UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

INTERCONEXIÓN, SEGURIDAD, PREVENCIÓN Y CORRECCION DE FALLAS DE ROUTERS CISCO DE LA SERIE 1700

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO MECÁNICO ELÉCTRICO

AREA: ELÉCTRICA ELECTRÓNICA

(T E L E C O M U N I C A C I O N E S)

P R E S E N T A N:

VICTOR ALBERTO REYES JIMÉNEZ

I S R A E L P É R E Z G O N Z Á L E Z

ASESOR: ING. ENRIQUE GARCIA GUZMÁN

FES Aragón

MÉXICO **2008**

AGRADECIMIENTOS

Esta tesis esta dedicada a mis padres, a quienes agradezco de todo corazón por su amor, cariño y comprensión. En todo momento los llevo conmigo.

Agradezco a Dios por permitirme llegar hasta este momento tan importante de mi vida y lograr esta meta en mi carrera y por llenar mi vida de bendiciones.

Agradezco a mis hermanos: Mario, Efraín y Alfonso por la compañía y el apoyo que me brindan. Se que cuento con ellos siempre.

Agradezco a mi asesor de tesis, Enrique García por todo el apoyo que nos brindo y sus valiosos consejos.

Agradezco a mi amigo de la universidad Alberto Reyes por su gran amistad y por ayudarme y estar conmigo a lo largo de la carrera, y aun después.

"Todo lo puedo en Cristo que me fortalece" Fil. 4:13

Israel Pérez González.

AGRADECIMIENTOS

Son tantas personas a las cuales debo parte de este triunfo, de lograr alcanzar mi culminación académica, la cual es el anhelo de todos los que así lo deseamos.

Mis padres, por darme la estabilidad emocional, económica, cariño y comprensión; para poder llegar hasta este logro, que definitivamente no hubiese podido ser realidad sin ustedes

A todos mis amigos pasados y presentes; pasados por ayudarme a crecer y madurar como persona y presentes por estar siempre conmigo apoyándome en todo las circunstancias posibles, también son parte de esta alegría,

También agradezco a mi asesor de tesis, Enrique García por todo el soporte que nos brindo, así como a mi amigo Israel Pérez inicialmente por su amistad seguido de apoyo que me brindo a lo largo de la carrera y también después en el ámbito laboral

Victor Alberto Reyes Jiménez.

INTERCONEXIÓN, SEGURIDAD, PREVENCIÓN Y CORRECCION DE FALLAS DE ROUTERS CISCO DE LA SERIE 1700

Capitulo 1: Conexión en red

Capitulo 2. Configuración de un router Cisco

Capitulo 3. Prevención de fallas en router Cisco

Marco teórico

Los logros tecnológicos dentro de la industria de las telecomunicaciones han sido significativos, en la mayoría de los complejos industriales, universidades y en casi cualquier tipo de institución, existe la necesidad de intercambiar una amplia gama de servicios disponibles hoy en día, tales como el audio, video y sobre todo la transmisión de datos en regiones separadas geográficamente, estas necesidades obligan a inversiones cada vez mayores en equipos y sistemas que procesen la información lo más rápido posible, no importando cual sea el origen y destino de esta.

Esta tendencia a crecer rápidamente ha forzado a crear infraestructuras confiables para consolidar y permitir el adecuado intercambio de información entre los usuarios que harán uso de esa infraestructura, por lo que las empresas o lugares donde existe esta demanda de servicios, buscan diferentes ofertas en equipos que satisfagan adecuadamente las necesidades de comunicación, considerando por supuesto, que el producto se seleccione de acuerdo a los objetivos de la empresa, buscando que el rendimiento sea el adecuado, así como el costo y la posibilidad de crecimiento en el futuro.

En esta tesis se mostraran los routers Cisco, así como su sistema operativo IOS, se describe a grandes rasgos la industria de telecomunicaciones, se explica como coinciden las líneas de productos Cisco con distintos sectores de la industria de las comunicaciones.

En los elementos básicos de los routers Cisco, se explicaran los componentes de hardware del router y se detalla como los administradores de red pueden iniciar una sesión en los routers Cisco para trabajar con ellos, incluyendo el reinicio para realizar tareas tan básicas como la recuperación de contraseñas. También se trataran los principales componentes de software de los routers Cisco, tanto la interfaz de comandos del IOS, como los conjuntos de características del mismo.

Se toca el sistema operativo de Cisco IOS, la jerarquía de comandos, las utilidades y como utilizar el subsistema de ayuda. Pero la importancia radica en el control del archivo de configuración y como se utiliza para la configuración de routers en las redes, la sintaxis de los comandos, como leer los estados de los dispositivos y como configurar los parámetros clave de los routers.

Objetivos:

- Con esta tesis se dará a conocer un estudio acerca de las técnicas de conexión de redes de datos a altas velocidades, las cuales son por medio de routers.

- Se describirá el funcionamiento y procesos de arranque de los routers, para identificar los distintos modos de configuración.

- El interesado empleará el nivel de conocimientos adquiridos para seleccionar, conectar y configurar routers cisco.

- Se utilizara la estructura y la terminología del Cisco IOS (Internetworking operating system).

- Se resolverá todo problema relacionado con la seguridad del router en la red, así como la correcta ubicación del equipo. También se analizaran los comandos para la detección y solución de fallas en la red y en el router Cisco.

Justificación

Esta tesis fue elaborada para mostrar un panorama más real de las redes en el campo laboral, ya que en la actualidad, muchas de las empresas manejan equipo de marca Cisco y los egresados de esta institución no cuentan con los conocimientos necesarios para ser competentes.

El primer capitulo de este trabajo ofrece información sobre redes Lan, Wan y las conexiones entre redes. También se detiene en el modelo de referencia de interconexión de sistemas abiertos (open system interconection u OSI) y en el modo en que este se relaciona con los protocolos de red del mundo real, en este capitulo también se presentan los conceptos básicos sobre el funcionamiento de los dispositivos de conexión entre redes.

En el siguiente capitulo se presentan los componentes de hardware más comunes que se pueden encontrar en un router Cisco. También introduce la configuración básica de los routers, así como una descripción general del sistema operativo de interconexión de redes de Cisco (IOS)

Por ultimo se presentaran varios métodos para restringir el acceso no autorizado a una red mediante el router, así como algunas soluciones a los posibles problemas que se pudieran presentar en una red.

El contenido de este trabajo les será de mucha utilidad ya que parte desde los conceptos más básicos de redes hasta como solucionar problemas de conectividad con el router.

Introducción

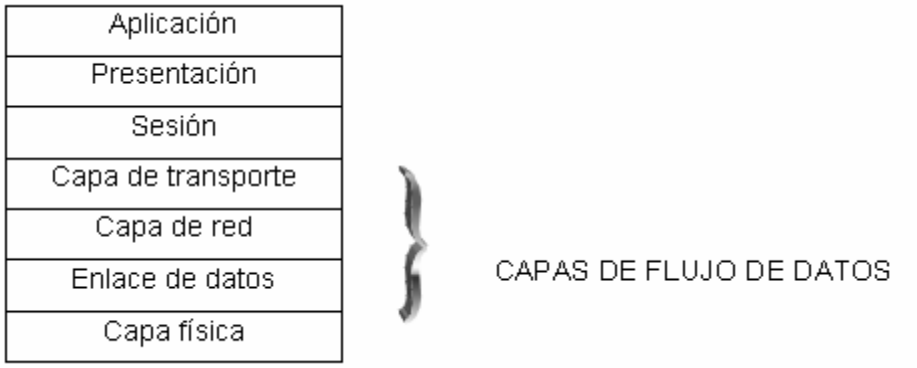
Redes

El objetivo de una red de datos consiste en facilitar la consecución de un instrumento de la productividad vinculado todas las computadoras y redes de computadoras de manera que los usuarios pueden tener acceso a la información con independencia del tiempo, ubicación y tipo de equipo informático.

El modelo OSI

Sirve de guía o marco de trabajo para crear e implementar estándares de red, dispositivos y esquemas de Internetworking

El modelo de referencia OSI consta de 7 capas, las cuatro capas del nivel inferior definen rutas para que los puestos finales puedan conectarse unos con otros y poder intercambiar datos



Las cuatro capas inferiores del modelo de referencia OSI son las responsables de definir como han de transformarse los datos a través de un cable físico a través de dispositivos de internetworking, asta el puesto de trabajo de destino, finalmente, asta la aplicación que esta en el otro lado.

Aplicación		
Presentación		
Sesión		
Transporte	Distribución fiable o no confiable corrección de errores antes de enviar	TCP UDP SPX
Red	Proporcionar direccionamiento lógico para que los routers determinen las rutas	IP IPX
Enlace de datos	Combinar bits en bytes y bytes en tramas acceso a medios con direcciones MAC detectar (no corregir) errores.	802.3/TIA-232 HDLC
Física	Trasladar bits entre dispositivos el que sigue es especificar voltaje, velocidad y patillaje del cable.	EIA/TIA-232 U.35

- *La capa física*.- Define el tipo de medio, tipo de conector y tipo de señalización. Esta especifica los requisitos eléctricos, mecánicos, pro sediméntales y funcionales para activar, mantener y desactivar el báculo físico ente sistemas finales. El HUB es un dispositivo de capa física. El HUB no manipula ni visualiza el tráfico de bus; se utiliza solo para extender el medio físico repitiendo la señal que recibe.

- *La capa de enlace de datos*.- Proporciona las comunicaciones entre puestos de trabajo en la primera capa lógica que hay por enzima de los bits del cable. El direccionamiento físico de los puestos finales se realiza el la capa de enlace de datos con el fin de facilitar en los dispositivos de red la determinación de si deben subir un mensaje a la pila del protocolo.

- *La capa de red*.- Define como debe de tener lugar el transporte de trafico entre dispositivos que no están conectados localmente en el mismo dominio de difusión.

  Las direcciones de la capa de red poseen habitualmente una estructura jerárquica en la cual se definen primero las redes y después los dispositivos ánodos de cada red.

  172.15.1.1- Dirección lógica

  La dirección de red lógica consta de 2 partes. Una parte identifica unívocamente cada red dentro del internetworking de redes mientras que la otra parte identifica unívocamente los distintos hosts existentes de cada una de estas redes combinando estas dos partes se obtiene una dirección única de red para cada dispositivo. Esta dirección única tiene dos funciones:

  - la parte de red identifica cada red dentro de la estructura del internetworking de redes. Lo que permite a los routers identificar trayectos a lo largo de la nube de redes. El router utiliza esta dirección para determinar donde ha de enviar los paquetes de red, de la misa forma que el código postal de una carta termina la provincia y ciudad a donde debe distribuirse el paquete.

  - la parte del host identifica un dispositivo en concreto o un puerto de dispositivo de la red, de la misma forma que la dirección de una carta permite identificar una ubicación dentro de una ciudad. Existen muchos protocolos de capa de red aunque todos ellos comparten la función de identificar redes y host a través de la estructura del internetworking la mayoría del estos protocolos poseen esquemas específicos para llevar a cabo esta tarea. TCP/IP es un protocolo habitual en redes enruladas.

Una dirección IP posee los siguientes componentes para identificar redes y host:

- una dirección de 32 bits dividida en cuatro secciones de 8 bits llamadas octetos. Esta dirección identifica una red y un host específicos de la red, subdividiendo los bits en partes correspondientes a la red y al host.

- una mascara de subred de 32 bits que esta dividida también en octetos de 8 bits. La mascara de subred se usa para determinar los bits que representan a la red y los que representan al host. El patrón de bits para una mascara de subred consiste en una cadena de unos seguida por los restantes bits, que son iguales a cero. La figura 1.20 muestra que la frontera entre unos y ceros marca la el limite entre las partes de la dirección que corresponden a la red y al host, que son los dos componentes necesarios para definir una dirección IP en un dispositivo final.

Como opera el router en la capa de red

Los routers operan en la capa de la capa de red registrando y grabando las diferentes redes y registrando la mejor ruta para las mismas. Los router colocan esta información en una tabla de enrutamiento, que concluye los siguientes elementos:

Dirección de red. Representa redes conocidas por el router. La dirección de red es específica del protocolo. Si un router soporta varios protocolos, tendrá una tabla por cada uno de ellos.

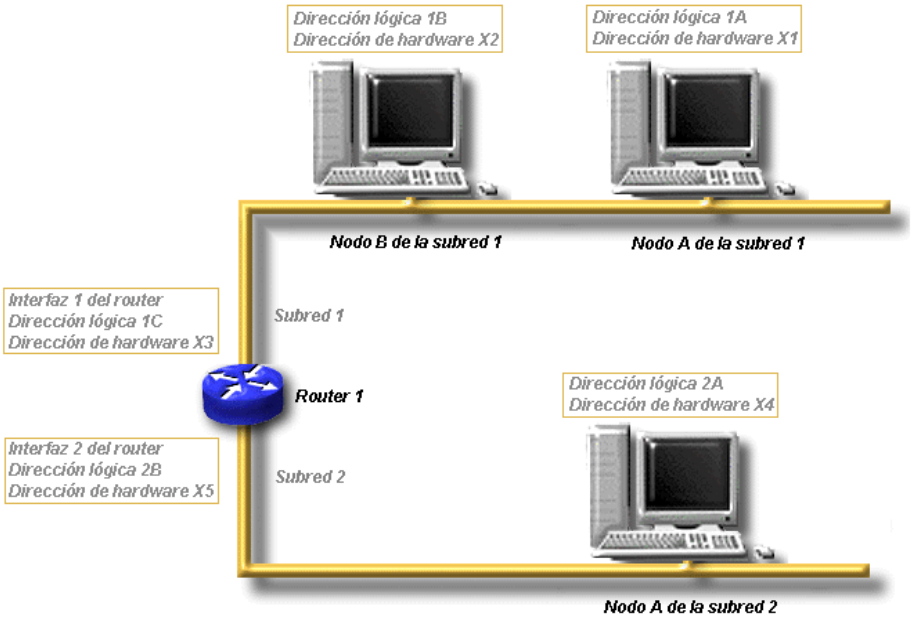
Interfaz. se refiere a la interfaz usada por el router para llegar a una red dada. Esta es la interfaz que será usada para enviar los paquetes destinados a la red que figura en la lista.

Métrica. se refiere al coste o distancia para llegar a la red de destino se trata de un valor que facilita al router la elección de la mejor ruta para alcanzar una red dada. Esta métrica cambia en función de la forma en que el router elige las rutas. entre las métricas mas habituales figuran el numero de redes que han de ser cruzadas para llegar al destino (conocido también como saltos), el tiempo en que se tarda en atravesar todas las interfaces asta una red dada (conocido también como retraso), o un valor asociado con la velocidad de un enlace (conocido también como ancho de banda).

Debido a que los routers funcionan en la capa de red del modelo OSI, se utilizan para separar segmentos en dominio de colisión y de difusión únicos. Cada segmento se conoce como una red y debe estar identificado por una dirección de red para que pueda ser alcanzado por un puesto final. Además de identificar cada segmento como una red, cada puesto de la red debe ser identificado también de forma univoca mediante direcciones lógicas.
Además de identificar redes y proporcionar conectividad, los routers deben proporcionar estas otras funciones.

Segmentación
En la siguiente figura se muestra una red que se a dividido en dos subredes distintas por medio de router. El tipo de conexión entre ambas subredes (ethernet, token ring, etc.)

Y el router en si carece de importancia en esta fase de la explicación, por lo que damos por sentado que se van a utilizar los protocolos necesarios y las conexiones de interfaz pertinentes para conectar las subredes al router



En este ejemplo, el router tiene dos interfaces de rede, la interfaz 1 y la interfaz 2, que están conectadas a la subred 1 y a la subred 2, respectivamente. El sistema de direccionamiento lógico que vamos a utilizar para asignar direcciones a los distintos nodos de la red (también se tienen que asignar direcciones lógicas a cada interfaz del router) es aplicar el numero de subred seguido de la letra que designa a dicha subred. Por tanto, al nodo A de la subred 1 se le asigna la dirección lógica 1A (primero la designación de la subred y después del nodo).

Cada nodo de la red también tendrá asignada una dirección de hardware (no olvide que las direcciones de hardware vienen ya asignadas de fábrica en las NIC: a las interfaces del router también se les asigna direcciones de hardware en el momento de su fabricación). Para mayor claridad, las direcciones de hardware asignadas a cada uno de los nodos de la red se componen de una x seguida de un número. Por ejemplo, la dirección del hardware para el nodo A de la subred 2 es X4 (tenga en cuenta que todas las direcciones de hardware son distintas y su asignación depende del fabricante)

Para hacerse una idea de cómo se dan las direcciones de estas interfaces de router y de los nodos en una red IP real, hemos incluido la relación de cada nodo e interfaz con una dirección IP de clases B:

Subred 1: 130.10.16.0
Nodo A: 130.10.16.2
Nodo B: 130.10.16.3
Interfaz 1 del router: 130.10.16.1
Subred 2:130.10.32.0
Nodo A: 130.10.32.2
Interfaz 2 del router: 130.10.32.1

Observen que la red esta dividida, y que los nodos y la interfaz del router de la subred 1 tienen asignado un tercer valor de octeto igual a 32.

Comunicación entre subredes diferentes
Vemos ahora la situación en que una computadora desea enviar Datos a otra computadora ubicada en otra subred.

El nodo A de la subred 1 desees enviar datos al nodo A de la subred 2. Esto significa que el nodo A de la subred1 desea enviar datos a la dirección lógica 2A no se encuentra en la subred local por lo que pasa a enviar los paquetes a su pasarela predeterminada, que no es mas que la interfaz del router que esta conectada a la subred 1. En este caso la dirección lógica de la pasarela del nodo A (de la subred 1) es 1C sin embargo como ocurría antes, esta dirección lógica tiene que resolverse en una dirección de hardware del la interfaz 1 del router.

Routers series 7000

Los routers cisco 7500 son routers de gama alta que normalmente sirven como router fronterizos (también llamados router de núcleo) y proporcionan el encaminamiento de paquetes entre dominios de encantamiento.

El router 7513 incorpora 11 ranuras de intercambio transparente (es decir, las tarjetas de interfaz pueden intercambiarse o insertarse incluso mientras se esta ejecutando el router). El 7513 puede proporcionar varias interfaces distintas como ethernet, fase- ethernet token ring, FDDI, T-1, sincrónica en serie de EISDN primario.

Routers series 4500

Los routers 4500 de cisco se consideran routers de nivel de distribución y se utilizan como puntos de conexión central para las redes LAN pequeñas y sitios remotos en una interconexión de redes.

El router 4500 se utiliza como un suerte de punto de distribución central para las sucursales remotas (que esta conectadas al 4500 por medio de routers de acceso) y la red LAN principal (que esta directamente conectada al router 4500 a través de un interfaz LAN)

Los routers cisco 4500 son modulares lo que significa que sus ranuras de interfaz pueden personalizarse con un determinado tipo de tarjetas de interfaz y un numero variable de puertos. Aun que esta considerado un router de capacidad media, el router cisco 4500 dispone de un amplio abanico de tarjetas de interfaz y puede soportar Ethernet, FastEthernet, token ring, FDDI, serie EISDN entre otras.

Routers series 2500

Los routers de la serie cisco 2500 resultan muy económicos y se consideran routers de nivel de acceso los routers de serie 2500 proporcionan mas puertos que los router de sucursal.

Puestos que los routers son dispositivos de la capa tres, pueden servirse del direccionamiento lógico para conducir los paquetes por las distintas redes que conecta. Los routers dividen la red corporativa en subred lógicas, que mantiene su propio tráfico local.

Conceptos básicos de encaminamiento de datos

Cuando la información tiene que pasar de una red a otra. El dispositivo de conexión entre redes que se encarga de mover los datos es el router (que se introdujo brevemente en el capitulo 4 “fundamentos básicos de la conexión entre redes”). Para encaminar datos en una interconexión de redes es preciso que se introduzcan dos eventos distintos: por un lado, que se determine la ruta apropiada para los paquetes y, por otro, que los paquetes se desplacen hasta su destino final.

Tanto la determinación de la ruta como el encaminamiento de los paquetes (o su conmutación, como también suele denominarse, ya que los paquetes son de hecho conmutados desde la interfaz entrante asta la interfaz saliente del router) se producen en la capa tres (capa de red) del modelo OSI. Otro evento importante que ocurre en la capa tres es la resolución o conversión de las direcciones lógicas (como numero IP cuando TCP/IP es el protocolo encaminado) en direcciones de hardware. Para comprender, por tanto el proceso global de encaminamiento de datos, debemos pues detenernos en cada de estos eventos.

Capitulo 1: Conexión en red

1.1. Definición de una red

Una red es un sistema de objetos o personas conectados de manera intrincada. Las redes están en todas partes, incluso en nuestros propios cuerpos. El sistema nervioso y el sistema cardiovascular son redes.

Las redes de comunicación de datos están diseñadas para hacer posible que dos computadores ubicados en cualquier lugar del mundo puedan comunicarse entre sí. También permiten que distintos tipos de computadores se puedan comunicar, ya sea que se trate de computadores Macintosh, PC o mainframe. La única condición importante es que todos los computadores y dispositivos entiendan los lenguajes o protocolos de los demás.

La mayoría de las redes de datos se clasifican como *redes de área local (LAN)* o *redes de área amplia (WAN)*. *Las LAN* generalmente se encuentran en su totalidad dentro del mismo edificio o grupo de edificios y manejan las comunicaciones entre las oficinas. *Las WAN* cubren un área geográfica más extensa y conectan ciudades y países. Las *LAN* y/o las *WAN* también se pueden conectar entre sí mediante internetworking.

1.2. Arquitecturas de red

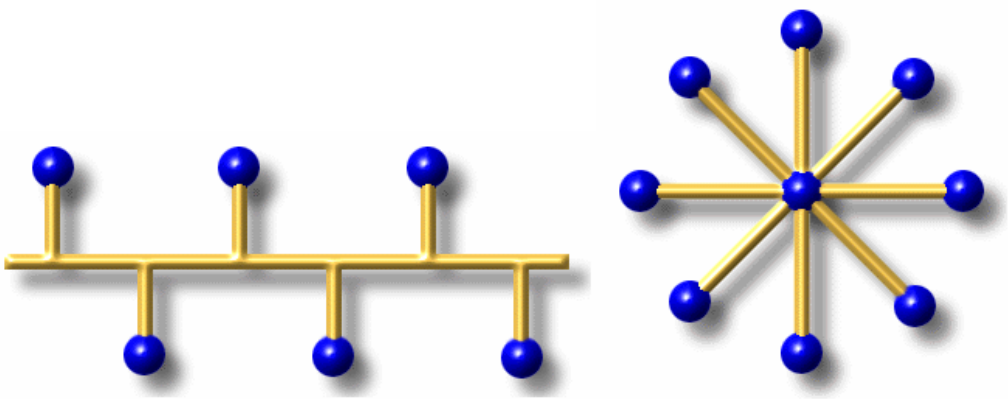
Las arquitecturas de red ofrecen distintos modos de resolver una cuestión crítica cuando se trata de construir una red: transferir los datos rápida y eficazmente por los dispositivos que componen la red. El tipo de arquitectura de red que se utilice, como Ethernet, no sólo determinará la topología de la red, si no que también definirá la forma en que los nodos de la red accederán a dichos medios. Existen

distintos tipos de arquitectura de red, todos ellos con una estrategia propia para conducir la información por la red.

1.2.1. Ethernet

Ethernet es la arquitectura de red mas utilizada hoy en día. Ethernet proporciona acceso a la red utilizando el acceso múltiple de percepción de portadora con detección de colisiones o CSMA/CD. Esta estrategia de acceso a la red consiste, básicamente, en que cada componente de la red o nodo escucha antes de transmitir los paquetes de información. De hecho, si dos nodos transmiten al mismo tiempo, se produce una colisión. Al captar una colisión, la computadora interrumpe la trasmisión y espera a que la línea quede libre. Una de las computadoras pasa entonces a transmitir los datos, logrando el control de la línea y completando la transmisión de los paquetes.

Ethernet es una arquitectura pasiva de espera y escucha. Las colisiones entre paquetes suelen ser frecuentes en la red y las computadoras tienen que disputarse el tiempo de transmisión. Las redes Ethernet suelen implantarse en topologías lógicas de bus y topologías físicas de estrella.



TOPOLOGÍA DE BUS

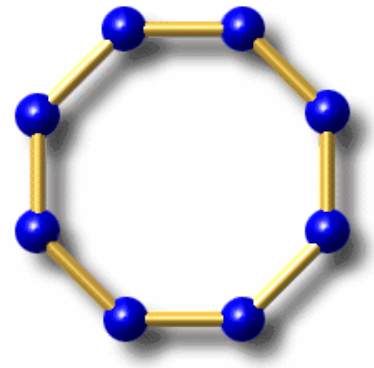
TOPOLOGÍA DE ESTRELLA

Cuando los paquetes están listos para su transmisión por el cable, su forma final pasa a denominarse trama, Ethernet emplea, de hecho, varios tipos de tramas, lo que puede ocasionar problemas en la red si no se han configurado todos los nodos para utilizar el mismo tipo de trama.

La principal ventaja de Ethernet se refiere al bajo coste que supone implementar una arquitectura de red de este tipo. Las NIC, cables y hubs de los que se sirve son bastante económicos frente al hardware que requieren otras arquitecturas como Token Ring. En cuanto a sus inconvenientes, el peor de todos tiene que ver con el número de colisiones que se producen por que cuantas mas colisiones se produzcan en una red, mas lentamente se ejecutará, pudiendo provocar incluso la caída total de la red.

1.2.2. Token ring

Token Ring de IBM es una red más segura y libre de colisiones que utiliza la pasada de señales o token como estrategia de acceso al canal de comunicación. Las redes Token Ring están conectadas en una topología en forma de estrella mediante una Unidad de Acceso Multiestación (MAU) que proporciona la conexión central para todos los nodos de la red. El anillo por el que circula la señal o token es en realidad un anillo lógico incluido dentro de la MAU.



TOPOLOGÍA DE ANILLO

El token circula por el anillo hasta que es captado por una computadora que desea enviar información por la red. La computadora que pasa el token a la siguiente computadora incluida en el anillo lógico recibe el nombre de vecino posterior activo más cercano (NAUN). Por su parte, la computadora que recibe la señal o token se conoce como vecino anterior activo más cercano (NADN).

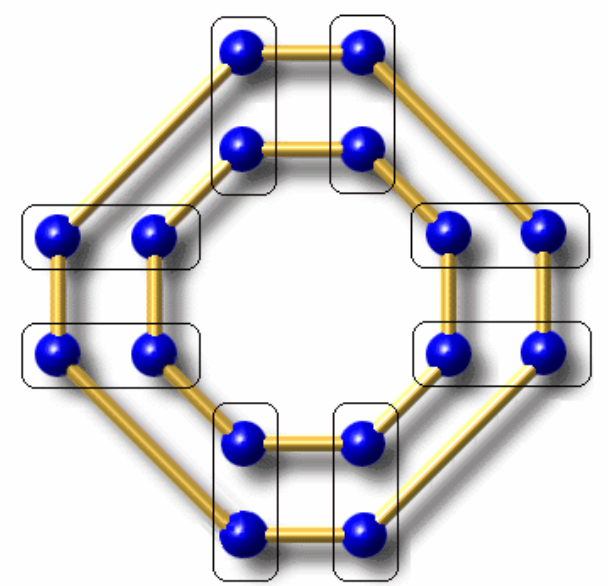
La arquitectura Token Ring se caracteriza por no provocar colisiones de datos y ofrecer el mismo nivel de acceso al canal de comunicación a todos los nodos incluidos en la red.
Token Ring también ofrece cierta tolerancia a fallos gracias a su estrategia de detección de errores denominada *beaconing*.

1.2.3. FDDI

La Interfaz de Datos Distribuidos por Fibra Óptica es una arquitectura que proporciona un entorno de alta velocidad y gran capacidad que puede utilizarse para conectar varios tipos distintos de redes. FDDI utiliza cables de fibra óptica y esta configurada en topología de anillo. FDDI se sirve de la pasada de señales o token como método de acceso al canal de comunicación y puede operar a grandes velocidades.

Puesto que FDDI utiliza una estrategia de pasada de token para acceder al canal de datos, no plantea problemas de seguridad y proporciona el mismo nivel de acceso a todos los nodos conectados a la red.

Puesto que FDDI utiliza una auténtica topología de anillo, las rotulas en el sistema de cableado pueden plantear serios problemas; para construir una tolerancia a fallos dentro de una red FDDI, se utiliza un segundo anillo. Y así, cuando una computadora puede no puede comunicarse con su vecino anterior mas próximo, pasa a enviar los datos al segundo anillo.



TOPOLOGÍA DE DOBLE ANILLO

Lógicamente, las implementaciones de FDDI requieren una tarjeta NIC especial. En lugar de utilizar hubs, se utilizan concentradores para conectar los nodos LAN a la red FDDI.

1.2.4. Apple talk

Es la arquitectura de red que utilizan las computadoras Macintosh de Apple. El hardware de red que se requiere en este caso ya esta instalado en cada Macintosh. El sistema de cableado que permite conectar computadoras Macintosh entre si se denomina LocalTalk y utiliza cables de par trenzado con un adaptador especial para macintosh.

Apple Talk es bastante parecida a Ethernet, puesto que también se trata de una arquitectura de red pasiva. Apple Talk utiliza el método CSMA/CA (siglas de acceso múltiple de percepción de portadora con evasión de colisiones) en el que las computadoras escuchan la red para determinar si el canal de comunicación

esta siendo ocupado. Una vez comprobado que el canal esta libre la computadora pasa a enviar el paquete a la red haciendo saber al resto de las computadoras, su intención de transmitir datos.

El hecho de que la computadora notifique al resto de nodo de la red su intención de transmitir datos reduce sustancialmente el número de colisiones posibles en una red CSMA/CA (en especial si se compara con Ethernet).

1.3. El modelo OSI

1.3.1. OSI, la pila de protocolos de red

Protocolo es el conjunto de normas que hacen que las comunicaciones sean más eficientes. Los siguientes son algunos ejemplos comunes:

- Cuando se maneja un automóvil, los conductores de los demás automóviles hacen (¡o deberían hacer!) una señal con la luz de giro si desean girar a la izquierda; si no lo hacen, las calles se transformarían en un caos.

- Al pilotear un avión, los pilotos deben obedecer normas sumamente específicas con respecto a la comunicación entre aeronaves y el control de tráfico aéreo.

- Al contestar el teléfono, alguien dice "Hola", luego la persona que realiza la llamada dice "Hola, habla Fulano de Tal... ", y así sucesivamente.

- En un restaurante de comida rápida con servicio a automóviles, si alguien no cumple con los protocolos habituales, generalmente recibe el pedido equivocado.

Una definición técnica del protocolo de comunicación de datos es: un conjunto de normas, o un acuerdo, que determina el formato y la transmisión de datos. La

capa n de un computador se comunica con la capa n de otro computador. Las normas y convenciones que se utilizan en esta comunicación se denominan colectivamente protocolo de la capa n.

Al principio de su desarrollo, las LAN, MAN y WAN eran en cierto modo caóticas. A comienzos de la década de los 80 se produjo una tremenda expansión en el área del desarrollo de redes. A medida que las empresas se dieron cuenta de que podrían ahorrar mucho dinero y aumentar la productividad con la tecnología de networking, comenzaron a agregar redes y a expandir las redes existentes casi simultáneamente con la aparición de nuevas tecnologías y productos de red. A mediados de la década de los 80, comenzaron a presentarse los primeros problemas emergentes de este crecimiento. Resultaba cada vez más difícil que las redes que usaban diferentes especificaciones pudieran comunicarse entre sí. La única manera de apartarse del modelo propietario de networking era que los fabricantes y proveedores se pusieran de acuerdo con respecto a un conjunto de estándares de networking.

La Organización internacional de normalización (ISO) investigó los esquemas de redes como, por ejemplo, DECNET, SNA y TCP/IP a fin de desarrollar un conjunto de normas. Como resultado de esta investigación, la ISO creó un modelo de red que ayudaría a los fabricantes a crear redes que fueran compatibles y que pudieran operar con otras redes. El modelo de referencia OSI, lanzado en 1984, fue el esquema descriptivo que crearon. Este modelo proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red que utilizaban las empresas a nivel mundial.

El modelo de referencia OSI es el modelo principal para las comunicaciones por red. Aunque existen otros modelos, en la actualidad la mayoría de los fabricantes de redes relacionan sus productos con el modelo de referencia OSI,

especialmente cuando desean enseñar a los usuarios cómo utilizar sus productos. Los fabricantes consideran que es la mejor herramienta disponible para enseñar cómo enviar y recibir datos a través de una red.

El modelo de referencia OSI permite que los usuarios vean las funciones de red que se producen en cada capa. Es un método para ejemplificar cómo viaja la información a través de una red. Explica, de forma visual, de qué modo la información, o los datos, se desplazan desde programas de aplicación (por ej., hojas de cálculo, documentos, etc.), a través de un medio de red (por ej., cables, etc.) hacia otro programa de aplicación que está ubicado en otro computador de una red, incluso si el emisor y el receptor poseen distintos tipos de redes.

En el modelo de referencia OSI, hay siete capas numeradas, cada una de las cuales ejemplifica una función de red particular. Esta división de las funciones de internetworking se denomina división en capas. Si la red se divide en estas siete capas, se obtienen las siguientes ventajas:

- Se dividen los aspectos interrelacionados del funcionamiento de la red en elementos menos complejos

- Se definen las interfaces estándar para la compatibilidad plug-and-play y la integración de componentes de varios fabricantes

- Permite que los ingenieros especialicen el diseño y promuevan la simetría en las distintas funciones modulares de internetworking de redes de modo que operen entre sí

- Impide que los cambios que se producen en un área afecten a las demás, para que cada área pueda evolucionar más rápidamente.

- Divide la complejidad de la internetworking en subconjuntos de operación separados, de aprendizaje más sencillo.

1.3.2. Las capas OSI

El problema de trasladar información entre computadores se divide en siete problemas más pequeños y de tratamiento más simple en el modelo de referencia OSI. Cada uno de los siete problemas más pequeños está representado por su propia capa en el modelo. Las siete capas del modelo de referencia OSI son:

Capa 1: La capa Física
Capa 2: La capa de Enlace de datos
Capa 3: La capa de Red
Capa 4: La capa de Transporte
Capa 5: La capa de Sesión
Capa 6: La capa de Presentación
Capa 7: La capa de Aplicación

Capa de aplicación

La capa de aplicación (séptima capa) del modelo OSI suministra servicios de red a los programas que están más cerca del usuario. Estos son programas como Internet Explorer, Netscape Communicator, Eudora Pro y otro software de aplicación para usuarios finales. Esta capa establece la comunicación con los socios correspondientes, sincroniza el acuerdo con respecto a los procedimientos para la recuperación de errores y el control de integridad de datos.
Los servicios, que suministran acceso a la red, incluyen:

- Telnet y Protocolo de Transferencia de Archivos (FTP)
- Protocolo de transferencia de archivos trivial (TFTP)
- Sistema de archivos de red (NFS)

- Protocolo de administración de red simple (SNMP)
- Protocolo de transferencia de correo simple (SMTP)
- Protocolo de transferencia de hipertexto (HTTP)

Los dispositivos que funcionan hasta esta capa incluyen hosts y gateways.

Capa de presentación

La capa de presentación garantiza que la información enviada por la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro sistema. De ser necesario, la capa de presentación realiza una traducción entre múltiples formatos de datos utilizando un formato común.

La capa de presentación también proporciona cifrado de datos para asegurar la protección a medida que los datos recorren la red. Cuando se reciben los datos cifrados, esta capa los descifra y formatea el mensaje antes de pasarlo a la capa de aplicación.

Los formatos de datos incluyen ASCII, EBCDIC, cifrado, jpeg, gif, mpeg, quicktime, flash, wav, avi y mp3.

Los dispositivos que funcionan hasta esta capa incluyen hosts y gateways.

Capa de sesión

La capa de sesión establece, administra, termina las sesiones entre dos hosts que se comunican y suministra sus servicios a la capa de presentación. También sincroniza el diálogo entre los dos hosts y administra el intercambio de datos entre ellos. La capa de sesión también toma medidas para la transferencia de datos

eficiente, clase de servicio, autorización de seguridad e informe de excepción de problemas de la capa de sesión, presentación y aplicación.

Los tres tipos de diálogos que se utilizan en la capa de sesión son unidireccional, half-duplex y full-duplex. Un diálogo unidireccional permite que la información fluya desde un dispositivo a otro sin requerir una transmisión de respuesta.

Half-duplex, que también se denomina transmisión alternada en dos vías (TWA), permite que los datos fluyan en dos direcciones desde un dispositivo a otro. Sin embargo, los dispositivos no pueden enviar una transmisión hasta que la señal anterior se haya recibido por completo. Cuando un dispositivo envía una transmisión y requiere que el dispositivo destino envíe una respuesta, el dispositivo destino debe esperar hasta que la transmisión inicial se complete antes de poder enviar la respuesta.

Full-duplex, que también se denomina transmisión simultánea en dos vías (TWS), permite que los dispositivos envíen datos a otro dispositivo sin tener que esperar hasta que el hilo esté libre. Cuando un dispositivo transmite una señal, el dispositivo destino no tiene que esperar hasta que la señal se complete para enviar una respuesta al dispositivo origen. El full-duplex permite que el tráfico de dos vías se produzca de forma simultánea durante una sesión de comunicación. El teléfono es un ejemplo de full-duplex.

Los protocolos incluyen el Sistema de Archivos de Red (NFS), Lenguaje de Consulta Estructurado (SQL), Llamada de Procedimiento Remoto (RPC), Sistema X-Window, Protocolo de Sesión Apple Talk (ASP) y Protocolo de Control de Sesión de Arquitectura de Red Digital (DNA SCP).

Los dispositivos que funcionan hasta esta capa incluyen hosts y gateways.

Capa de transporte

La capa de transporte divide los datos del sistema del host emisor en segmentos y reensambla los datos en una corriente de datos en el sistema del host receptor.

La capa de transporte busca suministrar un servicio de transporte de datos que aísle a las capas superiores de los detalles de la implementación de transporte. Específicamente, la tarea principal de la capa de transporte incluye temas tales como la obtención de un transporte confiable entre dos hosts. Al brindar un servicio de comunicación, la capa de transporte establece, mantiene y termina los circuitos virtuales de forma adecuada. Para brindar un servicio confiable, se utilizan la detección y recuperación de errores de transporte y los controles del flujo de información.

Cuando la capa de transporte recibe datos desde las capas superiores, divide la información en segmentos (pedazos más pequeños) para enviarlos a través de las capas inferiores del Modelo OSI y luego hacia el dispositivo destino.

Los protocolos que se utilizan en esta capa son:

- Intercambio Secuencial de Paquetes (SPX)
- Protocolo para el Control de la Transmisión (TCP)
- Protocolo de Datagrama de Usuario (UDP)
- Interfaz de usuario NetBIOS extendida (NetBEUI)

Los servicios que se utilizan en esta capa usan TCP para suministrar comunicación orientada a conexión con envío sin errores y UDP para suministrar comunicaciones no orientadas a conexión sin envío garantizado de paquetes (envío no confiable).

Los dispositivos que funcionan hasta esta capa incluyen hosts, switch multicapa y gateways.

Capa de red

La capa de red es una capa compleja que suministra conectividad y selección de ruta entre dos sistemas host que pueden estar geográficamente separados. Se puede considerar a la capa 3 como la capa de direccionamiento, selección de ruta, enrutamiento y conmutación.

Los protocolos que funcionan en esta capa incluyen:

Protocolos enrutados

- IPX
- IP

Protocolos de la capa 3

- Protocolo de Mensajes de Control en Internet (ICMP)
- Protocolo de Resolución de Direcciones (ARP)
- Protocolos de enrutamiento del Protocolo de Resolución Inversa de Direcciones (RARP)
- Protocolo de Información de Enrutamiento (RIP)
- Protocolo de Enrutamiento de Gateway Interior (IGRP)
- IGRP Mejorado (EIGRP)
- Primero la ruta libre más corta (OSPF)
- Protocolo de Gateway Exterior (EGP)
- Protocolo de Grupo de Administración de Internet (IGMP)

Los servicios incluyen direccionamiento de software y hardware, enrutamiento de paquetes entre hosts y redes, resolución de direcciones de hardware y software e informes de envío de paquetes.

Los dispositivos que funcionan hasta esta capa incluyen routers, switch multicapa y brouters.

Capa de enlace de datos

La capa de enlace de datos proporciona tránsito de datos confiable a través de un enlace físico. Al hacer esto, la capa de enlace de datos se ocupa del direccionamiento físico (en oposición al lógico), la topología de red, el acceso a la red, la notificación de errores, el envío ordenado de tramas y el control de flujo. Se puede decir que la capa 2 se refiere a las tramas y el control de acceso al medio.

CSMA/CD de Ethernet también funciona en esta capa para determinar cuáles son los dispositivos que deben transmitir en un momento dado para evitar las colisiones.

La NIC también es responsable por CSMA/CD en Ethernet. Si dos o más dispositivos intentan transmitir señales al mismo tiempo, se produce una colisión. CSMA/CD le indica al dispositivo que debe esperar una cantidad de tiempo determinada antes de transmitir otra señal para evitar otra colisión.

Los estándares 802 establecen que la capa de enlace de datos se divide en dos subcapas: Control de enlace lógico (LLC) y Control de acceso al medio (MAC). La subcapa LLC (IEEE 802.2) establece y mantiene la comunicación con otros dispositivos y proporciona conectividad con los servidores mientras se transfieren los datos. LLC administra el control de enlace y define los puntos de acceso al servicio (SAP).

La subcapa MAC mantiene una tabla de direcciones físicas de los dispositivos. Si un dispositivo debe participar en la red, se le asigna una dirección MAC exclusiva.

Se puede comparar la dirección MAC a la dirección del domicilio físico de una persona, que la oficina de correos utiliza para enviar la correspondencia.
Los protocolos que se utilizan en esta capa incluyen Control de Enlace de Datos de Alto Nivel (HDLC) para las conexiones WAN, incluyendo las transmisiones síncronas y asíncronas. El protocolo LLC (IEEE 802.2) suministra control de flujo en esta capa.

Las tecnologías que operan en esta capa incluyen más de 18 variedades de Ethernet (especificadas en el estándar IEEE 802.3 y otros estándares), Token Ring (IEEE 802.5) y otras tecnologías LAN basadas en tramas. También se suministran comunicaciones con la NIC.

Los dispositivos que funcionan hasta esta capa incluyen las NIC, puentes y switches. Mientras que los routers y los brouters se clasifican como dispositivos de la capa 3, para poder ejecutar sus funciones también deben operar en las capas 1 y 2.

Capa física

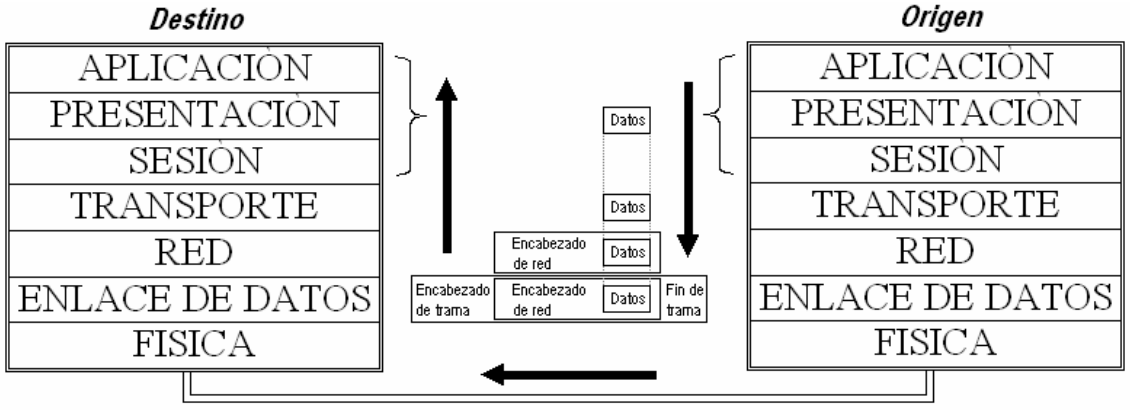
La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre los sistemas finales. Las características tales como niveles de voltaje, sincronización de los cambios de voltaje, velocidades de los datos físicos, distancias máximas de transmisión, conectores físicos y otros atributos similares son definidos por las especificaciones de la capa física.

La capa física está a cargo del desplazamiento de los bits de datos a través de los medios físicos. Los datos, bajo la forma de unos y ceros, se transforman en señales eléctricas, pulsos luminosos o señales inalámbricas. Estas señales se transportan por cables de cobre, fibra óptica o se emiten por medios inalámbricos,

mediante una NIC. Al recibir datos desde la red, la NIC transforma las señales eléctricas, los pulsos luminosos o las señales inalámbricas nuevamente en unos y ceros, que entonces pasan por las diversas capas del modelo OSI en sentido ascendente:

Los protocolos son los estándares de cableado, señalización y conexión. Los servicios incluyen Ethernet, Token Ring, FDDI y otras tecnologías LAN. Los dispositivos que funcionan en esta capa son los repetidores, repetidores multipuerto (también denominados hubs), unidades de acceso al medio (MAU) y transceivers (transmisores/receptores, para convertir un tipo de señal en otro).

En resumen en modelo OSI es un modelo de referencia que permite que los computadores comuniquen datos. Todas las comunicaciones de una red parten de un origen y se envían a un destino, y la información que se envía a través de una red se denomina datos o paquete de datos. Si un computador (host A) desea enviar datos a otro (host B), en primer término los datos deben empaquetarse a través de un proceso denominado encapsulamiento. Luego, a medida que los datos se desplazan a través de las capas del modelo OSI, reciben encabezados, pies y otra información, una vez que los datos han llegado a su destino comienza el proceso inverso hasta que finalmente se llega a la capa de aplicación



1.4. Protocolo TCP/IP

El Departamento de Defensa de EE.UU creó el modelo *TCP/IP* porque necesitaba una red que pudiera sobrevivir ante cualquier circunstancia, incluso una guerra nuclear.

Aunque el modelo OSI es universalmente reconocido, el estándar abierto histórico y técnico de la Internet es el modelo de referencia TCP/IP y el stack de protocolo TCP/IP. TCP/IP permite la comunicación de datos entre dos computadores, en cualquier lugar del mundo (o en el espacio exterior), prácticamente a la velocidad de la luz

El modelo TCP/IP tiene cuatro capas: la capa de aplicación, la capa de transporte, la capa de Internet y la capa de red.
Capa de aplicación

Los diseñadores del TCP/IP pensaban que los protocolos de nivel más alto debían incluir detalles de la capa de sesión y de presentación, de modo que simplemente crearon una capa de aplicación que administra los protocolos de nivel más alto, los aspectos de representación, codificación y control de diálogo. El modelo TCP/IP combina todos los problemas relacionados con la aplicación en una capa y da por sentado que estos datos están correctamente empaquetados para la siguiente capa.

Capa de transporte

La capa de transporte se refiere a los aspectos de calidad del servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores. Uno de sus protocolos, el protocolo para el control de la transmisión (TCP), ofrece maneras flexibles y de alta calidad para crear comunicaciones de red confiables, sin problemas de flujo y con un nivel de error bajo. TCP es un protocolo orientado a la conexión. Mantiene un diálogo entre el origen y el destino mientras

empaqueta la información de la capa de aplicación en unidades denominadas segmentos. Orientado a la conexión no significa que existe un circuito entre los computadores que están en comunicación (eso podría ser una conmutación o conmutación entre circuitos), sino que los segmentos de la Capa 4 van y vuelven durante un período determinado.

Capa de Internet

El propósito de la capa de Internet es enviar paquetes de origen desde cualquier red en la internetworking de redes y que estos paquetes lleguen a su destino independientemente de la ruta y de las redes que se utilizaron para llegar hasta allí. El protocolo específico que rige esta capa se denomina Protocolo Internet (IP). En esta capa se produce la determinación de la mejor ruta y la conmutación de paquetes.

Capa de red

El nombre de esta capa es muy amplio y se presta a confusión. También se denomina capa de host a red. Es la capa que se ocupa de todas las cuestiones que requiere un paquete IP para realizar realmente un enlace físico y luego realizar otro enlace físico. Esta capa incluye los detalles de tecnología de LAN y WAN y todos los detalles de la capa física y de enlace de datos del modelo OSI

1.4.1. Generalidades de la capa Internet de TCP/IP

En el modelo TCP/IP existe solamente un protocolo de red: el protocolo Internet, o IP, independientemente de la aplicación que solicita servicios de red o del protocolo de transporte que se utiliza. Esta es una decisión de diseño deliberada. IP sirve como un protocolo universal que permite que cualquier computador informático, se comunique en cualquier momento desde cualquier lugar del mundo.

1.4.1.1. Protocolo de resolución de direcciones

Otro protocolo IP es el protocolo de resolución de direcciones (ARP), ARP se usa para resolver o asignar una dirección IP de destino conocido a una dirección a una dirección de la subcapa MAC para permitir la comunicación en medios de multiacceso, como Ethernet. Para determinar la dirección de destino de un datagrama, se comprueba la tabla caché ARP del puesto emisor. Si la dirección no se encuentra en la tabla, se envía un ARP, que es un paquete de difusión, en un intento de localizar el puesto de destino. Cada puesto del segmento recibe la difusión y el puesto que posee la dirección IP responde al ARP

1.4.1.2. Protocolo de resolución de direcciones inversas

El protocolo de resolución direcciones inversas (RARP) es otro de los protocolos definidos en la capa IP. RARP se usa por los puertos individuales que no conocen sus propias direcciones IP. RARP permite que un puesto envíe una petición relativa a su propia dirección IP enviando su propia dirección MAC de capa 2 a un servidor RARP la petición RARP es un paquete de difusión. RARP se basa en la presencia de un servidor RARP con una entrada de tabla y otro medio en el cual cada subred pueda responder a sus peticiones.

1.4.2. Generalidades de direcciones TCP/IP

En un entorno TCP/IP, los puestos finales se comunican directamente con los servidores y otros puestos. Esta comunicación puede tener lugar debido a que cada nodo que utiliza el protocolo TCP/IP posee una dirección IP lógica de 32 bits única.

Cada datagrama IP incluye una dirección IP de origen y una dirección IP de destino que identifica las redes y el host de origen y destino.

Cada organización que conforma el internetworking de redes se ve como una red individual que debe ser alcanzable para que un host individual de esa organización pueda conectarse. Cada red de empresa posee una dirección de red única. Los hosts que pueblan la red comparten los mismos bits, y se diferencian en los bits restantes.

La dirección IP tiene 32 bits de longitud y consta de dos partes: el número de red y el número de host. La dirección IP es binaria en su origen. Básicamente, los 32 bits se descomponen en cuatro apartados de 8 bits cada uno, conocidos como octetos. Cada uno de estos octetos se convierte al formato decimal y se separan unos de otros mediante puntos.

Ejemplo decimal	172	16	122	204
Ejemplo binario	10101100	00010000	01111010	11001100

La asignación de direcciones está controlada por un organismo central, la American Registry Internetwork Numbers (ARIN).

1.4.2.1. Clases de direcciones IP

Las direcciones IP se dividen en tres clases distintas atendiendo al tamaño de la red que las utiliza. Existen interconexiones de redes IP de clase A, de clase B y de clase C.

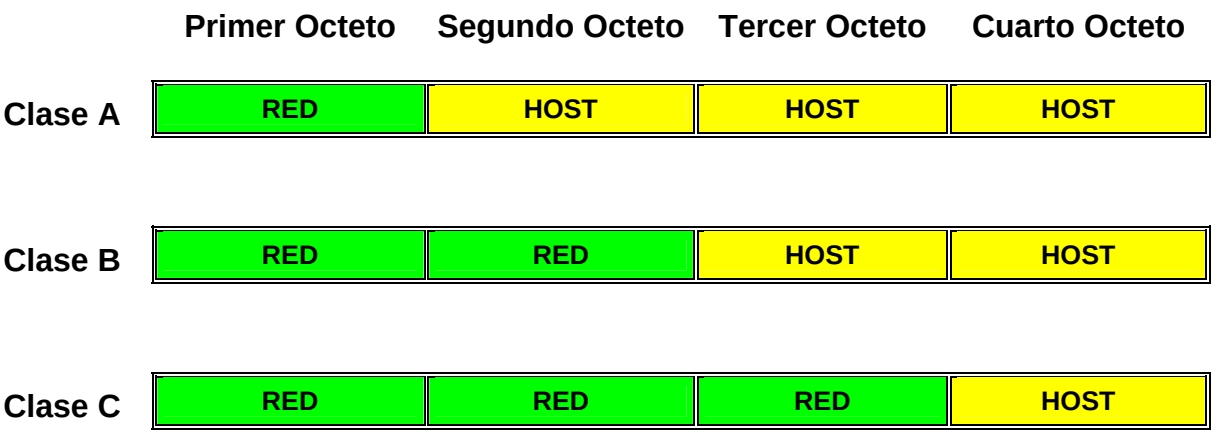
La clase A se utiliza para las redes muy grandes y proporciona hasta 16 millones de direcciones distintas de nodo para la red. Dada la estructuración de las direcciones IP, una red de clase A puede servir a un gran numero de computadoras host (nodos), pero solo pueden existir 127 redes de clase A.

La clase B se utiliza en las redes que también precisan de un gran número de direcciones de nodos, como grandes compañías o instituciones. Existen 16 384 direcciones de red de clase B, y cada clase B puede suministrar hasta 65 000 direcciones de host.

La clase C se utiliza para las pequeñas redes y existen más de 2 millones de dirección de red de clase C. Sin embargo, las redes de clase C sólo proporcionan 254 direcciones de nodo.

Cada una de estas clases utiliza un determinado Número de octetos en una dirección IP para designar la parte de la red incluida la dirección y la parte del nodo. Por ejemplo una dirección IP de clase A como 10.5.25.8 designa la red IP que utiliza el primer octeto. Esto significa que el número de red es 10. El resto de la dirección, 5.25.8, se refiere a la dirección de host.

En la siguiente tabla se muestran cada una de las clases IP de red y los octetos que utilizan para las direcciones de red y las direcciones de host, cuanto mayor es el número de octetos utilizados para las direcciones de host, mayor es el número de hosts que pueden existir. Y al revés: cuanto mayor es el número de octetos utilizados para las direcciones de red, mayor es el número de redes posibles.



Cada una de las clases IP utiliza un determinado número de octetos para las direcciones de red y un determinado número de octetos para las direcciones de nodo.

Clase	Rango del Primer octeto	Número de redes	Número de host	Dirección de muestra
A	1-126	126	16 777 214	10.15.121.5
B	128-191	16 384	65 534	130.13.44.52
C	192-223	2 097 152	254	200.15.23.8

Las direcciones de clase D y de clase E

Existen dos clases adicionales de direcciones IP de red: la clase D y la clase E. Las direcciones de red de clase D las utilizan los grupos de difusión múltiple que reciben datos en una interconexión desde una determinada aplicación o servicio de servidor. Un ejemplo de difusión múltiple de las direcciones de clase D es Microsoft NetShow, que puede difundir el mismo contenido a un grupo de usuarios de una sola vez. Las direcciones de clase E pertenecen a una clase experimental, y no pueden ser utilizadas por usuarios comunes.

1.4.2.2. Segmentación de subredes

La división en subredes permite tomar un número de redes LAN y conectarlas entre sí para formar una interconexión de redes. También permite fragmentar una gran red en subredes mas pequeñas conectadas entre sí por medio de routers. La segmentación de redes grandes utilizando routers permite maximizar el ancho de banda de la red ya que los routers mantienen el tráfico de cada subred en el entorno local, por lo que los datos no se difunden por toda la red. Cada una de las clases de red (A, B y C) pueden dividirse en subredes.

Vamos a tomar una red de clase A a modo de ejemplo para ir explicando cada uno de los pasos que nos permitan dividirla en distintas subredes.

El primer octeto de una red de clase A se sitúa en el rango decimal 1-126 supongamos por tanto, que le han asignado la dirección de red 10.0.0.0.

En las redes de clase A, el primer octeto define la dirección de red. Los tres octetos restantes se refieren a la información de la dirección de nodo ya que se tienen todas las posibles combinaciones en tres octetos. Estos suman un total de 24 posiciones de bit, por lo que el número de direcciones de nodo disponibles será igual a 16 777 214.

El paso siguiente se refiere a la determinación del número de subredes que se requieren. Con el ejemplo de la red de clase A, la operación abarcaría una amplia área geográfica y tendríamos que utilizar tanto la tecnología LAN como WAN para simplificar un poco las cosas, supongamos que queremos dividir una red de gran tamaño en treinta subredes (para lo cual necesitamos una interfaz de router separada para que sirva a cada subred; por tanto, y aunque solo se trate de treinta subredes, necesitaremos varios routers que cuenten con un determinado número de interfaces (como Ethernet) para conectar las distintas subredes).

Ahora que ya hemos determinado el número de subredes que necesitamos. Podemos empezar a trabajar en el proceso de “robar” bits para crear las subredes. Lo primero que debe crearse es la nueva máscara de subred que estará instalada en la red.

Crear la mascara de subred de la red.

Queremos crear 30 subredes. Por el momento nuestra dirección 10.0.0.0 solo proporciona bits para la dirección de red (el primer octeto) y bits para las direcciones de nodos (los otros tres octetos) ¿como crear entonces las subredes? Para ello, deben “robarse” algunos bits de los octetos de nodo y utilizarlos para crear las subredes (no se pueden quitar bits al octeto de red ya que este lo facilitan las personas que asignan redes IP y son, por tanto, intocables).

Pasamos pues a quitar bits del primer octeto de nodo para crear nuestras subredes (es decir el segundo octeto en la dirección 10.0.0.0, de izquierda a

derecha). Esto significa que el número de direcciones de nodo posibles va a disminuir, ya que vamos a tomar unos bits para crear las subredes (si se quitan bits para crear subredes, obviamente dispondremos de menos direcciones de nodo). Estos bits robados no solo nos van a permitir calcular rangos de direcciones IP para cada subred (cada una de las treinta subredes tendrá un rango distinto de dirección IP), si no también crear una nueva mascara de subred para toda la red. Esta nueva mascara de subred permitirá a los router y a los restantes dispositivos incluidos en la red saber que se ha dividida la red en subredes, además de indicarles el número de subredes lógicas que se han creado.

Pero antes de nada debemos calcular el número de bits que tenemos que sustraer para crear las treinta subredes. Sabemos que cada bit incluido es un octeto tiene un valor decimal asignado. Por ejemplo, el primer bit de orden inferior en el extremo derecho del octeto tiene determinado un valor decimal igual a 1; el bit situado a su izquierda tiene un valor de 2 y así sucesivamente. Por tanto, para crear 30 subredes, tenemos que sumar los valores decimales de los bits d orden inferior hasta alcanzar un valor total de 31. ¿Por qué 31 y no 30?

Por que no podemos utilizar la subred 0 que es lo que obtendríamos si robáramos únicamente el primer bit de orden inferior. La formula que deberíamos utilizar seria la siguiente: valor decimal total de bits de orden inferior robados menos 1. Tomemos los 5 primeros bits de orden superior (128, 64, 32, 16 y 8), es decir, tomados de izquierda a derecha. Y pasamos a sumarlos: 128+64+32+16+8=248. El resultado 248 es fundamental. Por lo general, una máscara de subred de clase A es igual a 255.0.0.0 pero esta red de clase A ha sido dividida en subredes (utilizando los bits del segundo octeto), por lo que la nueva máscara de subred pasa a ser 255.248.0.0. Esta nueva máscara de subred indica a los routers y demás dispositivos que la red de clase A contiene 30 subredes. (Esta máscara la utilizarán las interfaces de router y computadoras incluidas en la red al margen de la subred específica en la que se encuentren).

Calcular los rangos IP de subred

Antes utilizamos cinco bits de orden superior para determinar el número binario usado en el segundo octeto de nuestra nueva mascara de subred.

Estos bits de orden superior también proporcionan la clave para determinar los rangos de dirección IP para cada subred. Como recordara, los valores de orden decimales de orden superior que utilizamos para la máscara de subred eran 128, 64, 32, 16 y 8.

Tomemos el bit mas bajo de orden superior que utilizamos en el calculo de la nueva máscara de subred, es decir, 8. Este número será el que utilicemos como incremento para crear los rangos de dirección IP para las treinta subredes.

Por ejemplo la primera subred (de las treinta que queremos crear) empezara con la dirección IP 10.8.0.1. el 8 se utiliza como el incremento inicial para el segundo octeto en la dirección IP. No olvidemos que hemos tomado los bits del segundo octeto para crear las subredes. Por tanto, todas las direcciones IP que tengan un valor decimal de segundo octeto inferior a 8 son valores no validos. Para calcular el primer número de nuestra segunda subred, tenemos que sumar 8 al segundo octeto, obteniendo así 16 por tanto, la dirección inicial para la segunda subred será 10.16.0.1. Para determinar la dirección inicial para las restantes 28 subredes solo debe sumarse 8 al segundo octeto. Seguramente ahora se estará preguntando como hemos llegado al 0 en el tercer octeto y al 1 en el cuarto. Los valores decimales posibles en un octeto cualquiera van de 0 (donde todos los bits están determinados a 0) a 255 (donde todos los bits están determinados a 1) por tanto, la primera dirección IP en la subred puede tener todos los 0 en el tercer octeto. Pero, ¿por qué empieza el cuarto octeto con 1? Para entenderlo, debe recordar en cuanto a que la dirección de un nodo no puede ser representada por octetos que contengan todos 0 o todos 1. Si el cuarto octeto fuera 0, los dos octetos de nodo (el tercero y cuarto) tendrían que ser todos 0, algo que solo se

utiliza para designar la dirección de subred y que, por tanto, resultaría una dirección no valida para un nodo.

Para determinar el rango de direcciones para una determinada subred, debe tomarse la dirección inicial de dicha subred y utilizar todas las direcciones incluidas entre ella y la dirección inicial de la siguiente subred. Por ejemplo, nuestra primera subred contiene todas las direcciones incluidas entre 10.8.0.1 y 10.16.0.1 (esta ultima no incluida).

1.5. Dispositivos de conexión entre redes

La función básica de los computadores de una LAN es suministrar al usuario un conjunto de aplicaciones prácticamente ilimitado. El software moderno, la microelectrónica, y relativamente poco dinero le permiten ejecutar programas de procesamiento de texto, de presentaciones, hojas de cálculo y bases de datos. También le permiten ejecutar un navegador de Web, que le proporciona acceso casi instantáneo a la información a través de la World Wide Web. Puede enviar correo electrónico, editar gráficos, guardar información en bases de datos, jugar y comunicarse con otros computadores ubicados en cualquier lugar del mundo.

La clave de todo esto es la capacidad de una parte relativamente estandarizada y económica del hardware (el computador) para hacer una amplia variedad de cosas. Los dispositivos periféricos le permiten hacer mucho más

Las funciones básicas de los medios consisten en transportar un flujo de información, en forma de bits y bytes, a través de una LAN. Salvo en el caso de las LAN inalámbricas (que usan la atmósfera, o el espacio, como el medio) y las nuevas PAN (redes de área personal, que usan el cuerpo humano como medio de networking), por lo general, los medios de networking limitan las señales de red a

un cable o fibra. Los medios de networking se consideran componentes de Capa 1 de las LAN.

Se pueden desarrollar redes informáticas con muchos medios distintos. El cable coaxial, la fibra óptica o incluso el espacio libre pueden transportar señales de red, sin embargo, el medio principal del que se hablará en este trabajo se denomina cable de par trenzado no blindado de categoría 5 (UTP CAT 5)

1.5.1. Hub

Los hubs se consideran dispositivos de la Capa 1 ya que sólo verifican los bits y no buscan ninguna otra información de ninguna de las otras capas del modelo OSI El propósito de un hub, también denominado repetidor multipuerto, es amplificar y retemporizar las señales de red, a nivel de los bits, para una cantidad grande de usuarios (por ejemplo 4, 8 o incluso 24) utilizando un proceso que se denomina concentración. Si tiene varios dispositivos (por ejemplo hosts) que se deben conectar a un dispositivo compartido (por ej., un servidor), y el servidor razonablemente sólo necesita tener una NIC, entonces puede utilizar un hub.

La función del hub en una red token ring se ejecuta a través de la Unidad de conexión al medio (MAU). Físicamente, es similar a un hub, pero la tecnología token ring es muy distinta. En las FDDI, la MAU se denomina concentrador. Las MAU también son dispositivos de la Capa 1.

1.5.2. Bridge

El puente es un dispositivo de la Capa 2; utiliza un procesamiento de Capa 2 para tomar decisiones acerca de si debe o no debe enviar información.

Un puente conecta los segmentos de red y debe tomar decisiones inteligentes con respecto a si debe transferir señales al siguiente segmento. Un puente puede mejorar el desempeño de una red al eliminar el tráfico innecesario y reducir al mínimo las probabilidades de que se produzcan colisiones. El puente divide el tráfico en segmentos y filtra el tráfico basándose en la estación o en la dirección MAC.

Los puentes no son dispositivos complejos, analizan las tramas entrantes, toman decisiones de envío basándose en la información que contienen las tramas y envían las tramas a su destino

1.5.3. Switch

Los switches a primera vista, a menudo son similares a los hubs, ya que una de sus funciones es la conectividad (permitir que varios dispositivos se conecten a un punto de la red). La parte delantera de un switch tiene interfaces (puertos); la parte trasera posee un botón de encendido/apagado, una conexión de alimentación y un puerto de consola para administrar el switch.

El propósito de un switch es concentrar la conectividad, garantizando el ancho de banda. Un switch es un elemento que es capaz de combinar la conectividad de un hub con la regulación de tráfico de un puente en cada puerto. Realiza una conmutación de paquetes desde los puertos entrantes (interfaces) hacia los puertos salientes, suministrando a cada puerto un ancho de banda total.

El switch usa la dirección MAC para tomar sus decisiones de conmutación. Se puede pensar en cada puerto de un switch como si fuera un micropuente, lo que lo convierte en un dispositivo de Capa 2.

1.5.4. Router

Los routers tienen diversas apariencias según el modelo, pero las características externas clave son las interfaces de la parte posterior. Cada interfaz del router está conectada a una red o a un segmento de red distinto, de allí que se lo considere como un dispositivo de internetworking.

El propósito de un router es examinar los paquetes entrantes, elegir cuál es la mejor ruta para ellos a través de la red y luego conmutarlos hacia el puerto de salida adecuado. Los routers son los dispositivos de regulación de tráfico más importantes en las redes de gran envergadura. Los routers permiten que prácticamente cualquier tipo de PC (que utilice los protocolos adecuados) se comunique con cualquier otra PC en cualquier lugar del mundo (o en el espacio exterior). Mientras ejecutan estas funciones básicas, también pueden ejecutar muchas otras tareas.

Los routers toman sus decisiones de selección de rutas basándose en la información de la Capa 3 (las direcciones de red); por lo tanto, se los considera como dispositivos de la Capa 3.Los routers también pueden conectar distintas tecnologías de la Capa 2 como, por ejemplo, Ethernet, token-ring y FDDI, pero debido a su capacidad para enrutar paquetes, basándose en la información de la Capa 3, los routers se han transformado en la columna vertebral de la Internet, ejecutando el protocolo IP.

1.6 Router Cisco

1.6.1 Encaminamiento de datos

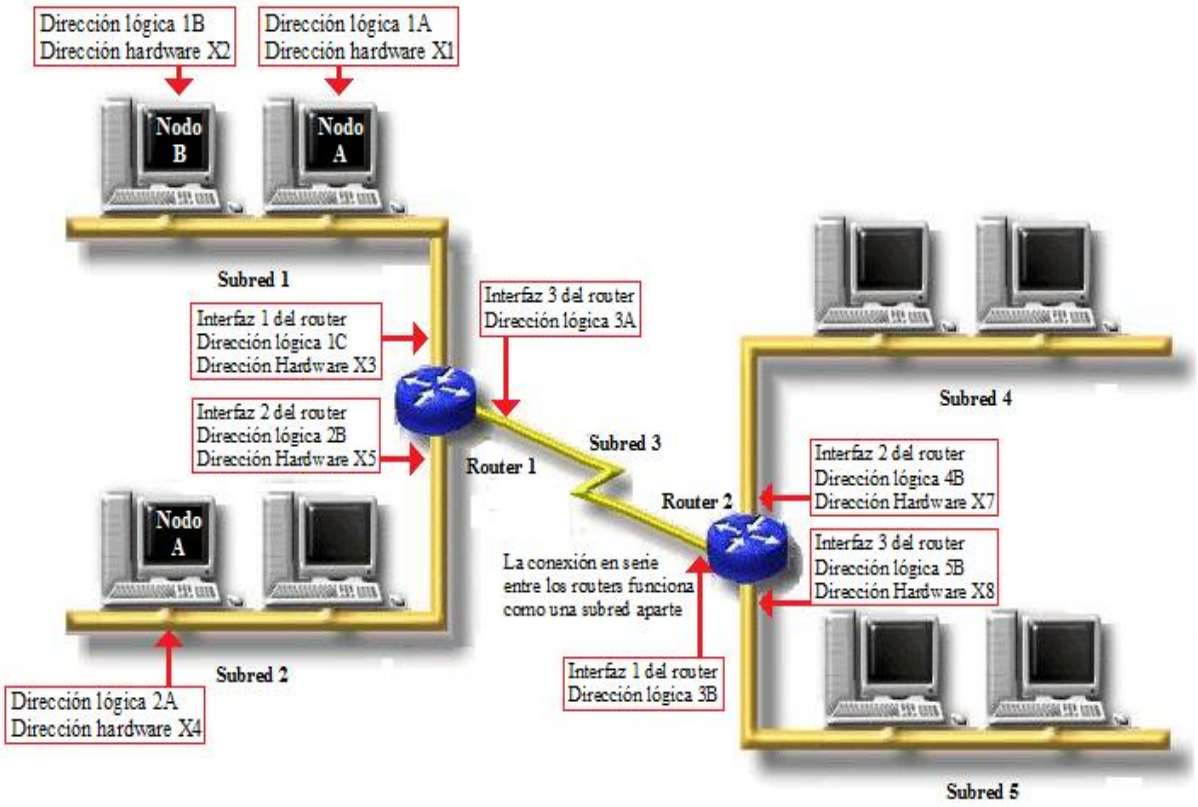
Cuando la información tiene que pasar de una red a otra, el dispositivo de conexión entre redes que se encarga de mover los datos es el router. Para encaminar datos en una interconexión de redes es preciso que se produzcan dos eventos distintos: por un lado, que se determine la ruta apropiada para los paquetes y, por otro, que los paquetes se desplacen hasta su destino final.

Tanto la determinación de la ruta como el encaminamiento de los paquetes se producen en la capa 3 del modelo OSI.

Determinación de la ruta

Los routers permiten dividir una red amplia en subredes lógicas: con ello, se consigue aislar el tráfico local en cada subred, permitiendo así sacar el máximo partido al ancho de banda disponible. El Router pasa entonces a encargarse de transmitir los paquetes de datos entre las subredes. Asimismo, los routers pueden servir de dispositivo de conexión entre la red y como dispositivo de conexión entre el resto de redes a las que esta conectada la propia red. El mejor ejemplo de conexión entre un gran número de redes distintas por motivos de comunicación es, sin duda alguna, Internet.

En la siguiente figura se muestra una red que se ha dividido en dos subredes distintas por medio de un router. En este ejemplo, el router tiene dos interfaces de red, la interfaz 1 y la interfaz 2, que están conectadas a la subred 1 y a la subred 2 respectivamente.



El sistema de direccionamiento lógico que vamos a utilizar para asignar direcciones a los distintos nodos de la red es aplicar el número de subred seguido de la letra que designa a dicha subred. Por tanto, al nodo A de la subred 1 se le asigna la dirección lógica 1A.

Cada nodo de la red también tendrá asignada una dirección de hardware. Para mayor claridad, las direcciones de hardware asignadas a cada uno de los nodos de la red se componen de una X seguida de un número. Por ejemplo, La dirección de hardware para el nodo A de la subred 2 es X4.

Cuando se conectan dos redes utilizando un router, se acaba con dos tipos distintos de trafico de datos: por un lado, con un trafico de datos local, donde los nodos de una misma subred se comunican entre si; y, por otro, con un trafico de

red, donde los nodos de las distintas subredes establecen comunicación. Este último tipo de tráfico es el que tiene que pasar por el Router.
Comunicación en la misma subred

En el nodo A de la subred uno tiene que enviar datos al nodo B de la subred uno. El nodo A sabe que los paquetes tienen que dirigirse a la dirección lógica 1B, además de saber que 1B reside en la misma subred.

Ahora bien, es posible que el nodo A ya sepa que la dirección lógica 1B se refiere a la dirección de hardware X2, de hecho, las computadoras suelen mantener pequeñas memorias de caché donde guardan este tipo de información para la resolución de direcciones lógicas en direcciones de hardware. Si el nodo A no conoce la dirección de hardware correspondiente a la dirección lógica 1B, pasará a enviar un mensaje a la red pidiendo que se resuelva la dirección lógica 1b en una dirección de hardware. Cuando reciba la información, enviará los paquetes al nodo B que los aceptará sin problemas ya que cuentan con su dirección de hardware X2.

Comunicación entre subredes diferentes
El nodo A de la subred 1 desea enviar datos al nodo A de la subred 2. Esto significa que el nodo A de la subred 1 desea enviar datos a la dirección lógica 2 A. El nodo A de la subred 1 sabe que la dirección 2A no se encuentra en la subred local, por lo que pasa a enviar los paquetes a su pasarela predeterminada, que no es más que la interfaz del router que esta conectada a la subred 1. En este caso, la dirección lógica de la pasarela del nodo A es 1C. Sin embargo, como ocurría antes, esta dirección lógica tiene que resolverse en una dirección de hardware, es decir, convertirse en la dirección de hardware en la dirección 1 del router.
Una vez más, y sirviéndose de mensajes de difusión, el Nodo 1 de la subred 1 recibe la información de dirección de hardware relacionada con la dirección lógica

1C (la dirección de hardware es X3) y pasa a enviar los paquetes al Router 1 a través de su interface 1.

Ahora que el Router tiene los paquetes, debe determinar el modo en que deberá reexpedirlos con el fin de que lleguen al nodo de destino. Para ello, consultará la tabla de encaminamiento y después conmutará los paquetes a la interfaz que está conectada a la subred de destino.

Conmutación de paquetes

Cuando los paquetes llegan al Router, se opera la conmutación de los mismos. Esto quiere decir que el Router moverá los paquetes desde la interfaz del Router por la que entraron y los conmutara hasta la interfaz del Router conectada a la subred a la que deben dirigirse.

Sin embargo, en determinados casos, es posible que los paquetes tengan que pasar por más de un Router para alcanzar su destino final. En nuestro ejemplo sólo participa un Router, el Router 1, que sabe que la dirección lógica 2 A se encuentra en la subred 2, por lo que pasa a conmutar los paquetes desde la interfaz 1 de Router a la interfaz 2 de Router.

Se recurre a los mensajes de difusión para resolver la dirección lógica 2 A en la dirección de hardware X4. Se asigna a los paquetes la dirección apropiada y el Router pasa después a reexpedirlos a la subred 2 cuando el Nodo A de la subred 2 ve los paquetes con la dirección de hardware X4, pasa a apropiarse de ellos.

1.6.2 Protocolos encaminados

Antes de pasar a describir los protocolos que determinan la ruta para los paquetes encaminados a través de un Router (y que también mantienen las tablas de encaminamiento de las que se sirve el Router para reexpedir paquetes), convendría comentar brevemente los protocolos encaminados.

Los protocolos de red más utilizados son: TCP/IP, IPX/SPX, Apple Talk y NetBEUI. De todos estos protocolos, solo TCP/IP, IPX/SPX y Apple Talk son encaminados. Esto se debe a que estos tres protocolos proporcionan información suficiente en el encabezado de la capa de red de sus paquetes para enviar los datos desde el nodo emisor hasta el nodo receptor, incluso si los paquetes tienen que pasar por distintas redes.

1.6.3 Protocolos de encaminamiento

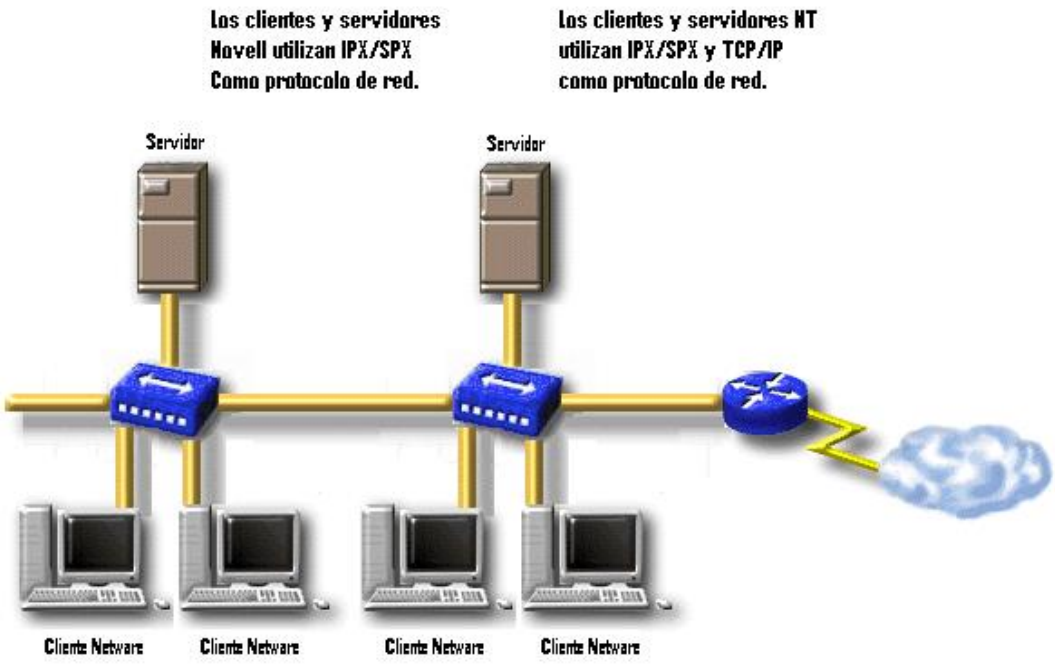
Aunque los protocolos, encaminados proporcionan el sistema de direccionamiento lógico que permite encaminar datos entre distintas redes, los protocolos de encaminamiento proporcionan además los mecanismos para mantener tablas de encaminamiento de *router.* Los protocolos de encaminamiento establecen la comunicación entre los *routers,* lo cual permite a los *routers* compartir la información de ruta que se utiliza para construir y mantener las tablas de encaminamiento.

Existen varios tipos de protocolos de encaminamiento, como el Protocolo de información de Encaminamiento *(Routing Information Protocol* o RIP), el protocolo de Abrir Primero la Vía Más Corta *(Open Shortest Path First* u OSPF), y el Protocolo Mejorado de Pasarela Interior *(Enhanced Interior Gateway Protocol* o EIGRP). Y, aunque estos protocolos utilizan métodos distintos para determinar la mejor ruta con el fin de expedir los paquetes de una red a otra, todos ellos cumplen básicamente el misino objetivo: acumular información de encaminamiento relacionada con un protocolo encaminado específico, como TCP/IP (IP es el segmento encaminado del conjunto de protocolos TCP/IP).

Suele ser común que en las redes LAN y WAN existan máquinas h*ost* y de servidor que ejecuten más de un protocolo de red para comunicarse. Por ejemplo, un servidor NT en su Dominio NT (un Dominio NT es una red gestionada por un

servidor NT llamado Controlador Primario de Dominio) puede utilizar TCP/IP para comunicarse con sus miembros cliente. Pero también puede servir como pasarela a las distintas impresoras y servidores de archivo que utilicen el sistema operativo NetWare de Novell; esto significa que el servidor NT también utilizará IPX/SPX como protocolo de red. Estos protocolos operan fundamentalmente en sus propias pilas de forma simultánea y no interfieren entre sí.

Esta misma idea de protocolos que operan de forma simultánea pero independiente se aplica a los protocolos de encaminamiento. En un mismo *router* pueden ejecutarse múltiples protocolos de encaminamiento independientes, construyendo y actualizando tablas de encaminamiento para distintos protocolos encaminados. Esto significa que el mismo entorno físico de red puede soportan de hecho, distintos tipos de conexiones en red.



Conceptos básicos de los protocolos de encaminamiento

Los protocolos de encaminamiento no solo deben proporcionar información para elaborar las tablas de encaminamiento (y ser capaces de actualizar adecuadamente los routers cuando las rutas de encaminamiento cambian), sino que además tienen que determinar la mejor ruta a través de la conexión entre redes: que deben seguir los paquetes de datos desde la computadora emisora hasta la computadora receptora. Los protocolos de encaminamiento están diseñados para optimizar las rutas dentro de una interconexión de redes, así como para ser estables y flexibles.

Los protocolos de encaminamiento también están diseñados para utilizar poca carga general a la hora de determinar y proporcionar la información de ruta. Esto significa que el propio *router* no tiene por qué ser una mega computadora con varios procesadores pata gestionar el encaminamiento de paquetes; En el apartado siguiente veremos los mecanismos de los que se sirven los protocolos de encaminamiento para determinar las rutas.

Algoritmos de encaminamiento

Un algoritmo es un proceso matemático que permite resolver un determinado problema. Referidos a los protocolos de encaminamiento, los algoritmos pueden considerarse como un conjunto de reglas o procesos que utiliza el protocolo de encaminamiento para determinar la conveniencia de una determinada ruta para transmitir los paquetes por la conexión entre las distintas redes. El algoritmo de encaminamiento permite construir la tabla de encaminamiento que utiliza el router a la hora de encaminar los paquetes.

Los algoritmos de encaminamiento se presentan en dos formaros posibles: como estáticos o dinámicos. Los algoritmos estáticos no son en realidad procesos, si no que están formados por información de correspondencia entre redes que el administrador de red introduce en la tabla de encaminamiento del router. Esta tabla

determinará el modo en que deben transmitirse los paquetes de un punto a otro de la red. Todas las rutas de la red pasarán entonces a ser estáticas, es decir, que no podrán modificarse.

El principal problema que plantean los algoritmos estáticos (además de tener que introducir manualmente en los *routers* toda la información que contienen) es que el ro*uter* no puede adaptarse a los cambios que puedan producirse en la topología de la red. Si un determinado *router* queda desactivado o una porción de la red deja de funcionar, no hay forma de que los *routers* se adapten a estos cambios y actualicen sus tablas de encaminamiento para que los paquetes puedan seguir su camino hasta el final.

Los algoritmos dinámicos se construyen y mantienen por medio de mensajes de actualización del encaminamiento. Estos mensajes, que contienen, información acerca de los cambios que se han operado en la red indican al software de encaminamiento que vuelva a calcular su algoritmo y actualice la tabla de encaminamiento del *router en* consecuencia.

Los algoritmos de encaminamiento (y los protocolos de encaminamiento que utilizan un determinado algoritmo) también se pueden clasificar en función del modo en que suministran la información actualizada a los distintos *routers* de la interconexión. Los algoritmos de encaminamiento por vector de distancia envían mensajes actualizados a intervalos establecidos de tiempo (por ejemplo, cada 30 segundos, como ocurre en el Protocolo de información de Encaminamiento o R1P). Los routers que utilizan algoritmos por vector de distancia pasan toda su tabla de encaminamiento al *router* vecino más próximo *(routers* a los que están directamente conectados). De esta forma se establece un sistema de actualizaciones que reacciona ante cualquier cambio que se opere en la red como la caída en dominó de una línea.

Por ejemplo, en la Figura 5.4, el *Router* 1 se da cuenta de que la conexión con la Red A se ha perdido. En su mensaje de actualización (que envía cada 30 segundos), incluye una tabla de encaminamiento revisada al *Router 2* haciéndole saber a su vecino que la ruta ala Red A ya no está disponible. En su siguiente mensaje de actualización, el *Router* 2 envía una tabla de encaminamiento revisada al *Router* 3, comunicándole que el *Router 2* ya no sirve como ruta para llegar a la Red A. Esta estrategia de actualización se prosigue hasta que todos los *routers* de la red saben que la línea de la Red A ha dejado de ser una ruta valida para las computadoras ubicadas en esa parte de la interconexión de redes.

El principal inconveniente del encaminamiento por vector de distancia se refiere a que los *router* utilizan básicamente información de oídas para construir sus tablas de encaminamiento; no disponen de una vista real de las conexiones de interfaz de un determinado *router.* Tienen, pues, que fiarse de la información que reciben de otro *router* sobre el estado de sus conexiones.

Otra estrategia para actualizar las tablas de encaminamiento en una interconexión de redes es el algoritmo de encaminamiento del estado del enlace. Los protocolos de encaminamiento del estado de enlace no sólo se encargan de identificar a sus *routers más,* próximos, sino que además intercambian paquetes de estado de enlace que informan a todos los ro*uters* de la red sobre el estado de sus distintas interfaces. Esto significa que sólo se envía información acerca de las conexiones directas de un determinado *router.* Y no toda la tabla de encaminamiento como ocurre en el encaminamiento por vector de distancia.

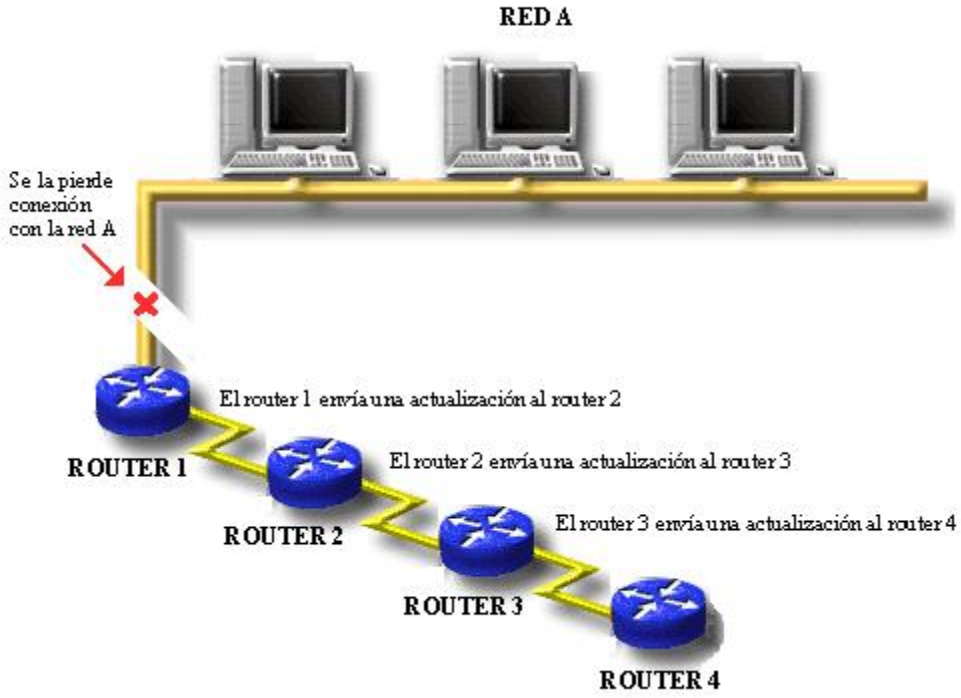


FIGURA 5.4

En el encaminamiento por vector de distancia, los vecinos más próximos proporcionan tablas de encaminamiento actualizadas.

Esto también significa que los *routers* de estado de enlace son capaces de construir una imagen más completó de toda la conexión entre redes y de tomar decisiones más inteligentes a la hora de seleccionar las rutas para el encaminamiento de los paquetes. la convergencia también se produce antes en un sistema de encaminamiento de estado del enlace que en los sistemas que utilizan !a estrategia de! vector de distancia.

Métrica de encaminamiento

Tras repasar los distintos tipos de algoritmos de encaminamiento que existen (estático y dinámico) y las dos estrategias que utilizan para actualizar sus tablas de encaminamiento (vector de distancia y el estado de enlace), vamos a ver cómo los protocolos de encaminamiento determinan, de hecho, la mejor ruta entre una computadora emisora y otra receptora cuando existe más de una ruta posible.

Los algoritmos de encaminamiento utilizan un sistema métrico para determinar la conveniencia de una determinada ruta. Para establecer dicha métrica se sirven de distintos parámetros, como la longitud de la ruta, el coste efectivo de enviar los paquetes por una determinada ruta, o la fiabilidad de una ruta entre las computadoras emisora y receptora.

Por ejemplo, RIP, un protocolo de encaminamiento por vector de distancia, utiliza el número de saltos como sistema métrico. Un salto es el paso de los paquetes de una red a otra. Si existen dos rutas posibles para transmitir los paquetes de una ubicación a otra, RIP elegirá la ruta que resulte más deseable en cuanto a que presenta un menor número de saltos. La figura 5.5 muestra una conexión entre redes donde existen dos rutas posibles para encaminar los paquetes entre las computadoras emisora y receptora. Puesto que la Ruta A sólo requiere de un salto, se considera la ruta óptima para transmitir los paquetes.

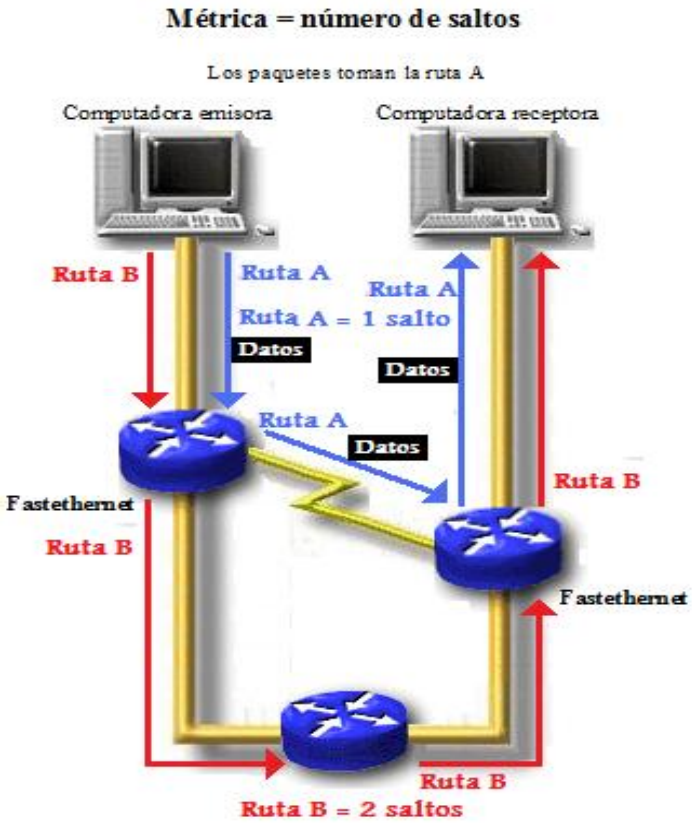


FIGURA 5.5

El problema que plantean los protocolos de encaminamiento que sólo utilizan una métrica ('como el número de saltos) es que suelen obcecarse con la búsqueda de la ruta más efectiva para un determinado conjunto de paquetes. RIP por ejemplo, no tiene en cuenta la velocidad ni la fiabilidad de las líneas a la hora de seleccionar la mejor ruta, fijándose únicamente en su número de saltos. Por ello, y como puede apreciarse en la Fisura 5.5 aunque la Ruta A es la ruta más efectiva en cuanto al número de saltos que se producen, los paquetes van a transmitirse, de hecho por la línea más lenta (una línea contratada de 56 kilobits). Esta línea no sólo resulta lenta sino a demás bastante cara. La Ruta B pasa por un cableado que (.pertenece a la compañía (forma parte de la infraestructura de la red) *y* ofrece un medio de transmisión mucho más rápido *(Fast Ethernet* a 1OO Mbps). Sin embargo, cuando se utiliza un protocolo de encaminamiento que adopta el número de saltos como métrica, forzosamente nos vemos obligados a utilizar la Ruta A.

Para hacer frente a la escasa flexibilidad que presenta la métrica de número de saltos, se puede recurrir a muchos otros protocolos de encaminamiento que utilizan una métrica más compleja, pero también más flexible. Por ejemplo, el Protocolo Mejorado de Pasarela Interior *(Interior Gafeway Routing Protocolo* o ÍGRP) es un protocolo de encaminamiento por vector de distancia capaz de utilizar hasta 255 métricas distintas, según lo configure el administrador de la red. Estas métricas pueden referirse al ancho de banda (la capacidad de transmisión de las líneas), a la carga (es decir, a la cantidad de tráfico que ya gestiona un determinado *router en l*a ruta), y al coste de la comunicación (los paquetes se envían por la ruta mas barata. Cuándo se combinan varias métricas de encaminamiento para determinar la ruta mas idónea para un paquete, se utiliza *un* método de determinación aun más complejo. Por ejemplo, y retomando el caso de la Fisura 5.5, un protocolo de encaminamiento que no utilice la métrica de número de saltos y se decante por otra métrica (como el coste de la comunicación) hubiera seleccionado la ruta con más saltos, pero que genera un coste menor a la hora de transmitir los paquetes.

Tipos de protocolos de encaminamiento

Las conexiones entre redes que se dan en el mundo real (en particular, aquéllas que abarcan el conjunto de la corporación empresarial) están compuestas por varios *routers* que proporcionan el mecanismo para transmitir los paquetes entre las distintas subredes que conforman la red. Para conducir los datos de forma eficaz, los *routers* conectados suelen dividirse también en subredes de la interconexión. Las subredes que integren varios *routers* se denominan áreas. Cuando se agrupan distintas áreas en una subred de nivel superior, dicho nivel administrativo recibe el nombre de dominio de encaminamiento.

La siguiente figura muestra una interconexión de redes dividida en áreas. Cada área se cierra con un ro*uter* de gama alta llamado *router* fronterizo (o ro*uter* de

núcleo). Los dos *routers* fronterizos están conectados entre sí, lo que, de hecho, conecta los dos dominios de encaminamiento (o sistemas autónomos, como se conocen en las interconexiones de redes IP).

El hecho de que las conexiones entre redes puedan dividirse en agrupamientos lógicos como los dominios de encaminamiento (o sistemas autónomos) es lo que dio origen a distintos tipos de protocolos de encaminamiento: protocolos de encaminamiento que proporcionan el encaminamiento de paquetes entre *routers* dentro de un mismo dominio de encaminamiento, y los protocolos de encaminamiento que proporcionan el encaminamiento de paquetes entre dominios de encaminamiento distintos.

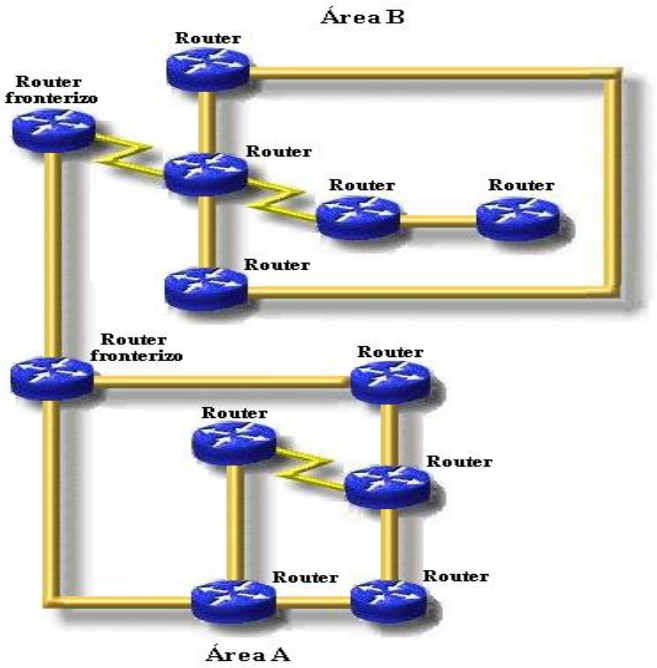


FIGURA 5,6

Las interconexiones de redes pueden dividirse en áreas que están conectadas entre sí por medio de *routers* fronterizos.

Los Protocolos Internos de Pasarela *(Interior Gateway protocols* o IGP) se encargan del encaminamiento de paquetes dentro de un dominio de encaminamiento**.** Los IGP, como RIP o IGRP, se configuran en cada uno de los routers incluidos en el dominio de *router.*

Los protocolos que transmiten los datos entre dominios de encaminamiento reciben el nombre de Protocolos Externos de Pasarela *(Exterior Gateway protocols* o EGP). Ejemplos de este tipo de protocolos son el Protocolo de Pasarela fronteriza *(Border Gateway Protocol* o BGP) y el Protocolo Externo de Pasarela *(Exterior Gateway Protocol* o EGP).

Protocolos Internos de Pasarela

Los Protocolos internos de Pasarela están formados por protocolos de encaminamiento basados en algoritmos por vector de distancia y del estado de enlace. Existen muchos tipos de IGP y su diferencia radica esencialmente en el número de métricas que utilizan para determinar las rutas de encaminamiento más adecuadas. El ÍGP más antiguo es el Protocolo de Información de Encaminamiento del que hablaremos en el apartado siguiente, y al que se ha ido sumando otros.

Protocolo de información de Encaminamiento

El Protocolo de Información de Encaminamiento *(Routing Information Protocol* o RIP) es un protocolo de encaminamiento IP por vector de distancia que utiliza el número de saltos como métrica para determinar la ruta más efectiva. Y aunque se trata del protocolo IGP más antiguo de todos, el protocolo RIP se sigue utilizando hoy en día.

RIP envía un mensaje de actualización del encaminamiento cada 30 segundos (tiempo predeterminado por Cisco), en el que se incluye toda la tabla de encaminamiento del router RIP utiliza el Protocolo de Datagrama de Usuario *(User*

Datagram Proíocol o UDP forma parte del conjunto de protocolos TCP/IP como método de encapsulación para el envío de avisos de encaminamiento)

El protocolo RIP presenta, sin embargo, una serie de restricciones ya que limita a 15 el número máximo de saltos para el encaminamiento de paquetes específicos. Esto significa que RIP resulta un buen protocolo pura las interconexiones pequeñas y homogéneas, pero su métrica carece de la flexibilidad que requieren las grandes redes.

Protocolo Interno de Encaminamiento de Pasarela

El Protocolo Interno de Encaminamiento de Pasarela (*Interior Gateway Routing Protocol* o IGRP) fue desarrollado por Cisco en la década de los ochenta. IGRP es un protocolo de encaminamiento basado en algoritmos por vector de distancia. IGRP utiliza una métrica compuesta que tiene en cuenta distintas variables; esto hace que supere algunas de las limitaciones de RIP, como la métrica de número de saltos y su incapacidad para encaminar paquetes en redes que requieran más de 15 saltos.

IGRP (comparado con RIP) también envía mensajes de actualización del encaminamiento a intervalos de tiempo más largos y utiliza un formato más eficiente para los paquetes actualizados que se transmiten entre routers. IGRP soporta además el uso de sistemas autónomos (al igual que las áreas a las que antes nos referíamos), por lo que los routers que ejecutan IGRP pueden aislarse dentro de aquellos dominios donde el tráfico entre routers sea local. Esto permite disminuir la cantidad de comunicaciones entre routers y optimizar el ancho de banda que se utiliza por toda la interconexión.

1.6.4 Interfaces del Router

Una interfaz de Router suministra la conexión física entre el Router y un tipo de medio físico de la red. Las interfaces de Cisco a menudo se denominan puertos y cada puerto viene designado físicamente de acuerdo de acuerdo con la topología de red a la que sirve. Por ejemplo una interfaz LAN, como un puerto Ethernet en el Router, se compone de un conector hembra RJ-45.

Los puertos incorporados se designan por su tipo de conexión seguido de un número. Por ejemplo si el primer puerto Ethernet en un Router se designa como E0, el segundo se designaría como E1, y así sucesivamente. Los puertos serie se designan siguiendo este mismo procedimiento, donde S0 corresponde al primer puerto serie.

Los routers de Cisco, como los de la serie 2500 o 1700, son básicamente routers estándar que vienen con un número predeterminado de puertos LAN y WAN. Los routers de gama alta, como el 4500 de cisco son modulares y, de hecho, contienen ranuras abiertas en las que pueden instalarse varias tarjetas de interfaz. No sólo pueden conectarse distintos tipos de tarjetas de interfaz (como LAN o WAN), si no que además puede seleccionarse el número de puertos deseados en cada tarjeta. Por ejemplo en una de las tres ranuras abiertas del Router 4500 se puede instalar una tarjeta Ethernet que contenga seis puertos Ethernet.

Los routers modulares designan sus puertos por el tipo de conexión que utilizan, seguido del número de ranura y del número de puerto. Por ejemplo, el primer puerto Ethernet en una tarjeta Ethernet instalada en la primera ranura del Router se designaría como Ethernet 1/0 (la ranura se designa primero, seguida del número de puerto).

1.6.4.1 Interfaces LAN

Los Router de Cisco soportan varias redes LAN ampliamente utilizadas. Las interfaces de Router más comunes para redes LAN son Ethernet, Fast Ethernet, Token Ring de IBM y la interfaz de Datos Distribuida por Fibra Óptica (FDDI).
Todos estos protocolos LAN utilizan el mismo sistema de direccionamiento físico de la capa de enlace de datos (es decir, la dirección MAC de hardware en una NIC, o la dirección MAC de hardware ubicada en el controlador de la interfaz de la interfaz de router). Estas direcciones son únicas para cada dispositivo. A continuación se ofrece un breve listado de todas las tecnologías LAN:

Ethernet. Se trata de una arquitectura pasiva de red que utiliza el acceso múltiple de percepción de portadora con detección de colisión (*carrier sense multiple access with collision detection* o CSMA/CD) como estrategia de acceso a la red. Se puede utilizar un router de Cisco para dividir una red Ethernet en subredes lógicas (como subredes IP). Normalmente, el router se conecta a la red Ethernet por medio de un cable de par trenzado (UTP) y un conector RJ-45.

Fast Ethernet. Utiliza la misma estrategia de acceso que una Ethernet normal (CSMA/CD) y se ejecuta en cables de par trenzado (lo mismo que Ethernet normal). Fast Ethernet requiere interfaces especiales en los routers (interfaces Fast Ethernet) y tarjetas de red Fast Ethernet en los nodos.

Token Ring. Es una arquitectura de red propietaria desarrollada por IBM. Las redes Token Ring se ejecutan en un anillo lógico (el anillo lo componen internamente las unidades de acceso multiestación (MAU) que se utilizan para conectar los distintos nodos de la red). Las redes Token Ring utilizan la pasada de señal (el token) como estrategia de acceso a la red. Los routers que se utilizan en las redes Token Ring deben contener una interfaz especial Token Ring para la conexión en red.

FDDI. FDDI es una red de pasada de señal que utiliza dos anillos redundantes (pasada de señales o tokens en direcciones opuestas) como método de tolerancia a fallos (la tolerancia a fallos permite que la red siga funcionando cuando uno de los anillos se interrumpe). FDDI, que a menudo se emplea como un segmento principal de fibra óptica para grandes redes o redes de área municipal. Los routers que se utilicen en las redes FDDI tienen que tener una interfaz FDDI.

Todos los protocolos LAN requieren una interfaz que coincida con la del router que utilizan.

1.6.4.2 Interfaces Wan

Las interfaces en serie de router permiten conectar varias redes LAN utilizando tecnologías WAN. Los protocolos WAN transmiten datos a través de interfaces asincrónicas y sincrónicas en serie (dentro de los routers), que están conectadas entre si mediante líneas contratadas y otras tecnologías de conectividad suministradas por terceros.

Las tecnologías WAN de la capa de enlace de datos que mas se utilizan en la actualidad son el control de enlace de datos de alto nivel (HDLC) , el Relé de trama (frame Relay), la Red Digital de Servicios Integrados (ISDN) y el protocolo punto a punto (PPP). Todos estos protocolos WAN se configuran en determinadas interfaces de router (como en una interfaz en serie o en una interfaz ISDN) cuando el router se encuentra en el modo de configuración.

- HDLC es un protocolo de la capa del enlace de datos que se encarga de encapsular los datos transferidos a través de enlaces sincrónicos de datos. Esto significa que un dispositivo como un DCE (equipo de comunicación de datos) proporciona una conexión a la red, así como una señal que sincroniza la transferencia de datos entre los dos extremos del enlace en

serie. En un router los puertos serie están conectados a un modem u otro tipo de dispositivo CSU/DSU a través de cables especiales, como un cable V.35. HDLC es el protocolo WAN predeterminado para los routers de Cisco. HDLC se considera un protocolo de punto a punto y proporciona una conexión directa entre dispositivos emisores y receptores (como dos routers).

- El protocolo punto a punto (PPP) es otro protocolo de la capa del enlace de datos que soportan los routers de Cisco. No es propietario, por lo que puede utilizarse para conectar router de cisco con dispositivos de conexión entre redes de otros fabricantes PPP opera, de hecho, tanto en el mundo sincrónico como asincrónico (lo que significa que puede proporcionar cualquiera de dos los tipos de encapsulación). PPP se configura en el puerto serie del router que proporciona la conexión a una línea dedicada u otro tipo de conexión WAN. Los usuarios suelen estar familiarizados con PPP ya que es el protocolo que se utiliza para conectar estaciones de trabajo con los proveedores de servicios Internet a través de un modem y líneas telefónicas analógicas.

- El Relé de Trama (Frame relay) es un protocolo de la capa del enlace de datos para la conmutación de paquetes que fue desarrollado originalmente para ser utilizado a través de las conexiones ISDN. Ahora reemplaza a X.25 como protocolo para redes conmutadas y utiliza circuitos virtuales para definir una ruta entre dos dispositivos de comunicación (como dos routers, por ejemplo) a través de una red WAN. En una conexión relé de trama un DTE, como un router, esta conectado a un DCE del tipo CSU/DSU (la mayoría de dispositivos CSU/DSU pueden conectarse a un router utilizando un cable serial V.35). Otra posibilidad es que el router este conectado directamente al equipo de conmutación de la compañía telefónica.

- La Red Digital de Servicios Integrados (ISDN o RDSI) utiliza tecnología digital para conducir datos, voz y video, a través de líneas telefónicas ya existentes. Se trata de un protocolo WAN asincrónico que requiere que la red este conectada a la línea telefónica a través de un equipo Terminal común mente denominado modem RDSI. Sin embargo, también pueden utilizarse router de Cisco que integren una interfaz BRI (BRI es el acrónimo de Basic Rate Interface o interfaz de velocidad básica). La interfaz BRI pasa entonces a conectarse directamente a las líneas telefónicas. Si el router utilizado no dispone de puerto BRI. Se tiene que conectar uno de los puertos serie existentes al modem RDSI.

1.6.4.3 Interfaces lógicas

Una interfaz lógica es una interfaz únicamente de software que se crea mediante el IOS de un router.

Las interfaces lógicas no existen como tales, es decir, no son interfaces de hardware de un router. Para entender el concepto de interfaz lógica, se puede considerar como una interfaz virtual creada por medio de una serie de comandos del software del router.

Los dispositivos reconocen estas interfaces virtuales como interfaces reales, lo mismo que una interfaz de hardware, como un puerto serie. Se pueden configurar distintos tipos de interfaces lógicas en un router, como interfaces de retrobucle, interfaces nulas e interfaces de túnel.

Interfaces de retrobucle

Es una interfaz que emula una interfaz física real en el router. Los retrobucles suelen configurarse en un router de gama alta utilizado como router de núcleo entre dos interconexiones corporativas de redes o entre una red corporativa e

Internet. Puesto que el router sirve como enlace fundamental entre interconexiones de redes, los paquetes de datos no deberían volcarse si una determinada interfaz física del router deja de funcionar. Por esto mismo, la interfaz virtual de retrobucle se crea y configura como la dirección de finalización para las sesiones del Protocolo de Pasarela Fronteriza (BGP). De esta forma, el tráfico se procesa localmente en el router, lo que garantiza la recepción íntegra de los paquetes en su destino final.

Interfaces nulas

Esta interfaz se configura en un router utilizando determinados comandos del router y sirve como un muro de contención para impedir el paso de un determinado tráfico de la red. Por ejemplo si no desea que el tráfico de una determinada red pase por un determinado router se puede configurar la interfaz nula de forma que reciba y vuelque todos los paquetes que la red envíe a dicho router. Por lo general, los listados de acceso se utilizan para filtrar el tráfico en una interconexión de redes y definir los routers que pueden utilizarse para determinadas redes.

Interfaces de túnel

Una interfaz de túnel es otra interfaz lógica que puede utilizarse para conducir un determinado tipo de paquetes a través de una conexión que normalmente no soporta dicho tipo de paquetes.

1.6.5 Interfaces de administración

1.6.5.1 Puerto consola

Puerto consola, se conecta a un PC, mediante este puerto podemos monitorear y configurar el router.

1.6.5.2 Puerto auxiliar

El puerto auxiliar es muy importante, ya que en dado caso de que el puerto consola no funcionara, podemos ocupar el puerto auxiliar como consola para poder acceder al router, además se le puede conectar un modem como línea de respaldo, la cual entrará en operación cuando se pierda el enlace principal, así hay menos posibilidades de que el usuario se quede sin conexión a la red.

Capitulo 2. Configuración de un router Cisco

2.1. Proceso de arranque del router

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

El objetivo de las rutinas de inicio del software Cisco IOS es iniciar la operación del router. El router 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 router tenga todo su hardware probado.
- Encontrar y cargar el software Cisco IOS que el router usa para su sistema operativo.
- Encontrar y aplicar las sentencias de configuración del router, incluyendo las funciones de protocolo y las direcciones de interfaz.

Un router utiliza la siguiente información proveniente del archivo de configuración cuando se inicia:

- Versión del software Cisco IOS.
- Identificación del router
- Ubicaciones de los archivos de arranque
- Información de protocolos
- Configuraciones de las interfaces

El archivo de configuración contiene comandos para personalizar la operación del router. El router utiliza esta información cuando se inicia. Si no hay ningún archivo de configuración disponible, el diálogo de configuración inicial del sistema lo guía a través del proceso de creación de este archivo.

La información de configuración del router puede ser generada por varios medios. Puede utilizar el comando **configure** del modo EXEC privilegiado para realizar la configuración desde una terminal virtual (remota), una conexión de módem o una terminal de consola. Esto nos permite introducir cambios en una configuración existente en cualquier momento. También se puede utilizar el comando **configure** del modo EXEC privilegiado para cargar una configuración desde un servidor de red TFTP, que le permite mantener y guardar información de configuración en un sitio central

Cuando se enciende un router Cisco, realiza una prueba automática de encendido (POST). Durante esta prueba automática, el router ejecuta diagnósticos desde la ROM para 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 router procede a inicializar el software.

Después de la prueba automática de encendido del router, se producen los siguientes eventos a medida que se inicializa el router:

- **Paso 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.
- **Paso 2**. El sistema operativo (Cisco 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 un Flash, o carga de red,

comandos del **sistema de arranque** en el archivo de configuración indican la ubicación exacta de la imagen.

- **Paso 3**. Se carga la imagen del sistema operativo. Cuando está cargado y funcionando, el sistema operativo ubica los componentes del hardware y software y muestra los resultados en la terminal de consola.
- **Paso 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 enrutamiento, brindan direcciones para las interfaces, establecen las características de los medios, etc.
- **Paso 5**. Si no existe ningún archivo de configuración válido en la NVRAM, el sistema operativo ejecuta una rutina de configuración inicial con preguntas denominada *diálogo de configuración del sistema*, también denominado *diálogo de configuración inicial*.

El modo de configuración inicial no debe ser el modo utilizado para introducir funciones complejas de protocolo en el router. 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 router.

2.2. Los distintos modos del router

Para configurar los routers de Cisco, se debe acceder a la interfaz de usuario en el router con una terminal o acceder al router de forma remota. Por razones de seguridad

El router ofrece tres modos básicos de acceso: el modo User (Usuario) el modo Privileged (Privilegiado) y el modo Configuration (Configuración).

Cada uno de estos modos básicos del router proporciona un grado más alto de acceso a la configuración del router y permiten, en mayor o menor grado, modificar la configuración del router.

Modo Usuario. Este modo proporciona un acceso limitado al router Se ofrece una serie de comandos no destructivos que permiten examinar algunos parámetros de configuración del router. No permite, sin embargo, introducir cambios en su configuración

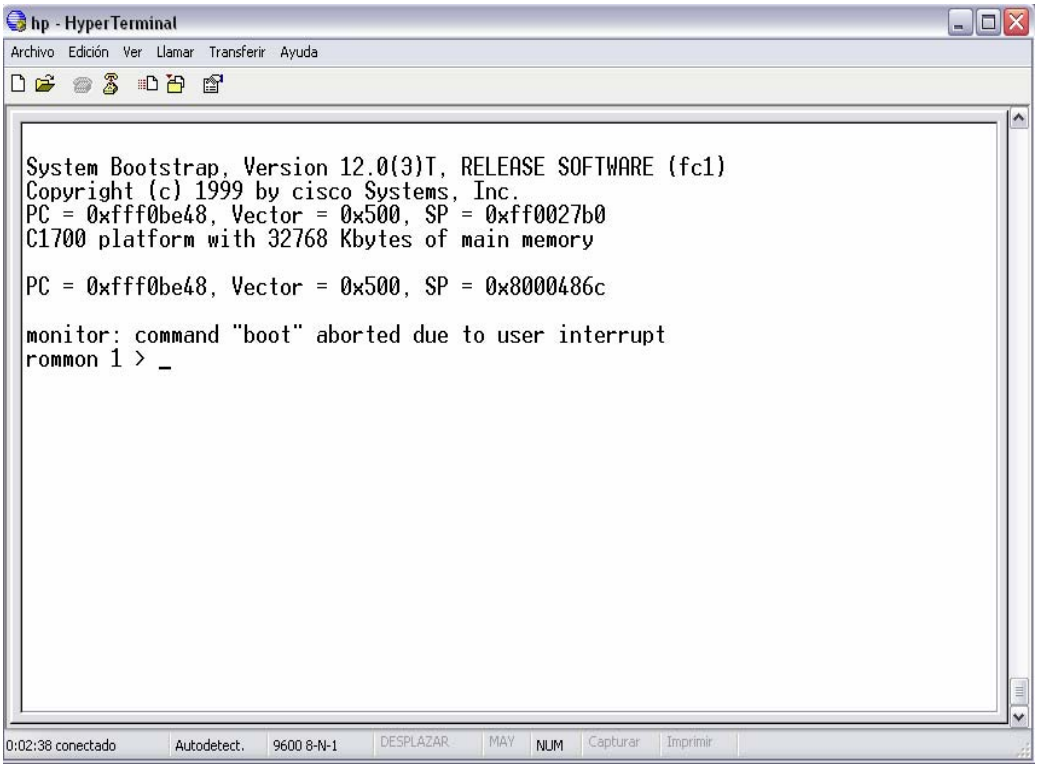
Modo Privilegiado. Conocido también como modo de Activación (Enable), este modo permite examinar en más profundidad el router y proporciona un conjunto de comandos más robustos que el modo Usuario. Tras acceder al modo Privilegiado utilizando la contraseña secreta o de activación (si no se especificó una contraseña secreta cifrada) se puede acceder a los comandos de configuración que proporciona el modo Configuración y editar, por tanto, la configuración del router.

Modo Configuración. También llamado modo de Configuración Global, este modo se lanza desde el modo Privilegiado y proporciona todos los comandos de configuración del router. Existen además subconjuntos del modo Configuración para los protocolos, interfaces y otros aspectos relativos a la operación del router.

2.2.1. Modo ronmon (ronmon >)

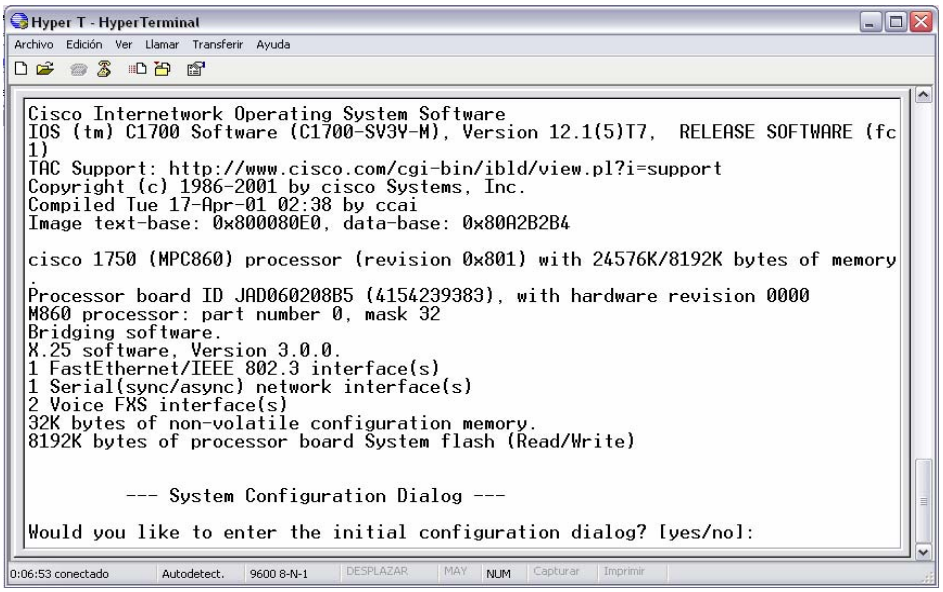
Existen otros modos de router que permiten configurar un router que no puede encontrar una imagen válida del lOS en la memoria Flash RAM o en aquellos casos en que se desea cargar el lOS del router desde otra fuente que no sea a memoria flash. El modo ROM Monitor (Monitor ROM) se lanza cuando el router no encuentra una imagen válida del lOS. Se puede configurar el router desde el indicador del Monitor ROM. El modo RXBoot (Arranque RX) se utiliza para ayudar a la guía del router cuando no encuentre una imagen valida del IOS. El modo

Monitor ROM permite además cambiar las contraseñas que se hayan olvidado o perdido



2.2.2. Modo setup

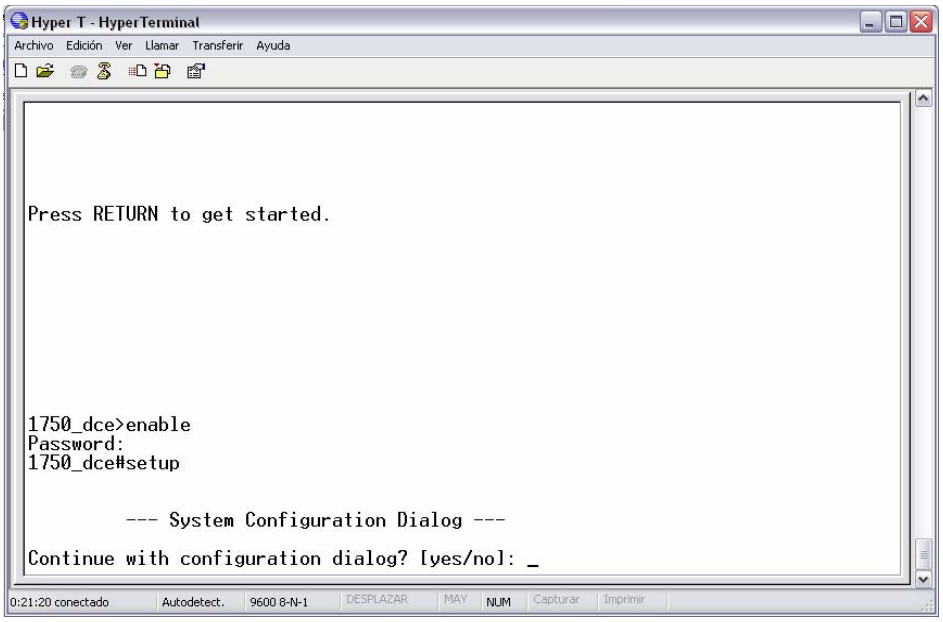
Al iniciar por primera vez un router Cisco, no existe configuración inicial alguna. El software del router pedirá un conjunto mínimo de detalles a través de un diálogo opcional llamado setup



Como ya se menciono anteriormente el modo setup solo sirve para configurar los parámetros de arranque más elementales, para salir de este modo solo se responde que NO a la pregunta inicial.

Would you like to enter the initial configuration dialog? [yes]: No
Would you like to terminate autoinstall? [yes]: INTRO

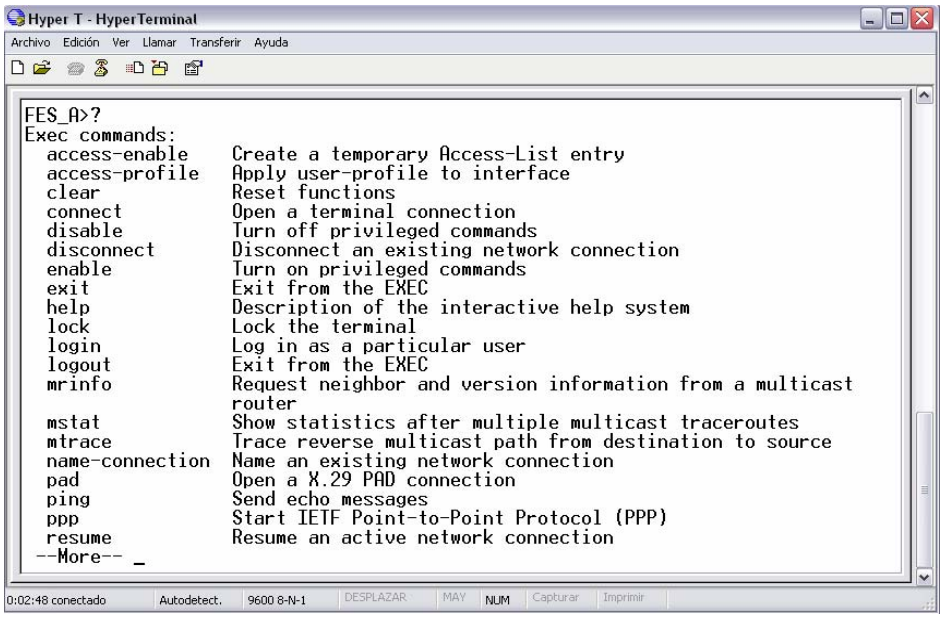
Para volver a inicializar el modo setup basta con ejecutar la orden *setup* en el modo privilegiado sin importar que ya exista una configuración previa o simplemente con volver a encender el equipo siempre y cuando este carezca de alguna configuración guardada en la NVRAM

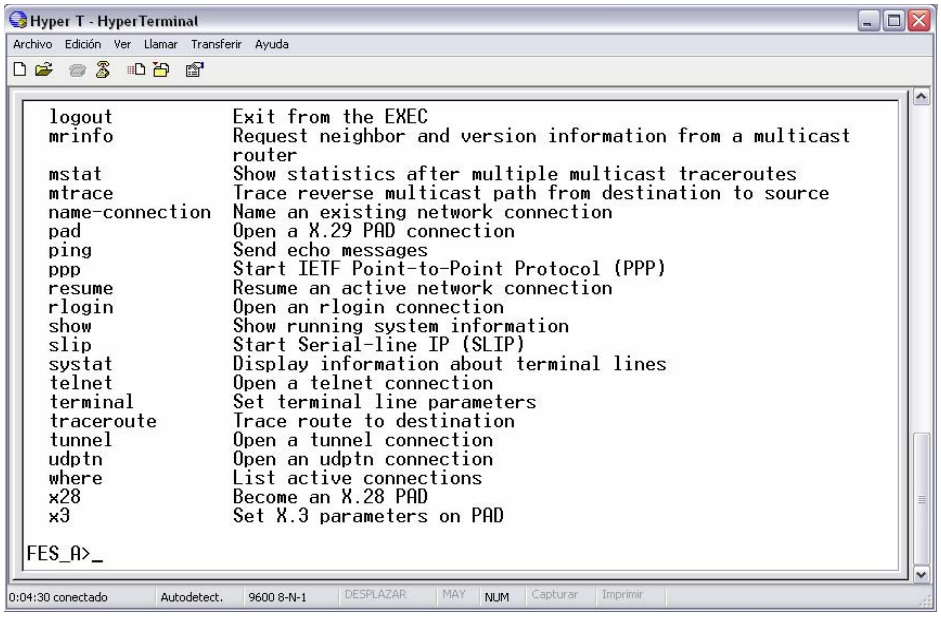


2.2.3. Modo usuario (no privilegiado *Router*>)

Como se menciono anteriormente el modo Usuario permite examinar, de forma limitada la configuración del router. El modo Usuario es el modo que se activa por defecto al volver a arrancar el router. El acceso a este modo también puede protegerse por medio de una contraseña de consola

En las siguientes figuras se muestra el indicador del modo Usuario así como algunos de los comandos disponibles con su descripción a la derecha, cabe señalar que los comandos varían de acuerdo al modelo del router y a la versión del IOS que se maneje





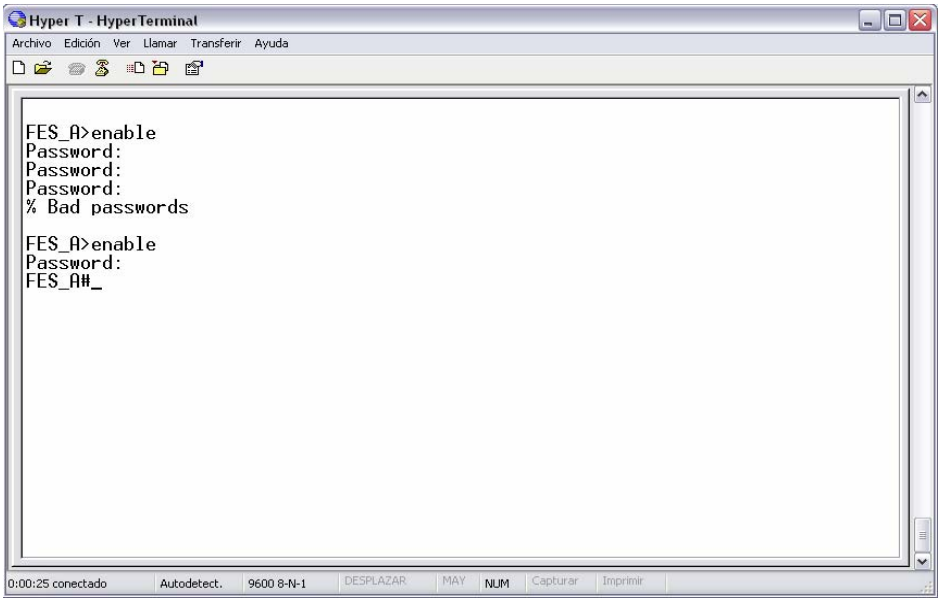
El funcionamiento del modo Usuario puede equipararse a la conocida fórmula de "se puede mirar pero no tocar". Sin embargo, lo que sí ofrece es una gran cantidad de información acerca del router y de su actual estado.

2.2.4. Modo privilegiado (*Router#*)

El modo Privilegiado proporciona todos los comandos incluidos en el modo usuario, además de ofrecer un amplio conjunto de comandos para examinar el estado del router (Como el comando *show running-config* que permite examinar la configuración actual de ejecución para el router). El modo Privilegiado también proporciona acceso al modo de configuración global mediante el comando *configure terminal.*

Con el modo Privilegiado se puede de hecho controlar el router. Por ello, es importante asignar una buena contraseña de activación para impedir que alguien modifique la configuración del router (si alguien tiene que acceder a alguno de los parámetros del router, siempre podrá hacerlo desde el modo Usuario)

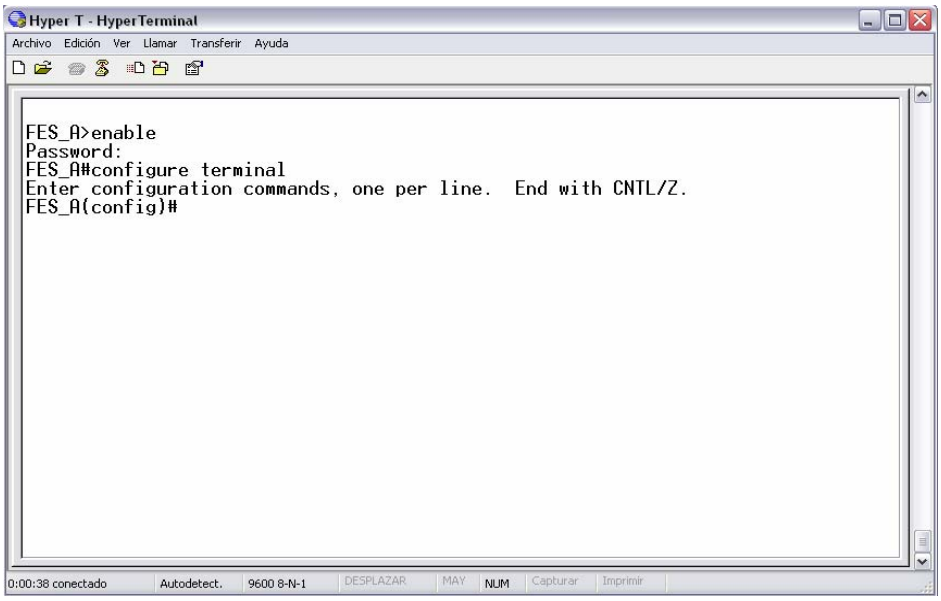
Para entrar al modo Privilegiado debe escribirse el comando *enable* desde el modo Usuario y después pulsar intro siempre y cuando no este protegido, de lo contrario pedirá una contraseña. El indicador del modo Privilegiado es el nombre del router seguido del carácter número #.



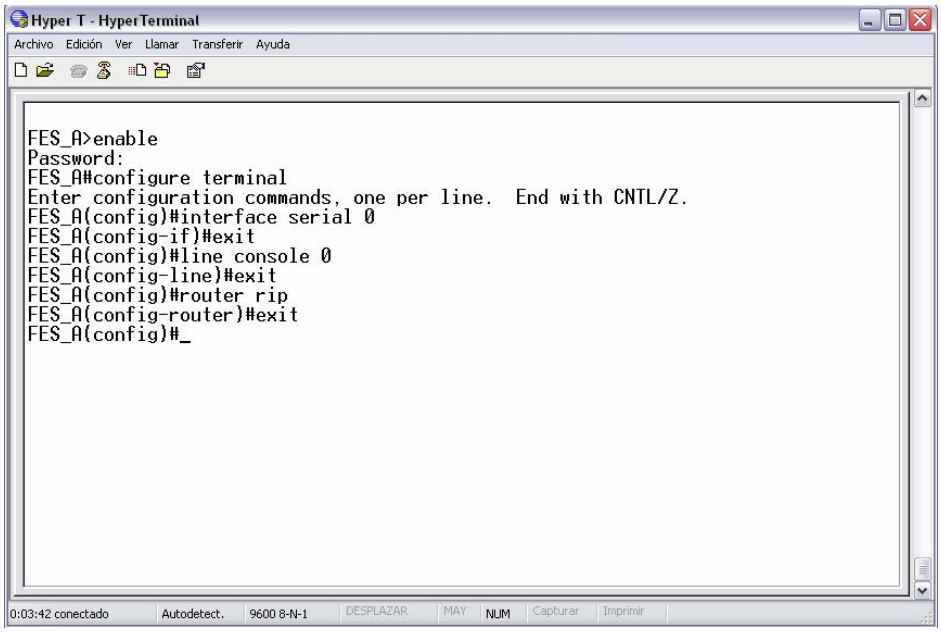
Una vez finalizado e trabajo en el modo privilegiado se debe finalizar la sesión, de no ser así, se dejara al descubierto el router y cualquiera que accediera por la terminal podría modificar la configuración, para volver al modo Usuario se utiliza la instrucción *logout*. De esta forma la próxima persona que se conecte a la consola del equipo deberá introducir la contraseña (siempre y cuando halla sido configurada) para entrar al modo Privilegiado, otra forma más usada para salir completamente del router es mediante el comando *exit*.

2.2.5. Modo de Configuración global (*Router(config)#*)

El modo de Configuración permite determinar todos los parámetros relacionados con el hardware y el software. Aquí pueden configurarse las interfaces, los protocolos encaminados y de encaminamiento. También pueden establecerse las contraseñas del router y configurar los protocolos WAN que utilizan las interfaces en serie del router. Algunas de las opciones de configuración referidas al router pueden establecerse en un router nuevo desde el cuadro de dialogo *System Configuration* (modo Setup). El modo de configuración permite acceder a todos los comandos que se requieren para configurar o ajustar la configuración de un router. Para acceder al modo de configuración global se debe ejecutar la instrucción *configure terminal* desde el modo privilegiado una vez adentro, el indicador cambiara a *Router(config)#*



El indicador seguirá cambiando en el modo de configuración global con algunos de los parámetros introducidos como por ejemplo al modificar alguna de las interfaces se ocupara el comando *interface serial 0*, al ejecutar la orden el indicador cambiara a *Router(config-if)#,* y ahora estarán disponibles otros comandos relacionados con la interfaz a configurar, para regresar a *Router(config)#*, solo basta con ejecutar la orden *exit*



2.3. Inicio de sesión de un router Cisco

Los computadores tienen cuatro componentes básicos: una CPU, memoria, interfaces y un bus. Un router también tiene estos componentes, y por lo tanto se puede considerar como un computador. Sin embargo, se trata de un computador especial. En lugar de tener componentes dedicados a dispositivos de salida de vídeo y audio, dispositivos de entrada como teclado y ratón y el software sencillo de interfaz gráfica que es típico del computador multimedia, el router se dedica exclusivamente al enrutamiento.

Al igual que los computadores, que necesitan sistemas operativos para ejecutar aplicaciones de software, los routers necesitan el software Sistema Operativo de Internetworking (IOS) para ejecutar archivos de configuración. Estos archivos de configuración controlan el flujo de tráfico a los routers. Específicamente, al usar protocolos de enrutamiento para dirigir los protocolos enrutados y las tablas de enrutamiento, toman decisiones con respecto a la mejor ruta para los paquetes. Para controlar estos protocolos y estas decisiones, es necesario configurar el router.

Dado que el router carece de interfaz grafica y dispositivos de entrada como un teclado, nos apoyamos en el uso de un PC para podernos comunicar con él y así poderlo configurar, esto se logra mediante el programa de HyperTerminal

2.3.1. Conexión al puerto consola

Los routers Cisco cuentan con un puerto consola serial asíncrono (CON o Console), con el cual la configuración del router puede ser introducida. La comunicación de un Router con una Pc se logra a través de un cable llamado *cable consola*, este cable consta de ocho hilos en uno de sus extremos cuenta con un conector RJ-45 que es usado para conectarse al puerto Consola del router mientras que en su otro extremo se encuentra un conector DB-9 hembra y por

separado un adaptador DB-9 a DB-25, esto se debe a que uno de los dos conectores será requerido de acuerdo a los requerimientos de la PC

2.3.2. Ensamblar un cable de consola

En la práctica no siempre se puede contar con un cable consola o simplemente se rompe alguno de los hilos o conectores y este deja de funcionar correctamente, para cualquiera que sea el caso, en la siguiente tabla se muestra la disposición de cada uno de los pines para ensamblar un cable consola con terminal BD-9 o DB-25

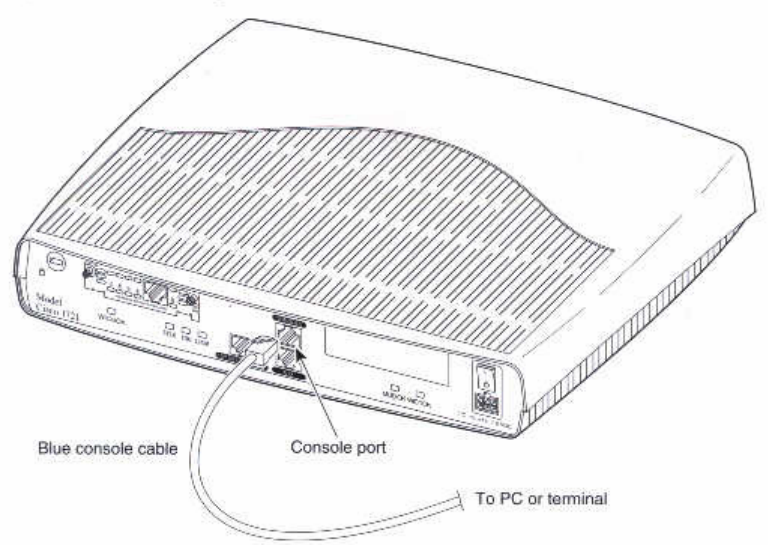
RJ-45	DB-25	DB-9	Señal
1	5	8	CTS
2	6	6	DSR
3	3	2	RXD
4	8	1	DCD
5	7	5	GND
6	2	3	TXD
7	20	4	DTR
8	4	7	RTS

2.3.3. Configuración de hyperterminal

Una vez hecha la conexión del router a la PC vía hardware, ahora es tiempo de configurar el software de la PC que como se menciono anteriormente es el programa de comunicaciones llamado Hyperterminal

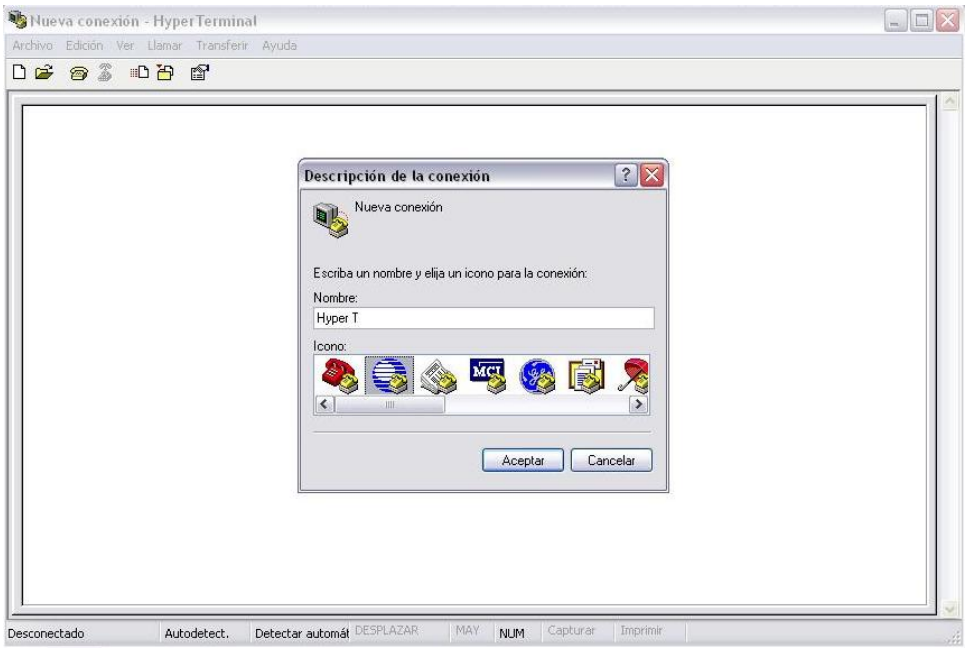
1. Se conecta la terminal DB-9 del cable consola al puerto serie del PC y la terminal RJ45 al puerto consola del Router

Nota: En caso de que el puerto Consola del router este dañado, se utiliza el puerto auxiliar

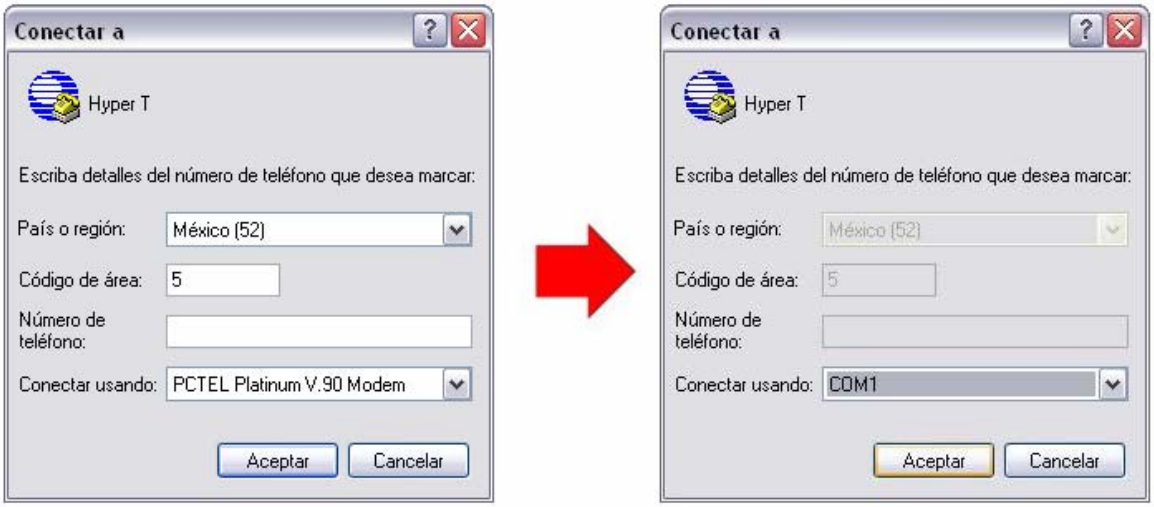


2. Ahora se abre el programa HyperTerminal que se encuentra en: Inicio\Programas\Accesorios\Comunicaciones

3. Se introduce un nombre a la conexión y se selecciona un icono



4. Al aparecer la siguiente ventana de designara el puerto que se va a utilizar, en este caso se ocupa el puerto serie de la PC por lo que se selecciona Com 1

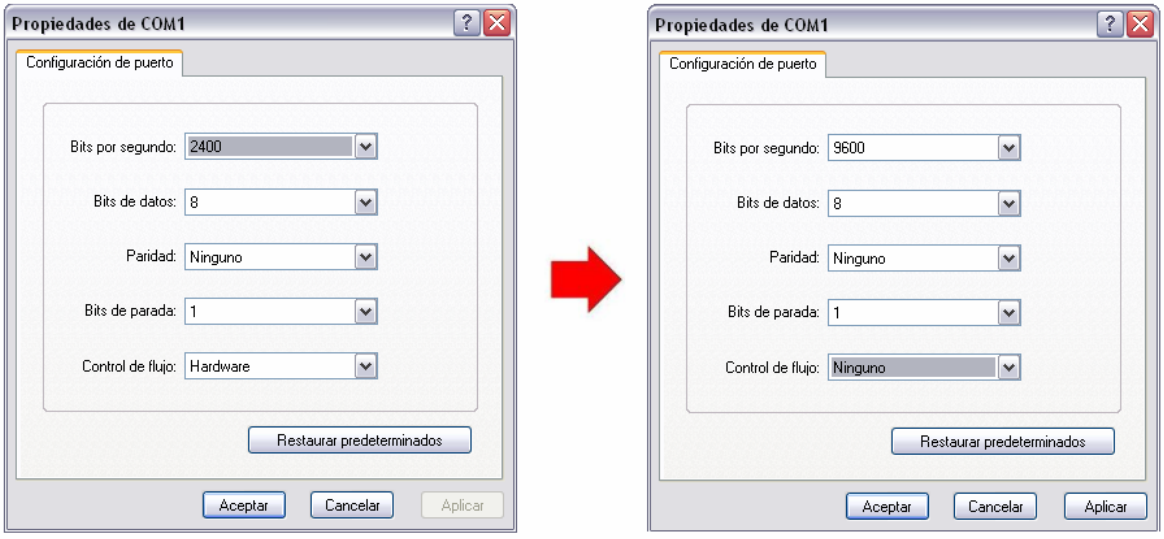


5. En la ventana propiedades de COM1, se configura el puerto COM 1 con los siguientes parámetros:

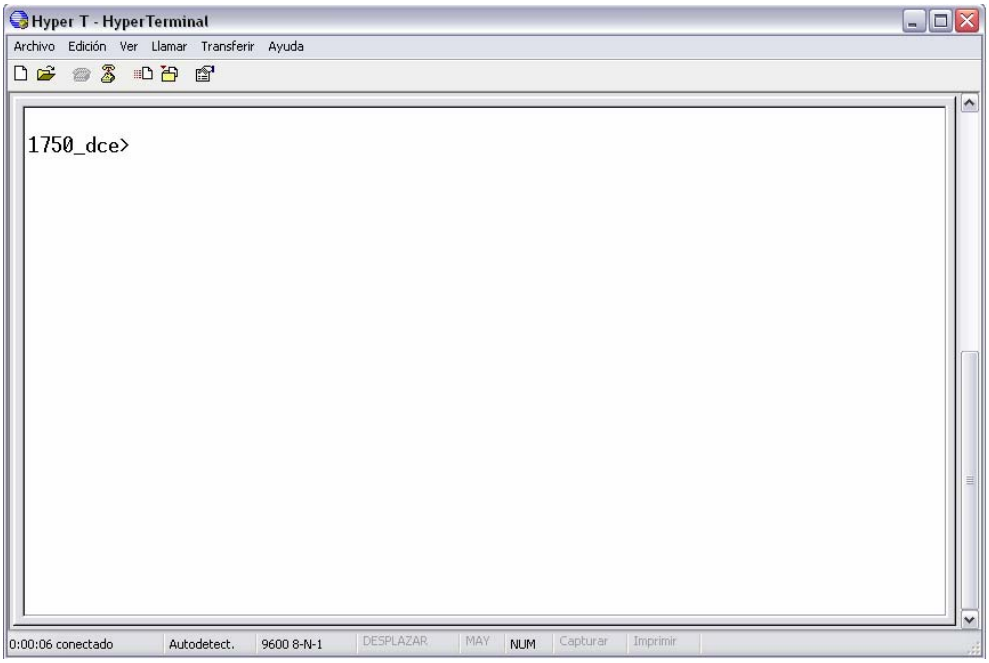
Bits por segundo: 9600
Bits de datos: 8
Paridad: Ninguna
Bits de parada: 1
Control de flujo: Ninguno

Nota: No todos los equipos manejan la velocidad de 9600, la velocidad de 9600 es la más utilizada en equipos Cisco no obstante puede ser incrementada o reducida dentro la línea de comando para de la línea consola.

Ambas velocidades deben coincidir (tanto del Router como la PC) de lo contrario no se podrá acceder a la interfaz de línea de comandos del Router, la velocidad del puerto consola viene especificada en el manual de instalación e incluso en algunos modelos esta grabado en el mismo chasis del equipo



6. Si todo ha sido configurado correctamente, aparecerá una ventana en blanco y al presionar Intro, se deberá desplegar un mensaje o un texto en la pantalla, de lo contrario se debe verificar antes que nada el cable de interconexión, como segundo punto se tiene que consultar el manual de instalación para determinar la velocidad a la cual esta configurado el puerto, si la velocidad coincide y persiste el problema es posible que el error radique en el puerto seleccionado en la PC por lo que solo es necesario cambiar el puerto Com 1 a Com 2 u otro que este disponible, en el ultimo de los casos el error se debe a que el puerto consola del router se encuentra dañado por lo que es necesario conectarse al puerto auxiliar del router.



2.4. Configuración usando el modo setup

Una de las rutinas de configuración inicial es el modo setup (configuración inicial). El propósito principal del modo de configuración inicial (setup) es realizar rápidamente una configuración mínima para cualquier router que no pueda obtener su configuración de alguna otra fuente.

Muchos de los indicadores en el diálogo de configuración del sistema del comando **setup** presentan respuestas por defecto entre corchetes **[ ]** al lado de la pregunta. Presione la tecla Retorno para usar esos valores por defecto. Si el sistema se ha configurado anteriormente, los valores por defecto que aparecen serán los valores actualmente configurados. Si se está configurando el sistema por primera vez, se suministran los valores de fábrica. Si no hay ningún valor por defecto de fábrica, como ocurre, por ejemplo, con las contraseñas, no aparece nada después del signo de pregunta **[?]** Durante el proceso de configuración inicial se puede presionar Control+C en cualquier momento para interrumpir el proceso y comenzar de nuevo. Una vez terminada la configuración inicial, todas las interfaces quedan administrativamente cerradas (shutdown).

```
        --- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: y
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
```

Si se selecciona el asistente de configuración básica solo se podrá configurar una de las interfaces del router, en este caso la FastEthernet o la Serial, en este

ejemplo no se utilizara el asistente de configuración básica dado a que se desea configurar ambas interfaces del router por lo que se le tecleo la palabra NO

Configuring global parameters:
Enter host name [Router]: FES_A

A continuación pide un nombre para el router, cualquier nombre, palabra o carácter es valido siempre y cuando este no tenga espacios, en caso de no poner nada se establecerá por defecto la palabra o caracteres contenidos en los corchetes

El siguiente punto es establecer las contraseñas, la primer contraseña que pide es el enable secret que tiene la principal característica de ser encriptada y es requerida para poder acceder al modo privilegiado desde cualquier puerto del router

La segunda contraseña requerida es el enable password, el enable password es una contraseña no encriptada por lo que al desplegar la configuración del equipo esta aparecerá tal cual fue introducida. La contraseña de enable password solo será pedida por el router para acceder al modo privilegiado desde cualquier puerto del router siempre y cuando no exista una contraseña enable secret previamente configurada

Por ultimo en cuanto las contraseñas, queda la clave para la terminal virtual que será requerida para entrar al modo usuario del router, este tipo de contraseña en caso de ser establecida, no será requerida para usuarios que se conecten en los puertos consola o auxiliar del router solo aplica para los que están conectados vía remota a través de cualquiera de las interfaces serial, ethernet, isdn, o cualquier otra

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: aragon

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: fesa

The virtual terminal password is used to protect
access to the router over a network interface.
Enter virtual terminal password: unam

A continuación se habilitaran los protocolos de enrutamiento, para este caso se utilizara RIP

Configure SNMP Network Management? [yes]: y
Community string [public]:
Configure IP? [yes]: y
Configure IGRP routing? [yes]: n
Configure RIP routing? [no]: y
Configure bridging? [no]:

Una vez configurados los protocolos de enrutamiento, siguen las interfaces, en la interfaz FastEthernet los parámetros que son requeridos son el tipo de tecnología Ethernet a conectar en este caso viene por defecto 100 Base TX, la siguiente pregunta es si va operar en full duplex (YES) o semi duplex (NO) (Se elegirá full duplex o semi duplex en función del equipo a conectar en la interfaz), por ultimo el

asistente preguntara si se desea introducir una dirección IP a la interfaz en caso de decir que YES se deberá introducir una dirección IP con su respectiva máscara

```
Configuring interface parameters:

Do you want to configure FastEthernet0  interface? [no]: y
  Use the 100 Base-TX (RJ-45) connector? [yes]:
  Operate in full-duplex mode? [no]: y
  Configure IP on this interface? [no]: y
  IP address for this interface: 10.10.10.1
  Subnet mask for this interface [255.0.0.0]:
  Class A network is 10.0.0.0, 8 subnet bits; mask is /8
```

Ahora se deberá configurar la interfaz Serial, para lo cual se deben conocer previamente los parámetros del proveedor de servicios como el encapsulamiento, el ancho de banda y la dirección IP asignada con su respectiva máscara

```
Do you want to configure Serial0  interface? [no]: y
  Some supported encapsulations are
        ppp/hdlc/frame-relay/lapb/x25/atm-dxi/smds
  Choose encapsulation type [hdlc]: ppp

  Serial interface needs clock rate to be set in dce mode.
  The following clock rates are supported on the serial interface.
        1200, 2400, 4800, 9600, 14400, 19200
        28800, 32000, 38400, 56000, 57600, 64000
        72000, 115200, 125000, 128000, 148000, 500000
        800000, 1000000, 1300000, 2000000, 4000000, 8000000

  choose speed from above : [2000000]: 128000
```

Configure IP on this interface? [no]: y
Configure IP unnumbered on this interface? [no]:
IP address for this interface: 196.46.25.1
Subnet mask for this interface [255.255.255.0] :
Class C network is 196.46.25.0, 24 subnet bits; mask is /24

Al completarse el proceso de configuración en el modo de configuración inicial (setup), en la pantalla aparece la configuración que se acaba de crear.

```
hostname FES_A
enable secret 5 $1$kiAY$ptGduzvqahVLDLPhkcED/0
enable password unam
line vty 0 4
password aragon
snmp-server community public
ip routing
no bridge 1
interface FastEthernet0
no shutdown
media-type 100BaseX
full-duplex
ip address 10.10.10.1 255.0.0.0
interface Serial0
no shutdown
encapsulation ppp
clock rate 128000
ip address 196.46.25.1 255.255.255.0
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
router rip
redistribute connected
```

```
network 10.0.0.0
network 196.46.25.0
end
```

Ahora hay a escoger tres opciones una es si se desea regresar al modo usuario sin guardar la configuración [0], con la numero [1] se vuelve a comenzar con la configuración a partir de *hostname* y con la opción [2] guardamos la configuración previamente desplegada

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.
Enter your selection [2]:
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.
Press RETURN to get started!
FES_A>
```

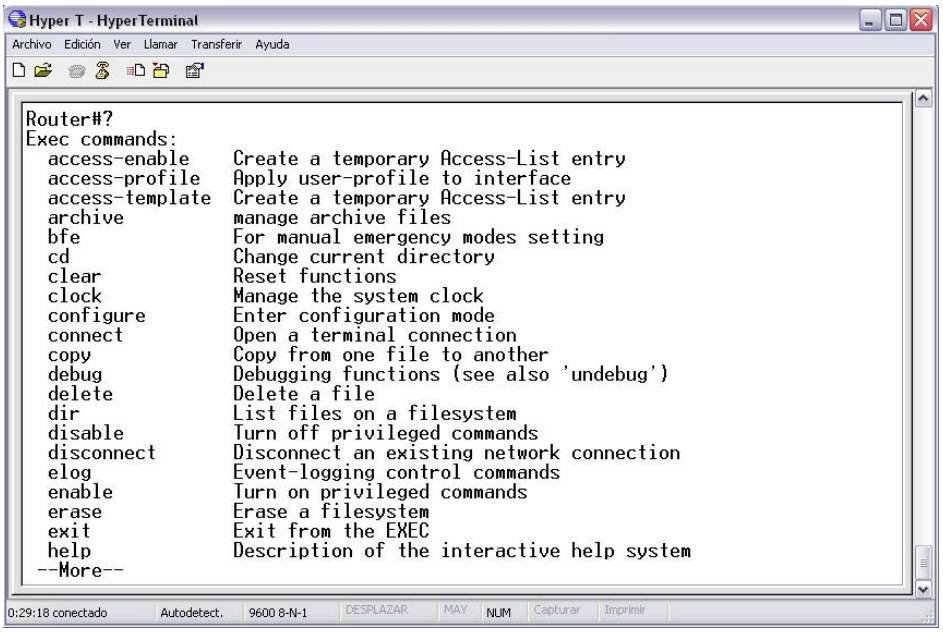
La principal desventaja que tiene este modo de configuración radica en que no se programan todos los parámetros necesarios para que el router trabaje satisfactoriamente como los protocolos de ruteo, rutas estáticas o subinterfaces, además debemos habilitar las interfaces mediante el modo de configuración global, porque, como ya se menciono anteriormente las interfaces quedan administrativamente cerradas

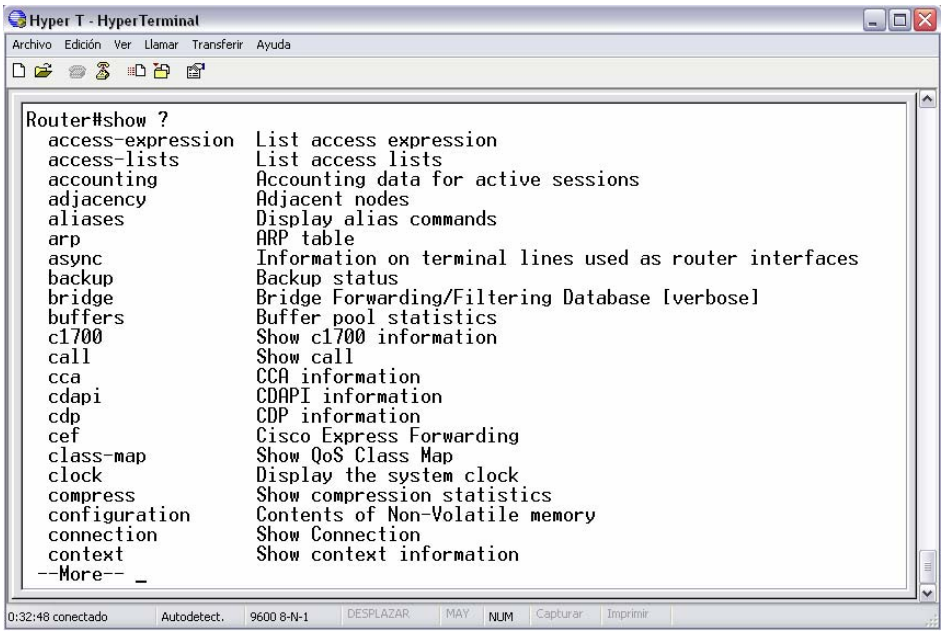
2.5. Configuración básica de un router Cisco

Antes de iniciar con la configuración del router se deben conocer algunas instrucciones especiales y combinaciones de teclas que facilitaran el uso de la interfaz de la línea de comandos del router.

Orden “?”

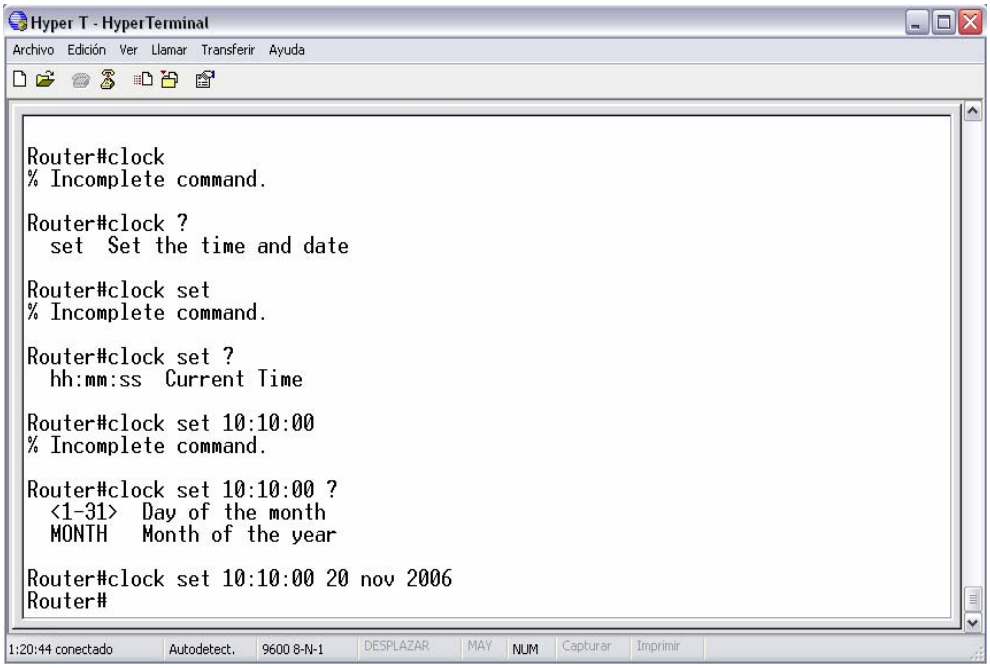
Cuando se escribe un signo de interrogación (?) en el indicador de en cualquiera de los modos del router excepto el modo setup, aparece una lista útil de comandos de uso común. Observe el "--More--" (Más) que aparece en la parte inferior de la pantalla de muestra. La pantalla muestra 22 líneas por vez. De modo que a veces se obtiene el indicador -- More -- en la parte inferior de la pantalla. Esto indica que hay múltiples pantallas disponibles como resultado; es decir, que hay más comandos disponibles. Aquí, o en cualquier otra parte del software Cisco IOS, siempre que aparece un indicador --More--, se puede ver la siguiente pantalla disponible presionando la barra espaciadora. Para visualizar solamente la siguiente línea, se presiona la tecla Retorno (o en algunos teclados la tecla Intro). Al presionar cualquier tecla (excepto intro, retorno y la barra espaciadora) se vuelve al indicador.



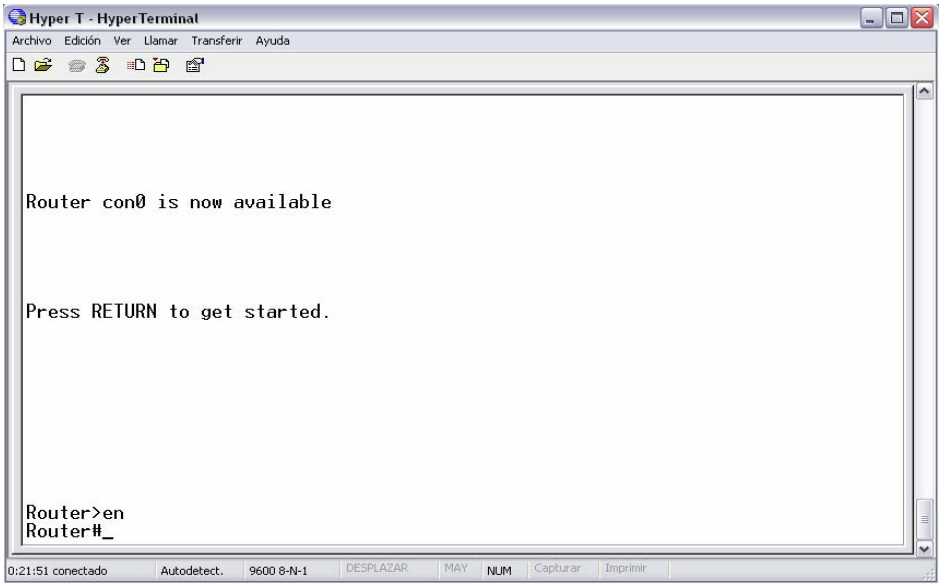


Nota: El resultado que aparece en pantalla varía, según el nivel del software Cisco IOS y la configuración del router.

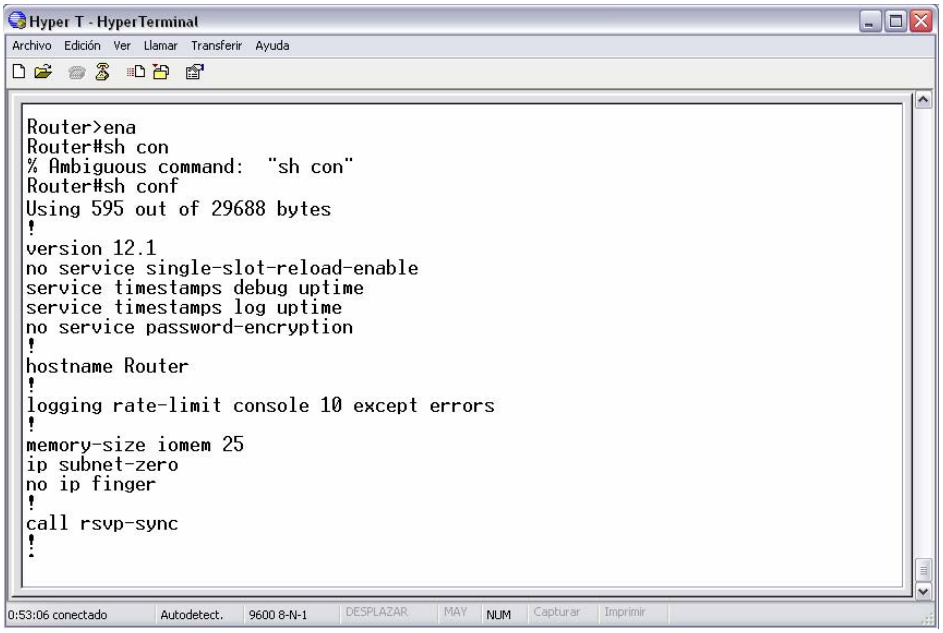
Como ejemplo se desea configurar el reloj, Si no sabe cuál es el comando que debe usar use el comando “?” para verificar la sintaxis de la configuración del reloj, como se puede observar el comando a utilizar es *clock,* al escribir solo la instrucción *clock* en la línea de comandos marcara la advertencia de comando incompleto, para esto nuevamente se tecleara la misma instrucción pero ahora seguido del comando “?”, al utilizar este ultimo comando, se desplegara en la pantalla una lista con el o los comandos disponibles para la función anterior en este caso *clock,* como resultado aparecerá la orden *set*. Al introducir la instrucción *clock set* volverá a aparecer el mensaje de comando incompleto, nuevamente se hará uso del comando “?”, y así se seguirá hasta que la instrucción sea completada



El sistema operativo de Cisco IOS, también permite el uso de abreviaciones en la mayoría de los comandos, como por ejemplo, para acceder al modo privilegiado en lugar de escribir *enable*, solo basta con teclear *en*



No todas la abreviaciones son siempre aceptadas, esto se debe en la mayoría de los casos a que existe más de un comando que empieza con las primeras letras que se acaban de introducir o el comando a ejecutar es muy viejo y ya no es aceptado por el IOS, en caso de existir más de un comando que tenga las mismas letras al principio basta con introducir unas cuantas letras más o poner la palabra completa.



En lo que corresponde a las combinaciones de teclas, la interfaz del usuario incluye un modo de edición mejorado que proporciona un conjunto de funciones de edición que permite editar una línea de comando mientras se escribe. Las secuencias de teclas indicadas en la siguiente tabla son para desplazar el cursor en la línea de comando para realizar correcciones o cambios.

Comando	Descripción
Control + A	Permite desplazarse hasta el principio de la línea de comando
Control + B	Permite desplazarse un carácter hacia atrás
Control + E	Permite desplazarse hasta el final de la línea de comando

Control + F	Permite desplazarse un carácter hacia adelante
Esc + B	Permite desplazarse una palabra hacia atrás
Esc + F	Permite desplazarse una palabra hacia adelante

Aunque el modo de edición mejorado se activa automáticamente en la versión actual del software, se puede desactivar si tiene guiones escritos que no interactúan bien mientras la edición mejorada se encuentra activada. Para desactivar el modo de edición mejorado, se escribe "terminal no editing" en el indicador de modo privilegiado.

El conjunto de comandos de edición incluye una función de desplazamiento horizontal para comandos que ocupen más de una línea en la pantalla. Cuando el cursor alcanza el margen derecho, la línea de comando se desplaza 10 espacios hacia la izquierda. Entonces no se pueden ver los primeros 10 caracteres de la línea, pero se puede desplazar hacia atrás y verificar la sintaxis al principio del comando. Para desplazarse hacia atrás, presione Control-B o la tecla flecha izquierda repetidas veces hasta llegar al principio del comando, o presione Control-A para volver directamente al principio de la línea.

La interfaz del usuario proporciona un historial, o registro, de los comandos que se han introducido. Esta función es particularmente útil para volver a introducir comandos o entradas largos o complejos. La función de historial de comandos permite completar las siguientes tareas:

- Establecer el tamaño del búfer de historial de comandos.
- Volver a introducir comandos.
- Desactivar la función de historial de comandos.

Por defecto, el historial de comandos se activa y el sistema registra 10 líneas de comandos en el búfer de historial. Para cambiar la cantidad de líneas de comando

que el sistema registra durante una sesión de terminal, se debe usar el comando *terminal history size* (tamaño de historial de terminal) o el comando *history size*. La cantidad máxima de comandos es 256, cabe señalar que búfer del historial de comandos ocupa espacio en la memoria ram del router por lo que no es aconsejable registrar más de 10 líneas

Para volver a introducir comandos que se encuentran en el búfer de historial, a partir del comando más reciente, presionar Control + P o la tecla flecha arriba repetidas veces para volver a introducir comandos sucesivamente más antiguos. Para volver a los comandos más recientes en el búfer de historial, después de volver a introducir comandos con Control + P o la tecla flecha arriba, presionar Control-N o la tecla flecha abajo repetidas veces para volver a introducir comandos sucesivamente más recientes.

Al escribir comandos, como abreviatura se pueden introducir los caracteres exclusivos del comando, presionar la tecla Tab, y la interfaz termina el comando. Las letras exclusivas identifican el comando, la tecla Tab simplemente reconoce visualmente que el router ha comprendido el comando específico que se desea introducir.

En la mayoría de los computadores también hay funciones adicionales de selección y copia. Se puede copiar una cadena de comandos anterior, y luego pegarla o insertarla como la entrada de comandos actual, y presionar Retorno. Se puede usar Control-Z para salir del modo de configuración.

Comando	Descripción
Router> show history	Muestra los últimos 10 comandos introducidos
Router> terminal history size number-of-lines	Establece el tamaño del búfer de comando

Router> no terminal editing	Inhabilita las funciones de edición avanzada
Router> terminal editing	Vuelve a habilitar las funciones de edición avanzada
Control + P o tecla flecha arriba	Hace aparecer nuevamente el ultimo comando introducido
Control + N o tecla flecha abajo	Hace aparecer nuevamente el comando más reciente
Tab	Completa la instrucción
Control + Z o Control + C	Sale del modo de configuración global para regresar al modo privilegiado

Existe una gran variedad de parámetros a configurar en un router, en este ejemplo, solo se configuraran los parámetros mínimos para que pueda funcionar. Antes de empezar, al prender un router Cisco nuevo o sin configuración inicial como ya se vio anteriormente, preguntara si se desea programar la configuración inicial para lo cual teclear **N** (no).

```
        --- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]:n
```

Una vez hecho esto en la pantalla se deberá iniciar en el modo usuario al presionar Intro:

```
Router>
```

En estos momentos el router se encuentra en el modo usuario, ahora se debe pasar al modo privilegiado para lo cual se ocupa el comando *enable* como ya se vio anteriormente

```
Router>enable
Router#
```

El siguiente paso es entrar al modo de configuración global

```
Router#configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

En el modo de configuración global se pueden configurar todos los parámetros del router, para empezar se configurara el nombre de host del router como FES A, cabe mencionar que el nombre que tecleamos deberá ir sin espacios, de lo contrario marcara un error.

```
Router(config)#
Router(config)#hostname FES A
                        ^
% Invalid input detected at '^' marker.
Router(config)#hostname FES_A
FES_A (config)#
```

Como se puede ver en el ejemplo, el router cambió su nombre de *Router* a *FES_A*. Ahora se introducirá una contraseña para que no cualquiera pueda tener acceso al modo privilegiado

```
FES_A(config)#enable password cisco
FES_A(config)#
```

Al no mostrarnos mensajes de error, ni solicitarnos más parámetros de la instrucción y pedirnos otro comando en la siguiente línea, se puede decir que el comando *enable password cisco* ha sido aceptado por el router, es decir, al introducir cualquier comando de configuración, al presionar Intro deberá pedir otro comando de lo contrario, la instrucción que se capturo está mal escrita o incompleta y no es aceptada por el router.

Volviendo al ejemplo, ahora se configurara la línea de consola, esto es para tener aún mayor seguridad sobre todo aquel que acceda al router conectándose

mediante el puerto consola ya que se le solicitara una contraseña para poder acceder al modo usuario

```
FES_A(config)#line console 0
FES_A(config-line)#login
FES_A(config-line)#password cisco1
FES_A(config-line)#exit
FES_A(config)#
```

El siguiente paso es configurar la línea virtual, la cual sirve para acceder al router de forma remota, las instrucciones son muy semejantes a las que se usaron en el puerto consola, en caso de no configurar la línea virtual ni la contraseña para acceder al modo privilegiado ningún host remoto tendrá acceso a la interfaz de línea de comandos del router

```
FES_A(config)#line vty 0 4
FES_A(config-line)#login
FES_A(config-line)#password cisco2
FES_A(config-line)#exit
```

Del mismo modo que en la configuración del puerto consola, si alguien quiere entrar al router por medio de una línea virtual, el router le pedirá la contraseña previamente definida para líneas virtuales que en este caso es cisco2, la cual le dará acceso al modo usuario.

Hasta el momento solo se han activado algunos comandos de seguridad para que no cualquiera pueda modificar la configuración del router, ahora se procederá a programar las interfaces, cabe señalar las interfaces que a continuación se programaran no son las únicas que se pueden encontrar en un router, pero si las más comunes

```
FES_A(config)#interface serial 0
FES_A(config-if)#ip address 195.65.23.1 255.255.255.0
```

```
FES_A(config-if)# bandwidth 128000
FES_A(config-if)#no shutdown
02:01:00: %LINK-3-UPDOWN: Interface Serial0, changed state to up
FES_A(config-if)#exit
```

En la primer línea, el comando *interface serial X* sirve para programar la interfaz serial numero X del router, en la segunda línea se configura una dirección IP con una mascara al puerto que se programo que en este caso es el puerto serial 0, enseguida se indica el acho de banda para dicha interfaz y por último el comando *no shutdown* habilita la interfaz, al darla de alta, aparecerá un mensaje el cual indica el cambio que ha sufrido la interfaz.

En el ejemplo anterior no se configuro algún tipo de encapsulación en especial por lo que el router adoptara una encapsulación hdlc (High Data Link Control - Control de enlace de datos de alto nivel) por default, existen más tipos de encapsulamiento, entre los más usados se encuentran ppp (Point-to-Point protocol) y frame-relay

Ahora se configurara el puerto FastEthernet

```
Router_A(config)#interface FastEthernet 0
FES_A(config-if)#ip address 195.65.28.1 255.255.255.0
FES_A(config-if)#no shutdown
02:01:00: %LINK-3-UPDOWN: Interface FastEthernet0, changed state to up
FES_A(config-if)#exit
```

La configuración del puerto FastEthernet es muy parecida a la del puerto serial en este ejemplo, aunque cabe decir que normalmente la configuración de la interfaz serial llega a ser un poco más compleja ya que se le suele añadir una encapsulación y subinterfaces con el fin de optimizar el ancho de banda, los parámetros de la interfaz serial (las direcciones ip, el tipo de encapsulamiento y el

ancho de banda entre otros), son definidos previamente por el proveedor de servicios

Una vez definidas las direcciones ip de las interfaces del router, el siguiente paso es declarar el protocolo de enrutamiento a utilizar, existen dos clases de enrutamiento el dinámico y el estático cada una tiene sus ventajas y desventajas, en este ejemplo se programara el enrutamiento dinámico RIP (Routing Information Protocol - Protocolo de información de enrutamiento)

```
FES_A(config)#router rip
FES_A(config-router)#network 195.65.23.0
FES_A(config-router)#network 195.65.28.0
FES_A(config-router)#exit
```

A primera instancia se utilizara el comando *router rip*, como se puede ver la línea de comando cambio de FES_A(config)# a FES_A(config-router)#, y por último mediante la declaración *network* se introducen las direcciones ip (únicamente las que corresponden a las redes, es decir, terminación 0) de las interfaces del router.

El siguiente paso es opcional el cual consiste en configurar la tabla ip host lookup.

```
FES_A(config)#ip host Router_A 195.65.23.1 195.65.28.1
FES_A(config)#ip host Router_B 195.65.23.2 195.65.25.1
FES_A(config)#ip host Router_C 195.65.25.2 195.65.26.1
```

Esta instrucción sirve para darle un tipo de nombre DNS a las direcciones 195.65.23.1 y 195.65.28.1 como Router_A, lo mismo pasa con las direcciones para Router_B y Router_C

Por ultimo antes de guardar los cambios que se han hecho, se debe revisar la configuración, esto se logra volviendo a modo privilegiado y ejecutando el comando *show running-config* (sh run).

```
FES_A(config)#show running-config
```

Finalmente se guarda la configuración en el modo privilegiado mediante alguno de los comandos *write* ó *copy running-config startup-config*

FES_A#write

2.6. Recuperación de contraseñas

Uno de los problemas más frecuentes y engorrosos cuando se trabaja con routers es la pérdida o la alteración de contraseñas, algo que efectivamente bloquea el acceso al router.

Habrá circunstancias en las cuales la contraseña para un router deberá reemplazarse. Es posible que la contraseña se haya olvidado o que el administrador anterior haya dejado de trabajar en la empresa propietaria del router. La técnica descrita requiere acceso físico al router para poder conectarle directamente el cable de consola. Cómo esta técnica es muy conocida, resulta imprescindible que los routers se encuentren en una ubicación segura, con acceso físico limitado

Antes de empezar, se debe saber en que registro se encuentra la configuración mediante el comando *show versión*, el cual se ejecutará desde modo usuario, normalmente la configuración se encuentra en el registro 0x2102

Es necesario poner el equipo en el modo *ronmon>* y esto es por medio del reinicio del equipo y al oprimir las teclas *control* + *pause* o *control* + *break* recién se encienda el router. Apareciendo el prom de la siguiente manera:

monitor: command "boot" aborted due to user interrupt

rommon 1 >

Ahora se tendrá que cambiar el registro de arranque de 0x2102 a 0x2142 (si el registro de configuración se encuentra en el registro 0x2142, se cambia al 0x2102) y reiniciar el router mediante el comando *reset* o simplemente apagando y volviendo a encender el router

```
rommon 1 > confreg 0x2142
rommon 2 > reset
```

El router solo cargará el IOS, la configuración anterior no será tomada en cuenta, por lo que al encender completamente preguntara si se desea empezar con la configuración inicial, a lo cual se responde que no

```
        --- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: n
```

El router enviara iniciara en el modo usuario, en estos momentos se entrará al modo de configuración global y para ejecutar el comando ***copy*** *startup-config running-config,* el cual copia la configuración de inicio en la memoria ram

```
Router>enable
Router#copy startup-config running-config
Destination filename [running-config]?
618 bytes copied in 0.480 secs
FES_A#
```

El siguiente paso es ver la configuración con el comando *show run*, al desplegar la configuración el password para entrar al modo usuario será mostrado al igual que la contraseña del modo privilegiado siempre y cuando no estén encriptados.

```
hostname FES_A
logging rate-limit console 10 except errors
enable password aragon
```

Si la contraseña fue encriptada aparecerá como una secuencia de caracteres sin sentido

```
hostname FES_A
logging rate-limit console 10 except errors
enable secret 5 $1$p3M.$bYh4zAV.51MQaPM7DS9gS0
```

Si la contraseña fue encriptada definitivamente tendrá que ser cambiada o eliminada

```
FES_A#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
FES_A(config)#enable secret aragon
```

Ahora se debe regresar al registro que tenia desde un principio de lo contrario cada vez que se reinicie el router este no cargara automáticamente la configuración, para no tener que volver a entrar a *ronmon>* se ejecuta el comando *config-register 0x2102* en el modo de configuración global donde 0x2102 es el registro en el cual el router iniciará la próxima vez que sea encendido o reiniciado.

```
FES_A(config)#config-register 0x2102
FES_A(config)#
```

Por ultimo se guardan los cambios realizados para esto se emplea el comando *copy* running-config startup-config o write para que copie la configuración de la ram a la nvram y finalmente para que el cambio de registro se efectúe se debe reiniciar el router

```
FES_A#copy running-config startup-config
FES_A#reload
```

Capitulo 3. Prevención de fallas en router Cisco

3.1 Seguridad

La seguridad está integrada en todas partes y con la ayuda de un enfoque de ciclo de vida de los servicios, las empresas pueden implementar, operar y optimizar la red de plataformas que defienden los procesos de negocio críticos contra el ataque y la desorganización, proteger la vida privada, y apoyar la formulación de políticas y controles de cumplimiento de la normativa.

Soluciones de seguridad a favor de la empresa

Desplegar un sólido, confiable, seguro Red. Cisco Self-Defending Network es una solución arquitectónica diseñada para la evolución del panorama de la seguridad.

A través de esta red como la plataforma mantiene a la gente y los activos de TI segura, la organización hace más resistentes y fiables, y permite el máximo impacto sobre las empresas de inversión en TI.

Soluciones

El control de las amenazas a la seguridad

La amenaza de Control de Cisco ofrece solución completa protección para su red a través de toda la red visibilidad, la simplificación de la política de control y sistema de protección proactiva.

Una parte de Cisco Self-Defending Network, la amenaza de Control de Cisco solución centraliza la política, configuración y gestión de eventos amenaza para:

- Proteger la red, servidores, puntos finales, y la información

- Regular el acceso a la red, aislar los sistemas infectados, evitar las intrusiones, y proteger los activos críticos para el negocio

- Contrarrestar el tráfico malicioso, como gusanos, virus y malware antes de que afecten a su negocio, a través de todos.

Amenaza para el control de puntos finales

Defender contra las amenazas más frecuentemente introducida por el uso de Internet, tales como virus, software espía y otro contenido malicioso que puede conducir a la pérdida de datos y degradan la productividad incluyen el agente de seguridad de Cisco para equipos de escritorio, Cisco ASA 5500 Series Appliances (Contenido de Seguridad Edition), Routers de Servicios Integrados, Cisco Intrusion Prevention Systems, y Cisco Network Admission Control

Control de amenazas para la infraestructura

Proteja su servidor de aplicaciones y la infraestructura contra ataques e intrusiones. Defender contra intentos internos y externos de penetrar o atacar los servidores y recursos de información mediante la aplicación y funcionamiento de las vulnerabilidades del sistema.

Amenaza de control para E-mail

Proteja su productividad empresarial, la disponibilidad de recursos, e información confidencial por correo electrónico de detener amenazas.

Seguridad en las comunicaciones

Garantizar la privacidad y la integridad de toda la información es vital para el negocio. A medida que su empresa utiliza la flexibilidad y la rentabilidad de Internet para ampliar su red de oficinas, teletrabajadores, clientes y socios, la seguridad es primordial. Mejorar la productividad, habilitar nuevas aplicaciones de negocio y mejorar la eficiencia de las empresas ayudan a cumplir con las regulaciones de privacidad de información

El Cisco Secure Communications solución es un conjunto de productos y servicios de seguridad del ciclo de vida que son un elemento esencial de la Cisco Self-Defending Network. Al incorporar la capacidad de garantizar que la red, los criterios de valoración, así como las aplicaciones y los mensajes, los sistemas de este enfoque basado en entrega global de seguridad de sus comunicaciones.

3.1.1 Ubicación del equipo

Los routers son equipos electrónicos muy delicados en cuanto a la temperatura y la humedad, es por eso que se debe tener un lugar donde la temperatura y la humedad estén controladas, además de estar aislado y libre de otras fuentes de calor.

Se le llama Site al área donde se encuentran los routers, y equipos como switches, servidores, access point, ups, y otros equipos, que hacen posible el correcto funcionamiento de una red de datos.

Se debe montar el router sobre un Rack y se recomienda colocarlo sobre una charola, para que no genere más calor, las condiciones del lugar deben ser con una temperatura entre 18 y 20 grados centígrados, y una humedad no mayor al 60%. Su alimentación debe estar aterrizada correctamente y respaldada por un no break o un ups.

Además debe situarse a una altura mayor a 1 metro y menor a 2.5 metros, esto para poder visualizar las alarmas q pueda presentar o el correcto funcionamiento del equipo.

3.1.2. Listas de control de acceso

Los administradores de red deben buscar maneras de impedir el acceso no autorizado a la red, permitiendo por otro lado el acceso autorizado. Aunque las herramientas de seguridad, como las contraseñas, equipos de callback y

dispositivos de seguridad física, son de ayuda, a menudo carecen de la flexibilidad del filtrado básico de tráfico, y los controles específicos que la mayoría de los administradores prefieren. Por ejemplo, un administrador de red puede permitir que los usuarios tengan acceso a Internet, pero puede no considerar conveniente que los usuarios externos hagan telnet a la LAN.

Los routers proporcionan capacidades básicas de filtrado de tráfico, como bloqueo del tráfico de Internet, con *listas de control de acceso* (ACL – Access control list). Una ACL es una colección secuencial de sentencias de permiso o rechazo que se aplican a direcciones o protocolos de capa superior

3.1.2.1. Definición de una ACL

Las ACL son listas de instrucciones que se aplican a una interfaz del router. Estas listas indican al router qué tipos de paquetes se deben aceptar y qué tipos de paquetes se deben denegar. La aceptación y rechazo se pueden basar en ciertas especificaciones, como dirección origen, dirección destino y número de puerto. Las ACL permiten administrar el tráfico y examinar paquetes específicos, aplicando la ACL a una interfaz del router.

Una de las principales ventajas de las ACL es que se pueden crear para todos los protocolos enrutados de red, como el Protocolo Internet (IP), el Intercambio de Paquetes de Internetwork (IPX) y appletalk, para filtrar los paquetes a medida que pasan por un router.

Las ACL se pueden configurar en el router para controlar el acceso a una red o subred. Las ACL filtran el tráfico de red controlando si los paquetes enrutados se envían o se bloquean en las interfaces del router. El router examina cada paquete para determinar si se debe enviar o descartar, según las condiciones especificadas en la ACL. Entre las condiciones de las ACL se pueden incluir la

dirección origen o destino del tráfico, el protocolo de capa superior, u otra información

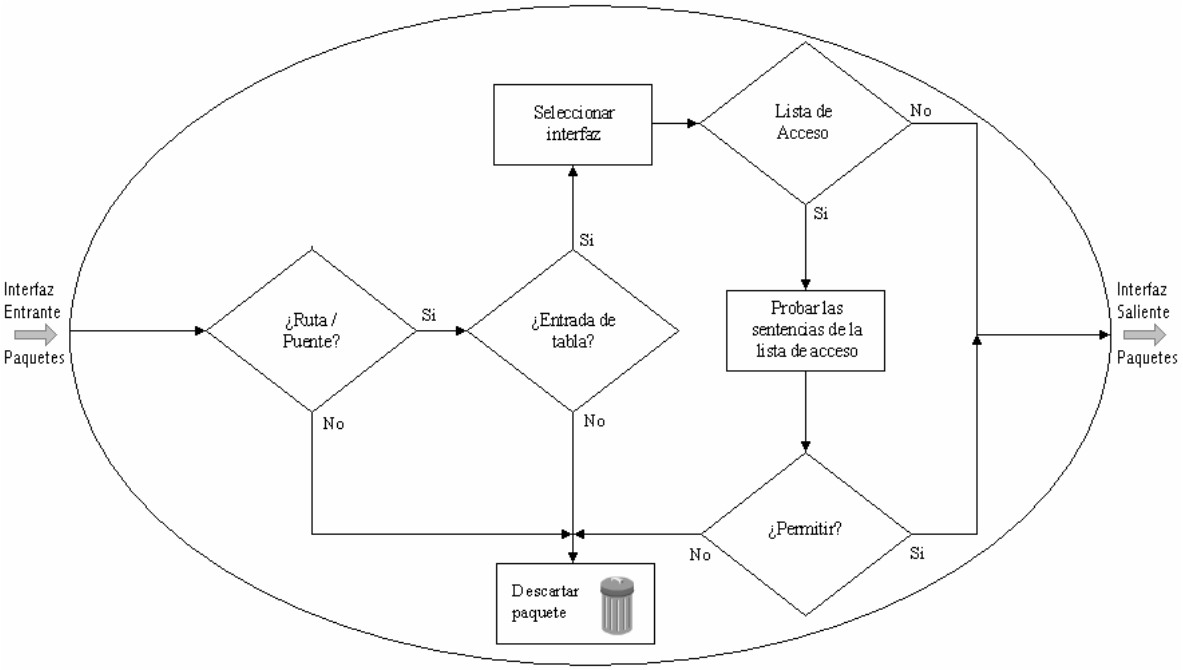
Concretamente, las ACL son una serie de declaraciones condicionales que pueden restringir la entrada o salida de paquetes desde una interconexión a un router de acuerdo con una serie de criterios. Cada ACL se lee en el orden en que viene incluida, lo que significa que los paquetes que entren a una determinada interfaz de router se comparan con los criterios de listado de arriba abajo. Los paquetes que se rechazan se descartan, por el contrario los paquetes que se aceptan son enviados como si no existiera la ACL.

Una ACL es un grupo de sentencias que define cómo los paquetes:

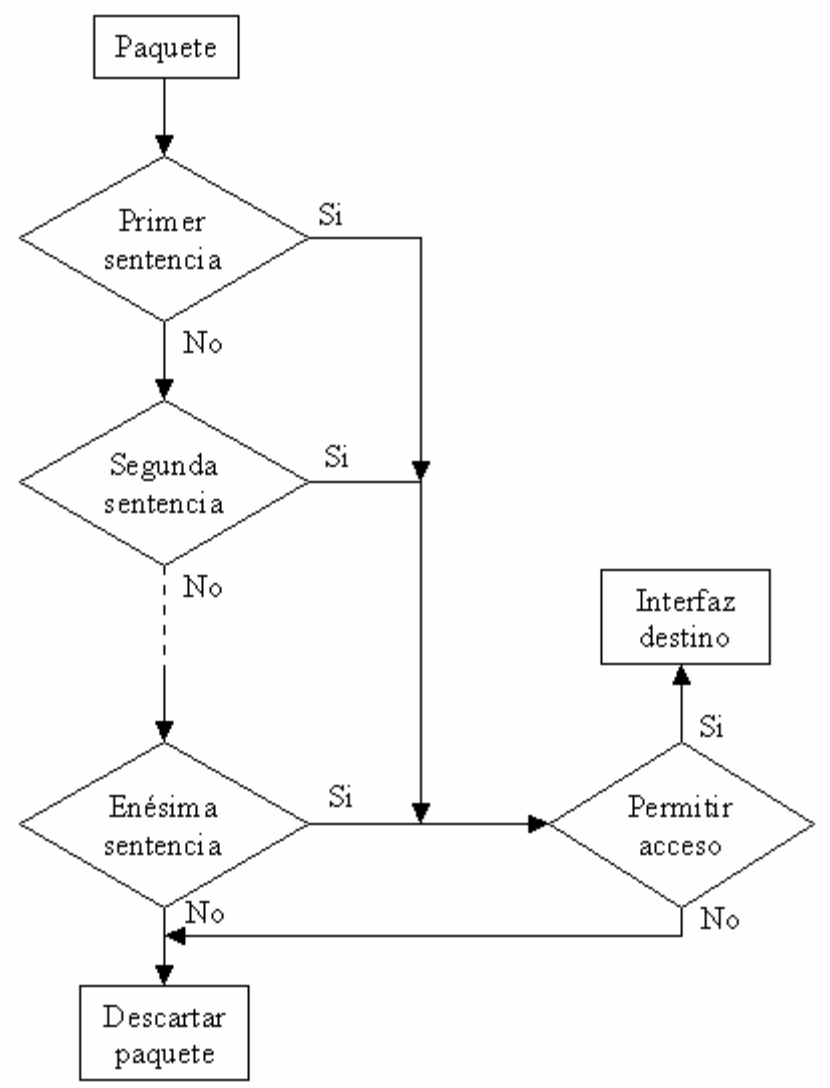
- Entran a las interfaces
- Se reenvían a través del router
- Salen de las interfaces del router

El principio del proceso de comunicaciones es el mismo, ya sea que las ACL se usen o no. Cuando un paquete entra en una interfaz, el router verifica si un paquete es enrutable o puenteable. Ahora, el router verifica si la interfaz entrante tiene una ACL. Si existe, ahora se verifica si el paquete cumple o no las condiciones de la lista. Si el paquete es permitido, entonces se compara con las entradas de tabla de enrutamiento para determinar la interfaz destino.

A continuación, el router verifica si la interfaz destino *tiene* una ACL. Si no la tiene, el paquete puede ser enviado directamente a la interfaz destino; por ejemplo, si usa *F0*, que no tiene ACL, el paquete usa *F0* directamente.



Si un paquete que entra al router no cumple con la primera declaración de la ACL, pasa a compararse con la siguiente declaración y así sucesivamente hasta la ultima declaración programada, si ninguno de los criterios de declaración se cumple el paquete es descartado, en caso contrario, una vez que el paquete coincide con alguna de las declaraciones, es nuevamente comparado pero ahora con las sentencias *permit* y *deny*, con las cuales será reexpedido a una interfaz del router o descartado respectivamente.



Las listas de acceso permiten que un administrador especifique condiciones que determinan la manera en que un router controlará el flujo de tráfico. Las listas de acceso se utilizan para permitir o denegar tráfico a través de una interfaz de router. Los dos tipos de listas de acceso son los siguientes:

3.1.2.2. ACL Estándar

Las listas de acceso estándar para IP verifican la dirección origen de los paquetes que se pueden enrutar. El resultado permite o deniega el resultado para todo un conjunto de protocolo, según las direcciones de red/subred/host.

Por ejemplo, se verifican los paquetes que vienen de E0 por dirección y protocolo. Si se permiten, los paquetes salen a través de S0, que se agrupa en la lista de acceso.

Si los paquetes son denegados por la lista de acceso estándar, todos los paquetes para esa categoría se descartan.

3.1.2.3. ACL Extendida

Las listas de acceso extendidas verifican las direcciones origen y destino de los paquetes. También pueden verificar protocolos, números de puerto y otros parámetros específicos. Esto ofrece a los administradores mayor flexibilidad para describir las verificaciones que debe realizar la lista de acceso. Se pueden permitir o denegar paquetes según su origen o destino.

Las listas de acceso extendidas también otorgan permisos y rechazos de manera menos uniforme. Por ejemplo, pueden permitir el tráfico de correo electrónico desde E0 a destinos S0 específicos, denegando al mismo tiempo conexiones remotas o transferencias de archivos.

Hay muchas razones para crear ACL. Por ejemplo, las ACL se pueden usar para:

- Limitar el tráfico de red y mejorar el desempeño de la red. Por ejemplo, las ACL pueden designar ciertos paquetes para que un router los procese antes de procesar otro tipo de tráfico, según el protocolo. Esto se denomina colocación en cola, que asegura que los routers no procesarán paquetes que no son necesarios. Como resultado, la colocación en cola limita el tráfico de red y reduce la congestión.

- Brindar control de flujo de tráfico. Por ejemplo, las ACL pueden restringir o reducir el contenido de las actualizaciones de enrutamiento. Estas restricciones se usan para limitar la propagación de la información acerca de redes específicas por toda la red.

- Proporcionar un nivel básico de seguridad para el acceso a la red. Por ejemplo, las ACL pueden permitir que un host acceda a una parte de la red y evitar que otro acceda a la misma área. Al Host A se le permite el acceso a la red de Recursos Humanos, y al Host B se le deniega el acceso a dicha red. Si no se configuran ACL en su router, todos los paquetes que pasan a través del router supuestamente tendrían acceso permitido a todas las partes de la red.

- Se debe decidir qué tipos de tráfico se envían o bloquean en las interfaces del router. Por ejemplo, se puede permitir que se enrute el tráfico de correo electrónico, pero bloquear al mismo tiempo todo el tráfico de telnet.

Si se crea una sentencia de condición que permita todo el tráfico, no se verificará ninguna sentencia agregada más adelante. Si necesita sentencias adicionales, en una ACL estándar o extendida se debe eliminar la ACL y volver a crearla con las nuevas sentencias de condiciones. Es por este motivo que es una buena idea editar una configuración de router en un PC con un editor de texto y luego solo pegarla mediante hyperterminal o utilizar un servidor de Protocolo de Transferencia de Archivos Trivial (TFTP).

Las listas de acceso pueden controlar el tráfico para la mayoría de los protocolos en un router Cisco. La siguiente tabla muestra los protocolos e intervalos numéricos de los tipos de lista de acceso.

IP estándar	1 – 99
IP extendida	100 – 199
IPX estándar	800 – 899
IPX extendida	1000 – 1099
Apple Talk	600 - 699

Un administrador introduce un número dentro del intervalo numérico del protocolo como el primer argumento de la sentencia de la lista de acceso global. El router identifica cuál es el software de lista de acceso que se debe usar según esta entrada numerada. La lista de acceso prueba las condiciones siguientes como argumentos. Estos argumentos especifican las pruebas según las reglas del conjunto de protocolo dado. El significado o validez del esquema de identificación estándar y extendido para las listas de acceso varía por protocolo.

Muchas listas de acceso son posibles para un protocolo. Se selecciona un número diferente del intervalo numérico del protocolo para cada nueva lista de acceso; sin embargo, el administrador sólo puede especificar una lista de acceso por protocolo, por interfaz, por dirección

Mascara Wildcard

El término *máscara wildcard* es la denominación aplicada al proceso de comparación de bits de máscara y proviene de una analogía con el "wildcard" (comodín) que equivale a cualquier otro naipe en un juego de póquer. La mascara wildcard es empleada en las ACL para indicarle al router si se le permitirá o denegará el acceso a una red, subred o host en particular, al igual que una mascara de red tiene un tamaño de 32 bits se divide en cuatro octetos, en la que cada octeto contiene 8 bits y ambas se comparan a una dirección IP, pero sus principal diferencia radica en que toma en cuenta los bits con valor lógico bajo “0” y los bits de nivel lógico alto “1” son ignorados. Las ACL usan máscaras wildcard

para identificar una sola o múltiples direcciones para las pruebas de aprobar o rechazar.

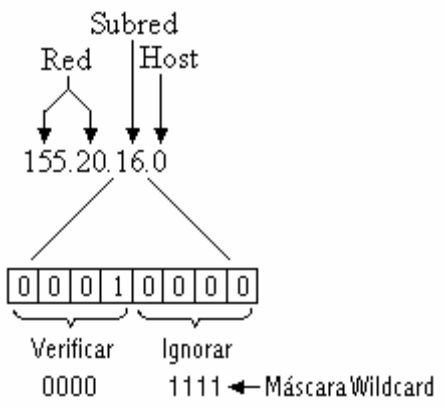
128	64	32	16	8	4	2	1	Posición del bit de octeto
0	0	0	0	0	0	0	0	Verificar todos los bits de la dirección IP
0	0	1	1	1	1	1	1	Verificar los bits en la posición 128 y 64 de la dirección IP
0	0	0	0	1	1	1	1	Verificar los cuatro bits más significativos (128-16)
1	1	1	1	1	1	0	0	Verificar únicamente los bits en la posición 2 y 1
1	1	1	1	1	1	1	1	Ignorar todos los bits

Un administrador debe verificar una dirección IP para verificar la existencia de subredes que se pueden permitir o denegar. Supongamos que la dirección IP es de Clase B (los primeros dos octetos son el número de red) con ocho bits de división en subredes (el tercer octeto es para las subredes). El administrador debe usar los bits de máscara wildcard IP para coincidir con las subredes 155.20.16.0 a 155.20.31.0. La máscara wildcard se usa para hacer esto de la siguiente manera:

Para empezar, la máscara wildcard verifica los primeros dos octetos (155.20), utilizando los bits de cero correspondientes en la máscara wildcard.

En el tercer octeto, donde se encuentra la dirección de subred, la máscara wildcard verifica que la posición del bit para el 16 binario esté activada y todos los bits superiores estén desactivados utilizando bits cero correspondientes en la máscara wildcard. Para los cuatro bits finales (de extremo inferior) en este octeto la máscara wildcard ignora el valor de estas posiciones, el valor de la dirección puede ser binario 0 o binario 1. De esta manera, la máscara wildcard coincide con

la subred 16, 17, 18, y así en adelante hasta la subred 31. La máscara wildcard no coincide con ninguna otra subred.



Como no interesan las direcciones de host individuales (un identificador de host no será .0.0 al final de la dirección), la máscara wildcard ignora el octeto final, utilizando los bits unos correspondientes en la máscara wildcard, por lo que la máscara wildcard tendrá el valor de 0.0.15.255

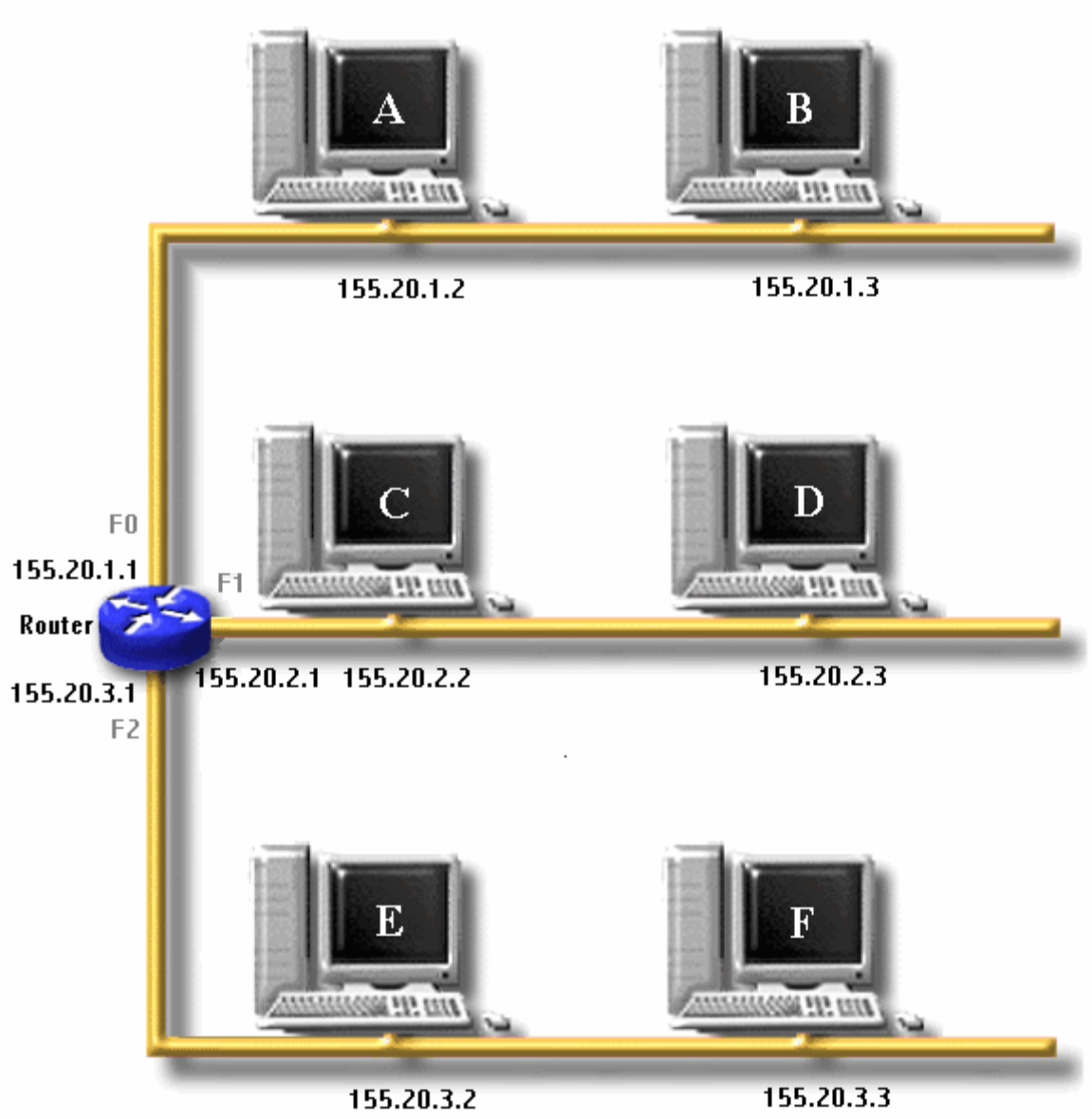
En este ejemplo, la dirección 155.20.16.0 con la máscara wildcard 0.0.15.255 coincide con las subredes 155.20.16.0 a 155.20.31.0.

Listas de acceso estándar se deben usar las ACL estándar cuando se desea bloquear todo el tráfico de una red, permitir todo el tráfico desde una red específica o denegar conjuntos de protocolo. Las ACL estándar verifican la dirección origen de los paquetes que se deben enrutar. El resultado permite o deniega el resultado para todo un conjunto de protocolo, según las direcciones de red, subred y host

Por ejemplo, supongamos que en la siguiente red se desea:

a. Permitir el acceso solo al host A con dirección IP 155.20.1.2 conectado en la subred 155.20.1.0

b. Denegar el acceso a todo host conectado en la subred 155.20.2.0
c. Permitir el acceso a cualquier host que pertenezca a la subred 155.20.3.0
d. Permitir que el host A con dirección IP 155.20.1.2 establezca sesiones telnet con el router



a. La creación de las ACL ya sean estándar o extendidas constan de dos pasos, el primero, es la declaración de la o las sentencias, que en este caso, se

desea que la subred 155.20.1.0 tenga acceso al router por consiguiente la sentencia quedaría:

```
FES_A(config)#access-list 1 permit 155.20.1.2 0.0.0.0
FES_A(config)#
```

Donde:

access-list	Comando para declarar una ACL
1	Número que le indica al router que se trata de una ACL Estándar, porque se encuentra en el rango de 1 - 99
Permit	Permitirá la entrada o salida del host A
155.20.1.2	Dirección IP del host A
0.0.0.0	Máscara wildcard que indica que se revisaran todos los octetos de la dirección IP

El segundo paso para crear una ACL, es aplicarlo a una interfaz del router, viendo el diagrama se aplicara a la interfaz FastEthernet 0

```
FES_A(config)#interface FastEthernet 0
FES_A(config-if)#ip access-group 1 in
FES_A(config-if)#
```

ip access-group	Especifica el control de acceso para paquetes
1	Indica que conjunto de instrucciones definidas previamente con la sentencia access-list 1 serán aplicadas a dicha interfaz
in	En este caso indica que el filtro será aplicado a la entrada de la interfaz, también se puede encontrar la instrucción out que especifica que el filtro estará en la salida de la interfaz

Un punto importante que se debe de tener en cuenta al usar ACL ya sean estándar o extendidas, es que al declarar una por lo menos sin importar si se le permitirá o denegará el acceso, automáticamente cualquier otra dirección IP que no coincida con alguna dirección declarada dentro de las ACL expuestas para dicha interfaz, será automáticamente descartada, como en este ejemplo, al introducir solo una lista con la dirección IP 155.20.1.2, el router verificara toda la dirección IP, si no coincide con dicha dirección esta será descartada, por este motivo, ya no es necesario introducir otra lista de acceso que impida el acceso al Host B

b. Para denegar el acceso a todo host conectado en la subred 155.20.2.0, en el modo de configuración global, se introducirá el siguiente comando

FES_A(config)#access-list 2 deny 155.20.2.0 0.0.0.255
FES_A(config)#

Donde:

access-list	Comando para declarar una ACL
2	Número que le indica al router que se trata de una ACL Estándar, porque se encuentra en el rango de 1 - 99
Deny	Denegara la entrada o salida de cualquier dispositivo de la red al router
155.20.2.0	Dirección IP en este caso de la subred
0.0.0.255	Máscara wildcard que indica que solo los primeros tres octetos serán revisados

Ahora se tiene que activar la lista de acceso en la interfaz deseada

FES_A(config)#interface FastEthernet 1
FES_A(config-if)#ip access-group 2 in

FES_A(config-if)#

c. Si se requiere permitir el acceso a cualquier host que pertenezca a la subred 155.20.3.0 se utilizaran los comandos:

FES_A(config)#access-list 3 permit 155.20.3.0 0.0.0.255
FES_A(config)#

Donde:

access-list	Comando para declarar una ACL
3	Número que le indica al router que se trata de una ACL Estándar, porque se encuentra en el rango de 1 - 99
Permit	Permitirá la entrada o salida de cualquier dispositivo en la red al router
155.20.3.0	Dirección IP en este caso de la subred
0.0.0.255	Máscara wildcard que indica que solo los primeros tres octetos serán revisados

El siguiente paso es activar la lista de acceso en la interfaz deseada

FES_A(config)#interface FastEthernet 2
FES_A(config-if)#ip access-group 3 in
FES_A(config-if)#

d. Por ultimo, se debe permitir que el host A con dirección IP 155.20.1.2 establezca sesiones telnet con el router

Para este caso en particular, se puede utilizar la misma lista de acceso creada para la interfaz FastEthernet 0, por lo que solo es necesario darla de alta pero ahora en la línea virtual

Router(config)#line vty 0 4
Router(config-line)#access-class 1 in
Router(config-line)#

Donde:

line vty 0 4	Comando para configurar la interfaz virtual
access-class	Filtro para conexiones basadas en ACL
1	Indica que conjunto de instrucciones definidas previamente con la sentencia access-list 1 serán aplicadas a dicha interfaz
In	El filtro será aplicado a la entrada de la interfaz

En una ACL estándar, de no poner un filtro para la línea virtual previamente configurada, cualquier otro dispositivo al cual se le permita el paso por el router podrá establecer sesiones telnet con el router (Obviamente se requerirán los passwords para entrar al IOS del router)

Para el ejemplo anterior, suponiendo que los host A y E deberán establecer sesiones telnet con el router, la lista de acceso 1 ya no servirá para filtrar la línea virtual porque impediría el acceso al host E, a menos de que se añada otra línea a la lista de acceso 1 que permita el paso del host E (access-list 1 permit 155.20.3.2 0.0.0.0), en este caso puede resultar más practico agregar la línea pero si fuesen más hosts en diferentes redes, lo mejor que se puede hacer es crear una nueva lista de acceso exclusiva para administrar la línea virtual, ya que si se incrementan las listas de acceso para una sola interfaz, esta se hará más lenta sin mencionar que demandara muchos más recursos al router a tal punto que podría colapsar la red

Los comandos *in* y *out* son utilizados para aplicar el filtro en la interfaz de entrada o salida, en el ejemplo anterior, se solo se utilizo *in*, el cual impedía el acceso

directo a la interfaz (a la cual los hosts están directamente conectados) por parte de los hosts no autorizados, por otro lado, el comando *out* permite que los hosts no autorizados se comuniquen con la interfaz a la que están directamente conectados pero impide que la información fluya, es decir, la información entra pero no sale.

Comandos any y host

Trabajar con representaciones decimales de bits wildcard binarios puede ser una tarea muy tediosa. Para los usos más comunes de las máscaras wildcard, se pueden usar abreviaturas. Estas abreviaturas reducen la cantidad de cosas que hay que escribir cuando se configuran condiciones de prueba de direcciones. Por ejemplo, supongamos que desea especificar que una prueba de ACL debe permitir cualquier dirección destino. Para indicar cualquier dirección IP, se debe introducir 0.0.0.0; luego, se debe indicar que la ACL debe ignorar (es decir, permitir sin verificar) cualquier valor, la máscara wildcard correspondiente para esta dirección debe ser de todos unos (es decir, 255.255.255.255). Se puede usar la abreviatura *any* para comunicar la misma condición de prueba al software de ACL Cisco IOS. En lugar de escribir 0.0.0.0 255.255.255.255, se puede usar solamente la palabra *any* como palabra clave.

Por ejemplo, en lugar de usar esto:

```
FES_A(config)#access-list 1 permit 0.0.0.0 255.255.255.255
FES_A(config)#
```

se puede usar esto:

```
FES_A(config)#access-list 1 permit any
FES_A(config)#
```

Otra condición común en la que Cisco IOS permite una abreviatura en la máscara wildcard de ACL es cuando se desea que coincidan todos los bits de una dirección

de host IP. Por ejemplo, supongamos que desea especificar que una prueba de una lista de acceso debe denegar una dirección de host IP específica. Para indicar una dirección IP de host, debe introducir la dirección completa (por ejemplo, 155.20.1.2); luego, para indicar que la lista de acceso debe verificar todos los bits en la dirección, la máscara wildcard correspondiente para esta dirección debe ser de todos ceros (es decir, 0.0.0.0). Se puede usar la abreviatura *host* para comunicar la misma condición de prueba al router. En lugar de escribir 155.20.1.2 0.0.0.0, se puede usar la palabra *host* frente a la dirección.

En lugar de usar esto:
FES_A(config)#access-list 1 permit 155.20.1.2 0.0.0.0
FES_A(config)#

se puede usar esto:
FES_A(config)#access-list 1 permit host 155.20.1.2
FES_A(config)#

Listas de control extendidas

Las listas de acceso extendidas se usan con mayor frecuencia para verificar condiciones porque ofrecen una mayor cantidad de opciones de control que las ACL estándar. Se puede usar una ACL extendida cuando se desea permitir el tráfico de la Web pero denegar el Protocolo de Transferencia de Archivos (FTP) o telnet desde las redes que no pertenecen a la empresa. Las ACL extendidas verifican las direcciones origen y destino de los paquetes. También pueden verificar protocolos, números de puerto y otros parámetros específicos. Esto ofrece mayor flexibilidad para describir las verificaciones que debe realizar la ACL. Se pueden permitir o denegar paquetes según su origen o destino. Por ejemplo, la ACL extendida puede permitir el tráfico de correo electrónico desde F0 a destinos S0 específicos, denegando al mismo tiempo conexiones remotas o transferencias de archivos

Para una sola ACL, se pueden definir múltiples sentencias. Cada una de estas sentencias debe hacer referencia al mismo nombre o número identificado, para relacionar las sentencias a la misma ACL. Se puede establecer cualquier cantidad de sentencias de condición, con la única limitación de la memoria disponible. Cuanto más sentencias se establezcan, mayor será la dificultad para comprender y administrar la ACL. Por lo tanto, la documentación de las ACL evita la confusión.

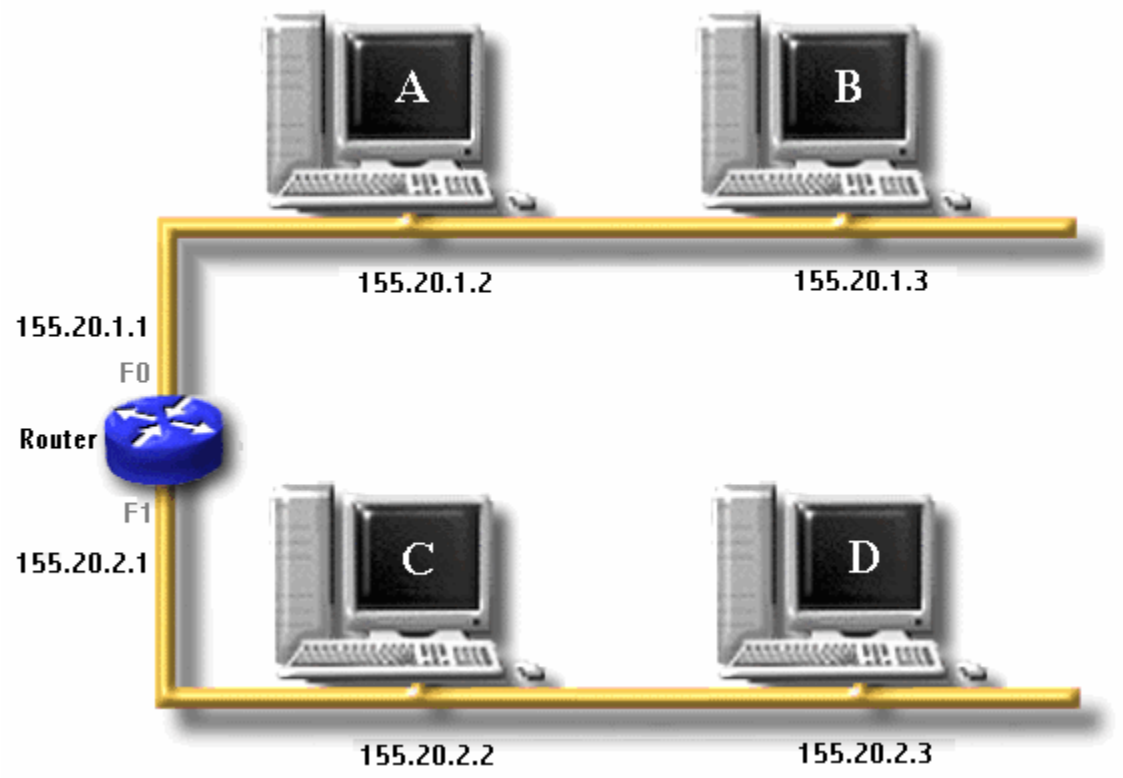
Para un control más preciso de filtrado de tráfico se usan las ACL extendidas. Las sentencias de las ACL extendidas verifican la dirección origen y destino. Además, al final de la sentencia de la ACL extendida, se obtiene precisión adicional con un campo que especifica el número de puerto de protocolo opcional TCP o del Protocolo de Datagrama del Usuario (UDP). Estos pueden ser números de puerto conocidos para TCP/IP. Algunos de los números de puerto más comunes son:

Número de puerto	Descripción	Protocolo IP
20	Datos FTP	TCP
21	Programa FTP	TCP
23	Telnet	TCP
25	Protocolo de transferencia de correo simple	TCP
69	TFTP	UDP
53	DNS	TCP/UDP
80	HTTP	TCP

Se puede especificar la operación lógica que la ACL extendida efectuará en protocolos específicos. Las ACL extendidas usan un número dentro del intervalo del 100 al 199.

En el siguiente ejemplo se explicara como crear una lista de acceso extendida.
En la siguiente red, de desea que:

a. Los hosts A y B dispongan de http pero no puedan transferir o recibir archivos fuera de la red 155.20.1.0
b. El host C no tenga salida al router pero el host D si, además de que cuente con todos los servicios disponibles en la red



a. Para que los hosts A y B dispongan de http pero no puedan transferir o recibir archivos fuera de la red 155.20.1.0, en el modo de configuración global se debe de introducir la siguiente instrucción:

FES_A(config)#access-list 101 permit tcp 155.20.1.0 0.0.0.255 0.0.0.0 255.255.255.255 eq 80
FES_A(config)#

Donde:

access-list	Comando para declarar una ACL
101	Identifica la lista utilizando un número dentro del intervalo de 100 a 199
Permit	Indica que se permitirá el trafico por la interfaz
Tcp	Protocolo usado, también se pueden utilizar otros protocolos como IP, UDP, ICMP GRE o IGRP
155.20.1.0 0.0.0.255	Dirección IP de origen con su respectiva máscara
0.0.0.0 255.255.255.255	Dirección IP destino con su respectiva máscara, la cual indica cualquier dirección
Eq	Operador que significa igual a, también se pueden poner *lt* (menor que), *gt* (mayor que) y *noeq* (desigual)
80	Especifica el número de puerto conocido, en este caso para Http

Al utilizar la instrucción anterior al igual que en las ACL estándar, ya no es necesario añadir otra sentencia que impida el intercambio de archivos, puesto que el router lo hace implícitamente. Por ultimo para el inciso a, queda aplicar el filtro a la interfaz, básicamente es el mismo comando empleado para las listas de control estándar lo único que cambia es el número de lista

FES_A(config)#interface FastEthernet 0
FES_A(config-if)#ip access-group 101 out
FES_A(config-if)#

En las ACL extendidas, también se puede hacer uso de los comandos *host* y *any*

b. Si se desea que el host C no tenga salida al router pero el host D si, además de que cuente con todos los servicios disponibles en la red tan solo se insertan las siguientes líneas:

FES_A(config)#access-list 102 permit tcp host 155.20.2.3 any
FES_A(config)#access-list 102 permit ip host 155.20.2.3 any

```
FES_A(config)#access-list 102 permit udp host 155.20.2.3 any
FES_A(config)#access-list 102 permit icmp host 155.20.2.3 any
FES_A(config)#
FES_A(config)#interface FastEthernet 1
FES_A(config-if)#ip access-group 102 out
FES_A(config-if)#
```

Al solo poner la dirección del host D en las listas de acceso, automáticamente el host C será descartado por el router

En el ejemplo anterior, hay tres puntos que se deben analizar detalladamente.

a. En el inciso b. ya no se empleo la sentencia *eq* y en el inciso a. si.

En el inciso b. no se usaron las sentencias *eq, lt*, *gt* ni *noeq* porque se requiere que el host D cuente con todos los servicios, es decir las sentencias *eq, lt*, *gt* y *noeq* sirven para delimitar los servicios de un protocolo en particular, como en el caso del inciso a. que fue TCP, la sentencia *eq 80* le indica al router que solo se permitirá el uso de http a los dispositivos involucrados en dicha ACL

b. En el inciso b. solo el host D tendrá acceso a todos los servicios

En este caso dado que no se prohibirá un servicio en particular como correos, intercambio de archivos o cualquier otro, lo más recomendable es usar una ACL estándar porque al ser más fáciles de redactar se ahorrara tiempo en la programación del router, se evitan posibles errores al capturar los comandos y principalmente, se usaran menos recursos del router

c. Protocolo ICMP

Aunque en este ejemplo solo se habilito el protocolo ICMP para el host D, es recomendable habilitarlo para todos los dispositivos de la red, sin importar que un dispositivo en particular como en este caso el Host C, no tenga permiso para comunicarse con otro dispositivo fuera de su red ya que en caso de una falla, el protocolo ICMP le será de gran ayuda al administrador de red, porque a través de él sabrá que dispositivo perdió conectividad en su red.

d. En los dos ejemplos anteriores no se elimino alguna ACL.

Para eliminar una lista de control de acceso, solo basta con anteponer la orden *no* al la lista sin importar que sea una ACL estándar o extendida aunque esto implica que todas las listas de acceso que tengan el mismo número de identificador serán borradas sin importar que en la instrucción especifiquemos que solo deseamos borrar una línea, por ejemplo, se acaban de introducir las siguientes líneas de una ACL:

```
FES_A(config)#access-list 1 permit 155.20.1.0 0.0.0.255
FES_A(config)#access-list 1 permit 155.20.2.0 0.0.0.255
FES_A(config)#access-list 1 permit 155.20.4.0 0.0.0.255
FES_A(config)#
```

Posteriormente el administrador se da cuenta que cometió un error, en lugar de permitir el acceso a la red 155.20.3.0, se lo dio a la red 155.20.4.0. Para remendar su error tendrá que borrar la línea *access-list 1 permit 155.20.4.0 0.0.0.255* con la instrucción.

```
FES_A(config)#no access-list 1 permit 155.20.4.0 0.0.0.255
FES_A(config)#
```

ó también puede usar el comando

```
FES_A(config)#no access-list 1
FES_A(config)#
```

Al emplear cualquiera de los comandos anteriores, no solo se borrara dicha línea sino también se eliminaran las líneas restantes que pertenezcan a la lista de acceso número 1 por consiguiente se tendrán que introducir de nuevo todas las líneas que conformaran a la lista de acceso número 1

```
FES_A(config)#access-list 1 permit 155.20.1.0 0.0.0.255
FES_A(config)#access-list 1 permit 155.20.2.0 0.0.0.255
FES_A(config)#access-list 1 permit 155.20.3.0 0.0.0.255
FES_A(config)#
```

3.1.2.4. ACL IP con nombre

Las listas de control nombradas permiten que las ACL IP estándar y extendidas se identifiquen con una cadena alfanumérica (nombre) en lugar de la representación numérica actual (1 a 199). Las ACL nombradas se pueden usar para eliminar entradas individuales para una ACL específica. Esto permite modificar sus ACL sin eliminarlas y luego reconfigurarlas. Se usan las ACL nombradas cuando:

- Se desea identificar intuitivamente las ACL utilizando un nombre alfanumérico.

- Existen más de 99 ACL simples y 100 extendidas que se deben configurar en un router para un protocolo determinado.

S debe tener en cuenta lo siguiente antes de implementar las ACL nombradas:

- Las ACL nombradas no son compatibles con las versiones de Cisco IOS anteriores a la versión 11.2.

- No se puede usar el mismo nombre para múltiples ACL. Además, las ACL de diferentes tipos no pueden tener el mismo nombre. Por ejemplo, no es

válido especificar una ACL estándar llamada UNAM y una ACL extendida con el mismo nombre.

El formato de una lista de acceso IP con nombre es:

Router(config)#ip access-list {standard / extended) nombre

En el modo de configuración de ACL, se especifica una o más condiciones de permitir o denegar. Esto determina si el paquete debe pasar o debe descartarse. En una ACL estándar los comandos son:

Router(config-std-nacl)#(permit / deny) (dirección IP) (mascara)

Mientras que en una ACL extendida:

Router(config-ext-nacl)#(permit / deny) (protocolo) (dirección IP origen) (mascara) (dirección IP destino) (mascara) eq (número de puerto)

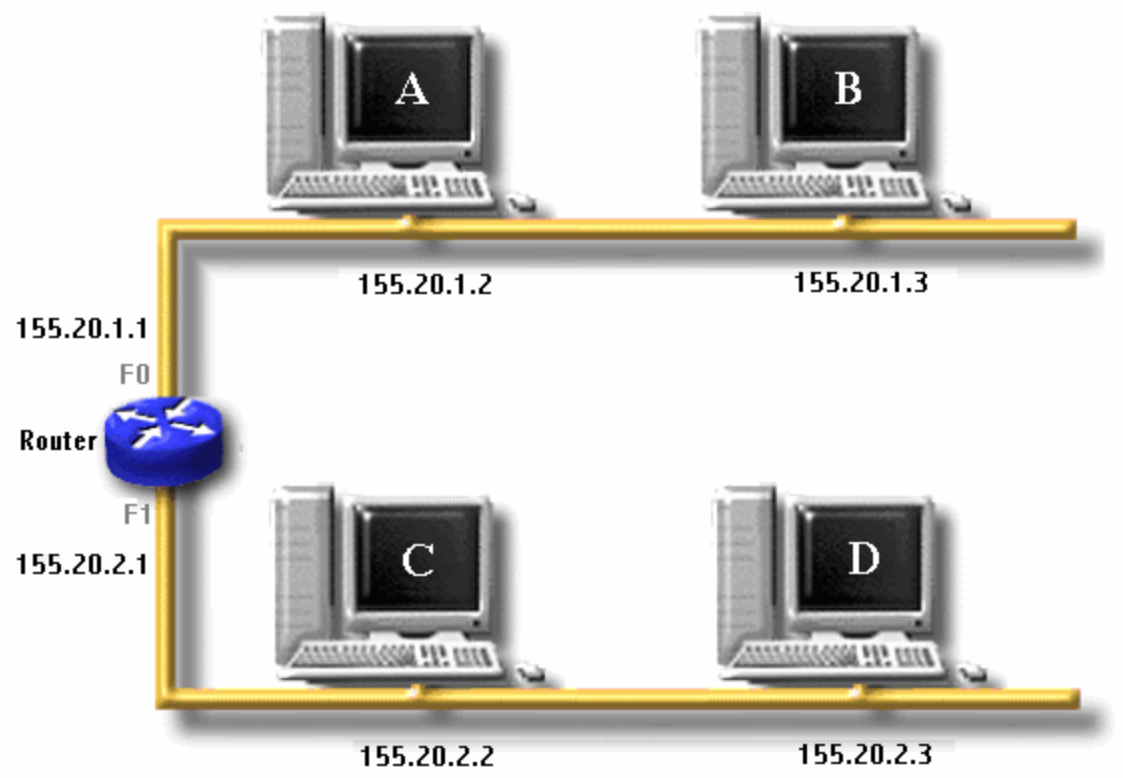
Cabe señalar que en las listas de control de acceso con nombre, también se pueden utilizar los comandos *host* y *any*

En el siguiente ejemplo se explicara como crear listas de control de acceso nombradas utilizando la red del ejemplo anterior

En la siguiente red, de desea que:

a. Los hosts A y B dispongan de http pero no puedan transferir o recibir archivos fuera de la red 155.20.1.0 y que el host A disponga de telnet

b. El host C no tenga salida al router pero el host D si, además de que cuente con todos los servicios disponibles en la red



a. Los hosts A y B dispongan de http pero no puedan transferir o recibir archivos fuera de la red 155.20.1.0 y que el host A disponga de telnet En este inciso, forzosamente se debe utilizar una ACL extendida la cual se llamará LANF0 por consiguiente las instrucciones a utilizar son:

FES_A(config)#ip access-list extended LANF0
FES_A(config-ext-nacl)#permit tcp 155.20.1.0 0.0.0.255 any eq 80
FES_A(config-ext-nacl)#permit tcp host 155.20.1.2 any eq 23
FES_A(config-ext-nacl)#

Donde:

ip access-list	Comando para crear una ACL con nombre
extended	En este caso se creara una ACL extendida
LANF0	Nombre de la ACL, se puede crear cualquier nombre como UNAM o Aragón
permit tcp	Permitir el uso de las interfaces del router para el protocolo tcp según los puertos habilitados
155.20.1.0 0.0.0.255	Dirección origen con su respectiva mascara de subred
any	Dirección destino, en este caso, cualquier dirección ip podrá ser alcanzada
eq 80	Habilitar el puerto 80 (http) del protocolo descrito anteriormente (tcp)
host 155.20.1.2	Dirección ip de un dispositivo en particular, al emplear el comando *host* se omite la mascara
eq 23	Habilitar el puerto 23 (telnet) del protocolo descrito anteriormente (tcp)

Por ultimo, al igual que en las ACL estándar y extendidas, solo hace falta aplicar el filtro a la o las interfaces deseadas solo que en este caso el número que anteriormente identificaba a la lista de acceso pasa a ser substituido por el nombre de la ACL

FES_A(config)#interface FastEthernet 0

FES_A(config-if)#ip access-group LANF0 in

FES_A(config-if)#

b. El host C no tenga salida al router pero el host D si, además de que cuente con todos los servicios disponibles en la red. En este punto, es más conveniente utilizar un filtro estándar por lo que los comandos a utilizar son:

```
FES_A(config)#ip access-list standard LANF1
FES_A(config-std-nacl)#permit host 155.20.2.3
FES_A(config-std-nacl)#
```

Donde:

ip access-list	Comando para crear una ACL con nombre
standard	En este caso se creara una ACL estándar
LANF1	Nombre de la ACL
permit	Permitir el acceso
host 155.20.2.3	Dirección IP del dispositivo, al emplear el comando host se omite la mascara

Y finalmente solo se habilita el filtro en la interfaz.

```
FES_A(config)#interface FastEthernet 1
FES_A(config-if)#ip access-group LANF1 in
FES_A(config-if)#
```

La principal ventaja que se tiene al usar las listas de control de acceso nombradas, es que si se desea borrar una línea permanecerán intactas las demás sin importar que pertenezcan a la misma lista de control, como por ejemplo, en la una ACL se tienen declarados los siguientes filtros:

```
FES_A(config)#ip access-list extended LANF0
FES_A(config-ext-nacl)#permit tcp 155.20.1.0 0.0.0.255 any eq 80
FES_A(config-ext-nacl)#permit tcp host 155.20.1.2 any eq 23
FES_A(config-ext-nacl)#permit udp 155.20.1.0 0.0.0.255 any eq 69
FES_A(config-ext-nacl)#deny ip host 155.20.1.2 any
```

FES_A(config-ext-nacl)#permit icmp any any
FES_A(config-ext-nacl)#

De la configuración anterior se debe borrar la línea *deny ip host 155.20.1.2 any,* como ya se menciono con anterioridad, para suprimir dicha línea no es necesario borrar todos los filtros anidados en la ACL LANF0 y volverlos a poner como sucede en la ACL estándar y extendidas, solo basta con entrar a LANF0 y anteponer el comando *no* al filtro que se desee eliminar
FES_A(config)#ip access-list extended LANF0
FES_A(config-ext-nacl)#no deny ip host 155.20.1.2 any
FES_A(config-ext-nacl)#

De esta forma todos los filtros a excepción de los que fueron suprimidos permanecerán intactos en la configuración, y esto se puede verificar muy fácilmente ejecutando el comando *show running-config*

FES_A#show running-config
Building configuration...

Current configuration : 1007 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname FES_A
!...
ip access-list extended LANF0
permit tcp 155.20.1.0 0.0.0.255 any eq www

permit tcp host 155.20.1.2 any eq telnet
permit udp 155.20.1.0 0.0.0.255 any eq tftp
permit icmp any any
!
line con 0
line aux 0
line vty 0 4
no scheduler allocate
!
end

Ahora que si se requiere quitar la ACL nombrada por completo, solo se antepone el comando *no* a la línea donde se nombró la lista

FES_A(config)#no ip access-list extended LANF0
FES_A(config)#

3.2. **Imagen del IOS**

Software de sistema de Cisco que proporciona funcionalidad, escalabilidad y seguridad comunes para todos los productos bajo la arquitectura Cisco Fusión. El software Cisco IOS permite la instalación y administración centralizada, integrada y automatizada de internetwork, garantizando al mismo tiempo un soporte para una amplia variedad de protocolos, medios, servicios y plataformas

Los routers arrancan el software Cisco IOS desde:

- la memoria Flash
- un servidor TFTP
- la ROM (no el software Cisco IOS completo)

El software Cisco IOS se carga en primer lugar desde la memoria Flash, luego desde un servidor de red y, por último, desde la ROM:

- Memoria flash: Se puede cargar una imagen del sistema desde la memoria programable de sólo lectura borrable eléctricamente (EEPROM). La información que se guarda en la memoria Flash no es susceptible a las fallas de red que se pueden producir al cargar imágenes de sistema desde los servidores TFTP.
- Servidor de red: En caso de que la memoria Flash se dañe, se establece una copia de respaldo especificando que se debe cargar una imagen de sistema desde un servidor TFTP.
- ROM: Si la memoria Flash se daña y el servidor de red no puede cargar la imagen, la opción bootstrap final del software es arrancar desde la ROM. Sin embargo, la imagen de sistema de la ROM posiblemente sea sólo una parte del software Cisco IOS, al que le faltarán los protocolos, las funciones y las configuraciones del software Cisco IOS completo. Además, si ha actualizado el software desde que adquirió el router, esta versión probablemente sea una versión antigua del software Cisco IOS.

El router ejecuta los comandos de arranque del sistema según sea necesario en el orden en el que se introdujeron originalmente en el modo de configuración

3.2.1 *Carga y descarga del IOS desde el modo privilegiado*

Antes de cargar una nueva versión de IOS a un router, se debe siempre guardar la versión anterior, esto es por motivos de seguridad, ya que se puede dar el caso de que la imagen no sea compatible o simplemente no funcione correctamente, para lograr esto se tiene que hacer uso de un servidor TFTP. En primer lugar, se debe verificar que exista una conexión entre el router y el host mediante el comando ping. Si el ping resultó exitoso se procederá con el siguiente paso, de lo contrario,

se puede conectar directamente al router con un host mediante un cable cruzado aunque al hacer esto, se debe cambiar alguna de las direcciones ip ya sea del router o del host para que estén en la misma red.

C:\WINDOWS>ping 180.175.11.1

Haciendo ping a 180.175.11.1 con 32 bytes de datos:

Respuesta desde 180.175.11.1: bytes=32 tiempo<10ms TDV=255
Respuesta desde 180.175.11.1: bytes=32 tiempo<10ms TDV=255
Respuesta desde 180.175.11.1: bytes=32 tiempo<10ms TDV=255
Respuesta desde 180.175.11.1: bytes=32 tiempo<10ms TDV=255

Estadísticas de ping para 180.175.11.1:
    Paquetes: enviados = 4, Recibidos = 4, perdidos = 0 (0% loss),
Tiempos aproximados de recorrido redondo en milisegundos:
    mínimo = 0ms, máximo = 0ms, promedio = 0ms

C:\WINDOWS>

Previamente debemos conocer algunos datos como el nombre del fichero que contiene el IOS y la cantidad de memoria de la cual disponemos en la flash, para saber esto, se hace uso del comando *show flash,* donde vemos que el nombre del fichero que contiene el IOS se llama *c1700-sv3y-mz.121-5.T7.bin* así como su tamaño además también se despliega el espacio usado, disponible y total de la memoria flash

FES_A#show flash
System flash directory:
File Length   Name/status
  1   5510172 c1700-sv3y-mz.121-5.T7.bin
[5510236 bytes used, 2878372 available, 8388608 total]

8192K bytes of processor board System flash (Read/Write)
FES_A#

Ahora desde el router se ejecuta la instrucción *copy flash tftp* enseguida el router solicitará el nombre del archivo que se va a copiar, la dirección ip del dispositivo con el cual efectuará la transferencia, y por ultimo con que nombre se guardará el archivo en dicho dispositivo

FES_A#copy flash tftp
Source filename []? c1700-sv3y-mz.121-5.T7.bin
Address or name of remote host []? 180.175.11.2
Destination filename [c1700-sv3y-mz.121-5.T7.bin]?
!!!
!!
5510172 bytes copied in 56.68 secs (98395 bytes/sec)
FES_A#

Carga del IOS

Existen varias formas de cargar una imagen del IOS a un router, la más común es mediante un servidor TFTP.

Ejemplo. Supongamos que deseamos actualizar el IOS del router, para esto se tiene que guardar la imagen por motivos de seguridad como ya vimos anteriormente. Los comandos a ejecutar son muy parecidos a los de la descarga, utilizamos el comando *copy tftp flash,* al igual que en la descarga nos solicitara la dirección ip del servidor tftp, el nombre del archivo, con que nombre lo queremos guardar y por ultimo nos preguntara si queremos borrar el contenido de la memoria flash

FES_A#copy tftp flash

Address or name of remote host ? 180.175.11.2
Source filename []? c1700-sv3y-mz.121-5.T7.bin
Destination filename [c1700-sv3y-mz.121-5.T7.bin]?
Accessing tftp://180.175.11.2/c1700-sv3y-mz.121-5.T7.bin...
Erase flash: before copying? [confirm]
Erasing the flash filesystem will remove all files! Continue? [confirm]
Erasing device...
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
ee ...erased
Erase of flash: complete
Loading c1700-sv3y-mz.121-5.T7.bin from 180.175.11.2 (via FastEthernet0): !!!!!!
!!!
!!!
!!!!!!!!!!!!!
[OK - 5510172/11020288 bytes]

Verifying checksum... OK (0xB025)
5510172 bytes copied in 87.768 secs (63335 bytes/sec)
FES_A#

3.2.2. Carga y descarga del IOS desde el modo ronmon

En ocasiones es necesario cargar el IOS desde *rommon*> o en algunos otros modelos desde >, porque puede darse el caso de que se dañe el IOS, borremos accidentalmente la memoria flash o al actualizar la versión del IOS está no trabaje correctamente.

A continuación, veremos como cargar una imagen mediante un servidor TFTP desde el modo *rommon>,* en este ejemplo emplearemos el comando *tftpdnld,* al

ejecutarlo nos pedirá que definamos una serie de parámetros algunos son opcionales así es que no hay problema si los omitimos

```
rommon 1 > tftpdnld
Illegal IP address.
usage: tftpdnld [-r]

  Use this command for disaster recovery only to recover an image via TFTP.
  Monitor variables are used to set up parameters for the transfer.
  (Syntax: "VARIABLE_NAME=value" and use "set" to show current variables.)
  "ctrl-c" or "break" stops the transfer before flash erase begins.

  The following variables are REQUIRED to be set for tftpdnld:
                  IP_ADDRESS: The IP address for this unit
           IP_SUBNET_MASK: The subnet mask for this unit
       DEFAULT_GATEWAY: The default gateway for this unit
                TFTP_SERVER: The IP address of the server to fetch from
                    TFTP_FILE: The filename to fetch

  The following variables are OPTIONAL:
       TFTP_VERBOSE: Print setting. 0=quiet, 1=progress(default), 2=verbose
       TFTP_RETRY_COUNT: Retry count for ARP and TFTP (default=7)
       TFTP_TIMEOUT: Overall timeout of operation in seconds (default=7200)
       TFTP_CHECKSUM: Perform checksum test on image, 0=no, 1=yes
(default=1)

  Command line options:
   -r: do not write flash, load to DRAM only and launch image
rommon 2 >
```

Los parámetros importantes que debemos introducir son:

- Una dirección ip temporal para el router
- Mascara de la dirección ip
- Puerta de salida que en este caso es la dirección ip del router
- La dirección ip del servidor tftp
- El nombre del archivo que contiene la imagen

Para introducir estos comandos hacemos uso del comando *set*, mediante el cual aparecerán los valores definidos para cada una de las variables anteriormente descritas

```
rommon 2 > set
PS1=rommon ! >
IP_ADDRESS=
IP_SUBNET_MASK=
DEFAULT_GATEWAY=
TFTP_SERVER=
TFTP_FILE=
TFTP_CHECKSUM=
BSI=0
RET_2_RTS=
?=1
rommon 3 >
```

Ahora se declaran cada una de las variables

```
rommon 3 > IP_ADDRESS=180.175.11.1
rommon 4 > IP_SUBNET_MASK=255.255.0.0
rommon 5 > DEFAULT_GATEWAY=180.175.11.1
rommon 6 > TFTP_SERVER=180.175.11.2
rommon 7 > TFTP_FILE=c1700-sv3y-mz.121-5.T7.bin
```

rommon 8 >

Si volvemos a ejecutar el comando *set* se despliegan los parámetros que hemos introducido

```
rommon 8 > set
PS1=rommon ! >
TFTP_CHECKSUM=
BSI=0
RET_2_RTS=
?=0
IP_ADDRESS=180.175.11.1
IP_SUBNET_MASK=255.255.0.0
DEFAULT_GATEWAY=180.175.11.1
TFTP_SERVER=180.175.11.2
TFTP_FILE=c1700-sv3y-mz.121-5.T7.bin
rommon 9 >
```

El siguiente paso es volver a ejecutar el comando *tftpdnld,* si lo hemos hecho correctamente, ahora nos preguntara si deseamos cargar la imagen a lo cual respondemos que si “y”

```
rommon 9 > tftpdnld

              IP_ADDRESS: 180.175.11.1
          IP_SUBNET_MASK: 255.255.0.0
      DEFAULT_GATEWAY: 180.175.11.1
             TFTP_SERVER: 180.175.11.2
               TFTP_FILE: c1700-sv3y-mz.121-5.T7.bin
```

Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash will be lost!
Do you wish to continue? y/n: [n]: y

Receiving c1700-sv3y-mz.121-5.T7.bin from 180.175.11.2
!!
!!
!!!!!!!!!!!!!!!!!!!!
File reception completed.
Copying file c1700-sv3y-mz.121-5.T7.bin to flash.
Erasing flash at 0x607f0000
Programming location 60540000
rommon 10 >

Finalmente estaremos de nuevo en *rommon>,* ahora introducimos el comando *reset* o simplemente apagamos y volvemos a encender el equipo y el router deberá cargar automáticamente la imagen
rommon 10 >reset
...
Press RETURN to get starteds RETURN to get started!

También se puede cargar la imagen directamente al router sin necesidad de guardarla en la memoria flash, el procedimiento es exactamente igual al descrito anteriormente pero lo único que cambia es que en lugar de utilizar el comando tftpdnld se usará la instrucción tftpdnld -r

Carga del IOS por xmodem

Existe otro método de cargar el IOS, esto es mediante el comando xmodem en el cual se utiliza el puerto consola y el programa hyperterminal, este método no es

muy utilizado porque no todos los routers cuentan con este comando, además de que la velocidad de transferencia es muy baja

Antes de iniciar la descarga de la imagen, primero debemos aumentar la velocidad del puerto consola de 9600 a 115200 para esto se tiene que entrar a la línea de consola y ejecutar el comando *speed xx* donde *xx* es la velocidad a la cual se trabajará, normalmente ya por configuración de fabrica esta velocidad es de 9600

FES_A(config)#line console 0
FES_A(config-line)#speed 115200
FES_A(config-line)#

Para cambiar la velocidad desde *rommon* se ejecuta el comando *confreg,* al ejecutarlo el equipo empezara a despegar una serie de preguntas de las cuales se tendrá que decir que si solo a dos, la primera dirá que si se desea cambiar la configuración, y la segunda si se quiere cambiar la velocidad de la consola, al contestar afirmativamente a esta ultima pregunta se deberá especificar la velocidad del puerto, en este caso se empleará 115200

rommon 1 > **confreg**

Configuration Summary
(Virtual Configuration Register: 0x3922)
enabled are:
load rom after netboot fails
console baud: 9600
boot: image specified by the boot system commands
or default to: cisco2-C1700

do you wish to change the configuration? y/n [n]: **y**

enable "diagnostic mode"? y/n [n]:
enable "use net in IP bcast address"? y/n [n]:
disable "load rom after netboot fails"? y/n [n]:
enable "use all zero broadcast"? y/n [n]:
enable "break/abort has effect"? y/n [n]:
enable "ignore system config info"? y/n [n]:
change console baud rate? y/n [n]: **y**
enter rate: 0 = 9600, 1 = 4800, 2 = 1200, 3 = 2400
4 = 19200, 5 = 38400, 6 = 57600, 7 = 115200 [0]: **7**
change the boot characteristics? y/n [n]:

Configuration Summary
(Virtual Configuration Register: 0x3922)
enabled are:
load rom after netboot fails
console baud: 115200
boot: image specified by the boot system commands
or default to: cisco2-C1700

do you wish to change the configuration? y/n [n]:
rommon 2 > **reset**

Una vez hecho este cambio, en la ventana de hyperterminal aparecerán símbolos raros o simplemente ya no responderá, no aparecerá nada, para esto, debemos modificar la configuración de hyperterminal cambiando únicamente los Bits por segundo de 9600 a 115200 para poder acceder al router. Ahora debemos reiniciar el router mediante el comando *reload* o simplemente apagando y encendiendo el router, una vez que prenda el equipo, se deben presionar las teclas *control* + *pausa* ó *control* + *break* para iniciar desde *rommon>*

FES_A#
FES_A#reload

00:30:20: %SYS-5-RELOAD: Reload requested
System Bootstrap, Version 12.0(3)T, RELEASE SOFTWARE (fc1)
Copyright (c) 1999 by cisco Systems, Inc.
PC = 0xfff0be48, Vector = 0x500, SP = 0xff0027c8
C1700 platform with 32768 Kbytes of main memory

program load complete, entry point: 0x80008000, size: 0x541300
PC = 0xfff0be48, Vector = 0x500, SP = 0x81fffeb0

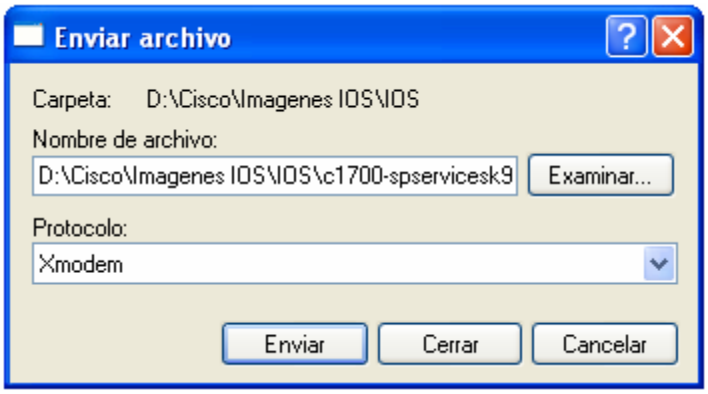
monitor: command "boot" aborted due to user interrupt
rommon 1 >

El siguiente paso el ejecutar el comando *xmodem –r c1700-sv3y-mz.121-5.T7.bin* donde *r* es opcional, si se utiliza copiara la imagen en la memoria RAM y la cargara cuando la transferencia concluya, sino se utiliza, copiará el IOS directamente en la memoria Flash

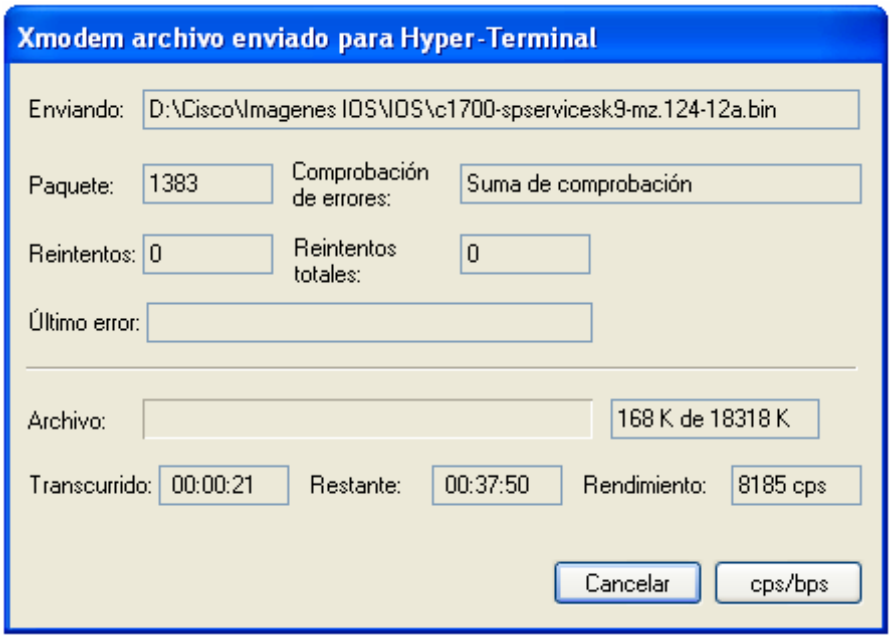
rommon 1 > xmodem –r *c1700-sv3y-mz.121-5.T7.bin*
Do not start the sending program yet...

Invoke this application only for disaster recovery.
Do you wish to continue? y/n [n]: y

Enseguida de decirle que si “y” desde el programa hyperterminal seleccionamos *transferir / enviar archivo,* le indicamos que se empleara el protocolo *xmodem*



Abrimos el archivo que contiene la imagen y deberá aparecer un cuadro como el siguiente:



Al final de la descarga

Download Complete

Program load comple, entry point: 0x80008000, size: 0x541300

Self decompressing the image. .

##

```
##################################################################################################################################################### [OK]
...
FES_A>
```

Nota: Puede ser que tengamos dos imágenes en nuestro equipo. En caso de estar de esa manera hay que configurar el cisco por medio del siguiente comando para indicarle cual imagen debe cargar

```
FES_A# config-terminal
FES_A(config)#boot-start-marker
FES_A(config)#boot system flash c1700-sv3y-mz.123-6a.bin
FES_A(config)#boot-end-marker
FES_A(config)#exit
FES_A# write
FES_A# reload
```

Una vez reiniciado el Router, podemos comprobar la versión de la imagen instalada con el siguiente comando:

```
FES_A> show version
```

Si por algún motivo al reiniciar el Router este no inicializara correctamente, se tendría que verificar el tipo de error que despliega la pantalla o descargar el IOS con el que se contaba con anterioridad.

3.3. Comandos básicos empleados para la detección de fallas

El router cisco es un equipo que tiene la capacidad de indicarnos su estado operacional, desde el estado de las interfaces hasta problemas de hardware. Dentro de los comandos más comunes se encuentran:

show version	show ip interface brief
show logging	show running-config
show startup-config	show diag
show arp	show voice call summary
show interface	debug

Show Version

Con ayuda del comando show versión se puede determinar el modelo del equipo y en algunos casos el numero de serie, cuanto tiempo ha permanecido el router activo, el modo en que fue encendido, el nombre y versión de la imagen IOS con la cual se encuentra operando, el tamaño de sus memorias RAM, NVRAM y flash, las interfaces que tiene y el registro de configuración en el que se encuentra.

Show ip interface brief

Muestra las direcciones ip y el estado de todas las interfaces del equipo

Router# show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0	10.108.00.5	YES	NVRAM	up	up
				administratively	
Ethernet1	unassigned	YES	unset	down	down
Loopback0	10.108.200.5	YES	NVRAM	up	up
Serial0	10.108.100.5	YES	NVRAM	up	up
Serial1	10.108.40.5	YES	NVRAM	up	up
Serial2	10.108.100.5	YES	manual	up	up
				administratively	
Serial3	unassigned	YES	unset	down	down

Campo	Descripción
Interface	Tipo de interface.
IP-Address	Dirección IP asignada a la interface
OK?	"Yes" means that the IP Address is currently valid. "No" means that the IP Address is not currently valid.
Method	▪ En el campo method se puede encontrar lo siguiente: ▪ RARP o SLARP - Protocolo de resolución de direcciones inverso (RARP) o Protocolo de resolución de direcciones de la línea serial(SLARP) ▪ BOOTP - Protocolo Bootstrap ▪ TFTP - Archivo de configuración obtenido de un servidor tftp ▪ manual - Se cambio el campo manualmente mediante la línea de comandos ▪ NVRAM -Archivo de configuración de la NVRAM ▪ IPCP - Comando de negociación de dirección IP ▪ DHCP - Comando **ip address dhcp** ▪ unassigned - No hay dirección IP asignada ▪ unset - No programada ▪ other - Desconocido
Status	▪ Indica el estado de la interface. Los valores que se pueden encontrar son: ▪ up—La interface esta activa ▪ down— La interface esta inactiva

	▪ administratively down—La interface esta administrativamente inactiva
Protocol	Indica el estado operacional del protocolo de ruteo en la interface.

Show logging

Para mostrar el estado y cambios registrados en el buffer del sistema. Solo se puede usar este comando en el modo privilegiado y previamente se debe de dar de alta en el modo de configuración global mediante la instrucción

Show running-config

Este comando permite ver la configuración actual alojada en la RAM. Esto es, la configuración activa y los cambios hechos en el router serán mostrados a través de esta instrucción. Desde el encendido del router, cualquier cambio de configuración no guardado será borrado cuando el router se reinicie.

Show startup-config

Este comando permite visualizar el archivo de configuración contenido en la en la memoria NVRAM del router. Este archivo de configuración es cargado a la memoria RAM cuando el router es encendido. Cualquier cambio hecho en la configuración del router no será guardado en le memoria NVRAM a menos de que dicho cambio sea salvado mediante los comandos “copy running-config startup-config” o “write”

Show diag

Muestra la información de hardware del router desde la motherboard hasta tarjetas de aplicación. Mediante este comando se puede conocer con exactitud las tarjetas que contiene el equipo y el slot en donde se encuentran conectadas así como su

número de serie y puede ser usado para confirmar que el equipo ha detectado las tarjetas de aplicación. El comando *show diag* se usa en el modo privilegiado.

Show arp

Muestra la tabla de entradas ARP (Protocolo de resolución de direcciones). Mediante este comando se pueden conocer las direcciones IP y MAC de los equipos que han establecido comunicación con alguna de las interfaces del router. El comando *show arp* se usa en el modo privilegiado.

La siguiente tabla es resultado de utilizar el comando show *arp*:

Router# show arp

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	131.108.42.112	120	0000.a710.4baf	ARPA	Ethernet3
AppleTalk	4028.5	29	0000.0c01.0e56	SNAP	Ethernet2
Internet	131.108.42.114	105	0000.a710.859b	ARPA	Ethernet3
AppleTalk	4028.9	-	0000.0c02.a03c	SNAP	Ethernet2
Internet	131.108.42.121	42	0000.a710.68cd	ARPA	Ethernet3
Internet	131.108.36.9	-	0000.3080.6fd4	SNAP	TokenRing0
AppleTalk	4036.9	-	0000.3080.6fd4	SNAP	TokenRing0
Internet	131.108.33.9	-	0000.0c01.7bbd	SNAP	Fddi0

Campo	Descripción
Protocol	Protocolo que se esta utilizando la dirección contenida en el campo Ardes
Address	Dirección de red que correponde al campo Address.
Age (min)	Tiempo en minutos desde que se registro la dirección en la tabla El símbolo – significa que la dirección es del router.
Hardware	Dirección MAC correspondiente al equipo registrado en la red LAN.

Addr	
Type	Indica el tipo de encapsulación que se esta utilizando para la dirección de red. Dentro de las posibles entradas que se pueden encontrar en este campo se encuentran: ARPA SNAP ETLK (EtherTalk) SMDS
Interface	Indica la interface asociada a la dirección de red.

Show voice call summary

Muestra el estado actual de los puertos de voz en el Router

PORT	CODEC	VAD	VTSP STATE	VPM STATE
======	=======	======	==================	==================
0/1/0	None	-	S_SETUP_REQ_PROC	FXSLS_WAIT_OFFHOOK
0/1/1	None	-	S_CONNECT	FXSLS_CONNECT
0/1/2	-	-	-	FXSLS_ONHOOK
0/1/3	g729r8	n	S_CONNECT	FXSLS_CONNECT
0/3/0	None	-	S_WAIT_RELEASE	EM_WAIT_CLR_DONE
0/3/1	-	-	-	FXSLS_ONHOOK

Campo	Descripción
Port	Indica la ubicación del puerto de voz, por ejemplo 0/3/1 (Modulo 0, Slot 3, Puerto 1)
Codec	Modo de compresión de voz usado, solo se usa el codec para llamar a un router diferente

Vad	Indica si la VAD (actividad de detección de voz) esta activada
VTSP STATE	Monitorean la actividad del puerto • S_SETUP_REQ_PROC-Petición para establecer llamada • S_CONNECT – Llamada establecida • S_WAIT_RELEASE – Fin de llamada, en espera de liberar la línea
VPM STATE	Monitorean la actividad del puerto • FXSLS_WAIT_OFFHOOK – En espera de descolgar el teléfono • FXSLS_CONNECT – Llamada establecida • EM_WAIT_CLR_DONE – Fin de llamada, en espera de colgar el teléfono

Show interface

El comando *show interfaces* es utilizado para desplegar en la pantalla todas la estadísticas de las interfaces físicas y lógicas configuradas. Dentro de la información más relevante proporcionada por esta instrucción se encuentran:

Estado actual de las interfaces
Direcciones Ip con su respectiva mascara
Carga de transmisión y recepción
Direcciones MAC (solo para interfaces LAN)
Encapsulamiento
Paquetes transmitidos y recibidos
Errores de retransmisión CRC

3.4. Metodología para realizar un mantenimiento preventivo a un Router Cisco

El mantenimiento preventivo consiste en la revisión periódica de ciertos aspectos, tanto de hardware como de software en un Router. Estos influyen en el desempeño fiable del sistema, en la integridad de los datos almacenados y en un intercambio de información correcta, a la máxima velocidad posible dentro de la configuración optima del sistema. Su propósito es prever las fallas manteniendo los equipos e instalaciones productivas en completa operación a los niveles y eficiencia óptimos.

Ventajas del Mantenimiento Preventivo:

- Confiabilidad, los equipos operan en mejores condiciones de seguridad, ya que se conoce su estado, y sus condiciones de funcionamiento.
- Mayor duración, de los equipos e instalaciones.
- Disminución de existencias en Almacén y, por lo tanto sus costos, puesto que se ajustan los repuestos de mayor y menor consumo.
- Menor costo de las reparaciones.

Pasos de un mantenimiento preventivo

1. Descarga la corriente electrostática del cuerpo antes de manipular el hardware del Router. Se elimina la estática de nuestro cuerpo, usando pulsera y mantel antiestático.
2. hacer un respaldo de la configuración del router para tener la configuración actualizada, y en caso de algún problema después del mantenimiento, se pueda configurar el equipo.
3. El siguiente paso es apagar el router y desconectar los cables externos, empezando con el de energía eléctrica, después se desconectaran los cables de datos que están en las interfaces WAN y LAN.
4. Limpieza del interior del Router, Para retirar el polvo te recomendamos utilizar un aparato soplador que sea capaz de lanzar un chorro de aire. Si

utilizas una aspiradora tienes que utilizar una brocha o pincel para ayudar en la remoción de grumos (combinación de polvo y grasa) teniendo precaución en el movimiento de los mismos para no dañar componentes o aflojar cables.

5. Revisión de cables internos. Hay que revisar los conectores internos del router (puntos en donde se enchufan cables), para asegurarse que no están flojos.
6. Limpieza exterior del router. Para retirar el polvo en el equipo se necesita espuma limpiadora para superficies plásticas y una franela.

3.5. Metodología para la solución de problemas (Reales o potenciales)

Los problemas siempre se presentan, incluso cuando se monitoriza la red, el equipamiento es fiable y los usuarios son cuidadosos, las cosas se tuercen. La prueba de fuego de un buen administrado de red es la capacidad de analizar, solucionar problemas y corregir problemas bajo la presión de un fallo de red que origine un tiempo de inactividad de la empresa

El primer paso a la hora de solucionar los problemas de la red consiste en definir el problema. Esta definición puede ser una consolidación de muchas fuentes distintas. Uno de los orígenes puede ser un problema o un informe del servicio técnico, que identifica el problema inicialmente. Otra fuente podría ser una conversación telefónica con el usuario en la que se tratara el problema con el fin de reunir mar información acerca de él, las herramientas de monitorización de redes pueden proporcionar una idea más completa acerca del problema especifico a resolver, otros usuarios y sus propias observaciones también proporcionaran información.

En este tema nos enfocaremos únicamente a la resolución de los problemas más usuales que se presentan un router Cisco.

Resolución de problemas de arranque del equipo

En un router Cisco hay ciertas cosas que pueden impedir un arranque correcto del router

- Un archivo de configuración con una sentencia boot system incorrecta o ausente
- Un valor incorrecto en el registro de configuración
- Una imagen dañada en la memoria flash
- Un fallo en el hardware

Cuando el router arranca, busca en el archivo de configuración una sentencia boot system. Esta sentencia puede obligar al router a arrancar desde otra imagen en lugar de hacerlo desde la imagen del IOS almacenada en la memoria flash. Para identificar el origen de la imagen de arranque, ejecute el comando show versión y busque la línea que identifica el origen de la imagen de arranque

Router#show version
Cisco IOS Software, C1700 Software (C1700-IPBASEK9-M), Version 12.4(10), RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Tue 15-Aug-06 23:47 by prod_rel_team
ROM: System Bootstrap, Version 12.2(7r)XM1, RELEASE SOFTWARE (fc1)

Una configuración errónea del registro de configuración impide que el IOS se cargue desde la memoria flash, el valor del registro de configuración le indica al router donde obtener la imagen del IOS. Esto puede confirmarse con el comando show versión y observando la ultima línea del registro de configuración

Router#show version
Configuration register is 0x2102
Router#

En la siguiente tabla se describen otros comandos útiles sobre el estado del router

Comando	**Descripción**
Show versión	Muestra la configuración de hardware del sistema, la versión del software, los nombres y los orígenes de los archivos de configuración, las imágenes de arranque e indica la razón por la que l sistema arrancó la ultima vez
Show processes	Muestra información acerca de los procesos activos
Show protocols	Muestra protocolos configurados. Este comando muestra el estado de cualquier protocolo de capa 3 configurado
Show memory	Muestra estadísticas sobre la memoria del router, incluyendo estadísticas de memoria libre
Show stacks	Monitoriza el uso de la pila de procesos y rutinas de interrupción
Show buffers	Proporciona estadísticas para los almacenes de búfer del router
Show flash	Muestra información sobre el dispositivo de memoria flash
Show running-config	Muestra el archivo de configuración activo
Show startup-config	Muestra el archivo de configuración en copia de seguridad
Show interface	Muestra estadísticas para todas las interfaces configuradas

El valor correcto varía en las diferentes plataformas hardware. La documentación del software Cisco IOS debe incluir una copia impresa de la salida del comando *show versión*. Si no se tiene acceso a esta documentación hay recursos en el CD de documentación de Cisco o en cisco.com para identificar el valor correcto del

registro de configuración. Corrija el error cambiando el registro de configuración y almacene este último como configuración de inicio

Si el problema persiste, el router podría tener dañado un archivo de imagen en la memoria flash. Si es el caso, deberá aparecer un mensaje de error durante el arranque. El mensaje de error podría visualizarse de esta forma
Open: read error…requested 0x4 bytes, got 0x0
Troble reading device magic number
Boot: cannot open “flash:”
Boot: cannot determine first file name on device “flash:”ú

Si la imagen en la memoria flash está dañada, se debe cargar un nuevo IOS en el router. Si el problema no se ha identificado en esta sección, el router podría tener un problema de hardware, si es el caso se deben retirar todas las tarjetas de aplicaciones del Router, si aún después de retirarlas y volver a encender el equipo este no responde o se queda bloqueado después de un tiempo, hay un error en la Motherboard del equipo por lo que lo único que queda por hacer es cambiar el chasis. En caso contrario se deben meter una a una las tarjetas de aplicaciones para determinar cual es la que esta ocasionando conflictos al equipo cabe mencionar que para instalar una tarjeta el router debe estar apagado de lo contrario se corre el riesgo de dañar tanto la tarjeta como el modulo

Resolución de problemas en una interfaz serie
Otro de los problemas más frecuentes que se presentan en los Router’s es la perdida de comunicación, dicha perdida de comunicación puede ser atribuida a distintos factores.
La salida del comando *show interfaces serial* muestra información especifica de las interfaces serie. Se utiliza e comando *show interface serial* para verificar la configuración adecuada de la encapsulación HDLC o PPP. Cuando está

configurado HDLC debe aparecer *Encapsulation HDLC* en la salida del comando *show interface serial*

```
FES_A#show interfaces serial 0
Serial0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 200.20.2.1/24
  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 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     176 packets input, 10038 bytes, 0 no buffer
     Received 41 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     145 packets output, 11082 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 output buffer failures, 0 output buffers swapped out
     5 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
FES_A#
```

Cuando está configurado PPP

```
FES_A#show interfaces serial 0
Serial0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 200.20.2.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
  Keepalive set (10 sec)
  LCP Open
  Open: IPCP, CDPCP
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:02:53
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 1000 bits/sec, 3 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     195 packets input, 9597 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
     272 packets output, 14426 bytes, 0 underruns
     0 output errors, 0 collisions, 5 interface resets
     0 output buffer failures, 0 output buffers swapped out
     10 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

En la siguiente tabla se identifican los posibles estados de problema que pueden presentarse en la línea de estado de la interfaz de la salida *show interface serial*

Serial x is down, line protocol is down
Serial x is up, line protocol is down
Serial x is up, line protocol is up (looped)
Serial x is up, line protocol is down (disabled)
Serial x is administratively down, line protocol is down

Posible estado del problema

Línea de estado	**Posible condición**	**Solución del problema**
Serial x is up, line protocol is up	Es la condición de línea de estado adecuada	No es necesaria acción alguna
Serial x is down, line protocol is down	El router no intuye una señal CD, (Es decir, el CD está inactivo). Se ha producido un problema en la compañía telefónica; la línea se ha caído o no está conectada al módem (CSU/DSU) El cableado es defectuoso o incorrecto.	1. Comprobar los leds del MODEM para ver si el CD está activo, o inserte una caja de registro en la línea para comprobar la señal de CD 2. Comprobar que se están utilizando el cable t la interfaz adecuados (Consultar la documentación de instalación de hardware) 3. Insertar una caja de registro y comprobar todos los leds de control

	Se ha producido un fallo de hardware	4. Contactar al proveedor de línea alquilada o de otro servicio para saber dónde esta el problema 5. Intercambiar las partes que fallan 6. Si sospecha que es defectuosos el hardware del router, cambie la línea serie a otro puerto. Si la conexión se activa, la interfaz anteriormente conectada tiene un problema
Serial x is up, line protocol is down	El router local o remoto esta mal configurado El router remoto no está enviando mensajes de actividad Se ha producido un problema en la línea alquilada o en otro servicio del proveedor (ruido en la línea, mala configuración o falla en el switch) Hay un problema de sincronía en el cable	1. Poner el módem en el modo de loopback local y ejecutar el comando show interfaces serial para determinar si el protocolo de línea de activa. Si se activa el protocolo de línea, el problema es probablemente de la compañía telefónica o un fallo en el router remoto 2. Si el problema parece estar en el extremo remoto, repetir el paso 1 en e módem remoto. 3. Comprobar todo el cableado. Cerciorarse de que el cable

	Ha fallado un módem local o remoto Ha fallado el hardware del router local o remoto	este conectado a la interfaz correcta, al módem apropiado y al punto de terminación de red de la compañía telefónica apropiado. Utilizar el comando *show controllers* para determinar qué cable está conectado a qué interfaz 4. Habilitar el comando EXEC debug serial interface 5. Si el protocolo de línea no se activa en el modo de loopback local, y la salida del comando EXEC *debug serial interface* muestra que el contador de actividad no se incrementa, es probale que halla un problema con el hardware del router. Intercambiar el hardware de la interfaz del router 6. Si el protocolo de línea se activa y se incrementa el contador de actividad, el problema no está en el router local 7. Si sospecha que hay un fallo en el hardware del router,

		cambie la línea serie a un puerto que no este utilizando. Si la conexión se reestablece, la interfaz conectada anteriormente tiene un problema
Serial x is up, line protocol is down (Modo DCE)	El comando de configuración de interfaz *clock rate* ha desaparecido	1. Añadir el comando de configuración de interfaz clock rate en la interfaz serie Clock rate bps Bps es la velocidad de reloj deseada en bits por segundo 1 200; 2 400, 4 800, 9 600, 38 400, 56 000, 64 000, 72 000, 125 000, 148 000, 250 000, 500 000, 800 000, 1 000 000, 1 300 000, 2 000 000, 4 000 000 u 8 000 000
	El dispositivo DTE no soporta o no está configurado para el modo SCTE (Temporización terminal)	2. Si es posible, establecer el dispositivo DTE a un Módem SCTE (Transmisión de reloj serie externo), Si el CSU/DSU no soporta SCTE, se debe de desactivar SCTE en la interfaz del router Cisco
	La CSU o DSU remota ha fallado	3. Verifique que está utilizando el cable correcto 4. Si el protocolo de línea todavía esta caído, es

		posible que haya un fallo de hardware o un problema en el cableado. 5. Sustituir las partes que fallan, si es necesario.
Serial x is up, line protocol is up (looped)	Existe un bucle en el circuito, el número de secuencia en el paquete de actividad cambia a un número aleatorio cuando inicialmente se ha detectado el bucle. Si por el enlace se devuelve el mismo numero aleatorio, existe un bucle	1. Utilice el comando EXEC privilegiado *show running-config* para buscar cualesquiera entradas del comando de configuración de interfaz loopback 2. Si se encuentra una entrada del comando de configuración de interfaz loopback, utilizar el comando de configuración de interfaz *no loopback* para eliminar el bucle 3. Si no se encuentra el comando de configuración de interfaz loopback, examine la CSU/DSU para determinar si están configuradas en el modo de loopback manual. Si es así, deshabilitar el loopback manual 4. Restablezca la CSU/DSU e inspeccionar el estado de la línea. Si el protocolo de la

		línea se activa, no es necesaria ninguna otra acción 5. Si la CSU/DSU no está configurada en el modo loopback manual, contactar al proveedor de de la línea alquilada o de otro servicio para recibir asistencia para la resolución de problemas con la línea
Serial x is up, line protocol is down (disabled)	Se ha producido un error de velocidad debido a un problema en el servicio de la compañía telefónica. El hardware del router es erroneo (Interfaz)	1. Solucionar los problemas de la línea con un analizador serie y una caja de registro. *2.* Bucle CSU/DSU (Bucle DTE). Si el problema persiste es posible que haya un problema con el hardware. Si el problema no continua, es probable que se trate de un problema en la compañía telefónica *3.* Sustituya el hardware defectuoso, según sea necesario (Router local o remoto, CSU/DSU, switch)
Serial x is administratively down, line	La configuración del router incluye el comando de	1. Compruebe la configuración del router para el comando *shutdown*

protocol is down	configuración de interfaz shutdown. Existe una dirección IP duplicada	2. Utilizar el comando de configuración de interfaz *no shutdown* para eliminar el comando *shutdown* 3. Verificar que no hay direcciones IP idénticas utilizadas por el comando EXEC privilegiado *show running-config* o el comando EXEC *show interfaces* 4. Si hay direcciones duplicadas, resolver el conflicto cambiando una de las direcciones IP

El comando EXEC *show controllers* es otra importante herramienta de diagnostico para solucionar problemas con las líneas serie. La sintaxis del comando, dependiendo de la plataforma es la siguiente:

- Para las interfaces serie de los router serie cisco 7000 se utiliza el comando EXEC *show controllers cbus*

- Para los productos de acceso Cisco series 1700, 2000, 2500, 2600, 3000 y 4000, se utiliza el comando EXEC *show controllers.*

Router#show controllers serial 0/0
Interface serial0/0
Hardware is PowerQUICC MPC860
DTE V.35 TX and RX clocks detected

Idb at 0x81414E2C, driver data structure at 0x8141753Cl
SCC Registers:
General [GSMR]=0x0000, Protocol-specific [PSMR]=0x8
Events [SCCE]=0x0000, Mask [SCCM]=0x001F, Status [SCCS]=0x06
Transmit on Demand [TODR]=0x0, Data Sync [DSR]=0x7E7E

La salida de *show controllers* indica el estado de los canales de la interfaz y si hay conectado un cable a la interfaz. Se observa que en la interfaz serie 0/0 hay conectado un cable V.35 DTE

Si la interfaz aparece como UNKNOWN (en lugar de V.35, EIA/TIA-449 o algún otro tipo de interfaz serial), probablemente el problema se deba a un cable mal conectado. También es posible un problema la tarjeta. Si se desconoce el puerto de la interfaz, la correspondiente visualización del comando EXEC *show interfaces* muestra que la interfaz y código de línea están caídos.

A continuación se enumeran algunos comandos debug que resultan útiles para resolver problemas serie y WAN:

- *Debug interface serial 0/0*. Verifica si los paquetes de actividad HDLC se están incrementado. Si no es así, puede haber un problema de temporización en la tarjeta de interfaz o en la red.

Router#debug interface serial 0/0
Serial network interface debugging i son
Router#
00:06:47: Serial0/0: HDLC myseq 29, mineseen 29*, yourseen 29, line up
00:06:57: Serial0/0: HDLC myseq 30, mineseen 30*, yourseen 30, line up
00:07:07: Serial0/0: HDLC myseq 31, mineseen 31*, yourseen 31, line up
00:07:17: Serial0/0: HDLC myseq 32, mineseen 32*, yourseen 32, line up
Router#undebug all
All possible debugging has been turned off
Router#

- *Debug arp.* Indica si el router esta enviando información acerca o aprendiendo sobre los routers (con paquetes arp) en el otro lado de la nube WAN. Se recomienda usar este comando cuando alguno de los nodos de una red TCP/IP estén respondiendo y otros no

- *Debug frame-relay lmi*. Proporciona información LMI (Interfaz de Administración local) que resulta útil para determinar si un switch frame-relay y un router están enviando y recibiendo paquetes LMI

- *Debug ppp negotiation*. Muestra paquetes PPP que se transmiten durante el inicio de PPP, donde se negocian las opciones PPP

- *Debug ppp* packet. Muestra paquetes PPP que están enviándose y recibiéndose. Este comando muestra volcados de paquete de bajo nivel

- *Debug ppp errors*. Muestra los errores PPP (como las tramas ilegales o mal formadas) que están asociadas con la negociación y el funcionamiento de una conexión PPP

- *Debug ppp chap*. Muestra los intercambios de paquetes PPP CHAP y PPP PAP.

NOTA. Como a la salida de la depuración se le asigna una depuración alta en el proceso CPU, puede inutilizable al sistema. Por esta razón, los comandos debug solo deben utilizarse para resolver problemas específicos o durante las sesiones de solución de problemas. Además, es mejor utilizar los comandos debug durante periodos de escaso tráfico en la red y pocos usuarios. La depuración durante esos periodos reduce la posibilidad de que un aumento en la carga de procesamiento del comando debug afecte al uso del sistema.

Conclusiones

Resulta sorprendente comprobar lo rápido que ha cambiado la tecnología informática en los últimos 10 años. Lo que antes parecía una tecnología demasiado cara o compleja para las pequeñas y medianas empresas, ahora esta siendo aceptada a una velocidad de vértigo.

Los dispositivos de conexión entre redes y, en particular, los routers, son algunas de las tecnologías de las que se servían las antiguas “grandes compañías” a las que ahora recurren incluso las empresas más modestas.

Los routers baratos de gama baja proporcionan conexión a los proveedores de servicio y a la red pública telefónica a las pequeñas compañías que buscan mayor ancho de banda ahora que Internet se ha impuesto como una herramienta de comunicación y marketing.

Con el constante crecimiento de las empresas el objetivo perseguido también se refiere a las estrategias necesarias para conservar en ancho de banda de las propias redes de área local (LAN); y de hecho la segmentación de LAN con routers se ha convertido en una solución viable y muy eficiente en términos de coste.

Para la administración de una red es saber configurar el router por eso el sistema operativo IOS y el archivo de configuración son las dos cosas en las que se debe de poner mayor atención para administrar los routers, estos cambios y movimientos se llevan a acabo con comandos. Por su puesto además de dos modos de operación del enrutador que se dividen en 7, las tres primeras son modos de inicio y los cuatro restantes se suelen llamar habilitados incluso dentro de estos hay tres de operación de inicio de sistema que te dicen que comandos hay que usar y que parte del router hay que actualizar. Como pueden ser el config-maker herramienta de gama media para LAN y conectividad con WAN.

Como en la mayoría de las empresas las fallas se hacen presentes por razones muy diversas por eso es importante tomar en cuenta y prevenir fallas desde las más comunes hasta las menos esperadas, saber localizarlas, tener la paciencia y la habilidad de encontrarlas y resolver fallas, por eso Cisco tiene un sistema muy amigable para interactuar con el software y directamente con el hardware

El mantenimiento de una red debe ser constante por eso debemos conocer las fallas y las soluciones más comunes para actuar en forma efectiva sin perdida de tiempo ni esfuerzo, los protocolos de enrutamiento solucionan problemas de forma automática sin esperar la intervención del administrador de la red, con esto se prueba que el acceso a través del IOS ayuda enormemente a la solución del problema por medio de comandos que ayudan a identificar los fallos como son el acceso a equipos, malas configuraciones, rendimientos de la red, la solución puede comenzar desde la más sencilla como checar direcciones IP, comparándolos con ejecución de comandos para tener una buena configuración, se debe hacer un PING, estados de conexión el protocolo de la línea prueba, si esta bien la interfaz de línea, probar la lista de acceso que prueba si se configuró bien el router que son las cuestiones más comunes.

Otra forma de ver el equipo es a través de la inspección física de los equipos, checar las interfaces, los cables, alimentación, luces y cuando sean más intensos los problemas se requerirá una inspección interna del equipo para encontrar la falla y resetear el equipo para volverlo a encender.

Con esta explosión de la tecnología de conexión entre redes en el mundo empresarial, los profesionales se han visto obligados no solo a configurar y manipular router, sino también a resolver los posibles problemas que pudieran plantear estos y otro tipo dispositivos de conexión entre redes. Aunque ya existen excelentes manuales y materiales de formación acerca de la conexión entre redes

y los productos de cisco, casi todos ellos van dirigidos A los profesionales de las tecnologías de la información con muchos años de experiencia y formación a sus espaldas.

Faltaba por llegar una tesis introductoria al que los profanos en la materia pudieran remitirse sin problemas.

Bibliografía

- **ROUTERS CISCO. Joe Habraken. Editorial Prentice Hall 1ª Edición Madrid, 2000**

- **ACADEMIA DE NETWORKING DE CISCO SYSTEMS CCNA 1 Y 2. Autor CISCO PRESS. Editorial Pearson Educación 1ª Edición Madrid, 2004**

- **GUIA DEL SEGUNDO AÑO CCNA 3 Y 4: EL UNICO LIBRO DE TEXTO AUTORIZADO POR EL PROGRAMA DE LA ACADEMIA DE NETWORKING DE CISCO SYSTEMS. David Fayerman Aragon. Editorial Pearson Educación de México 3ª Edición México, 2004**

- **INTERCONEXIÓN DE DISPOSITIVOS DE RED CISCO. Steve McQuerry. Editorial Pearson Educación 1ª Edición Madrid, 2001**

- **www.cisco.com**

- **www.garciagaston.com.ar**

- **http://cisco.com/web/psa/products/tsd_products_support_troubleshoot_and_alerts.html**

- **http://cisco.com/web/psa/products/tsd_products_support_configure.html**

- **http://cisco.com/web/psa/products/tsd_products_support_install_and_upgrade.html**