UNIVERSIDAD NACIONAL DE INGENIERIA

FACULTAD DE INGENIERIA ELECTRICA Y ELECTRONICA

"Configuración y Administración del Protocolo de Control de Transmisión/Protocolo Internet en Redes de Computadores bajo Sistema Operativo UNIX"

TITULACION POR EXAMEN PROFESIONAL

PARA OPTAR EL TITULO PROFESIONAL DE:

INGENIERO ELECTRONICO

Armando Alonso Anaya Saavedra

Promoción 1990 - 1

LIMA - PERU - 1995

A mi abuela Mercedes y a mi madre Yolanda, por el abnegado esfuerzo en la formación de mi persona

SUMARIO

Es natural en los computadores generar y procesar datos pero esta información sería inútil si no fuese compartida a todas las personas que la necesitan mas aún si el procesamiento de información se realiza en diferentes computadoras ubicadas en localidades distantes. Es por ello la necesidad de interconectarse y comunicarse entre los diferentes computadores y elementos de la red tales como impresoras, servidores de terminales, etc. siendo estos ubicados en distancias desde 500 mts o estar ubicadas en otro local.

Es por ello el objetivo de instalar y administrar el software de red TCP/IP para sistemas UNIX, que tiene un rol preponderante en las comunicaciones de redes de área local UNIX, el cual consiste en un conjunto de protocolos de comunicaciones de datos.

La instalación del software adecuado nos permitirá comunicarnos entre diferentes computadores de sistemas UNIX y compartir la información y recursos.

Configuración y Administración del Protocolo de Control de Transmisión/Protocolo Internet en Redes de Computadores bajo Sistema Operativo UNIX

EXTRACTO

Título : Configuración y Administración del Protocolo de Control de Transmisión/Protocolo Internet en Redes de Computadores bajo Sistema Operativo UNIX.

Autor : Sr. Armando Alonso Anaya Saavedra

Para optar el Título de Ingeniero Electrónico

Facultad : Ingeniería Eléctrica y Electrónica

Universidad Nacional de Ingeniería

Año : 1995

Al presentarse la necesidad de la interconección entre diferentes computadores para compartir información y recursos se analizó el software que nos permitiría interconectarlos. Este software de TCP/IP es standard por lo que se puede usar para diferentes versiones de sistemas operativos UNIX, tanto para el SCO UNIX o el UNIX system V Release 4.

Luego de recolectar información de los hosts y routers que se deseaban interconectar y las rutas a tomar para llegar a cada host se procedió a configurar el

sistema en cada uno de ellos buscando la solución óptima. Esta etapa es un proceso continuo de acuerdo a como crezca la red debido a la adición de otros hosts de otras localidades y sus respectivos recursos. Es de considerar que esta etapa es de mayor actividad en los inicios del proceso y que va disminuyendo cuando la red va alcanzando la topología planeada.

La etapa siguiente a la configuración es la puesta en marcha del sistema, verificando la comunicación entre hosts y la posibilidad del uso de los diversos recursos de la red tales como terminales, impresoras, unidades de cintas, etc.

La última etapa consiste en la afinación de la red y la adición de los servicios necesarios para el correcto trabajo de los usuarios tomando en consideración la seguridad del sistema , restringiendo recursos a usuarios que no necesitan de ellos o que puedan dar mal uso.

TABLA DE CONTENIDOS

TABLA DE ILUSTRACIONES

PROLOGO

El presente trabajo tiene como propósito mostrar la forma de instalar, configurar y administrar el software de comunicaciones TCP/IP en computadores de sistemas UNIX, definiendo los conceptos, mostrando los motivos del uso de determinados protocolos del conjunto de protocolos TCP/IP y configurando los archivos del sistema que nos permita el uso de TCP/IP. Servirá también como guía para aquellos administradores de redes que necesiten interconectar computadores con sistema UNIX. Los ejemplos han sido trabajados en sistema operativo UNIX System V Release 4 de AT&T pero cabe recalcar que el software TCP/IP es estándar de sistema en sistema Pudiendo existir pequeñas diferencias en las líneas de comando o en las opciones de los comandos, pero estas variaciones no deberían causar mayores problemas.

El trabajo realizado por lo tanto muestra los fundamentos básicos para entender la forma en que trabaja la arquitectura TCP/IP , la configuración del software para lograr que la red esté operativa y la configuración del sistema para tener determinados servicios operativos.

CAPITULO I
DESCRIPCION DE LA ARQUITECTURA EN ESTUDIO

1.1 Protocolo de Control de Transmisión / Protocolo Internet.

El Protocolo de Control de Transmisión / Protocolo Internet (Transmission Control Protocol / Internet Protocol TCP/IP) es un conjunto de protocolos ampliamente usados que habilitan diferentes nodos de ambientes heterogéneos con otros.

El concepto general de conectividad entre redes surge de la investigación conducida por la Agencia de Proyectos de Investigación Avanzada para la Defensa (Defense Advanced Research Projects Agency DARPA). Dentro de esta investigación, DARPA desarrolló el TCP/IP como un conjunto de protocolos para la comunicación entre redes e implementó ARPAnet que luego desarrolló en Internet. TCP/IP define formatos y reglas para la transmisión y recepción de información en forma independiente de la organización de la red o del hardware de la computadora. A pesar de que los protocolos han sido

desarrollados para Internet, también son aplicables para otros casos donde varias redes deben ser conectados.

La red es una red de conmutación de paquetes. Una red conmutada de paquetes transmite información en la red en pequeños segmentos llamados paquetes. Si una computadora transmite un archivo extenso a otra computadora , el archivo es dividido en varıos paquetes en el origen y reemsamblado en el destino. Los protocolos TCP/IP definen el formato, incluyendo el origen, el destino, el tamaño y el tipo del paquete como también la ruta de computadoras en la red para los cuales la recepción y la retransmisión de paquetes es necesario.

El conjunto de protocolos TCP/IP consta de 4 estratos que podrían rotularse como físico, de envío, de servicio y de aplicación. El estrato físico no es especificado y se tiene libertad para realizar cualquier transmisión física, incluyendo a las redes de área vasta, de área metropolitana y de área local.

El protocolo Internet (IP) de TCP/IP es más o menos equivalente al estrato de la red del modelo OSI (Interconección de Sistemas Abiertos , Open System Interconection OSI), en tanto que TCP

corresponde cuando menos al estrato de transporte.

Los otros protocolos asociados con TCP/IP se relacionan con el estrato de aplicación e incluyen el protocolo de transferencia de archivos (File Transfer Protocol FTP) , el protocolo simple de transferencia de correspondencia Simple Mail Protocol Transfer SMPT) y los protocolos de emulación de terminales (telnet).

El conjunto de protocolos TCP/IP corresponde a un modelo de red de comunicaciones definida por la Organización Internacional de Normalización (International Standard Organization ISO). Este modelo es llamado modelo de referencia para la interconección de Sistemas Abiertos (Open System Interconnection OSI). El modelo OSI describe un sistema de red de computadoras en la cual la comunicación de la red ocurre entre procesos en niveles discretos e identificables. Cada nivel de un host dado provee servicios a niveles por encima de él y recibe servicios de los niveles debajo de él. Este modelo consta de 7 niveles que son:

Nivel de aplicación .- Es el nivel donde residen los procesos que los usuarios ejecutan.

Nivel de presentación .- Usado por las aplicaciones que necesitan intercambiar datos, por lo que deben

estar normalizados en la representación de los datos. Brinda rutinas de presentación para normalización. Estas funciones son manejadas dentro de las aplicaciones de TCP/IP.

Nivel de sesión.- En forma similar que el nivel de presentación, el nivel de sesión no es identificado como un nivel separado en TCP/IP. El nivel de sesión administra la conección entre aplicaciones. En TCP/IP esta función se realiza en el nivel de transporte. Para TCP/IP se usan los términos de "socket" y "puerto" para describir el camino con el que se comunican las aplicaciones.

Nivel de transporte.- Garantiza que el receptor tenga los datos tal como fue enviada. En TCP/IP es realizada por el Protocolo de Control de Transmisión (TCP). Aunque TCP/IP ofrece un segundo servicio en este nivel que es el Protocolo de Datagrama de Usuarios (User Datagram Protocol UDP).

Nivel de red.- Administra las conecciones através de la red y aisla los niveles superiores de los detalles de los niveles inferiores.

Nivel de enlace.- Maneja la distribución segura de los datos através de los niveles físicos de la red. TCP/IP escasamente crea protocolos en este nivel.

Nivel físico.- Define las características del

hardware necesario para la señal de transmisión. En este estrato se define el nivel de voltaje , el número y disposición de los pines.

En la figura 1.1 se muestra la relación entre el modelo de referencia OSI y la arquitectura de protocolo TCP/IP.

El sistema estratificado permite concentrar el esfuerzo sobre las funciones de un determinado nivel. No es necesario para ellos crear todo los mecanismos para enviar información através de la red. Ellos deben conocer solamente que servicios necesita el software para proveer al nivel superior, que servicios deben ser entregados al software por parte de los niveles por debajo de él, y que conjunto de protocolos proveen estos servicios.

En la tabla 1.1 se da una lista de los protocolos más comunes del conjunto TCP/IP, los servicios que brindan y la relación entre protocolos y los niveles del modelo de referencia OSI.

Las aplicaciones desarrolladas por TCP/IP generalmente usan varios protocolos del conjunto. La suma de los niveles del conjunto de protocolos es también conocido como la pila de protocolos.

Las aplicaciones de los usuarios se comunican

Figura 1.1. Modelo de Referencia OSI

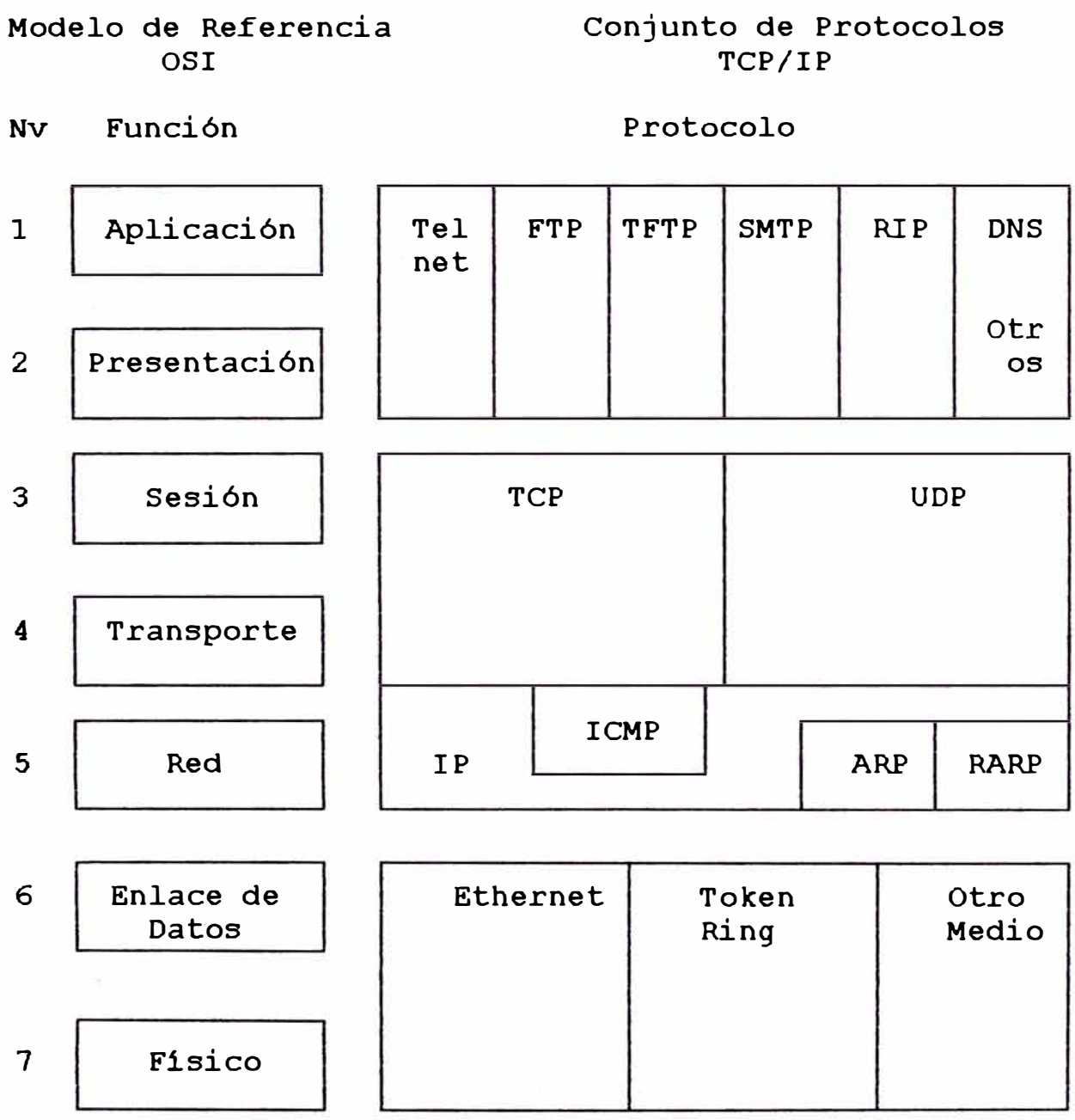


Tabla 1.1.Protocolos TCP/IP

Protocolos	Servicios
Internet Protocol	Provee servicio de empaquetamiento entre nodos.
Internet Control Message Protocol (ICMP)	Control de transmisión de error y control de mensajes entre hosts y gateways.
Address Resolution Protocol (ARP)	Brinda el mapa de las direcciones internet a las direcciones físicas.
Reverse Address Resolution Protocol(RARP)	Brinda el mapa de las direcciones físicas a las direcciones internet.
Transmission Control Protocol (TCP)	Brinda un flujo confiable y controlado entre los servicios y los clientes.
User Datagram Protocol (UDP)	Brinda un flujo el cual no es confiable.
File Transfer Protocol (FTP)	Brinda servicios de aplicación para la transferencia de archivos.
Telnet	Brinda servicio de emulación de terminal
Routing Information Protocol (RIP)	Permite el intercambio de información entre (routers).

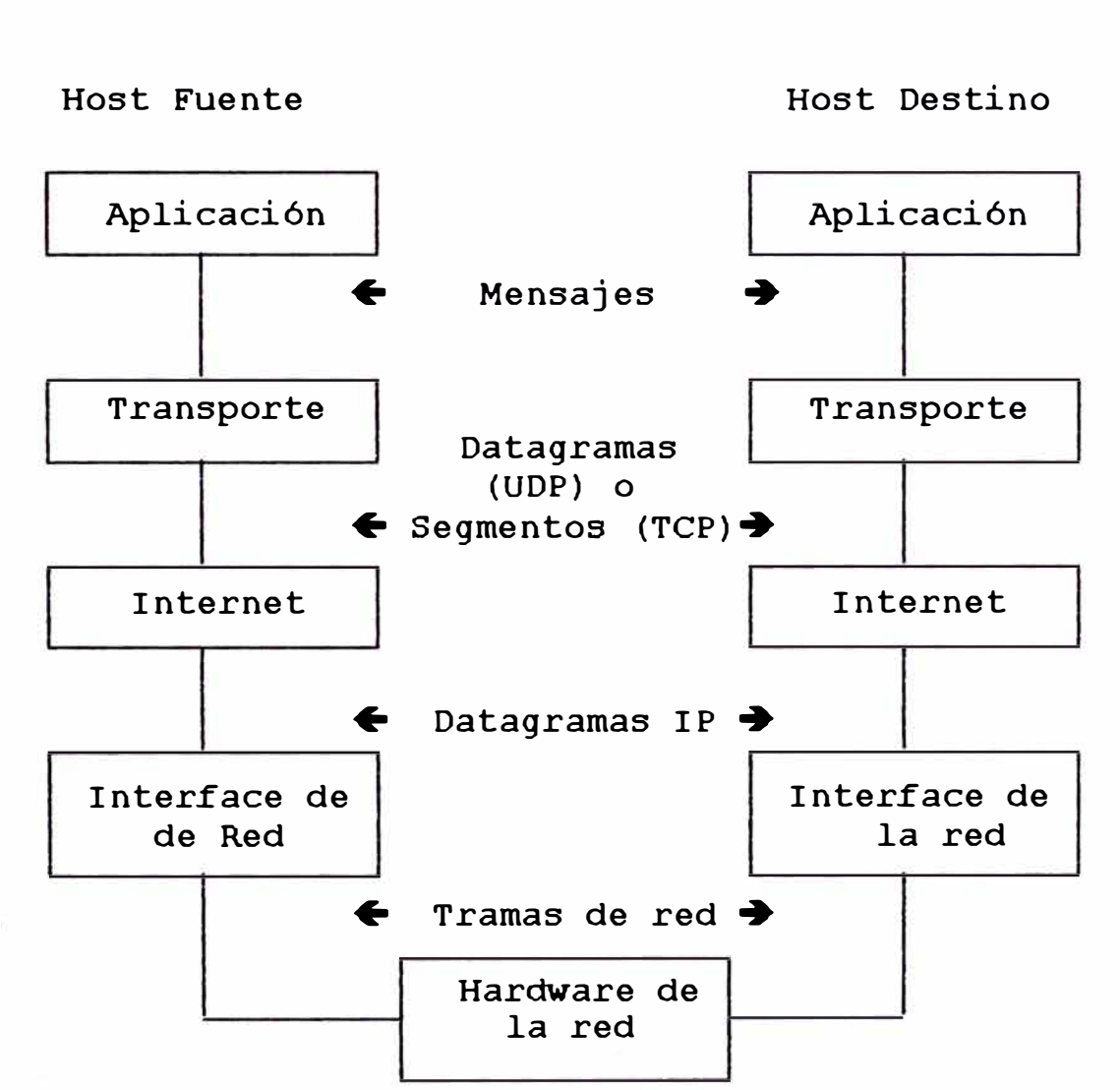
con el nivel superior del conjunto de protocolos. El nivel superior del computador fuente pasa información a los niveles inferiores de la pila, los cuales lo pasan a la red física . La red física transfiere la información al computador destino. Los niveles inferiores de la pila de protocolos del computador destino pasa la información a los niveles superiores, los cuales lo pasan a la aplicación destino.

Cada nivel del protocolo dentro del conjunto TCP/IP tiene varias funciones, estas funciones son independientes de otros niveles. Cada nivel espera recibir ciertos servicios del nivel superior y cada nivel brinda ciertos servicios al nivel inferior.

La figura 1.2 muestra los niveles del conjunto TCP/IP y los términos que se usan en cada uno. Cada nivel de la pila de protocolos del computador fuente se comunica con el mismo nivel del computador destino. Los estratos del mismo nivel en el fuente y destino tienen la misma jerarquía. La aplicación tanto en el fuente como en el destino son de la misma jerarquía . Las aplicaciones que usan TCP se refieren a los datos como corriente, mientras las aplicaciones que usan UDP las llaman mensajes.

TCP llama a los datos como segmento y UDP llama

Figura 1.2 . Estratos del Protocolo TCP/IP



a la estructura de sus datos un paquete. El nivel Internet ve a todo los datos como bloques llamados datagramas. La data transmitida es referida como tramas.

1.2 Nivel de acceso a la red.

Es el nivel más bajo de la jerarquía de protocolos TCP/IP. Los protocolos de este nivel distribuyen los datos a otros dispositivos que están directamente conectados a la red. Este nivel comprende los 3 niveles OSI más bajos (Físico, Enlace y Red).

Dos ejemplos de requerimientos para comentarios (Request For Comments RFC) que definen a protocolos de este nivel son:

RFC 826, Protocolo de Resolución de Dirección (Address Resolution Protocol ARP), que relaciona las direcciones IP con las direcciones Ethernet.

- RFC 894, Modelo para la Transmisión de Datagramas IP sobre redes Ethernet, que especifica como se encapsulan los datagramas IP para su transmisión en una red Ethernet.

1.3 Nivel Internet.

El nivel superior al de acceso de la red es el nivel Internet. IP brinda el servicio básico de distribución de paquetes en las que las redes TCP/IP están construídos. Todos los protocolos que

están en el nivel superior o inferior usan el protocolo Internet para distribuir datos.

1.3.1 Protocolo Internet.

IP es un protocolo sin conexión porque todos los paquetes son transmitidos independientemente unos de otros. IP no intercambia una información de control (handshake) para establecer una conección punto a punto antes de la transmisión de los datos. A diferencia del circuito telefónico donde un circuito es establecido y mantenido y en el cual la distribución de la información que viaja a través de ella está garantizada; IP depende de protocolos de otros niveles para establecer la conección si se requiere un servicio de coneccion orientada.

En IP, todos los paquetes son distribuídos por el servicio de distribución de paquetes el cual es inseguro debido a que la distribución no está garantizada. Un paquete puede ser enviado a la dirección equivocada, duplicado o perdido en el trayecto a su destino. IP no tiene detección de error ni código de recuperación.

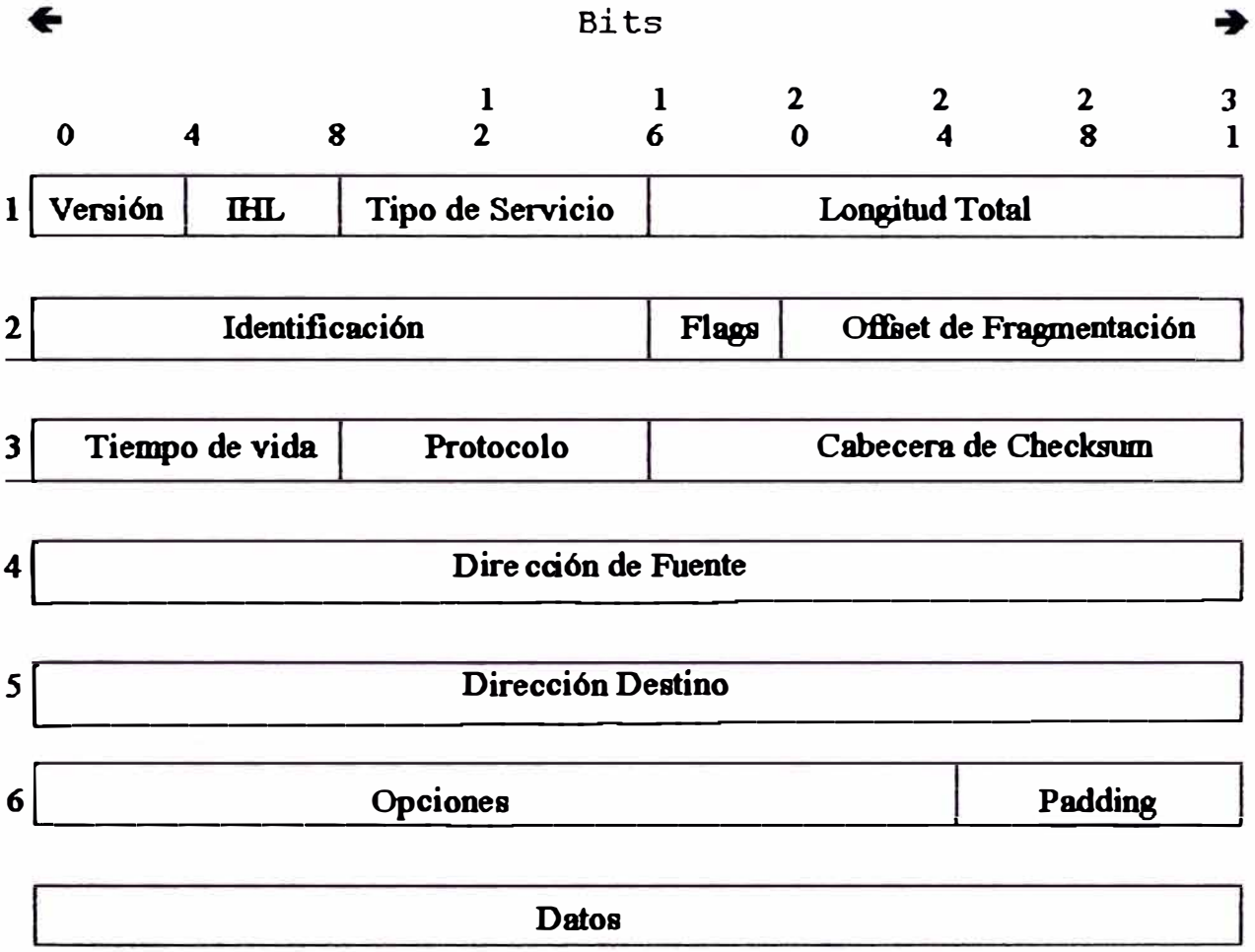
Las aplicaciones TCP/IP que usan este servicio pueden mantener un rastro del estado de la distribución através de la recepción de una replica del nodo destino o usando uno de los protocolos de

los niveles de transporte del conjunto de TCP/IP. Adicionalmente, los routers en Internet pueden enviar un mensaje de error ICMP (Internet Control Message Protocol) para informar acerca de algún problema existente.

El protocolo Internet define la forma que los paquetes deben tomar y el enrutamiento de los paquetes cuando sean transmitidos o recibidos. La forma que el paquete toma se llama datagrama IP. Un datagrama IP es análogo a una trama física transmitida en la red. Un datagrama tiene una sección de cabecera que contiene las direcciones IP del transmisor y del receptor entre otra información y una sección de data. La figura 1.3 muestra el formato general de un datagrama IP. Cada tipo de red transmite paquetes IP en la sección de datos de su trama física.

A diferencia de la trama de red, que tiene una longitud física definida por los requerimientos técnicos de las características físicas de la red, la longitud de un datagrama está definida por el software de la red. Cuando un datagrama es transmitido por una trama de red, es encapsulado en

Figura 1.3. Formato de Datagrama IP



La Cabecera del Datagrama IP está conformada desde la palabra 1 hasta la Palabra 6.

el área de datos de la trama de red. El software IP de un nodo crea una datagrama que cabe en la trama física de la red. En el trayecto al destino, un datagrama puede pasar por diferentes tipos de redes las cuales pueden tener diferentes longitudes de tramas físicas.

Para manejar esta faceta de paquetes de transmisión, el IP especifica un método de división de datagramas en fragmentos dentro de cada nodo que debe retransmitir los datagramas, y un método de reemsamblaje en el nodo destino. Ello se debe por que un router que recibe paquetes de una red puede necesitar fragmentar los paquetes IP para retransmitirlo a otra red, si la segunda red tiene una longitud de trama más pequeño que el primero. Los paquetes fragmentados, no son reensamblados hasta llegar a su destino final.

1.3.2 Equipos de comunicaciones.

1.3.2.1 Routers/Gateways.

Los Routers y Gateways son usualmente la misma cosa. Son generalmente computadoras que conectan 2 o más redes y toman decisiones acerca del enrutamiento de los paquetes entre las redes y ayuda a distribuir estos paquetes a su destino. Los routers y gateways pueden conectar 2 redes de

área local independientes o una red de área local a una red de área vasta, usando una dirección IP para distribuirla.

1.3.2.2 Bridge.

Un bridge es similar a un gateway, excepto que usa una dirección física para distribuir los paquetes, funciona en los niveles físicos y enlace de datos. Un bridge usualmente conecta redes de tipos similares, tal como Ethernet a Ethernet y Token Ring a Token Ring pero también puede ser a redes de tipos diferentes.

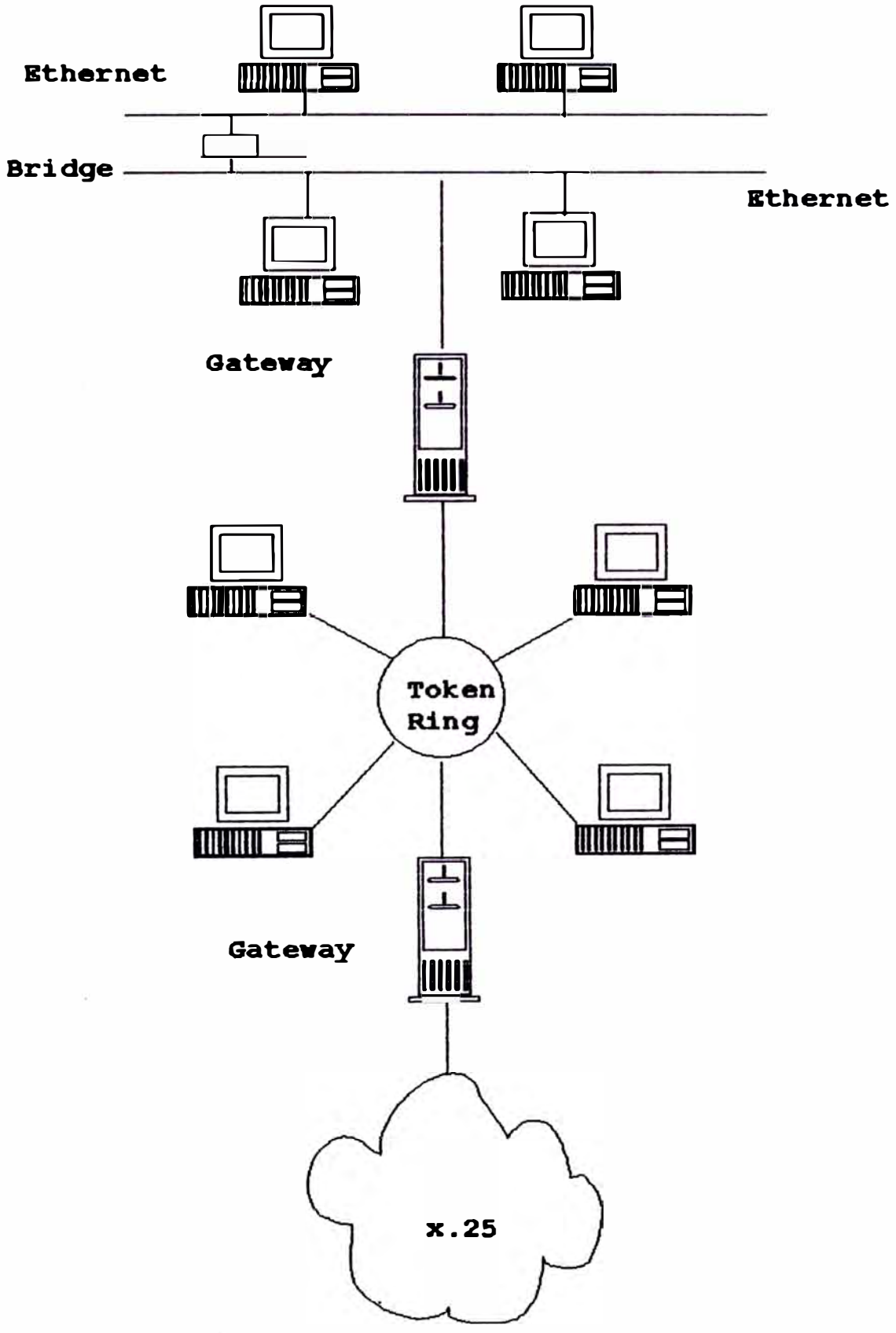
En la figura 1.4 se muestra como son normalmente usados los routers y bridges para unir redes.

1.3.3 Enrutamiento de datagramas.

El enrutamiento se refiere a la transmisión de un datagrama de un nodo a otro de la misma red o de diferente. El término también se refiere a los caminos que son escogidos para transmitir un datagrama IP desde su origen a su destino, basado en las direcciones IP contenidas en el datagrama.

Las dos clases básicas de enrutamiento son la directa y la indirecta.

Figura 1.4 . Conectividad de Redes con Bridges y Gateways



1.3.3.1 Enrutamiento directo.

El enrutamiento directo es la transmisión de un datagrama de un nodo a otro dentro de una sola red. Dentro de la red, el nodo envia un datagrama IP el cual pregunta a los otros nodos de la red por la dirección física que corresponde a la dirección IP, encapsula el datagrama IP en una trama física que contiene la dirección física y lo envía directamente a la dirección física del nodo de la red.

1.3.3.2 Enrutamiento indirecto.

El enrutamiento indirecto es la transmisión de un datagrama de una red a otra através de un nodo llamado router. Cuando un datagrama es enviado a un nodo de otra red, las porciones de red de la dirección IP origen y el de la dirección IP destino son diferente. El nodo emisor reconoce está diferencia y envía este paquete al router que conecta a la red origen con otras redes, como se muestra en la figura 1.4. Dos redes individuales solo pueden estar conectados, si al menos existe una computadora que esta unida a ambas redes y es capaz de pasar los datos en forma que sea compatible con ambas redes.

El nodo emisor tiene una tabla de direcciones

IP de uno o más computadores de la red que sirven como routers a otras redes. Busca la dirección IP del router en su tabla y transmite un requerimiento ARP al router para la dirección física del router. Luego envía un paquete conteniendo el datagrama IP a la dirección física del router. Cuando el router recibe el datagrama IP, usa la dirección IP en el datagrama para enviarlo a su destino final. Si la dirección IP está en la red conectado directamente al router , el router envia el datagrama IP directamente al nodo destino. Para todas las otras direcciones, el router solo tiene la dirección del otro router que puede enrutar el paquete a su destino.

Debido a que un datagrama es enviado através de diversas redes, puede ser necesario que en el router se tenga que dividir en pedazos más pequeños. Esto ocurre cuando el router conecta redes diferentes fisicamente.

Cada tipo de red tiene una unidad máxima de transmisión (Maximun Transmission Unit MTU) que es el paquete más largo que se puede transmitir. Si el datagrama recibido es más largo que el MTU de la otra red, el datagrama se divide en fragmentos más pequeños para su transmisión. Este

proceso se llama fragmentación.

1.3.4 Mensajes de error y control.

Otro protocolo en el conjunto TCP/IP es el Protocolo Internet de Mensajes de Control (Internet Control Message Protocol ICMP). Los paquetes ICMP contienen información acerca de fallas de la red: nodos y gateways inoperativos, congestión de paquetes en un gateway. El software IP interpreta un mensaje ICMP y toma la acción apropiada. Debido a que el mensaje ICMP puede necesitar viajar a través de varias redes para llegar a su destino, se encapsula en la porción de data del datagrama IP.

1.4 Nivel de transporte.

Los protocolos más importantes de este nivel es el Protocolo de Control de Transmisión (Transmission Control Protocol TCP) y el Protocolo de Datagrama del Usuario (User Datagram Protocol UDP). TCP brinda un servicio de distribución de datos confiable con detección y corrección de errores. UDP brinda un servicio de distribución de datagramas sin conección.

1.4.1 Protocolo de datagrama del usuario.

El protocolo de datagrama del usuario (User Datagram Protocol UDP) brinda un servicio de

distribución inseguro y sin conexión para enviar y recibir mensajes de procesos específicos en los nodos de recepción y emisión similar al servicio de distribución que brinda IP. El TCP agrega servicios de distribución confiable en lo alto del protocolo UDP. Uno de los motivos por el cual es usado es cuando la cantidad de datos es pequeña, y el trabajo de crear conecciones y asegurar la distribución es mayor que la retransmisión de los datos.

El protocolo UDP define un conjunto de destinos como puertos de protocolos. Los puertos de protocolos pueden ser de 2 tipos: puertos de asignación conocida y puertos de límites dinámicos. En los puertos de asignación conocida, TCP/IP reserva ciertos números de puertos para determinadas aplicaciones. Los números entre 1 y 255 son números de puertos de asignación conocida y son asignados a una amplia gama de aplicaciones usadas. Todas las aplicaciones TCP/IP usan los mismos números de puertos de la misma forma. En el caso de puertos de límites dinámicos, una aplicación que requiere servicios para un proceso debe preguntar primero por la identificación del puerto que usa el proceso. Luego de ello puede

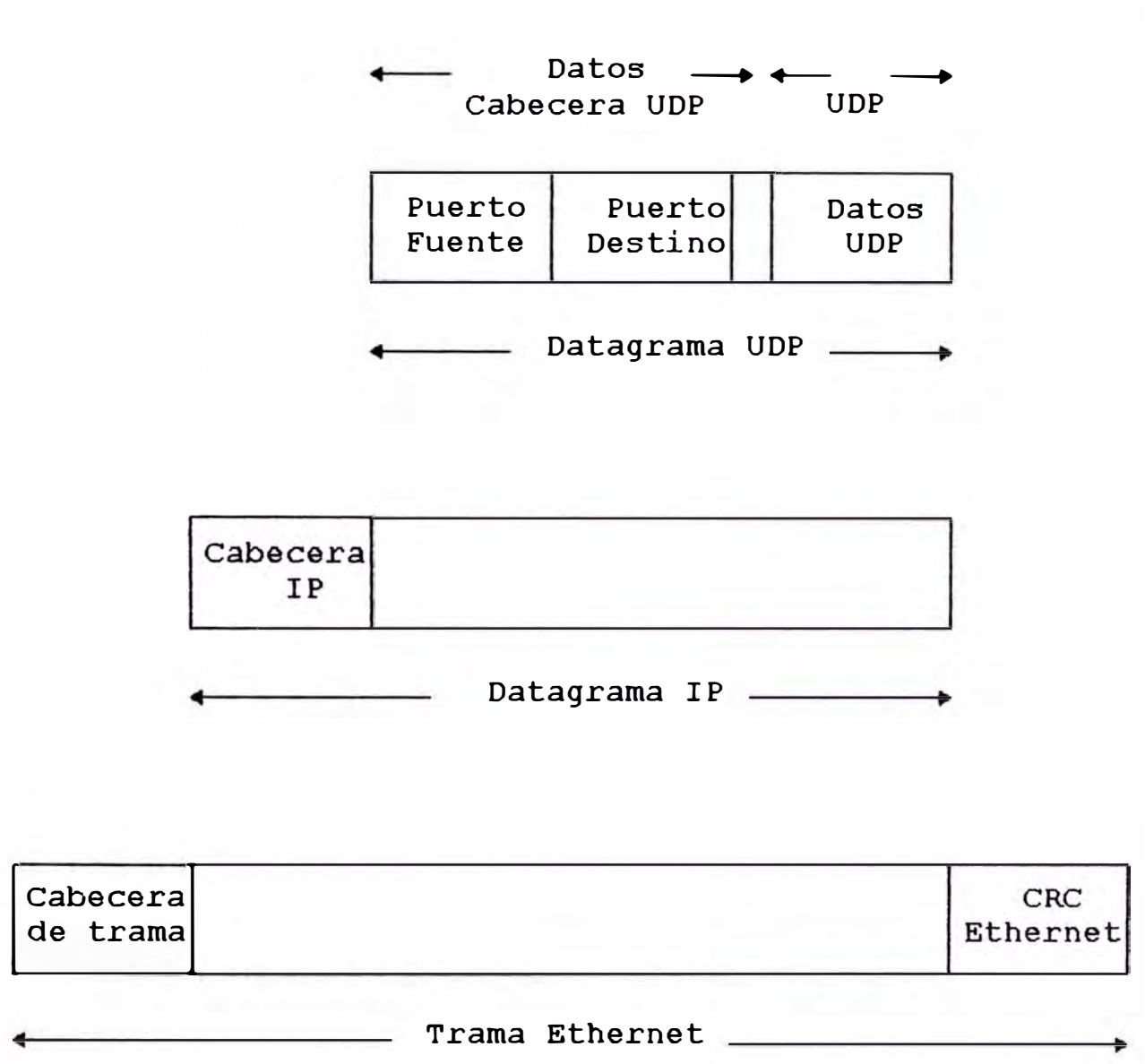
dirigir los datagramas UDP a ese puerto.

El protocolo UDP permite a varios clientes usar el mismo número de puerto y diferentes direcciones IP. Esto usa a las interfaces del nivel de transporte (Transport Layer Interfaces TLI) y socket. Los datagramas UDP entrantes son distribuídos al cliente el cual coincide el número de puerto y la dirección destino. Si no existiese el cliente con esas condiciones, el paquete es distribuído al cliente cuya dirección es 0.0.0.0, si no existiese el cliente con esta dirección, el paquete es eliminado.

El datagrama UDP es encapsulado en uno o más datagramas IP los mismos que se encapsulan en tramas físicas. La figura 1.5 muestra un datagrama UDP encapsulado en un datagrama IP,el cual a su vez es encapsulado en una trama Ethernet con ello se demuestra como el concepto de estratificación afecta la construcción de paquetes enviados a través de la red.

En este ejemplo, la dirección IP dirige el datagrama IP al nodo correcto. En el destino, el software IP extrae el datagrama UDP y los distribuye al nivel UDP. El nivel UDP distribuye los datos UDP y la información de control al puerto

Figura 1.5 .Encapsulamiento de un datagrama UDP.



de protocolo destino que es especificado.

El datagrama UDP también contiene un puerto de protocolo fuente para que el proceso destino pueda responder correctamente.

1.4.2 Protocolo de control de transmisión.

Para aplicaciones que deben enviar o recibir grandes volumenes de datos, el servicio de distribución de paquetes inseguro y sin conexión es inapropiado. Los programadores de aplicaciones pueden tener que desarrollar manejadores extensos de error y módulos de estado de la información para observar el progreso y el estado de la transferencia de la data para cada obligación. El conjunto de protocolos TCP/IP evita este problema usando el protocolo de control de transmisión (Transmission Control Protocol TCP) el cual es un protocolo de distribución confiable en el que se establece un circuito virtual entre 2 aplicaciones, y se envia una corriente de bytes al destino en exactamente el mismo orden que fueron dejados en la fuente. Antes de que la transmisión comience, las aplicaciones en los extremos de la transmisión obtienen un puerto TCP de sus respectivos sistemas operativos. Estos son análogos a los puertos usados por el protocolo UDP. La aplicación que inicia la

transferencia, conocida como el lado activo, generalmente obtiene un puerto dinamicamente. La aplicación que responde el requerimiento de transferencia, conocido como el lado pasivo, generalmente usa un puerto de asignación conocida. El lado activo llama a un puerto de asignación conocida en el lado pasivo.

Como los datagramas UDP, los segmentos TCP son encapsulados en un datagrama IP. TCP hace esperar a la corriente de bytes en espera de suficiente cantidad de datos para completar un datagrama antes de enviarlo. La corriente de bytes no es estructurado, lo que significa que antes de la transmisión de datos , ambas aplicaciones (emisor y receptor) deben concordar en el contenido de la corriente de bytes. El protocolo TCP usa transmisión full-duplex. Full duplex significa que 2 corrientes de datos pueden viajar en direcciones opuestas simultaneamente. Por lo que la aplicación receptora puede enviar información de control a la aplicación emisora mientras que ésta continue enviando datos.

El protocolo TCP da a cada segmento un número secuencial. En el extremo receptor del circuito virtual, la aplicación verifica la secuencia de los

números para asegurar que todos los segmentos han sido recibidos y procesados en estricto orden. Cuando el extremo receptor consigue el siguiente segmento de la secuencia, envia una señal de reconocimiento (acknowledgment) al nodo emisor. Cuando el nodo emisor recibe la señal de reconocimiento, indica a la aplicación que el último segmento ha sido satisfactoriamente enviado. Si el nodo emisor no recibe una señal de reconocimiento por un segmento dentro de un cierto tiempo, el segmento se retransmite. Este esquema, conocido como reconocimiento positivo con retransmisión, asegura que la distribución sea confiable.

1.5 Nivel de aplicación.

Este nivel incluye todos los procesos que usan los protocolos del nivel de Transporte para distribuir datos.

Los protocolos de aplicaciones comunmente usados son:

- Protocolo de información de enrutamiento (Routing Information Protocol RIP). Permite la construcción dinámica de tablas de enrutamiento.
- Sistema de Archivos de Redes (Network File System NFS) . Permite compartir archivos de varios hosts de

la red.

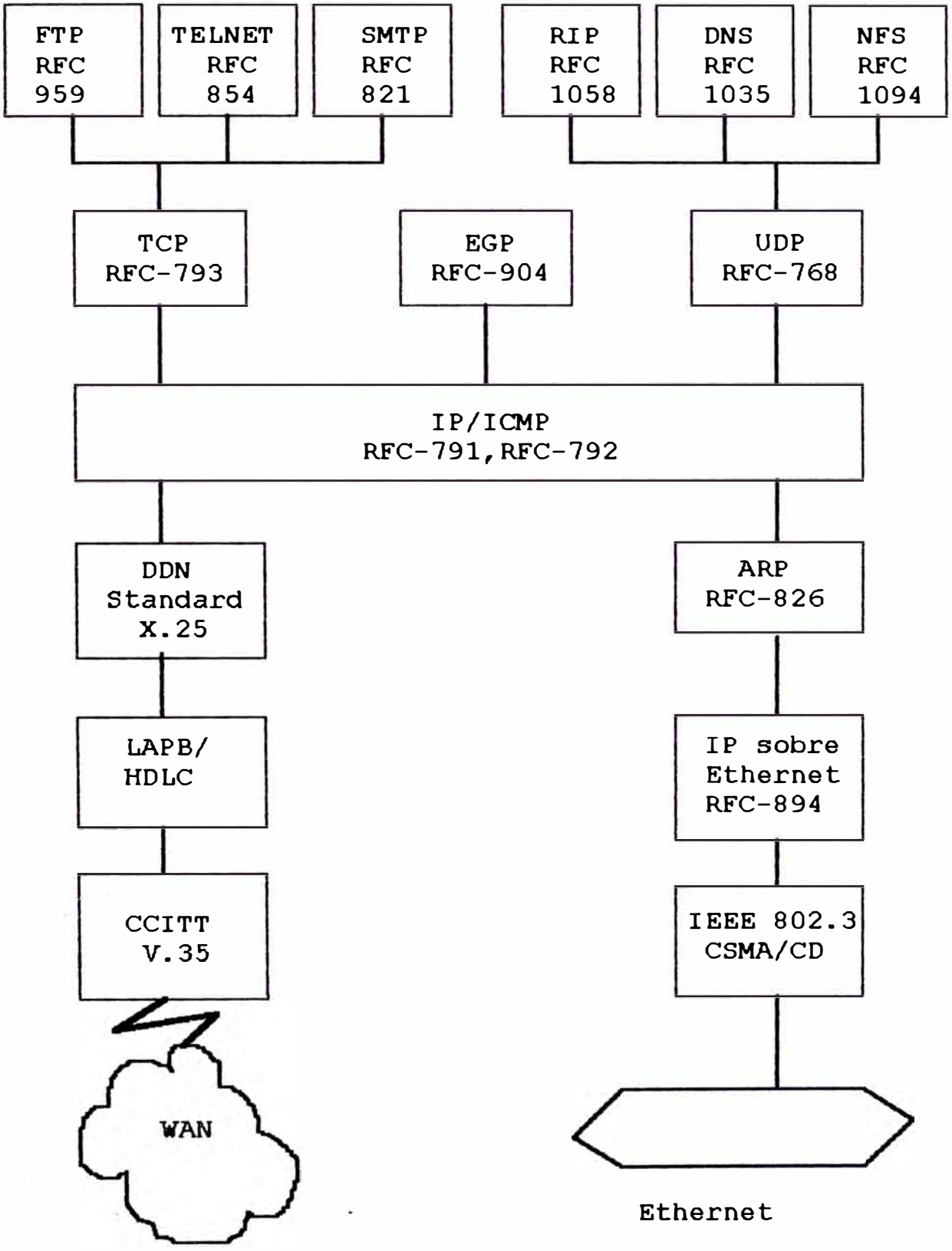
Varios protocolos como FTP y TELNET pueden ser usados si el usuario tiene conocimiento de la red. Otros protocolos como RIP se ejecutan sin conocimiento del usuario.

La figura 1.6 muestra la jerarquía de protocolos. Cada protocolo está con su respectivo RFC que lo define. Se muestra en el nivel de aplicación que FTP, TELNET y SMTP recaen en TCP mientras que NFC, DNS y RIP recaen en UDP. Pocos protocolos de aplicación como el Protocolo de Puertas Exteriores (Exterior Gateway Protocol EGP), protocolo de enrutamiento, no usa el nivel de transporte, usando directamente el nivel IP.

Una aplicación de transferencia de archivos usando TCP/IP realiza las siguientes operaciones para enviar los archivos:

1. El nivel de aplicación pasa un conjunto de bytes al nivel de transporte del computador fuente.
2. El nivel de transporte divide el conjunto de bytes en segmentos TCP, agrega una cabecera con un número según una determinada secuencia para aquel segmento y pasa el segmento al nivel internet (IP).

Figura 1.6. Protocolos TCP/IP dentro de un gateway



3. El nivel IP crea un paquete con una porción de data conteniendo al segmento TCP. El nivel IP agrega una cabecera conteniendo las direcciones IP de los computadores fuente y destino. El nivel IP también determina la dirección física del computador destino o los computadores intermedios que están en el camino al host destino. Pasa el paquete y la dirección física al nivel de enlace.
4. El nivel de enlace transmite el paquete IP en una porción de data de una trama de enlace al computador destino. Esto puede incluir un encaminamiento através de sistemas intermedios.
5. En el computador destino, el nivel de enlace disgrega la cabecera de enlace y pasa el paquete IP al nivel IP.
6. El nivel IP verifica la cabecera del paquete IP. Si la suma de chequeo contenida en la cabecera no corresponde con la suma de chequeo calculado por el nivel IP, se rechaza el paquete.
7. Si las sumas de chequeos son iguales, el nivel IP disgrega la cabecera del paquete IP y pasa el segmento TCP al nivel TCP. El nivel TCP verifica la secuencia del número para

determinar la corrección de la secuencia del segmento.

8. El nivel TCP calcula una suma de chequeo de la data. Si no corresponde la suma con la transmitida en la cabecera, el nivel TCP rechaza el segmento. Si corresponde y el segmento esta en la secuencia correcta, el nivel TCP envía una señal de asentimiento a la computadora fuente.
9. En el computador destino, el nivel TCP disgrega la cabecera TCP y pasa los bytes del segmento recibido a la aplicación.
10. La aplicación en el computador destino recibe el conjunto de bytes como si estuviese conectado a la aplicación de la computadora fuente.

TCP/IP usa 3 esquemas para distribuir los datos entre 2 hosts, estos son:

- Direccionamiento, Direcciones IP, que identifican a cada host de la red, para distribuir los datos en el host correcto.
- Enrutamiento, Routers que distribuyen los datos en el host correcto.
- Multiplexado, Números de protocolos y puertos para distribuir los datos al software correcto dentro del

host.

- Direcciones Físicas y Direcciones Internet.

1.6 Dirección IP y dirección física.

En el nivel de enlace, los nodos de una red se comunican con otros nodos de la red usando direcciones específicas de la red. Un nodo de la red puede ser una microcomputadora, un servidor de archivos, una impresora o cualquier dispositivo con su respectivo implementación TCP/IP.

Cada nodo tiene una dirección física para el dispositivo de hardware específico que lo conecta a la red. Las direcciones físicas tienen diferentes formas en diferentes redes. Por ejemplo una dirección física de una red Ethernet es un valor númerico de 6 bytes, asignado por la fabrica. Las redes X.25 usan estandares X.121 para las direcciones físicas, que consisten en números de 14 dígitos. Las redes LocalTalk usan direcciones de 3 bytes, consistentes en un número de red de 2 bytes y un número de nodo de 1 byte. En una red LocalTalk, el número de red es estático, pero el número de nodo es asignado dinamicamente cada momento que el nodo se inicializa.

La dirección IP para un nodo es una dirección lógica la cual es independiente del hardware y de

la configuración de la red, manteniendo su misma forma. Es un valor número de 4 bytes (32 bits) que identifica a ambos, a una red y un host local o nodo (computador u otro dispositivo) de la red. La dirección IP es representado con notación decimal separada por puntos. Cada byte es representado por un número decimal, y los bytes son separados por puntos (por ejemplo, 150.0.1.100). En algunos casos las direcciones IP son representados en forma octal o hexadecimal. Cada aplicación de transmisión envía también su dirección IP en el paquete. La aplicación de recepción puede replicar al emisor usando la dirección IP enviada en el paquete.

Puesto que las direcciones IP son independientes de cualquier tipo de red, ellos pueden ser usados para enviar paquetes de un tipo de red a otro. En cada tipo de red, el software TCP/IP realiza la correspondencia entre la dirección física y la dirección IP en la misma red.

Para asignar una dirección IP en el caso de no pertenecer a la comunidad Internet, se puede escoger de forma arbitraria, pero teniendo las siguientes consideraciones:

La porción de red de cada dirección debe coincidir con la dirección de la red.

La dirección IP de cada nodo debe ser única dentro de la red.

1.7 Clases de direcciones IP.

La dirección IP de 4 bytes está dividido en 2 partes:

Una porción de red, que identifica a la red.

Una porción de host, que identifica al nodo.

Las direcciones IP están diferenciadas en 3 clases basados en los 2 bits más significativos del primer byte de los 4 que compone la dirección. Esto se debe para que los routers puedan extraer con facilidad la porción de red de la dirección.

Esta división puede pertenecer a 1 de 3 grupos dentro de la dirección de 32 bits. Esta división corresponde a 3 clases de direcciones Internet: Clase A, Clase B y Clase C. Sin considerar la clase de dirección, todos los nodos en una sola red comparten la misma porción de red y cada nodo tiene una única porción de host.

1.7.1 Dirección clase A.

Una dirección IP clase A consiste de una porción de red de un byte seguido por una porción de host de 3 bytes. El bit más alto de la porción de red siempre es 0. Dentro de una interconección de redes se puede tener hasta 126 redes de clase A

(del 1 al 126) con más de 16 millones de nodos en cada red (las redes 0 y 127 están reservadas).

Por ejemplo ('n' = dirección de red y 'h' = dirección del host)

Clase A 0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh

(7 bits de la dirección de la red, 24 bits de la dirección del host). La figura 1.7 muestra la estructura de una dirección clase A.

1.7.2 Dirección clase B.

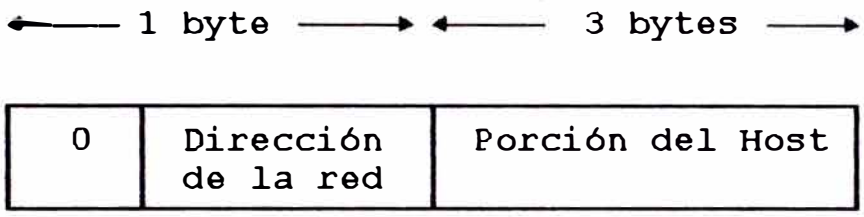
Una dirección IP clase B consiste de una porción de red de 2 bytes seguido por una porción de host de 2 bytes. Los 2 bits más altos de la porción de red siempre son 10. Por lo que en una interconección de red se puede tener hasta aproximadamente 16 mil redes de clase B con más de 65 mil nodos cada uno. La figura 1.7 muestra la estructura de una dirección clase B.

1.7.3 Dirección clase C.

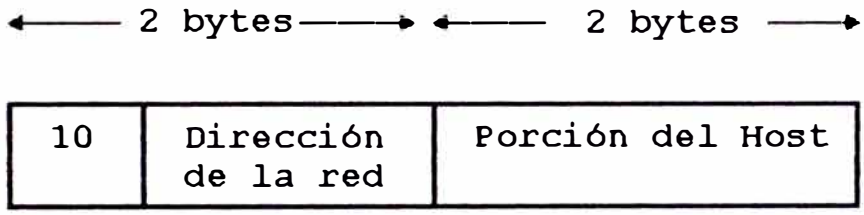
Una dirección IP clase C consiste en una porción de red de 3 bytes seguido por una porción de host de 1 byte. Los tres bits más altos de la porción de red siempre son 110. Por lo que en una interconección de red se puede tener hasta aproximadamente 16 millones de redes de clase C con hasta 254 nodos cada uno .

Figura 1.7. Estructura de una dirección IP.

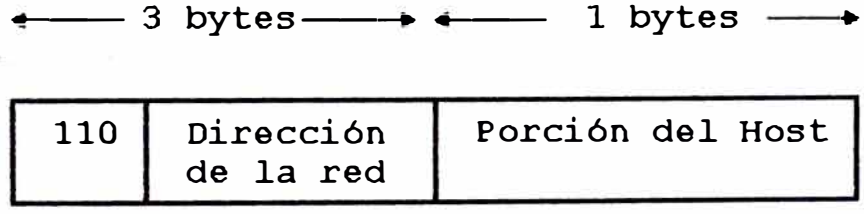
Clase A



Clase B



Clase C



La figura 1.7 muestra la estructura de una dirección clase C.

Los rangos de las direcciones IP de las 3 clases son las siguientes:

001 - 127	(001.h.h.h - 127.h.h.h)	Clase A
128 - 191	(128.n.h.h - 191.n.h.h)	Clase B
192 - 223	(192.n.n.h - 223.n.n.h)	Clase C

La dirección IP del host denominado sunatx es 150.200.1.245 es de clase B, siendo la porción de red 150.200.0.0 y la porción de host #.#.1.245.

La porción de red de una dirección IP debería ser el mismo para todos los nodos de una red.

Las reglas de direccionamiento IP se reserva las siguientes direcciones para propósitos especiales:

- **Direcciones de redes** .- Estos son direcciones IP en que la porción de host son todos ceros. Por ejemplo 150.200.0.0 es la dirección de la red de clase B.
- **Direcciones de Broadcast.**- Estos son direcciones en la que la porción de host son todos unos. Un paquete con una dirección broadcast está destinado para todos los nodos de la red. Por convención,

ningún nodo tiene asignado la porción de red a unos.

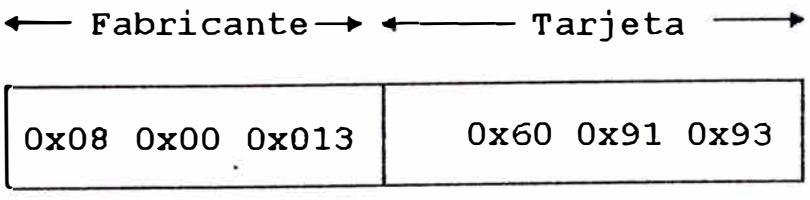
- **Direcciones de Lazos.**- Son direcciones reservadas 127.0.0.0 y 127.0.0.1.

1.8 Traducción de la dirección internet a física.

Cada medio físico tiene su propio dirección física para los nodos de aquel medio. Las direcciones físicas son también llamadas direcciones de control de acceso al medio (Media Access Control MAC). Las redes Ethernet usan direcciones MAC de 6 bytes.

Un ejemplo de la forma de una red Ethernet se muestra en la figura de abajo. La dirección MAC completa es siempre única para cada nodo. Los 3 primeros bytes representan el número único de identificación del fabricante, y los restantes 3 bytes, que pueden ser duplicados, representa el número de identificación de la tarjeta.

Dirección Física Ethernet



Las direcciones IP son independientes del

hardware. Cuando un paquete IP es transmitido en la red, primero es encapsulado con la trama física usado por la red. En la figura 1.5 se mostraba un paquete IP encapsulado en una trama Ethernet. El paquete IP contiene una dirección Internet para un nodo, pero la trama Ethernet debe tener una dirección física para que sea distribuído en la red. Por lo que el nodo emisor debe ser capaz de determinar que dirección física de la red corresponde a que dirección IP contenida en el paquete IP.

1.9 Sub-redes.

La estructura estándar de una dirección IP se puede modificar localmente usando algunos bits de la dirección del host, con lo que creamos redes adicionales y reducimos el máximo número de hosts de cada red. Estos nuevos bits de red define una red dentro de una red mayor, que se llama sub-red.

Para la división de nuestra red se ha tomado las siguientes razones:

Para usar múltiples medios.- Sería imposible, incoveniente o muy caro el conectar todos los nodos a un solo medio de red cuando estos nodos se ubican muy lejos.

- Reducir congestión.- El tráfico entre nodos de una

sola red usa una red de banda ancha. Por lo que se necesita más ancho de banda cuando se tiene mas nodos en la red. La congestión es reducida en una sola y pequeña red.

- Reducir el uso de CPU.- La reducción del uso de CPU de los nodos conectados es similar a reducir la congestión. Mas nodos en la red causan mas envíos. Aun si un envío no es emitido a un nodo en particular, cada nodo debe reaccionar a aquel envío, antes de decidir si lo acepta o lo rechaza.

- Aislar una red.- Dividiendo una gran red en otras pequeñas, se limita el impacto de los problemas de uno de ellas sobre las otras. Los problemas pueden ser de hardware o software.

- Mejorar la seguridad.- En un medio de red como Ethernet, cada nodo de la red tiene acceso a todos los paquetes enviados en esa red. Se puede brindar un tráfico más sensible a una determinada red.

1.10 Métodos de división de la red.

Se tiene las siguientes opciones para dividir una red:

- Crear números de red.- Se puede crear para cada nueva red un número propio.

- Obtener nuevos números de red.- Si el número de red es asignado por una entidad, estos debe ser

pedidos a ella. Este es el caso de las empresas que están conectadas a Internet. Todos los números de red deben estar asignadas por el Centro de Información de Red (Network Information Center NIC).
- Crear subredes.- Si se ha asignado una red clase A o B, es más fácil dividir la red en sub-redes que requerir redes adicionales. Se puede usar el número de red que uno ya tiene y dividirlo en sub-redes.

Cada subred funciona como si fuese una red independiente. Para redes remotas , las sub-redes aparecen como una sola red. Ello significa que la red necesita solo una dirección Internet y las redes remotas no deben preocuparse por la ubicación de un nodo en particular de la sub-red.

Una máscara de una sub-red indica como es dividido la porción del host de la dirección IP dentro de las direcciones de la sub-red y las porciones de dirección del host local. La máscara de red es un número de 32 bits de los cuales son unos los bits que pertenencen a la porción de dirección de red o sub-red y son ceros los que pertenecen a la porción de dirección del host. Con una porción de dirección de red IP de clase B de 150.244 y una dirección de sub-red de 4 bits, la máscara consistiría en 20 unos y 12 ceros. Por lo que una

máscara de una sub-red extiende la porción de dirección de red. La figura 1.8 muestra los ejemplos de direcciones IP, la relación con la máscara de sub-red y la correspondiente sub-red.

1.10.1 Direccionamiento de una sub-red.

El Centro de Información de Red (Network Information Center NIC) asigna 3 clases de redes IP de acuerdo a su tamaño, como se muestra en la tabla 1.2.

Cuando la NIC asigna una identificación Internet muy alta, existen pocos bits en la porción local para identificar cada host de la red; las identificaciones bajas son para redes grandes.

El direccionamiento de una sub-red es el uso de una sola identificación IP para identificar un número de sub-redes de una organización.

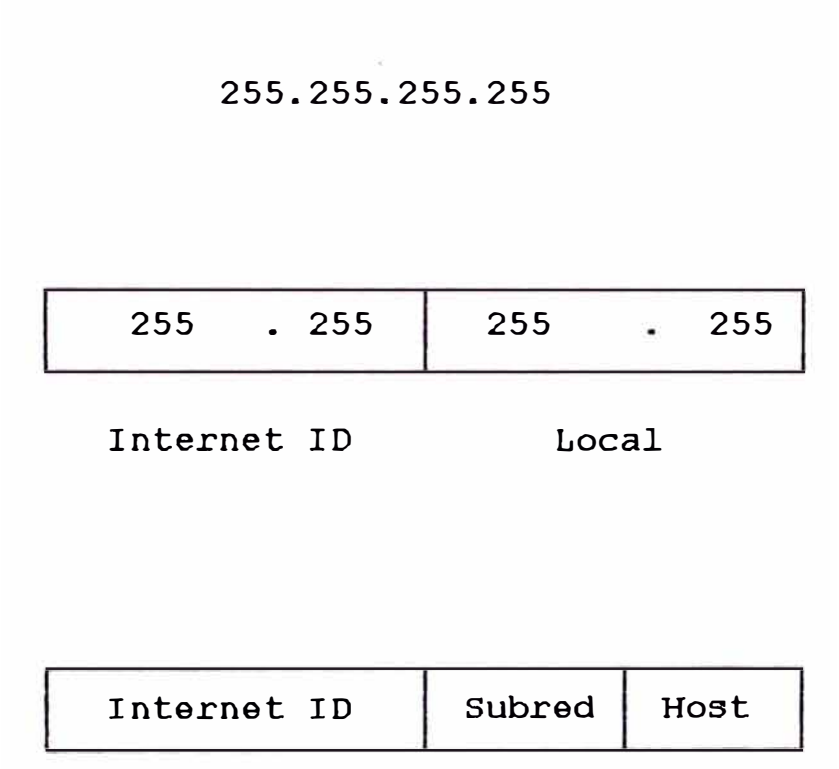
El método divide la porción local de cada dirección IP en una identificación de la sub-red y una identificación del host. Por lo que puede dividirse la red en sub-redes y asignar una identificación de la sub-red a cada red física. La figura 1.9 muestra la dirección IP y como se divide para identificar una sub-red y un número de host.

Figura 1.8 . Máscara de una sub-red y direcciones IP

Tabla 1.2. Clases de Dirección de redes

Clase	Longitud de la ID Internet	Longitud de la porción Local	Tamaño de la red
Clase A	8 bits	24 bits	Grandes
Clase B	16 bits	16 bits	Medianas
Clase C	24 bits	8 bits	Pequeñas

Figura 1.9 . Direccionamiento de una Subred



Por ejemplo en una red clase B, se puede usar el tercer octeto para identificar a la sub-red y el cuarto obteto para identificar al host de cada sub-red.

El direccionamiento mediante sub-redes permite al administrador de cada sub-red asignar en forma fácil la dirección de cada host. Una sub-red con valores de ceros no es recomendado por la RFC 950.

La máscara de la sub-red es un número de 32 bits que define cuantos bits de la dirección identifica a la red y cuantos al host. Un 1 indica que el bit identifica a la red, un 0 indica que identifica al host.

La identificación de la sub-red para la red de clase B del ejemplo anterior era del tercer octeto y la identificación de la red es de 16 bits por lo que su máscara de la sub-red sería:

255.255.255.0

o en binario

11111111 11111111 11111111 00000000

La máscara de la sub-red debería ser determinado por el número físico de redes de la organización y el máximo número de hosts de cada red.

La tabla 1.3 muestra las diferentes máscaras disponibles para una red de clase B, que tiene solamente un octeto en la porción local.

1.11 Tabla de enrutamiento.

Tanto los routers como los hosts pueden enrutar datos entre redes, para ello deben realizar ciertas decisiones de enrutamiento. Para muchos host, las decisiones de enrutamiento son:

- Si el host destino está en la red local, los datos son distribuídos al host destino.
- Si el host destino está en una red remota, los datos son enviados al router local.

El módulo IP determina a que clase pertenece la red chequeando los bits de mayor orden de la dirección. Si el destino de la red es una subred se aplica la máscara de subred a la dirección destino.

Luego de determinar la red destino, el módulo IP busca la red en la tabla local de enrutamiento que dirige los paquetes a su destino. La tabla puede ser construída por el administrador del sistema o por los protocolos de enrutamiento.

La tabla de enrutamiento se puede visualizar con el comando nėtstat y la opción -r , que muestra los siguientes campos:

Tabla 1.3. Máscara de la Sub-red de Clase B

Máx Nº de sub-redes	Max Nº Hosts/ Subred	Máscara de Subred	Longitud de ID de Subred	Longitud de ID de Host
2	16382	255.255.192.0	2	14
6	8190	255.255.224.0	3	13
14	4094	255.255.240.0	4	12
30	2046	255.255.248.0	5	11
62	1022	255.255.252.0	6	10
126	510	255.255.254.0	7	9
254	254	255.255.255.0	8	8
510	126	255.255.255.128	9	7
1022	62	255.255.255.192	10	6
2046	30	255.255.255.224	11	5
4094	14	255.255.255.240	12	4

- Destino — La red destino.
- Router — El route que se debe usar para llegar al destino.
- Banderas — Describe ciertas características de la ruta. Toma los siguientes valores:
  - U — Indica que la ruta está operativa.
  - H — Indica que encamina a un host específico. (Muchas rutas son a redes).
  - G — La ruta usa un gateway. Las redes directamente conectadas no tienen G.
  - D — Ruta que ha sido agregada debido al redireccionamiento de ICMP. Luego los paquetes adicionales para el destino no necesitarán ser redireccionadas.
- Refcnt — Muestra el número de veces que la ruta ha sido referida para establecer la conección.
- Use — Muestra el número de paquetes que ha sido transmitidos por esta ruta.
- Interface — Indica el nombre de la interface de red que es usada por esta ruta.

Una tabla de enrutamiento no contiene rutas de extremo a extremo, solo contiene las rutas al siguiente router, llamado siguiente salto, por el camino a la red destino. Como un datagrama se mueve de un gateway a otro, llegará el momento que esté conectado directamente a su red destino. Es este último gateway el que finalmente distribuya los datos al host destino.

1.12 Resolución de direcciones Internet a direcciones físicas.

La dirección IP y la tabla de enrutamiento dirigen un datagrama a una red física específica, pero cuando los datos viajan através de una red, estos obedecen a los protocolos del nivel físico de la red. Las redes físicas TCP/IP no entienden el direccionamiento IP.

Una dirección IP es correspondida a una dirección física usando el protocolo de resolución de direcciones (Address Resolution Protocol ARP) en una red. Cuando un nodo envía un paquete usando IP, éste debe determinar que dirección física de la red corresponde a la dirección IP especificada en el paquete IP. Para encontrar la dirección física, el nodo envía un paquete ARP conteniendo la dirección IP destino. Luego éste paquete ARP busca una

respuesta del nodo que tenga la dirección IP destino, el nodo con la dirección IP destino envia su dirección física al nodo emisor.

1.13 Resolución cache de dirección.

Para que sea más rápido la transmisión de paquetes y reducir el número de requerimientos de envío, que debe ser examinado por cada nodo de la red, estos tienen un cache de resolución de direcciones. Cada vez que el nodo envía un requerimiento ARP y recibe una respuesta, éste crea una entrada en su cache de resolución de dirección. Esta entrada tiene la relación entre la dirección IP y la dirección física.

Cuando el nodo envía otro paquete IP, la dirección es buscada en el cache. Si lo encuentra, el nodo usa la correspondiente dirección física. El nodo envía un requerimiento ARP en el caso de que la dirección IP no esté en el cache.

CAPITULO II
CONFIGURACION DEL SISTEMA

2.1 Características del UNIX.

El sistema operativo UNIX es un sistema multiusuario y multitarea, conformado por 2 partes que son el Kernel (núcleo principal del sistema Operativo) y el file system.

El kernel es un conjunto de programas residentes en memoria que coordinan los procesos básicos y los recursos del computador, ocupándose de los discos unidades de cintas, terminales , impresoras, líneas de comunicación y cualquier otro dispositivo. El File System o sistema de archivos es la estructura para la organización de datos en UNIX, quizás es la parte más importante del UNIX y que proporciona los medios para organizar el almacenamiento de los datos.

2.2 Estructura de un file system.

El file system está compuesto por un conjunto de directorios, archivos ordinarios y archivos especiales.

Un directorio es una colección de archivos y

otros directorios.

Un archivo ordinario es una colección de caracteres que son almacenados en el disco. Un archivo puede contener el texto de un reporte de estado o el código de un programa que se haya escrito. Cualquier información que se desee guardar debe ser escrita en un archivo.

Un archivo especial representa a un dispositivo físico tal como un terminal o una ımpresora.

Estos componentes brindan las formas de organizar, recuperar y administrar la información. El conjunto de todos los directorios y archivos están organizados en una estructura en forma de árbol como se muestra en la figura 2.1.

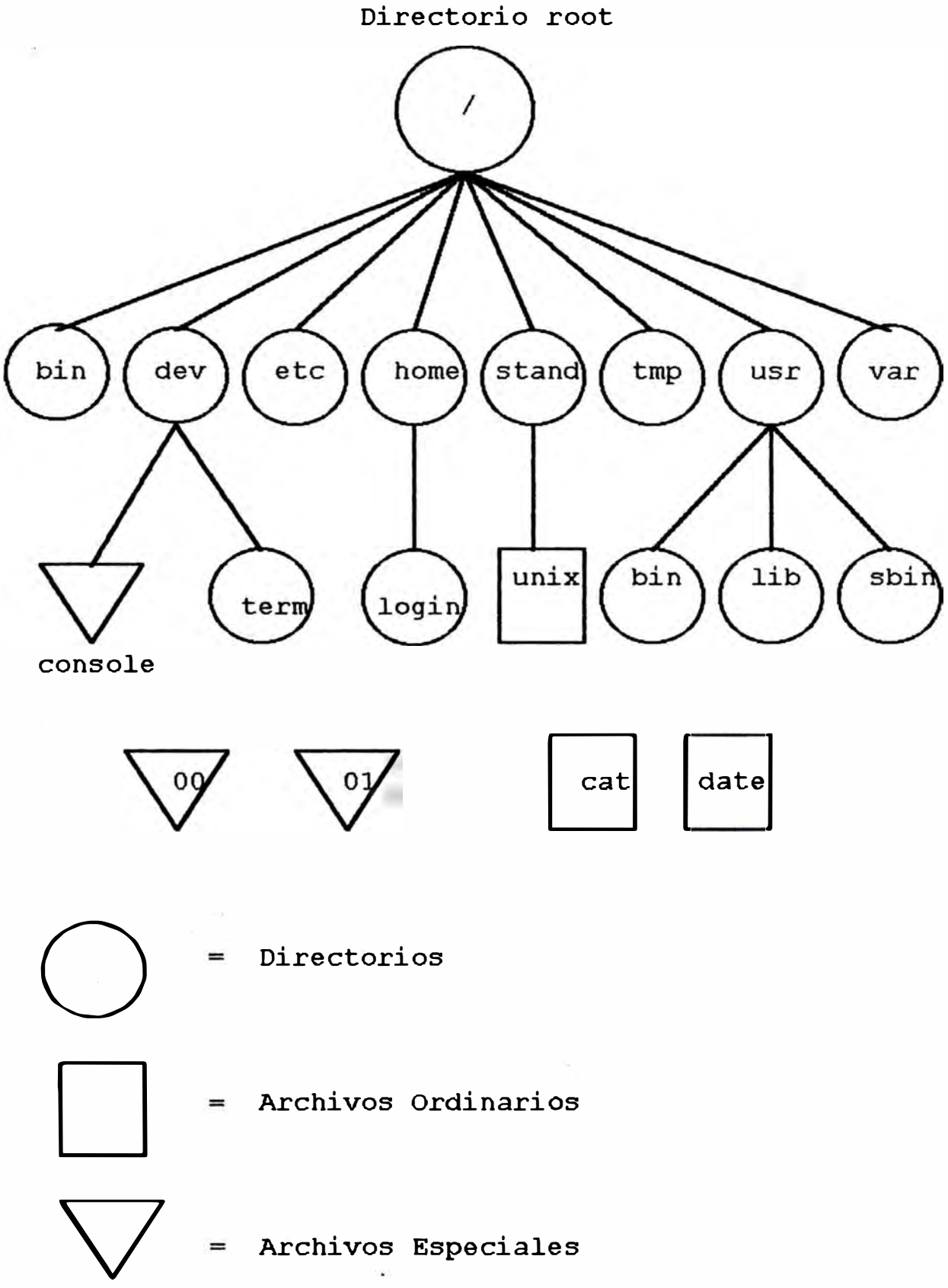
El directorio llamado root es la fuente de esta estructura de archivos. En cuanto se descienda por las ramas que se extienden de root, se alcanzará diferentes directorios del sistema tal como bin, dev,lib,usr.

2.3 Estructura del directorio raíz "root".

A continuación se indican los principales archivos y directorios que conforman el directorio raíz (root) del UNIX System V Release 4 de AT&T:

- bin . directorio donde se encuentran los archivos binarios del sistema operativo (ejecutables).

Figura 2.1. Estructura de un File System



- dev . directorio donde se encuentran los archivos especiales de los dispositivos del sistema.
- etc . directorio donde se ecncuentran los archivos y herramientas de administración del sistema como : scripts de arranque y apagado del sistema, archivos de autenticación de usuarios, archivos de configuración del TCP/IP, etc.
- stand . directorio donde se ubican los programas de inicialización del sistema como el boot.
- home . directorio donde se ubican los archivos de los usuarios.

mnt directorio vacío usado para montar file systems temporales.

lost+found directorio donde se ubican los archivos que no tienen referencia durante el proceso de verificación del sistema de archivos (File System Check fsck).

2.4 Protocolo de resolución de dirección inversa.

El Protocolo de resolución de dirección inversa (Reverse Address Resolution Protocol RFC 903 RARP) es una variante del ARP. RARP traduce las direcciones pero en forma inversa, convirtiendo direcciones ethernet a direcciones IP.

Cuando una estación de trabajo no tiene disco, éste envia un requerimiento de su dirección IP, por

lo que el servidor al recibirlo buscará en el archivo /etc/ethers. Si lo encuentra envia la dirección correspondiente.

2.5 Número de protocolo.

El número de protocolo es un byte ubicado en la tercera palabra de la cabecera del datagrama. El valor identifica el protocolo del nivel superior a IP al que se debe pasar los datos.

Estos números de protocolos están definidos en el archivo /etc/protocol como se muestra en el archivo 2.1.

Cuando llega un datagrama a su destino, el nivel IP sabe que tiene que distribuirlo a un protocolo de transporte. Para identificar quien recibe el datagrama, IP ve el número de protocolo y lo confronta con la tabla. Identificado el protocolo se le envía el datagrama.

2.6 Número de puerto.

Luego de que IP pasa los datos entrantes al protocolo de transporte, el protocolo de transporte lo debe pasar al proceso de aplicación correcta. Los procesos de aplicación (llamados también servicios de red) son identificados por números de puertos que son valores de 16 bits.

Archivo 2.1. Texto de archivo /etc/protocol

```
#
# Internet      (IP) protocols
#
ip   0     IP    # internet protocol, psuedo protocol
number
icmp 1     ICMP  # internet control message protocol
ggp  2     GGP   # gateway-gateway protocol
tcp  6     TCP   # transmission control protocol
pup  12    PUP   # PARC    universal packet protocol
udp  17    UDP   # user datagram protocol
```

El número de proceso fuente, que identifica al proceso que envia los datos, y el número de puerto destino que identifica el proceso que va a recibir los datos son contenidos en la primera palabra de la cabecera de cada segmento TCP y de cada paquete UDP.

Estos números de puertos están definidos en el archivo /etc/services como se muestra en el archivo 2.2. Los números de puertos por debajo del 256 son reservados a servicios conocidos (como ftp y telnet). Los número de puertos del 256 al 1024 son usados por servicios UNIX.

Los números de puertos no son únicos, éstos lo son dentro de un específico protocolo de transporte. Es la combinación de los números de protocolo y puerto que identifica a un específico proceso que debe recibir los datos.

Un datagrama llega a su destino usando la dirección IP que tiene en la quinta palabra de la cabecera del datagrama. IP usa el número de protocolo de la tercera palabra de la cabecera del datagrama para distribuirla al respectivo protocolo de transporte. La primera palabra de los datos distribuídos al protocolo de transporte contiene el número de puerto destino para que el protocolo de transporte lo pase a la aplicación específica.

Archivo 2.2. Texto del archivo /etc/services

```
#
# Network services, Internet style
#
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
chargen         19/tcp          ttytst-source
chargen         19/udp          ttytst-source
ftp-dat         20/tcp
ftp             21/tcp
telnet          23/tcp
smtp            25/tcp          mail
time            37/tcp          timserver
time            37/udp          timserver
named           53/tcp
named           53/udp
nicname         101/tcp         hostnames #
pop2            109/tcp
pop3            110/tcp
exist           545/tcp
vftp            1777/udp
udp             1888/udp
#
# Host specific functions
#
tftp            69/udp
finger          79/tcp
host table      468/udp
#
# Unix specific services
#
exec            512/tcp
rexec           512/tcp
rlogin          513/tcp   login
remsh           514/tcp   shell rsh cmd# no passwords used
who             513/udp   whod
syslog          514/udp
talk            517/udp
ntalk           518/udp
route           520/udp   router routed #521 also
erpc            121/udp
printer         515/tcp   spooler
```

Continuación de archivo 2.2. /etc/services

```
nfsd            2049/udp
snmp            161/udp
snmp-trap       162/udp
snmp-agent      167/udp
bootps          67/udp
bootpc          68/udp
listen          2766/tcp
spi2            1543/tcp  #SPI package
serv-bancos     1540/tcp
serv-ruc        1542/tcp
serv-ruc cc     1544/tcp
serv-comp5      1560/tcp
serv-comp55     1562/tcp
PE0             7000/tcp
PE1             7001/tcp
PE2             7002/tcp
PE3             7003/tcp
xserver0        6000/tcp
```

La figura 2.2 muestra el proceso de distribución.

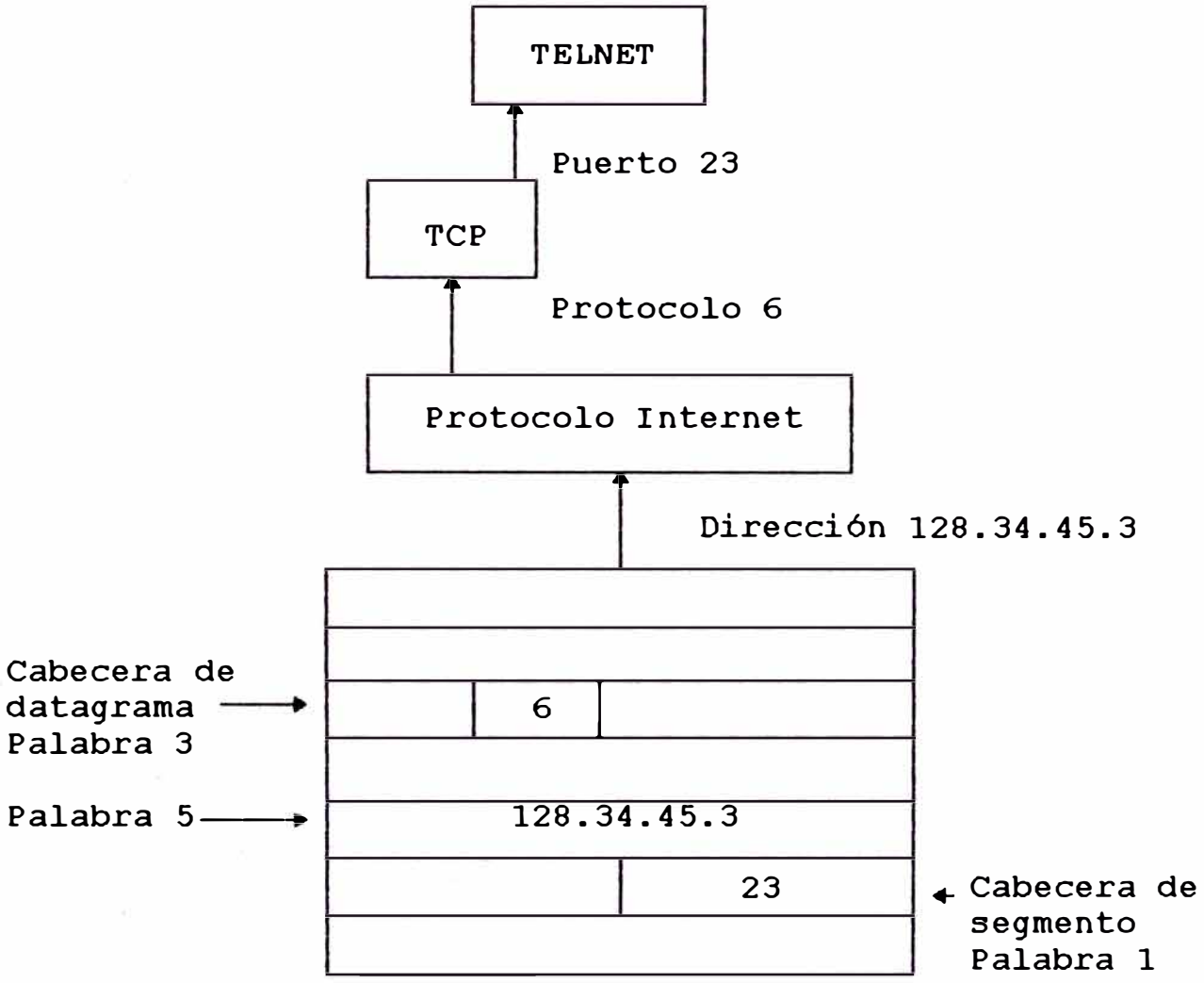
2.7 Sockets.

Puertos conocidos son aquellos que tienen asignados números de puertos específicos con lo que los computadores son capaces de conocer a que puerto conectar para un determinado servicio de red. Esto simplifica el proceso de conección debido a que el emisor y el receptor conocen previamente a que proceso le corresponde el número de puerto. Un ejemplo de ello es el proceso TELNET con número de puerto 23.

Otra clase de número de puertos son los asignados dinamicamente con lo que los procesos no tienen números pre-asignados. Son asignados cuando es necesario. El sistema se asegura de no asignar el mismo número de puertos a 2 procesos, y que esos números estén por encima del rango de números estándares.

Los puertos asignados dinamicamente brindan la flexibilidad necesaria para soportar varios usuarios. Cuando un usuario ejecuta TELNET se le da como puerto fuente un número asignado dinámicamente y como puerto destino, el puerto conocido 23.

Figura 2.2. Números de Protocolos y Puertos



Si otro usuario ejecuta TELNET se le dará como puerto fuente otro número y como puerto destino, el puerto conocido 23. La pareja de puertos, fuente y destino es lo que identifica a cada conección de red.

La combinación de una dirección IP y un número de puerto se le llama socket. Un socket identifica a un solo proceso de red.

2.8 Nombres y direcciones.

Cada interface de red que está conectado a una red es identificado por una dirección IP, por lo que cada uno de ellos puede tener un nombre. Ello se debe a que es más fácil memorizar un nombre que un número.

Existen dos métodos para traducir nombres a direcciones IP. Uno es buscando el nombre del host en el archivo llamado tabla de host (/etc/hosts) y el otro es usando un sistema de base de datos distribuídos.

2.9 Tabla de hosts.

Es un simple archivo de texto y es el /etc/hosts. Cada entrada tiene un campo de dirección IP con su respectivo alias o nombre. Aunque este método ha sido reemplazado por el Servicio de nombres de dominios (Domain Name Service DNS) ,

todavía se usa. El Uso de DNS se justifica por las siguientes razones:

El tiempo que se usa para realizar el mantenimiento de las tablas de información en cada host, por ejemplo si la red es dinámica, lo que implicaría agregar, modificar o borrar frecuentemente los datos de los hosts.

- El espacio en disco requerido en cada host para almacenar el archivo.
- La demora en la búsqueda secuencial del nombre o la dirección en el archivo.

Para configurar TCP/IP en un host, se debe considerar:

Dirección del router por defecto, si es que el sistema se comunica con otros hosts que no están en la red local.

- Protocolo de enrutamiento, si se usa un protocolo de enrutamiento, cada dispositivo debe saber que protocolo es.
- Servidor de nombres de los hosts, ya sea através de /etc/hosts o DNS.

Máscara de la sub-red, para comunicarse apropiadamente, cada sistema en la red debe usar la misma máscara de subred.

Dirección de comunicación general, que debe ser

igual para cada computadora de una red.

2.10 Obtención de una dirección IP.

Cada uno de las interfaces de la red TCP/IP debe tener una única dirección IP. Si las comunicaciones TCP/IP están limitadas a una red local, la dirección IP sólo necesita ser única localmente por lo que no es necesario consultar al NIC. Lo recomendable es solicitarlo al NIC por si cambia la política de la empresa y necesiten conectarse con Internet, no siendo necesario cambiar las direcciones. Luego de ello se asigna las direcciones de los hosts.

Se puede asignar las direcciones de los hosts de dos maneras:

- Una dirección a la vez, donde cada host en forma individual tiene asignada una dirección, quizas en forma secuencial dentro de un rango.

Grupos de direcciones, donde bloques de direcciones son asignados a pequeñas organizaciones dentro de toda la organización asignando luego a sus respectivos hosts individuales.

Esta segunda forma será la usada para una red que esté dividida en subredes.

2.11 Obtención de una nombre de dominio.

Similar a la obtención de la dirección IP éste

se solicita a la NIC. También se solicita el dominio in-addr.arpa. Este dominio especial es conocido como dominio inverso puesto que traduce direcciones IP a nombres de dominios.

2.12 Selección de un nombre para el host.

Luego de obtener las direcciones IP se debe escoger los nombres de los hosts que deben ser únicos dentro de la red.La RFC 1178 brinda sugerencias para escoger el nombre. Algunas de ellas son:

- Use palabras reales que sean cortas (8 caracteres o menos), fáciles de deletrear y recordar. El objetivo de usar nombres en vez de direcciones IP es que los nombres son más fáciles de usar.

Evitar el uso de nombre de proyectos, nombre numéricos y jerga técnica. Los proyectos y personas cambian con el tiempo. Especificar un host con el nombre de una persona o proyecto nos obligaría a cambiarlo en el futuro.

- Usar solo caracteres alfanuméricos, no caracteres especiales.
- El nombre debe empezar con una letra.

2.13 Planificación de la ruta.

El enrutamiento es el proceso de selección de un camino através del cual se enviará los datos a un

hosts. Cuando se envia datos a otro hosts de la misma red local, no se usa. El enrutamiento es realizado por un host denominado gateway o router, por lo que una ruta através de él debe ser definida. Hay 2 formas de realizarlo:

- El enrutamiento puede ser manejado por una tabla de rutas estáticas. Las tablas de rutas estáticas son más usados cuando el número de routers es limitado. Las tablas estáticas no son modificadas dinamicamente cada vez que las condiciones de la red cambie, por lo que los cambios en la tabla debe ser realizado manualmente por el administrador de la red. Ambientes complejos requieren una mayor flexibilidad de que provee una tabla de enrutamiento estática.

- El enrutamiento puede ser manejado por una tabla de enrutamiento dinámico que responde a las condiciones cambiantes de la red. Tablas de enrutamiento dinámico son construídas por protocolos de enrutamiento. Protocolos de enrutamiento intercambian información que ellos usan para actualizar la tabla de enrutamiento. El enrutamiento dinámico es usado cuando existen múltiples routers en la red, y cuando más de un router puede alcanzar el mismo destino.

Muchas redes usan una combinación de enrutamiento dinámico y estático. Varios sistemas de la red usan tablas de enrutamiento estático, otros ejecutan protocolos de enrutamiento. Mientras que es frecuente que los host usen tablas de enrutamiento estático y los routers usualmente ejecutan protocolos de enrutamiento.

El administrador de la red es el responsable de decidir que tipo de enrutamiento se usa y de escoger el router por defecto de cada host. Aquí algunas guías para la planificación de enrutamiento:

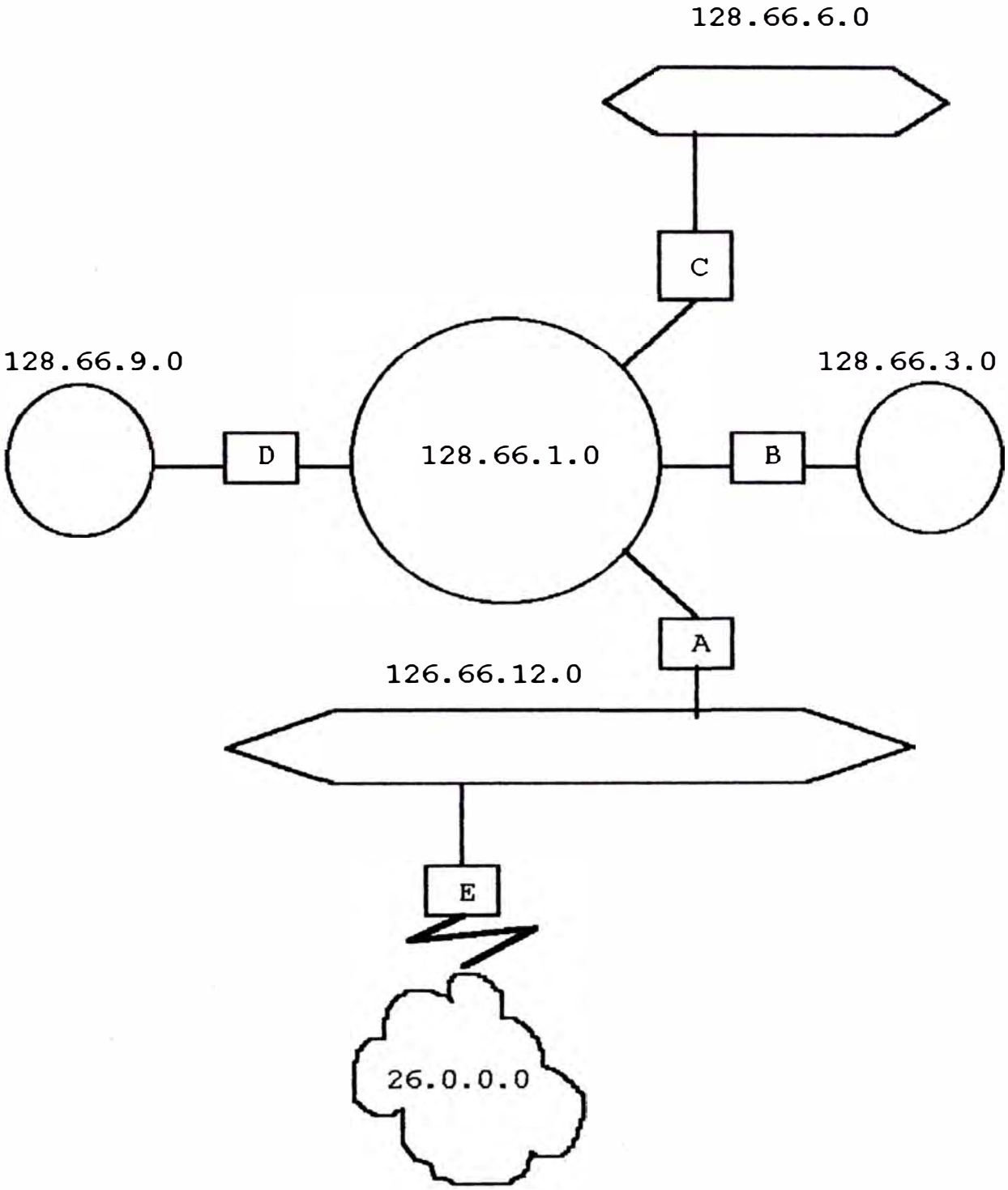
- Una red sin routers a otras redes TCP/IP. En este caso no se necesita ninguna configuración especial de enrutamiento. Si no se está conectado con otras redes TCP/IP , no se necesita routers IP.
- Una red con un único gateway. Si se tiene un solo gateway, no se necesita ejecutar protocolos de enrutamiento. Se especifica el único gateway como el gateway por defecto en la tabla estática de enrutamiento.
- Una red con gateways internos a otros subredes y un único gateway al mundo. Uno puede especificar estáticamente cada ruta a la subred y hacer el gateway al mundo como una ruta por defecto. La decisión se basa en el esfuerzo que concierne el

mantenimiento de una tabla estática versus el tráfico de ejecutar un protocolo de enrutamiento en los hosts y las redes.

- Una red con múltiples gateways al mundo. Si se tiene múltiples gateways para alcanzar el mismo destino, use un protocolo de enrutamiento. Esto permite a los gateways la adaptación de los cambios de la red, brindando acceso redundante a redes remotas.

En la figura 2.3 se muestra una red de clase B con 5 gateways identificados de A a E. Una sub-red central (128.66.1.0) conecta con otras 5 sub-redes. Uno de las subredes tiene un gateways a una red externo clase A. Se podría correr un protocolo de enrutamiento en la sub-red central (128.66.1.0) y tal vez en la subred 128.66.12.0, que está conectado a la red de clase A 26.0.0.0. El enrutamiento dinámico es apropiado debido a que tienen múltiples gateways. Si no tuviesen enrutamiento dinámico, el administrador debería actualizar manualmente cada uno de los gateways cuando ocurriese un cambio en la red. Un error durante la actualización manual podría cortar el servicio de red.

Figura 2.3. Enrutamiento y sub-redes



De otro lado se podría escoger enrutamiento estático para las otras subredes (128.66.3.0, 128.66.6.0 y 128.66.9.0). Estas subredes usan solo un gateway para alcanzar todos sus destinos. En el caso de cambios externos a las subredes no cambia el enrutamiento puesto que esto se realizará através de una única ruta, através del mismo gateway.

Los hosts en estas sub-redes especifican al gateway de la sub-red como la ruta por defecto. Los host de la sub-red 128.66.3.0 especifican a B como el gateway por defecto mientras que los hosts de la sub-red 128.66.9.0 especifican a D como el gateway por defecto.

2.14 Definición de una máscara de sub-red.

Las razones topológicas para hacer sub-redes son:

Superar limitaciones de la distancia. Varios dispositivos de la red tienen estrictas limitaciones de distancia. Por ejemplo la máxima longitud de un cable grueso es 500 mts. , la máxima longitud de un cable delgado es 300 mts.

- Conectar redes físicamente diferentes. Routers IP pueden ser usados para enlazar redes que tienen diferentes e incompatibles tecnologías de red entre niveles.

- Filtrar el tráfico entre redes. El tráfico local permanece en la subred local. Solamente el tráfico para otras redes es dirigido através del gateway.

Adicional a ello, las subredes sirven para propósitos de organización tales como:

- Simplificar la administración de la red. Sub-redes pueden ser usados para delegar la administración de las direcciones , problemas técnicos y otras responsabilidades a pequeñas organizaciones dentro de toda la organización. Esto es una herramienta efectiva de administración para un grupo de técnicos limitado.

Reconocer la estructura de la organización. La estructura de una organización puede requerir una administración independiente de cada red para varias divisiones.

- Aislar el tráfico. Ciertas organizaciones pueden preferir tener un tráfico local aislado para una red que es principalmente accesible solo a miembros de esa organización.

- Aislar problemas potenciales. Si cierto segmento va a ser menos confiable que el resto de la red, sería recomendable hacer una sub-red de ese segmento para prevenir que cualquier falla de esta interfiera en las actividades del resto.

En nuestro caso se escogió una máscara de sub-red 255.255.0.0

2.15 Especificación de la dirección de comunicación general.

La dirección de comunicación general es aquella en la que todos los bits de hosts se ponen en 1. Cuando se envía algún mensaje a esta dirección, ésta es enviado a todos los dispositivos de la red. Para la red desarrollada , en el host sunatx es 150.200.255.255 y la topología de esta red se muestra en la figura 2.4.

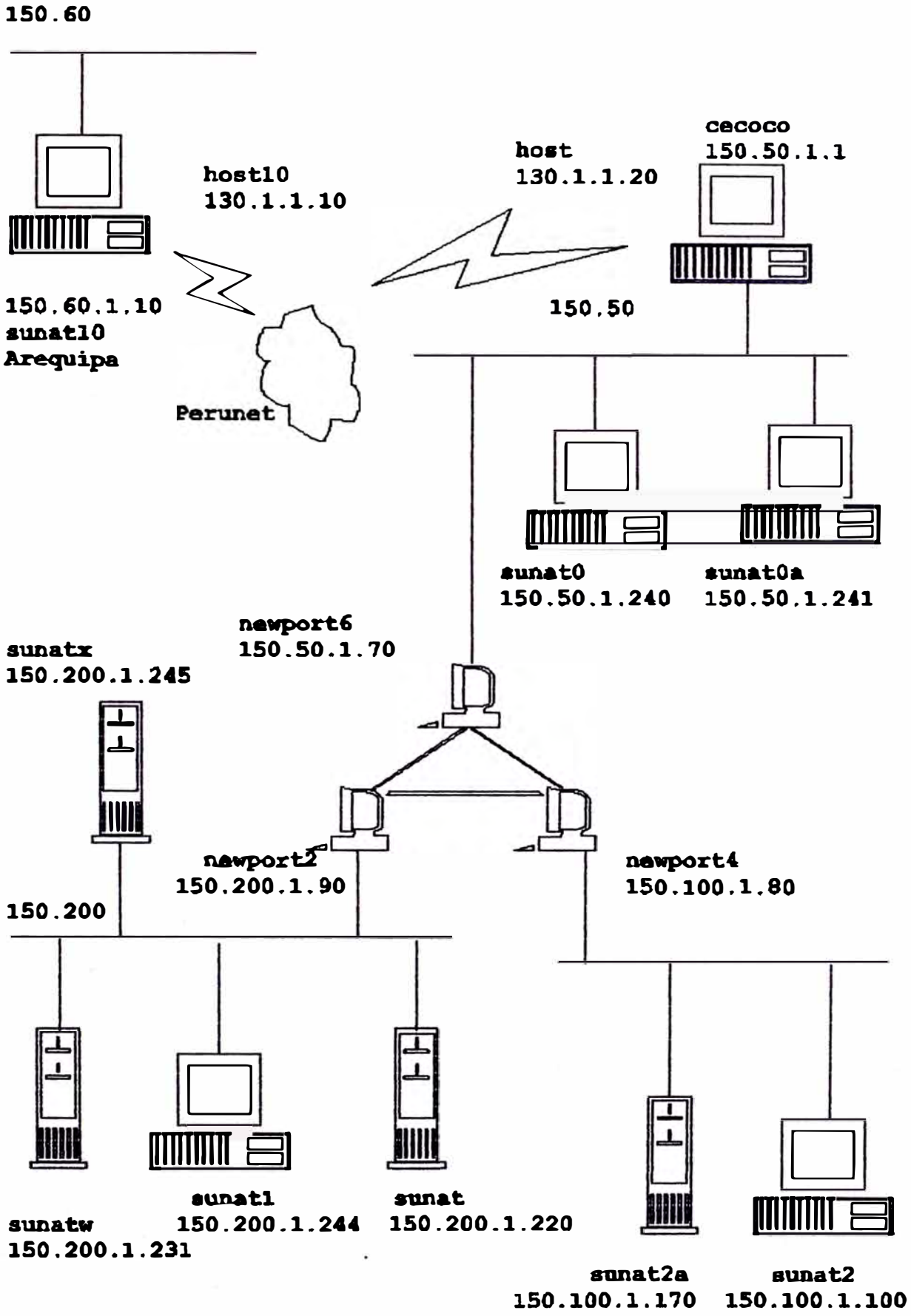
2.16 Realización de hojas de planificación.

Luego de juntar la información básica, el administrador de la red la debe diseminar. Se debe crear una corta lista de información .

La hoja de información tiene los siguientes datos:

- Nombre.
- Dirección IP.
- Máscara de la subred.
- Gateway por defecto.
- Dirección de comunicación general.
- Protocolo de enrutamiento.

Figura 2.4. Red Sunat



Se ha tomado en consideración de no ejecutar protocolos de enrutamiento debido a la cantidad de routers que se cuenta y la estabilidad de la asignación de direcciones, por lo que el mantenimiento de los archivos tablas es eventual. Tenemos las hojas de planificación siguientes:

En el local de la Av. Wilson.

- **Nombre** : sunatx
- **Dirección IP** : 150.200.1.245
- **Máscara de la subred** : 255.255.0.0
- **Gateway por defecto** : 150.200.1.90 newport2
- **Dirección de comunicación general** : 150.200.255.255

- **Nombre** : sunat1
- **Dirección IP** : 150.200.1.244
- **Máscara de la subred** : 255.255.0.0
- **Gateway por defecto** : 150.200.1.90 newport2
- **Dirección de comunicación general** : 150.200.255.255

- **Nombre** : sunat
- **Dirección IP** : 150.200.1.220
- **Máscara de la subred** : 255.255.0.0
- **Gateway por defecto** : 150.200.1.90 newport2

- **Dirección de comunicación general** : 150.200.255.255

- **Nombre** : sunatw
- **Dirección IP** : 150.200.1.231
- **Máscara de la subred** : 255.255.0.0
- **Gateway por defecto** : 150.200.1.90 newport2
- **Dirección de comunicación general** : 150.200.255.255

En el local del distrito de Miraflores.

- **Nombre** : sunat2
- **Dirección IP** : 150.100.1.100
- **Máscara de la subred** : 255.255.0.0
- **Gateway por defecto** : 150.100.1.80 newport4
- **Dirección de comunicación general** : 150.100.255.255

- **Nombre** : sunat2a
- **Dirección IP** : 150.100.1.170
- **Máscara de la subred** : 255.255.0.0
- **Gateway por defecto** : 150.100.1.80 newport4
- **Dirección de comunicación general** : 150.100.255.255

En el local del distrito de San Isidro

- **Nombre** : sunat0
- **Dirección IP** : 150.50.1.240
- **Máscara de la subred** : 255.255.0.0
- **Gateway por defecto** : 150.50.1.1 newport6
- **Dirección de comunicación general** : 150.50.255.255

- **Nombre** : sunat0a
- **Dirección IP** : 150.50.1.241
- **Máscara de la subred** : 255.255.0.0
- **Gateway por defecto** : 150.50.1.1 newport6
- **Dirección de comunicación general** : 150.50.255.255

En el Departamento de Arequipa

- **Nombre** : sunat10
- **Dirección IP** : 150.60.1.10
- **Máscara de la subred** : 255.255.0.0
- **Gateway por defecto** : 130.1.1.10 Host10
- **Dirección de comunicación general** : 150.60.255.255

Con las hojas de planificación se logra construir los archivos /etc/hosts y /etc/networks como se muestra en los archivos 2.3 y 2.4.

Archivo 2.3. /etc/hosts

```
#
#     WIN-TCP HOST TABLE
#
#Internet   Host    Aliases          # Comments
#

127.0.0.1       me       loopback localhost
150.50.1.240    sunat0
150.50.1.1      cecoco     # HOST DE COMUNICACIONES-NCR
150.50.1.241    sunat0a
150.50.1.243    sunat0b
150.50.1.244    sunat0c
150.50.1.242    sunatiat
150.50.1.14     sunat14
150.75.1.100    sunatcc    # CENTRO CIVICO  - NCR
150.100.1.100    sunat2    # HOST MIRAFLORES - NCR
150.100.1.110   sunat2b    # SERVER ( AST Fiscalizac. )
150.100.1.170    sunat2a   # HOST MIRAFLORES - PRICO NCR
150.200.1.244    sunat1    # HOST LIMA - DEC
150.200.1.220    sunat     # HOST LIMA - DEC
150.200.1.245    sunatx    # HOST DESARROLLO LIMA - NCR
150.200.1.231    sunatw    # HOST DESARROLLO LIMA - NCR
#########################################################
#######
#HOSTS PROVINCIAS

150.60.1.10      sunat10   # AREQUIPA - HOST
150.60.1.11     sunat10a   # AREQUIPA
150.54.1.1       sunat4    # PIURA - HOST
150.54.1.2       sunat4a   # PIURA
150.61.10.4     sunat11    # CHICLAYO - HOST
150.61.10.3     sunat11a   # CHICLAYO
150.56.10.22    sunat6     # TRUJILLO - HOST
150.56.10.6     sunat6a    # TRUJILLO
150.58.1.10     sunat8     # ICA - HOST
150.58.1.20     sunat8a    # ICA
150.62.1.1      sunat12    # TACNA - HOST
150.62.1.2      sunat12a   # TACNA
150.59.1.100    sunat9     # HUANCAYO - HOST
150.59.1.120    sunat9a    # HUANCAYO
150.57.1.110    sunat7     # CUZCO - HOST
150.57.1.100    sunat7a    # CUZCO
150.55.1.110    sunat5     # IQUITOS - HOST
150.55.1.100    sunat5a    # IQUITOS - HOST
#ROUTERS
150.50.1.70     newport6   # SAN ISIDRO
150.100.1.80    newport4   # MIRAFLORES
```

Continuación de Archivo 2.3. /etc/hosts

```
150.200.1.90    newport2   # LIMA
150.75.1.60     newport8   # CENTRO CIVICO

#SERVERS
150.50.3.1      server1    # SOTANO
150.50.3.2      server2    # PISO 5
150.50.3.3      server5    # PISO 5

#TARJETAS X25
130.1.1.20      host       # LIMA
130.1.1.10       host10    # AREQUIPA
130.1.1.4       host4      # PIURA
130.1.1.11       host11    # CHICLAYO
130.1.1.6       host6      # TRUJILLO
130.1.1.9       host9      # HUANCAYO
130.1.1.5       host5      # LORETO
130.1.1.7       host7      # CUSCO
130.1.1.12      host12     # TACNA
130.3.1.8       # TACNA
#SLIP
130.4.1.20      host_h
130.3.1.21      host_slip
130.2.1.22      host_v
```

Archivo 2.4. /etc/networks

```
#
# Internet networks (reordered for local efficiency)
#
Loopback  127        software-loopback-net
sunat_san 150.50
sunat_cc         150.75              # CENTRO CIVICO
sunat_mir       150.100              # MIRAFLORES
sx25            130.1                # RED X25
net30           150.30               # PRUEBA
net40           150.40               # PRUEBA
sunat           150.200              # WILSON
net10           150.60               # AREQUIPA
net4            150.54               # PIURA
net11           150.61               # CHICLAYO
net6            150.56               # TRUJILLO
net9            150.59               # HUANCAYO
net5            150.55               # IQUITOS
net7            150.57               # CUZCO
net12           150.62               # TACNA
net8            150.58               # ICA
net_ucayali     150.70               # UCAYALI
slip_net_ica    130.3                # SLIP
rcp_net         161.132.37
```

2.17 El demonio Internet.

La configuración del kernel trae los servicios básicos de transporte y de datagrama IP dentro del UNIX. Varios protocolos son explícitamente iniciados por archivos de inicio. Esta técnica es usada por RIP y DNS. Los demonios (procesos que no están asociados a terminales y ejecutan tareas periódicas) que sirven a estos protocolos, routed y named respectivamente, son corridos desde un archivo de inicio.

Otros demonios de la red no son iniciados individualmente. Estos demonios son iniciados por un super-servidor que escucha los requerimientos de servicio de la red e inicia el demonio apropiado para procesar el requerimiento. Este super-servidor se llama el demonio internet.

El demonio internet (inetd) comienza a correr a la hora de inicio desde un file. Cuando comienza, inetd lee su configuración desde el archivo /usr/etc/inet.conf, el cual contiene los nombres de los servicios que inetd escucha y ejecuta.

Los campos de una entrada del archivo inet.conf son:

Nombre Indica el nombre del servicio.

Tipo — El tipo del servicio de distribución de datos que usa, es tambien llamado tipo de socket. Los tipos de socket más comunmente usados son:

- stream — El servicio de distribución de corriente es brindado por TCP.
- dgram — El servicio de distribución de paquetes (datagrama) es brindado por UDP.
- raw — Servicio directo de datagramas IP.

Protocolo — Es el nombre del protocolo y es dado en el archivo /etc/protocols. Su valor usualmente es "tcp" o "udp". Por ejemplo el protocolo FTP usa TCP como protocolo en el nivel de transporte.

Espera — El valor de este campo puede ser "wait" o "nowait". Usualmente los servidores de tipo datagrama requieren "wait" y los servidores de tipo stream requieren "nowait". Si el estado es "wait", inetd esperará para que el servidor libere el socket

antes de empezar a escuchar más requerimientos para el socket. Si el estado es "nowait", inetd puede inmediatamente empezar a escuchar más requerimientos de conección para el socket. Servidores con estado "nowait" usan sockets dinámicos.

uid — Es el nombre del usuario bajo el que corre el servidor. Normalmente es root. Hay dos excepciones. El servicio finger que se ejecuta como usuario nobody o daemon, y el servicio uucp que se ejecuta como usuario uucp.

server — Es el nombre completo del programa servidor que es iniciado por inetd. Es más eficiente para inetd brindar pequeños servicios directamente en vez de iniciar servidores separados para estas funciones. Para estos pequeños servicios, el valor del campo del servidor es "internal", que indica que el servicio es uno interno de inetd.

Argumentos — Estos son los argumentos de la línea

de comando que son pasados al programa servidor cuando son invocados. Esta lista siempre comienza con argv[0] (El nombre del servidor).

2.18 El comando ifconfig.

Configura o verifica los valores de configuración de las interfaces de la red. Es usado para poner la dirección IP, la máscara de la sub-red y la dirección de comunicación general de cada interface. Los argumentos que brindan la información básica son:

interface — El nombre de la red de interface que se desee configurar.

dirección — Es la asignada a la interface. Se puede ingresar como dirección, la dirección Ip o el nombre del host. Es preferible la dirección IP porque si se usa el nombre de host, ifconfig debe relacionar el nombre del host a la dirección antes de que la dirección sea asignada a la interface. Si se decide usar el nombre del host, se coloca el nombre del host y su dirección en el archivo

/etc/hosts.

netmask mask — Es la máscara de la sub-red. Se ignora en el caso de que no se haya dividido la red en sub-redes.

broadcast — La dirección de comunicación general es aquella en la cual los bits del host están en uno.

Para determinar todos las interfaces disponibles en el sistema, se usa el comando netstat. Ejemplo:

#netstat -ai

Name	Mtu	Network	Address	Ipkts	Ierrs	Opkts	Oerrs
en0	1492	sunat mir	sunat2	2919410	0	3543105	0
lo0	4096	Loopback	me	1170	0	1168	0

Tenemos los siguientes campos:

Nombre — Muestra el nombre actual asignado a la interface. Este es el nombre que se da a ifconfig para identificar la interface. Un asterisco (*) indica que no esta habilitado (no esta "up").

Mtu — Máxima unidad de transmisión (Maximun Transmission Unit) de una trama, que puede ser transmitida por la interface sin ser fragmentada.

Net/Dest	La Red/Destino (Network/Destination) muestra la red o el host destino al que la interface accede. Usualmente tiene la dirección Ip de una red. Contiene la dirección de un host si la interface ha sido configurada punto a punto. Un enlace punto a punto es una conección directa entre 2 computadoras.
Dirección	La dirección IP muestra la dirección IP asignada a la interface.
Ipkts	El campo de paquetes entrantes muestra la cantidad de paquetes que la interface ha recibido.
Ierrs	El campo de errores entrantes muestra la cantidad de paquetes dañados ha recibido.
Opkts	El campo de paquetes salientes muestra la cantidad de paquetes que ha enviado através de la interface.
Oerrs	El campo de errores salientes muestra la cantidad que han causado un error de condición.
Collis	Muestra la cantidad de colisiones Ethernethan sido detectados por esta

interface.

Queue — Muestra la cantidad de paquetes en espera de ser transmitidos através de esta interface. Normalmente es 0.

2.19 TCP/IP sobre una línea serial.

TCP/IP puede correr sobre diferentes medios físicos Estos medios pueden ser cables Ethernet, como en una red local, o por circuitos telefónicos como en una red de area vasta. Una interface serial es una interface que envía datos como series de bits através de una sola línea, al contrario de una interface paralela que envía bits en paralelo através de varias líneas simultaneamente.

Las líneas seriales son usadas para crear redes de área vasta. Con la necesidad de estandarizar estas comunicaciones se crearon 2 protocolos de línea serial: línea serial IP (Serial Line IP SLIP) y protocolo punto a punto (Point-to-Point Protocol PPP)

2.20 Protocolos seriales.

SLIP que fue creado primero que PPP, permite a los hosts aislados enlazarse vía TCP/IP sobre una red telefónica. Define un mecanismo de fragmentación de los datagramas para su transmisión. SLIP envía datagramas através de la línea serial como serie de

bytes, usando caracteres especiales para marcar cuando estos deben ser agrupados como un datagrama. SLIP define 2 caracteres especiales para este propósito:

El caracter SLIP END, un solo byte con valor decimal 192. Cuando el SLIP receptor encuentra un caracter END, sabe que el datagrama se completó y puede ser enviado a IP.

El caracter SLIP ESC, un solo byte con valor decimal 219 que es usado para escapar de los caracteres de control del SLIP. Si el SLIP emisor encuentra un byte de valor a un caracter SLIP END o a un caracter SLIP ESC en el datagrama que está enviando, convierte el caracter en una secuencia de 2 caracteres. La secuencia de 2 caracteres son ESC 220 para el caracter END y ESC 221 para el caracter ESC (No es el caracter ASCII ESC). Cuando el SLIP receptor encuentra la secuencia de 2 bytes, lo convierte nuevamente a los valores de un solo byte. Este procedimiento previene al SLIP receptor de interpretaciones incorrectas de un byte dato como final del datagrama.

SLIP es descrito en RFC 1055, " Transmisión No Estándar de Datagramas IP através de Líneas Seriales: SLIP ". Como indica el nombre de RFC, SLIP

no es un estándar IP. La RFC no propuso un estándar, documentó un protocolo existente. La RFC identifica las deficiencias en SLIP, que caen en dos categorías:

- El protocolo SLIP no define ninguna información de control de enlace que pudiera ser utilizado para controlar dinámicamente las características de conección. Por lo que SLIP asume ciertas características de enlace y solo puede ser usado cuando ambos hosts conocen la dirección de cada uno y solo cuando los datagramas IP son transmitidos.

SLIP no compensa cuando las línea telefónicas tienen baja velocidad y son ruidosas. El protocolo no brinda un mecanismo de corrección de errores o compresión de datos.

Para muchas aplicaciones estos problemas carecen de importancia debido a que interesa el envio de datagramas IP. Los modems tienen su propio mecanismo de compresión y corrección de errores. Con estas condiciones dadas, SLIP es considerado adecuado para la conección entre 2 hosts aislados.

Para superar las deficiencias de SLIP, PPP fue desarrollado como un estándar Internet. Dos RFCs que documentan a PPP son el RFC 1171, " PPP para la Transmisión de Datagramas Multiprotocolos através de

Enlaces Punto a Punto " y el RFC 1172 " Opciones Iniciales de Configuración de PPP ".

PPP supera las deficiencias del SLIP con un protocolo de 3 niveles:

- Protocolo del nivel de enlace de Datos.- Es una modificación de la versión de Control de Enlace de Datos de Alto Nivel (High Level Data Link Control HDLC). PPP modifica HDLC agregando un campo que permite a PPP pasar el tráfico por múltiples protocolos de nivel de red. HDLC es un protocolo internacional estándar que envía datos en forma segura y síncrona através de líneas seriales de comunicación. PPP también usa una propuesta de transmisión através de líneas asíncronas. Por lo que PPP puede garantizar la distribución confiable através de cualquier tipo de líneas seriales.

Protocolo de control de enlace.- (Link Control Protocol LCP) brinda información de control. Es usado para establecer la conección, configuración de parámetros, chequeo de la calidad del enlace y terminar la conección. Durante la configuración de parámetros, LCP configura la compresión. LCP fue desarrollado especificamente para PPP.

- Protocolos de control de la red.- Son protocolos individuales que brindan información de

configuración y control para los protocolos del nivel de red. Cada protocolo de red (DECNET, IP, OSI, etc.) tienen su propio protocolo de Control de Red. El Protocolo de Control de Red definido en los RFCs 1171 y 1172 es el Protocolo de Control Internet (Internet Control Protocol IPCP).

PPP es un protocolo más elaborado que el SLIP pero más difícil para implementar y no tan ampliamente disponible.

2.21 Selección de un protocolo serial.

PPP es preferido porque es un estándar Internet por lo que asegura su operatividad entre sistemas de una amplia variedad de proveedores. Las características que brinda lo hacen una buena alternativa como un protocolo libre (no definido a una determinada marca) para conectar routers através de líneas seriales. Sin embargo, SLIP por ser el primero en disponibilidad como protocolo de línea serial y por su implementación simple , tiene mayor disposición para diferentes clase de hardware que PPP.

2.22 Instalación del protocolo SLIP.

Para la instalación del protocolo SLIP se deberá ingresar al archivo netconfig y agregar una cadena. En el se indicará la línea tty que será

usado por slip , por ejemplo ttyla, la velocidad en baudios y las direcciones de las interfaces origen y destino. Luego de ello se reconstruirá el kernel.

SLIP ya está instalado por lo que se configurará la interface de red del SLIP para ello usaremos el comando slattach.

La sintaxis de slattach es la siguiente:

#slattach device dir IP_origen dir IP destino velocidad

El enlace con el computador de la oficina zonal de huanuco se realiza através del host sunat2b ubicado en la Intendencia Regional I (Miraflores) para ello se da el comando de la siguiente manera:

slattach ttyla 130.4.1.21 130.4.1.20 4800 &

Este comando identifica el dispositivo serial (ejemplo /dev/ttyla) en vez de la interface de la red IP (ejemplo sl01). Sin embargo al ejecutar el comando netstat para verificar el estado del interface SLIP, éste muestra el nombre de la interface. Para liberar el dispositivo serial se ejecuta el comando sldetach. El comando slattach es puesto en el archivo /etc/tcp cuando el netconfig

instala el SLIP.

El comando slattach espera que la conección física al sistema remoto exista cuando slattach es invocado. La conección física puede ser una conección directa, una línea liberada o una línea dial.

2.23 Configuración de rutas.

El enrutamiento permite al tráfico de una red local alcanzar su destino en cualquier punto. Todos los sistemas enrutan los datos pero no todos ejecutan protocolos de enrutamiento. El enrutamiento es el acto por el que se direcciona datagramas basados en información de una tabla. Protocolos de enrutamiento son programas que intercambian información que es usada para construir las tablas. Existen 3 modos de configuración de rutas y son:

2.23.1 Enrutamiento mínimo.

Una red que no tiene ingreso directo, completamente aislada, a otras redes TCP/IP y no ha sido dividido en subredes requiere un enrutamiento mínimo. Una tabla de enrutamiento mínimo es construído por el comando ifconfig cuando la interface está configurado.

2.23.2 Enrutamiento estático.

Una red con un número limitado de gateways para

conectarse a otras redes TCP/IP puede ser configurada con un enrutamiento estático. La tabla de enrutamiento estático es construído manualmente por el administrador del sistema usando el comando route. Tablas de enrutamiento estático no varían de acuerdo a los cambios del sistema, por lo que deberían ser usados donde las rutas no cambien. Pero cuando los destinos remotos pueden ser alcanzados através de una sola ruta, es la mejor alternativa.

2.23.3 Enrutamiento dinámico.

Una red con más de una posible ruta para el mismo destino debería usar un enrutamiento dinámico. Una tabla de enrutamiento dinámico es construída de la información que es intercambiada por los protocolos de enrutamiento. Los protocolos son diseñados para distribuir información que dinámicamente varía las rutas que reflejan las condiciones cambiantes de la red. Los protocolos de enrutamiento manejan de mejor manera y más rápido complejas situaciones de enrutamiento de lo que puede hacer un administrador de sistema. Los protocolos de enrutamiento no solo están diseñados para cambiar a la mejor ruta alternativa cuando la principal está inoperativa sino también para

decidir cual es la mejor ruta. En una red donde existen múltiples caminos a un mismo destino, un protocolo de enrutamiento debe ser usado.

2.24 Construcción de una tabla de enrutamiento estático.

Rutas através de gateways externos deben ser agregados a la tabla de enrutamiento para alcanzar hosts remotos. Una forma de hacerlo es construyendo una tabla de enrutamiento estático con el comando route.

Usando el comando UNIX route se agrega o elimina manualmente entradas en la tabla de enrutamiento.

```
#route add [host|net] destino gateway metric
```

El primer argumento luego de route es la palabra add o delete con lo que se le indica que agregue una nueva ruta o elimine una ya existente. Una de estas palabras debe estar presente.

El siguiente valor es host o net, luego es la dirección destino que es la dirección que se desea alcanzar por esta ruta. La dirección destino puede ser especificadó como una dirección IP, un nombre de red del archivo /etc/networks, un nombre de host del archivo /etc/hosts o por la palabra default. Si la

palabra default es usada para la dirección destino, route crea una ruta por defecto (dirección con la dirección IP 0.0.0.0). La ruta por defecto es usado cuando no está especificado una ruta para un destino. Si la red tiene solo un gateway, se debe usar la ruta por defecto para dirigir todo el tráfico a redes remotas através de ese gateway.

Luego tenemos la dirección del gateway. Esto es una dirección IP de un gateway externo através del cual los datos son enviados a la dirección destino. La dirección debe ser la dirección de un gateway conectado directamente a la red. Las rutas TCP/IP especifican el siguiente salto (next-hop) en el camino hacia el destino remoto. Este siguiente salto debe ser directamente accesible al host local por lo que debe estar directamente conectado a la red.

El último argumento de la línea de comando es la métrica de enrutamiento. La métrica de enrutamiento no es usado cuando las rutas son eliminadas, pero si es requerido cuando la ruta es agregada. A pesar de ser requerido, route solo usa la métrica para decidir si es una ruta através de una interface directamente conectada a la red o es una ruta através de un gateway externo. Si la métrica es 0, la ruta está instalada como una ruta

través de una interface local y el flag G que se visualiza ejecutando el comando netstat -ı no aparece. Si el valor de la métrica es mayor que 1, la ruta está instalada con el flag G, la dirección del gateway es asumida como la dirección de un gateway externo. El enrutamiento estático no tiene otro uso de la métrica. El enrutamiento dinámico tiene un uso real de la variación de los valores de la métrica.

Se agregará las rutas estáticas en la red de la Intendencia de Miraflores, en la cual como tenemos un solo router para alcanzar a las redes de las demás regionales, lo derivamos hacia ella. Estas rutas las podemos definir en el momento de inicialización del sistema por lo que en cada uno de los hosts que conforman la red (sunat2, sunat2a , sunat2b) lo ponemos en un script llamado S61route ubicado en el directorio /etc/rc2.d el cual se ejecutará por le sistema en el momento que ingrese en el estado 2 que es el de multiusuario.

```
/usr/etc/route add net sunat     newport4 1
/usr/etc/route add net sunat_mir newport4 2
/usr/etc/route add net sunat_san newport4 2
/usr/etc/route add net sunat_cc  newport4 1
/usr/etc/route add net sx25      newport4 1
```

2.25 Protocolos de enrutamiento.

Todos los protocolos de enrutamiento realizan las mismas funciones básicas. Determinan la mejor ruta a cada destino y distribuyen información de enrutamiento entre los sistemas de una red. La forma como realizan estas funciones y toman decisiones acerca de las rutas más adecuadas es lo que los diferencia unas de otras

2.25.1 Protocolos de enrutamiento internos.

Los protocolos de enrutamiento están divididos en 2 grupos generales: protocolos internos y externos. Un protocolo interno es usado dentro de una red independiente. En TCP/IP estos sistemas de red independientes tienen el nombre de sistemas autónomos. Dentro de un sistema autónomo, la información de enrutamiento es intercambiada usando un protocolo interno escogido por el administrador. Existen varios protocolos internos para escoger.

El más común es el protocolo de información de enrutamiento (Routing Information Protocol RIP), está incluído como parte del software de UNIX. Es apropiado para redes de área local.

RIP selecciona la ruta con la menor cantidad de saltos (métrica) como la mejor. El número de

saltos representa el número de gateways através del cual debe pasar los datos para llegar a su destino. La menor cantidad de gateways usados es el camino más corto, y el camino más corto es el mejor. Este método de selección de la mejor ruta es llamado el algoritmo del vector de distancia.

El camino más largo que acepta RIP es 15 saltos, si la métrica de una ruta es mayor que 15, el destino se considera inalcanzable y se desecha la ruta. Por este motivo RIP no es apropiado para sistemas autónomos grandes donde los datos deben pasar por más de 15 gateways. Además, la idea de que el camino más corto es el mejor, no toma en consideración la congestión o el retardo en la ruta, por lo que se desarrollaron otros protocolos internos para superar estas limitaciones.

Hello es un protocolo interno que fue desarrollado para usar el retardo como un factor de decisión para la selección de la mejor ruta. Delay es el período de tiempo que toma a un datagrama para realizar un viaje de ida y vuelta entre la fuente y el destino. Un paquete Hello tiene el tiempo cuando ha sido enviado. Cuando el paquete llega a su destino, el sistema receptor, el sistema receptor calcula el tiempo que ha

demorado. Hello no es tan comunmente usado.

2.25.2 Protocolos de enrutamiento externos.

Protocolos externos son usados para intercambiar información de enrutamiento entre sistemas autónomos. La información de enrutamiento contiene las redes que deben alcanzar para llegar hasta un determinado sistema autónomo.

Uno de los protocolos externos comunmente usado es el Protocolo Externo de Gateway (Exterior Gateway Protocol EGP).

2.26 Protocolo de información de enrutamiento.

RIP es distribuído con muchos sistemas UNIX, y es ejecutado por el demonio routed. El demonio routed construye dinamicamente la tabla de enrutamiento basado en las actualizaciones RIP.

Cuando routed empieza, él envía un requerimiento para las actualizaciones de de enrutamiento, luego espera por las respuestas de su requerimiento. Cuando un sistema está configurado para ejecutar el protocolo RIP, recibe el requerimiento y responde con un paquete actualizado basado en la información de su tabla de enrutamiento. El paquete actualizado contiene las direcciones de los destinos y sus respectivas métricas de su tabla de enrutamiento. Los paquetes

actualizados no solo son enviados cuando son requeridos, se envían periódicamente para mantener la veracidad de la información de enrutamiento.

Cuando una actualización RIP es recibida, routed toma la información de la respuesta y actualiza la tabla de enrutamiento. Si la actualización contiene una ruta a un destino que no existe en la tabla de enrutamiento local, esta nueva ruta será añadido. Si la actualización contiene una ruta que su destino ya está en la tabla local, la nueva ruta será usada solo si tiene un costo bajo. El costo de una ruta es determinado por la suma del costo en alcanzar el gateway que envió la actualización a la métrica contenida en el paquete de actualización. Si la métrica total es menor que la métrica de la ruta actual, la nueva ruta será usada.

RIP también elimina rutas de la tabla de enrutamiento. Existen dos maneras en las que esto se realiza. Primero, si el gateway a un destino indica que el costo de la ruta es mayor que 15, la ruta es eliminada. Segundo, RIP asume que un gateway que no envía actualizaciones está muerto (inoperativo). Todas las rutas através de ese gateway serán eliminadas si las actualizaciones no son recibidas

por un detreminado período de tiempo. Este período de tiempo es usualmente de 30 segundos. Si no se recibe actualizaciones por espacio de 180 segundos, todas las rutas de ese gateway serán eliminadas de la tabla de enrutamiento.

Para ejecutar RIP usando el demonio de enrutamiento (routed) se deberá ejecutar el siguiente comando:

```
#routed
```

CAPITULO III
CONFIGURACION DE SERVICIOS DE RED

3.1 Aplicaciones de red.

Existen diferentes aplicaciones de red las cuales brindan servicios a los usuarios para los propósitos de la red.

Entre ellos tenemos los comandos r que son un conjunto de aplicaciones de red propio de UNIX, comparable con ftp y telnet. Los más importantes son:

rlogin El login remoto brinda un ingreso interactivo a hosts remotos. Su función es similar a telnet.

rcp La copia remota permite que los archivos sean copiados de un sistema a otro sistema remoto. Su sintaxis es similar al del comando cp excepto que el camino del archivo debe incluir el nombre del host remoto. rcp es usualmente comparado con ftp. Ambos mueven archivos entre hosts de una red, pero ftp corre como un programa interactivo con varios subcomandos,

mientras rcp se ejecuta en una simple línea de interface.

rsh El shell remoto pasa un comando al host remoto para ejecutarlo. La salida y error estándar de una ejecución remota son retornados al host local. No hay paralelo de rsh en los protocolos TCP/IP.

La seguridad de la ejecución en hosts remotos de los comandos r se consigue configurando los archivos /etc/hosts.equiv y $HOME/.rhosts. En lugar de la verificación de password, estos comandos usan su propio sistema basados en host y usuarios de confianza. Estos usuarios de confianza en hosts de confianza son permitidos de ingresar en el sistema local sin solicitarles un password. Hosts de confianza son llamados " hosts equivalentes" porque el sistema asume que los usuarios que han sido permitidos de ingresar a un host de confianza deberían tener el ingreso similar en el host local. El sistema asume que las cuentas de los usuarios con el mismo nombre en ambos hosts pertenecen al mismo usuario. Este sistema de verificación requiere base de datos que definan a los hosts de confianza y a los usuarios de confianza. Las bases de datos usados

para configurar los comandos r son:

/etc/hosts.equiv, que defiene a los hosts y usuarios de confianza en todo el sistema.

-.rhosts, que define los hosts y usuarios de confianza para una cuenta de un usuario individual.

3.2 El archivo /etc/hosts.equiv.

El archivo /etc/hosts.equiv definen los hosts y usuarios que están permitidos de ejecutar los comandos r en el host local. Este archivo puede definir hosts y usuarios que están explicitamente negados de un ingreso seguro. Esto no significa de que estén negados de ingresar, sino que al realizarlo se les solicitará un password.

El formato básico de las entradas en el archivo /etc/hosts.equiv es:

[+|-][nombre_de host][nombre_de_usuario]

Si un host se le ha otorgado equivalencia con el local, los usuarios que hayan ingresado a ese host podrán ingresar con cuentas del mismo nombre en el host local sin solicitarles password. El nombre de usuario (opcional) es el nombre del usuario que puede ingresar a todas las cuentas de los usuarios sin solicitarle password, además de

poder ingresar a la cuenta con el mismo nombre.

El nombre_de_host puede estar precedido por un signo menos (-) que indicaría en forma explícita que aquel host no es un host equivalente, por lo que los usuarios de ese host deberán siempre ingresar un password para usar los comandos r. En el caso de que el signo menos preceda a un usuario, éste será solicitado por un password cada vez que use algún comando r. Tomando esa consideración se configura el archivo /etc/hosts.equiv como se muestra en el archivo 3.1

3.3 El archivo .rhosts.

El archivo .rhosts otorga o niega el acceso a los comandos r sin requerimiento de password a una cuenta de un usuario específico. Está ubicado en el directorio hogar del usuario y contiene entradas que definen hosts y usuarios de confianza. Las entradas en el archivo .rhosts usa exactamente el mismo formato que las entradas en el archivo hosts.equiv, y funciona de la misma manera. La diferencia radica en el alcance del acceso otorgado por las entradas de los 2 archivos. En el archivo .rhosts, las entradas permiten o niegan a la cuenta de un solo usuario, mientras que las entradas del archivo de control hosts.equiv lo realizan sobre todo un

sistema.

Esta diferencia puede ser mostrada en el siguiente ejemplo. Tengamos la siguiente entrada:

sunat0 admprico

Esta entrada en el archivo hosts.equiv del host sunat2 nos indica que el usuario admprico del host sunat0 puede ingresar a cualquier cuenta en sunat2 sin requerimiento de password. La misma entrada en el archivo .rhosts del directorio hogar del usuario manprico permite que admprico de sunat0 realice un rlogin en sunat2 sin requerimiento de password, pero no le permite ingresar a otras cuentas sin antes pedirle un password.

Se usa el archivo .rhosts para establecer una equivalencia entre diferentes cuentas que le pertenecen a un usuario. La entrada mostrada arriba se puede realizar si las cuentas manprico y admprico pertenece a una misma persona.

Cuando ingresa un usuario, el archivo /etc/hosts.equiv es buscado primero, seguido luego por el archivo .rhosts del usuario en caso que exista. La primera similitud explícita determina si se permite un ingreso sin requerimiento de password

o no se permite.

Cuando un usuario intenta ingresar al sistema vía comandos r, el archivo /etc/hosts.equiv no es verificado, solo el archivo /.rhosts es consultado. Esto permite un ingreso de un usuario root remoto más controlado. Si el archivo /etc/hosts.equiv fuera usado para el ingreso de un usuario root, las entradas que permiten un ingreso de confianza a los hosts daría a los usuarios root de estos hosts remotos, los privilegios de root. De esta manera uno puede ingresar hosts de confianza sin preocuparse que los usuarios root ingresen como usuario root en el host local.

Archivo 3.1. /etc/hosts.equiv de sunat0

```
host10    rbcon101
host10    rbcon102
host11    rbcon111
host11    rbcon112
host12    rbcon121
host12    rbcon122
host4    rbcon041
host4    rbcon042
host5    rbcon051
host5    rbcon052
host6    rbcon061
host6    rbcon062
host7    rbcon071
host7    rbcon072
host8    rbcon081
host8    rbcon082
host9    rbcon091
host9    rbcon092
sunat      conruc10
sunat      conruc12
sunat      conruc13
sunat      conruc18
sunat      conruc19
sunat      conruc20
sunat      conruc24
sunat      conruc25
sunat      conruc27
sunat      conruc28
sunat      conruc29
sunat      conruc30
sunat      conruc31
sunat      conruc32
sunat      conruc33
sunat      conruc34
sunat      conruc35
sunat      conruc36
sunat      conruc37
sunat      conruc38
sunat      conruc39
sunat      conruc5
sunat      oper1
sunat      rbcons16
sunat      rbcons19
sunat      rbcons37
sunat      rbcons38
```

Continuación de Archivo 3.1 /etc/hosts.equiv de sunat0

```
sunat     rbcons39
sunat     rbcons4
sunat     rbcons40
sunat     rbcons41
sunat     rbruc05
sunat     rbruc06
sunat     rbruc48
sunat     rbruc51
sunat     rbruc56
sunat2    conruc15
sunat2    conruc22
sunat2    conruc26
sunat2    conruc4
sunat2    conruc7
sunat2    conruc8
sunat2    conruc40
sunat2    rbcons1
sunat2    rbcons10
sunat2    rbcons11
sunat2    rbcons12
sunat2    rbcons13
sunat2    rbcons14
sunat2    rbcons15
sunat2    rbcons16
sunat2    rbcons17
sunat2    rbcons18
sunat2    rbcons2
sunat2    rbcons20
sunat2    rbcons21
sunat2    rbcons22
sunat2    rbcons23
sunat2    rbcons24
sunat2    rbcons26
sunat2    rbcons27
sunat2    rbcons28
sunat2    rbcons29
sunat2    rbcons3
sunat2    rbcons30
sunat2    rbcons31
sunat2    rbcons32
sunat2    rbcons33
sunat2    rbcons34
sunat2    rbcons35
sunat2    rbcons36
sunat2    rbcons42
```

Continuación de Archivo 3.1 /etc/hosts.equiv de sunat0

```
sunat2    rbcons5
sunat2    rbcons6
sunat2    rbcons8
sunat2    rbcons9
sunat2    rbruc01
sunat2    rbruc02
sunat2    rbruc03
sunat2    rbruc04
sunat2    rbruc07
sunat2    rbruc08
sunat2    rbruc09
sunat2    rbruc10
sunat2    rbruc11
sunat2    rbruc12
sunat2    rbruc13
sunat2    rbruc14
sunat2    rbruc15
sunat2    rbruc16
sunat2    rbruc17
sunat2    rbruc18
sunat2    rbruc19
sunat2    rbruc20
sunat2    rbruc21
sunat2    rbruc22
sunat2    rbruc23
sunat2    rbruc24
sunat2    rbruc25
sunat2    rbruc26
sunat2    rbruc27
sunat2    rbruc28
sunat2    rbruc30
sunat2    rbruc31
sunat2    rbruc32
sunat2    rbruc33
sunat2    rbruc34
sunat2    rbruc35
sunat2    rbruc36
sunat2    rbruc37
sunat2    rbruc38
sunat2    rbruc39
sunat2    rbruc40
sunat2    rbruc41
sunat2    rbruc42
sunat2    rbruc43
sunat2    rbruc44
sunat2    rbruc45
```

Continuación de Archivo 3.1 /etc/hosts.equiv de sunat0

```
sunat2    rbruc46
sunat2    rbruc47
sunat2    rbruc49
sunat2    rbruc50
sunat2    rbruc52
sunat2    rbruc53
sunat2    rbruc54
sunat2    rbruc55
sunat2    rbruc57
sunat2    rbruc58
sunat2    rbruc59
sunat2    rbruc60
sunat2    rbruc61
sunat2    rbruc62
sunat2    rbruc63
sunat2    rbruc64
sunat2    rbruc67
sunat2    admucla
sunat2    ucs01
sunat2    ucs02
sunat2    ucs03
sunat2    ucs04
sunat2    ucs05
sunat2    ucs06
sunat2    ucs07
sunat2    ucs08
sunat2    ucs09
sunat2    ucs10
sunat2    ucs11
sunat2    ucs31
```

CONCLUSIONES

1. Existen 2 maneras de conectividad de PC's: conectar el DOS PC como un terminal conectado al host o como un nodo de una red.

En la primera alternativa se puede realizar una conexión serial, cuando los usuarios deseen comunicarse con el sistema UNIX, ejecutarán un programa emulador o programa de telecomunicaciones. Una vez en línea los usuarios podrán realizar cualquier aplicación en UNIX. Con los programas de telecomunicaciones los usuarios de PCs en DOS podrán copiar archivos desde o a file systems en UNIX. Cuando no estén ejecutando el programa emulador podrán trabajar normalmente con sus PCs.

En la segunda alternativa es establecer una conexión DOS-a-UNIX para que el sistema UNIX aparezca como un drive de disco adicional. Esto requiere una conexión a la red por lo que se le conoce como estilo de red. Estos archivos pueden ser copiados a la PC, pero también pueden ser usados directamente por aplicaciones DOS tales como Qpro,

Excell, etc. como si estuviesen en un disco local. Comparado con el programa emulador en el cual cada archivo que se desee usar, debe ser copiado primero al disco local , esto es un gran adelanto.

La desventaja de la conexión a red es que el software siempre se encuentra presente. A diferencia de que el programa emulador que solo toma espacio en la memoria de la PC cuando es realmente usado, el software de red es cargado en la memoria cuando la PC es encendida. Como sabemos en la memoria tenemos cargados aplicaciones, software de red, drive de dispositivos, etc. Como resultado podemos inducir a un "RAM cram" que es el llenado de la memoria.

Entre las 2 opciones, la más recomendable es la conexión como terminales debido a que es la más economica.

Una tarjeta serial es más económica que una de red además que usa un cable barato. El software de emulación está en similar situación.

2. Con el Routing Information Protocol, el router manda su tabla de enrutamiento cada 30 segundos, los routers receptores comparan esta información con su respectiva tabla y las actualizan con la nueva información. En una red grande con un elevado volumen de tráfico, RIP puede ser mas que una

solución, un problema. Si la red tiene poca cantidad de routers, con destinos remotos bien definidos, el usar el comando route es suficiente. En el caso de una red en la cual los routers cambian con frecuencia, se debe tomar las precauciones del caso al usar RIP.

3. Se deberá tener cuidado en la configuración de los archivos .rhosts y host.equiv para evitar el acceso de usuarios. Puesto que la seguridad es un problema de personas no de los hosts, por lo que se deberá implementar procedimientos de seguridad y designación de personal responsable de velar por ello.

4. En la asignación de la dirección y dominio de la red la organización autorizada de ello es el Centro de Información de Red. En el caso de no pertenecer a la Red Internet se puede asignar arbitrariamente, pero en el caso de ingresar a la Red Internet, esta le asignará la dirección y el dominio por lo que la acción de la modificación es laboriosa con respecto al tamaño de la red. En el caso de la red de la SUNAT , la modificación no ha sido realizada y está con las direcciones arbitrariamente asignadas.

5. TCP/IP nos brinda un conjunto de protocolos estándares, de libre distribución y que es

independiente del hardware de la computadora. Es por ello que TCP/IP es ideal para unificar diferentes hardware y software. Y es posible usarlo sin necesidad de pertenecer a la Red Internet.

BIBLIOGRAFIA

Comunicaciones en UNIX
Autor : Jean - Marie Rifflet
Edición 1992

Redes de Area Local
Autor : Thomas W. Madrón
Grupo Noriega Editores
Edición 1992

Redes de Ordenadores. Protocolos, Normas e Interfaces
Autor : Uyless Black
Ediciones Rama
Edición 1993

StarPRO WIN-TCP. Administrator's Guide
Property NCR Corporation
Edición 1994

SCO TCP/IP. Runtime System for SCO UNIX Systems
Administrator's Guide
Property Santa Cruz Operation System
Edición 1992

TCP/IP Transport Supervisor's Guide
Property Novell Inc
Edición 1993

TCP/IP Network Administration
O'Reilly & Associates, Inc.
Edición 1994

Unix World Magazine
Mc Graw Hill's Magazine
Junio 1992, Julio 1992, Setiembre, 1992, Diciembre 1992,
Enero 1993