.

L

LAN: Red de área local. Redes de datos de alta velocidad y bajo nivel de errores que abarcan un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LAN conectan estaciones de trabajo, dispositivos periféricos, terminales y otros dispositivos que se encuentran en un mismo edificio u otras áreas geográficas limitadas. Los estándares de LAN especifican el cableado y la señalización en las capas física y de

enlace de datos del modelo OSI. Ethernet, FDDI y Token Ring son tecnologías LAN de uso muy difundido. Comparar con MAN y WAN.

Latencia: Retardo entre el momento en que el dispositivo solicita acceso a una red y el momento en el que se le otorga permiso para transmitir también sucede en el momento en que un dispositivo recibe una trama y el momento en que la trama sale desde el puerto destino.

LED: Diodo emisor de luz. Dispositivo semiconductor que emite luz producida por la conversión de energía a eléctrica. Las lámparas de estado en los dispositivos de hardware generalmente son LED.

Línea de acceso telefónico: Circuito de comunicaciones que se establece mediante una conexión de circuito conmutada usando la red de la compañía telefónica.

Línea de comunicación: Enlace físico (como, por ejemplo, un cable o circuito de teléfono) que conecta uno o más dispositivos con uno o más dispositivos.

Línea de mira: Característica de determinados sistemas de transmisión como, por ejemplo, los sistemas láser, de microondas e infrarrojos, en los que no puede existir ninguna obstrucción en la ruta directa entre el transmisor y el receptor.

Línea dedicada: Línea de comunicaciones que se reserva indefinidamente para transmisiones, en lugar de conmutarse cuando se requiere transmitir. Ver también línea arrendada.

Lista de acceso: Lista que mantienen los routers Cisco para controlar el acceso hacia o desde el router para diversos servicios (por ejemplo, para evitar que los paquetes que tienen una determinada dirección IP salgan de una interfaz específica del router).

LSA: Publicación de estado de enlace. Paquete de broadcast que usan los protocolos de estado de enlace que contiene información acerca de los vecinos y los costos de la ruta. Los routers receptores usan las LSA para mantener sus tablas de enrutamiento.

Login: Nombre de usuario utilizado para obtener acceso a una computadora o a una red. A diferencia del password, el login no es secreto, ya que generalmente es conocido por quien posibilita el acceso mediante este recurso.

M

MAC: Control de acceso al medio. La más baja de las dos subcapas de la capa de enlace de datos definida por el IEEE. La subcapa MAC administra acceso al medio compartido como, por ejemplo, si se debe usar transmisión de tokens o contención. Ver también capa de enlace de datos y LLC.

MICIP: Protocolo de capa de red que encapsula paquetes IP en DDS o transmisión a través de AppleTalk.

Malla: Topología de red en la que los dispositivos se organizan de una manera administrable, segmentada, con varias interconexiones, a menudo redundantes, ubicadas estratégicamente entre nodos de la red. Ver también malla completa y malla parcial.

Malla completa: Término que describe a una red en la que los dispositivos están organizados en una topología de malla, en la que cada nodo de la red tiene un circuito físico o un circuito virtual que lo conecta a todos los otros nodos de la red. Una malla completa brinda una gran cantidad de redundancia pero, dado que su implementación puede resultar excesivamente cara, generalmente se la reserva para los backbones de la red. Ver también malla y malla parcial.

MAN: Red de área metropolitana. Red que abarca un área metropolitana. Por lo general, una MAN abarca un área geográfica más grande que una LAN, pero más pequeña que una WAN.

MAP: Protocolo de automatización de fabricación. Arquitectura de red creada por General Motors para satisfacer las necesidades específicas las instalaciones fabriles. El MAP especifica una LAN de transmisión de tokens similar a IEEE 802.4. Ver también IEEE 802.4. –

Mapa de cableado: Característica suministrada por la mayoría de los analizadores de cable. Se usa para probar las instalaciones de cableado de par trenzado, y muestra cuáles hilos están conectados a cuáles pilles, en conectores macho y hembra.

Mapa de topología: Herramienta para administrar un switch ATM LightStream 2020 que examina una red y muestra el estado de sus nodos y enlaces troncales. El mapa de topología es una aplicación basada en HP OpenView que se ejecuta en un NMS.

Máscara de red: Combinación de bits que se usa para describir qué parte de una dirección se refiere a la red o subred y qué parte se refiere al host. Algunas veces se denomina simplemente máscara. Ver también máscara de subred.

Máscara wildcard: Cantidad de 32 bits que se usan de forma conjunta con una dirección IP para determinar cuáles son los bits de una dirección IP que se deben ignorar al comparar esa dirección con otra dirección IP. La máscara wildcard se especifica al configurar las listas de acceso.

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

Megabyte (MB): 1.048.576 bytes; 1.024 Kilobytes.

Megahertz: Unidad de medida de la frecuencia de reloj del microprocesador (en millones de ciclos por segundo).

Memoria RAM: Memoria de acceso aleatorio cuyo contenido permanecerá presente mientras el computador permanezca encendido.

Memoria ROM: Memoria de sólo lectura. Chip de memoria que sólo almacena permanentemente instrucciones y datos de los fabricantes.

Microonda: este enlace esta constituido por dos transceptores de radio provistos de antenas parabólicas que se apuntan directamente entre si. La radio puede transportar transmisiones punto a punto de muchos anchos de banda. Su alcance varia según el tamaño de la antena, el clima en la zona y la magnitud de la potencia emitida contemplando todos estos conjuntos la señal puede llegar hasta 80 Km.

Módem: (Modulator,Demodulator). Dispositivo que se conecta a la computadora y a la linea telefónica y que permite comunicarse con otras computadoras a través del sistema telefónico. Básicamente, los módems sirven a las computadoras de la misma manera que los teléfonos sirven a las personas.

Mouse: Permite convertir el movimiento de la mano en desplazamiento de un cursor obre la pantalla.

Multicast: la multidifusión (multicast) permite que grupos de usuarios seleccionados reciban la misma transmisión de datos en una red los cuales están identificados por una mica dirección de grupo de destino IP.

N

Navegador de Web: Aplicación de cliente de hipertexto basada en GUI como, por ejemplo, Mosaic, que se usa para acceder a documentos de hipertexto y otros servicios ubicados en innumerables servidores remotos a través de la WWW e Internet. Ver también hipertexto, Internet, Mosaic y WWW.

NBP: Protocolo de enlace de denominación. Protocolo AppleTalk de nivel de transporte que convierte un nombre dado en forma de una cadena de caracteres en una dirección de internetwork.

NET: Título de entidad de red. Direcciones de red, definidas por la arquitectura de red ISO.

NetBIOS: Sistema básico de entrada/salida de red. API que usan las aplicaciones de una LAN IBM para solicitar servicios de procesos de red de nivel inferior. Estos servicios pueden incluir establecimiento y terminación de sesión y transferencia de información

NetWare: NOS distribuido de uso generalizado desarrollado por Novell. Suministra acceso remoto transparente a archivos, y muchos otros servicios de red distribuida.

Networking: Conexión de cualquier conjunto de computadores, impresoras, routers, switches y otros dispositivos con el propósito de comunicarse a través de algún medio de transmisión.

NIC: Tarjeta de interfaz de red. Placa que suministra capacidades de comunicación de red hacia y desde un sistema computacional. También denominado adaptador.

NOS: Sistema operativo de red. Término genérico que se usa para referirse a lo que en realidad son sistemas de archivos distribuidos. Los ejemplos de NOS incluyen LAN Manager, NetWare, NFS y VINES.

Número de host: Parte de una dirección IP que designa qué nodo de la subred se está direccionando.

Número de red: Parte de una dirección IP que especifica la red a la que pertenece el host.

Número de saltos: Métrica de enrutamiento que se usa para medir la distancia entre un origen y un destino. El RIP usa el número de saltos como su única métrica.
NVRÁM: RAM no volátil. RAM que retiene su contenido cuando una unidad se apaga. En los productos Cisco, la NVRAM se usa para guardar la información de configuración.

Nodo: En una red de área local, un nodo es un dispositivo que está conectado a la red y es capaz de comunicarse con otros dispositivos de la misma.

Nombre de usuario: La secuencia de caracteres que lo identifica. Al conectarse a una computadora, generalmente necesita proporcionar su nombre y contraseña de usuario. Esta información se usa para verificar que la persona está autorizada para usar el Sistema.

O

Operador de red: Persona que monitorea y controla una red de forma continua, ejecutando tareas varias.

Oscilación: Señal secundaria superpuesta a la onda de 60 Hz. Tiene una magnitud que varía entre el 15% y el 100% del voltaje normal de la línea de alimentación. Ver sobrevoltaje, pico y baja de voltaje.

OSI: Interconexión de sistemas abiertos. Programa internacional de normalización creado por la ¡SO y la UIT-T para desarrollar estándares de interconexión que faciliten la interoperabilidad de equipos de múltiples proveedores.

OSINET: Asociación internacional diseñada para promover OS! en las arquitecturas de los proveedores.

OSPF: Versión abierta del algoritmo "Primero la ruta libre más corta". Algoritmo de enrutamiento TOP jerárquico, de estado de enlace, propuesto como sucesor de RIP en la comunidad Internet. Las características de OSPF incluyen enrutamiento por menor costo, enrutamiento de múltiples rutas y balanceo de carga. El OSPF deriva de una versión inicial del protocolo ISIS.

P

PAD: Ensamblador/desamblador de paquetes. Dispositivo que se usa para conectar dispositivos simples (como terminales de modo de carácter) a una red, los cuales no admiten toda la funcionalidad de un protocolo específico. Los PAD almacenan los datos en el búfer de los PAD y ensamblan y desensamblan los paquetes que se envían a dichos dispositivos finales.

Panel de conexión: Conjunto de ubicaciones de pm y puertos que se puede montar en un bastidor o una consola de pared en el armario de cableado. Los paneles de conexión actúan como conmutadores que conectan los cables de las estaciones de trabajo entre sí y con el exterior.

Paquete: Agrupación lógica de información que incluye un encabezado que contiene información de control y (generalmente) datos del usuario. Los paquetes a menudo se usan para referirse a las unidades de datos de la capa de red. Los términos datagrama, trama, mensaje y segmento también se usan para describir las agrupaciones de información lógica en las diversas capas del modelo de referencia OSI y en los diversos círculos tecnológicos.

Paquete de choque: Paquete que se envía al transmisor para informarle que hay congestión y que debe reducir su velocidad de envío.

Par trenzado: Medio de transmisión de relativa baja velocidad compuesto por dos cables aislados dispuestos en un patrón en espiral regular. Los cables pueden ser blindados o no blindados. El uso del par trenzado es común en aplicaciones de telefonía y es cada vez más común en las redes de datos. Ver también STP y UTP.

Paradiafonía: Energía de interferencia transferida de un circuito a otro.

PBX: Central telefónica privada. Conmutador telefónico digital o analógico ubicado en las instalaciones del suscriptor y que se usa para interconectar redes telefónicas privadas y públicas.

PCI: Información de control de protocolo. Información de control que se agrega a los datos del usuario para formar un paquete OSI.

Pila de protocolo: Conjunto de protocolos de comunicación relacionados que operan de forma conjunta y, como un grupo, cumplen con la comunicación en alguna o en las siete capas del modelo de referencia OSI. No todas las pilas de protocolo abarcan cada capa del modelo y, a menudo, un solo protocolo de la pila se dirige a una cantidad de capas a la vez. El TCP/IP es un protocolo de pila típico.

Ping: Abreviatura para Packet Internet Groper o Packet Inter-network Groper, una utilidad que se usa para determinar si una dirección IP en particular está disponible. Funciona enviando un paquete a la dirección especificada y esperando una respuesta. El PING se usa principalmente para diagnosticar las fallas de las conexiones de Internet.

Plan de distribución: Diagrama simple que indica dónde están ubicados los tendidos de cable y la cantidad de habitaciones hacia las que se dirigen.

POP: Punto de presencia. Punto de presencia es el punto de interconexión entre las instalaciones de comunicación suministradas por la empresa telefónica y el servicio de distribución principal del edificio.

Portadora: Onda electromagnética o corriente alterna de una sola frecuencia, adecuada para modulación por parte de otra señal portadora de datos. Ver también modulación.

POST: Autocomprobación de encendido. Conjunto de diagnósticos de hardware que se ejecutan en un dispositivo de hardware cuando ese dispositivo se enciende.

Protocolo de enrutamiento: PrQtocolo que logra el enrutamiento a través de la implementación de un algoritmo de enrutamiento específico. Los ejemplos de protocolos de enrutamiento incluyen el IGRP, el OSPF y el RIP.

Puerto: Interfaz de un dispositivo de internetworking (como, por ejemplo, un router) En terminología ip, un proceso de capa superior que recibe información de las capas Inferiores. Un conector hembra de un panel de conexión el cual acepta el mismo tamaño de conector que el de un rj45. Los cables de conexión se usan en estos puertos para realizar interconexiones entre los computadores conectados al panel. Es esta interconexión conexión la que permite la operación de la lan.

Página Web: Documento de World Wide Web. Una página Web suele consistir en un archivo HTML, con sus archivos asociados de gráficos y secuencias de comandos, en un directorio determinado de un equipo concreto (y, por tanto, identificable mediante una dirección URL).

Periféricos: Cualquier dispositivo de hardware conectado a una computadora.

Pixel: (PlCture cELL). Es la parte más pequeña de una pantalla de video, constituido por uno o más puntos que se consideran como una unidad. Es por tanto, el bloque de construcción de imágenes.

Protocolo: Método por el que los equipos se comunican en Internet. El protocolo más común en el World Wide Web es HTTP. Otros protocolos de Internet incluyen FTP, Gopher y telnet. El protocolo forma parte de la dirección URL completa de un recurso.

Proveedor: Institución o empresa que provee acceso a uno o varios servicios de Internet.

R

RAM: Memoria de acceso directo aleatorio. Memoria volátil que puede ser leída y escrita por un microprocesador.

Red: Conjunto de computadores, impresoras, routers, switches y otros dispositivos que se pueden comunicar entre sí a través de algún medio de transmisión.

Red de conexión única: Red que tiene una sola conexión con un router
Redireccionar: Parte de los protocolos ICMP y ES-IS que permiten que un router le indique a un host que puede ser más efectivo usar otro router.

Redistribución: Permitir que la información de enrutamiento detectada a través de un protocolo de enrutamiento sea distribuida en los mensajes de actualización de otro protocolo de enrutamiento. A veces denominada redistribución de ruta.

Redundancia: En internetworking, la duplicación de dispositivos, servicios o conexiones de modo que, en caso de que se produzca una falla, los dispositivos, servicios o conexiones redundantes puedan ejecutar el trabajo de aquellos que han fallado. Ver también sistema redundante.

Rendimiento: Velocidad de la información que llega a, y posiblemente atraviesa, un punto particular de un sistema de red.

Repetidor: Dispositivo que regenera y propaga señales eléctricas entre dos segmentos de red.

Retardo: El tiempo que hay entre el inicio de una transacción por parte del emisor y la primera respuesta recibida por el emisor. También, el tiempo que se requiere para mover un paquete desde el origen hacia el destino a través de una ruta específica.

RF: Radiofrecuencia. Término genérico que se usa para referirse a frecuencias que corresponden a transmisiones radioeléctricas. Las redes de televisión por cable y de banda ancha usan tecnología RF.

Router: Dispositivo de capa de red que usa una o más métricas para determinar la ruta óptima a través de la cual se debe enviar el tráfico de red. Los routers envían paquetes desde una red a otra basándose en la información de la capa de red.

RIP: Protocolo de información de enrutamiento. IGP que se suministra con los sistemas UNIX BSD. El IGP más común de Internet.

RMON: Monitoreo remoto. Especificación de agente MIB que se describe en la RFC 1271 que define las funciones para el monitoreo remoto de los dispositivos conectados a la red.

ROM: Memoria de sólo lectura. Memoria no volátil que un microprocesador puede leer, pero no escribir.

Ruta estática: Ruta que está configurada e ingresada en la tabla de enrutamiento de forma explícita. Las rutas estáticas tienen prioridad sobre las rutas elegidas por los protocolos de enrutamiento dinámicos.

Ruta por defecto: Entrada de la tabla de enrutamiento que se utiliza para dirigir tramas para las cuales el salto siguiente no aparece explícitamente en la tabla de enrutamiento.

S

Segmento: La sección de una red limitada por puentes, routers o switches. Término que se usa en la especificación TCP para describir una unidad de información de la capa de transporte. Los términos datagrama, trama, mensaje y paquete también se usan para describir las agrupaciones de información lógica en las diversas capas del modelo de referencia OSI y en los diversos círculos tecnológicos.

SMTP: Protocolo simple de transferencia de correo. Protocolo Internet que suministra servicios de correo electrónico

Sondeo: Método de acceso en el que el dispositivo de red primario pregunta, en forma ordenada, si los secundarios tienen algún dato para transmitir. La pregunta se realiza en forma de mensaje que se envía a cada dispositivo secundario, lo que le otorga al secundario el derecho de transmitir.

Switch: Dispositivo de red que filtra, reenvía o inunda tramas basándose en la dirección destino de cada trama. El switch opera en la capa de enlace de datos del modelo OSI.

Switch LAN: Switch de alta velocidad que envía paquetes entre segmentos de enlace de datos. La mayoría de los switches LAN envían tráfico basándose en las direcciones MAC. Esta variedad de switch LAN a veces de denomina switch de trama. Los switches LAN a menudo se clasifican de acuerdo con el método que usan para enviar tráfico: conmutación de paquetes por método de corte y conmutación de paquetes por almacenamiento y envío. Los switches multicapas son un subconjunto inteligente de los switches LAN.

Servidor: Computadora o programa que brinda un servicio específico al "cliente', que se ejecuta en otras computadoras. El término puede referirse tanto a un equipo de una red que envía archivos o ejecuta aplicaciones para otros equipos de la red; el software que se ejecuta en el equipo servidor y que efectúa la tarea de servir archivos y ejecutar aplicaciones; o bien, en la programación orientada a objetos, un fragmento de código que intercambia información con otro fragmento de código cuando se pide.

SO: (Sistema Operativo). Programa o conjunto de programas que permiten administrar los recursos de hardware y software de una computadora.

Software: Todos los componentes no físicos de una PC (Programas).

T

TI: Servicio de portadora de WAN digital. TI transmite datos con formato DS- 1 a 1.544 Mbps a través de la red de conmutación telefónica, usando codificación AMI o B8ZS. Comparar con El. Ver también AMI, B8ZS y DS-1.

Tabla de enrutamiento: Tabla que se guarda en un router o en algún otro dispositivo de internetworking que ayuda a identificar las rutas hacia destinos de red en particular y, en algunos casos, las métricas asociadas con esas rutas.

TFTP: Protocolo de Transferencia de Archivos Trivial. Versión simplificada del FTP que permite que los archivos se transfieran desde un computador a otra a través de una red.

Terminal: Dispositivo simple en el que los datos se pueden introducir o recuperar desde una red. Generalmente, las terminales tienen un monitor y un teclado pero no tienen ningún procesador ni unidad de disco local.

Topología: Disposición física de los nodos y medios de red dentro de una estructura de networking empresarial.

Topología de anillo: Topología de red que consta de un conjunto de repetidores conectados entre sí mediante enlaces de transmisiones unidireccionales para formar un solo bucle cerrado. Cada estación de la red se conecta a la red en el repetidor. Aunque lógicamente están organizadas en anillo, las topologías de anillo a menudo están organizadas en una estrella de bucle cerrado.

Topología de bus: Arquitectura LAN lineal en la que las transmisiones de las estaciones de red se propagan a lo largo del medio y son recibidas por todas las otras estaciones.

Topología en árbol: Topología LAN similar a la topología bus, salvo que las redes en árbol pueden tener ramificaciones con múltiples nodos. Las transmisiones desde una estación atraviesan la longitud del medio y son recibidas por todas Las otras estaciones.

Topología en estrella: Topología LAN en la que los puntos de terminación de una red se conectan a un switch central común mediante enlaces punto a punto. Una topología de anillo que está organizada como estrella implementa una estrella de loop cerrado unidireccional en lugar de enlaces punto a punto.

Topología en estrella jerárquica: Topología en estrella extendida en la que un hub central se conecta a través de cableado vertical con otros hubs que dependen del mismo.

Transceiver: Unidad de conexión al medio. Dispositivo que se usa en las redes Ethernet e IEEE 802.3 que suministra la interfaz entre el puerto AUI de una estación y el medio común de Ethernet. La MAU, que se puede incorporar a una estación o puede ser un dispositivo individual, ejecuta funciones de capa física, incluyendo la conversión

de datos digitales desde la interfaz Ethernet, detección de colisiones e inyección de bits en la red.

Tunneling: Arquitectura que está diseñada para suministrar los servicios necesarios para implementar cualquier esquema de encapsulamiento punto a punto estándar.
Tarjeta de Interfaz de Red: (NIC). Dispositivo a través del cual computadoras de una red transmiten y reciben datos.

TCP/IP: (Transmisor Control Protocol/Internet Protocol). Conjunto de protocolos que definen a la Internet. Fueron originalmente diseñados para el sistema operativo Unix, pero actualmente puede encontrarse en cualquier sistema operativo.

Telnet: Protocolo que permite al usuario de Internet conectarse y escribir comandos en un equipo remoto vinculado a Internet como si el usuario estuviera utilizando un terminal de texto conectado directamente al equipo. Forma parte del conjunto de protocolos TCP/IP.

Tiempo Real: Método para procesar la información en cuanto se recibe.

U

Unicast: En redes conmutadas ethernet, transferencia de archivos/paquetes entre dos entidades. Una difusión única puede iniciarla un servidor a una estación de trabajo, una estación a un servidor, una estación a una impresora o cualquier otra unidad única hacia otra entidad

UPS: (Uninterruptible Power Supply ó Suministro de Energía Ininterrumpida). Es un estabilizador electrónico que está preparado para suplir al computador cuando se presenten caídas de energía o cambios de voltaje.

URL: (Universal Resource Locator ó Localizador de Recursos Universal). Identifica de manera única la ubicación de un equipo, directorio o archivo en Internet. La dirección URL también indica el protocolo de Internet apropiado, como HTTP o FTP. Por ejemplo: http://www.microsoft.com.

USB: Tecnología que facilita la conexión de periféricos a la computadora. Esta reconoce automáticamente los dispositivos nuevos y no hay que insertar una placa controladora para el dispositivo, ya que se conecta a la parte trasera de la PC a un enchufe especial (puerto USB). La tarjeta madre debe tener esta tecnología en su CHIPSET para poder conectar dispositivos de este tipo.

UTP: Cable de para trenzado no apantallado, lo que significa que no tiene envoltura alrededor del grupo de conductores. Estos cables se usan principalmente en redes de voz y datos

Usuario: Cualquier individuo que interactúa con el computador a nivel de aplicación. Los programadores, operadores y otro personal técnico no son considerados usuarios cuando trabajan con el computador a nivel profesional.

V

Vector: Segmento de datos de un mensaje SNA. Un vector está compuesto por un campo de longitud, una clave que describe el tipo de vector y datos específicos del vector.

Virtuatización: Proceso que se usa para implementar una red basada en segmentos de red virtuales. Los dispositivos se conectan a segmentos virtuales independientemente de su ubicación física y de su conexión física con la red.

VLAN: LAN virtual. Grupo de dispositivos en una LAN que se configuran (usando software de administración) de modo que se puedan comunicar como si estuvieran conectadas al mismo cable cuando, de hecho, están ubicadas en una cantidad de segmentos LAN distintos. Dado que las VLAN se basan en conexiones lógicas y no físicas, son extremadamente flexibles.

VLSM: Máscara de subred de longitud variable. Capacidad de especificar una máscara de subred distinta para el mismo número de red en distintas subredes. Las VLSM pueden ayudar a optimizar el espacio de dirección disponible.

VTP: Protocolo de terminal virtual. Aplicación ISO para establecer una conexión de terminal virtual a través de una red.

Virus: Programa que se duplica a sí mismo en un sistema informático, incorporándose a otros programas que son utilizados por varios sistemas. Estos programas pueden causar problemas de diversa gravedad en los sistemas que los almacenan, se propagan a través de cualquier medio de almacenamiento, o a través de la LAN, o de la misma Internet.

W

WAN: Red de área amplia. Red de comunicación de datos que sirve a usuarios dentro de un área geográficamente extensa y a menudo usa dispositivos de transmisión provistos por un servicio público de comunicaciones. Frame Relay, SMDS y X.25 son ejemplos de WAN. Comparar con LAN y MAN.

WorkGroup Director: Herramienta de software de Cisco para la administración de redes basadas en SNMP Workgroup Director se ejecuta en estaciones de trabajo UNIX, ya sea como una aplicación independiente o integrada con otra plataforma de administración de red basada en SNMP, brindando un sistema de gestión poderoso y transparente para los productos de grupo de trabajo de Cisco.

WWW: World Wide Web. Gran red de servidores de Internet la cual suministra servicios de hipertexto y otros a terminales que ejecutan aplicaciones de clientes como, por ejemplo, un navegador de Web. Ver también navegador de Web.