65

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES

"ARAGON"

"PLAN DE CONECTIVIDAD DE LA COMISION DE AVALUOS DE BIENES NACIONALES"

T E S I S

QUE PARA OBTENER EL TÍTULO DE :

INGENIERO EN COMPUTACIÓN

P R E S E N T A :

CESAR ERNESTO VAZQUEZ MORENO

MEXICO D.F. 2001

INDICE

Introducción

El interés por realizar este trabajo de tesis, surge de la necesidad que existe en la Comisión de Avalúos de Bienes Nacionales, de integrar la información y de encontrar la solución a las carencias que se presentan en los sistemas de telecomunicaciones actuales.

La Comisión de Avalúos de Bienes Nacionales (CABIN) es un órgano desconcentrado de la Secretaría de Contraloría y Desarrollo Administrativo que se encarga de controlar administrativa y operativamente los avalúos de los bienes inmuebles de propiedad Federal, ya sea para efectos de compra-venta como de arrendamiento.

Visión

Considerar a la Comisión de Avalúos de Bienes Nacionales como una Institución Pública con autosuficiencia financiera, autonomía de gestión, confiable y eficiente, que preste sus servicios desde una plataforma de productividad, que propicie el ahorro y responda a las necesidades de los promoventes en forma ágil y oportuna.

Su objetivo es coadyuvar con el Gobierno Federal, en la administración, preservación y protección de su patrimonio inmobiliario y en la racionalización del gasto público, mediante la realización de las actividades valuatorias y de justipreciación de rentas que le sean encomendadas, atendiendo siempre al interés público y los aspectos pertinentes de la política inmobiliaria establecida.

Para el ejercicio de sus atribuciones, la CABIN se integra con las siguientes unidades administrativas:

- Presidencia
- Dirección General de Avalúos
- Dirección General del Patrimonio Inmobiliario Federal
- Dirección General de Administración y Obras en Edificios Públicos
- Dirección General Jurídica
- Dirección General de Administración y Finanzas
- Delegaciones Regionales

Así como por los siguientes órganos colegiados:

- Cuerpo Colegiado de Avalúos de Oficinas Centrales
- Cuerpo Colegiado de Avalúos en cada Delegación Regional

La Comisión de Avalúos de Bienes Nacionales (CABIN) se creó el 13 de julio de 1950 con el objetivo de practicar los avalúos de los bienes inmuebles que lo sean por naturaleza o por disposición de la ley, cuando en la operación sean parte las dependencias y entidades de la administración pública federal centralizada y paraestatal y determinar el monto de la renta que estas últimas deben cobrar o pagar por los inmuebles que den o tomen en arrendamiento.

El actual ámbito de facultades de la CABIN ya rebasó la sola materia valuatoria y de justipreciaciones, como lo fue desde sus inicios hace 50 años, pues el Gobierno Federal ha decidido organizar las diversas actividades y atribuciones relacionadas con su patrimonio inmobiliario alrededor de este órgano desconcentrado de la Secretaría de Contraloría y Desarrollo Administrativo.

Por esta razón, la Comisión centra hoy sus actividades en tres áreas fundamentales:

- La primera es el área del patrimonio inmobiliario federal. En ella se llevan a cabo actividades de registro de títulos de propiedad y derechos reales, de catastro, de administración de inmuebles y de archivo, precisamente por la importancia que tiene para todos los mexicanos la preservación física, legal y documental de su patrimonio inmobiliario.

- La segunda es el área responsable de construir mantener y administrar los inmuebles federales de uso compartido por dos o más dependencias o entidades, tales como los 37 palacios federales, los 54 puertos fronterizos y un sin número de hangares y bodegas.

- La tercera es la práctica ya tradicional de los avalúos de bienes inmuebles que lo sean por naturaleza o por disposición de la ley, siempre y cuando en la operación sean parte las dependencias y entidades de la Administración Pública Federal y las justipreciaciones de renta que estas últimas deben cobrar o pagar por los inmuebles que den o tomen en arrendamiento. Adicionalmente, se realizan trabajos valuatorios de activos, como negocio en marcha, maestros, de plantas industriales y de complejos turísticos, entre otros.

Para alcanzar el objetivo anteriormente expuesto, este trabajo se divide en cinco capítulos que a continuación se describen brevemente.

Capítulo I. Marco Problemático

En el capítulo I se identifica el problema de conectividad de la CABIN, se exponen las características generales de la red actual.

Capítulo II. Marco Teórico

El capítulo II presenta todas las fuentes que se consultaron durante la investigación. En él se incluye el acopio de libros, revistas, periódicos, asistencia a conferencias e información obtenida por Internet.

Capítulo III. Marco Conceptual

Este capítulo contiene la información principal obtenida y aprendida con las actividades del capítulo II. Aquí se presentan, algunas aportaciones generales, historia de las redes, topologías, sistemas operativos y el por qué fueron seleccionados.

Capítulo IV. Marco Metodológico

El marco metodológico es la memoria técnica propuesta. para llevar a efecto la compra de material. la distribución de nodos de red y toda la información para la instalación del sistema de cableado estructurado.

Capítulo V. Marco Instrumental

Es la distribución del proyecto en tiempo y actividades para que sea llevado a cabo.

Conclusiones

Aquí se encuentran las conclusiones obtenidas del trabajo de investigación en general.

Anexos

Se presentan como anexos. estándares que se ocupan en los sistemas de cableado estructurado y protocolos de comunicación necesarios para que la red local pueda trabajar.

Capítulo I

Marco Problemático y Propuesta de Proyecto

1.1 Descripción del Problema

En virtud de que existe una problemática seria en cuanto al mal funcionamiento de la red de datos de la CABIN y partiendo de la próxima implantación de nuevos sistemas de información para las áreas Técnica de Administración y Finanzas, es indispensable la realización de un proyecto que abarque la reestructuración de un sistema de cableado estructurado, capaz de soportar estándares y nuevas tecnologías que existen en el mercado, ya que la infraestructura de la red actual no cuenta ni siquiera con las características mínimas, lo cual repercutirá en la consecución exitosa de los proyectos antes mencionados.

La CABIN requiere administrar totalmente la información generada por la operación diaria en los procesos de valuación de bienes inmuebles, por lo cual necesita de una infraestructura de telecomunicaciones robusta y eficiente que soporte los proyectos de comunicaciones y desarrollo de sistemas, que la Comisión de Avalúos de Bienes Nacionales tiene pensado implantar a corto plazo.

Es importante para la CABIN el apoyar los procesos operativos de los diversos departamentos de la Institución con tendencias tecnológicas que representen soluciones informáticas y telemáticas para soportar su labor cotidiana de forma eficiente y flexible, que permitan la convivencia con otros sistemas, para así obtener el beneficio de una base informática corporativa integral.

1.2 Características generales de la red de datos actual

- Es una red IEEE 802.3 con aproximadamente 60 usuarios activos, distribuidos en los pisos del 1 al 7.
- La ubicación de todos los concentradores se encuentra en el sexto piso.
- El cableado está hecho con UTP categoría 5 y el enlace principal está hecho por concentradores en cascada.
- Los concentradores utilizados son marca 3com de 8,12 y 16 puertos, y PalmHub de 8 puertos.
- Los nodos de red son distribuidos a través de plafón, pero sin canalizar y la distribución en las áreas de trabajo se hace directamente al equipo(sin "jacks").
- Varios cables se encuentran sin conectar y muchas conexiones no están rematadas adecuadamente.
- Plataformas de trabajo utilizadas: Windows NT y Unix.
- Servidores: Ordenadores y una estación de trabajo SUN Sparc Classic.
- Equipo de comunicaciones: 1 ruteador Marca Cisco 2500 y 2 DS0's de 64 kbs.

1.3 Principales problemas detectados

- El cableado está mal rematado.
- No existen canalizaciones.
- Los equipos de comunicación están ubicados en lugares polvosos, húmedos, sin iluminación y mecánicamente inestables.
- No existe una memoria técnica (croquis, mapas, tablas de asignación de nodos, usuarios, estándares, etcétera).
- No hay etiquetación.
- El diseño general de un esquema de conectividad no es el adecuado.
- Hay una derivación excesiva en los concentradores.
- Su energización no es la adecuada (no cuentan con fuentes no-interrumpibles de energía).

1.4 Propuesta del Proyecto de Conectividad

El sistema de cableado que se propone será confiable y cumplirá con los estándares especificados para la infraestructura de telecomunicaciones existente en el mercado.

Las Normas a seguir son:

ANSI/EIA/TIA 568
ANSI/EIA/TIA 569
ANSI/EIA/TIA 606
TSB-67

La cantidad de nodos a instalar serán 300, tomando en cuenta el crecimiento esperado de los usuarios de la CABIN.

No se cuenta con la distribución de estos servicios por piso, por lo que se incluye en esta propuesta una memoria técnica.

Se propone también un esquema con tecnologías de conectividad que cumplen con Normas y Estándares de punta que existen en el mercado.

Se utilizará equipo y material existente para minimizar costos.

Etapas del proyecto

Primera

Estudio y estimaciones sobre material, recursos humanos y tiempo de instalación y configuración, además de la planeación y todos los detalles a considerar.

Segunda

Implantación del cableado vertical("Back bone") e instalación de equipo activo.

Tercera

Implementación del cableado horizontal. Cuarto de Comunicaciones y nodos.

Cuarta

Instalación de Servidores(Arquitectura, Sistema Operativo, Servicios)

Quinta

Configuración de los equipos a usuarios, configuración de los dispositivos de red y terminación de detalles e imprevistos.

Sexta

Modificación y entrega de la memoria técnica.

Capítulo II
Marco Teórico

1. ConceptosTeóricos Básicos

El cableado estructurado proporciona varios beneficios en las redes de comunicación, los cuales se mencionan a continuación:

- Mayor velocidad: el cableado estructurado transmite información hasta 10 veces más rápido que un cable coaxial 10 BaseT y con el cable apropiado puede llegar alcanzar una velocidad de 155 Mb/Seg.

- Más seguridad: al ser una topología en estrella cada conexión es individual, lo que impide que haya caídas de grupos de red.

- Mayor flexibilidad: la Norma EIA/TIA 568A para el cableado de edificios comerciales, planifica una instalación de cables de comunicación, sin tener la necesidad del conocimiento previo de las necesidades del usuario, es decir, la telefonía, computación, CTV, etcétera

- Mejor administración: la existencia de un único centro de cables y su documentación de acuerdo a la Norma EIA/TIA 606, facilita su administración.

- Menores costos de mantenimiento: no se necesita contratar personal especializado para realizar cambios de funciones, lo que implica costos e independencia.

- Menor inversión inicial: por instalar un solo sistema de cables para datos y telefonía, existe un ahorro en conductos, mano de obra y materiales.

- Inversión con futuro: El uso de las Normas EIA y TIA es un Estándar reconocido y aprobado por la mayoría de los fabricantes de los productos de comunicación, computación y telefonía, y asegura el rendimiento y la seguridad para la implantación de futuras tecnologías que requieren mayor velocidad en la red.

1.1 Estándares relacionados con el cableado

El Instituto Americano Nacional de Estándares, la Asociación de Industrias de Telecomunicaciones y la Asociación de Industrias Electrónicas (ANSI/TIA/EIA) publican conjuntamente Estándares para la manufactura, instalación y rendimiento de equipo y sistemas de telecomunicaciones y electrónico. Cinco de estos Estándares de ANSI/TIA/EIA son los que definen las características que deben considerarse para la instalación de cableado de telecomunicaciones en edificios. Cada Estándar cubre una parte especifica del cableado del edificio. Los Estándares establecen el cable, arquitectura, diseño y prácticas de instalación requeridas. Cada Estándar ANSI/TIA/EIA menciona Estándares relacionados y otros materiales de referencia. La mayoría de los Estándares

incluyen secciones que definen términos importantes. acrónimos y simbolos.

Los cinco Estándares principales de ANSI/TIA/EIA que gobiernan el cableado de telecomunicaciones en edificios son los siguientes:

- Estándar ANSI/TIA/EIA-570 de Alambrado de Telecomunicaciones Residencial y Comercial Liviano.
- Estándar ANSI/TIA/EIA-568-A de Alambrado de Telecomunicaciones para Edificios Comerciales.
- Estándar ANSI/TIA/EIA-569 de Rutas y Espacios de Telecomunicaciones para Edificios Comerciales.
- Estándar ANSI/TIA/EIA-606 de Administración para la Infraestructura de Telecomunicaciones de Edificios Comerciales.
- Estándar ANSI/TIA/EIA-607 de Requerimientos de Puesta a Tierra y Puenteado de Telecomunicaciones de Edificios Comerciales.

Otros Estándares que comúnmente se consideran para la instalación de cableado estructurado. se mencionan a continuación:

- ISO/IEC 11801 Generic Cabling for Customer Premises.
- National Electrical Code 1996 (NEC).
- Código Eléctrico Nacional 1992 (CODEC) .
- EN 50173.

1.1.1 Estándar ANSI/TIA/EIA 568 cableado estructurado

Alambrado de Telecomunicaciones para Edificios Comerciales. Este Estándar define un sistema genérico de alambrado de telecomunicaciones para edificios comerciales que puedan soportar un ambiente de productos y proveedores múltiples.

El propósito de este Estándar es permitir el diseño e instalación del cableado de telecomunicaciones contando con poca información acerca de los productos de telecomunicaciones que posteriormente se instalarán.

La instalación de los sistemas de cableado durante el proceso de instalación y/o remodelación son significativamente más baratos e implican menos interrupciones que después de ocupado el edificio.(Ver Anexo 1)

1.1.2 Estándar ANSI/TIA/EIA 569 cableado estructurado

Rutas y Espacios de Telecomunicaciones para Edificios Comerciales

Este Estándar reconoce tres conceptos fundamentales relacionados con telecomunicaciones y edificios:

- Los edificios son dinámicos. Durante la existencia de un edificio. las remodelaciones son más

la regla que la excepción. Este Estándar reconoce, de manera positiva, que el cambio ocurre.

- Los sistemas de telecomunicaciones y de medios son dinámicos. Durante la existencia de un edificio, los equipos de telecomunicaciones cambian dramáticamente. Este Estándar reconoce este hecho siendo tan independiente como sea posible, de proveedores de equipo.
- Telecomunicaciones son más que datos y voz.. Telecomunicaciones también incorpora otros sistemas tales como: control ambiental, seguridad, audio, televisión, alarmas y sonido. De hecho, telecomunicaciones incorpora todos los sistemas de bajo voltaje que transportan información en los edificios.

Este Estándar reconoce un precepto de fundamental importancia, que un edificio quede exitosamente diseñado, construido y equipado para telecomunicaciones. Es imperativo que el diseño de las telecomunicaciones se incorpore durante la fase preliminar de diseño arquitectónico. (Ver Anexo 2)

1.1.3 Estándar ANSI/TIA/EIA 606 cableado estructurado

Propone un esquema de administración uniforme independiente de las aplicaciones: especifica los requerimientos administrativos de la infraestructura de telecomunicaciones para edificios nuevos, campus o remodelaciones.

Este Estándar establece guías para dueños, usuarios finales, consultores, contratistas, diseñadores, instaladores y administradores de la infraestructura de telecomunicaciones y sistemas relacionados. (Ver Anexo 3).

1.1.4 Estándar del código de colores

Las etiquetas en los dos extremos deben ser del mismo color.
Las interconexiones hechas entre campos de terminación generalmente son de dos colores.

1.1.5 Estándar ANSI/TIA/EIA TSB 67

Estándar americano de especificaciones de prueba sobre cableados de par trenzado no apantallado.

1.1.6 Estándar EN 50173

Normativa Estándar europea de cableado.

1.1.7 Estándar ISO/IEC 11801

Estándar mundial de cableado. Hace referencia a las siguientes clases de velocidad de transmisión:

A. Sistemas hasta 100 Khz.
B. Sistemas hasta 1 Mhz.
C. Sistemas hasta 16 Mhz.
D. Sistemas hasta 100 Mhz.

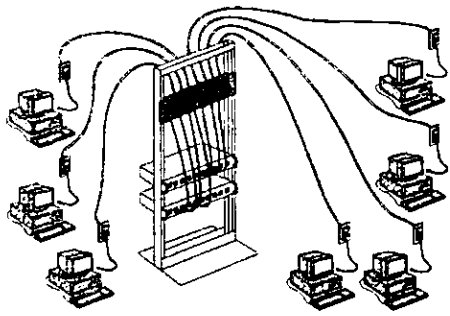


Figura 1.Panel de Parcheo en un esquema de cableado estructurado.

1.2 Cuarto de Telecomunicaciones (SITE)

Un cuarto de telecomunicaciones es el área en un edificio utilizada para el uso exclusivo del equipo asociado con el sistema de cableado. El espacio del "SITE" no debe ser compartido con instalaciones eléctricas que no sean de telecomunicaciones: debe ser capaz de albergar equipo de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado.

El diseño debe considerar, además de voz y datos, la incorporación de otros sistemas de información del edificio tales como: televisión por cable (CATV), alarmas, seguridad, audio y otros sistemas de telecomunicaciones. Todo edificio debe contar con al menos un "SITE" de telecomunicaciones o cuarto de equipo, no hay un límite máximo en la cantidad de cuartos de telecomunicaciones que pueda haber en un edificio.

1.2.1 Consideraciones de diseño

El diseño de un Cuarto de Telecomunicaciones depende de:

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

1.2.2 Altura

La altura mínima recomendada del cielo raso es de 2.6 metros.

1.2.3 Ductos

El número y tamaño de los ductos utilizados para acceder al cuarto de telecomunicaciones varía con respecto a la cantidad de áreas de trabajo, sin embargo se recomienda por lo menos tres ductos de 100 milímetros (4 pulgadas) para la distribución del cable del backbone.

Los ductos de entrada deben contar con elementos de retardo de propagación de incendio «firestops».

1.2.4 Puertas

La(s) puerta(s) de acceso debe(n) ser de apertura completa, con llave y al menos de 91 centímetros de ancho y 2 metros de alto. La puerta debe ser removible y abrir hacia afuera (o de lado a lado). La puerta debe abrir al ras del piso y no debe tener postes centrales.

1.2.5 Polvo y electricidad estática

Se debe evitar el polvo y la electricidad estática utilizando piso de concreto, terrazo, loza o similar (no utilizar alfombra). De ser posible, aplicar tratamiento especial a las paredes pisos y cielos para minimizar el polvo y la electricidad estática.

1.2.6 Control ambiental

En cuartos que no tienen equipo electrónico la temperatura del cuarto de telecomunicaciones debe mantenerse continuamente (24 horas al día, 365 días al año) entre 10 y 35 grados centígrados. La humedad relativa debe mantenerse menor a 85%. Debe haber un cambio de aire por hora.

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

1.2.7 Plafón

Se debe evitar el uso de plafón en los cuartos de telecomunicaciones.

1.2.8 Prevención de inundaciones

Los cuartos de telecomunicaciones deben estar libres de cualquier amenaza de inundación. No debe haber tubería de agua pasando por (sobre o alrededor) el cuarto de telecomunicaciones. De haber riesgo de ingreso de agua, se debe proporcionar drenaje de piso. De haber regaderas contra incendio, se debe instalar una canoa para drenar un goteo potencial de las regaderas.

1.2.9 Iluminación

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

1.2.10 Localización

Con el propósito de mantener la distancia horizontal de cable promedio en 46 metros o menos

(con un máximo de 90 metros), se recomienda localizar el cuarto de telecomunicaciones lo más cerca posible del centro del área a servir.

1.2.11 Potencia

Debe haber tomacorrientes suficientes para alimentar los dispositivos a instalarse en los andenes. El Estándar establece que debe haber un mínimo de dos tomacorrientes dobles de 110V C.A. dedicados de tres hilos. Deben ser circuitos separados de 15 a 20 amperios. Estos dos tomacorrientes podrían estar dispuestos a 1.8 metros de distancia uno de otro. Considerar la alimentación eléctrica de emergencia con activación automática. En muchos casos es deseable instalar un panel de control eléctrico dedicado al cuarto de telecomunicaciones. La alimentación específica de los dispositivos electrónicos se podrá hacer con UPS y regletas montadas en los andenes.

Separado de estas tomas debe haber tomacorrientes dobles para herramientas, equipo de prueba etc. Estos tomacorrientes deben estar a 15 cm. del nivel del piso y dispuestos en intervalos de 1.8 metros alrededor del perímetro de las paredes.

El cuarto de telecomunicaciones debe contar con una barra de puesta a tierra que a su vez debe estar conectada a un cable de mínimo 6 AWG con aislamiento verde al sistema de puesta a tierra de telecomunicaciones según las especificaciones de ANSI/TIA/EIA-607

1.2.12 Seguridad

Se debe mantener el cuarto de telecomunicaciones con llave en todo momento. Se deben asignar llaves al personal que esté en el edificio durante las horas de operación.

Se debe mantener el cuarto de telecomunicaciones limpio, ordenado y cerrado.

1.2.13 Requisitos de tamaño

Debe haber al menos un cuarto de telecomunicaciones o cuarto de equipo por piso y por áreas que no excedan los 1000 metros cuadrados. Instalaciones pequeñas podrán utilizar un solo cuarto de telecomunicaciones si la distancia máxima de 90 metros no se excede.

Área a Servir Edificio Normal	**Dimensiones Mínimas del Cuarto de Alambrado**
500 m^2 o menos	3.0 m. x 2.2 m.
Mayor a 500 m^2, menor a 800 m^2	3.0 m. x 2.8 m.
Mayor a 800 m^2, menor a 1000 m^2	3.0 m. x 3.4 m.

Área a Servir Edificio Pequeño	**Utilizar para el Alambrado**
100 m. o menos	Montante de pared o gabinete encerrado.
Mayor a 500 m^2, menor a 800 m^2	Cuarto de 1.3 m. x 1.3 m. o Closet angosto de 0.6 m. x 2.6 m.

* Algunos equipos requieren un fondo de al menos 0.75 m.

1.2.14 Disposición de equipos

Los andenes ("racks") deben contar con al menos 82 cm. de espacio de trabajo libre alrededor (al frente y detrás) de los equipos y páneles de telecomunicaciones. La distancia de 82 cm. se debe medir a partir de la superficie más salida del andén de acuerdo al NEC, NFPA-70 Artículo 110-16, debe haber un mínimo de 1 metro de espacio libre para trabajar equipo con partes expuestas sin aislamiento.

Todos los andenes y gabinetes deben cumplir con las especificaciones de ANSI/EIA-310. La tornillería debe ser métrica M6.

Se recomienda dejar un espacio libre de 30 cm. en las esquinas.

1.2.15 Paredes

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

1.3 UTP

En este tipo de cable, los conductores aislados se trenzan entre sí en pares y todos los pares del cable a su vez. Esto reduce las interferencias entre pares y la emisión de señales. Estos cables se utilizan, sobre todo, para los sistemas de cableado integral, combinando telefonía y redes de transmisión de datos, principalmente 10baseT.

Se clasifican en 5 categorías:

- Categoría 1 - Se utiliza para voz, analógica y digital; hasta 20.000 bps.
- Categoría 2 - Utilizado para voz y aplicaciones de datos; hasta 4 Mbps.
- Categoría 3 - Usado en aplicaciones LAN de alta velocidad; hasta 16 Mbps.

Figura 2. Cable UTP Nivel 5

- Categoría 4 - Utilizado de preferencia en Token Ring; hasta 20 Mbps.
- Categoría 5 - Se usa en aplicaciones de LAN de muy alta velocidad; 100 Mbps. (FDDI sobre cobre, ATM Norma TAXI) y se está estudiando su aptitud para alcanzar 155 Mbps. (ATM Norma OC-3).(Ver Anexo 5)

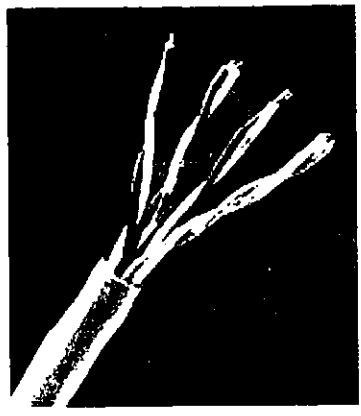


Figura 3. Trenzado característico del cableado UTP Nivel 5

1.3.1 Cable UTP categoría 5

Estructura del cable.- El cable UTP para redes actualmente empleado es el de 8 hilos categoría 5, es decir cuatro pares trenzados formando una sola unidad. Estos cuatro pares vienen recubiertos por una vaina plástica que mantiene el grupo unido, mejorando la resistencia ante interferencias externas. Es importante notar que cada uno de los cuatro pares tiene un color diferente, pero a su vez, cada par tiene un cable de un color específico y otro blanco con algunas franjas del color de su par, tal como se muestra en la figura 3.

Esta disposición de los cables permite una adecuada y fácil identificación de los mismos con el objeto de proceder a su instalación.

Vale la pena indicar que el cable UTP tiene un pariente muy cercano, el STP o Par Trenzado Blindado, con una mayor protección contra interferencias, aunque lamentablemente con un precio mayor. Todo Administrador de red sabe perfectamente que el cable UTP es por demás suficiente para cualquier tipo de exigencia, aunque su resistencia a interferencias no es la del STP, es mas alta, cuando es tendido por canaletas.

Conector RJ-45: Este conector es el que ha brindado un gran empuje a estas redes, pues es

muy sencillo conectarlo a las tarjetas y a los concentradores, además es seguro gracias a un mecanismo de enganche que posee, mismo que lo mantiene firmemente ajustado a otros dispositivos, no como en el cable coaxial donde permanentemente se presentan fallas en la conexión.

Figura 4. Conectores RJ-45

La figura 4 muestra el conector RJ-45, con 8 contactos para los 8 hilos del cable UTP, tanto de perfil como una vista superior e inferior. En este punto cabe indicar que el orden de los colores está estandarizado, justamente en la forma en que se muestra en la figura 3.

Un aspecto general a toda instalación de este tipo de cableado es que todos los elementos deben corresponder a la categoría 5, ya que esto asegura que todos los elementos del cableado pueden soportar las mismas velocidades de transmisión, resistencia eléctrica, etcétera. El conector en este caso no es la excepción.

1.4 TCP/IP

Aunque poca gente sabe lo que es TCP/IP todos lo emplean indirectamente y lo confunden con un solo protocolo cuando en realidad son varios, de entre los cuales destaca y es el más importante el protocolo IP. Bajo este nombre(TCP/IP)se esconde uno de los protocolos más usados del mundo, debido a que es el más usado por Internet y está muy extendido en el sistema operativo UNIX.

En 1973 , la DARPA inició un programa de investigación de tecnologías de comunicación entre redes de diferentes características. El proyecto se basaba en la transmisión de paquetes de información y tenía por objetivo la interconexión de redes. De este proyecto surgieron dos redes: una de investigación, ARPANET, y una de uso exclusivamente militar, MILNET. Para comunicar las redes, se desarrollaron varios protocolos: El Protocolo de Internet y los protocolos de control de transmisión. Posteriormente estos protocolos se englobaron en el conjunto de protocolos TCP/IP.

En 1980, se incluyó en el UNIX 4.2 de BERKELEY, y fue el protocolo militar Estándar en 1983. Con el nacimiento en 1983 de INTERNET, este protocolo se popularizó bastante y su destino va unido al de Internet. ARPANET dejó de funcionar oficialmente en 1990. (Ver Anexo 4)

1.5 Ruteo

Ruteo es el acto de mover información a través de redes, desde un punto de origen a un punto destino, en esta ruta. Al menos encontramos un punto intermedio. A menudo el ruteo puede parecerse al puenteo, sin embargo son cosas diferentes pero puede pasar inadvertido por un observador casual.

La diferencia principal entre ambos es que el puenteo ocurre en la capa 2 (capa de enlace) del Modelo OSI y el ruteo ocurre en la capa 3 (capa de red). Esta característica le da al ruteo y puenteo información diferente para usar en el proceso de mover la información del origen al destino, así que las dos funciones cumplen sus tareas de diferente manera.

El tema de Ruteo ha sido cubierto por las ciencias de la computación hace más de 2 décadas, pero el ruteo alcanzó la popularidad comercial a mediados de los 80's aunque con mucho retraso.

La razón principal de este retraso es que las redes en los años 70's eran muy simples y los ambientes eran muy homogéneos. (Ver anexo 5)

Capítulo III

Marco Conceptual

1. Concepto de Redes

En su nivel más elemental, una red consta de dos ordenadores conectados entre sí, por un cable, de modo que puedan compartir datos. Todas las redes, no importa que complejas sean, provienen de esta forma. Mientras que la idea de conectar dos ordenadores por un cable, no parece extraordinaria, fue un logro muy importante en las comunicaciones.

Las redes nacen de la necesidad de compartir datos oportunamente, los ordenadores personales son una herramienta maravillosa para producir documentos, hojas de cálculo, gráficas y otros tipos de información, pero no permiten compartir de manera rápida los datos que se han producido. Sin una red, los documentos tienen que imprimirse para que otros puedan editarlos o utilizarlos. En el mejor de los casos se tienen que dar los archivos en diskettes a otras personas para que sean copiados en sus ordenadores, si la otra persona hace cambios al documento no hay manera de juntar los cambios, esto se conoció y se sigue conociendo, como trabajo en ambiente independiente ("stand-alone").

Figura 6. Ambiente de trabajo independiente.

Un grupo de ordenadores y otros dispositivos conectados en conjunto, es llamado "red" ("Network") y el concepto de ordenadores conectados y que comparten recursos es llamado "Implantación de una Red" ("Networking").

Figura 7 Ambiente de trabajo en red.

Los ordenadores que son parte de una red pueden compartir lo siguiente:

- Datos
- Mensajes
- Gráficas
- Impresoras
- Fax
- Modems
- Otros recursos de la arquitectura

2. Red de Area Local

Las redes comenzaron probablemente en diez ordenadores conectados entre sí con una impresora. La tecnología limitó el tamaño de las redes, incluyendo el número de ordenadores conectados y la distancia que puede haber entre ellas. Por ejemplo a principios de los 80 el método más popular de cableado permitiría cerca de 30 usuarios sobre un largo máximo de cable de 180 metros aproximadamente. Tales redes podrían estar en el piso de un edificio o dentro de una pequeña compañía. Para muchas compañías de hoy, esta configuración todavía es adecuada. Este tipo de redes, dentro de un área limitada es conocida como "Red de un Área Local" (LAN)

2.1 La expansión de las redes

Las primeras LAN no podían adecuarse a las necesidades de las redes de los negocios grandes ya que éstos tenían oficinas en varios lugares y como ya se conocían las ventajas de las redes, se fueron desarrollando más aplicaciones para trabajar sobre este ambiente, los grandes negocios vieron la necesidad de extender sus redes, para permanecer en la competencia. Hoy en día las LAN se han convertido en los pilares de las grandes empresas.

El alcance de las redes cambia cuando se conectan usuarios en diferentes ciudades o países, la LAN crece y se convierte en una WAN(Red de Área Amplia). El número de usuarios en una compañía puede crecer ahora en miles.

Hoy, la mayoría de los grandes negocios almacenan y comparten una gran cantidad de datos importantes, están en un ambiente de red, esto es, porque las redes son actualmente tan esenciales para los negocios, como las máquinas de escribir o los archiveros.

2.2 ¿Por qué usar una Red?

Las organizaciones implantan redes principalmente para compartir recursos y habilitar comunicaciones en línea. Los recursos incluyen datos, aplicaciones y periféricos. Un periférico es un dispositivo, como un disco duro externo, una impresora, un ratón, Un MODEM o un control para juegos. La comunicación en línea incluye enviar mensajes a otros usuarios que están conectados en ese instante o enviar correo electrónico.

2.3 Impresoras y otros periféricos

Antes de las ventajas de la red, los usuarios necesitaban imprimir trabajos en sus propios graficadores, impresoras y otros periféricos. Antes de que las redes existieran, la única forma de compartir una impresora era esperar el turno en un ordenador, sentarse y conectar la impresora.

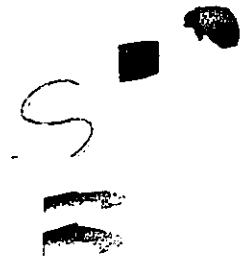


Figura 8 Periféricos y otros dispositivos

Las redes ahora hacen posible que varias personas compartan tanto datos como impresoras simultáneamente, si mucha gente necesita usar una impresora, ellos pueden utilizar todas las impresoras disponibles en la red.

Figura 9 La información y los recursos son compartidos en un ambiente de red

2.4 Datos

Antes de que existieran las redes, la gente que quería compartir información estaba limitada a:

- Decir la información en forma verbal
- Escribir Memorandos.
- Poner la información en un disquete, tomarlo físicamente, llevarlo a otro ordenador y copiar los datos.
- Las redes pueden reducir la necesidad de la comunicación vía papel y hacer más fácil el acceso a cualquier información y hacerla disponible para todas las personas que la necesiten.

2.5 Aplicaciones

Las redes pueden ser usadas para normalizar las aplicaciones, como procesadores de palabra, hojas de cálculo; de esta forma se asegura que todos en la red usen la misma aplicación y la misma versión, esta normalización puede simplificar las tareas de soporte y es más fácil conocer muy bien una sola aplicación que aprender cuatro o cinco diferentes, lo mismo pasa con las versiones ya que se instalan de igual manera todas las aplicaciones de la red.

La mayoría de los negocios invierten en redes por el correo electrónico y las tareas programadas, los administradores pueden usar estas utilerías para comunicarse rápida y efectivamente con un gran número de personas y para programar una compañía entera en las tareas que se realizan cotidianamente.

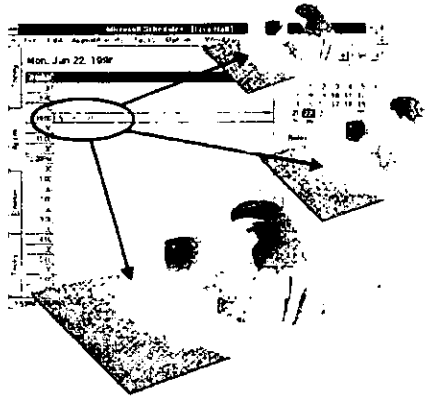


Figura 10 Normalización de aplicaciones

3 Los 2 grandes tipos de redes

3.1.1 Redes punto a punto

En este tipo de redes, no existe un servidor dedicado o jerarquía entre ordenadores, todos los ordenadores son iguales y por lo tanto ambos son cliente/servidor y no hay uno asignado a la administración de la red . el usuario de cada ordenador determina qué información de su ordenador va a compartirse en la red.

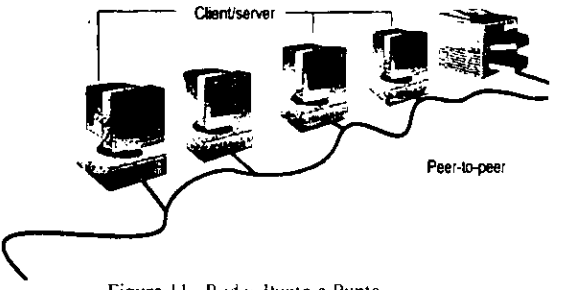


Figura 11 Redes Punto a Punto

3.1.2 Tamaño

Las redes punto a punto son también llamadas Trabajo en Grupo(WorkGroups). El término trabajo en grupo implica un grupo pequeño de personas, en este tipo de redes típicamente existen conectadas diez personas o menos.

3.1.3 Costo

Estas redes son relativamente simples. Por que cada ordenador funciona como cliente/servidor, no hay necesidad de un servidor central o de otros componentes de alta capacidad en la red. Esta red puede ser mas barata que una red basada en servidor.

3.1.4 Sistema Operativo

En estas redes los programas no necesitan tener el mismo nivel de ejecución y seguridad como los programas diseñados para las redes basadas en servidor.

En un sistema operativo como Windows 95, Windows para Trabajo en Grupo, ya vienen diseñados para trabajar con este tipo de redes, no se requiere de programa adicional para configurar una red de este tipo.

3.1.5 Implantación

En un ambiente típico de una red punto a punto, las consideraciones a tratar ya son estándares

por lo que la implementación tiene que incluir lo siguiente:

Los ordenadores tienen que estar ubicados en el escritorio del usuario.
El usuario actúa como su propio administrador y planea su propia seguridad.
Un simple, visible y fácil sistema de cableado es usado. el cual conecta el ordenador a la red.

¿Dónde es apropiado este tipo de redes?

Es una buena opción en ambientes donde:

- Hay diez o menos usuarios.
- El usuario está ubicado en la misma área
- La seguridad no es un objetivo
- No se contempla un crecimiento excesivo
- Considerando estas referencias, hay ocasiones en que este tipo de redes son la mejor solución.

3.2 Red Basada en Servidor

En una red que tiene más de diez usuarios, una red punto a punto no es la adecuada, por lo tanto las redes tienen un servidor dedicado. Un servidor dedicado es aquel que no funciona como cliente o estación de trabajo. Este servidor es "dedicado" porque está optimizado para agilizar el servicio de peticiones hechas por los clientes de red, y se encarga de la seguridad de archivos y directorios, las redes bajo este esquema se han vuelto el modelo estándar para las redes.

A medida que las redes incrementan su tráfico y su tamaño, más de un servidor es necesitado, separando las tareas entre varios servidores asegurándose que cada tarea sea ejecutada de la forma más eficiente posible.

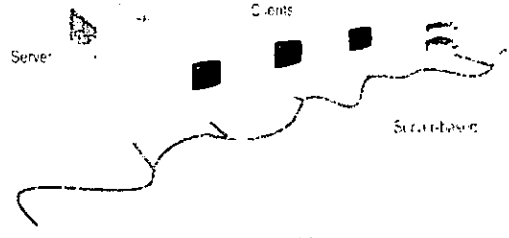


Figura 12 Redes basadas en servidores

3.2.1 Servidores especializados

La variedad de tareas que los servidores deben ejecutar son variadas y complejas. Los servidores de las redes grandes se convierten en especializados para acomodar las necesidades de los usuarios que crecen constantemente.

Pueden existir servidores para diferente servicios, por ejemplo:

Servidor de Archivos e Impresión

Maneja el acceso a los recursos de impresoras y archivos, por ejemplo si se usa una comunicación de un procesador de palabras, esta aplicación se ejecuta en el ordenador pero el archivo se encuentra almacenado en el servidor de archivos, de esta forma al utilizar el archivo el ordenador lo almacena en su memoria y lo trabaja localmente, en otras palabras este tipo de servidores se utilizan para la impresión y el almacenaje de datos y archivos.

Servidores de Aplicación

Estos servidores proporcionan los datos con los que trabajan las aplicaciones cliente/servidor, por ejemplo los servidores almacenan una gran cantidad de datos que están estructurados de cierta forma que hacen más fácil su consulta, esto difiere del servidor de archivos e impresión ya que en el servidor de aplicación se queda la base de datos y sólo se envía al cliente el resultado de la solicitud de información, en lugar de enviarse todo el archivo.

Una aplicación cliente corre localmente y debe tomar los datos de un servidor de aplicación en vez de bajar la base de datos completa a la memoria del ordenador

Servidor de correo

Estos servidores manejan el correo electrónico de usuarios en diferentes redes.

Servidor de Faxes

Maneja el tráfico de faxes dentro de una red, compartiendo una o más tarjetas de fax-modem.

Figura 13 Esquema de servidores especializados

Servidores de comunicación

Manejan el flujo de datos y mensajes de correo electrónico en la misma red o en otras redes, "mainframes" o usuarios que usan Modems y líneas telefónicas para conectarse al servidor.

3.2.2 Ventajas de una red basada en servidor

Compartición de recursos

Un servidor está diseñado para proveer acceso a muchos archivos e impresoras mientras mantiene un nivel de ejecución y seguridad para el usuario.

El control y la administración de datos se vuelve centralizado en este esquema, esta forma es más fácil que si estuvieran los datos dispersos en varios ordenadores.

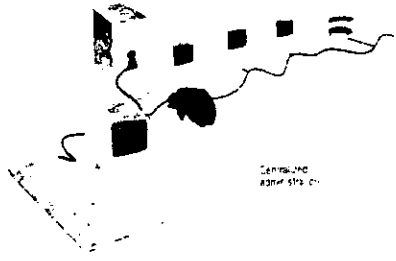


Figura 14 Seguridad en servidores

Seguridad

Debe ser la razón primordial para escoger este tipo de esquema ya que se aprovechará mejor la red, en este ambiente la seguridad será manejada por un administrador quien pondrá las políticas y las aplicará a los usuarios.

Respaldos

Porque los datos importantes están centralizados en uno o varios servidores, siempre es necesario respaldarlos para asegurar que la información siempre estará segura y disponible en caso de cualquier percance.

Redundancia

A través de los sistemas en redundancia los datos en cualquier servidor pueden ser duplicados y guardados en línea, por si algo llega a suceder a la fuente primaria de almacenamiento, la copia puede ser utilizada para continuar con el trabajo.

3.2.3 Razones por las cuales se escogió una red basada en servidor

- Se utilizarán aplicaciones cliente/servidor.
- Provee gran seguridad y más control.
- La cantidad de usuarios a manejar es de 500.
- La CABIN requiere un sistema centralizado de monitoreo y administración.
- Los recursos compartidos necesitan tener restricciones y ser regulados.
- Se utilizará más de un Servidor.
- Los servidores tendrán tareas específicas.

4 Diseño de la Red

El término topología o más específicamente topología de red se refiere al arreglo físico de los ordenadores, cables y otros componentes de la red. Topología es el término estándar que la mayoría de los profesionales ocupa cuando se refiere al diseño básico de la red.

Escoger una topología de red determinada impacta en:

- El tipo de equipo de red que se necesite
- Capacidades de equipamiento
- Crecimiento de la red
- La manera en que la red será administrada

Desarrollar un buen sentido de cómo las topologías son usadas es una buena herramienta para entender las capacidades de los diferentes tipos de redes.

Los ordenadores serán conectados según compartan recursos o realicen alguna tarea de comunicación, la red debe usar cable para conectar un ordenador con otro. Sin embargo esto no es tan fácil como enchufarle un cable a el ordenador y conectarlo con otro. Diferentes tipos de cables, combinados con diferentes tipos de tarjetas de red, sistemas operativos de red y otros componentes requieren diferentes tipos de arreglos.

Una topología de red implica un cierto número de condiciones, por ejemplo, una topología en particular puede no determinar el tipo de cable usado pero sí cómo va ir colocado sobre el piso, paredes, mamparas.

Una topología puede determinar cómo los ordenadores se comunican en la red. diferentes topologías requieren diferentes métodos de comunicación y estos métodos tienen una gran influencia sobre la red.

4.1 Estándares de topologías

Todas las redes se diseñan en base a 3 topologías:

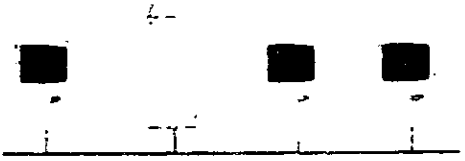


Figura 15 Topología de Bus

- Bus
- Estrella
- Anillo

La topología de bus es conocida también como de "bus lineal". Este es el método más simple y común de conectar una red. Este consta de un sólo cable, llamado "Backbone" o segmento que conecta a todos los ordenadores en la red en una sola línea.

4.1.1 Comunicación sobre el bus

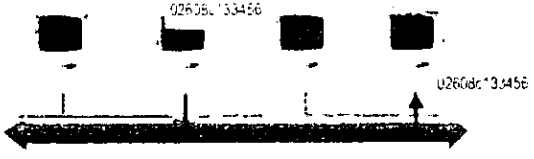


Figura 16 Comunicación sobre el bus

Los ordenadores sobre una red de topología bus se comunican por una dirección de datos y ponen sus datos en el cable en forma de señal electrónica

Los datos son enviados en forma electrónica a todos los ordenadores de la red, sin embargo, la información es aceptada sólo por el ordenador con el que coincida la dirección proveniente del mensaje original y sólo un ordenador a la vez puede enviar mensajes.

Como sólo un ordenador puede enviar mensajes a la vez, el funcionamiento de la red es afectado por el número de ordenadores conectados al bus. A más ordenador en el bus más es el tiempo de espera en que cada ordenador pone su mensaje en el bus y la red se vuelve lenta.

No hay una medida estándar para el impacto de número de ordenadores sobre la red, la cantidad de veces que la red esta lenta, no está relacionada exclusivamente con el número de ordenadores sobre la red, esto depende de un cierto número de factores entre los que destacan:

- Capacidades de arquitectura de los ordenadores en la red.
- Número de veces que los ordenadores trasmiten datos
- El tipo de aplicación que esté en ejecución en la red
- El tipo de cable usado en la red
- Distancia entre ordenadores en la red

La topología de bus es pasiva. Los ordenadores sólo están escuchando el bus por si los datos enviados van para ellos, no hay responsable por los datos que se mueven de un ordenador a otro. Si un ordenador falla, esto no afecta al resto de la red, en una topología activa los ordenadores regeneran la señal y mueven los datos a través de la red.

4.1.2 Señal de Anuncio

La señal viaja de un extremo al otro del cable. Si la señal fuera permitida para continuar ininterrumpidamente, esta señal se mantiene al principio y al final del cable para prevenir que otros ordenadores envíen señales, después de esto la señal debe ser detenida una vez que haya alcanzado la dirección del destino

4.1.3 Terminador

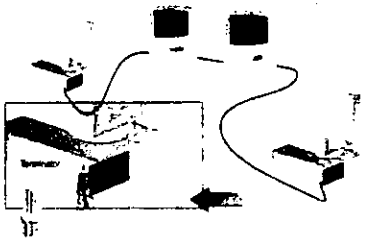


Figura 17 Terminador

Para detener las señales de anuncio, un componente llamado terminador es colocado en cada extremo del cable para absorber las señales libres. Al absorber estas señales el cable queda limpio para que otro ordenador pueda enviar datos.

Cada extremo del cable debe estar conectado a algo, por ejemplo un extremo puede estar conectado a un ordenador o a un conector para extender el largo cable, cualquier extremo abierto del cable debe ser terminado para prevenir las señales de anuncio.

4.1.3 Comunicación Rota

Una interrupción en la red va a ocurrir cuando el cable es físicamente cortado en dos o más piezas o si un extremo del cable se desconecta, en ambos casos uno o más extremos del cable no tienen terminador, la señal se convierte en Anuncio y toda la actividad de la red se va a detener. Esto se conoce como "la red está abajo".

Los ordenadores van a trabajar pero sin comunicación entre ellos.

4.2 Estrella

En esta topología los ordenadores son conectados por cables a un componente centralizado llamado concentrador. Las señales son transmitidas desde un ordenador a través del concentrador a todos los ordenadores de la red. Esta topología fue la primera en utilizarse para conectar los grandes servidores.

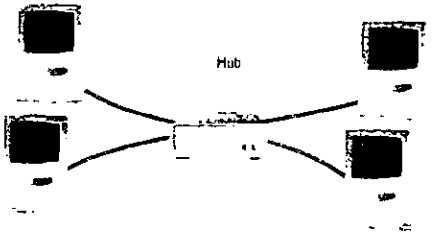


figura 18 Topología de Estrella

La red en estrella ofrece recursos y administración centralizada, sin embargo como cada ordenador está conectado a un punto central, esta topología requiere de un gran manejo de cable en las grandes instalaciones de redes, además de que si el punto central falla, la red entera se cae.

Si un ordenador o cable que está conectado al concentrador falla, sólo ese ordenador queda fuera de la red no enviará datos, el resto de los ordenadores trabajarán normalmente.

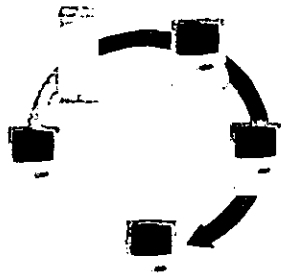


Figura 19 Topología de Anillo

4.3 Anillo

Esta topología conecta a los ordenadores en un sencillo anillo de cable, no hay extremos, la señal viaja a través del anillo en círculos en una dirección y pasa a través de cada ordenador, a diferencia de la topología de bus pasiva, cada ordenador actúa como repetidor de la señal y reenvía la señal al siguiente ordenador ya que la señal pasa por cada una de ellas, la falla de un ordenador impacta en toda la red.

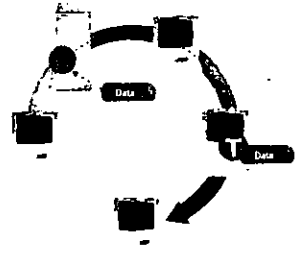


Figura 20 Transmisión del "Token"

4.3.1 Token Passing

El método de Transmisión de datos a través del anillo es conocido como "Token Passing". El "token" es pasado de ordenador en ordenador hasta que uno lo toma para enviar datos, el ordenador que va a enviar datos modifica el "token", pone la dirección electrónica sobre el dato y lo envía a través del anillo.

El dato es pasado por cada ordenador hasta que encuentra quien tenga la dirección del dato.

El ordenador que recibe el dato regresa el mensaje al ordenador que envía indicando que el mensaje ha sido recibido, después de la verificación, el ordenador que envía crea un nuevo "token" y lo libera en la red.

Podría parecer que este método toma mucho tiempo, pero actualmente el "token" viaja a velocidades extremadamente rápidas, Un "token" puede circular en un anillo de 200 metros de diámetro en aproximadamente 10,000 veces por segundo.

4.4 Concentradores

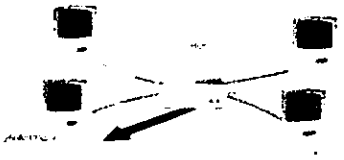


Figura 21 Esquema de Concentradores

Es un componente de red que se ha convertido en un equipo estándar en la mayoría de las redes. En una topología de red, el concentrador es el equipo central.

4.4.1 Concentradores Activos

La mayoría de los Concentradores son activos ya que regeneran y transmiten la señal de la misma forma que lo hace un repetidor. Los concentradores usualmente tienen 8, 12, 24 puertos para conectar los ordenadores a la red, en algunas ocasiones son conocidos como repetidores multipuertos, estos equipos requieren de energía eléctrica para trabajar.

4.4.2 Concentradores Pasivos

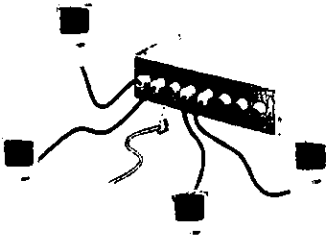


Figura 22 Una ruptura en este esquema afecta solo al segmento, la red sigue trabajando.

Algunos tipos de Concentradores son pasivos, por ejemplo: algunos "closets" de cableado o páneles de parcheo que actúan como puntos de conexión pero no amplifican o regeneran la señal, y éstos no requieren de energía eléctrica para trabajar.

4.4.3 Concentradores Híbridos

Los concentradores modernos que trabajan con varios tipos de cables son llamados concentradores híbridos. Una red basada en concentradores puede ser ampliada conectando más de un concentrador.

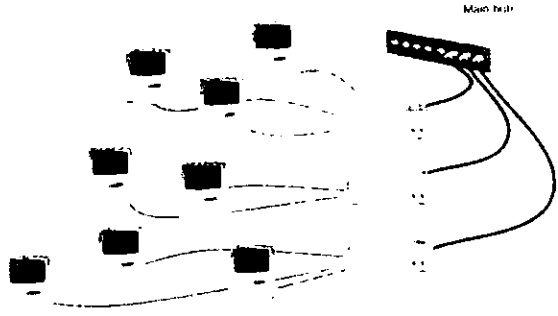


Figura 23 Concentradores Híbridos

4.4.4 Consideraciones de los Concentradores

Estos dispositivos son versátiles y ofrecen varias ventajas sobre redes que no tienen concentradores, en la topología estándar de bus lineal, una ruptura en el cable va a provocar que la red se caiga. Con la topología de Bus, sin embargo, una ruptura en cualquiera de los cables conectados al concentrador sólo afecta a ese segmento, el resto de la red se mantiene funcionando.

Otros beneficios de las topologías basadas en concentradores son:

Cambian o amplían el sistema de cableado como se necesite, simplemente conectando otro ordenador a otro concentrador.

Usa diferentes puertos para acomodar una variedad de tipos de cable.

Centraliza el monitoreo de la actividad y tráfico, muchos concentradores activos contienen características de diagnóstico para indicar dónde hay o no conexión.

4.5 Combinación de Topologías

4.5.1 Bus en Estrella

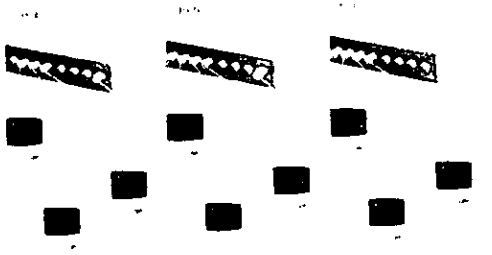


Figura 25 Combinación de Topologías Bus-Estrella

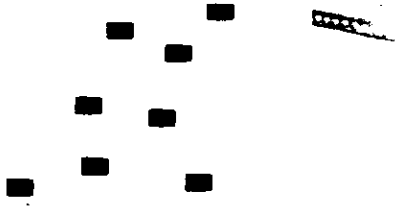


Figura 26 Combinación de topologías Anillo-Estrella

Es una combinación de la topología de bus y estrella. en esta topología hay varias redes en topología estrella enlazadas por un bus lineal.

Si un ordenador se cae, no afectará al resto de la red, si un concentrador se cae. todos los ordenadores sobre el concentrador pierden la comunicación y si este concentrador está conectado a otro esta comunicación se va a perder también.

4.5.2 Anillo en estrella

Es parecida a la bus en estrella, es concentrado en un concentrador el cual contiene el anillo. en esta topología los concentradores son conectados a un concentrador principal.

4.5.3 Razones por las cuales se instalará una red tipo Bus en estrella.

- Fácil de modificar y de agregar nuevos ordenadores.
- Centraliza el monitoreo y administración.
- La falla de un ordenador no afecta en el desempeño de la red.
- El número de usuarios contemplados es de 500.
- Es la topología más económica.
- No hay mucho espacio para utilizar tubería.
- Es fácil detectar falla.

5. Ethernet: como arquitectura de red de la CABIN

5.1 Orígenes de Ethernet

En 1960, cuando la ARPANET sólo llevaba unos meses en funcionamiento, un equipo de la Universidad de Hawai, dirigido por Norman Abramson, quería poner en marcha una red para interconectar terminales ubicadas en las islas de Kauai, Maui y Hawai, con un ordenador central situado en Honolulu, en la isla de Oahu.

Abramson y su equipo consiguieron varios transmisores de radio taxis con los cuales, mediante modems hechos de manera artesanal, pusieron en marcha una red de radio enlaces entre las islas. En lugar de asignar un canal diferente para la comunicación de Oahu hacia y desde cada isla (lo cual habría requerido seis canales), se asignaron únicamente dos: uno a 413,475 MHz para las transmisiones de Oahu a las demás islas y otro a 407,350 MHz para el sentido inverso.

El canal de Oahu no planteaba problemas pues tenía un único emisor. Sin embargo, el canal de retorno era compartido por tres emisores (Kauai, Maui y Hawaii), por lo que se requería un protocolo de control de acceso al medio (MAC; Media Access Control). Esta red se llamó ALOHANET y el protocolo utilizado se llamó ALOHA.

El funcionamiento de ALOHA es muy simple: Cuando un emisor quiere transmitir una trama, simplemente la emite sin preocuparse si el canal está libre. Una vez que termina, se pone a la escucha esperando recibir la confirmación de que la información ha sido recibida correctamente por el destinatario. Si la confirmación no llega en un tiempo razonable, el emisor supone que ha ocurrido una colisión, en cuyo caso espera un tiempo aleatorio y reenvía la trama.

Debido a la constante colisión de las estaciones, cuando los emisores coincidían en tiempo o en bits, dos años más tarde se propuso una mejora al protocolo ALOHA, la cual consistía en establecer de antemano unos intervalos de tiempo de duración constante para la emisión de las tramas. De alguna manera las estaciones estarían sincronizadas y todas sabrían cuándo empezaría cada intervalo. A esta mejora en el protocolo se le denominó ALOHA ranurado porque utilizaba tiempo ranurado (a intervalos).Mientras Abramson montaba ALOHANET en 1970, un estudiante llamado Robert Metcalfe, quien estudiaba la red de Abramson, planteó mejoras que podrían introducirse al protocolo ALOHA para aumentar su rendimiento. La idea básica era muy simple: antes de transmitir, las estaciones deberían detectar si el canal ya estaba en uso, en cuyo caso esperarían a que la estación activa terminara

de transmitir. Además, mientras cada estación transmitía, estaría vigilando el medio físico continuamente por si se producía alguna colisión. Si esto ocurría, pararía y transmitiría más tarde. Años después, este protocolo MAC recibiría la denominación CSMA/CD (Carrier Sense Multiple Access/Collision Detect: Acceso múltiple con detección de portadora/Detección de colisiones).

En 1972 Metcalfe comenzó a trabajar en el Centro de Investigación de Xerox en Palo Alto, California. Se le encomendó la tarea de conectar ordenadores e impresoras entre sí para compartir archivos e imprimir. La comunicación tenía que ser de muy alta velocidad ya que la cantidad de información era enorme.

Esta red, la cual denominaron inicialmente Alto Aloha Network, fue mejorando gradualmente hasta que en 1973 cambió su nombre por el de Ethernet, en referencia a la teoría física según la cual las ondas electromagnéticas viajaban por un fluido denominado éter que se suponía llenaba todo el espacio (Metcalfe llamaba éter al cable coaxial por el que se transmitían los bits a todas las estaciones).

La red ya tenía todas las características esenciales de la Ethernet actual. Empleaba CSMA/CD para minimizar la probabilidad de colisión, y en caso de que ésta se produjera ponía en funcionamiento el mecanismo de retroceso exponencial binario para reducir gradualmente la "agresividad" del emisor, con lo que éste se auto adaptaba a situaciones de muy diverso nivel de tráfico.

Tenía también topología de bus y funcionaba a 2.94 Mbps sobre un cable coaxial de 1.6 Km de longitud. Las direcciones eran de 8 bits y el CRC (Cyclical Redundancy Checking: Verificación cíclica de la redundancia) de las tramas de 16 bits. El protocolo utilizado a nivel de red era el PUP (PARC Universal Packet), el cual evolucionaría hasta convertirse en el XNS (Xerox Network System: Sistema de red Xerox).En 1976 Xerox creó una división para el desarrollo de la red Ethernet, la cual cambió de nombre por X-wired por cuestiones de mercadotecnia. En esta red cada usuario disponía de un ordenador conectado directamente a la red local, integrando en ella todas las funciones. No existía ningún control centralizado de la red; la comunicación entre dos usuarios ocurría directamente sin intermediarios y en condiciones de igual a igual (peer to peer). Ligada a esta arquitectura distribuída estaba la necesidad de una red de muy alta velocidad.

Aunque la red de Xerox parecía ir en el camino correcto, la empresa no era lo suficientemente grande para imponerse frente a sus competidores, y la tecnología no dejaba de ser propietaria, por lo que debía desarrollarse como un estándar abierto y en cooperación con otros fabricantes. Entonces Xerox formó una alianza con Digital Equipment Corporation e Intel para darle a la red el impulso tecnológico y comercial que necesitaba.

Nuevamente con el nombre de Ethernet, la alianza decidió aumentar la velocidad de la red a 10 Mbps. Actualmente, la Ethernet original de 2.94 Mbps se conoce como Ethernet Experimental para distinguirla de la red de 10 Mbps, que apareció como producto comercial.

5.2 Nuevos medios físicos

Los componentes de las primeras redes Ethernet eran muy caros. El cable coaxial (10BASE-5), aunque de costo elevado, resultaba insignificante al lado de los componentes electrónicos. Sin embargo, gradualmente la electrónica fue bajando de precio, por lo que los cables y su instalación

comenzaron a representar una parte significativa del presupuesto de la red. Además, el grosor y rigidez de estos cables los hacía poco apropiados para entornos de oficina. Los usuarios demandaban productos más finos y baratos, como el 10BASE-2, el cual fue incorporado al estándar 802.3 en 1985. También se incluyó fibra óptica en el estándar como medio de transmisión para permitir mayores distancias y mejorar la conectividad entre edificios.

En 1984 el Comité 802.3 comenzó a estudiar la posibilidad de implantar Ethernet en cable telefónico. Muchos expertos aseguraban que una red de 10 Mbps no podría funcionar sobre cable de pares trenzados debido a su mayor atenuación a altas frecuencias comparada con los cables coaxiales. Sin embargo, en 1985 salió al mercado un producto denominado LattisNet que permitía utilizar cableado UTP (Unshielded Twisted Pair; Par trenzado sin blindaje) para construir redes Ethernet de 10 Mbps. y en 1990 se estandarizó 10BASE-T (T=Twisted), el cual ofrecía mayor velocidad. Cuando Ethernet salió al mercado a principios de los ochenta, muchos consideraban que 10 Mbps era una velocidad excesiva. Sin embargo, las mejoras en arquitectura de sistemas y en los paquetes y programas empezaron a saturar las redes Ethernet. Con la finalidad de cubrir esta demanda, en 1995 fue aprobada una versión de Ethernet que funcionaba a 100 Mbps, y que actualmente conocemos como "Fast Ethernet".

Las redes "Fast Ethernet" se difundieron con gran rapidez -su uso inclusive se ha extendido hasta el usuario final- y como consecuencia, los precios bajaron. Esto generó un requerimiento de velocidades superiores en el "backbone"; por ello, en 1995 los expertos comenzaron a estudiar un nuevo aumento en la velocidad sobre un factor de diez, y crearon lo que hoy denominamos Gigabit Ethernet.

5.3 Características de "Fast Ethernet"

Algunas aplicaciones multimedia, "groupware" o "imaging" pueden provocar que las redes que utilizan 10 Mbps, como Ethernet, se vuelvan lentas. Además, los ordenadores y estaciones de trabajo de alto desempeño no trabajan óptimamente en redes de 10 Mbps debido a que sus aplicaciones requieren un gran ancho de banda para mover enormes cantidades de datos de una manera rápida.

"Fast Ethernet" (100BASE-T) ofrece a los usuarios un gran número de ventajas con respecto a otras tecnologías de conexión de redes de alta velocidad, y proporciona el sistema más sencillo de migración de 10BASE-T a 100 Mbps. No se trata de una tecnología nueva que los usuarios deban aprender como ATM (Asynchronous Transfer Mode; Modo de transferencia asíncrona), FDDI (Fiber Distributed Data Interface; Interfase de datos distribuídos por fibra) ó 100VG. Dado que la especificación MAC permanece invariable con respecto a la red Ethernet a 10 Mbps, su funcionamiento es similar al de "Ethernet".

Las especificaciones de "Fast Ethernet" incluyen mecanismos para la auto negociación de la velocidad del medio. Esto hace posible proveer interfases Ethernet de doble velocidad que pueden correr a 10 Mbps ó 100 Mbps automáticamente. Este proceso de auto negociación permite a los dispositivos a cada extremo de la red intercambiar información y configurarse automáticamente para operar juntos a la máxima velocidad. Por ejemplo, la auto negociación puede determinar si un nodo de 100 Mbps se conecta a uno de 10 Mbps o a un adaptador de 100 Mbps, y entonces ajusta su modo de funcionamiento.

100BASE-T está dirigida a los tipos de cableado más comunes (par trenzado de cobre y fibra óptica), por lo que los usuarios pueden tener la tranquilidad de que funcionará en cualquier lugar. En muchos casos, las instalaciones pueden actualizarse a 100BASE-T sin reemplazar el cableado ya existente.

"Fast Ethernet" es una opción costo-efectiva para el "backbone" y conectividad del servidor. y mantiene una total compatibilidad e interoperabilidad con "Ethernet". Los datos pueden moverse entre "Ethernet" y "Fast Ethernet" sin traducción protocolar. Además, usa las mismas aplicaciones y los mismos "drivers" usados por "Ethernet" tradicional y está basado en un esquema de cableado en estrella, topología fiable y de fácil detección de problemas. En cuanto a las desventajas de esta tecnología, podemos mencionar las siguientes:

- Si el cableado existente no se encuentra dentro de los estándares, puede haber un costo sustancial al volver a cablear.
- "Fast Ethernet" puede ser más rápido que las necesidades de las estaciones de trabajo individuales y más lento que las necesidades de la red entera. La tecnología no es escalable más allá de 100 Mbps, por lo que un perfeccionamiento tecnológico puede requerir una inversión mayor.

5.4 Aplicaciones que soporta la arquitectura

Guillermo Luca, ingeniero del área de Ingeniería, Industria, Gobierno y Finanzas de Cisco Systems México, asegura que cualquier aplicación puede funcionar en "Ethernet". Aplicaciones de datos, voz y videoconferencia pueden trabajar en "Ethernet" sin ningún problema, gracias a los bajos tiempos de transferencia de paquetes que se soportan en los "switches" LAN y al soporte de calidad de servicio (QoS).

Por su parte, Evelio Martínez, consultor en telecomunicaciones e informática de Praxis Telecom. asegura que Ethernet y "Fast Ethernet" son utilizados a nivel de LAN, mientras que Gigabit Ethernet es empleado a nivel de MAN (interconexión de LANs, backbones, troncales, video en tiempo real y multimedia). En este sentido, Gigabit Ethernet compite con otras tecnologías de alta velocidad como ATM y FDDI.

5.5 Razones por las cuales se escogió ethernet para la red en la CABIN

Ethernet es en la actualidad el estándar de las redes locales, es soportado por todos los sistemas operativos de red y tiene entre otras, las siguientes características:

- El estándar Ethernet permite reutilizar la infraestructura actual sin necesidad de reemplazarla cuando es necesario.
- "Fast Ethernet": el sistema más sencillo de migración de 10BASE-T a 100 Mbps.
- Ethernet puede usar varios protocolos de comunicación incluyendo TCP/IP, el cual trabaja con todos los ambientes de UNIX.
- Se puede proveer de desempeño haciendo varios segmentos de la red y uniéndolos con puentes o ruteadores

- Trabaja con los sistemas operativos más populares del mercado

6 Windows NT 4.0

La historia de Windows NT comienza a principios de los 80, cuando Microsoft estaba trabajando en un sistema original de ventanas que corriera sobre MS-DOS, ellos se unieron con IBM para crear un reemplazo más poderoso que el DOS para plataformas intel x86, el sistema operativo resultante fue conocido como OS/2, al mismo tiempo que el OS/2 era desarrollado Microsoft continuó trabajando en un nuevo sistema operativo más poderoso, que el sistema operativo que ya tenía.

Esta nueva tecnología en sistemas operativos debía correr en diferentes plataformas de procesadores. Ellos planearon hacer esto programando en lenguaje C que es portable en múltiples plataformas. A finales de octubre de 1988, Microsoft empleó a un hombre nombrado David Cutler que era un gurú respetado de los sistemas operativos de la Digital Equipment Corporation, para ayudarles a diseñar su nuevo sistema operativo

El nombre original previsto era NT OS/2 porque en ese entonces, Microsoft ayudaba a desarrollar OS/2 e integraba partes de él en su nuevo sistema operativo (NT).

Después de casi dos años de trabajo, los primeros dígitos binarios de NT OS/2 se ejecutaron en un procesador de Intel i860. Al mismo tiempo, David Cutler le dijo a Bill Gates que el NT estaría listo para marzo de 1991. A principios de 1990, como los equipos dedicados al NT fueron formados dentro de Microsoft.

La decisión fue hecha eventualmente a principios de 1991 para basar la personalidad de NT en Sistemas actuales de Microsoft Windows versión 3.0 y no en OS/2, en otras palabras la personalidad del nuevo sistema operativo fue para ser liberado después de Windows 3.0. El nombre de OS/2 NT fue descartado y el nuevo nombre fue Windows NT. Cuando la versión 3.0 del Windows normal fue liberado por Microsoft a principios de 1990, ésta tuvo mucho auge rápidamente, a principios de 1991, IBM se enteró que Microsoft planeaba utilizar Windows y no OS/2 como la interfase a utilizar en su nuevo Sistema Operativo. Microsoft aplicó su ambiente de Windows al NT. Bill Gates y su equino de Windows NT, lideareado por David Cutler, siguieron hacia adelante con el desarrollo de NT. Microsoft cortó todos los lazos con IBM hasta en su desarrollo de OS/2. La codificación y la prueba del NT continuó en los meses siguientes, y la versión 3.1 de Windows NT se liberó en julio de 1993.

Aunque ésta era la primera versión de Windows NT, Microsoft tomó la decisión para nombrar la versión 3.1 en vez de 1.0 para que de alguna manera, se integrara con su OS actual de Windows que estaba ya en el mercado

Pensaron que el nombramiento de la versión 1.0 podía hacer a la gente escéptica de su confiabilidad. La versión 3.5 de Windows NT salió poco tiempo más adelante. Incluso desde la versión 3.1, el sistema operativo ha sido totalmente 32-bit. Microsoft ha continuado refinando su sistema operativo sobre los años con una serie de paquetes y de parches , diseñados para reparar defectos y ediciones de seguridad. Una revisión importante, versión 4.0, liberada en agosto de 1996 con la interfase utilizada en Windows 95. Se construye de dieciséis millones de líneas de programación de código de C y de C++. La versión siguiente de Windows NT, Windows 2000, está actualmente en

la etapa beta y de las promesas para muchas nuevas tecnologías que emergen.

Según lo observado previamente, Windows NT 4.0 viene en dos sabores, servidores y estación de Trabajo. El servidor del NT es de gran alcance y versátil. Puede ser utilizado para todo, desde un servidor de archivos en una LAN, hasta un servidor hecho y derecho de Internet, proporcionando correo, Web, ftp o a cualquier combinación de servicios basados TCP/IP. El servidor y estación de trabajo del NT pueden actuar como ruteadores de TCP/IP. En la versión de Estación de trabajo del NT es un sistema operativo de escritorio de 32-bit de gran alcance que actúa como el compañero perfecto del cliente al servidor del NT. Es también Windows NT un excelente Sistema Operativo independiente compatible con la mayoría de los programas, no permite que los programas hagan llamadas directas a la arquitectura, que es la razón por la que algunos juegos no se ejecutan en ella.

6.1 Características por las cuales se escogió a Windows NT 4.0 como sistema operativo de la LAN de la CABIN

6.1.2 Portabilidad

Windows NT fue escrito casi totalmente en C, que es un lenguaje que se mueve fácilmente de plataforma a plataforma. Microsoft aisló la parte del sistema operativo que tuvo que ser escrito para la arquitectura especifica en algo llamado capa de abstracción de arquitectura(HAL). Cuando Microsoft deseó mover el NT a diversas plataformas, todo lo que tuvo que hacer fue recompilar el código fuente para la arquitectura nueva y crear una nueva capa de la abstracción de arquitectura. Windows NT se ejecutará en la configuración de Intel x86, la configuración del RISC de las MIPS, la alfa Digital, y Motorola PowerPC RISC. Como nota interesante, Windows 2000 se ejecutará sólamente en las plataformas de x86 y Digital.

6.1.3 Multitareas

Permite que un ordenador realice aparentemente más de una tarea simultáneamente Los procesadores no pueden trabajar en muchas cosas al mismo tiempo, pero los sistemas operativos se pueden diseñar de una manera tal que manejen muchas tareas al mismo tiempo, y compartir el procesador. Windows NT hace cola de las tareas, dando a cada una un nivel de prioridad. El NT tiene 32 diversos niveles de la prioridad (0 - 31). Entonces, basado en esa información (además de la otra información), el sistema operativo hace algo de la tarea 1, algo de la tarea 2, algo de la tarea 3, y algo de la tarea 1 otra vez. Intercambia cada tarea dentro y fuera del procesador, dando la ilusión que el ordenador está haciendo muchas cosas en el mismo tiempo. Windows NT también hace un trabajo muy bueno en las tareas que aislan en memoria, de modo que si una tarea cuelga o llega a ser de otra manera inoperable, se pueda "matar" fácil y rápidamente, algo como UNIX. Los programas no permiten utilizar las áreas de memoria que el Sistema Operativo está utilizando, y también no permiten utilizar las áreas de memoria que otros programas están utilizando. Esto reduce la ocasión que una aplicación que falla afectará la integridad del sistema operativo o de otros programas.

6.1.4 Ayuda Simétrica del multiprocesamiento

Usando una técnica llamada Multiprocesamiento Simétrico (SMP), Windows NT es capaz de utilizar más de un procesador en el mismo sistema. A diferencia del multiprocesamiento asimétrico, que asigna diversos tipos de tareas a diversos procesadores, el multiprocesamiento simétrico es capaz de asignar cualquier tarea a cualquier procesador en el sistema. Esto tiene como resultado final usar cada procesador a su máximo, Windows NT utilizará dos procesadores en su forma de estación de trabajo, y cuatro procesadores en su forma de servidor (ocho para la edición Enterprise). Algunas versiones especiales de Windows NT tienen la capacidad para utilizar hasta 32 procesadores. Éste era originalmente el límite superior para la cual la arquitectura Windows NT fue diseñada, Microsoft no utiliza oficialmente la versión de servidor con más de 8 procesadores. Los vendedores del sistema que desean utilizar más de 8 procesadores deben rehacer un CD-ROM de Windows NT con un conjunto de valores de registro y por consiguiente, la capa de abstracción de arquitectura(HAL) puede también necesitar ser reescrita.

6.1.5 Seguridad

El gobierno de los Estados Unidos le dio a Windows NT una certificación de seguridad C2, esta clase de seguridad provee protección discreta e incluso capacidades de auditoria para controlar usuarios y las acciones que ellos inician. Esto significa que se puede configurar el Windows NT para mantener un alto nivel de seguridad y permite a los administradores poner protección desde el nivel más bajo que es un archivo.

NT resuelve muchos problemas de seguridad clásicos con unas soluciones innovadoras, una de las cosas interesantes de NT es la forma de entrar al sistema, se debe teclear la secuencia Ctrl.+Alt+Del, ésta es una gran medida de seguridad para los programas que intentan robar contraseñas.

6.1.6 Soporte para RAID

Windows NT tiene ayuda para una característica muy compleja de la Arquitectura llamada RAID (Arreglo redundante de discos). El RAID permite una gran capacidad de almacenamiento, mejora el funcionamiento y confiabilidad. Hace esto de diversas maneras dependiendo del nivel del RAID que se ocupe. El RAID es capaz, por ejemplo, de espejear un disco, es decir guarda simplemente una copia del original en otro disco de las mismas características, los Niveles más altos de RAID guardarán realmente dos dígitos binarios de cada mordedura (hay 8 dígitos binarios en un octeto) en diversos discos, separando los datos hacia fuera y acelerando la extracción. Windows NT utiliza accionamientos de disco SCSI para poner el RAID en ejecución.

6.1.7 Incrementa la estabilidad y robustez sobre Windows 95 y 98

Se puso más atención en la estabilidad de Windows NT 4.0 Era esencial que el NT fuera muy estable para ser una alternativa viable a UNIX como sistema operativo de escritorio y de servidor. Windows 95 y 98 son notablemente inestables y no tienen un gran desempeño con las aplicaciones de la alta demanda TCP/IP. Las pantallas azules son pocas comparadas con Windows 95 y 98. Así que en resumen, el NT 4.0 es mucho más estable y confiable que Windows 95 y 98 debido a cómo era diseñado y debido a su herencia, que es enteramente diferente de Windows 95 y 98.

6.1.8 Fácil de Usar

Windows NT 4.0 utiliza la misma interfase familiar que Windows 95. La misma interfase para la arquitectura o tipo de procesador, un importante beneficio en un ambiente heterogéneo. Las herramientas de Windows NT se diseñan para facilitar la administración y la configuración de servicios comunes como las el DNS y DHCP. Como una ventaja agregada, estas aplicaciones de administración. las puede manejar con seguridad cualquier servidor en la empresa desde una PC. facilitando la carga de trabajo cotidiano.

7 Sistema Operativo Unix

Durante los años 60. un grupo en los laboratorios de Bell desarrollaba un sistema operativo multiusos llamado Multics. Los laboratorios de Bell se retiraron del proyecto en 1969, momento en el cual Multics había llegado a ser excesivamente complejo. Uno de los programadores de Bell. un hombre llamado Ken Thompson, continuó para ocuparse vanamente con un sistema operativo multitareas al que él llamó Unix.

El proyecto de Unix fue alineado a la gerencia como vehículo para la preparación de documentos los primeros utilizadores de Unix estaban en el departamento de la patente de Bell. que utilizó paquetes y programas para la preparación de documentos del sistema. Dennis Ritchie escribió un compilador de C bajo Unix, y en 1973 Thompson y Ritchie reescribieron el núcleo de Unix. Todos los tipos de unix que existen provienen de esta versión. La orientación dual hacia la programación y la preparación de documentos se ha conservado.

AT&T en ese entonces no estaba en el negocio de los ordenadores, dio las copias del código de fuente de Unix, pero conservó la marca registrada. Esta benevolencia conduce a una proliferación de las versiones de Unix. Una tensión dominante fue desarrollada en la Universidad de California en Berkeley, de ahí que las versiones se etiquetan " DEB" (para el "Berkeley Software Distribution"). La versión actual del funcionamiento de Unix usada en STScI (el OS del sol 4) es una variación de la versión 4,2 del DEB. La otra tensión dominante es la línea de AT&T, que se ha llamado el " sistema cinco". el " sistema siete", y ahora se conoce como "sistema V" que ha tenido por lo menos tres versiones. Las diferencias principales entre las dos tensiones, por lo menos en el nivel de utilización. consisten en los comandos que están disponibles en solamente un tipo, y en la disponibilidad de opciones en otros comandos.

7.1 Las Características Generales que se utilizaron para adoptar a UNIX como el sistema operativo de Internet para la CABIN son las siguientes:

- Es un sistema operativo multiusuario, con capacidad de simular multiprocesamiento no interactivo.
- Está escrito en un lenguaje de alto nivel : C.
- Dispone de un lenguaje de control programable llamado SHELL.
- Ofrece facilidades para la creación de programas y sistemas, y el ambiente para las tareas de diseños de software.
- Emplea manejo dinámico de memoria por intercambio o paginación.
- Tiene capacidad de interconexión de procesos.

- Emplea un sistema jerárquico de archivos, con facilidades de protección de archivos, cuentas y procesos.
- Tiene facilidad para redireccionamiento de Entradas/ Salidas.
- Garantiza un alto grado de portabilidad.
- Paso de parámetros
- Sustitución textual de variables y cadenas.
- Comunicación bidireccional entre órdenes de shell.

El sistema se basa en un Núcleo llamado Krenel, que reside permanentemente en la memoria, y que atiende a todas las llamadas del sistema, administra el acceso a los archivos y el inicio o la suspensión de las tareas de los usuarios.

La comunicación con el sistema UNIX se da mediante un programa de control llamado SHELL. Este es un lenguaje de control, un intérprete y un lenguaje de programación, cuyas características lo hacen sumamente flexible para las tareas de un centro de cómputo. Como lenguaje de programación abarca los siguientes aspectos:

Ofrece las estructuras de control normales: secuenciación, iteración condicional, selección y otras.

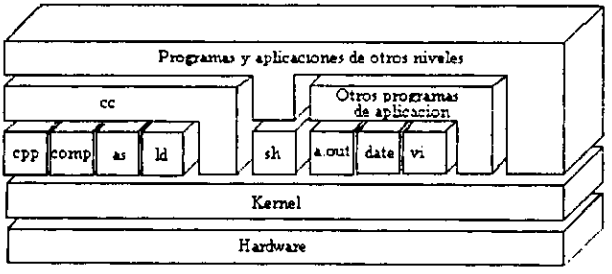


Figura 27 Arquitectura del Sistema Unix

El shell permite modificar en forma dinámica las características con que se ejecutan los programas en UNIX:

Las entradas y salidas pueden ser redireccionadas o redirigidas hacia archivos, procesos y dispositivos:

Es posible interconectar procesos entre sí.

Diferentes usuarios pueden "ver" versiones distintas del sistema operativo debido a la capacidad del shell para configurar diversos ambientes de ejecución. Por ejemplo, se puede hacer que un usuario entre directamente a su sección, ejecute un programa en particular y salga automáticamente del sistema al terminar de usarlo.

El núcleo del sistema operativo Unix (llamado Kernel) es un programa escrito casi en su totalidad en lenguaje "C". Con excepción de una parte del manejo de interrupciones, expresada en el lenguaje ensamblador del procesador en el que opera.

Las funciones del núcleo son permitir la existencia de un ambiente en el que sea posible atender a varios usuarios y múltiples tareas en forma concurrente, repartiendo al procesador entre todos ellos e intentando mantener en grado óptimo la atención individual.

El Kernel opera como asignador de recursos para cualquier proceso que necesite hacer uso de las facilidades de cómputo. Es el componente central de Unix y tiene las siguientes funciones:

- Creación de procesos, asignados de tiempos de atención y sincronización.
- Asignación de la atención del procesador a los procesos que lo requieren.
- Administración de espacio en el sistema de archivos que incluye: acceso, protección y administración de usuarios, comunicación entre usuarios y entre procesos, manipulación de E/S y administración de periféricos.
- Supervisión de la transmisión de datos entre la memoria principal y los dispositivos periféricos.

El Kernel reside siempre en la memoria central, el control sobre el ordenador, por lo que ningún otro proceso puede interrumpirlo; sólo pueden llamarlo para que proporcione algún servicio de los ya mencionados. Un proceso llama al Kernel mediante módulos especiales conocidos como llamadas al sistema.

El Kernel consta de dos partes principales la sección de control de procesos y la de control de dispositivos. La primera asigna recursos, programas y procesos, atiende sus requerimientos de servicio; la segunda, supervisa la transferencia de datos entre la memoria principal y los dispositivos periféricos. En términos generales, cada vez que algún usuario oprime una tecla de una terminal, o que debe leer o escribir información del disco magnético, se interrumpe al procesador central y el núcleo se encarga de efectuar la operación de transferencia.

Cuando se inicia la operación de el ordenador debe cargarse en la memoria una copia del núcleo, que reside en el disco magnético (operación denominada bootstrap). Para ello, se deben inicializar algunas interfases básicas de la arquitectura; entre ellas, el reloj que proporciona interrupciones periódicas. El Kernel también prepara algunas estructuras de datos que abarcan una sección de almacenamiento temporal para transferencia de información entre terminales y procesos. una sección de almacenamiento temporal para transferencia de información entre terminales y procesos. una sección para almacenamiento de descriptores de archivos y una variable que indica cantidad de memoria principal.

A continuación , el Kernel inicializa un proceso especial, llamado proceso 0. En general, los procesos se crean mediante una llamada a una rutina del sistema (fork),que funciona por un mecanismo de duplicación de procesos. Sin embargo, esto no es suficiente para crear el primero de ellos, por lo que el Kernel asigna una estructura de datos y establece apuntadores a una sección especial de la memoria, llamada tabla de procesos, que contendrá los descriptores de cada uno de los procesos existentes en el sistema.

Después de haber creado el proceso 0, se hace una copia del mismo, con lo que se crea el proceso 1; éste muy pronto se encargará de "dar vida" al sistema completo, mediante la activación de otros procesos que también forman parte del núcleo. Es decir, se inicia una cadena de activaciones de procesos entre los cuales destaca el conocido como despachador, o "scheduler", que es el responsable de decidir cuál proceso se ejecutará y cuáles van a entrar o salir de la memoria central. A partir de ese momento se conoce el numero 1 como proceso de inicialización del sistema "init».

El proceso "init» es el responsable de establecer la estructura de procesos en Unix. Normalmente, es capaz de crear al menos dos estructuras distintas de procesos, el modo monousuario y el multiusuario. Comienza activando el intérprete del lenguaje de control (Shell) en la terminal principal o consola del sistema y proporcionándole privilegios de "superusuario" . En la modalidad de un solo usuario la consola permite iniciar una primera sesión, con privilegios especiales, e impide que las otras líneas de comunicación acepten iniciar sesiones nuevas. Esta modalidad se usa con frecuencia para revisar y reparar sistemas de archivos, realizar pruebas de funciones básicas del sistema y para otras actividades que requieren uso exclusivo del ordenador.

"Init» crea otro proceso, que espera pacientemente a que alguien entre en sesión en alguna línea de comunicación. Cuando esto sucede, realiza ajustes en el proceso de la línea y ejecuta el programa "login", que se encarga de atender inicialmente a los nuevos usuarios. Si la clave del usuario, y la contraseña proporcionadas son las correctas, entonces entra en operación el programa "Shell", que en lo sucesivo se encargará de la atención normal del usuario que se dio de alta en esa terminal.

A partir de ese momento el responsable de atender al usuario en esa terminal es el intérprete "Shell".

Cuando se desea terminar la sesión hay que desconectarse de "Shell" (y, por lo tanto, de Unix), mediante una secuencia especial de teclas (usualmente <CLT>-D). A partir de ese momento la terminal queda disponible para atender a un nuevo usuario.

7.1.2 Administración de Archivos y Directorios

El sistema de archivos de Unix, está basado en un modelo árbol y recursivo, en el cual los nodos pueden ser tanto archivos como directorios, y estos últimos pueden contener a su vez directorios o subdirectorios. Debido a esta filosofía, se maneja al sistema con muy pocas órdenes que permiten una gran gama de posibilidades. Todo archivo de Unix está controlado por múltiples niveles de protección, que especifican los permisos de acceso al mismo. La diferencia que existe entre un archivo de datos, un programa, un manejador de entrada/salida o una instrucción ejecutable se refleja en estos

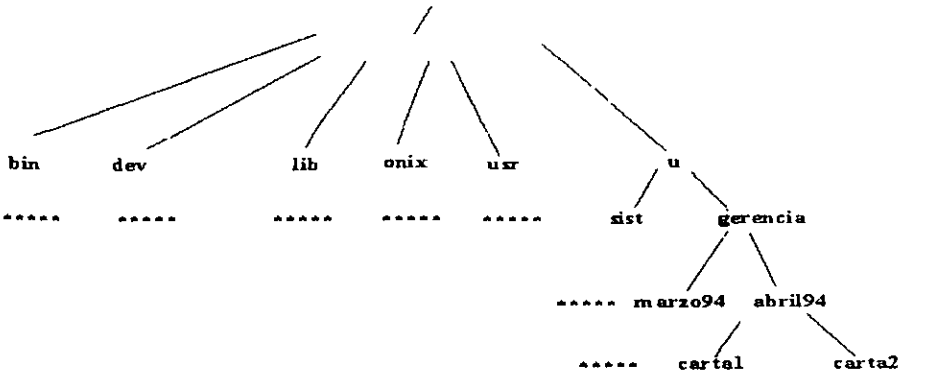


Figura 28. Sistema de archivos en árbol.

parámetros, de modo que el sistema operativo adquiere características de coherencia y elegancia que lo distinguen.

La raíz del sistema de archivos (conocida como "root:) se denota con el símbolo "/", y de ahí se desprende un conjunto de directorios que contienen todos los archivos del sistema de cómputo . Cada directorio, a su vez, funciona como la subraíz de un nuevo árbol que depende de él y que también puede estar formado por directorios o subdirectorios y archivos. Un archivo siempre ocupará el nivel más bajo dentro del árbol porque de un archivo no pueden depender otros, si así fuera, sería un directorio. Es decir, los archivos son como las hojas del árbol.

Se define en forma unívoca el nombre de todo archivo (o directorio) mediante lo que se conoce como su trayectoria (path name): es decir, el conjunto completo de directorios, a partir de "root" (/), por los que hay que pasar para poder llegar al directorio o archivo deseado. Cada nombre se separa de los otros con el símbolo /. Aunque tan sólo el primero de ellos se refiere a la raíz.

/u/gerencia tiene toda esta trayectoria como nombre absoluto, pero se llama gerencia/abril94/carta2, sin la diagonal inical, si se observa desde el directorio /u. Para los usuarios que están normalmente en el directorio /u/gerencia, el archivo se llama abril94/carta2. Así, también puede existir otro archivo llamado carta2, pero dentro de algún otro directorio y en caso de ser necesario se emplearía el nombre de la trayectoria (completa o en partes, de derecha izquierda) para distinguirlos.

Como se dijo antes, desde el punto de vista del directorio abril94, que pertenece al directorio gerencia del directorio /u, basta con el nombre carta2 para apuntar al archivo en cuestión.

En esta forma se maneja el sistema completo de archivos y se dispone de un conjunto de órdenes de Shell (además de múltiples variantes) para hacer diversas manipulaciones, como crear directorio, moverse dentro del sistema de archivos, copiarlos, etcétera.

Unix incluye, además, múltiples esquemas para crear, editar y procesar documentos. Existen varios tipos de editores, formadores de textos, macroprocesadores para textos, formadores de tablas,

preprocesadores de expresiones matemáticas y un gran número de ayudas y utilerías, que se mencionan más adelante.

A continuación se describe el modo de funcionamiento de Unix, con base en un modelo de estudio de sistemas operativos que lo divide en "capas" jerárquicas para su mejor comprensión.

7.1.3 Manejo de archivos y de información

Como ya se describió, la estructura básica del sistema de archivos es jerárquica, lo que significa que los archivos están almacenados en varios niveles. Se puede tener acceso a cualquier archivo mediante su trayectoria, que especifica su posición absoluta en la jerarquía, y los usuarios pueden cambiar su directorio actual a la posición deseada. Existe también un mecanismo de protección para evitar accesos no autorizados. Los directorios contienen información para cada archivo, que consiste en su nombre y en un número que el Kernel utiliza para manejar la estructura interna del sistema de archivos, conocido como el nodo-i. Hay un nodo –i para cada archivo que contiene información de su directorio en el disco, su longitud,los nodos y las fechas de acceso, el autor, etc. Existe además, una tabla de descriptores de archivo, que es una estructura de datos residente en el disco magnético, a la que tiene acceso mediante el sistema mencionado de E/S por bloques.

El control del espacio libre en el disco se mantiene en una lista ligada de bloques disponibles. Cada bloque contiene la dirección en disco del siguiente en la cadena. El espacio restante contiene las direcciones de grupos de bloques del disco que se encuentren libres. De esta forma, con una operación de E/S, el sistema obtiene un conjunto de bloques libres y un apuntador.

Las operaciones de E/S en archivos se llevan a cabo con la ayuda de la correspondiente entrada del nodo-i en la tabla de archivos del sistema. El usuario normalmente desconoce los nodos-i porque las referencias se hacen por el nombre simbólico de la trayectoria. Los procesos emplean internamente funciones primitivas (llamadas al sistema) para tener acceso a los archivos, las más comunes son "open","creat","read","write","seek","close" y "unlink"; aunque sólo son empleadas por los programadores, no por los usuarios finales del sistema.

Toda esta estructura física se maneja "desde afuera" mediante la filosofía jerárquica de archivos y directorios ya mencionada, y en forma totalmente transparente para el usuario. Además, desde el punto de vista del sistema operativo, un archivo es muy parecido a un dispositivo.

Las ventajas de tratar a los dispositivos de E/S en forma similar a los archivos normales son múltiples, un archivo y un dispositivo de E/S son muy parecidos, los nombres de los archivos y de los dispositivos tienen la misma sintaxis y significado, así que a un programa que espera un nombre de archivo como parámetro puede dársele un nombre de dispositivo (con esto se logra interacción rápida y fácil entre procesos de alto nivel).

El sistema Unix ofrece varios niveles de protección para el sistema de archivos , que consisten en asignar a cada archivo el número único de identificación de su dueño, junto con nueve bits de protección, que especifican permisos de lectura, escritura y ejecución para el propietario, para otros miembros de su grupo (definido por el administrador del sistema) y para el resto de los usuarios. Antes de cualquier acceso se verifica su validez consultando estos bits, que residen en el nodo-i de

todo archivo. Además existen otros tres bits que se emplean para manejos especiales, relacionados con la clave del superusuario.

Otra característica de Unix es que no requiere que el conjunto de sistemas de archivos resida en un mismo dispositivo.

Es posible definir uno o varios sistemas "desmontables", que residen físicamente en diversas unidades de disco. Existe una orden ("mkfs:) que permite crear un sistema de archivos adicional , y una llamada al sistema ("mount") con la que se añade (y otra con la que se desmonta) uno de ellos al sistema de archivos global.

El control de las impresoras de un ordenador que funciona con el sistema operativo Unix consiste en un subsistema ("SPOOL") que se encarga de coordinar los pedidos de impresión de múltiples usuarios. Existe un proceso de Kernel que en forma periódica revise las colas de servicio de las impresoras para detectar la existencia de pedidos e iniciar entonces las tareas de impresión. Este tipo de procesos, que son activados en forma periódica por el núcleo del sistema operativo, reciben en Unix el nombre de "daemons" (demonios), tal vez porque se despiertan y aparecen sin previo aviso. Otros se encargan de activar procesos en tiempos previamente determinados por el usuario, o de escribir periódicamente los contenidos de los 'buffers" de memoria en el disco magnético.

7.1.4 Procesos y Manejo del Procesador

En Unix se ejecutan programas en un medio llamado "procesos de usuario". Cuando se requiere una función del Kernel, el proceso de usuario hace una llamada especial al sistema y entonces el control pasa temporalmente al núcleo. Para esto se requiere de un conjunto de elementos de uso interno que se mencionan a continuación.

Se conoce como imagen a una especie de fotografía del ambiente de ejecución de un proceso, que incluye una descripción de la memoria, valores de registros generales, status de archivos abiertos, el directorio actual etcétera. Una imagen es el estado actual de un ordenador virtual, dedicada a un proceso en particular.

Un proceso puede encontrarse en uno de varios estados : en ejecución, listo para ejecutar, o en espera.

Cuando se invoca una función del sistema, el proceso de usuario llama al Kernel como subrutina. Hay un cambio de ambientes y, como resultado, se tiene un proceso del sistema. Estos dos procesos son dos fases del mismo original que nunca se ejecutan en forma simultánea.

Existe una tabla de procesos que contiene una entrada por cada uno de ellos con los datos que requiere el sistema:

Identificación , direcciones de los segmentos que emplea en la memoria , información que necesita el "scheduler" y otros, la entrada de la tabla de procesos se asigna cuando se crea el proceso y se libera cuando éste termina.

Para crear un proceso se requiere la inicialización de una entrada en la tabla, así como la creación de segmentos de texto y de datos. Además, es necesario modificar la tabla cuando cambia el estado del proceso o cuando recibe un mensaje de otro (para sincronización, por ejemplo). Cuando un proceso termina, su entrada en la tabla se libera y queda otro disponible para que otro nuevo la utilice.

En el sistema operativo Unix los procesos pueden comunicarse internamente entre sí, mediante el envío de mensajes o señales. El mecanismo conocido como interconexión (pipe) crea un canal entre dos procesos mediante una llamada a una rutina del Kernel, y se emplea tanto para pasar datos unidireccionalmente entre las imágenes de ambos, como para sincronizarlos ya que si un proceso intenta escribir en un pipe ocupado, debe esperar a que el receptor lea los datos pendientes. Lo mismo ocurre en el caso de una lectura de datos inexistentes: el proceso que intenta leer debe esperar a que el proceso productor deposite los datos en el canal de intercomunicación.

Entre las diferencias llamadas al sistema para el manejo de procesos que existen en Unix están las siguientes. Algunas de las cuales ya han sido mencionadas: "fork" (sacar una copia a un proceso), "exec" (cambiar la identidad de un proceso), "kill" (enviar una señal a un proceso), "signal" (especificar la acción por ejecutar cuando se recibe una señal de otro proceso), y "exit" (terminar un proceso).

Dentro de las tareas del manejo del procesador destaca la asignación dinámica ("scheduling"), que en Unix resuelve el "scheduler" mediante un mecanismo de prioridades. Cada proceso tiene asignada una prioridad, las prioridades de los procesos de usuario son menores que la más pequeña de un proceso del sistema.

El "motor" que mantiene en movimiento un esquema de multiprogramación es, por un lado, el conjunto de interrupciones que genera el desempeño de los procesos y, por otro, los constantes recordatorios que hace el reloj del procesador para indicar que se terminó la fracción de tiempo dedicada a cada proceso.

Es un sistema de tiempo compartido, se divide el tiempo en un determinado número de intervalos o fracciones y se asigna cada una de ellas a un proceso. Además Unix toma en consideración que hay procesos en espera de una operación de E/S y que ya no pueden aprovechar su fracción. Para asegurar una distribución adecuada del procesador, los procesos se calculan dinámicamente las prioridades de estos últimos con el fin de determinar cuál será el proceso que se ejecutará cuando se suspenda el proceso activo actual

7.1.5 Manejo De Memoria

Dependiendo de el ordenador en la que se ejecute, Unix utiliza dos técnicas de manejo de memoria: swapping y memoria virtual.

Lo estándar en Unix es un sistema de intercambio de segmentos de un proceso entre memoria principal y memoria secundaria, llamado swapping lo que significa que se debe mover la imagen de un proceso al disco si éste excede la capacidad de la memoria principal, y copia el proceso completo a memoria secundaria. Es decir, durante su ejecución, los procesos son cambiados hacia memoria secundaria conforme se requiera.

Si un proceso necesita crecer, pide más memoria al sistema operativo y se le da una nueva sección, lo suficientemente grande para acomodarlo. Entonces, se copia el contenido de la sección usada al área nueva, se libera la sección antigua y se actualizan las tablas de descriptores de procesos. Si no hay suficiente memoria en el momento de la expansión, el proceso se bloquea temporalmente y se le asigna espacio en memoria secundaria. Se copia a disco y, posteriormente, cuando se tiene el espacio adecuado- lo cual sucede normalmente en algunos segundos- se devuelve a memoria principal.

Está claro que el proceso que se encarga de los intercambios entre memoria y disco (llamado swapper) debe ser especial y jamás podrá perder su posición privilegiada en la memoria central. El Kernel se encarga de que nadie intente siquiera interrumpir este proceso del cual dependen todos los demás. Este es el proceso 0 mencionado antes. Cuando se decide traer a la memoria principal un proceso en estado de "listo para ejecutar", se le asigna memoria y se copian allí sus segmentos. Entonces, el proceso cargado compite por el procesador con todos los demás procesos cargados. Si no hay memoria, el proceso de intercambio examina la tabla de procesos para determinar cuál puede ser interrumpido y llevado al disco.

Hay una pregunta que surge entonces, cuál de los posibles procesos que están cargados será desactivado y cambiado a memoria secundaria ? Los procesos que se eligen son aquellos que están esperando operaciones lentas (ES), o que llevan cierto tiempo sin haberse movido al disco. La idea es tratar de repetir en forma equitativa las oportunidades de ejecución entre todos los procesos, tomando en cuenta sus historias recientes y sus patrones de ejecución.

Otra pregunta es ¿ cuál de todos los procesos que están en el disco será traído a memoria principal ? La decisión se toma con base en el tiempo de resistencia en memoria secundaria. El proceso más antiguo es el que se llama primero, con una pequeña penalización para los grandes.

Cuando Unix opera en máquinas más grandes, suele disponer de manejo de paginación por demanda. En algunos sistemas el tamaño de la página en Unix es de 512bytes; en otros, de 1024. Para reemplazo se usa un algoritmo que mantiene en memoria las páginas empleadas más recientemente.

Un sistema de paginación por demanda ofrece muchas ventajas en cuanto a flexibilidad en la atención concurrente de múltiples procesos y proporciona además, memoria virtual, es decir, la capacidad de trabajar con procesos mayores que el de la memoria central. Estos esquemas son bastante complejos y requieren del apoyo de la arquitectura especializado.

7.1.6 Manejo de entradas y salidas

El sistema de entrada/salida se divide en dos sistemas complementarios: el estructurado por bloques y el estructurado por caracteres. El primero se usa para manejar cintas y discos magnéticos y emplea bloques de tamaño fijo (512 o 1024 bytes) para leer o escribir. El segundo se utiliza para atender a las terminales, líneas de comunicación e impresoras, y funciona byte por byte.

En general, el sistema Unix emplea programas especiales (escritos en C) conocidos como controladores (drivers) para atender a cada familia de dispositivos de E/S Los procesos se comunican con los dispositivos mediante llamadas a su manejador. Además, desde el punto de vista de los procesos, los manejadores aparecen como si fueran archivos en los que se lee o escribe, con esto se logra gran

homogeneidad y elegancia en el diseño.

Cada dispositivo se estructura internamente mediante descriptores llamados número mayor, número menor y clase (de bloque o de caracteres) para cada clase hay un conjunto de entradas, en una tabla, que aporta a los controladores de los dispositivos. El número mayor se usa para asignar un controlador, correspondiente a una familia de dispositivos, el menor pasa al controlador, como un argumento, y éste lo emplea para tener acceso a uno de varios dispositivos físicos semejantes.

Las rutinas que el sistema emplea para ejecutar operaciones de E/S están diseñadas para eliminar las diferencias entre dispositivos y los tipos de acceso. No existe distinción entre aleatorio y secuencial, ni hay un tamaño de registro lógico impuesto por el sistema. El tamaño de un archivo ordinario está determinado por el número de bytes escritos en él; no es necesario predeterminar el tamaño de un archivo.

El sistema mantiene una lista de áreas de almacenamiento temporal (buffer), asignadas a los dispositivos de bloques. El Kernel usa estos buffers con el objeto de reducir el tráfico de E/S. Cuando un programa solicita una transferencia, se busca en los buffers internos para ver si el bloque que se requiere ya se encuentra en la memoria principal (como resultado de una operación de lectura anterior). Si es así, entonces no será necesario realizar la operación física de entrada o salida.

Existe todo un mecanismo de manipulación interna de buffers (y otro de manejo de listas de bytes), necesario para controlar el flujo de datos entre los dispositivos de bloques (y de caracteres) y los programas que los requieren.

Por último, y debido a que los manejadores de los dispositivos son programas escritos en lenguaje C, es relativamente fácil reconfigurar el sistema para ampliar o eliminar dispositivos de E/S en el ordenador, así como para incluir tipos nuevos.

7.1.7 Lenguaje de control del sistema operativo

Entre los rasgos distintivos de Unix está el lenguaje de control que emplea, llamado Shell. Es importante analizar dos funciones más de Shell, llamadas redireccionamiento e interconexión.

Asociado con cada proceso hay un conjunto de descriptores de archivo numerados 0,1 y 2, que se utilizan para todas las transacciones entre los procesos y el sistema operativo.

El descriptor de archivo 0 se conoce como la entrada estándar; el descriptor de archivo 1, como la salida estándar, y el descriptor 2, como el error estándar. En general, todos están asociados con la terminal de video pero debido a que inicialmente son establecidos por Shell, es posible reasignarlos.

En la teoría de lenguajes formales desempeñan un importante papel las gramáticas llamadas de tipo 3 (también conocidas como regulares), que tienen múltiples aplicaciones en el manejo de lenguajes. Existen unas construcciones gramaticales conocidas como expresiones regulares, con las que se puede hacer referencia a un conjunto ilimitado de nombres con estructura lexicográfica similar, esto lo aprovecha Shell para dar al usuario facilidades expresivas adicionales en el manejo de los

nombres de los archivos. Así por ejemplo, el nombre carta se refiere a todos los archivos que comiencen con el prefijo carta" y que sean seguidos por cualquier subcadena, incluyendo la cadena vacía; por ello, si se incluye el nombre carta" en alguna orden. Shell la aplicará a los archivos carta, carta 2 y cualquier otro que cumpla con esa especificación abreviada. En general, en lugares donde se emplea un nombre o una trayectoria, Shell permite utilizar una expresión regular que sirve como abreviatura para toda una familia de ellos y automáticamente reporte el pedido de atención para los componentes. Existen además otros caracteres especiales que Shell reconoce y emplea para el manejo de expresiones regulares, lo que proporciona al lenguaje de control de Unix mayor potencia y capacidad expresiva.

En Unix existe también la posibilidad de ejecutar programas sin tener que atenderlos en forma interactiva, sino simulando paralelismo (es decir, atender de manera concurrente varios procesos de un mismo usuario). Esto se logra agregando el símbolo & al final de la línea en la que se escribe la orden de ejecución. Como resultado, Shell no espera que el proceso "hijo" termine de ejecutar (como haría normalmente), sino que regresa a atender al usuario inmediatamente después de haber creado el proceso asincrónico , simulando en esta forma el procedimiento por lotes (batch). Para cada uno de estos procesos Shell proporciona además, el número de identificación por lo que si fuera necesario el usuario podría cancelarlo posteriormente o averiguar el avance de la ejecución.

La comunicación interna entre procesos (es decir, el envío de mensajes con los que los diversos procesos se sincronizan y coordinan) ocurre mediante el mecanismo de interconexiones (pipes) ya mencionado, que conecta la salida estándar de un programa a la entrada estándar de otro, como si fuera distinto. Desde Shell puede emplearse este mecanismo con el símbolo | en la línea donde se escribe la orden de ejecución.

Así en el ejemplo:

(califica < tarea | sort > lista) &

se emplean las características de interconexión, redireccionamiento y asincronía de procesos para lograr resultados difíciles de obtener en otros sistemas operativos. Aquí si se pide que, en forma asincrónica (es decir, dejando que la terminal siga disponible para atender otras tareas del mismo), se ejecute el programa califica para que lea los daños que requiere del archivo tareas, al terminar, se conectará con el proceso sort (es decir, pasará los resultados intermedios) para que continúe el procedimiento y se arreglen los resultados en orden alfabético, al final de todo esto los resultados quedarán en el archivo lista.

Con esta otra orden, por ejemplo, se busca obtener todos los renglones que contengan las palabras "contrato" o "empleado" en los archivos en disco cuyos nombres comiencen con la letra "E" (lo cual se denota mediante una expresión regular), para lograrlo, se hace uso de una función llamada grep, especial para el manejo de patrones y combinaciones de expresiones regulares dentro de los archivos:

grep-n 'contrato' 'empleado' E*

Los resultados aparecen así:
Emple1:5: en caso de que un empleado decide hacer uso de la facilidad.

Emple1:7: y el contrato así como lo considere las obligaciones de la...

Emple2:9: Cláusula II: El contrato colectivo de trabajo.

Emple2:15:. Fracción III. El empleado tendrá derecho, de acuerdo con lo ...

El tercer renglón, por ejemplo, muestra el noveno renglón del archivo Emple2, que contiene una de las palabras buscadas.

Como Unix fue diseñado para servir de entorno en las labores de diseño y producción de programas, ofrece- además de su filosofía misma – un rico conjunto de herramientas para la creación de sistemas complejos, entre las que destaca el subsistema make. Este último ofrece una especie de lenguaje muy sencillo, con el cual el programador describe las relaciones estructurales entre los módulos que configuran un sistema completo para que de ahí en adelante se encargue de mantener el sistema siempre al día. Es decir, si se modifica algún módulo, se reemplaza o se añade otro, las complicaciones individuales, así como las cargas y ligas a que haya lugar, serán realizadas en forma automática, por esta herramienta. Con una sola orden, es posible efectuar decenas de compilaciones y ligas predefinidas entre módulos, y asegurarse de que en todo momento se tiene la última versión de un sistema ya que también se lleva cuenta autómatica de las fechas de creación, modificación y compilación de los diversos módulos. De esta manera, se convierte en una herramienta casi indispensable al desarrollar aplicaciones que requieren decenas de programas que interactúan entre sí o que mantienen relaciones jerárquicas.

La lista completa de funciones, órdenes de subsistemas que forman parte de las utilerías del sistema operativo Unix es realmente grande e incluye más de un centenar que se pueden agrupar en los siguientes rubros:

- Compiladores de compiladores
- Ejecución de programas
- Facilidades de comunicaciones
- Funciones para control de status
- Funciones para control de usuarios
- Funciones para impresión
- Herramientas de desarrollo de programación
- Lenguaje C, funciones y bibliotecas asociados
- Macroprocesamiento
- Manejo de directorios y archivos
- Manejo de gráficas
- Manejo de información
- Manejo de terminales
- Mantenimiento y respaldos
- Otros lenguajes algorítmicos integrados
- Preparación de documentos

Además que tiene muchas ventajas sobre otros sistemas operativos como:

- Ejecuta programas más rápido
- Muy poca restricción de la arquitectura
- Corre sobre muchas arquitecturas DEC, IBM, HP, SGI, Sun, Intel
- Su sintaxis en comandos es corta
- Utiliza sistema de archivos y no dispositivos
- Existe software gratuito
- Acceso fácil a datos y periféricos sobre la red
- Es un sistema abierto para el control de usuarios
- Tiene la habilidad de combinar comandos y funciones.

Capítulo IV

Marco Metodológico

Propuesta de Memoria Técnica

Se realizará el tendido de 300 nodos sencillos de datos, en las Instalaciones de la Av. Revolución. instalando canalización de tubería conduit galvanizada pared delgada de 0.25 y 0.51 mm. En el área de oficinas se pondrá canaleta plegable al muro, y para alimentar las áreas de modulares se recorrerá por mamparas.

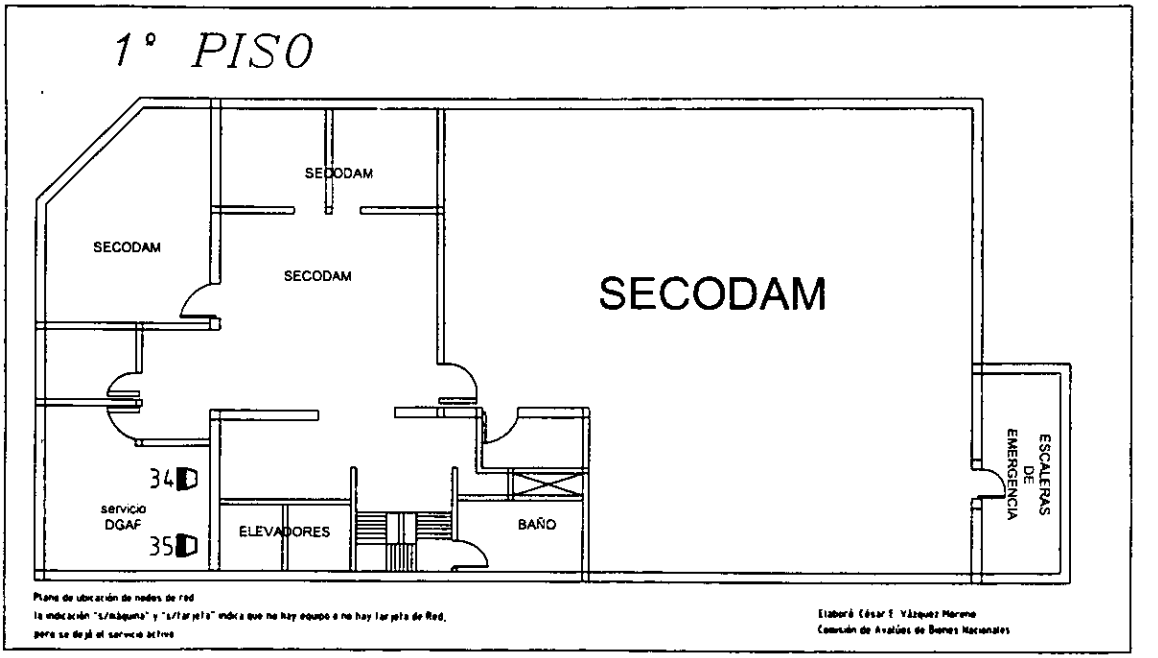
Cada nodo de red contará con un "face plate" sencillo, los cuales estarán rematados en "jacks" nivel 5 referentes al subsistema horizontal, el subsistema vertical se rematará en paneles de 48 puertos identificados para datos, instalados en un "rack" de 7 pies con organizadores sencillos de 3.5 y de 1.75 pulgadas y otros de 7 pies.

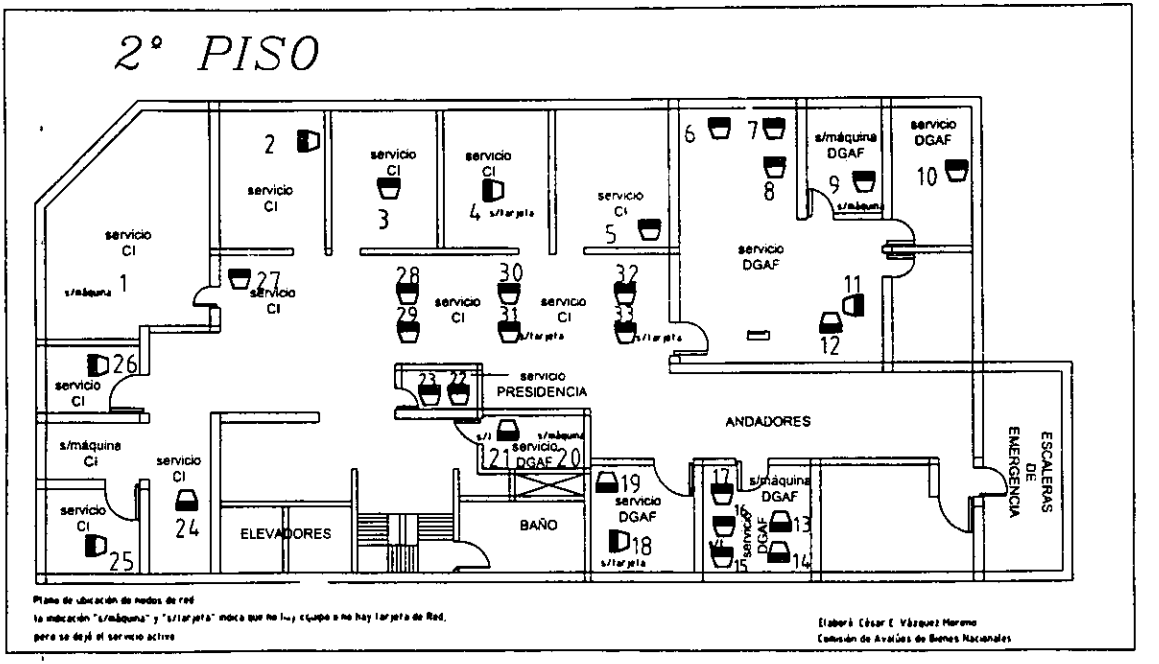
El sistema de administración se identificará con la siguiente nomenclatura: d001 hasta d200. De acuerdo a la norma EIA/TIA 568-B siendo la configuración de esta instalación.

Contenido

- Planos de Ubicación de Nodos por piso
- Relación de direcciones IP asignadas
  Señalización de acometida de cableado
  Relación de usuarios por nodo
- Relación de Material y equipo utilizado
- Diagrama de conexión de la Red Metropolitana de la CABIN

1 Planos de Ubicación de Nodos por piso

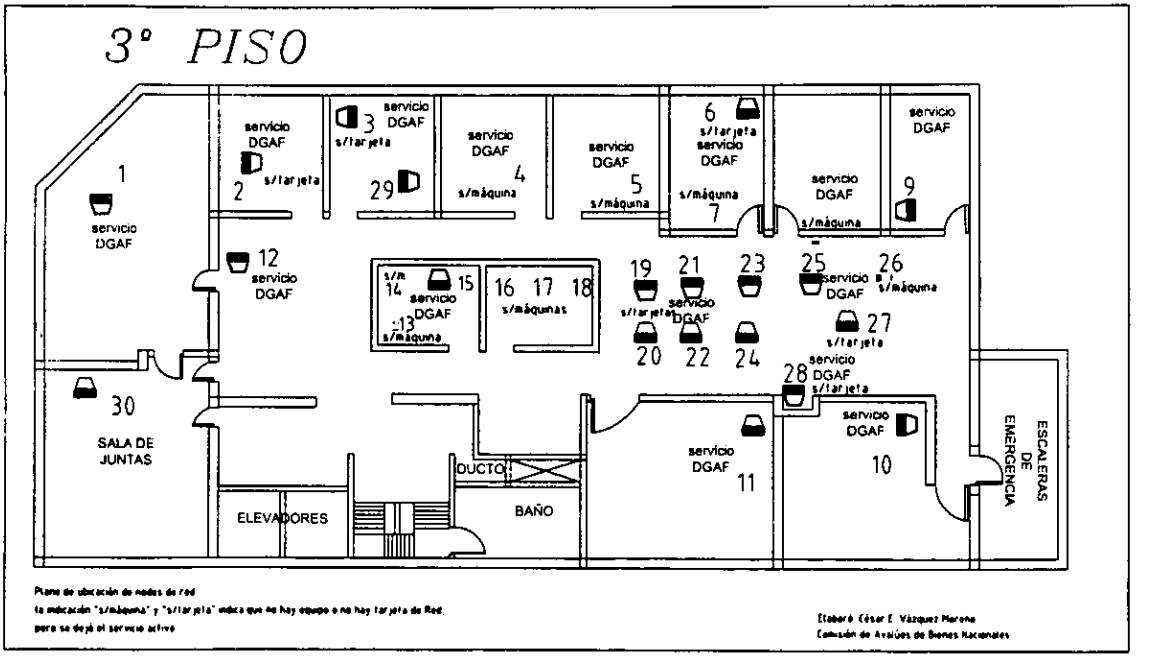


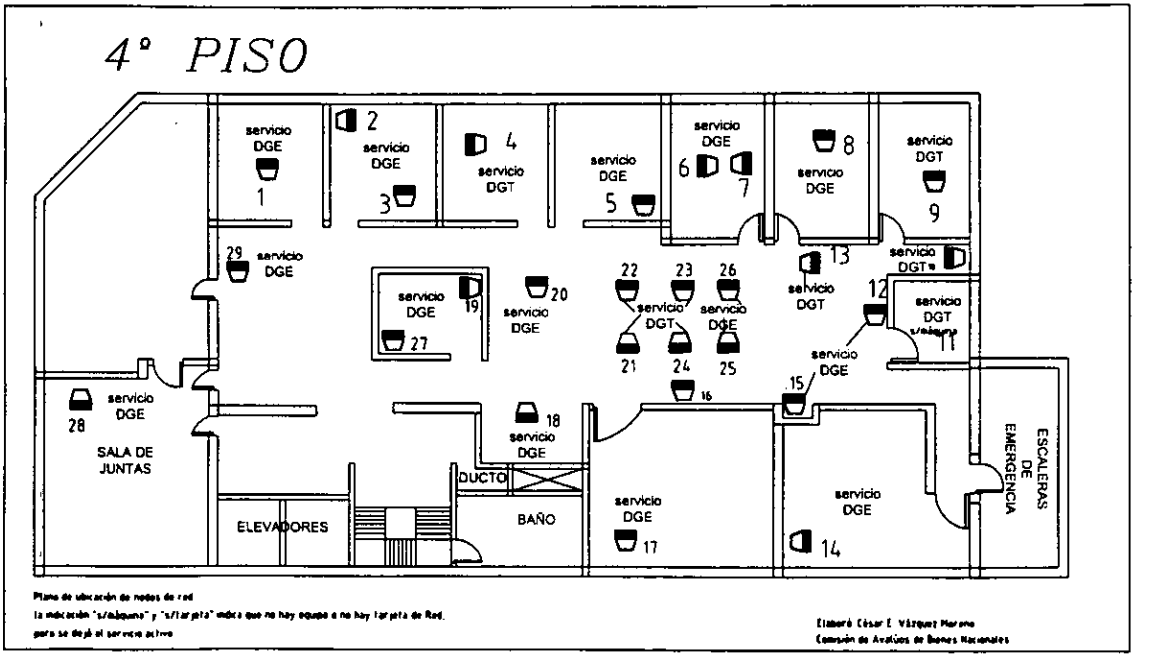


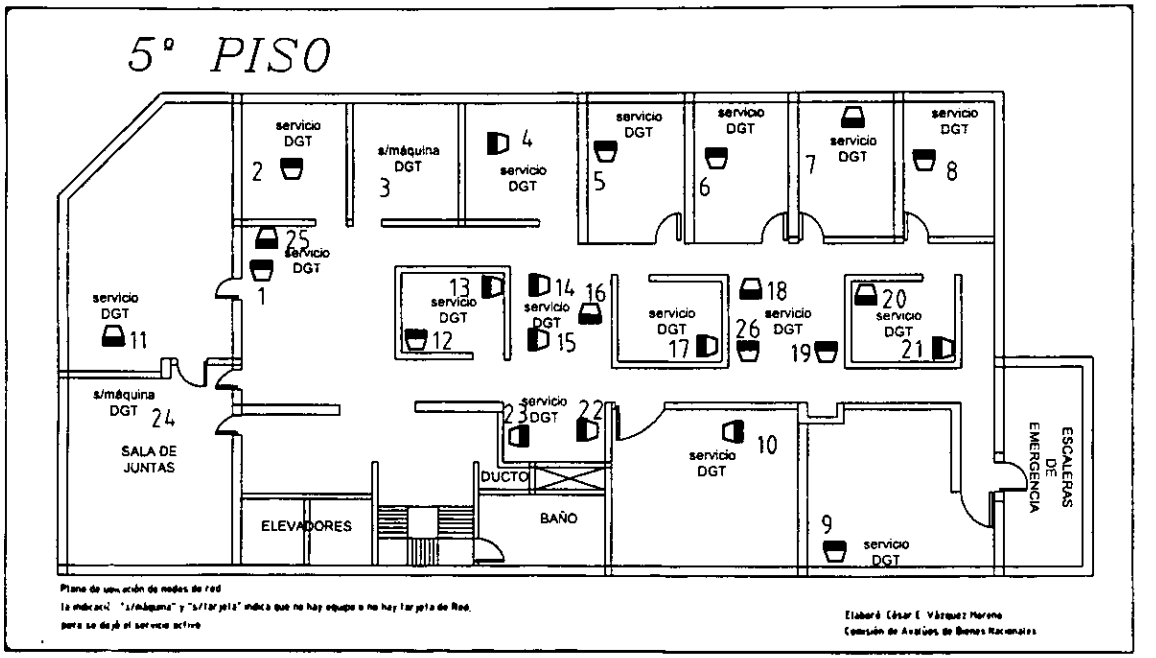
Plano de ubicación de nodos de red

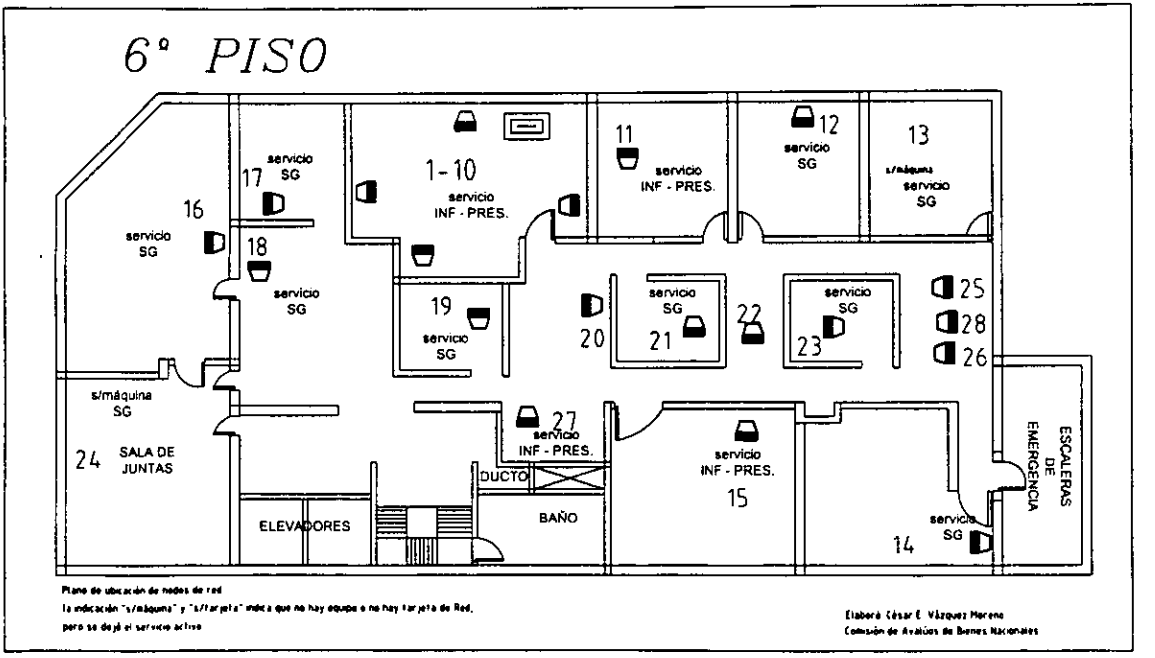
la indicación "s/máquina" y "s/tarjeta" indica que no hay equipo o no hay tarjeta de Red, pero se dejó el servicio activo

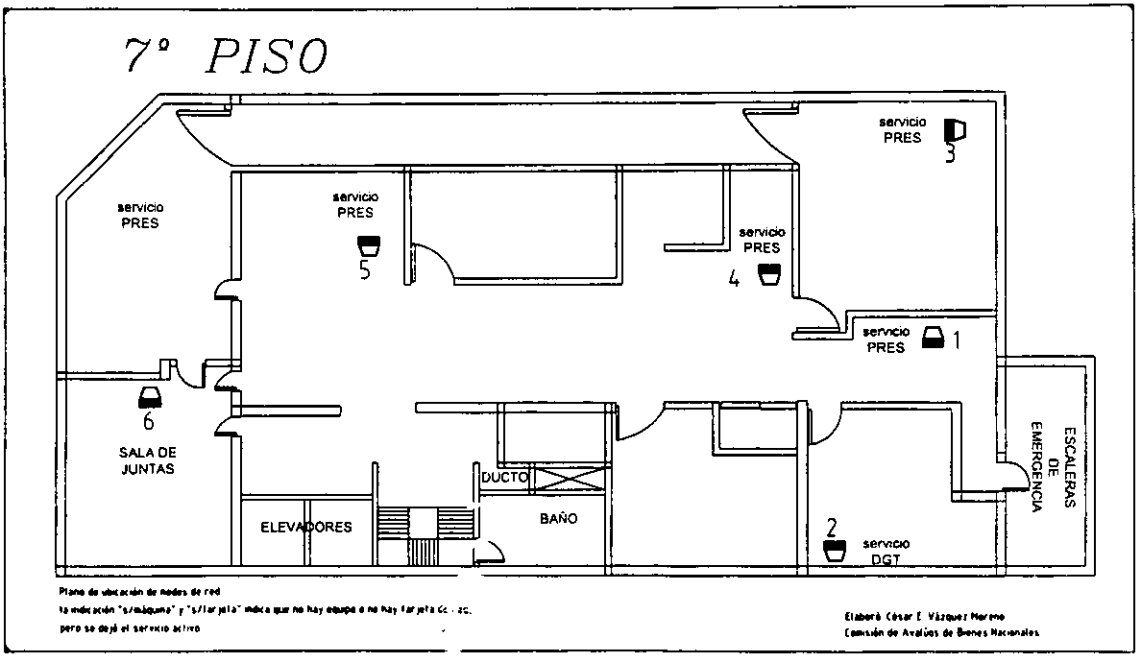
Elaboró César E. Vázquez Moreno
Comisión de Avalúos de Bienes Nacionales


3° PISO
servicio DGAF
s/tarjeta
s/máquina
SALA DE JUNTAS
ELEVADORES
DUCTO
BAÑO
ESCALERAS DE EMERGENCIA
Plano de ubicación de nodos de red
la indicación "s/máquina" y "s/tarjeta" indica que no hay equipo o no hay tarjeta de Red
pero se dejó el servicio activo
Elaboró César E. Vázquez Moreno
Comisión de Avalúos de Bienes Nacionales


4° PISO
servicio DGE
1
2
3
4
servicio DGT
5
6
7
8
9
servicio DGT
29
servicio DGE
19
20
27
22
23
26
servicio DGT
servicio DGE
21
24
25
13
servicio DGT
12
servicio DGT
11
16
15
28
SALA DE JUNTAS
18
DUCTO
BAÑO
ELEVADORES
17
14
ESCALERAS DE EMERGENCIA
Plano de ubicación de nodos de red
la indicación "s/máquina" y "s/tarjeta" indica que no hay equipo o no hay tarjeta de Red,
para se dejó al servicio activo
Elaboró César E. Vázquez Moreno
Comisión de Análisis de Bienes Nacionales


5º PISO
servicio DGT
2
s/máquina DGT
3
4
servicio DGT
5
6
7
8
25
1
servicio DGT
13
12
14
15
16
17
18
26
19
20
21
11
s/máquina DGT
24
SALA DE JUNTAS
23
22
10
DUCTO
BAÑO
ELEVADORES
9
ESCALERAS DE EMERGENCIA


6° PISO
servicio SG
17
16
18
1-10
servicio INF - PRES.
11
12
13
s/máquina
19
20
21
22
23
25
28
26
s/máquina SG
24
SALA DE JUNTAS
27
DUCTO
BAÑO
ELEVADORES
15
14
ESCALERAS DE EMERGENCIA
Plano de ubicación de nodos de red
la indicación "s/máquina" y "s/tarjeta" indica que no hay equipo o no hay tarjeta de Red,
pero se deja el servicio activo
Elaboró César E. Vázquez Moreno
Comisión de Avalúos de Bienes Nacionales



Plano de ubicación de nodos de red
la indicación "s/maquina" y "s/tarjeta" indica que no hay equipo o no hay tarjeta (c. .zc.
pero se dejó el servicio activo

Elaboró César E. Vázquez Moreno
Comisión de Avalúos de Bienes Nacionales

2 Asignación de direcciones IP, Señalizaión de Acometida y Usuarios por nodo

RELACIóN DEL 1er PISO EN EL DEPTO. DE CAJAS

PERSONA	MTS.	#HUB	#PUERTO	#CABLE	UBICACIóN	INSTALACIóN	DIRECCIóN IP
LAURA GARCIA	18	3	7	1	34	↓	172.30.110.108
DORA E. VILLARROEL	20	3	16	2	35	↓	172.30.110.109

RELACIóN DEL 2do PISO DE CONTALORIA INTERNA

PERSONA	MTS.	#HUB	#PUERTO	#CABLE	UBICACIóN	INSTALACIóN	DIRECCIóN IP
JAIME PEREZ	14	1	5	7	1	↑	S/M*
ROGELIO MEDINA	7	1	1	9	2	↑	172.30.110.117
MARICRUZ GARCIA	10	1	10	10	3	↑	172.30.110.118
JAVIER F. AGUILAR	13	1	11	11	4	↑	S/T**
PEDRO GONZALEZ	16	1	12	12	5	↑	172.30.110.119
GUILMARO A. JIMENEZ	22	1	13	13	6	↑	172.30.110.19
CARLOS GONZALEZ	17	1	14	14	7	↑	172.30.110.17
YANINA SHULZ	22	2	1	16	8	↑	172.30.110.18
FAISAL SABAJ	25	2	2	17	9	↑	S/M*
LIDIA YESCAS	28	2	3	18	10	↑	172.30.110.22
SILVIA VILLAVISENCIC	33	2	4	19	11	↑	172.30.110.21
CLARA CASTRO	30	2	5	20	12	↑	
MARICELA TRUJILLO	34	2	6	21	13	↑	172.30.110.26
DANIEL BADILLO	30	2	7	22	14	↑	172.30.110.27
ESTELA PEREZ	27	1	16	23	15	↑	S/T**
PATRICIA SUAREZ	27	2	9	24	16	↑	172.30.110.25
GERARDO RODRIGUEZ	25	2	10	25	17	↑	172.30.110.24
ALFONSO GONZALEZ	25	2	11	28	18	↑	S/T**
HUGO GUERRERO	28	2	12	29	19	↑	172.30.110.23
FELIPE GOMEZ	18	2	13	30	20	↑	172.30.110.110
JOSE TRINIDAD	12	2	14	31	21	↑	S/M*
LUIS ESQUIVEL	15	2	15	32	22	↑	172.30.110.112
SABINO LARA	14	2	16	33	23	↑	172.30.110.111
MARIA D.C. GARCIA	15	1	3	5	24	↑	172.30.110.113
ESTEBAN MARTINEZ	15	1	2	4	25	↑	172.30.110.114
FAUSTO AVENDAÑO	15	1	4	6	26	↑	172.30.110.115
CLAUDIA QUIÑONES	9	1	6	8	27	↓	172.30.110.116
JULIAN CARTA	19	3	6	39	28	↓	172.30.110.120
SILVIA PEREZ	23	3	15	38	29	↓	172.30.110.121
SAUL PONCE	18	3	3	36	30	↓	172.30.110.16
HIPOLITA PEREZ	21	3	4	37	31	↓	S/T**
MARTIN SERRANO	18	3	1	34	32	↓	S/T**
ISIDRO GOMEZ	21	3	2	33	33	↓	S/T**

S/M* (SIN MAQUINA)
S/T** (SIN TARJETA DE RED)

NOTA: SE AGREGA PLANO DE UBICACIóN. LAS FLECHAS INDICAN LA INSTALACIóN ↑ POR ARRIBA Y ↓ POR ABAJO.

RELACIóN DEL 3er PISO DE DIR. GRAL DE ADMON. Y FIN.

PERSONA	MTS.	#HUB	#PUERTO	#CABLE	UBICACIóN	INSTALACIóN	DIRECCIóN IP
NORMA CRUZ	33	1	6	6	27	↓	S/T**
UBILFREDO CONSTANTINO	30	1	2	2	9	↑	172.30.110.33
JOSE CRUZ	25	1	4	4	6	↑	172.30.110.31
ERNESTO ALARCON	28	1	3	3	8	↑	172.30.110.32
JOSE CRUZ	25	1	5	5	7	↑	S/T**
SANDRA MANCEBO	30	1	7	7	26	↓	S/M*
MEDRANO JIMENEZ	16	1	9	8	4	↑	S/M*
MA.D.CARMEN VALDESPINO	9	1	10	9	3	↑	S/T**
SILVERIO SANCHEZ	9	1	11	10	29	↑	172.30.110.129
SERGIO SANCHEZ	25	2	2	18	21	↓	172.30.110.34
GUADALUPE GASCA	25	2	5	22	23	↓	172.30.110.35
GUADALUPE ESCAMILLA	30	2	6	23	24	↓	172.30.110.36
VIRGINIA JIMENEZ	28	2	7	24	22	↓	172.30.110.127
GABRIELA BEJARANO	18	2	10	28	12	↑	172.30.110.29
MARCIANO DELGADO	21	2	11	29	10	↑	172.30.110.38
ALEJANDRO HERNANDEZ	33	2	12	30	28	↑	S/T**
CARLOS CARRION	23	2	15	33	11	↑	172.30.110.126
PATRICIA PEDRON	25	1	12	11	13	↓	S/M*
ROSARIO VELAZQUEZ	25	1	14	13	15	↓	172.30.110.30
S/M	13	2	4	20	20	↓	S/M*
S/M	25	2	3	19	19	↓	S/M*
S/T	5			26	2	↑	S/M*
GILBERTO N. GARCIA	20	2	4	20	5	↑↓	S/M*
S/M	25	1	13	12	14	↓	S/M*
S/M	25	1	15	14	16	↓	S/M*
S/M	27	1	16	15	17	↓	S/M*
S/M	26	2	1	16	18	↓	S/M*
LUCIA ARTEAGA	33	1	1	1	25	↓	172.30.110.37
						↑	172.30.110.28
LAURA RAMIREZ	8	2	14	32	1	↑	172.30.110.125

S/M* (SIN MAQUINA)
S/T** (SIN TARJETA DE RED)

NOTA: SE AGREGA PLANO DE UBICACIóN. LAS FLECHAS INDICAN LA INSTALACIóN ↑ POR ARRIBA Y ↓ POR ABAJO.

RELACIóN DEL 4to PISO DE DIRECCIóN GRAL. DE AVALUOS

PERSONA	MTS.	#HUB	#PUERTO	#CABLE	UBICACIóN	INSTALACIóN	DIRECCIóN IP
ANGELA ROJO	6	1	1	1	1	↑	172.30.110.41
PEDRO PASTRANA	6	1	2	2	2	↑	172.30.110.42
PETRA FRAGOSO	15	1	3	3	3	↑	S/T**
MARCOS IBAÑEZ	12	1	4	4	4	↑	172.30.110.43
TERESA MENDIETA	15	1	5	5	5	↑	172.30.110.44
ALEJANDRO CAMBEROS	18	1	6	6	6	↑	172.30.110.45
ITZEL DE LA CRUZ	18	1	7	7	7	↑	172.30.110.46
MA.DELA LUZ GARDUÑO	19	1	9	8	8	↑	172.30.110.47
HUMBERTO SANDOVAL	25	1	10	9	9	↑	S/T**
ARTURO MALAGON	27	1	11	10	10	↑	172.30.110.48
ARTURO MALAGON	30	1	12	11	11	↑	S/M*
VERONICA N. LOPEZ	26	1	13	12	12	↑	172.30.110.59
PATRICIA RODRIGUEZ	20	1	14	13	13	↑	172.30.110.49
ANGELES PAGONA	30	1	15	14	14	↑	172.30.110.123
JAZMIN ORTIZ	26	1	16	15	15	↑	172.30.110.60
ELVIA ESQUIVEL	23	2	1	16	16	↑	172.30.110.122
SALVADOR ROMERO	23	2	2	17	17	↑	172.30.110.62
GABRIELA MAYORCA	17	2	3	18	18	↑	172.30.110.55
EDITH GONZALEZ	15	2	4	19	19	↓	172.30.110.54
EDUARDO MARRUFO	17	2	5	20	20	↓	172.30.110.53
ROSARIO MIRANDA	24	2	6	24	21	↓	172.30.110.56
GUILLERMO ROMERO	24	2	7	23	22	↓	172.30.110.52
EDMUNDO PARRA	21	2	9	25	23	↓	172.30.110.124
BEATRIZ SABAROBA	21	2	10	21	24	↓	172.30.110.57
GUADALUPE APOLINAR	24	2	11	22	25	↓	172.30.110.58
CLAUDIA RANGEL	24	2	12	26	26	↓	172.30.110.50
GUILLERMO LOPEZ	21	2	13	27	27	↓	S/T**
SALA DE JUNTAS	15	2	14	28	28	↑	172.30.110.39
ROSARIO VILLANUEVA	9	2	15	29	29	↑	172.30.110.40

S/M* (SIN MAQUINA)
S/T** (SIN TARJETA DE RED)

NOTA: SE AGREGA PLANO DE UBICACIóN.
LAS FLECHAS INDICAN LA INSTALACIóN
↑ POR ARRIBA Y ↓ POR ABAJO.

RELACIóN DEL 5to PISO DE DIRECCIóN GRAL. TECNICA

PERSONA	MTS.	#HUB	#PUERTO	#CABLE	UBICACIóN	INSTALACIóN	DIRECCIóN IP
ELIZABETH RODRIGUEZ	8	1	3	1	1	▲	172.30110.65
ALAN PSHIVA	2	1	15	16	2	▲	172.30.110.67
HUMBERTO GAYTAN	11	2	5	13	3	▲	S/T**
MIGUEL MARTINEZ	16	1	10	3	4	▲	172.30.110.68
ANTONIO GARDUÑO	20	1	4	7	6	▲	172.30.110.70
JOSE MORA	22	1	7	5	7	▲	172.30.110.71
JAVIER VELA	29	1	6	6	8	▲	172.30.110.72
RODOLFO CEJA	30	1	9	15	9	▲	172.30.110.75
VICTOR LOMELI	28	1	1	8	10	▲	172.30.110.76
DIRECTOR	16	1	14	14	11	▲	172.30.110.64
MARIO VELAZQUEZ	26	2	9	26	12	▼	172.30.110.84
JOEL COLIN M.	20	2	8	25	13	▼	172.30.110.83
NOEMI CORDOBA	22	1	12	2	14	▼	172.30.110.81
EBSON BERDEJA	21	1	16	9	15	▼	172.30.110.82
JUANA BARRIOS	26	1	13	11	16	▼	172.30.110.80
EUSEBIA GALLARDO	21	2	3	20	17	▼	172.30.110.79
MARIA D. P. MARTINEZ	27	2	4	21	18	▼	172.30.110.78
ELSA PANTOJA	22	2	1	17	19	▼	172.30.110.77
JUAN M. FERNANDEZ	24	1	2	19	20	▼	172.30.110.73
EFREN ECHEVERRIA	22	2	11	18	21	▼	172.30.110.74
ALEJANDRO GARCIA	22	2	7	24	22	▲	172.30.110.85
MIGUEL GONZALEZ	22	2	6	23	23	▲	172.30.110.86
SALA DE JUNTAS	17	2	5	22	24	▲	S/M*
ALEJANDRO CORTES	16	1	10	4	5	▲	172.30.110.69
MA.LUISA ESCOBEDO	6	2	12	27	25	▲	172.30.110.66

S/M* (SIN MAQUINA)
S/T** (SIN TARJETA DE RED)

NOTA: SE AGREGA PLANO DE UBICACIóN.
LAS FLECHAS INDICAN LA INSTALACIóN
▲ POR ARRIBA Y ▼ POR ABAJO.

RELACIóN DEL 6to. PISO DE SECRETARIA GENERAL

PERSONA	MTS.	#HUB	#PUERTO	#CABLE	UBICACIóN	INSTALACIóN	DIRECCIóN IP
SISTEMAS	7	1	1	1	1	↑	S/M*
SISTEMAS	8	1	2	2	2	↑	172.30.110.252
SISTEMAS	7			3	3	↑	S/M*
SISTEMAS	7			4	4	↑	S/M*
SISTEMAS	8	1	5	5	5	↑	172.30.110.253
SISTEMAS	8	2	14	6	6	↑	172.30.110.250
SISTEMAS					7	↑	S/M*
SISTEMAS					8	↑	S/M*
SISTEMAS					9	↑	S/M*
SISTEMAS					10	↑	S/M*
BENJAMIN ALVARADO	8	1	11	11	11	↑	172.30.110.93
MA.DEL PILAR REYES	9	1	12	12	12	↑	172.30.110.94
IGNACIO LOPEZ	14	1	13	13	13	↑	S/M*
JOSE A. SANCHEZ	16	1	14	14	14	↑	172.30.110.100
ANTONIO KLIMOS	13	1	6	15	15	↑	172.30.110.101
DIRECTOR	13	2	1	16	16	↑	172.30.110.87
MARIELENA GARFIAS	9	2	2	17	17	↑	S/T**
MIRIAN RODRIGUEZ	13	2	3	18	18	↑	172.30.110.88
DANIEL VAZQUEZ	8	2	4	19	19	↑	172.30.110.89
BEATRIZ GARCIA	12	2	5	20	20	↓	172.30.110.95
JOAQUIN JIMENEZ	14	2	6	21	21	↓	172.30.110.92
ANGEL BALTAZAR	18	2	7	22	22	↓	172.30.110.91
JOSE SEVILLA	22	2	15	23	23	↓	172.30.110.96
SALA DE JUNTAS	20	2	9	24	24	↑	S/M*
NATALIA HERNANDEZ	20	2	10	25	25	↓	172.30.110.97
ROSALINDA MANSO	20	2	11	26	26	↓	172.30.110.99
ROCIO JIMENEZ	11	2	12	27	27	↑	172.30.110.90
SARA MONTOYA	20	2	13	28	28	↓	172.30.110.98

RELACIóN DEL 7mo. PISO DE PRESIDENCIA

PERSONA	MTS.	#HUB	#PUERTO	#CABLE	UBICACIóN	INSTALACIóN	DIRECCIóN IP
CRISTINA LOPEZ	19	2	16	1	1	↑	172.30.110.105
FERNANDO VAZQUEZ	28	1	7	2	2	↑	172.30.110.106
SAMUEL ALLALA	16	1	16	3	3	↑	172.30.110.104
ALEJANDRA DIAZ	17	1	15	4	4	↑	172.30.110.103
IRMA DEL C. GALVAN	22	1	9	5	5	↑	172.30.110.102
SALA DE JUNTAS	30	1	10	6	6	↑	172.30.110.107

S/M* (SIN MAQUINA)
S/T** (SIN TARJETA DE RED)

NOTA: SE AGREGA PLANO DE UBICACIóN, LAS FLECHAS INDICAN LA INSTALACIóN ↑ POR ARRIBA Y ↓ POR ABAJO.

3 Relación de Material y equipo utilizado

TOTAL DE CABLE UTILIZADO POR CADA PISO:

PISO 1	38 mts
PISO 2	666 mts
PISO 3	665mts
PISO 4	571 mts
PISO 5	496 mts
PISO 6	305 mts
PISO 7	132 mts
TOTAL	2872 mts

TOTAL DE CONECTORES RJ45 POR PISO

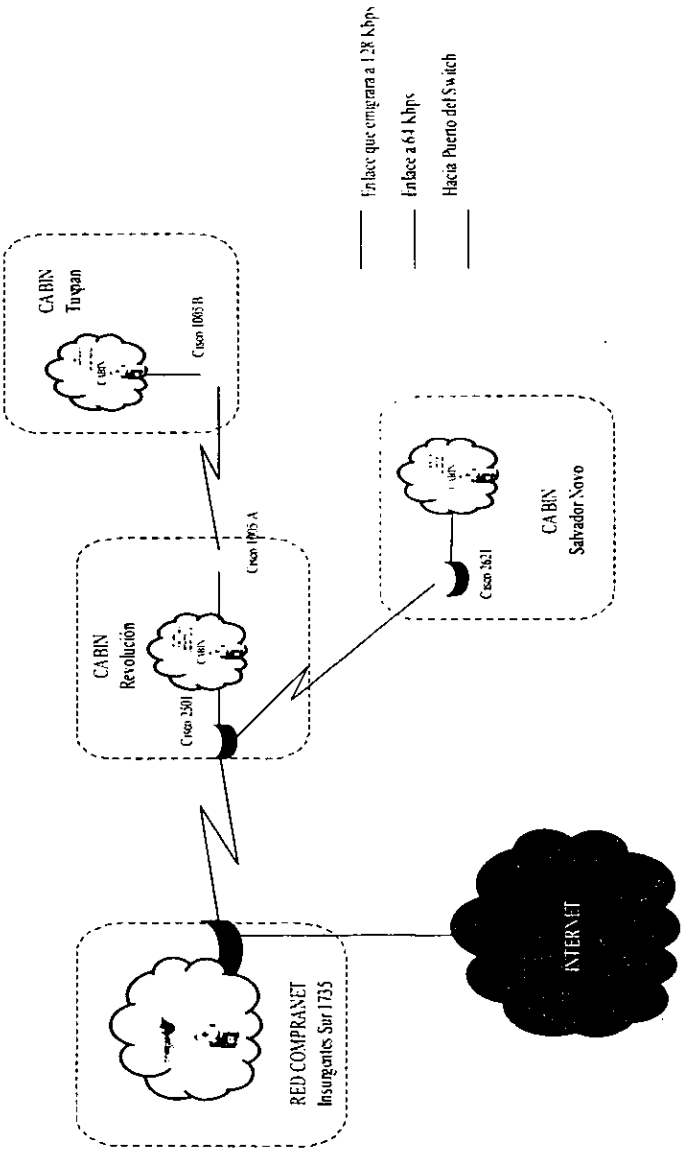
PISO 1	4
PISO 2	68
PISO 3	65
PISO 4	60
PISO 5	50
PISO 6	50
PISO 7	16
TOTAL	313

TOTAL DE HUBS Y PUERTOS POR PISO

PISO 1	0hubs	PUERTOS	2 pts
PISO 2	3hubs	PUERTOS	35 pts
PISO 3	2hubs	PUERTOS	29 pts
PISO 4	2hubs	PUERTOS	29 pts
PISO 5	2hubs	PUERTOS	25 pts
PISO 6	2hubs	PUERTOS	22 pts
PISO 7	(nota: en este piso el hubs los Nodos estan en el Hub del 6to. Piso)	PUERTOS	6 pts
TOTAL	11hubs		

TOTAL DE CINTURONES	120
TOTAL DE CINTAS DE AISLAR	15
TOTAL DE CINTAS ADHESIVAS	3
TOTAL DE CANALETAS	19
SE UTLIZO 1 SILICON DE CARTULLO	
SE UTILIZO 1 CAJA DE PLASTIGRAPAS	

3 Diagrama de conexión de la Red Metropolitana de la CABIN



Capítulo V

Marco Instrumental

En este capítulo se llevará a cabo la propuesta para el control, seguimiento de las actividades y supervisión del proyecto.

Actividades a realizarse y tiempos estimados

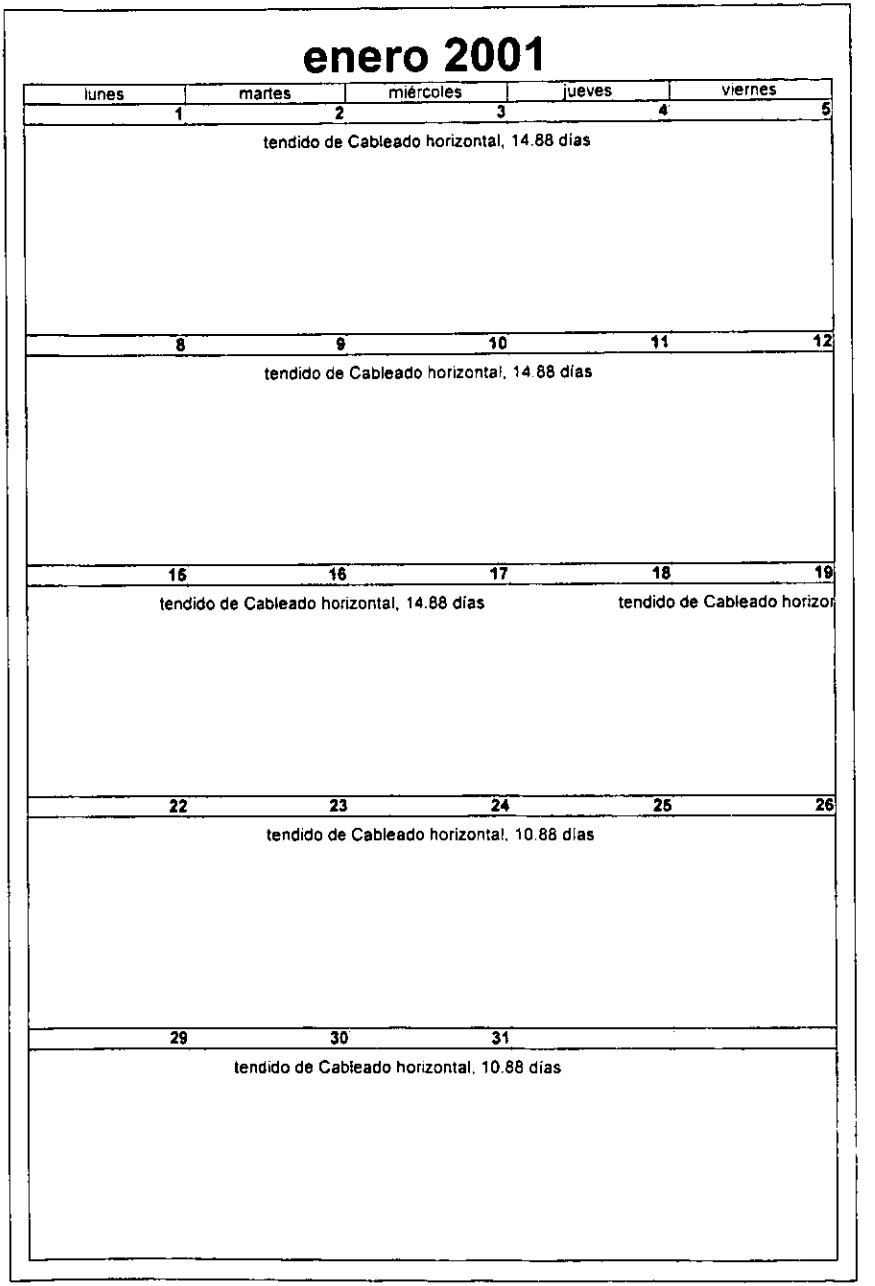
Nombre de la Actividad	Duración (Aproximada)	Fecha de Inicio (Propuesta)	Etapa
Planeación y Estimación de la cantidad de material a utilizar	1dia	4/12/00	Primera
Planeación y Estimación del equipo activo	1dia	5/12/00	Primera
Planeación y Estimación de la cantidad de personal a utilizar	1dia	6/12/00	Primera
Estimación del tiempo a utilizar para la configuración de equipos	1dia	7/12/00	Primera
Estimación del tiempo a utilizar para la configuración de servidores y equipos de comunicación	1dia	8/12/00	Primera
Tendido de Cableado Vertical	7 días	11/12/00	Segunda
Tendido de Cableado horizontal	49 días	22/12/00	Tercera
Instalación de Servidores	Indefinido	11/12/00	Cuarta
Instalación de Clientes y Tarjetas	Indefinido	11/12/00	Quinta
Memoria Técnica	14dias	4/9/01	Sexta

Propuesta de Recursos

Nombre del Recurso	Grupo	Unidad	Costo	Cantidad Estimada
Cable UTP Nivel 5	MATERIAL	Bobina	$1,500.00	9 bobinas
Conectores rj45	MATERIAL	caja	$500.00	7 cajas
Instalador de Canaleta y Cable	RH	Jornada	$400.00	1 diaria
Guía Metálica	MATERIAL	pieza	$800.00	2 piezas
Escalera	MATERIAL	pieza	$800.00	1 piezas
Herramienta en Gral.	MATERIAL	Lote	$3,500.00	1 lote
Charolas	MATERIAL	Pieza	$600.00	7 piezas
Hubs	ACTIVO	Pieza	$2500.00	17 piezas
Varios	MATERIAL	Lote	$250.00	1 lote
Canaleta	MATERIAL	Ml	$60.00	3000ml
Líder de Proyecto	RH	hora	$250.00	
Administrador	RH	hora	$350.00	

diciembre 2000

lunes	martes	miercoles	jueves	viernes
				1
4	5	6	7	8
Plan y Estimac	Plan y Estimac	Planeacion y E	Estimacion de	Estimacion del
11	12	13	14	15
		Instalacion de Servidores, 7 88 días Instalacion de Clientes y Taejetas, 6.88 días		
18	19	20	21	22
				tendido de Cableado
	Instalacion de Servidores, 7.88 dias			
Instalacion de Clientes y Taejetas,				
25	26	27	28	29
	tendido de Cableado horizontal, 4 88 días			tendido de Cableado


enero 2001
lunes
martes
miércoles
jueves
viernes
1
2
3
4
5
tendido de Cableado horizontal, 14.88 días
8
9
10
11
12
tendido de Cableado horizontal, 14.88 días
15
16
17
18
19
tendido de Cableado horizontal, 14.88 días
tendido de Cableado horizor
22
23
24
25
26
tendido de Cableado horizontal, 10.88 días
29
30
31
tendido de Cableado horizontal, 10.88 días

febrero 2001

lunes	martes	miércoles	jueves	viernes
			1	2
tendido de Cableado horizontal, 10.88 días				tendido
5	6	7	8	9
tendido de Cableado horizontal, 10.88 días				
12	13	14	15	16
tendido de Cableado horizontal, 10.88 días				
19	20	21	22	23
tendido de	tendido de Cableado horizontal, 10.88 días			
26	27	28		
tendido de Cableado horizontal, 10.88 días				

marzo 2001

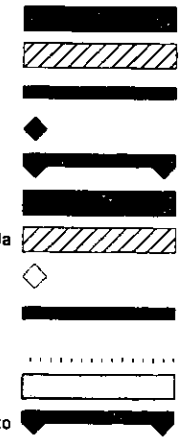
lunes	martes	miércoles	jueves	viernes
			1	2
tendido de Cableado horizontal, 10.88 días				
5	6	7	8	9
tendido de Cableado horizontal,		tendido de Cableado horizontal, 10.88 días		
12	13	14	15	16
tendido de Cableado horizontal, 10.88 días				
19	20	21	22	23
tendido de Cableado horizontal, 10.88 días		tendido de Cableado horizontal, 10.88 días		
26	27	28	29	30
tendido de Cableado horizontal, 10.88 días				

abril 2001

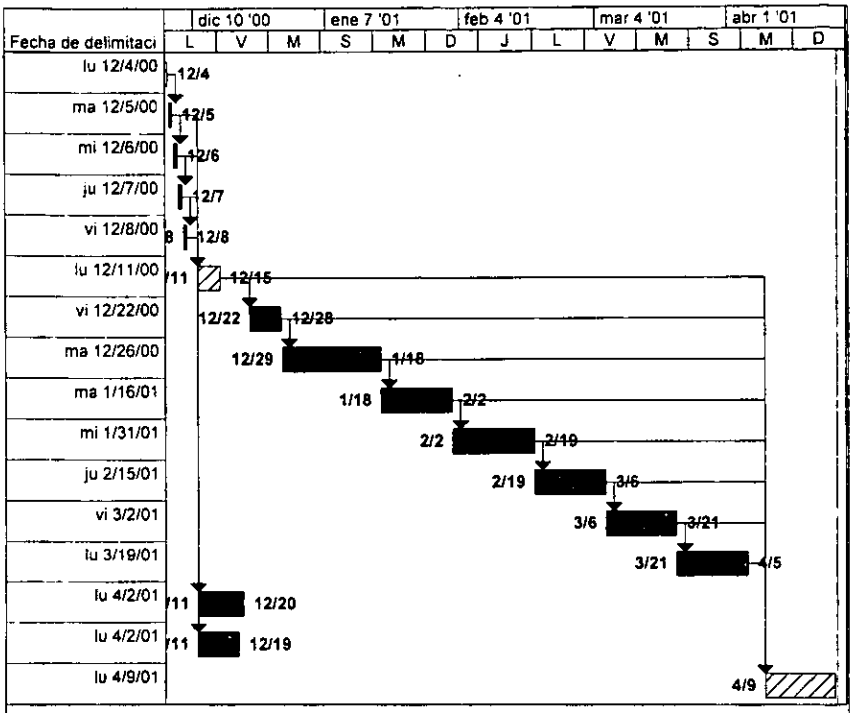
lunes	martes	miércoles	jueves	viernes
2	3	4	5	6
tendido de Cableado horizontal, 10.88 días				
9	10	11	12	13
Memoria Tecnica, 10.88 días				
16	17	18	19	20
Memoria Tecnica, 10.88 días				
23	24	25	26	27
Memoria Tecni				
30				

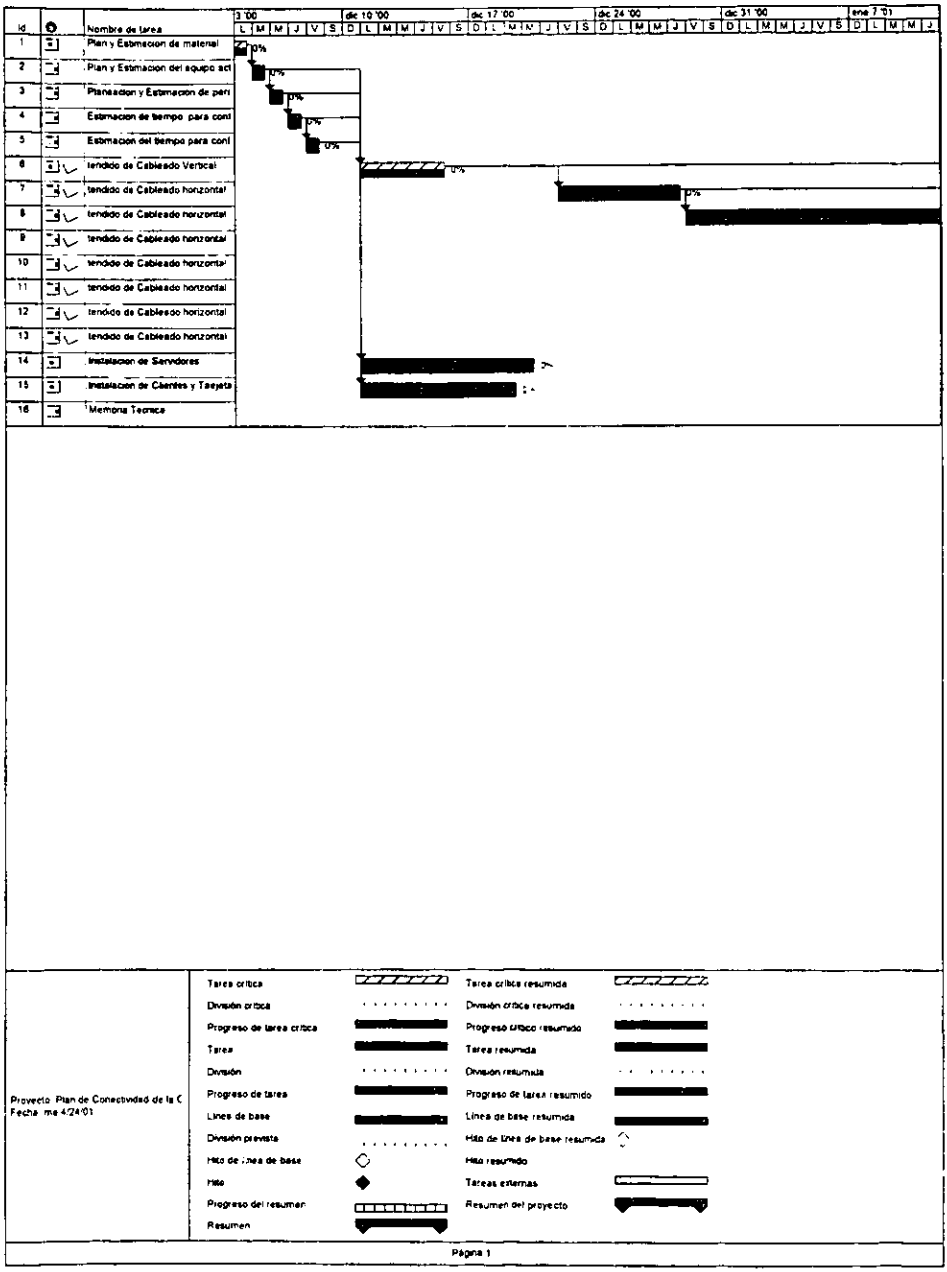
Id	Nombre de tarea	Duración	Tipo de delimitación
1	Plan y Estimacion de material	0.88 días	Debe comenzar el
2	Plan y Estimacion del equipo activo	0.88 días	No comenzar antes del
3	Planeacion y Estimacion de person	0.88 días	No comenzar antes del
4	Estimacion de tiempo para configu	0.88 días	No comenzar antes del
5	Estimacion del tiempo para configu	0.88 días	No comenzar antes del
6	tendido de Cableado Vertical	4.88 días	Debe comenzar el
7	tendido de Cableado horizontal	4.88 días	No comenzar antes del
8	tendido de Cableado horizontal	14.88 días	No comenzar antes del
9	tendido de Cableado horizontal	10.88 días	No comenzar antes del
10	tendido de Cableado horizontal	10.88 días	No comenzar antes del
11	tendido de Cableado horizontal	10.88 días	No comenzar antes del
12	tendido de Cableado horizontal	10.88 días	No comenzar antes del
13	tendido de Cableado horizontal	10.88 días	No comenzar antes del
14	Instalacion de Servidores	7.88 días	No finalizar después del
15	Instalacion de Clientes y Taejetas	6.88 días	No finalizar después del
16	Memoria Tecnica	10.88 días	No comenzar antes del

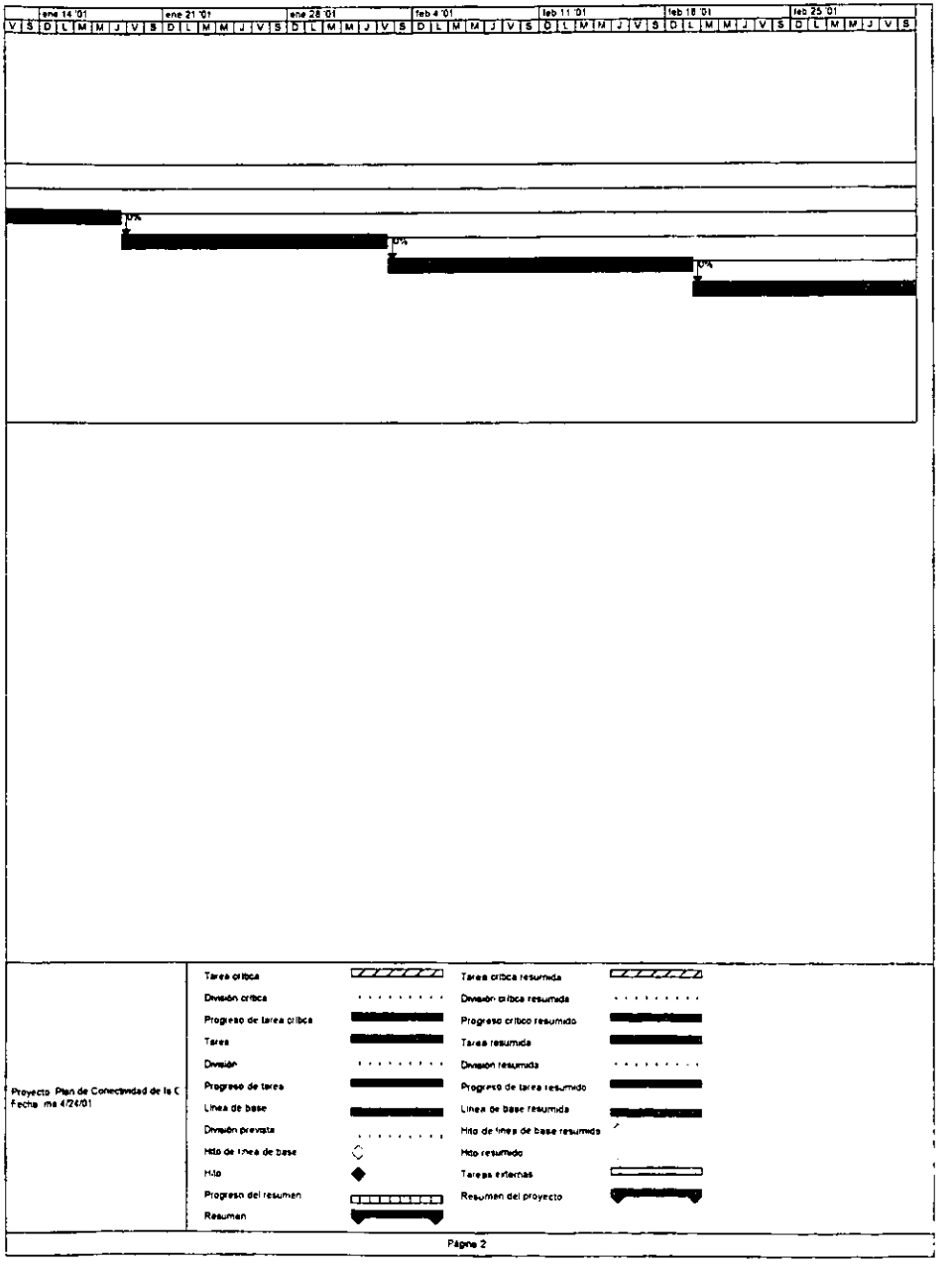
Proyecto: Plan de Conectividad de la
Fecha: ma 4/24/01

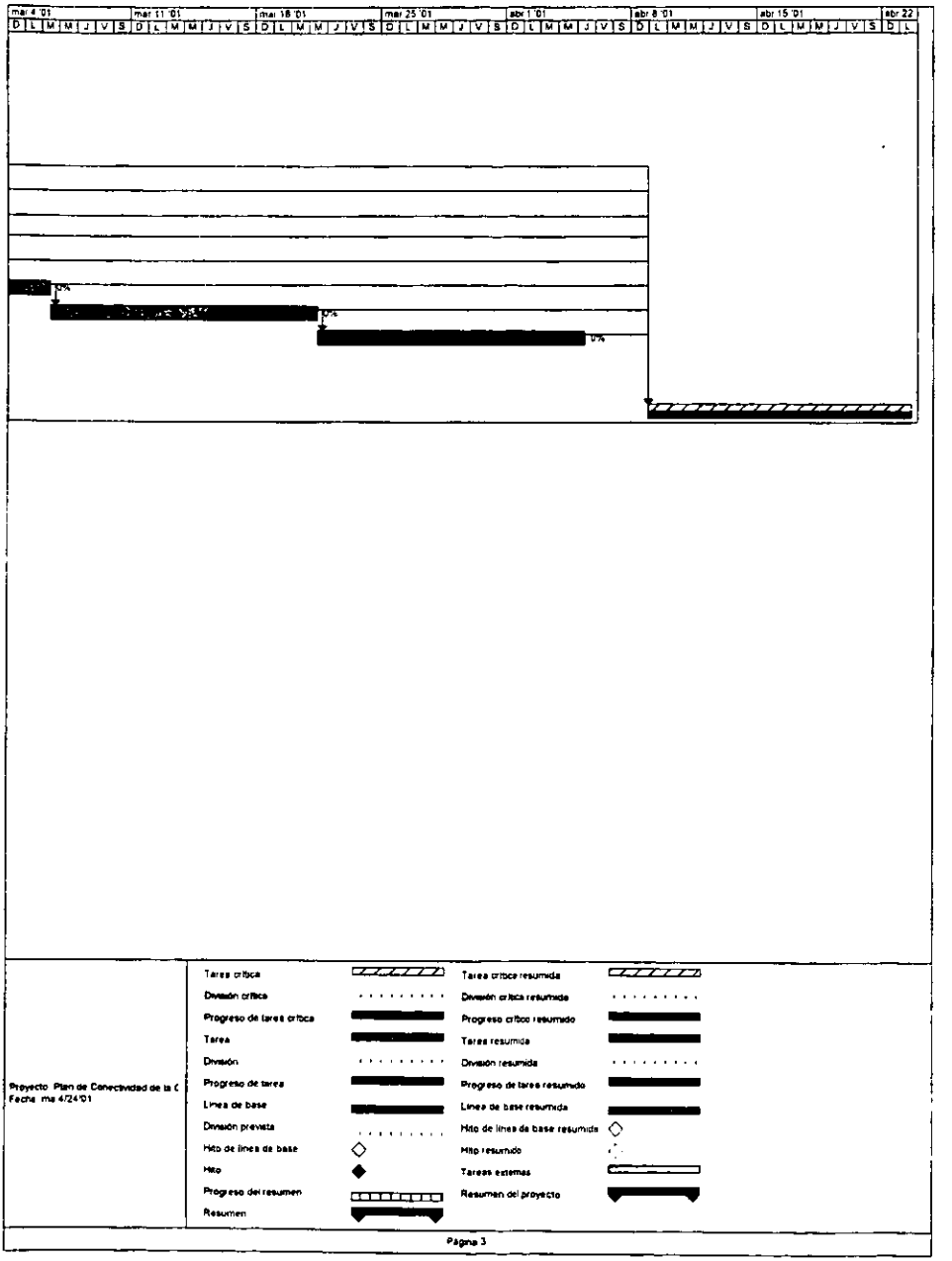


Página 1


dic 10 '00
ene 7 '01
feb 4 '01
mar 4 '01
abr 1 '01
Fecha de delimitaci
L V M S M D J L V M S M D
lu 12/4/00
ma 12/5/00
mi 12/6/00
ju 12/7/00
vi 12/8/00
lu 12/11/00
vi 12/22/00
ma 12/26/00
ma 1/16/01
mi 1/31/01
ju 2/15/01
vi 3/2/01
lu 3/19/01
lu 4/2/01
lu 4/2/01
lu 4/9/01
12/4
12/5
12/6
12/7
12/8
12/15
12/22
12/28
12/29
1/18
1/18
2/2
2/2
2/19
2/19
3/6
3/6
3/21
3/21
4/5
12/20
12/19
4/9
Proyecto: Plan de Conectividad de la
Fecha: ma 4/24/01
Tarea
Tarea crítica
Progreso
Hito
Resumen
Tarea resumida
Tarea crítica resumida
Hito resumido
Progreso resumido
División
Tareas externas
Resumen del proyecto
Página 2


Id
Nombre de tarea
3 '00
dic 10 '00
dic 17 '00
dic 24 '00
dic 31 '00
ene 7 '01
1 Plan y Estimacion de material
2 Plan y Estimacion del equipo act
3 Planeacion y Estimacion de peri
4 Estimacion de tiempo para cont
5 Estimacion del tiempo para cont
6 tendido de Cableado Vertical
7 tendido de Cableado horizontal
8 tendido de Cableado horizontal
9 tendido de Cableado horizontal
10 tendido de Cableado horizontal
11 tendido de Cableado horizontal
12 tendido de Cableado horizontal
13 tendido de Cableado horizontal
14 Instalacion de Servidores
15 Instalacion de Clientes y Tarjeta
16 Memoria Tecnica
Proyecto: Plan de Conectividad de la C
Fecha: mie 4/24/01
Tarea critica
División critica
Progreso de tarea critica
Tarea
División
Progreso de tarea
Linea de base
División prevista
Hito de línea de base
Hito
Progreso del resumen
Resumen
Tarea critica resumida
División critica resumida
Progreso critico resumido
Tarea resumida
División resumida
Progreso de tarea resumido
Linea de base resumida
Hito de línea de base resumida
Hito resumido
Tareas externas
Resumen del proyecto
Página 1


ene 14 '01
ene 21 '01
ene 28 '01
feb 4 '01
feb 11 '01
feb 18 '01
feb 25 '01
V S D L M M J V S D L M M J V S D L M M J V S D L M M J V S D L M M J V S D L M M J V S
0%
0%
0%
Proyecto: Plan de Conectividad de la C
Fecha: mié 4/24/01
Tarea crítica
División crítica
Progreso de tarea crítica
Tarea
División
Progreso de tarea
Línea de base
División prevista
Hito de línea de base
Hito
Progreso del resumen
Resumen
Tarea crítica resumida
División crítica resumida
Progreso crítico resumido
Tarea resumida
División resumida
Progreso de tarea resumido
Línea de base resumida
Hito de línea de base resumido
Hito resumido
Tareas externas
Resumen del proyecto
Página 2


mar 4 '01
mar 11 '01
mar 18 '01
mar 25 '01
abr 1 '01
abr 8 '01
abr 15 '01
abr 22
Proyecto: Plan de Conectividad de la C
Fecha: mié 4/24/01
Tarea crítica
División crítica
Progreso de tarea crítica
Tarea
División
Progreso de tarea
Línea de base
División prevista
Hito de línea de base
Hito
Progreso del resumen
Resumen
Tarea crítica resumida
División crítica resumida
Progreso crítico resumido
Tarea resumida
División resumida
Progreso de tarea resumido
Línea de base resumida
Hito de línea de base resumida
Hito resumido
Tareas externas
Resumen del proyecto
Página 3

Conclusiones

La característica principal de este proyecto consistió en realizar un plan de telecomunicaciones, que satisfaciera la necesidad de conectividad de la CABIN, la solución aquí propuesta se basó en la visión a futuro de la Alta Dirección de la Comisión de Avalúos de Bienes Nacionales que previó un sistema automatizado para el registro de solicitudes, control y seguimiento de los avalúos realizados, así como la creación y mantenimiento de una base de datos inmobiliaria, susceptible de ser comercializada; todo esto por Internet.

La Comisión de Avalúos de Bienes Nacionales contará con una infraestructura que le permitirá llevar a cabo proyectos informáticos ambiciosos, al tener una base de telecomunicaciones moderna, eficiente y bien organizada. Con estas herramientas, la Comisión estará preparada para afrontar los retos que el mercado ofrezca en materia de soporte técnico, aplicaciones de oficina y sistemas prioritarios especializados.

Para llegar a los objetivos antes mencionados, este proyecto proporcionará los elementos necesarios para crear una nueva infraestructura que contenga características tales como:

- Una tecnología capaz de soportar voz y datos a través de un sistema de cableado estructurado que permita utilizar los más modernos equipos de comunicación telefónica (Servidores "PBX") y de datos.

- Se podrán desarrollar ahora los sistemas informáticos programados para el siguiente año fiscal, en especifico, el "Sistema Integral de Información de Avalúos" y el "Sistema Integral de Administración y Finanzas" que son los sistemas medulares de esta Comisión.

- Quedarán enlazados los tres inmuebles que componen la CABIN en la ciudad de México utilizando enlaces dedicados a 128Kb, contratados con Telmex y logrando así tener una red metropolitana que dará servicio a mas de 300 usuarios.

- Esta comisión tendrá presencia en Internet a través de COMPRANET que a su vez este órgano pertenece a la red institucional del gobierno federal, logrando así que las nueve delegaciones regionales que forman parte de la Comisión de Avalúos de Bienes Nacionales puedan tener acceso al "Sistema Integral de Información de Avalúos" de forma remota.

- Será creado un sistema de mensajería más rápido y eficiente, contemplando para este sistema los servicios de correo electrónico, programación de actividades y sincronización de agendas.

Por lo que concluyo que el desarrollo de este proyecto me llevó a afianzar mis conocimientos teóricos sobre redes y telecomunicaciones adquiridos en mis estudios profesionales.

El manejo de tecnología de punta, como es el caso de ruteadores, sistemas de telecomunicaciones complejos y redes, ha actualizado mi conocimiento el cual puede ser aplicado en muchas áreas del campo profesional.

La aplicación de conceptos directamente al diseño, desarrollo e implantación de sistemas funcionales, y el trabajo de investigación y documentación realizado, así como la convivencia con personal altamente especializado ha enriquecido y ampliado mi visión del ámbito profesional, dándome experiencia sobre áreas del campo laboral que antes no tenía, como son: la Administración y optimización de recursos, manejo de personal, organización de actividades laborales y la habilidad de manejar grandes proyectos, profesional y éticamente.

Anexo 1

Estándar ANSI/TIA/EIA 568 cableado estructurado

Las normas sobre las cuales rige este estándar son:

Sistema de cableado estructurado horizontal.

Abarca desde la estación de trabajo del usuario final, hasta el cuarto de telecomunicaciones y consta de dos elementos básicos:

1. Cable Horizontal y Hardware de Conexión (también llamado "cableado horizontal"). Proporcionan los medios para transportar señales de telecomunicaciones.

2. Rutas y Espacios Horizontales (también llamado "sistemas de distribución horizontal"). Son utilizados para distribuir y soportar cable horizontal y conectar hardware entre la salida del área de trabajo y el cuarto de telecomunicaciones. Estas rutas y espacios son las "canaletas y rosetas" del cableado horizontal.

El cableado horizontal incluye:

- Las salidas (rosetas) de telecomunicaciones en el área de trabajo del usuario final.
- Cables y conectores de transición instalados entre las salidas del área de trabajo del usuario final y el cuarto de telecomunicaciones.
- Páneles de parcheo (patch) y cables de parcheo utilizados para configurar las conexiones de cableado horizontal en el cuarto de telecomunicaciones.

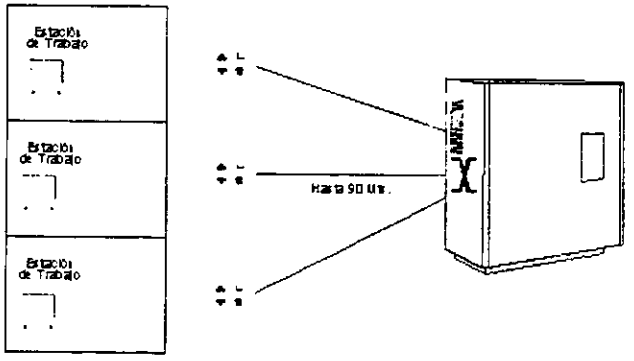


Figura 1. Esquema de Cableado Horizontal

Consideraciones de diseño

Los costos en materiales, mano de obra e interrupción de labores al hacer cambios en el cableado horizontal pueden ser muy altos. Para evitar estos costos, el cableado horizontal debe ser capaz de manejar una amplia gama de aplicaciones de usuario. La distribución horizontal debe ser diseñada para facilitar el mantenimiento y la reubicación de áreas de trabajo.

El cableado horizontal deberá diseñarse para ser capaz de manejar diversas aplicaciones de usuario, incluyendo:

- Comunicaciones de voz (teléfono).
- Comunicaciones de datos.
- Redes de área local.

El diseñador también debe considerar incorporar otros sistemas de información del edificio (por ejemplo: otros sistemas, como televisión por cable, control ambiental, seguridad, audio, alarmas y sonido) al seleccionar y diseñar el cableado horizontal.

Sistema de cableado estructurado vertical

Comprende los elementos ubicados entre los gabinetes de comunicación. Se aceptan varios medios de transmisión: cable UTP de 4 pares a 100 ohms, cable STP de 4 pares a 150 ohms, cable de fibra óptica 8.7/125µm, monomodo. Cuando se transmiten señales de voz generalmente se emplean cables multipares que deben ir perfectamente identificados y marcados para su fácil determinación. El cableado vertical abarca del closet de cableado del edificio al closet de cableado de cada piso y enlaza en todos los cableados del edificio a un centro único.

Topología

El cableado horizontal se debe implementar en una topología de estrella. Cada salida del área de trabajo del usuario final debe estar conectada directamente al cuarto de telecomunicaciones excepto cuando se requiera hacer transición al cable de alfombra (UTC).

No se permiten parcheos (múltiples apariciones del mismo par de cables en diversos puntos de distribución) en cableados de distribución horizontal.

Algunos equipos requieren componentes (como adaptadores RS-232) en la salida del área de telecomunicaciones. Estos componentes deben instalarse externos a la salida, esto garantiza la utilización del sistema de cableado estructurado para otros usos.

Tipos de cable

Los tres tipos de cable reconocidos para distribución horizontal son:

- Par trenzado, cuatro pares, sin blindaje (UTP) de 100 ohmios, 22/24 AWG
- Par trenzado, dos pares, con blindaje (STP) de 150 ohmios, 22 AWG
- Fibra óptica, dos fibras, multimodo 62.5/125 µm

El cable a utilizar por excelencia es el par trenzado sin blindaje UTP de cuatro pares categoría 5. El cable coaxial de 50 ohms se acepta pero no se recomienda en instalaciones nuevas.

Distancia del cable

La distancia horizontal máxima es de 90 metros para UTP. Esta es la distancia desde el área de trabajo del usuario final hasta el cuarto de telecomunicaciones. Al establecer la distancia máxima se hace la previsión de 10 metros adicionales para la distancia combinada de cables de parcheo (3 metros) y cables utilizados para conectar equipo en el área de trabajo del usuario final y el cuarto de telecomunicaciones.

Consideraciones para conectores de salida

- Un mínimo de 2 rosetas por área de trabajo.
- Un conector para cable UTP / 100Ω. 4 pares.

Los tipos de conectores

- Cable UTP / 10Ω, 4 pares.
- Cable STP / 150Ω, 2 pares.
- Fibra óptica 62.5 / 125µm, 2 fibras.

Destrenzado máximo en la terminación

- Categoría 5: 0.5 pulg.
- Categoría 4: 1.0 pulg.

Manejo del cable

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

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

Evitado de interferencia electromagnética

A la hora de establecer la ruta del cableado de los closets de alambrado a los nodos. es una consideración primordial evitar el paso del cable por los siguientes dispositivos:

- Motores eléctricos grandes o transformadores (mínimo 1.2 metros).
- Cables de corriente alterna.
  - Mínimo 13 cm. para cables con 2KVA o menos.
  - Mínimo 30 cm. para cables de 2KVA a 5KVA.
  - Mínimo 91cm. para cables con más de 5KVA.

- Luces fluorescentes y balastros (mínimo 12 centímetros).
- El ducto debe ir perpendicular a las luces fluorescentes y cables o ductos eléctricos.
- Intercomunicadores (mínimo 12 cm.).
- Equipo de soldadura.
- Aires acondicionados, ventiladores, calentadores (mínimo 1.2 metros).
- Otras fuentes de interferencia electromagnética y de radio frecuencia.

Estándar ANSI/TIA/EIA 568 A y B cableado estructurado

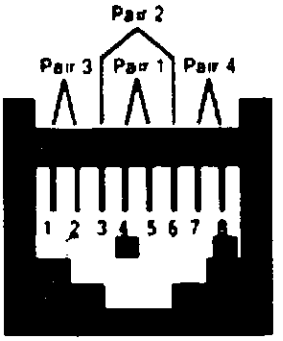
El cable par trenzado 10BASE-T puede ser conectado como "Directo" o en algunos casos. conexión "Cruzada" dependiendo de la aplicación. Para estaciones de trabajo conectadas a un concentrador, se utiliza conexión "Directa" como se ilustra en la tabla A. En algunos casos (por ejemplo: el enlace en cascada de un concentrador a otro. o el enlace de sólo dos estaciones de trabajo). se puede utilizar cableado "cruzado" como se ilustra en la tabla B.

Cableado RJ-45 "Directo"

Número de pin	Número de pin
1 (transmite +)	1 (transmite +)
2 (transmite -)	2 (transmite -)
3 (recibe +)	3 (recibe +)
6 (recibe -)	6 (recibe -)
4,5,7,8	No se utilizan

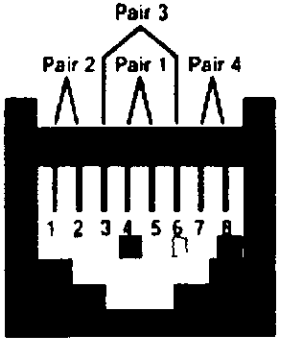
Cableado RJ-45 "Cruzado"

Número de pin	Número de pin
1 (transmite +)	3 (recibe +)
2 (transmite -)	6 (recibe -)
3 (recibe +)	1 (transmite +)
6 (recibe -)	2 (transmite -)
4,5,7,8	No se utilizan



T568A
1 Blanco / verde
2 Verde
3 Blanco / naranja
4 Azul
5 Blanco/Azul
6 Naranja
7 Blanco / café
8 Café

Figura 2 Código de color T568A



T568B
1 Blanco / naranja
2 Naranja
3 Blanco / verde
4 Azul
5 Blanco/Azul
6 Verde
7 Blanco / café
8 Café

Figura 3 Código de colores T568B

Anexo 2

Estándar ANSI/TIA/EIA 569 cableado estructurado

Este estándar rige sobre:

- Ducto dentro de pared (conduit).
- Tipo de ducto conduit
- Metal rígido (conduit).
- Pvc rígido.

Supervisa el cumplimiento de estos requerimientos:

- Estándares eléctricos.
- Ninguna sección debe contener más de 2 dobleces a 90°
- El radio de giro interior debe ser mínimo 6 veces el diámetro interior.
- Si se usa conduit mayores de 2", el radio debe ser mínimo, 10 veces del diámetro interior.
- Para fibra óptica el radio debe ser 10 veces el diámetro interior.

Ductos perimetrales (por superficie).

Alimenta estaciones de trabajo donde los dispositivos de telecomunicaciones pueden ser accesados por la red.

Estilos:

- Ductos por superficie de una canaleta.
- Ductos por superficie multicanal.

Radio de doblaje del cable no menor de 4 veces el diámetro del cable.

Capacidad práctica de llenado de 30-60% dependiendo del radio de doblaje.

Anexo 3

Estándar ANSI/TIA/EIA 606 cableado estructurado

Este estándar se enfoca en la terminación del tipo de cable, localizado en área de trabajo, closet de interconexión, cuarto de equipos y entrada de servicios.

El medio (cable / fibra) de telecomunicaciones entre terminaciones.

Ductos entre terminaciones y derivaciones.

Espacios donde se efectúan las terminaciones.

Empalmes y tierras.

Crea y mantiene registros de información para cada elemento del cableado.

Tiene una relación lógica entre el identificador (etiquetas) y el registro.

El sistema de administración debe incluir etiquetas, registros, reportes, diagramas y órdenes de trabajo.

Los ductos deben contar con una identificación única, este identificador puede ser una etiqueta permanente y debe ir en cada extremo del tendido.

Los espacios que ocupan los medios conductores de cable deben ser identificados.

El cable principal (BACKBONE) y los horizontales deben etiquetarse a cada extremo.

Cada punto de terminación debe ser etiquetado (pánel de identificación, placas de salida).

Los empalmes y el sistema de tierras deben ser identificados.

Anexo 4

Protocolo TCP/IP

Algunos de los motivos de su popularidad son:

- Independencia del fabricante
- Soporta múltiples tecnologías
- Puede funcionar en máquinas de cualquier tamaño
- Estándar de E.U desde 1983

La arquitectura de un sistema en TCP/IP tiene una serie de metas:

- La independencia de la tecnología usada en la conexión a bajo nivel y la arquitectura del ordenador
- Conectividad Universal a través de la red
- Reconocimientos de extremo a extremo
- Protocolos estandarizados

1. Estructura Interna

El modelo básico en Internet es el modelo Cliente / servidor. El Cliente es un programa que le solicita a otro que le preste un servicio. El Servidor es el programa que proporciona este servicio.

La arquitectura de Internet está basada en capas. Esto hace más fácil implementar nuevos protocolos. El conjunto de protocolos TCP/IP, al estar integrado plenamente en Internet, también dispone de este tipo de arquitectura. El modelo de capas de TCP/IP es algo diferente al propuesto por ISO (*International Standard Organization*) para la interconexión de sistemas abiertos (OSI). (Ver figuras 1 y 2).

<table>
<tr><td>Aplicación</td><td rowspan="3">TELNET</td><td rowspan="3">FTP</td><td rowspan="3">SNMP</td><td rowspan="3">SMTP</td><td rowspan="3">DNS</td><td rowspan="3">HTTP</td></tr>
<tr><td>Presentación</td></tr>
<tr><td>Sesión</td></tr>
<tr><td>Transporte</td><td colspan="6">TCP</td></tr>
<tr><td>Red</td><td colspan="6">IP</td></tr>
<tr><td rowspan="2">Liga de Datos</td><td colspan="4">802.2</td><td>X.25</td><td>LLC/SNAP</td></tr>
<tr><td>802.3</td><td colspan="2">802.5</td><td colspan="2">LAPB</td><td>ATM</td></tr>
<tr><td>Física</td><td>Ethernet</td><td>Token Ring</td><td>FDDI</td><td colspan="2">Linea Síncrona WAN</td><td>SONET</td></tr>
</table>

Fig. 1. Relación del modelo TCP IP con el modelo OSI

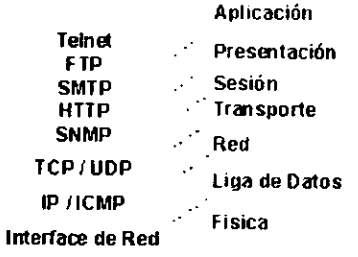


Fig. 2. Modelo de capas de TCP/IP

2. Capa de Aplicación

Esta capa corresponde a las aplicaciones que están disponibles para los usuarios, como TELNET, FTP, SNMP.

2.1. BOOTP (Bootstrap Protocol)

En lugar de utilizar el protocolo ARP, una máquina que acaba de ponerse en funcionamiento por primera vez, puede utilizar el protocolo *bootstrap* para obtener la dirección IP e información sobre su sector de arranque. Este método tiene algunas ventajas respecto al protocolo ARP.

Formato del mensaje

Descripción de los campos: (Ver Tabla 1)

- Tipo (*Type*): Este campo identifica si el mensaje es una solicitud o una respuesta
- Cabecera (*Header*): Este campo identifica el tipo de dirección de *hardware*
- Longitud-H (*H-Length*): Este campo identifica la longitud de la dirección de *hardware* en octetos
- Contador de saltos (*Hop count*): Este mensaje es usado con el protocolo BOOTP a través de varios Gateways. Cada paso por un *Gateways* aumenta en uno el contador.
- ID de Transacción (*transaction ID*): Lo utiliza la estación de trabajo para asignar las respuestas a las solicitudes
- Segundos (*Seconds*): Se utiliza para calcular el tiempo transcurrido desde el envío de la solicitud hasta la recepción de la respuesta.
- Dirección IP del Cliente (*Client IP address*): Este campo lo completa el cliente, si la conoce. En otro caso se pone a cero.
- Dirección IP del servidor (*Server IP address*): Puede ser introducido por el cliente, si la conoce. Cuando el valor es diferente de cero, sólo el servidor especificado puede contestar a la solicitud. Esta es una forma de forzar al servidor para que proporcione la información de arranque.
- Dirección IP del *Gateways* (*Gateways IP address*): Este campo lo pone en cero el cliente, y si la solicitud la obtiene un *Gateways*, este escribe su dirección en este campo.
- Dirección de *Hardware* del cliente (*Client Hardware Address*): Este campo lo completa el cliente
- Nombre del servidor *Host* (*Server Host Name*): Este campo es opcional, y puede ponerlo a cero tanto el servidor como el cliente.
- Nombre del archivo de arranque (*Boot File Name*): Puede ponerlo a cero el cliente, o poner un nombre genérico. El servidor reemplazará este campo por la ruta completa del archivo completo.
- Area del Fabricante (*Vendor-specific area*): Puede tener un código escrito por el cliente.

Tabla 1.
Formato del mensaje BOOTP

Octet +0	*Octet +1*	*Octet +2*	*Octet +3*
7 6 5 4 3 2 1 0	7 6 5 4 3 2 1 0	7 6 5 4 3 2 1 0	7 6 5 4 3 2 1 0
Type	*Header Type*	*H-Length*	*Hop Count*
Transaction ID			
Seconds		*Zero*	
Client IP Address			
Response IP Address			
Server IP Address			
Gateways IP Address			
Client Hardware Address (16 Octets)			
Server Host Name (64 Octets)			
Boot File Name (128 Octets)			
Vendor-Specific Area (64 Octets)			

2..2 DNS (Domain Name Service)

Muchos usuarios prefieren utilizar un nombre que sea más fácil de recordar que una dirección numérica. Para hacer esto, un servidor debe transformar el nombre en la dirección correcta. Esto se hacía originalmente en Internet mediante una tabla única situada en un servidor central donde estaban contenidos todos los nombres de *Host*. Esto era posible debido a que solo existían unos cientos de servidores, pero debido a un gran aumento del número de servidores, fue necesario descentralizar el servidor de nombres y dividirlo en múltiples DNS (servidores de nombres de dominio).

Esto redujo el tiempo de respuesta del servidor y disminuyó el tráfico en la red.

La estructura del sistema de dominios es similar a la estructura de directorios del DOS o del UNIX, es decir, es una estructura en forma de árbol, y los archivos están identificados con una ruta de acceso. La diferencia es que en el DNS la ruta empieza con el nombre del nodo en vez del directorio raíz. Además, las rutas en un servidor DNS se escriben en sentido inverso a las del DOS.

Desde el punto de vista de un programa, el funcionamiento de este servicio en muy simple. El programa proporciona un nombre de dominio, y el DNS le devuelve su dirección IP.

Nombres de dominio

El programa de usuario proporciona el nombre de dominio como una secuencia de palabras. Las palabras están listadas de izquierda a derecha, y la que representa la zona más cercana al usuario es la primera.

Los programas DNS manipulan el nombre del dominio proporcionado por el usuario de manera que sea fácilmente interpretado por otros programas. Para los programas, cada nombre de dominio contiene una secuencia de etiquetas, y cada etiqueta contiene un octeto de longitud seguido por una cadena de caracteres de un subconjunto ASCII. Este subconjunto está formado por caracteres alfa (A-Z), dígitos (0-9) y un signo menos (-).

Arquitectura del DNS

DNS es un protocolo de la capa de aplicación y está clasificado como una utilidad por convenio entre los usuarios y el administrador del sistema, en vez de una parte integrada en los servicios de usuario.

Elementos de programas de DNS

En términos de las especificaciones, DNS consiste en un programa de usuario, un cliente, un servidor de nombres, y un servidor de nombres remoto. Cada *Host* debe implementar un mecanismo utilizando el cliente DNS para convertir nombres de *Host* en direcciones IP.

Elementos de Datos de DNS

Un nodo DNS se representa por una etiqueta en el interior del nombre de dominio, y todos los nodos tienen unos archivos de recursos (*resource records (RRs)*) que contienen información que habilita el programa DNS para encontrar el nombre de dominio solicitado.

Formato de un RR. (Ver Tabla 2 y 3)

Nombre del propietario (*Owner Name*) o (SNAME) es el nombre del nodo al cual pertenece el Resource Record. Este nombre que será comparado con el nombre proporcionado por el programa de usuario El nombre está en formato DNS con unos octetos de longitud seguido por cadenas ASCII.

Tipo (*Type*) es un entero de 16 bits que describe el tipo de Resource Record. (Ver Tabla 1).

Clase (*Class*) es un entero de 16 bits que define la clase del Resource Record. Un RR de Internet tiene el campo igual a 1.

Tiempo de vida (*Time-to-live*) es un entero de 32 bits que especifica el intervalo de tiempo en el cual el RR debe ser almacenado en la memoria cache, antes de ser actualizado con la información del origen. El valor cero significa que el RR debe ser utilizado sólo en la transacción en progreso, y no tiene que ser almacenado. El valor cero también se utiliza para datos muy volátiles.

Longitud RD (*RDLength*) es un entero de 16 bits especifica la longitud en octetos del campo RDATA.

RData es una cadena de longitud variable de octetos que describen el recurso. El formato de esta información varía según el tipo y clase del RR. Para el tipo A RR (Internet) , el campo RData contiene una dirección IP de 32 bits.

Otro elemento de datos del DNS es el SLIST. El SLIST es una estructura que describe los servidores de nombres y la zona donde el cliente está intentando enviar una solicitud actualmente.

Tabla 2.
Tipos de *Resource Records*

Valor	Codigo	Significado
1	A	La direccion de un *Host*
2	NS	Un servidor de nombres autorizado
5	CNAME	El nombre canonico de un alias
6	SOA	Inicio de la zona de autoridad
11	WKS	Descripcion de un servicio conocido
12	PTR	Un puntero de nombre de dominio
13	HINFO	Información de un *Host*
14	MINFO	Información del Mailbox o de una lista de correo
15	MX	Intercambio de correo
16	TXT	Cadena de texto
22	NSAP	Cadena hacia un servicio de transporte OSI
23	NSAP-PTR	Puntero de nombre de dominio NSAP
252	AXFR	Solicitud de tranferencia de un a zona entera
253	MAILB	Solicitud de los archivos del Mailbox
255		Solicitud de todos los archivos

Tabla 3.
Formato de un *Resource Record*

msb	–						lsb
7	6	5	4	3	2	1	0
Owner name							
Type							
Class							
Time to live							
RDLength							
RData							
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

Funcionamiento del DNS

Un programa manda una solicitud a un cliente (*resolver*) que contiene un nombre de dominio para el cual se quiere la dirección IP asociada. La solicitud suele hacerse con una subrutina. o un puntero hacia el nombre de dominio en la pila del sistema. Los nombres de dominio en el cache del *Resolver* (cliente) están en un formato estándar contenido en RRs. Existen tres posibles respuestas de un *Resolver* al programa de usuario.

Uno o más RRs conteniendo la dirección IP solicitada. En el caso de que el nombre proporcionado fuera un alias, el *Resolver* simplemente devuelve el nombre de dominio al que hace referencia el alias.

Un mensaje de error en el nombre, que significa que el nombre proporcionado no existe.
Un error de datos no encontrado, que significa que el nombre proporcionado existe, pero no se refiere a ninguna dirección IP.

Formato de un mensaje DNS

El Protocolo DNS utiliza mensajes enviados por el UDP para trasladar solicitudes y respuestas entre servidores de nombres. La transferencia de zonas completas la hace el TCP.

El formato de un mensaje DNS tiene cinco partes.

- Cabecera define el formato de las otras partes
- Pregunta es el objetivo a resolver
- Respuesta es la resolución del objetivo
- Autoridad es la referencia a un servidor autorizado
- Adicional es información relacionada, pero no la respuesta.

Formato de la cabecera. (Ver Tabla 6)

La cabecera contiene los siguientes campos:
ID es un campo de 16 bits utilizado para relacionar solicitudes y respuestas.
QR es un campo de 1 bit que identifica el mensaje como una solicitud (0) o una respuesta (1).
OPcode es un campo de 4 bits que describe el tipo de mensaje. (Ver Tabla 4)

Tabla 4.
Codigo de operacion/Tipo de mensaje

Codigo	Descripcion
0	Solicitud normal (nombre a direccion)
1	Solicitud Inversa (direccion a nombre)
2	Solicitud del estado del servidor

A es un campo de 1 bit que cuando tiene valor 1 indica que la respuesta la ha hecho un servidor autorizado

T es un campo de 1 bit que cuando toma valor 1 indica que el mensaje ha sido truncado
RQ es un campo de 1 bit que cuando está puesto a 1, indica la solicitud de un servicio, recursivo por parte del servidor de nombres. Este servicio normalmente no esta disponible.

RA es un campo de 1 bit que indica la disponibilidad del servicio recursivo.

Z es un campo de 3 bits reservado para un uso futuro y su valor debe ser 0.

RCode es un campo de 4 bits que lo rellena el servidor de nombres, y sirve para indicar el estado de la búsqueda. (Ver Tabla 5)

Tabla 5.
Estado de la busqueda

Codigo	Descripcion
0	Sin errores
1	Error de Imposible interpretar el formato de la busqueda
2	Error de Imposible procesar el servidor
3	Error de nombre inexistente
4	Tipo de busqueda no soportado
5	Solicitud rechazada

QDCount es un campo de 16 bits que indica el número de entradas en la sección de Preguntas.

ANCount es un campo de 16 bits que indica el número de Resource Records en la sección de Respuesta.

NSCount es un campo de 16 bits que define el numero de Resource Records en la sección de Autoridad.

ARCount es un campo de 16 bits que define el número de Resource Records en la sección de Archivos Adicionales.

Tabla 6.
Formato de la cabecera DNS

	Octet +0								*Octet +1*								*Octet +2*								*Octet +3*							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
+0	ID																QR	Opcode			A	T	RQ		RA	Z			Rcode			
+4	QDCOUNT																ANCOUNT															
+8	NSCOUNT																ARCOUNT															

Formato de la sección Preguntas

Esta sección la construye el cliente, y siempre está presente. Contiene el nombre de dominio objetivo, seguido por los campos Qtype y Qclass. Esta sección es idéntica en longitud y formato que la definida para los campos CName, tipo y clase de un Resource Record.

Formato de la sección Respuesta

Esta sección contiene uno o más RRs.

Formato de la sección Autoridad

La sección autoridad contiene uno o más RRs que apuntan hacia los orígenes de la información autorizada.

Formato de la sección Adicional

Esta sección contiene uno o más RRs que proporcionan fuentes adicionales de información.

2.3. Echo Protocol

El servidor eco utiliza el puerto de UDP número 7 para escuchar las solicitudes de eco del cliente. El cliente utiliza un número de puerto UDP libre para el número de puerto de origen y manda un mensaje por medio del UDP al servidor eco. El servidor recibe la solicitud, intercambia las direcciones de origen y destino, intercambia las identificaciones de puertos y devuelve el mensaje al cliente.

2.4. NTP (Network Time Protocol)

El NTP se utiliza para sincronizar los servidores con una precisión de nanosegundos.

Formato del mensaje. (Ver Tabla 10)

El mensaje NTP está formado por los siguientes campos:

Indicador de Ajuste (*Leap Indicator*)(LI): Es un campo de 2 bits que indica el ajuste debido al periodo de rotación de la Tierra. (Ver Tabla 7)

Tabla 7.
Indicador de Ajuste

Valor	Significado
00	Sin advertencias
01	-1 segundo
10	+1 segundo
11	Condicion de alarma (Reloj no sincronizado)

Número de Versión (*Versión Number*) (VN): Es un campo de 3 bits que indica el número de versión.

Reservado (*Reserved*): Es un campo de 3 bits, que tiene valor cero.

Estrato (*Stratum*): Este campo tiene una longitud de 8 bits, y se utiliza para indicar el estrato local del reloj. (Ver Tabla 8)

Tabla 8.
Estrato del reloj local

Valor	Significado
0	Sin especificar
1	Referencia primaria
2..n	Referencia secundaria (via NTP)

Poll: Este campo tiene una longitud de 8 bits. Indica el intervalo máximo de tiempo entre mensajes.

Precisión: Este campo tiene una longitud de 8 bits e indica la precisión del reloj local.

Distancia de sincronía (*Sincronize distance*): Este es un campo de 32 bits, que indica el retraso aproximado de la primera ruta de sincronización.

Nivel de velocidad aproximado (*Estimated Drift Rate*): Es un campo de 32 bits que indica el nivel de velocidad del reloj local.

Identificador del reloj de referencia (*Reference Clock Identifier*): Campo de 32 bits que indica un reloj de referencia particular. (Ver Tabla 9)

Tabla 9.
Identificador de reloj de referencia

Valor	Codigo	Significado
0	DCN	Determinado por el algoritmo DCN
1	WWVB	Radio Reloj WWVB (60 KHz)
1	GOES	Reloj de satelite GOES (450 MHz)
1	Radio Reloj WWV	WWV (5/10/15 MHz)

Fecha y Hora (*Timestamps*) :Existen 3 *Timestamps* (Fecha y Hora) de 64 bits cada uno.

TBLA 10.
Formato del NTP

	Octet +0								*Octet +1*								*Octet +2*								*Octet +3*							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
+0	LI		VN		0	0	0		*Statum*								*Poll*								*Precision*							
+4	*Synchronizing Distance*																															
+8	*Estimated Drift rate*																															
+12	*Reference clock Identifier*																															
+16	*Reference clock Timestamp*																															
+24	*Originate Timestamp*																															
+32	*Receive Timestamp*																															
+40	*Transmit Timestamp*																															

2.5. SNMP (Simple Network Management Protocol)

El protocolo SNMP se utiliza para administrar múltiples redes físicas de diferentes fabricantes, es decir Internet, donde no existe un protocolo común en la capa de Enlace. La estructura de este protocolo se basa en utilizar la capa de aplicación para evitar el contacto con la capa de enlace.

Formato del mensaje
Existen tres partes en un mensaje SNMP:
Número de versión (*Version number*): Se utiliza para identificar el nivel de SNMP
Cadena de Comunidad (*Community string*): Se utiliza para la seguridad, restringiendo el acceso a los datos.

PDU: Esta sección contiene los comandos y respuestas, llamados PDU (Protocol Data Units).

2.6. ICMP

Internet es un sistema autónomo que no dispone de ningún control central. El protocolo ICMP (Internet Control Message Protocol), proporciona el medio para que el software de hosts y gateways intermedios se comuniquen. El protocolo ICMP tiene su propio número de protocolo (número 1), que lo habilita para utilizar el IP directamente. La implementación de ICMP es obligatoria como un subconjunto lógico del protocolo IP. Los mensajes de error de este protocolo los genera y procesa TCP/IP, y no el usuario.

Formato del mensaje ICMP

Cada Mensaje ICMP está compuesto por los siguientes campos:
Tipo (Ver Tabla 11)

Código

Checksum

Otras variables

Tabla 11.
Tipos de mensaje ICMP

Tipo	Tipo de Mensaje
0	Respuesta de Eco
3	Destino Inalcanzable
4	Origen saturado
5	Redireccion (cambiar ruta)

8	Solicitud de eco
11	Tiempo excedido para un datagrama
13	Problema de parametros en un datagrama
13	Solicitud de fecha y hora
14	Respuesta de fecha y hora
17	Solicitud de nascara de direccion
18	Respuesta de mascara de direccion

Solicitud de Eco. (Ver Tabla 12)

Un *Host* puede comprobar si otro *Host* es operativo mandando una solicitud de eco. El receptor de la solicitud la devuelve a su origen. Esta aplicación recibe el nombre de *Ping*. Esta utilidad encapsula la solicitud de eco del ICMP (tipo 8) en un datagrama IP y lo manda a la dirección IP.

El receptor de la solicitud de eco intercambia las direcciones del datagrama IP, cambia el código a uniformar y lo devuelve al origen.

Tabla 12.
Formato del mensaje de Eco ICMP

	Octet +0								*Octet +1*								*Octet +2*								*Octet +3*							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
+0	*Type*								*Code*								*Checksum*															
+4	*Identifier*																*Sequence number*															
	Optional Data																															

Informes de Destinos Inalcanzables. (Ver Tabla 13)

Si un *Gateways* no puede enviar un datagrama a la dirección de destino, éste manda un mensaje de error ICMP al origen. El valor del campo tipo es 3 y el tipo de error viene dado por el campo código. (Ver Tabla 14).

Tabla 13.
Codigos de Inalcanzable

Codigo	Descripcion
0	Red no alcanzable
1	*Host* no alcanzable
2	Protocolo no alcanzable
3	Puerto no alcanzable
4	Necesaria fragmentacion con la opcion DF
5	Fallo de la ruta de origen
6	Red de Destino desconocida
7	*Host* de Destino desconocido
8	Fallo del *Host* de Origen
9	Red prohibida administrativamente
10	*Host* prohibido administrativamente
11	Tipo de servicio de Red no alcanzable
12	Tipo de servicio de *Host* no alcanzable

Tabla 14
Formato del mensaje ICMP de destino inalcanzable

Octet +0								*Octet +1*								*Octet +2*								*Octet +3*							
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
Type								*Code*								*Checksum*															
Internal header plus 64 bits of datagram																															

Control de flujo

Para contener los datagramas IP, un *Gateways* dispone de un *buffer*. Si el número de datagramas es grande, el *buffer* se satura. En este momento el *Gateways* descarta todos los mensajes que recibe hasta que obtiene un nivel de *buffer* aceptable. Cada datagrama descartado hace que el *Gateways* mande un mensaje ICMP de control de flujo al origen. Esto informa, que un mensaje ha sido descartado.

Originalmente el mensaje ICMP de control de flujo se enviaba cuando el *buffer* estaba lleno, pero esto llegaba demasiado tarde y el sistema ya estaba saturado.

El algoritmo se cambió para que el mensaje ICMP de control de flujo se enviara cuando el *buffer* estuviera al 50%.

Formato del mensaje

El formato del mensaje de control de flujo es idéntico al mensaje de Inalcanzable, excepto que el tipo es 4 y el código es 0.

Cambio de ruta (redireccionamiento)

Los Gateways en cualquier Internet contienen las tablas de redireccionamiento más comunes. Cuando la ruta por defecto no es la mas adecuada, el *Gateways* puede enviar al *Host* un mensaje de redireccionamiento ICMP que contiene la ruta correcta.

Formato del mensaje

El formato del mensaje ICMP de control de flujo es igual al del mensaje de Inalcanzable, excepto que el tipo es 5 y el valor del código es variable entre 1 y 3. Los motivos para la redirección y sus códigos se pueden consultar en la Tabla 15.

Tabla 15.
Codigos de Redireccion

Codigo	Razon para la redireccion
1	Por el *Host*
2	Por el tipo de servicio y red
3	Por el tipo de servicio y *Host*

Tiempo de vida excedido

Para prevenir bucles en la redirección, el datagrama IP contiene un tiempo de vida definido por el origen. A medida que cada *Gateways* procesa el datagrama, el valor del campo disminuye en una unidad. Posteriormente el *Gateways* verifica si el valor del campo es 0. Cuando se detecta un 0, el *Gateways* manda un mensaje de error ICMP y descarta el datagrama.

Formato del mensaje

El formato del mensaje de error es igual al del mensaje de Inalcanzable, pero el tipo es 11, y el código es igual a 0 (contador sobrepasado), o 1 (tiempo de reensamblaje de fragmento excedido).

Errores de parámetros

Un error de parámetros se produce cuando el que origina el datagrama lo construye mal, o el datagrama está dañado Si un Gateways encuentra un error en el datagrama, manda un mensaje ICMP de error de parámetros al origen y descarta el datagrama.

Formato del mensaje

El formato del mensaje ICMP de error de parámetros es igual al de Inalcanzable, pero su tipo es 12, y el código es 0 si se utilizan punteros, o 1 si no se utilizan.

Mensaje Fecha y hora del ICMP

El Mensaje Fecha y hora del ICMP es una herramienta útil para diagnosticar problemas de Internet, y recoger información acerca del rendimiento.

El protocolo NTP (Network Time Protocol), puede utilizarse para marcar el tiempo inicial, y puede guardar la sincronización en milisegundos del reloj.

Formato del mensaje. (Ver Tabla 16)

El mensaje Fecha y secuencia los siguientes campos: Tipo, Código, Checksum, Identificador, Número de y hora receptor, Fecha y hora original, Fecha y hora receptor y Fecha y hora de transmisión. El tipo es igual a 13 para el origen y 14 para el *Host* remoto. El código es igual a 0. El identificador y el número de secuencia se usan para identificar la respuesta. El Fecha y hora original es el tiempo en el que el emisor inicia la transmisión, el Fecha hora tiene es el tiempo inicial en el que el receptor recibe el mensaje. El Fecha y hora de transmisión es el tiempo en que el receptor inicia el retorno del mensaje.

Tabla 16.
Formato ICMP de fecha y hora

Octet +0								*Octet +1*								*Octet +2*								*Octet +3*							
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
Type								*Code*								*Checksum*															
Identifier																Sequence number															
Originate Timestamp																															
Receive Timestamp																															
Transmit Timestamp																															

Máscara de subred

Cuando un *Host* quiere conocer la máscara de subred de una LAN física, puede mandar una solicitud ICMP de máscara de subred.

Formato del Mensaje

El formato es igual a los primeros ocho octetos del ICMP Fecha y hora. El valor del campo tipo es 17 para la solicitud de máscara de subred y 18 para la respuesta. El código es 0, el identificador y el número de secuencia se utilizan para identificar la respuesta.

2.7. IGMP

EL IGMP (Internet Group Management Protocol) es un protocolo que funciona como una extensión del protocolo IP.

Se utiliza exclusivamente por los miembros de una red multicast para mantener su status de miembros, o para propagar información de direccionamiento.

Un *Gateways* multicast manda mensajes una vez por minuto como máximo. Un *Host* receptor responde con un mensaje IGMP, que marca al *Host* como miembro activo. Un *Host* que no responde al mensaje se marca como inactivo en las tablas de direccionamiento de la red multicast.

2.8. Protocolos de actualización de la tabla de direccionamineto

Los protocolos que se describen a continuación se utilizan en el proceso automático de actualización de la tabla de direccionamiento.

EGP (Exterior *Gateways* Protocol)

Un dominio de direccionamiento es un grupo de redireccionadores que usan un IGP(Internal *Gateways* Protocol) común. Una forma de reducir el volumen de información intercambiado se basa en que un dominio de redireccionamiento utilice un *Gateways* seleccionado para comunicar información de direccionamiento con los Gateways seleccionados de otros dominios. El *Gateways* seleccionado se considera como un *Gateways* exterior, y el protocolo usado entre Gateways exteriores es el EGP.

El protocolo EGP se compone de tres partes:

- Neighbor Adquisition Protocol
- Neighbor Reachability Protocol (NR)
- Network Reachability Determination

El *Neighbor Adquisition Protocol* se utiliza simplemente para establecer comunicación. Consta de una Solicitud y una Respuesta.

El *Neighbor Reachability Protocol* se basa en un mensaje "Hello" (comando), y una respuesta "I heard you". Se utiliza para saber si la comunicación continúa.

El mensaje *Network Reachability* se usa para comprobar si el siguiente "vecino" es un camino válido para llegar a un destino particular.

EL principal inconveniente del protocolo EGP es que crea una estructura en forma de árbol, es decir que si hay problemas en Internet, los Gateways sólo saben que hay problemas en el *Gateways* exterior.

BGP-3 (Border *Gateways* Protocol)

El problema del protocolo EGP, fue el que impulsó a diseñar e implementar el protocolo BGP.

El protocolo BGP es un protocolo interno de sistema autónomo. Un sistema autónomo puede contener múltiples dominios de direccionamiento, cada uno con su propio protocolo interno de sistema autónomo, o IGP. Dentro de cada sistema autónomo puede haber varios Gateways que se pueden comunicar con los Gateways de otros sistemas. También se puede elegir un *Gateways* para lograr un informe de la información de direccionamiento para el sistema autónomo. En cualquier caso, un sistema autónomo aparece ante otro sistema autónomo como un direccionador consistente. Esto elimina la estructura de árbol del protocolo EGP.

GGP (*Gateways*-to-*Gateways* Protocol)

Los primeros Gateways de Internet utilizaban un IGP llamado *Gateways*-to-*Gateways* Protocol , que fue el primer IGP utilizado. Usando GGP cada *Gateways* manda un mensaje a todos los otros Gateways de su grupo autónomo que contiene una tabla con las direcciones que el *Gateways* ha direccionado, con su vector de distancia asociado.

RIP (Routing Information Protocol)

El RIP es un IGP desarrollado bastante después del GGP, y está basado en el vector / distancia. Si un *Gateways* conoce varias rutas para llegar a un destino, asigna un coste a la ruta en función de los saltos de Gateways que deba realizar. (Cuantos más Gateways tenga que cruzar, más saltos deberá realizar).

Cada 30 segundos envía un mensaje con su tabla de direccionamiento a los demás que actualizan sus tablas con los datos recibidos. (Esto produce un incremento del tráfico de red).

Este algoritmo tiene algún fallo, como por ejemplo no detecta bucles en la transmisión de la ruta. Esto daría un problema: que dos rutas que se llamen entre indefinidamente, ellas estarían emitiendo tablas de direccionamiento

Otro error es que no obliga a la autentificación de los intercambios, por lo que cualquier persona podría recibir información de las rutas enviadas por los Gateways.

Existen dos versiones RIP I y RIP II (Soporta máscaras de subred).

Hello Protocol

Un IGP similar al RIP es el Hello Protocol. La diferencia básica es que el RIP cuenta los saltos de Gateways, y el Hello mide la distancia por el tiempo transcurrido. Este protocolo tiene un problema asociado al vector de distancia. El problema tiene dos etapas. La primera etapa es cuando los Gateways descubren una ruta más corta para llegar a un determinado destino. Esta ruta es más corta y más rápida, lo que provoca que el tráfico de red pase a utilizar esta nueva ruta.

La segunda etapa empieza cuando los Gateways descubren que la nueva ruta es más lenta que la ruta vieja, debido a que al desviar el trafico de red a la nueva ruta, ésta se satura, y todos los usuarios vuelven a la ruta vieja.

OSPF (Open Shortest Path First)

Uno de los protocolos IGP más nuevos es el OSPF. Este protocolo ofrece un mayor grado de sofisticación con caracteristicas como: Rutas basadas en el tipo de servicio, la distancia, nivel de carga, etc.

El formato del mensaje OSPF es más complejo que el RIP. Tiene una cabecera fija de 24 octetos, y una parte variable para especificar el tipo del mensaje. Existen cinco tipos de mensaje, como se puede ver en la Tabla 17.

Tabla 17.
Tipos de mensaje OSPF

Tipo	Significado
1	Hola (Utilizado para comprobar la accesibilidad)
2	Descripción de la Base de Datos
3	Solicitud del estado del enlace
4	Actualización del estado del enlace
5	Reconocimiento del estado del enlace

3. CAPA DE TRANSPORTE

Provee comunicación extremo a extremo desde un programa de aplicación a otro. Puede proveer un transporte confiable asegurándose de que los datos lleguen sin errores y en la secuencia correcta. Coordina a múltiples aplicaciones que se encuentren interactuando con la red simultáneamente de tal manera que los datos que envíe una aplicación sean recibidos correctamente por la aplicación remota.

En esta capa se encuentran los protocolos UDP y TCP.

3.1. UDP (User Datagram Protocol)

El protocolo UDP (User Datagram Protocol) proporciona aplicaciones con un tipo de servicio de datagramas orientado a transacciones. El servicio es muy parecido al protocolo IP en el sentido de que no es fiable y no está orientado a la conexión. El UDP es simple, eficiente e ideal para aplicaciones como el TFTP y el DNS.. Una dirección IP sirve para dirigir el datagrama hacia una máquina en particular, y el número de puerto de destino en la cabecera UDP se utiliza para dirigir el datagrama UDP a un proceso específico localizado en la cabecera IP. La cabecera UDP, también contiene un número de puerto origen que permite al proceso recibido conocer cómo responder al datagrama.

Formato del mensaje. (Ver Tabla 18)

El datagrama UDP contiene cuatro campos, que son Número del Puerto de Origen, Número del Puerto de Destino, Longitud del mensaje y Checksum.

Tabla 18.
Formato del UDP

	Octet +0								*Octet +1*								*Octet +2*								*Octet +3*							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
+0	*Source Port*																*Destination Port*															
+4	*Message Length*																*Checksum*															
	UDP Data																															

Números de Puerto de Origen y Destino

Estos números, junto con las direcciones IP definen el punto final de la comunicación. El número del puerto de origen, puede tener valor si no se usa. El número del puerto de destino sólo tiene sentido en el contexto de un datagrama UDP y una dirección IP en particular.

El número de puerto de origen es un campo de 16 bits. El puerto de destino tiene la misma longitud.

Longitud del Mensaje

Este campo tiene una longitud de 16 bits y contiene el número total de octetos que forman el datagrama, incluida la cabecera.

Checksum

El uso del *checksum* es opcional, y este campo debe ponerse a cero si no es utilizado. Mientras que el *checksum* del datagrama IP sólo tiene en cuenta la cabecera del mensaje, el UDP tiene su propio *checksum* para garantizar la integridad de los datos. La longitud de este campo es de 16 bits, y está formado por la suma de los campos del UDP, y algunos campos del IP.

Para incluir los campos del IP, se construye una pseudo cabecera UDP. Esta pseudo cabecera de 12 octetos se utiliza únicamente para efectos de calcular la suma. (Ver Tabla 19)

Tabla 19.
Pseudo-Cabecera UDP

	Octet +0								Octet +1								Octet +2								Octet +3							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
Pseudo Header	Source IP Adress																															
	Destination IP Address																															
	Zero								Protocol ID								Length															
	Source Port																Destination Port															
	Message Length																Checksum															
	UDP Data																															
	UDP Data								Zero																							

3.2 CP (Transmission Control Protocol)

El protocolo TCP proporciona un servicio de comunicación que forma un circuito, es decir, que el flujo de datos entre el origen y el destino parece ser continuo TCP proporciona un circuito virtual el cual es llamado conexión.

Al contrario de los programas que utilizan UDP, los que utilizan el TCP tienen un servicio de conexión entre los programas llamados y los que llaman, chequeo de errores, control de flujo y capacidad de interrupción.

Interfaces TCP

Existen dos tipos de interfase entre la conexión TCP y los otros programas.

El primero es utilizar la pila de los programas de la capa de red. Como en esta capa sólo esta el IP protocolo, el interfase lo determina este protocolo. El segundo tipo es el interfaz del programa de usuario. Este interfase puede variar según el sistema operativo, pero en general tiene las siguientes caracteristicas.

El interface envuelve el programa de usuario llamando a una rutina que introduce entradas en una estructura de datos llamada el bloque de control de transmisión (TCB). Las entradas se realizan inicialmente en la pila de *hardware* y transferidas al TCB por medio de una rutina de sistema. Estas entradas permiten al TCP asociar un usuario con una conexión particular, de modo que pueda aceptar comandos de un usuario y mandarlos a otro usuario en la otra parte de la conexión. TCP utiliza unos identificadores únicos para cada parte de la conexión. Esto se utiliza para recordar la asociación entre dos usuarios. Al usuario se le asigna un nombre de conexión para utilizarlo en futuras entradas del TCB. Los identificadores para cada extremo de la conexión se llaman sockets. El socket local se construye concatenando la dirección IP de origen y el número de puerto de origen. El socket remoto se obtiene concatenando la dirección IP de destino y el número de puerto de destino.

El par de sockets de una conexión forman un único número en Internet. El UDP tiene los mismos sockets, pero no los recuerda. Esta es las diferencia entre un protocolo orientado a conexión y otro a no conexión. A continuación se explican los comandos más usuales:

Open: Inicia una conexión o comienza a escuchar un socket. El usuario tiene un nombre de conexión local que actúa como un puntero dentro del TCB.

Send: El comando *Send* manda datos del *buffer* especificado.

Receive: El comando *Receive* es un mensaje de error si el nombre local proporcionado no es utilizado antes con el comando *Open*.

Close: El comando *Close* hace que se cierre una conexión. Se produce un error si la conexión especificada no ha sido abierta, o si no se tiene autorización para cerrar la conexión.

Status: El comando *Status* sólo tiene una variable asociada, que es el nombre de la conexión.

Abort: El comando *Abort* hace que todos los comandos Send y Receive asociados al nombre de la conexión local se interrumpan. La entrada del usuario del TCB se elimina y se envía un mensaje especial de reinicio a la entidad del otro lado de la conexión.

El TCP recuerda el estado de cada conexión por medio del TCB. Cuando se abre una conexión, se efectúa una entrada única en el TCB. Un nombre de conexión se le asigna al usuario para activar los comandos de la conexión. Cuando se cierra una conexión se elimina su entrada del TCB.

Control de Flujo

El protocolo TCP puede controlar la cantidad de datos que debe enviar mediante el campo *Window*. Este campo indica el número máximo de octetos que pueden ser recibidos. El receptor de un segmento con el campo *window* a cero, no puede enviar mensajes al emisor, excepto mensajes de prueba. Un mensaje de prueba es un mensaje de un solo octeto que se utiliza para detectar redes u *hosts* inalcanzables.

Formato del segmento TCP

El segmento TCP consiste en una cabecera y datos. A continuación se describen los campos del segmento TCP.

Numero de puerto del Origen/destino (*Source/Destination Port Numbers*):Este campo tiene una longitud de 16 bits.

Números de Secuencia (*Secuence Numbers*): Existen dos números de secuencia en la cabecera TCP. El primer número de secuencia es el numero de secuencia final (*SSN*). El SSN es un número de 32 bits.El otro numero de secuencia es el Numero de secuencia esperado de recepción. también llamado Número de Reconocimiento (*acknowledgement number*).

Longitud de la cabecera (*Header Length*):Este campo tiene una longitud de 4 bits y contiene un entero igual al número de octetos que forman la cabecera TCP dividido por cuatro.

Código de Bits (*Code bits*):El motivo y contenido del segmento TCP lo indica este campo.

Este campo tiene una longitud de seis bits.

Bit URG (bit +5):Este bit identifica datos urgentes.

Bit ACK (bit +4):Cuando este bit se pone a 1, el campo reconocimiento es válido.

Bit PSH (Bit +3):Aunque el *buffer* no esté lleno, el emisor puede forzar a enviarlo.

Bit RST (Bit +2):Poniendo este bit, se aborta la conexión. Todos los buffers asociados se vacían.

Bit SYN (Bit +1):Este bit sirve para sincronizar los números de secuencia.

Bit FIN (Bit +0):Este bit se utiliza sólo cuando se está cerrando la conexión.

Ventana (*Window*): Este campo contiene un entero de 32 bits. Se utiliza para indicar el tamaño de *buffer* disponible que tiene el emisor para recibir datos.

Opciones (*Options*): Este campo permite que una aplicación negocie durante la configuración de la conexión características como el tamaño máximo del segmento TCP. Si este campo tiene el primer octeto a cero, esto indica que no hay opciones.

Relleno (*Padding*):Este campo consiste en un número de octetos (De uno a tres), que tienen valor cero y sirven para que la longitud de la cabecera sea divisible por cuatro.

Checksum: Mientras que el protocolo IP no tiene ningún mecanismo para garantizar la integridad de los datos, ya que sólo comprueba la cabecera del mensaje, el TCP dispone de su propio método para garantizar dicha integridad.

Como en el *Checksum* del protocolo TCP también se incluyen campos del protocolo IP, es necesario construir una pseudo-cabecera TCP que se considera únicamente a efectos de cálculo.(Ver Tabla 20 y 21)

Tabla 20.
Formato del *Checksum* TCP

	Octet +0								*Octet +1*								*Octet +2*								*Octet +3*							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
Data in Checksum	*Source IP Adress*																															
	Destination IP Address																															
	Zero								*Protocol Number*								*Number of octets in header and data*															
	TCP Header																															
	TCP Data																															
	TCP Data								*Zero*																							

Tabla 21.
Formato del mensaje TCP

	msb							lsb
	7	6	5	4	3	2	1	0
TCP Header	*Source Port*							
	Destination Port							
	Sequence Number							
	Acknowledgement Number							
	Header Length				*Reserved*			
	RSV		*Code Bits*					
	Window							
	Checksum							
	Urgent Pointer							
	Options							
	Padding							
	TCP Data							
	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

Estados del TCP

El inicio, mantenimiento y cierre de una conexión requiere que el TCP recuerde toda la información relativa a cada conexión. Esta información se almacena en una entrada para cada conexión dentro del TCB. Cuando se abre una conexión, la entrada en el TCB se realiza con todas las variables inicializadas con sus respectivos valores. Durante la conexión, la entrada del TCB es actualizada a medida que cambia la información. A continuación se describen algunos de los estados del TCP:

0. CLOSED: No existe, sólo para referencia.

1. LISTEN: Se espera solicitud de conexión de un TCP remoto.

2. SYN-SEN: Se espera un mensaje de solicitud de conexión después de haber enviado una solicitud de conexión.

3. SYN-RECEIVED: Se espera confirmación de un reconocimiento de solicitud de conexión, después de haber enviado y recibido una solicitud de conexión.

4. ESTABLISHED: Representa una conexión abierta. Los datos recibidos pueden ser enviados a un protocolo de una capa superior. Este es el estado normal de la fase de transferencia de la conexión.

5. FIN-WAIT-1: Se espera la solicitud de fin de conexión de un TCP remoto, o un reconocimiento de una solicitud de fin de transmisión enviada anteriormente.

6. FIN-WAIT-2: Se espera una solicitud de fin de conexión de un TCP remoto.

7. CLOSE-WAIT: Se espera una solicitud de fin de conexión de un protocolo de una capa superior.

8. CLOSING: Se espera el conocimiento de una solicitud de final de conexión de un TCP remoto.

9. LAST-ACK: Se espera el conocimiento de una solicitud de final de conexión enviada anteriormente al TCP remoto.

10. TIME-WAIT: Se espera el tiempo necesario para que el TCP remoto haya recibido el conocimiento de la solicitud del fin de conexión.

4. CAPA DE RED

Controla la comunicación entre un equipo y otro. Conforma los paquetes IP que serán enviados por la capa inferior. Desencapsula los paquetes recibidos pasan a la capa superior la información dirigida a una aplicación.

4.1 IP (Internet Protocol) Versión 4

El Protocolo IP proporciona un sistema de distribución que es poco fiable incluso en una base sólida. El protocolo IP especifica que la unidad básica de transferencia de datos en el TCP/IP es el datagrama.

Los datagramas pueden ser retrasados, perdidos, duplicados, enviados en una secuencia incorrecta o fragmentados intencionalmente para permitir que un nodo con un *buffer* limitado pueda coger todo el datagrama. Es la responsabilidad del protocolo IP reensamblar los fragmentos del datagrama en el orden correcto. En algunas situaciones de error los datagramas son descartados sin mostrar ningún mensaje, mientras que en otras situaciones los mensajes de error son recibidos por la máquina origen (esto lo hace el protocolo **ICMP**).

El protocolo IP también define cuál será la ruta inicial por la que serán mandados los datos.

Cuando los datagramas viajan de unos equipos a otros, es posible que atraviesen diferentes tipos de redes. El tamaño máximo de estos paquetes de datos puede variar de una red a otra, dependiendo del medio físico que se emplee para su transmisión. A este tamaño máximo se le denomina MTU (*Maximum Transmission Unit*), y ninguna red puede transmitir un paquete de tamaño mayor a esta MTU. El datagrama consiste en una cabecera y datos. (Ver Tabla 22)

Longitud de la Cabecera

Este campo ocupa 4 bits, y representa el número de octetos de la cabecera dividido por cuatro, lo que hace que éste sea el número de grupos de 4 octetos en la cabecera.

Version

El campo versión ocupa 4 bits. Este campo hace que diferentes versiones del protocolo IP puedan operar en la Internet. En este caso se trata de la versión 4.

Tipo de servicio

Este campo ocupa un octeto de la cabecera IP, y especifica la precedencia y la prioridad del datagrama IP. Los tres primeros bits del octeto indican la precedencia. Los valores de la precedencia pueden ser de 0 a 7. Cero es la precedencia normal, y 7 está reservado para control de red. Muchos Gateways ignoran este campo.

Los otros 4 bits definen el campo prioridad que tiene un rango de 0 a 15. Las cuatro prioridades que están asignadas son: 0, (por defecto, servicio normal), 1 (minimizar el coste monetario), 2 (máxima fiabilidad), 4 (Maximizar la transferencia), 8 (El bit +4 igual a 1, define minimizar el retraso). Estos valores son utilizados por los routers para direccionar las solicitudes de los usuarios.

Longitud Total

Este campo se utiliza para identificar el número de octetos en el datagrama total.
Identificación

El valor del campo identificación es un número secuencial asignado por el *Host* origen. El campo ocupa dos octetos. Los números oscilan entre 0 y 65.535, que cuando se combinan con la dirección del *Host* forman un número único en la Internet. El numero se usa para ayudar en el reensamblaje de los fragmentos de datagramas.

Fragmentos Offset

Cuando el tamaño de un datagrama excede el MTU, éste se segmenta.
El fragmento Offset representa el desplazamiento de este segmento desde el inicio del datagrama entero.

Flags

El campo flag ocupa 3 bits y contiene dos flags. El bit +5 del campo flags se utiliza para indicar el último datagrama fragmentado cuando toma valor cero. El bit +7 lo utiliza el servidor origen para evitar la fragmentación. Cuando este bit toma valor diferente de cero y la longitud de un datagrama excede el MTU, el datagrama es descartado y un mensaje de error es enviado al *Host* de origen por medio del protocolo ICMP.

Tiempo de Vida

El campo "Tiempo de Vida " ocupa un octeto. Representa el número máximo de segundos que un datagrama puede existir en Internet, antes de ser descartado. Un Datagrama puede existir como máximo 255 segundos. El número recomendado para IP es 64.

El originador del datagrama manda un mensaje **ICMP** cuando el datagrama es descartado.

Protocolo

El campo protocolo se utiliza para identificar la capa de mayor nivel más cercana usando el IP. Este es un campo de 0 bits, que normalmente identifica tanto la capa TCP (valor 6), como la capa UDP (valor 17) en el nivel de transporte, pero puede identificar hasta 255 protocolos de la capa de transporte.

Checksum

El checksum proporciona la seguridad de que el datagrama no ha sido dañado ni modificado. Este campo tiene una longitud de 16 bits.

El checksum incluye todos los campos de todos los campos de la cabecera IP, incluido el mismo, cuyo valor es cero a efectos de cálculo.

Un *Gateways* o nodo que efectúe alguna modificación en los campos de la cabecera (por ejemplo en el tiempo de vida), debe recalcular el valor del checksum antes de enviar el datagrama.

Los usuarios del IP deben proporcionar su propia integridad en los datos, ya que el checksum es solo para la cabecera.

Dirección de Origen

Este campo contiene un identificador de red (Netid) y un identificador de *Host* (Hostid). El campo tiene una longitud de 32 bits. La dirección puede ser de clase A, B, C.

Dirección de Destino

Este campo contiene el Netid y el Hostid del destino. El campo tiene una longitud de 32 bits. La dirección puede ser de clase A, B, C o D (ver **Direcciones IP**).

Opciones

La existencia de este campo viene determinada por la longitud de la cabecera. Si está es mayor de cinco, por lo menos existe una opción.

Aunque un *Host* no está obligado a poner opciones, puede aceptar y procesar opciones recibidas en un datagrama. El campo Opciones es de longitud variable. Cada octeto está formado por los campos Copia, Clase de opción y Número de opción.

El campo Copia sirve para que cuando un datagrama va a ser fragmentado y viaja a través de nodos o Gateways. Cuando tiene valor 1, las opciones son las mismas para todos los fragmentos, pero si toma valor 0, las opciones son eliminadas.

Clase de opción es un campo que cuando tiene valor 0, indica datagrama o control de red; Cuando tiene valor 2, indica depuración o medida. Los valores 1 y 3 están reservados para un uso futuro.

El Número de opción indica una acción especifica.

Tabla 22.
Características de la Opción IP

Clase de Opción	Numero de Opcion	Octetos	Descripción
0	0	1	Fin de alineamiento
0	1	1	Para alinear dentro de una lista de opciones
0	2	11	Seguridad (aplicaciones militares)
0	3	var	Ruteo del Origen
0	7	var	Grabar/trazar ruta
0	9	var	Ruteo estricto del Origen
2	4	var	Fecha y hora de Internet

Padding

Cuando está presente el campo Pad, consiste en 1 a 3 octetos puestos a cero, si es necesario, para hacer que el número total de octetos en la cabecera sea divisible por cuatro.

Datos

El campo datos consiste en una cadena de octetos. Cada octeto tiene un valor entre 0 y 255. El tamaño de la cadena puede tener un mínimo y un máximo, dependiendo del medio físico. El tamaño máximo está definido por la longitud total del datagrama. El tamaño del campo Datos en octetos es igual a:

(Longitud Total del Datagrama) - (Longitud de la cabecera)

Tabla 23.
Formato del Datagrama IP

	msb						lsb	
	7	6	5	4	3	2	1	0	
IP Header	*Version*				*Header Length*				+0
	Type of Service								+1
	Total Length								+2
									+3
	Identification								+4
									+5
	Flags				*Fragment Offset*				+6
									+7
	Time to Live								+8
	Protocol								+9
	Header Checksum								+10
									+11
	Source Address of Originating Host								+12
									+13
									+14
									+15
	Destination Address of Target Host								+16
									+17
									+18
									+19
	Options								+20
									+21
									+22
	Padding								+23
MSB	*IP Data*								+0
									+1
									+n

4.2 Direcciones IP

Las direcciones IP hacen que el envío de datos entre ordenadores se haga de forma eficaz, de un modo similar al que se utilizan en los números de teléfono.

Las direcciones IP tienen 32 bits, formados por cuatro campos de 8 bits, separados por puntos. Cada campo puede tener un valor comprendido entre 0 y 255. Esta compuesta por una dirección de red, seguida de una dirección de subred y de una dirección de host.

Clases de Direcciones IP

La clase A contiene 7 bits para direcciones de red, con lo que permite tener hasta 128 redes, con 16.777.216 ordenadores cada una. Las direcciones estarán comprendidas entre 0.0.0.0. y 127.255.255.255., y la mascara de subred será 255.0.0.0.

La clase B contiene 14 bits para direcciones de red y 16 bits para direcciones de hosts. El número máximo de redes es 16.536, con 65.536 ordenadores por red. Las direcciones estarán comprendidas entre 128.0.0.0. y 191.255.255.255.. y la mascara de subred será 255.255.0.0.

La clase C contiene 21 bits para direcciones de red y 8 para hosts, lo que permite tener un total de 2.097.142 redes. cada una de ellas con 256 ordenadores. Las direcciones estarán comprendidas entre 192.0.0.0. y 223.255.255.255., y la máscara de subred será 255.255.255.0.

La clase D se reserva todas las direcciones para multidestino (multicast), es decir, un ordenador transmite un mensaje a un grupo específico de ordenadores de esta clase. Las direcciones estarán comprendidas entre 224.0.0.0. y 239.255.255.255.

La clase E se utiliza exclusivamente para fines experimentales. Las direcciones están comprendidas entre 240.0.0.0. y 247.255.255.255.

4.3. IP (Internet Protocol) Versión 6

Esta es una nueva versión del protocolo IP, llamada IPv6, aunque también es conocida como IPng *(Internet Protocol Next Generation)*. Es la versión 6, debido a que la número 5 no pasó de la fase experimental. La compatibilidad con la versión 4 es prácticamente total, ya que se han incluido características de compatibilidad. Algunas de las modificaciones, están encaminadas a mejorar la seguridad en la red, que apenas existía en la versión 4.

Formato de la cabecera. (Ver Tabla 24)

Esta cabecera ocupa el doble que la anterior, pero se ha simplificado omitiendo algunos campos y haciendo que otros sean opcionales. De esta manera, los *routers* no tienen que procesar tanta información. Los campos son los siguientes:

Versión: Este campo ocupa 4 bits y contiene el número de versión del IP, en este caso 6.
Prioridad: Ocupa 4 bits, e indica la importancia del paquete que se esta enviando.

Etiqueta de Flujo: Ocupa 24 bits. Indica que el paquete requiere un tratamiento especial por parte de los *routers* que lo soporten.

Longitud: Ocupa 16 bits. Indica la longitud en bytes de los datos del mensaje siguiente Cabecera: Ocupa 8 bits e indica a qué protocolo corresponde la cabecera que esta a continuación de la actual.

- Tiempo de vida: Ocupa 8 bits y tiene la misma función que en la versión 4.
- Dirección de origen: Ocupa 128 bits (16 octetos), y es el número de dirección del origen.
- Dirección de Destino: Ocupa 128 bits (16 octetos). Es el número de dirección del destino.

Tabla 24.
Formato de la Cabecera del IPv6

Octet +0								*Octet +1*								*Octet +2*								*Octet +3*							
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
Versión								Prioridad								Etiqueta de flujo															
Longitud																Siguiente cabecera								Tiempo de vida							
Dirección de Origen (128 bits)																															
Dirección de Destino (128 bits)																															

4.4. Direcciones IP Versión 6

El cambio más significativo en las direcciones, ha sido que ahora, se refieren a un interfaz y no a un nodo, aunque como cada interfaz pertenece a un nodo, es posible referirse a éstos mediante su interfaz.

El número de direcciones diferentes se ha multiplicado de una manera exagerada. Teóricamente es posible tener 2^{128} direcciones diferentes. Este numero quiere decir que se podrían llegar a tener más de 665.000 trillones de direcciones por metro cuadrado, aunque si siguieran una jerarquía, este número decrece hasta 1564 direcciones por metro cuadrado, en el peor caso, o tres trillones siendo optimistas.

En el IPv6 existen tres tipos básicos de direcciones:

Direcciones *unicast*: están dirigidas a un único interfaz en la red. Actualmente se dividen en varios grupos, y existe un grupo especial que facilita la compatibilidad con las direcciones de la versión 4.

Direcciones *anycast*: Identifican a un conjunto de interfaces de red. El paquete se enviará a cualquier interfaz que forme parte del conjunto. En realidad son direcciones *unicast* que se encuentran asignadas a varios interfaces.

Direcciones *multicast*: Identifican a un conjunto de interfaces de la red, de manera que cada paquete es enviado a cada uno de ellos individualmente.

5. CAPA FÍSICA

Este nivel corresponde al *hardware*. En este nivel están los protocolos ARP y RARP.

5.1. ARP

El protocolo ARP (Address Resolution Protocol), es el encargado de convertir las direcciones IP en direcciones de la red física.

El funcionamiento del protocolo ARP es bastante simple. Cuando una máquina desea enviar un mensaje a otra máquina que está conectada a través de una red ethernet se encuentra con un problema: la dirección IP de la máquina en cuestión es diferente a la dirección física de la misma. La máquina que quiere enviar el mensaje sólo conoce la dirección IP del destino, por lo que tendrá que encontrar un modo de traducir la dirección IP a la dirección física. Esto se hace con el protocolo ARP.

Este protocolo utiliza una tabla denominada Tabla de Direcciones ARP, que contiene la correspondencia entre direcciones IP y direcciones físicas utilizadas recientemente. Si la dirección solicitada se encuentra en esta tabla el proceso se termina en este punto, puesto que la máquina que origina el mensaje ya dispone de la dirección física de la máquina destino.

Si la dirección buscada no está en la tabla, el protocolo ARP envía un mensaje a toda la red. Cuando un ordenador reconoce su dirección IP envía un mensaje de respuesta que contiene la dirección física. Cuando la máquina origen recibe este mensaje ya puede establecer la comunicación con la máquina destino y esta dirección física se guarda en la tabla de direcciones ARP.

Formato del mensaje ARP. (Ver Tabla 26)

El mensaje ARP está formado por 28 octetos. En los campos que se describen a continuación, se supone un Interfaz Ethernet.

Tipo de *Hardware*

El campo *Hardware* indica el tipo de interfaz de *Hardware*. Por Ejemplo, el valor de una red Ethernet es 1.

Tabla 25.
Tipo de Interfaz de *Hardware*

Tipo	Descripcion
1	Ethernet (10mb)
2	Experimental Ethernet (3 mb)
3	Amateur Radio X.25
4	Proteon ProNET Token Ring
5	Chaos
6	IEEE 802 Network
7	ARCNET
8	Hyperchannel
9	Lanstar
10	Autonet Short Address
11	LocalTalk
12	LocalNet

Números de Protocolo

El campo protocolo identifica el protocolo Ether usado. Por ejemplo el valor del interfaz Ethernet es 0800 hex.

Longitud de la dirección *Hardware*

El valor para Ethernet es 6. lo que proporciona 48 bits para una dirección Ethernet (12 semi-octetos)

Longitud del Protocolo

Este campo se usa para definir la longitud de la dirección de red. Para una red IP es 4.

Operación

Especifica el código de la operación. La solicitud ARP tiene valor 1 y la respuesta ARP tiene valor 2.

Dirección *Hardware* del Origen

Los campos dirección *Hardware* del Origen dirección IP del Origen, y dirección IP del Destino, los completa el emisor (si los conoce). El receptor añade la dirección *Hardware* del Destino y devuelve el mensaje al emisor con el código de operación 2. (El código de la Respuesta ARP).

La dirección *Hardware* de Origen (para Ethernet) esta formada por octetos que representan una dirección Ethernet de 48 bits, o un numero.

Dirección IP de Origen

La dirección IP de Origen puede ser una dirección de clase A, B o C. (Ver Direcciones IP para obtener una definición de estas clases).

Dirección *Hardware* de Destino
Este campo esta formado igual que el campo dirección *Hardware* de Origen.

Dirección IP de Destino
Este campo es igual al campo dirección IP de Origen

Tabla 26.
Formato del ARP

	Octet +0	*Octet +1*	*Octet +2*	*Octet +3*
	7 6 5 4 3 2 1 0	7 6 5 4 3 2 1 0	7 6 5 4 3 2 1 0	7 6 5 4 3 2 1 0
+0	*Hardware*		*Protocol*	
+4	*Length HW Addr.*	*Protocol Length*	*Operation*	
+8	*Source Hardware Address*			
+12	*Source Hardware Address*		*Source IP Address*	
+16	*Source IP Address*		*Destination Hardware Address*	
+20	*Destination Hardware Address*			
+24	*Destination IP Address*			

5.2. RARP

El protocolo RARP (Reverse Address Resolution Protocol) es el encargado de asignar una dirección IP a una dirección física.
Formato del Mensaje RARP

El formato del RARP es similar al del ARP. El valor del código de operación para una solicitud es 3 y el valor para una respuesta es 4.

Anexo 5

Ruteo

Componentes de Ruteo

El ruteo envuelve dos actividades básicas: Determinar el camino de ruteo óptimo y transportar grupos de información a través de las redes (comúnmente llamados paquetes). En el contexto del proceso de ruteo este último proceso se conoce como switching(conmutación). Aún que el switcheo es directo, la determinación de la ruta a tomar puede ser muy compleja.

Determinación de la Ruta

La métrica es una medida estándar, la cual se utiliza para medir el largo de la ruta a tomar, y es usado por los algoritmos de ruteo para determinar la ruta óptimo hacia el destino. Para ayudar al proceso de determinación de la ruta, los algoritmos de ruteo inicializan y mantienen las tablas de ruteo, las cuales contienen información de las rutas. La información de las rutas varía dependiendo de los algoritmos de ruteos utilizados.

Los algoritmos de Ruteo llenan las tablas con una variedad de información. La asociación de " brincos destino " le dicen al ruteador qué destino en particular puede ser el óptimo para enviar los paquetes a un ruteador en particular representando el "next hop" (el siguiente brinco) en el camino hacia el destino final. Cuando un ruteador recibe un paquete, éste checa la dirección de destino e intenta asociar la dirección con el siguiente brinco.

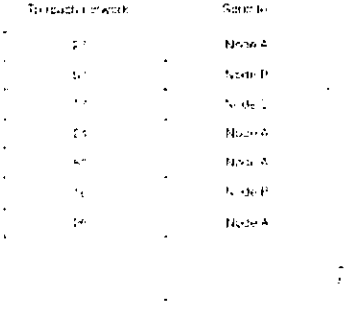


Figura 1 Tablas de Ruteo

Las tablas de ruteo también pueden contener otro tipo de información, como datos acerca de la ruta más confiable. Los ruteadores comparan las métricas para determinar las rutas óptimas, y esas métricas difieren dependiendo del diseño que usan los algoritmos de ruteo.

Los ruteadores se comunican entre sí y mantienen sus tablas de ruteo a través de la transmisión de una variedad de mensajes. Analizando la actualización de todos los ruteadores, un ruteador puede construir una imagen detallada de la topología de la red. Un anuncio de liga estática, un ejemplo de mensaje enviado entre ruteadores, informa a otros ruteadores del estado de los enlaces de envío. La información de enlace también puede ser usada para construir una imagen completa de la topología para permitir que los ruteadores determinen la ruta óptima hacia la red destino.

Switching

Los algoritmos de switcheo son relativamente simples y son básicamente los mismos para la mayoría de los protocolos de ruteo. En la mayoría de los casos, El host origen determina que debe enviar un paquete a otro host. Y adquiere la dirección física del ruteador de alguna manera, el host origen envía ahora un paquete con la dirección física del host destino.

De esta forma el ruteador examina la dirección del paquete destino y determina si conoce o no cómo reenviar el paquete al siguiente salto. Si el ruteador no conoce cómo reenviar el paquete por lo regular el paquete se pierde, pero si sabe cómo reenviarlo, el ruteador le cambia la dirección física al paquete con la dirección del siguiente salto y lo transmite. El siguiente brinco puede ser el host destino, pero si no, comúnmente es otro ruteador. El cual hace el mismo procedimiento de switcheo, como los paquetes son enviados a través de redes, la dirección física del paquete cambia pero el protocolo de direccionamiento permanece igual.

La descripción anterior describe el proceso de switcheo entre host origen y destino, la Organización Internacional de Estándares (ISO) desarrolló una terminología jerárquica que describe completamente este proceso. Usando esta terminología, los dispositivos de red que no cuentan con la capacidad de reenviar paquetes entre subredes son llamados equipos terminales y los sistemas que tienen esta capacidad son llamados equipos intermedios, éstos, se dividen en los que se pueden comunicar con equipos que se encuentran en el mismo dominio o red(equipos intradominios) y los que están fuera del dominio(equipos interdominios).El ruteo de dominios es generalmente considerado por ser una porción de red bajo políticas administrativas comunes que están reguladas por una serie de guías particulares. El ruteo de dominio es llamado sistema autónomo. Con ciertos protocolos el ruteo de dominio puede ser dividido en ruteo de áreas , pero los protocolos de ruteo internos son usados también para hacer el proceso de switcheo entre redes internas, así como entre redes diferentes.

Pueden existir numerosos ruteadores en el proceso de switcheo

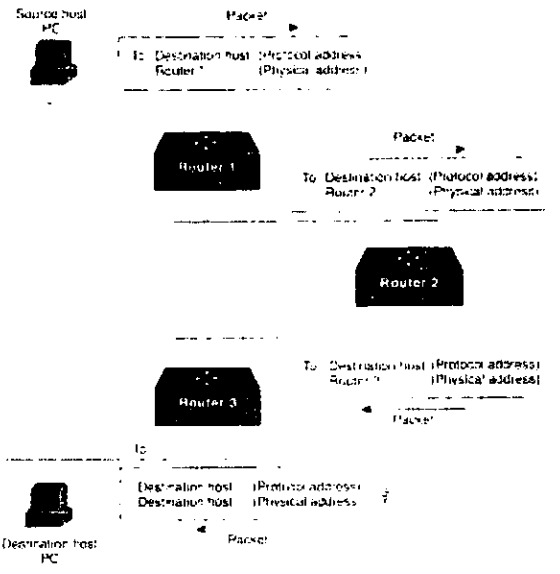


Figura 2 Switcheo entre ruteadores

Algoritmos de Ruteo

Podemos diferenciar los algoritmos de ruteo basándonos en varias características, primero la meta particular del diseño del algoritmo que afecta el resultado del protocolo de ruteo, segundo existen varios tipos de algoritmos de ruteo y cada algoritmo tiene un diferente impacto en la red y sobre los recursos del ruteador, finalmente los algoritmos de ruteo usan una variedad de métricas que afectan el cálculo óptimo de las rutas. A continuación analizaremos estas características de los algoritmos de ruteo.

Metas de Diseño

Los algoritmos de ruteo a menudo tienen estas metas de diseño:

- Optimización
- Simplicidad y bajo costo
- Robustez y Estabilidad
- Rápida Convergencia
- Flexibilidad

Optimización se refiere a la capacidad de que el algoritmo de ruteo seleccione la mejor ruta lo cual depende de las métricas los anchos de las métricas para hacer los cálculos. Un algoritmo de ruteo por ejemplo puede utilizar un número de brincos y retardos, aun que puede manejar retardos más largos y pesados para el cálculo. Naturalmente el protocolo debe definir estrictamente el algoritmo para el cálculo de las métricas.

Los algoritmos de ruteo también son diseñados para ser los más simple posibles, en otras palabras deben ser funcionalmente eficientes, con un mínimo de software y que ocupe poco espacio en memoria. La eficiencia es particularmente importante ya que el software que el algoritmo de ruteo ejecuta debe correr en equipos con características técnicas muy limitadas.

Los algoritmos de ruteo deben ser robustos, esto significa que debe estar preparado para cualquier circunstancia inusual e imprevista como fallas de hardware, malas implementaciones o condiciones de carga elevadas ya que los ruteadores son los puntos de intersección entre las redes, pueden causar serios problemas si llegaran a fallar. los mejores algoritmos de ruteo son a menudo los que han pasado pruebas de tiempo y proveen mayor estabilidad, bajo varias condiciones de la red.

Además los algoritmos de ruteo tienen que converger rápidamente. La convergencia es el proceso de acordar entre ruteadores las rutas óptimas, cuando un evento en la red causa que se pierda la conexión o que este disponible, el ruteador distribuye el mensaje de actualización de rutas entre las redes. Forzando a la recalculación de las rutas optimas y eventualmente causando que los demás ruteadores estén de acuerdo con la ruta. Los algoritmos de ruteo que convergen lento, pueden causar un retraso en las salidas de la red.

En el retraso de ruteo, que se muestra en la figura siguiente, el paquete llega al ruteador 1(r1) en el tiempo 1(t1), el ruteador ha sido actualizado y conoce la ruta óptima hacia el destino y llama al ruteador 2 (r2) que será la siguiente parada. Entonces 1 envía el paquete a r2 pero como éste no ha sido actualizado cree que la ruta óptima es r1, por lo tanto r2 envía el paquete de regreso a r1 y el paquete continúa yendo y viniendo hasta que r2 recibe la actualización o hasta que el paquete ha sido switchado el número de veces emitidas.

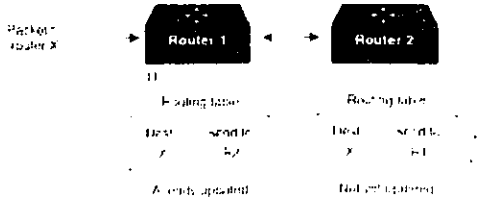


Figura 3 Retraso de ruteo

Los algoritmos de ruteo deben ser también flexibles, esto significa que ellos deben adaptarse rápida y acertadamente a la variedad de circunstancias que existe en la red, pensemos por ejemplo que un segmento de la red ha perdido la comunicación, los ruteadores son enterados del problema,y los algoritmos de ruteo rápidamente seleccionan la siguiente mejor ruta para todos las salidas que utilizaban ese segmento. los algoritmos puedes ser programados para adaptarse a los cambios que se dan en el ancho de banda, el tamaño de la pila del ruteador, los tiempos de retraso en la red, y otras variables.

Tipos de Algoritmos

Los algoritmos se pueden clasificar por características, a continuación se describen:

- Estática Vs Dinámica
- Una ruta Vs Multi Rutas
- Plana Vs jerárquica
- Host inteligentes Vs Ruteo inteligente
- Intradomnios Vs Interdominios
- Estado de enlace Vs Vectores de distancia

Los algoritmos de ruteo estáticos son los más rígidos de todos, y son tablas de ruteo establecidos por el administrador, desde el principio del ruteo, estos mapeos no cambian a excepción de que el administrador las altere. Los algoritmos que usan ruteo estático son simples para diseño y trabajan bien en ambientes de redes donde el tráfico es relativamente predecible y donde los diseños de la red son relativamente simples. Porque los sistemas de ruteo estáticos no reaccionan a los cambios que se producen en las redes, generalmente se consideran poco utilizables en las grandes redes de hoy en día, donde se tienen tantos cambios, La mayoría de los algoritmos dominantes en los años 90 fueron los algoritmos de ruteo dinámico, los cuales se ajustan los cambios de circunstancias que se presentan en la red que continuamente están cambiando, analizando los mensajes de actualización de rutas. Si el mensaje indica que se ha producido un cambio en la red, el software del ruteador recalcula y envía mensaje actualizado con las nuevas rutas. Estos mensajes se encuentran en la red, por lo que propician que los ruteadores ejecuten de nuevo sus algoritmos y actualicen sus tablas de ruteo.

Los algoritmos dinámicos de ruteo se pueden suplir con las rutas estáticas cuando sea apropiado. Un ruteador de último recurso(Un ruteador a donde se envían todos los paquetes que no son ruteados), por ejemplo puede ser designado para que actúe como repositorio para todos los paquetes que no son ruteados, asegurándose que al menos todos los paquetes sean manejados de alguna forma.

Ruta única Vs Múltiples Rutas

Algunos protocolos sofisticados permiten múltiples rutas para el mismo, a diferencia de los algoritmos de una sola ruta, estos algoritmos permiten alternar el tráfico entre múltiples líneas.. la ventaja de utilizar múltiples rutas es obvia: ellos pueden proveer substancialmente una mejora de procesamiento y confiabilidad.

Plana Vs jerárquica

Algunos algoritmos de ruteo operan en un espacio plano, mientras que otros operan con rutas jerárquicas, En el sistema de ruteo plano los ruteadores se encuentran por pares. En el sistema jerárquico de ruteo de algunos ruteadores forman parte de un backbone de ruteo (espina dorsal), los paquetes de un ruteador que no se encuentra en el backbone viaja a uno que sí está en el backbone y viaja sobre él hasta encontrar la zona destino, después son enviados a uno o más ruteadores que no pertenecen al backbone hasta llegar al destino.

A menudo los sistemas de ruteo diseñan grupos lógicos de nodos, llamados dominios, autónomos o áreas. En el sistema de ruteo jerárquico los ruteadores se pueden comunicar entre dominios, mientras otros sólo pueden comunicarse con ruteadores de su mismo dominio, en las redes muy grandes pueden existir niveles jerárquicos, con otros ruteadores de mayor jerarquía formando así un backbone.

La ventaja principal de un ruteo jerárquico es que la mayoría del tráfico es entre la misma compañía (o en el mismo dominio) porque internamente los ruteadores necesitan saber sólo acerca de los ruteadores que están conectados internamente dentro del mismo dominio, sus algoritmos de ruteo pueden ser simplificados y dependiendo del algoritmo de ruteo que empiece a ser utilizado, la actualización del tráfico de ruteo puede ser reducido.

Host Inteligentes Vs Ruteadores Inteligentes

Algunos algoritmos de ruteo asumen que el host origen va a determinar toda la ruta completa, esto es usualmente conocido como ruteo de origen, en los sistemas de ruteo de origen los ruteadores actúan como dispositivos de almacenamiento y reenvió de paquetes al siguiente brinco.

Otros Algoritmos asumen que el host no conoce nada acerca del ruteo, en este tipo de ruteo, los ruteadores son los que calculan las rutas basados en sus propios cálculos, en el primer sistema el host tiene un ruteo inteligente y en el segundo sistema los routers tienen el ruteo inteligente.

La diferencia entre Host Inteligente y Ruteo Inteligente es que el primero encuentra una ruta óptima y el otro detecta el tráfico existente. A menudo los sistemas de host inteligentes escogen la mejor ruta, ya que ellos descubren típicamente todas las rutas posibles hacia el destino antes de enviar el paquete. Ellos escogen la mejor ruta basados en su sistema de definición óptima, esto es detectando todos los ruteadores existentes. No obstante a menudo requiere de generar tráfico en la red y por lo regular una gran cantidad de tiempo.

Dominios Internos (Intradominios)Vs Dominios Externos (Interdominios)

Algunos algoritmos de ruteo trabajan sólo dentro de los dominios, otros trabajan dentro y entre los dominios, la naturaleza de estos tipos de algoritmos es diferente, por esta razón un algoritmo

de ruteo intradominios óptimo podría no ser necesariamente un algoritmo de ruteo óptimo entre dominios.

Estados de Enlace Vs Vectores de Distancia

Los algoritmos de estado de Enlace (también conocidos como algoritmos de primer atajo) llenan de información de ruteo a todos los nodos en la red interna. Cada Ruteador, sin embargo, envía solamente la porción del vector de ruteo que describe el estado de sus propias conexiones.

Los algoritmos de vector de distancia (también conocidos como algoritmos de Bellman-Ford) hacen una llamada para que cada ruteador envíe todos o una cierta porción de su vector de ruteo, solamente a sus vecinos. Esencialmente, los algoritmos del estado de enlace envían actualizaciones pequeñas por todas partes, mientras que los algoritmos de vector de distancia envían actualizaciones más grandes solamente a los ruteadores vecinos.

Porque convergen más rápidamente, los algoritmos del estado de enlace son algo menos propensos a los bucles de ruteo que los algoritmos de vector de distancia. Por otra parte, los algoritmos del estado de enlace requieren más potencia y memoria de CPU que los algoritmos del vector de distancia. Por lo tanto los algoritmos de estado de enlace, pueden ser más costosos al ponerlos en ejecución. A pesar de sus diferencias, ambos tipos de algoritmo se ejecutan bien en la mayoría de las circunstancias.

Métricas de Ruteo

Las tablas de ruteo contienen información que el software de switcheo utiliza para seleccionar la mejor ruta. Pero cómo son construidas específicamente estas tablas de ruteo ¿cuál es la naturaleza específica de la información que ellas contienen?, cómo hacen los algoritmos de ruteo para determinar qué ruta es mejor que otra?.

Los algoritmos de ruteo tienen que usar muchas métricas para determinar qué ruta es la mejor. Algoritmos sofisticados de ruteo basan su selección de ruteo sobre múltiples métricas, combinándola en una sola métrica(Híbrida), las siguientes métricas son usadas:

- Tamaño de la ruta
- Confiabilidad
- Retraso
- Ancho de Banda
- Carga
- Costo de comunicación

El tamaño de la ruta es la métrica más común de ruteo. Algunos protocolos de ruteo permiten que los administradores de la red asignen costes arbitrarios a cada conexión de la red. En este caso,

la longitud de camino es la suma de los costes asociados a cada conexión atravesada. Otros protocolos de ruteo definen la cuenta de Brincos, una métrica que especifique el número de pasos a través de ruteadores de la red , que un paquete debe tomar en el camino de un origen a un destino.

La confiabilidad en el contexto de los algoritmos de ruteo, se refiere a la formalidad (descrita generalmente en los términos de la cantidad de bit-error) de cada conexión de la red. Algunas conexiones de la red a menudo pueden más abajo que otras. Después de que una red falle, ciertas conexiones de la red se pudieron reparar más fácilmente o más rápidamente que otras conexiones. Cualquier factor de la confiabilidad puede ser considerado en la asignación de los grados de la confiabilidad, que son valores numéricos arbitrarios asignados generalmente a las conexiones de la red por los administradores de la red.

El Retardo de ruteo se refiere a la longitud del tiempo requerido para mover un paquete desde un origen a un destino sobre la red. El retardo depende de muchos factores, incluyendo la anchura de banda de la red la cola de espera en cada ruteador, el tráfico de todas las conexiones de la red y de la distancia física entre estas. Porque el retardo es una conglomeración de varias variables importantes, es una métrica común y útil.

El ancho de banda se refiere a la capacidad disponible del tráfico de una conexión. En igualdad de circunstancias, una conexión de Ethernet 10-Mbps sería preferible a una línea de 64-kbps. Aunque el ancho de banda es un grado del rendimiento de procesamiento alcanzable máximo en una conexión, las rutas con conexiones con mayor anchura de banda no proporcionan necesariamente rutas mejores que las rutas con conexiones más lentas. Si por ejemplo, una conexión más rápida está más ocupada, el tiempo real requerido para enviar un paquete al destino podría ser mayor.

La carga se refiere al grado en el cual un recurso de la red, tal como un ruteador, está ocupado. La carga se puede calcular en una variedad de maneras, incluyendo la utilización de la CPU y los paquetes procesados por segundo. Vigilar estos parámetros sobre una base continua puede ser recurso-intensivo de carga.

El coste de la comunicación es otra métrica importante, especialmente porque algunas compañías pueden no cuidar el desempeño sobre funcionamiento, tanto como cuidar la operación del funcionamiento. Aunque el retardo de la línea puede ser más largo, enviarán los paquetes sobre sus propias líneas públicas que cobran dinero por tiempo de uso.

Glosario

Alámbrica: una comunicación es alámbrica cuando utiliza canales de comunicación basados en cables metálicos.

Aleatorio: un fenómeno físico es aleatorio cuando tiene asociados aspectos probabilísticos. es decir, que no pueden ser descritos con certeza.

Ancho de banda: la diferencia entre la frecuencia máxima y la mínima contenidas en una señal.

Atenuación: disminución en la magnitud de una señal.

Bidireccional: una comunicación bidireccional es aquella en la cual puede ser enviada información tanto desde un transmisor hacia un receptor como desde este último hacia el primero.

Bits: palabra que significa símbolos o dígitos binarios; proviene de *binary digits*; es también una medida de la cantidad de información contenida en un mensaje, definida por C. E. Shannon.

Bridges. Permite que las redes se puedan conectar con otras redes que usan el mismo protocolo. Con NetWare, los bridges se pueden instalar directamente en el servidor incluyendo simplemente placas de interfaz de red adicionales. Los bridges también se pueden situar en cualquier punto en la red.

Canal: se usa para identificar una trayectoria a través de la cual serán enviadas señales; también se usa para describir una banda de frecuencias.

Cobertura: es el área geográfica que está incluida en una red o un servicio de telecomunicaciones.

Codificar: representar cada uno de los símbolos provenientes de microondas: es un término que se refiere a señales cuyas frecuencias sean mayores de aproximadamente 500 MHz.

Gateway. Permiten interconectar sistemas con distintos protocolos. por ejemplo se puede conectar una red NetWare con un sistema basado en una computadora central IBM mediante un gateway. Los usuarios de la red pueden accesar al IBM a través del gateway.

Internetwork. Redes interconectadas, se pueden conectar dos o más redes para formar un sistema en red que cubra toda un área. también puede unirse una red extensa en varias redes más pequeñas para optimizar el rendimiento.

LAN (Local Area Network).Red de Area Local. es un sistema de software y hardware conectado por un transmisor de datos común y limitado geográficamente a un área de 10 kilómetros, normalmente localizada en un sólo edificio o grupo de edificios pertenecientes a una organización (de 3 a 50 nodos).

MAN (Metropolitan Area Network).Red Metropolitana, se trata de un conjunto de redes de área local interconectadas dentro de un área específica, como un campus, un polígono industrial o una ciudad, que puede cubrir distancias alrededor de los 80 km. Se ha de utilizar una base de cabelludo o sistema de conexiones especiales a alta velocidad, como una compañía telefónica, para conectar las redes en un sistema interconectado.

Muestreo: proceso mediante el cual se representa una señal continua por medio de valores discretos de la misma, llamados muestras.

Network Architecture. (Arquitectura de Red): define la estructura del sistema de cableado y de estaciones de trabajo conectadas a éste, además de las reglas utilizadas para transferir señales de una estación de trabajo a otra. La estructura física del sistema de cableado se denomina topología de la red.

Network Topology (Topología de una red): es la descripción de como va el cableado de un nodo a otro. Es fácil verlo como un plano del sistema de cableado. El cable puede ser lineal, yendo de un punto del edificio a otro distinto, como una serpiente, o puede cerrarse sobre sí mismo como un anillo. Otra topología es en estrella, en la cual los cables salen de un elemento central o concentrador.

NIC (Network Interface Controller). Placas de interfaz de red, se pueden encontrar entre distintos tipos según se desee configurar o cablear la red. Los tres tipos más usuales son Arcnet, Ethernet y Token Ring. En la actualidad se puede adquirir placas de interfaz de red que admiten diversos medios, lo que hace mucho más fácil la planificación y configuración de las redes.

Nodos: puntos en los cuales se ubican equipos de procesamiento en una red, y a los cuales están conectados los enlaces de la misma.

PCN / PCS: personal communication network / personal communication system: servicios personales de comunicación.

Print Server. Servidor de Impresión, es un módulo cargable NetWare que permite establecer servicios de impresión sobre el servidor. Un servicio de impresión admite hasta 16 impresoras, pero sólo cinco de ellas pueden estar conectadas directamente al propio servidor. El resto puede conectarse a las estaciones de trabajo, pudiendo ser utilizadas por los usuarios de las estaciones de trabajo.

Privacía: característica que señala el hecho de que solo los usuarios autorizados de la información pueden tener acceso a ella.

Protocolo: conjunto de reglas para que pueda ser realizado un proceso de comunicaciones.

Punto a multipunto: comunicación que se origina en un punto geográfico y que puede estar destinada a muchos receptores en puntos geográficamente distante.

Radiotelefonía celular: telefonía basada en transmisiones de radio, que usan una red cuya área de cobertura está dividida en células.

Redes conmutadas: redes de telecomunicaciones que usan el principio de conmutación: compartir canales entre diferentes conversaciones.

Redundancia: dígitos que se agregan a un mensaje, tales que, a pesar de no contener información, ayudan a detectar o corregir errores.

Repeater. Repetidores, como se indico anteriormente, un repetidor amplifica la señal de un cable más allá de sus límites normales. Normalmente consiste en una pequeña caja de conexiones de entrada y salida. Utilizados a menudo en las redes Ethernet, también están disponibles para las redes Arcnet y Token Ring.

Router. Puede utilizarse tanto en las redes como en las metropolitanas o de gran alcance. Los routers funcionan sobre nivel de red del protocolo en niveles, lo que significa que la información de direccionamiento de los paquetes pueden monitorearse y utilizarse para administrar la red, también puede utilizarse para dirigir el tráfico en la red por el mejor camino posible, o dividirlo por dos caminos distintos.

Ruido: perturbaciones indeseadas que tienden a oscurecer el contenido de información en una señal.

Rutas: sucesión de enlaces que conducen la información a través de una red, desde su origen hasta su destino.

Señalizar: proceso mediante el cual se notifica algo (es decir, se envía una señal de control de un equipo de la red a otro.

Server. Una red esta constituida por un conjunto de computadoras que acceden a los recursos y archivos de un Servidor Central, pero que cada computadora ejecuta sus propios procesos. El servidor se utiliza exclusivamente para controlar el almacenamiento y recuperación de información, las tareas de gestión de la red, la gestión de usuarios y la seguridad.

Tasas de transmisión: número de símbolos digitales que se transmiten por un canal en cada segundo.

Teleconferencias: realización de conferencias y juntas entre personas utilizando redes de telecomunicaciones.

WAN (Wide Area Network).Se trata de una red que cubre varios países e incluso el mundo. Un buen ejemplo puede ser el sistema de reservaciones de las líneas aéreas.

Workstation. Estaciones de Trabajo, cuando una computadora se conecta a una red la primera se convierte en un nodo de la última, y se puede tratar como una estación de trabajo, pueden ser computadoras personales con DOS, sistemas Macintosh de Apple, sistemas con el OS/2 o estaciones de trabajo sin disco.