Dto:	Operación y red	Proyecto:	CCNA
Autor:	Elva y Chechu	Fecha:	01/04/02
Asunto:	Preparación para certificación CCNA Cisco Systems		
Estado:	Pendiente revisión	Revisión:	1.0

INTERCONEXIÓN DE DISPOSITIVOS DE RED CISCO

CCNA #640-507

Autores: ELVA y CHECHU

CISCO SYSTEMS

TABLA DE CONTENIDOS

CONCEPTOS GENERALES DE INTERCONEXIÓN

El objetivo de este capitulo es repasar los conceptos básicos del **internetworking**. Estos conceptos serán utilizados a lo largo del documento y son fundamentales para comprender las funciones de los dispositivos.

DEFINICIÓN DE CONCEPTOS DE RED

El objetivo de una red de datos consiste en facilitar la consecución de un incremento de la productividad vinculando 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.

Las redes de datos han cambiado nuestra forma de ver nuestras empresas y empleados. Ya no es necesario mantener una ubicación común para todos los empleados si se quiere acceder a la información que estos necesitan para desarrollar su trabajo. Debido a esto, hay muchas organizaciones que han cambiado sus estrategias comerciales para utilizar estas redes de la forma en que llevan a cabo su actividad empresarial. Hoy día es frecuente que una empresa organice el **internetworking** corporativo de tal forma que permita optimizar sus recursos. La figura 1.1 muestra que la red está definida en función de agrupamientos de empleados(usuarios), siguiendo los siguientes criterios:

- La oficina principal es aquella donde todos están conectados a una LAN y donde está ubicada la mayoría de la información corporativa. Una oficina principal podría contar con cientos o miles de usuarios que dependen de la red para desarrollar su trabajo. La oficina principal podría consistir en un edificio con muchas redes de área local(LAN), o bien en un campus de edificaciones de ese estilo. Dado que todos los usuarios necesitan acceder a recursos e información centralizados, es habitual encontrarse con una LAN backbone de alta velocidad, así como un centro de datos general con computadoras mainframe y servidores de aplicaciones.

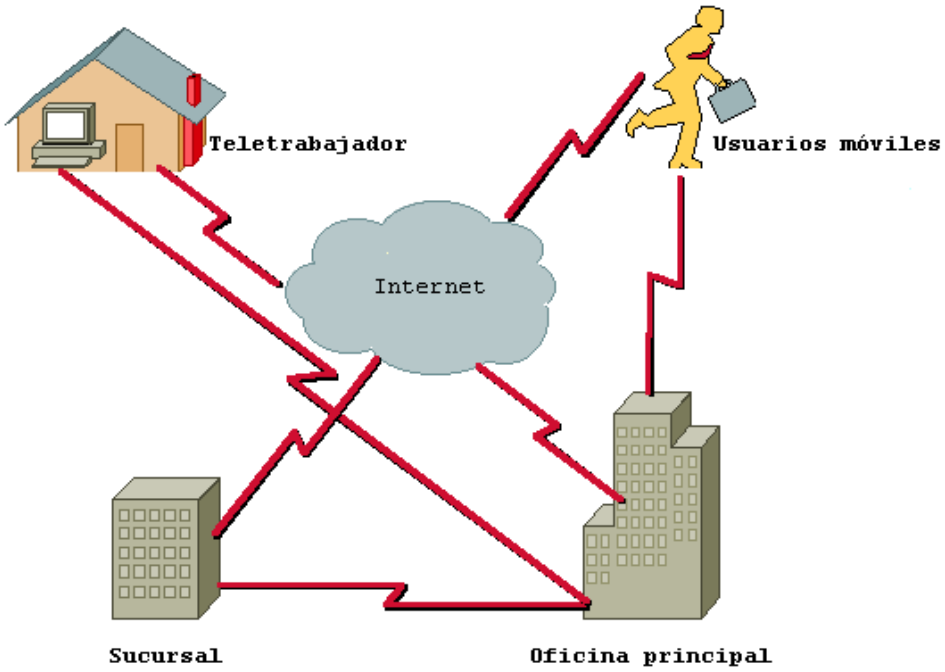
- Las demás conexiones consisten en una diversidad de ubicaciones de acceso remoto que necesitan conectarse a los recursos de las oficinas principales y/o entre ellas, incluidas las siguientes:

- **Sucursales**. Se trata de ubicaciones remotas donde trabajan grupos más reducidos de individuos. Estos usuarios se conectan entre si por medio de una LAN. Para acceder a la oficina principal, los usuarios utilizan servicios de redes de área amplia(WAN). Aunque parte de la información podría estar almacenada en la sucursal, lo más probable es que los usuarios tengan que acceder a la mayoría de los datos desde la oficina principal. La frecuencia con la que se accede a la red de la oficina principal determina si las conexiones WAN deben ser permanentes, o bien mediante acceso telefónico.

- **Teletrabajadores.** Se trata de empleados que trabajan desde sus domicilios. Estos usuarios requieren, generalmente, conexiones puntuales(bajo demanda) con la oficina principal y/o sucursal para acceder a los recursos de la red.

- **Usuarios móviles**. Se trata de individuos que trabajan desde distintas ubicaciones y dependen de distintos servicios para poder conectarse a la red. Cuando están en las oficinas principales o sucursales, estos usuarios se conectan a la LAN. Cuando se encuentran fuera de la oficina, normalmente dependen de servicios de acceso telefónico para conectarse a la red corporativa.

Figura 1.1 Estrategia de redes corporativas.

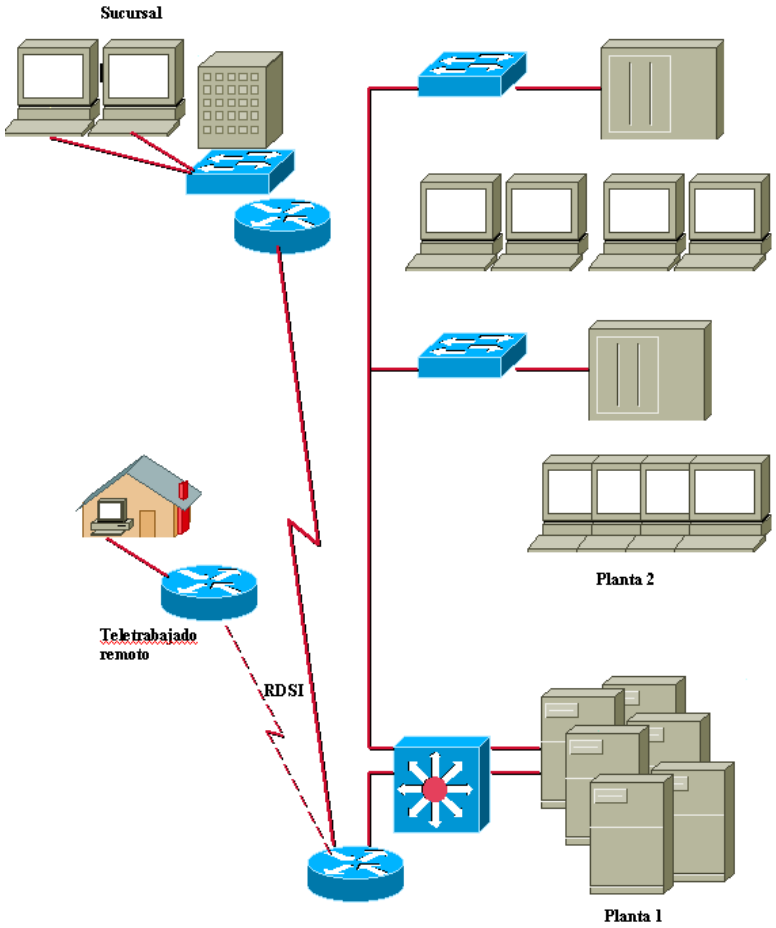


Para conocer los tipos de equipo y servicios que es necesario implementar en un red y cuándo deben utilizarse, es importante tener en cuenta las necesidades comerciales y de los usuarios. Esto permite subdividir la red en un modelo jerárquico que se expande desde el equipo de usuario final hasta el núcleo(backbone) de la red.

Para subdividir un **internetworking** de redes en componentes más pequeños, Cisco utiliza un modelo jerárquico de tres niveles(capas), como se describe en el siguiente apartado.

Dto:	Operación y red	Proyecto:	CCNA
Autor:	Elva y Chechu	Fecha:	01/04/02
Asunto:	Preparación para certificación CCNA Cisco Systems		
Estado:	Pendiente revisión	Revisión:	1.0

Figura 1.2 Interconexión de grupos



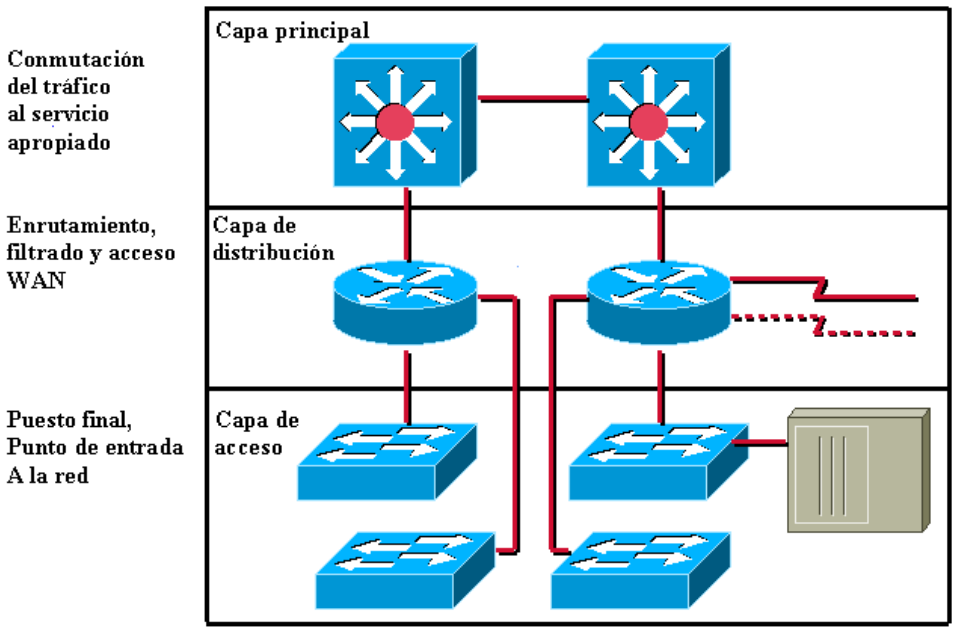
ADAPTACIÓN DE LAS NECESIDADES DE EMPRESA A UN MODELO JERÁRQUICO

Con el fin de simplificar el diseño, implementación y administración de las redes, cisco utiliza un modelo jerárquico para describir la red. Aunque la práctica de este método suele estar asociado con el proceso de diseña de una red, es importante comprender el modelo para poder determinar el equipo y características que van a necesitar en la red.

Tradicionalmente, las redes de campus han colocado la logística y servicios básicos a nivel de red en el centro de la red, compartiendo el ancho de banda a nivel de usuario. Sin embargo, conforme el desarrollo comercial se va apoyando cada vez más en la red como herramienta de productividad, los servicios de red distribuidos y la conmutación van migrando hasta el nivel de puesto de trabajo.

Las demandas del usuario y las aplicaciones de red han obligado a los profesionales de las redes a utilizar patrones de tráfico en la red como criterio para construir un **internetworking**. Las redes no pueden ser divididas en subredes basándose únicamente en el número de usuarios. La aparición de servidores capaces de ejecutar aplicaciones globales tiene también una incidencia directa en la carga de la red. Un tráfico elevado en la red global supone tener que emplear técnicas de enrutamiento y conmutación más eficaces.

Figura 1.3



Modelo jerárquico de red basado en tres capas.

Los patrones de tráfico son hoy día los que dictan el tipo de servicios necesarios para los usuarios finales de la red. Para construir correctamente un **internetworking** de redes que pueda dar una respuesta eficaz a las necesidades de un usuario, se utiliza un modelo jerárquico de tres capas para organizar el flujo de tráfico(véase la figura 1.3).

El modelo consta de tres capas:

- Acceso.
- Distribución.
- Núcleo principal.

Cada una de estas capas tiene una función en el suministro de servicios de red, como se describe en los siguientes apartados.

CAPA DE ACCESO

La capa de acceso de la red es el punto en el que cada usuario se conecta a la red. Ésta es la razón por la cual la capa de acceso se denomina a veces capa de puesto de trabajo. Los usuarios, así como los recursos a los que estos necesitan acceder con más frecuencia, están disponibles a nivel local. El tráfico hacia y desde recursos locales está confinado entre los recursos, switches y usuarios finales. En la capa de acceso podemos encontrar múltiples grupos de usuarios con sus correspondientes recursos.

En muchas redes no es posible proporcionar a los usuarios un acceso local a todos los servicios, como archivos de bases de datos, almacenamiento centralizado o acceso telefónico al web. En estos casos, el tráfico de usuarios que demandan estos servicios se desvía a la siguiente capa del modelo: la capa de distribución.

CAPA DE DISTRIBUCIÓN

La capa de distribución de la red(denominada a veces de grupo de trabajo) marca el punto medio entre la capa de acceso y los servicios principales de la red. La función primordial de esta capa es realizar funciones tales como enrutamiento, filtrado y acceso a WAN. En un entorno de campus, la capa de distribución abarca una gran diversidad de funciones, entre las que figuran las siguientes:

- Servir como punto de acumulación para acceder a los dispositivos de capa.
- Erutar el tráfico para proporcionar acceso a los departamentos o grupos de trabajo.
- Segmentar la red en múltiples dominios de difusión / multidifusión.
- Traducir los diálogos entre diferentes tipos de medios, como Token Ring y Ethernet.
- Proporcionar servicios de seguridad y filtrado.

La capa de distribución puede resumirse como la capa que proporciona una conectividad basada en una determinada política, dado que determina cuándo y cómo los paquete pueden acceder a los servicios principales de la red. La capa de distribución determina la forma más rápida para que la petición de un usuario(como un acceso al servidor de archivos) pueda ser remitida al servidor. Una vez que la capa de distribución ha elegido la ruta, envía la petición a la capa del núcleo principal. La capa principal podrá entonces traspasar rápidamente la petición al servicio apropiado.

CAPA DEL NÚCLEO PRINCIPAL

La capa del núcleo principal(también llamada capa backbone), se encarga de desviar el tráfico lo más rápidamente posible hacia los servicios apropiados. Normalmente, el tráfico transportado se dirige o proviene de servicios comunes a todos los usuarios. Estos servicios se conocen como servicios globales o corporativos. Algunos de tales servicios pueden ser e-mail, el acceso a Internet o la videoconferencia.

Cuando un usuario necesita acceder a un servicio corporativo, la petición se procesa al nivel de la capa de distribución. El dispositivo de la capa de distribución envía la petición del usuario al núcleo. Este se limita a proporcionar un transporte rápido hasta el servicio corporativo solicitado. El dispositivo de la capa de distribución se encarga de proporcionar un acceso controlado al núcleo.

Para construir una red de forma eficaz, es necesario entender en primer lugar cómo se utiliza el **internetworking** de redes, las necesidades corporativas y las demandas de los usuarios. Estas necesidades pueden ser adaptadas a un modelo que pueda usarse para construir el **internetworking** de redes.

Una de las mejores formas de comprender cómo construir un **internetworking** de redes pasa por asimilar la forma en que el tráfico circula a través de la red. Esto se consigue por medio de un marco de trabajo de red conceptual, el más popular de los cuales es el modelo de referencia OSI. Éste se describe posteriormente.

EL MODELO DE REFERENCIA OSI

El modelo de referencia OSI ofrece varias funciones a la comunidad que participa del **internetworking:**

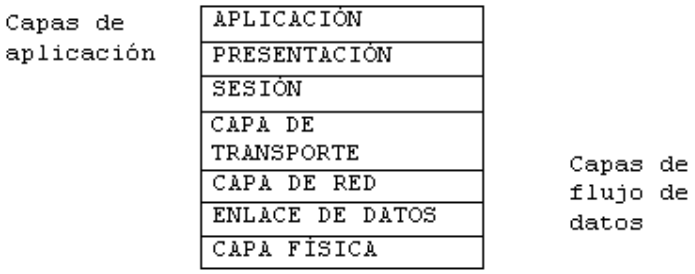
- Proporciona una forma de entender cómo opera un **internetworking** de redes.
- Sirve de guía o marco de trabajo para crear e implementar estándares de red, dispositivos y esquemas de **internetworking.**

Estas son algunas de las ventajas de utilizar un modelo estructurado en capas.

- Separa la compleja operación de **internetworking** en elementos más simples.
- Permite a los ingenieros centrarse en el diseño y desarrollo de funciones modulares.
- Proporciona la posibilidad de definir interfaces estándar para compatibilidad "plug-and-play" e integración multifabricante.

El modelo de referencia OSI consta de siete capas. Las cuatro capas de nivel inferior definen rutas para que los puestos finales puedan conectarse unos con otros y poder intercambiar datos. Las tres capas superiores definen cómo han de comunicarse las aplicaciones de los puestos de trabajo finales entre ellas y con los usuarios.

Figura 1.4 Modelo de referencia OSI



En los siguientes apartados se desglosan las capas y se describe cómo funcionan para conseguir la conectividad en la red.

CAPAS SUPERIORES

Las tres capas del modelo de referencia OSI se denominan habitualmente capas de **aplicación**. Estas capas están relacionadas con la interfaz de usuario, formatos y acceso a las aplicaciones. La figura 1.5 ilustra las capas superiores y proporciona información acerca de su funcionalidad con algunos ejemplos.

- **Capa de aplicación**. Es la capa de nivel superior del modelo. Aquí, el usuario o la aplicación dialoga con los protocolos para acceder a la red. Por ejemplo, se accede a un procesador de textos por el servicio de transferencia de archivos de esta capa.

- **Capa de presentación.** La capa de presentación proporciona diversas funciones de conversión y codificación que se aplican a los datos de la capa de aplicación. Estas funciones aseguran que los datos enviados desde la capa de aplicación de un sistema podrán ser leídos por la capa de aplicación de otro sistema. Un ejemplo de funciones de codificación sería el cifrado de datos una vez que éstos salen de una aplicación. Otro ejemplo podrían ser los formatos de imágenes jpeg y gif que se muestran en paginas web. Este formato asegura que todos los navegadores web podrán mostrar las imágenes, con independencia del sistema operativo utilizado.

Figura 1.5 Capas superiores.

Aplicación	Interfaz de usuario	Telnet HTTP
Presentación	Presentación de datos Proceso especial como cifrado	ASCII EBCDIC JPEG
Sesión	Mantener separados datos de distintas aplicaciones	Sistema operativo/ Programa de acceso a aplicaciones
Transporte		
Capa de red		
Enlace de datos		
Capa física		

- **Capa de sesión**. La capa de sesión es la responsable de establecer, administrar y concluir las sesiones de comunicaciones entre entidades de la capa de presentación. La comunicación en esta capa consiste en peticiones de servicios y respuestas entre aplicaciones ubicadas en diferentes dispositivos. Un ejemplo de este tipo de coordinación podría ser el que tiene lugar entre un servidor y un cliente de base de datos.

CAPAS INFERIORES

Las cuatro capas inferiores del modelo de referencia OSI son las responsables de definir cómo han de transferirse los datos a través de un cable físico, por medio de dispositivos de **internetworking**, hasta el puesto de trabajo de destino y, finalmente, hasta la aplicación que está al otro lado. La figura 1.6 resume las funciones básicas de estas cuatro capas. Posteriormente, describiremos con más detalle cada una de estas capas.

COMUNICACIÓN ENTRE CAPAS DEL MODELO DE REFERENCIA OSI

Es responsabilidad de la pila de protocolo proporcionar comunicación entre los distintos dispositivos de la red. Una pila de protocolo es el conjunto de reglas que definen cómo ha de viajar la información a través de la red. Un ejemplo de esto podría ser TCP/IP. El modelo de referencia OSI proporciona un marco común necesario para la mayoría de las pilas de protocolo.

Aplicación		
Presentación		
Sesión		
Transporte	Distribución fiable o no fiable 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	802.3 802.2 HDLC
Física	Trasladar bits entre dispositivos Especificar voltaje, velocidad y patillaje de cable.	EIA/TIA-232 V.35

Figura 1.6 Capas inferiores

Cada capa del modelo permite que los datos circulen a través de la red. Estas capas intercambian información para proporcionar la debida comunicación entre los dispositivos de red. Las capas se comunican entre sí a usando unidades de datos del protocolo(PDU). Estas PDU controlan información que se agrega a los datos del usuario. La información de control reside en campos denominados **cabecera** e **información final**. En la figura 1.7, la cabecera MAC(Control de acceso al medio) y la secuencia de verificación de trama (FCS) de la capa de enlace de datos representa una cabecera y una información final.

Debido a que la PDU puede incluir información diferente según suba o baje por las capas, se le asignan nombres con arreglo al tipo de información que transporta. Por ejemplo, en la pila de protocolos TCP/IP(véase la figura 1.7), una vez que se ha agregado una cabecera TCP de capa de transporte a los datos de la capa superior, dicha unidad se denomina **segmento**. El segmento se baja entonces a la capa de red, donde se le añade una cabecera IP, convirtiéndose en un **paquete.** El paquete se inserta en una cabecera de capa ", convirtiéndolo en una **trama**. Por último, la trama se convierte en bits y las señales eléctricas se transmiten a través del medio de la red.

Este método de bajar datos a la pila y agregar cabeceras e información final se denomina **encapsulado**. Una vez que los datos han sido encapsulados y pasados a través de la red, el dispositivo receptor quita toda la información agregada, usando los mensajes de la cabecera como instrucciones para subir los datos de la pila hasta la aplicación apropiada.

El encapsulado de datos es un concepto muy importante en redes. Su función es describir cómo comunican las capas de cada dispositivo, llamadas capas **iguales**, parámetros críticos como una dirección e información de control.

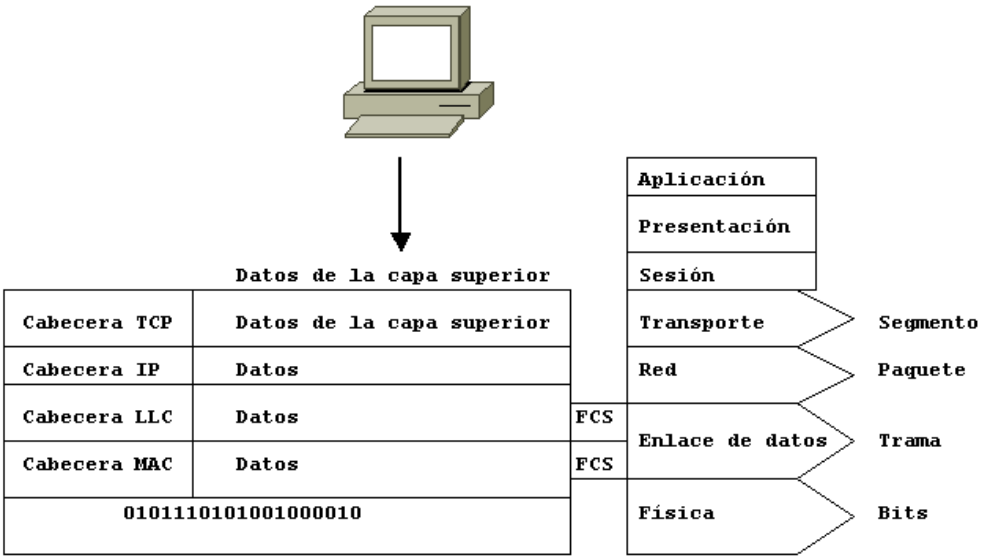


Figura 1.7 Encapsulado de datos.

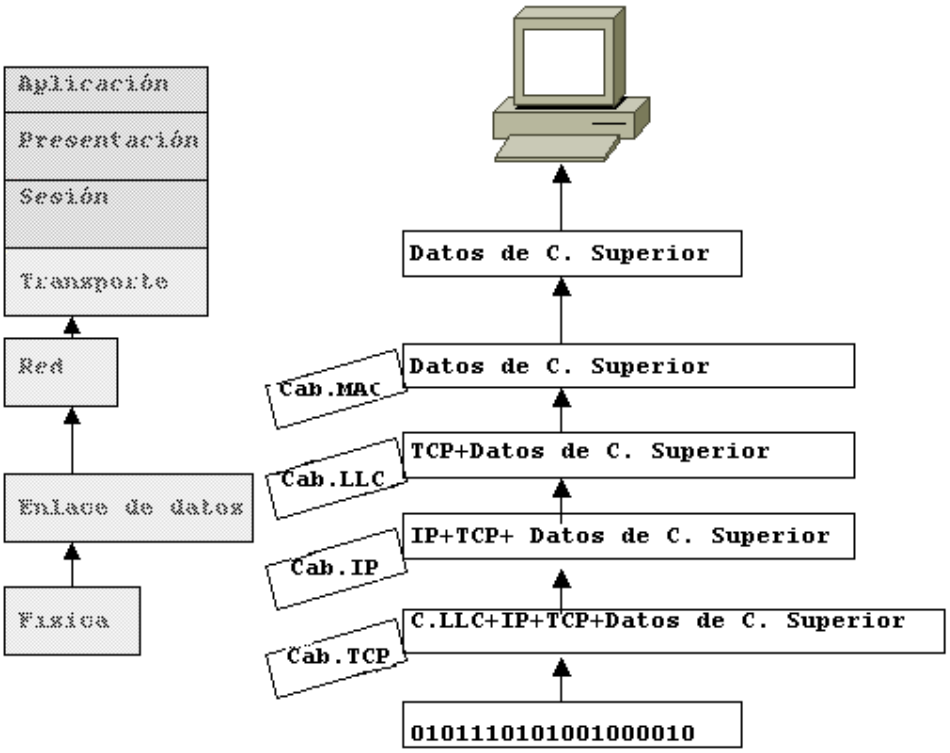
Aunque el encapsulado puede parecer un concepto muy abstracto, en realizad es muy simple. Imagine que desea enviar una taza de café a un amigo que reside en otra ciudad.

¿Cómo llegaría la taza a su destino? Básicamente, sería transportada por carretera o por aire. No tendría sentido salir y colocar la taza en la carretera o lanzarla al aire esperando que llegue a su destino. Se necesita un servicio que se encargue de recogerla y entregarla. Así, llamaría a su agencia de transportes de confianza y le entregaría la taza. Pero eso no es todo. Necesita también proporcionar al transportista la información necesaria acerca del destino de la taza. Así, deberá facilitar a la agencia la dirección de entrega para usar ese medio de transporte. Pero, previamente, tendrá que empaquetar la taza. Este sería el proceso completo:

Paso 1 Empaquetar la taza.
Paso 2 Pegar una etiqueta con la dirección en la caja.
Paso 3 Dar la taza a una agencia de transportes.
Paso 4 La agencia transporta el material.

Este proceso es parecido al método de encapsulado que utilizan las pilas de protocolo para enviar datos a través de las redes. Una vez que reciba el paquete, su amigo tendrá que recorrer parte del proceso a la inversa. Tomará el paquete de manos del transportista, leerá la etiqueta para descubrir quién se lo envía y por ultimo, quitará el embalaje para extraer la taza. El proceso inverso del encapsulado se denomina desencapsulado. La figura 1.8 ilustra el proceso de desencapsulado en una pila de protocolo.

Figura 1.8 Desencapsulado.



Como profesionales de las redes, nuestra responsabilidad consiste en implementar redes que permitan el transporte de los datos de los usuarios. Para poder implementar y configurar dispositivos que se encarguen de esta tarea, es necesario entender bien el proceso de las capas inferiores del modelo OSI. Comprendiendo bien este proceso, la configuración y resolución de conflictos relacionados con dispositivos de red serán manos problemáticas.

FUNCIONES DE LA CAPA FÍSICA

Para comprender completamente el proceso de la red, se hace necesario examinar detalladamente cada una de las capas inferiores. Comenzando por la capa física. Como aparece ilustrado en la figura 1.9, a continuación procederemos a examinar las funciones de cada capa.

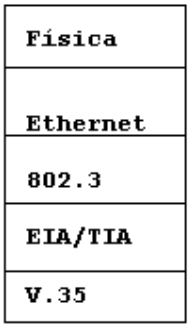


Figura 1.9 Capa física

La paca física define el tipo de medio, tipo de conector y tipo de señalización. Éste especifica los requisitos eléctricos, mecánicos, procedimentales y funcionales para activar, mantener y desactivar el vinculo físico entre sistemas finales. La capa física especifica también características tales como niveles de voltaje, tasas de transferencia de datos, distancias máximas de transmisión y conectores físicos. En el ejemplo que hemos usado anteriormente, la capa física sería la carretera por la cual se transporta la taza. La carretera es una conexión física entre diferentes ciudades que permiten ir de un sitio a otro. Cada carretera posee sus propias reglas, como las relativas al límite de velocidad o al peso, del mismo modo que cada medio de red posee su propio ancho de banda y unidad máxima de transmisión(MTU).

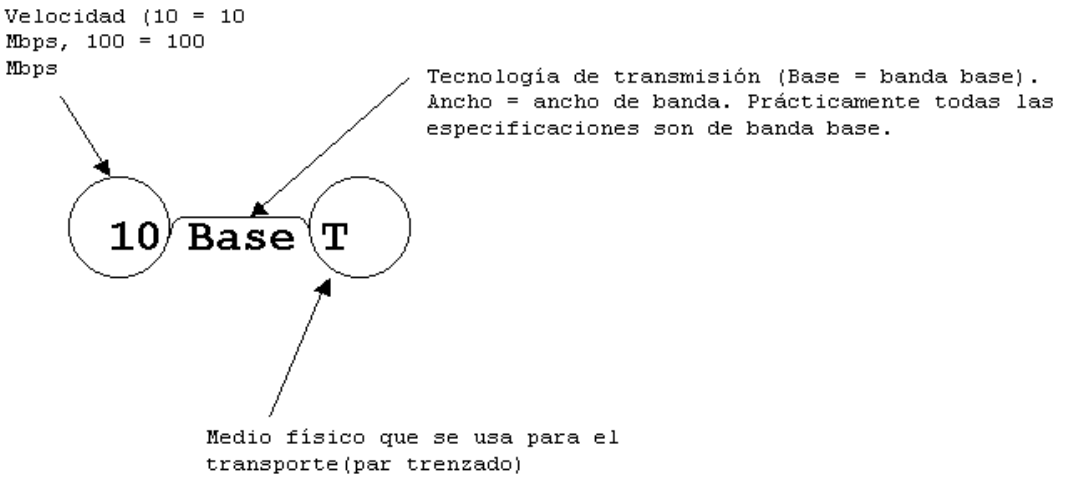
MEDIOS FÍSICOS Y CONECTORES

El medio físico y los conectores usados para conectar dispositivos al medio vienen definidos por estándares da la capa física.

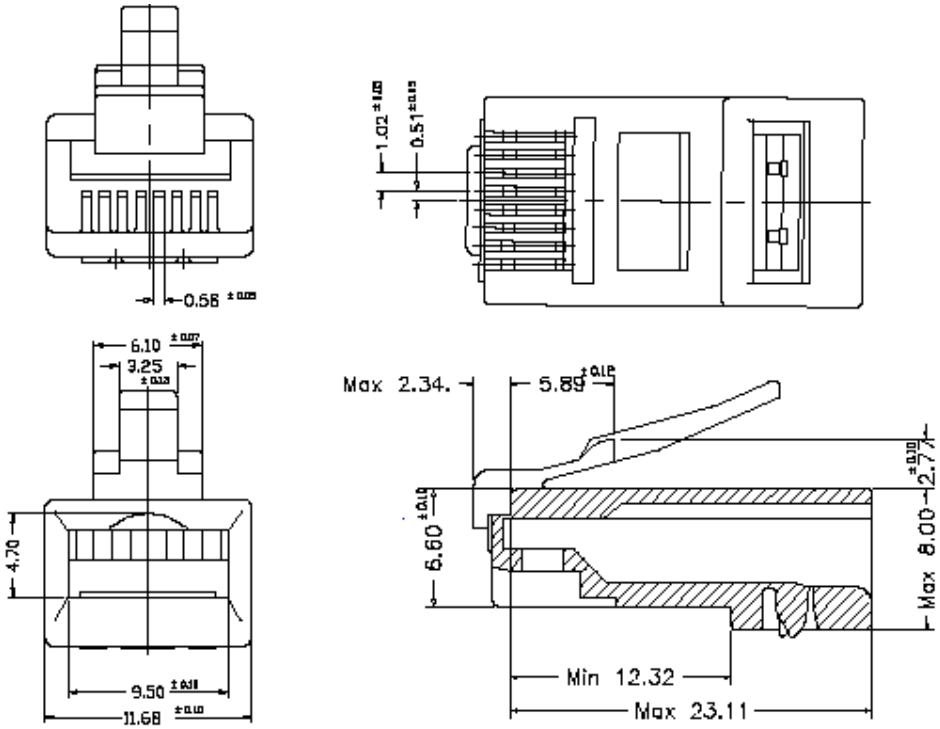
Los estándares de Ethernet e IEEE 802.3 (CSMA/CD) definen una topología de bus para LAN que opera a una tasa de señalización de 10 megabits (Mbps). La figura 1.10 ilustra la definición de los estándares de cableado de tres capas físicas, que responden a las siguientes descripciones:

- **10Base2.** Conocido como Thinnet. Permite segmentos de red de hasta 185 metros sobre cable coaxial para interconectar o encadenar dispositivos.
- **10Base5**. Conocido como Thinknet. Permite segmentos de red de hasta 500 metros sobre grandes cables coaxiales con dispositivos en el cable para recibir señales.
- **10BaseT**. Transporta señales Ethernet hasta 100 metros de distancia en cable de par trenzado económico hasta un concentrador centralizado denominado hub.

ESPECIFICACIONES DE CABLEADO



CONECTOR RJ-45



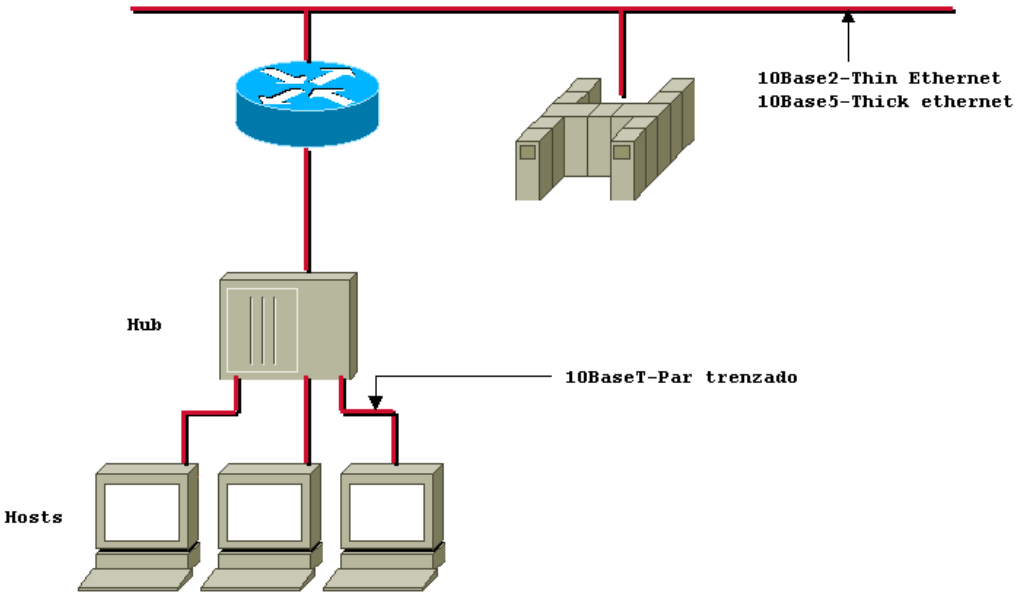


Figura 1.10 Definición de estándares de cableado 10 base de capa física.

Los estándares 10Base5 y 10Base2 proporcionan acceso a múltiples puestos de trabajo en el mismo segmento conectado entre sí los dispositivos a un segmento Ethernet común. Los cables 10Base5 se unen al bus usando un cable y una interfaz de unidad de conexión (AUI). Las redes 10Base2 encadenan dispositivos usando cable coaxial y conectores T para conectar los puestos de trabajo al bus común.

Ya que el estándar 10BaseT proporciona acceso a puestos individuales, cada equipo ha de estar conectado a una estructura de bus común para poder interconectar todos los dispositivos. El hub viene a ser el bus de los dispositivos Ethernet y es análogo al segmento.

DOMINIOS DE COLISIÓN / DIFUSIÓN

Dado que todos los puestos de un segmento ethernet están conectados a un mismo medio físico, las señales enviadas a través del cable son recibidas por todos los dispositivos. Esto significa, además, que si dos dispositivos envían una señal al mismo tiempo se producirá una colisión entre ambas. La estructura Ethernet debe, por tanto, disponer de reglas que permitan que sólo un puesto tenga acceso al medio en un momento dado. También debe existir algún medio de detectar y corregir los errores conocidos como colisiones(cuando dos o más puestos tratan de transmitir al mismo tiempo).

Cuando se trata de redes locales, es fundamental definir dos conceptos de suma importancia:

- **Dominio de colisión.** Grupo de dispositivos conectados al mismo medio físico, de tal manera que si dos dispositivos acceden al medio al mismo tiempo, el resultado sea un colisión entre las dos señales.

- **Dominio de difusión.** Grupo de dispositivos de la red que envían y reciben mensajes de difusión entre ellos.

Estos términos le ayudarán a comprender la estructura básica de los patrones de tráfico y le facilitarán la definición de las necesidades relativas a dispositivos tales como switches y routers.

La mayoría de los segmentos Ethernet que existen hoy día son dispositivos interconectados por medio de hubs. Los hubs permiten la concentración de muchos dispositivos Ethernet en un dispositivo centralizado, que conecta todos los dispositivos en una misma estructura de concentrador físico. Esto significa que todos los dispositivos conectados al hub comparten el mismo medio y, en consecuencia, comparten los mismos dominio de colisión, dominio de difusión y ancho de banda. La conexión física resultante es la que corresponde a una topología de red, en oposición a una topología lineal. La figura 1.11 muestra una conexión típica a un hub.

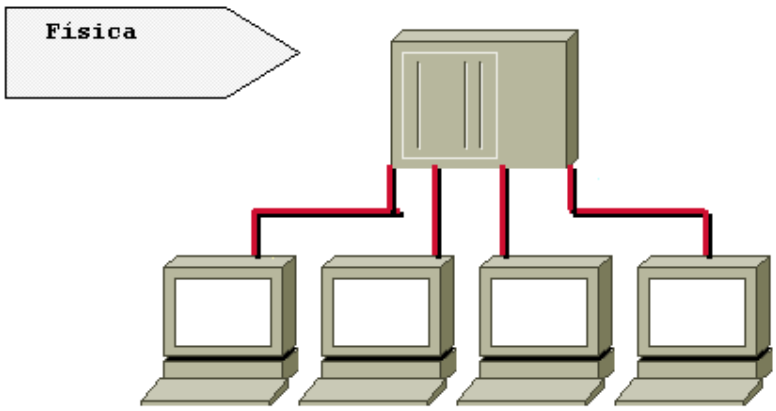


Figura 1.11 Hub Ethernet.

El hub no manipula ni visualiza el tráfico del bus; se utiliza sólo para extender el medio físico repitiendo la señal que recibe de un puerto a todos los demás puertos. Esto significa que un hub es un dispositivo de capa física, sin ninguna función propia de capas superiores. Sin embargo, esto no cambia las reglas de Ethernet. Los puestos de trabajo siguen compartiendo el bus del hub, lo que significa que sigue existiendo contención.

Debido a que todos los dispositivos están conectados al mismo medio físico, un hub es un dominio de colisión individual. Si un puesto envía una difusión, el hub la propaga a todos los demás puestos, de manera que también se convierte en un dominio de difusión individual.

La tecnología Ethernet utilizada en este ejemplo se conoce como acceso múltiple con detección de portadora(carrier) y detección de colisiones (CSMA/CD). En la practica, esto significa que varios puestos pueden tener acceso al medio y que, para que un puesto pueda acceder al medio, deberá "escuchar"(detectar la portadora) para asegurarse que ningún otro puesto esté utilizando el mismo medio. Si el medio se encuentra en uso, el puesto procederá a mantener en suspenso el envío de datos. En caso de que haya dos puestos que no detectan ningún otro tráfico, ambos tratarán de transmitir al mismo tiempo, dando como resultado una colisión.

Por ejemplo, si dos vehículos tratan de ocupar la misma carretera al mismo tiempo, colisionarían. En una red, al igual que con los coches, la colisión resultante provoca algún tipo de daño. De hecho, las tramas dañadas se convierten en tramas de error, las cuales son detectadas por los puestos como una colisión, lo cual obliga a ambas estaciones a volver a transmitir sus respectivas tramas. Existe un algoritmo de repetición que determina cuándo los puestos deben volver a transmitir, con el fin de minimizar la posibilidad de que tenga lugar otra colisión. Cuantas más estaciones haya en un segmento de Ethernet, mayor es la probabilidad de que tenga lugar una colisión. Estas colisiones excesivas son la razón principal por la cual las redes se segmentan en dominios de colisión más pequeños, mediante el uso de conmutadores(switches) y puentes(bridges).

FUNCIONES DE LA CAPA DE ENLACE DE DATOS

Antes De que el tráfico pueda entrar en la red, es necesario dar algunos detalles acerca de dónde ir y lo que se ha de hacer al llegar al destino. La capa de enlace de datos proporciona esta función. La capa de enlace de datos es la Capa 2 del modelo de referencia OSI, y puede cambiar en función de la topología implementada. La figura 1.13 muestra varias topologías físicas junto a algunos de los correspondientes métodos de encapsulado de enlace de datos.

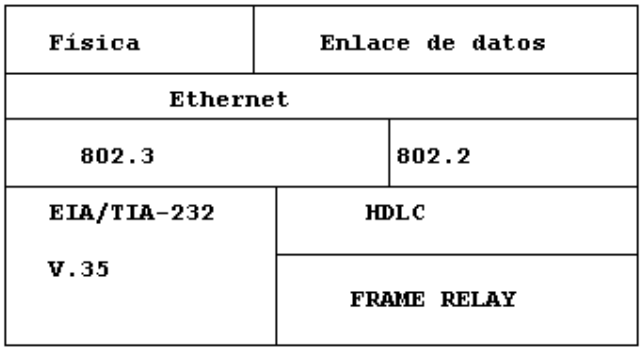


Figura 1.13. Capa de enlace de datos.

La finalidad de esta capa es proporcionar las comunicaciones entre puestos de trabajo en una primera capa lógica que hay por encima de los bits del cable. El direccionamiento físico de los puestos finales se realiza en la capa de enlace de datos con el fin de facilitar a los dispositivos de red la determinación de si deben subir un mensaje a la pila de protocolo. También hay campos en esta capa para indicar al dispositivo cual es la pila de la capa superior donde deben pasar los datos(como IP, IPX, Apple Talk, etc.). La capa de enlace de datos da soporte a servicios basados en la conectividad y no basados en ella, y proporciona la secuencia y control de flujo.

Para proporcionar estas funciones, la capa de vínculo de datos IEEE está definida mediante dos subcapas:

- **Subcapa de control de acceso al medio(MAC) (802.3).** La subcapa de control de acceso al medio es la responsable de determinar cómo han de ser transportados los datos a través del cable físico. Ésta es la parte de la capa de vínculo de datos que se comunica hacia abajo con la capa física. En ella se definen funciones tales como el direccionamiento físico, topología de la red, disciplina de la línea, notificación de errores, distribución ordenada de tramas u control óptimo de flujo.

- **Subcapa de control de enlace lógico(LLC) (802.2).** La subcapa de control de enlace lógico es la responsable de la identificación lógica de los distintos tipos de protocolos y el encapsulado posterior de los mismos para ser transmitidos a través de la red. Un identificador de código de tipo o punto de acceso al servicio(SAP) es el encargado de realizar la identificación lógica. El tipo de la trama LLC utilizado por un puesto final depende del identificador que espera el protocolo de la capa superior. Entre las opciones LLC adicionales figuran el soporte para conexiones entre aplicaciones que se ejecutan en la LAN, el control de flujo a la capa superior y la secuencia de bit de control. Para algunos protocolos, LLC define servicios fiables y no fiables para la transferencia de datos, en lugar de la capa de transporte.

TRAMAS DE LA SUBCAPA MAC

La figura 1.14 ilustra la estructura de trama para tramas IEEE 802.3 de la subcapa MAC. La figura 1.14 muestra la estructura de la trama estándar a modo de ejemplo de cómo se utiliza el control de información para transmitir datos en esta capa. Éstas son las definiciones de los campos de la subcapa MAC:

- La trama IEEE 802.3 comienza con un patrón alternado de unos y ceros llamado **preámbulo.** El preámbulo avisa a los puestos receptores de la llegada de una trama.

- Inmediatamente a continuación del preámbulo se encuentran los campos de **dirección física de origen** y **destino.** Dichas direcciones se conocen como **direcciones de la capa MAC**. Éstas son únicas para cada dispositivo del **internetworking** de redes. En la mayoría de las tarjetas LAN, la dirección MAC se graba en la ROM, lo que explica el término burned-in-address(BIA). Cuando sé inicializa la tarjeta de red, esta dirección se copia en la RAM para identificar el dispositivo en la red.

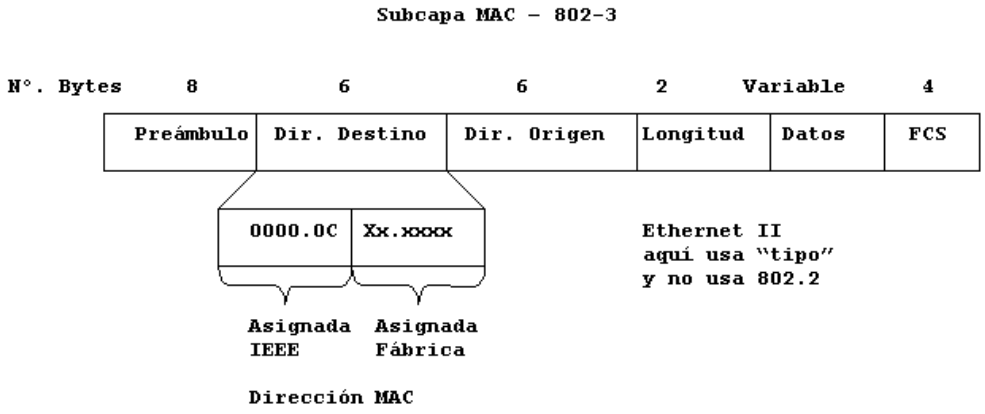


Figura 1.14. Trama de la subcapa MAC.

La dirección MAC consta de 48 bits y viene expresada en 12 dígitos hexadecimales. Los primeros 24 bits, o 6 dígitos hexadecimales, de la dirección MAC contienen un código de identificación del fabricante o vendedor. Otro nombre por el que se conoce a esa parte de la dirección es Organizationally Unique Identifier(OUI). Los últimos 24 bits, o 6 dígitos hexadecimales, están administrados por cada fabricante y presentan, por lo general, el número de serie de la tarjeta.

La dirección de origen es siempre una dirección de unidifusión(nodo simple), mientras que la dirección de destino puede ser una unidifusión, multidifusión(grupo de nodos) o difusión(todos los nodos).

- En las tramas IEEE 802.3, el campo de dos bytes que sigue a la dirección de origen es el campo **longitud**, e indica el número de bytes de datos que siguen a este campo y preceden al campo de secuencia de verificación de trama(FCS).

- A continuación del campo longitud se encuentra el campo **datos**, que incluye la información de control LLC, además de otra información de control de capa superior y los datos del usuario.

- Por último, a continuación del campo de datos hay un campo de 4 byts FCS que contiene un valor de verificación de redundancia cíclica (CRC). La CRC se crea por el dispositivo emisor y se vuelve a calcular por el dispositivo receptor para comprobar si ha habido daños en la trama durante su tránsito.

TRAMAS DE LA SUBCAPA LLC

Hay dos tipos de tramas LLC: Punto de acceso al servicio (SAP) y Protocolo de acceso a subred (SNAP). El tipo de trama que utilice el sistema depende de la aplicación que se encuentre en ejecución en el mismo. Algunas aplicaciones se definen mediante un SAP ID, mientras que otras utilizan un código de tipo. La figura 1.15 muestra el formato de los tipos de trama SAP y SNAP.

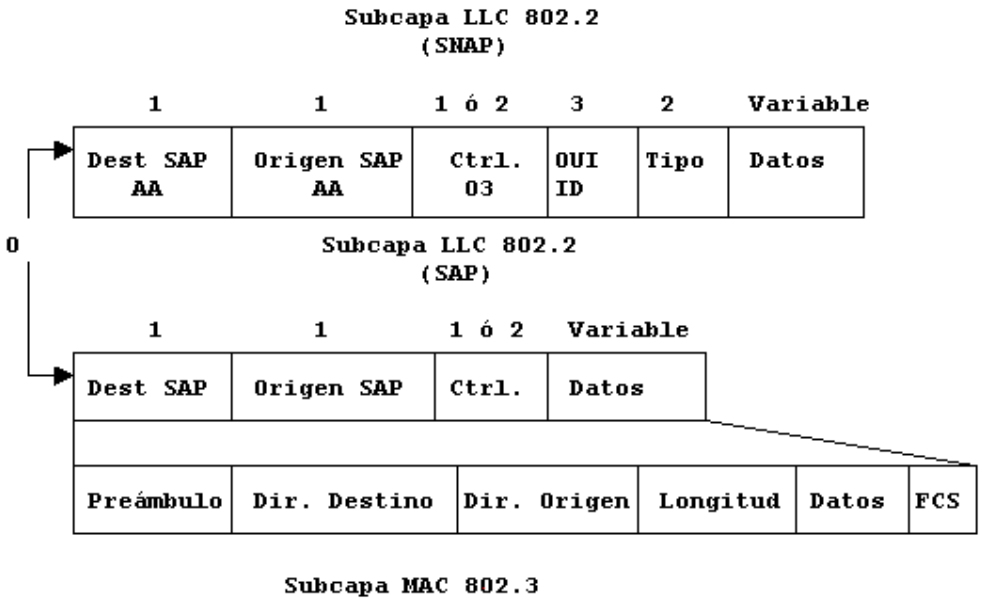


Figura 1.15. Tramas SAP y SNAP de la subcapa LLC.

En la cabecera LLC, los campos de destino SAP(DSAP) y origen SAP(SSAP) tienen un byte cada uno y actúan como punteros para protocolos de capa superior en un puesto. Por ejemplo, una trama con un SAP de 06 hex está destinado para IP, mientras que una trama con SAP E0 hex estaría destinado para IPX. Desde la perspectiva de estas subcapas MAC inferiores, el proceso SAP proporciona una interfaz apropiada para las capas superiores de la pila del protocolo. Estas entradas SAP permiten que las conexiones físicas y de enlace de datos proporcionen servicios para muchos protocolo de capa superior.

Para especificar que la trama utilizada SNAP, las direcciones SSAP y DSAP han de establecerse ambas en AA hex, y el campo de control, en 03 hex. Además de los campos SAP, una cabecera SNAP tiene un campo código de tipo que permite la inclusión del EtherType. El EtherType se encarga de definir cuál es el protocolo de capa superior que recibirá los datos.

En una trama SNAP, los tres primeros bytes de la cabecera SNAP que sigue al campo de control corresponden al código del vendedor OUI. A continuación del código de vendedor OUI hay un campo de dos bytes que contiene el EtherType para la trama. Aquí es donde se implementa la compatibilidad en ascenso con Ethernet Versión II. Como trama 802.3, hay un campo FCS de 4 bytes a continuación de los datos y contiene un valor CRC.

DISPOSITIVOS DE LA CAPA DE ENLACE

Los bridges y switches de la Capa 2 son dispositivos que funcionan en la capa de enlace de datos de la pila del protocolo. La figura 1.16 muestra los dispositivos que se encuentran habitualmente en la Capa 2. La conmutación de la Capa 2 se basa en el puenteado por hardware. En un switch, el reenvío de tramas se controla por medio de un hardware especial llamada circuitos integrados específicos de aplicaciones (ASIC). La tecnología ASIC permite que un chip de silicio pueda ser programado para realizar una función específica durante el proceso de fabricación del mismo. Esta tecnología permite que las funciones puedan llevarse a cabo a una velocidad mucho mayor que si el chip estuviese programado por software. Debido a la tecnología ASIC, los switches proporcionan escalabilidad a velocidades de gigabits con una latencia baja.

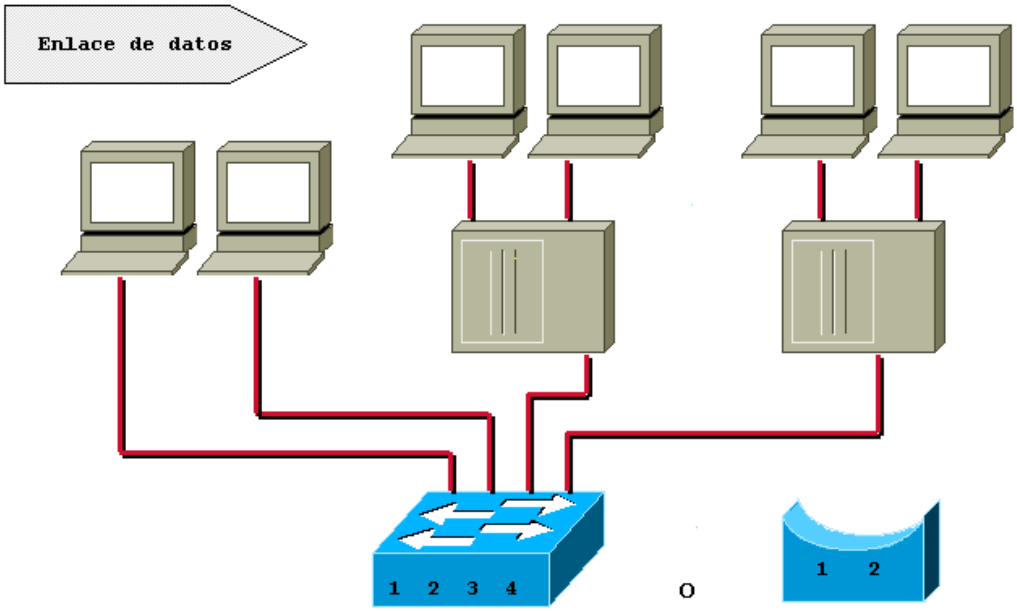


Figura 1.16 **Dispositivos de enlace de datos.**

Nota_

Aunque hay switches de Capa 3 y Capa 4 capaces de realizar enrutamiento, en este documento utilizaremos el término switch para referirnos a un dispositivo de Capa 2.

Cuando un bridge o switch recibe una trama, utiliza la información del enlace de datos para procesar dicha trama. En un entorno de bridges transparente, el bridge procesa la trama determinada si ésta necesita ser copiada en otros segmentos conectados. Un bridge transparente detecta todas las tramas que cruzan un segmento y visualiza cada trama y el campo de dirección de origen para determinar en qué segmento reside el puesto de origen. El bridge transparente guarda esta información en memoria en lo que se conoce como **tabla de envío**. La tabla de envío contiene un listado de todos los puestos finales(desde los cuales el bridge puede detectar una trama en un periodo de tiempo determinado) y el segmento en el que éste reside. Cuando un bridge detecta una trama en la red, examina la dirección de destino y la compara con la tabla de envío para determinar si ha de filtrar, inundar o copiar la trama en otro segmento.

Este proceso de decisión tiene lugar como se indica a continuación:

- Si el dispositivo de destino está en el mismo segmento que la trama, el bridge bloquea el paso de la trama a otro segmento. Este proceso se conoce como **filtrado**.

- Si el dispositivo de destino se encuentra en un segmento diferente, el bridge envía la trama al segmento apropiado.

- Si la dirección de destino es desconocida para el bridge, éste envía la trama a todos los segmentos excepto a aquel de donde se ha recibido la información. Este proceso se denomina **inundación**.

Debido a que el bridge aprende todos los puestos finales a partir de las direcciones de origen, nunca aprenderá la dirección de difusión. Por tanto, todas las difusiones serán inundadas a todos los segmentos del bridge o switch. En consecuencia, todos los segmentos de un entorno basado en bridge o switches se consideran residentes en el mismo dominio de difusión.

Nota_

Este documento se centra en el puenteado transparente dado que ésta es la función que lleva a cabo la serie de switches Catalyst 1900. Ésta es, además, la forma más común de puenteado/conmutación en entornos Ethernet. Téngase en cuenta también que existen otros tipos de bridges, como bridges en rutas de origen, en los cuales el origen determina la ruta que debe seguirse a través de la red, y bridges de traducción, que permiten que una trama pase de una ruta de origen a un entorno transparente entre Ethernet y Token Ring.

Una red puenteada/conmutada proporciona una excelente administración del tráfico. La finalidad del dispositivo de Capa 2 es reducir las colisiones al asignar a cada segmento su propio dominio de colisión. Cuando hay dos o más paquetes que necesitan entrar en un segmento, quedan almacenados en memoria hasta que el segmento esté disponible.

Las redes punteadas/conmutadas poseen las siguientes características:

- Cada segmento posee su propio dominio de colisión.

- Todos los dispositivos conectados al mismo bridge o switch forman parte del mismo dominio de difusión.

- Todos los segmentos deben utilizar la misma implementación al nivel de la capa de enlace de datos como, por ejemplo, Ethernet o Token Ring. Si un puesto final concreto necesita comunicarse con otro puesto final a través de un medio diferente, se hace necesaria la presencia de algún dispositivo, como puede ser un router o un bridge de traducción, que haga posible al diálogo entre los diferentes tipos de medios.

- En un entorno conmutado, puede haber un dispositivo por segmento, y todos los dispositivos pueden enviar tramas al mismo tiempo, permitiendo de este modo que se comparta la ruta primaria.

FUNCIONES DE LA CAPA DE RED

La capa de red define cómo tener lugar el transporte de tráfico entre dispositivos que no están conectados localmente en el mismo dominio de difusión. Para conseguir esto se necesitan dos elementos de información:

- Una dirección lógica asociada a cada puesto de origen y de destino.
- Una ruta a través de la red para alcanzar el destino deseado.

La figura 1.17 muestra la ubicación de la capa de red en relación con la capa de enlace de datos. La capa de red es independiente de la de enlace de datos y, por tanto, puede ser utilizada para conectividad se usa la estructura lógica de direccionamiento.

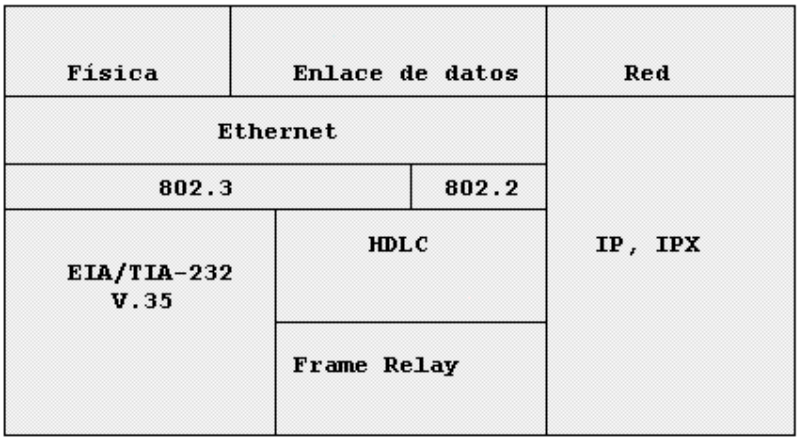


Figura 1.17 Localización de la capa de red en el modelo del protocolo.

Los esquemas de direccionamiento lógico se utilizan para identificar redes en un internetworking de redes y la ubicación de los dispositivos dentro del contexto de dichas redes. Estos esquemas varían en función del protocolo de capa de red que se utilice. En este documento se describe cómo opera la capa de red para las pilas de los protocolos TCP/IP e IPX.

DIRECCIONES DE LA CAPA DE RED

Las direcciones de la capa de red(denominadas **direcciones lógicas** o **virtuales**) se sitúan en la Capa 3 del modelo de referencia OSI. A diferencia de las direcciones de la capa de vínculo de datos, que suelen residir en un espacio de direcciones plano, las direcciones de la capa de red poseen habitualmente una estructura jerárquica en la cual se definen primero las redes y después los dispositivos o nodos de cada red. En otras palabras, las direcciones de la capa de red son como direcciones postales, que describen el lugar de residencia de un individuo por medio de un código postal y una dirección (calle). El código postal define la ciudad, provincia o estado, mientras que la dirección representa una ubicación especifica dentro de esa ciudad. Esto contrasta con las direcciones de la capa MAC, de naturaleza plana. Un buen ejemplo de dirección plana podría ser el sistema de numeración de la seguridad social o del Documento nacional de identidad, donde cada persona posee un número único que lo identifica.

COMO OPERA EL ROUTER EN LA CAPA DE RED

Los routers operan en la capa de red registrando y grabando las diferentes redes y eligiendo la mejor ruta para las mismas. Los routers colocan esta información en una tabla de enrutamiento, que incluye los siguientes elementos(véase figura 1.18):

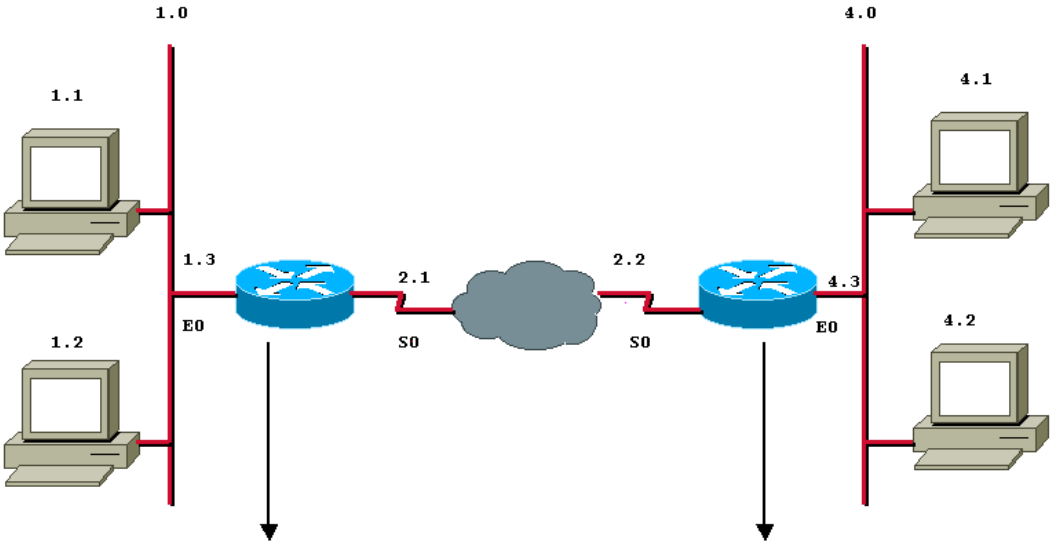
- **Dirección de red**. Representa redes conocidas por el router. La dirección de red es específica del protocolo. Si un router soporta varios protocolos, tendrá una tabla por cada uno de ellos.

- **Interfaz**. Se refiere a la interfaz usada por el router para llegar a una red dada. Ésta es la interfaz que será usada para enviar los paquetes destinados a la red que figura el la lista.

- **Métrica**. Se refiere al coste o distancia para llegar a la red de destino. Se trata de un valor que facilita el 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 más habituales figuran el número de redes que han de ser cruzadas para llegar al destino(conocido también como **saltos**), el tiempo que se tarda en atravesar todas las interfaces hasta 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 dominios 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 unívoca mediante direcciones lógicas. Esta estructura de direccionamiento permite una configuración jerárquica de la red, ya que está definida por la red en la que se encuentra, así como por un identificador de host.

Para que los routers puedan operar en una red, es necesario que cada tarjeta esté configurada en la red única que ésta representa. El router debe tener también una dirección de host en esa red. El router utiliza la información de configuración de la tarjeta para determinar la parte de la dirección correspondiente a la red, a fin de construir una tabal de enrutamiento.



T. Enrutamiento		
RED	INT	Métrica
1	E0	0
2	S0	0
4	S0	1

T. Enrutamiento		
RED	INT	Métrica
1	S0	1
2	S0	0
4	E0	0

Figura 1.18 Tablas de enrutamiento.

Además de identificar redes y proporcionar conectividad, los router deben proporcionar estas otras funciones:

- Los routers no envían difusiones de Capa 2 ni tramas de multidifusión.
- Los routers intentan determinar la ruta más óptima a través de una red enrutada basándose en algoritmos de enrutamiento.
- Los routers separan las tramas de Capa 2 y envían paquetes basados en direcciones de destino Capa 3.
- Los routers asignan una dirección lógica de Capa 3 individual a cada dispositivo de red; por tanto, los routers pueden limitar o asegurar el tráfico de la red basándose en atributos identificables con cada paquete. Estas opciones, controladas por medio de listas de acceso, pueden ser aplicadas para incluir o sacar paquetes.
- Los routers pueden ser configurados para realizar funciones tanto de puenteado como de enrutamiento.
- Los routers proporcionan conectividad entre diferentes LAN virtuales (VLAN) en entornos conmutados.
- Los routers pueden ser usados para desplegar parámetros de calidad de servicio para tipos específicos de tráfico de red.

Además de las ventajas que aporta su uso en un campus, los routers pueden utilizarse también para conectar ubicaciones remotas con la oficina principal por medio de servicios WAN.

Los routers soportan una gran variedad de estándares de conectividad al nivel de la capa física, lo cual ofrece la posibilidad de construir WAN. Además, pueden proporcionar controles de acceso y seguridad, que son elementos necesarios cuando se conectan ubicaciones remotas.

FUNCIONES DE LA CAPA DE TRANSPORTE

Para poder conectar dos dispositivos en la construcción de una red, es necesario establecer una conexión o sesión. La capa de transporte define las directrices de la conexión entre dos puestos finales. Una sesión constituye una conexión lógica entre las capas de transporte iguales en los puestos de origen y destino. La figura 1. muestra la relación de algunos protocolos de capa de transporte con sus respectivos protocolos de capa de red.

Estos protocolos proporcionan diferentes funciones de capa de transporte.

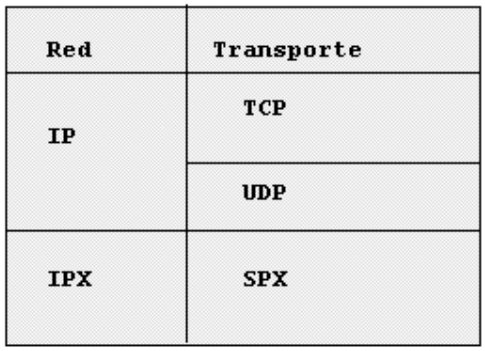


Figura 1.19 Protocolos de capa de transporte

Concretamente, la capa de transporte define las funciones que se describen a continuación:

- Permitir a los puestos finales ensamblar y desensamblar múltiples segmentos de capa superior en el mismo flujo de datos de la capa de transporte. Esto se consigue asignando identificadores de aplicación de capa superior. Dentro de la suite del protocolo TCP/IP, estos identificadores se conocen como **números de puerto**. El modelo de referencia OSI denomina a estos identificadores como puntos de acceso al servicio (SAP). La capa de transporte utiliza estos números de puerto para identificar elementos de la capa de aplicación como FTP O Telnet. Un ejemplo de número de puerto es el 23, que identifica la aplicación Telnet. Los datos con un número de puerto de transporte 23 serán destinados a la aplicación Telnet.

- Permitir a las aplicaciones solicitar transportes fiables de datos entre sistemas finales que están en comunicación. Los transportes fiables utilizan una relación orientada a la conexión entre los sistemas en comunicación para conseguir los siguientes objetivos:

  - Asegurar que los segmentos distribuidos serán confirmados al remitente.
  - Proporcionar la retransmisión de cualquier segmento que no sea confirmado.
  - Colocar de nuevo los segmentos en su orden correcto en el puesto receptor.
  - Proporcionar control y evitar congestiones.

En la capa de transporte, los datos pueden ser transmitidos de forma fiable o no fiable. Para IP, el protocolo TCP es fiable u orientado a conexión, mientras que UDP no es fiable, o independiente de la conexión.

REPASO DE LA CAPA INFERIOR OSI

Una vez que hemos definido y descrito las cuatro capas inferiores del modelo OSI y repasado los conceptos de dominios de colisión y de difusión, hagamos un resumen de toso lo que hemos aprendido.

Cada dispositivo de los que muestra la figura 1.20 opera en una capa diferente del modelo OSI:

- En la Capa 1 (la capa física) esta el hub. El hub transmite nuestros paquetes y actúa como dispositivo concentrador para otros dispositivos de red. El hub forma una segmento individual, proporcionando un dominio de colisión y un dominio de difusión.

- El switch y el bridge son dispositivos de Capa 2. Estos dispositivos dividen nuestra red en segmentos independientes, con pocos usuarios por segmento. Cada segmento se sitúa en un dominio de conexión individual, por lo que en la figura, cada bridge y cada switch soportan cuatro dominios de colisión. En cambio, el tráfico de difusión se propaga a través de todos los segmentos, de manera que hay un sólo dominio de difusión asociado a cada dispositivo.

- En la Capa 3 (la capa red), el router proporciona rutas para todas las redes del internetworking de redes. El router divide la red en dominios de colisión y dominios de difusión independientes. En la Figura 1.20 podemos ver que hay cuatro dominios de difusión y cuatro dominios de difusión.

FUNCIONES DE LOS DISPOSITIVOS DE RED

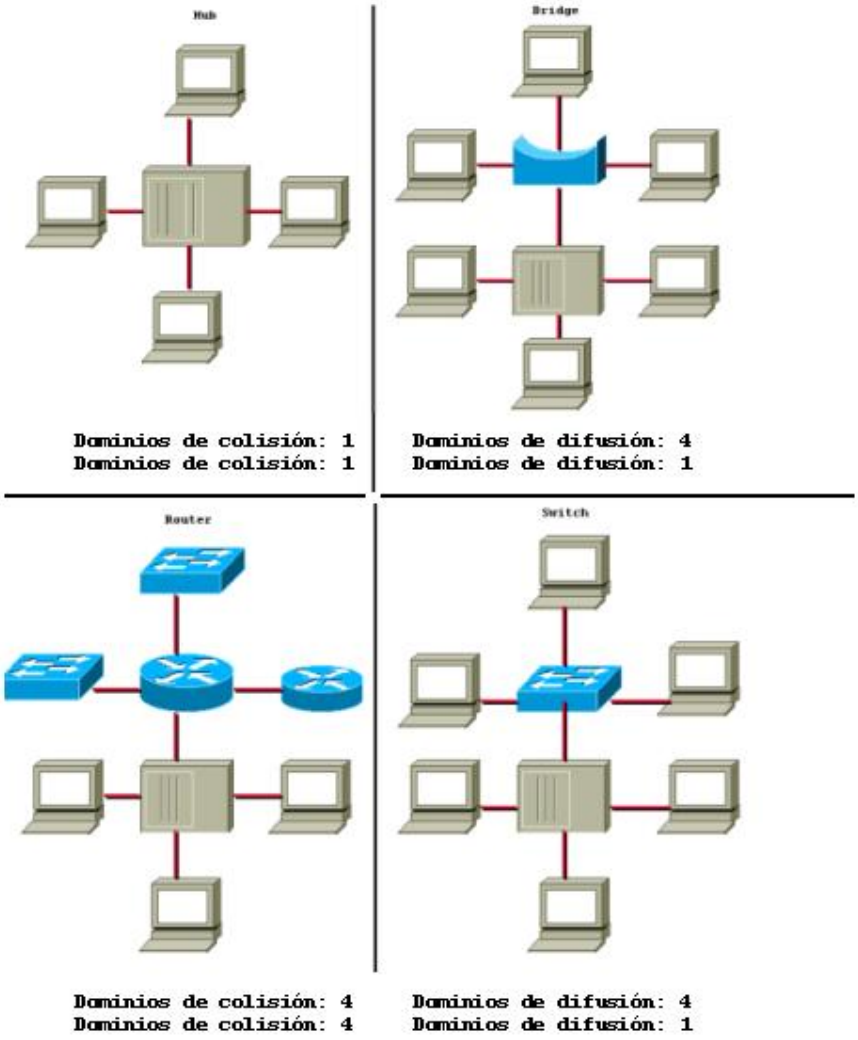


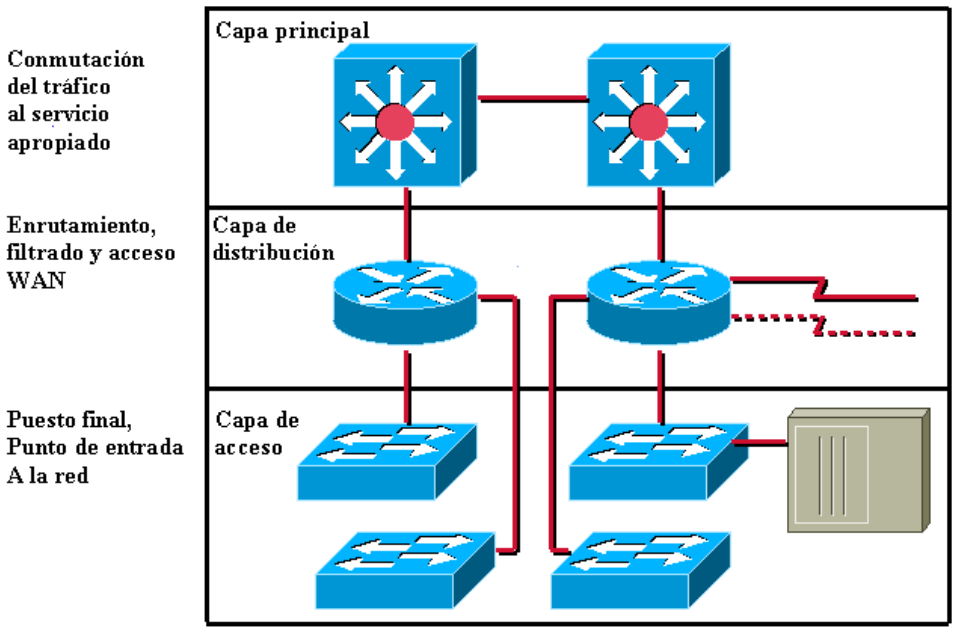
Figura 1.20 Funciones de los dispositivos de red.

SELECCIÓN DE PRODUCTOS CISCO.

Anteriormente, hemos hablado del modelo jerárquico usado para diseñar e implementar redes. La figura 1.21 resume la estructura de este modelo, visto con anterioridad. Dada la función específica de la red, y teniendo en cuenta todo lo explicado en relación con el servicio que ofrece cada capa, debe ser posible determinar los productos Cisco que satisfacen las demandas concretas del internetworking.

A continuación se resumen los factores a tener en cuenta a la hora de seleccionar dispositivos de red:

- El dispositivo debe proporcionar toda la funcionalidad y características demandadas.
- El dispositivo ha de poseer la capacidad y rendimiento esperados.
- El dispositivo debe ser fácil de instalar y ofrecer la posibilidad de una administración centralizada.
- El dispositivo debe proporcionar flexibilidad a la red.
- El dispositivo debe responder a la inversión realizada, de acuerdo con la infraestructura de la red existente.
- El dispositivo ha de ofrecer un medio de migración que contemple cambios y crecimientos futuros.



Modelo jerárquico de red basado en tres capas.

Figura 1.21 Modelo jerárquico de red basado en tres capas.

La tarea más importante consiste en conocer bien las necesidades e identificar las funciones y características que responden a dichas necesidades. Para poder conseguir esto, se ha de obtener información acerca de dónde deberá operar el dispositivo en la estructura jerárquica del internetworking y considerar factores tales como una fácil instalación, requisitos de capacidad, etc.

Hay otros factores, como el acceso remoto, que juegan también un papel importante a la hora de seleccionar un producto. Cuando se necesita soporte para el acceso remoto se ha de determinar en primer lugar la clase de servicios WAN que pueden satisfacer la demanda actual. A continuación, se deberá seleccionar el dispositivo apropiado.

El tipo y número de conexiones WAN requeridas afectan significativamente a la elección de los dispositivos. El factor más importante a la hora de elegir servicios WAN es la disponibilidad del servicio. También es importante conocer cuáles son los requisitos de ancho de banda y coste total del servicio. La figura 1.22 muestra un grafico que relaciona el coste de utilización de algunos servicios WAN habituales. Como puede ver, dependiendo de la utilización, podría resultar más efectivo desde el punto de vista del coste conseguir un servicio que proporciones una tasa de transferencia fija.

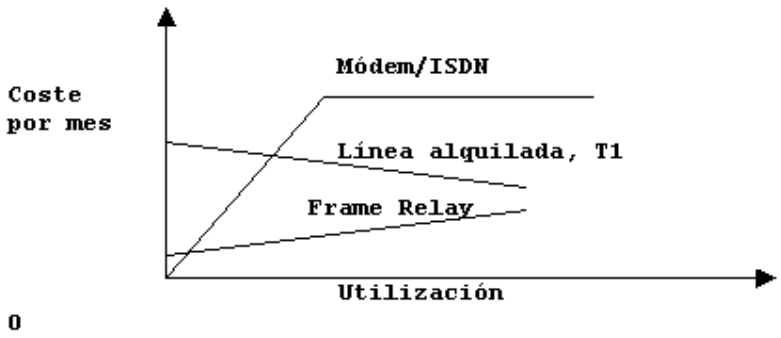


Figura 1.22 Utilización comparada con el coste WAN.

También es importante elegir un servicio que pueda ser soportado por el producto.

Cuando se trata de determinar los requisitos de ancho de banda de un servicio WAN, se debe examinar el tipo de tráfico que tendrá dicho servicio. La figura 1.23 da una idea de como se adapta la tecnología WAN a una aplicación determinada.

Una vez elegido el tipo de dispositivo de red que se necesita, se puede seleccionar un producto específico. Cisco Systems ofrece una gran variedad de productos de red, incluyendo hubs, switches y routers.

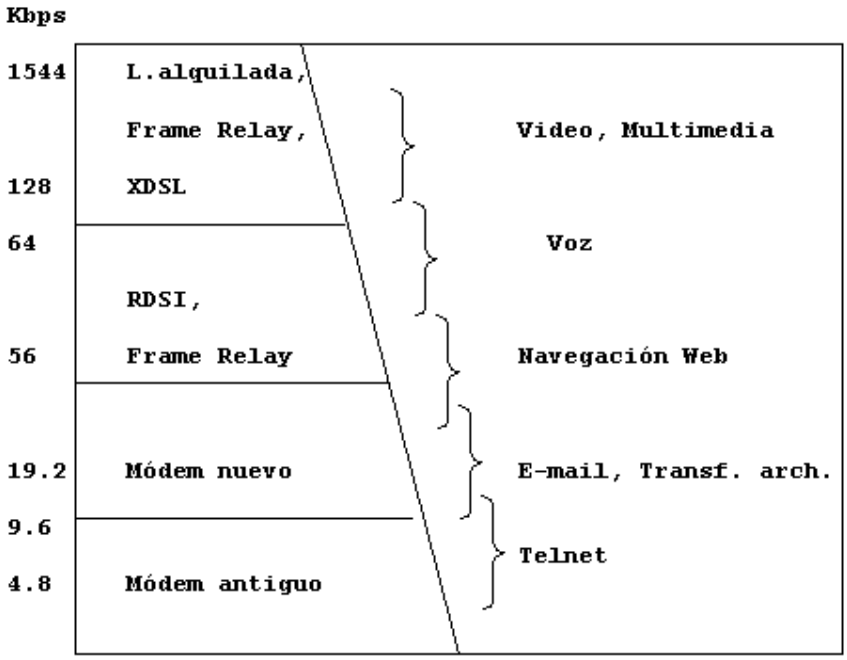


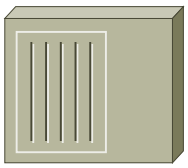
Figura 1.23 requisitos de ancho de banda para aplicaciones.

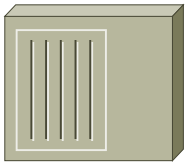
HUBS DE CISCO

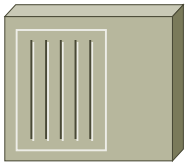
La figura 1.24 muestra la oferta de selección de hubs, junto con una muestra de la línea de productos cisco en esta gama. Esta figura presenta los productos en una Línea decreciente de prestaciones. El coste de estos productos es superior conforme bajamos en el escalafón.

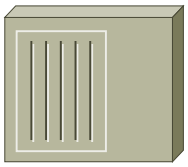
Los criterios que deben utilizarse para la selección de hub incluyen la velocidad del medio necesaria, el número de puertos a cubrir, facilidad de instalación y las necesidades de administración remota. La serie Micro Hub representa la línea de prestaciones mínimas, con densidades de puertos fijas de baja velocidad. FastHub 100 y 200 representan soluciones intermedias, que ofrecen una conectividad a alta velocidad, junto a algunas características básicas de administración. Las series FastHub 300 y 400 ofrecen la máxima flexibilidad, con puertos modulares y manejabilidad; sin embargo, en este caso se trata de dispositivos de 100 Mbps exclusivamente.

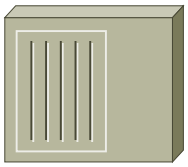
Antes de implementar un hub, debe averiguar que puestos necesitan 10 Mbps y cuáles precisan de 100 Mbps. Los hubs de nivel inferior ofrecen sólo 10 Mbps, mientras que los de nivel medio ofrecen ambas especificaciones. Los dispositivos de nivel medio ofrecen posibilidades de crecimiento y migración.


Cisco 1500 Micro Hub


Cisco 1528 Micro Hub 10/100


Cisco Fast Hub 100


Cisco Fast Hub 200


Cisco Fast Hub 300

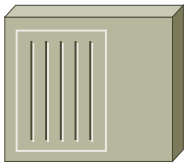

Cisco Fast Hub 400

Figura 1.24 Línea de productos hub de Cisco.

El alcance de las conexiones consolidadas tiene que ver con los puertos hub que demandan los usuarios. Los hubs permiten diversas densidades de puertos, y es posible apilar hubs para conseguir múltiplos de densidades de hubs individuales.

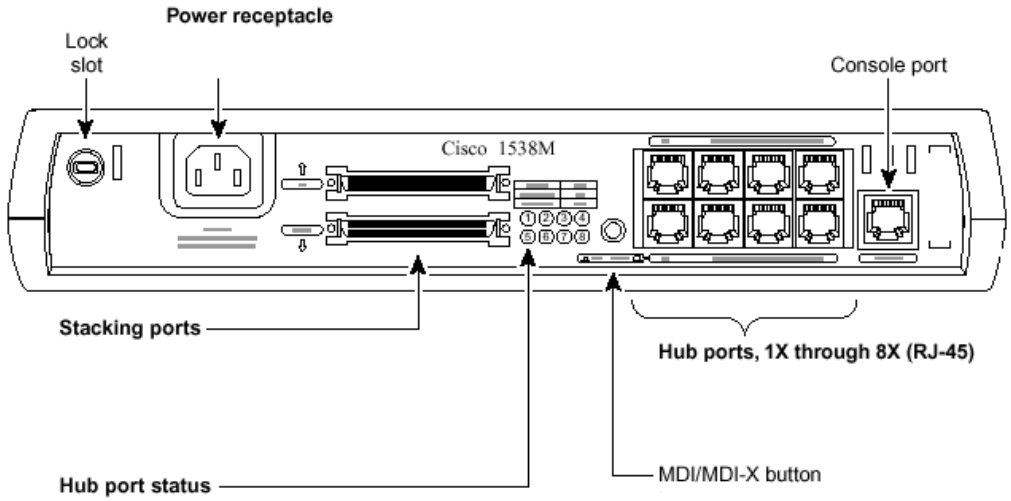
La mayoría de los hubs son tan sencillos como conectar y funcionar. Para la mayoría de los hubs no existe puerto de consola o administración. Si desea poder administrar el hub, deberá seleccionar alguno de la gama alta.

CLASES GENERALES DE CONCENTRADORES DE CISCO

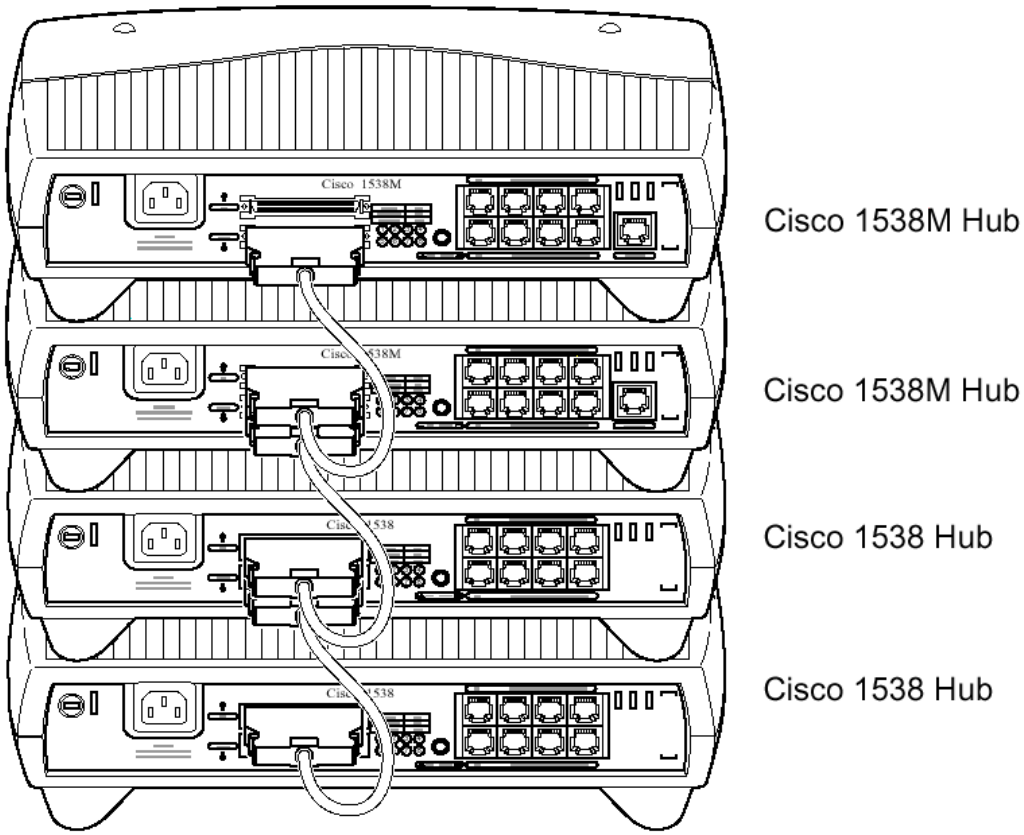
Serie	Descripción
Serie FastHub 400 de Cisco	Concentradores Fast Ethernet 10/100 de alto rendimiento tanto en modelos modulares como de configuración fija, con 12 o 24 puertos por módulo y hasta cientos de puertos por pila. Todos los modelos son apilables en versiones administrada o administrable.
Serie Micro Hub 1500 de Cisco	Concentradores Fast Ethernet 10/100 de bajo coste en modelos de escritorio con configuración fija de 8 puertos para la pequeña oficina u oficina particular. Los dos modelos Micro Hub son apilables; uno es administrado, el otro administrable.
Concentrador 10BaseT	Desarrollado con Hewlett-Packard, éste es un concentrador Fast Ethernet 10/100 de configuración fija administrado y optimizado para usarlo con los conmutadores de las series Catalyst 1900 y 2820 de Cisco. No es apilable, pero puede configurarse en cascada.
Concentradores especiales	Concentradores que se usan en entornos especializados como FDDI.

Serie de productos	Descripción
Cisco MicroHub 1538	Dispositivo autosensible de ocho puertos 10/100 que viene en variantes administras y administrables, donde una unidad administrativa se puede utilizar para administrar indirectamente otras tres unidades administrables en una pila de cuatro concentradores.
Serie Cisco FastHub	Cuatro modelos que oscilan entre 12 y 24 puertos con 10/100 puertos autosensibles por chasis.

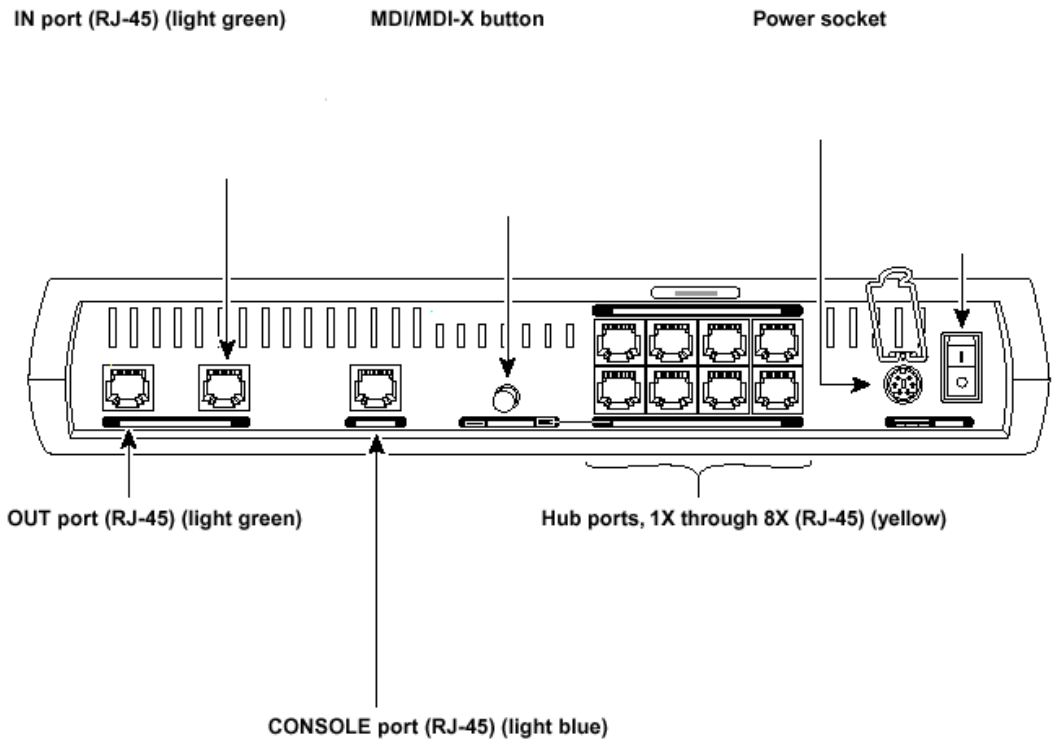
PANEL DE LED Y COMPONENTES DE UN HUB CISCO 1538M



HUB CISCO 1538M APILADOS



PANEL DE MICRO HUB 1501



SWITCHES CATALYST

La figura 1.25 muestra un ejemplo de la línea de productos switch de Cisco. La figura presenta una selección de productos con nivel de prestaciones decreciente e indica dónde pueden ser usados dichos productos en la red.

Hay una serie de temas clave a la hora de seleccionar productos switch:

- Requisitos de velocidad de medio.
- Necesidad de comunicaciones interswitching(troncalidad).
- Necesidad de segmentación de difusión (VLAN).
- Necesidades de densidad de puertos.
- Necesidades de coherencia en la interfaz de configuración.

Ya que una de las principales ventajas de los switches es la variedad de velocidades de enlace que ofrecen, un aspecto clave es considerar si se necesitan accesos de 10 o 100 Mbps.

Otros factores a tomar en consideración en relación con los switches son el número de puertos, la necesidad de una mayor segmentación mediante VLAN, así como diferentes conexiones a medios y topologías y funcionalidad corporativa, como enlaces interswitched para troncalidad. Muchas de estas funciones se examinan con más detalle más adelante. Por último, tal vez se desee que todos los dispositivos de red tengan una interfaz de configuración de usuario coherente. Los switches de Cisco poseen una gran variedad de interfaces de usuario, desde la línea de comandos, hasta menús y el web. Estas interfaces pueden llegar a jugar un papel importante en la selección de los productos.

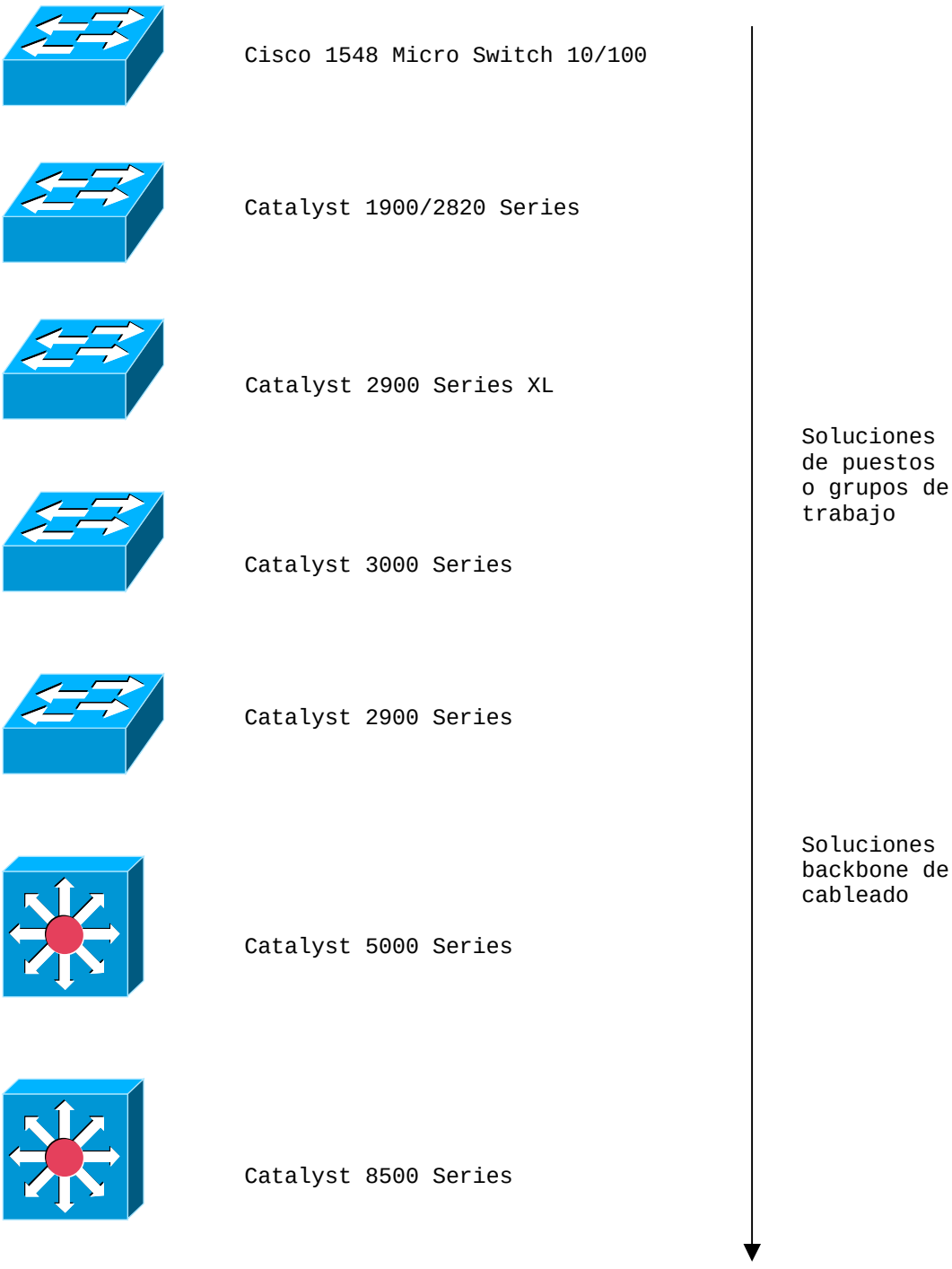


Figura 1.25 Línea de productos switch de Cisco.

ROUTERS DE CISCO

La figura 1.26 muestra un esquema de la línea de routers Cisco. La figura presenta la gama de productos en orden descendente de prestaciones y muestra dónde pueden ser utilizado cada uno de ellos en la red.

He aquí algunos temas relativos a la selección de productos de enrutamiento:

- Necesidad de escalar las características de enrutamiento.
- Requisitos de densidad / variedad de puertos.
- Capacidad y rendimiento.
- Interfaz de usuario común.

Un criterio fundamental a la hora de seleccionar un router es saber las características de servicio que se necesitan. Los routers de las distintas líneas de productos Cisco ofrecen conjuntos de características diferentes.

Las densidades de puerto y velocidades de interfaz aumentan, por lo general, cuando se sube en la gama de routers Cisco. Por ejemplo, la serie 12000 es la primera en una categoría de productos Gigabit switch routers(GSR). El 12000 GSR soporta inicialmente un enlace backbone IP a OC-12(622 Mbps) y puede escalarse para manejar enlaces de hasta OC-48(2,4 Gbps). En cambio, el router de la serie 800 está diseñado para poder operar con conexiones Ethernet de 10 Mbps para la red SOHO y servicios RDSI(ISDN) de 128 Kbps para Internet y oficinas corporativas.

Si la red requiere enlaces WAN, la selección de router pasa por averiguar qué dispositivo proporciona el tipo y número necesario de enlaces dentro de un coste razonable. Una red de producción típica tendrá varios switches LAN interconectados a la WAN mediante un router.

Tenga presente que los productos expuestos anteriormente son sólo un ejemplo de una oferta puntual de Cisco. La línea de productos Cisco está en constante evolución en respuesta a las necesidades de los clientes y a cuestiones relacionadas con la migración de la tecnología.

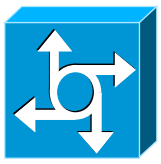

Cisco 700/800 Series **Soluciones domesticas**


Cisco 1600/1700 series


Cisco 2500 Series **Soluciones de pequeña oficina**


Cisco 2600 Series


Cisco 3600 Series **Soluciones de sucursal**


AS 5000 Series


Cisco 4000 Series


Cisco 7000 Series

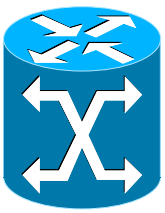

Cisco 12000 GSR Series

Figura 1.26 Línea de productos Cisco de enrutamiento.

CORTAFUEGOS

Un cortafuegos es un punto de comprobación entre una red privada y una o más redes públicas. Es una pasarela que decide selectivamente qué pueden entrar o salir de una red privada. Para ello, el cortafuegos debe ser la única pasarela entre la red que protege y el exterior. Si el tráfico no pasa a través del cortafuegos, la seguridad que éste suministrada no tiene ningún valor. Un principio básico es que todo tráfico externo debe pasar a través del cortafuegos.

El cortafuegos es una clase de enrutador, que funciona interceptando e inspeccionando cada paquete que entra por cualquiera de sus interfaces de red. La inspección varia dependiendo de la sofisticación del cortafuegos y de lo exigente que sea la política de seguridad.

SERVIDORES PROXI

Un servidor proxy es una aplicación que actúa como intermediario entre dos sistemas finales. Los servidores proxy funcionan en la capa de aplicación (nivel 7) de los cortafuegos, donde se obliga a los extremos de una conexión a canalizar la sesión a través del proxy. Esto se realiza creando y ejecutando un proceso en los cortafuegos que crea una imagen espejo de un servicio como si estuviera ejecutándose en todos los equipos finales.

Un servidor Proxy esencialmente convierte una sesión de dos partes en una sesión de cuatro partes, donde los procesos intermedios emulan los dos equipos reales. Como operan en el nivel 7, los servidores proxy también se conocen con el nombre de cortafuegos de la capa de aplicación. Es necesario ejecutar un servicio proxy por cada tipo de aplicación.

Como los servidores proxy centralizan toda la actividad para una aplicación en un solo servidor, éstos presentan la oportunidad ideal de realizar varias funciones útiles. Tener la aplicación ejecutándose justo delante de los cortafuegos ofrece la oportunidad de inspeccionar los paquetes para buscar más cosas que las direcciones origen/destino y los números de puerto. Esta es la razón por la que prácticamente todos los cortafuegos modernos incorporan alguna forma de arquitectura de servidor proxy.

CONFIGURACIONES DE DOBLE TARJETA

Una configuración de cortafuegos de doble tarjeta desactiva el enrutamiento entre las tarjetas de interfaz de red. Al hacer esto se obliga a que todo el tráfico pase a través de un servidor proxy antes de que pueda enrutarse al exterior hacia otra interfaz. Ésta es la razón por la que los cortafuegos de servidor proxy usan configuraciones de doble tarjeta. Otro uso de la doble tarjeta es cuando se quiere que los usuarios de dos redes accedan a un solo recurso, pero no se desea enrutar tráfico entre ellos.

REGISTRO DE EVENTOS Y NOTIFICACIÓN

El mantenimiento de un registro es un parte importante de todo el papel que realiza un cortafuegos. La mayoría de los cortafuegos pueden configurarse para cargar información de registro a un servidor de seguridad en cualquier lugar de la red, donde se analiza para conocer mejor la política de seguridad de empresa.

Los cortafuegos también pueden configurarse para generar mensajes de alerta si se sobrepasan ciertos umbrales especificados. En operaciones de red más sofisticadas, estas alertas se direccionan inmediatamente a una consola que se maneja para que el equipo de red pueda responder al evento con algunas medidas(normalmente desactivando la interfaz de red donde se ha realizado la violación aparente de seguridad).

CONFIGURACIÓN DE LA CARACTERÍSTICA DE CORTAFUEGOS DEL IOS

El cortafuegos de IOS es una opción de valor añadido al software IOS de Cisco. Se compra como lo que se conoce con el nombre de conjunto de características de IOS. Los cortafuegos IOS se usan para convertir un enrutador Cisco estándar en un cortafuegos realmente robusto añadiendo varias funciones de seguridad por encima del filtrado de tráfico básico del software estándar IOS:

- **Context-Based Access Control (CBAC) (Control de acceso basado en el contexto).** Una forma avanzada de filtrado de tráfico que examina la información de la capa de aplicación(nivel 7), como http, para conocer el estado de las conexiones TCO o UDP.

- **Traducción de direcciones (PAT y NAT).** Disfraza las direcciones IP internas insertando direcciones origen disfrazadas sobre paquetes enviados al exterior de los cortafuegos. PAT y NAT ocultan la topología interna de la red a los hackers.

- **Soporte de servidor de seguridad.** El enrutador puede configurarse como un cliente para servidores TACACS+, RADIUS o servidores de seguridad Kerberos, donde el nombre de los usuarios y las contraseñas pueden almacenarse en una clase de base de datos de servidor de autenticación de usuarios.

- **Detección de ataque por denegación de servicio.** Detecta los patrones de tráfico característicos de los llamados ataques por denegación de servicio y envían mensajes de alerta. (Los ataques por denegación de servicio intentan denegar servicio inundando una red con peticiones de servicio, como comando de correo electrónico ilegales o mensajes electrónicos infinitos.)

- **Bloqueo Java.** La habilidad de bloquear mensajes Java de forma selectiva desde una red(los subprogramas Java son programas que pueden descargar y que funcionan por sí mismos; se pueden programar para herir cualquier equipo que tenga la fatal idea de ejecutarlos).

- **Cifrado.** La habilidad de hacer incomprensible el contenido de un paquete a todos los sistemas, excepto a aquellos a los que se les ha suministrado un código(clave) para descodificarlo.

- **Autenticación de enrutador vecino.** Un comando mediante el que un enrutador puede obligar a otro enrutador vecino a autenticar su identidad, o todos los paquetes enrutados desde él serán bloqueados.

- **Alertas de seguridad y registro de eventos.** Mensajes que alertan a la administración de red que existe un problema de seguridad y el registro de todos los eventos de seguridad para recopilación y análisis posterior.

La mayoría de estas posibilidades se habilitan mediante el control de acceso basado en el contexto, que es la tecnología central en el software de cortafuegos IOS.

CÓMO FUNCIONA EL CONTROL DE ACCESO BASADO EN EL CONTEXTO

El control de acceso basado en contexto es un conjunto de comandos IOS que se pueden usar para inspeccionar paquetes de forma mucho más sencilla que usando las listas de acceso normales. El CBAC funciona haciendo un seguimiento de las conexiones exteriores iniciadas desde dentro de los cortafuegos. CBAC identifica las sesiones rastreando las direcciones origen / destino y los números de puerto origen / destino extraídos de los paquetes. Cuando una respuesta regresa del equipo remoto de la sesión en forma de tráfico entrante, CBAC determina la sesión a la que pertenecen los paquetes entrantes. CBAC mantiene de esta forma una lista dinámica de sesiones activas y es capaz de hacer malabarismos con las excepciones de seguridad dependiendo de cada caso. Esta lista dinámica, llamada tabla de estado, hace un seguimiento del estado de las sesiones válidas hasta que finalizan. La tabla de estado de CBAC se mantiene a sí misma eliminando las sesiones cuando los usuarios las finalizan o desechándolas después de un período máximo permitido de inactividad llamado tiempo de espera. Los valores de tiempo de espera los especifica el administrador de red para cada protocolo de transporte.

PRINCIPALES FUNCIONES DEL CORTAFUEGOS DE IOS

El cortafuegos IOS mejora de forma selectiva las reglas de seguridad basadas en el contexto de cada sesión. Para realizar esto, los cortafuegos IOS deben inspeccionar paquetes de forma más cuidadosa que lo hacen las simples listas de acceso. Por esta razón, el software de cortafuegos de IOS es granular en su aplicación de las reglas de inspección. Granular aquí significa que las reglas de inspección se aplican de forma mucho más selectiva que el esquema permitir/denegar <<todo o nada>>, que usa en las listas de acceso. Esto hace a los cortafuegos más flexibles y crea una barrera de seguridad más resistente de piratear.

- **Inspección SMTP**. Muchos de los peores ataques de virus se inyectan por sí mismos en las redes seguras mediante el correo electrónico. Además de inspeccionar cada paquete en busca del número de puerto SMTP, los cortafuegos IOS inspeccionan los paquetes SMTP en busca de comandos ilegales. Cualquier paquete SMTP que contenga un comando diferente de los 15 comandos legales de SMTP será desechado como hostil.

- **Inspección Java**. Algunas políticas de seguridad de red prohíben descargar subprogramas Java de redes externas debido a su potencial poder destructivo. Una política de seguridad que por mandato ordena a todos los usuarios internos a deshabilitar Java en sus exploradores Web, no se puede hacer cumplir. Los cortafuegos IOS permiten bloquear los programas Java entrantes en el cortafuegos y también diseñar una lista de sitios seguros(amistosos) externos desde los que la descarga de subprogramas Java no se bloqueará (p es posible permitir subprogramas de todos los sitios, excepto de los sitios explícitamente definidos como hostiles).

- **Inspección H.323**. NetMeeting es una de las principales aplicaciones que usa el protocolo H.323 que requiere el uso de un segundo canal(sesión), además del canal H.323 que se mantiene en la tabla de estado CBAC. Los cortafuegos IOS pueden configurarse para inspeccionar un canal genérico TCP, además del canal H.323, con el fin de permitir a las conexiones de NetMeeting funcionar a través del cortafuegos.

- **Inspección RCP**. El comando de inspección de la RPC(Remote Procedure Call; Llamada de procedimiento remoto) del cortafuegos IOS permite que se le introduzcan números de programa. Por ejemplo, si el número del programa para NFS(Network File System Protocol; Protocolo de sistema de archivos de red) especifica en un comando RPC, entonces el tráfico NFS puede operar a través de la interfaz del cortafuegos.

CÓMO CONFIGURAR LOS CORTAFUEGOS IOS

La traducción de direcciones se configura en los cortafuegos IOS usando los comandos **nat** y **pat**. El primer paso para configurar los cortafuegos IOS es configurar la traducción para enmascarar direcciones IP internas del mundo exterior.

La seguridad basada en el contexto se configura en los cortafuegos IOS creando reglas de inspección. Las reglas de inspección (también llamadas conjuntos de reglas) se aplican a listas de acceso que gobiernan interfaces de red específicas de cortafuegos. Por tanto la configuración de un cortafuegos IOS, se realiza principalmente usando dos variantes de los dos comandos:

- **Access-list.** Un comando que se usa para definir las reglas de acceso básicas para la interfaz.
- **Ip inspect**. Un comando que se usa para definir que CBAC buscará en la interfaz.

La lista de acceso especifica las reglas normales que se aplican al tráfico entrante en la interfaz. Las reglas de inspección CBAC modifican dinámicamente las listas de acceso según sea necesario para crear entradas temporales en los cortafuegos IOS para sesiones válidas. CBAC define una sesión válida a medida que coincida cualquier conexión TCP o UDP con el criterio de la lista de acceso.

Además de crear entradas temporales en los cortafuegos, CBAC aplica reglas de inspección para detectar varias clases de ataques de red y generar mensajes de alerta, que se suelen enviar a la consola de administración de red.

CARACTERÍSTICAS DE ADMINISTRACIÓN DE SESIÓN DE LOS CORTAFUEGOS IOS

- Los comandos de sesión max-incomplete.
  - **ip inspect max-incomplete.** Comando para hacer un seguimiento y controlar sesiones medio abiertas.
  - **max-incomplete high.**
- Los comandos inspect one-minute.
  - **inspect one-minute**. Comando para controlar sesiones semiabiertas.

- Otros comandos de interceptación de TCP
  - **inspect synwait-time**. Controla ataques SYNflood borrando las peticiones de conexiones SYN que han estado pendientes durante un tiempo limite especificado(el valor predeterminado es 30 sg).
  - **Ispect finwait-time.** Controla los ataques FINflood.
  - **Inspect max-incomplete host**. Especifica los valores umbral y tiempo de espera para la detección de denegación de servicio TCP de un equipo.
  - **Inspect tdp idle-time** e **inspect udp idle-time**. Ofrece protección genérica configurando los timepos de inactividad máximos para las conexiones.

EL CORTAFUEGOS PIX DE CISCO

El cortafuegos PIX es el principal producto Cisco para tareas de cortafuegos. El conjunto de características de cortafuegos IOS está destinado a clientes preocupados por el precio o por tareas de acordonar el acceso a la red de la empresa. PIX es todo un paquete preparado por Cisco para competir, hombro con hombro, con los principales productos cortafuegos que existen actualmente en el mercado. El cortafuegos PIX difiere de los cortafuegos IOS en estas cuestiones:

- **Hardware/software integrado.** El cortafuegos PIX es un paquete integrado en una plataforma hardware construida a propósito para ofrecer servicios intensivos de cortafuegos. No se incluye como un paquete software independiente.
- **Adaptive Security Algorithm(ASA)**. No es ni un filtro de cortafuegos de aplicación proxy. PIX implementa una arquitectura que ofrece rendimiento disminuyendo el uso del proxy.
- **Opción VPN integrada**. Una tarjeta complemento de procesador configura redes privadas virtuales que soportan el cifrado avanzado Internet Security (IPSec) y los estándares Internet Key Exchange(IKE, Intercambio de claves de Internet).

El sistema electrónico y el software del cortafuegos PIX están ajustados específicamente para equilibrar la funcionalidad de seguridad avanzada con la necesidad de un alto rendimiento.

El comando **nameif**(nombre de interfaz) del cortafuegos PIX le deja especificar niveles de seguridad relativos para interfaces, tanto dentro como fuera de los cortafuegos.

Como ocurre con el cortafuegos IOS, los paquetes no pueden atravesar el cortafuegos PIX sin una conexión y un estado. El Adaptative Security Algorihm (Algoritmo de seguridad adaptativo) comprueba los paquetes entrantes usando las siguientes reglas:

- Todas las conexiones entrantes deben configurarse de forma explícita mediante un comando **conduit**. Los conductos especifican las direcciones IP externas a las que se les permite conectar a las direcciones internas más allá del cortafuegos PIX.

- Se permiten todas las conexiones externas, excepto aquéllas configuradas como denegadas en las listas de acceso exterior.

- Las conexiones exteriores estáticas pueden configurarse usando el comando **static**, sobrepasando los grupos de traducción dinámica creados con los comandos **global** y **nat** o **pat**.

PIX FIREWALL 520

PIX FIREWALL 520

ENSAMBLADO Y CABLEADO DE DISPOSITIVO CISCO

El objetivo de este documento es la instalación y configuración de dispositivos Cisco. Aunque hay muchos servicios y parámetros de configuración que son comunes a la mayoría de los productos Cisco, este documento esta centrado en los productos de gama baja, como las series 1600, 2600, 400 y 3600, o las series de switches 1900 y 2820. En este capitulo aprenderá a cablear los dispositivos Cisco para conseguir la debida conectividad entre los dispositivos de la red, y a configurar el propio dispositivo Cisco.

CABLEADO DE LA LAN

La interconexión de dispositivos de red tienen lugar a través de un cableado estructurado de la red de área local (LAN) y la red de área amplia (WAN).

En el cableado de una LAN se examinan los siguientes elementos:

- Implementación de la capa física de la LAN.
- Situación de Ethernet en el campus.
- Comparación de los requisitos de medios para Ethernet.
- Distinción entre conectores.
- Implementación de UTP.
- Cableado del campus.

IMPLEMENTACIONES DE LA CAPA FÍSICA.

El tema del cableado de la LAN tiene lugar en la Capa 1 del modelo de referencia OSI. Hay muchas topologías que soportan LAN y muchos tipos de medios físicos diferentes. Este documento se centra en Ethernet como conexión física y de enlace de datos para muchas de las conexiones de la LAN; en consecuencia, gran parte de este apartado se basa en los aspectos físicos de dicha topología. La figura 2.1 muestra un subconjunto de implementaciones de capa física que pueden ser aplicados para soportar Ethernet

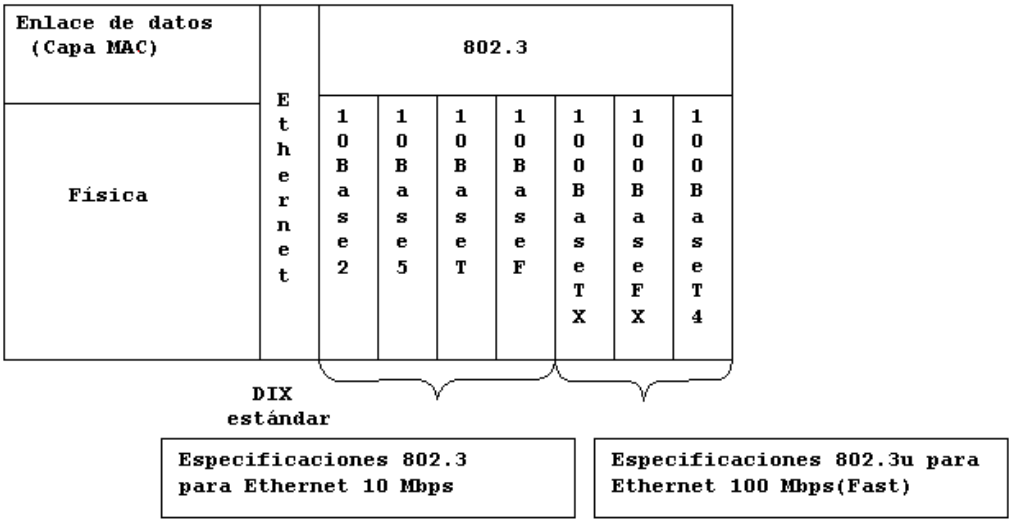


Figura 2.1 Ethernet: implementaciones de LAN.

SITUACIÓN DE ETHERNET EN EL CAMPUS

Dada una gran variedad de velocidades de Ethernet que pueden ser implementadas en el campus, se necesita determinar cuándo, si procede, y dónde es preciso llevar a cabo una o más implementaciones de Fast Ethernet. La tecnología disponible es capaz de soportar implementaciones de Ethernet de 10 ó 100 Mbps a través de la LAN, siempre que se disponga de la infraestructura de cableado y el hardware apropiado.

Dónde y qué tipo de conectividad debe usarse, puede relegarse a la jerarquía de la red del núcleo, distribución y acceso, temas tratados anteriormente. La tabal 2.1 ofrece especificaciones de conectividad Ethernet sugeridas de acuerdo con el modelo jerárquico de tres capas.

Tabla 2.1. Recomendaciones de conectividad Ethernet en un modelo de red jerárquico.

	Situación Ethernet 10BaseT	Situación Fast Ethernet
Capa de acceso	Proporciona conectividad entre el dispositivo de usuario final y el switch de acceso.	Ofrece acceso al servidor a 100Mbps a PC de alto rendimiento y puestos de trabajo.
Capa de distribución	No suele usarse en esta capa.	Proporciona conectividad entre las capas de acceso y distribución. Proporciona conectividad desde la capa de distribución hasta la capa principal. Proporciona conectividad desde el bloque del servidor hasta la capa principal
Capa principal	No suele usarse en esta capa.	Proporciona conectividad interswitch.

Como se aprecia en la tabla 2.1 Ethernet 10 Mbps se implementa generalmente en la capa de acceso para conectarse a los puestos de trabajo, reservándose tecnologías más rápidas para la interconexión de los dispositivos de red, como routers y switches. Sin embargo hay muchos diseñadores que están considerando el uso de Gigabit Ethernet al nivel de las capas principal, de acceso y de distribución. El coste del cableado y los adaptadores pueden hacer inabordable la implementación de Gigabit Ethernet en las tres capas. Antes de tomar cualquier decisión, se ha de tener en cuenta las necesidades de la red y los posibles requisitos futuros, que tal vez pudieran sobrecargar la red si se usan medios lentos.

En general, la tecnología Fast Ethernet puede usarse en una red de campus de diferentes formas:

- Fast Ethernet se utiliza como enlace entre los dispositivos de la capa de distribución y la capa de acceso, soportando el tráfico agregado desde cada segmento Ethernet sobre el enlace de acceso.

- Muchas redes cliente/servidor padecen el problema de que demasiados clientes intentan acceder al mismo servidor, creando un cuello de botella en el punto donde el servidor se conecta a la LAN. Para mejorar el rendimiento cliente/servidor a través de la red del campus, los servidores corporativos se conectan entre sí por medio de enlaces Fast Ethernet con Ethernet conmutada, se puede crear una solución efectiva para evitar redes lentas.

- Los enlaces Fast Ethernet pueden usarse también para proporcionar conexión entre la capa de distribución y la capa principal. Dado que el modelo de red de campus soporta enlaces duales entre cada router de la capa de distribución y el switch principal, el tráfico combinado desde múltiples switches de acceso pueden ser equilibrado por medio de dichos enlaces.

COMAPARACIÓN DE LOS REQUISITOS DE MEDIOS PARA ETHERNET

Además De considerar las necesidades de la red, antes de dedicarse por una implementación de Ethernet, se han de tener en cuenta los requisitos de medio y conectores de cada implementación.

Las especificaciones de cables y conectores utilizados para soportar Ethernet provienen del conjunto de estándares de la Electronic Industries Association y de la más recientes Telecommunications Industry Association (EIA/TIA) Commercial Building Telecommunications Wiring Standars. La EIA/TIA especifica un conector tipo Rj-45 para el cable de par trenzado sin blindaje (UTP). Las letras "Rj" son las iniciales de registrer jack, y el número 45 hace referencia a un tipo de cable específico.

En la Tabla 2.2 se puede ver una comparación entre las especificaciones de cable y conector para las implementaciones de Ethernet más populares. La diferencia más importante a observar aquí es el medio utilizado para Ethernet 10 Mbps y Ethernet 100 Mbps. En las redes de hoy día, donde se combinan necesidades de 10 Mbps y 100 Mbps, se debe atender prioritariamente a la necesidad de cambiar a la Categoría 5 de UTP para soportar Fast Ethernet.

Como implica el acrónimo UTP(unahielded twisted-pair, par trenzado sin blindaje), esta conexión consta de pares de cables trenzados, embutidos en una funda no blindada. Estos cables no tienen blindaje porque UTP obtiene toda su protección del efecto de cancelación de los pares trenzados. El efecto de cancelación mutua del cable trenzado minimiza la absorción de radiación de energía eléctrica del entorno próximo. Esto ayuda a reducir los problemas al transmitir señales, como cruces(interferencia métrica en un cable que está situado cerca del cable que envía la señal) y los efectos de campos eléctricos próximos(ruido).

Tabla 2.2 Especificaciones de cableado y conectores Ethernet.

	10Base5	10BaseT	100BaseTX	100Base FX
Medio	Coaxial de 50 ohmios	EIA/TIA Categoría 3, 4,5 UTP, par 2	EIA/TIA Categoría 5 UTP, par 2	Fibra multimodo 62,5/125 micrones
Longitud de Segmento Máxima	500 metros	100 metros	100 metros	400 metros
Topología	Bus	Estrella	Estrella	Punto a punto
Conector	AUI	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)	Conector duplex de interfaz de medios (MIC)ST

DISTINCIÓN ENTRE CONECTORES

La figura 2.3 ilustra distintos tipos de conectores utilizados en cada implementación de capa física. De los tres ejemplos mostrados, el conector Rj-45 y el jack son los más utilizados.

IMPLEMENTACIÓN DE UTP

Si se fija en un conector final Rj-45 transparente, verá ocho cables de colores. Estos cables están trenzados en cuatro pares dentro de la envoltura final. Cuatro de los cables son conductores tip(del T1 al T4), mientras que los otros son conductores ring(de R1 a R4). Tip y ring son términos que provienen de los albores del teléfono. Hoy día, estos términos se refieren al cable positivo(tip) y al cable negativo (ring) del par. Los cables del primer puerto de un cable o conector vienen designados como T1 y R1, los del segundo como T2 y R2, y así sucesivamente. Las Tablas 2.3 y 2.4 muestran los detalles de dos estándares de cableado UTP.
Un conector Rj-45 es un componente macho colocado al final del cable. Mirando del conector macho con el clip en la parte superior, la ubicación de los pins vienen numeradas del 1, a la izquierda, hasta el 8 a la derecha, como muestra la Figura 2.4.

La clavija jack es el componente hembra de un dispositivo de red, clavija aérea o de chasis. Mirando el puerto del dispositivo, las ubicaciones de las hembras de conexión corresponden al 1 a la izquierda, y al 8 en el extremo derecho.

Para que pueda pasar la corriente eléctrica entre el conector y el jack, el orden de los cables debe seguir los estándares EIA/TIA 586ª y 586B, como se describen en las tablas 2.3 y 2.4. Además de identificar la categoría correcta del cable EIA/TIA usado para conectar un dispositivo, es necesario determinar se si debe usar un cable cruzado o un cable directo.

Figura 2.3 Tipos de conectores para el cableado Ethernet

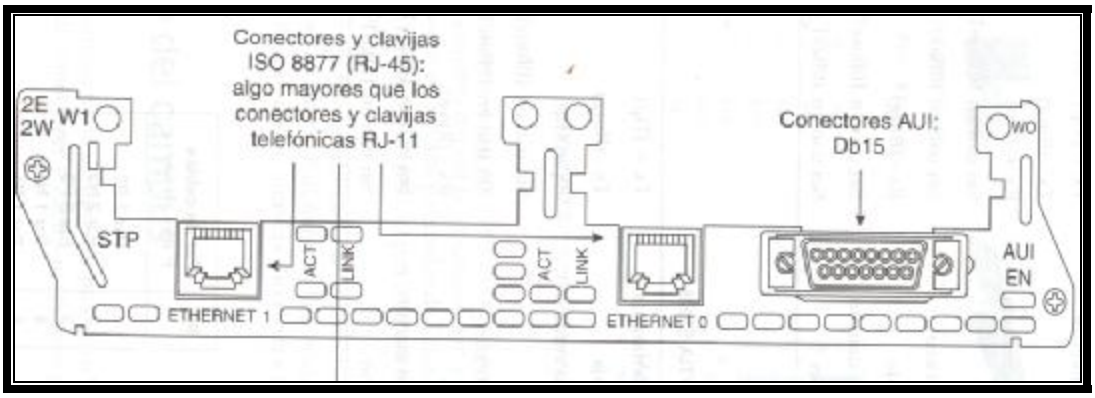


Tabla 2.3 Estándar de cableado UTP EIA/TIA 568A.

Pin 1	Par 2	Blanco/verde	Tx + (Tip)
Pin 2	Par 2	Verde	Tx -(Ring)
Pin 3	Par 3	Blanco/naranja	Rx +(Tip)
Pin 4	Par 1	Azul	Sin uso en 10BaseT y 100BaseT
Pin 5	Par 1	Blanco/azul	Sin uso en 10BaseT y 100BaseT
Pin 6	Par 3	Naranja	Rx-(ring)
Pin 7	Par 4	Blanco/Marrón	Sin uso en 10BaseT y 100BaseT
Pin 8	Par 4	Marrón	Sin uso en 10BaseT y 100BaseT

Tabla 2.4 Estándar de cableado UTP EIA/TIA 568B.

Pin 1	Par 2	Blanco/naranja	Tx + (Tip)
Pin 2	Par 2	Naranja	Tx -(Ring)
Pin 3	Par 3	Blanco/verde	Rx +(Tip)
Pin 4	Par 1	Azul	Sin uso en 10BaseT y 100BaseT
Pin 5	Par 1	Blanco/azul	Sin uso en 10BaseT y 100BaseT
Pin 6	Par 3	Verde	Rx-(ring)
Pin 7	Par 4	Blanco/Marrón	Sin uso en 10BaseT y 100BaseT
Pin 8	Par 4	Marrón	Sin uso en 10BaseT y 100BaseT

CABLE DIRECTO

Un cable directo mantiene las conexiones de pin a través de todo su recorrido. En consecuencia, el cable conectado al pin 1 debe ser el mismo en ambos extremos del cable. La figura 2.5 muestra que los conectores Rj-45 en ambos extremos presentan todos los hilos en el mismo orden. Si se sostienen los dos extremos RJ-45 de un cable uno al lado de otro en la misma orientación, se verán todos los cables de color(o hileras de pin) en cada extremo del conector. Si el orden de los cables de color es el mismo en los dos extremos, se trata de un cable directo.

Utilice cables directos para conectar dispositivos como PC o routers a dispositivos como hubs o switches. La figura 2.6 muestra las guías de conexión cuando se usan cables directos.

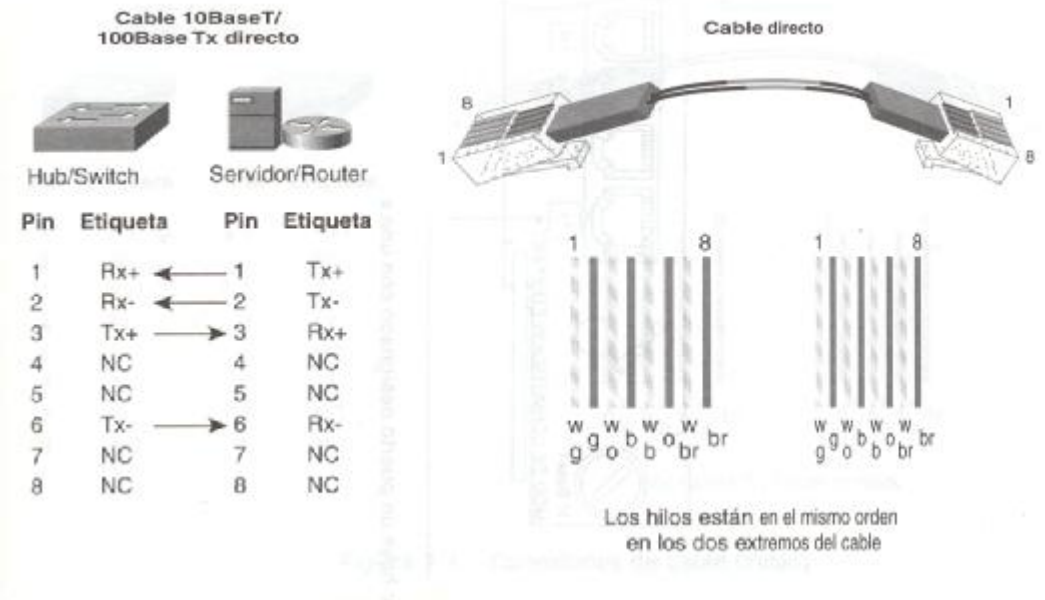


Figura 2.5 Conexiones de cable directo.

Figura 2.6 Determinación de cuándo se debe usar un cable directo.

CABLE CRUZADO

Un cable cruzado invierte los pares críticos para conseguir una correcta alineación, transmisión y recepción de señales en dispositivos con tales conectores. Los conectores RJ-45 en ambos extremos poseen algunos de los hilos en el extremo del cable, cruzados con patillas(pins) diferentes en el otro extremo. Concretamente, en el caso particular de Ethernet, el pin 1 de un lado debe conectarse al pin 3 del otro extremo. Además el pin 2 de un extremo debe estar conectado al pin 6 del extremo opuesto.

Los cables cruzados se utilizan para conectar dispositivos similares, por ejemplo, switch con switch, switch con hub, hub con hub, router con router, o PC con PC.

Figura 2.8 Determinación de cuándo se debe usar un cable cruzado.

CABLEADO DEL CAMPUS

Para cablear un escenario de tipo campus, se debe determinar el medio físico que se utilizará y el tipo de conectores y cables necesarios para interactuar con los dispositivos de red.

La figura 2.9 ilustra que pueden ser necesarios diferentes tipos de cables en una red dada. El tipo de cableado requerido debe basarse en todo caso el tipo Ethernet que se implemente. En general, debe determinarse el medio físico utilizado-10 Mbps o 100 Mbps-. Este parámetro es indicado de la categoría de cable que se va a necesitar. Por último, se ha de localizar la interfaz y determinar si se necesita un cable de tipo directo o cruzado.

Sugerencia_

El cable de la Categoría 5 es un medio ideal para el cableado de un edificio o un campus, dado que soporta tasas de transferencia de 10 y 100 Mbps. Así, si se requiere una migración de uno a otro, no es necesario volver a cablear el sistema.

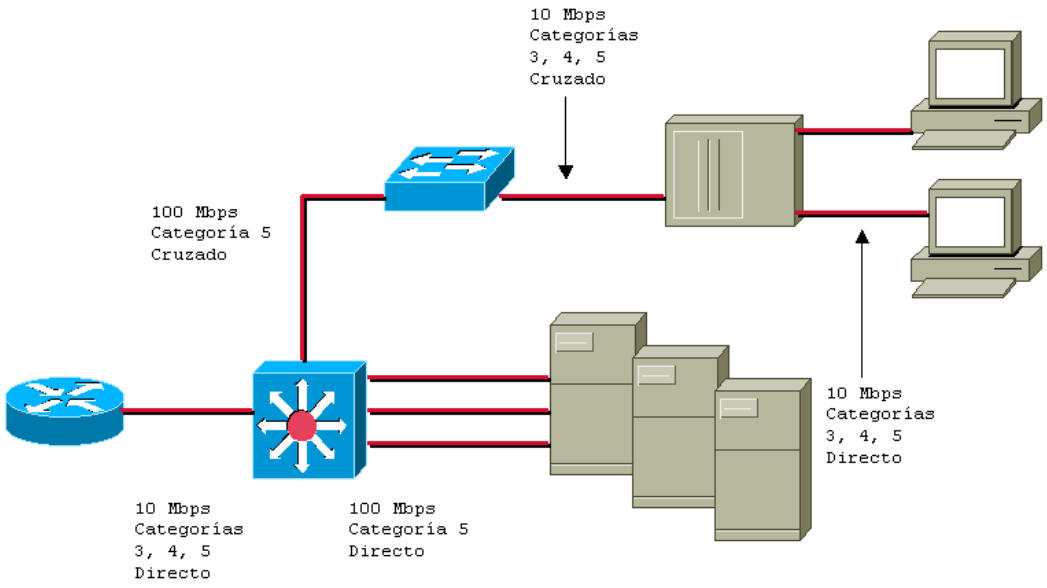
CABLEADO DE LA WAN.

Para poder conectar nuestras redes a otras redes remotas, a veces es necesario utilizar servicios WAN. Los servicios WAN proporcionan distintos métodos de conexión, y los estándares de cableado difieren de los usados en las LAN. Por tanto, es importante entender los tipos de cableado necesarios para conectar estos servicios. La figura 2.10 ilustra el cableado de una WAN típica.

En este apartado se examinan los siguientes temas:

- Implementaciones de la capa física de una WAN.
- Distinción entre conectores serie WAN.
- Cableado de routers para conexiones en serie.
- Cableado de routers para conexiones BRI de RDSI.

Figura 2.9 Las redes pueden requerir diversos tipos de cables.



IMPLEMENTACIONS DE LA CAPA FÍSICA DE UNA WAN

Hay muchas implementaciones físicas para transportar el tráfico de una WAN. Las necesidades pueden variar en función de la distancia entre los equipos y los servicios, la velocidad y el propio servicio. El tipo de capa física que se elija dependerá de la distancia, velocidad y del tipo de interfaz donde necesiten conectarse.

Las conexiones serie se utilizan para dar soporte a servicios WAN tales como líneas dedicadas que ejecutan Poin-to-point Protocol(PPP), High-Level Data Link Control (HDLC) o encapsulados Frame Relay, en la Capa 2. Las velocidades de la conexión oscilan generalmente entre 56Kbps y T1/E1 (1,544/2.048 Mbps). Otros servicios WAN, como RDSI, ofrecen conexiones de acceso telefónico bajo demanda o servicios de línea telefónica de respaldo.

Una interfaz de acceso básico (BRI) de RDSI está compuesta de dos canales Bearer de 64 Kbps para datos y un canal Delta a 16 Kbps utilizado para la señalización y otras tareas de administración de enlaces. PPP se utiliza normalmente para transportar datos sobre canales B.

DISTINCIÓN ENTRE CONEXIONES WAN EN SERIE

La transmisión en serie es el método de transmisión de datos en la que los bits de datos se transmiten por medio de un único canal. Esta transmisión de uno en uno contrasta con la transmisión de datos en paralelo, que es capaz de pasar varios bits al mismo tiempo. Para la comunicación a larga distancia, las WAN utilizan la transmisión en serie. Para transportar la energía por medio de bits, los canales serie usan un rango de frecuencias óptico o electromagnético.

HDLC PPP	FRAME RELAY	RDSI BRI(con PPP)
EIA/TIA-232 EIA/TIA-449 X.21 V.24 V.35 HSSI		RJ-45 NOTA: el patillaje Es distinto del RJ-45 Usando en Campus

Figura 2.11 Implementaciones de capa física de WAN.

Las frecuencias, descritas en términos de ciclos por segundo (o hercios), funcionan como una banda o espectro para las comunicaciones, por ejemplo, las señales transmitidas por medio de líneas telefónicas de voz de hasta 3 KHz (miles de hercios)-. El tamaño de esta frecuencia se denomina **ancho de banda.**

Hay varios tipos de conexiones físicas que permiten establecer conexiones con servicios WAN en serie. Dependiendo de la implementación física elegida, o del tipo de implementación física impuesto por el proveedor, es necesario seleccionar el tipo de calve serie adecuado para usar con el router. La figura 2.12 muestra las distintas opciones de conectores serie disponibles. Tenga en cuenta que los puertos serie de la mayoría de los dispositivos Cisco utilizan un conector patentado de 60 pins. En consecuencia, en los extremos de los routers de la mayoría de los cables adaptadores para puertos se usa un conector macho de 60 pins, teniendo que adaptarse el extremo del cable que comunica con la red al hardware especifico del servicio WAN.

Otra forma de expresar el ancho de banda consiste en especificar la cantidad de datos en bits por segundo(bps) que pueden ser transportados usando dos de las implementaciones de capa física mostradas en la figura 2.12. la tabla 2.5 compara los estándares físicos de las distintas opciones de conexión WAN en serie.

CABLEADO DEL ROUTER PARA CONEXIONES SERIE

Además de determinar el tipo de cable, se ha de determinar si se necesitan conectores de equipo de terminal de datos(DTE) o de equipo de terminación de circuito de datos (DCE) para el sistema. DTE es el punto final del dispositivo de usuario en el enlace WAN. DCE es, por lo general, el punto donde la responsabilidad de distribuir los datos pasa por las manos del proveedor de servicios.

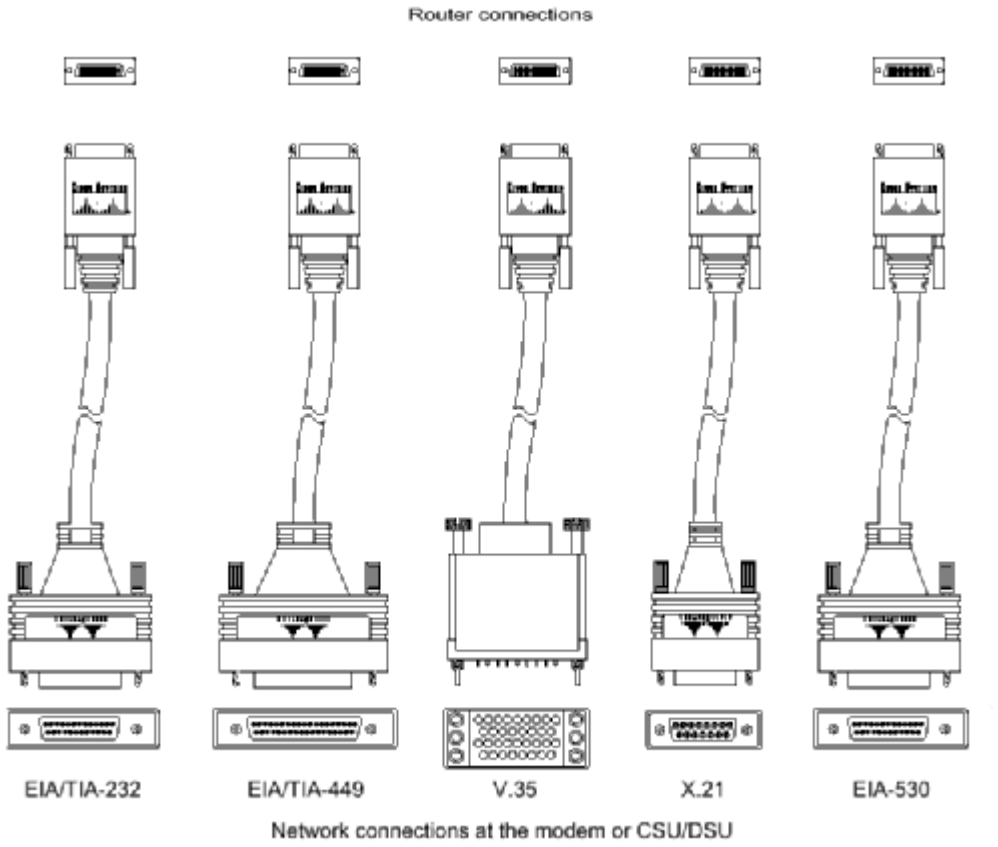


Figura 2.12 Opciones de conexión WAN en serie.

Si se va ha establecer una conexión directa con el proveedor de servicios, o con un dispositivo que va a realiza un cronometrado de señales, el router es un DTE y no necesita un cable serie DTE. Este suele ser el caso de los routers.

Hay ocasiones, no obstante, en que el router necesita ser el DCE. Por ejemplo si se está diseñando un escenario frente a frente en un entorno de prueba, uno de los routers debe ser un DTE y el otro un DCE.

Tabla 2.5 Comparación entre estándares físicos.

Datos en bps	Distancia(en metros) EIA/TIA-232	Distancia(en metros) EIA/TIA-449
2400	60	1.250
4800	30	625
9600	15	312
19.200	15	156
38.400	15	78
115.200	3,7	N/D
T1(1.544.00 bps)	N/D	15

Cuando se define el cableado para una conectividad en serie, los routers deben tener un puerto modular fijo. El tipo de puerto usado afectará a la sintaxis que se utilizará posteriormente para configurar cada interfaz.

La figura 2.14 muestra un ejemplo de un router con puertos(interfaces) serie fijos. Cada puerto posee una etiqueta indicativa del tipo y número de puerto, como "serial 0". Para configurar una interfaz fija, es necesario especificar la interfaz utilizando esta misma nomenclatura.

Otros routers poseen puertos modulares. La figura 2.15 muestra ejemplos de routers con puertos serie modulares. Normalmente, cada puerto posee una etiqueta de tipo de puerto, número de ranura(ubicación del módulo) y número de puerto. Para configurar un puerto en una ranura(ubicación del módulo) y número de puerto. Para configurar un puerto en una tarjeta modular, se le pedirá que especifique la interfaz con arreglo a la siguiente sintaxis:

<tipo de puerto><número de ranura>/<número de puerto>

Un ejemplo podría ser serial 1/0

Nota_

El convenio para designar puertos puede variar dependiendo del tipo de router que se tenga. Por ejemplo, algunos routers de alto nivel, como los dispositivos de la serie 7500, puede disponer de un procesador de interfaz virtual. La designación de estos puertos podría incluir, además, la ranura VIP.

<tipo de puerto><número de ranura>/<número de adaptador de puerto>/<número de puerto>

Un ejemplo podría ser serial 1/0/0

Nota_

El router 1603 mostrado en la figura 2.15 posee interfaces serie tanto fijas como modulares. Aunque el puerto serie representado es una interfaz modular, se ha de configurar como si fuese fija, usando una etiqueta para el tipo y número de puerto, como serial 0.

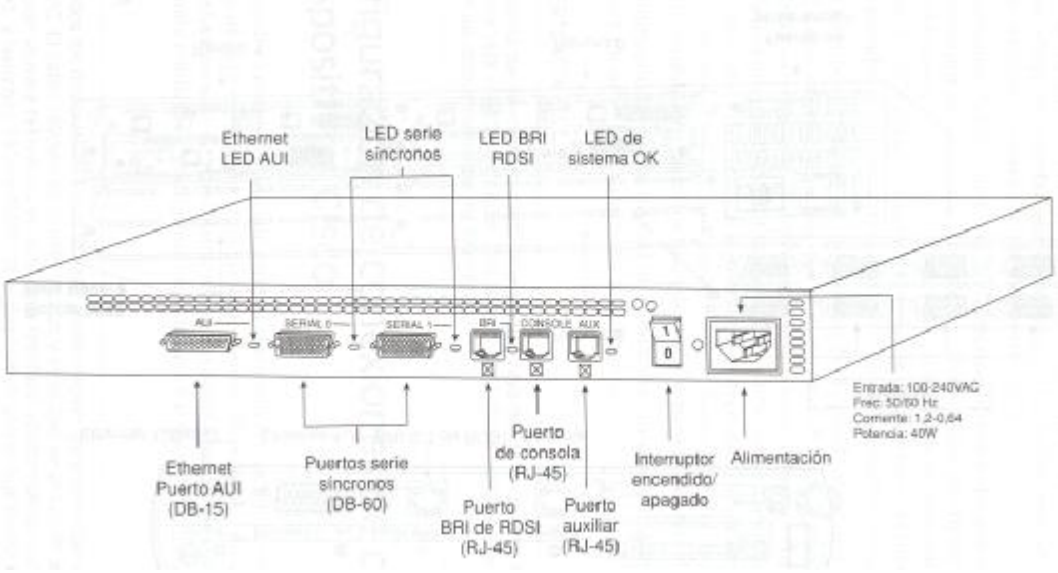


Figura 2.14 Puertos serie fijos en un router 2500

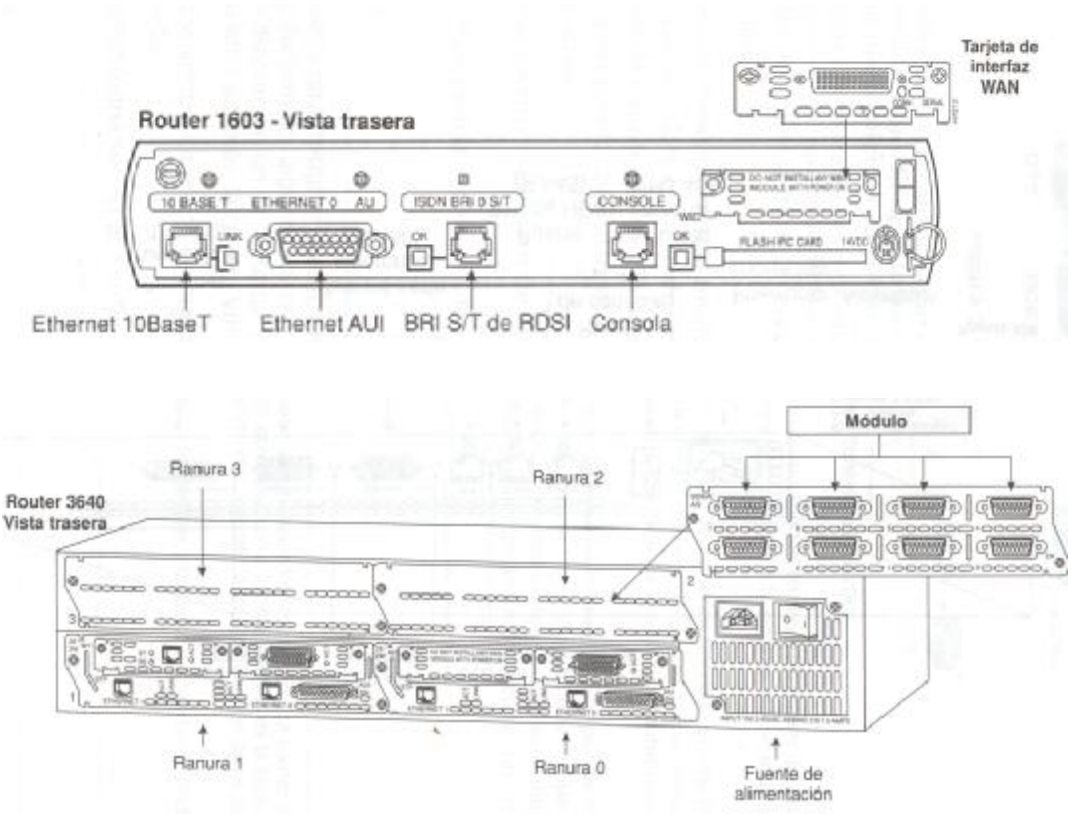


Figura 2.15 Puertos serie modulares en router 1603 y en router 3640.

CABLEADO DE ROUTERS PARA CONEXIONES BRI DE RDSI

En el cableado de BRI, se pueden utilizar dos tipos de interfaz-BRI S/T y BRI U-. Para determinar el tipo de interfaz que se necesita, se ha de determinar si uno mismo, o el proveedor de servicios, contará con un dispositivo NT1.

Un dispositivo NT1 es un dispositivo intermedio entre el router y el switch RDSI del router del proveedor(la nube) que conecta el cableado del suscriptor de cuatro hilos con el bucle local convencional de dos hilos. NT1 se refiere a un dispositivo de terminación de red de tipo 1. En Norteamérica, el NT1 lo suele proporcionar el cliente, mientras que en el resto del mundo, es el proveedor de servicios el que suministra el dispositivo NT1.

Si necesita proporcionar un dispositivo NT1, puede usar una BRI de RDSI con una interfaz U: una interfaz U indica que el dispositivo NT1 está integrado. Si utiliza un dispositivo NT1 externo, o si el proveedor de servicios utiliza un dispositivo NT1, el router necesitará una interfaz BRI S/T. Dado que los routers pueden tener múltiples tipos de interfaz RDSI, necesitará determinar la interfaz que necesita al adquirir el router. Para determinar el tipo de conector RDSI que posee el router, basta fijarse en la etiqueta del puerto.

Para interconectar el puerto BRI de RDSI con el dispositivo del proveedor de servicios, deberá usar un cable UTP directo de la Categoría 5.

Advertencia_

Es importante insertar un cable directo que vaya desde un puerto BRI de RDSI hasta un conector jack o un switch RDSI. Una BRI de RDSI utiliza voltajes que podrían dañar seriamente los dispositivos que no sean RDSI.

CONFIGURACIÓN DE CONEXIONES DE CONSOLA A DISPOSITIVOS CISCO.

Para poder configurar inicialmente el dispositivo Cisco, necesitará proporcionar una conexión de administración directamente con el dispositivo. En el caso de los equipos Cisco, dicha conexión de administración se denomina **puerto de consola**. El puerto de consola permite controlar y configurar un hub, switch o router Cisco.

Nota_

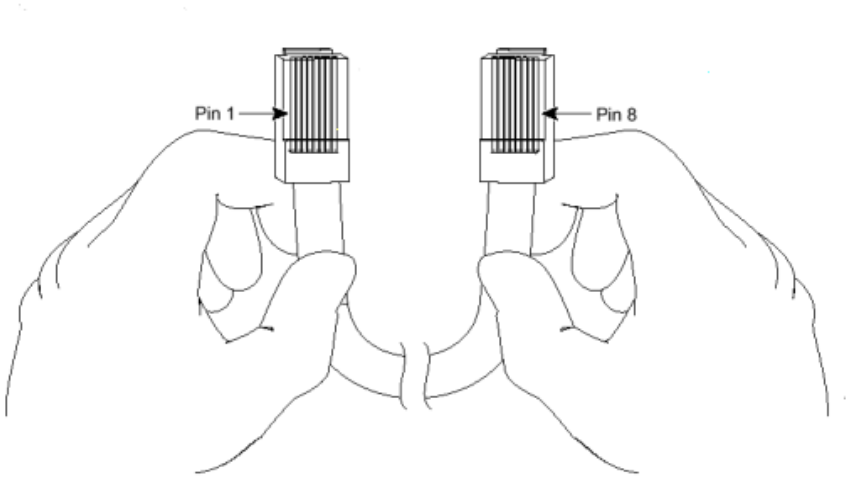
No todos los dispositivos Cisco utilizan rollover para conectar un puerto de consola a un PC. El cable rollover es más común y es el que se utiliza en los routers y switches a los que se hace referencia en este documento(es decir , routers de las series 1600, 2500, 2600 y 3600, y switches 1900 y 2800). Si el dispositivo con el que ha de trabajar es diferente, consulte la documentación del mismo para averiguar los requisitos de conectividad para la consola.

El cable rollover posee una distribución de pins distinta a la de los cables Rj-45 directos o cruzados usados con Ethernet o BRI de RDSI. La asignación de pin de un rollover es como se indica a continuación.

1-8
2-7
3-6
4-5
5-4
6-3
7-2
8-1

Para configurar la conexión entre un terminal y el puerto de una consola Cisco, ha de hacer lo siguiente:

IDENTIFICAR UN CABLE ROLLOVER



Paso 1

Cablear el dispositivo usando un cable rollover. Necesitará un adaptador Rj-45 a DB-9 o Rj-45 a DB-25 para el PC o terminal.

Paso 2

Configurar la aplicación de emulación de terminal con los siguiente parámetros de puerto COM: 9600 bps, 8 bits de datos, sin paridad, 1 bit de paro y sin control de flujo. Esto proporcionará acceso a la consola fuera de banda.

Nota_

El puerto AUX incluido en algunos dispositivos puede usarse para proporcionar administración fuera de banda vía módem. Es necesario configurar el puerto AUX usando el puerto de consola para poder hacer uso de él. El puerto AUX utiliza también los parámetros 9600 bps, 8 bits de datos, sin paridad y 1 bit de paro. El puerto AUX puede usarse también para otras funciones, como la transferencia de datos para enrutamiento basado en acceso telefónico.

OPERATIVIDAD Y CONFIGURACIÓN DE UN DISPOSITIVO CISCO IOS

En este apartado aprenderá el proceso de iniciar y configurar un switch y un router Cisco.
También aprenderá a realizar tareas usando la interfaz de usuario del software Cisco IOS. Para instalar dispositivos Cisco en la red, es necesario que conozca el proceso de inicio del switch y del router Cisco, así como describir y reconocer una secuencia normal de arranque. También es importante proporcionar una configuración inicial para el switch y aplicar una configuración inicial básica al router usando la utilidad de instalación.

Una vez establecida una configuración inicial, necesitará describir y usar los modos de comando para interactuar con el software Cisco IOS. Deberá aprender a usar la ayuda en línea asociada a la interfaz de línea de comandos **show** del switch y del router Cisco para determinar características operativas fundamentales del switch.

OPERACIONES BÁSICAS DEL SOFTWARE CISCO IOS

La plataforma de software del sistema operativo de internetwork de Cisco (IOS) está implementada sobre distintos componentes hardware descritos en este documento. El software IOS proporciona servicios de red y permite aplicaciones en red. Es la arquitectura de software integrada en todos los routers Cisco y es también el sistema operativo de la serie de switches Catalyst 1900 de empresa.

Cisco IOS habilita servicios de red en todos esos productos, entre los que figuran los siguientes:

- Características para soportar los protocolos y funciones de red elegidos.
- Conectividad para proporcionar un tráfico de alta velocidad entre dispositivos.
- Seguridad para controlar el acceso e impedir el uso no autorizado de la red.
- Escalabilidad para agregar interfaces y capacidad conforme crezcan las necesidades del trabajo en red.

Es posible acceder a una interfaz de línea de comandos (CLI) Cisco IOS a través de una conexión de consola, una conexión vía módem o una sesión Telnet. Sea cual sea el método de conexión utilizado, el acceso a la interfaz de línea de comandos IOS se denomina en general **sesión EXEC.**

Cuando se inicia un switch Catalyst por primera vez, se usa una configuración inicial con una serie de parámetros predeterminados.

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

OPERACIONES AL INICIO DEL ROUTER/SWITCH

Cuando un switch Catalyst o un router Cisco se ponen en marcha, hay tres operaciones fundamentales que han de llevarse a cabo en el dispositivo de red:

Paso 1

El dispositivo localiza el hardware y lleva a cabo una serie de rutinas de detección del mismo. Un término que se suele utilizar para describir este conjunto inicial de rutinas es power-on self test (POST), o pruebas de inicio.

Paso 2

Una vez que le hardware se muestra en una disposición correcta de funcionamiento, el dispositivo lleva a cabo rutinas de inicio del sistema. Estas rutinas inician el switch o el router localizando y cargando el software del sistema operativo.

Paso 3

Tras cargar el sistema operativo, el dispositivo trata de localizar y aplicar las opciones de configuración que definen los detalles necesarios para operar en la red.

Generalmente, hay una secuencia de rutinas de retirada que proporcionan alternativas al inicio del software cuando es necesario.

UBICACIONES DE CONFIGURACIÓN DEL ROUTER/SWITCH

El switch y el router pueden ser configurados desde distintas ubicaciones:

- En la instalación inicial, el administrador de la red configura generalmente los dispositivos de la red desde un terminal de consola, conectado por medio del puerto de consola.
- Si el administrador debe dar soporte a dispositivos remotos, una conexión local por módem con el puerto auxiliar del dispositivo permite a aquél configurar los dispositivos de red.

- Para determinados routers y switches, puede que exista un CD-ROM que proporcione una aplicación de configuración rápida, como Cisco Fast Step, con el fin de facilitar al máximo esa tarea.

Una vez realizada la conexión inicial, hay otras fuentes externas para el software que permiten conectarse a interfaces de dispositivo:

- Dispositivos con direcciones IP establecidas pueden permitir conexiones Telnet para la tarea de configuración.
- Descargar un archivo de configuración de un servidor Trivial File Transfer Protocol (TFTP).
- Configurar el dispositivo por medio de un navegador Hypertext Transfer Protocol (http).

Nota_

Los tres métodos que acabamos de mencionar presuponen la existencia de una configuración IP activa y la conectividad de la red al dispositivo.

MODOS DE COMANDO IOS

El software Cisco IOS utiliza una interfaz de línea de comandos como su entorno de consola tradicional. Aunque el software IOS constituye la tecnología principal que se extiende a muchos otros productos, los detalles operativos de Cisco IOS varían en función de los distintos dispositivos de internetworking.

Para introducir comandos en la interfaz de usuario, se han de escribir las entradas en alguno de los distintos modos de comando de la consola. Cada modo de comando está indicado por un símbolo distinto.

¿QUÉ SUCEDE CUANDO SE INICIA UN SWITCH?

La puesta en marcha inicial del switch incluye los siguientes pasos:

Paso 1

Antes de iniciar el switch, compruebe lo siguiente:

- Todas las conexiones del cableado de la red deben estar aseguradas.
- El terminal debe estar conectado el puerto de la consola.
- Debe estar seleccionada la aplicación del terminal de la consola.

Paso 2

Conecte el enchufe del cable de alimentación y encienda el dispositivo, si posee un interruptor de encendido. No todos los dispositivos cuentan con interruptor. Los que no lo tienen, arrancan en cuanto se enchufan a la red eléctrica.

Nota_

Este documento trata sólo del switch 1900 enterprise. Los comandos de información y configuración del switch son específicos de la línea de productos de la serie 1900. Es posible que en otros switches sea diferente.

LED DE ESTADO EN UN SWITCH CATALYST

Los switches Catalyst poseen varios LED de estado que están generalmente en verde cuando el switch funciona normalmente, y se vuelve ámbar cuando existe algún mal funcionamiento

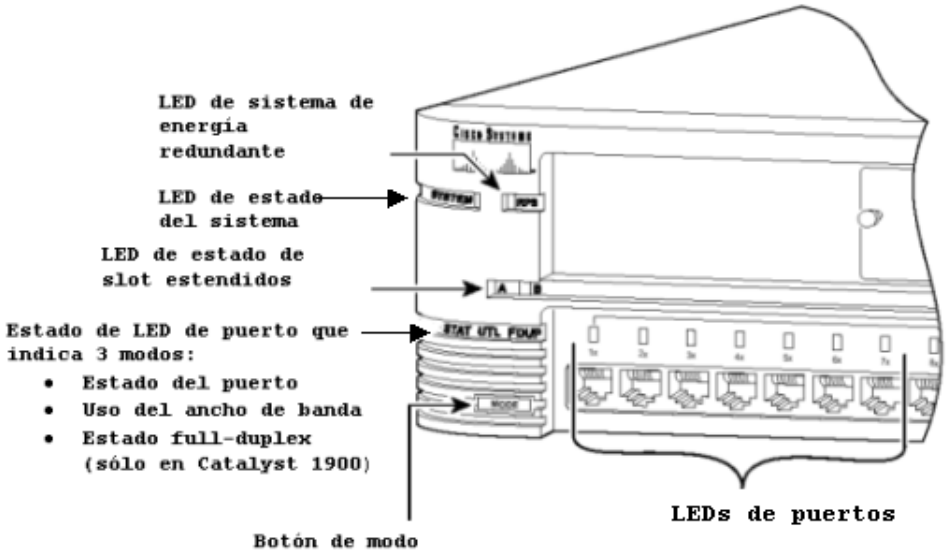


Figura 3.1 LED en un switch Catalyst

La tabla 3.1 explica las funciones de los LED System y del redundant power suply (RPS), o suministro redundante de energía, en un switch Catalyst, según los estados de las luces.

Tabla 3.1 Descripción de los estados de los LED System y RPS en un switch Catalyst.

LED del switch	Descripción
LED System	Verde: el sistema está encendido y operativo. Ámbar: el sistema no funciona bien.
Suministro redundante de Energía operativo.	Verde: RPS operativo. Ámbar: RPS instalado, pero no Verde intermitente: tanto el RPS como el suministro de energía interno están activados y la energía interna está alimentando al switch.

Los LED de puerto del switch Catalyst poseen varios modos de operación. Como verá más adelante, las rutinas de arranque iniciales utilizan los LED para mostrar el estado de las pruebas al inicio (POST).

Si el switch está activado y en marcha, pulsando el botón MODE(véase figura 3.1), se conmuta entre los demás modos de los LED. Estos tres modos indican:

- Estado del puerto.
- Utilización de ancho de banda por parte del switch.
- Soporte full-duplex.

La tabla 3.2 contiene una lista de los modos de los LED y lo que éstos indican en función de los distintos colores o tipo de iluminación.

Tabla 3.2 Descripciones de los estados de los modos de LED de puerto de un switch Catalyst.

Modo LED de puerto	Descripción
Estado LED de puerto (STAT)	**Verde:** enlace presente. **Verde intermitente:** actividad. **Verde y ámbar alternativos:** falta de enlace. **Ámbar:** el puerto no envía señales.
Utilización(UTL)	LED del 1 al 8 activados: 0,1 a <6 Mbps. LED del 9 al 16 activados: 6 a <120 Mbps. LED del 17 al 24 activados: 120 a <280 Mbps.
Full duplex(FDUP)	**Verde:** puertos configurados en modo full-duplex. **No verde:** puertos en modo half-duplex.

Los valores de utilización mostrados corresponden a un switch de 24 puertos. Éstos serán los valores para el switch de 12 puertos:

1 a 4: 0,1 a <1,5 Mbps

5 a 8: 1,5 a 20 Mbps

9 a 12: 29 a 120 Mbps

El POST Catalyst se ejecuta sólo cuando se enciende el switch. El POST utiliza los LED de los puertos de switch para indicar el avance y estado de la prueba. Inicialmente, los LE de todos los puertos están en verde. Esta condición indica el inicio del POST y que los LED funcionan correctamente. Cada uno de los 16 primeros LED de puerto(del 1x al 16x) están asociados con una de las pruebas POST, como indica la tabla 3.3

En un Catalyst 1912, el LED Ax se usa en lugar del puerto 16x como indicativo de la prueba ECU DRAM.

Después de cada test POST, el LED de dicha prueba indica los resultados de la misma:

- Si la prueba se ha completado sin fallos, el LED correspondiente se apaga.
- Si la prueba ha revelado algún fallo, el LED correspondiente se vuelve ámbar; el LED del sistema también se vuelve ámbar en este caso.

Tras un proceso POST sin fallos, los LED se vuelven intermitentes y después se apagan.

Si hay fallos fatales, como se indica en la Tabla 3.3, switch no es operativo. Con errores no fatales, el switch seguirá operativo, aunque con una funcionalidad limitada.

INICIO DE UNA SESIÓN EN UN SWITCH 1900 TRAS EL ARRANQUE

Si se detectan fallos en la prueba POST durante el arranque inicial, serán informados a la consola. Si el POST se completa con éxito, la primera pantalla que aparezca será la Menu Console Logon Screen, o pantalla del menú de inicio de sesión en la consola, como muestra el ejemplo 3.1.

Ejemplo 3.1 Menu console Logon Screen.

```
Catalyst 1900 Management Console
Copyright © Cisco Systems, Inc. 1993-1998
All rights reserved.
Enterprise Edition Software
Ethernet Address: 00-50-BD-73-E2-C0

PCA Number: 73-3121-01
PCA Serial Number: FAA0252A0QX
Model Number: WS-C1924-EN
System Serial Number: FAA0304S0U3
Power Suplí S/N: PHI025101F3
.....
1 user(s) now active on Management Console.

      User Interface Menu
      [M] Menus
      [K] Command Line
      [I] IP Configuration

Enter Selection:
```

Tabla 3.3 Asociaciones de prueba LED/POST

LED	Componente verificado	Tipo de fallo
LED 16X	ECU DRAM	Fatal.
LED 15x	No utilizado	
LED 14x	No utilizado	
LED 13x	No utilizado	
LED 12x	Motor enviado	Fatal.
LED 11x	Motor enviando SRAM	Fatal.
LED 10x	Paquete DRAM	Fatal.
LED 9x	ISLT ASIC	Fatal.
LED 8x	Control/estado del puerto.	Fatal.
LED 7x	Interruptor de cronómetro del sistema	Fatal.
LED 6x	Contenido direccionable (CAM) SRAM	Fatal.
LED 5x	Reloj en tiempo real	No fatal: si falla esta prueba, el switch envía paquetes. Sin embargo, si el switch se viene abajo inesperadamente, no podrá reiniciarse automáticamente.
LED 4x	Puerto de consola	No fatal: si falla esta prueba, no podrá acceder a la consola de administración a través del puerto de consola. Sin embargo, puede hacer un Telnet a la consola de administración.
LED 3x	CAM	Fatal.
LED 2x	Burued in address	No fatal: si falla esta prueba, el switch usa su Ethernet por omisión y comienza a enviar paquetes.
LED 1x	Puerto loopback	No fatal: si falla esta prueba, se ha perdido parte de la funcionalidad de uno o más puertos. El switch desactiva los puertos que fallan en él test y el mensaje de error en el Menu Console Logon Screen indica el puerto o puertos que no han pasado la prueba. Utilice sólo puertos que haya pasado la prueba.

En la pantalla de inicio de sesión hay tres opciones:

- Teclee **M** para entrar en el modo menú.
- Teclee **K** para entrar en el modo de línea de comandos.
- Teclee **I** para entrar en el modo de configuración IP.

El modo **M** es el modo menú. Este modo puede usarse para configurar todos los parámetros del switch. El modo menú proporciona descripciones y sugerencias relativas a los parámetros de configuración. Éste puede ser un modo útil cuando no se está familiarizado con los parámetros que se desea configurar. Es el único modo disponible en un switch 1900 estándar.

Cuando se configura el switch desde la interfaz de usuario que se ejecuta en una consola o terminal remotos, el software Cisco IOS proporciona una interfaz de línea de comandos (CLI), opción **K**, denominada comúnmente modo EXEC. El procedimiento EXEC interpreta los comandos introducidos y lleva a cabo las operaciones correspondientes. Para acceder a este modo es necesario haber iniciado la sesión previamente en el dispositivo.

Como se dijo anteriormente, por razones de seguridad, el proceso EXEC posee dos niveles de acceso a los comandos: el modo usuario y el modo privilegiado.

- **Modo usuario**. Entre las tareas típicas figuran la comprobación del estado del switch (modo sólo comprobar).
- **Modo privilegiado**. Entre las tareas típicas están el cambio de la configuración del switch.

Nota_
Por motivos de seguridad el dispositivo de red no muestra la contraseña introducida. Sin embargo, si está configurando un dispositivo de red sobre un enlace vía módem o por medio de Telnet, la contraseña se enviará en texto legible. Telnet no ofrece un método de paquetes seguros.

AYUDA DE TECKADO EN LA INTERFAZ DE LÍNEA DE COMANDOS DEL SWITCH

El switch Catalyst utiliza software Cisco IOS con varias opciones de ayuda para entradas en la línea de comandos, incluidas las siguientes:

- **Ayuda relativa al contexto**. Proporciona una lista de comandos y argumentos asociados con cada comando específico.
- **Mensajes de error de consola**. Identifica problemas con los comandos del switch introducidos incorrectamente para que puedan ser corregidos.
- **Búfer de historial de comandos**. Permite volver a llamar largos y complicados comandos o entradas para volver a ejecutarlos, revisarlos o corregirlos.

AYUDA RELATIVA AL CONTEXTO

Un signo de interrogación (?) durante una sesión EXEC proporciona siempre ayuda en pantalla. Hay dos tipos de ayuda relativa al contexto disponibles: ayuda de texto y ayuda relativa a la sintaxis de un comando.

Puede utiliza ? para obtener una lista de todos los comandos que comienzan por una secuencia de caracteres determinada. Para ello, escriba el carácter o caracteres seguidos del signo ? . No incluya ningún espacio de separación delante del signo de interrogación. El switch mostrará un lista de todos los comandos que comienzan con los caracteres especificados.

También puede usar ? para conseguir ayuda acerca de la sintaxis específica de un comando. Introduzca ? en lugar de una palabra clave o argumento sobre cuya sintaxis no está seguro. Recuerde que ha de incluir un espacio delante de ?. El dispositivo de red mostrará en pantalla una lista de las operaciones disponibles para el comando en cuestión, donde <cr> representa un retorno de carro.

Sugerencia_
Es posible abreviar los comandos en Cisco IOS introduciendo el número suficiente de caracteres. Por ejemplo, en lugar de teclear el comando show interface, bastaría introducir sh int.

MENSAJES DE ERROR DE CONSOLA PARA SWITCHES

Los mensajes de error de consola del sistema de ayuda del switch Catalyst permiten identificar problemas relativos a entradas de comandos incorrectas. La implementación del mensaje le ayudará a averiguar cómo debe modificar la entrada de la línea de comandos para corregir el problema.

La tabla 3.4 muestra un listado donde se describen algunos errores CLI comunes y explica cómo obtener ayuda.

Tabla 3.4 Mensajes de error CLI comunes.

Mensajes de error	Significado	Cómo obtener ayuda
%Ambiguous command: "show con"	No se han introducido suficientes caracteres para que el switch pueda reconocer la orden.	Vuelva a introducir la orden seguida de un signo de interrogación(?) sin espacio entre la orden y dicho signo.
%Incomplete command	No se han introducido todas las palabras clave o valores requeridos por la orden	Vuelva a introducir la orden seguida de un signo de interrogación (?) con un espacio entre la orden y dicho signo.
% Invalid input detected at `^` marker	Se ha introducido la orden incorrectamente. El circunflejo (^) marca el punto donde se ha detectado el error.	Introduzca un signo de interrogación (?) para obtener un listado de todas las órdenes que están disponibles en este modo de comando.

BÚFER DE HISTORIAL DE COMANDOS PARA SWITCHES

Revisar el historial de comandos proporciona una lista del contenido del búfer de sustitución del switch. Se trata de una lista de los comandos introducidos recientemente. Para ver dichos comandos, introduzca el comando **history** del software Cisco IOS.

```
Switch#history
```

A continuación verá una lista con el historial de comandos, lo que le permitirá volver a utilizar cualquiera de ellos sin necesidad de teclearlo de nuevo.

Para volver a presentar un comando introducido con anterioridad, pulse la tecla flecha arriba. Si sigue pulsando esa misma tecla, accederá a otros comandos anteriores. Algunos teclados no disponen de tecla flecha arriba, o es posible que la aplicación no soporte el uso de dichas teclas. Una alternativa a la flecha arriba es la combinación de teclas Ctrl-p. Para recorrer el historial de comandos en sentido inverso, puede usar la combinación de teclas Ctrl-n. Una vez que llegue al comienzo o el final de la lista, no seguirán mostrándose más comandos. La tabla 3.5 describe las funciones del historial de comandos.

Sugerencia_

Aunque es posible almacenar hasta los últimos 256 comandos introducidos, no es aconsejable hacerlo. Estos comandos utilizan recursos de memoria valiosos y son descartados al final de cada conexión con la consola.

Tabla 3.5 Desplazamiento en el historial de comandos

Comando o combinación de teclas	Funcionalidad
Ctrl-p o tecla flecha arriba	Rellamada al último comando(previo).
Ctrl-n o tecla flecha abajo	Rellamada al comando más reciente.
Switch>show history	Muestra el contenido del búfer de comandos.

Nota_

La serie de switches 1900 soporta dos versiones de software: estándar y enterprise. La versión enterprise es la que está siendo objeto de discursión en este documento, debido a que posee funciones mejoradas. El software estándar no soporta la opción de interfaz de línea de comandos para su configuración. Agunos switches de la serie 1900 pueden ser actualizados a la versión de software enterprise, pero no es algo aplicable a todos los modelos.

¿QUÉ OCURRE CUANDO SE INICIA UN ROUTER?

Las rutinas de inicio del software Cisco IOS tiene por objetivo inicializar las operaciones del router. Para ello, las rutinas de puesta en marcha deben hacer lo siguiente:

- Asegurarse que el router cuenta con hardware verificado(POST).
- Localizar y cargar el software Cisco IOS que usa el router para su sistema operativo.
- Localizar y aplicar las instrucciones de configuración relativas a los atributos específicos del router, funciones del protocolo y direcciones de interfaz.

El router se asegura de que el hardware haya sido verificado. Cuando un router Cisco se enciende, realiza unas pruebas al inicio(POST). Durante este autotest, el router ejecuta una serie de diagnósticos para verificar la operatividad básica de la CPU, la memoria y la circuiteria de la interfaz.

Tras verificar que el hardware ha sido probado, el router procede con la inicialización del software. El modo Setup es el modo en el que entra un router no configurado al arrancar.

Nota_

Se puede utilizar el protocolo simple de administración de redes(SNMP) para administrar y configurar un dispositivo de red.

Nota_

MD5 son las siglas de Message Digest 5 y está definido por la RFC 1321. MD5 es un algoritmo de encriptación de un solo sentido, usado para codificar los datos.

Modo Setup para la inicialización del router.

```
--System Configuration Dialog  --

Continue with configuration dialog? [yas7no]: yes

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

Algunas rutinas de inicio actúan como operaciones de retroceso, capaces de hacer arrancar el router cuando otras rutinas fracasan. Un ejemplo de este comportamiento es el modo Boot ROM. Este es el modo en el que el router entra cuando no existe una copia viable del software IOS en la memoria del dispositivo. Esta flexibilidad permite que el software IOS se inicie bajo diversas situaciones iniciales.

SECUENCIAS DE TECLAS DE EDICIÓN CLI

Secuencia de teclas de edición en línea de comandos	Descripción
Ctrl-a	Traslada el cursor al comienzo de la línea.
Ctrl-e	Traslada el cursor la final de la línea.
Ctrl-f	Traslada el cursor un carácter a la derecha.
Ctrl-b	Traslada el cursor un carácter a la izquierda.
Esc-f	Traslada el cursor una palabra a la derecha.
Esc-b	Traslada el cursor una palabra a la izquierda.
Ctrl-d	Borra un carácter.
Ctrl-k	Borra todo a la derecha del cursor.
Ctrl-x	Borra todo a la izquierda del cursor.
Ctrl-w	Borra una palabra.
Ctrl-u	Borra la línea.
Ctrl-r	Actualiza la línea de comando y todo lo escrito hasta este punto.
Retroceso	Borra un carácter a la izquierda del cursor.
Tab	Completa un comando introducido parcialmente si se han escrito suficientes caracteres para evitar ambigüedades.

Nota_
Se puede completar una cadena de caracteres tecleando sólo los primeros caracteres de la misma y pulsando Tab. La salida en pantalla puede variar en función del nivel de software Cisco y de la configuración del router.

CONFIGURACIÓN DE UN ROUTER DESDE LA LINEA DE COMANDOS

El primer método de configuración del router presentado fue la propia utilidad Setup. Esta utilidad permite crear una configuración inicial básica. Para opciones de configuración más especificas y complejas, se debe usar la interfaz de línea de comandos para entrar en el modo de configuración del terminal.

Desde el modo de configuración global se tiene acceso a varios modos específicos de configuración, entre los que figuran los siguientes:

- **Interfaz.** Soporta comandos que permiten operaciones de configuración basadas en el uso de una interfaz. El símbolo correspondiente a este modo es el siguiente:

  Router(config-if)#

- **Subinterfaz.** Soporta comandos que permiten configurar múltiples interfaces virtuales (lógicas) en una misma interfaz física. El símbolo de este modo de configuración es el siguiente:

  Router(config-subif)#

- **Controlador.** Soporta comandos que permiten configurar controladores(por ejemplo, controladores E1 y T1). El símbolo de este modo de configuración es el siguiente:

  Router(config-controller)#

- **Línea**. Soporta comandos que permiten configurar la operatividad de una línea terminal. El símbolo de este modo de configuración es el siguiente:

  Router(config-line)#

- **Router.** Soporta comandos que permiten configurar un protocolo de enrutamiento IP. El símbolo de este tipo de configuración es el siguiente:

  Router(config-router)#

- **IPX-router**. Soporta comandos para configurar el protocolo de capa de red Novell. El símbolo correspondiente a este modo de configuración es el siguiente:

  Router(config-ipx-router)#

INTERFACES DE 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 tiene designado físicamente 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(que esta conectado a un hub Ethernet por medio de un cable de par trenzado con conectores machos RJ-45 en cada extremo).

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(en determinados casos, el puerto Ethernet se configura como hub, como ocurre con el router 2505). Los puertos serie se designan siguiendo este mismo procedimiento, donde S0 corresponde al primer puerto serie.

Los router de Cisco, como los de la serie 2500, son básicamente router estándar que vienen con un número predeterminado de puertos LAN, WAN y en serie. 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), sino 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(como el 4500) 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 numero de puerto).

Los router de la gama alta utilizan tarjetas VIP. Los routers de gama alta, como la serie 12000 de Cisco, utilizan tarjetas de Procesador de Interfaz Versátil (Versatile Interface Processor o VIP). Cada tarjeta VIP puede disponer de dos ranuras para tarjetas de interfaz. Este tipo de routers se construyen de forma personalizada, y sus interfaces se ajustan directamente a las necesidades de interfaz que pueda requerir una interconexión amplia de redes. Algunos routers como los pertenecientes a la serie 12000, también suministran interfaces de intercambio transparente, que permiten agregar tarjetas adicionales sin interrumpir el funcionamiento del router(ni el de la red que está conectada al mismo).

La configuración de una determinada interfaz depende del tipo de protocolo de red que utilice la red a la que está conectado el puerto de la interfaz.

INTERFACES LÓGICAS

Antes de dar por concluida esta explicación sobre las interfaces de router, conviene comentar brevemente las 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.

Una interfaz 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.

Otro tipo de interfaz lógica es la interfaz nula. Esta interfaz se configura en un router utilizando determinados comandos de router y sirve como un muro de contención para impedir el paso de un determinado trafico de la red. Por ejemplo, si no desea que el trafico de una determinada red pase por un determinado router(y que lo haga por otros routers incluidos en la interconexión) se puede configurar la interfaz nula de forma que reciba y vuelque todos los paquetes que la red envié a dicho router.

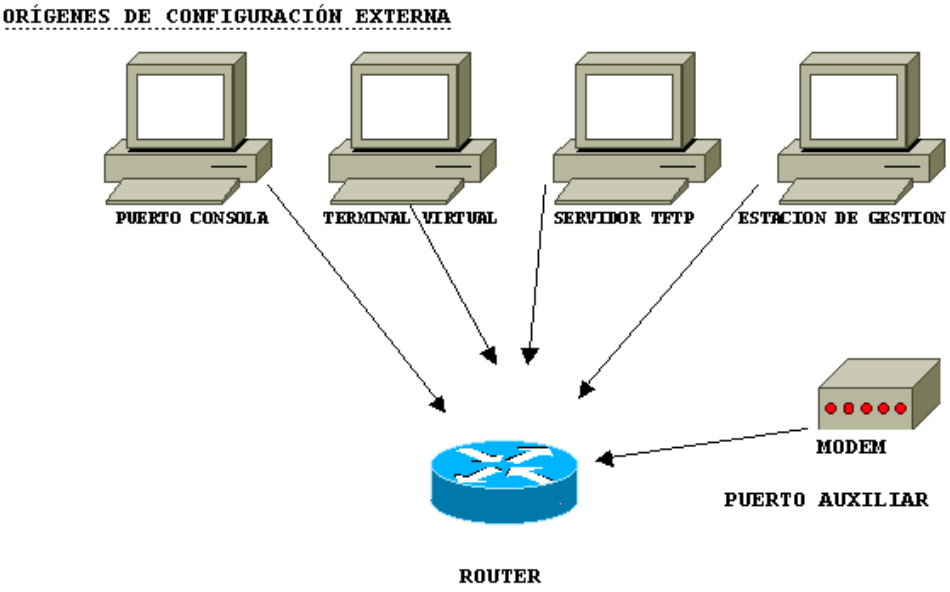
Una interfaz de túnel es otra interfaz lógica que puede utilizarse para conducir un determinado tipo de paquetes a través de una conexión que normalmente no soporta dicho tipo de paquetes.

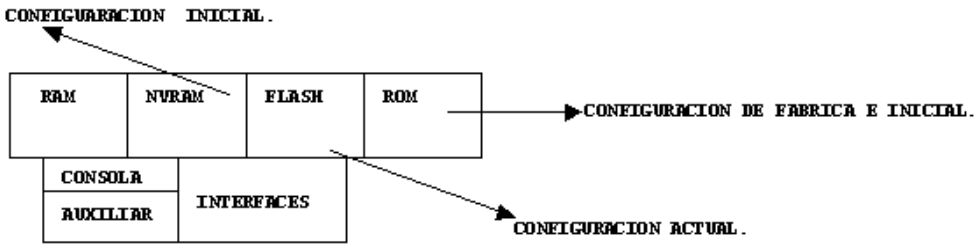
FAMILIARIZARSE CON EL ROUTER

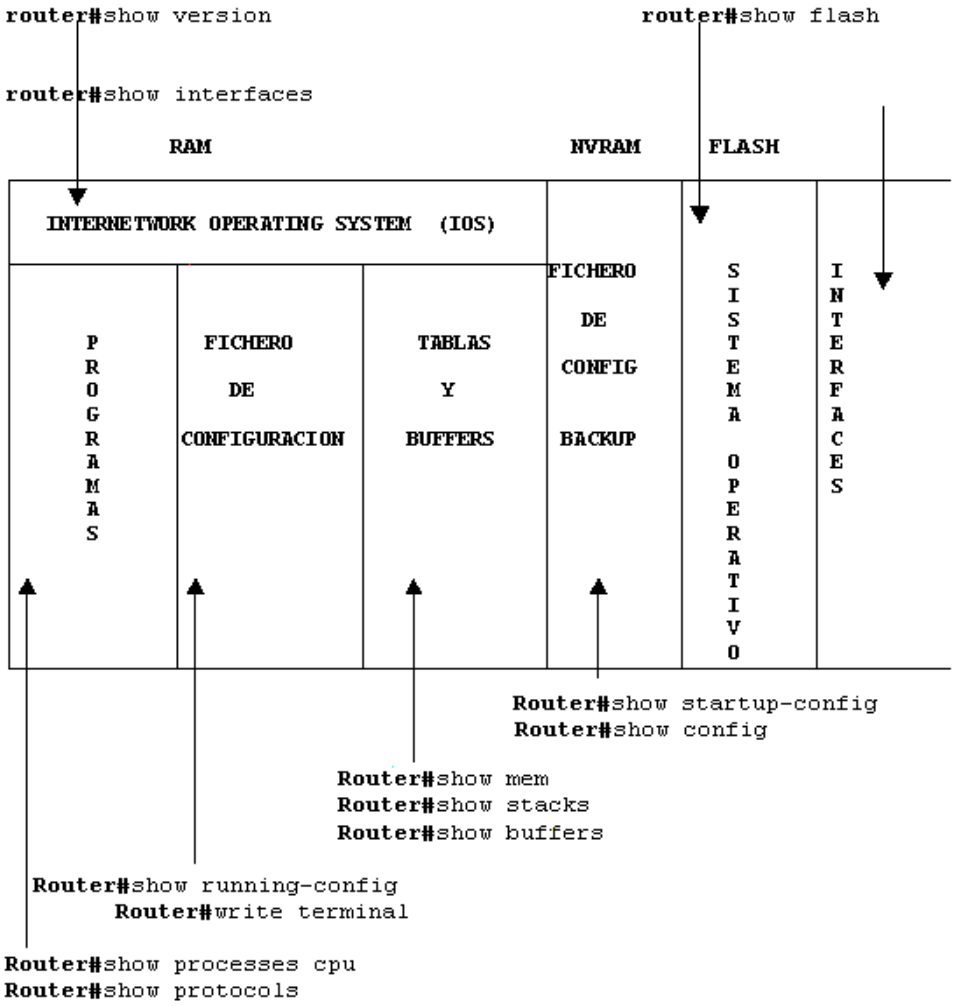
Los routers proporcionan el hardware y software necesarios para encaminar paquetes entre redes. Se trata de dispositivos importantes de interconexión que permiten conectar subredes LAN y establecer conexiones de área amplia entre las subredes.

Existen muchos modelos distintos de routers de Cisco, cada uno de ellos diseñado para satisfacer las necesidades de una determinada conexión en red o grupo de conexiones de redes. El número y tipo de puertos que integran los distintos modelos de routers varían, por lo que conviene adquirir aquél(o aquellos) que cuenten con las conexiones que requiera la interconexión que desea implementarse. (Muchos de los routers de gama alta permiten personalizar el tipo y número de interfaces).

ORÍGENES DE CONFIGURACIÓN EXTERNA







Nota_ utilizar write terminal con versiones 10.3 o menores y utilizar show config con versiones 10.3 o menores.

MODOS DEL ROUTER

Interface	Router(config-if)#
Subinterface	Router(config-subif)#
Controller	Router(config-controller)#
Map-list	Router(config-map-list)#
Map-class	Router(config-map-class)#
Line	Router(config-line)#
Route	Router(config-route)#
Ipx-route	Router(config-ipx-route)#
Route-map	Router(config-route-map)#

MODO DE CONFIGURACION DE INTERFACE

Router(config)#interfaz tipo puerto
Router(config)#interfaz tipo slot/puerto

Tipo: incluye serial, Ethernet, token ring, fddi, hssi, loopback, dialer, nule, async, bri, tunnel.

Router(config-if)#shoutdown

Utiliza este comando para deshabilitar el interfaz sin alterar sus entradas de configuración.

Router(config-if)#no shoutdown

Habilita una interfaz que ha sido deshabilitada con shoutdown

Router(config-if)#exit

Abandona el modo de configuración de interfaz

Router(config-if)#interfaz tipo numero de subinterfaz

Después de establecer el interfaz primario, utiliza este comando para establecer interfaces virtuales en un único interfaz físico.

Router(config-if)#bandwidth[ancho de banda][64]

Router(config-if)#clockrate{xxxxx][64000]

Utiliza el comando **clockrate** para proporcionar reloj [DCE] desde un interfaz serie.

En los router Cisco 4x00, se debe seleccionar el tipo de medio para el interfaz Ethernet.

Router(config)#interface ethernet[número]

Router(config-if)#media-type 10baset

Antes de establecer subinterfaces, se debe configurar 1° el interfaz primario.

Router(config)#interface serial0

Router(config-if)#interface serial 0.1 point

Router(config-if)#interface serial 0.2 multi

Modo usuario:

Acceso limitado al router.
Acceso remoto.
Router>

Modo privilegiado:

Análisis detallado del router.
Herramientas de detección de problemas.
Control de ficheros
Router#

Modo Setup:

Dialogo asistido, utilizado para establecer una configuración inicial.

Modo de configuración global:

Comandos de configuración simples.
Router(config)#

Otros modos de configuración:

Configuraciones multilínea y complejas.
Router(config-mode)#

Modo RXBOOT:

Recuperación de catástrofe en el caso de perdida de password o borrado accidental del sistema operativo de la memoria flash.

CONFIGURACION DE PASSWORD

```
Router(config)#line console 0
Router(config-line)#login
Router(config-line)#password[contraseña]
```

PASSSWORD DE TERMINAL VIRTUAL

```
Router(config)#line vty 0-4
Router(config-line)#login
Router(config-line)#password[contraseña]
```

PASSWORD DE ENABLE

```
Router(config)#enable password[contraseña]
```

ENCRIPTACION DE PASSWORD

```
Router(config)#service password-encryption
Router(config)#service password-encryption
```

NOMBRE DEL ROUTER

```
Router(config)#hostname[nombre]
```

IMAGEN DE CONEXION

```
Router(config)#banner motd#MENSAJE#
```

DESCRIPCION DE INTERFACES

Router(config)#interface ethernet 0

Router(config-if)#descripción Red local

El cable DTE posee un conector macho. (Router)
El cable DCE posee un conector hembra. (La temporización la suministra el proveedor de servicios)(CSU/DSU Unidad de servicio de canal, unidad de servicio de datos)

HABILITAR UNA INTERFAZ

No shutdown comando que habilita una interfaz.

Show version obtenemos el registro actual de configuración, en la última línea nos indica el contenido del registro de configuración. Si el valor de este registro es 0x2102, esto indica que el sistema obtiene la imagen de la memoria flash.

CONFIGURACION BASICA UTILIZANDO EL MODO SETUP.

Setup comando que inicia el programa de configuración mediante dialogo.

Router#setup

Cuando hemos creado la configuración, el router nos pregunta si queremos utilizarla.

ENTRAR EN MODO CONFIGURACIÓN DE LÍNEA

Router(config)#
Router(config)#line console 0
Router(config-line)#no exec-timeout
Router(config-line)#login (pide la password para entrar a la línea de consola).
Router(config-line)#password[clave](introduce password para acceder a la línea de consola).
Router(config-line)#

Router(config)#enable password[clave](introduce enable password).
Router(config)#enable secret[clave2](introduce password enable secret).

Router(config)#line vty 04(se sitúa sobre las líneas terminales de 0 a 4).
Router(config-line)#login (pide password para acceder a la línea de terminal virtual).
Router(config-line)#password[clave](introduce password para acceder a la línea de consola).
Router(config-line)#Ctrl-Z
Router#

LOS COMANDOS BOOT SYSTEM

Los comandos BOOT SYSTEM especifican el nombre y la ubicación de la imagen IOS que se debe cargar.

Router(config)#boot system flash[nombre_archivo]

Indica al router que debe arrancar utilizando la IOS que esta ubicada en la memoria flash.

Router(config)#boot system rom

Router(config)#boot system tftp[nombre_archivo][dirección_servidor]

Indica al router que al arrancar ha de cargar la imagen IOS de un servidor TFTP.

Si no existen comandos BOOT SYSTEM en la configuración, el router carga por omisión el primer archivo encontrado en la memoria flash y la ejecuta.

MODO MONITOR ROM

Rommon>

Router(config)#config-register[especificación del registro de configuración predeterminado]

[Ctrl-Z]

Router#reload

SECUENCIA DE ARRANQUE DEL ROUTER

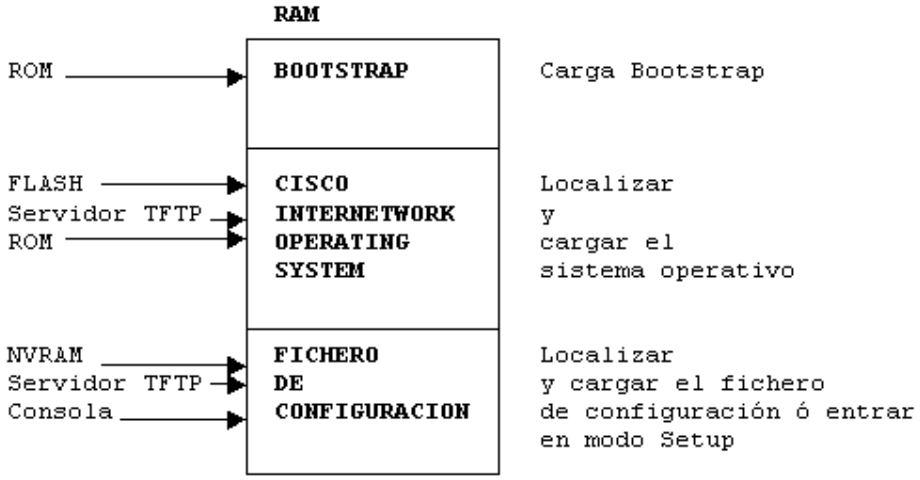
Primero se localiza el archivo de la imagen IOS especificado y se carga normalmente en la RAM para ser ejecutada, algunos routers como los de la serie 2500, no dispone de una arquitectura que pueda dar cabida a la imagen IOS, tablas de sistema y bucles de sistema en la RAM, por lo que el soft IOS se ejecuta directamente desde la memoria flash.

Si la imagen es cargada desde la flash a la RAM, deberá ser descomprimida previamente. Los archivos se guardan comprimidos en la memoria flash al objeto de ahorrar espacio. El archivo IOS se inicia una vez descomprimido en la RAM.

El comando **show flash** muestra el contenido de la flash, que incluye los nombres y tamaños de la imagen IOS.

Una ver cargado e iniciado el IO, el router debe ser configurado para poder ser utilizado. Si hay una configuración previa guardada en la NVRAM será ejecutada. Si no hay ninguna configuración en la NVRAM, el router dará comienzo al proceso de instalación automática. La instalación automática, tratas de descargar una configuración de un servidor tftp ó entrará en la utilidad SETUP, o de configuración inicial.

SECUENCIA DE ARRANQUE



COMANDOS RELACIONADOS CON EL ARRANQUE

Router#show startup-config (show config*)

Router#show running-config (write term*)

Router#erase startup-config (write erase*)

Router#reload

Router#setup

Nota_
Utilizar estos comandos (*) para routers con versión de IOS 10.3 ó inferior.

CONJUNTO DE CARACTERÍSTICAS DEL SOFTWARE IOS

Como los conjuntos de características de IOS dependen del hardware del enrutador en el que se ejecutan, se aplican dos reglas muy básicas:

- No puede hacer funcionar todos los conjuntos de características en todas las plataformas de enrutador.
- Algunas veces, características específicas de un conjunto de características se ejecutarán o no, dependiendo de la plataforma del enrutador.

Los conjuntos de características no hacen más que ofrecer funcionalidad agrupada en paquetes lógicos que los clientes pueden usar.

Agrupar los conjuntos de características en familias es la forma que tiene Cisco de ofrecer una semblanza de orden a las políticas de precios y las trayectorias de actualización.

Por ultimo, los conjuntos de características también se agrupan en variantes de productos de software:

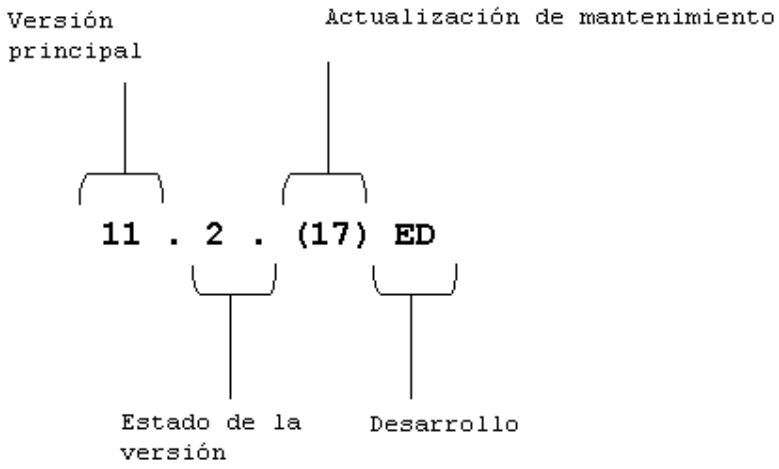
- **BASIC(Básico).** El conjunto de características básico para la plataforma hardware.
- **Plus(Avanzado).** El conjunto de características básico y características adicionales, que dependen de la plataforma hardware seleccionada.
- **Encryption(Cifrado).** Agragar una característica de cifrado de 40 bit(Plus 40) o bien de 56 bit(Plus 56) encima del conjunto de características básico o bien del Plus. El objetivo último de los conjuntos de características es guiarle a través del proceso de pedido, por ejemplo IOS Feature Set Enterprise 56 para un Cisco 7500/RSP que ejecuta la versión 11, sin cometer un error que le cueste al proyecto de actualización de red dos semanas de retraso.

ANATOMINA DE LOS NÚMEROS DE VERSIÓN DE CISCO.

Los números de versión del software de IOS tienen cuatro partes básicas. La primera parte es una versión principal, que marca el First Customers Hipmens; FCS (Primera Versión de Cliente) de una versión estable de software de IOS, de alta calidad para clientes para usar en sus redes de producción. Las versiones principales se definen mejor de la siguiente forma:

- **Estado**. El <<2>> de la figura, marca el FCS de varios estados de versión principal(primera versión, versión general de desarrollo, versión de vida corta, etc.). Se suele hacer mención a las versiones de los estados en tiempo futuro, cuando todavía están en planificación, pero no se han puesto en funcionamiento.

Las cuatro partes principales de un número de versión de IOS



- **Actualización de mantenimiento**. El 17 de la figura, que denota el soporte para otras plataformas o características más allá de las que están disponibles en las FCS de las principales versiones.

La cuarta parte del número de versión es el desarrollo. Una versión General Deployment(Desarrollo general) es para que la utilicen todos los usuarios. Las versiones Early Deployment; ED(Desarrollo temprano) se utilizan para ofrecer una nueva funcionalidad o tecnología a los clientes para desarrollar de forma limitada en sus redes. Limited Deployment; LD(Desarrollo limitado) denota un ciclo de vida restringido por FCS y GD.
En cualquier momento puede haber varias versiones principales en uso.

SISTEMA DE ARCHIVOS IOS

Sistema de archivos en memoria flash
Sistemas de archivos de red(TFTP, RCP y FTP)

Cualquier otro medio de lectura y escritura de datos(como la NVRAM, la configuración en ejecución, la ROM, la memoria RAM del sistema, el micro código incluido en el sistema, Xmodem, el registro del sistema de carga de flash, módems e interfaces BRI MUX)

La característica Sistema de archivos IOS(IFS) proporciona una interfaz única para todos los sistemas de archivos usados en el router.

"Cisco IOS File System Commands"

Una característica clave de IFS es el uso del convenio Universal Resource Locator (URL) para especificar los archivos en dispositivos de red y la propia red.

IMAGEN IOS

El uso de un servidor de red permite descargar archivos de imagen y configuración a través de la red. El servidor de red puede ser otro router, un puesto de trabajo o un sistema host.

Tener acceso al servidor.

Verificar que el servidor dispone de espacio suficiente para albergar la imagen del software IOS.

Verificar los requisitos relativos a la denominación de archivos.

Crear el archivo de destino que ha de recibir la carga, si es necesario. Este paso depende del sistema operativo del servidor de red.

INTRODUCCIÓN A LAN SWITCHING

CONCEPTOS DE LAN SWITCHING

Los conmutadores permiten a las empresas migrar de redes locales de medio compartido a redes conmutadas de gran capacidad.

Incremento en las capacidades de los procesadores, grandes requerimientos de aplicaciones cliente-servidor y multimedia, requieren mayor ancho de banda en los entornos de medio compartido.

Los switches proporcionan conexiones a estaciones individuales, servidores, segmentos de red, troncales u otros conmutadores.

Un conmutador de LAN es un dispositivo que proporciona mayor densidad de puertos a menor coste que los tradicionales Hub.

Un Lan switch es un dispositivo que consiste en un gran número de puertos que conectan segmentos de red local(Ethernet y Token Ring).

Puertos de alta velocidad(100-Mbps Fast Ethernet, Fiber Distributed Data Interface[FDDI]o 155-Mbps ATM) que conectan el LAN switch a otros dispositivos de la red.

Ancho de banda dedicado por puerto.

Asignación de menos usuarios por segmento, incrementando el promedio de ancho de banda disponible por usuario(MICROSEGMENTACIÓN).

Creación de segmentos privados o dedicados, es decir un usuario por segmento, dándole a este host un ancho de banda dedicado de 10 Mbps.

Cada usuario recibe acceso instantáneo al ancho de banda asignado y no tiene que competir con el ancho de banda disponible con otros usuarios.

Consecuencia: falta de colisiones.

Un conmutador de LAN envía tramas basadas en direcciones de nivel 2(direcciones MAC).

Los conmutadores soportan:

- Comunicaciones dedicadas entre dispositivos.
- Múltiples conversaciones simultaneas.
- Comunicaciones full-duplex.
- Adaptación a la velocidad del medio.

Las comunicaciones dedicadas entre dispositivos de red, libres de colisiones, incrementan la rapidez de operaciones tediosas como las transferencias de ficheros.

Múltiples conexiones simultaneas en la red, gran cantidad de paquetes conmutados al mismo tiempo.

La comunicación full-duplex(enviar y recibir al mismo tiempo) dobla el ancho de banda permitido.

Adaptación a la velocidad del medio, transporte de datos entre 10 y 100 Mbps, optimizando el ancho de banda.

SWITCHES

El objetivo del switch es **segmentar la red en diferentes dominios de colisión**, retransmisión y filtrado. Aprender direcciones, reenviar, filtrar paquetes y evitar bucles.

El switch segmenta el trafico de manera que los paquetes destinados a un dominio de colisión determinado, no se propague a otro segmento.

El switch hace esto aprendiendo las direcciones de los host.

Enviar una trama a todos los puertos conectados se denomina "inundar" la trama.

Debido a que los switches controlan él trafico para múltiples segmentos del al mismo tiempo, han de implementar memoria búfer para que puedan recibir y transmitir tramas independientemente en cada puerto o segmento.

FILTRADO DE TRAMAS

El switch no retransmite la trama nada mas que al puerto especifico al que va dirigida, preservando el ancho de banda del resto de enlaces.

Las tramas de difusión y multidifusión constituyen un caso especial.

Un switch nunca aprende direcciones de difusión o multidifusión, dado que las direcciones no aparecen en estos casos como dirección de origen de la trama.

La tercera función del switch es **evitar bucles**.

Las redes están diseñadas por lo general con enlaces y dispositivos redundantes. Estos diseños eliminan la posibilidad de que un punto de fallo individual, originan al mismo tiempo varios problemas que deben ser tenidos en cuenta.

Sin algún servicio de evitación de bucles implementado, cada switch inundaría las difusiones en un bucle infinito. Esta situación se conoce como BUCLE DE PUENTE.

La propagación continua de estas difusiones a través del bucle produce una tormenta de difusión, lo que da como resultado un desperdicio del ancho de banda, así como impactos serios en el rendimiento de la red u del host.

Podrían ser distribuidas múltiples copias de tramas sin difusión a los puestos de destino.

Muchos protocolos esperan recibir una sola copia de cada transmisión. La presencia de múltiples copias de la misma trama podría ser causa de errores irrecuperables.

Una inestabilidad en el contenido de la tabla de direcciones MAC da como resultado que se reciban varias copias de una misma trama en diferentes puertos del switch.

ARBOL DE EXTENSION

El protocolo de Árbol de extensión es un protocolo de tipo puente a puente desarrollado por DEC, revisado posteriormente por IEEE 802 y publicado en la especificación IEEE 802.1

El objetivo del árbol de extensión es mantener una red libre de bucles.

Un camino libre de bucles se consigue cuando un dispositivo es capaz de reconocer un bucle en la topología y bloquear uno o más puertos redundantes.

El protocolo Árbol de extensión explora constantemente la red, de forma que cualquier fallo o adición en un enlace, switch o bridge es detectado al instante. Cuando cambia la topología de red, el algoritmo de árbol de extensión reconfigura los puertos del switch o el bridge para evitar una perdida total de la conectividad, o la creación proporciona una topología de red libre de bucles llevando a cabo las siguientes operaciones.

SE ELIGE UN BRIDGE RAÍZ.

En un dominio de difusión solo puede existir un bridge raíz. Todos los puertos del bridge raíz se encuentran en estado de retransmisión y se denominan puertos designados. Cuando esta en este estado, un puerto puede enviar y recibir trafico.

PARA CADA BRIDGE NO RAÍZ HAY UN PUERTO RAÍZ.

El puerto raíz corresponde a la ruta de menor coste desde el bridge no raíz, hasta el bridge raíz. Los puertos raíz se encuentran en estado de retransmisión y proporcionan conectividad hacia atrás al bridge raíz. La ruta de menor coste al switch raíz se basa en el ancho de banda.

EN CADA SEGMENTO HAY UN PUERTO DESIGNADO.

El puerto designado se selecciona en el switch/bridge que posee el trayecto de menor coste hacia el bridge raíz. Los puertos designados se encuentran en estado de retransmisión y son los responsables del reenvío de tráfico por el segmento.
Los puertos no designados se encuentran normalmente en estado de bloqueo con el fin de romper la topología de bucle.

ESTRADOS DEL ÁRBOL DE EXTENSIÓN

Boqueo, escucha, aprendizaje, retransmisión.

LA CONMUTACIÓN COMPARADA CON ÉL PUENTEO

PUENTEADO:

Basado principalmente en SW, Una instancia de árbol de extensión por bridge, normalmente hasta 16 puertos por bridge.

CONMUTACIÓN:

Basado principalmente en HW (ASIC), múltiples instancias de árbol de extensión por switch, más puertos en un switch.

RETRANSMISIÓN DE TRAMAS.

Hay tres modos de operación primarios:

GUARDAR Y RETRANSMITIR:

El switch debe recibir la trama completa para retransmitirla. Lee las direcciones origen, destino, comprueba el CRC, aplica los filtrados y retransmite.
Si la CRC es incorrecta se descarta la trama.

MODO CORTE:

El switch verifica la dirección de destino en cuanto recibe la cabecera de la trama, y comienza de inmediato a enviar la trama. La desventaja de este modo, es que el switch podría retransmitir una trama de colisión o una trama con un valor de CRC incorrecto.

SIN FRAGMENTOS:

Modo de corte modificado, el switch lee los primeros 64 bytes antes de retransmitir la trama. Normalmente las colisiones tienen lugar en los primeros 64 bytes de una trama. El switch filtra las tramas que están libres de colisiones, por defecto el switch Catalyst 1900.

LATENCIA:

Retraso ocasionado por un dispositivo de red.

Puertos 10MB = Full-duplex
Puertos 100Mb = Half-duplex

Auto: Establece el modo duplex de negociación automática.
Full: Establece el modo full-duplex
Full-flow control: Establece el modo full-duplex sin control de flujo.
Half: Establece el modo half-duplex

VLAN LAN VIRTUALES

Seguridad, segmentación, flexibilidad.

Las VLAN permiten agrupar usuarios de un dominio de difusión común, con independencia de su ubicación física en la red. Usando la tecnología VLAN se pueden agrupar lógicamente puertos del switch y los usuarios conectados a ellos en comunidades de interés común. Las VLAN pueden existir en un solo switch o bien abarcar varios de ellos.

Las características básicas de configuración de una VLAN son los siguientes:

- Cada VLAN lógica es como un bridge físico independiente.
- Las VLAN pueden extenderse a múltiples switch.
- Enlaces troncales se encargan de transportar trafico por múltiples VLAN.

TRUNKING

Proceso que permite realizar el puenteado/conmutación entre switch.

ENLACES ENTRE SWITCH

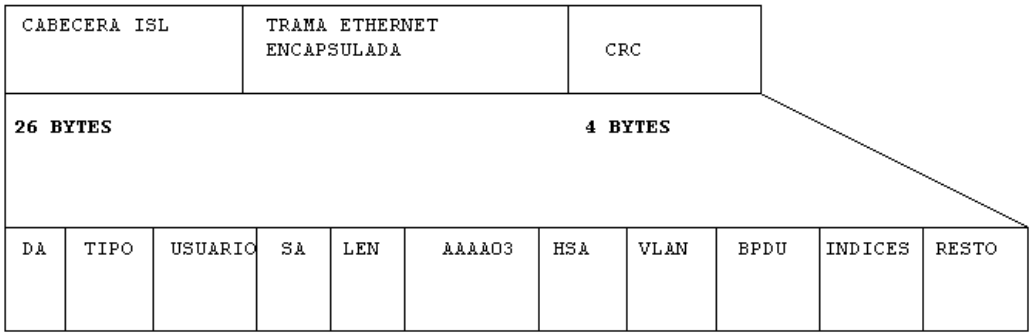
ISL Inter-Switch-Link. Los enlaces troncales ISL permiten las VLAN viajar por todo el entramado de una red conmutada.

Las características fundamentales de ISL son las siguientes:

- Ejecutada con ASIC
- No intrusivas en los puertos clientes, los clientes no ven la cabecera ISL.
- Efectiva entre switches, router y switches y switches y servidores con tarjetas de interfaz de red ISL.

ISL es un protocolo propietario de CISCO que se utiliza para interconectar varios switches y mantener la información de VLAN conforme él tráfico viaja entre los switches.

ENCAPSULADO ISL



VLAN TRUNKING PROTOCOL

Para conseguir colectividad VLAN a través del entramado de switches, VLAN deben estar configuradas en cada switch.

El VLAN trunking protocol (VTP) proporciona un medio sencillo de mantener una configuración de VLAN coherente a través de toda la red conmutada.

VTP permite soluciones de red conmutada fácilmente escalables a otras dimensiones, reduciendo la necesidad de configuración manual de la red.

VTP es un protocolo de mensajería de capa 2 que mantiene la coherencia de la configuración VLAN a través de un dominio de administración común, gestionando las adiciones, supresiones y cambios de nombre de las VLAN a través de las redes.

Un dominio VTP es u switch o varios switches interconectados que comparten un mismo entorno VTP. Cada switch se configura para residir en un único dominio VTP.

VTP OPERA EN UNO DE ESTOS TRES MODOS:

Modo servidor, modo cliente o modo transparente.
El modo VTP predeterminado es el modo servidor.

En modo servidor puedes crea, modificar y suprimir VLAN y otros parámetros de configuración que afectan a todo el dominio VTP.

En modo servidor, las configuraciones de VLAN se guardan en la memoria de acceso aleatoria no volátil(NVRAM).

Un dispositivo que opera en modo VTP cliente no puede crear, cambiar ni suprimir VLAN.

Un cliente VTP no guarda la configuración VLAN en memoria no volátil.

Tanto en modo cliente como en modo servidor, los switches sincronizan su configuración VLAN con la del switch que tenga el número de revisión más alto en el dominio VTP.

Un switch que opera en VTP transparente no crea avisos VTP ni sincroniza su configuración de VLAN, con la información recibida desde otros switch del dominio de administración. Reenvía los avisos VTP recibidos desde otros switches que forman parte del mismo dominio de administración.

Un switch configurado en el modo transparente pueden crear, suprimir y modificar VLAN, pero los cambios no se transmiten a otros switch del dominio, afectan tan solo al switch local.

Cuando se configura UTP es importante elegir el modo adecuado, ya que UTP es una herramienta muy potente y puede crear problemas en la red.

El modo servidor debe elegirse para el switch que se usará para crear, modificar o suprimir VLAN.

El modo cliente debe configurarse para cualquier switch que se añada al dominio VTP para prevenir un posible reemplazo de configuraciones de VLAN.

El modo transparente debe usarse en un switch que necesite para avisos VTP a otros switches, pero que necesitan también capacidad para administrar sus VLAN independientemente.

MODO SERVIDOR:
Envía / retransmite avisos VTP.
Sincroniza la información de configuración de VLAN con otros switches.
El switch Catalyst puede crear VLAN.
El switch Catalyst puede modificar VLAN.
El switch Catalyst puede suprimir VLAN.

MODO CLIENTE:
Envía / retransmite avisos VTP.
Sincroniza la información de configuración de VLAN con otros switches.
Las configuraciones de VLAN no se guardan en la NVRAM.
El switch Catalyst no puede crear VLAN.
El switch Catalyst no puede suprimir VLAN.
El switch Catalyst no puede modificar VLAN.

MODO TRANSPARENTE:
Retransmite avisos VTP.
No sincroniza la información de configuración de VLAN con otros switches.
Las configuraciones de VLAN se guardan en la NVRAM.
El switch Catalyst puede crear VLAN.
El switch Catalyst puede modificar VLAN.
El switch Catalyst puede suprimir VLAN.

Los avisos VTP se inundan a través del dominio de administración cada 5 minutos o cuando haya un cambio en la configuración de las VLAN.
El aviso VTP tiene un número de revisión de configuración, el número de revisión más alto indica la configuración más actual.

Para reiniciar el número de revisión de configuración en el Catalyst 1900 utilice el comando privilegiado:

delete vtp

RECORTE VTP:

Utiliza avisos VLAN para determinar cuándo una conexión troncal esta inundando tráfico innecesariamente.

El recorte VTP aumenta el ancho de banda disponible al restringir él trafico para acceder a dispositivos de red apropiados.

CONFIGURACIÓN DE UNA VLAN

Habilitar dominios VTP, definir un enlace troncal, crear una VLAN y verificar el correcto funcionamiento de la VLAN.

- El número máximo de VLAN depende del switch (1900 hasta 64 VLAN).
- VLAN1 es una de las VLAN predeterminas de fabrica.
- Los avisos CDP y VTP se envían desde la VLAN1.
- La dirección IP del Catalyst 1900 esta en el dominio de difusión VLAN1.
- El switch debe hallarse en los modos VTP servidor o transparente para poder crear, añadir o suprimir VLAN.

Si la VLAN va ha añadirse únicamente a un switch local, utilice el modo transparente.
Si se desea propagar las VLAN a otros switches del dominio, utilice el modo servidor.

Un switch se encuentra por omisión en estado VTP servidor, de modo que pueda añadirse, modificarse o suprimirse VLAN.
La pertenencia de los puertos de switch a las VLAN se asigna manualmente puerto a puerto.(pertenencia VLAN estática o basada en puertos).

Parámetros predeterminados de configuración VTP para el switch Catalyst 1900

Nombre del dominio: ninguno
Modo VTP: servidor
Contraseña VTP: ninguna (debe ser la misma para todos los switch del dominio)
Recorte VTP: deshabilitado
Interrupción VTP: habilitada (genera un mensaje SNMP cada vez que se envía un nuevo mensaje VTP).

Utiliza el comando de configuración global VTP para especificar el modo operativo, nombre de dominio, contraseña, generación de interrupciones y posibilidad de recorte.

switch(config)#vtp[server|trasparent|client]domain[nombre de dominio]trap[enable|disable]password[contraseña]pruning[enable|disable]

VTP TIENE DOS VERSIONES:

1ª versión soporta solo Ethernet.
2ª versión Ethernet y Token ring.

Configuración de línea troncal.
Establecer un puerto Fast Ethernet en el modo troncal.
Protocolo(DISL) Dinamic Inter-Switch Link, que gestiona la negociación troncal ISL automáticamente.

switch(config)#vlan[numero]name[nombre vlan]

ASIGNACIÓN DE PUERTOS A UNA VLAN

Cada vez que crea una VLAN puede asignar estáticamente un puerto o un número de puertos a la VLAN. Un puerto puede pertenecer a una sola VLAN.

switch(config)#vlan-membership[static|dynamic]vlan#
Dinamic significa que el Catalyst 1900 requiere una VMPS para la información de la VLAN basado en una dirección MAC.
Todos los puertos pertenecen por omisión a la VLAN predeterminada, VLAN1.

ENRUTAMIENTO ENTRE VLAN

En un entorno de VLAN conmutada, los paquetes se conmutan sólo entre puertos designados para residir en el mismo "dominio de difusión".

Las VLAN llevan a cabo particiones en la red y separación de tráfico en la capa 2. Por tanto, la comunicación entre VLAN no puede tener lugar sin un dispositivo de capa 3, como un router, responsable de establecer comunicaciones entre distintos dominios de difusión.

Router enclavado: Router conectado a un switch principal.

Para llevar a cabo funciones de enrutamiento entre VLAN, han de darse las siguientes circunstancias:

- El router debe conocer como llegar a todas las VLAN interconectadas para determinar cuales son los dispositivos finales, incluidas las redes que están conectadas a la VLAN, cada dispositivo final debe estar direccionado con una dirección de capa de red, como la dirección IP.

  Cada router debe conocer además la ruta hasta cada red LAN de destino.
  El router tiene ya información acerca de las redes que están conectadas directamente. Por tanto, deberá aprender las rutas a las redes que no están conectadas directamente.

- Debe existir una conexión física en el router para cada VLAN, o bien se debe habilitar la troncalidad en una conexión física individual.

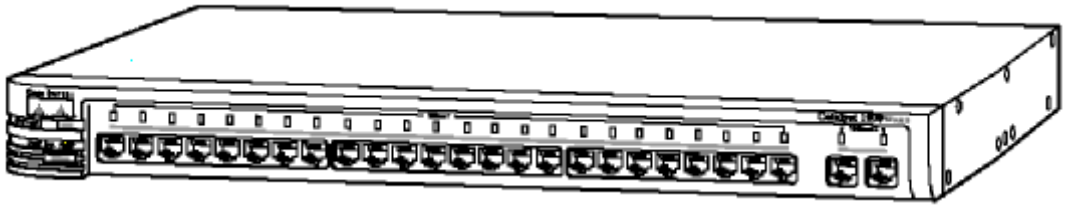
MODELOS DE SWITCHES CATALYST DE CISCO

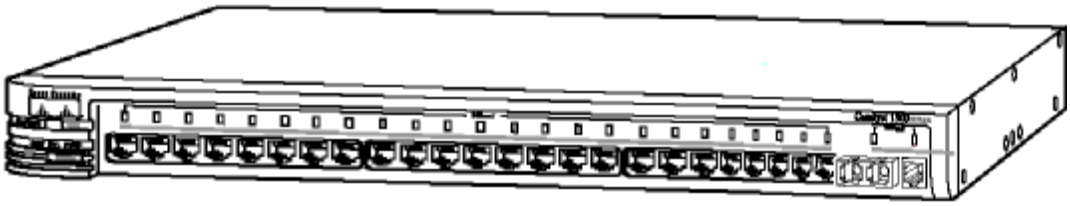
Serie de productos	Descripción
Serie MicroSwitch 1548	Conmutadores de acceso con 8 puertos Ethernet con conectividad autosensible para equipos con Ethernet de 10 Mbps y Fast Ethernet de 100 Mbps. Hay dos modelos, uno preparado suficientemente para soportar la administración remota.
Serie Catalyst 1900	Cuatro modelos con 12 y 24 puertos Ethernet y dos vínculos hacia arriba para enlaces Fast Ethernet. No se puede apilar.
Serie Catalyst 2820	Cuatro modelos destinados para agregar concentradores o servidores. Tiene 24 puertos Fast Ethernet, además dos ranuras para elegir módulos de alta velocidad, Fast Ethernet, FDDI o ATM. No se puede apilar.

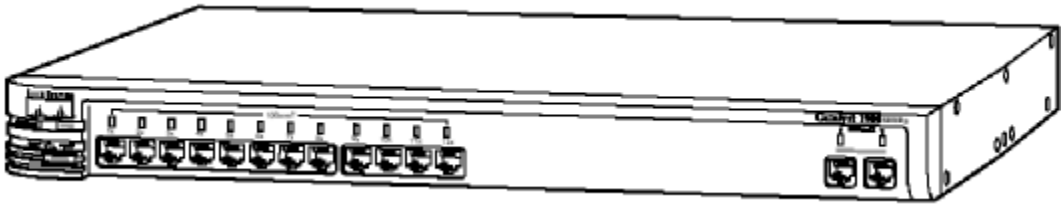
Serie de productos	Descripción
Serie Catalyst 2900	Cuatro modelos con 12 ó 48 puertos para Ethernet/Fast Ethernet 10/100 autosensibles. No se puede apilar.
Serie Catalyst 2900XL	Cinco modelos en dos paquetes básicos con 12 ó 24 puertos y dos vínculos hacia arriba de fibra óptica. No se puede apilar.

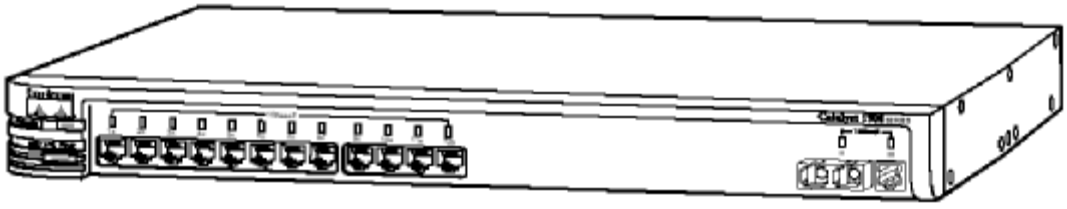
Serie de productos	Descripción
Series Catalyst 3000	Tres modelos de conmutadores multicapa con 16 o 24 puertos 10BaseT en configuraciones fijas. soporta diferentes especificaciones Ethernet y tipos de vínculos WAN. Se pueden apilar hasta ocho conmutadores en cualquier combinación de modelos.
Series Catalyst 3500XL	Tres modelos con 12 o 24 puertos 10/100 BaseT Ethernet y 2 puertos de vinculación hacia arriba de 2 Gigabit. Los 3500XL se pueden apilar hasta nueve unidades mediante una estructura de conmutador de hasta 10 Gbps. La serie 3500 es nueva y se está posicionando como la primera solución de Cisco para la conectividad de bajas prestaciones de Ethernet Gigabit.
Series 3900	Dos modelos con 20 puertos fijos de Token Ring y dos ranuras para módulos de expansión, cada uno con cuatro puertos para soportar más usuarios Token Ring, una vinculación hacia arriba ATM o dos vinculaciones hacia arriba Fast Ethernet. Se pueden apilar hasta ocho conmutadores
Serie Catalyst 4000	Un modelo con un chasis modular de tres ranuras que soporta 10/100/1000 Ethernet. Un módulo tiene 48 puertos 10/100 y otro módulo tiene 32 puertos 10/100 con distintas opciones de vinculación hacia arriba de Ethernet Gigabit. No se puede apilar.
Familia Catalyst 5000	Familia de dos series con cinco modelos, con chasis modular de 2 a 5 ranuras y entre 48 y 528 puertos soportando 100BaseX, 1000X, ATM, FDDI o Token Ring Backplane de 1.2 Gbps a 3.6 Gbps. No apilable.

Serie de productos	Descripción
Familia Catalyst 6000	Familia de cuatro modelos de conmutadores de alto rendimiento multicapa con 6 o 9 ranuras que soportan 384 puertos 10/100 y vinculación hacia arriba Ethernet Gigabit. La solución de Cisco para redes troncales Gigabit. No apilable.
Serie Catalyst 8500	Dos modelos con 5 o 13 ranuras que soportan conmutación ATM multiservicio, optimizado para agregar tráfico multiprotocolo. No apilable. La solución de Cisco para redes troncales ATM.

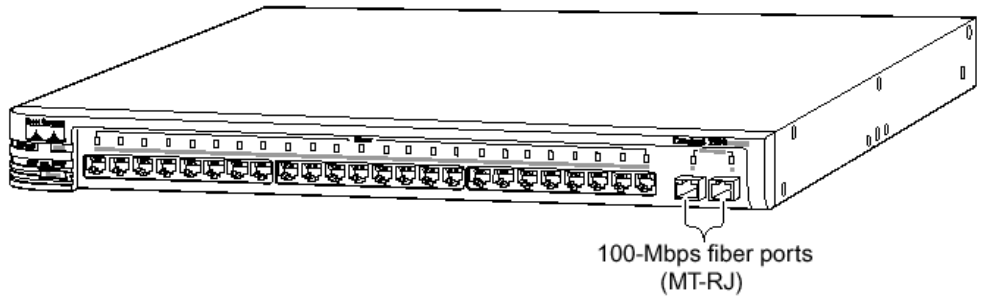


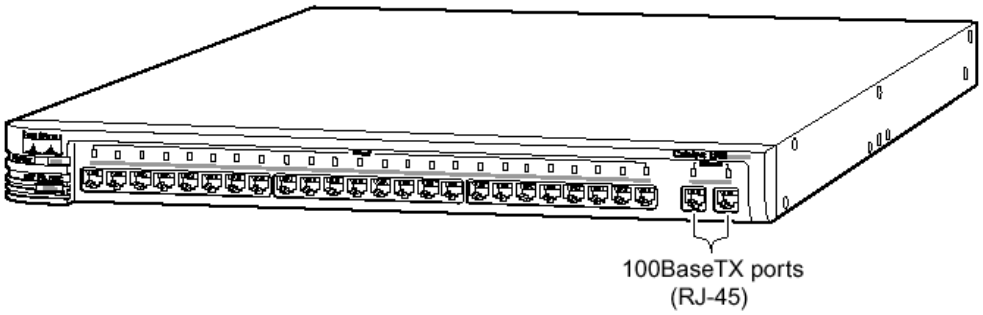


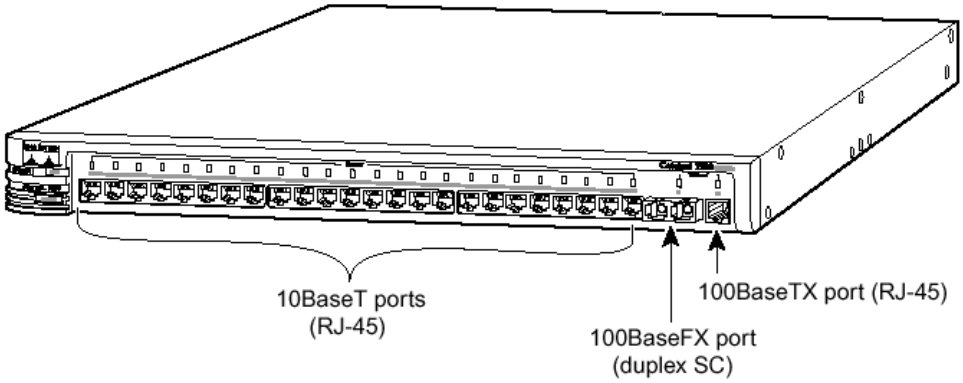


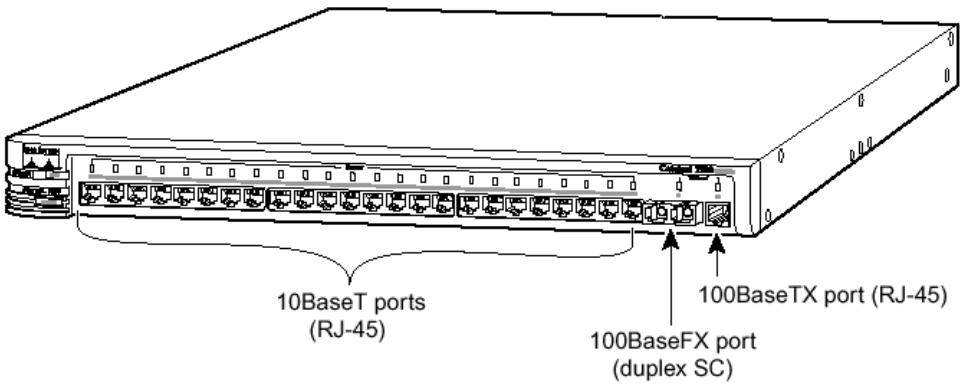


IDENTIFICAR LOS PUERTOS DE UN SWITCH CATALYST DE CISCO



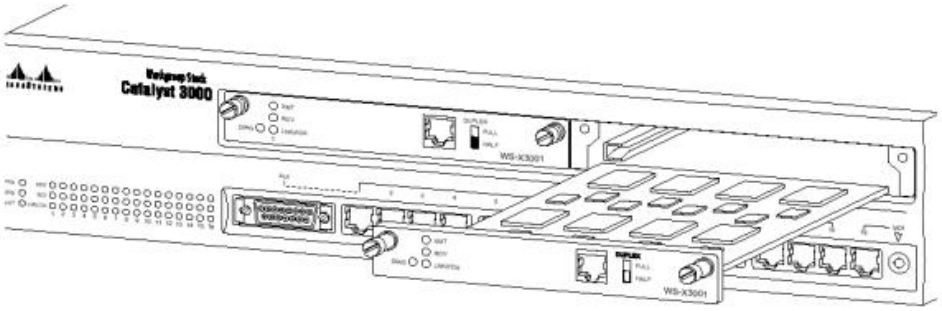




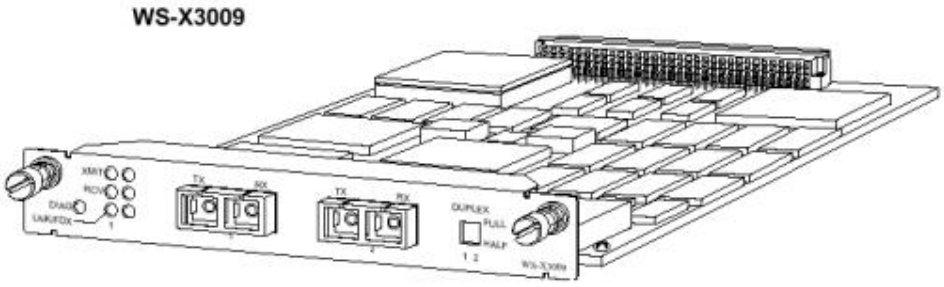


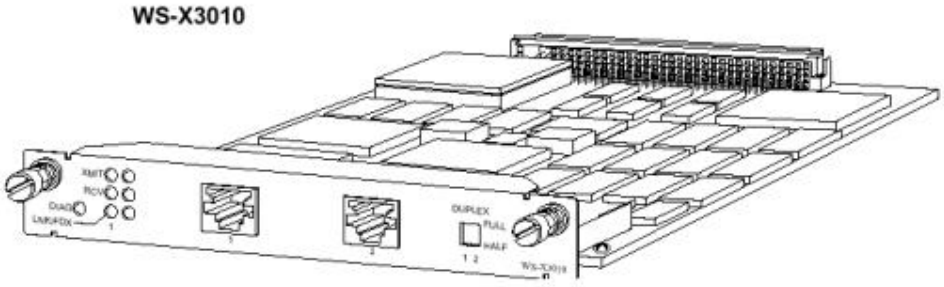
SWITCH CATAYST 30000.

INSERTANDO UN MODULO DE EXPANSIÓN 100 BASETX.

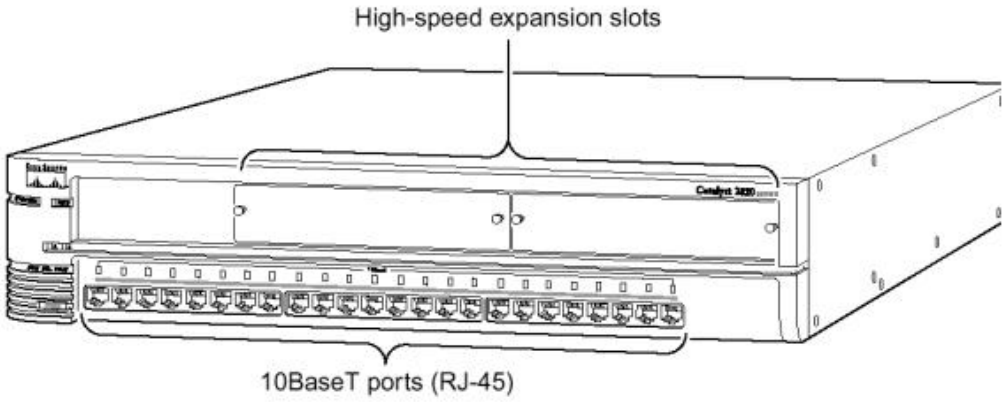


MÓDULOS DE EXPANSIÓN ISL.

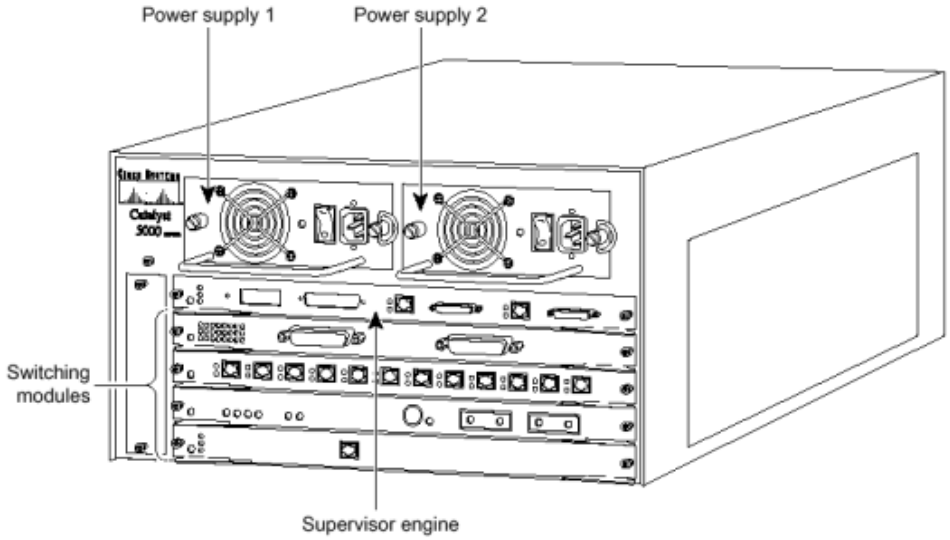




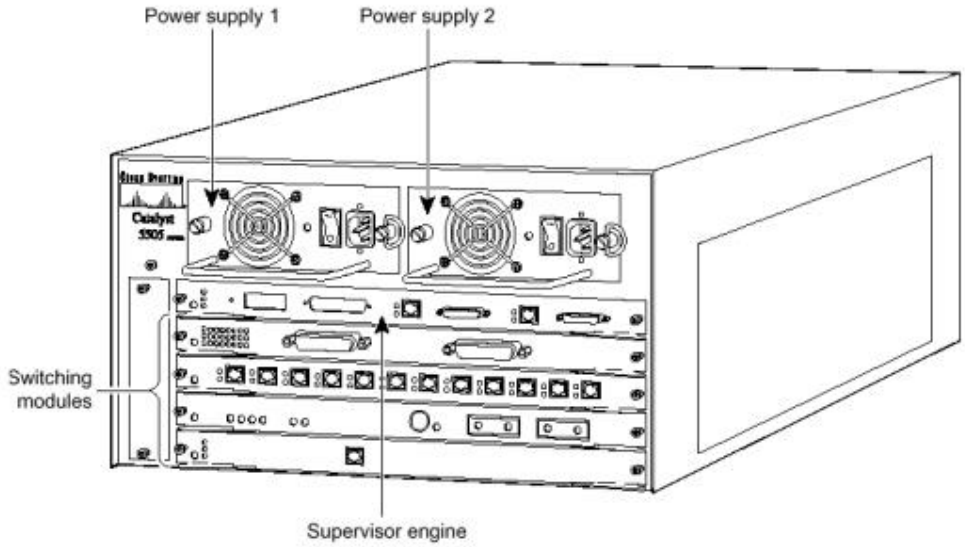
SWITCH CATALYST 2820 PANEL FRONTAL PUERTO Y MÓDULOS DE EXPANSIÓN.



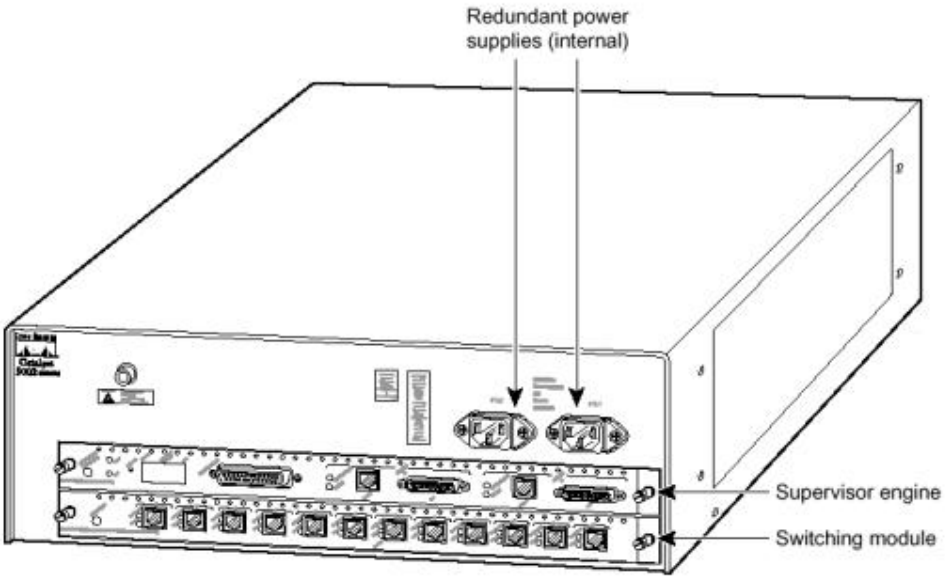
SWITCH CATALYST 5000



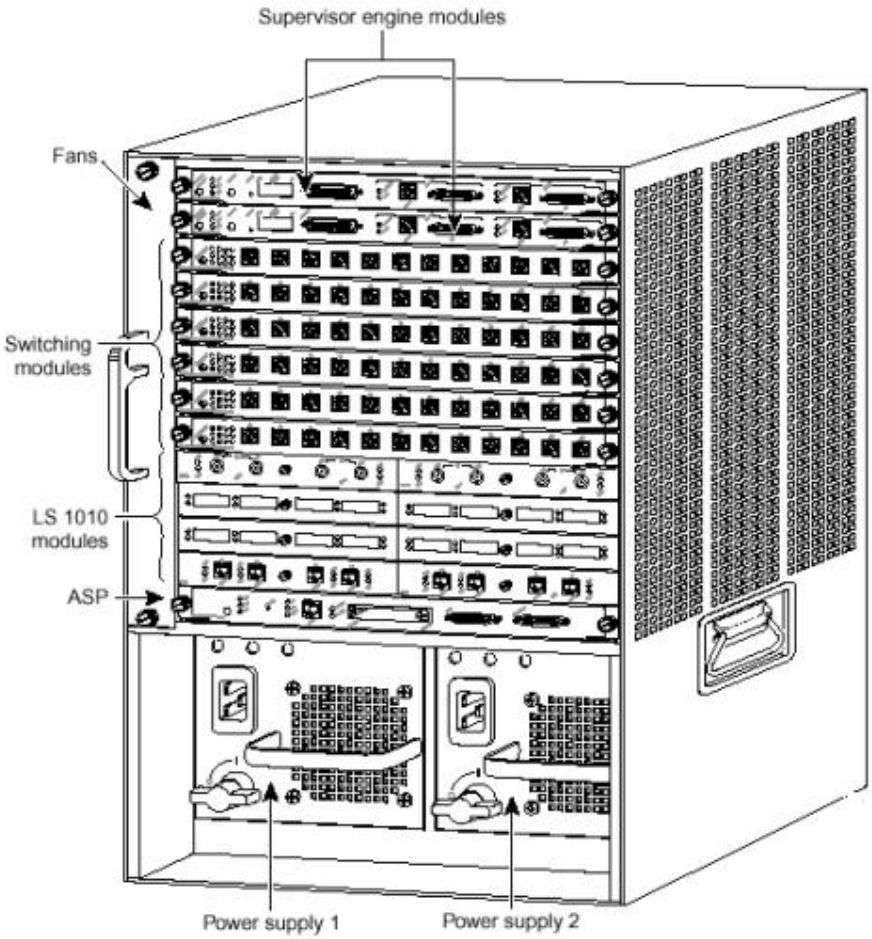
SWITCH CATALYST 5005



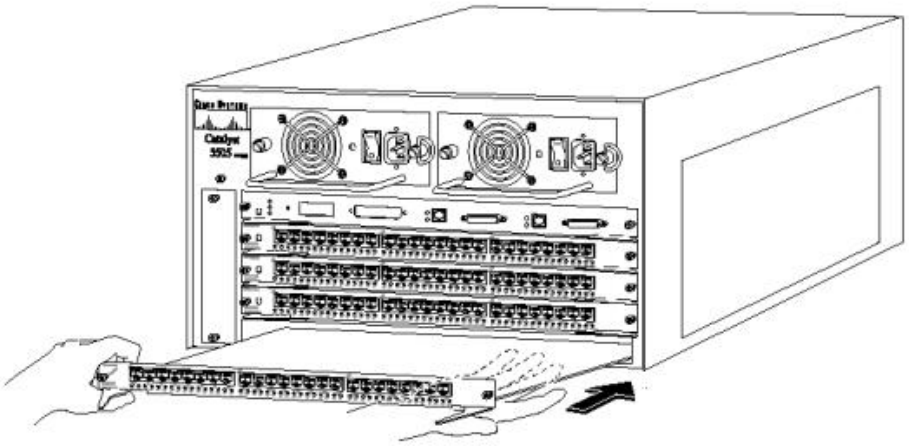
SWITCH CATALYST 5002

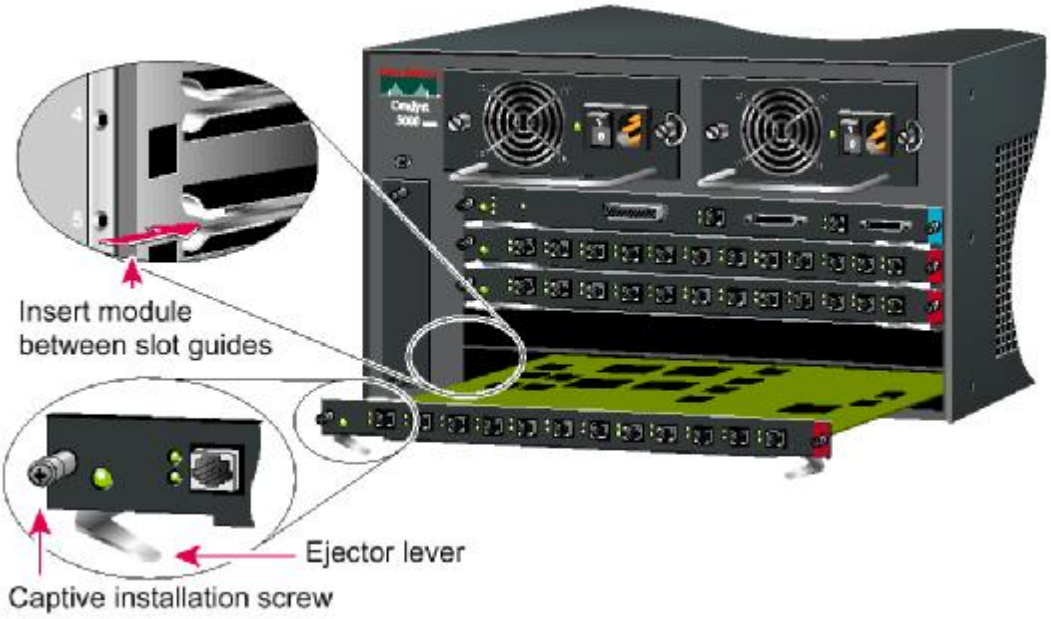


SWITCH CATALYST 5500



INSTALANDO UN MODULO EN UN SWITCH CATALYS 5500





Para soportar la troncalidad ISL, la interfaz física Fast Ethernet del router debe estar subdividida en múltiples interfaces lógicas direccionables, una por cada VLAN. Las interfaces lógicas resultantes se llaman subinterfaces.

Para configurar un "router enclabado" para el enrutamiento VLAN, ha de realizar las siguientes tares:

1. Habilitar ISL en el puerto del switch conectado al router.
2. Habilitar el encapsulado ISL en la subinterface Fast Ethernet del router.
3. Asignar una dirección de capa de red de casa subinterface.

COMANDOS DE INFORMACION DE ENRUTAMIENTO:

router#show ip protocols

router#show ip route

Nota_
Si un dispositivo(interfaz) esta configurado como DCE debería poner reloj.

PROTOCOLO CDP (CISCO DICOVERY PROTOCOL)

Se utiliza para obtener información de router que están conectados localmente.

Utilizar CDP para obtener información de nuestro propio router. Obtener información CDP de los routers vecinos, tales como plataforma y protocolo.

Alterar los intervalos por el cual un router envía y mantiene los update de CDP.

Deshabilitar el protocolo CDP en nuestro router local.

Router#show cdp[numero de interfaz]
Cdp timer[xxsg] Cambia el tiempo entre actualizaciones de paquetes cdp, es necesario estar en modo de configuración global.
El cambio afecta a todas las interfaces.
Router#configure terminal
Router(config)#cdp timer xx
Router(config)#ctrl-z
Router#
Router#show cdp interface

Show cdp neighbors para obtener los nombres y tipos de plataforma de routers vecinos, nombres y versión de la imagen Cisco IOS.

Show cdp neighbors detail para obtener datos de routers vecinos en más detalle.

Router#show cdp traffic Para saber el trafico de cdp que ocurre en el router.

Hay dos formas de deshabilitar CDP, una es en un interfaz especifico y la otra de forma general.

Router#configure terminal
Router(config)#[número de interfaz]
Router(config-if)#no cdp enable
Router(config-if)#Ctrl-Z

Show cdp interface muestra el estado de todos los interfaces que tienen activado CDP.

No cdp run deshabilita CDP en el router.

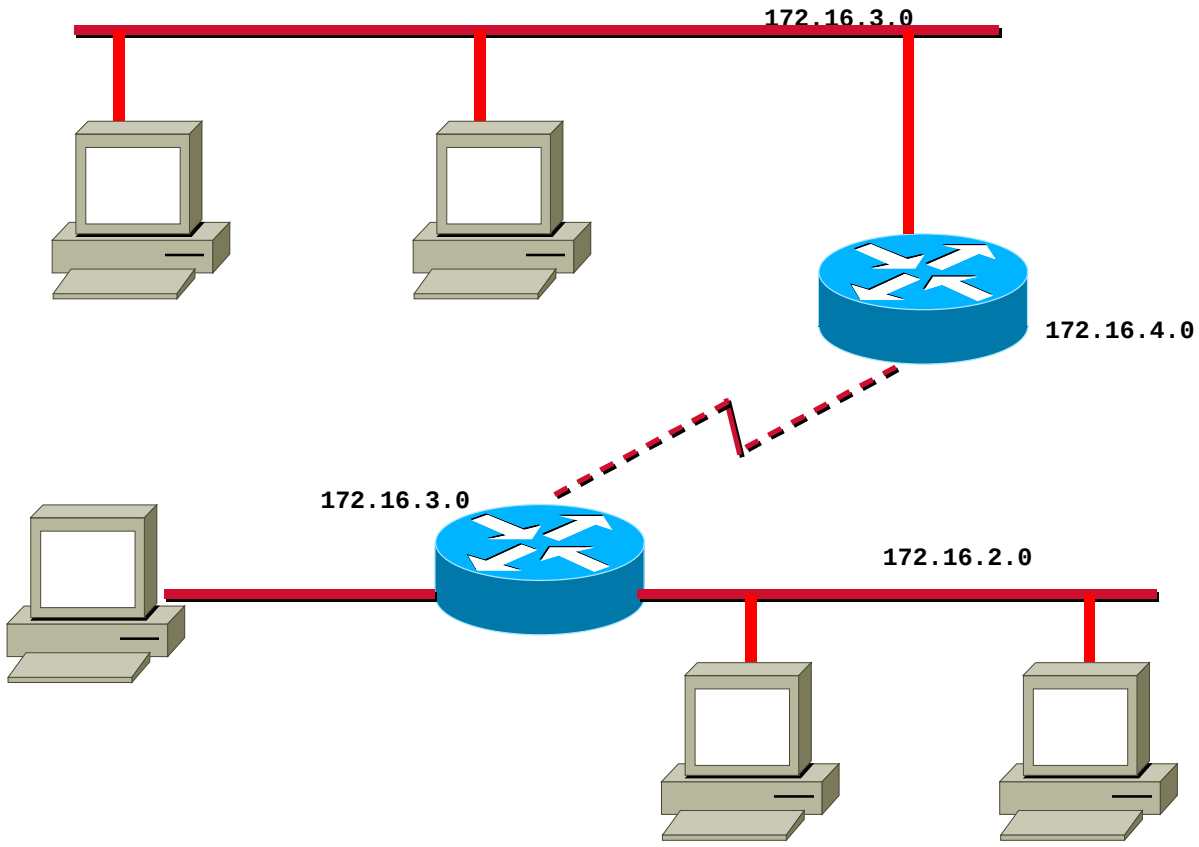
Cdp run habilita CDP en el router

Router(config-if)#cdp enable habilita CDP en el router.

Logout comando para salir del router.

EL SOFTWARE DE CISCO SOPORTA 3 TIPOS DE DIFUSION:

- **INUNDACION**
- **DIFUSIONES DIRIGIDAS**
- **DIFUSIÓN A TODAS LAS SUBREDES**



Difusión dirigida 172.16.3.255
Difusión de red local 255.255.255.255
Difusión a todas las subredes 172.16.255.255

Difusiones inundadas: 255.255.255.255 no se propagan, sino que son consideradas difusiones locales.

Difusiones dirigidas: a una red especifica, están permitidas y son retransmitidas por el router. Estas difusiones dirigidas contienen todos los bits a 1 en la parte de la dirección correspondiente al host.

Difusiones a todas las subredes: Para difundir un mensaje a todos los host de todas las subredes de una red individual, las partes de host y de la subred de la dirección deben tener todos los bits a 1.

Nota_
En IOS versión 12.0 los router no retransmiten por omisión las difusiones dirigidas y las difusiones a todas las subredes. Se debe usar el comando **ip directed-broadcast** para activar esta característica.

DIRECCIONAMIENTO IP

Ipv4 32 bits, cuatro octetos de 8 bits, separados por puntos. Cada campo de 8 bits puede tener un valor entre 00000000 (o decimal y 11111111(255 decimal).
Existen cinco clases de redes A, B, C, D y E (esta diferenciación viene dada en función del número de ordenadores que va ha tener la red).

CLASE A

0.0.0.0-127.255.255.255
Contiene siete bits para direcciones de red (el primer bit del octeto es siempre cero) y los 24 bits restantes representan a direcciones de equipo. Permite un máximo de 128 redes aunque en realidad tiene 126 ya que están reservadas las redes cuya dirección de red empieza por 0 y por 127, cada una de las cuales pueden tener 16.777.216 ordenadores,(aunque en realidad tiene 16.777.214 ya que se reservan aquellas direcciones de equipos que son todo ceros o todo unos).

CLASE B

128.0.0.0-191.255.255.255
Contiene 14 bits para direcciones de red(ya que el valor de los 2 primeros bits del primer octeto ha de ser siempre 10) y 16 bits para direcciones de equipo, lo que permite tener un máximo de 16.384 redes, cada una de las cuales puede tener 65.536 ordenadores, (aunque en realidad tiene 65.534 ordenadores cada una), se reservan todo ceros y todo unos.

CLASE C

192.0.0.0-223.255.255.255
Contiene 21 bits para direcciones de red(ya que el valor de los tres primeros bits del primer octeto a de ser siempre 110) y 8 bits para direcciones de equipo, lo que permite tener un máximo de 2.097.152 redes cada una de las cuales puede tener 256 ordenadores(aunque en realidad tiene 254 ordenadores, ya que se reservan las direcciones cuyos valores sean todo ceros o todo unos.

CLASE D

224.0.0.0-239.255.255.255
Se reservan todas las direcciones para multidestino(multicasting)
El valor de los cuatro primeros bits del primer octeto ha de ser siempre 1110 y los últimos 28 bits representan los grupos multidestino.

CLASE E

240.0.0.0-255.255.255.255
Se utiliza con fines experimentales únicamente y no esta disponible para él publico.
El valor de los cuatro primeros bits del primer octeto ha de ser siempre 1111.

La asignación de direcciones esta controlada por un organismo central, la American Registry Internetwork Numbers (ARIN) www.arin.net

CLASE A

0NNNNNNN HOST HOST HOST

Rango(1-126) El primer bit es 0, rango de números de 1.0.0.0 a 126.0.0.0, número de redes posibles 126, la 127 esta reservada. Número de host posibles 16.777.216.

CLASE B

10NNNNNN RED HOST HOST

Rango(128-191) Los dos primeros bits son 10 el rango de numero de redes es de 128.0.0.0 a 191.255.0.0, el número de redes posibles es 16.384, el número de host posibles es de 65.536.

CLASE C

110NNNNN RED RED HOST

Rango(192-223) Los tres primeros bits son 110 el rango de número de red va desde el 192.0.0.0 hasta 223.255.255.0, el número de redes posibles es 2.097.152.

CLASE D

1110MMMM G.MULTIDIFUSION G.MULTIDIFUSION G.MULTIDIFUSION

Multidifusión Rango(224-239) Los cuatro primeros bits son 1110, el rango de número de red es desde 224.0.0.0 hasta 239.255.255.255

CLASE E

Investigación El rango de números de red es desde 240.0.0.0 hasta 247.255.255.255

Las direcciones:

De 10.0.0.0 hasta 10.255.255.255
De 172.16.0.0 hasta 172.31.255.255
De 192.168.0.0 hasta 192.168.255.255

Son direcciones reservadas para ser usadas como direcciones privadas internas y no para conectarse directamente a la Internet publica.

Cada dispositivo o interfaz debe poseer un número de host distinto de 0.

MASCARA DE SUBRED

Se usa para determinar la parte de red, subred y host de una dirección IP.

Un valor de 32 bits que contiene una sucesión de 1 para los ID de red y subred y una serie de bits a 0 para el ID de host.

Si de la dirección de equipo se toman unos bits para indicar también la dirección de red, se estará estableciendo una subred. La combinación de las partes correspondientes a las direcciones de red y subred se conoce con el nombre de prefijo de red extendida.

DETERMINAR EL NUMERO DE SUBREDES NECESARIAS

El paso a seguir cuando se desea segmentar una red, es decidir el número de subredes que se necesitan y así establecer las direcciones IP de cada subred y su mascara correspondiente.

Si se toma como ejemplo que la red que se va a segmentar es una clase B(con mascara de red 255.255.0.0)y con dirección 164.56.00(en representación decimal), resulta que su dirección(en representación binaria) es:

Dirección de red		Dirección de equipo	
10100100	00111000	00000000	00000000

Se considera que con 8 subredes es suficiente para cubrir las necesidades. El primer paso, es pasar ha convertir en numero decimal 8 a su representación binaria(1000).

Dirección de red		Dirección de subred	Dirección de equipo	
10100100	00111000	1000	0000	00000000

El número binario 1000 necesita cuatro bits para representarse, y por tanto, se han de tomar cuatro bits de la dirección de equipo para indicar la dirección de subred.
Y su mascara de red es: 255.255.240.0 que corresponde a:

Dirección de red		Dirección de subred	Dirección de equipo	
11111111	11111111	1111	0000	00000000

Que indica que hay 20 bit para marcar la dirección de red y 12 bits para la dirección de equipos.(El tercer octeto será 11110000 que corresponde a 240 en decimal).

Otra manera de representar la mascara de subred es indicarla en notación alternativa indicando la dirección IP en decimal de la red (en el ejemplo seria 164.56.0.0/20).
Otro aspecto a considerar es el número de subredes que se pueden tener con la mascara 255.255.240.0

Binario	Decimal
00000000	0
00010000	16
00100000	32
00110000	48
01000000	64
01010000	80
01100000	96
01110000	112
10000000	128
10010000	144
10100000	160
10110000	176
11000000	192
11010000	208
11100000	224
11110000	240

Como se pude observar, hay dieciséis posibles combinaciones que se pueden obtener utilizando los cuatro bits del octeto. Pero no todas las combinaciones son susceptibles de utilización. Así, la combinación con todo ceros (164.56.0.0/20) no se puede utilizar porque es equivalente a la dirección 164.56.0.0/16 y puede ocasionar problemas a los protocolos de encaminamiento y de la misma manera, la combinación con todo unos daría una dirección de difusión(164.56.255.255) equivalente a la dirección de difusión de la dirección 164.56.0.0/16. Por lo que quedarían 14 subredes posibles.

Se puede usar la ecuación 2n-2 (2 elevado a n – 2) para determinar el número de subredes que se pueden obtener (n indica el número de bits que va a utilizar).
De esta manera, se obtienen las subredes que se indican en la tabla siguiente:

N° Bits	N° de subredes
-	
2	
6	
14	
30	
62	
126	
254	

Ahora se deberá considerar si las subredes que se necesitan actualmente(8)y las posibles combinaciones que se pueden obtener con los 4 bits(14) son suficientes para las necesidades futuras o se debe ampliar el número de bits que se pasan a la dirección de subred.

DETERMINAR EL NUMERO DE EQUIPOS DISPONIBLES

Para determinar el número de equipos disponibles en cada segmento de red este está en función de bits que se han dejado para determinar la dirección de equipo(en el ejemplo anterior es 12)

Para ello, se utiliza la misma formula anterior ya que tampoco se puede utilizar las direcciones de equipos con todo ceros o todo unos. De esta manera, se obtiene que con 12bits se puede disponer de 4.094 equipos en cada segmento.

NUMERO DE BITS	1	2	3	4	5	6	7	8
INCREMENTO	128	64	32	16	8	4	2	1
MASCARA SUBRED	128	192	224	240	248	252	254	255
N° DE REDES	0	2	6	14	30	62	126	254

2n – 2 (n = n° de bits de red) = numero de redes posibles
2n – 2 (n = n° de bits de equipo) = numero de equipos posibles

CALCULAR LA RED DE UNA DIRECCIÓN

DIRECCION
MASCARA
---
1 - 1 = 1
1 - 0 = 0
0 - 0 = 0

0.0.0.0 Se usa como origen de una dirección de solicitud de una configuración de arranque. También denota el encaminamiento por defecto de una tabla de encaminamiento.

127.0.0.0 Reservada.

127.0.0.1 Interna. El cliente y el servidor se encuentran en la misma maquina.

127.0.0.2-**127.255.255.255** Reservadas.

191.255.0.0 Reservada.

128.0.0.0 Reservada.

255.255.255.0 Reservada.

240.0.0.0-**255.255.255.254** Reservada.

255.255.255.255 Difusión a todos los nodos locales de la LAN.

El router y cualquiera de los host pueden determina cual es el segmento local, realizando una comparación lógica con la máscara de subred.

Los bits de la subred se toman del campo de host de la dirección. El número de bits de la subred tomados del campo del host viene identificado en la máscara de subred.

Cada bit en la máscara de subred se utiliza para determinar como debe ser interpretado el bit correspondiente en la dirección IP, como se indica a continuación:

1 binario para los bits de red.
1 binario para los bits de subred.
2 binario para los bits de host.

Los bits de la subred provienen de los bits de orden superior del campo de host.

Dado que las mascaras de subred no están definidas por octetos sino por bits, es necesario convertir las direcciones decimal con puntos en valores binarios y de nuevo en decimal con puntos.

El router que utiliza direcciones IP en formato binario, realiza una operación AND lógica para obtener el número de subred.
Un ADN lógico es un operador booleano que permite realizar comparaciones binarias.

AND LÓGICO

AND	0	1
0	0	0
1	0	1

Las direcciones de subred no tienen porque abarcar octetos completos. Un octeto puede ser dividido en una parte de subred y una parte de host.

IDENTIFICACIÓN DE DIRECCIONES IP

Dada una dirección IP y una mascara de subred, se puede utilizar el proceso ilustrado para identificar la dirección de subred, la dirección de difusión, la primera dirección utilizable, y la ultima dirección utilizable.

Paso 1

Escribir la dirección de 32 bits en notación binaria.

Paso 2

Escribir la macara de subred en binario, justamente debajo de la anterior.

Paso 3

Trazar una línea vertical justamente después del ultimo bit 1 de la mascara de subred.

Paso 4

En una fila inferior, colocar todos los bits a 0 para los restantes espacios libres(a la derecha de la línea vertical). Esta es la subred.

Paso 5

En la siguiente fila, colocar a la derecha de la línea todo 1 hasta alcanzar los 32 bits. Esto es la dirección de difusión.

Paso 6

A la derecha de la línea en la fila siguiente, colocar todos los bits a 0 en los espacios libres restantes, hasta llegar al ultimo espacio libre. Colocar un 1 en dicho espacio. Esto dará la primera dirección utilizable.

Paso 7

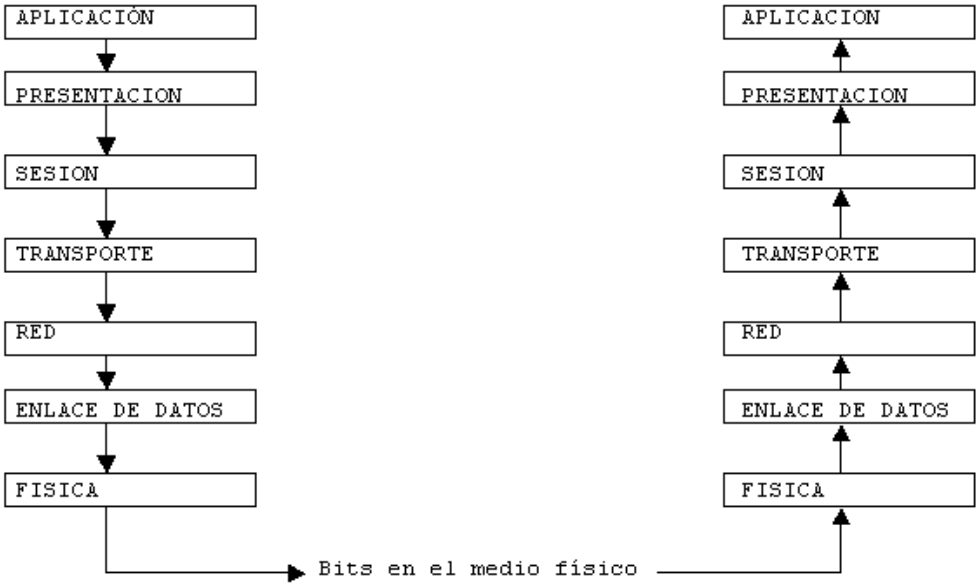
En la fila siguiente, colocar a la derecha, de la línea todos los bits a 1 en los restantes espacios libres hasta llegar al ultimo espacio. Colocar un 0 en dicho espacio libre. Esto dará la ultima dirección utilizable.

Paso 8

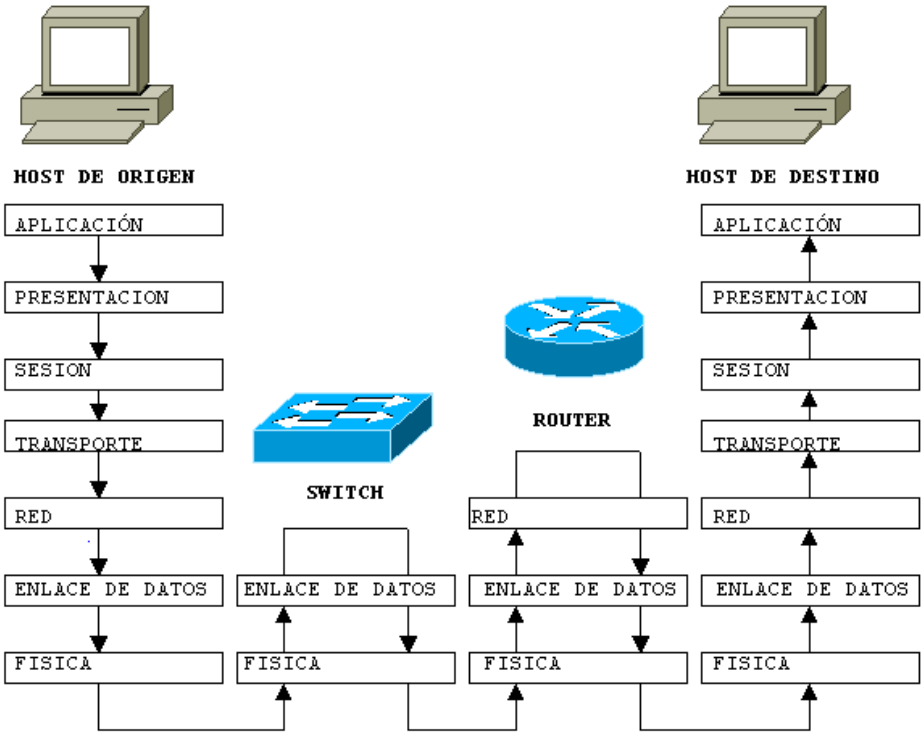
Copiar todos los bits escritos en el paso 1 en los campos que hay a la izquierda de la línea vertical, en cuatro líneas.

Paso 9

Convertir las cuatro filas finales a notación decimal.



Flujo de datos desde una aplicación origen hasta una aplicación destino a través de las 7 capas del modelo de referencia OSI.



Modelo de referencia OSI de representación de datos que viajan desde un host origen, a través de un switch y de un router Cisco, hasta un host de destino.

BRIDGES Y SWITCHES

Los dispositivos Cisco se encuadran en 3 categorías principales: Bridges, switches, routers y servidores de acceso.

Un **bridge** es un dispositivo de red que funciona en la capa de enlace de datos. Los bridges conectan varios segmentos de red de la capa de enlace de datos en un único segmento de red lógico.
Existen diferentes tipos de bridges:

- Transparente o de aprendizaje.
- Encapsulatión
- Conversión
- Origen-ruta.
- Conversión origen-ruta.

Origen-ruta y el bridging de conversión de origen-ruta se utilizan en entornos Token Ring.

El bridging permite la separación física y lógica del trafico cuando resulta necesario reducir las cargas de tráfico en un segmento de red. La principal ventaja de bridging radica en que se garantiza la fiabilidad, disponibilidad, capacidad de ampliación y de gestión de la red al segmentar las redes lógicas en varios componentes físicos.

Los bridges realizan su función examinando la información de la capa de enlace de datos de cada paquete y reenviando el paquete a otros segmentos físicos sólo si es necesario.

El bridge conoce la información sobre que paquetes debe enviar a que segmentos de red y la almacena en una tabla de envío. Esta contiene una lista de direcciones conocidas de la capa de enlace de datos y el segmento de red asociado donde se cree que existen estos dispositivos.

Los bridges se comunican entre si para determinar el mejor método para enviar paquetes a una capa de enlace de datos de destino determina utilizando el Protocolo de Árbol de Extensión(Spanning Tree Protocol, Stp).

Este protocolo permite a los bridges crear topologías sin bucles a través de las que se pueden enviar paquetes. Se necesita una **topología sin bucles** una topología que garantiza que cada paquete llega a todos los segmentos de una red una sola vez, en el entorno de bridging para evitar tormentas de difusión y que varios bridges paralelos envíen un paquete a un segmento determinado varias veces.

Una **tormenta de difusión** es un evento de segmento de red en el que un **paquete de difusión**(es decir un paquete que debe llegar a todas las estaciones del segmento) se envían en un bucle continuo, hasta que el segmento se ve sobrecargado por el tráfico.

El tipo más sencillo de bridge, un **bridge transparente**, puede gestionar exclusivamente la conexión de protocolos de capa de enlace de datos similares.

Los **bridges de encapsulación** y **de conversión** se pueden considerar bridges transparentes, con la funcionalidad adicional de permitir la interoperación de los diferentes protocolos de capa de enlace de datos.

Los bridges de encapsulación encapsulan marcos completos de cada capa de enlace de datos en otra de enlace de datos, lo que permiten el bridging transparente entre las capas de enlace de datos diferente. Dos bridges de encapsulación, cada uno con un puerto Ethernet y con un puerto serie pueden puentear segmentos de red Ethernet cuando se conectan mediante un enlace serie.

Los bridges de conversión realizan la función de bridges transparentes entre tipos de protocolos de capa de enlace de datos diferentes.

Un bridge de conversión puede convertir marcos Ethernet en marcos Token Ring. Si dos dispositivos están en medios diferentes conectados por un bridge de conversión, parecen estar en un segmento de red lógico.
La interconexión transparente de dos medios diferentes puede proporcionar la conectividad necesaria para dos dispositivos que necesiten comunicarse exclusivamente en la capa de enlace de datos.

Un switch Cisco es básicamente u bridge multipuerto que ejecuta IOS.
Los switches que funcionan en una capa de enlace de datos, realizan las mismas funciones básicas que los bridges. La diferencia fundamental entre un bridge y un switch no es técnica, sino de empaquetado.

Los switches pueden tener más puertos que los bridges, así como coste por puerto inferior y disponer de funciones de administración integradas con las que no cuenta el bridge.
Al examinar la funcionalidad de bridges y switches en el contexto del modelo de referencia OSI no difieren.

Muchos switches tienen varios puertos que admiten un único protocolo de capa de enlace de datos, como Ethernet y un menor número de puertos de capa de enlace de datos de alta velocidad que se utilizan para conectarse a medios más rápidos, como ATM o Fast Ethernet.

Si un switch tiene dos o más interfaces diferentes para dos o más protocolos de capa de enlace de datos se le puede considerar un bridge de conversión.

Actualmente, muchos switches tienen interfaces que funcionan a diferentes velocidades, como Ethernet, Fast Ethernet y Gigabit Ethernet.

ROUTER

Dispositivo que direcciona paquetes a través de la red basándose en la información de capa de red.

Los routers conocen las direcciones de la capa de red de un paquete y disponen de algoritmos, que se llaman protocolos de enrutamiento, para crear tablas que permitan determinar la ruta que deben tomar los paquetes para llegar a su destino final.

En un router multiprotocolo(el que conoce varios formatos de direcciones de capa de red y distintos protocolos de enrutamiento), el router mantiene tablas de enrutamiento independientes para cada uno de los protocolos de capa de red que enruta.

Los bridges y switches conectan dos o más redes físicas en una sola red lógica, mientras que los routers conectan dos o más redes lógicas y las rutas entre ellas utilizando la información que crean los protocolos de enrutamiento y que se almacena en las tablas de enrutamiento. Las ventajas de los routers(en comparación con cualquier tipo de bridge) son que dividen física y lógicamente una red en varios componentes que se pueden administrar, permiten el control de paquetes enrutados y enrutan varios protocolos diferentes de capa de red de manera simultánea.

SERVIDORES DE ACCESO

También recibe el nombre de **servidor de comunicaciones**, es un dispositivo que conecta dispositivos asíncronos a una red. Una aplicación común de un servidor de acceso consiste en conectar una computadora a Internet por medio de un módem. El servidor de acceso combina las funciones de un router con las de un protocolo asíncrono. Si una máquina se conecta a un servidor de acceso por medio de una interfaz asíncrona, este proporciona el software que permite a la maquina aparecer en la red. Por ejemplo un servidor de acceso pude tener 16 puertos asíncronos y un solo puerto Ethernet.

Cualquier dispositivo que se conecte a un puerto asíncrono parece estar en Ethernet donde reside el servidor de acceso, lo que permiten que los usuarios ejecuten IP, IPX o Apple Talk para trabajar desde una máquina remota, de la misma manera que si se encontraran en la red local.

PRINCIPIOS BASICOS DE LA CONFIGURACION DE LOS DISPOSITIVOS

Todos los dispositivos Cisco tienen un puerto de consola que se utiliza para acceder al dispositivo desde un terminal conectado directamente a él. El puerto de consola suele ser un puerto RS-232C o RJ-45 con la etiqueta "Console".

Hay que conectar un terminal dedicado o una computadora con un emulador de terminal.

Cisco proporciona los cables necesarios para conectar el puerto de consola a sus dispositivos.
Algunos dispositivos como el router Cisco 7500, requieren la utilización de un conector RS-232C en ambos extremos del cable RJ-45, mientras que otros como los pertenecientes a la serie Cisco 2500 no lo necesitan.

Hay que configurar el terminal para comunicarse con el dispositivo.

- Emulación de VT100.
- 9.600 baudios.
- Sin paridad.
- 8 bits de datos.
- 1 bit de parada.

EL DIALOGO DE CONFIGURACIÓN DEL SISTEMA

Durante el encendido inicial, todos los routers y servidores de acceso entran en el modo de diálogo de configuración del sistema. Este modo interactivo aparece en la pantalla de la consola y realiza preguntas que facilitan la configuración de los elementos básicos de IOS.

El diálogo de configuración del sistema pide información primero sobre los parámetros globales del sistema y después sobre los específicos de la interfaz.

IOS personaliza automáticamente el cuadro de dialogo de configuración del sistema, según la plataforma y las interfaces instaladas en el router.
Las interfaces aparecen como no configuradas, por lo que esta columna muestra el valor **unassigned**.

La columna **Method** se refiere a la configuración de la interfaz, ya sea de manera manual o automáticamente desde la red. Aun no se han configurado las interfaces(**no set**).

Las ultimas dos columnas indican el estado de la interfaz y el protocolo de enlace de datos que se ejecute en la interfaz. Por defecto todas las interfaces comienzan con un estado y un protocolo de capa de enlace de datos **down**.

Cisco etiqueta el dispositivo con los nombres en los puertos físicos en el exterior de la unidad.

IOS acepta la respuesta que aparece entre ([]) como entrada predeterminada a las preguntas.

Los dos niveles de comandos IOS son el privilegiado y el no privilegiado.

Debe configurar una contraseña para cada dispositivo.

Esta contraseña es la clave para acceder al modo privilegiado. Las contraseñas privilegiadas deben mantenerse en secreto. Es muy aconsejable que utilice el modo **enable secret** y no el más obsoleto **enable password**, porque el comando **enable secret** utiliza un algoritmo criptográfico unidireccional.

Un terminal virtual es una conexión de terminal lógico a un dispositivo IOS. Por defecto todos los dispositivos IOS permiten cinco sesiones Telnet de terminal virtual simultaneas (numeradas del 0 al 4. Cuando el dispositivo IOS está activo en una red, puede usar el programa Telnet para acceder a las funciones de IOS desde el terminal virtual de la misma manera que si accediera al dispositivo desde el puerto de consola.

La salida por pantalla generada el ejecutar el comando de diálogo de configuración del sistema es un scrip de comandos de configuración que el dispositivo por si mismo, sino que crea un scrip de comandos de configuración que el dispositivo interpreta y utiliza para su configuración.

SISTEMA DE AYUDA

El sistema de ayuda IOS se puede utiliza en el modo ejecutable para facilitar la asignación a un dispositivo. El sistema de ayuda tiene en cuenta el contexto, lo que significa que la ayuda que reciba depende de lo que se esté intentando hacer con IOS en este momento.

Por ejemplo, si escribe **?** en el indicativo del dispositivo, aparece la información siguiente:

```
Router>?
```

Los comandos IOS aparecen a la izquierda de la pantalla, mientras que a la derecha aparece una breve descripción de los mismos. Algunos comandos se ejecutan con una sola palabra, el sistema de ayuda lo indica mostrando que la opción disponible es introducir un retorno de carro tras el comando, marcado con **<cr>** en la pantalla.

```
Router>lock ?
<cr>
```

También se puede utilizar el sistema de ayuda para buscar las opciones disponibles para completar un comando ejecutable.

IOS dispone de muchos comandos para comprobar el estado de un dispositivo en un momento dado. La mayoría de estos comandos comienzan por **show**.

El sistema de ayuda de IOS también completa los comandos parciales si se pulsa la tecla **Tab**. Si escribe un comando ejecutable que no deja lugar a ambigüedades en su interpretación y seguidamente pulsa la tecla Tab, IOS completa el comando.

Algunos dispositivos IOS tienen varios módulos de Hub, cada uno de ellos con su propia consola de acceso virtual(Modulo de Switch de ruta
RSM y el módulo del modo de transferencia asíncrono ATM, de un switch Catalyst).

MODOS PRIVILEGIADO Y NO PRIVILEGIADO

Desde el modo ejecutable se pueden ejecutar dos niveles básicos de comandos.
No privilegiado, el prompt es el símbolo mayor que(>) tras el nombre del dispositivo.

Router>

En este modo se puede examinar el estado del dispositivo IOS, pero no se pueden cambiar los parámetros.

El segundo nivel comprende los comandos privilegiados y se conoce también como **enable mode**.
Los dispositivos IOS en modo privilegiado, cambian el símbolo > de indicativo, por una almohadilla(#).
El comando ejecutable **enable** pasa del modo no privilegiado al modo privilegiado.
Utilice el comando **disable** para pasar del modo privilegiado al modo no privilegiado.

PROBLEMAS DE CONFIGURACIÓN DE MEMORIA

De las 3 partes de memoria de un dispositivo IOS, dos contienen la configuración del dispositivo. La tercera contiene el sistema operativo IOS.

La diferencia entre los comandos de configuración y el sistema operativo IOS radica en que los primeros se utilizan para configurar el dispositivo, mientras que el sistema operativo IOS es el software que se ejecuta en el dispositivo.

Hay dos tipos de memoria que almacenan los comandos de configuración IOS.

Memoria de acceso aleatorio(RAM, Ramdom-Access Memory) y la memoria de acceso aleatorio no volátil/NVRAM, Nonvolatile Ramdom-Access Memory).

También el sistema operativo IOS puede cargarse en un tercer tipo de memoria, la memoria sólo lectura programable y susceptible de borrado (EEPROM, Electronically Erasable Programmable Read-Only Memory) también conocida como memoria Flash.
Para ejecutar cualquiera de los comandos relativos a la memoria en un dispositivo hay que entrar en modo privilegiado.

MEMORIA DE CONFIGURACIÓN DE DISPOSITIVOS

La configuración actual o de ejecución, de un dispositivo IOS se puede ver con el comando ejecutable **show running-config**. La salida por pantalla de este comando muestra los comandos IOS que esta ejecutando el dispositivo.

La configuración en ejecución de un dispositivo se almacena en la RAM, que se borra al apagar el dispositivo. Debe guardar su configuración actual en la NVRAM, llamada configuración de inicio, si desea que el dispositivo reanude la misma configuración de ejecución tras un ciclo de actividad. Para guardar la configuración de ejecución en la NVRAM se utiliza el comando ejecutable **copy**, que copia desde la primera ubicación de la memoria a la segunda.

Router#copy running-config startup-config

El comando **copy** también puede utilizarse al inversa, copiando desde la primera configuración de inicio a la configuración de ejecución.

Router#copy startup-config running-config

Al copiar desde la configuración de inicio de la NVRAM a la configuración de ejecución de la RAM, tenga en cuenta el potencial problema ocasionado por la fusión de los comandos de configuración IOS.

Router#show startup-config

Ver la configuración de inicio.

La primera línea de la configuración de inicio muestra la cantidad de NVRAM que ocupa la configuración y la cantidad de NVRAM total disponible en el dispositivo.

Router#erase startup-config

Borra la configuración de inicio.

Borra la configuración de inicio y recarga el dispositivo, hace que el dispositivo IOS comience con el cuadro de diálogo de configuración del sistema.

Reload Comando ejecutable privilegiado que recarga el router.

MEMORIA FLASH DE IOS

La memoria Flash es una ubicación en la que el dispositivo Cisco contiene las imágenes binarias ejecutables de IOS que constituyen el sistema operativo del dispositivo.

No confundir la imagen IOS con las configuraciones de IOS. Una configuración de IOS indica al dispositivo su configuración actual, mientras que una imagen de IOS es el programa binario real que analiza y ejecuta la configuración.

Dependiendo de la cantidad de memoria Flash instalada y del tamaño de la imagen IOS que se desee almacenar en ella, el dispositivo puede contener varias imágenes de IOS.

Si tiene varias imágenes de IOS en un determinado dispositivo, puede configurar la que desea que se ejecute. Puede copiar en los dispositivos de IOS las imágenes IOS recibidas de Cisco utilizando distintos protocolos de transferencia de archivos basados en TCP/IP, entre los que se incluye TFTP, FTP y el protocolo de copia remota(Remote Copy Protocol, RCP) de UNIX.

RCP requiere una configuración del dispositivo basado en IOS y un servidor RCP, el uso de RCP representa ciertos riesgos de seguridad.
La decisión de usar TFTP o FTP para transferir la imagen IOS desde un servidor al dispositivo IOS depende de varios factores.

- La disponibilidad de TFTP o FTP.
- El tipo de conexión de red disponible LAN (FTP) WAN (TFTP).
- El nivel de seguridad TFTP no requiere ningún tipo de identificación ni autenticación para realizar la transferencia. FTP requiere un nombre de usuario y una contraseña para realizarla.

USO DE TFTP PARA LA TRANSFERENCIA DE IMAGEN IOS

Para poder transferir una imagen IOS al dispositivo, hay que tener el archivo de dicha imagen en un servidor TFTP. Si ya la tiene, ejecutar el comando **copy tftp flash** para iniciar la transferencia. El router muestra el contenido actual de la memoria Flash y después solicita la dirección IP del servidor TFTP y el nombre de la imagen de IOS antes de confirmar el proceso de copia. En el último paso el dispositivo verifica que el archivo se ha cargado sin errores.

Todos los comandos ejecutables que utiliza la red para realizar una acción devuelven un signo de exclamación(!) cuando funcionan y un (.) cuando no lo hacen.

Si desea copiar la imagen IOS desde la memoria Flash del dispositivo a un servidor TFTP use el comando ejecutable **copy flash tftp**.

Router#show flash

Permite ver el contenido de la memoria Flash.

Algunos dispositivos Cisco IOS ejecutan la imagen de IOS desde la memoria Flash y no pueden sobrescribirla durante su ejecución. Estos dispositivos IOS utilizan el sistema de ayuda de carga de la memoria Flash para copiar las imágenes de IOS desde un servidor TFTP.

USO DE FTP PARA LA TRANSFERENCIA DE IMÁGENES IOS

A diferencia de TFTP, FTP requiere un nombre de usuario y una contraseña para identificar y autentificar el dispositivo IOS y su administrador en el servidor FTP antes de transferir la imagen del software IOS. Se utilizan dos métodos para introducir el nombre de usuario y la contraseña como parte del comando.

- Especificar el nombre de usuario y la contraseña como parte del comando **copy ftp**.
- Predefinir el nombre de usuario y la contraseña por medio de los comandos de configuración global **ip ftp username** e **ip ftp password**.

El primer método es más útil cuando varios usuarios realizan las actualizaciones de la imagen del software. El segundo método resulta útil cuando un solo individuo realiza las actualizaciones cuando se ha configurado una cuenta específica de acceso y contraseña con el único propósito de transferir imágenes de software IOS. En cualquier caso, el nombre de usuario y la contraseña correspondientes deben encontrarse en el servidor FTP antes de iniciar el proceso de transferencia.

Hay que tener el archivo de la imagen IOS en un servidor FTP, utilizar el comando ejecutable privilegiado **copy** ftp://username:password **falsh** para especificar el nombre de usuario y la contraseña para la autenticación e iniciar la transferencia.

El router muestra el contenido actual de la memoria flash y a continuación le pide la dirección IP del servidor FTP y el nombre de la imagen IOS antes de confirmar el proceso de copia. Opcionalmente se pueden especificar la dirección IP del servidor FTP y el nombre de la imagen IOS como parte del comando **copy** (**copy ftp flash**).

ftp://username:password@ftpservername/ios-image-name

En el ultimo paso del proceso, el dispositivo verifica que el archivo se ha cargado sin errores.

Para copiar la imagen IOS desde la memoria Flash del dispositivo a un servidor FTP utilizar el comando ejecutable **copy flash ftp**. Hay que especificar el nombre de usuario y la contraseña necesario, ya sea como parte del comando copy o predefiniéndolos en la configuración de ejecución.

Es aconsejable guardar una copia de todas las imágenes de IOS en un servidor y hacer copias de seguridad de los archivos con cierta frecuencia.

GESTIÓN DEL ESPACIO DE MEMORIA FLASH

Todos los comandos que transfieren imágenes de software IOS a la memoria Flash calcularán el espacio disponible, y si fuera necesario, pedirán que borre y comprima el contenido existente en la memoria flash para liberar espacio.

En determinadas ocasiones es posible que desee borrar el contenido de la memoria flash total o parcialmente independientemente del proceso de transferencia. Puede borrar el contenido completo de la memoria Flash con el comando ejecutable privilegiado **erase flash**. Para borrar una imagen de IOS determinada de la memoria Flash, utilice el comando **delete**.

En los dispositivos Cisco que tienen una tarjeta de memoria Flash externa(normalmente ubicados en la ranura **slot0**), el comando **delete** sólo marca la imagen IOS para su eliminación; pero no realiza su borrado ni libera espacio en la memoria Flash. Debe ejecutar el comando **squeeze** para completar el proceso de borrado del archivo.

MODO DE CONFIGURACION DE USUARIO

Para configurar un dispositivo IOS hay que utilizar el comando ejecutable privilegiado **configure**. Este dispone de tres opciones:

Configuración desde el terminal
Configuración desde la memoria
Configuración desde la red

Ctrl+P(anterior) y Ctrl+N(siguiente) para desplazarse por la lista de comandos.

La opción predeterminada, que es la primera, permite configurar el dispositivo IOS desde el terminal en tiempo real. IOS ejecuta los comandos inmediatamente después de que los escriba.

A continuación, el dispositivo cambia el indicativo para mostrar que esta en modo de configuración y que permite introducir comandos de configuración.

Cuando finalice de introducir comandos de configuración, pulse Ctrl+Z.

Router(config)#hostname[nombre]
Router(config)#Ctrl+Z
Router#

Hostname Comando de configuración global que permite nombrar el dispositivo.

La segunda opción, la configuración desde la memoria, permite copiar el contenido de la configuración de inicio del dispositivo, que se encuentra almacenado en la memoria NVRAM, en la configuración actual. Esta opción resulta útil si se ha modificado un parámetro de configuración en tiempo real y desea volver a la configuración previa, guardada en la configuración de inicio. Este comando **configure** realiza la misma función que el comando **copy startup-config running-config**.

La tercera opción, la configuración desde la red, permite cargar un archivo de configuración desde el servidor que ejecuta el protocolo TFTP.

Cuando se configura un dispositivo IOS desde un servidor TFTP, de forma predeterminada éste intenta cargar un archivo con el nombre del dispositivo seguido de la cadena -confg.

Es posible que un dispositivo no pueda cargar un archivo de configuración debido a problemas con la conexión de red IP o a una violación de TFTP.

COMANDOS DE CONFIGURACIÓN

Los comandos de configuración se utilizan para configurar dispositivos IOS.
Los comandos de configuración se pueden introducir desde el terminal, cargarse desde la configuración de inicio o descargarse por medio de un archivo a través de TFTP y el comando ejecutable **configure**.

Todos los comandos IOS pertenecen a una de las tres categorías siguientes:

- Comandos globales.
- Comandos principales.
- Subcomandos

Un comando global es un comando de configuración que afecta a la configuración global de IOS.
Ip ruting comando de configuración global que activa el enrutamiento IP.
Un comando principal es aquel que permite la utilización de subcomandos para configurar el dispositivo. Un comando principal no configura el dispositivo IOS por sí sólo, se necesitan subcomandos para completar la configuración.

Un comando principal requiere el contexto de un subcomando para configurar el dispositivo.

La combinación de un comando principal y un subcomando es la combinación correcta para configurar un dispositivo IOS.

El sistema de ayuda de IOS esta disponible durante la configuración de los dispositivos.

Utilice el comando (?) para ver las opciones de configuración disponibles.

ELIMINACION DE LOS COMANDOS DE CONFIGURACIÓN

Los comandos de configuración predeterminados de un dispositivo IOS, agregue la palabra clave **no** al principio del mismo, siga el mismo procedimiento para eliminar cualquier comando global, comando principal o subcomando.

COMANDOS DE CONFIGURACIÓN PREDETERMINADOS

Los comandos de configuración predeterminados de Cisco IOS no aparecen en show running-config o show startup-config. Si introduce un comando que es un comando de configuración predeterminado, el dispositivo acepta el comando sin excepciones. Por ejemplo:. Todas las interfaces series de los routers Cisco tienen predeterminada la encapsulación HDLC. Si escribe el subcomando de configuración de interfaz **encapsulation hdlc** para una interfaz serie, no añadirá una línea nueva de configuración en el router.

Todos los comandos IOS tienen una configuración predeterminada.

El comando de configuración **default** como acción previa a cualquier comando global, comando principal o subcomando devuelve el valor de configuración a su configuración predeterminada. Muchos comandos de configuración IOS aparecen desactivados por defecto, de manera que su forma predeterminada es la misma que la forma **no**.

FUSIÓN Y SUSTITUCIÓN DE LOS COMANDOS DE CONFIGURACIÓN

Un nuevo comando de configuración puede sustituir un comando existente, lo que en el caso de IOS supone la eliminación automática de este último.

Por otra parte es posible fusionar un comando nuevo con otro existente en vez de sustituirlo.

Documentación de Cisco:
www.cisco.com/univercd/cc/td/doc/product/index.htm

PRINCIPIOS BASICOS DE LAS INTERFACES DE LOS DISPOSITIVOS

Una interfaz, es una conexión entre un dispositivo CISCO y un medio de la red.

Todas las interfaces tienen tecnologías subyacentes que se usan para transferir datos a través de un medio físico, como el cobre o la fibra.

Los protocolos que se encuentran en la capa física del modelo de referencia OSI definen las características físicas de la interfaz y del medio.

Los protocolos que funcionan en la capa de enlace de datos(capa 2)del modelo de referencia OSI, implementan la tecnología para trasladar datos entre la capa de red y la capa física.

Cada una de las interfaces de un dispositivo CISCO recibe el nombre de puerto. Los dispositivos CISCO etiquetan los puertos de diferentes formas.
En los dispositivos CISCO de configuración fija, las interfaces se numeran de forma secuencial sin nombrar la ranura.(Ejemplo Serie 2500)

Si el dispositivo es modular y tiene tarjetas de interfaz intercambiables, los interfaces se numeran utilizando el tipo de sintaxis ranura/puerto.

Algunos routers, tienen tarjetas procesador de interfaz versátil(versatile interface processor, VIP).Cada una de estas tarjetas cuenta con una o dos ranuras para loa adaptadores de puertos.

Un adaptador de puerto es un circuito electrónico con interfaces que se inserta en un procesador de interfaz versátil. Cada adaptador de puerto, puede tener varias interfaces.

En este tipo de puertos,(en la actualidad solamente los routers de la serie 7000, 7500 y 12000)se usa una sintaxis tipo de ranura/adaptador de puerto/puerto para especificar la interfaz.

El comando ejecutable show interfaces permite ver el estado de todas las interfaces de los dispositivos CISCO.

La primera línea muestra el tipo de medio de la interfaz y el número de la misma. Una interfaz que aparece en estado up(activa)funciona con normalidad desde le punto de vista eléctrico y recibe la señal adecuada de los cables que tiene conectados. Otros estados posibles para la interfaz son down(inactiva) y administratively down(administrativamente inactiva). Una interfaz inactiva esta operativa, pero no se comunica correctamente con el medio al que esta conectada. Una interfaz administrativamente inactiva esta configurada para estar apagada y no esta operativa.

En la segunda línea aparece el tipo de Hardware físico de la interfaz, al igual que la dirección de la capa de enlace de datos de la interfaz. La encapsulación de las interfaces de las redes de área local no suelen necesitar configuración, mientras que las redes de área amplia si que la necesitan.

La razón de la diferencia es que las interfaces LAN suelen ejecutar un único protocolo de capa de enlace de datos, mientras que las interfaces WAN pueden ejecutar muchos protocolos de capa de enlace de datos diferentes.

EL COMANDO ENCAPSULATION

La encapsulación de una interfaz define el formato de datos enviados y el protocolo de enlace de datos de la interfaz. La encapsulación de una interfaz, se define con el subcomando de configuración de interfaz **encapsulation**.

EL COMANDO SHUTDOWN

Si se desea cambiar el estado administrativo de una interfaz de activa a inactiva o viceversa, hay que usar el comando de configuración **shutdown** o **no shutdown**.

EL COMANDO DESCRIPTION

El subcomando de interfaz **description** se puede usar para añadir una descripción de texto que aparece en la salida del comando **show interfaces**.

Esta descripción puede tener hasta 255 caracteres.

Es aconsejable agregar una descripción a cada una de las interfaces para documentar su utilización.

TECNOLOGIAS DE REDES DE AREA LOCAL

Los dispositivos CISCO admiten varias tecnologías LAN.

- Ethernet e IEEE 802.3.
- Fast Ethernet.
- Gigabit Ethernet.
- Token Ring.
- Interfaz de datos distribuidos por fibra.

Todos estos protocolos operan en la capa de enlace de datos del modelo de referencia OSI y se usan en un entorno LAN para transportar datos punto a punto a velocidades entre 4Mb y 1Gb.

Todos estos protocolos LAN comparten el mismo esquema de direcciones de capa de enlace de datos. Las direcciones son hexadecimales de 6 bytes, que son únicas en le mundo. Estas direcciones, reciben el nombre de direcciones de control de acceso al medio(Media Access Control, MAC). Dicha dirección se graba en la memoria de solo lectura(Read-Only Memory, ROM) de la propia tarjeta de la interfaz. Para asegurarse de que cada interfaz tiene una dirección única, a cada fabricante se le asigna un prefijo de 20 bits de la dirección de 6 bytes.

A CISCO se le ha asignado un prefijo de 20 bits de 0060.5(en formato hexadecimal, en el que cada dígito representa 4 bits). Posteriormente el fabricante puede asignar los 28 bits restantes de cualquier forma, siempre que la dirección sea única.

Técnicamente es posible que IOS use en una interfaz de LAN determinada una dirección de enlace de datos diferente a la vía(burned-in-address) que se encuentra en la ROM. La práctica de cambiar la vía de una interfaz de LAN es poco frecuente, pero resulta útil en algunas configuraciones de redes complejas.

ETHERNET E IEEE 802.3

Ethernet y el protocolo del Instituto de Ingeniería Eléctrica y Electrónica(Institute of Electrical and Electronics Engineers, IEEE) 802.3 son los protocolos de LAN que más se usan en la actualidad.

Ethernet lo desarrollaron a mediados de los años 70 varios investigadores del Centro de Investigación de Palo Alto(Palo Alto Research Center, PARC) de XEROS. XEROS, Digital Equipament Corporation e Intel Corporation lo estandarizaron en 1978. Mas tarde el IEEE estandarizó un protocolo similar llamado IEEE 802.3. Los usos de los campos de las tramas varían ligeramente entre Ethernet y IEEE 802.3.

Muchos de los protocolos IEEE empiezan con el esquema de numeración 802, lo que indica el año y el mes en que se formó el comité original.

Tanto Ethernet como 802.3 IEEE usan una tecnología de red denominada acceso múltiple con detección de portadora y detección de colisiones(carrier sense múltiple access colisión detect, CSMD/CD) para permitir el acceso a un bus de 10Mb común en le que se comunican todos los dispositivos. Varios de los dispositivos de un bus CSMD/CD pueden detectar cuando hay tráfico en le bus común(la detección de portadora) y cuando hablan a la vez dos nodos(la detección de la colisión).

El protocolo CSMD/CD también especifica cómo funciona un dispositivo en caso de colisión.
Los dispositivos Ethernet e IEEE 802.3 pueden comunicarse en modo semiduplex, un modo en el que el dispositivo puede enviar o recibir una trama, peor ambas cosas a la vez. Los segmentos comunes de Ethernet e IEEE 802.3 funcionan en modo semiduplex. Ethernet e IEEE 802.3 funcionan en modo duplex completo cuando un dispositivo puede enviar y recibir una trama al mismo tiempo. Este modo solamente se encuentra disponible en una topología en la que están conectados directamente dos dispositivos usando Ethernet o IEEE 802.3, como por ejemplo, un dispositivo conectado a un Switch Ethernet.

Los routes CISCO se pueden usar para separar segmentos Ethernet tanto lógica como físicamente.

FAST ETHERNET

Es un protocolo CSMA/CD que funciona a 100Mb, lo que supone 10 veces más velocidad que Ethernet o IEEE 802.3, el protocolo usa el mismo medio físico(cobre, par trenzado y fibra). Fast Ethernet puede funcionar en semiduplex o en duplex completo. La mayoría de los dispositivos Fast Ethernet, pueden detectar automáticamente si el segmento al que están conectados es Ethernet(10Mb) o Fast Ethernet(100Mb) y también pueden detectar el duplex apropiado(semiduplex o duplex completo).

Fast Ethernet se suele utilizar en los switches como enlace ascendente para las interfaces Ethernet.

SUBCOMANDOS DE CONFIGURACION DE LAS INTERFACES FAST ETHERNET Y ETHERNET

En algunos routers CISCO de las series 4000 y 7000,cada interfaz Ethernet y Fast Ethernet puede elegir entre varios tipos de medios para conectarse con el router.

El subcomando de configuración de interfaz **media-type** para indicar al router que tipo de conexión se encuentra activa en la interfaz.

Las interfaces de unidad de conexión(Attachment Unit Interfaces, AUI) y los conectores RJ-45(a las que IOS denomina 10BaseT para indicar cable de par trenzado) son los tipos de medios válidos para las interfaces Ethernet e IEEE 802.3.
Los AUI son conectores de 15 pins. Las interfaces independientes de los medios(Media-Independent Interfaces, MII) y los conectores RJ-45 son los tipos de medios válidos para las interfaces Fast Ethernet.
En las interfaces Fast Ethernet, se puede definir el duplex de forma manual mediante el subcomando de configuración de interfaces **full-duplex**. Si se elimina este comando con el comando **no full-duplex**, la interfaz vuelve a su modo de semiduplex predeterminado.

GIGABIT ETHERNET

Gigabit Ethernet(o IEEE 802.3z) se basa en el estándar IEEE 802.3.

Gigabit Ethernet se comunica con los dispositivos a 1Gbps.

Desde la capa de enlace de datos y mas arriba en la pila de protocolos OSI, Gigabit Ethernet funciona exactamente igual que Ethernet. En la capa física, Gigabit Ethernet utiliza un tipo de interfaz que también se usa en otra tecnología LAN de alta velocidad, llamada **Fiber Chanel**.

Gigabit Ethernet combina la capa física de Fiber Chanel y el formato de trama de la capa de enlace d datos que utiliza IEEE 802.3, Ethernet y Fast Ethernet.

Gigabit Ethernet utiliza el algoritmo CSMA/CD y puede funcionar en modo semiduplex o duplex completo.
Los routers de la serie 7500 de CISCO y los Switches de la serie Catalyst 5500 admiten interfaces Gigabit Ethernet. En la actualidad, los routers de la serie 7500 admiten una única interfaz Gigabit Ethernet por ranura.

TOKEN RING

Token ring es una tecnología LAN desarrollada por IBM(International Business Machines) y estandariza como el protocolo IEEE 802.5. Opera en una topología lógica por anillos. Usa un protocolo llamado Token Capture para conceder acceso al medio físico de la red, implementado a dos velocidades 4 Mbps y 16 Mbps.

Un dispositivo de un Token Ring debe capturar un paquete especial llamado Token.

Un Token atraviesa el anillo en una dirección lógica contraria a las agujas del reloj.
Si un dispositivo a capturado el token puede transmitir una trama por el anillo.

En las redes Token Ring de 16 Mbps, el sistema fuente envía un Token nuevo antes de recibir la trama de datos, usando una característica que se llama **early token release(envío temprano del token)**.

A diferencia de CAMA/CD, el protocolo token capture evita totalmente las colisiones, ya que únicamente el dispositivo que ha capturado el token puede transmitir una trama en Token Ring. Además, es posible calcular el tiempo máximo que debe esperar un dispositivo antes de poder transmitir una trama, con lo que se hace que el protocolo token capture sea determinista.

SUBCOMANDOS DE CONFIGURACIÓN DE LA INTERFAZ DE TOKEN RING

El subcomando de configuración de interfaz de IOS **ring-speed** se usa para especificar si la interfaz de Token Ring es de 4 o de 16 Mbps; todos los dispositivos de un Token Ring deben funcionar a la misma velocidad; las configuraciones mixtas de velocidades de anillo no están permitidas por el protocolo y pueden hacer que el anillo quede inoperativo.

Si decide utilizar la característica **early token release** en un anillo de 16Mbps, todos los dispositivos del Token Ring deben tener activada esta característica.

El subcomando de configuración de interfaz de IOS **early-token-release** activa early token release en una interfaz.

```
Router(config)#ring-speed[4 o 16]
Router(config)#early-token-release
Router(config)#Ctrl+Z
```

INTERFAZ DE DATOS DITRIBUIDOS POR FIBRA

La interfaz de datos distribuidos por fibra(Fiber Distributed Data Interface FDDI) es otro protocolo de LAN de captura de token.

El comité de estándares ANSI X3T9.5 estandarizó el protocolo FDDI a mediados de los ochenta.

FDDI un anillo de fibra dual que transmite datos en direcciones opuestas. Durante el funcionamiento normal, FDDI usa sólo un anillo, denominado anillo primario.
Sólo usa el segundo anillo, denominado anillo de respaldo, cuando se produce un fallo en el anillo primario. Cuando hay una única rotura en el anillo primario, los dispositivos más cercanos a la rotura entran en modo de ajuste y usan el anillo de respaldo para formar un bucle que asegure que el anillo FDDI siga completo.

FDDI funciona a 100Mbits por segundo. Debido a este ancho de banda y su redundancia inherente, suele usarse como enlace ascendente de alta velocidad desde un switch a un backbone de un router o como tecnología de backbone de Campus.
Los bridges, switches y routers Cisco admiten FDDI para el bridging, switching y enrutamiento transparente y de conversión de los protocolos de capa de red.
Las propiedades físicas de cada fibra (PHY-A es el anillo primario y PHY-B es el anillo de respaldo).

TECNOLOGÍAS DE REDES DE AREA AMPLIA Y REDES DE ACCESO TELEFONICO

Los dispositivos Cisco admiten un gran número de tecnologías WAN y de acceso telefónico.

- HDLC
- PPP
- X-25
- FRAME RELAY
- ATM
- DSL
- RDSI

Estos protocolos de WAN trasladan los datos de una ubicación a otra a través de una interfaz serie asíncrona o síncrona.

Las transmisiones series síncronas son señales digitales que se transmiten con una temporización precisa de un dispositivo a otro. Por su parte, la transmisión asíncrona no se realiza con temporización precisa y confía el la información de control(denominado bits de inicio y finalización)que indican el inicio y la finalización de los datos.

HDLC, síncrono, sólo funciona punto a punto conectando un dispositivo con otro con una encapsulación y direccionamiento mínimos.

PPP, diseñado originalmente para enlaces serie punto a punto, ha evolucionado para trabajar en entornos tanto síncronos como asíncronos. Los protocolos X-25, Frame Relay y ATM no funcionan en un entorno estricto de enlaces serie punto a punto, si no que utilizan circuitos virtuales para trasladar los datos.

DSL es una tecnología que proporciona codificación a las conexiones serie de lata velocidad a través de cable de cobre convencional para distancias limitadas.

RDSI, es una tecnología WAN que utiliza la red telefónica para digitalizar los datos. Puede funcionar en un entorno punto a punto o multipunto.

Un **circuito virtual**(virtual circuit, VT) es un mecanismo de comunicación en el que se establece una ruta para el traslado de información antes de que se envíen los datos, proceso conocido como colocar una llamada. Todos los paquetes de datos relacionados con la llamada siguen la misma ruta a través de la red, con lo que no aseguramos que los datos llegan al destino en el mismo orden en el que se enviaron. Al terminar la transferencia de datos, se finaliza la llamada.

Los **circuitos virtuales conmutados**(switched virtual circuits, SVC) son los que se pueden establecer y suprimir según los requiera la red.

Los **circuitos virtuales permanentes**(permanent virtual circuit, PVC) los establece la red de forma permanente y nunca se suprimen. Los circuitos virtuales múltiples(SVC y PVC) pueden residir en una sólo interfaz serie de un router Cisco. En este caso, cada uno de los circuitos virtuales puede tratarse como una interfaz separada, denominada **subinterfaz**. Las subinterfaces pueden implementarse para cualquier protocolo de WAN que utilice circuitos virtuales.

El sistema de teléfono es un sistema análogo a un VC. Cada llamada de teléfono que hacemos puede considerarse como un circuito virtual. Casi todas las llamadas telefónicas que hacemos son análogas a los SVC. Si realizamos una llamada de teléfono una vez y no colgamos nunca, seria un PVC.

Los protocolos WAN de Cisco que usan circuitos virtuales trasladan los datos de dos formas diferentes. El **switching de paquetes** es un método de transmisión de datos que envía en unidades de longitud variable, también llamadas paquetes.

El switching de paquetes en la capa de enlace de datos traslada los paquetes desde la capa de red y los encapsula con un direccionamiento de capa de enlace de datos específico.

A medida que los paquetes de enlace de datos, atraviesan la red, cada nodo intermedio de switching de paquetes situado entre el origen y el destino, lee la dirección de enlace de datos del paquete y lo reenvía. El paquete recorre la ruta del circuito virtual establecida previamente hasta que se alcanza la dirección de enlace de datos de destino.

ATM y el servicio de datos multimegabit conmutados, SMDS convierte los datos de los paquetes en celdas de longitud fija y realizan Relay de celda.

El **Relay de celda** es un método de transmisión de datos que envía datos en pequeñas unidades de tamaño fijo, también llamadas celdas, que pueden procesar el hardware de una manera eficaz. El funcionamiento del Relay de celda es similar al switching de paquetes, sólo que los datos del sistema de origen se convierten primero en celdas de longitud fija en vez de en paquetes.

Es importante tener en cuenta las dos capas de direccionamiento a considerar cuando el switching de paquetes o Relay de celdas traslada datos al nivel de redes a través de la red.

El switching de paquetes y las direcciones de switching de las celdas se encuentran en la capa de enlace datos del modelo de referencia OSI.

Protocolo	**Punto a punto**	**switching paq.**	**Relay**	**Asíncrono**	**Síncrono**
HDLC	SI	NO	NO	NO	SI
PPP	SI	NO	NO	SI	SI
X.25	SI	SI	NO	NO	SI
FRAME RELAY	SI	SI	NO	NO	SI
ATM	SI	NO	SI	NO	SI
DSL	SI	NO	NO	NO	SI
RDSI	SI	NO	NO	SI	SI

Es frecuente que los router Cisco enruten paquetes de la capa de red, como paquetes IP, a través de una red de switching de paquetes como Frame Relay.

A continuación el router encapsula todo el paquete IP en Frame Relay, añadiendo direccionamiento Frame Relay. El paquete se conmuta a través de los switches de la red Frame Relay para hacer que el paquete siga avanzando por el circuito desde el router de origen al de destino. Los router se ven conectados directamente a través de la red Frame Relay; no ven los switches Frame Relay como nodos intermediarios para el trafico de la capa de red.

HIGH-LEVEL DATA LINK CONTROL

El protocolo HDLC es un protocolo síncrono ordenado por bits y desarrollado por la ISO (Organización Internacional para la Normalización). HDLC se utiliza para conectar un router Cisco con otro. Los routers Cisco utilizan la encapsulación HDLC de forma predeterminada en todos los interfaces serie síncronos.

Cisco HDLC es una versión patentada del protocolo, no se comunica a través de un enlace serie con ningún protocolo HDLC de otro fabricante. La naturaleza patentada de Cisco HDLC no es inusual. Las implementaciones HDLC de todos los fabricantes están patentadas, ya que HDLC es un protocolo derivado del protocolo patentado Control de enlace de datos síncrono(Sincronous Data Link Control, SDLC), que fue desarrollado originalmente por IBM.

PROTOCOLO PUNTO A PUNTO

Es un protocolo WAN de enlace de datos. PPP se diseño como un protocolo abierto para trabajar con varios protocolos de capa de red, como IP, IPX y Apple Talk.

Se puede considerar a PPP la versión no patentada de HDLC, aunque el protocolo subyacente es considerablemente diferente. PPP funciona tanto con encapsulación síncrona como asíncrona porque el protocolo usa un identificador para denotar el inicio o el final de una trama. Dicho indicador se utiliza en las encapsulaciones asíncronas para señalar el inicio o el final de una trama y se usa como una encapsulación síncrona orientada a bit.

PPP se basa en el protocolo de control de enlaces (Link Control Protocol, LCP), que establece, configura y pone a prueba las conexiones de enlace de datos que utiliza PPP. El protocolo de control de red (Network Control Protocol, NCP) es un conjunto de protocolos(uno por cada capa de red compatible con PPP) que establece y configura diferentes capas de red para que funcionen a través de PPP. Para IP, IPX y Apple Talk, las designaciones NCP son IPCP, IPXCP y ATALKCP, respectivamente.

SUBCOMANDOS DE CONFIGURACIÓN DE LA INTERFAZ DE PPP

Subcomandos de configuración de interfaz de IOS **encapsulation ppp** activa PPP síncrono en una interfaz serie.

Router(config)#encapsulation ppp

X-25

Es un protocolo de switching de paquetes que admite tanto SVC como PVC y que fue desarrollado por primera vez en los años setenta.

La ITU es la agencia administra el protocolo X-25.
X-25 fundamentalmente define una red para las comunicaciones de datos similar a la red telefónica y traslada los datos mediante circuitos virtuales. La comunicación entre dos dispositivos comienzan con la llamada de un dispositivo a otro a fin de establecer un SVC o PVC, sigue con la transferencia de los datos y posteriormente acaba con la finalización de la llamada.

El protocolo X-25 define una comunicación punto a punto entre el equipo terminal de datos (Data Terminal Equipment, DTE) y equipo de terminación de circuito de datos (Data Circuit-Terminating Equipment, DCE). Los DTE (como los routers de Cisco) se conectan con los DCE (como los módems), que se conectan a su vez con uno o más switches WAN X-25 y en último termino con otro DTE.

DCE es un dispositivo que compone el extremo de la red la interfaz de usuario a red. DCE proporciona una conexión física a la red, reenvía el tráfico y ofrece una señal de reloj que se usa para sincronizar la transmisión de datos entre los dispositivos DCE y DTE. DTE es un dispositivo en el extremo del usuario de una interfaz de red a usuario que sirve como origen de los datos, destino o como ambos. DTE se conecta con una red de datos a través de un dispositivo DCE (por ejemplo un módem) y suele usar las señales de reloj que genera el DCE.

Una llamada a través de una red X-25 se inicia cuando el DTE de origen realiza una llamada al DCE al que se esta conectado. Los switches X-25 de la red deciden cómo enrutar la llamada del origen al destino. Todos los datos se conmutan entonces desde el DTE de origen al destino. Todos los datos se conmutan entonces desde el DTE de origen al destino DTE a través de la red X-25.

El protocolo X-25 utiliza un esquema de direcciones denominadas X.121.

La recomendación ITU-T X.121 especifica los formatos de la dirección de origen y de destino para el protocolo X-25 de la capa de enlace de datos.

Los switches X-25 enrutan las llamadas por la ruta de un circuito virtual basándose en las direcciones X.121 de origen y destino.

Las direcciones X.121 varían en su longitud y pueden tener hasta 14 dígitos decimales, los primeros 4 dígitos de la dirección X.121 se denominan código de identificación de red de datos (Data Network Identificatión Code, DNIC).

Tras el DNIC, el resto de los dígitos de la dirección se pueden utilizar como decida el administrador de la red.

SUBCOMADOS DE CONFIGURACIÓN DE LA INTERFAZ DE X-25

router(config-if)#encapsulation ppp

Las direcciones X.121 del enlace de datos X.25 no se graban en la RAM como las direcciones LAN. Esto significa que hay que comunicarle a un router la dirección local X.121 de una interfaz serie X.25, lo que se realiza con el subcomando de configuración de interfaz **x25 address**. Con los switches X.25 de algunos fabricantes es necesario establecer un tamaño máximo para los paquetes de entrada y de salida (el valor predeterminado es 128 bytes). Es posible que también haya que configurar el router Cisco con el tamaño de paquetes de entrada (ips, input packet size) y el tamaño de paquetes de salida (ops, output paket sice) adecuados en la interfaz serie con los comandos **x25 ips** y **x25 ops** a fin de funcionar correctamente en la red X-25. Las redes X-25 tienen un tamaño de ventana de entrada y salida predeterminado para los paquetes que usan los mecanismos de control de flujo. Es posible que sea necesario configurar el tamaño predeterminado de las ventanas de entrada (win) y de salida (wout) para que la red X-25 funcione correctamente, al igual que también haga falta definir un tamaño máximo de los paquetes (el tamaño predeterminado de las ventanas de entrada y salida es de dos paquetes). Los subcomandos de configuración de interfaz de IOS **x25win** y **x25wont** define el tamaño de las ventanas de entrada y salida. Suele ser necesaria la condición de estos parámetros entre el DTE y el DCE para posibilitar que la capa de enlace de datos de X-25 funcione correctamente.

```
router(config)#encapsulation x25
router(config)#x25 addess[dirección]
router(config)#x25 ips[tamaño]
router(config)#x25 ops[tamaño]
router(config)#x25 win[tamaño]
router(config)#x25 wont[tamaño]
router(config)#Ctrl+Z
```

LAPB (Link Access Procedure Balanced) es el protocolo de capa de enlace de datos que utiliza la pila de protocolo X-25 y que esta basado en HDLC. Si se desea ver el estado de los circuitos virtuales X-25 de un dispositivo Cisco, se puede utilizar el comando ejecutable **show x25 vc.**

FRAME RELAY

Frame Relay es un protocolo de switching de paquetes de WAN que se desarrollo únicamente para su uso a través de RDSI.
Las propuestas iniciales para Frame Relay se presentaron en el comité CCITT en 1984.

Frame Relay es un protocolo de switching de paquetes que tienen PVC y SVC. La mayoría de las redes Frame Relay actuales usan PVC, SVC se esta implementando.

Frame Relay utiliza la configuración de llamadas, la transferencia de datos y el proceso de determinación de llamadas, como ya abordamos anteriormente con X-25.

Una vez establecida la llamada, el router traslada los datos y luego da por finalizada la llamada.

Frame Relay usa direcciones llamadas identificadores de conexión de enlace de datos (Data-Link Connectión Identifiers, DLCI). Cada DLCI puede tener importancia local o global a través de la red Frame Relay.

Lo más habitual es que cada DLCI tenga sólo importancia local, para un router, el número DLCI de cada lado de un circuito virtual puede ser el mismo, ya que Frame Relay asigna un número DLCI local a un circuito virtual en cada switch de la LAN.

En 1990, Cisco, Digital Equipment Corporatión, Northern Telecom y StrataCom formaron un consorcio, tomaron el protocolo Frame Relay básico de CCITT y añadierón extensiones a las características del protocolo, que permiten que los dispositivos de interconexión de redes se comuniquen fácilmente con una red Frame Relay.

Estas características, que se denominen Interfaz de gestión local (Local Management Interface, LNI) permiten que los dispositivos DTE de Frame Relay, como los router se comuniquen con dispositivos DCE de Frame Relay e intercambien la información que se utiliza para pasar el tráfico de interconexión de red a través de una WAN de Frame Relay.

Los mensajes LMI ofrecen información sobre los valores DLCI actuales, la importancia global o local de los valores DLCI y el estado de los circuitos virtuales.

Al consorcio LMI, se les conoce ahora como la banda de los cuatro LMI.

Además del consorcio LMI es estándar (ANSI) ha desarrollado un estándar LMI denominado Annex-D que se utiliza a nivel mundial en las redes Frame Relay.

SUBCOMANDOS DE CONFIGURACIÓN DE LA INTERFAZ DE FRAME RELAY

Subcomando de configuración de interfaz **encapsulation frame-relay**.

Posteriormente se puede utilizar el subcomando **frame-relay interface-dlci** para establecer el DLCI de la interfaz. Los dispositivos Cisco usan de forma predeterminada el LMI de Cisco en las interfaces Frame Relay. Es posible establecer el tipo de LMI utilizando el subcomando de interface **frame-relay lmi-type**.

```
Router(config)#encapsulation frame
Router(config)#frame-relay interface-dlci[numero]
Router(config)#frame-relay lmi-type[tipo]
Router(config)#Ctrl+Z
```

También se pueden contar con varios circuitos virtuales en una sola interfaz serie y tratar a cada uno de ellos como una interfaz separada, que se llama subinterfaz, como una interfaz de utilizar subinterfaces es que se pueden asignar características de capa de red diferentes a cada subinterfaz y circuito virtual, como el enrutamiento IP en un circuito virtual y el enrutamiento Apple Talk en otro. Es posible definir interfaces virtuales con el comando **interface serial slot/port.number**

El parámetro number especifica el número de interfaz asociado con el slot/port (ranura/puerto).

Los dos tipos de subinterfaces son **punto a punto** y **multipunto**. Las interfaces punto a punto se utilizan cuando un solo circuito virtual conecta un router con otro.

Una subinterfaz punto a punto es como un circuito virtual que emula un enlace serie dedicado.

Les sugerimos que siga un esquema de numeración para los números de las interfaces que elija.

Le recomendamos que haga coincidir el número de la subinterfaz con el número DLCI del circuito virtual.

El estado de los circuito virtuales de Frame Relay se puede examinar utilizando el comando ejecutable **show frame pvc** o **show frame svc maplist**. Los SVC necesitan la opción maplist, que ofrece en una lista la correspondencia del dispositivo actual con el resto de dispositivos para llamar y establecer SVC.

MODO DE TRANSFERENCIA ASÍNCRONO

ATM es un estándar definido por la ITU-T para Relay de celda.

En el caso de ATM todas las celdas tienen 53 bytes de longitud.

Al usar Relay de celda, ATM esta diseñado para manejar tipos de servicios de red entre los que se incluyen voz, vídeo y datos. Una red ATM consta de switches ATM(dispositivos DCE) y puntos finales ATM(dispositivos DTE). Los puntos finales envían información a los switch ATM, que segmentan la información en celdas y conmutan las celdas a través de la red. Este proceso es el mismo para los 3 tipos de tráfico que maneja la red ATM.

ITU-T basó ATM en el estándar Red digital de servicios integrados de banda ancha (Broadband Integrated Services Digital Network, B-ISDN) que se diseño inicialmente para enviar voz, vídeo y datos a través de una red publica. Una coalición de empresas formo el Forum ATM que ha creado especificaciones para la interoperatividad de varios fabricantes y extensiones ATM para redes publicas y privadas.

Hasta la fecha, el Forum ATM ha escrito 3 versiones de la interfaz de usuario a red.

(User-Network Interface, UNI) un protocolo similar en concepto a LMI de Frame Relay que regularizan la comunicación entre los dispositivos ATM y los switches. El Forum ATM también ha publicado documentos que definen las comunicaciones estándar entre los switches ATM (llamada Interfaz privada de red a red o PNN, Private Network-to Network Interface) y un método para emular las arquitecturas clásicas LAN a través de ATM, que se denominan Emulación de LAN (LAN Emulatión, LANE)

ATM cuenta también con un servicio sin conexión que le permite funcionar de manera parecida a una tecnología LAN.

ATM proporciona servicios tanto orientados a conexión como sin conexión mediante canales virtuales. Un canal virtual es similar a un circuito virtual en X-25 o Frame Relay.

La red ATM define las conexiones a través de la red ATM como rutas virtuales, que se identifican mediante números de identificador de ruta virtual(virtual path identifier, VPI).

Una ruta virtual es un paquete de canales virtuales que están conmutados a través de la red ATM basándose en el mismo VPI.

Un canal virtual se identifica mediante la combinación de un VPI y un identificador de canal virtual (virtual channel identifier, VCI): El VPI define la ruta que recorre el canal virtual a través de la red, mientras que el VCI es exclusivo para cada conexión de VPI. Los números VPI y VCI sólo tienen importancia local, al igual que los números DLCI para Frame Relay suelen tener solamente importancia local. Los switches ATM asignan los números VPI/VCI a través de un enlace particular con el siguiente dispositivo de la conexión (en la dirección de destino).

Las redes ATM agrupan las rutas virtuales en grupos, que se denominan rutas de transmisión. Una ruta de transmisión contiene rutas virtuales, que a su vez contiene canales virtuales.

Las redes ATM pueden usar 2 tipos diferentes de direccionamiento, uno basado en el direccionamiento E.164(un esquema de direccionamiento similar a los números de teléfono) y otro basado en las direcciones punto de acceso a servicio de red(network service access point, NSAP) OSI. El esquema de direccionamiento e.164 fue desarrollado por la ITU-T y es esquema de direccionamiento NSAP fue añadido por el forum ATM. Es habitual usar el direccionamiento E.164 en redes ATM publicas que proporcionen las portadoras de comunicaciones y el direccionamiento NSAP en redes ATM privadas, como una que conecte switches ATM y dispositivos de interconexión de redes. ATM ha definido 3 capas de adaptación ATM. Las capas de adaptación ATM(AAL) son1 protocolos que forman parte del modelo de referencia OSI en la parte superior de la capa de enlace de datos. Estas capas, son responsables de proporcionar los diferentes servicios ATM a los protocolos de la capa de la red. AAL1 es un servicio orientado a conexión que se suele utilizar para emular circuitos virtuales a través de la red ATM. Las aplicaciones habituales de AAL1 son las conexiones de voz y vídeo.

AAL3/4 admite datos tanto orientados a conexión como sin conexión. Muchas conexiones AAL 3/4 las utilizan los ISP de servicios para redes para datos sin conexión. AAL 3/4 esta diseñado para integrarse fácilmente en la SMDS otra tecnología estándar de Relay de celda.

AAL 5, admite también servicios tanto orientados a conexión como sin conexión. AAL 5 se utiliza para transferir información que no necesite integrarse fácilmente con SMDS, como datos a través de una LAN o WAN privada. La mayoría de las conexiones ATM en redes privadas usan AAL 5.

ATM admite garantías de calidad de servicio (QoS) a través de la red.

Cada uno de los dispositivos ATM interactúa con la red ATM para ofrecer una determinada calidad de servicios para cada ruta virtual basándose en un contrato de tráfico y normativas de tráfico.

Un contrato de tráfico especifica los requisitos de canal virtual, como el pico de ancho de banda, el ancho de banda medio sostenido y tamaño de ráfaga. La formación de tráfico controla el flujo de tráfico para que se ajuste al contrato de tráfico, restringiendo las ráfagas de datos, pasando las celdas en un flujo constante y limitando los picos de las velocidades de datos.

Las normativas de tráfico aplican el contrato de tráfico examinando el flujo actual de tráfico y comparándolo con el contrato de tráfico. Los procedimientos de normativas de tráfico pueden hacer que los switches descarten celdas si violan el contrato en situación de congestión.

SUBCOMANDOS DE CONFIGURACIÓN DE LA INTERFAZ ATM

Las interfaces de ATM de Cisco son procesadores dedicados de la interfaz o adaptadores de puerto en una tarjeta VIP.
Esto implica que no es necesario especificar el subcomando de interfaz **encapsulation** para las interfaces ATM. La encapsulación ATM es lo único que admite el hardware. No hay que especificar los circuitos virtuales que existen en una interfaz determinada utilizando el comando de interfaz **atm pvc**.
Ejemplo:
Configuración de PVC 1 usando VPI 0 y VCI 100 para un canal virtual AAL 5.

```
Router#configure
Router(config)#int atm2/0
Router(config-if)#atm pvc 1 0 100 aal5snap
Router(config-if)#Ctrl+Z
```

LINEA DE ABONADO DIGITAL

La línea de abonado digital(Digítal subscriber Line, DSL) es una tecnología que se ha generalizado en los últimos años y que tiene capacidad para ofrecer ancho de banda dedicado de alta capacidad a los usuarios finales. DSL emplea una topología de red en estrella, teniendo el centro de la estrella conexiones dedicadas a los nodos hoja con cable de cobre de par trenzado.

El ancho de banda entre los nodos hoja y el centro de la estrella puede variar de 64Kbps a 8Mbps, dependiendo de las características del cable de cobre, las interconexiones físicas, la distancia que recorre la señal, las condiciones medioambientales y la tecnología DSL especifica utilizada. Las distancias más cortas, las interconexiones mínimas y el cable de cobre de gran calibre pueden arrojar mayores velocidades de transmisión de datos.

La tecnología ADSL proporciona ancho de banda asimétrico entre el centro de la estrella y un nodo hoja, la transmisión de datos desde el centro de la estrella al nodo hoja es más rápida(3 veces más) que la ruta contraria.

Un módem ADSL crea tres canales separados:

- Canal de flujo ascendente
- El canal duplex
- Un canal de servicio telefónico básico

El equipo de red como los router y los bridges se conectan a los módem ADSL utilizando la tecnología WAN como ATM o Frame Relay. Cada uno de los usuarios finales, o algunas veces cada canal por usuario final, sería para el equipo de red como un circuito virtual separado. En una interfaz WAN de alta velocidad a un módem ADSL, un router puede admitir un gran número de circuitos virtuales y sus correspondientes usuarios.

Cisco fabrica una serie de routers, la serie 600 que cuenta con interfaces DSL. Los routers Cisco de la serie 600 pueden actuar como Ethernet para los bridges o routers DSL, o pueden ser módems tanto para conexiones ADSL como SDSL. En este momento, la serie 6000 de Cisco funciona utilizando una variante de IOS denominada Sistema Operativo de banda ancha de Cisco (Cisco Broadband Operating System, CBOS). La configuración de CBOS es diferente que la de IOS pero Cisco tiene previsto cambiar esta interfaz de usuario de CBOS para que sea compatible con el IOS. La combinación de los productos IOS y CBOS permite crear una red con una gran variedad de entornos.

RED DIGITAL DE SERVICIOS INTEGRADOS (RDSI)

RDSI o ISDN es una tecnología WAN orientada a conexión que usa la tecnología digital para digitalizar voz, datos, vídeo y otro tipo de información a través de la línea telefónica existente.

Los dispositivos que se conectan a la red RDSI son terminales. LOS 2 tipos de terminales son los que comprenden los estándares RDSI, que se denominan equipo del terminal tipo 1 (TE1) y los que preceden a los estándares RDSI, que se denominan equipo de terminal tipo 2 (TE2). TE2 se conecta a la red RDSI usando un adaptador de terminal (terminal adapter, TA). Los TE1 no necesitan TA.

RDSI ofrece 2 tipos de servicios:
Interfaz de acceso básico, BRI e interfaz de acceso primario, PRI.

Un identificador de perfil de servicio (Service Profile Identifier, SPID) es un número que utilizan algunas portadoras telefónicas para definir los servicios disponibles para un dispositivo RDSI. En muchos casos, el número SPID es equivalente del número de teléfono del dispositivo RDSI. El dispositivo RDSI ofrece el SPID al switch RDSI, que permite entonces que el dispositivo acceda a la red para recibir servicio BRI o PRI. Si no se proporciona un SPID valido, muchos switches RDSI no permiten que un dispositivo RDSI realice una llamada a través de la red.

SUBCOMANDOS DE CONFIGURACION DE INTERFAZ DE RDSI

La configuración de RDSI en los dispositivos Cisco IOS exige que se informe al dispositivo del tipo de switch RDSI al que se encuentra conectado. Este requisito es necesario porque el terminal RDSI necesita comunicarse con cada uno de los switches RDSI de los diferentes fabricantes de manera exclusiva.

Es posible encontrar todos los tipos de switch RDSI al que esta conectado el dispositivo IOS que se esté utilizando acudiendo al sistema de ayuda de IOS con el comando de configuración **isdn switch-type?**.

Hace falta que el dispositivo IOS conozca el fabricante de switch RDSI con el que hablará, ya que cada fabricante tienen un protocolo exclusivo para señalización.

Si no está configurado el tipo de switch RDSI adecuado, el dispositivo Cisco no puede comunicarse con el switch RDSI de las instalaciones de la portadora telefónica.
Para cada una de las interfaces BRI RDSI es necesario especificar los SPID utilizando para ello los subcomandos de interfaz **isdn spid1** y **isdn spid2**.

Cada SPID identifica a un canal B exclusivo de switch RDSI. Es necesario especificar los 2 SPID diferentes para una interfaz BRI. Para usar PRI RDSI en un dispositivo Cisco, se necesita una interfaz PRI RDSI, este tipo de interfaz es compatible con los routers y los servidores de acceso de gama alta y media, como por ejemplo, los routers de las series 3600, 4000 y 7000 de Cisco y los servidores de acceso 5300 de Cisco.

La PRI se comunica con el switch RDSI a través de un controlador T1.

Un controlador T1 es un paquete de software de enlace de datos que maneja la señalización del enlace de datos en la interfaz. Es preciso especificar la información especifica al enlace de datos para el controlador T1, como el método de entramado y el método de codificación de líneas.

En el siguiente ejemplo, configuramos un controlador T1 en la interfaz serial1/0 para un entramado de supertramas apiladas(Extended superframe, ESF), codificación de líneas binarias con sustitución de 8 ceros(Binary 8-zero substitución, B8ZS) y una RDSI de acceso principal que usa 24 periodos de tiempo. ESF es un tipo de entramado que se usa en los circuitos T1.

Consta de 24 tramas de 192 bits de datos cada una, proporcionando el bit número 193 la temporización y otras funciones. B8ZS es un mecanismo de codificación de líneas que garantiza la densidad a través de un enlace al sustituir un código especial siempre que se envíen 8 ceros consecutivos y posteriormente elimina el código especial en el extremo final de la conexión.

```
Router#configure
Router(config)#controller T1 1/0
Router(config-if)#framing esf
Router(config-if)#linecode b8zs
Router(config-if)#pri-group timeslots 1-24
Router(config-if)#Ctrl-Z
```

SPOOFING

Significa que la interfaz RDSI siempre pretende estar preparada para enrutar paquetes, aunque es posible que no tenga realizada una llamada digital válida. La interfaz RDSI engaña al protocolo de enrutamiento y al resto del software del dispositivo IOS para que crea que la interfaz está encendida y en funcionamiento(y no está es spoofing) durante un periodo de tiempo hasta que la llamada no hace nada.

La interfaz corta entonces la llamada y vuelve al modo spoofing hasta que necesite realizar otra llamada digital para enrutar datos. Este mecanismo(fingir que la interfaz está en funcionamiento, realizar la llamada digital para transferir los datos y luego cortar la llamada cuando no es necesaria) se denomina **Enrutamiento bajo demanda.**

RESUMEN DE COMANDOS

Ethernet y Fast Ethernet **media-type[ani, 10baseT, mii, 100basex]**

Fast Ethernet y Gigabit ethernet **full-duplex**

Token Ring **ring-speed[4|16] Early-toke-ring**

X-25 **x25 address x121 address x25 ips X25 ops x25win x25 wont**

Frame Relay **Frame-Relay interface-dlic frame relay lmi-tipe**

ATM **atm pvc**

DSL **set bridging set interface**(solamente CBOS)

RDSI **isdn switch-type isdn spid1 isdn spid2 pri-group timeslots**

T1 **framing linecode**

TCP/IP PROTOCOLO DE CONTROL DE TRANSMISION/PROTOCOLO DE INTERNET

Protocolo IP enrutado de la capa 3.
Funcionalidad extremo a extremo en la capa 4.
TCP/IP se usa como protocolo de acceso a Internet y para interconectar dispositivos de redes corporativas.

El conjunto de protocolos TCP no solo incluye especificaciones de capa 3 y 4, sino también especificaciones para aplicaciones comunes, como correo electrónico, emulación de terminal y transferencia de archivos.

Transferencia de archivos: **TFTP, FTP, NFS.**
Correo electrónico: **SMTP**
Login remoto: **TELNET Y RELOGIN**
Administración de red: **SNMP**
Administración de nombres: **DNS**

OSI	TCP/IP
Aplicación	Aplicación
Presentación	
Sesión	
Transporte	Transporte
Red	Red
Enlace de datos	Capa de interfaz de red
Física	

GENERALIDADES DE LA CAPA DE TRANSPORTE

Los servicios de transporte permiten que los usuarios puedan segmentar y volver a ensamblar varias aplicaciones de la capa superior en el mismo flujo de datos de la capa de transporte.
Este flujo de datos de la capa de transporte proporciona servicios de transporte de extremo a extremo. El flujo de datos de la capa de transporte constituye la conexión lógica entre los puntos finales de la red el host origen o emisor y el host de destino o receptor.

La capa de transporte realiza dos funciones: Control de flujo por ventanas deslizantes y fiabilidad obtenida a través de números de secuencia y acuse de recibo.

El control de flujo es un mecanismo que permiten a los host en comunicación negociar la cantidad de datos que se transmiten cada vez.

La fiabilidad proporciona un mecanismo para garantizar la distribución de cada paquete.

En la capa de transporte hay dos protocolos:

TCP:

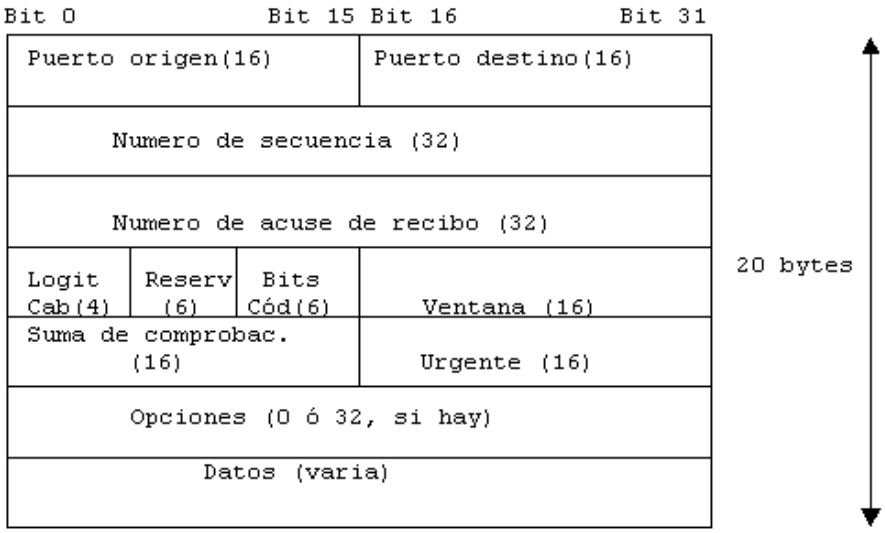
Se trata de un protocolo fiable, orientado a conexión. En un entorno orientado a la conexión, se ha de establecer una conexión entre ambos extremos antes de que pueda tener lugar la transferencia de información.

TCP es el responsable de la división de los mensajes en segmentos y el reensamblado posterior de los mismos cuando llegan a su destino, volviendo a enviar cualquiera que no haya sido recibido.
TCP proporciona un circuito virtual entre las aplicaciones de usuarios finales.

UDP (PROTOCOLO DE DATAGRAMA DE USUARIO)

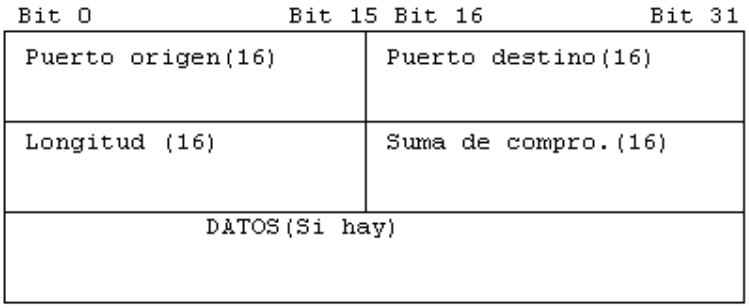
Es un protocolo sin conexión ni acuse de recibo. Aunque UDP es el responsable de transmisión de mensajes, no existe verificación de la distribución de segmentos en esta capa.
UDP depende de los protocolos de capa superior para conseguir la debida fiabilidad.

CABECERA TCP



Puerto origen: Número de puerto que llama (16 bits).
Puerto destino: Número del puerto al que se llama (16 bits).
Número de secuencia: Número usado para garantizar la corrección en la secuencia de la llegada de datos(32 bits).
Número de acuse de recibo: Siguiente octeto TCP esperado(4 bits).
Reservado: Fijado en 0(6 bits).
Bits de código: Funciones de control, como el establecimiento y la finalización de una sesión(6 bits).
Ventana: Número de octetos que el dispositivo espera aceptar (16) bits).
Suma de comprobación: Suma de comprobación de cabecera y campos de datos (16 bits).
Urgente: Indica el final de los datos urgentes(16 bits).
Opciones: Algo ya definido, tamaño máximo del segmento TCP(0 a 32 bits, si hay)

CABECERA UDP



UDP es utilizado por TFTP, SNMP, NFS, DNS.

Tanto TCP como UDP utilizan los números de puerto para pasar información a las capas superiores. Los números de puerto se usan para registra las diferentes conversaciones que están teniendo lugar al mismo tiempo en la red.

FTP----------21 Puerto para dialogo para la transferencia de archivos.
TELNET----------23 Puerto de conexión remota mediante Telnet.
SMTP----------25 Protocolo simple de transferencia de correo.
DNS----------53 Servidor de nombres de dominios.
TFTP----------69
SNMP----------161 Usado para recibir peticiones de gestión de red.
RIP----------520
POP3----------110 Servidor de recuperación de correo del PC.
NNTP----------119 Acceso a las noticias de red.
FTPDATA---------20 Puerto de transferencia de datos para la transferencia de archivos.
DISCARD---------9 Descartar el datagrama de usuario/Descarta todos los datos entrantes.
CHANGEN---------19 Intercambiar flujos de caracteres.
ECHO----------7 UDP/ Eco del datagrama de usuario de vuelta al emisor.
FECHA Y HORA----13(Daytime)
BooTPS----------67
BooTPC----------68
SunRCP----------111
NTP----------123
SNMP-trap-------162

A las conversaciones donde no están implicadas aplicaciones con números de puertos bien definidos/conocidos se les asigna números de puerto aleatoriamente elegidos dentro de un rango específico. Estos números de puerto se utilizan como direcciones de origen y destino en el segmento TCP.

Los números por debajo de 1024 se consideran puertos bien conocidos.

Los números por encima de 1024 se consideran puertos asignados dinámicamente.

DNS usa los dos protocolos de transporte, utiliza UDP para la resolución del nombre y TCP para transferencias en la zona del servidor.

RFC 1700 define todos los números de puerto bien conocidos para TCP/IP en www.iana.org

Los sistemas finales usan los números de puerto para seleccionar la aplicación apropiada.

Los números de puerto de origen son asignados dinámicamente por el host del origen, números por encima de 1023.

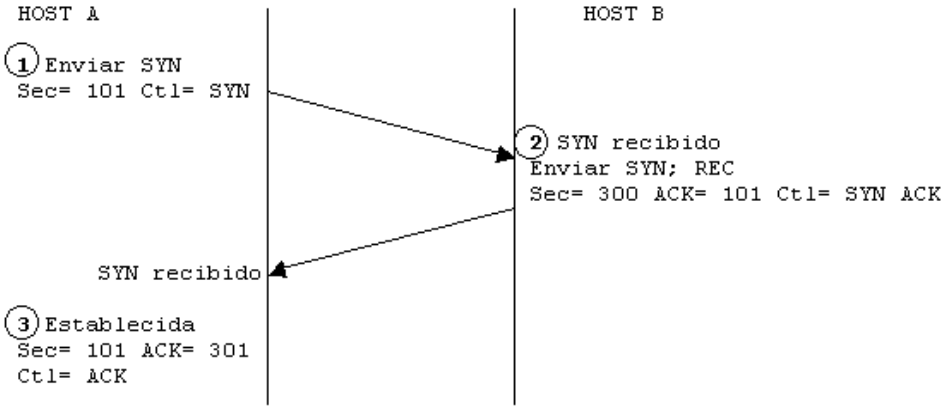
ESTABLECIMIENTO DE UNA CONEXIÓN TCP.

TCP esta orientado a la conexión, por lo que requiere que establezca la conexión antes de que puedan iniciarse la transferencia de datos.

Los host deben sincronizar sus números de secuencia inicial(ISN).
La sincronización se lleva a cabo mediante un intercambio de segmentos de establecimiento de conexión que transportan un bit de control llamado SYN(de sincronización), y los números de secuencia inicial.

La solución requiere un mecanismo apropiado para recoger un número de secuencia inicial y que reciba una confirmación de que la transmisión se ha realizado con éxito, mediante un acuse de recibo(ACK) por parte del otro lado.

INTERCAMBIO DE SEÑALES A 3 VIAS



Paso-1

El Host A envía al Host B SYN. Mi número de secuencia es 100, el número ACK es 0, el bit ACS no esta establecido. El bit SYN esta establecido.

Paso-2

El Host B envía al Host A ACK. Espero ver 101 a continuación, mi número de secuencia es 300, ACK ha sido establecido. El bit SYN del Host B al Host A ha sido establecido.

Paso-3

El Host A envía al Host B ACK. Espero ver 301 a continuación, mi número de secuencia es 101, el bit ACK ha sido establecido. El bit SYN ha sido establecido.

Es necesario un intercambio de señales de 3 vías, debido a que los números de secuencia no están ligados a ningún reloj global de la red y los TCP podrían tener diferentes mecanismos para recoger los números de secuencia inicial.

El tamaño de ventana determina la cantidad de datos que acepta el puerto receptor de una vez, antes de que vuelva un acuse de recibo.

TCP proporciona una secuencia de segmentos con un acuse de recibo de referencia.

Cada datagrama es numerado antes de la transmisión. En el puesto receptor, TCP se encarga de volver a ensamblar los segmentos en un mensaje completo.

Los segmentos que no son reconocidos dentro de un periodo de tiempo determinado, da lugar a una nueva retransmisión.

Si falta un número de secuencia en la serie, se retransmite el segmento correspondiente.

CONTROL DE FLUHO PARA TCP/UDP

Para gobernar el flujo de datos entre dispositivos, TCP usa un mecanismo de control de flujo.

El TCP receptor devuelve una "ventana" al TCP emisor. Esta ventana especifica el número de octetos comenzando por el número de referencia, que el TCP receptor está preparado para recibir en este momento.

Los tamaños de la ventana TCP varia durante la vida de una conexión. Cada acuse de recibo contiene un aviso de ventana que indica la cantidad de bytes que el receptor puede aceptar.

TCP mantiene también una ventana de control de congestión que suele tener el mismo tamaño que la ventana de receptor, pero que se divide en dos cuando se pierde un segmento.

UDP está diseñado para que las aplicaciones proporcionen sus propios procesos de recuperación de errores. Aquí se cambia por velocidad.

PRINCIPIOS BÁSICOS DE TCP/IP

TCP/IP desarrollado a mediados de los 80 como proyecto de la DARPA(Defense Advanced Research Projects Agency) para proporcionar servicios de comunicación a nivel nacional para las universidades y entidades de investigación, TCP/IP se ha convertido en el estándar de facto de los protocolos para la conexión en red de sistemas computacionales distintos.

Es un conjunto de protocolos de comunicación que define la forma de dirigirse a las distintas computadoras de la red, los métodos que se utilizan para pasar la información de una computadora a otra y algunos servicios que se pueden utilizar entre computadoras.

El protocolo Internet (IP), el componente de direcciones TCP/IP, funciona en la capa 3 del modelo de referencia OSI. Todas las direcciones que quieren comunicarse con otra tienen una dirección IP única.

Los 2 protocolos de transporte principales, el protocolo de datagrama de usuario, UCP y el protocolo de control de transmisión, TCP están en la capa 4 del modelo de referencia OSI para TCP/IP, los protocolos de transporte son responsables de los mecanismos básicos de transferencia, del control de flujos y la comprobación de errores en las comunicaciones entre estaciones.

UDP se considera poco fiable, la estación receptora no confirma la recepción de los paquetes. Se considera sin conexión porque no hace falta que ninguna estación remitente avise a la estación receptora de su deseo de formar un canal de comunicaciones sobre el que pasar datos.

TCP se considera un protocolo orientado a conexión, ya que la estación remitente debe avisar a la receptora de su deseo de formar el canal se comunicaciones. Los paquetes se marcaran con números de secuencia y las estaciones remitente y receptora se intercambia acuses de recibo mutuos confirmando la recepción de los paquetes.

La dirección IP es una dirección binaria de 32 bits escrita en cuatro grupos de 8 bits llamados octetos. La dirección completa representa los tres componentes del modelo de direcciones IP(es decir, las partes de red, subred y host de la dirección).

Cada valor de 8 bits de los octetos pueden adoptar el valor de 0 o de 1.

Los 3 componentes describen los distintos niveles de la especifidad de la entidad dentro de un conjunto de sistemas de red. El componente de host es más especifico, ya que describe la dirección de una sola estación de trabajo o servidor. El componente de red es más general, ya que describe la dirección de un conjunto de host dentro de la misma lógica de computadores. El componente de subred se encuentra entre los otros dos componentes. Describe la dirección de un subconjunto de los host dentro de un espacio de direcciones global de la red.

La subred se crea "tomando prestada" una parte del componente de host para crear subgrupos de direcciones dentro de la misma red lógica. El componente de subred suele identificar un conjunto de sistemas de un segmento de LAN o de WAN. De izquierda a derecha. La parte de red, la subred y el host.

Existen 5 clases de direcciones IP.

- Clase A
- Clase B
- Clase C
- Clase D
- Clase E

Si no hay subredes la dirección nos indica que parte de la dirección de la red que leer como parte de red y que parte hay que leer como parte de host. Algunos dispositivos, como los routers necesitan descifrar esta información para evitar datos al destino apropiado.

Sin embargo, si una red tiene subredes, no es posible decir a primera vista que parte de host de la dirección se ha perdido prestada para crear la subred. Para resolver este dilema las direcciones IP tienen una máscara de subred(máscara de red).

La máscara de red es un número binario de 32 bits, agrupado en 4 octetos que se expresan en notación decimal.
Los bits de la máscara de red tienen un valor 1 en todas las posiciones, a excepción de la parte de host de la dirección IP.
Se pueden agrupar varias direcciones IP de red de una clase determinada en lo que se llama una superred o un bloque de enrutamiento entre dominios sin clase(classless interdomain route, CIDR).

Algunas de las antiguas redes de clase A se han subdividido y se han otorgado en forma de bloques CIDR más pequeñas.
La organización que recibe una asignación de un bloque CIDR es libre de volver a subdividir ese espacio de direcciones de red como subredes dentro de su red lógica o como asignaciones a sus clientes.

Mediante la subdivisión de estos antiguos bloques grandes de direcciones de red, se ha podido utilizar un mayor número de direcciones IP de red y se ha ralentizado el agotamiento de las mismas.

CONFIGURACIÓN DE DIRECCIONES IP

Las direcciones para solicitar un espacio de direcciones IP a los registros se pueden encontrar en cada uno de los sitios web de los registros específicos.
ARIN: American Registry for Internet Numbers www.arin.net
RIPE: Reseaux IP Europeens www.ripe.net
APNIC: Asia Pacific Network Información Center www.arnic.net

Si la red no va a conectarse a Internet o tiene intención de utilizar técnicas avanzadas de firewall y de conversión de direcciones de red(NAT) que se encuentran en productos como Cisco Systems Private Internet Exchange(PIX), es muy recomendable utilizar direcciones IP de una clase de direcciones que se han designado como direcciones privadas porque la información acerca de estas redes no la propaga en Internet ningún ISP o NSP.

El conjunto de direcciones IP privadas se define en la RFC 1918 "Address Allocatión for Private Internets"

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

La forma en que se asigne el espacio depende fundamentalmente del número de host que vallan ha estar conectados a un segmento dado de la LAN, del número de segmentos de LAN/WAN que haya en la red y de la cantidad de espacio de direcciones que haya en la red. Si la red va a utilizar direcciones IP privadas, la cantidad de espacio de direcciones disponible no es un problema.

Es conveniente utilizar un esquema de subred eficaz que no sobre asigne direcciones a segmentos, como interfaces de WAN punto a punto, independientemente del espacio de direcciones que esté asignado a la red.

El centro de asistencia técnica(Technical Assistance Center, TAC) de Cisco Systems ha creado un calculador para el diseño de subredes IP(IP Subnet Design Calculator) que pueden descargar los usuarios registrados.

CONFIGURACION DE LA INTERFAZ DE LAN

Algunos dispositivos como los routers, tienen una dirección IP única en cada uno de los segmentos de LAN vinculados a ellos. Por consiguiente, el router sabe qué redes están conectadas a cada interfaz y donde deben enviarse los paquetes para dichas redes.

Algunos dispositivos como los switch y los bridges tienen una sola dirección IP para todo el sistema. Esta dirección IP se utiliza exclusivamente para la administración remota y la administración de red.

Los protocolos WAN no admiten una asignación dinámica de la dirección de enlace de datos a la dirección IP y requieren la configuración de las direcciones IP para comunicarse con otras estaciones a través de una interfaz WAN.

La asignación de direcciones IP tanto a las interfaces LAN como de WAN se realiza con el subcomando de configuración de Cisco IOS **ip address**.

Este comando exige que se introduzcan la dirección IP y la máscara de red de dicha dirección IP.

Router(config-if)#ip address[dirección IP][máscara de subred]

Es aconsejable reservar algunas direcciones IP del principio o del final de cada espacio de direcciones de red de la LAN para los routers y cualesquiera otros dispositivos de la infraestructura de la red. Tener un grupo coherente de direcciones para varios dispositivos de red en todos los segmentos de la LAN facilita la solución de problemas, ya que permite reconocer rápidamente direcciones IP especificas.

Router(config-if)#**ip address[dirección IP][máscara de red]**

Debe asignar una dirección IP de red a cada una de las conexión WAN punto a punto(o subinterfaces punto a punto).

Router(config)#**interface serial 0.16 point-to-point**
Router(config-if)#**ip address[dirección IP][máscara de red]**

Las interfaces IP no numeradas de WAN punto a punto se configuran utilizando el subcomando de interfaz **ip unnumbered**. El comando requiere que se introduzca un parámetro de interfaz de referencia para que los protocolos de enrutamiento de IP pueden utilizar una dirección IP real al ejecutarse a través de la interfaz no numerada. Esta interfaz puede ser física o una interfaz virtual como la interfaz loopback.

Ninguno de los dos extremos del enlace WAN puede tener número, es decir, no es posible asignar una dirección a un extremo y que el otro no tenga número.

Router(config)#**interface serial 1**
Router(config-if)#**ip unnumbered loopback 0**

Las interfaces IP no numeradas tienen dos inconveniente. No es posible establecer una conexión de un terminal virtual(por ejemplo a través del protocolo Telnet), directamente con la interfaz serie o utilizar SNMP para realizar consultas a través de la interfaz serie.

Si la interfaz no numerada aparece en una interfaz de LAN y dicha interfaz esta apagada o tiene un fallo, es posible que no pueda tener acceso al dispositivo. Este es el motivo por el que es aconsejable que las interfaces no numeradas estén referenciadas a interfaces virtuales, como la interfaz loopback.

DIRECCIONAMIENTO DE LAS INTERFACES DE WAN MULTIPUNTO

Una interfaz WAN multipunto, es aquella en la que se pueden acceder a varios dispositivos a través de una sola conexión a un medio WAN. Los elementos que se envían a los interfaces de WAN multipunto no saben cual es la estación de destino, por lo que hay que asignar direcciones a las interfaces de WAN multipunto para las comunicaciones IP. Además las tecnologías WAN multipunto, tienen metodología de direcciones de enlaces de datos para distinguir las distintas estaciones de la WAN, por lo que debe haber una asignación de la dirección IP a la dirección de enlace de datos. La excepción es que Frame Relay sí tiene un método de asignación dinámico llamado ARP inverso(Inverse ARP).

```
Router(config)#int serial 1/1
Router(config-if)#encapsulation Frame-Relay ietf(tipo de
encapsulación)
Router(config-if)#no inverse-arp
Router(config-if)#ip address[dirección IP][mascara de red]
Router(config-if)#Frame-Relay map IP[dirección IP]30 cisco broadcast
Router(config-if)#Frame-Relay map IP[dirección IP]50(50 = DLCI)
broadcast
Router(config-if)#Ctrl+z
```

El subcomando de interfaz de IOS no inverse-arp desactiva la función de asignación dinámica ARP inverso.
La palabra clave broadcast del final del comando Frame-Relay map indica al router que reenvíe las difusiones para esta interfaz a este circuito virtual específico.

En el ejemplo, se permite que la función ARP inverso realice una asignación dinámica de las direcciones IP a números DLCI, no habría necesidad de utilizar los comandos Frame-Relay map. En su lugar la interfaz envía consultas ARP inverso a todos los circuitos identificados como activos por parte de la red Frame Relay en esta interfaz.

El resultado de dichas consultas sería que los dispositivos mas alejados responderían con sus direcciones IP en el circuito virtual particular y el DLCI en que se realice la consulta.

Nota_

Palabras clave y comandos opcionales.

Al igual que la mayoría de los comandos de software IOS, todos los comandos de asignación de enlaces de datos a IP tiene palabras clave opcionales que cambian el comportamiento del circuito virtual o activan y desactivan características especiales en dicho circuito, como la compresión.

Explicación completa de todas las palabras clave opcionales ver www.cisco.com/univercd/home/home.htm

El uso de ARP inverso reduciría el ejemplo anterior a:

```
Router#configure
Router(config)#interface serial 1/1
Router(config-if)#encapsulation Frame-Relay ietf
Router(config-if)#ip address 131.108.130.1 255.255.255.0
Router(config-if)#Ctrl+Z
```

La configuración de Frame Relay requiere cierto cuidado. Si se utiliza ARP inverso para realizar la asignación de direcciones IP a DLCI, los errores de configuración pueden provocar que circuitos virtuales inesperados se asignen dinámicamente a dispositivos desconocidos.

La mezcla de las encapsulaciones del IETF y del "grupo de los cuatro" de Cisco en la misma interfaz Frame Relay requiere el uso del comando **Frame-Relay map**.

El direccionamiento estático de interfaces WAN X-25 se realiza de forma muy parecida a Frame Relay con el comando **static map**. Las direcciones IP de las interfaces X.121 que se utilizan para configurar los circuitos virtuales entre los sistemas de la red X-25. Cada uno de los circuitos virtuales se identifican por la dirección X.121 que se utiliza para configurar la conexión.

```
Router#configure
Router(config)#interface serial 1/2
Router(config-if)#encapsulation x25
Router(config-if)#x25 address[NNNNNNNN] (dirección X.121)
Router(config-if)#ip address[dirección IP][máscara de subred]
Router(config-if)#x25 map ip[dirección IP][dirección X.121]broadcast
Router(config-if)#x25 map ip[dirección IP][dirección X.121]broadcast
Router(config-if)#x25 map ip[dirección IP][dirección X.121]broadcast
Router(config-if)#Ctrl+Z
```

Debe introducirse la palabra clave **name** del comando **dialer map** para relacionar correctamente la dirección IP y el número de teléfono con el sistema remoto. Además la palabra clave **name** se utiliza como parte del proceso de autenticación cuando se establece una conexión con un sistema remoto.

Configuración RDSI acceso básico.

```
Router#configure
Router(config)#interface bri 0
Router(config-if)#ip address[dirección Ip][mascara de subred]
Router(config-if)#dialer map ip[dirección ip]name[nombre]broadcast[n°
tlfn]
Router(config-if)# dialer map ip[dirección ip]name[nombre]broadcast[n°
RDSI]
Router(config-if)#Ctrl+Z
```

Al igual que los restantes tipos de interfaces, ATM requiere el comando **ip address** básico.
Sin embargo, con las interfaces ATM, el tipo de comando utilizado para asignar direcciones IP a la capa de enlace de datos depende del tipo de protocolo ATM y del tipo de circuitos virtuales que se hayan utilizado. Estas son las tres posibles variaciones de protocolos:

Encapsulación Control de enlace lógico/Protocolo de acceso a subred(Logical Link Control/Subnetwork Access Protocol, LLC/SNAP) con PVC.

En este modelo, se establece un circuito virtual permanente a través de la red ATM. Los paquetes se identifican de tal forma que se sabe que van a destinados a una dirección IP al otro extremo del circuito virtual específico.

Encapsulación LLC/SNAP con PVC.

En este modelo, los paquetes IP se identifican como si fueran destinados a una dirección de la capa de enlace ATM definida de manera estática. Los switch ATM establecen el circuito virtual bajo demanda cuando el router solicita una conexión a la dirección ATM para una dirección IP específica.

IP con ARP.

En este modelo, la dirección de la capa de enlace ATM de una dirección IP específica se introduce dinámicamente por medio de una estación llamada servidor **ARP ATM**.

La encapsulación LLC/SNAP con PVC hace uso del subcomando de configuración de interfaz de IOS **map-group** y del comando de configuración global de IOS **map-list** para asignar las direcciones IP a PVC específicos.

```
Router#configure
Router(config)#interface atm 1/0
Router(config-if)#atm pvc 3 0 21 aal5snap
Router(config-if)#atm pvc 5 0 22 aalsnap
Router(config-if)#ip address[dirección IP][máscara de subred]
Router(config-if)#map-group[nombre]
Router(config-if)#map-list[nombre]
Router(config-map-list)#ip[dirección ip]atm-vc[n°]broadcast
Router(config-map-list)# ip[dirección ip]atm-vc[n°]broadcast
Router(config-map-list)#Ctrl+Z
```

La encapsulación LLC/SNAP con SVC hace uso del subcomando de configuración de interfaz de IOS **map-group** y del comando de configuración global de IOS **map-list** para asignar las direcciones IP a las direcciones NSAP que se usan para identificar los dispositivos remotos de la red ATM.

```
Router#configure
Router(config)#interface atm 1/0
Router(config-if)#atm nsap[dirección mac]
FE.DCBA.01.987654.3210.ABCD.EF12.3456.7890.1234.12
Router(config-if)#ip address[dirección IP][mascara de subred]
Router(config-if)#map-group[nombre]
Router(config-if)#map-list[nombre]
Router(config-map-list)#ip[dirección ip]atm-nsap A1.9876.AB.123456.
7890.FEDC.BA.1234.5678.ABCD.12
Router(config-map-list)# ip[dirección ip]atm-snap B2.9876.AB.123456.
7890.FEDC.BA.1234.5678.ABCD.12
Router(config-map-list)#Ctrl+Z
```

La variación clásica de IP con ARP necesita el subcomando **ip address** para configurar las direcciones IP de la interfaz. El subcomando de configuración de interfaz ATM **atm arp-server** identifica la dirección del servidor ARP ATM que puede resolver direcciones IP en direcciones NSAP ATM, lo que es necesario para establecer los circuitos virtuales.

Interfaz ATM con la variación clásica de IP con ARP.

```
Router#configure
Router(config)#interface atm 1/0
Router(config-if)#atm nsap
FE.DCBA.01.987654.3210.ABCD.EF12.3456.7890.1234.1
Router(config-if)#ip address[dirección IP][máscara de subred]
Router(config-if)#atm arp-server nsap
01.ABCD.22.030000.0000.0000.0000.0000
Router(config-if)#Ctrl+Z
```

VERIFICACIÓN DE LA CONFIGURACIÓN DE LAS DIRECCIONES IP

La verificación de las direcciones IP y de otros atributos IP que se hayan asignado a las interfaces puede realizarse a través de uno de los tres comandos ejecutables.

Show interface ofrece información general acerca de cada interfaz.
Sise introduce una interfaz específica como parámetro para el comando, solo aparecerá dicha interfaz. Si no se especifica ningún interfaz, se muestran todos.

Show ip interface ofrece una completa visión de los parámetros asociados con al configuración IP de una interfaz. Si se proporciona como parámetro una interfaz sólo aparece la información sobre dicha interfaz específica. Si no aparece información acerca de todas las interfaces.

Show ip interface brief permite ver un conciso resumen de la información IP y del estado de todas las interfaces disponibles en el dispositivo.

Además de comprobar la configuración IP en la propia interfaz, se puede ver las asignaciones tanto estáticas como dinámicas WAN multipunto. Para ello, utilizamos los comandos ejecutables de IOS **show Frame-Relay map**, **show atm map**, **show x.25 map** y **show dialer maps**.

Ejemplo:

```
Router#show Frame-Relay map
Serial0.16(up): point-to-point dlci, dlci 16(0x10, 0x400), broadcast,
status defined, active.
```

Las máscaras de red se pueden representar tanto en formato decimal con puntos, como en formato de cómputo de bits.

El comando ejecutable de IOS **terminal ip netmask-format decimal** solo surge efecto en la sesión de terminal virtual actual, para mantener este formato en todas las sesiones de los terminales virtuales o las consolas, hay que aplicar el subcomando de configuración de línea de IOS **ip netmask-format decimal**.

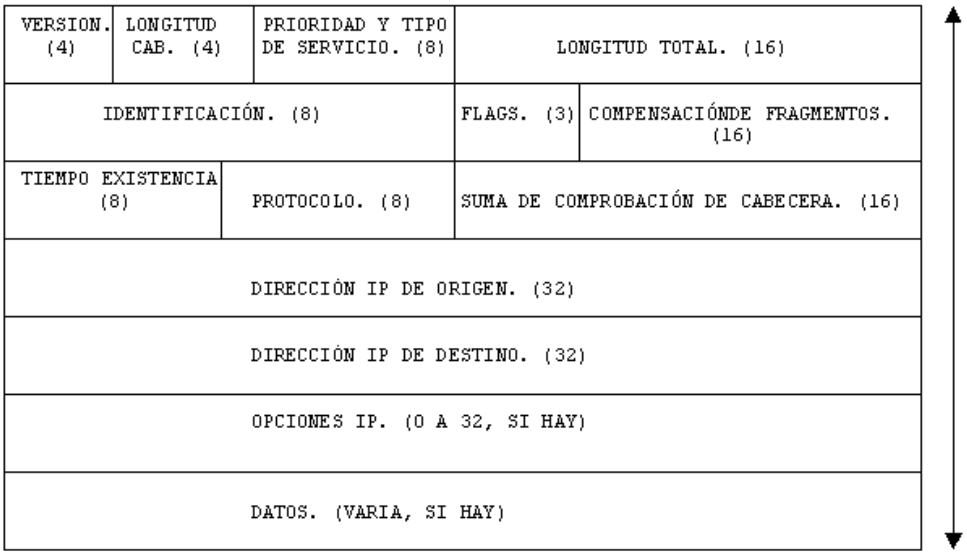
```
Router#configure
Router(config)#line vty 0 4
Router(config-line)#ip netmask-format decimal
Router(config-line)#Ctrl+Z
```

CAPA DE INTERNET

IP, ICMP, ARP, RARP.

CABECERA IP

20 bytes



Versión: Número de versión 4 bits

Longitud de cabecera: Longitud de cabecera en palabras de 43 bits.

Prioridad y tipo de servicio: Como debe ser gestionado el datagrama. Los 3 primeros bits son de prioridad.

Longitud total: Longitud total de la cabecera más los datos.

Identificación: Valor único del datagrama IP.

Flags: Especifica si debe tener lugar la fragmentación.

Compensación de fragmentos: Proporciona fragmentación de datagramas que permiten MTU diferidas en Internet.

TTL: Tiempo de existencia.

Protocolo: protocolo de capa superior (capa 4) que envía el datagrama.

Suma de comprobación: Comprobación de la integridad de la cabecera.

Dirección IP origen: Dirección IP de origen de 32 bits.

Opciones IP: Comprobación de la red, depuración, seguridad y otros.

Datos: Datos del protocolo de la capa superior.

Números de protocolo en RFC 1700.

Números de protocolo
ICMP------1
IGRP------9
Ipv6------41
GRE(Encapsulado genérico de enrutamiento)-------7
Intercambio de paquetes entre redes en el Protocolo Internet(IPX en IP)-------111
Protocolo de Tunneling de capa 2 (L"TP)---------115

RARP Protocolo de resolución de direcciones inversas.

Se usa por los puestos 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.

DCHP es una implementación más moderna de RARP.

CONFIGURACIÓN DE DIRECCIONES IP.

Asignar dirección lógica de red y gateway predeterminada al switch.
Como asignar la dirección lógica de red a una interfaz del router.
Como especificar el formato de mascara de subred.
Como asignar nombres de host a direcciones IP.
Como definir servidores de nombres.
Como obtener una lista de nombres y direcciones de host.

Cuando la mascara de red se muestre en formato hexadecimal siempre va precedida de 0X y suele ser en sistemas Unix.

255.255.255.0 = 0XFFFFFF00

Para especificar el formato de máscara de red en una sesión de un router, utilizar el comando:

term ip netmask-format[bicount|decimal|hexadecimal]

Para especificar el formato de máscara de red para una línea especificada, utilizar el comando:

ip netmask-format[bicount|decimal|hexadecimal]

ASIGANACION DE NOMBRES DE HOST A DIRECCIONES IP.

Para asignar manualmente nombres de host a direcciones, debe utilizar el comando:

ip host[nombre][número de puerto tcp][dirección ip][dirección ip]

nombre: Es cualquier nombre que describa el destino.
número de puerto tcp: Es el número opcional que identifica el puerto TCP que debe usarse cuando se emplee el nombre del host con un comando Telnet O EXEC.
dirección: Es la dirección o direcciones IP donde puede localizar el dispositivo.
Cada dirección IP puede tener asociado un solo host.
El router puede ser configurado, para registrar los nombres de dominio (hasta un máximo de 6 routers), este se encargará de gestionar la cache de nombres (cache que acelera el proceso de convertir nombres a direcciones).

ip name-server define el host que puede proporciona el servicio de nombres.

ip domain-lookup activa la traducción de nombres a direcciones en el router.

DETERMINACIÓN DE ROUTAS IP.

Las rutas se pueden determinar por medio de rutas estáticas o mediante protocolos de enrutamiento dinámico.
El enrutamiento es el proceso por el cual un elemento pasa de una ubicación a otra.

Para poder enrutar paquetes de información un router (o cualquier otro elemento que se encargue de realizar el enrutamiento, como puestos UNIX encargados de ejecutar el motor de enrutamiento, o switches de la capa 3) debe conocer lo siguiente:

Dirección de destino: ¿Cuál es el destino del elemento que necesita ser enrutado?

Fuentes de información: Desde que fuente(otros routers) puede aprender el router las rutas hasta los destinos especificados.

Rutas posibles: ¿Cuáles son las rutas iniciales posibles hasta los destinos perseguidos?

Rutas optimas: ¿cuál es la mejor ruta hasta el destino especificado?

MANTENIMIENTO Y VERIFICACIÓN DE LA INFORMACIÓN DE ENRUTAMIENTO.

Una forma de verificar que las rutas hasta los destinos conocidos son validas y las más actualizadas.

La información de enrutamiento que el router aprende desde sus fuentes de enrutamiento se colocan en su propia tabla de enrutamiento. El router se vale de esta tabla para determinar los puertos de salida que debe utilizar para retransmitir un paquete hasta su destino. La tabla de enrutamiento es la fuente principal de información del router acerca de las redes.

Si la red de destino está conectada directamente, el router ya sabrá el puerto que debe usar para reenviar paquetes.

Si las redes de destino no están conectados directamente, el router debe aprender y calcular la ruta más óptima a usar para reenviar paquetes a dichas redes. La tabla de enrutamiento se constituye usando uno de estos dos métodos:

- Manualmente, por el administrador de la red.
- A través de procesos dinámicos que se ejecutan en la red.

RUTAS ESTÁTICAS

Aprendidas por el router a través del administrador, que establece dicha ruta manualmente, quien también debe actualizar cuando tenga lugar un cambio en la topología.

RUTAS DINÁMICAS

Rutas aprendidas automáticamente por el router, una vez que el administrador ha configurado un protocolo de enrutamiento que permite el aprendizaje de rutas.

HABILITACIÓN DE RUTAS ESTÁTICAS

Las rutas estáticas se definen administrativamente y establecen rutas específicas que han de seguir los paquetes para pasar de un puerto de origen hasta un puerto de destino.

La gateway(puerta de enlace) de ultimo recurso, es la dirección a la que el router debe enviar un paquete destinado a una red que no aparece en su tabla de enrutamiento.

Las rutas estáticas se utilizan habitualmente en enrutamientos desde una red hasta una red de conexión única, ya que no existe más que una ruta de entrada y salida en una red de conexión única, evitando de este modo la sobrecarga de tráfico que genera un protocolo de enrutamiento.

La ruta estática se configura para conseguir conectividad con un enlace de datos que no esté directamente conectado al router. Para conectividad de extremo a extremo, es necesario configurar la ruta en ambas direcciones.

Las rutas estáticas permiten la construcción manual de la tabla de enrutamiento.

El comando **ip route** configura una ruta estática, los parámetros del comando definen la ruta estática.

Las entradas creadas en la tabla usando este procedimiento permanecerán en dicha tabla mientras la ruta siga activa. Con la opción **permanet**, la ruta seguirá en la tabla aunque la ruta en cuestión haya dejado de estar activa.

ip route[red][máscara][dirección ip][interfaz][distancia][permanet]

red: Es la red o subred de destino.
máscara: Es la máscara de subred.
dirección: Es la dirección IP del router del próximo salto.
interfaz: es el nombre de la interfaz que debe usarse para llegar a le red de destino.
distancia: Es un parámetro opcional, que define la distancia administrativa.
permanent: un parámetro opcional que especifica que la ruta no debe se eliminada, aunque la interfaz deje de estar activa.

Es necesario configurar una ruta estática en sentido inverso para conseguir una comunicación en ambas direcciones.

La ruta predeterminada:

Es un tipo especial de ruta estática que se utiliza cuando no se conoce una ruta hasta un destino determinado, o cuando no es posible almacenar en la tabla de enrutamiento la información relativa a todas las rutas posibles.

APRENDIZAJE DINÁMICO DE RUTAS MEDIANTE PROTOCOLOS DE ENRUTAMIENTO

Con rutas estáticas, el administrador a de volver a configurar todos los routers para ajustarlos cuando se produce un cambio en la red.

El enrutamiento dinámico se apoyo en un protocolo que se encarga de difundir y recopilar conocimientos.

Un protocolo de enrutamiento define el conjunto de reglas que ha de usar el router para comunicarse con los routers vecinos(el protocolo de enrutamiento determina las rutas y mantiene las tablas de enrutamiento).

Un protocolo de enrutamiento es un protocolo de capa de red que intercepta los paquetes en tránsito para aprender y mantener la tabla de enrutamiento.

En cambio los protocolos enrutados, como TCP/IP e IPX, definen el formato y uso de los campos de un paquete con el fin de proporcionar un mecanismo de transporte para él tráfico entre usuarios.

En cuanto el protocolo de enrutamiento determina una ruta valida entre routers, el router puede poner en marcha un protocolo enrutado.

Los protocolos de enrutamiento describen las siguiente información:

- Como han de comunicarse las actualizaciones.
- Que conocimiento ha de comunicarse.
- Cuando se ha de comunicar el conocimiento.
- Como localizar los destinatarios de las actualizaciones..

Hay dos clases de protocolos de enrutamiento:

Protocolos de gateway interior (IGP)

Se usan para intercambiar información de enrutamiento dentro de un sistema autónomo. (RIP, IGRP)

Protocolos de gateway exterior (EGP)

Se usan para intercambiar información de enrutamiento entre sistemas autónomos. (BGP)

Un sistema autónomo es u conjunto de redes bajo un dominio administrativo común.

Los números de sistemas autónomos en Europa los asigna (RIPE-NIC)

RIPE-NIC = Reseaux IP Europeennes-Network Información Center.

El uso de números de sistema autónomos asignados por RIPE, solo es necesario si el sistema utiliza algún BGP, o una red publica como Internet.

CONFIGURACIÓN DEL ENRUTAMIENTO IP

La asignación de una dirección IP única a cada uno de los dispositivos de red, es necesaria pero no suficiente, para permitirles comunicarse entre ellos. Los dispositivos de una red IP también deben conocer la ruta a otros dispositivos de la misma red autónoma o de Internet para enviar paquetes de datos entre ellos. En lugar de que cada dispositivo de la red tenga una lista completa de los restantes dispositivos y donde se encuentran en la red, el router actúa como una especie de guardia urbano, realizando dos funciones en la red IP.

1° El router recibe paquetes de una estación, determina la ruta óptima al destino y a continuación, coloca el paquete en el siguiente segmento de LAN o de WAN que lleva a ese destino. Este proceso se puede repetir varias veces a medida que un paquete de datos se mueve de un router al siguiente en una intranet compleja o en la propia Internet. Este proceso se describe como enrutamiento o switching de paquetes.

2° Los routers deben saber donde esta la otra red IP y las restantes subredes, ambas dentro de la misma red autónoma y fuera de dicha red(como dentro de Internet).

Para determinar donde están las restantes redes, los routers emplean una tabla de enrutamiento, que crean los algoritmos y protocolos de enrutamiento.
Los protocolos de enrutamiento pueden ser de naturaleza estática o dinámica.

En los protocolos estáticos, el administrador configura manualmente las tablas de enrutamiento.

Los protocolos estáticos no son robustos, ya que no son capaces de reaccionar a los cambios de la red y hay que volver a configurarlos manualmente para cada cambio. Los protocolos dinámicos confían en los routers para revelar información sobre las diferentes redes y subredes con las que están conectados.

CONFIGURACIÓN DE LOS COMANDOS DE ENRUTAMIENTO DE IP

Para activar el enrutamiento IP se utiliza el comando de configuración global de IOS **ip routing**. Por defecto, el software IOS está configurado para el enrutamiento IP en dispositivos tales como los routers independientes.

Si se ha desactivado el enrutamiento IP en algún dispositivo, hay que volverlo a activar antes de conmutar los paquetes y activar los protocolos de enrutamiento.

Por defecto, algunos dispositivos router integrados de Cisco no tienen activado el enrutamiento IP.

Hay que utilizar en ellas el comando **ip routing** para llevar a cabo los procesos de switching de paquetes y de protocolo de enrutamiento.

```
Router#configure
Router(config)#ip routing
Router(config)#Ctrl+Z
```

Tras activar el enrutamiento IP, se puede crear la tabla de enrutamiento que se va a utilizar para conmutar paquetes. **De forma predeterminada, cuando una dirección IP se encuentra configurada en un interfaz y ésta se encuentra en estado operativo, la información de la red para la interfaz se sitúa en la tabla de enrutamiento. Todas las interfaces operativas conectadas al router se sitúan en la tabla de enrutamiento.** Si sólo hay un router en la red, éste tiene información sobre todas las redes o subredes diferentes y no hay necesidad de configurar un enrutamiento estático o dinámico. Sólo en el caso de que existan dos o más routers en la red se necesitan entradas de tabla de enrutamiento estáticas o dinámicas.

Para ver la tabla de enrutamiento IP se utiliza el comando ejecutable de IOS **show ip route**. Cuando se introduce el comando sin parámetros, aparece toda la tabla de enrutamiento.

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

El comando **show ip route** es la herramienta clave que se utiliza para determinar la ruta que sigue los paquetes a través de la red. La primera sección de la salida es la leyenda de la primera columna de la propia tabla.

Indica de donde se derivó la ruta.

El gateway de ultimo recurso es la dirección de red del router al que se deberán enviar los paquetes destinados al exterior de la red cuando no haya ninguna información de enrutamiento específica relativa a cómo llegar al destino.

La ultima sección de la salida por pantalla es la propia tabla de enrutamiento.

Aparecen todos los números de red asociados con las direcciones IP que se introdujeron en las respectivas interfaces, junto con la máscara de red de computo de bits y el nombre de la interfaz asociada.

Es importante darse cuenta de que son las direcciones de red y de subred, no las direcciones IP de cada uno de los dispositivos, las que aparecen en la tabla de enrutamiento.

El comando **show ip route** también tiene parámetros opcionales que se pueden utilizar para solicitar solamente determinados tipos de rutas.

Show ip route connected muestra solamente las rutas que se conozcan de interfaces en funcionamiento conectadas directamente.

Show ip route static sólo muestra los routers derivados de comandos de ruta de red configurados manualmente.
Si se escribe una dirección de red específica como parámetro del comando, sólo aparecerá la información de dicha ruta específica.

CONFIGURACION DEL ENRUTAMIENTO ESTÁTICO

Situaciones en las que se aconsejan las rutas estáticas:

- Un circuito de datos es especialmente poco fiable y deja de funcionar constantemente. En estas circunstancias, un protocolo de enrutamiento dinámico podrá producir demasiada inestabilidad, mientras que las rutas estáticas no cambian.

- Existe una sola conexión con un solo ISP. En lugar de conocer todas las rutas globales de Internet, se utiliza una sola ruta estática.

- Se puede acceder a una red a través de una conexión de acceso telefónico. Dicha red no puede proporcionar las actualizaciones constantes que requieren un protocolo de enrutamiento dinámico.

- Un cliente o cualquier otra red vinculada no desean intercambiar información de enrutamiento dinámico. Se puede utilizar una ruta estática para proporcionar información a cerca de la disponibilidad de dicha red.

La configuración de las rutas estáticas se realiza a través del comando de configuración global de IOS **ip rute**. El comando utiliza varios parámetros, entre los que se incluyen la dirección de red y la máscara de red asociada, así como información acerca del lugar al que deberían enviarse los paquetes destinados para dicha red.

La información de destino puede adoptar una de las siguientes formas:

- Una dirección IP específica del siguiente router de la ruta.
- La dirección de red de otra ruta de la tabla de enrutamiento a la que deben reenviarse los paquetes.

Una interfaz conectada directamente en la que se encuentra la red de destino.

Router#**configure**
Router(config)#**ip route[dirección IP de destino][máscara subred de IP destino][IP del primer salto por el que ha de pasar para ir a la IP de destino]**
Router(config)#**Ctrl+Z**

Nota_
La especificación de una interfaz como destino para una ruta estática es uno de los principales errores de configuración que se realizan al utilizar el comando ip route.
Algunos administradores creen por error que los paquetes se reenvían correctamente al siguiente router de la ruta simplemente apuntando la ruta hacia una interfaz específica.
Los paquetes se reenvían al router del próximo salto solamente si se especifica la dirección IP del mismo o se especifica otra ruta de red que atraviese el router del próximo salto.

Ejemplo de como se específica una interfaz conectada directamente como destino del comando **ip route**.

```
Router#configure
Router(config)#ip route[dirección IP destino][máscara subred][interfaz conectado directamente]
Router(config)#Ctrl+Z
```

Cuando se buscan las redes del router y la de destino en la tabla de enrutamiento el comportamiento predeterminado del router coincide con la pareja dirección de red/máscara de red más específica de la clase de red de la dirección IP de destino.

Si el paquete tiene varias rutas para el mismo destino el paquete se envía por la ruta más específica.

CONFIGURACIÓN DE ENRUTAMIENTO SIN CLASE

Por defecto, el router funciona en modo con clase. Para que un router funcione sin clase y haga coincidir la dirección IP de destino con la dirección IP de este CIDR, hay que configurar previamente el comando de configuración global de IOS **ip classless**.

```
Router#configure
Router(config)#ip classless
Router(config)#Ctrl+Z
```

CONFIGURACIÓN DE PROTOCOLOS DE ENRUTAMIENTO DINAMICO.

Los protocolos de enrutamiento dinámico se configuran en un router para poder describir y administrar dinámicamente las rutas disponibles en la red.

Para habilitar un protocolo de enrutamiento dinámico, se han de realizar las siguientes tares:

- Seleccionar un protocolo de enrutamiento.
- Seleccionar las redes IP a enrutar.

También se han de asignar direcciones de red/subred y las máscaras de subred apropiadas a las distintas interfaces.

El enrutamiento dinámico utiliza difusiones y multidifusiones para comunicares con otros routers.

El comando **router** es el encargado de iniciar el proceso de enrutamiento.

router(config)#[protocolo][palabra_clave]

Protocolo es RIP, IGRP, OSPF o IGRP.

Palabra clave se refiere al sistema autónomo que se usará con los protocolos que requieran este tipo de sistemas, como IGRP.

Es necesario también el comando **network**, ya que permite que el proceso de enrutamiento determine las interfaces que participaran en el envío y recepción de actualizaciones de enrutamiento. El comando **network** indica el protocolo de enrutamiento en todas las interfaces, de un router que tenga direcciones IP dentro del ámbito de redes especificado.

El comando **network** permite, además que el router anuncie esa red a otros routers.

router(config-router)#network[número de red]

Donde el parámetro número de red especifica una red conectada directamente.

El parámetro número de red para RIP e IGRP debe estar basado en la clase principal de números de red y no en números de subred o direcciones individuales. El número de res debe identificar también una red a la que el router este conectado físicamente.

Una vez el protocolo y elegidas las redes ha anunciar, el router comienza a aprender dinámicamente las redes y rutas disponibles en la interconexión de redes.

CONFIGURACIÓN DE LAS RUTAS RESUMEN Y LAS PREDETERMINADAS

Mediante el uso de las rutas resumen y las rutas de red predeterminadas, los routers pueden obtener información sobre la disponibilidad. Tanto las rutas resumen como las predeterminadas proporcionan información adicional de la ruta cuando ninguna de las rutas coincide específicamente con un dirección IP.

Las rutas resumen proporcionan información de accesibilidad dentro de un espacio de direcciones determinado. La ruta resumen, que normalmente sigue a los limites de la red con clase, se suelen utilizar para proporcionar información predeterminada de accesibilidad acerca de las subredes que no se encuentran específicamente en la tablas de enrutamiento, pero que existen en la Intranet.

Si hubiera una ruta resumen en la tabla de enrutamiento, el paquete se reenviará desde la interfaz hacia el destino de próximo salto para la ruta resumen.

La ruta resumen suele apuntar a otra ruta de subred de la Intranet, pero también puede apuntar a una dirección IP específica del próximo salto. En cualquier caso, el objetivo del router resumen es dirigir los paquetes hacia otros routers de la Intranet que tengan un información de enrutamiento más completa. La ruta resumen se puede configurar utilizando los comandos de configuración global de IOS **ip default-network** o **ip route**.

Si se utiliza el comando **ip default-network** una subred no conectada que existe en la Intranet se introduce como parámetro en el comando. Si se utiliza el comando **ip route**, la ruta resumen, la máscara de red y la subred no conectada se introducen como parámetros del comando.

Router#**configure**
Router(config)#**ip default-network[dirección IP de la subred no conectada que se utiliza para la accesibilidad predeterminada]**
Router(config)#**Ctrl+Z**
Router(config)#**ip route[dirección IP ruta resumen][máscara][dirección IP de la subred no conectada que se utiliza para la accesibilidad predeterminada]**
Router(config)# **Ctrl+Z**

Una vez configurada, la ruta resumen aparece en la tabla de enrutamiento como la ruta de red menos específica como una máscara de recuento de bits más pequeña que las restantes rutas de red y de subred de la tabla.

Nota_
Si la subred conectada se encuentra dentro del mismo espacio de direcciones de la red con clase de una interfaz conectada directamente al router, el software IOS sustituye el comando **ip default-network** por la versión de la ruta resumen del comando ip route.

El concepto básico de la ruta predeterminada es que si un router no tiene información de enrutamiento específica para un destino, utilizará la ruta predeterminada a la red específica donde haya routers con información más completa. Aunque la ruta predeterminada es parecida a la ruta resumen, se utiliza para distinguir paquetes a destinos IP que están fuera de la Intranet autónoma y de los límites de las direcciones con clase de una entidad determinada.

Métodos para configurar una red predeterminada utilizando el software IOS:

- Configurar una red predeterminada utilizando una ruta externa conocida dinámicamente.
- Configurar una red predeterminada utilizando una ruta externa configurada estáticamente.
- Configurar una red predeterminada utilizando la dirección reservada 0.0.0.0.

La principal diferencia entre los distintos métodos de configuración de redes predeterminadas es si se conoce algún tipo de información de enrutamiento dinámico de un origen externo, sólo hay que indicar que una de ellas es la red predeterminada, para lo que se utiliza el comando de configuración global de IOS **ip default-network**.

El parámetro de este comando es una ruta que tiene las siguientes características:

Existe en una tabla de enrutamiento, no esta conectada al router que se configura y se encuentra fuera del espacio de direcciones con clase configurado en cualquiera de las interfaces del router.

```
Router#configure
Router(config)#ip default-network[dirección IP]
Router(config)#Ctrl+Z
```

Una vez configurado el router muestra que ha aceptado esta red como predeterminada y que se puede tener acceso a la ruta señalándola como el **gateway** de último recurso de la salida de show ip route. El router coloca un asterisco junto a la ruta para indicar que es candidata para la red predeterminada, ya que se pueden configurar varias redes predeterminadas.

Si el enrutamiento dinámico no se intercambia con un proveedor externo, es posible utilizar una ruta estática para apuntar a la dirección de red externa que se utiliza como predeterminada.

El ultimo método de configuración de redes predeterminadas implica la instalación de una ruta estática en una dirección de red especial, a saber 0.0.0.0.

Esta dirección se considera reservada. En los entornos UNIX y RIP indica la ruta a todos los destinos IP desconocidos.

En el software IOS del router, la dirección de red 0.0.0.0 es la dirección de red menos especifica. Con su mascara de red implícita de 0.0.0.0, o 0 bits, esta ruta coincide con cualquier destino IP fuera de las direcciones con clase. Si se configura el comando **ip classless**, la ruta coincide con cualquier dirección de los destinos IP desconocidos tanto dentro como fuera del espacio de direcciones con clase.

Nota_

Si el comando **ip classless** no esta configurado y no se conocen las rutas a los destinos IP de dentro y fuera de la Intranet, hay que configurar tanto la ruta resumen con clase como la ruta de red predeterminada. Este requisito se deriva de la asunción de que todos los routers de una dirección IP con clase tienen un conocimiento completo de todas las subredes de dicho espacio de direcciones. Cuando se trabaja en el **ip classless** mode, la ruta predeterminada simple a la red 0.0.0.0/0 es suficiente como valor predeterminado tanto para los destinos de las subredes internas como de las redes externas ya que une todos los destinos IP desconocidos.

Cuando configure una ruta de red predeterminada, siga estas directrices importantes:

- Si la información de enrutamiento dinámico no se intercambia con la entidad externa, como un IPS, el uso de una ruta estática a 0.0.0.0/0 suele ser la forma mas fácil de generar una ruta predeterminada.

- Si la información de enrutamiento dinámico no se intercambia con uno o varios IPS, el uso del comando **ip default-network** es la forma mas apropiada de designar una o varias rutas de red predeterminadas posibles.

- Es aceptable configurar varios routers en la Intranet con el comando **ip default-network** para indicar que una ruta coincida dinámicamente es la predeterminada. No es apropiado configurar mas de un router de la Intranet con una ruta predeterminada a 0.0.0.0/0 a menos que dicho router tenga una conexión a Internet a través de un ISP. Si lo hace puede provocar que los routers sin conectividad con destinos desconocidos se envíen paquetes a ellos mismos, con lo que se produce una imposibilidad de acceso. La excepción es aquellos routers que no intercambian la información de enrutamiento dinámico o que tienen solamente conexiones ocasionales con la Intranet a través de medios tales como RDSI o SVC de Frame Relay.

- Los routers que no intercambian información de enrutamiento dinámico o que se encuentran en conexiones de acceso telefónico, como RDSI o SVC de Frame Relay, deben configurarse como una ruta predeterminada o a 0.0.0.0/0 como ya se ha indicado.

- Si una Intranet no está conectada a ninguna red externa, como Internet, la configuración de red predeterminada debe colocarse en uno o varios routers que se encuentren en el núcleo de la red y que tengan toda la topología de enrutamiento de red de la Intranet específica.

Sugerencia_

Si una red predeterminada se configura utilizando una ruta estática a 0.0.0.0/0 y el router funciona en modo IP sin clase a través del comando **ip classless**, es muy fácil crear un bucle de enrutamiento entre un ISP y la red si no están asignadas todas las direcciones de red. Si dicho bucle se produce en muchos paquetes, el resultado puede ser un consumo innecesario del ancho de banda de conexión a Internet y muchas congestiones a causa de que un gran número de usuarios intentan acceder a Internet.

Para evitar dicho bucle, hay que proporcionar una ruta resumen del espacio de direcciones de la red que descarte los paquetes dirigidos a direcciones IP no asignadas del espacio de direcciones de la red. Para lograrlo defina la interfaz no existente **Null0** como destino de una ruta. Una ruta resumen para la red que descartaría los paquetes a los destinos no asignados sería la ruta [dirección IP][máscara]Null0. Esta ruta se instalaría en el router de conexión a Internet, que es el ultimo router en recibir los paquetes antes de que se reenvíen al ISP.

ASIGNACION DE UNA RUTA PREDETERMINADA A UNA SUBRED DESCONOCIDA DE UNA RED CONECTADA DIRECTAMENTE.

Un router asume por omisión que todas las subredes de una red conectada directamente deben hallarse en la tabla de enrutamiento IP. Si se recibe un paquete con una dirección de destino correspondiente a una subred desconocida de alguna red conectada directamente, el router supondrá que dicha subred no existe y descartará el paquete. Este comportamiento se mantiene aunque la tabla de enrutamiento IP contenga una ruta predeterminada.

Con **ip classless** configurada, si se recibe un paquete con una dirección de destino correspondiente a una subred de una red conectada directamente, el router la asignará a la ruta predeterminada y la reenviara al siguiente punto de salto especificado en la ruta predeterminada.

no ip classless los paquetes con dirección de destino que apunten a subredes desconocidas de una red conectada directamente son descartados.

VERIFICACIÓN DE LA CONFIGURACIÓN DEL ENRUTAMIENTO IP

El principal comando para verificar la configuración del enrutamiento IP es el comando ejecutable de IOS **show ip route**. Es la herramienta que se utiliza para ver el estado de la tabla de enrutamiento IP. Este comando le muestra si las rutas configuradas o que se deben conocer están presentes en el router en el momento actual.

La salida del comando, le proporciona la información siguiente:

- Una lista de todas las rutas y máscaras de red que hay actualmente en la tabla de enrutamiento.
- La dirección IP del siguiente nodo y la interfaz de salida para dichas rutas(en el caso de rutas directamente conectadas, sólo se ofrece la interfaz de salida).
- Si la ruta se conoce dinámicamente, también se refleja el tiempo(en segundos) que la ruta ha estado en la tabla o el tiempo transcurrido desde la última actualización, dependiendo del protocolo de enrutamiento.

La distancia administrativa y la métrica del protocolo de enrutamiento de todas las rutas menos las conectadas directamente. La distancia administrativa es el número a la izquierda de la barra que aparece entre corchetes y que sigue a la ruta de red y la mascara de cuenta de bits. L métrica del protocolo de enrutamiento es el número a la derecha de la barra que aparece entre corchetes.

La distancia administrativa es un valor numérico que representa la fiabilidad del origen de la actualización del enrutamiento. Cada tipo de ruta y de protocolo de enrutamiento tiene asignado una distancia administrativa determinada. Cuanto más abajo sea dicho valor, más fiable es el origen.

DISTANCIA ADMINISTRATIVA

Es posible utilizar varios protocolos de enrutamiento y rutas estáticas al mismo tiempo.

Si existen varias fuentes de enrutamiento que proporcionan información común, se utiliza un valor de distancia administrativa para valorar la fiabilidad de cada fuente de enrutamiento y averiguar cual es más digna de confianza.

La especificación de valores administrativos permite al software IOS discriminar entre distintas fuentes de información de enrutamiento.

Para cada red aprendida, IOS selecciona la ruta a partir de la fuente de enrutamiento que tenga menor distancia administrativa.

Una distancia administrativa es un valor entre 0 y 255.

La distancia administrativa menor, tiene una probabilidad mayor de ser usada.

DISTANCIAS ADMINISTRATIVAS PREDETERMINADAS DEL SOFTWARE IOS ACTUAL.

La métrica del protocolo de enrutamiento es un número que se utiliza para clasificar las rutas por preferencia cuando existe más de una ruta al mismo destino.

ORIGEN DE RUTA	DISTANCIA PREDETERMINA
Interfaz conectada	0
Ruta estática	1
Resumen de ruta IGRP mejorado	5
BGP externo	20
IGRP mejorado interno	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
BGP interno	200
Desconocido	255

La métrica suele ser un número compuesto que refleja las diferencias características de la ruta, como la longitud y el coste de la ruta. Cada uno de los diferentes protocolos de enrutamiento dinámico posee un algoritmo diferente para calcular la métrica.

Otra herramienta que le ofrece un vistazo rápido del estado de la tabla de enrutamiento es el comando ejecutable de IOS **show ip mask**. Si se da una dirección de red como parámetro, este comando genera una lista de las máscaras que se han aplicado a una determinada dirección de red, así como el número de rutas que tiene cada una de ellas.

Este comando resulta muy practico para identificar los errores de direccionamiento y los de configuración de rutas estáticas, ya que resalta las máscaras de red que aparecen de modo inesperado en la tabla de enrutamiento.

Router#**show ip maks[dirección IP]**

Una gran mayoría de los protocolos de enrutamiento dinámico envía actualizaciones automáticamente de la información de enrutamiento que contienen los routers.

La información incluye actualizaciones para agregar o suprimir rutas de la tabla de enrutamiento y mantener actualizadas las que se encuentran en la tabla. No obstante, es posible eliminar una entrada determinada de la tabla de enrutamiento o todo su contenido manualmente.

También se puede actualizar una determinada ruta o toda la tabla de enrutamiento con el propósito de depurarla. Puede utilizar el comando ejecutable de IOS **clear ip route** para eliminar una ruta específica o todo el contenido de la tabla de enrutamiento, o una pareja de dirección y máscara de red, que logra la eliminación de esa ruta específicamente.

Se recomienda cautela a la hora de decidir la eliminación de la tabla de enrutamiento completa. La actualización de la información contenida en la tabla requiere un tiempo que oscila entre unos segundos y varios minutos. Durante este intervalo, puede darse una falta de conexión en los paquetes que progresan por el router y hacia él por medio de una sesión de terminal virtual. Asimismo, la supresión del contenido de la tabla puede provocar una utilización excesiva de la CPU, dependiendo del protocolo de enrutamiento dinámico que esté en uso y del tamaño de la tabla de enrutamiento.

Router#**clear ip route***

Router#**clear ip route[dirección IP][máscara]**

DISTANCIA ADMINISTRATIVA

Es posible utilizar varios protocolos de enrutamiento y rutas estáticas al mismo tiempo.

Si existen varias fuentes de enrutamiento que proporcionan información común, se utiliza un valor de distancia administrativa para valorar la fiabilidad de cada fuente de enrutamiento y averiguar cual es más digna de confianza.

La especificación de valores administrativos permite al software IOS discriminar entre distintas fuentes de información de enrutamiento.

Para cada red aprendida, IOS selecciona la ruta a partir de la fuente de enrutamiento que tenga menor distancia administrativa.

Una distancia administrativa es un valor entre 0 y 255.

La distancia administrativa menor, tiene una probabilidad mayor de ser usada.

Valores de distancia administrativa predeterminados:

Interfaz conectada	0
Dirección de ruta estática	1
EIGRP	90
IGRP	100
OSPF	110
RIP	120
EIGRP externo	170
Desconocido/No fiable	255(No será usado para pasar trafico).

Dentro de un sistema autónomo, la mayoría de los algoritmos de enrutamiento IGP pueden ser clasificados con alguno de los tipos siguientes:

VECTOR DE DISTANCIA:

El enrutamiento basado en vector de distancia determina la dirección (vector) y la distancia a cualquier enlace de la interconexión. (RIP, IGRP)

ESTADO DE ENLACE:

El sistema de estado de enlace, recrea la topología exacta de todo el interconexionado de redes para el calculo de rutas.(OSPF, NLSP)

HÍBRIDO EQUILIBRADO:

El esquema híbrido equilibrado combina aspectos de los algoritmos de estado de enlace y de vector de distancia. (EIGRP)

PROTOCOLOS DE ENRUTAMIENTO POR VECTOR DE DISTANCIA.

Los algoritmos de enrutamiento basados en vectores, pasan copias periódicas de una tabla de enrutamiento de un router a otro y acumulan vectores de distancia. (Distancia es una medida de longitud, mientras que vector significa una dirección).

Las actualizaciones regulares entre routers comunican los cambios en la topología.

Cada protocolo de enrutamiento basado en vectores de distancia utilizan un algoritmo distinto para determinar la ruta optima.

El algoritmo genera un número, denominado métrica de ruta, para cada ruta existente a través de la red. Normalmente cuanto menor es este valor, mejor es la ruta.

Las métricas pueden calcularse basándose en un sola o en múltiples características de la ruta.

LAS MÉTRICAS USADAS HABITUALMENTE POR LOS ROUTERS SON:

Número de saltos:
Número de routers por los que pasará un paquete.

Pulsos:
Retraso en un enlace de datos usando pulsos de reloj de PC IBM(msg)

Coste:
Valor arbitrario, basado generalmente en el ancho de banda, el coste económico u otra medida, que puede ser asignado por un administrador de red.

Ancho de banda:
Capacidad de datos de un enlace. Por ejemplo, un enlace Ethernet de 10Mb será preferible normalmente a una línea dedicada de 64Kb.

Retraso:
Cantidad de actividad existente en un recurso de red, como un router o un enlace.

Carga:
Cantidad de actividad existente en un recurso de red, como un router o un enlace.

Fiabilidad:
Normalmente, se refiere al valor de errores de bits de cada enlace de red.

MTU:
Unidad máxima de transmisión. Longitud máxima de trama en octetos que puede ser aceptada por todos los enlaces de la ruta.

BUCLE DE ENRUTAMIENTO.

Resolución de bucles de enrutamiento.

MÉTRICA MÁXIMA:

El protocolo de enrutamiento permite la repetición del bucle de enrutamiento hasta que la métrica exceda del valor máximo permitido.

HORIZONTE DIVIDIDO:

Nunca resulta útil volver a enviar información acerca de una ruta a la dirección de donde ha venido la actualización original.

ENVENENAMIENTO DE RUTAS:

El router crea una entrada en la tabla donde guarda el estado coherente de la red en tanto que otros routers convergen gradualmente y de forma correcta después de un cambio en la topología.
La actualización inversa es una circunstancia especifica esencial del horizonte dividido.
El objetivo es asegurarse de que todos los routers del segmento hayan recibido información acerca de la ruta envenenada.

TEMPORIZADORES:

Los temporizadores hacen que los routers no apliquen ningún cambio que pudiera afectar a las rutas durante un periodo de tiempo determinado. Dicho periodo se calcula generalmente de forma que sea mayor el espacio de tiempo requerido para actualizar toda la red tras un cambio de enrutamiento.

ACTUALIZACIONES DESENCADENADAS:

Es una nueva tabla de encaminamiento que se envía de forma inmediata, en respuestas a un cambio.

TEMPORIZACIONES Y ACTUALIZACIONES DESENCADENADAS:

El temporizador establece que cuando una ruta no es valida no será aceptada una nueva ruta con una métrica igual o peor para el mismo destino en un periodo de tiempo determinado, la actualización desencadenada tiene tiempo suficiente para propagarse a toda la red.

PROTOCOLOS DE ENRUTAMIENTO DE ESTADO DE ENLACE

Los protocolos de estado de enlace constituyen tablas de enrutamiento basándose en una base de datos de la topología. Esta base de datos se elabora a partir de paquetes de estado de enlace que se pasan entre todos los routers para describir el estado de una red.

El algoritmo de la ruta más corta primero usa la base de datos para construir la tabla de enrutamiento.

El algoritmo de la ruta más corta primero usa la base de datos para construir la tabla de enrutamiento.

El enrutamiento por estado de enlace, utiliza paquetes de estado de enlace(LSP), una base de datos topología, el algoritmo SPF, el árbol SPF resultantes y por ultimo, una tabla de enrutamiento con las rutas y puertos de cada red.

- Los protocolos de estado de enlace solo envían actualizaciones cuando hay cambios en la topología.
- Las actualizaciones periódicas son menos frecuentes que en los protocolos por vector de distancia.
- Las redes que ejecutan protocolos de enrutamiento por estado de enlace pueden ser segmentadas en distintas áreas jerárquicamente organizadas, limitando así el alcance de los cambios de rutas.
- Las redes que ejecutan protocolos de enrutamiento por estado de enlace soportan direccionamiento sin clase.
- Las redes con protocolos de enrutamiento por estado de enlace soportan resúmenes.

CONFIGURACION DE LOS PROTOCOLOS DE ENRUTAMIENTO IP

Diseñar redes que utilicen exclusivamente rutas estáticas, sería tedioso administrarlas y no responderían bien a las interrupciones y a los cambios de topología que suelen suceder con cierta frecuencia. Para responder a estos problemas se desarrollaron los protocolos de enrutamiento dinámico. Los protocolos de enrutamiento dinámico son algoritmos que permiten que los routers publiquen, o anuncien, la existencia de la información de ruta de red IP necesaria para crear la tabla de enrutamiento. Dichos algoritmos también determinan el criterio de selección de la ruta que sigue el paquete cuando se le presenta al router esperando una decisión de switching. Los objetivos del protocolo de enrutamiento consisten en proporcionar al usuario la posibilidad de seleccionar la ruta idónea en la red, reaccionar con rapidez a los cambios de la misma y realizar dichas tareas de la manera más sencilla y con la menor sobrecarga del router posible.

Los protocolos de enrutamiento se dividen en dos categorías principales: protocolos de gateway interior(Interior Gateway Protocols, IGP) y protocolos de gateway exterior(Exterior Gateway Protocols, EGP). Los protocolos IGP están diseñados para intercambiar información sobre la red y las subredes entre los routers de un sistema autónomo; es decir, entre routers que ejecutan un protocolo de enrutamiento común en el marco de un dominio administrativo. Los protocolos EGP están diseñados para intercambiar exclusivamente información sobre la red entre routers que pertenezcan a diferentes sistemas independientes.

El protocolo EGP con mayor utilización en la actualidad es el protocolo de gateway fronterizo versión 4(Boarder Gateway Protocol 4, BGP-4). Es el protocolo de enrutamiento predominante utilizado para intercambiar información entre empresas, proveedores de servicios de red en Internet.

Entre los protocolos IGP; los dos atributos principales que diferencian uno de otro son la metodología de propagación y el hecho de que sean con o sin clase. Los dos métodos más comunes de propagación son el vector de distancia y el estado de enlace.

En el método de vector de distancia, todos los routers envían las tablas de enrutamiento, completa o parcialmente, a los routers vecinos en mensajes de actualización de intervalos de tiempo regulares. S medida que la información de enrutamiento se va repartiendo por la red, los routers pueden calcular la distancia a todas las redes y subredes de la Intranet.

Con el método de estado de enlace, cada router envía información de conexión local completa a todos los demás routers de la Intranet. Como cada router recibe toda la información de conexión local , puede crear una imagen completa de la Intranet al ejecutar un complejo algoritmo llamado Primero la ruta más corta(Shortest Path First, SPF) en contraste con la información de conexión.

Los protocolos IGP también se diferencian por ser con o sin clase. Los protocolos de enrutamiento con clase no poseen la capacidad de intercambiar información de máscara de red entre los diferentes routers. Por esa razón, estos protocolos deben asumir que se ha aplicado una máscara de red o subred uniforme al espacio de direcciones común de la red.

Esta limitación prohíbe el uso de máscaras de subred de longitud variable(VLSM), por lo que la utilización del espacio de direcciones de la red no alcanza un nivel óptimo. Asimismo no se puede pasar entre los routers la información de máscara de red, de manera que la información de las direcciones de red se deben resumir en los limites de las direcciones de red con clase. Los protocolos de enrutamiento con clase son entre otros, el protocolo de información de enrutamiento(Routing Information Protocol, RIP) versión 1 y el protocolo de enrutamiento de gateway interior(Interior Gateway Protocol, IGRP) de Cisco Systems.

Los protocolos de enrutamiento sin clase se distinguen de los protocolos con clase por su capacidad para llevar información de máscara de red junto a la información de ruta de red. Por esa razón, los protocolos sin clase pueden soportar varias máscaras de subred dentro del espacio de direcciones de una red y por ello, pueden implementar VLSM. Al transportar la información de máscara de red, los protocolos sin clase también pueden implementar direccionamiento de superred o bloques CIDR.

Además, los protocolos sin clase no requieren el resumen de las subredes en los principales límites de red, que sí necesitan los protocolos con clase(aunque el comportamiento predeterminado sea crear los resúmenes). Se puede propagar información detallada de la subred desde el espacio principal de direcciones de red a otro, porque las máscaras de red proporcionan información específica sobre las subredes disponibles. La capacidad del enrutamiento sin clase para propagar la información de la subred desde un espacio principal de direcciones de la red a otro facilita la utilización de redes no contiguas. La red no contigua ocurre cuando el espacio principal de direcciones de la red se rompe en dos o más partes debido a un segundo espacio de direcciones de la red. Los protocolos de enrutamiento que se consideran sin clase son RIP versión 2, IGRP mejorado(Enchanced IGRP, EIGRP) de Cisco Systems, IETF Open Shortest Path First(OSPF) y el estándar ISO Intermediate System-to-Intermediate System Interdomain Routing Exchange Protocol(IS-IS).

Muchas variables influyen en el proceso de seleccionar un protocolo de enrutamiento dinámico para su uso en una red.

- **Topología de red.** Algunos protocolos de enrutamiento usan una jerarquía lógica para ampliar y distribuir la información de ruta de la red de manera apropiada. Los protocolos del tipo OSPF e IS-IS requieren el establecimiento de un backbone y áreas lógicas. Estos protocolos pueden exigirle que rediseñe la topología de la red física o que cree un diseño inicial de red para que operen con un rendimiento óptimo.

- **Resumen de ruta y dirección.** En una Intranet grande, el beneficio de reducir el número de entradas en la tabla de enrutamiento supone la reducción de la relativa complejidad de la red, así como la reducción de la carga de los routers. La creación de resúmenes requiere que el protocolo de enrutamiento admita VLSM y que posea la capacidad de propagar información de la máscara de red con las rutas de red. Los protocolos sin clase, como OSPF y EIGRP, son muy adecuados para la creación de resúmenes.

- **Velocidad de convergencia.** Uno de los criterios más importantes es la velocidad con la que un protocolo de enrutamiento identifica la ruta que no esta disponible, selecciona una nueva y propaga la información sobre ésta. Si la red admite aplicaciones de importancia crucial, el administrador se inclinará hacia el protocolo de enrutamiento que posea un velocidad de convergencia mayor.

- Los protocolos de vector de distancia suelen necesitar más tiempo para converger que los de estado de enlace, porque la información sobre la nueva ruta debe pasar de nodo en nodo a cada uno de los routers sucesivos de la Intranet. Los protocolos RIP versión 1 e IGRP suelen ser más lentos al converger que EIGRP y OSPF.

- **Criterio de selección de ruta** A la hora de determinar el protocolo de enrutamiento dinámico adecuado que se debe implementar, es de vital importancia el papel que desempeñan los atributos de la ruta individual que utiliza el protocolo de enrutamiento para crear la métrica de ruta. Cuando las diferentes rutas de la Intranet se compongan de varios tipos de medios LAN y WAN, puede ser desaconsejable un protocolo que dependa estrictamente del número de saltos de router para determinar la selección de la ruta, como es el caso de RIP. RIP considera que el salto de router en un segmento de Fast Ethernet tiene el mismo coste relativo que un salto de router por un enlace WAN de 56 Kbps. Entre otros, los atributos de ruta de red que utilizan los diferentes protocolos para calcular su métrica son la longitud de ruta, la fiabilidad, el retraso, el ancho de banda y la carga.

- **Capacidad de ampliación.** La relativa capacidad de ampliación del protocolo de enrutamiento es muy importante, dependiendo de los tipos de routers que haya en la Intranet y del tamaño de la misma. Los protocolos de vector de distancia consumen menos ciclos de CPU que los protocolos de estado de enlace con sus complejos algoritmos SPF. Los protocolos de estado de enlace consumen menos ancho de banda LAN y WAN que los protocolos de vector de distancia porque sólo se propaga la información sobre cambios, no la tabla de enrutamiento completa.

- **Sencillez de implementación.** Si la red no es excesivamente compleja, resulta más sencillo implementar protocolos que no requieren una reestructuración de la red o topologías muy bien organizadas y diseñadas. Por ejemplo RIP, IGRP y EIGRP no requieren mucha planificación ni organización en la topología para que se puedan ejecutar de manera eficaz. OSPF y IS-IS requieren que se hayan pensado muy cuidadosamente la topología de red y los modelos de direccionamiento antes de su implementación.

- **Seguridad.** Si la red intercambia información IGP con un filial o entre las divisiones de la misma empresa, se debería poder autentificar el origen de la información de enrutamiento. Algunos protocolos como OSPF y EIGRP admiten poderosos métodos de autenticación, como la autenticación de claves MD5.

La selección de un protocolo de enrutamiento para cualquier red depende mucho de los siguientes factores:

- Si se va a agregar un router a la topología de red existente.
- El diseño de la red.
- La presencia de routers y protocolos de enrutamiento ya existentes.
- La experiencia y el grado de familiaridad que tenga el administrador con el enrutamiento TCP/IP.
- La necesidad de intercambiar información de enrutamiento con dispositivos de sistemas finales, como un servidor.

CONFIGURACIÓN DEL PROTOCOLO DE INFORMACIÓN DE ENRUTAMIENTO.

RIP es uno de los protocolos de enrutamiento más antiguos utilizado por dispositivos basados en IP.
Su implementación original fue para el protocolo Xerox PUP a principios de los 80. Gano popularidad cuando se distribuyo con UNÍS como protocolo de enrutamiento para esa implementación TCP/IP.
RIP es un protocolo de vector de distancia que utiliza la cuenta de saltos del router como métrica. La cuenta de saltos máxima de RIP es 15. Cualquier ruta que exceda de los 15 saltos se etiqueta como inalcanzable al establecerse la cuenta de saltos en 16. En RIP la información de enrutamiento se propaga de un router a los otros vecinos por medio de una difusión de IP usando el protocolo UDP y el puerto 520.

El protocolo RIP versión 1 es un protocolo de enrutamiento con clase que no admite la publicación de la información de la máscara de red. El protocolo RIP versión 2 es un protocolo sin clase que admite CIDR, VLSM, resumen de rutas y seguridad mediante texto simple y autenticación MD5.

La configuración del protocolo de enrutamiento RIP consiste en tres pasos básicos: posibilitar que el router ejecute el protocolo RIP, decidir la versión de RIP que se desea ejecutar y configurar las direcciones e interfaces de la red que deben incluirse en las actualizaciones de enrutamiento. Para posibilitar que el router ejecute RIP, se utiliza el comando principal de configuración de IOS **router rip**.

Para seleccionar la versión de RIP que se desea ejecutar, se utiliza el subcomando de configuración de enrutamiento de IOS **versión**.

El comando **versión** adopta un valor de 1 ó 2 para especificar la versión de RIP que se va a utilizar. Si no se especifica la versión, el software IOS adopta como opción predeterminada el envío de RIP versión 1 pero recibe actualizaciones de ambas versiones, 1 y 2.

Se pueden especificar las interfaces y las direcciones de red que se deben incluir en las publicaciones de enrutamiento RIP con el subcomando de configuración de enrutamiento de IOS **network**. Este comando toma como parámetro la dirección de red con clase que se debe incluir en las actualizaciones de enrutamiento. El comando **network** debe utilizarse para identificar sólo aquellas direcciones IP de red que están conectadas directamente con el router que se esta configurando y que deben incluirse en el proceso de enrutamiento RIP.

En estas actualizaciones de enrutamiento sólo se incluyen las interfaces que tienen direcciones IP en la red identificada.

Nota_

Es posible combinar las versiones 1 y 2 de RIP en una misma red, aunque la versión 1 no admite muchas de las funciones de la versión 2. La combinación de ambas versiones puede provocar problemas de interoperabilidad. La omisión de la versión configurada globalmente y la especificación de la versión por interfaz se logra mediante los subcomandos de configuración de interfaz de IOS **ip rip send versión** e **rip recive versión**.

HABILITACIÓN DE RIP

- Es un protocolo de enrutamiento basado en vectores distancia.
- Se utiliza el número de saltos como métrica para la selección de rutas.
- El número máximo de saltos permitido es 15.
- Se difunden actualizaciones de enrutamiento por medio de la tabla de enrutamiento completa cada 30 segundos, por omisión.
- RIP puede realizar equilibrado de carga en un máximo de seis rutas de igual coste (la especificación por omisión es de cuatro rutas).
- RIP-1 requiere que se use una sola máscara de red para cada número de red de clase principal que es anunciado. La máscara es una máscara de subred de longitud fija.
  El estándar RIP-1 no contempla actualizaciones desencadenadas.
- RIP-2 permiten máscaras de subred de longitud variable(VLSM) en la interconexión. (El estándar RIP-2 permite actualizaciones desencadenadas, a diferencia de RIP-1

La definición del número máximo de rutas paralelas permitidas en la tabla de enrutamiento faculta a RIP para llevar a cabo el equilibrado de carga.

El comando **maximum-paths** habilita el equilibrado de carga.

HABILITACIÓN DE IGRP

IGRP es un protocolo de enrutamiento basado en vectores de distancia desarrollado por CISCO, sus características son:

Escalabilidad mejorada:

Enrutamiento en redes más grandes, posee un número máximo predeterminado de 100 saltos, aunque puede ser configurado con hasta 255 saltos.

Métrica sofisticada:

Métrica compuesta que proporciona una mayor flexibilidad en la selección de rutas. Se usa el retraso de interconexión y el ancho de banda y se pueden incluir otros parámetros como la fiabilidad, la carga y la MTU.

Soporte de múltiples rutas:

IGRP puede mantener hasta un máximo de seis rutas de coste diferente entre redes de origen y destino. Se pueden usar varias rutas para aumentar el ancho de banda disponible o para conseguir redundancia de rutas.

IGRP permite actualizaciones desencadenadas.

MÉTRICAS IGRP.

IGRP utiliza una métrica de enrutamiento compuesta.

La ruta que posea la métrica más baja será considerada la ruta óptima.

Las métricas de IGRP están ponderadas mediante constantes desde K hasta K5.

Convierten los vectores de métrica IGRP en cantidades escalables.

Ancho de banda: Valor mínimo de ancho de banda en la ruta.

Retraso: Retraso de interfaz acumulado a lo largo de la ruta.

Fiabilidad: Fiabilidad entre el origen y el destino, determinado por el intercambio de mensajes de actividad.

Carga: Carga de un enlace entre el origen y el destino, medido en bits por segundo.

MTU: Valor de la unidad máxima de transmisión de la ruta.

La fiabilidad y la carga no tienen unidades propias y pueden tomar valores entre 0 y 255. El ancho de banda puede tomar valores que reflejan velocidades desde 1200 bps hasta 106 bps.

El retraso puede ser cualquier valor entre 1 hasta 2×10^{23}

EQUILIBRADO DE CARGA DE COSTE DESIGUAL EN IGRP.

IGRP soporta múltiples rutas entre un origen y un destino, es posible que dos líneas de igual ancho de banda puedan transportar una misma trama de tráfico de forma cooperativa, con conmutación automática a la segunda línea si la primera falla.

El equilibrado de la carga de coste desigual permite distribuir el trafico entre un máximo de seis rutas de distinto coste, para conseguir un mayor rendimiento y fiabilidad.

A la hora de implementar el equilibrado de carga de coste desigual en IGRP se aplican las siguientes reglas generales.

- IGRP puede aceptar hasta seis rutas para una red de destino dada(cuatro es la especificación predeterminada).
- El router del próximo salto en cualquiera de las rutas debe estar más próximo al destino que lo está el router local por su mejor ruta. Esto garantiza la ausencia de bucles de enrutamiento.
- La métrica de la ruta alternativa debe encontrarse en un rango especifico en relación con la métrica local óptima.

PROCESO DE ENRUTAMIENTO IGRP.

IGRP requiere un número de sistema autónomo. Este número de sistema autónomo no tiene que estar registrado. Sin embargo, todos los routers de un sistema autónomo deben usar el mismo número de sistema autónomo.

router(config-router)#router igrp[sistema autónomo]

router(config-router)#network[número de red ip]

EQUIIBRADO / COMPARTICIÓN DE CARGA EN IGRP

IGRP soporta tanto el equilibrado de carga como la comparición de carga.

Utilizar el comando **variance** para configurar el equilibrado de la carga de coste desigual definiendo la diferencia entre la métrica óptima y la peor métrica aceptable.

router(config-router)#variance[multiplicador]

Multiplicador especifica el rango de valores de métrica que serán aceptadas para el equilibrado de la carga.

Puede usar el comando **traffic-share[balanced|min]** para controlar la forma en que debe distribuirse el trafico entre rutas de comparición de carga IGRP.

router(config-router)#traffic-share[balanced|min]

Balanced = El trafico se distribuye proporcionalmente a las relaciones entre las distintas métricas.

Min = Especifica que deben usarse las rutas de coste mínimo.

VERIFICACIÓN DE LA INFORMACIÓN DE ENRUTAMIENTO.

show ip protocols Incluye sistema autónomo, temporizadores de enrutamiento, redes y distancia administrativa.

show ip route Muestra el contenido de la tabla de enrutamiento Ip.

debug ip igrp transactions Muestra información de las transacciones entre redes IGRP.

debug ip igrp events Muestra resumen de la información de enrutamiento IGRP.

CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO DE GATEWAY INTERIOR DE CISCO

IGRP de Cisco es un protocolo de vector de distancia mejorado que fue desarrollado por Cisco Systems e mediados de los 80. Fue diseñado para corregir algunos de los defectos de RIP y para proporcionar un mejor soporte para redes grande con enlaces de diferentes anchos de banda.

IGRP calcula su métrica en base a diferentes atributos de ruta de red que pueden configurar el usuario, como el retraso de res, ancho de banda y el retraso basados en la velocidad y capacidad relativas de la interfaz. Los atributos de carga y fiabilidad se calculan según el rendimiento de la interfaz en la gestión de tráfico real de la red, aunque no están activados de manera predeterminada para las decisiones de enrutamienro de Cisco IOS.

Como RIP, IGRP utiliza publicaciones IP para comunicar la información de enrutamiento a los routers vecinos. No obstante, IGRP está designado como su propio protocolo de capa de transporte. No depende de UDP o TCP para comunicar la información de la ruta de red.(Como IGRP no tiene mecanismos de retroalimentación, funciona de una manera similar a UDP).

IGRP ofrece tres importantes mejoras sobre el protocolo RIP. En primer lugar, la métrica de IGRP puede admitir una red con un número máximo de 255 saltos de router. En segundo lugar, la métrica de IGRP puede distinguir entre los diferentes tipos de medios de conexión y los costes asociados a cada uno de ellos. En tercer lugar, IGRP ofrece una convergencia de funcionalidad envían la información sobre cambios en la red a medida que está disponible, en vez de esperar a las horas programadas con regularidad para la actualización.

La configuración del proceso de enrutamiento IGRP consiste en dos pasos: posibilitar que el router ejecute el protocolo IGRP e identificar las direcciones e interfaces de la red que deben incluirse en las actualizaciones de enrutamiento. Para posibilitar que el router ejecute IGRP se utiliza el comando principal de configuración de IOS **router igrp**. Este comando requiere un parámetro que se conoce como **process-id**(identificador de proceso). El **process-id** puede ser un número entero del 1 al 65535 para distinguirlos. Se pueden ejecutar varios procesos IGRP en un router que interconecte dos divisiones de una compañía que quieran mantener una administración de red independiente entre sí. Todos los routers de una división deben compartir el mismo **process-id** con los otros routers de la división.

Se puede especificar las interfaces y las direcciones de red que se deben incluir en las publicaciones de enrutamiento IGRP con el subcomando de configuración de enrutamiento de IOS **network**. Este comando toma como un parámetro la dirección de red con clase que se debe incluir en las actualizaciones de enrutamiento. El comando **network** debe utilizarse para identificar sólo aquellas direcciones IP de red que están conectadas directamente con el router que se esta configurando y que deben incluirse en el proceso de enrutamiento IGRP. En las actualizaciones de enrutamiento sólo se incluyen las interfaces que tienen direcciones IP en la red identificada.

```
Router#configure terminal
Router(config)#router igrp [process id]
Router(config-router)#newtwork [dirección IP]
Router(config-router)#Ctrl+Z
```

CONFIGURACIÓN DEL PROTOCOLO PRIMERO LA RUTA MÁS CORTA

El grupo de trabajo OSPF del IETF diseño el protocolo Primero la ruta libre más corta(Open Shortest Path First,OSPF) a finales de los 80. Se diseño para cubrir las necesidades de las redes IP, incluyendo VLSM, autenticación de origen de ruta, convergencia rápida, etiquetado de rutas conocidas mediante protocolos de enrutamiento externo y publicaciones de ruta de multidifusión. El protocolo OSPF versión 2, la implementación más actualizada, aparece especificado en la RFC 1583.

OSPF funciona dividiendo una Intranet o un sistema autónomo en unidades jerárquicas de menor tamaño. Cada una de estas áreas se enlaza a un área backbone mediante un router fronterizo. Todos los paquetes direccionados desde una dirección de una estación de trabajo de un área a otra de un área diferente atraviesan el área backbone, independientemente de la existencia de una conexión directa entre las dos áreas.

Aunque es posible el funcionamiento de una red OSPF únicamente con el área backbone, OSPF escala bien cuando la red se subdivide en un número de áreas más pequeñas.

OSPF es un protocolo de enrutamiento por estado de enlace. A diferencia de RIP e IGRP que publican sus rutas sólo a routers vecinos, los routers OSPF envían Publicaciones del estado de enlace(Link-State Advertisment, LSA) a todos los routers pertenecientes al mismo área jerárquica mediante una multidifusión de IP. La LSA contiene información sobre las interfaces conectadas, la métrica utilizada y otros datos adicionales necesarios para calcular las bases de datos de la ruta y la topología de red. Los routers OSPF acumulan información sobre el estado de enlace y ejecutan el algoritmo SPF(que también se conoce con el nombre de su creador, Dijkstra) para calcular la ruta más corta a cada nodo.

Para determinar que interfaces reciben las publicaciones de estado de enlace, los routers ejecutan el protocolo OSPF Hello. Los routers vecinos intercambian mensajes hello para determinar qué otros routers existen en una determinada interfaz y sirven como mensajes de actividad que indican la accesibilidad de dichos routers.

Cuando se detecta un router vecino, se intercambia información de topología OSPF.
Cuando los routers están sincronizados, se dice que han formado una adyacencia.
Las LSA se envían y reciben sólo en adyacencias.

La información de la LSA se transporta en paquetes mediante la capa de transporte OSPF. La capa de transporte OSPF define un proceso fiable de publicación, acuse de recibo y petición para garantizar que la información de la LSA se distribuye adecuadamente a todos los routers de un área. Existen cuatro tipos de LSA. Los tipos más comunes son los que publican información sobre los enlaces de red conectados de un router y los que publican las redes disponibles fuera de las áreas OSPF.

La métrica de enrutamiento de OSPF se calcula como la suma de los OSPF a lo largo de la ruta hasta alcanzar una red. El coste OSPF de un enlace se calcula en base al ancho de banda de la interfaz y es configurable por parte del usuario.

La configuración del proceso de enrutamiento OSPF consiste en dos pasos: posibilitar que el router ejecute el protocolo OSPF e identificar las direcciones e interfaces de la red que deben incluirse en las actualizaciones de enrutamiento y las áreas a las que pertenecen las interfaces.

Para posibilitar que el router ejecute OSPF, se utiliza el comando principal de configuración de IOS **router ospf**. Este comando requiere como parámetro un número entero, o **process-id**, en caso de que se ejecuten varios procesos OSPF en un mismo router. Como en otros protocolos de enrutamiento, es necesario configurar las interfaces y direcciones de red que se incluirán en las publicaciones de enrutamiento OSPF. Además, deben identificarse las áreas OSPF en las que residen las interfaces.

Utilice el subcomando de configuración de enrutamiento de IOS **network area** para identificar las direcciones e interfaces de la red que quieren incluir en OSPF, así como para identificar las áreas a las que pertenecen. Este comando adopta dos parámetros. El primer parámetro es la dirección de red y la máscara wildcard utilizada para compararla con las direcciones IP asignadas a las interfaces. La máscara wildcard es un método para igualar direcciones IP o rangos de éstas. Cuando se aplica la máscara wildcard a la dirección IP de una interfaz y la dirección de red resultante coincide con la dirección de la red en el comando **network area**, la interfaz queda incluida en el proceso de enrutamiento OSPF para el área especificada. El segundo parámetro, que se conoce como **area id**(identificador de área), se utiliza para identificar el área a la que pertenece la interfaz. El **area id** puede ser un número entero o un número decimal con puntos como, por ejemplo, una dirección IP.

```
Router#configure terminal
Router(config)#router ospf [process id]
Router(config-router)#newtwork [dirección IP][máscara wildcard][area id]
Router(config-router)#Ctrl+Z
```

Como en el caso de los protocolos ya presentados, sólo aquellas direcciones e interfaces de red que coincidan con las direcciones de los comandos **network area** quedan incluidas en las actualizaciones de enrutamiento OSPF.

OSFF funciona con el principio de que las LSA pueden ser difundidas a todos los routers de un mismo sistema autónomo. No obstante, muchos medios WAN(como las líneas serie punto a punto, Frame Relay punto a punto y Frame Relay multipunto) no son medios de difusión y no admiten la multidifusión. Sin la capacidad de multidifundir la información de enrutamiento LSA, el administrador de la red tendrá que configurar manualmente las relaciones de adyacencia entre los routers en las interfaces punto a punto y multipunto de la red. No obstante, se pueden eliminar la necesidad de la configuración manual de los routers vecinos. Se suelen dar instrucciones a OSPF para que considere la interfaz punto a punto como un medio de difusión y una interfaz multipunto como una red parcial de difusión. El subcomando de configuración de IOS **ip ospf network** controla el tipo de red a la que OSPF piensa que está conectada la interfaz. Este comando adopta como parámetro una de las siguientes opciones:

- **Broadcast.** Considera el medio como uno de difusión, asumiendo que se pueden transmitir y recibir las multidifusiones.
- **Non-broadcast**. Considera el medio como un medio de no difusión. Esta opción requiere que el administrador configure manualmente las relaciones de adyacencia mediante el subcomando de configuración de enrutamiento de IOS **neighbor**.
- **Point-to-multipoint**. Considera el medio como un medio de difusión parcial. El router del hub(concentrador) de una topología punto a multipunto posee circuitos virtuales a los diversos routers que carecen de conexión directa.

```
Router#configure t
Router(config)#interface serial 0.1 point-to-point
Router(config-int)#ip ospf network broadcast
Router(config-int)#interface serial 1
Router(config-int)#ip ospf network point-to-multipoint
Router(config-int)#Ctrl.+Z
```

A diferencia de los otros protocolos de enrutamiento IGP, OSPF no genera una ruta predeterminada cuando se configura con el comando **ip default-network**. Para OSPF, el router límite de sistema autónomo debe estar configurado manualmente para que se le pueda forzar a generar una ruta predeterminada para el resto del dominio OSPF. El subcomando de configuración de enrutamiento de IOS **ip default-information originate** hace que OSPF genere la ruta predeterminada.

```
Router#configure t
Router(config)#ip default-network [dirección IP]
Router(config-router)#router ospf 25000
Router(config-router)#ip default-information originate
Router(config-router)#Ctrl.+Z
```

CONFIGURACIÓN DEL PROTOCOLO DE ENRUTAMIENTO DE GATEWAY INTERIOR MEJORADO IP DE CISCO.

El protocolo de enrutamiento de gateway interior mejorado (Enchaced Interior Gateway Routing Protocol, EIGRP) es una versión mejorada del protocolo IGRP original desarrollado por Cisco Systems. EIGRP mantiene el mismo algoritmo de vector de distancia y la información de métrica original de IGRP; no obstante, se han mejorado apreciablemente el tiempo de convergencia y los aspectos relativos a la capacidad de ampliación. EIGRP ofrece características que no se encontraban en su antecesor, IGRP como el soporte para VLSM y los resúmenes de ruta arbitrarios.

Además, EIGRP ofrece características que se encuentran en protocolos como OSPF, como las actualizaciones increméntales parciales y un tiempo de convergencia reducido.
EIGRP combina las ventajas de los protocolos de estado de enlace con las de los protocolos de vector de distancia.

Como en el caso del protocolo IGRP, EIGRP publica la información de la tabla de enrutamiento sólo a los routers vecinos.

No obstante, a diferencia de IGRP, estos routers vecinos se descubren por medio de un protocolo Hello sencillo intercambiado por los routers que pertenecen a la misma red física. Una vez descubiertos los routers vecinos, EIGRP utiliza un protocolo de transporte fiable para garantizar la entrega correcta y ordenada de la información y las actualizaciones de la tabla de enrutamiento. Un router hace el seguimiento de sus propias rutas conectadas y, además, de todas las rutas publicas de los routers vecinos. Basándose en esta información, EIGRP puede seleccionar eficaz y rápidamente la ruta de menor coste hasta un destino y garantizar que la ruta no forma parte de un bucle de enrutamiento. Al almacenar la información de enrutamiento de los routers vecinos, el algoritmo puede determinar con mayor rapidez una ruta de sustitución o un sucesor factible en caso de que haya un fallo de enlace o cualquier otro evento de modificación de la topología.

El saludo y la información de enrutamiento EIGRP son transportados mediante el protocolo de transporte EIGRP. El transporte EIGRP define un protocolo fiable de publicación, acuse de recibo y petición para garantizar que el saludo y la información de enrutamiento de distribuyen adecuadamente a todos los routers vecinos.

La configuración del proceso de enrutamiento EIGRP consta de dos pasos: posibilitar que el router ejecute el protocolo EIGRP e identificar las direcciones e interfaces de la red que deben incluirse en las actualizaciones de enrutamiento.

Para posibilitar que el router ejecute EIGRP, se utiliza el comando principal de configuración de IOS **router eigrp**.

Este comando requiere como parámetro un número entero, o **process-id**, en caso de que se ejecuten varios procesos EIGRP en un mismo router. Como en el caso del protocolo IGRP, se pueden especificar las interfaces y las direcciones de red que se deben incluir en las publicaciones de enrutamiento EIGRP con el subcomando de configuración de enrutamiento de IOS **network**. Este comando toma como un parámetro la dirección de red con clase que se debe incluir en las actualizaciones de enrutamiento. El comando **network** debe utilizarse para identificar sólo aquellas direcciones IP de red que están conectadas directamente con el router que está configurando y que deben incluirse en el proceso de enrutamiento EIGRP. En las actualizaciones de enrutamiento sólo se incluyen las interfaces que tienen direcciones IP en la red identificada.

CONFIGURACIÓN DEL PROTOCOLO DE GATEWAY FRONTERIZO

El protocolo de gateway fronterizo (Boarder Gateway Protocolo, BGP) es un protocolo de gateway exterior (Exterior Gateway Protocolo, EGP). A diferencia de los IGP, que intercambian información acerca de las redes y las subredes que hay dentro del mismo dominio de enrutamiento o sistema autónomo, los EGP están diseñados para intercambiar la información de enrutamiento entre los dominios de enrutamiento o los sistemas autónomos. BGP es el principal método de intercambio de información de red entre empresas, ISP y NSP en Internet. BGP ofrece ciertas ventajas con respecto a su predecesor, el Protocolo de gateway exterior (Exterior Gateway Protocolo, EGP).

La ventaja más notable es que garantizar el intercambio sin bucles de la información de enrutamiento entre sistemas autónomos. La versión 4 de BGP es la más reciente revisión del mismo. Ofrece algunas ventajas sobre las versiones anteriores, como la gestión de bloques CIDR. BGP, que ha sido adoptado por el IETF, se especifica en las RFC 1163, 1267 y 1771. Estas RFC definen las versiones 2, 3 y 4 de BGP, respectivamente.

Los routers BGP se configuran con la información del vecino a fin de que se puedan formar una conexión TCP fiable sobre la que transportar información de la ruta de acceso del sistema autónomo y la ruta de la red. A diferencia de algunos de los IGP, BGP utiliza TCP como protocolo de transporte en lugar de definir el suyo propio. Tras establecer una sesión BGP entre vecinos, esta sigue abierta a menos que se cierre específicamente o que haya un fallo en el enlace. Si dos routers vecinos intercambian información de ruta y sesiones BGP, se dicen que son iguales BGP. La información de ruta intercambiada entre iguales incluye el par número de red/sistema autónomo de la ruta y otros atributos de las rutas. La ruta de acceso de sistema autónomo es una cadena de números del sistema autónomo a través de la que se puede llegar a la ruta publicada.

En principio los iguales BGP intercambian todo el contenido de las tablas de enrutamiento BGP. Posteriormente, sólo se envían actualizaciones increméntales entre los iguales para avisarles de las rutas nuevas o eliminadas. A diferencia de las tablas de rutas IGP, no es necesario para que las tablas de rutas BGP se actualicen periódicamente.

En su lugar, todas las rutas BGP guardan el último número de versión de la tabla que se ha publicado a sus iguales, así como su propia versión interna de la tabla. Cuando se recibe un cambio en un igual. La versión interna de la tabla se incrementa y se compara con las versiones publicadas en la tabla de estos iguales. Este proceso asegura que todos los iguales del router se mantienen sincronizados con todos los cambios que se procesan. BGP también guarda una tabla de rutas BGP independiente que contiene todas las rutas de acceso posibles a las redes publicadas. En la tabla de selección de la ruta principal se almacena solamente la ruta de acceso óptima y ésta es la única que se publica a los restantes iguales BGP.

Los iguales BGP se dividen en dos categorías: iguales BGP externos (EBGP) e iguales BGP internos (IBGP). Se dice que los iguales BGP que se encuentran en dominios administrativos o sistemas autónomos distintos y que intercambian información de enrutamiento son iguales EBGP. Los iguales EBGP suelen ser otras organizaciones, ISP o NSP con los que los sistemas autónomos deseen compartir información relativa a las rutas del sistema autónomo o que se han conocido de otras fuentes externas.

Los iguales BGP que se encuentran en el mismo dominio administrativo o sistema autónomo y que intercambian información de enrutamiento se dice que son iguales IBGP. Los iguales IBGP son routers del mismo sistema autónomo que necesitan compartir las rutas BGP conocidas externamente para tener una imagen completa de todas las rutas posibles a los destinos externos y para volverlas a publicar a los restantes iguales EBGP. Los iguales IBGP son habituales cuando un sistema autónomo tiene más de una relación con iguales BGP externos, como dos conexiones a Internet. Los iguales IBGP son un método más simple y sencillo de compartir rutas derivadas de iguales EBGP.

La alternativa a este método es redistribuir las rutas EBGP conocidas de un IGP (como EIGRP o OSPF) para transportarlas a través del sistema autónomo y a continuación, redistribuirlas a las rutas desde el IGP de vuelta al BGP para publicarlas a través de EBGP a otros iguales BGP externos. La redistribución de rutas puede provocar la pérdida de la información de la métrica del enrutamiento y potenciales bucles de enrutamiento. Además de la protección de los peligros de la redistribución de rutas, los iguales IBGP ofrecen todos los controles administrativos, las ponderaciones y las capacidades de filtrado asociadas con el protocolo BGP, y mantienen una imagen coherente de la información de enrutamiento publicada el mundo exterior a través de BGP.

Sin la aplicación de controles y ponderaciones administrativas, la selección de la ruta BGP óptima se basa en la longitud de la ruta de acceso del sistema autónomo para una ruta de red.
La longitud se define como el número de sistemas autónomos distintos necesarios para acceder a la red. Cuanto menor sea la distancia, más deseable será la ruta de acceso. A través del uso de los controles administrativos, BGP es uno de los protocolos de enrutamiento más flexibles y totalmente configurables disponibles. Ofrece a los administradores de red la capacidad de implementar una gran variedad de normativas de enrutamiento a través de los atributos de ruta, tales como la métrica Multi-Exit Discriminator (MED) y las características de filtrado y del atributo Local Preference como, por ejemplo, las listas de distribución.

Sugerencia_

Antes de implantar las normativas de enrutamiento BGP a través del uso de MED, Local Preference y otros atributos, asegúrese de que conoce perfectamente los efectos de estos modificadores.

Si una red tiene conexiones con varios ISP, se suele ejecutar BGP para que pueda seleccionarse la mejor ruta de acceso a las redes externas. Habitualmente no es necesario ejecutar BGP cuando hay una conexión con un solo ISP, ya que se llega a todas las rutas de acceso a las redes externas a través de un solo proveedor. Sin embargo, algunos proveedores prefieren cambiar de BGP para conocer la ruta de acceso a las redes de sus clientes y para proporcionar las rutas de red para el enrutamiento predeterminado.

La configuración del proceso de enrutamiento BGP consta de tres fases: La activación del router para que ejecute BGP, la identificación de las direcciones de red que hay que publicar a los routers iguales.

Para activar el router con el fin de que utilice BGP se utiliza el comando de configuración global de IOS **router bgp**.

Este comando utiliza como parámetro un número entero que es el número del sistema autónomo (ASN) que ha asignado a esta red uno de los registros de direcciones de red (RIPE, APNIC o ARIN). Para evitar la duplicación accidental, los registros deben asignar un ASN único a cada uno de los sistemas autónomos independientes que esté conectado a Internet. La duplicación de ASN puede provocar que no se publique una red a causa de una detección errónea de los bucles. Si BGP se ejecuta en una red completamente privada que no está conectada a Internet, los ASN deberían seleccionarse del bloque de ASN privados de rango 32768 a 64511.

La identificación de los routers iguales se realiza a través del uso del subcomando de configuración de enrutamiento de IOS **neighbor remote-as**. Este comando utiliza dos parámetros: la dirección IP del router vecino y un ASN. Cuando el ASN especificado como **remote-as** es distinto del especificado en el comando de configuración global **router bgp**, se considera que el vecino es un igual BGP externo (EBGP). La dirección IP de un router vecino que sea igual EBGP suele ser una dirección de una interfaz de red conectada directamente.

Cuando el ASN especificado como **remote-as** es igual al especificado en el comando de configuración global **router bgp**, se considera que el vecino es un igual BGP interno (IBGP). La dirección IP del router vecino que sea un igual IBGP es una dirección IP válida y accesible para dicho igual. Los iguales IBGP se pueden ubicar en una interfaz de red conectada directamente(como con varias conexiones ISP en una ubicación) o una red sin conexión vinculada a un router distante del sistema autónomo (como con varias conexiones ISP en distintas ubicaciones).

Dado que no es necesario que las direcciones IP de los iguales IBGP se encuentren en una interfaz de red conectada directamente, a menudo es aconsejable utilizar la dirección de la interfaz loopback como dirección de origen y de destino de los iguales IBGP. Dado que la interfaz loopback no está asociada a ninguna interfaz física, estará activa y accesible siempre que haya una ruta de acceso a su dirección IP asociada a través del enrutamiento IP o de las rutas estáticas.

Para configurar una interfaz loopback como dirección IP de origen para los iguales IBGP, utilice el subcomando de configuración de enrutamiento de IOS **neighbor** con la palabra clave **update-source**. La palabra clave **update-source** de ir seguida del nombre y número de una interfaz loopback correctamente configurada y con la dirección adecuada del router que está configurando.

Si un router tiene muchos vecinos iguales BGP, suele ser difícil recordar qué direcciones IP y ASN pertenecen a cada igual. Con la palabra clave **description** del subcomando de configuración de enrutamiento de IOS **neighbor**, es posible añadir comentarios que puedan facilitar al administrador de la red la obtención de información.

La identificación de las redes del sistema autónomo que se van a publicar a los iguales EGBP se realiza mediante el uso del subcomando de configuración de enrutamiento de IOS **network**.

Este comando utiliza como parámetro la dirección de red que se va a publicar a los routers iguales y la palabra clave opcional **mask**, seguidas por una máscara de red de dicha dirección. Si no se incluye ninguna máscara de red, se asume la dirección de red con clase.

Mediante el uso de la máscara de red, BGP puede publicar subredes y bloques CIDR a los routers iguales. Las redes conocidas de otros sistemas autónomos a través de EBGP se intercambiarán entre los iguales IBGP del sistema autónomo.

Nota_

Tenga en cuenta que los routers BGP publican las rutas conocidas de un igual BGP a todos sus otros iguales BGP. Por ejemplo las rutas conocidas a través de EBGP con su ISP se volverán a publicar a los iguales EBGP. Mediante la publicación reiterada de las rutas, la red puede pasar ha ser una red de tránsito entre los proveedores con los que se conecte, Esto podría irritar a los proveedores y provocar grandes congestiones en la red. Si no se desean crear dichas redes de transito, utilice las capacidades de filtrado de rutas de **distribute-list** y **route-maps** para controlar la publicación reiterada de las rutas conocidas.

Si las rutas BGP no se distribuyen en el proceso de enrutamiento de IGP, la sincronización de BGP se desactivará con el comando de configuración de ruta de IOS **no synchronization**. Con la sincronización activa, no se publicará ninguna ruta de igual EBGP, a menos que dicha ruta aparezca en la tabla de selección de rutas primarias de igual y se conozca a través del proceso de enrutamiento de IGP. Dará como resultado una mayor velocidad de convergencia de BGP.

Si los iguales IBGP intercambian información de enrutamiento conocida de iguales EBGP, es importante indicar que igual IBGP debe de tener una ruta a la dirección de próximo salto para la ruta que se va a conocer del igual EBGP.

Si las direcciones del próximo salto no forman parte del conjunto de direcciones de red al que el IGP proporciona información de enrutamiento, utilice el comando **redistribute**, para publicar las rutas estáticas o conectadas directamente de dichas direcciones en el proceso de enrutamiento de IGP.

ADMINISTRACIÓN DE LA INFORMACIÓN DEL PROTOCOLO DE ENRUTAMIENTO DINÁMICO.

Normalmente los administradores de redes desean aplicar una norma administrativa para controlar el flujo de la información de enrutamiento de la red dentro y fuera de la misma. Estas normas incluyen determinar que routers participarán en el proceso de enrutamiento, si la información de la subred se propaga entre diferentes espacios de direcciones de la red principal y las rutas que deben compartirse entre los distintos routers. Al implementarse estas normas se pueden controlar los patrones de acceso de tráfico a la red y su seguridad.

Uno de los atributos más importantes a la hora de administrar los protocolos de enrutamiento dinámico es la posibilidad de permitir o denegar la propagación de las rutas de la red desde un router a la red.

Esta capacidad para filtrar la información de enrutamiento permite restringir el acceso a una sección de la red desde otra. En el caso del protocolo BGP, al restringir la propagación y la publicación de rutas a routers iguales se evita que un sistema autónomo permita el transito de paquetes entre dos o más proveedores de servicios de Internet sin darse cuenta.

La herramienta principal para el filtrado de la información de enrutamiento es el subcomando de configuración de enrutamiento de IOS **distribute-list**. Las funciones de filtrado del comando **distribute-list** se activan con el uso de listas de acceso son herramientas de tipo genérico que definen los criterios de filtrado. Cuando se aplican junto con subcomandos de protocolo de enrutamiento, las listas de acceso pueden definir las rutas permitidas o denegadas.

El comando **distribute-list** aplica una lista de acceso a una situación determinada de control de propagación de rutas. El comando **distribute-list** admite varios parámetros: el nombre o número de una lista de acceso IP, la palabra clave **in** u **out**, que controla la dirección en la que ocurre el filtrado, y un identificador de interfaz, que es optativo, entre otros. Este indicador indica que el filtrado solo debe efectuarse en las actualizaciones de enrutamiento para esa interfaz específicamente. Si se omite el identificador, la lista de distribución se aplica a todas las actualizaciones de enrutamiento que coinciden con la lista de acceso.

Nota_

Debido a la naturaleza de desbordamiento, o inundación de los paquetes LSA en los protocolos de estado de enlace, como OSPF e IS-IS, no es posible filtrar la información de enrutamiento entrante. El filtrado de enrutamiento saliente sólo es aplicable a las rutas externas.

Cuando el comando **distribute-list** se aplica como subcomando de un proceso de enrutamiento, el filtrado definido en **distribute-list** se aplica a todos los orígenes de las actualizaciones de enrutamiento. En muchas ocasiones, puede ser preferible aplicar el filtrado solo a un origen de la información, como un determinado igual BGP. El filtrado de actualizaciones entrantes o salientes de determinados iguales BGP se logra aplicando el comando **distribute-list** a un determinado vecino BGP como una palabra clave opcional del subcomando BGP **neighbor**.

A veces, podría querer que un router escuche las actualizaciones de enrutamiento de una interfaz determinada, pero que no publique dicha información de enrutamiento a los otros routers de la interfaz. Cuando se desea esta configuración, se dice que el router opera en modo pasivo. El subcomando de configuración de enrutamiento de IOS **passive-interface** configura el modo pasivo. Este comando toma como parámetro el identificador de la interfaz sobre el que se suprimen las actualizaciones de enrutamiento salientes.

Es posible que desee configurar un router con una lista de los routers vecinos específicos con los que este puede intercambiar información de enrutamiento dinámico. Por ejemplo para implementar el protocolo OSPF en un medio de no difusión, hay que especificar los routers vecinos para que el protocolo funcione correctamente.

Como otra posibilidad, puede implementar un entorno mas seguro en el que solo los routers vecinos especificados puedan intercambiar información de enrutamiento de un modo punto a punto. El subcomando de configuración de enrutamiento de IOS **neighbor** se utiliza para especificar la dirección IP de un router vecino con el que intercambiar la información de enrutamiento. cuando se utiliza junto con el comando **passive-interface**, la información de enrutamiento se intercambia solo con los routers vecinos especificados en intercambios punto a punto(de no difusión). El comando **neighbor** toma como parámetro una dirección IP para el router vecino.

Ocasionalmente los routers basados en Cisco IOS necesitan comunicar la información de enrutamiento a otros dispositivos que no admiten el protocolo de enrutamiento seleccionado para la red.
Para dar soluciones a tales situaciones el software IOS tiene una capacidad de pasar la información de enrutamiento de un protocolo de enrutamiento dinámico a otro. Este proceso recibe el nombre de distribución de rutas.

El subcomando de configuración de enrutamiento de IOS **redistribute** se utiliza para activar la predistribución de rutas. Este comando toma como argumento el nombre del proceso de enrutamiento del que se quieren redistribuir las rutas. También se pueden especificar las palabras **static** o **connected** en vez del nombre de un proceso de enrutamiento. El uso de la palabra clave **static** permite que las rutas estáticas configuradas manualmente se publiquen en el proceso de enrutamiento. La palabra clave **connected** permite que las rutas para interfaces conectadas directamente y que no coincidan con la dirección especificada en el subcomando de enrutamiento **network** se publique en el proceso de enrutamiento.

Como cada protocolo de enrutamiento dinámico utiliza un método diferente para calcular su métrica, puede resultar imposible realizar la conversión métrica de manera automática.
A continuación hay una lista de las conversiones métricas automáticas que admite IOS:

RIP puede redistribuir automáticamente las rutas estáticas. Asigna a las rutas estáticas una métrica de 1 (directamente conectado).

IGRP puede redistribuir automáticamente las rutas estáticas y la información de otros sistemas automáticos con enrutamiento IGRP. IGRP asigna a las rutas estáticas una métrica que las identifica como directamente conectadas. IGRP no modifica la métrica de rutas derivadas de las actualizaciones IGRP de otros sistemas autónomos.

Cualquier protocolo puede redistribuir otros protocolos de enrutamiento si tiene definida una métrica predeterminada.

La métrica predeterminada se define con el subcomando de configuración de enrutamiento de IOS **default-metric**.

El comando toma como argumento uno o más atributos de métricas de protocolos de enrutamiento, basándose en el protocolo de enrutamiento determinado que se esté configurando.

Sugerencia_
La redistribución de la información de enrutamiento de un protocolo a otro puede resultar compleja.

La redistribución reciproca(en la que se pasan rutas de un protocolo a otro y viceversa) puede causar bucles de enrutamiento porque no se hacen comprobaciones del correcto funcionamiento de las rutas que se redistribuyen. Si es posible, se debe evitar la redistribución reciproca. Si la redistribución reciproca es absolutamente necesaria, utilice los comandos a determinados protocolos de enrutamiento.

El subcomando de configuración de enrutamiento de IOS **no auto-summary** evita el resumen automático de las direcciones en los limites de la red con clase y permite la propagación de la información de la subred.

VISUALIZACIÓN DE LA INFORMACIÓN DEL PROTOCOLO DE ENRUTAMIENTO DINÁMICO.

La configuración y operatividad de los protocolos de enrutamiento dinámico se puede verificar con una serie de comandos ejecutables de IOS. Estos comandos se dividen en dos categorías: independientes del protocolo y específicos del protocolo.

El comando ejecutable de IOS **show ip route** se puede utilizar para determinar si las rutas se conocen mediante protocolos de enrutamiento dinámico y para determinar sus atributos.

Mediante el comando ejecutable de IOS **show ip protocols** se pueden determinar los protocolos que se ejecutan y sus diferentes atributos. Este comando toma un parámetro opcional con la palabra clave **summary**. La versión del comando con **summary**. La versión del comando **summary** ofrece una lista exclusivamente del nombre del protocolo de enrutamiento y del process-id, si es aplicable.

La versión estándar del comando **show ip protocols** ofrece una lista de todos los protocolos de enrutamiento que se ejecutan y de sus numerosos atributos, como orígenes de actualización de enrutamiento, aplicación de filtros de distribución de listas, información de métrica y las redes que se publican.

Los protocolos de enrutamiento complejos, como EIGRP, OSPF y BGP, proporcionan acceso a muchos atributos, tablas y bases de datos de información sobre su funcionamiento, configuración y topología.

COMANDOS EJECUTABLES DE IOS PARA EIGRP.

Show ip eigrp interfaces
Muestra información sobre las interfaces configuradas para IP EIGRP:

Show ip eigrp neighbors
Muestra los vecinos descubiertos por IP EIGRP.

Show ip eigrp topology
Muestra el número de paquetes enviados y recibidos por proceso(s) IP EIGRP.

Show ip ospf
Muestra información general sobre los procesos de enrutamiento OSPF.

Show ip ospf database
Muestra varias listas de información relativa a la base de datos OSPF.

Show ip ospf database network
Muestra la información de enlace de red desde la base de datos de OSPF.

Show ip ospf database external
Muestra la información de enlace de red externa desde la base de datos OSPF.

Show ip ospf database database summary
Muestra la información de resumen pertinente a la base de datos OSPF.

Show ip ospf border-routers
Muestra las entradas de la tabla de enrutamiento interna OSPF a routers fronterizos(Area Border Routers, ARB) y routers límite de sistema autónomo(Autonomus System Boundary Routers, ASBR).

Show ip ospf interface
Muestra la información específica de la interfaz y relativa a OSPF.

Show ip ospf neighbor
Muestra información de vecinos OSPF.

Comandos ejecutables de IOS para BGP.

Show ip bgp cidr-only
Muestra las rutas BGP que contienen máscaras de red de subred y superred.

Show ip bgp filter-list *número de lista de acceso*.
Muestra las rutas que coinciden con la lista de acceso de rutas del sistema autónomo.

Show ip bgp regexp *expression regular*
Muestra las rutas que coinciden con la expresión regular específica introducida en la línea de comandos.

Show ip bgp neighbors*[dirección]*routers
Muestra las rutas conocidas desde un vecino BGP determinado.

Show ip bgp neighbors*[dirección]*advertised
Muestra las rutas publicas a un vecino BGP determinado.

Show ip bgp neighbors*[dirección]*paths
Muestra las rutas publicas a un vecino BGP determinado.

Show ip bgp paths
Muestra todas las rutas BGP de la base de datos BGP.

Show ip bgp summary
Muestra el estado de todas las conexiones con iguales BGP.

CONFIGURACIÓN DE LOS FILTROS IP A TRAVÉS DE LISTAS DE ACCESO.

Desde la primera vez que se conectaron varios sistemas para formar una red, ha existido una necesidad de restringir el acceso a determinados sistemas o partes de la red por motivos de seguridad, privacidad y otros. Mediante la utilización de las funciones de filtrado de paquetes del software IOS, un administrador de red puede restringir el acceso a determinados sistemas, segmentos de red, rangos de direcciones y servicios, basándose en una serie de criterios. La capacidad de restringir el acceso cobra mayor importancia cuando la red de una empresa se conecta con otras redes externas, como otras empresas asociadas o Internet.

ADMINISTRACION BASICA DEL TRAFICO IP MEDIANTE LISTAS DE ACCESO.

Los router se sirven de las listas de control de acceso (ACL) para identificar el tráfico.

Esta identificación puede usarse después para filtrar el tráfico y conseguir una mejor administración del trafico global de la red.

Las listas de acceso constituyen una eficaz herramienta para el control de la red. Las listas de acceso añaden la flexibilidad necesaria para filtrar el flujo de paquetes que entra y sale de las diferentes interfaces del router.

El filtrado de paquetes permiten controlar el movimiento de paquetes dentro de la red.

Este control puede ayudar a limitar él tráfico originado por el propio router.

Una **lista de acceso** IP es un listado secuencial de condiciones de permiso o prohibición que se aplican a direcciones IP o a protocolos IP de capa superior.

Las listas de acceso identifican tráfico que ha de ser filtrado en su transito por el router, pero no pueden filtrar él trafico originado por el propio router.

Las listas de acceso pueden aplicarse también pueden aplicarse a los puertos de líneas de terminal virtual para permitir y denegar trafico Telnet entrante o saliente, no es posible bloquear el acceso Telnet desde dicho router.

Se pueden usar listas de acceso IP para establecer un control más fino o la hora de separar el tráfico en diferentes colas de prioridades y personalizadas.

Una lista de acceso también pueden utilizarse para identificar el trafico "interesante" que sirve para activar las llamadas del enrutamiento por llamada telefónica bajo demanda(DDR).

Las listas de acceso son mecanismos opcionales del software Cisco IOS que pueden ser configurados para filtrar o verificar paquetes con el fin de determinar si deben ser retransmitidos hacia su destino, o bien descartados.

LISTAS DE ACCESO ESTÁNDAR

Las listas de acceso IP estándar comprueban las direcciones de origen de los paquetes que solicitan enrutamiento. El resultado es el permiso o la denegación de la salida del paquete por parte del protocolo, basándose en la dirección IP de la red-subred-host de origen.

LISTAS DE ACCESO EXTENDIDAS

Las listas de acceso comprueban tanto la dirección de origen como la de destino de cada paquete. También pueden verificar protocolos especificados, números de puerto y otros parámetros.
Las listas de acceso pueden aplicarse de las siguientes formas:

LISTAS DE ACCESO DE ENTRADA

Los paquetes entrantes son procesados antes de ser enrutados a una interfaz de salida, si el paquete pasa las pruebas de filtrado, será procesado para su enrutamiento.(evita la sobrecarga asociada a las búsquedas en las tablas de enrutamiento si el paquete ha de ser descartado por las pruebas de filtrado).

LISTAS DE ACCESO DE SALIDA

Los paquetes entrantes son enrutados a la interfaz de salida y después son procesados por medio de la lista de acceso de salida antes de su transmisión.
Las listas de acceso expresan el conjunto de reglas que proporcionan un control añadido para los paquetes que entran en interfaces de entrada, paquetes que se trasmiten por el router, y paquetes que salen de las interfaces de salida del router.
Las listas de acceso no actúan sobre paquetes originados en el propio router, como las actualizaciones de enrutamiento a las sesiones Telnet salientes.

OPERATIVIDAD DE LAS LISTAS DE ACCESO

Cuando un paquete llega a una interfaz, el router comprueba si el paquete puede ser retransmitido verificando su tabla de enrutamiento. Si no existe ninguna ruta hasta la dirección de destino, el paquete es descartado.

A continuación, el router comprueba si la interfaz de destino esta agrupada en alguna lista de acceso. De no ser así, el paquete puede ser enviado al búfer de salida.

Si el paquete de salida está destinado a un puerto, que no ha sido agrupado a ninguna lista de acceso de salida, dicho paquete será enviado directamente al puerto destinado.

Si el paquete de salida está destinado a un puerto ha sido agrupado en una lista de acceso outbound, antes de que el paquete pueda ser enviado al puerto destinado será verificado por una serie de instrucciones de la lista de acceso asociada con dicha interfaz. Dependiendo del resultado de estas pruebas, el paquete será admitido o denegado.

Para las listas de salida **permit** significa enviar al búfer de salida, mientras que **deny** se traduce en descartar el paquete.
Para las listas de entrada **permit** significa continuar el procesamiento del paquete tras su recepción en una interfaz, mientras que **deny** significa descartar el paquete.

Cuando se descarta un paquete IP, ICMP devuelve un paquete especial notificando al remitente que el destino ha sido inalcanzable.

PRUEBA DE CONDICIONES EN LISTAS DE ACCESO

Las instrucciones de una lista de acceso operan en un orden lógico secuencial.
Evalúan los paquetes de principio a fin, instrucción a instrucción. Si la cabecera de un paquete se ajusta a una instrucción de la lista de acceso, el resto de las instrucciones de la lista serán omitidas, y el paquete será permitido o denegado según se especifique en la instrucción competente.

Si la cabecera de un paquete no se ajusta a una instrucción de la lista de acceso, la prueba continua con la siguiente instrucción de la lista.
El proceso de comparación sigue hasta llegar al final de la lista, cuando el paquete será denegado implícitamente.

Una vez que se produce una coincidencia, se aplica la opción de permiso o denegación y se pone fin a las pruebas de dicho paquete. Esto significa que una condición que deniega un paquete en una instrucción no puede ser afinada en otra instrucción posterior.

La implicación de este modo de comportamiento es que el orden en que figuran las instrucciones en la lista de acceso es esencial. Hay una instrucción final que se aplica a todos los paquetes que no han pasado ninguna de las pruebas anteriores. Esta condición final se aplica a todos esos paquetes y se traducen en una condición de denegación del paquete.

En lugar de salir por alguna interfaz, todos los paquetes que no satisfacen las instrucciones de la lista de acceso son descartadas.

Esta instrucción final se conoce como la **denegación implícita de todo**, al final de cada lista de acceso. **Aunque esta instrucción no aparece en la configuración del router, siempre esta activa**. Debido a dicha condición, es necesaria que en toda lista de acceso exista al menos una instrucción **permit**, en caso contrario la lista de acceso bloquearía todo el tráfico.

IMPLEMENTACIÓN DE LISTAS DE ACCESO

Una lista de acceso puede ser aplicada a múltiples interfaces. Sin embargo, sólo puede haber una lista de acceso por protocolo, por dirección y por interfaz.

- Utilice sólo números de listas de acceso dentro del rengo definido por CISCO para el protocolo y el tipo de listas que va ha crear.

- Sólo se permite una lista por protocolo, dirección e interfaz. Es posible tener varias listas para una interfaz, pero cada una debe pertenecer a un protocolo diferente.

- Procesamiento de principio a fin:

- Organice las listas de acceso de modo que las referencias más específicas a una red o subred aparezcan delante de las más generales. Coloque las condiciones de cumplimiento más frecuente antes de las menos habituales.
- Las adiciones a las listas se agregan siempre al final de éstas, pero siempre delante de la condición de denegación implícita.
- No es posible agregar a eliminar selectivamente instrucciones de una lista cuando se usan listas de acceso numeradas, pero sí cuando se usan listas de acceso IP con nombre(característica de Cisco IOS v.11.2)

- Denegación implícita de todo:

- A menos que termine una lista de acceso con una condición de permiso implícito de todo, se denegará todo el trafico que no cumpla ninguna de las condiciones establecidas en la lista.
- Toda lista de acceso deben incluir al menos una instrucción **permit**. En caso contrario, todo el trafico será denegado.

- Cree una lista de acceso antes de aplicarla a la interfaz. Una interfaz con una lista de acceso inexistente o indefinida aplicada al mismo dará paso(permitirá) a todo el trafico.

- Las listas de acceso permiten filtrar sólo el tráfico que pasa por el router. No pueden hacer de filtro para el tráfico originado por el propio router.

COMANDOS BASICOS DE LISTAS DE ACCESO

Las listas de acceso contienen instrucciones globales que se aplican para identificar paquetes. Estas listas se crean con el comando **access-list**.

El comando de configuración de interfaz **ip access-group** activa la lista de acceso IP en una interfaz.

Router(config)#access-list[n° de lista de acceso][permit|deny][condiciones de prueba]

La opción permit significa que al paquete le será permitido pasar a través de las interfaces que se apliquen en la lista.

La opción deny significa que el router descartará el paquete. Los últimos parámetros de la instrucción especifican las condiciones de pruebas.

La prueba puede ser tan simple como comprobar una dirección de origen individual, la lista puede expandirse para incluir varias condiciones de prueba.

Router(config)#[protocolo]access-group[n° de lista de acceso][in|out]

Se activa una lista de acceso IP en una interfaz.

Listas de acceso IP	**Rango numérico identificador**
Estándar	1 a 99
Extendida	100 a 199
Con nombre	Nombre(Cisco IOS 11.2 y posterior)

Listas de acceso IPX	**Rango numérico identificador**
Estándar	800 a 899
Extendida	900 a 999
Filtros SAP	1000 a 1099
Con nombre	Nombre (Cisco IOS 11.2F y posterior)

LISTAS DE ACCESO TCP/IP

Una lista de acceso aplicada a una interfaz hace que el router busque en la cabecera de la capa 3 y posiblemente en la cabecera de la capa 4 un paquete del tráfico de la red al que aplicar las condiciones de prueba.

Las listas de acceso IP estándar verifican sólo la dirección de origen en la cabecera del paquete(Capa 3).
Las listas de acceso IP extendidas pueden verificar otros muchos elementos, incluidas opciones de la cabecera del segmento(Capa 4), como los números de puerto.

Para el filtrado de paquetes TCP/IP, las listas de acceso IP verifica las cabeceras del paquete y de la capa superior, para detectar lo siguiente:

- Direcciones IP de origen para listas de acceso estándar. Las listas de acceso estándar están identificadas por los números entre 1 y 99.
- Direcciones IP de origen y destino, protocolos específicos y números de puerto TCP y UDP, con listas de acceso extendidas. Las listas de acceso extendidas están identificadas por los números entre 10 y 199.

Puede ser necesario probar condiciones para un grupo o rengo de direcciones IP, o bien para una dirección IP individual.
La comparación de direcciones tiene lugar usando máscaras que actúan a modo de comodines en las direcciones de la lista de acceso, para identificar los bits de la dirección IP que han de coincidir explícitamente y cuales pueden ser ignorados.

El enmascaramiento wildcard para los bits de direcciones IP utiliza los números 1 y 0 para referirse a los bits de la dirección.

- Un bit de máscara wildcard 0 significa "comprobar el valor correspondiente"
- Un bit de mascara wildcard 1 significa "No comprobar(ignorar) el valor del bit correspondiente"

Para los casos más frecuentes de enmascaramiento wildcard se pueden utilizar abreviaturas.

Host = mascara comodín 0.0.0.0
Any = 0.0.0.0 255.255.255.255

Router(config)#access-list[n° de lista de acceso][permit|deny][dirección de origen][mascara comodín]

- **Numero de lista de acceso** Identifica la lista a la que pertenece la entrada. Se trata de un número entre 1 y 99.
- **Permit|deny** indica si esta entrada permitirá o bloqueará el tráfico a partir de la dirección especificada.
- **Dirección de origen** identifica la dirección IP de origen.
- **Mascara wildcard** identifica los bits del campo de la dirección que serán comprobados.

La mascara predeterminada es 0.0.0.0(coincidencia de todos los bits).

Router(config)#ip access-group[n° de lista de acceso][in|out]

- **Número de lista de acceso** indica el número de lista de acceso que será aplicada a esa interfaz.
- **In|out** selecciona si la lista de acceso se aplicará como filtro de entrada o de salida.

Si no se especifica nada, se adoptará la opción **out** por omisión.

ELIMINAR UNA LISTA DE ACCESO DE UNA INTERFAZ

1. **no ip access-group[n° de lista de acceso]** en la interfaz
2. **no access-list[n° de lista de acceso]** comando global

CONTROL DE ACCESO VTY

Líneas de terminal virtual. Existen por omisión, cinco de estas líneas de terminal virtual numeradas del 0 al 4.
Una lista de acceso extendida para Telnet de salida no impide sesiones Telnet iniciadas en el router.

El filtrado de Telnet se considera normalmente una función de lista de acceso IP extendida, debido a que está filtrando un protocolo de nivel superior.
Se puede crear una lista de acceso estándar donde se identifique la dirección de origen y se aplica a las líneas vty usando el comando **access-class.**

El comando **access-class** se aplica también a listas IP estándar para filtrar sesiones Telnet salientes del router mediante líneas vty.

COMO APLICAR UNA LISTA DE ACCESO ESTÁNDAR A LOS PUERTOS TELNET.

router(config)#line vty[#|rango vty]

indica una línea vty especifica a configurar.

Rango-vty indica un rango de líneas vty a las que se aplicará la configuración.
Utilice el comando **access-class** para enlazar la lista de acceso existente a una línea o rango de líneas de terminal.

router(config-line)#access-class[n° de lista de acceso][in|out]

Número de lista de acceso indica el número de la lista de acceso a vincular a una línea de terminal. Este es un valor decimal entre 1 y 99.

In impide que el router pueda recibir conexiones Telnet desde las direcciones de origen que aparecen en la lista de acceso.

Out impide que los puertos vty del router pueden iniciar conexiones Telnet a las direcciones definidas en la lista de acceso estándar.
Tenga en cuenta que la dirección de origen especificada en la lista de acceso estándar se considera como una dirección de destino cuando se usa **access-class out**.

La denegación implícita a todo se sigue aplicando a la lista de acceso.

LISTAS DE ACCESO IP EXTENDIDAS

Las listas de acceso estándar realizan el filtrado basándose en una máscara y una dirección de origen.
Este tipo de listas permiten o deniegan el acceso a todo el protocolo TCP/IP.

Las instrucciones de las listas de acceso IP extendidas permiten verificar direcciones tanto origen como destino.

Estándar

Filtros basados sólo en una dirección de origen.

Permite o deniega todo el protocolo TCP/IP.

Rango de 1 a 99.

Extendida

Filtros basados en direcciones de origen y destino y números de puerto de origen y destino.

Especifica un protocolo IP y un número de puerto.

Rango de 100 a 199.

Al final se puede conseguir una mayor precisión en el filtrado especificando el protocolo y los números de puerto UDP o TCP opcionales.

Utilizando el protocolo y número de puerto UDP o TCP opcional, se puede especificar el tipo de operación lógica que la lista de acceso extendida ha de realizar en los protocolos indicados.

N° de puerto	**Protocolo IP**
20	Datos del protocolo FTP
21	Programa FTP
23	Telnet
25	SMTP
69	TFTP
53	DNS

www.isi.edu/in-notes/iana/assignments/ports-numbers

CONFIGURACION DE UNA LISTA DE ACCESO EXTENDIDA.

Agregar una lista de acceso extendida a un router a modo de filtro de paquetes es una proceso que consta de dos pasos:
En primer lugar, se ha de crear la lista de acceso. A continuación, se debe aplicar la lista a una interfaz.

Utilice el comando **access-list** para crear una entrada que exprese una condición en un filtro complejo:

Router(config)#access-list[n° de lista de acceso][permit|deny][protocol][dirección de origen][mascara comodín][puerto del operador][dirección de destino][mascara de destino][puerto del operador][establisehed][log]

Numero de lista de acceso: identifica la lista mediante un numero entre 100 y 199.
Permit|deny: indica si la entrada permitirá o bloqueara la dirección especificada.
Protocolo: puede ser IP, TCP, UDP, ICMP, GRE o IGRP.
Origen y destino: identifican direcciones IP de origen y destino.
Mascara origen y mascara destino: Son las mascaras comodín. Las **0** indican las posiciones que deben coincidir, y los **1** las "que no importan".
Puerto del operador: puede ser: **lt**(menor que)**gt**(mayor que)**eq**(igual a)o **neq**(distinto que) y un número de puerto de protocolo.
Establisehed Se usa solo para TCP de entrada. Esto permite que él trafico TCP pase si el paquete utiliza una conexión ya establecida(por ejemplo posee un conjunto de bits ACK)
Log Envía un mensaje de registro a la consola.

El comando **ip access-group** aplica una lista de acceso extendida existente a una interfaz. Solo se puede hacer una lista de acceso por protocolo, dirección e interfaz.

Router(config-if)#ip access-group[n° de lista de acceso][in|out]

N° de lista de acceso indica el número de la lista de acceso que será aplicado a ese interfaz.
In|out selecciona si la lista de acceso se aplicará como filtro de entrada o de salida. Si no se especifica nada se adoptará la opción **out** por omisión.

LISTAS DE ACCESO IP CON NOMBRE

Característica que apareció en CISCO IOS 11.2, permite identificar lista de acceso IP estándar y extendidas mediante cadenas alfanuméricas(nombres) en lugar de números de 1 a 199.

Con listas de acceso IP numeradas, para modificar una lista tendría que borrar primero la lista de acceso numerada y volver a introducirla de nuevo con las correcciones necesarias.
En una lista de acceso numerada no es posible borrar instrucciones individuales.

Las listas de acceso IP con nombre permiten eliminar entradas individuales de una lista especifica. El borrado de entradas individuales permite modificar las listas de acceso sin tener que eliminarlas y volver a configurarlas desde el principio. Sin embargo no es posible insertar elementos selectivamente en una lista.

Si se agrega un elemento a la lista, este se coloca al final de la misma.

No es posible usar el mismo nombre para varias listas de acceso.

Las listas de acceso de diferentes tipos tampoco pueden compartir nombre.

CREAR Y ACTIVAR UNA LISTA DE ACCESO IP CON NOMBRE

Router(config)#ip access-list[standard|extended][nombre]nombre único
Router(config[std|ext]nac1)#[permit|deny][condiciones de prueba]
Router(config[std|ext]nac1)#no[permit|deny][condiciones de prueba]
Router(config-if)#ip access-group[nombre][in|out]

Para eliminar una instrucción individual, anteponga **no** a la condición de prueba.

DIRECTRICES PARA LA IMPLEMENTACION DE LISTAS DE ACCESO ESTANDAR, EXTENDIDAS Y CON NOMBRE.

El orden en el que aparecen las instrucciones en la lista de acceso es fundamental para un filtrado correcto. La practica recomendada consiste en crear las listas de acceso en un servidor TFTP usando un editor de texto y descargarlas después en un router vía TFTP.

Las listas de acceso se procesan de arriba abajo. Si coloca las pruebas más especificas y las que se verificaran con mas frecuencia al comienzo de la lista de acceso, se reducirá la carga de procesamiento. Solo las listas de acceso con nombre permiten la supresión, aunque no la alteración del orden de instrucciones individuales en la lista. Si desea reordenar las instrucciones de una lista de acceso, deberá eliminar la lista completa y volver a crearla en el orden apropiado o con las instrucciones correctas.

Todas las listas de acceso terminan con una instrucción implícita "denegar todo".

Las listas de acceso extendidas, deben colocarse normalmente lo más cerca posible del origen del trafico que será denegado.

VERIFICACION Y CONTROL DE LISTAS DE ACCESO.

Router#show ip interface[tipo de interfaz][n° de interfaz]verifica si una lista de acceso esta asociada a un interfaz. Muestra información de la interfaz IP.
Router#show access-list muestra contenido de todas las listas de acceso.
Router#show[protocolo]access-list[n° lista de acceso|nombre]

Las capacidades de filtrado de paquetes de las listas de acceso IP del software IOS permite las restricción del flujo de paquetes según los siguientes criterios:

- Dirección IP de origen.
- Dirección IP de origen y destino.
- Tipos de protocolos IP, incluyendo TCP, UDP e ICMP.
- Servicios de protocolo TCP origen y destino, como envío de correo electrónico y Telnet.
- Servicios de protocolo UDP de origen y destino, como bootp y NetBIOS datagram.
- Servicios de protocolo ICMP, como Eco ICMP y Puerto inalcanzable ICMP.

La lista anterior no esta completa. La flexibilidad de las listas de acceso IP le ofrece al administrador una decisión muy amplia en cuanto a lo que se filtra y cómo se aplican los filtros. La clave para comprender las listas de acceso IP en el software IOS reside en que la tares de filtrado de paquetes está dividida en dos pasos muy diferentes. En primer lugar, el criterio de filtrado se define mediante el uso de los comandos **access-list** e **ip access-list**. En segundo lugar, el criterio de filtrado se aplica a las interfaces elegidas. Ya hemos considerado un método de aplicar el filtrado de lista de acceso, en conjunción con el comando **distribute-list** para filtrar la información de enrutamiento. En los apartados que aparecen a continuación, nos centraremos en la utilización de las listas de acceso en conjunción con el comando **ip access-group**.

DEFINICIÓN DE LAS LISTAS DE ACCESO.

Los criterios de filtrado se definen en una lista de instrucciones de permiso y denegación que se llama lista de acceso. Cada línea de esa lista de acceso se contrasta consecutivamente con las direcciones IP y demás información de un paquete de datos hasta que hay una coincidencia. Tan pronto como ocurre dicha coincidencia, se sale de la lista. Este proceso hace que las listas de acceso tengan una gran dependencia del orden.

Cuando se desarrolló originalmente, el software IOS sólo disponía de un comando para crear listas de acceso, el comando **access-list**. Mediante el uso de este comando y una serie de rangos relevantes de números, el administrador de red puede especificar el protocolo de red para el que se crea la lista.

Un rango numérico 1 a 99 denota una lista de acceso IP estándar y el rango 900 a 999 denota un filtro de paquetes IPX.

Alegando la necesidad de una mayor flexibilidad y un mayor número de listas de acceso, los diseñadores del software IOS crearon versiones del comando **access-list** para IP e IPX que permiten litas de acceso con nombre asignado. Puede utilizar una cadena arbitraria de caracteres en vez de un número para identificar la lista de acceso.

El comando para crear listas de acceso IP con nombre asignado es **ip access-list**, también existe el comando **ipx access-list** para listas **IPX** con nombre asignado.

Ya sea numerada o con nombre asignado, las listas de acceso IP pertenecen a una de estas dos categorías: estándar o extendida. Una lista de acceso IP estándar evalúa sólo la dirección IP de origen de un paquete, mientras que la lista de acceso extendida puede evaluar las direcciones IP de origen y destino, el tipo de protocolo IP y los puertos de origen y de destino de la capa de transporte.

Use el comando de configuración global de IOS **access-list** para establecer una lista de acceso numerada.

Como se explicó con anterioridad, el comando **access-list** toma como parámetro un número de lista. Las listas de acceso IP estándar se establecen por un número en el rango 1 a 99. Las listas de acceso IP extendidas se ven por un número en el rango 100 a 199. Tras el número de lista de cada línea de la lista de acceso encontrará la palabra clave **permit** o **deny**, seguida de la dirección, la máscara wildcard, el protocolo y el número de puerto del protocolo que se filtra.

```
Router#configure t
Router(config)#access-list[número][deny|permit][dirección IP]
Router(config)# access-list[número][deny|permit][dirección IP][máscara
wildcard]
Router(config)#^Z
```

El orden de las líneas de la lista de acceso determina el funcionamiento del filtro.

Sugerencia_

Las listas de acceso hacen uso del concepto conocido como máscara wildcard. Aunque parece similar a la máscara de red, la máscara wildcard se diferencia en que las posiciones de bit establecidas a 1 coinciden con cualquier valor. Una máscara wildcard de 0.0.0.255 coincide con cualquier número en el rango 0 a 255 que aparezca en el cuarto octeto de una dirección IP. Una máscara wildcard de 0.0.3.255 coincide con cualquier dirección IP que tenga un 0, 1, ó 3 en el tercer octeto y cualquier número en el cuarto octeto basado en la computación binaria. Las máscaras wildcard permiten que el administrador de red especifique rangos de direcciones que entran en los limites de bit de los números binarios.

Sugerencia_

Todas las listas de acceso tienen un **deny** implícito al final de la lista. Esto significa que cualquier paquete que no coincida con el criterio de filtrado de alguna de las líneas de la lista de acceso será denegado. Para una mejor resolución de problemas y un mayor control administrativo de la seguridad de la red, le recomendamos que ponga un **deny** explicito al final de la lista con la palabra clave opcional **log**. Esta acción hace que los paquetes que no coincidan con la lista queden registrados como una violación en la consola, o si tiene activado el registro de sistema(syslogging), en el servidor syslog. También puede aplicar la palabra clave opcional **log** a cualquier línea de la lista de acceso para que el administrador desee tener información de registro grabada.

Las listas de acceso IP con nombre asignado se crean con el comando de configuración **ip access-list**. Este comando toma como parámetros las palabras clave **extended** o **standard** para denotar el tipo de lista de acceso con nombre asignado que se crea y nombre mismo de dicha lista.

El comando **ip access-list** hace que la configuración del software IOS conmute al submodo de configuración de lista de acceso. Una vez en el submodo de configuración de lista de acceso, sólo se tienen que proporcionar los estados **permit** y **deny**, junto con la dirección de red y otros criterios de filtrado. No necesita repetirse el nombre de la lista de acceso con nombre designado en todas las líneas de la lista.

Ya sean numeradas o con nombre asignado, uno de los desafíos de la gestión de listas de acceso radica en recordar por qué determinados host, redes o servicios tienen el acceso permitido o denegado. A lo largo del tiempo, pueden cambiar los administradores de la red que deben responsabilizarse de mantener las listas de acceso en varios dispositivos de la red y las razones de determinar entradas de las listas de acceso pueden olvidarse.

En las primeras versiones del software IOS, la única manera de documentar la información sobre las listas de acceso(o cualquier comando de configuración) consistía en agregar comentarios a una copia del archivo de la configuración de inicio que se almacenaba en el servidor. Desgraciadamente, dichos comentarios se ignoran cuando el archivo de configuración se carga en la memoria del router, así que no existe en la NVRAM o memoria de ejecución.

Las versiones más recientes del software IOS han introducido la capacidad de agregar comentarios a los comandos de las listas de acceso numeradas y con nombre asignado.

Para agregar comentarios a las listas de acceso numeradas se usa la palabra clave **remark** en lugar de **permit** o **deny** tras el comando de configuración global de IOS **access-list** y el número de la lista. Los comentarios se pueden colocar en cualquier lugar de la lista de acceso y pueden tener una longitud máxima de 100 caracteres.

```
Router#configure t
Router(config)#access-list [número] remark [comentario]
Router(config)#access-list [número] [permit|deny][protocolo][dirección
origen][dirección destino][condición][protocolo]
Router(config)#^Z
```

Para agregar comentarios a las listas de acceso con nombre asignado, se utiliza el comando de submodo de configuración de listas de acceso IP **remark**. De igual manera que con los estados **permit** y **deny** que se usan en este subcomando, el comando **remark** se utiliza después de entrar en el submodo de configuración de listas de acceso con el comando **ip access-list** seguido del nombre de la lista. Como en el caso de los comentarios de las listas de acceso numeradas, estos comentarios pueden tener una longitud máxima de 100 caracteres.

APLICACIÓN DE LISTAS DE ACCESO

Una vez definidos los criterios de filtrado de la lista de acceso, se deben aplicar a una o más interfaces para que se puedan filtrar los paquetes. La lista de acceso se puede aplicar en dirección entrante o saliente en la interfaz. Cuando una paquete viaja en dirección entrante, entra en el router desde la interfaz. Cuando viajen en dirección saliente, abandonan el router y se dirigen a la interfaz. La lista de acceso se aplica mediante el subcomando de configuración de interfaz de IOS **ip access-group**. Este comando toma como parámetro la palabra clave **in** u **out**. Si no se proporciona un parámetro, se presupone la palabra clave **out**.

```
Router#configure t
Router(config)#interface[tipo][número]
Router(config)#ip access-group [número de lista de acceso] [in|out]
Router(config)#^Z
```

Una vez configuradas, se pueden ver y verificar las listas de acceso con los comandos ejecutables de IOS **show access-list** y **show ip access-list**. El primer comando muestra todas las listas de acceso definidas en el router, mientras que el segundo sólo muestra las listas de acceso IP definidas en el router, mientras que el segundo sólo muestra las listas de acceso IP definidas en el router, ya sean numeradas o con nombre asignado. Cada comando puede tomar como parámetro una lista de acceso numerada o con nombre asignado específica y sólo se puede visualizar el contenido de esa lista. Si se proporciona un parámetro, se mostrarán todas las listas.

```
Router#show access-list
```

Los comandos **show access-list** y **show ip access-list** cuentan el número de coincidencias de cada línea de la lista de acceso y muestra ese número entre paréntesis. Esta información puede resultar útil para determinar las líneas de la lista de acceso que están sirviendo al propósito para el que fueron creadas. También puede ayudar a resolver problemas y revelar los posibles errores de configuración de las listas de acceso.

Los contadores de coincidencias de los comandos **show access-list** y **show ip access-list** se pueden reiniciar con el comando ejecutable de IOS **clear ip access-list counters**. Este comando toma un parámetro opcional del número o nombre de una lista de acceso IP en la que quiera reiniciar los contadores de coincidencias. Si no se especifica un parámetro, se reinician los contadores de coincidencias de todas las listas de acceso IP.

Router#**clear ip access-list counters [número de lista o nombre]**

Es un poco difícil de terminar dónde utilizar las listas de acceso. Cuando se aplican como filtros de paquetes con el comando ip access-group, la salida del comando show ip interfaces muestra las listas de acceso aplicadas y las interfaces en las que se han aplicado.

Cuando las listas de acceso se aplican como filtros de paquetes con el comando distribute-list, la salida del comando show ip protocols indica la aplicación entrante o saliente de los filtros a los protocolos de enrutamiento específicos. Esta explicación de los comandos para ver y verificar las listas de acceso no está completa, porque las listas de acceso funcionan como el activador para muchas de las funciones de filtrado del software IOS. Cada aplicación específica de las listas de acceso tiene sus comandos de verificación correspondientes.

Las capacidades de filtrado de paquetes IP del software Cisco IOS proporcionan herramientas muy poderosas para limitar el acceso a los recursos, tanto dentro como fuera de la red de una entidad. No obstante el diseño de un esquema de protección *firewall* es una tares importante y compleja.

CONFIGURACIÓN DE LOS SERVICIOS BÁSICOS DE ACCESO TELEFONICO POR IP.

El software IOS permite el acceso remoto en los routers y servidores de acceso. La capacidad de acceso remoto se encuentra disponible tanto en el acceso telefónico asíncrono mediante módulos de módems integrados y externos, como a través de RBSI(ISDN). El acceso remoto ofrece a los usuarios y a los routers remotos la capacidad de conectarse con servicios de red IP cuando no están conectados directamente a una red a través de una interfaz de LAN o de WAN.

Hay numerosos productos basados en IOS compatibles con los servicios de acceso remoto. Estos productos ofrecen muchas opciones de configuración, tanto en su hardware como en las características del software IOS.

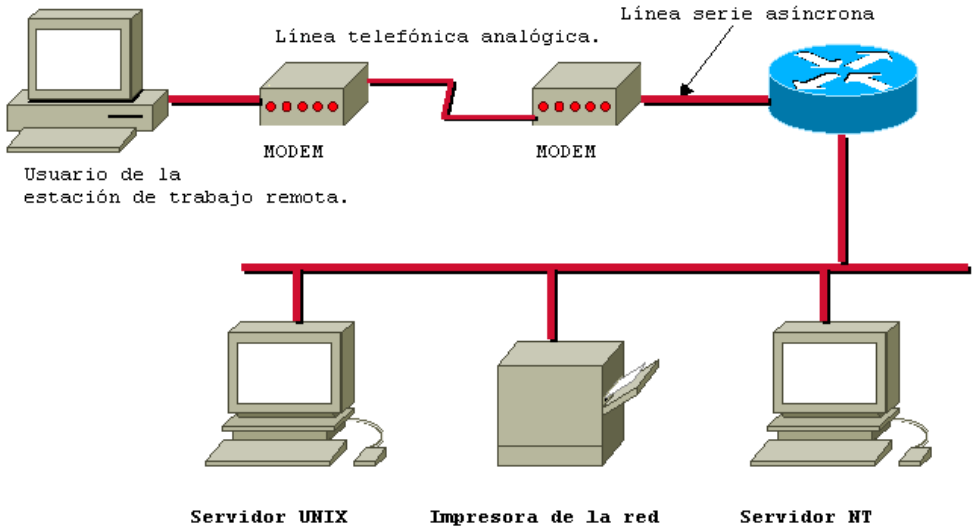
Para asegurarse de la fiabilidad de la conexión a través de un servicio de acceso telefónico, como, por ejemplo un módem o RDSI, IP se transporta en un protocolo de capa de enlace a través del servicio de acceso telefónico. Hay varios protocolos de la capa de enlace de datos compatibles con los servicios de acceso telefónico, entre los que se incluyen PPP, DIC, SLIP(Serial Line IP) y Frame Relay.

La configuración de los servicios de acceso remoto puede dividirse en tres campos principales:

- La configuración de la línea o la interfaz.
- La configuración de la seguridad.
- La configuración del protocolo IP.

CONFIGURACIÓN DE ACCESO TELEFÓNICO ASÍNCRONO

El acceso telefónico asíncrono implica la utilización de módems analógicos para convertir los datos en cadenas de información que se puedan trasladar a través de las líneas telefónicas. Estos módems pueden estar integrados en el producto, como en el caso de servidor de acceso Cisco AS5200 y el router 3600, o bien conectarse externamente, como en el caso del servidor de acceso 2511 y el puerto auxiliar de la mayoría de los routers Cisco.



Hay líneas serie asíncronas físicas conectadas a los módems o líneas virtuales dentro de los módulos de módems integrados, las líneas y los módems deben estar correctamente configurados para asegurar una comunicación adecuada. La velocidad de la línea, el método de control de flujo, la dirección de la llamada telefónica y el tipo de módem conectado son algunos de los aspectos más importantes a configurar.

Para establecer la velocidad a la que el servidor se comunica con los módems, utilizamos el subcomando de configuración de línea de IOS **speed**. El comando toma como parámetro un entero que representa la velocidad, como número de bits por segundo, a la que transmitir y recibir. La velocidad debería establecerse a la mayor que admita el puerto de datos del módem(la mayor velocidad que admite el servidor de acceso es de 115.200 bps).

A fin de definir el método que se utiliza para controlar el flujo de información desde el servidor de acceso a los módems, utilizamos el subcomando de configuración de línea de IOS **flowcontrol**. El comando toma como parámetro la palabra clave **hardware** o **software**. Estas palabras clave representan los dos tipos de control de flujo compatibles. Con velocidades superiores a los 9.600 bps se recomienda el uso de control de flujo del hardware.

```
Router#configure t
Router(config)#line[rango de líneas]
Router(config-line)#speed 115200
Router(config-line)#flowcontrol [hardware | software]
Router(config-line)#^Z
```

Una vez seleccionados los métodos de control de la velocidad y del control de flujo, hay que proporcionarle al servidor de acceso la información relativa al tipo de módem conectado y a la dirección del acceso telefónico. La información sobre el tipo de módem facilita la tarea de configuración de acceso telefónico al eliminar la necesidad de configurar los valores del módem de forma manual. Además, el servidor de acceso puede restablecer los valores del módem tras cada llamada para asegurar el funcionamiento adecuado del conjunto de accesos telefónicos.

La información relativa a la configuración del acceso telefónico le dice al servidor de acceso cómo reaccionar a las señales enviadas por el módem durante el establecimiento de la llamada. El subcomando de configuración de línea de IOS **modem** se utiliza para configurar tanto el tipo de módem conectado como la dirección de acceso telefónico. Para configurar el tipo de módem utilizamos el comando **modem autoconfigure**. Este comando toma como parámetro la palabra clave **discovery** o **type.** La palabra clave **discovery** le da instrucciones al servidor al servidor de acceso para que intente determinar el tipo de módem conectado a fin de seleccionar los valores del mismo. La palabra clave **type**, seguida de uno de los tipos de módem predefinidos o definidos por el usuario, le da instrucciones al servidor de acceso para que seleccione los valores del módem del tipo con nombre.

El software IOS admite muchos tipos de módems, entre los que se incluyen U.S Robotics Courier, el U.S Robotics Sportster Y Telebit T3000. Si no esta definido previamente el tipo, el usuario puede establecer tipos adicionales y los valores correspondientes mediante el comando de configuración de IOS **modencap**. Para establecer la dirección del acceso telefónico usamos como parámetro las palabras clave **dialin** o **inout** con el comando **modem**.

Sugerencia_

Aunque las líneas asíncronas se utilicen solamente para dial-in, le recomendamos que establezca las líneas para operaciones inout durante la configuración inicial y la resolución de problemas. Esto le proporciona acceso al terminal virtual a través del protocolo Telnet directamente a la línea asíncrona para la configuración y la verificación manual del módem. Este método de acceso virtual se conoce como Telnet inverso.

Una vez finalizada la configuración de la línea asíncrona, la seguridad del servidor de acceso es el siguiente paso del proceso de configuración.

La primera es el proceso de autenticación, el proceso de identificar quien intenta acceder. La segunda fase es autorizar al usuario identificado para que realice tareas especificadas o darle al usuario acceso a servicios específicos. Para los propósitos de acceso telefónico por IP, introducimos un tipo de autenticación y un tipo de autorización que hace uso de la información del usuario configurado localmente.

Estos comandos de autenticación y autorización hacen uso de la información del usuario configurada localmente. De manera opcional, podría utilizarse un servidor de acceso como TACACS+ o un RADIUS en lugar de la información configurada a nivel local.

Para autenticar a los usuarios que intentan acceder a los servicios de IP a través de PPP, se utiliza el tipo de autenticación AAA de **ppp**. Se activa mediante el comando de configuración de IOS **aaa authentication ppp**. El comando toma como parámetro un nombre de lista de autenticación o la palabra clave **default** y uno o varios métodos de autenticación, como local o, TACACS+.

Una vez identificado el usuario PPP, hay que autorizar a dicho usuario para que pueda utilizar los servicios de red(uno de los cuales es PPP). Para autorizar el uso de los servicios de la red, utilizamos el comando **aaa authorization network**. Este comando toma como parámetro uno o varios tipos de autorización.

```
Router#configure t
Router(config)# aaa authentication default ppp local
Router(config)# aaa authorization network default if-authenticated
Router(config)#^Z
```

La información de la autenticación para los usuarios PPP se configura a nivel local, por lo que hay que configurar los nombres de usuario y las contraseñas reales para autenticación. Esta información se configura mediante el comando de configuración global de IOS **username.** El comando toma como parámetro la identificación del usuario a utilizar para la autenticación, la palabra clave **password** y la contraseña a utilizar para autentificar al usuario. Aunque la contraseña se escribe en texto perfectamente legible, se convierte en una cadena cifrada si está activado el cifrado de contraseña.

```
Router#configure t
Router(config)#username [nombre de usuario]password [clave]
Router(config)# username [nombre de usuario]password [clave]
Router(config)#^Z
```

El paso final para configurar los servicios de acceso telefónico asíncronos de IP es ofrecer la información sobre el protocolo IP que se usa para establecer y mantener la sesión de acceso telefónico mediante IP. En vez de introducirse la información sobre el protocolo IP como subcomando de línea, la información del protocolo se asocia con el tipo de interfaz que representa la línea asíncrona, igual que con cualquier otro medio LAN o WAN. Este tipo de interfaz se denomina interfaz asíncrona, y cada línea asíncrona del servidor de acceso tiene una interfaz asíncrona correspondiente. La información del protocolo IP puede introducirse individualmente en cada interfaz asíncrona en la que pueden ocurrir sesiones de acceso telefónico, o sólo una vez mediante una interfaz asíncrona colectiva denominada interfaz asíncrona de grupo.

La interfaz asíncrona de grupo puede utilizarse para simplificar las tareas de configuración cuando se apliquen los mismos comandos de configuración a varias interfaces asíncronas. Cuando se utiliza la interfaz de IOS **group-range** para identificar qué interfaces asíncronas individuales deberían incluirse en la estructura del grupo.

La información del protocolo IP que se asigna a las interfaces asíncronas se divide en tres categorías:

- La configuración de la dirección IP para la interfaz asíncrona.
- La información de la dirección IP que se ofrece a los usuarios de acceso telefónico.
- La información relativa a cómo debería funcionar IP y PPP en la interfaz asíncrona.

Empezamos por examinar los comandos de funcionamiento de PPP e IP. En primer lugar hay que indicarle a la interfaz asíncrona que utilice PPP como método de encapsulación para los servicios IP. Para especificar el tipo de encapsulación, utilizamos el comando de configuración de interfaz de IOS **encapsulation**. El comando toma como parámetro una palabra clave(por ejemplo, **ppp**o **slip**) que defina el tipo de encapsulación que se utiliza en la interfaz.

Una vez configurado PPP, el administrador de la red tiene la opción de configurar la línea asíncrona para que funcione solamente como un puerto de servicios de red de acceso telefónico(es decir, al usuario sólo se le permite utilizar los servicios de red configurados en el puerto, como PPP o SLIP) o permitir que el usuario reciba un indicativo ejecutable en el acceso telefónico y elija manualmente que servicio ejecutar. Para especificar el funcionamiento deseado, utilizamos el subcomando de configuración de interfaz de IOS **async mode**. El comando toma como parámetros la palabra clave **interactive** o **dedicated** para definir el funcionamiento deseado.

El nivel de conocimientos del usuario de acceso telefónico y la manera de utilizar la interfaz asíncrona suelen determinar el modo a elegir: interactivo o dedicado. Si se configura un funcionamiento dedicado, se impide que el administrador de la red acceda telefónicamente y se le autorice a utilizar los comandos ejecutables. El modo interactivo puede admitir tanto comandos ejecutables como servicios de red. Sin embargo, el inconveniente del modo interactivo es que los usuarios poco experimentados pueden configurar mal su software de acceso telefónico y situarse en un indicativo ejecutable sin darse cuenta.

Cuando se usa el modo interactivo, un conjunto adicional de comandos de línea simplifica el proceso de acceso telefónico para el usuario. Estos comandos permiten que el servidor de acceso determine el tipo de conexión que se está intentando sin exigir que el usuario especifique el servicio en un indicativo ejecutable. A ese proceso se le denomina selección automática. Se activa mediante el subcomando de configuración de línea de IOS **autoselect**. Este comando toma como parámetro una palabra clave que describe el protocolo de capa de enlace que se seleccionará automáticamente o el momento en que se realiza la selección automática (normalmente en el momento de autenticación del usuario).

Usar la selección automática cuando está configurado el modo interactivo ofrece el método más sencillo para la mayoría de los usuarios para acceder a los servicios PPP e IP en el servidor de acceso.

El último comando de operaciones PPP que se necesita en la interfaz le da instrucciones a PPP para que realice la autenticación y autorización de los usuarios de acceso telefónico antes de establecer los servicios PPP e IP. Así se asegura que sólo obtienen acceso a los servicios de la red disponibles en el servidor de acceso los usuarios autorizados.

Este comando también informa al servidor de acceso del protocolo de autenticación que se van ha utilizar entre el servidor de acceso y el cliente de acceso telefónico. Se pueden usar tres protocolos: Protocolo de autenticación de intercambio de señales de desafio(Challenge Handshake Authentication Protocolo, CHAP), Protocolo de Autenticación de intercambio de señales de desafió de Microsoft (Microsoft Challenge Handshake Authentication Protocolo, MS-CHAP) y Protocolo de autenticación de contraseña (Password Authentication Protcol, PAP).

El subcomando de configuración de interfaz de IOS **ppp authentication** le da instrucciones el servidor de acceso para que realice el proceso de autenticación. El comando toma como parámetro la palabra clave **chap, ms-chap** o **pap** para especificar el protocolo de autenticación. En el mismo comando de configuración es posible especificar un solo protocolo o una combinación de varios si los usuarios de acceso telefónico acceden con varios protocolos de autenticación. El comando toma también una palabra clave opcional, **calling**, que le da instrucciones al servidor de acceso para que lleve a cavo la autenticación inicial solamente en las llamadas de acceso telefónico entrantes. El valor predeterminado es realizar la autenticación inicial tanto en las llamadas entrantes como en las salientes. Las implementaciones de algunos fabricantes no responden a las autenticaciones iniciales si reciben una llamada entrante.

Con el gran número de usuarios de acceso telefónico de Microsoft de hoy en día, el administrador de la red podría elegir añadir compatibilidad con Microsoft Point-to-Point Compresión, (MPPC). La compresión optimiza la transmisión de información a través de un medio como la línea de acceso telefónico, lo que permite que se transmita más información de la que sería posible normalmente. En líneas de acceso telefónico relativamente lentas que funcionan entre 28.800 y 53.000 bps, la compresión puede acelerar la velocidad a la que se transmite la información casi al doble.

La compresión para los usuarios de acceso telefónico se realiza mediante el subcomando de configuración de interfaz de IOS **compress**. El comando **compress** toma como parámetro la palabra clave **mmpc, stac** o **predictor** para indicar el tipo de compresión que se ha de negociar cuando un usuario de acceso telefónico establece una conexión. Las palabras clave **stac** y **predictor** indican la utilización de los algoritmos de compresión STAC o Predictor. STAC es un algoritmo de compresión habitual que admiten muchos clientes de acceso telefónico, incluyendo sistemas de Windows 95 y sería una buena elección si se admite un grupo grande de usuarios de acceso telefónico de Windows 95 o que sean de Microsoft. Predictor es un algoritmo mucho menos habitual. La selección de Microsoft Point-to-Point Compresión se realiza mediante la palabra clave **mppc**. Dado que Windows NT solamente es compatible con MPPC y que Windows 95/98 admite tanto la compresión MPPC como la STAC, la selección de este algoritmo de compresión le ofrece la mayor flexibilidad al administrador de una red que integre varios sistemas operativos de Microsoft.

```
Router#configure t
Router(config)#interface group-async 1
Router(config-if)#group-range 1 16
Router(config-if)#encapsulation ppp
Router(config-if)#async mode interactive
Router(config-if)#ppp authentication chap ms-chap pap callin
Router(config-if)#compress mppc
Router(config-if)#line 1 16
Router(config-line)#autoselect ppp
Router(config-line)#autoselect during-login
Router(config-line)#^Z
```

Teniendo definido el modo operativo de PPP, ahora es posible realizar el direccionamiento IP en las interfaces asíncronas. Normalmente, los usuarios de acceso telefónico por IP sólo cuentan con una dirección IP asociada con sus estaciones de trabajo. Lo podemos contrastar un router de acceso telefónico, que tiene todo un segmento de LAN conectado y necesita realizar enrutamiento con éxito en el sitio central para una comunicación adecuada. Como cada usuario de acceso telefónico individual utiliza una dirección IP en una conexión de acceso telefónico separada y, por tanto, una interfaz asíncrona separada, la dirección IP real de la interfaz asíncrona no resulta importante. De hecho, cada una de las interfaces asíncronas pueden tratarse como si residiera en el mismo espacio de dirección IP en una conexión de acceso telefónico separada y, por tanto una interfaz asíncrona separada, la dirección IP real de la interfaz asíncrona no resulta importante. De hecho cada una de las interfaces asíncronas puede tratarse como si residiera en el mismo espacio de dirección IP que la interfaz de LAN conectada. Estas interfaces asíncronas pueden tratarse incluso como si la dirección IP del usuario de acceso telefónico se asignara desde dicho espacio de dirección. Mirándolo desde una perspectiva diferente, el usuario de acceso telefónico esta conectado lógicamente al segmento de LAN mediante un cable de gran longitud, la línea telefónica. No se asigna ninguna dirección IP a la línea telefónica de la misma forma que una estación de trabajo de LAN se conecta mediante un cable 10BaseT.

La estación de trabajo recibe una dirección IP del mismo espacio de direcciones de red IP que está asignado a la interfaz de LAN del servidor de acceso. El servidor de acceso tiene la responsabilidad de aceptar paquetes desde la LAN en nombre del usuario de acceso telefónico. Dirige dichos paquetes a la llamada telefónica de acceso adecuada. El servidor de acceso logra inyectando una ruta de host(una ruta de red con una máscara de red de 32 bits) en la tabla de enrutamiento del servidor de acceso cuando se establece una conexión de acceso telefónico y respondiendo a solicitudes ARP de las direcciones IP asignadas a las sesiones de acceso telefónico.

Las interfaces asíncronas en si no tienen direcciones IP cuando utilizan el método anterior, así que puede usarse el subcomando de configuración de interfaz de IOS **ip unnumbered** para activar el procesamiento de IP en las interfaces asíncronas.
Se utiliza para especificar la interfaz LAN del servidor de acceso como la interfaz de referencia.

La ultima fase a la hora de establecer la conexión de acceso telefónico por IP en la interfaz asíncrona es configurar qué direcciones IP se asignan a un cliente de acceso telefónico en el momento de la conexión. El subcomando de configuración de interfaz de IOS **peer default ip address** determina el método utilizado para asignar una dirección IP al cliente de acceso telefónico. Especificando una dirección IP en particular como parámetro para el comando, es posible asignar direcciones IP individuales a cada interfaz asíncrona. Sin embargo, se precisa que cada una de las interfaces asíncronas se configure manualmente con la dirección IP que se asignará a los clientes de acceso telefónico que se conecten en esa interfaz.

Un método más flexible consiste en asignar direcciones IP de uno o varios grupos de direcciones que se hayan establecido en el servidor de acceso con el comando **parameter poll**. Este método les ofrece también a los usuarios que han asignado direcciones IP permanentemente la flexibilidad de acceder a cualquier puerto del módem, ya que el servidor de acceso acepta la dirección IP sugerida del cliente de acceso telefónico si se encuentra en un grupo de direcciones predefinido. Cuando se especifica el método de grupos, va acompañado por un nombre específico de grupo de direcciones.

Los grupos de direcciones se definen mediante el comando de configuración global de IOS **ip local poll**. Este comando toma como parámetro un nombre de grupo y las dicciones IP inicial y final que forman dicho grupo. Las direcciones IP deben ser de la misma red IP que la interfaz de LAN del servidor de acceso. Por supuesto, estas direcciones no deberían asignarse a ninguna estación de trabajo que resida en el segmento LAN.

Aunque los grupos de direcciones son el método más flexible para asignar direcciones IP, no existe ningún método para coordinar la asignación a través de varios servidores de acceso. En esta situación, puede resultar mejor asignar direcciones desde un servidor central de autoridad de direcciones, como por ejemplo un servidor DHCP. Para adoptar este método, el software IOS actúa como un cliente DHCP proxy, solicitando una dirección IP del servidor DHCP en nombre del cliente de acceso telefónico. Este método de configuración se activa especificando el parámetro de palabra clave **dhcp** en el comando **peer default ip address**. El servidor de acceso debe estar también configurado con la dirección IP de un servidor DHCP para solicitar direcciones a través del comando de configuración global de IOS **ip dhcp-server**. Los grupos de direcciones definidos en el servidor DHCP contendrían direcciones de la dirección de red IP de la interfaz de LAN del servidor de acceso.

Muchas implementaciones de PPP de clientes de acceso telefónico hacen uso de un método no estándar para obtener direcciones IP de los servidores de nombres DNS y NetBIOS/WINS durante el proceso de establecimiento de la llamada. Este método se describe en la RFC informativa 1877, "PPP Internet Protocol Control Potrocol Extensions for Name server Addresses". Aunque no es un estándar este método se ha instalado profusamente sobre todo en las implementaciones de acceso de Microsoft.

El servidor de acceso puede admitir también los métodos descritos en la RFC 1877 para suministrar tanto las direcciones de nombres de usuario DNS como NetBIOS/WINS. Las implementaciones más antiguas utilizan el comando de configuración global de IOS **async-bootp** para configurar estas opciones. Cuando se configuran las direcciones IP de los servidores DNS, el comando toma como parámetro la palabra clave **nbns-server**, seguida de una o varias direcciones IP.

Nota_

Aunque proporcionar direcciones de los servidores de nombres DNS y NetBIOS/WINS tienen poco que ver con BOOTP, se utilizó el comando **async-bootp** para activar esta característica en el software IOS añadiendo extensiones a los comandos del protocolo de negociación SLIP BOOTP existentes. Este método se eligió en su momento en vez de crear comandos PPP y mecanismos separados para implementar una RFC no estándar.

El inconveniente de usar el comando **async-bootp** para proporcionar direcciones de los servidores DNS y NetBIOS/WINS es que dicho comando es de configuración global de IOS. Esto conlleva que las direcciones configuradas mediante el comando se ofrezcan a todos los usuarios de acceso telefónico del servidor de acceso, sea cual sea la interfaz de acceso a la que puedan estar conectados. Ha demostrado ser un método poco flexible para los administradores de red que desean admitir varios tipos de conexiones de acceso telefónico o diferentes clases de usuarios y que desean proporcionar diferentes direcciones de servidor para dichas conexiones o usuarios. En las versiones más modernas del software IOS, el subcomando de configuración de interfaz de IOS **ppp ipcp** le ofrece al administrador de la red un control más granular de estas opciones por interfaz. Cuando se configuran las direcciones IP de los servidores DNS, el comando toma como parámetro la palabra clave **dns**, seguida de una o dos direcciones IP.

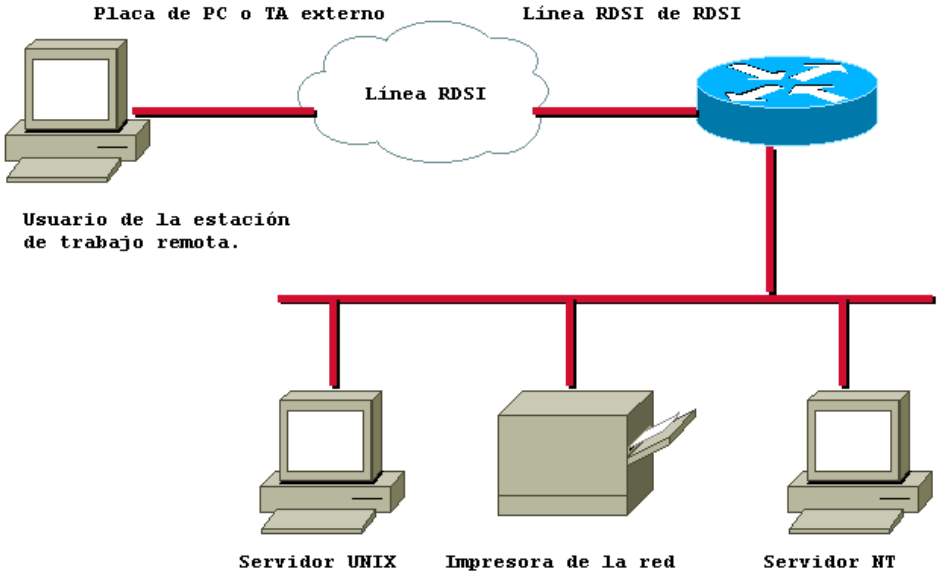
```
Router#configure t
Router(config)#interface group-async 1
Router(config-if)#ppp ipcp dns [dirección ip][dirección ip]
Router(config-if)#ppp ipcp wins [dirección ip]
Router(config-if)#^Z
```

CONEXIONES RDSI(ISDN)

Al igual que el acceso telefónico asíncrono, el acceso RDSI(ISDN) supone la utilización de la red telefónica pública para permitir que los usuarios de las estaciones de trabajo remotas accedan a los servicios de una red cuando no están conectados directamente mediante una interfaz LAN o de WAN. RDSI se diferencia del acceso telefónico asíncrono en que las llamadas se transmiten usando señales digitales síncronas. Los datos se transforman en cadenas de información digital mediante las interfaces RDSI integradas en el router o mediante la utilización de dispositivos de conexión externos RDSI que se denominan adaptadores de terminal (TA).

Los usuarios de las estaciones de trabajo remotas también pueden usar placas de PC RDSI integradas o TA externas para conectarse con el servicio RDSI.

Muchas de las tareas de configuración necesarias para configurar los servicios de acceso telefónico asíncrono por IP se necesitan también para establecer los servicios de acceso telefónico RDSI por IP. Sin embargo, a diferencia de la configuración asíncrona, no se precisan comandos de línea porque el router tiene una interfaz RDSI integrada directamente o porque el TA está conectado directamente a una interfaz serie asíncrona. Si el router tiene una interfaz RDSI integrada, cualquier comando que controle la interacción de la interfaz RDSI con la red RDSI se aplica directamente a la interfaz. Si el router se conecta a la red RDSI mediante un TA externo, se configura a través de sus propios métodos para la correcta interacción con la red RDSI. Esto reduce la configuración de los servicios de acceso telefónico RDSI por IP a dos tareas: establecer la seguridad y definir la información de IP.



Al igual que las interfaces asíncronas, las interfaces RDSI pueden configurarse individualmente o como un grupo. Cuando se configuran como un grupo, los comandos de configuración para las diferentes interfaces RDSI están asociados con un tipo de interfaz denominada interfaz del que realiza la llamada. Las interfaces RDSI individuales se siguen configurando con sus comandos específicos de RDSI, como por ejemplo la información SPID. Sin embargo, los comandos operativos y del protocolo PPP y IP se configuran en la interfaz de quien realiza la llamada. Cada una de las interfaces RDSI incluida en la estructura de interfaces de quien realiza la llamada se configura con el comando **dialer rotary-group**. Este comando toma como parámetro un entero que representa a la interfaz de quien realiza la llamada a la que pertenece la interfaz.

Al igual que con el acceso telefónico asíncrono, la autenticación de PPP y la autorización de red se realizan respectivamente con los comandos de configuración global de IOS **aaa authentication ppp** y **aaa authorization network**. El comando de configuración global de IOS **username** se utiliza para definir los nombres de usuario remotos que acceden a la red.

Al igual que en las interfaces asíncronas, la información del protocolo IP que se asigna a las interfaces RDSI se divide en tres categorías:

- La información relativa a cómo debería funcionar IP y PPP en la interfaz RDSI.
- La configuración de la dirección IP para la interfaz RDSI.
- La información de la dirección IP que se ofrece a los usuarios de acceso telefónico.

Como hemos visto con IP asíncrono, para establecer PPP como protocolo de capa de enlace de datos para IP en las interfaces RDSI usamos el subcomando de configuración de interfaz de IOS **encapsulation.**

La activación de la autenticación de PPP antes de comenzar los servicios de red por IP y la especificación del protocolo de autenticación se realiza con el subcomando de configuración de interfaz de IOS **ppp authentication**. De forma opcional, puede añadirse compresión de Microsoft con el subcomando de configuración de interfaz de IOS **compress mppc**.

RDSI es un servicio canalizado, es decir, que puede admitir varias conexiones a través de la misma interfaz física. Ello permite que los clientes de RDSI de acceso telefónico puedan establecer más de una conexión a la vez con un servidor de acceso. Esta capacidad ofrece a la estación RDSI de acceso telefónico acceso al doble de la capacidad de línea usando una sola interfaz física. La utilización eficaz de varios canales se realiza con una multiplexión de los datos a través de las diferentes conexiones usando un algoritmo de software para PPP denominado multienlace. El multienlace PPP puede activarse mediante el subcomando de configuración de interfaz de IOS **ppp multilink**.

Para controlar cuándo están en funcionamiento o apagados los canales RDSI, se define una lista de paquetes interesantes mediante el comando de configuración global de IOS **dialer-list**. Este comando toma como parámetro protocolos de redes específicas que se deberían considerar interesantes para el propósito de hacer(o mantener) activo un canal. Además, pueden usarse listas de acceso para proporcionar mayor granulidad, a nivel de direcciones IP específicas y de tipos de servio de protocolo de transporte. Las reglas **dialer-list** se aplican a una interfaz a través del subcomando de configuración de interfaz de IOS **dialer-group**, que específica el número de la lista como parámetro del comando.

Nota_

Un mayor control de la asignación del ancho de banda mediante el uso de varios canales RDSI se define en la RFC 2125 "Bandwidth Allocation Protocol (BACP)". El protocolo de asignación de ancho de banda(Bandwidth Allocation Protocol, BAP), que es un subconjunto de BACH, ofrece un conjunto de reglas que rigen la asignación dinámica del ancho de banda por medio de un control de las llamadas (un método estándar para incorporar y eliminar enlaces desde un conjunto multienlace). Los servidores de acceso y los clientes de acceso telefónico negocian las reglas bajo las que se añade o se elimina ancho de banda dinámico durante una sesión. BACH es una característica que se incorporó en la versión 11.4 del software IOS.

La asignación de las direcciones IP de las interfaces RDSI del servidor de acceso y de las estaciones de trabajo de acceso telefónico remoto funciona de la misma forma que con las interfaces asíncronas. No es necesario asignar direcciones IP específicas a las interfaces RDSI del servidor de acceso telefónico RDSI. La interfaz puede configurarse sin numeración mediante el subcomando de configuración de interfaz de Cisco IOS **ip unnumbered.** Es posible asignar las direcciones IP de los clientes de acceso telefónico remoto con cualquiera de los tres métodos examinados anteriormente usando el subcomando **peer default ip addres**.

Entre estos métodos se incluye asignar una dirección IP remota individual asociada con cada una de las interfaces RDSI, usando un grupo de direcciones IP que se asignarán a los clientes RDSI remotos o asignando las direcciones IP obtenidas del servidor DHCP a los clientes RDSI remotos.

También pueden proporcionarse direcciones IP de los servidores de nombres DNS y NetBIOS/WINS a los clientes de acceso telefónico por RDSI usando los métodos de la RFC 1877. Al igual que con las interfaces asíncronas, a los clientes RDSI se les ofrece esas direcciones configurando los comandos de configuración global de IOS **async-bootp dns-server** y **async-bootp nbns-server**, o los subcomandos de configuración de interfaz de IOS **ppp ipcp dns** y **ppp ipcp wins**. Usando cualquiera de los métodos, se ofrecen direcciones IP como parámetros de comandos.

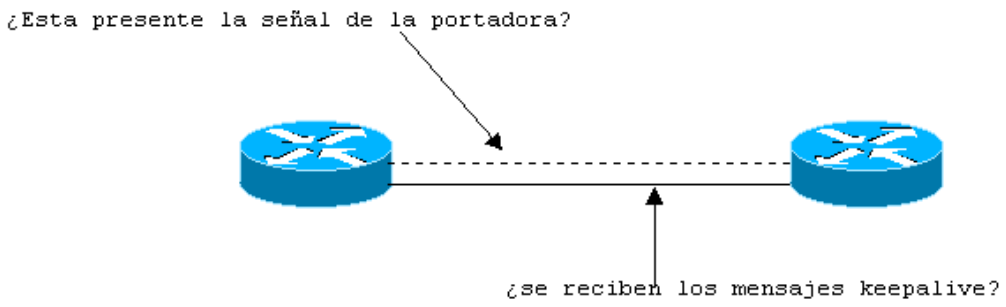
VERIFICACIÓN DE LA CONECTIVIDAD IP Y SOLUCION DE PROBLEMAS.

En algún momento todos los administradores deben solucionar la queja de un usuario que no puede llegar a algún destino de la red. La ausencia de conexión puede ser el resultado de fallos en la red causados por problemas en el servicio WAN, una mala configuración de los routers u otros dispositivos de la red, controles de listas de acceso(intencionados o no) y otras miles de posibilidades. Aunque no existe sustituto para el equipo de prueba de la red, como los analizadores de protocolos, el router, sí se proporcionan varias herramientas de gran utilidad para verificar la conectividad IP e investigar los problemas potenciales.

El router debería de tener una ruta específica o algún tipo de ruta predeterminada o resumen a todos los destinos a los que pueda llegar una estación IP. Una de las mejores herramientas para solucionar los problemas es el comando **show ip route**.

Cuando una estación tiene problemas para conectarse con otras estaciones(ya sea dentro o fuera de la Intranet), uno de los primeros pasos para la resolución de problemas es verificar que el router más próximo al usuario cuenta con una ruta a la dirección IP de destino. Si no se encuentra una ruta específica o si no está presente la ruta predeterminada o resumen esperada, probablemente haya que investigar los protocolos de enrutamiento dinámico para determinar porque no está presente la ruta.

¿EL ENLACE ESTA OPERATIVO?



Hardware(nivel físico)
- Cable
- Conectores
- Interfaces

Nivel de enlace de datos
- Mensajes keepalive
- Información de control
- Información de usuario

Sh controle int Comprueba a nivel físico cuando una interfaz esta down.

COMANDO PING

Si se establece que existe una ruta hacia el destino deseado, se debería probar para determinar si el router puede llegar el destino. Los usuarios de UNÍS están familiarizados con el comando **ping**, que es un acrónimo de **Paket Internet Groper**. El comando **ping**, que se ejecuta en el router, hace uso del Protocolo de control de mensajes IP(IP Control Message Protocol, ICMP) para enviar peticiones de eco a una dirección IP de destino. La estación que recibe la petición de eco ICMP envía una respuesta de eco ICMP. De esta manera, una estación origen puede determinar si se puede contactar con la estación de destino y cuanto tiempo tarda aproximadamente la petición de eco y la respuesta en llegar y volver de la estación de destino.
El router envía un número de peticiones de eco ICMP e informa mediante el signo exclamación(!)que se reciben todas las respuestas. También informa del número de intentos de peticiones de eco y del número de respuestas de eco recibidas, además de calcular el porcentaje de pings que han tenido éxito. También se calculan los tiempos mínimos y máximos y medios de respuesta.

Nota_
Cuando un router hace un ping a una dirección IP por primera vez o tras un prolongado periodo de tiempo, no suele recibir la primera respuesta de eco, lo que tiene como consecuencia que se respondan cuatro de las cinco respuestas al ping. Esto se debe a que el router debe esperar una resolución ARP de la dirección IP antes de enviar las respuestas de eco. Normalmente, la respuesta ARP no llega a tiempo para que se enviéé la primera petición de eco y se reciba la respuesta antes de que expire el tiempo de la petición.

DIFERENTES CARACTERES DE RESPUESTA QUE SE PUEDEN RECIBIR COMO RESULTADO DE UN PING.

! Cada signo de exclamación indica la recepción de una respuesta.
La respuesta de eco se recibió satisfactoriamente.

. Cada punto indica que el servidor de la red agoto el tiempo esperando una respuesta.
La petición de eco seguramente llegó al destino, pero éste no consiguió responder o no tenía una ruta de regreso al origen de la petición.

U No se puede acceder al destino.
La dirección IP de destino no coincide con una dirección MAC o no permite peticiones de eco ICMP. El router emisor ha recibido un mensaje "destination unreachable" de ICMP.

N No se puede acceder a la red.
No hay ruta a la red de destino para la dirección IP de destino.
El router emisor ha recibido un mensaje "network unreachable" de ICMP.

Q Se solicita que deje de enviar el origen.
La dirección IP de destino esta recibiendo más paquetes de los que puede almacenar en la memoria intermedia. El destino a enviado al router un mensaje "source quench" de ICMP diciéndole al remitente que retroceda.

M No se pudo realizar la fragmentación.
Un paquete ha excedido la unidad máxima de transmisión de un segmento de la red en la ruta hacia el destino y se ha activado el bit no fragmentar. El router emisor ha recibido un mensaje "could no fragment" de ICMP.

A No se puede acceder administrativamente al destino.
Se ha descartado el paquete a la dirección de destino al encontrar un filtro de paquetes o un firewall. El router emisor ha recibido un mensaje "administratively unreachable" de ICMP.

? El paquete es de tipo desconocido.
El router emisor ha recibido una respuesta desconocida a la petición.

El comando Ping tiene tanto versión privilegiada como no privilegiada. En el modo ejecutable de usuario, la versión no privilegiada solamente permite que el usuario especifique una dirección IP. La versión privilegiada, disponible con el modo ejecutable activado, permite que el usuario modifique parámetros de la petición de eco, incluyendo el número de peticiones, el tamaño de los paquetes enviados, el valor del tiempo de espera, la dirección IP de origen de la petición, el modelo de datos de la petición de eco y otros muchos valores.

Si se sospecha que la falta de conectividad se debe a la ausencia de una ruta en el router de flujo descendente o a que un paquete está tomando una ruta incorrecta, el router cuenta con un comando denominado **trace** que permite verificar la ruta que sigue un paquete hasta alcanzar la dirección IP de destino. La función **trace** es similar a la utilidad **traceroute** de UNÍS. Al igual que el comando ping, el comando ejecutable de IOS **trace** tiene tanto versión privilegiada como no privilegiada. LA versión privilegiada permite que el usuario modifique los parámetros, al igual que con el comando ping.

La función trace hace uso del mensaje "TTL-Expired"(Time To Live) para identificar los routers en una ruta hacia la dirección IP de destino. El router de origen envía un paquete UDP con un TTL de 1 hacia el destino. El primer router de la ruta recibe el paquete y disminuye el campo TTL en 1. En consecuencia, el TTL expira (llega a 0) y el router no reenvía el paquete. En su lugar, este primer router de la ruta devuelve un mensaje "TTL-Expired" de ICMP al origen del paquete, de modo que éste conoce ahora el primer salto de router de la ruta.

El router de origen envía ahora otros paquetes UDP, pero establece el TTL en 2. El primer router de la ruta recibe el paquete, disminuye el TTL a 1 y reenvía el paquete al segundo router de la ruta. El segundo router recibe el paquete, disminuye el TTL a 0 y no reenvía el paquete porque ha espirado el TTL. El segundo router devuelve un mensaje "TTL-Expired" de ICMP a la estación origen y ahora el router de origen conoce el segundo router de la ruta. Este proceso continua hasta que el paquete llega a la dirección IP de destino final. El paquete se dirige a puertos UDP con número alto, normalmente superior a 33434, que no admite el dispositivo de destino. Por tanto , la dirección IP de destino responde con un mensaje "Port unreachable" de ICMP, que alerta al router de origen de que se ha llegado al destino final.

Los valores del tiempo que aparecen tras el nombre y las direcciones IP de los routers en la ruta de red, representan una aproximación del tiempo de ida y vuelta transcurrido desde la dirección de origen del router de la ruta. Para cada dirección IP de destino aparecen hasta tres valores de tiempo, uno por cada uno de los tres paquetes(sondas). Algunos dispositivos tienen limitaciones en la velocidad a la que pueden responder con mensajes ICMP. En dichos dispositivos podrían aparecer menos de tres valores de tiempo. Por cada sonda que no responde al dispositivo por limitaciones de velocidad, aparece un asterisco en lugar del valor de tiempo.

Además de limitar la velocidad de los mensajes ICMP es posible que algunos routers de la ruta no respondan con un mensaje "TTL-Expired" de ICMP. Algunos pueden volver a usar el TTL del paquete entrante, lo que provoca la caducidad del TTL del mensaje ICMP antes de que el mensaje pueda regresar al remitente. Y en algunos casos, los filtros de paquetes pueden evitar que los paquetes de respuesta de ICMP llegen al router de origen. En todos estos casos en la línea de salida se ve una línea de asteriscos en vez de la información de la dirección.

La versión privilegiada del comando **trace** permite el ajuste de los parámetros del comando, incluyendo si las direcciones IP se resuelven de forma inversa a los nombres de host, el número de sondas enviadas por cada fase TTL, un valor mínimo y máximo de TTL, etc.

Si una estación a la que se puede acceder mediante una interfaz de LAN conectada directamente no responde, la razón puede ser que el router no sea capaz de asignar la dirección IP a la dirección MAC.

Para comprobar las direcciones MAC que el router ha sido capaz de resolver, utilizamos el comando ejecutable de IOS **show ip arp**. Este comando toma como parámetro una dirección IP específica, una interfaz específica o una dirección MAC de 48 bits específica. Sólo muestra las entradas ARP para dicho parámetro. Si no se introduce ningún parámetro, aparecen todas las entradas ARP de IP.

La salida del comando incluye la asignación IP de ARP, la antigüedad de la entrada en la tabla y la interfaz a la que está asociada la entrada ARP(el router elimina una entrada ARP de la tabla ARP tras cuatro horas de manera predeterminada).

Las estadísticas generales sobre el funcionamiento del protocolo IP en el router pueden obtenerse con el comando **show ip traffic**. Incluye contadores para información como el número total de paquetes recibidos y enviados por el router, el número de transmisiones recibidas y enviadas, estadísticas de protocolo ICMP/UDP/TCP y muchas más cosas.

Estas estadísticas pueden ayudar a determinar si el router ha enviado o recibido un eco ICMP, si una dirección IP no logra resolver una dirección MAC(lo que se conoce con un fallo de encapsulación) y donde se están enviando o recibiendo ciertos paquetes de protocolos de enrutamiento. Los comandos de **show ip traffic** son acumulativos y solamente se ponen a cero cuando se vuelve a cargar o reiniciar el router.

Los contadores de la salida de **show ip traffic** cuentan tanto los eventos que han ocurrido como los tipos de paquetes que se han enviado y recibido. Si los contadores de fallos de encapsulación aumentan, indicaran que el router no ha recibido respuestas ARP a sus peticiones ARP para los paquetes que intercambian conmutarse a las interfaces de destino y que éstos se descartaron. El contador de echos ICMP indica cuántos pings está generando el router, mientras que el contador de contestaciones de echos indica el número de pings al que está respondiendo.

Existen numerosos comandos ejecutables de IOS **debug** para ayudar a determinar el funcionamiento de IP en el router. Estos comandos **debug** ofrecen una salida de diagnostico tanto general como detallada que pueden ayudar a la hora de solucionar problemas y comprobar el funcionamiento del router, los protocolos de enrutamiento y otras funciones.

COMANDOS DEBUG PARA IP

Debug ip routing
Muestra los cambios que ocurren en la tabla de enrutamiento como resultado de incorporaciones y supresiones de rutas.

Degug ip packet
Muestra las direcciones IP de origen y destino de los paquetes que atraviesan el router. Este comando **debug** puede sobrecargar al router, así que debe usarse con precaución. Se recomienda que se utilice una lista de acceso junto con este comando para limitar la carga de la CPU.

Debug ip udp
Muestra los paquetes UDP enviados al router

Debug ip icmp
Muestra los paquetes ICMP enviados al router y generados por él.

Debug arp
Muestra las peticiones ARP generadas por el router y las respuestas enviadas a él.

Los comandos de depuración de los distintos protocolos de enrutamiento dinámico son, entre otros: **debug ip rip, degug ip eigrp, debug ip igrp, debug ip ospf** y **debug ip bgp.**
Todos ellos tienen parámetros opcionales que controlan qué información de depuración del protocolo de enrutamiento ve el usuario. Hay que tener mucho cuidado al utilizar algunas de las versiones de estos comandos, ya que utilizan muchos recursos de la CPU.

Sugerencia_

Cuando se utilicen los comandos **debug**, que se sabe que aumentan la carga de la CPU, no los ejecute en el puerto de la consola. En su lugar, desactive el registro de la consola mediante el comando de configuración global de IOS no **logging buffered**. A continuación ejecutamos el comando desde una sesión de terminal virtual y vemos la salida de dicha sesión. Si la sesión no responde, puede usarse la consola para desactivar la depuración, ya que ésta tiene mayor prioridad que la sesión de terminal virtual. La salida de depuración puede verse entonces en el búfer del registro mediante el comando ejecutable de IOS show log. Si esta activado syslog, también puede verse la salida del archivo de registro del servidor syslog.

CONFIGURACIÓN DE LOS SERVICIOS DE DENOMINACIÓN DE DOMINIO.

En las redes TCP/IP actuales, la mayoría de la gente hace referencia a los servidores, las impresoras, las estaciones de trabajo y otros dispositivos IP por sus nombres más que por sus direcciones IP. Recordar las direcciones IP puede resultar fácil para el administrador de la red que esta muy familiarizado con ella, pero para el usuario medio, resulta más sencillo recordar el nombre de un sistema. Para este fin, los servidores que convierten los nombres en direcciones IP, denominados servidores del Servicio de denominación de dominio (Domain Name Service, DNS), suelen residir en algún lugar de la Intranet de una entidad. Los routers pueden hacer uso del sistema DNS para convertir los nombres en direcciones IP y para ayudar a reducir el número de direcciones IP que debe recordar el administrador.

DNS suele venir activado en el software Cisco IOS. Sin embargo, si se ha desactivado, puede restablecerse mediante el comando de configuración global de IOS **ip domain-lookup**. Una vez activado DNS, debería configurarse un dispositivo IOS con el nombre de domino en el que resida y con la dirección IP de los servidores de nombres DNS que pueda utilizar para la resolución de nombres.

El nombre de dominio puede configurarse mediante el comando de configuración global de IOS **ip domain-name**.

El servidor(es) de nombres DNS puede configurarse mediante el comando de configuración global de IOS **ip name-server**. El comando **ip name-server** toma una o varias direcciones IP de servidores de nombres como parámetros. Si el dispositivo IOS reside dentro de varios dominios DNS, puede usarse el comando de configuración global de IOS **ip domain-list** para especificar una lista de nombres de dominio que deberían ser postergados a nombres inhábiles.

Para comprobar la configuración del DNS en el router, podemos utilizar el comando ejecutables de IOS **show host**. Además, el comando **show host** muestra una lista de hosts a los que se les ha convertido el nombre a dirección IP y también la antigüedad de cada entrada.

Las asignaciones de nombres de host a dirección IP pueden también configurarse de manera estática en el router en las situaciones en las que no se encuentren disponibles los servidores DNS, se prefiera crear nombres especiales diferentes a los DNS o se

desee asignar puertos de servidores terminales individuales a direcciones IP.

La asignación de nombre estático a dirección IP se configura con el comando de configuración global de IOS **ip host**. El comando **ip host** toma como parámetros un nombre de host, un puerto opcional del protocolo Telnet y una o varias direcciones IP a las que se puede convertir el nombre de host.

Las asignaciones estáticas de nombre de host a dirección IP pueden verificarse también mediante el comando **show host**.

Las entradas estáticas de la tabla de nombres de host pueden distinguirse de las que se conocen mediante DNS por el campo **Flags** para la entrada del nombre de host. Un tipo de indicador **Temp.** Indica que el nombre se conoció de forma dinámica mediante DNS y ha salido temporalmente de la tabla tras un periodo de tiempo. Un tipo de indicador **perm** indica que el nombre se configuró estáticamente y nunca se suprimirá de la tabla con el tiempo.

Las entradas temporales de la tabal de host IP pueden borrarse mediante el comando ejecutable de IOS **clear host**. Las asignaciones individuales de nombres de host pueden borrarse introduciendo un nombre de host como parámetro para el comando. Si se introduce un asterisco como parámetro, pueden borrarse todas las entradas de host temporales.

REENVÍO DE DIFUSIÓN IP

Una de las ventajas que ofrecen los routers en una red es la restricción de los paquetes de difusión IP y MAC al segmento de LAN local. La mayoría de las difusiones se utilizan para solicitar información como una dirección MAC desconocida para una dirección IP (ARP) en un segmento local, por lo que aislar las difusiones al segmento de LAN local no presenta problemas inherentes y es altamente beneficioso para el rendimiento de la red.

En algunas situaciones las estaciones IP utilizan las difusiones UDP para localizar servicios que pueden no estar en el segmento de LAN local. Por ejemplo, las aplicaciones que utilizan NetBIOS sobre IP usan difusiones UDP para localizar el tipo de servicio particular que necesita el usuario. Si el servicio reside en un segmento de LAN que no sea al que está conectado la estación del usuario, el router bloquea la difusión, con lo que el servicio deja de estar disponible. Otros servicios, como DCHP y Bootstrap Protocol (BOOTP), envían difusiones UDP para ayudar a las estaciones IP a determinar sus direcciones IP durante el proceso de inicio; las difusiones las reciben servidores que asignan direcciones.
Si dichos servidores residen fuera del segmento de LAN local, una estación IP no puede recibir una dirección IP asignada por el usuario.

Para compensar las características de aislamiento de la difusión del router, el software IOS tiene la capacidad de reenviar difusiones UDP a un host o subred específica. Esta característica, que se denomina reenvío de difusión de IP, se activa utilizando el subcomando de configuración de interfaz de IOS **ip helper-address** y el comando de configuración global de IOS **ip forward-protocol**.

Una aplicación habitual de estos comandos es reenviar las peticiones de direcciones DCHP desde un segmento de LAN local al segmento de LAN en el que reside el servidor DCHP.

Para activar el reenvío de difusiones, podemos aplicar el comando **ip helper-address** a los segmentos en los que el router recibe las difusiones. El comando **ip helper-address** toma como parámetro una dirección IP de host de host o una dirección IP de difusión. La dirección que se introduce es una dirección de host del servidor DCHP específico o la dirección de difusión del segmento de LAN en el que reside el servidor DCHP.

En vez de reenviarse directamente al servidor DCHP, la difusión podría reenviarse al segmento de LAN en el que reside el servidor DCHP. Esta alternativa resulta de gran utilidad cuando hay más de un servidor DCHP que podría contestar a la petición.

El comando **ip helper-address** se utiliza para especificar dónde se deberían reenviar las difusiones. El comando **ip forward-protocol** se utiliza para controlar qué emisiones UDP se reenvían. De manera predeterminada, se reenvían varios tipos de difusión UDP siempre que se aplica a la interfaz el comando **ip halper-address**:

- Protocolo de transferencia de archivos trivial(trivial File Transfer Protocol, TFTP) (puerto 69).
- Sistema de denominación de dominio(puerto 53).
- Servicio de tiempo(puerto 37).
- Servidores de nombres NetBIOS(puerto 137).
- Servidor de datagramas NetBIOS(puerto 138).
- Datagramas de clientes y servidores del protocolo Boot(BOOTP)(puertos 67 y 68).
- Servicio TACCS(puerto 49).

Si hay una aplicación que emita en un puerto que no aparezca en la lista y hay que reenviar sus difusiones, utilizamos el comando **ip forward-protocol** para especificar que el tipo de difusión particular debería incluirse entre los que se reenvían. Con la incorporación de la palabra clave **no**, también es posible utilizar este comando para restringir que se reenvíe cualquiera de los protocolos predeterminados. El comando **ip forward-protocol** toma como parámetro el tipo de reenvío a realizar(como por ejemplo, UDP) y el número de puerto específico de protocolo a reenviar.

La configuraciones de **ip helper-address** se puedenverificar con el comando **show interface**.

Nota_
Otras referencias: otras aplicaciones de difusión

La técnico de reenvío de difusión que hemos visto esta diseñada para satisfacer las demandas de un entorno de reenvío de difusión limitado. Se ajusta a la perfección a tareas como el reenvío de peticiones de direcciones IP mediante DCHP o BOOTP a un servidor o grupo de servidores que residan en una ubicación central de la red.

Existen otras aplicaciones para las que se puede necesitar un reenvío de más considerable. Estas aplicaciones suelen utilizar difusiones para compartir información entre un elevado grupo de usuarios de estaciones de trabajo a través de una gran parte de la red. Dichas aplicaciones no son muy convenientes para el modelo de direcciones helper. En su lugar, necesitan técnicas avanzadas, como el desbordamiento de UDP y la duplicación difusión a multidifusión, para evitar que se inunde la CPU del router por el trafico y la duplicación de paquetes de difusión.

ASIGNACIÓN DE DIRECCIONES DINÁMICAS CON UN SERVIDOR DCHP DE IOS.

En la sección anterior tratamos el reenvío de peticiones de asignación de direcciones DCHP como una de las aplicaciones para el reenvío de difusión de IP. Cuando un router reenvía estas peticiones de asignación de dirección, se dice que actúa como un agente de retransmisión DCHP. El papel del agente de retransmisión DCHP es recibir las difusiones locale de las LAN para la asignación de direcciones y reenviarlas a un servidor DCHP identificado previamente. El servidor DCHP suele ser una estación de trabajo o un servidor como un sistema UNIX o Windows NT que ejecuta un paquete de software o un servicio de servidor DCHP. De forma alternativa, un router o un servidor de acceso basado en IOS puede servir como fuente para las asignaciones dinámicas de direcciones.

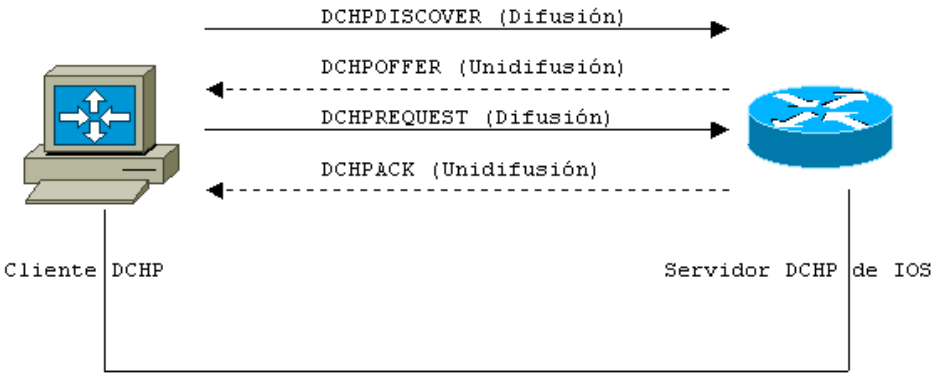
El servidor DCHP del software IOS funciona de forma similar a los servidores DCHP basados en estaciones de trabajo, aceptando peticiones/renovaciones de asignación de direcciones y asignando las direcciones desde grupos predefinidos de direcciones denominados conjuntos. Los conjuntos de direcciones pueden configurarse para proporcionar información adicional al cliente que lo solicite, como la(s) dirección(es) de los servidores DNS, el router predeterminado y otro tipo de información útil. El servidor DCHP de IOS pueden aceptar difusiones de segmentos LAN conectados a nivel local o de peticiones DCHP que hayan reenviado otros agentes de retransmisión DCHP dentro de la red.

Nota_

Aparte del servidor DCHP basado en el software IOS, Cisco Systems fabrica un servidor DNS y DCHP basado en estaciones de trabajo denominado Cisco Network Registrar que se ejecuta en sistemas operativos como Solaris, HP-UX y Microsoft Windows. Para tomar la decisión de utilizar el servidor DCHP basado en IOS o un servidor DCHP basado en estaciones de trabajo, hay que tener en cuenta muchos factores, incluyendo el tamaño de la red, el número de nodos que necesitan direcciones dinámicas, la frecuencia de las peticiones y renovaciones de direcciones, la necesidad de redundancia y los costes. En general, el servidor DCHP basado en IOS es más práctico en redes pequeñas o de mediano tamaño para un modelo descentralizado, como, por ejemplo varias oficinas remotas. Los servidores DCHP basados en estaciones de trabajo son más apropiados para grandes organizaciones que necesiten redundancia y un esquema de administración muy centralizado.

El servidor DCHP de IOS participará normalmente en dos fases del proceso de asignación de direcciones: la DHCPOFFER y la DHCPACK.

Cuando un cliente DHCP solicita una dirección del servidor DCHP. El cliente DCHP envía un mensaje de difusión DHCPDISCOVER para localizar a un servidor DCHP. Un servidor DCHP ofrece parámetros de asignación de direcciones al cliente en una respuesta de unidifusión DCHPOFFER. El cliente DCHP le devuelve entonces un mensaje de difusión formal DCHPREQUEST para la asignación de direcciones ofertada al servidor DCHP. El servidor DCHP envía una respuesta de unidifusión DCHPPACK para indicar que las direcciones solicitadas se le han asignado al cliente. Los cuatro pasos que se ilustran en la figura representan el proceso normal de negociación de direcciones sin errores ni conflictos. El proceso completo de asignación de direcciones, incluyendo el tratamiento de los mensajes DCHPDECLINE, se describe en la RFC 2131, "Dynamic Host Configuration Protocol".



Asignación de direcciones DCHP por un servidor DCHP.

Para activar que el router basado en IOS o el servidor de acceso Haga de servidor DCHP, hay que realizar cuatro fases de configuración principales:

- Identificar la ubicación para registrar la información de las asignaciones DCHP.
- Crear una lista de direcciones IP que excluir de la asignación dinámica.
- Crear un conjunto de direcciones que utilizar para la asignación dinámica.
- Añadir atributos adicionales a los conjuntos de direcciones que se proporcionarán a las estaciones que lo soliciten.

El primer paso para activar el servidor DCHP de Ios es configurar una ubicación en la red para registrar y almacenar las asignaciones de direcciones DCHP (denominadas también conjuntos). Esta ubicación suele ser una estación de trabajo o un servidor que admita TFTP, FTP o el protocolo de transferencia de archivos RCP.

Especificar esta ubicación permite que el router o el servidor de acceso se reinicie sin perder información sobre que direcciones están asignadas a qué sistemas de cliente DCHP.

Además, proporciona una ubicación para registrar los conflictos de asignación de direcciones que pueden surgir durante el proceso de negociación de DCHP. Para especificar la ubicación, utilizamos el comando de configuración global de IOS **ip dchp database**. El comando toma como parámetro un URL que especifica la dirección y el nombre de archivo de servidor que utiliza para el registro. El comando de configuración puede repetirse varias veces para determinar el almacenamiento de varios conjuntos en múltiples servidores.

Durante el de asignación de direcciones, el servidor DCHP de IOS pretende asegurar que la dirección IP que se ofrece no está en uso. Lo hace enviando una serie de paquetes ping a la dirección que se ofrece antes de responder al cliente DCHP. Si la dirección está en uso, se registra como un conflicto y no se ofrece hasta que el administrador de la red lo resuelve.

Si no hay ningún servidor disponible para el registro de conjuntos de direcciones DCHP y el comando **ip dchp database** no está configurado, también debe desactivarse el registro de los conflictos DCHP. La desactivación del registro de conflictos se lleva a cabo con el comando de configuración global de IOS **no ip dchp conflict logging**.

Cuando se establece una ubicación para registrar los conjuntos, se crea una lista de direcciones que se deberían excluir como asignaciones ofertadas de forma dinámica. Esta lista incluye la dirección de los routers en un rango de direcciones determinado, cualquier dirección asignada de manera estática o una dirección que debería estar reservada y no ofrecerse a ningún cliente DCHP. Para construir estas listas, utilizamos el comando de configuración global de IOS **ip dchp excluded-address**. El comando puede representar las direcciones inicial y final de un rango de direcciones IP. El comando puede repetirse varias veces en la configuración para excluir varias direcciones IP que no sean continuas o que abarquen varios conjuntos de asignación de direcciones IP.

El paso final para activar el servidor DCHP de IOS es la definición de los conjuntos de asignaciones de direcciones IP que se utilizan para proporcionar las direcciones dinámicas. Como mínimo, el conjunto de direcciones DCHP especifica el rango de direcciones que se ofrecerán a los clientes DCHP que soliciten direcciones (sin incluir las direcciones excluidas). Es posible definir más de un conjunto en el servidor DCHP de IOS si hay varios segmentos de LAN conectados al router o servidor de acceso que actúa como servidor DCHP o si sirve direcciones para varios segmentos de LAN en cualquier parte de la red.

El comando de configuración global de IOS **ip dchp pool** establece un conjunto de asignaciones de direcciones. El comando toma como parámetro o una cadena arbitraria que describa el conjunto, o un número entero. Una vez definidos, los comandos de conjuntos de direcciones adicionales se introducen desde el modo de subcomando de configuración de DCHP, que denota el indicador **(config-dchp)#**.

El subcomando de configuración DCHP de IOS **network** se utiliza para definir el rango de direcciones que ofrecerá a los clientes DCHP un determinado conjunto de direcciones. El subcomando **network** precisa dos parámetros, una dirección de red IP y un máscara de red o máscara de recuento de bits. Las direcciones de red y las máscaras especificadas para un conjunto determinado deberían corresponderse con la dirección de red y la máscara del segmento de LAN para las que ofrecerá direcciones este conjunto. Cuando el servidor DCHP proporcione direcciones para varios segmentos de LAN, deberían definirse conjuntos DCHP separados, cada uno con un comando **network** con la dirección y la máscara apropiada para dicho segmento de LAN.

Otros subcomandos de configuración de DCHP permiten que el administrador de la red configure el servidor de IOS de forma que proporcione información suplementaria al cliente DCHP utilizando el proceso de negociación de direcciones. La información adicional suele ser la(s) dirección(es) del router predeterminado del cliente en el segmento de Lan, las direcciones de los servidores DNS, las direcciones de los servidores NetBIOS/WINS y otro tipo de información que tendría que configurar manualmente en cada uno de los clientes bien el usuario, bien el administrador de la red. La siguiente es la lista de los subcomandos de configuración DCHP que se configuran más frecuentemente:

- Subcomando **domain-name**. Especifica el nombre del dominio DNS al que pertenece este cliente.
- Subcomando **dns-server**. Especifica una o varias direcciones IP de los servidores DNS que puede solicitar el cliente para resolver los nombres de direcciones IP.
- Subcomando **netbios-name-server**. Especifica una o varias direcciones IP de servidores NetBIOS/WINS a los que pueden preguntar los clientes NetBIOS(normalmente estaciones de trabajo de Microsoft) para localizar los recursos de red.
- Subcomando **default-router**. Especifica una o varias direcciones IP de un router predeterminado a las que los clientes pueden reenviar los paquetes para los destinos desconocidos.
- Subcomando **lease**. Especifica cuánto tiempo es válida una dirección asignada DCHP (un contrato) antes de necesitar renovación.

Los subcomandos **dns-server, netbios-name-server** y **default-router** toman como parámetros de una u ocho direcciones IP con las que puede contactar el cliente para cada una de dichas funciones. El subcomando **domain-name** toma como parámetro una cadena arbitraria que representa el nombre del dominio DNS para el cliente. El subcomando **lease** toma como parámetros hasta tres enteros para especificar el número de días, horas y minutos que es válida una dirección asignada.

También puede usarse la palabra clave **infinite** para especificar que un contrato es válido un periodo limitado de tiempo. El subcomando **netbios-node-type** toma como parámetro los valores de los caracteres b, p, m, o h, que representan un nodo de difusión de NetBIOS, un nodo igual a igual, un nodo mixto o un nodo híbrido , respectivamente, para indicar el modo operativo del cliente. Si no esta familiarizado con estos modos operativos, se recomienda seleccionar el modo híbrido.

Como mencionamos anteriormente, es posible configurar varios conjuntos de direcciones DCHP en el mismo servidor DCHP de IOS. A la colección del conjunto de direcciones DCHP en dicho servidor se la conoce como base de datos DCHP. La base de datos DCHP está organizada en una estructura jerárquica o de árbol, de modo que un conjunto de direcciones puede ser una subred de la dirección de red del conjunto de direcciones DCHP diferente. La estructura jerárquica permite que las propiedades las herede el conjunto de direcciones, que es una subred de la otra. Las propiedades comunes a varios conjuntos deberían definirse como el nivel de red o de subred más alto apropiado para el servidor DCHP o la red que se esta configurando.

Cuando estén definidos los conjuntos de direcciones y sus propiedades, y el servidor DCHP de IOS haya comenzado a asignar direcciones IP, se puede verificar el funcionamiento del servidor DCHP utilizando varios comandos ejecutables de IOS. La verificación de que el servidor DCHP de IOS registra la información de las asociaciones y los conflictos en la estación de trabajo o servidor configurado se realiza a través del comando ejecutable de IOS **show ip dchp database**. Este comando utiliza como parámetro la dirección URL para mostrar la información acerca de una ubicación específica para las bases de datos del registro. Si no se introduce ninguna, aparece la información de todas las ubicaciones.

La salida del comando **show ip dchp database** indica la ubicación en la que se escribe la información de las asociaciones, la fecha y hora en la que se leyó o se escribió por última vez en la base de datos de asociaciones, el estado de la última lectura o escritura, y el número de veces que se ha conseguido o no escribir en la base de datos de asociaciones.

Es posible ver determinadas asignaciones de direcciones con el comando ejecutable de IOS **show ip dchp binding**. Si se introduce en el comando una dirección IP como parámetro opcional, sólo se mostrará la información de las asociaciones de dicha dirección; en caso contrario, aparecerá la de todas.

La información de los conflictos de direcciones que se han producido cuando el servidor DCHP de Ios intentaba asignar una dirección a un cliente DCHP se pueden ver con el comando **show ip dchp conflic**. Si se introduce en el comando una dirección IP como parámetro opcional, sólo se mostrará la información de los conflictos de dicha dirección (si hay información); en caso contrario, aparecerá la de todas.

La columna **Detection Meted** indica qué método ha utilizado el servidor DCHP de IOS para determinar que la dirección estaba en conflicto. El método de detección ping indica que antes de la asignación de direcciones, el servidor DCHP de IOS ha intentado hacer un ping a la dirección y ha recibido una respuesta correcta. El método de detección Gratuitous ARP indica que antes de la asignación de direcciones, el servidor DCHP de IOS ha detectado una entrada ARP activa y válida para la dirección en su tabla ARP. Cualquiera de estos métodos de detección indica que es posible que la dirección se esta utilizando(quizás a causa de un uso no autorizado o porque alguien olvidó añadirla a la lista de direcciones excluidas).

La verificación de que el servidor DCHP de IOS está recibiendo y respondiendo a las solicitudes de DCHP se puede lograr con el comando ejecutable de IOS **show ip dchp server statistics**. El comando ofrece información útil, como el número de conjuntos de direcciones configuradas, la cantidad de memoria que consume la base de datos de asociaciones de DCHP y los contadores que indican el número de distintos tipos de mensajes de DCHP que se han enviado y recibido.

REDUNDANCIA DE IP CON EL HOST STANDBY ROUTER PROTOCOL

A mochos administradores de red le preocupa tener puntos de fallo únicos en la red. Desean proporcionar tanto rutas de acceso redundantes como equipo redundante en lugares clave de la red para evitar que cualquier dispositivo cause que los recursos vitales de la red dejen de poder utilizarse. Los routers(y algunos servidores) gestionan perfectamente varias rutas de acceso IP mediante el intercambio de información de enrutamiento acerca de las distintas rutas de acceso de la red, seleccionando las mejores rutas de acceso en cualquier momento y volviendo a enrutarlas cuando haya algún cambio en las rutas de acceso a causa de algún fallo del circuito o del equipo.

Si embargo, muchas implementaciones de las estaciones de trabajo, de los servidores y de las impresoras no pueden intercambiar información de enrutamiento dinámico. Estos dispositivos se suelen configurar con la dirección IP del gateway predeterminado, que sirve como conducto al resto de la red. Si falla el router que es el gateway predeterminado, el dispositivo se limita a comunicarse solamente con el segmento local de red IP y está incomunicado con el resto de la red. Aunque exista un router redundante que pudiera servir como gateway predeterminado, no hay método dinámico que pueda utilizar las estaciones de trabajo para conmutar a otra dirección IP del gateway predeterminado y la reconfiguración manual suele desbordar los conocimientos técnicos del usuario.

Para ayudar a los administradores de redes en esta problemática situación, Cisco Systems ha desarrollado el Hot Standby Router Protocol (HRSP). HRSP se ha desarrollado para el segmento LAN, donde hay una gran cantidad de routers y dispositivos que utilizan solamente una dirección IP estática del gateway predeterminado.

El concepto de SEP es bastante simple. El administrador crea una dirección virtual para el gateway predeterminado y la asigna a los routers redundantes que participan en el protocolo SEP en el segmento LAN específico. Los dispositivos IP están configurados para utilizar la dirección virtual del gateway como gateway predeterminado. Los routers administran esta dirección, comunicándose entre ellos para determinar que router es el responsable del reenvío del trafico enviado a la dirección IP virtual. A intervalos regulares, intercambian información para determinar que routers siguen estando presentes y son capaces de reenviar trafico. Si falla el router principal, o primario, de un grupo de routers con SEP, hay un router de reserva en el mismo grupo que empieza a reenviar el tráfico del grupo SEP. Dado que los routers deciden por si mismos cuál reenvía el trafico a la dirección virtual y dado que las estaciones de trabajo de un segmento sólo conocen la dirección Ip virtual como su gateway predeterminado, un fallo del router de reenvío principal es prácticamente indetectable por parte de los usuarios de estaciones de trabajo y no requiere intervención por parte del usuario o del administrador de la red.

HSRP es muy flexible. El administrador de red puede controlar todo el comportamiento de los routers de un grupo SEP (incluyendo que router es el router de reenvío principal, cuales son los routers de reserva, si éstos conservan la función de reenvío cuando pueda volver a utilizarse el router de reenvío principal, y la capacidad de otra interfaz del router para conducir el trafico al router de reserva).

La presencia de dos o más routers que pueden actuar como gateway predeterminados en el mismo segmento de LAN es la primera parte de los criterios para configurar el protocolo SEP. La otra parte de los criterios es tener dispositivos IP en la red que sólo puedan admitir una sola dirección IP como gateway predeterminado. En este caso, las impresoras, los servidores y las estaciones de trabajo se ajustan a los criterios.

La configuración básica de SEP requiere solamente el subcomando de configuración de interfaz de IOS **standby ip**. Este comando utiliza como parámetro la dirección IP que se utiliza como dirección virtual del gateway predeterminado. El comando se aplica a todos los routers de la misma red IP lógica que participen en el mismo grupo HSRP.

Una vez que este configurada la dirección de reserva de HSRP, los routers negocian cuál de ellos será el router de reenvío principal, y cual el de reserva. Además, ambos routers introducen en la tabla ARP la dirección IP y la dirección MAC de la dirección virtual. El router de reenvío principal comienza el reenvío del tráfico enviado a la dirección IP virtual de reserva, así como la respuesta a pings y la aceptación de las sesiones de los terminales virtuales de dicha dirección. Observe que la dirección MAC de la dirección IP virtual de las interfaces Ethernet, Fast Ethernet, Gigabit Ethernet y FDI tiene la forma 0000.0c07.acXX donde XX es un identificador de grupos HSRP. La dirección MAC de la dirección IP virtual de Token Ring es una dirección funcional con la forma 1000.xxxx.xxxx.

Sugerencia_

Algunos dispositivos de Token Ring no aceptan la dirección MAC de un dispositivo IP como dirección funcional de grupo. En este caso utilice el subcomando de configuración de interfaz de IOS **standby use-bia** para obligar a la dirección IP virtual de HSRP a utilizar la dirección impresa en el hardware de la interfaz, que limita el número de grupos HSRP de la interfaz a una.

Como ya se ha indicado, el administrador de red tiene varias opciones de configuración que controlan el comportamiento de HSRP. Para controlar cuál es el router de reenvío principal, se utiliza el subcomando de configuración de interfaz de IOS **standby priority**. El comando adopta como parámetro un valor entre 0 y 255. El router del grupo HSRP que tenga la prioridad más alta se convierte en el router de reenvío.

Si el router de reserva tiene que convertirse en el activo, asume automáticamente dicho papel. Es posible controlar si el primer router principal reanuda su papel de reenvío activo cuando pueda volver a utilizarse. El subcomando de interfaz de IOS **standby preempt** hace que el router reanude la función de reenvío activo a partir de otro router con prioridad más baja.

En algunas situaciones, el estado operacional de una interfaz afecta directamente al router que se elige como router de reenvío activo. Esto ocurre en particular cuando cada uno de los routers del grupo HSRP tiene una ruta de acceso distinta a otras partes de la red.

El software IOS ofrece una característica de HSRP para que un router pueda ajustarse a la prioridad HSRP de un grupo HSRP de forma que se pueda convertir en el router de reenvío activo. Esta funcionalidad, recibe el nombre de seguimiento de interfaces, se activa con el subcomando de configuración de interfaz de IOS **standby trac**. Este comando adopta como parámetro la interfaz a la que se le va a realizar el seguimiento y opcionalmente, la cantidad que hay que reducir de la prioridad HSRP en la interfaz configurada. Si no se especifica ningún valor de reducción de prioridad, el router deduce la cantidad estándar de diez de la prioridad HSRP.

El funcionamiento de HSRP puede verificarse con el comando ejecutable de IOS **show standby**. El comando adopta como parámetro opcional la interfaz específica en la que se va ha mostrar la información la información de HSRP. Sin dicho parámetro la información de HSRP aparece en todas las interfaces.

El comando **show standby** muestra la información de HSRP, que incluye el estado de los reenvíos, la prioridad HSRP y las interfaces a las que realizan seguimientos del router al que se realizan consultas. También muestra información acerca de la dirección IP de reserva configurada y las direcciones IP de los posibles routers de reserva de cada grupo HSRP.

Una de las desventajas del HSRP original era que no permitía al administrador de red compartir la carga del tráfico que cruza ambos routers del grupo de reserva. Básicamente, el router de reserva estaría inactivo a menos que fallará el router de reenvío activo.

Para solucionar este problema, se añadió al software IOS la capacidad para admitir varios grupos HSRP en la misma interfaz. En la misma interfaz se pueden crear varios grupos HSRP, cada uno de ellos con una dirección IP virtual distinta, para respaldarse unos a otros.

Con dos grupos HSRP y dos direcciones IP virtuales definidas, el administrador de red puede configurar el gateway predeterminado en algunos de los host con una de las direcciones virtuales de HSRP, y en los host restantes, con la otra. Aunque no consigue un equilibrado de la carga exactamente igual, esta configuración comparte la carga entre los dos routers en lugar de sobrecargar sustancialmente uno de ellos mientras el otro se queda completamente inactivo.

Mediante la especificación de un número de grupo en todos los comandos **standby**, se pueden crear varios grupos HSRP. Por ejemplo, **standby 1 ip address [dirección IP]** y **standby 1 priority 100** especifican que estos comando HSRP se aplican al grupo de reserva 1. Los comandos **standby 2 ip address [dirección IP]** y **standby 2 priority 100** especifican que estos comando HSRP se aplican al grupo de reserva 2.

RESUMEN DE COMANDOS EJECUTABLES PARA IP

clear host
Elimina las entradas temporales de la tabla de host IP.
Clear ip access-list counters
Borra el cómputo del número de veces que ha coincidido cada una de las líneas de una lista de acceso IP.
Clear ip route
Borra toda la tabla de enrutamiento o, si se especifica, una ruta en particular.
Ping ip-address
Realiza pruebas para determinar si se puede comunicar con la dirección IP que se indica y si ésta responde.
Show {frame-relay | atm | x25 | dialer} map
Muestra las asignaciones de direcciones IP a direcciones de enlace de datos en el tipo de medios de WAN especificado.
Show access-list
Muestra todas las listas de acceso definidas en el router
Show host
Verifica la configuración DNS de un router y muestra una lista de host que han resuelto sus nombres a direcciones IP.
Show interface[interfaz]
Proporciona información general acerca de una interfaz, incluyendo la dirección IP y la máscara de red.
Show ip access-list
Muestra todas las listas de acceso IP definidas en el router.
Show ip arp
Muestra todas las direcciones IP que el router ha podido resolver a direcciones MAC.
Show ip dchp binding
Muestra información acerca de las asignaciones de direcciones de direcciones del servidor DCHP de IOS.
Show ip dchp conflict
Muestra la información acerca de los conflictos de direcciones IP que detecta el servidor DCHP de IOS durante el proceso de asignación.

Show ip dchp database
Muestra información acerca de la ubicación y estado de la base de datos que ha utilizado el servidor DCHP de IOS para registrar las asociaciones y conflictos de DCHP.
Show ip dchp server statistics
Muestra información sobre el estado y los contadores relacionados con el funcionamiento del servidor DCHP de IOS.
Show ip interface brief
Muestra un pequeño resumen de la información de las direcciones IP y el estado de todas las interfaces disponibles en el dispositivo.
Show ip interface[interfaz]
Muestra todos los parámetros asociados con la configuración de una interfaz IP.
Show ip mask [dirección de red]
Muestra las máscaras de red que se han aplicado a la red designada y el número de rutas que utiliza cada máscara.
Show ip protocols
Muestra los protocolos de enrutamiento que están ejecutando y varios de sus atributos. Si se utiliza con la palabra clave **summary**, muestra solamente los nombres de los protocolos y los números de los identificadores de los procesos.
Show ip route
Muestra la tabla de enrutamiento IP del router.
Show ip route connected
Muestra las rutas asociadas con las interfaces del router operacionales conectadas directamente.
Show ip route[dirección IP]
Muestra la información de enrutamiento de la ruta especificada.
Show ip route static
Muestra las rutas que se derivan de los comandos de rutas de red configurados manualmente.
Show ip traffic
Presenta las estadísticas globales de funcionamiento de IP en el router.
Show standby
Muestra información sobre el funcionamiento de HSRP.
Terminal ip netmask-format{decimal | bit-count | hexadecimal}
Especifica el formato de visualización de las máscaras de red que se van a utilizar durante la sesión de la consola o del terminal virtual existente.
Trace[dirección IP]
Muestra todos los pasos de ruta de acceso a la red por los que viajan los paquetes para llegar a la dirección IP indicada.

RESUMEN DE COMANDOS DE CONFIGRACIÓN PARA IP

aaa authentication ppp [método de lista]
especifica que ppp debe autenticarse a través del método aaa de la lista.
aaa authorization network [método]
especifica que los servicios de red deben autenticarse a través del método de aaa de la lista.
access-list
crea una lista de acceso numerada y sus criterios de filtros asociados.

arp-server
identifica el servidor arp de atm que pueden resolver direcciones ip en direcciones nsap de atm.
async-bootp dns-server[dirección ip]
especifica direcciones ip de un servidor dns proporcionadas a los clientes de acceso telefónico durante el establecimiento de llamadas de forma global.
async-bootp nbns-server[dirección ip]
especifica las direcciones ip de un servidor de nombres netbios/wins proporcionadas a los clientes de acceso telefónico durante el establecimiento de llamadas de forma global.
async mode{interactive | dedicated}
especifica el método de interacción del usuario en una interfaz asíncrona para los usuarios de acceso telefónico.
autoselect ppp
especifica que el proceso de selección automático debe realizarse durante el proceso de autenticación.
compress
especifica que el algoritmo de compresión debe intentar negociarse durante la negociación del acceso telefónico por ppp.
default-metric
asigna la métrica de enrutamiento que se va a utilizar durante la redistribución de rutas entre los protocolos de enrutamiento dinámicos.
defaul-router[dirección]
define una o varias direcciones ip predeterminadas del router que ofrece a los clientes dchp el servidor dchp de ios.
dialer-group[entero]
especifica el grupo de marcadores al que pertenece una interfaz y específica qué lista de marcadores se utiliza para definir el tráfico de interés.
dialer-list[número de lista]protocol[método de tipo]
Define una lista de marcadores que especifica los protocolos de red y métodos que se utilizan para definir el tráfico como interesante para las sesiones de acceso telefónico.
dialer map ip
Asigna una dirección ip al nombre de sistema y al número de teléfono para las llamadas rdsi.
dialer rotary-group[entero]
Asigna una interfaz rdsi a la estructura del grupo de la interfaz de quien realiza la llamada.
distribute-list
Aplica una lista de acceso a la tares de filtrar la recepción y la publicación de las rutas de red.
dns-server[dirección]
Define una o varias direcciones ip del servidor dns que ofrece a los clientes dchp el servidor dchp de ios.
domain-name[dominio]
Define un nombre de dominio dns que ofrece a los clientes dchp el servidor dchp de ios.
flowcontrol{hardware | software}
Especifica el método de control de flujos en una línea asíncrona.

Frame-relay map ip
Asigna una dirección IP a un DLCI Frame Realy
Group-range [principio fin]
Específica que interfaces asíncronas se incluyen en las estructuras de interfaces del grupo asíncrono.
Ip access-group list{in | out}
Aplica la lista de acceso indicada a la tarea de filtrar paquetes entrantes o salientes en una interfaz.
Ip access-list{extended | standard}[nombre]
Crea una lista de acceso IP con nombre y sus criterios de filtrado asociado.
Ip address [dirección ip][máscara de red]
Asigna una dirección IP y una máscara de red a las interfaces de LAN y de WAN.
Ip classless
Activa el router para que funcione en modo sin clase, en el que las direcciones IP de destino coinciden con las rutas de la superred y de los bloques CIDR.
Ip default-information originate
Hace que OSPF genere la ruta predeterminada desde el router límite de sistema autónomo para el resto del dominio OSPF.
Ip default-network[dirección de red]
Configura la dirección de red especificada como red de resumen o predeterminada.
{no}ip dchp conflict logging
Activa o desactiva el registro de la información de los conflictos de direcciones por parte del servidor DCHP de IOS.
ip dchp database[dirección URL]
Define la ubicación y método para registrar la información de las asociaciones y de los conflictos de direcciones por parte del servidor DCHP de IOS.
ip dchp exclude-address
Especifica una o varias direcciones IP que deben excluirse de las ofertas de DCHP a los clientes DCHP por parte del cliente DCHP de IOS.
ip dchp poll[nombre]
Crea un conjunto de direcciones DCHP que se puede configurar con otros subcomandos de configuración DCHP.
ip dchp-server[dirección IP]
Especifica la dirección IP de un servidor DCHP que puede asignar dinámicamente direcciones IP a los clientes de acceso telefónico.
ip domain-list[nombre]
Establece una lista de nombres de dominios que añadir a los nombres de host no cualificados.
ip domain-lookup
Activa el DNS.
domain-name[nombre]
Configura el nombre del dominio principal que añadir a los nombres de host no cualificados.
ip forward-protocol udp type
Controla que tipo de difusiones UDP se reenvían.
ip helper-address[dirección IP]
Reenvía difusiones UDP a la dirección IP especificada.
ip host
Configura la asignación estática de un nombre de host a las direcciones IP.

ip local pool{default | poll-name}[dirección IP de inicio y dirección IP de final]
Crea un conjunto de direcciones IP para asignar dinámicamente direcciones IP a los clientes de acceso telefónico.
ip dchp-server[dirección ip]
Configura servidore de nombres DNS.
ip netmask-format{decimal | bit-count | hexidecimal}
Configura el formato de visualización de las máscaras de red que se va a utilizar durante las sesiones de las consolas o de los terminales virtuales.
ip ospf network{broadcast | non-broadcast | point-to-multipoint}
Configura el tipo de red(difusión, no difusión o punto a multipunto) que OSPF cree que está conectada ala interfaz.
ip rip {send | receive} versión
Especifica que versión de RIP se envía y recibe en una interfaz específica.
ip route 0.0.0.0 0.0.0.0 [dirección ip de destino]
Configura una ruta predeterminada de 0.0.0.0.
ip route [dirección de red][máscara de red][dirección ip de destino]
Configura una ruta estática
ip route [dirección de red][máscara de red][dirección ip de subred]
Configura un ruta resumen, adoptando como parámetros la ruta resumen, la máscara de red y la subred no conectada.
ip routing
Activa el enrutamiento IP del router.
Ip subnet-zero
Permite asignar una interfaz a la primera subred del conjunto de direcciones de red(subred cero).
Ip unnumbered [interfaz]
Configura una interfaaz IP de WAN punto a punto no numerada
Map-group
Asigna un grupo de asignación con nombres a una interfaz para que lo use a la hora de asignar direcciones IP a las direcciones de enlace de datos ATM en una interfaz.
Map-list
Crea un lista de asignación con nombres para configurar la asignación de direcciones IP a los PVC o SVC en el direccionamiento ATM.
modem autoconfigure{discover | tipo de módem}
Especifica que un módem conectado a una línea asíncrona debe configurarse automáticamente por descubrimiento por el uso de los parámetros del tipo de módem con nombre.
modem {dialin | inout}
Especifica la dirección permitida de las llamadas asíncronas.
neighbor[dirección IP]
Especifica la dirección IP de un router vecino con el que intercambiar información de enrutamiento dinámico.
neighbor[dirección IP]description
Permite añadir comentarios al comando **neighbor** de BGP.
neighbor[dirección IP]distribute-list
Permite el filtro de rutas BGP a igual BGP.
neighbor[dirección IP]remote-as asn
Configura el router vecino con la dirección indicada en el sistema autónomo indicado como igual BGP.
neighbor[dirección IP]update-source[interfaz]
Especifica que la dirección IP de origen para establecer la sesión de igual BGP debe derivarse de la interfaz con nombre.

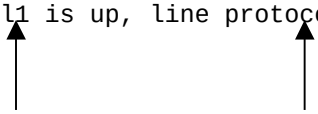
netbios-name-server[dirección]
Define una o varias direcciones IP del servidor NetBIOS/WINS que ofrece a los clientes DCHP el servidor DCHP de IOS.
netbios-node-type[tipo]
Define el modo de comportamiento de NetBIOS que ofrece a los clientes DCHP el servidor DCHP de IOS.
network[dirección de red]
Especifica que las direcciones conectadas que coincidan con la dirección de red indicada deben incluirse en las publicaciones del enrutamiento.
network[dirección de red]area [número de área]
Especifica que las interfaces conectadas que coincidan con la dirección de red indicada deben incluirse en las publicaciones del enrutamiento OSPF y que las interfaces deben asignarse al área especificada.
network[número de red][máscara | longitud del prefijo]
Especifica el conjunto de direcciones IP que se ofrecerán a los clientes DCHP de un conjunto de direcciones DCHP determinado por parte del servidor DCHP de IOS.
no autosummary
Evita el resumen automatico de direcciones en los limites de la red con clase y permite la propagación de la información de la subred.
no inverse-arp
Desactiva la función de asignación de la dirección IP a DLCI de Frame Relay.
passive-interface[interfaz]
Configura el router para escuchar pero no publicar la información de enrutamiento en la interfaz indicada.
peer default ip address{pool | dchp | dirección IP}
Especifica el método que se ha utilizado para asignar una dirección IP a una estación de trabajo cliente de acceso telefónico.
Ppp authentication[método]
Especifica que debe realizarse la autenticación PPP antes de permitir que den comienzo los servicios de red. Entre el servidor de acceso y el cliente de acceso telefónico se utiliza el protocolo de autenticación de nombre.
Ppp ipcp{dns | wins}
Especifica las direcciones IP de los servidores DNS o NetBIOS/WINS que se proporcionan a los clientes de acceso telefónico durante el establecimiento de sesiones PPP a través de interfaz.
Ppp multilink
Especifica que debe activarse la multiplexión de canales basada en software en una interfaz.
Redistribute protocol
Permite la redistribución de rutas desde el protocolo indicado.
Router{rip | igrp | ospf | eigrp |bgp}
Permite al router ejecutar el protocolo de enrutamiento dinámico.
Speed [bits por segundo]
Especifica la velocidad de transmisión de una línea asíncrona.
Stanby ip[dirección ip]
Configura la dirección IP indicada como dirección IP virtual de un grupo HSRP.
Standby preempt
Hace que un router HSRP de mayor prioridad reanude el reenvío activo cuando vuelva a estar disponible.

Standby priority[prioridad]
Asigna un valor de prioridad a un router HSRP para controlar la selección del router de reenvío principal.
Standby track[interfaz]
Activa el ajuste dinámico de la prioridad HSRP basándose en el estado operacional de la interfaz especificada.
Standby use-bia
Obliga a la dirección IP virtual de HSRP a asociarse con la dirección MAC impresa en el hardware de una interfaz.
{no}synchronization
Activa o desactiva el requisito de que las rutas se conozcan a través del proceso de enrutamiento de IGP antes de publicarlas a los vecinos EBGP.
username[nombre][password][palabra]
Define la pareja nombre de usuario local/contraseña que se va a utilizar para autenticar a los usuarios de acceso telefónico.
versión[versión de RIP]
Especifica la versión de RIP que se utiliza en un router con RIP activo.
x25 map ip
Asigna una dirección IP a una dirección X.121.

INTERPRETAR SHOW INTERFACE

Router#show int s1

Serial1 is up, line protocol is up



Operativo Serial is up, line protocol is up
Problema de conexión Serial1 is up, line protocol is down
Problema de interface Serial1 is down, line protocol is down
Dehabilitado Serial is administratively down, line protocol is down

La siguiente tabla define muchos de los elementos sobre los que se informa cuando se usa el comando **show interfaces:**

Five-minutes rates(input or output)(Intervalos de cinco minutos)(entrada o salida)

El promedio de bits y paquetes que pasan por la interfaz cada segundo, muestreados durante los últimos cinco minutos.

Aborts(Cancelaciones)

Terminación repentina de los paquetes de transmisión de un mensaje.

Buffer failures(Fallos del buffer)

Paquetes desechados por falta de disponibilidad de memoria búfer del enrutador.

BW

Ancho de banda de la interfaz en kilobits por segundo(Kbps). Esto se puede utilizar como una métrica de protocolo de enrutamiento.

Bytes

Número total de bytes trasmitidos a través de la interfaz.

Carrier transitions(Transacciones de portadora)

Una portadora es la señal electromagnética modulada por las transmisiones de datos sobre líneas serie(como el sonido que emite el módem). Las transiciones de portadora son eventos donde se interrumpe la señal, a menudo cuando se reinicia la NIC remota.

Collisions(Colisiones)

Número de mensajes retransmitidos debido a una colisión Ethernet.

CRC

Comprobación de redundancia cíclica, una técnica común para detectar errores de transmisión. CRC funciona dividiendo el tamaño del contenido de una trama por un número primo y comprobando el resto con el que hay almacenado en la trama por el nodo emisor.

DLY

Demora del tiempo de respuesta de la interfaz, medido en microsegundos(ns), no en milisegundos(ms).

Dibble conditions(Condiciones de exceso)

Tramas que son ligeramente demasiado largas, pero que las sigue procesando la interfaz.

Drops(Caídas)

Número de paquetes desechados por falta de espacio en la cola.

Encapsulation(Encapsulación)

Método de encapsulación asignado a una interfaz(si existe). Funciona ajustando los datos en la cabecera de un protocolo para <tunelizar> los datos que de otra forma serían incompatibles a través de redes externas. Por ejemplo, Inter.-Switch Link de Cisco ISL; Enlace entre conmutadores encapsula tramas de muchos protocolos.

Errors(input or output) Errores entrada o salida

Una condición en la que se descubre que una transmisión no coincide con lo que se esperaba, normalmente está relacionado con el tamaño de la trama o del paquete. Los errores se detectan usando varias técnicas, como CRC.

Frame(Trama)

Número de paquetes que tienen un error de CRC y un tamaño de trama parcial. Suele indicar que el dispositivo Ethernet funciona incorrectamente.

Giants(Gigantes)

Paquete mayor que el paquete de tamaño máximo que permite la tecnología, 1.518 bytes o más en las redes Ethernet. Todos los paquetes gigantes se desechan.

Ignored(Ignorado)

Número de paquetes desechado por la interfaz por falta de búfer de memoria del búfer de la interfaz(en contraposición con la memoria búfer del enrutador).

Interface resets(Reinicios de Interfaz)

Cuando la interfaz se deshace de todos los paquetes y comienza con uno nuevo. El reinicio suele ocurrir cuando el nodo emisor tarda demasiado en transmitir los paquetes.

Keepalives(Mensajes de supervivencia)

Mensajes enviados por un dispositivo de red a otro para notificarle que el circuito virtual entre ellos sigue activo.

Last input or output(Última entrada o salida)

Horas, minutos, y segundos desde que la interfaz transmitió o recibió con éxito el ultimo paquete. Es una buena herramienta para determinar cuándo ha comenzado el problema.

Load(Carga)

Carga de la interfaz como una fracción del número 255. Por ejemplo, 64/255 representa un 25 por 100 de la carga. Se puede utilizar este contador como una métrica del protocolo de enrutamiento.

Loopback(Ciclo invertido)

Si se ha activado el ciclo invertido. Loopback es donde envían las señales desde la interfaz y, luego, se devuelvan a ella desde algún punto de la ruta de comunicaciones; se utiliza para probar el uso del enlace.

MTU

Unidad de transmisión máxima para paquetes que pasan a través de la interfaz, expresado en bytes.

Output hang(Bloqueo de salida)

Tiempo transcurrido desde el último reinicio de la interfaz. Toma su nombre del hecho de que la interfaz <se bloquea> porque la transmisión tarda demasiado tiempo.

Overruns(Saturaciones)

Número de veces que la interfaz del enrutador satura el nodo receptor enviando más paquetes de los que pueden manejar el búfer del nodo. Toma su nombre del hecho de que la interfaz del enrutador <satura> al emisor.

Queues(input and output) Colas(entrada y salida)

Número de paquetes en la cola. El número a continuación de la barra invertida es el tamaño máximo de la cola.

Queuing strategy(Estrategia de encolamiento)

FIFO significa First In, First Out(Primero en entrar primero en salir), que significa que el enrutador maneja paquetes en ese orden LIFO significa Last In, First Out(Último en entrar, primero en salir). FIFO es la estrategia predeterminada.

Rely(Confianza)

Fiabilidad de la interfaz como una fracción del número 255. Por ejemplo, 255/255 equivale al 100 por 100 de fiabilidad. Se puede utilizar este contador como una métrica del protocolo de enrutamiento.

Runts(Diminutos)

Paquete menor que el tamaño del paquete mínimo que permite la tecnología, 64 bytes o menos en las redes Ethernet. Todos los paquetes diminutos se desechan.

Throttles(Aceleradores)

Número de veces que una interfaz avisa a una NIC emisora que está siendo saturada por los paquetes que se envían y para reducir el ritmo de envío. Toma su nombre del hecho de que la interfaz pregunta a la NIC que <desacelere>.

Underruns(Agotamientos)

Número de veces que el nodo emisor satura la interfaz enviando más paquetes de los que puede manejar el búfer. Toma su nombre del hecho de que la interfaz del enrutador <agota> al emisor.

CONECTARSE A TERMINALES VIRTUALES UTILIZANDO TELNET Y SSH.

Los métodos más habituales para acceder a cualquier dispositivo en el que se ejecuta IOS son a través del puerto de la consola o a través de líneas de terminales virtuales(virtual terminal lines, vty). Estas líneas son un tipo de software que permiten conectarse a un router a través de una red de datos. Los dispositivos IOS admiten cinco sesiones simultáneas a través de líneas de terminales virtuales.

Los dos métodos más frecuentes para conectarse a una línea de terminal virtual son el uso de un cliente Telnet o el uso de un cliente Secure Shell(SSH). Los clientes Telnet utilizan un protocolo estándar definido en RFC 854 para proporcionar una conexión no segura al software de servidor que se ejecuta en una línea de terminal virtual. Por defecto, todos los dispositivos con IOS tienen un servidor Telnet habilitado en todas las líneas de terminales virtuales.

SSH es un protocolo que proporciona una conexión cifrada segura entre un cliente y un servidor SSH que funcionen en una línea de terminal virtual con funciones que sean similares a una conexión Telnet. En contraste al servidor Telnet, los servidores SSH no están habilitados por defecto en las líneas terminales virtuales.

Ciertos dispositivos IOS pueden ser clientes Telnet o clientes SSH, para lo que se utilizan los comandos Telnet o SSH.

Nota_
Actualmente, hay dos versiones de SSH: SSH versión 1 y SSH versión 2. En estos momentos, Cisco IOS sólo admite la primera de ellas.

Los clientes y servidores SSH pueden realizar la autenticación de usuarios a través de un sistema criptográfico con claves públicas que inventaron Rivest, Shamir y Adelman (RSA). La autenticación de usuarios RSA de los clientes SSH no es compatible con el servidor SSH de Cisco IOS. Cisco IOS autentica a los usuarios utilizando solamente una combinación de ID de usuario y contraseña. El servidor SSH de IOS utiliza RSA para generar la pareja de claves que se utiliza para configurar sesiones cifradas en el cliente.

SSH asegura la conexión entre el cliente y el servidor SSH utilizando el algoritmo de cifrado DES(56bits) o Triple DES(168bits). Sin embargo, no todas las versiones de IOS admiten DES o Triple DES y, a veces hay que utilizar el comando **show versión** para ver si la versión de IOS que se utiliza admite estos algoritmos de cifrado.

Nota_
Algunos algoritmos de cifrado (entre los que se incluye el cifrado de datos de 56 bits) están sujetos a los controles de exportación del gobierno de Estados Unidos. El uso de estos algoritmos (y de la versión de IOS que los admite) fuera de Estados Unidos requiere una licencia de exportación.

ACTIVACIÓN DEL SERVIDOR SSH

Para activar el servidor SSH y permitir a los clientes SSH conectarse a líneas de terminales virtuales, el dispositivo con IOS debe tener un nombre de *host* y nombre de dominio configuran con los comandos de configuración global **hostname** e **ip domain-name**, que ya se han explicado.

Para configurar el servidor SSH, hay que generar una pareja de claves de RSA que se utiliza para cifrar la sesión entre y el servidor. En el dispositivo con IOS, la pareja de claves de RSA se genera utilizando el comando de configuración global **crypto key generate rsa**. Al generar una pareja de claves de RSA para el dispositivo con IOS, se activa automáticamente el servidor SSH en las líneas de terminales virtuales. Para suprimir una clave de RSA se utiliza comando de configuración global **crypto key zeroize rsa**, que desactiva automáticamente el servidor SSH.

Nota_
El comando de configuración global **crypto key generate rsa** no aparecerá en la salida por pantalla de **show running-config** ni de **startup-config**.

```
Router#configure t
Router(config)#crypto key generate rsa
Router(config)#ip ssh
Router(config)#ctrl.+Z
```

VERIFICACIÓN DE LA CONFIGURACIÓN DE SSH

La clave de RSA pública que utiliza SSH se puede ver con el comando ejecutable **show crypto key mypubkey rsa**:

Además es posible ver las sesiones de SSH activas de cualquier dispositivo con IOS utilizando el comando **show ip ssh**:

CÓMO ASEGURAR EL PUERTO DE LA CONSOLA Y LOS TERMINALES VIRTUALES

En el nivel de los dispositivos individuales con IOS, es posible definir una contraseña de acceso a través del puerto de la consola utilizando el comando principal de IOS **line console 0** y el subcomando de IOS **password**. En las líneas de terminales virtuales, se pueden agregar contraseñas utilizando el comando principal **vty 04** y el subcomando **password**.

Bto:	Operación y red	**Proyecto:**	CCNA
Autor:	Elva y Chechu	**Fecha:**	01/04/02
Asunto:	Preparación para certificación CCNA Cisco Systems		
Estado:	Pendiente revisión	**Revisión:**	1.0

Con el subcomando de línea **access-list**, es posible especificar una lista de direcciones IP que sean capaces de conectarse a las líneas de terminales o a las que sea posible acceder desde las líneas de terminales de cualquier dispositivo con IOS. Es posible especificar si se utiliza una clase de acceso para las sesiones entrantes o salientes mediante el uso de una palabra clave **in** u **out**. Este subcomando utiliza una lista de acceso IP para habilitar las direcciones IP antes de que se inicie cualquier sesión entrante o saliente. El subcomando **access-list** se puede utilizar para permitir que solamente las estaciones de trabajo del administrador de red puedan acceder a las líneas de terminales virtuales de los dispositivos con IOS, que es un método adicional para asegurar el acceso a los dispositivos.

Las contraseñas de consola y de los terminales virtuales se guardan en texto sin formato en la configuración activa y en la de inicio. Si desea cifrar todas las contraseñas que muestran los comandos ejecutables(como **show running-config** o **show startup-config**), puede utilizar el comando de configuración global **service password-encryption**. Como resultado de este comando, las versiones cifradas de las contraseñas dejan de poder verse a través de ningún comando ejecutable. No se preocupe si olvida la contraseña, Cisco ha documentado varios procedimientos de recuperación de contraseñas para cada tipo de dispositivo.

Una alternativa a la configuración de contraseñas dispositivo a dispositivo para el control de acceso es utilizar un protocolo de control de acceso en la red. Estos protocolos de control de acceso realizan tres funciones: autenticación, autorización y contabilidad, que en conjunto se conocen como AAA. La **autenticación** es el proceso de identificación y verificación de los usuarios. En Cisco IOS, se pueden utilizar varios métodos para autenticar a los usuarios, entre los que se incluyen una combinación de un nombre de usuario t contraseña, o el paso de una clave única. La **autorización** determina lo que pueden hacer los usuarios una vez que han sido autenticados, como, por ejemplo, obtener acceso y realizar tareas en determinados dispositivos de la red o *host* de acceso. La **contabilidad** es el método de grabación de los que los usuarios hacen o han hecho.

AAA requiere dos componentes: un cliente dos componentes: un cliente que funcione un dispositivo con Cisco IOS y el software relacionado del servidor de control de acceso, que suelen utilizarse en las estaciones de trabajo de la red. Remote Authentication Dial-In User Service(RADIUS) y Terminal Access Controller Access Control System (TACACS+) son dos de los protocolos que suelen utilizarse para proporcionar comunicación entre el cliente AAA de un dispositivo Cisco y el software del servidor de control de acceso.

Piense en un usuario que utiliza la aplicación Telnet para conectarse a un router en el que no se ha configurado ningún protocolo de control de acceso. Inmediatamente, se solicita al usuario la contraseña de la línea de terminal virtual:

```
% telnet router
Trying...

Password:
```

Si el usuario escribe la contraseña correcta, recibe acceso al modo ejecutable del router.
Este usuario no está sujeto a ningún proceso de autenticación y autorización, y es libre para realizar cualquier tipo de tares(incluyendo la entrada al modo privilegiado, siempre que se conozca la contraseña)

Además, el usuario que realiza esta acción no está registrado. Sin duda alguna, dicha directiva abierta no es aceptable en la inmensa mayoría de las redes. Una excepción puede encontrarse en aquellos entornos de laboratorio o de pruebas en los que el acceso no contabilizado a un dispositivo por parte de muchos usuarios no afecta a la seguridad, configuración o rendimiento de la red.

Si se configura un dispositivo Cisco IOS para utilizar algún protocolo de control de acceso, el dispositivo solicita al usuario un nombre de usuario y una contraseña.

```
% telnet router
Trying...

Username: Usuario
Password:
```

Con un protocolo de control de acceso, el dispositivo con Cisco IOS realiza las siguientes tareas:

1. El cliente de control de acceso del dispositivo solicita el nombre de usuario y la contraseña al recibir la solicitud entrante de conexión por Telnet.
2. El cliente de control de acceso consulta al usuario y envía la combinación de nombre de usuario y contraseña del mensaje de solicitud de autenticación al servidor de control de acceso.
3. El servidor de control de acceso autentica la combinación de nombre de usuario y contraseña. La combinación otorga o deniega la combinación, y devuelve el mensaje apropiado al cliente. El servidor puede proporcionar al cliente información acerca de su autorización. El servidor acaba con la transacción.
4. El cliente de control de acceso permite o deniega la combinación de nombre de usuario y contraseña. Si se permite, el usuario consigue acceder al sistema y está autorizado para realizar las acciones especificadas en la información de autorización que pasa el servidor.

ACTIVACIÓN DE AAA

Para activar los servicios de AAA en Cisco IOS, hay que utilizar el comando de configuración **aaa new-model**.

Seguidamente, se puede activar el cliente AAA para una configuración específica de autenticación, autorización y contabilidad utilizando los siguientes comandos de configuración global: **aaa authentication, aaa authorization** y **aaa accounting**. Todos los comando AAA se configuran utilizando listas de métodos. Una lista de métodos es una lista configurada que describe los métodos AAA que se van a intentar, en la secuencia ordenada, para autenticar a un usuario, autorizar una actividad o contabilizar una acción. Por ejemplo, con listas de métodos se pueden especificar varios mecanismos de autenticación en un intento de autenticar a un usuario en caso de que falle el método inicial. Un dispositivo con IOS intenta utilizar el primer método que aparece en la lista para autenticar a los usuarios; si dicho método no responde, el dispositivo prueba con el siguiente método de autenticación de la lista de métodos. El proceso continua hasta que s produce una comunicación correcta con un método de autenticación de la lista o hasta que hayan utilizado todos los métodos de la lista. Las listas de métodos de autorización y contabilidad funcionan de forma parecida a las descritas anteriormente por la autenticación.

Nota_
Los dispositivos con IOS intentan utilizar el siguiente método de una lista de métodos solamente si el dispositivo no puede comunicarse con el método anterior. Por ejemplo, si algún método de autenticación responde pero no autentica al usuario, no se utiliza el siguiente método de autenticación.

Dos protocolos de AAA habituales son RADIUS y TACACS+. Con los comandos de configuración global **aaa authentication, aaa authorization** y **aaa accounting** se puede especificar el método que hay que utilizar cuando RADIUS utiliza el método **group radius** TACACS+ utiliza el método **group tacacs+**.

El comando **aaa authentication** especifica los protocolos de autenticación en una lista de métodos ordenada, que el dispositivo puede intentar para verificar el acceso. El comando **aaa authorization** permite especificar si se realiza la autorización en los comandos ejecutables o al comienzo de las sesiones ejecutables o de la red(como las sesiones PPP). También permite especificar el protocolo que se utiliza para realizar estas tareas. El comando **aaa accounting** permite especificar cuándo se envían mensajes de contabilidad al servidor AAA, como, por ejemplo, al principio o al final de las sesiones de cada uno de los usuarios o después de cada comando. Este comando también especifica el tipo de contabilidad que realiza el cliente AAA. Puede justificar la actividad del sistema IOS, los servicios relacionados con la red (como PPP o ARAP) y las sesiones ejecutables. Puede utilizar TACACS+ y RADIUS para enviar información contable desde un cliente AAA a un servidor AAA.

La autenticación AAA se activa en las sesiones de conexión mediante el uso del comando de configuración global **aaa authentication login**. El primer protocolo de autenticación de la lista de métodos es TACACS+.

Si el agente TACACS+ no es capaz de ponerse en contacto con el servidor para realizar la autenticación, el dispositivo realiza la autenticación a través de un segundo método(a saber, mediante el uso del comando de configuración global **enable secret** o **enable password**). Esta lista de métodos se ve en el comando **aaa authentication login** como la opción **group tacacs+**, seguida de la opción **enable**.

Sugerencia_

Es aconsejable que no utilice un solo protocolo de AAA para la autenticación de las sesiones de conexión en los dispositivos con IOS. Un segundo método de autenticación de las sesiones de conexión garantiza que siempre se puede obtener acceso a cualquier dispositivo si no está disponible algún servidor AAA.

Al configurar los comandos **aaa accounting** y **aaa authorization**, se aplica la misma lógica que con los comandos **aaa authentication**. Es posible especificar otros métodos de autorización para las sesiones ejecutables y las sesiones de red(como PPP) utilizando las opciones **exec** y network en el comando de configuración global **aaa authorization**. La palabra clave del método **if-authenticated** indica al cliente AAA que otorgue autorización si la autenticación ha pasado por la sesión.

Para finalizar, se contabilizan todas las sesiones ejecutables cuando han dejado de utilizar el protocolo TACACS+ utilizando el comando de configuración global **aaa accounting**.

Opcionalmente, puede definir sus propios grupos de servidores AAA utilizando el comando de configuración global **aaa server group** y el subcomando **server**. Los grupos de servidores AAA definidos por los usuarios son útiles cuando se tiene un grupo de usuarios que utilizan un servidor AAA y otro grupo de usuarios que utilizan otro servidor AAA. Estos dos grupos pueden utilizar o no el mismo protocolo de AAA(como RADIUS). Antes de la invención de los grupos de servidores AAA, solamente podía utilizarse un solo conjunto de servidores AAA para cada método para todos los usuarios. Un ejemplo frecuente del uso de grupos de servidores AAA es la autenticación de usuarios de acceso telefónico utilizando un servidor RADIUS.

En las secciones siguientes podrá ver como especificar los servidores RADIUS y TACACS+ en el cliente AAA.

RADIUS

El protocolo RADIUS lo publicó originalmente la empresa Livingston Enterprises,Inc., como un protocolo estándar que intercambia información de AAA entre un cliente y un servidor RADIUS. RADIUS es un protocolo abierto; varios dispositivos de red tienen un cliente RADIUS.

Un servidor RADIUS es una estación de trabajo en la que se ejecuta el software de servidor RADIUS de un fabricante u organización como Livingston, Merit o Microsoft. Para especificar la dirección IP del servidor RADIUS con el que se comunica el cliente con IOS se utiliza el comando de configuración global **radius-server host**.

Al realizar la autenticación, el protocolo RADIUS cifra las contraseñas enviadas entre el cliente y el servidor. Para que se realice el cifrado de contraseñas hay que configurar una cadena secreta tanto en el servidor RADIUS como en Cisco IOS. Para configurar esta cadena en el cliente con Cisco IOS, utilice el comando de configuración global **radius-server key**.

TACACS+

TACACS+ es un protocolo de AAA que es conceptualmente parecido a RADIUS.

TACACS+ es la tercera revisión del protocolo TACACS. La segunda revisión se llama Extended TACACS o XTACACS. TACACS+ es un procoloco patentado de Cisco y todos los dispositivos con IOS tienen un cliente TACACS+ nativo.

El software del servidor TACACS+ se puede obtener de varios lugares, incluyendo Cisco(en el producto CiscoSecure) y otros fabricantes, en muchas estaciones de trabajo.
Para especificar la dirección IP del servidor TACACS+ con el que se cominica el cliente con IOS se utiliza el comando de configuración global **tacacs-server key.**

COMPARACIÓN ENTRE RADIUS Y TACACS+

Hay muchas diferencias entre RADIUS y TACACS+, pero su funcionalidad es esencialmente la misma. RADIUS, que es un estándar, utiliza la capa de transporte UDP.
TACACS+, que está patentado, utiliza la capa de transporte TCP. RADIUS funciona bien en entornos sólo con IP, mientras que TACACS+ es útil en entornos multiprotocolo.
Actualmente, Radius admite más atributos en el protocolo y permite que el cliente y el servidor pasen más información que TACACS+. RADIUS cifra solamente la contraseña enviada entre el cliente y el servidor, mientras que TACACS+ cifra toda la comunicación.

Muchos fabricantes admiten uno de estos protocolos o el otro discuten vehementemente los méritos del protocolo de AAA que utilizan. Cisco admite ambos protocolos. Si la red es en mayor parte heterogénea, RADIUS es quizás el protocolo de AAA correcto, ya que actualmente muchos fabricantes lo admiten. Sin embargo, si la red utiliza principalmente dispositivos Cisco, es muy probable que TACACS+ sea la solución adecuada.

PREVENCIÓN BÁSICA CONTRA ATAQUES

Las características de intercepción de TCP (TCP intercept) y de envío de ruta inversa de unidifusión (unicast reverse path fowarding) de IOS permiten configurar una cierta seguridad contra dos tipos de ataques de denegación de servicio: desbordamiento de SYN de TCP y falsificación de la dirección IP de origen.

Un ataque de denegación de servicio es aquel en el que un pirata informático (hacker) sobrecarga un recurso de red con trafico cuya intención no es dañar datos, sino utilizar suficientes recursos de la red para que no pueda realiza su función. Por ejemplo un ataque de desbordamiento de SYN(sincronización) de TCP se produce cuando un pirata informático desborda un servidor con un gran número de solicitudes de SYN de TCP (que se utiliza para iniciar una conexión TCP) desde una dirección IP de origen inválida. Todas estas solicitudes tienen una dirección IP de origen a la que no se puede acceder, lo que significa que no se pueden establecer las conexiones. El gran número de conexiones abiertas que no se establece desborda al servidor y puede provocar que deniegue el servicio a las peticiones válidas, impidiendo que los usuarios se conecten al servidor y, por consiguiente, realizando las tareas deseadas.

INTERCEPCIÓN DE TCP

La característica de intercepción de TCP facilita la prevención de desbordamientos de SYN, ya que intercepta y valida las solicitudes de conexiones por TCP cuando atraviesan un router. Esta característica también puede interceptar los mensajes SYN de TCP entrantes o vigilar las conexiones TCP cuando el router los reenvía.

En el modo de intercepción, el router intercepta activamente todas las SYN de TCP y responde por el servidor destino real con un ACK y una SYN de TCP. Éste es el primer paso de un proceso de establecimiento de conexiones TCP estándar llamado saludo a tres bandas (three-way handshake). Seguidamente, el router espera un ACK de TCP de la segunda SYN de TCP del origen. Cuando se recibe dicho ACK, el router ha establecido una conexión TCP válida con el origen y se ha completado el saludo a tres bandas. A continuación el router envía la SYN de TCP original al servidor destino real y realiza un segundo saludo a tres bandas. Después, el router une las dos conexiones TCP de forma transparente y reenvía paquetes entre ellas mientras la conexión esté activa.

En el modo de intercepción, la característica de intercepción de TCP facilita la prevención del ataque de DoS a la SYN de TCP, ya que los paquetes de aquellos host a los que no se pueda acceder nunca llegarán al servidor destino. El router puede configurarse para que intercepte solicitudes en función de una lista de acceso IP ampliada, lo que permite especificar las peticiones que debe interceptar.

Una alternativa a la interceptación de todas las conexiones TCP es que esta característica vigile las peticiones de conexión cuando las reenvía el router. Si una conexión TCP no consigue iniciarse en un intervalo configurable, el software IOS interceptará y terminará el intento de conexión.

La característica de intercepción de TCP se configura con el comando de configuración global de IOS **ip tcp intercept mode**. El comando de configuración global **ip tcp intercept list** asigna una lista de acceso IP ampliada para especificar qué solicitudes debe interceptar el router. El comando **ip tcp intercept watch-timeout** especifica el número de segundos que debe permitir el router antes de restablecer cualquier conexión TCP que no haya completado un saludo a tres bandas válido con el servidor destino. Por defecto, un router restablecerá una conexión TCP si no se completa un saludo a tres bandas en treinta segundos.

El comando ejecutable **show tcp intercept connections** muestra todas las conexiones TCP incompletas y establecidas. El comando ejecutable **show tcp intercept statistics** muestra estadísticas relativas al comportamiento de la característica de intercepción de TCP.

ENVÍO DE RUTA INVERSA DE UNIDIFUSIÓN

La característica de envío de ruta inversa (Reverse Path Forwarding, RPF) de unidifusión puede ayudar a impedir el ataque de DoS mediante falsificación de la dirección IP de origen (a veces llamado simulación IP o IP *spoofing*). El ataque mediante falsificación dela dirección IP de origen utiliza direcciones IP de origen mal formadas o una IP de origen en constante cambio para atacar a una red. Si su red recibe el ataque de una dirección IP de origen mal formada o de un conjunto de direcciones IP de origen en constante cambio, es fácil que sea imposible configurar una lista de acceso IP para detener el ataque.

Nota_

La característica de RPF de unidifusión sólo está disponible en los dispositivos con IOS si se utiliza Cisco Express Forwarding (CEF). CEF es un mecanismo avanzado que se utiliza para reenviar paquetes y para crear tablas de enrutamiento IP. Actualmente, CEF sólo funciona en ciertos dispositivos de gama alta con IOS.

La característica de RPF de unidifusión ayuda a resolver este problema mediante el descarte automático de aquellos paquetes IP que no tengan una cuenta IP de origen que se pueda verificar. El router verifica las direcciones IP viendo todos los paquetes recibidos en la interfaz para asegurarse de que la dirección de origen y la interfaz de origen del router aparece en la tabla de enrutamiento IP y coinciden con la interfaz en la que se ha recibido el paquete. La ruta recibida y la ruta hacia atrás, tal como se ve en la tabla de enrutamiento con la dirección IP de origen, deben ser simétricas. Una ruta es simétrica si un paquete llega a la interfaz de un router en una de las rutas con mejor retorno con el origen del paquete, sin limitarse a la interfaz exacta del router de origen, lo que permite utilizar las técnicas de enrutamiento, como un balanceo de cargas del mismo costo.

Si no hay ninguna ruta inversa en la misma interfaz de origen ni ninguna ruta de retorno desde donde se recibió el paquete, podría significar que se ha modificado la dirección de origen o que se ha descartado el paquete. La verificación de que es posible acceder a la dirección de origen a través de la ruta inversa en la que se reenviará el paquete ayuda a evitar la falsificación de direcciones IP de origen.

La característica de RPF de unidifusión se puede utilizar en cualquier configuración de la red en la que haya una sola ruta de conectividad desde la red. Si se tiene una sola ruta de conectividad, incluso con varias rutas con reparto de carga, el enrutamiento de la red es casi siempre simétrico. Esta configuración suele producirse en el punto de salida de flujo ascendente a Internet de la red. La característica de RPF de unidifusión no debe utilizarse en la red interna cuando existen varias rutas diferentes a los destinos IP.

La configuración de la característica de RPF de unidifusión se realiza mediante un solo subcomando de la interfaz, **ip verify unicast reverse-path**. En un entorno común, este comando sólo se aplicaría a la interfaz (o interfaces en los entornos de reparto de cargas) de flujo ascendente del router que se conecta a Internet.

Los dispositivos con Cisco IOS tienen la capacidad de registrar mensajes acerca de la actividad del sistema. Estos mensajes de registro pueden ser útiles para hacer seguimientos de la actividad del sistema, de los errores y de las notificaciones. El registro utiliza ocho niveles de mensajes de notificación:

Nivel 0: Emergencias
El sistema no puede utilizarse.

Nivel 1: Alertas
Hace falta una acción inmediata para restaurar la estabilidad del sistema.

Nivel 2: Criticas
Se han producido condiciones críticas que pueden necesitar atención.

Nivel 3: Errores
Se han producido condiciones de error que pueden ayudar a hacer seguimientos de los problemas.

Nivel 4: Avisos
Se han producido condiciones de aviso que no son graves.

Nivel 5: Notificaciones
Condiciones normales pero significativas que exigen notificación.

Nivel 6: Informativo
Estos mensajes informativos no requieren ninguna acción.

Nivel 7: Depuración
Son mensajes de depuración que solamente se utilizan para solucionar los problemas del sistema.

En IOS, el usuario define el nivel mínimo de mensajes de registro (en términos de gravedad) que desee que se registren. Para ello hay que identificar el nivel por nombre en el comando de configuración. Emergencias (Nivel 0) es el nivel más grave, mientras que depuración(Nivel 7) es el menos grave. Todos los mensajes de nivel que identifique y de los niveles más graves se envían a uno de estos cuatro lugares:

- Un servidor **syslog**, que se configura con el comando **loogging trap**.
- Un búfer interno del dispositivo, que se configura con el comando **logging buffered**.
- El puerto de la consola de un dispositivo, que se configura con el comando **loogging console**.
- Las líneas terminales de un dipositivo, que se configura con el comando **logging monitor**.

Los anteriores comandos **logging** son comandos de configuración global que le permiten especificar el nivel de los mensajes enviados a cada ubicación de registro. Un servidor syslog es una excelente ubicación de registro, ya que el sistema suele guardar los mensajes en un disco. Además, dado que syslog es un programa de uso general que utilizan muchos programas distintos, puede tener un origen central para registrar mensajes de diferentes dispositivos.

El búfer interno del dispositivo es un útil programa de registro si no se tiene ningún servidor syslog o si se desea que cada uno de los dispositivos mantenga un registro de eventos independiente. El tamaño predeterminado de este búfer es de 4.096 bytes. Dicho tamaño se puede modificar con el comando **logging buffered**.
En algunas situaciones el búfer interno del dispositivo esta en la memoria RAM del dispositivo, por lo que se pierde con cada recarga del dispositivo.

El registro de mensajes en la consola o en las líneas terminales de un dispositivo(incluyendo sesiones de terminales virtuales) es útil para la notificación inmediata de los eventos críticos. Las cuatro ubicaciones de registro distintas no son mutuamente exclusivas y se pueden utilizar varios programas de registro al mismo tiempo.

Nota_
Para ver los mensajes de registro en una línea terminal o en una sesión de terminal virtual debe utilizar el comando ejecutable **terminal monitor**. Este comando se puede ejecutar en modo privilegiado.

Los mensajes del servidor syslog pueden configurarse con el comando **logging trap**.

Para activar el registro sysloog en IOS hay que utilizar el comando de configuración global **logging** para especificar la dirección IP del host que realiza el registro.
Es posible registrar mensajes en más de una de las ubicaciones.

Nota_

El programa syslog registra los mensajes del sistema en un archivo de texto en UNIX y en otros tipos de estaciones de trabajo. Para registrar los mensajes de dispositivos con IOS en un servidor syslog, debe configurar el proceso de syslog. Para activar el programa syslog local7, el programa que utilizan todos los dispositivos con IOS, hay que ser superusuario en una estación de trabajo UNIX. Como superusuario (acceso raiz), debe añadir la siguiente línea al archivo /etc/syslog.conf:

Local7.debug /var/adm/router.log

A continuación reinicie el demonio de syslog en la estación de trabajo UNIX, lo que se suele hacer con el siguiente comando:

%kill –HUP `cat /etc/syslog.pid`

Si todo funciona bien, ya está listo para que los dispositivos con IOS se registren en esta estación UNIX.

Si un dispositivo con IOS está configurado para registrarse en un búfer interno, los resultados del registro se pueden ver con el comando ejecutable **show logging**.

Sugerencia_

Es aconsejable activar el registro a nivel de depuración en, al menos una ubicación de registro, ya que eso permite garantizar que se graban todos los mensajes de error que envía el dispositivo con IOS. La mayor parte de los administradores de redes tienden a establecer **logging trap debug** para activar syslog, a fin de que registre todos los mensajes de los dispositivos con IOS.

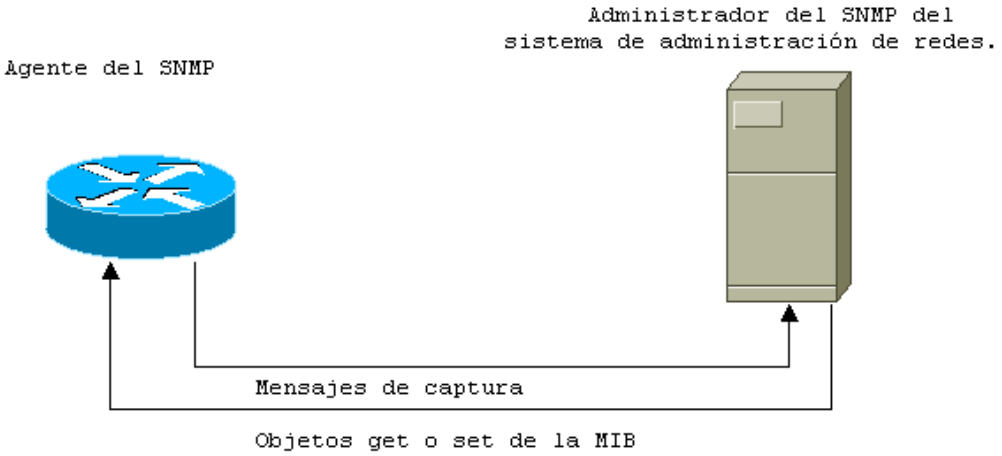
ADMINISTRACIÓN BASICA DE REDES.

La administración de redes es el proceso de gestión de fallos, control de configuraciones, supervisión de rendimiento, aseguramiento de la seguridad y contabilidad de actividades en una red de datos. Es necesario que todas estas tareas tengan un control absoluto sobre algún entorno de la red de datos, que es uno de los componentes esenciales de cualquier organización. El ISO Network Management Forum ha definido la administración de redes como la suma de todas las actividades necesarias para realizar la administración de los fallos, la configuración, el rendimiento, la seguridad y la contabilidad de una red de datos.

Las plataformas de administración de redes son sistemas de software diseñados para realizar las actividades de administración de red. Algunos ejemplos de plataformas de administración de redes son: Hewlett-Packard OpenView, Cabletron Spectrum, Sun Solstice Enterprise Manager, IBM NetView/ AIX y CiscoWorks2000. Estas plataformas proporcionan la arquitectura de software para las aplicaciones de administración de redes que realizan una gran variedad de tareas.

No se pueden agrupar en una sola categoría. Algunas presentan un mapa de la red y comprueban el estado de todos los dispositivos de la red, lo que proporciona una función de administración de fallos. Algunas herramientas de administración del rendimiento diseñan la utilización de los enlaces de la red y envían advertencias si se producen errores en alguna interfaz de LAN. Sin embargo, otras vigilan la seguridad de la red y envían advertencias a través del correo electrónico o de buscapersonas.

Las aplicaciones de administración de redes se comunican con el software de los dispositivos de la red llamados agentes. La comunicación entre el administrador y el agente permite el primero recopilar un conjunto estándar de información, que se define en una base de información de administración(Management Information Base, MIB). Cada dato que hay en una MIB recibe el nombre de objeto. Una MIB contiene objetos útiles para que los administradores realicen las tareas de administración de red.



Los dos tipos de MIB son estándar y están patentados. Las MIB estándar, como MIB-II (RFC 1213), proporcionan objetos básicos aplicables a casi todos los dispositivos de una red de datos. Por ejemplo, MIB-II contiene la información del sistema acerca de un dispositivo, como su tiempo de actividad y nombre, los contadores de errores y del trafico específico de la interfaz, y la información del protocolo de IP. Las MIB específicas de la tecnología, que son estándar son para protocolos como Frame Relay(RFC 1285) o Token Ring(RFC 1315). Contienen objetos que se relacionan con una tecnología específica de un dispositivo de red. Las MIB específicas de los fabricantes, que están patentadas, definen objetos específicos de los dispositivos de red de un solo fabricante.

Las aplicaciones de administración de redes recogen la información de la MIB de los dispositivos y cambian el comportamiento de dichos dispositivos de red mediante el uso de un protocolo de administración de redes. El Protocolo simple de gestión de redes(Simple Network Management Protocol, SNMP), definido en la RFC 1157, es el protocolo estándar de administración de redes más profusamente utilizado. SNMP usa UDP en la capa de transporte e IP en la capa de red. También existen protocolos patentados de administración de redes y algunos fabricantes los han implementado en sus dispositivos de red.

La comunicación entre un agente SNMP y un administrador se produce con cinco tipos de paquetes:

- Get-Request.
- Get-Next-Request.
- Set-Request.
- Get-Reponse.
- Trap.

Un Get-Request es un mensaje del administrador a un agente en el que se solicita un conjunto de objetos de MIB especificos, como el nombre de un dispositivo, su ubicación, su número de interfaces físicas, etc.

Un Get-Next-Request es un mensaje del administrador a un agente en el que se solicita algún dato tabular. Este tipo de mensajes es útil en la eliminación de las tablas de la MIB y en la recuperación de una tabla como la tabla de enrutamiento IP. Un Set-Request es un mensaje en el que se solicita al agente que cambie el valor de un objeto de MIB específico, como, por ejemplo, que cambie el estado de una interfaaz de un dispositivo. Los agentes responden a cada Get-Requet, Get-Next-Request o Set_Request enviando al administrador un Get-Response que contenga los valores solicitados de los objetos de MIB o que muestre el valor de un objeto de MIB que se ha cambiado. Un mensaje Trap es un mensaje no solicitado del agente al administrador relativo a un evento.

Todos los agentes SNMP se configuran con una cadena de verificación llamada **cadena de comunidad**. Esta cadena se incluye en todas las solicitudes del administrador para obtener o definir la información de MIB. El agente la verifica antes de responder. Una cadena de comunidad tiene una autenticación débil codificada en ASCII, por lo que no es conveniente utilizar solamente este método para asegurar el acceso SNMP a un agente.

El comando de configuración global de Cisco IOS **snmp-server community** configura el agente con la cadena de comunidad. Una opción de este comando permite estipular que la cadena de comunidad se puede aplicar a los mensajes de sólo lectura-escritura dirigidos al agente. Los mensajes Get-Request y Get-Next-Request son de sólo lectura, mientras que los Set-Request son de lectura y escritura. Las palabras clave utilizadas para establecer sólo lectura y escritura son **RO** y **RW**, respectivamente. La cadena de comunidad de sólo lectura predeterminada para muchas aplicaciones de administración de redes es **public**, mientras que la de lectura y escritura suele ser **private**. Una opción final de este comando global es especificar una lista de acceso IP estándar de aquellos host a los que se les permite realizar consultas al agente utilizando cadenas de comunidad válidas.

Nota_

Para aumentar la seguridad del agente SNMP en cualquier dispositivo con IOS, es aconsejable configurar varias cadenas de comunidad para el acceso RO y RW. Además, es recomendable limitar los host que pueden realizar consultas al dispositivo con IOS a través de SNMP mediante el uso de la opción **access-list** del comando **snmp-server community**.

Para enviar mensajes Trap SNMP, hay que configurar el dispositivo con Cisco IOS. Los seis mensajes Trap SNMP estándar que envían todos los agentes se definen en la RFC 1157:

- ColtStart.
- WarmStart.
- LinkUp.
- LinkDown.
- AuthenticationFailure.
- EgpNeighborLoss.

Un coldStart significa que el agente acaba de iniciarse. La trap warmStart indica que el propio software del agente se acaba de restablecer. En la practica, la mayor parte de los agentes sólo envían Traps coldStart, ya que el agente se suele reiniciar cuando se enciende el dispositivo en el que el agente se está ejecutando. Las Traps linkUp y linkDown alertan a un administrador acerca del cambio de estado de algún enlace del dispositivo. Un authenticationFailure indica que un administrador ha enviado al agente una solicitud SNMP con una cadena de comunidad incorrecta. Finalmente, la Trap egpNeighborLoss indica al administrador que no se puede acceder a un vecino con el protocolo External Gateway Protocol (EGP). Este ultimo Trap casi nunca se utiliza, ya que EGP se ha reemplazado por BGP4.

Los seis anteriores mensajes trap son los Traps SNMP estándar, pero no son los únicos que pueden evitar los agente. Muchas MIB definen Traps especificos de los protocolos, como traps específicos de RDSI(ISDN), Frame Relay o BGP$. Actualmente IOS admite los traps para una variedad de protocolos y para funciones de IOS, entre los que se incluyen BGP, Frame Relay, RDSI, X.25, monitor de entorno y cambios en la configuración de IOS.

Cisco IOS puede configurarse para enviar Traps SNMP a cualquier número de administradores. Para especificar la dirección IP y la cadena de comuidad del administrador al que debe enviarse las Traps, hay que utilizar el comando **snmp-server host**. Los parámetros opcionales del comando **snmp-server host** tambien sirven para especificar que queremos que el agente envíe Traps SNMP.

Sugerencia_

Es conveniente configurar el agente SNMP para que envíe Traps relativos a todas las tecnologías que están activas en el dispositivo. Los mensajes Traps SNMP no suelen consumir mucho ancho de banda y pueden proporcionar información útil para diagnosticar problemas de red.

Es posible configurar manualmente el agente SNMP en IOS con la ubicación física y la persona de contacto del dispositivo. A continuación, las aplicaciones de administración de red pueden recuperar esta información. Para configurar esta información hay que utilizar los comandos de configuración global **snmp-server loction** y **snmp-server contact**. Ambos comandos permiten escribir una cadena de texto de 255 caracteres para describir la ubicación o la persona de contacto.

El comando ejecutable **show snmp** muestra las estadísticas SNMP de un dispositivo dado.

Este comando es útil para ayudarle a supervisar la actividad de SNMP en el dispositivo.

CONTROL DE TIEMPO BÁSICO

Cisco IOS permite a los dispositivos hacer un seguimiento de la fecha y hora actuales utilizando un reloj del sistema. Este reloj se inicia cuando enciende el dispositivo y puede distribuir el tiempo a varios sistemas internos, como la grabación de la fecha y hora de los cambios en la configuración, la visualización del tiempo en los mensajes de registro en el búfer y el envío de la fecha y la hora en los mensajes de SNMP. En los router Cisco 7000, el tiempo del reloj del sistema se define a través de hardware. En los restantes modelos, el reloj del sistema se define de forma predeterminada con el valor de medianoche del 1 de marzo de 1993.

Una vez definido, el reloj del sistema determina si la fecha y la hora son de un origen fiable. Si el origen de la hora es fiable, se redistribuye a otros procesos IOS; en caso contrario, la hora solo se utiliza para la visualización. En las próximas secciones se explicara como asegurarse de que el origen de la hora definida, como un reloj atómico, es un origen fiable.

Los routers de la serie 7000 contienen un calendario que hace un seguimiento de la fecha y la hora en los recintos del sistema y los cortes eléctricos. En un recinto del sistema, el calendario siempre se utiliza inicialmente para definir el reloj del sistema. A continuación es posible que otro protocolo modifique o actualice el reloj. En una red en la que no exista ningún otro origen de hora con autoridad, se puede utilizar el calendario como origen de hora con autoridad y puede pasarse a otros procesos(como el protocolo Network Time Protocol). Para ver el valor actual del sistema del calendario se utiliza el comando ejecutable **show calendar**.

Nota_
Si desea que algún dispositivo con IOS indique la fecha y hora actual en los mensajes de depuración y de registro, utilice el comando de configuración global **service timestamps**. Puede mostrar el tiempo que ha transcurrido desde que se reinició el dispositvo, la fecha y hora utilizando GMT o la zona hararia local y la hora con una precisión que llega hasta los milisegundos. Es recomendable utilizar los comandos de configuración **service timestamps log datetime localtime** y **service timestamps debug datatime localtime**. El comando **service timestamps log datetime localtime** añade la fecha y hora a los mensajes de registro, mientras que **service timestamps debug datatime localtime** las añade a los de depuración.

Para fijar el reloj del sistema puede utilizar varias fuentes. Éstas son las tres más utilizadas:

- Manualmente.
- NTP.
- SNMP.

CONFIGURACIÓN MANUAL DE LA FECHA Y HORA

Si el dispositivo con IOS está aislado y no puede utilizar una fuente horaria con autoridad externa, es posible definir la fecha y la hora de forma manual. Estos valores son válidos hasta que el dispositivo se restablezca o se vuelva a cargar. Estos servicios de control de tiempo manuales sólo deben utilizarse cuando no haya posibilidades de recurrir a ninguna fuente horaria con autoridad.

Para definir manualmente la zona horaria de un dispositivo IOS se utiliza el comando de configuración global **clok timezone**. Este comando adopta como opciones la zona horaria en la que se encuentra el dispositivo y el número de horas de diferencia entre esa hora y la hora de Grenwich.

Si la zona horaria en la que se encuentra el dispositivo con IOS utiliza el cambio de horario de varano, es necesario utilizar el comando de configuración global **clok summer-time recurring**. Este comando de configuración adopta como argumentos el nombre de la zona horaria en verano, como la hora de verano del Pacifico(PDT). La hora del sistema se fija utilizando el comando de configuración global **clok set**.

Para definir manualmente el calendario en los routers de la serie 7000 se utiliza el comando de configuración global **calendar set**. Para que este calendario sea una fuente de fecha y hora válida para otras funciones de IOS, utilice el comando de configuración global **clock calendar-valid.**

NETWORK TIME PROTOCOL

Network Time Protocol (NTP), documentado en la RFC 1305, es un protocolo que sincroniza las horas de los dispositivos que funcionan en una red IP de datos. Cisco IOS contiene un proceso NTP que permite a los dispositivos enviar y recibir paquetes NTP.
Muchos fabricantes tiene procesos NTP similares en sus dispositivos y host, lo que hace que NTP sea el mecanismo preferido para sincronizar la hora en toda la red.

NTP distribuye por toda la red un valor horario que obtiene de una fuente horaria con autoridad. Como ya se ha indicado, es posible definir de forma manual que cualquier dispositivo con IOS sea esta fuente horaria, aunque es preferible que la fuente sea un reloj atómico conectado a un servido de tiempo. Para utilizar NTP no es necesario tener un reloj atómico propio. La hora puede sincronizarse con otra fuente que reciba información de un reloj atómico.

Al igual que muchos relojes de red a través de la línea telefónica, NTP mide la distancia entre el dispositivo en el que se ejecuta y una fuente horaria con autoridad en incrementos que recibe el nombre de **estrato.** Un reloj que sea una fuente horaria de **estrato 1** esta conectado directamente a un reloj atómico, una fuente de **estrato2** esta sincronizada con una fuente de **estrato 1**, y así sucesivamente. Los dispositivos con IOS no pueden conectarse directamente a una fuente horaria de **estrato 1**. El proceso NTP de Cisco IOS se sincroniza automáticamente con la fuente horaria que tiene el estrato más bajo.

Dto.:	Operación y red	Proyecto:	CCNA
Autor:	Elva y Chechu	Fecha:	01/04/02
Asunto:	Preparación para certificación CCNA Cisco Systems		
Estado:	Pendiente revisión	Revisión:	1.0

El proceso NTP de Cisco no se sincroniza con un fuente horaria que no este a su vez sincronizada con otra fuente horaria del mismo estrato o inferior. Si NTP encuentra una fuente horaria que tenga una hora completamente distinta de otras de la red, no se sincroniza a ella, aunque sea la que tiene el estrato más bajo.

Para comunicar dos dispositivos que utilicen NTP se crea una **asociación**. En cisco IOS, las asociaciones se configuran con los comandos de configuración global **ntp server** o **ntp peer**. Una **asociación de servidores** significa que el dispositivo con IOS establece una asociación con el dispositivo configurado, no a la inversa. En una **asociación entre iguales**, los dispositivos establecen una asociación entre sí. El tipo de asociación más habitual es la asociación de servidores, en la que una fuente horaria con autoridad es el servidor de varios procesos NTP en distintos dispositivos.

Sugerencia_

Se recomienda buscar una fuente horaria con autoridad en Internet para que sirva a la red. Estas fuentes se pueden buscar con herramientas de búsqueda en la Web y se actualizan regularmente(busque la palabra clave NTP). Una práctica habitual es tener varias fuentes horarias con autoridad desde las distintas ubicaciones desde donde la red puede conectarse a Internet. Por ejemplo, si la red tiene una conexión a Internet en Europa y otra en Estados Unidos, elija una fuente horaria con autoridad en cada continente y deje que NTP sincronice con la mejor fuente horaria disponible.

En los router de la serie 7000 es posible realizar sincronizaciones periódicas de NTP al sistema de calendario. Para llevar a cavo esta tarea, utilice el comando de configuración global **ntp update-calendar.**

En una LAN es posible enviar y recibir mensajes NTP utilizando los mensajes de difusión, con lo que se elimina la necesidad de configurar y crear una asociación con todos los dispositivos NTP de la misma. Para escuchar los mensajes de difusión NTP en una interfaz, utilice el subcomando de configuración de interfaz **ntp broadcast client**. Para difundir mensajes NTP a un segmento determinado de la LAN, utilice el subcomando de interfaz **ntp broadcast.** Una configuración frecuente es definir los dispositivos con IOS en una asiciación de servidores con una fuente horaria con autoridad de Internet y, a continuación, difundir mensaje NTP a todas las interfaces de LAN en las que se encuentren los restantes dispositivos NTP.

Para ver las asociaciones NTP de cualquier dispositivo con IOS, utilice el comando ejecutable **show ntp associations.** El primer carácter de cada línea indica el estado de una asociación especifica, en términos de si esta sincronizada(la ultima línea es una clave para los caracteres de la primera columna). La salida por pantalla también muestra la dirección de cada una de las asociaciones configuradas, el nivel del estrato de la fuente horaria y el servidor maestro.

El estado de NTP se puede ver utilizando el comando ejecutable de IOS **show ntp status**.

Si desea desactivar NTP, puede hacerlo en una interfaz específica utilizando el subcomando de interfaz **ntp disable**. Con el comando de configuración global **ntp access-group**, es posible limitar el tipo de asociación NTP que puede tener un dispositivo con IOS. Este comando requiere que especifique el tipo de asociación permitido en un conjunto especifico de direcciones IP dado de una lista IP de acceso. Puede permitir al dispositivo establecer una asociación entre pares o una asociación de servidores. También puede permitirle aceptar solicitudes de tiempo solamente de sistemas o permitir solamente mensajes NTP.

SIMPLE NETWORK TIME PROTOCOL

Los router Cisco 1003, 1004 y 1005 sólo utilizan Simple Network Time Protocol(SNTP), que está documentado en la RFC 2030. SNTP es una versión simplificada de NTP que puede recibir la hara solamente de servidores NTP. SNTP no puede ser una fuente horaria con autoridad para otros dispositivos. Cisco ha considerado apropiada esta funcionalidad limitada, ya que estos routers de la serie Cisco 1000 son dispositivos pequeños con un número fijo de interfaces y un rendimiento relativamente bajo. SNTP proporciona al dispositivo que utiliza IOS información horaria que es precisa hasta alrededor de 100 milisegundos.

SNTP puede configurarse para solicitar y aceptar paquetes de servidores configurados utilizando el comando de configuración global **sntp server**. Puede hacer que el proceso SNTP del router escuche difusiones NTP utilizando el comando de configuración global **sntp broadcast client**. Si configura un servidor especifico y la capacidad del router para recibir información de difusión, el dispositivo prefiere el servidor con estratos más altos o el servidor configurado si los estratos de varias fuentes son los mismos. Las estadísticas de SNTP se pueden ver con el comando ejecutable **show sntp**.

CONFIGURAR UN ROUTER CON CONFIGMAKER DE CISCO

¿QUÉ ES CONFIGMAKER DE CISCO?

ConfigMaker es una herramienta básica de configuración de router que Cisco distribuye de forma totalmente gratuita. Se puede descargar desde el sitio web de Cisco y, en el formato CD-ROM, incluye las últimas versiones de IOS de Cisco. ConfigMaker puede utilizarse para construir la configuración de un router(se pueden incluso construir las configuraciones de todos los routers incluidos en una interconexión de redes) y después descargarla en el router a través de la red. Si la red no esta todavía instalada y ejecutándose, puede descargar la configuración del router desde un PC que ejecute ConfigMaker y que esté conectado al router a través del puerto de la consola. ConfigMaker es una buena forma de agilizar la instalación y ejecución de un nuevo router, pero la configuración de un router sólo puede ajustarse y personalizarse a través de la línea de comandos. ConfigMaker tampoco proporciona ninguno de los comandos de control del router(como **show**, aunque si puede utilizarse **ping** dentro de ConfigMaker).

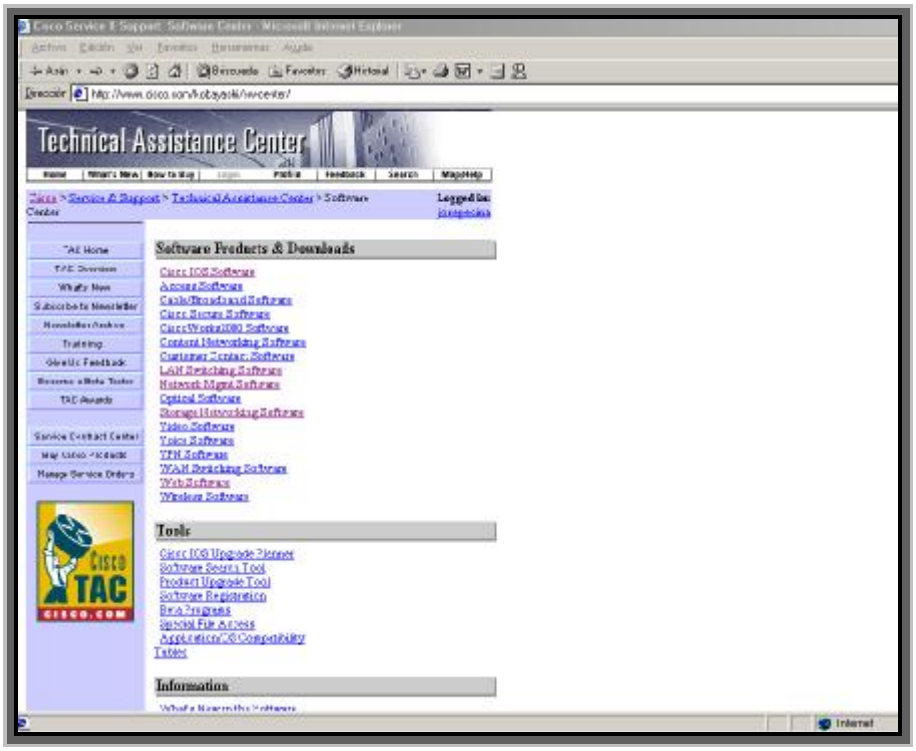
Uno de los problemas que plantea el uso de ConfigMaker para configurar un router es que el router tiene que tener instalada la versión 11.2 o posterior de IOS de Cisco.

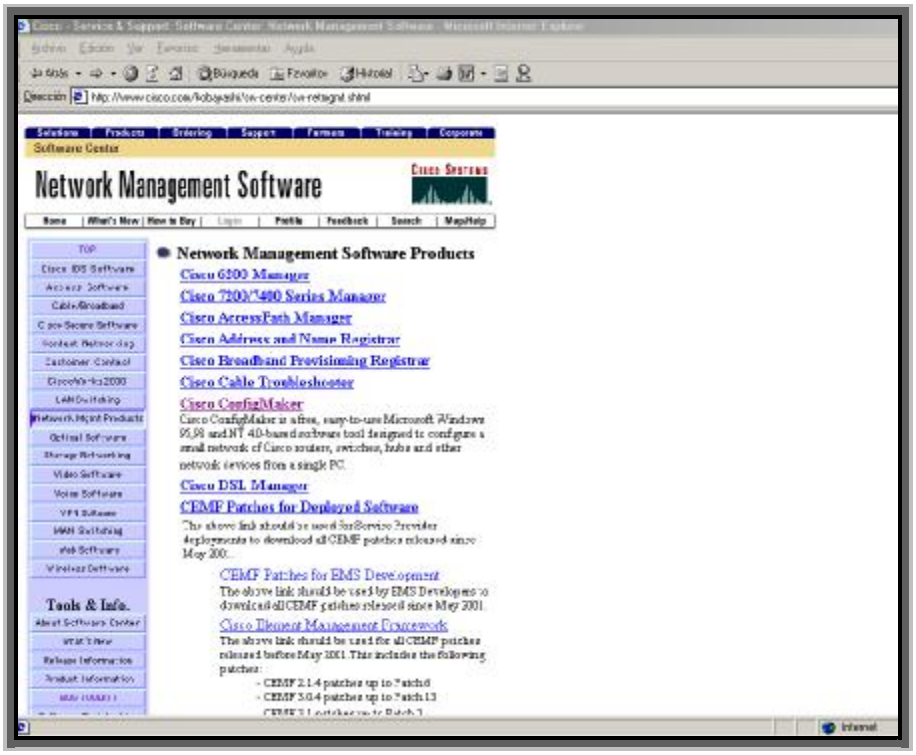
DESCARGAR CONFIGMAKER

Si no ha recibido ConfigMaker de Cisco con una actualización del IOS o con el router, se puede descargar desde el sitio web de Cisco. De hecho, puede descargarse incluso si no se tiene un router cisco, aunque tampoco servirá de mucho, ya que no puede utilizarse para configurar dispositivos de interconexión de redes procedentes de otros fabricantes. Cuando descarga ConfigMaker desde el sitio web de Cisco, se tiene que rellenar un formulario de registro.

Para descargarlo, abra su navegados web y conéctese a Internet. En el cuadro de dirección del navegador, escriba http://www.cisco.com/warp/public/734/configmaker después pulse Intro. Cuando se abra la pagina web de ConfigMaker, haga clic en el enlace **to download Cisco ConfigMaker, clic here**. Se abrirá la pagina del formulario de registro. Rellene el formulario y después haga clic en **Submit**. Aparecerán una serie de enlaces a distintos sitios FTP desde los que puede descargar el archivo de instalación de ConfigMaker. Seleccione un sitio FTP y complete el proceso de descarga.

Cuando la descarga se hay completado, ya puede instalar ConfigMaker en su computadora.





INSTALAR CONFIGMAKER

ConfigMaker, DE Cisco puede ejecutarse en computadoras que utilicen Microsoft Windows 95, 98, NT 4.0 y Windows 2000. Los requisitos básicos del sistema para ejecutar el softwareson los siguientes:

- Computadora 486 o superior(se recomienda Pentium).
- 16MB de RAM.
- 20MB de espacio libre en disco duro.
- Monitor SVGA a 800 X 600 con al menos 256 colores.
- Controlador de CD-ROM(si se instala ConfigMaker desde un CD).

DISEÑAR UNA INTERCONEXIÓN DE REDES CON CONFIGMAKER

ConfigMaker es, en realidad una herramienta de dibujo en la que puede crear un mapa o diagrama de una conexión entre redes. Existen iconos para routers, hubs, LAN, redes corporativas y para otros muchos dispositivos. Básicamente, tiene que arrastrar el dispositivo que desee utilizar hasta el área del diagrama de red.

Cuando arrastre dispositivos, como routers de Cisco, hasta el área del diagrama, el programa le pedirá que asigne un nombre a dicho dispositivo, así como las distintas contraseñas que desee utilizar para restringir el uso(se le pedirá que proporcione la contraseña de conexión para el router y la contraseña del modo Privilegiado). En el caso de los routers, se le pedirá también que especifique los protocolos de red(IP, IPX y Apple Talk) que soportará el router.

ConfigMaker gestiona una serie de tareas por medio de asistentes de uso sencillo. Por un lado está el **Address Network Wizard**(Asistente de dirección de red), que puede utilizarse para asignar direcciones a las interfaces de router instaladas en los distintos routers de la interconexión, y por otro el **Deliver Configuration Wizard**(Asistente de entregue de la configuración), que proporciona los pasos que deben seguirse para cargar la configuración de router en un determinado router.

Lo primero que debe hacerse al diseñar una interconexión de redes con ConfigMaker es iniciar el software. Se puede lanzar ConfigMaker desde el menú **Inicio** de Windows(haga clic en **Inicio**, seleccione **Programas,** y después haga clic en **Cisco ConfigMaker**) o haga doble clic en el icono **ConfigMaker** ubicado en el escritorio de Windows.

Al margen del método que se utilice, la ventana de aplicación de ConfigMaker se abrirá. Si esta es la primera vez que inicia ConfigMaker el programa le preguntará si desea ver el **Getting Started Tutorial** (un tutorial de inicio).

La ventana **ConfigMaker Application** está dividida en distintas áreas clave(también denominadas ventanas):

- Ventana **Devices**: Esta ventana proporciona iconos para una serie de dispositivos de Cisco, como routers, hubs y conmutadores. También contiene iconos para dispositivos de red como LAN y redes corporativas.
- Ventana **Connection**: Esta ventana proporciona los iconos para los dispositivos tipos de conexiones que pueden establecerse entre los dispositivos en el diagrama de red. Existen conexiones LAN, como Ethernet y conexiones WAN, como DIC y PPP.
- Ventana **Network Diagram**: Este es el espacio reservado para construir el diagrama de red utilizando los iconos de los dispositivos de la ventana **Device** y los distintos iconos de la ventana **Connection**.
- Lista de tareas: esta ventana proporciona una lista de comprobación de todas las tareas que deben completarse para construir un diagrama de interconexión y conectar los dispositivos en el diagrama. La ventana de la lista de tareas puede ocultarse para disponer de más espacio en la ventana **Diagram**. Para ello, haga clic en el menú **View** y después en **Task List** para desactivar la casilla de verificación y cerrar la ventana de tareas de la ventana de aplicación(si después desea abrirla en la ventana de aplicación, siga el mismo procedimiento, pero esta vez activando la casilla de verificación).
- Barra de estado: Proporciona información sobre el estado de los dispositivos cuando se cargan las configuraciones de ConfigMaker a un determinado dispositivo.

Ahora que ya conoce los distintos paneles que conforman la ventana de ConfigMaker, puede empezar a construir un diagrama de interconexión. El primer paso que debe ejecutar es añadir los dispositivos, por ejemplo routers, que formarán parte de la interconexión de redes.

OBTENER AYUDA EN CONFIGMAKER.

ConfigMaker es el típico programa Windows y como tal, proporciona un sistema de ayuda contextual. Para acceder al mismo, haga clic en el menú Help. Puede utilizar las fichas Contents, Index y Find para obtener ayuda acerca de las distintas características de ConfigMaker.

AÑADIR LOS DISPOSITIVOS

Añadir dispositivos al diagrama de interconexiones es muy sencillo. Se pueden añadir routers y otro tipo de dispositivos, como LAN.

AÑADIR ROUTERS A LA VENTANA DIAGRAM

Desplácese con el ratón por la lista **Device** hasta que localice la carpeta del router que desea añadir al diagrama. Haga clic en el símbolo **(+)** situado a la izquierda de la carpeta para abrirla.

Para añadir un router al diagrama haga clic en el icono del router deseado y después en la ventana **Diagram**. Se abrirá el asistente **Cisco router Wizard**.

En el cuadro **device name**(nombre del dispositivo) de la ventana del asistente, introduzca el nombre que desee asignar el router. Después de introducir el nombre, haga clic en **Next**.

La siguiente pantalla del asistente le pedirá que asigne una contraseña de router y una contraseña de activación(modo Privilegiado). Escriba las contraseñas que desee en los correspondientes cuadros y después haga clic en **Next.**

La siguiente pantalla le preguntará qué protocolos de red desea activar en el router. IP es el protocolo predeterminado, pero tambien puede añadir IPX y Apple Talk. Haga clic en las casillas de verificación de los protocolos que desee activar, y después haga clic en **Next**.

La última pantalla del asistente le informa de que el router se añadirá al diagrama. Haga clic en **Finish** para finalizar el proceso.

El router se mostrará en la ventana **Diagram**. Puede cambiar su ubicación en la misma arrastrándolo con el ratón. Ahora que ya tenemos un router en el diagrama, vamos a agregar una LAN que podamos conectar al router.

Deshacerse de los iconos.
Si selecciona un icono de las ventanas Device o Connection y se da cuenta de que ha seleccionado el que no debía, pulse Esc para desechar el icono antes de transferirlo a la ventana Diagram. Si ya ha ubicado en la ventana, seleccione el dispositivo y pulse la tecla Supr.

Añadir una Lan es muy sencillo. Sólo tiene que localizar el icono **LAN Ethernet** en la ventana **Devices**. Haga clic en el icono dentro de la ventana **Devices** y después haga clic en la ventana **Diagram** allí donde desee ubicar el icono de LAN.

La LAN Ethernet aparecerá en la ventana **Diagram**.

CONECTAR LAN A ROUTERS

Conectar una LAN a un router no entraña ninguna dificultad. Todo lo que tiene que hacer es seleccionar el tipo de conexión apropiado desde la ventana **Connection** y después ubicarlo entre el router y la LAN. En este punto, también tendrá que introducir la información de direccionamiento, como la dirección IP para la interfaz del router y la máscara de subred. Si seleccionó IPX y Apple Talk como protocolos soportados al añadir el router en el diagrama, además deberá proporcionar la información de direccionamiento para estos dos protocolos.

Localice el icono de Lan en la ventana **Connection**. Haga clic en el icono para seleccionarlo.

Haga clic en el router y después en la LAN seleccionada. Con ello se establecerá la conexión entre ambos dispositivos.

En cuanto haga clic en el segundo icono(la LAN), el asistente Wizard aparecerá en la pantalla. Este asistente le ayudara a establecer la conexión entre la LAN y la interfaz del router. Haga clic en **Next** para empezar.

El asistente le pedirá que introduzca la dirección IP y la máscara de subred para la interfaz, en el router(si esta encaminando IPX, le pedirá que introduzca la dirección de red IPX y en el caso de Apple Talk, el rango de cable y el nombre de zona). Introduzca la dirección IP para la interfaz del router en el cuadro **IP address**.

Introduzca la máscara de subred para la interfaz en el cuadro **Subnet Mask**. Alternativamente, puede introducir el número de bits de red más el número de bits de subred que haya utilizado para crear las subredes.

El asistente Ethernet Wizard dispone de una calculadora IP.
Si hace clic en el botón IP en la pantalla Ethernet Wizard donde ha introducido la dirección IP y la máscara de subred para la interfaz del router, podrá consultar el rango de direcciones que están disponibles en la subred que haya establecido, así como la difusión y dirección de subred para dicha subred de la que está extrayendo la actual dirección IP. Cuando calcule los rangos de direcciones IP en la subred puede utilizar la calculadora IP en el asistente Ethernet Wizard para comprobar los cálculos.

Una vez introducidas la dirección IP y la máscara de subred, haga clic en **Next** para continuar

La ultima pantalla del asistente le informará de que la conexión se ha creado perfectamente. Haga clic en **Finish** para cerrar el asistente.

La conexión se mostrará entre el router y la LAN. Para consultar el direccionamiento asociado a la conexión(la interfaz del router), haga clic en el menú **View**, seleccione **Attributes**, y después apunte a una de estas tres opciones: **IP Address, IPX Address** o **AppleTalk Address**(en función del tipo de direccionamiento de red que haya utilizado en la LAN y en el router).

Como recordará, puede tener más de un esquema de direccionamiento en el router, por lo que puede seleccionar más de una opción en el submenú **Attributes**.

Ahora que hemos visto cómo puede conectarse una LAN a un router, veamos cómo debe utilizarse ConfigMaker para configurar conexiones en serie entre routers.

CONECTAR ROUTERS ENTRE SI

Los routers pueden conectarse entre si utilizando cableado LAN(puede conectar dos routers en ConfigMaker utilizando la conexión Ethernet) o conectarlos remotamente utilizando conexiones en serie y un determinado protocolo WAN como PPP o Rele de Trama. ConfigMaker simplifica la creación de una conexión en serie entre los routers incluidos en el diagrama.

CONECTAR UN ROUTER A OTRO ROUTER CON UN PROTOCOLO WAN

Con los dos routers visibles en la ventana **Diagram**, hag clic en el tipo de conexión **Wan Protocol**(como PPP) dentro de la ventana **Connection.**

Haga clic en el primer router y después en el segundo para especificar dónde desea crear la conexión.

En cuanto haga clic en el icono del segundo router, se abrirá el asistente para el protocolo WAN que haya seleccionado(como PPP o HDLC).

Para iniciar el proceso de conexión, haga clic en **Next**.

En la pantalla siguiente el asistente le pedirá que seleccione una interfaz en serie para configurar la conexión WAN. Utilice el cuadro desplegable de la pantalla del asistente para seleccionar la interfaz en serie que desee utilizar. Después haga clic en **Next** para continuar.

En la pantalla siguiente el asistente le pedirá que introduzca la información de direccionamiento para el puerto serie que haya seleccionado. Introduzca la dirección IP y la máscara de subred, y después haga clic en **Next** para continuar.

En la pantalla siguiente, el asistente le pedirá que seleccione la interfaz en serie en el otro router. Tras seleccionar la interfaz en serie en el cuadro desplegable, haga clic en **Next**.

Introduzca la información de direccionamiento, como hizo para el otro router. Haga clic en **Next** para continuar.

La pantalla siguiente le preguntará si desea crear una conexión de copia de seguridad para esta conexión WAN. Haga clic en **Next.**

En la ultima pantalla, el asistente le indicará que se ha creado sin problemas una conexión WAN. Haga clic en **Finish**.

La conexión se creará en la ventana **Diagram**. Si tiene activado el atributo **View Addressing**, podrá ver la información de direccionamiento para la interfaz en serie de los routers creados.

DESCARGAR LA CONFIGURACIÓN EN UN ROUTER

Se puede utilizar ConfigMaker para construir un diagrama completo de interconexión de redes. Se pueden conectar LAN y routers, host y routers, y hasta conectar routers entre sí. De hecho, prácticamente todos los dispositivos que puedan requerirse y los distintos tipos de conexiones están disponibles en las ventanas **Device** y **Connection**. Una vez construida la interconexión, se pueden utilizar directamente en el router los parámetros de configuración introducidos para las interfaces del router(o routers).

Puede descargar una configuración a un router o a varios routers utilizando un PC que ejecute ConfigMaker y esté conectado a la misma red a la que estén conectados los routers. Pero para ello, tiene que haber configurado antes el PC y los routers con las direcciones IP para que ConfigMaker pueda transmitir la configuración por la red. Esto supone "preconfigurar" el router utilizando la consola del router.

Una forma fácil de transmitir rápidamente una configuración a un router que no contiene ningún tipo de información de configuración, es descargar la configuración desde un PC que ejecute ConfigMaker y que esté conectado al router a través del puerto de la consola y el cable enrollado de la consola. El PC se conecta al router del mismo modo que se conecta una consola de PC.

Lo primero que debe comprobar antes de transmitir la configuración, es que ConfigMaker transmita el puerto de configuración utilizando el puerto serie oportuno en la computadora. El puerto predeterminado es COM 1.

Si tiene que cambiar el parámetro COM del puerto, haga clic en el menú **View**, y después seleccione **Options.** En el cuadro de dialogo **Options**, utilice el cuadro desplegable de puerto COM para seleccionar el puerto COM adecuado y haga clic en **OK.**

TRANSMITIR UNA CONFIGURACIÓN DE ROUTER UTILIZANDO EL PUERTO DE LA CONSOLA.

Con el diagrama de interconexión abierto en ConfigMaker que contiene la configuración del router desea transmitir, seleccione el icono de router apropiado.

Haga clic en el botón **Deliver** incluido en la barra de herramientas de ConfigMaker. Se abrirá el asistente **Deliver Configuration wizard**, mostrando el router que ha seleccionado en el diagrama.

Haga clic en **Next** para continuar. En la pantalla siguiente, el asistente le pedirá que se asegure de que ningún otro programa esté utilizando el puerto COM que se utilizará para transmitir la configuración(si ese PC sirve también como consola del router, asegúrese de que su software de emulación de terminal no se esté ejecutando en ese momento.

Cuando esté preparado para transmitir la configuración, haga clic en **Next**.

El estado de la transmisión de la configuración se mostrará en la pantalla del asistente. La configuración que tuviera el router en ese momento(si tenía alguna)se borrará, y después el router volverá a iniciarse. La nueva configuración se cargará en la memoria NVRAM del router.

Aparecerá una última pantalla en la que el asistente la indicará el nombre del router, el método de entrega(la consola) y la hora y fecha en que se completó dicha entrega.
Haga clic en **Finish** para cerrar el cuadro del asistente.

El router esta ahora configurado con la información de configuración que ha descargado. Utilice su software de emulación de terminal y comprueba la configuración descargada.

Cuando termine de trabajar en un determinado diagrama de interconexión, haga clic en el botón **save** incluido en la barra de herramientas de ConfigMaker. En el cuadro de dialogo **Save as,** escriba un nombre para el diagrama de interconexión y utilice el cuadro desplegable **Save In** para especificar una unidad y carpeta para el archivo. Haga clic en **save** dentro del cuadro de dialogo para guardar el diagrama.

Para salir de ConfigMaker, haga clic en el menú **File** y después en **Exit**.

ConfigMaker sirve para configurar LAN Ethernet, OJO ConfigMaker no permite configurar LAN Token ring.V

Con soporte para un amplio abanico de dispositivos y protocolos de Cisco, solo hasta enrutadores de la serie 4000, no tiene soporte para la gama alta de Cisco, series 7000 y sucesivas.

En el centro del escritorio de ConfigMaker hay un área de diagrama de red en la que se colocan, configuran y enlazan entre si los objetos de la red. Al principio el área esta vacío.

El diagrama de red esta rodeado de tres ventanas:

Ventana Device. Origen de los dispositivos que hay que arrastrar y colocar en el área de diagrama de red.

Ventana Conections. Origen para conexiones de red que hay que arrastrar y colocar en el área de diagrama de red.

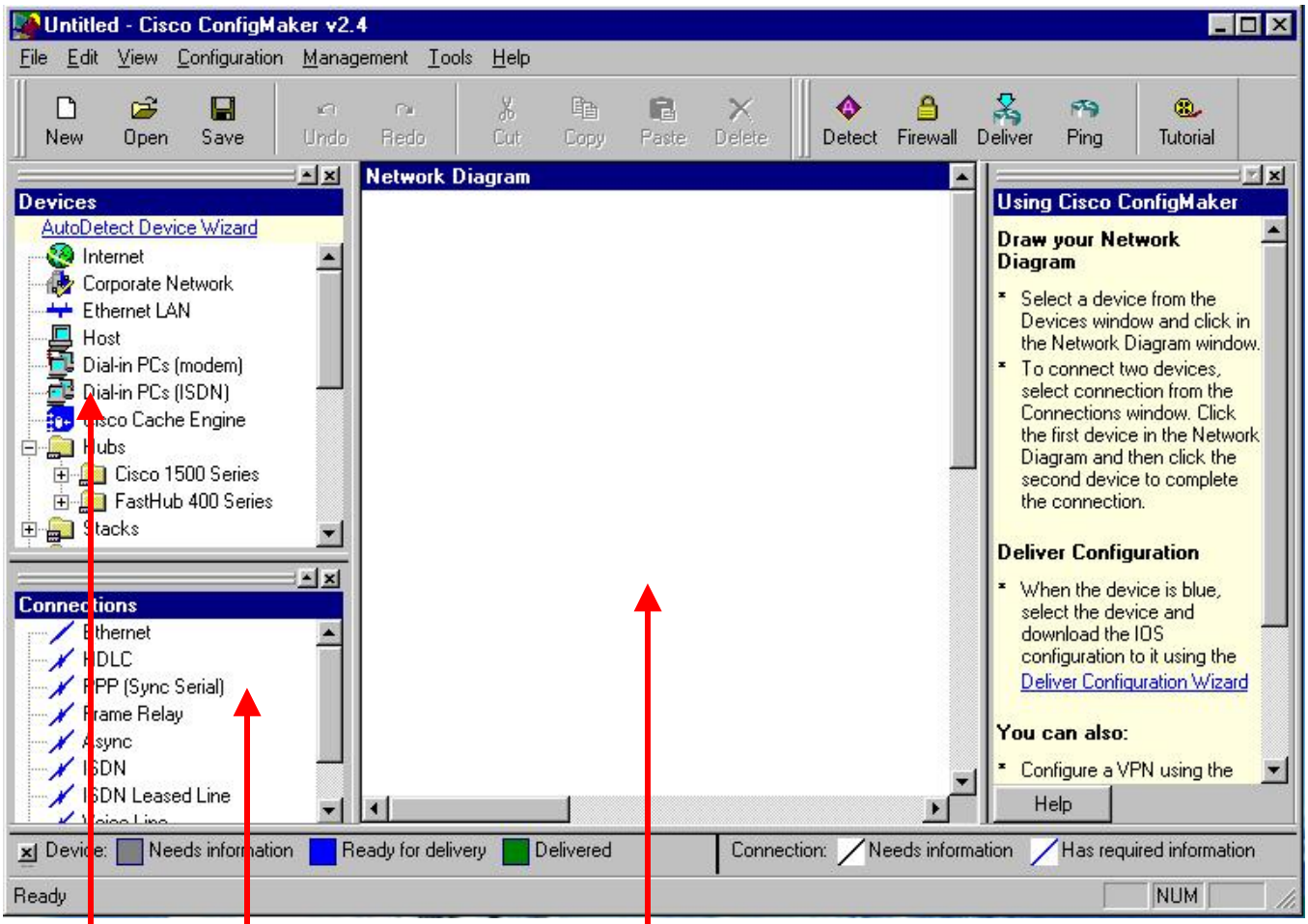
Task List. Lista de comprobación de los pasos cronológicos que deben realizarse en la configuración de la red.
El primer paso es arrastrar y colocar los dispositivos desde la ventana Device al área de diagrama de red, a medida que se coloca cada dispositivo en el diagrama de red, ConfigMaker solicita los valores de configuración necesarios para que sea funcional.
Una vez colocados los dispositivos en el diagrama de red hay que conectarlos a una red, esto se hace arrastrando una o más conexiones desde la ventana conections.

ConfigMaker es algo más que un programa de diagramas de red. Cada elemento que se coloca en el diagrama dispone de inteligencia. A medida que se coloca cada objeto en el diagrama de red(dispositivo o conexión), ConfigMaker pregunta acerca de detalles de elementos de línea como configuraciones, nombres y cosas similares.
Esta información se almacena en una base de datos oculta detrás del diagrama y la usa ConfigMaker para verificar la consistencia interna. ConfigMaker impone una metodología para asegurar la calidad sobre el proceso de diseño de red:

- Conforme se agrega un dispositivo a la red, se recopila información sobre él.
- Se comprueba la consistencia de la información con el resto de la base de datos.
- Si se produce un error, ConfigMaker avisa al usuario para que lo corrija.
- La lógica basada en reglas de ConfigMaker sigue comprobando toda la red para verificar que es correcta mientras se agrega un nuevo dispositivo.

También tienes la herramienta Fast Step para configurar e instalar pequeños enrutadores y servidores de acceso Cisco. Las dos herramientas usan una interfaz gráfica de usuario. Las dos herramientas te las puedes bajar de Internet: http://www.cisco.com/public/sw-center/sw-netmgmt.shtml

Ahora mucha practica y dedicación.



CONEXIONES

DISPOSITIVOS

DIAGRAMA

FAST STEP.

Una herramienta de gama baja que se ejecuta sobre Windows y se utiliza para configurar e instalar pequeños enrutadores y servidores de acceso de Cisco, pensada para que la utilicen los usuarios menos expertos.

Es una utilidad de configuración que se incluye con los enrutadores y servidores de acceso de gama baja. Está destinada para que la utilice el usuario de red principiante con el fin de configurar conexiones punto a punto entre un PC y un proveedor de servicios de Internet (PSI) o intranets corporativas. Fast Step se ejecuta sobre Microsoft Windows 95, 98, NT, 2000. Se distribuye en un CD-ROM para su instalación en un PC Windows. Fast Step se puede utilizar de dos formas:

- Para configurar el enrutador interactivamente mientras está conectado al enrutador, ya sea mediante un cable serie desde el puero COM del PC al puero de consola del enrutador o mediante un enlace Ethernet.
- Para generar un archivo de configuración con el fin de descargarlo posteriormente al enrutador, o como base para configurar otros enrutadores(es posible leer el archivo mediante Setup Wizar de Fast Step).

Después de instalar Fast Step si hace clic en el icono se iniciará una secuencia de cuadros de dialogo solicitando al usuario que introduzca la información necesaria para configurar e instalar el enrutador. La secuencia puede abarcar alrededor de una docena de cuadros de dialogo, dependiendo de las opciones elegidas. Para ayudar a ordenar las cosas cada pantalla de Fast Step tiene una ventana Tareas en el lado izquierdo. Usted puede ver su situación en el proceso buscando qué tarea está destacada en la ventana Tasks en la parte izquierda de cada pantalla de Fast Step.

Fast Step divide las tareas de configuración en cuatro pasos.

Paso	Descripción de tares
Find and connect	Proporcionar el nombre del enrutador; seleccionar modo de configuración(interactivo o descarga); definir el tipo de conexión (PSI u organización); ofrecer valores de configuración; acceder a la dirección IP y a los números de teléfono, nombre de usuario, contraseña, etc.
Security	Especificar nombre de enrutador, contraseña de sólo lectura de enrutador y contraseña de habilitación secreta del enrutador; especificar los tipos de servicios (servidor Web, servidor de correo, servido FTP).
Local Addressing	Especificar direcciones IP para conexiones LAN proporcionadas por PSI o por Intranet de una organización.
Setup and Test	Guardar el archivo config en el enrutador y ponerlo a funcionar, guardar el archivo config para usarlo con otros enrutadores.

Dto.:	Operación y red	Proyecto:	CCNA
Autor:	Elwa y Chechu	Fecha:	01/04/02
Asunto:	Preparación para certificación CCNA Cisco Systems		
Estado:	Pendiente revisión	Revisión:	1.0

INTRODUCCIÓN A CISCO FAST STEP

El software Cisco Fast Step incluye una aplicación Setup y una aplicación Monitor. Esta versión del conjunto de aplicaciones está diseñada para su utilización con los siguientes routers:

- Routers de la serie Cisco 800.

Otras versiones de Cisco Fast Step admiten los siguientes routers:

- Routers de las series Cisco 1601 a 1604 equipados con una interfaz WAN en placa (también es compatible con WIC opcional).
- Cisco 1605 con dos interfaces Ethernet en placa (también es compatible con WIC opcional).
- Routers Cisco 2509 y 2511.
- Routers Cisco 2610.
- Routers de las series Cisco 5200 y 5300.

SETUP

Cisco Fast Step Setup configura y realiza una prueba al router a través de la red Ethernet o del cable serie de configuración. Pone a prueba la funcionalidad del router y sus conexiones. Si hay cualquier tipo de problemas, Setup sugiere recomendaciones para solucionarlos.

MONITOR

Cisco Fast Step Monitor muestra información detallada sobre el funcionamiento del router en la LAN, incluyendo el estado de las interfaces WAN, detalle de los errores y estadísticas de uso.

Nota_
La configuración que depende del país está vinculada a la Configuración Regional de Windows del PC que ejecuta el software Cisco Fast Step.

Nota_
Cisco Fast Step admite también routers de la serie Cisco 700. Sin embargo, como los routers de la serie Cisco 700 utilizan un sistema operativo exclusivo en Internet, es preciso utilizar un conjunto de aplicaciones de Cisco Fast Step diferente.

UTILIZAR LA AYUDA EN LÍNEA DE CISCO FAST STEP

La ayuda de Cisco Fast Step tiene tres modalidades:

- Ayuda de Windows proporciona información detallada para ayudarle a sacar el mayor partido posible del software Cisco Fast Step. Haga clic en Ayuda en la ventana de Cisco Fast Step para que aparezca la ayuda de Windows. La ayuda que aparece se corresponde con la ventana que se esté utilizando. El sistema de ayuda es similar a otros sistemas de ayuda basados en Windows; se utilizan enlaces de hipertexto para desplazarse de un tema a otro.

Para hacer que aparezca la ayuda de Windows, haga clic en el botón Ayuda en la ventana de la aplicación.

- Ayuda rápida proporciona una breve descripción del tema activo. Aparece en un campo azul cercano a la parte inferior de las ventanas de Setup (la Ayuda rápida no se encuentra disponible en Monitor). Cuando se abre una ventana, aparece una descripción general de la misma. A medida que se desplaza el puntero del ratón por los campos de la pantalla, el contenido de la ventana cambia a fin de describir el campo. Si aparece un mensaje en respuesta a un error, el fondo de la zona de Ayuda rápida pasa a ser amarillo.

Si se desea que aparezca la ayuda rápida para una zona específica de la pantalla, mantenga el puntero del ratón durante tres o más segundos sobre el campo deseado.
Para que vuelva a aparecer el texto de ayuda general, mantenga el puntero del ratón en una zona neutral de la ventana.

- La Ayuda contextual muestra una breve descripción de un campo en un recuadro situado al lado de dicho campo.

Para que aparezca la ayuda de acercamiento, sitúe el puntero del ratón sobre un campo.

BOTONES DE LOS COMANDOS

Hay cuatro botones de comandos en la parte inferior de la mayoría de las ventanas de Cisco Fast Step:

- Con Siguiente se pasa a la siguiente tarea. Hay que hacer clic en él cuando se termina de introducir información en una ventana.

- Prueba o configuración es un botón dinámico que aparece cuando falla un estado de configuración o prueba. Este botón le permite pasar directamente al estado de prueba o de configuración sin tener que pasar por los cuadros de diálogo intermedios.

- Con Atrás se vuelve a la ventana anterior.

- Con Salir se abandona la aplicación y se guardan los valores introducidos. Cuando se reinicia la aplicación se regresa automáticamente a este punto.

- Con Ayuda se accede al sistema de ayuda en línea de Windows.

INFORMACIÓN GENERAL SOBRE LAS VENTANAS

Casi todas las ventanas de Cisco Fast Step Setup tienen el mismo formato. En el lado izquierdo de la ventana se encuentra la Lista de tareas, que divide el proceso de configuración del router en grupos primarios de tareas. Indica qué tareas se han realizado y cuántas quedan por hacer.

Las tareas individuales se llevan a cabo en la zona superior derecha de la ventana. Aquí es donde se indican las preferencias seleccionando elementos o introduciendo parámetros.

En la esquina inferior derecha de las ventanas de Setup se encuentra ubicada una zona de ayuda rápida (las ventanas de Monitor no cuentan con zonas de ayuda rápida). La zona de ayuda rápida muestra breves descripciones del elemento que se está señalando. A medida que se desplaza la flecha del puntero por la ventana, el texto de la ayuda rápida cambia (los campos inactivos aparecen tenues y si se hace clic en ellos no pasa nada).

ORDEN HABITUAL DE LA CONFIGURACIÓN

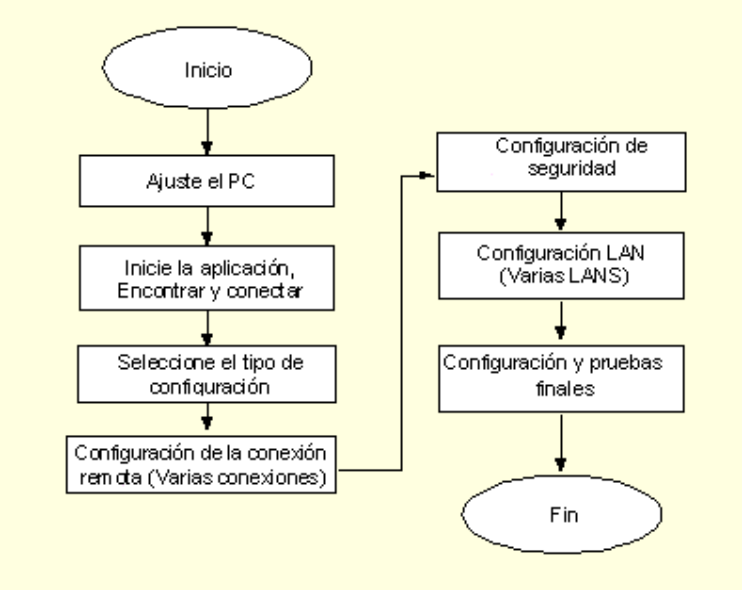
El siguiente diagrama muestra el orden habitual de la configuración de Cisco Fast Step. Cada bloque representa un grupo que contiene ventanas relacionadas.

Setup encuentra el router, conectándose con él para configurarlo. Entonces determina si utilizar la información sobre la configuración que está en un archivo de disco existente o seguir el asistente para configurar el router y crear un archivo de instalación.

Setup solicita en primer lugar las configuraciones de la conexión (WAN) remota y seguidamente las de la LAN. Si hay dos o más puertos LAN, solicita información de los dos. A continuación solicita la información de seguridad para el router.

Setup carga toda la configuración en el router y prueba todas las conexiones. Si existen problemas, se regresa a la ventana apropiada.

Por último, Setup ajusta la/s computadora/s para que pueda/n acceder a redes remotas.



DETERMINACIÓN DEL ESCENARIO DE LOS PROTOCOLOS

Setup determina el número de conexiones remotas que se crean y se conecta con el proveedor de servicios Internet, la red remota de la empresa o una interfaz WAN utilizada para hacer de conexión de seguridad de dichas ubicaciones de la siguiente manera:

- Para una red remota de la empresa, Setup le solicita que los protocolos se enruten a la red remota.
- Para un proveedor de servicios Internet, Setup asume que IP es el único protocolo que hay que enrutar.

La siguiente tabla describe cómo se determinan las configuraciones en cada uno de los escenarios.

Protocolo	Una conexión remota	Dos conexiones remotas	WAN primaria y de seguridad
IP	Enrutamiento estático, enviando todo el tráfico de Internet a la interfaz WAN.	La interfaz WAN enruta a IP y es la puerta de enlace a Internet. Si las dos interfaces se están enrutando a IP, se asume que la conexión con el proveedor de servicios Internet es la puerta de enlace.	Las rutas estáticas se utilizan para enviar todo el tráfico de Internet a las interfaces WAN.
IPX	Utiliza el número de red IPX LAN, el tipo de entramado y el número de red IPX WAN 1.	Utiliza el número de red IPX LAN, el tipo de entramado y los números de red IPX WAN 1 y WAN 2.	Compatible.

Fast Step solamente solicita la dirección WAN si no se puede adquirir automáticamente a través del protocolo de control IP.

EL ENRUTAMIENTO EN CISCO FAST STEP

Cisco Fast Step procura aclararle lo más posible los temas relativos al enrutamiento, pero es importante comprender algunas de las limitaciones, ya que implican una configuración particular en el extremo remoto.

En los tipos WAN que no utilizan el protocolo RDSI, RIP está activado. Sin embargo, en una conexión RDSI, si RIP está activado, la línea está activa constantemente.
En IP, todos los paquetes que no están destinados a la LAN salen a la WAN a través de la puerta de enlace predeterminada.

En una única conexión con el proveedor de servicios Internet o la red remota de la empresa, no se necesita ningún tipo de enrutamiento para conectarse a la red; la ruta predeterminada al proveedor de servicios Internet o a la red remota de la empresa es la única ruta disponible.

Para descubrir la ruta durante la configuración, Cisco Fast Step Setup activa provisionalmente RIP y convierte las tablas RIP y SAP en rutas estáticas y SAP.

La excepción es la utilización de IPX sin IP. Los paquetes que no saben dónde ir (y con IP se enviarían a la WAN de manera predeterminada) no se envían automáticamente a una puerta de enlace predeterminada. Por lo tanto, es preciso forzar la ruta de manera estática o dinámica. Si se salta las pruebas o si se utiliza Setup en el modo Crear Archivo, es necesario agregar rutas IPX y SAP uno mismo.

SOPORTE TÉCNICO DEL ROUTER

Existe un soporte técnico disponible para el software Cisco Fast Step y para el router Cisco. Póngase en contacto con el administrador del sistema o con el proveedor de servicios en los números de teléfono y en las direcciones de correo electrónico que aparecen en la ventana Soporte técnico.

Tenga a mano la información de la ventana Soporte técnico, ya que su personal se la pedirá y la utilizará para ayudarle a solucionar el problema.

La información del soporte técnico capturada viene de los siguientes comandos IOS:

```
show version
show running-config
show controllers
show stacks
show interfaces
show process memory
show process cpu
show buffers
```

REALIZAR UN BACKUP DE LA IMAGEN CISCO IOS.

Cargar la imagen Cisco IOS desde varias fuentes.

Crear y copiar un backup de la imagen IOS desde un servidor TFTP.

```
Router#configure terminal
Router(config)#boot system ?
WORD System image filename
Flash boot from flash memory
Mop boot from a Decnet MOP server
Rcp boot from a server via rcp
Tftp boot from a tftp server
```

Cuando arrancamos desd3e un servidor TFTP necesitamos un parámetro adicional que es la dirección de este.

FLASH

Boot system flash[nombre fichero IOS]

ROM

Boot system rom

TFTP SERVER

Boot system tftp[nombre del fichero][dirección del servidor tftp]

Copy flahs tftp copia una imagen de cisco IOS de la memoria Flash a un servidor TFTP. Este comando necesita del parámetro nombre del fichero y del parámetro dirección del servidor tftp.
Para parar el proceso de copia se utiliza el parámetro "Ctrl ^"

Copy tftp flash comando que copia una imagen cisco IOS desde un servidor TFTP a la flash del router, este comando necesita de los parámetros, nombre del fichero y dirección del servidor tftp.
NOTA: Si el fichero que queremos copiar ya existe el router lo notificará y preguntará si se quiere borrar el existente.

Dto:	Operación y red	Proyecto:	CCNA
Autor:	Elva y Chechu	Fecha:	01/04/02
Asunto:	Preparación para certificación CCNA Cisco Systems		
Estado:	Pendiente revisión	Revisión:	1.0

UTILIZAR UN SERVIDOR TFTP PARA GUARDAR LA CONFIGURACIÓN DE UN ROUTER.

Guardar las configuraciones de router en una ubicación distinta de la propia memoria NVRAM del router es una forma de proteger el tiempo y el esfuerzo invertidos en configurar un determinado router. La posibilidad de guardar una copia de seguridad del archivo de configuración es una parte fundamental del desarrollo de algún tipo de tolerancia a fallos dentro de la interconexión de redes construida.

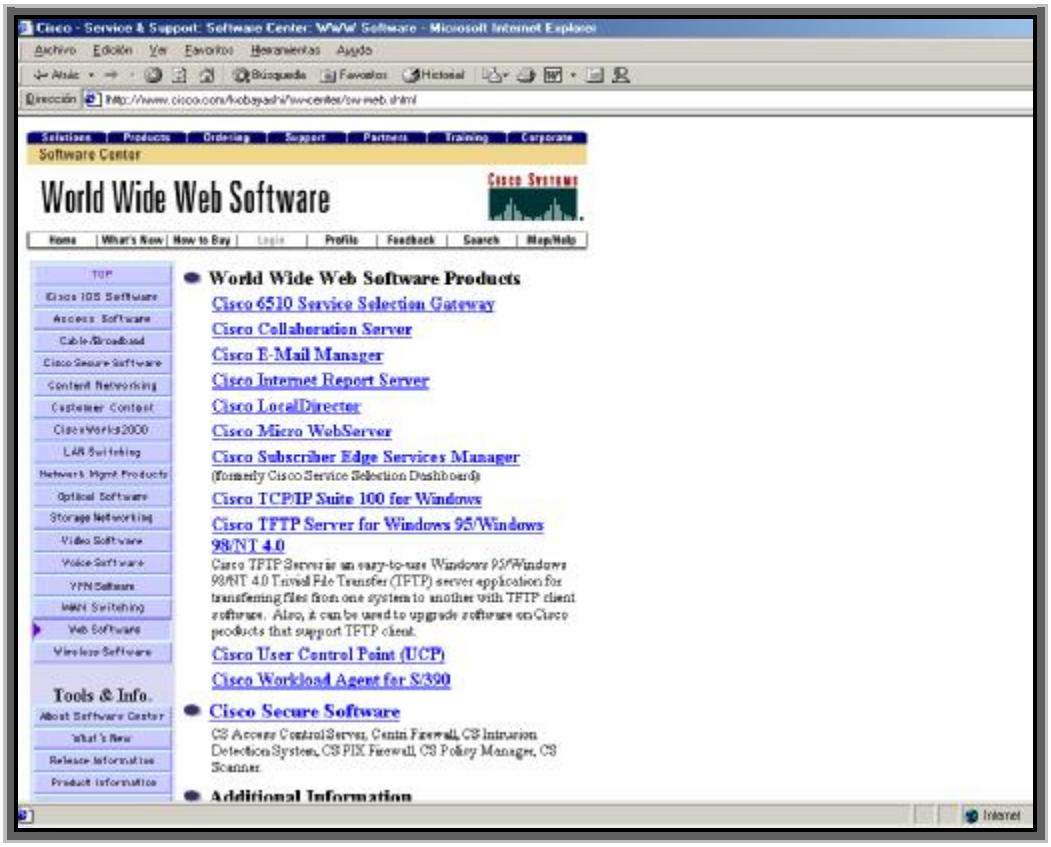
Existen varios paquetes de software de servidor TFTP. Cisco proporciona una aplicación gratuita de servidor TFTP a los usuarios registrados de productos Cisco. El software de servidor TFTP puede descargarse desde el sitio web de Cisco, en **www.cisco.com**.

Un programa compartido de servidor TFTP es el servidor TFTP SolarWinds disponible en **http://www.solarwinds.net/** **SolarWinds** incluye una serie de herramientas especificas para routers Cisco.

El software de servidor se inicia y después se ejecutan los comandos pertinentes en el router. El servidor TFTP es más bien pasivo durante todo el proceso, pero la mayoría de aplicaciones de servidor TFTP incluyen una ventana en la que se muestra el estado de una copia dirigida al servidor o procedente del mismo.

Si desea utilizar el software de servidor TFTP de Cisco, todo lo que tiene que hacer es conectarse al sitio web de cisco(**www.cisco.com**) y hacer clic en el enlace **Software Center** de la pagina de inicio de Cisco.

Dto:	Operación y red	**Proyecto:**	CCNA
Autor:	Elwa y Chechu	**Fecha:**	01/04/02
Asunto:	Preparación para certificación CCNA Cisco Systems		
Estado:	Pendiente revisión	**Revisión:**	1.0



INSTALAR EL SOFTWARE DE SERVIDOR TFTP DE CISCO

El software de servidor TFTP de Cisco puede instalarse en una estación de trabajo Windows 95/98 que se encuentre en la misma red que el router(esto significa que el router será la pasarela predeterminada del servidor TFTP). La dirección IP para la estación de trabajo tiene que estar además instalada en el mismo rango de subred.

Una vez determinado el direccionamiento IP, puede pasar a instalar el software de servidor TFTP en la estación de trabajo. El proceso de instalación es muy sencillo.

Una vez que el software esta instalado en la estación de trabajo que se utilizara como servidor TFTP, puede pasar a copiar archivos a y desde el router.

REALIZAR UNA COPIA EN EL SERVIDOR TFTP

Como dijimos anteriormente, se puede copiar el archivo de la configuración de arranque desde la NVRAM, o el archivo de configuración de la ejecución desde la RAM, al servidor TFTP. Esto nos permitirá restaurar el archivo de configuración de arranque en el router desde el servidor TFTP en caso de catástrofe.

COPIAR EL ARCHIVO DE ARRANQUE EN EL SERVIDOR TFTP

Inicie el software del servidor TFTP en la estación de trabajo: seleccione **inicio, Programas,** y después haga clic en **Cisco TFTP Server**. Se abrirá la ventana **TFTP Server**. La ventana no es más que un cuadro vació y gris en el que sólo se incluye la dirección IP del servidor TFTP(la computadora en la que se está ejecutando el software) en la barra de titulo.

En la consola del router, lance el modo privilegiado.En el indicador del router, introduzca **copy startup-config tftp**, y después pulse Intro.

El sistema le pedirá que proporcione la dirección IP de host remoto. Introduzca la dirección IP del servidor TFTP. Después pulse Intro.

El sistema le pedirá que facilite el nombre del archivo que desea copiar en el servidor. Por defecto, se muestra el nombre del router seguido de **config**(como **cisco2505-config**). Pulse Intro para aceptar la opción predeterminada o introduzca un nombre del archivo de configuración que desea copiar y pulse Intro.

Se le pedirá que confirme la tarea que va a llevarse a cavo. Pulse Intro para confirmar(en caso contrario escriba **n** para decir que no y volver al indicador del modo privilegiado).

El archivo se escribirá en el servidor TFTP. El indicador **Writing router name-config !![OK]** que se muestra en la pantalla significa que la copia se ha realizado sin problemas. De hecho, si vuelve a la estación de trabajo del servidor TFTP y consulta la ventana del servidor, verá que se ha creado un registro de la copia. La ventana del servidor TFTP también confirma que la copia se ha realizado con éxito.

VISUALIZAR EL ARCHIVO COPIADO

Puede consultar el archivo de configuración que se ha copiado utilizando el Explorador de Windows en la estación de trabajo del servidor TFTP. Con el botón derecho del ratón haga clic en el icono MI PC y seleccione Explorar en el menú contextual. La ubicación predeterminada para la carpeta del servidor TFTP es C:\CiscoSystems\CiscoTFTPServer. Acceda a esta carpeta desde el explorador y podrá ver la copia del archivo de configuración que se ubicó allí durante el proceso de copia.

Tambien se puede copiar el archivo de configuración de la ejecución desde la RAM utilizando el mismo procedimiento arriba descrito. La única diferencia es que el comando que se debe introducir en el paso 3 es **copy running-config tftp**.

REALIZAR UNA COPIA DESDE EL SERVIDOR TFTP

La operación inversa, copiar un archivo desde el servidor TFTP al router, es tan sencilla como el proceso descrito en el apartado anterior. Se puede copiar un archivo de configuración desde el servidor TFTP a la memoria NVRAM del router o copiar la configuración desde el servidor directamente a la memoria RAM como una nueva configuración.

Si se copia el archivo a la NVRAM, no solo pasará a convertirse en el nuevo archivo de configuración del router, sino también será la configuración de arranque cuando se vuelva a arrancar el router. Veamos como se copia el archivo de configuración desde el servidor a la memoria NVRAM donde pasa a convertirse en la nueva configuración de arranque para el router.

Inicie el software del servidor TFTP en la estación de trabajo.

En la consola del router, lance el modo privilegiado. En el indicador del router escriba **copy tftp startup-config**, y después pulse Intro.

El sistema le pedirá que proporcione la dirección IP del host remoto. Introduzca la dirección IP del servidor TFTP. Después pulse Intro.

El sistema le pedirá que facilite el nombre del archivo de configuración incluido en el servidor TFTP que desea copiar. Introduzca el nombre en el indicador. Pulse Intro para continuar.

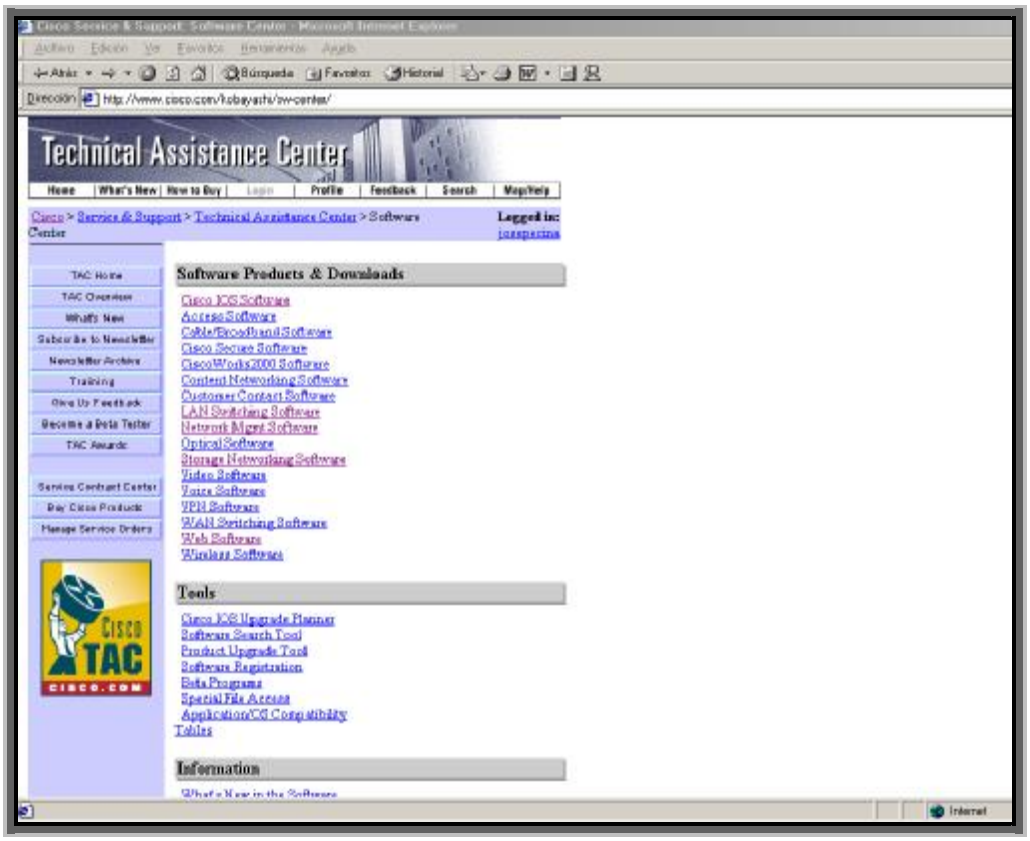
Se le pedirá que confirme la tarea que va a llevarse a cavo. Pulse Intro para confirmar(en caso contrario escriba **n** para decir que no y volver al indicador del modo privilegiado).

El archivo se cargará en el router y pasará a ser la configuración activa(guardad en la NVRAM). Aparecerá de nuevo un menjase **[OK]** en el router indicando que el proceso se ha completado con éxito. Puede volver al servidor TFTP y ver la confirmación del proceso en la pantalla.

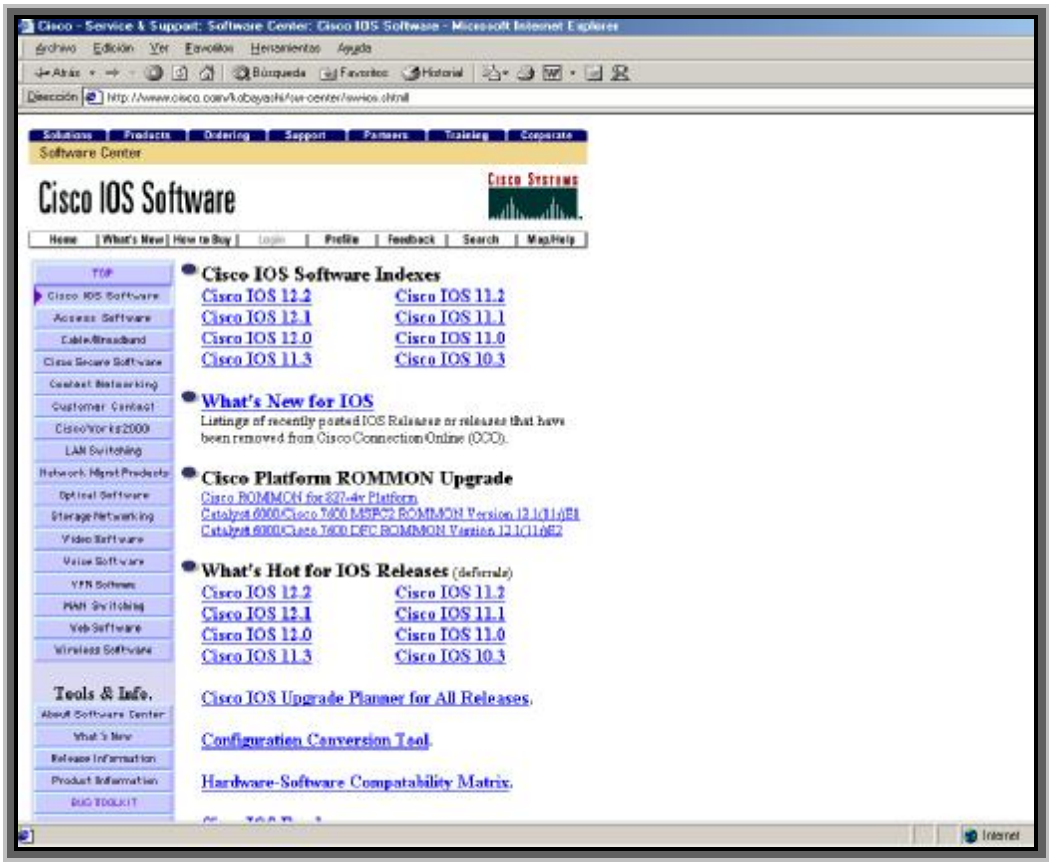
CARGAR UN NUEVO IOS DESDE EL SERVIDOR TFTP

Como HABRÁ Podido comprobar, copiar desde y hacia el servidor TFTP es un proceso realmente sencillo. También puede utilizar el servidor TFTP para copiar varias versiones del IOS de Cisco en la memoria flash RAM del router. De esta forma, la actualización del sistema operativo en el router será como coser y cantar.

Cisco ajusta constantemente el IOS instalado en sus routers. Actualmente existen varias versiones distintas del mismo. Lógicamente, como ocurre con los restantes sistemas operativos, siempre se acaban detectando errores que pasan a corregirse, por lo que también existen versiones de actualización para las nuevas versiones del IOS. Puede consultar las versiones más recientes de IOS en el sitio web de cisco.



Para descargar imágenes de sistema operativos(es decir archivos), se tiene que contar primero con un contrato de actualización con el distribuidor de Cisco que realizo la venta del router. Un contrato de actualización válido tiene que incluir un número con el que poder registrarse en el sitio web de Cisco para descargar archivos del IOS. Esta página incluye enlaces a distintas imágenes IOS y también proporciona un planificador IOS que permite seleccionar las nuevas versiones del IOS para el router que tenga.



Para cargar la nueva versión del IOS en la memoria flash RAM de un router, descargue la imagen del IOS que proceda en su caso desde el sitio web de Cisco. Ubique el archivo del IOS en la carpeta de arranque del servidor TFTP. Por defecto, esta carpeta se encuentra en C:\CiscoSystems\CiscoTFTPServer , y puede utilizar el explorador de Windows para copiar o mover el archivo a la carpeta apropiada.

Ahora ya puede copiar la nueva versión del IOS en la memoria flash del router. Tenga el cuenta que esta nueva versión sustituirá a la versión anterior. Puede elegir que la memoria flash RAM no se borre durante el proceso de copia, pero eso no significa que vaya a terminar con varias copias de IOS en la flash; depende del espacio disponible en la memoria flash.

Una vez cargado el archivo en el servidor TFTP, ya puede iniciar el proceso que transfiera el archivo del IOS al router.

COPIAR UN NUEVO IOS A LA MEMORIA FLASH RAM DEL ROUTER

Inicie el software del servidor TFTP en la estación de trabajo.

En la consola del router, lance el modo privilegiado. En el indicador del router, escriba **copy tftp flash** y después pulse Intro.

El sistema indicara que el router va a proceder a realizar la copia, aunque las funciones del router se detendrán mientras se actualiza la imagen del IOS. Para proceder pulse Intro.

El sistema le pedirá que especifique la dirección IP del host remoto. Introduzca la dirección IP del servidor TFTP. Después pulse Intro.

El sistema le pedirá entonces que especifique el nombre del archivo IOS incluido en el servidor TFTP que desea copiar. Introduzca el nombre en el indicador, asegurándose de que dicho archivo es la imagen del IOS. Pulse Intro para continuar.

Después se le pedirá el nombre del archivo de destino. Acepte el nombre que se ofrece por defecto y pulse Intro.

El sistema le indicara entonces que la memoria flash RAM se borrará antes de cargar la nueva versión del IOS y le pedirá que confirme esta acción. Pulse Intro para confirmarla. Puesto que la memoria flash contiene la versión actual del IOS, el sistema le pedirá una segunda confirmación. Pulse Intro para aceptar.

Se le pedirá entonces si desea guardar la configuración modificada del sistema. Escriba **yes**, y después pulse Intro.

El sistema le pedirá una última confirmación antes de proceder a borrar la memoria flash. Escriba **yes**, y después pulse Intro.

La imagen de IOS que existía se borrará y será reemplazada por la nueva imagen del IOS. En el router aparecerá una serie de puntos de exclamación mientras se realiza el proceso, que puede tardar algunos minutos debido al tamaño de algunas imágenes del IOS(la versión 11.2 del IOS ocupa 6MB). Si echa una ojeada a la ventana del servidor TFTP de Cisco, verá repetirse una serie de símbolos numéricos(#) por la pantalla mientras se ejecuta el proceso.

El router volverá a arrancarse cuando termine de copiarse el nuevo archivo del IOS. Para ello, pulse Intro e introduzca la contraseña de consola(si el sistema la pide) para ir al indicador del modo Usuario. Para ver la nueva imagen del IOS, escriba **show flash** en el indicador, y después pulse Intro. La nueva imagen de IOS(el nombre del archivo que introdujo en el paso anterior)debería estar ubicado en la memoria flash del router.

También puede copiar la nueva imagen del IOS en el servidor TFTP si así lo desea. De esta forma dispondrá de una copia de seguridad en caso de que se estropee la memoria flash RAM en el router o simplemente para guardar una copia de IOS en una segunda ubicación para mayor seguridad. Para ello, debe introducir, en el indicador del modo privilegiado, el comando **copy flash tftp**. Tendrá que especificar la dirección IP del servidor y el resto de información descrita en los pasos anteriores.

Los servidores TFTP suponen un excelente almacén para guardar archivos alternativos de configuración y actualizaciones del IOS. Proporcionan el espacio suficiente para almacenar sus copias de seguridad del que carece el router.

NOVELL IPX

Netware 5, las redes Novell pueden funcionar de forma nativa sobre TCP/IP, sin necesidad de soporte IPX.
Novell ofrece sus propios productos de enrutamiento.
Los router CISCO ofrecen las siguientes características en entornos de redes Novell:

- Soporte para variedad de interfaces(RDSI) y (ATM).
- Listas de acceso y filtros para IPX,(RIP),protocolo de publicación de servicios(SAP),programa de control de red(NCP) y sistema básico de entrada/salida de red(NETBIOS).
- Protocolos de enrutamiento escalable(EIGRP)y el protocolo de servicios de enlace NETWARE(NLSP).
- Intervalos de actualización RIP y SAP configurables.
- Soporte para redes de área local(LAN) sin servicio.
- Enrutamiento por llamada telefónica bajo demanda(DDR)y SPOOFING para IPX e intercambio secuencial de paquetes(SPX).
- Características avanzadas de diagnostico, administración y resolución de conflictos.

PILA DEL PROTOCOLO NETWARE IPX

Novell IPX/SPX intercambio de paquetes entre redes/intercambio secuencial
de paquetes.

Conjunto de protocolos propietario, derivado del conjunto de protocolos sistemas de redes de XEROS(XNS).

<table>
<tr><th>Modelo de referencia OSI</th><th colspan="5">Protocolos de Novell Netware</th></tr>
<tr><td>Aplicación</td><td rowspan="3">RIP
NLSP</td><td rowspan="3">SAP</td><td rowspan="3">NCP</td><td rowspan="3">NETBIOS</td><td rowspan="2">APLICACIONES</td></tr>
<tr><td>Presentación</td></tr>
<tr><td>Sesión</td><td>SPX</td></tr>
<tr><td>Transporte</td><td colspan="5">IPX
Intercambio de paquetes entre redes.</td></tr>
<tr><td>Red</td><td colspan="5">Protocolos de acceso al medio</td></tr>
<tr><td>Enlace de datos</td><td colspan="5" rowspan="2">(Ethernet, Token ring, Wan, otros)</td></tr>
<tr><td>Física</td></tr>
</table>

IPX es:

Un protocolo de datagramas sin conexión que no requiere acuse de recibo para cada paquete.(Es parecido a IP y a UDP).
Un protocolo de la capa tres que define las direcciones de la capa de red, y que incluye un designador de red.nodo.

Novell Netware utiliza su propio:
Protocolo de información de enrutamiento(IPX/RIP) para facilitar el intercambio de la información de enrutamiento.

Protocolo de publicación de servicios(SAP) para publicar, o anunciar y localizar servicios de red. Un tipo de difusión SAP es obtener el servidor más cercano (GNS), que permite a un cliente localizar el "servidor más cercano" para iniciar una sesión.
Si hay dos servidores en la misma red, el primero que responda será aceptado como "el servidor más cercano" aunque no sea el que se encuentre físicamente más cerca del origen.

Programa de control de red(NCP) para proporcionar conexiones cliente-servidor y servicios a nivel de aplicación.

Intercambio secuencial de paquetes (SPX) para servicios de la capa 4 basados en conexiones. IPX y SPX combinados equivalen a TCP/IP.

Novell ha desarrollado un protocolo de enrutamiento por estado de enlace denominado Netware Link Services Protocol (NLSP). NLSP se basa en el protocolo de enrutamiento ISO IS-IS.

Novell dispone también de un servicio de directorios llamado Novell Directory Services (NDS). NDS se utiliza para registrar y localizar servicios de red como alternativa a SAP.

A las capas físicas y de enlace de datos se accede a través de la interfaz abierta de datos (ODI). ODI es una especificación de Novell que proporciona una interfaz estandarizada para las tarjetas de interfaz de red (NIC) que permite, el uso de múltiples protocolos en la misma NIC.

CARACTERISTICAS DE NETWARE:

- Una dirección Novell IPX consta de 80 bits 32 bits para el número de red y 48 bits para el numero de nodo. Se expresa en formato hexadecimal.
- El número de nodo contiene la dirección MAC de una interfaz, o puede ser definida administrativamente para interfaces serie.
- Novell IPX soporta múltiples redes lógicas en una interfaz individual. Cada red requiere un tipo de encapsulado diferente.
- IPX/RIP es el protocolo de enrutamiento predeterminado.
- Los clientes de Netware localizan los servicios de red disponibles, conforme los servidores y routers Novell anuncian o publican, estos servicios mediante difusiones SAP.

DIRECCIONAMIENTO NOVELL IPX

El direccionamiento Novel IPX utiliza una dirección que consta de dos elementos:

El número de red(32)bits y el número de nodo(48) bits.

El número de red IPX puede tener hasta ocho dígitos hexadecimales.

Normalmente sólo se incluyen los números significativos(los 0 a la izquierda no aparecerán).

El administrador de red asigna el número de red IPX a los servidores y routers. Los clientes aprenden las direcciones de red de forma dinámica, a partir del servidor.

El número de nodo IPX posee 12 dígitos hexadecimales. Este número suele ser la dirección MAC obtenida de una interfaz de red con dirección MAC.

Las interfaces serie no poseen direcciones MAC, la misma dirección MAC sería usada por todas las interfaces series del dispositivo.

El uso de la dirección MAC en la dirección lógica IPX elimina la necesidad de un protocolo de resolución de direcciones(ARP). Como la dirección MAC es una parte conocida de la dirección IPX, el puesto podría usar esta información para obtener la dirección de destino en la cabecera de la Capa 2.

NÚMEROS DE RED NOVELL IPX

Los servidores de archivos Novell pueden tener una o varias tarjetas de red(NIC).

Todos los servidores de archivos Novell poseen una red interna virtual(o lógica).

El número de red IPX de esta red interna debe ser único en la interconexión y este siempre será .0000.0000.0001.

Existe un proceso de enrutamiento interno que transmite paquetes entre la red IPX externa. Este número de red interna se usa para anunciar servicios Netware a la red.

El servidor de archivos contiene tanto una tabla de información de routers (RIT) y una tabla de información de servicios (SIT). El contenido completo de ambas tablas se difunde a las redes IPX conectadas directamente coda 60 segundos, por omisión.

Una vez que el proceso IPX ha sido habilitado en el router Cisco, el router escucha las difusiones RIT y SIT de la red y crea también RIT y SIT en el router Cisco. El router pasa entonces a participar de la difusión de esta información cada 60 segundos. Todos los routers que proporcionan conectividad entre dispositivos locales deben compartir el mismo número de red IPX y tipo de encapsulado de dichos dispositivos.

Es posible especificar múltiples encapsulados en una interfaz, pero sólo en el caso de que hayan sido asignadas múltiples números de red, donde cada número de red pertenece a un solo tipo de encapsulado y cada tipo de encapsulado tiene un solo número de red. Aunque puede haber varios tipos de encapsulado en una misma interfaz, los clientes y servidores con tipos de encapsulados diferentes no pueden comunicarse directamente entre ellos. El encapsulado por omisión en los routers Cisco es Novell Ethernet_802.3, definido por la palabra clave de Cisco novell-ether.

ENCAPSULADO DE PAQUETES NOVELL IPX

Netware permite múltiples estructuras de tramas de capa 2 para paquetes Novell IPX.

Hay cuatro tipos de tramas Ethernet.

Ethernet_802.3 Llamado también "raw Ethernet" es el tipo predeterminado para Netware versiones 2.x a 3.11.

DA	SA	LONG	CARGA ÚTIL IPX	FCS

Ethernet_802.2 Predeterminado para Netware versiones 3.12 y posteriores.

DA	SA	LONG	DSAP	SSAP	CTRL	CARGA ÚTIL IPX	FCS

Ethernet_II Es el que se usa con TCP/IP y DECnet.

DA	SA	TIPO	CARGA ÚTIL IPX	FCS

Ethernet_SNAP Se usa con TCP/IP y Apple Talk.

DA	SA	LONG	AA	AA	CTRL	OUI	TYPE	CARGA ÚTIL IPX	FCS

Cuando se configura una red IPX, se necesita especificar un tipo de encapsulado no predeterminado, ya sea en los servidores y clientes Novell o en el router Cisco.

Cisco y Novell asignan nombres diferentes al mismo tipo de encapsulado.

TIPO DE MEDIO	NOMBRE NOVELL IPX	NOMBRE CISCO
Ethernet	Ethernet 802.3	novell-ether
	Ethernet 802.2	sap
	Ethernet_II	ARPA
	Ethernet SNAP	snap
Token Ring	Token Ring_SNAP	snap
	Token Ring	sap
FIDI	FIDI_SNAP	snap
	FIDI_802.2	sap
	FIDI_Raw	novell-fddi

Asegurarse de que los tipos de encapsulado coincidan en todos los clientes, servidores y routers que deban estar en comunicación directa dentro del mismo segmento.

El tipo de encapsulado Ethernet predeterminado en los routers Cisco no coincide con el tipo de encapsulado Ethernet predeterminado en los servidores Novell con versiones 3.12 y posteriores. Para que coincidan los tipos de encapsulado, deberá definir los tipos manualmente usando la opción encapsulatión en el comando ipx network red.

Nota_
El tipo de encapsulado IPX predeterminado para servidores Netware versiones 3.12 y posteriores es Ethernet_802.2. Esto es lo que Cisco denomina encapsulado SAP.

Tenga en cuenta que el encapsulado predeterminado para router Cisco es novell-ether, o lo que Novell llama Ethernet_802.3. Si estos tipos de encapsulado no coinciden, no podrá localizar servicios para los servidores en la interconexión.

PROTOCOLO NETWARE

IPX RIP es un protocolo de enrutamiento basado en vectores distancia y es el protocolo de enrutamiento predeterminado para IPX. Utiliza dos métricas para tomar decisiones de enrutamiento: PULSOS (una medida de tiempo equivalente a 1/8 segundos) y números de saltos(recuento de números de routers por los que se pasa), hasta un máximo de 15.

RIP comprueba sus 2 métricas de vectores distancia comparando en primer lugar los pulsos de trayectos alternativos. Si hay 2 o más trayectos que arrojan el mismo valor de pulsos, RIP procede a comparar el número de saltos.

Cada router IPX difunde periódicamente copias de su tabla de enrutamiento RIP a las redes conectadas directamente al mismo.
El algoritmo de horizonte dividido impide que los vecinos difundan tablas RIP con información IPX de vuelta a las redes de donde han recibido dicha información.

RIP utiliza también un temporizador para controlar las condiciones en las cuales un router, IPX queda inoperativo sin que exista una comunicación explícita a sus vecinos.

Las actualizaciones periódicas reinician los temporizadores. Las actualizaciones de la tabla de enrutamiento se envían por omisión, a intervalos de 60 segundos. El tamaño de paquete predeterminado es de 576 bytes y puede contener hasta 50 entradas.

Todos los servidores de interconexión Netware anuncian sus tipos y direcciones de servicios.

Todas las versiones de Netware soportan difusiones SAP para anunciar y localizar servicios de red registrados. La adicción, localización y supresión de servicios en interconexión tiene lugar dinámicamente mediante anuncios SAP.

Cada servicio SAP es un tipo de objeto identificado por un número hexadecimal.

www.novell.com Lista completa de los SAP existentes.

Todos los servidores y routers guardan una lista completa de los servicios disponibles a través de la red en tablas de información de servicios(SIT).
SAP se sirve de un mecanismo de caducidad temporal como medio para identificar y eliminar las entradas de la tabla que ya no son validas.

Los anuncios de servicios tienen lugar por omisión cada 60 segundos. El tamaño máximo de paquete es de 576 bytes y puede contener hasta siete entradas.

Los routers no retransmiten difusiones SAP. En lugar de ello, cada router construye su propia tabla SAP y retransmite dicha tabla a otros dispositivos de su segmento.
Este cliente Netware difunde una consulta GNS SAP, el router Cisco no responde a la consulta GNS.

CONFIGURACIÓN DEL ENRUTAMINETO IPX

Tareas globales:

Iniciar el proceso de enrutamiento IPX.

Habilitar la compartición de carga, si es apropiado para la red. La compartición de la carga permite que el router utilice múltiples rutas de igual coste para alcanzar un destino. Esto equilibra la transmisión de paquetes a través de múltiples routers y enlaces de red.

Tareas de interfaz:

Asignar números de red únicos a cada interfaz. Es posible asignar múltiples números de red a una interfaz, lo que permite el uso de distintos tipos de encapsulados.

Configurar el tipo de encapsulado opcional, si es diferente del predeterminado.

TAREAS GLOBALES PARA LA CONFIGURACIÓN DEL ENRUTAMIENTO IPX

Ip routing
Habilita el enrutamiento IPX y los servicios SAP. Es posible especificar una dirección de nodo opcional para las interfaces series. Si no especifica dirección de nodo, el router Cisco usará la dirección MAC de una interfaz LAN para las interfaces serie.

Router(config)#ipx routing[nodo]
Si elige configurar el número de nodo manualmente usando una dirección de nodo definida administrativamente en lugar de dejar que el router utilice la dirección MAC predeterminada, no debe utilizar la misma dirección de nodo en dos o más dispositivos de un segmento compartido. Si lo hace así, se produciría un conflicto y se inhabilitaría IPX en estas interfaces.

Ipx maximum-past habilita la compartición de carga.

Router(config)#ipx maximum-past[rutas] Opción predeterminada 1 máximo 512

TAREAS DE INTERFAZ PARA LA CONFIGURACIÓN DEL ENRUTAMIENTO IPX

Ipx network Habilita el enrutamiento IPX en una interfaz particular, le asigna el número de red IPX y opcionalmente, selecciona un tipo de encapsulado.

Router(config)#ipx network[red]encapsulation[tipo de encapsulado]

Red Es el número de red, que es un número hexadecimal de 8 dígitos que identifica de forma unívoca un segmento de cableado de red. El número de red puede ser un valor en el rango de 1 a FFFFFFFD. No es necesario especificar los ceros a la izquierda.

Encapsulation Es la opción que permite especificar el tipo de encapsulado(trama) que usará en la interfaz.

Tipo de encapsulado Especifica alguno de los tipos de encapsulado siguientes:
Arpa, novell-ether, novell-fidi, sap, snap.
IPX es una red lógica. Es posible asignar múltiples redes lógicas a un mismo cable físico.
Para asignar números de red a interfaces que soporten múltiples redes, normalmente se usan subinterfaces.
Una subinterfaz es un mecanismo por el cual una interfaz física puede soportar múltiples subinterfaces o redes lógicas. Es posible asociar varias subinterfaces o redes lógicas a una misma interfaz física.
Cada subinterfaz utiliza un número de red o tipo de encapsulado distinto y el tipo de encapsulado debe coincidir con el de los clientes y servidores que usen ese mismo número de red.

Interfaz tipo número.número de subinterfaz
Crea la subinterfaz lógica en la interfaz física. Los números de subinterfaces pueden ser elegidos arbitrariamente en el rango de 1 a 4294967293.

Ipx network red encapsulation[tipo de encapsulado]
Especifica el número de redIPX y el tipo de encapsulado para cada subinterfaz.

VERIFICACION Y CONTROL DEL ENRUTAMIENTO IPX

Show ipx interface Estado IPX y parámetros en todas las interfaces IPX.

Show ipx route Contenido de la tabla de enrutamiento IPX.

Show ipx servers Contenido de la tabla de servidores IPX.

Show ips traffic Número y tipo de paquetes IPX que están siendo enrutados.

Debug ipx routing activity Muestra información acerca de los paquetes de actualización RIP.

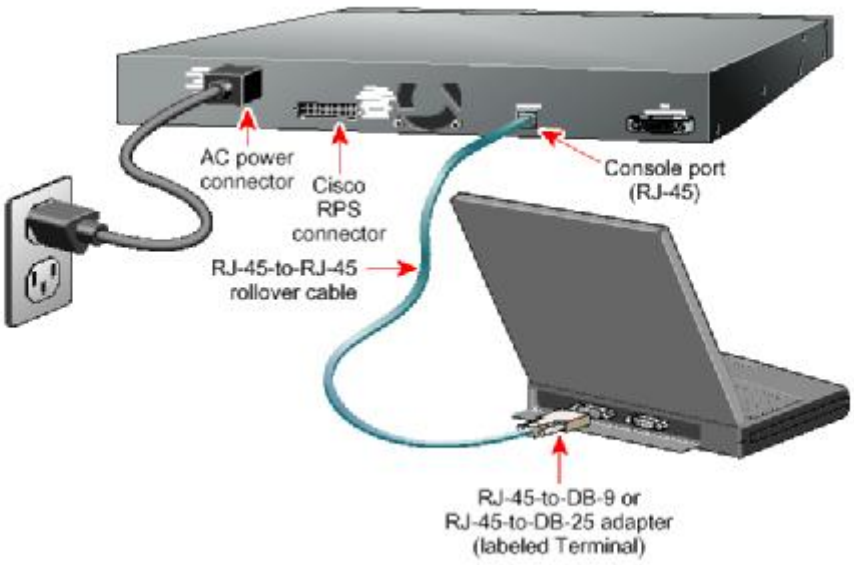
Debug ipx sap activity Muestra información acerca de los paquetes de actualización SAP.

Ping ipx Verifica la accesibilidad al host IPX.

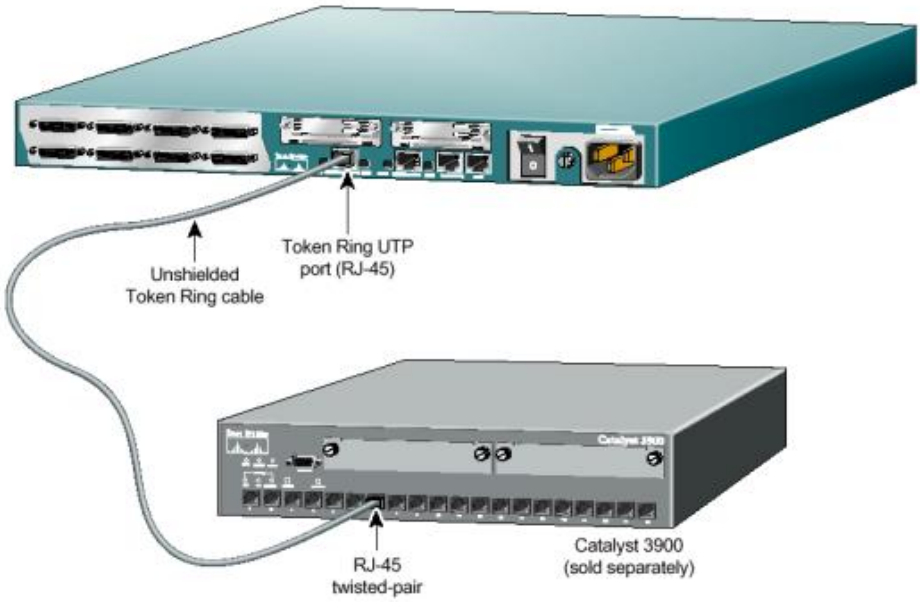
CONEXIÓN AL ROUTER A TRAVÉS DEL PUERTO DE CONSOLA

Todos los enrutadores de Cisco tienen un puerto de consola en la parte posterior. Está ahí para ofrecer una forma de conectar un terminal al enrutador y poder trabajar sobre él. El puerto de consola(a veces conocido con el nombre de puerto de administración). Lo utilizan los administradores para iniciar directamente la sesión en un enrutador, es decir, sin una conexión de red. La consola se debe utilizar para instalar enrutadores en las redes porque, por supuesto, en dicho momento no hay una conexión de red mediante la que trabajar.

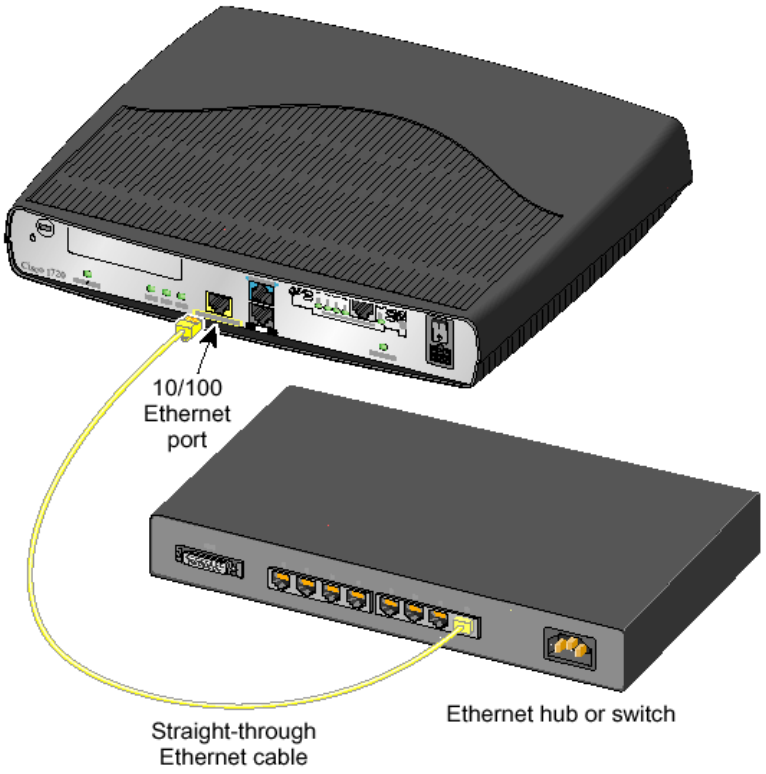
Pero sobre todo, el papel del puerto de consola es estar allí como eventualidad en caso de emergencia. Cuando un enrutador esta completamente caído, en otras palabras, cuando ya no está disponible para procesar paquetes de red, no se puede acceder a él mediante la red. Aquí es donde el puerto de consola ofrece una forma segura de iniciar la sesión en el enrutador para corregir cosas. La desventaja, por supuesto, es que alguien debe estar en la misma ubicación física que el enrutador para conectarse a él.

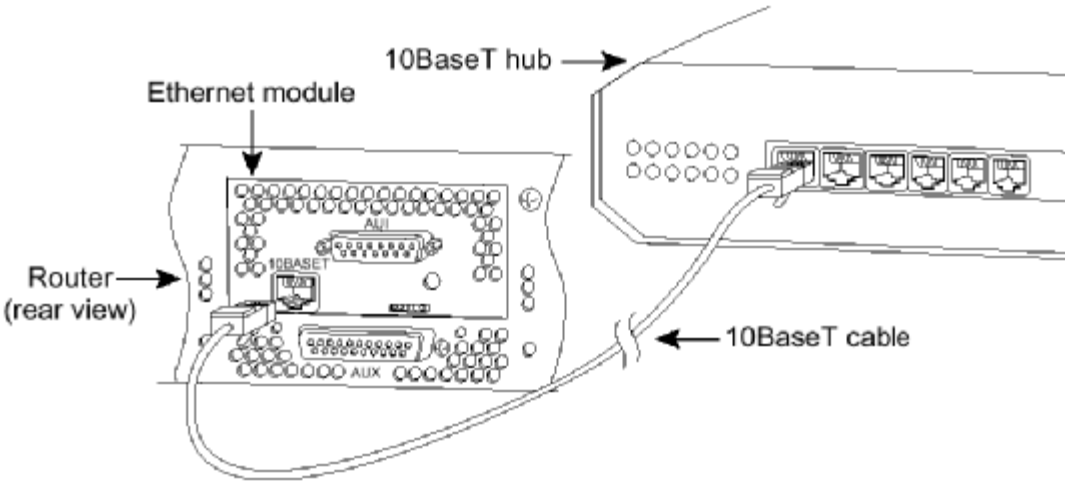


CONEXIÓN DE UN ROUTER A UN SWITCH



CONEXIÓN DE UN ROUTER A UN HUB





Dto:	Operación y red	Proyecto:	CCNA
Autor:	Elva y Chechu	Fecha:	01/04/02
Asunto:	Preparación para certificación CCNA Cisco Systems		
Estado:	Pendiente revisión	Revisión:	1.0

IDENTIFICAR LOS DISTINTOS MODELOS DE ROUTERS CISCO

Este documento ofrece una visión de conjunto sobre la infraestructura de la interconexión de redes desde lo más básico, comenzando con la tecnología subyacente y terminando con el nivel de producto. Si es un principiante lea este documento y conocerá los fundamentos de la interconexión de redes. Como las tecnologías se tratan de forma genérica, comprenderá las tecnologías y los componentes necesarios para hacer que cualquier red funciones.

Infraestructura de red, dispositivos sobre los que funciona una red.

- **Enrutadores.** Estos dispositivos enrutan datos entre local area network(LAN; redes de área local). Los enrutadores ponen el Inter. En interconexión de redes; sin ellos, Internet no sería posible. Los enrutadores usan direcciones de Internet Protocol(IP, Protocolo de Internet) con el fin de calcular la mejor ruta para los paquetes a través de las redes.

- **Conmutadores**. Estos dispositivos también envían datos entre distintas LAN. Los conmutadores son más rápidos que los enrutadores, pero no usan direcciones IP y, por tanto, no tienen la capacidad de los enrutadores para encontrar trayectorias a través de grandes redes.

- **Cortafuegos**. Éstos son básicamente enrutadores especialmente preparados para filtrar paquetes con el fin de asegurar el procesamiento de datos dentro de la red interna de una empresa. Son enrutadores especializados que actúan como controles entre un red, y el exterior. Funcionan comprobando cada paquete para que cumpla con la política de seguridad que ha sido programada, con el fin de hacerla respetar. Un cortafuegos forma un cuello de botella intencionado del tráfico y monitoriza constantemente las conexiones internas7externas para verificar que se cumple la seguridad. Los cortafuegos más potentes tienen hardware especializado, pero no tienen por qué tenerlo. Un enrutador normal puede programarse para realizar muchas tareas de un cortafuegos, aunque es preferible un dispositivo cortafuegos dedicado en la mayoría de los casos.

- **Servidores de acceso.** Estos dispositivos dedicados contestan a las llamadas telefónicas de usuarios remotos y los conectan a la red. La mayoría de los servidores de acceso se usan como Internet Service Providers(ISP, Proveedores de servicio de Internet) para conectar a usuarios particulares y pequeñas empresas a Internet. Un servidor de acceso es un dispositivo especializado que, dicho bruscamente, actúa como un módem por un lado y como un concentrador por el otro. Los servidores de acceso conectan usuarios remotos a las redes. La mayoría de los millones de puertos de servidores de acceso en el mundo los administran los ISP para atender las llamadas telefónicas de abonados a Internet. Algunos realizan funciones más especializadas, pero el objetivo principal del servidor de acceso es conectar usuarios de acceso telefónico remoto a una red .

- **Concentradores**. El lento concentrador acepta cables de PC y servidores para crear LAN independientes llamadas segmentos LAN, los bloques básicos para construir una red. Un concentrador es un dispositivo pasivo que actúa como punto de conexión central mediante la inspección de cables procedentes de equipos independientes, principalmente PC, servidores e impresoras, para formar un segmento LAN independiente. Los equipos conectados al propio concentrador son miembros de dicho segmento LAN, y comparten el ancho de banda del concentrador para sus comunicaciones. Esto se debe a que un concentrador simplemente repite las señales de entrada a todos los dispositivos conectados a sus puertos.

El conjunto, de estos cinco tipos de dispositivos forman la infraestructura de Internet. El único otro ingrediente principal son los enlaces de telecomunicaciones.

IOS Abreviatura de Internet Operating System (Sistema operativo de redes). Éste es el sistema propietario de Cisco para su línea de hardware de interconexión de redes.

La línea de productos de Cisco se alinea de acuerdo a la escala de clientes. En otras palabras, agrupan y ponen el precio a cada modelo del producto de acuerdo al tamaño y la sofisticación del mercado del cliente.

ENRUTADORES SOHO

Son los enrutadores de gama baja. Permite a las pequeñas organizaciones conectarse a los PSI enrutador a enrutador, en vez de cómo usuarios de acceso telefónico ahorra dinero en conexiones telefónicas, el rendimiento es mayor y se mejora la fiabilidad. El termino series significa aquí un chasis que se configura de forma diferente en la planta de fabricación para diferentes modelos del producto, normalmente dependiendo del circuito impreso que se instale en ellos.

Tres series de enrutadores SOHO

Serie de productos	Descripción
Cisco 90	Enrutador de Acceso DSL para conectar un usuario. No tiene un IOS que se pueda configurar el usuario.
Serie Cisco 700	Enrutadores de acceso RDSI para conectar hasta 30 usuarios. No tiene un IOS que se pueda configurar el usuario.
Serie Cisco 800	Enrutadores de acceso RDSI para conectar hasta 20 usuarios. Incluye el IOS y tiene capacidad de cifrado VPN.

Los productos SOHO enfatizan las tecnologías de acceso telefónico(DSL y RDSI).

ENRUTADORES CISCO DE GAMA MEDIA

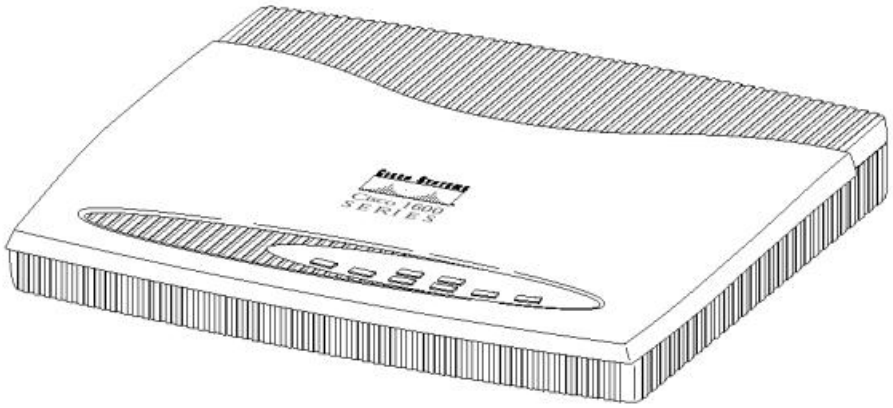
Cisco tiene varios niveles de productos de enrutadores de acceso Dependiendo de la serie de productos puede configurarse varias combinaciones de tecnologías LAN y medios WAN. Modular significa que se puede actualizar el chasis insertando uno o más módulos. Los dispositivos no modulares tienen una configuración fija.

Serie de productos	Descripción
Serie Cisco 1000	Enrutadores de acceso Ethernet para conectar a una RDSI o a un vinculo serie WAN.
Enrutador Cisco 1401	Enrutador de acceso Ethernet para conectar a un ATM o una red troncal DSL.
Serie Cisco 1600	Enrutador de acceso Ethernet para conectar a una RDSI o a un enlace WAN. Incluye la capacidad de cifrado VPN.
Serie Cisco 2500	Enrutador/concentrador Ethernet o Token Ring o modelos de servidor de acceso telefónico para conectar uno o más segmentos LAN a una RDSI o a un enlace serie.
Serie Cisco 2600	Solución modular y de bajo coste para que funcione como enrutador, pasarela de voz/datos o servidor de acceso telefónico. Conecta una o dos LAN Ethernet o Token Ring a vínculos RDSI, T! canalizado, Ethernet, módem analógicos o ATM. También soporta voz/fax y Frame Relay.
Serie Cisco 3600	Enrutador modular de alta densidad para acceso telefónico o para tráfico enrutador a enrutador. Soporta vínculos RDSI, líneas serie, T1 canalizado, módem digitales y ATM. También soporta voz/fax y Frame Relay.

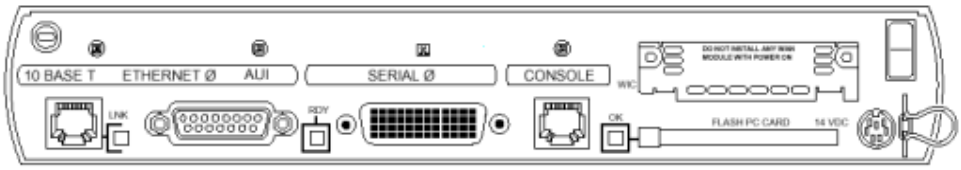
SERIES 4000 Y 7000 DE ENRUTADORES DE RED TRONCAL

Serie de productos	Descripción
Serie Cisco 4000	enrutadores de tres ranuras que soportan Ethernet, Fast Ethernet, Token Ring, FDI, HSSI, Líneas serie, RDSI, T1 canalizada y ATM.
Serie Cisco 7000	Enrutadores centrales de 4 a 13 ranuras que soportan Ethernet, Fast Ethernet, Token Ring, FDI, HSSI, líneas serie, RDSI, T1 canalizada, paquetes sobre DS3 y ATM.
Serie Cisco 12000	Enrutador conmutador de 8 a 12 ranuras Gigabit Ethernet optimizado para IP. Dispone de tarjetas especiales para vínculos WAN OC-12 y OC-48.

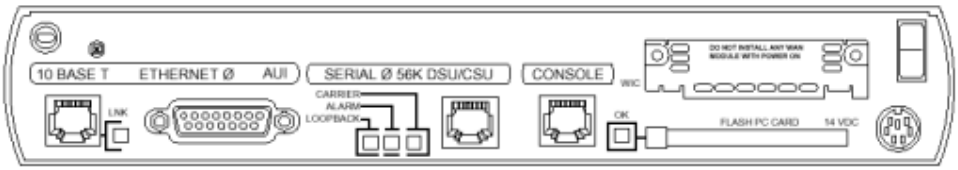
ROUTER 1600 FRONTAL



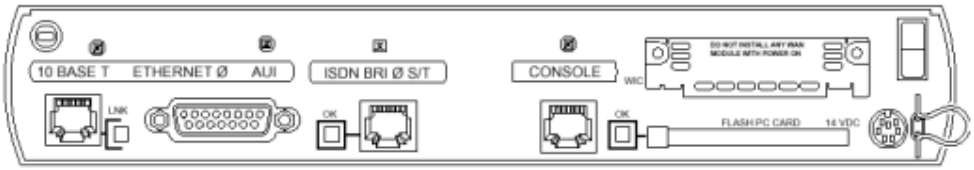
ROUTER CISCO 1601



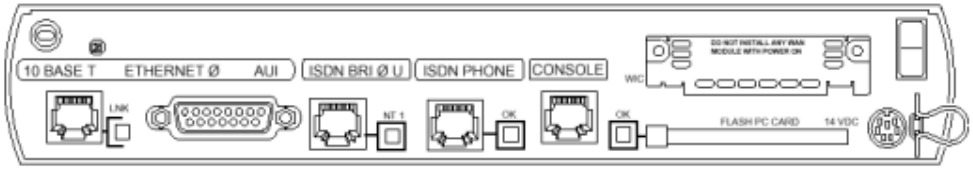
ROUTER CISCO 1602



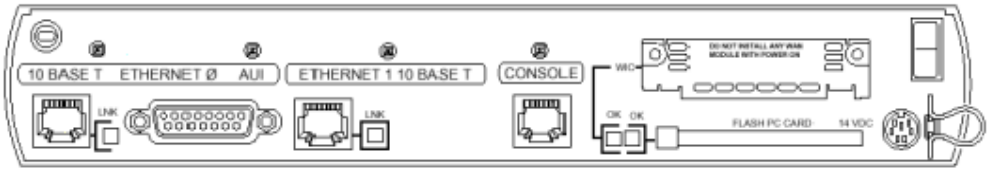
ROUTER CISCO 1603



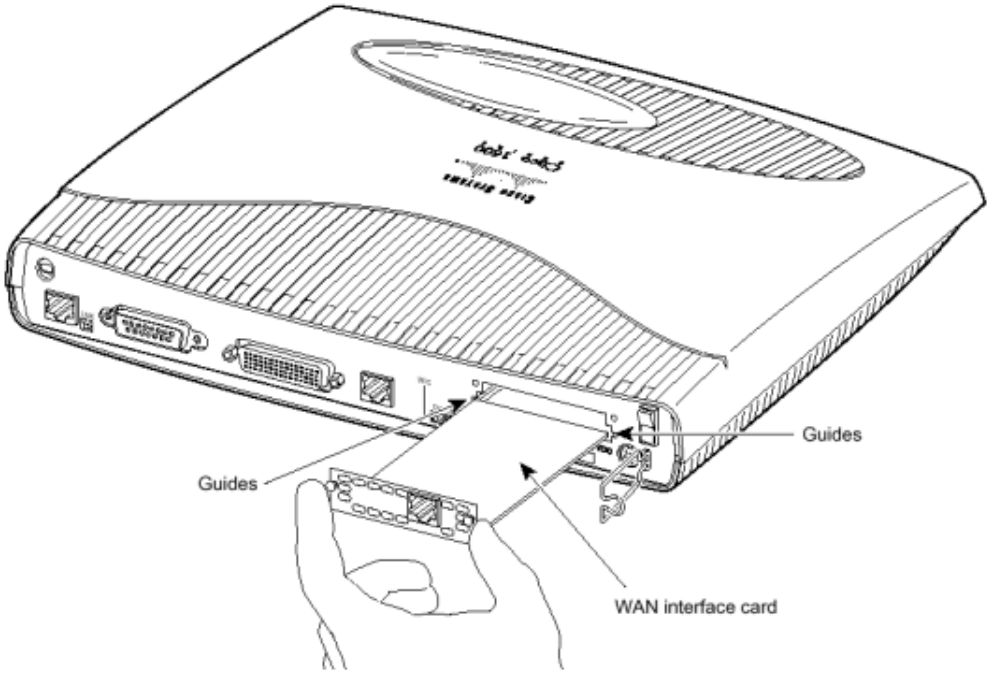
ROUTER CISCO 1604



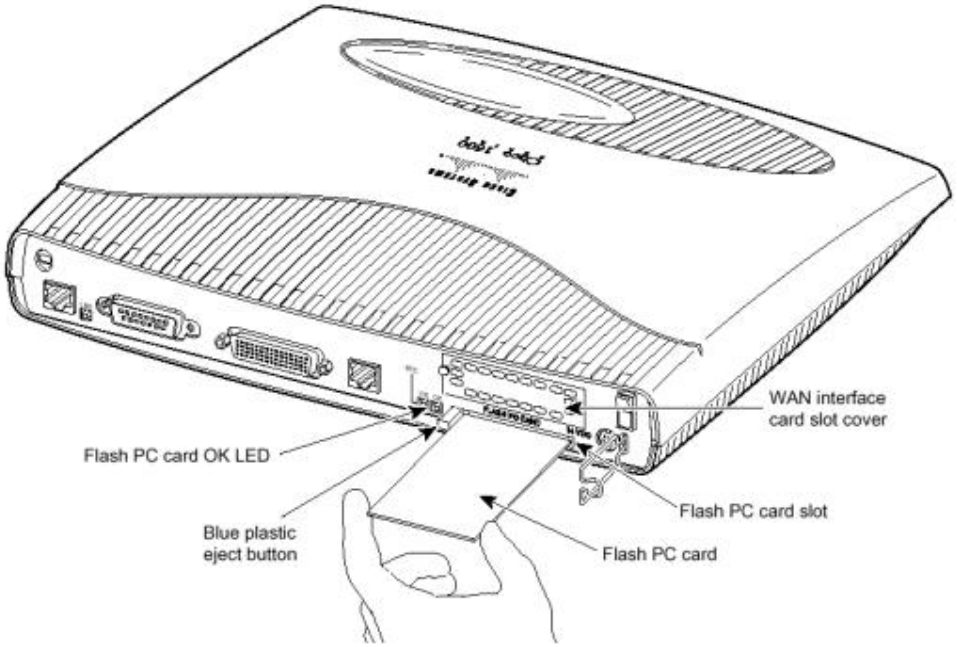
ROUTER CISCO 1605



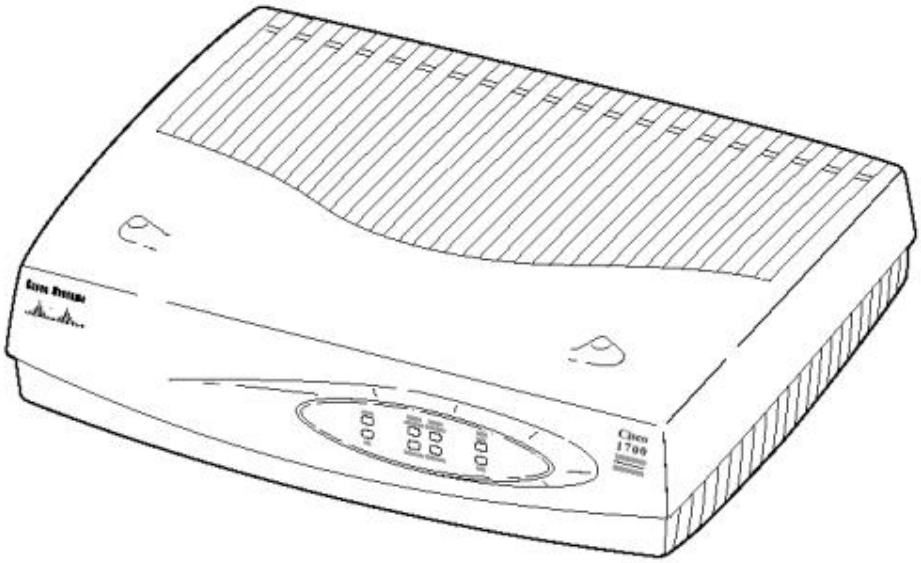
INSTALANDO LA TARJETA INTERFAZ WAN EN UN ROUTER 16001

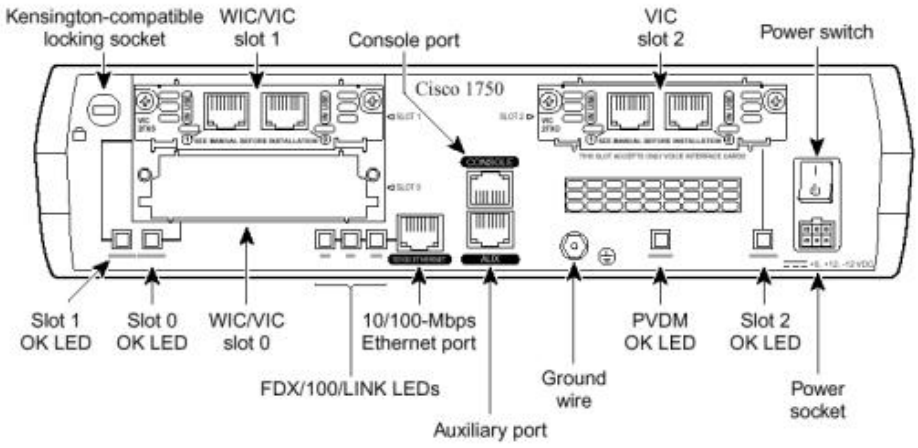


INSTALANDO LA TARJETA FLASH EN UN ROUTER CISCO 1601



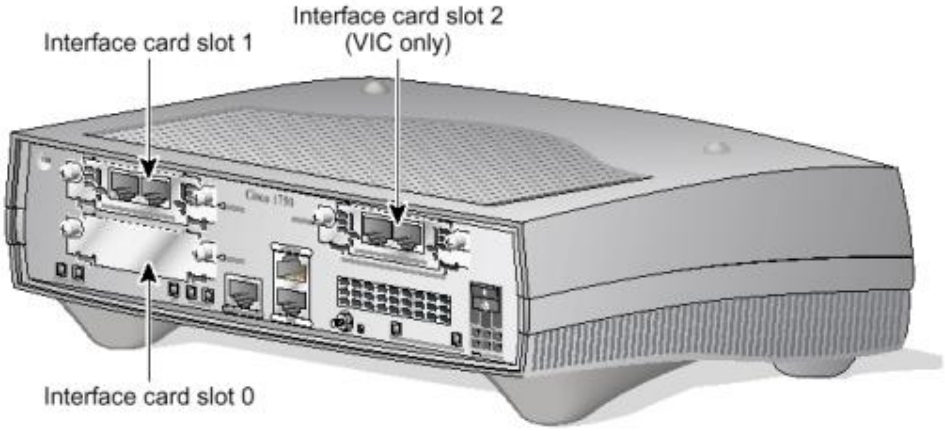
ROUTER CISCO 1700 FRONTAL



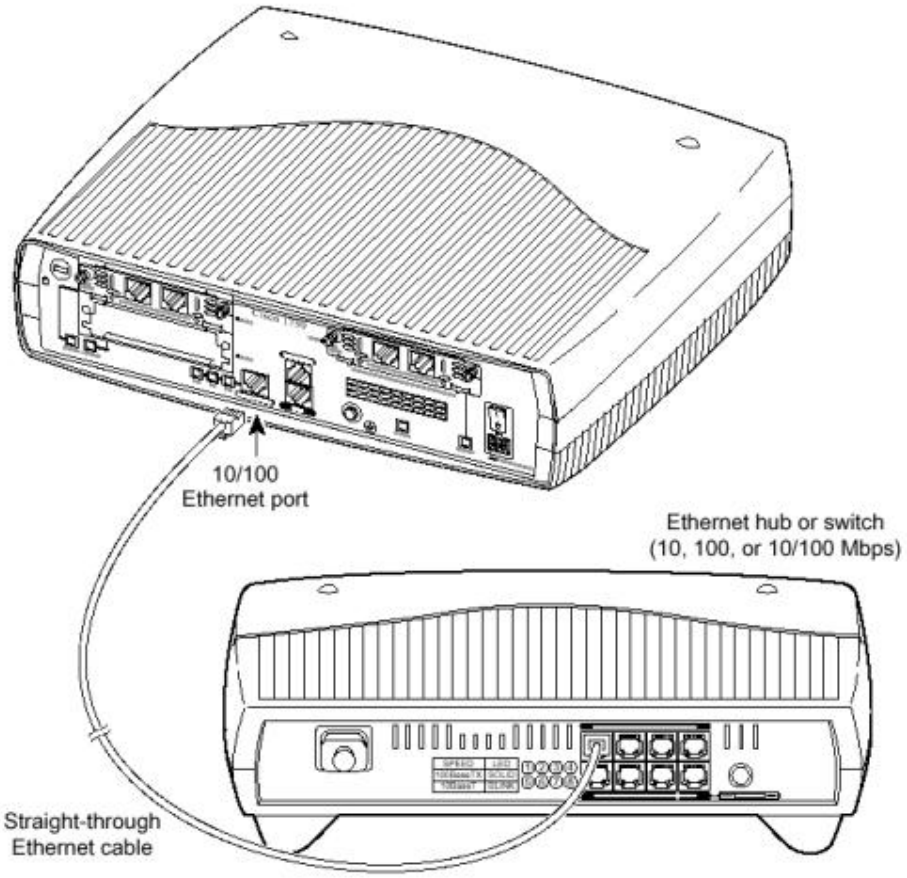


ROUTER CISCO 1720

ROUTER CISCO 1750



CONEXIÓN DE UN ROUTER 1700 A UN HUB O SWITCH



MODULOS Y PUERTOS DEL ENRUTADOR

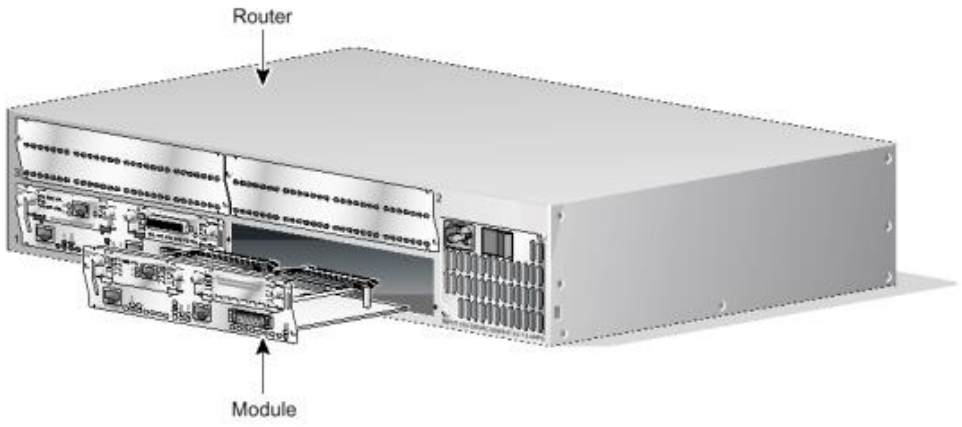
Una de las ventanas del enrutador hacia la red es a través de sus puertos y módulos. Sin ellos, un enrutador es una caja inútil. Los puertos y los módulos que se colocan en un enrutador definen lo que éste puede hacer.

La interconexión de redes puede ser algo difícil, con una combinación de productos, protocolos, medios, conjuntos de características, estándares, etc., aparentemente sin fin. Los acrónimos aparecen de forma tan rápida y son tan difíciles de recordar que puede ser desesperante aprender cómo configurar correctamente un enrutador. Pero si se elige el producto correcto de enrutador, se reducirá este problema a proporciones manejables.
Es evidente que Cisco no puede fabricar un modelo de enrutador que encaje en los requisitos específicos de cada cliente. Para hacerlos más flexibles de configurar, los enrutadores se dividen en dos partes principales.

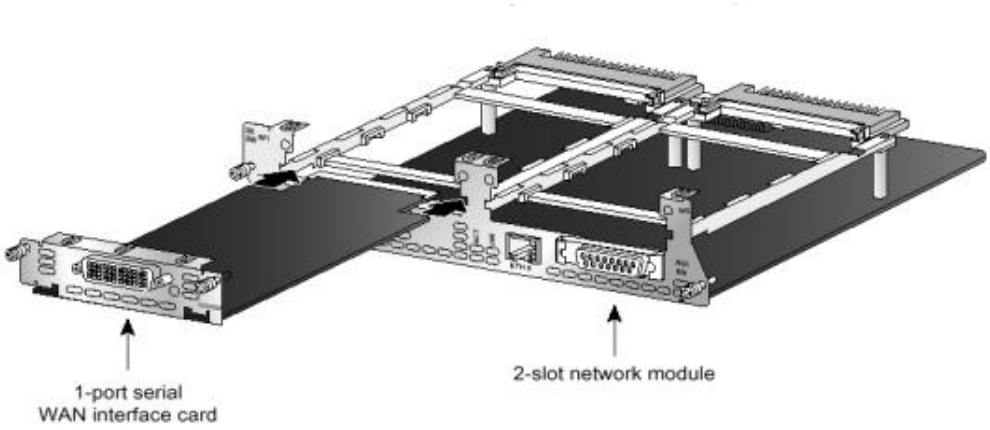
- **El chasis.** La caja donde se coloca y los componentes básicos dentro de la misma, como la fuente de corriente, los ventiladores, los paneles anterior y posterior, luces indicadoras y las ranuras.

- **Puertos y módulos.** Las placas de circuito impreso que se introducen en la caja del enrutador.

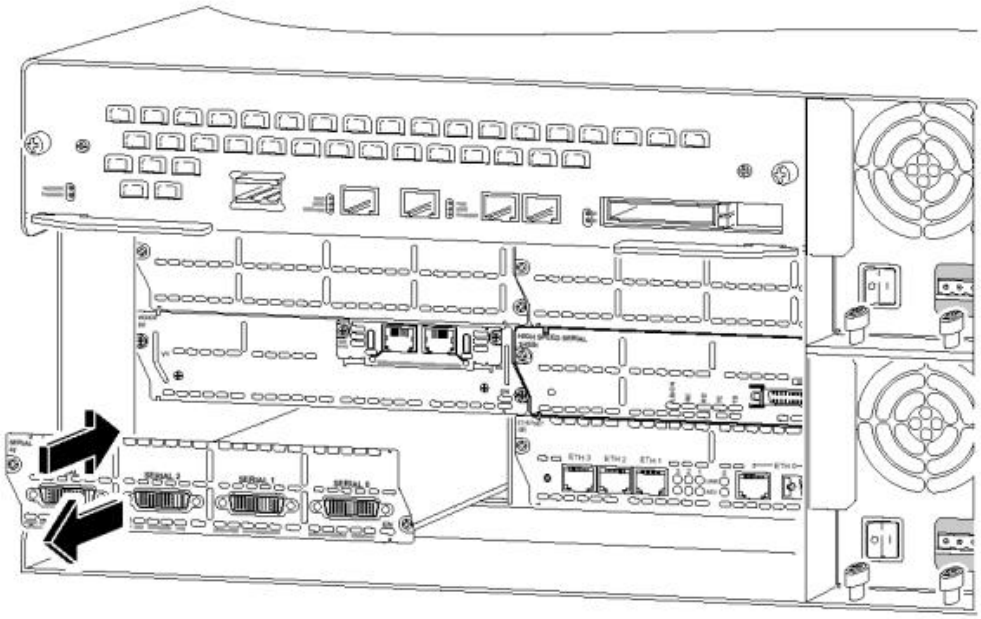
INSTALANDO UN MODULO DE RED EN UN ROUTER MODULAR



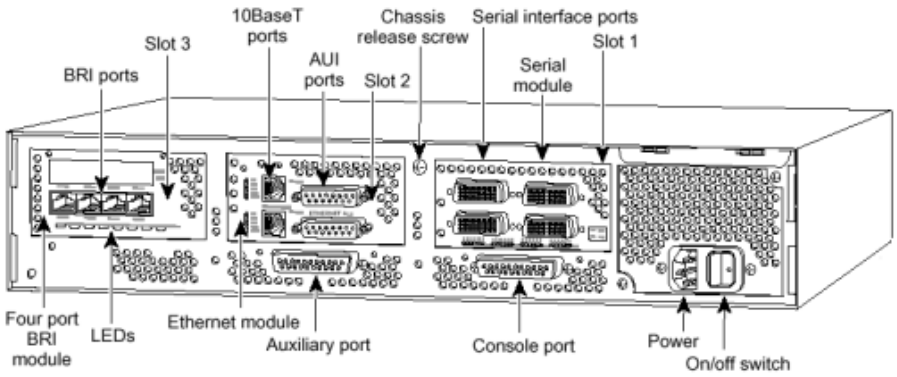
INSTALANDO UNA TARJETA INTERFAZ WAN SERIE EN UN SLOT DOBLE DE UN MODULO DE RED.



EXTRACCIÓN EN CALIENTE DE UN MODULO DE RED.

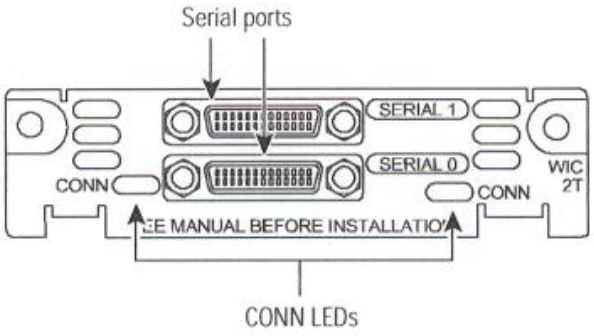


VISTA REAL DE NÚMERO DE SLOT Y PUERTOS DE INTERFAZ.

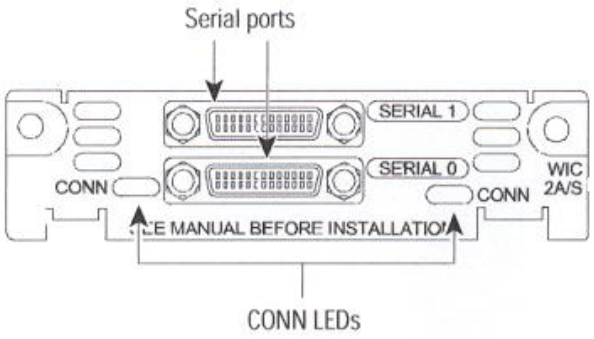


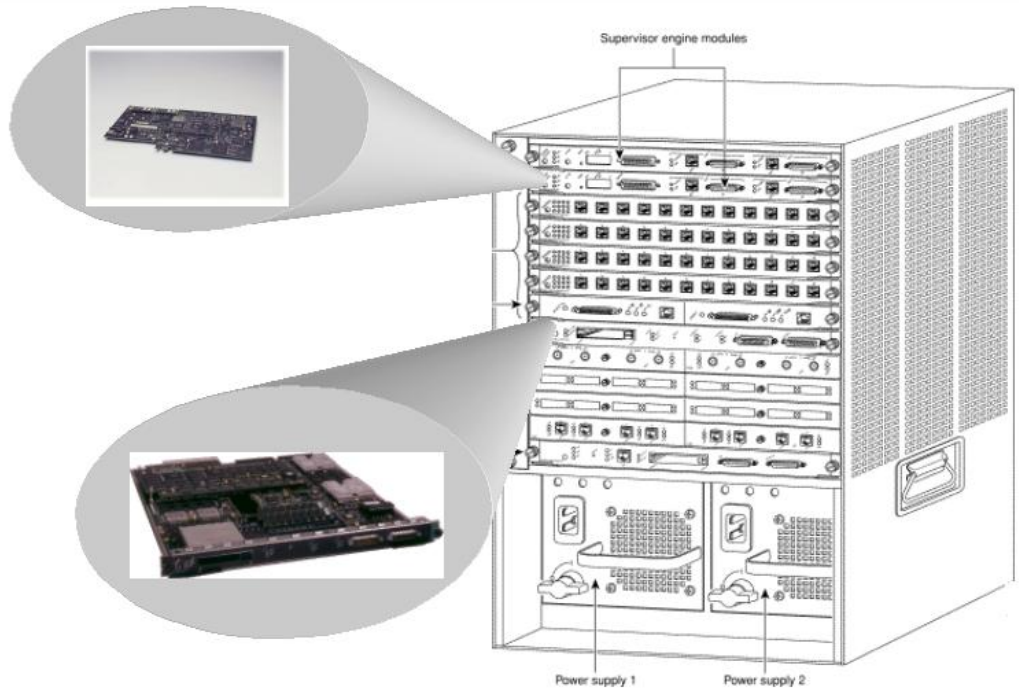
TARJETAS WIC

WIC serie de alta velocidad y dos puertos (hasta 4 Mbps por puerto)



WIC serie de alta velocidad y dos puertos asinc/sinc (hasta 128 Kbps por puerto)





ROUTER DE ACCESO MODULAR DE LA SERIE CISCO 2600

Con la familia de routers de acceso modular de la serie Cisco 2600, Cisco Systems extiende la versatilidad, integración y potencia de clase empresarial a las oficinas sucursales.
La serie Cisco 2600 comparte las interfaces modulares con las series Cisco 1600 y 3600, ofreciendo una solución rentable para satisfacer las necesidades actuales de las oficinas remotas en aplicaciones tales como:

- Acceso seguro a Internet/intranet con firewall opcional
- Integración multiservicio de voz y datos
- Servicios de acceso analógico y digital por acceso telefónico
- Acceso a redes privadas virtuales (VPN)
- LAN virtuales (VLAN)

La arquitectura modular de la serie Cisco 2600 permite actualizar las interfaces para ajustarlas a la expansión de la red o a los cambios tecnológicos que se producen cuando se instalan nuevos servicios y aplicaciones. Mediante la integración de las funciones de los distintos dispositivos independientes en una sola unidad compacta, la serie Cisco 2600 reduce la complejidad de gestionar la solución para redes remotas. Equipado con un potente procesador RISC, la serie Cisco 2600 ofrece la potencia adicional necesaria para el soporte de avanzadas funciones de calidad de servicio (QoS) y de seguridad indispensables en las oficinas remotas de hoy en día.

La serie Cisco 2600 está disponible en seis configuraciones base:

- Cisco 2610: un puerto Ethernet
- Cisco 2611: dos puertos Ethernet
- Cisco 2612—Un puerto Ethernet, un puerto Token Ring
- Cisco 2613: un puerto Token Ring
- Cisco 2620: un puerto Ethernet 10/100 Mbps conautodetección
- Cisco 2621: dos puertos Ethernet con detección automática de 10/100 Mbps

Todos los modelos también tienen dos ranuras para tarjetas de interfaz WAN (WIC), una ranura para el módulo de red y una ranura para un módulo de integración avanzada (AIM).

Las tarjetas de interfaz WAN disponibles para los routers Cisco 1600, 1720, 2600 y 3600 ofrecen soporte para una amplia gama de opciones serie, ISDN (RDSI) de acceso básico y de unidad de servicio de canal/unidad de servicio de datos (integrated channel service unit/data service unit, CSU/DSU) para conectividad WAN principal y de respaldo.

Los módulos de red disponibles para las series Cisco 2600 y 3600 admiten una amplia gama de aplicaciones, incluyendo la integración multiservicio voz/datos, acceso por acceso telefónico analógico e ISDN (RDSI), y concentración de dispositivos serie. El módulo de integración avanzada para compresión de datos interno de la serie Cisco 2600 descarga del sistema la tarea de realizar compresión de datos a alta velocidad. Desde la CPU principal del 2600, que permite una transferencia de datos comprimidos de un máximo de 8 Mbps a la vez que preserva las ranuras externas de la interfaz para otras aplicaciones.

VENTAJAS PRINCIPALES

La serie Cisco 2600 ofrece soporte para potenciar las soluciones de extremo a extremo de las soluciones de red Cisco con las siguientes ventajas:

- **Protección de la inversión**: Ya que la serie Cisco 2600 admite componentes modulares actualizables en la instalación, los clientes pueden cambiar con facilidad las interfaces de red sin tener que realizar una "actualización integral" de la solución implementada en la red de la oficina remota. Otra forma en que la ranura AIM de la plataforma Cisco 2600 protege la inversión económica es ofreciendo la capacidad de expansión necesaria para dar soporte a servicios avanzados, tales como compresión y cifrado de datos asistida por hardware, aunque esta última función estará disponible próximamente.

- **Bajo coste de propiedad:** Mediante la integración de las funciones de las CSU/DSU, dispositivos de terminación de red ISDN (RDSI) (NTI), módems firewalls, dispositivos de compresión o cifrado y demás equipamiento de los recintos de cableado de las sucursales en una sola unidad, la serie Cisco 2600 ofrece una solución que ahorra espacio y que puede gestionarse remotamente usando aplicaciones de gestión de red tales como CiscoWorks y CiscoView

- **Integración multiservicio de voz y datos:** la serie Cisco 2600 refuerza el compromiso de Cisco para incorporar capacidades de integración multiservicio de voz y datos a su cartera de productos, lo que permite a los administradores de red ahorrar costes de llamadas entre oficinas que se encuentran a mucha distancia y habilitar futuras aplicaciones de activación por voz tales como la mensajería integrada y los centros de llamadas basados en Web. Utilizando los módulos de voz/fax, el router Cisco 2600 puede instalarse en redes de Voz sobre IP (VoIP) y Voz sobre Frame Relay (VoFR).

- **Componente de una solución extremo a extremo de Cisco:** Como componente de una completa solución de red de Cisco, la serie Cisco 2600 permite que las empresas extiendan una infraestructura de red rentable y transparente hasta las sucursales.

OPCIONES DE HARDWARE/SOFTWARE

Los routers de la serie Cisco 2600 ofrecen una amplia selección de interfaces Ethernet, Token Ring y LAN Ethernet 10/100 con detección automática. Además, todos los modelos incluyen dos ranuras para tarjetas de interfaz WAN (WIC), una ranura para el módulo de red y una ranura para una ranura para un módulo de integración avanzada (AIM).

OPCIONES DE TARJETA DE INTERFAZ WAN

La serie Cisco 2600 admite todas las tarjetas de interfaz WAN disponibles para las series Cisco 1600, 1700 y 3600, así como dos nuevas tarjetas de interfaz WAN de doble puerto serie para aprovechar al máximo la densidad de las interfaces y la eficiencia de las ranuras. Las nuevas tarjetas de interfaz WAN de doble puerto serie cuentan con el nuevo conector Smart Serial, compacto y de alta densidad, para la conexión de una amplia gama de interfaces eléctricas cuando se usan con el cable de transición adecuado.

SOFTWARE CISCO IOS

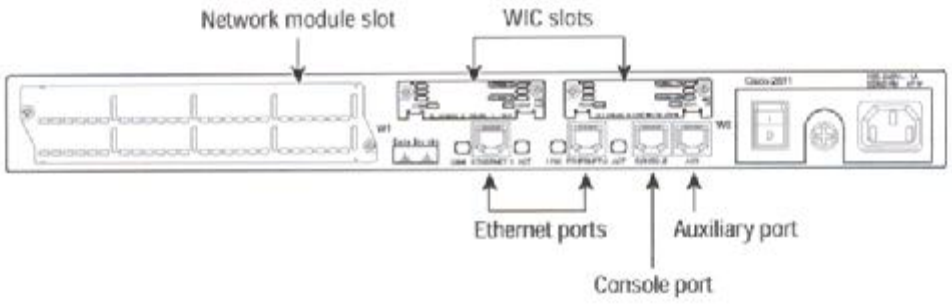
Al ser compatible con toda la gama de conjuntos de características de software Cisco IOS disponibles, la serie Cisco 2600 puede operar la gama de servicios de red más amplia del mercado. Los conjuntos de características base admiten los protocolos y estándares más utilizados, tales como NAT, OSPF, Border Gateway Protocol (BGP), Remote Access Dial-In User Service (RADIUS), IP Multicast, RMON y las características de optimización de WAN (como Bandwidth on Demand; Custom, Priority and Weighted Fair Queuing, Dial Back-up y RSVP). Los conjuntos de características "Plus" contienen un número adicional de características de valor añadido, como por ejemplo los protocolos de mainframe de legado, DLSw, L2TP, L2F, integración de voz/datos, modo de transferencia asíncrona (ATM), VLAN, Netflow, etc. Otros conjuntos de características incluyen cifrado IPSec y 3DES, así como capacidades de firewall certificadas ICSA. La serie Cisco 2600 es compatible con la versión de Cisco IOS 11.3(2) y superiores. Es posible encontrar una lista detallada del contenido de los conjuntos de características de Cisco IOS en la notas de la versión IOS del Cisco 2600 y en el boletín de productos de características de software y requisitos de memoria del Cisco 2600.

ESPECIFICACIONES TÉCNICAS

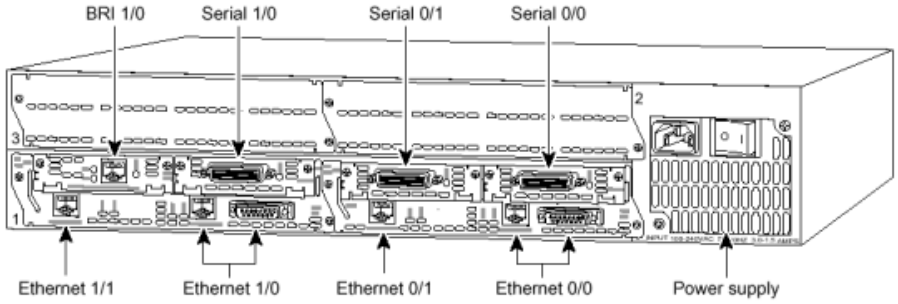
- Procesador: Motorola MPC860 40 MHz (Cisco 261X), Motorola MPC860 50 MHz (Cisco 262x)
- Memoria Flash: 4 a 16 Mb (32 Mb máx. en Cisco 262x)
- Memoria de sistema (DRAM): de 24 a 64 MB
- Ranuras para tarjetas de interfaz WAN: 2
- Ranuras para módulos de red: 1
- Ranura AIM: 1
- Consola/velocidad auxiliar: 115,2 Kbps (máxima)
- Anchura: 17,5 pulgadas (44,5 cm.)
- Altura: 1,69 pulgadas (4,3 cm.)
- Profundidad: 11,8 pulgadas (30 cm.)
- Peso (mín.): 8,85 lb. (4,02 kg.)
- Peso (máx.): 10,25 lb. (4,66 kg.)
- Disipación de potencia: 72 W (máximo)
- Voltaje de corriente alterna (CA) de entrada: de 100 240 VCA
- Frecuencia: de 47 64 Hz
- Tensión de entrada CA: 1,5 amperios
- Voltaje de corriente continua (CC) de entrada: -38V a-75 V
- Tensión CC de entrada 2 amperios
- Temperatura de funcionamiento: de 32 a 104 F (de 0 a 40 C)
- Temperatura de no funcionamiento: de -13 a 158 F (de -25 a 70 C)
- Humedad relativa: de 5 a 95% sin condensación
- Nivel de ruido (mín.): 38 dbA
- Nivel de ruido (máx.): 42 dbA

ROUTER CISCO 2611

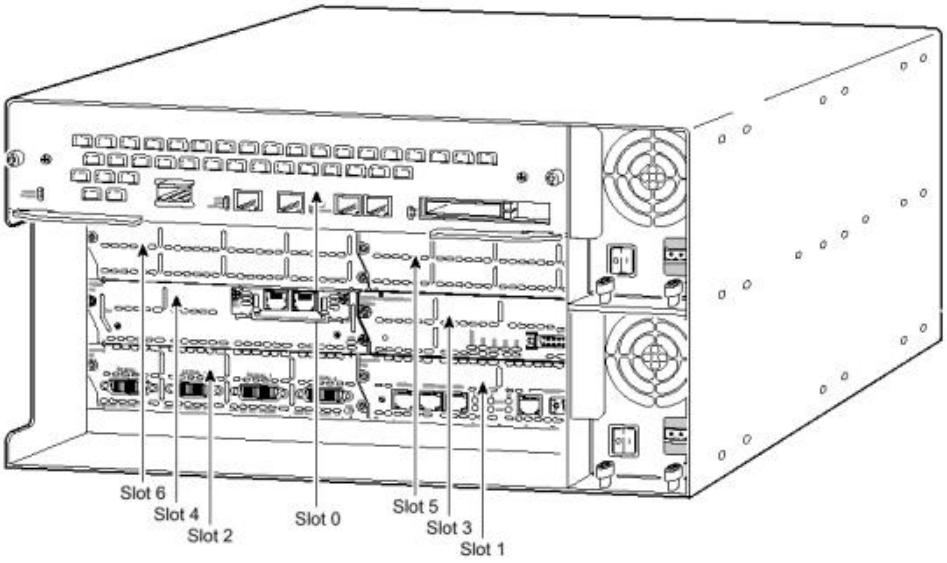
Vista del panel posterior de la serie Cisco 2600 (se muestra el Cisco 2611)



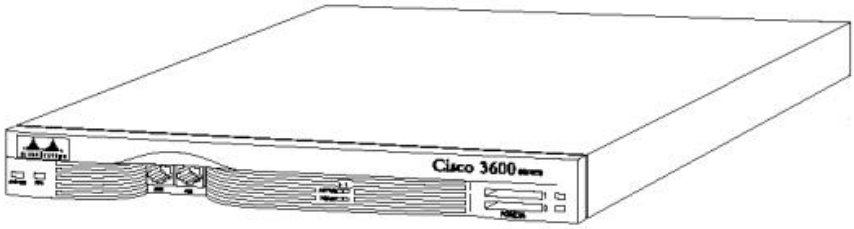
ROUTER CISCO 3600

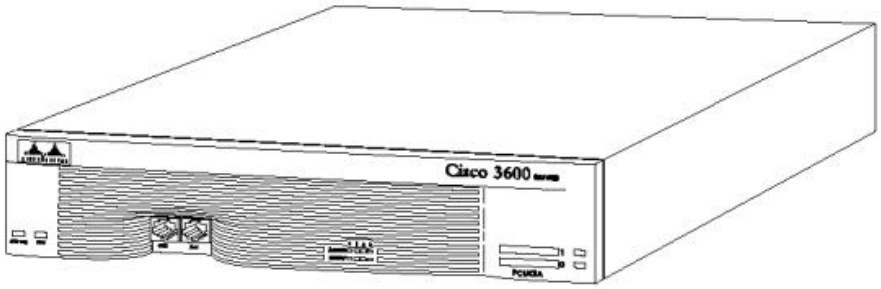


ROUTER CISCO 3600



FRONTAL DE ROUTER CISCO 3620 Y 3640





Bto:	Operación y red	Proyecto:	CCNA
Autor:	Elva y Chechu	Fecha:	01/04/02
Asunto:	Preparación para certificación CCNA Cisco Systems		
Estado:	Pendiente revisión	Revisión:	1.0

ROUTER CISCO SERIE 700

Este Apartado contiene una visión general de los routers Cisco de la serie 700 para small office/home ofice(SOHO)y una breve visión de las tareas básicas de configuración inicial. La serie 700 de routers RDSI(Red digital de servicios integrados) de Cisco para small office/home office proporcionan una solución de bajo coste para equipar oficinas remotas con conectividad RDSI.

GENERALIDADES Y CONFIGURACIÓN DE LOS ROUTERS CISCO SERIE 700

Todos los productos de la familia de la serie 700 de Cisco ofrecen máxima flexibilidad para el acceso remoto. La familia de productos ahora incluye los Cisco 761M, 762M, 765M, 766M, 771M, 772M, 775M y 776M. Estos productos ofrecen opcionalmente dos interfaces telefónicas analógicas para permitir a dispositivos como por ejemplo, teléfonos estándar, faxes y módems, compartir una línea BRI(Interfaz de acceso básico) de RDSI, eliminando la necesidad de múltiples líneas de teléfono o caros teléfonos RDSI. Cuatro delos modelos de Cisco 700(los modelos 765M, 766M, 775M y 776M) ofrecen soporte para dos líneas telefónicas básicas, así como soporte para servicios telefónicos suplementarios sobre RDSI. Estos servicios telefónicos incluyen llamada en espera, cancelación de llamada en espera, mantenimiento de llamada, recuperación de llamada, conferencia a tres y desvío de llamada. La figura C.1 ilustra cómo los routers serie 700 pueden proporcionar servicios de red para SOHO.

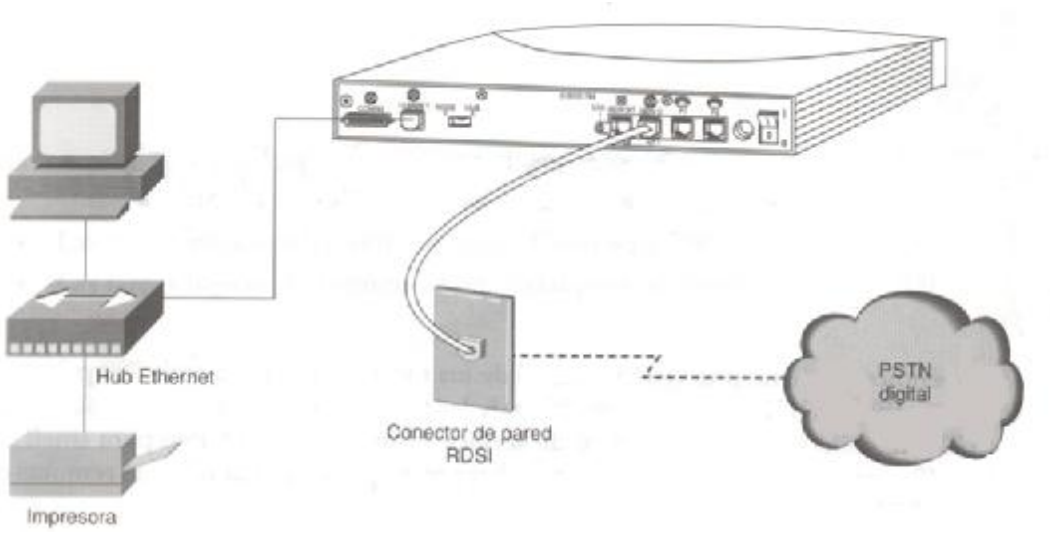


Figura C.1 Router Cisco serie 700

Los routers Cisco serie 700 soportan todos enrutamiento IP e IPX, puenteado transparente, Protocolo simple de administración de redes(SNMP) y autenticación multinivel.
Todos los routers Cisco serie 700 soportan el Protocolo de punto a punto multienlace (MP), proporcionando un ancho de banda de hasta 128 Kbps(precomprimidos).

Todos los modelos de esta familia también incorporan el software ClickStart, que permite a los usuarios configurar routers Cisco serie 700 utilizando un navegador World Wide Web estándar, como Netscape Navigator. ClickStart es una interfaz de configuración gráfica de fácil manejo que divide el proceso de instalación en varios pasos simples, pidiendo al usuario la información necesaria, permitiéndole así configurar un nuevo router en unos pocos minutos.

PERFILES DE UN ROUTER CISCO SERIE 700

Un **perfil** es un conjunto de configuraciones asociado con un dispositivo remoto especifico. Después de ser definidos por el usuario, los perfiles son grabados y almacenados en la memoria de acceso aleatorio no volátil(NVRAM) (la memoria utilizada para almacenar la configuración del router).

En lugar de utilizar un conjunto de configuraciones para operar con todos los dispositivos remotos, puede personalizar su router Cisco serie 700 para utilizar conjuntos individuales de configuración, o perfiles personalizados para cada dispositivo remoto.

Los routers Cisco serie 700 están configurados con tres perfiles permanentes. Estos tres perfiles pueden ser modificados pero no borrados:

- **LAN**. Determina cómo son transferidos los datos desde el router a la LAN. Se utiliza para enrutamiento y con las conexiones Ethernet.
- **Interno**. Determina cómo se pasan los datos entre el motor del bridge y el motor de router IP/IPX. Se utiliza cuando el enrutamiento está habilitado.
- **Estándar**. Utilizado para conexiones RDSI entrantes que no tienen un perfil. El perfil estándar no soporta enrutamiento. Este perfil debería utilizarse para proporcionar la configuración adecuada y medidas de seguridad para llamadas desconocidas.

Al encender el router, se cargan los perfiles. En la figura C.2 pueden verse los perfiles del router.

Los perfiles de usuario permiten a los usuarios crear conjuntos personalizados de parámetros de configuración, como filtros, umbrales de demanda y contraseñas para cada sitio remoto al que se llama. Los perfiles permiten realizar llamadas bajo demanda a diferentes números de teléfono basándose en filtros de demanda que son adaptados a cada sitio remoto.

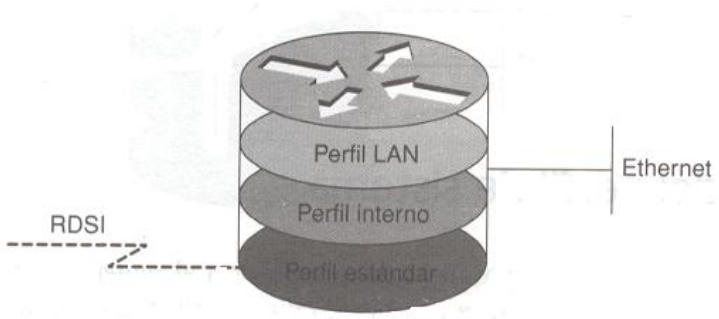


Figura C.2 Perfiles de un router Cisco serie 700

Los parámetros del sistema son independientes de los perfiles y afectan al router como un sistema. Estos parámetros sólo pueden ser modificados en el símbolo del nivel de sistema**(Router_name>** o **>).**

COMANDOS CISCO IOS-700

Puesto que la serie 700 de Cisco no utiliza el software estándar Cisco IOS, sino el software Cisco IOS-700, hay varios comandos con los que debe familiarizarse.

Algunos de estos comandos son análogos a los comandos IOS, y otros son únicos.

Set default

Recarga el router y reinicia la configuración a los valores predeterminados de fábrica. Se pierde la configuración actual.

Upload

Muestra la configuración completa del router, incluyendo todos los perfiles.

Cd

Cuando se introduce este comando sin argumentos, mueve la interfaz de usuario al modo del nivel de sistema o perfil de sistema. Si se le añade el nombre de un perfil existente, mueve la interfaz de usuario al perfil especificado. Los siguientes comandos serán introducidos en ese perfil. Este comando es similar al comando **cd** que encontramos en MS-DOS o UNIX.

Show config

Muestra la configuración del perfil desde el cual el comando es introducido.

Nota_
A diferencia del software IOS, no existe un comando para grabar la configuración. No hay configuración actual o grabada. Cada vez que se introduce un comando, éste se almacena en la NVRAM.

COMANDOS DEL PERFIL DE SISTEMA

El perfil de sistema contiene parámetros que afectan al router como un todo y se aplican al resto de perfiles a menos que ese perfil contenga un comando que sobrescriba el parámetro del sistema.

A continuación se listan algunos comandos del perfil de sistema comúnmente utilizados(algunas veces conocidos como comandos de nivel de sistema).

Set systemname

Especifica el nombre del router, que se muestra como parte del símbolo y se utiliza para autenticación.

Set switch tipo_de_switch

Configura el tipo de switch RDSI con el que se interconecta el router.

Set 1 spid número_ de_spid

Especifica el número de SPID(Identificador del perfil del servicio), si es necesario. Si se necesita un segundo SPID, se utiliza el comando **set 2 spid número_de_spid.**

COMANDOS DEL PERFIL LAN

El perfil LAN incluye la configuración de interfaz Ethernet.

A continuación se listan algunos comandos comúnmente utilizados para la configuración del perfil LAN.

Set ip address dirección

Específica la dirección IP para la interfaz Ethernet 10BaseT.

Set ip netmask máscara_de_subred

Especifíca la máscara de subred para la interfaz Ethernet 10BaseT.

Set ip routing on

Habilita el enrutamiento IP RIP (Protocolo de información de enrutamiento) para la interfaz Ethernet 10BaseT.

COMANDOS DEL PERFIL DE USUARIO

Un perfil de usuario contiene la configuración para un destino alcanzable a través de la interfaz RDSI.

A continuación se listan algunos de los comandos utilizados para crear y configurar un perfil de usuario.

Set user nombre perfil

Crea un perfil con el nombre especificado y mueve la interfaz de usuario al nuevo perfil.

Set ip address dirección

Especifica la dirección IP para la interfaz RDSI.

Set ip netmask máscara_de_subred

Especifica la máscara de subred para la interfaz RDSI.

Set ip route destination 0.0.0.0/0 gateway 0.0.0.0

Establece una ruta estática a la red de destino especificada a través de la dirección del router de próximo salto indicado. En este ejemplo, se definen cualquier dirección y cualquier router. Esto es lo mismo que una ruta predeterminada. Al indicar una subred específica y un router específico, sólo podrá permitir el tráfico a esos destinos tan sólo. (Esto es una forma de filtrado).

Set bridging off

Desactiva el puenteado sobre la interfaz RDSI. Por defecto, el puenteado está habilitado.

EJEMPLO DE CONFIGURACIÓN DE UN ROUTER CISCO SERIE 700

```
> set systemname 700
700> set switch 5ess
700> set 1 spid 01408555123411
700> set 1 spid 01408555432111
700> cd lan
700:LAN> set ip address 172.144.10.1
700:LAN> set ip netmask 255.255.255.0
700:LAN> set ip routing on
700:LAN> cd
700> set user Central
700:Central> set number 5554567
700:Central> set ppp secret client <password>
700:Central> set ip routing on
700:Central> set ip route destination 0.0.0.0/0 gateway 172.16.5.2
700:Central> set ip address 172.16.5.1
700:Central> set ip netmask 255.255.255.0
```

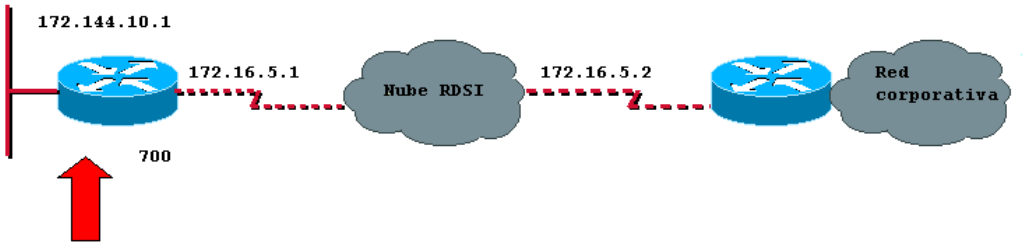


Figura C.3 Configuración típica de SOHO.

A continuación se lista algunos comandos adicionales que son útiles para la localización de problemas y la administración.

Ping dirección

Envía peticiones de eco ISMP(Protocolo de mensajes de control de Internet) a la dirección especificada.

Reboot

Reinicia el router.

Call número

Inicia una llamada manual al número especificado.

Nota_

Para información adicional sobre el software y hardware Cisco serie 700, consulte la **Cisco 700 Serie Router installation Guide,** la **Cisco 700 Series Command Reference,** el CD_ROM de documentación, o la CCO.

RECUPERACIÓN DE CONTRASEÑAS

Este apartado contiene una visión general del registro de configuración virtual usado por el router durante la inicialización. También trata sirve cómo conseguir acceso a un router si olvida o pierde su contraseña. Para entender el proceso de recuperación, primero debe conocer el registro de configuración usado por el router en el proceso de arranque.

EL REGISTRO DE CONFIGURACIÓN VIRTUAL

Cuando un router arranca, se comprueba el registro de configuración virtual para determinar(entre otras cosas) el modo en que debe entrar tras el arranque, dónde conseguir la imagen del software y cómo gestionar el archivo de configuración de la NVRAM. Este registro de 16 bits controla funciones como la velocidad en baudios del puerto de la consola, la operación de carga del software, la habilitación o deshabilitación de la tecla de interrupción durante las operaciones normales, la dirección de multidifusión predeterminada, así como establecer una fuente para arrancar el router. El registro de configuración es 0x2102(un valor hexadecimal). La forma binaria del valor del registro es la siguiente:

0010 0001 0000 0010

Los bits están numerados desde el 0 al 15, comenzando por el bit más a la derecha. Por tanto, los bits 1, 8 y 13 estarían activos en esta configuración. El resto de bits estarían a cero. La tabla D.1 explica el significado de cada bit del registro de configuración virtual.

CÓMO CAMBIAR LA CONFIGURACIÓN DEL REGISTRO DE CONFIGURACIÓN VIRTUAL

Puede cambiar los valores del registro de configuración a través del software IOS o en el modo monitor de ROM. Algunas razones comunes para modificar el valor del registro de configuración virtual son la recuperación de una contraseña perdida, cambiar la velocidad en baudios de la consola, y habilitar o deshabilitar la función de interrupción. Otra razón para modificar el valor del registro de configuración virtual puede ser para controlar el proceso de arranque.

Nota_

Si el router no encuentra ningún comando boot System y no hay imágenes en la memoria Flash, el router utiliza el valor de arranque en red en el registro de configuración para formar un nombre de archivo desde el cual arrancar en red con una imagen del sistema predeterminada almacenada en el servidor de la red vía TFTP(véase la tabla D.3).

Para cambiar el registro de configuración mientras se está ejecutando el software de sistema IOS, siga estos pasos:

Paso 1

Introduzca el comando **enable** y su contraseña para entrar en el nivel privilegiado, tal y como se indica:

```
Router>enable
Password:
Router#
```

Paso 2

En el símbolo del sistema del nivel privilegiado, introduzca el comando **configura terminal**. La contestación será la siguiente

```
Router#configure terminal
Enter configuration commands, one per line.
Edit with DELETE, CTRL/W, and CTRL/U; end with CTRL/Z
Router(config)#
```

Paso 3

Para establecer los contenidos del registro de configuración, introduzca el comando de configuración **config-register valor**, donde **valor** es un número hexadecimal precedido por 0x(véase la tabla D.1)

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

Paso 4

Salga del modo de configuración pulsando ctrl.-Z. Los nuevos valores serán escritos en el registro de configuración virtual; sin embargo, los nuevos valores no tendrán efecto hasta que el software del sistema sea recargado cuando reinicie el router.

Paso 5

Para mostrar el valor de registro de configuración actualmente en uso y el valor que será utilizado en la siguiente carga, introduzca el comando EXEC **show versión**. El valor será mostrado en la última línea de la pantalla de esta forma:

```
Configuration registrer is 0x2142 (will be ox21o2 at next reload)
```

Paso 6

Reinicie el router. El nuevo valor tomará efecto. Los cambios en el registro de configuración tienen efecto sólo cuando el router se reinicia, lo cual ocurre cuando apaga y enciende el router o cuando envía el comando **reload** desde la consola. No es necesario grabar la configuración actual para que los valores del registro sean almacenados. Cuando envíe el comando **reload**, se le mostrará un mensaje pidiéndole si quiere grabar su configuración antes del proceso de reinicio. Si lo único que cambió en el modo de configuración es el registro de configuración, la respuesta a esta pregunta es generalmente no.

Nota_

Aunque este apartado trata sobre el concepto de registro de configuración virtual, no todos los routers tienen idénticos parámetros. Por ejemplo, los nombres de archivos listados en la tabla D.3 son diferentes en plataformas distintas, y en algunos routers, se utiliza un bit adicional para la velocidad de la consola para permitir velocidades mayores. Para información más detallada sobre su hardware específico, compruebe su CD de documentación o el CCO.

Tabla D.1 Significado de los bits de un registro de configuración virtual común.

Numero(s)de bit	Valor hexadecimal	Significado
00 a 03	0x0000 a 0x000F	Capo de arranque (véase tabla D.2).
04	0x0010	No definido.
05	0x0020	No definido
06	0x0040	Provoca que el software del sistema ignore los contenidos de la NVRAM.
07	0x0080	Bit OEM habilitado.
08	0x0100	Interrupción deshabilitada.
09	0x0200	No definido.
10	0x0400	Multidifusión IP con todo 0 si el bit está activo. Este bit trabaja con el bit 14, tal y como muestra la Tabla D.4.
11 a 12	0x0800 a 0x1800	Velocidad de línea de consola(véase la tabla D.5).
13	0x2000	Arranca con el software predeterminado de la ROM si el arranque en red falla.
14	0x4000	Multidifusión IP no tiene números de red. Este valor trabaja con el bit 10, tal y como muestra la tabal D.4.
15	0x8000	Habilita los mensajes de diagnostico e ignora los contenidos de la NVRAM.

Advertencia_

Para evitar confusiones y posibles caídas del router, recuerde que los valores válidos del registro de configuración deben ser combinaciones de valores y no tan sólo valores individuales listados en la tabla D.1. Por ejemplo, el valor predeterminado de fabrica de 0x2102 es una combinación de valores.

Los cuatro bits más bajos del registro de configuración(bits 3, 2, 1 y 0) forman el campo de arranque(véase la tabla D.2). El campo de arranque especifica un número en formato binario. Si establece el valor del campo de arranque a 0, deberá arrancar el sistema operativo manualmente introduciendo el comando b **en el símbolo de arranque, tal y como sigue:**

> b [tftp] flash *nombre_de_archivo*

A continuación puede ver varias opciones del comando b:

- **b.** Arranca el software de sistema predeterminado desde la ROM.
- **b flash.** Arranca el primer archivo en la memoria Flash.
- **b *nombre_de_archivo* [host].** Arranca en red utilizando TFTP.
- **b flash [*nombre_de_archivo*]** Arranca el archivo (nombre_de_archivo) desde la memoria Flash.

Tabla D.2 Explicación del campo de arranque(bits del registro de configuración 00 a 03).

Campo de arranque	Significado
0x0	Tras el arranque, este valor indica al router que entre en el modo monitor de ROM.
0x1	Tras el arranque, este valor habilita al router para arrancar desde su imagen en ROM. Esto también es conocido como modo de arranque.
0x2 a 0xf	Especifica un nombre de archivo de arranque en red predeterminado. Puede habilitar comando de arranque del sistema que sobrescriban el nombre del archivo de arranque en red predeterminado.

Si establece el valor del campo de arranque en el rango de 0x2 a 0xf, hay un comando System boot válido almacenado en el archivo de configuración. Si establece el campo de arranque a cualquier otro patrón de bits, el router utiliza el número resultante para formar un archivo de arranque predeterminado para el arranque en red(véase la tabla D.3).

El router crea un nombre de archivo de arranque predeterminado como parte de los procesos de configuración automáticos. Para formar el nombre de archivo de arranque, el router comienza con la palabra Cisco y le añade el equivalente octal del número del campo de arranque, un guión y el nombre del tipo de procesador. La tabla D.3 muestra un listado de las acciones o los nombres de archivos de arranque predeterminados para los routers serie 2500.

Tabla D.3 Nombres de archivos de arranque predeterminados.

Acción/Nombre de archivo	Bit3	Bit2	Bit1	Bit0
Modo de arranque	0	0	0	0
Software de ROM	0	0	0	1
Cisco2-igs	0	0	1	0
Cisco3-igs	0	0	1	1
Cisco4-igs	0	1	0	0
Cisco5-igs	0	1	0	1
Cisco6-igs	0	1	1	0
cisco7-igs	0	1	1	1
cisco10-igs	1	0	0	0
cisco11-igs	1	0	0	1
cisco12-igs	1	0	1	0
cisco13-igs	1	0	1	1
cisco14-igs	1	1	0	0
cisco15-igs	1	1	0	1
cisco16-igs	1	1	1	0
cisco17-igs	1	1	1	1

Nota_

Un comando de configuración boot System válido en la configuración del router de la NVRAM reemplaza siempre el nombre del archivo de arranque en red predeterminado.

En el ejemplo D.1, el registro de configuración virtual se programa para arrancar el router desde la memoria Flash e ignorar las interrupciones durante el siguiente reinicio del router.

Ejemplo D.1 Programación del registro de configuración para arrancar desde Flash.

```
Router#configure terminal
Enter configuration commands, one por line.
Edit with DELETE, CTRL/W, and CTRL/U; end with CTRL/Z
Config-registrer 0x2102
Boot System flash [filename]
^Z
router#
```

Aunque los cuatro bits más bajos de este registro controlan las características de arranque, hay en él otros bits que se encargan de controlar otras funciones. Concretamente, el bit 8 controla la tecla de la consola. La activación del bit 8(el valor predeterminado de fábrica)hace que el procesador ignore la pulsación de la tecla de ininterrupción de la consola. El borrado del bit 8 indica al procesador que interprete la tecla de interrupción como un comando para forzar al sistema a entrar en el modo monitor de ROM, deteniendo por tanto el proceso de operación normal. El envío de una interrupción en los primeros 60 segundos mientras el router reinicia afectará al router, a pesar de los valores de la configuración. Después de los primeros 60 segundos, una interrupción sólo funcionará si el bit 8 está a 0.

El bit 10 es el encargado de controlar la parte correspondiente al host en la dirección de multidifusión Internet. La activación del bit 10 hace que el procesador utilice todo 0; la deshabilitación del bit 10(el valor predeterminado de fábrica) hace que el procesador utilice todo 1. El bit 10 interactúa con el bit 14, cuya misión es controlar las partes de red y subred de la dirección de multidifusión. La tabla D.4 muestra el efecto combinado de los bits 10 y 14.

Tabla D.4. Valores del registro de configuración para el destino de la dirección de multidifusión IP.

Bit 14	Bit 10	Dirección(<red><host>)
Desactivado	Desactivado	<todo 1><todo 1>
Desactivado	Activado	<todo 0><todo 0>
Activado	Activado	<red><todos 0>
Activado	Desactivado	<red><todos 1>

Los bits 5, 11 y 12 del registro de configuración determinan la velocidad en Baudios del terminal de consola.

La tabla D.5 muestra los valores de bits para las cuatro velocidades en baudios que están disponibles. (El valor predeterminado de fábrica para la velocidad en baudios es 9600).

Tabla D.5. Valores de la velocidad en baudios del terminal de consola del sistema.

Baudios	Bit 12	Bit 11
9600	0	0
4800	0	1
1200	1	0
2400	1	1

El bit 13 determina la respuesta del router a un fallo del arranque. La activación del bit 13 hace que el router cargue el software operativo de la ROM después de cinco intentos fallidos de carga un archivo de arranque desde la red. La desactivación del bit 13 hace que el router continúe intentando cargar un archivo de arranque desde la red indefinidamente. El valor predeterminado de fábrica para el bit 13 es 1.

HABILITACIÓN DEL ARRANQUE DESDE LA MEMORIA FLASH

Para habilitar el arranque desde la memoria Flash, establezca los valores de los bits 3,2,1 y 0 del registro de configuración a un valor entre 2 y F en conjunción con el comando de configuración boot system flash[nombre_de_archivo]. El valor actual de 2 a F no es realmente relevante aquí. Sirve tan sólo para decirle al router que no arranque desde su imagen del IOS de la ROM.

Estando activa la imagen del software IOS del sistema, introduzca el comando configure terminal en el símbolo del modo privilegiado y especifique un nombre de archivo de la Flash desde el que arrancar. Esto se puede ver en el Ejemplo D.2.

Ejemplo D.2. Especificación de un nombre de archivo Flash.

```
router#configure terminal
Enter configuration commands, one per line.
Edit with DELETE, CTRL/W, and CTRL/U; end with CTRL/Z
Router(config)#boot System flash[nombre_de_archivo]
```

Para deshabilitar la interrrupción y habilitar el router para arrancar desde la flash, introduzca el comando **config-register** con el valor mostrado en el ejemplo D.3.

Ejemplo D.3. Establecer el registro de configuración predeterminado.

```
Router#configure terminal
Enter configuration commands, one per line.
Edit with DELETE, CTRL/W, and CTRL/U; end with CTRL/Z
Router(config)#config-reg 0x2102
^Z
router#
```

EL PROCESO DE RECUPERACIÓN DE CONTRASEÑAS

La recuperación de contraseñas le permite alcanzar el control administrativo de su dispositivo si ha perdido u olvidado su contraseña. La premisa básica es simple. Necesita conseguir acceso a su router sin la contraseña. A continuación, necesita restaurar la configuración y reestablecer la contraseña con un valor conocido. Hay dos procedimientos de recuperación de contraseña(discutidos a continuación) que involucran los siguientes pasos:

Paso 1

Configure el router para arrancar sin leer la memoria de configuración (NVRAM). Esto se conoce también como modo de prueba del sistema.

Paso 2

Reinicia el sistema.

Paso 3

Acceda al modo habilitar(lo que puede hacerse sin contraseña si esta en el modo de prueba del sistema).

Paso 4

Vea o cambie la contraseña, o bien borre la configuración.

Paso 5

Reconfigure el router para arrancar y leer la configuración en la NVRAM como hace normalmente.

Paso 6

Reinicie el sistema.

Nota_

Algunas recuperaciones de contraseña requieren que un terminal de consola envíe una señal de interrupción, de modo que debe familiarizarse como su terminal o PC emulador de terminal envía esta señal. Por ejemplo, ProComm utiliza el modo predeterminado de las teclas Alt-b para generar la señal de interrupción. El HyperTerminal de Windows precisa que pulse Ctrl-pausa.

PROCEDIMIENTO 1 DE RECUPERACIÓN DE CONTRASEÑA.

Puede utilizar este primer método para recuperar contraseñas perdidas en los siguientes routers Cisco:

- Cisco serie 2000.
- Cisco serie 2500.
- Cisco serie 3000.
- Cisco serie 4000 con una CPU Motorola 680x0.
- Cisco serie 7000 ejecutando Cisco IOS versión 10.0 o posterior en memorias ROM instaladas en la tarjeta del procesador de ruta. El router puede arrancar el software Cisco IOS versión 10.0 en la memoria Flash, pero también necesita la ROM en la tarjeta del procesador.
- Serie IGS ejecutando Cisco IOS versión 9.1 o posterior en memorias ROM.

Para recuperar una contraseña hábil utilizando el procedimiento uno, sigua estos pasos:

Paso 1

Conecte un terminal o PC con software de emulación de terminal al puerto de consola del router.

El valor del registro de configuración esta en la última línea de la pantalla. Anote si el registro de configuración esta configurado para habilitar o deshabilitar interrupciones.

El valor predeterminado de fabrica del registro de configuración es 0x2102. Observe que el tercer dígito empezando por la derecha en este valor es impar, la interrupción esta habilitada.

Paso 2

Apage y encienda el router.

Paso 3

Pulse la tecla de interrupción del terminal durante los primeros sesenta segundos del encendido del router.

Aparecerá el símbolo > sin nombre del router. Si no aparece el símbolo, el terminal no esta enviando la señal de interrupción correcta. En este caso, compruebe la configuración del terminal o del emulador de terminal. Para ver el registro de configuración actual, puede escribir el valor **e/s 2000002.**

Nota_

El número que referencia la localización del registro de configuración puede cambiar entre distintas plataformas. Compruebe la documentación específica de su producto para localizar el número exacto que debe utilizar.

Paso 4

Introduzca **o/r 0x2142** en el símbolo > para arrancar desde la memoria Flash, u **o/r 0x2141** para arrancar desde las ROM de arranque.

Nota_

El primer carácter es la letra o no el número cero. Si tiene memoria Flash y esta intacta, 0x2142 es el mejor valor. Utilice 0x2141 sólo si la memoria Flash a sido borrada o no esta instalada.

Paso 5

En el símbolo >, introduzca el comando **initialize** para iniciar el router. Esto hace que el router se reinicie pero ignore su configuración grabada. Aparecerá la pantalla de configuración del sistema.

Nota_

Si utiliza normalmente el comando **boot network**, o si tiene múltiples imágenes en la memoria Flash y arranca con una imagen no predeterminada, la imagen en la memoria Flash podría ser diferente.

Paso 6

Responda **no** a las preguntas de la configuración del sistema hasta que aparezca el siguiente mensaje:

Paso 7

Pulse la tecla retorno.
Aparecerá el símbolo **router>.**

Paso 8

Introduzca el comando **enable.**
Aparecerá el símbolo **Router#.**

Paso 9

Elija una de las siguientes opciones:
Para ver la contraseña, si no está encriptada, introduzca el comando **show startup-config**.

Para cambiar la contraseña(si está encriptada, por ejemplo), introduzca los siguientes comandos.

```
Router#copy startup-config running-configN
Router#configure terminal
Router(config-if)enable secret 1234abcd
```

Paso 10

Puesto que ignorar la NVRAM y elegir abortar la configuración dejará todas las interfaces en estado de apagado, es importante habilitar todas las interfaces con el comando **no shutdown**, como se muestra aquí:

```
Router(config)#interface ethernet 0
Router(config-if)#no shutdown
```

Paso 11

Grabe su nueva contraseña con los siguientes comandos:

```
Router(config-if)#ctrl-z
Router#copy rounning-config startup-config
```

Nota_

El comando enable secret proporciona un incremento en la seguridad al almacenar la contraseña de habilitación utilizando una función criptografica no reversible; sin embargo, no podrá recuperar una contraseña perdida que haya sido encriptada.

Paso 12
Introduzca el comando **configure terminal** en el símbolo del nivel EXEC para entrar en el modo de configuración.

Paso 13
Introduzca el comando **config-register** y el valor original que almacenó en el Paso 1.

Paso 14
Pulse Ctrl-z para abandonar el editor de configuración.

Paso 15
Introduzca el comando **reload** en el símbolo del nivel EXEC privilegiado.

PROCEDIMIENTO 2 DE RECUPERACIÓN DE CONTRASEÑAS

Utilice este segundo método para recuperar contraseñas perdidas en los siguientes routers Cisco:

- Cisco 1003.
- Cisco serie 1600.
- Cisco serie 3600.
- Cisco serie 4500.
- Cisco serie 7200.
- Cisco serie 7500.
- Routers basados en DT Orion.
- Plataformas AS5200 y AS5300.

Para recuperar una contraseña utilizando el procedimiento 2, siga estos pasos:

Paso 1
Conecte un terminal o un PC con software de emulación de terminal al puerto de consola del router.
El valor del registro de configuración está en la última línea de la pantalla. Anote si el registro de configuración está configurado para habilitar o deshabilitar interrupciones.
El valor predeterminado de fábrica del registro de configuración es 0x2102. Observe que el tercer dígito empezando por la derecha en este valor es impar, lo cual deshabilita las interrupciones. Si el tercer dígito no es impar, la interrupción está habilitada.

Paso 2
Apague y encienda el router.

Paso 3
Pulse la tecla de interrupción del terminal durante los primeros 60 segundos del encendido del router.

Aparecerá el símbolo **rommon>.** Si no aparece, el terminal no está enviando la señal de interrupción correcta. En este caso, compruebe la configuración del terminal o del emulador de terminal.

Paso 4

Introduzca el comando **confreg** en el símbolo **rommon>**. Grabe el valor actual del registro de configuración virtual tal y como se muestra en la salida de este comando.

Aparecerá la siguiente pregunta:

```
Do you wish to change configuration [y/n]?
```

Paso 5

Responda **yes** y pulse retorno.

Paso 6

Acepte los valores predeterminados para las siguientes preguntas hasta que aparezca la siguiente pregunta:

```
Ignore System config info [y/n]?
```

Paso 7

Responda **yes**.

Paso 8

Responda no a las siguientes preguntas hasta que aparezca la siguiente pregunta:

```
Change boot characteristics [y/n]?
```

Paso 9

Responda **yes**

Aparecerá la siguiente pregunta:

```
Enter to boot:
```

Paso 10

Introduzca **2** en este símbolo y pulse Retorno si está arrancando desde la memoria Flash. O bien, si la memoria Flash ha sido borrada, introduzca **1**.

Se mostrará un resumen de la configuración, y aparecerá la siguiente pregunta:

```
Do you wish to change configuration [y/n]?
```

Paso 11

Responda **no** y pulse Retorno.

Aparecerá el siguiente símbolo:

```
Rommon>
```

Paso 12

Introduzca el comando **reset** en el símbolo del modo privilegiado **rommon>**, o inicie el ciclo de arranque del router.

Paso 13

Durante el arranque del router, responda no en todas las preguntas de configuración hasta que aparezca el siguiente símbolo:

```
Router>
```

Paso 14

Introduzca el comando enable para entrar en el modo de habilitación.

Aparecerá el símbolo **Router#**.

Paso 15

Elija una de las siguientes opciones:

Para ver la contraseña, si no está encriptada, introduzca el comando **show startup-config.**

Para combiar la contraseña(si está encriptada, por ejemplo), introduzca los siguientes comando:

```
Router#copy startup-config running-config
Router#configure terminal
Router(config)#enable secret 1234abcd
```

Paso 16

Puesto que ignorar la NVRAM y elegir abortar la configuración dejará todas las interfaces en el estado apagado, es importante habilitar todas las interfaces con el comando **no shutdown**, como se muestra aquí:

```
Router(config)#interface ethernet 0
Router(config-if)#no shutdown
```

Paso 17

Grabe su nueva contraseña utilizando los siguientes comando:

```
Router(config-if)#ctrl-z
Router#copy runnin-config startup-config
```

Nota_

El comando enable secret proporciona un incremento en la seguridad al almacenar la contraseña de habilitación utilizando una función criptográfica no reversible; sin embargo, no podrá recuperar una contraseña perdida que haya sido encriptada.

Paso 18

Introduzca el comando **configure terminal** en el símbolo.

Paso 19

Introduzca el comando **config-register** y el valor original que almacenó en el Paso 1.

Paso 20

Pulse ctrl.-z para abandonar el editor de configuración.

Paso 21

Introduzca el comando **reload** en símbolo.

Información básica de las contraseñas del enrutador y sus usos

Punto de control	Tipo de contraseña	¿Qué está restringido?
Puerto consola	Línea	Iniciar una sesión mediante una línea local a través del puerto de consola.
Puerto AUX	Línea	Iniciar la sesión mediante una línea módem (o local) conectada al puerto auxiliar.
Inicio de sesión de red	Terminal virtual	Iniciar la sesión en el enrutador mediante una conexión de red usando Telnet sobre una línea VTY.
EXEC privilegiado	Enable o Enable Secret	Entrar al nivel más potente privilegiado EXEC del entorno IOS.

CONTRASEÑAS DE LÍNEA

Las contraseñas de línea se usan para controlar quién puede iniciar la sesión en un enrutador. Se usan para definir protección por contraseña en la línea terminal de consola, línea AUX(auxiliar) y en cualquiera de las cinco líneas (VTY) de terminal virtual.

Es necesario establecer al menos una contraseña para las líneas VTY del enrutador. Si no se define una contraseña de línea, cuando intente iniciar la sesión en el enrutador mediante Telnet, aparecerá un mensaje de error *password required but none set*(es necesaria una contraseña, pero no ha escrito ninguna).

Dto:	Operación y red	Proyecto:	CCNA
Autor:	Elva y Chechu	Fecha:	01/04/02
Asunto:	Preparación para certificación CCNA Cisco Systems		
Estado:	Pendiente revisión	Revisión:	1.0

RECUPERACIÓN DE CONTRASEÑA LINE

Es necesario forzar al enrutador al modo diagnostico de fabrica para recuperar una contraseña de linea perdida. Consulte la documentación de instalación y mantenimiento del hardware para el producto. Una vez forzado el enrutador al modo diagnostico de fábrica, siga estos pasos:

1. Conteste yes cuando se le pregunte si quiere establecer las direcciones de fabricante. Aparece el símbolo del sistema test-system>.

2. Introduzca el comando enable para acceder al símbolo del sistema test-system>.

3. Escriba config-term, luego escriba show startup-config. Ahora verá el archivo de configuración del sistema. Busque la contraseña y anótela.

4. Reinicie el enrutador.

5. Use la contraseña recuperada de línea(la que anotó) para iniciar la sesión en el enrutador.

RESUMEN DE COMANDOS

COMANDOS PARA LA RESOLUCION DE PROBLEMAS

Ping[dirección de nodo] comando utilizado para comprobar la conexión entre dos routers distintos(**ping** seguido de dirección IP) en la interfaz del router remoto. También puede utilizarse para comprobar la conexión entre los nodos de red.

Show controler Permite ver el estado de los controladores de interfaz en el router.

Show interface[tipo de interfaz][n° de interfaz] un magnifico comando para consultar todos los parámetros relacionados con una determinada interfaz del router.

Show stacks Muestra los mensajes de error relacionados con la detección anormal de un router cuando este vuelve ha iniciarse.

Trace[direcciónIP] Muestra la ruta entre un router y otro router o nodo de la interconexión. Este comando también puede utilizarse con direcciones apple talk.

Reload comando de modo privilegiado que arranca de nuevo el router

Quit comando usuario/privilegiado que te permite salir del router.

Ctrl-Z comando para cerrar una sesión de configuración.

Banner motd[carácter final de portada] comando de configuración global que permite crear una portada para la pantalla de conexión al router. El carácter final de portada puede ser cualquier carácter alfanumérico que indique al modo de configuración que ahí termina el texto de la portada.

Disable permite salir del modo privilegiado y volver al modo usuario.

Enable permite acceder al modo privilegiado. Debe introducirse contraseña de activación, para lanzar el modo privilegiado.

Set clock Comando privilegiado que permite determinar la fecha y hora en el router.

COMANDOS DE ANALISIS DEL ROUTER

Show cdp neighbor muestra los routers que están directamente conectados al router mediante una conexión LAN o en serie.

Show clock Muestra los parámetros de hora y fecha para el router.

Show flash Muestra el o los archivos IOS que incluye el router en la flash RAM y el total de memoria flash ram disponible y utilizada.

Show hub muestra información sobre el estado de los puertos hub en un router 2505.

show tech-support comando que reporta toda la información del router.

show dialer visualizas el canal que esta activo.

Show interface ethernet[n° de interfaz] muestra la configuración actual de la interfaz Ethernet especificada.

Show interface serial[n° de interfaz] muestra la configuración actual de la interfaz serie especificada.

Show interface relaciona todas las interfaces del router y las estadísticas relacionadas con la interfaz, como su actual configuración y encapsulación.

COMANDOS DE MEMORIA DEL ROUTER

Copy flash tftp copia un archivo IOS de la memoria flash a un servidor TFTP.

Copy running-config startup-config copia la configuración que se esta ejecutando en la memoria NVRAM del router.

Copy startup-config tftp copia la configuración de arranque de la NVRAM al servidor TFTP.

Copy tftp flash comando privilegiado para copiar un archivo IOS del servidor TFTP a la memoria flash ram del router.

Copy tftp startup-config comando privilegiado para copiar un archivo de configuración de arranque del servidor tftp a la memoria NVRAM del router.

Erase startup-config borra la configuración de arranque de la memoria NVRAM del router.

Show running-config Muestra la configuración del router que se esta ejecutando en la RAM.

Show startup-config comando que muestra la configuración del router almacenada en la memoria NVRAN del router. La carga el router cuando arranca de nuevo.

COMANDOS DE CONFIGURACION DE CONTRASEÑAS Y NOMBRES DEL ROUTER

Enable secret password[contraseña] comando de configuración global que permite cambiar la contraseña secreta del modo privilegiado en el router.

Hostname[nombre] permite cambiar el nombre del router

Line console 0 permite lanzar el modo configuración de línea para determinar la contraseña del router.

Line vty 04 permite lanzar el modo de configuración de terminal para establecer la contraseña de la terminal virtual para el router.

Password[contraseña] se utiliza en el modo configuración de línea de consola 0 para determinar la contraseña de conexión al router; también se utiliza en el modo de configuración de línea vty 04 para especificar la contraseña virtual para el router.

COMANDOS DE CONFIGURACIÓN DE INTERFAZ

Config permite lanzar el modo configuración global.

Ctrl + Z se utiliza para cerrar una sesión de configuración.

Enable cdp activa una determinada interfaz(desde el indicador config-if del modo configuración) para mostrar los routers vecinos conectados(puede entonces utilizar el comando show cdp neighbor en el router9.

Encapsulation[tipo de encapsulación] comando de configuración especificado de interfaz que permite determinar el tipo de encapsulación para una interfaz LAN o en serie incluida en el router.

Interface Ethernet[numero de interfaz] comando de configuración global que permite configurar parámetros relacionados con una determinada interfaz ethernet.

Interface serial[numero de interfaz] comando de configuración global que permite configurar parámetros relacionados con una determinada interfaz en serie.

COMANDOS RELACIONADOS CON IP

Access-list[#listado]permit or deny[dirección IP][mascara comodín] comando de configuración global para crear un listado de acceso. Debe incluirse la dirección de la red o nodo que se aceptará o rechazará, así como la mascara comodín. Repita este comando para cada línea que aparezca en el listado de acceso. El **#rango de lista** para IP es 1-99.

Debug IP IGRP transaction permite ver las estadísticas referidas a los mensajes de actualización IGRP en el router.

Debug ip rip permite ver los mensajes de actualización enviados y recibidos por el router.

Ip acces-group[n° de listado]out or in comando de configuración de interfaz donde se asocia un determinado listado de acceso Ip a un interfaz. El parámetro **out** o **in** se utiliza para filtrar el trafico que entre o salga de dicha interfaz.

Ip address[dirección ip][mascara de subred] utilizado en el modo config-if para asignar una dirección IP a una interfaz del router. Al comando ip address le sigue la dirección IP y la subred que se asigne al interfaz.

Ip ruting comando de configuración global que permite el encaminamiento IP en el router.

Ip unnumbered[interfaz o interfaz lógica] introducido en el indicador config-if este comando permite indicar que una interfaz en serie no dispone de una dirección IP propia. El parámetro interfaz o interfaz lógica, debe referirse a un interfaz router(como un puerto ethernet) en el router que si tiene asignada una dirección IP.

Network[numero principal de red] utilizado con los comandos router rip y router igrp para especificar las redes principales IP a las que esta directamente conectado el router.

No debug all desactiva la depuración(comando del modo privilegiado).

No ip ruting comando de configuración global que desactiva el encaminamiento IP en el router.

Router igrp[numero de sistema autónomo] comando de configuración global que activa el encaminamiento igrp. El numero de sistema autónomo correspondiente al numero AS para el dominio de encaminamiento al que pertenece el router(si existe un AS).

Route rip comando de configuración global que activa el encaminamiento rip.

Show access-list[número de listado] permite ver un determinado listado de acceso. El numero de listado corresponde al número que se asigno al listado cuando se creo.

Show ip interfaces[tipo y numero de interfaz] permite ver los parámetros de configuración IP asociados para una determinada interfaz.

Show protocol proporciona información referente a las actualizaciones del protocolo de encaminamiento enviadas y recibidas por el router(como difusiones rip).

Show ip rute muestra la tabla de encaminamiento rip o igrp para el router.

telnet[dirección ip] comando del modo usuario y privilegiado que permite conectar remotamente con otro router.

COMANDOS RELACIONADOS CON WAN

Bandwidth[ancho de banda] comando **config-if** para determinar el ancho de banda de una interfaz serie.

Clock rate[velocidad de reloj] comando **config-if** para determinar la velocidad de reloj en una interfaz en serie cuando el router se utiliza como un dispositivo DCE.

Encapsulation[protocolo WAN] comando **config-if** para determinar el tipo de encapsulación para una interfaz en serie(como ppp y hdlc).

Frame –relay interface-dlci[#de dlci] comando **config-if** que permite determinar el número DLCI para una interfaz activada para relé de trama.

Frame-relay lmi-type[tipo LMI] comando **config-if** para determinar el tipo de LMI para una interfaz configurada para relé de trama.

Isdn spid[nombre del canal spid][# de spid] comando de configuración global que permite introducir el numero único SPID para cada canal ISDN.

Isdn switch type basic-[identificador de conmutador] comando de configuración global que permite determinar el tipo de conmutador ISDN al que esta conectado el router.

Show frame-relay lmi muestra los mensajes no validos enviados o recibidos a través de la conexión de relé de trama del router.

Show frame-relay map muestra la asignación DLCI a las interfaces del router.

X25address[dirección de enlace de datos]comando **config-if** que permite especificar la dirección de enlace de datos para x25, cuando x25 se especifica como tipo de encapsulación.

X25ips[bits] comando **config-if** que permite determinar el tamaño del paquete de entrada para una interfaz x25.

X25ops[bits] comando **config-if** que permite determinar el tamaño del paquete
de salida para una interfaz x25.

X25win[numero de paquetes] comando **config-if** que permite determinar el tamaño de la ventana de entrada para una interfaz x25.

X25wout[numero de paquetes] comando **config-if** que permite determinar el tamaño de la ventana de salida para una interfaz x25.

Ctrl-Z estemos en el nivel que estemos volvemos al modo privilegiado.

Service Password-encryption nos da un servicio visual de las password que utiliza el fichero de configuración.

Logging synchronous evita que los mensajes inesperados que aparecen en pantalla, nos desplacen los comandos que estamos escribiendo en el momento. Este comando se introduce en el modo de configuración de línea.

```
Router(config)#line vty 04
Router(config-line)#logging synchronous
Router(config)#line console 0
Router(config-line)#logging synchronous
```

Show running-config muestra la configuración que corre en la memoria RAM.

Show startup-config Visualiza la configuración de la memoria RAM.

Copy running-config startup-config Almacena el contenido de la memoria Ram en la memoria NVRAM.

Show controller[numero de interfaz] Desde el modo privilegiado, se puede verificar si un interfaz esta cableado como DTE o como DCE.

GLOSARIO

Algoritmo. Procedimiento matemático o lógico para realizar un cálculo o para resolver un problema. Sucesión de operaciones elementales, perfectamente especificadas y ordenadas, que sirven para hacer algo preciso.

Ancho de banda (Bandwidth): Define la cantidad de información que puede ser transmitida en un periodo de tiempo determinado a través de una Red. Es la diferencia entre la frecuencia más alta y la más baja de un canal de transmisión (en hertzs, Hz). Margen de frecuencias capaz de transmitirse por una red de telecomunicaciones.

ANSI (American National Standards Institute): El Instituto Nacional Norteamericano de Normalización es la organización responsable de aprobar las normas de los EEUU en muchas áreas, ordenadores y comunicaciones, y es miembro de ISO.

Apantallamiento. Recubrimiento de un cable por el que se transmite información en forma de señal electromagnética, con el fin de evitar las interferencias que pudiesen alterar la información.

Arbol. Estructura de representación de la información que consiste en un único registro "padre" del que dependen cero o más registros "hijos" que, a su vez, pueden dar origen a nuevos subárboles.

ASCII. **American Standard Code for Information Interchange**. Código estándar americano para intercambio de la información. Esquema normalizado de codificación de caracteres introducido en 1.963 y muy utilizado en muchas máquinas. Sistema de codificación de caracteres alfanuméricos en 7 bits para la operación interna del computador y su comunicación con los periféricos. Este sistema, promovido por el ANSI (American National Standard Institute), es ampliamente utilizado por ordenadores personales, estaciones de trabajo y miniordenadores.

ATM. **Asynchronous Transfer Mode**. Modo de Transferencia Asíncrona. Técnica de conmutación por paquetes de alta velocidad adecuada para redes de área metropolitana (MAN), transmisión de banda ancha y redes digitales de servicios integrados (RDSI).

Analógico: Es una forma de transmitir o representar la realidad que imita aquello que representa con infinitos términos intermedios, como hace el teléfono convencional con las características de la voz.

Anonymous FTP: Es aquel FTP que permite a un usuario la captura de documentos, ficheros, programas y otros datos contenidos en archivos existentes en cualquier lugar de Internet sin necesidad de tener un registro de usuario y contraseña

ARPANET (Advanced Research Projects Agency Network): Red pionera de larga distancia financiada por ARPA (hoy DARPA) con finalidades militares, que fue el eje central del desarrollo de Internet.

Asíncrono. Dos señales son asíncronas o no están sincronizadas, cuando sus correspondientes instantes significativos no coinciden. También es un término referido a una transmisión no sincronizada, en la cual el sincronismo entre emisor y receptor se establece de nuevo en el terminal, para cada carácter transmitido, mediante la recepción de un bit de arranque; se finaliza con un bit de parada. Es el modo típico para transmisiones en telegrafía, minicomputadores y ordenadores personales.

Backup. Véase Copia de Seguridad.

Backbone. Red principal de una red de comunicaciones.

Banda ancha. Técnica de comunicaciones en la que las señales digitales se transmiten moduladas, pudiendo enviarse por un solo canal múltiples señales simultáneas. La UIT-T define también como banda ancha a las comunicaciones digitales a más de 2 Mbps.

Banda base. Técnica de comunicaciones en la que las señales digitales codificadas se transmiten en su forma original, es decir, sin modulación.

Base de datos. **Data base**. Conjunto de datos no redundantes, almacenados en un soporte informático, organizados de forma independiente de su utilización y accesibles simultáneamente por distintos usuarios y aplicaciones. La diferencia de una BD respecto a otro sistema de almacenamiento de datos es que estos se almacenan en la BD de forma que cumplen tres requisitos básicos: no redundancia, independencia y concurrencia.

BIOS. **Basic Input-Output System**. Conjunto de rutinas básicas que se almacenan en memoria ROM. Este sistema incluye rutinas para el teclado, la pantalla, los puertos paralelos y serie y para servicios internos como hora y fecha. Acepta solicitudes desde las unidades de los dispositivos en el sistema operacional, así como desde los programas de aplicaciones.

Bit. **Binary Digit**. Dígito binario. Unidad mínima de información con la que trabajan los ordenadores. Es un dígito del sistema binario que puede tener el valor 0 o 1.

Bit de datos. Son los bits que configuran un carácter, excluyendo a los de inicio, parada y paridad.

Bit de paridad. Consiste en un único bit, que indica si el número de bits con valor "1" enviados es par o impar. Es el método más elemental de detección de errores.

Baudio (Baud): Número de veces por segundo que cambia el estado de la señal de un medio de transmisión. Aplicado al modem, la señal que envía por la línea telefónica.

Bridge. **Puente**. Unidad Funcional que interconecta dos redes de área local que utilizan el mismo protocolo de control de enlace lógico pero distintos protocolos de control de acceso al medio dentro del nivel 2 de OSI.

Buffer. Segmento reservado de memoria que se usa para almacenar datos mientras se procesan. Conjunto de registros conectados en paralelo que actúan como memoria intermedia para almacenar datos temporalmente para compensar y adaptar diferencias de velocidad entre emisor y receptor.

Bus. Conjunto de líneas que transportan información binaria entre la UCP, la memoria principal y la unidad de entrada/salida. Facilitan la transmisión de datos entre dispositivos situados en dos puntos terminales, pudiendo, únicamente, transmitir uno de ellos en un momento dado.

Byte. Agrupación fundamental de información binaria formada por 8 bits. Es la unidad mínima que puede direccionarse, pero no la unidad mínima que puede tratarse.

Canal. Denominación general para una vía de transmisión lógica o física.

CCITT. **Comitée Consultatif International Télégraphique et Téléphonique**. Comité Consultivo Internacional de Telegrafía y Telefonía. Antiguo órgano competente de la Unión Internacional de Telecomunicaciones de las Naciones Unidas en asuntos de telefonía, telegrafía y datos, que coordinaba los Sistemas telefónicos y de comunicación de datos de todo el mundo. Con frecuencia, sus recomendaciones técnicas se convierten en normas reconocidas internacionalmente. Ha sido sustituido por la UIT-T (Unión Internacional de Telecomunicaciones - Telemática, ITU-T: International Telecommunicacion Union - Telematics).

Cliente/Servidor. Arquitectura de sistemas de información en la que los procesos de una aplicación se dividen en componentes que se pueden ejecutar en máquinas diferentes. Modo de funcionamiento de una aplicación en la que se diferencian dos tipos de procesos y su soporte se asigna a plataformas diferentes.

Codificación. Transformación de un mensaje en forma codificada, es decir, especificación para la asignación unívoca de los caracteres de un repertorio (alfabeto, juego de caracteres) a los de otro repertorio. **||** Conversión de un valor analógico en una señal digital según un código prefijado.

Código. Cada una de las secuencias de caracteres que transforman los elementos de un repertorio en otro.

Código ASCII. Véase ASCII.

Código binario. Código en el que los elementos se representan solamente por los valores "1" y "0". Es el código empleado principalmente dentro de los circuitos de los equipos físicos.

Contraseña. Véase Password.

Control de Calidad. Conjunto de actividades destinadas a comprobar que el proyecto se ha desarrollado de acuerdo con la metodología y estándares establecidos, así como a garantizar que cumple con los requisitos especificados.

Control de Enlace Lógico. Véase LLC.

Controlador. **Driver.** Conjunto de programas, dispositivo electrónico (o ambos) que controla el intercambio de información entre el ordenador y un periférico.

Copia de seguridad. **Backup**. Replicación periódica y almacenamiento externo (usualmente en discos y/o cintas) de datos y programas en previsión de posibles contingencias. Reproducción de los datos actuales guardados en un soporte informático, para tenerlos disponibles en caso de que un desastre del sistema impida recuperar los datos con los que se está trabajando.

CPU. **Central Processing Unit.** Unidad Central de Proceso. Parte principal del ordenador que incluye la unidad aritmético-lógica (ALU) y la unidad de control (UC).

CSMA/CD. **Carrier Sense Multiple Access with Collision Detection**. Protocolo de comunicaciones para una red de área local que utiliza una estructura en bus. Define los niveles físico y de enlace del modelo OSI para el método de acceso a la red por el cual una estación obtiene el uso del medio físico para enviar un mensaje a través de la red. La especificación de este protocolo se describe en las normas IEEE 802.3 e
ISO 8802.3, ambas basadas en el estándar Ethernet.

Canal B. Denominación del ITU-T, antiguamente CCITT, para un canal con una velocidad de transmisión de 64 Kbit/s, destinado al transporte de los flujos de información del usuario, en el acceso básico o acceso primario de la Red Digital de Servicios Integrados (RDSI).

Canal D. Denominación del ITU-T, antiguamente CCITT, para el canal que, en la Red Digital de Servicios Integrados, se utiliza para transferencia de la información de señalización y así establecer las comunicaciones en los canales B asociados.

Canal de señalización. En telefonía móvil es el canal de intercambio de información entre la estación base y los móviles. La señalización opera a diferentes velocidades y tiene funciones individuales.

Canal de sincronización. En el sistema GSM de telefonía móvil es el canal que transmite la información para la sincronización de la trama (número de la trama asignado a la estación móvil) y la identificación de la estación base transceptora (BTS). En inglés se expresa de forma abreviada como "SCH".

Conmutación. Conjunto de operaciones necesarias para unir entre sí los circuitos, con el fin de establecer una comunicación temporal entre dos o más estaciones o puestos. La conmutación está asociada principalmente a una central telefónica y consta de dos partes básicas: 1) el establecimiento, mantenimiento y liberación de la comunicación (procesamiento de la llamada) coordinados por el control; 2) el establecimiento de la vía física por la cual se produce la comunicación realizada por la red de conexión.

Conmutación de células. Técnica de transmisión utilizada en servicios de circuitos de conmutación con células de longitud fija. Se denomina frecuentemente como "Cell Relay". El principal ejemplo es el Modo de Transferencia Asíncrono conocido como "ATM".

Conmutación de circuitos. Es una técnica en la que los equipos que se comunican entre sí utilizan un canal físico dedicado extremo a extremo, que se mantiene durante el tiempo de duración de la llamada o por el periodo de contratación.

Conmutación de paquetes. Es un método de comunicación exclusivamente digital, en el que los mensajes que se transmiten se dividen en segmentos y que, junto a la información adicional necesaria para su encaminamiento en la red, se convierten en paquetes. Éstos son transferidos a través de la red mediante procesos de almacenamiento y reenvío sobre circuitos. virtuales (circuitos no físicos), que permiten la compartición de los canales físicos de comunicaciones de la red, pues solamente los ocupan durante el tiempo de transmisión.

Conmutación digital. En el entorno de telefonía se refiere al establecimiento de conexiones a través de un centro de conmutación o central telefónica mediante operaciones con señales digitalizadas, es decir, sin convertirlas a su forma analógica original. Las señales de datos están normalmente en forma digital (excepto cuando se convierten a analógicas mediante un módem), por lo tanto, el término "conmutación digital" raramente se utiliza en relación con datos porque las señales siguen siendo digitales aunque puedan conmutarse en base a un circuito conmutado.

Conmutación rápida de paquetes. Término genérico para perfeccionar tecnologías de conmutación de paquetes, como los modos de transporte denominados "Frame Relay" y "Cell Relay". Se diferencia de la conmutación de paquetes según la recomendación X.25, por su transporte a alta velocidad. También permite la transmisión de voz, datos y vídeo.

Cracker (Intruso): Es una persona que intenta acceder a un sistema informático sin autorización, y a menudo tienen malas intenciones, en contraste con los hackers.

Decodificación. Conversión de un valor digital en una señal analógica. **||** Proceso de reconversión de un mensaje codificado al mensaje que dio lugar a la codificación.

DECnet. Red de comunicaciones de Digital, que soporta RAL de estilo Ethernet y WAN de banda base y de banda ancha en líneas públicas y privadas.

DRAM. **Dynamic Random Access Memory**. Memoria de acceso aleatorio dinámica. Los elementos de memoria mantienen su contenido mediante un refresco periódico.

Dúplex. Circuito o canal bidireccional que puede transmitir la información simultáneamente en ambas direcciones. **||** En impresión se utiliza para impresiones a dos caras.

DARPA (Defense Advanced Research Projects Agency): Organismo dependiente del Departamento de Defensa norteamericano, que jugó un papel importante en el nacimiento de Internet con la red ARPANET.

Dial-up (Conexión por línea conmutada): Es una conexión temporal establecida entre ordenadores por línea telefónica normal.

Digital: Es una forma de representar la realidad mediante unas corrientes de valores finitos formadas por unos y ceros.

DNS (Domain Name System): El "Sistema de Nombres de Dominio" es un servicio de búsqueda de direcciones IP de sistemas centrales (o hosts) basándose en los nombres de dominio de estos.

Dominio: Estructura jerárquica que organiza las máquinas de Internet de forma que sea fácil recordar su nombre.

EEPROM. **Electrically Erasable Programmable Read Only Memory**. Memoria de sólo lectura programable y borrable eléctricamente. Memoria de sólo lectura que puede ser borrada con señales eléctricas.

EIA/TIA. **Electronic Industry Association / Telecommunication Industry Association**, Asociación de la industria electrónica / Asociación de la industria de telecomunicaciones.

Encapsulación. Permite la conexión de varias redes informáticas entre sí para formar una sola red de nivel más alto. Cuando se utiliza encapsulación, se define un nuevo nivel de protocolo; esto proporciona una semántica uniforme para servicios tales como conmutación de paquetes, correo electrónico, etc. **||** En programación orientada a objetos, es la asociación de datos y funciones que tiene el efecto de ocultar al solicitante de una función la forma en que ésta se ha desarrollado.

EPROM. **Erasable-Programable Read-Only Memory**. Memoria de sólo lectura borrable y programable. PROM que se puede borrar por la acción de la luz ultravioleta.

Equipo físico. **Hardware**. Circuitería electrónica. En general, todos los elementos físicos de un equipo informático.

Equipo lógico. **Software**. Programas del sistema, de aplicación, de utilidades, procedimientos, reglas y su documentación asociada, relacionados con la operación de un ordenador. Conjunto de instrucciones y datos que un ordenador es capaz de entender.

Estándar. Conjunto de reglas y regulaciones acordado por una organización oficial de estándares (estándar de jure) o por aceptación general en el mercado (estándar de facto).

Ethernet. Red de área local ISO 8023 que transmite a 10 Mbits/s y pueden conectarse en total hasta 1024 nodos. Conjunto de especificaciones que definen el funcionamiento de redes locales CSMA/CD.

Emulación de terminal: Proceso por el que nuestro ordenador simula mediante software una terminal (pantalla y teclado, sin disco, memoria ni CPU). Es necesario para usar Telnet o ejecución remota.

Encriptado: Proceso de codificación y ocultación de paquetes de datos para impedir su lectura por terceros y asegurar la confidencialidad de determinadas transacciones.

Enlace (Link): Apuntador de hipertexto que sirve para saltar a otra página web, a otro servidor, o a otro servicio (correo, FTP) cuando se navega por Internet.

Etiqueta: Códigos empleados en el lenguaje HTML (entre < >) para describir la página, con los que se definen los estilos de texto, imágenes e hiperenlaces, entre otras cosas. También llamadas "marcas".

FADU. **File Access Data Unit**. Véase Unidad de datos de acceso a fichero.

FDDI. **Fiber Distributed Data Interface**. Especificación de una red de área local con topología en anillo, método de acceso por paso de testigo cuya estructura se implementa sobre un cable de fibra óptica. Esta norma fue desarrollada por el ANSI.

Frame. Encuadre, bloque, secuencia, trama

Frame Relay. Sistema de transporte para la transmisión de datos (paquetes) a alta velocidad (hasta 45 Mbits/s) mediante celdas de longitud variable.

Firewall: El "cortafuegos" es una medida de seguridad que se coloca entre una Red local e Internet, que filtra los paquetes que entran y salen hacia Internet desde una red local.

Frecuencia. El número de ciclos por segundo de una onda. Se mide en Hertzios (Hz), que indican el número de cambios por segundo.

FTP. **File Transfer Protocol**. Protocolo para la Transferencia de Ficheros.

Gateway. **Puerta de acceso, pasarela.** Unidad de interfuncionamiento. Dispositivo de comunicaciones que interconecta sistemas diseñados conforme a protocolos propietarios, o entre un sistema con un protocolo propietario y un sistema abierto o una red RAL, teniendo lugar una conversión completa de protocolos hasta la capa 7 del modelo de referencia OSI.

GIF. **Graphics Interchange File**. Formato de fichero para intercambio de gráficos.

Gigabyte. **GB.** Unidad de memoria que equivale a 1.024 MB.
GUI. **Graphic User Interface**. Interfaz Gráfica de Usuario. Un tipo de interfaz de usuario que sustituye las pantallas basadas en caracteres por pantallas de gráficos de alta resolución, con todos los puntos direccionables, que utiliza ventanas para mostrar simultáneamente múltiples aplicaciones y permite además que el usuario introduzca datos a través del teclado o de un dispositivo apuntador, como por ejemplo, un ratón, un lápiz óptico o una bola.

Hardware. Véase Equipo físico.

Hacker (Pirata): Persona que goza alcanzando un conocimiento profundo sobre el funcionamiento interno de un sistema, de un ordenador o de un a red de ordenadores. (Este término se suele usar como peyorativo, cuando en este sentido se debería utilizar el término cracker.

HDLC. **High level Data Link Control**. Protocolo de comunicaciones orientado al bit, normalizado por ISO.

Host. En una red informática, es un ordenador central que facilita a los usuarios finales servicios tales como capacidad de proceso y acceso a bases de datos, y que permite funciones de control de red.

Hub. Equipo para diversos tipos de cables y para diversas formas de acceso que sirve de plataforma integradora para distintas clases de cables y de arquitectura.

IEEE. **Institute of Electrical and Electronics Engineers.** Instituto de Ingeniería Eléctricos y Electrónicos. Organismo normalizador de métodos de acceso y control para redes de área local. Es miembro de ANSI e ISO.

IP. **Internet Protocol.** Protocolo internet. Protocolo sin conexión (connectionless) encargado de controlar la información por la red. Permite la integración de otras subredes. Véase TCP/IP.

ISDN. **Integrated Services Digital Network**. Véase RDSI.
Normalización. Es el máximo organismo de normalización a nivel internacional con sede en Ginebra. Su **Technical Committe** 97 (TC97) es responsable del modelo de referencia de siete capas definidos para sistemas de comunicaciones directas (Véase OSI). Edita propuestas de normas internacionales "Draft International Standard (DIS)". Juntamente con el IEC son los dos organismos competentes para emitir normas internacionales.

ITU. **International Telecommunication Union**. Unión Internacional de Telecomunicaciones. Antiguo CCITT. Véase UIT-T.

Jerarquía. Red ordenada de conceptos u objetos en la cual unos están subordinados a otros.

Java: Lenguaje de programación orientado a objetos, especialmente concebido para crear aplicaciones que funcionen en Internet.

JPEG. **Joint Photographic Experts Group**. El consorcio internacional de hardware, software e industrias editoriales dedicadas a desarrollar estándares internacionales para la compresión de imágenes fotográficas fijas en sistemas digitales.

Kbps. Kilobits por segundo. Medida de velocidad de transmisión.

KiloByte. **KB.** Unidad de medida de memoria. Equivalencia: 1 KByte = 10^3 Bytes = 1.024 Bytes.

LAN. **Local Area Network**. Red de área local. Véase RAL.

LLC. **Logical Link Control (Protocol).** Control de enlace lógico. Protocolo de nivel de enlace del modelo OSI definido para redes de área local.

MAC. **Medium Access Control**. Protocolo de control de acceso al medio empleado para la propagación de las señales eléctricas. Define el subnivel inferior de la capa 2 del modelo OSI (nivel de enlace).

MAN. **Metropolitan Area Network**. Red de Area Metropolitana. Red de comunicaciones que cubre un área geográfica como una ciudad o un suburbio.

Mbps. **Megabits por segundo.** Medida de velocidad de transmisión. 1Mbps = 10^6 bps (bits por segundo).

MegaByte. **MB.** Unidad de medida de memoria que equivale a 1.024 KB.

Memoria caché. Memoria intermedia de acceso aleatoria muy rápida entre la unidad central de proceso y la memoria principal que almacena los datos o instrucciones extraídos más frecuente y recientemente de la memoria principal.

Módem/Fax. Módem que también permite enviar y recibir datos a/desde una máquina fax.

Módem. Modulador/demodulador. Equipo para la transmisión de datos que convierte señales analógicas en digitales y viceversa. Elemento físico que permite transmitir información entre dos ordenadores mediante una línea telefónica.

Modulación. Modificación de alguno de los parámetros de una onda portadora por una señal moduladora que se quiere transmitir.

OSI. **Open Systems Interconnection**. Interconexión de Sistemas Abiertos. Estándar ISO para comunicaciones a nivel mundial que define una estructura con el fin de implementar protocolos en 7 estratos o capas. El control se transfiere de un estrato al siguiente comenzando en el estrato de aplicación en una estación, llegando hasta el estrato inferior, por el canal hasta la próxima estación y subiendo nuevamente la jerarquía. Las 7 capas o estratos son: Físico, Enlace de datos, Red, Transporte, Sesión, Presentación y Aplicación. El OSI requiere una enorme cooperación para que sea un estándar universal como el sistema telefónico.

PABX. **Private Automatic Branch Exchanges**. Centralita privada automática, con conexión a la red pública.

PAD. **Packet Assembler-Disassembler**. Ensamblador-Desensamblador de paquetes. Equipo que permite, mediante el empaquetamiento y desempaquetamiento de datos, la conexión de terminales que no están pensados para la conmutación de paquetes (p.e. terminales start-stop) a redes de conmutación de paquetes.

Paquete. Secuencia de dígitos binarios, incluyendo datos y señales de control, que se transmite y conmuta como un todo.

Password. **Contraseña.** Palabra clave que identifica al usuario para proteger y definir el acceso a un equipo y por la que se identifica al usuario.

PBX. **Private Automatic Branch Exchanges**. Centralita privada automática, con conexión a la red pública.

PC. **Personal Computer**. Ordenador Personal. Ordenador generalmente monousuario y monotarea, que utiliza como CPU un microprocesador. Tradicionalmente asociado a los ordenadores de uso personal o doméstico.

PCI. **Peripheral Component Interconnect**. Bus de 32 bits de longitud de palabra de datos para los ordenadores personales.

PCM. **Pulse Code Modulation**. Método para transformar una señal analógica en un valor digital. Uno o más canales se mezclan para formar un sólo canal.

Portadora. Frecuencia portadora. Señal con una determinada frecuencia utilizada en transmisión como soporte para transmitir información.

Protocolo. Conjunto formal de convenciones que gobiernan el formato y control de datos. Conjunto de procedimientos o reglas para establecer y controlar transmisiones desde un dispositivo o proceso fuente a un dispositivo o proceso objeto.

Protocolo de comunicaciones. Reglas preestablecidas para efectuar la conexión electrónica entre dos sistemas de comunicación. Puede haber diferentes tipos, que establecen desde las normas para las tensiones eléctricas en los extremos de los contactos metálicos hasta reglas lógicas de alto nivel, como la organización de los datos a trasmitir, su modo de identificación, codificación, etc. Conjunto de reglas y convenios que posibilitan la transmisión de información a través de una red de telecomunicaciones. Conjunto de reglas semánticas y sintácticas que rigen el comportamiento de las unidades funcionales en las comunicaciones.

Protocolo Internet. Véase IP.

Puerto. **Port**. Conector de la placa base para instalar elementos externos.

RAID. **Redundant Array of Inexpensive Disks.** Batería Redundante de Discos de Bajo Coste. Configuraciones de arrays de discos con los que se obtiene mayor fiabilidad ante fallos y se mejora la tasa de transferencia de datos.

RAL (LAN). Red de Area Local (**Local Area Network**). Conexión física entre equipos (estaciones, servidores, ordenadores) y periféricos (impresoras, trazadores, gateways, etc.) para la transmisión de la información de bit en serie con la finalidad de compartir recursos con tiempos de acceso muy breves.

RAM. **Random Access Memory.** Memoria de Acceso Aleatorio; memoria de acceso directo; memoria viva. Memoria volátil de escritura y lectura, habitualmente utilizada como almacén temporal de datos.

Ranura de expansión. Zócalos conectados en la placa base del ordenador en los cuales se insertan las tarjetas de expansión.

RDSI (ISDN). Red Digital de Servicios Integrados (**Integrated Services Digital Network**). Red que evoluciona a partir de la redelefónica; permite la conectividad digital de usuario a usuario, porporcionando servicios telefónicos y no-telefónicos.

ROM. **Read Only Memory.** Memoria permanente sólo de lectura. Memoria sólo accesible para la lectura de su contenido, no para su modificación.

Router. Enrutador, encaminador de paquetes hacia su destino por la ruta óptima.

Router (Direccionador): Dispositivo que se encarga de dirigir el tráfico en una red. la información pasa de nuestro ordenador a un router, y luego de router a router, hasta que el destino está en la misma red local que el último.

RPC. **Remote Procedure Call**. Llamada de Procedimiento Remoto. Modelo de comunicación mediante el cual las funciones hacen solicitudes en forma de llamadas a procedimientos distribuidos en la red. La ubicación de los procedimientos es transparente a la aplicación solicitante.

RTC. **Red Telefónica Conmutada.** Se refiere a las comunicaciones que emplean el teléfono, con acceso por medio de llamada, normalmente utilizadas para comunicaciones de voz.

SAI. Sistema de Alimentación eléctrica Ininterrumpida.

Semidúplex. Circuito o canal que puede transmitir la información alternativamente (no simultáneamente) en ambas direcciones.

Señalización. Es el intercambio de información o mensajes dentro de una red de telecomunicación para controlar, establecer, conmutar, encaminar, supervisar y gestionar sus comunicaciones.

Servidor. Ordenador que ofrece sus prestaciones a varios ordenadores clientes conectados a una red.

Sesión. En la arquitectura de red, conjunto de actividades que tienen lugar durante el establecimiento, mantenimiento y liberalización de una conexión, con vistas a permitir una comunicación de datos entre unidades funcionales.

TCP/IP. **Transmission Control Protocol/Internet Protocol**. Protocolo de Control de Transmisión/Protocolo Interredes. Protocolo para el control de la transmisión orientado a la conexión (**connection-oriented**) TCP, establecido sobre el protocolo internet (IP). Su amplia extensión permite reconocerla como una norma de facto aunque no es una norma internacional. Mientras que TCP es un protocolo de transporte (nivel cuatro de OSI), el IP es un protocolo de red. Son un conjunto de normas (nivel tres de OSI) para RALs definidas en Estados Unidos para los organismos de defensa para la DARPA (Defense Advanced Research Projects Agency), donde está definida la forma en que deben comunicarse los ordenadores, las redes entre sí y el encaminamiento del tráfico de la red.

Token Bus. Protocolo para transmisión de datos en una red de área local, utilizando una estructura en anillo. Define los niveles físico y de enlace del modelo OSI. La especificación de este protocolo se recoge en la norma IEEE 802.4 del IEEE y en la norma 8802.4 de la ISO.

Token Ring. Protocolo para transmisión de datos en una red de área local, utilizando una estructura en bus. Define los niveles físico y de enlace del modelo OSI. La especificación de este protocolo se recoge en la norma IEEE 802.5 del IEEE y en la norma 8802.5 del ISO.

UIT-T. **Unión Internacional de Telecomunicaciones, Sección Telemática.** Organo competente de la Unión Internacional de Telecomunicaciones de las Naciones Unidas en asuntos de telefonía, telegrafía y datos. Los miembros que forman parte de la UIT-T son todas las operadoras públicas (PTT, **Postal Telephone and Telegraph Administrations**) del mundo. Sus 18 comisiones (I-XVIII) son las encargadas de emitir las conocidas recomendaciones del UIT-T. Antes denominada CCITT.

UTP. **Unshielded Twisted Pair**. Par trenzado no apantallado.

VRAM. **Video Random Access Memory.** Memoria de Acceso Aleatorio del Monitor. Memoria empleada para almacenar las imágenes representadas en pantalla.

WAN. **Wide Area Network**. Red de área extensa.

X.25. Interfaz para la transmisión de datos en redes de conmutación de paquetes (PSDN, Packed Switched Data Network). Está definido por las 3 primeras capas del modelo OSI. Permite circuitos virtuales así como recuperación de datos y recuperación de errores. Son recomendaciones de la UIT-T para intercomunicaciones de paquetes. Véase Iberpac.

BIBLIOGRAFÍA

Configuración de routers Cisco Cisco Press
Allan Leinwand / Bruce Pinsky

Interconexión de dispositivos de red de Cisco Cisco Press
Steven McQuerry

Router Cisco Serie practica Prentice Hall
Joe Habraken

Manual de Cisco MacGraw-Hill
Tom Shaughnessy / Toby Velte

Academia de networking de Cisco Sistems Guía del primer año
Cisco Press

OTROS TITULOS DE INTERES

Arquitecturas de enrutamiento en Internet **Cisco Press**
Halabi/McPherson

Tecnologías de interconectividad de redes Cisco Press / Prentice Hall
Merilee Ford / H.kimlen / Steve Spanier / Tim Stenvenson

Interconectividad Manual para resolución de problemas
Cisco Press / Precntice hall
M.Kim Lew / Spunk M. Loy / tim Stevenson / Kathleen Guayanés

RDSI conceptos funcionalidades y servicios MacGraw-Hill
Gary Kessler / Peter Southwick

Tecnologías adsl y xdsl MacGraw-Hill
Walter Gavalski

Redes Locales Ra-Ma
Jose Luis y cristina Raya