**UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO**

**FACULTAD DE ESTUDIOS PROFECIONALES**

**“ARAGON”**

# CONECTIVIDAD: PUENTES Y RUTEADORES

## TESIS PROFESIONAL

**Para Obtener La Licenciatura En:**

## INGENIERIA MECANICA - ELECTRICA


**PRESENTA:**

**SOTO ZAVALA JOSE LUIS**

**VALGAÑÓN CRUZ LINO EDGAR**


**San Juan de Aragón, México** **2006**

## AGRADECIMIENTOS:

Agradezco muy sinceramente al Ingeniero Benito Barranco Castellanos por haberme apoyado y motivado a terminar mis estudios durante todos estos años.

Agradezco al Ingeniero Luis Nemesio por haberme facilitado los medios, su amistad y la orientación para concluir mis estudios.

Agradezco al ingeniero Henri Escamilla Toloza por haberme dado el apoyo, su tiempo, amistad y conocimientos para concluir mi carrera a lo largo de estos años.

Quiero agradecer muy especialmente todo el apoyo, la paciencia y la dedicación que han tenido conmigo a lo largo de toda mi carrera:

Agradezco a muchas personas que por alguna causa no mencione una por una, pero saben que les agradezco el haber estado con migo en muchos momentos buenos y malos de mi carrera y haberme ayudado a salir adelante, gracias por haber creido en mi.

## A la Universidad Nacional Autónoma de México.

Por darme el orgullo de pertenecer a la máxima casa de estudios, a la cual me siento muy orgulloso de pertenecer, gracias por los conocimientos transmitidos a lo largo de estos años.

## A la Facultad de Estudios Superiores Aragón.

Por ser la escuela que me brindo la oportunidad de terminar mis estudios.

## A Todos Mis Profesores.

Por todos los consejos, conocimientos, paciencia y su tiempo brindado incondicionalmente durante todos estos años.

## A Mis Sinodales.

Por la dedicación y tiempo otorgado para la revisión de este trabajo.

## A mi Asesor de Tesis.

Ing. Benito Barranco Castellanos.

De manera especial le agradezco por haberme brindado su amistad, valioso tiempo, conocimientos y apoyo a pesar de su gran carga de trabajo, ya que sin su ayuda, hubiera sido imposible terminar este trabajo. ¡Muchas gracias¡

# CONECTIVIDAD: PUENTES Y RUTEADORES

## Tabla de contenido


| | | Página |
|---|---|---|
| **Introducción** | | **1** |
| **Capítulo I.** | **Interconectividad** | **6** |
| | Redes de datos | 6 |
| | Puentes | 13 |
| | Ruteadores | 16 |
| | Diferencias entre puentes y ruteadores | 18 |
| | Otros dispositivos de interconexión | 18 |
| | **Protocolos TCP/IP** | **21** |
| | Operación y arquitectura | 21 |
| | Protocolos enrutados vs. protocolos de ruteo | 26 |
| | Protocolos de nivel de red | 27 |
| | Servicios sobre TCP/IP | 30 |
| | SNMP (Protocolo Simple de Gestión de Red) | 34 |
| | Interfaces | 36 |
| | Ruteo para IP | 38 |
| | Tipos de "Broadcasting" | 45 |
| **Capítulo II.** | **Puentes y Switches** | **48** |
| | Fundamentos del puenteo y la conmutación | 48 |
| | Arquitectura y funcionamiento de los puentes | 51 |
| | Algoritmo IEEE.802.1 | 52 |
| | Algoritmo IEEE.802.5 | 54 |
| | Switches | 56 |
| **Capítulo III.** | **Configuración Ruteadores** | **60** |
| | Ruteo de paquetes | 60 |
| | Elementos de la función de ruteo | 64 |
| | Algoritmos de ruteo | 64 |
| | Protocolos de ruteo | 69 |
| | Políticas de ruteo | 73 |
| **Capítulo IV.** | **Practicas** | **75** |
| | Inicialización | 75 |
| | Configuración básica | 78 |
| | Configuración de interfaces | 83 |
| | Listas de acceso | 86 |
| | Ruteo estático | 88 |
| **Anexo 1. Conversión (decimales a binarios)** | | **90** |
| **Anexo 2. Prácticas** | | **91** |
| **Anexo 3. Glosario de comandos de configuración para ruteadores CISCO** | | **120** |
| **Anexo 4. Números de puerto reservados para TCP y UDP** | | **127** |
| **Anexo 5. Comandos utilizados en versiones anteriores ala versión 11.0 del sistema operativo lOS de CISCO** | | **129** |
| **Glosario** | | **130** |
| **Bibliografía** | | **135** |

# Introducción

A medida que las empresas se han vuelto cada vez más dependientes de las computadoras y las redes para manejar sus actividades, la disponibilidad de los sistemas informáticos se ha vuelto crucial. Actualmente, la mayoría de las empresas necesitan un nivel alto de disponibilidad y algunas requieren incluso un nivel continuo de disponibilidad, ya que les resultaría extremadamente difícil funcionar sin los recursos informáticos.

Los procedimientos manuales, si es que existen, sólo serían prácticos por un corto periodo. En caso de un desastre, la interrupción prolongada de los servicios de computación puede llevar a pérdidas financieras significativas, sobre todo si está implicada la responsabilidad de la gerencia de informática. Lo más grave es que se puede perder la credibilidad del público o los clientes y, como consecuencia, la empresa puede terminar en un fracaso total.

Imagínese una situación que interrumpa las operaciones de las computadoras durante una semana o un mes; imagine la pérdida de todos los datos de la empresa, todas las unidades de respaldo del sitio y la destrucción de equipos vitales del sistema ¿Cómo se manejaría semejante catástrofe? Si Ud. se ve en esta situación y lo único que puede hacer es preguntarse "¿Y ahora qué?" ¡ya es demasiado tarde! La única manera efectiva de afrontar un desastre es tener una solución completa y totalmente probada para recuperarse de los efectos del mismo.

Se puede considerar como un desastre la interrupción prolongada de los recursos informáticos y de comunicación de una organización, que no puede remediarse dentro de un periodo predeterminado aceptable y que necesita el uso de un sitio o equipo alterno para su recuperación.

Ejemplos obvios son los grandes incendios, las inundaciones, los terremotos, las explosiones, los actos de sabotaje, etcétera.

Cuando se diseña una red de datos se desea sacar el máximo rendimiento de sus capacidades. Para conseguir esto, la red debe estar preparada para efectuar conexiones a través de otras redes, sin importar qué características posean.

El objetivo de la Interconexión de Redes (internetworking) es dar un servicio de comunicación de datos que involucre diversas redes con diferentes tecnologías de forma transparente para el usuario. Este concepto hace que las cuestiones técnicas particulares de cada red puedan ser ignoradas al diseñar las aplicaciones que utilizarán los usuarios de los servicios.

Los dispositivos de interconexión de redes sirven para superar las limitaciones físicas de los elementos básicos de una red, extendiendo las topologías de esta.

Algunas de las ventajas que plantea la interconexión de redes de datos, son:

- Compartición de recursos dispersos.
- Coordinación de tareas de diversos grupos de trabajo.
- Reducción de costos, al utilizar recursos de otras redes.
- Aumento de la cobertura geográfica.
- Tipos de Interconexión de redes

Se pueden distinguir dos tipos de interconexión de redes, dependiendo del ámbito de aplicación:

- Interconexión de Área Local (RAL con RAL)

Una interconexión de Área Local conecta redes que están geográficamente cerca, como puede ser la interconexión de redes de un mismo edificio o entre edificios, creando una Red de Área Metropolitana (MAN)

**Interconexión de Área Extensa (RAL con MAN y RAL con WAN)**

La interconexión de Área Extensa conecta redes geográficamente dispersas, por ejemplo, redes situadas en diferentes ciudades o países creando una Red de Área Extensa (WAN). Las principales tendencias del mercado de sistemas de interconexión de redes son las siguientes:

**Tendencias de encaminamiento**

El mercado está en expansión, cada vez hay más ofertas de productos y además estos incorporan nuevas facilidades de encaminamiento. Tanto los fabricantes de concentradores como los de multiplexores están incorporando en sus productos capacidades de encaminamiento, unos con redes de área metropolitana y extensa, y otros incorporando facilidades de interconexión de RALs.

**Equipos de interconexión a bajo coste**

Los fabricantes están presentando equipos de bajo coste que permiten la interconexión de dependencias remotas. Las soluciones de encaminamiento son de diversos tipos: integradas en servidores de red, en concentradores, en pequeños equipos router, etc. Todos estos productos son fáciles de gestionar, operar y mantener.

**Routers multiprotocolo**

Estos dispositivos han permitido a los usuarios transportar protocolos diferentes sobre la misma infraestructura de red, lo cual permitiría ahorrar en costes de la infraestructura de transmisión y una potencial mejora de la interoperabilidad.

**Interconexión de LAN/WAN bajo Switchers**

Los conmutadores han evolucionado rápidamente dotándose de altas capacidades y velocidad de proceso. Pensados para soportar conmutación ATM (Asynchronous Transfer Mode, Modo de Transferencia Asíncrono) bajo una arquitectura punto a punto, han logrado gran implantación como mecanismo de interconexión de redes de área local heterogéneas, Token Ring y Ethernet en un mismo dominio. Esto se consigue dado que el conmutador permite la segmentación de la red en subredes conectadas a cada uno de sus puertos que puede gestionar de manera independiente.

**Capacidad de gestión**

Los fabricantes están dotando a sus dispositivos de interconexión con mayores capacidades de gestión que permitan la monitorización de la red mediante estaciones de gestión y control de los dispositivos de la red, enviando comandos por la red desde la estación de gestión hasta el dispositivo de la red para cambiar/inicializar su configuración.

**Análisis de las necesidades del comprador**

Las razones para proceder a la adquisición de sistemas de interconexión de redes pueden estar determinadas por diferentes factores. Es labor del responsable de compras la realización de un análisis de necesidades existentes dentro de su organización que permita determinar las necesidades actuales y futuras de los usuarios y las limitaciones o restricciones que ha de plantearse respecto al dimensionamiento de la red y de los dispositivos de interconexión. Es necesario tener en cuenta y analizar en profundidad los costes y beneficios asociados para obtener argumentos de peso en la toma de decisiones.

En la fase de análisis de necesidades, fase inicial del proceso de adquisición, hay que tener en cuenta todos aquellos requisitos, limitaciones y restricciones que afecten, entre otros, a los siguientes puntos:

**Ventajas de la interconexión de redes**

Hay que determinar si algunas de las ventajas que proporciona la interconexión de redes es aplicable a las necesidades de la organización. La interconexión de redes proporcionan diferentes ventajas:

- Compartición de recursos dispersos o de otras redes.
- Extensión de la red y aumento de la cobertura geográfica.
- Segmentación de una red.
- Separación entre redes.
- Conversión de protocolos.

Antes de segmentar una red es recomendable realizar un estudio de flujos de datos, porque puede suceder que al realizar la partición en segmentos se aumente el tráfico en los segmentos en vez de disminuirlo.

**Número de redes que van a ser conectadas y topología de las redes**

El conocimiento del número de redes a interconectar y las características específicas de cada uno de ellas, permitirá dimensionar correctamente tanto la estructura de la red final como los elementos necesarios para realizar la interconexión.

También se han de analizar las necesidades de adquisición de nuevas redes o infraestructura de red para poder dar soporte a la futura red. Es necesario delimitar claramente el tipo de redes existentes (Ethernet, TokenRing, FDDI, etc), su topología (estrella, bus, anillo, etc), su distribución espacial en el entorno de operación (localización y distancias). Es recomendable realizar planos del entorno en cuestión.

**Características del entorno físico de operación**

La interconexión de redes exige por lo general el tendido de cableado en las dependencias por las que se extienden las redes y ello es una labor cuya complejidad, impacto y coste depende de varios factores. Entre éstos habrá que considerar el área cubierta por las redes y por su interconexión (ubicaciones, departamentos y edificios a interconectar), sus topologías, las peculiaridades constructivas de los locales o edificios, y otras cuestiones que pueden afectar no sólo al coste sino incluso a la viabilidad de la implantación de la interconexión de redes.

**Estimación del coste de adquisición, operación y mantenimiento**

El costo de adquisición de dispositivos de interconexión de red tiene varios componentes, directos e indirectos. Todos ellos han de ser tenidos en cuenta si se quiere realizar una previsión razonable de fondos. Los principales factores de coste son los siguientes: Dispositivos físicos de la red: medio de transmisión, elementos de conexión de los nodos, etc. Dispositivos lógicos de la red: sistemas de gestión, control y mantenimiento. Instalación: acondicionamiento de locales, canalización, tendido de cables, conexión de dispositivos, etc. Costes indirectos: redimensionamiento de nodos pasivos y activos, elementos complementarios, etc. En ningún caso debe despreciarse a priori la importancia de ningún tipo de costes.

El responsable público de adquisición deberá de disponer de una estrategia de redes perfectamente elaborada para poder satisfacer las necesidades que se puedan plantear en un futuro. Cuando una red está instalada, ésta crece de forma continuada, aumentando en equipos anteriormente no considerados y llegando a lugares no contemplados, soportando nuevas aplicaciones..., lo cual demandará capacidades no imperativas inicialmente

**Factores relevantes en el proceso de adquisición**

En la definición del objeto del contrato y los requisitos inherentes al mismo, así como en la valoración y comparación de ofertas de los licitadores pueden intervenir muchos factores y de muy diversa índole.

Es de suma importancia que todos los factores relevantes que intervienen en el proceso de contratación queden debidamente recogidos en el pliego de prescripciones técnicas que regule el contrato. Así mismo, es conveniente que las soluciones ofertadas por los licitadores sean recogidas en los cuestionarios disponibles a tal efecto:

No obstante y a título orientativo en este apartado se hace mención de aquellos factores, que entre los anteriores, pueden intervenir en el proceso de adquisición de equipos y sistemas de interconexión de redes y cuyo seguimiento debe efectuarse exhaustivamente:

**Número de puertas disponibles**

Cuando se decide seleccionar un dispositivo de interconexión no sólo hay que tener en cuenta el número de puertas necesarias; hay que pensar en el crecimiento futuro. Interesa dejar un número de puertas disponibles para tener siempre capacidad de crecimiento. Es importante definir un tanto por ciento de puertas libres respecto a las utilizadas. Este porcentaje varía de una implantación a otra y normalmente está condicionado también por el coste de los dispositivos. Algunos de los dispositivos necesitan conexión remota o local de consola, por lo que habrá que tener en cuenta que el dispositivo presente esta característica.

**Gestión disponible**

La complejidad de las redes impone la necesidad de utilizar sistemas de gestión capaces de controlar, administrar y monitorizar las redes y los dispositivos de interconexión. Los routers son dispositivos que necesitan que se realicen funciones de gestión. En los otros dispositivos es recomendable que tengan esta facilidad. Es conveniente analizar si la gestión del dispositivo ofertada es propietaria o es abierta, tendiendo siempre a la última opción.

**Pruebas de aceptación final**

En función de los elementos técnicos que intervienen y del alcance abarcado, se definen distintos tipos de pruebas sobre los siguientes entornos de una red de datos:

1. Operativa de Red:

Se distingue entre lo que es un funcionamiento normal de la red y el funcionamiento o reacción de ésta ante los diversos fallos que puedan producirse. Entendiendo por funcionamiento normal, aquél en el que los equipos y la red se encuentran en óptimas condiciones.

**Funcionamiento normal.**

Se realizarán las comprobaciones de las siguientes funcionalidades:

- Comunicaciones entre Puertos.
- Comprobar las comunicaciones a través de una red.
- Comprobar las comunicaciones con redes externas.
- Comprobar la existencia de derechos de acceso a los distintos puertos de las tarjetas de los diferentes equipos.

Configuraciones dinámicas.

- Comprobar que las inserciones o extracciones de tarjetas de una red, no afectan al funcionamiento de la misma.
- Comprobar que la extracción o inserción de una tarjeta router, no afecta al funcionamiento de las redes locales conectadas a ese router.
- Comprobar que un cambio en la configuración de una tarjeta, no afecta al funcionamiento del resto de la red.

**Funcionamiento ante fallos.**

Se realizarán pruebas destinadas a la comprobación de cómo reacciona la red, en el caso de que se produzcan fallos en distintos elementos de la misma. Comprobar que las redes siguen funcionando aisladamente, después de la caída de un ramal. Comprobar el funcionamiento de las redes ante la caída de una tarjeta de un equipo.

2. Gestión de Red

Funcionamiento propio del sistema de gestión:

- Comprobar el funcionamiento de la red ante la caída del sistema de gestión.
- Comprobar que existe un control de accesos al sistema de gestión de red, con distintos niveles de seguridad.

Monitorización de la red.

- Comprobar que el sistema de monitorización gráfica responde en tiempo real a los eventos que ocurren en la red.
- Comprobar que se pueden visualizar distintos niveles dentro de la topología de la red.

Tratamiento de alarmas.

- Comprobar que el fallo, y posterior recuperación de elementos de la red, provoca las alarmas adecuadas.
- Comprobar la existencia de herramientas de prueba remota.
- Comprobar la existencia de distintos niveles de alarmas, y que pueden ser definidas por el usuario.

Analizar con las herramientas disponibles la actividad de la red y la creación de informes sobre la misma.

# Capítulo 1

## Interconectividad

A medida que las redes de área local fueron adquiriendo un papel más importante en la actividad de las empresas, Corporaciones e instituciones, la posibilidad de ampliar y conectar LAN's entre sí se convirtió en una necesidad imperiosa.

La ampliación y conexión de redes LAN a nivel local pudo llevarse a cabo por medio de dispositivos de conexión entre redes (o *dispositivos de interconexión)* como repetidores, puentes, conmutadores y ruteadores. Sin embargo, para conectar redes LAN más distanciadas geográficamente resulta imprescindible recurrir a otro tipo de tecnología. La necesidad por hallar una tecnología que permitiera a los administradores de red conectar redes LAN repartidas por extensas áreas geográficas se convirtió en algo crucial a medida que las empresas fueron creciendo y pasaron a convertirse en grandes Corporaciones.

Ampliar una red para cubrir grandes distancias puede hacerse aplicando algunas de las tecnologías de conectividad o de interconexión, actualmente disponibles. Las redes pueden conectarse a los servicios que presta la red telefónica pública conmutada o las compañías privadas de telecomunicaciones.

### Redes de datos

Una Red de Computadoras, llamada también Red de Datos, es el conjunto de computadoras, terminales y dispositivos (impresoras, módems, graficadores, escáners, etc.) que se comunican entre sí por algún medio, proporcionando el entorno necesario, para que los usuarios, desde diferentes ubicaciones (local, remota, etc.), tengan acceso, en condiciones similares, a la información.

La conexión puede ser directa (a través de un cable) o indirecta (a través de un módem). Los distintos dispositivos en la red se comunican entre sí utilizando un conjunto predefinido de reglas (el protocolo), lo cual permite a los usuarios tener intercomunicación de datos y compartir recursos.

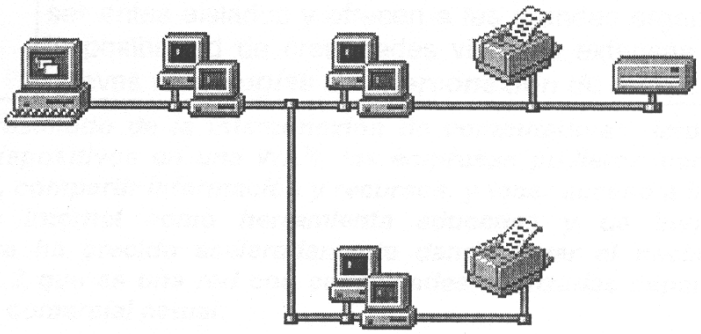


**Fig. 1.1** Red de datos

**Evolución histórica**

A continuación se describe un panorama general sobre la evolución histórica de las redes de datos:

| Década | Descripción |
|---|---|
| 60 y 70 | La informática se concebía como un servicio estructurado jerárquicamente, reflejando en gran medida la estructura interna de las organizaciones. |
| 80 | Surgieron las Redes de Área Local *(LAN)*, a la vez que nuevos métodos de organización, proponiendo una estructuración de las organizaciones basada en grupos de trabajo especializados y coordinados entre sí mediante mecanismos más dinámicos y flexibles. |

| Década | Descripción |
|---|---|
| 90 | Surge la necesidad de transferir información rápidamente y con eficiencia, no solamente dentro de una misma empresa sino de una empresa a otra, la solución fue la creación de Redes de Área Metropolitana *(MAN)* y Redes *de Área Amplia (WAN)*. Como las WAN podían conectar redes de usuarios dentro de áreas geográficas extensas, esto permitió que las empresas se comunicaran entre sí a través de grandes distancias, por lo que las redes LAN dejan de ser entes aislados y ofrecen a las grandes organizaciones la posibilidad de crear redes virtuales extensas mediante nuevas ***tecnologías de interconexión de redes***. |

Como resultado de la interconexión de computadoras, impresoras y otros dispositivos en una WAN, las empresas pudieron comunicarse entre sí, compartir información y recursos, y tener acceso a Internet. El uso de Internet como herramienta educativa y de investigación científica ha crecido aceleradamente dando lugar al nacimiento de Internet 2 que es una red con capacidades avanzadas separada de la Internet comercial actual.

Clasificación y funciones Las redes de datos se han clasificado como sigue:

- Redes LAN (Local Area Network). Diseñadas para realizar las siguientes funciones:
    - Operar dentro de un área geográfica limitada (dentro del mismo edificio o grupo de edificios).
    - Permitir que varios usuarios accedan a medios con ancho de banda alto.
    - Controlar la red de forma privada con administración local.
    - Proporcionar conectividad continua a los servicios locales.
    - Conectar dispositivos físicamente adyacentes.

- Redes WAN (Wide Area Network). Diseñadas para realizar las siguientes funciones:
    - Operar en áreas geográficamente extensas (conectan ciudades y países).
    - Suministrar conectividad continua y parcial.
    - Conectar dispositivos separados por grandes distancias, e incluso a nivel mundial.

**Tecnología de La interconectividad** *tecnología de ínterconectívídad de redes* surgió como una solución a tres problemas:

- ***LAN's aisladas***. Imposibilitaban la comunicación electrónica entre diferentes oficinas o departamentos.
- ***Duplicación de recursos***. Se debía suministrar el mismo hardware y software a cada departamento y oficina, así como tener grupos de soporte separados.
- ***Falta de administración de red***. No había un método centralizado para administrar y reparar las redes.

**¿Qué es la interconexión de redes?** En sentido estricto, la ***conexión entre redes* o *interconexión de redes*** se refiere a la conexión entre dos o más redes LAN que siguen funcionando como entidades autónomas.

En sentido más amplio, la ***interconexión de redes*** es una estrategia que permite ampliar, segmentar y conectar redes LAN con el fin de maximizar el ancho de banda en las mismas y entre las mismas.

El objetivo de la ***Interconexión de Redes*** *(intemetworking)* es dar un servicio de comunicación de datos que involucre diversas redes con iguales o diferentes tecnologías de forma transparente para el usuario, mediante dispositivos de interconexión.

Un buen ejemplo de esto extraído del mundo real es *Internet.*

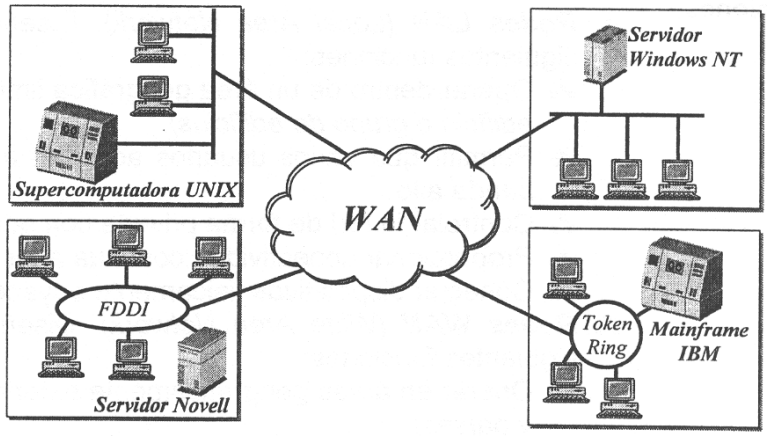



**Fig. 1.2** Interconexión de Redes

**Ventajas de la interconexión** Algunas de las ventajas que plantea la interconexión de redes de datos, son:

- Compartición de recursos dispersos.
- Coordinación de tareas de diversos grupos de trabajo.
- Reducción de costos, al utilizar recursos de otras redes.
- Aumento de la cobertura geográfica.

**Tipos de interconexión de redes** Se pueden distinguir dos tipos de interconexión de redes, dependiendo del ámbito de aplicación:

- ***Interconexión de Área Local.*** Conecta redes que están geográficamente cerca, como puede ser la interconexión de redes de un mismo edificio o entre edificios.
- ***Interconexión de Área Extensa.*** Conecta redes geográficamente dispersas, por ejemplo, redes situadas en diferentes ciudades o países creando una red *WAN.*

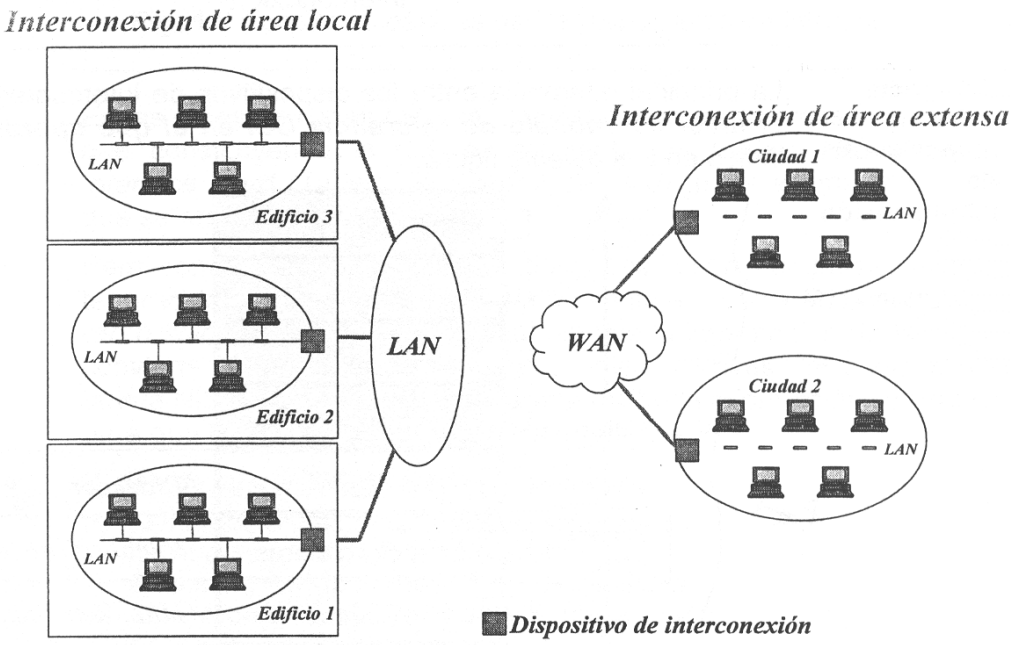



**Fig. 1.3** Tipos de interconexión de redes

**Dispositivos de interconexión** Cuando se tienen redes locales ubicadas en diferentes edificios o en diferentes pisos dentro de un edificio y se desea interconectarlas para que los usuarios de una red puedan comunicarse con los usuarios de otra, es necesario utilizar ***dispositivos de interconexión***, los cuales superan las limitaciones físicas de los elementos básicos de una red, y su función principal es la de extender las topologías de red.

Estos dispositivos de interconexión son: *concentradores* o ***hubs***, ***repetidores***, *puentes* o ***bridges***, *encaminadores* o ***routers*** y *pasarelas* o ***gateways***.

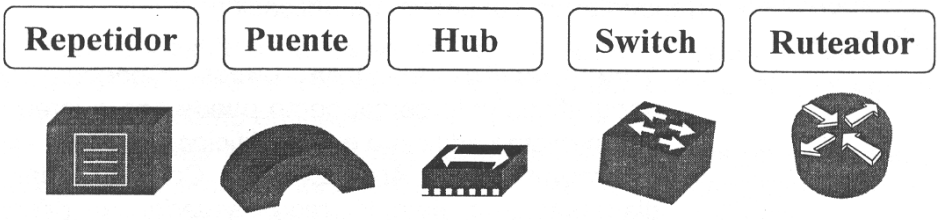



**Fig. 1.4** Ejemplo de la representación de algunos dispositivos de interconexión

## Diferencia entre los dispositivos de interconexión

La principal diferencia entre los dispositivos de interconexión está **en *el nivel del modelo de referencia OSI en el que operan***, como se indica en la siguiente figura:

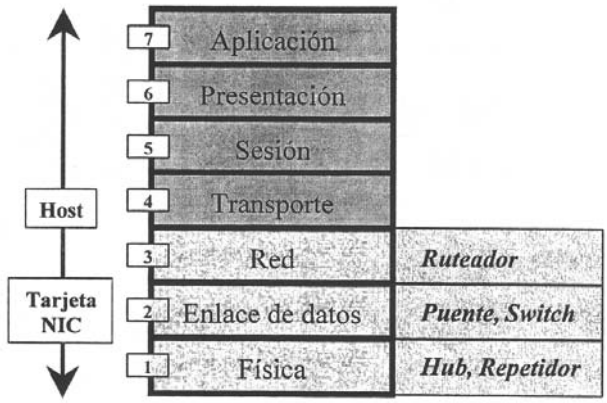



**Fig. 1.5** Dispositivos de interconexión en el modelo de referencia OSI

### Funciones básicas de los dispositivos de interconexión

Los dispositivos de interconexión de redes proporcionan algunas (o *todas)* de las siguientes funciones básicas:

- ***Extensión de la red***. Permiten ampliar el rango de distancia que puede alcanzar una red *(por ejemplo el repetidor).*
- ***Definición de segmentos dentro de la red.*** Al dividir la red en segmentos se consigue aumentar las prestaciones de la red ya que cada tramo soporta sólo su propio tráfico y no los de los otros segmentos *(por ejemplo el puente* o *switch).*
- ***Separación entre redes.*** Mediante estos dispositivos las grandes redes se pueden componer de otras más pequeñas interconectadas entre sí, de forma transparente para el usuario. Varias redes físicas pueden combinarse para formar una única red lógica *(por ejemplo el ruteador).*

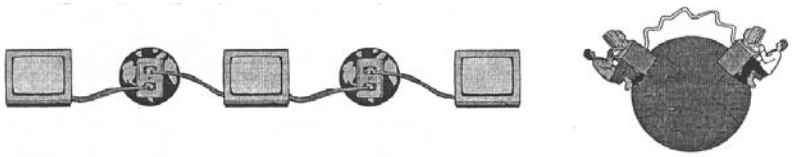


**Fig. 1.6** Funciones básicas de los dispositivos de interconexión

## Tarjeta NIC

En las redes de computadoras, uno de los elementos más importantes que constituyen a la red, es sin duda, la ***Tarjeta NIC*** *(Network Interface Card, Tarjeta de Interfaz de Red),* pues es mediante ésta que se realiza el acceso a la red.

Para comunicarse con el resto de la red, cada computadora debe tener instalada una tarjeta NIC *(también se les llama adaptadores de red* o *sólo tarjetas de red),* la cual obtiene la información de la PC, la convierte al formato adecuado y la envía a través del cable a otra tarjeta NIC de la red local. Esta tarjeta recibe la información, la traduce para que la PC pueda entender y la envía a la PC.

**El tipo de tarjeta NIC determina lo siguiente:**

- El método usado para enviar y recibir datos.
- La velocidad de transmisión de datos.
- El tamaño y formato de las tramas de datos.
- El método de acceso al medio de transmisión.
- El tipo de medio de transmisión.
- La topología de la red.
- La tecnología de interconexión: Ethernet, Token Ring, FDDI, ATM, Frame Relay.

## Funciones de la tarjeta NIC

Son ocho las funciones que realiza la tarjeta NIC, las cuales se describen a continuación:

1. ***Establece la comunicación con el equipo.*** La comunicación de la PC a la tarjeta NIC se realiza a través de un bus de comunicación *(con alguno de los métodos DMA,. Entrada / salida, memoria compartida)*.

2. ***Buferización.*** Cuando la tarjeta NIC recibe datos de la LAN, los almacena temporalmente en una memoria llamada buffer antes de pasarlos a la memoria principal del CPU de la PC. Este almacenamiento temporal es necesario porque los datos pueden llegar a una velocidad más rápida que aquella con la cual la NIC puede procesarlos, para: *cambiar los datos de serie a paralelo, desempaquetarlos* y *transferirlos al destino.*

3. ***Formación de tramas.*** Los datos que la tarjeta NIC recibe de la aplicación en la PC son encapsulados en un paquete *(trama),* donde el encabezado incluye la dirección fuente y destino, mientras que la cola contiene una secuencia de datos para que el receptor pueda detectar errores en la comunicación.

4. ***Conversión serie / paralelo.*** La tarjeta NIC recibe datos de la PC en modo paralelo (*8, 16 ó 32 bits a un tiempo),* según el tamaño del bus, y los transfiere al medio de comunicación de la LAN en modo serie *(bit por bit).* Por esto es necesario que la NIC haga la conversión de los datos de modo serie a paralelo y viceversa.

5. ***Codificación / decodificación* en *línea.*** Para transferir los datos sobre el medio de comunicación, la tarjeta NIC representa los datos en un código determinado.

6. ***Acceso al medio de comunicación.*** En las redes locales el medio de comunicación es compartido, por lo que sólo una PC transmite aun tiempo dado, lo que hace necesario controlar el acceso al medio.

7. ***Establecimiento de parámetros de transmisión.*** En la fase de establecimiento de una comunicación, la tarjeta NIC fuente envía a la tarjeta NIC destino los parámetros de comunicación que se deben utilizar, como por ejemplo: *tamaño de los buffers, tamaño de las tramas, etc.*

8. ***Transmisión* y *recepción de los datos.*** Todas las funciones anteriores tienen como fin que la tarjeta NIC pueda transferir y recibir datos desde y hacia la LAN.

La evolución de la tecnología ha ocasionado que la NIC no sólo se asocie al término tarjeta. Hoy en día se puede generalizar el término a dispositivo.

**Operaciones para una Red LAN**

Las operaciones necesarias para el trabajo de una red LAN corresponden a las capas 1 y 2 del modelo OSI *(ver figura* 1.5):

- Las funciones en la capa 1 ***(física)*** corresponden al establecimiento, mantenimiento y desactivación de un enlace físico para transferir la secuencia de bits de una estación a otra *(niveles de voltaje)*
- Las funciones en la capa 2 ***(Enlace de datos)*** se describen a continuación:
    - ***Encapsulado.*** Organización de los paquetes en tramas.
    - ***Identificación.*** Indicación de origen y destino de las tramas.
    - ***Secuencia.*** Etiquetación de cada trama con un número de folio.
    - ***Control de flujo.*** Mecanismo para evitar que el transmisor sature al receptor con tramas de información.
    - ***Control de error.*** Instalación de protocolos para la detección de errores que puedan ocurrir en la transmisión.
    - ***Codificación/decodificación de señales.*** Representación de la secuencia de bits con señales eléctricas transmitidas en el canal de comunicación.
    - ***Sincronización.*** Generación y remoción de secuencias de bits para identificar cada una de las tramas entre las dos estaciones que intercambian información..

*En una red local, se tienen varias computadoras conectadas, pero en ellas no se lleva a cabo todas las funciones de la capa de red, aún cuando se debe asegurar que un mensaje de una computadora fuente sea entregado a otra destinataria. Las razones son las siguientes:*

- *En una red local no hay enrutamiento ni "switcheo o conmutación" intermedio.*
- *Algunas funciones de la capa de red se instalan en la capa de enlace de datos.*

## Enlace de datos

Una particularidad importante a considerar, es que en las redes locales la capa de ***enlace de datos*** debe de soportar el acceso aun sistema que tiene múltiples computadoras fuentes y destinos, por lo que es necesario diseñar algunas funciones de la capa de red. Para realizar esto, la capa de enlace de datos se divide en dos sub capas:

- LLC (Logical Link Control, Control de Enlace Lógico).
- MAC (Medium Access Control, Control de Acceso al Medio).

- En la sub capa *LLC,* se realizan las siguientes funciones:
    - Control de flujo de extremo a extremo para regular la transferencia de mensajes entre transmisor y receptor.
    - Control de error para garantizar la entrega de un mensaje de la fuente al destino sin error .

La sub capa LLC, agrega un encabezado a los datos que recibe del usuario de la capa superior. Este encabezado ***administra*** el enlace entre la entidad local LLC y la entidad remota LLC. Los datos de usuario y el encabezado LLC forman un ***PDU*** *(Protocol Data Unit, Unidad de Datos del Protocolo)* de LLC. El *PDU* preparado por la sub capa LLC debe ser enviado de la estación fuente a su igual en la estación destino, esto se realiza mediante el uso de los servicios de la capa ***MAC****,* la cual agrega un encabezado y una cola resultando de aquí *la* ***trama****,* como se muestra en la siguiente figura:

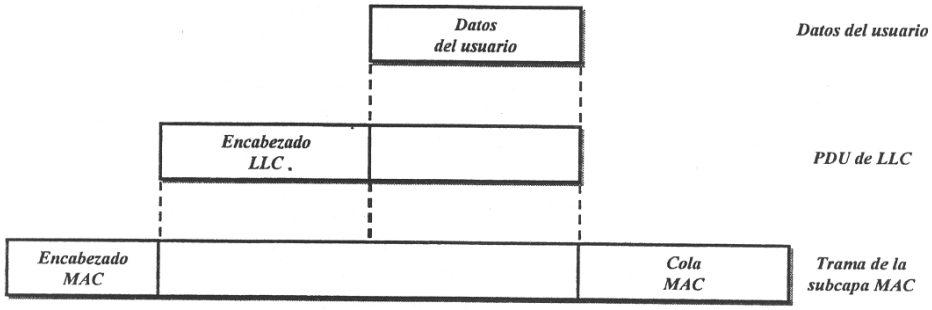



**Fig. 1.7** Trama MAC y PDU de LLC

En la sub capa *MAC,* se realizan las siguientes funciones:

- Encapsulado de los datos en las tramas de transmisión y desencapsulado en las de recepción.
- Aplicación del algoritmo CRC *(Cyclic Redundancy Check, Verificación de Redundancia Cíclica)* para la detección de errores en la transmisión.

## Puentes

**Descripción** Los ***puentes*** son dispositivos de conectividad inteligentes *(toman decisiones),* constituidos como nodos de la red, que conectan entre sí dos segmentos, transmitiendo de uno a otro el tráfico generado no local. Al distinguir los tráficos locales y no locales, estos dispositivos disminuyen el mínimo total de paquetes circulando por la red por lo que, en general, habrá menos colisiones y resultará más difícil llegar a .la congestión de la red.

Los puentes operan en el Nivel de Enlace del modelo de referencia OSI, en el nivel de trama MAC *(Medium Access Control, Control de Acceso al Medio),* y se utilizan para conectar o extender redes *(que operan bajo distintos protocolos de Capa* 2) y conexiones a redes de área extensa.

**Aplicación** Las aplicaciones de los puentes se encontraban en soluciones de interconexión de LAN's dentro de una interconexión de redes de tamaño pequeño-medio, creando una única red lógica y obteniendo facilidad de instalación, mantenimiento y transparencia a los protocolos de niveles superiores. También fueron útiles en conexiones donde se requerían funciones de filtrado.

### Funciones principales

Un puente ejecuta tres funciones principales:

- ***Aprendizaje de las direcciones de nodos en cada red.*** El puente no realiza ningún cambio al contenido o formato de las tramas que recibe. Tiene que tener cierta inteligencia, pues debe ser capaz de conocer qué direcciones de red existen en cada uno de los segmentos, de manera que pueda decidir si una trama debe retransmitirla al otro segmento o no. Incluso si existen más de dos segmentos de red interconectados por puentes, un puente debe conocer a qué direcciones se puede llegar, no sólo desde el otro segmento, sino atravesando otros puentes.
- ***Filtrado de las tramas destinadas a la red local.*** Los puentes se encargan de filtrar el tráfico que pasa de uno a otro segmento de red según la dirección de destino y una tabla que relaciona las direcciones y la red en que se encuentran las estaciones asignadas.

- ***Envío de las tramas destinadas a la red remota.*** Además de unir dos segmentos de red, puede haber varios segmentos de red unidos por puentes. Cuando una computadora envía un mensaje a un segmento que no está unido directamente al mismo puente que la computadora que envía el mensaje, el mensaje debe atravesar varios puentes hasta llegar a la computadora de destino. Por ello, un puente debe tener cierto conocimiento de los segmentos de red que existen más allá de aquellos a los que está conectado.

**Funcionamiento básico**

Los segmentos de red conectados a través de un puente aparentan ser una única red, ya que realizan su función transparentemente; es decir, las estaciones no necesitan conocer la existencia de estos dispositivos, ni siquiera si una estación pertenece auno u otro segmento.

Un ***puente conecta dos segmentos de red,*** como se muestra en la figura siguiente:

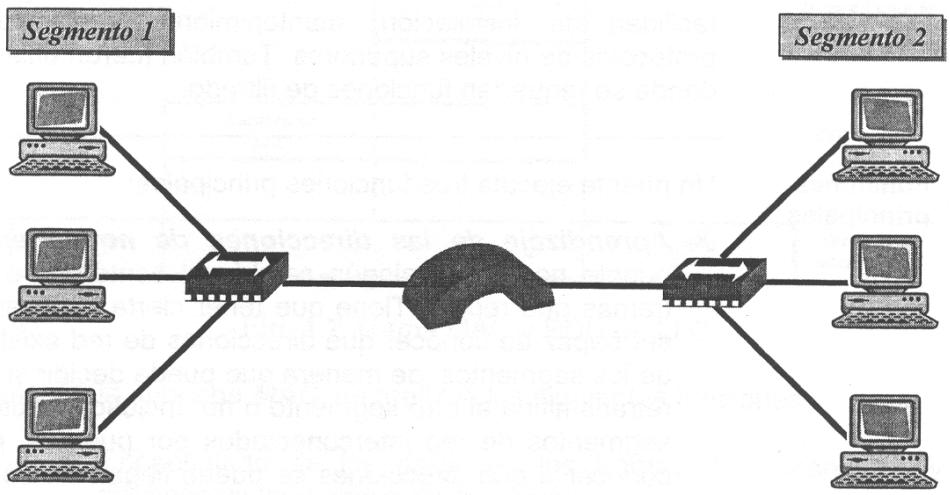



**Fig. 1.8** Funcionamiento básico de un puente

El funcionamiento básico de un puente es muy sencillo: El puente recoge todos los paquetes que circulan en el segmento 1, por ejemplo. Cuando hay un paquete para el segmento 2, retransmite dicho paquete en el segmento 2. Actúa de la misma forma cuando hay un paquete del segmento 2 dirigido al segmento 1.

**Tipos de puentes**

Una clasificación habitual de los puentes distingue entre puentes locales y puentes remotos:

- ***Puentes Locales.*** Sirven para enlazar directamente dos segmentos de red físicamente cercanos, es decir, proporcionan conectividad entre segmentos de una red dentro de un área local, como puede ser una oficina, una planta de un edificio o un edificio.
- ***Puentes Remotos.*** Se conectan en parejas, enlazando dos o más segmentos de red locales, formando una red de área extensa, a través de líneas telefónicas, por ejemplo, enlaces dedicados, líneas RDSI, etc.

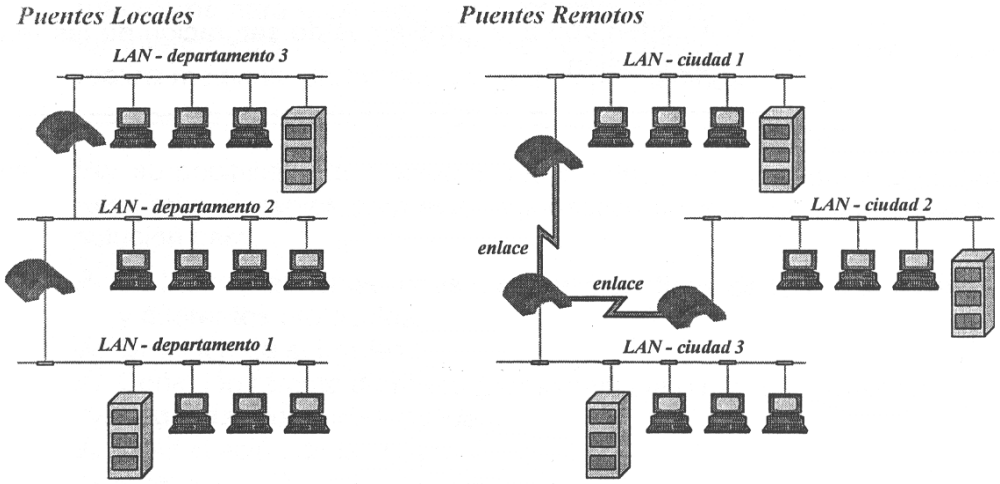



**Fig. 1.9** Tipos de puentes

**Ventajas**

Algunas ventajas de la utilización de puentes se describen a continuación:

- ***Fiabilidad.*** Utilizando puentes se segmentan las redes de forma que una falla sólo imposibilita las comunicaciones en un segmento.
- ***Eficiencia.*** Segmentando una red se limita el tráfico por segmento, no influyendo el tráfico de un segmento en el de otro.
- ***Seguridad.*** Creando diferentes segmentos de red se pueden definir distintos niveles de seguridad para acceder a cada uno de ellos, siendo no visible por un segmento la información que circula por otro.
- ***Dispersión.*** Cuando la conexión mediante repetidores no es posible debido a la excesiva distancia de separación, los puentes permiten romper esa barrera de distancias.

**Desventajas**

Algunas desventajas de la utilización de puentes se describen a continuación:

- En su concepción original, hoy en día los puentes se pueden considerar en la mayoría de los casos como obsoletos, pero la tecnología sigue siendo vigente en la utilización de los equipos de conmutación conocidos como switches.
- Son ineficientes en grandes interconexiones de redes, debido ala gran cantidad de tráfico administrativo que se genera.
- Pueden surgir problemas de temporización cuando se encadenan varios puentes.
- Pueden aparecer problemas de saturación de las redes por tráfico de difusión.

# Ruteadores

**Descripción**

Son dispositivos *inteligentes (toman decisiones, tienen procesador propio)* que trabajan en el Nivel de Red del modelo de referencia OSI, por lo que son dependientes del protocolo particular de cada red. Envían paquetes de datos de un protocolo común, desde una red a otra.

Convierten los paquetes de información de la red de área local, en paquetes capaces de ser enviados mediante redes de área extensa. Durante el envío, el ruteador examina el paquete buscando la dirección de destino y consultando su propia tabla de direcciones, la cual mantiene actualizada intercambiando direcciones con los demás ruteadores para establecer rutas de enlace a través de las redes que los interconectan. Este intercambio de información entre ruteadores se realiza mediante protocolos de gestión propietarios.

**Aplicaciones**

Por su posibilidad de segregar tráfico administrativo y determinar las rutas más eficientes para evitar congestión de red, son una excelente solución para:

- La interconexión de redes con múltiples tipos de LAN's *y/o* WAN's y diferentes protocolos.
- Creación de subredes.
- Conexión remota de redes *(por ejemplo la conexión a Internet).*
- Seguridad *(entradas, salidas).*
- Optimización de las rutas.
- Administración.

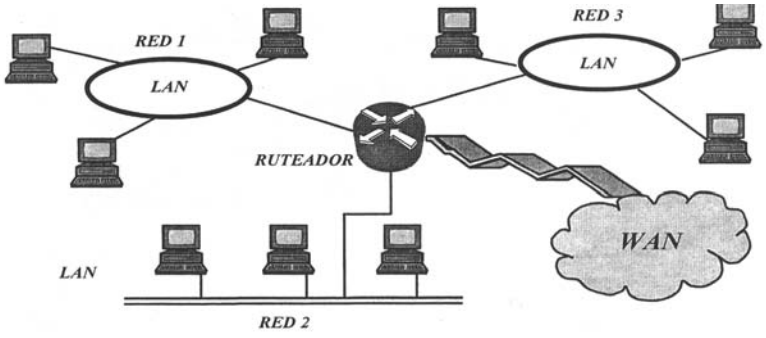



**Fig. 1.10** Interconexión de redes utilizando ruteadores

**Principales funciones de un ruteador**

Los ruteadores a diferencia de los puentes, trabajan en el nivel 3 de OSI y toman decisiones de encaminamiento.

Las prlnclpa es unciones que ha de realizar un ruteador son:

- ***Establecer un enlace entre LAN's***. Como mínimo se necesita un control de la conexión a nivel físico y de enlace.
- ***Establecer procedimientos de encaminamiento entre diferentes máquinas de diferentes LAN's.***
- ***Controlar la existencia y la disponibilidad de las redes de interconexión que permiten comunicar dos LAN's.***
- ***Proporcionar las siguientes funciones sin la necesidad de modificar la arquitectura de las LAN's conectadas, es decir de una manera transparente:***
- ***Gestión:***

  - De diferentes esquemas de direccionamiento empleados por las redes de interconexión.
  - De diferentes time-out *(evento que se presenta cuando un dispositivo de red espera escuchar a otro dentro de un periodo específico de tiempo, pero la respuesta no llega)* .

- ***Administración:***
  - Control del estado de las redes de interconexión.
  - Control de acceso, ya que cada red tiene sus propias técnicas de control de acceso a los usuarios.
  - Técnicas de encaminamiento que permiten evitar situaciones de congestión, y minimizar de alguna manera el costo en tiempo o en utilización de recursos.

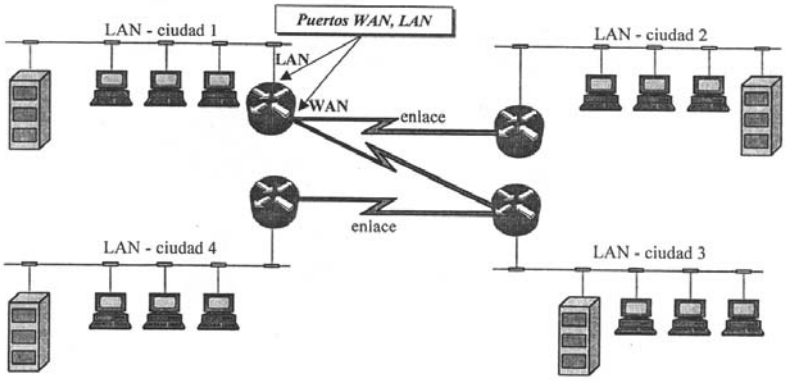



**Fig. 1.11** Ejemplo del uso de ruteadores

**Ventajas**

Algunas *ventajas* de la utilización de ruteadores, se describen a continuación:

- ***Seguridad***. Permiten el aislamiento de tráfico, y los mecanismos de encaminamiento facilitan el proceso de localización de fallos en la red.
- ***Flexibilidad.*** Las redes interconectadas con ruteador no están limitadas en su topología, siendo estas redes de mayor extensión y más complejas que las redes enlazadas con puente.
- ***Soporte de protocolos.*** Son dependientes de los protocolos utilizados, aprovechando de una forma eficiente la información de cabecera de los paquetes de red.
- ***Relación costo / beneficio.*** El costo es superior al de otros dispositivos, en términos de precio de compra, pero no en términos de explotación y mantenimiento para redes de una complejidad mayor.
- ***Control de flujo y encaminamiento.*** Utilizan algoritmos de enrutamiento adaptativos, que gestionan la congestión del tráfico con un control de flujo que redirige hacia rutas alternativas menos congestionadas.

**Desventajas**

Algunas *desventajas* que se presentan al utilizar ruteadores se listan a continuación:

- Lentitud de proceso de paquetes respecto a los puentes.
- Necesidad de gestionar el subdireccionamiento en el Nivel de Enlace.
- Precio superior a los puentes.

## Diferencias entre puentes y ruteadores

**Descripción**

- Aparentemente un puente y un ruteador realizan funciones de ruteo similares. La diferencia está en que ***un puente actúa* en *el nivel de enlace***, sólo redirige tráfico, y ***un ruteador* en *el nivel de red***, indica trayectos para el tráfico, por lo que ambos utilizan información completamente diferente para llevar a cabo su trabajo. Por ello, los métodos y algoritmos de ruteo son también diferentes.
- La función de puenteo es una función de la capa 2, por lo que *los puentes* ***utilizan las direcciones de Control de Acceso al Medio o de capa MAC*** asignadas por el fabricante del hardware. La función de ruteo es una función de la capa 3, por lo que ***los ruteadores utilizan direcciones lógicas*** asignadas por el administrador de red.
- Las direcciones de nivel de enlace, habitualmente la dirección MAC, son únicas para una determinada interfaz de red, dentro de un determinado nivel de red. Por ejemplo, las direcciones MAC de tarjetas Ethernet siempre son únicas. Las direcciones del nivel de red están compuestas de dos partes: una parte que identifica la red y otra que identifica un equipo o computadora dentro de esa red.
- Los puentes difieren de los ruteadores puesto ***que los puentes se valen de direcciones físicas***, mientras ***que los ruteadores utilizan direcciones IP***.

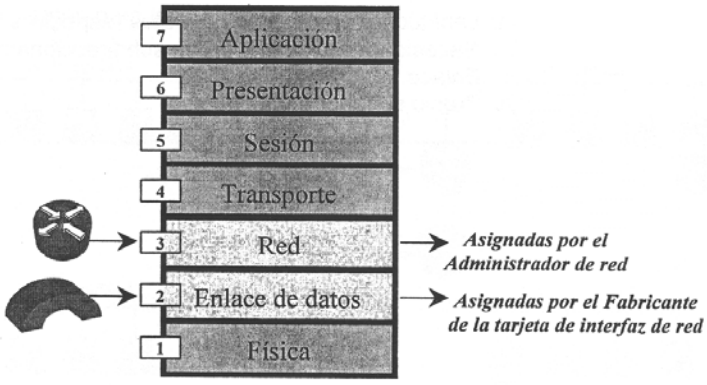



**Fig. 1.12** Ruteadores vs. Puentes

## Otros dispositivos de interconexión

**Descripción**

Como ya se mencionó anteriormente, los componentes que permiten realizar la interconexión de computadoras y redes son los repetidores, puentes, conmutadores, ruteadores y pasarelas.

En los temas anteriores se describieron los puentes y ruteadores, por lo que a continuación se dará una visión general de los demás dispositivos que también se pueden emplear para la interconexión de computadoras y redes.

**Repetidores**

Los *repetidores* solamente toman en cuenta las características físicas de la señal, de manera que los protocolos de enlace, red, etc., no se toman en cuenta. Su función básica es de amplificación de la señal eléctrica.

Un repetidor es un dispositivo que permite conectar dos segmentos de red. Esencialmente se trata de considerar dos segmentos de red como si fuese uno solo, salvando de esta forma las restricciones de distancias que establece el protocolo dado. Un repetidor recibe señales desde uno de los segmentos, las amplifica, marca los tiempos y las retransmite al otro segmento, esto en ambos sentidos. De esta forma se evita la pérdida que puede sufrir la señal en un cable demasiado largo o en un cable con demasiados dispositivos conectados, regenerándola señal original hacia el otro segmento.

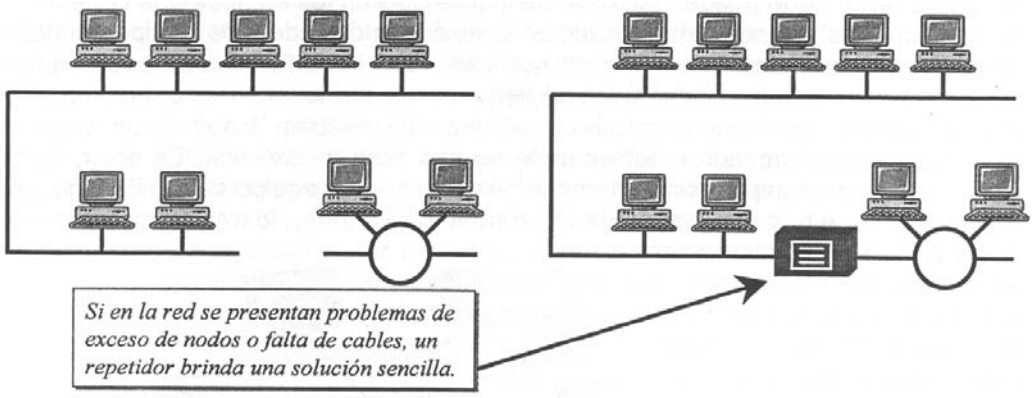



**Fig. 1.13** Ejemplo de la utilización de un repetidor

Un repetidor no realiza ninguna acción compleja sobre las señales que recibe. No es capaz de discriminar información, ni acumularla para conectar medios que tengan distintas velocidades. De manera que si recibe señales con errores, las amplifica y retransmite exactamente como él las ha recibido.

Aunque el uso de repetidores puede extender la longitud de la red, hay que tener ciertas precauciones al utilizarlos. Un repetidor simplemente retransmite todo lo que recibe de manera que al extender la red se está añadiendo a la misma todo el tráfico de las dos partes, con lo que resultará más fácil que ésta se sature. Así mismo, el número de repetidores que se pueden colocar es limitado. Suelen ser un elemento primordial en algunos tipos de comunicación como la comunicación inalámbrica o las comunicaciones ópticas, pero con el objetivo de salvar mayores distancias.

***Un repetidor sólo se puede utilizar para extender el tamaño de la red. Es como poder utilizar un cable mayor para conectar dispositivos.***

**Hub(concentrador)**

Un hub o concentrador es un elemento que ha evolucionado mucho con los años. Nace a partir de un elemento de concentración de cableado, principalmente, para redes del tipo CSMN/CD (utilizado por Ethemet). Los primeros concentradores no eran más que repetidores de señal, aunque ésta primera función ya permitía a los administradores de la red dividirla en segmentos diferenciados mejorando la gestión de la misma, aislando y controlando el tráfico. De ahí se pasa a los concentradores con cierta capacidad de gestión, que pueden informar de incidencias en los equipos que conecta.

Un concentrador recibe conexiones de todos los equipos conectadoS al mismo, de manera que existe una línea física entre cada equipo y el concentrador, el cual tiene un elemento interno, denominado plano posterior (backplane), al que se conectan todas estas conexiones, formando efectivamente un bus para todos ellos. Es decir, todos los equipos comparten ese bus. Cuando un equipo transmite algo, llega al bus, ya través de él se transmite a todos los equipos conectados al concentrador.

**Fig. 1.14** Ejemplo de la utilización de un concentrador *(hub)*

Con su evolución aparecieron concentradores con varios buses que permitían gestionar por separado varios segmentos de red. Y así han ido añadiendo más funcionalidad para convertirse en un elemento que continuación incorpora funciones que eran típicas de otros más complejos. En la actualidad la tendencia es a convertirse en elementos de interconexión para redes de alta velocidad.

El uso de los concentradores permite crear segmentos de equipos que, a su vez, se conectan con otros segmentos, bien a través de una jerarquía de concentradores, lo que pone a todos a un mismo nivel desde el punto de vista de la red, teniendo tan sólo en cuenta las temporizaciones máximas del protocolo, o bien, mediante puentes, ruteadores, etc.

***Un concentrador es el dispositivo apropiado para instalar una red local de forma rápida. Basta, básicamente, con conectar todas las computadoras al concentrador y configurar un protocolo y las direcciones de red.***

**Switch (conmutador)**

Los switches o conmutadores son componentes con una función en el nivel de enlace, como los puentes, y surgen como una evolución de los mismos *(de hecho, el switch se denomina puente multipuerto)*. En muchos casos, incluso, van ocupando el lugar en que antes se utilizaban puentes para la interconexión. Además de las funciones de los puentes, aportan mayor rendimiento, un mayor número de puertos, menor costo por puerto, mayor flexibilidad y funciones adicionales como el filtrado. Un switch es capaz de tomar decisiones, lo que implica que la LAN sea mucho más eficiente *(conmutan datos sólo desde el puerto al cual está conectado el host correspondiente)*.

Un switch y un hub tienen algunas similitudes, ya que los dos tienen varios puertos de conexión, dado que una de sus funciones es la concentración de conectividad (permitir que varios dispositivos se conecten a un punto de la red). El propósito del switch es concentrar la conectividad, lo que permite que la transmisión de datos sea más eficiente. El switch conmuta paquetes desde los puertos (las interfaces) de entrada hacia los puertos de salida, suministrando a cada puerto el ancho de banda total *(la velocidad de transmisión de datos en el backbone de la red)* .

En la representación del switch en la figura siguiente, las flechas indican las rutas individuales que pueden tomar los datos en un switch, a diferencia del hub, donde los datos fluyen por todas las rutas.

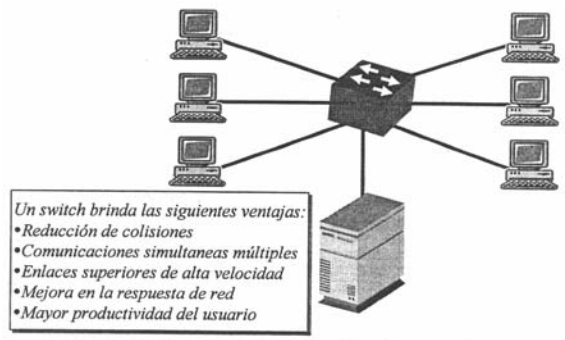



**Fig. 1.15** Ejemplo de la utilización de un switch

**Gateway**

Un gateway actúa en niveles superiores al de red, pudiendo llegar al nivel de aplicación. Se requiere de un gateway en aquellos casos en que la adaptación entre las dos redes requiera una conversión de los protocolos superiores al protocolo de red. Proporcionan conectividad entre redes de distinta naturaleza. Por ejemplo, si desde una red Novell se deseara acceder a computadoras en una red *SNA (System Network Architecture, Arquitectura de Redes de Sistema)*, se necesitaría un gateway que pudiese hacer la traducción completa de los protocolos Novell a los protocolos propios de la arquitectura SNA. El gateway estaría conectado a ambas redes como intermediario y tiene que implantar ambos protocolos completos. Sin embargo, esta adaptación a veces no es tan buena como uno desearía pues hay funciones de una arquitectura de red que la otra no es capaz de proporcionar, o viceversa. Al introducir un gateway se incrementa el retardo de transmisión de los mensajes entre ambas redes más que con los anteriores dispositivos de interconexión.

***Rara vez se requiere un gateway. Este tipo de dispositivos de interconexión se utiliza cuando los sistemas que hay que poner a funcionar conjuntamente siguen especificaciones diferentes, incluso desde el punto de vista del usuario.***

***Cabe aclarar que en IP, anteriormente gateway era un término que se referia a un dispositivo de enrutamiento. Actualmente, el término ruteador se utiliza para describir nodos que desempeñan esta función y gateway se refiere a un dispositivo especial que realiza una conversión de capa de aplicación de la información de una pila de protocolo a otro, como se mencionó anteriormente.***

# Protocolos TCP/IP

En toda comunicación entre dos computadoras existen varios esquemas de funcionamiento. Una comunicación entre computadoras no es más que un intercambio de información, que generalmente suele ser bidireccional. Estas formas de comunicación pueden seguir varios esquemas como son el jerárquico, el maestro / esclavo o el cliente / servidor. Estos esquemas definen de forma genérica el modo en el que se intercambia la información.

Internet, y en general las de comunicación modernas, utilizan el modelo cliente / servidor, el cual se basa en la asignación de roles alas entidades que participan en la comunicación de manera que uno pide información *(cliente)* y el otro la sirve *(servidor).*

El conjunto de protocolos TCP/IP ha sido de vital importancia para el desarrollo de las redes de comunicación, sobre todo para Internet. El ritmo de expansión de Internet también es una consecuencia de estos protocolos, sin los cuales, conectar redes de distintas naturalezas *(diferente Hardware, sistema operativo, etc.),* hubiera sido mucho más difícil, por no decir imposible. Así pues, podemos decir que los protocolos TCP/IP fueron y son el motor necesario para que las redes en general, e Internet en particular, se mejoren y se pueda lograr una buena "autopista de la información".

## Operación y arquitectura

El Protocolo de Internet *(IP)* y el Protocolo de Control de Transmisión *(TCP),* se desarrollaron inicialmente en 1973 por el informático estadounidense Vinton Cerf como parte de un proyecto y patrocinado por la Agencia de Programas Avanzados de Investigación *(ARPA)* del Departamento Estadounidense de Defensa *(DOD).*

Internet comenzó siendo una red informática del ARPA *(llamada ARPANET)* que conectaba redes de varias universidades y laboratorios de investigación en Estados Unidos. La idea inicial de la ARPA era crear una red descentralizada, que en el caso de un hipotético ataque nuclear ruso, pudiera seguir en funcionamiento, incluso en el caso de que alguna de sus partes fuera destruida. Esta idea inicial ha persistido hasta nuestros días. La materialización de la idea de descentralización se llevó a la práctica a través de dos protocolos. Inicialmente se utilizó NCP

*(Network Communication Protocol),* aunque las carencias del mismo se detectaron rápidamente y se sustituyó por TCP/IP *(Transmission Control Protocol/Internet Protocol)* .

Aunque la idea detrás de la implementación de TCP/IP era crear un protocolo escalable y adaptable a redes de grandes dimensiones, lo cierto es que dicha escalabilidad no contemplaba en ningún caso una red de la característica global que tiene Internet. En ningún caso TCP/IP se diseñó con la idea de que fuera el protocolo de lo que es el embrión de lo que serán las futuras superautopistas de la información.

**¿Qué es el modelo de capas TCP/IP?**

TCP/IP es el nombre que agrupa al conjunto de protocolos utilizado por las computadoras conectadas a Internet, permitiendo que éstas puedan comunicarse entre sí. En Internet se encuentran conectadas computadoras de clases muy diferentes, y con hardware y software incompatibles en muchos casos, además de todos los medios Y: formas posibles de conexión. Esto es una de las grandes ventajas del TCP/IP, ya que se encarga de que la comunicación entre todos sea , posible. TCP/IP, gracias al diseño que se realiza de su modelo de capas en las arquitecturas de comunicaciones, consigue abstraer las particularidades de cada computadora y su sistema operativo : asociado. Todos los sistemas operativos existentes en la actualidad, permiten la transmisión y recepción de información TCP/IP.

**Arquitectura**

***TCP/IP es una familia de protocolos*** cuya arquitectura comprende principalmente las capas 3 a 7 del modelo OSI, como se puede observar en la siguiente figura:

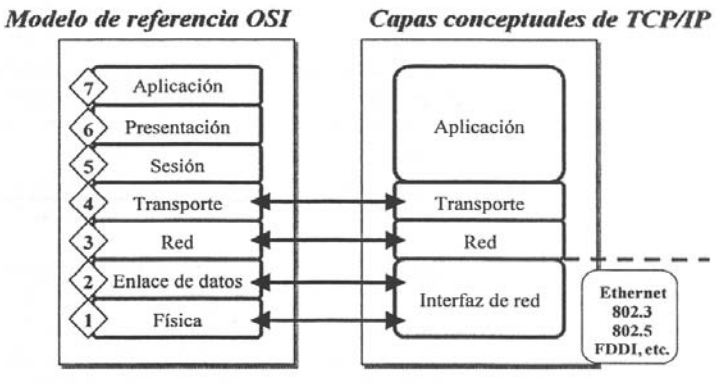



**Fig. 1.16** Comparación de arquitecturas OSI y TCP/IP

Donde:

- Las dos últimas capas se engloban en una sola, llamada de aplicación.
- TCP/IP ***no incluye una capa de sesión*** debido a que ésta es propia de los sistemas de tiempo compartido, que no se emplean en un medio como el de TCP/IP, caracterizado por su ***Modelo Cliente / servidor***.

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

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

**Modelo Cliente/ Servidor**

En toda comunicación entre dos computadoras existen varios esquemas de funcionamiento. Estos esquemas definen en forma genérica el modo en el que se intercambia información. TCP/IP se basa en el ***Modelo Cliente / servidor***, en donde cualquier dispositivo que inicia comunicaciones se llama ***Cliente*** y el dispositivo que responde, ***Servidor***.

En la siguiente figura se ilustra cómo el servidor responde *(sirve)* a las solicitudes del cliente:

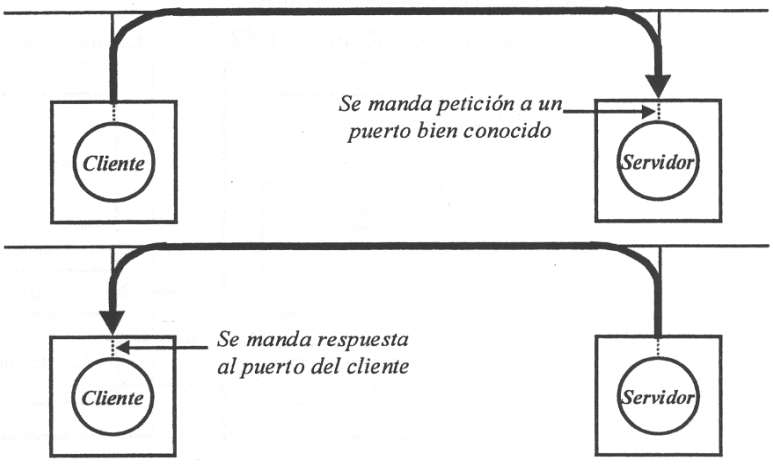



**FIG. 1.17** Modelo de interacción Cliente / servidor

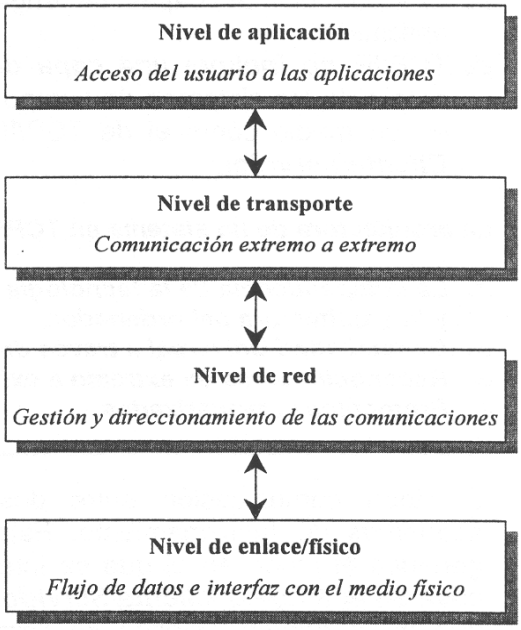



**Fig. 1.18** Arquitectura TCP/IP

En base a la figura anterior, a continuación se describen los niveles de la arquitectura de TCP/IP:

- **Aplicación**. Es la correspondencia con los niveles 5, 6 y 7 del modelo OSI (aplicación, presentación y sesión). Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de archivos (FTP), conexión remota (Telnet) y otros más recientes, como el protocolo HTTP (Hypertext Transfer Protocol) que proporciona el servicio de WWW (World Wide Web).
- **Transporte.** Coincide con el nivel de transporte del modelo OSI. En función de las características de la comunicación que se establece (orientada o no orientada a conexión) en este nivel coexisten dos protocolos TCP y UDP. Es el nivel encargado de determinar el tipo de servicio que se presta mediante la utilización del concepto de ***puerto***, el cual define el punto de acceso al servicio utilizado. En Internet cada aplicación tiene definido un puerto que se identifica mediante un número (número de puerto) en el nivel de transporte. Los ***números de puerto*** (definidos en RFC1700), se usan para enviar información a las capas superiores y para mantener un seguimiento de las distintas conversaciones que atraviesan la red al mismo tiempo. Tanto TCP como UDP usan números de puerto como se puede observar en la siguiente figura:

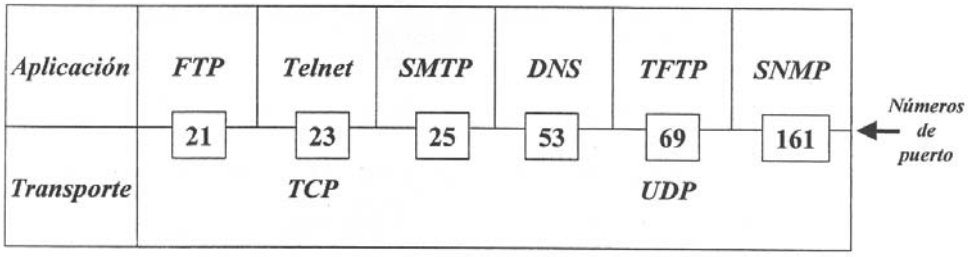



**Fig. 1.19** Números de puerto

***Puedes consultar los números de puerto reservados para TCP y UDP en el Anexo* 4.**

- ***Red.*** Coincide con el nivel de red del modelo OSI. Incluye al protocolo IP, que se encarga de enviar los paquetes de información a sus destinos correspondientes. Este nivel es el encargado de diferenciar unívocamente todas y cada una de las máquinas conectadas a Internet, mediante la asignación de una dirección IP (o dirección de red). Esta dirección es única para cada máquina conectada a Internet, lo cual indica uno de los mayores problemas de aplicabilidad que en la actualidad tiene el protocolo IP, ya que dichas direcciones se están agotando. La nueva versión de IP (IPv6) deberá solucionar este problema definitivamente.
- ***Enlace.*** Se encarga de realizar todas las operaciones relativas al transporte en sí de la información y de la compatibilidad de los formatos en los que se envía con los dispositivos y medios de transmisión por los que discurre. ***TCP/IP no especifica ningún protocolo concreto en el nivel***, por tanto, es tecnológicamente compatible con casi cualquier especificación para esa capa.

### Funcionamiento de los protocolos TCP/IP

Para entender el funcionamiento de los protocolos TCP/IP debe tenerse en cuenta la arquitectura que ellos proponen para comunicar redes. Tal arquitectura ve como iguales a todas las redes a conectarse, sin tomar en cuenta el tamaño de ellas, ya sean locales o de cobertura amplia, como se muestra en la siguiente figura:

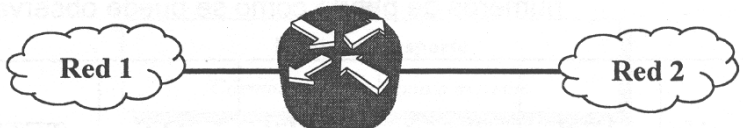



**Fig. 1.20** Arquitectura de interconexión de redes en TCP/IP

Esta arquitectura define que todas las redes que intercambiarán información deben estar conectadas a una misma computadora o equipo de procesamiento (dotados con dispositivos de comunicación), atales computadoras se les denominan ***compuertas***, pudiendo recibir otros nombres como ***ruteadores*** o ***puentes***.

### ¿Cómo funciona TCP/IP?

El TCP/IP necesita funcionar sobre algún tipo de red o de medio físico que proporcione sus propios protocolos para el nivel de enlace de Internet. Por este motivo hay que tener en cuenta que los protocolos utilizados en este nivel pueden ser muy diversos y no forman parte del conjunto TCP/IP. Sin embargo, esto no debe ser problemático puesto que una de las funciones y ventajas principales del TCP/IP es proporcionar una abstracción del medio de forma que sea posible el intercambio de información entre medios diferentes y tecnologías que inicialmente son incompatibles.

Para transmitir información a través de TCP/IP, ésta debe dividirse en unidades de menor tamaño, lo cual proporciona grandes ventajas en el manejo de los datos. En TCP/IP cada una de estas unidades de información recibe el nombre de datagrama. Los datagramas son conjuntos de datos que se envían como mensajes independientes.

### Ubicación de protocolos TCP/IP

La ubicación de la familia de los protocolos TCP/IP en las capas citadas se indica en la tabla siguiente:

| Capa | Protocolos | Función |
|---|---|---|
| ***Aplicación*** | *FTP File Transfer Protocol* | Permite la transferencia de archivos de un programa de aplicación que esté corriendo en una computadora a otro que esté corriendo en una computadora remota. |
| | *HTTP Hypertext Transfer Protocol* | El Protocolo de Transferencia de Hipertexto funciona con la WWW *(World Wide Web).* |
| | *SMTP Simple Mail Transfer Protocol* | Permite la transferencia de correo electrónico entre dos sistemas TCP/IP. |
| | *TELNET* | Permite a un sistema TCP/IP emular una terminal de otro sistema. |
| | *SNMP Simple Network Managment Protocol* | Se utiliza para administrar, monitorear y controlar una red de comunicaciones. |
| | *NFS Network File System* | Sistema de manejo de archivos. |

| Capa | Protocolos | Función |
|---|---|---|
| ***Transporte*** | *TCP Transport Control Protocol* | Es el protocolo de transporte orientado a conexión de la familia de protocolos TCP/IP. |
| | *UDP User Datagram Protocol* | Es un protocolo de transporte no orientado a conexión. |
| ***Red*** | *IP Internet Protocol* | Es el protocolo de ruteo de paquetes de la capa de red. Conjuntamente con TCP/IP, da nombre a esta familia de protocolos. |
| | *ICMP Internet Control Message Protocol* | Es el protocolo de la familia TCP/IP empleado para diagnosticar y probar redes TCP/IP y para reportar errores ocurridos en la red. |
| | *ARP Address Resolution Protocol* | Este protocolo se usa para traducir direcciones IP a direcciones MAC de la red LAN. |
| | *RARP Reverse Address Resolution Protocol* | Es un protocolo empleado para traducir direcciones físicas en la LAN a direcciones IP. |

## Protocolos enrutados VS. protocolos de ruteo

**Descripción**

Un *protocolo* es una descripción formal de un conjunto de reglas y convenciones que gobiernan la forma en la que los dispositivos de una red intercambian información.

Generalmente, existe confusión entre los términos ***protocolo enrutado (o enrutable)*** y ***protocolo de ruteo (o de enrutamiento)*** por lo que a continuación se describe cada uno, con la finalidad de comprender la diferencia fundamental que existe entre estos.

Para iniciar, podríamos pensar en una red con varios ruteadores y host, donde se tiene que resolver el problema de enviar paquetes de forma exitosa a través de la red aunque haya un ruteador fuera de servicio y aún así elegir siempre la mejor ruta restante a través de la red. Para lograr esto, se requeriría del uso de algún tipo de esquema de direccionamiento *(un protocolo enrutado)* además del medio para que los ruteadores se comuniquen entre sí *(un protocolo de ruteo).*

**Protocolo enrutado**

Los protocolos que suministran soporte para la capa de red se denominan *protocolos enrutados* (o *enrutables).* Este tipo de protocolos pueden ser enrutados por un ruteador y este debe poder interpretar la internetwork *(internet)* lógica según lo que especifica dicho protocolo.
Un protocolo de enrutado tiene las siguientes funciones:

- Define una dirección de origen y destino.
- Transporta la información en capa 3.
- Proporciona suficiente información en su dirección de capa de red para permitir que un paquete se envíe desde un host a otro tomando como base el esquema de direccionamiento.
- Define los formatos de campo y uso dentro de un paquete. Los paquetes generalmente se transfieren de un sistema final a otro.

**Ejemplos de protocolo enrutado:**

IP, AppleTalk, DECnet, IPX.

***Para que un protocolo sea enrutable debe brindar la capacidad para asignar un número de red, así como un número de host, a cada dispositivo individual.***
***El Protocolo Internet (IP) es un protocolo de la capa de red, y como tal se puede enrutar a través de una internetwork, que es una red de redes.***

**Protocolo de ruteo**

Partamos de la idea de que *ruteo* es el proceso de descubrimiento de una ruta hacia el host de destino. Entonces los ***protocolos de ruteo*** (o *de enrutamiento)* determinan las rutas que siguen los protocolos enrutados hacia los destinos *(logra el enrutamiento a través de la implementación de un algoritmo de ruteo específico).* De manera más sencilla, los protocolos de ruteo dirigen los protocolos de red a través de una interred.

***Ejemplos de protocolos de ruteo TCP/IP:***

RIP, IGRP, EIGRP, OSPF

***En el capítulo* 4 se *describe la función* y *caracteristicas de los protocolos de ruteo.***

## Protocolos de nivel de red

**El nivel de red**

El *nivel de red* tiene las siguientes características:

- Rutea los paquetes de la fuente al destino final a través de ruteadores intermedios. Tiene que saber la topología de la subred, evitar la congestión, y manejar los casos cuando la fuente y el destino están en redes distintas.
- Normalmente es la interfaz entre el portador y el cliente. Sus servicios son los servicios de la subred.
- La gran decisión en el nivel de red es si el servicio debiera ser orientado a la conexión o sin conexión:
    - ***Sin conexión (Internet)***. La subred no es confiable; porta bits y no más. Los hosts tienen que manejar el control de errores. El nivel de red ni garantiza el orden de paquetes ni controla su flujo. Los paquetes tienen que llevar sus direcciones completas de destino.
    - ***Orientado a la conexión (sistema telefónico).*** Los pares en el nivel de red establecen conexiones con características tal como la calidad, el costo, y el ancho de banda. Se entregan los paquetes en orden y sin errores, la comunicación es dúplex, y el control de flujo es automático.

El punto central en este debate es dónde ubicar la complejidad. En el servicio orientado a la conexión está en el nivel de red, pero en el servicio sin conexión está en el nivel de transporte.

A continuación se describen la función y características de los protocolos de este nivel.

### IP Protocolo Internet

***IP*** (Internet Protocol) es un protocolo no fiable y no orientado a conexión, base del funcionamiento del protocolo TCP/IP .

Este protocolo tiene como misión principal ocultar la complejidad de la capa de acceso al medio, creando una vista virtual de la red. IP fue diseñado para interconexión de redes, y se ocupa de la transmisión de bloques de datos, llamados datagramas de origen a destino, donde orígenes y destinos son hosts identificados por una dirección IP única, pero no garantiza que lleguen a su destino sin error, sin pérdida o sin duplicación.

El protocolo IP implementa dos funciones básicas: direccionamiento y fragmentación. El módulo Internet usa las direcciones contenidas en la cabecera de los datagramas para hacer llegar a estos a sus destinos. Así mismo, existen otros campos en la cabecera que permiten gestionar la fragmentación y posterior reensamblado de datagramas, para poder transmitir a través de redes que trabajen con tamaños de paquete pequeños.

### ICMP Protocolo de Mensajes de Control de Internet

***ICMP*** (Internet Control Message Protocol), es un protocolo que se utiliza para evaluar la disponibilidad de rutas hacia otras máquinas y para descubrir cierta información sobre la red.

Los ruteadores utilizan ICMP para enviarse mensajes sobre situaciones anómalas en la red o para enviar a determinadas computadoras información sobre nuevas rutas. Por tanto, ICMP es una de las partes integrales de IP que proporciona comunicación fuera de lo normal entre ruteadores, y entre ruteadores y computadoras. Un mensaje ICMP viaja en el campo de datos de un datagrama de IP.

Supongamos que un ruteador recibe un paquete que no puede enviar a su destino final, envía al origen un mensaje ICMP de destino inalcanzable al origen. Es posible que el mensaje no se pueda enviar porque no hay ninguna ruta conocida hacia el destino, como se observa en el caso de la figura siguiente:

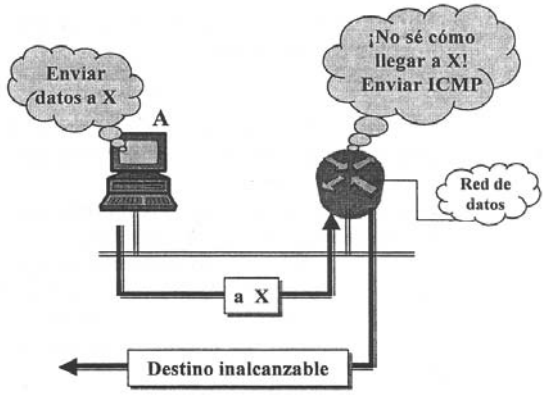



**Fig. 1.21** Ejemplo de funcionamiento de la prueba de ICMP

### Usos especiales de ICMP

Hay algunos programas especiales, como *Ping y Traceroute,* que hacen uso del protocolo ICMP:

- ***Ping***. Permite verificar si determinado destino puede ser alcanzado. Para ello este programa envía un mensaje ICMP de requerimiento de eco, espera por la réplica y luego reporta si el destino responde.
- ***Traceroute***. Permite encontrar todos los ruteadores a lo largo de una trayectoria a determinado destino. Para ello envía una serie de datagramas y espera respuesta de cada uno de ellos.

### Resolución de direcciones

Haciendo una revisión de varias tecnologías de redes físicas se puede decir que dos máquinas, en una red física, se pueden comunicar solamente si conocen sus direcciones físicas (también denominadas direcciones de hardware o direcciones MAC) de red.

Para que los dispositivos se puedan comunicar, los dispositivos emisores necesitan tanto las direcciones IP como las direcciones MAC de los dispositivos destino. Cuando tratan de comunicarse con dispositivos cuyas direcciones IP conocen, deben determinar las direcciones MAC. TCP/IP cuenta con el protocolo ***ARP***, que puede detectar automáticamente la dirección MAC, permite que una computadora descubra la dirección MAC de la computadora que está asociada con una dirección IP. El caso contrario, para encontrar la dirección IP de un dispositivo, TCP/IP cuenta con el protocolo ***RARP***. A continuación se describe cada uno de estos protocolos.

### ARP Protocolo de Resolución de Direcciones

***ARP*** (Address Resolution Protocol), es un protocolo muy importante para el funcionamiento de las redes. Su misión es identificar y relacionar las direcciones IP con las direcciones MAC. Esto resulta fundamental en redes de área local para identificar el destino de la transmisión. Existen numerosas ocasiones donde se conoce la dirección IP de destino, pero no la dirección hardware. En este caso se utiliza el protocolo ARP para enviar un mensaje de difusión por la red para preguntar por la dirección hardware asociada a la dirección IP ala que se quiere enviar el paquete.

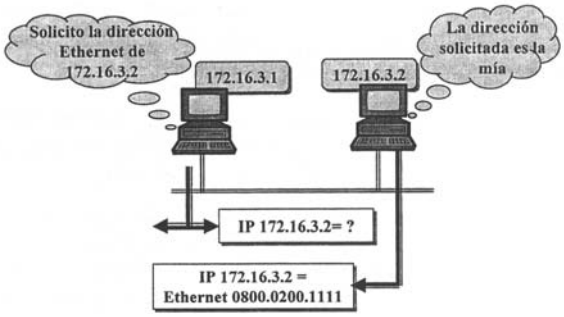



**Fig. 1.22** Ejemplo de funcionamiento de ARP (IP →MAC)

### RARP Protocolo inverso de asociación de direcciones

El protocolo RARP (Reverse Address Resolution Protocol) que es lógica inversa de ARP, usa la difusión de mensajes para determinar la dirección IP asociada con una dirección MAC en particular. Este protocolo, es en especial importante para los nodos sin disco, los cuales podrían no saber su dirección de internet al arrancar. Por ejemplo, cuando una estación sin unidad de almacenamiento arranca, envía ala red un mensaje multidifusión con su dirección física (obtenida directamente del hardware). El servidor de direcciones buscará la dirección física del solicitante y le enviará un mensaje indicándole su dirección IP.

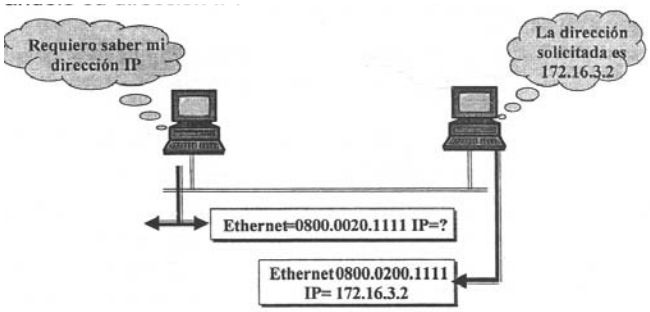



**Fig. 1.23** Ejemplo del funcionamiento de RARP (MAC → IP)

***ICMP, ARP y RARP son protocolos de control.***
***RARP depende de la presencia de un servidor RARP con una tabla de entrada u otro medio para responder a las peticiones.***

## Servicios sobre TCP/IP

### El nivel de aplicación

El ***nivel de aplicación*** proporciona la base para la utilización de numerosas aplicaciones que permiten que las redes TCP/IP presten un gran número de servicios que generan un gran valor añadido en torno al protocolo. Existen multitud de aplicaciones para este nivel, las cuales se diferencian entre sí porque manejan formatos de datos diferentes y tienen asignados números de puertos específicos y únicos para que el nivel TCP pueda distinguirlas sin problemas.

***La mayoría de las aplicaciones que operan en un entorno de red se clasifican como aplicaciones cliente / servidor, ya que cuentan con dos componentes que les permiten operar: el lado del cliente y el lado del servidor.***

### Transferencia de Hipertexto

El ***protocolo HTTP*** (Hypertext Transfer Pro tocol, Protocolo de Transferencia de Hipertexto) **proporciona el servicio WWW** que es el medio de comunicación entre computadoras más popular que existe en la actualidad, ya que permite la distribución masiva de textos, imágenes, audio, vídeo, aplicaciones, etc. , utilizando el modelo cliente/servidor entre máquinas situadas en cualquier parte del mundo con la utilización de Internet. Una de las principales razones del crecimiento sorprendente de la Web es la facilidad con la que se puede acceder a la información *(los hipervínculos hacen que la WWW sea fácil de navegar).*

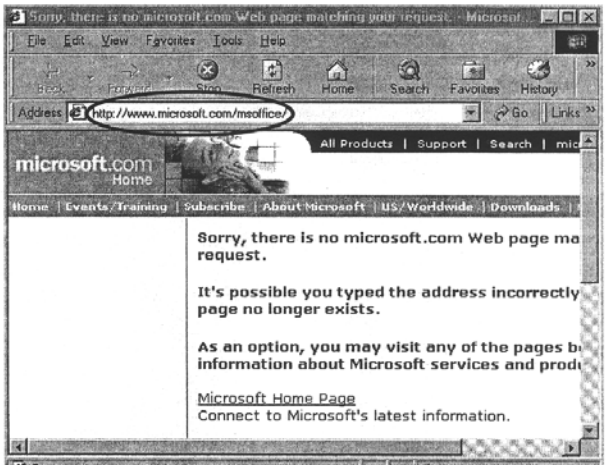



**Fig. 1.24** Pagina Web

De la figura anterior, las partes que comprenden la dirección son:

- ***http://*** indica al navegador cuál es el protocolo que debe utilizar.
- ***www*** indica al navegador con qué tipo de recurso desea conectarse.
- ***microsoft.com*** identifica el DNS de la dirección IP del servidor de Web.
- ***msoffice*** identifica la ubicación específica de la carpeta (en el servidor) que contiene la página Web.

**Transferencia de archivos**

FTP (File Transfer Protocol) es el protocolo que se utiliza para la ***transferencia de archivos*** entre máquinas. Aunque los usuarios algunas veces transfieren archivos por medio del correo electrónico, el correo está diseñado principalmente para mensajes cortos de texto. Los protocolos TCP/IP incluyen un programa de aplicación para transferencia de archivos, el cual permite que loS usuarios envíen o reciban archivos arbitrariamente grandes de programas o de datos. El sistema proporciona una manera de verificar que los usuarios cuenten con autorización o, incluso, de impedir el acceso.

La transferencia de archivos a través de una red de redes TCP/IP es confiable debido a que las dos máquinas comprendidas se comunican de manera directa, sin tener que confiar en máquinas intermedias para hacer copias del archivo a lo largo del camino.

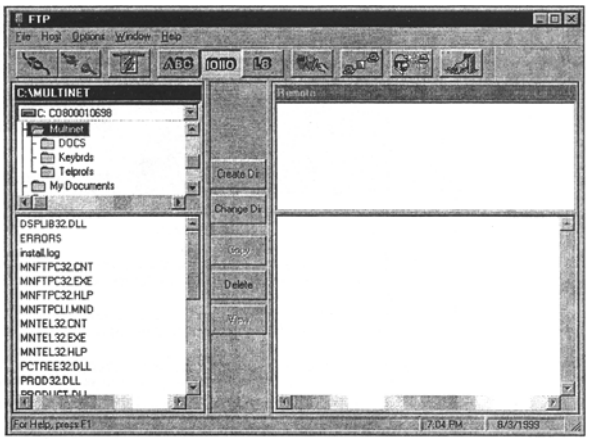



**Fig. 1.25** Ventana FTP para transferencia de archivos

FTP es una aplicación cliente/servidor al igual que el correo, electrónico y Telnet. Requiere software de servidor que se ejecuta en un host al que se puede acceder a través del software de cliente como se muestra en la siguiente figura:

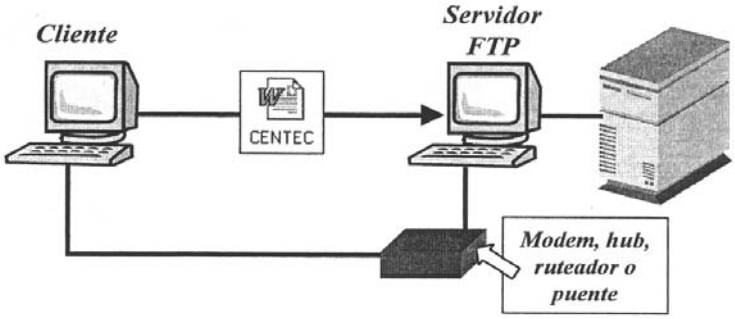



**Fig. 1.26** Sesion FTP

***Un servidor FTP suministra archivos que se pueden descargar desde el servidor y un lugar en el que se pueden cargar archivos del cliente.***

**Acceso remoto**

***Telnet*** es la aplicación que se utiliza para realizar sesiones remotas en máquinas que se encuentran alejadas. Con Telnet se pueden utilizar todas las capacidades de una máquina que puede estar situada a miles de kilómetros de distancia con la apariencia de estar frente a ella.

El ***acceso remoto:***

- Permite que un usuario que esté frente a una computadora se conecte a una máquina remota y establezca una sesión interactiva.
- Hace aparecer una ventana en la pantalla del usuario, la cual se conecta directamente con la máquina remota al enviar cada golpe de tecla desde el teclado del usuario a una máquina remota y muestra en la ventana del usuario cada carácter que la computadora remota genere.

Cuando termina la sesión de acceso remoto, la aplicación regresa al usuario a su sistema local.

Se considera al cliente de Telnet como una máquina local y al servidor de Telnet como un host remoto. Una sesión Telnet conecta una computadora cliente aun host para permitir que el cliente controle al host de forma remota, como se muestra en la siguiente figura:

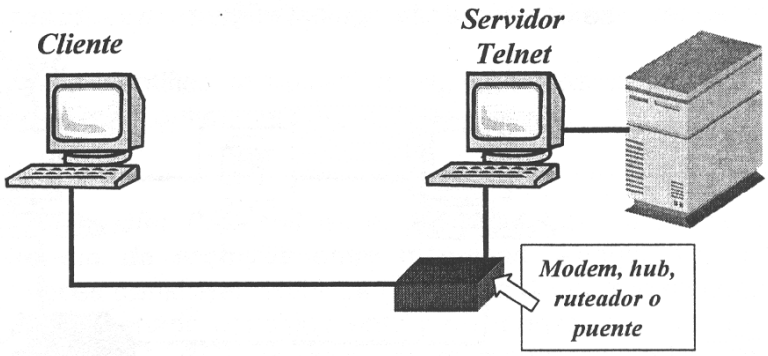



**Fig. 1.27** Sesión Telnet

Para realizar una conexión desde un cliente Telnet, se debe seleccionar una opción de conexión. Un cuadro de diálogo indica que se debe proporcionar:

- Un ***"Nombre de host"*** que es la dirección IP *(DNS)* de la computadora remota con la que desea conectarse.
- Un ***"Tipo de terminal"*** que describe el tipo de emulación de terminal que desea que la computadora ejecute.

Como se muestra en la siguiente figura:

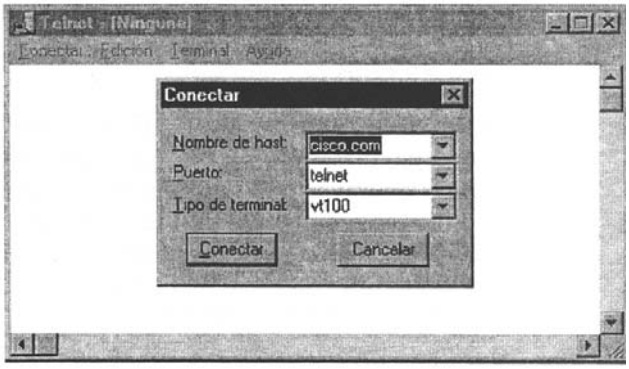



**Fig. 1.28** Cuadro de dialogo para realizar conexiones remotas

**Correo electrónico**

***SMTP*** *(Simple Mail Transfer Protocol),* es uno de los protocolos más antiguos establecidos para el modelo TCP/IP. Su misión es el ***envío*** y ***recogida de mensajes de correo electrónico.*** Este correo permite identificar a usuarios dentro de máquinas de manera unívoca y tiene posibilidades para envío de textos, aplicaciones, archivos de cualquier tipo, etc.

El proceso para enviar un mensaje por correo electrónico involucra dos procedimientos:

1. Enviar el mensaje de correo electrónico a la oficina de correos del usuario.
2. Entregar el mensaje desde esa oficina de correos al cliente de correo electrónico del usuario *(es decir, el destinatario).*

Como se muestra en la siguiente figura:

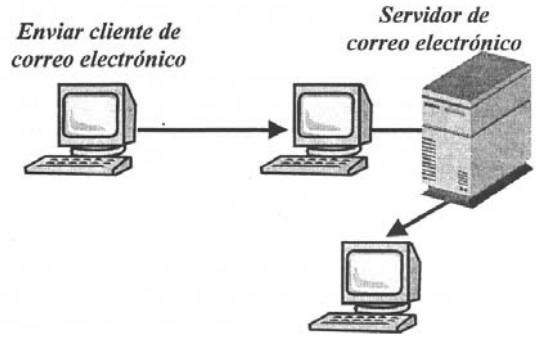



**Fig. 1.29** Proceso de envío de mensajes por correo electrónico

Aunque existen muchos sistemas de correo electrónico, al utilizar TCP/IP se logra que la entrega sea más confiable debido a que no se basa en computadoras intermedias para distribuir los mensajes de correo. Un sistema de entrega de correo TCP/IP opera al hacer que la máquina del transmisor contacte directamente la máquina del receptor. Por lo tanto, el transmisor sabe que, una vez que el mensaje salga de su máquina local, se habrá recibido de manera exitosa en el sitio de destino.

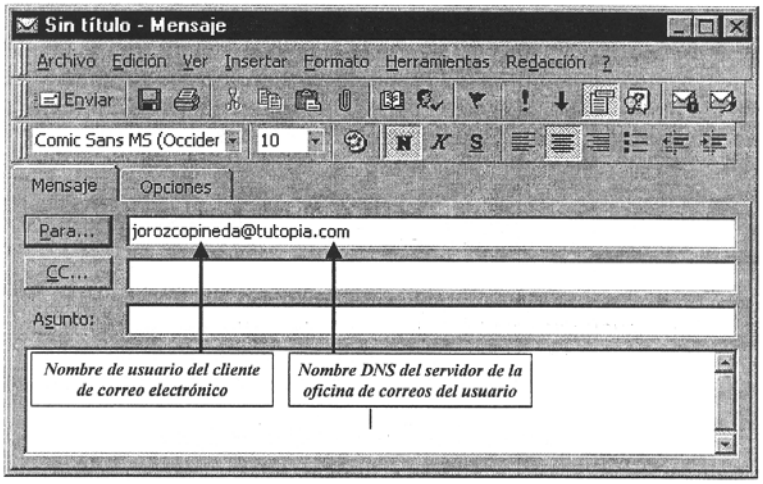



**Fig. 1.30** Mensaje de correo electrónico con dirección.

***En una dirección de correo electrónico el nombre del destinatario solo es importante una vez que el mensaje llega a la dirección de la oficina de correos, que es una entrada DNS que representa la dirección IP del servidor de la oficina de correos.***

### Otras aplicaciones

Dentro de las aplicaciones que se tienen disponibles se pueden diferenciar tres tipos que responden fundamentalmente a la oficialidad que tienen los estándares establecidos con respecto a las mismas. De esta manera se pueden distinguir los siguientes tipos de aplicaciones:

- Oficiales. Tienen oficialmente asignado un número de puerto que deben respetar todos los fabricantes y que tienen todas sus funciones e implementaciones oficial y públicamente establecidas a través de los correspondientes RFC.
- Propietarias. Tienen oficialmente un número de puerto asignado en la Internet Society, pero que no tienen protocolos públicos a través de RFC, ya que se trata de implementaciones propias de fabricantes como ocurre por ejemplo con el protocolo NFS ampliamente difundido en numerosos sistemas operativos.
- Experimentales. Son protocolos que utilizan números de puerto no oficialmente asignados para su funcionamiento temporal durante los períodos de prueba o, simplemente, para uso interno.

## SNMP (Protocolo Simple de Gestión de Red)

### Descripción

El ***protocolo SNMP*** (Simple Network Management Protocol), define un intercambio de información de ***gestión de redes*** basadas en TCP/IP, donde en la forma más básica existe un Sistema Manejador y un Sistema Manejado por medio de bases de datos de información. La simplicidad del mismo muy pronto dejó al descubierto deficiencias como: problemas para transferir grandes cantidades de información, poca ó ninguna seguridad, así como los débiles mecanismos de autenticación y privacidad.

### Sistema manejador de red

El punto principal de un Sistema manejador de red es un conjunto de aplicaciones que reúnen las necesidades para ejercer las funciones. Como mínimo un sistema incluirá aplicaciones básicas para desarrollar las funciones de monitoreo, control de configuración y administración de las cuentas de los usuarios. Sistemas más sofisticados podrían incluir aplicaciones más elaboradas para estas categorías y con más posibilidades para la corrección de las fallas.

### Manejador y Agente

La idea básica de una sistema manejador de red es la existencia de un *Manejador y un Agente* como se muestra en la siguiente figura:

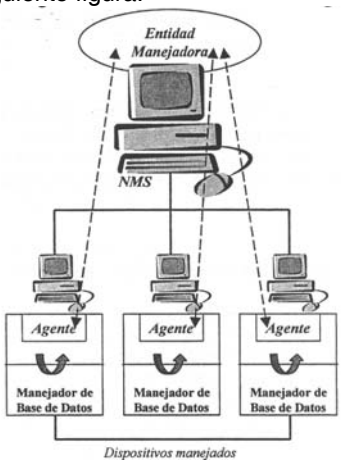



**Fig. 1.31** Sistema Manejador de Red (Manejador y Agente)

En base a la figura anterior:

- ***Manejador.*** En cualquier configuración, al menos un nodo Manejador posee un software que soporta SNMP. La estación Manejadora generalmente proporciona una interfaz al administrador de la red para controlar y observar los procesos de manejo de la misma. Esta interfaz permite al usuario realizar acciones *(desactivar un enlace, colectar estadísticas de un proceso determinado, etc.)* y proporcionar información general del sistema.
- ***Agente.*** Por otro lado los dispositivos de red a ser manejados, incluyendo servidores, estaciones de trabajo, computadoras personales, ruteadores, etc., son equipados con un módulo que incluye un software de Agente. El agente es responsable de:
    - Colectar y mantener información sobre su ambiente local.
    - Proporcionar información al Manejador de la red, ya sea en respuesta aun requerimiento o como un aviso de que algo anormal está ocurriendo.
    - Responder a los comandos ejecutados por el manejador para cambiar o alterar los parámetros de operación o configuración local.

Para realizar las funciones anteriores, cada Agente mantiene un MIB (Manejador de Información Básica) que contiene toda la información (tanto reciente como histórica) sobre su configuración local y el tráfico que maneja. La estación Manejadora mantendrá un MIB global con la información resumida de todos los agentes.

***Un NMS (Sistema de Administración de la Red):***

- ***Es un sistema que tiene la responsabilidad de administrar por lo menos parte de una red.***
- ***Generalmente es una computadora razonablemente potente y bien equipada, por ejemplo, una estación de trabajo de ingeniería.***
- ***Se comunica con los agentes para ayudar a realizar un seguimiento de las estadísticas y los recursos de la red.***

**SNMPv2**

Como realmente las capacidades de SNMP para el manejo básico de una red eran buenas, se decidió introducir esta nueva versión orientada a corregir las capacidades de transmisión de grandes cantidades de información, sin embargo seguía sin ofrecer solución alguna en cuanto a seguridad y privacidad se refiere. Con esta versión no se podía autenticar la fuente del mensaje de manejo y mucho menos proporcionar encriptación del mismo. En una red de gestión donde no exista o no sea posible la autenticación, hay probabilidades de que usuarios no autorizados fácilmente puedan ejercer tareas de manejo o más aún espiar información cuando ésta es pasada de un Sistema manejado aun Sistema manejador. Es por ello que muchas implementaciones en SNMPv1/SNMPv2 son limitadas a capacidades de " Sólo Lectura", lo que como consecuencia reduce las utilidades de control y monitoreo de la red.

**SNMPv3**

Para corregir las deficiencias de seguridad, de tanta importancia hoy en día con la evolución de Internet en el mercado, se reunió un grupo de trabajo que produjo una serie de estándares cuyo resultado es ***SNMPv3***. En estos documentos se definen las especificaciones de seguridad y control de acceso de las redes manejadas o gestionadas con SNMP, y que por supuesto incluyen las funcionalidades de las versiones SNMPv1 y SNMPv2.

SNMPv3 es un protocolo de manejo de red interoperable, que proporciona seguridad de acceso a los dispositivos por medio de una, combinación de autenticación y encripción de paquetes que trafican por la red. Las capacidades de seguridad que SNMPv3 proporcionan son:

- **Integridad del Mensaje.** Asegura que el paquete no haya sido violado durante la transmisión. .
- **Autenticación**. Determina que el mensaje proviene de una fuente válida.
- **Encripción**. Encripta el contenido de un paquete como forma de prevención.

# Interfaces

## Descripción

Hasta este momento, se han tratado los principios y conceptos que sustentan los protocolos TCP/IP sin especificar ***la interfaz que existe entre los programas de aplicación y el software de protocolo***.

En este tema describiremos el ejemplo de una interfaz entre programas de aplicación y protocolos TCP/IP. Es importante considerar los siguientes puntos:

- Debemos distinguir entre los protocolos de interfaz y el TCP/IP debido a que los estándares no especifican exactamente cómo es que interactúan los programas de aplicación con el software de protocolo. Por ello, la arquitectura de interfaz no está estandarizada, su diseño descansa fuera del campo de lo relacionado con el protocolo.
- En la práctica es inapropiado unir a los protocolos con una interfaz en particular pues ninguna arquitectura de interfaz funciona bien en todos los sistemas.
- En particular, como el software de protocolo reside en el sistema operativo de una computadora, los detalles de la interfaz dependen del sistema operativo.

### Conexión de red entre dos programas o procesos

La capa de transporte usa puertos de protocolo para identificar aplicaciones específicas o protocolos dentro de cada computadora host. De este modo cada proceso que usa la red en una computadora usa un puerto de protocolo como una dirección.

La ***conexión de red entre dos programas o procesos*** comprende lo siguiente:

- Un puerto de protocolo local que especifica la dirección donde un proceso recibe mensajes.
- Una dirección de host local que identifica la computadora que recibirá los paquetes de datos.
- Un puerto de protocolo remoto que identifica el proceso o programa destino.
- Una dirección de host remoto que identifica la computadora remota.
- Un protocolo que especifica cómo los programas transfieren datos a través de la red.

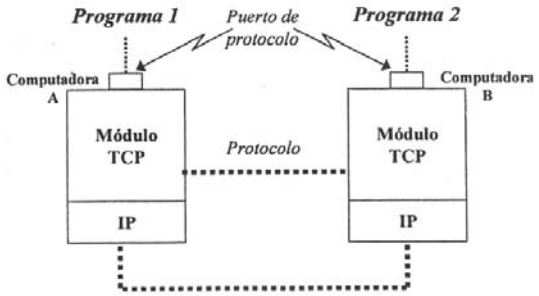



**Fig. 1.32** Conexión de red entre dos programas

**Concepto de socket**

En todas las áreas de la tecnología se tiende siempre a crear modelos simplificados o niveles que sean transparentes a usuarios de aplicaciones superiores. Con esta premisa surgió el paradigma “socket" popularizado por la Berkeley Software Distribution (BSD) de la Universidad de California, en Berkeley.

Este **socket**, o enchufe, consiste en un conjunto de órdenes para gestionar la transmisión de datos en cualquier aplicación o programa, pero a diferencia de lo ocurrido hasta entonces donde cada programador se hacia las suyas propias, se trata de un conjunto de órdenes standard común para todos los usuarios del entorno para el que es creado (en el caso de BSD se trata del entorno UNIX).

La combinación de dirección IP de host y el puerto TCP de la aplicación se llama una ***dirección de socket***. El **socket** es una representación abstracta de un extremo final en la comunicación entre dos procesos, como se muestra en la siguiente figura, donde para que ocurra la comunicación a través de una ***interlaz de socket***, un programa necesita un ***socket*** en cada extremo de la conexión de red:

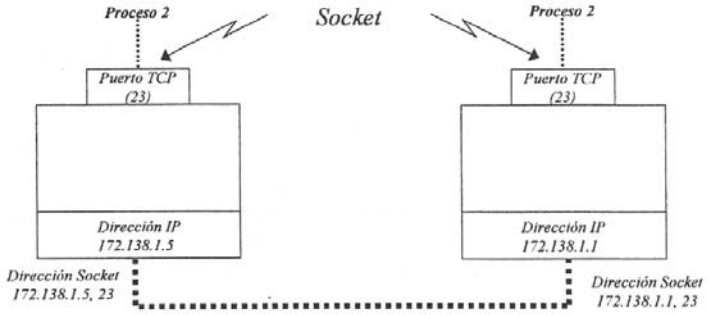



**Fig. 1.33** El Socket

**Interfaz de socket**

La ***intelfaz de socket*** es una ***API*** (Application Program Interfaces, Interfaz de Programación de Aplicaciones) para una red TCP/IP, y la API es un grupo de funciones de software o rutinas que permiten a un programador desarrollar aplicaciones para usarse en una red TCP/IP.

La interfaz de socket usa el método de open-read-write-close, que emplea el sistema operativo UNIX para las llamadas de sistema de entrada/salida. En este método, ***cuando un programador UNIX desea usar un archivo hace lo siguiente:***

1. Abre el archivo (open).
2. Comienza a leer o escribir (read/write).
3. Finalmente cierra el archivo (close).

En UNIX se siguen las mismas llamadas de sistema para accesar hardware, como impresoras, unidades de cinta y archivos; es decir, se mapea el hardware y archivos al sistema de archivos. Por lo tanto, ***para usar una red TCP/IP, un programa corriendo en una computadora realiza lo siguiente***:

1. Abre una comunicación de red (open).
2. Lee y escribe (read/write) datos a través de la conexión, es decir, hace la transferencia de datos.
3. Cierra la conexión (close).

Ahora bien ***para crear o abrir un archivo en UNIX***:

1. Se especifica una descripción del archivo, que incluye el nombre del archivo y cómo desea usar las operaciones de leer o escribir.
2. Solicita al sistema operativo un descriptor que identifique el archivo.
3. El sistema operativo responde a la llamada con un valor (un número entero) que identifica en forma única al archivo especificado.

***Hecha la descripción de cómo trabaja UNIX, se debe decir que la interfaz de socket opera del mismo modo.***

***Entre los Sockets existentes en la actualidad tenemos algunos que permiten la transmisión de datos tanto en una red de área local como por línea telefónica, de forma que se crea una conexión virtual entre el ordenador remoto que accede por módem y la red. Es posible trabajar de esta forma, como si estuviésemos conectados físicamente a la red, pudiendo recibir y mandar datos que tenemos en nuestro ordenador y haciendo uso de los programas que más se adapten a nuestras necesidades y gustos (como lo era por ejemplo Winsock).***

## Ruteo para IP

**Descripción**

El enrutamiento se refiere al proceso de determinar la trayectoria que un datagrama debe seguir para alcanzar su destino. A los dispositivos que pueden elegir las trayectorias se les denomina ruteadores. En el proceso de ruteo intervienen tanto los equipos como las compuertas que conectan redes *(recordar que el término compuerta es impuesto por la arquitectura TCP/IP de conexión de redes, sin embargo una compuerta puede realizar diferentes funciones a diferentes niveles, una de esas funciones puede ser la de enrutamiento y por tanto recibir el nombre de ruteador)*

**Destinos de un ruteador**

El tipo de ruteador más común (ruteador básico) posee información sobre cuatro tipos de destinos:

- Nodos directamente conectados a una de las redes a las que tiene conexión el ruteador.
- Nodos pertenecientes a otras redes de los que se proporciona información específica a los ruteadores.
- Nodos pertenecientes a redes remotas de los que el ruteador ha , .recibido un mensaje ICMP .
- Una dirección por defecto para todos aquellos paquetes para los .que el ruteador no tiene información de destino.

**Direcciones IP**

El protocolo IP usa direcciones lógicas para identificar alas computadoras que están conectadas en una red. Así mismo, un ruteador en una red toma como base la dirección destino en un datagrama para decidir a qué nodo debe transferirlo en la red. Más específicamente, una dirección IP se asigna a la tarjeta NIC, que conecta la computadora a la red, más que a la computadora misma.

Las direcciones IP tienen una longitud de 32 bits (4 octetos), y normalmente cada octeto de la dirección se convierte a un número decimal, y cada uno de estos números se separan por puntos, como se indica en el siguiente ejemplo (ver anexo 1):

| *11111000* | *10000010* | *00101011* | *00001001* |
|---|---|---|---|
| *248* | *130* | *43* | *9* |

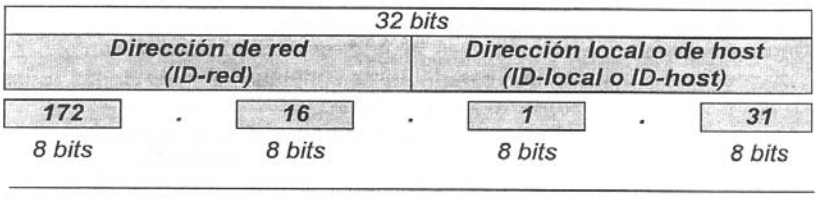
De modo que la dirección 11111000 10000010 00101011 00001001 se expresa en forma decimal como 248.130.43.9.

**Formato de una dirección IP**

El formato de una dirección IP está constituido por las dos partes siguientes:

- Dirección de red. Identifica a la red física a la cual está conectada la computadora, y es única a nivel internacional, por lo cual es asignada por Internet a través del NIC (Network Information Center) .
- Dirección local o de host. Identifica una computadora individual en la red y es asignada localmente por el administrador.

Y se distribuye como se muestra en el siguiente ejemplo:




Hay cinco clases de direcciones IP, según se muestra en la siguiente tabla:

| Clase | Descripción |
|---|---|
| A | Las direcciones comienzan con un número entre 1 al 127.<br>Usan 7 bits para identificar a la red *(el primer bit, del primer octeto siempre será 0)* y 24 bits para identificar al host dentro de la red, por lo que puede emplearse para direccionar hasta 127 redes *($2^7$– 1, ya que la dirección 00000000 no se emplea)* y 16'777,216 host *($2^{24}$)* en cada red.<br>0 \| Red \| Host<br>8 bits \| 24 bits<br>Así, en esta clase se tiene un pequeño número de redes con un gran número de computadoras conectadas. El alcance de los números de red son *1.0.0.0* a *126.0.0.0 (la red 0 está reservada para el sistema y la red 127 está reservada para el Loop Back).*<br>Actualmente ya no hay disponibilidad de esta clase de direcciones en Internet. |

| Clase | Descripción |
|---|---|
| *B* | Las direcciones comienzan con un número entre 128 al 191.<br>Estas direcciones tienen una cantidad media de redes y un número medio de computadoras en cada red. Específicamente usan 14 bits para identificar redes *(los primeros dos bits, del primer octeto siempre serán 10)* y 16 bits para identificar host dentro de cada red, por lo que se pueden tener 16,384 redes y 65,536 host en cada red.<br>10 \| Red \| Host<br>16 bits \| 16 bits<br>El alcance de los números de red son *128.1.0.0* a *191.254.0.0*.<br>Esta clase de direcciones está también prácticamente agotada en Internet. |
| *C* | Las direcciones comienzan con un número entre 192 al 223.<br>Estas direcciones dejan 21 bits para identificar la red *(los primeros tres bits, del primer octeto siempre serán 110)* y 8 bits para identificar los host dentro de la red, por lo que se pueden direccionar 2'097,152 redes *($2^{21}$)* y 256 host en cada red.<br>110 \| Red \| Host<br>24 bits \| 8 bits<br>El alcance de los números de red son *192.0.1.0* a *223.254.254.0*.<br>Aún hay disponibilidad de esta clase de direcciones en Internet. |
| *D* | Las direcciones comienzan con un número entre 224 al 239.<br>Esta clase de direcciones se emplean para multicast, es decir, para que un conjunto de computadoras compartan una misma dirección, lo cual permite que una copia de un mensaje con una dirección de multicast se entregue a cada una de las computadoras que comparten esta dirección. |

| Clase | Descripción |
|---|---|
| *E* | Las direcciones comienzan con un número entre 240 al 255.<br>Esta clase de direcciones se reservan para uso en el futuro. |

**Formato de las clases de direcciones IP**

A continuación se especifica más a detalle el formato de cada una de las cinco clases de direcciones IP, en base a lo descrito en el bloque anterior:

**Generalidades de las direcciones IP**

Es necesario destacar que:

- Una dirección que contiene sólo bits "1 " representa una dirección de broadcast, es decir, una dirección que todas las computadoras de red reconocen como suya.
- Así mismo, una dirección en la que todos los bits son "0" significa “esta computadora" o “esta red".

Por ejemplo, para la red 176.10.0.0, que es clase B, donde los últimos 16 bits forman el campo de host (o la parte de la dirección que corresponde al host), el broadcast que se debe enviar a todos los dispositivos de esa red incluye una dirección destino 176.10.255.255 (*ya que 255 es el valor decimal de un octeto que contiene 11111111*).

Revisemos los siguientes ejemplos para reafirmar el concepto:

| Para una dirección clase… | Broadcast |
|---|---|
| ***A***, por ejemplo 99.0.0.0 será un número reservado para una red. | 99.255.255.255 |
| ***B***, por ejemplo 156.1.0.0 será un número "de cable" de red reservado. | 156.1.255.255 |
| ***C***, por ejemplo 203.1.17.0 será un número de red reservado. | 203.1.17.255 |

***Consulta la información complementaria en el siguiente tema "Tipos de Broadcasting", donde se trata este tema con más detalle.***

**Subredes**

Consideremos el caso de una empresa a la que se le ha asignado una dirección de Internet de clase A o de clase B y que dispone de un espacio de direcciones bastante considerable; por ejemplo, si tiene una dirección de clase A tiene disponibles 16'777, 214 direcciones de host, o si es de clase B, 65,534, como ya se había mencionado anteriormente. La empresa puede subdividir el espacio de direcciones disponible de host en varios grupos, creando *subredes* dentro de la red global de la organización, con el propósito de:

- Evitar problemas de congestión en la red .
- Conservar moderado el tamaño de las tablas en un ruteador.
- La conveniencia de tener una red compleja, construida con base en varias redes LAN y WAN.

Las ventajas de crear subredes son:

- Mayor flexibilidad.
- Mayor eficiencia en el uso de las direcciones de red.
- Las redes de menor tamaño permiten la existencia de dominios de broadcast de menor tamaño, un aspecto importante para el diseño de red.

**Formato de las direcciones de subred**

Para instalar el concepto de subred, la dirección IP se extiende a las tres partes siguientes:

- Dirección de red o de Internet. Identifica ala red perteneciente a la empresa dentro del conjunto mundial de redes.
- Dirección de la subred (red física). Identifica a una red LAN o WAN particular dentro del conjunto de subredes de la organización.
- Dirección de host. Identifica aun host dentro de la subred.

Para la constitución de la parte de subred en una dirección IP, se usa una porción de los bits más significativos de la parte de la dirección de host para designar subredes, como se muestra a continuación:

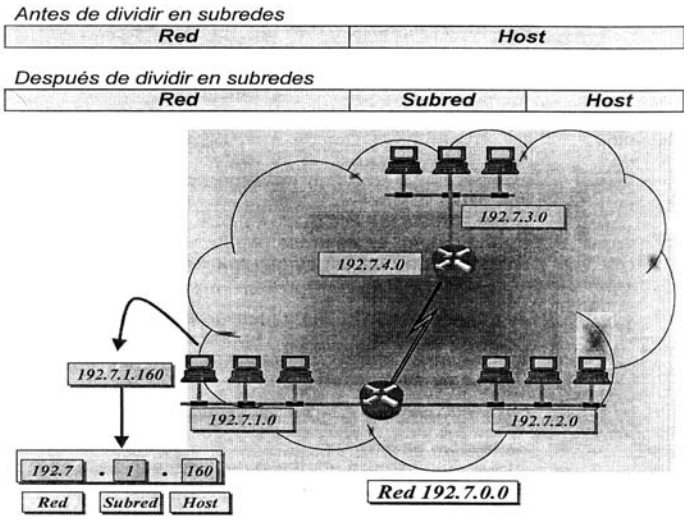



**Fig. 1.34** Subredes

**Mascara de subred**

El método que usa el software IP para marcar los bits de la dirección de host que son transformados en números de subred es conocido como ***máscara de subred***.

Los bits de la máscara de subred:

- Puestos a "0" corresponden al ID del host.
- Puestos a "1 " corresponden a la parte de red (red Internet o subred) .

La máscara permite la decodificación del número de la red dividida en subredes. Sin una máscara de subred, el número de subred no se puede usar para enrutar datos, ya que la máscara de subred le indica a los dispositivos de red cuál es la parte de una dirección que corresponde al campo de red y cuál es la parte que corresponde al campo de host.

Una máscara de subred tiene una longitud de 32 bits y tiene 4 octetos, al igual que la dirección de ret como se ilustra en el siguiente ejemplo:

| | Red | | Subred | Host |
|---|---|---|---|---|
| Notación binaria | 11111111 | 11111111 | 11111111 | 00000000 |
| Notación decimal | 255 . | 255 . | 255 . | 0 |

Se considera una buena práctica usar bits contiguos, comenzando por la izquierda, para valores de la máscara de subred, pero esto no es un requerimiento.

El propósito es determinar correctamente cuántos bits se pueden "robar" o "pedir prestados" a los campos de host para extender el número de red. El primer paso de este proceso es identificar que sí las máscaras no son definidas, el software IP toma las siguientes máscaras por omisión:

- Para direcciones clase **A: 255.0.0.0**
- Para direcciones clase **B: 255.255.0.0**
- Para direcciones clase **C: 255.255.255.0**

***Esto establece la máscara "mínima". La máscara máxima debe dejar por lo menos 2 bits para numerar los hosts.***

***Es importante aclarar que las máscaras indicadas para cada una de las clases de red, no crean ninguna subred.***

**Determina de ción de la máscara de subred**

Para determinar la máscara de subred para una dirección IP de subred particular, realiza lo siguiente:

| Paso | Acción |
|---|---|
| 1 | Expresa la dirección IP de subred en forma binaria. |
| 2 | Cambia la porción de red y subred de la dirección por todos unos. |
| 3 | Cambia la porción del host de la dirección por todos ceros. |
| 4 | Realiza la operación AND booleano *(el AND Booleano de un bit es similar a la multiplicación (0 AND 0 = 0, 0 AND 1 = 0, 1 AND 0 = 0, 1 AND 1 = 1).* |
| 5 | Convierte la expresión en números binarios nuevamente a la notación decimal punteada. |

***Ejemplo:***

| | Red | | Subred | Host |
|---|---|---|---|---|
| ***Dirección IP del host 172.16.2.120*** | 10101100 | 00010000 | 00000010 | 01111000 |
| ***AND*** | | | | |
| ***Máscara de subred 255.255.255.0*** | 11111111 | 11111111 | 11111111 | 00000000 |
| ***Subred*** | 10101100 | 00010000 | 00000010 | 00000000 |
| | 172 | 16 | 2 | 0 |

La máscara de subred por default para una red de Clase B sería 255.255.0.0 *(si no se pide ningún bit prestado)* que es el equivalente en notación decimal punteada de los 1's en los 16 bits que corresponden al número de red de Clase B. Si se pidieran prestados 8 bits para el campo de subred, la máscara de subred incluiría 8 bits 1 adicionales y se transformaría en 255.255.255.0.

En el ejemplo, si la máscara de subred 255.255.255.0 se asociara con la dirección de Clase B 172.16.2.120 (8 bits que se han pedido prestados para la división en subredes), el ruteador sabría que debe enrutar el paquete hacia la subred 172.16.2.0 en lugar de hacerlo simplemente a la red 172.16.0.0.

**Creación de subredes**

$$2^n-2$$

Con esta fórmula se pude determinar la cantidad de subredes o host que se pueden utilizar al crear subredes en una red, donde:

**n =** ***número de bits usados para determinar la cantidad de subredes*** *o* ***host que contendrá una red.***

Cuando se desean crear subredes, los bits de la máscara de subred provienen de los bits de mayor orden del campo de host, como se indica a continuación:

| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 | | |
|---|---|---|---|---|---|---|---|---|---|
| ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | | |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | = | 128 |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | = | 192 |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | = | 224 |
| 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | = | 240 |
| 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | = | 248 |
| 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | = | 252 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | = | 254 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | = | 255 |

**Ejemplo de creación de subredes**

Sea la dirección clase B: 170.250.0.0
Máscara de subred: 255.255.240.0
Que en binario es: 11111111 11111111 **1111**0000 00000000

¿Cuántas subredes y cuántos host es posible direccionar?
Hay 4 bits asignados a la mascarilla, así el número de subredes es:

$$2^n-2=2^4-2=16-2=14 \text{ subredes}$$

Y el número de host será:

$$2^{12}-2=4{,}096-2=4{,}094 \text{ host}$$

**Número de subredes y hosts para redes clase B**

La siguiente tabla muestra información para determinar el número de subredes y de hosts, así como la máscara de subred adecuada para las redes clase B:

| No. de bits | Máscara de subred | No. de subredes | No. de hosts |
|---|---|---|---|
| 2 | 255.255.192.0 | **2** $(2^2-2)$ | **16,382** $(2^{14}-2)$ |
| 3 | 255.255.224.0 | **6** $(2^3-2)$ | **8,190** $(2^{13}-2)$ |
| 4 | 255.255.240.0 | **14** $(2^4-2)$ | **4,094** $(2^{12}-2)$ |
| 5 | 255.255.248.0 | **30** $(2^5-2)$ | **2,046** $(2^{11}-2)$ |
| 6 | 255.255.252.0 | **62** $(2^6-2)$ | **1,022** $(2^{10}-2)$ |
| 7 | 255.255.254.0 | **126** $(2^7-2)$ | **510** $(2^9-2)$ |
| 8 | 255.255.255.0 | **254** $(2^8-2)$ | **254** $(2^8-2)$ |
| 9 | 255.255.255.128 | **510** $(2^9-2)$ | **126** $(2^7-2)$ |
| 10 | 255.255.255.192 | **1,022** $(2^{10}-2)$ | **62** $(2^6-2)$ |
| 11 | 255.255.255.224 | **2,046** $(2^{11}-2)$ | **30** $(2^5-2)$ |
| 12 | 255.255.255.240 | **4,094** $(2^{12}-2)$ | **14** $(2^4-2)$ |
| 13 | 255.255.255.248 | **8,190** $(2^{13}-2)$ | **6** $(2^3-2)$ |
| 14 | 255.255.255.252 | **16,382** $(2^{14}-2)$ | **2** $(2^2-2)$ |

**Ejercicio**

Determina en la siguiente tabla el número de subredes y de hosts, así como la máscara de subred adecuada para las redes clase C:

| No. de bits | Máscara de subred | No. de subredes | No. de hosts |
|---|---|---|---|
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| 6 | | | |

# Tipos de "Broadcasting"

**Descripción**

Los sistemas de difusión generalmente también ofrecen la posibilidad de dirigir un paquete a todos los destinos colocando un código especial en el campo de dirección. Cuando se transmite un paquete con este código, cada máquina en la red lo recibe y 10 procesa. Este modo de operación se llama difusión (broadcasting).

La difusión, es una capacidad presente en casi todos los protocotos de red que permite mandar un mensaje a todos los destinos de red posibles.

**Dirección broadcast**

Una dirección de broadcast es una dirección compuesta exclusivamente por números unos en el campo de host. Cuando se envía un paquete de broadcast en una red, todos los dispositivos de la red lo captan. Por ejemplo, en una red con un identificador 176.10.0.0, el mensaje de broadcast que llega a todos los hosts tendría la dirección 176.10.255.255.

Una dirección de broadcast es bastante similar al envío de correo masivo. El código postal dirige el correo hacia el área correspondiente, y la dirección de broadcast "Residente actual" vuelve a dirigir el correo hacia cada una de las direcciones. Una dirección IP de broadcast utiliza el mismo concepto. El número de red designa el segmento y el resto de la dirección le indica a cada host IP de esa red que éste es un mensaje de broadcast y que cada dispositivo debe prestar atención al mensaje. Todos los dispositivos en una red reconocen su propia dirección IP del host, así como la dirección de broadcast de la red.

**Tipos de broadcasting**

- ***Multicast (multidifusión)***. Modo de difusión de información en vivo que permite que ésta pueda ser recibida por múltiples nodos de la red y por lo tanto por múltiples usuarios. Algunos sistemas de difusión también contemplan la transmisión de un subconjunto de las máquinas, algo conocido como multidifusión. Un esquema posible consiste en reservar un bit para indicar multidifusión. Los restantes n-1 bits de dirección pueden contener un número de grupo. Cada máquina se puede "suscribir" a cualquier grupo o a todos. Cuando se envía un paquete a cierto grupo, se entrega a todas las máquinas que se suscribieron a ese grupo.

- **Unicast (unidifusión)**. Una dirección que solamente puede ser reconocida por un sistema anfitrión.

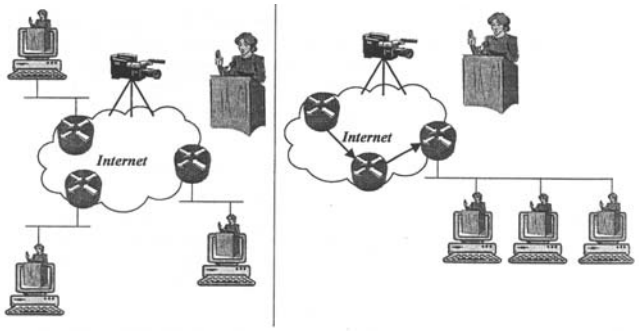



**Fig. 1.35** Transmisión multicast y unicast respectivamente

**Redes de broadcast**

Las ***redes de difusión*** (broadcast networks) es un tipo de medio de transmisión que agrupa a las computadoras cercanas geográficamente en medios de transmisión compartidos.

Estas redes hacen que muchas computadoras puedan compartir un i canal de transmisión común. Las computadoras envían paquetes a este canal de transmisión, que convenientemente identificados, se reciben por la máquina destino que los identifican como suyos y:

- En una red de broadcast la cuestión principal es cómo determinar quién usa un canal para er cual existe competencia. Los protocolos para esto pertenecen aun subnivel del nivel de enlace que se llama el subnivel de MAC (Medium Access Control, o Control de Acceso al Medio). Es muy importante en las LAN's, que normalmente usan canales de broadcast.
- Se puede asignar un solo canal de broadcast usando un esquema, estático o dinámico, como se describe a continuacion.
    - ***Asignación estática.*** Se usa algún tipo de multiplexación (MDF o MDT) para dividir el ancho de banda en N porciones, de que cada usuario tiene uno. Problemas:
        - Si menos de N usuarios quieren usar el canal, se pierde ancho de banda.
        - Si más de N usuarios quieren usar el canal, se niega servicio a algunos, aun cuando hay usuarios que no usan sus anchos de banda alocados.
- Porque el tráfico en sistemas computaciones ocurre en ráfagas, muchos de los sub canales van a estar desocupados por mucho del tiempo.
- ***Asignación dinámica.*** Usa el ancho de banda mejor. Hay muchos protocolos basados en cinco suposiciones principales:
    - ***Modelo de estación***. Hay N estaciones independientes que generan marcos para la transmisión. La probabilidad de generar un marco en el período delta t es lambda delta t, donde lambda es una constante. Después de generar un marco una estación hace nada hasta que se transmita el marco con éxito.
    - ***Canal único***. Hay un solo canal disponible para la comunicación. Todos pueden transmitir usándolo y pueden recibir de él.
    - **Choques**. Si se transmiten dos marcos simultáneamente, se chocan y se pierden ambos. Todas las estaciones pueden detectar los choques.
    - Tiempo continuo o dividido. En el primer caso se puede empezar con la transmisión de un marco en cualquier instante. En el segundo se parte el tiempo con un reloj de maestro que las transmisiones empiezan siempre al inicio de una división.

- Detección del portador o no. Las estaciones pueden detectar que el canal está en uso antes de tratar de usarlo, o no. En el primer caso ninguna estación tratará transmitir sobre una línea ocupada hasta que sea desocupada. En el último las estaciones transmiten y solamente luego pueden detectar si hubo un choque.

# Capítulo II
## Puentes y Switches

Algunos objetivos que se cubren con el uso de puente frente a una gran red son: una mayor fiabilidad, ya que si falla una de las redes la otra puede seguir funcionando, un mayor aislamiento de la información, manteniendo dentro de cada segmento el tráfico propio, un mayor rendimiento, al circular por cada segmento sólo el tráfico de dicho segmento, entre otras.

El puente no realiza ningún cambio al contenido o formato de las tramas que recibe. Tiene que tener cierta inteligencia, pues debe ser capaz de conocer qué direcciones de red existen en cada uno de los segmentos, de manera que pueda decidir si una trama debe retransmitirla al otro segmento o no. Incluso si existen más de dos redes o segmentos de red interconectadas por puentes, un puente debe conocer a qué direcciones se puede llegar, no sólo desde el otro segmento, sino atravesando otros puentes. Es en este punto donde surgen los distintos tipos de puentes y sus estrategias de funcionamiento, que se verán en este capítulo.

Un switch, al igual que un puente, es un dispositivo de la capa 2. De hecho, el switch se denomina puente multipuerto cuyo propósito es concentrar la conectividad, haciendo que la transmisión de datos sea más eficiente. El switch conmuta paquetes desde los puertos (las interfaces) de entrada hacia los puertos de salida, suministrando a cada puerto el ancho de banda total. Básicamente un switch es un administrador inteligente del ancho de banda.

## Fundamentos del puenteo y la conmutación

**¿Qué son los puentes y los switches?**

Los puentes y los switch es son dispositivos de comunicación de datos que operan, principalmente, en la capa 2 del modelo de referencia OSI Como tales, se les conoce ampliamente como dispositivos de la capa de enlace de datos. Estos dispositivos analizan las tramas entrantes, toman decisiones de envío con base en la información contenida en las tramas y envían las tramas a su destino.

La siguiente tabla muestra un panorama general de estos dispositivos:

| Puente | Switch |
|---|---|
| Estuvieron disponibles en el mercado a principios de los años 80. En ese entonces se usaban para conectar y habilitar el ruteo de paquetes entre redes homogéneas, más recientemente ya también ***el puenteo*** entre redes diferentes ha quedado definido y estandarizado.<br><br>Hay diferentes tipos de puentes que han resultado ser importantes como dispositivos de interconectividad de redes:<br><br>- El ***puente transparente*** que se presenta principalmente en entornos Ethernet.<br>- El ***puente de enrutamiento fuente*** que se utiliza sobre todo en entornos Token Ring. | Dispositivos de la capa de enlace de datos que, como los puentes, permiten la interconexión de múltiples segmentos físicos de LAN en una sola red de gran tamaño. Los switches envían y distribuyen el tráfico con base en sus direcciones MAC. Sin embargo, a pesar de que la función de ***conmutación*** se lleva a cabo en hardware y no en software, es significativamente más rápida. Los switches utilizan tanto la conmutación almacenar y enviar como la conmutación rápida para reenviar tráfico.<br><br>Hay muchos tipos de switches entre los que se cuentan:<br><br>- Los ***switches ATM.***<br>- Los ***switches LAN***.<br>- Varios tipos de ***switches WAN***. |

**Diferencias entre puentes y switches**

Aunque los puentes y los switches comparten los atributos más importantes, todavía existen varias diferencias entre ellos:

- Los **switches** son significativamente mas ve oces porque realizan la conmutación por hardware. Los **puentes** lo hacen por software y pueden interconectar las LAN de distintos anchos de banda *(por ejemplo, una LAN Ethemet de 10 Mbps y una LAN Ethernet de 100 Mbps se pueden conectar mediante un switch)*.
- Los **switches** pueden soportar densidades de puerto más altas que los puentes.
- Algunos **switches** soportan la conmutación rápida, que reduce la latencia y los retardos de la red. Los puentes soportan sólo la conmutación de tráfico de guardar y enviar.
- Los **switches** reducen las colisiones y aumentan el ancho de banda en los segmentos de red ya que suministran un ancho de banda dedicado para cada segmento de red.

**Puenteo y conmutación**

Hoy en día la ***tecnología de conmutación*** se ha convertido en la heredera evolutiva de las soluciones de interconectividad de redes basadas en el puenteo. Las implementaciones de conmutación dominan ahora las aplicaciones en las que se implementaron ***tecnologías de puenteo*** en diseños de red anteriores.

El desempeño superior del rendimiento eficiente total, la mayor densidad de puertos, un menor costo por puerto y mayor flexibilidad, han contribuido a que aparezcan los switches como una tecnología de reemplazo de los puentes y como complemento de la tecnología de ruteo.

***El puenteo y la conmutación se presentan en el nivel de enlace de ~ datos, que controla el flujo de datos, maneja los errores en la transmisión, proporciona el direccionamiento físico y administra el acceso al medio físico de transmisión.***

**Ventajas**

La transparencia de protocolos en las capas superiores es una gran ventaja tanto del puenteo como de la conmutación. Como ambos tipos de dispositivos trabajan a nivel capa de enlace, no es necesario que examinen la información de las capas superiores. Esto significa que tanto la función de puenteo como la de conmutación, pueden direccionar rápidamente el tráfico que represente cualquier protocolo de la capa de red. No es raro que un puente transfiera AppleTalk, DECnet, TCP/IP y otro tipo de tráfico entre dos o más redes.

**Operaciones básicas de los equipos de conmutación**

La conmutación es una tecnología que alivia la congestión, en las LAN Ethernet, reduciendo el tráfico y aumentando el ancho de banda. Los switches, también denominados switch es de LAN, a menudo reemplazan los hubs compartidos y funcionan con infraestructuras de cable existentes, de manera que su instalación puede realizarse con un mínimo de problemas en las redes existentes.

En la actualidad, en las comunicaciones de datos, todos los equipos de conmutación y de enrutamiento ejecutan dos operaciones básicas:

- Conmutación de tramas de datos: Esta es una operación de "guardar y enviar" en la que una trama llega aun medio de entrada y se transmite aun medio de salida.
- Mantenimiento de operaciones de conmutación: Los switch es crean y mantienen tablas de conmutación y buscan loops. Los ruteadores crean y mantienen tanto tablas de ruteo como tablas de servicios.

**Colisión**

Uno de los problemas que se puede producir, cuando dos bits se propagan al mismo tiempo en la misma red, es una colisión.

En las grandes redes hay muchos dispositivos conectados, donde se pueden producir problemas graves como resultado del exceso de tráfico en la red. Si hay solamente un cable que interconecta todos los dispositivos de una red, o si los segmentos de una red están conectados solamente a través de dispositivos no filtrantes (repetidores), puede ocurrir que más de un usuario trate de enviar datos a través de la red al mismo tiempo.

Ethernet permite que sólo un paquete de datos por vez pueda acceder al cable. Si más de un nodo intenta transmitir simultáneamente, se produce una colisión y se dañan los datos de cada uno de los dispositivos.

**Dominio de colisión**

El área dentro de la red donde los paquetes se originan y colisionan, se denomina **dominio de colisión**, e incluye todos los **entornos de medios compartidos** (un alambre puede estar conectado con otro a través de cables de conexión, transceptores, paneles de conexión, repetidores e incluso hubs).

Cuando se produce una colisión, los paquetes de datos involucrados se destruyen, bit por bit. Para evitar este problema, la red debe disponer de un sistema que pueda manejar la competencia por el medio (contención).

En general, se cree que las colisiones son malas ya que degradan el desempeño de la red. Sin embargo, una cantidad determinada de colisiones es una función natural de un entorno de medios compartidos (es decir, un dominio de colisión) ya que una gran cantidad de computadores intentan comunicarse entre sí simultáneamente, usando el mismo cable.

**Segmentación**

Se puede reducir el tamaño de los dominios de colisión utilizando dispositivos inteligentes de networking que pueden dividir los dominios (puentes, switches y ruteadores). Este proceso se denomina ***segmentación***.

Un puente puede eliminar el tráfico innecesario en una red con mucha actividad dividiendo la red en segmentos y filtrando el tráfico basándose en la dirección de la estación. El tráfico entre dispositivos en el mismo segmento no atraviesa el puente, y afecta otros segmentos. Esto funciona bien, siempre y cuando el tráfico entre segmentos no sea demasiado. En caso contrario, el puente se puede transformar en un cuello de botella, y de hecho puede reducir la velocidad de la comunicación. La mejor solución para este problema es la utilización de switches para la correcta segmentación de una ***LAN***.

**Motivos de la segmentación de las LAN**

Exiten dos motivos fundamentales para dividir una LAN en segmentos:

- Aislar el tráfico entre segmentos.
- Obtener un ancho de banda mayor por usuario, al crear dominios de colisión más pequeños.

Las LAN de gran tamano se congestionan rápidamente con tráfico y colisiones y virtualmente no ofrecen ningún ancho de banda. En este caso es conveniente dividir la LAN en dominios de colisión (unidades autónomas) utilizando dispositivos como, por ejemplo, puentes, switch es y ruteadores.

**Ventajas de la segmentación con puentes y switches**

Segmentar las redes de gran tamaño en unidades independientes, por medio de puentes y switch es ofrecen las siguientes ventajas:

- Reducción del tráfico que experimentan los dispositivos en todos los segmentos conectados ya que sólo se envía un determinado porcentaje de tráfico.
- Actúan como barrera de protección (firewall) ante algunos errores de red potencialmente perjudiciales.

- Aceptan la comunicación entre una cantidad de dispositivos mayor que la que se soportaría en cualquier LAN única conectada al puente.
- Extienden la longitud efectiva de una LAN, permitiendo la conexión de estaciones distantes que anteriormente no era posible.

## Arquitectura y funcionamiento de los puentes

**Arquitectura**

Cuando un puente entra en operación, la base de datos de retransmisión está vacía, posteriormente se llena y se mantiene dinámicamente durante la operación normal del puente. Así, cuando se recibe una trama, se lee la dirección fuente y el número de puerto del puente en el cual se recibió, y ambos datos se registran en la base de datos de retransmisión. Después, como al inicio de su operación el puente no conoce el puerto de retransmisión, envía una copia de esa trama por todos los otros puertos. Este procedimiento se repite en cada puente, lo que permite que cada uno de ellos construya su base de datos de retransmisión.

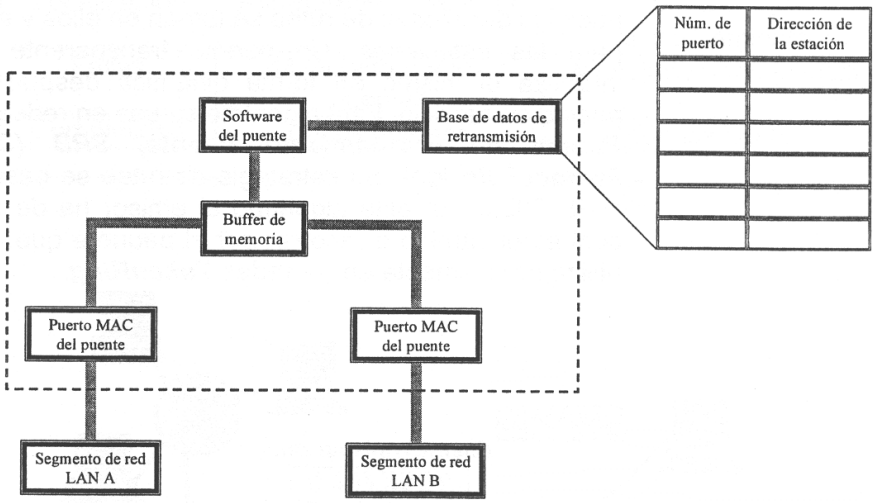



**Fig. 2.1** Arquitectura de un Puente

***El aspecto de los puentes varía enormemente según el tipo de puente. Aunque los ruteadores y los switches han adoptado muchas de las funciones del puente, estos siguen teniendo importancia en muchas redes. Para comprender la conmutación y el enrutamiento, primero se requiere comprender cómo funciona un puente.***

**Estrategias de ruteo de los puentes**

Un punto muy importante a considerar en el funcionamiento de los puentes, es su técnica de filtrado y envío (bridging) que utilizan, por lo cual los puentes se pueden clasificar en base a las estrategias de ruteo:

- ***Puente transparente, STP (Spanning Tree Protocol, Protocolo de Árbol en Expansión).*** Su estrategia de ruteo se basa en el algoritmo IEEE 802.1, llamado algoritmo de spahning free. En este algoritmo el puente toma todas las decisiones de ruteo, por lo cual la presencia de uno o más puentes entre dos estaciones que se comunican es transparente para ellas. Los puentes que utilizan el algoritmo de spanning tree se llaman ***puentes transparentes***, pues las decisiones de ruteo se toman en ellos y son transparentes para las estaciones. Un puente transparente se configura e inicializa él mismo en forma dinámica después de haber sido puesto en servicio. Este algoritmo se usa en redes Ethernet.

- ***Puente de Enrutamiento Fuente, SRB (Source Routing Protocol Bridge)***. Su estrategia de ruteo se basa en el algoritmo IEEE 802.5. En este algoritmo el emisor ha de indicar al puente cuál es el camino a recorrer por el paquete que quiere enviar. Se utiliza normalmente en las redes ***TokenRing.***

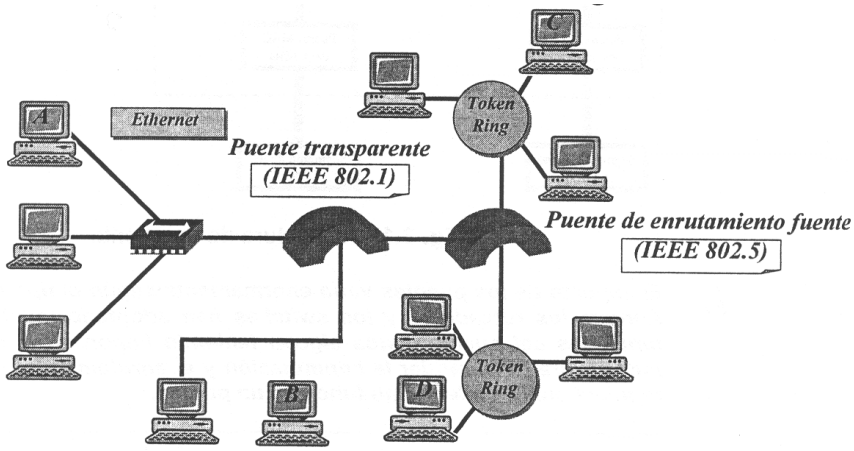



**Fig. 2.2** Clasificación de los puentes en base a estrategias de ruteo

**Comparación de los puentes**

La siguiente tabla muestra una comparación entre el puente transparente y el puente de enrutamiento fuente en base a diversos aspectos:

| Aspecto | Puente transparente | Puente de enrutamiento fuente |
|---|---|---|
| Orientación | Sin conexiones | Orientado a conexión |
| Transparencia | Completamente transparente | No transparente |
| Configuración | Automática | Manual |
| Enrutamiento | Subóptimo | Óptimo |
| Localización | Aprendizaje en reversa | Marcos de descubrimiento |
| Fallas | Manejado por los puentes | Manejado por los hosts |
| Complejidad | En los puentes | En los hosts |

# Algoritmo IEEE 802.1

**Introducción**

Como ya se mencionó anteriormente, el algoritmo ***IEEE 802.1*** *(algoritmo de spanning tree, árbol de expansión),* lo utilizan los puentes transparentes, por lo que a continuación abordaremos este tema, para después describir el algoritmo ya mencionado.

**Puentes transparentes**

Los puentes transparentes se utilizan normalmente en redes Ethernet y se denominan de esta forma porque para las computadoras conectadas a la red, es como si no existiesen. Para ellas es igual si están o si no están. Un puente transparente va aprendiendo la topología de la red, es decir, las direcciones hardware, por observación de los mensajes que se transmiten por ella.

**Operación de un puente transparente**

Cuando se conecta un puente transparente, inicialmente no tiene información de qué equipos están conectados a cada segmento de red. Cuando el puente lee un mensaje del segmento A de la red, por ejemplo, proveniente de la computadora 1, ya sabe que la computadora 1 está en el segmento A y añade esta entrada en la tabla, ver figura siguiente:

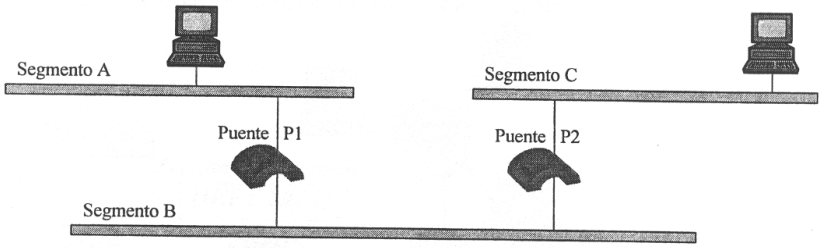



**Fig. 2.3** Aprendizaje de la red por un puente transparente

Cuando el puente recibe una trama para un determinado destino examina la tabla, si existe una entrada que indica dónde se encuentra el equipo de destino, lo envía a ese segmento de red. Si no se encuentra, retransmite la trama por todos los puertos de salida, excepto por el que se recibió la trama. De esta forma, en algún momento, el equipo de destino responderá, con lo que el puente recibirá una trama hacia la estación de origen, apuntando en la tabla el segmento donde está conectado dicho equipo. La próxima vez que se repita la comunicación ya sabrá dónde localizarle.

**Solución a problemas**

En una red grande, es normal que existan varios caminos entre dos estaciones. En este caso, el funcionamiento anterior de los puentes transparentes puede hacer que no se retransmitan los mensajes de manera oportuna, perdiéndose, o que se creen bucles de mensajes que pueden colapsar la red.

Sin embargo, las redes con múltiples caminos de comunicación son muy interesantes, pues permiten la comunicación aunque haya problemas en algunos de los puentes que conectan segmentos de red. Para que no ocurran problemas, en redes reales se utiliza otro tipo de algoritmos como el ***algoritmo del árbol de expansión***. De hecho, los puentes están obligados a implementar este algoritmo de acuerdo con la norma **IEEE 802.1**.

**Algoritmo de árbol de expansión**

El algoritmo de árbol de expansión se describe a continuación:

- Da identificadores únicos a los puentes, que puede ser su dirección MAC.
- Cada puerto del puente queda identificado por su identificador de puerto y la dirección MAC del puente.
- Se asigna a cada puerto un costo de trayecto. Al final se elegirá el trayecto cuyo costo sea el menor. Si el costo se asigna a uno, el costo de un trayecto es el número de saltos que hay que realizar.
- Se selecciona el puente con menor identificador como puente raíz. En realidad al principio todos se declaran raíz, estado que van cediendo por observación de los identificadores del resto.
- A continuación el resto de los puentes determinan cuáles de sus puertos que están conectados al puente raíz lo hace con el costo mínimo. A estos puertos se les denomina puertos raíz. Los puertos raíz son los únicos por los que se puede realizar la retransmisión de tramas. El resto de los puertos no retransmiten las tramas hacia el puente raíz. Si se encuentran dos trayectos con el mismo costo se elige el puente con un menor identificador.

- Los puentes van construyendo de esta forma los caminos hacia el puente raíz. Con esto se consigue que entre cada dos segmentos sólo exista un trayecto, ya que si existiese más de uno, uno de ellos quedaría bloqueado al no ser considerado el de menor costo.

Para llevar a cabo este proceso, los puentes intercambian información utilizando un tipo de tramas especiales denominadas Unidades de Datos del Protocolo de Puente (BPDU, Bridge Protocol Data Unit). Estas tramas contienen información sobre identificadores de puente y puerto, el puente raíz y el costo calculado hasta el puente raíz. Inicialmente todos los puentes consideran que el puente raíz son ellos mismos. Según van conociendo la identidad de otros puentes van indicando que el puente raíz es aquel que menor identificación tenga.

**Ejemplo de construcción de un árbol de expansión**

La siguiente figura muestra un ejemplo de cómo se construiría un árbol de expansión de la red. Para calcular el árbol de expansión, se ha seguido el algoritmo expuesto anteriormente:

1. Se selecciona el puente raíz como el puente número 1 que conecta la red A con la red B.
2. Para la red A, el puente que tiene acceso ala red C con costo mínimo es el puente 2, por lo que el puente 3 bloquea su conexión con la red A.
3. Para la red B, sólo existe el puente 4, que mantiene su conexión. El costo acumulado de llegar al puente raíz para el puente 2 es de 4 y para el puente 4 es de 2. Dos puertos raíz se han marcado con la letra R en su parte exterior.
4. Para la red D el costo por el puente 5 es de 5 (1 +2+2), que mantiene su conexión.
5. Para la red C el costo por el puente 2 (el puente 3 ya está bloqueado) es de 8 (4+4). El costo para el puente 5 es de 6 (1+1+2+2), por lo que se bloquea el enlace del puente 2 con la red C.

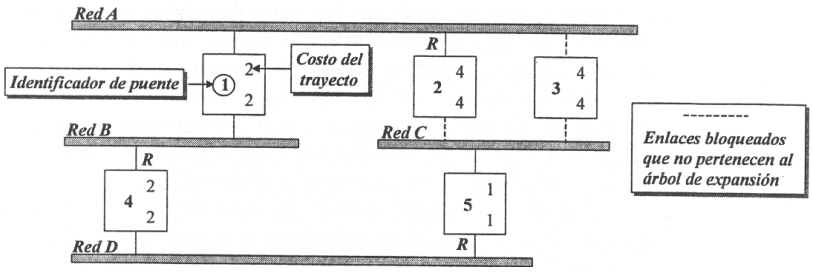



**Fig. 2.4** Redes locales conectadas con puentes y su árbol de expansión

Como se puede observar, en la red resultante, teniendo sólo en cuenta los enlaces sólidos, ya que los enlaces con línea discontinua no permiten el paso de información, no existen bucles.

# Algoritmo IEEE 802.5

**Introducción**

Como ya se mencionó anteriormente, el algoritmo **IEEE 802.5** *(Algoritmo Source Routing Bridge, enrutamiento fuente)*, lo utilizan los puentes de enrutamiento fuente, por lo que a continuación abordaremos este tema, para después describir el algoritmo ya mencionado.

**Puentes de enrutamiento**

En este tipo de enrutamiento es el equipo transmisor quien decide el trayecto que va a seguir el mensaje que emite. Los puentes recogen fuente los mensajes de los segmentos de red a los que están conectados y si alguna trama indica que el mensaje debe pasar por él lo retransmiten hacia el siguiente segmento de red indicado en la propia trama.

***En el enrutamiento fuente, es el nodo que envía la información quien determina la ruta que sigue la información hasta el nodo de destino, aunque tenga que atravesar varias redes.***

**Algoritmo de enrutamiento fuente**

En esencia, el enrutamiento desde el origen supone que el transmisor de cada marco sabe si el destino está en su propia LAN. Cuando la máquina de origen envía un marco a una LAN diferente, establece en 1 el bit de orden mayor de la dirección de origen, para marcarlo. Además, incluye en la cabecera del marco la trayectoria exacta que seguirá el marco. Esta trayectoria se construye como sigue:

Cada LAN tiene un número único de 12 bits, y cada puente tiene un número de 4 bits que lo identifica de manera única en el contexto de su LAN. Por tanto, dos puentes distanciados pueden tener el número 3, pero dos puentes entre las mismas dos LAN deben tener números de puente distintos. Entonces, una ruta es una secuencia de números de puente, LAN, puente. LAN,...Haciendo referencia a la siguiente figura, la ruta de A a D sería (L 1, B1, L2, B2, L3).

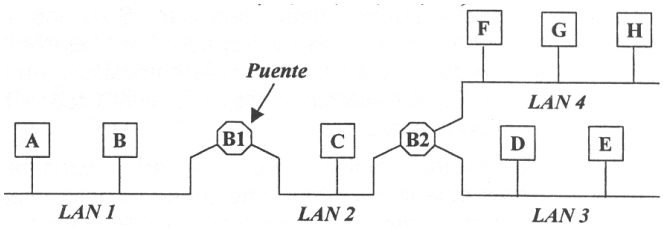



**Fig. 2.5** Ejemplo de la secuencia de una ruta

Un puente con enrutamiento fuente sólo está interesado en aquellos marcos que tienen el bit de orden mayor del destino puesto en 1. Para cada uno de tales marcos que ve, examina la ruta buscando el número de la LAN por la que llegó el marco. Si este número de LAN va seguido de su propio número de puente, el puente reenvía el marco a la LAN cuyo número sigue a su número de puente en la ruta. Si el número de la LAN entrante va seguido del número de algún otro puente, no reenvía el marco.

Implícito en el diseño del enrutamiento fuente está el hecho de que cada máquina de la interred conoce o puede encontrar la mejor trayectoria a todas las demás máquinas. La manera de descubrir estas rutas es una parte importante del algoritmo. El concepto básico es que, si el origen desconoce un destino, difunde un marco preguntando dónde está. Este marco de descubrimiento es reenviado por cada puente de modo que llegue a todas las LAN de la interred. Cuando regresa la respuesta, los puentes registran en ella su identidad, por lo que el transmisor original puede ver la ruta exacta que siguió y escoger la mejor.

**Posibles implementaciones del algoritmo**

Este algoritmo se presta para tres posibles implementaciones:

1. ***Software.*** El puente opera en modo promiscuo, copiando todos los marcos en su memoria para ver si tienen establecido en 1 el bit de orden mayor de destino. De ser así, se sigue examinando el marco, de otro modo, no se continúa la inspección.
2. ***Híbrida.*** La interfaz de LAN del puente inspecciona el bit de orden mayor del destino y sólo acepta los marcos que tienen el bit establecido. Esta interfaz es fácil de incorporar en el hardware y reduce de manera importante la cantidad de marcos que debe inspeccionar el puente.
3. ***Hardware.*** La interfaz de la LAN no sólo revisa el bit de orden mayor del destino, sino que también examina la ruta para ver si este puente debe reenviar. Sólo los marcos que sí deben reenviarse son entregados al puente. Esta implementación requiere del hardware más complejo, pero no desperdicia ciclos de CPU del puente, porque se filtran todos los marcos que no son pertinentes.

Estas tres implementaciones varían considerablemente en costo y desempeño. La primera no tiene un costo adicional de hardware por la interfaz, pero puede requerir una CPU muy rápida para manejar todos los marcos.

**Elementos del campo de directiva de ruta**

Para poder llevar a cabo el enrutamiento fuente, es necesario que los equipos sepan el camino que pueden seguir los mensajes hacia su destino. Para ello se utilizan mensajes especiales de descubrimiento de ruta. En el campo de directiva de ruta a seguir se pueden poner cuatro elementos distintos:

- ***Null.*** Indica que ningún puente debe retransmitir el mensaje. Por tanto, el mensaje debe estar dirigido a una computadora de la misma red que el emisor.
- ***Sin difusión***. En este caso, en el mensaje debe ir la ruta completa que debe seguir el mensaje. La ruta completa debe incluir los puentes y direcciones de red por los que debe pasar el mensaje, de manera que defina una ruta completa desde origen a destino.
- ***Con difusión.*** La trama llegará a toda la red a través de todos los puentes. La computadora de destino recibirá tantos mensajes como posibles caminos pueda seguir el mismo. En cada puente, al retransmitir la trama se añade información del puente que se ha utilizado y la red a la que se transmite. De esta forma, al llegar ala computadora de destino,-:ésta ya conoce la ruta que debe utilizar para responder a la computadora origen. La computadora de destino envía un mensaje de respuesta por cada mensaje recibido. Cuando la computadora de origen recibe todas las respuestas selecciona uno de los caminos, normalmente, el primero que recibe, pues será el más rápido.
- ***Con difusión única.*** La trama se envía ala red para que siga el árbol de expansión. Al seguir el árbol de expansión, la computadora de destino recibirá una única copia del mensaje. En cada puente se añade a la trama el camino que ha ido siguiendo, al igual que en el caso anterior. Cuando la computadora origen reciba respuesta a su mensaje, en él podrá encontrar la ruta completa para comunicarse con la computadora destino.

Evidentemente el caso de encontrar la ruta utilizando la difusión única genera muchas menos tramas en la red que el uso de difusión completa. Sin embargo, es necesario conocer con anterioridad el árbol de expansión de la red.

## Switches.

**Introducción**

Como ya mencionamos al principio del capítulo, los switches son dispositivos de enlace de datos que, al igual que los puentes, permiten que múltiples segmentos físicos de LAN se interconecten para formar una sola red de mayor tamaño. De forma similar a los puentes, los switches envían e inundan el tráfico con base a las direcciones MAC. Dado que la conmutación se ejecuta en el hardware en lugar del software, es significativamente más veloz. Se puede pensar en cada puerto de switch como un micropuente; este proceso se denomina microsegmentación. De este modo, cada puerto de switch funciona como un puente individual y otorga el ancho de banda total del medio a cada host.

***Como en el caso de los puentes, los switch es conectan segmentos de la LAN, usan una tabla de direcciones MAC para determinar el segmento en el que es necesario transmitir un datagrama y reducen el tráfico. Los switches operan a velocidades mucho más altas que los puentes y pueden soportar nuevas funcionalidades como, por ejemplo, las LAN virtuales.***

**Ventajas** Un switch brinda muchas ventajas como por ejemplo:

- Permitir que varios usuarios se comuniquen en paralelo a través del uso de circuitos virtuales y segmentos de red dedicados en un entorno libre de colisiones. Esto aumenta al máximo el ancho de banda disponible en el medio compartido.
- Desplazarse a un entorno de LAN conmutado es muy económico ya que el hardware y el cableado se pueden volver a utilizar.
- Los administradores de red tienen mayor flexibilidad para administrar la red a través de la potencia del switch y del software para configurar la LAN.

**Tipos de switches**

Existen varios tipos de switches entre otros:

- ***Switches ATM.*** Ofrecen una conmutación a alta velocidad y anchos de banda que pueden incrementarse en el grupo de trabajo, la troncal de la red corporativa y en un área de gran cobertura. Estos switches soportan aplicaciones de voz, video y datos y están diseñados para conmutar unidades de información de tamaño fijo (celdas), las cuales se utilizan en las comunicaciones de ATM.
- ***Switches LAN.*** Estos se utilizan para interconectar segmentos múltiples de LAN. La conmutación en LAN representa una comunicación dedicada, libre de colisiones entre los dispositivos de la red, que puede soportar múltiples conversaciones simultáneas. Estos switch es están diseñados para conmutar tramas de datos a altas velocidades.

**Switches LAN**

Los primeros ***switches LAN*** fueron desarrollados en 1990. Eran dispositivos de la capa 2 dedicados a resolver problemas de ancho de banda. Los más recientes están evolucionando hacia dispositivos multicapa capaces de manejar los problemas de protocolo asociados a las aplicaciones de gran ancho de banda que, históricamente, han sido resueltos por los ruteadores. En la actualidad, los switches LAN se están utilizando para reemplazar a los concentradores en el gabinete de cableado, ya que las aplicaciones de usuario están demandando un mayor ancho de banda.

Un switch LAN es un dispositivo que presenta una densidad de puertos mucho mayor, aun costo más bajo que los puentes tradicionales. Esto implica que los switches LAN pueden dar cabida a diseños de red que tengan un menor número de usuarios por segmento, incrementando así el ancho de banda promedio disponible por usuario.

***Para que los switches LAN se puedan usar no es necesario hacer cambios en los concentradores existentes, ni en las tarjetas de red ni en el cableado.***

**Propiedades de filtraje y envío**

Los switches de LAN se consideran puentes multipuerto sin dominio de colisión debido a la microsegmentación. Los datos se intercambian, a altas velocidades, haciendo la conmutación de paquetes hacia su destino. Al leer la información de Capa 2 de dirección MAC destino, los switch es pueden realizar transferencias de datos a altas velocidades, de forma similar a los puentes. El paquete se envía al puerto de la estación receptora antes de que la totalidad del paquete ingrese al switch. Esto provoca niveles de latencia bajos y una alta tasa de velocidad para el envío de paquetes.

***A la tendencia hacia un menor número de usuarios por segmento se le conoce como microsegmentación, la cual permite la creación de segmentos privados o dedicados (un usuario por segmento). Cada usuario recibe acceso instantáneo a todo el ancho de banda y no tiene que competir por el uso del ancho de banda disponible. Como resultado, no se presentan colisiones.***

**Red virtual dentro del switch**

La conmutación Ethernet aumenta el ancho de banda disponible en una red. Esto se hace creando segmentos de red dedicados, o conexiones punto a punto, y conectando estos segmentos en una red virtual dentro del switch. Este circuito de red virtual existe sólo cuando se deben comunicar dos nodos. Esto se denomina circuito virtual ya que existe sólo cuando es necesario y se establece dentro del switch.

Aunque el switch de LAN reduce el tamaño de los dominios de colisión, todos los hosts conectados al switch se encuentran todavía en el mismo dominio de broadcast, por lo tanto, un broadcast desde un nodo será visto por todos los demás nodos conectados a través del switch de LAN.

**Segmentación con switches**

El propósito de la conmutación de LAN es aliviar las insuficiencias de ancho de banda y los cuellos de botella de la red como, por ejemplo, los que se producen entre un grupo de PCs y un servidor de archivos remoto. Un switch de LAN es un puente multipuerto de alta velocidad que tiene un puerto para cada nodo, o segmento, de la LAN. El switch divide la LAN en microsegmentos, creando de tal modo dominios libres de colisiones a partir de un dominio de colisión que antes era de mayor tamaño.

**Reenvío en la conmutación LAN**

Los switch es LAN se pueden caracterizar por el método de reenvío que soportan:

- En el ***método de conmutación almacenar y enviar*** se verifican los errores y se eliminan las tramas erróneas. Con este método el switch LAN:
    1. Copia toda la trama en sus memorias de almacenamiento que están sobre la propia tarjeta y calcula la CRC (Verificación de la Redundancia Cíclica).
    2. La trama se elimina si contiene un error en la CRC o si es una **trama pequeña** (menos de 64 bytes incluyendo la CRC) o una **trama grande** (más de 1518 bytes incluyendo la CRC).
    3. Si la trama no contiene ningún error, el switch LAN mira la dirección destino en su tabla de conmutación o de envío y determina la interfaz de salida. Después envía la trama hacia su destino.

- En el método de conmutación rápida de paquetes, la latencia se reduce eliminando la verificación de errores. Con este método el switch LAN :
    1. Copia solamente la dirección destino en sus memorias de almacenamiento sobre la misma tarjeta.
    2. Posteriormente, mira la dirección destino de su tabla de conmutación, determina la interfaz de salida y envía la trama hacia su destino.

***Un switch que utiliza la conmutación rápida presenta una latencia muy pequeña ya que empieza a enviar la trama tan pronto como lee la dirección destino y determina la interfaz de salida.***

**Ancho de banda de la conmutación LAN**

Los switch LAN también pueden ser caracterizados de acuerdo con la proporción de ancho de banda que se asigne a cada puerto:

- La ***conmutación simétrica*** ofrece una distribución equitativa del ancho de banda de cada puerto. Un switch simétrico presenta conexiones conmutadas entre puertos con el mismo ancho de banda. Este tipo de conmutación se optimiza para una gran carga de tráfico distribuida de manera razonable.
- La ***conmutación asimétrica*** presenta una distribución diferente, o desigual, del ancho de banda entre algunos puertos. Un switch LAN asimétrico ofrece conexiones conmutadas entre puertos con diferente ancho de banda (por ejemplo, combinaciones 10Base T y 100Base T). Este tipo de conmutación está optimizada para flujos de tráfico cliente / servidor donde varios clientes se comunican con un servidor al mismo tiempo, lo que requiere más ancho de banda dedicado al puerto del servidor para evitar ahí un cuello de botella.

***Un administrador de red debe evaluar la cantidad de ancho de banda que se requiere para las conexiones entre dispositivos, para acomodar el flujo de datos de aplicaciones de red cuando decida seleccionar un switch asimétrico o simétrico.***

**El switch LAN y el modelo de referencia OSI**

Los switch es LAN se categorizan de acuerdo con la capa OSI en la que filtran y envían o conmutan las tramas:

- Un switch LAN de la capa 2 es similar a un puente multipuerto desde el punto de vista operativo, pero tiene una capacidad mucho mayor y soporta muchas nuevas características, como la operación dúplex total. Este switch desempeña conmutación y filtrado con base en la dirección MAC de la capa de enlace de datos de 081 (capa 2). Como con los puentes, es completamente transparente a los protocolos de red ya las aplicaciones de usuario.
- Un switch LAN de la capa 2 con características de la capa 3 puede tomar decisiones de conmutación con base en más información que solamente la dirección MAC de la capa 2. Dicho switch debe incorporar algunas características de control del tráfico de la capa 3, como la administración del tráfico de multidifusión y difusión, seguridad a través de listas de acceso y fragmentación IP.
- Un switch multicapa toma decisiones de conmutación y filtrado con base en direcciones de la capa de enlace de datos de 081 (capa 2) y direcciones de la capa de red (capa 3). Este tipo de switch decide dinámicamente si comutar (capa 2) o rutear (capa 3) el tráfico entrante. Además este switch conmuta un grupo de trabajo y rutea entre diferentes grupos de trabajo.

# Capítulo III
## Configuración de Ruteadores

El ruteador es la herramienta básica para conectar redes entre sí. Se trata de dispositivos inteligentes que seleccionan las rutas de conexión óptimas entre el remitente y el destinatario para garantizar que el tráfico fluya sin problemas. Cuando un ruteador detecta problemas en una ruta particular, rutea nuevamente los paquetes por otra trayectoria óptima. Pero el tráfico en Internet se expande últimamente a una tasa vertiginosa de 20% mensual, lo cual está haciendo que el trabajo de los ruteadores sea cada vez más difícil. La infraestructura de Internet se ha vuelto un rompecabezas de miles de ruteadores y switches conectados por una inmensa malla de líneas de fibra, líneas arrendadas y conexiones basadas en paquetes, todo ello sufriendo bajo el peso del tráfico de los usuarios.

## Ruteo de paquetes

**Descripción**

La función más importante de la capa de red es la de conducir los paquetes de datos de la fuente al destino. Designaremos esta función con el nombre de ruteo, y al equipo que la realiza con el de ruteador. Así, el ruteo es el proceso de descubrir, seleccionar y emplear la mejor trayectoria o camino para transmitir un paquete de datos de un nodo a otro en una red.

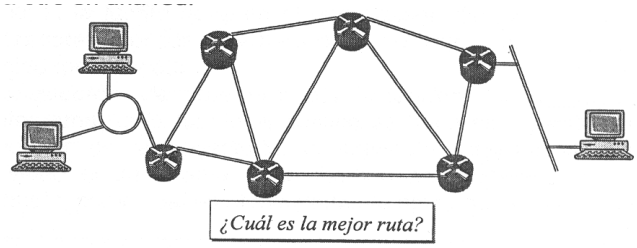



**Fig. 3.1** Función del ruteador

**Datagrama IP**

El protocolo IP es la implementación más popular de un esquema de direccionamiento de red jerárquico. A medida que la información fluye por las distintas capas del modelo OSI, los datos se encapsulan en cada capa. En la capa de red, los datos se ***encapsulan*** en datagramas también conocidos como ***datagramas IP*** (unidad básica de transferencia en una red de redes TCP/IP).

El **datagrama IP** se subdivide en dos secciones principales:

- ***Encabezado***. IP determina la forma del encabezado del datagrama, el cual contiene la información que controla hacia dónde y cómo es enviado el datagrama.
- ***Área de datos***. IP no se ocupa de los datos en sí, es decir, no especifica el formato de ésta sección.

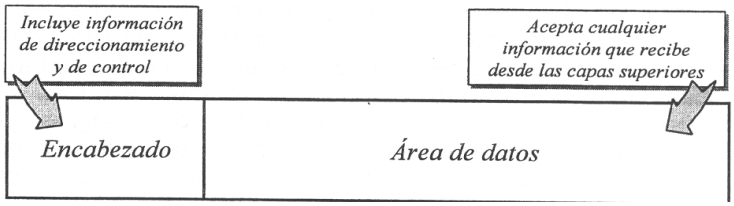



**Fig. 3.2** Forma general de un datagrama IP

***El tamaño del datagrama se determina por la aplicación que envía los datos, y puede ser tan grande como 64 Kb, incluido el encabezado.***

**Trayectoria del datagrama IP**

Para ir de la fuente al destino, un datagrama IP sigue una trayectoria formada por una secuencia de ruteadores.

Hay dos métodos de llegar de la fuente al destino:

1. Se especifica la ruta desde la fuente (source route). En este método la fuente pone en el encabezado del paquete la lista de ruteadores, por los que pasará el mensaje. Este método no ha tenido mucho éxito.
2. Conducción de ruteador por ruteador. La conducción del datagrama de la fuente al destino se hace escogiendo, en cada ruteador de la trayectoria, el siguiente ruteador al cual será enviado el datagrama. Este método ha probado ser flexible y robusto, por lo cual es el comúnmente empleado en las redes.

**Tipos de ruteo**

Existen dos tipos de ruteo, el directo y el indirecto:

- ***Ruteo Directo.*** Transmisión de datagramas IP entre dos equipos de la misma red física sin la intervención de compuertas. El emisor encapsula el datagrama en la trama de la red, efectuando la vinculación entre la dirección física y la dirección IP, y envía la trama resultante en forma directa al destinatario. Debido a que en el ruteo directo los datagramas se transmiten de un equipo a otro, en la misma red física, el proceso es muy eficiente. La vinculación entre la dirección física y la IP se realiza mediante el ARP .
- ***Ruteo Indirecto***. Las compuertas forman una estructura cooperativa, interconectada. Las compuertas se envían los datagramas hasta que se alcanza a la compuerta que puede distribuirla en forma directa a la red destino. En el indirecto la transmisión del datagrama se efectúa mediante la intercesión de las compuertas. Aquí la compuerta que actúa como ruteador debe de estar provista de mecanismos para conocer, y por tanto decidir, la trayectoria de la red que se desea alcanzar. En este direccionamiento un equipo debe enviar a una compuerta el datagrama con destino a una red física distante. La compuerta de la red física envía el datagrama a otras compuertas hasta alcanzar a aquel que puede emitirlo en forma directa a la red destino. La compuerta debe conocer las rutas hacia las diferentes redes externas, ellas pueden utilizar a su vez un ruteo indirecto en el caso de no conocer la ruta a una red específica. Las compuertas conocen las trayectorias a otra red mediante Tablas de Ruteo.

La siguiente figura representa lo descrito anteriormente

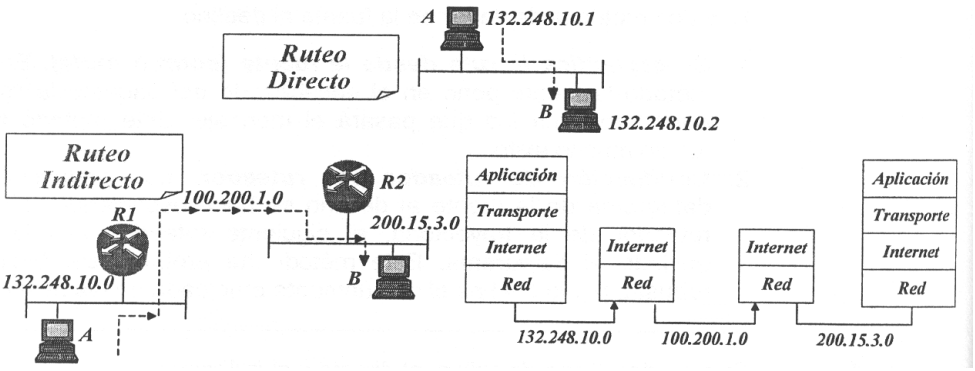



**Fig. 3.3** Tipos de ruteo

***Para que una computadora conozca si una ruta es directa o indirecta no tiene más que examinar su campo de red y su campo de subred que son parte de su propia dirección de red. Si el número de red y subred de origen y destino coinciden se tiene una ruta directa. En cualquier lotro caso se tendrá que recurrir a la utilización de rutas indirectas.***

**Tablas de ruteo IP**

Este es el algoritmo comúnmente utilizado para el ruteo de IP. Las tablas de ruteo están presentes en todo equipo que almacene ¡ información de cómo alcanzar posibles destinos. En las, tablas no se j almacena la ruta específica a un equipo, sino aquella a la red donde se encuentre. Cada puerto de comunicación de la compuerta debe poseer una dirección IP. La decisión de a dónde remitir un datagrama se toma basándose en la tabla de ruteo. No hay formato único para la tabla de ruteo ya que éste depende de cada marca de ruteador; sin embargo, en general en todos los formatos se incluyen. los campos indicados en la siguiente figura:

| *Destino* | *Siguiente ruteador* | *Máscara de ruteo* | *Métrica* | *Tipo* | *Actualización* |
|---|---|---|---|---|---|
| 170.8.3.0 | 170.8.3.1 | 255.255.255.0 | 0 | DIR | |
| 170.8.4.0 | 170.8.3.7 | 255.255.255.0 | 90 | REM | |

**Fig. 3.4** Esquema general de una tabla de ruteo

De la figura anterior tenemos lo siguiente

| Campo | Descripción |
|---|---|
| ***Destino*** | Es la dirección IP de la red, o host destino. La dirección de destino en un datagrama siempre se refiere al destino último. Cuando un ruteador reenvía el datagrama a otro ruteador, la dirección de ese ruteador *(siguiente ruteador)* no aparece en el encabezado del datagrama. |
| ***Siguiente ruteador*** | Es la dirección IP del ruteador que es el siguiente ruteador en la trayectoria a la red destino. |
| ***Máscara de ruteo*** | Es la máscara para la interfaz o puerto del ruteador que define los bits del campo destino que son significativos en el campo de dirección de red. Los ceros indican campo de dirección de host. |
| ***Métrica*** | Es el valor asignado a la ruta para ayudar a determinar la ruta. |
| ***Puerto o interfaz del ruteador*** | Es el puerto físico a través del cual debe ser enviado el datagrama para hacerlo llegar al siguiente ruteador. |
| ***Tipo*** | Este campo hace referencia al tipo de ruta que puede ser:<br>***DIR, Directa.*** El ruteador está conectado directamente a la red local destino.<br>***REM, Remota.*** El destino es alcanzable a través del ruteador indicado en el campo *"siguiente hop o ruteador"*. |
| ***Actualización*** | Este campo indica el número de segundos desde que esta ruta fue actualizada por última vez. |

Función de Ya sabemos que un ruteador usa una tabla de ruteo para seleccionar ruteo el siguiente ruteador al cual enviar el datagrama para hacerlo llegar a un destino dado. En forma más general, la función de ruteo se refiere a todas las tareas que se realizan para descubrir y anunciar trayectorias de un nodo aun destino y para transmitir los paquetes de datos a ese destino.

A continuación se describirá el funcionamiento de un ruteador en base a la figura siguiente

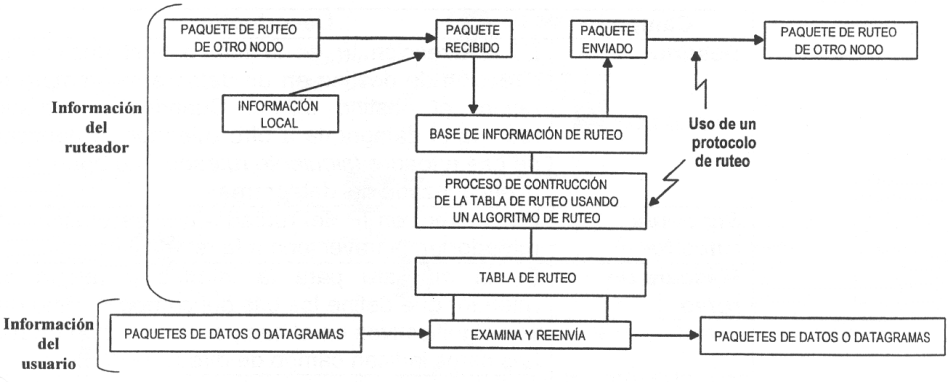



**Fig. 3.5** Esquema de la función de ruteo.

1. Un ruteador recibe información de actualizaciones de ruteo de otro ruteador y de su medio de trabajo, como la información de configuración introducida manualmente por el administrador. El ruteador usa esos datos para actualizar su base de información de ruteo.
2. El ruteador usa un protocolo de ruteo (tema que se verá más adelante) para anunciar toda o parte de la información de su base de información de ruteo.
3. La base de información de ruteo consiste en una tabla de registros con los siguientes campos:
    - Siguiente ruteador: Nodo al cual se deben enviar los paquetes para hacerlos llegar a su destino.
    - Métrica: Especifica la forma de métrica para la ruta.
4. El algoritmo de ruteo usa la base de información de ruteo para computar la tabla de ruteo.
5. La computación de la base de información de ruteo y de la tabla de ruteo se realiza de forma transparente para el usuario, al mismo tiempo que el ruteador usa la tabla de ruteo para seleccionar una trayectoria para enviar todo paquete que llega de un enlace de entrada.

**Proceso de ruteo**

A continuación se describe el proceso de ruteo de un paquete, para proporcionar una idea más intuitiva de cómo funciona dentro de una computadora:

| La computadora pregunta... | Si la respuesta es... | |
|---|---|---|
| | Afirmativa entonces... | Negativa entonces... |
| ***¿Soy yo el destino?*** | El datagrama ha llegado. | Continuar con la siguiente pregunta. |
| ***¿Es una ruta directa?*** | El datagrama se envía directamente a la red con la dirección hardware y la dirección IP de la máquina de destino. | Continuar con la siguiente pregunta. |
| ***¿Aparece la dirección de la red de destino en las rutas indirectas?*** | Se envía el datagrama al ruteador encargado de esa ruta indirecta. | Continuar con la siguiente pregunta. |
| ***¿Está especificada una ruta por defecto?*** *(ver capítulo 5)* | Se envía al ruteador que acoge las rutas por defecto. | Se llega a una situación de error ya que la red destino es inalcanzable. *En estos casos, la computadora suele generar un error del tipo network unreachable (red inalcanzable).* |

Este proceso iterativo se repite en todos los nodos por donde pasa el datagrama hasta que éste, finalmente, llega a su destino o se descarta. Esto se debe en parte, a la posibilidad que tiene cualquier computadora IP de actuar como ruteador o como computadora.

# Elementos de la función de ruteo

**Descripción**

La determinación de la mejor trayectoria a un destino dado en un ruteador depende de los siguientes elementos:

- La métrica de ruteo.
- El algoritmo de ruteo.
- La topología de la red.
- El protocolo de ruteo.

A continuación se describe cada uno de estos elementos.

**Métrica de ruteo**

Cuando un algoritmo de ruteo actualiza una tabla de ruteo, su objetivo principal es determinar cuál es la mejor información que debe incluir en la tabla. Cada algoritmo de ruteo interpreta lo que es mejor a su manera. El algoritmo genera un número, denominado métrica, para cada ruta a través de la red. Normalmente, cuanto menor sea la métrica, mejor será la ruta. Se pueden calcular las métricas tomando como base una sola característica de la ruta; se pueden calcular métricas más complejas combinando varias características. Las métricas utilizadas con mayor frecuencia por los ruteadores son:

| Criterio | Elección basada en… |
|---|---|
| ***Ancho de banda*** | La capacidad de transmisión de datos de un enlace *(por ejemplo, entre un enlace Ethernet de 10 Mb/s y una línea arrendada de 64 Kb/s, se elige la primer opción).* |
| ***Retardo*** | La longitud del tiempo requerido para transportar un paquete a lo largo de cada enlace desde el origen hacia el destino. |
| ***Carga*** | La cantidad de actividad en un recurso de red *(como por ejemplo un ruteador o un enlace).* |
| ***Confiabilidad*** | El índice de error de cada enlace de red. |
| ***Número de saltos*** | La cantidad de ruteadores que un paquete debe atravesar antes de llegar a su destino. Es el criterio más simple, y consiste en elegir el camino con menor número de saltos a través de la red. Este es un criterio que se puede medir fácilmente y que debería minimizar el consumo de recursos de la red. |
| ***Tictacs*** | El retardo en un enlace de datos que utiliza los tictacs de reloj PC de IBM *(aproximadamente 55 milisegundos).* |
| ***Costo*** | Valor arbitrario, generalmente basado en el ancho de banda, el gasto monetario y otras mediciones, asignado por un administrador de la red. El criterio de menor número de saltos lo constituye el encaminamiento de mínimo costo, donde se asocia un costo a cada enlace y, para cualesquiera dos estaciones conectadas, se elige la ruta a través de la red que implique el costo mínimo. |

# Algoritmos de ruteo

Los ***algoritmos de ruteo*** emplean comúnmente una tabla de ruteo en la que almacenan información referente a los posibles destinos y cómo llegar a ellos.

Las tablas de ruteo se generan a partir de dos procesos:

- La inicialización del proceso de ruteo.
- El intercambio de tablas con otros ruteadores.

Una vez que las tablas están listas para ser consultadas, es necesario que se actualicen con cierta frecuencia, de tal manera que reflejen los cambios que se den en la topología de la red. En redes pequeñas estos cambios pueden ser incorporados por el administrador local, pero en una red grande sería muy complicado y es imprescindible automatizar la actualización. Estos

mecanismos automáticos de actualización conocidos como ***algoritmos de ruteo*** permiten además el intercambio de información entre compuertas vecinas.

**Topología de red**

La topología de la red puede ser plana o estar organizada en redes de ruteo jerárquicas. En una red plana no hay jerarquías y todos los ruteadores están al mismo nivel lógico. Generalmente, esta red es apropiada para sistemas pequeños. En cambio, cuando la red es grande, la topología es jerárquica y se divide en áreas. Cada área tiene sus propios ruteadores, que suelen ser de nivel 1. Las áreas se conectan con ruteadores de nivel 2, que transmiten tráfico entre ellas. Cuando una sola entidad administra un conjunto de áreas, ruteadores, enlaces y computadoras, por ejemplo una empresa, una institución educativa o una dependencia gubernamental, se le llama sistema autónomo. La red Internet es un conjunto de sistemas autónomos.

**Protocolo de ruteo**

Las tareas de un protocolo de ruteo son la creación de la tabla de ruteo (usando un algoritmo de ruteo), el mantenimiento actualizado de esas tablas y la selección del siguiente ruteador al cual enviar el paquete de datos. Para esta tarea se requiere que los ruteadores intercambien información acerca del estado de la red. En el ambiente TCP/IP, se usan los siguientes protocolos de ruteo:

- RIP
- OSPF
- EGP
- BGP
- IGRP

**Algoritmos de ruteo**

Requisitos Los algo ritmos de ruteo, ya descritos anteriormente, están que deben orientados generalmente para cumplir uno o varios de los siguientes cumplir requisitos necesarios determinar el camino óptimo al destino:

| Requisito | Descripción |
|---|---|
| ***Optimización*** | Se refiere a la capacidad que tiene el ruteador de seleccionar la mejor ruta. Esta depende de los parámetros que elige para determinarla. Por ejemplo, un algoritmo puede utilizar el número de saltos y el retardo, pero este último puede influir más en el resultado final, es decir, tiene más importancia que el otro parámetro. |
| ***Simplicidad*** | Los algoritmos son diseñados para ser lo más simples posible, es decir, para que requieran el mínimo procesamiento del ruteador, no lo ocupen demasiado y no se convierta en una carga pesada para la carga general de la red. Esta característica permite al algoritmo operar con redes de ancho de banda pequeño y en equipo con escasos recursos. |
| ***Robustez / estabilidad*** | Los algoritmos de ruteo deben operar correctamente bajo casi cualquier circunstancia, tal como fallas del hardware, alta carga en la red, implementación incorrecta, etc. Este es un punto crucial en su diseño, pues los ruteadores representan nodos que interconectan redes diferentes y cualquier falla que presenten afectará seriamente la comunicación entre las redes. |
| ***Convergencia rápida*** | Se llama convergencia al proceso mediante el cual los ruteadores determinan las mejores rutas. Cuando en la internet se dan situaciones que cambian su topología *(alguna red se cayó, otra acaba de ser dada de alta, etc.)*, los ruteadores intercambian entre sí actualizaciones de ruteo que utilizan para calcular nuevas rutas y eventualmente llegar a un acuerdo sobre la jerarquía de selección de las rutas para todos los destinos posibles. |
| ***Flexibilidad*** | Los protocolos de ruteo deben ser capaces de adaptarse a una amplia variedad de circunstancias. Por ejemplo, suponiendo que una red se cayó, los ruteadores que se han enterado cambiarán las rutas que cruzaban por esa red por la siguiente mejor opción contenida en las tablas de ruteo. La mayoría de los ruteadores pueden ser programados para adaptarse a cambios en anchos de banda, retardos en la red y otros parámetros. |

**Clasificación**

Los algoritmos de ruteo pueden ser clasificados por su tipo como sigue:

- Estático o dinámico
- Single-Path o Multi-Path
- Plano o Jerárquico
- De anfitrión inteligente o ruteador inteligente
- Intradominio o interdominio
- Estado de enlace o vector distancia

A continuación se describe cada uno de estos algoritmos de ruteo.

**Estático o Dinámico**

- El algoritmo estático no es un algoritmo automatizado sino un mapeo establecido manualmente por el administrador, al inicio del proceso de ruteo. Este tipo de ruteo únicamente cambia si el administrador si el administrador lo establece, por lo que sólo es recomendable en una internet pequeña, estable y de tráfico relativamente predecible.
- El algoritmo dinámico, en cambio, se ajusta en tiempo real a las circunstancias cambiantes de la internet gracias al análisis que desarrollan sobre todo mensaje de ruteo. Si el mensaje indica que se ha producido un cambio en la red, el software del ruteador calcula nuevamente sus rutas, actualiza sus tablas y envía a sus vecinos actualizaciones de ruteo, estimulándolos a calcular de nuevo sus rutas. Sin embargo, bajo ciertos ambientes es posible que los algoritmos dinámicos se complementen con rutas estáticas.

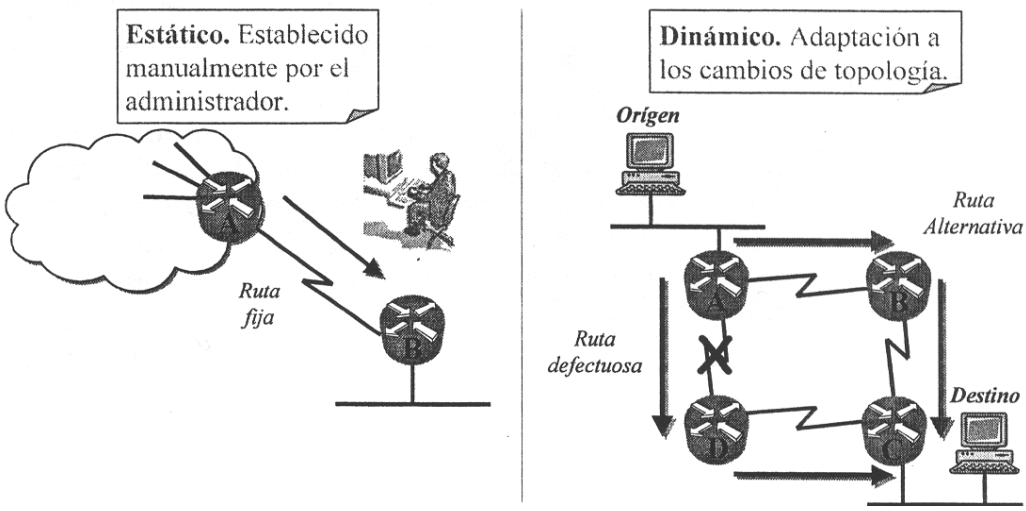



**Fig. 3.6** Algoritmos estático y dinámico.

**Single-Path o Multi-Path**

- El algoritmo Single-Path se refiere a la capacidad que tiene el ruteador de conmutar tráfico a un solo canal en caso de que fallen los otros.
- El algoritmo Multi-Path se refiere a la capacidad que tiene el ruteador de balancear tráfico multicanalizador sobre enlaces paralelos, característica que se traduce en mayor confiabilidad y eficiencia.

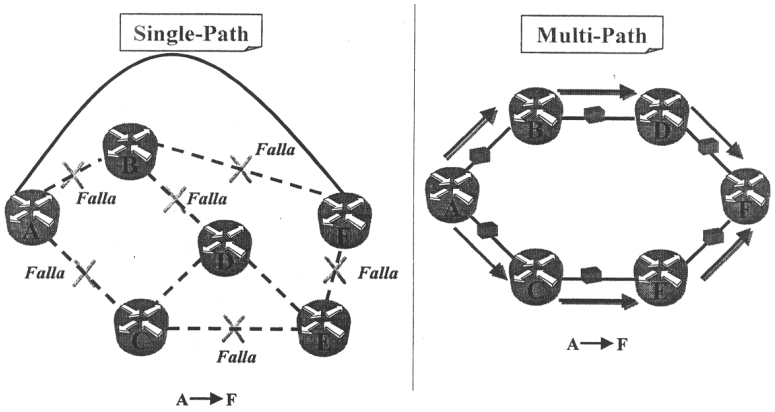



**Fig. 3.7** Algoritmos Single-Path y Multi-Path

**Plano o Jerárquico**

En un sistema plano de ruteo todos los ruteadores son pareja de los demás (pairs). Un ***algoritmo plano*** se puede ver como un esquema donde se asigna a un dispositivo la siguiente dirección disponible, y no se tiene en cuenta la estructura del esquema de direccionamiento (Analogía: la numeración de las actas de nacimiento, ya que se asignan de forma secuencial)

En un sistema ***jerárquico*** algunos ruteadores forman parte del backbone (la columna vertebral de la red) de ruteo de red interna. Los paquetes de ruteadores que no pertenecen al backbone son enviados a este y circulan en él hasta que llegan al ruteador de acceso / salida en el área general de destino. Las columnas vertebrales de ruteo son conocidas como dominios, sistemas autónomos o áreas. Sólo algunos ruteadores pueden establecer comunicación con ruteadores de dominios distintos al propio, aunque por lo general la comunicación entre ruteadores de un mismo dominio puede ser limitada. En internets grandes pueden existir múltiples niveles de jerarquía. La principal ventaja de los algo ritmos jerárquicos es que por su funcionamiento se adaptan fácilmente a la organización de muchas compañías. La mayor parte de la comunicación ocurre dentro de pequeños grupos (dominios), por lo que los ruteadores de interdominio sólo necesitan intercambiar información con sus vecinos de dominio, lo que simplifica enormemente el diseño de los algoritmos y el tráfico en la red.

Se puede ver como un esquema donde las direcciones IP tienen una estructura específica y no se asignan al azar *(Analogía: los códigos postales que se utilizan en el sistema de correos, donde la dirección es determinada por la ubicación del edificio y no por un número asignado al azar)*.

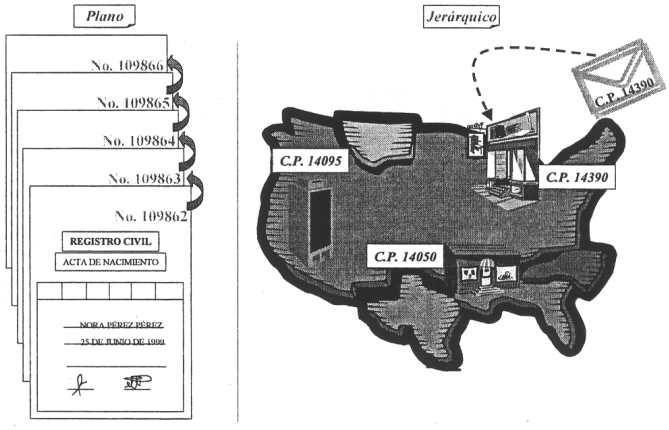



**Fig. 3.8** Analogías de los algoritmos Plano y Jerárquico

**De anfitrión inteligente o ruteador inteligente**

Algunos algoritmos de ruteo asumen que el anfitrión origen determinará la ruta a seguir hasta alcanzar el destino. A esto se le conoce como ruteo origen/fuente.

- Los ***algoritmos de anfitrión inteligente*** (o ruteo origen) donde los ruteadores actúan como equipos de almacenamiento y envío (store and forward) exclusivamente, no partícipan en la toma de decisiones. Estos algoritmos con frecuencia escogen las mejores rutas, pues descubren todas las rutas posibles antes de enviar los datos, lo que implica un incremento sustancial de tiempo de procesamiento y tráfico de autodescubrimiento.
- Los ***algoritmos de ruteador inteligente*** no conceden al anfitrión ni voz ni voto para el proceso de ruteo, sólo los ruteadores pueden determinar las rutas con base a sus cálculos.

**Intradominio o interdominio**

- Los algoritmos ***intradominio*** sólo pueden operar dentro de un mismo dominio (sistema autónomo).
- Los algoritmos ***interdominio*** están diseñados para operar dentro y entre sistemas autónomos.

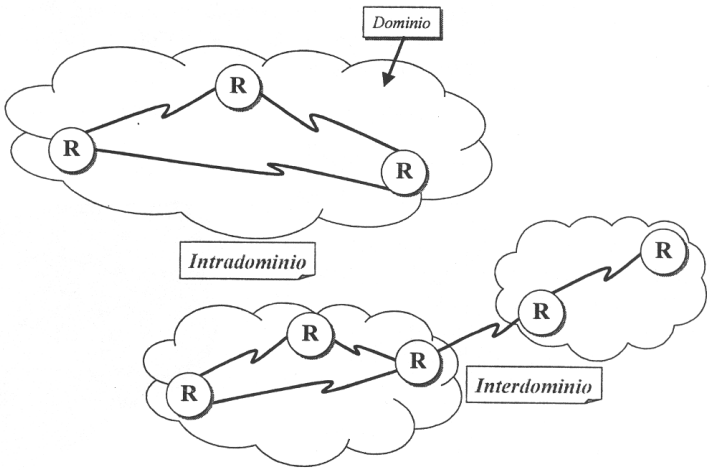



**Fig. 3.9** Algoritmos intradominio e interdominio

**Estado de enlace o vector distancia**

- Los algoritmos de estado de enlace (también conocidos como SPF, "primero abrir la ruta más corta), llevan la información de ruteo a todos los nodos de la internet. Sin embargo, todo ruteador envía exclusivamente aquella porción de su tabla de ruteo que describe el estado de sus propios enlaces. Envían pequeñas actualizaciones por toda la internet. Estos algoritmos convergen más rápidamente y por lo tanto es más difícil que caigan en lazos de ruteo; por otro lado, requieren mayor poder de procesamiento y memoria que los algoritmos de vector distancia.
- Los algoritmos de vector distancia obligan a todo ruteador a intercambiar sus tablas de ruteo solamente con sus vecinos. Envían actualizacione grandes sólo a sus vecinos, es decir, cada ruteador recibe una tabla de ruteo de los ruteadores directamente vecinos. Por ejemplo, en la figura siguiente, el Ruteador B recibe información del Ruteador A. El Ruteador B agrega un número de vector distancia (como por ejemplo el número de saltos), aumentando de esta manera el vector distancia y luego transfiere esta nueva tabla de ruteo a su otro vecino, el Ruteaodor C. Este mismo proceso paso a paso se produce en todas las direcciones entre los ruteadores directamente vecinos.

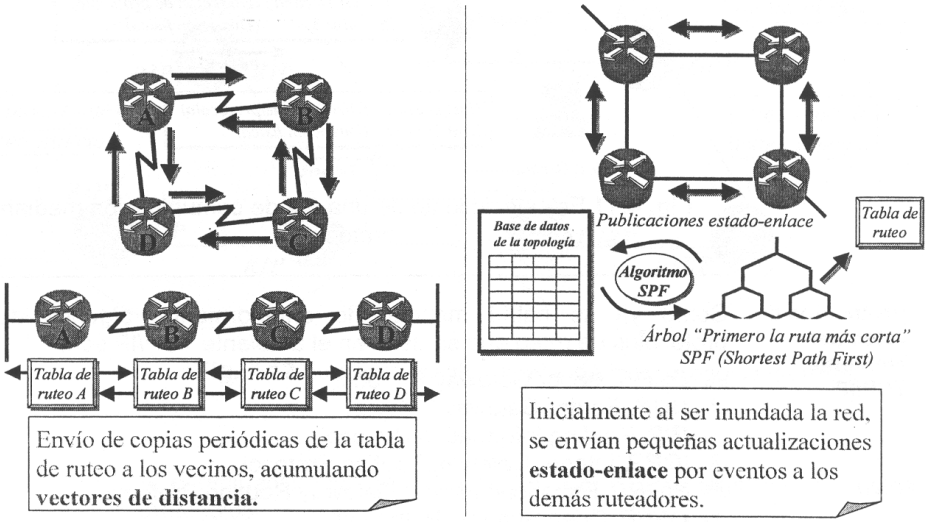



**Fig. 3.10** Algoritmos estado de enlace y vector distancia

## Protocolos de ruteo

**Descripción**

Recordando que un protocolo de ruteo logra el ruteo a través de la implementación de un algoritmo de ruteo específico, según lo descrito en el capítulo 2, agregaremos que tiene las siguientes características:

- Soporta un protocolo de enrutado proporcionando mecanismos para compartir la información de ruteo.
- Sus mensajes se desplazan entre los ruteadores.
- Permite que los ruteadores se comuniquen con otros ruteadores para mantener actualizadas las tablas.

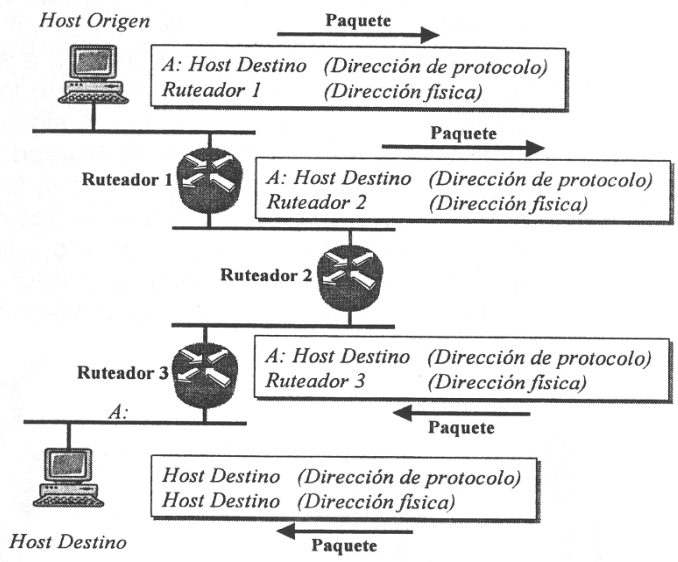



**Fig. 3.11** Establecimiento de una red de comunicación mediante protocolos

**Protocolos de ruteo ambiente TCP/IP**

Como ya se había mencionado anteriormente, algunos de los protocolos de ruteo que se usan en el ambiente TCP/IP son:

- ***EGP***, Exterior Gateway Protocol
- ***BGP***, Border Gateway Protocol
- ***RIP***, Routing Information Protocol
- ***IGRP***, Interior Gateway Routing Protocol
- ***EIGRP***, Enhanced Interior Gateway Routing Protocol
- ***OSPF***, Open Shortest Path First

**Tipos de protocolos de ruteo**

Los protocolos de ruteo pueden ser interiores o exteriores. Un protocolo de ruteo interior opera dentro de un sistema autónomo, mientras que un protocolo de ruteo exterior se usa en el ruteo entre sistemas autónomos.

La tabla siguiente muestra la clasificación de los protocolos de ruteo:

| Protocolo | Tipo |
|---|---|
| EGP | Exterior |
| BGP | Exterior |
| RIP | Interior |
| IGRP | Interior |
| EIGRP | Interior |
| OSPF | Interior |

**Esquema general de funcionamiento**

El siguiente esquema, representa el funcionamiento general de los protocolos de ruteo:

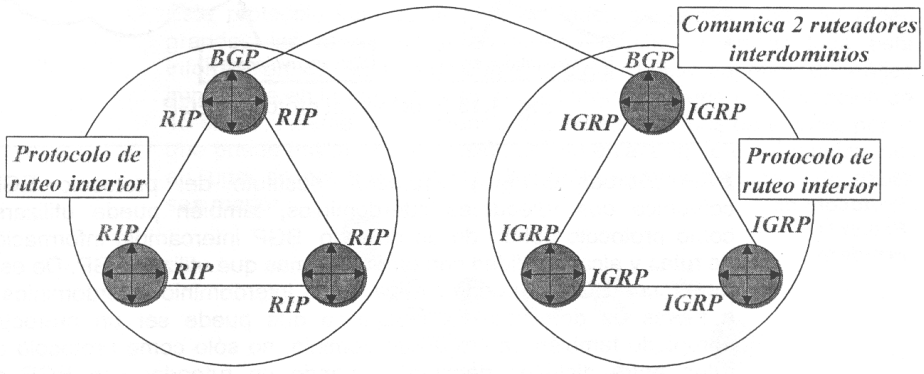



**Fig. 3.12** Funcionamiento general de los protocolos de ruteo

A continuación se describe la función y características de estos protocolos.

**EGP *Protocolo de Parsarela Exterior***

***EGP*** *(Exterior Gateway Protocol),* comunica dos ruteadores en la frontera de los dominios. Durante mucho tiempo se utilizó como protocolo de ruteo para la conexión entre distintos dominios de redes, es decir, básicamente, redes con distintos administradores. Es un protocolo que sólo indica a través de qué ruteadores se puede llegar al destino. Esta información de alcanzabilidad se ha demostrado que no es suficiente en una red tan compleja como la Internet actual. Por eso se desarrolló BGP, como mejora para la interconexión de redes de distintos dominios.

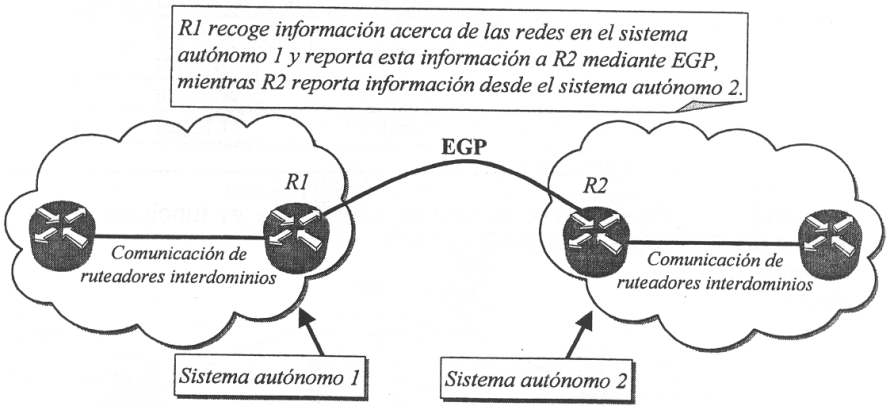



**Fig. 3.13** Función del protocolo EGP

**BGP *Protocolo de Pasarela Frontera***

***BGP*** *(Border Gateway Protocol),* sustituto del protocolo EGP, comunica dos ruteadores interdominios, también puede utilizarse como protocolo dentro de un dominio. BGP intercambia información de rutas y alcanzabilidad con otros sistemas que utilizan BGP. De esta forma, con BGP se puede realizar ruteo interdominio, interdominios o. a través de dominios. Esto significa que puede ser un protocolo; apropiado también dentro de un dominio, no sólo como protocolo de ruteo entre distintos dominios. Cuando un ruteador con BGP se conecta a la red, se conecta con un ruteador vecino con BGP e intercambia en él la información sobre rutas. Periódicamente los ruteadores avisan a sus vecinos de que siguen en funcionamiento. , Cuando un ruteador detecta un cambio en la red, se envían mensajes, de actualización al resto de ruteadores utilizando BGP, de manera que la transmisión sea fiable. En estos mensajes de actualización se indican las rutas que son factibles y las rutas que hay que abandonar porque ya no se pueden utilizar.

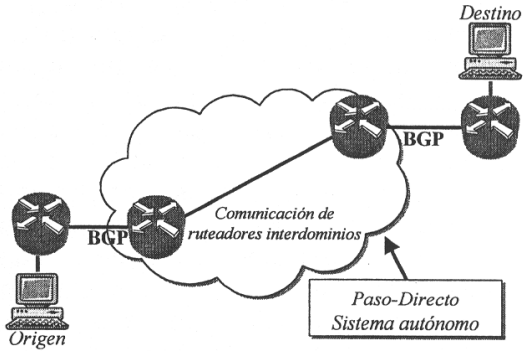



**Fig. 3.14** Función del protocolo BGP

**RIP *Protocolo de Información de Ruteo***

***RIP*** *(Routing Information Protocol),* es el protocolo de ruteo interior más utilizado en el intercambio de información entre ruteadores que forman parte de un sistema autónomo. RIP utiliza un algoritmo que cuenta el número de saltos que tiene que realizar un paquete para llegar al destino *(algoritmo de vector de distancia*).

Este protocolo sólo se emplea en redes pequeñas, pues en redes grandes las tablas de ruteo crecen mucho, y enviar toda esta información de unos ruteadores a otros puede suponer un tráfico importante en la red. Por otro lado, el protocolo tiene una limitación de 15 saltos. Además no diferencia entre distintos tipos de enlace, por lo que puede enviar la información por un enlace lento o congestionado, en lugar de por uno rápido o libre, sólo porque el número de saltos sea menor.

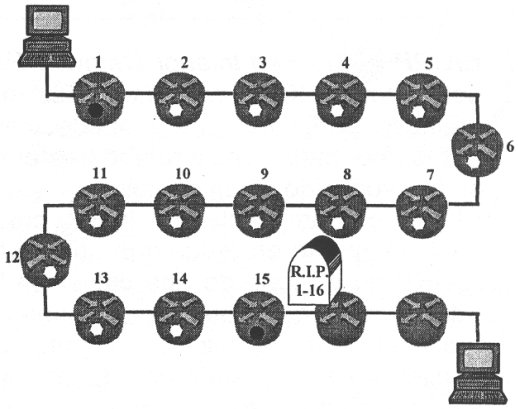



**Fig. 3.15** RIP y su limitación en el numero de saltos

### IGRP *Protocolo de Ruteo de Pasarela Interior*

***IGRP*** *(Interior Gateway Routing Protocol),* es un protocolo desarrollado por Cisco, comunica dos ruteadores internos, es decir, dos ruteadores dentro de un mismo dominio de administración. Aunque es un protocolo de vector de distancia, tiene en cuenta factores adicionales, además del número de saltos hacia el destino, como el retardo, el ancho de banda disponible, la tasa de errores y la ocupación de los enlaces. Por otra parte, puede dividir el tráfico entre varios caminos igual de buenos o parecidos. En IGRP se envían actualizaciones periódicamente, cada 90 segundos, a todos los ruteadores vecinos. Tras detectar un cambio se desencadena un proceso de actualización hacia el resto de ruteadores vecinos, de manera que la información se difunde rápidamente por la red.

| *Métrica* | *Cantidad de ruteadores máximo* | *Orígenes* |
|---|---|---|
| *Ancho de banda*<br>*Carga*<br>*Retardo*<br>*Confiabilidad* | *255, se ejecuta con éxito en las grantes internetworks en el mundo* | *Cisco* |

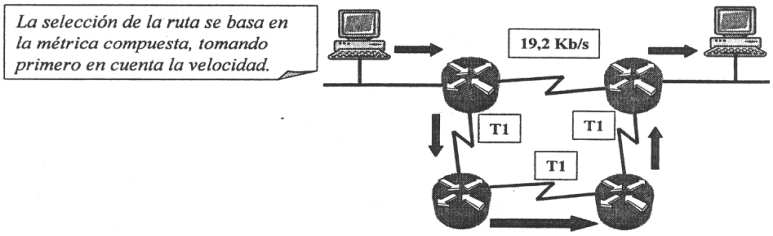



**Fig. 3.16** Función del protocolo IGRP

### EIGRP *Protocolo de Ruteo de Pasarela Interior Mejorado*

***EIGRP*** *(Enhanced Interior Gateway Routing Protocol),* es una mejora del protocolo IGRP para interredes muy grandes. Utiliza las mismas métricas que IGRP, pero añade ciertas mejoras importantes, que reducen el tráfico entre ruteadores enviando información sólo cuando se ha producido algún cambio.

EIGRP es compatible con IGRP, por lo que es posible incorporarlo paulatinamente en redes que utilicen IGRP. Cuando un ruteador con EIGRP no dispone de ruta calculada hacia un destino, solicita a sus ruteadores vecinos que calculen una. Esta petición se propaga por la red hasta que se calcula una ruta. Sólo se envían actualizaciones parciales y sólo cuando una de las métricas de una ruta cambia. Por ello, el tráfico que genera es mucho menor que IGRP.

**OSPF *Primero la Ruta Libre mas Corta***

**OSPF** (*Open Shortest Path First),* es un protocolo con muy buenas características de escalabilidad y respuesta frente a cambios de la red. Es un protocolo abierto, lo que significa que su especificación pertenece al dominio público. OSPF divide una red en áreas, dentro de cada área los ruteadores contienen información completa de todos los ruteadores, interfaces y enlaces dentro de dicha área. Los ruteadores que sirven de conexión con equipos fuera del área mantienen bases de datos separadas para la información de dentro del área y para la información de fuera del área.

Al empezar, un ruteador envía mensajes de saludo en la red para conocer a los ruteadores vecinos, y éstos le responderán con sus correspondientes mensajes de saludo. Estos mensajes se envían periódicamente para indicar a sus ruteadores vecinos que siguen en funcionamiento. El protocolo elige un ruteador designado, responsable de generar avisos de estado del enlace que sirven a los ruteadores de información para completar las bases de datos sobre la red, reduciendo drásticamente el tráfico que se genera.

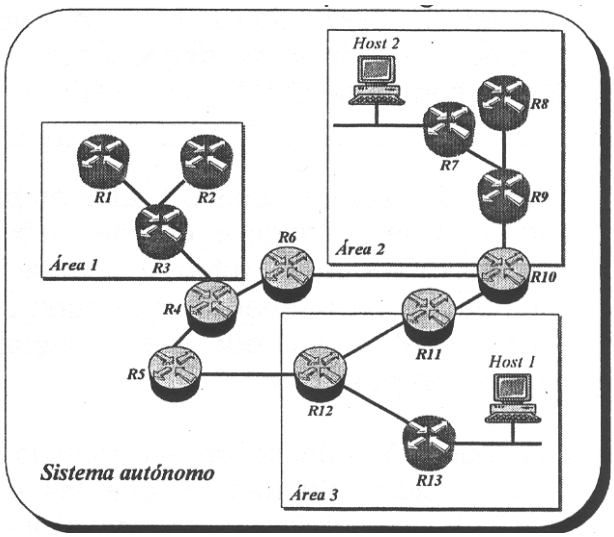



**Fig. 3.17** Función del protocolo OSPF

En la figura, los ruteadores 4, 5, 6, 10, 11, y 12 conforman el backbone (parte de una red que actúa como ruta primaria para el tráfico que, con mayor frecuencia, proviene de y se destina a otras redes). Si el Host 1 (*Área 3*) requiere enviar un paquete al Host 2 (*Área 2*), el paquete se envía al ruteador 13, el cual lo remite al ruteador 12, el cual 10 envía al ruteador 11. Este entonces remite el paquete a lo largo del backbone al área del ruteador en frontera 10, que envía el paquete a través de dos ruteadores intra-área (Ruteadores 9 y 7) para ser remitido al Host 2.

## Políticas de ruteo

**Ruteo como política segura**

Cuando el número de usuarios en los grupos de trabajo se incrementa, el crecimiento de los broadcast puede eventualmente causar una legítima preocupación sobre lo siguiente:

- Rendimiento en. la red.
- Problemas de aislamiento.
- Los efectos de radiar el broadcast en el rendimiento del CPU de la estación final.
- Seguridad en la red.

La decisión de ***instalar un ruteador****,* y así establecer el ***ruteo como política segura****,* para prevenir estos problemas potenciales, es a menudo basado en el nivel de confort psicológico de la organización.

Generalmente la cantidad de tráfico de broadcast en un grupo de 100 a 200 usuarios, no es un problema significativo a menos que haya un mal funcionamiento en el equipo o un protocolo se comporte mal. Los factores de riesgo dominantes en grupos de trabajo grandes, son la seguridad y el costo del negocio por una tormenta de broadcast u otro tipo de comportamiento que tire la red.

**Ruteo basado en políticas**

La idea de los protocolos basados en políticas es seleccionar las rutas con el fin de restringir el uso de ciertos recursos a ciertas clases de clientes. Ya que el ruteo y asignación de recursos dinámico no controlado puede tener un muy buen comportamiento de tiempo real, pero puede ser impredecible e inestable, se ha planteado el ***ruteo basado en políticas***.

Las redes de tránsito deben anunciar sus políticas de filtrado para prevenir ciclos de ruteo y que los paquetes se descarten. No es suficiente descubrir una política al verificar que los paquetes están siendo descartados cuando ocurre un time out de un nivel superior, por eso las restricciones políticas deben estar incorporadas en el cálculo de las rutas y el proceso de selección.

***En conclusión, podemos decir que el ruteo basado en políticas es un esquema de direccionamiento que envía paquetes a interlaces específicas basándose en las políticas de configuración del usuario. En estas políticas es posible especificar que el tráfico que se envía desde una red específica se debe enviar a través de una interfaz A, y que el resto del tráfico se debe enviar a través de la interfaz B.***

# CAPITULO IV
## PRACTICAS

La configuración del ruteador es un aspecto muy dependiente de la marca del fabricante, aunque el proceso de instalación es muy similar en diferentes modelos y marcas.

## Inicialización

**Componentes de configuración interna**

Los *componentes de la configuración interna del ruteador* son los siguientes:

- ***RAM/DRAM.*** Almacena las tablas de ruteo, el caché ARP, el caché de conmutación rápida, el bufering de paquetes *(RAM compartida)* y las colas de espera de paquetes. La RAM también proporciona memoria temporal y/o de trabajo para el archivo de configuración de un ruteador mientras el ruteador se enciende. El contenido de la RAM se pierde si se produce un corte de energía eléctrica o reinicio.

- ***NVRAM.*** La RAM no volátil almacena el archivo de configuración de copia de seguridad / inicio del ruteador. El contenido de la NVRAM se conserva durante un corte de energía o reinicio.

- ***Flash.*** ROM borrable y reprogramable que retiene la imagen y el microcódigo del sistema operativo. La memoria Flash activa las actualizaciones del software sin eliminar o reemplazar los chips del procesador. El contenido de la Flash se conserva durante los cortes de energía o reinicio. La memoria Flash puede almacenar múltiples versiones del software IOS.

- ***ROM.*** Contiene diagnósticos de encendido, un programa bootstrap y software del sistema operativo. Las actualizaciones del software en la ROM requieren la eliminación y el reemplazo de chips enchufables en la CPU.

- ***Interfaces.*** Conexiones de red, en la motherboard o en módulos de interfaz separados, a través de las cuales los paquetes entran y salen de un ruteador.

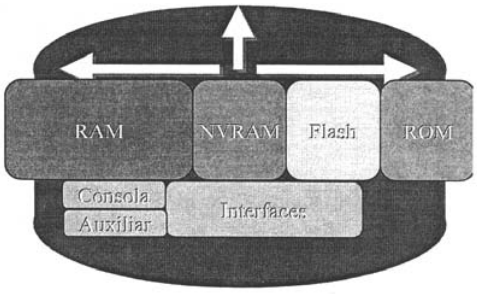



**Fig. 4.1** Componentes de configuración interna del ruteador

## Conexiones

La siguiente figura muestra el ***puerto de consola,*** el cual permite la ***conexión directa con el ruteador*** para poder configurarlo:

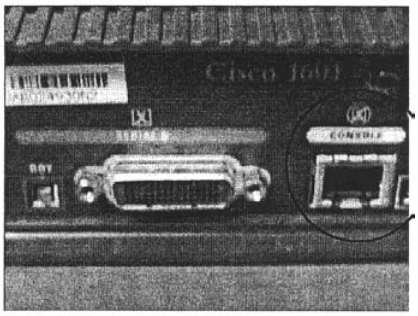


**Fig. 4.2** Conexión del puerto de consola

### Secuencia de inicio

Hay tres pasos en la *inicialización de un ruteador.* Este es probablemente un buen momento para repasar la secuencia de inicio acerca de lo que hace una PC en el momento del arranque como analogía en la inicialización del ruteador.

***Los tres pasos principales en la secuencia de inicio de un PC son:***

1. Las pruebas automáticas de arranque del hardware,
2. La carga del sistema operativo y
3. La selección de una aplicación por parte del usuario.

***El ruteador pasa por un proceso semejante:***

1. Se verifica el hardware *(a través de códigos almacenados en la ROM),*
2. Se carga el software IOS *(desde diversas fuentes),* y
3. Se carga la configuración del ruteador *(software de aplicación),* desde diversas fuentes.

Un ruteador se inicializa cargando el ***bootstrap,*** el sistema operativo y un archivo de configuración. Si el ruteador no puede encontrar un archivo de configuración, entonces entra en el modo de configuración. El ruteador almacena, en la NVRAM, una copia de seguridad de la nueva configuración desde el modo de configuración inicial.

### Objetivo de las rutinas de inicio del software IOS

El *objetivo de las rutinas de inicio del software IOS* es iniciar la operación del ruteador, el cual debe ofrecer un desempeño confiable en su trabajo de conectar las redes del usuario definidas en su configuración. Para hacer esto, las rutinas de inicio deben:

- Asegurarse de que el ruteador tenga todo su hardware probado.
- Encontrar y cargar el software IOS que el ruteador usa para su sistema operativo.
- Encontrar y aplicar las declaraciones de configuración acerca del ruteador, incluyendo las funciones de protocolo y las direcciones de interfaz.

Cuando se enciende un ruteador, realiza una prueba automática de encendido. Durante esta prueba automática, el ruteador ejecuta diagnósticos desde la ROM en todos los módulos de hardware. Estos diagnósticos verifican la operación básica de la CPU, memoria y puertos de interfaz de red. Después de verificar las funciones de hardware, el ruteador procede a inicializar el software.

**Proceso de inicialización del rutedor**

Después de la prueba automática de encendido del ruteador, se produce el siguiente proceso a medida que se inicializa:

| Etapa | Descripción |
|---|---|
| 1 | El cargador genérico de bootstrap, que se encuentra en la ROM, se ejecuta en la tarjeta de la CPU. Un bootstrap es una operación simple predeterminada para cargar instrucciones que a su vez hacen que se carguen otras instrucciones en la memoria, o provocan la entrada a otros modos de configuración. |
| 2 | El sistema operativo IOS se puede encontrar en uno de varios lugares. Se revela la ubicación en el campo de arranque del registro de configuración. Si el campo de arranque indica una Flash, o carga de red, los comandos boot system en el archivo de configuración indican la ubicación exacta de la imagen. |
| 3 | Se carga la imagen del sistema operativo. Cuando el sistema operativo está cargado y funcionando, el sistema operativo ubica los componentes del hardware y software y muestra los resultados en la terminal de consola. |

| Etapa | Descripción |
|---|---|
| 4 | El archivo de configuración guardado en la NVRAM se carga en la memoria principal y se ejecuta línea por línea. Estos comandos de configuración inician procesos de ruteo, brindan direcciones para las interfaces, establecen las características de los medios, etc. |
| 5 | Si no existe ningún archivo de configuración válido en la NVRAM, el sistema operativo ejecuta una rutina de configuración inicial impulsada por preguntas denominadas cuadro de diálogo de configuración del sistema, también denominado cuadro de diálogo de configuración inicial. |

**Comandos relacionados con el inicio del ruteador**

Existen cinco ***comandos relacionados con el inicio del ruteador***, que son: ***show run, show start, erase startup-config, reload y setup***.

Vamos a comparar las similitudes y diferencias del uso de la interfaz de línea de comando y el comando setup para configurar el ruteador.

- ***show startup-config.*** Muestra las copias de respaldo de los archivos de configuración que se ubican en la NVRAM.
- ***show running-config***. Muestra los archivos de configuración activos ubicados en la RAM.
- ***erase startup-config.*** Elimina la copia de respaldo del archivo de configuración en la NVRAM.
- ***reload (reboot)***. Vuelve a cargar el ruteador, haciéndolo pasar por todo el proceso de inicio.
- ***setup.*** Se usa para entrar en el modo de configuración inicial desde el indicador EXEC privilegiado.

***El modo de configuración inicial no debe ser el modo utilizado para introducir funciones complejas de protocolo en el ruteador. Se debe usar el modo de configuración inicial para realizar una configuración mínima, y luego se deben usar los diferentes comandos de modo de configuración, en lugar de configuración inicial, para la mayoría de las tareas de configuración del ruteador.***

## Configuración básica

### Descripción general

Entre los tipos de información en un archivo de configuración del ruteador se encuentran:

- La versión del software lOS
- La identificación del ruteador
- Las ubicaciones de los archivos de arranque
- La información de protocolo y
- Las configuraciones de interfaz.

### Modos de acceso

Por razones de seguridad, el ruteador tiene dos *niveles de acceso* a los comandos:

- Modo usuario. Las tareas ti picas incluyen la verificación del estado del ruteador. En este modo no se permite la configuración del ruteador .
- Modo privilegiado. Las tareas típicas incluyen el cambio de la configuración del ruteador.

***Para configurar un ruteador se puede hacer:***

- ***Usando la interfaz de usuario en la consola o terminal del ruteador***
- ***Mediante el acceso remoto.***

***Para hacer esto, debes conectarte al ruteador antes de introducir un comando EXEC.***

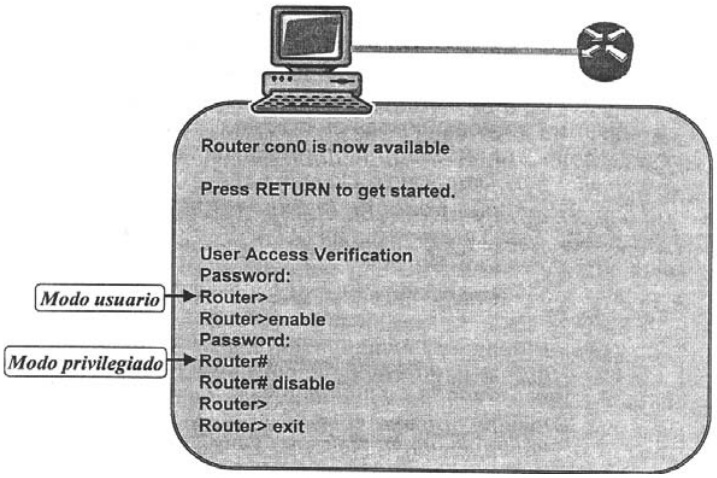



**Fig. 4.3** Modos de acceso a los comandos de configuración.

**Habilitación del modo privilegiado**

Al conectarte por primera vez a un ruteador, aparece un *indicador de modo usuario,* como se muestra en la figura siguiente:

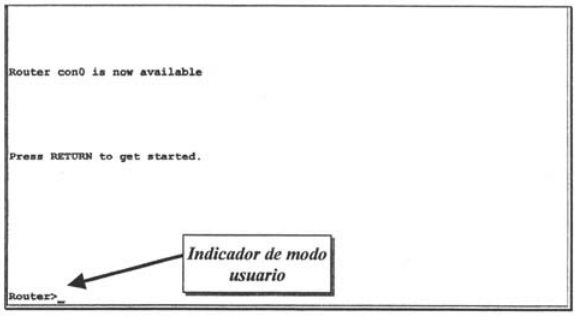



**Fig. 4.4** Pantalla de modo usuario

Los comandos disponibles en este nivel son un subconjunto de los comandos disponibles en el nivel privilegiado. En su mayor parte, estos comandos permiten visualizar información sin cambiar los parámetros de configuración del ruteador.

Para acceder al conjunto completo de comandos, se debe *habilitar primero el modo privilegiado,* realizando lo siguiente:

| Paso | Acción |
|---|---|
| 1 | Escribe *enable (habilitar)*, en el indicador > *(en el indicador password (contraseña), se habilita una contraseña secreta).* |

***Una vez realizado lo anterior, el indicador se transforma en el signo #, mientras se esté en este modo. Desde el modo privilegiado puede acceder al modo de configuración global y otros modos específicos de configuración, entre ellos:***

- ***interface (interfaz)***
- ***subinterface (subinterfaz)***
- ***líne (línea)***
- ***router (ruteador)***
- ***router map (mapa de ruteador)***
- ***otros modos de configuración***

***Lo que se ve en pantalla varía según el nivel específico del y la configuración del ruteador.***

| | |
|---|---|
| **2** | Escribe ***exit*** *(salir)*para desconectarte del ruteador. |

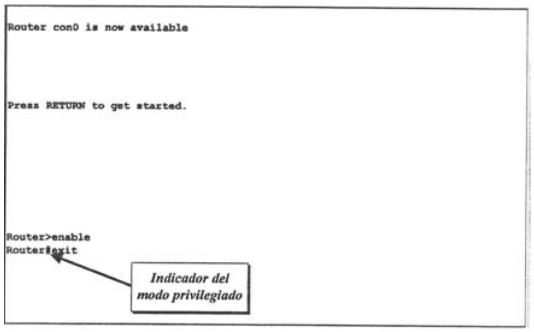



**Fig. 4.5** Pantalla de modo privilegiado.

### Lista de comandos del modo usuario

Cuándo se escribe un signo de interrogación **(¿)** en el indicador del modo usuario aparece una ***lista de comandos*** a los que se tiene acceso en este nivel:

```
Router>?
  access-profile   Apply user-profile to interface
  clear            Reset functions
  connect          Open a terminal connection
  disable          Turn off privileged commands
  disconnect       Disconnect an existing network connection
  enable           Turn on privileged commands
  exit             Exit from the EXEC
  help             Description of the interactive help system
  lock             Lock the terminal
  login            Log in as a particular user
  logout           Exit from the EXEC
  mrinfo           Request neighbor and version information from a multicast
                   router
  mstat            Show statistics after multiple multicast traceroutes
  mtrace           Trace reverse multicast path from destination to source
  name-connection  Name an existing network connection
  pad              Open a X.29 PAD connection
  ping             Send echo messages
  ppp              Start IETF Point-to-Point Protocol (PPP)
  resume           Resume an active network connection
  rlogin           Open an rlogin connection
  set              Set system parameter (not config)
--More--
```

**Fig. 4.6a** Comandos modo usuario

```
  logout           Exit from the EXEC
  mrinfo           Request neighbor and version information from a multicast
                   router
  mstat            Show statistics after multiple multicast traceroutes
  mtrace           Trace reverse multicast path from destination to source
  name-connection  Name an existing network connection
  pad              Open a X.29 PAD connection
  ping             Send echo messages
  ppp              Start IETF Point-to-Point Protocol (PPP)
  resume           Resume an active network connection
  rlogin           Open an rlogin connection
  set              Set system parameter (not config)
  show             Show running system information
  slip             Start Serial-line IP (SLIP)
  systat           Display information about terminal lines
  telnet           Open a telnet connection
  terminal         Set terminal line parameters
  traceroute       Trace route to destination
  tunnel           Open a tunnel connection
  where            List active connections
  x28              Become an X.28 PAD
  x3               Set X.3 parameters on PAD

Router>_
```

**Fig. 4.6b** Comandos modo usuario

**Lista de comandos del modo privilegiado**

```
Router#?
  access-profile   Apply user-profile to interface
  access-template  Create a temporary Access-List entry
  bfe              For manual emergency modes setting
  cd               Change current directory
  clear            Reset functions
  clock            Manage the system clock
  configure        Enter configuration mode
  connect          Open a terminal connection
  copy             Copy from one file to another
  debug            Debugging functions (see also 'undebug')
  delete           Delete a file
  dir              List files on a filesystem
  disable          Turn off privileged commands
  disconnect       Disconnect an existing network connection
  enable           Turn on privileged commands
  erase            Erase a filesystem
  exit             Exit from the EXEC
  help             Description of the interactive help system
  lock             Lock the terminal
  login            Log in as a particular user
  logout           Exit from the EXEC
  more             Display the contents of a file
 --More--
```

**Fig. 4.7a** Comandos modo privilegiado

```
  mrinfo           Request neighbor and version information from a multicast
                   router
  mstat            Show statistics after multiple multicast traceroutes
  mtrace           Trace reverse multicast path from destination to source
  name-connection  Name an existing network connection
  no               Disable debugging functions
  pad              Open a X.29 PAD connection
  ping             Send echo messages
  ppp              Start IETF Point-to-Point Protocol (PPP)
  pwd              Display current working directory
  reload           Halt and perform a cold restart
  resume           Resume an active network connection
  rlogin           Open an rlogin connection
  rsh              Execute a remote command
  send             Send a message to other tty lines
  set              Set system parameter (not config)
  setup            Run the SETUP command facility
  show             Show running system information
  slip             Start Serial-line IP (SLIP)
  systat           Display information about terminal lines
  telnet           Open a telnet connection
  terminal         Set terminal line parameters
  traceroute       Trace route to destination
 --More--
```

**Fig. 4.7b** Comandos modo privilegiado

```
PPP             Start IETF Point-to-Point Protocol (PPP)
pwd             Display current working directory
reload          Halt and perform a cold restart
resume          Resume an active network connection
rlogin          Open an rlogin connection
rsh             Execute a remote command
send            Send a message to other tty lines
set             Set system parameter (not config)
setup           Run the SETUP command facility
show            Show running system information
slip            Start Serial-line IP (SLIP)
systat          Display information about terminal lines
telnet          Open a telnet connection
terminal        Set terminal line parameters
traceroute      Trace route to destination
tunnel          Open a tunnel connection
undebug         Disable debugging functions (see also 'debug')
verify          Verify a file
where           List active connections
write           Write running configuration to memory, network, or terminal
x28             Become an X.28 PAD
x3              Set X.3 parameters on PAD

Router#_
```

**Fig. 4.7c** Comandos modo privilegiado

**Modos de examinar, mantener y modificar componentes**

Un ruteador posee componentes configurables. Dispone de *modos para examinar, mantener y modificar los componentes.* La lista siguiente describe algunos ejemplos de comandos:

- ***show.*** Utilizado para examinar.
- ***Cdp.*** Muestra entradas sobre los vecinos
- ***telnet.*** Se utiliza para acceder a otros ruteadores
- ***ping, trace, telnet,*** **y** ***debug.*** Se usan como comandos de prueba.

***El comando ping envía un paquete al host de destino*** **y** ***luego espera un paquete de respuesta de ese host. Los resultados de este protocolo de eco pueden ayudar a evaluar la confiabilidad de ruta a host, las demoras en la ruta,*** **y** ***si se puede acceder al host, o si éste está funcionando.***

**Modos del ruteador**

Ya sea que se acceda desde la consola o mediante una sesión Telnet, un ruteador se puede colocar en diferentes modos, cada uno de los cuales ofrecen diferentes funciones:

| Modo | Descripción |
|---|---|
| ***EXEC del usuario*** | Modo de visualización exclusivamente en el que el usuario puede visualizar alguna información acerca del ruteador, pero no puede realizar cambios. Examen limitado del ruteador. Acceso remoto. ***Router>*** |
| ***EXEC privilegiado*** | Soporta los comandos de depuración y prueba, el examen detallado del ruteador, la manipulación de los archivos de configuración, y el acceso a los modos de configuración. Examen detallado del ruteador. Depuración y prueba. Manipulación de archivos. Acceso remoto. ***Router#*** |
| ***SETUP (configuración inicial)*** | Presenta en la consola un cuadro de diálogo interactivo basado en prompts que ayuda al nuevo usuario a crear una configuración básica inicial. |
| ***De configuración global*** | Implementa poderosos comandos de una línea que ejecutan tareas simples de configuración. ***Router (config) #*** |
| ***RXBOOT*** | Modo de mantenimiento que se puede usar, para recuperar las contraseñas perdidas, o en caso de que el sistema operativo se borre de forma accidental de la memoria Flash. |

**Configuración de contraseña**

Se puede garantizar la seguridad del sistema utilizando ***contraseñas*** para restringir el acceso. Las contraseñas se pueden establecer tanto en líneas individuales como en el modo EXEC privilegiado:

- ***line console 0.*** Establece una contraseña en la terminal de consola.
- ***line vty* 0 4.** Establece protección mediante contraseña en las sesiones Telnet entrantes.
- ***enable-password.*** Restringe el acceso al modo EXEC privilegiado.

**Configuración de los protocolos de. ruteo**

Resulta muy simple *configurar los protocolos de ruteo* en el ruteador. En el modo de configuración, se usan los comandos de una línea: ***router rip, router igrp* 1, *router bgp* 1**
Una vez que se habilita un protocolo de ruteo a través de un comando global:

1. Aparece el prompt del modo de configuración del ruteador ***Router (config-router)#.***
2. Escribe un signo de interrogación ***(?)*** para obtener una lista de los subcomandos de configuración del protocolo de ruteo.

```
Router(config)#router ?
  bgp                 Border Gateway Protocol (BGP)
  egp                 Exterior Gateway Protocol (EGP)
  eigrp               Enhanced Interior Gateway Routing Protocol (EIGRP)
  igrp                Interior Gateway Routing Protocol (IGRP)
  isis                ISO IS-IS
  iso-igrp            IGRP for OSI networks
  mobile              Mobile routes
  odr                 On Demand stub Routes
  ospf                Open Shortest Path First (OSPF)
  rip                 Routing Information Protocol (RIP)
  static              Static routes
  traffic-engineering Traffic engineered routes

Router(config)#router rip
Router(config-router)#?
  auto-summary            Enable automatic network number summarization
  default                 Set a command to its defaults
  default-information     Control distribution of default information
  default-metric          Set metric of redistributed routes
  distance                Define an administrative distance
  distribute-list         Filter networks in routing updates
  exit                    Exit from routing protocol configuration mode
  flash-update-threshold  Specify flash update threshold in second
```

**Fig. 4.8** Comandos de configuración de protocolos de ruteo

## Configuración de interfaces

**Modos de configuración de interfaz**

La configuración se realiza mediante comandos tales como *ethemet 0*, *serial* 0, *bri* 0, *token ring* ° y comandos similares; las direcciones IP y las máscaras de subred y un comando *no shutdown* son lo mínimo requerido para considerar que una interfaz ha sido configurada. El uso del comando *ping* se presenta como medio para verificar la ***configuración de la interfaz.*** Se debe resaltar la importancia de poder hacer *ping* a las diversas interfaces de una red; *ping* es una herramienta primaria para probar la conectividad de la red.

| Comando | Descripción |
|---|---|
| ***Router (config)# interface type port*** ***Router (config)# interface type slot/port*** | El tipo incluye serial ethernet, token ring y otros. |
| ***Router (config-if)# shutdown*** | Este comando se usa para desactivar una interfaz administrativamente. |
| ***Router (config-if)# no shutdown*** | Activa una interfaz que ha sido desactivada. |
| ***Router (config-if)# exit*** | Salir del modo de configuración de interfaz actual. |

**Aspectos sobre la configuración de interfaces**

Es importante puntualizar algunos aspectos sutiles de la configuración de interfaces:

- *En las interfaces seriales,* los parámetros como velocidad de reloj y ancho de banda se pueden configurar.
- *En las interfaces Ethernet* en determinados ruteadores, se debe especificar el tipo de medio. Al configurar Frame-Relay y usar subinterfaces, se debe configurar en primer lugar la interfaz primaria.

**Descripción de las partes generales de un archivo de configuración del ruteador**

```
LAB-B#show running-config
Building configuration...
Current configuration:
!
version 11.2                          Versión del software Cisco IOS
service timestamps debug uptime       Mensajes de depuración del sistema con
                                      indicación de tiempo
service timestamps log uptime         Mensajes de registro con indicación de tiempo
no service password-encryption        Inhabilita el cifrado de contraseña del sistema.
no service udp-small-servers          Inhabilita los servicios UDP menores como,
                                      por ejemplo, Echo, Discard, Chargen
no service tcp-small-servers          Inhabilita los servicios TCP menores como,
                                      por ejemplo, Echo, Discard, Chargen, Daytime
!
hostname LAB-B                        Nombre del router
!
enable password cisco                 Contraseña del modo EXEC privilegiado,
                                      contraseña del comando "enable"
!
ip subnet-zero                        Permite subredes "subred cero", lo que significa
                                      que la dirección que identifica la subred puede
                                      ser una subred y que el router tiene una forma
                                      para distinguir las subredes
no ip domain-lookup                   No define el nombre del dominio por defecto,
                                      utilice esta opción cuando el servicio DNS no
                                      esté disponible
ip name-server 201.100.11.1           Especifica la dirección del servidor de nombre
ipx routing 1897.e38b.3101            Especifica la dirección IPX de este router, esta
                                      opción también activa el enrutamiento IPX;
                                      no es necesario activar el enrutamiento IP ya
                                      que IOS enruta paquetes IP por defecto y la
                                      configuración en ejecución (running-config) por
                                      lo general no pone en pantalla los parámetros
!                                     por defecto.
interface Ethernet0                   Inicia configuración de Ethernet 0
description connected to Cisco1501_1  Descripción de esta interfaz
ip address 219.17.100.1 255.255.255.0 Especifica la subred y la dirección IP
!
interface Ethernet1                   Inicia configuración de Ethernet 1
no ip address                         Inhabilita IP
shutdown                              Inhabilita esta interfaz; todas las interfaces se
                                      activan por defecto. Este comando la desactiva.
                                      Utilice "no shutdown" para activarla nuevamente.
!
interface Serial0                     Inicia configuración de Serial 0
description connected to LAB-C        Descripción de esta interfaz
ip address 199.6.13.1 255.255.255.0   Especifica la subred y la dirección IP
clockrate 64000                       Especifica la velocidad de reloj para este
                                      DCE (conector hembra); el otro extremo
                                      no necesita especificar la velocidad de reloj
```

**Fig. 4.9a** Ejemplo de archivos de configuración de un ruteador

```
interface Serial1                          Inicia configuración de Serial 1
description connected to LAB-A             Descripción de esta interfaz
ip address 201.100.11.2 255.255.255.0      Especifica la subred y la dirección IP
clockrate 64000                            Especifica la velocidad de reloj para este
                                           DCE (conector hembra). El otro extremo no
                                           necesita especificar la velocidad de reloj
!
router rip                    Esto inicia la configuración RIP; RIP es un protocolo de
                              enrutamiento por vector de distancia, de 15 saltos como
                              máximo, y que envía actualizaciones cada 30 segundos.
version 2                     Especifica la versión de protocolo
network 219.17.100.0          Habilita el enrutamiento de redes IP especificadas;
                              le indica a IOS que envíe y reciba actualizaciones RIP
                              hacia y desde todas las interfaces con esta red
network 199.6.13.0            Habilita el enrutamiento en redes IP especificadas;
                              le indica a IOS que envíe y reciba actualizaciones RIP
                              hacia y desde todas las interfaces con esta red.
network 201.100.11.0          Habilita el enrutamiento en redes IP especificadas,
                              le indica a IOS que envíe y reciba actualizaciones RIP
                              hacia y desde todas las interfaces con esta red
!
ip http server                Habilita la configuración del router desde un navegador
                              mediante el software ClickStart de Cisco IOS
no ip classless               No sigue regla sin clase
!
snmp-server community public RO  Especifica una contraseña para snmp
                                 de lectura solamente
snmp-server community public RO  Especifica una contraseña para snmp
                                 de lectura-escritura
!
line con 0                    Especifica el tiempo de inactividad para desconexión;
exec-timeout 5 0              si no se produce ninguna entrada desde la consola 0
                              dentro de los minutos y segundos especificados,
                              el router desconecta al usuario.
line aux 0                    Inicia la configuración de Aux 0
line vty 0 4                  Inicia la configuración de vty 0 a 4
password cisco                Especifica la contraseña para conectarse a estas líneas
login                         Habilita la verificación de contraseña
!
end                           Finaliza la configuración en ejecución (running-config)
```

**Fig. 4.9b** Ejemplo de archivos de configuración de un ruteador

**Proceso de configuración del ruteador**

A continuación se describe el proceso de configuración del ruteador

| Inicio | |
|---|---|
| **¿El prompt es correcto?** | **Entonces…** |
| ***Sí*** | Entrar al modo privilegiado.<br>***Router >enable*** |
| ***No*** | Verificar las conexiones físicas y repetir el paso 1. |
| **¿Router # OK?** | **Entonces…** |
| ***Sí*** | Establecer contraseñas.<br>***Router (config-line)# contraseña*** |
| ***No*** | Ejecutar recuperación de contraseñas y repetir el paso 2. |
| **¿Las contraseñas son correctas?** | **Entonces…** |
| ***Sí*** | Configurar interfaces.<br>***Router (config-if)#int (E0, S0, etc.)*** |
| ***No*** | ***Router (config-line)# contraseña*** |
| **¿Están bien todas las interfaces?** | **Entonces…** |
| ***Sí*** | Configurar protocolos de ruteo.<br>***Router (config)#router (RIP, IGRP usw.)*** |
| ***No*** | ***Router (config-if)#int (E0, S0, etc.)*** |
| **¿Están bien los protocolos de ruteo?** | **Entonces…** |
| ***Sí*** | Configurar DNS.<br>***Router (config)#ip host*** |
| ***No*** | ***Router (config)#router (RIP, IGRP usw.)*** |
| **¿El DNS es correcto?** | **Entonces…** |
| ***Sí*** | Examine config.<br>***Show run***<br>Verificar conectividad, etc. |
| ***No*** | ***Router (config)#ip host*** |
| **¿La configuración es correcta?** | **Entonces…** |
| ***Sí*** | Save config<br>***Copy run start*** |
| ***No*** | Inicio |
| **Stop** | |

# Listas de acceso

**Descripción**

Las *listas de acceso* son instrucciones con condiciones que establece el administrador, con la finalidad de que el ruteador manipule el tráfico cubierto por la lista de acceso de manera extraordinaria. Estas listas ofrecen un control adicional para el procesamiento de paquetes específicos de una forma única.

Dentro de las funciones que cumplen las listas de acceso dentro de un ruteador, están las siguientes:

- Implementación de procedimientos de ***seguridad / acceso***.
- *Operar como* ***firewall*** *(muro de seguridad)* de protocolo.

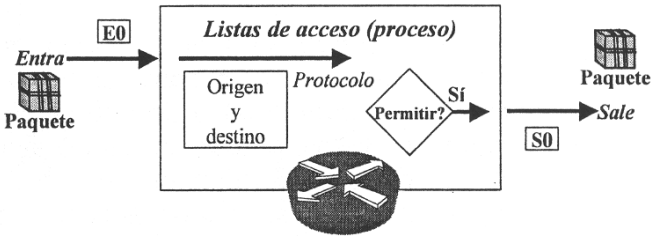



**Fig. 4.10** Lista de acceso

**Tipos de listas de acceso**

Existen principalmente los dos *tipos de listas de acceso* siguientes:

- *Listas de acceso estándar.* Estas listar para IP verifican la dirección de origen de los paquetes que pueden enrutarse. El resultado *permite* o *denega* la salida de un conjunto de protocolos completo en base a la dirección de *red/subred/host.* Por ejemplo, en la figura anterior se verifica la dirección y el protocolo de los paquetes que entran por E0:
    - Si los paquetes están permitidos salen por SO, que está agrupado en la lista de acceso.
    - Si la lista de acceso estándar denega los paquetes, estos son desechados.
- *Listas de acceso extendidas.* Estas listas verifican tanto la dirección de origen como la dirección de destino, así como también pueden verificar protocolos específicos, números de puerto y otros parámetros. Esto se traduce en mayor flexibilidad para los administradores en la determinación sobre qué revisión debe realizar la lista de acceso. Por ejemplo, en la figura anterior se puede ver que la salida de los paquetes se puede permitir *o* denegar en base a su origen o destino, por ejemplo, puede permitir el tráfico de correo electrónico entre EO y destinos específicos de SO mientras denega logins remotos o transferencia de archivos.

**Funcionamiento de las listas de acceso**

En las listas de acceso se establecen las reglas que permiten tener un control adicional sobre los paquetes que ingresan por las interfaces de entrada, sobre los paquetes que pasan a través del ruteador y sobre los paquetes que salen por las interfaces de salida del ruteador *(las listas de acceso no actúan sobre los paquetes que se originan en el ruteador mismo).*

El comienzo del proceso es el mismo, independientemente de que se utilicen o no listas de acceso *(ver figura siguiente):*

1. Cuando un paquete ingresa a una interfaz, el ruteador verifica si éste es enrutable, en caso contrario el paquete es descartado. Una entrada de la tabla de ruteo indica una dirección de destino, alguna métrica o estado de ruteo y la interfaz a utilizar.
2. A continuación el ruteador verifica si la interfaz de destino está agrupada con una lista de acceso, en caso contrario, el paquete puede enviarse al buffer de salida.
3. La interfaz E0 se ha agrupado con una lista de acceso extendida. El administrador define la lista de acceso mediante expresiones precisas y lógicas. Antes de que un paquete pueda proceder hacia esa interfaz, se prueba mediante una combinación de instrucciones de la lista de acceso asociadas a dicha interfaz.
4. En base a las pruebas de la lista de acceso extendida, el paquete se puede autorizar lo cual significa que:
    - *Las listas de entrada* continúan procesando el paquete después de recibirlo en una interfaz de entrada.

- *Las listas de salida* lo envían al buffer de salida para E0; porque los resultados de las pruebas pueden denegar el permiso, es decir, el paquete sería descartado.

5. La lista de acceso del ruteador brinda control de firewall para denegar el uso de la interfaz E0. Al descartar los paquetes, algunos protocolos devuelven un paquete que notifica al emisor que el destino es inalcanzable.

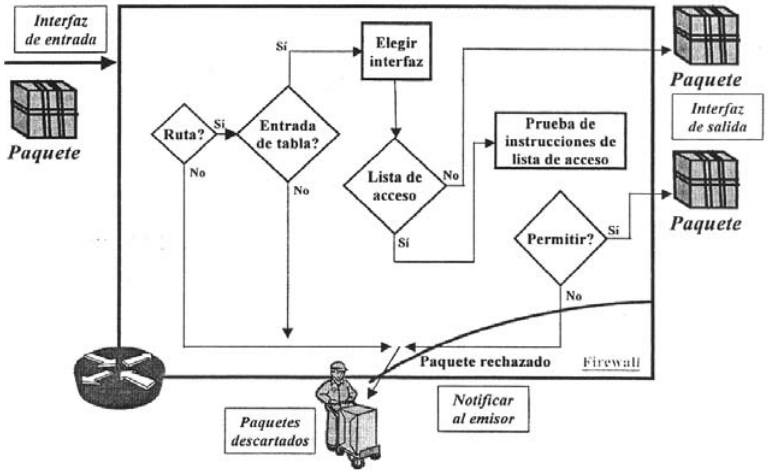



**Fig. 4.11** Funcionamiento de las listas de acceso

## Ruteo estático

**Descripción**

Las ***rutas estáticas*** son definidas manualmente por el administrador de red, que lo introduce en la configuración de un ruteador. El administrador debe actualizar manualmente esta entrada de ruta estática siempre que un cambio en la topología de la internetwork requiera una actualización.

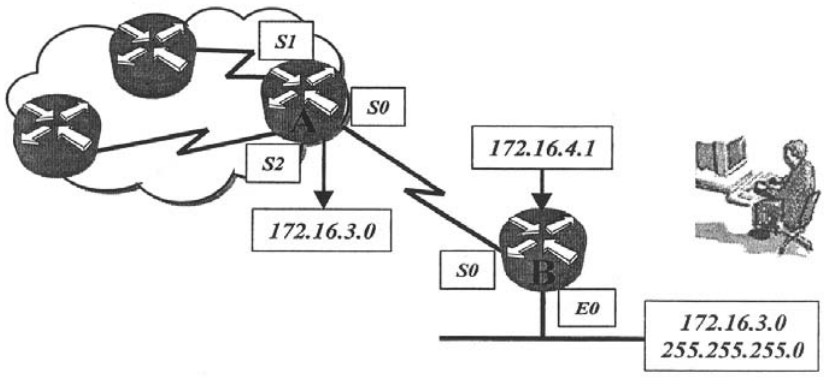



**Fig. 4.12** Rutas estáticas *(manipuladas por el administrador)*

**Características**

El ***ruteo estático*** posee varias aplicaciones útiles. Mientras que el ruteo dinámico tiende a revelar todo lo que se conoce acerca de la internetwork, es posible que por razones de seguridad se desee ocultar parte de una internetwork. El ***ruteo estático*** permite especificar la información que se desea revelar acerca de particiones restringidas.

Cuando se puede acceder a una red a través de un solo camino, una ***ruta estática*** hacia la red puede ser suficiente. Este tipo de partición se denomina ***red de conexión única.*** La ***configuración del ruteo estático*** para una red de conexión única evita el gasto que implica el ruteo dinámico.

**Rutas por default**

Para que en los equipos no exista una tabla excesivamente grande, que contenga todas las rutas a las redes que se interconecta el equipo, es de gran utilidad definir una *ruta por default.* A través de esta ruta se deberán alcanzar todas las redes destino. La ruta por default apunta a un dispositivo que actúa como compuerta de la red donde se encuentre ubicado el equipo que la posee. Entonces, las ***rutas por default*** se justifica en los siguientes puntos:

- Si cada tabla de ruteo conservara información sobre todos los destinos posibles, el espacio sería insuficiente.
- Es necesario que con un mínimo de información, el equipo pueda tomar decisiones de ruteo.
- Una técnica para mantener tablas de ruteo pequeñas consiste en enviar los datagramas a destinos predeterminados *(redes predeterminadas).*

***Las rutas por default son un caso especial de rutas estáticas. Haciendo una analogía con una carretera, la ruta por default estaría representada por la idea "si no sabes cómo llegar hacia ese lugar, sigue la carretera hasta que veas alguna indicación del camino al destino". Es importante puntualizar que las rutas por default no garantizan que el paquete encuentre su destino, pero lo coloca en redes que probablemente sepan cómo llevarlo hacia ese lugar.***

# Anexo 1

## Conversión (decimales a binarios)

**Descripción**

En la siguiente tabla se puede consultar la conversión de números decimales a números binarios, de la que se hace referencia en el capítulo 2.

| | | | |
|---|---|---|---|
| 0 00000000 | 64 01000000 | 128 10000000 | 192 11000000 |
| 1 00000001 | 65 01000001 | 129 10000001 | 193 11000001 |
| 2 00000010 | 66 01000010 | 130 10000010 | 194 11000010 |
| 3 00000011 | 67 01000011 | 131 10000011 | 195 11000011 |
| 4 00000100 | 68 01000100 | 132 10000100 | 196 11000100 |
| 5 00000101 | 69 01000101 | 133 10000101 | 197 11000101 |
| 6 00000110 | 70 01000110 | 134 10000110 | 198 11000110 |
| 7 00000111 | 71 01000111 | 135 10000111 | 199 11000111 |
| 8 00001000 | 72 01001000 | 136 10001000 | 200 11001000 |
| 9 00001001 | 73 01001001 | 137 10001001 | 201 11001001 |
| 10 00001010 | 74 01001010 | 138 10001010 | 202 11001010 |
| 11 00001011 | 75 01001011 | 139 10001011 | 203 11001011 |
| 12 00001100 | 76 01001100 | 140 10001100 | 204 11001100 |
| 13 00001101 | 77 01001101 | 141 10001101 | 205 11001101 |
| 14 00001110 | 78 01001110 | 142 10001110 | 206 11001110 |
| 15 00001111 | 79 01001111 | 143 10001111 | 207 11001111 |
| 16 00010000 | 80 01010000 | 144 10010000 | 208 11010000 |
| 17 00010001 | 81 01010001 | 145 10010001 | 209 11010001 |
| 18 00010010 | 82 01010010 | 146 10010010 | 210 11010010 |
| 19 00010011 | 83 01010011 | 147 10010011 | 211 11010011 |
| 20 00010100 | 84 01010100 | 148 10010100 | 212 11010100 |
| 21 00010101 | 85 01010101 | 149 10010101 | 213 11010101 |
| 22 00010110 | 86 01010110 | 150 10010110 | 214 11010110 |
| 23 00010111 | 87 01010111 | 151 10010111 | 215 11010111 |
| 24 00011000 | 88 01011000 | 152 10011000 | 216 11011000 |
| 25 00011001 | 89 01011001 | 153 10011001 | 217 11011001 |
| 26 00011010 | 90 01011010 | 154 10011010 | 218 11011010 |
| 27 00011011 | 91 01011011 | 155 10011011 | 219 11011011 |
| 28 00011100 | 92 01011100 | 156 10011100 | 220 11011100 |
| 29 00011101 | 93 01011101 | 157 10011101 | 221 11011101 |
| 30 00011110 | 94 01011110 | 158 10011110 | 222 11011110 |
| 31 00011111 | 95 01011111 | 159 10011111 | 223 11011111 |
| 32 00100000 | 96 01100000 | 160 10100000 | 224 11100000 |
| 33 00100001 | 97 01100001 | 161 10100001 | 225 11100001 |
| 34 00100010 | 98 01100010 | 162 10100010 | 226 11100010 |
| 35 00100011 | 99 01100011 | 163 10100011 | 227 11100011 |
| 36 00100100 | 100 01100100 | 164 10100100 | 228 11100100 |
| 37 00100101 | 101 01100101 | 165 10100101 | 229 11100101 |
| 38 00100110 | 102 01100110 | 166 10100110 | 230 11100110 |
| 39 00100111 | 103 01100111 | 167 10100111 | 231 11100111 |
| 40 00101000 | 104 01101000 | 168 10101000 | 232 11101000 |
| 41 00101001 | 105 01101001 | 169 10101001 | 233 11101001 |
| 42 00101010 | 106 01101010 | 170 10101010 | 234 11101010 |
| 43 00101011 | 107 01101011 | 171 10101011 | 235 11101011 |
| 44 00101100 | 108 01101100 | 172 10101100 | 236 11101100 |
| 45 00101101 | 109 01101101 | 173 10101101 | 237 11101101 |
| 46 00101110 | 110 01101110 | 174 10101110 | 238 11101110 |
| 47 00101111 | 111 01101111 | 175 10101111 | 239 11101111 |
| 48 00110000 | 112 01110000 | 176 10110000 | 240 11110000 |
| 49 00110001 | 113 01110001 | 177 10110001 | 241 11110001 |
| 50 00110010 | 114 01110010 | 178 10110010 | 242 11110010 |
| 51 00110011 | 115 01110011 | 179 10110011 | 243 11110011 |
| 52 00110100 | 116 01110100 | 180 10110100 | 244 11110100 |
| 53 00110101 | 117 01110101 | 181 10110101 | 245 11110101 |
| 54 00110110 | 118 01110110 | 182 10110110 | 246 11110110 |
| 55 00110111 | 119 01110111 | 183 10110111 | 247 11110111 |
| 56 00111000 | 120 01111000 | 184 10111000 | 248 11111000 |
| 57 00111001 | 121 01111001 | 185 10111001 | 249 11111001 |
| 58 00111010 | 122 01111010 | 186 10111010 | 250 11111010 |
| 59 00111011 | 123 01111011 | 187 10111011 | 251 11111011 |
| 60 00111100 | 124 01111100 | 188 10111100 | 252 11111100 |
| 61 00111101 | 125 01111101 | 189 10111101 | 253 11111101 |
| 62 00111110 | 126 01111110 | 190 10111110 | 254 11111110 |
| 63 00111111 | 127 01111111 | 191 10111111 | 255 11111111 |

# Práctica 1
## Verificando la configuración de red

## Panorama general

**Introducción**

Esta práctica nos apoyará en la familiarización de la configuración de red que se requiere para conectar una PC a una red de área local y poder acceder a Internet. El propósito de esta práctica es descubrir cuál es la configuración de red de sus estaciones de trabajo y de qué manera se utiliza. Se deberá revisar la configuración y los controladores de la Tarjeta de Interfaz de Red *(NIC)* y la configuración de protocolo TCP/IP para la estación de trabajo de cliente típica de Windows en una red Ethernet basada en servidores. Esta información es muy valiosa cuando se tiene algún problema para conectarse a una red o siempre que se tenga que configurar una nueva estación de trabajo.

**Objetivo** Al término de la práctica, el participante realizará la configuración de red de las estaciones de trabajo conectadas ala red de área local para visualizar la división de tráfico TCP/IP.

**Material y equipo**

Para realizar esta práctica se requiere de lo siguiente:

- 1 PC con Windows NT (como servidor)
- PC's con Windows 98 y tarjeta de red Ethernet con conectores RJ45
- Un hub del tipo plug&play (conectar y listo) con al menos 8 conectores RJ45.
- 10 cables Ethernet de conexión directa (straight-through) de par trenzado no blindado (UTP o Híbrido) Categoría 5 (CAT 5) con conectores RJ45 en los extremos, para conexión PC-nodo.

## Desarrollo

**Conexiones**

Realiza la conexión de las PC 's y el Hub utilizando los cables de red requeridos.

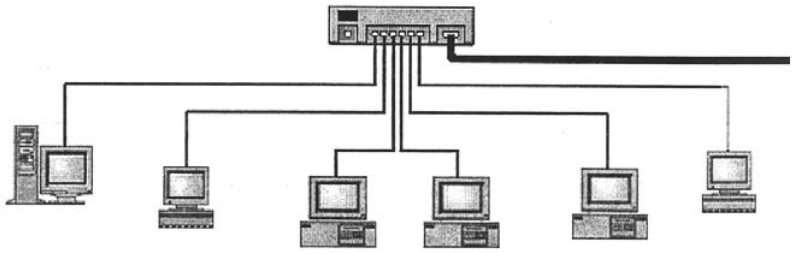


**Fig. P1.1** Conexión estaciones de trabajo-hub

***Verifica que las luces de enlace que corresponden al hub y las Tarjetas de interfaz de red (NIC) de las estaciones de trabajo estén encendidas, lo cual indicará que todas las conexiones físicas son las correctas.***

**Configuración de las estaciones de trabajo**

1. Rotula tu estación de trabajo según te indique el instructor en base a la tabla siguiente (es recomendable también que los ruteadores y hubs se rotulen).

2. Establece la configuración de red correspondiente a la estación de trabajo asignada, en base a la tabla siguiente:

| No. de Estación de Trabajo | Dirección IP de Estación de Trabajo | Máscara de subred de Estación de Trabajo | Dirección IP del gateway por defecto |
|---|---|---|---|
| 1 | 192.5.5.10 | 255.255.255.0 | 192.5.5.1 |
| 2 | 192.5.5.11 | 255.255.255.0 | 192.5.5.1 |
| 3 | 192.5.5.12 | 255.255.255.0 | 192.5.5.1 |
| 4 | 205.7.5.10 | 255.255.255.0 | 205.7.5.1 |
| 5 | 205.7.5.11 | 255.255.255.0 | 205.7.5.1 |
| 6 | 205.7.5.12 | 255.255.255.0 | 205.7.5.1 |

***La dirección del gateway por defecto, no es necesaria si no se tiene ruteador.***

Para realizar lo anterior:

Activa ***Inicio / Configuración / Panel de control / Red*** y da clic en el botón *Propiedades,* con lo que aparecerá la siguiente caja de diálogo donde podrás especificar una dirección IP ala estación de trabajo que te corresponda.

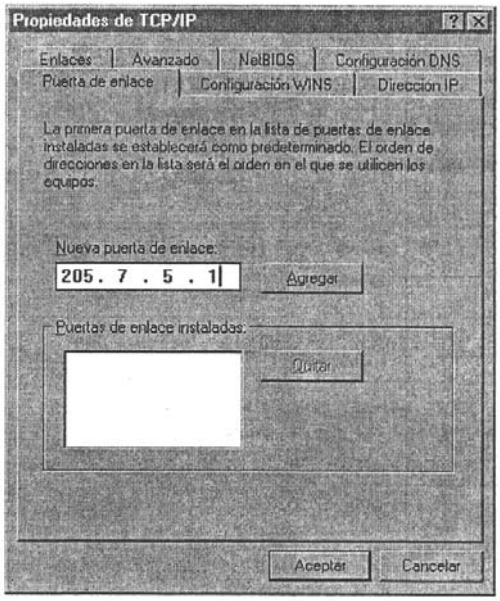



**Fig. P1.2** Caja de dialogo para especificar una dirección IP

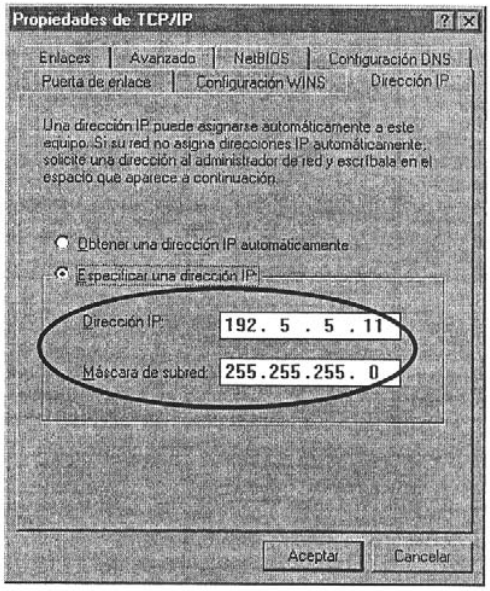



**Fig. P1.3** Caja de diálogo para especificar puerta de enlace

***Para especificar la puerta de enlace se puede poner la misma dirección de la estación de trabajo correspondiente si no se cuenta con ruteador***.

***Las siguientes herramientas son una ayuda para verificar la configuración de red y controlar que la NIC esté funcionando correctamente:***

- ***Desde el indicador del sistema operativo ejecuta WINIPCFG.EXE (Windows 95 ó 98) o IPCONFIG.EXE (Windows NT).***
- ***Activa Panel de control / sistema / Administrador de dispositivos para verificar que la NIC y los controladores estén funcionando correctamente.***

3. Desde el indicador del sistema operativo, ejecuta el comando ***ping*** para realizar pruebas de funcionamiento a cada uno de los host.

**Ejemplo:**

Si te encuentras en la estación de trabajo número 11 puedes mandar un ping para comprobar la conexión a cada una de las estaciones de trabajo *(de la* 2 *a la* 6), como se muestra a continuación:

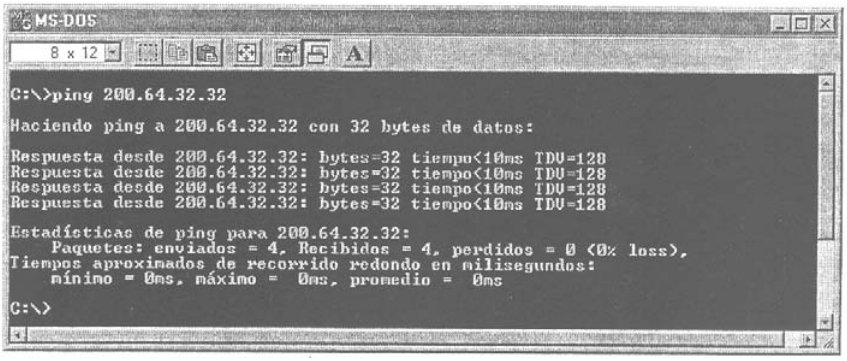



**Fig. P1.4** Ejemplo de conexión sin problemas

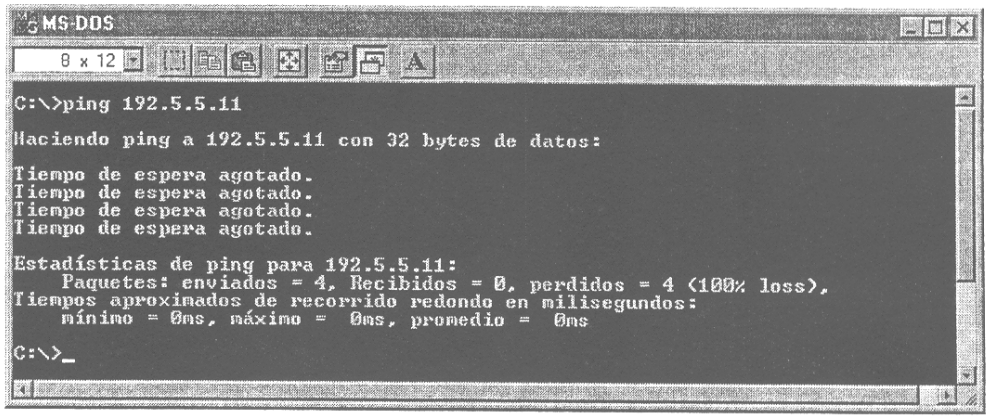



**Fig. P1.5** Ejemplo de conexión con problemas

# Práctica 2
## Inicialización del ruteador

## Panorama general

**Introducción**

Los tres pasos principales en la secuencia de inicio de un PC son las pruebas automáticas de arranque del hardware, la carga del sistema operativo, y la selección de una aplicación por parte del usuario. El ruteador pasa por un proceso semejante: se verifica el hardware *(a través de códigos almacenados en la ROM),* se carga el software IOS, y se carga la configuración del ruteador. Esta práctica presenta la interfaz del usuario de línea de comando, del Sistema Operativo de Internetwork *(IOS).* Se realizará la conexión al ruteador y se utilizarán distintos niveles de acceso para introducir comandos en "Modo usuario" y "Modo privilegiado". La interfaz de comandos del IOS es el método más común para configurar un ruteador de Cisco.

**Objetivo** Al término de la práctica, el participante:

- Inicializará el ruteador usando la conexión correspondiente para accesar a él.
- Realizará la configuración inicial del ruteador desde el diálogo de configuración.
- Accesará a los distintos niveles de configuración.
- Verificará la función de algunos comandos disponibles en los distintos niveles de acceso.

**Material y equipo**

Para realizar esta práctica se requiere de lo siguiente:

- 1 PC con Windows NT (como servidor).
- Programa HyperTerminal cargado en la PC asignada como estación de trabajo
- 6 PC's con Windows 98 y tarjeta de red Ethernet (los controladores de la tarjeta deben estar disponibles) con conectores RJ45.
- Un hub del tipo plug&play (conectar y listo) con al menos 8 conectores RJ45.
- 10 cables UTP CA T 5, con conectores RJ45 en los extremos, para conexión PC-nodo.
- Cable de conexión directa (Straight Through), para las conexiones hub-PC y hub router.
- Adaptador de DB-9 a RJ-45 para Conexiones al puerto serial.
- 2 Cables Rollover (de consola), para la conexión PC-ruteador.
- 2 Ruteadores CISCO 2500/3000 con versiones de IOS 12.1 (2500) ó 9.14 ó v. 9.21 (3000).

## Desarrollo

**Identificación**

Es importante obtener información del ruteador con el que se va a general trabajar, para identificar sus características físicas y comenzar a relacionar estas con su función.

Llena la siguiente tabla con la información requerida:

| Examina del ruteador ... | Información |
|---|---|
| *Número de modelo* | |
| *Puerto de consola*<br>*¿A cuál de los puertos de la terminal de consola (estación de trabajo de PC) está conectado?* | |
| *Cables*<br>*¿Qué tipo de cable es el cable de consola (straigh-through, rollover o cross-connect)?* | |

**Conexión para accesar al ruteador**

Podemos decir que básicamente un ruteador es una microcomputadora dedicada que internamente tiene una unidad de procesamiento central, un sistema operativo, RAM y ROM.

Lo que es importante identificar es que los ruteadores no cuentan con unidad de disco, teclado ni monitor, con lo que surge la pregunta ***¿ Cómo accesar al ruteador para configurarlo ?***

Una de las formas es conectarse directamente al ruteador a través de una estación de trabajo, suministrándole así un monitor y un teclado, que constituirán su ***"consola"*** que nos permitirá introducir comandos y así comunicarnos directamente con el ruteador.

***En esta práctica se propone trabajar con una estación de trabajo (con el programa Hyper Terminal (emulación de terminal) cargado) que funcione como la consola del ruteador.***
**Se** ***requiere conectar dicha estación de trabajo con el ruteador mediante la interfaz de consola del ruteador utilizando un cable rollover*** **(** ***de consola), como se muestra en la figura siguiente.***

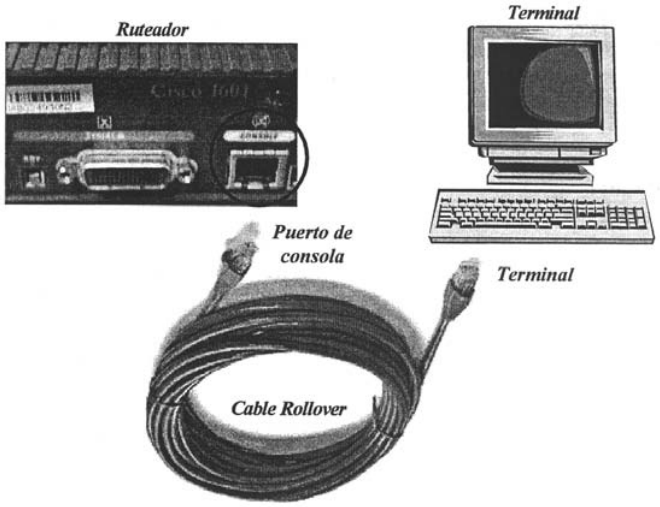



**Fig. P2.1** Conexión ruteador-terminal mediante cable rollover

***El programa Hyper Terminal de la estación de trabajo debe tener la siguiente configuración:***

| | |
|---|---|
| ***Puerto COM:*** | ***Directo a COM1*** |
| ***Bits por segundo:*** | ***9600*** |
| ***Bits de datos:*** | ***8*** |
| ***Paridad:*** | ***Ninguno*** |
| ***Bits de parada:*** | ***2*** |
| ***Control de flujo:*** | ***Ninguno*** |

**¿Cómo accesar al ruteador?**

Para accesar al ruteador, se debe crear una sesión que conecte el puerto serial de la terminal con la interfaz de consola del ruteador:

1. Desde la terminal que está conectada ala interfaz de consola del ruteador, da clic en ***Inicio / Programas / Accesorios / HyperTerminal / Hyper Terminal***, aparecerá la siguiente caja de diálogo:

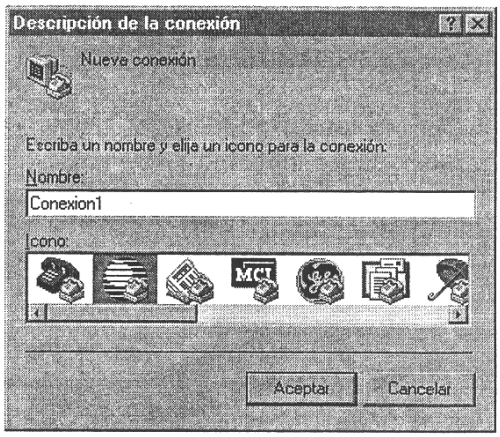



**Fig. P2.2** Descripción de la conexión

2. Teclea el nombre y selecciona el icono que deseas para la conexión.
3. Da clic en Aceptar, aparecerá la siguiente ventana de la conexión creada, desde donde se podrá accesar al ruteador:

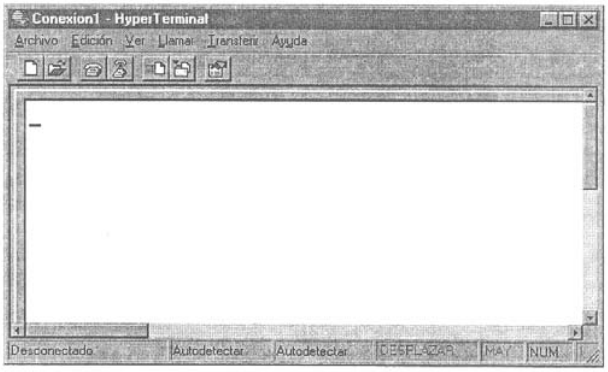



**Fig. P2.3** Ventana de conexión para accesar al ruteador

**Configuración inicial**

Para realizar una configuración inicial se requiere que el ruteador esté apagado y con la memoria NVRAM vacía, de esta manera, al prender el ruteador este no detectará configuración en la NVRAM y entrará al modo de ***Configuración Inicial*** *(la cual presenta en la consola un cuadro de diálogo interactivo basado en prompts que ayuda a crear una configuración básica inicial).*

***Si la memoria NVRAM no está vacía, se requiere hacer lo siguiente:***

1. ***Entrar al modo privilegiado.***
2. ***Ejecutar el comando erase startup-confíg.***
3. ***Apagar el ruteador.***
4. ***Prender el ruteador para que se inicialice.***

**¿Qué pasa cuando se enciende un ruteador?**

Como ya se había mencionado en el capítulo 5, cuando se enciende un ruteador este realiza una prueba automática de encendido. Durante esta prueba automática, el ruteador ejecuta diagnósticos desde la ROM en todos los módulos de hardware. Estos diagnósticos verifican la operación básica del CPU, memoria y puertos de interfaz de red. Después de verificar las funciones de hardware, el ruteador procede a inicializar el software.

***Verifica que las luces ubicadas* en *la parte trasera del ruteador (que indican que todo está correcto) estén encendidas.***

**Ejercicio de configuración inicial**

Realiza la configuración inicial del ruteador, siguiendo los cuadros de diálogo interactivos que se presentan en pantalla, como se muestra en el siguiente ejemplo:

```
System Bootstrap, Version 11.1(20)AA2, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
Copyright (c) 1999 by cisco Systems, Inc.
C3600 processor with 65536 Kbytes of main memory

Main memory is configured to 64 bit mode with parity disabled


program load complete, entry point: 0x80008000, size: 0x657ed0

Self decompressing the image :
################################################################################
################################################################################
#
Editado...

TN3270 Emulation software.
Primary Rate ISDN software, Version 1.1.
4 Ethernet/IEEE 802.3 interface(s)
2 Channelized E1/PRI port(s)
DRAM configuration is 64 bits wide with parity disabled.
125K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)
```

**Fig. P2.4a** Pantalla de prueba automática de encendido

```
         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: yes



At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: no


First, would you like to see the current interface summary? [yes]:


Controller Timeslots D-Channel Configurable modes Status
E1 0/0     31         15        pri/channelized     Administratively up
E1 0/1     31         15        pri/channelized     Administratively up

Any interface listed with OK? value "NO" does not have a valid configuration

Interface              IP-Address      OK? Method Status                Protocol
Ethernet3/0            unassigned      NO  unset  up                    down
Ethernet3/1            unassigned      NO  unset  up                    down
Ethernet3/2            unassigned      NO  unset  up                    down
Ethernet3/3            unassigned      NO  unset  up                    down

Configuring global parameters:

  Enter host name [Router]: nombre del ruteador

  The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: password para entrar al modo privilegiado

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: password para entrar al modo privilegiado, solo es
                         utilizado cuando no se declara el secret
```

**Fig. P2.4b** Pantallas de diálogo de configuración

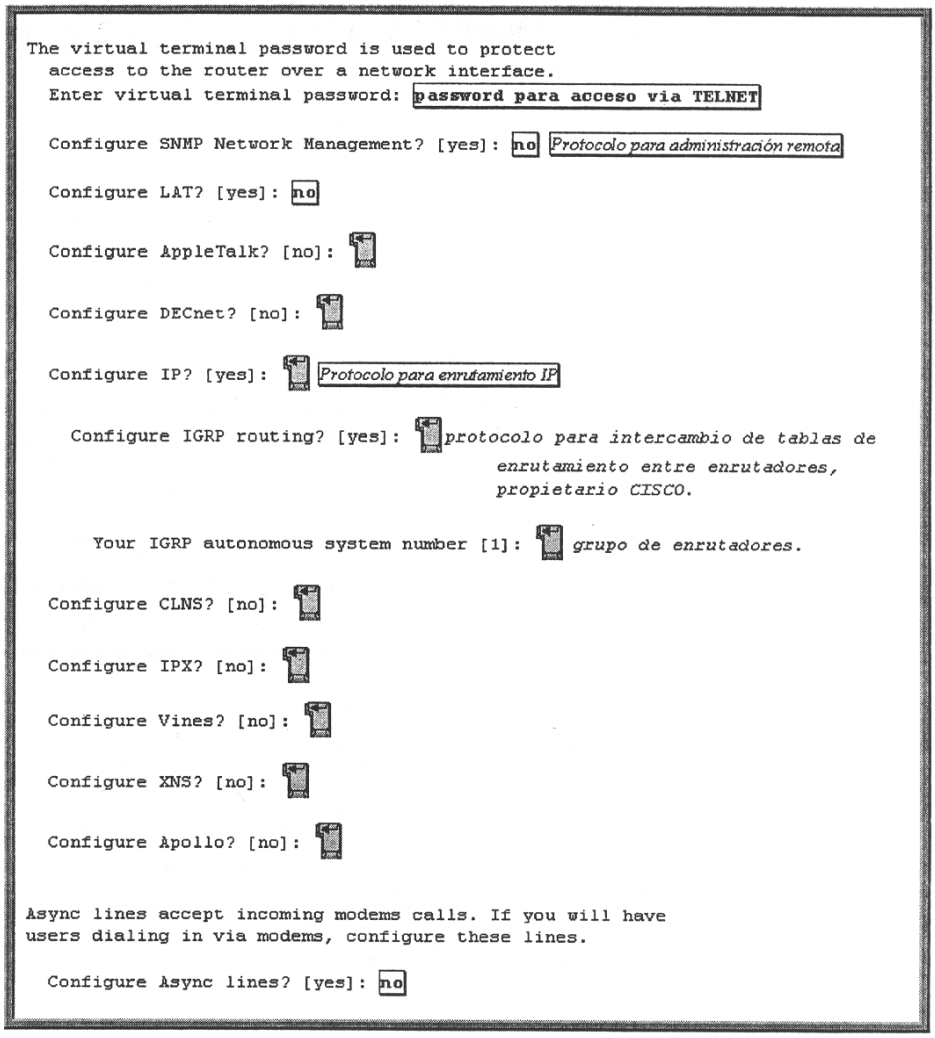



**Fig. P2.4c** Pantallas de diálogo de configuración

***Continúa con la configuración según lo indique el instructor (Ctrl C para salir de la configuración) o hasta finalizar que es cuando el sistema muestra la configuración que ha sido creada, ofreciendo opciones de salvado de dicha configuración.***
***Observa en el diálogo que cuando se desea dar la [respuesta por default], sólo requieres presionar para que el sistema tome dicha respuesta.***

**Acceso al modo usuario**

Cuando el ruteador indica que está disponible, al presionar  se accesa al modo usuario:

```
Router con0 is now available


Press RETURN to get started.


Router>_
```

*Indicador de modo usuario*

**Fig. P2.5** Pantalla de acceso Modo Usuario

**Identificación de funciones de comandos modo usuario**

Presiona  en el indicador de modo usuario, y se desplegará la siguiente pantalla con la lista de comandos disponibles para este nivel de acceso.

```
Router>?
  access-profile   Apply user-profile to interface
  clear            Reset functions
  connect          Open a terminal connection
  disable          Turn off privileged commands
  disconnect       Disconnect an existing network connection
  enable           Turn on privileged commands
  exit             Exit from the EXEC
  help             Description of the interactive help system
  lock             Lock the terminal
  login            Log in as a particular user
  logout           Exit from the EXEC
  mrinfo           Request neighbor and version information from a multicast
                   router
  mstat            Show statistics after multiple multicast traceroutes
  mtrace           Trace reverse multicast path from destination to source
  name-connection  Name an existing network connection
  pad              Open a X.29 PAD connection
  ping             Send echo messages
  PPP              Start IETF Point-to-Point Protocol (PPP)
  resume           Resume an active network connection
  rlogin           Open an rlogin connection
  set              Set system parameter (not config)
 --More--
```

**Fig. P2.6** Pantalla 1 de comandos disponibles del modo usuario

***Observa que al final de la pantalla aparece -- More -- lo cual indica que el desplegado no ha terminado, presiona*** Barra espaciadora ***para desplegar la siguiente pantalla.***

**Ejercicio de comandos modo usuario**

Ejecuta lo que se indica en la siguiente tabla y describe lo que se despliega al hacerlo:

| | Comando | Descripción |
|---|---|---|
| 1 | *s?* | |
| 2 | *show ?* | |
| 3 | *ping ?* | |
| 4 | *help* | |
| 5 | *enable* | |
| 6 | *exit* | |

***Es importante mencionar que el signo? Permite obtener información de los comandos de varias maneras, en el caso del ejercicio:***

- ***s? (sin espacio) desplegó los comandos que inician con s.***
- ***show ? (con espacio) desplegó todas las opciones del comando show.***

**Identificando resultados del comando show versión**

Estando en modo usuario, es posible ver información del sistema, con el comando show versión. A continuación se presenta la pantalla del resultado generado por un ruteador CISCO 2501 al ejecutar dicho comando:

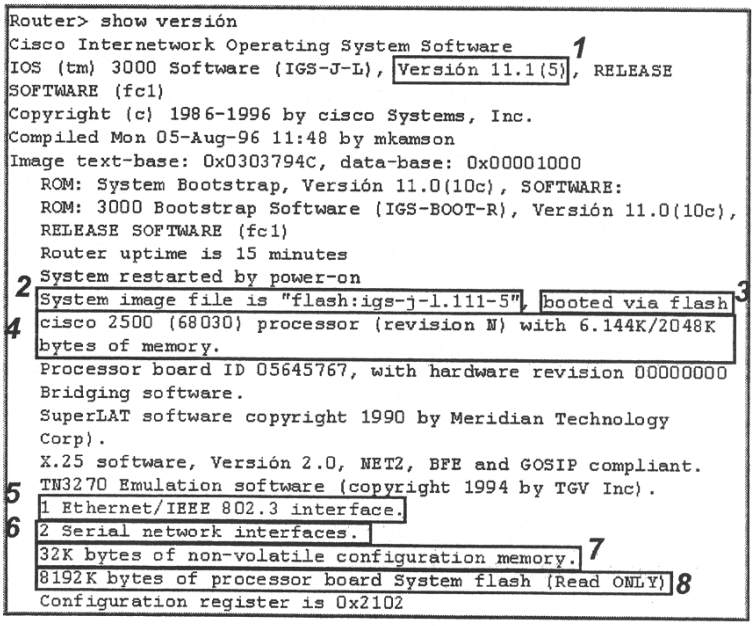



**Fig. P2.7** Pantalla de resultado del comando *show version*

En base a la pantalla anterior, podemos identificar los siguientes datos:

| Dato | Resultado |
|---|---|
| ***1. Versión de IOS*** | Versión 11.1(5) |
| ***2. Nombre del archivo de imagen de sistema (IOS)*** | flash:igs-j-l.111-5 |
| ***3. Dónde se arrancó la imagen de IOS*** | La memoria Flash |
| ***4. Tipo de procesador (CPU) y cantidad de memoria RAM que tiene el ruteador*** | Procesador Cisco 2500 (68030) (revisión N) con 6144K/2048K bytes de memoria |
| ***5. Interfaces Ethernet del ruteador*** | 1 interfaz Ethernet/IEEE 802.3 |
| ***6. Interfaces seriales del ruteador*** | 2 interfaces de red seriales |
| ***7. Cantidad de NVRAM*** | 32K bytes de memoria de configuración no volátil |
| ***8. Cantidad de memoria flash que tiene el ruteador*** | 8192K bytes de memoria flash de Sistema en la placa del procesador (SÓLO lectura) |

**Ejercicio show versión**

Ejecuta el comando ***show versión*** y anota en la tabla siguiente los datos que arroja en relación al ruteador con el cual estás trabajando:

| Dato | Resultado |
|---|---|
| ***Versión de IOS*** | |
| ***Nombre del archivo de imagen de sistema (IOS)*** | |
| ***Dónde se arrancó la imagen de IOS*** | |
| ***Tipo de procesador (CPU) y cantidad de memoria RAM que tiene el ruteador*** | |
| ***Interfaces Ethernet del ruteador*** | |
| ***Interfaces seriales del ruteador*** | |
| ***Cantidad de NVRAM*** | |
| ***Cantidad de memoria flash que tiene el ruteador*** | |

***Para no teclear comandos completos, es posible:***

- ***Usar el modo abreviado, es decir, teclear la parte que identifica al comando, por ejemplo, en el caso del ejercicio basta teclear sh ver (en lugar de show version).***
- ***Teclear una parte del comando y completarlo presionando***  ***.***

**Acceso al modo privilegiado**

Para accesar al modo privilegiado del ruteador, teclea ***enable*** *(o en)* en el indicador de modo usuario, y presiona  . Aparecerá la siguiente pantalla:

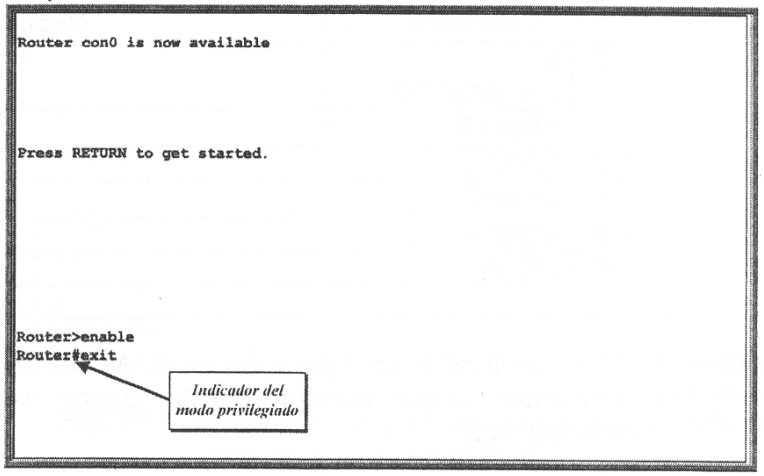



**Fig. P2.8** Pantalla de acceso modo privilegiado

**Identificación de funciones de comandos modo privilegiados**

Presiona  en el indicador de modo privilegiado, y se desplegará la siguiente pantalla con la lista de comandos disponibles para este nivel de acceso:

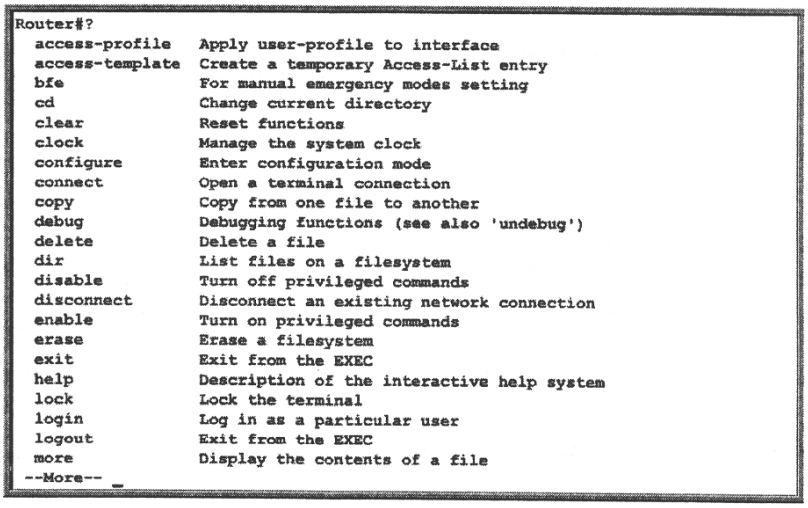



**Fig. P2.9** Pantalla 1 de comandos disponibles del modo privilegiado

**Ejercicio de comandos modo privilegiado**

Ejecuta lo que se indica en la siguiente tabla y describe lo que se despliega al hacerlo:

| | Comando | Descripción |
|---|---|---|
| 1 | *t?*<br>*(sin espacio)* | |
| 2 | *show ?* | |
| 3 | *enable* | |
| 4 | *clear ?* | |
| 5 | *copy ?* | |
| 6 | *clock* | |

**Verificando la configuración de la RAM**

Para verificar la configuración en RAM del ruteador activo, ejecuta el comando ***show running-config*** desde el indicador del modo privilegiado:

```
Router#sh ru
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
enable password
!
!
ip subnet-zero
!
!
!
interface Ethernet0
 no ip address
 shutdown
!
 --More--
```

**Fig. P2.10a** Ejemplo del archivo de configuración que se guarda en la RAM

```
interface Ethernet1
 no ip address
 shutdown
!
interface Serial0
 no ip address
 shutdown
!
!
!
ip classless
!
!
line con 0
 transport input none
line aux 0
line vty 0 4
 session-timeout 60
!
end
```

**Fig. P2.10b** Ejemplo del archivo de configuración que se guarda en la RAM

**Verificando la configuración de la NVRAM**

Para verificar la configuración en NVRAM del ruteador activo, ejecuta el comando ***show startup-config*** desde el indicador del modo privilegiado:

```
Router#sh star
Using 1129 out of 129016 bytes
!
version 12.0
service config
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
logging buffered 4096 debugging

editado...

line vty 0 4
password prov
 login
!
end
```

**Fig. P2.11** Ejemplo del archivo de configuración en la NVRAM

***Para salir de la sesión teclea exit en el indicador y presiona***  .

# Práctica 3
## Configuración básica del ruteador

## Panorama general

**Introducción**

Una de las primeras tareas básicas de configuración del ruteador es asignarle un nombre. Se considera que el nombre del ruteador es el nombre de host y es el nombre que muestra el prompt del sistema. Si no se configura ningún nombre, el nombre del ruteador por defecto del sistema es *Ruteador.* Es posible asignarle un nombre al ruteador en el modo de configuración global.

Otra tarea recomendada es configurar un cartel con el mensaje del día para que se visualice en todas las terminales conectadas. Este cartel se visualizará al momento de la conexión y es útil para transmitir mensajes que afectan a todos los usuarios del ruteador *(por ejemplo, interrupciones inminentes del sistema)*

**Objetivo** Al término de la práctica, el participante realizará la configuración básica de un ruteador desde el modo de configuración global.

**Material y equipo**

Para realizar esta práctica se requiere de lo siguiente:

- 1 PC con Windows NT (como servidor).
- Programa HyperTerminal cargado en la PC asignada como estación de trabajo
- 6 PC's con Windows 98 y tarjeta de red Ethernet (los controladores de la tarjeta deben estar disponibles) con conectores RJ45.
- Un hub del tipo plug&play (conectar y listo) con al menos 8 conectores RJ45.
- 10 cables UTP CA T 5, con conectores RJ45 en los extremos, para conexión PC-nodo.
- Cable de conexión directa (Straight Through), para las conexiones hub-PC y hub router.
- Adaptador de DB-9 a RJ-45 para Conexiones al puerto serial.
- 2 Cables Rollover (de consola), para la conexión PC-ruteador.
- 2 Ruteadores CISCO 2500/3000 con versiones de lOS 12.1 (2500) ó 9.14 ó 9.21 (3000).

## Desarrollo

**Descripción**

Como se mencionó en el capítulo 5, el modo de configuración global, general implementa poderosos comandos de una línea que ejecutan tareas simples de configuración. Estando en este modo, se pueden configurar parámetros globales del ruteador.

**Acceso al modo de configuración global**

Para accesar al modo de configuración global se debe realizar lo siguiente:

1. Accesar al modo privilegiado
2. Ejecutar el comando ***config***, el sistema preguntará si se desea realizar la configuración desde terminal, memoria o red, dando por default la opción [terminal].
3. Presiona  , el sistema indicará que has entrado a la configuración de comandos, uno por línea.

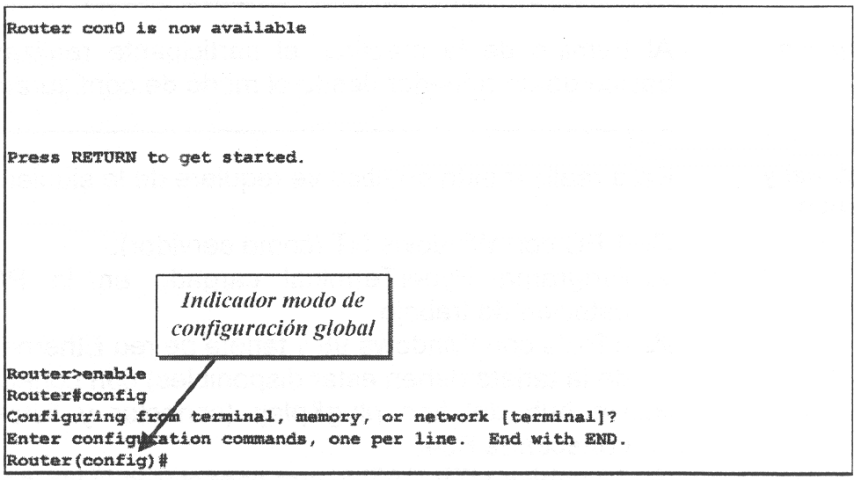
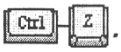



**Fig. P3.1** Pantalla de acceso al modo configuración global

***Observa que el prompt cambia agregando (config), lo cual indica que se ha accesado al modo de configuración global.***

***Para salir de este modo de configuración debes presionar*** 

.

**Identificación de función de comandos modo de configuración global**

Presiona [?] en el indicador de modo de configuración global, y se desplegará la siguiente pantalla con la lista de comandos disponibles en este modo:

```
Router(config)#?
  aaa                      Authentication, Authorization and Accounting.
  access-list              Add an access list entry
  alias                    Create command alias
  appletalk                Appletalk global configuration commands
  arap                     Appletalk Remote Access Protocol
  arp                      Set a static ARP entry
  async-bootp              Modify system bootp parameters
  autonomous-system        Specify local AS number to which we belong
  banner                   Define a login banner
  boot                     Modify system boot parameters
  bridge                   Bridge Group.
  buffers                  Adjust system buffer pool parameters
  busy-message             Display message when connection to host fails
  call-history-mib         Define call history mib parameters
  chat-script              Define a modem chat script
  clock                    Configure time-of-day clock
  config-register          Define the configuration register
  decnet                   Global DECnet configuration subcommands
  default                  Set a command to its defaults
  default-value            Default character-bits values
  dnsix-dmdp               Provide DMDP service for DNSIX
  dnsix-nat                Provide DNSIX service for audit trails
--More--
```

**Ejercicio de comandos modo de configuración global**

Ejecuta los siguientes comandos de este modo, para identificar su función y descríbela brevemente en la tabla siguiente:

| | Comando | Función |
|---|---|---|
| 1 | *access-list* | |
| 2 | *clock* | |
| 3 | *boot* | |
| 4 | *banner* | |
| 5 | *arp* | |

**Asignando nombre al ruteador**

Como se ha venido observando, cuando no se ha configurado el nombre del ruteador, el nombre por default del sistema es *Ruteador*. Para asignarle nombre al ruteador activo:

1. Estando en el modo de configuración global, teclea ***hostname*** seguido del nombre que deseas darle al ruteador.
2. Presiona Ctrl + Z para salir de este modo de configuración.
3. Verifica la configuración en RAM y NVRAM (como se vió en la práctica 2), y observa que el nombre del host no ha sido modificado en la NVRAM.

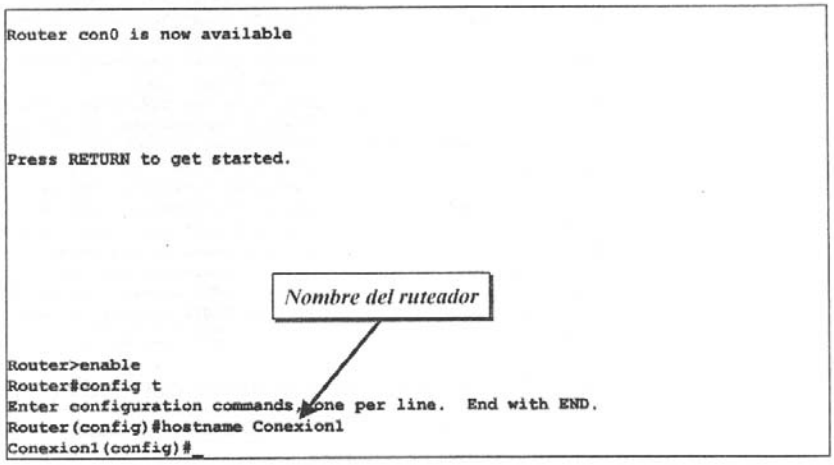



**Fig. P3.3** Asignación de nombre al ruteador

***Observa que el prompt cambia de acuerdo al nombre asignado al ruteador.***

**Estableciendo contraseña para modo privilegiado**

Para establecer la contraseña secreta para accesar al modo privilegiado, debes realizar lo siguiente:

1. Estando en el modo de configuración global, teclea ***enable secret*** seguido de la contraseña que deseas establecer.
2. Presiona Ctrl + Z para salir de este modo de configuración.
3. Entra al modo de acceso usuario.
4. Entra al modo de acceso privilegiado.

```
Press RETURN to get started.




Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]? t
Enter configuration commands, one per line.  End with END.
Router(config)#hostname Conexion1
Conexion1(config)#enable secret curso
Conexion1(config)#
00:02:04: %SYS-5-CONFIG_I: Configured from console by console
Conexion1#disable
Conexion1>enable
Password:
Conexion1#_
```

**Fig. P3.4** Contraseña secreta de acceso al modo privilegiado

***Observa que la próxima vez que entres al modo privilegiado, el sistema solicitará la contraseña secreta para entrar a este nivel de acceso.***

***Para establecer la contraseña de texto del modo privilegiado, la cual es opcional, teclea enable password seguido de la contraseña que deseas establecer.***

**Estableciendo contraseña para consola y TELNET**

Para establecer las contraseñas para consola y Telnet, debes realizar lo siguiente:

1. Estando en el modo de configuración global, teclea ***line console 0*** y presiona  , el prompt cambiará ahora a ***(config-line)***.
2. Teclea ***login*** y presiona  .
3. Teclea ***password*** seguido del password que deseas establecer para consola y presiona  .
4. Teclea ***line vty 0 4*** y presiona  .
5. Teclea ***login*** y presiona  .
6. Teclea ***password*** seguido del password que deseas establecer para Telnet.

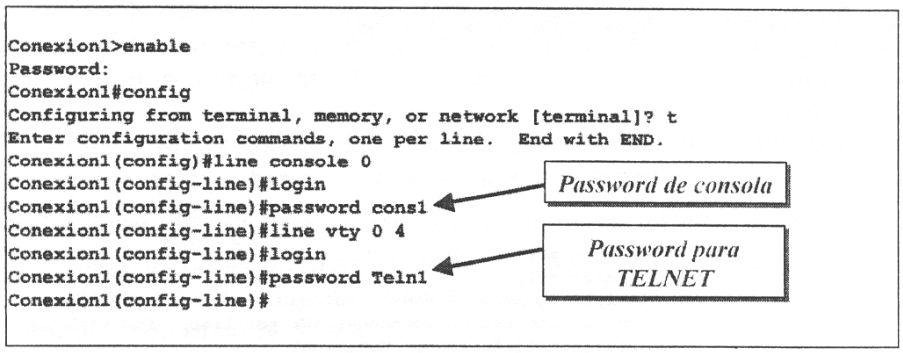



**Fig. P3.5** Contraseñas para consola y Telnet

7. Presiona Ctrl + Z para salir de este modo de configuración.
8. Verifica los cambios realizados con ***sh running-config***.

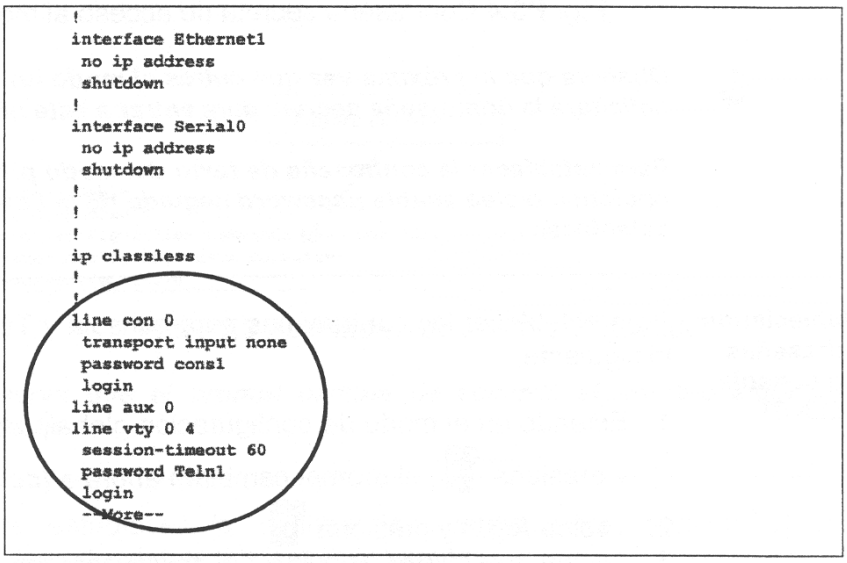



**Fig. P3.6** Verificando contraseñas establecidas para consola y Telnet

**Verificando información de interfaces**

Estando en el modo privilegiado, mediante el comando ***show interlaces*** podemos obtener información sobre características, configuración, estado y estadísticas de una interfaz. Es posible obtener información de todas las interfaces o bien de alguna en específico. Este comando es de gran utilidad para realizar tareas de mantenimiento. A continuación se presenta un ejemplo de la información relacionada con este comando:

```
Router#show interfaces
Ethernet0 is administratively down, line protocol is down
   Hardware is Lance, address is 0010.7b81.4e2c(bia 0010.7b81.4e2c)
   MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
      reliability 252/255, txload 1/255, rxload 1/255
   Encapsulation ARPA, loopback not set
   Keepalive set (10 sec)
   ARP type: ARPA, ARP Timeout 04:00:00
   Last input never, output 00:00:20, output hang never
   Last clearing of "show interface" counters never
   Queueing strategy: fifo
   Output queue 0/40, 0 drops; input queue 0/75, 0 drops
   5 minute input rate 0 bits/sec, 0 packets/sec
   5 minute output rate 0 bits/sec, 0 packets/sec
      0 packets input, 0 bytes, 0 no buffer
      Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
      0 input packets with dribble condition detected
      6 packets output, 360 bytes, 0 underruns
      6 output errors, 0 collisions, 3 interface resets
      0 babbles, 0 late collision, 0 deferred
      6 lost carrier, 0 no carrier
      0 output buffer failures, 0 output buffers swapped out
 --More--
```

**Fig. P3.7a** Información generada con el comando *show interfaces*

```
Ethernet1 is administratively down, line protocol is down
   Hardware is Lance, address is 0010.7b81.4e2d(bia 0010.7b81.4e2d)
   MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
      reliability 252/255, txload 1/255, rxload 1/255
   Encapsulation ARPA, loopback not set
   Keepalive set (10 sec)
   ARP type: ARPA, ARP Timeout 04:00:00
   Last input never, output 00:00:20, output hang never
   Last clearing of "show interface" counters never
   Queueing strategy: fifo
   Output queue 0/40, 0 drops; input queue 0/75, 0 drops
   5 minute input rate 0 bits/sec, 0 packets/sec
   5 minute output rate 0 bits/sec, 0 packets/sec
      0 packets input, 0 bytes, 0 no buffer
      Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
      0 input packets with dribble condition detected
      6 packets output, 360 bytes, 0 underruns
      6 output errors, 0 collisions, 3 interface resets
      0 babbles, 0 late collision, 0 deferred
      6 lost carrier, 0 no carrier
      0 output buffer failures, 0 output buffers swapped out
Serial0 is administratively down, line protocol is down
 --More--
```

**Fig. P3.7b** Información generada con el comando *show interfaces*

```
Serial0 is administratively down, line protocol is down
   Hardware is HD64570
   MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
      reliability 255/255, txload 1/255, rxload 1/255
   Encapsulation HDLC, loopback not set
   Keepalive set (10 sec)
   Last input never, output never, output hang never
   Last clearing of "show interface" counters never
   Input queue: 0/75/0 (size/max/drops); Total output drops: 0
   Queueing strategy: weighted fair
   Output queue: 0/1000/64/0 (size/max total/threshold/drops)
      Conversations  0/0/256 (active/max active/max total)
      Reserved Conversations 0/0 (allocated/max allocated)
   5 minute input rate 0 bits/sec, 0 packets/sec
   5 minute output rate 0 bits/sec, 0 packets/sec
      0 packets input, 0 bytes, 0 no buffer
      Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 packets output, 0 bytes, 0 underruns
      0 output errors, 0 collisions, 1 interface resets
      0 output buffer failures, 0 output buffers swapped out
      0 carrier transitions
      DCD=down  DSR=down  DTR=down  RTS=down  CTS=down
Router#
```

**Fig. P3.7c** Información generada con el comando *show interfaces*

***Para obtener información sobre alguna interfaz en específico se hace mediante el comando show interfaces seguido de la interfaz que deseamos consultar (por ejemplo s0).***

**Configurando una ruta estática**

Desde el modo de configuración global, es posible configurar una ruta estática mediante el comando ***ip route*** *(con el cual* se *define la ruta hacia una red* o *una subred IP destino),* seguido de los parámetros de descripción correspondiente, con la siguiente estructura:

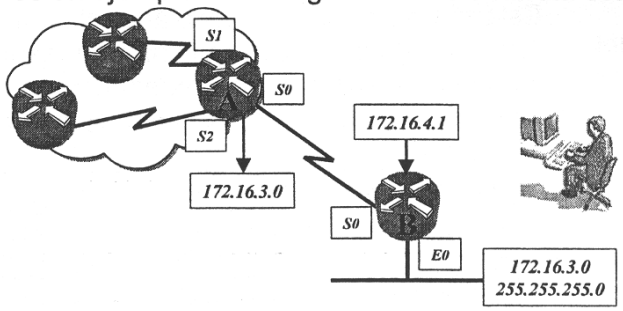
***Router (config)#ip route network [mask] {addresslinterface} [distanceJ***

**Donde:**

| Parámetro | Descripción |
|---|---|
| ***network*** | Es la red o subred destino. |
| ***mask*** | Es la máscara de subred. |
| ***address*** | Es la dirección IP del ruteador del salto siguiente. |
| ***interface*** | Es el nombre de la interfaz que se debe utilizar para llegar a la red destino. |
| ***distance*** | Es la distancia administrativa. |

**Ejercicio de configuración de una ruta estática**

El siguiente es un ejemplo de configuración de una ruta estática:




*ip route 172.16.3.0 255.255.255.0 172.16.4.1*

Donde:

| | |
|---|---|
| ***ip route 172.16.3.0*** | Especifica una ruta estática hacia la subred destino. |
| ***255.255.255.0*** | La máscara de subred que indica el uso de 8 bits para la subred están activos. |
| ***172.16.4.1*** | Dirección IP del ruteador del salto siguiente en la ruta hacia el destino. |

En base a las especificaciones de la red implementada en el aula, práctica la configuración de rutas estáticas hacia diferentes destinos.

**Verificando la tabla de ruteo**

Estando en el modo privilegiado, mediante el comando ***show ip route*** podemos obtener información sobre la tabla de ruteo del ruteador activo. Este comando identifica las redes o subredes conocidas, ya sea conectadas directamente o bien a través de otros elementos de la red, como se muestra en el siguiente ejemplo:

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
       T - traffic engineered route

Gateway of last resort is not set

     1.0.0.0/28 is subnetted, 2 subnets
C       1.1.1.0 is directly connected, Ethernet3/0
C       1.1.2.0 is directly connected, Serial0/0:0
```

*Dos subredes directamente conectadas*

**Fig. P3.8** Información generada con el comando *show ip route*

**Informe resumido del estado de las interfaces**

Estando en el modo privilegiado, el comando ***show ip interface brief*** *(sh ip int b)* nos muestra un informe resumido del estado actual de las interfaces *(caídas* y *levantadas)* con su correspondiente dirección IP, como se muestra en el siguiente ejemplo:

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Serial0/0:0            1.1.2.3         YES NVRAM  up                    up
Ethernet3/0            1.1.1.5         YES NVRAM  up                    up
Ethernet3/1            unassigned      YES unset  administratively down down
Ethernet3/2            unassigned      YES unset  administratively down down
Ethernet3/3            unassigned      YES unset  administratively down down
```

**Fig. P3.9** Informe del estado de las interfaces

# Práctica 4
## Configuración de interfaces del ruteador

## Panorama general

### Introducción

Muchas funciones se habilitan de forma individual por interfaz. Los comandos de configuración de interfaz modifican la operación de un puerto Ethernet, Token Ring, FDDI o serial. Los subcomandos de interfaz siempre se colocan a continuación de un comando de interfaz; el comando de interfaz define el tipo de interfaz.

La configuración se realiza mediante comandos tales como ethernet 0, serial 0, bri 0, token ring 0 y comandos similares; las direcciones IP y las máscaras de subred y un comando no shutdown son lo mínimo requerido para considerar que una interfaz ha sido configurada.

El uso del comando ping se presenta como medio para verificar la configuración de la interfaz. Se debe resaltar la importancia de poder hacer ping a las diversas interfaces de una red; ping es una herramienta primaria para probar la conectividad de la red.

**Objetivo** Al término de la práctica, -el participante configurará las interfaces del ruteador mediante los comandos de interfaz correspondientes.

### Material y equipo

Para realizar esta práctica se requiere de lo siguiente:

- 1 PC con Windows NT (como servidor).
- Programa HyperTerminal cargado en la PC asignada como estación de trabajo
- 6 PC's con Windows 98 y tarjeta de red Ethernet (los controladores de la tarjeta deben estar disponibles) con conectores RJ45.
- Un hub del tipo plug&play (conectar y listo) con al menos 8 conectores RJ45.
- 10 cables UTP CA T 5, con conectores RJ45 en los extremos, para *conexión PC-nodo.*
- Cable de conexión directa (Straight Through), para las conexiones hub-PC y hub router.
- Adaptador de DB-9 a RJ-45 para Conexiones al puerto serial.
- Cables Rollover (de consola), para la conexión *PC-ruteador.*
- 2 Ruteadores CISCO 2500/3000 con versiones de lOS 12.1 (2500) ó 9.14 ó 9.21 (3000).

## Desarrollo

### Configurando puerto o interfase específicos

Estando en el modo de configuración global, es posible configurar algún puerto o interfaz en especifico entrando al modo de configuración especifica, como se muestra en el siguiente ejemplo:

```
Router(config)#interface s 0/0:0
Router(config-if)#?
Interface configuration commands:
  access-expression   Build a bridge boolean access expression

editado...

  ip                  Interface Internet Protocol config commands
  ipx                 Novell/IPX interface subcommands
  isis                IS-IS commands
  iso-igrp            ISO-IGRP interface subcommands
  keepalive           Enable keepalive
  vines               VINES interface subcommands
  xns                 XNS interface subcommands
```

**Fig. P4.1** Configuración de puerto o interfaz específicos

***Observa que el prompt del sistema cambia indicando el elemento que se está configurando.***

### Verificando controladores de las Interfaces

Estando en el modo privilegiado, el comando show controllers ofrece información acerca de los controladores de las interfaces. Esta información es muy útil cuando se configuran interfaces seriales y se desea conocer si el puerto es DTE o DCE, como se muestra en el siguiente ejemplo:

```
Router#show controllers
Controller 0 is type: unbalanced E1 in slot 0
Serial interface 0/0:0  Munich32 version 3.2
Total chip configuration successes: 12, failures: 0, timeouts: 0
  Interrupt Queue Element(index=3551): interrupt is enabled
  0x0000000 0x0000000 0x0000000 0x0000000 0x0000000 0x0000000
  0x0000000 0x0000000 0x0000000 0x0000000 0x0000000 0x0000000

Editado...

  02 params=0x40000000 data ptr=0x0000000 next ptr=0x4D00439C
  List of timeslots (sw): 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
                          18 19 20 21 22 23 24 25 26 27 28 29 30 31
  List of all timeslots (hw):
   00:20002000 01:00FF00FF 02:00FF00FF 03:00FF00FF 04:00FF00FF 05:00FF00FF
   06:00FF00FF 07:00FF00FF 08:00FF00FF 09:00FF00FF 10:00FF00FF 11:00FF00FF
   12:00FF00FF 13:00FF00FF 14:00FF00FF 15:00FF00FF 16:00FF00FF 17:00FF00FF
   18:00FF00FF 19:00FF00FF 20:00FF00FF 21:00FF00FF 22:00FF00FF 23:00FF00FF
   24:00FF00FF 25:00FF00FF 26:00FF00FF 27:00FF00FF 28:00FF00FF 29:00FF00FF
   30:00FF00FF 31:00FF00FF
  Bandwidth: 1984, idle channel: Unassigned, idle ts bitfield: 0x0
  0 missed datagrams, 1 overruns, 0 memory errors
  0 transmitter underruns, 0 throttles, 0 enables, 0 bad interrupt elements
```

**Fig. P4.2** Información de controladores de las interfaces

### Configurando dirección IP y activación de interfaz

Para configurar dirección IP y activar una interfaz, realiza lo siguiente (ver figura siguiente):

1. Verifica la información de la interfaz que deseas configurar.
2. Entra al modo de configuración global.
3. Especifica la interfaz a configurar con ***interfase*** seguido de la descripción de interfaz.
4. Especifica la dirección IP con ***ip address*** seguido de la dirección IP y la máscara de subred correspondiente.
5. Establece una descripción de la configuración con ***description*** seguido de la descripción que deseas *(opcional).*
6. Activa la interfaz con el comando no shutdown.

```
Router#sh int e 3/1
Ethernet3/1 is administratively down, line protocol is down
  Hardware is AmdP2, address is 00d0.baf4.2bb1 (bia 00d0.baf4.2bb1)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 252/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
Editado...

Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router (config)#interface ethernet 3/1
Router (config-if)#ip address 1.1.8.12 255.255.255.240
Router (config-if)#description configurando_ethernet
Router (config-if)#no shutdown
Router (config-if)#ctrl+z
Router#
00:35:50: %LINK-3-UPDOWN: Interface Ethernet3/1, changed state to up
00:35:51: %SYS-5-CONFIG_I: Configured from console by console
```

**Fig. P4.3** Asignación de dirección IP y activación de interfaz

***Realiza el procedimiento anterior p*ara cada una de las interfaces. *Guarda la configuración actual en la configuración inicial con Copy running-config startup-config desde el modo privilegiado.***

**Verificando configuración de interfaces**

Verifica la información de la interfaz ya configurada:

1. Sal del modo de configuración global.
2. Verifica el resultado con ***sh ip int brief***.
3. Verifica el resultado con ***show running-config***.

```
Router#sh ip int brief
Interface              IP-Address      OK? Method Status                Protocol
Serial0/0:0            1.1.2.3         YES manual up                    up
Ethernet3/0            1.1.1.5         YES manual up                    down
Ethernet3/1            1.1.8.12        YES manual up                    down
Ethernet3/2            unassigned      YES unset  administratively down down
Ethernet3/3            unassigned      YES unset  administratively down down
```

**Fig. P4.4** Verificación de configuración con *sh ip int brief*

```
Router#show running-config
Building configuration...

Current configuration:
!
editado...
!
interface Ethernet3/1
 description configurando_ethernet
 ip address 1.1.8.12 255.255.255.240
 no ip directed-broadcast
!
interface Ethernet3/2
 no ip address
 no ip directed-broadcast
 shutdown
```

**Fig. P4.5** Verificación de configuración con *show running-config*

# Práctica 5
## Determinación de la mejor ruta

### Panorama general

**Introducción**

Dos de los propósitos principales de un ruteador son la determinación de la ruta mediante la búsqueda en la tabla de enrutamiento, y conmutar el paquete hacia la interfaz correcta. Es un buen momento para comparar esta toma de decisiones inteligente *(basada en el direccionamiento IP jerárquico)* con la toma de decisiones menos inteligente de los puentes y switches.

Para el tráfico que atraviesa una nube, la determinación de ruta se produce en la capa de red *(Capa* 3). La función de determinación de ruta permite al ruteador evaluar las rutas disponibles hacia un destino y establecer el manejo preferido de un paquete.

Los servicios de enrutamiento utilizan información sobre la topología al evaluar las rutas de una red. Esta información la puede configurar el administrador de red o se puede recopilar a través de procesos dinámicos ejecutados en la red.

La capa de red hace interfaz con las redes y proporciona servicios de entrega de paquetes de máximo esfuerzo y de extremo a extremo para su usuario, la capa de transporte. La capa de red utiliza la tabla de enrutamiento IP para enviar paquetes desde la red origen ala red destino.
Después de que el ruteador determina qué ruta debe utilizar, procede a enviar el paquete. Toma el paquete que aceptó en una interfaz y lo envía hacia otra interfaz o puerto que represente la mejor ruta hacia el destino del paquete.

Los ruteadores pueden soportar varios protocolos de enrutamiento independientes y mantener tablas de enrutamiento para varios protocolos enrutados. Esta capacidad le permite al ruteador entregar paquetes de varios protocolos enrutados a través de los mismos enlaces de datos.

**Objetivo** Al término de la práctica, el participante simulará la determinación de la mejor ruta que debe seguir un ruteador en base a número de saltos y costo.

**Material y equipo** Sólo diagrama de la página siguiente.

## Desarrollo

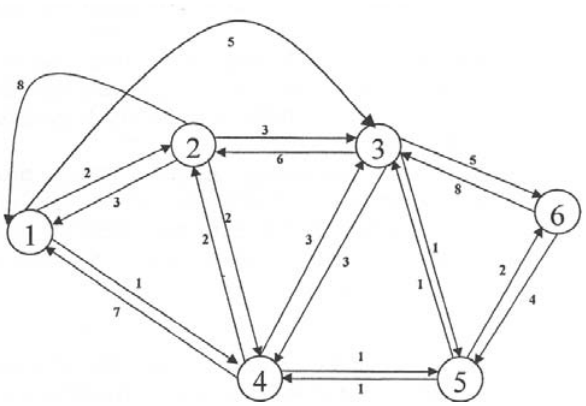
**Descripción general**

La elección de una ruta se fundamenta generalmente en algún criterio de funcionamiento. El más simple consiste en elegir el camino con menor número de saltos a través de la red. Este es un criterio que se puede medir fácilmente y que debería minimizar el consumo de recursos de la red. Una generalización del criterio de menor número de saltos lo constituye el encaminamiento de mínimo costo. En este caso se asocia un costo a cada enlace y, para cualesquiera dos estaciones conectadas, se elige aquella ruta a través de la red que implique el costo mínimo.

**Ejercicio**

En la figura siguiente se muestra una red en la que las dos líneas con flecha entre cada par de nodos representa un enlace entre ellos, y los números asociados representan el costo actual del enlace en cada sentido.

1. ¿Cuál es la ruta más corta *(menor número de saltos)* desde el nodo 1 hasta el nodo 6? *Respuesta* 1-3-6, *costo* (5+5=10).
2. ¿Cuál es la ruta con costo mínimo? *Respuesta* 1-4-5-6, *costo* (1 +1 +2=4).
3. ¿Cuál es la ruta más corta y la ruta con costo mínimo del nodo 1 al 5?
4. ¿Cuál es la ruta más corta y la ruta con costo mínimo del nodo 1 al 3?




***Los costos se asignan a los enlaces en función de los objetivos de diseño. Por ejemplo, el costo podría estar inversamente relacionado con la velocidad (es decir, a mayor velocidad menor costo) o con el retardo actual de la cola asociada al enlace. En el primer caso, la ruta de mínimo costo maximizaría la eficiencia, mientras que en el segundo se minimizaría el retardo.***

# Anexo 3

## Glosario de comandos de configuración para ruteadores CISCO

**Contenido**

En este anexo se presenta lo siguiente:


| Tema | Ver página |
|---|---|
| Comandos modo privilegiado | A3 - 2 |
| Comandos modo usuario | A3 - 15 |
| Edición de comandos de línea | A3 - 18 |


## Comandos modo privilegiado

**Router#?** Despliega la lista de comandos disponibles en este modo.

**Router# access-enable** Crea una entrada temporal de la lista de acceso.

**Router# access- template** Crea una entrada temporal de la lista de acceso.

**Router# appn** Envía una orden al subsistema del APPN.

**Router# atmsig** Ejecuta comandos de señal Atm.

**Router# bfe** Pone en modo de emergencia manual.

**Router# calendar** Manejar el calendario del hardware.

**Router# cd** Cambia el dispositivo actual.

**Router# clear** Restablece funciones.

**Router# clear line** Termina una sesión remota a tu ruteador *(desde la consola).*

**Router#clock** Maneja el reloj del sistema.

**Router#cmt** Inicia o detiene las funciones de conexión FDDI.

**Router# configure** Entra al modo de configuración.

**Router# connect** Abre una conexión terminal.

**Router#copy** Copia los datos de configuración o de la imagen.

**Router#copy {file source} {file destination}** Se utiliza para copiar los archivos de configuración entre la RAM *(running- config),* la NVRAM *(startup-config)* y un servidor FTP.

**Router#debug** Funciones de depuración.

**Router#delete** Borra un archivo.

**Router#dir** Lista los archivos del dispositivo dado.

**Router# disable** Deshabilita los comandos del modo privilegiado.

**Router# disconnect** Desconecta una conexión de la red existente.

**Router# enable** Permite accesar al modo privilegiado.

**Router# erase** Borra flash o memoria de configuración.

**Router#erase startup-config** Elimina la copia de respaldo del archivo de configuración en la NVRAM.

**Router# exit** Salir de EXEC.

**Router# format** Dar formato al dispositivo.

**Router# help** Describe la ayuda interactiva del sistema.

**Router# lat** Abre una conexión lat.

**Router# lock** Pone candado a la terminal.

**Router# login** Habilita la verificación de contraseña. Identifica como un usuario particular.

**Router# logout** Salir de EXEC.

**Router# mbranch** Traza una ruta multicast descendente a la ramificación (bifuración) del árbol.

**Router# mrbranch** Traza una ruta inversa multicast a la ramificación (bifuración) del árbol.

**Router# mrinfo** Pide información del vecino y de la versión de un ruteador multicast.

**Router# mstat** Muestra las estadísticas después de que se rastrea la ruta del multicast múltiple.

**Router# mtrace** Rastrea la ruta multicast inversa desde el destino a la fuente.

**Router# name- connection** Nombra una conexión de red existente.

**Router# ncia** Inicia o detiene el servidor NCIA.

**Router# no** Desactiva las funciones de depuración.

**Router# pad** Abre una conexión X.29 PAD (atenuador fijo).

**Router# ping** Envía mensajes de eco para evaluar la confiabilidad de ruta a host, las demoras en la ruta, y si se puede acceder al host, o si éste está funcionando.

**Router#ping ip-address** ping *(packet internet groper)* se utiliza para verificar la conectividad. El ping también despliega información del mínimo, el promedio y el máximo tiempo que le toma a los paquetes ping encontrar el sistema especificado y regresar.

**Router# ppp** Arranque del protocolo Punto a Punto (PPP).

**Router# pwd** Despliega el dispositivo actual.

**Router# reboot** Vuelve a cargar el ruteador, haciéndolo pasar por todo el proceso de inicio.

**Router# reload** Detiene y realiza un reinicio.

**Router# resume** Resume una conexión de red activa.

**Router# rsh** Ejecuta un comando remoto.

**Router# sdlc** Envía frames de prueba SDLC.

**Router# send** Envía mensajes a otras líneas tty.

**Router#setup** Entra al modo de configuración inicial. El propósito básico del modo *setup* es realizar rápidamente una sencilla configuración con las facilidades mínimas para cualquier ruteador que no puede encontrar su configuración desde otra fuente.

**Router# show** Muestra la información del sistema activo.

**Router# show cdp** Despliega información de CDP *(Cisco Oeveloped Neighbor),* tiene disponibles las opciones de *entry, interface, neighbors* y *traffic.*

**Router# show controller type-interface number** Despliega información de su interfaz física. Este comando es usado con las interfaces seriales para determinar qué tipo de cable está conectado sin tener que inspeccionarlo físicamente.

**Router# show interfaces** Este comando muestra estadísticas de las interfaces de red en el ruteador.

Donde:

| Campo | Descripción |
|---|---|
| **ARP type** | Tipo de Protocolo de Resolución de Direcciones asignado. |
| **BW** | Ancho de banda de la interfaz en kbits/s. El parámetro ancho de banda es usado para calcular la métrica de los protocolos de ruteo. |
| **Bytes** | Número total de bytes, incluyendo datos y encapsulación MAC, transmitidos por el sistema. |
| **bytes input** | Número total de bytes, incluyendo datos y encapsulación MAC, recibidos en paquetes libres de errores por el sistema. |
| **Collisions** | Número de mensajes retransmitidos debido a una colisión Ethernet. Esto es normalmente el resultado de una LAN sobreextendida *(cables demasiado largos, más de un repetidor entre estaciones, o demasiados pueltos en cascada).* Un paquete que colisiona se cuenta sólo una vez en los paquetes de salida. |
| **CRC** | Chequeo de redundancia cíclica generada por la estación LAN originaria o el dispositivo final cuando no coincide su cálculo de chequeo con los datos recibidos. En una LAN, esto usualmente indica ruido o problemas en la transmisión en la interfaz LAN o en su bus. Un número alto de CRC's es normalmente el resultado de colisiones o que una estación esté transmitiendo mal sus datos. |
| **DLY** | Retardo de la interfaz en microsegundos. |
| **Encapsulation** | Método de encapsulación asignado a la interfaz. |
| **Ethernet ...is {up** \| **down** \| **administratively down}.** | Indica si la interfaz física está actualmente activa o si el administrador fa deshabilitó. |
| **Five minute input rate, Five minute output rate** | Promedio de bits y paquetes transmitidos por segundo en los últimos 5 minutos. |
| ***frame*** | Número de paquetes recibido incorrectamente teniendo un error CRC. En una LAN, esto es normalmente el resultado de colisiones o del mal funcionamiento del dispositivo Ethernet. |
| **giants** | Número de paquetes descartados por exceder el tamaño máximo de un paquete. Cualquier paquete Ethernet con más de 1 ,518 bytes es considerado un gigante. |
| **Hardware** | Indica el tipo de hardware *(por ejemplo MCI Ethernet, SCI, cBus Ethernet)* y su dirección MAC. |
| **ignored** | Número de paquetes ignorados por la interfaz porque la interfaz física corrió lento en los buffers internos. Estos buffers son diferentes que otros buffers del sistema mencionados anteriormente. Las tormentas de broadcasts y el ruido pueden causar que la cuenta de *ignored* se |

| | |
|---|---|
| | incremente. |
| **input error** | Incluye en la cuenta a runts, giants, no buffer, CRC, frame, overrun e ignored. Otros errores relacionados con la entrada pueden también causar que la cuenta de errores entrantes sea incrementada, y algunos datagramas podrían tener más de un error, por lo que esta suma podría no coincidir con la suma de errores de entrada. |
| **Input packets with dribble condition detected** | El error dribble bit indica que una trama es ligeramente mas larga. Este contador de errores de trama es incrementado sólo para propósitos de información, el ruteador acepta la trama. |
| **Internet Address** | Indica la dirección de Internet seguida por un prefijo. |
| **keepalive** | Indica si el keepalive fue enviado. |
| **Last clearing** | Tiempo en que los contadores que miden las estadísticas acumulativas mostradas en este informe *(número de bytes transmitidos y recibidos}* fueron puestos a cero por última vez.<br>*** Indica que el tiempo pasado es demasiado grande para ser desplegado. |
| **Last input** | Dato en hrs/min/seg desde que el último paquete fue *recibido exitosamente* por una interfaz, lo que permite saber cuando una interfaz muerta falló. |
| **line protocol is {up \| down}** | Indica si los procesos del software que se ocupan del protocolo de la línea consideran la interfaz utilizable *(es decir si los keepalives son exitosos).* Si la interfaz pierde tres keepalives consecutivos, el protocolo de línea es puesto en down. |
| **load** | Carga de la interfaz (255/255 es *completamente saturada),* calculada como un promedio exponencial en 5 min. |
| **loopback** | Indica si el loopback está o no configurado. |
| **MTU** | Unidad máxima de transmisión de la interfaz. |
| **no buffers** | Número de paquetes que se recibieron pero fueron descartados por no tener espacio en buffer en el sistema principal. |
| **output** | Dato en hrs/min/seg desde que el último paquete fue *transmitido exitosamente* por una interfaz, lo que permite saber cuando una interfaz muerta falló. |
| **output hang** | Dato en hrs/min/seg desde que la interfaz fue restablecida por última vez (o *si nunca 10 ha sido)* debido a una transmisión que duró demasiado tiempo. |
| **Output queue, input queue, drops** | Número de paquetes de salida y entrada en cola. Cada número es seguido por una diagonal, el tamaño máximo de la cola, y el número de paquetes eliminados por estar llena la cola. |
| **overrun** | Número de veces que el hardware de recepción fue incapaz de entregar los datos recibidos al buffer porque la velocidad de entrada excedió a la habilidad de entrega de datos del receptor. |
| **packets input** | Número total de paquetes libres de errores recibidos por el, sistema. |
| **packets output** | Número total de mensajes transmitidos por el sistema. |
| **Received ...broadcasts** | Número total de paquetes broadcast o multicasts recibidos por esta interfaz. El número de broadcasts debe mantenerse tan bajo como sea posible *(aproximadamente de menos del* 20 % *del total de paquetes entrantes).* |
| **rely** | Confiabilidad de la interfaz (255/255 es *e1100% de confiabilidad),* calculada como un promedio exponencial en 5 min. |
| **runts** | Número de paquetes descartados por ser más pequeños que el tamaño mínimo de un paquete. Cualquier paquete Ethernet con menos de 64 bytes es considerado un enano. Los enanos son causados usualmente por colisiones *(más de un enano por cada millón de bytes recibidos debe ser investigado).* |

| | |
|---|---|
| **Underruns** | Número de veces que el transmisor ha corrido más rápido de lo que el ruteador puede entregar. Puede ser que en algunas interfaces nunca se reporte. |

**Router# show session** Verifica la conectividad vía Telnet, despliega la lista de hosts que han establecido una sesión.

**Router# show user** Muestra si el puerto de consola está activo y la lista de todas las sesiones Telnet, con la dirección IP o el alias IP del host origen, en el dispositivo local.

**Router# start- chat** Inicia una charla escrita en línea.

**Router# tarp** Comandos TARP (Protocolo de Resolución de Referencia ID).

**Router# telnet ip-address** Establece una conexión remota vía telnet.

**Router# terminal** Activa los parámetros de terminal de línea.

**Router# test** Prueba subsistemas, memoria e interfaces.

**Router# tn3270** Abre una conexión tn3270.

**Router# undebug** Desactiva funciones de depuración.

**Router# undelete** Recuperar un archivo borrado.

**Router# verify** Verifica la prueba checksum de un archivo Flash.

**Router# where** Lista las conexiones activas.

**Router# which-route** Hace que OSI consulte la tabla de ruteo y despliega resultados.

**Router# write** Escribe la configuración activa a la memoria, red o terminal.

**Router# x3** Conjunto de parámetros X.3 en PAD.

**Router#show flash** Despliega el contenido de la memoria flash.

**Router#show hosts** Despliega la lista de nombres de hosts y sus direcciones asociadas.

**Router#show running- config** Muestra los archivos de configuración activos ubicados en la RAM.

**Router#show startup-config** Despliega el archivo de configuración que se encuentra almacenado en la NVRAM, y la cantidad de memoria utilizada.

**Router#slip** Arranque de IP Serial-Línea *(SLIP)*

**Router#telnet** Abre una conexión Telnet.

**Router#term ip netmask- format {bitcount** | **decimal** | **hexadecimal}** Despliega la configuración del formato de la máscara de red para la sesión actual.

**Router#trace ip-address** Permite conocer las rutas que los paquetes toman entre dispositivos.

**Router# traceroute** Traza la ruta al destino.

**Router#tunnel** Abre una conexión de túnel.

**Router# xremote** Entra al modo XRemote.

**Router (config)# enable password** Configura el password de enable para entrar al modo de configuración.

**Router (config)# enable secret password** Configura el password *"secreto"* para entrar al modo de configuración

**Router (config)# exit** Sale del modo de configuración de interfaz actual.

**Router** (**config)#interf ace {type interface} {number interfase}** Este comando te permite accesar a la interfase deseada para configurarla.

**Router (config)# interface type number** Acceso a la configuración de una interfaz específica. Donde el tipo incluye serial, Ethernet, Token Ring fddi, hssi, loopback, dialer, null, async, atm, bri y tunnel, y el número es usado para identificar una interface individual.

**Router (config)# interface type slot port** Acceso a la configuración de una interfaz en un ruteador modular.

**Router (config)#ip domain- lookup** Habilita la translación de nombre a direcciones en el ruteador, lo cual significa que el ruteador enviará paquetes de broadcast del sistema de nombres.

**Router (config)#ip host name address** Define un nombre de host como equivalente de una dirección IP.

**Router (config)#ip name-server server- address1 [[server- address2] ... [server- address6]]** Define el o los hosts que pueden proveer el servicio de nombres *(DNS),* pueden existir hasta un máximo de 6 direcciones IP especificadas como un servidor de nombres.

**Router (config)# line console 0** Acceso a la configuración de la consola.

**Router (config)#line vty 0 4** Acceso a las líneas de acceso remoto vty.

**Router (config)# no shutdown** Activa la interfaz que ha sido des activada.

**Router (config)# shutdown** Deshabilita la interfaz.

**Router (config-if)# bandwith BW** Configura el ancho de banda de la interfaz.

**Router (config-if)# clock rate rate** Configura la velocidad del reloj en la interfaz.

**Router (config-if)# description {banner text}** Estando dentro de la interfaz deseada, con este comando puedes añadirle una descripción.

**Router (config-if)# ip address ip- address subnet-mask** Inicia el procesamiento IP en una interfaz del ruteador, y le asigna una dirección y una máscara de subred.

**Router (config-li ne )# exec-timeout 00** Este comando asegura que jamás se saldrá de la consola.

**Router (config-line)# ip netmask- format {bitcount I decimal I hexadecimal}** Configura el formato de máscara de red para una línea específica.

**Router (config-line)# login** Permite configurar el login de acceso de la consola.

**Router (config-line)# password password** Configuración del password

**Router** (**config- subif)# encapsulation isl vlan identifier** Habilita ISL en una subinterfaz del ruteador perteneciente a una VLAN.

## COMANDOS MODO USUARIO

**Router> access-enable** Crea una entrada temporal de la lista de acceso.

**Router>cd** Cambia el dispositivo actual.

**Router>clear** Restablece funciones.

**Router> connect** Abre una conexión terminal.

**Router>dir** Lista los archivos del dispositivo dado.

**Router> disconnect** Desconecta una conexión de red existente.

**Router> enable** Habilita el modo privilegiado.

**Router>exit** Sale de EXEC.

**Router>help** Describe la ayuda interactiva del sistema.

**Router>lat** Abre una conexión lat.

**Router>lock** Cierra *(con candado)* la terminal.

**Router>login** Habilita la verificación de contraseña. Identifica *como* un usuario particular.

**Router>logout** Sale de EXEC.

**Router> mrinfo** Pide información del vecino y de la versión de un ruteador multicast.

**Router>msat** Muestra las estadísticas después de que se rastrea la ruta del multicast múltiple.

**Router>name- connection** Nombra una conexión de la red existente.

**Router>pad** Abre una conexión X.29 PAD (atenuador fijo).

**Router>ping** Envía mensajes de eco para evaluar la confiabilidad de ruta a host, las demoras en la ruta, y si se puede acceder al host, o si éste está funcionando.

**Router>ppp** Arranque del protocolo Punto a Punto (PPP).

**Router>pwd** Despliega el dispositivo actual.

**Router> resume** Resume una conexión de red activa.

**Router>show** Muestra la información del sistema activo.

**Router>slip** Arranque de IP Serial-Línea *(SLIP).*

**Router>systat** Despliega información sobre líneas terminales.

**Router>telnet** Abre una conexión Telnet.

**Router> terminal** Activa los parámetros de terminal de línea.

**Router> tn3270** Abre una conexión tn3270.

**Router> traceroute** Traza la ruta al destino.

**Router>tunnel** Abre una conexión de túnel.

**Router>where** Lista las conexiones activas.

**Router>x3** Conjunto de parámetros X.3 en PAD.

**Router> xremote** Entra al modo XRemote.

## Edición de comandos de línea

**Descripción** La tabla siguiente describe las teclas rápidas que se pueden utilizar para la edición de comandos de línea:

| Tecla rápida | Función |
|---|---|
| Ctrl-A | Mueve el cursor al inicio de la línea de comando. |
| Ctrl-E | Mueve el cursor al final de la línea de comando. |
| Esc-B | Mueve el cursor una palabra hacia atrás. |
| Esc-F | Mueve el cursor un caracter hacia delante. |
| Ctrl-B | Mueve el cursor un caracter hacia atrás. |
| Ctrl-F | Mueve el cursor una palabra hacia delante. |
| Ctrl-D | Borra un solo carácter. |
| Ctrl-R | Vuelve a desplegar una línea. |
| Ctrl-U | Borra una línea. |
| Ctrl-W | Borra una palabra. |
| Ctrl-Z | Finaliza el modo de configuración y retorna al modo EXEC. |
| Tab | Completa un comando parcialmente introducido si se tienen los suficientes comandos para que no sea ambiguo. |

Esc ***no aplica en todas las terminales.***

# Anexo 4

## Números de puerto reservados para TCP y UDP

### Números de puerto

**Descripción**

Algunos puertos se reservan tanto en TCP como en UDP, aunque es posible que las aplicaciones no estén diseñadas para soportarlos. Los números de puerto tienen los siguientes intervalos asignados:

- Los números inferiores a 255 se usan para aplicaciones públicas.
- Los números del 255 al 1023 son asignados a empresas para aplicaciones comercializables
- Los números superiores a 1023 no están regulados.

**Números de puerto TCP**

| Decimal | Palabra clave | Descripción |
|---|---|---|
| 0 | | Reservado. |
| 1-4 | | No asignado. |
| 5 | RJE | Entrada remota de tareas. |
| 7 | ECHO | Echo. |
| 9 | DISCARD | Discard. |
| 11 | USERS | Usuarios activos. |
| 13 | DAYTIME | Hora. |
| 15 | NETSTAT | Quién está conectado o NETSTAT. |
| 17 | QUOTE | Cita del día. |
| 19 | CHARGEN | Generador de caracteres. |
| 20 | FTP-DATA | Protocolo de transferencia de archivos *(datos)*. |
| 21 | FTP | Protocolo de transferencia de archivos. |
| 23 | TELNET | Conexión del terminal |
| 25 | SMTP | Protocolo de transferencia de correo simple. |
| 37 | TIME | Hora |
| 39 | RLP | Protocolo de ubicación de recursos. |
| 42 | NAMESERVER | Servidor de nombres de host. |
| 43 | NICNAME | Quién es |

| Decimal | Palabra clave | Descripción |
|---|---|---|
| 53 | DOMAIN | Servidor de denominación de dominio. |
| 67 | BOOTPS | Servidor de protocolo Bootstrap. |
| 68 | BOOTPC | Cliente de protocolo Bootstrap. |
| 69 | TFTP | Protocolo de transferencia de archivos trivial. |
| 75 | | Cualquier servicio privado de conexión telefónica. |
| 77 | | Cualquier servicio RJE privado. |
| 79 | FINGER | Finger. |
| 95 | SUPDUP | Protocolo SUPDUP. |
| 101 | HOSTNAME | Servidor de nombre de host NIC. |
| 102 | ISO-TSAP | ISO-TSAP. |
| 113 | AUTH | Servicio de autenticación. |
| 117 | UUCP-PATH | Servicio de ruta UUCP. |
| 123 | NTP | Protocolo de tiempo de red. |
| 133-159 | | No asignado. |
| 160-223 | | Reservado. |
| 224-241 | | No asignado. |
| 242-255 | | No asignado. |

**Números de puertos UDP**

| Decimal | Palabra clave | Descripción |
|---|---|---|
| 0 | | Reservado. |
| 1-4 | | No asignado. |
| 5 | RJE | Entrada remota de tareas. |
| 7 | ECHO | Echo. |
| 9 | DISCARD | Discard. |
| 11 | USERS | Usuarios activos. |
| 13 | DAYTIME | Hora. |
| 15 | NETSTAT | Quién está conectado o NETSTAT. |
| 17 | QUOTE | Cita del día. |
| 19 | CHARGEN | Generador de caracteres. |

| Decimal | Palabra clave | Descripción |
|---|---|---|
| 20 | FTP-DATA | Protocolo de transferencia de archivos *(datos)*. |
| 21 | FTP | Protocolo de transferencia de archivos. |
| 23 | TELNET | Conexión del terminal |
| 25 | SMTP | Protocolo de transferencia de correo simple. |
| 37 | TIME | Hora |
| 39 | RLP | Protocolo de ubicación de recursos. |
| 42 | NAMESERVER | Servidor de nombres de host. |
| 43 | NICNAME | Quién es |
| 53 | DOMAIN | Servidor de denominación de dominio. |
| 67 | BOOTPS | Servidor de protocolo Bootstrap. |
| 68 | BOOTPC | Cliente de protocolo Bootstrap. |
| 69 | TFTP | Protocolo de transferencia de archivos trivial. |
| 75 | | Cualquier servicio privado de conexión telefónica. |
| 77 | | Cualquier servicio RJE privado. |
| 79 | FINGER | Finger. |
| 123 | NTP | Protocolo de tiempo de red. |
| 133-159 | | No asignado. |
| 160-223 | | Reservado. |
| 224-241 | | No asignado. |
| 242-255 | | No asignado. |

# Anexo 5

## Comandos utilizados en versiones anteriores a la versión 11.0 del sistema operativo IOS de CISCO

**Descripción**

Los comandos que a continuación se presentan son los comandos que se utilizan con versiones anteriores a la versión 11.0 del sistema operativo IOS de Cisco *(por ejemplo para la versión* 9.14 *ó* 9.21 *para ruteadores CISCO* 3000)

***Estos comandos han sido reemplazados por nuevos comandos, pero siguen desempeñando sus funciones normales en la versión 11.x, pero ya no se documentan. En las futuras versiones se eliminó el soporte para estos comandos.***

**Métodos de configuración**

A continuación se presenta el proceso general para la configuración de ruteadores, estableciendo las diferencias para hacerlo con versiones anteriores a 11.0 o con versiones posteriores a 11.x del sistema operativo IOS de CISCO:

| Anteriores a 11.0 | Posteriores a 11.x |
|---|---|
| **Realizar cambios en el modo de configuración** | |
| **Examinar resultados** | |
| Router# write terminal | Router# show running-config |
| **Sí son los resultados esperados…<br>Entonces Guardar cambios en la copia de respaldo** | |
| Router# write memory | Router# copy running-config startup-config |
| Router# write network | Router# copy running-config tftp |
| **Examinar archivo de copia de respaldo** | |
| Router# show configuration | Router# show startup-config |
| **No son los resultados esperados…<br>Entonces eliminar cambios** | |
| Router(config)# no ….. | Router(config)# no ….. |
| Router# configuration memory | Router# configiguration memory |
| Router# configuration network | Router# copy tftp running-config |
| Router# write erase | Router# erase startup-config |
| Router# reload | Router# reload |
| **Regresar a…<br>Realizar cambios en el modo de configuración** | |

**Conclusiones.**

A medida que las empresas se han vuelto cada vez más dependientes de las computadoras y las redes para manejar sus actividades, la disponibilidad de los sistemas informáticos se ha vuelto crucial. Actualmente, la mayoría de las empresas necesitan un nivel alto de disponibilidad y algunas requieren incluso un nivel continuo de disponibilidad, ya que les resultaría extremadamente difícil funcionar sin los recursos informáticos.

Los procedimientos manuales, si es que existen, sólo serían prácticos por un corto periodo. En caso de un desastre, la interrupción prolongada de los servicios de computación puede llevar a pérdidas financieras significativas, sobre todo si está implicada la responsabilidad de la gerencia de informática. Lo más grave es que se puede perder la credibilidad del público o los clientes y, como consecuencia, la empresa puede terminar en un fracaso total.

Imagínese una situación que interrumpa las operaciones de las computadoras durante una semana o un mes; imagine la pérdida de todos los datos de la empresa, todas las unidades de respaldo del sitio y la destrucción de equipos vitales del sistema ¿Cómo se manejaría semejante catástrofe? Si Ud. se ve en esta situación y lo único que puede hacer es preguntarse "¿Y ahora qué?" ¡ya es demasiado tarde! La única manera efectiva de afrontar un desastre es tener una solución completa y totalmente probada para recuperarse de los efectos del mismo.

Se puede considerar como un desastre la interrupción prolongada de los recursos informáticos y de comunicación de una organización, que no puede remediarse dentro de un periodo predeterminado aceptable y que necesita el uso de un sitio o equipo alterno para su recuperación.

Ejemplos obvios son los grandes incendios, las inundaciones, los terremotos, las explosiones, los actos de sabotaje, etcétera.

Cuando se diseña una red de datos se desea sacar el máximo rendimiento de sus capacidades. Para conseguir esto, la red debe estar preparada para efectuar conexiones a través de otras redes, sin importar qué características posean.

El objetivo de la Interconexión de Redes (internetworking) es dar un servicio de comunicación de datos que involucre diversas redes con diferentes tecnologías de forma transparente para el usuario. Este concepto hace que las cuestiones técnicas particulares de cada red puedan ser ignoradas al diseñar las aplicaciones que utilizarán los usuarios de los servicios.

Los dispositivos de interconexión de redes sirven para superar las limitaciones físicas de los elementos básicos de una red, extendiendo las topologías de esta.

Algunas de las ventajas que plantea la interconexión de redes de datos, son:

- Compartición de recursos dispersos.
- Coordinación de tareas de diversos grupos de trabajo.
- Reducción de costos, al utilizar recursos de otras redes.
- Aumento de la cobertura geográfica.

# Glosario

| Termino | Descripción |
|---|---|
| Ancho De Banda | Diferencia entre las frecuencias más altas y más bajas disponibles para las señales de red. También se utiliza este término para describir la capacidad de rendimiento medida de un medio o un protocolo de red específico. |
| ARP | ***Address Resolution Protocol, Protocolo de Resolución de Direcciones****.* Protocolo TCP/IP utilizado para asignar una dirección IP de alto nivel a una dirección de hardware físico de bajo nivel *(IP→MAC).* ARP se utiliza a través de una sola red física y está limitada a redes que soportan difusión de hardware. Se define en RFC 826. |
| ARPA | Agencia de Proyectos de Investigación Avanzada. Organización de investigación y desarrollo que forma parte del Departamento de la Defensa de los EE.UU. ARPA es responsable por numerosos avances tecnológicos en comunicaciones y networking. ARPA se convirtió en DARPA, pero volvió a ser ARPA (en 1994) |
| Backbone network | Red de columna vertebral de la red. Cualquier red que forme la interconexión central para una red de redes. Una columna vertebral de red nacional es una WAN; una columna vertebral de red corporativa puede ser una LAN |
| Backplane | Conexión entre una tarjeta o un procesador de interfaz y los buses de datos y los de distribución de energía en un chasis Cisco. |
| Broadcast | Paquete de datos enviado a todos los nodos de una red. Los broadcasts se identifican mediante una dirección de broadcast. |
| Broadcast de IP | Técnica de enrutamiento que permite que el tráfico de IP se propague desde un origen hasta una serie de destinos o desde varios orígenes hacia varios destinos. En lugar de enviar un paquete a cada destino, un paquete se envía aun grupo de broadcast identificado a través de una sola dirección IP de grupo de destino. |
| BSD | **Distribución Estándar de Berkeley**. Término utilizado para describir cualquiera de una serie de sistemas operativos de tipo UNIX basados en el sistema operativo BSD de la UC Berkeley. |
| Búfer | Área de almacenamiento utilizada para manejar datos en tránsito. Los búferes se usan en la internetworking para compensar las diferencias en velocidad de procesamiento entre dispositivos de red. Se pueden almacenar ráfagas de datos en los búferes hasta que los dispositivos de procesamiento más lentos las puedan manejar. A veces se denomina *búfer de paquetes.* |
| Conmutación | Encaminamiento de paquetes en un ruteador de una interfaz entrante a una interfaz saliente. |
| CRC | **Verificación por Redundancia Cíclica**. Técnica de verificación de errores en la cual el receptor de la trama calcula un residuo dividiendo el contenido de la trama por un divisor binario primo y compara el residuo calculado con el valor almacenado en la trama por el nodo emisor. |
| CSMA/CD | **Acceso Múltiple con Detección de Portadora / Detección de Colisiones**. Mecanismo de acceso a medios mediante el cual los dispositivos que están listos para transmitir datos primero verifican el canal en busca de una portadora. El dispositivo puede transmitir si no se detecta ninguna portadora durante un período de tiempo determinado. Si dos dispositivos transmiten al mismo tiempo, se produce una colisión que es detectada por todos los dispositivos que coliden. Esta colisión subsecuentemente demora las retransmisiones desde esos dispositivos durante un período de tiempo de duración aleatoria. El acceso CSMA / CD es utilizado por Ethernet e IEEE 802.3. |

| | |
|---|---|
| Datagrama | Agrupamiento lógico de información enviada como unidad de capa de red a través de un medio de transmisión sin establecer previamente un circuito virtual. Los datagramas IP son las unidades, principales de información de la Internet. Los términos ***trama, mensaje, paquete y segmento*** también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos. |
| Dirección | Localización de memoria en la RAM de una máquina determinada, identificador numérico o nombre simbólico que especifica la ubicación de una máquina o dispositivo en particular en una red, y un medio para identificar una red, subred o nodo completos dentro de una red.<br>Conjunto de bytes asignados aun dispositivo en una red que sirven para identificarlo de manera unívoca dentro de esa red. Se diferencia entre dirección física, que suele venir fijada por el fabricante de la tarjeta de red, y dirección lógica que, normalmente, la asigna el administrador de la red. |
| Dirección de broadcast | Dirección especial reservada para enviar un mensaje a todas las estaciones. Por lo general, una dirección de broadcast es una dirección MAC de destino compuesta exclusivamente por todos los números uno. |
| Dirección IP | Dirección de 32 bits asignada a los hosts que usan TCP/IP. Una dirección IP corresponde a una de cinco clases *(A, B,* C, *D* o *E)* y se escribe en forma de 4 octetos separados por puntos (formato decimal con punto). Cada dirección consta de un número de red, un número opcional de subred, y un número de host.. Los números de red y de subred se utilizan conjuntamente para el enrutamiento, mientras que el número de host se utiliza para el direccionamiento aun host individual dentro de la red o de la subred. Se utiliza una máscara de subred para extraer la información de la red y de la subred de la dirección IP. También denominada dirección de Internet. |
| Dirección MAC | Dirección de capa de enlace de datos estandarizada, necesaria para cada puerto o dispositivo que se conecta a una LAN. Otros dispositivos de la red usan estas direcciones para ubicar puertos específicos en la red y para crear y actualizar las tablas de enrutamiento y las estructuras de los datos. Las direcciones MAC tienen una longitud de 6 bytes y son controladas por el IEEE. También denominada dirección de hardware, dirección de capa MAC o dirección física. |
| DMA | **Acceso Directo a la Memoria**. La transferencia de datos desde un dispositivo periférico, como una unidad de disco duro, a la memoria sin que los datos pasen a través del microprocesador. DMA transfiere datos a la memoria a altas velocidades sin gasto de procesador. |
| DNS | **Sistema de Denominación de Dominio**. Sistema utilizado en Internet para convertir los nombres de los nodos de red en direcciones. |
| Encapsulación | Empaquetamiento de datos en un determinado encabezado de protocolo, por ejemplo, los datos Ethernet se encapsulan en un encabezado Ethernet antes de ser transmitidos por red. |
| Ethernet | La arquitectura de red más utilizada que proporciona acceso ala red mediante CSMA/CD. |
| Ethernet 802.3 | Protocolo de LAN de IEEE que especifica una implementación de la capa física y la sub capa MAC de la capa de enlace de datos. IEEE 802.3 utiliza el acceso CSMA/CD a una serie de velocidades a través de diversos medios físicos. Las extensiones del estándar IEEE 802.3 especifican implementaciones para Fast Ethernet. |
| Ethernet 802.5 | Protocolo de LAN de IEEE que especifica una implementación de la capa física y la sub capa MAC de la capa de enlace de datos. IEEE 802.5 usa acceso de transmisión de tokens a 4 ó 16 Mbps en cableado STP y es similar a Token Ring de IBM. |

| | |
|---|---|
| FDDI | **Interfaz de Datos Distribuida por Fibra.** Estándar LAN definido por 1 ANSI X3T9.5, que especifica una red de transmisión de tokens de, 100 Mbps con cableado de fibra óptica y distancias de transmisión de hasta 2 km. FDDI utiliza una arquitectura de anillo doble para proporcionar redundancia. |
| Gateway | En la comunidad IP I término antiguo que se refiere aun dispositivo de enrutamiento. Actualmente, el término *ruteador* se utiliza para describir nodos que desempeñan esta función y *gateway* se refiere a un dispositivo especial que realiza una conversión de capa de aplicación de la información de una pila de protocolo a otro. |
| Hipervínculos | Es un una palabra, frase o imagen en una página Web que, cuando se hace clic en él, lo transfiere a otra página Web. La página Web contiene (a menudo, oculta dentro de su descripción HTML) una ubicación de dirección que se denomina Localizador de Recursos Uniforme (URL). |
| Host | Sistema informático en una red. Similar al término *nodo,* salvo que *host* normalmente implica una computadora, mientras que nodo generalmente se aplica a cualquier sistema de red, incluyendo servidores de acceso y ruteadores. |
| HTTP | **Hypertext Transfer Protocol, Protocolo de Transferencia de Hipertexto**. Funciona con la World Wide Web *(WWW),* la parte de crecimiento más rápido y más utilizada de Internet. Una de las principales razones de este crecimiento sorprendente de la Web es la facilidad con la que se puede acceder a la información. Un navegador de Web, es una aplicación cliente /servidor, lo que significa que requiere tanto un componente cliente como un componente servidor para que funcione. |
| Interconexión de redes | Conexión de varias redes LAN. Esto es lo que se conoce como red de redes. |
| Interfaz | Conexión física entre el ruteador y un determinado tipo de medio: físico de conexión de red. Las interfaces también se conocen como puertos |
| Interfaz socket | Es una ***API*** *(Application Program Interfaces, Interfaz de Programación de Aplicaciones)* para una red TCP/IP, y la API es un grupo de funciones de software o rutinas que permiten a un programador desarrollar aplicaciones para usarse en una red TCP/IP. |
| Internet | Término utilizado para referirse a la internetwork más grande del mundo, que conecta decenas de miles de redes de todo el mundo y con una cultura que se concentra en la investigación y estandarización basada en el uso real. Muchas tecnologías de avanzada provienen de la comunidad de la Internet. La Internet evolucionó en parte de ARPANET. |
| Internetworking (Enlace de redes) | Término general utilizado para referirse a la industria que ha surgido en torno de la cuestión de la conexión de redes entre sí. El término se puede referir a productos, procedimientos y tecnologías. |
| Intranet | Red corporativa interna, no conectada a Internet, que sin embargo utiliza protocolos de Internet como son los protocolos que utilizan los navegadores web, para que los usuarios corporativos puedan compartir información. |
| IOS | **Internetworking Operating System, Sistema Operativo de Interconexión de Redes.** Software del sistema operativo propietario de Cisco que suministra el hardware de ruteador para encaminar paquetes en una interconexión. El IOS incorpora conjuntos de comandos y funcionalidades de software para controlar y configurar el ruteador. |
| LAN | **Red de Área Local.** Red de datos de alta velocidad y bajo nivel de error que cubre un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LAN conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un solo edificio u otra área geográficamente limitada. Los estándares de LAN especifican el cableado |

| | |
|---|---|
| | y la señalización en la capa física y la capa de enlace de datos del modelo de referencia OSI. Ethernet, FDDI y Token Ring son tecnologías de LAN ampliamente utilizadas. |
| LLC | **Control de Enlace Lógico.** La capa superior de las dos sub capas de enlace de datos definidas por el IEEE. La sub capa LLC maneja el control de errores, control del flujo, entramado y el direccionamiento de sub capa MAC. El protocolo LLC más generalizado es IEEE 802.2, que incluye variantes no orientadas a la conexión y orientadas a conexión. |
| Loop Back | ***Interfaz interna*** de las computadoras que se identifica utilizando la dirección 127.0.0.1. Siempre que se utilice esta dirección se está realizando una conexión con la propia computadora. |
| MAC | **Control de Acceso al Medio.** Capa inferior de las dos sub capas de la capa de enlace de datos, según la define el IEEE. La sub capa MAC maneja el acceso a los medios compartidos, por ejemplo, si se utilizara la transmisión o la contención de tokens. |
| MAN | Red de Área Metropolitana. Red que abarca un área metropolitana. Generalmente, una MAN abarca un área geográfica más grande que una LAN, pero cubre un área geográfica más pequeña que una WAN. |
| Multicast | **Multidifusión.** Técnica que permite que copias de un solo paquete se transfieran aun subconjunto seleccionado de todos los posibles destinos. Algunos tipos de hardware (por ejemplo, Ethernet) soportan la multidifusión y permiten que una interfaz de red pertenezca a uno o más grupos de multidifusión. El IP soporta una capacidad de multidifusión de red de redes.<br>Paquetes únicos copiados por la red y enviados aun subconjunto específico de direcciones de red. Estas direcciones se especifican en el campo de direcciones de destino. |
| Networking | Interconexión de cualquier grupo de computadoras, impresoras, ruteadores, switches y otros dispositivos con el propósito de comunicarse a través de algún medio de transmisión. |
| Nodo | Cualquier dispositivo incluido en la red, como una computadora, ruteador o servidor. |
| Paquete | Agrupación lógica de información que incluye un encabezado que contiene la información de control y (generalmente) los datos del usuario. El término "paquete" se usa con mayor frecuencia para referirse a las unidades de datos de la capa de red.<br>Se trata en términos generales, de cualquier bloque pequeño de datos enviado a través de una red de conmutación de paquetes. |
| PDU | ***Unidad de Datos del Protocolo.*** Término con el que se designa ala información que envía un protocolo de cualquier nivel a otro dispositivo. Suele constar de una cabecera y datos. |
| RARP | ***Reverse Address Resolution Protocol, Protocolo Inverso de Resolución de Direcciones.*** Protocolo TCP/IP que una máquina sin disco utiliza al arrancar para encontrar su dirección IP *(MAC→IP).* La máquina difunde una solicitud que contiene su dirección de hardware físico y un servidor responde enviando a la máquina su dirección IP. RARP toma su formato de nombre y mensaje de otro protocolo de resolución de dirección IP, ARP. |
| RDSI | **Red Digital de Servicios Integrados.** Protocolo de comunicación ofrecido por compañías telefónicas que permiten que las redes telefónicas transporten datos, voz y otros tráficos de origen. |
| RFCs | ***Request For Comments, Solicitud de Comentarios****.* Serie de documentos empleada como medio de comunicación primario para transmitir información acerca de la Internet. Algunas RFCs son designadas por el IAB como estándares de Internet. La mayoría de las |

| | |
|---|---|
| | RFCs documentan especificaciones de protocolos tales como Telnet y FTP, pero algunas son humorísticas o históricas. Las RFCs pueden encontrarse en línea en distintas fuentes. |
| Ruta | Recorrido a través de una internetwork. En general, una ruta es la trayectoria que el tráfico de red toma de su fuente a su destino. En una red de redes TCP/IP, cada datagrama IP es ruteado de manera independiente; las rutas pueden cambiar dinámicamente. |
| Segmento | Sección de una red limitada por puentes, routers o switches. |
| Servidor | **Dispositivo que suministra recursos de comunicación de datos a las máquinas cliente incluidas en la red.** |
| SNA | **Arquitectura de Redes de Sistema.** Arquitectura de red grande, compleja, con gran cantidad de funciones, desarrollada en los 70 por IBM. Similar en algunos aspectos al modelo de referencia OSI, pero con varias diferencias. SNA está compuesto esencialmente por siete capas. |
| Time-out | Tiempo fuera. Es un evento que se presenta cuando un dispositivo de red espera escuchar a otro dispositivo de red dentro de un periodo específico de tiempo, pero la respuesta no llega. El tiempo fuera que resulta, en general provoca la retransmisión de la información o la disolución de la sesión entre los dos dispositivos. |
| Token Ring | Es una LAN con protocolo de acceso de estafeta circundante desarrollada y soportada por IBM. La red Token Ring corre a 4 ó 16 Mb/s sobre una topología de anillo. |
| Trama | Agrupación lógica de información enviada como unidad de capa de enlace de datos en un medio de transmisión. Generalmente se refiere al encabezado ya la información final, utilizados para la sincronización y el control de errores, que rodean los datos de usuario contenidos en la unidad. |
| Unicast | Mensaje que se envía a un solo destino de red. |
| WAN | Red de Área Amplia. Red de comunicación de datos que sirve a usuarios dentro de un área geográfica extensa ya menudo usa dispositivos de transmisión suministrados por proveedores de servicio comunes. Frame Relay, SMDS y X.25 son ejemplos de WAN. |
| WWW | World Wide Web. Red de servidores de Internet de gran tamaño que suministra hipertexto y otros servicios para terminales que ejecutan aplicaciones cliente tales como un navegador WWW. |

**UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO**
**DIRECCIÓN GENERAL DE ORIENTACIÓN Y SERVICIOS EDUCATIVOS**
**SUBDIRECCIÓN DE SERVICIO SOCIAL Y VINCULACIÓN LABORAL**
**DEPARTAMENTO DE BOLSA UNIVERSITARIA DE TRABAJO**

La Dirección General de Orientación y Servicios Educativos (DGOSE) te invita a un reclutamiento para el programa de ***Siemens Business Learning Program*** que convoca la Empresa **SIEMENS** para estudiantes de últimos semestres y recién egresados UNAM que cumplan con el siguiente perfil:

- Estudiantes de últimos semestres (terminar la carrera en 2007)
- Recién egresados (en 2005 o 2006)
- 80% inglés comprobable:TOEIC (700 puntos) o TOEFL (520 puntos)
- Edad: 20 a 26 años
- Disponibilidad para cambiar de residencia (temporal)
- Disponibilidad de tiempo completo por año y medio (8:30 - 17:30)
- **Carreras**:

  Ingeniería Eléctrica Electrónica
  Ingeniería Mecánica
  Ingeniería Mecánica Eléctrica
  Ingeniería Mecatrónica
  Ingeniería en Computación
  Ingeniería Industrial
  Ingeniería en Telecomunicaciones

- Duración: un año seis meses

- Apoyo mensual $8,000.00

Si cubres el perfil y te interesa participar en el reclutamiento envía tu currículum en inglés y español al correo reune@servidor.unam.mx y señala en **asunto Reclutamiento SIEMENS**. Preséntate a la **plática informativa** el **martes 7 de noviembre del año en curso a las 9:00 hrs. o 17:00 hrs. en sede por confirmar.**

Es **indispensable** se cubra el requisito del **manejo del idioma inglés que se solicita**. Para mayores informes comunícate a la Bolsa Universitaria de Trabajo al 5550-8823 de 9 a 15 hrs. con Carmen Vázquez y al 5622-0420 y 21 de 9 a 15 hrs. y de 17 a 19:30 hrs.

Espero que esta convocatoria sea de tu interés.

Saludos

**Laura P. Montoya Jiménez**
**Jefa de la Bolsa Universitaria de Trabajo**
**Subdirección de Servicio Social y Vinculación Laboral**
**Dirección General de Orientación y Servicios Educativos**
**UNAM**