Cisco | Networking Academy®
Mind Wide Open™

CCNA Exploration 4.0

Acceso a la WAN

Tour del curso | Introducción del curso | Iniciar el curso

CAPITULO I – "Introducción a las redes WAN"

1.0 Introducción del capítulo

1.0.1 Introducción del capítulo

Cuando una empresa crece y agrega sucursales, servicios de comercio electrónico u operaciones globales, una sola red LAN ya no es suficiente para satisfacer los requisitos de la empresa. En la actualidad, el acceso a una red de área extensa (WAN, Wide Area Network) se ha vuelto esencial para las empresas grandes.

Existe una variedad de tecnologías WAN que satisfacen las diferentes necesidades de las empresas y hay muchas maneras de agrandar la red. Al agregar el acceso WAN, se presentan otros aspectos a tomar en cuenta, como la seguridad de la red y la administración de las direcciones. Por lo tanto, el diseño de una WAN y la elección de los servicios de red adecuados de una portadora no es una cuestión simple.

En este capítulo, primero analizará algunas de las opciones disponibles para diseñar WAN empresariales, las tecnologías disponibles para implementarlas y la terminología utilizada para explicarlas. Aprenderá a seleccionar las tecnologías, los servicios y los dispositivos WAN apropiados para satisfacer los requisitos cambiantes de una empresa en evolución. Las actividades y las prácticas en el laboratorio confirman y refuerzan su aprendizaje.

Al finalizar este capítulo, podrá identificar y describir las tecnologías WAN apropiadas para habilitar servicios WAN integrados a través de una red empresarial con varias ubicaciones.

En este capítulo, aprenderá a:

- Describir cómo la arquitectura empresarial de Cisco proporciona servicios integrados a través de una red empresarial.
- Describir conceptos claves de la tecnología WAN.
- Seleccionar la tecnología WAN apropiada para satisfacer diferentes requisitos comerciales empresariales.

1.1 Provisión de servicios integrados a la empresa

1.1.1 Introducción de redes de área extensa (WAN)

¿Qué es una WAN?

Una WAN es una red de comunicación de datos que opera más allá del alcance geográfico de una LAN.

Las WAN se diferencian de las LAN en varios aspectos. Mientras que una LAN conecta computadoras, dispositivos periféricos y otros dispositivos de un solo edificio u de otra área geográfica pequeña, una WAN permite la transmisión de datos a través de distancias geográficas mayores. Además, la empresa debe suscribirse a un proveedor de servicios WAN para poder utilizar los servicios de red de portadora de WAN. Las LAN normalmente son propiedad de la empresa o de la organización que las utiliza.

Las WAN utilizan instalaciones suministradas por un proveedor de servicios, o portadora, como una empresaproveedora de servicios de telefonía o una empresa proveedora de servicios de cable, para conectar los sitios de una organización entre sí con sitios de otras organizaciones, con servicios externos y con usuarios remotos. En general, las WAN transportan varios tipos de tráfico, tales como voz, datos y video.

Las tres características principales de las WAN son las siguientes:

- Las WAN generalmente conectan dispositivos que están separados por un área geográfica más extensa que la que puede cubrir una LAN.
- Las WAN utilizan los servicios de operadoras, como empresas proveedoras de servicios de telefonía, empresas proveedoras de servicios de cable, sistemas satelitales y proveedores de servicios de red.
- Las WAN usan conexiones seriales de diversos tipos para brindar acceso al ancho de banda a través de áreas geográficas extensas.

¿Por qué son necesarias las WAN?

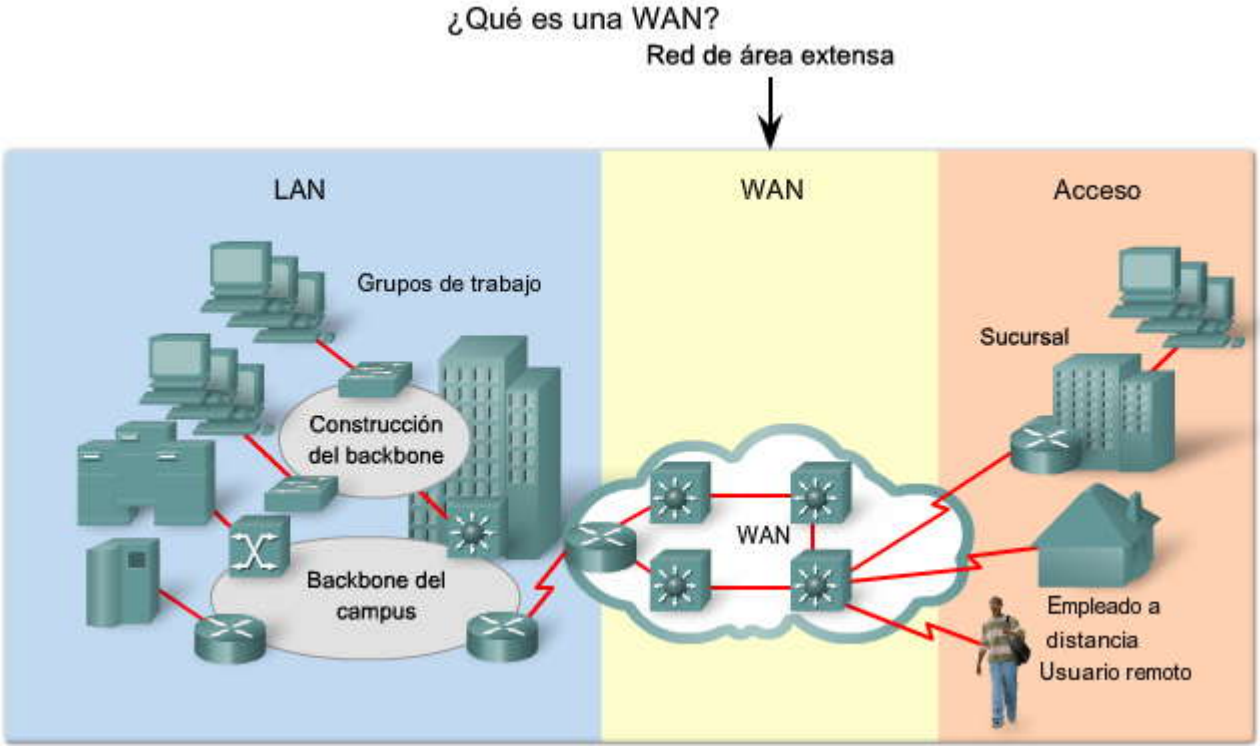
Las tecnologías LAN proporcionan velocidad y rentabilidad para la transmisión de datos dentro de organizaciones, a través de áreas geográficas relativamente pequeñas. Sin embargo, hay otras necesidades empresariales que requieren la comunicación entre sitios remotos, incluidas las siguientes:

- Los empleados de las oficinas regionales o las sucursales de una organización necesitan comunicarse y compartir datos con la sede central.
- Con frecuencia, las organizaciones desean compartir información con otras organizaciones que se encuentran a grandes distancias. Por ejemplo, los fabricantes de software comunican periódicamente información sobre productos y promociones a los distribuidores que venden sus productos a los usuarios finales.
- Con frecuencia, los empleados que viajan por temas relacionados con la empresa necesitan acceder a la información que se encuentra en las redes corporativas.

Además, los usuarios de computadoras domésticas necesitan enviar y recibir datos que recorren distancias cada vez mayores. Aquí se ofrecen algunos ejemplos:

- Ahora es común en muchos hogares que los consumidores se comuniquen con bancos, tiendas y una variedad de proveedores de bienes y servicios a través de las computadoras.
- Los estudiantes buscan información para las clases mediante índices de bibliotecas y publicaciones ubicadas en otras partes del país y del mundo.

Como, obviamente, no es posible conectar computadoras a nivel nacional o mundial de la misma manera en la que las computadoras de una LAN se conectan con cables, han evolucionado diferentes tecnologías para cubriresta necesidad. Internet se está utilizando cada vez más como una alternativa económica al uso de una WAN empresarial para algunas aplicaciones. Hay nuevas tecnologías disponibles para las empresas que proporcionan seguridad y privacidad para las comunicaciones y las transacciones a través de Internet. El uso de redes WAN solas o en combinación con Internet permite a las organizaciones y a los particulares satisfacer sus necesidades de comunicaciones de área extensa.



1.1.2 La empresa en evolución

Las empresas y sus redes

A medida que las empresas crecen, contratan más empleados, abren sucursales y se expanden a mercados globales. Estos cambios ejercen influencia sobre los requisitos de servicios integrados e impulsan los requisitos de red de la empresa. En este tema, analizaremos las maneras en las que las redes de una empresa cambian para adaptarse a los requisitos empresariales cambiantes.

Cada empresa es única y la manera en la que una organización crece depende de muchos factores, tales como el tipo de productos y servicios que vende la empresa, la filosofía de administración de los dueños y el clima económico del país en donde opera la empresa.

En épocas de desarrollo económico lento, muchas empresas se concentran en aumentar su rentabilidad mediante la mejora de la eficacia de las operaciones existentes, el aumento de la productividad de los empleados y la reducción de los costos de

operación. El establecimiento y la administración de redes pueden representar gastos importantes de operación e instalación. Para justificar un gasto de esta envergadura, las empresas esperan que sus redes funcionen de manera óptima y que puedan brindar un conjunto de servicios y aplicaciones en constante crecimiento para respaldar la productividad y la rentabilidad.

A modo de ejemplo, utilicemos una empresa ficticia llamada Span Engineering y observemos cómo cambian los requisitos de red a medida que la pequeña empresa local se convierte en una empresa global.

Haga clic en las fichas de la figura para ver cada etapa de crecimiento y la topología de red correspondiente.

Oficina pequeña (una única LAN)

Span Engineering, empresa consultora especializada en medioambiente, ha desarrollado un proceso especial para convertir la basura doméstica en electricidad y está desarrollando un proyecto piloto para un gobierno municipal en su área local. La empresa, que fue creada hace cuatro años, ha crecido hasta contar con 15 empleados: seis ingenieros, cuatro diseñadores de diseño asistido por computadora (CAD), un recepcionista, dos socios de alto nivel y dos asistentes de oficina.

La gerencia de Span Engineering espera tener proyectos a escala completa una vez que el proyecto piloto demuestre exitosamente la factibilidad del proceso. Hasta ese momento, la empresa debe administrar sus costos cuidadosamente.

Para la oficina pequeña, Span Engineering utiliza una única LAN para compartir información entre las computadoras y para compartir dispositivos periféricos, como una impresora, un trazador gráfico de gran escala (para imprimir planos de ingeniería) y equipo de fax. Recientemente actualizaron la LAN para proporcionar un servicio económico de voz sobre IP (VoIP, Voice over IP) para ahorrar en costos de líneas telefónicas independientes para los empleados.

La conexión a Internet se realiza a través de un servicio común de banda ancha llamado línea de suscripción digital (DSL, Digital Subscriber Line) que es suministrado por el proveedor de servicios de telefonía local. Con tan pocos empleados, el ancho de banda no es un problema importante.

La empresa no puede afrontar el costo de contar con personal de soporte de tecnología de la información (TI) propio, de manera que utiliza los servicios de soporte del mismo proveedor del servicio. La empresa también utiliza un servicio de hosting en lugar de adquirir y operar sus propios servidores de FTP y correo electrónico. La imagen muestra un ejemplo de una oficina pequeña y su red.

Campus (varias LAN)

Cinco años después, Span Engineering ha crecido con rapidez. Tal y como los propietarios deseaban, la empresa fue contratada para diseñar e implementar una instalación de conversión de basura de tamaño real, poco tiempo después de la implementación exitosa de la primera planta piloto. Desde entonces, también han obtenido otros proyectos en municipalidades vecinas y en otras partes del país.

Para administrar la carga de trabajo adicional, la empresa contrató más personal y alquiló más oficinas. Ahora es una empresa pequeña a mediana con cientos de empleados. Se desarrollan muchos proyectos de manera simultánea, y cada uno requiere un gerente de proyecto y personal de soporte. La empresa se ha organizado en departamentos funcionales y cada departamento cuenta con su propio equipo de organización. Para satisfacer sus necesidades crecientes, la empresa se mudó a varios pisos de un edificio de oficinas más amplio.

A medida que la empresa se expandió, la red también creció. En lugar de ser una única LAN pequeña, la red ahora está compuesta por varias subredes, cada una dedicada a un departamento diferente. Por ejemplo, todo el personal de ingeniería está en una LAN, mientras que el personal de mercadotecnia está en otra LAN. Estas LAN múltiples están unidas para crear una red que abarca a toda la empresa, o campus, que se extiende en varios pisos del edificio.

Ahora la empresa cuenta con personal propio de TI para dar soporte a la red y mantenerla. La red incluye servidores para correo electrónico, transferencia de datos y almacenamiento de archivos, herramientas y aplicaciones de productividad basadas en la Web, además de la Intranet de la empresa para proporcionar documentos internos e información a los empleados. Además, la empresa tiene una Extranet que proporciona información de proyectos sólo a clientes designados.

Sucursal (WAN)

Después de cinco años, Span Engineering ha tenido tanto éxito con su proceso patentado que la demanda de sus servicios se disparó y ahora se están desarrollando nuevos proyectos en otras ciudades. Para administrar esos proyectos, la empresa ha abierto pequeñas sucursales más cercanas a los sitios de los proyectos.

Esta situación presenta nuevos desafíos para el equipo de TI. Para administrar la entrega de información y servicios en toda la empresa, Span Engineering ahora tiene un centro de datos que aloja las diversas bases de datos y servidores de la empresa.

Para garantizar que todas las partes de la empresa puedan tener acceso a los mismos servicios y aplicaciones, independientemente de la ubicación de las oficinas, la empresa ahora necesita implementar una WAN.

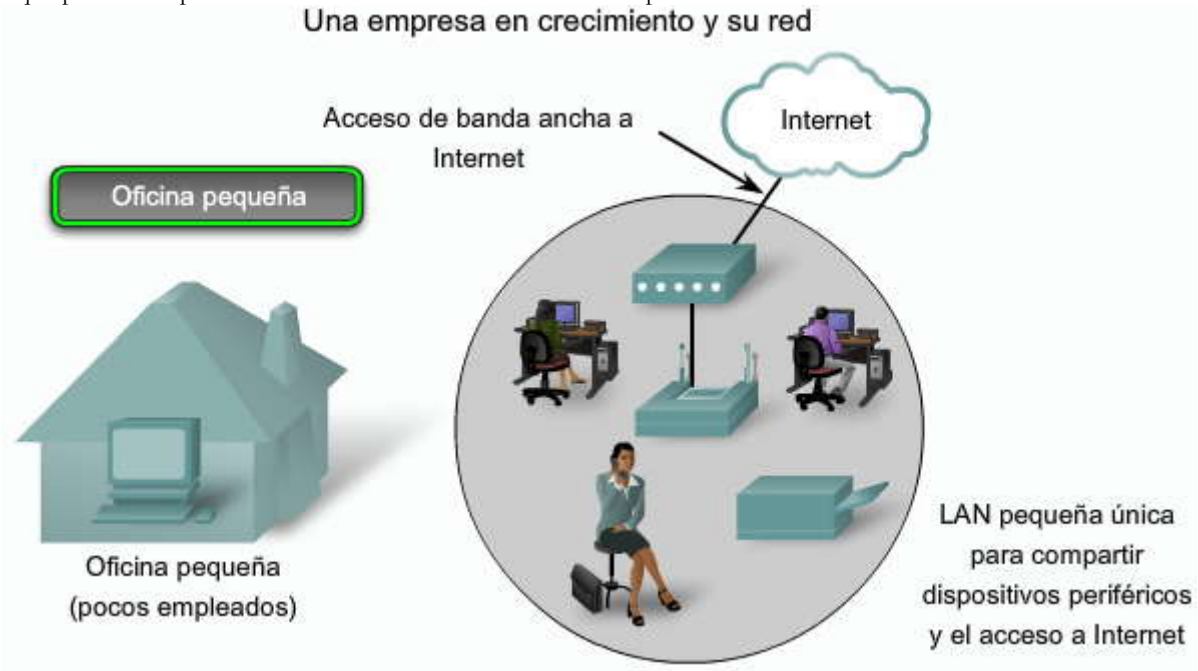
Para las oficinas de las sucursales ubicadas en ciudades vecinas, la empresa decide utilizar líneas privadas dedicadas a través del proveedor de servicios local. Sin embargo, para las oficinas que se encuentran en otros países, Internet es ahora una opción atractiva de conexión WAN. Si bien la conexión de las oficinas mediante Internet es económica, también presenta ciertos aspectos relacionados con la seguridad y la privacidad que el equipo de TI debe tener en cuenta.

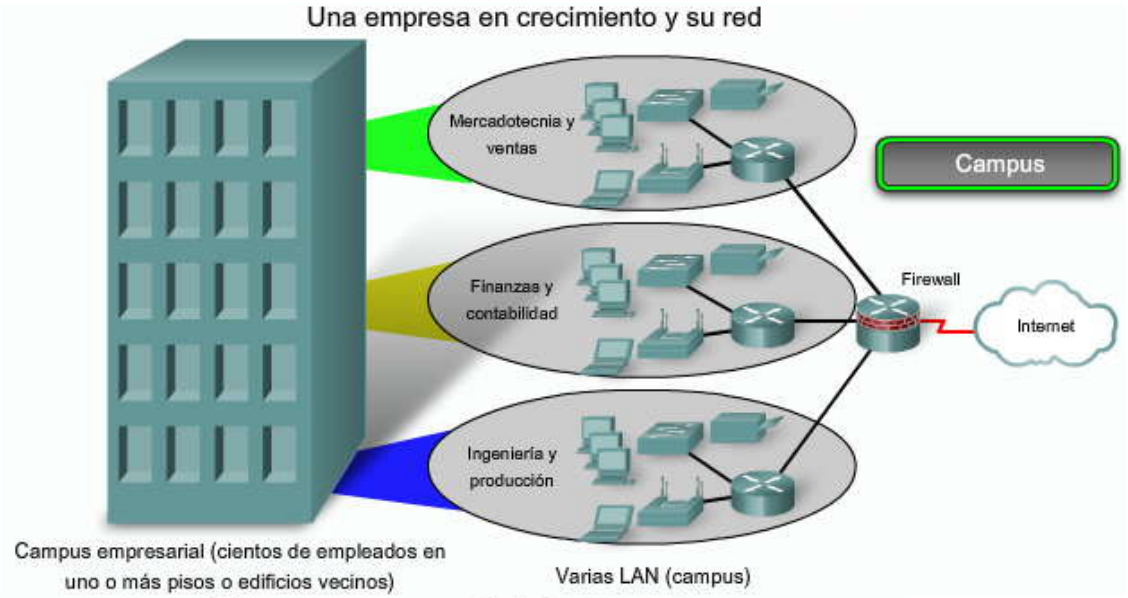
Distribuida (Global)

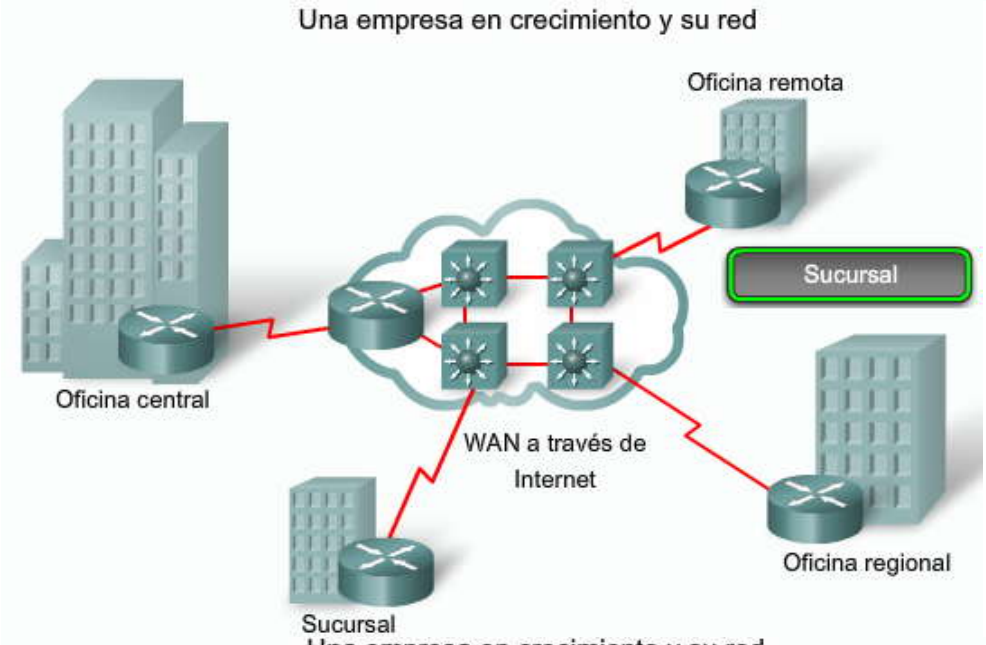
Span Engineering ya tiene 20 años de actividad y cuenta con miles de empleados distribuidos en oficinas de todo el mundo. El costo de la red y los servicios relacionados es ahora un gasto importante. La empresa desea proporcionar a sus empleados los mejores servicios de red al menor costo posible. La optimización de los servicios de red le permitiría a cada empleado trabajar con un alto nivel de eficiencia.

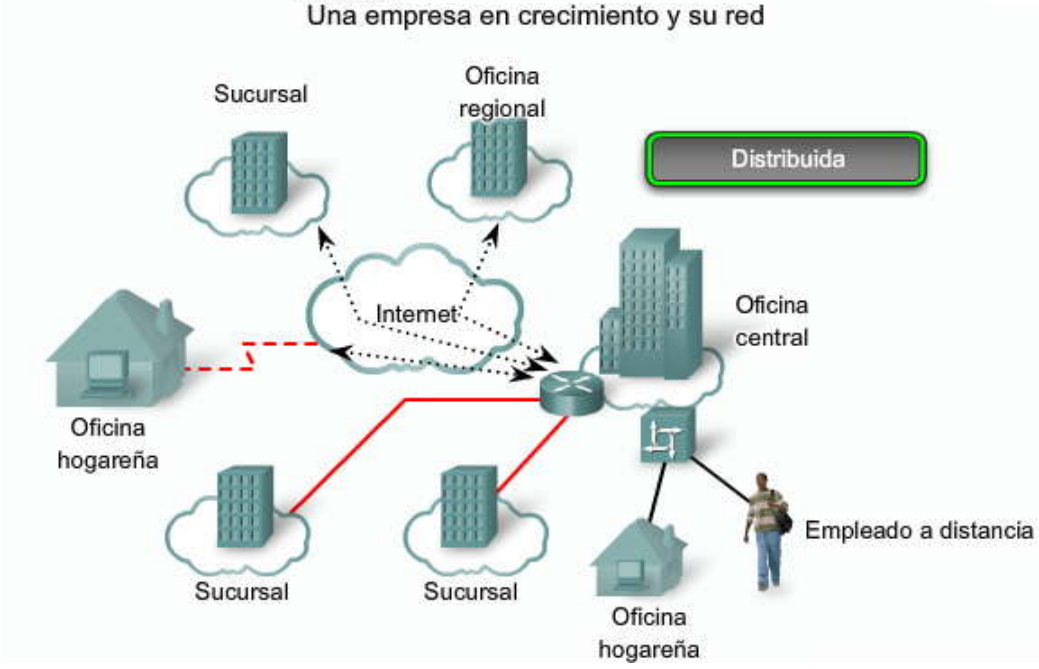
Para aumentar la rentabilidad, Span Engineering necesita reducir sus gastos operativos. Ha trasladado algunas de sus oficinas a áreas menos costosas. La empresa también fomenta el trabajo a distancia y la formación de equipos de trabajo virtuales. Se están utilizando aplicaciones basadas en la Web, incluidas las conferencias a través de la Web, e-learning y herramientas de colaboración en línea, a fin de aumentar la productividad y reducir costos. Las redes privadas virtuales (VPN, Virtual Private Networks) de sitio a sitio y acceso remoto permiten a la empresa utilizar Internet para conectarse con los empleados y las instalaciones de todo el mundo de manera sencilla y segura. Para satisfacer estos requisitos, la red debe proporcionar los servicios convergentes necesarios y asegurar la conectividad WAN a través de Internet con personas particulares y oficinas remotas.

Como hemos visto en este ejemplo, los requisitos de la red de una empresa pueden cambiar drásticamente a medida que la empresa crece con el tiempo. La distribución de los empleados ahorra costos de muchas maneras, pero genera mayores exigencias para la red. La red no solamente debe cubrir las necesidades operativas cotidianas, sino que además debe poder adaptarse y crecer a medida que la empresa cambia. Para enfrentar estos desafíos, los diseñadores y los administradores de red eligen cuidadosamente las tecnologías, los protocolos y los proveedores de servicios de red, y optimizan las redes con muchas de las técnicas que enseñamos en esta serie de cursos. El siguiente tema describe un modelo de red para diseñar redes que puedan adaptarse a las necesidades cambiantes de las empresas en evolución de la actualidad.




Una empresa en crecimiento y su red
Mercadotecnia y ventas
Finanzas y contabilidad
Ingeniería y producción
Campus
Firewall
Internet
Campus empresarial (cientos de empleados en uno o más pisos o edificios vecinos)
Varias LAN (campus)


Una empresa en crecimiento y su red
Oficina remota
Sucursal
Oficina central
WAN a través de Internet
Oficina regional
Sucursal


Una empresa en crecimiento y su red
Sucursal
Oficina regional
Distribuida
Internet
Oficina central
Oficina hogareña
Sucursal
Sucursal
Oficina hogareña
Empleado a distancia

Modelo de diseño jerárquico

El modelo de red jerárquico es una herramienta de alto nivel, útil para diseñar una infraestructura de red confiable. Proporciona una vista modular de una red, lo que simplifica el diseño y la creación de una red que pueda crecer en el futuro.

Modelo de red jerárquico

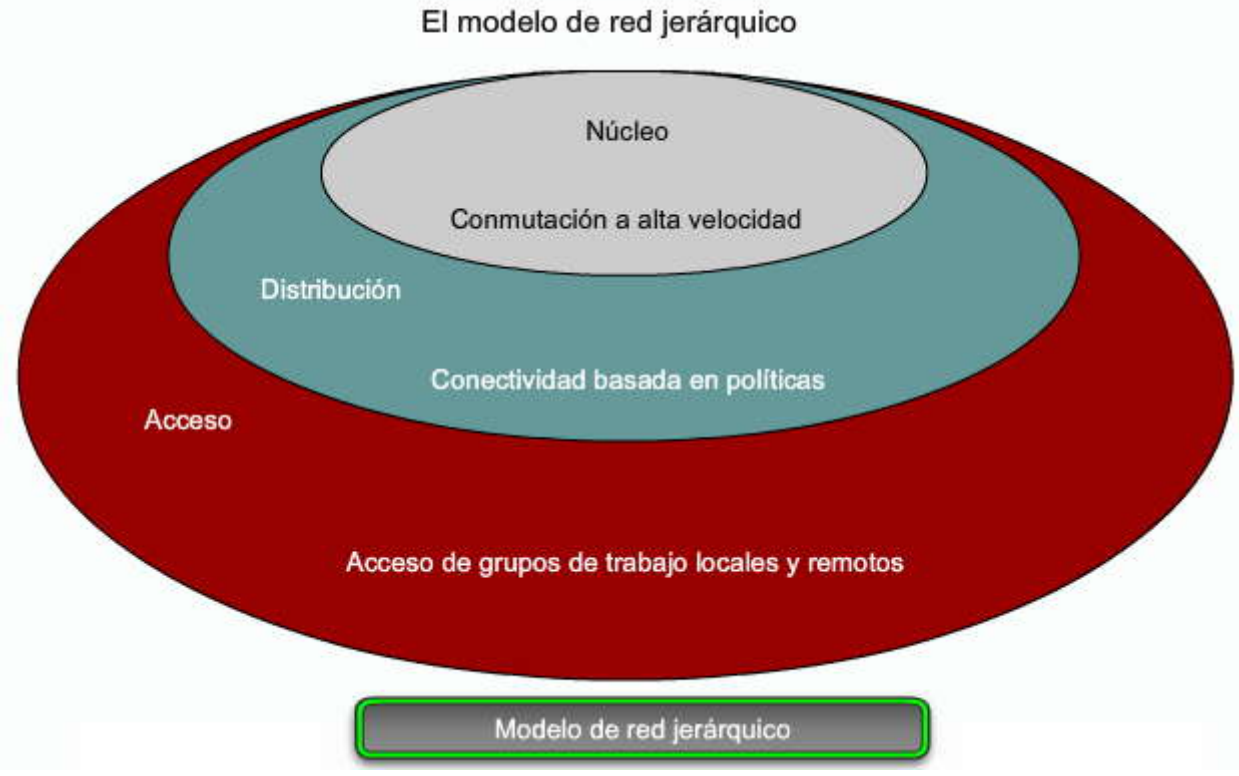
Como tal vez recuerde de CCNA Exploration: conmutación de LAN y redes inalámbricas, el modelo de red jerárquico divide la red en tres capas:

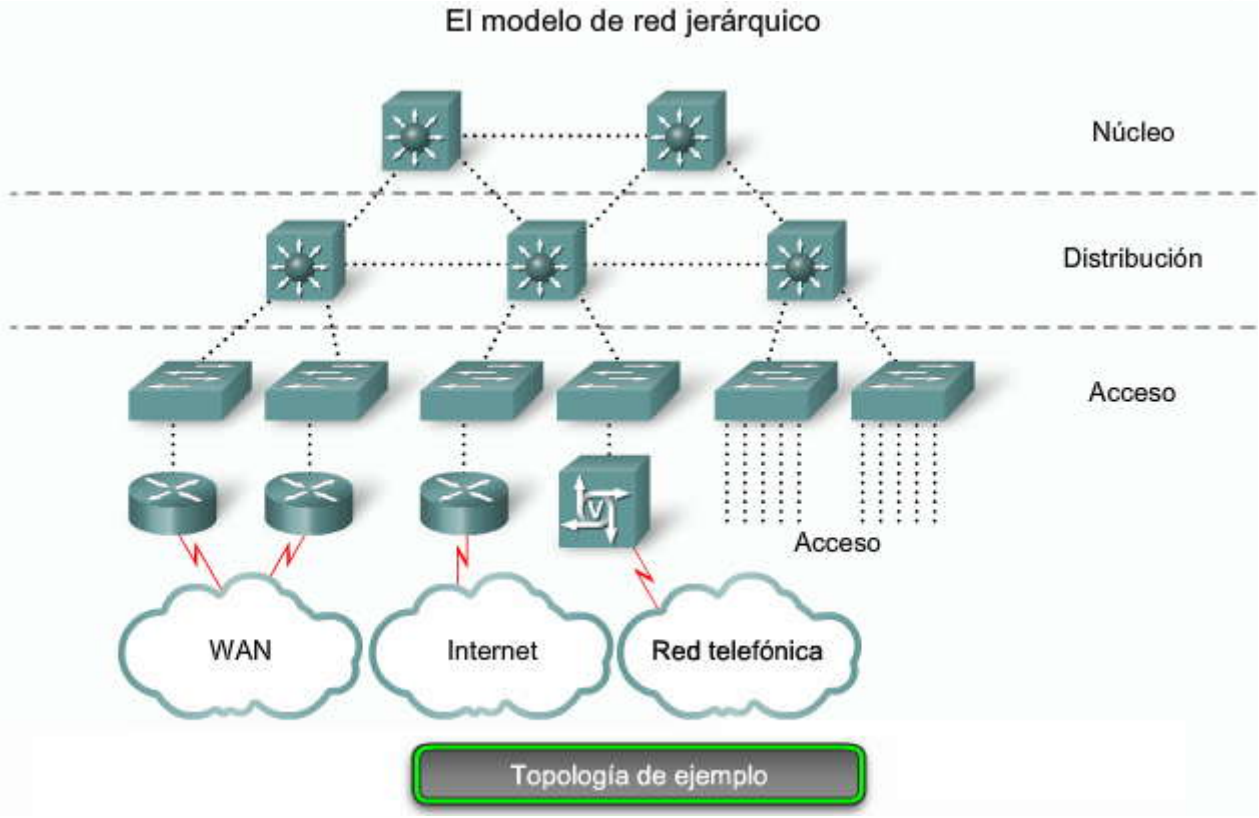
- **Capa de acceso**: permite el acceso de los usuarios a los dispositivos de la red. En una red de campus, la capa de acceso generalmente incorpora dispositivos de conmutación de LAN con puertos que proporcionan conectividad a las estaciones de trabajo y a los servidores. En el entorno de la WAN, puede proporcionar a los trabajadores a distancia o a los sitios remotos acceso a la red corporativa a través de la tecnología WAN.
- **Capa de distribución**: agrupa los armarios de cableado y utiliza switches para segmentar grupos de trabajo y aislar los problemas de la red en un entorno de campus. De manera similar, la capa de distribución agrupa las conexiones WAN en el extremo del campus y proporciona conectividad basada en políticas.
- **Capa núcleo (también conocida como backbone)**: enlace troncal de alta velocidad que está diseñado para conmutar paquetes tan rápido como sea posible. Como el núcleo es fundamental para la conectividad, debe proporcionar un alto nivel de disponibilidad y adaptarse a los cambios con rapidez. También proporciona escalabilidad y convergencia rápida.

Haga clic en el botón Topología de ejemplo en la imagen.

La figura representa el modelo de red jerárquico en entornos de campus. El modelo de red jerárquico proporciona una estructura modular que permite flexibilidad en el diseño de la red y facilita la implementación y la resolución de problemas de la infraestructura. Sin embargo, es importante comprender que la infraestructura de la red es solamente la base de una arquitectura integral.

Las tecnologías de networking han avanzado considerablemente en los últimos años, lo que produjo redes cada vez más inteligentes. Los elementos de red actuales son más sensibles a las características del tráfico y se pueden configurar para proporcionar servicios especializados en función de aspectos como los tipos de datos que transportan, la prioridad de los datos e incluso las necesidades de seguridad. Si bien la mayoría de estos diversos servicios de infraestructura no están incluidos en este curso, es importante comprender que afectan el diseño de la red. En el siguiente tema, analizaremos la Arquitectura empresarial de Cisco, que expande el modelo jerárquico mediante el uso de inteligencia de red para considerar la infraestructura de la red.





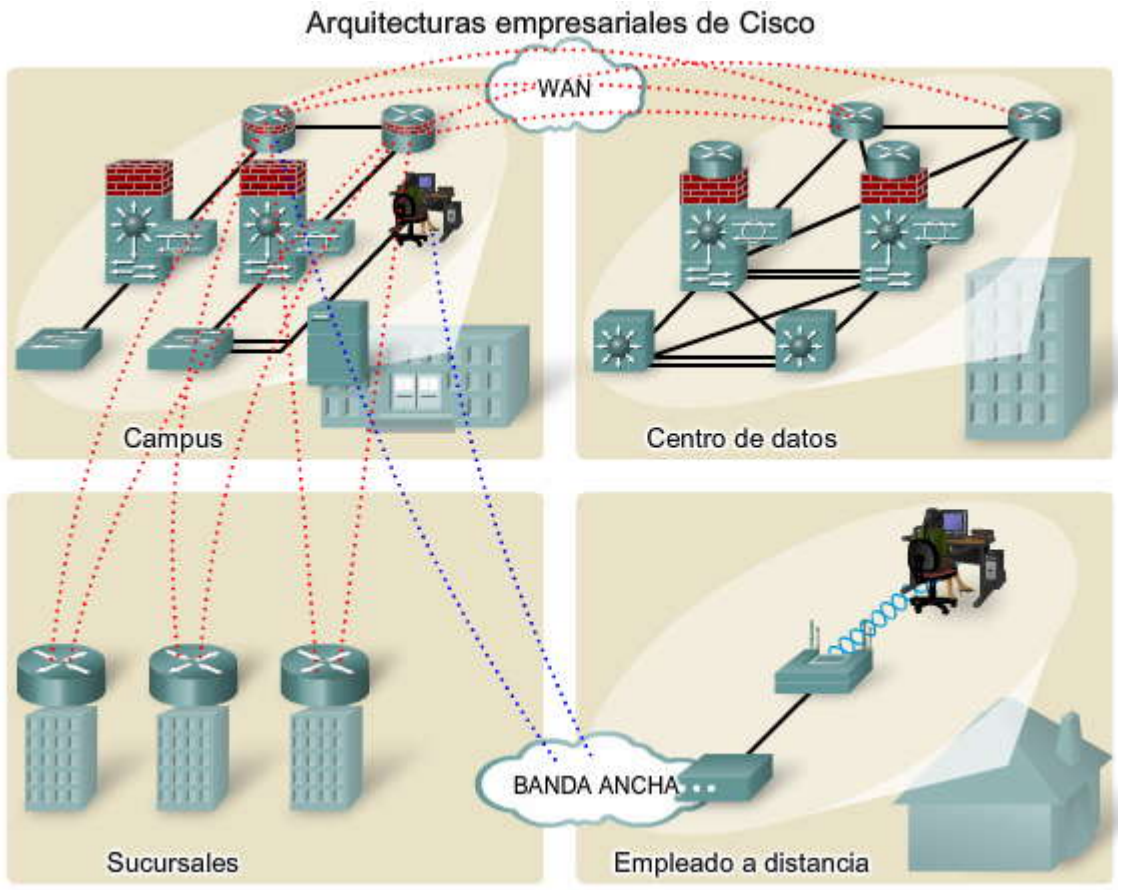
La arquitectura empresarial

Como se describió anteriormente, las diferentes empresas necesitan diferentes tipos de redes, según la manera en la que se organizan la empresa y sus objetivos comerciales. Desafortunadamente, con mucha frecuencia las redes crecen sin ningún tipo de planificación a medida que se agregan componentes en respuesta a necesidades inmediatas. Con el tiempo, esas redes se vuelven complejas y su administración es costosa. Como la red es una mezcla de tecnologías más recientes y antiguas, puede resultar difícil prestar servicios de soporte y mantenimiento de red. Las interrupciones del servicio y su mal rendimiento son una fuente constante de problemas para losadministradores de red.

Para ayudar a evitar esta situación, Cisco ha desarrollado una arquitectura recomendada que se denomina Arquitectura empresarial de Cisco y que tiene trascendencia en las diferentes etapas de crecimiento de una empresa. Esta arquitectura está diseñada para proporcionar a los planificadores de la red una planificación para el crecimiento de la misma, a medida que la empresa avanza por las diferentes etapas. Al seguir la planificación sugerida, los gerentes de TI pueden planificar actualizaciones futuras de la red que se integrarán sin inconvenientes con la red existente y respaldarán la necesidad de servicios que crece de manera constante.

A continuación, se mencionan algunos ejemplos de los módulos de la arquitectura que son relevantes para la situación de Span Engineering descrita anteriormente:

- Arquitectura de campus de la empresa
- Arquitectura de sucursales de la empresa
- Arquitectura del centro de datos de la empresa
- Arquitectura de trabajadores a distancia de la empresa



Módulos de la arquitectura empresarial

La arquitectura empresarial de Cisco está compuesta por módulos que representan vistas específicas que se centran en cada lugar de la red. Cada módulo tiene una infraestructura de red diferente con servicios y aplicaciones de red que se extienden a través de los módulos. La arquitectura empresarial de Cisco incluye los siguientes módulos.

Deslice el puntero sobre cada módulo de la imagen.

Arquitectura de campus de la empresa

Una red de campus es un edificio o un grupo de edificios conectados en una red empresarial que está compuesta por muchas LAN. En general, un campus se limita a un área geográfica fija, pero puede abarcar varios edificios vecinos, como un complejo industrial o parque comercial. En el ejemplo de Span Engineering, el campus abarcaba varios pisos del mismo edificio.

La arquitectura de campus de empresa describe los métodos recomendados para crear una red escalable y a la vez atender las necesidades de las operaciones de las empresas con un estilo de campus. La arquitectura es modular y puede fácilmente expandirse para incluir edificios o pisos adicionales en el campus a medida que la empresa crece.

Arquitectura de extremo empresarial

Este módulo ofrece conectividad para servicios de voz, video y datos fuera de la empresa. Este módulo permite a la empresa utilizar Internet y recursos de socios y proporcionar recursos a sus clientes. Con frecuencia, este módulo funciona como enlace entre el módulo de campus y los demás módulos de la arquitectura empresarial. Las arquitecturas WAN y MAN (Redes de área metropolitana, Metropolitan-Area Networks) empresariales, para las que las tecnologías descritas más adelante en este curso son relevantes, se consideran parte de este módulo.

Arquitectura de sucursal de la empresa

Este módulo permite a las empresas extender las aplicaciones y los servicios encontrados en el campus a miles de ubicaciones y usuarios remotos o a un grupo pequeño de sucursales. Una gran parte de este curso se concentra en las tecnologías que, a menudo, se implementan en este módulo.

Arquitectura de centro de datos de la empresa

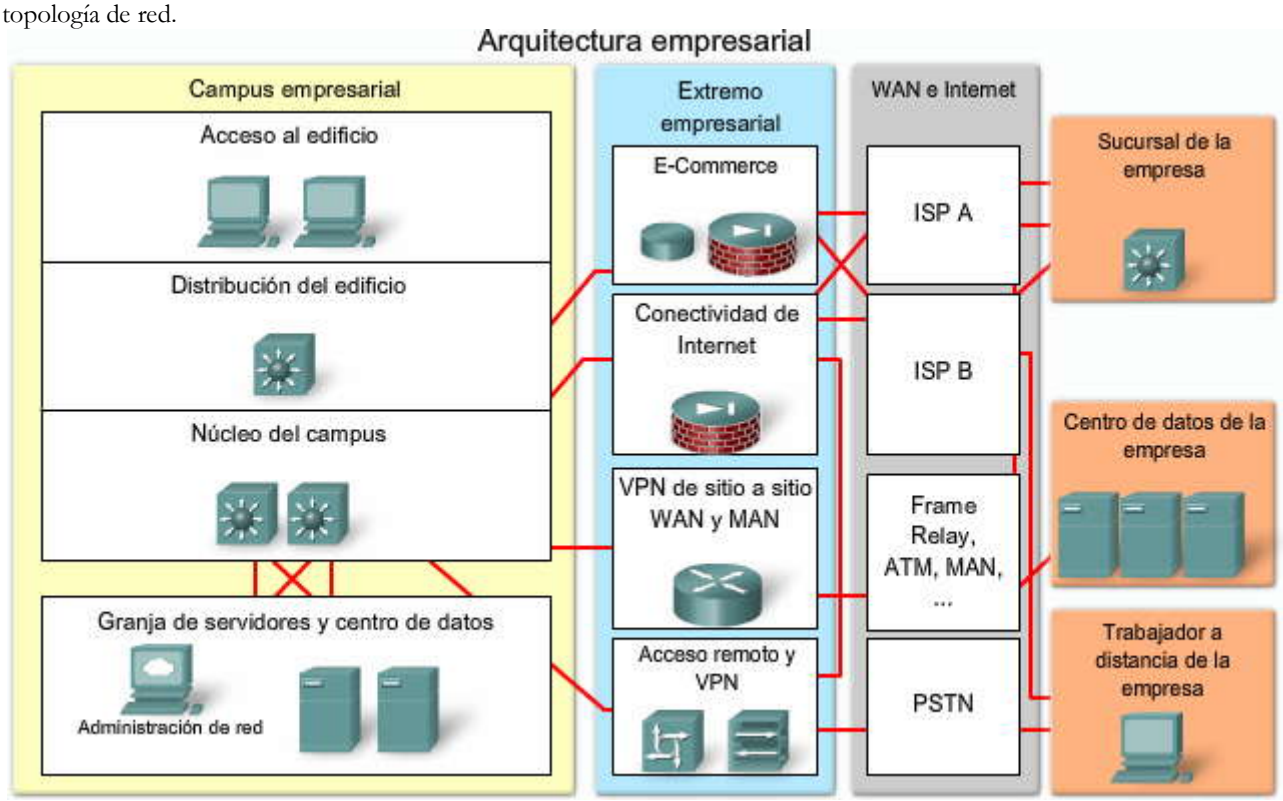
Los centros de datos son responsables de administrar y mantener los numerosos sistemas de datos que son vitales para el funcionamiento de las empresas modernas. Los empleados, los socios y los clientes utilizan los datos y los recursos del centro de datos para crear, colaborar e interactuar de manera eficaz. En la última década, el surgimiento de Internet y las tecnologías basadas en la Web han hecho que los centros de datos sean más importantes que nunca, ya que mejoran la productividad y los procesos comerciales y aceleran el cambio.

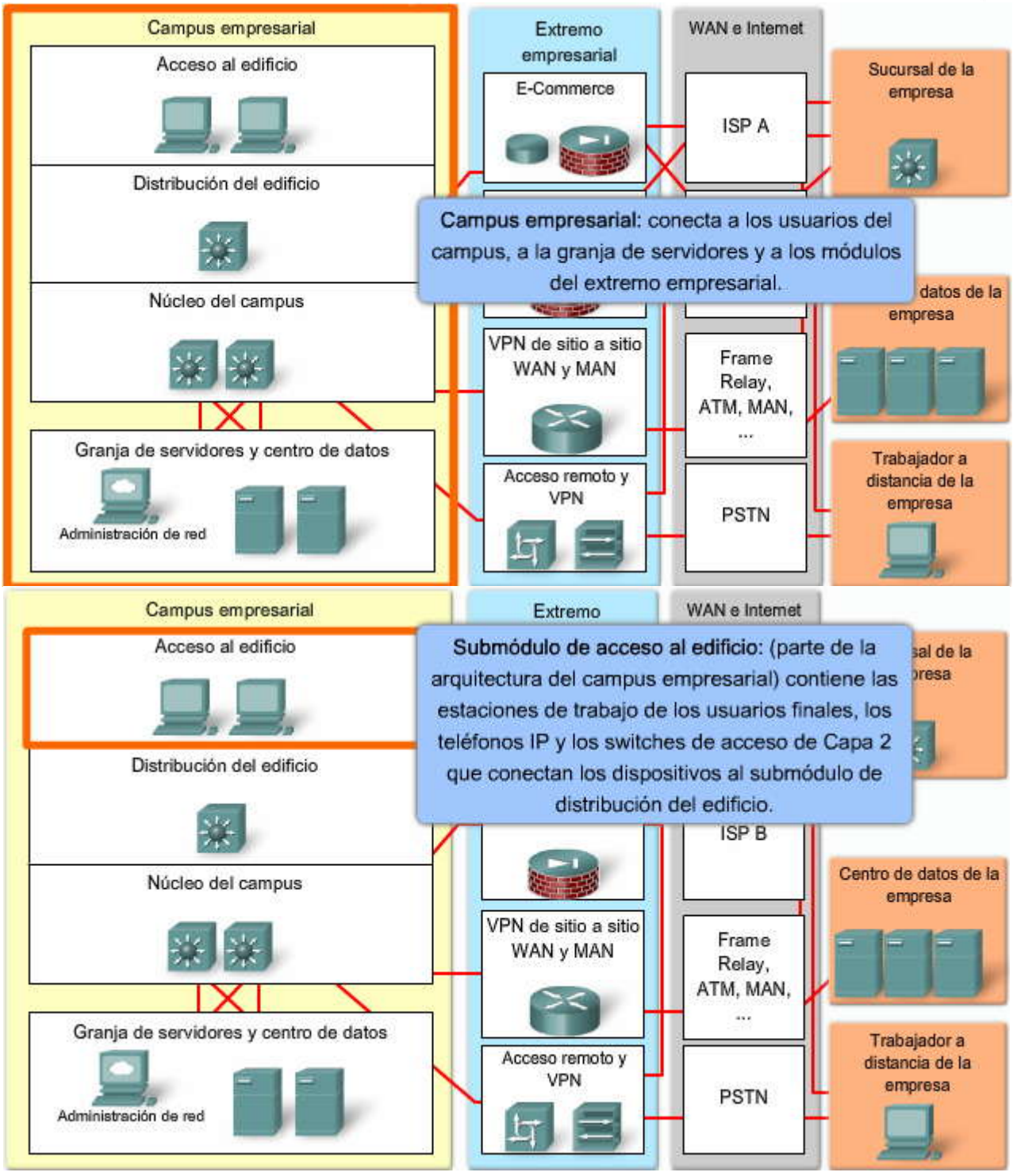
Arquitectura de trabajadores a distancia de la empresa

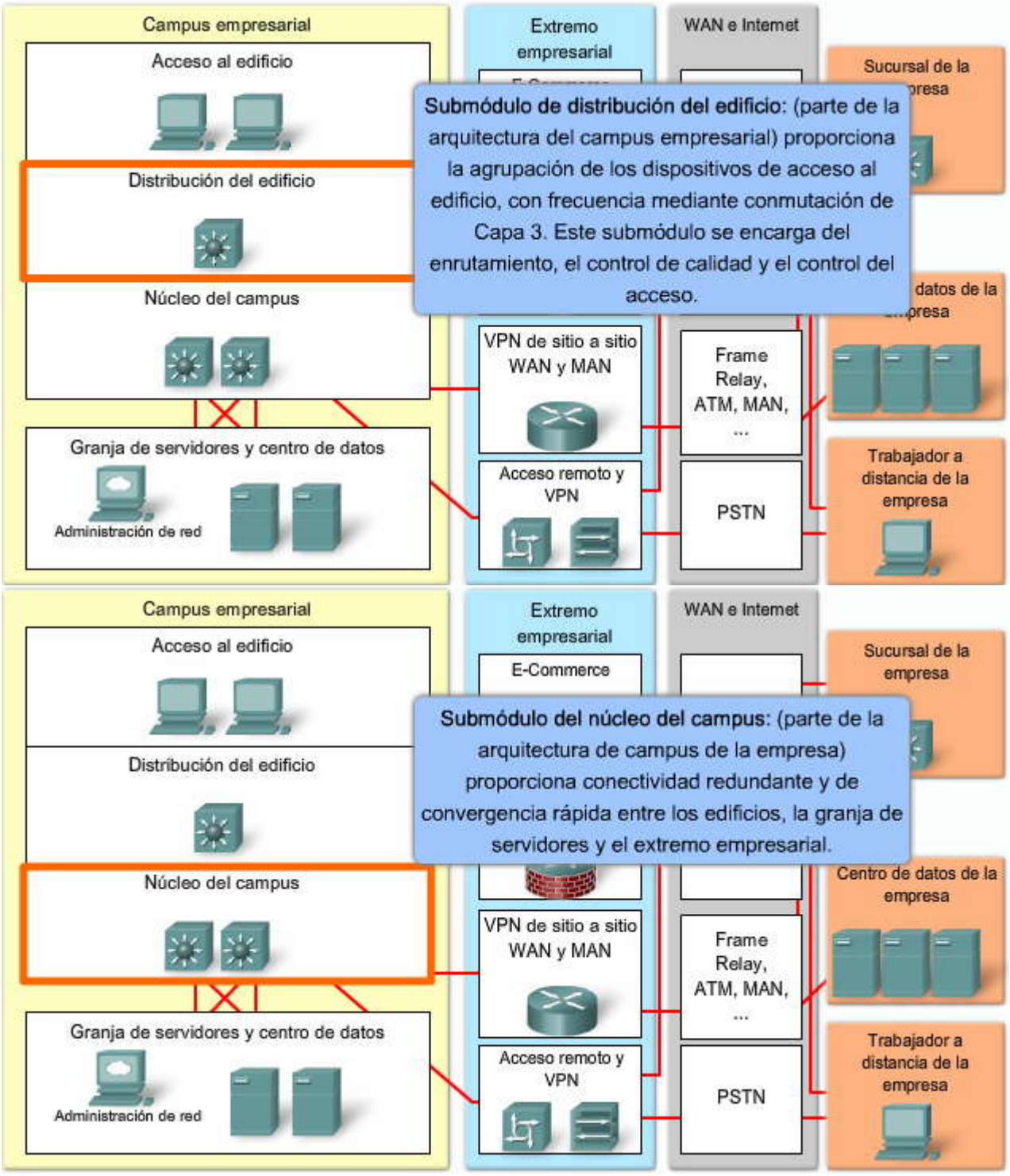
Muchas empresas de la actualidad ofrecen un entorno de trabajo flexible a sus empleados al permitirles trabajar desde sus oficinas en el hogar. Trabajar a distancia es aprovechar los recursos de red de la empresa desde el hogar. El módulo de trabajadores a distancia recomienda que las conexiones desde el hogar utilicen servicios de banda ancha, comomódem por cable o DSL para conectarse a Internet y desde allí a la red corporativa. Como Internet presenta riesgos de seguridad importantes para las empresas, es necesario tomar medidas especiales para garantizar que las comunicaciones de los trabajadores a distancia sean seguras y privadas.

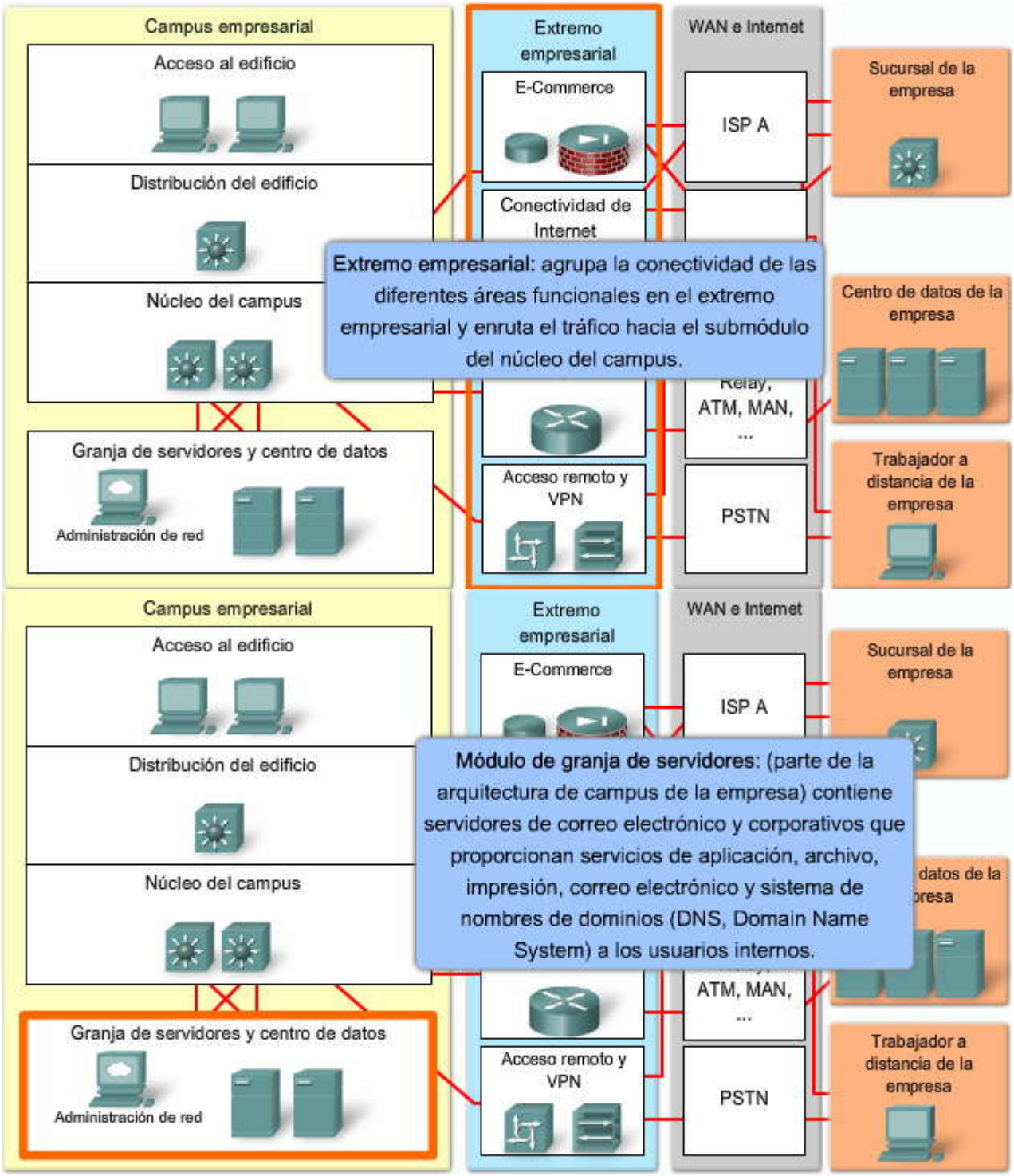
Haga clic en el botón Topología de ejemplo en la imagen.

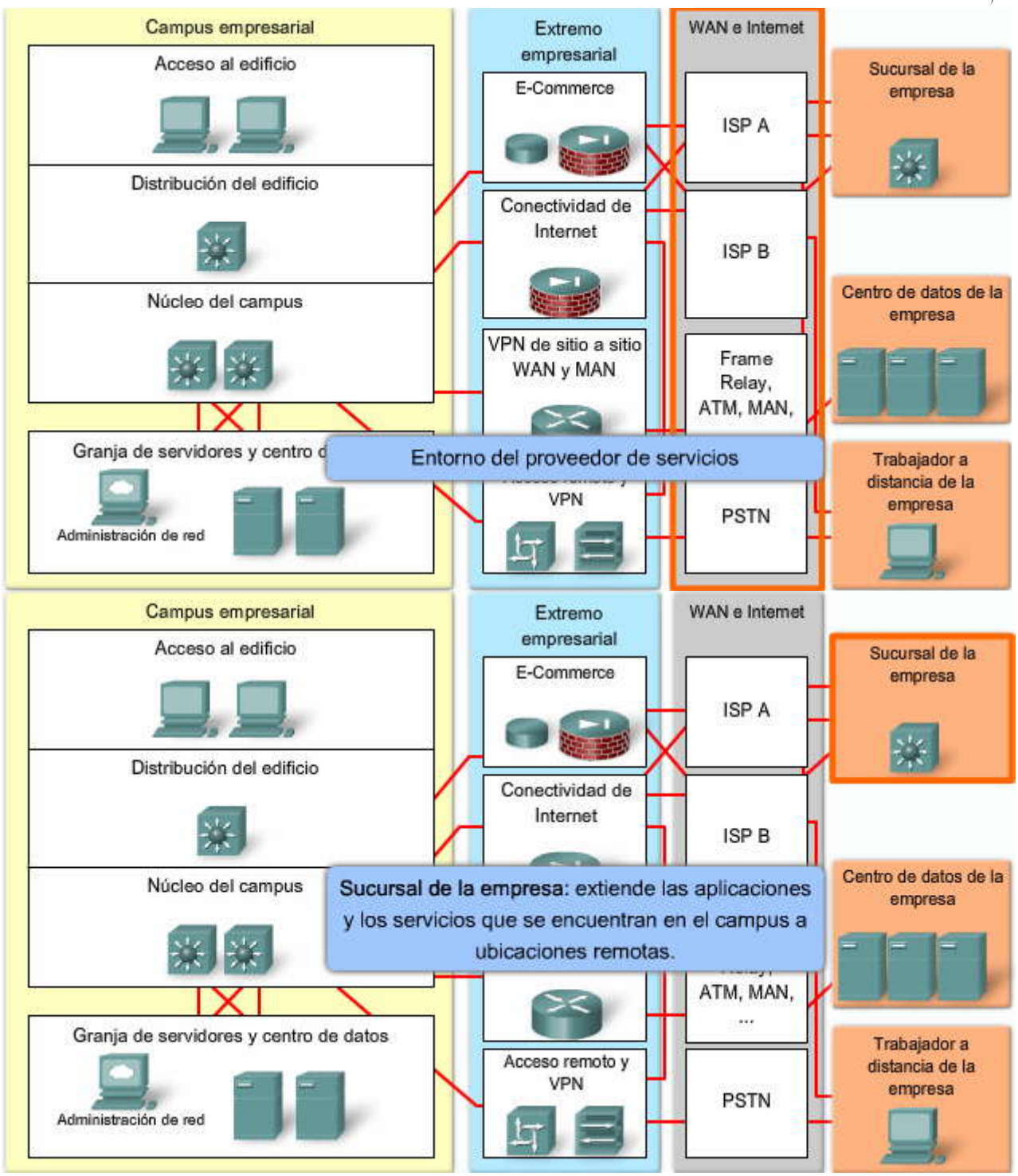
La imagen muestra un ejemplo de cómo se pueden utilizar estos módulos de arquitectura empresarial para construir una topología de red.

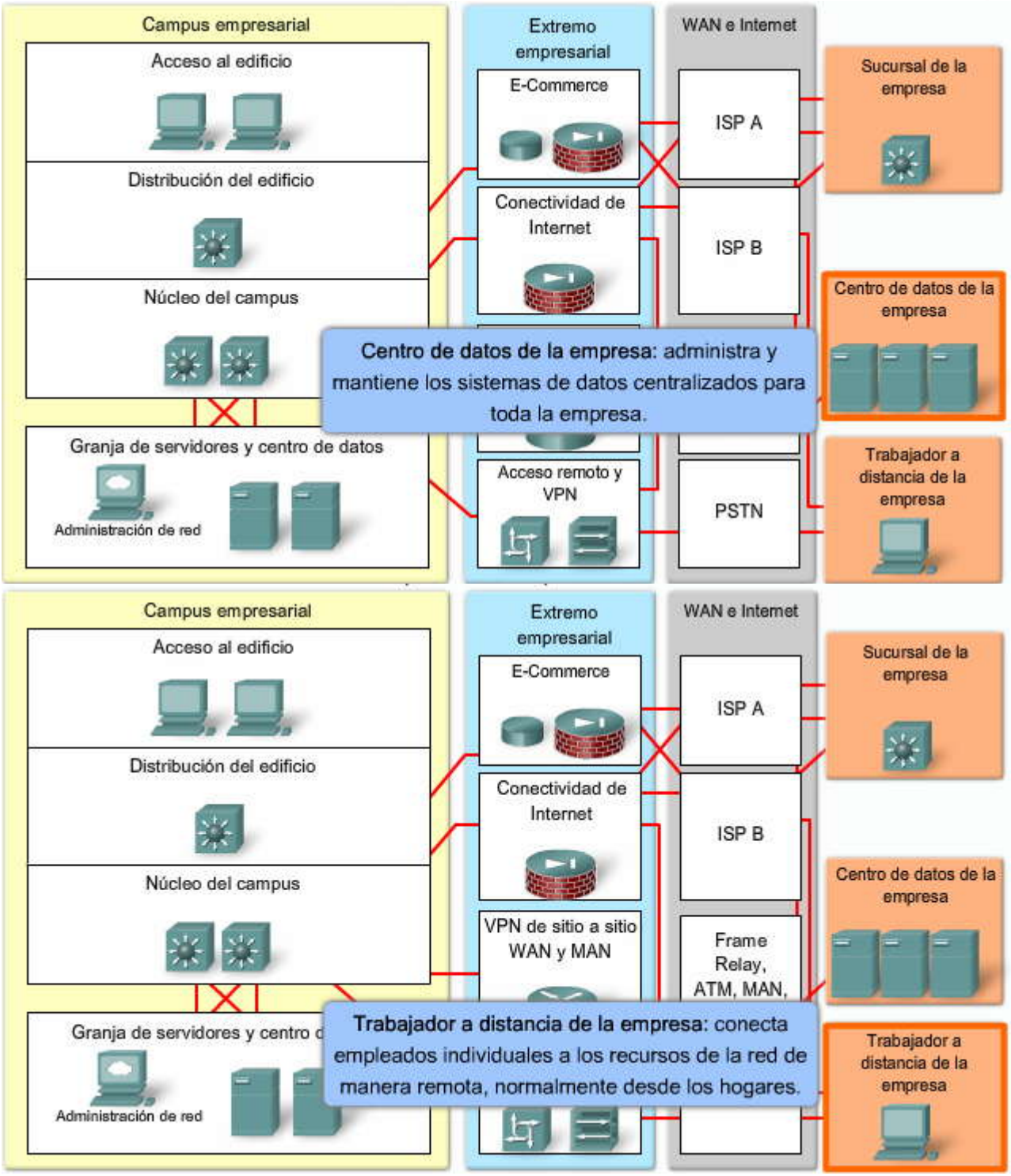


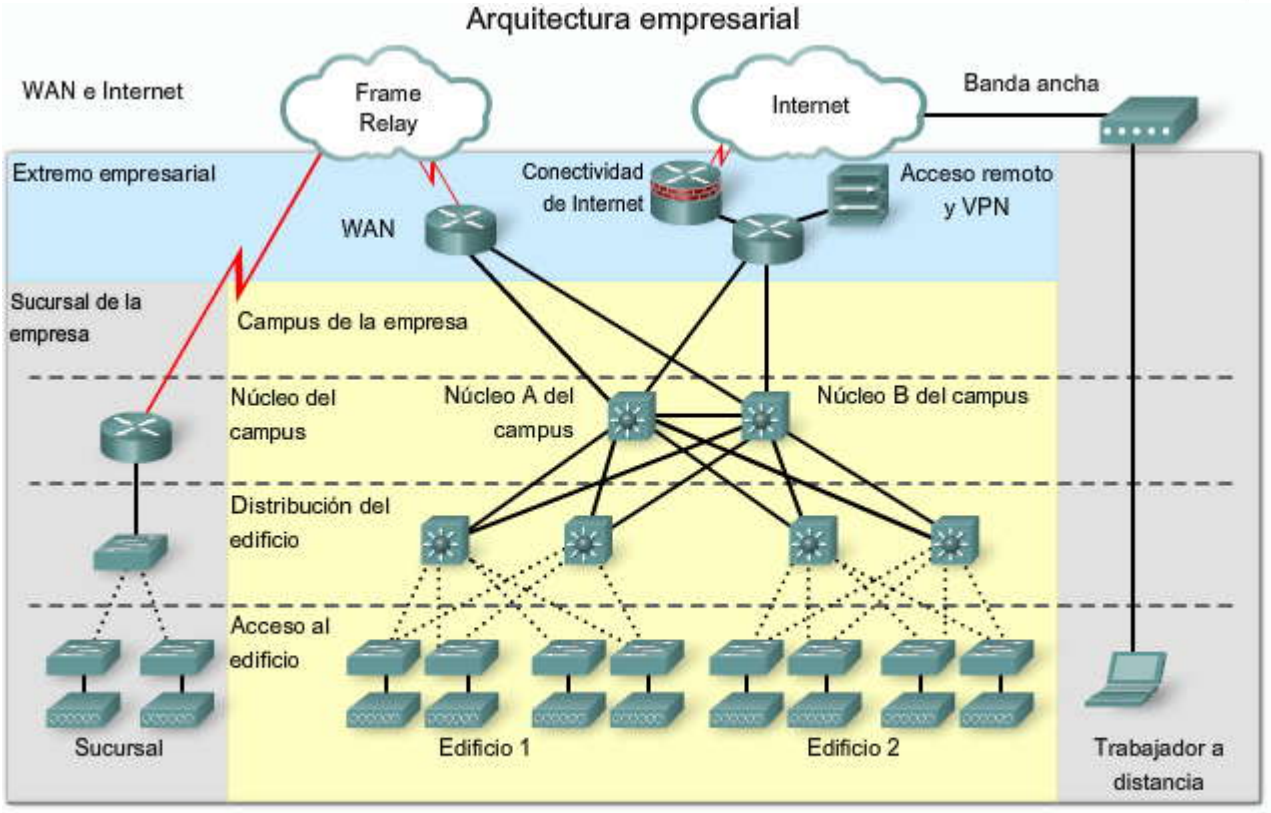

Campus empresarial
Acceso al edificio
Distribución del edificio
Núcleo del campus
Granja de servidores y centro de datos
Administración de red
Extremo empresarial
E-Commerce
VPN de sitio a sitio WAN y MAN
Acceso remoto y VPN
WAN e Internet
ISP A
Frame Relay, ATM, MAN, ...
PSTN
Sucursal de la empresa
datos de la empresa
Trabajador a distancia de la empresa
Campus empresarial: conecta a los usuarios del campus, a la granja de servidores y a los módulos del extremo empresarial.
Campus empresarial
Acceso al edificio
Distribución del edificio
Núcleo del campus
Granja de servidores y centro de datos
Administración de red
Extremo
WAN e Internet
ISP B
VPN de sitio a sitio WAN y MAN
Frame Relay, ATM, MAN, ...
Acceso remoto y VPN
PSTN
Centro de datos de la empresa
Trabajador a distancia de la empresa
Submódulo de acceso al edificio: (parte de la arquitectura del campus empresarial) contiene las estaciones de trabajo de los usuarios finales, los teléfonos IP y los switches de acceso de Capa 2 que conectan los dispositivos al submódulo de distribución del edificio.


Campus empresarial
Acceso al edificio
Distribución del edificio
Núcleo del campus
Granja de servidores y centro de datos
Administración de red
Extremo empresarial
VPN de sitio a sitio WAN y MAN
Acceso remoto y VPN
WAN e Internet
Frame Relay, ATM, MAN, ...
PSTN
Sucursal de la empresa
Trabajador a distancia de la empresa
Submódulo de distribución del edificio: (parte de la arquitectura del campus empresarial) proporciona la agrupación de los dispositivos de acceso al edificio, con frecuencia mediante conmutación de Capa 3. Este submódulo se encarga del enrutamiento, el control de calidad y el control del acceso.
Campus empresarial
Acceso al edificio
Distribución del edificio
Núcleo del campus
Granja de servidores y centro de datos
Administración de red
Extremo empresarial
E-Commerce
VPN de sitio a sitio WAN y MAN
Acceso remoto y VPN
WAN e Internet
Frame Relay, ATM, MAN, ...
PSTN
Sucursal de la empresa
Centro de datos de la empresa
Trabajador a distancia de la empresa
Submódulo del núcleo del campus: (parte de la arquitectura de campus de la empresa) proporciona conectividad redundante y de convergencia rápida entre los edificios, la granja de servidores y el extremo empresarial.

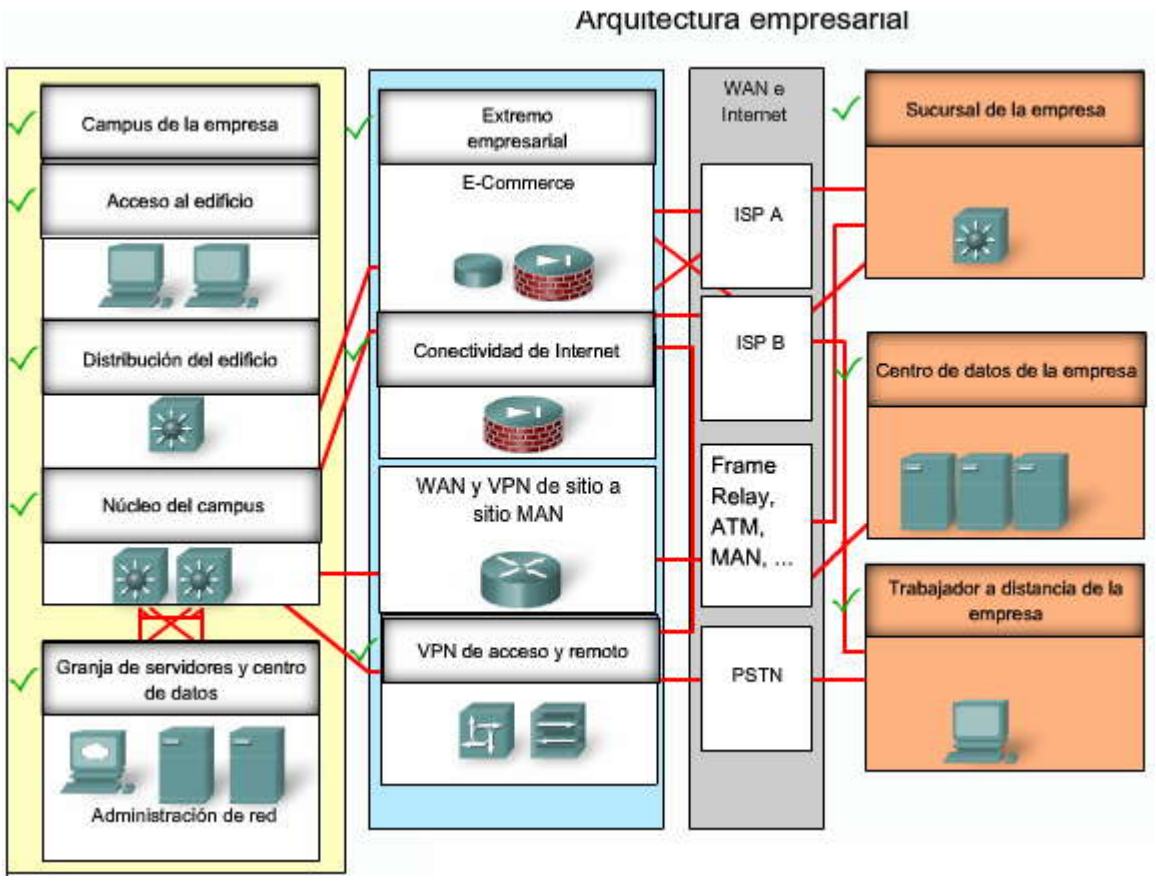

Campus empresarial
Acceso al edificio
Distribución del edificio
Núcleo del campus
Granja de servidores y centro de datos
Administración de red
Extremo empresarial
E-Commerce
Conectividad de Internet
Acceso remoto y VPN
WAN e Internet
ISP A
Relay, ATM, MAN, ...
PSTN
Sucursal de la empresa
Centro de datos de la empresa
Trabajador a distancia de la empresa
Extremo empresarial: agrupa la conectividad de las diferentes áreas funcionales en el extremo empresarial y enruta el tráfico hacia el submódulo del núcleo del campus.
Campus empresarial
Acceso al edificio
Distribución del edificio
Núcleo del campus
Granja de servidores y centro de datos
Administración de red
Extremo empresarial
E-Commerce
Acceso remoto y VPN
WAN e Internet
ISP A
ATM, MAN, ...
PSTN
Sucursal de la empresa
Trabajador a distancia de la empresa
Módulo de granja de servidores: (parte de la arquitectura de campus de la empresa) contiene servidores de correo electrónico y corporativos que proporcionan servicios de aplicación, archivo, impresión, correo electrónico y sistema de nombres de dominios (DNS, Domain Name System) a los usuarios internos.


Campus empresarial
Acceso al edificio
Distribución del edificio
Núcleo del campus
Granja de servidores y centro d
Administración de red
Extremo empresarial
E-Commerce
Conectividad de Internet
VPN de sitio a sitio WAN y MAN
VPN
WAN e Internet
ISP A
ISP B
Frame Relay, ATM, MAN,
PSTN
Sucursal de la empresa
Centro de datos de la empresa
Trabajador a distancia de la empresa
Entorno del proveedor de servicios
Campus empresarial
Acceso al edificio
Distribución del edificio
Núcleo del campus
Granja de servidores y centro de datos
Administración de red
Extremo empresarial
E-Commerce
Conectividad de Internet
Acceso remoto y VPN
WAN e Internet
ISP A
ISP B
ATM, MAN, ...
PSTN
Sucursal de la empresa
Centro de datos de la empresa
Trabajador a distancia de la empresa
Sucursal de la empresa: extiende las aplicaciones y los servicios que se encuentran en el campus a ubicaciones remotas.


Campus empresarial
Acceso al edificio
Distribución del edificio
Núcleo del campus
Granja de servidores y centro de datos
Administración de red
Extremo empresarial
E-Commerce
Conectividad de Internet
Acceso remoto y VPN
WAN e Internet
ISP A
ISP B
PSTN
Sucursal de la empresa
Centro de datos de la empresa
Trabajador a distancia de la empresa
Centro de datos de la empresa: administra y mantiene los sistemas de datos centralizados para toda la empresa.
Campus empresarial
Acceso al edificio
Distribución del edificio
Núcleo del campus
Granja de servidores y centro d
Administración de red
Extremo empresarial
E-Commerce
Conectividad de Internet
VPN de sitio a sitio WAN y MAN
WAN e Internet
ISP A
ISP B
Frame Relay, ATM, MAN,
Sucursal de la empresa
Centro de datos de la empresa
Trabajador a distancia de la empresa
Trabajador a distancia de la empresa: conecta empleados individuales a los recursos de la red de manera remota, normalmente desde los hogares.



Arquitectura empresarial | Topología de ejemplo



1.2 Conceptos de tecnología WAN

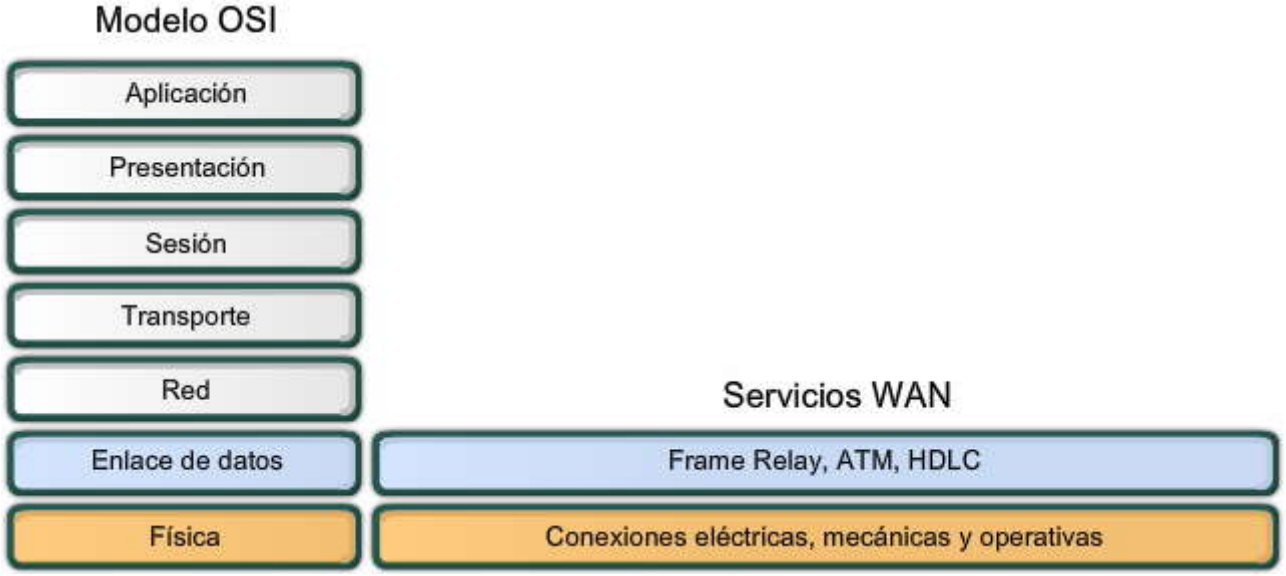
1.2.1 Descripción general de la tecnología WAN

Redes WAN y modelo OSI

Como se describió en relación con el modelo de referencia OSI, las operaciones de una WAN se centran principalmente en las Capas 1 y 2. Los estándares de acceso WAN normalmente describen tanto los métodos de entrega de la capa física como los requisitos de la capa de enlace de datos, incluyendo la dirección física, el control del flujo y la encapsulación. La definición y la administración de los estándares de acceso WAN están a cargo de varias autoridades reconocidas, entre ellas la Organización Internacional de Normalización (OIE), la Asociación de la Industria de las Telecomunicaciones (TIA,Telecommunications Industry Association) y la Asociación de Industrias Electrónicas (EIA, Electronic Industries Alliance).

Los protocolos de capa física (capa 1 del modelo OSI) describen cómo proporcionar las conexiones eléctricas, mecánicas, operativas y funcionales a los servicios brindados por un proveedor de servicios de comunicaciones.

Los protocolos de la capa de enlace de datos (Capa 2 del modelo OSI) definen cómo se encapsulan los datos para su transmisión a lugares remotos y los mecanismos de transferencia de las tramas resultantes. Se utiliza una variedad de tecnologías diferentes, como Frame Relay y ATM. Algunos de estos protocolos utilizan los mismos mecanismos básicos de entramado, control de enlace de datos de alto nivel (HDLC, High-Level Data Link Control), una norma ISO o uno de sus subgrupos o variantes



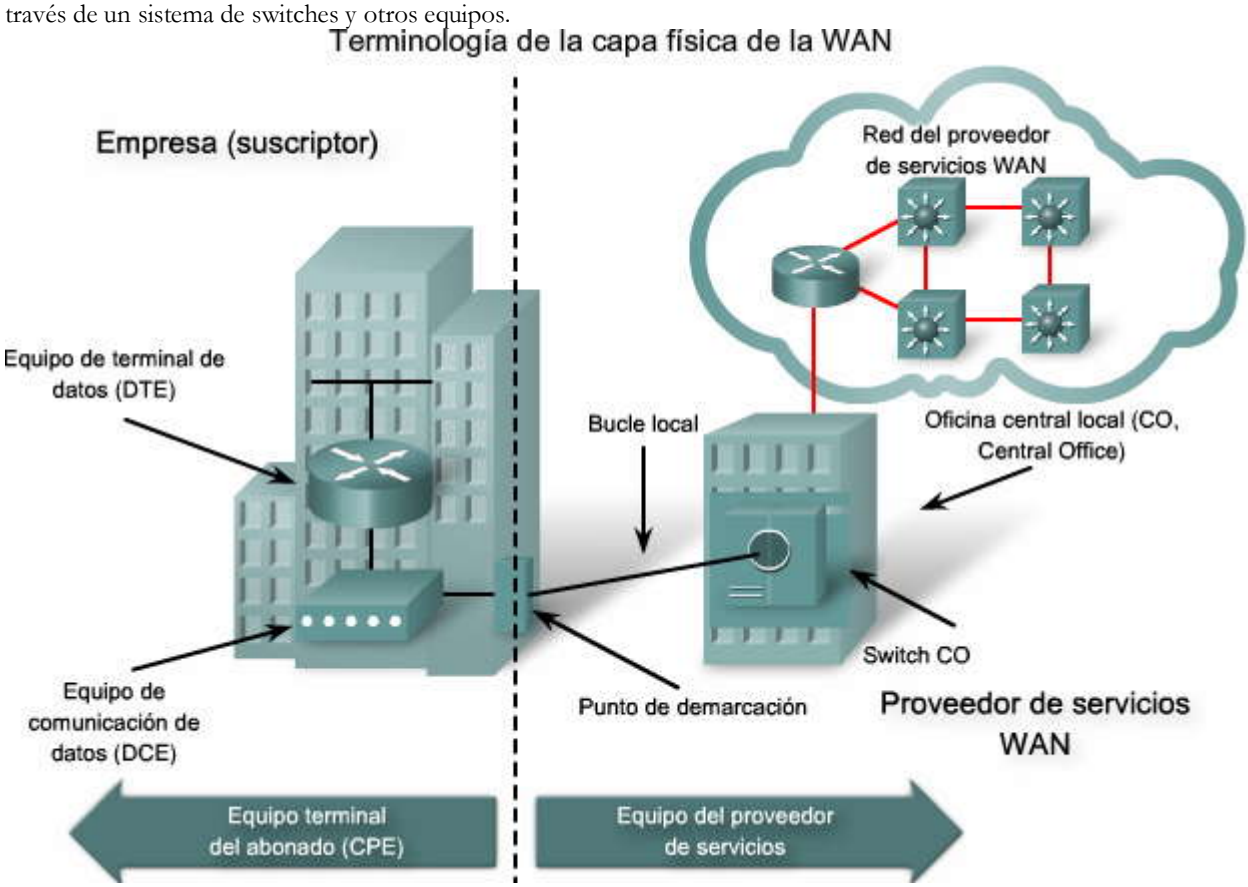
1.2.2 Conceptos de capa física de la WAN

Terminología de la capa física de la WAN

Una de las diferencias primordiales entre una WAN y una LAN es que una empresa u organización debe suscribirse a un proveedor de servicio WAN externo para utilizar los servicios de red de una portadora WAN. Una WAN utiliza enlaces de datos suministrados por los servicios de una operadora para acceder a Internet y conectar los sitios de una organización entre sí, con sitios de otras organizaciones, con servicios externos y con usuarios remotos. La capa física de acceso a la WAN describe la conexión física entre la red de la empresa y la red del proveedor de servicios. La imagen muestra la terminología utilizada comúnmente para describir las conexiones físicas de la WAN, por ejemplo:

- **Equipo local del cliente (CPE, Customer Premises Equipment)**: dispositivos y cableado interno localizados en las instalaciones del suscriptor y conectados con un canal de telecomunicaciones de una portadora. El suscriptor es dueño de un CPE o le alquila un CPE al proveedor de servicios. En este contexto, un suscriptor es una empresa que contrata los servicios WAN de un proveedor de servicios u operadora.
- **Equipo de comunicación de datos (DCE, Data Communications Equipment)**: también llamado equipo de terminación de circuito de datos, el DCE está compuesto por dispositivos que ponen datos en el bucle local. La tarea principal del DCE es suministrar una interfaz para conectar suscriptores a un enlace de comunicación en la nube WAN.
- **Equipo terminal de datos (DTE, Data Terminal Equipment)**: dispositivos del cliente que pasan los datos de la red o la computadora host de un cliente para transmisión a través de la WAN. El DTE se conecta al bucle local a través del DCE.

- **Punto de demarcación**: punto establecido en un edificio o un complejo para separar los equipos del cliente de los equipos del proveedor de servicios. Físicamente, el punto de demarcación es la caja de empalme del cableado que se encuentra en las instalaciones del cliente y que conecta los cables del CPE con el bude local. Normalmente se coloca en un lugar de fácil acceso para los técnicos. El punto de demarcación es el lugar donde la responsabilidad de la conexión pasa del usuario al proveedor de servicios. Esto es muy importante porque cuando surgen problemas, esnecesario determinar si la resolución o la reparación son responsabilidad del usuario o del proveedor de servicios.
- **Bucle local**: Cable telefónico de cobre o fibra que conecta el CPE del sitio del suscriptor a la CO del proveedor de servicios. El bucle local a veces se denomina "última milla".
- **Oficina central (CO, Central Office)**: instalaciones o edificio del proveedor de servicios local en donde los cables telefónicos se enlazan con las líneas de comunicación de fibra óptica de largo alcance y completamente digitales a través de un sistema de switches y otros equipos.

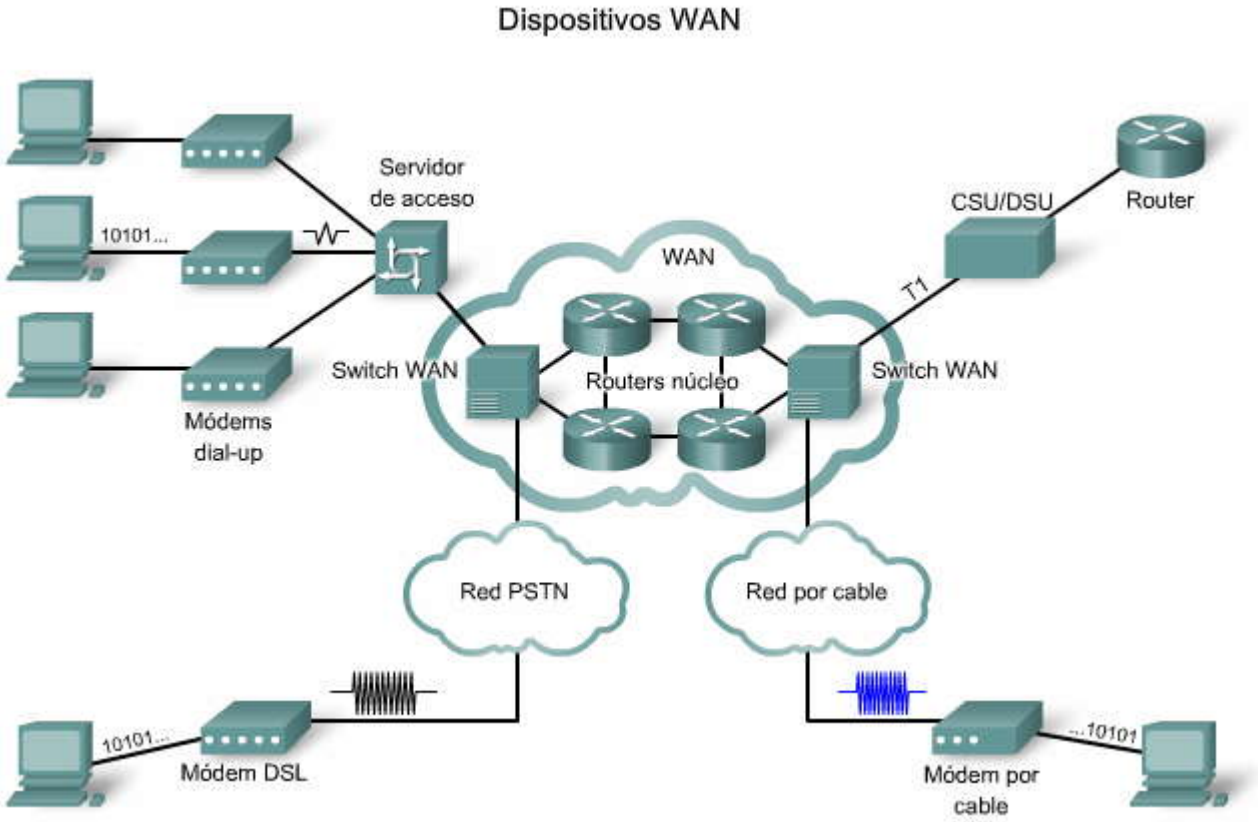


Dispositivos WAN

Las WAN utilizan numerosos tipos de dispositivos que son específicos para los entornos WAN, entre ellos:

- **Módem**: modula una señal portadora analógica para codificar información digital y demodula la señal portadora para decodificar la información transmitida. Un módem de banda de voz convierte las señales digitales producidas por una computadora en frecuencias de voz que se pueden transmitir a través de las líneas analógicas de la red de telefonía pública. En el otro extremo de la conexión, otro módem vuelve a convertir los sonidos en unaseñal digital para que ingrese a una computadora o a una conexión de red. Los módems más rápidos, por ejemplo los módems por cable y los módems DSL, transmiten mediante el uso de frecuencias de banda ancha mayores.
- **CSU/DSU**: las líneas digitales, por ejemplo las líneas portadoras T1 o T3, necesitan una unidad de servicio de canal (CSU, channel service unit) y una unidad de servicio de datos (DSU, data service unit). Con frecuencia, las dos se encuentran combinadas en una sola pieza del equipo, llamada CSU/DSU. La CSU proporciona la terminación para la señal digital y garantiza la integridad de la conexión mediante la corrección de errores y la supervisión de la línea. La DSU convierte las tramas de la línea Portadora T en tramas que la LAN puede interpretar y viceversa.
- **Servidor de acceso**: concentra las comunicaciones de usuarios de servicios de acceso con marcación. Un servidor de acceso puede tener una mezcla de interfaces analógicas y digitales y admitir a cientos de usuarios al mismo tiempo.
- **Switch WAN**: dispositivo de internetworking de varios puertos que se utiliza en redes portadoras. Estos dispositivos normalmente conmutan el tráfico, por ejemplo Frame Relay, ATM oX.25, y operan en la capa de enlace de datos del modelo de referencia OSI. Dentro de la nube también es posible utilizar switches de red pública de telefonía conmutada (PSTN, Public Switched Telephone Network) para conexiones de conmutación de circuitos, por ejemplored digital de servicios integrados (ISDN, Integrated Services Digital Network) o conexión telefónica analógica.

- **Router**: proporciona puertos de interfaz de internetworking y acceso WAN que se utilizan para conectarse con la red del proveedor de servicios. Estas interfaces pueden ser conexiones seriales u otras interfaces WAN. En algunos tipos de interfaces WAN se necesita un dispositivo externo, como una CSU/DSU o un módem (analógico, por cable o DSL) para conectar el router al punto de presencia (POP, point of presence) local del proveedor de servicios.
- **Router núcleo**: router que reside en el centro o backbone de la WAN y no en la periferia. Para cumplir con esta función, el router debe soportar varias interfaces de telecomunicaciones de la mayor velocidad que se utilice en el núcleo de la WAN y debe poder reenviar los paquetes IP a la velocidad máxima por todas esas interfaces. El router también debe admitir los protocolos de enrutamiento que se utilizan en el núcleo.



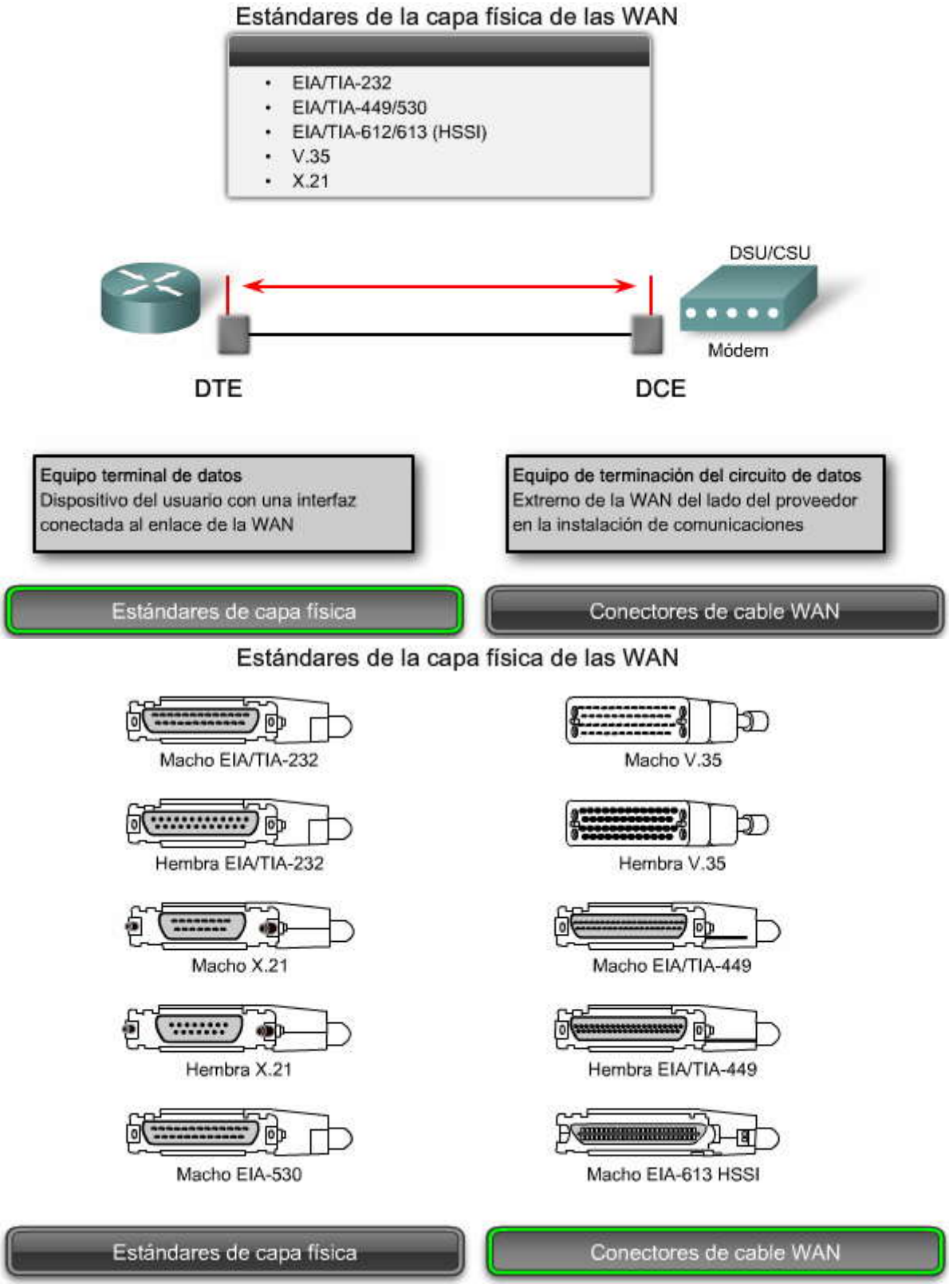
Estándares de la capa física de una WAN

Los protocolos de la capa física de las WAN describen cómo proporcionar conexiones eléctricas, mecánicas, operativas y funcionales para los servicios WAN. La capa física de la WAN también describe la interfaz entre el DTE y el DCE. La interfaz DTE/DCE utiliza diversos protocolos de capa física, entre ellos:

- **EIA/TIA-232**: este protocolo permite velocidades de señal de hasta 64 Kbps en un conector D de 25 pins en distancias cortas. Antiguamente denominado RS-232. La especificación ITU-T V.24 es en efecto lo mismo.
- **EIA/TIA-449/530**: este protocolo es una versión más rápida (hasta 2 Mbps) del EIA/TIA-232. Utiliza un conector D de 36 pins y admite cables más largos. Existen varias versiones. Este estándar también se conoce como RS-422 y RS-423.
- **EIA/TIA-612/613**: este estándar describe el protocolo de interfaz serial de alta velocidad (HSSI, High-Speed Serial Interface), que brinda acceso a servicios de hasta 52 Mbps en un conector D de 60 pins.
- **V.35**: este es el estándar de ITU-T para comunicaciones síncronas entre un dispositivo de acceso a la red y una red de paquetes. Originalmente especificado para soportar velocidades de datos de 48 kbps, en la actualidad soporta velocidades de hasta 2.048 Mbps con un conector rectangular de 34 pins.
- **X.21**: este protocolo es un estándar de UIT-T para comunicaciones digitales síncronas. Utiliza un conector D de 15 pins.

Estos protocolos establecen los códigos y parámetros eléctricos que los dispositivos utilizan para comunicarse entre sí. La selección del protocolo está determinada en mayor medida por el método de comunicación del proveedor de servicios.

Haga clic en el botón Conectores de cable WAN de la imagen para ver los tipos de conectores de cable relacionados con cada protocolo de la capa física.



1.2.3 Conceptos de la capa de enlace de datos de la WAN

Protocolos de enlace de datos

Además de los dispositivos de la capa física, las WAN necesitan protocolos de la capa de enlace de datos para establecer el vínculo a través de la línea de comunicación, desde el dispositivo emisor hasta el dispositivo receptor. Este tema describe los protocolos comunes de enlace de datos que se utilizan en las redes empresariales de la actualidad para implementar conexiones WAN.

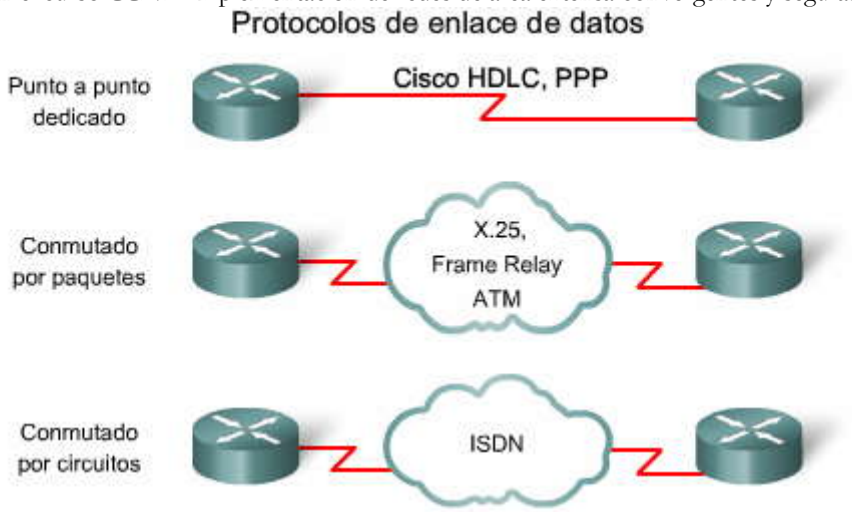
Los protocolos de la capa de enlace de datos definen cómo se encapsulan los datos para su transmisión a lugares remotos, así como también los mecanismos de transferencia de las tramas resultantes. Se utiliza una variedad de tecnologías diferentes, como ISDN, Frame Relay o ATM. Muchos de estos protocolos utilizan los mismos mecanismos básicos de entramado, HDLC, un estándar ISO o uno de sus subgrupos o variantes. ATM se diferencia de los demás porque utiliza celdas pequeñas de un tamaño fijo de 53 bytes (48 bytes para datos), mientras que las demás tecnologías de conmutación de paquetes utilizan paquetes de tamaño variable.

Los protocolos de enlace de datos WAN más comunes son:

- HDLC
- PPP
- Frame Relay
- ATM

ISDN y X.25 son protocolos de enlace de datos más antiguos que en la actualidad se utilizan con menor frecuencia. Sin embargo, ISDN se sigue incluyendo en este curso porque se utiliza para proporcionar redes VoIP con enlaces PRI. X.25 se menciona para ayudar a explicar la importancia de Frame Relay. Además, X.25 se sigue utilizando en los países en vías de desarrollo, donde se usan redes de datos de paquetes (PDN, packet data network) para transmitir transacciones de tarjetas de crédito y tarjetas de débito de tiendas minoristas.

Nota: Otro protocolo de capa de enlace de datos es el protocolo de conmutación de etiquetas multiprotocolos (MPLS, Multiprotocol Label Switching). Los proveedores de servicios están implementando MPLS con mayor frecuencia para proporcionar una solución económica para transportar tráfico de redes de conmutación de circuitos y de conmutación por paquetes. Puede operar a través de cualquier infraestructura existente, por ejemplo IP, Frame Relay, ATM o Ethernet. Se sitúa entre la Capa 2 y la Capa 3 y, a veces, se denomina protocolo de Capa 2.5. Sin embargo, MPLS no está incluido en este curso. Se describe en el curso CCNP: Implementación de redes de área extensa convergentes y seguras.



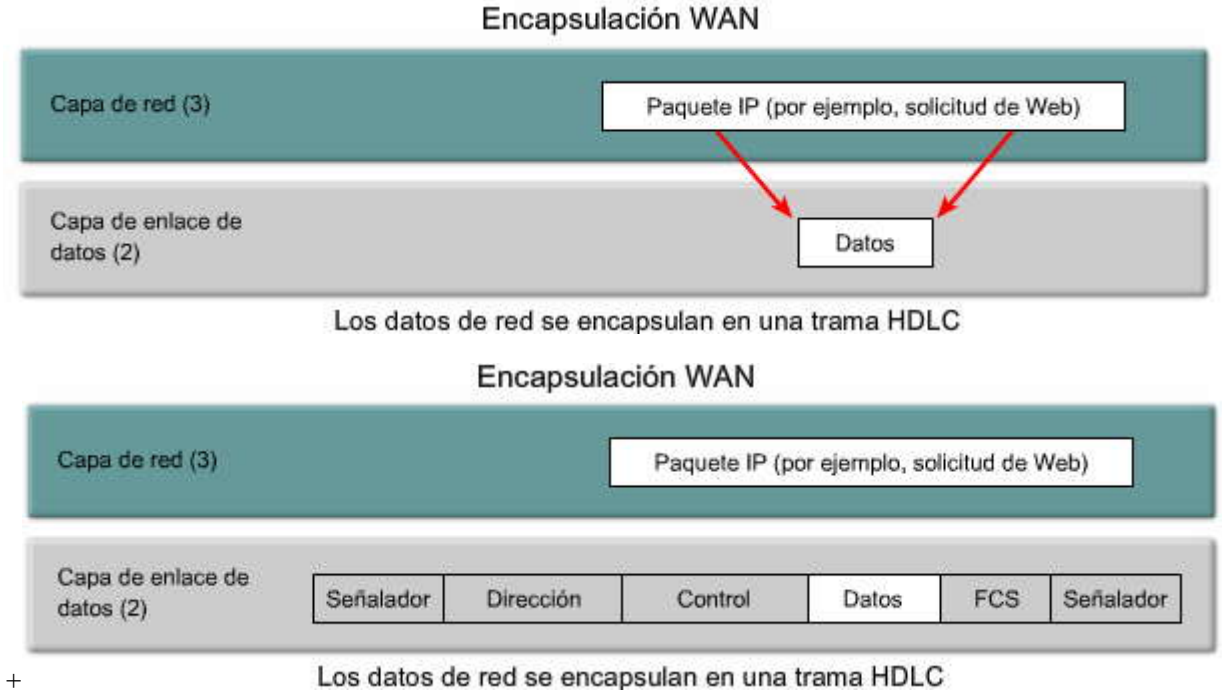
Protocolo	Uso
Procedimiento de acceso al enlace balanceado (LAPB)	X.25
Procedimiento de acceso al enlace en el canal D (LAPD)	Canal D RDSI
Trama de procedimiento de acceso al enlace (LAPF)	Frame Relay
Control de enlace de datos de alto nivel (HDLC)	Valor predeterminado de Cisco
Protocolo punto a punto (PPP)	Conexiones conmutadas WAN seriales

Encapsulación WAN

Los datos de la capa de red se envían a la capa de enlace de datos para ser transmitidos a través de un enlace físico que normalmente es de punto a punto sobre una conexión WAN. La capa de enlace de datos crea una trama alrededor de los datos de la capa de red, de modo que se apliquen los controles y verificaciones necesarias. Cada tipo de conexión WAN utiliza un protocolo de Capa 2 para encapsular un paquete mientras atraviesa el enlace WAN. Para asegurarse de que se esté

utilizando el protocolo de encapsulación correcto, se debe configurar el tipo de encapsulación de Capa 2 utilizado en cada interfaz serial del router. El protocolo de encapsulación que se debe usar depende de la tecnología WAN y del equipo. HDLC fue propuesto en 1979 y, por este motivo, la mayoría de los protocolos de entramado que se desarrollaron después se basan en él.

Haga clic en el botón Reproducir de la imagen para ver cómo encapsulan el tráfico los protocolos de enlace de datos WAN.

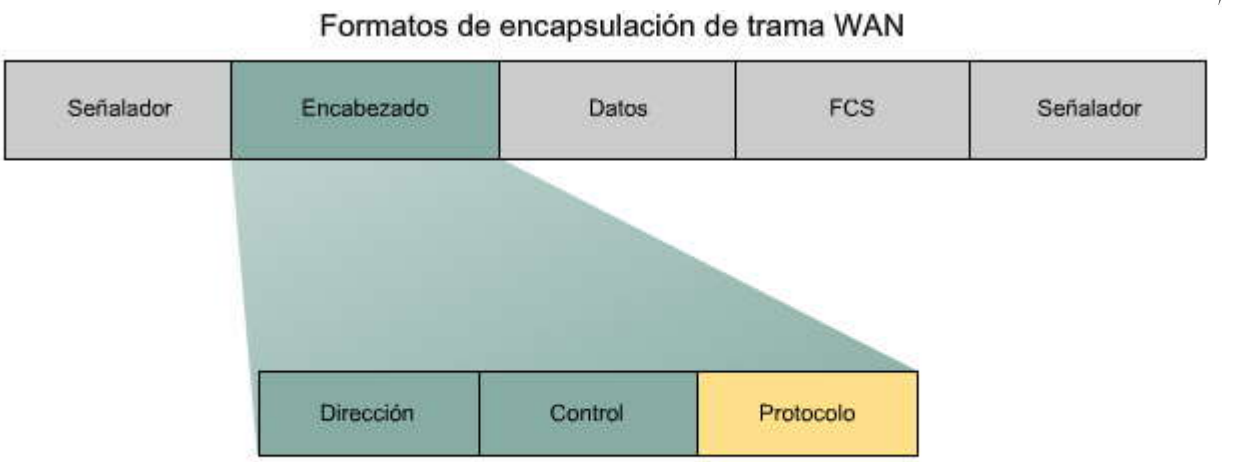


Formatos de encapsulación de tramas WAN

Al examinar la porción del encabezado de una trama HDLC, se pueden identificar campos comunes que utilizan muchos protocolos de encapsulación WAN. La trama siempre comienza y termina con un campo de señaladores de 8bits. El patrón de los bits es 01111110. El campo de la dirección no se necesita para enlaces WAN, que casi siempre son punto a punto. Aún así, el campo de la dirección está presente y puede ocupar 1 o 2 bits. El campo de control depende del protocolo, pero normalmente indica si el contenido de los datos es información de control o si se trata de datos de la capa de red. El campo de control normalmente ocupa 1 byte.

Juntos, los campos de control y la dirección se denominan encabezado de la trama. El dato encapsulado sigue el campo de control. Entonces, una secuencia de verificación de trama (FCS, frame check sequence) utiliza el mecanismo de comprobación de redundancia cíclica (CRC, cyclic redundancy check) para establecer un campo de 2 o 4 bytes.

Se utilizan varios protocolos de enlace de datos, incluidos subgrupos y versiones propietarias de HDLC. Tanto PPP como la versión de Cisco de HDLC tienen un campo adicional en el encabezado para identificar el protocolo de capa de red de los datos encapsulados.



Generalmente, el campo de la dirección de un encabezado de WAN es una dirección broadcast en un enlace punto a punto. El campo de control identifica la porción de los datos como información o control. El campo del protocolo identifica el protocolo de Capa 3 que se va a utilizar (por ejemplo: IP, IPX).

1.2.4 Conceptos de conmutación WAN

Conmutación de circuitos

Las redes de conmutación de circuitos son las que establecen un circuito (o canal) dedicado entre los nodos y las terminales antes de que los usuarios puedan comunicarse.

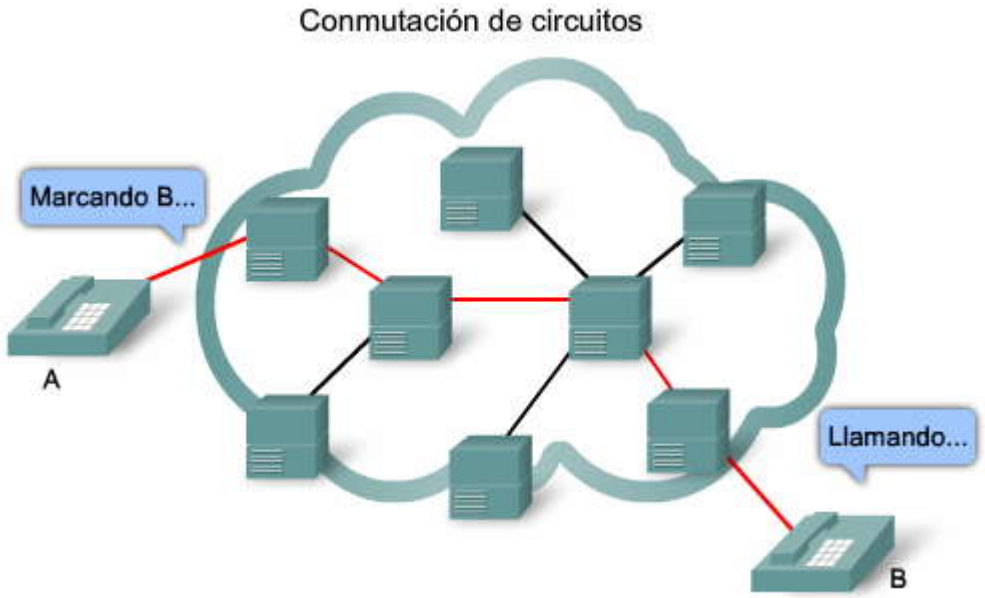
Por ejemplo, cuando un suscriptor realiza una llamada telefónica, el número marcado se utiliza para realizar conmutaciones en los puntos de intercambio a lo largo de la ruta de la llamada, de modo que haya un circuito continuo entre quien hace la llamada y quien la recibe. Debido a la operación de conmutación usada para establecer el circuito, el sistema telefónico se conoce como red conmutada por circuito. Si los módems reemplazan a los teléfonos, entonces el circuito conmutado puede transportar datos de computadora.

Varias conversaciones comparten la ruta interna que sigue el circuito entre los intercambios. La multiplexación por división temporal (TDM, Time Division Multiplexing) asigna a cada conversación una parte de la conexión por turno. TDM garantiza que una conexión de capacidad fija esté disponible para el suscriptor.

Si el circuito transporta datos de computadora, es posible que el uso de esta capacidad fija no sea eficiente. Por ejemplo, si se utiliza el circuito para tener acceso a Internet, habrá "ráfagas" de actividad en el circuito mientras se transfiere una página Web. Entonces, es posible que le siga un periodo sin actividad mientras el usuario lee la página y luego otra ráfaga de actividad mientras se transfiere la página siguiente. Esta variación en el uso entre máximo y nada es típica del tráfico informático de red. Como el suscriptor tiene uso exclusivo de la capacidad fija asignada, los circuitos conmutados, en general, son una forma cara de transferir datos.

PSTN e ISDN son dos tipos de tecnología de conmutación de circuitos que pueden utilizarse para implementar una WAN en un contexto empresarial.

Haga clic en el botón Reproducir en la imagen para ver cómo funciona la conmutación de circuitos.



Conmutación de paquetes

A diferencia de la conmutación de circuitos, la conmutación de paquetes divide los datos del tráfico en paquetes que se envían a través de una red compartida. Las redes de conmutación de paquetes no requieren que se establezca un circuito y permiten que muchos pares de nodos se comuniquen a través del mismo canal.

Los switches de una red conmutada por paquetes determinan el siguiente enlace por donde se debe enviar el paquete en función de la información de direccionamiento de cada paquete. Hay dos maneras de determinar este enlace: sin conexión u orientada a conexión.

- Los sistemas sin conexión, tal como Internet, transmiten toda la información de direccionamiento en cada paquete. Cada switch debe evaluar la dirección para determinar a dónde enviar el paquete.
- Los sistemas orientados a conexión predeterminan la ruta del paquete y cada paquete sólo necesita llevar un identificador. En el caso de Frame Relay, estos se denominan identificadores de control de enlace de datos (DLCI, Data Link Control Identifiers). El switch determina la ruta a seguir buscando el identificador en las tablas que tiene en su memoria. Este grupo de entradas en las tablas identifica una ruta o circuito particular a través del sistema. Si este circuito está físicamente disponible, sólo mientras el paquete esté pasando por él, se llama circuito virtual (VC, virtual circuit).

Como los enlaces internos entre los switches se comparten entre varios usuarios, los costos de la conmutación de paquetes son más bajos que aquéllos de conmutación de circuitos. Los retardos (latencia) y la variación en los retardos (fluctuación de fase) son mayores en las redes conmutadas por paquetes que en las conmutadas por circuitos. Esto ocurre porque se comparten los enlaces y es necesario que un switch reciba todos los paquetes antes de seguir adelante. A pesar de la latencia y a las fluctuaciones de fase inherentes a las redes compartidas, la tecnología moderna permite el transporte satisfactorio de las comunicaciones de voz y hasta video por estas redes.

Haga clic en el botón Reproducir en la imagen para ver un ejemplo de conmutación de paquetes.

El servidor A está enviando datos al servidor B. Cuando el paquete atraviesa la red del proveedor, llega al switch del segundo proveedor. El paquete se agrega a la cola y se envía después de que los demás paquetes de la cola hayan sido enviados. Finalmente, el paquete llega al servidor B.

Circuitos virtuales

Las redes conmutadas por paquetes pueden establecer rutas a través de los switches para realizar conexiones particulares de extremo a extremo. Estas rutas se denominan circuitos virtuales. Un VC es un circuito lógico creado dentro de una red compartida entre dos dispositivos de red. Existen dos tipos de VC.

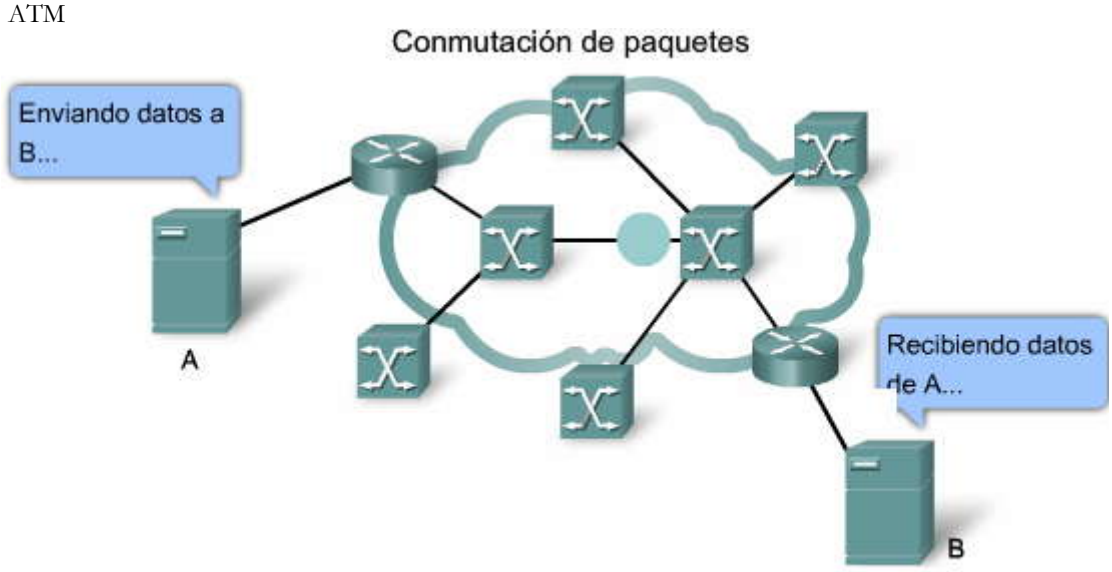
- **Circuito virtual permanente (PVC, Permanent Virtual Circuit)**: un circuito virtual establecido de forma permanente que consta de un modo (transferencia de datos). Los PVC se utilizan cuando la transferencia de datos entre dispositivos es constante. Los PVC reducen el uso del ancho de banda relacionado con el establecimiento y la terminación de los VC, pero aumentan los costos debido a la disponibilidad constante del circuito virtual. En general, los PVC, son configurados por el proveedor de servicios cuando el cliente solicita el servicio.

- Circuito virtual conmutado (SVC, **Switched Virtual Circuit)**: son circuitos virtuales que se establecen dinámicamente a pedido y que se terminan cuando se completa la transmisión. La comunicación a través de un SVC consta de tres fases: establecimiento del circuito, transferencia de datos y terminación del circuito. La fase de establecimiento involucra la creación del VC entre los dispositivos origen y destino. La transferencia de datos implica la transmisión de datos entre los dispositivos a través del VC, y la fase de terminación de circuito implica la interrupción del VC entre los dispositivos origen y destino. Los SVC se utilizan en situaciones en las que la transmisión de datos entre los dispositivos es intermitente, principalmente para ahorrar costos. Los SVC liberan el circuito cuando se completa la transmisión, lo que genera menos costos de conexión que los que generan los PVC, que mantienen la disponibilidad del circuito virtual de manera constante.

Conexión a una red de conmutación de paquetes

Para conectarse a una red de conmutación de paquetes, el suscriptor necesita un bucle local a la ubicación más cercana donde el proveedor ofrece el servicio. Esto se llama punto de presencia (POP, point-of-presence) del servicio. Por lo general, se trata de una línea arrendada dedicada. Esta línea es mucho más corta que una línea arrendada conectada directamente a las diferentes ubicaciones del suscriptor y muchas veces transporta VC. Como es poco probable que todos los VC enfrenten la máxima demanda al mismo tiempo, la capacidad de la línea arrendada puede ser menor a la de la suma de los VC individuales. Los siguientes son ejemplos de conexiones de conmutación de paquetes o celdas:

- X.25
- Frame Relay
- ATM



Los datos rotulados se pasan de switch a switch. Es posible que tenga que esperar su turno en un vínculo.

Las operaciones WAN se realizan en las capas ____ y ____ del modelo OSI.	✓ física ✓ enlace de datos
Un cable de cobre o fibra conecta el equipo terminal del abonado (CPE, customer premise equipment) con el/la ____ más cercano/a del proveedor de servicios.	✓ intercambio
El punto de ____ física es el lugar en donde la responsabilidad de la conexión pasa del usuario al proveedor de servicios.	✓ demarcación
Un/a ____ es un dispositivo WAN que convierte señales digitales al formato analógico para transmitirlas a través de una línea analógica, y después convierte esta señal analógica nuevamente al formato digital para que el dispositivo receptor de la red pueda recibirla y procesarla.	✓ módem
El campo de la/el ____ de los formatos de trama WAN no es necesario porque los enlaces WAN casi siempre son punto a punto.	✓ dirección
Una red de conmutación por ____ es la que establece un canal dedicado entre los nodos y las terminales antes de que los usuarios puedan comunicarse.	✓ circuitos
Una red de conmutación por ____ no requiere un canal dedicado entre los nodos. Muchos pares de nodos pueden comunicarse por el mismo canal.	✓ paquetes

1.3 Opciones de conexión WAN

1.3.1 Opciones de conexión de enlace WAN

En la actualidad, existen muchas opciones para implementar soluciones WAN. Ellas difieren en tecnología, velocidad y costo. Estar familiarizado con estas tecnologías es una parte importante del diseño y evaluación de la red.

Las conexiones WAN pueden establecerse sobre una infraestructura privada o una infraestructura pública, por ejemplo Internet.

Opciones de conexión de WAN privadas

Las conexiones WAN privadas incluyen opciones de enlaces de comunicación dedicados y conmutados.

Enlaces de comunicación dedicados

Cuando se requieren conexiones dedicadas permanentes, se utilizan líneas punto a punto con diversas capacidades que tienen solamente las limitaciones de las instalaciones físicas subyacentes y la disposición de los usuarios de pagar por estas líneas dedicadas. Un enlace punto a punto ofrece rutas de comunicación WAN preestablecidas desde las instalaciones del cliente a través de la red del proveedor hasta un destino remoto. Laslíneas punto a punto se alquilan por lo general a una operadora y se denominan también líneas arrendadas.

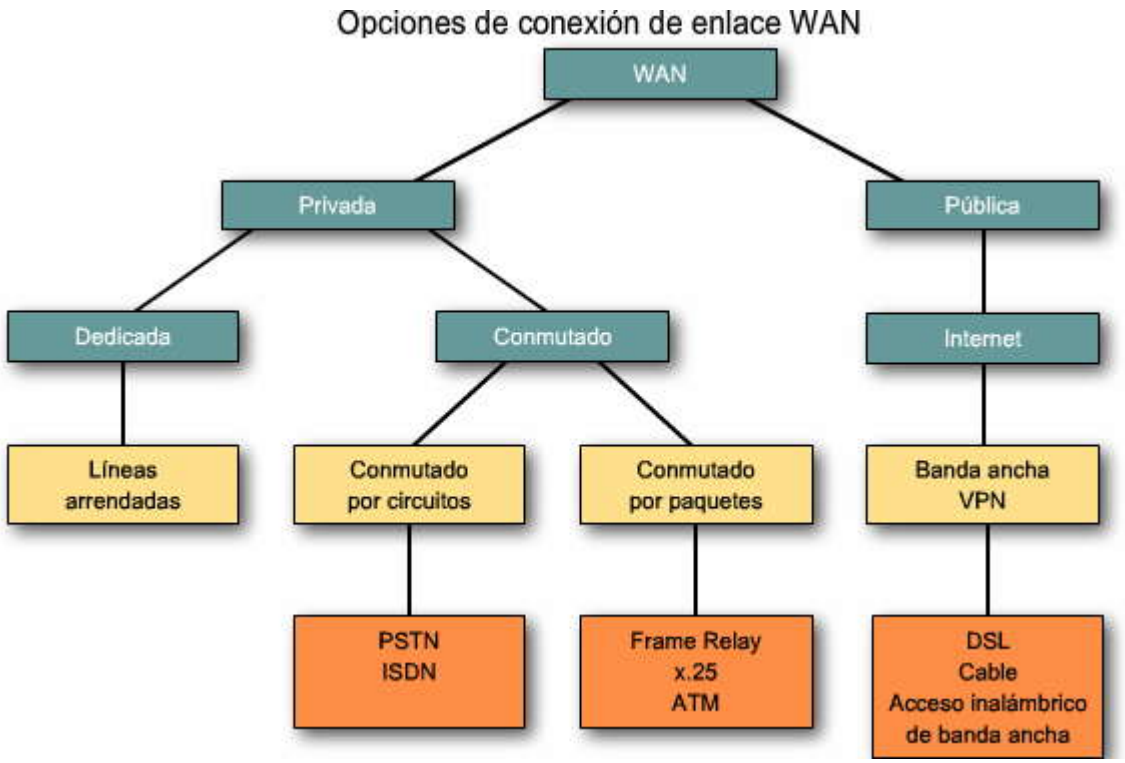
Enlaces de comunicación conmutados

Los enlaces de comunicación conmutados pueden ser por conmutación de circuitos o conmutación de paquetes.

- **Enlaces de comunicación por conmutación de circuitos**: la conmutación de circuitos establece dinámicamente una conexión virtual dedicada para voz o datos entre el emisor y el receptor. Antes de que comience la conmutación, es necesario establecer la conexión a través de la red del proveedor de servicios. Entre los enlaces de comunicación por conmutación de circuitos se encuentran el acceso telefónico analógico (PSTN) e ISDN.
- **Enlaces de comunicación por conmutación de paquetes**: muchos usuarios WAN no utilizan de manera eficiente el ancho de banda fijo que está disponible para los circuitos dedicados, conmutados o permanentes porque el flujo de datos fluctúa. Los proveedores de comunicaciones cuentan con redes de datos disponibles para brindar un mejor servicio a estos usuarios. En las redes con conmutación de paquetes, los datos se transmiten en tramas, celdas o paquetes rotulados. Los enlaces de comunicación por conmutación de paquetes incluyen Frame Relay, ATM, X.25 y Metro Ethernet.

Opciones de conexión WAN públicas

Las conexiones públicas utilizan la infraestructura global de Internet. Hasta hace poco, Internet no era una opción viable de sistema de redes para muchas empresas debido a los importantes riesgos de seguridad y la falta de garantías de rendimiento adecuadas en una conexión de extremo a extremo a través de Internet. Sin embargo, con el desarrollo de la tecnología VPN, Internet ahora es una opción económica y segura para conectarse con trabajadores a distancia y oficinas remotas cuando no es fundamental contar con garantías de rendimiento. Los enlaces de conexión WAN a través de Internet se establecen a través de servicios de banda ancha, por ejemplo DSL, módem por cable y acceso inalámbrico de banda ancha, y en combinación con la tecnología VPN para proporcionar privacidad a través de Internet.



1.3.2 Opciones de conexión de enlace dedicado

Líneas arrendadas

Cuando se necesitan conexiones dedicadas permanentes, se utiliza un enlace punto a punto para proporcionar rutas de comunicación WAN preestablecidas desde las instalaciones del cliente a través de la red del proveedor hasta un destino remoto. Las líneas punto a punto se alquilan por lo general a una operadora y se denominan líneas alquiladas. Este tema describe la manera en la que las empresas utilizan las líneas arrendadas para proporcionar una conexión WAN dedicada.

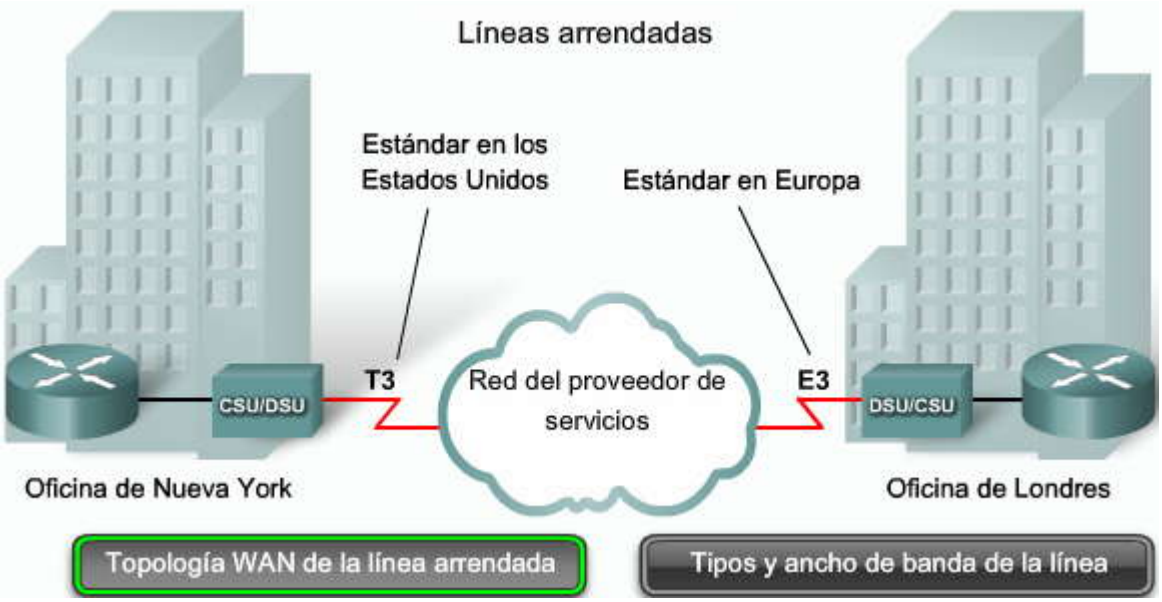
Haga clic en el botón Tipos y ancho de banda de la línea en la imagen para ver una lista de los tipos de líneas arrendadas disponibles y sus capacidades de velocidad de bits.

Las líneas arrendadas están disponibles en diferentes capacidades y en general el precio depende del ancho de banda requerido y de la distancia entre los dos puntos conectados.

En general, los enlaces punto a punto son más caros que los servicios compartidos como Frame Relay. El costo de las soluciones de línea dedicada puede tornarse considerable cuando se utilizan para conectar varios sitios separados por distancias mayores. Sin embargo, a veces los beneficios superan el costo de la línea arrendada. La capacidad dedicada elimina la latencia o las fluctuaciones de fase entre los extremos. La disponibilidad constante es esencial para algunas aplicaciones, como es el caso de VoIP o video sobre IP.

Cada conexión de línea alquilada requiere un puerto serial de router. También se necesita un CSU/DSU y el circuito físico del proveedor de servicios.

Las líneas arrendadas ofrecen una capacidad dedicada permanente y se utilizan con mucha frecuencia en la construcción de redes WAN. Éstas han sido la conexión tradicional de preferencia, aunque presentan varias desventajas. Las líneas arrendadas tienen una capacidad fija, pero el tráfico WAN con frecuencia es variable, lo que hace que no se utilice la capacidad total. Además, cada punto final necesita una interfaz física independiente en el router, lo que aumenta los costos de equipos. Todo cambio en la línea arrendada, en general, requiere que el proveedor haga una visita al establecimiento.



Opción de conexión WAN: Líneas arrendadas

Afirmación: Las líneas arrendadas	Verdadero	Falso
se consideran enlaces WAN dedicados.	✓	
son ideales para conectar usuarios separados por una distancia grande.		✓
constan de varios circuitos virtuales conmutados.		✓
tienen menor latencia y fluctuación de fase en comparación con otros enlaces WAN.	✓	
pueden operar a velocidades de bits muy elevadas.	✓	
no requieren ninguna configuración de llamada, dado que siempre están activadas.	✓	
son los enlaces de WAN de menor costo para interconexiones.		✓
se usan con mayor frecuencia como respaldo de los circuitos de conexión telefónica.		✓

1.3.3 Opciones de conexión por conmutación de circuitos

Conexión telefónica analógica

Cuando se necesitan transferencias de datos de bajo volumen e intermitentes, los módems y las líneas telefónicas analógicas ofrecen conexiones conmutadas dedicadas y de baja capacidad. Este tema describe las ventajas y las desventajas del uso de opciones de conexión telefónica analógica e identifica los tipos de situaciones empresariales que se benefician más con este tipo de opción.

La telefonía tradicional utiliza un cable de cobre llamado bucle local para conectar el equipo telefónico que se encuentra en las instalaciones del suscriptor a la CO. La señal que circula por el bucle local durante una llamada es una señal electrónica que varía continuamente y que es una traducción de la voz del suscriptor, analógica.

Los bucles tradicionales locales pueden transportar datos informáticos binarios a travésde la red telefónica de voz mediante un módem. El módem modula los datos binarios en una señal analógica en el origen y demodula la señal analógica a datos binarios en el destino. Las características físicas del bucle local y su conexión a la PSTN limitan la velocidad de la señal a menos de 56 kbps.

Para empresas pequeñas, estas conexiones de acceso telefónico de velocidad relativamente baja son adecuadas parael intercambio de cifras de ventas, precios, informes de rutina y correo electrónico. Al usar el sistema de conexión automático de noche o durante los fines de semana para realizar grandes transferencias de archivos y copias de respaldo de datos, la empresa puede aprovechar las tarifas más bajas de las horas no pico (cargos por línea). Las tarifas se calculan según la distancia entre los extremos, la hora del día y la duración de la llamada.

Las ventajas del módem y las líneas analógicas son la simplicidad, la disponibilidad y el bajo costo de implementación. Las desventajas son la baja velocidad en la transmisión de datos y el tiempo de conexión relativamente largo. Los circuitos dedicados tienen poco retardo o fluctuación de fase para el tráfico punto a punto, pero el tráfico de voz o video no funciona de forma adecuada a estas bajas velocidades de bits.

WAN construida con conexión intermitente mediante un módem y la red telefónica de voz.

Red digital de servicios integrados

La red digital de servicios integrados (ISDN, Integrated Services Digital Network) es una tecnología de conmutación de circuitos que permite al bucle local de una PSTN transportar señales digitales, lo que da como resultado una mayor capacidad de conexiones conmutadas. La ISDN cambia las conexiones internas de la PSTN de señales portadoras analógicas a señales digitales de multiplexación por división temporal (TDM). La TDM permite que dos o más señales o corrientes de bits se transfieran como canales secundarios de un canal de comunicación. Las señales parecen transferirse de manera simultánea, pero físicamente se turnan para utilizar el canal. Un bloque de datos del canal secundario 1 se transmite durante la ranura de tiempo 1, los del canal secundario 2 durante la ranura de tiempo 2, y así sucesivamente. Una trama de TDM está compuesta por una ranura de tiempo por canal secundario. En el Capítulo 2, PPP, se describe la TDM con mayor detalle

La ISDN convierte el bucle local en una conexión digital TDM. Este cambio permite que el bucle local lleve señales digitales, lo que da como resultado conexiones conmutadas de mayor capacidad. La conexión utiliza canales de portadora de 64 kbps (B) para transportar voz o datos y una señal, canal delta (D) para la configuración de llamadas y otros propósitos.

Existen dos tipos de interfaces ISDN:

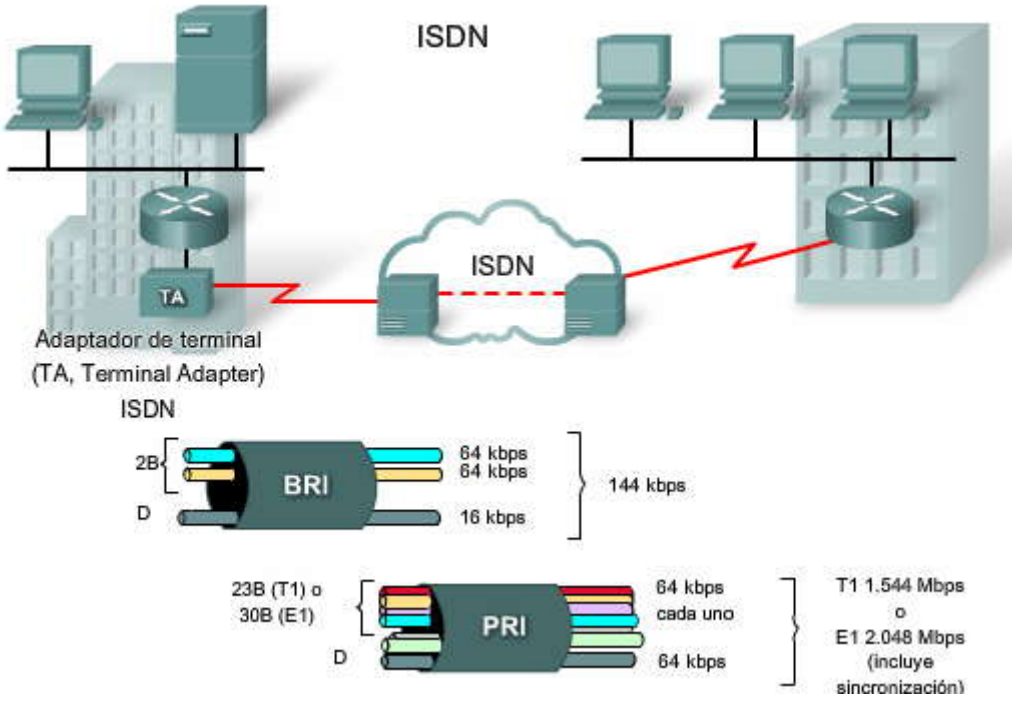
- **La ISDN de interfaz de acceso básico (BRI, Basic Rate Interface)** está destinada al uso doméstico y para las pequeñas empresas, y provee dos canales B de 64 kbps y un canal D de 16 kbps. El canal D BRI está diseñado para control y con frecuencia no se utiliza su potencial máximo, ya que tiene que controlar solamente dos canales B. Por lo tanto, algunos proveedores permiten que los canales D transmitan datos a una velocidad de transmisión baja como las conexiones X.25 a 9.6 kbps.
- **La ISDN de interfaz de acceso principal (PRI, Primary Rate Interface)** también está disponible para instalaciones más grandes. La PRI ofrece 23 canales B de 64 kbps y un canal D de 64 kbps en América del Norte, lo que da un total de velocidad de transmisión de hasta 1.544 Mbps. Esto incluye una carga adicional de sincronización. En Europa, Australia y otras partes del mundo, PRI ISDN ofrece 30 canales B y un canal D para un total de velocidad de transmisión de hasta 2.048 Mbps, incluida la carga de sincronización. En América del Norte, PRI corresponde a una conexión T1. La velocidad de PRI internacional corresponde a una conexión E1 o J1.

Para las WAN pequeñas, la ISDN BRI puede ofrecer un mecanismo de conexión ideal. BRI posee un tiempo de establecimiento de llamada que es menor a un segundo y el canal B de 64 kbps ofrece mayor capacidad que un enlace de módem analógico. Si se requiere una mayor capacidad, se puede activar un segundo canal B para brindar un total de 128 kbps. Aunque no es adecuado para el video, esto permite la transmisión de varias conversaciones de voz simultáneas, además del tráfico de datos.

Otra aplicación común de ISDN es la de ofrecer capacidad adicional según la necesidad en una conexión de línea arrendada. La línea arrendada tiene el tamaño para transportar el tráfico usual mientras que ISDN se agrega durante los periodos de demanda pico. La ISDN también se utiliza como respaldo si la línea arrendada falla. Las tarifas de ISDN se calculan según cada canal B y son similares a las de las conexiones analógicas.

Con la ISDN PRI se pueden conectar varios canales B entre dos extremos. Esto permite que se realicen videoconferencias y conexiones de datos de banda ancha sin latencia ni fluctuación de fase. Sin embargo, el uso de conexiones múltiples puede resultar muy costoso para cubrir grandes distancias.

Nota: Si bien ISDN sigue siendo una tecnología importante para las redes de proveedores de servicios telefónicos, está disminuyendo en popularidad como opción de conexión a Internet a causa de la introducción de la conexión DSL de alta velocidad y otros servicios de banda ancha. La sección "Perspectivas para la industria y los consumidores" (en inglés) en http://en.wikipedia.org/wiki/ISDN brinda un buen análisis de las tendencias mundiales de ISDN.



Afirmación: La conexión dialup analógica	Verdadero	Falso
se considera como un enlace WAN conmutado.	✓	
se basa en la tecnología de conmutación de celdas.		✓
permite establecer una conexión en muy poco tiempo.		✓
envía señales digitales a través del bucle local de Telco.		✓
requiere un modulador/demodulador para enviar señales digitales a la PSTN.	✓	
las ventajas incluyen el bajo costo y la disponibilidad.	✓	

Afirmación: La conexión dialup ISDN	Verdadero	Falso
se considera como un enlace WAN dedicado.		✓
se basa en la tecnología de conmutación de circuitos.	✓	
posee un tiempo reducido de establecimiento de llamada.	✓	
consta de canales B y un canal D.	✓	
no es adecuado para usar como enlace de respaldo.		✓

1.3.4 Opciones de conexión por conmutación de paquetes

Tecnologías WAN comunes por conmutación de paquetes

Las tecnologías WAN de conmutación de paquetes más comunes utilizadas en las redes WAN empresariales de la actualidad incluyen Frame Relay, ATM y X.25 heredado.

Haga clic en el botón X.25 en la imagen.

X.25

X.25 es un protocolo de capa de red heredado que proporciona una dirección de red a los suscriptores. Los circuitos virtuales se establecen a través de la red con paquetes de petición de llamadas a la dirección destino. Un número de canal identifica la SVC resultante. Los paquetes de datos rotulados con el número del canal se envían a la dirección correspondiente. Varios canales pueden estar activos en una sola conexión.

Las aplicaciones típicas de X.25 son los lectores de tarjeta de punto de venta. Estos lectores utilizan X.25 en el modo de conexión telefónica para validar las transacciones en una computadora central. Para estas aplicaciones, el ancho de banda bajo y la latencia alta no constituyen un problema, y el costo bajo hace que X.25 sea accesible.

Las velocidades de los enlaces X.25 varían de 2400 bps a 2 Mbps. Sin embargo, las redes públicas normalmente tienen una capacidad baja con velocidades que rara vez superan los 64 kbps.

En la actualidad, las redes X.25 están en franca decadencia y están siendo reemplazadas por tecnologías más recientes de capa 2, como Frame Relay, ATM y ADSL. Sin embargo, se siguen utilizando en muchos países en vías de desarrollo, en donde el acceso a las tecnologías más recientes es limitado.

Haga clic en el botón Frame Relay que se muestra en la imagen.

Frame Relay

Si bien el diseño de la red parece ser similar al de las redes X.25, Frame Relay se diferencia de X.25 en varios aspectos. El más importante es que es un protocolo mucho más sencillo que funciona a nivel de la capa de enlace de datos y no en la capa de red. Frame Relay no realiza ningún control de errores o flujo. El resultado de la administración simplificada de las tramas es una reducción en la latencia y las medidas tomadas para evitar la acumulación de tramas en los switches intermedios ayudan a reducir las fluctuaciones de fase. Frame Relay ofrece velocidades de datos de hasta 4 Mbps y hay proveedores que ofrecen velocidades aún mayores.

Los VC de Frame Relay se identifican de manera única con un DLCI, lo que garantiza una comunicación bidireccional de un dispositivo DTE al otro. La mayoría de las conexiones de Frame Relay son PVC y no SVC.

Frame Relay ofrece una conectividad permanente, compartida, de ancho de banda mediano, que envía tanto tráfico de voz como de datos. Frame Relay es ideal para conectar las LAN de una empresa. El router de la LAN necesita sólo una interfaz, aún cuando se estén usando varios VC. La línea alquilada corta que va al extremo de la red Frame Relay permite que las conexiones sean económicas entre LAN muy dispersas.

Frame Relay se describe con más detalles en el Capítulo 3, "Frame Relay".

Haga clic en el botón ATM que se muestra en la imagen.

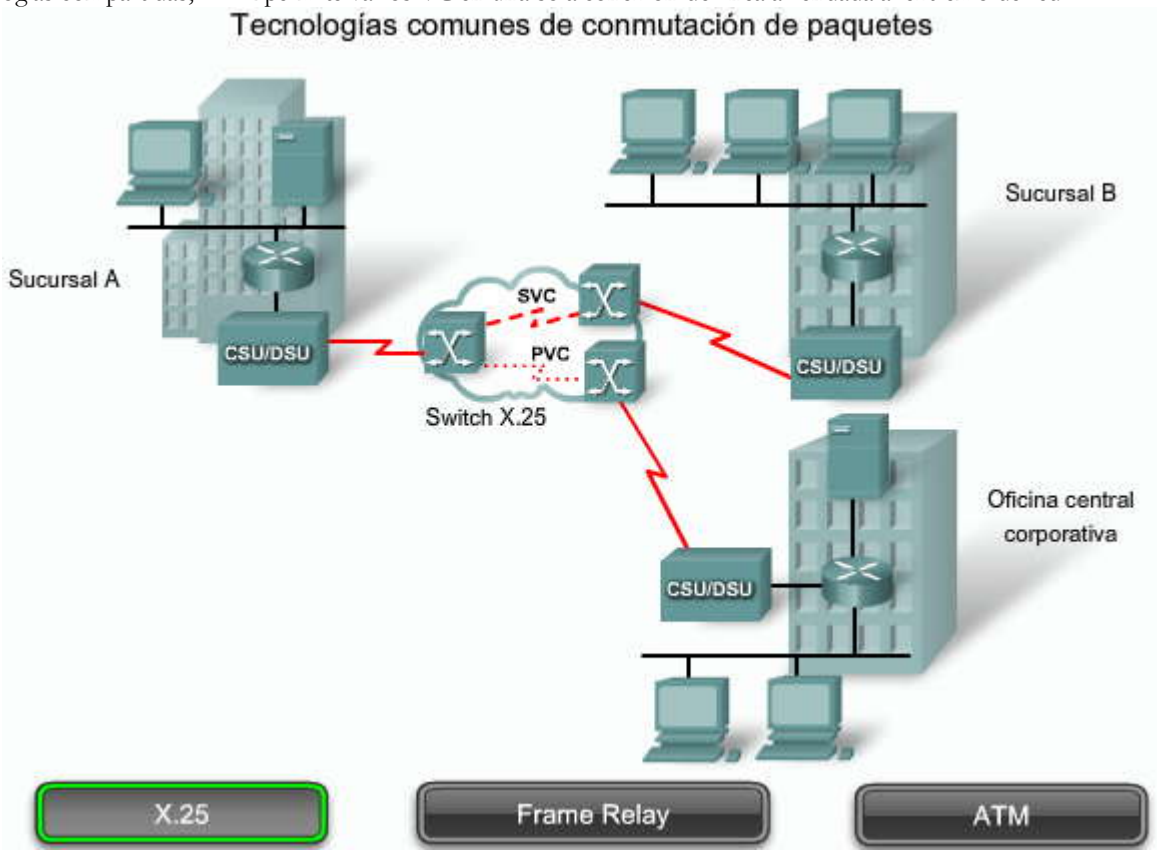
ATM

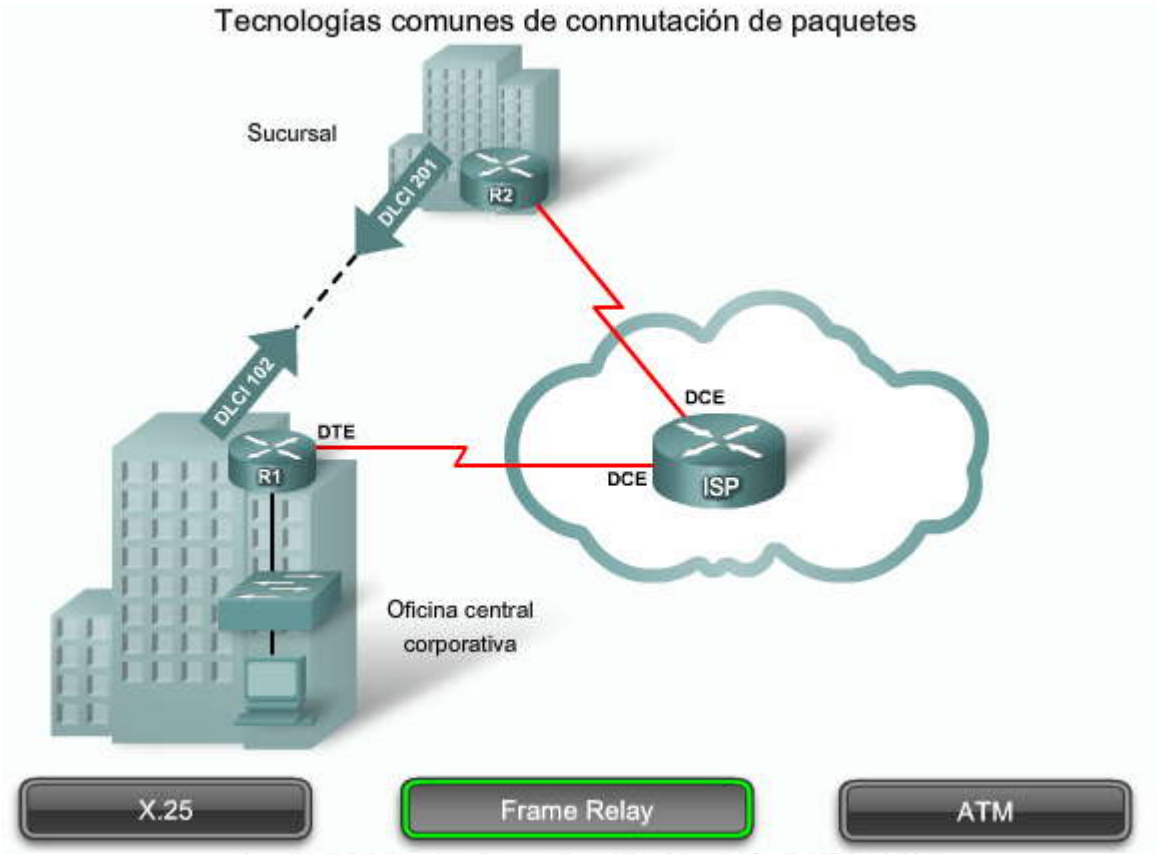
Modo de transferencia asíncrona (ATM, Asynchronous Transfer Mode) es capaz de transferir voz, video y datos a través de redes privadas y públicas. Tiene una arquitectura basada en celdas, en lugar de tramas. Las celdas ATM tienen siempre una longitud fija de 53 bytes. La celda ATM contiene un encabezado ATM de 5 bytes seguido de 48 bytes de contenido ATM. Las celdas pequeñas de longitud fija son adecuadas para la transmisión de tráfico de voz y video porque este tráfico no tolera demoras. El tráfico de video y voz no tiene que esperar a que se transmita un paquete de datos más grande.

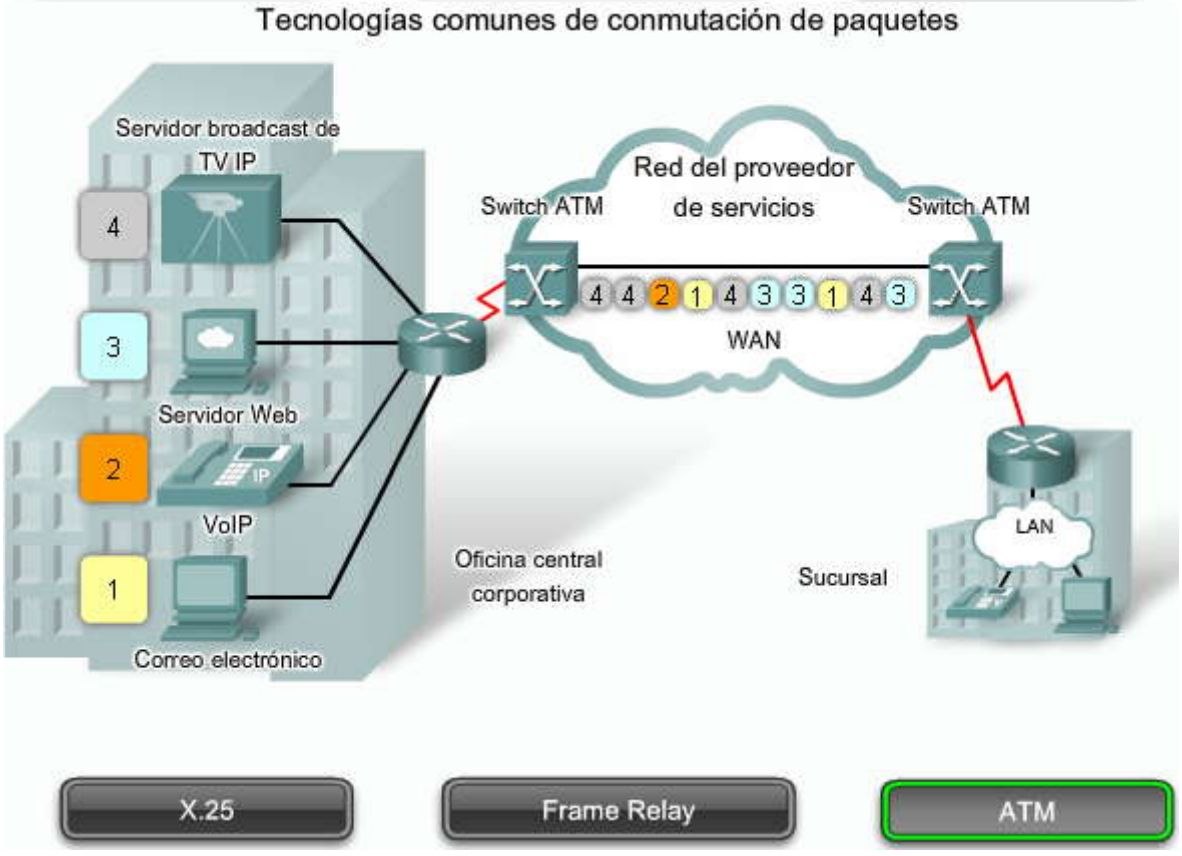
La celda ATM de 53 bytes es menos eficiente que las tramas y paquetes más grandes de Frame Relay y X.25. Además, la celda ATM tiene una carga general de por lo menos 5 bytes por cada 48 bytes de contenido. Cuando la celda está transportando paquetes de capa de red segmentados, la carga general es mayor porque el switch ATM tiene que poder reagrupar los paquetes en el destino. Una línea ATM típica necesita casi un 20 por ciento más de ancho de banda que Frame Relay para transportar el mismo volumen de datos de capa de red.

ATM fue diseñado para ser extremadamente escalable y soporta velocidades de enlace desde T1/E1 hasta OC-12 (622 Mbps) y superiores.

ATM ofrece tanto los PVC como los SVC, aunque los PVC son más comunes en las WAN. Además, como otras tecnologías compartidas, ATM permite varios VC en una sola conexión de línea arrendada al extremo de red.




Tecnologías comunes de conmutación de paquetes
Sucursal
DLCI 201
R2
DLCI 102
DTE
R1
DCE
DCE
ISP
Oficina central
corporativa
X.25
Frame Relay
ATM


Tecnologías comunes de conmutación de paquetes
Servidor broadcast de
TV IP
4
3
Servidor Web
2
IP
VoIP
1
Correo electrónico
Red del proveedor
de servicios
Switch ATM
Switch ATM
4 4 2 1 4 3 3 1 4 3
WAN
LAN
Oficina central
corporativa
Sucursal
X.25
Frame Relay
ATM

Opción de conexión WAN: Frame Relay

Afirmación: Frame Relay	Verdadero	Falso
se considera como un enlace WAN digital orientado a conexión.	✓	
se basa en la tecnología de conmutación de paquetes.	✓	
tiene menor gasto y latencia que X.25.	✓	
se puede usar para interconectar las LAN.	✓	
en la mayoría de los casos, se implementa con circuitos virtuales permanentes.	✓	
se usa en circuitos que van de 56 kbps a 45 Mbps.	✓	
los costos se basan únicamente en la distancia recorrida por los paquetes.		✓
no es flexible y no soporta ráfagas de datos.		✓
puede usar una sola interfaz física para varias conexiones.	✓	

1.3.5 Opciones de conexión por Internet

Servicios de banda ancha

Las opciones de conexión de banda ancha normalmente se utilizan para conectar empleados que trabajan a distancia con el sitio corporativo a través de Internet. Estas opciones incluyen cable, DSL e inalámbrica.

Haga clic en el botón DSL que se muestra en la imagen.

DSL

La tecnología DSL es una tecnología de conexión permanente que utiliza líneas telefónicas de par trenzado existentes para transportar datos de alto ancho de banda y brindar servicios IP a los suscriptores. Un módem DSL convierte una señal Ethernet proveniente del dispositivo del usuario en una señal DSL que se transmite a la oficina central.

Las líneas del suscriptor DSL múltiples se pueden multiplexar a un único enlace de alta capacidad con un multiplexor de acceso DSL (DSLAM) en el sitio del proveedor. Los DSLAM incorporan la tecnología TDM para agrupar muchas líneas del suscriptor en un único medio, en general una conexión T3 (DS3). Las tecnologías DSL actuales utilizan técnicas de codificación y modulación sofisticadas para lograr velocidades de transmisión de datos de hasta 8.192 Mbps.

Hay una amplia variedad de tipos, estándares y estándares emergentes de DSL. En la actualidad, DSL es una opción popular entre los departamentos de TI de las empresas para darle soporte a las personas que trabajan en sus hogares. Por lo general, el suscriptor no puede optar por conectarse a la red de la empresa directamente, sino que primero debe conectarse a un ISP para establecer una conexión IP con la empresa a través de Internet. En este proceso se generan riesgos de seguridad, pero se pueden solucionar con medidas de protección.

Haga clic en el botón Módem por cable en la imagen.

Módem por cable

El cable coaxial es muy usado en áreas urbanas para distribuir las señales de televisión. El acceso a la red está disponible desde algunas redes de televisión por cable. Esto permite que haya un mayor ancho de banda que con el bucle local de teléfono.

Los módems por cable ofrecen una conexión permanente y una instalación simple. El suscriptor conecta una computadora o un router LAN al módem por cable, que traduce las señales digitales a las frecuencias de banda ancha que se utilizan para transmitir por una red de televisión por cable. La oficina de TV por cable local, que se denomina extremo final del cable, cuenta con el sistema informático y las bases de datos necesarios para brindar acceso a Internet. El componente más importante que se encuentra en el extremo final es el sistema de terminación de módems de cable (CMTS, cable modem termination system) que envía y recibe señales digitales de módem por cable a través de una red de cables y es necesario para proporcionar los servicios de Internet a los suscriptores del servicio de cable.

Los suscriptores de módem por cable deben utilizar el ISP correspondiente al proveedor de servicio. Todos los suscriptores locales comparten el mismo ancho de banda del cable. A medida que más usuarios contratan el servicio, el ancho de banda disponible puede caer por debajo de la velocidad esperada.

Haga clic en el botón Acceso inalámbrico de banda ancha que aparece en la imagen.

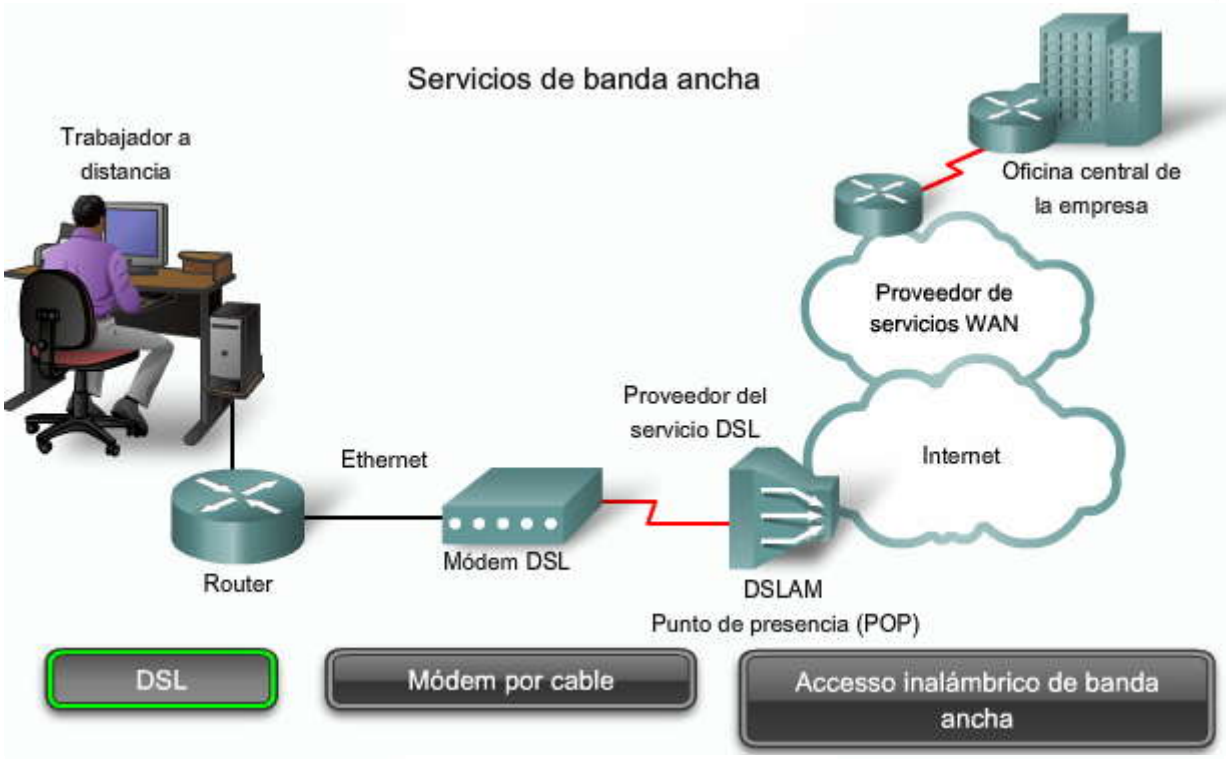
Acceso inalámbrico de banda ancha

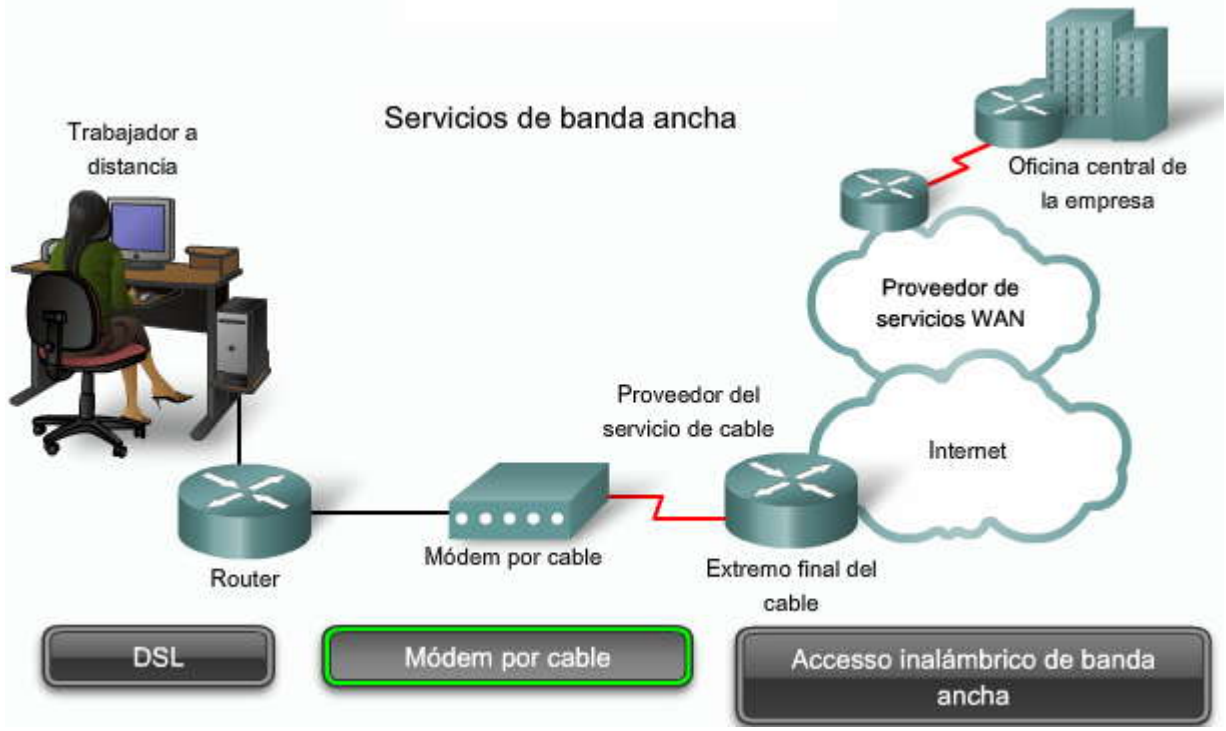
La tecnología inalámbrica utiliza el espectro de radiofrecuencia sin licencia para enviar y recibir datos. El espectro sin licencia está disponible para todos quienes posean un router inalámbrico y tecnología inalámbrica en el dispositivo que estén utilizando.

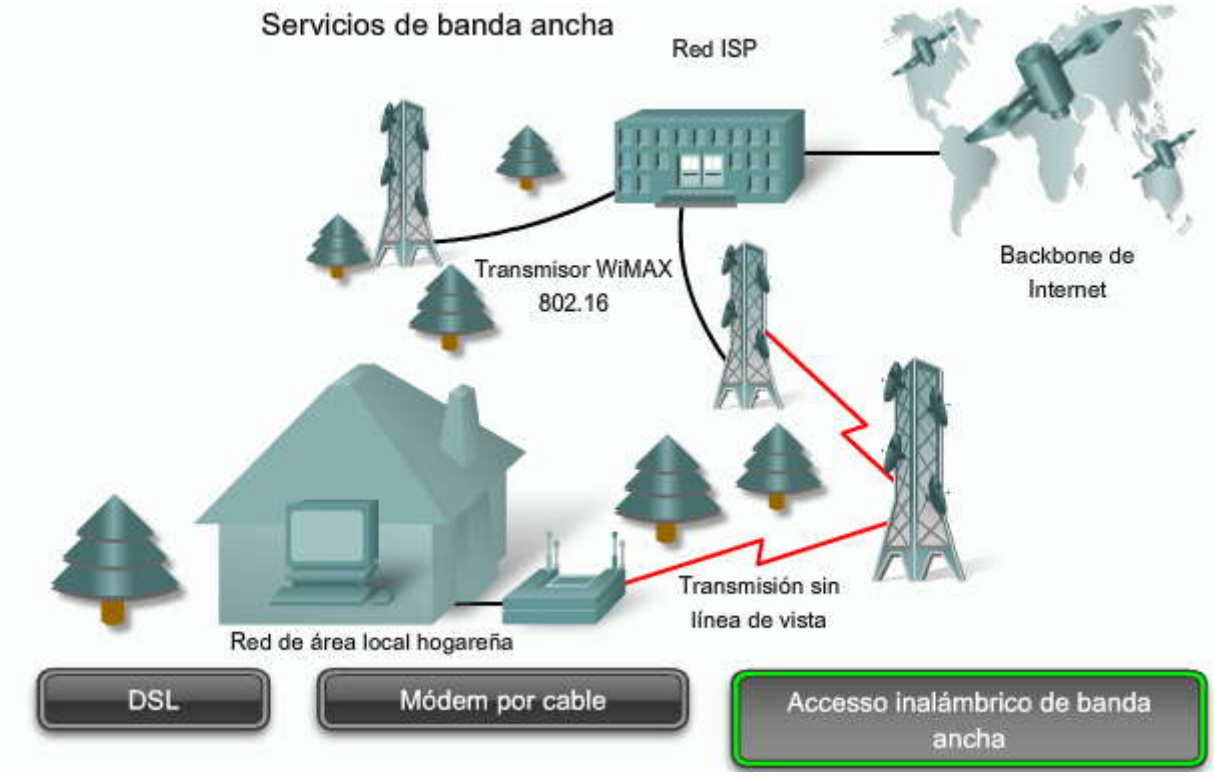
Hasta hace poco, una de las limitaciones del acceso inalámbrico era la necesidad de encontrarse dentro del rango de transmisión local (normalmente, menos de 100 pies) de un router inalámbrico o un módem inalámbrico que tuviera una conexión fija a Internet. Los siguientes nuevos desarrollos en la tecnología inalámbrica de banda ancha están cambiando esta situación:

- **WiFi municipal**: muchas ciudades han comenzado a establecer redes inalámbricas municipales. Algunas de estas redes proporcionan acceso a Internet de alta velocidad de manera gratuita o por un precio marcadamente menor que el de otros servicios de banda ancha. Otras son para uso exclusivo de la ciudad, lo que permite a los empleados de los departamentos de policía y de bomberos, además de otros empleados municipales, realizar algunas de sus tareas laborales de manera remota. Para conectarse a una red WiFi municipal, el suscriptor normalmente necesita un módem inalámbrico que tenga una antena direccional de mayor alcance que los adaptadores inalámbricos convencionales. La mayoría de los proveedores de servicios entregan el equipo necesario de manera gratuita o por un precio, de manera similar a lo que hacen con los módems DSL o por cable.
- **WiMAX**: la interoperabilidad mundial para el acceso por microondas (WiMAX, Worldwide Interoperability for Microwave Access) es una nueva tecnología que se está comenzado a utilizar. Se describe en el estándar 802.16 del IEEE (Instituto de Ingeniería Eléctrica y Electrónica). WiMAX proporciona un servicio de banda ancha de alta velocidad con acceso inalámbrico y brinda una amplia cobertura como una red de telefonía celular en lugar de hacerlo a través de puntos de conexión WiFi pequeños. WiMAX funciona de manera similar a WiFi, pero a velocidades más elevadas, a través de distancias más extensas y para una mayor cantidad de usuarios. Utiliza una red de torres de WiMAX que son similares a las torres de telefonía celular. Para tener acceso a la red WiMAX, los suscriptores deben contratar los servicios de un ISP que tenga una torre WiMAX en un radio de 10 millas de su ubicación. También necesitan una computadora compatible con WiMAX y un código de encriptación especial para obtener acceso a la estación base.
- **Internet satelital**: normalmente es utilizada por usuarios rurales que no tienen acceso a los servicios de cable y DSL. Una antena satelital proporciona comunicaciones de datos de dos vías (carga y descarga). La velocidad de carga es de aproximadamente la décima parte de la velocidad de descarga de 500 kbps. Las conexiones DSL y por cable tienen velocidades de descarga mayores, pero los sistemas satelitales son unas 10 veces más rápidos que un módem analógico. Para tener acceso a los servicios de Internet satelital, los suscriptores necesitan una antena satelital, dos módems (uplink o enlace de carga y downlink o enlace de descarga) y cables coaxiales entre la antena y el módem.

Los servicios de banda ancha DSL, por cable e inalámbrico se describen con más detalles en el Capítulo 6, "Servicios de trabajadores a distancia".


Servicios de banda ancha
Trabajador a distancia
Oficina central de la empresa
Proveedor de servicios WAN
Proveedor del servicio DSL
Internet
Ethernet
Router
Módem DSL
DSLAM
Punto de presencia (POP)
DSL
Módem por cable
Accesso inalámbrico de banda ancha


Servicios de banda ancha
Trabajador a distancia
Oficina central de la empresa
Proveedor de servicios WAN
Proveedor del servicio de cable
Internet
Router
Módem por cable
Extremo final del cable
DSL
Módem por cable
Accesso inalámbrico de banda ancha



Tecnología VPN

Cuando un trabajador a distancia o de una oficina remota utiliza servicios de banda ancha para conectarse a la WAN corporativa a través de Internet, se corren riesgos de seguridad. Para tratar las cuestiones de seguridad, los servicios de banda ancha ofrecen funciones para utilizar conexiones de red privada virtual (VPN, Virtual Private Network) a un servidor VPN, que por lo general se encuentra ubicado en la empresa.

Una VPN es una conexión encriptada entre redes privadas a través de una red pública como Internet. En lugar de utilizar una conexión de Capa 2 dedicada, como una línea arrendada, las VPN utilizan conexiones virtuales denominadas túneles VPN que se enrutan a través de Internet desde una red privada de la empresa al sitio remoto o host del empleado.

Beneficios de las VPN

Los beneficios de las VPN incluyen los siguientes:

- **Ahorro de costos**: las VPN permiten a las organizaciones utilizar Internet global para conectar oficinas remotas y usuarios remotos al sitio corporativo principal, lo que elimina enlaces WAN dedicados costosos y bancos de módems.
- **Seguridad**: las VPN proporcionan el mayor nivel de seguridad mediante el uso de protocolos de encriptación y autenticación avanzados que protegen los datos contra el acceso no autorizado.
- **Escalabilidad**: como las VPN utilizan la infraestructura de Internet dentro de ISP y de los dispositivos, es sencillo agregar nuevos usuarios. Las corporaciones pueden agregar grandes cantidades de capacidad sin agregar una infraestructura importante.
- **Compatibilidad con la tecnología de banda ancha**: los proveedores de servicios de banda ancha como DSL y cable soportan la tecnología VPN, de manera que los trabajadores móviles y los trabajadores a distancia pueden aprovechar el servicio de Internet de alta velocidad que tienen en sus hogares para acceder a sus redes corporativas. Las conexiones de banda ancha de alta velocidad de nivel empresarial también pueden proporcionar una solución rentable para conectar oficinas remotas.

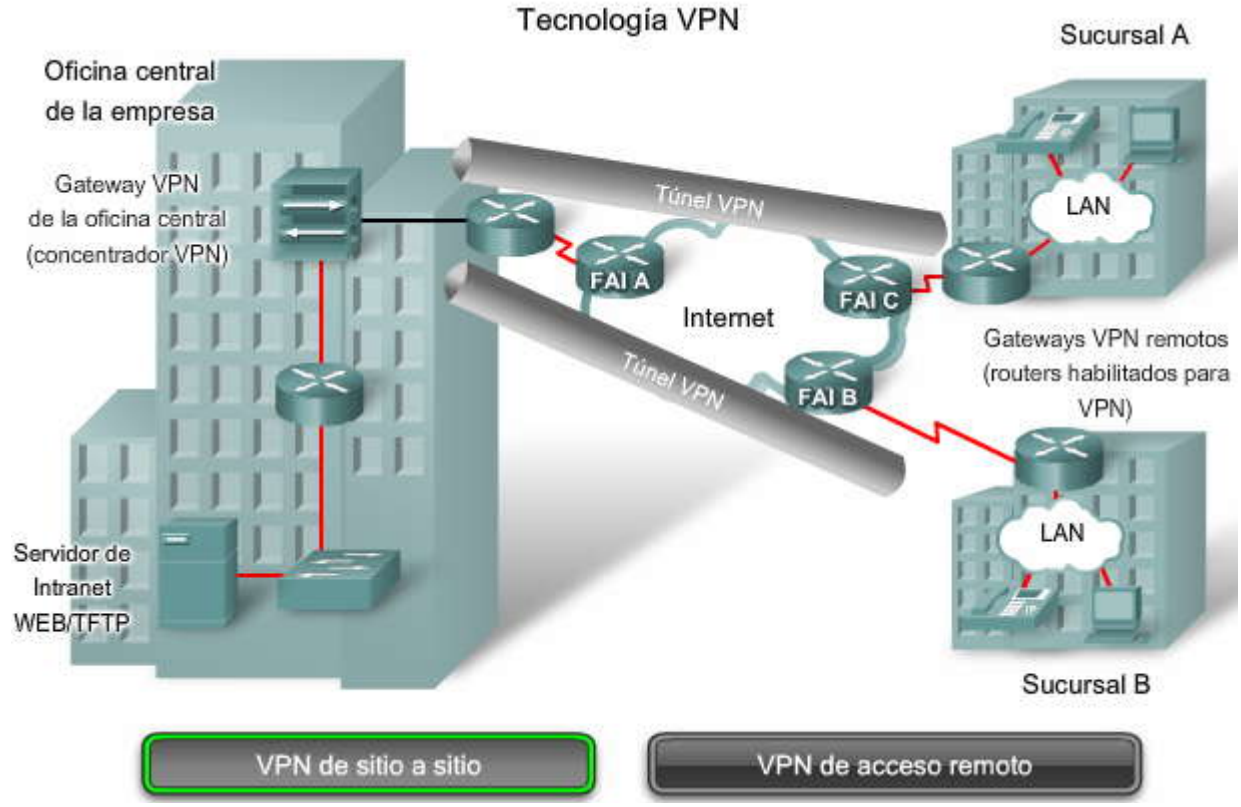
Tipos de acceso VPN

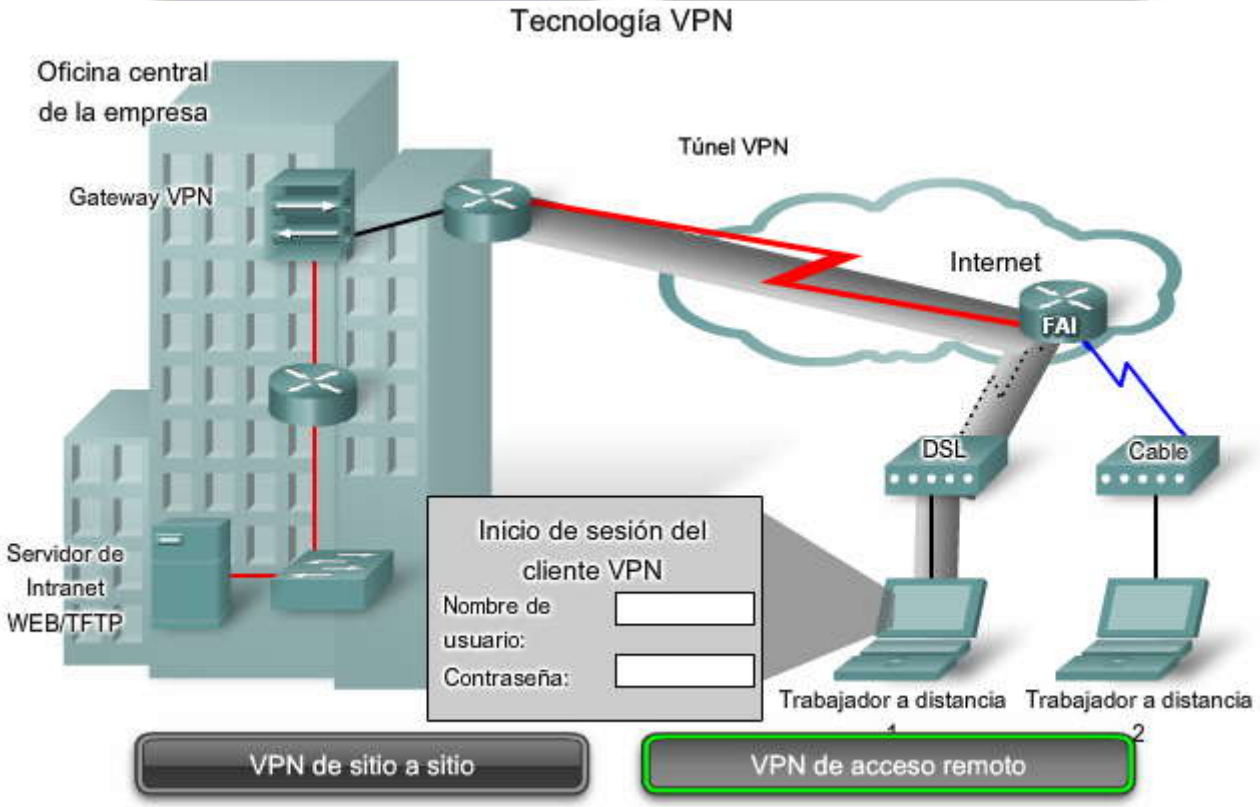
Existen dos tipos de acceso VPN:

- **VPN de sitio a sitio**: estas VPN conectan redes enteras entre sí; por ejemplo, pueden conectar la red de una sucursal con la red de la sede principal de la empresa, como se muestra en la imagen. Cada sitio cuenta con un gateway de la VPN, como un router, un firewall, un concentrador de VPN o un dispositivo de seguridad. En la imagen, la sucursal remota utiliza una VPN de sitio a sitio para conectarse con la oficina central de la empresa.

- **VPN de acceso remoto**: las VPN de acceso remoto permiten a hosts individuales, como trabajadores a distancia, usuarios móviles y consumidores de Extranet, tener acceso a la red empresarial de manera segura a través de Internet. Normalmente, cada host tiene instalado el software cliente de VPN o utiliza un cliente basado en la Web.

Haga clic en el botón VPN de acceso remoto o el botón VPN de sitio a sitio en la imagen para ver un ejemplo de cada tipo de conexión VPN.



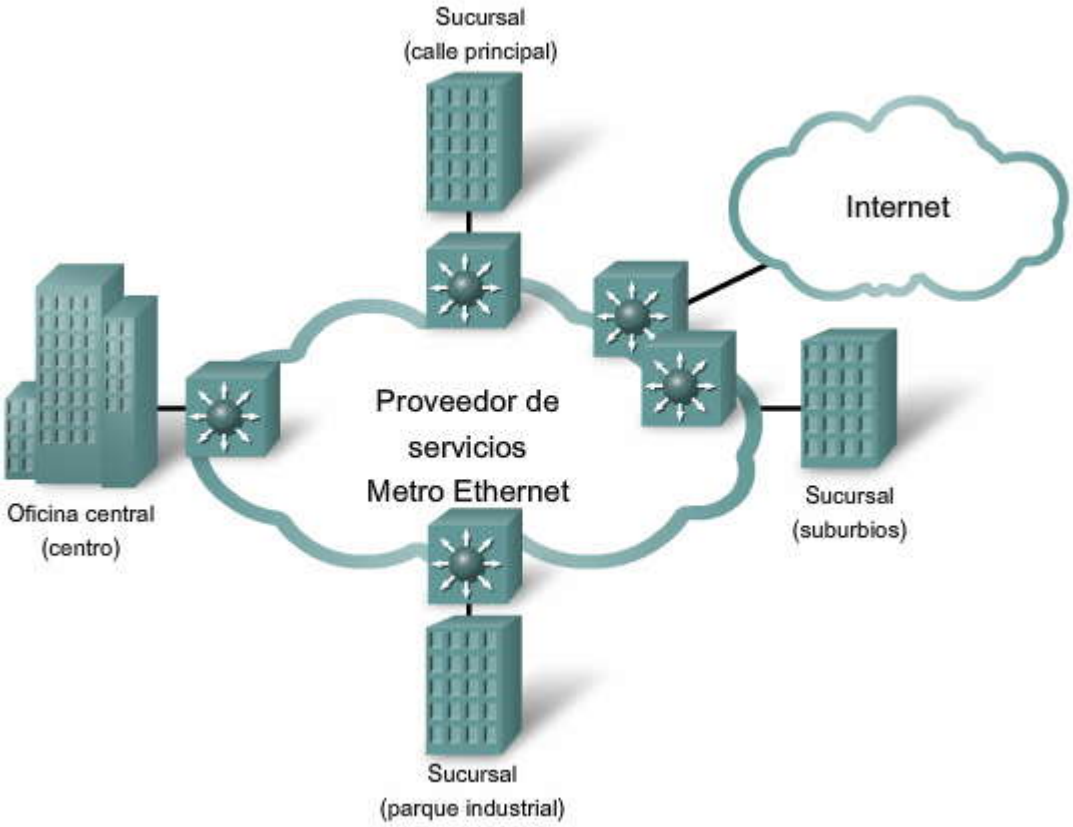


Metro Ethernet

Metro Ethernet es una tecnología de red que está avanzando con rapidez y que lleva Ethernet a las redes públicas mantenidas por empresas de telecomunicaciones. Utiliza switches Ethernet que leen la información IP y permiten a los proveedores de servicios ofrecer a las empresas servicios convergentes de voz, datos y video, por ejemplo, telefonía IP, streaming video, generación de imágenes y almacenamiento de datos. Al extender Ethernet al área metropolitana, las empresas pueden proporcionar a sus oficinas remotas un acceso confiable a las aplicaciones y los datos de la LAN de la sede principal corporativa.

Los beneficios de Metro Ethernet incluyen los siguientes:

- **Reducción de gastos y administración**: Metro Ethernet proporciona una red conmutada de Capa 2 de ancho de banda elevado que puede administrar datos, voz y video en la misma infraestructura. Esta característica aumenta el ancho de banda y elimina conversiones costosas a ATM y Frame Relay. La tecnología permite a las empresas conectar una gran cantidad de sitios de un área metropolitana entre sí y a Internet de manera económica.
- **Integración sencilla con redes existentes**: Metro Ethernet se conecta fácilmente con las LAN de Ethernet existentes, lo que reduce los costos y el tiempo de instalación.
- **Mayor productividad empresarial**: Metro Ethernet permite a las empresas aprovechar aplicaciones IP que mejoran la productividad y que son difíciles de implementar en redes TDM o Frame Relay, como comunicaciones IP por host, VoIP, streaming video y broadcast video.



Selección de una conexión de enlace WAN

Ahora que ya analizamos las diferentes opciones de conexión WAN, ¿cómo elegir la mejor tecnología para satisfacer los requisitos de una empresa en particular? En la imagen, se comparan las ventajas y las desventajas de las opciones de conexión WAN que analizamos en este capítulo. Esta información es un buen comienzo. Además, como ayuda para el proceso de toma de decisiones, incluimos algunas preguntas que debe hacerse al elegir una opción de conexión WAN.

¿Cuál es el propósito de la WAN?

¿Desea conectar sucursales locales de la misma ciudad, conectar sucursales remotas, conectarse a una única sucursal, conectarse con clientes, conectarse con socios comerciales o alguna combinación de estas opciones? Si la WAN se utilizará para proporcionar acceso limitado a la Intranet de la empresa a clientes o socios comerciales autorizados, ¿cuál es la mejor opción?

¿Cuál es el alcance geográfico?

¿Es local, regional, global, de uno a uno (única sucursal), de una a varias sucursales, de varias a varias (distribuido)? Según el alcance, algunas opciones de conexión WAN pueden ser mejores que otras.

¿Cuáles son los requisitos de tráfico?

Los requisitos de tráfico que se deben considerar son:

- El tipo de tráfico (sólo datos, VoIP, video, archivos grandes, streaming de archivos) determina los requisitos de calidad y rendimiento. Por ejemplo, si envía mucho tráfico de voz o streaming video, ATM puede ser la mejor opción.
- Los volúmenes de tráfico para cada destino, según el tipo (voz, video o datos), determinan la capacidad de ancho de banda necesaria para la conexión de la WAN al ISP.
- Los requisitos de calidad pueden limitar las opciones. Si el tráfico es muy sensible a la latencia y a la fluctuación de fase, puede eliminar todas las opciones de conexión WAN que no puedan proporcionar la calidad requerida.
- Los requisitos de seguridad (integridad, confidencialidad y seguridad de los datos) son otro factor importante si el tráfico es de naturaleza muy confidencial o si proporciona servicios esenciales, como respuesta en caso de emergencia.

¿La WAN debe utilizar una infraestructura privada o pública?

Una infraestructura privada ofrece la mejor seguridad y confidencialidad, mientras que la infraestructura pública de Internet ofrece una mayor flexibilidad y un menor gasto continuo. Su elección depende del propósito de la WAN, los tipos de tráfico que transporta y el presupuesto operativo disponible. Por ejemplo, si el propósito es proporcionar servicios seguros de alta velocidad a una sucursal cercana, la mejor opción puede ser una conexión conmutada o dedicada privada. Si el propósito es conectar muchas oficinas remotas, la mejor opción puede ser una WAN pública que utilice Internet. Para operaciones distribuidas, la solución puede ser una combinación de las opciones.

Para una WAN privada, ¿debe utilizarse una red dedicada o conmutada?

Las transacciones de gran volumen en tiempo real tienen requisitos especiales que pueden favorecer una línea dedicada, como el tráfico que se transmite entre el centro de datos y la oficina central corporativa. Si desea establecer una conexión con una única sucursal, puede utilizar una línea arrendada dedicada. Sin embargo, esta opción puede ser muy costosa para una WAN que se conecta con varias oficinas. En ese caso, una conexión conmutada puede ser mejor.

Para una WAN pública, ¿qué tipo de acceso VPN se necesita?

Si el propósito de la WAN es conectar una oficina remota, una VPN de sitio a sitio puede ser la mejor opción. Para conectar trabajadores a distancia o clientes, las VPN de acceso remoto son una mejor opción. Si la WAN presta servicios a una combinación de oficinas remotas, trabajadores a distancia y clientes autorizados, como en el caso de una empresa global con operaciones distribuidas, tal vez sea necesario utilizar una combinación de opciones de VPN.

¿Qué opciones de conexión están disponibles a nivel local?

En algunas áreas, no todas las opciones de conexión WAN están disponibles. En este caso, el proceso de selección se simplifica, aunque puede ocurrir que el rendimiento de la WAN resultante no sea el óptimo. Por ejemplo, en un árearemota rural, tal vez la única opción disponible sea el acceso a Internet satelital de banda ancha.

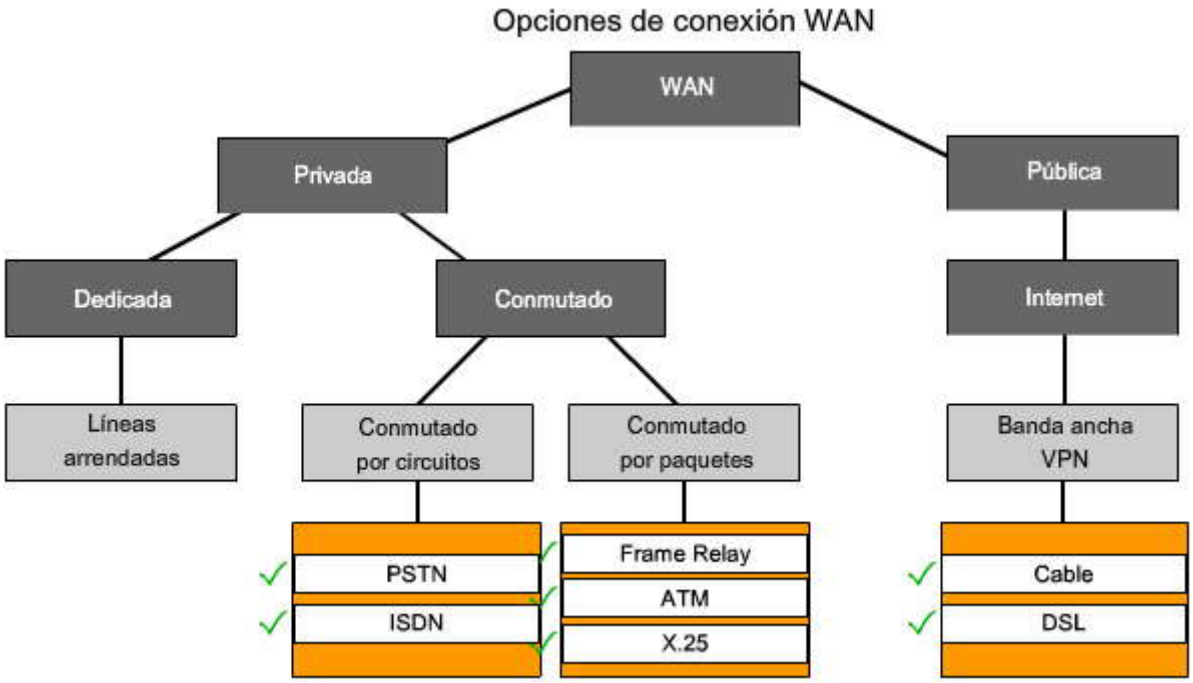
¿Cuál es el costo de las opciones de conexión disponibles?

Según la opción que seleccione, la WAN puede generar un gasto continuo importante. El costode una opción en particular debe evaluarse contra el grado de satisfacción de los demás requisitos. Por ejemplo, una línea arrendada dedicada es la opción más costosa, pero el gasto tal vez se justifique si es fundamental garantizar la transmisión segura de grandes cantidades de datos en tiempo real. Para aplicaciones que no son tan exigentes, tal vez sea más adecuada una opción de conexión conmutada o a través de Internet, que son más económicas.

Como puede ver, hay muchos factores importantes que se deben considerar al elegir una conexión WAN apropiada. Si sigue las pautas descritas anteriormente, así como las que se describen en la arquitectura empresarial de Cisco, debería poder elegir una conexión WAN apropiada para satisfacer los requisitos de diferentes situaciones empresariales.

Elección de una conexión de enlace WAN

Opción	Descripción	Ventajas	Desventajas	Protocolos modelos utilizados
Línea arrendada	Conexión punto a punto entre dos computadoras o redes de área local (LAN).	La más segura	Costosa	PPP, HDLC, SDLC, HNAS
Conmutación de circuitos	Se crea una ruta de circuitos dedicada entre los extremos. El mejor ejemplo son las conexiones dialup.	Menos costosa	Configuración de llamada	PPP, ISDN
Conmutación de paquetes	Los dispositivos transportan paquetes a través un único enlace compartido punto a punto o punto a multipunto a través de la red de la portadora. Se transmiten paquetes de longitud variable a través de circuitos virtuales permanentes (PVC, permanent virtual circuits) o circuitos virtuales conmutados (SVC, switched virtual circuits).		Medio compartido a través del enlace	X.25, Frame Relay
Relay de celda	Similar a la conmutación de paquetes, pero usa celdas de longitud fija en lugar de paquetes de longitud variable. Los datos se dividen en celdas de longitud fija y se transportan a través de circuitos virtuales	ideal para el uso simulado de voz y datos	La carga puede ser considerable.	ATM
Internet	Conmutación de paquetes sin conexión mediante el uso de Internet como infraestructura de la WAN. Se utiliza el direccionamiento de la red para entregar paquetes. Debido a cuestiones de seguridad, se debe usar la tecnología VPN.	Menos costosa, disponible en todo el mundo	La menos segura	VPN, DSL, módem por cable, inalámbrica



1.4 Prácticas de laboratorio del capítulo

1.4.1 Repaso del reto

En esta práctica de laboratorio repasará conceptos básicos de enrutamiento y conmutación. Intente hacer lo más posible por su cuenta. Cuando no pueda avanzar por su cuenta, consulte el material previo.

Nota: La configuración de tres protocolos de enrutamiento independientes (RIP, OSPF y EIGRP) para enrutar la misma red no se considera una mejor práctica en absoluto. Debe considerarse como una peor práctica y no es algo que se haría en una red de producción. Aquí lo hacemos para que usted pueda repasar los principales protocolos de enrutamiento antes de continuar y para que vea una ilustración drástica del concepto de distancia administrativa.

1.5 Resumen del capítulo

1.5.1 Resumen del capítulo

Una WAN es una red de comunicación de datos que opera más allá del alcance geográfico de una LAN.

A medida que las empresas crecen, incorporan más empleados, abren sucursales y se expanden a mercados globales, sus requisitos de servicios integrados cambian. Estos requisitos comerciales determinan los requisitos de la red.

La arquitectura empresarial de Cisco expande el modelo de diseño jerárquico mediante la subdivisión de la red empresarial en las áreas física, lógica y funcional.

La implementación de una arquitectura empresarial de Cisco proporciona una red segura y sólida de alta disponibilidad que facilita la implementación de redes convergentes.

Las WAN funcionan en relación con el modelo de referencia OSI, principalmente en la Capa 1 y la Capa 2.

Los dispositivos que colocan los datos en el bucle local se denominan equipos de terminación de circuito de datos o equipos de comunicación de datos (DCE). Los dispositivos del cliente que transmiten datos al DCE se llaman equipo terminal de datos (DTE). El DCE principalmente suministra una interfaz para el DTE hacia el enlace de comunicación en la nube WAN.

El punto de demarcación física es donde la responsabilidad de la conexión pasa de la empresa al proveedor de servicios.

Los protocolos de la capa de enlace de datos definen cómo se encapsulan los datos para su transmisión a lugares remotos, así como también los mecanismos de transferencia de las tramas resultantes.

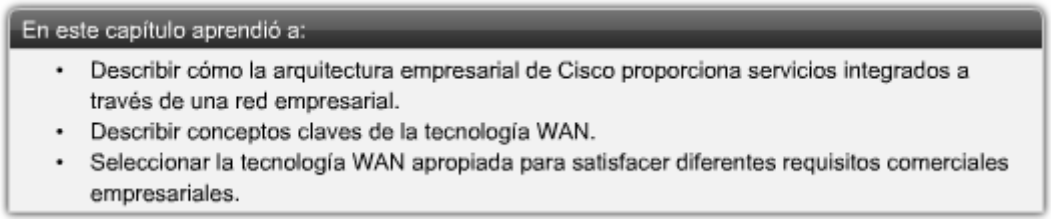
Una red de conmutación de circuitos establece un circuito (o canal) dedicado entre los nodos y las terminales antes de que los usuarios puedan comunicarse.

Una red conmutada por paquetes divide los datos del tráfico en paquetes que se envían a través de una red compartida. Las redes de conmutación de paquetes no requieren que se establezca un circuito y permiten que muchos pares de nodos se comuniquen a través del mismo canal.

Un enlace punto a punto ofrece rutas de comunicación WAN preestablecidas desde las instalaciones del cliente a través de la red del proveedor hasta un destino remoto. Los enlaces punto a punto utilizan líneas arrendadas para proporcionar una conexión dedicada.

Las opciones de WAN por conmutación de circuitos incluyen el acceso telefónico analógico e ISDN. Las opciones de WAN por conmutación de paquetes incluyen X.25 Frame Relay y ATM. ATM transmite datos en celdas de 53 bytes en lugar de utilizar tramas. ATM es más adecuado para tráfico de video.

Las opciones de conexión de WAN a través de Internet incluyen servicios de banda ancha, como DSL, módem por cable o conexión inalámbrica de banda ancha y Metro Ethernet. La tecnología VPN permite a las empresas proporcionar acceso seguro a los trabajadores a distancia a través de Internet mediante servicios de banda ancha.



Esta actividad abarca muchas de las habilidades que adquirió en los primeros tres cursos de Exploration. Las habilidades incluyen la construcción de una red, la aplicación de un esquema de direccionamiento, la configuración del enrutamiento, VLAN, STP y VTP y la prueba de la conectividad. Debe repasar estas habilidades antes de continuar. Además, esta actividad le brinda la oportunidad de repasar los aspectos básicos del programa Packet Tracer. Packet Tracer se integra durante este curso. Debe saber cómo navegar en el entorno de Packet Tracer para completar este curso. Use los tutoriales si necesita revisar los principios fundamentales de Packet Tracer, estos se encuentran en el menú Ayuda de Packet Tracer.

Las instrucciones detalladas se encuentran dentro de la actividad, al igual que en el enlace al PDF a continuación.
Instrucciones de la actividad (PDF)

Haga clic en el icono de Packet Tracer para obtener más detalles.

CAPITULO II – "PPP"

2.0 Introducción del capítulo

2.0.1 Introducción del capítulo

Este capítulo es el inicio de su exploración a las tecnologías WAN mediante la introducción a las comunicaciones punto a punto y el protocolo punto a punto (PPP, Point-to-Point Protocol).

Una de las conexiones WAN más frecuentes es la conexión punto a punto. Las conexiones punto a punto se utilizan para conectar las LAN a las WAN del proveedor de servicio y para conectar los segmentos LAN dentro de la red empresarial. La conexión punto a punto entre una LAN y una WAN también se conoce como conexión serial o en línea arrendada, ya que estas líneas se alquilan a una empresa de comunicaciones (por lo general un compañía telefónica) y su uso es exclusivo de la empresa que solicita el alquiler. Las empresas pagan para obtener una conexión continua entre dos sitios remotos, y la línea se mantiene activa y disponible en todo momento. La comprensión del funcionamiento de los enlaces de comunicaciones punto a punto para brindar acceso WAN es importante para la comprensión general del funcionamiento de las WAN.

El protocolo punto a punto (PPP) proporciona conexiones multiprotocolo entre LANy WAN que manejan TCP/IP, IPX y AppleTalk al mismo tiempo. Puede emplearse a través de par trenzado, líneas de fibra óptica y transmisión satelital. El PPP proporciona el transporte a través del modo de ATM, Frame Relay, ISDN y los enlaces ópticos. En las redes modernas, la seguridad es un aspecto clave. El PPP le permite autenticar las conexiones mediante el uso del protocolo de autenticación de contraseña (PAP, Password Authentication Protocol) o el más eficaz protocolo de autenticación de intercambio de señales (CHAP, Challenge Handshake Authentication Protocol). Este aspecto se enseñará en la sección cuatro.

Además, en este capítulo aprenderá los conceptos clave de las comunicaciones seriales y cómo configurar y resolver los problemas de una conexión serial PPP en un router de Cisco.

En este capítulo, aprenderá a:

- Describir los conceptos fundamentales de la comunicación serial punto a punto.
- Describir los conceptos claves acerca del PPP.
- Configurar la encapsulación PPP.
- Explicar y configurar la autenticación PAP y CHAP.

2.1 Enlaces seriales punto a punto

2.1.1 Introducción a las comunicaciones seriales

¿Cómo funciona la comunicación serial?

Ya sabe que la mayoría de las PC cuentan con puertos paralelos y seriales. También sabe que la electricidad sólo puede desplazarse en una velocidad. Una forma de obtener bits para desplazarse más rápidamente a través del cable es comprimir los datos de manera que se reduzcan la cantidad de bits y se requiera menos tiempo en el cable. Otra posibilidad para aumentar la velocidad es transmitir simultáneamente los bits. Aunque las computadoras utilizan conexiones paralelas relativamente cortas entre los componentes interiores, emplean unbus serial para convertir las señales para la mayoría de las conexiones externas.

Comparemos las comunicaciones seriales y paralelas.

Haga clic en el botón Serial y paralelo para ver la animación.

- Con una conexión serial, la información se envía a través de un cable, un bit de datos a la vez. El conector serial de 9 pins de la mayoría de las computadoras emplea dos bucles de cable, uno en cada dirección, para la comunicación de datos, y cables adicionales para controlar el flujo de información. Independientemente de la dirección que se siga, los datos se transmiten a través de un solo cable.
- Una conexión paralela envía simultáneamente los bits a través de más cables. En el caso del puerto paralelo de 25 pins de su computadora, hay ochos cables que transmiten datos para transmitir 8 bits simultáneamente. Debido a que hay ocho cables que transmiten datos, el enlace paralelo, en teoría, transfiere los datos ocho veces más rápido que una conexión serial. De manera que, según esta teoría, el tiempo que tarda una conexión paralela para enviar un byte es el mismo que tarda una conexión serial para enviar un bit.

Esta explicación trae por consecuencia algunas preguntas. ¿Qué significa teóricamente más rápido? Si la conexión paralela es más rápida que la serial, ¿es la más apropiada para realizar una conexión a una WAN? En realidad, a menudo, los enlaces seriales pueden cronometrarse considerablemente más rápido que los enlaces paralelos y logran una mayor velocidad para la transmisión de datos debido a dos factores que afectan las comunicaciones paralelas: lainterferencia por sesgo de reloj y crosstalk.

Haga clic en el botón Sesgo de reloj que se muestra en la imagen.

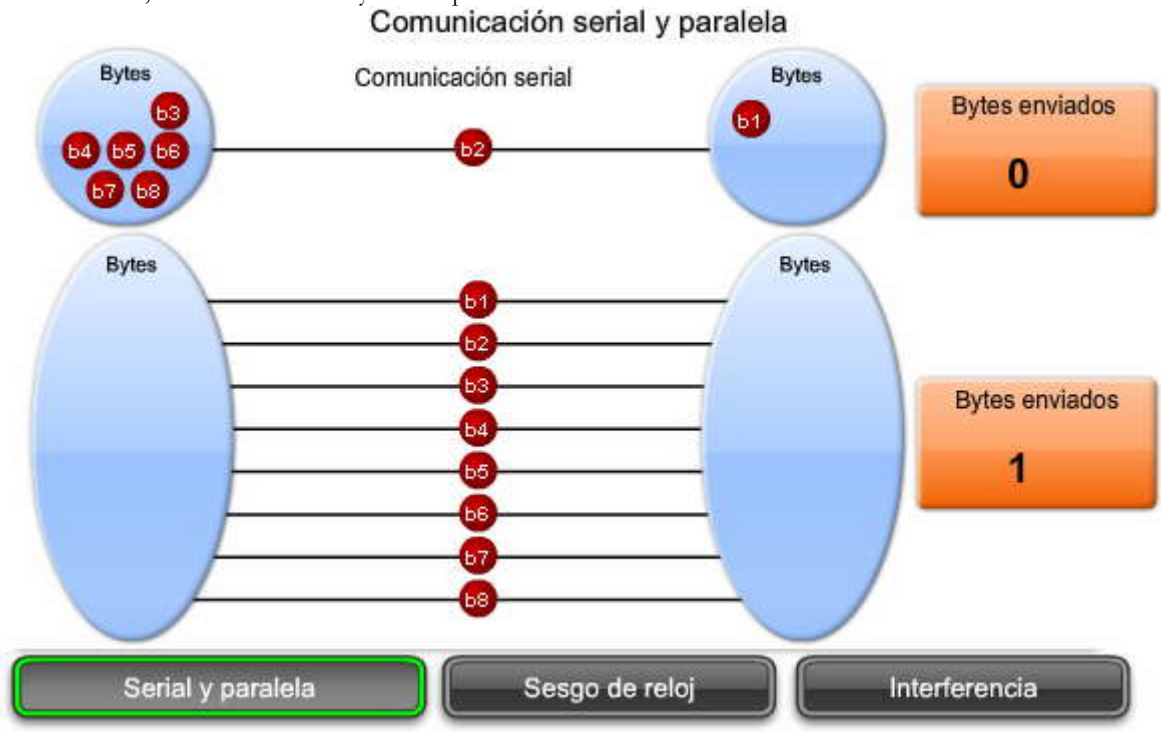
En una conexión paralela, es incorrecto presuponer que los 8 bits que envía el emisor al mismo tiempo llegan al receptor de manera simultánea. En realidad, algunos de los bits llegan más tarde que el resto. Esto se conoce como sesgo de reloj. La superación del sesgo de reloj no es una tarea intrascendente. El extremo receptor debe sincronizarse con el transmisor y, luego, esperar hasta que todos los bits hayan llegado. El proceso de lectura, espera, cierre, espera para la señal de reloj y la transmisión de los 8 bits aumentan el tiempo de transmisión. En las comunicaciones paralelas, un pestillo es un sistema de almacenamiento de datos usado para guardar información en los sistemas lógicos secuenciales. Cuanto más hilos se utilicen y cuanto mayor sea el alcance de la conexión, se complica más el problema y aumenta el retardo. La necesidad de temporización reduce la transmisión paralela mucho más de lo que, en teoría, se espera.

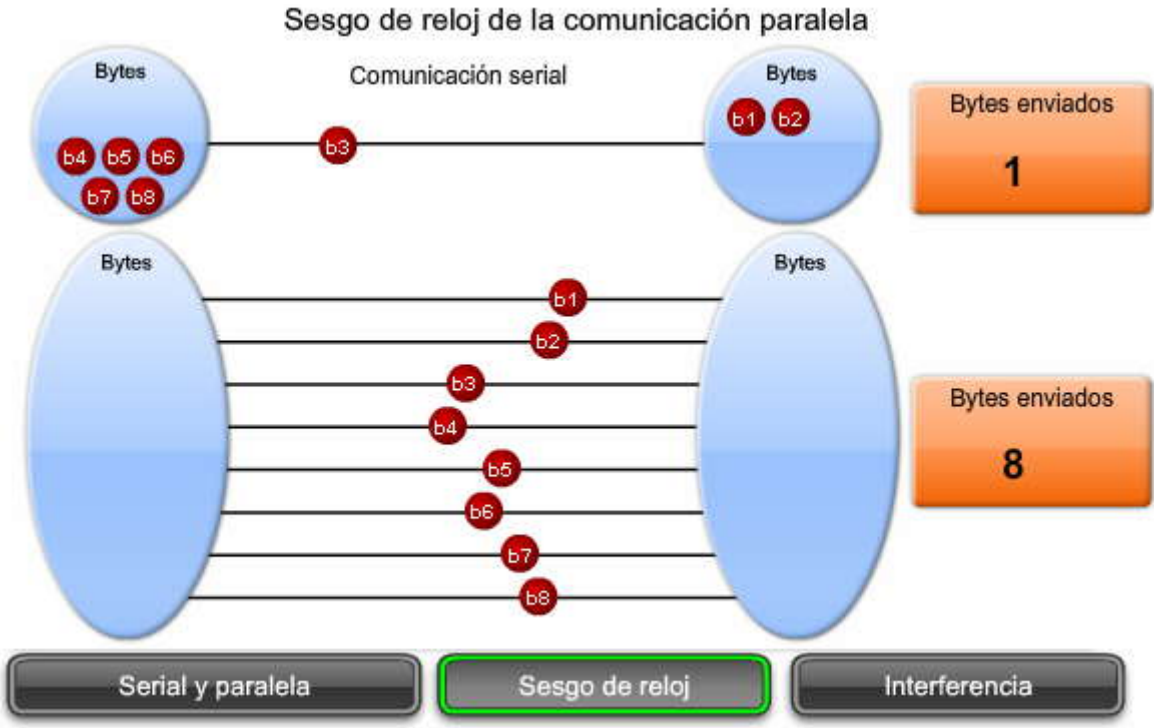
Este factor no se aplica a los enlaces seriales, ya que la mayoría de estos no necesitan temporización. Las conexiones seriales requieren menos hilos y cables. Ocupan menos espacio y pueden aislarse mejor de las interferencias producidas por otros hilos y cables.

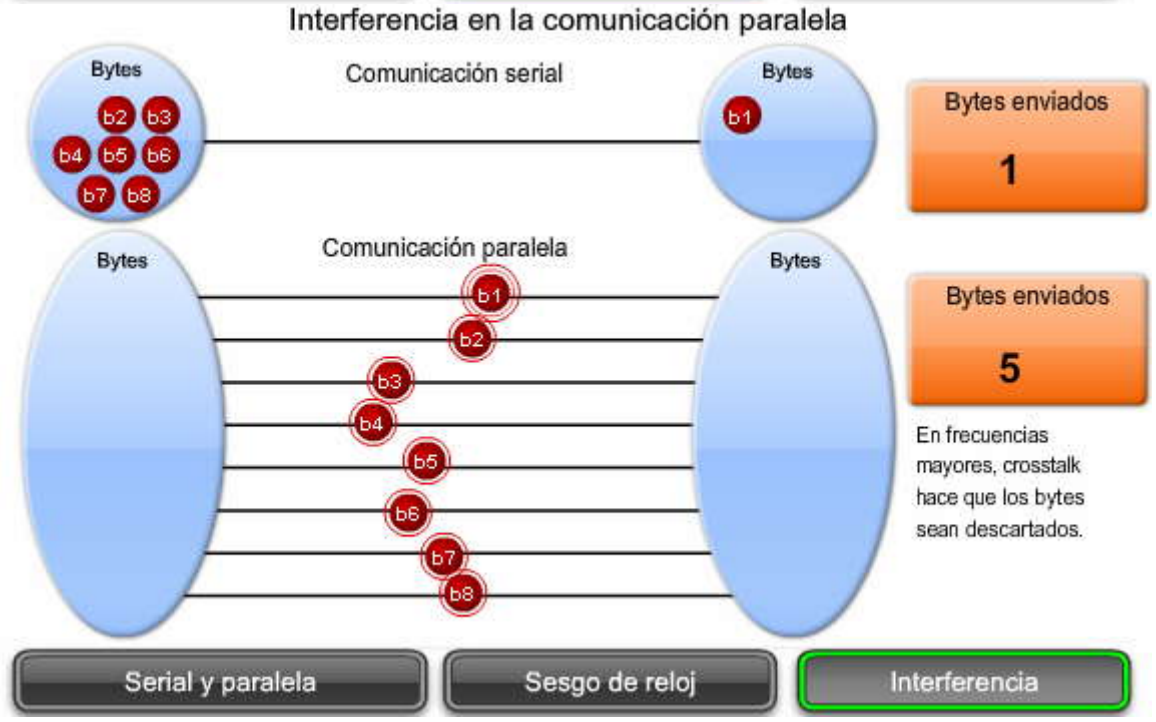
Haga clic en el botón Interferencia que se muestra en la imagen.

Los hilos paralelos se agrupan físicamente en manojos en un cable paralelo y las señales pueden marcarse entre ellas. La posibilidad de crosstalk a través de los hilos implica más procesamiento, especialmente a frecuencias más altas. Los buses seriales de las computadoras, como los routers, compensan el crosstalk antes de la transmisión de bits. Debido a que los cables seriales tienen menos hilos, hay menos crosstalk y los dispositivos de red transmiten comunicaciones serial es a frecuencias más altas y más eficaces.

En la mayoría de los casos, las comunicaciones seriales son considerablemente más económicas. Las comunicaciones seriales utilizan menos hilos, cables más baratos y menos pins conectores.







Estándares de comunicación serial

Todas las comunicaciones de largo alcance y la mayoría de las redes informáticas utilizan conexiones seriales, ya que el costo del cable y las dificultades de la sincronización hacen que las conexiones paralelas no sean prácticas. La ventaja más importante es que el cableado es más sencillo. Además, los cables seriales pueden ser más extensos que los cables paralelos, ya que hay menos interacción (crosstalk) entre los conductores del cable. En este capítulo, concentraremos nuestro interés en las comunicaciones seriales que conectan las LAN y WAN.

La imagen es una representación sencilla de un comunicación serial. Los datos se encapsulan mediante el protocolo de comunicación utilizado por el router emisor. La trama encapsulada se envía en un medio físico hacia la WAN. Aunque hay varias maneras de atravesar la WAN, el router emisor utiliza el mismo protocolo de comunicaciones para desencapsular la trama cuando ésta llega.

Hay numerosos estándares de comunicación serial diferentes y cada uno utiliza un método de señalización distinto. Hay tres estándares de comunicación serial claves que afectan las conexiones entre LAN y WAN:

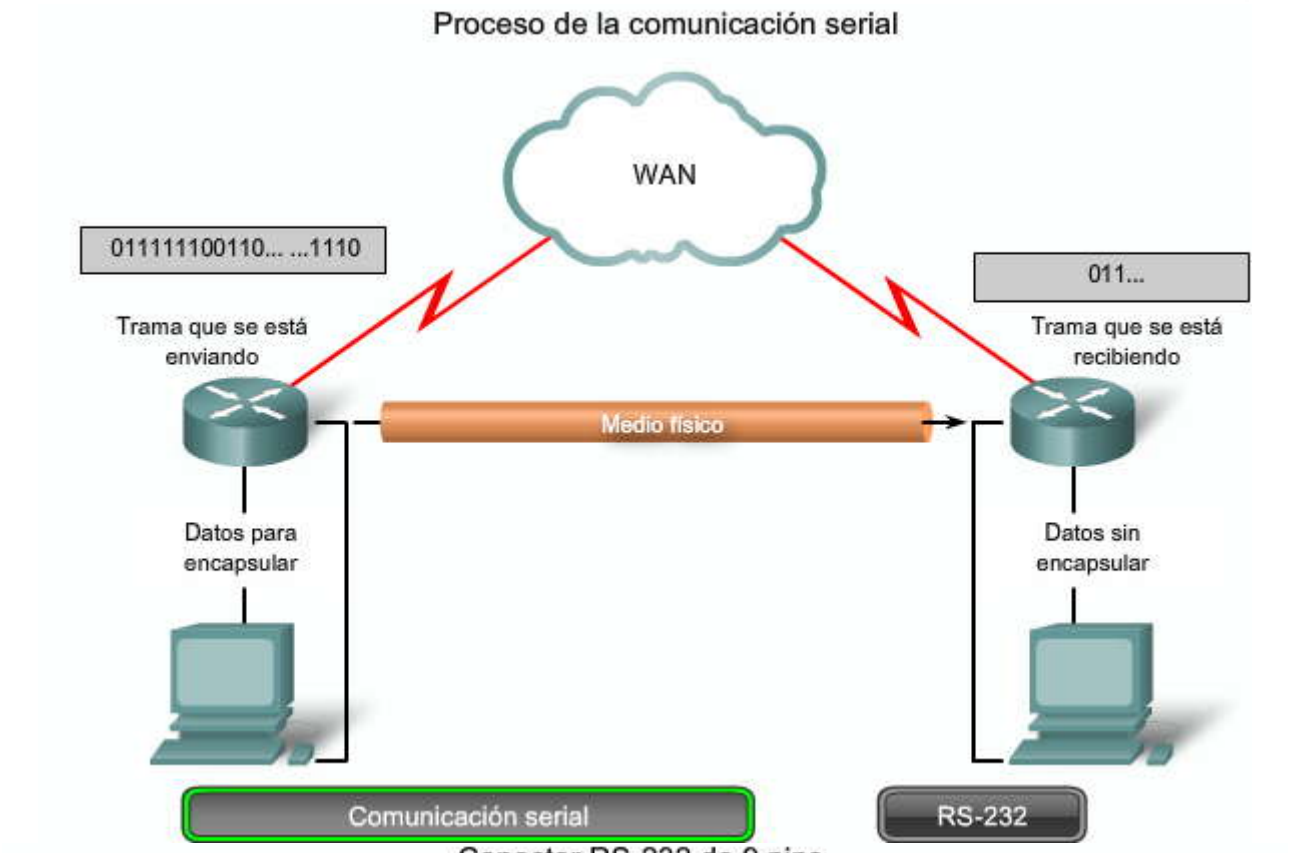
- **RS-232**: la mayoría de los puertos seriales en las computadoras personales cumplen con los estándares RS-232C o los más recientes RS-422 y RS-423. Se utilizan los conectores de 9 y 25 pins. Un puerto serial es una interfaz de aplicación general que puede utilizarse para casi cualquier tipo de dispositivo, como módems, mouse e impresoras. Muchos de los dispositivos de red utilizan conectores RJ-45 que también cumplen con el estándar RS-232. La imagen muestra un ejemplo de un conector RS-232.
- **V.35**: este estándar de la Unión Internacional de Telecomunicaciones (ITU, International Telecommunication Union) para el intercambio de datos síncronos y de alta velocidad que, por lo general, se utiliza para la comunicación entre el módem y el multiplexor, combina el ancho de banda de varios circuitos telefónicos. En los Estados Unidos, V.35 es el estándar de interfaz que se emplea en la mayoría de los routers y DSU que se conectan a las portadoras T1. Los cables V.35 son conjuntos seriales de alta velocidad diseñados para admitir velocidades de transmisión de datos más altas y la conectividad entre los DTE y los DCE en las líneas digitales. Más adelante, en este mismo capítulo, se incluirá más información acerca de los DTE y DCE.
- **HSSI**: la interfaz serial de alta velocidad (HSSI, High-Speed Serial Interface) admite velocidades de transmisión de hasta 52 Mbps. Los ingenieros utilizan la HSSI para conectar routers en las LAN con las WAN mediante líneas de alta velocidad como las líneas T3. Los ingenieros también utilizan la HSSI para proporcionar conectividad de alta velocidad entre las LAN mediante Token Ring o Ethernet. HSSI es una interfaz DTE/DCE desarrollada por Cisco Systems y sistema de redes T3plus para cubrir las necesidades de comunicación de alta velocidad mediante enlaces WAN.

Haga clic en el botón RS-232 que se muestra en la imagen.

Además de utilizar diferentes métodos de señalización, cada uno de estos estándares utiliza diferente tipos de cables y conectores. Cada estándar juega un papel distinto en la topología entre LAN y WAN. Aunque este curso no examina los detalles de los esquemas de pins de V.35 y HSSI, un rápido vistazo a un conector RS-232 de 9 pins utilizado para conectar una computadora a un módem permite ejemplificar el concepto. Un tema que se tratará más adelante analiza los cables V.35 y HSSI.

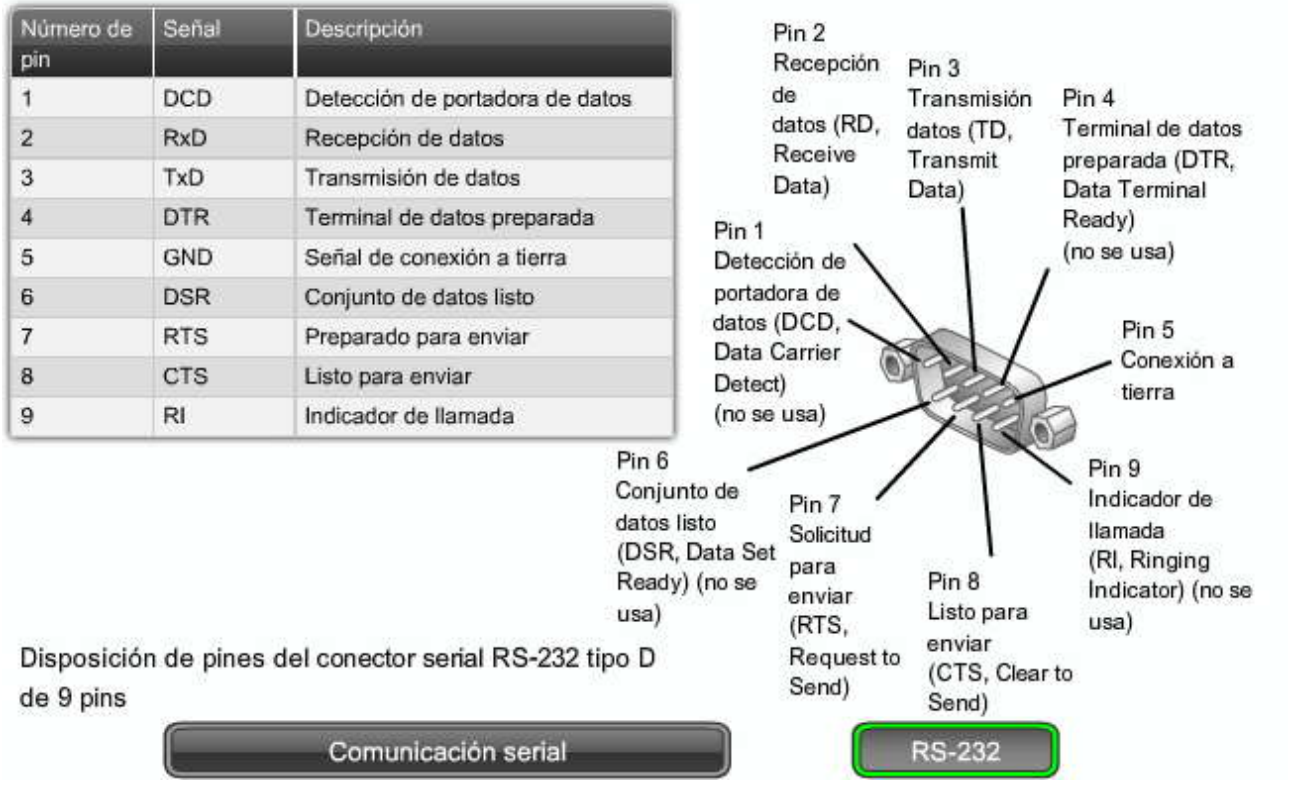
- Pin 1: la detección de portadora de datos (DCD, Data Carrier Detect) indica que la portadora para los datos de transmisión está ACTIVADA.
- Pin 2: el pin de recepción (RXD) transmite datos desde el dispositivo serial hasta la computadora.
- Pin 3: el pin de transmisión (TxD) transmite datos desde la computadora hasta el dispositivo serial.
- Pin 4: la terminal de datos preparada (DTR, Data Terminal Ready) le indica al módem que la computadora está lista para transmitir.
- Pin 5: conexión a tierra.
- Pin 6: el conjunto de datos listo (DSR, Data Set Ready) es similar a DTR. Indica que el conjunto de datos está ACTIVADO.
- Pin 7: el pin Solicitud para enviar (RTS) solicita espacio libre para enviar los datos a un módem.
- Pin 8: el dispositivo serial utiliza el pin listo para enviar (CTS, Clear to Send) para acusar recibo de la señal RTS de la computadora. En casi todos los casos, RTS y CTS están ACTIVADOS durante toda la sesión de la comunicación.
- Pin 9: un módem de respuesta automática utiliza el indicador de llamada (RI, Ring Indicator) para indicar la recepción de una señal de llamada telefónica.

Los pins DCD y RI sólo están disponibles en las conexiones con un módem. Estas dos líneas rara vez se utilizan, ya que la mayoría de los módems transmiten información del estado hacia la computadora cuando se detecta la señal de una portadora (cuando se realiza una conexión hacia otro módem) o cuando el módem recibe una señal de llamada desde la línea telefónica.



Conector RS-232 de 9 pins

Número de pin	Señal	Descripción
1	DCD	Detección de portadora de datos
2	RxD	Recepción de datos
3	TxD	Transmisión de datos
4	DTR	Terminal de datos preparada
5	GND	Señal de conexión a tierra
6	DSR	Conjunto de datos listo
7	RTS	Preparado para enviar
8	CTS	Listo para enviar
9	RI	Indicador de llamada



2.1.2 TDM

Multiplexación por división temporal

Bell Laboratories creó la multiplexación por división temporal (TDM, Time Division Multiplexing) para maximizar el flujo de tráfico de voz que se transmite mediante un medio. Antes de la multiplexación, cada llamada telefónica solicitaba su propio enlace físico. Esta solución era costosa y difícil de implementar. La TDM divide el ancho de banda de un solo enlace en canales separados o en periodos de tiempo. La TDM transmite dos o más canales a través del mismo enlace mediante la

asignación de diferentes intervalos de tiempo (periodo de tiempo) para la transmisión de cada canal. En efecto, los canales se turnan para emplear el enlace.

TDM es un concepto de capa física. No considera la naturaleza de la información que se somete a la multiplexación en el canal de salida. La TDM es independiente del protocolo de Capa 2 que utilizaron los canales de entrada.

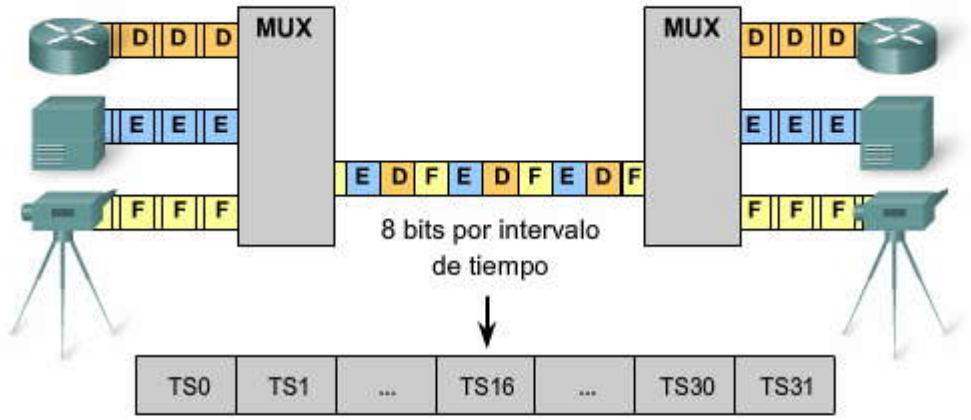
La TDM puede explicarse por analogía al tráfico de autopistas. Para transportar el tráfico desde cuatro rutas a otra ciudad, puede enviar todo el tráfico por un solo carril si las rutas de alimentación cuentan con el mismo flujo de tráfico y si éste está sincronizado. De manera que, si cada una de las cuatro rutas coloca un automóvil en la autopista principal cada cuatro segundos, la autopista obtendrá un vehículo a la velocidad de uno por segundo. Siempre y cuando la velocidad de los automóviles esté sincronizada, no habrá colisión. En el destino, sucede lo contrario y los automóviles son retirados de la autopista y se les coloca en las rutas locales mediante el mismo mecanismo síncrono.

Este es el principio que se utiliza en la TDM síncrona al enviar los datos mediante un enlace. La TDM aumenta la capacidad del enlace de transmisión mediante la división del tiempo en intervalos más cortos, de manera que el enlace transmita los bits desde diferentes fuentes de entrada. Esto aumenta, con efectividad, la cantidad de bits transmitidos por segundo. Con la TDM, tanto el transmisor como el receptor saben exactamente cuál es la señal que se envía.

En nuestro ejemplo, el multiplexor (MUX) del transmisor admite tres señales diferentes. El MUX divide cada señal en segmentos. Coloca cada segmento en un solo canal y los inserta en un periodo de tiempo.

En el extremo receptor, un MUX reensambla el stream de TDM en tres flujos de datos, tomando como única referencia el tiempo que tarda cada bit en llegar. Una técnica llamada entrelazado rastrea la cantidad y la secuencia de los bits desde cada transmisión específica, de manera que puedan reensamblarse con rapidez y eficacia para volver a su forma original después de llegar al destino. Aunque el entrelazado de byte realiza la misma función, debido a que hay ocho bits en cada byte, el proceso requiere un periodo de tiempo más largo.

Multiplexación por división temporal

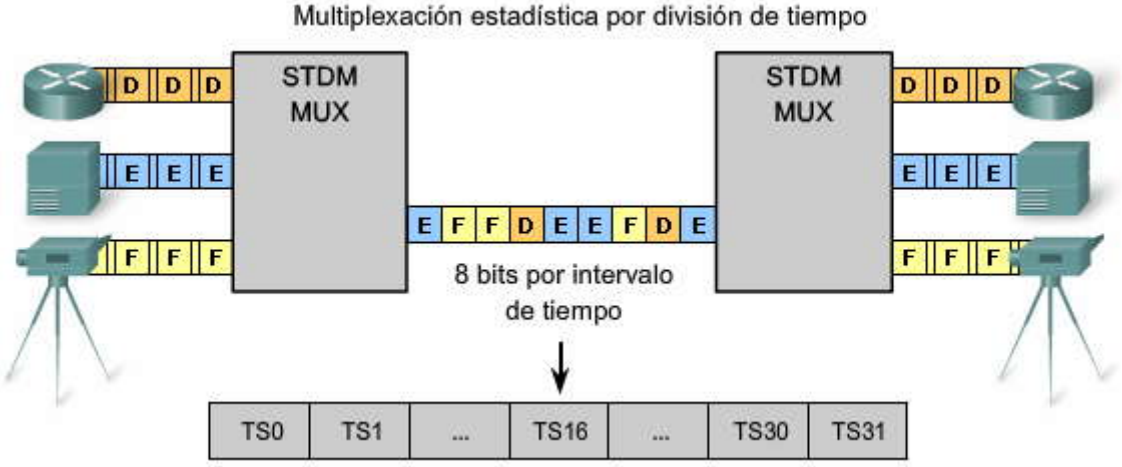


- La multiplexación por división temporal (TDM, Time Division Multiplexing) comparte tiempo de transmisión disponible en un medio al asignar intervalos de tiempo a usuarios.
- El multiplexor (MUX) acepta entradas desde dispositivos conectados en cadena y trasmite los datos de manera interminable.
- Las líneas telefónicas T1/E1 y la red digital de servicios integrados (ISDN, Integrated Services Digital Network) son ejemplos comunes de la TMD síncrona.

Multiplexación estadística por división temporal

Como otra analogía, compare la TDM con 32 vagones de un tren. Cada uno es propiedad de una empresa de transporte diferente y todos los días el tren parte con los 32 vagones. Si una de las empresas tiene una carga que enviar, el vagón se carga. Si la empresa no tiene nada que enviar, el vagón permanece vacío, pero sigue siendo parte del tren. No es rentable transportar contenedores vacíos. La TDM comparte esta deficiencia cuando el tráfico es intermitente, ya que, incluso en este caso, se asigna un periodo de tiempo cuando el canal no tiene datos para transmitir.

Multiplexación estadística por división temporal (STDM, Statistical time-division multiplexing) fue diseñada para superar esta deficiencia. La STDM utiliza una extensión variable para el periodo de tiempo, lo que permite que los canales compitan para obtener cualquier espacio libre del periodo. Utiliza un búfer de memoria que almacena temporalmente los datos durante los periodos correspondientes a las horas picos de tráfico. La STDM no desperdicia el tiempo de la línea de alta velocidad con canales inactivos con este esquema. La STDM exige que cada transmisión transmita la información de identificación (un identificador de canal).



Ejemplos de TDM: ISDN y SONET

Un ejemplo de una tecnología que utiliza TDM síncrono es ISDN. El acceso básico (BRI) ISDN cuenta con tres canales que constan de dos canales B de 64 kbps (B1 y B2) y un canal D de 16 kbps. La TDM tiene nueve intervalos de tiempo, que están separados según la secuencia que se muestra en la imagen.

En mayor escala, la industria de las telecomunicaciones utiliza el estándar SONET o SDH para el transporte óptico de los datos de TDM. La red SONET utilizada en América del Norte, y la SDH, utilizada en otros lugares, son dos estándares estrechamente relacionados que especifican los parámetros de interfaz, las velocidades, los formatos de trama, los métodos de multiplexación y la administración para TDM síncrona en fibra óptica.

Haga clic en el botón SONET que se muestra en la imagen.

La imagen muestra un ejemplo de TDM estadística. SONET/SDH toma streams de bits n, realiza la multiplexación de estos y modula óptimamente la señal enviándola mediante un dispositivo emisor de luz a través de la fibra con una velocidad de bits igual a (velocidad de bits de entrada) x n. Así, el tráfico que llega al multiplexor SONET desde cuatro lugares a 2.5 Gbps, sale como un solo stream a 4 x 2.5 Gbps o 10 Gbps. Este principio se ejemplifica en la imagen, la cual muestra un aumento en la velocidad de bits por un factor de 4 en el intervalo de tiempo T.

Haga clic en el botón DS0 que se muestra en la imagen.

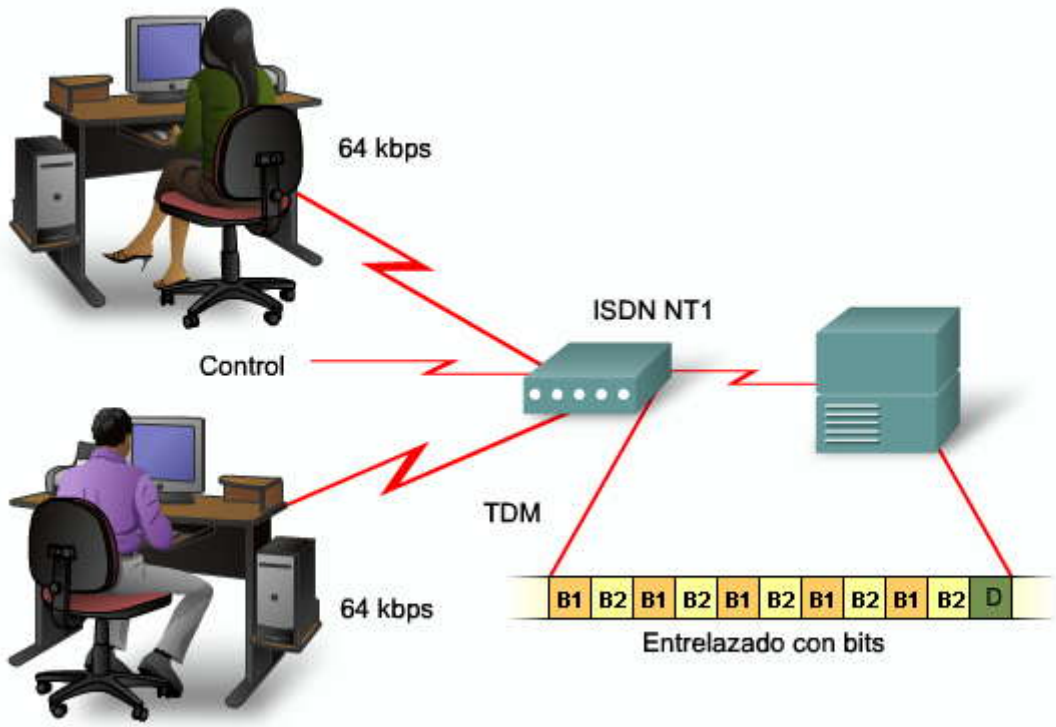
La unidad original utilizada en las llamadas telefónicas de multiplexación es 64 kbps, lo que representa una llamada telefónica. Se le denomina DS0 (señal digital de nivel cero). En América del Norte, 24 unidades DS0 se someten a la multiplexación mediante la TDM en una señal cuya velocidad de bits es mayor. La velocidad incorporada es de 1.544 Mbps para las transmisiones a través de las líneas T1. Fuera de América del Norte, 32 unidades DS0 se someten a la multiplexación para la transmisión E1 a 2.048 Mbps.

La jerarquía del nivel de la señal para la multiplexación telefónica se muestra en la tabla. Al margen de esto, aunque, por lo general, a la transmisión a 1.544 Mbps se le conoce como T1, es más correcto llamarla DS1.

Haga clic en el botón Jerarquía de la portadora T que se muestra en la imagen.

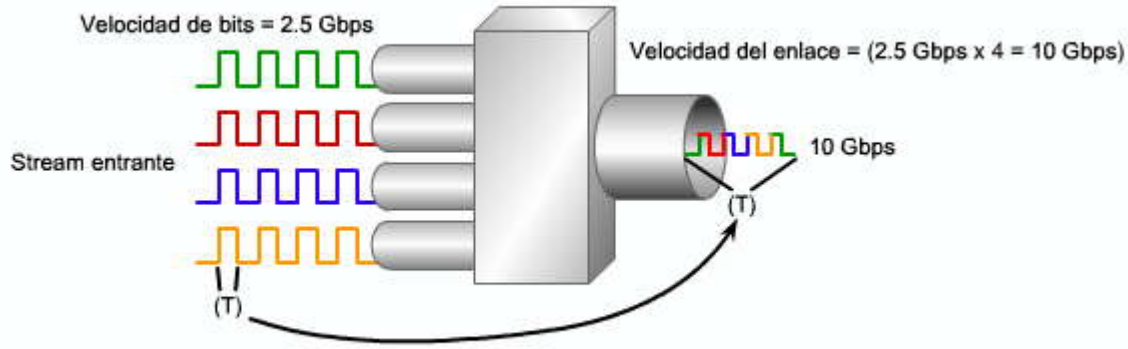
La portadora T hace referencia a la combinación de las DS0. Por ejemplo, un T1 = 24 DS0, un T1C = 48 DS0 (o 2 T1) y así sucesivamente. La imagen muestra un ejemplo de la jerarquía de infraestructura de la portadora T. La jerarquía de la portadora E es similar.

Ejemplo de TDM: ISDN



ISDN | SONET | DS0 | Jerarquía de la portadora T

Ejemplo de TDM: SONET

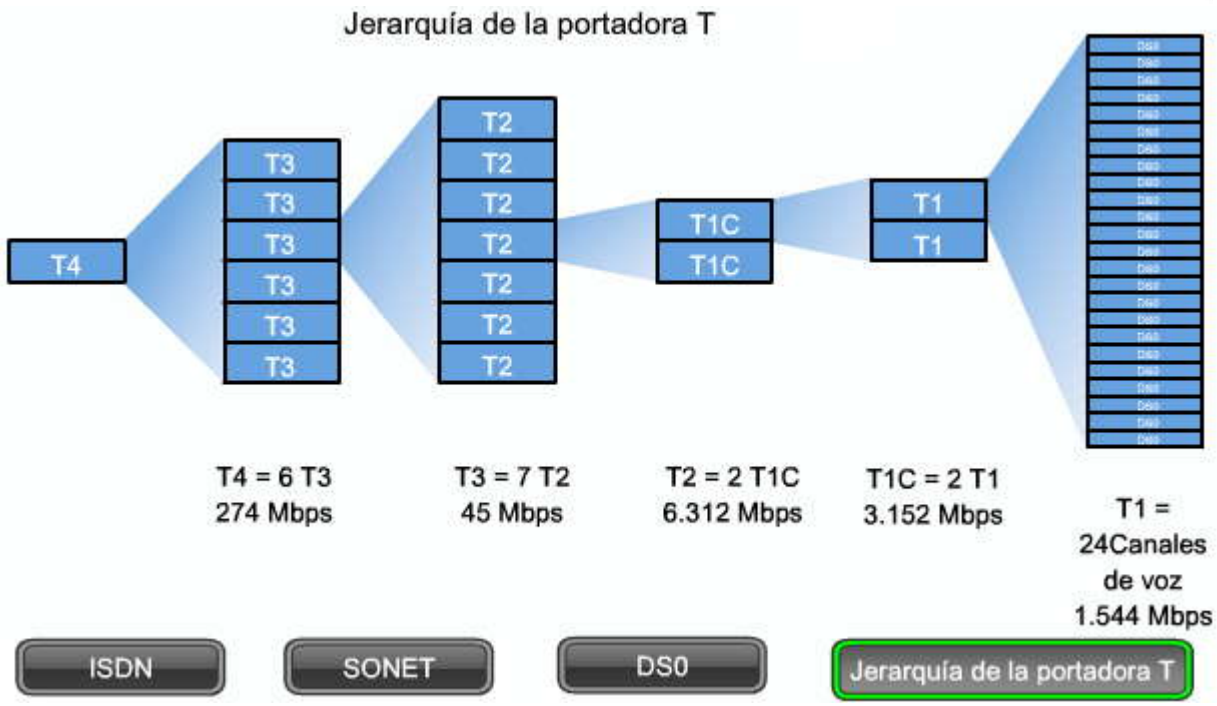


ISDN | SONET | DS0 | Jerarquía de la portadora T

UNIDADES DS0

Bit de señal	Velocidad	Ranuras de voz
DS0	64 kbps	1 DS0
DS1	1.544 Mbps	24 DS0
DS2	6.312 Mbps	96 DS0
DS3	44.736 Mbps	672 DS0 o 28 DS1

ISDN | SONET | DS0 | Jerarquía de la portadora T

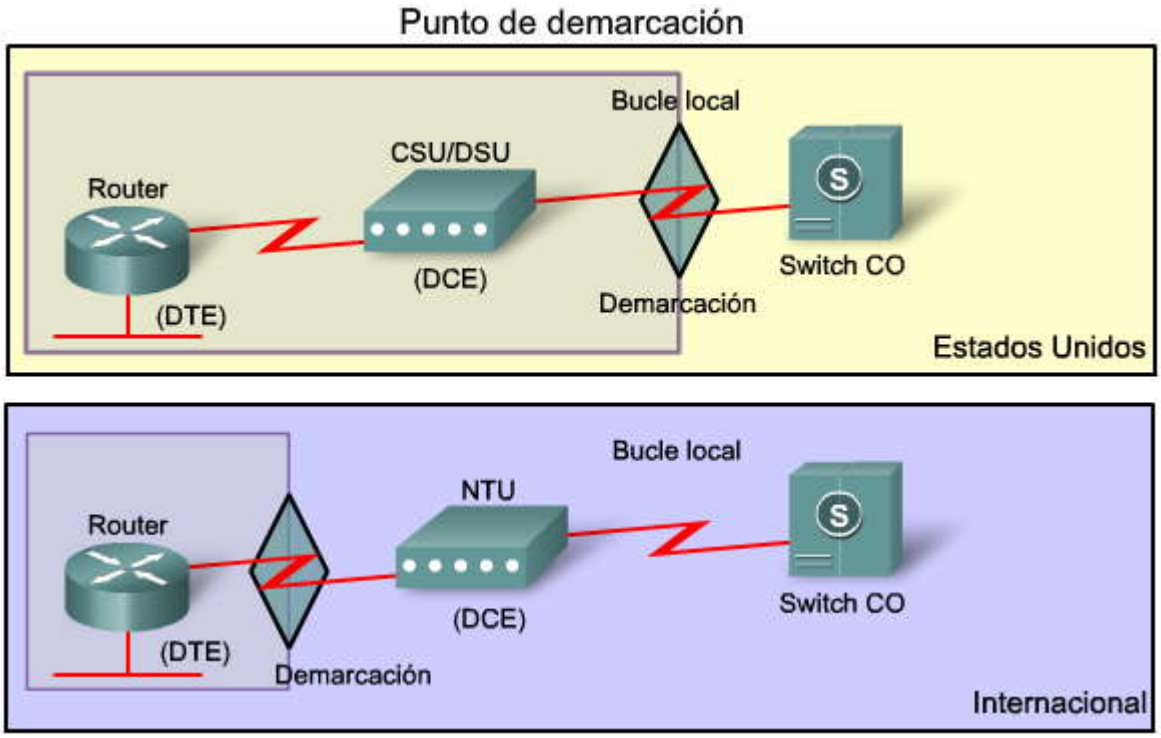


2.1.3 Punto de demarcación

Punto de demarcación

Antes de la desregulación en América del Norte y en otros países, las empresas telefónicas eran dueñas del bucle local, incluidos el cableado y el equipo en las instalaciones de los clientes. La desregulación forzó a las empresas telefónicas a individualizar su infraestructura de bucle local para permitir que otros proveedores proporcionen el equipo y los servicios. Esto creó la necesidad de delinear qué parte de la red pertenecía a la empresa telefónica y qué parte pertenecía al cliente. Este punto de la delineación es el punto de demarcación o demarc. El punto de demarcación marca el punto en donde su red se interconecta con la red que pertenece a otra organización. En la terminología telefónica, ésta es la interfaz entre el equipo terminal del abonado (CPE, customer-premises equipment) y el equipo del proveedor de servicios de red. El punto de demarcación es el lugar de la red donde finaliza la responsabilidad del proveedor de servicios.

El ejemplo representa una situación de ISDN. En los Estados Unidos, un proveedor de servicios provee bucles locales a las instalaciones del cliente y el cliente provee el equipo activo, como la unidad de servicio del canal o la unidad de servicio de datos (CSU, channel service unit/DSU, data service unit) donde termina el bucle local. Esta terminación a menudo se produce en un armario de telecomunicaciones y el cliente es responsable de mantener, reemplazar y reparar el equipo. En otros países, el proveedor de servicios provee y administra la unidad de terminación de la red (NTU, Network Terminating Unit). Esto permite que el proveedor de servicios administre el bucle local y resuelva de forma activa sus problemas cuando el punto de demarcación ocurre después de la NTU. El cliente conecta un dispositivo CPE, como por ejemplo un router o un dispositivo de acceso de frame relay, a la NTU por medio de una interfaz serial V.35 o RS-232.



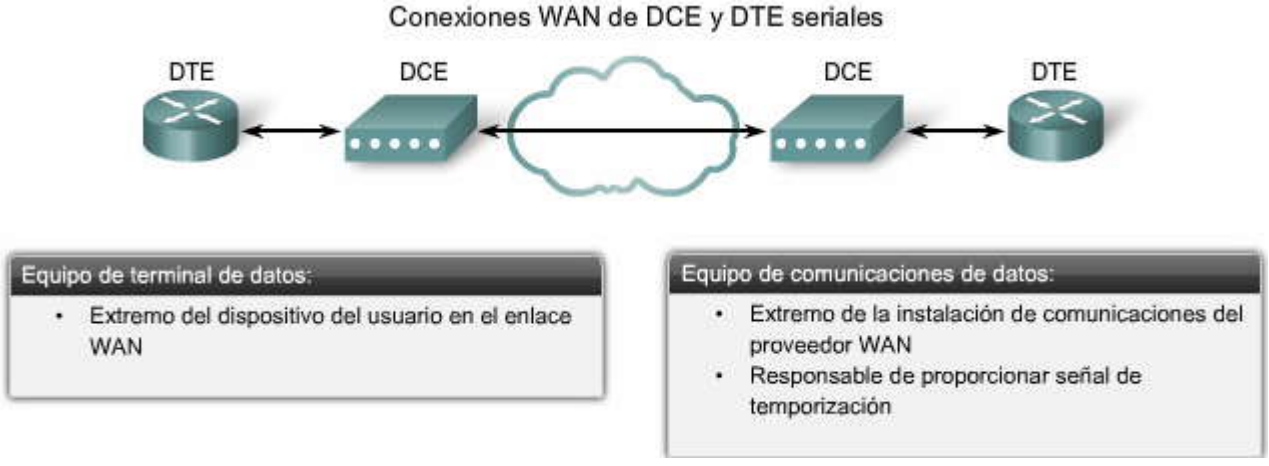
2.1.4 DTE y DCE

DTE-DCE

Desde el punto de vista de la conexión a la WAN, una conexión serial posee un dispositivo DTE en un extremo de la conexión y un dispositivo DCE en el otro extremo. La conexión entre los dos dispositivos DCE es la red de transmisión del proveedor de servicios WAN. En este caso:

- el CPE, que en general es un router, es el DTE. El DTE también podría ser un terminal, una computadora, una impresora o una máquina de fax si se conectaran directamente a la red del proveedor de servicios.
- El DCE, en general un módem o CSU/DSU, es el dispositivo que se utiliza para convertir los datos del usuario del DTE en una forma que sea aceptable para el enlace de la transmisión del proveedor del servicio WAN. La señal se recibe en el DCE remoto, que decodifica la señal nuevamente en una secuencia de bits. El DCE remoto luego señala esta secuencia al DTE remoto.

La Asociación de Industrias Electrónicas (EIA, Electronics Industry Association) y el Sector de Normalización de las Telecomunicaciones de la Unión de Telecomunicaciones Internacional (UIT-T, International Telecommunication Union Telecommunications Standardization Sector) han trabajado muy activamente en el desarrollo de estándares que permiten que los DTE se comuniquen con los DCE. La EIA denomina al DCE como el equipo de comunicación de datos, mientras que la ITU-T lo llama equipo de terminación de circuitos de datos.



Estándares de los cables
Originalmente, el concepto de los DCE y los DTE se basó en dos tipos de equipos: el equipo terminal que generaba o recibía datos y el equipo de comunicación que sólo transmitía datos. En el desarrollo del estándar RS-232, había razones que justificaban la necesidad de un cableado diferente para los conectores RS- 232 de 25 pins en estos dos tipos de equipos. Aunque estas razones ya no son importantes, tenemos dos tipos diferentes de cables: uno para la conexión de un DTE con un DCE y otro para la conexión directa entre dos DTE.

La interfaz DTE/DCE para un estándar en particular define las siguientes especificaciones:

- Mecánica/física: número de pins y tipo de conector
- Eléctrica: define los niveles de tensión para 0 y 1
- Funcional: especifica las funciones que se ejecutan al asignar significados a cada una de las líneas de señalización de la interfaz
- Procesal: especifica la secuencia de eventos para la transmisión de los datos

Haga clic en el botón Cables seriales que se muestra en la imagen.

El estándar original RS-232 sólo definía las conexiones entre los DTE y los DCE, que eran módems. Sin embargo, si desea conectar dos DTE, como dos computadoras o dos routers en el laboratorio, se necesita un cable especial llamado módem nulo que reemplaza a un DCE. En otras palabras, los dos dispositivos se conectan sin emplear un módem. Un módem nulo es un método de comunicación para conectar directamente dos DTE, como una computadora, un terminal o una impresora, a través de un cable serial RS-232. Con una conexión con módem nulo, las líneas de transmisión (Tx) y recepción (Rx) están entrecruzadas tal como muestra la imagen.

Haga clic en el botón DB-60 en la imagen.

El cable para la conexión DTE a DCE es un cable de transición serial y blindado. El extremo del router del cable de transición serial blindado puede ser un conector DB-60, que se conecta al puerto DB-60 en una tarjeta de interfaz WAN serial. El otro extremo del cable de transición serial está disponible con el conector apropiado para el estándar que se va a usar. Por lo general, el proveedor WAN o la CSU/DSU determina el tipo de cable. Los dispositivos Cisco admiten los estándares seriales EIA/TIA-232, EIA/TIA-449, V.35, X.21 y EIA/TIA-530.

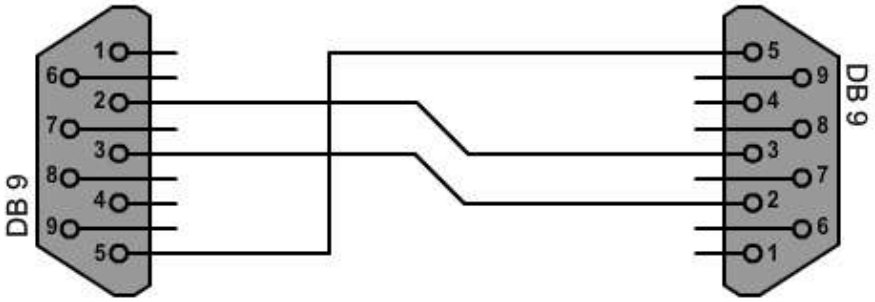
Haga clic en el botón Serial inteligente en la imagen.

Para admitir mayores densidades en un factor de forma más pequeño, Cisco ha introducido el cable serial inteligente. El extremo de la interfaz del router del cable serial inteligente es un conector de 26 pins mucho más compacto que el conector DB-60.

Haga clic en el botón Router a router que se muestra en la imagen.

Cuando utilice un módem nulo, tenga en cuenta que las conexiones síncronas requieren una señal de reloj.Un dispositivo externo o uno de los DTE pueden generar esta señal de reloj. Cuando se conecta un DTE con un DCE, el puerto serial en el router es el extremo DTE de la conexión predeterminada y la señal de reloj, por general, es provista por un dispositivo CSU/DSU o un dispositivo DCE similar. Sin embargo, al utilizar un cable de módem nulo en una conexión router a router, una de las interfaces seriales se debe configurar como el extremo DCE para proporcionar la señal de reloj para la conexión.

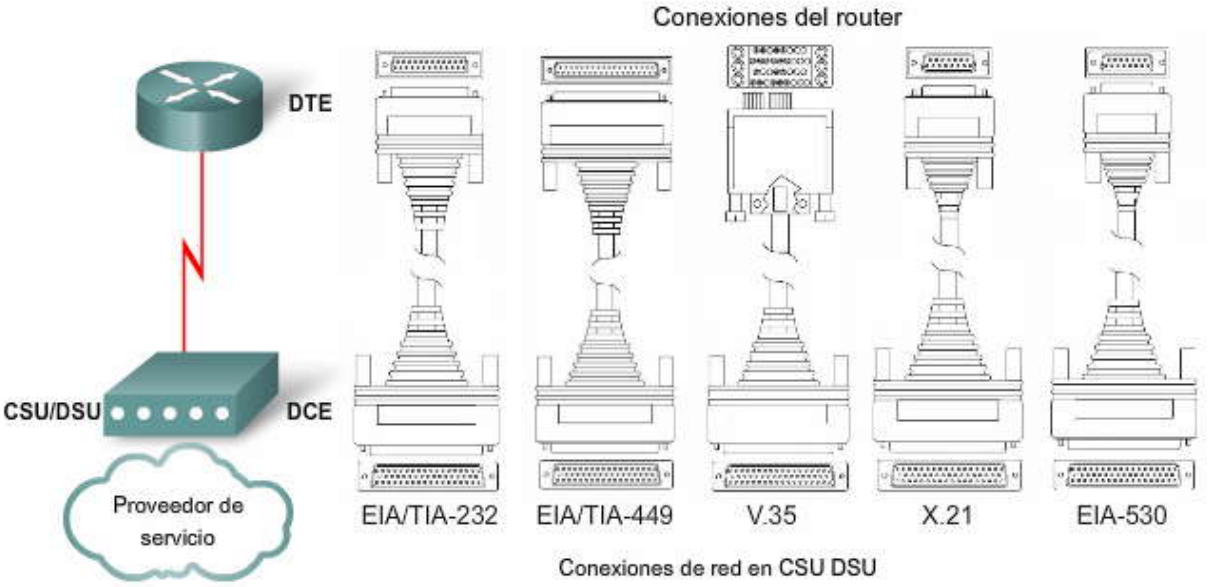
Módem nulo para conectar 2 DTE



Conector 1	Conector 2	Función
2	3	Rx ← Tx
3	2	Tx → Rx
5	5	Señal de conexión a tierra

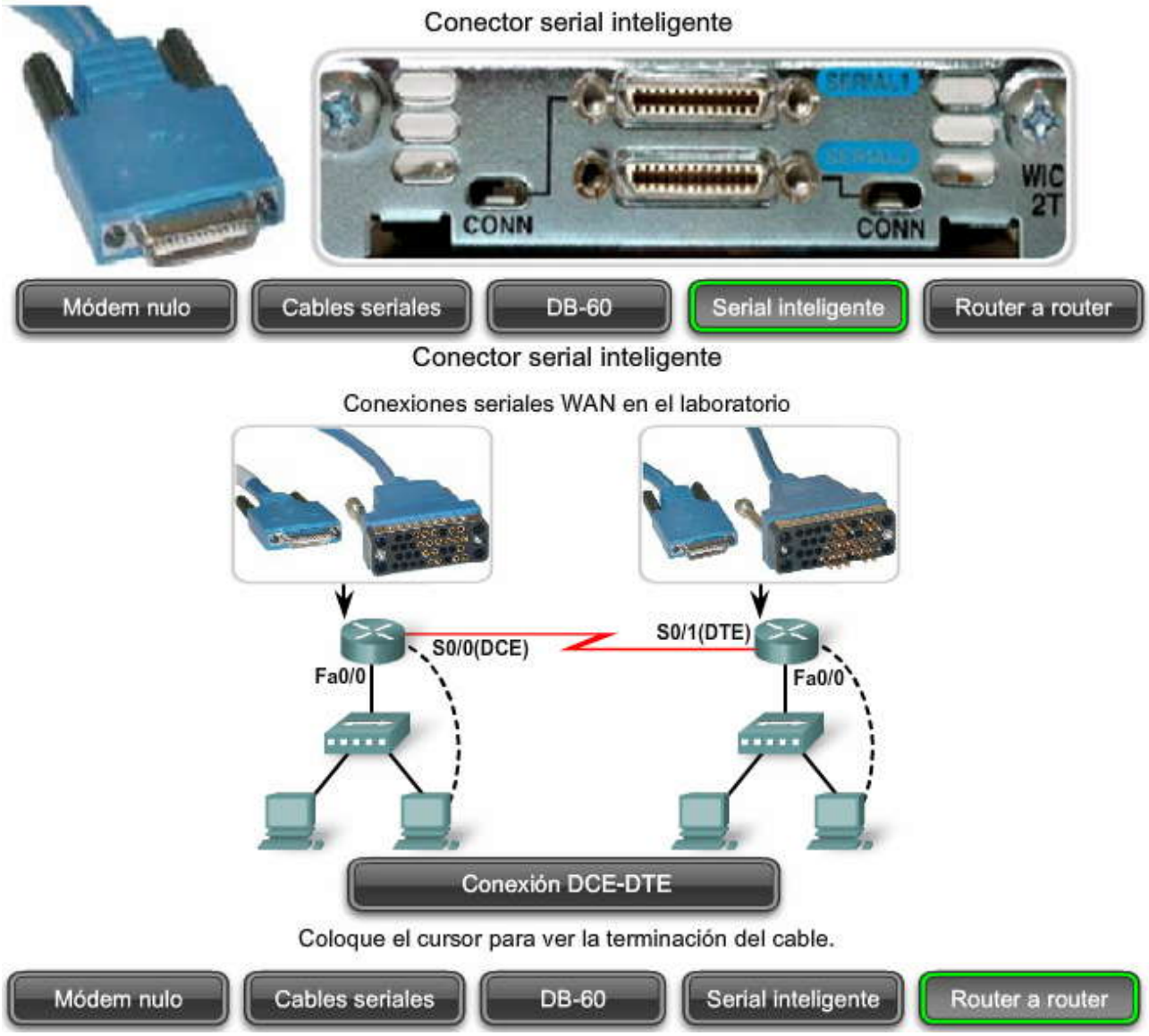
Observe los entrecruzamientos: Pin 2 a Pin 3 y Pin 3 a Pin 2

Opciones de conexión serial de WAN



Conexiones de red en CSU DSU

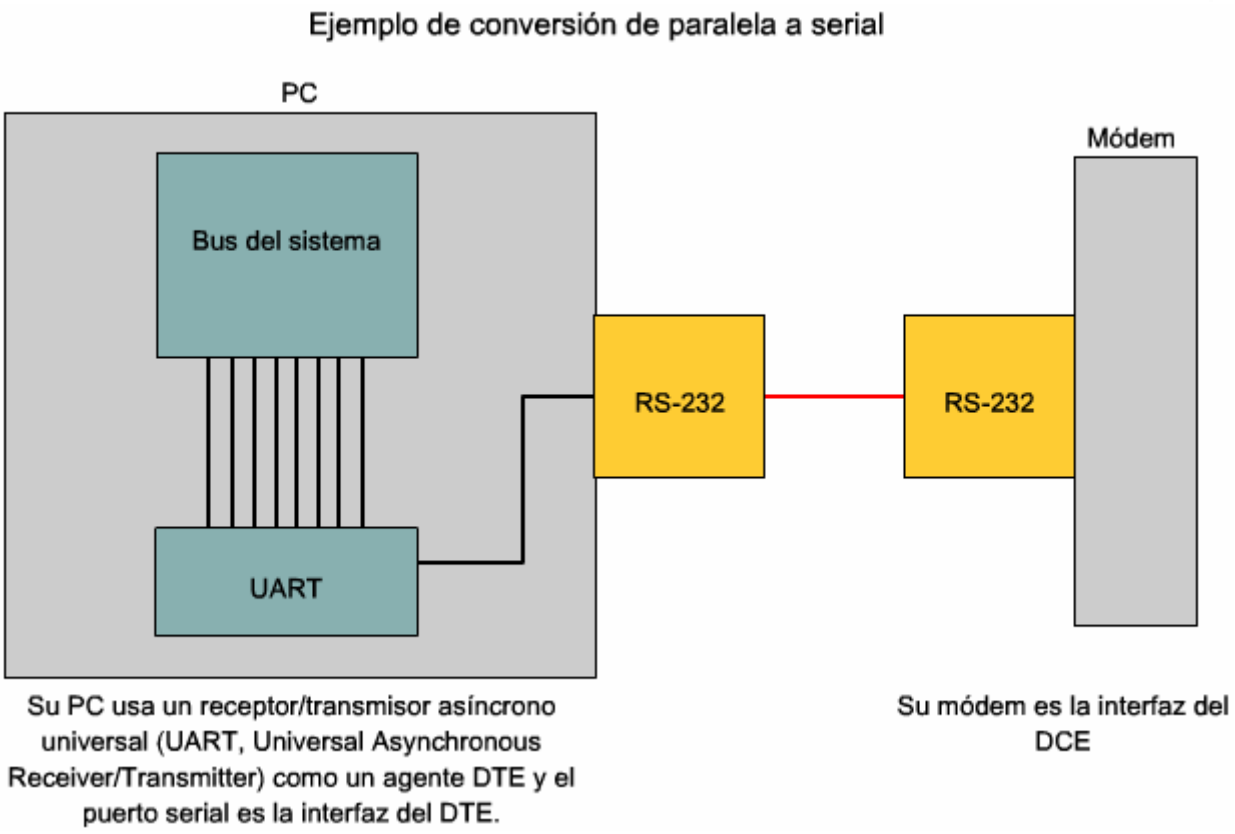
Conexión del router DB-60



Conversión de paralela a serial

Los términos DTE y DCE son relativos según la parte de la red que esté observando. RS-232C es el estándar recomendado (RS, recommended standard) que describe el protocolo y la interfaz física para una velocidad relativamente baja, una comunicación de datos seriales entre las computadoras y los dispositivos relacionados. En un principio, la EIA definió RS-232C para los dispositivos teleimpresores. El DTE es la interfaz RS-232C que utiliza una computadora para intercambiar datos con un módem u otro dispositivo serial. El DCE es la interfaz RS-232C que un módem u otro dispositivo serial utiliza en el intercambio de datos con la computadora.

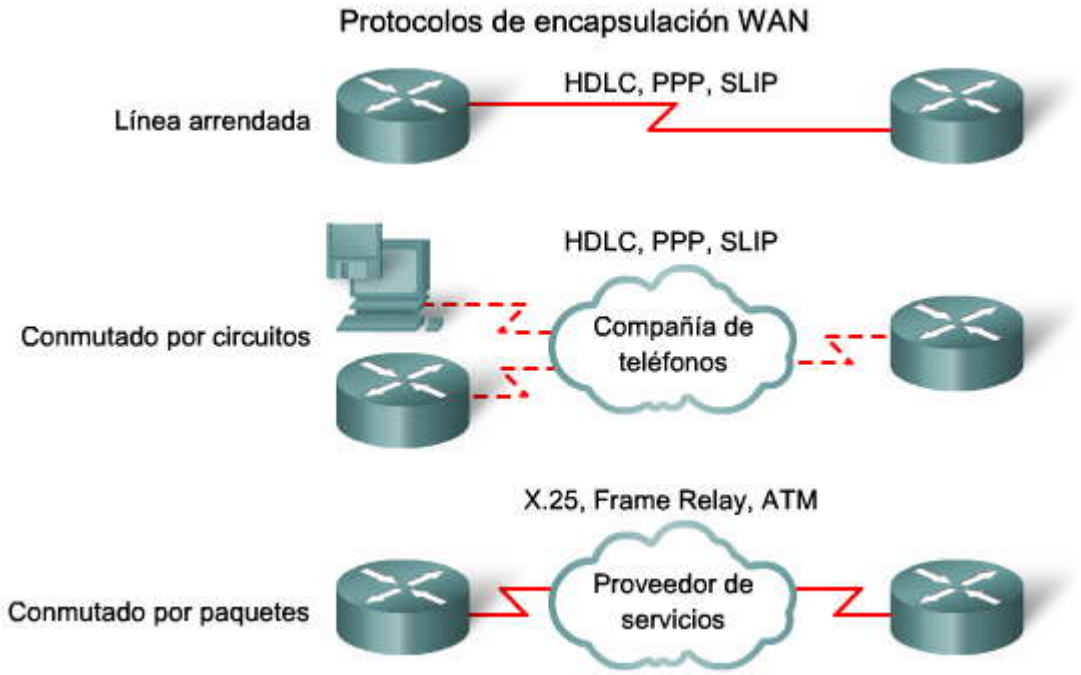
Por ejemplo, su computadora, en general, utiliza una interfaz RS-232C para comunicar e intercambiar datos con dispositivos seriales conectados, como un módem. La computadora también tiene un chipTransmisor/Receptor asíncrono universal (UART, Universal Asynchronous Receiver/Transmitter) en la motherboard. Dado que los datos de la computadora circulan por los circuitos paralelos, el chip UART convierte los grupos de bits de un stream paralelo a un stream serial de bits. Para trabajar más rápido, un chip UART tiene búferes para que el chip pueda almacenar datos en caché provenientes del bus del sistema mientras procesa los datos que salen del puerto serial. El UART es el agente DTE de su computadora y se comunica con el módem u otro dispositivo serial, que, según lo establecido en el estándar RS-232C, tiene una interfaz complementaria llamada interfaz DCE.



2.1.5 Encapsulación HDLC

Protocolos de encapsulación WAN
En cada conexión WAN, los datos se encapsulan dentro de tramas, antes de cruzar el enlace WAN. Para asegurar que se utiliza el protocolo correcto, usted debe configurar el tipo de encapsulación de la Capa 2 adecuado. La elección del protocolo depende de la tecnología WAN y del equipo de comunicación. En la imagen, se muestran los protocolos WAN más comunes y el lugar donde se utilizan; luego, se observan descripciones breves.

- **HDLC**: el tipo de encapsulación predeterminada en las conexiones punto a punto, los enlaces dedicados y las conexiones conmutadas por circuito cuando el enlace utiliza dos dispositivos Cisco. El HDLC es ahora la base para el PPP síncrono, empleado por muchos servidores para conectarse a una WAN, más comúnmente a Internet.
- **PPP**: suministra conexiones de router a router y de host a red, a través de circuitos síncronos y asíncronos. El PPP funciona con varios protocolos de capa de red, como IP e intercambio de paquetes de internetworking (IPX, Internetwork Packet Exchange). El PPP también tiene mecanismos de seguridad incorporados como el PAP y elCHAP. La mayor parte de este capítulo trata del PPP.
- **Protocolo Internet de línea serial (SLIP, Serial Line Internet Protocol)**: un protocolo estándar para conexiones seriales punto a punto que usan TCP/IP. SLIP ha sido desplazado en gran medida por PPP.
- **X.25/procedimiento de acceso al enlace balanceado (LAPB, Link Access Procedure, Balanced)**: estándar de la UIT-T que define cómo se mantienen las conexiones entre DTE y DCE para el acceso remoto a terminales y las comunicaciones informáticas en las redes de datos públicas. X.25 especifica a LAPB, un protocolo de capa de enlace de datos. X.25 es un predecesor de Frame Relay.
- **Frame Relay**: un protocolo estándar industrial, de capa de enlace de datos, conmutado, que maneja múltiples circuitos virtuales. Frame Relay es un protocolo que pertenece a una generación inmediatamente posterior a X.25. Frame Relay descarta algunos de los procesos que consumen el tiempo (como la corrección de errores y el control del flujo) utilizados en X.25. El próximo capítulo trata sobre Frame Relay.
- **ATM**: el estándar internacional para relay de celdas mediante el cual los dispositivos envían múltiples tipos de servicio (como, por ejemplo, voz, vídeo o datos) en celdas de longitud fija (53 bytes). Las celdas de longitud fija permiten que el procesamiento se lleve a cabo en el hardware, lo que disminuye los retrasos en el tránsito. ATM aprovecha losmedios de transmisión de alta velocidad, como E3, SONET y T3.



Encapsulación HDLC
HDLC es un protocolo orientados a bit síncrono de capa de enlace de datos, desarrollado por la Organización Internacional de Normalización (OIE). El estándar actual para HDLC es ISO 13239. HDLC se desarrolló a partir del estándar control de enlace de datos síncrono (SDLC, Synchronous Data Link Control) propuesto en la década de 1970. El HDLC brinda servicio orientado a la conexión y sin conexión.

El HDLC utiliza transmisión serial síncrona para brindar comunicación libre de errores entre dos puntos. El HDLC define una estructura del entramado de Capa 2 que permite el control del flujo y el control de errores mediante el uso de acuses de recibo. Cada trama presenta el mismo formato, ya sea una trama de datos o una trama de control.

Cuando desee transmitir tramas sobre enlaces síncronos o asíncronos, debe recordar que aquellos enlaces no tienen un mecanismo para marcar el inicio y el fin de las tramas. El HDLC utiliza un delimitador de trama o señalador para marcar el inicio y el fin de cada trama.

Cisco desarrolló una extensión del protocolo HLDC para solucionar la incapacidad de brindar compatibilidad multiprotocolo. A pesar de que el HDLC de Cisco (también conocido como cHDLC) está patentado, Cisco permitió que otros proveedores de equipos de red lo implementen. Las tramas HDLC de Gsco contienen un campo para identificar el protocolo de red que se está encapsulando. Las imágenes comparan el HLDC con el HLDC de Cisco.

Haga clic en el botón Tipos de tramas HDLC que se muestra en la imagen.

El HDLC define tres tipos de tramas, cada una con un formato de campo de control diferente. Las siguientes descripciones resumen los campos que se muestran en la imagen.

Señalador: el campo señalador inicia y finaliza la verificación de errores. La trama siempre comienza y finaliza con un campo señalador de 8 bits. El patrón de bit es 01111110. Ya que existe la probabilidad de que este patrón se lleve a cabo en los datos reales, el sistema HDLC de envío siempre inserta un bit 0 después de cada cinco 1 en el campo de datos, por lo tanto, en la práctica, la secuencia del señalador sólo puede ocurrir en los extremos de las tramas. El sistema receptor quita los bits insertados. Cuando las tramas se transmiten en forma consecutiva, el señalador del final de la primera trama se utiliza como señalador de inicio de la trama siguiente.

Dirección: el campo dirección contiene la dirección HDLC de la estación secundaria. Esta dirección puede contener una dirección específica, un grupo de direcciones o una dirección de broadcast. Una dirección principal es tanto un origen como un destino de comunicación que elimina la necesidad de incluir la dirección de la principal.

Control: el campo de control utiliza tres formatos diferentes, según el tipo de trama HDLC usada.

- **Trama de información (I):** las tramas I contienen información de la capa superior y alguna información de control. Esta trama envía y recibe números de secuencia y el bit de sondeo final (P/F) realiza el control de flujo y error. El

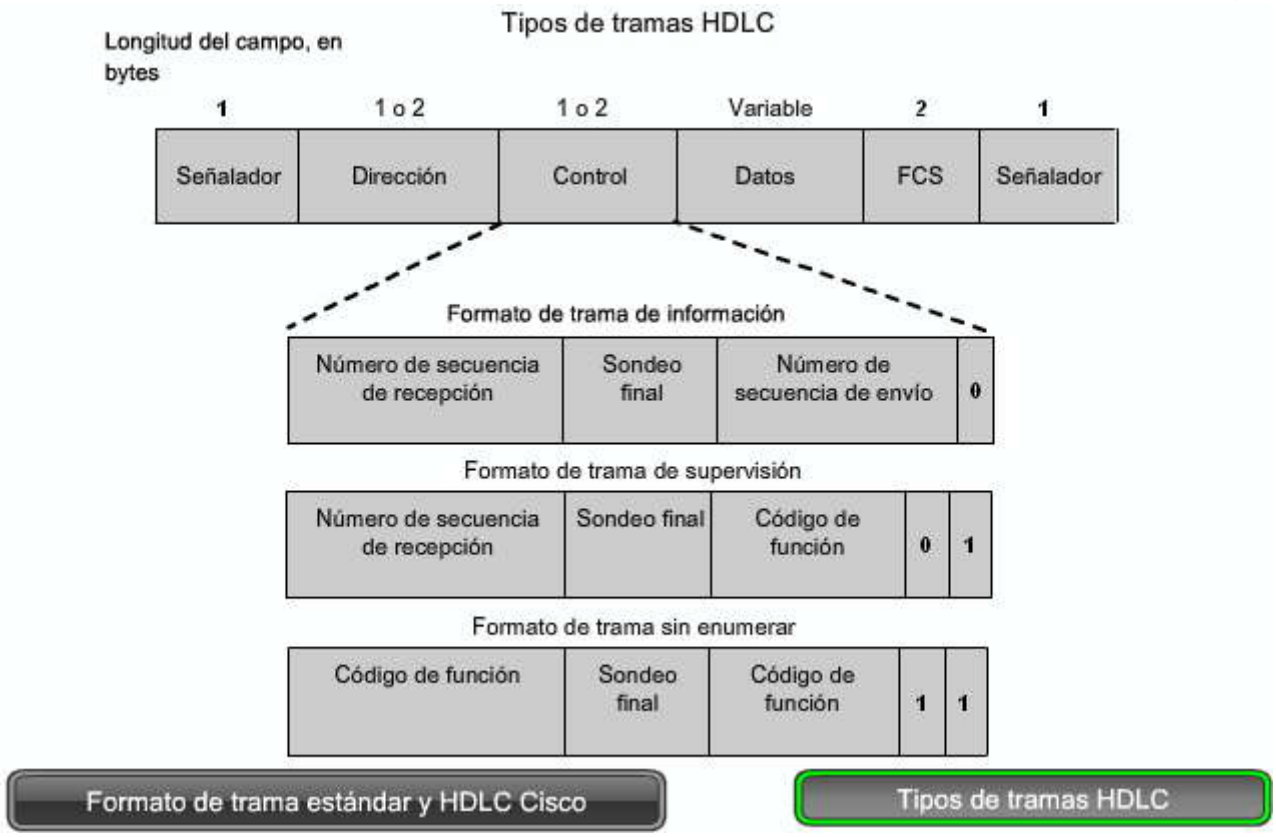
número de secuencia de envío hace referencia al número de la trama que se envía a continuación. El número de secuencia de recepción proporciona el número de la trama que se recibe a continuación. Tanto el transmisor como el receptor mantienen los números de secuencia de recepción y transmisión. Una estación primaria utiliza el bit P/F para indicar a la estación secundaria si solicita una respuesta inmediata o no. Una estación secundaria utiliza el bit P/F para indicar a la primaria si la trama actual es la última en su repuesta actual.

- **Trama de supervisión (S):** las tramas S brindan información de control. Una trama S puede solicitar y suspender la transmisión, informar sobre el estado y acusar recibo de las tramas I. Las tramas S no tienen un campo información.
- **Trama sin enumerar (U):** las tramas U admiten objetivos de control y no están secuenciadas. Una trama U puede utilizarse para iniciar secundarias. De acuerdo con la función de la trama U, su campo control es de 1 o 2 bytes. Algunas tramas U contienen un campo información.

Protocolo (sólo usado en el HLDC de Cisco): este campo especifica el tipo de protocolo encapsulado dentro de la trama (por ejemplo, 0x0800 para IP).

Datos: el campo de datos contiene una unidad de información de ruta (PIU, Path Information Unit) o una información de identificación de intercambio (XID, Exchange Identification).

Secuencia de verificación de trama (FCS, Frame Check Sequence): la FCS precede al delimitador del señalador de fin y, por lo general, es un recordatorio de cálculo de la verificación de redundancia cíclica (CRC, Cyclic Redundancy Check). El cálculo de la CRC se vuelve a realizar en el receptor. Si el resultado difiere del valor que se encuentra en la trama original, se supone que ocurrió un error.



2.1.6 Configuración de encapsulación HDLC

Configuración de encapsulación HDLC
El HDLC de Cisco es el método de encapsulación predeterminado que utilizan los dispositivos Cisco en las líneas seriales síncronas.

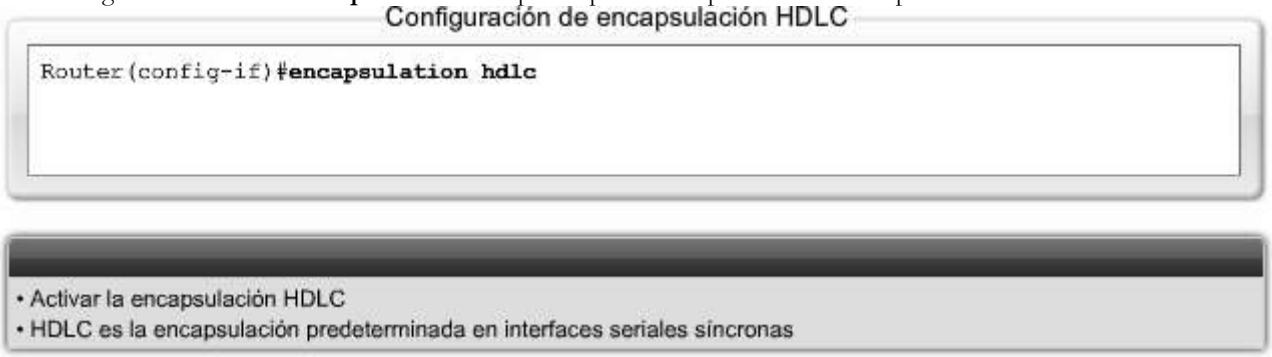
Usted utiliza el HDLC de Cisco como un protocolo punto a punto en líneas arrendadas entre dos dispositivos de Cisco. Si va a realizar una conexión a un dispositivo que no es de Cisco, utilice un PPP síncrono.

Si se cambió el método de encapsulación predeterminado, utilice el comando **encapsulation hdlc** en modo privilegiado para volver a habilitar el HDLC.

Se deben seguir dos pasos para habilitar la encapsulación HDLC:

Paso 1. Ingresar el modo de configuración de interfaz de la interfaz serial.

Paso 2. Ingresar el comando **encapsulation hdlc** para especificar el protocolo de encapsulación en la interfaz.



El resultado del comando **show interfaces serial** muestra información específica acerca de las interfaces seriales. Al configurar el HDLC, se podrá observar la leyenda "Encapsulation HDLC" (encapsulación HDLC), como aparece resaltado en la imagen.

Haga clic en el botón Estados posibles que se muestra en la imagen.

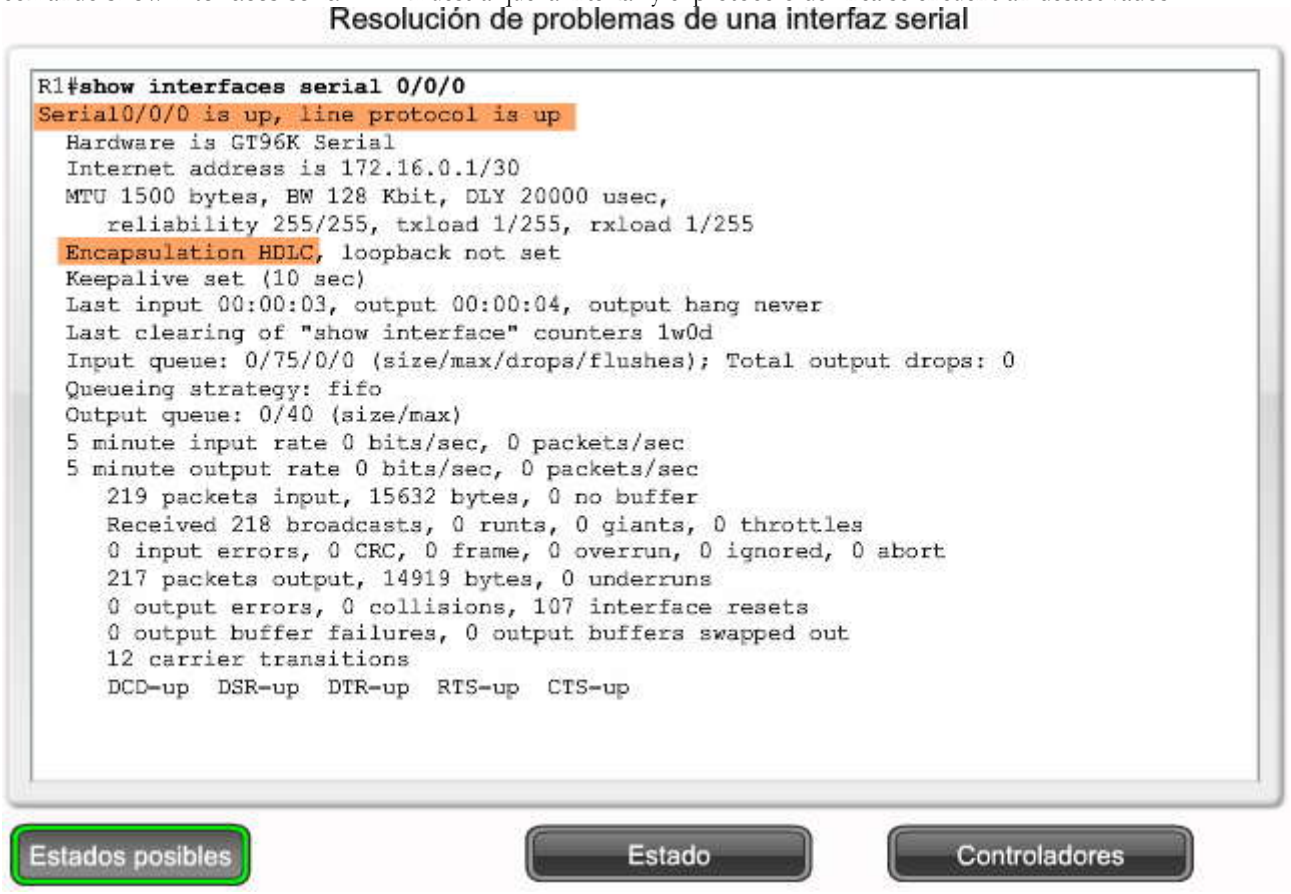
El comando **show interface serial** devuelve uno de los cinco estados posibles. Usted puede identificar cualquiera de los siguientes cinco estados posibles de problemas en la línea de estado de la interfaz:
Haga clic en el botón Estado que se muestra en la imagen.

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

Haga clic en el botón Controladores que se muestra en la imagen.

El comando **show controllers** es otra herramienta importante al diagnosticar las fallas en las líneas seriales. El resultado indica el estado de los canales de la interfaz y si un cable está conectado a la interfaz o no. En la imagen, la interfaz serial 0/0 tiene conectado un cable DCE V.35. La sintaxis del comando varía de acuerdo con la plataforma. Los routers serieCisco 7000 usan una tarjeta de controlador cBus para conectar los enlaces seriales. Con estos routers, use el comando**show controllers cbus**.

Si el resultado de la interfaz eléctrica se muestra como **UNKNOWN** (desconocido), en lugar de **V.35**, **EIA/TIA-449** o algún otro tipo de interfaz eléctrica, el problema seguramente radica en un cable conectado de forma incorrecta. También es posible que se trate de un problema con el cableado interno de la tarjeta. Si se desconoce la interfaz eléctrica, el resultado del comando **show interfaces serial <x>** muestra que la interfaz y el protocolo de línea se encuentran desactivados.



Resolución de problemas de una interfaz serial

Línea de estado	Condición posible	Problema / Solución
Serial x is up, line protocol is up	Esta es la condición de línea de estado adecuada.	No requiere ninguna acción.
Serial x is down, line protocol is down (DTE mode)	El router no detecta una señal de CD, lo que significa que el CD no está activo. Se ha producido un problema con el proveedor de servicios de portadora WAN, lo que significa que la línea está inactiva o no está conectada a las CSU/DSU. El cableado es defectuoso o incorrecto. Se ha producido una falla de hardware (CSU/DSU).	1. Verifique los LED de las CSU/DSU para ver si el CD está activo o inserte una caja de conexiones en la línea para verificar la señal de CD. 2. Consulte la documentación de instalación de hardware para verificar que se está utilizando el cable y la interfaz correctos. 3. Inserte una caja de conexiones y revise todos los conductores de control. 4. Póngase en contacto con el servicio de línea arrendada u otro servicio de portadora para ver si hay un problema. 5. Reemplace las piezas defectuosas. 6. Si cree que hay un hardware de router defectuoso, cambie la línea serial a otro puerto. Si la conexión se activa, la interfaz conectada anteriormente tiene un problema.
Serial x is up, line protocol is down (DTE mode)	Un router local o remoto está mal configurado. El router remoto no está enviando mensajes de actividad. Se ha producido un problema de servicio de portadora o de línea arrendada, lo que significa que hay una línea con exceso de ruido o un switch mal configurados o con fallas. Se ha producido un problema de temporización en el cable, lo que significa que la transmisión externa del reloj serial (SCTE, Serial Clock Transmit External) no está configurada en las CSU/DSU. La SCTE está diseñada para compensar el desplazamiento de fase de reloj en los cables largos. Cuando el dispositivo del DCE usa la SCTE, en lugar de su reloj interno, para realizar un muestreo de datos desde el DTE, está más preparado para tomar una muestra de los datos sin error, aunque se produzca un desplazamiento de fase en el cable. Una CSU/DSU remota o local ha fallado.	1. Coloque el módem, CSU o DSU en el modo loopback local y use el comando **`show interfaces serial`** para determinar si el protocolo de línea se activa. Si se activa el protocolo de línea, lo más probable es que exista un problema de proveedor de servicios de portadora WAN o una falla en el router remoto. 2. Si parece que el problema está en el extremo remoto, repita el Paso 1 en el módem, en la CSU o DSU remoto. 3. Revise todo el cableado. Asegúrese de que el cable esté conectado a la interfaz correcta, a la CSU/DSU correcta y al punto de terminación de red del proveedor de servicio de portadora WAN correcto. Use el comando exec **`show controllers`** para determinar cuál es el cable conectado a cada interfaz. 4. Active el comando exec debug **`serial interface`** . 5. Si el protocolo de línea no se activa en el modo loopback local y si el resultado del comando exec**`debug serial interface`** muestra que el contador de mensajes de actividad no aumenta, es posible que haya un problema con el hardware del router. Intercambie el hardware de interfaz del router. 6. Si el protocolo de línea se activa y si el contador de mensajes de actividad aumenta, el problema no está en el router local. 7. Si se sospecha que existe un hardware del router defectuoso, cambie la línea serial a un puerto sin usar. Si la conexión se activa, la interfaz conectada anteriormente tiene un problema.

	El hardware del router, que puede ser local o remoto, ha fallado.	
Serial x is up, line protocol is down (DCE mode)	Falta el comando clockrate interface configuration. El dispositivo DTE no admite o no está configurado para el modo SCTE (temporización de terminales). La CSU o DSU remota falló.	1. Agregue el comando **clockrate** interface configuration en la interfaz serial. Sintaxis: **frecuencia de reloj** *bytes por segundo* Descripción de sintaxis: clockrate bps (frecuencia de reloj bytes por segundo): 1200, 2400, 4800, 9600, 19 200, 38 400, 56 000, 64 000, 72 000, 125 000, 148 000, 250 000, 500 000, 800 000, 1 000 000, 1 300 000, 2 000 000, 4 000 000 u 8 000 000 2. Si parece que el problema está en el extremo remoto, repita el Paso 1 en el módem, la CSU o DSU remotos. 3. Verifique que se esté usando el cable correcto. 4. Si el protocolo de línea sigue inactivo, es posible que exista una falla de hardware o un problema de cableado. Inserte una caja de conexiones y observe los conductores. 5. Si es necesario, reemplace las piezas defectuosas.
Serial x is up, line protocol is up (looped)	Existe un bucle en el circuito. El número de secuencia del paquete de mensaje de actividad cambia a un número aleatorio cuando se detecta inicialmente un bucle. Si se devuelve el mismo número aleatorio a través del enlace, existe un bucle.	1. Use el comando exec privilegiado **show running-config** para buscar cualquier entrada del comando de configuración de interfaz **loopback**. 2. Si hay una entrada del comando de configuración de interfaz **loopback**, use el comando de configuración de interfaz **no loopback** para quitar el bucle. 3. Si no hay un comando de configuración de interfaz **loopback**, examine las CSU/DSU para determinar si están configuradas en el modo loopback manual. Si es así, desactive el loopback manual. 4. Después de desactivar el modo loopback en las CSU/DSU, restablezca las CSU/DSU e inspeccione el estado de la línea. Si el protocolo de línea se activa, no es necesario realizar otra acción. 5. Si, después de haber realizado la inspección, la CSU o la DSU no se pueden configurar en forma manual, póngase en contacto con el servicio de línea arrendada u otro servicio de portadora para obtener asistencia para la resolución de problemas de la línea.
Serial x is up, line protocol is down (disabled)	Se produjo un elevado porcentaje de error debido a un problema con el proveedor de servicios WAN. Ha ocurrido un problema con el hardware de la CSU o de la DSU. El hardware (interfaz) del router está dañado.	1. Resuelva los problemas de la línea con un analizador serial y una caja de conexiones. Busque el intercambio de señales CTS y DSR. 2. Bucle de CSU/DSU (bucle de DTE). Si el problema persiste, es probable que se trate de un problema de hardware. Si el problema no persiste, es probable que haya un problema con el proveedor de servicio WAN. 3. Si es necesario, elimine el hardware defectuoso (CSU, DSU, switch, router local o remoto).
Serial x is administratively down, line protocol is down	La configuración del router incluye el comando **shutdown** interface configuration. Existe una dirección IP duplicada.	1. Verifique la configuración del router para buscar el comando **shutdown**. 2. Use el comando de configuración de interfaz **no shutdown** para quitar el comando **shutdown**. 3. Verifique que no haya direcciones IP idénticas mediante el comando exec privilegiado **show running-config**o el comando exec**show interfaces** . 4. Si hay direcciones duplicadas, resuelva el conflicto mediante el cambio de una de las direcciones IP.

Resolución de problemas de una interfaz serial

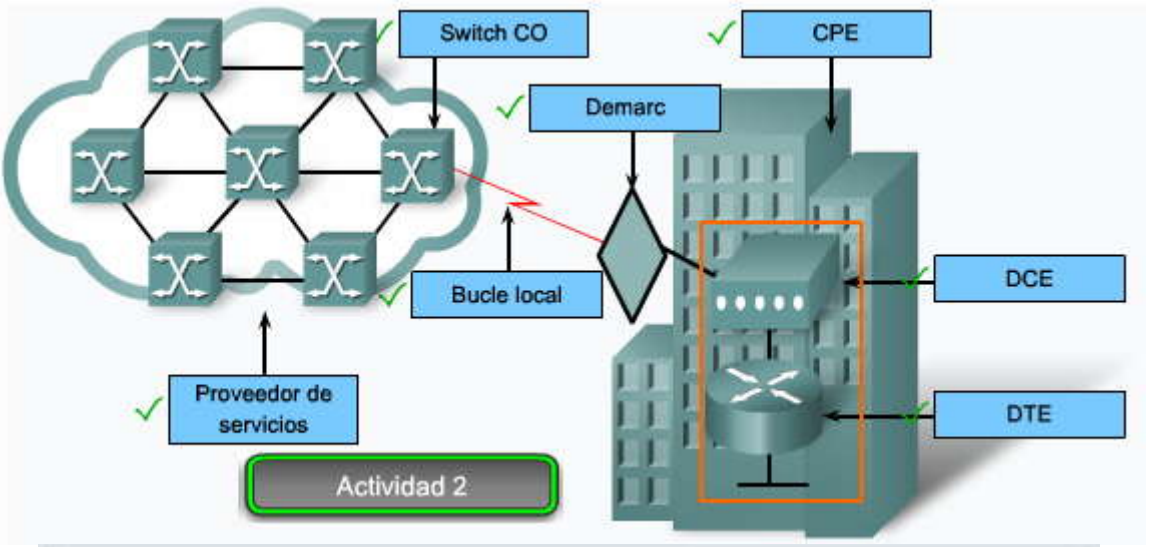
```
R1#show controllers serial 0/0/0
Interface Serial0/0/0
Hardware is GT96K
DCE V.35, clock rate 64000
idb at 0x62938244, driver data structure at 0x6293A608
wic_info 0x6293AC04
Physical Port 0, SCC Num 0
MPSC Registers:
MMCR_L=0x000304C0, MMCR_H=0x00000000, MPCR=0x00000000
CHR1=0x00FE007E, CHR2=0x00000000, CHR3=0x000005F4, CHR4=0x00000000
CHR5=0x00000000, CHR6=0x00000000, CHR7=0x00000000, CHR8=0x00000000
CHR9=0x00000000, CHR10=0x00003008
SDMA Registers:
SDC=0x00002201, SDCM=0x00000080, SGC=0x0000C000
CRDP=0x073BD020, CTDP=0x073BD450, FTDB=0x073BD450
Main Routing Register=0x00038E00 BRG Conf Register=0x0005023F
Rx Clk Routing Register=0x76583888 Tx Clk Routing Register=0x76593910
GPP Registers:
Conf=0x43430002, Io=0x4646CA50, Data=0x7F6B3FAD, Level=0x80004
Conf0=0x43430002, Io0=0x4646CA50, Data0=0x7F6B3FAD, Level0=0x80004
0 input aborts on receiving flag sequence
0 throttles, 0 enables
0 overruns
0 transmitter underruns
 --More--
```

Estados posibles | Estado | Controladores

En esta actividad, practicará la resolución de problemas de las interfaces seriales. Las instrucciones detalladas están proporcionadas dentro de la actividad, al igual que en el enlace al PDF a continuación.
Haga clic en el icono Packet Tracer para obtener más detalles.

Actividad 1

	Serial	Paralelo
Usada para la mayoría de las comunicaciones externas	✓	
Usada para las conexiones cortas entre componentes internos		✓
Envía información a través de un hilo, un bit de datos a la vez	✓	
Envía información a través de diversos hilos simultáneamente		✓
Es susceptible al sesgo de reloj y a crosstalk		✓
Es más económica su implementación	✓	
Usa RS-232, V.35 y estándares HSSI	✓	



La multiplexación por división temporal es un concepto de capa _____. No considera la naturaleza de los datos que se envían desde el canal.	física
La multiplexación estadística por división temporal usa una extensión de intervalo de tiempo _____.	variable
_____ es un ejemplo de TDM.	SONET
El _____ es el lugar de la red en donde finaliza la responsabilidad del proveedor de servicios.	demarc
El _____ es el equipo local para el cliente y proporciona el lado _____ de una conexión WAN serial.	CPE, DTE
_____ es el tipo de encapsulación predeterminada en las conexiones punto a punto, los enlaces dedicados y las conexiones conmutadas por circuito cuando el enlace utiliza dos dispositivos Cisco.	HDLC
_____ suministra conexiones de router a router y de host a red a través de circuitos síncronos y asíncronos.	PPP
_____ es un protocolo estándar industrial, de capa de enlace de datos conmutado, que maneja múltiples circuitos virtuales. Es un protocolo que pertenece a la generación inmediatamente posterior a _____ .	Frame Relay, X.25

Actividad 4

¿Qué comando verifica si un cable está conectado a una serial 0/0/0 y si es DTE o DCE?

```
Router#
```

¿Qué comando verifica el tipo de encapsulación usado en la serial 0/0/0?

```
Router#
```

¿Qué comando restaura los valores predeterminados de Cisco en la encapsulación en una interfaz serial?

```
Router(config-if)#
```

2.2 Conceptos del PPP

2.2.1 Introducción al PPP

¿Qué es el PPP?

Recuerde que HDLC es el método de encapsulación serial predeterminada al conectar dos routers Cisco. Con un campo tipo protocolo agregado, la versión de HDLC de Cisco está patentada. Por lo tanto, el HDLC de Cisco sólo puede funcionar

con otros dispositivos de Cisco. Sin embargo, cuando necesite conectarlo a un router que no sea Cisco, debe utilizar la encapsulación PPP.

La encapsulación PPP se diseñó cuidadosamente para que sea compatible con los hardware de soporte que más se usan. El PPP encapsula tramas de datos para la transmisión a través de los enlaces físicos de la Capa 2. El PPP establece una conexión directa mediante cables seriales, líneas telefónicas, líneas troncales, teléfonos celulares, enlaces de radio especializados o enlaces de fibra óptica. Existen muchas ventajas al usar el PPP, incluido el hecho de que no está patentado. Además, incluye varias funciones que no están disponibles en el HDLC:

- la función Administración de calidad del elance monitorea la calidad del mismo. Si se detectan muchos errores, el PPP desactiva el enlace.
- El PPP admite la autenticación PAP y CHAP. Esta función se explica y se práctica en secciones subsiguientes.

El PPP contiene tres componentes principales.

- El protocolo HDLC para la encapsulación de datagramas a través de enlaces punto a punto.
- Un protocolo de control de enlace (LCP, Link Control Protocol) extensible para establecer, configurar y probar la conexión de enlace de datos.
- Una familia de protocolos de control de red (NCP, Network Control Protocols) para establecer y configurar distintos protocolos de capa de red. El PPP permite el uso simultáneo de múltiples protocolos de capa de red. Algunos de los NCP más comunes son el protocolo de control del protocolo de Internet, el protocolo de control Appletalk, el protocolo de control Novell IPX, el protocolo de control Cisco Systems, el protocolo de control SNA y el protocolo de control de compresión.

2.2.2 Arquitectura de capas PPP

Arquitectura PPP

Una arquitectura de capas es un modelo, diseño o plan lógico que ayuda a la comunicación entre las capas interconectadas. La imagen traza la arquitectura de capas del PPP en contraste con el modelo de interconexión de sistema abierto (OSI, Open System Interconnection). EL PPP y OSI comparten la misma capa física, pero el PPP distribuye las funciones del LCP y el NCP de manera diferente.

En la capa física, puede configurar el PPP en una variedad de interfaces, las que incluyen:

- Serial asíncrona
- Serial síncrona
- HSSI
- ISDN

El PPP funciona a través de cualquier interfaz DTE/DCE (RS-232-C, RS-422, RS-423 o V.35). El único requisito absoluto impuesto por el PPP es un circuito duplex, dedicado o conmutado, que pueda funcionar en un modo serial de bits asíncrono o síncrono, transparente a tramas de capa de enlace del PPP. El PPP no impone ninguna otra restricción con respecto a la velocidad de transmisión que no sea aquella impuesta por la interfaz DTE/DCE que se encuentre en uso.

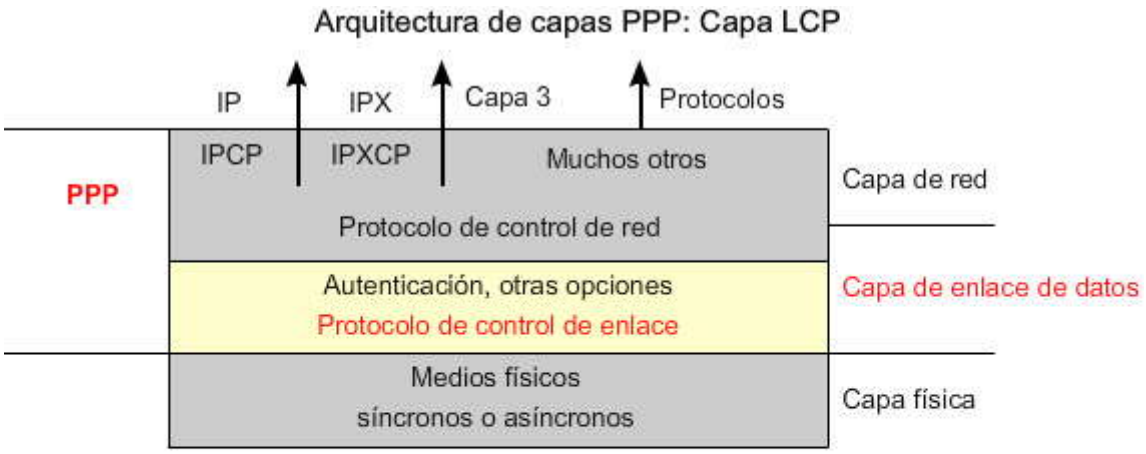
La mayoría del trabajo realizado por el PPP se produce en el enlace de datos y las capas de red mediante el LCP y los NCP. EL LCP establece la conexión PPP y sus parámetros, los NCP manejan configuraciones de protocolo de capa superior y el LCP finaliza la conexión PPP.

Arquitectura PPP: capa del protocolo de control de enlace
El LCP es la parte que realmente realiza el trabajo en el PPP. El LCP se ubica en la parte más alta de la capa física y se utiliza para establecer, configurar y probar la conexión de enlace de datos. El LCP establece el enlace punto a punto. El LCP también negocia y establece las opciones de control en el enlace de datos WAN, manejadas por los NCP.

El LCP brinda configuración automática de las interfaces en cada extremo, lo que incluye:

- El manejo de límites variables en el tamaño del paquete
- La detección de errores comunes de configuración
- La finalización del enlace
- La determinación de cuándo un enlace funciona correctamente o cuándo falla

El PPP también utiliza el LCP para acordar, de forma automática, acerca de formatos de encapsulación (autenticación, compresión, detección de errores) tan pronto como se establezca el enlace.



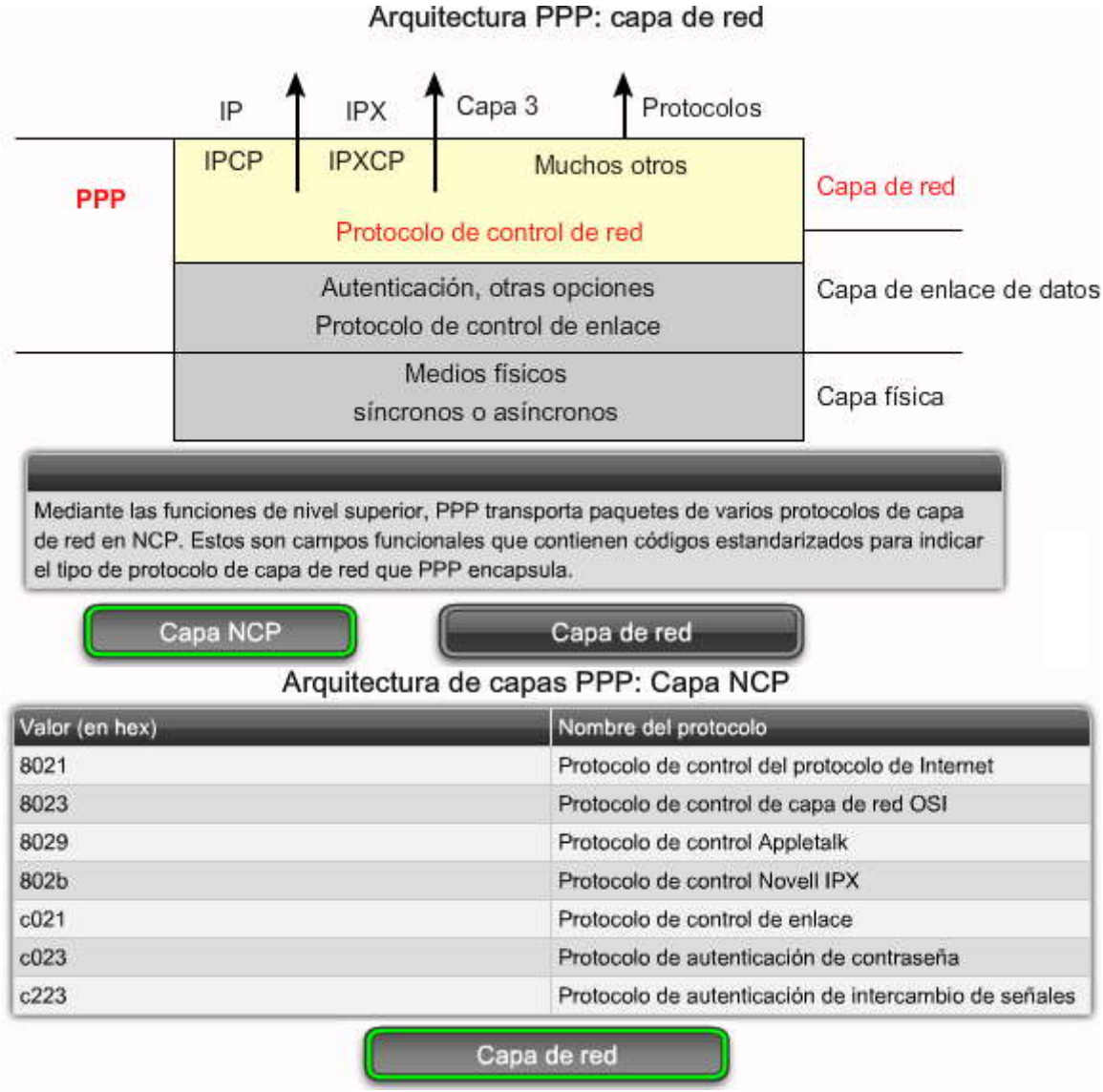
PPP ofrece opciones de servicio en LCP y es utilizado principalmente para negociar y para verificar las tramas cuando se implementan los controles punto a punto especificados por un administrador.

Arquitectura PPP: capa del protocolo de control de red
Los enlaces punto a punto tienden a empeorar muchos problemas con la familia actual de protocolos de red. Por ejemplo, la asignación y administración de direcciones IP, la cual resulta un problema incluso en entornos LAN, es especialmente dificultosa en enlaces punto a punto conmutados por circuito (tales como los servidores con módem dialup). El PPP se ocupa de estos problemas mediante los NCP.

El PPP permite que varios protocolos de capa de red operen en el mismo enlace de comunicación. Para cada protocolo de capa de red utilizado, el PPP utiliza un NCP distinto. Por ejemplo, el IP utiliza el protocolo de control de IP (IPCP, IP Control Protocol) y el IPX utiliza el protocolo de control IPX (IPXCP, IPX Control Protocol).

Haga clic en el botón capa de red que se muestra en la imagen.

Los NCP incluyen campos funcionales que contienen códigos estandarizados (números de campo de protocolo del PPP que se muestran en la imagen) para indicar el protocolo de capa de red que el PPP encapsula. Cada NCP administra las necesidades específicas solicitadas por sus respectivos protocolos de capa de red. Los diversos componentes del NCP encapsulan y negocian opciones para múltiples protocolos de capa de red. El uso de los NCP para configurar los diversos protocolos de capa de red se explica y se practica más adelante en este capítulo.



Arquitectura de capas PPP: Capa NCP

Valor (en hex)	Nombre del protocolo
8021	Protocolo de control del protocolo de Internet
8023	Protocolo de control de capa de red OSI
8029	Protocolo de control Appletalk
802b	Protocolo de control Novell IPX
c021	Protocolo de control de enlace
c023	Protocolo de autenticación de contraseña
c223	Protocolo de autenticación de intercambio de señales

Capa de red

2.2.3 Estructura de la trama PPP

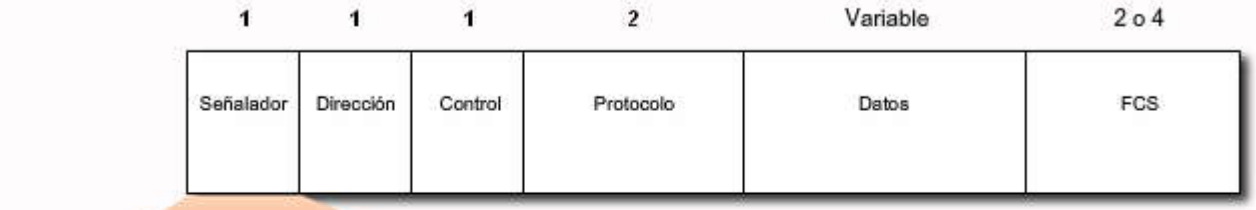
Estructura de la trama PPP
Una trama PPP tiene seis campos, tal como se muestra en la imagen.

Coloque el cursor del mouse sobre cada campo para encontrar información acerca de lo que contiene y hace cada uno.

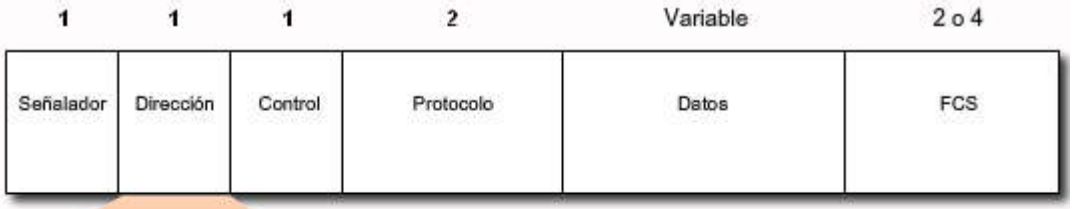
El LCP puede negociar modificaciones en la estructura de la trama PPP estándar.

Campos de la trama PPP

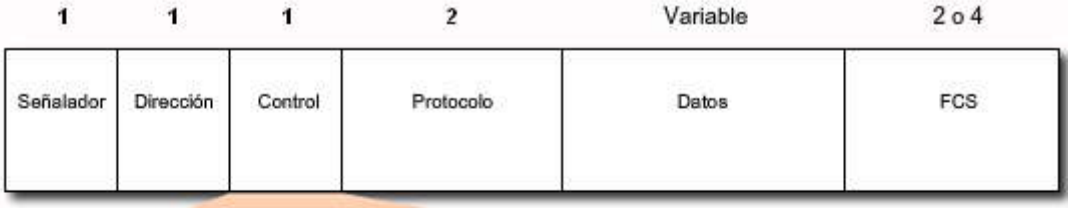
Longitud del campo, en bytes



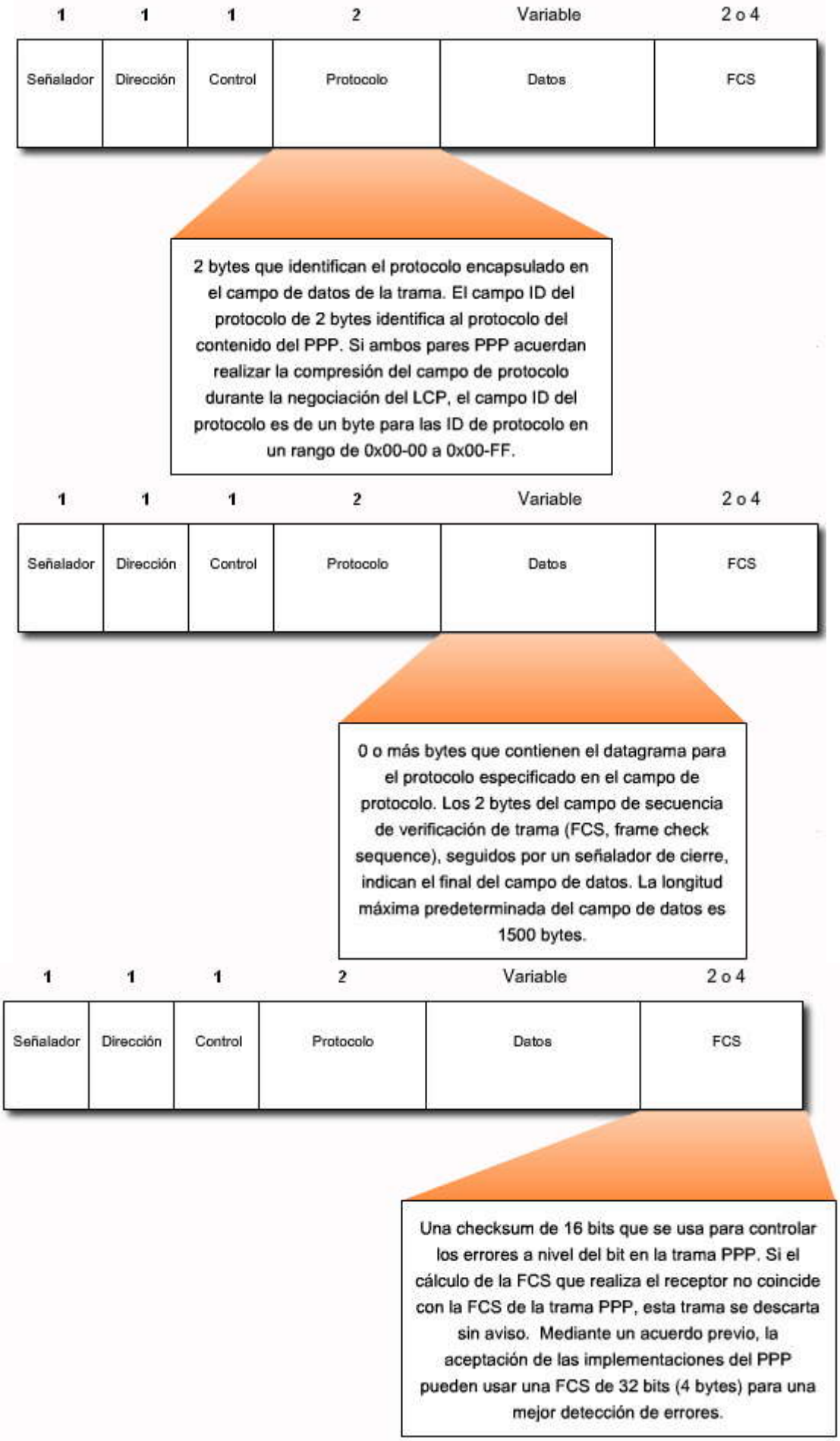
Indica el comienzo o el fin de una trama y consiste en la secuencia binaria 01111110 para identificar una trama PPP. Se establece el valor en 0x7E (secuencia de bits 011111110) para indicar el comienzo y el final de una trama PPP. En tramas PPP sucesivas sólo se usa un caracter de señalador único.



Está formada por la dirección de broadcast estándar, que es la secuencia binaria 11111111. El PPP no asigna direcciones de estaciones individuales.



1 byte formado por la secuencia binaria 00000011, que requiere la transmisión de datos del usuario en una trama no secuencial. Esto proporciona un servicio de enlace sin conexión que no requiere que se establezcan enlaces de datos o estaciones de enlaces. En entornos HDLC, el campo Dirección se usa para asignar la trama al nodo de destino. En un enlace punto a punto, no es necesario asignar el nodo de destino. Por lo tanto, para el PPP el campo Dirección se establece en 0xFF, la dirección de broadcast. Si ambos pares PPP acuerdan realizar la compresión de los campos de control y de dirección durante la negociación del LCP, el campo Dirección no se incluye.

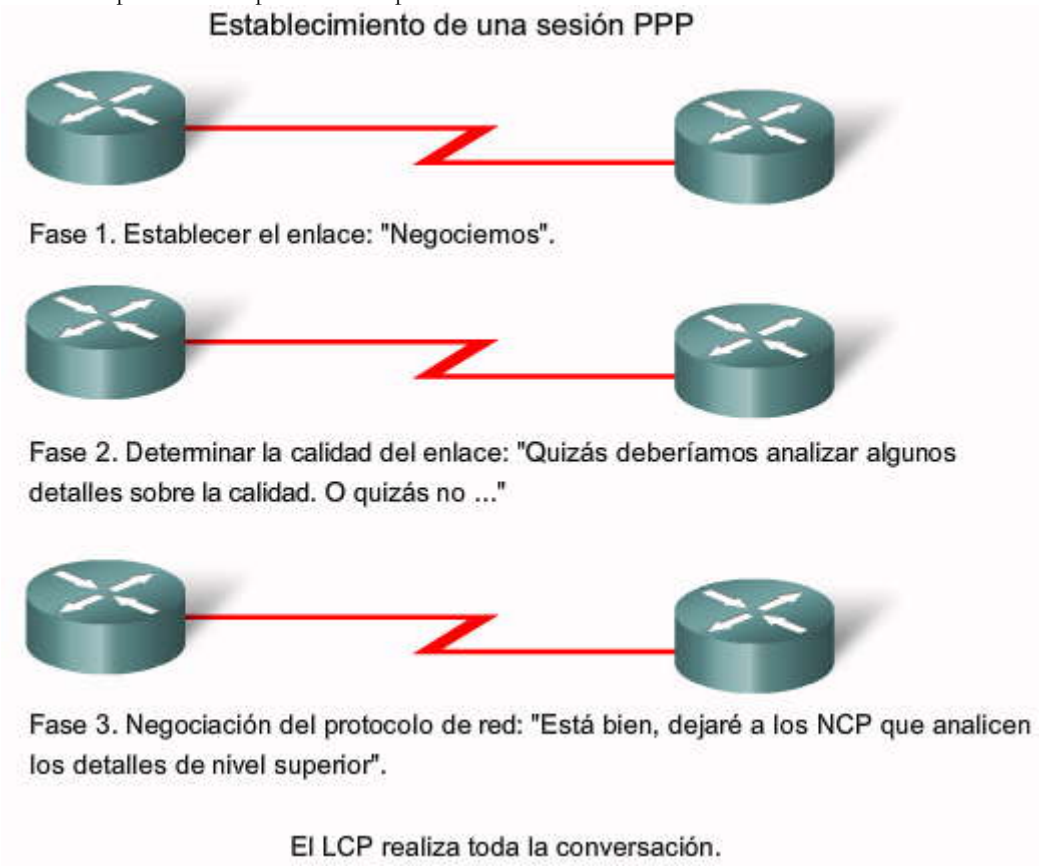

1
1
1
2
Variable
2 o 4
Señalador
Dirección
Control
Protocolo
Datos
FCS
2 bytes que identifican el protocolo encapsulado en el campo de datos de la trama. El campo ID del protocolo de 2 bytes identifica al protocolo del contenido del PPP. Si ambos pares PPP acuerdan realizar la compresión del campo de protocolo durante la negociación del LCP, el campo ID del protocolo es de un byte para las ID de protocolo en un rango de 0x00-00 a 0x00-FF.
1
1
1
2
Variable
2 o 4
Señalador
Dirección
Control
Protocolo
Datos
FCS
0 o más bytes que contienen el datagrama para el protocolo especificado en el campo de protocolo. Los 2 bytes del campo de secuencia de verificación de trama (FCS, frame check sequence), seguidos por un señalador de cierre, indican el final del campo de datos. La longitud máxima predeterminada del campo de datos es 1500 bytes.
1
1
1
2
Variable
2 o 4
Señalador
Dirección
Control
Protocolo
Datos
FCS
Una checksum de 16 bits que se usa para controlar los errores a nivel del bit en la trama PPP. Si el cálculo de la FCS que realiza el receptor no coincide con la FCS de la trama PPP, esta trama se descarta sin aviso. Mediante un acuerdo previo, la aceptación de las implementaciones del PPP pueden usar una FCS de 32 bits (4 bytes) para una mejor detección de errores.

2.2.4 Establecimiento de una sesión PPP

Establecimiento de una sesión PPP
La imagen muestra las tres fases del establecimiento de una sesión PPP.

- **Fase 1. Establecimiento del enlace y negociación de la configuración**: antes de que el PPP intercambie cualquier datagrama de capa de red (por ejemplo, IP), el LCP primero debe abrir la conexión y negociar los parámetros de configuración. Esta fase se completa cuando el router receptor envía una trama de acuse de recibo de configuración de vuelta al router que inicia la conexión.
- **Fase 2. Determinación de la calidad del enlace (opcional)**: el LCP prueba el enlace para determinar si su calidad es suficiente para establecer los protocolos de capa de red. El LCP puede demorar la transmisión de la información del protocolo de capa de red hasta que esta fase se complete.
- **Fase 3. Negociación de la configuración del protocolo de capa de red**: después de que el LCP haya finalizado la fase de determinación de la calidad del enlace, el NCP adecuado puede configurar, de manera separada, los protocolos de capa de red, y activarlos y desactivarlos en cualquier momento. Si el LCP cierra el enlace, informa a los protocolos de la capa de red para que puedan tomar las medidas adecuadas.

El enlace permanece configurado para las comunicaciones hasta que las tramas LCP o NCP explícitas cierran el enlace o hasta que se produzca algún hecho externo (por ejemplo, el vencimiento de un temporizador de inactividad o la intervención de un usuario). El LCP puede finalizar el enlace en cualquier momento. Por lo general, esto se realiza cuando uno de los routers solicita finalización, pero puede ocurrir debido a un evento físico, como la pérdida de una portadora o el vencimiento de un temporizador de periodo de espera.



2.2.5 Establecimiento de un enlace con el LCP

Operación LCP

La operación LCP incluye provisiones para el establecimiento de enlace, mantenimiento de enlace y finalización de enlace. La operación LCP utiliza tres clases de tramas LCP para llevar a cabo el trabajo de cada una de las fases del LCP.

- Las tramas de establecimiento de enlace establecen y configuran un enlace (Configure-Request, Configure-Ack, Configure-Nak y Configure-Reject)

- Las tramas de mantenimiento de enlace administran y depuran un enlace (Code-Reject, Protocol-Reject, Echo-Request, Echo-Reply, y Discard-Request)
- Las tramas de finalización de enlace finalizan un enlace (Terminate-Request y Terminate-Ack)

La primera fase de la operación LCP es el establecimiento del enlace. Esta fase se debe completar con éxito antes de que se intercambie algún paquete de capa de red. Durante el establecimiento de enlace, el LCP abre la conexión y negocia los parámetros de configuración.

Haga clic en el botón Negociación de enlace que se muestra en la imagen.

El proceso de establecimiento de enlace comienza con el dispositivo de inicio que envía una trama Configure-Request al contestador. La trama Configure-Request incluye un cantidad variable de opciones de configuración que se necesitan establecer en el enlace. En otras palabras, el iniciador envió una "lista de sugerencias" al contestador.

La lista de sugerencias del iniciador incluye opciones para establecer cómo quiere que se cree el enlace, lo que incluye el protocolo o los parámetros de autenticación. El contestador procesa la lista de sugerencias y, si es aceptable, responde con un mensaje Configure-Ack. Después de recibir el mensaje Configure-Ack, el proceso continúa con la etapa de autenticación.

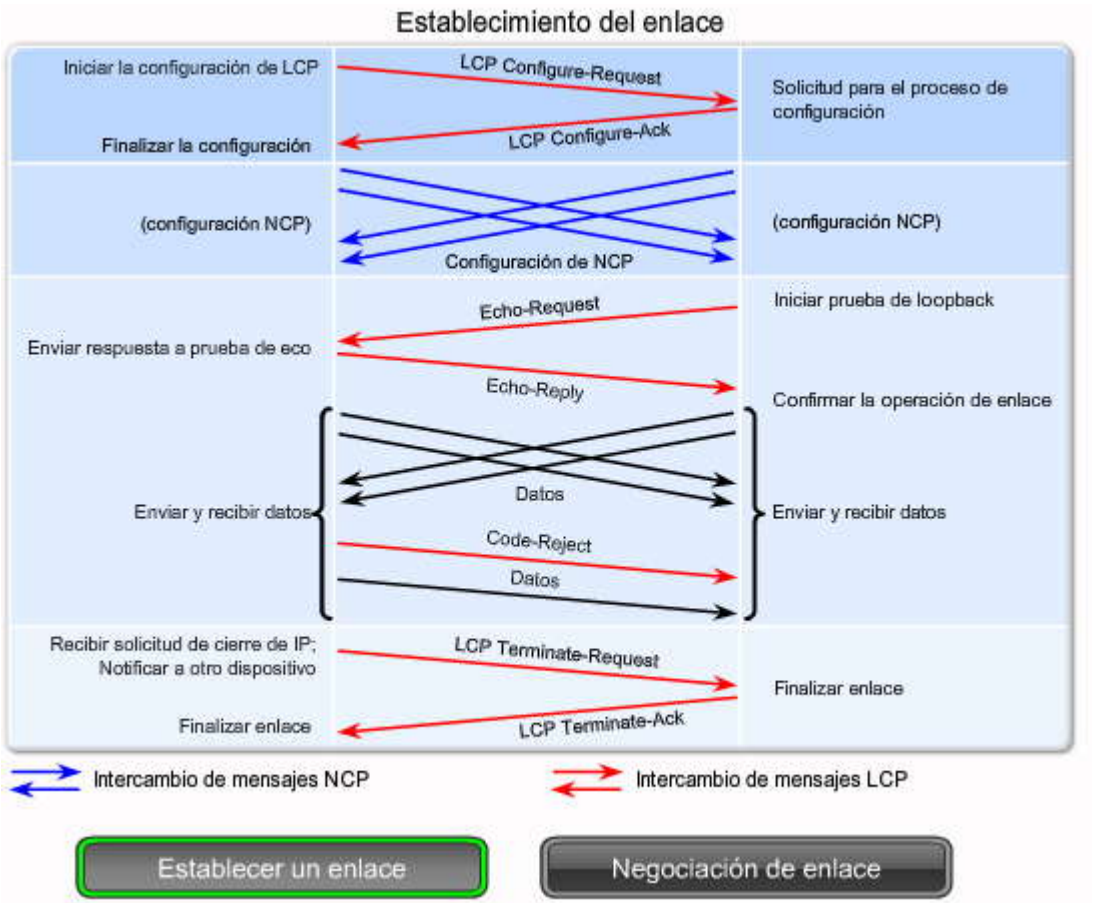
Si las opciones no son aceptables o reconocidas, el contestador envía un mensaje ConfigureNak o Configure-Reject. Si se recibe un Configure-Ack, la operación del enlace se entrega al NCP. Si un mensaje Configure-Nak o Configure-Reject se envía al solicitante, el enlace no se establece. Si la negociación falla, el iniciador necesita reiniciar el proceso con opciones nuevas.

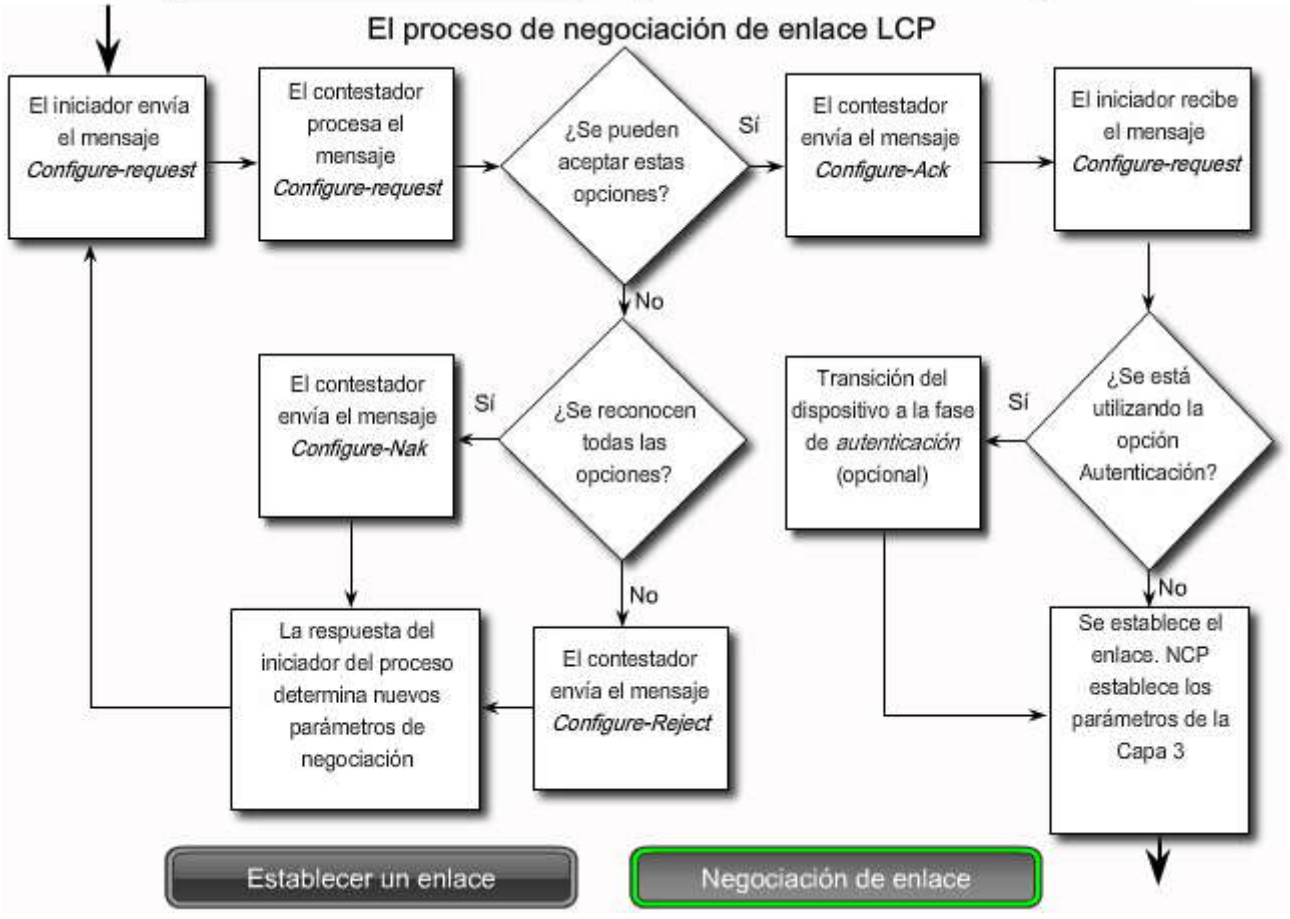
Durante el mantenimiento de enlace, el LCP puede utilizar mensajes para proporcionar comentarios y probar el enlace.

- Code-Reject y Protocol-Reject: estas tramas brindan comentarios cuando un dispositivo recibe una trama no válida debido a un código LCP no reconocido (tipo de trama LCP) o un mal identificador de protocolo. Por ejemplo, si se recibe un paquete que no es interpretable desde el peer, un paquete Code-Reject se envía en respuesta.
- Echo-Request, Echo-Reply y Discard-Request: estas tramas se pueden utilizar para probar el enlace.

Después de que se complete la transferencia de datos en la capa de red, el LCP finaliza el enlace. En la imagen, observe que el NCP sólo termina el enlace de la capa de red y el del NCP. El enlace permanece abierto hasta que el LCP lo termina. Si el LCP termina el enlace antes del NCP, la sesión NCP también termina.

El PPP puede terminar el enlace en cualquier momento. Esto puede suceder debido a la pérdida de la portadora, falla de la autenticación, falla de la calidad del enlace, el vencimiento de un temporizador de periodo de espera o el cierre administrativo del enlace. El LCP cierra el enlace al intercambiar los paquetes de terminación. El dispositivo que inicia el cierre envía un mensaje Terminate-Request. El otro dispositivo responde con un Terminate-Ack. Una solicitud de finalización indica que el dispositivo que realiza el envío necesita cerrar el enlace. Cuando el enlace se está cerrando, el PPP informa a los protocolos de capa de red para que puedan tomar las medidas adecuadas.





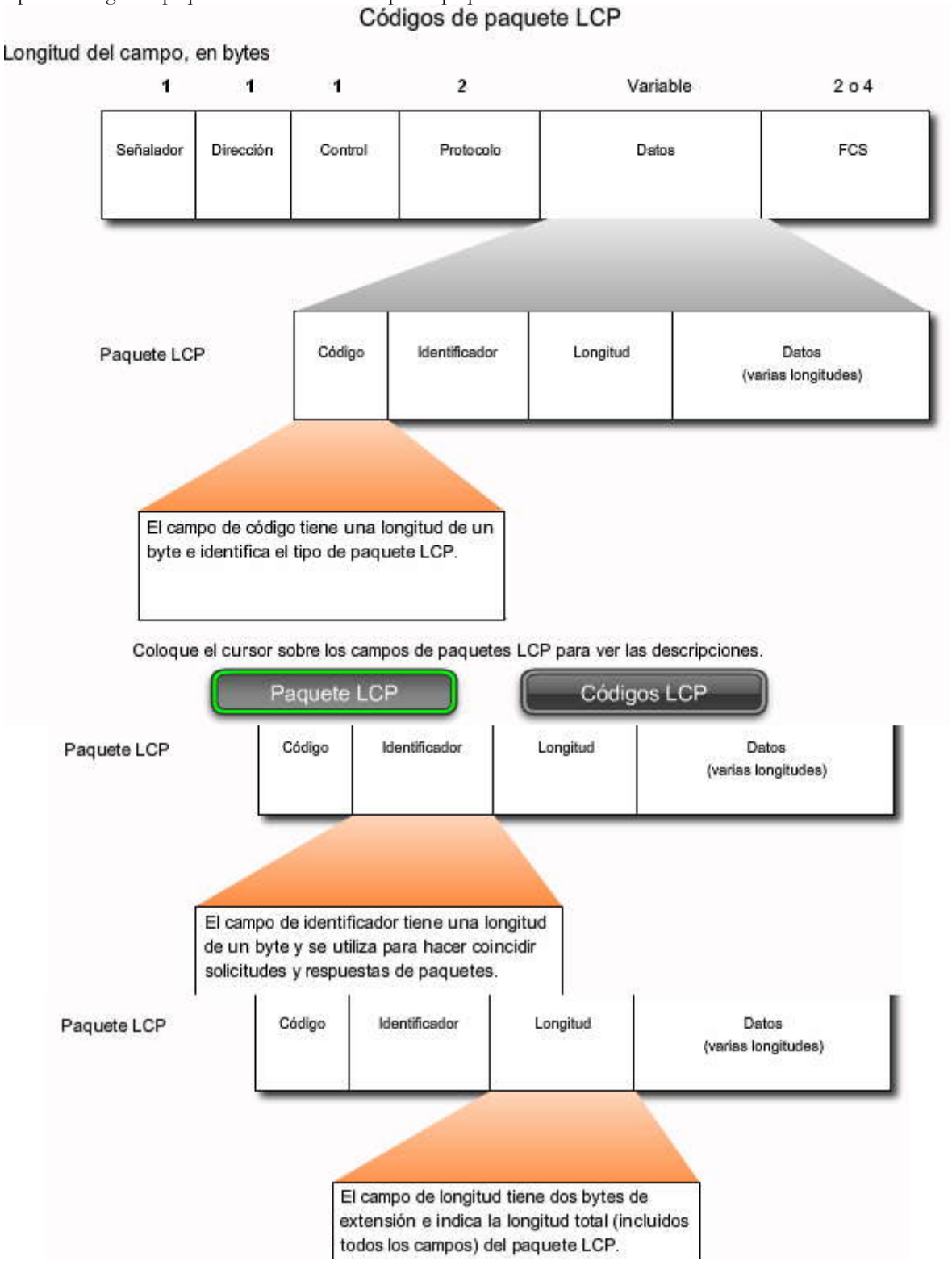
Paquete LCP
La imagen muestra los campos en un paquete LCP.

Coloque el cursor en cada campo y lea la descripción.

Cada paquete LCP es un único mensaje LCP que consiste en un campo de código LCP que identifica el tipo de paquete LCP, un campo de identificador para que las solicitudes y las respuestas puedan coincidir y un campo de longitud que indica el tamaño del paquete LCP y los datos específicos del tipo de paquete LCP.

Haga clic en el botón Códigos LCP en la imagen.

Cada paquete LCP tiene una función específica en el intercambio de información de configuración, según el tipo de paquete. El campo de código del paquete LCP identifica el tipo de paquete de acuerdo con la tabla.



Campos de paquete LCP

Código LCP	Tipo de paquete LCP	Descripción
1	Configure-Request	Se envía para abrir o restablecer una conexión PPP. El mensaje Configure-Request contiene una lista de opciones LCP con cambios para los valores de las opciones predeterminadas.
2	Configure-Ack	Se envía cuando todos los valores de todas las opciones LCP en la última solicitud de configuración recibida son reconocidos y aceptados. Cuando ambos pares PPP envían y reciben acuses de recibo de configuración, se completa la negociación LCP.
3	Configure-Nack	Se envía cuando todas las opciones LCP son reconocidas, pero los valores de algunas opciones no son aceptados. El mensaje Configure-Nak incluye las opciones que producen la falla y sus valores aceptados.
4	Configure-Reject	Enviado cuando las opciones de LCP no son reconocidas o aceptadas para la negociación. El mensaje Configure-Reject incluye las opciones no reconocidas o no negociables.
5	Terminate-Request	Se envía opcionalmente para cerrar la conexión PPP.
6	Terminate-Ack	Se envía en respuesta al mensaje Terminate-Request.
7	Code-Reject	Se envía cuando se desconoce el código LCP. Este mensaje incluye el paquete LCP que produce la falla.
8	Protocol-Reject	Se envía cuando la trama PPP contiene un ID de protocolo desconocido. Este mensaje incluye el paquete LCP que produce la falla. El mensaje Protocol-Reject es enviado normalmente por un par PPP en respuesta a un NCP de PPP para un protocolo de LAN no habilitado en el par PPP.
9	Echo-Request	Se envía opcionalmente para probar la conexión PPP.
10	Echo-Reply	Se envía en respuesta a un mensaje Echo-Request. Los mensajes Echo-Request y Echo-Reply de PPP no están relacionados con los mensajes Echo Request y Echo Reply de ICMP.
11	Discard-Request	Se envía opcionalmente para practicar el enlace en la dirección de salida.

Paquete LCP Códigos LCP

Opciones de configuración PPP
El PPP se puede configurar para admitir varias funciones que incluyen:

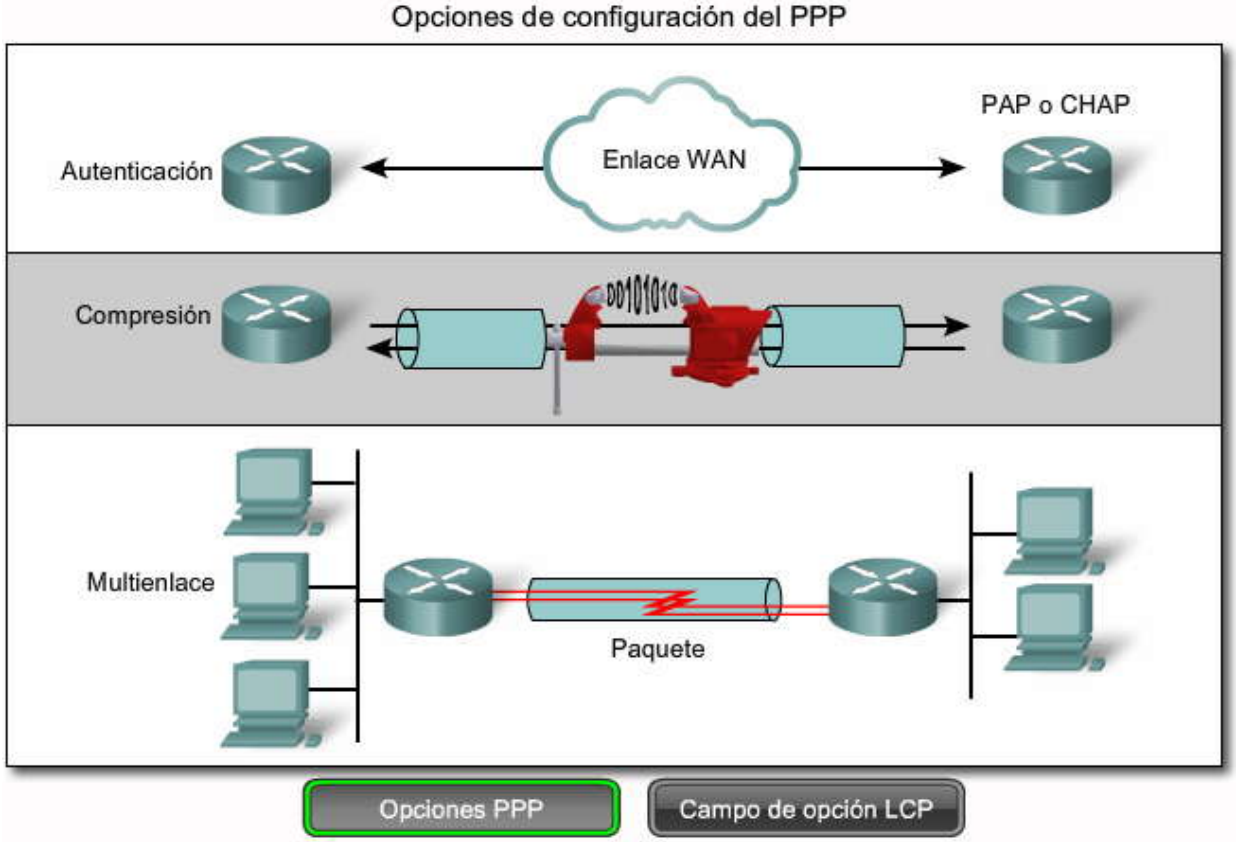
- Autenticación con PAP o CHAP
- Compresión con Stacker o Predictor
- Multienlace que combina dos o más canales para aumentar el ancho de bandaWAN

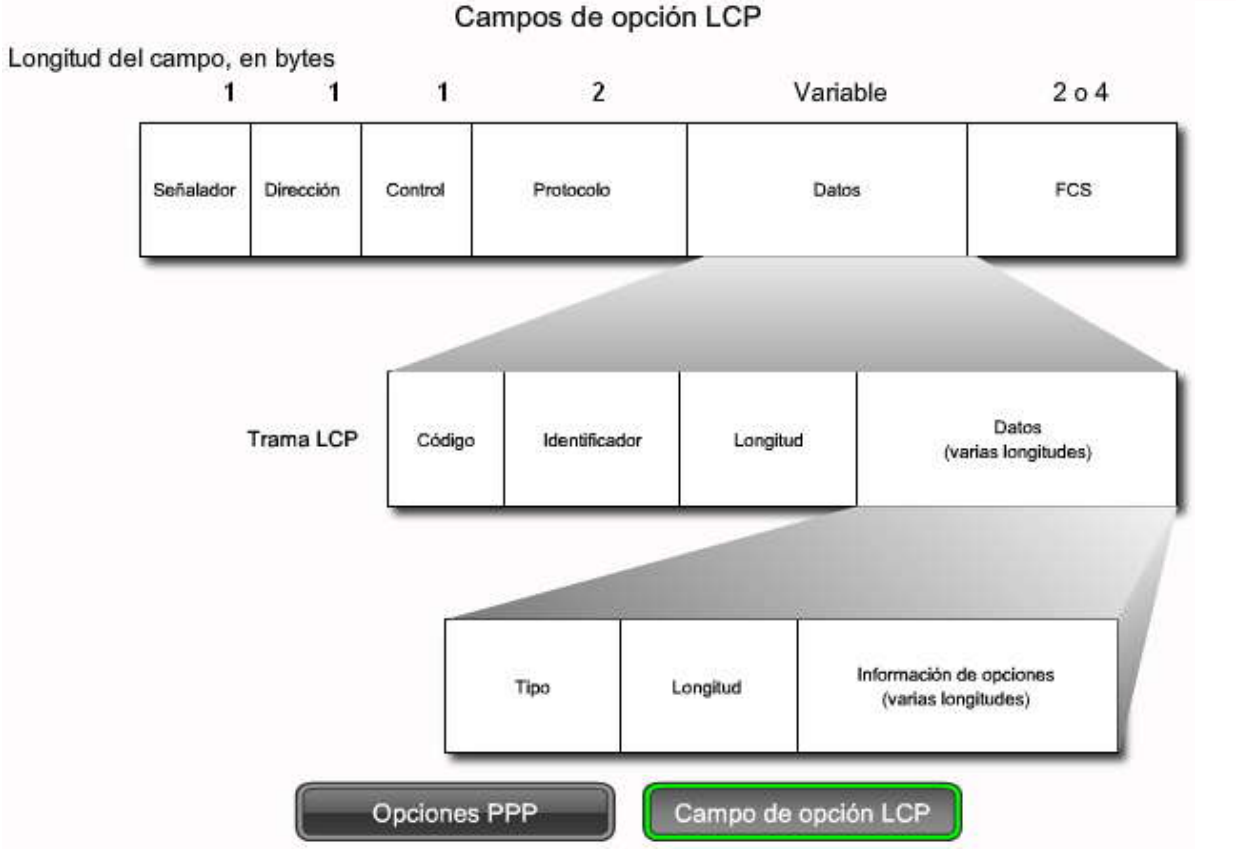
Estas opciones se analizan con mayor detalle en la próxima sección.

Haga clic en el botón Campo de opción LCP en la imagen.

Para negociar el uso de estas opciones PPP, las tramas de establecimiento del enlace LCP contienen información de opciones en el campo Datos de la trama LCP. Si no se incluye ninguna opción de configuración en una trama LCP, se adopta el valor predeterminado para esa configuración.

Esta fase queda completa después de enviar y recibir una trama de acuse de recibo de configuración.





2.2.6 Explicación de NCP

Proceso NCP

Una vez que se haya iniciado el enlace, el LCP pasa el control al NCP adecuado. A pesar de estar diseñado, inicialmente, para datagramas IP, el PPP puede contener datos desde varios tipos de protocolos de capa de red al usar un enfoque modular en su implementación. También puede contener dos o más protocolos de Capa 3 de forma simultánea. Su modelo modular permite que el LCP establezca el enlace y luego entregue los detalles de un protocolo de red a un NCP específico. Cada protocolo de red tiene un NCP correspondiente. Cada NCP tiene un RFC correspondiente. Hay NCP para IP, IPX, AppleTalk y muchos más. Los NCP usan el mismo formato de paquete que los LCP.

Después de que el LCP haya configurado y autenticado el enlace básico, el NCP adecuado se solicita para completar la configuración específica del protocolo de capa de red que se está usando. Cuando el NCP haya configurado, de manera exitosa, el protocolo de capa de red, el protocolo de red se encuentra en estado abierto en el enlace LCP establecido. En este punto, el PPP puede contener los paquetes de protocolos de capa de red correspondientes.

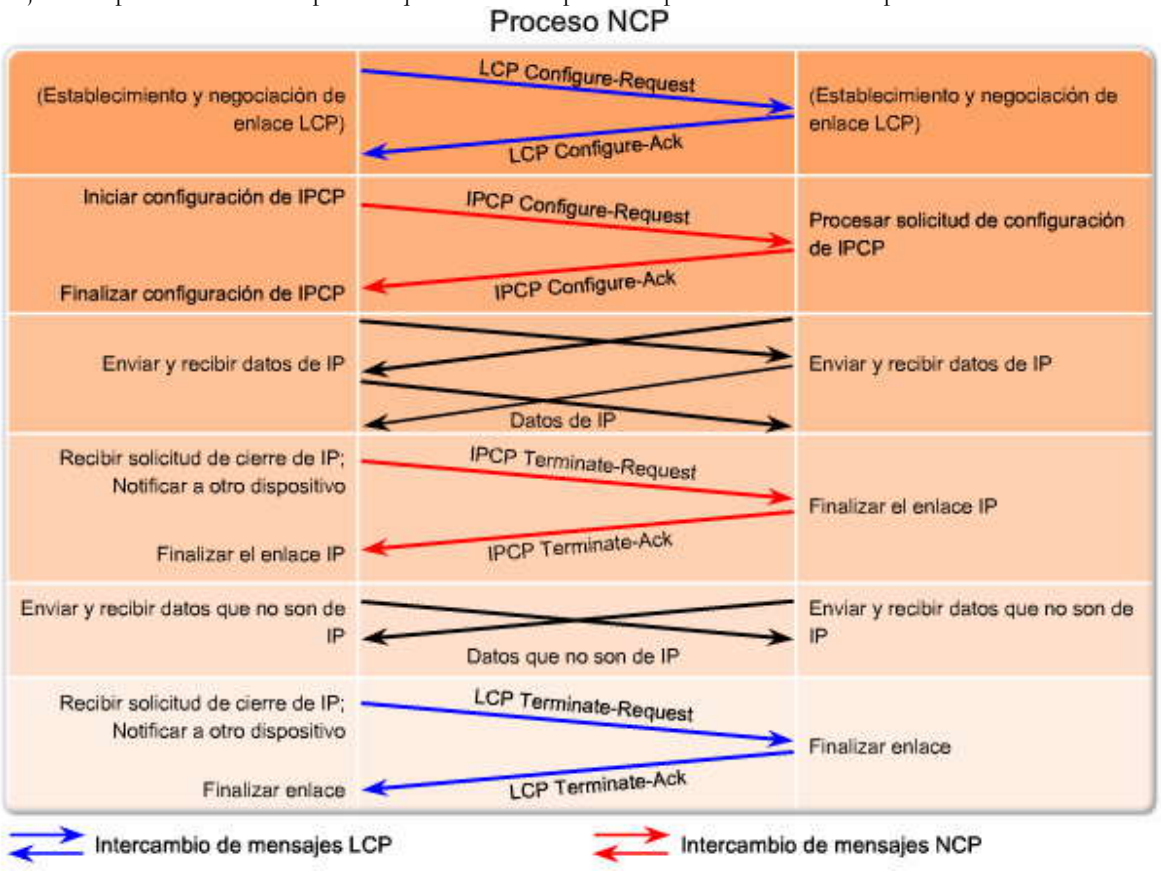
Ejemplo de IPCP

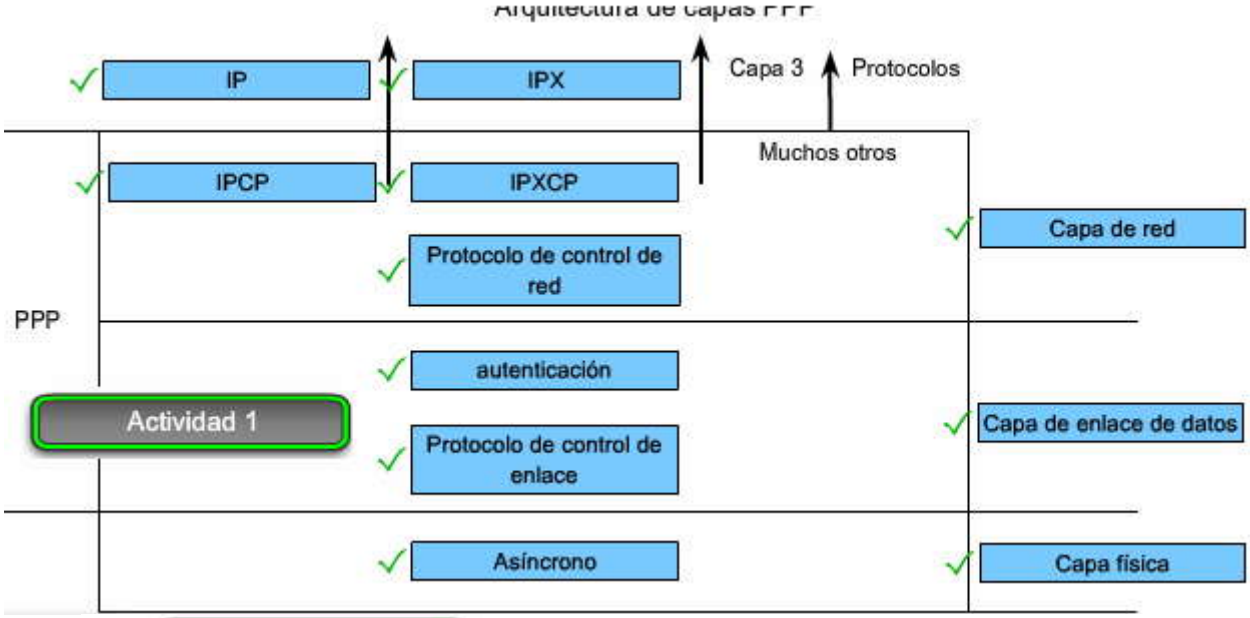
Como un ejemplo de cómo trabaja la capa NCP, se utiliza IP, que es el protocolo de Capa 3 más común. Una vez que el LCP estableció el enlace, los routers intercambian mensajes IPCP y negocian opciones específicas del protocolo. IPCP es responsable de la configuración, la activación y la desactivación de los módulos de IP en ambos extremos del enlace.

IPCP negocia dos opciones.

- Compresión: permite que los dispositivos negocien un algoritmo para comprimir encabezados TCP e IP y ahorrar ancho de banda. La compresión de encabezados TCP/IP Van Jacobson reduce el tamaño de bs encabezados TCP/IP a sólo 3 bytes. Esto puede ser un avance importante en líneas seriales lentas, en especial para el tráfico interactivo.
- Dirección IP: permite que el dispositivo de inicio especifique una dirección IP para enrutar tráfico IP sobre el enlace PPP o para solicitar una dirección IP para el contestador. En general, los enlaces de red dialup usan la opción de dirección IP.

Cuando el proceso NCP se completa, el enlace se pasa al estado abierto y el LCP toma el control nuevamente. El tráficode enlace consta de toda posible combinación de paquetes LCP, NCP y protocolos de capa de red. La imagen muestra cómo los mensajes LCP pueden ser usados por cualquiera de los dispositivos para administrar o depurar el enlace.



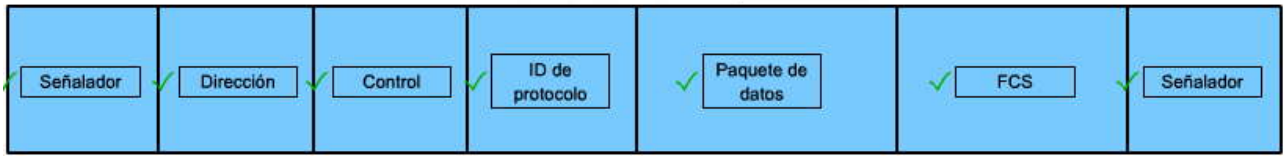


Actividad 2

Funciones LCP y NCP

	LCP	NCP
Negocia y establece las opciones de control en el enlace de datos WAN	✓	
Transporta paquetes desde varios protocolos de capa de red		✓
La función principal es establecer, configurar y probar la conexión de enlace de datos	✓	
Finaliza el enlace	✓	
Activa y desactiva los protocolos de capa de red		✓
Determina cuándo un enlace funciona correctamente o cuándo falla	✓	
Encapsula y negocia las opciones para IP e IPX		✓

Formato de trama PPP **Actividad 3**



Completar oraciones

Actividad 4	
PPP utiliza el protocolo _____ como base para encapsular datagramas a través de enlaces punto a punto.	HDLC
PPP utiliza _____ para establecer, configurar y probar la conexión de enlace de datos.	LCP
PPP usa _____ para establecer y configurar los distintos protocolos de capa de red.	NCP
La secuencia binaria para el campo de dirección en una trama PPP es _____.	11111111
Se completa la fase de establecimiento del enlace cuando una trama _____ de configuración ha sido enviada y recibida.	acuse de recibo
IPCP negocia dos opciones: compresión y asignaciones _____.	Dirección IP
Cuando el proceso NCP se completa, el enlace pasa al estado _____ y el LCP toma el control nuevamente.	Abierto

2.3 Configuración del PPP

2.3.1 Opción de configuración del PPP

Opciones de configuración del PPP

En la sección anterior, se presentaron las opciones LCP que usted puede configurar para satisfacer los requisitos específicos de conexiones WAN. El PPP puede incluir las siguientes opciones LCP.

- **Autenticación**: los routers pares intercambian mensajes de autenticación. Dos opciones de autenticación son el Protocolo de autenticación de contraseña (PAP) y el Protocolo de autenticación de intercambio de señales (CHAP). La autenticación se explica en la siguiente sección.
- **Compresión**: aumenta el rendimiento efectivo en conexiones PPP al reducir la cantidad de datos en la trama que debe viajar a través del enlace. El protocolo descomprime la trama al llegar a su destino. Dos protocolos de compresión disponibles en los routers Cisco son Stacker y Predictor.
- **Detección de errores**: identifica condiciones defectuosas. Las opciones de Calidad y Número mágico ayudan a garantizar un enlace de datos confiable y sin bucles. El campo Número mágico ayuda a detectar enlaces que se encuentran en una condición de loopback. Hasta que la opción de configuración del número mágico se haya negociado de manera exitosa, el número mágico se debe trasmitir como cero. Los números mágicos se generan de manera aleatoria en cada extremo de la conexión.
- **Multienlace**: los IOS Cisco Versión 11.1 y posteriores admiten el PPP multienlace. Esta alternativa proporciona el balanceo de carga en las interfaces del router utilizadas por PPP. El PPP multienlace (también conocido como MP, MPPP, MLP o Multienlace) proporciona un método para diseminar el tráfico a través de múltiples enlaces físicos WAN a la vez que proporciona la fragmentación y el reensamblaje de paquetes, la secuencia adecuada, la interoperabilidad de múltiples proveedores y el balanceo de carga en el tráfico entrante y saliente. El multienlace no se incluye en este curso.
- **Devolución de llamadas en PPP**: para aumentar la seguridad, el IOS de Cisco Versión 11.1 y posteriores ofrece devolución de llamadas en PPP. Con esta opción LCP, un router Cisco puede actuar como cliente de la devolución de llamada o servidor de la devolución de llamada. El cliente realiza la llamada inicial, solicita que el servidor le devuelva la llamada y finaliza la comunicación inicial. El router de devolución de llamadas responde al llamado inicial y se comunica nuevamente con el cliente según las sentencias de configuración. El comando es **ppp callback** [**accept** | **request**].

Cuando las opciones se configuran, un valor de campo correspondiente se inserta en el campo Opción del LCP.

Códigos de campo de opciones configurables

Nombre de la opción	Tipo de opción	Longitud de la opción	Descripción
Unidad máxima de recepción (MRU, maximum receive unit)	1	4	La MRU es el tamaño máximo de una trama PPP y no puede exceder 65 535. El valor predeterminado es 1500 y si ningún par cambia este parámetro, no se negocia.
Mapa de caracteres de control asíncrono (ACCM, Asynchronous Control Character Map)	2	6	Es un mapa de bits que le permite a los caracteres escapar de los enlaces asíncronos. Los escapes de caracteres se efectúan en forma predeterminada.
Protocolo de autenticación	3	5 o 6	Este campo indica el protocolo de autenticación, ya sea el PAP o el CHAP.
Número mágico	5	6	Es un número elegido de manera aleatoria para distinguir un par y detectar las líneas de loopback.
Compresión de protocolo	7	2	Un señalador que indica que la ID del protocolo PPP se comprimirá a un solo octeto cuando la ID del protocolo de 2 bytes se encuentre en el rango de 0x00-00 a 0x00-FF.
Compresión de campos de dirección y control	8	2	Un señalador que indica que el campo Dirección de PPP (siempre establecido en 0xFF) y el campo Control de PPP (siempre establecido en 0x03) se eliminarán del encabezado PPP.
Devolución de llamada	13 o 0x0D	3	Un indicador de 1 octeto que muestra cómo se determinan las devoluciones de llamadas.

2.3.2 Comandos de configuración PPP

Comandos de configuración del PPP

Antes de que realmente configure el PPP en una interfaz serial, analizaremos los comandos y la sintaxis de estos comandos tal como se muestra en la imagen. Esta serie de ejemplos le indican cómo configurar el PPP y algunas de las opciones.

Ejemplo 1: Habilitación del PPP en una interfaz

Para configurar el PPP como el método de encapsulación usado por una interfaz serial o ISDN, use el comando de configuración de interfaz **encapsulation ppp**.

El siguiente ejemplo activa la encapsulación PPP en una interfaz serial 0/0:

R3#**configure terminal**

R3(config)#**interface serial 0/0**

R3(config-if)#**encapsulation ppp**

El comando **encapsulation ppp** no tiene argumentos; sin embargo, primero debe configurar el router con un protocolo de enrutamiento IP para usar encapsulación PPP. Debe recordar que si no configura el PPP en un router Cisco, la encapsulación predeterminada para las interfaces seriales es el HDLC.

Ejemplo 2: Compresión

Puede configurar la compresión de un software punto a punto en interfaces seriales después de que haya activado la encapsulación PPP. Debido a que esta opción activa un proceso de compresión de software, el rendimiento del sistema se puede afectar. Si el tráfico ya consta de archivos comprimidos (por ejemplo .zip, .tar o .mpeg), no use esta opción. La imagen muestra la sintaxis del comando para el comando **compress**.

Para configurar la compresión en PPP, introduzca los siguientes comandos:

R3(config)#**interface serial 0/0**

R3(config-if)#**encapsulation ppp**

R3(config-if)#**compress** [**predictor** | **stac**]

Ejemplo 3: Monitoreo de la calidad del enlace

Tenga presente de nuestro análisis las fases LCP, que el LCP brinda una fase de determinación de la calidad del enlace opcional. En esta fase, el LCP prueba el enlace para determinar si su calidad es suficiente para usar protocolos de Capa 3. El comando **ppp quality** *percentage* garantiza que el enlace satisface los requisitos de calidad que estableció, de lo contrario el enlace se cerraría.

Los porcentajes se calculan tanto para las direcciones entrantes como para las salientes. La calidad de salida se calcula al comparar la cantidad total de paquetes y bytes enviados con la cantidad total de paquetes y bytes recibidos por el nodo de destino. La calidad de entrada se calcula al comparar la cantidad total de paquetes y bytes recibidos con la cantidad total de paquetes y bytes enviados por el nodo de destino.

Si el porcentaje de calidad del enlace no se mantiene, el enlace se considera de mala calidad y se desactiva. El monitoreo de la calidad del enlace (LQM, Link Quality Monitoring) implementa un retraso para que el enlace no rebote hacia arriba y hacia abajo.

Este ejemplo de configuración monitorea los datos que se decartan del enlace y evita la formación de bucles en la trama:

R3(config)#**interface serial 0/0**

R3(config-if)#**encapsulation ppp**

R3(config-if)#**ppp quality 80**

Use el comando **no ppp quality** para desactivar el LQM.

Ejemplo 4: Balanceo de carga a través de enlaces

El PPP multienlace (también conocido como MP, MPPP, MLP o Multienlace) proporciona un método para diseminar el tráfico a través de múltiples enlaces físicos WAN, a la vez que proporciona la fragmentación y el reensamblaje de paquetes, la secuencia adecuada, la interoperabilidad de múltiples proveedores y el balanceo de carga en el tráfico entrante y saliente.

El MPPP permite que los paquetes se fragmenten y envía estos fragmentos, de forma simultánea, sobre múltiples enlaces punto a punto a las mismas direcciones remotas. Los múltiples enlaces físicos se presentan en respuesta a un umbral de carga definido por el usuario. El MPPP puede medir la carga sólo en el tráfico entrante o sólo en el tráfico saliente, pero no en la carga combinada del tráfico entrante y el tráfico saliente.

Los siguientes comandos ejecutan el balanceo de carga en múltiples enlaces:

Router(config)#**interface serial 0/0**

Router(config-if)#**encapsulation ppp**

Router(config-if)#**ppp multilink**

El comando **multilink** no tiene argumentos. Para desactivar el multienlace PPP, use el comando **no ppp multilink**.

Comandos de configuración PPP

```
Router(config-if)#compress [predictor | stac]
```

Palabra clave	Descripción
Predictor	(Opcional) Especifica que se utilizará un algoritmo de compresión predictor.
Stac	(Opcional) Especifica que se utilizará un algoritmo de compresión Stacker (LZS).

```
Router(config-if)#ppp quality percentage
```

Palabra clave	Descripción
Porcentaje	Especifica el umbral de calidad del enlace. El rango es de 1 a 100.

2.3.3 Verificación de una configuración de encapsulación serial PPP

Verificación de la configuración de encapsulación PPP
Use el comando **show interfaces serial** para verificar la configuración correcta de la encapsulación HDLC o PPP. El resultado del comando en la imagen muestra una configuración PPP.

Al configurar el HDLC, el resultado del comando **show interfaces serial** debería mostrar "encapsulation HDLC" (encapsulación HDLC). Cuando configura el PPP, puede verificar los estados LCP y NCP.

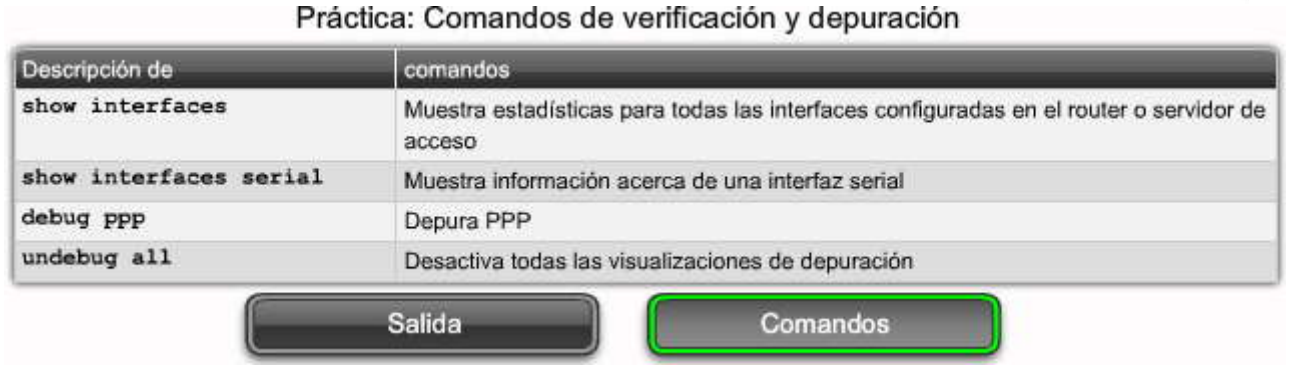
Haga clic en el botón Comandos que se muestra en la imagen.

La imagen resume los comandos utilizados al verificar el PPP.

Verificación de una configuración de encapsulación serial PPP

```
R2#show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:07, output 00:00:07, output hang never
  Last clearing of "show interface" counters 00:00:11
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/32 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 96 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     6 packets input, 76 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     7 packets output, 84 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

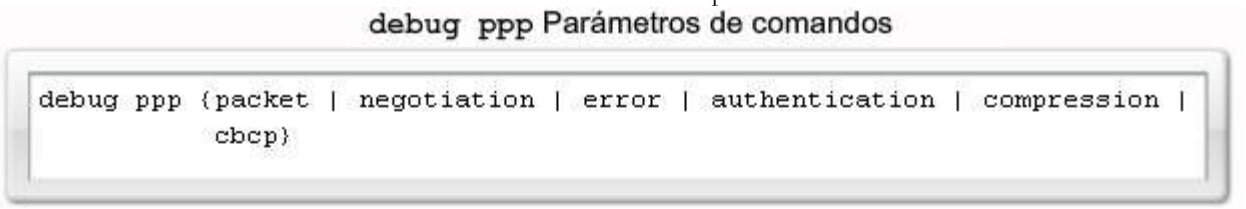
Salida | Comandos



2.3.4 Resolución de problemas de encapsulación PPP

Resolución de problemas de la configuración de la encapsulación serial
En este punto, usted ya sabe que el comando **debug** se usa para la resolución de problemas y que se accede a él desde el modo exec privilegiado de la interfaz de línea de comando. La depuración muestra información acerca de las distintas operaciones del router y el tráfico relacionado, generado o recibido por el router, y acerca de cualquier mensaje de error. Es una herramienta muy útil e informativa, pero usted siempre debe recordar que el IOS de Cisco trata la depuración como una tarea de prioridad alta. Puede consumir una gran cantidad de recursos y el router es forzado a procesar-conmutar los paquetes que se están depurando. La depuración no se debe usar como una herramienta de monitoreo, ya que se debe usar por un periodo de tiempo corto para la resolución de problemas. Cuando se realiza la resolución de problemas de una conexión serial, se utiliza el mismo enfoque que ha usado en otras tareas de configuración.

Use el comando **debug ppp** para mostrar información acerca de la operación del PPP. La imagen muestra la sintáxis del comando. La forma **no** de este comando desactiva el resultado de la depuración.

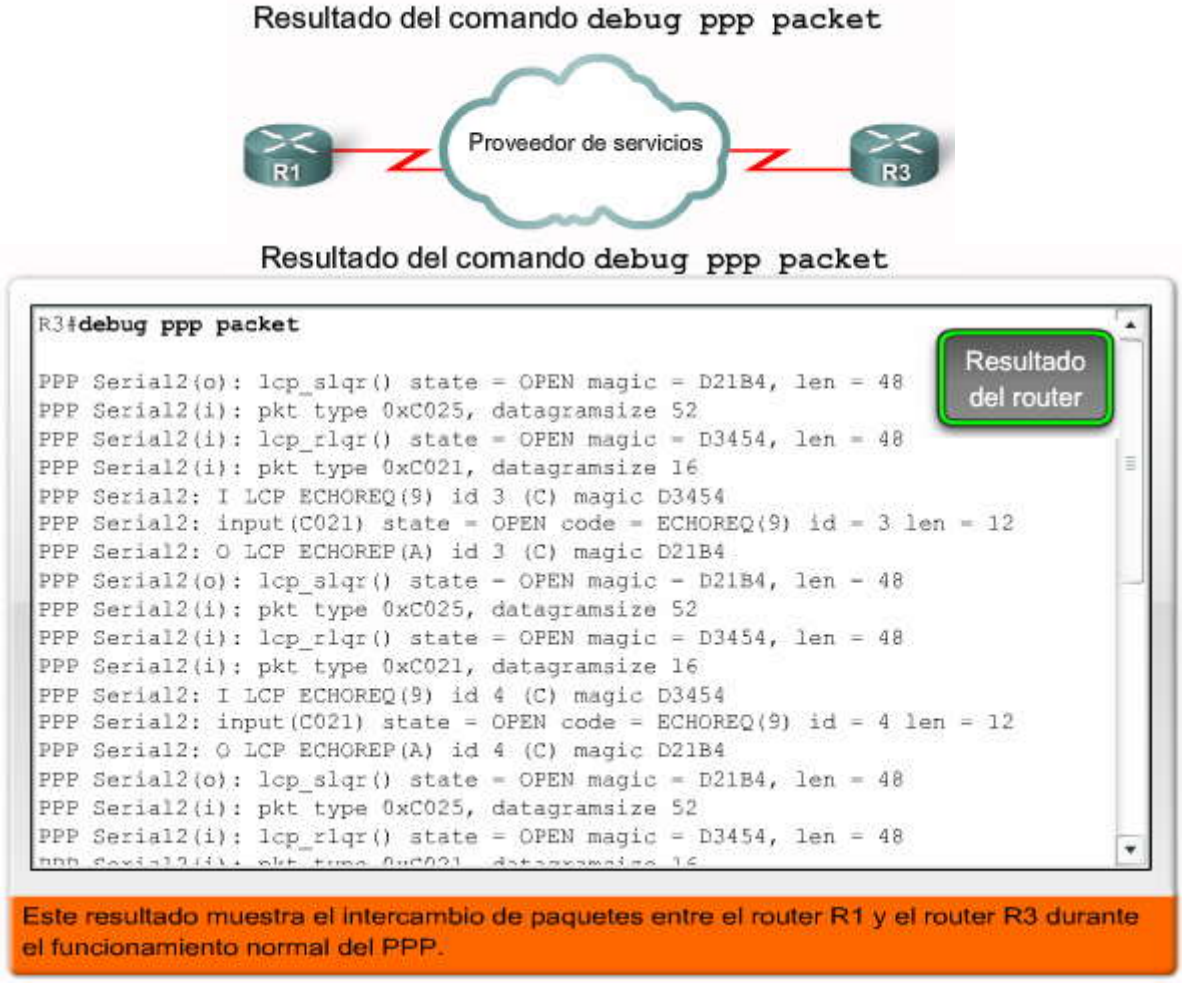


Parámetro	Uso
paquete	Muestra los paquetes PPP enviados y recibidos. (Este comando muestra las descargas de los paquetes de bajo nivel).
negociacin	Muestra los paquetes PPP enviados durante el inicio de PPP, cuando se negocian las opciones de PPP.
error	Muestra los errores de protocolo y las estadísticas de error relacionadas con la negociación y operación de la conexión PPP.
autenticacin	Muestra mensajes de protocolo de autenticación, incluidos los intercambios de paquetes del protocolo de autenticación de señales (CHAP, Challenge Authentication Protocol) y del protocolo de autenticación de contraseña (PAP, Password Authentication Protocol).
compresin	Muestra información específica para el intercambio de conexiones PPP mediante MPPC. Este comando es útil para obtener información sobre los números de secuencias de los paquetes incorrectos cuando la compresión MPPC se encuentra habilitada.
cbcp	Muestra los errores de protocolo y las estadísticas relacionadas con las negociaciones de conexión PPP mediante el uso de MSCB.

Resultado del comando debug ppp packet
Un buen comando para utilizar cuando resuelva problemas de la encapsulación de la interfaz serial es el comando **debug ppp packet**. El ejemplo en la imagen es resultado del comando **debug ppp packet**, tal como se observa desde el monitor de calidad de enlace (LQM, Link Quality Monitor) de la conexión. El ejemplo de muestra describe intercambios de paquetes bajo operación normal de PPP. Éste es sólo un listado parcial, pero suficiente para prepararlo para la práctica de laboratorio.

Observe cada línea en el resultado y únala al significado del campo. Utilice la siguiente guía para su análisis del resultado.

- PPP: resultado de la depuración PPP.
- Serial2: número de la interfaz asociado con esta información de depuración.
- (o), S: el paquete que se detectó es un paquete saliente.
- (i), E: el paquete que se detectó es un paquete entrante.
- lcp_slqr(): nombre del procedimiento; LQM en ejecución, envíe un informe de la calidad del enlace (LQR, Link Quality Report).
- lcp_rlqr(): nombre del procedimiento; LQM en ejecución, recibió un LQR.
- input (C021): el router recibió un paquete del tipo de paquete especificado (en hexadecimal). Un valor de C025 indica un paquete de tipo LQM.
- state = ABIERTO: estado PPP; estado normal es OPEN (ABIERTO).
- magic = D21B4: el número mágico para el nodo indicado. Cuando se indica el resultado, éste es el número mágico del nodo en el que se habilita la depuración. El número mágico real depende de si el paquete detectado se indica como E o S.
- datagramsize = 52: longitud del paquete, incluido el encabezado.
- code = ECHOREQ(9): identifica el tipo de paquete recibido en forma de cadena y hexadecimal.
- len = 48: longitud del paquete sin encabezado.
- id = 3: número de identificación por formato de paquete de protocolo de control de enlace (LCP, Link Control Protocol).
- pkt type 0xC025: tipo de paquete en hexadecimal. Los paquetes típicos son C025 para LQM y C021 para LCP.
- LCP ECHOREQ (9): solicitud de eco. El valor entre paréntesis es la representación hexadecimal del tipo LCP.
- LCP ECHOREP (A): respuesta de eco. El valor entre paréntesis es la representación hexadecimal del tipo LCP.



Resultado del comando debug ppp negotiation

La imagen muestra el resultado del comando **debug ppp negotiation** en una negociación normal, en donde ambas partes acuerdan sobre los parámetros del programa de control de red (NCP, network control program). En este caso, se propone y se reconoce el IP del tipo de protocolo. Se toma el resultado de una línea o dos a la vez:

las primeras dos líneas indican que el router está tratando de activar el LCP y que utilizará las opciones de negociación indicadas (protocolo de calidad y número mágico). Los campos de valores son los valores de las opciones en sí mismas. C025/3E8 se traduce a protocolo de calidad LQM. 3E8 es el periodo de informe (en centésimas de segundo). 3D56CAC es el valor del Número mágico para el router.

ppp: enviando CONFREQ, tipo = 4 (CI_QUALITYTYPE), valor = C025/3E8

ppp: enviando CONFREQ, tipo = 5 (CI_MAGICNUMBER), valor = 3D56CAC

Las próximas dos líneas indican que el otro lado negoció por las opciones 4 y 5, y que solicitó y reconoció a ambas. Si el extremo que responde no admite las opciones, el nodo que responde envía un CONFREJ. Si el extremo que responde no acepta el valor de la opción, éste envía un CONFNAK con el campo de valor modificado.

ppp: received config for type = 4 (QUALITYTYPE) acked

ppp: received config for type = 5 (MAGICNUMBER) value = 3D567F8 acked (ok)

Las próximas tres líneas indican que el router recibió un CONFACK del lado que responde y muestra valores de opción aceptados. Utilice el campo rcvd id para verificar si el CONFREQ y el CONFACK tienen el mismo campo de id.

PPP Serial4: state = ACKSENT fsm_rconfack(C021): rcvd id 5

ppp: config ACK received, type = 4 (CI_QUALITYTYPE), value = C025

ppp: config ACK received, type = 5 (CI_MAGICNUMBER), value = 3D56CAC

La siguiente línea indica que el router tiene el enrutamiento de IP habilitado en esta interfaz y que el IPCP NCP negoció satisfactoriamente.

ppp: ipcp_reqci: returning CONFACK
(ok)

Resultado del comando debug ppp error
Puede utilizar el comando **debug ppp error** para mostrar los errores de protocolo y las estadísticas de los errores relacionados con la negociación y la operación de la conexión PPP. Estos mensajes pueden aparecer cuando la opción del protocolo de calidad está habilitada en una interfaz que ya está ejecutando PPP. La imagen muestra un ejemplo.

Observe cada línea en el resultado y únala al significado del campo. Utilice la siguiente guía para su análisis del resultado.

- PPP: resultado de la depuración PPP.
- Serial3(i): número de la interfaz relacionada con esta información de depuración; indica que éste es un paquetede entrada.
- rlqr recibe una falla: el receptor no acepta el pedido para negociar la opción del protocolo de calidad.
- myrcvdiffp = 159: número de paquetes recibidos durante el periodo especificado.
- peerxmitdiffp = 41091: número de paquetes enviados por el nodo remoto durante este periodo.
- myrcvdiffo = 2183: número de octetos recibidos durante este periodo.
- peerxmitdiffo = 1714439: número de octetos enviados por el nodo remoto durante este periodo.
- umbral = 25: porcentaje de error máximo aceptable en esta interfaz. Este porcentaje se calcula con el valor de umbral ingresado en el comando **ppp quality** *percentage* de configuración de la interfaz. Un valor de número 100 menos es el porcentaje de error máximo. En este caso, se ingresó el número 75. Esto significa que el router local debe mantener un porcentaje mínimo de error de 75 o el enlace PPP se cerrará.
- OutLQRs = 1: actual número de secuencia del envío LQR del router local.
- LastOutLQRs = 1: último número de secuencia que el lado del nodo remoto ha visto desde el nodo local.

Resultado del comando debug ppp error

```
R1# debug ppp error
PPP Serial3(i): rlqr receive failure. successes = 15
PPP: myrcvdiffp = 159 peerxmitdiffp = 41091
PPP: myrcvdiffo = 2183 peerxmitdiffo = 1714439
PPP: threshold = 25
PPP Serial2(i): rlqr transmit failure. successes = 15
PPP: myxmitdiffp = 41091 peerrcvdiffp = 159
PPP: myxmitdiffo = 1714439 peerrcvdiffo = 2183
PPP: 1->OutLQRs = 1 LastOutLQRs = 1
PPP: threshold = 25
PPP Serial3(i): lqr_protrej() Stop sending LQRs.
PPP Serial3(i): The link appears to be looped back.
```

Resultado del router

En esta actividad, podrá practicar el cambio de encapsulación en las interfaces seriales. Las instrucciones detalladas están proporcionadas dentro de la actividad, al igual que en el enlace al PDF a continuación.
Instrucciones de la actividad (PDF)

2.4 Configuración de PPP con autenticación

2.4.1 Protocolos de autenticación PPP

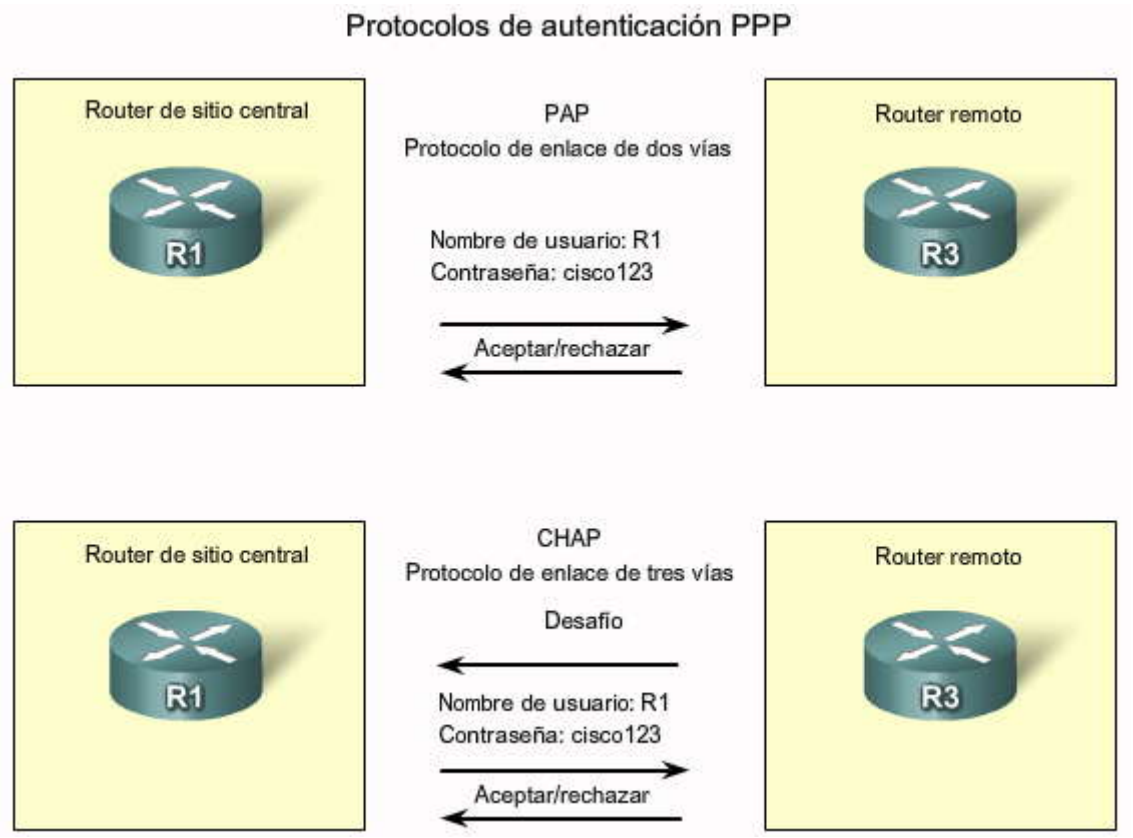
Protocolo de autenticación PAP

PPP define un LCP extensible que permite la negociación de un protocolo de autenticación para autenticar su peer antes de permitir que los protocolos de capa de red transmitan a través del enlace. RFC 1334 define dos protocolos para autenticación, tal como se muestra en la imagen.

PAP es un proceso muy básico de dos vías. No hay encriptación: el nombre de usuario y la contraseña se envían en texto sin cifrar. Si esto se acepta, la conexión se permite. CHAP es más seguro que PAP. Implica un intercambio de tres vías de un secreto compartido. Más adelante, en este mismo capítulo, se describirá este proceso.

La fase de autenticación de una sesión PPP es opcional. Si se usa, se puede autenticar el peer, luego de que el LCP establezca el enlace y elija el protocolo de autenticación. Si se utiliza, la autenticación se lleva a cabo antes de que comience la fase de configuración del protocolo de la capa de red.

Las opciones de autenticación requieren que la parte del enlace que realiza la llamada introduzca la información de autenticación. Esto ayuda a garantizar que el usuario tenga el permiso del administrador de la red para efectuar la llamada. Los routers pares intercambian mensajes de autenticación.



2.4.2 Protocolo de autenticación de contraseña (PAP)

Una de las muchas funciones del PPP es que ejecuta la autenticación en Capa 2 además de otras capas de autenticación, encriptación, control de acceso y procedimientos de seguridad generales.

Iniciando PAP

PAP ofrece un método sencillo para que un nodo remoto establezca su identidad por medio del protocolo de enlace de dos vías. PAP no es interactivo. Cuando se utiliza el comando **ppp authentication pap**, el nombre de usuario y la contraseña se envían como un paquete de datos LCP, en lugar de que el servidor envíe un aviso de inicio de sesión y espere una respuesta. La imagen muestra que luego de que PPP completa la fase de establecimiento de enlace, el nodo remoto envía repetidamente un par nombre de usuario-contraseña a través del enlace hasta que el nodo que envía lo reconoce o finaliza la conexión.

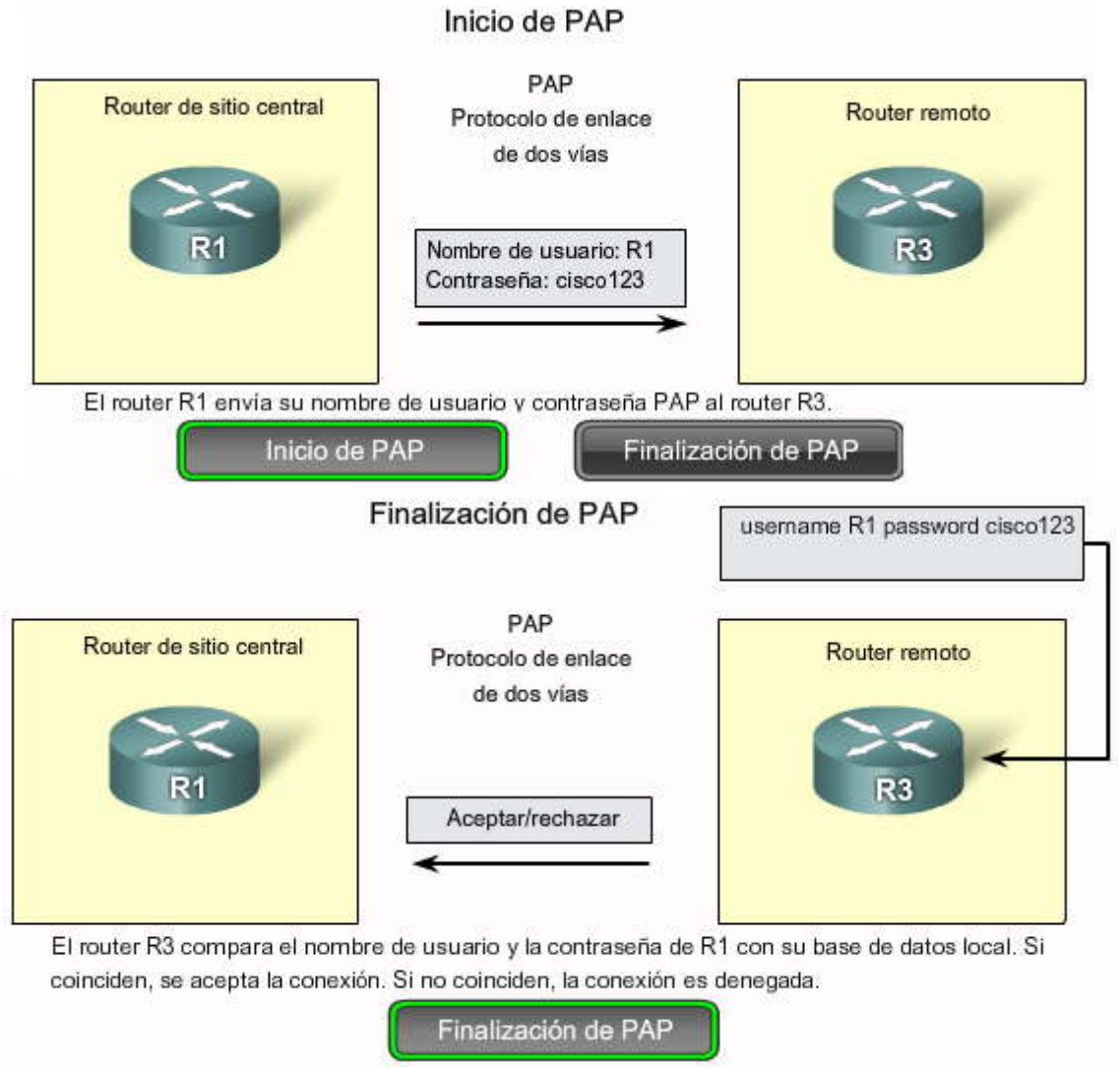
Haga clic en el botón Finalización de PAP en la imagen.

En el nodo receptor, un servidor de autenticación, que permite o deniega la conexión, controla el nombre de usuario-contraseña. Se reenvía al solicitante un mensaje de aceptación o rechazo.

PAP no es un protocolo de autenticación sólido. Al utilizar PAP, las contraseñas se envían por el enlace en texto no cifrado, y no hay protección contra la reproducción o los intentos de descubrimiento mediante intentos reiterados de ensayo y error. El nodo remoto tiene control de la frecuencia y la temporización de los intentos de conexión.

Sin embargo, hay veces que el uso de PAP se puede justificar. Por ejemplo, a pesar de sus limitaciones, PAP se puede usar en los siguientes entornos:

- Una gran base instalada de aplicaciones de cliente que no soportan CHAP
- Incompatibilidades entre diferentes implementaciones de proveedores de CHAP
- Situaciones en las que una contraseña de texto simple debe estar disponible para simular un inicio de sesión en el host remoto



2.4.3 Protocolo de autenticación de intercambio de señales (CHAP)

Protocolo de autenticación de intercambio de señales (CHAP)
Una vez que se establece la autenticación con PAP, esencialmente deja de funcionar. Esto deja la red vulnerable para los ataques. A diferencia de PAP, que sólo autentica una vez, CHAP realiza comprobaciones periódicas para asegurarse de que el nodo remoto todavía posee un valor de contraseña válido. El valor de la contraseña es variable y cambia impredeciblemente mientras el enlace existe.

Después de completar la fase de establecimiento del enlace PPP, el router local envía un mensaje de comprobación al nodo remoto.

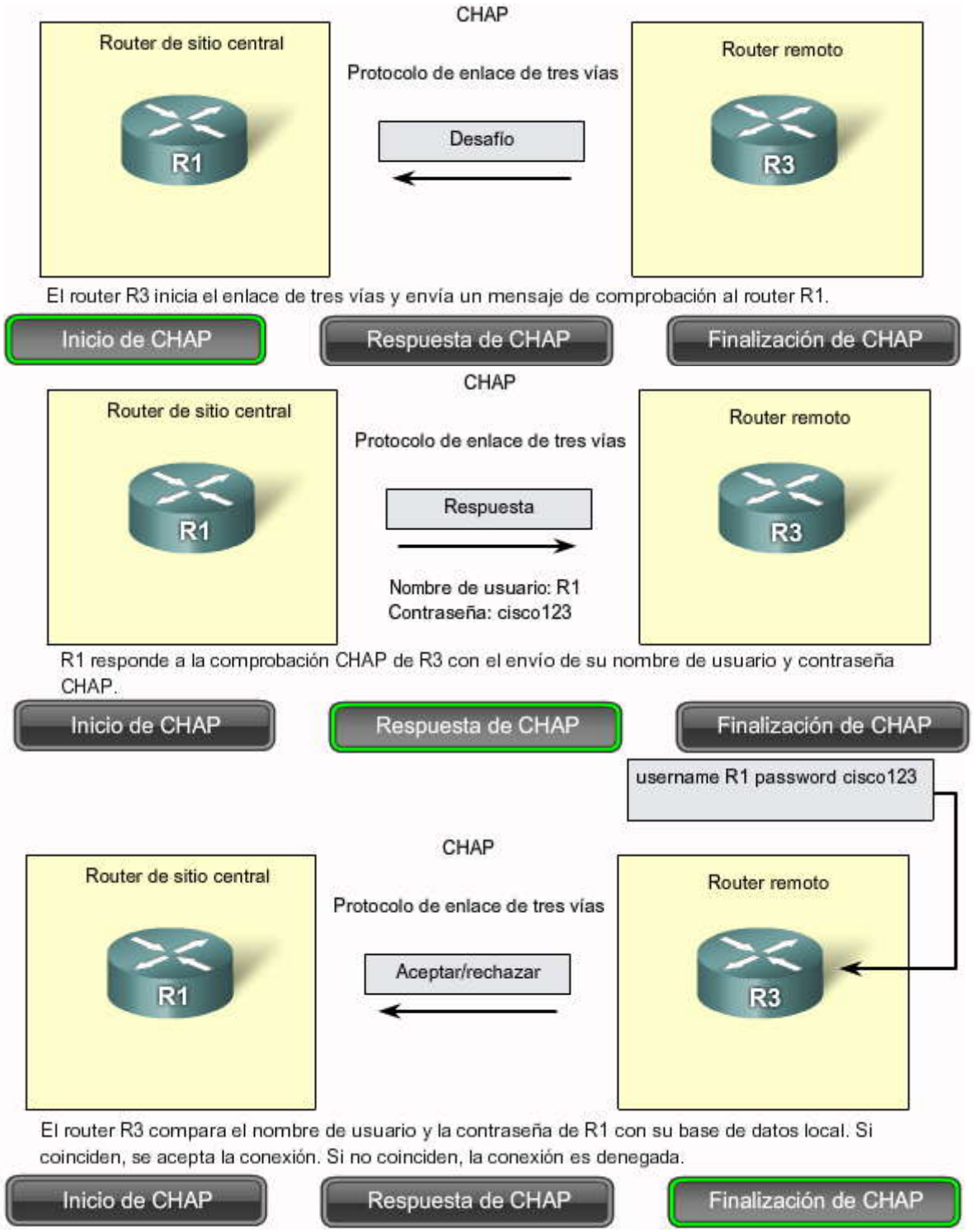
Haga clic en el botón Respuesta de CHAP que se muestra en la imagen.

El nodo remoto responde con un valor que se calcula con una función hash de una vía, la cual es generalmente Message Digest 5 (MD5) basada en la contraseña y el mensaje de comprobación.

Haga clic en el botón Finalización de CHAP en la imagen.

El router local verifica la respuesta y la compara con su propio cálculo del valor hash esperado. Si los valores concuerdan, el nodo de inicio acusa recibo de la autenticación. En caso contrario, el nodo de inicio termina la conexión inmediatamente.

El CHAP brinda protección contra los intentos de reproducción a través del uso de un valor de comprobación variable que es exclusivo e impredecible. Como la comprobación es única y aleatoria, el valor hash resultante también es único y aleatorio. El uso de comprobaciones reiteradas limita el tiempo de exposición ante cualquier ataque. El router local o un servidor de autenticación de terceros tiene el control de la frecuencia y la temporización de las comprobaciones.



2.4.4 Encapsulación y proceso de autenticación del PPP

Encapsulación y proceso de autenticación del PPP

Puede utilizar un diagrama de flujo para entender el proceso de autenticación PPP al configurar PPP. El diagrama de flujo brinda un ejemplo visual de las decisiones lógicas realizadas por PPP.

Por ejemplo, si una solicitud entrante de PPP no requiere autenticación, entonces PPP avanza al siguiente nivel. Si una solicitud entrante de PPP requiere autenticación, puede ser autenticada mediante el uso de la base de datos local o un servidor de seguridad. Como se muestra en el diagrama de flujo, una autenticación satisfactoria avanza hacia el próximo nivel, mientras que una autenticación fallida desconectará y descartará la solicitud entrante de PPP.

Haga clic en el botón Ejemplo de CHAP y luego en el botón Reproducir para ver un ejemplo animado.

Siga los pasos a medida que la animación avanza. El router R1 desea establecer una conexión autenticada PPP CHAP con el router R2.

Paso 1. En un principio, el R1 negocia la conexión del enlace mediante el uso de LCP con el router R2 y los dos sistemas acuerdan utilizar autenticación CHAP durante la negociación LCP de PPP.

Paso 2. El router R2 genera una identificación y un número aleatorio y los envía a R1, junto con el nombre de usuario, como un paquete de desafío CHAP.

Paso 3. R1 utilizará el nombre de usuario del desafiante (R2) y lo compara con la base de datos local para encontrar una contraseña asociada. Luego, el R1 genera un único número hash MD5 mediante el uso del nombre de usuario, la identificación, el número aleatorio y la contraseña secreta compartida de R2.

Paso 4. Luego, el router R1 envía a R2 la ID del desafío, el valor hash y el nombre de usuario (R1).

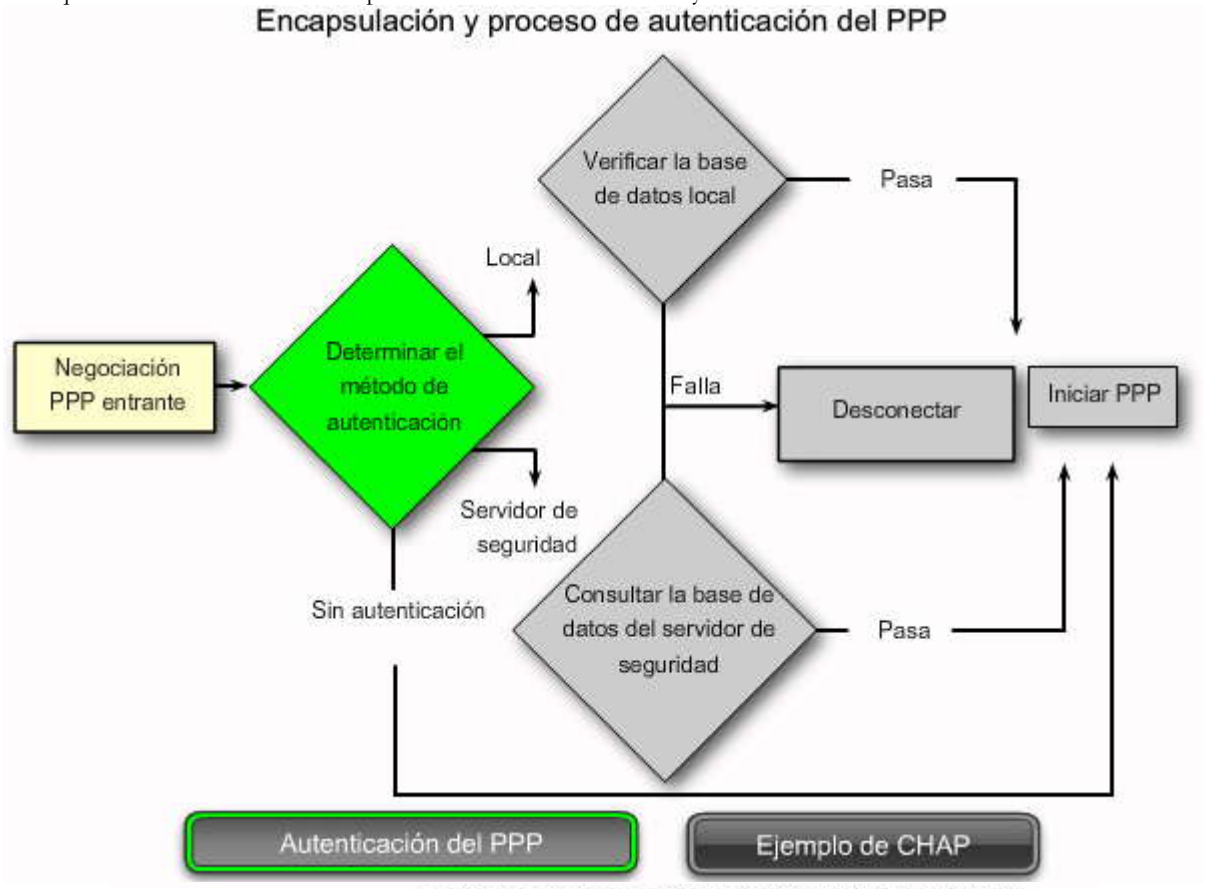
Paso 5. R2 genera su propio valor hash con la identificación, la contraseña secreta compartida y el número aleatorio que originalmente envió a R1.

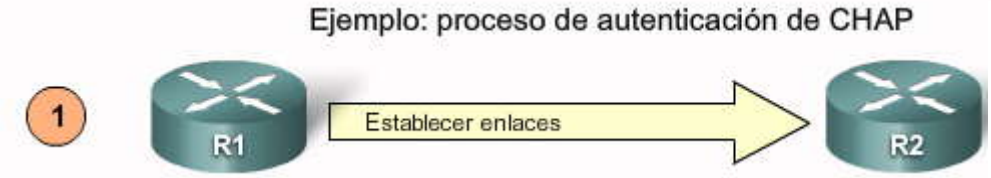
Paso 6. R2 compara su valor hash con el valor hash enviado por R1. Si los valores son iguales, R2 envía a R1 una respuesta de enlace establecido.

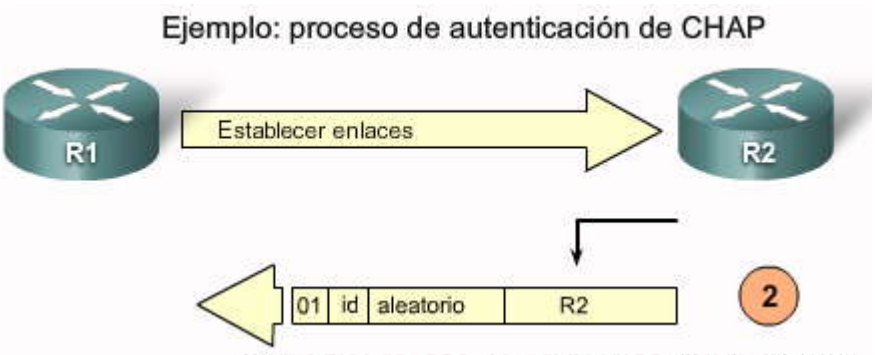
Si falla la autenticación, se construye un paquete de falla CHAP a partir de los siguientes componentes:

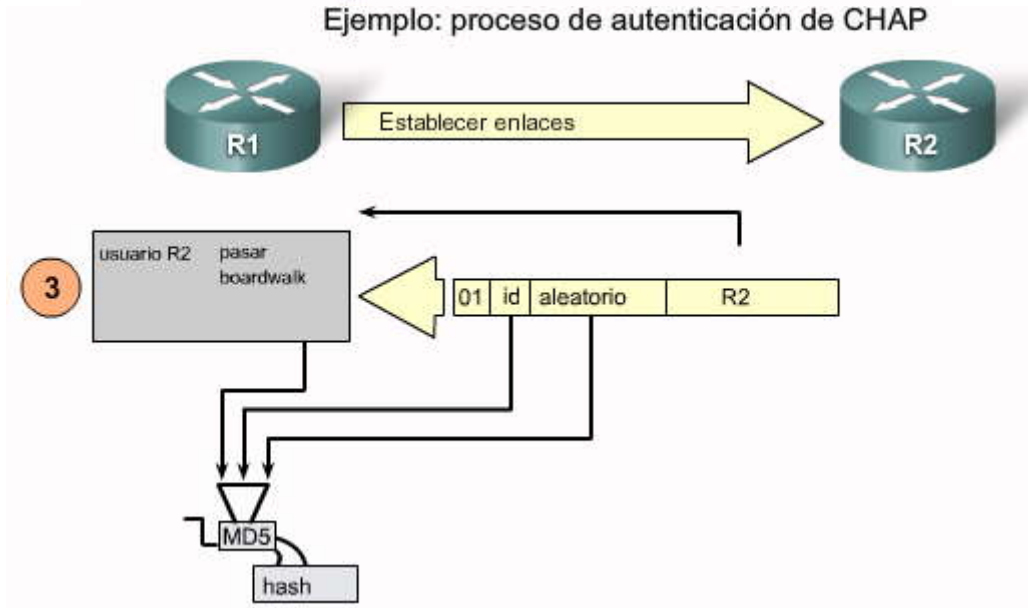
- 04 = tipo de mensaje de falla CHAP
- id = copiado del paquete de respuesta
- "Falla de autenticación" o algún mensaje de texto parecido, que sirve de explicación legible para el usuario

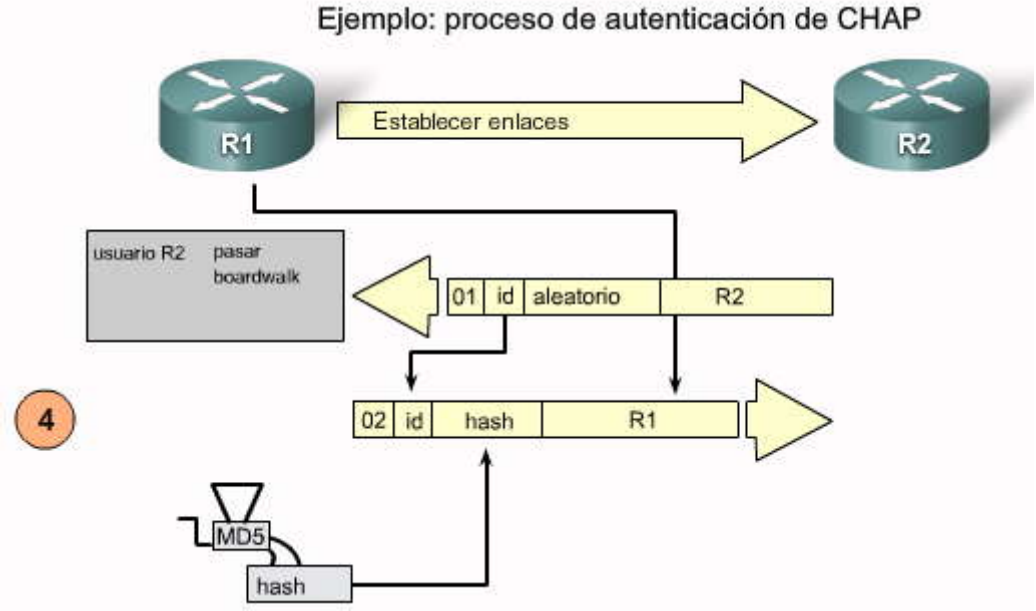
Observe que la contraseña secreta compartida debe ser idéntica en R1 y R2.

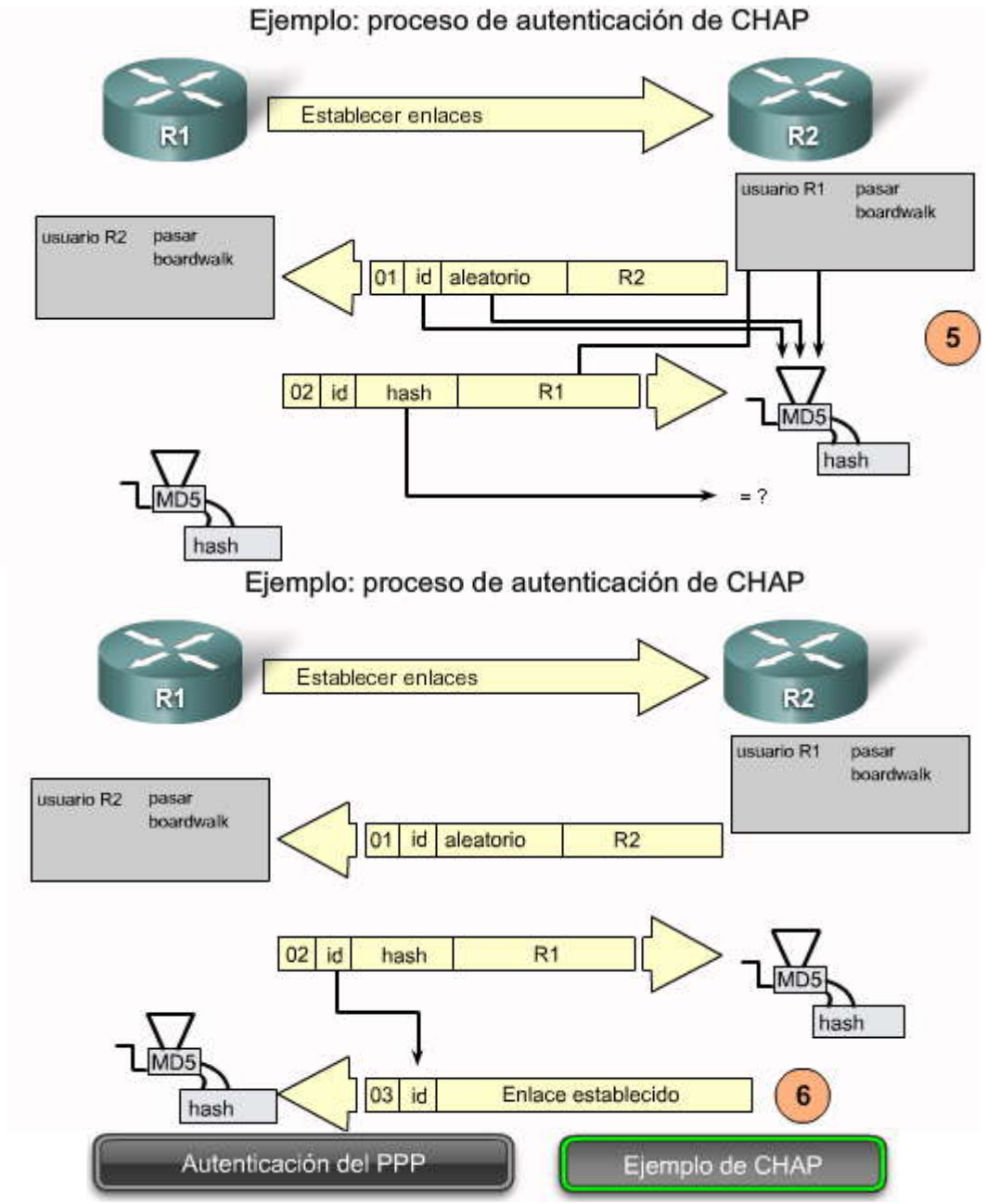





Ejemplo: proceso de autenticación de CHAP
R1
Establecer enlaces
R2
01
id
aleatorio
R2
2


Ejemplo: proceso de autenticación de CHAP
R1
Establecer enlaces
R2
usuario R2
pasar
boardwalk
3
01
id
aleatorio
R2
MD5
hash


Ejemplo: proceso de autenticación de CHAP
R1
Establecer enlaces
R2
usuario R2
pasar
boardwalk
01
id
aleatorio
R2
4
02
id
hash
R1
MD5
hash



2.4.5 Configuración de PPP con autenticación

El comando ppp authentication

Para especificar el orden en que se requieren los protocolos CHAP o PAP en la interfaz, utilice el comando de configuración de interfaz **ppp authentication**, como se muestra en la imagen. Use la forma **no** del comando para inhabilitar esta autenticación.

Luego de habilitar la autenticación CHAP o PAP, o ambas, el router local requiere que el dispositivo remoto compruebe su identidad antes de permitir que el tráfico de datos fluya. Esto se hace de la siguiente manera:

- La autenticación PAP requiere que el dispositivo remoto envíe un nombre y una contraseña para controlar si hay coincidencias de entradas en la base de datos de nombres de usuario local o en la base de datos remota TACACS/TACACS+.
- La autenticación CHAP envía una comprobación al dispositivo remoto. El dispositivo remoto debe encriptar el valor de la comprobación con un secreto compartido y devolver el valor encriptado y su nombre al router local mediante un mensaje de respuesta. El router local utiliza el nombre del dispositivo remoto para buscar el secreto correspondiente en la base de datos de nombres de usuario local o la base de datos remota TACACS/TACACS+. Utiliza el secreto buscado para encriptar la comprobación original y verificar que los valores encriptados coincidan.

Nota: AAA/TACACS es un servidor dedicado que se utiliza para autenticar usuarios. AAA significa "autenticación, autorización y contabilidad". Los clientes TACACS envían una consulta a un servidor de autenticación TACACS. El servidor puede autenticar al usuario, autorizar lo que el usuario puede realizar y registrar lo que el usuario ha hecho.

Usted puede habilitar PAP, CHAP o ambos. Si se habilitan ambos métodos, el primer método especificado se solicita durante la negociación del enlace. Si el peer sugiere el uso del segundo método o simplemente rechaza el primero, entonces se prueba el segundo método. Algunos dispositivos remotos soportan sólo CHAP y algunos sólo PAP. El orden en el cual usted especifica los métodos se basa en su inquietud acerca de la habilidad de los dispositivos remotos para negociar correctamente el método apropiado, así como también en su inquietud respecto a la seguridad de la línea de datos. Los nombres de usuarios y las contraseñas PAP se envían en cadenas de texto sin cifrar y pueden ser interceptados y reutilizados. CHAP ha eliminado la mayoría de los agujeros de seguridad conocidos.

El comando **ppp authentication**

```
ppp authentication {chap | chap pap | pap chap | pap} [if-needed]
[list-name | default] [callin]
```

El comando ppp authentication	
chap	Habilita CHAP en una interfaz serial.
pap	Habilita PAP en una interfaz serial.
chap pap	Habilita CHAP y PAP y realiza la autenticación de CHAP antes que la de PAP.
pap chap	Habilita CHAP y PAP y realiza la autenticación de PAP antes que la de CHAP.
`if-needed` (opcional)	Usado con TACACS y XTACACS. No realice la autenticación CHAP o PAP si el usuario ya ha proporcionado la autenticación. Esta opción está disponible sólo en interfaces asíncronas.
`list-name` (opcional)	Usado con AAA/TACACS+. Especifica el nombre de una lista de métodos TACACS+ de nombre de lista auténtico, el sistema utiliza la opción predeterminada. Las listas se crean con el comando aaa **`authentication ppp`**.
default (opcional)	Usado con AAA/TACACS+. Creado con el comando **`aaa authentication ppp`**.
`callin`	Especifica la autenticación sólo en las llamadas entrantes (recibidas).

Configuración de la autenticación de PPP
El procedimiento que se describe en la tabla detalla la configuración de la encapsulación PPP y los protocolos de autenticación PAP/CHAP. Es esencial realizar una configuración correcta, ya que PAP y CHAP utilizarán estos parámetros para la autenticación.

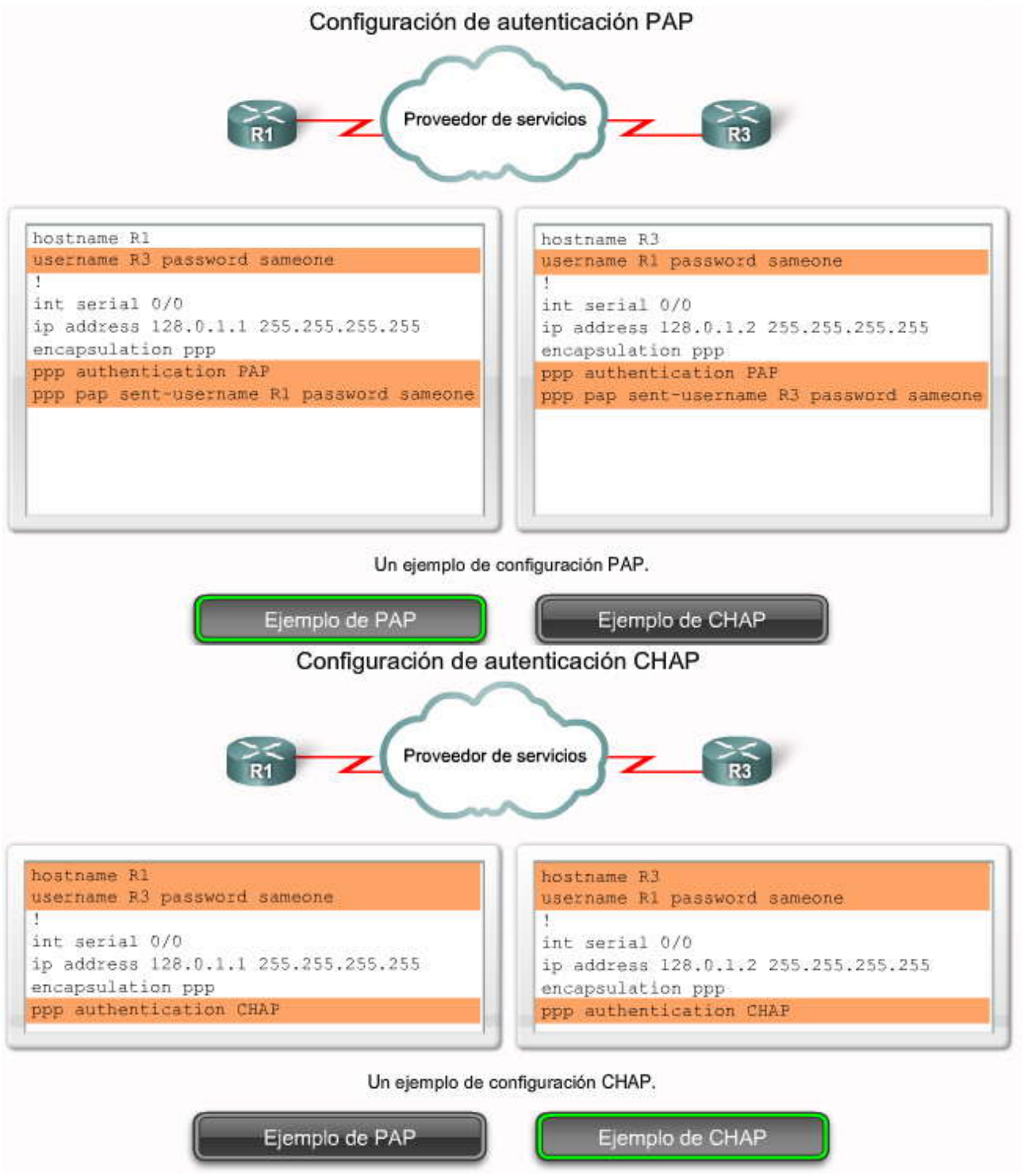
Haga clic en el botón Ejemplo de PAP que se muestra en la imagen.

La imagen presenta un ejemplo de una configuración de autenticación PAP de dos vías. Ambos routers autentican y son autenticados de modo que los comandos de autenticación PAP se reflejan entre sí. El nombre de usuario y la contraseña PAP que cada router envía debe coincidir con aquellos especificados en el comando **username** *name* **password** *password* del otro router.

PAP ofrece un método sencillo para que un nodo remoto establezca su identidad, mediante el protocolo de enlace de dos vías. Esto se realiza sólo en el momento del establecimiento inicial del enlace. El nombre de host de un router debe coincidir con el nombre de usuario que el otro router ha configurado. Las contraseñas también deben coincidir.

Haga clic en el botón Ejemplo de CHAP que se muestra en la imagen.

CHAP verifica periódicamente la identidad del nodo remoto por medio de un protocolo de enlace de tres vías. El nombre de host de un router debe coincidir con el nombre de usuario que el otro router ha configurado. Las contraseñas también deben coincidir. Esto ocurre durante el establecimiento inicial del enlace y se puede repetir en cualquier momento, una vez establecido el enlace. La imagen es un ejemplo de una configuración CHAP.



2.4.6 Resolución de problemas de una configuración PPP con autenticación

Resolución de problemas de una configuración PPP con autenticación
La autenticación es una función que requiere ser implementada correctamente para no comprometer la seguridad de su conexión serial. Siempre verifique su configuración con el comando **show interfaces serial** de la misma manera que lo hizo sin autenticación.

Nunca suponga que su configuración de autenticación funciona sin haberla probado. La depuración permite confirmar su configuración y corregir cualquier deficiencia. El comando que se utiliza para depurar la autenticación de PPP es **debug ppp authentication**.

La imagen muestra un resultado del ejemplo del comando **debug ppp authentication**. A continuación, se presenta una interpretación del resultado:

La línea 1 dice que el router no puede autenticar la interfaz Serial0 debido a que el peer no envió un nombre.

La línea 2 dice que el router no pudo validar la respuesta CHAP porque el NOMBRE DE USUARIO "pioneer" no se encontró.

La línea 3 dice que no se encontró ninguna contraseña para "pioneer". Las otras posibles respuestas en esta línea podrían haber sido: ningún nombre recibido para autenticar, nombre desconocido, sin secreto para el nombre dado, respuesta breve MD5 recibida o error de comparación MD5.

En la última línea, el código = 4 significa que ocurrió una falla. Los siguientes son otros valores de código:

- 1 = Comprobación
- 2 = Respuesta
- 3 = Éxito
- 4 = Error

id = 3 es el número de identificación por formato de paquete LCP.

len = 48 es la longitud de paquete sin el encabezado.

Resolución de problemas de una configuración PPP con autenticación

```
R2# debug ppp authentication

Serial0: Unable to authenticate. No name received from peer
Serial0: Unable to validate CHAP response. USERNAME pioneer not found.
Serial0: Unable to validate CHAP response. No password defined for USERNAME pioneer
Serial0: Failed CHAP authentication with remote.
Remote message is Unknown name
Serial0: remote passed CHAP authentication.
Serial0: Passed CHAP authentication with remote.
Serial0: CHAP input code = 4 id = 3 len = 48
```

La encapsulación PPP permite dos tipos diferentes de autenticación: PAP (protocolo de autenticación de contraseña) y CHAP (protocolo de autenticación de intercambio de señales). PAP utiliza una contraseña de texto sin cifrar, mientras que CHAP solicita un hash de una vía que provee más seguridad que PAP. En esta actividad, realizará la configuración de PAP y CHAP, así como también revisará la configuración de enrutamiento OSPF. Las instrucciones detalladas se proporcionan dentro de la actividad, al igual que en el enlace al PDF a continuación.
Instrucciones de la actividad (PDF)

CAPITULO III – "FRAME RELAY"

3 Frame Relay
3.0 Introducción
3.0.1 Introducción
Frame Relay es un protocolo WAN de alto rendimiento que funciona en las capas físicas y de enlace de datos del modelo de referencia OSI.

Eric Scace, ingeniero de Sprint International, inventó Frame Relay como una versión más simple del protocolo X.25, para usar en las interfaces de la red digital de servicios integrados (ISDN). Hoy, se usa a través de una variedad de otras interfaces de redes. Cuando Sprint implementó por primera vez Frame Relay en su red pública, usaron switches StrataCom. La adquisición de Cisco de StrataCom en 1996 marcó su entrada al mercado de las empresas de comunicaciones.

Los proveedores de red comúnmente implementan Frame Relay para voz y datos, comotécnica de encapsulación, utilizada entre redes de área local a través de una red de área extensa (WAN, Wide Area Network). Cada usuario final obtiene una línea privada (o línea arrendada) a un nodo Frame Relay. La red Frame Relay administra la transmisión a través de una ruta cambiante transparente para todos los usuarios finales.

Frame Relay se ha convertido en uno de los protocolos WAN más utilizados, principalmente ya que es económico en comparación con las líneas dedicadas. Además, la configuración del equipo del usuario en una red Frame Relay es muy simple. Las conexiones Frame Relay se crean al configurar routers CPE u otros dispositivos para comunicarse con un switch Frame Relay del proveedor de servicios. El proveedor de servicio configura el switch Frame Relay, que ayuda a mantener las tareas de configuración del usuario final a un nivel mínimo.

En este capítulo, se describe Frame Relay y se explica cómo configurarlo en un router Cisco.

En este capítulo, aprenderá a:

- Describir los conceptos fundamentales de la tecnología Frame Relay en relación con los servicios WAN empresariales, incluida la operación, los requisitos de implementación, asignación y operación de la interfaz de administración local (LMI, Local Management Interface).
- Configurar un circuito virtual permanente (PVC, permanent virtual circuit) básico de Frame Relay, incluida la configuración y la resolución de problemas de Frame Relay en una interfaz serial de router y la configuración de una asignación de Frame Relay estática.
- Describir los conceptos avanzados de la tecnología Frame Relay en relación con los servicios WAN empresariales, incluidas las subinterfaces, el ancho de banda y el control de flujo.
- Configurar un PVC de Frame Relay avanzado, incluida la resolución de problemas relacionados a la posibilidad de conexión, la configuración de subinterfaces, y la verificación y la resolución de problemas de una configuración de Frame Relay.

3.1 Conceptos básicos de Frame Relay
3.1.1 Introducción a la tecnología Frame Relay

Frame Relay: Una tecnología WAN eficaz y flexible

Frame Relay se ha convertido en la tecnología WAN más utilizada del mundo. Grandes empresas, gobiernos, ISP y pequeñas empresas usan Frame Relay, principalmente a causa de su precio y flexibilidad. A medida que las organizaciones crecen y dependen cada vez más de un transporte de datos fiable, las soluciones de líneas arrendadas tradicionales se vuelven imposibles de costear. El ritmo de los cambios tecnológicos y las fusiones yadquisiciones en la industria de networking demandan y exigen más flexibilidad.

Frame Relay reduce los costos de redes a través del uso de menos equipo, menos complejidad y una implementación más fácil. Aún más, Frame Relay proporciona un mayor ancho de banda, mejor fiabilidad y resistencia a fallas que las líneas privadas o arrendadas. Debido a una mayor globalización y al crecimiento de excesivas topologías de sucursales, Frame Relay ofrece una arquitectura de red más simple y un menor costo de propiedad.

El uso de un ejemplo de una red empresarial grande contribuye a ilustrar los beneficios del uso de una WAN Frame Relay. En el ejemplo que se muestra en la figura, Span Engineering tiene cinco campus en América del Norte. Al igual que la mayoría de las organizaciones, los requisitos de ancho de banda de Span no se adecuan a una solución "talle único".

Lo primero que se debe considerar es el requisito de ancho de banda de cada sitio. Dado que se trabaja desde las sedes, la conexión de Chicago a Nueva York requiere una velocidad máxima de 256 Kbps. Otros tres sitios necesitan una velocidad máxima de 48 kbps para conectarse con las sedes, mientras que la conexión entre las sucursales de Nueva York y Dallas requiere sólo 12 kbps.

Antes de que Frame Relay estuviera disponible, Span arrendó líneas dedicadas.

Haga clic en el botón Líneas dedicadas que se muestra en la figura.

A través del uso de líneas arrendadas, cada sitio de Span se conectaba a través de un switch ubicado en la oficina central de la empresa telefónica local, a través del bucle local y luego en toda la red. Los sitios de Chicago y Nueva York usan una línea T1 dedicada (equivalente a 24 canales DS0) para conectarse al switch, mientras que los otros sitios usan conexiones ISDN (56 kbps). Dado que el sitio de Dallas se conecta con Nueva York y Chicago, tiene dos líneas arrendadas localmente. Los proveedores de red han provisto a Span con un DS0 entre las oficinas centrales respectivas, excepto por el tubo más grande que conecta Chicago con Nueva York, que tiene cuatro DS0. Los DS0 tienen un precio diferente según la región y se ofrecen por lo general a un precio fijo. Estas líneas son verdaderamente dedicadas, el proveedor de red reserva esa línea para el uso exclusivo de Span. No hay uso compartido, y Span paga por el circuito de extremo a extremo, independientemente de la cantidad de ancho de banda que use.

Una línea dedicada proporciona pocas oportunidades prácticas para una conexión de más, sin que se necesiten más líneas del proveedor de red. En el ejemplo, prácticamente todas las comunicaciones deben fluir a través de las sedes corporativas, simplemente para reducir el costo que implican las líneas adicionales.

Si analiza los requisitos de casa sitio en relación con el ancho de banda, se observa una falta de eficacia:

- De los 24 canales DS0 disponibles en la conexión T1, el sitio de Chicago sólo usa siete. Algunas empresas de comunicaciones ofrecen conexiones T1 fraccionales en incrementos de 64 kbps, pero esto requiere un multiplexor especializado en el extremo del cliente para canalizar las señales. En este caso, Span ha optado por el servicio T1 completo.
- De igual forma, el sitio de Nueva York sólo usa cinco de sus 24 DS0 disponibles.
- Dado que Dallas necesita conectarse con Chicago y Nueva York, hay dos líneas que se conectan a través de la oficina central con cada sitio.

El diseño de líneas arrendadas también limita la flexibilidad. A menos que los circuitos ya estén instalados, la conexión con nuevos sitios generalmente requiere instalar nuevos circuitos y exige un tiempo considerable para la implementación. Desde la perspectiva de fiabilidad de la red, imagine los costos adicionales en dinero y complejidad que implica agregar circuitos de respaldo y redundantes.

Haga clic en el botón Frame Relay que se muestra en la figura.
La red Frame Relay de Span usa circuitos virtuales permanentes (PVC, Permanent Virtual Circuit). El PVC es la ruta lógica en un enlace Frame Relay de origen, a través de la red, y en un enlace Frame Relay de destino a su destino final. Compare esto con la ruta física utilizada por una conexión dedicada. En una red con acceso Frame Relay, el PVC define de forma exclusiva la ruta entre dos puntos finales. El concepto de circuitos virtuales se explica en más detalle más adelante en esta sección.

La solución Frame Relay de Span ofrece rentabilidad y flexibilidad.

Rentabilidad de Frame Relay

Frame Relay es una opción más rentable por dos motivos. En primer lugar, con líneas dedicadas, los clientes pagan por una conexión de extremo a extremo. Esto incluye el bucle local y el enlace de red. Con Frame Relay, los clientes sólo pagan por el bucle local y por el ancho de banda que compran al proveedor de red. La distancia entre los nodos no es importante. Mientras están en un modelo de líneas dedicadas, los clientes usan líneas dedicadas proporcionadas en incrementos de 64 kbps, los clientes Frame Relay pueden definir sus necesidades de circuitos virtuales con más granularidad, con frecuencia en incrementos pequeños como 4 kbps.

El segundo motivo de la rentabilidad de Frame Relay es que comparte el ancho de banda en una base más amplia de clientes. Comúnmente, un proveedor de red puede brindar servicio a 40 clientes o más de 56 kbps, en un circuito T1. El uso de líneas dedicadas requeriría más DSU/CSU (uno para cada línea), así como también enrutamiento y conmutación más complicados. Los proveedores de red ahorran dado que hay menos equipos para comprar y mantener.

La flexibilidad de Frame Relay

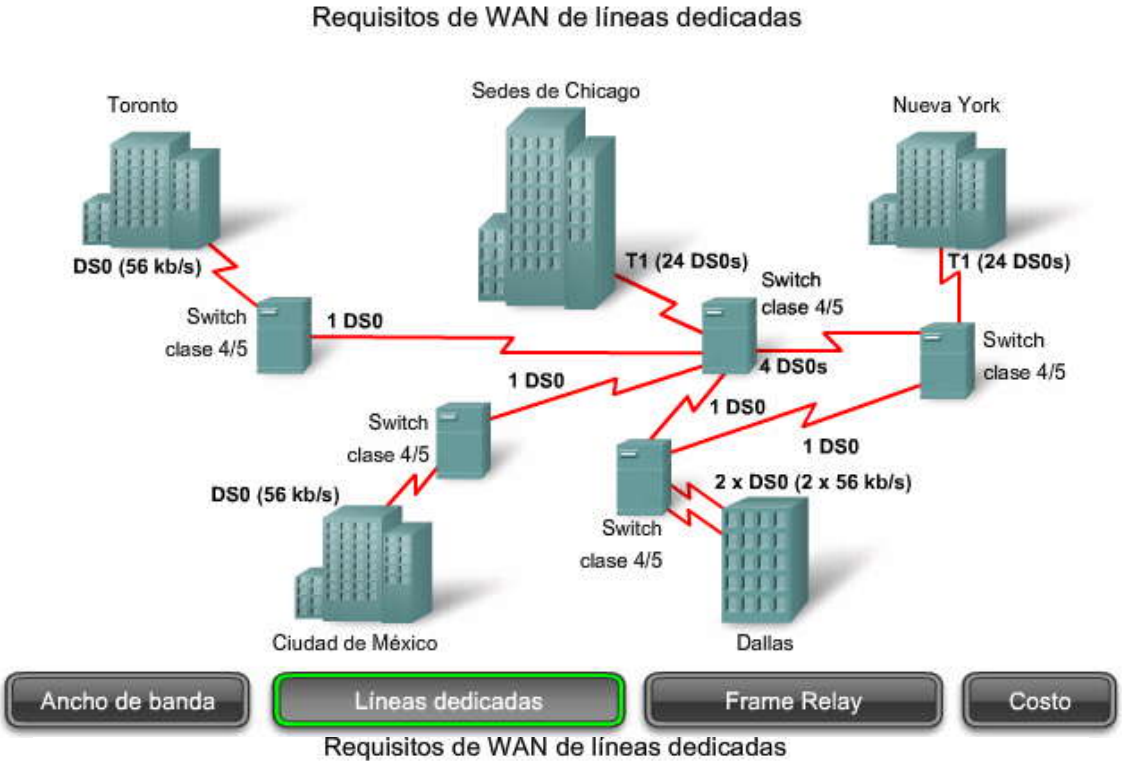
Un circuito virtual proporciona considerable flexibilidad en el diseño de red. Si observa la figura, puede ver que todas las oficinas de Span se conectan a la nube Frame Relay a través de sus respectivos bucles locales. Lo que sucede en la nube no debe preocuparle en este momento. Lo único que importa es que cuando una oficina de Span desea comunicarse con cualquier otra oficina de Span, no necesita más que conectarse a un circuito virtual que lleve a la otra oficina. En Frame Relay, el extremo de cada conexión tiene un número de identificación denominado identificador de conexión de enlace de datos (DLCI, Data Link Connection Identifier). Cualquier estación puede conectarse con otra simplemente si escribe la

dirección de esa estación y el número de DLCI de la línea que necesita usar. En una sección posterior, aprenderá que cuando se configura Frame Relay, todos los datos de todos los DLCI configurados fluyen a través del mismo puerto del router. Intente reflejar la misma flexibilidad usando líneas dedicadas. No sólo es complicado, sino que también requiere un número considerablemente mayor de equipos.

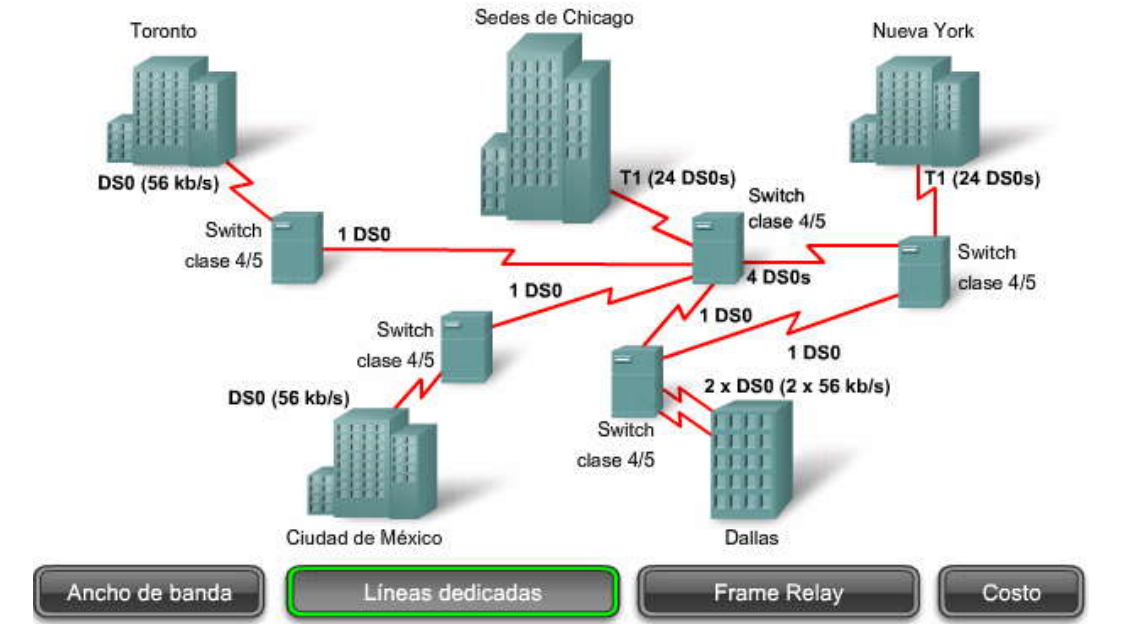
Haga clic en el botón Costo que se muestra en la figura.

La tabla muestra una comparación del costo representativa para conexiones ISDN y Frame Relay comparables. Si bien los costos iniciales en el caso de Frame Relay son más altos que para ISDN, el costo mensual es considerablemente más bajo. Frame Relay es más fácil de administrar y configurar que ISDN. Además, los clientes pueden incrementar su ancho de banda a medida que sus necesidades crezcan en el futuro. Los clientes de Frame Relay pagan sólo por el ancho de banda que necesitan. Con Frame Relay, no hay cargos por hora, si bien las llamadas ISDN se miden y pueden dar lugar a altos cargos mensuales no previstos de la empresa telefónica si se mantiene una conexión de tiempo completo.

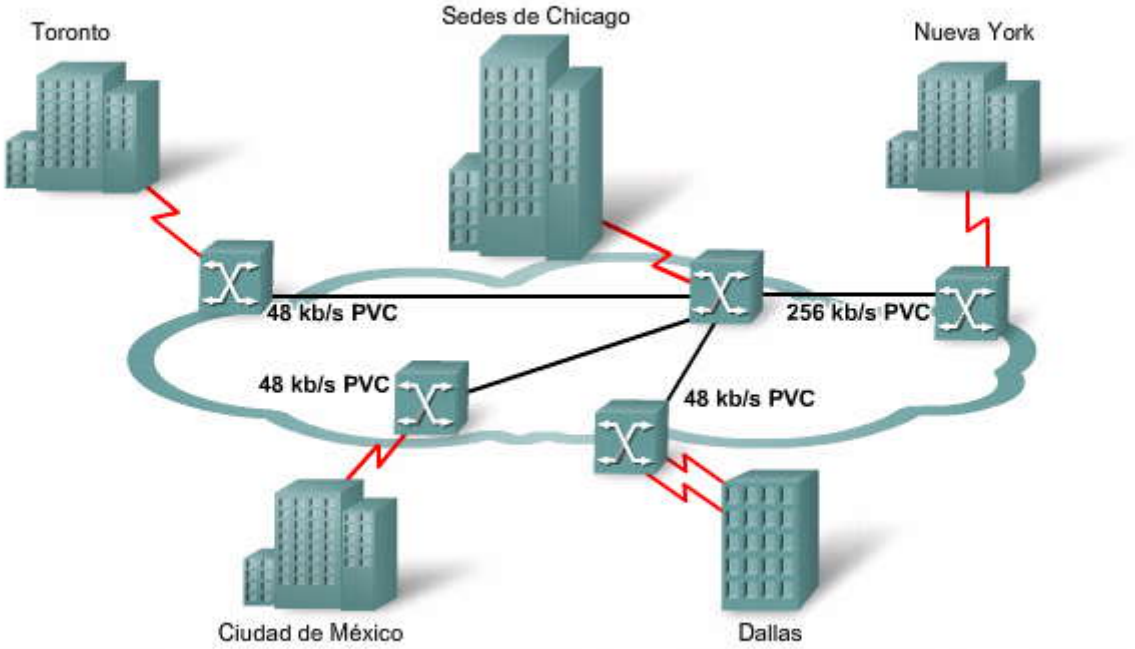
Los siguientes temas ampliarán su comprensión de Frame Relay a través de la definición de conceptos clave incorporados en el ejemplo.



Requisitos de WAN de líneas dedicadas



Requisitos de WAN de Frame Relay



Ancho de banda | Líneas dedicadas | Frame Relay | Costo

Costos de Frame Relay

	ISDN de 64 kbps	Frame Relay de 56 kbps
Cargo mensual por bucle local	**$185**	**$85**
Configuración de ISP	**$380**	**$750**
Equipo	**$700**	**$1600**
Cargo mensual de ISP	**$195**	**$195**
Cargos por única vez	**$1080**	**$2660**
Cargos mensuales	**$380**	**$280**

Equipo: Router ISDN $700*
Router Cisco $1600*

*Dólares estadounidenses

Ancho de banda | Líneas dedicadas | Frame Relay | Costo

WAN Frame Relay

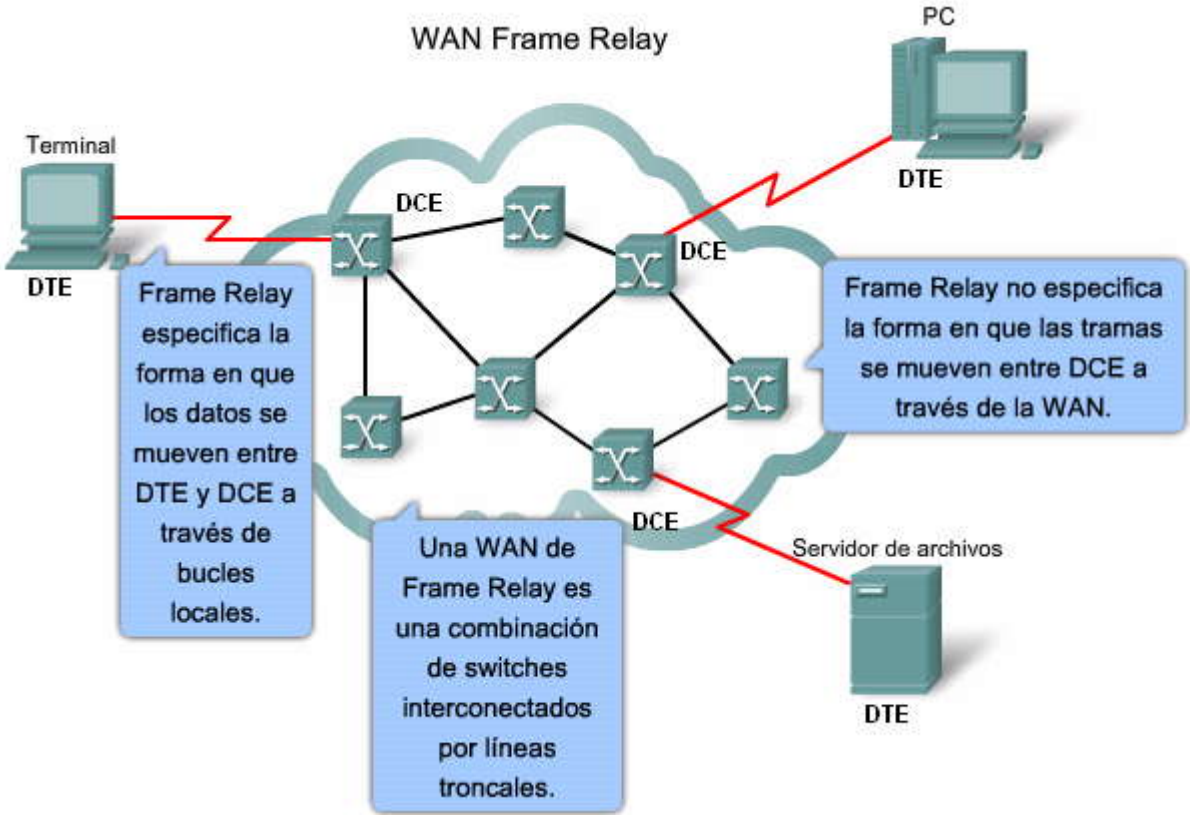
A finales de la década de 1970 y principios de la década de 1990, la tecnología WAN que unía los sitios finales usaba con frecuencia el protocolo X.25. Ahora considerado un protocolo heredado, el X.25 era una tecnología de conmutación de paquetes muy popular, dado que ofrecía una conexión muy fiable a través de infraestructuras de cableado no fiables. Lo hacía al incluir controles de errores y flujo adicionales. No obstante, estas funciones adicionales sumaban gastos fijos al protocolo. Su principal aplicación era el procesamiento de autorizaciones de tarjetas de crédito y para cajeros automáticos. Este curso menciona el X.25 sólo con fines históricos.

Cuando cree una WAN, independientemente del transporte que elija, siempre hay un mínimo de tres componentes básicos o grupos de componentes que se conectan en dos sitios. Cada sitio necesita su propio equipo (DTE) para acceder a la oficina central de la empresa telefónica que presta servicios al área (DCE). El tercer componente se encuentra en el medio, y une los dos puntos de acceso. En la figura, ésta es la parte proporcionada por el backbone de Frame Relay.

Frame Relay tiene menores gastos que X.25 dado que cuenta con menos capacidades. Por ejemplo, Frame Relay no ofrece corrección de errores, las instalaciones modernas WAN ofrecen servicios de conexión más confiables y un mayor grado de fiabilidad que otras instalaciones. El nodo Frame Relay simplemente suelta paquetes sin notificar cuando detecta errores. Cualquier corrección de errores necesaria, como la retransmisión de datos, se deja a los puntos finales. De esta forma, se agiliza la propagación de extremo a extremo del cliente a través de la red.

Frame Relay administra el volumen y la velocidad de manera eficaz mediante la combinación de las funciones necesarias de las capas de enlace de datos y de red en un simple protocolo. Como protocolo de enlace de datos, Frame Relay ofrece acceso a una red, delimita y entrega tramas en el orden adecuado y reconoce los errores de transmisión a través de una comprobación de redundancia cíclica estándar. Como protocolo de red, Frame Relay proporciona múltiples conexiones lógicas a través de un único circuito físico y permite que la red enrute datos a través de estas conexiones a sus destinos previstos.

Frame Relay funciona entre un dispositivo de usuario final, como un puente de LAN o router, y una red. La red en sí puede usar cualquier método de transmisión compatible con la velocidad y eficacia que requieren las aplicaciones de Frame Relay. Algunas redes usan Frame Relay en sí, pero otras usan la conmutación digital de circuitos o los sistemas de relay de celdas ATM. La figura muestra un backbone de conmutación de circuitos según se indica por los switches Clase 4/5. Los gráficos restantes de esta sección muestran backbones de conmutación de paquetes Frame Relay más actuales.

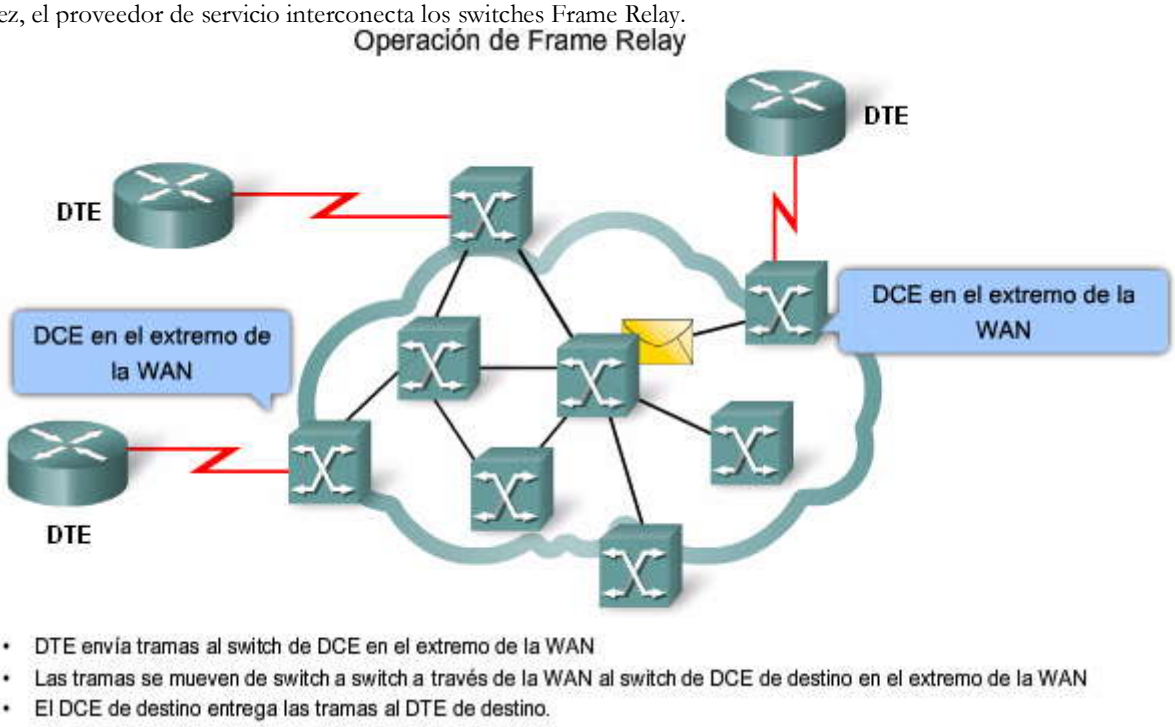


Funcionamiento de Frame Relay

La conexión entre un dispositivo DTE y un dispositivo DCE comprende un componente de capa física y un componente de capa de enlace:

- El componente físico define las especificaciones mecánicas, eléctricas, funcionales y de procedimiento necesarias para la conexión entre dispositivos. Una de las especificaciones de interfaz de capa física más comúnmente utilizadas es la especificación RS-232.
- El componente de capa de enlace define el protocolo que establece la conexión entre el dispositivos DTE, como un router, y el dispositivo DCE, como un switch.

Cuando las empresas de comunicaciones usan Frame Relay para interconectar las LAN, un router de cada LAN es el DTE. Una conexión serial, como una línea arrendada T1/E1, conecta el router al switch Frame Relay de la empresa de comunicaciones en el punto de presencia (POP) más cercano para la empresa. El switch Frame Relay es un dispositivo DCE. Los switches de red mueven tramas desde un DTE en la red y entregan tramas a otros DTE en forma de DCE. Otros equipos informáticos que no se encuentren en la LAN pueden también enviar datos a través de la red Frame Relay. Dichos equipos utilizan como DTE un dispositivo de acceso Frame Relay (FRAD). A menudo, FRAD hace referencia a un ensamblador/desensamblador de Frame Relay que es un artefacto dedicado o un router configurado para admitir Frame Relay. Se encuentra en las instalaciones del cliente y se conecta con el puerto del switch en la red del proveedor de servicio. A su vez, el proveedor de servicio interconecta los switches Frame Relay.



3.1.2 Circuitos virtuales

Circuitos virtuales

La conexión a través de una red Frame Relay entre dos DTE se denomina circuito virtual (VC, Virtual Circuit). Los circuitos son virtuales dado que no hay una conexión eléctrica directa de extremo a extremo. La conexión es lógica y los datos se mueven de extremo a extremo, sin circuito eléctrico directo. Con los VC, Frame Relay comparte el ancho de banda entre varios usuarios, y cualquier sitio puede comunicarse con otro sin usar varias líneas físicas dedicadas.

Hay dos formas de establecer VC:

- Los SVC, circuitos virtuales conmutados, se definen dinámicamente mediante el envío de mensajes de señalización a la red (CALL SETUP, DATA TRANSFER, IDLE, CALL TERMINATION).
- Los PVC, circuitos virtuales permanentes, son preconfigurados por la empresa de comunicaciones y, una vez configurados, sólo funcionan en los modos DATA TRANSFER e IDLE. Tenga en cuenta que algunas publicaciones hacen referencia a los PVC como VC privados.

Haga clic en el botón Reproducir que se muestra en la figura.

En la figura, hay un VC entre los nodos emisores y receptores. El VC sigue la ruta A, B, C y D. Frame Relay crea un circuito virtual al almacenar la asignación de puerto de entrada a puerto de salida en la memoria de cada switch y, por lo tanto, vincula un switch con otro hasta identificar una ruta continua de un extremo del circuito a otro. Un VC puede atravesar cualquier cantidad de dispositivos intermedios (switches) ubicados dentro de la red Frame Relay.

La pregunta que puede surgirle en este momento es: "¿Cómo se identificanlos diversos nodos y switches?".

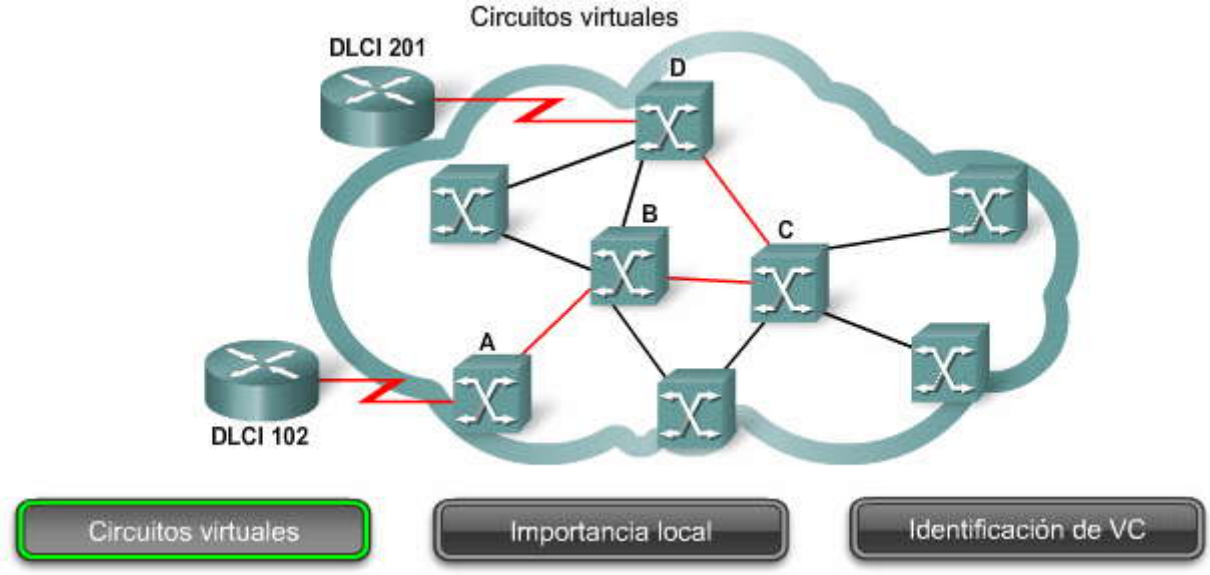
Haga clic en el botón Importancia local que se muestra en la figura.

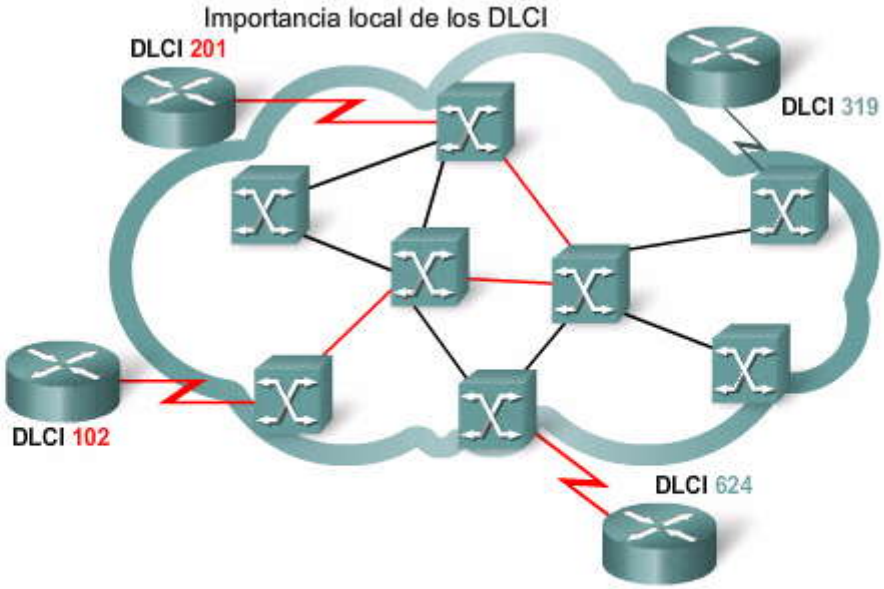
Los VC proporcionan una ruta de comunicación bidireccional de un dispositivo a otro. Los VC se identifican a través de DLCI. Los valores de DLCI comúnmente son asignados por el proveedor de servicios Frame Relay (por ejemplo, la compañía telefónica). Los DLCI Frame Relay tienen importancia local, es decir que los valores en sí no son únicos en la WAN Frame Relay. El DLCI identifica un VC al equipo en un punto final. El DLCI no tiene importancia más allá del enlace único. Dos dispositivos conectados por un VC pueden utilizar un valor DLCI distinto para referirse a la misma conexión.

Los DLCI con importancia local se han convertido en el principal método de direccionamiento, dado que se puede usar la misma dirección en diferentes ubicaciones al mismo tiempo que se hace referencia a distintas conexiones. El direccionamiento local evita que un cliente se quede sin DLCI a medida que la red crece.

Haga clic en el botón Identificación de VC y en el botón Reproducir que se muestran en la figura.
Ésta es la misma red que se presentó en la figura anterior pero, ahora, a medida que la trama se mueve por la red, Frame Relay etiqueta cada VC con un DLCI. El DLCI se almacena en el campo de dirección de cada trama transmitida, para indicar a la red cómo se debe enrutar la trama. El proveedor de servicios Frame Relay asigna los números de DLCI. Por lo general, los DLCI 0 a 15 y 1008 a 1023 se reservan para fines especiales. Por lo tanto, los proveedores de servicios generalmente asignan los DLCI comprendidos entre 16 y 1007.

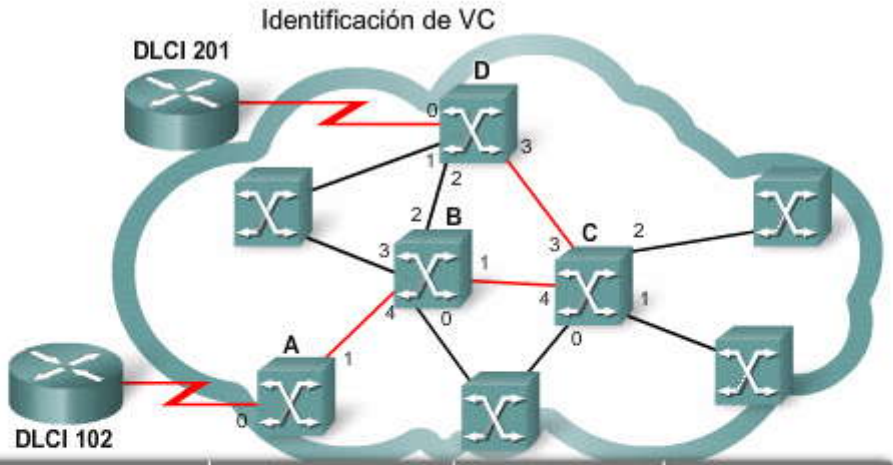
En este ejemplo, la trama usa DLCI 102. Sale del router (R1) usando el Puerto 0 y el VC 102. En el switch A, la trama sale del Puerto 1 mediante el VC 432. Este proceso de asignación de puertos de VC continúa a través de la WAN hasta que la trama alcanza su destino en DLCI 201, según se muestra en la figura. El DLCI se almacena en el campo de direcciones de cada trama transmitida.





Los valores de DLCI tienen importancia local, lo que significa que sólo son únicos para el canal físico en el que residen. Por lo tanto, los dispositivos de los extremos opuestos de una conexión pueden usar los mismos valores DLCI para referirse a diferentes circuitos virtuales.

Circuitos virtuales | Importancia local | Identificación de VC



Tramo	VC	Puerto	VC	Puerto
A	102	0	432	1
B	432	4	119	1
C	119	4	579	3
D	579	3	201	0

Circuitos virtuales | Importancia local | Identificación de VC

VC múltiples

Frame Relay se multiplexa estadísticamente, lo que significa que transmite sólo una trama por vez, pero que pueden coexistir muchas conexiones lógicas en una única línea física. El dispositivo de acceso Frame Relay (FRAD, Frame Relay Access Device) o el router conectado a la red Frame Relay puede tener varios VC que lo conectan a diversos puntos finales. Los VC múltiples de una única línea física se distinguen, dado que cada VC tiene su propio DLCI. Recuerde que el DLCI tiene sólo importancia local y puede ser diferente en cada extremo de un VC.

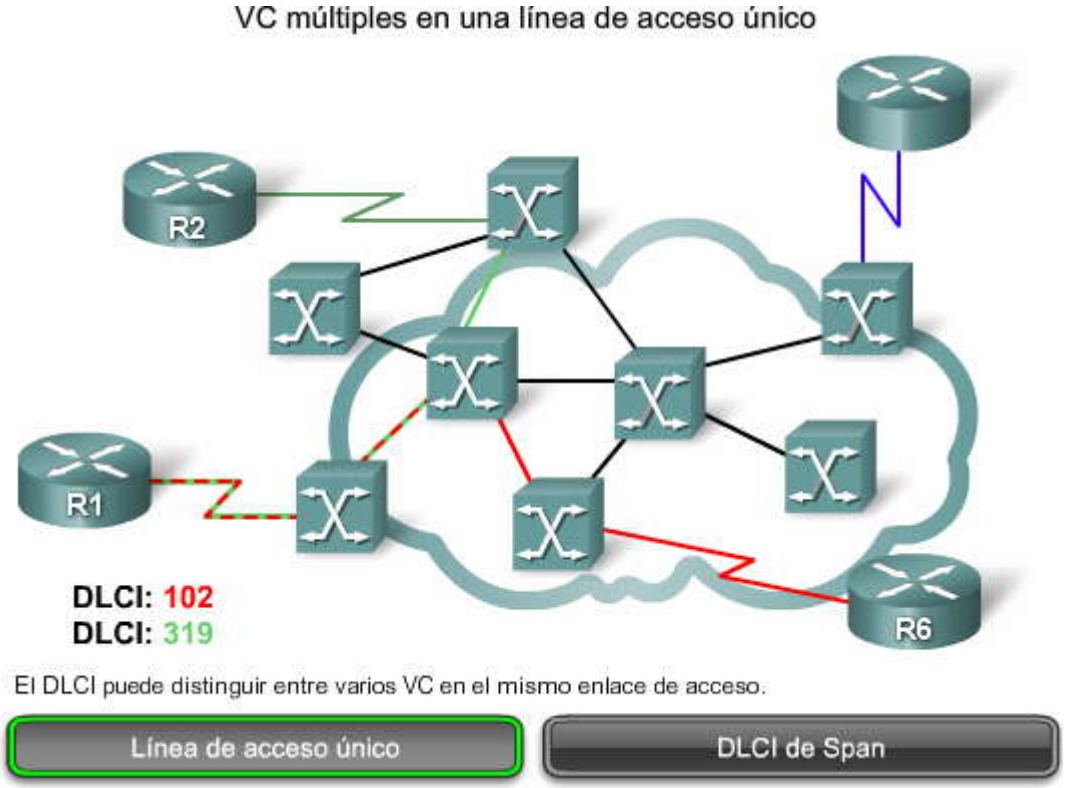
La figura muestra un ejemplo de dos VC en una única línea de acceso, cada uno con su propio DLCI, conectado a un router (R1).

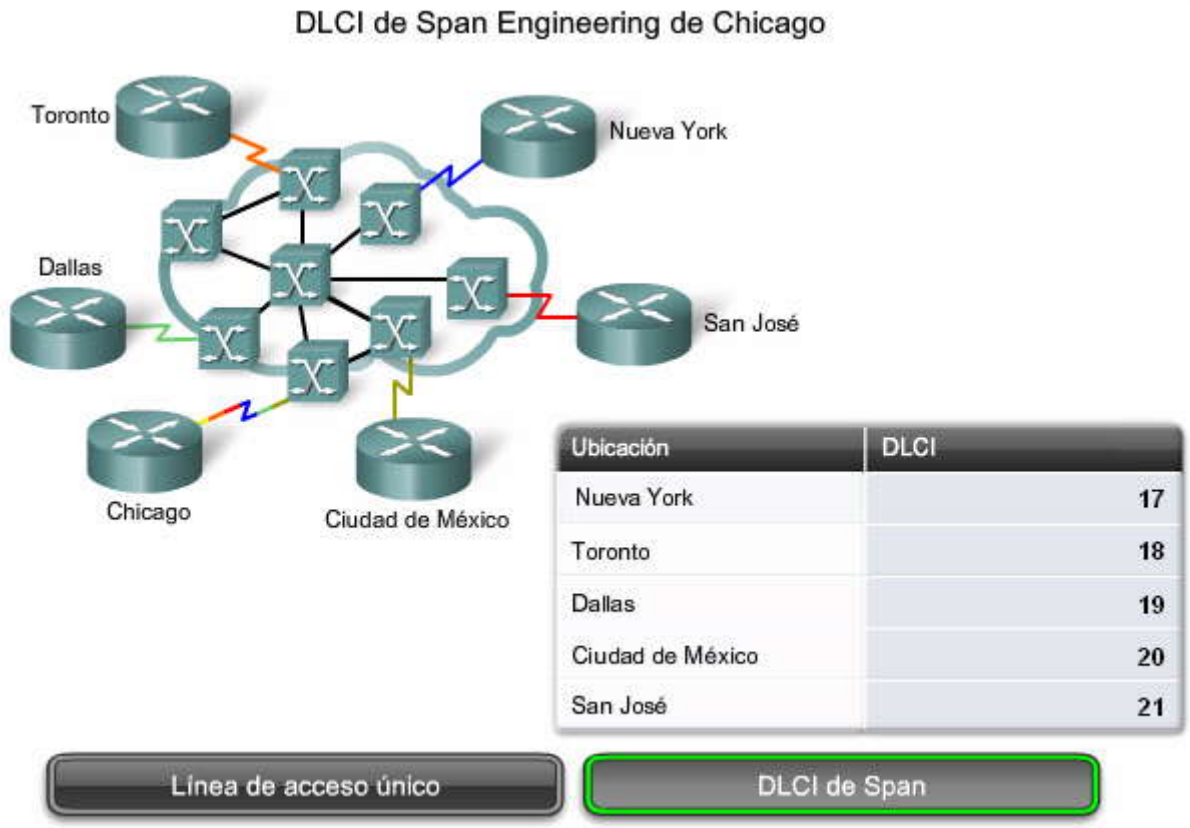
Esta capacidad suele reducir la complejidad del equipo y la red requerida para conectar varios dispositivos, lo que constituye un reemplazo rentable de una malla de líneas de acceso. Con esta configuración, cada punto final necesita sólo una línea de acceso única e interfaz. Se generan ahorros adicionales ya que la capacidad de la línea de acceso se establece según las necesidades de ancho de banda promedio de los VC, y no según las necesidades máximas de ancho de banda.

Haga clic en el botón DLCI de Span que se muestra en la figura.
Por ejemplo, Span Engineering tiene cinco ubicaciones, con sus sedes en Chicago. Chicago está conectado a la red mediante cinco VC y cada uno de ellos recibe un DLCI. Para ver las asignaciones de DCLI respectivas de Chicago, haga clic en la ubicación de la tabla.

Beneficios de costo de los VC múltiples

Recuerde el ejemplo anterior de cómo Span Engineering evolucionó de ser una red de líneas dedicadas hasta convertirse en una red Frame Relay. Específicamente, observe la tabla que compara el costo de una única conexión Frame Relay con el de una conexión ISDN de tamaño similar. Observe que, con Frame Relay, los clientes pagan por el ancho de banda que usan. De hecho, pagan por un puerto Frame Relay. Cuando incrementan la cantidad de puertos, según se ha descrito anteriormente, pagan por más ancho de banda. No obstante, ¿pagarán por más equipos? La respuesta corta es "no", dado que los puertos son virtuales. No hay cambios en la infraestructura física. Compare esta situación con la compra de más ancho de banda a través de líneas dedicadas.





3.1.3 Encapsulación Frame Relay

El proceso de encapsulación Frame Relay

Frame Relay toma paquetes de datos de un protocolo de capa de red, como IP o IPX, los encapsula como la parte de datos de una trama Frame Relay y, luego, pasa la trama a la capa física para entregarla en el cable. Para comprender el funcionamiento, resulta útil entender cómo se relaciona con los niveles más bajos del modelo OSI.

La figura muestra cómo Frame Relay encapsula los datos para su transporte y los mueve hacia la capa física para su entrega.

En principio, Frame Relay acepta un paquete de un protocolo de capa de red como IP. A continuación, lo ajusta con un campo de dirección que incluye el DCLI y una checksum. Se agregan campos señaladores para indicar el comienzo y el fin de la trama. Los campos señaladores marcan el comienzo y el fin de la trama, y siempre son los mismos. Los señaladores están representados como el número hexadecimal 7E o como el número binario 01111110. Después de haber encapsulado el paquete, Frame Relay pasa la trama a la capa física para su transporte.

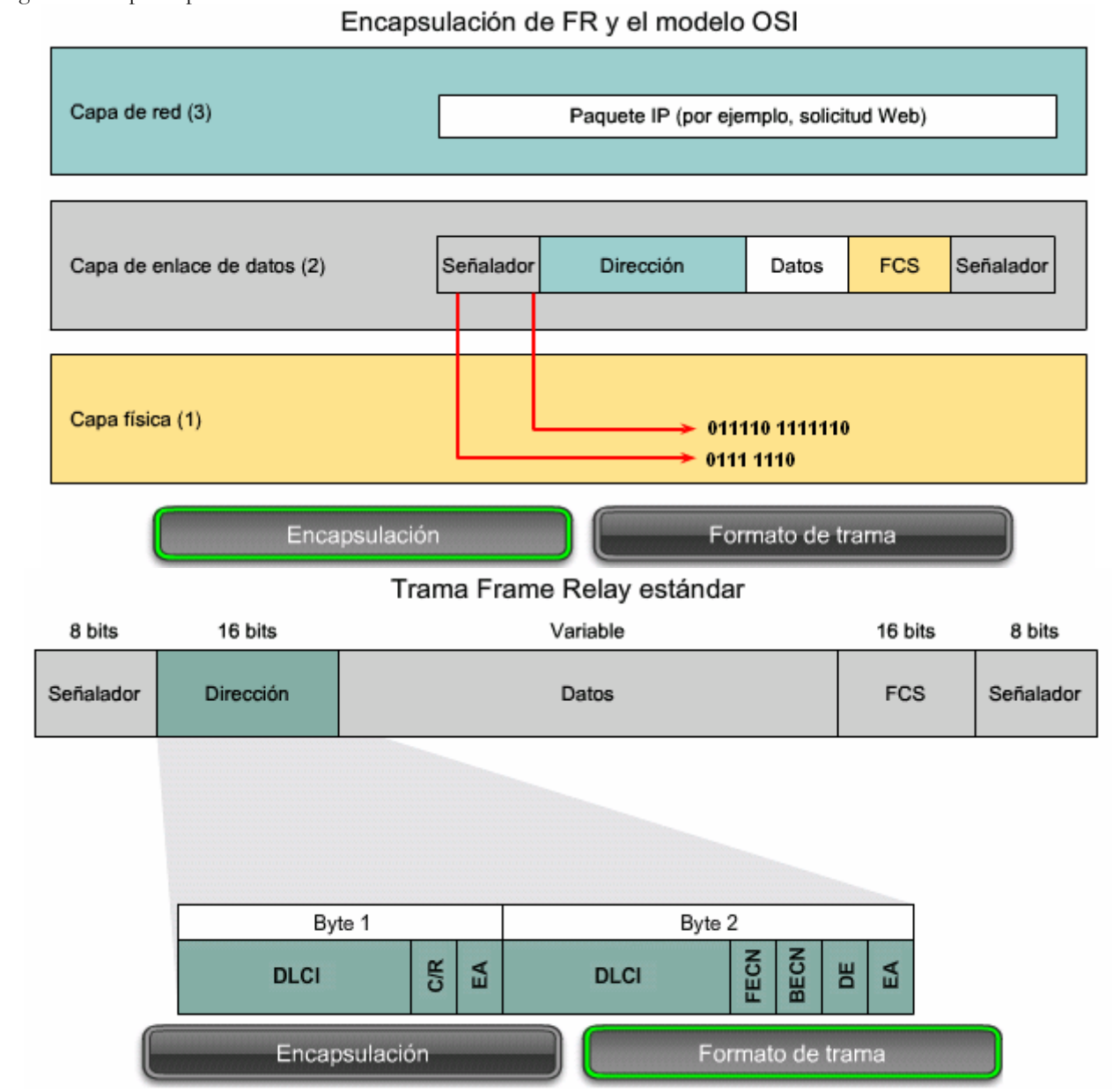
Haga clic en el botón Formato de trama que se muestra en la figura.

El router CPE encapsula cada paquete de Capa 3 dentro de un encabezado Frame Relay y tráiler antes de enviarlo a través del VC. El encabezado y el tráiler están definidos por la especificación de Servicios de portadora del Procedimiento de acceso al enlace para Frame Relay (LAPF), ITU Q.922-A. Específicamente, el encabezado Frame Relay (campo de dirección) incluye lo siguiente:

- DLCI: el DLCI de 10 bits es la esencia del encabezado Frame Relay. Este valor representa la conexión virtual entre el dispositivo DTE y el switch. Cada conexión virtual multiplexada en el canal físico está representada por un único DLCI. Los valores de DLCI tienen importancia local solamente, lo que significa que son únicos sólo para el canal físico en el que residen. Por lo tanto, los dispositivos situados en los extremos opuestos de una conexión pueden usar valores DLCI distintos para referirse a la misma conexión virtual.
- Dirección extendida (EA): si el valor del campo EA es 1, el byte actual está determinado como el último octeto DLCI. Si bien las implementaciones actuales de Frame Relay usan un DLCI de dos octetos, esta capacidad no permite DLCI más largos en el futuro. El octavo bit de cada byte del campo Dirección indica la EA.
- C/R: el bit que sigue al byte de DLCI más significativo en el campo Dirección. El bit C/R no está definido en este momento.

- Control de congestión: incluye 3 bits que controlan los mecanismos de notificación de congestión de Frame Relay. Los bits FECN, BECN y DE son los últimos tres bits en el campo Dirección. El control de congestión se explica en un tema posterior.

La capa física en general es EIA/TIA-232, 449 ó 530, V.35, o X.21. Las tramas Frame Relay son un subconjunto del tipo de trama HDLC. Por lo tanto, están delimitadas por campos señaladores. El señalador de 1 byte usa el patrón de bits 01111110. La FCS determina si hubo errores en el campo Dirección de Capa 2 durante la transmisión. La FCS se calcula antes de la transmisión a través del nodo emisor, y el resultado se inserta en el campo FCS. En el otro extremo, un segundo valor de FCS se calcula y compara con la FCS de la trama. Si los resultados son iguales, se procesa la trama. Si existe una diferencia, la trama se descarta. Frame Relay no notifica el origen cuando se descarta una trama. El control de errores tiene lugar en las capas superiores del modelo OSI.



3.1.4 Topologías de Frame Relay

Cuando se requiere conectar más de dos sitios, debe considerar la topología de las conexiones entre ellos. Una topología es el mapa o el diseño visual de la red Frame Relay. Debe considerar la topología desde diferentes perspectivas para comprender la red y el equipo utilizado para crear la red. Complete las topologías en relación con su diseño, implementación, operación y mantenimiento para que incluyan mapas de información general, mapas de conexiones lógicas, mapas funcionales y mapas de dirección que muestran el equipo detallado y enlaces de canal.

Las redes rentables Frame Relay vinculan docenas e incluso cientos de sitios. Si se tiene en cuenta que una red corporativa puede abarcar numerosos proveedores de servicio e incluir redes de negocios adquiridos que se diferencian en el diseño básico, documentar las topologías puede ser un proceso muy complicado. No obstante, cada red o segmento de red puede verse como uno de los tres tipos de topología: estrella, malla completa o malla parcial.

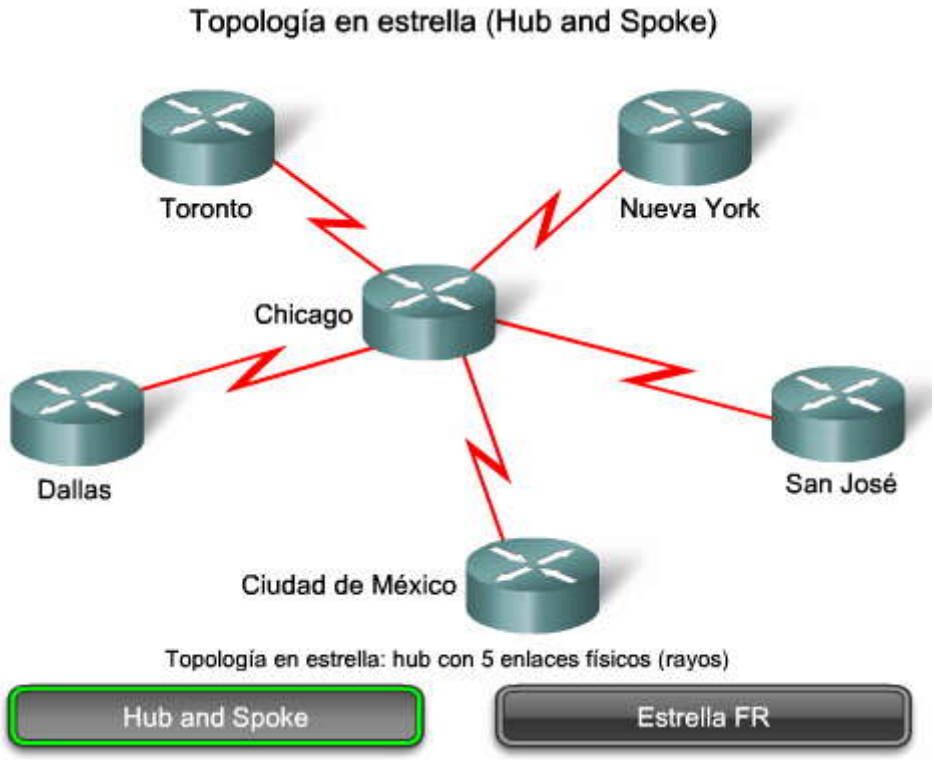
Topología en estrella (Hub and Spoke)

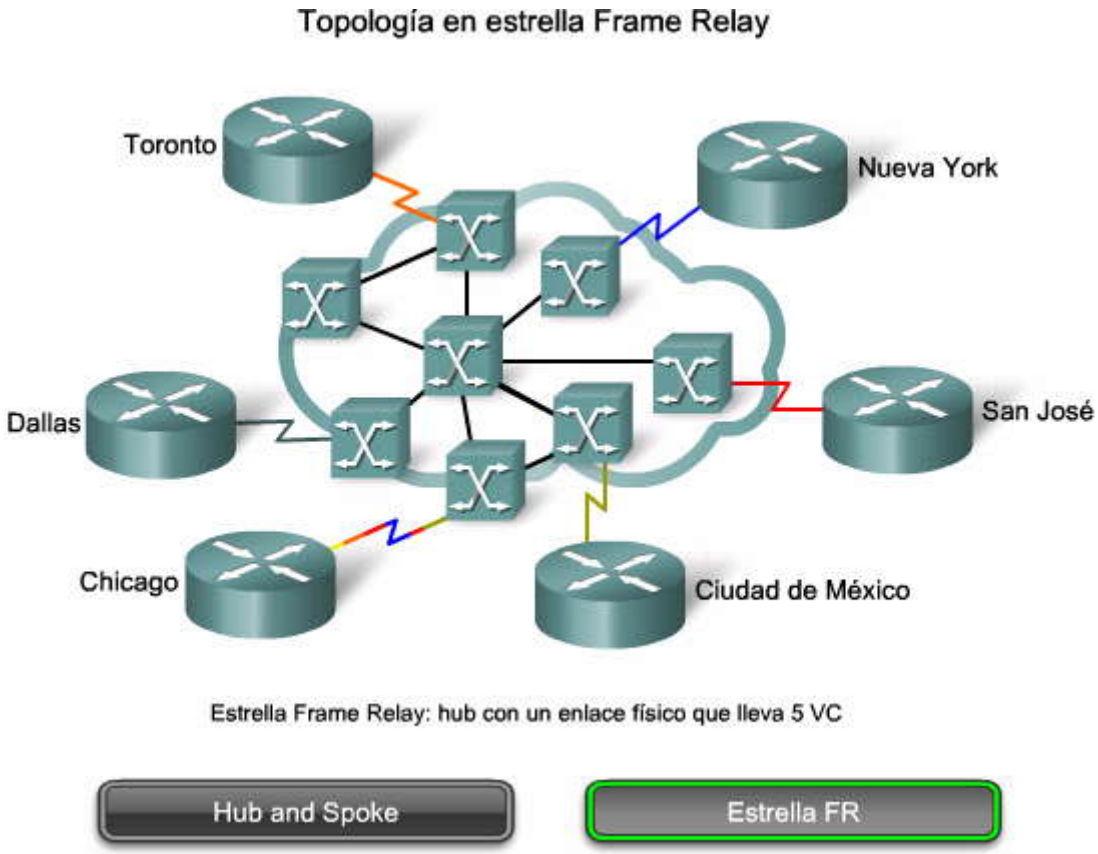
La topología de WAN más simple es una estrella, como se muestra en la figura. En esta topología, Span Engineering tiene un sitio central en Chicago que actúa como hub y alberga los servicios primarios. Observe que Span ha crecido y recientemente abrió una oficina en San José. El uso de Frame Relay hizo que esta expansión sea relativamente fácil.

Las conexiones con cada uno de los cinco sitios remotos actúan como rayos. En una topología en estrella, la ubicación del hub generalmente se elige por el costo más bajo de la línea arrendada. Al implementar una topología en estrella con Frame Relay, cada ubicación remota tiene un enlace de acceso a la nube de Frame Relay mediante un único VC.

Haga clic en el botón Estrella FR que se muestra en la figura.

De esta forma se muestra la topología en estrella en el contexto de una nube Frame Relay. El hub de Chicago tiene un enlace de acceso con varios VC, uno por cada sitio remoto. Las líneas que van desde la nube representan las conexiones de un proveedor de servicios Frame Relay y terminan en las instalaciones del cliente. Por lo general, son líneas cuya velocidad varía de 56 000 bps a E-1 (2048 Mbps) y más. Se asigna uno o más números DLCI a cada punto final de la línea. Debido a que los costos de Frame Relay no se establecen en función de la distancia, no es necesario que el hub esté situado en el centro geográfico de la red.





Topología de malla completa

Esta figura representa una topología de malla completa que usa líneas dedicadas. Se elige una topología de malla completa cuando los servicios a los que se debe tener acceso están geográficamente dispersos y se necesita un acceso altamente fiable. Una topología de malla completa conecta cada uno de los sitios con los demás. El uso de interconexiones de líneas arrendadas, interfaces seriales adicionales y líneas suma costos. En este ejemplo, se requieren diez líneas dedicadas para interconectar cada sitio en una topología de malla completa.

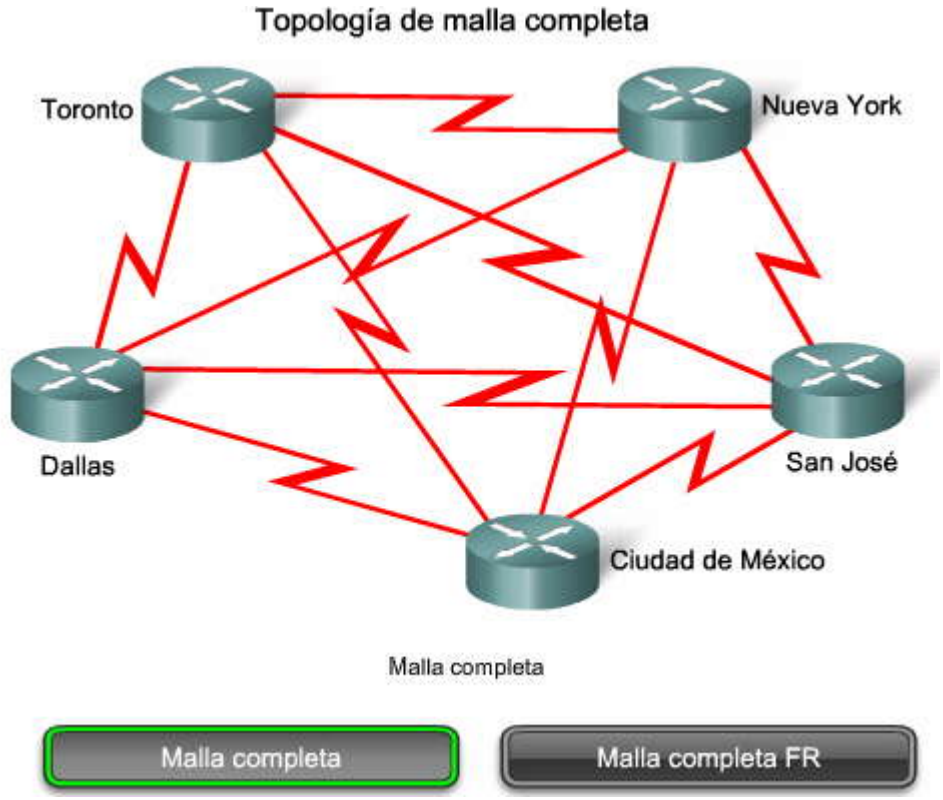
Haga clic en Malla completa FR que se muestra en la figura.

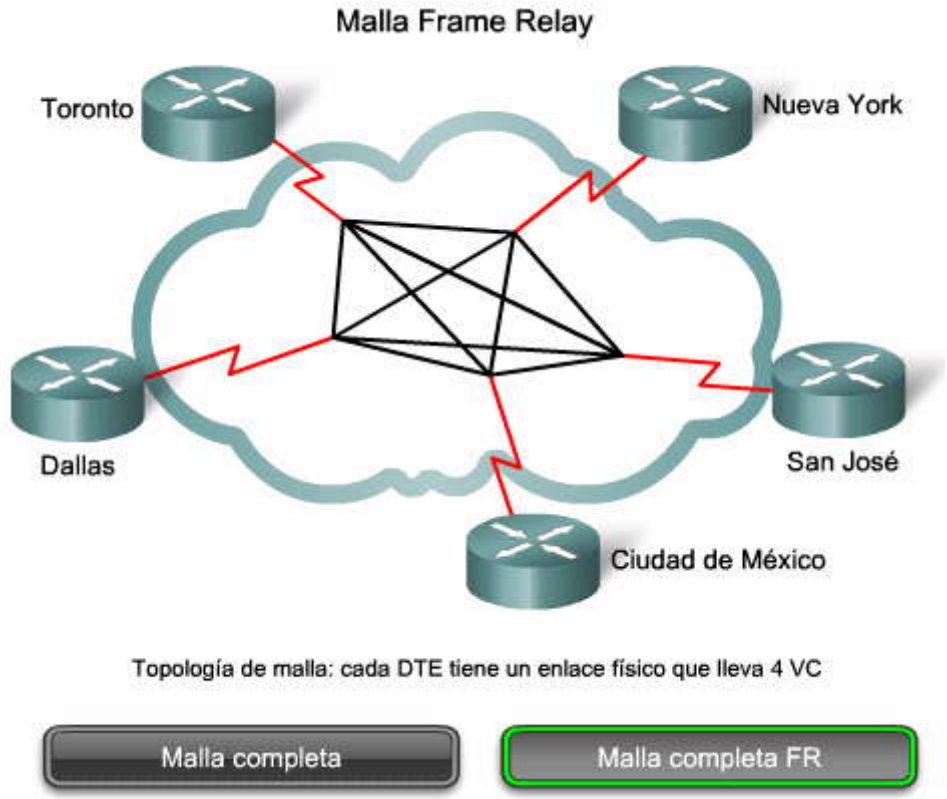
Usando Frame Relay, el diseñador de red puede crear varias conexiones simplemente configurando VC adicionales en cada enlace existente. Esta actualización de software aumenta la topología en estrella hasta transformarla en topología de malla completa, sin el costo de hardware adicional o líneas dedicadas. Dado que los VC usan la multiplexación estadística, varios VC ubicados en un enlace de acceso generalmente usan de mejor forma Frame Relay que los VC individuales. La figura muestra cómo Span utilizó cuatro VC en cada enlace para escalar su red sin agregar nuevo hardware. Los proveedores de servicios aplican cargos por el ancho de banda adicional, pero esta solución por lo general es más rentable que el uso de líneas dedicadas.

Topología de malla parcial

Para redes grandes, pocas veces se puede acceder a una topología de malla completa, dado que la cantidad de enlaces requerida incrementa considerablemente. El problema no está relacionado con el costo del hardware, sino que existe un límite teórico de menos de 1000 VC por enlace. En la práctica, el límite es menor.

Por este motivo, las redes más grandes suelen configurarse en una topología de malla parcial. Con la malla parcial, hay más interconexiones que las necesarias para una disposición en estrella, pero no tantas como para malla completa. El esquema real depende de las necesidades de flujo de datos.





3.1.5 Asignación de direcciones Frame Relay

Antes de que un router Cisco pueda transmitir datos a través de Frame Relay, necesita conocer los mapas de DLCI locales en la dirección de Capa 3 del destino remoto. Los routers Cisco admiten todos los protocolos de capa de red a través de Frame Relay, como IP, IPX y AppleTalk. Esta asignación de dirección a DLCI puede lograrse a través de la asignación estática o dinámica.

ARP inverso

El protocolo de resolución de direcciones inverso (ARP) obtiene direcciones de Capa 3 de otras estaciones de direcciones de Capa 2, como el DLCI en las redes Frame Relay. Se usa principalmente en redes Frame Relay y ATM, donde las direcciones de Capa 2 de VC a veces se obtienen de la señalización de Capa 2 y las direcciones de Capa 3 correspondientes deben estar disponibles antes de poder usar estos VC. Mientras ARP traduce las direcciones de Capa 3 a direcciones de Capa 2, ARP inverso efectúa el proceso opuesto.

Asignación dinámica

La asignación de direcciones dinámica depende de ARP inverso para resolver una dirección de protocolo de red de próximo salto a un valor de DLCI local. El router Frame Relay envía solicitudes de ARP inverso en su PVC para descubrir la dirección del protocolo del dispositivo remoto conectado a la red Frame Relay. El router usa las respuestas para completar una tabla de asignación de direcciones a DLCI en el router Frame Relay o servidor de acceso. El router crea y mantiene esta tabla de asignación, que incluye todas las solicitudes ARP inverso resueltas, incluidas las entradas de asignación dinámica y estática.

La figura muestra el resultado del comando **show frame-relay map**. Puede ver que la interfaz está activa y que la dirección IP de destino es 10.1.1.2. El DLCI identifica la conexión lógica que se usa para alcanzar esta interfaz. Este valor se muestra de tres formas: su valor decimal (102), su valor hexadecimal (0x66) y su valor según aparecería en el cable (0x1860). Ésta es una entrada estática, no una dinámica. El enlace usa encapsulación Cisco a diferencia de la encapsulación IETF.

En los routers Cisco, el ARP inverso está habilitado de forma predeterminada para todos los protocolos habilitados en la interfaz física. Los paquetes de ARP inverso no se envían para los protocolos que no están habilitados en la interfaz.

Haga clic en el botón Asignación estática que se muestra en la figura.

El usuario puede elegir sobrescribir la asignación dinámica de ARP inverso especificando una asignación estática manual para la dirección de protocolo del próximo salto a un DLCI local. Un mapa estático funciona de igual forma que un ARP inverso dinámico mediante la asociación de una dirección de protocolo de próximo salto a un DLCI Frame Relay local. No puede usar el ARP inverso y una sentencia de asignación para el mismo DLCI y protocolo.

Un ejemplo del uso de la asignación de direcciones estática es una situación en la que un router situado en el otro extremo de la red Frame Relay no admite el ARP inverso dinámico para un protocolo de red específico. Para proporcionar accesibilidad, se requiere una asignación estática para completar la dirección de capa de red remota a la resolución de DCLI local.

Otro ejemplo es en una red Frame Relay hub-and-spoke. Use la asignación de direcciones estática en los routers spoke para permitir la conexión spoke a spoke. Dado que los routers spoke no tienen conectividad directa entre sí, el ARP inverso dinámico no funciona entre ellos. El ARP inverso dinámico depende de la presencia de una conexión punto a punto directa entre los dos extremos. En este caso, el ARP inverso dinámico sólo funciona entre hub and spoke, y los spoke requieren la asignación estática para permitir la conexión entre sí.

Configuración de la asignación estática

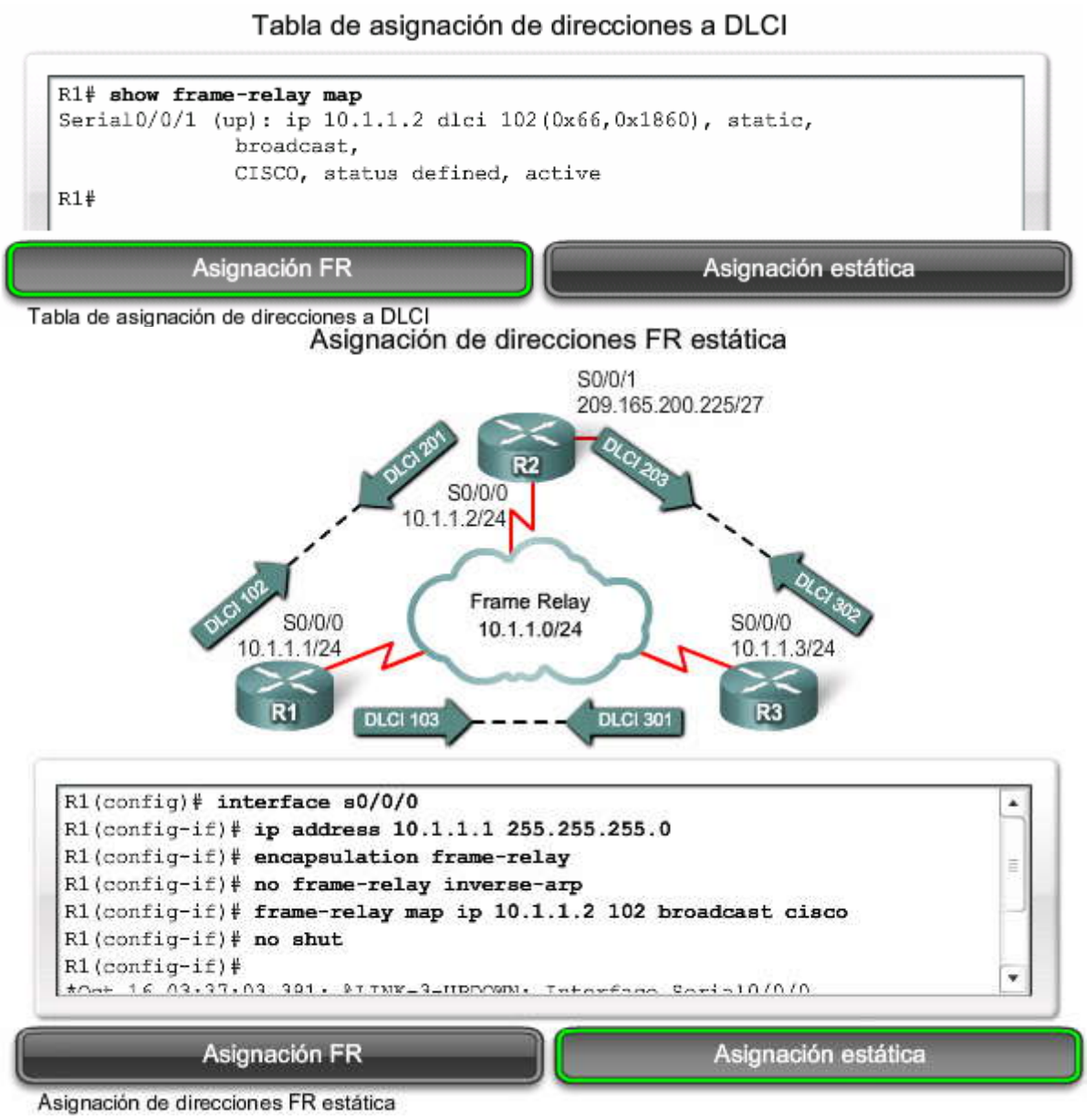
La definición de la asignación estática depende de las necesidades de su red. A continuación se incluyen diversos comandos que puede usar:

Para asignar entre una dirección de protocolo de próximo salto y una dirección destino de DLCI, use este comando: **frame-relay map protocol** *protocol-address dlci* [broadcast] [**ietf**] [**cisco**].

Use la palabra clave **ietf** al conectarse a un router no perteneciente a Cisco.

Puede simplificar en gran medida la configuración para el protocolo Open Shortest Path First (OSPF) mediante la adición de la palabra clave opcional **broadcast** al efectuar esta tarea.

La figura proporciona un ejemplo de la asignación estática en un router Cisco. En este ejemplo, la asignación estática de direcciones se realiza en la interfaz serial 0/0/0, y la encapsulación Frame Relay utilizada en DLCI 102 es CISCO. Según puede observarse en los pasos de configuración, la asignación estática de la dirección mediante el comando **frame-relay map** permite a los usuarios seleccionar el tipo de encapsulación Frame Relay utilizado en función de los VC. En la próxima sección se analiza en más detalle la configuración de la asignación estática.



Interfaz de administración local (LMI)

Una revisión del historial de networking lo ayudará a comprender la función que desempeña la Interfaz de administración local (LMI, Local Management Interface). El diseño de Frame Relay proporciona transferencia de datos conmutados por paquetes con un mínimo retardo de extremo a extremo. El diseño original omite todo aquello que pueda contribuir al retardo.

Cuando los fabricantes implementaron la Frame Relay como tecnología aparte y no como componente de la ISDN, decidieron que era necesario que los DTE pudieran obtener información sobre el estado de la red de forma dinámica. No obstante, el diseño original no incluía esta función. Un consorcio formado por Cisco, Digital Equipment Corporation (DEC), Northern Telecom y StrataCom extendió el protocolo Frame Relay para proporcionar capacidades adicionales para entornos de internetworking complejos. En conjunto, se hace referencia a estas extensiones como LMI.

Básicamente, la LMI es un mecanismo activo que proporciona información de estado sobre las conexiones Frame Relay entre el router (DTE) y el switch Frame Relay (DCE). Cada 10 segundos aproximadamente, el dispositivo final sondea la red en busca de una respuesta de secuencia no inteligente o información de estado de canal. Si la red no responde con la información solicitada, el dispositivo del usuario puede considerar que la conexión está inactiva. Cuando la red responde con una respuesta FULL STATUS, incluye información de estado sobre los DLCI que están asignados a esa línea. El dispositivo final puede usar esta información para determinar si las conexiones lógicas pueden transmitir datos.

La figura muestra el resultado del comando **show frame-relay lmi**. El resultado muestra el tipo de LMI utilizado por la interfaz Frame Relay y los contadores de la secuencia de intercambio de estado de la LMI, incluidos los errores como tiempos de espera agotados de LMI.

Es fácil confundir la LMI con la encapsulación. La LMI es una definición de los mensajes usados entre DTE (R1) y DCE (el switch Frame Relay propiedad del proveedor de servicios). La encapsulación define los encabezados utilizados por un DTE para comunicar información al DTE en el otro extremo de un VC. El switch y su router conectado se ocupan de usar la misma LMI. El switch no se ocupa de la encapsulación. Los routers de punto final (DTE) se ocupan de la encapsulación.

Extensiones LMI

Además de las funciones del protocolo Frame Relay para la transferencia de datos, la especificación Frame Relay incluye las extensiones LMI opcionales que son sumamente útiles en un entorno de internetworking. Algunas de las extensiones son:

- **Mensajes de estado de VC**: proporcionan información sobre la integridad de PVC a través de la comunicación y la sincronización entre dispositivos, así como de informes periódicos sobre la existencia de nuevos PVC y la eliminación de los PVC ya existentes. Los mensajes de estado de los VC impiden que se envíen datos a agujeros negros (PVC que ya no existen).
- **Multicasting**: permite que el emisor transmita una única trama que se entrega a varios destinatarios. El multicasting admite la entrega eficaz de mensajes de protocolo de enrutamiento y procedimientos de resolución de direcciones que generalmente se envían a muchos destinos simultáneamente.
- **Direccionamiento global**: otorga a los identificadores de conexión una importancia global, más que local, lo que permite que se puedan usar para identificar una interfaz específica en relación con la red Frame Relay. El direccionamiento global hace que la red Frame Relay se asemeje a una LAN en relación con el direccionamiento, y los ARP se desempeñen exactamente igual que a través de una LAN.
- **Control de flujo simple**: proporciona un mecanismo de control de flujo XON/XOFF (de conexión/desconexión) que se aplica a toda la interfaz Frame Relay. Está destinado a los dispositivos cuyas capas superiores no pueden utilizar los bits de notificación de congestión y que necesitan algún nivel de control de flujo.

Haga clic en el botón Identificadores LMI que se muestra en la figura.

El campo DLCI de 10 bits admite 1024 identificadores de VC: de 0 a 1023. Las extensiones LMI se reservan algunos de estos identificadores y, por lo tanto, reducen la cantidad de VC permitidos. Los mensajes LMI se intercambian entre los DTE y los DCE mediante los DLCI reservados.

Existen varios tipos de LMI, todos incompatibles entre sí. El tipo de LMI configurado en el router debe coincidir con el utilizado por el proveedor de servicios. Los routers Cisco admiten tres tipos de LMI:

- Cisco: extensión LMI original
- Ansi: las correspondientes al estándar ANSI T1.617 Anexo D
- q933a: las correspondientes al estándar UIT Q933 Anexo A

Comenzando con la versión 11.2 del software IOS de Cisco, la función predeterminada de detección automática de LMI detecta el tipo de LMI admitido por el switch Frame Relay conectado directamente. En función de los mensajes de estado de LMI que recibe del switch Frame Relay, el router configura automáticamente su interfaz con el tipo de LMI admitido reconocido por el switch Frame Relay.

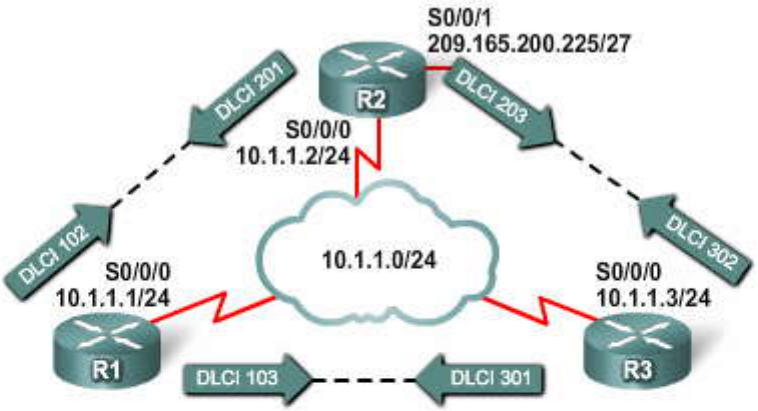
Si es necesario configurar el tipo de LMI, use el comando de configuración de interfaz **frame-relay lmi-type** [**cisco** | **ansi** | **q933a**]. La configuración del tipo de LMI deshabilita la función de detección automática.

Cuando configura manualmente el tipo de LMI, debe configurar el intervalo activo en la interfaz Frame Relay para evitar que se agote el tiempo de espera de los intercambios de estado entre el router y el switch. Los mensajes de intercambio de estado de LMI determinan el estado de la conexión de PVC. Por ejemplo, una gran falta de coincidencia en el intervalo activo en el router y el switch puede hacer que el switch declare al router muerto.

De forma predeterminada, el intervalo de tiempo activo es de 10 segundos en las interfaces seriales Cisco. Puede cambiar el intervalo activo con el comando de configuración de interfaz **keepalive**.

En la actividad siguiente, se practica determinar el tipo de LMI y la configuración del mensaje activo.

Estadísticas de LMI




```
R1#show frame-relay lmi
LMI Statistics for interface Serial0/0/0 (Frame Relay DTE) LMI
TYPE = ANSI
Invalid Unnumbered info 0 Invalid Prot Disc 0
Invalid dummy Call Ref 0 Invalid Msg Type 0
Invalid Status Message 0 Invalid Lock Shift 0
Invalid Information ID 0 Invalid Report IE Len 0
Invalid Report Request 0 Invalid Keep IE Len 0
Num Status Enq. Sent 9 Num Status msgs Rcvd 0
Num Update Status Rcvd 0 Num Status Timeouts 9
```

Estadísticas de LMI | Identificadores LMI

Identificadores LMI

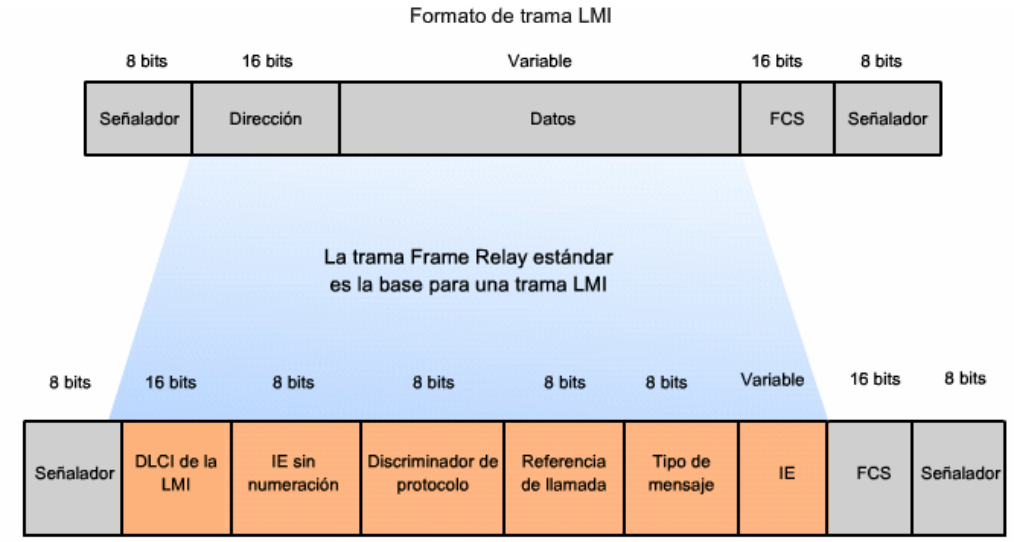
Identificadores de VC	Tipos de VC
0	LMI (ANSI, UIT)
1...15	Se reserva para uso futuro
992...1007	CLLM
2008...1022	Se reserva para uso futuro (ANSI, UIT)
1019...1020	Multicasting (Cisco)
1023	LMI (Cisco)

Estadísticas de LMI | Identificadores LMI

Formato de trama LMI

Los mensajes LMI se envían a través de una variante de las tramas LAPF. El campo de dirección lleva uno de los DLCI reservados. Seguido al campo DLCI se encuentran los campos de control, de discriminación de protocolos y de referencia de llamada, los cuales no cambian. El cuarto campo indica el tipo de mensaje LMI.

Los mensajes de estado ayudan a verificar la integridad de los enlaces físicos y lógicos. Esta información resulta fundamental en un entorno de enrutamiento, ya que los protocolos de enrutamiento toman decisiones según la integridad del enlace.



Uso de LMI y ARP inverso para asignar direcciones

Los mensajes de estado de LMI combinados con los mensajes de ARP inverso permiten al router asociar direcciones de capa de red y de enlace de datos.

Haga clic en el botón LMI 1 y reproducir para observar cómo comienza el proceso de la LMI.

En este ejemplo, cuando R1 se conecta con la red Frame Relay, envía un mensaje de consulta de estado LMI a la red. La red contesta con un mensaje de estado LMI que contiene detalles de cada VC configurado en el enlace de acceso.

Periódicamente, el router repite la consulta de estado, pero las respuestas subsiguientes sólo incluyen los cambios de estado. Después de una determinada cantidad de respuestas abreviadas, la red envía un mensaje de estado completo.

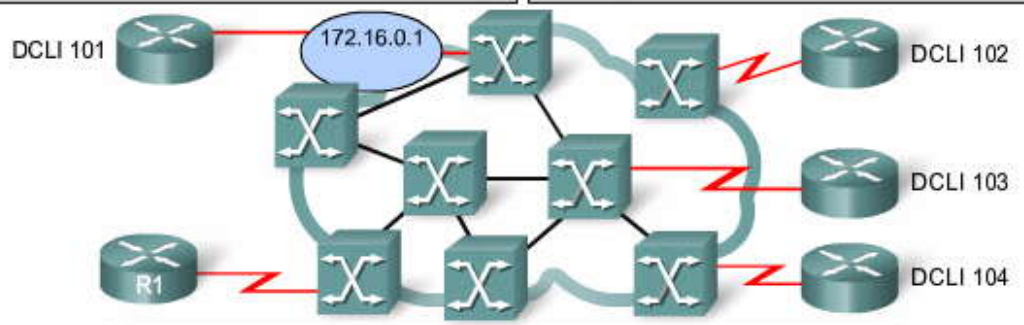
Haga clic en el botón LMI 2 y reproducir para ver la próxima etapa.

Si el router necesita asignar los VC a las direcciones de capa de red, envía un mensaje de ARP inverso desde cada VC. El mensaje de ARP inverso incluye la dirección de capa de red del router, de modo que el DTE o el router remoto puedan realizar la vinculación. La respuesta de ARP inverso permite al router hacer los registros necesarios en su tabla de asignaciones de direcciones a DLCI. Si el enlace soporta varios protocolos de capa de red, se envían mensajes de ARP inversos para cada uno de ellos.

Uso de LMI y ARP inverso para asignar direcciones

El DTE envía ARP inversos en un circuito virtual de Mapeo de circuitos virtuales a la dirección de red

El DTE remoto responde con la dirección de Capa 3

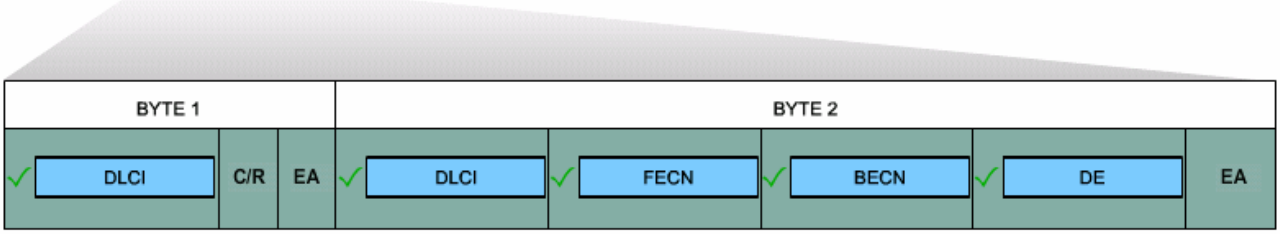


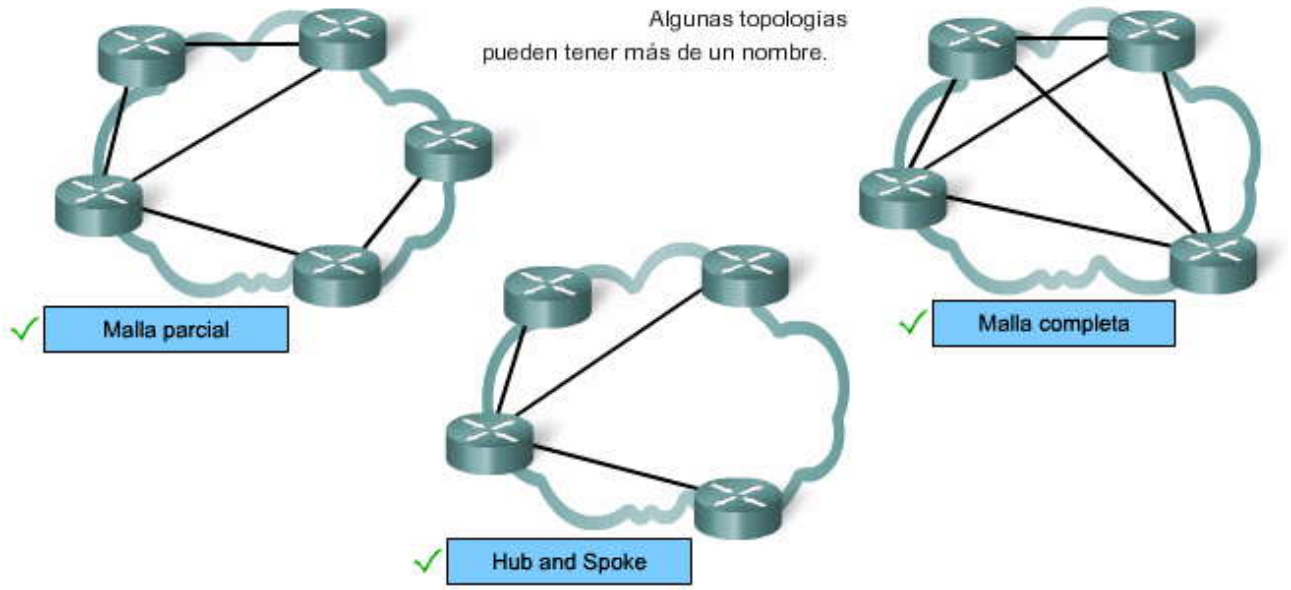
DLCI	Estado
101	Activo
102	Activo
103	Activo
104	Activo

LMI 1 | LMI 2

Frame Relay se ha convertido en la tecnología WAN de uso más frecuente, principalmente por su ____ y ____.	✓ precio ✓ flexibilidad
Frame relay es una tecnología de conmutación ____que es una versión simplificada del estándar ____ anterior.	✓ paquete ✓ X.25
Frame Relay usa una técnica de "máximo esfuerzo" que consiste en simplemente ____ paquetes cuando detecta errores, lo que deja la corrección de errores necesaria (como la retransmisión de datos) a cargo de los puntos finales.	✓ descarta
Frame Relay transmite datos entre los dispositivos ____ del usuario y los dispositivos ____ en el extremo de la WAN.	✓ DTE ✓ DCE
La conexión a través de la red Frame Relay entre dos DTE se denomina ____ virtual (VC).	✓ circuito
Los circuitos virtuales ____ se establecen de forma dinámica mediante el envío de mensajes de señalización a la red.	✓ Conmutado
Los circuitos virtuales ____ son preconfigurados por la portadora y siempre funcionan en el modo de TRANSFERENCIA DE DATOS o INACTIVO.	✓ Permanente
Los circuitos virtuales proporcionan comunicaciones bidireccionales y se identifican mediante un ____ de forma única, que no tiene significado más allá del enlace único.	✓ DLCI

en el encabezado de Frame Relay.





La asignación dinámica de direcciones depende de ____ Frame Relay para resolver una dirección de protocolo de red de próximo salto a un valor DLCI local.	✓ ARP inverso
Para configurar la asignación estática de direcciones, use el comando ____ en el modo de configuración de interfaz.	✓ frame-relay map
Las extensiones ____ al protocolo Frame Relay proporcionan capacidades adicionales para complejos entornos de internetworking.	✓ Interfaz de administración local
Los tipos de LMI incluyen cisco, ____ y ____.	✓ ansi ✓ q933a
Los ____ combinados con los mensajes ____ permiten que un router vincule direcciones de capa de red con direcciones de la capa de enlace de datos.	✓ mensajes de estado LMI ✓ ARP inverso

3.2 Configuración de Frame Relay

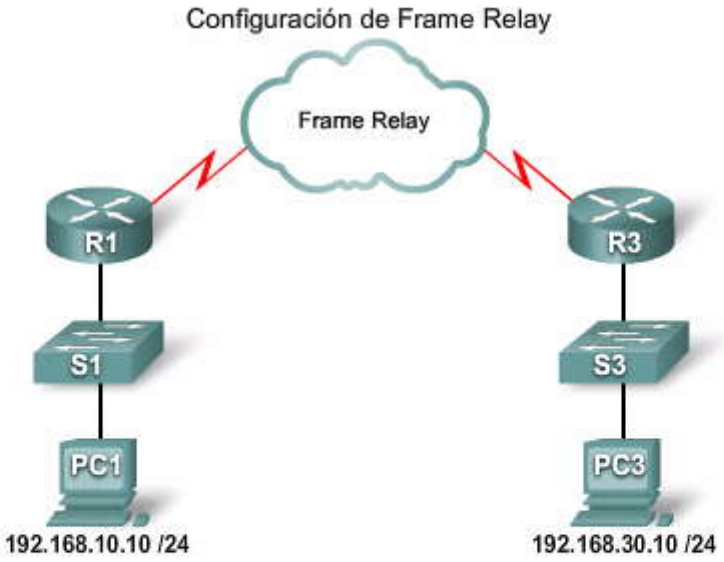
3.2.1 Configuración básica de Frame Relay

Tareas de configuración de Frame Relay

Frame Relay se configura en un router Cisco desde la interfaz de la línea de comando del IOS de Cisco (CLI). Esta sección describe los pasos requeridos para habilitar Frame Relay en su red, además de algunos de los pasos opcionales para mejorar o personalizar su configuración.

La figura muestra el modelo de configuración básica utilizado para este debate. Más adelante en esta sección, se agrega hardware adicional al diagrama para ayudar a explicar tareas de configuración más complejas. En esta sección, configurará los routers Cisco como dispositivos de acceso Frame Relay o DTE conectados directamente a un switch Frame Relay dedicado, o DCE.

La figura muestra una configuración de Frame Relay típica y enumera los pasos que se deben seguir. Estos pasos se explican y se practican en este capítulo.



Tareas requeridas	Tareas opcionales
• Habilitar encapsulación Frame Relay en una interfaz • Configurar asignación dinámica o estática de direcciones	• Configurar LMI • Configurar SVC Frame Relay • Configurar conformación del tráfico Frame Relay • Personalizar Frame Relay para su red • Supervisar y mantener las conexiones Frame Relay

Habilitar encapsulación Frame Relay

Esta primera figura muestra cómo se configuró Frame Relay en las interfaces seriales. Implica la asignación de una dirección IP, la configuración del tipo de encapsulación y la asignación de ancho de banda. La figura muestra los routers de cada extremo del enlace Frame Relay con las secuencias de comandos de configuración para los routers R1 y R2.

Paso 1. Configuración de la dirección IP en la interfaz

En un router Cisco, Frame Relay se admite con mayor frecuencia en las interfaces seriales síncronas. Use el comando **ip address** para definir la dirección IP de la interfaz. Puede ver que se ha asignado la dirección IP 10.1.1.1/24 a R1 y la dirección IP 10.1.1.2/24 a R2.

Paso 2. Configuración de encapsulación

El comando de configuración de interfaz **encapsulation frame-relay** habilita la encapsulación Frame Relay y permite el procesamiento Frame Relay en la interfaz admitida. Hay dos opciones de encapsulación entre las que puede elegir; las cuales se describen a continuación.

Paso 3. Establecimiento del ancho de banda

Use el comando **bandwidth** para definir el ancho de banda de la interfaz serial. Especifique el ancho de banda en kbps. Este comando notifica al protocolo de enrutamiento que el ancho de banda se configura estadísticamente en el enlace. Los protocolos de enrutamiento EIGRP y OSPF usan el valor del ancho de banda para calcular y determinar la métrica del enlace.

Paso 4. Configuración del tipo de LMI (opcional)

Es un paso opcional dado que los routers Cisco detectan automáticamente el tipo de LMI. Recuerde que Cisco admite tres tipos de LMI: Cisco, ANSI Anexo D y Q933-A Anexo A, y que el tipo de LMI predeterminado para los routers Cisco es cisco.

Opciones de encapsulación

Recuerde que el tipo de encapsulación predeterminado en una interfaz serial de un router Cisco es la versión de HDLC propiedad de Cisco. Para cambiar la encapsulación de HDLC a Frame Relay, use el comando **encapsulation frame-relay**

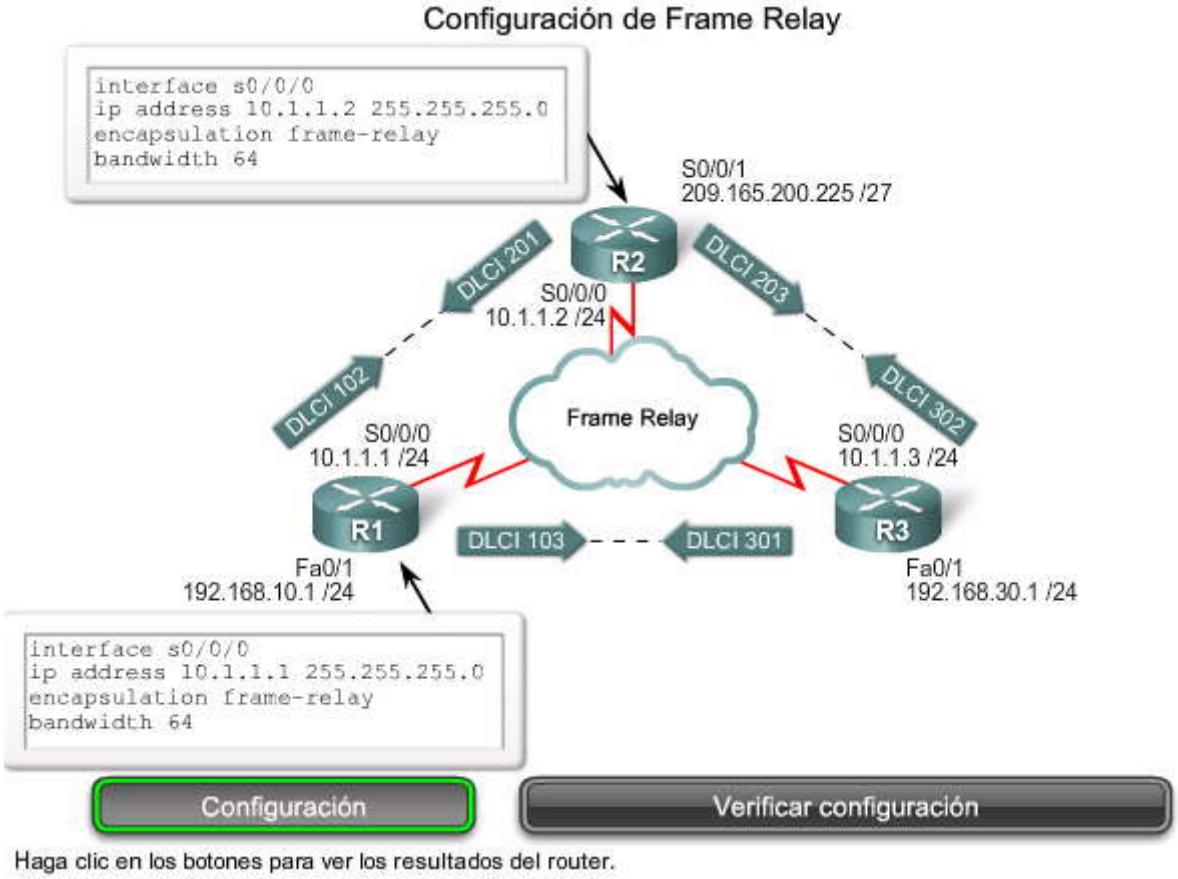
[**cisco** | **ietf**]. La forma **no** del comando **encapsulation frame-relay** quita la encapsulación Frame Relay de la interfaz y regresa la interfaz a la encapsulación de HDLC predeterminada.

La encapsulación Frame Relay predeterminada habilitada en las interfaces admitidas es la encapsulación Cisco. Use esta opción para conectarse a otro router Cisco. Muchos dispositivos de otras marcas también soportan este tipo de encapsulación. Usa un encabezado de 4 bytes, 2 bytes identifican el DLCI y 2 bytes identifican el tipo de paquete.

El tipo de encapsulación IETF cumple con RFC 1490 y RFC 2427. Use esta opción si se conecta a un router no perteneciente a Cisco.

Haga clic en el botón Verificar que se muestra en la figura.

Este resultado del comando **show interfaces serial** verifica la configuración.



3.2.2 Configuración de mapas estáticos de Frame Relay

Configuración de un mapa estático de Frame Relay

Los routers Cisco admiten todos los protocolos de capa de red a través de Frame Relay, como IP, IPX y AppleTalk; y la asignación de dirección a DLCI puede lograrse a través de la asignación de direcciones dinámica o estática.

La asignación dinámica se efectúa a través de la función ARP inverso. Dado que ARP inverso está habilitado de forma predeterminada, no se requieren comandos adicionales para configurar la asignación dinámica enuna interfaz.

La asignación estática se configura manualmente en un router. Establecer la asignación estática depende de sus necesidades de red. Para asignar entre una dirección protocolo de próximo salto y una dirección destino de DLCI, use el comando **frame-relay map** *protocol protocol-address dlci* [**broadcast**].

Uso de la palabra clave broadcast

Frame Relay, ATM y X.25 son redes de acceso múltiple sin broadcast (NBMA, Non-Broadcast Multiple Access). Las redes NBMA permiten sólo la transferencia de datos de un equipo a otro a través de un VC o de un dispositivo conmutado. Las redes NBMA no admiten el tráfico multicast ni broadcast, de modo que un único paquete no puede llegar a todos los destinos. Esto requiere enviar un broadcast para replicar los paquetes manualmente a todos los destinos.

Algunos protocolos de enrutamiento pueden requerir opciones de configuración adicionales. Por ejemplo, RIP, EIGRP y OSPF exigen configuraciones adicionales para ser admitidos en redes NBMA.

Dado que NBMA no admite tráfico de broadcast, el uso de la palabra clave **broadcast** es una forma simplificada de enviar actualizaciones de enrutamiento. La palabra clave **broadcast** permite enviar broadcast y multicast a través del PVC y, de hecho, convierte al broadcast en un unicast de modo que el otro nodo obtenga las actualizaciones de enrutamiento.

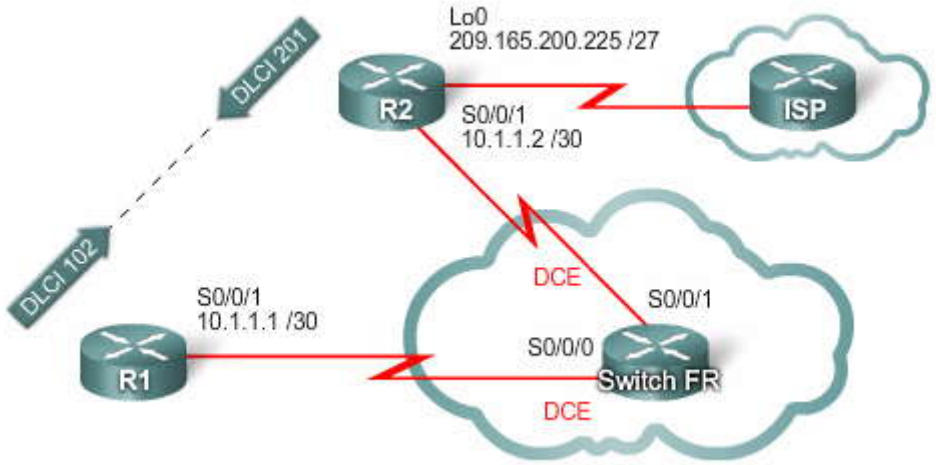
En el ejemplo de configuración, R1 usa el comando **frame-relay map** para asignar el VC a R2.

Haga clic en el botón Parámetros que se muestra en la figura.

La figura muestra cómo usar las palabras clave al configurar asignaciones de direcciones estáticas.

Haga clic en el botón Verificar que se muestra en la figura.

Para verificar la asignación de Frame Relay, use el comando **show frame-relay map**.



Configuración de un mapa estático Frame Relay

Configuración para R1

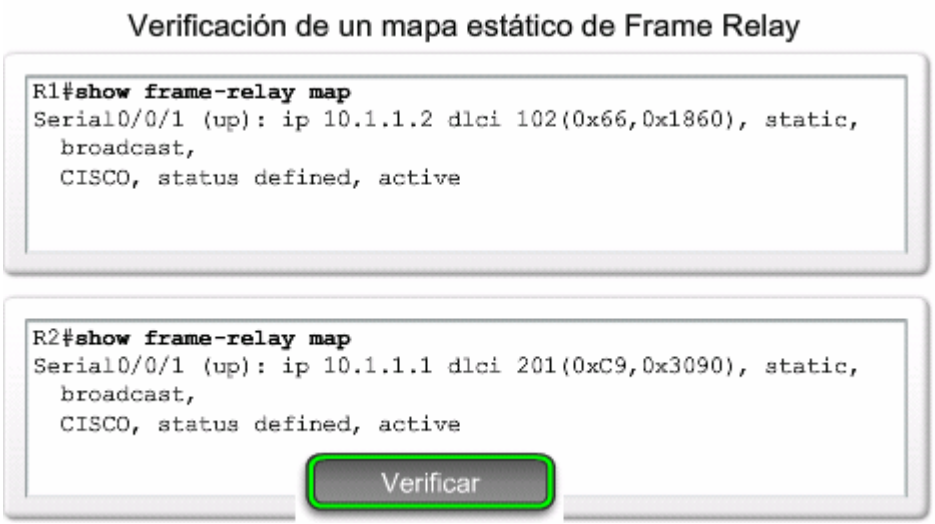
```
interface s0/0/1
ip address 10.1.1.1 255.255.255.252
encapsulation frame-relay
bandwidth 64
frame-relay map ip 10.1.1.2 102 broadcast
```

Mapas estáticos

Parámetros de comando

Parámetros de comando	Descripción
protocolo	Define el protocolo admitido, puenteo o control de enlace lógico: appletalk, decnet, dlsw, ip, ipx, llc2, rsrb, vines y xns.
protocol-address	Define la dirección de capa de red de la interfaz del router de destino.
dlci	Define el DLCI local mediante el cual se conecta a la dirección de protocolo remoto.
broadcast	(Opcional) Permite broadcasts y multicasts por medio de VC. Esto permite el uso de protocolos de enrutamiento dinámico en el VC.

Parámetros



3.3 Conceptos avanzados de Frame Relay

3.3.1 Solución de problemas relacionados a la posibilidad de conexión

Horizonte dividido

De forma predeterminada, una red Frame Relay proporciona conectividad NBMA entre sitios remotos. Las nubes NBMA generalmente usan una topología hub-and-spoke. Desafortunadamente, el funcionamiento de un enrutamiento básico, basado en el principio de horizonte dividido, puede generar problemas relacionados con la posibilidad de conexión en una red NBMA Frame Relay.

Recuerde que el horizonte dividido es una técnica que se usa para evitar un routing loop en redes que usan protocolos de enrutamiento de vector distancia. La actualización mediante horizonte dividido reduce los bucles de enrutamiento, al no permitir que una actualización de enrutamiento recibida en una interfaz sea reenviada por la misma interfaz.

La figura muestra R2, un router spoke, que envía una actualización de enrutamiento broadcast a R1, el router hub.

Los routers que admiten varias conexiones a través de una única interfaz física tienen varios PVC que terminan en una única interfaz. R1 debe replicar los paquetes broadcast, por ejemplo, los broadcasts de actualización de enrutamiento, en todos los PVC y enviarlos a los routers remotos. Los paquetes broadcast replicados pueden consumir ancho de banda y aumentar considerablemente la latencia en el tráfico de usuario. La cantidad de tráfico de broadcast y la cantidad de VC que terminan en cada router deben evaluarse durante la fase de diseño de una red Frame Relay. El tráfico excesivo, como las actualizaciones de enrutamiento, pueden afectar la entrega de datos críticos del usuario, especialmente cuando la ruta de entrega incluye enlaces de bajo ancho de banda (56 kbps).

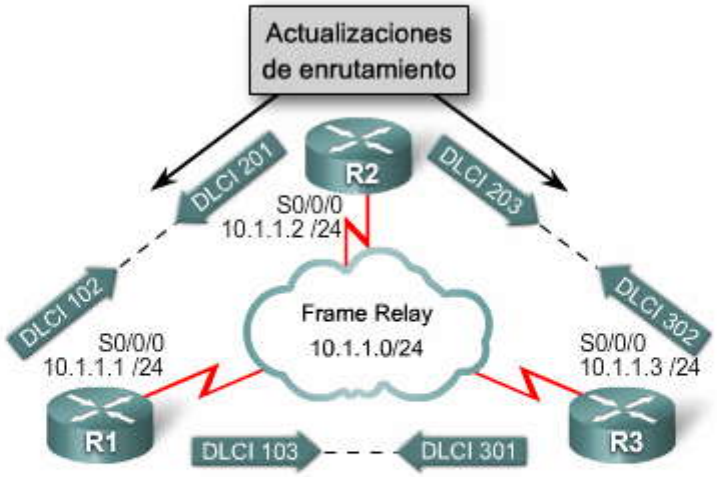
Haga clic en el botón Problema de horizonte dividido que se muestra en la figura.

R1 tiene varios PVC en una única interfaz física, de modo que la regla de horizonte dividido evita que R1 reenvíe esa actualización de enrutamiento a través de la misma interfaz física a otros routers spoke remotos (R3).

Deshabilitar el horizonte dividido puede parecer una solución simple, ya que permite que las actualizaciones de enrutamiento se envíen a la misma interfaz física en la que se originaron. No obstante, sólo IP le permite deshabilitar el horizonte dividido; IPX y AppleTalk no. Además, la deshabilitación de horizonte dividido aumenta las posibilidades de bucles de enrutamiento en cualquier red. El horizonte dividido puede deshabilitarse para las interfaces físicas con un único PVC.

La siguiente solución evidente para solucionar el problema de horizonte dividido es usar una topología de malla completa. No obstante, esta solución es costosa, ya que se requieren más PVC. La solución preferida es usar subinterfaces, lo cual se explica en el siguiente tema.

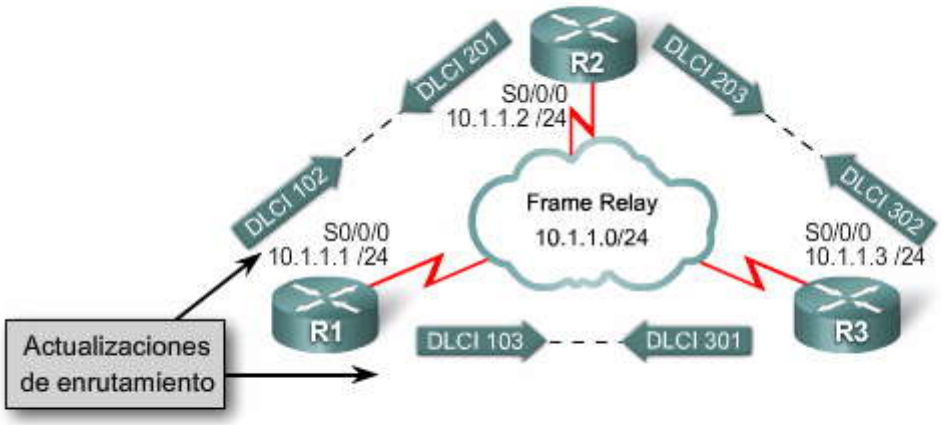
Regla de horizonte dividido



Problema: La actualización recibida en una interfaz física no se retransmite por esa misma interfaz: horizonte dividido.

Regla de horizonte dividido | Problema de horizonte dividido

Problema de horizonte dividido



Problema: El tráfico de broadcast se debe replicar para cada conexión activa.

Regla de horizonte dividido | Problema de horizonte dividido

Subinterfaces Frame Relay

Frame Relay puede partir una interfaz física en varias interfaces virtuales denominadas subinterfaces. Una subinterfaz es simplemente una interfaz lógica directamente asociada con una interfaz física. Por lo tanto, se puede configurar una subinterfaz Frame Relay para cada uno de los PVC que ingresan a una interfaz serial física.

Para habilitar el reenvío de actualizaciones de enrutamiento de broadcast en una red Frame Relay, puede configurar el router con subinterfaces asignadas lógicamente. Una red con mallas parciales puede dividirse en varias redes punto a punto de mallas completas más pequeñas. Se puede asignar a cada subred punto a punto una dirección de red única, que permite que los paquetes recibidos en una interfaz física se envíen a la misma interfaz física, dado que se envían en VC de diferentes subinterfaces.

Las subinterfaces Frame Relay pueden configurarse en modo punto a punto y en modo multipunto:

- Punto a punto: una única subinterfaz punto a punto establece una conexión de PVC a otra interfaz física o subinterfaz en un router remoto. En este caso, cada pareja de routers punto a punto está en su propiasubred y cada subinterfaz punto a punto tiene un solo DLCI. En un entorno punto a punto, cada subinterfaz actúa como interfaz punto a punto. En general, hay una subred separada para cada VC punto a punto. Entonces, el tráfico de actualización de enrutamiento no está sujeto a la regla del horizonte dividido.
- Multipunto: una única subinterfaz multipunto establece varias conexiones de PVC a varias interfaces físicas o subinterfaces de routers remotos. Todas las interfaces involucradas se encuentran en la misma subred. La subinterfaz actúa como interfaz NBMA Frame Relay de modo que el tráfico de actualización de enrutamiento está sujeto a la regla de horizonte dividido. En general, todos los VC multipunto pertenecen a la misma subred.

La figura ilustra dos tipos de subinterfaces admitidas por los routers Cisco.

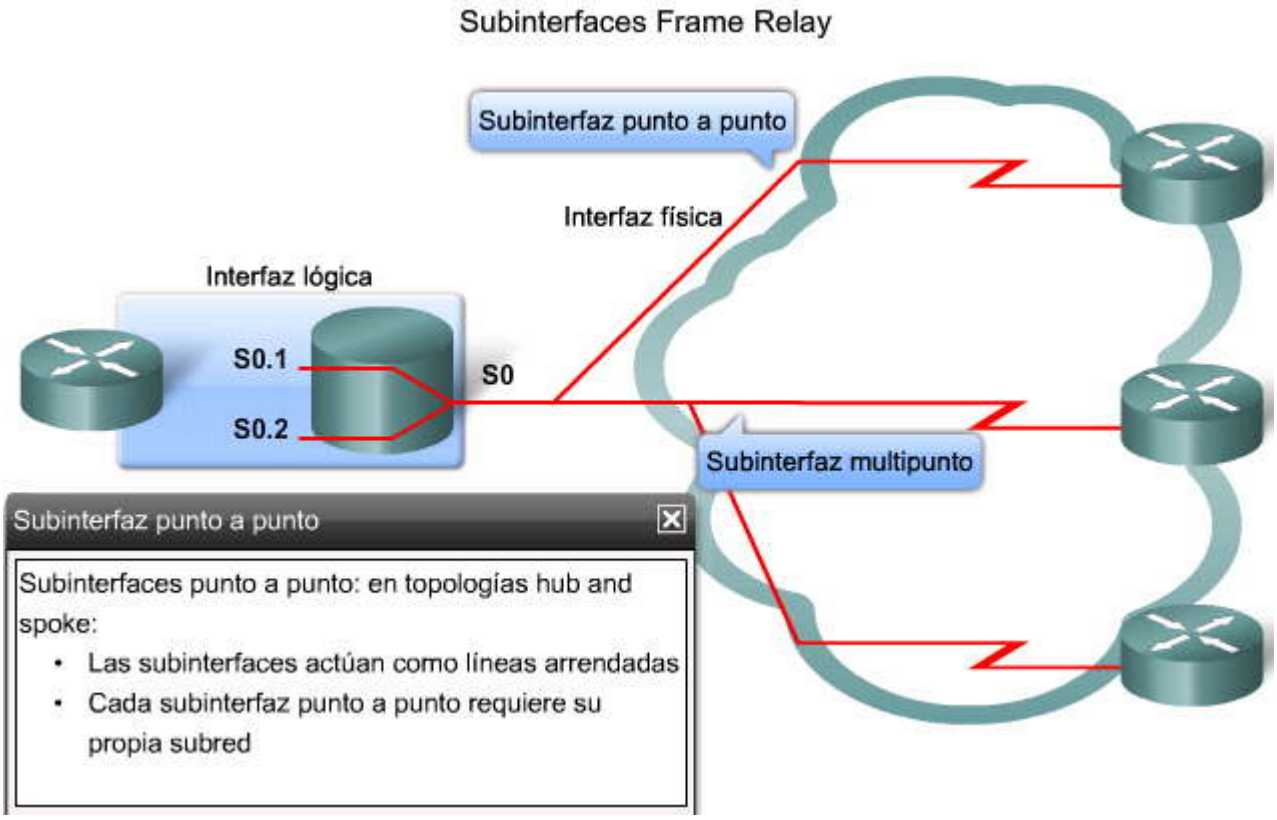
En entornos de enrutamiento con horizonte dividido, es posible reenviar las actualizaciones de enrutamiento recibidas en una subinterfaz a través de otra subinterfaz. En una configuración de subinterfaces, cada VC puede configurarse como conexión punto a punto. Esto permite que cada subinterfaz actúe de modo similar a una línea arrendada. Al utilizar una interfaz Frame Relay punto a punto, cada pareja de routers punto a punto se encuentra en su propia subred.

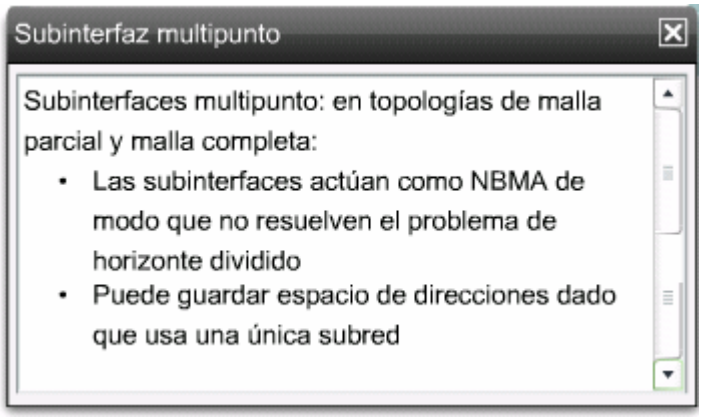
El comando **encapsulation frame-relay** está asignado a la interfaz física. Todos los demás aspectos de la configuración, tales como la dirección de capa de red y los DLCI se asignan a cada subinterfaz.

Puede usar configuraciones multipunto para conservar las direcciones. Puede resultar especialmente útil si no se usa la Máscara de subred de longitud variable (VLSM). Sin embargo, las configuraciones multipunto podrían funcionar mal, dadas las consideraciones de tráfico de broadcasts y del horizonte dividido. La opción de subinterfaz punto a punto se creó para evitar esos problemas.

Coloque el mouse sobre la subinterfaz punto a punto y la subinterfaz multipunto de la figura para conocer un resumen descriptivo.

La configuración de subinterfaces se explica y se practica en la siguiente sección.





3.3.2 Pago de Frame Relay

Terminología clave

Los proveedores de servicios crean redes Frame Relay mediante switches muy grandes y eficaces pero, como cliente, sus dispositivos sólo ven la interfaz del switch del proveedor de servicios. Los clientes suelen no estar expuestos a los trabajos internos de la red, que pueden crearse en función de tecnologías de muy alta velocidad, como T1, T3, SONET o ATM.

Desde la perspectiva de un cliente, Frame Relay es una interfaz y uno o más PVC. Los clientes simplemente compran los servicios de Frame Relay a un proveedor de servicios. No obstante, antes de pensar cómo pagar los servicios de Frame Relay, hay algunos términos y conceptos clave que debe conocer, según se ejemplifica en la figura.

- **Velocidad de acceso o velocidad de puerto**: desde la perspectiva del cliente, el proveedor de servicios proporciona una conexión serial o un enlace de acceso a la red Frame Relay a través de una línea arrendada.La velocidad de la línea es la velocidad de acceso o velocidad de puerto. La velocidad de acceso es la velocidad con la que sus circuitos de acceso se unen a la red Frame Relay. Comúnmente son 56 kbps, T1 (1.536 Mbps) o T1 fraccional (un múltiplo de 56 kbps o 64 kbps). Las velocidades de puerto se miden en el switch Frame Relay. No es posible enviar datos a velocidades superiores a la velocidad de puerto.
- **Velocidad de información suscrita (CIR)**: los clientes negocian la velocidad de información suscrita (CIR, Committed Information Rate) con proveedores de servicios para cada PVC. La CIR es la cantidad de datos que una red recibe del circuito de acceso. El proveedor de servicios garantiza que el cliente pueda enviar datos a la CIR. Todas las tramas recibidas a la CIR o por debajo de ella son aceptadas.

Una enorme ventaja de Frame Relay es que la capacidad de cualquier red que no se usa se pone a disposición o se comparte con todos los clientes, por lo general, sin cargos adicionales. Esto permite a los clientes usar "ráfagas" a través de sus CIR como beneficio adicional. Las ráfagas se explican en el siguiente tema.

Haga clic en el botón Ejemplo que se muestra en la figura.

En este ejemplo, aparte de los costos de cualquier CPE, el cliente paga por tres componentes de Frame Relay de la siguiente manera:

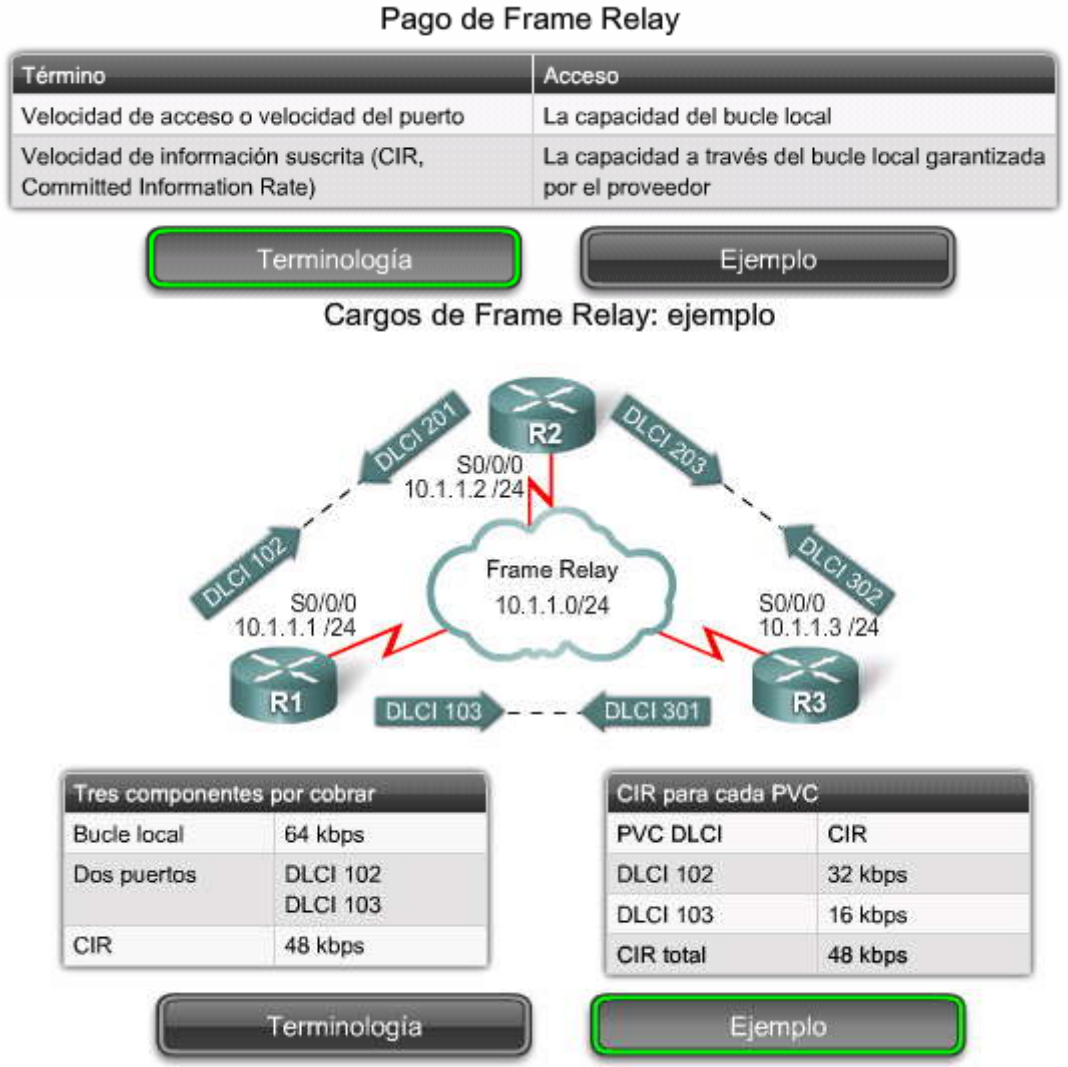
- Velocidad de acceso o de puerto: El costo de la línea de acceso de DTE a DCE (cliente a proveedor de servicios). Se aplican los cargos a esta línea en función de la velocidad de puerto que se ha negociado e instalado.
- PVC: este componente de costo está basado en los PVC. Una vez establecido un PVC, el costo adicional para aumentar la CIR suele ser pequeño y puede realizarse en pequeños incrementos (4 kbps).
- CIR: los clientes normalmente elijen una CIR inferior a la velocidad de puerto o acceso. Esto les permite aprovechar las ráfagas.

En el ejemplo, el cliente paga por lo siguiente:

- Una línea de acceso con una velocidad de 64 kbps que conecta su DCE al DCE del proveedor de servicios a través del puerto serial S0/0/0.
- Dos puertos virtuales, uno a 32 kbps y el otro a 16 kbps.
- Una CIR de 48 kbps en toda la red Frame Relay. Generalmente es una tarifa plana y no está relacionada con la distancia.

Sobresuscripción

A veces, los proveedores de servicios venden más capacidad de la que tienen, porque suponen que no todos demandan la capacidad a la que tienen derecho todo el tiempo. Esta sobresuscripción se asemeja a las aerolíneas que venden más pasajes de los que tienen porque prevén la posibilidad de que algunos de los clientes que hicieron reservas no se presenten. Dada la sobresuscripción, hay momentos en que la suma de las CIR de varios PVC a una ubicación determinada supera la velocidad de puerto o del canal de acceso. Esto puede provocar problemas de tráfico, como la congestión o la pérdida de tráfico.



Ráfagas

Una enorme ventaja de Frame Relay es que la capacidad de cualquier red que no se usa se pone a disposición o se comparte con todos los clientes, por lo general, sin cargos adicionales.

A través del ejemplo anterior, la figura muestra una velocidad de acceso en el puerto serial S0/0/0 del router R1 de 64 kbps. Esta velocidad es más alta que las CIR combinadas de los dos PVC. En circunstancias normales, los dos PVC no deben transmitir más de 32 kbps y 16 kbps, respectivamente. Siempre y cuando la cantidad de datos de los dos PVC que se envíen no excedan su CIR, deben transmitirse por la red.

Dado que los circuitos físicos de la red Frame Relay se comparten entre los suscriptores, puede haber momentos en que haya un exceso de ancho de banda disponible. Frame Relay puede permitir que los clientes accedan de forma dinámica a este ancho de banda adicional y usen "ráfagas" a través de sus CIR de forma gratuita.

Las ráfagas permiten que los dispositivos que necesitan temporalmente ancho de banda adicional lo pidanprestado, sin costos adicionales, a otros dispositivos que no lo usan. Por ejemplo, si PVC 102 transfiere un archivo grande, puede usar cualquiera de los 16 kbps no utilizados por PVC 103. Un dispositivo puede usar una ráfaga equivalente a la velocidad de acceso y suponer que los datos aún se transmitirán. La duración de una transmisión por ráfaga debe ser breve, menos de tres o cuatro segundos.

Se usan diversos términos para describir las velocidades de ráfagas, por ejemplo, velocidad de información de ráfaga suscrita (CBIR, Committed Burst Information Rate) y tamaño de ráfaga excesiva (BE, Excess Burst).

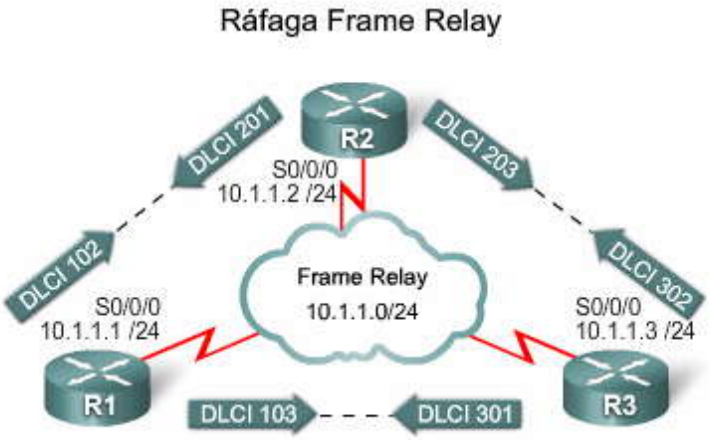
La CBIR es una velocidad negociada superior a la CIR que el cliente puede usar para transmitir durante una ráfaga breve. Permite que el tráfico se transmita por ráfagas a velocidades más altas, según el ancho de banda disponible de la red. No obstante, no puede exceder la velocidad de puerto del enlace. Un dispositivo puede transmitir por ráfagas equivalentes a la CBIR y suponer la correcta transmisión de los datos. La duración de una transmisión por ráfaga debe ser breve, menos de tres o cuatro segundos. Si persiste una larga ráfaga, se debe comprar una CIR más alta.

Por ejemplo, DLCI 102 tiene 32 kbps CIR, 16 kbps BE, y 48 kbps CBIR. Las tramas enviadas en este nivel están marcadas como elegible para descarte (DE, Discard Eligible) en el encabezado de la trama, lo que indica que pueden perderse si hay congestión o si no hay suficiente capacidad en la red. Las tramas ubicadas dentro de la CIR negociada no son susceptibles del descarte (DE = 0). Las tramas superiores a la CIR tienen el bit DE configurado en 1, lo que las marca como susceptibles del descarte en el caso de una congestión en la red.

BE es el término utilizado para describir el ancho de banda disponible por encima de la CBIR, hasta la velocidad de acceso del enlace. A diferencia de la CBIR, no se negocia. Las tramas pueden transmitirse en este nivel, pero hay más posibilidades de perderlas.

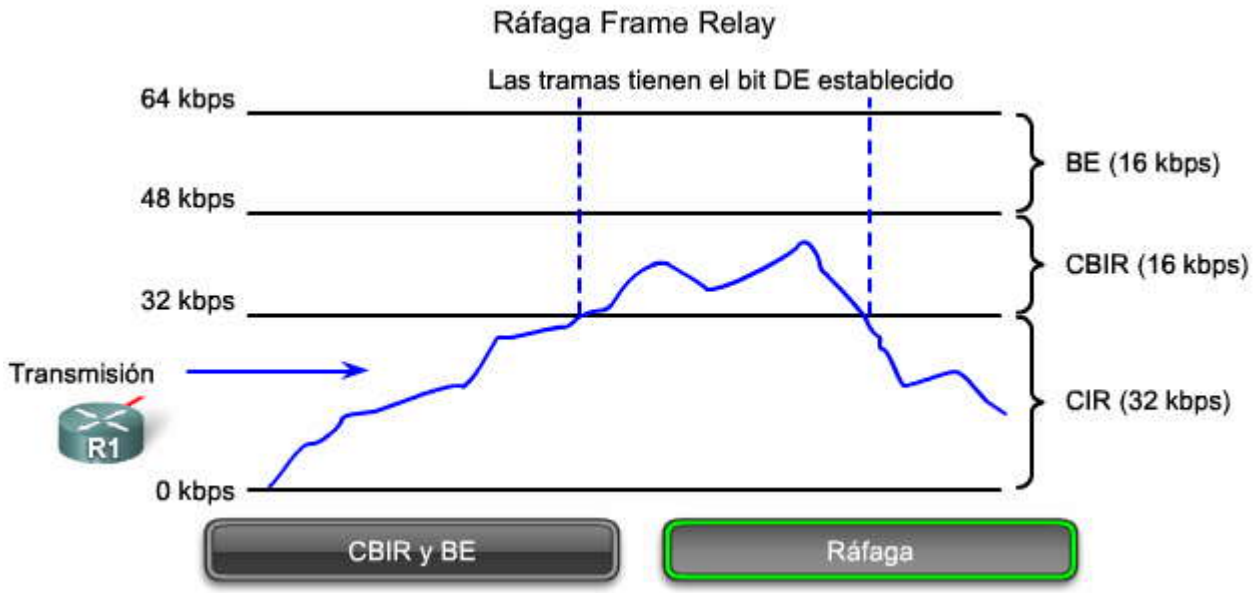
Haga clic en el botón Ráfaga que se muestra en la figura.

La figura ejemplifica la relación existente entre los diferentes términos de ráfagas.



PVC DCLI	CIR (normal)	CBIR (ejemplo)	BE
DCLI 102	32 kbps	48 kbps	16 kbps
DCLI 103	16 kbps	0 kbps	48 kbps
	Todas las tramas se reenvían	Las tramas se reenvían pero con la marca DE	Habrá más posibilidades de que las tramas se descarten

CBIR y BE | Ráfaga



3.3.3 Control de flujo de Frame Relay

Página 1:
Frame Relay reduce la sobrecarga de red mediante la implementación de mecanismos simples de congestión-notificación en lugar de control de flujo explícito por VC. Estos mecanismos de congestión-notificación son la Notificación explícita de congestión hacia adelante (FECN, Forward Explicit Congestion Notification) y la notificación explícita de congestión hacia atrás (BECN, Backward Explicit Congestion Notification).

Para comprender mejor los mecanismos, se presenta el gráfico que muestra la estructura de la trama Frame Relay para su revisión. FECN y BECN están controlados por un único bit que se encuentra en el encabezado de la trama. Permiten que el router sepa que hay congestión y que debe detener la transmisión hasta revertir esta situación. BECN es una notificación directa. FECN es una notificación indirecta.

El encabezado de la trama también incluye un bit Elegible para descarte (DE), que identifica tráfico menos importante que puede perderse durante períodos de congestión. Los dispositivos DTE pueden establecer el valor del bit DE en 1, para indicar que la trama tiene menor importancia que otras tramas. Cuando la red se congestiona, los dispositivos DCE descartan las tramas con el bit DE configurado en 1, antes de descartar aquellas sin esta configuración. De esta forma se reducen las posibilidades de que se pierdan datos críticos durante períodos de congestión.

En períodos de congestión, el switch Frame Relay del proveedor aplica las siguientes reglas lógicas a cada trama entrante en función de si se excede la CIR:

- si la trama entrante no excede la CIBR, la trama se transmite.
- Si una trama entrante excede la CIBR, se marca como DE.
- Si una trama entrante excede la CIBR además de la BE, se descarta.

Haga clic en el botón Cola de la figura y en Reproducir, que se muestra en la animación.

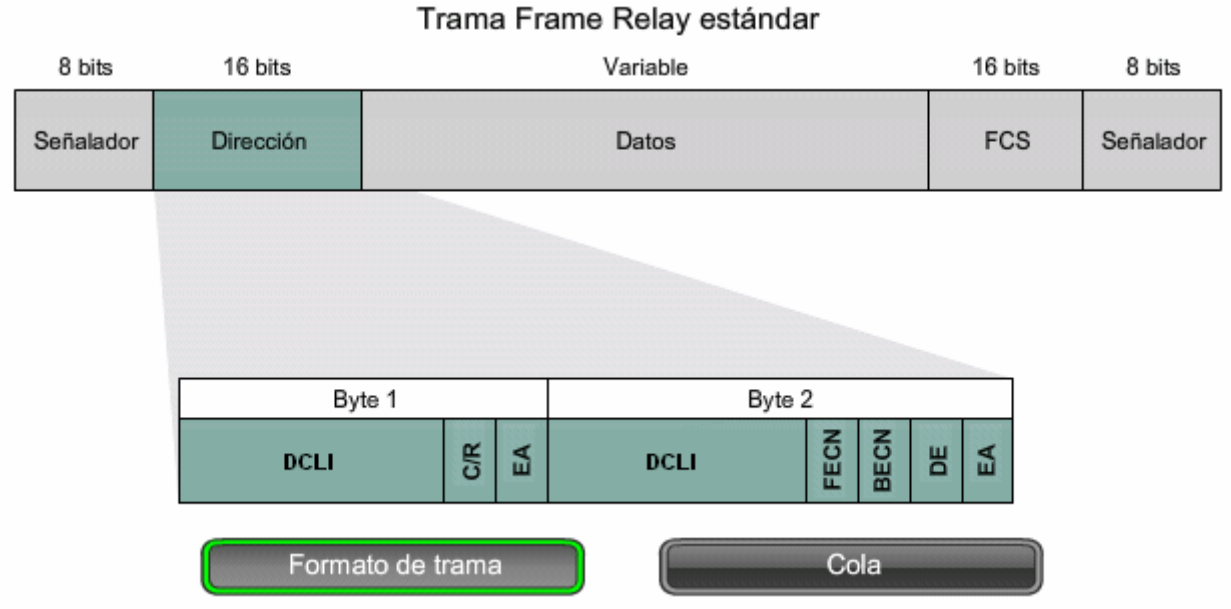
Las tramas que entran a un switch se ponen en cola en el búfer antes de su envío. Como en cualquier sistema de colas, es posible que haya una acumulación excesiva de tramas en el switch. Eso provoca retardos. Los retardos acarrean retransmisiones innecesarias que tienen lugar cuando los protocolos de nivel superior no reciben acuses de recibo dentro de un lapso determinado. En casos graves, esto puede provocar un descenso importante en la velocidad de la red. Para evitar este problema, Frame Relay incluye una función de control de flujo.

La figura muestra un switch con una cola que se completa. Para reducir el flujo de tramas a la cola, el switch notifica el problema a DTE mediante los bits de la notificación explícita de la congestión en el campo de dirección de la trama.

- El bit de FECN, indicado por la letra "F" en la figura, está establecido en cada trama que el switch *recibe* en el enlace congestionado.
- El bit de BECN, indicado por la letra "B" en la figura, está establecido en cada trama que el switch *coloca* en el enlace congestionado.

Se espera que los DTE que reciben tramas con el grupo de bits ECN establecidos intenten reducir el flujo de tramas hasta que la congestión desaparezca.

Si la congestión tiene lugar en un enlace troncal interno, los DTE pueden recibir una notificación aún cuando ellos no sean la causa.

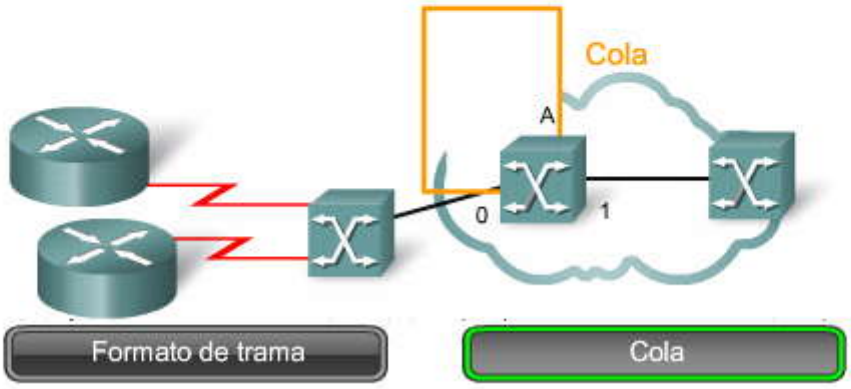


Control de ancho de banda FR: Cola

Mientras que el switch A coloca una trama grande en la interfaz 1, otras tramas para esta interfaz se ponen en cola.

Se advierte a los dispositivos de recepción de la existencia de la cola mediante el establecimiento del bit FECN

Se advierte a los dispositivos ascendentes de la existencia de la cola mediante el establecimiento del bit BECN, aunque es posible que no hayan contribuido a la congestión



Solución de problemas relacionados a la posibilidad de conexión

Las redes Frame Relay generalmente se construyen en una topología _____, lo que causa problemas relacionados a la posibilidad de conexión.	hub-and-spoke
El horizonte dividido es una técnica que se usa para evitar _____ en redes que usan protocolos de vector distancia.	routing loops
La solución de los problemas relacionados con la posibilidad de conexión requiere el uso de una topología _____, que es costosa, o el uso de _____.	malla completa subinterfaces
En las configuraciones _____, se utiliza una sola subinterfaz para establecer una conexión de PVC en relación con otra interfaz física o subinterfaz en un router remoto.	punto a punto
En las configuraciones _____, se utiliza una sola subinterfaz para establecer varias conexiones de PVC a varias interfaces físicas o subinterfaces en routers remotos.	multipunto
El comando _____ se configura en la interfaz física. Todos los demás aspectos de la configuración, tales como la dirección de capa de red y los DLCI se configuran en la subinterfaz.	encapsulation frame-relay

Control de flujo y ancho de banda de Frame Relay

Definición	Término
El número máximo de bits que la red garantiza entregar en circunstancias normales.	Ráfaga suscrita (Bc)
La diferencia entre la velocidad garantizada y la velocidad máxima permitida por el proveedor de servicios.	Velocidad de información excesiva (EIR, Excess Information Rate)
Cuando un switch Frame Relay experimenta congestión, define estos bits en cada trama que recibe.	Notificación explícita de la congestión (ECN, Explicit Congestion Notification)
Velocidad a la que el proveedor de servicios acuerda aceptar bits en el VC.	Velocidad de información suscrita (CIR, Committed Information Rate)
Es una notificación directa que indica congestión.	BECN
Es una notificación indirecta que indica que hay congestión.	FECN
Este bit se establece si la trama recibida cambia el contador por encima de la ráfaga suscrita.	Elegible para descarte (DE, Discard Eligibility)

3.4 Configuración avanzada de Frame Relay

3.4.1 Configuración de las subinterfaces Frame Relay

Recuerde que el uso de subinterfaces Frame Relay garantiza que se trata a una sola interfaz física como múltiples interfaces virtuales para sobrellevar las reglas de horizonte dividido. Los paquetes recibidos en una interfaz virtual pueden enviarse a otra interfaz virtual, incluso si se configuran en la misma interfaz física.

Las subinterfaces resuelven las limitaciones de las redes Frame Relay al proporcionar una forma de subdividir una red Frame Relay con mallas parciales en numerosas subredes más pequeñas, con mallas completas (o punto a punto). Se asigna a cada subred su propio número de red y aparece ante los protocolos como si pudiera alcanzarse a través de una interfaz separada. Las subinterfaces punto a punto pueden no tener números para usar con IP, lo que reduce la carga de direccionamiento que podría generarse de otra forma.

Para crear una subinterfaz, use el comando **interface serial**. Especifique el número de puerto, seguido de un punto (.), y luego del número de la subinterfaz. Para solucionar problemas con más facilidad, use el DLCI como número de subinterfaz. También debe especificar si la interfaz es punto a punto o multipunto mediante la palabra clave **multipoint** o **point-to-point**, dado que no existe un valor predeterminado. Estas palabras clave se definen en la figura.

El siguiente comando crea una subinterfaz punto a punto para PVC 103 a R3: R1(config-if)#**interface serial 0/0/0.103 point-to-point**.

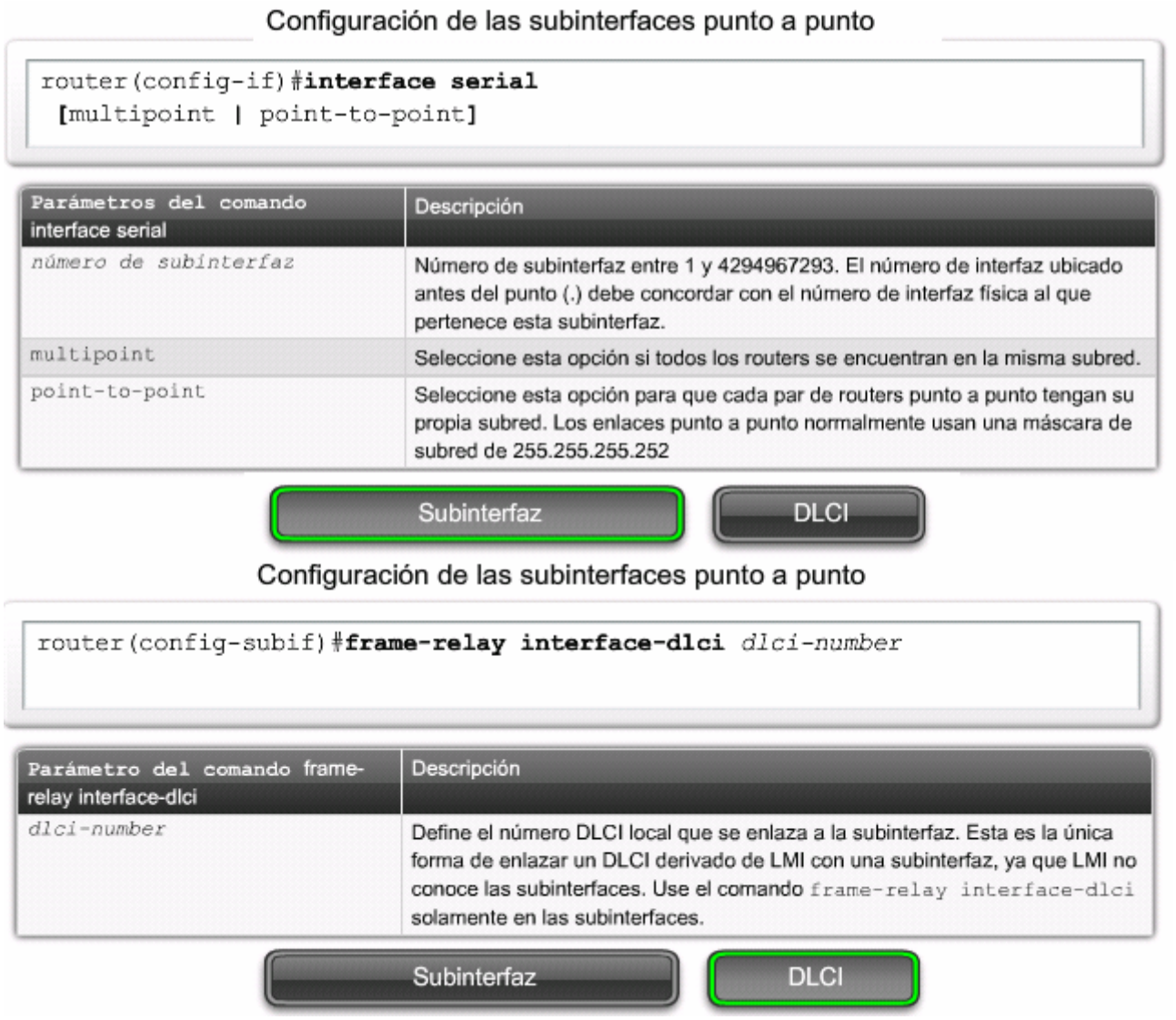
Haga clic en el botón DLCI que se muestra en la figura.

Si la subinterfaz se configura como punto a punto, se debe configurar también el DLCI local para la subinterfaz, para distinguirla de la interfaz física. También se requiere el DLCI para las subinterfaces multipunto en las que se habilita el ARP inverso. No es necesario para las subinterfaces multipunto configuradas con mapas de rutas estáticas.

El proveedor de servicios Frame Relay asigna los números DLCI. Estos números van del 16 al 992 y, por lo general, sólo tienen importancia local. El rango varía en función de la LMI utilizada.

El comando **frame-relay interface-dlci** configura el DLCI local en la subinterfaz. Por ejemplo: R1(config-subif)#**frame-relay interface-dlci 103**.

Nota: Desafortunadamente, la modificación de la configuración de una subinterfaz Frame Relay existente puede no proporcionar el resultado previsto. En estas situaciones, posiblemente sea necesario guardar la configuración y volver a cargar el router.



Configuración de ejemplo de subinterfaces

En la figura, R1 tiene dos subinterfaces punto a punto. La subinterfaz s0/0.0.102 se conecta con R2, y la subinterfaz s0/0/0.103 se conecta con R3. Cada subinterfaz está en una subred diferente.

Para configurar las subinterfaces en una interfaz física, siga estos pasos:

Paso 1. Quitar cualquier dirección de capa de red asignada a la interfaz física. Si la interfaz física tiene una dirección, las subinterfaces locales no reciben las tramas.

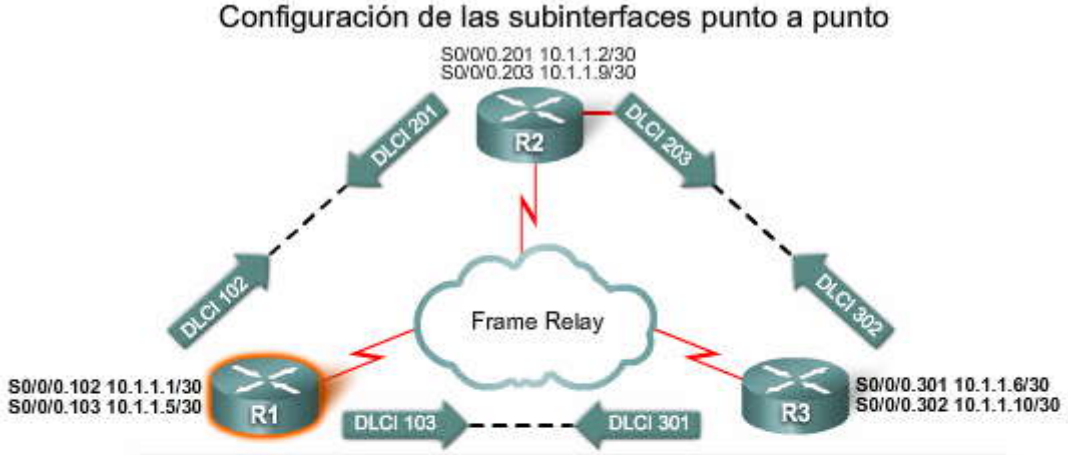
Paso 2. Configurar la encapsulación Frame Relay en la interfaz física mediante el comando **encapsulation frame-relay**.

Paso 3. Para cada uno de los PVC definidos, crear una subinterfaz lógica. Especifique el número de puerto, seguido de un punto (.), y luego del número de la subinterfaz. Para solucionar problemas con más facilidad, se sugiere que el número de la subinterfaz coincida con el número de DLCI.

Paso 4. Configurar una dirección IP para la interfaz y el ancho de banda.

En este punto, configuraremos el DLCI. Recuerde que el proveedor de servicios de Frame Relay asigna los números de DLCI.

Paso 5. Configurar el DLCI local en la subinterfaz mediante el comando **frame-relay interface-dlci**.




```
interface s0/0/0
 no ip address
 encapsulation frame-relay
 no shut
exit

interface s0/0/0.102 point-to-point
 ip address 10.1.1.1 255.255.255.252
 bandwidth 64
 frame-relay interface-dlci 102
exit

interface s0/0/0.103 point-to-point
 ip address 10.1.1.5 255.255.255.252
 bandwidth 64
 frame-relay interface-dlci 103
end
```

3.4.2 Verificación del funcionamiento de Frame Relay

Frame Relay suele ser un servicio muy confiable. De todas formas, hay ocasiones en las que la red funciona a niveles inferiores a los previstos y se necesita solucionar problemas. Por ejemplo, los usuarios posiblemente notifiquen conexiones lentas e intermitentes en el circuito. Los circuitos pueden desactivarse. Independientemente del motivo, las interrupciones de la red son muy costosas en relación con la pérdida de la productividad. Una práctica recomendada es verificar su configuración antes de que surjan inconvenientes.

En relación con este tema, sigue un procedimiento de verificación para garantizar el correcto funcionamiento, antes de iniciar su configuración en una red activa.

Verificar interfaces Frame Relay

Después de configurar un PVC Frame Relay y al solucionar un problema, verifique que Frame Relay funcione correctamente en esa interfaz mediante el comando **show interfaces**.

Recuerde que, con Frame Relay, el router se considera normalmente un dispositivo DTE. Sin embargo, los routers Cisco pueden configurarse como switches Frame Relay. En tales casos, el router se convierte en dispositivo DCE cuando se configura como switch Frame Relay.

El comando **show interfaces** muestra cómo se configura la encapsulación, junto con valiosa información de estado de la Capa 1 y 2, que incluye:

- Tipo de LMI
- DLCI de la LMI
- Tipo de DTE/DCE Frame Relay

El primer paso consiste siempre en confirmar que las interfaces estén bien configuradas. La figura muestra un ejemplo de resultado del comando **show interfaces**. Algunos de los datos que puede ver son los detalles sobre la encapsulación, el DLCI en la interfaz serial configurada por Frame Relay y el DLCI utilizado para la LMI. Debe confirmar que estos valores sean los valores previstos. De lo contrario, posiblemente deba efectuar cambios.

Haga clic en el botón LMI que se muestra en la figura para verificar el rendimiento de la LMI.

El siguiente paso consiste en observar algunas estadísticas de LMI mediante el comando **show frame-relay lmi**. En el resultado, observe si existen elementos "no válidos" diferentes a cero. Esto ayuda a aislar el problema y reducirlo a un problema de comunicaciones de Frame Relay entre el switch de la empresa de comunicaciones y su router.

La figura muestra un ejemplo de resultado que indica la cantidad de mensajes de estado intercambiados entre el router local y el switch Frame Relay local.

Ahora observe las estadísticas de la interfaz.

Haga clic en el botón Estado de PVC que se muestra en la figura para verificar el estado del PVC.

Use el comando **show frame-relay pvc** [**interface***interface*] [**dlci**] para ver las estadísticas del PVC y del tráfico. Este comando también resulta útil para ver la cantidad de paquetes BECN y FECN que el router recibe. El estado del PVC puede ser activo, inactivo o eliminado.

El comando **show frame-relay pvc** muestra el estado de todos los PVC configurados en el router. También puede especificar un PVC en particular. Haga clic en Estado de PVC de la figura para ver un ejemplo de resultado del comando **show frame-relay pvc 102**.

Una vez que haya recopilado todas las estadísticas, use el comando **clear counters** para restaurar los contadores de estadísticas. Espere 5 ó 10 minutos después de restablecer los contadores para volver a ejecutar los comandos **show**. Observe si hay errores adicionales. Si necesita comunicarse con la empresa de comunicaciones, estas estadísticas ayudan en la resolución de problemas.

Una tarea final consiste en confirmar si el comando **frame-relay inverse-arp** resolvió una dirección IP remota a un DLCI local. Use el comando **show frame-relay map** para mostrar las entradas de las asignaciones actuales y la información sobre las conexiones.

Haga clic en el botón ARP inverso que se muestra en la figura.

El resultado muestra la siguiente información:

- 10.140.1.1 es la dirección IP de un router remoto, que se aprende de forma dinámica a través de un proceso de ARP inverso.
- 100 es el valor decimal del número DLCI local.
- 0x64 es la conversión hexadecimal del número DLCI, 0x64 = 100 decimal.
- 0x1840 es el valor tal como se mostraría en el cable, debido a la forma en la que los bits de DLCI se reparten en el campo de dirección de la trama Frame Relay.
- La capacidad broadcast/multicast está habilitada en el PVC.
- El estado del PVC es activo.

Para borrar las asignaciones de Frame Relay creadas de forma dinámica mediante el ARP inverso, use el comando **clear frame-relay-inarp**. **Haga clic en el botón Borrar asignaciones** para ver un ejemplo de este paso.

Verificación del funcionamiento de Frame Relay: Observar las interfaces

```
R1#show interface serial 0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  LMI enq sent  59, LMI stat recvd 59, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 0, LMI stat sent  0, LMI upd sent  0
  LMI DLCI 1023  LMI type is CISCO  frame relay DTE
  FR SVC disabled, LAPF state down
  Broadcast queue 0/64, broadcasts sent/dropped 11/0, interface broadcasts 0
  Last input 00:00:05, output 00:00:05, output hang never
  Last clearing of "show interface" counters 00:09:55
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     67 packets input, 2367 bytes, 0 no buffer
```

Interfaces | LMI | Estado de PVC | ARP inverso | Borrar asignaciones

Verificación del funcionamiento de Frame Relay: Estadísticas de LMI

```
R1#show frame-relay lmi
LMI Statistics for interface Serial0/0/1 (Frame Relay DTE) LMI TYPE = CISCO
  Invalid Unnumbered info 0          Invalid Prot Disc 0
  Invalid dummy Call Ref 0           Invalid Msg Type 0
  Invalid Status Message 0           Invalid Lock Shift 0
  Invalid Information ID 0           Invalid Report IE Len 0
  Invalid Report Request 0           Invalid Keep IE Len 0
  Num Status Enq. Sent 76            Num Status msgs Rcvd 76
  Num Update Status Rcvd 0           Num Status Timeouts 0
  Last Full Status Req 00:00:48      Last Full Status Rcvd 00:00:48
------------------------------------------------------------------------
R1#show frame-relay lmi
LMI Statistics for interface Serial0/0/1 (Frame Relay DTE) LMI TYPE = CISCO
  Invalid Unnumbered info 0          Invalid Prot Disc 0
  Invalid dummy Call Ref 0           Invalid Msg Type 0
  Invalid Status Message 0           Invalid Lock Shift 0
  Invalid Information ID 0           Invalid Report IE Len 0
  Invalid Report Request 0           Invalid Keep IE Len 0
  Num Status Enq. Sent 78            Num Status msgs Rcvd 78
  Num Update Status Rcvd 0           Num Status Timeouts 0
  Last Full Status Req 00:00:02      Last Full Status Rcvd 00:00:02
```

Interfaces | LMI | Estado de PVC | ARP inverso | Borrar asignaciones

Verificación del funcionamiento de Frame Relay: Estado de PVC

```
R1#show frame-relay pvc 102
PVC Statistics for interface Serial0/0/1 (Frame Relay DTE)
DLCI = 102, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/1.102
  input pkts 12             output pkts 20           in bytes 2816
  out bytes 5455            dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                 out bytes dropped 0
  in FECN pkts 0            in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0           in DE pkts 0             out DE pkts 0
  out bcast pkts 15         out bcast bytes 4935
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 00:13:27, last time pvc status changed 00:07:47
------------------------------------------------------------------
R2#show frame-relay pvc 201
PVC Statistics for interface Serial0/0/1 (Frame Relay DTE)
DLCI = 201, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/1.201
  input pkts 11             output pkts 8            in bytes 3619
  out bytes 2624            dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                 out bytes dropped 0
  in FECN pkts 0            in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0           in DE pkts 0             out DE pkts 0
  out bcast pkts 8          out bcast bytes 2624
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
```

Interfaces | LMI | Estado de PVC | ARP inverso | Borrar asignaciones

Verificación del funcionamiento de Frame Relay: Verificar ARP inverso

```
R1#sh frame-relay map
Serial0/0/0 (up): ip 10.140.1.1 dlci 100(0x64,0x1840), dynamic, broadcast,
              CISCO, status defined, active
```

ARP inverso

Verificación del funcionamiento de Frame Relay: Borrar asignaciones de Frame Relay

```
R1#clear frame-relay inarp
R1#show frame-relay map
Serial0/0/1.102 (up): point-to-point dlci, dlci 102(0x66,0x1860), broadcast
          status defined, active
```

```
R2#clear frame-relay inarp
R2#show frame-relay map
Serial0/0/1.201 (up): point-to-point dlci, dlci 201(0xC9,0x3090), broadcast
          status defined, active
```

Borrar asignaciones

3.4.3 Resolución de problemas de configuración de Frame Relay

Si el procedimiento de verificación indica que su configuración de Frame Relay no funciona correctamente, debe ejecutar la resolución de problemas de configuración.

Use el comando **debug frame-relay lmi** para determinar si el router y el switch Frame Relay envían y reciben paquetes LMI correctamente.

Observe la figura y analice el resultado de un intercambio de LMI.

- "out" (salida) se refiere a los mensajes de estado de LMI enviados por el router.
- "in" (entrada) se refiere a los mensajes recibidos del switch Frame Relay.
- Un mensaje de estado de LMI completo es de "tipo 0" (no se muestra en la figura).
- Un intercambio de LMI es de "tipo 1".
- "dlci 100, estado 0x2" significa que el estado del DLCI 100 es activo.

Cuando se efectúa una solicitud de ARP inverso, el router actualiza su tabla de asignación con tres posibles estados de conexión de LMI. Estos estados son activo, inactivo y eliminado.

- Los estados ACTIVO indican un circuito de extremo a extremo (DTE a DTE) exitoso.
- El estado INACTIVO indica una conexión con éxito con el switch (DTE a DCE) sin un DTE detectada en el otro extremo del PVC. Esto puede deberse a una configuración residual o incorrecta en el switch.
- El estado ELIMINADO indica que el DTE se configura para un DLCI que el switch no reconoce como válido para esa interfaz.

Los valores posibles del campo de estado son los siguientes.

- 0x0: Significa que el switch tiene el DLCI programado pero por alguna razón no se puede usar. Es posible que esto ocurra porque el extremo opuesto del PVC está desactivado.
- 0x2: significa que el switch Frame Relay tiene el DLCI y que todo está en funcionamiento.
- 0x4: significa que el switch Frame Relay no tiene este DLCI programado para el router, pero que estuvo programado en algún momento en el pasado. Esto puede deberse a una reversión del DLCI en el router, o que el proveedor de servicios haya eliminado el PVC de la nube Frame Relay.

Resolución de problemas del funcionamiento de Frame Relay

```
R1#debug frame-relay lmi
Frame Relay LMI debugging is on
Displaying all Frame Relay LMI data
R1#
*Sep 12 00:09:35.425: Serial0/0/1(out): StEnq, myseq 110, yourseen 109, DTE up
*Sep 12 00:09:35.425: datagramstart = 0x3F4055D4, datagramsize = 13
*Sep 12 00:09:35.425: FR encap = 0xFCF10309
*Sep 12 00:09:35.425: 00 75 01 01 01 03 02 6E 6D
*Sep 12 00:09:35.425:
*Sep 12 00:09:35.425: Serial0/0/1(in): Status, myseq 110, pak size 13
*Sep 12 00:09:35.425: RT IE 1, length 1, type 1
*Sep 12 00:09:35.425: KA IE 3, length 2, yourseq 110, myseq 110
R1#
*Sep 12 00:09:45.425: Serial0/0/1(out): StEnq, myseq 111, yourseen 110, DTE up
*Sep 12 00:09:45.425: datagramstart = 0x3F4050D4, datagramsize = 13
*Sep 12 00:09:45.425: FR encap = 0xFCF10309
*Sep 12 00:09:45.425: 00 75 01 01 01 03 02 6F 6E
*Sep 12 00:09:45.425:
*Sep 12 00:09:45.425: Serial0/0/1(in): Status, myseq 111, pak size 13
*Sep 12 00:09:45.425: RT IE 1, length 1, type 1
*Sep 12 00:09:45.425: KA IE 3, length 2, yourseq 111, myseq 111
R1#undebug all
All possible debugging has been turned off
R1#
-----------------------------------------
R2#debug frame-relay lmi
Frame Relay LMI debugging is on
```

```
R2#debug frame-relay lmi
Frame Relay LMI debugging is on
Displaying all Frame Relay LMI data
R2#
*Sep 12 00:07:12.773: Serial0/0/1(out): StEnq, myseq 82, yourseen 81, DTE up
*Sep 12 00:07:12.773: datagramstart = 0x3F401B14, datagramsize = 13
*Sep 12 00:07:12.773: FR encap = 0xFCF10309
*Sep 12 00:07:12.773: 00 75 01 01 01 03 02 52 51
*Sep 12 00:07:12.773:
*Sep 12 00:07:12.773: Serial0/0/1(in): Status, myseq 82, pak size 13
*Sep 12 00:07:12.773: RT IE 1, length 1, type 1
*Sep 12 00:07:12.773: KA IE 3, length 2, yourseq 82, myseq 82
R2#
*Sep 12 00:07:22.773: Serial0/0/1(out): StEnq, myseq 83, yourseen 82, DTE up
*Sep 12 00:07:22.773: datagramstart = 0x3F6AEFD4, datagramsize = 13
*Sep 12 00:07:22.773: FR encap = 0xFCF10309
*Sep 12 00:07:22.773: 00 75 01 01 01 03 02 53 52
*Sep 12 00:07:22.773:
*Sep 12 00:07:22.773: Serial0/0/1(in): Status, myseq 83, pak size 13
*Sep 12 00:07:22.773: RT IE 1, length 1, type 1
*Sep 12 00:07:22.773: KA IE 3, length 2, yourseq 83, myseq 83
R2#undebug all
All possible debugging has been turned off
R2#
```

3.5 Prácticas de laboratorio del capítulo

3.6 Resumen

3.6.1 Resumen del capítulo

Página 1:

Frame Relay proporciona más ancho de banda, fiabilidad y resistencia a las fallas que las líneas privadas o arrendadas. Frame Relay ha reducido los costos de red a través del uso de menos equipos, menos complejidad y una implementación más fácil. Por estos motivos, Frame Relay se ha convertido en la tecnología WAN más utilizada del mundo.

Una conexión Frame Relay entre un dispositivo DTE del extremo de la LAN y un dispositivo DCE ubicado en el extremo de la portadora tiene un componente de capa de enlace y un componente de capa física. Frame Relay toma los paquetes de datos y los encapsula en una trama de Frame Relay y, a continuación, transmite la trama a la capa física para su entrega en el cable. La conexión a través de la red de la portadora es un VC identificado por un DLCI. Se pueden multiplexar varios VC mediante un FRAD. Las redes Frame Relay generalmente usan una topología de malla parcial optimizada para los requisitos de flujo de datos de la base de clientes de la empresa de comunicaciones.

Frame Relay usa el ARP inverso para asignar DCLI a las direcciones IP de las ubicaciones remotas. La asignación dinámica de direcciones depende del ARP inverso para resolver una dirección de protocolo de red de próximo salto a un valor DLCI local. El router Frame Relay envía solicitudes de ARP inverso en su PVC para descubrir la dirección del protocolo del dispositivo remoto conectado a la red Frame Relay. Los routers DTE Frame Relay usan la LMI para proporcionar información de estado sobre su conexión con el switch DCE Frame Relay. Las extensiones LMI proporcionan información de internetworking adicional.

Las primeras dos tareas para configurar Frame Relay en un router Cisco consisten en habilitar la encapsulación Frame Relay en la interfaz y, luego, configurar la asignación estática o dinámica. Después de esto, hay numerosas tareas opcionales que pueden efectuarse según se requieran, incluida la configuración de la LMI, los VC, la conformación del tráfico y la personalización de Frame Relay en la red. La supervisión de las conexiones Frame Relay existentes es la tarea final.

La configuración Frame Relay debe considerar el problema de horizonte dividido que surge al converger varios VC en una única interfaz física. Frame Relay puede partir una interfaz física en varias interfaces virtuales denominadas subinterfaces. También se explicó y se practicó la configuración de subinterfaces.

La configuración de Frame Relay se ve afectada por la forma en la que los proveedores de servicios aplican cargos por conexiones que usan unidades de velocidades de acceso y velocidades de información suscrita (CIR). Una de las ventajas de estos esquemas de cargos es que la capacidad de red no utilizada está disponible o se comparte con todos los clientes, por lo general, sin costos adicionales. Esto les permite a los usuarios usar ráfagas de tráfico durante breves períodos.

La configuración del control de flujo en una red Frame Relay también se ve afectada por los esquemas de cargos del proveedor de servicios. Puede configurar la cola y la forma del tráfico de acuerdo con la CIR. Se pueden configurar DTE para controlar la congestión en la red mediante la adición de bits BECN y FECN a las direcciones de la trama. También se pueden configurar DTE para establecer un bit de elegible para descarte que indique que la trama puede descartarse en preferencia a otras tramas en el caso de una congestión. Las tramas que se envían en exceso de la CIR se marcan como "elegibles para descarte" (DE), lo que significa que pueden perderse en el caso de congestión dentro de la red Frame Relay.

Finalmente, una vez configurado Frame Relay, aprendió a verificar y a solucionar los problemas de las conexiones.

CAPITULO IV – “Seguridad de la red ”

4.0 Introducción del capítulo

4.0.1 Introducción del capítulo

La seguridad se ha convertido en un aspecto primordial de la implementación y la administración de red. El desafío general de la seguridad es encontrar un equilibrio entre dos requisitos importantes: la necesidad de abrir redes para respaldar las oportunidades comerciales en evolución y la necesidad de proteger la información comercial privada, personal y estratégica.

La aplicación de una política de seguridad eficaz es el paso más importante que puede dar una organización para proteger su red. Brinda pautas acerca de las actividades que deben llevarse a cabo y los recursos que deben utilizarse para proporcionar seguridad a la red de una organización.

En este capítulo no se analiza la seguridad a nivel de la Capa 2. Para obtener información acerca de las medidas de seguridad de la LAN de Capa 2, consulte el curso Exploration: Conmutación y conexión inalámbrica.

En este capítulo, aprenderá a:

- Identificar amenazas de seguridad en redes empresariales
- Describir métodos para mitigar amenazas de seguridad en redes empresariales
- Configurar la seguridad básica del router
- Deshabilitar servicios e interfaces de routers no utilizados
- Utilizar la característica de bloqueo en un paso de SDM de Cisco
- Administrar los archivos e imágenes de software con el Sistema de archivos integrados (IFS, Integrated File System) del IOS de Cisco

4.1 Introducción a la seguridad de la red

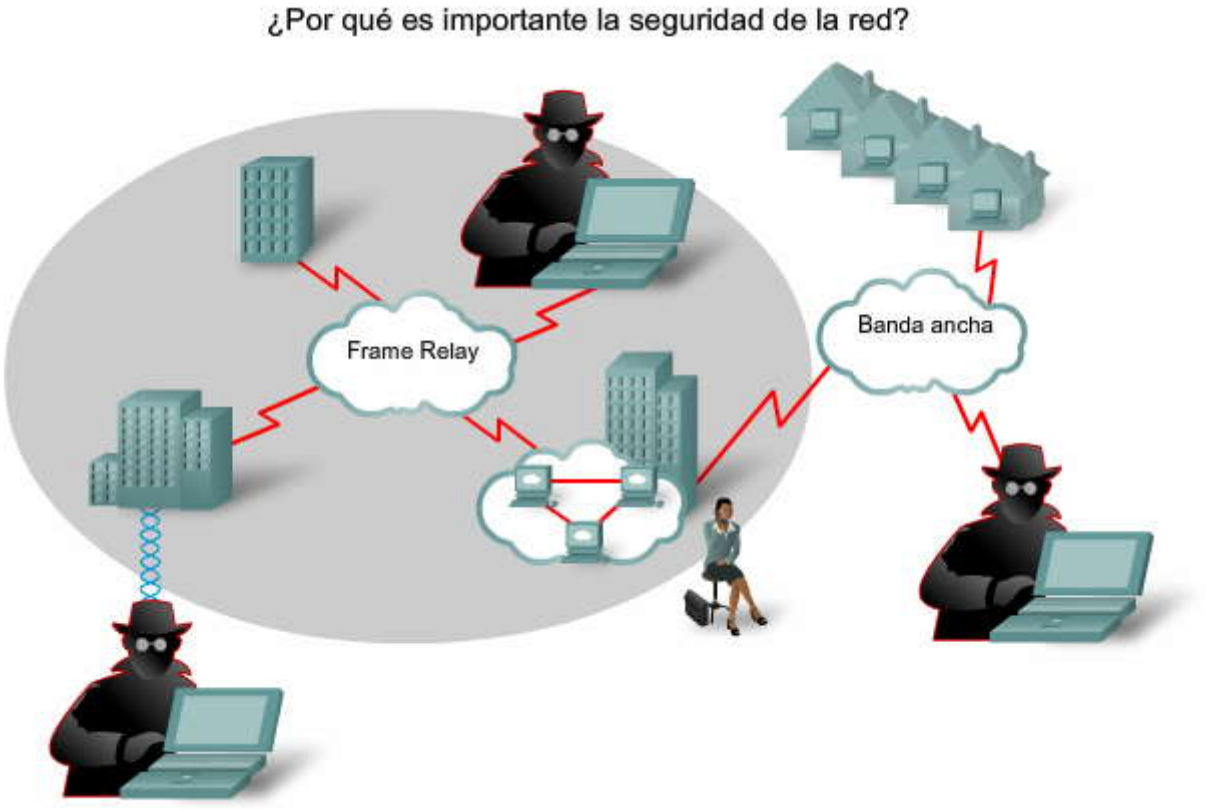
4.1.1 ¿Por qué es importante la seguridad de la red?

¿Por qué es importante la seguridad de la red?

En muy poco tiempo, las redes informáticas crecieron en tamaño y en importancia. Si la seguridad de la red se encuentra afectada, podría tener consecuencias graves, como la pérdida de privacidad, el robo de información e, incluso, responsabilidad legal. Para que esta situación constituya un desafío aun mayor, los tipos de amenazas potenciales a la seguridad de la red se encuentran siempre en evolución.

A medida que el comercio electrónico y las aplicaciones de Internet siguen creciendo, es muy difícil encontrar el equilibrio entre estar aislado y abierto. Además, el aumento del comercio móvil y de las redes inalámbricas exige soluciones de seguridad perfectamente integradas, más transparentes y más flexibles.

En este capítulo, se realiza un recorrido relámpago por el mundo de la seguridad de la red. Aprenderá acerca de los distintos tipos de amenazas, el desarrollo de políticas de seguridad de la organización, técnicas de alivio y herramientas del software IOS de Cisco para ayudar a proteger las redes. El capítulo termina con un vistazo de la administración de imágenes del software IOS de Cisco. Si bien esto quizás no parezca un problema de seguridad, las imágenes y configuraciones del software IOS de Cisco se pueden eliminar. Los dispositivos comprometidos de esta manera representan riesgos para la seguridad.



Las redes actuales deben equilibrar la accesibilidad a los recursos de red con la protección contra robo de datos sensibles.

La creciente amenaza a la seguridad

Con los años, las herramientas y los métodos de ataque a las redes han evolucionado. Como se observa en la figura, en 1985 los agresores debían tener conocimientos avanzados de informática, programación y networking para utilizar herramientas rudimentarias y realizar ataques básicos. Con el correr del tiempo, y a medida que los métodos y las herramientas de los agresores mejoraban, ya no necesitaban el mismo nivel avanzado de conocimientos. Esto, efectivamente, disminuyó los requisitos de nivel inicial para los agresores. Quienes antes no hubieran cometido delitos informáticos, ahora pueden hacerlo.

Con la evolución de los tipos de amenazas, ataques y explotaciones, se han acuñado varios términos para describir a las personas involucradas. Estos son algunos de los términos más comunes:

- **Hacker de sombrero blanco**: una persona que busca vulnerabilidades en los sistemas o en las redes y, a continuación, informa estas vulnerabilidades a los propietarios del sistema para que las arreglen. Son éticamente opuestos al abuso de los sistemas informáticos. Por lo general, un hacker de sombrero blanco se concentra en proporcionar seguridad a los sistemas informáticos, mientras que a un hacker de sombrero negro (el opuesto) le gustaría entrar por la fuerza en ellos.
- **Hacker**: es un término general que se ha utilizado históricamente para describir a un experto en programación. Recientemente, este término se ha utilizado con frecuencia con un sentido negativo, para describir a una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa.
- **Hacker de sombrero negro**: otro término que se aplica a las personas que utilizan su conocimiento de las redes o los sistemas informáticos que no están autorizados a utilizar, generalmente para beneficio personal o económico. Un cracker es un ejemplo de hacker de sombrero negro.
- **Cracker**: es un término más preciso para describir a una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa.
- **Phreaker**: una persona que manipula la red telefónica para que realice una función que no está permitida. Un objetivo común del phreaking es ingresar en la red telefónica, por lo general a través de un teléfono público, para realizar llamadas de larga distancia gratuitas.
- **Spammer**: persona que envía grandes cantidades de mensajes de correo electrónico no solicitado. Por lo genera, los spammers utilizan virus para tomar control de computadoras domésticas y utilizarlas para enviar sus mensajes masivos.
- **Estafador**: utiliza el correo electrónico u otro medio para engañar a otras personas para que brinden información confidencial, como números de tarjetas de crédito o contraseñas. Un estafador se hace pasar por una persona de confianza que tendría una necesidad legítima de obtener información confidencial.

Pensar como un agresor

El objetivo del agresor es afectar un objetivo de red o a una aplicación que se ejecuta dentro de una red. Muchos agresores usan el siguiente proceso de siete pasos para obtener información y plantear un ataque.

Paso 1. Realizar un análisis del perfil (reconocimiento). La página Web de una empresa puede conducir a información, como las direcciones IP de los servidores. Desde allí, un agresor puede crear una imagen del perfil de seguridad o de la "huella" de la empresa.

Paso 2. Enumerar los datos. Un agresor puede ampliar el perfil controlando el tráfico de la red con un programa detector de paquetes, como Wireshark, buscando información como los números de versión de los servidores FTP y de los servidores de correo. Una referencia cruzada con bases de datos de vulnerabilidades expone las aplicaciones de la empresa a explotaciones potenciales.

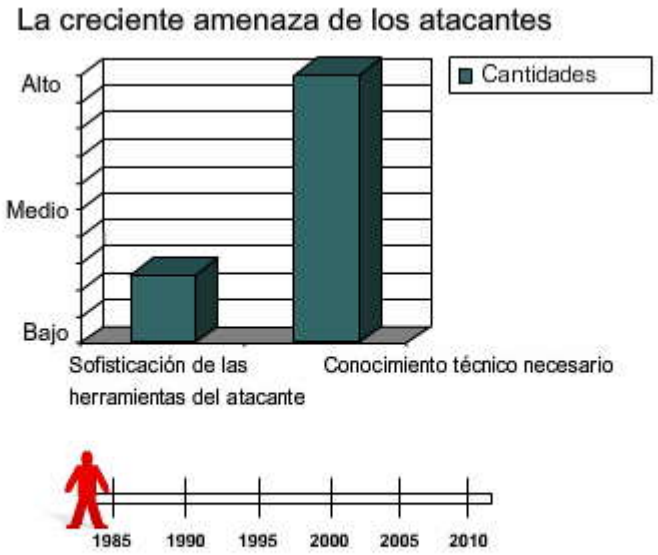
Paso 3. Manipular a los usuarios para obtener acceso. Algunas veces, los empleados eligen contraseñas que se pueden descifrar fácilmente. En otros casos, los empleados pueden ser engañados por agresores talentosos para revelar información confidencial relacionada con el acceso.

Paso 4. Aumentar los privilegios. Una vez que los agresores obtienen acceso básico, utilizan sus habilidades para aumentar los privilegios de la red.

Paso 5. Recopilar más contraseñas y secretos. Con privilegios de acceso mejorados, los agresores utilizan su talento para obtener acceso a información confidencial bien protegida.

Paso 6. Instalar virus de puerta trasera. Las puertas traseras proporcionan a los agresores una forma de ingresar al sistema sin ser detectados. La puerta trasera más común es un puerto de escucha TCP o UDP abierto.

Paso 7. Potenciar el sistema comprometido. Una vez que un sistema está comprometido, los agresores lo utilizan para llevar a cabo ataques en otros hosts de la red.



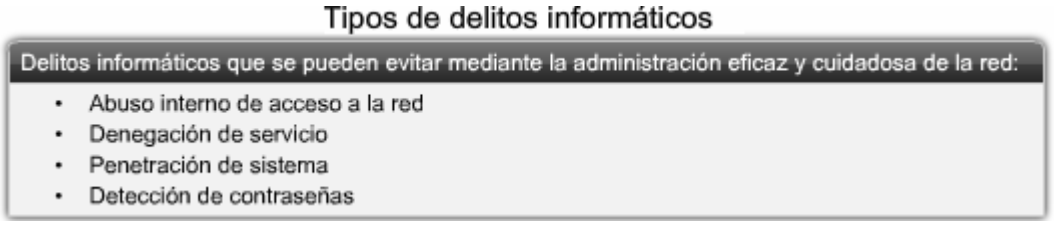
Tipos de delitos informáticos

Con la mejora de las medidas de seguridad en el transcurso de los años, algunos de los tipos de ataques más comunes disminuyeron en frecuencia, y surgieron nuevos tipos. La concepción de soluciones de seguridad de red comienza con una evaluación del alcance completo de los delitos informáticos. Estos son los actos de delitos informáticos denunciados con más frecuencia que tienen implicancias en la seguridad de la red:

- Abuso del acceso a la red por parte de personas que pertenecen a la organización
- Virus
- Robo de dispositivos portátiles

- Suplantación de identidad en los casos en los que una organización está representada de manera fraudulenta como el emisor
- Uso indebido de la mensajería instantánea
- Denegación de servicio
- Acceso no autorizado a la información
- Bots dentro de la organización
- Robo de información de los clientes o de los empleados
- Abuso de la red inalámbrica
- Penetración en el sistema
- Fraude financiero
- Detección de contraseñas
- Registro de claves
- Alteración de sitios Web
- Uso indebido de una aplicación Web pública
- Robo de información patentada
- Explotación del servidor DNS de una organización
- Fraude en las telecomunicaciones
- Sabotaje

Nota: En algunos países, es posible que algunas de estas actividades no constituyan un delito, pero siguen siendo un problema.



Redes abiertas versus redes cerradas

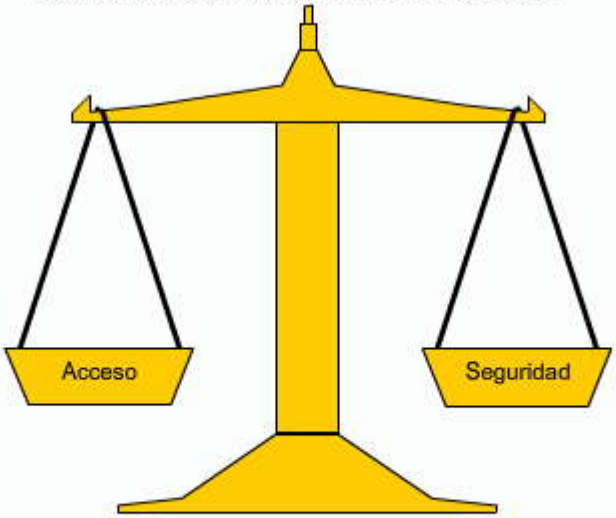
El desafío general de seguridad al que se enfrentan los administradores de redes es equilibrar dos necesidades importantes: mantener las redes abiertas para respaldar los requisitos comerciales en evolución y proteger la información comercial privada, personal y estratégica.

Los modelos de seguridad de la red siguen una escala progresiva, desde "abierto": se otorga permiso a cualquier servicio, a menos que esté expresamente denegado, hasta "restrictivo": se deniega permiso a servicios de forma predeterminada, a menos que sean considerados necesarios. En el caso de redes abiertas, los riesgos de seguridad son evidentes. En el caso de las redes cerradas, las reglas de lo que está permitido son definidas en forma de política por una persona o un grupo dentro de la organización.

Realizar un cambio en la política de acceso puede ser tan simple como pedirle a un administrador de red que active un servicio. Según la empresa, un cambio podría exigir modificar la política de seguridad de la empresa para permitirle al administrador activar el servicio. Por ejemplo, una política de seguridad podría prohibir el uso de los servicios de mensajería instantánea (IM), pero el reclamo por parte de los empleados podría lograr que la empresa cambie la política.

Una alternativa extrema para administrar la seguridad es cerrar por completo una red al mundo exterior. Una red cerrada proporciona conectividad solamente a las personas y sitios conocidos de confianza. Una red cerrada no permite conectarse a las redes públicas. Como no hay conectividad con el exterior, las redes diseñadas de esta manera se consideran seguras contra los ataques externos. Sin embargo, todavía hay amenazas internas. Una red cerrada no es de mucha ayuda para impedir ataques desde el interior de la empresa.

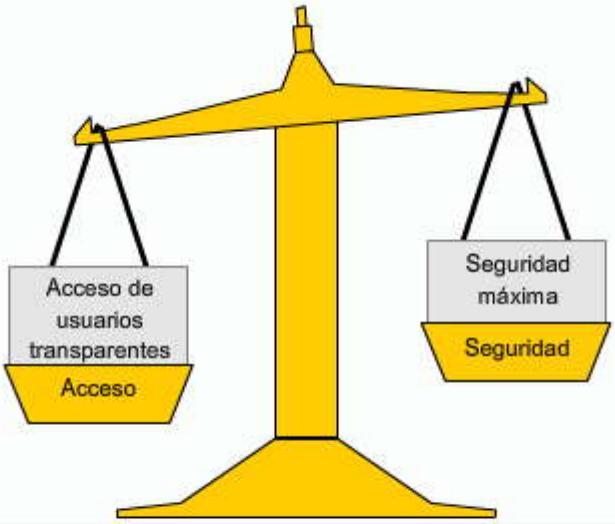
Redes cerradas versus redes abiertas



Los administradores de red buscan llegar a un equilibrio entre acceso y seguridad.

Equilibrio | Abierto | Restrictivo | Cerrado

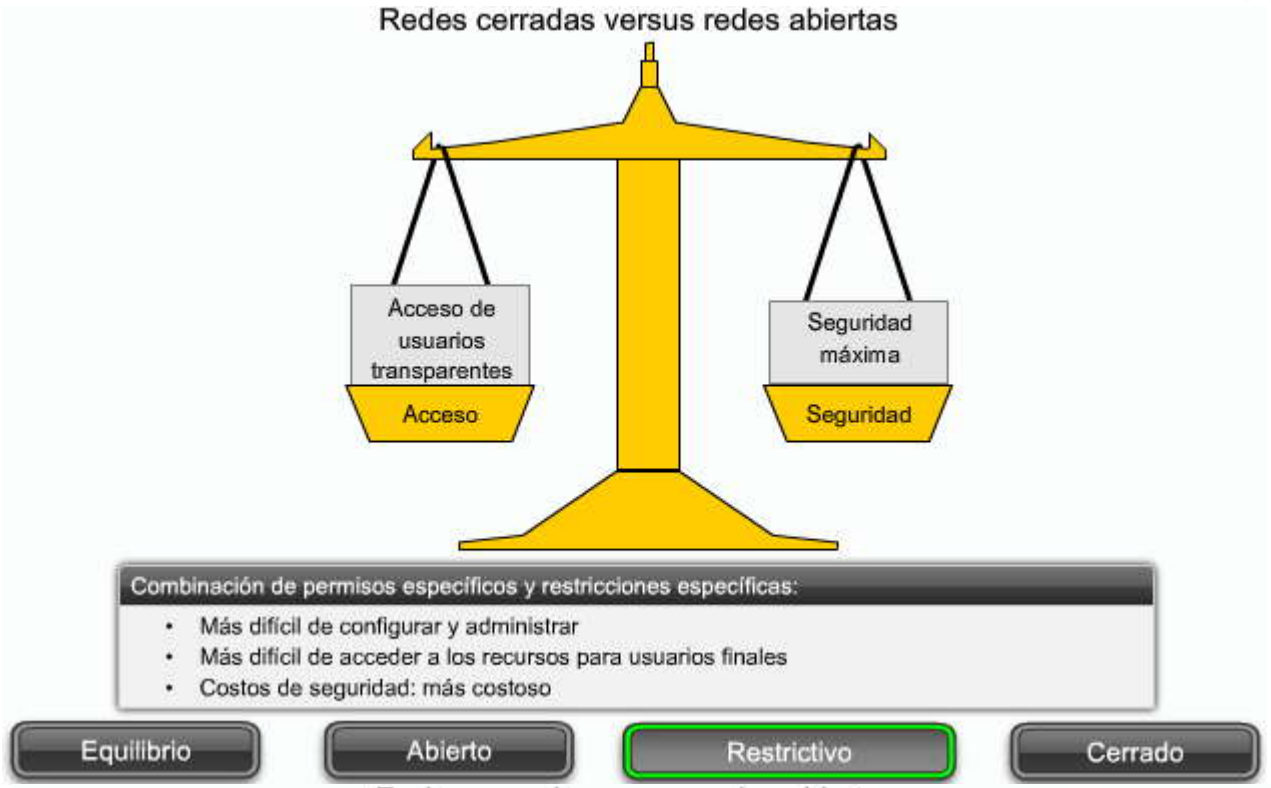
Redes cerradas versus redes abiertas

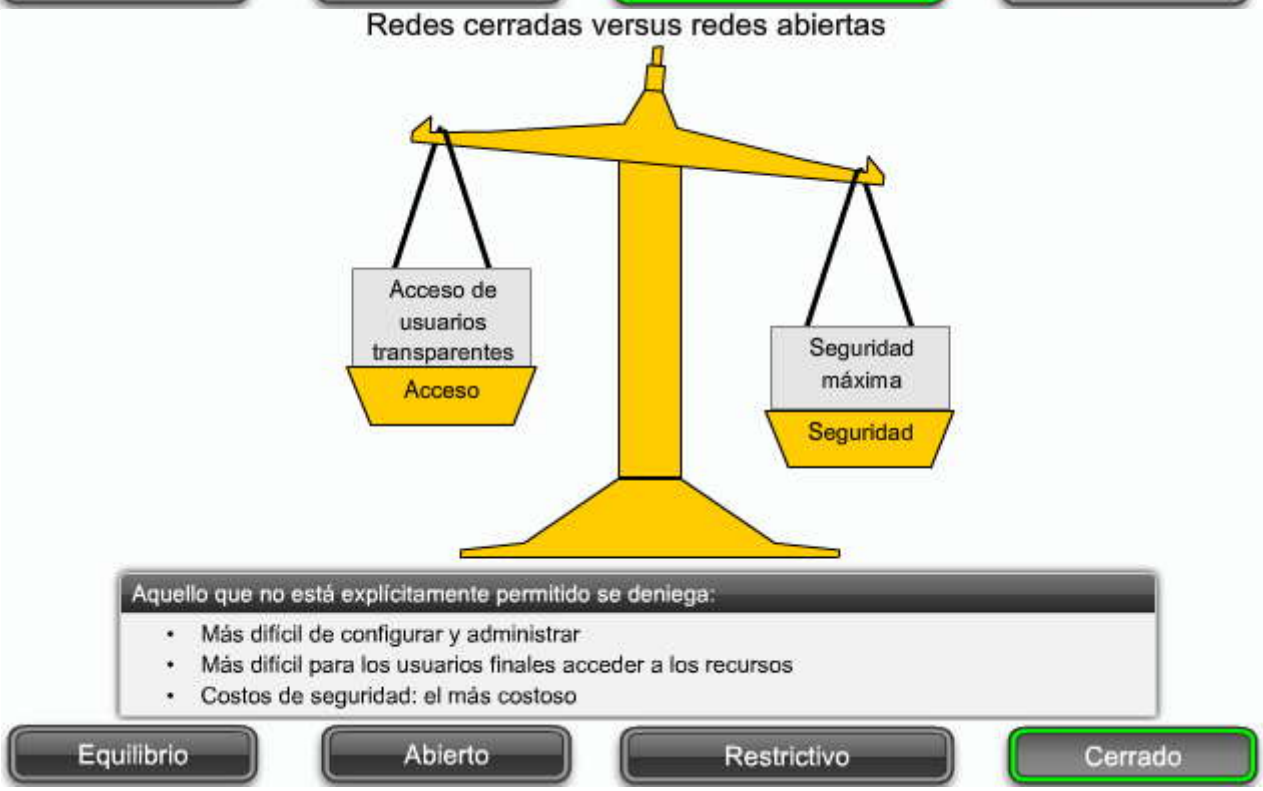


Permite todo lo que no está explícitamente denegado:

- Fácil de configurar y administrar
- Fácil para los usuarios finales acceder a los recursos de la red
- Costos de seguridad: el menos costoso

Equilibrio | Abierto | Restrictivo | Cerrado





Desarrollo de una política de seguridad

El primer paso que debe dar una organización para proteger sus datos y a sí misma del reto de la responsabilidad es desarrollar una política de seguridad. Una política es un conjunto de principios que guían los procesos de toma de decisiones y permiten que los líderes de una organización distribuyan la autoridad con confianza. RFC2196 establece que "una política de seguridad es una declaración formal de las normas por las que se deben regir las personas que obtienen acceso a los bienes de tecnología e información de una organización. Una política de seguridad puede ser tan simple como una breve Política de uso aceptable para recursos de red, o puede contener varios cientos de páginas y detallar cada aspecto de conectividad y las políticas asociadas.

Una política de seguridad debe cumplir los siguientes objetivos:

- Informar a los usuarios, al personal y a los gerentes acerca de los requisitos obligatorios para proteger los bienes de tecnología e información
- Especificar los mecanismos a través de los cuales se pueden cumplir estos requisitos
- Proporcionar una línea de base a partir de la que se pueda adquirir, configurar y auditar redes y sistemas informáticos para que cumplan la política

Definir una política de seguridad puede ser desalentador si se hace sin orientación. Es por ello que la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) han publicado un documento norma de seguridad denominado ISO/IEC 27002. Este documento hace referencia específicamente a la tecnología de la información y esboza un código de prácticas para la administración de la seguridad de la información.

La norma ISO/IEC 27002 pretende ser una base común y una guía práctica para desarrollar normas de seguridad de la organización y prácticas eficaces de administración de seguridad. El documento consta de 12 secciones:

- Evaluación de riesgos
- Política de seguridad
- Organización de la seguridad de la información
- Administración de activos
- Seguridad de los recursos humanos
- Seguridad física y ambiental
- Administración de las comunicaciones y operaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de los sistemas informáticos
- Administración de incidentes de seguridad de la información
- Administración para la continuidad de la empresa
- Cumplimiento

El presente capítulo se concentra en la sección de políticas de seguridad. Para leer acerca de todas las secciones, vaya a http://en.wikipedia.org/wiki/ISO/IEC_27002. En los temas 4.1.5 "La rueda de seguridad de la red" y 4.1.6 "La política de seguridad de la empresa", se analiza el desarrollo del documento de políticas de seguridad de la red.

4.1.2 Amenazas comunes a la seguridad

Vulnerabilidades

En el análisis de la seguridad de la red, los tres factores comunes son vulnerabilidad, amenaza y ataque.

La vulnerabilidad es el grado de debilidad inherente a cada red y cada dispositivo. Esto incluye routers, switches, equipos de escritorio, servidores e, incluso, dispositivos de seguridad.

Las amenazas son las personas interesadas y calificadas para aprovechar cada una de las debilidades en materia de seguridad. De dichas personas se puede esperar que busquen continuamente nuevas explotaciones y debilidades.

Las amenazas utilizan una diversidad de herramientas, secuencias de comandos y programas, para lanzar ataques contra redes y dispositivos de red. Por lo general, los dispositivos de red atacados son los extremos, como los servidores y los equipos de escritorio.

Hay tres vulnerabilidades o debilidades principales:

- Debilidades tecnológicas
- Debilidades en la configuración
- Debilidades en la política de seguridad

Haga clic en el botón Tecnología de la figura.

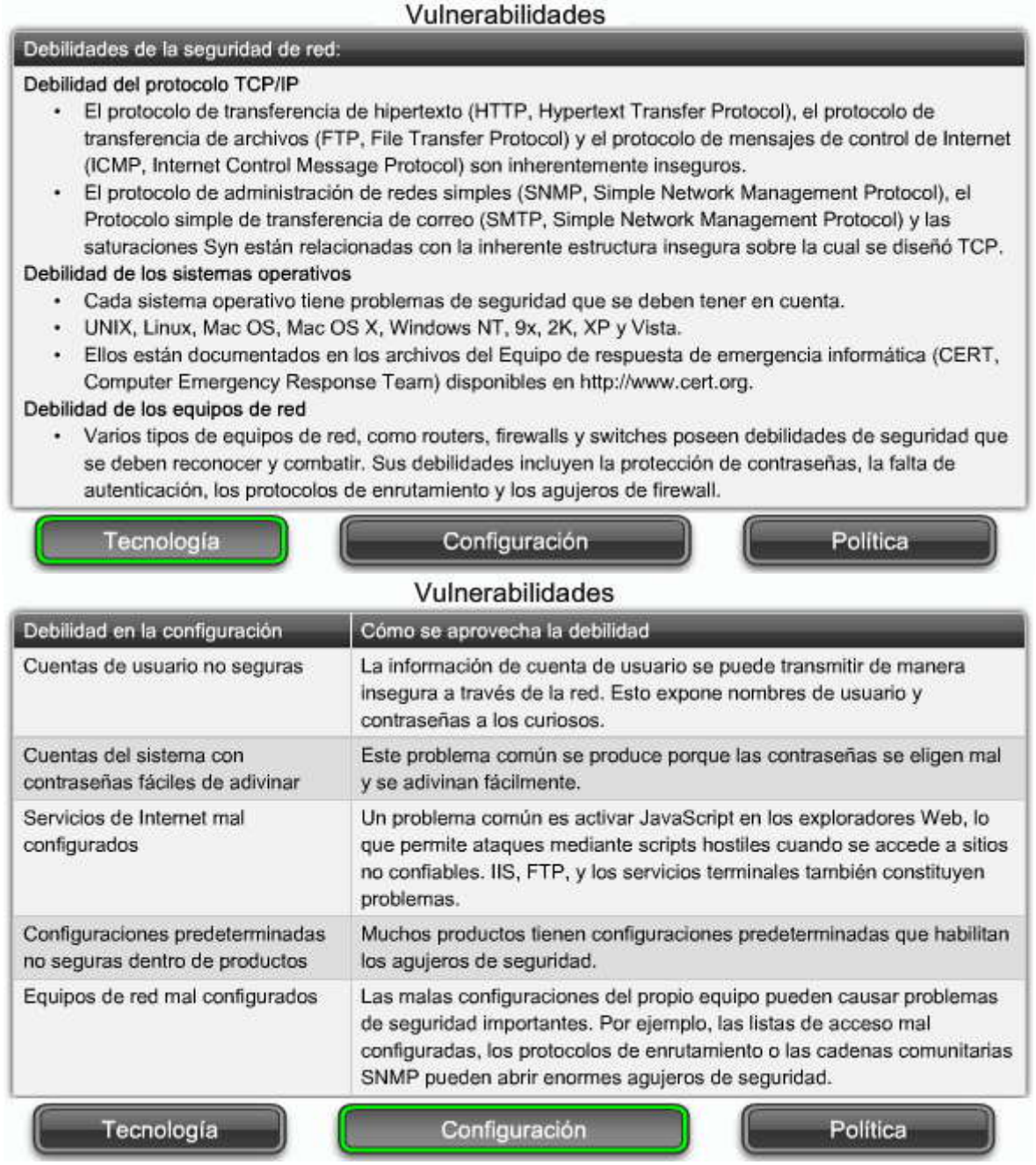
Las tecnologías informáticas y de red tienen debilidades de seguridad intrínsecas. Entre ellas, las debilidades del protocolo TCP/IP, del sistema operativo y de los equipos de red.

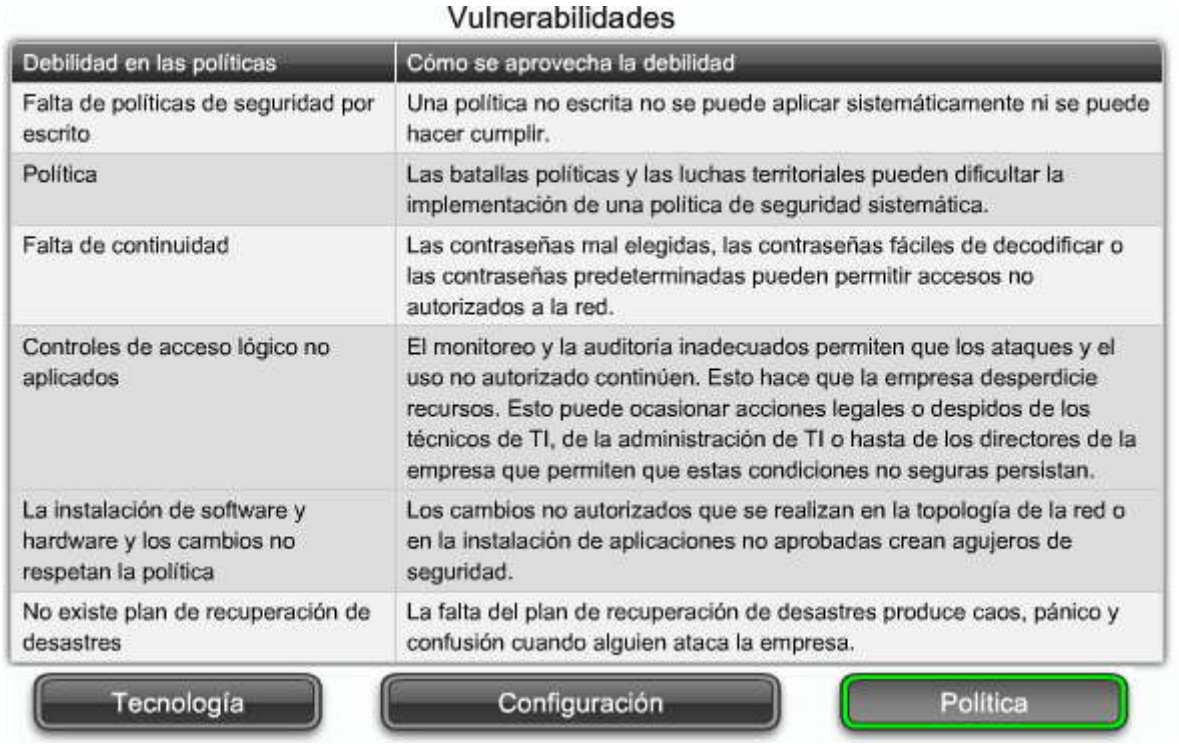
Haga clic en el botón Configuración de la figura.

Los administradores o los ingenieros de redes necesitan aprender cuáles son las debilidades de la configuración y configurar correctamente sus dispositivos informáticos y de red para compensarlas.

Haga clic en el botón Política de la figura.

Hay riesgos de seguridad en la red si los usuarios no respetan la política de seguridad. En la siguiente figura, se enumeran algunas debilidades comunes de la política de seguridad y la manera en que se explotan dichas debilidades.





Amenazas a la infraestructura física

Cuando se piensa en la seguridad de la red, o incluso en la seguridad informática, uno imagina agresores que explotan las vulnerabilidades del software. Una clase de amenaza menos glamorosa, pero no menos importante, es la seguridad física de los dispositivos. Un agresor puede denegar el uso de los recursos de la red si dichos recursos pueden ser comprometidos físicamente.

Las cuatro clases de amenazas físicas son:

- **Amenazas al hardware**: daño físico a los servidores, routers, switches, planta de cableado y estaciones de trabajo
- **Amenazas ambientales**: temperaturas extremas (calor o frío extremos) o condiciones extremas de humedad (humedad o sequedad extremas)
- **Amenazas eléctricas**: picos de voltaje, voltaje suministrado insuficiente (apagones), alimentación ilimitada (ruido) y pérdida total de alimentación
- **Amenazas al mantenimiento**: manejo deficiente de los componentes eléctricos clave (descarga electrostática), falta de repuestos fundamentales, cableado insuficiente y rotulado incorrecto

Algunos de estos problemas deben ser abordados dentro de una política de la organización. Algunos están sujetos a un buen liderazgo y administración dentro de la organización. Las consecuencias de la mala suerte pueden desbaratar una red si la seguridad física no está bien preparada.

A continuación, se presentan algunas formas de mitigar las amenazas físicas:

- Mitigación de amenazas al hardware
- Mitigación de amenazas ambientales
- Mitigación de amenazas eléctricas

Haga clic en el botón Hardware de la figura.

Mitigación de amenazas al hardware

Cierre el armario del cableado y permita el acceso sólo al personal autorizado. Bloquee el acceso a través de techos falsos, pisos falsos, ventanas, conductos o puntos de entrada que no sean el punto de acceso seguro. Use el control de acceso electrónico y registre todas las tentativas de entrada. Controle las instalaciones con cámaras de seguridad.

Haga clic en el botón Ambiental de la figura.

Mitigación de amenazas ambientales

Cree un entorno operativo propicio, a través del control de la temperatura, de la humedad, el flujo de aire positivo, las alarmas ambientales remotas, y la grabación y vigilancia.

Haga clic en el botón Eléctrico de la figura.

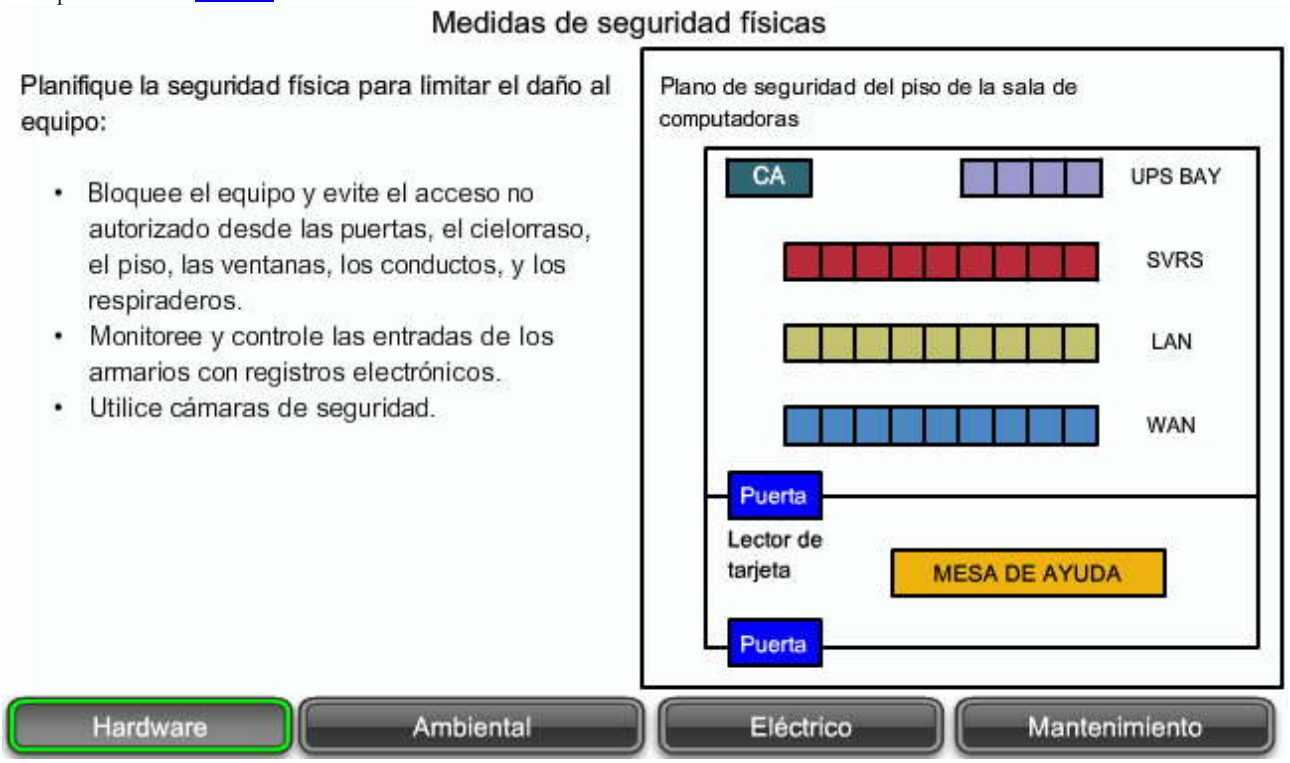
Mitigación de amenazas eléctricas

Disminuya los problemas de alimentación eléctrica instalando sistemas UPS y conjuntos de generadores, mediante un plan de mantenimiento preventivo, la instalación de suministros de energía redundante y alarmas y vigilancia remotas.

Haga clic en el botón Mantenimiento de la figura.

Mitigación de amenazas al mantenimiento

Mitigación de amenazas relacionadas con el mantenimiento: use tendidos de cables limpios, rotule los cables y componentes críticos, use procedimientos de descarga electrostática, tenga una provisión de repuestos fundamentales y controle el acceso a los puertos de la consola.



Medidas de seguridad físicas

Restrinja el daño mediante la creación de un adecuado ambiente operativo:

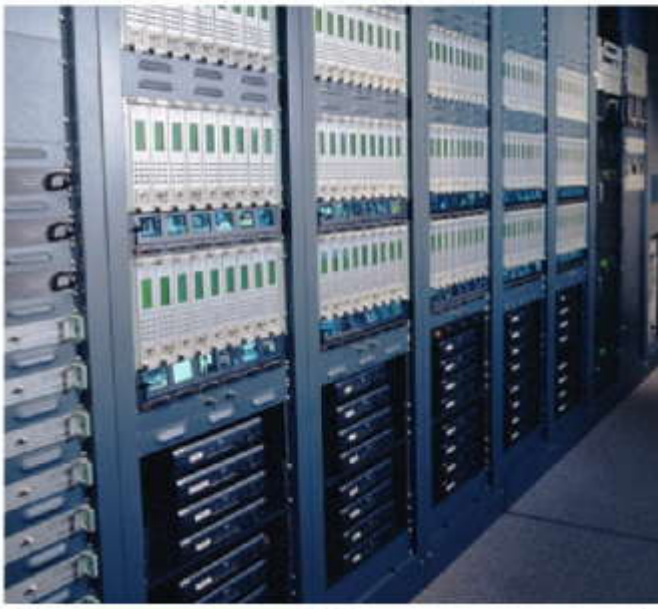
- Control de temperatura
- Control de humedad
- Flujo de aire positivo
- Alarma ambiental remota y grabación y vigilancia

Hardware | Ambiental | Eléctrico | Mantenimiento

Medidas de seguridad físicas

Restrinja los problemas de suministro eléctrico:

- Instale sistemas de UPS
- Instale grupos de generadores
- Siga un plan de mantenimiento preventivo
- Instale fuentes de energía redundantes
- Mantenga sistemas de alarmas y vigilancia



Hardware | Ambiental | Eléctrico | Mantenimiento

Amenazas a las redes

Anteriormente, en este capítulo, se enumeraron los delitos informáticos comunes que repercuten sobre la seguridad de la red. Estos delitos se pueden agrupar en cuatro clases principales de amenazas a las redes:

Amenazas no estructuradas

Las amenazas no estructuradas consisten principalmente en personas sin experiencia que usan herramientas de piratería informática de fácil acceso, como secuencias de comandos de shell y crackers de contraseñas. Hasta las amenazas no estructuradas, que se ejecutan con el único propósito de probar las habilidades de un agresor, pueden provocar daños graves a una red. Por ejemplo, si se hackea el sitio Web de una empresa, se puede dañar la reputación de dicha empresa. Aunque el sitio Web esté separado de la información privada que se encuentra detrás de un firewall protector, el público no lo sabe. Lo que el público percibe es que el sitio podría no ser un entorno seguro para realizar negocios.

Amenazas estructuradas

Las amenazas estructuradas provienen de personas o grupos que tienen una mayor motivación y son más competentes técnicamente. Estas personas conocen las vulnerabilidades del sistema y utilizan técnicas de piratería informática sofisticadas para introducirse en las empresas confiadas. Ingresan en computadoras de empresas y del gobierno para cometer fraude, destruir o alterar registros o, simplemente, para crear confusión. Por lo general, estos grupos están involucrados en los principales casos de fraude y robo denunciados en los organismos de aplicación de la ley. Utilizan tácticas de piratería informática tan complejas y sofisticadas que sólo los investigadores especialmente capacitados entienden lo que está ocurriendo.

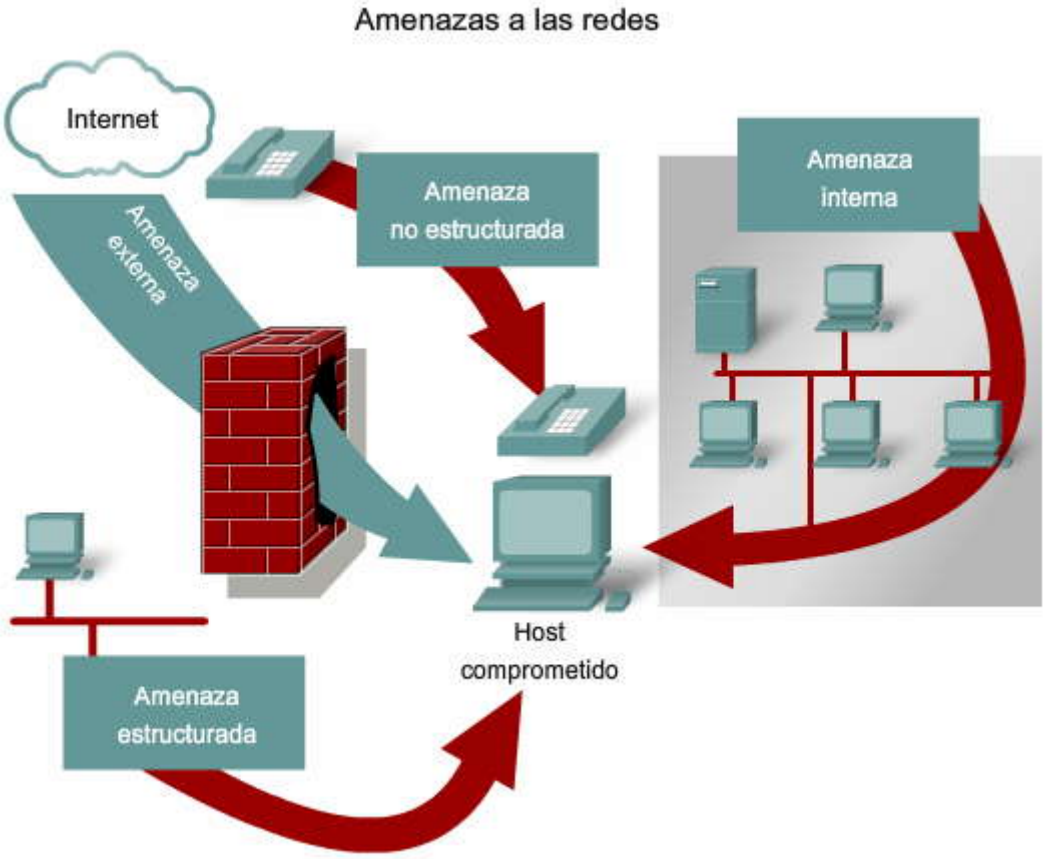
En 1995, Kevin Mitnick fue condenado por ingresar a computadoras de distintos estados de los EstadosUnidos con fines delictivos. Ingresaba en la base de datos del Departamento del Automotor de California, rutinariamente tomaba control de los hubs de conmutación telefónica de Nueva York y California y robaba números de tarjetas de crédito. Inspiró la película "Juegos de guerra" del año 1983.

Amenazas externas

Las amenazas externas pueden provenir de personas u organizaciones que trabajan fuera de una empresa y que no tienen acceso autorizado a los sistemas informáticos ni a la red. Ingresan a una red principalmente desde Internet o desde servidores de acceso telefónico. Las amenazas externas pueden tener distintos grados de gravedad según la experiencia del agresor, ya sea aficionado (no estructurado) o experto (estructurado).

Amenazas internas

Las amenazas internas son las provocadas por una persona que tiene acceso autorizado a la red, ya sea mediante una cuenta o acceso físico. Al igual que en el caso de las amenazas externas, la gravedad de una amenaza interna depende de la experiencia del agresor.



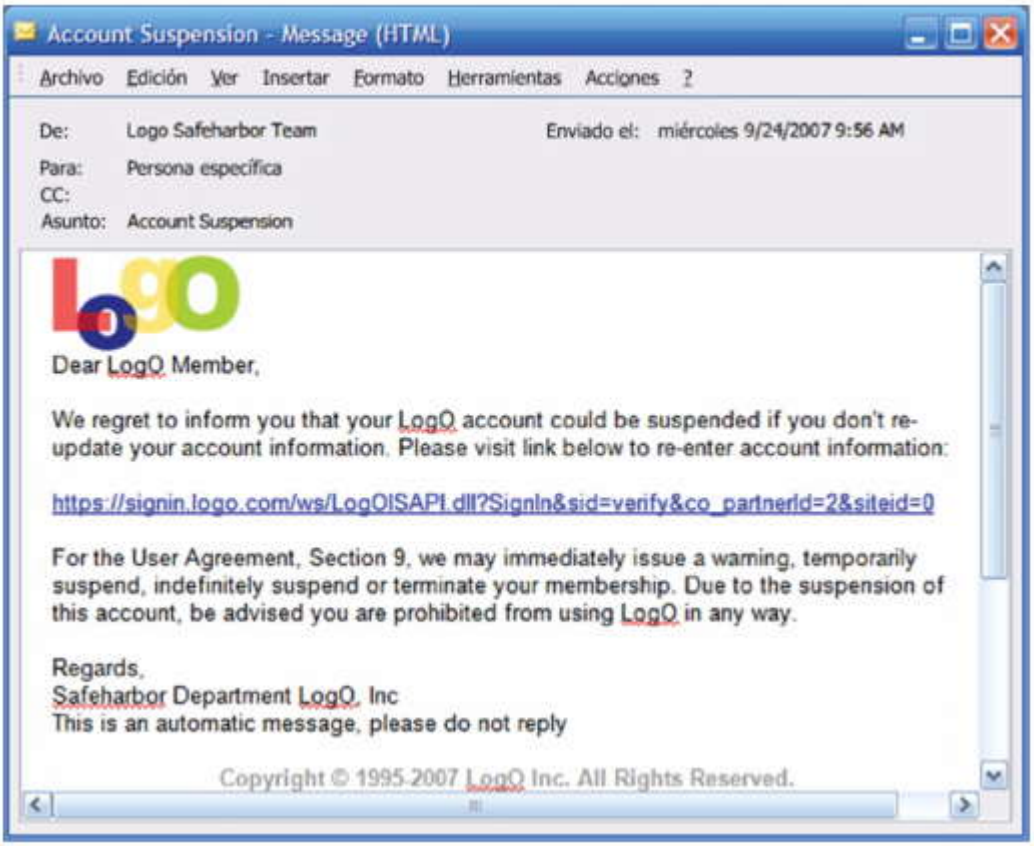
Ingeniería social

La piratería informática más sencilla no requiere habilidad informática alguna. Si un intruso puede engañar a un miembro de una organización para que le proporcione información valiosa, como la ubicación de los archivos o de las contraseñas, el proceso de piratería informática se torna mucho más fácil. Este tipo de ataque se denomina ingeniería social, y se aprovecha de las vulnerabilidades personales que pueden ser descubiertas por agresores talentosos. Puede incluir apelaciones alego de un empleado, o bien puede tratarse de una persona simulada o un documento falsificado que logra que una persona proporcione información confidencial.

La suplantación de identidad es un tipo de ataque de ingeniería social que involucra el uso de correo electrónico u otros tipos de mensajes para intentar engañar a otras personas, de modo que brinden información confidencial, como números de tarjetas de crédito o contraseñas. El estafador se hace pasar por una persona de confianza que tiene una necesidad aparentemente legítima de obtener información confidencial.

Con frecuencia, los fraudes de suplantación de identidad involucran el envío de correo no deseado que aparenta provenir de sitios de banca o de subastas en línea. La figura muestra una réplica de dicho correo electrónico. La empresa real utilizada como señuelo de este ejemplo se ha modificado. Estos correos electrónicos contienen hipervínculos que parecen legítimos, pero que, en realidad, llevan a los usuarios a un sitio Web falso creado por el estafador para capturar su información. El sitio aparenta pertenecer a la parte cuya identidad se falsificó en el correo electrónico. Cuando el usuario introduce la información, se registra para que la utilice el estafador.

Los ataques de suplantación de identidad pueden prevenirse educando a los usuarios e implementando pautas de información cuando se reciben correos electrónicos sospechosos. Los administradores también pueden bloquear el acceso a determinados sitios Web y configurar filtros que bloqueen el correo electrónico sospechoso.



4.1.3 Tipos de ataques a redes

Tipos de ataques a redes

Hay cuatro clases de ataques principales.

Reconocimiento

Es el descubrimiento y la asignación no autorizados de sistemas, servicios o vulnerabilidades. También se conoce como recopilación de información y, en la mayoría de los casos, precede a otro tipo de ataque. El reconocimiento es similar a un ladrón que está reconociendo un barrio en busca de casas vulnerables para entrar a robar, como una residencia desocupada, puertas fáciles de abrir o ventanas abiertas.

Acceso

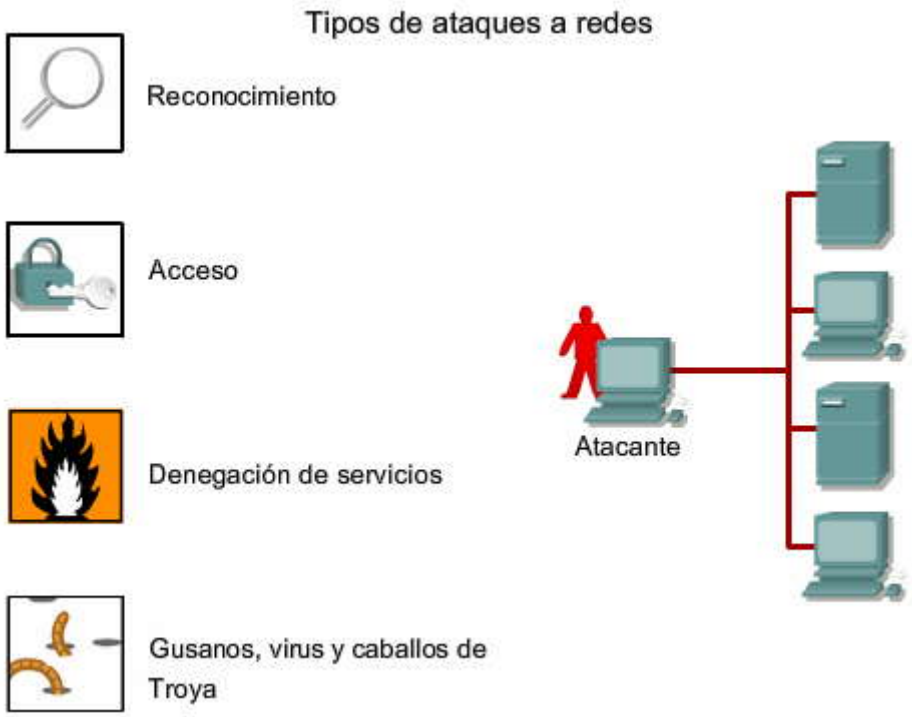
El acceso a los sistemas es la capacidad de un intruso de obtener acceso a un dispositivo respecto del cual no tiene cuenta ni contraseña. Por lo general, el ingreso o acceso a los sistemas implica ejecutar un acto de piratería informática, una secuencia de comandos o una herramienta que explota una vulnerabilidad conocida del sistema o de la aplicación que se está atacando.

Denegación de servicio

La denegación de servicio (DoS) se lleva a cabo cuando un agresor desactiva o daña redes, sistemas o servicios, con el propósito de denegar servicios a los usuarios a quienes están dirigidos. Los ataques de DoS incluyen colapsar el sistema o desacelerarlo hasta el punto en que queda inutilizable. No obstante, la DoS puede ser tan sencilla como eliminar o dañar información. En la mayoría de los casos, ejecutar el ataque implica simplemente ejecutar un acto de piratería informática o una secuencia de comandos. Por estas razones, los ataques de DoS son los más temidos.

Virus, gusanos y caballos de Troya

El software malicioso puede ser insertado en un host para perjudicar o dañar un sistema, puede replicarse a sí mismo, o denegar el acceso a las redes, los sistemas o los servicios. Los nombres comúnmente utilizados para este tipo de software son gusanos, virus y caballos de Troya.



Ataques de reconocimiento
Los ataques de reconocimiento pueden consistir en uno de los siguientes:

- Consultas de información en Internet
- Barridos de ping
- Escaneos de puertos
- Programas detectores de paquetes

Los agresores externos pueden utilizar herramientas de Internet, como las utilidades nslookup y whois, para determinar fácilmente el espacio para la dirección IP asignado a una empresa o entidad. Una vez determinado el espacio para la dirección IP, un agresor puede hacer ping en las direcciones IP disponibles públicamente para identificar las direcciones que están activas. Para ayudar a automatizar este paso, el agresor puede utilizar una herramienta de barrido de pings, como fping o gping, que hace ping sistemáticamente a todas las direcciones de red de un alcance o una subred determinada. Es similar a revisar una sección de la guía telefónica y llamar a cada número para ver quién responde.

Cuando se identifican las direcciones IP activas, el intruso utiliza un escáner de puertos para determinar qué puertos o servicios de red están activos en las direcciones IP en uso. Un escáner de puertos es software, como Nmap o Superscan, diseñado para buscar puertos abiertos en un host de red. El escáner de puertos consulta a los puertos para determinar el tipo y la versión de la aplicación, además del tipo y la versión del sistema operativo (OS) que se está ejecutando en el host objetivo. Sobre la base de esta información, el intruso puede determinar si hay una vulnerabilidad que pueda explotarse. Como se muestra en la figura, es posible usar una herramienta de exploración de redes, comoNmap, para detectar hosts, escanear puertos, detectar versiones y sistemas operativos. Muchas de estas herramientas están disponibles y son fáciles de utilizar.

Los agresores internos pueden intentar "infiltrarse" en el tráfico de la red.

Sondeo de redes y detección de paquetes son términos comunes para infiltración. La información compilada mediante la infiltración puede utilizarse para realizar otros ataques a la red.

Los siguientes son dos usos comunes de infiltración:

- **Recopilación de información**: los intrusos de la red pueden identificar nombres de usuarios, contraseñas o información que se transportan en un paquete.
- **Robo de información**: puede concretarse mientras los datos se transmiten a través de la red interna o externa. El intruso de la red también puede robar datos de computadoras en red obteniendo acceso no autorizado. Entre los ejemplos, se encuentran ingresar o infiltrarse en instituciones financieras y obtener números de tarjetas de crédito.

Un ejemplo de datos susceptibles de infiltración son las cadenas comunitarias (SNMP) versión 1, que se envían en texto no cifrado. El SNMP es un protocolo de administración que proporciona un medio para que los dispositivos de red recopilen información acerca de su estado y la envíen a un administrador. Un intruso podría infiltrarse en las consultas de SNMP y recopilar datos valiosos sobre la configuración de los equipos de la red. Otro ejemplo es la captura de nombres de usuario y contraseñas a medida que atraviesan una red.

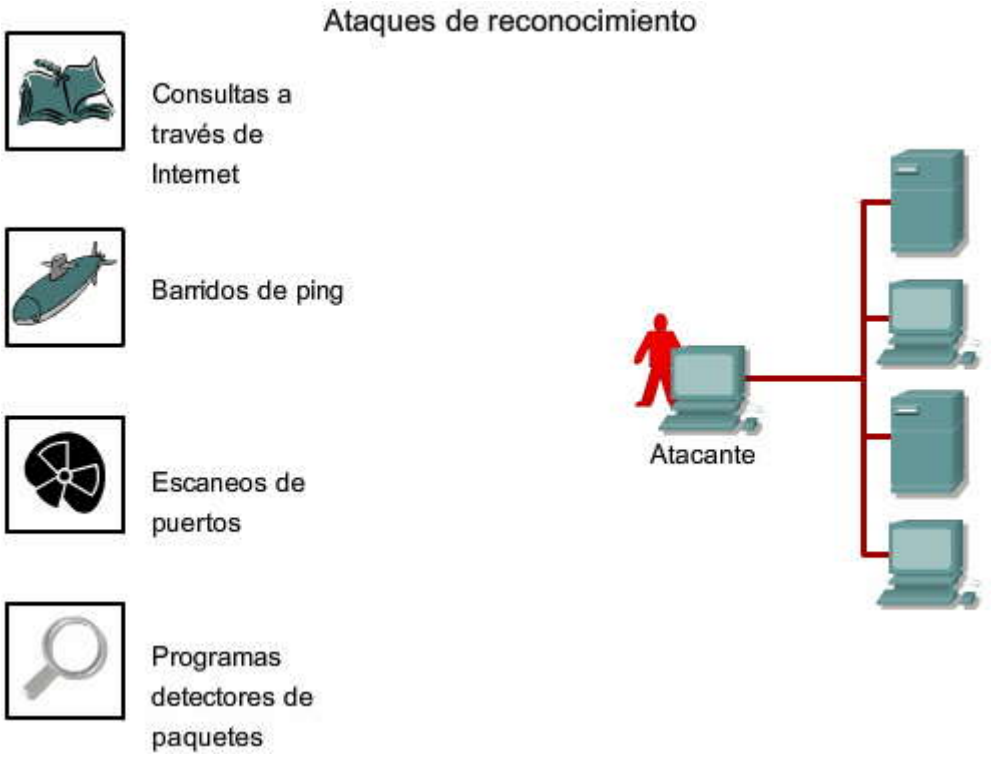
Un método común de infiltrarse en las comunicaciones consiste en capturar TCP/IP u otros paquetes de protocolos y decodificar los contenidos utilizando un analizador de protocolos o una utilidad similar. Un ejemplo de dicho programa es Wireshark, que se ha estado utilizando extensamente en todos los cursos de Exploration. Una vez capturados los paquetes, se les puede examinar en busca de información vulnerable.

Los siguientes son tres de los métodos más eficaces de contrarrestar la infiltración:

- Uso de redes conmutadas en lugar de hubs para que el tráfico no se transmita a todos los extremos o hosts de la red.
- Uso de encriptación que cumpla las necesidades de seguridad de los datos de la organización, sin imponer una carga excesiva en los usuarios o los recursos del sistema.
- Implementación y aplicación de una directiva de política que prohíba el uso de protocolos con conocida susceptibilidad a la infiltración. Por ejemplo, el SNMP versión 3 puede encriptar cadenas comunitarias, de manera que una empresa podría prohibir el uso de SNMP versión 1, pero permitir SNMP versión 3.

La encriptación proporciona protección para los datos susceptibles de ataques de infiltración, crackers de contraseñas o manipulación. Casi todas las empresas tienen transacciones que podrían tener consecuencias negativas si las viera un infiltrado. La encriptación garantiza que cuando los datos confidenciales pasan a través de un medio susceptible de infiltración, no se puedan alterar ni observar. El descifrado es necesario cuando los datos llegan al host de destino.

Un método de encriptación se denomina encriptación sólo de contenido. Este método encripta la sección de contenido (sección de datos) después de un encabezado del Protocolo de datagrama de usuario (UDP) o TCP. Esto permite que los routers y switches del software IOS de Cisco lean la información de la capa de red y envíen el tráfico como cualquier otro paquete IP. La encriptación sólo de contenido permite que la conmutación del flujo y todas las características de las listas de acceso funcionen con el tráfico encriptado, al igual que lo harían con el tráfico de texto sin cifrar, y así preservar la calidad de servicio (QoS) deseada de todos los datos.



Ataques de acceso

Los ataques de acceso explotan las vulnerabilidades conocidas de los servicios de autenticación, los servicios de FTP y los servicios Web para obtener acceso a cuentas Web, bases de datos confidenciales y otra información confidencial.

Ataques a las contraseñas

Los ataques a las contraseñas pueden implementarse mediante un programa detector de paquetes para proporcionar cuentas de usuarios y contraseñas que se transmiten como texto sin cifrar. Por lo general, los ataques a las contraseñas hacen referencia a intentos repetidos de conectarse a un recurso compartido, como un servidoro un router, para identificar una cuenta de usuario, una contraseña o ambas. Estos intentos repetidos se denominan ataques de diccionario o ataques de fuerza bruta.

Para llevar a cabo un ataque de diccionario, los agresores pueden utilizar herramientas, como L0phtCrack o Cain. Estos programas intentan conectarse reiteradamente como usuario mediante el uso de palabras incluidas en un diccionario. Los ataques de diccionario suelen ser exitosos, porque los usuarios tienden a elegir contraseñas sencillas queson palabras cortas, únicas y fáciles de predecir, como el agregado del número 1 a una palabra.

Otro método de ataque a las contraseñas utiliza tablas arco iris. Una tabla arco iris es una serie precalculada de contraseñas que se forma creando cadenas de posibles contraseñas de texto sin cifrar. Cada cadena se crea a partir de una "conjetura" seleccionada al azar de la contraseña de texto sin cifrar y, a continuación, se aplican variaciones de ésta. El software de ataque aplica las contraseñas de la tabla de arco iris hasta resolver la contraseña. Para llevar a cabo un ataque con tabla de arco iris, los agresores pueden utilizar una herramienta, por ejemplo, L0phtCrack.

Una herramienta de ataque de fuerza bruta es más sofisticada, porque busca, de manera exhaustiva, mediante combinaciones de conjuntos de caracteres, para calcular cada contraseña posible formada por esos caracteres. La desventaja es que se necesita más tiempo para llevar a cabo este tipo de ataque. Las herramientas de ataque de fuerza brutahan logrado resolver contraseñas simples en menos de un minuto. Es posible que, para resolver contraseñas más largas y más complejas, se necesiten días o semanas.

Los ataques a las contraseñas pueden mitigarse si se instruye a los usuarios para que usen contraseñas complejas y se especifican longitudes mínimas para éstas. Los ataques de fuerza bruta podrían mitigarse si se restringe la cantidad de intentos de conexión fallidos. Sin embargo, también es posible realizar un ataque de fuerza bruta en línea. Por ejemplo, si un agresor espía una contraseña encriptada, ya sea infiltrándose o ingresando a un archivo de configuración, podría intentar resolver la contraseña sin estar realmente conectado al host.

Explotación de confianza

El objetivo de un ataque de explotación de confianza es comprometer un host de confianza, mediante su uso, con el fin de llevar a cabo ataques en otros hosts de una red. Si un host de una red de una empresa está protegido por un firewall (host interno), pero un host de confianza que se encuentra afuera del firewall (host externo) puede obtener acceso a él, el host interno puede ser atacado a través del host externo de confianza.

El medio utilizado por los agresores para obtener acceso al host externo de confianza y los detalles de laexplotación de confianza no se analizan en este capítulo. Para obtener información acerca de la explotación de confianza, consulte el curso Seguridad de la Red de la Academia de Networking.

Los ataques basados en la explotación de confianza pueden ser mitigados a través de restricciones estrictas en los niveles de confianza dentro de una red, por ejemplo, las VLAN privadas pueden ser implementadas en segmentos de servidores públicos en los que hay varios servidores públicos disponibles. Los sistemas quese encuentran dentro de un firewall no pueden confiar en absoluto en los sistemas que se encuentran afuera. Dicha confianza debe limitarse a protocolos específicos y debe ser autenticada por algo más que una dirección IP, siempre que sea posible.

Redirección de puertos

Un ataque de redirección de puertos es un tipo de ataque de explotación de confianza que utiliza un host comprometido para pasar tráfico a través de un firewall que, de lo contrario, estaría bloqueado.

Considere un firewall con tres interfaces y un host en cada interfaz. El host externo puede llegar al host que se encuentra en el segmento de servicios públicos, pero no al host interno. Este segmento de acceso público, normalmente, se conoce como zona desmilitarizada (DMZ). El host que se encuentra en el segmento de servicios públicos puede llegar al host externo y al interno. Si los agresores pudieran comprometer el host que se encuentra en el segmento de servicios públicos, podrían instalar software para redirigir el tráfico desde el host externo directamente al interno. Si bien ninguna comunicación infringe las normas implementadas en el firewall, ahora, el host externo ha logrado conectarse con el host interno a través del proceso de redirección de puertos del host de servicios públicos. Un ejemplo de utilidad que puede proporcionar este tipo de acceso es netcat.

La redirección de puertos puede ser mitigada principalmente mediante el uso de modelos de confianza adecuados, específicos para la red (como se mencionó anteriormente). Cuando un sistema es atacado, un sistema de detección de intrusión (IDS) basado en hosts puede ayudar a detectar a un agresor e impedir la instalación de dichas utilidades en un host.

Ataque man-in-the-middle

Los ataques man-in-the-middle (MITM) son realizados por agresores que logran ubicarse entre dos hosts legítimos. El agresor puede permitir que se realicen transacciones normales entre hosts, y manipular la conversación entre ambos sólo periódicamente.

Hay muchas maneras en las que un agresor puede ubicarse entre dos hosts. Los detalles de estos métodos se encuentran fuera del alcance de este curso, pero una breve descripción de un método popular, el proxy transparente, ayuda a ejemplificar la naturaleza de los ataques MITM.

En el caso de un ataque mediante un proxy transparente, un agresor puede encontrar a una víctima mediante un correo electrónico de suplantación de identidad o alterando un sitio Web. Entonces, la URL de un sitio Web legítimo tiene la URL de los agresores añadida delante de ella (anexada al principio). Por ejemplo, http:www.legitimate.com se convierte en http:www.attacker.com/http://www.legitimate.com.

1. Cuando una víctima solicita una página Web, el host de la víctima realiza la solicitud al host del agresor.

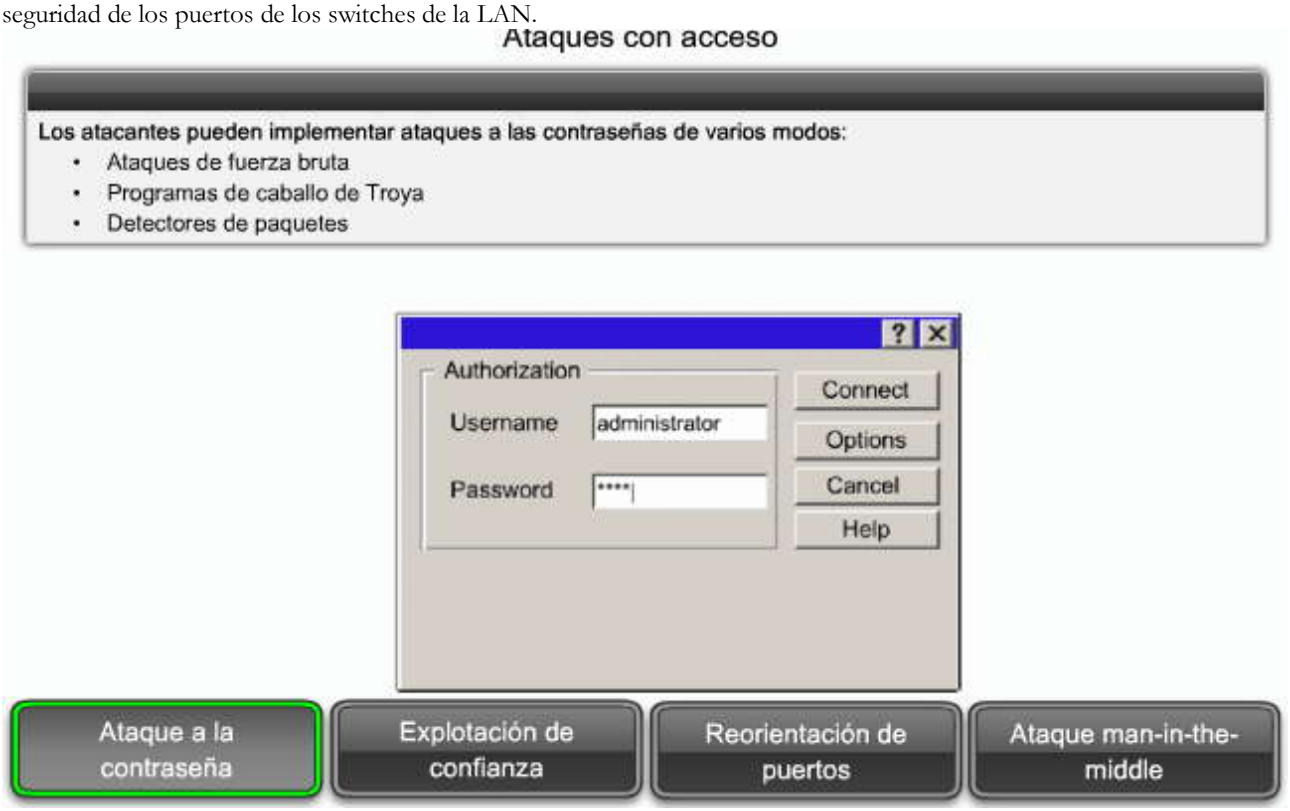
2. El host del agresor recibe la solicitud y busca la página verdadera en el sitio Web legítimo.

3. El agresor puede modificar la página Web legítima y aplicar las transformaciones a los datos que deseen realizar.

4. El agresor envía la página solicitada a la víctima.

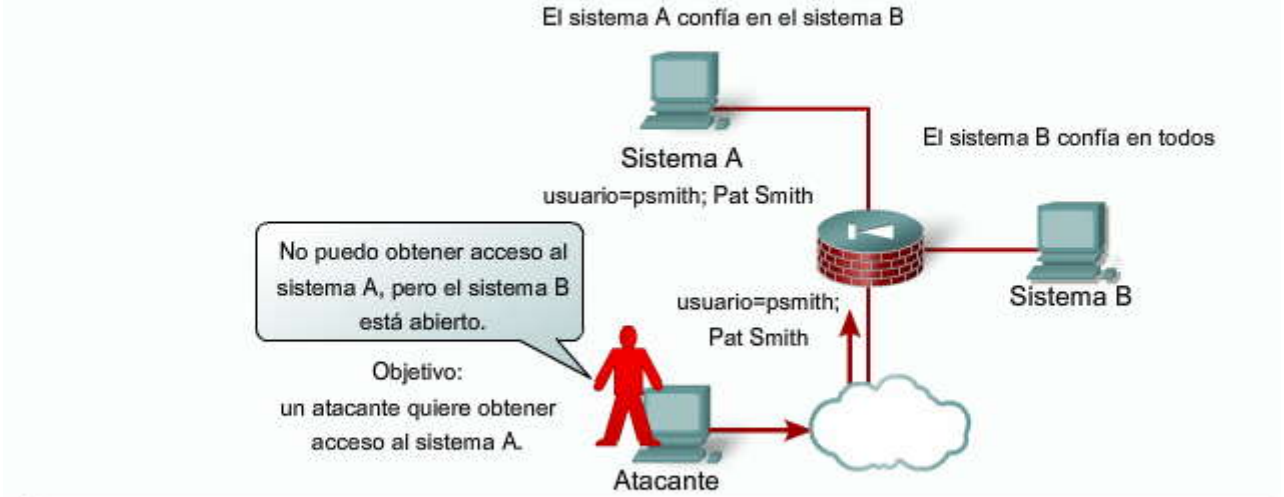
Otros tipos de ataques MITM son potencialmente aun más perjudiciales. Si los agresores logran colocarse en una posición estratégica, pueden robar información, apropiarse de una sesión en curso para obtener acceso a recursos de redes privadas, llevar a cabo ataques de DoS, dañar los datos transmitidos o introducir nuevos datos en las sesiones de la red.

La mitigación de los ataques MITM de la WAN se logra utilizando túneles VPN, lo que permite que el agresor vea sólo el texto encriptado, indescifrable. Los ataques MITM de la WAN utilizan herramientas tales como ettercap y envenenamiento ARP. Por lo general, la mayor parte de la mitigación de ataques MITM de la LAN se puede reducir configurando la seguridad de los puertos de los switches de la LAN.

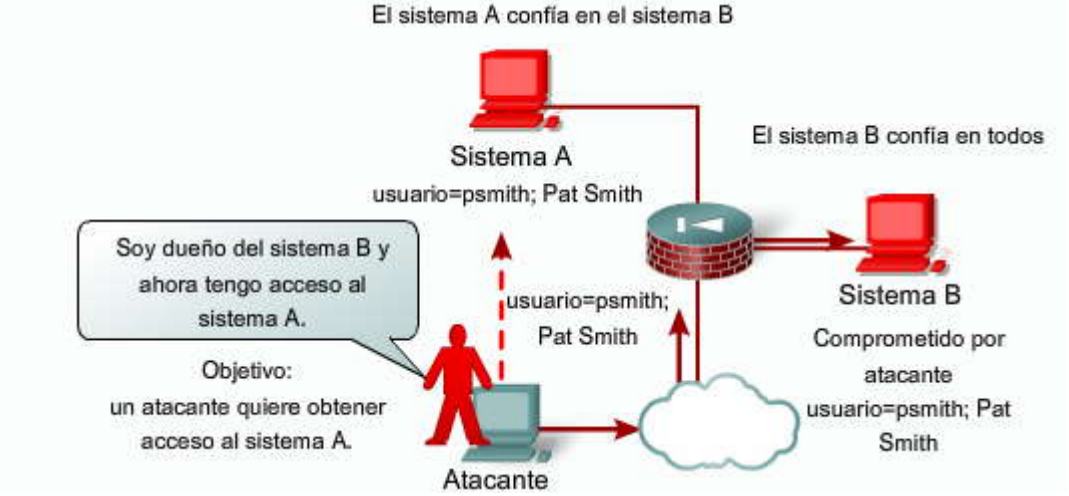


Ataques con acceso

SO de la red	Modelos de confianza
Windows	Dominios Active Directory (AD)
Linux y UNIX	Sistema de archivos de red (NFS, Network File System) Servicio de información de red Plus (NIS+, Network Information Service Plus)

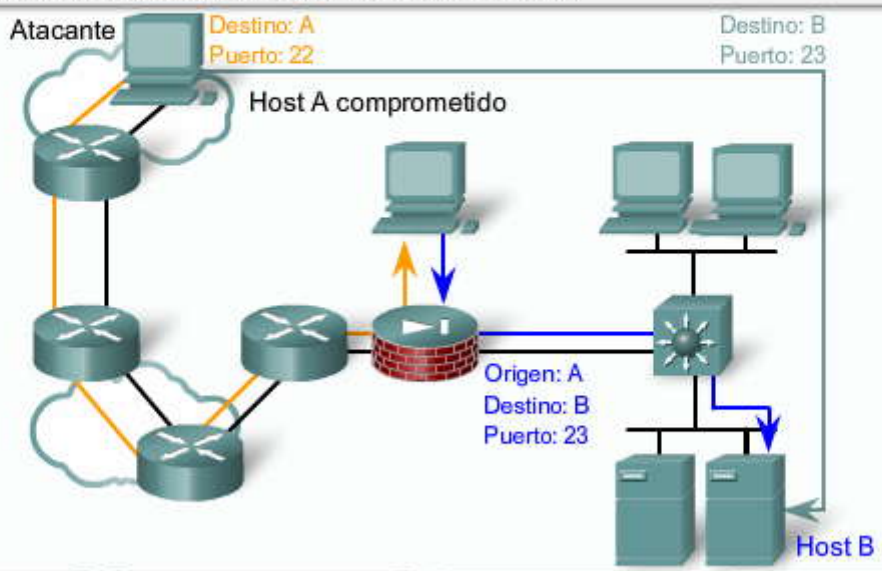


Ataque a la contraseña | **Explotación de confianza** | Reorientación de puertos | Ataque man-in-the-middle



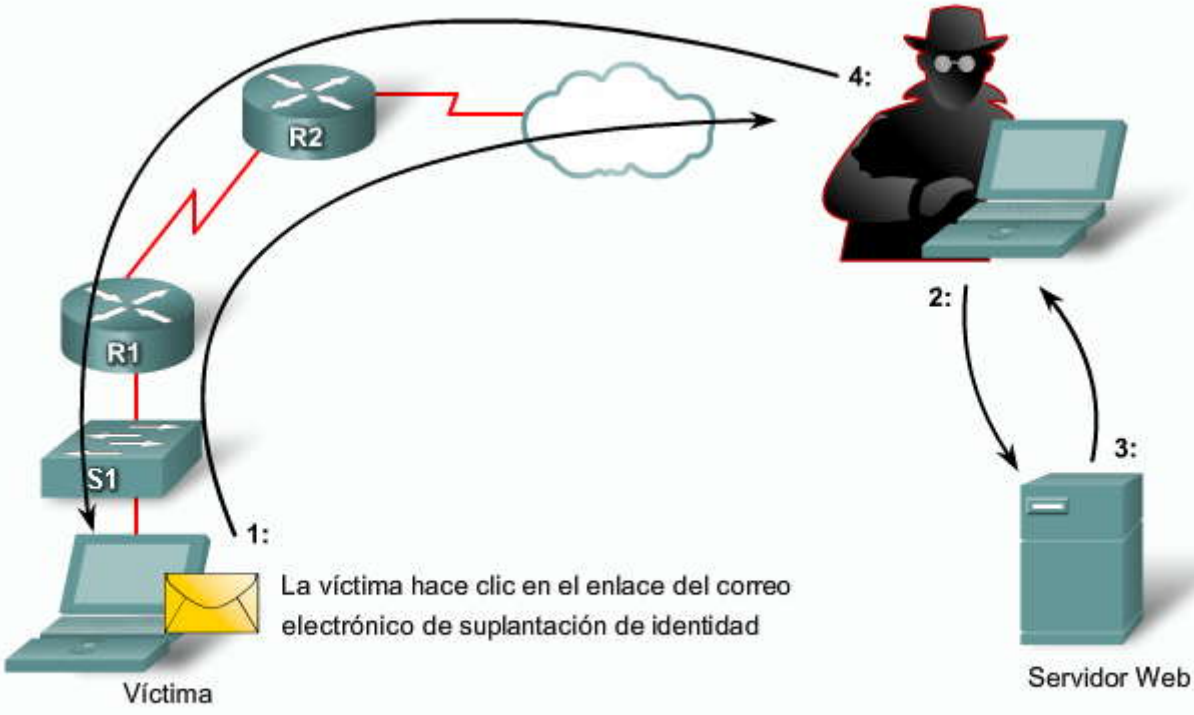
Ataques con acceso

La reorientación de puertos es un tipo de ataque de explotación de confianza que utiliza un host comprometido para pasar tráfico a través de un firewall que, en otro caso, lo hubiera detenido. En general, se mitiga mediante el uso de modelos de confianza correctos. Los software antivirus y los IDS basados en hosts pueden ayudar a detectar al atacante y a evitar que instale utilidades reorientadoras de puerto en el host.



Ataque a la contraseña | Explotación de confianza | Reorientación de puertos | Ataque man-in-the-middle

Ataques con acceso



Ataque a la contraseña | Explotación de confianza | Reorientación de puertos | Ataque man-in-the-middle

Ataques de DoS

Son la forma más promocionada de ataques y también están entre los más difíciles de eliminar. Incluso dentro de la comunidad de agresores, los ataques de DoS son clasificados como triviales y se consideran de mal gusto, porque requieren muy poco esfuerzo para su ejecución. No obstante, debido a su fácil implementación y al daño potencialmente significativo, los ataques de DoS merecen especial atención de los administradores de seguridad.

Los ataques de DoS adoptan muchas formas. En definitiva, impiden que las personas autorizadas utilicen un servicio consumiendo recursos del sistema. A continuación, se incluyen algunos ejemplos de amenazas DoS comunes:

Haga clic en el botón Ping de la muerte de la figura.

Los ataques de ping de la muerte cobraron popularidad hacia fines de la década de 1990. Aprovecharon las vulnerabilidades de los sistemas operativos más antiguos. Estos ataques modificaron la parte IP de un encabezado de paquete de ping para indicar que hay más datos en el paquete de los que realmente había. Un ping normalmente tiene de 64 a 84 bytes, mientras que uno de la muerte podría tener hasta 65 535 bytes. Enviar un ping de este tamaño puede colapsar una computadora objetivo más antigua. La mayoría de las redes ya no son susceptibles de sufrir este tipo de ataque.

Haga clic en el botón Saturación SYN de la figura.

Un ataque de saturación SYN explota el protocolo de enlace de tres vías TCP. Implica enviar varias peticiones de SYN (más de 1000) a un servidor objetivo. El servidor responde con la respuesta habitual SYN-ACK, pero el host malicioso nunca responde con el ACK final para terminar el protocolo de enlace. Esto paraliza el servidor hasta que finalmente se queda sin recursos y no puede responder a un pedido válido de host.

Los otros tipos de ataques DoS incluyen:

- **Bombas de correo electrónico**: los programas envían mensajes de correo electrónico masivo a personas, listas o dominios, y monopolizan los servicios de correo electrónico.
- **Applets maliciosos**: son los programas Java, JavaScript o ActiveX que destruyen o paralizan los recursos informáticos.

Ataques DDos

Los ataques de DoS distribuida (DDoS) están diseñados para saturar los enlaces de la red con datos legítimos. Estos datos pueden sobrecargar un enlace de Internet y hacer que el tráfico legítimo sea descartado. DDoS utiliza métodos de ataque similares a los ataques DoS estándar, pero opera a una escala mucho mayor. Generalmente, cientos o miles de puntos de ataque intentan saturar un objetivo.

Haga clic en el botón DDoS de la figura.

Por lo general, un ataque DDoS tiene tres componentes.

- Hay un Cliente que habitualmente es una persona que lanza el ataque.
- Un Manipulador es un host comprometido que está ejecutando el programa del agresor y cada Manipulador es capaz de controlar varios Agentes
- Un Agente es un host comprometido que ejecuta el programa del agresor y es responsable de generar un flujo de paquetes que se dirige hacia la víctima deseada.

Entre los ejemplos de ataques DDoS se pueden mencionar los siguientes:

- Ataque SMURF
- Red de saturación grupal (TFN)
- Stacheldraht
- MyDoom

Haga clic en el botón Ataque Smurf de la figura.

Los ataques Smurf utilizan mensajes ping de broadcast suplantados para saturar un sistema objetivo. Comienza cuando un agresor envía una gran cantidad de peticiones de eco ICMP a la dirección de broadcast de la red desde direcciones IP de origen suplantadas válidas. Un router podría ejecutar la función broadcast de Capa 3 a broadcast de Capa 2, la mayoría de los hosts responde uno por uno con una respuesta de eco ICMP, lo cual multiplica el tráfico por la cantidad de hosts que respondan. En una red multiacceso de broadcast, potencialmente podría haber cientos de máquinas que contesten a cada paquete de eco.

Por ejemplo, suponga que la red tiene 100 hosts y que el agresor tiene un enlace T1 de alto rendimiento. El agresor envía un flujo de 768 kbps de paquetes de solicitud de eco ICMP con una dirección origen suplantada de la víctima a la dirección de broadcast de una red objetivo (denominada sitio de rebote). Estos paquetes de pings llegan al sitio de rebote de la red de broadcast de 100 hosts, y cada uno lleva el paquete y responde a él, lo que crea 100 respuestas de ping de salida. Se utiliza un total de 76,8 megabits por segundo (Mbps) de ancho de banda hacia afuera desde el sitio de rebote después que el tráfico se multiplica. A continuación, esto se envía a la víctima o al origen suplantado de los paquetes que se originen.

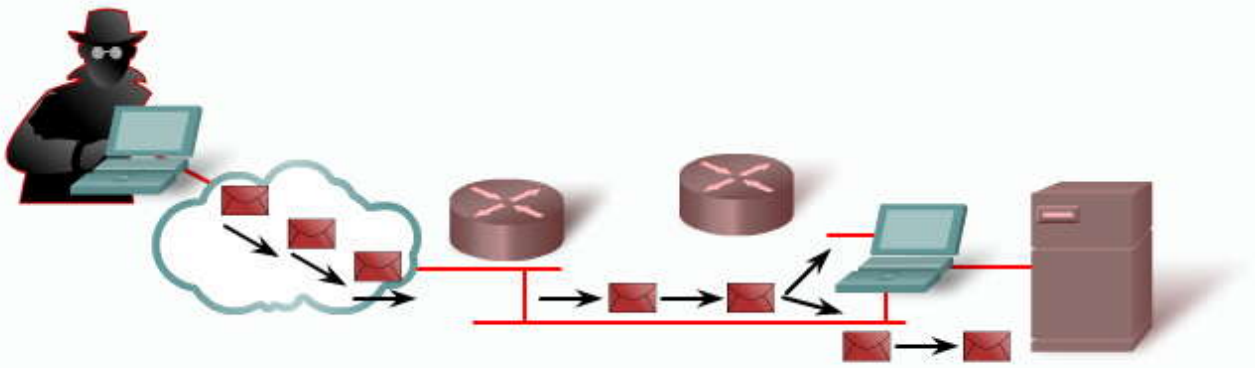
La desactivación de la capacidad de broadcast dirigido de la infraestructura de la red impide que la red sea utilizada como sitio de rebote. La capacidad de broadcast dirigida viene desactivada de manera predeterminada en el software IOS de Cisco desde la versión 12.0.

Los ataques de DoS y DDoS pueden ser mitigados implementando listas de control de acceso especiales contra la suplantación y contra la DoS. Los ISP también pueden implementar una velocidad del tráfico, que limite la cantidad de tráfico no fundamental que atraviesa los segmentos de la red. Un ejemplo común consiste en limitar la cantidad detráfico de ICMP cuyo ingreso está permitido en una red, porque este tráfico se utiliza sólo a los fines de realizar diagnósticos.

Los detalles del funcionamiento de estos ataques exceden el alcance de este curso. Para obtener información, consulte el curso Seguridad de la Red de la Academia de Networking.

Ataques de DoS y de DDoS

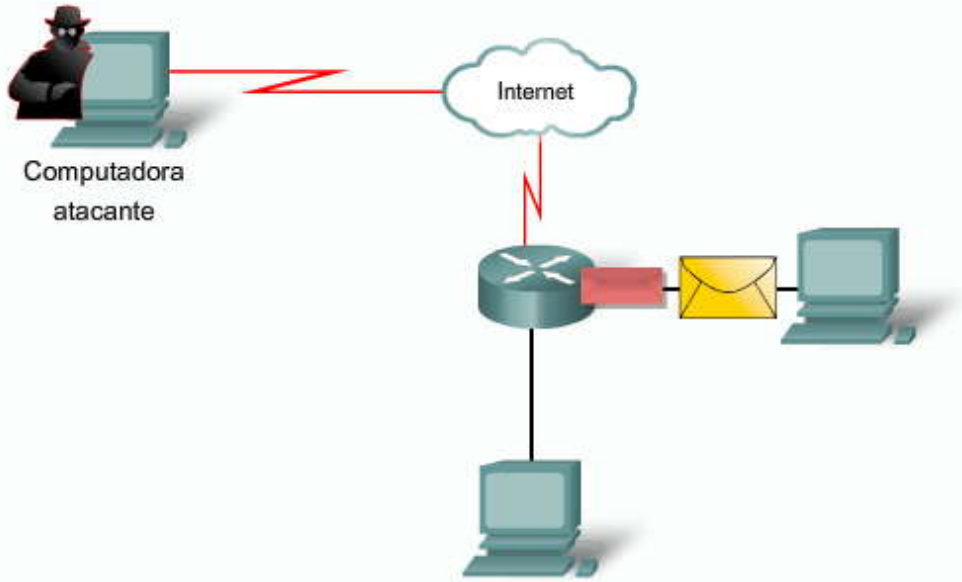
Sobrecargas de recursos	Datos mal formados
Espacio en disco, ancho de banda, búferes	Paquetes de tamaños excesivos como el ping de la muerte
Saturación de ping como el smurf	Paquete superpuesto como el winuke
Tormentas de paquetes como las bombas UDP y fraggle	Datos no gestionados como el teardrop



Los ataques de DoS evitan que el personal autorizado use un servicio mediante la utilización de los recursos del sistema.

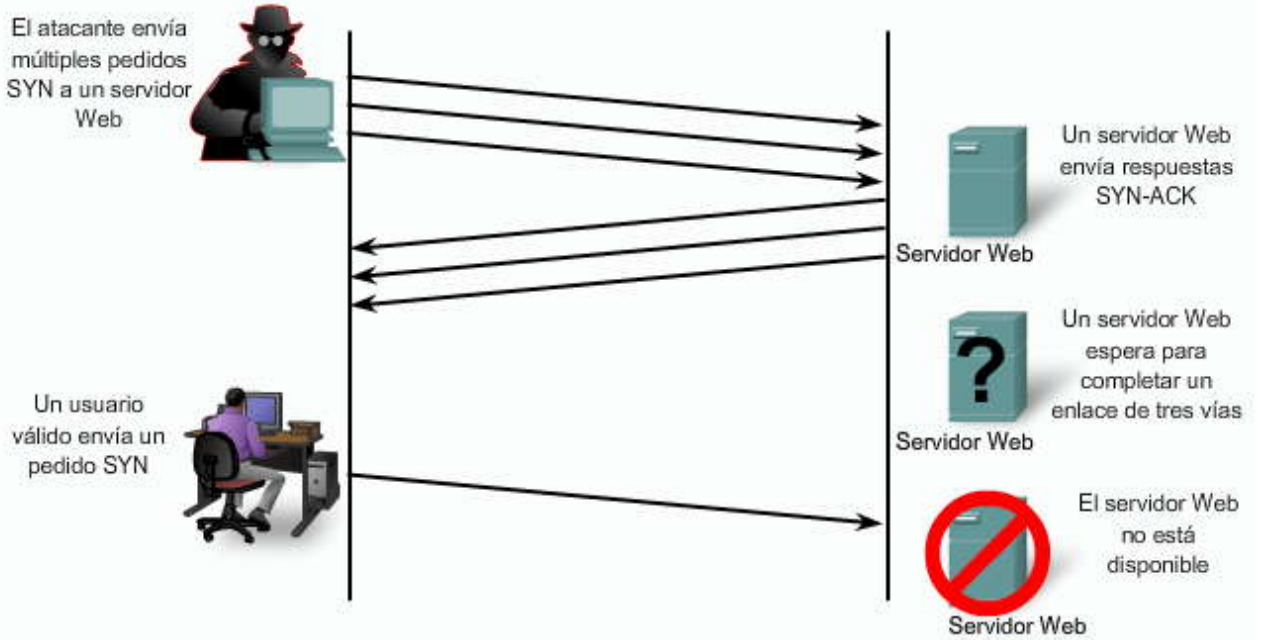
Ataque de DoS | Ping de la muerte | Saturación SYN | DDoS | Ataque Smurf

Ataques de DoS y de DDoS

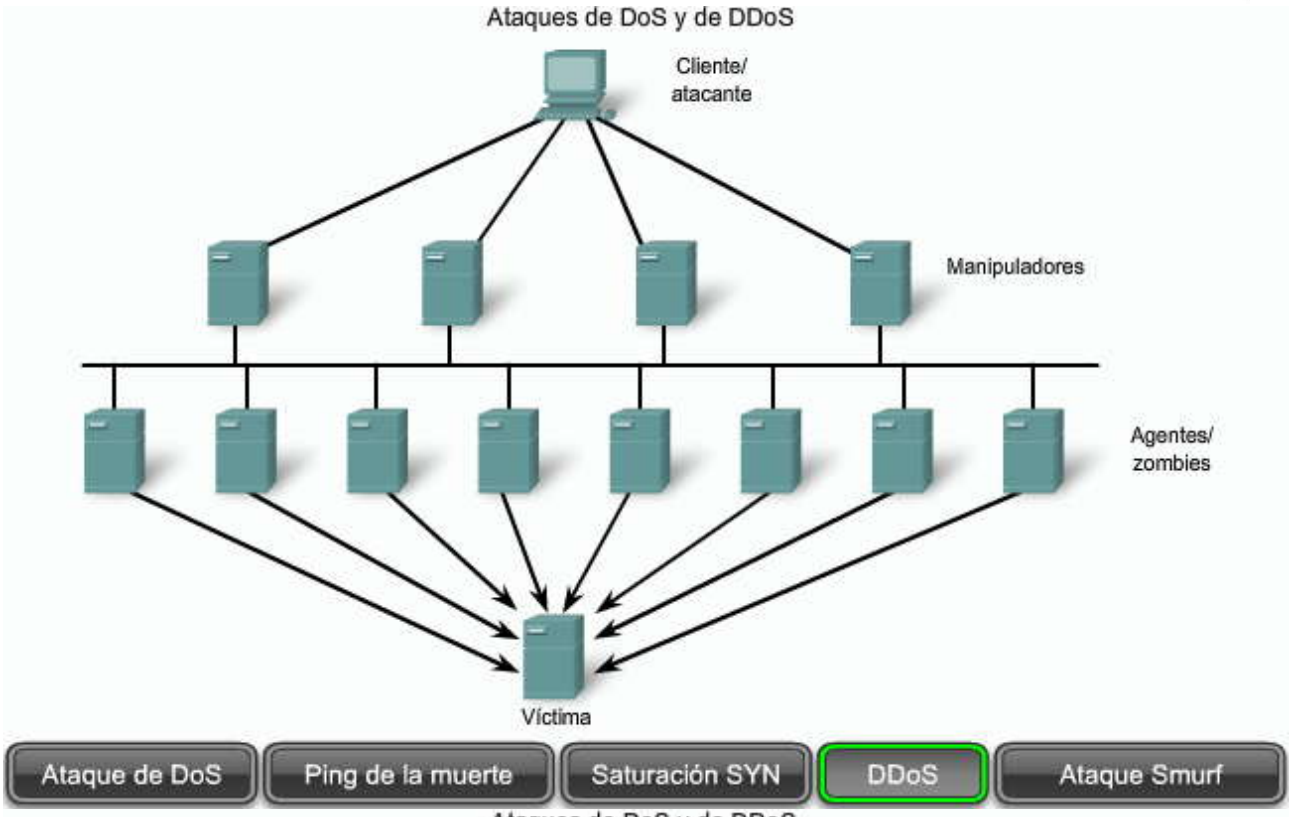


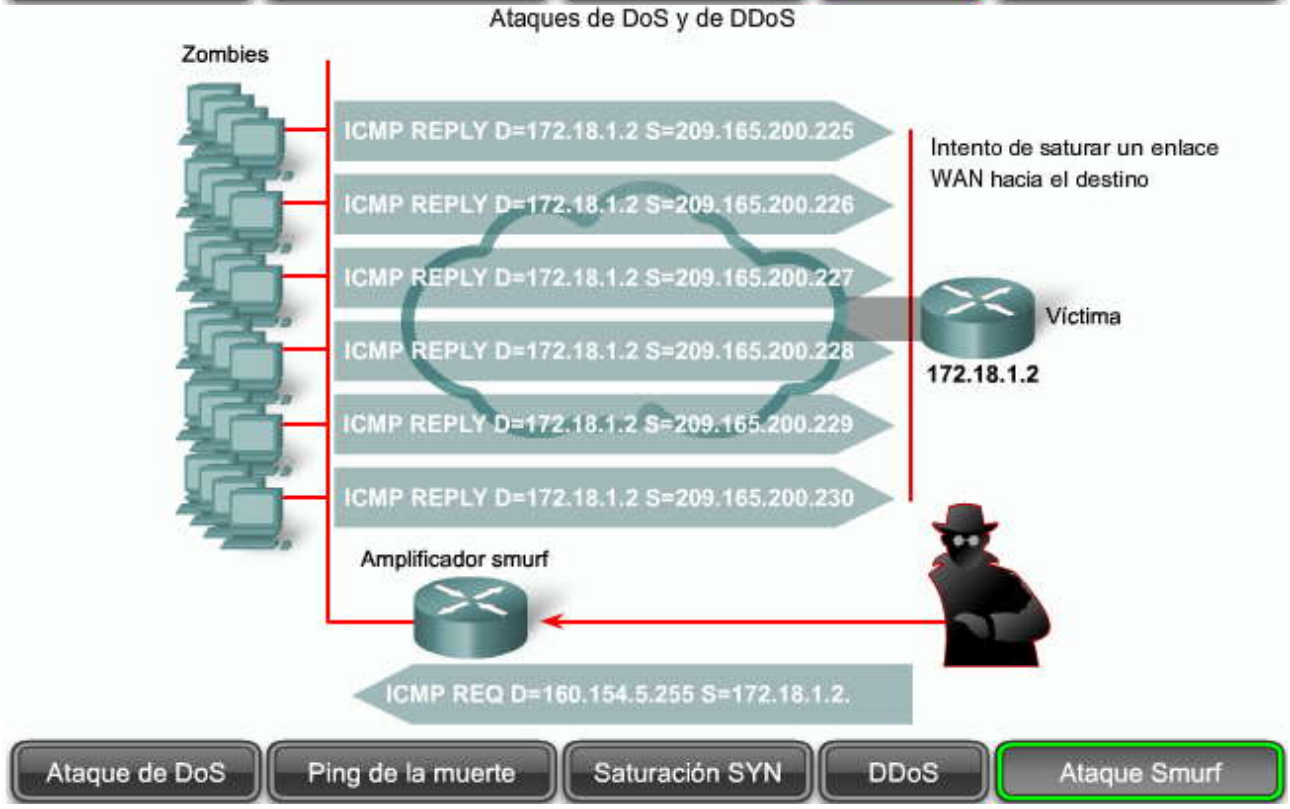
Ataque de DoS | Ping de la muerte | Saturación SYN | DDoS | Ataque Smurf

Ataques de DoS y de DDoS



Ataque de DoS | Ping de la muerte | Saturación SYN | DDoS | Ataque Smurf





Ataques de código malicioso

Las principales vulnerabilidades de las estaciones de trabajo de los usuarios finales son los ataques de gusanos, virus y caballos de Troya.

Un gusano ejecuta un código e instala copias de sí mismo en la memoria de la computadora infectada, lo que, a su vez, puede infectar a otros hosts.

Un virus es software malicioso asociado a otro programa, con el propósito de ejecutar una función particular no deseada en una estación de trabajo.

Un caballo de Troya es distinto de un gusano o de un virus sólo en el sentido de que toda la aplicación fue escrita para que tenga la apariencia de otra cosa, cuando en realidad es una herramienta de ataque.

Gusano

La anatomía de un ataque de un gusano es la siguiente:

- **La vulnerabilidad que lo hace posible**: un gusano se instala a sí mismo explotando las vulnerabilidades conocidas de los sistemas, como usuarios finales ingenuos que abren archivos adjuntos ejecutables no verificados de correos electrónicos.
- **Mecanismo de propagación**: tras obtener acceso a un host, un gusano se copia a sí mismo en dicho host y, a continuación, selecciona nuevos objetivos.
- **Contenido**: una vez que el host está infectado con un gusano, el agresor obtiene acceso al host, frecuentemente como usuario privilegiado. Los agresores podrían utilizar una explotación local para elevar su nivel de privilegio al de administrador.

Por lo general, los gusanos son programas independientes que atacan un sistema e intentan explotar una vulnerabilidad específica del objetivo. Si se logra explotar correctamente la vulnerabilidad, el gusano copia su programa del host agresor al sistema recientemente explotado para comenzar nuevamente el ciclo. En enero de 2007, un gusano infectó la popular comunidad MySpace. Los usuarios que no sospecharon facilitaron la propagación del gusano, que comenzó a reproducirse a sí mismo en los sitios de los usuarios con la alteración "w0rm.EricAndrew".

Para mitigar los ataques de gusanos, se requiere agilidad por parte del personal de administración del sistema y de la red. La coordinación entre el personal de administración del sistema, de ingeniería de la red y de las operaciones de seguridad es fundamental para responder con eficacia a un incidente ocasionado por un gusano. Se recomienda llevar a cabo los siguientes pasos para mitigar los ataques de gusanos:

- **Contención**: contener la propagación del gusano en la red y dentro de ella. Compartimentar las partes no infectadas de la red.
- **Inoculación**: comenzar a colocar parches en todos los sistemas y, si fuera posible, buscar sistemas vulnerables.
- **Cuarentena**: realizar un seguimiento de cada máquina infectada dentro de la red. Desconectar, quitar o bloquear las máquinas infectadas de la red.
- **Tratamiento**: limpiar y colocar parches en cada uno de los sistemas infectados. Es posible que algunos gusanos requieran reinstalar todo el sistema central para limpiar el sistema.

Virus y caballos de Troya

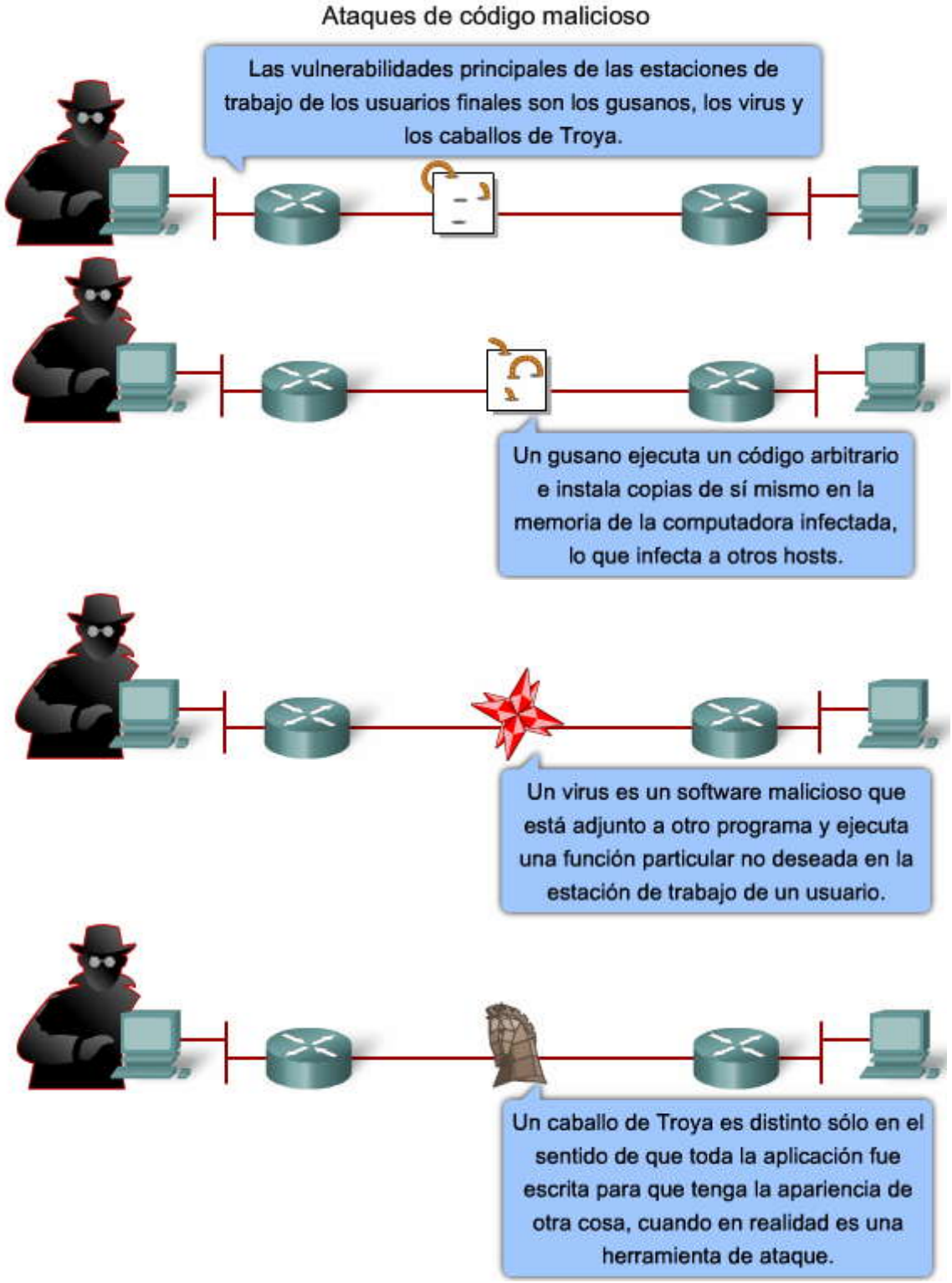
Un virus es software malicioso asociado a otro programa para ejecutar una función particular no deseada en una estación de trabajo. Un ejemplo es un programa asociado a command.com (el intérprete principal de los sistemas de Windows) y elimina determinados archivos e infecta las demás versiones de command.com que puede encontrar.

Un caballo de Troya es distinto sólo en el sentido de que toda la aplicación fue escrita para que tenga la apariencia de otra cosa, cuando en realidad es una herramienta de ataque. Un ejemplo de caballo de Troya es una aplicación de software que ejecuta un juego sencillo en una estación de trabajo. Mientras que el usuario está ocupado con el juego, el caballo de Troya envía por correo una copia de sí mismo a cada dirección de la libreta de direcciones del usuario. Los otros usuarios reciben el juego y lo ejecutan y, de esa manera, propagan el caballo de Troya a las direcciones de cada libreta de direcciones.

Por lo general, un virus requiere un mecanismo de entrega, un vector, como puede ser un archivo comprimido o algún otro archivo ejecutable adjunto a un correo electrónico para transportar el código del virus de un sistema a otro. El elemento clave que distingue un gusano informático de un virus informático es que, para la propagación de un virus, se necesita interacción humana.

Estos tipos de aplicaciones pueden ser contenidos a través del uso eficaz de software antivirus a nivel del usuario y, potencialmente, a nivel de la red. El software antivirus puede detectar la mayoría de los virus y muchas aplicaciones de caballos de Troya e impedir su propagación en la red. Estar actualizado en materia de las últimas evoluciones de estos tipos de ataques también puede ayudar a adoptar una postura más eficaz respecto de estos ataques. A medida que se lanzan nuevas aplicaciones de virus o caballos de Troya, las empresas necesitan mantenerse actualizadas con las últimas versiones de software antivirus.

Sub7, o subseven, es un caballo de Troya común que instala un programa de puerta trasera en los sistemas de los usuarios. Es muy común, tanto en el caso de los ataques estructurados como en el de los no estructurados. Como amenaza no estructurada, los agresores sin experiencia pueden utilizar el programa para hacer desaparecer los cursores del mouse. Como amenaza estructurada, los crackers pueden utilizarlo para instalar capturadores de pulsaciones (programas que registran todas las pulsaciones de teclas de los usuarios) para capturar información confidencial.



4.1.4 Técnicas generales de mitigación

Seguridad basada en hosts y en servidores

Aseguramiento de dispositivos

Cuando se instala un nuevo sistema operativo en una computadora, la configuración de seguridad se establece en los valores predeterminados. En la mayoría de los casos, este nivel de seguridad no es apropiado. Se deben adoptar algunos pasos sencillos, que se aplican a todos los sistemas operativos:

- Los nombres de usuario y las contraseñas predeterminados deben cambiarse de inmedato.
- Se debe restringir el acceso a los recursos del sistema exclusivamente a las personas autorizadas para utilizar esos recursos.
- Se deben desconectar y desinstalar los servicios y las aplicaciones innecesarios, siempre que sea posible.

En la Sección 4.2 "Seguridad de los routers Cisco", se describe el aseguramiento de los dispositivos en forma más detallada.

Es fundamental proteger los hosts de la red, como las PC y los servidores de la estación de trabajo. Estos hosts deben asegurarse cuando se agregan a la red, y deben actualizarse con parches de seguridad, a medida que estas actualizaciones estén disponibles. Se pueden adoptar pasos adicionales para asegurar estos hosts. Los antivirus, firewalls y la detección de intrusiones son herramientas valiosas que se pueden utilizar para asegurar los hosts de la red. Dado que muchos recursos de la empresa pueden estar contenidos en un único servidor de archivos, es particularmente importante que se pueda acceder a los servidores y que estén disponibles.

Software antivirus

Instale software antivirus de host para protegerse contra virus conocidos. El software antivirus puede detectar la mayoría de los virus y muchas aplicaciones de caballos de Troya e impedir su propagación en la red.

El software antivirus hace esto de dos maneras:

- Escanea archivos y compara su contenido con virus conocidos en un diccionario de virus. Las coincidencias se marcan de una manera definida por el usuario final.
- Controla los procesos sospechosos que se ejecutan en un host que podrían ser indicativos de la presencia de una infección. Este control podría incluir capturas de datos, monitoreo de puertos y otros métodos.

La mayoría del software antivirus comercial utiliza estos dos enfoques.

Haga clic en el botón Antivirus de la figura.

Actualice el software antivirus prestando mucha atención.

Firewall personal

Las PC conectadas a Internet mediante una conexión dial-up, DSL o cable módem son tan vulnerables como las redes empresariales. Los firewalls personales residen en la PC del usuario e intentan impedir ataques. Los firewalls personales no están diseñados para las implementaciones de la LAN, como firewalls basados en aplicaciones o basados en servidores, y pueden impedir el acceso a la red si se instalan con otros clientes, servicios, protocolos o adaptadores de networking.

Haga clic en el botón Firewalls personales de la figura.

Algunos de los proveedores de software de firewalls personales incluyen McAfee, Norton, Symantec y Zone Labs.

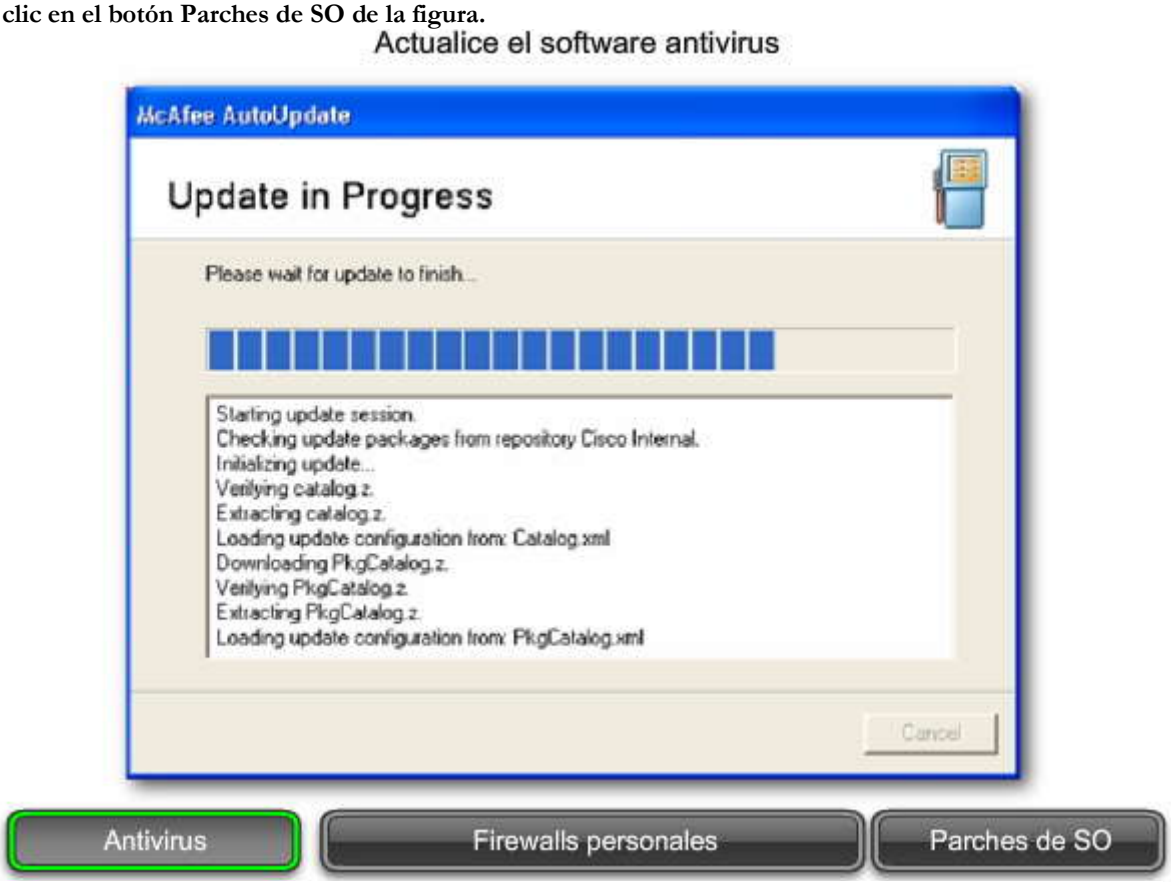
Parches para sistemas operativos

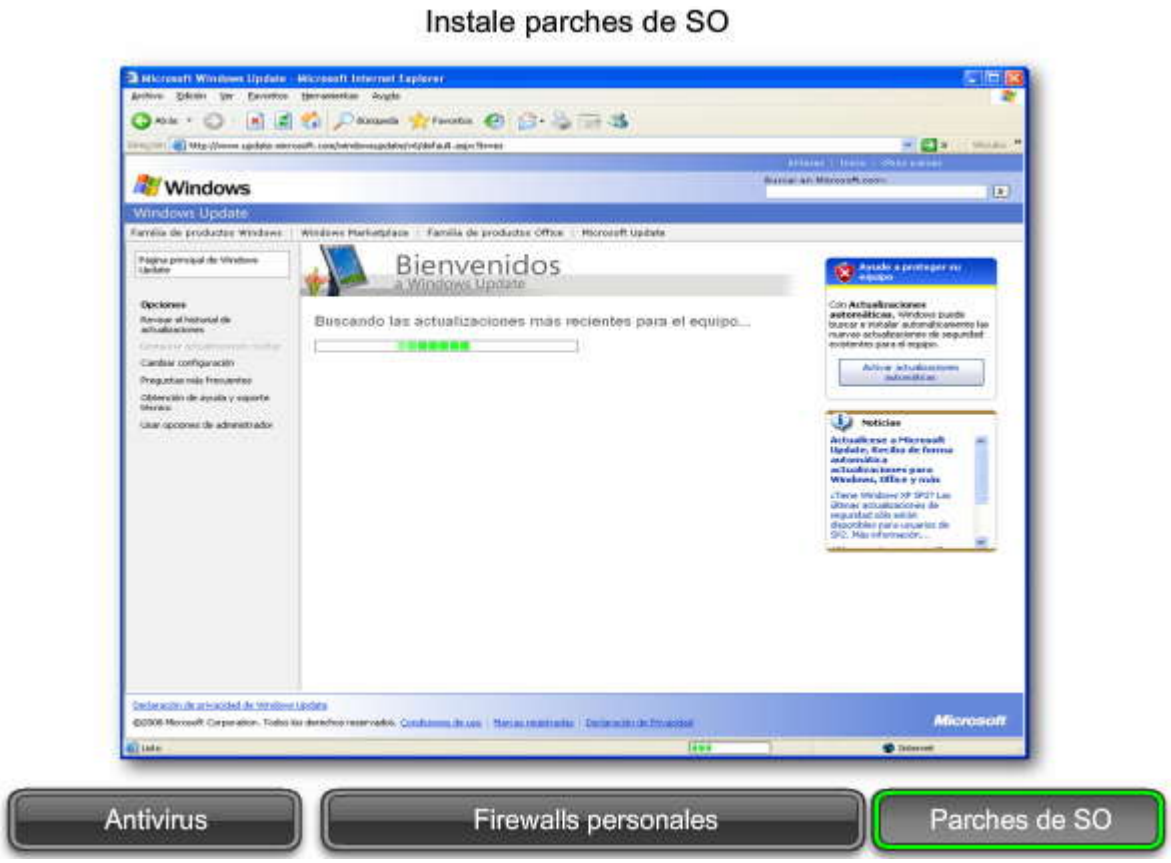
La forma más eficaz de mitigar un gusano y sus variantes es descargar las actualizaciones de seguridad del proveedor del sistema operativo e instalar parches en todos los sistemas vulnerables. Es difícil en el caso de sistemas de usuarios no controlados de la red local, y es aun más problemático si estos sistemas están conectados de manera remota a la red mediante una red privada virtual (VPN) o un servidor de acceso remoto (RAS). La administración de varios sistemas implica la creación de una imagen estándar del software (sistema operativo y aplicaciones reconocidas cuyo uso está autorizado en sistemas cliente implementados) que se implementa en sistemas nuevos o actualizados. Es posible que estas imágenes no contengan los últimos parches, y el proceso de volver a crear la imagen continuamente para integrar el parche más reciente puede convertirse rápidamente en una tarea que demanda mucho tiempo desde un punto de vista administrativo. Colocar parches en todos los sistemas requiere que dichos sistemas estén de alguna manera conectados a la red, lo que puede no ser posible.

Una solución a la administración de parches de seguridad críticos consiste en crear un servidor central de parches con el cual todos los sistemas deben comunicarse después de un período determinado. Los parches que no se aplican a un host se descargan automáticamente del servidor de parches y se instalan sin la intervención del usuario.

Además de realizar actualizaciones de seguridad desde el proveedor del SO, la determinación de qué servicios se pueden explotar puede ser simplificada por el uso de herramientas de auditoría de seguridad que buscan vulnerabilidades.

Haga clic en el botón Parches de SO de la figura.





Detección y prevención de intrusiones

Los sistemas de detección de intrusión (IDS) detectan ataques contra una red y envían registros a una consola de administración. Los sistemas de prevención de intrusión (IPS) impiden ataques contra la red y deben proporcionar los siguientes mecanismos activos de defensa además de la detección:

- **Prevención**: impide la ejecución del ataque detectado.
- **Reacción**: inmuniza el sistema contra ataques futuros de origen malicioso.

Cada tecnología puede ser implementada a nivel de la red o a nivel del host, o a ambos niveles para brindar máxima protección.

Sistemas de detección de intrusión basada en hosts

Por lo general, la intrusión basada en hosts se implementa como tecnología de línea interna o pasiva, según el proveedor.

La tecnología pasiva, que fue la tecnología de primera generación, se denomina sistema de detección de intrusión basada en hosts (HIDS). HIDS envía registros a una consola de administración una vez que se produjo el ataque y se provocó el daño.

La tecnología de línea interna, denominada sistema de prevención de intrusión basada en hosts (HIPS), realmente detiene el ataque, impide el daño y bloquea la propagación de gusanos y virus.

La detección activa puede configurarse para apagar la conexión de la red o para detener los servicios afectados automáticamente. Se pueden tomar medidas correctivas inmediatamente. Cisco proporciona HIPS mediante el software del agente de seguridad de Cisco.

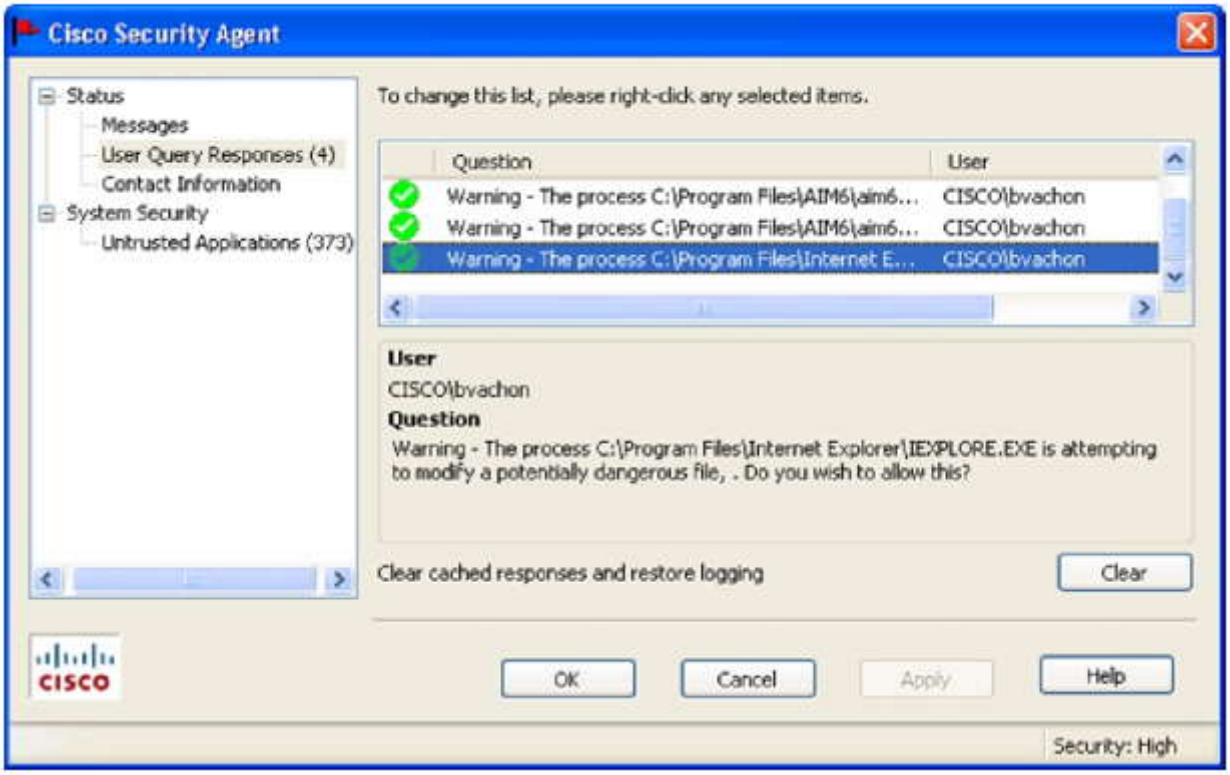
El software del HIPS debe ser instalado en cada host, ya sea el servidor o la pc de escritorio, para controlar las actividades realizadas en el host y en contra de éste. Este software se denomina software agente. El software agente realiza el análisis de la detección y la prevención de intrusión. El software agente también envía registros y alertas a un servidor centralizado de política/administración.

La ventaja del HIPS es que puede controlar los procesos del sistema operativo y proteger los recursos críticos del sistema, incluidos los archivos que pueden existir sólo en ese host específico. Esto significa que puede notificar a los administradores

de la red cuando un proceso externo intenta modificar un archivo del sistema para incluir un programa oculto de puerta trasera.

La figura ejemplifica una implementación típica del HIPS. Los agentes se instalan en los servidores de acceso público y en los servidores empresariales de correo y de aplicaciones. El agente denuncia eventos a un servidor de consola central ubicado en el interior del firewall corporativo. Como alternativa, los agentes del host pueden enviar registros como correo electrónico a un administrador.

Detección y prevención de intrusiones



Aplicaciones y dispositivos de seguridad comunes

La seguridad es un aspecto primordial que se debe tener en cuenta al planificar una red. En el pasado, el único dispositivo que se tenía en cuenta con respecto a la seguridad de la red era el firewall. El firewall, por sí solo, ya no es apropiado para garantizar la seguridad de la red. Se requiere un enfoque integrado que incluya un firewall, prevención de intrusión y VPN.

Un enfoque integrado en cuanto a la seguridad (además de los dispositivos necesarios para lograrla) respeta los siguientes bloques básicos:

Control de amenazas: regula el acceso a la red, aísla los sistemas infectados, previene intrusiones y protege los bienes al contrarrestar el tráfico malicioso, como los gusanos y los virus. Los siguientes dispositivos proporcionan soluciones para el control de amenazas:

- Aplicaciones de seguridad adaptables ASA de la serie 5500 de Cisco
- Routers de servicios integrados (ISR)
- Control de admisión a la red
- Agente de seguridad de Cisco para equipos de escritorio
- Sistemas de prevención de intrusión de Cisco

Comunicaciones seguras: asegura los extremos de la red con VPN. Los dispositivos que permiten que una organización implemente una VPN son los routers ISR Cisco con la solución de VPN del IOS de Cisco, los dispositivos de la serie ASA 5500 de Cisco y los switches Catalyst 6500 de Cisco.

Control de admisión a la red (NAC): proporciona un método basado en funciones que impide el acceso no autorizado a una red. Cisco ofrece una aplicación de NAC.

El Software IOS de Cisco de los Routers de servicios integrados (ISR) de Cisco

Cisco proporciona muchas de las medidas de seguridad necesarias para los clientes dentro del software IOS de Cisco. El software IOS de Cisco cuenta con el Firewall IOS de Cisco, IPsec, VPN de SSL y servicios de IPS.

Aplicación de seguridad adaptable ASA de la serie 5500 de Cisco

En un momento, el firewall PIX era el único dispositivo que una red segura podía implementar. El PIX evolucionó hasta convertirse en una plataforma que integra muchas características de seguridad diferentes, denominada Aplicación de seguridad adaptable (ASA) de Cisco. El ASA de Cisco cuenta con un firewall, seguridad de voz, VPN de SSL e IPsec, IPS y servicios de seguridad de contenidos en un solo dispositivo.

Sensores IPS de la serie 4200 de Cisco

En las redes más grandes, los sensores IPS de la serie 4200 de Cisco proporcionan un sistema de prevención de intrusiones de línea interna. Este sensor identifica, clasifica y detiene el tráfico malicioso de la red.

Aplicación de NAC de Cisco

La aplicación de NAC de Cisco utiliza la infraestructura de la red para hacer cumplir la política de seguridad respecto de todos los dispositivos que intentan obtener acceso a los recursos informáticos de la red.

Agente de seguridad de Cisco (CSA)

El software del Agente de seguridad de Cisco ofrece capacidades de protección contra amenazas para sistemasinformáticos de servidor, escritorio y punto de servicio (POS). CSA defiende estos sistemas contra ataques planificados, spyware, rootkits y ataques de día cero.

La cobertura exhaustiva de estas aplicaciones excede el alcance de este curso. Consulte el CCNP para obtener más información sobre los cursos: Implementación de redes seguras y convergentes de área amplia y Seguridad de la red 1 y 2.

4.1.5 La rueda de seguridad de la red

La mayoría de los incidentes de seguridad se producen porque los administradores de sistemas no implementan las medidas correctivas disponibles, y los agresores o los empleados descontentos explotan el descuido. Por lo tanto, el problema no es solamente confirmar la existencia de una vulnerabilidad técnica y encontrar una medida correctiva que funcione, también es fundamental verificar que dicha medida se implemente y funcione correctamente.

Para ayudar en el cumplimiento de una política de seguridad, la Rueda de seguridad, un proceso continuo, ha demostrado ser un enfoque eficaz. La Rueda de seguridad promueve la repetición de las pruebas y de la aplicación de medidas de seguridad actualizadas continuamente.

Para comenzar con el proceso de la Rueda de seguridad, en primer lugar, desarrolle una política de seguridad que permita la aplicación de medidas de seguridad. Una política de seguridad tiene las siguientes funciones:

- Identificar los objetivos de seguridad de la organización.
- Documentar los recursos que se deben proteger.
- Identificar la infraestructura de la red con mapas e inventarios actuales.
- Identificar los recursos críticos que deben protegerse, como recursos de investigación y desarrollo, financieros y humanos. Esto se denomina análisis de riesgo.

La política de seguridad es el hub en el cual se basan los cuatro pasos de la Rueda de seguridad. Los pasos son asegurar, controlar, probar y mejorar.

Paso 1: Asegurar

Asegurar la red mediante la aplicación de la política de seguridad y de las siguientes soluciones de seguridad:

- **Defensa contra amenazas**
- **Inspección con estado y filtrado de paquetes**: filtre el tráfico de la red para permitir solamente tráfico y servicios válidos.

Nota: La inspección con estado hace referencia a un firewall que mantiene la información del estado de una conexión en una tabla de estados, a fin de que pueda reconocer los cambios en la conexión que podrían indicar que un agresor está intentando apropiarse de una sesión o manipular una conexión.

- **Sistemas de prevención de intrusión**: impleméntelos a nivel de la red y del host para detener el tráfico malicioso en forma activa.
- **Parches para vulnerabilidades**: aplique modificaciones o medidas para detener la explotación de las vulnerabilidades conocidas.
- **Desactivación de los servicios innecesarios**: cuanto menor sea la cantidad de servicios activados, más difícil será para los agresores obtener acceso.

Conectividad segura

- **VPN**: encripte el tráfico de la red para impedir la divulgación no deseada a personas no autorizadas o maliciosas.
- **Confianza e identidad**: implemente restricciones estrictas sobre los niveles de confianza dentro de una red. Por ejemplo, los sistemas que se encuentran dentro de un firewall no pueden confiar completamente en los sistemas que se encuentran fuera de un firewall.
- **Autenticación**: proporcione acceso sólo a los usuarios autorizados. Un ejemplo de esto es el uso de contraseñas que se pueden utilizar por única vez.
- **Cumplimiento de políticas**: asegúrese de que los usuarios y los dispositivos finales cumplan con la política de la empresa.

Paso 2: Controlar

Controlar la seguridad involucra métodos activos y pasivos de detectar violaciones de seguridad. El método activo más utilizado es la auditoría de los archivos de registro a nivel del host. La mayoría de los sistemas operativos incluyen la función de auditoría. Los administradores de sistemas deben activar el sistema de auditoría para cada uno de los hosts de la red y tomarse el tiempo necesario para controlar e interpretar las entradas de los archivos de registro.

Entre los métodos pasivos se encuentra el uso de dispositivos IDS para detectar intrusiones automáticamente. Este método requiere menos atención por parte de los administradores de seguridad de la red que los métodos activos. Estos sistemas pueden detectar violaciones a la seguridad en tiempo real y se pueden configurar para responder automáticamente antes de que un intruso provoque daños.

Un beneficio adicional del control de la red es la verificación de que las medidas de seguridad implementadas en el paso 1 de la Rueda de seguridad se hayan configurado y estén funcionando correctamente.

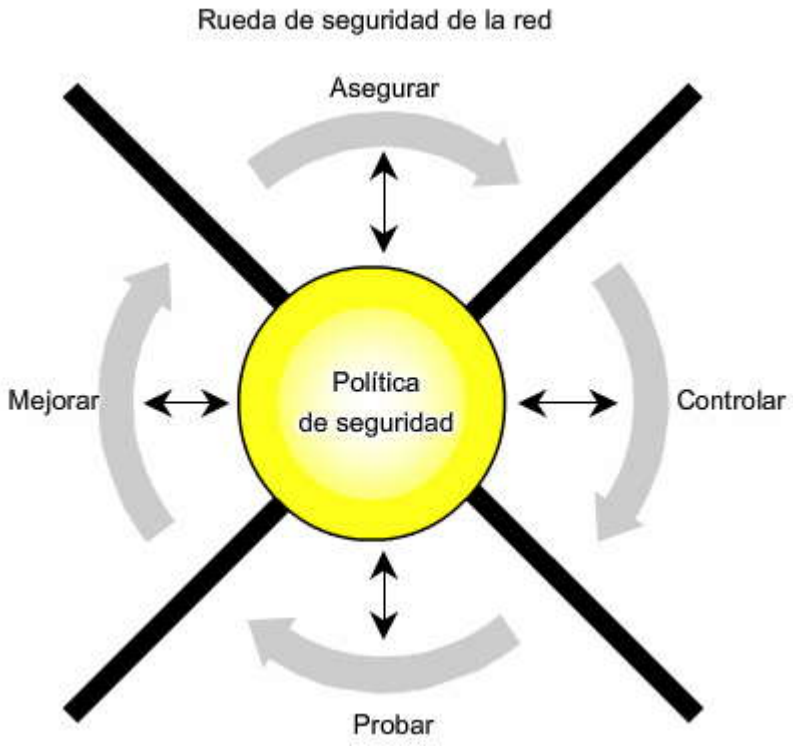
Paso 3: Probar

En la fase de pruebas de la Rueda de seguridad, las medidas de seguridad se someten a pruebas de manera proactiva. Particularmente, se verifica la funcionalidad de las soluciones de seguridad implementadas en el paso 1 y los métodos de auditoría y detección de intrusión del sistema implementados en el paso 2. Las herramientas de evaluación de las vulnerabilidades, como SATAN, Nessus o Nmap son útiles para probar las medidas de seguridad de la red periódicamentea nivel de la red o del host.

Paso 4: Mejorar

La fase de mejoras de la Rueda de seguridad implica el análisis de los datos recopilados durante las fases de control y de prueba. Este análisis contribuye al desarrollo y a la implementación de mecanismos de mejoras que intensifican la política de seguridad y tiene como consecuencia la adición de ítems al paso 1. Para mantener una red lo más segura posible, el ciclo de la Rueda de seguridad debe repetirse continuamente, porque todos los días aparecen nuevas vulnerabilidades y riesgos en la red.

Con la información compilada a partir de las fases de control y de pruebas, los IDS pueden ser utilizados para implementar mejoras a la seguridad. La política de seguridad debe modificarse a medida que se descubren nuevas vulnerabilidades y nuevos riesgos.



4.1.6 La política de seguridad de la empresa

¿Qué es una política de seguridad?

Una política de seguridad es un conjunto de pautas establecidas para proteger a la red de los ataques, ya sean desde el interior o desde el exterior de una empresa. Para elaborar una política se debe comenzar por formular preguntas. ¿De qué manera la red ayuda a la organización a lograr su visión, su misión y su plan estratégico? ¿Cuáles son las implicaciones que tienen los requisitos de la empresa en la seguridad de la red y de qué manera esos requisitos se traducen en la compra de equipos especializados y en las configuraciones que se cargan en los dispositivos?

Una política de seguridad favorece a una organización de las siguientes maneras:

- Proporciona un medio para auditar la seguridad actual de la red y compara los requisitos con lo que se encuentra instalado.
- Planifica mejoras de seguridad, incluidos equipos, software y procedimientos.
- Define las funciones y las responsabilidades de los ejecutivos, administradores y usuarios de la empresa.
- Define qué comportamientos están permitidos y cuáles no.
- Define un proceso para manejar los incidentes de seguridad de la red.
- Permite la implementación y el cumplimiento de la seguridad global al funcionar como norma entre los sitios.
- Crea una base para fundar acciones legales, en caso de ser necesario.

Una política de seguridad es un documento dinámico, en el sentido de que se trata de un documento que nunca está terminado y que se actualiza constantemente con los cambios operados en los requisitos de la tecnología y de los empleados. Actúa como puente entre los objetivos de administración y los requisitos específicos de la seguridad.

¿Qué es una política de seguridad?

"Una política de seguridad es una declaración formal de las reglas a las cuales se debe adherir el personal que tiene acceso a los bienes tecnológicos y de información de una organización".

(RFC 2196, Manual de seguridad de sitio)

Funciones de una política de seguridad

Una política de seguridad integral cumple las siguientes funciones esenciales:

- Protege a las personas y a la información
- Establece las normas de comportamiento esperado de los usuarios, de los administradores de sistemas, de la dirección y del personal de seguridad
- Autoriza al personal de seguridad a realizar controles, sondeos e investigaciones
- Define y autoriza las consecuencias de las violaciones

La política de seguridad es para todos, incluso para los empleados, contratistas, proveedores y clientes que tienen acceso a la red. Sin embargo, debe tratar a cada uno de estos grupos de manera diferente. A cada grupo sólo se le debe mostrar la parte de la política correspondiente a su trabajo y a su nivel de acceso a la red.

Por ejemplo, no siempre es necesario dar una explicación de por qué se hace algo. Puede suponer que el personal técnico ya sabe por qué se incluye un requisito particular. Es probable que los directivos no estén interesados en los aspectos técnicos de un requisito particular; ellos pueden querer sólo una descripción general de alto nivel o el principio en el cual se basa el requisito. Sin embargo, cuando los usuarios finales conocen la razón por la que se incluyó un control particular de seguridad, es más probable que respeten la política. Por lo tanto, seguramente un documento no va a satisfacer las necesidades de toda la audiencia de una organización grande.

Funciones de una política de seguridad

- Proteger a las personas y a la información
- Establecer la normas de comportamiento esperadas de los usuarios, de los administradores del sistema, de la dirección y del personal de seguridad
- Autorizar al personal de seguridad a monitorear, sondear e investigar
- Definir y autorizar las consecuencias de las violaciones

Componentes de una política de seguridad

El Instituto SANS (http://www.sans.org) proporciona pautas desarrolladas con la colaboración de una cantidad de empresas líderes de la industria, incluida Cisco, para desarrollar políticas de seguridad integrales para pequeñas y grandes organizaciones. No todas las organizaciones necesitan todas estas políticas.

A continuación, se describen las políticas de seguridad generales que pueden ser invocadas por una organización:

- **Declaración de autoridad y alcance**: define qué persona dentro de la organización propone la política de seguridad, quién es responsable de implementarla y qué áreas están contempladas por la política.
- **Política de uso aceptable (AUP)**: define el uso aceptable de los equipos y servicios informáticos y las medidas de seguridad de los empleados adecuadas para proteger los recursos corporativos y la información confidencial de la organización.
- **Política de identificación y autenticación**: define qué tecnologías usa la empresa para garantizar que sólo el personal autorizado obtenga acceso a sus datos.
- **Política de acceso a Internet**: define qué es lo que la empresa tolera y lo que no tolera con respecto al uso de su conectividad a Internet por parte de empleados e invitados.
- **Política de acceso al campus**: define el uso aceptable de los recursos tecnológicos del campus por parte de bs empleados y de los invitados.
- **Política de acceso remoto**: define la forma en la que los usuarios remotos pueden utilizar la infraestructura de acceso remoto de la empresa.

- **Procedimiento para el manejo de incidentes**: especifica quién responde ante incidentes de seguridad y cómo se deben manejar.

Además de estas secciones clave de políticas de seguridad, otras que pueden ser necesarias en determinadas organizaciones incluyen:

- **Política de solicitud de acceso a las cuentas**: formaliza el proceso de solicitud de cuentas y de acceso dentro de la organización. Los usuarios y los administradores de sistemas que no cumplen los procesos estándar de solicitudes de cuentas y de acceso pueden dar lugar al inicio de acciones legales contra la organización.
- **Política de evaluación de adquisiciones**: define las responsabilidades respecto de las adquisiciones de la empresa y los requisitos mínimos de las evaluaciones de adquisiciones que el grupo de seguridad de la información debe llevar a cabo.
- **Política de auditoría**: define las políticas de auditoría para garantizar la integridad de la información y de los recursos. Incluye un proceso para investigar incidentes, garantizar el cumplimiento de las políticas de seguridad y controlar la actividad de los usuarios y del sistema donde corresponda.
- **Política de confidencialidad de la información**: define los requisitos necesarios para clasificar y asegurar la información de la manera correspondiente en cuanto a su nivel de confidencialidad.
- **Política de contraseñas**: define las normas para crear, proteger y modificar contraseñas sólidas.
- **Política de evaluación de riesgos**: define los requisitos y otorga la facultad al equipo de seguridad de la información a identificar, evaluar y subsanar riesgos de la infraestructura de la información asociados con la conducción de los negocios.
- **Política global de servidores Web**: define las normas exigidas por todos los hosts Web.

Con el uso generalizado del correo electrónico, es posible que una organización también desee tener políticas específicamente relacionadas con el correo electrónico, como:

- **Política de correos electrónicos enviados automáticamente**: documenta la política que restringe el envío automático de correos electrónicos a un destino externo sin aprobación previa del gerente o director quecorresponda.
- **Política de correo electrónico**: define las normas relativas al contenido a fin de impedir que se manche la imagen pública de la organización.
- **Política de spam**: define cómo denunciar y tratar el spam.

Las políticas de acceso remoto podrían incluir:

- **Política de acceso telefónico**: define el acceso telefónico adecuado y su uso por personal autorizado.
- **Política de acceso remoto**: define las normas para conectarse a la red de la organización desde cualquier host o red externos a la organización.
- **Política de seguridad de las VPN**: define los requisitos de las conexiones de las VPN a la red de la organización.

Debe observarse que los usuarios que desafían o infringen las reglas de una política de seguridad pueden ser sometidos a medidas disciplinarias, que incluyen la rescisión del contrato de trabajo.

Componentes de una política de seguridad

Procedimiento	Descripción
Declaración de autoridad y alcance	Esta sección especifica quién propone la política de seguridad y qué áreas abarca.
Política de uso aceptable	Esta sección especifica lo que la empresa permitirá y lo que no con respecto a su infraestructura de información.
Políticas de identificación y autenticación	Esta sección especifica qué tecnologías, qué equipos o qué combinación de éstos se deben utilizar para asegurar que sólo los individuos autorizados tengan acceso a los datos.
Política de acceso a Internet	Esta sección especifica lo que la empresa considera uso ético y correcto de sus capacidades de acceso a Internet.
Política de acceso al campus	Esta sección especifica cómo los usuarios utilizan la infraestructura de datos de la empresa en los campus.
Política de acceso remoto	Esta sección especifica cómo acceden a la infraestructura de datos de la empresa los usuarios remotos.
Procedimiento para el manejo de incidentes	Esta sección especifica la forma en que la empresa crea un equipo de respuesta a incidentes y los procedimientos que utiliza durante el incidente y después de que éste ocurra.

Actividad 1 — Atacantes de la red

_____ es un término general que se ha utilizado históricamente para describir a un experto en programación de computadoras.	Pirata informático
_____ es un término más preciso para describir a una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa.	Cracker
_____ es un término que se utiliza para describir a la persona que manipula la red telefónica para hacerla cumplir una función que, por lo general, no está permitida.	Pirata telefónico
_____ es un término que se utiliza para describir a la persona que envía una gran cantidad de mensajes de correos electrónicos no solicitados.	Remitente de correo no deseado
_____ es un término que se utiliza para describir a una persona que emplea el correo electrónico u otro medio para engañar a otras personas a fin de que le brinden información confidencial, como números de tarjetas de crédito o contraseñas.	Estafador
_____ es un término que se utiliza para describir a las personas que utilizan sus habilidades para encontrar las vulnerabilidades en los sistemas o las redes y, luego, informan esas vulnerabilidades a los propietarios del sistema para que se las pueda solucionar.	Pirata informático de sombrero blanco
_____ es otro término que se utiliza para describir a las personas que emplean su conocimiento sobre los sistemas informáticos para irrumpir en las redes o en los sistemas que no están autorizadas a usar.	Pirata informático de sombrero negro

Tipos de ataques a redes — Actividad 2

	Ataques de reconocimiento	Ataques con acceso	Ataques de DoS y de DDoS
Correo electrónico bomba			✓
Consultas de información en Internet	✓		
Ataque Man-in-the-middle		✓	
Programas detectores de paquetes	✓		
Ataques a la contraseña		✓	
Ping de la muerte			✓
Barridos de ping	✓		
Escaneos de puertos	✓		

4.2 Protección de los routers Cisco

4.2.1 Aspectos de la seguridad de los routers

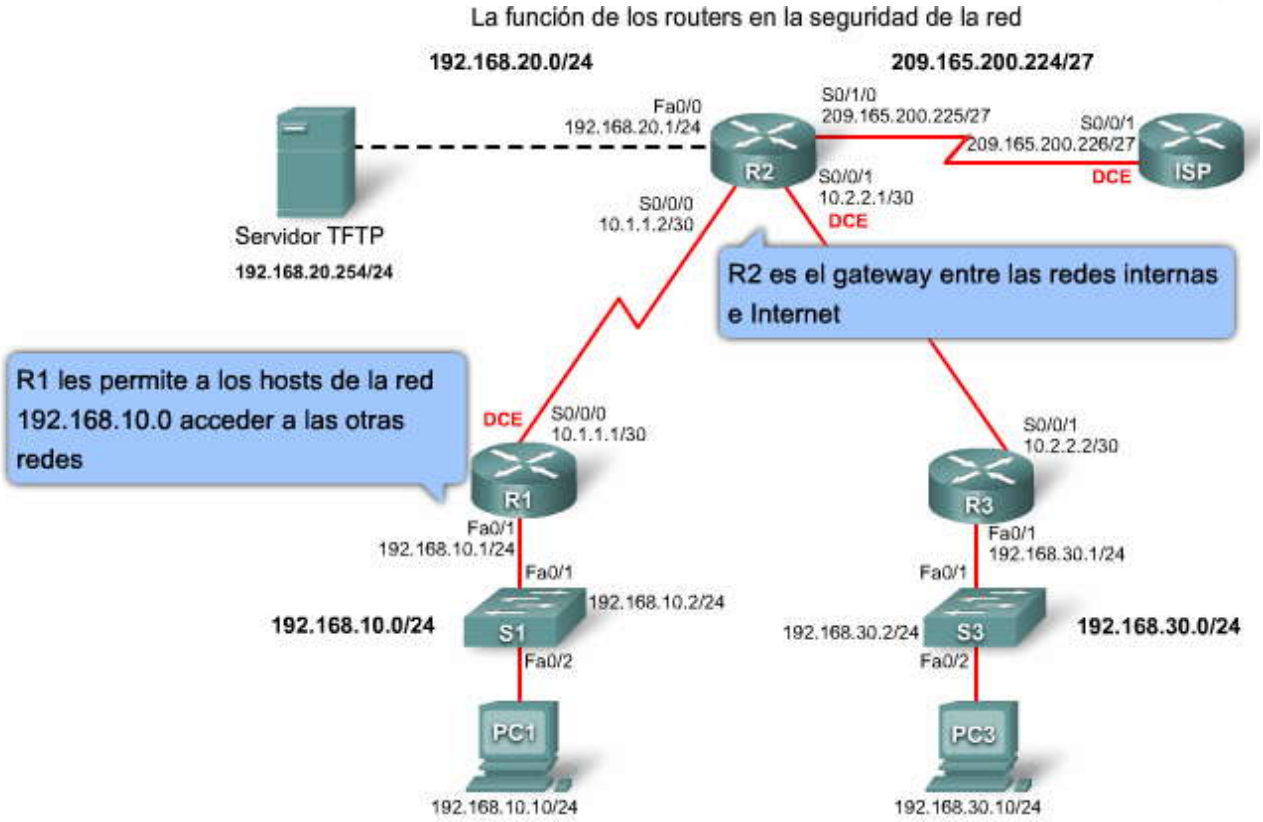
La función de los routers en la seguridad de la red

Usted sabe que puede crear una LAN mediante la conexión dedispositivos con switches básicos de la LAN de Capa 2. A continuación, puede utilizar un router para enrutar el tráfico entre las diferentes redes según direcciones IP de Capa 3.

La seguridad de los routers es un elemento crítico de las implementaciones de seguridad. Los routers son objetivos definidos de los agresores de las redes. Si un agresor puede comprometer y obtener acceso a un router, puede ser una ayuda potencial para ellos. Conocer las funciones que cumplen los routers en la red le ayudará a comprender sus vulnerabilidades.

Los routers cumplen las siguientes funciones:

- Publicar las redes y filtrar a quienes pueden utilizarlas.
- Proporcionar acceso a los segmentos de las redes y a las subredes.



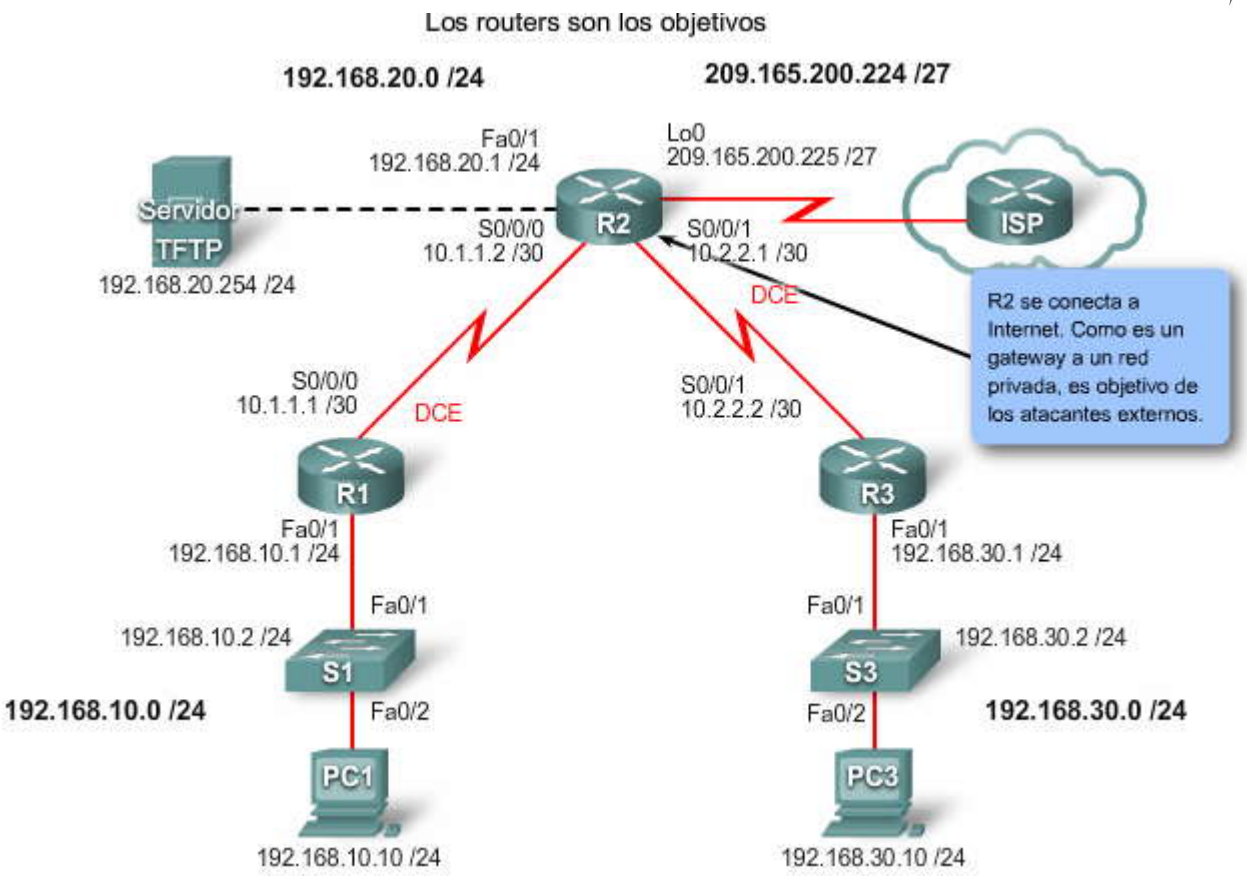
Los routers son objetivos

Dado que los routers proporcionan gateways a otras redes, son objetivos obvios y están sujetos a una diversidad de ataques. A continuación, se dan algunos ejemplos de los diversos problemas de seguridad:

- El compromiso del control de acceso puede exponer los detalles de configuración de la red y, de este modo, se facilita la concreción de ataques contra otros componentes de la red.
- El compromiso de las tablas de enrutamiento puede disminuir el rendimiento, denegar los servicios de comunicación de la red y exponer información confidencial.
- La configuración incorrecta de un filtro de tráfico del router puede exponer los componentes internos de la red a escaneos y ataques, lo que ayuda a los agresores a evitar su detección.

Los agresores pueden comprometer a los routers de diferentes maneras, de modo que no hay un enfoque que los administradores puedan utilizar para combatirlos. Las maneras en las que los routers pueden ser comprometidos son similares a los tipos de ataques que aprendió anteriormente en este capítulo, incluidos los ataques de explotación de confianza, suplantación de identidad de IP, apropiación de sesiones y ataques MITM.

Nota: Esta sección se centra en la protección de los routers. La mayoría de las mejores prácticas analizadas también se pueden utilizar para proteger los switches. Sin embargo, esta sección no contempla las amenazas de Capa 2, como los ataques de flooding de direcciones MAC y ataques de STP, porque están contemplados en CCNA Exploration: Conmutación y transmisión inalámbrica de LAN.



Protección de su red

La protección de los routers que se encuentran dentro del perímetro de la red es un primer paso importante para protegerla.

Piense en la seguridad de los routers en función de las siguientes categorías:

- Seguridad física
- Actualización del IOS de los routers cuando sea conveniente
- Copia de seguridad de la configuración y del IOS de los routers
- Aseguramiento del router para eliminar el abuso potencial de los puertos y servicios no utilizados

Para proporcionar seguridad física, ubique el router en un cuarto cerrado con llave, donde sólo pueda ingresar personal autorizado. Asimismo, dicho cuarto no debe tener interferencia electrostática ni magnética y debe tener controles de temperatura y humedad. Para disminuir la posibilidad de DoS debido a una falla de alimentación, instale una fuente de energía ininterrumpible (UPS) y mantenga los componentes de repuesto disponibles.

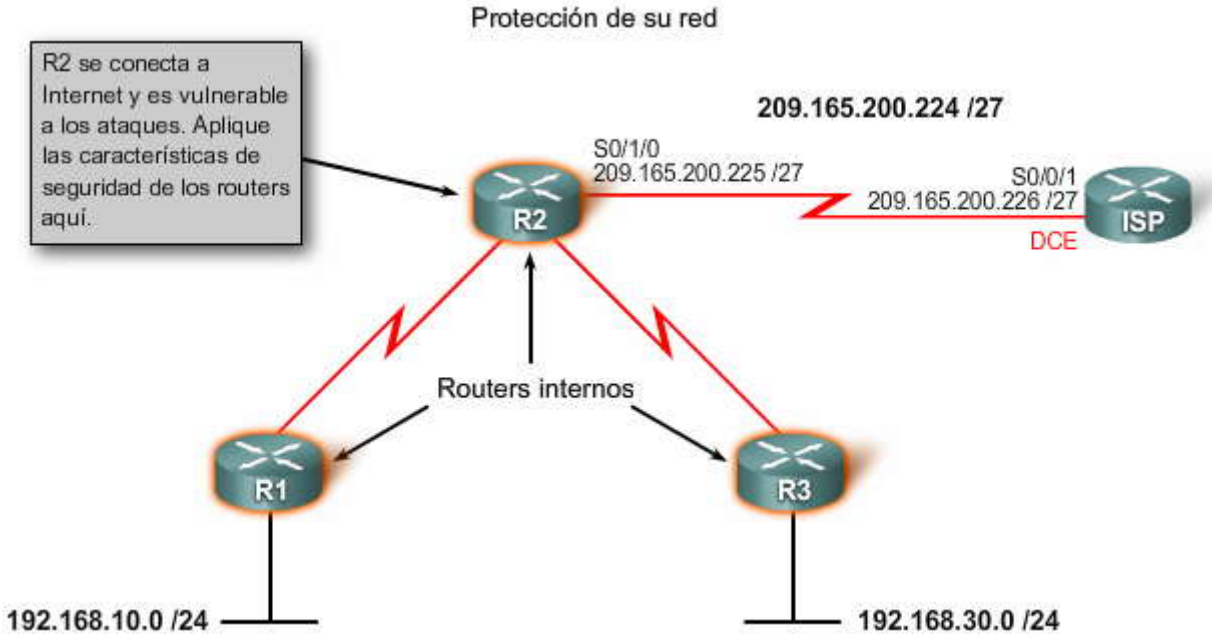
Los dispositivos físicos utilizados para conectarse al router se deben guardar en un local cerrado con llave, o deben permanecer en poder de una persona de confianza para que no se vean comprometidos. Un dispositivo que se deja al aire libre podría tener troyanos o algún otro tipo de archivo ejecutable almacenado en él.

Provea al router de la máxima cantidad de memoria posible. La disponibilidad de memoria puede servir como protección contra algunos ataques DoS, mientras que admite la gama más amplia de servicios de seguridad.

Las características de seguridad de un sistema operativo evolucionan con el tiempo. Sin embargo, la última versión de un sistema operativo puede no ser la versión más estable disponible. Para obtener el mejor rendimiento de la seguridad de su sistema operativo, utilice la versión estable más reciente que cumpla los requisitos de las características de su red.

Debe tener siempre una copia de seguridad de una configuración y el IOS a mano para el caso de que se produzca una falla en un router. Mantenga una copia segura de la imagen del sistema operativo del router y del archivo de configuración del router en un servidor TFTP como respaldo.

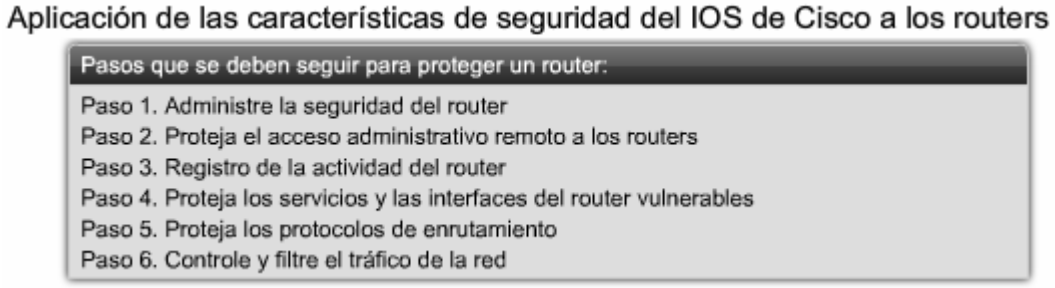
Asegure el router para hacerlo tan seguro como sea posible. Un router tiene muchos servicios activados de forma predeterminada. Muchos de estos servicios son innecesarios y pueden ser utilizados por un agresor para compilar o explotar información. Debe asegurar la configuración de su router mediante la desactivación de los servicios innecesarios.



4.2.2 Aplicación de las características de seguridad del IOS de Cisco a los routers

Antes de configurar las características de seguridad del router, debe planificar todos los pasos de la configuración de seguridad del IOS de Cisco.

La figura muestra los pasos que se deben seguir para proteger un router. Los primeros cuatro pasos se analizan en este capítulo. Si bien las listas de control de acceso (ACL) se analizan en el capítulo siguiente, son una tecnología crítica y deben configurarse para controlar y filtrar el tráfico de la red.



4.2.3 Administración de la seguridad de los routers

La seguridad básica de los routers consiste en la configuración de contraseñas. Una contraseña sólida es el elemento más fundamental para controlar el acceso seguro a un router. Por este motivo, siempre se deben configurar contraseñas sólidas.

Entre las buenas prácticas en materia de contraseñas se incluyen las siguientes:

- No escribir las contraseñas ni dejarlas en lugares obvios, como el escritorio o monitor.
- Evitar el uso de palabras del diccionario, nombres, números de teléfono y fechas. El uso de palabras del diccionario hace que las contraseñas sean vulnerables a los ataques de diccionario.
- Combinar letras, números y símbolos. Incluir, por lo menos, una letra minúscula, una letra mayúscula, un dígito y un carácter especial.
- Escribir mal una contraseña deliberadamente. Por ejemplo, **Smith** se puede escribir **Smyth** o también puede incluir números, como **5mYth**. Otro ejemplo podría ser **Seguridad** escrita **5ecur1dad**.
- Crear contraseñas largas. La mejor práctica es tener, como mínimo, ocho caracteres. Puede hacer cumplir la longitud mínima si se utiliza una característica que poseen los routers del IOS de Cisco, que se analiza más adelante en este tema.

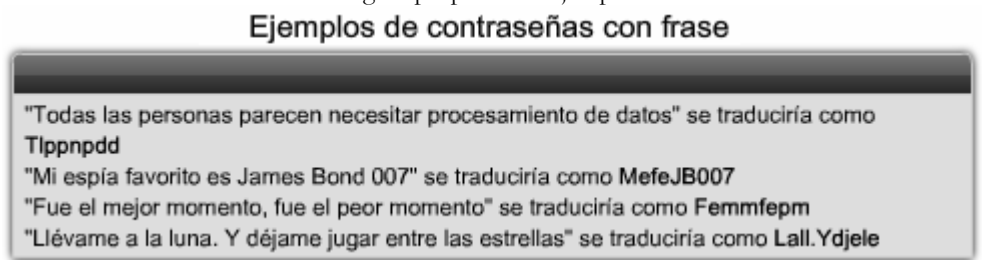
- Modificar las contraseñas con la mayor frecuencia posible. Debe tener una política que defina cuándo y con qué frecuencia se deben modificar las contraseñas. La modificación de las contraseñas suele tener dos ventajas. Esta práctica limita la ventana de oportunidad en que un pirata informático puede descifrar una contraseña y limita la ventana de exposición una vez que se ha comprometido una contraseña.

Nota: Los espacios anteriores a la contraseña se ignoran, pero todos los espacios posteriores al primer carácter no se ignoran.

Contraseñas con frases

Un método recomendado para crear contraseñas complejas sólidas es utilizar contraseñas con frases. Una contraseña con frase es básicamente una oración o frase que sirve como contraseña más segura. Asegúrese de que la frase sea lo suficientemente larga como para que sea difícil de adivinar pero fácil de recordar y de escribir correctamente.

Utilice una oración, una cita de un libro o la letra de una canción que pueda recordar fácilmente como base de su contraseña sólida o contraseña con frase. La figura proporciona ejemplos de contraseñas con frases.



De forma predeterminada, el software IOS de Cisco deja contraseñas en texto sin cifrar cuando se introducen en un router. Esto no es seguro, ya que cualquiera que pase por detrás suyo mientras observa la configuración de un router podría espiar por encima de su hombro y ver la contraseña.

Si se usa el comando **enable password** o el comando **username** *username* **password** *password* estas contraseñas se mostrarían al observar la configuración en ejecución.

Por ejemplo:

R1(config)# **username Student password cisco123**
R1(config)# **do show run | include username**
username Student password 0 cisco123
R1(config)#

El **0** que aparece en la configuración en ejecución indica que la contraseña no está oculta.

Por este motivo, todas las contraseñas deben estar encriptadas en un archivo de configuración. El IOS de Cisco ofrece dos esquemas de protección de contraseñas:

- Encriptación simple, que se denomina esquema de tipo 7. Utiliza el algoritmo de encriptación definido por Cisco y oculta la contraseña mediante el uso de un algoritmo de encriptación simple.
- Encriptación compleja, que se denomina esquema de tipo 5. Utiliza un hash MD5 más seguro.

La encriptación del tipo 7 puede ser utilizada por los comandos **enable password**, **username** y **line password**, incluidos vty, line console y aux port. No ofrece una gran protección, ya que sólo oculta la contraseña utilizando un algoritmo de encriptación simple. Pese a que no es tan segura como la encriptación de tipo 5, sigue siendo mejor que no utilizar ninguna encriptación.

Para encriptar contraseñas mediante la encriptación de tipo 7, use el comando de configuración global **service password-encryption** como se lo muestra en la figura. Mediante este comando las contraseñas que aparecen en la pantalla no son legibles.

Por ejemplo:

R1(config)# **service password-encryption**
R1(config)# **do show run | include username**

username Student password 7 03075218050061
R1(config)#

El **7** que aparece en la configuración en ejecución indica que la contraseña está oculta. En la figura, se puede ver que la contraseña de la consola de línea ahora está oculta.

Haga clic en el botón Configurar la contraseña de la figura.

Cisco recomienda utilizar la encriptación de Tipo 5 en lugar de la de Tipo 7, cuando sea posible. La encriptación MD5 es un método de encriptación fuerte. Debe ser utilizado siempre que sea posible. Se configura reemplazando la palabra clave **password** por **secret**.

Por lo tanto, para proteger el nivel privilegiado EXEC tanto como sea posible, siempre debe configurar el comando **enable secret** como se observa en la figura. También debe asegurarse de que la contraseña secreta sea única y no coincida con ninguna otra.
Un router siempre utiliza la contraseña secreta antes que la contraseña de enable. Por este motivo, el comando **enable password** nunca se debe configurar, ya que puede revelar la contraseña de un sistema.
Nota: Si se olvida la contraseña privilegiada EXEC, entonces tendrá que ejecutar el procedimiento de recuperación de contraseña. Este procedimiento se aborda más adelante en este capítulo.

Los nombres de usuario de la base de datos local también deben estar configurados mediante el comando de configuración global **username** *username* **secret** *password*. Por ejemplo:

R1(config)# **username Student secret cisco**
R1(config)# **do show run | include username**
username Student secret 5 1z245$lVSTJzuYgdQDJiacwP2Tv/
R1(config)#

Nota: Es posible que algunos procesos no puedan utilizar contraseñas encriptadas de tipo 5. Por ejemplo, PAP y CHAP requieren contraseñas en texto sin cifrar y no pueden utilizar contraseñas encriptadas MD5.

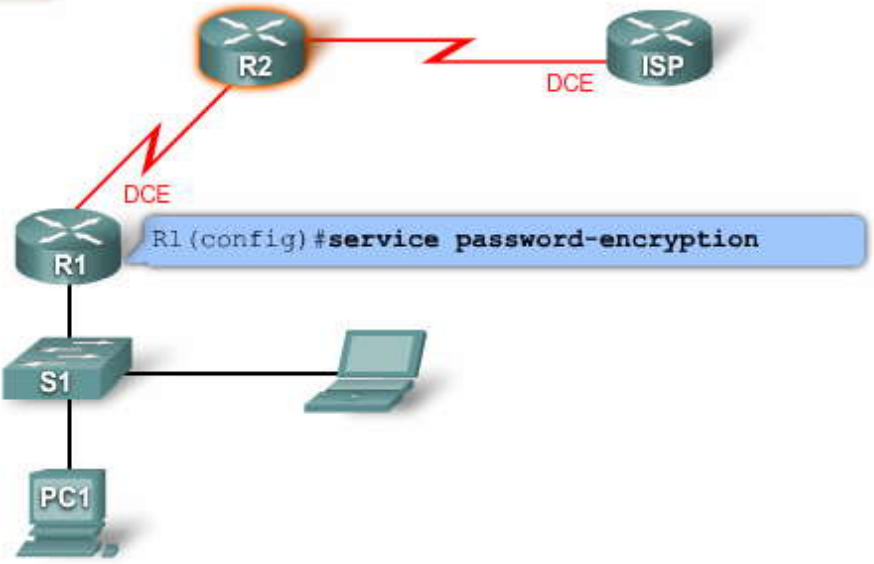
Haga clic en el botón Longitud de la contraseña de la figura.

El software IOS de Cisco Versión 12.3(1) y posteriores permite que los administradores definan la longitud mínima en caracteres de todas las contraseñas de los routers utilizando el comando de configuración global **security passwords min-length**, como se observa en la figura. Este comando proporciona acceso con mayor seguridad al router, al permitirle que especifique una longitud mínima para las contraseñas, y elimina las contraseñas comunes que predominan en la mayoría de las redes, como "lab" y "cisco".

Este comando afecta a las contraseñas de usuario nuevas, las de enable y las secretas, y las contraseñas de línea creadas una vez que el comando fue ejecutado. El comando no afecta las contraseñas de routers actuales.

Config

Configuración de contraseñas de router



El administrador encripta todas las contraseñas en el archivo de configuración.

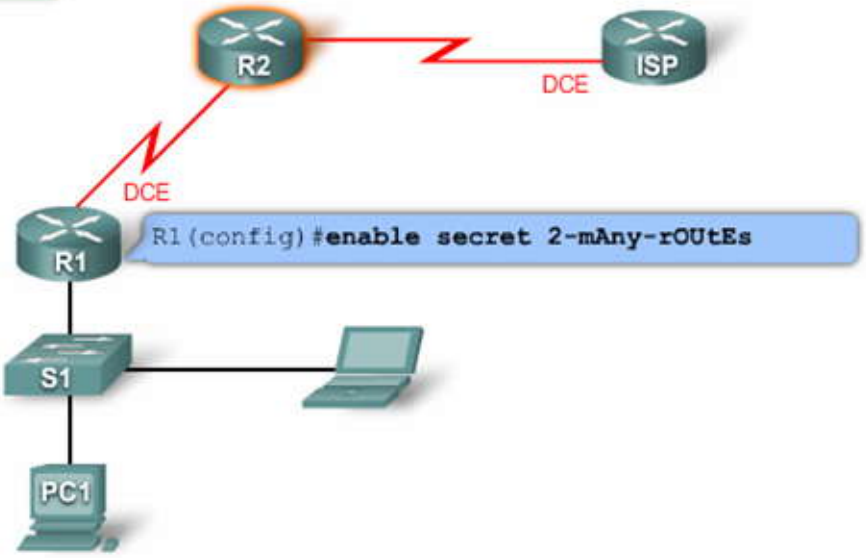
Encriptar la contraseña | Configurar la contraseña | Longitud de la contraseña

Paso 2: Encripte las contraseñas

```
R1(config)#service password-encryption
R1(config)#end

R1#show running-config
!
Line con 0
Password 7 0956F57A109A
-----Output Omitted----
```

Config

Configuración de contraseñas de router

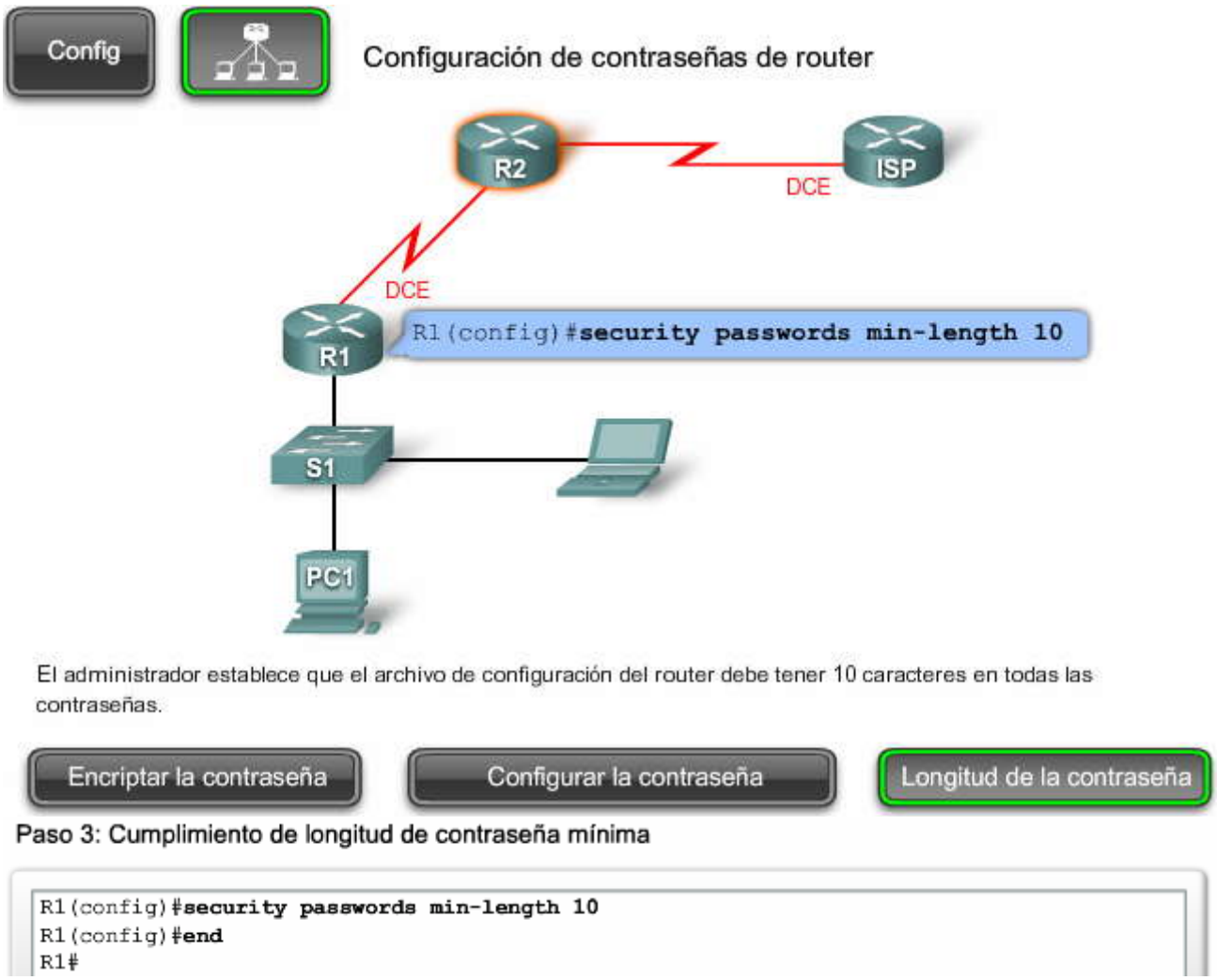


El administrador configura una contraseña tipo 5 (hash MD5) e inhabilita la contraseña tipo 7.

Encriptar la contraseña | Configurar la contraseña | Longitud de la contraseña

Paso 1: Configure las contraseñas de router

```
R1(config)#
R1(config)#enable secret 2-mAny-rOUtEs
R1(config)#no enable password
R1(config)#end
R1#
```



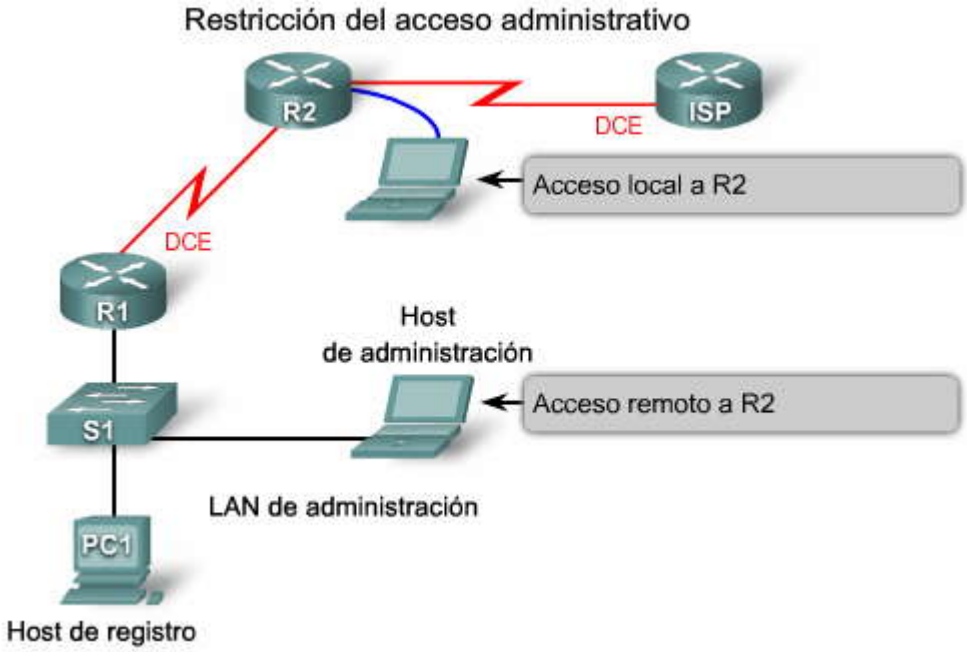
4.2.4 Protección del acceso remoto administrativo a los routers

Protección del acceso administrativo a los routers

Los administradores de redes pueden conectarse a un router o conmutar de forma local o remota. El acceso local a través del puerto de la consola es el método preferido por un administrador para conectarse a un dispositivo a fin de manejarlo, porque es seguro. A medida que las empresas crecen y aumenta la cantidad de routers y switches de la red, la carga de trabajo del administrador para conectarse a todos los dispositivos a nivel local puede ser abrumadora.

El acceso administrativo remoto es más conveniente que el acceso local para los administradoresque tienen que manejar muchos dispositivos. Sin embargo, si no se implementa de manera segura, un agresor podría recopilar información confidencial valiosa. Por ejemplo, implementar el acceso administrativo remoto mediante Telnet puede ser muy inseguro porque Telnet envía todo el tráfico de la red en forma de texto sin cifrar. Un agresor podría capturar el tráfico de la red, mientras un administrador se encuentra conectado remotamente a un router, y descubrir las contraseñas del administrador o la información de configuración del router. Por lo tanto, el acceso remoto administrativo debe ser configurado con mayores precauciones de seguridad.

Para proteger el acceso administrativo a los routers y switches, primero debe proteger las líneas administrativas (VTY, AUX), y después configurar el dispositivo de red para que encripte el tráfico en un túnel SSH.



Acceso remoto administrativo con Telnet y SSH

Tener acceso remoto a los dispositivos de la red es fundamental para manejar una red de manera eficaz. El acceso remoto generalmente implica permitir conexiones de Telnet, Shell Seguro (SSH), HTTP, HTTP seguro (HTTPS) o SNMP al router desde un equipo que se encuentra en la misma internetwork que el router.

Si se requiere acceso remoto, sus opciones son las siguientes:

- Establecer una red de administración dedicada. La red de administración debe incluir sólo hosts de administración identificados y conexiones a dispositivos de infraestructura. Podría lograrse si se utiliza una VLAN de administración u otra red física a la cual se deben conectar los dispositivos.
- Encriptar todo el tráfico entre la computadora del administrador y el router. En cualquiera de esos casos,se puede configurar un filtro de paquetes que permita que solamente el protocolo y los hosts de administración identificados obtengan acceso al router. Por ejemplo, permitir que sólo la dirección IP del host de administración inicie una conexión SSH con los routers de la red.

El acceso remoto no sólo se aplica a la línea de VTY del router, también se aplica a las líneas de TTY y al puerto auxiliar (AUX). Las líneas de TTY proporcionan acceso asíncrono a un router a través de un módem. Si bien son menos comunes que lo que fueron en otro momento, todavía existen en algunas instalaciones. Proteger estos puertos es aun más importante que proteger los puertos del terminal local.

La mejor manera de proteger un sistema es garantizar que se apliquen controles adecuados en todas las líneas, incluidas las líneas de VTY, TTY y AUX.

Los administradores deben asegurarse de que las conexiones en todas las líneas estén controladas mediante un mecanismo de autenticación, incluso en las máquinas supuestamente inaccesibles desde redes no confiables. Esto es especialmente importante en el caso de las líneas de VTY y de las líneas conectadas a módems u otros dispositivos de acceso remoto.

Las conexiones se pueden evitar por completo en cualquier línea mediante la configuración del router con los comandos **login** y **no password**. Ésta es la configuración predeterminada de los VTY, pero no de los TTY ni del puerto AUX. Por lo tanto, si estas líneas no son exigidas, asegúrese de que estén configuradas con la combinación de comandos**login** y **no password**.

Haga clic en Config en el botón Evitar conexiones para ver un ejemplo.

Controles en los puertos VTY

De manera predeterminada, todas las líneas de VTY están configuradas para aceptar cualquier tipo de conexión remota. Por razones de seguridad, las líneas de VTY se deben configurar para aceptar conexiones sólo con los protocolos realmente necesarios. Esto se hace mediante el comando **transport input**. Por ejemplo, un VTY que debe recibir sólo sesiones de

Telnet estaría configurado con **transport input telnet**, y un VTY que permite las sesiones de Telnet y de SSH estaría configurado con **transport input telnet ssh**.

Haga clic en el botón Acceso VTY de la figura.

El primer ejemplo de configuración muestra la forma de configurar el VTY para que acepte solamente conexiones de Telnet y de SSH, mientras que el segundo ejemplo muestra la manera de configurar el VTY para que acepte solamente conexiones de SSH. Si la imagen del IOS de Cisco de un router admite SSH, se recomienda enfáticamente activar solamente ese protocolo.

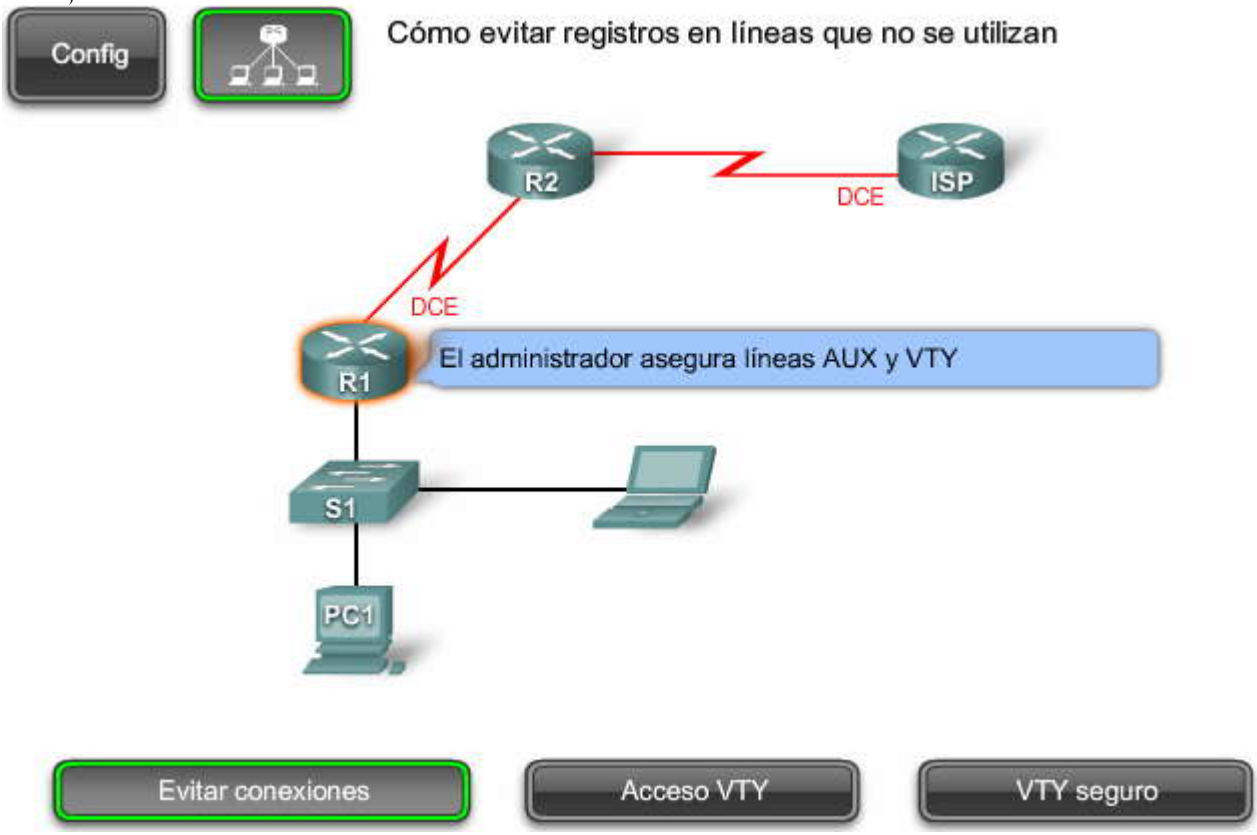
Un dispositivo del IOS de Cisco tiene una cantidad limitada de líneas de VTY, por lo general, cinco. Cuando todos los VTY están en uso, no se pueden establecer más conexiones remotas. Esto crea la posibilidad de realizar un ataque DoS. Si un agresor puede abrir sesiones remotas para todos los VTY del sistema, es posible que el administrador legítimo no se pueda conectar. El agresor no tiene que conectarse para hacer esto. Las sesiones simplemente se pueden dejar en la ventana de inicio de sesión.

Una forma de disminuir esta exposición es configurar la última línea de los VTY para que acepten sólo las conexiones provenientes de una única estación de trabajo administrativa específica, mientras que los otros VTY pueden aceptar conexiones de cualquier dirección de una red corporativa. Esto garantiza que, por lo menos, una línea de VTY esté a disposición del administrador. Para implementar esto, las ACL, junto con el comando **ip access-class** de la última línea de VTY, deben estar configurados. Esta implementación se analiza en el Capítulo 5

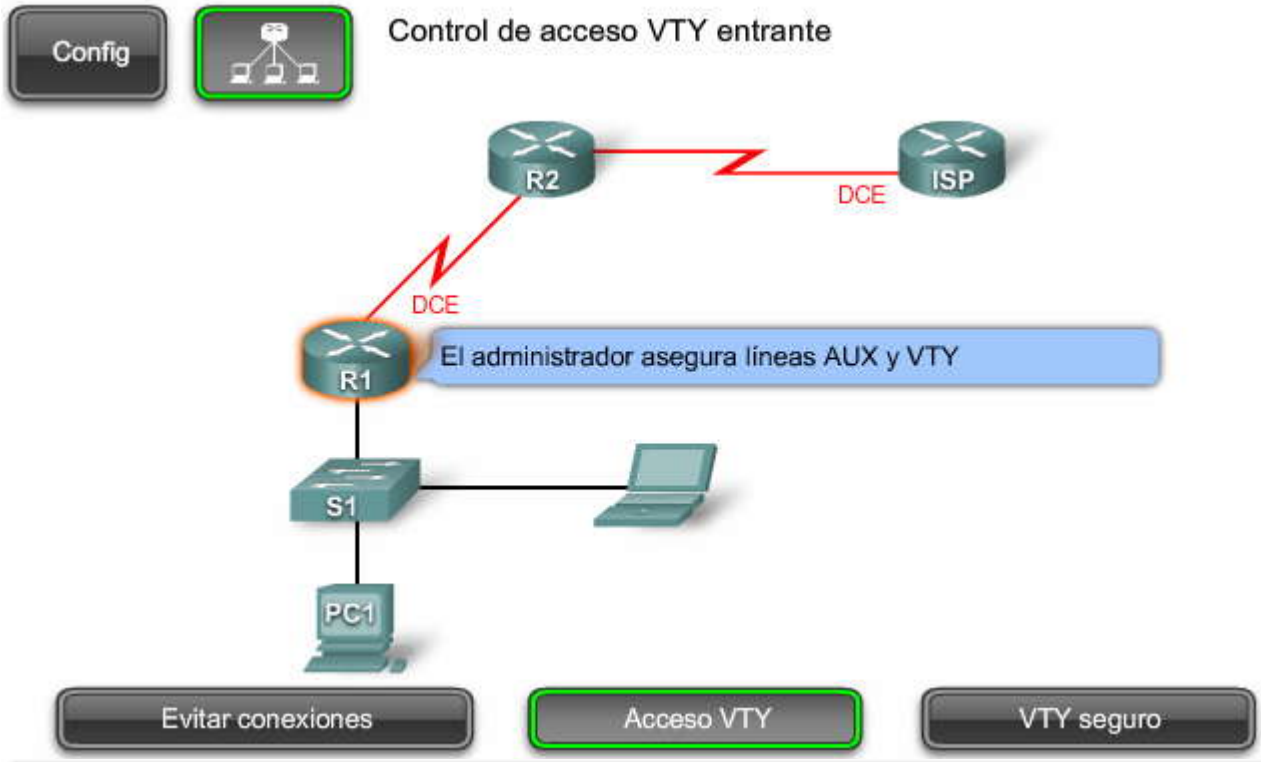
Otra táctica útil es configurar los tiempos de espera de los VTY mediante el comando **exec-timeout**. Esto impide que una sesión inactiva consuma el VTY en forma indefinida. A pesar de que su eficacia contra los ataques deliberados es relativamente limitada, proporciona algo de protección contra las sesiones que se dejan accidentalmente inactivas. Del mismo modo, la activación de los mensajes de actividad de TCP en las conexiones entrantes mediante el comando **service tcp-keepalives-in** puede ayudar a resguardarse de los ataques maliciosos y de las sesiones huérfanas provocadas por colapsos del sistema remoto.

Haga clic en el botón VTY seguro de la figura.

La configuración muestra la manera en la que se debe configurar el tiempo de espera ejecutivo en 3 minutos y activar los mensajes de actividad del TCP.



```
R1(config)# line aux 0
R1(config-line)# no password
R1(config-line)# login
% Login disabled on line 65, until 'password' is set
R1(config-line)# exit
R1(config)#
```

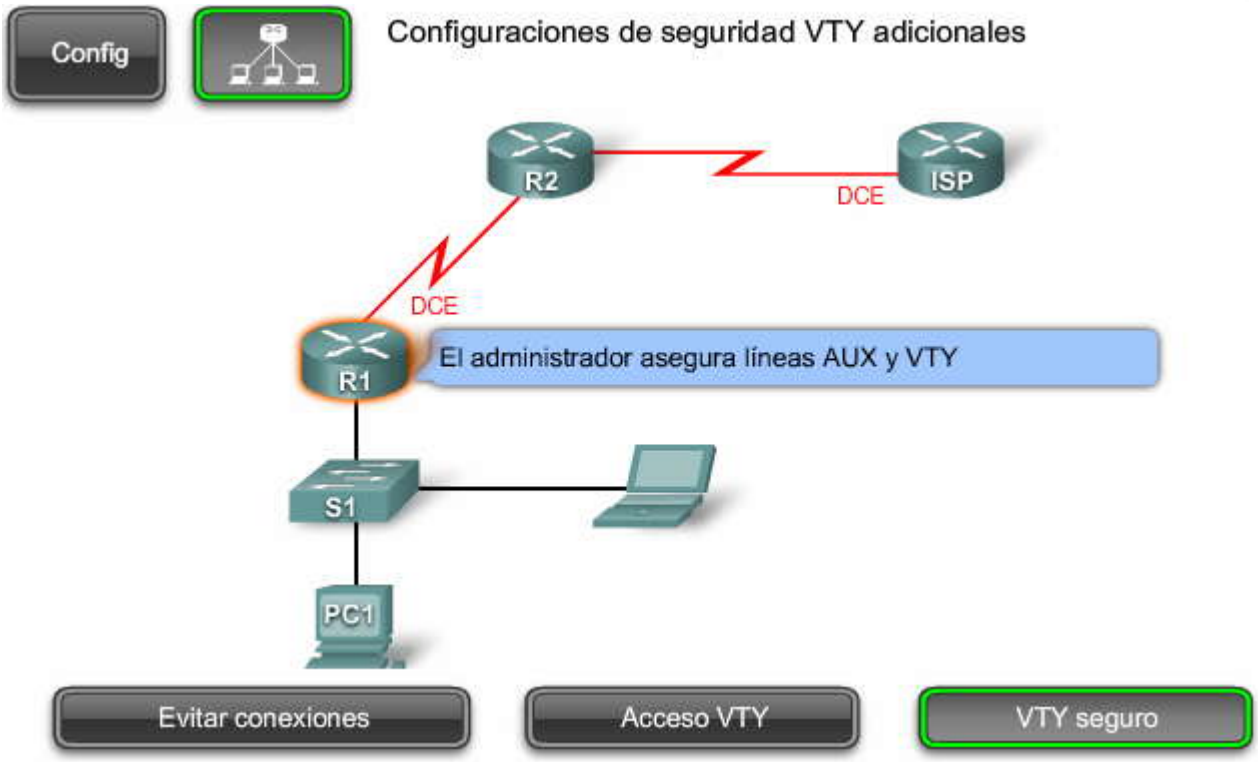



```
R1(config)# line vty 0 4
R1(config-line)# no transport input
R1(config-line)# transport input telnet ssh
R1(config-line)# exit
```

Admite sesiones Telnet y SSH entrantes.

```
R1(config)# line vty 0 4
R1(config-line)# no transport input
R1(config-line)# transport input ssh
R1(config-line)# exit
```

Sólo admite sesiones SSH entrantes.




```
R1(config)# line vty 0 4
R1(config-line)# exec-timeout 3
R1(config-line)# exit
R1(config)# service tcp-keepalives-in
```

c

Implementación de SSH para proteger el acceso administrativo remoto

Tradicionalmente, al acceso administrativo remoto de los routers se configuraba mediante Telnet en el puerto TCP 23. Sin embargo, Telnet se desarrolló en un tiempo en el que la seguridad no era un problema. Por este motivo, todo el tráfico de Telnet se envía en forma de texto sin cifrar.

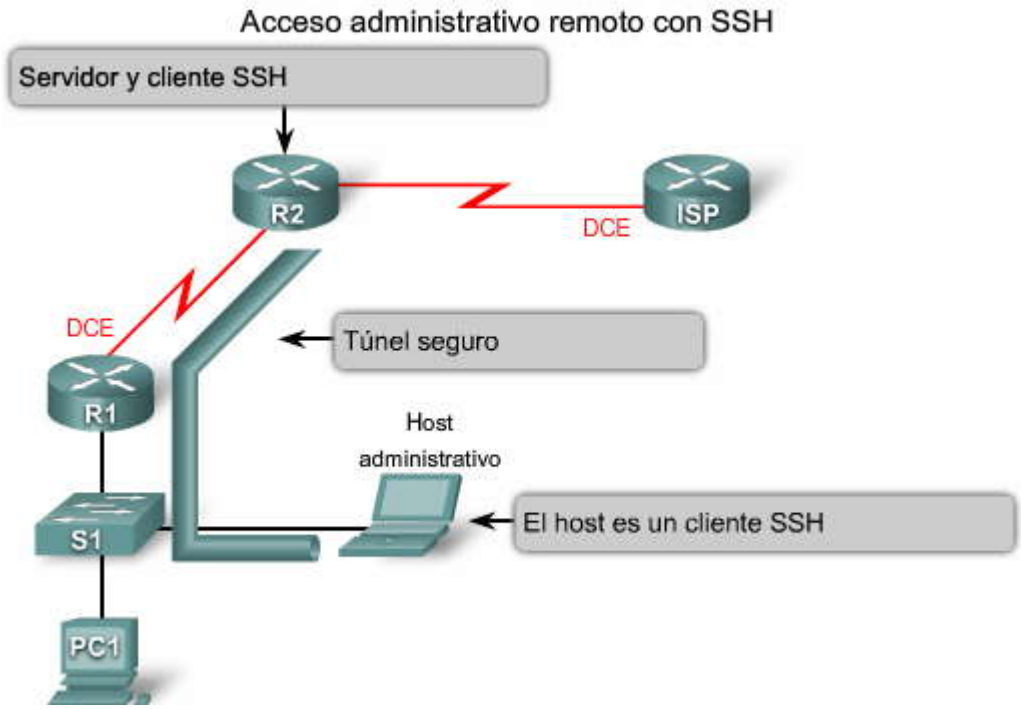
SSH reemplazó a Telnet como la mejor práctica para proporcionar administración remota de los routers con conexiones que admiten una sólida privacidad e integridad de las sesiones. SSH utiliza el puerto TCP 22. Brinda una funcionalidad similar a la de una conexión Telnet saliente, con la excepción de que la conexión se encuentra encriptada. Mediante la autenticación y la encriptación, SSH hace posibles las comunicaciones seguras a través de una red insegura.

No todas las imágenes del IOS de Cisco admiten SSH. Sólo lo hacen las imágenes criptográficas. Por lo general, los ID de imagen de los nombres de estas imágenes son k8 o k9. Los nombres de las imágenes se analizan en la Sección 5.

La característica de acceso de línea de terminal SSH permite a los administradores configurar los routers con acceso seguro y realizar las siguientes tareas:

- Conectarse a un router que tiene varias líneas de terminales conectadas a consolas o puertos seriales de otros routers, switches y dispositivos.
- Simplificar la conectividad a un router desde cualquier lugar mediante la conexión segura al servidor de terminales de una línea específica.
- Permitir que los módems conectados a los routers sean utilizados para realizar marcado saliente de manera segura.
- Exigir autenticación a cada una de las líneas a través de un nombre de usuario y una contraseña definidos a nivel local, o un servidor de seguridad, como TACACS+ o RADIUS.

Los routers Cisco pueden actuar como cliente y servidor SSH. De manera predeterminada, ambas funciones se encuentran activadas en el router cuando se activa SSH. Como cliente, un router puede realizar un SSH a otro router. Como servidor, un router puede aceptar conexiones SSH cliente.



Configuración de la seguridad de SSH

Para permitir SSH en el router, se deben configurar los siguientes parámetros:

- Nombre de host
- Nombre de dominio
- Claves asimétricas
- Autenticación local

Entre los parámetros de configuración opcionales se encuentran:

- Tiempos de espera
- Reintentos

Los siguientes pasos configuran el SSH en un router.

Paso 1: Defina los parámetros de los routers

Configure el nombre de host del router con el comando **hostname** *hostname* del modo de configuración.

Paso 2: Defina el nombre de dominio

Se debe crear un nombre de dominio para activar el SSH. En este ejemplo, escriba el comando **ip domain-name cisco.com** del modo de configuración global.

Paso 3: Genere claves asimétricas

Debe crear una clave que el router pueda utilizar para encriptar su tráfico de administración de SSH con el comando **crypto key** *generate rsa* del modo de configuración. El router responde con un mensaje que muestra la norma de denominación de las claves. Elija el tamaño del módulo de la clave que debe estar entre 360 y 2048 para sus Claves de propósito general. Elegir un módulo de clave mayor a 512 puede llevar algunos minutos. Como mejor práctica, Cisco recomienda utilizar una longitud de módulo mínima de 1024. Debe saber que la creación y el uso de un módulo más largo llevan más tiempo, pero ofrece mayor seguridad.

Puede obtener más información sobre el comando **crypto key** en el curso Seguridad de la red.

Paso 4: Configure la autenticación local y el vty

Debe definir un usuario local y asignar una comunicación de SSH a las líneas de vty, como se observa en la figura.

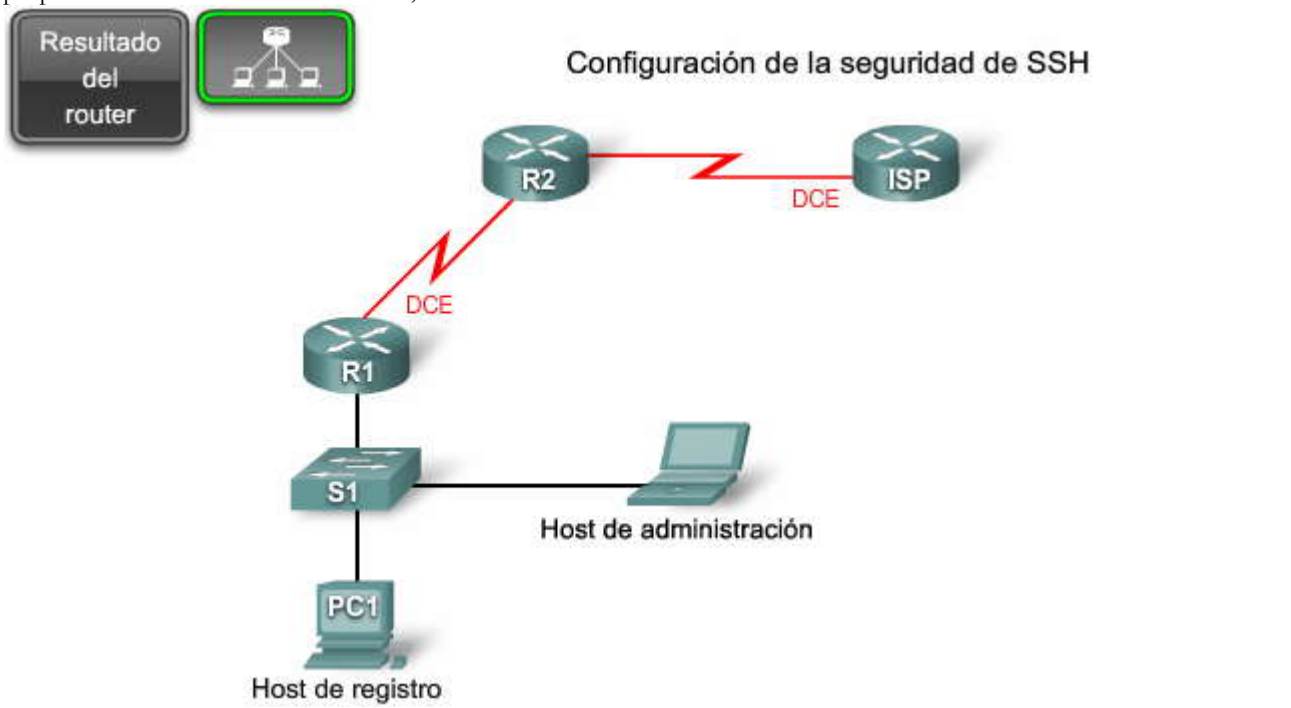
Paso 5: Configure tiempos de espera de SSH (opcional)

Los tiempos de espera brindan seguridad adicional a la conexión, pues finalizan las conexiones prolongadas e inactivas. Use el comando **ip ssh time-out** *seconds* **authentication-retries** *integer* para activar los tiempos de espera y los reintentos de autenticación. Configure el tiempo de espera del SSH en 15 segundos y la cantidad de reintentos en 2:

Para conectarse a un router configurado con un SSH, debe utilizar una aplicación de SSH cliente como PuTTY o TeraTerm. Debe asegurarse de elegir la opción SSH y de que utilice el puerto TCP 22.

Haga clic en el botón Usar SSH de la figura.

Al usar TeraTerm para conectarse de manera segura al router R2 con SSH, una vez que se inició la conexión, el R2 muestra una ventana en la que se solicita el nombre de usuario, seguida por otra que solicita la contraseña. Si suponemos que se proporcionan las credenciales correctas, TeraTerm muestra el indicador de EXEC del usuario del router R2.



Paso 1: Establezca los parámetros del router

```
Router(config)#hostname R2
R2(config)#
```

Paso 2: Establezca el nombre de dominio

```
R2(config)#ip domain-name cisco.com
```

Paso 3: Genere claves asimétricas

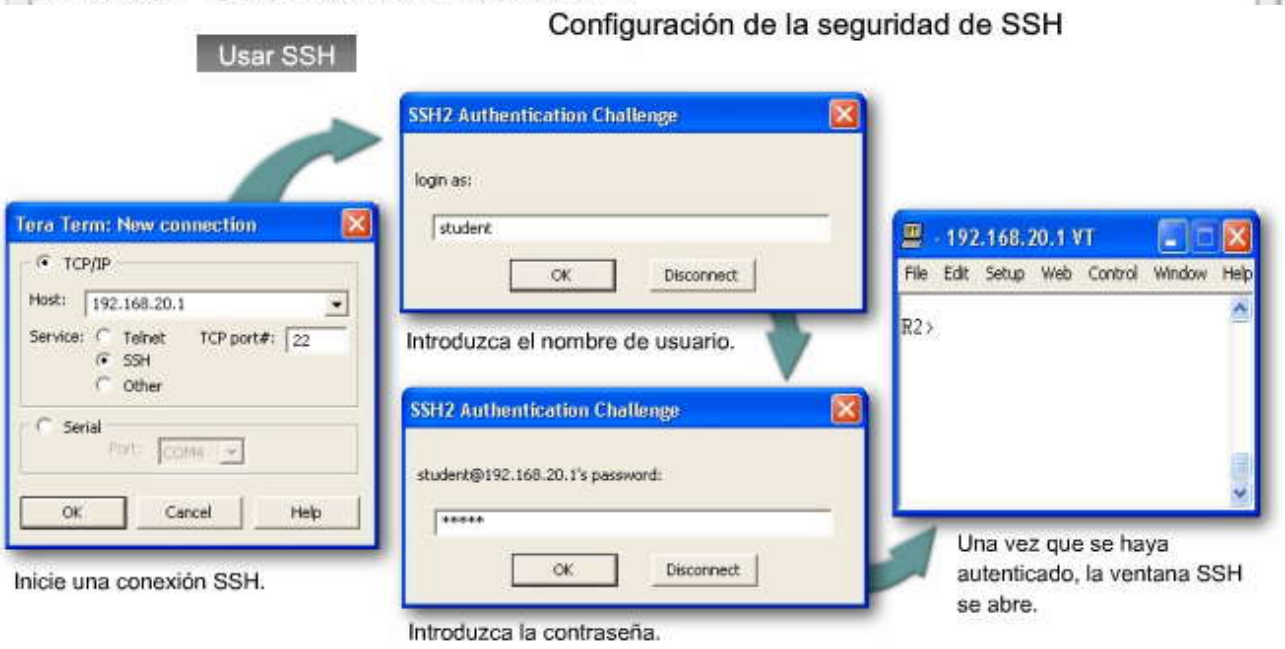
```
R2(config)#crypto key generate rsa

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys.
Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...
```

Paso 4: Configure la autenticación local y el VTY

```
R2(config)# username student secret cisco
R2(config)# line vty 0 4
R2(config-line)# transport input ssh
R2(config-line)# login local
```

Paso 5: Configure los tiempos de espera de SSH

```
R2(config)# ip ssh time-out 15
R2(config)# ip ssh authentication-retries 2
```



Paso 1: Establezca los parámetros del router

Paso 2: Genere claves asimétricas

Paso 3: Configure los tiempos de espera y el nombre de usuario de SSH

Paso 4: Configure la autenticación local y el VTY

```
Router(config)#hostname R1
R1(config)#ip domain-name cisco.com
R1(config)#
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: Enter
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]
*Sep 21 15:41:51.015: %SSH-5-ENABLED: SSH 1.5 has been enabled
R1(config)#ip shh time-out 15
R1(config)#ip ssh authentication-retries 2
R1(config)#username student password cisco
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#end
```

4.2.5 Actividad de registro de los routers

Los registros le permiten verificar que un router esté funcionando correctamente o determinar si el router está comprometido. En algunos casos, un registro puede mostrar qué tipos de sondeos o ataques se están intentando perpetrar contra el router o la red protegida.

La configuración del registro (syslog) en el router se debe realizar con cuidado. Envíe los registros del router a un host de registro designado. El host de registro debe estar conectado a una red confiable o protegida, o a una interfaz de router

aislada y dedicada. Asegure el host de registro eliminando todas las cuentas y todos los servicios innecesarios. Los routers admiten distintos niveles de registro. Los ocho niveles van desde 0, emergencias que indican que el sistema es inestable, hasta 7 para depurar mensajes que incluyen toda la información del router.

Los registros se pueden enviar a una variedad de ubicaciones, incluida la memoria del router o un servidor syslog dedicado. Los servidores syslog brindan una mejor solución porque todos los dispositivos de red pueden enviar sus registros a una estación central en donde un administrador puede analizarlos. Un ejemplo de aplicación de servidores syslog es Kiwi Syslog Daemon.

Considere también la posibilidad de enviar los registros a un segundo dispositivo de almacenamiento, por ejemplo, a medios de escritura única o a una impresora dedicada, para manejar el peor de los casos (por ejemplo, un compromiso del host de registro).

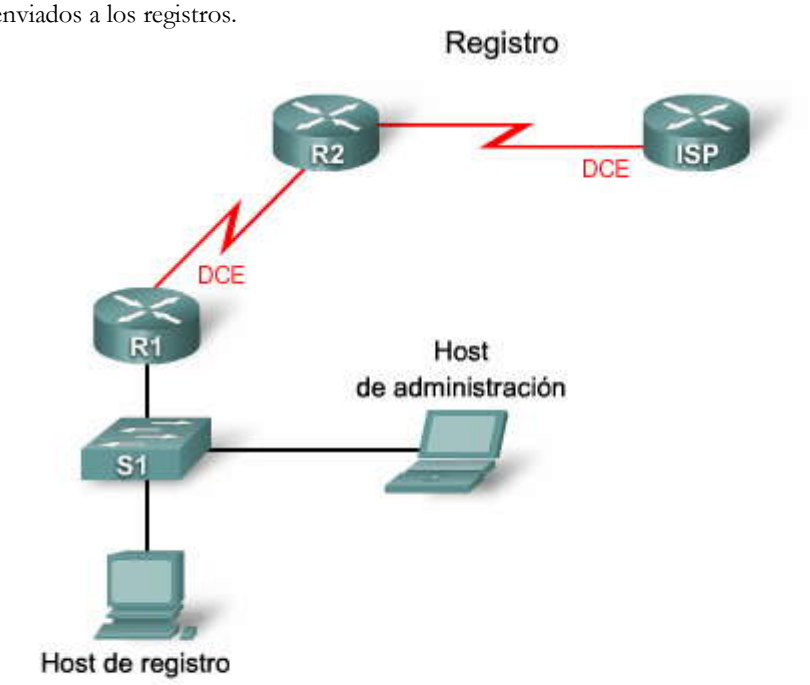
El dato más importante que debe recordar acerca del registro es que los registros se deben revisar con regularidad. Si controla los registros regularmente, podrá apreciar el comportamiento normal de su red. Una sólida compresión del funcionamiento normal y su reflejo en los registros lo ayuda a identificar las condiciones anormales o de ataque.

Las marcas horarias precisas son importantes para el registro. Las marcas horarias le permiten rastrear los ataques a la red de manera más creíble. Todos los routers pueden mantener su propia hora del día, pero, por lo general, esto no es suficiente. En cambio, dirija el router a, por lo menos, dos servidores de tiempo diferentes confiables para garantizar la precisión y la disponibilidad de la información sobre el tiempo. Es posible que un servidor del Protocolo de hora de red (NTP) deba configurarse para proporcionar una fuente de tiempo sincronizada para todos los dispositivos. La configuración de esta opción excede el alcance de este curso.

Por ejemplo:

R2(config)#**service timestamps ?**
debug Timestamp debug messages
log Timestamp log messages
<cr>
R2(config)#**service timestamps**

Más adelante, en este capítulo, aprende acerca del comando **debug**. Los resultados del comando **debug** también pueden ser enviados a los registros.



El host de registro está:

- Dedicado al almacenamiento de registros
- Conectado a una red protegida o a una interfaz del router dedicada

4.3 Servicios de red de router seguro

4.3.1 Servicios e interfaces de routers vulnerables

Servicios e interfaces de routers vulnerables

Los routers Cisco admiten una gran cantidad de servicios de red en las capas 2, 3, 4 y 7, como se describe en la figura. Algunos de estos servicios son protocolos de Capa de aplicación que permiten a los usuarios y a los procesos del host a conectarse al router. Otros son procesos automáticos y configuraciones destinados a admitir configuraciones heredadas o especializadas que representan riesgos de seguridad. Algunos de estos servicios pueden restringirse o desactivarse para mejorar la seguridad sin distorsionar el uso operativo del router. Debe utilizarse la práctica de seguridad general de los routers para respaldar sólo el tráfico y los protocolos que una red necesita.

Generalmente, la mayoría de los servicios enumerados en esta sección no son necesarios. La tabla de la figura describe servicios generales de los routers vulnerables y enumera las mejores prácticas asociadas a esos servicios. Desconectar un servicio de red en el router mismo no le impide respaldar una red en que se utiliza ese protocolo. Por ejemplo, una red puede requerir servicios TFTP para respaldar los archivos de configuración y las imágenes del IOS. Por lo general, este servicio es proporcionado por un servidor TFTP dedicado. En algunos casos, un router también podría configurarse como servidor TFTP. Sin embargo, esto es muy poco frecuente. Por lo tanto, en la mayoría de los casos, el servicio TFTP del router debe desactivarse.

En muchos casos, el software IOS de Cisco admite la desactivación total de un servicio o la restricción del acceso a segmentos particulares de una red o a conjuntos de hosts. Si una parte determinada de una red necesita un servicio, pero el resto no, se deben utilizar las características de la restricción para limitar el alcance del servicio.

Normalmente, desactivar una característica de red automática impide que un tipo determinado de tráfico sea procesado por el router, o le impide viajar a través del router. Por ejemplo, el enrutamiento de origen IP es una característica poco utilizada del IP que se puede usar en los ataques contra la red. A menos que sea necesario para el funcionamiento de la red, el enrutamiento de origen IP debe estar desactivado.

Nota: El CDP se potencia en algunas implementaciones de Teléfono IP. Debe tenerse en cuenta antes de desactivar el servicio en general.

Servicios vulnerables del router

Característica	Descripción	Predeterminado	Recomendación
Protocolo de descubrimiento de Cisco (CDP)	Protocolo de capa 2 patentado entre dispositivos de Cisco.	Habilitado	El CDP no se necesita casi nunca, deshabilítelo.
Servidores pequeños TCP	Servicios de red TCP estándar: echo, chargen, etc.	>=11.3: deshabilitado 11.2: habilitado	Esta es una característica de versiones anteriores; deshabilítela de manera explícita.
Servidores UDP pequeños	Servicios de red UDP estándar: echo, discard, etc.	>=11.3: deshabilitado 11.2: habilitado	Esta es una característica de versiones anteriores; deshabilítela de manera explícita.
Finger	Servicio de búsqueda de usuario UNIX, permite listado remoto de usuarios.	Habilitado	Las personas sin autorización no deben conocer esto; deshabilítelo.
Servidor HTTP	Algunos dispositivos de Cisco del sistema operativo Internetwork (IOS, Internetwork Operating System) ofrecen una configuración basada en Web.	Varía según el dispositivo	Si no está en uso, deshabilítelo de manera explícita; de lo contrario, restrinja el acceso.
Servidor BOOTP	Realice el mantenimiento para permitir que otros routers arranquen desde éste.	Habilitado	Esto se necesita con poca frecuencia y puede abrir un agujero en la seguridad; deshabilítelo.

Carga automática de la configuración	El router intentará cargar su configuración mediante TFTP.	Deshabilitado	Esto se utiliza con poca frecuencia; deshabilítelo si no se encuentra en uso.
Enrutamiento IP de origen	Característica IP que permite que los paquetes especifiquen sus propias rutas.	Habilitado	Esta característica, muy poco usada, puede ser beneficiosa en ataques; deshabilítela.
ARP proxy	El router actuará como un proxy para una resolución de dirección de capa 2.	Habilitado	Deshabilite este servicio salvo que el router esté funcionando como puente LAN.
Broadcast dirigido IP	Los paquetes pueden identificar un LAN objetivo para broadcasts.	>=11.3: habilitado	El broadcast dirigido se puede utilizar para ataques; deshabilítelo.
Comportamiento del enrutamiento sin clase	El router enviará paquetes que no tengan una ruta concreta.	Habilitado	Ciertos ataques se pueden beneficiar de éste; deshabilítelo salvo que su red lo solicite.
Notificaciones de IP inalcanzables	El router notificará a los emisores, de manera explícita, acerca de direcciones IP incorrectas.	Habilitado	Puede ayudar con la asignación de red; deshabilitado en interfaces para redes que no son confiables.
Respuesta de la máscara IP	El router enviará una máscara de dirección IP de la interfaz en respuesta a una solicitud de máscara del protocolo de mensajes de control de Internet (ICMP, Internet Control Messaging Protocol).	Deshabilitado	Puede ayudar con la asignación de dirección IP; deshabilítela explícitamente en interfaces de redes que no son confiables.
Redireccionamientos IP	El router enviará un mensaje de redirección ICMP en respuesta a ciertos paquetes IP ruteados.	Habilitado	Puede ayudar con la asignación de red; deshabilítelo en interfaces de redes que no son confiables.
Servicio NTP	El router puede actuar como un servidor de tiempo para otros dispositivos y hosts.	Habilitado (siempre que NTP esté configurado)	Si no está en uso, deshabilítelo de manera explícita; de lo contrario, restrinja el acceso.
Protocolo de administración de red simple	Los routers pueden admitir consulta y configuración remota del protocolo de administración de red simple (SNMP, Simple Network Management Protocol).	Habilitado	Si no está en uso, deshabilítelo de manera explícita; de lo contrario, restrinja el acceso.
Servicio de nombres de dominio	Los routers pueden realizar la resolución de nombre servicio de nombre de dominio (DNS, Domain Name Service).	Habilitado (broadcast)	Configure la dirección del servidor DNS de manera explícita o deshabilite DNS.

Hay una variedad de comandos necesarios para desactivar servicios. El resultado **show running-config** de la figura proporciona una configuración de muestra de varios servicios que se han desactivado.
A continuación, se enumeran los servicios que, normalmente, deben desactivarse. Entre éstos se destacan:

- Los servicios pequeños tales como echo, discard y chargen: use el comando **no service tcp-small-servers** o **no service udp-small-servers**.
- BOOTP: use el comando **no ip bootp server**.
- Finger: use el comando **no service finger**.
- HTTP: use el comando **no ip http server**.
- SNMP: use el comando **no snmp-server**.

También es importante desactivar los servicios que permiten que determinados paquetes pasen a través del router, envíen paquetes especiales o se utilicen para la configuración del router remoto. Los comandos correspondientes para desactivar estos servicios son:

- Protocolo de descubrimiento de Cisco (CDP): use el comando **no cdp run**.

- Configuración remota: use el comando **no service config**.
- Enrutamiento de origen: use el comando **no ip source-route**.
- Enrutamiento sin clase: use el comando **no ip classless**.

Las interfaces del router pueden ser más seguras si se utilizan determinados comandos en el modo de configuración de interfaz:

- Interfaces no utilizadas: use el comando **shutdown**.
- Prevención de ataques SMURF: use el comando **no ip directed-broadcast**.
- Enrutamiento ad hoc: use el comando **no ip proxy-arp**.

Interfaces vulnerables del router

```
! ----- IP and network services Section
no cdp run
no ip source-route
no ip classless
no service tcp-small-servers
no service udp-small-servers
no ip finger
no service finger
no ip bootp server
no ip http server
no ip name-server
! ----- Boot control section
no boot network
no service config
! ----- SNMP Section (for totally disabling SNMP)
! set up totally restrictive access list
no access-list 70
access-list 70 deny any
! make SNMP read-only and subject to access list
snmp-server community aqiytj1726540942 ro 11
! disable SNMP trap and system-shutdown features
no snmp-server enable traps
no snmp-server system-shutdown
no snmp-server trap-auth
! turn off SNMP altogether
```

Vulnerabilidades de SNMP, NTP y DNS
La figura describe tres servicios de administración que también deben estar protegidos. Los métodos para desactivar o ajustar las configuraciones de estos servicios exceden el alcance de este curso. Estos servicios están contemplados en el CCNP: Curso Implementación de redes seguras y convergentes de área amplia.
Las descripciones y las pautas para proteger estos servicios se enumeran a continuación.

SNMP

SNMP es el protocolo de Internet estándar del monitoreo y la administración remotos automatizados. Hay varias versiones distintas de SNMP con propiedades de seguridad diferentes. Las versiones de SNMP anteriores a la versión 3 transportan información en forma de texto sin cifrar. Normalmente, se debe utilizar la versión 3 de SNMP.

NTP

Los routers Cisco y otros hosts utilizan NTP para mantener sus relojes con la hora del día exacta. Si es posible, los administradores de la red deben configurar todos los routers como parte de una jerarquía de NTP, lo que convierte a un router en el temporizador maestro y proporciona su hora a otros routers de la red. Si no hay una jerarquía de NTP disponible en la red, debe desactivar NTP.

Desactivar NTP en una interfaz no impide que los mensajes de NTP viajen a través del router. Para rechazar todos los mensajes de NTP en una interfaz determinada, use una lista de acceso.

DNS

El software IOS de Cisco admite la búsqueda de nombres de hosts con el Sistema de nombres de dominios (DNS). DNS proporciona la asignación entre nombres, como central.mydomain.com a las direcciones IP, como 14.2.9.250.

Desafortunadamente, el protocolo DNS básico no ofrece autenticación ni aseguramiento de la integridad. De manera predeterminada, las consultas de nombres se envían a la dirección de broadcast 255.255.255.255.

Si hay uno o más servidores de nombres disponibles en la red y se desea utilizar nombres en los comandos del IOS de Cisco, defina explícitamente las direcciones del servidor de nombres utilizando el comando de configuración global **ip name-server** *addresses*. De lo contrario, desactive la resolución de nombres DNS con el comando **no ip domain-lookup**. También es conveniente asignarle un nombre al router mediante el uso del comando **hostname**. El nombre asignado al router aparece en el indicador.

Vulnerabilidades de SNMP, NTP y DNS

Protocolo	Vulnerabilidad
SNMP	Las versiones 1 y 2 pasan información de administración y cadenas de comunidad (contraseñas) en texto sin cifrar
NTP	El NTP deja los puertos de escucha abiertos y vulnerables
DNS	Puede ayudar a los atacantes a conectar las direcciones IP a nombres de dominio

4.3.2 Protección de los protocolos de enrutamiento

Descripción general de la autenticación del protocolo de enrutamiento

Como administrador de la red, debe saber que sus routers corren el riesgo de sufrir ataques en la misma medida que sus sistemas de usuario final. Las personas que cuentan con un programa detector de paquetes, como Wireshark pueden leer la información que se propaga entre routers. En general, los sistemas de enrutamiento pueden sufrir ataques de dos maneras:

- Interrupción de pares
- Falsificación de información de enrutamiento

La interrupción de pares es el menos crítico de los dos ataques, porque los protocolos de enrutamiento se reparan a sí mismos, lo que hace que la interrupción dure solamente un poco más que el ataque mismo.

Una clase más sutil de ataque se centra en la información que se transporta dentro del protocolo de enrutamiento. La información de enrutamiento falsificada, generalmente, puede utilizarse para hacer que los sistemas se proporcionen información errónea (mientan) entre sí, para provocar un DoS o hacer que el tráfico siga una ruta que, normalmente, no seguiría. Las consecuencias de falsificar información de enrutamiento son las siguientes:

1. El tráfico se redirecciona para crear routing loops, como se observa en la figura

2. El tráfico se redirecciona para que pueda monitorearse en un enlace inseguro

3. El tráfico se redirecciona para descartarlo

Una forma sencilla de atacar el sistema de enrutamiento es atacar a los routers, mediante la ejecución de los protocolos de enrutamiento, obtener acceso a los routers e introducir información falsa. Tenga en cuenta que cualquier persona que esté "escuchando" puede capturar actualizaciones de enrutamiento.

Haga clic en el botón Reproducir de la figura para ver una animación de un ataque de routing loop.

La animación muestra un ejemplo de un ataque que crea un routing loop. Un agresor logró conectar directamente el enlace entre los routers R2 y R3. El agresor inyecta información de enrutamiento falsa dirigida al router R1 solamente, e indica que R3 es el destino preferido para la ruta del host 192.168.10.10/32. Pese a que R1 tiene una entrada de tabla de enrutamiento a la red 192.168.10.0/24 conectada directamente, agrega la ruta inyectada a su tabla de enrutamiento debido a la mayor longitud de la máscara de subred. Una ruta que tiene una correspondiente máscara de subred de mayor longitud se considera superior a una ruta con una máscara de subred más corta. En consecuencia, cuando un router recibe un paquete, selecciona la máscara de subred de mayor longitud porque constituye una ruta más precisa hacia el destino.

Cuando PC3 envía un paquete a PC1 (192.168.10.10/24), R1 no envía el paquete al host PC1. En cambio, enruta el paquete hacia el router R3, porque, en lo que a ello respecta, la mejor ruta hacia 192.168.10.10/32 es a través de R3. Cuando R3 obtiene el paquete, observa su tabla de enrutamiento y envía el paquete nuevamente hacia R1, lo que crea el loop.

La mejor manera de proteger la información de enrutamiento en la red es autenticar los paquetes del protocolo de enrutamiento mediante el algoritmo message digest 5 (MD5). Un algoritmo como MD5 permite a los routers comparar las firmas que deben ser todas iguales.

Haga clic en el botón Proteger actualización de la figura.

La figura muestra la manera en la que cada router de la cadena de actualización crea una firma. Los tres componentes de dicho sistema incluyen:

1. Algoritmo de encriptación que, por lo general, es de conocimiento público

2. Clave utilizada en el algoritmo de encriptación, que es un secreto compartido por los routers que autentican sus paquetes

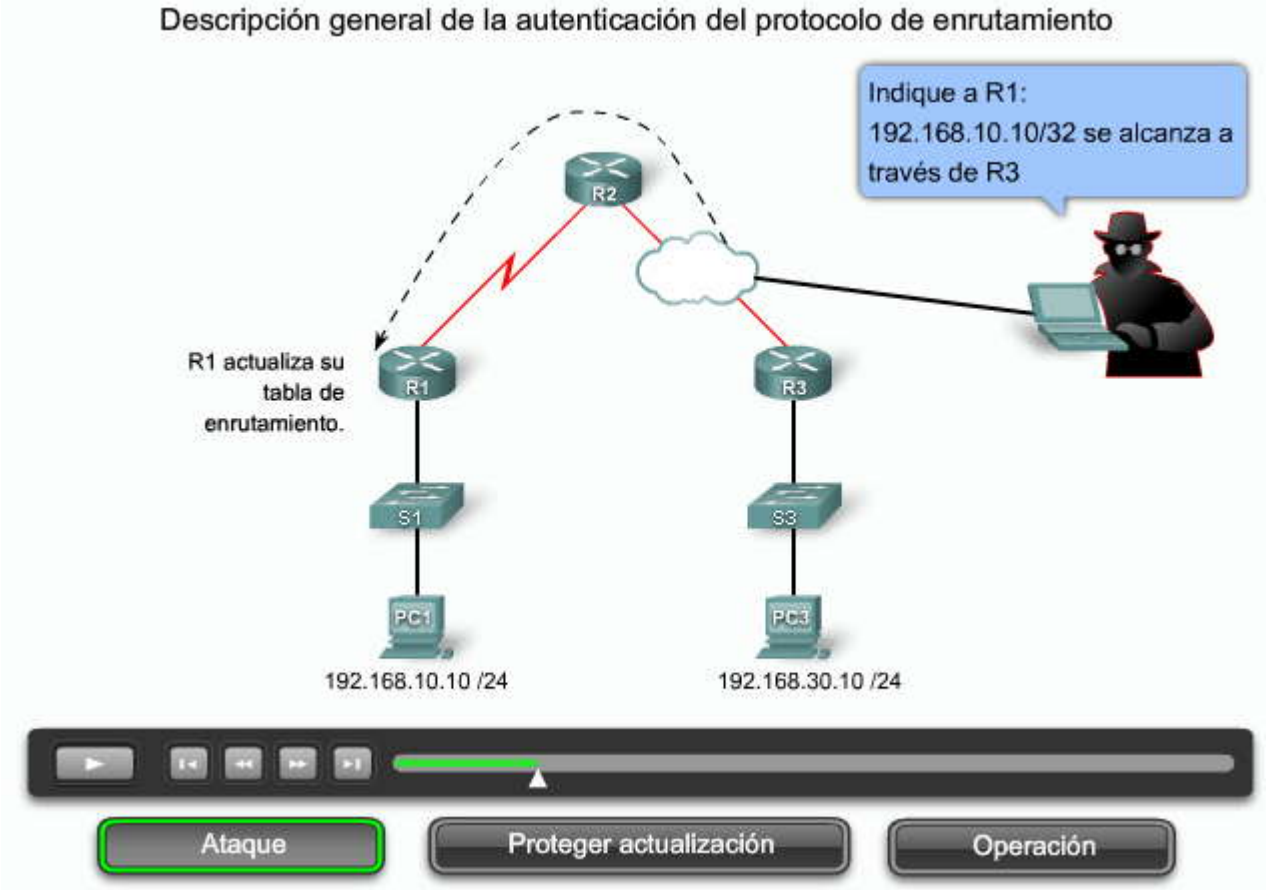
3. Contenidos del paquete en sí mismo

Haga clic en el botón Operación de la figura.

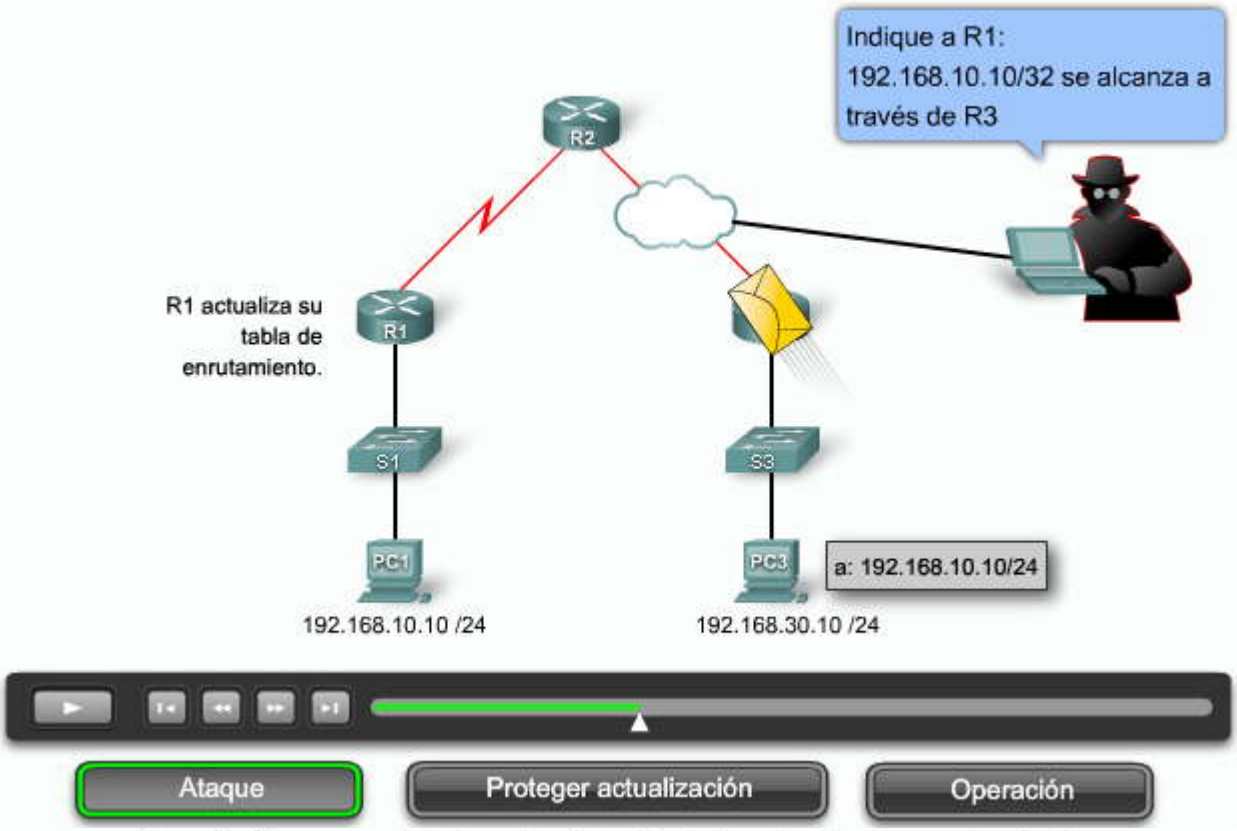
Haga clic en Reproducir para ver una animación.

En la animación, vemos la manera en la que cada router autentica la información de enrutamiento. Por lo general, el creador de la información de enrutamiento produce una firma mediante la clave y los datos de enrutamiento que está por enviar como entradas al algoritmo de encriptación. Los routers que reciben estos datos de enrutamiento pueden repetir el proceso utilizando la misma clave, los datos que recibió y los mismos datos de enrutamiento. Si la firma que el receptor computa es la misma que la que computa el remitente, los datos y la clave deben ser los mismos que transmitió el remitente y la actualización se autentica.

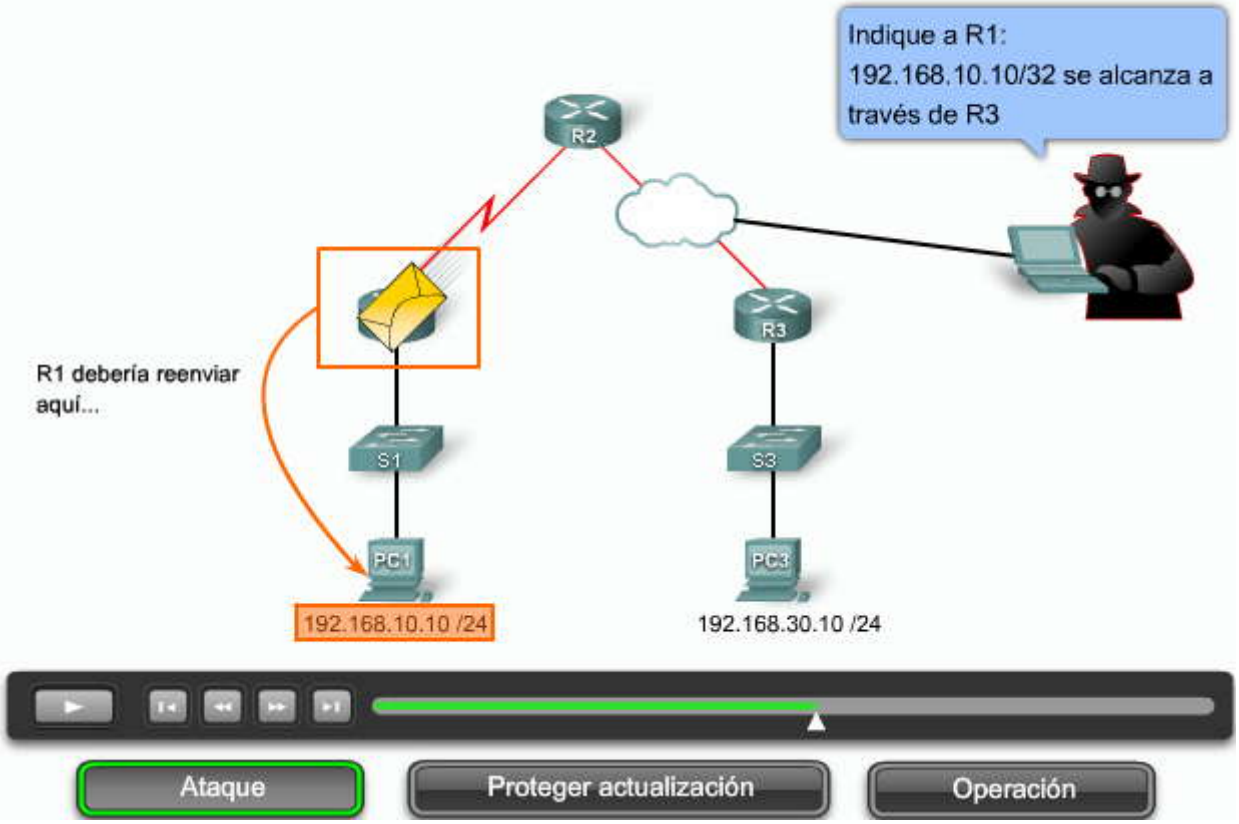
RIPv2, EIGRP, OSPF, IS-IS y BGP, todos ellos admiten diversas formas de autenticación MD5.



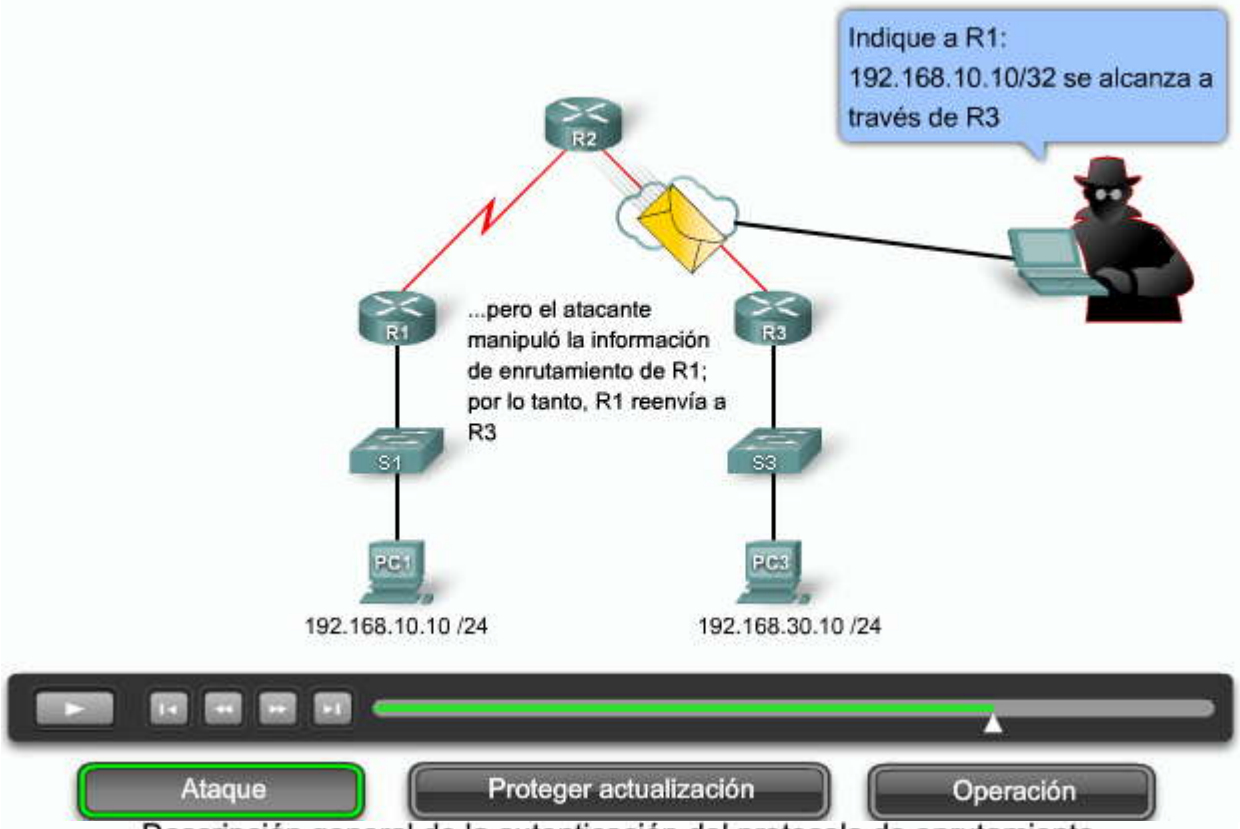
Descripción general de la autenticación del protocolo de enrutamiento



Descripción general de la autenticación del protocolo de enrutamiento

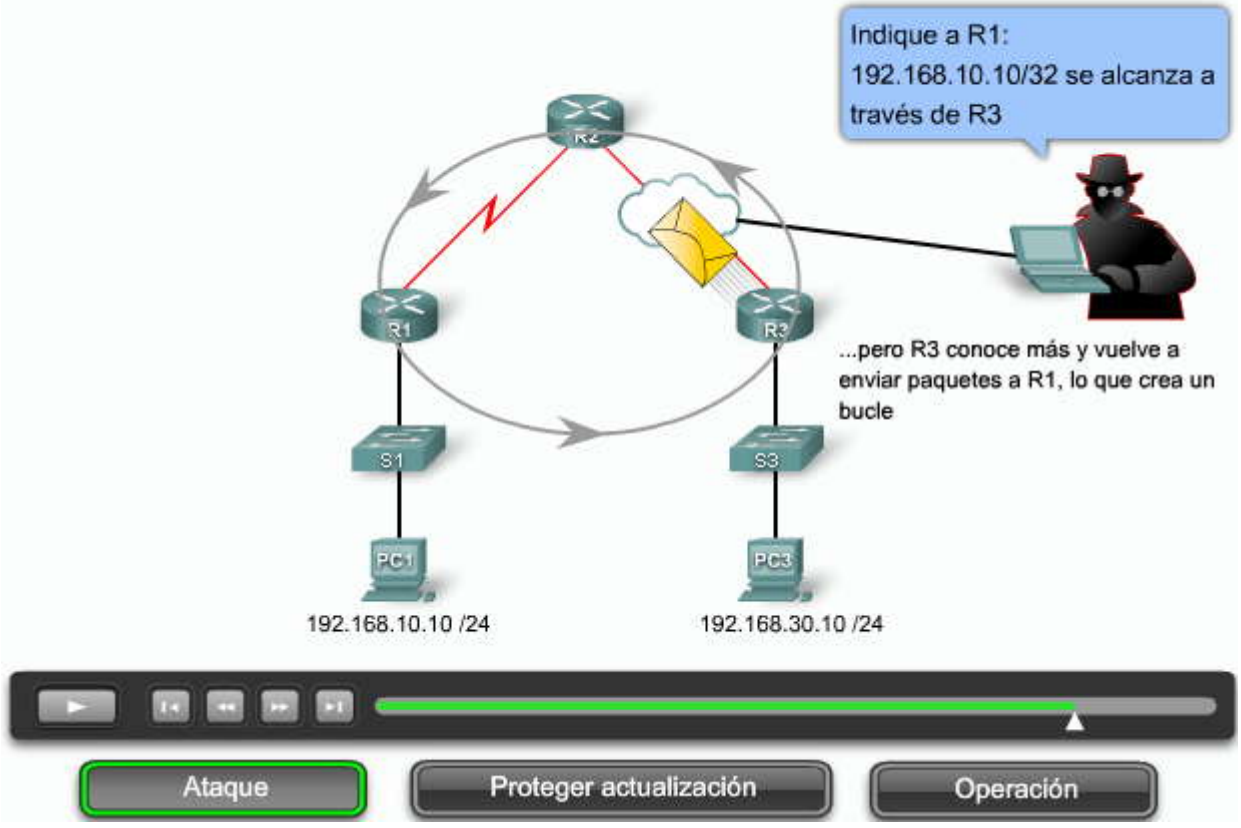


Descripción general de la autenticación del protocolo de enrutamiento

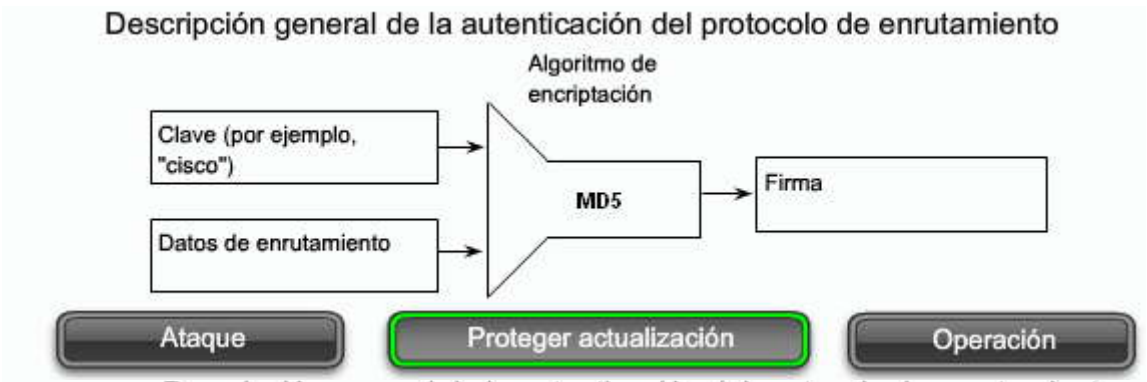


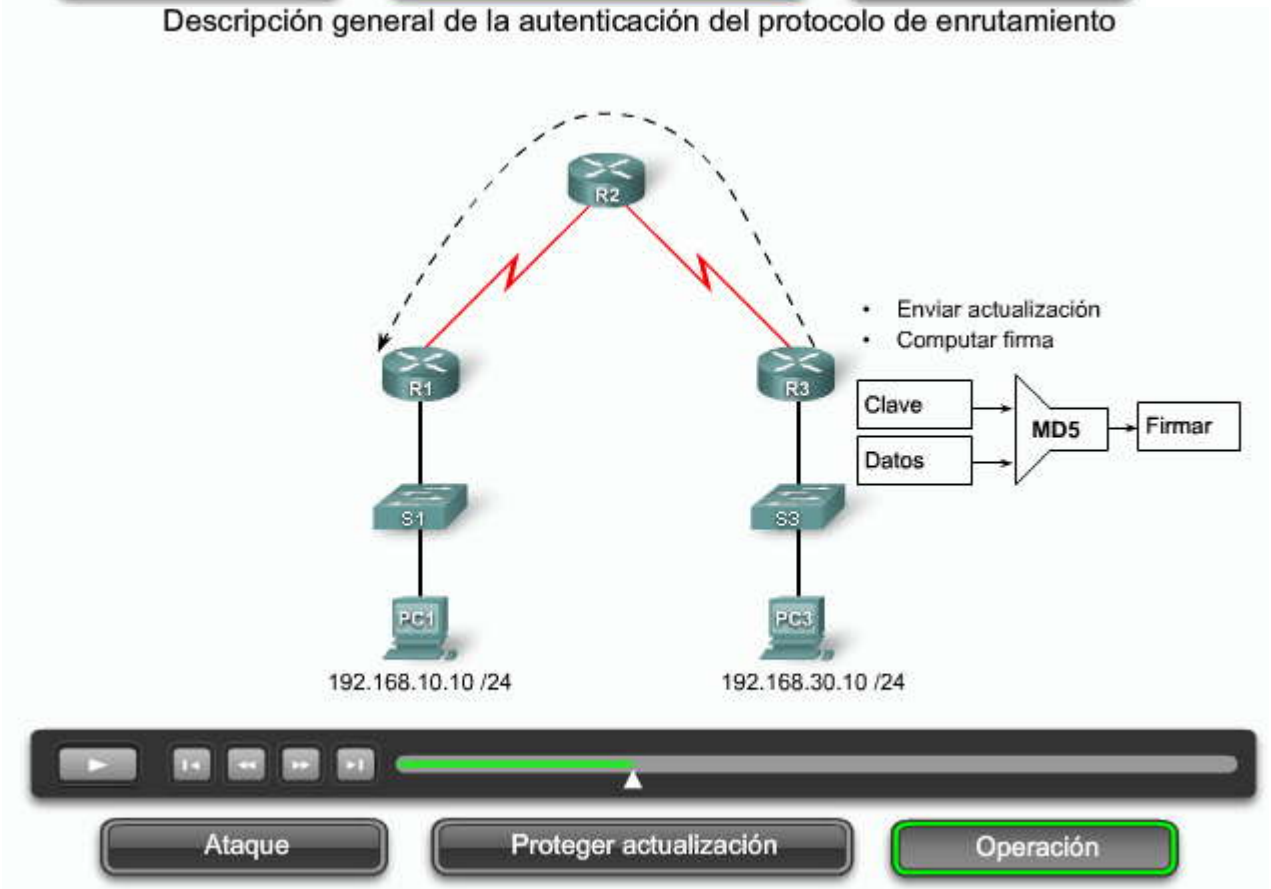
Ataque | Proteger actualización | Operación

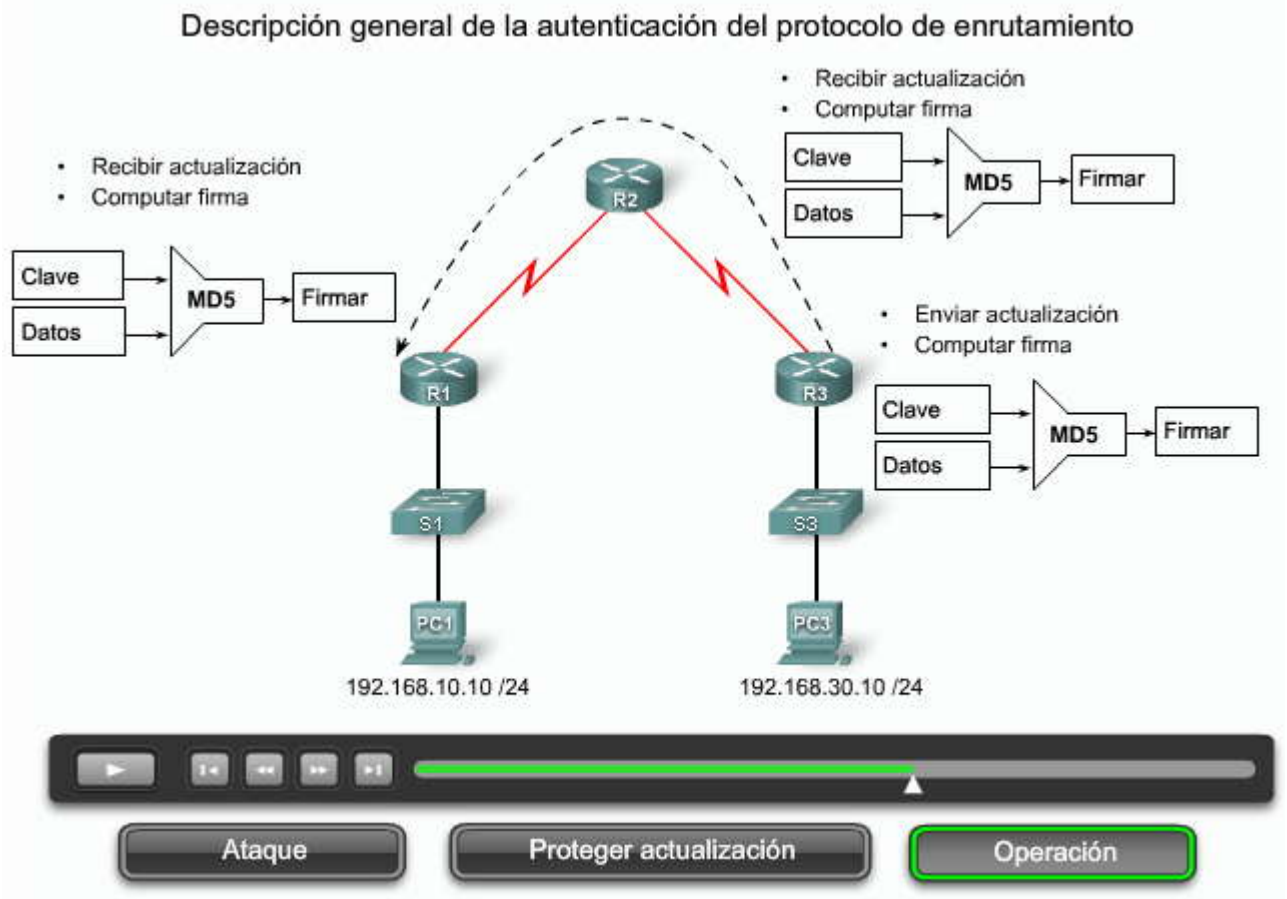
Descripción general de la autenticación del protocolo de enrutamiento



Ataque | Proteger actualización | Operación


Descripción general de la autenticación del protocolo de enrutamiento
Algoritmo de encriptación
Clave (por ejemplo, "cisco")
Datos de enrutamiento
MD5
Firma
Ataque
Proteger actualización
Operación


Descripción general de la autenticación del protocolo de enrutamiento
R2
R1
R3
S1
S3
PC1
PC3
192.168.10.10 /24
192.168.30.10 /24
Enviar actualización
Computar firma
Clave
Datos
MD5
Firmar
Ataque
Proteger actualización
Operación



Configuración de RIPv2 con autenticación del protocolo de enrutamiento

La topología de la figura muestra una red configurada con el protocolo de enrutamiento RIPv2. RIPv2 admite la autenticación del protocolo de enrutamiento. Para proteger las actualizaciones de enrutamiento, cada router debe configurarse para admitir la autenticación. Los pasos para proteger las actualizaciones de RIPv2 son los siguientes:

Paso 1. Impida la propagación de actualizaciones de enrutamiento RIP

Paso 2. Impida la recepción de actualizaciones RIP no autorizadas

Paso 3. Verifique el funcionamiento del enrutamiento RIP

Impedir la propagación de actualizaciones de enrutamiento RIP

Debe impedir que un intruso que esté escuchando en la red reciba actualizaciones a las que no tiene derecho. Debe hacerlo forzando todas las interfaces del router a pasar al modo pasivo y, a continuación, activando sólo aquellas interfaces que son necesarias para enviar y recibir actualizaciones RIP. Una interfaz en modo pasivo recibe actualizaciones pero no las envía. Debe configurar las interfaces en modo pasivo en todos los routers de la red.

Haga clic en el botón Config del Paso 1.

La figura muestra los comandos de configuración necesarios para controlar qué interfaces participan en las actualizaciones de enrutamiento. Las actualizaciones de enrutamiento nunca deben ser publicadas en interfaces que no están conectadas a otros routers. Por ejemplo, las interfaces LAN del router R1 no se conectan a otros routers y, por lo tanto, no deben publicar actualizaciones de enrutamiento. Sólo la interfaz S0/0/0 del router R1 debe publicar actualizaciones de enrutamiento.

En los resultados de la pantalla, el comando **passive-interface default** desactiva las publicaciones de routers en todas las interfaces. Esto también incluye la interfaz S0/0/0. El comando **no passive-interface s0/0/0** activa la interfaz S0/0/0 para enviar y recibir actualizaciones RIP.

Haga clic en el botón Paso 2 de la figura.

Impedir la recepción de actualizaciones RIP no autorizadas

En la figura, se impide que el intruso intercepte actualizaciones RIP porque la autenticación MD5 ha sido activada en los routers, R1, R2 y R3; los routers que participan en las actualizaciones RIP.

Haga clic en el botón Config del Paso 2.

Los resultados muestran los comandos necesarios para configurar la autenticación del protocolo de enrutamiento en el router R1. Los routers R2 y R3 también deben ser configurados con estos comandos en las interfaces adecuadas.

El ejemplo muestra los comandos necesarios para crear una cadena de claves denominada RIP_KEY. Pese a que es posible considerar varias claves, nuestro ejemplo muestra sólo una clave. La clave 1 está configurada para contener una cadena de claves denominada cisco. La cadena de claves es similar a una contraseña y los routers que intercambian claves de autenticación deben estar configurados con la misma cadena de claves. La interfaz S0/0/0 está configurada para admitir la autenticación MD5. La cadena RIP_KEY y la actualización de enrutamiento se procesan mediante el algoritmo MD5 para producir una firma única.

Una vez que R1 está configurado, los otros routers reciben actualizaciones de enrutamiento encriptadas y, en consecuencia, ya no pueden descifrar las actualizaciones provenientes de R1. Esta condición se mantiene hasta que cada router de la red esté configurado con autenticación del protocolo de enrutamiento.

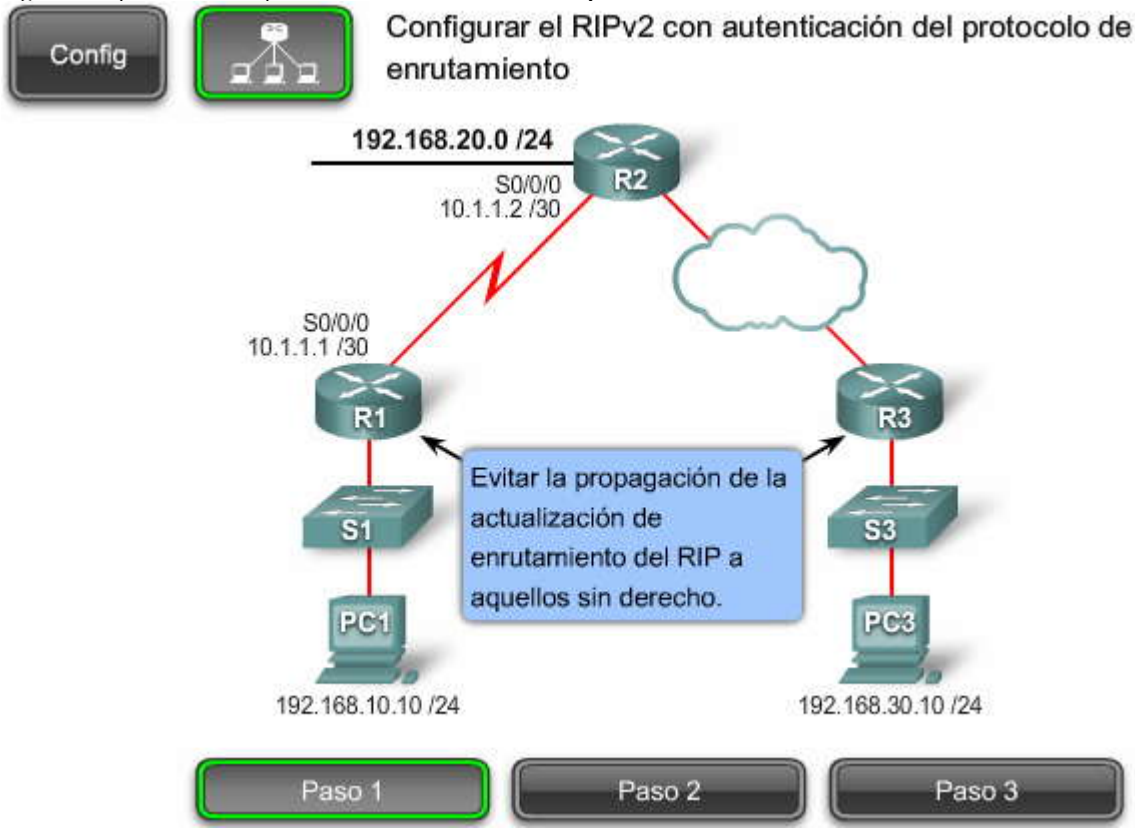
Haga clic en el botón Paso 3 de la figura.

Verificar el funcionamiento del enrutamiento RIP

Después de configurar todos los routers de la red, debe verificar el funcionamiento del enrutamiento RIP en la red.

Haga clic en el botón Config del Paso 3.

Al usar el comando **show ip route**, el resultado confirma que el router R1 se ha autenticado con los demás routers y ha logrado adquirir las rutas provenientes de los routers R2 y R3.

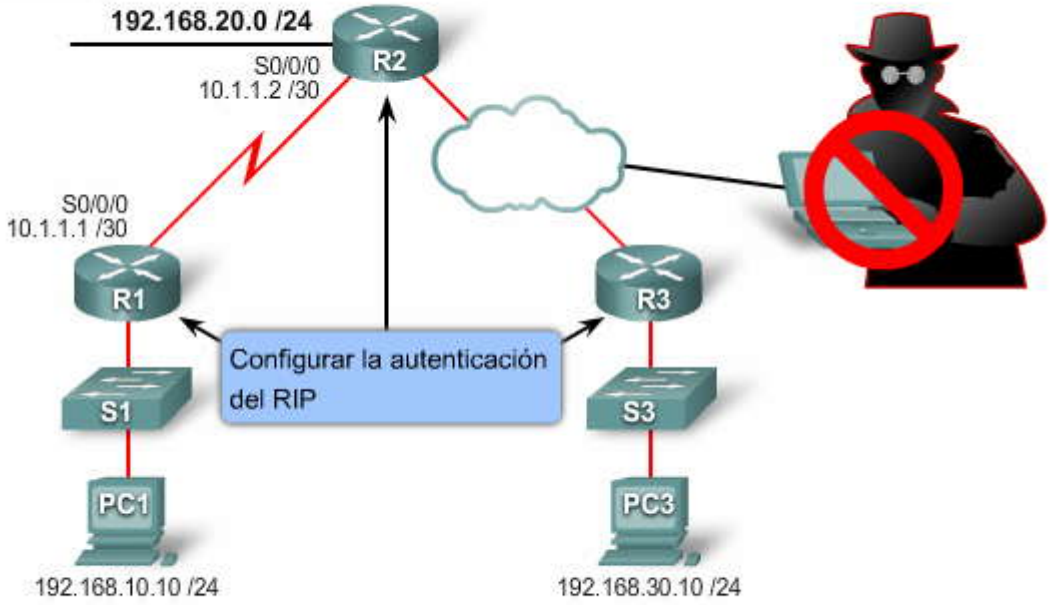


Paso 1: Evitar la propagación de la actualización del enrutamiento del RIP

```
R1(config)#router rip
R1(config-router)#passive-interface default
R1(config-router)#no passive-interface s0/0/0
```

Config

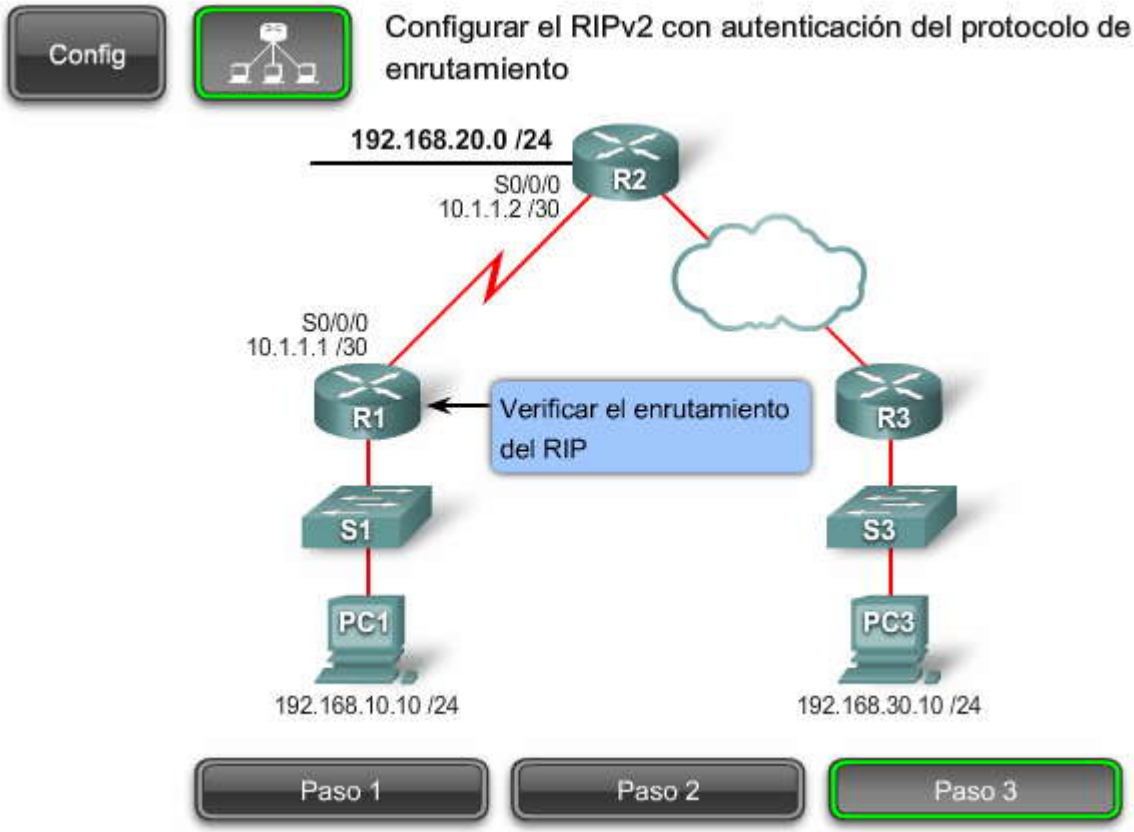
Configurar el RIPv2 con autenticación del protocolo de enrutamiento



Paso 1 | Paso 2 | Paso 3

Paso 2: Evitar la recepción de actualizaciones del RIP sin autorización

```
R1(config)#key chain RIP_KEY
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string cisco

R1(config)#int s0/0/0
R1(config-if)#ip rip authentication mode md5
R1(config-if)#ip rip authentication key-chain RIP_KEY
```



Paso 3: Verificar el enrutamiento del RIP

```
R1#show ip route
Codes: C - connected, S - static, R - RIP,
---Output Omitted---

R    192.168.30.0/24 [120/2] via 10.1.1.2, 00:00:16, Serial0/0/0
C    192.168.10.0/24 is directly connected, FastEthernet0/0
R    192.168.20.0/24 [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0
     10.0.0.0/8 is variably subnetted, 2 subnets, 1 masks
---Output omitted---
```

Descripción general de la autenticación del protocolo de enrutamiento de EIGRP y OSPF

La autenticación del protocolo de enrutamiento también debe ser configurada para otros protocolosde enrutamiento, como EIGRP y OSPF. Para obtener más detalles acerca de la autenticación del protocolo de enrutamiento de EIGRP y OSPF, consulte CCNP2: Implementación de redes seguras y convergentes de área amplia.

Haga clic en el botón EIGRP de la figura.

EIGRP

La figura muestra los comandos necesarios para configurar la autenticación del protocolo de enrutamiento de EIGRP en el router R1. Estos comandos son muy similares a los que utilizó para la autenticación MD5 de RIPv2. Los pasos necesarios para configurar la autenticación del protocolo de enrutamiento de EIGRP en el router R1 son los siguientes:

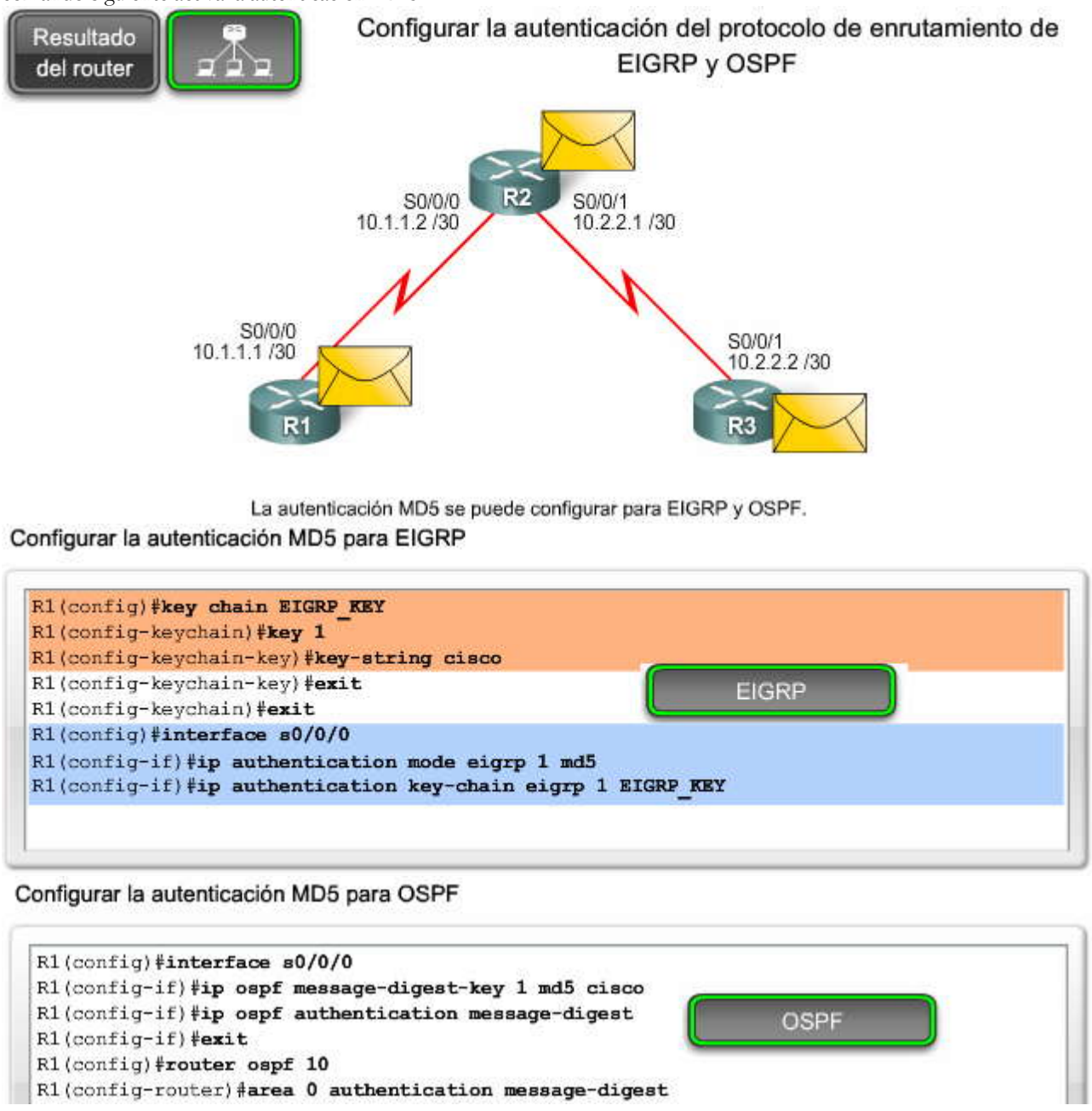
Paso 1. El área superior resaltada muestra cómo crear una cadena de claves para ser utilizada por todos los routers de la red. Estos comandos crean una cadena de claves denominada EIGRP_KEY y coloca su terminal en el modo de configuración de cadena de claves, un número de clave 1 y un valor de cadena de claves de cisco.

Paso 2. El área inferior resaltada muestra cómo activar la autenticación MD5 de los paquetes de EIGRP que viajan a través de una interfaz.

Haga clic en el botón OSPF de la figura.

OSPF

La figura muestra los comandos necesarios para configurar la autenticación del protocolo de enrutamiento de OSPF en el router R1 de la interfaz S0/0/0. El primer comando especifica la clave que se utilizará para la autenticación MD5. El comando siguiente activa la autenticación MD5.



Esta actividad contempla la autenticación sencilla de OSPF y la autenticación MD5 (message digest 5) de OSPF. Puede activar la autenticación en OSPF para intercambiar información de actualizaciones de enrutamiento de manera segura. Con la autenticación sencilla, se envía la contraseña como texto sin cifrar a través de la red. La autenticación sencilla se utiliza cuando los dispositivos dentro de un área no pueden admitir la autenticación MD5 más segura. Con la autenticación MD5, la contraseña no se envía a través de la red. MD5 se considera el modo de autenticación de OSPF más seguro. Cuando configura la autenticación, debe configurar un área completa con el mismo tipo de autenticación. En esta actividad, configura la autenticación sencilla entre R1 y R2, y la autenticación MD5 entre R2 y R3.
Se proporcionan instrucciones detalladas dentro de la actividad y en el siguiente enlace al PDF.
Instrucciones de la actividad (PDF)

4.3.3 Bloqueo de su router con Auto Secure de Cisco

AutoSecure de Cisco utiliza un único comando para desactivar procesos y servicios no esenciales del sistema y elimina amenazas de seguridad potenciales. Puede configurar AutoSecure en el modo EXEC privilegiado mediante el comando **auto secure** en uno de estos dos modos:

- **Modo interactivo**: este modo le indica opciones para activar y desactivar servicios y otras características de seguridad. Es el modo predeterminado.
- **Modo no interactivo**: ejecuta automáticamente el comando auto secure con la configuración predeterminada recomendada de Cisco. Este modo se activa con la opción del comando no-interact.

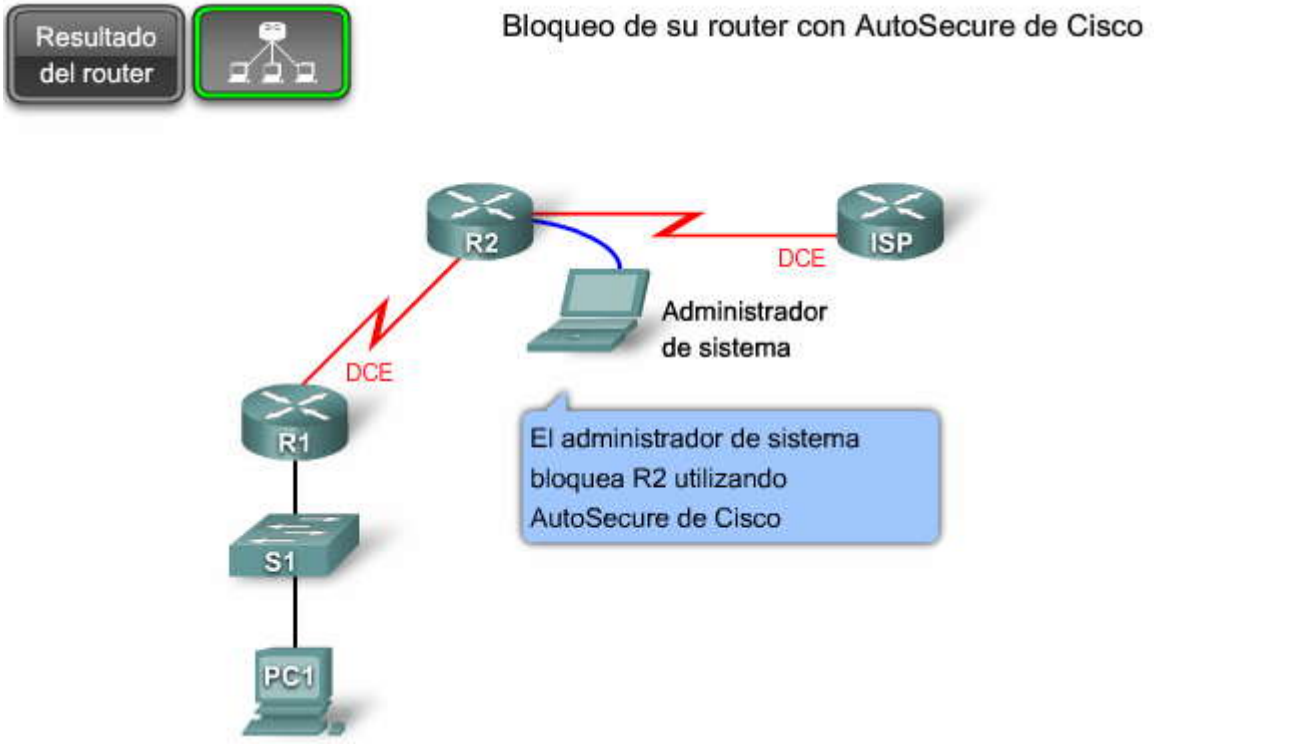
Haga clic en el botón Resultados del router de la figura.

AutoSecure en un router Cisco

Los resultados de la pantalla muestran un resultado parcial de la configuración de AutoSecure de Cisco. Para iniciar el proceso de proteger un router, emita el comando **auto secure**. AutoSecure de Cisco le pide una cantidad de elementos, entre los que se incluyen:

- Detalles de la interfaz
- Títulos
- Contraseñas
- SSH
- Características del firewall del IOS

Nota: El Administrador de routers y dispositivos de seguridad (SDM, Security Device Manager) proporciona una característica similar al comando AutoSecure de Cisco. Esta característica se describe en la sección "Uso del SDM de Cisco".



```
R1#auto secure
Is this router connected to internet? [no]:y
Enter the number of interfaces facing internet [1]:1
Enter the interface name that is facing internet:Serial0/1/0
Securing Management plane services..

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol
(output omitted)
```

4.4 Uso del SDM de Cisco

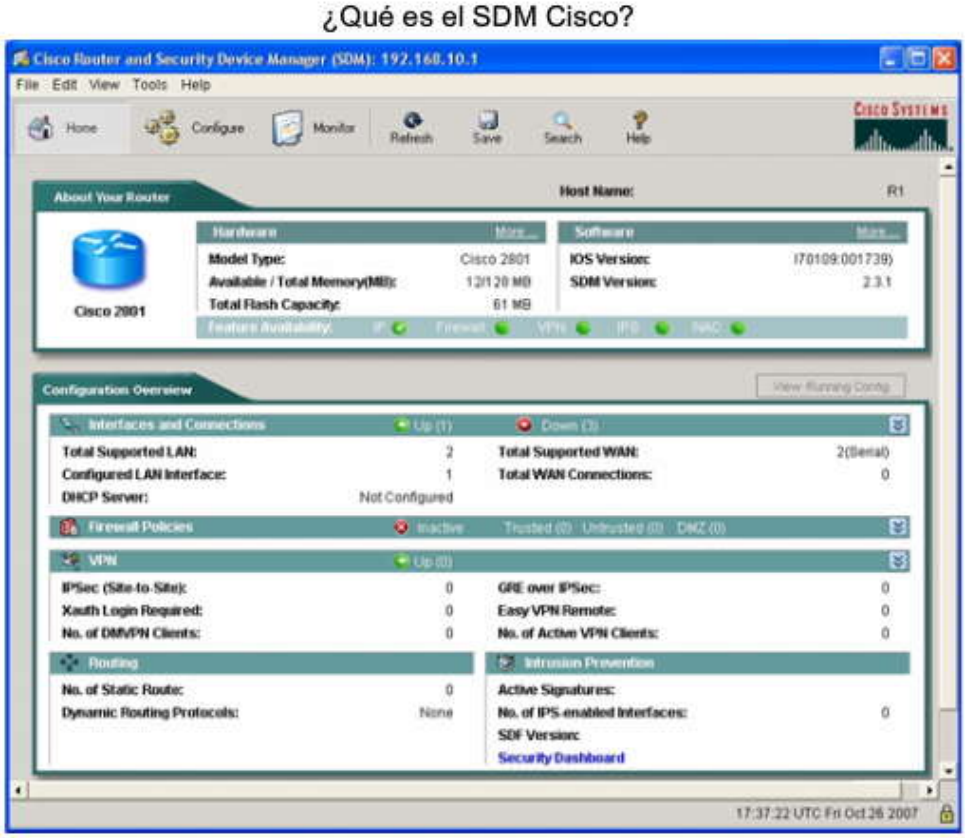
4.4.1 Descripción general del SDM de Cisco

¿Qué es el SDM de Cisco?

El Administrador de routers y dispositivos de seguridad (SDM) es una herramienta de administración de dispositivos basada en la Web y fácil de usar, diseñada para configurar la LAN, la WAN y las características de seguridad en los routers basados en el software IOS de Cisco.

La figura muestra la pantalla principal del SDM. La interfaz ayuda a los administradores de redes de empresas pequeñas a medianas a realizar las operaciones cotidianas. Proporciona asistentes inteligentes fáciles de usar, automatiza la administración de seguridad de los routers y brinda ayuda en línea y tutoriales integrales.

SDM de Cisco admite una amplia gama de versiones de software IOS de Cisco. Viene preinstalado en todos los nuevos routers de servicios integrados de Cisco. Si no está preinstalado, debe instalarlo. Los archivos del SDM se pueden instalar en el router, en una PC o en ambos. Una ventaja de instalar el SDM en la PC es que ahorra memoria del router y le permite utilizar el SDM para administrar otros routers de la red. Si el SDM de Cisco se encuentra preinstalado en el router, Cisco recomienda utilizar el SDM de Cisco para realizar la configuración inicial.

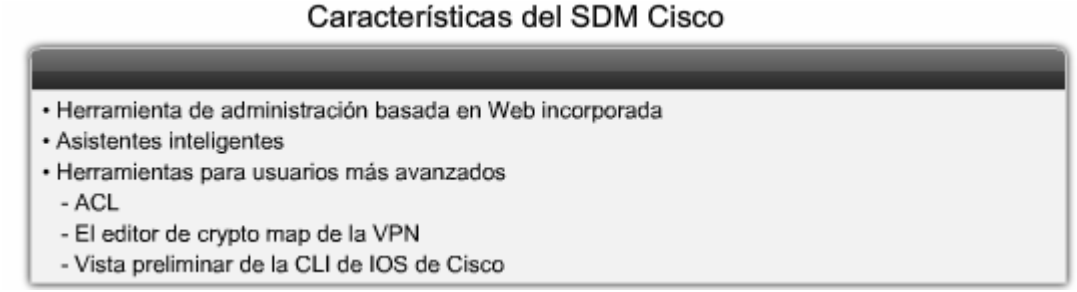


Características del SDM de Cisco

El SDM de Cisco simplifica la configuración de los routers y de la seguridad mediante el uso de varios asistentes inteligentes que permiten la configuración eficiente de la red privada virtual (VPN) de los routers clave y los parámetros del firewall del IOS de Cisco. Esta capacidad permite a los administradores rápida y fácilmente implementar, configurar y controlar los routers de acceso de Cisco.

Los asistentes inteligentes del SDM de Cisco guían a los usuarios paso por paso a través del flujo de trabajo de la configuración de router y de seguridad mediante la configuración sistemática de las interfaces LAN y WAN, el firewall, IPS y las VPN.

Los asistentes inteligentes del SDM de Cisco pueden detectar configuraciones incorrectas de manera inteligente y proponer modificaciones, como permitir el tráfico DHCP a través de un firewall si la interfaz WAN está dirigida al DHCP. La ayuda en línea incorporada al SDM de Cisco contiene información de respaldo adecuada, además de los procedimientos paso a paso necesarios para ayudar a los usuarios a introducir los datos correctos en el SDM de Cisco.



4.4.2 Configuración de su router para que sea compatible con el SDM de Cisco

El SDM de Cisco debe estar instalado en todos los routers de Cisco nuevos. Si tiene un router que ya está en uso, pero no tiene SDM de Cisco, puede instalarlo y ejecutarlo sin interrumpir el tráfico de la red. Antes de instalarlo en un router en funcionamiento, debe asegurarse de que el archivo de configuración del router cuente con algunos valores de configuración. La figura muestra una topología en la que el administrador del sistema instala el SDM de Cisco en el router R1.

Para configurar el SDM de Cisco en un router que ya está en uso, sin interrumpir el tráfico de la red, siga estos pasos:

Paso 1. Obtenga acceso a la interfaz CLI de Cisco del router mediante la conexión Telnet o de consola

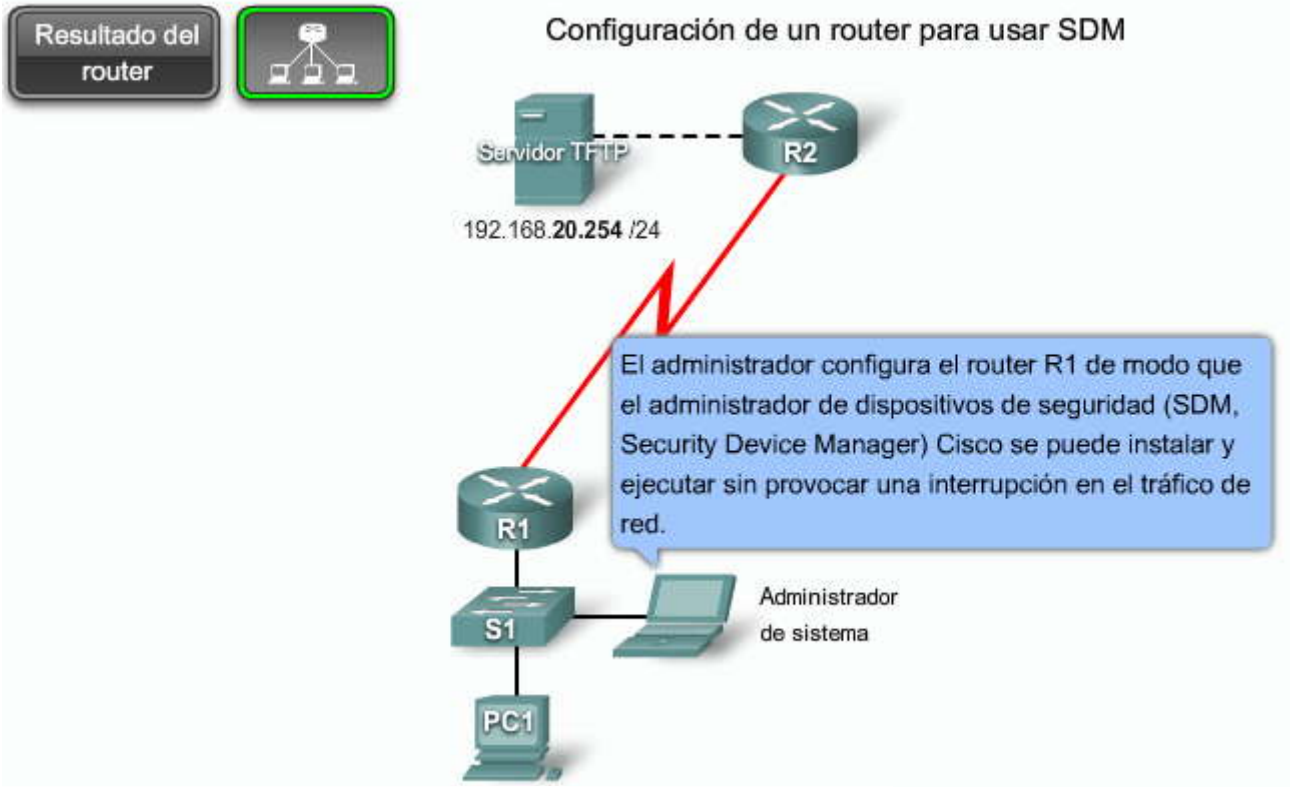
Paso 2. Active los servidores HTTP y HTTPS en el router

Paso 3. Cree una cuenta de usuario configurada con nivel de privilegio 15 (active los privilegios)

Paso 4. Configure SSH y Telnet para la conexión local y nivel de privilegio 15

Haga clic en el botón Resultado del router de la figura.

Los resultados de la pantalla muestran un ejemplo de la configuración necesaria para asegurarle que puede instalar y ejecutar el SDM de Cisco en un router de producción sin interrumpir el tráfico de la red.



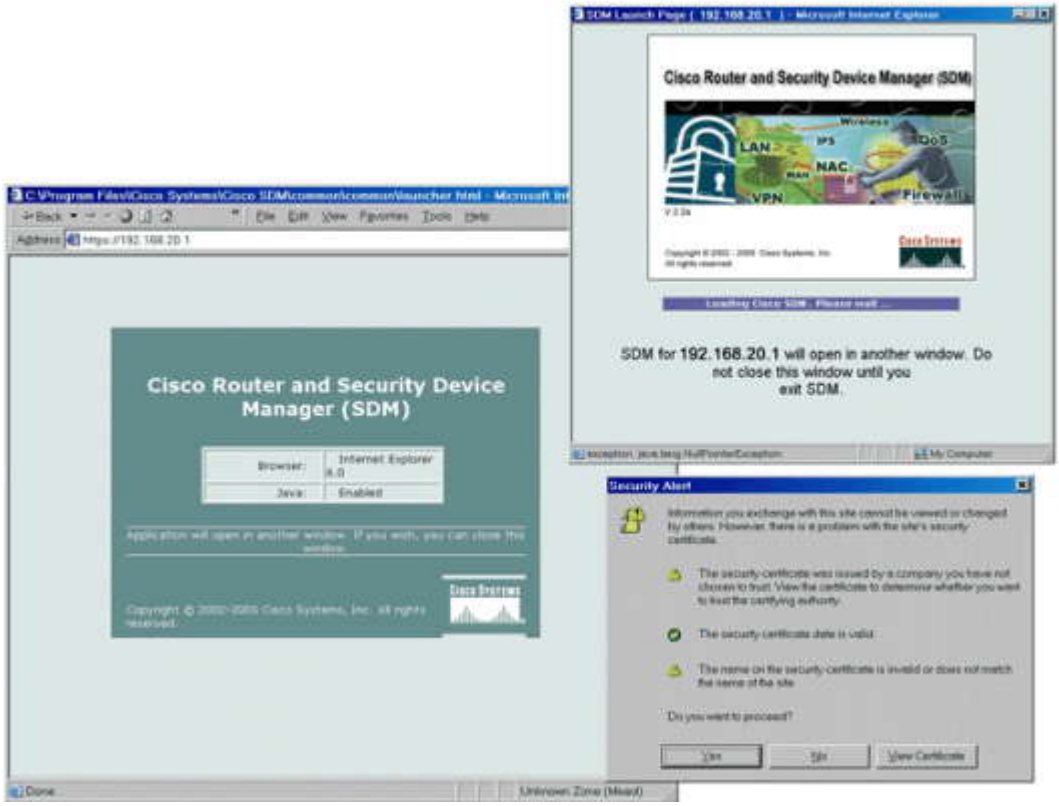

```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# ip http server
R1(config)# ip http secure-server
R1(config)# ip http authentication local
R1(config)# username Student privilege 15 secret cisco
R1(config)# line vty 0 4
R1(config-line)# privilege level 15
R1(config-line)# login local
R1(config-line)# transport input telnet ssh
R1(config-line)# exit
```

4.4.3 Inicio del SDM de Cisco

El SDM de Cisco se almacena en la memoria flash del router. También se puede almacenar en una PC local. Para iniciar el SDM de Cisco utilice el protocolo HTTPS y coloque la dirección IP del router en el explorador. La figura muestra el explorador con la dirección https://198.162.20.1 y la página de inicio del SDM de Cisco. El prefijo http:// puede ser utilizado si no hay SSL disponible. Cuando aparece el cuadro de diálogo de nombre de usuario y contraseña (no se muestra), escriba un nombre de usuario y una contraseña para la cuenta privilegiada (nivel de privilegio 15) en el router. Una vez que aparece la página de inicio, aparece un applet Java con signo del SDM de Cisco que debe permanecer abierto mientras se ejecuta el SDM de Cisco. Dado que se trata de un applet Java con signo del SDM de Cisco, es posible que se le solcite que acepte un certificado. La alerta de seguridad del certificado aparece en el extremo inferior derecho de la figura.

Nota: Los pasos de la secuencia de inicio de sesión pueden variar según si ejecuta SDM de Cisco desde una PC o, directamente, desde un router ISR de Cisco.

Inicio del SDM de Cisco



4.4.4 La interfaz SDM de Cisco

Descripción general de la página de inicio de SDM de Cisco

Después de iniciar el SDM de Cisco y una vez conectado, la primera página que se muestra es la página Descripción general.

Esta página muestra el modelo del router, la cantidad total de memoria, las versiones de flash, IOS y SDM, el hardware instalado y un resumen de algunas características de seguridad, como estado del firewall y la cantidad de conexiones de VPN activas.

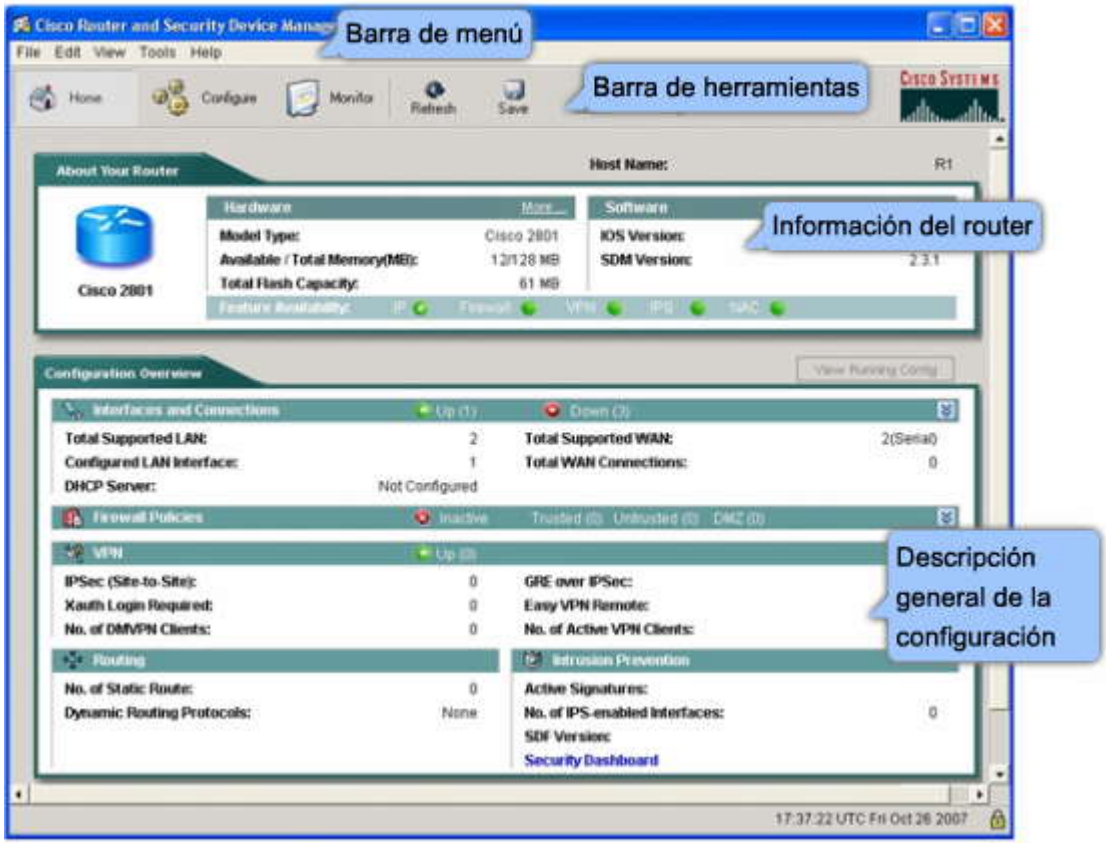
Específicamente, proporciona información básica sobre el hardware, el software y la configuración del router:

- Barra de menú: la parte superior de la pantalla tiene una barra de menú típica con los elementos de menú Archivo, Edición, Ver, Herramientas y Ayuda.
- Barra de herramientas: debajo de la barra de menú, están los asistentes y modos de SDM que se pueden seleccionar.
- Información del router: el modo actual se muestra del lado izquierdo, debajo de la barra de herramientas.

Nota: La barra de menú, la barra de herramientas y el modo actual se muestran siempre en la parte superior de cada pantalla. Las demás áreas de la pantalla cambian de acuerdo con el modo y la función que se está ejecutando.

- Descripción general de la configuración: resume los valores de configuración. Para visualizar la configuración en ejecución, haga clic en el botón **Ver configuración en ejecución**

Descripción general de la página de inicio del SDM Cisco



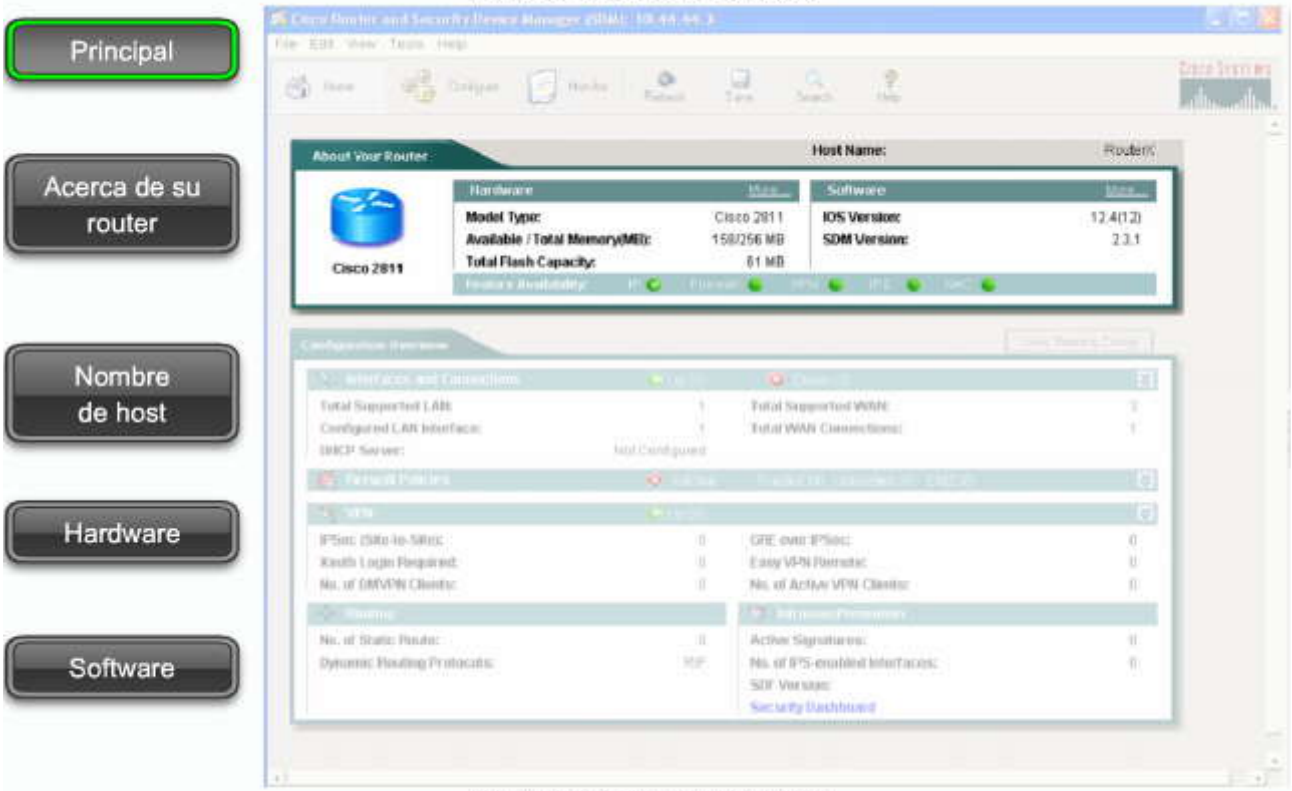
Área Acerca de su router

Al hacer clic en los botones de la figura, puede ver los detalles asociados con cada uno de los siguientes elementos dela GUI:

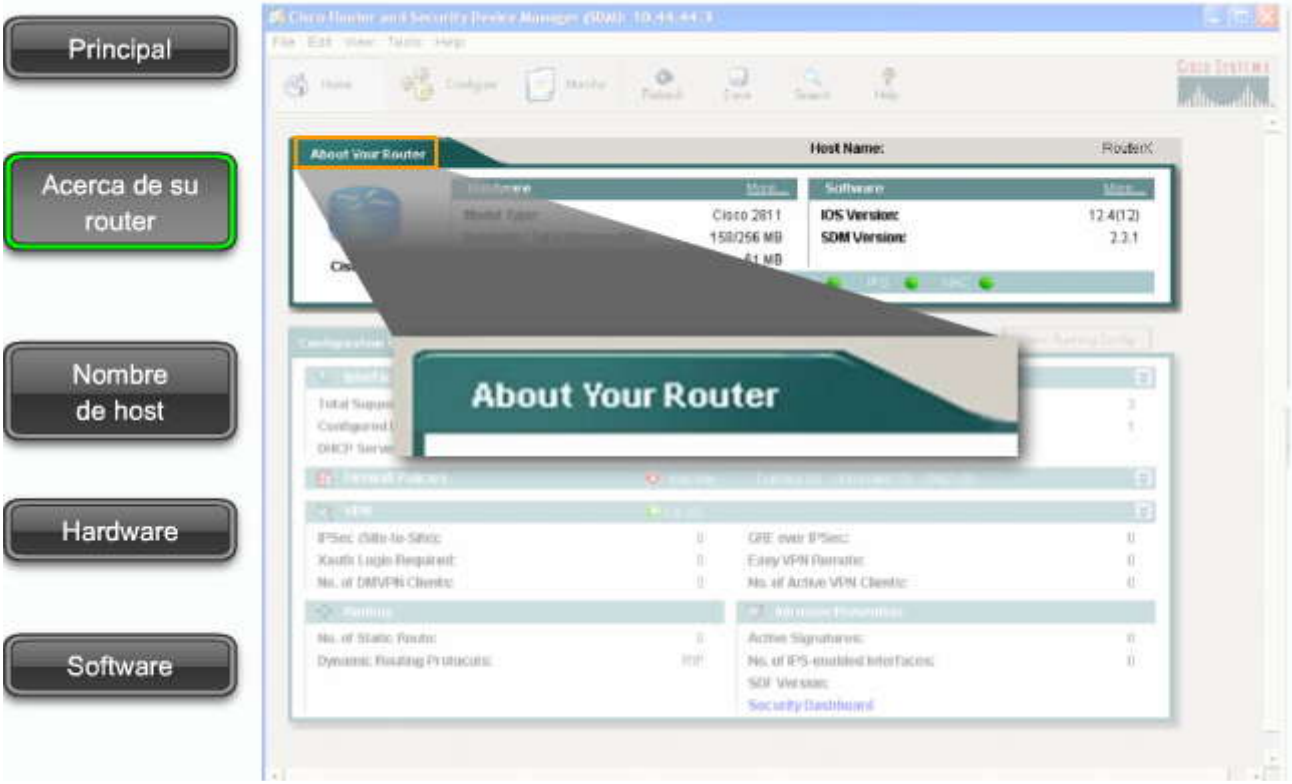
Acerca de su router: el área de la página de inicio del SDM de Cisco que le muestra información básica sobre el hardware y el software del router e incluye los siguientes elementos:

- Nombre de host: esta área muestra el nombre de host configurado para el router, que es RouterX.
- Hardware: esta área muestra el número de modelo del router, las cantidades disponibles y totales deRAM disponible y la cantidad de memoria Flash disponible.
- Software: esta área describe el software IOS de Cisco y las versiones de SDM de Cisco que se están ejecutando en el router.
- La barra Disponibilidad de características, que se encuentra en la parte inferior de la ficha Acerca de su router muestra las características disponibles en la imagen del IOS de Cisco que está utilizando el router. Si el indicador que se encuentra la lado de cada característica es verde, la característica está disponible. Si es rojo, no está disponible. Las marcas de verificación indican que la característica está configurada en el router. En la figura, el SDM de Cisco muestra que las características IP, firewall, VPN, IPS y NAC están disponibles, pero sólo IP está configurada.

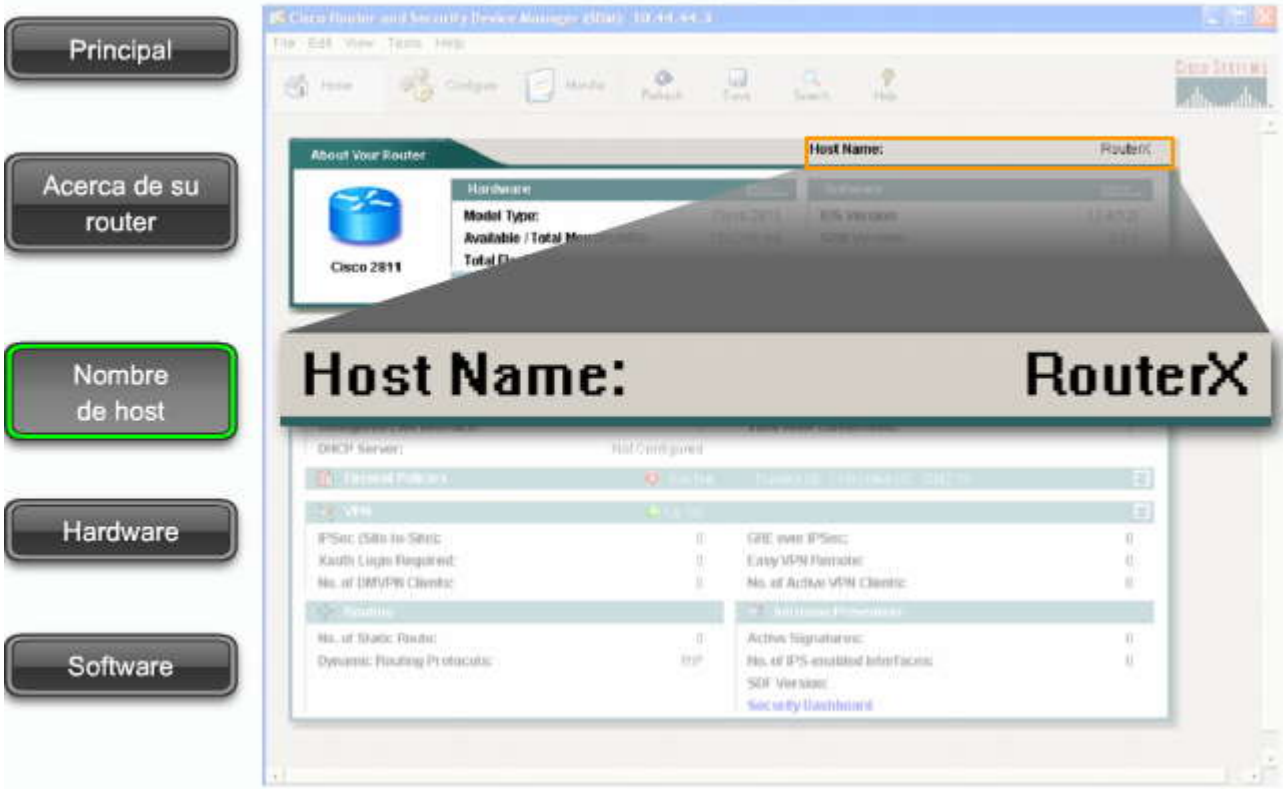
Acerca del área del router



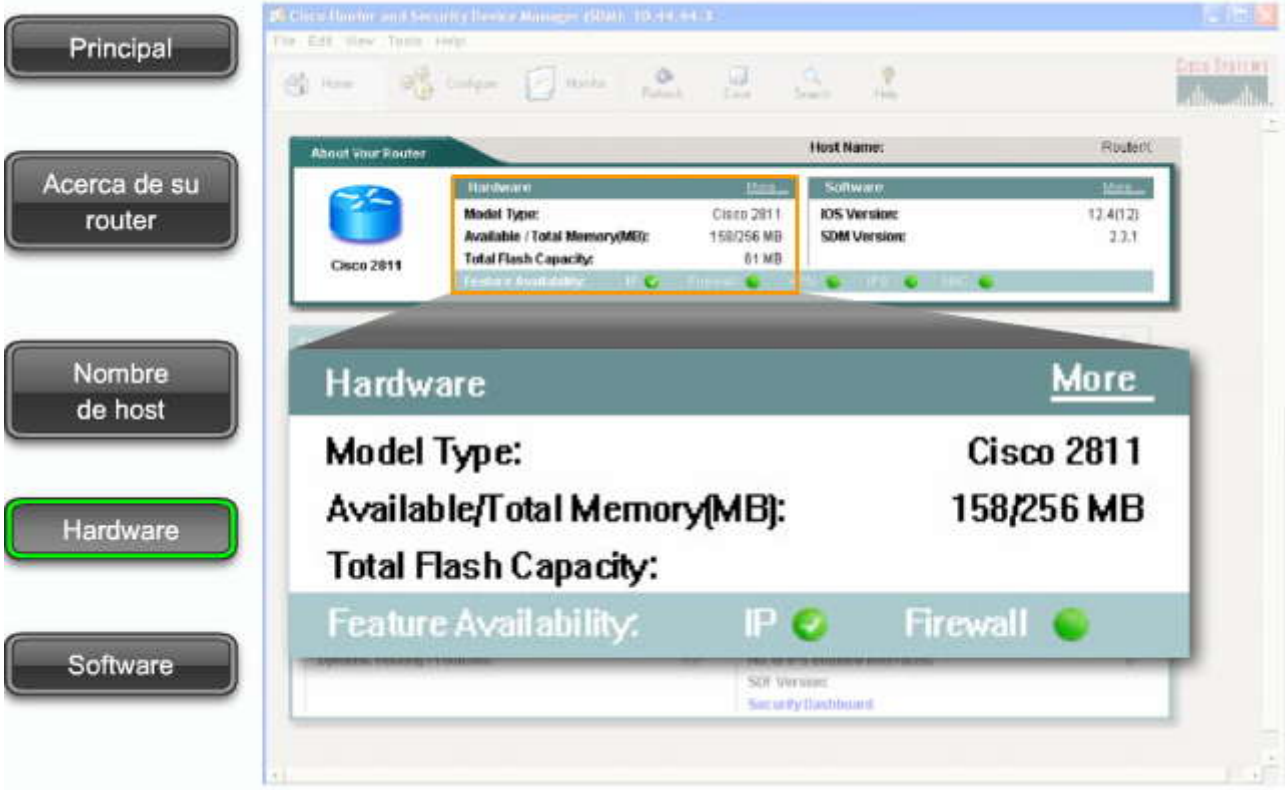
Acerca del área del router



Acerca del área del router



Acerca del área del router



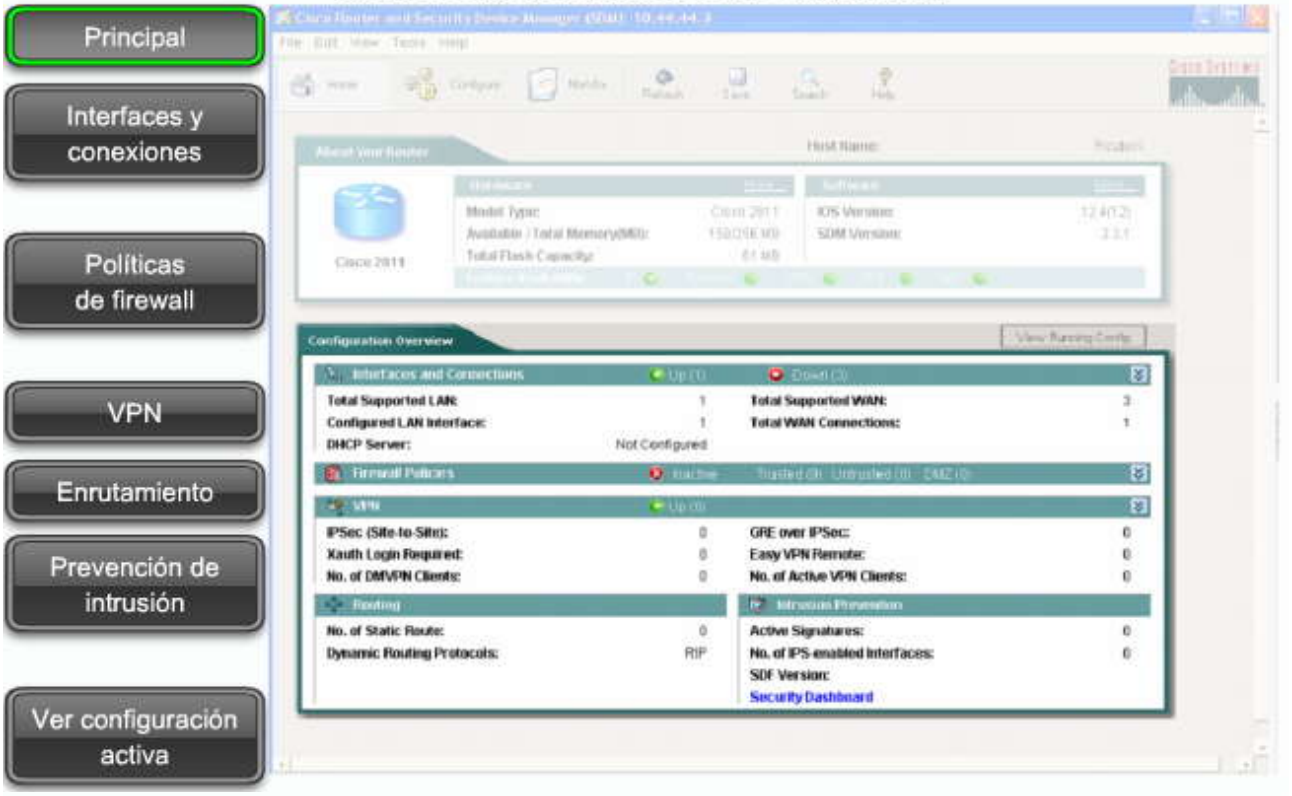
Área Descripción general de la configuración

La figura muestra el área de la descripción general de la configuración de la página de inicio del SDM de Cisco. Al hacer clic en los botones de la figura, puede ver los detalles asociados con cada uno de los siguientes elementos de la GUI:

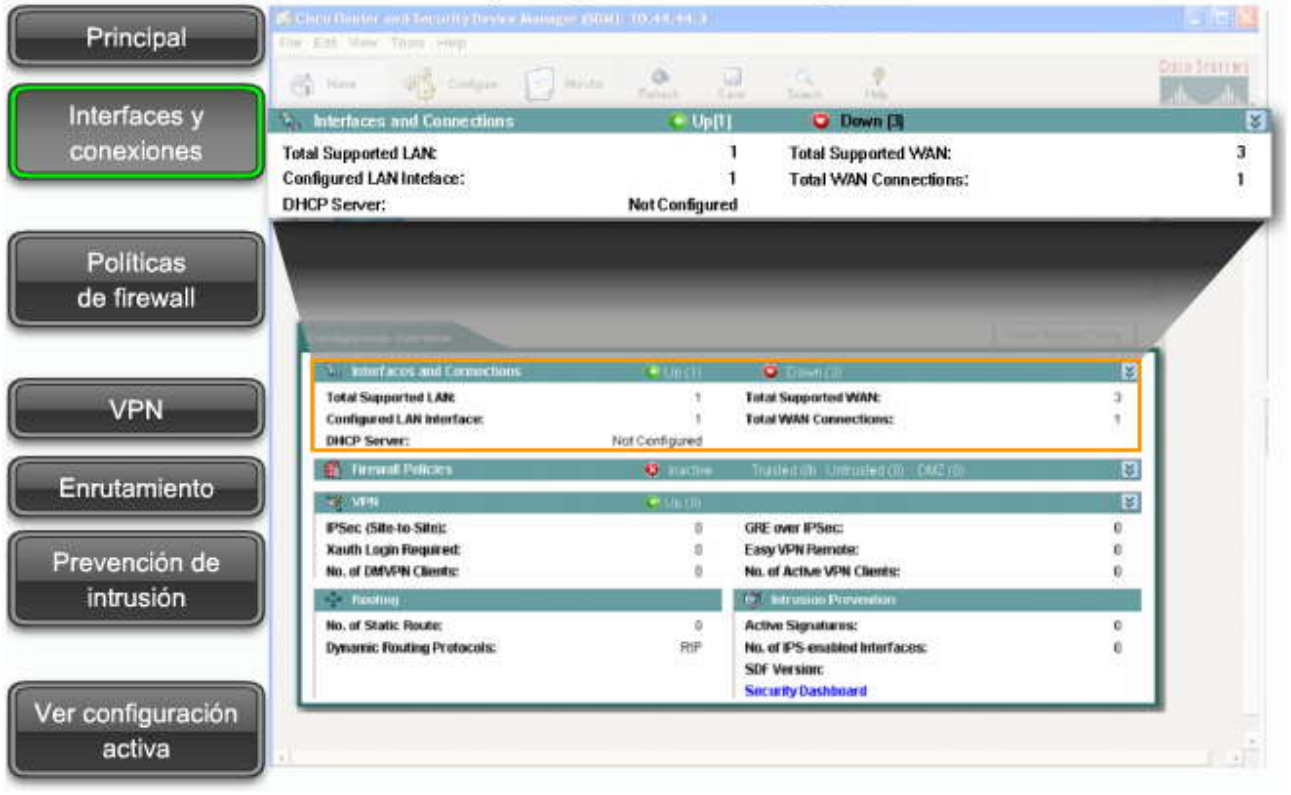
Interfaces y conexiones: esta área muestra información relacionada con las interfaces y conexiones, incluidas la cantidad de conexiones que se encuentran activas e inactivas, la cantidad total de interfaces LAN y WAN que están presentes en el router y la cantidad de interfaces LAN y WAN actualmente configuradas en el router. También muestra información de DHCP.

- **Políticas del firewall**: esta área muestra información relativa al firewall, por ejemplo, si hay un firewall implementado, la cantidad de interfaces confiables (internas), interfaces no confiables (externas) e interfaces de la DMZ. También muestra el nombre de la interfaz a la cual se ha aplicado un firewall, si la interfaz está diseñada como interfaz interna o externa y si la regla de NAT se ha aplicado a esta interfaz.
- **VPN**: esta área muestra información relacionada con las VPN, incluidas la cantidad de conexiones VPN activas, la cantidad de conexiones VPN configuradas sitio a sitio y la cantidad de clientes VPN activos.
- **Enrutamiento**: esta área muestra la cantidad de rutas estáticas, y qué protocolos de enrutamiento están configurados.

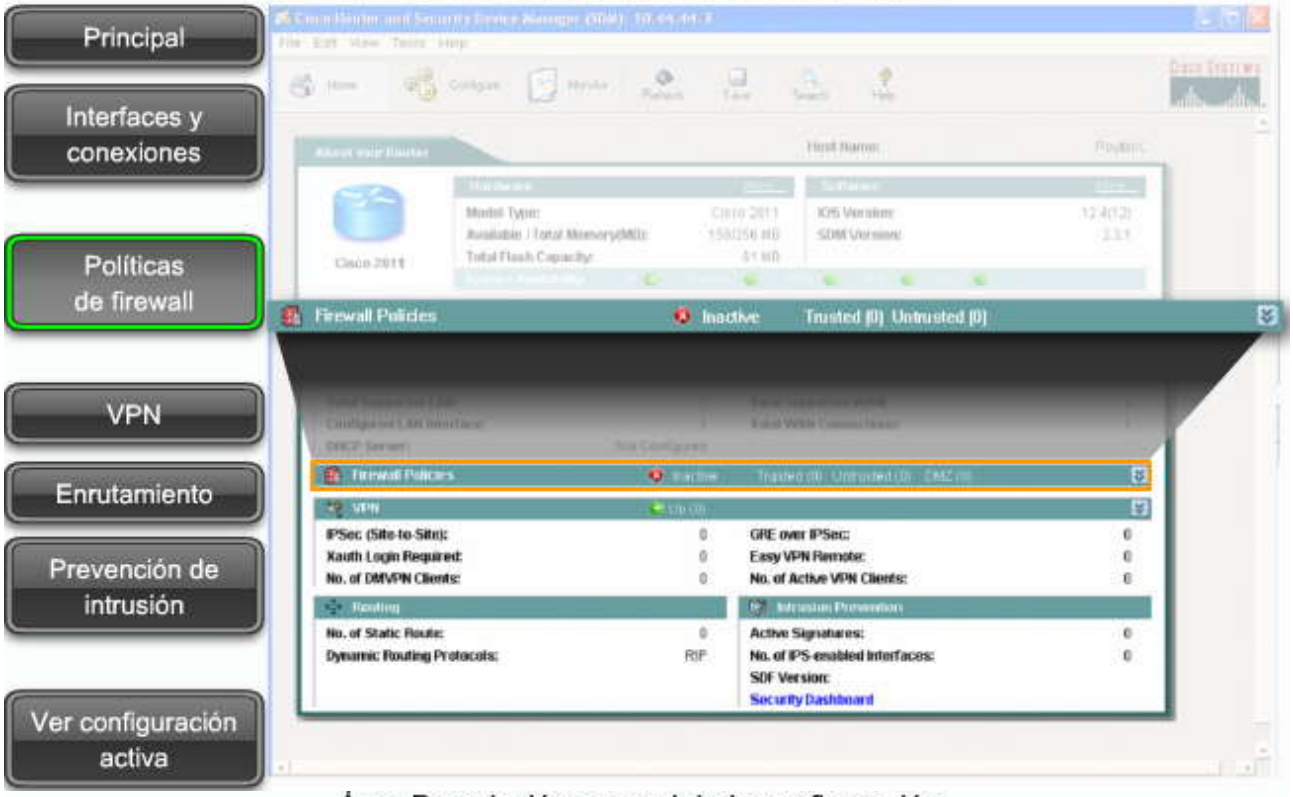
Área Descripción general de la configuración



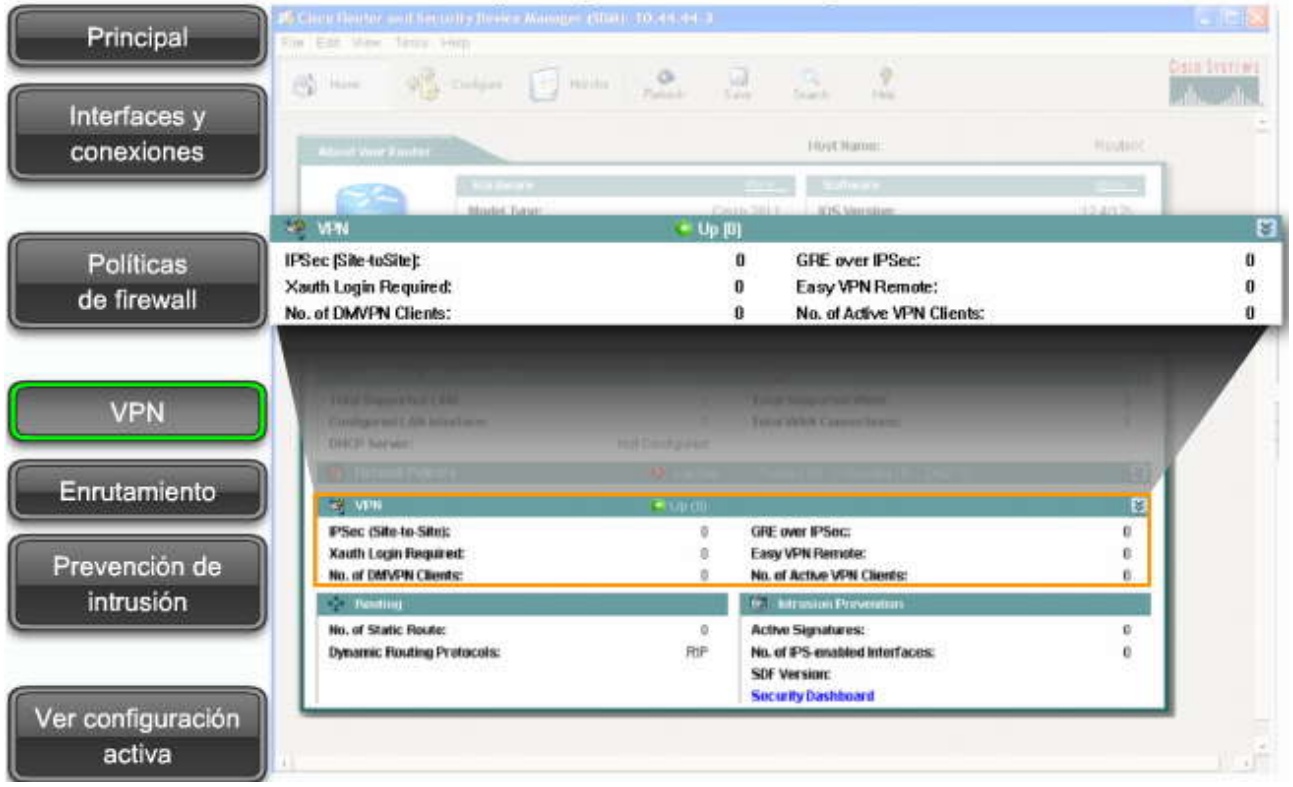
Área Descripción general de la configuración



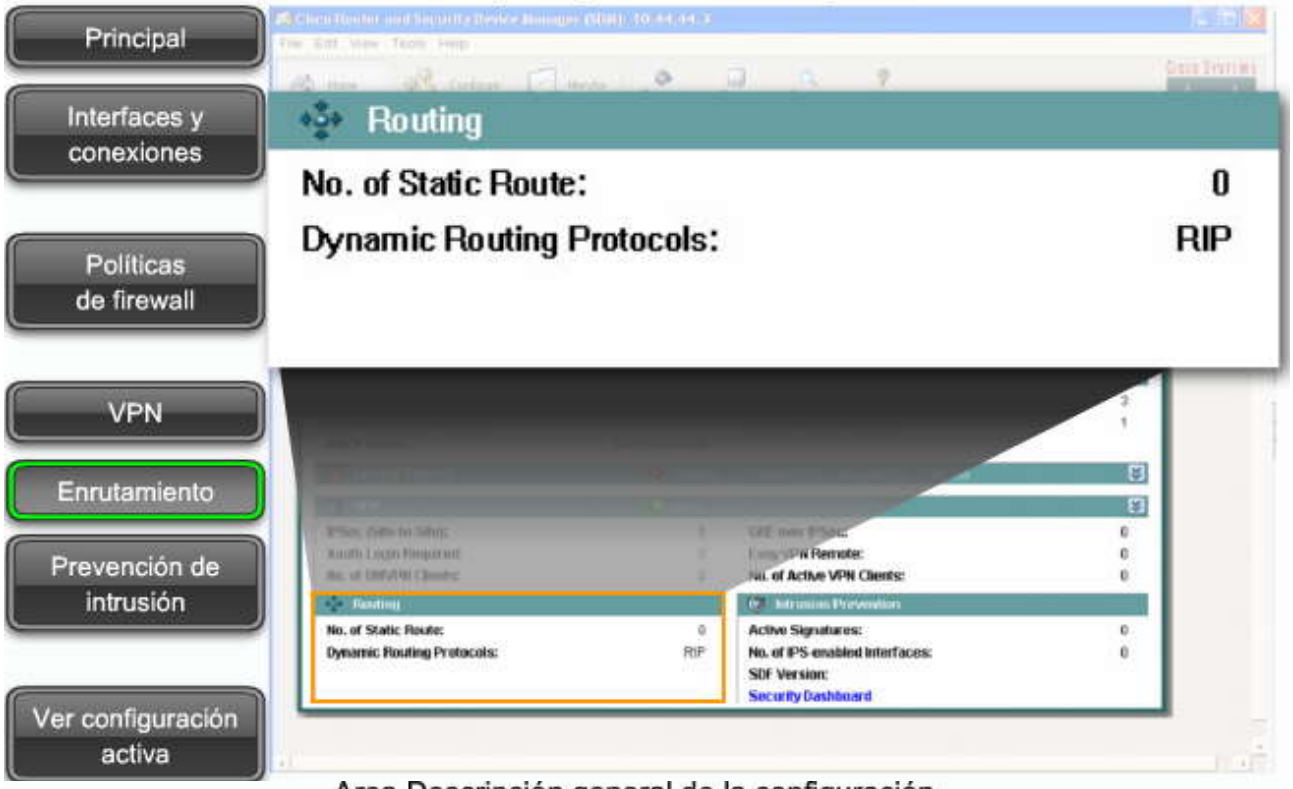
Área Descripción general de la configuración



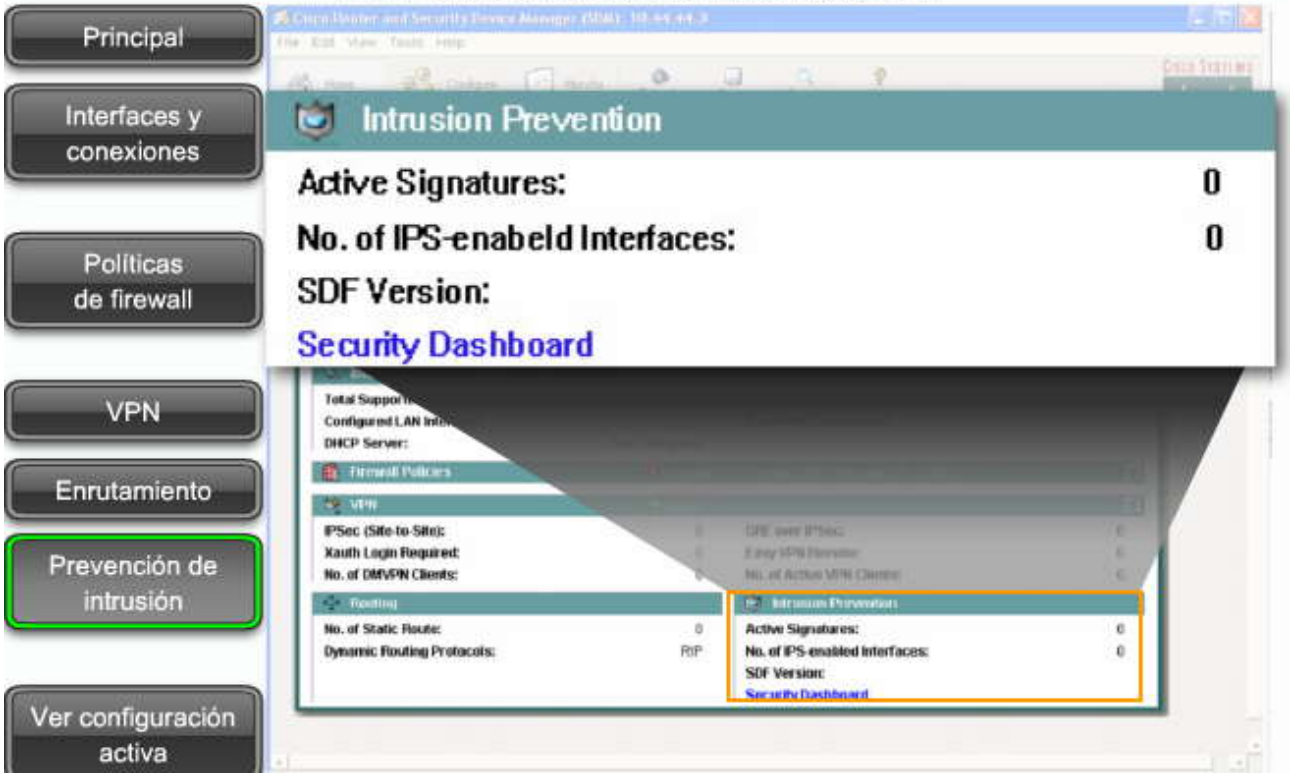
Área Descripción general de la configuración



Área Descripción general de la configuración



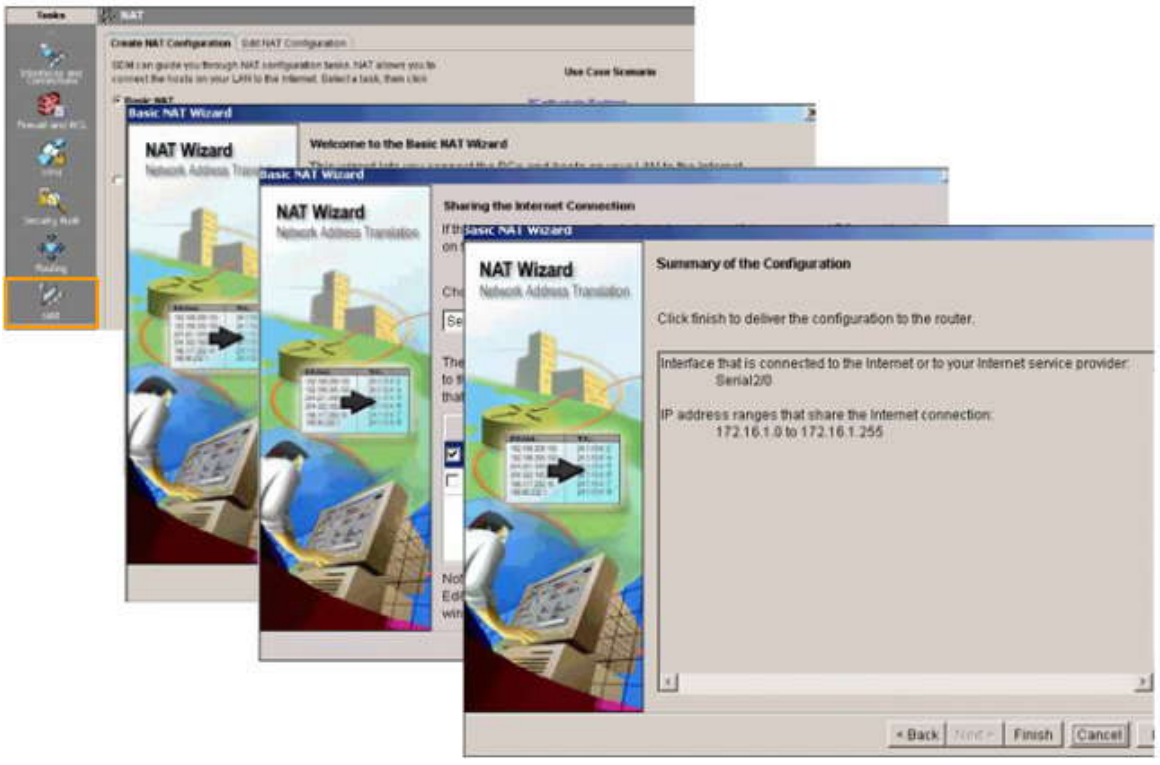
Area Descripción general de la configuración



4.4.5 Asistentes del SDM de Cisco

El SDM de Cisco proporciona una cantidad de asistentes que lo ayudan a configurar un router ISR de Cisco. Una vez seleccionada una tarea en el área de tareas de la GUI del SDM de Cisco, el panel de tareas le permite seleccionar un asistente. La figura muestra varias pantallas de la GUI del SDM de Cisco para el asistente de NAT básica. La NAT se analiza más adelante en las secciones de Servicios de direccionamiento IP.
Consulte http://www.cisco.com/go/sdm para obtener la información más reciente acerca de los asistentes del SDM de Cisco y las interfaces que admiten.

Asistentes del SDM de Cisco



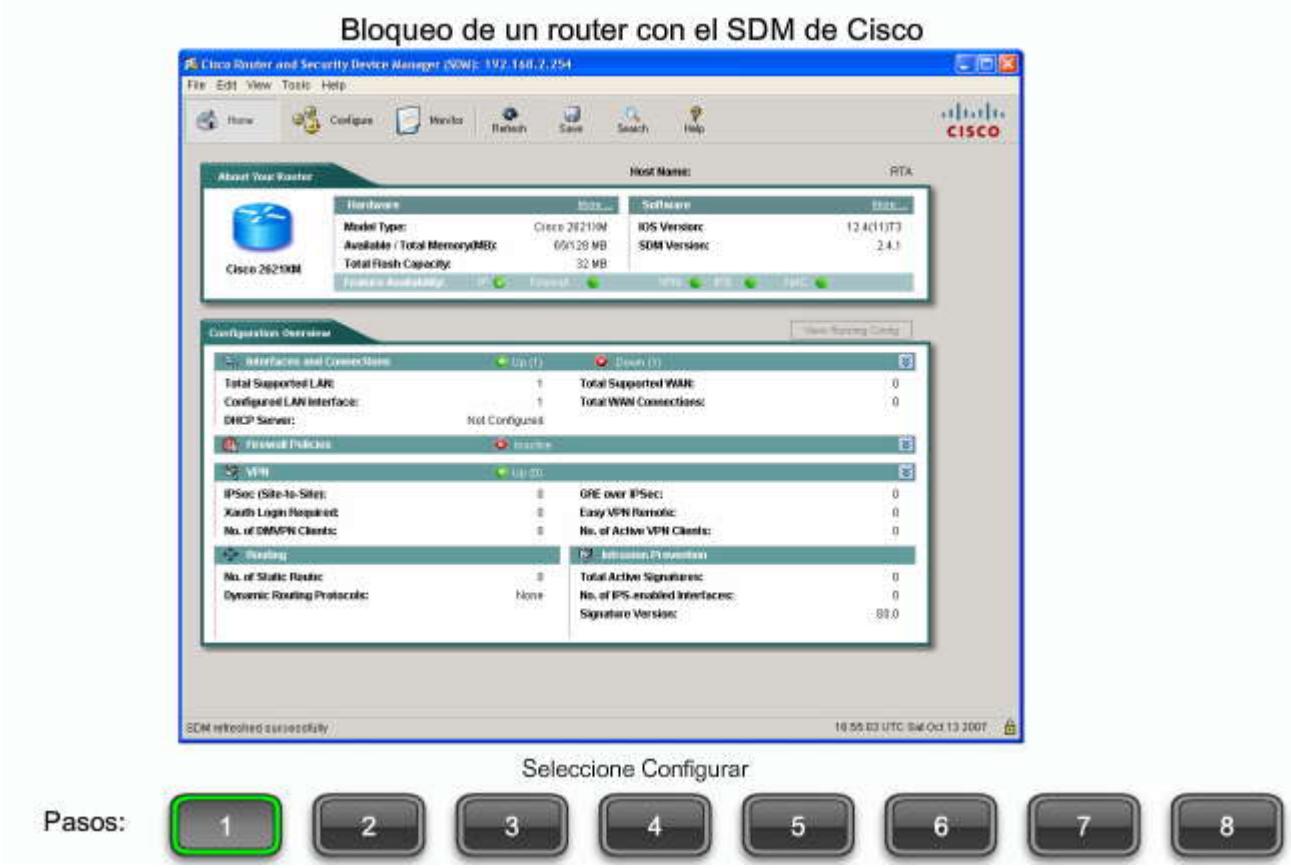
4.4.6 Bloqueo de un router con el SDM de Cisco

El asistente para el bloqueo del SDM de Cisco en un paso implementa casi todas las configuraciones de seguridad que ofrece AutoSecure de Cisco. El acceso al asistente para el bloqueo en un paso se logra desde Configurar interfaz de la GUI al hacer clic en la tarea Auditoría de seguridad. El asistente para el bloqueo en un paso prueba la configuración de su router para detectar potenciales problemas de seguridad y automáticamente realiza los cambios necesarios enla configuración a fin de corregir los problemas detectados.

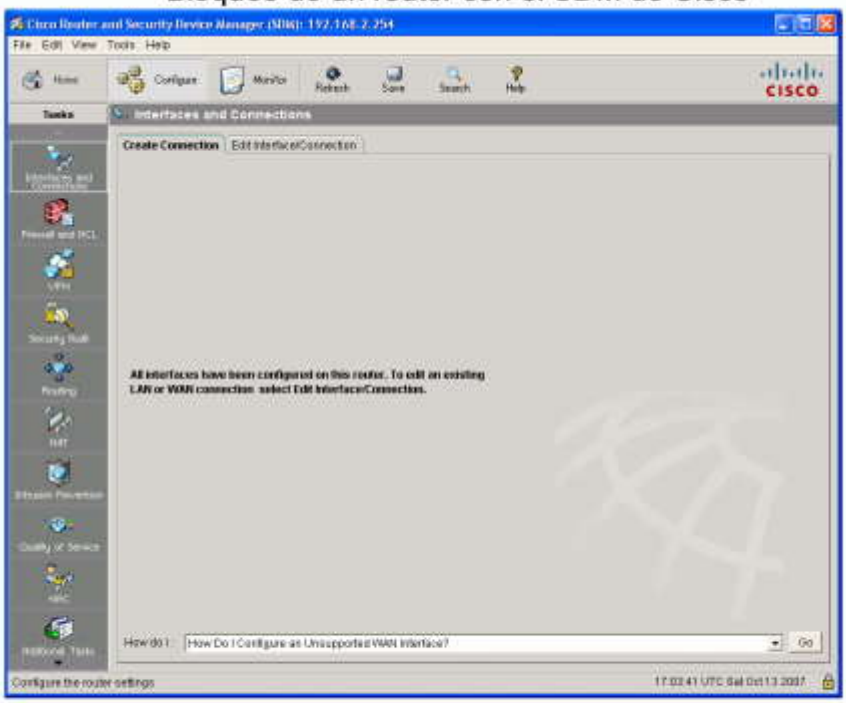
No dé por sentado que la red es segura sencillamente porque ejecutó un bloqueo en un paso. Además, no todas las características de AutoSecure de Cisco están implementadas en el SDM de Cisco. Las características de AutoSecure que se encuentran implementadas de manera diferente en el SDM de Cisco incluyen las siguientes:

- Desactiva SNMP y no configura la versión 3 de SNMP.
- Activa y configura SSH en las imágenes encriptadas del IOS de Cisco.
- No activa el Punto de control de servicio ni desactiva otros servicios de acceso y transferencia de archivos, como el FTP.

Haga clic en los botones de la figura para explorar los pasos del asistente de bloqueo en un paso de Cisco.



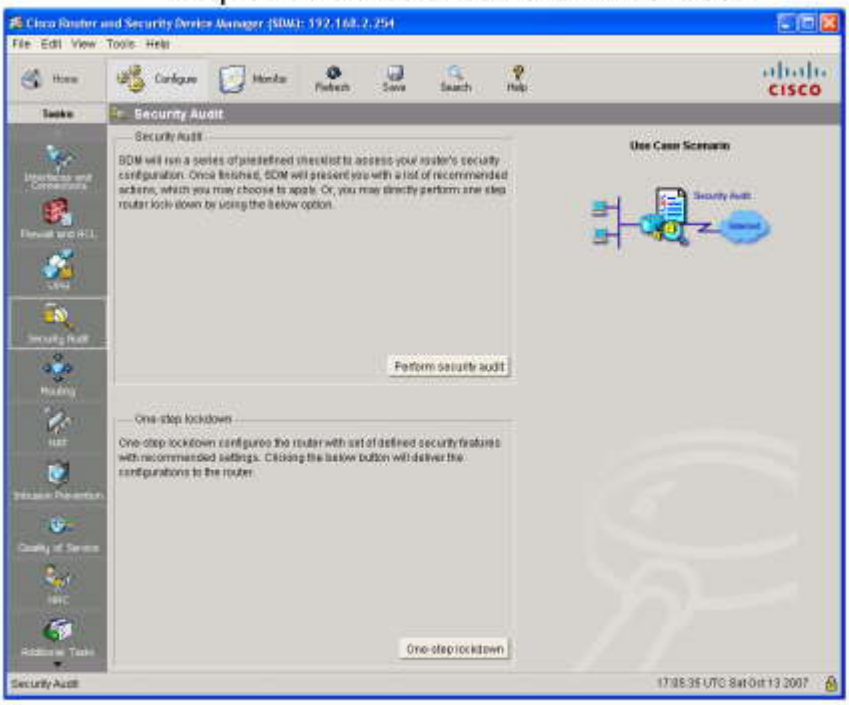
Bloqueo de un router con el SDM de Cisco



Seleccione Auditoría de seguridad.

Pasos: 1 2 3 4 5 6 7 8

Bloqueo de un router con el SDM de Cisco



Haga clic en Bloqueo de un paso.

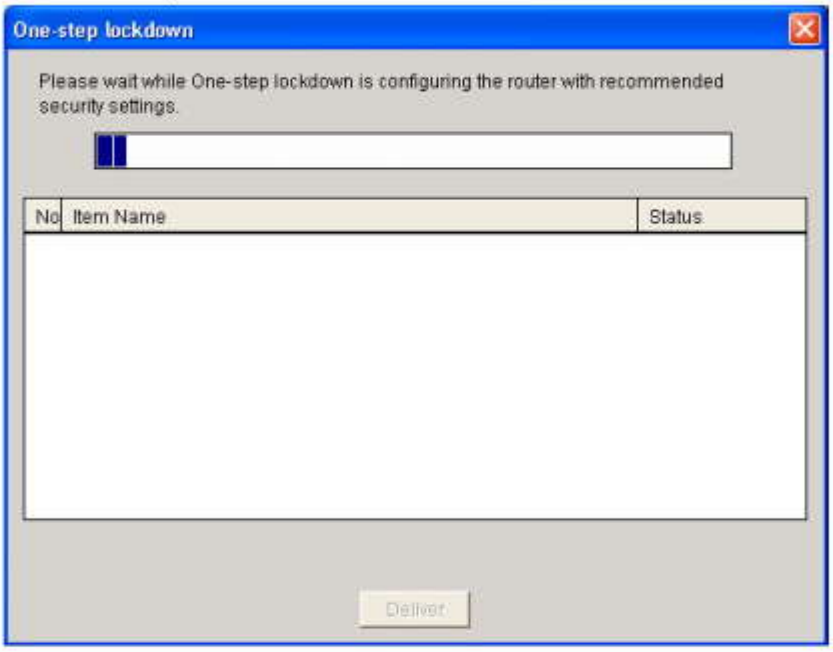
Pasos: 1 2 3 4 5 6 7 8

Bloqueo de un router con el SDM de Cisco

En el cuadro de diálogo de advertencia del SDM de Cisco, seleccione Sí.

Pasos: 1 2 3 **4** 5 6 7 8

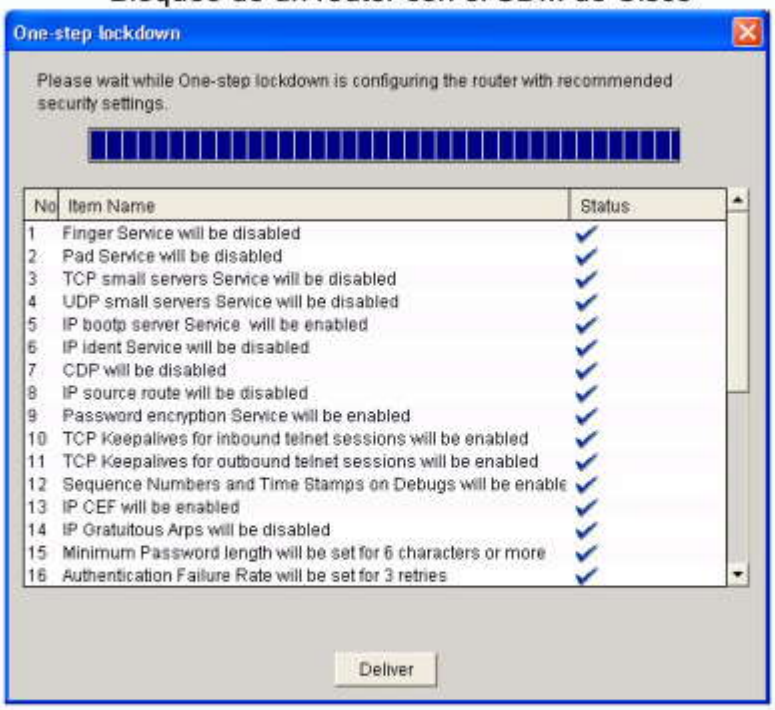
Bloqueo de un router con el SDM de Cisco



El SDM revisa la configuración actual y la compara con las prácticas de seguridad más conocidas.

Pasos: 1 2 3 4 **5** 6 7 8

Bloqueo de un router con el SDM de Cisco



Luego, el SDM muestra una lista de las configuraciones recomendadas.

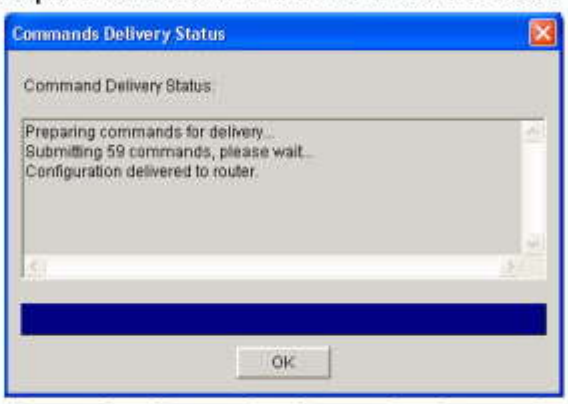
Pasos: 1 2 3 4 5 **6** 7 8

Bloqueo de un router con el SDM de Cisco

Los comandos se envían al router.

Pasos: 1 2 3 4 5 6 **7** 8

Bloqueo de un router con el SDM de Cisco



Pasos: 1 2 3 4 5 6 7 **8**

4.5 Administración segura de routers

4.5.1 Mantenimiento de las imágenes del software IOS de Cisco

Periódicamente, el router requiere que se carguen actualizaciones en el sistema operativo o en el archivo de configuración. Estas actualizaciones son necesarias para reparar vulnerabilidades de seguridad conocidas, admitir nuevas características que permiten implementar políticas de seguridad más avanzadas o mejorar el rendimiento.

Nota: No siempre resulta conveniente actualizar a la última versión del software IOS de Cisco. Muchas veces esa versión no es estable.

Hay pautas determinadas que debe seguir al modificar el software IOS de Cisco en un router. Las modificaciones se clasifican en actualizaciones o cambios de versión. Una actualización reemplaza una versión con otra sin actualizar el conjunto de características. El software podría ser actualizado para reparar un defecto o para reemplazar una versión que ya no es compatible. Las actualizaciones son gratis.

Un cambio de versión reemplaza una versión con otra que tiene un conjunto de características actualizado. El software podría ser reemplazado por una nueva versión para agregar nuevas características o tecnologías, o para reemplazar una versión que ya no sea compatible. Los cambios de versión no son gratuitos. Cisco.com ofrece pautas para ayudar a determinar qué método se aplica.

Cisco recomienda seguir un proceso de migración de cuatro fases para simplificar las operaciones y la administración de la red. Cuando sigue un proceso que se puede repetir, también puede beneficiarse de los menores costos de las operaciones, la administración y la capacitación. Las cuatro fases son:

- **Planificar**: establecer metas, identificar recursos, definir el perfil del hardware y el software de la red y crear un cronograma preliminar para migrar a nuevas versiones.
- **Diseñar**: elegir nuevas versiones del IOS de Cisco y crear una estrategia para migrar a las versiones.
- **Implementar**: programar y ejecutar la migración.
- **Operar**: controlar el progreso de la migración y realizar copias de seguridad de las imágenes que se están ejecutando en su red.

En Cisco.com hay una cantidad de herramientas disponibles para ayudar a migrar el software IOS de Cisco. Puede utilizar las herramientas para obtener información sobre versiones, conjuntos de características, plataformas e imágenes. Las siguientes herramientas no requieren conectarse a Cisco.com:

- **Guía de referencia del IOS de Cisco**: cubre los aspectos básicos de la familia del software IOS de Cisco
- **Documentos técnicos del software IOS de Cisco**: documentación de cada una de las versiones del software IOS de Cisco
- **Centro de Software**: descargas del software IOS de Cisco

Selector del software IOS de Cisco: busca las características necesarias para una determinada tecnología

Las siguientes herramientas requieren cuentas de conexión válidas en Cisco.com:

- **Juego de herramientas para reparar defectos**: busca modificaciones de software conocidas basadas en la versión de software, el conjunto de características y las palabras clave
- **Feature Navigator de Cisco**: busca las versiones compatibles con un conjunto de características de software y con el hardware, y compara las versiones
- **Software Advisor**: compara las versiones, compara las características del software IOS de Cisco y del SO Cisco Catalyst con las versiones y averigua qué versión del software es compatible con un determinado dispositivo de hardware
- **Planificador de actualizaciones del IOS de Cisco**: busca las versiones por hardware, versión y conjunto de características, y descarga las imágenes del software IOS de Cisco

4.5.2 Administración de las imágenes del IOS de Cisco

Sistemas de archivos y dispositivos del IOS de Cisco

La disponibilidad de la red puede estar en riesgo si se compromete el sistema operativo o la configuración de un router. Los agresores que obtienen acceso a los dispositivos de infraestructura pueden modificar o eliminar archivos de configuración. También pueden cargar imágenes del IOS no compatibles o eliminar la imagen del IOS. Las modificaciones se invocan automáticamente o se invocan una vez que se reinicia el dispositivo.

Para mitigar estos problemas, debe poder guardar, hacer una copia de seguridad y restaurar la configuración y las imágenes del IOS. Para ello, debe aprender a realizar algunas operaciones de administración de archivos en el software IOS de Cisco.

Los dispositivos del IOS de Cisco cuentan con una característica denominada Sistema de archivos integrados (IFS) del IOS de Cisco. Este sistema le permite crear, navegar y manipular directorios en un dispositivo Cisco. Los directorios disponibles dependen de la plataforma.

Por ejemplo, la figura muestra el resultado del comando **show file systems** que enumera todos los sistemas de archivos disponibles en un router Cisco 1841. Este comando proporciona información útil, como la cantidad de memoria disponible y libre, el tipo de sistema de archivos y sus permisos. Los permisos incluyen sólo lectura (ro), sólo escritura (wo) y lectura y escritura (rw).

Si bien hay varios sistemas de archivos enumerados, a nosotros nos interesan los sistemas de archivos tftp, flash ynvram. Los demás sistemas de archivos enumerados exceden el alcance de este curso.

Los sistemas de archivos de la red incluyen el uso de FTP, FTP trivial (TFTP) o Protocolo de copia remota (RCP). Este curso se centra en el TFTP.

Tenga en cuenta que el sistema de archivos flash también está precedido por un asterisco que indica que se trata del actual sistema de archivos predeterminado. Recuerde que el IOS de arranque está ubicado en flash; por lo tanto, el símbolo numeral (#) agregado al listado de flash indica que se trata de un disco de arranque.

Haga clic en el botón Flash de la figura.

Esta figura enumera el contenido del sistema de archivos predeterminado actual, en este caso flash, como indicaban los asteriscos que precedían la lista de la figura anterior. Hay varios archivos ubicados en flash, sin embargo, lo que nos interesa específicamente es el último listado, que es el nombre de las imágenes de archivos del IOS actual que se ejecutan en RAM.

Haga clic en el botón NVRAM de la figura.

Para ver el contenido de NVRAM, debe modificar el sistema de archivos predeterminado actual mediante el comando de cambio de directorio **cd**. El comando de directorio en uso actual **pwd** verifica que estemos ubicados en el directorio NVRAM. Por último, el comando **dir** enumera los contenidos de NVRAM. Pese a que hay varios archivos de configuración enumerados, lo que nos interesa específicamente es el archivo de configuración de inicio.

Sistemas de archivos

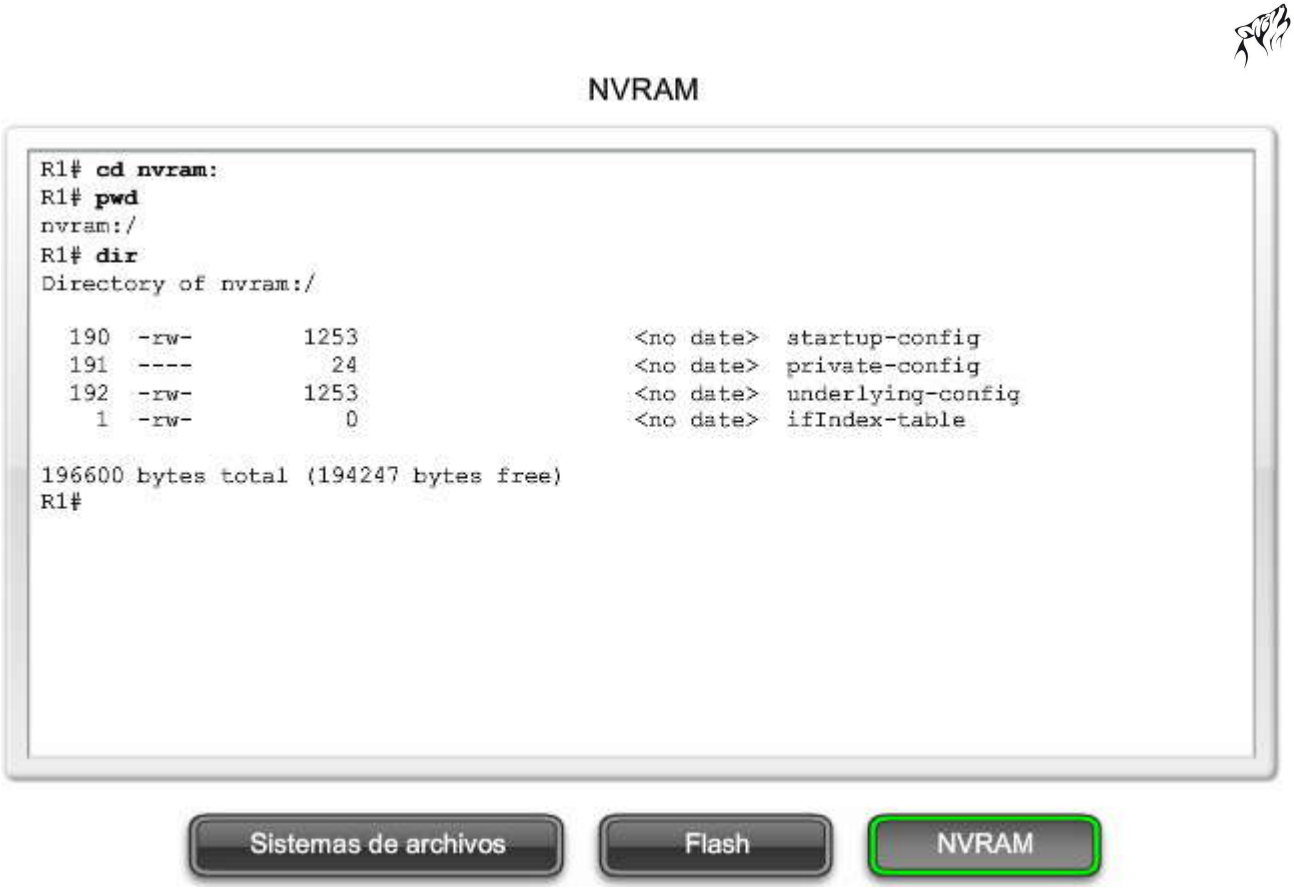
```
R1# show file system
File Systems:

     Size(b)     Free(b)      Type  Flags  Prefixes
           -           -    opaque     rw   archive:
           -           -    opaque     rw   system:
           -           -    opaque     rw   null:
           -           -   network     rw   tftp:
      196600      194247     nvram     rw   nvram:
*   31932416      462848      disk     rw   flash:#
           -           -    opaque     wo   syslog:
           -           -    opaque     rw   xmodem:
           -           -    opaque     rw   ymodem:
           -           -   network     rw   rcp:
           -           -   network     rw   pram:
           -           -   network     rw   ftp:
           -           -   network     rw   http:
           -           -   network     rw   scp:
           -           -   network     rw   https:
           -           -    opaque     ro   cns:

R1#
```

Sistemas de archivos | Flash | NVRAM

Flash

```
R1# dir

Directory of flash:/

    1  -rw-         720  Sep 11 2007 15:59:54 +00:00  pre_autosec.cfg
    2  -rw-        1821  Jul 11 2006 10:30:42 +00:00  sdmconfig-18xx.cfg
    3  -rw-     4734464  Jul 11 2006 10:31:20 +00:00  sdm.tar
    4  -rw-      833024  Jul 11 2006 10:31:44 +00:00  es.tar
    5  -rw-     1052160  Jul 11 2006 10:32:14 +00:00  common.tar
    6  -rw-        1038  Jul 11 2006 10:32:36 +00:00  home.shtml
    7  -rw-      102400  Jul 11 2006 10:32:58 +00:00  home.tar
    8  -rw-      491213  Jul 11 2006 10:33:20 +00:00  128MB.sdf
    9  -rw-     1684577  Jul 11 2006 10:34:00 +00:00  securedesktop-ios-3.1.1.27-k9.pkg
   10  -rw-      398305  Jul 11 2006 10:34:34 +00:00  sslclient-win-1.1.0.154.pkg
   11  -rw-    22149320  Mar 28 2007 16:02:28 +00:00  c1841-advipservicesk9-mz.124-13a.bin

31932416 bytes total (462848 bytes free)
R1#
```

Sistemas de archivos | Flash | NVRAM



Prefijos de URL para los dispositivos Cisco

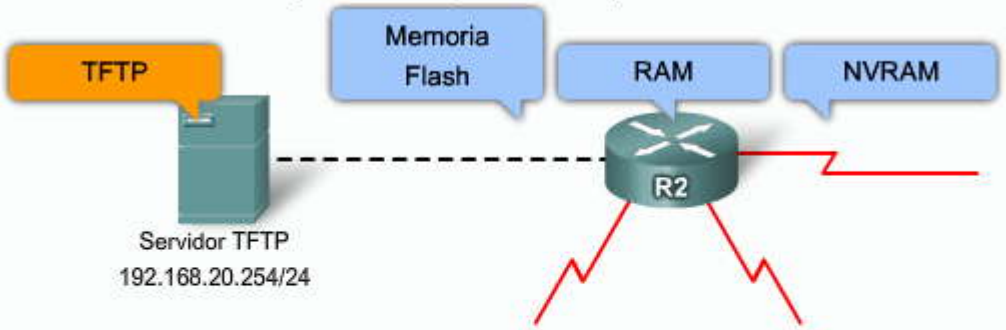
Cuando el administrador de una red desea mover los archivos dentro de un equipo, el sistema operativo ofrece una estructura visible de archivos para especificar orígenes y destinos. Los administradores no necesitan tener claves visuales cuando trabajan en la CLI de un router. El comando show file systems del tema anterior muestra los diversos sistemas de archivos disponibles en la plataforma del Cisco 1841.
Las ubicaciones de los archivos se especifican en el IFS de Cisco que utiliza la convención URL. Las URL utilizadas por las plataformas IOS de Cisco tienen una apariencia similar al formato que usted conoce de la Web.

Por ejemplo, el TFTP de muestra de la figura es: tftp://192.168.20.254/configs/backup-configs.

- La expresión "tftp": se denomina prefijo.
- Todo lo que aparece después de la doble barra oblicua (//) define la ubicación.
- 192.168.20.254 es la ubicación del servidor TFTP.
- "configs" es el directorio maestro.
- "backup-configs" es el nombre del archivo.

El prefijo URL especifica el sistema de archivos. Desplácese sobre los diversos botones de la figura para ver los prefijos comunes y la sintaxis asociada a cada uno.

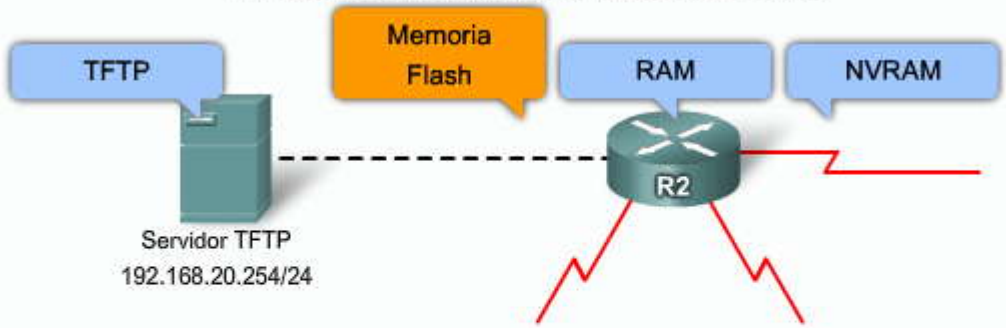
Prefijos de URL para los dispositivos Cisco



Prefijo	Ruta URL
tftp:	[[[//location]/directory]/filename]
tftp://192.168.20.254/configs/backup-config	

TFTP | Memoria Flash | RAM | NVRAM

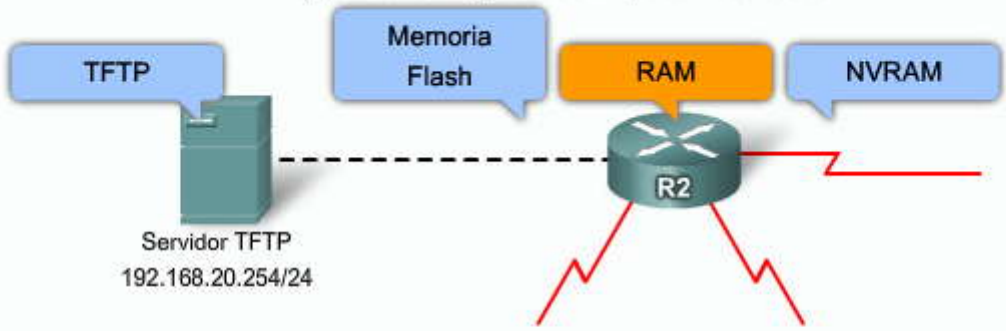
Prefijos de URL para los dispositivos Cisco



Prefijo	Ruta URL
flash:	[[/directory/]filename]
flash:configs/backup-config	

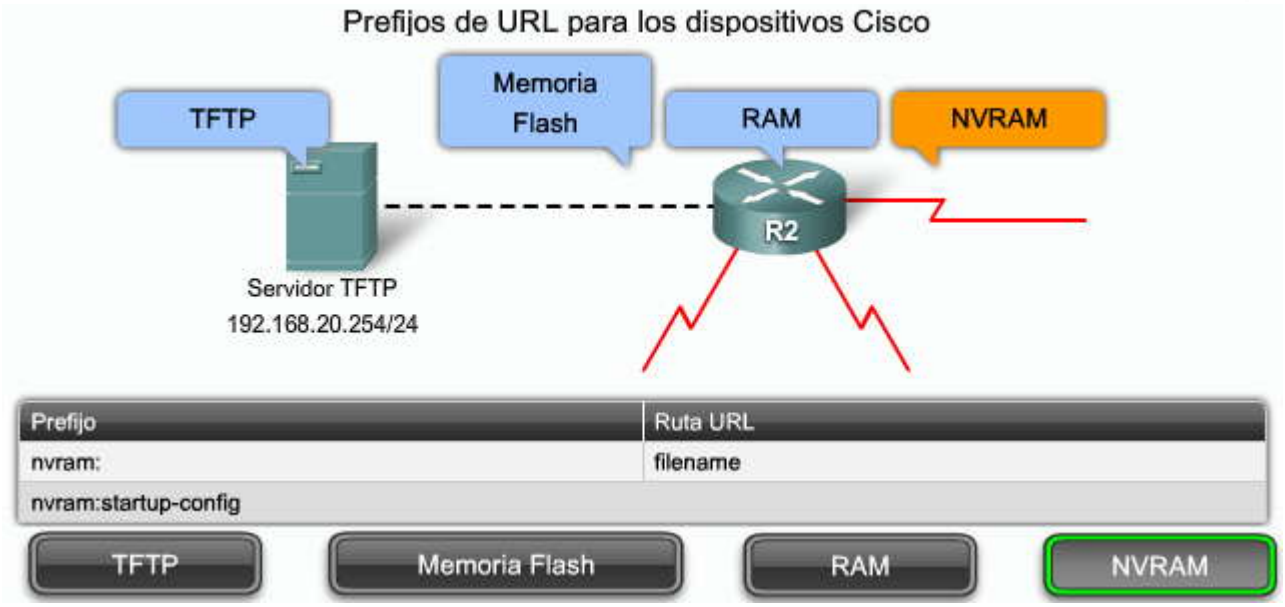
TFTP | Memoria Flash | RAM | NVRAM

Prefijos de URL para los dispositivos Cisco



Prefijo	Ruta URL
system:	filename
system:running-config	

TFTP | Memoria Flash | RAM | NVRAM



Comandos para administrar los archivos de configuración

Una buena práctica para mantener la disponibilidad del sistema es asegurarse de tener siempre copias de seguridad de los archivos de configuración de inicio y de los archivos de imagen del IOS. El comando **copy** del software IOS de Cisco se utiliza para mover los archivos de configuración de un componente o dispositivo a otro, como RAM, NVRAM o un servidor TFTP. La figura resalta la sintaxis del comando.

A continuación, se proporcionan ejemplos del uso común del comando **copy**. Los ejemplos enumeran dos métodos que se pueden utilizar para realizar las mismas tareas. El primer ejemplo es una sintaxis sencilla, y el segundo proporciona un ejemplo más explícito.

Copiar la configuración en ejecución de la RAM a la configuración de inicio de NVRAM:

R2# **copy running-config startup-config**

copy system:running-config nvram:startup-config

Copiar la configuración en ejecución de la RAM a una ubicación remota:

R2# **copy running-config tftp:**

R2# **copy system:running-config tftp:**

Copiar una configuración desde un origen remoto a la configuración en ejecución:

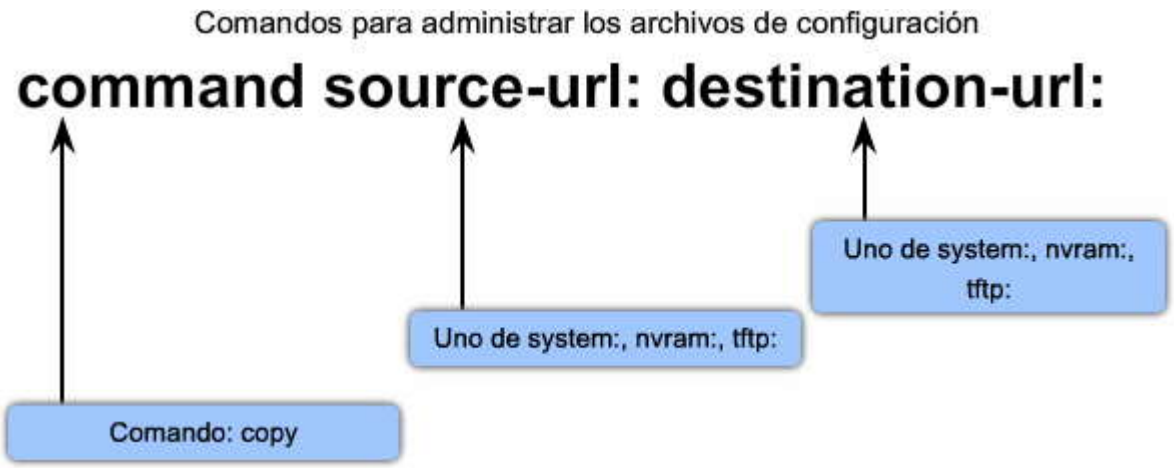
R2# **copy tftp: running-config**

R2# **copy tftp: system:running-config**

Copiar una configuración de un origen remoto a la configuración de inicio:

R2# **copy tftp: startup-config**

R2# **copy tftp: nvram:startup-config**



Normas de denominación de archivos del IOS de Cisco

El archivo de la imagen IOS de Cisco se basa en una norma de denominación especial. El nombre del archivo de imagen del IOS de Cisco contiene varias partes, cada una con un significado específico. Es importante que comprenda esta norma de denominación al actualizar y seleccionar un IOS.

Por ejemplo, el nombre de archivo de la figura se explica de la siguiente manera:

La primera parte, **c1841**, identifica la plataforma en la que se ejecuta la imagen. En este ejemplo, la plataforma es una Cisco 1841.
La segunda parte, **ipbase**, especifica el conjunto de características. En este caso, "ipbase" hace referencia a la imagen básica de internetworking de IP. Otros posibles conjuntos de características son:

i: designa el conjunto de características IP

j : designa el conjunto de características empresariales (todos los protocolos)**s**: designa un conjunto de características PLUS (más colas, manipulación o traducciones)

56i: designa la encriptación DES de IPsec de 56 bits

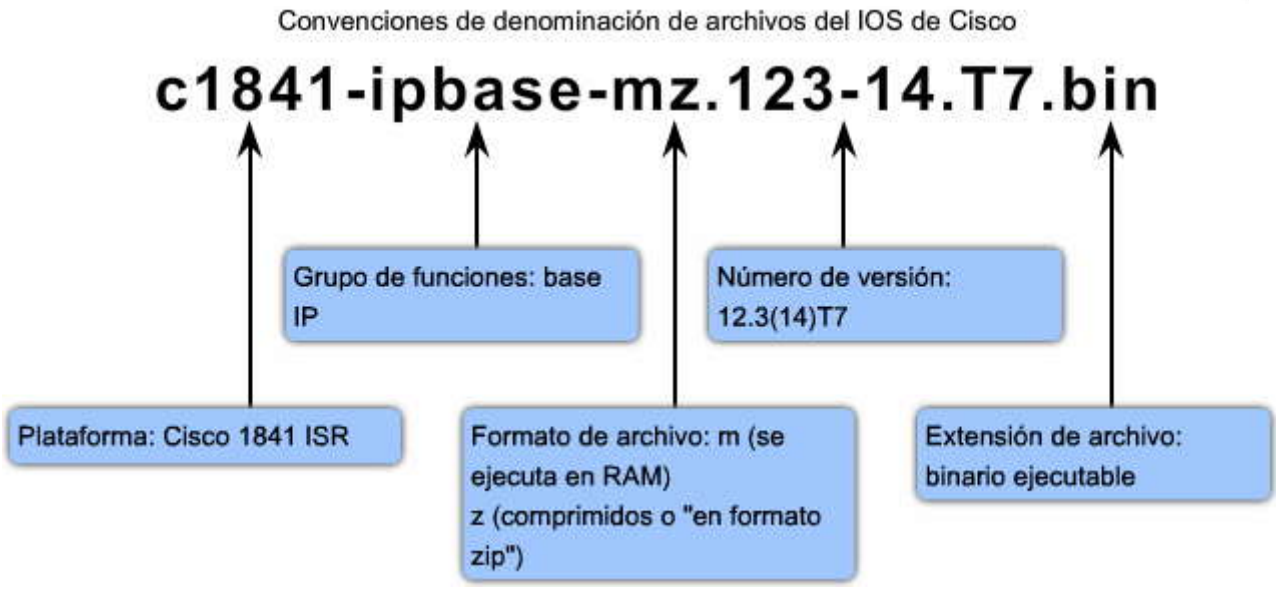
3: designa el firewall/IDS

k2: designa la encriptación 3DES de IPsec (168 bits)

La tercera parte, **mz**, indica el lugar en que se ejecuta la imagen y si el archivo está comprimido. En este ejemplo, "mz" indica que el archivo se ejecuta desde la RAM y está comprimido.

La cuarta parte, **12.3-14.T7**, es el número de versión.

La parte final, **bin**, es la extensión del archivo. La extensión .bin indica que se trata de un archivo binario ejecutable.



4.5.3 Administración de las imágenes del IOS de Cisco

Uso de los servidores TFTP para administrar imágenes del IOS

Por lo general, las internetworks de producción abarcan áreas extensas y contienen varios routers. Una tarea importante del administrador consiste en actualizar continuamente la versión de las imágenes del IOS de Cisco IOS cada vez que se descubren explotaciones y vulnerabilidades. Asegurarse de que todas sus plataformas estén ejecutando la misma versión del software IOS de Cisco, cada vez que sea posible, también es una práctica atinada. Por último, en todas las redes, siempre es prudente conservar una copia de seguridad de la imagen del software IOS de Cisco para el caso de que la imagen del sistema que se encuentra en el router se dañe o se borre por accidente.

Los routers de amplia distribución necesitan un sitio para ubicar el origen o la copia de seguridad de las imágenes de software. El uso de un servidor TFTP de red permite que se carguen y descarguen imágenes y configuraciones a través de la red. El servidor TFTP de red puede ser otro router, una estación de trabajo o un sistema de hosts.

Con el crecimiento de las redes, el almacenamiento de las imágenes y los archivos de configuración del software IOS de Cisco, en el servidor TFTP central, permite controlar la cantidad y el nivel de revisión de las imágenes y los archivos de configuración del software IOS de Cisco que se deben conservar.

Antes de modificar una imagen del software IOS de Cisco en el router, debe llevar a cabo las siguientes tareas:

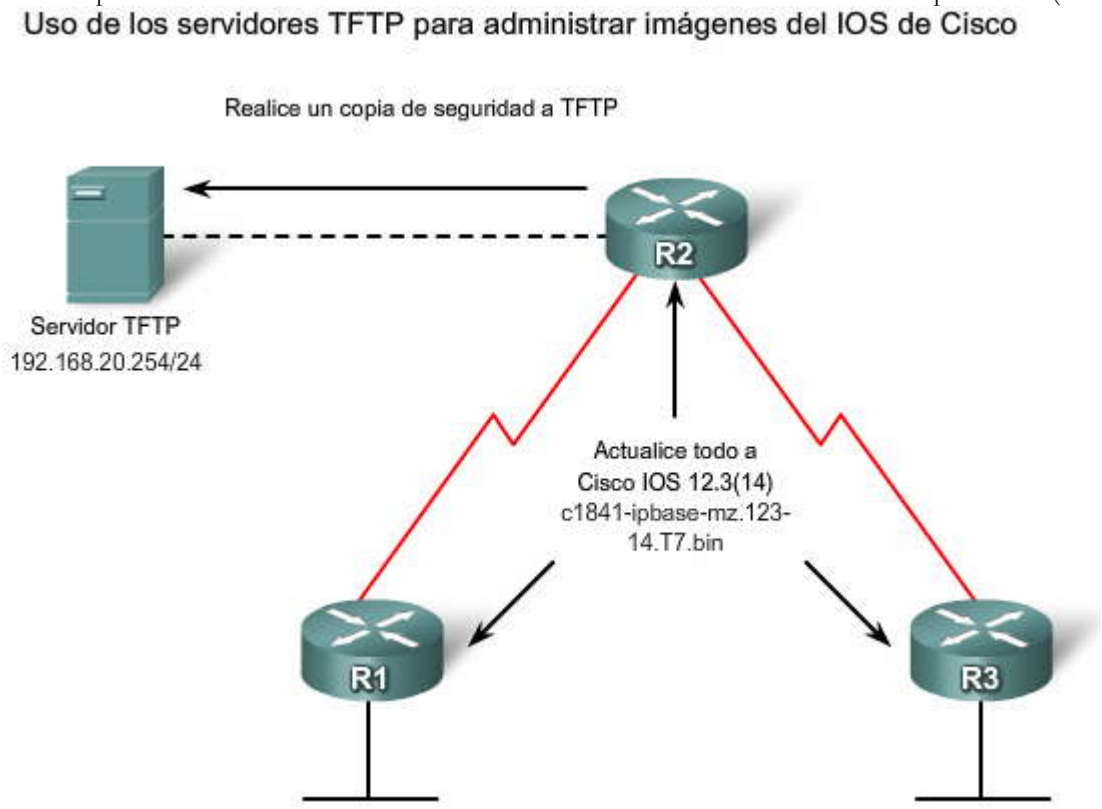
- Determinar la memoria necesaria para la actualización y, si fuera necesario, instalar más memoria.
- Configurar y probar la capacidad de transferencia de archivos entre el host del administrador y el router.
- Programar el tiempo de inactividad necesario, normalmente, fuera del horario laboral, para que el router lleve a cabo la actualización.

Cuando esté listo para completar la actualización, siga estos pasos:

- Cierre todas las interfaces del router que no sean necesarias para realizar la actualización.
- Realice una copia de seguridad del sistema operativo actual y del archivo de configuración actual en un servidor TFTP.
- Cargue la actualización para el sistema operativo o el archivo de configuración.
- Realice una prueba para confirmar que la actualización funciona correctamente. Si el resultado de las pruebas es satisfactorio, puede volver a activar las interfaces que desactivó. Si el resultado de las pruebas no es satisfactorio, salga de la actualización, determine dónde estuvo el error y comience nuevamente.

Para los operadores de red, constituye un gran desafío minimizar el tiempo de inactividad que se genera después de que un router ha sido comprometido, y el software operativo y los datos de configuración se han borrado del almacenamiento persistente. El operador debe recuperar una copia archivada (si es que existe) de la configuración y restaurar una imagen de trabajo al router. A continuación, se debe llevar a cabo la recuperación de cada router afectado, lo que contribuye al tiempo de inactividad total de la red.

Tenga en cuenta que la característica de configuración flexible del software IOS de Cisco permite a un router proteger y mantener una copia de trabajo de la imagen y de la configuración del sistema operativo en ejecución, de manera que esos archivos puedan tolerar intentos maliciosos de borrar los contenidos del almacenamiento persistente (NVRAM y flash).



4.5.4 Realización de una copia de seguridad y una actualización de la imagen del software

Realización de una copia de seguridad de la imagen del software IOS

Entre las tareas básicas de administración, se incluyen guardar copias de seguridad de sus archivos de configuración y descargar e instalar archivos de configuración actualizados cuando se indique. Un archivo de imagen de copia de seguridad de software se crea copiando el archivo de imagen de un router a un servidor TFTP de red.

Para copiar una imagen del software IOS de Cisco de la memoria flash al servidor TFTP de red, debe seguir los pasos que se sugieren a continuación.

Haga clic en los botones Topología y Config de la figura, a medida que completa cada paso.

Paso 1. Haga ping en el servidor TFTP para asegurarse de que tiene acceso a él.

Paso 2. Verifique que el servidor TFTP tenga suficiente espacio en disco para contener la imagen del software IOS de Cisco. Use el comando **show flash:** del router para determinar el tamaño del archivo de imagen del software IOS de Cisco.

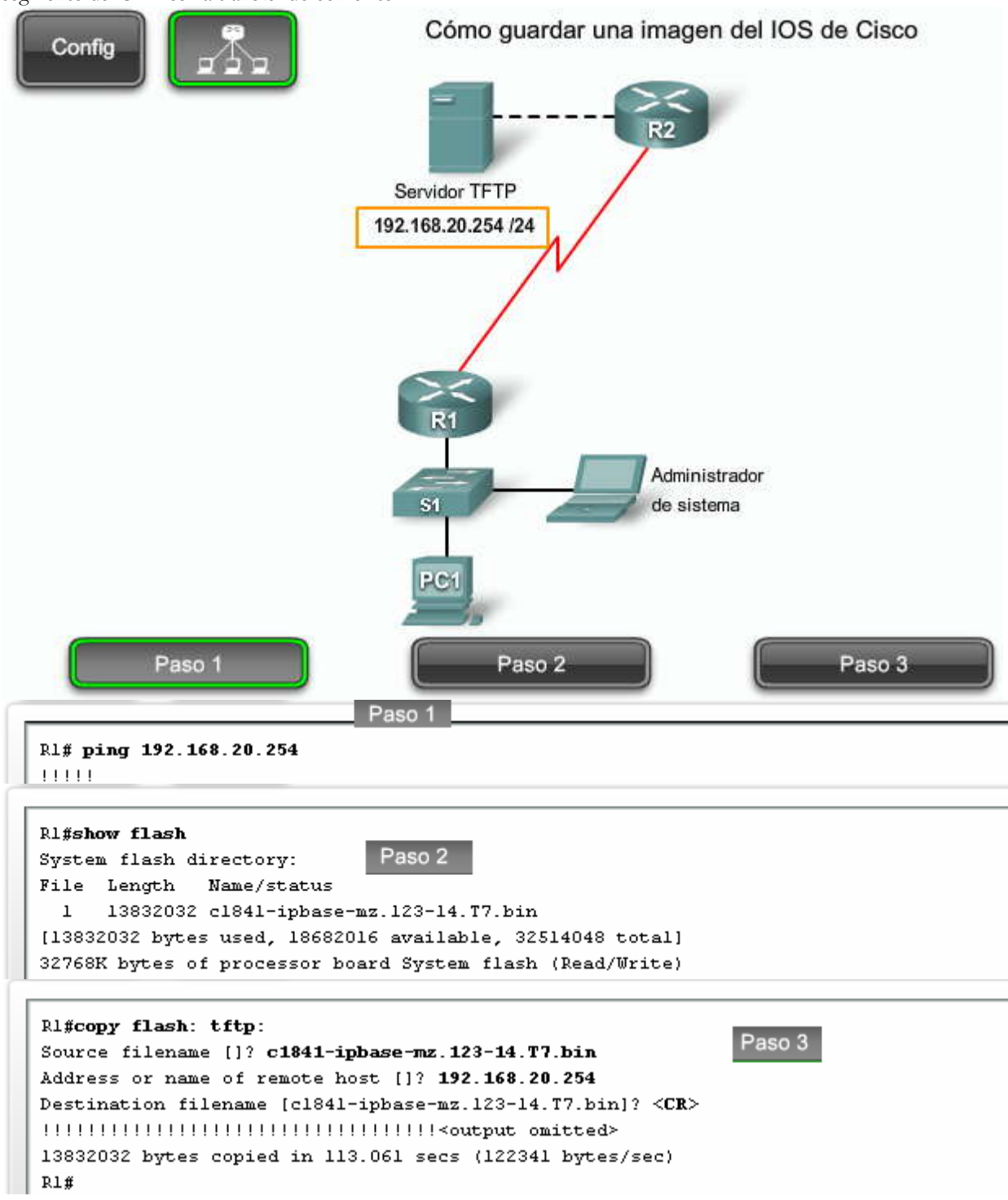
El comando **show flash:** es una herramienta importante para recopilar información acerca de la memoria del router y del archivo de imagen. Puede determinar los siguientes elementos:

- Cantidad total de memoria flash en el router
- Cantidad de memoria flash disponible
- Nombre de todos los archivos almacenados en la memoria flash

Una vez completados los pasos 1 y 2, realice una copia de seguridad de la imagen del software.

Paso 3. Copie el archivo de imagen del sistema actual del router en el servidor TFTP de red mediante el comando **copy flash: tftp:** en el modo EXEC privilegiado. El comando requiere que escriba la dirección IP del host remoto y el nombre de los archivos de imagen del sistema de origen y destino.

Durante el proceso de copia, los signos de exclamación (!) indican el progreso. Cada signo de exclamación significa que un segmento del UDP se ha transferido con éxito.



Actualización de las imágenes del software IOS

Actualizar un sistema a una versión de software más nueva requiere descargar un archivo de imagen del sistema diferente en el router. Use el comando **copy tftp: flash:** para descargar la nueva imagen desde el servidor TFTP de red.

Haga clic en el botón Config de la figura.

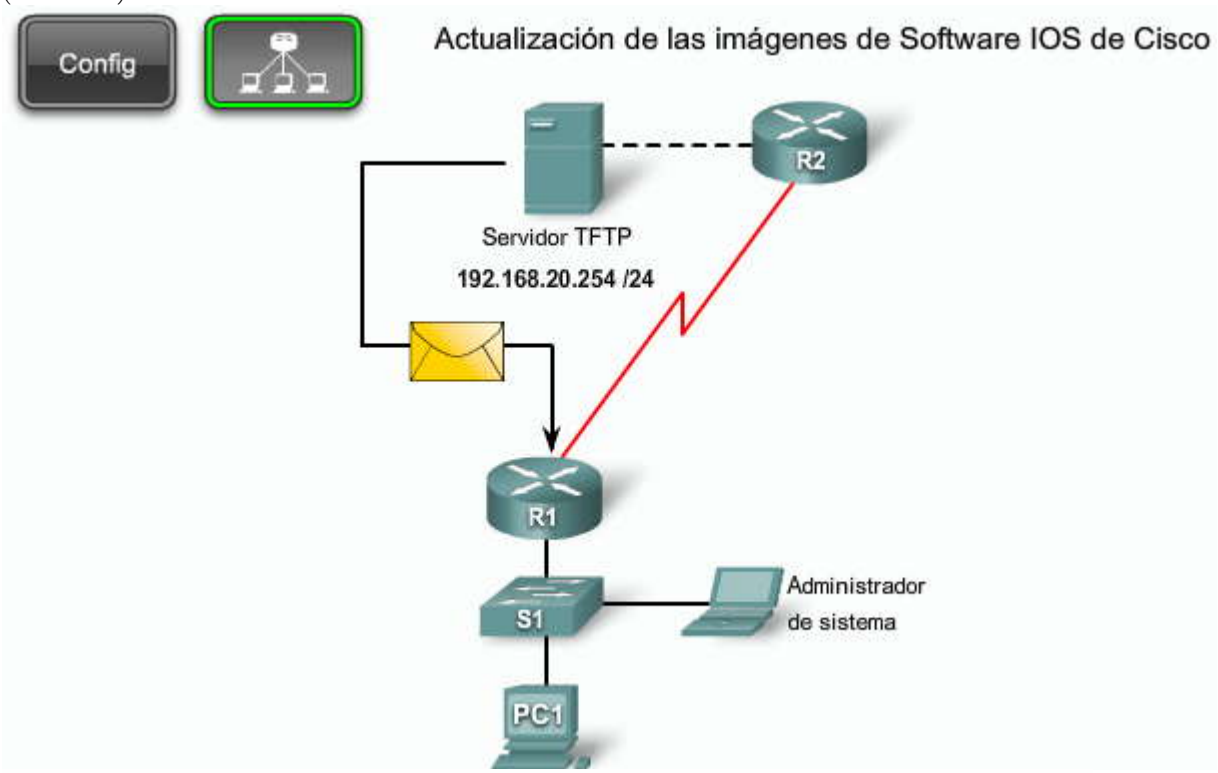
El comando le solicita que escriba la dirección IP del host remoto y el nombre del archivo de imagen del sistema de origen y destino. Escriba el nombre de archivo de la imagen de la actualización correspondiente, tal como aparece en el servidor.

Una vez confirmadas estas entradas, aparece el indicador Erase flash: . Borrar la memoria flash deja espacio para la nueva imagen. Borre la memoria flash si ésta no es suficiente para más de una imagen del IOS de Cisco. Si no hay memoria flash

libre disponible, se debe llevar a cabo la rutina de borrado para poder copiar nuevos archivos. El sistema le informa acerca de estas condiciones y le solicita una respuesta.

Cada signo de exclamación (!) significa que un segmento del UDP se ha transferido con éxito.

Nota: Asegúrese de que la imagen del IOS de Cisco cargada sea adecuada para la plataforma del router. Si se carga una imagen incorrecta del IOS de Cisco, el router podría no arrancar, lo que requeriría intervención del monitor de la ROM (ROMmon).




```
R1#copy tftp: flash:
Address or name of remote host [192.168.20.254]? <CR>
Source filename []? c1841-ipbase-mz.123-14.T7.bin
Destination filename [c1841-ipbase-mz.123-14.T7.bin]?<CR>
Accessing tftp://192.168.20.254/c1841-ipbase-mz.123-14.T7.bin…

Erase flash: before copying? [confirm] <CR>
Erasing the flash filesystem will remove all files! Continue? [confirm] <CR>
Erasing device… eeeeeee (output omitted) erased
Erase of flash: complete
Loading c1841-ipbase-mz.123-14.T7.bin from 192.168.20.254 (via Serial 0/0/0):
!!!!!! (output omitted)
```

En esta actividad, configura el acceso a un servidor TFTP y carga una imagen del IOS de Cisco más nueva y más avanzada. Pese a que Packet Tracer simula una actualización de la imagen del IOS de Cisco en un router, no simula una copia de seguridad de la imagen del IOS de Cisco en el servidor TFTP. Además, pese a que la imagen a la que está actualizando es más avanzada, esta simulación de Packet Tracer no refleja la actualización al activar comandos más avanzados. Se sigue utilizando el mismo conjunto de comandos de Packet Tracer.
Se proporcionan instrucciones detalladas dentro de la actividad y en el siguiente enlace al PDF.
Instrucciones de la actividad (PDF)

4.5.5 Recuperación de las imágenes del software

Restauración de las imágenes del software IOS

Un router no funciona sin su software IOS de Cisco. Si se elimina o se daña el IOS, un administrador debe copiar una imagen en el router para que funcione nuevamente.

Una forma de lograrlo sería utilizar la imagen del IOS de Cisco que se guardó anteriormente en el servidor TFTP. En el ejemplo de la figura, se hizo una copia de seguridad de la imagen del IOS de R1 en un servidor TFTP conectado a R2. R1 no logra conectarse a ese servidor TFTP en su estado actual.

Cuando un IOS de un router se elimina accidentalmente de la memoria flash, el router sigue funcionando porque IOS se está ejecutando en la memoria RAM. Sin embargo, es esencial que el router no se reinicie en este momento, ya que no podría encontrar un IOS válido en flash.
En la figura, el IOS del router R1 se ha eliminado accidentalmente de la memoria flash. Desafortunadamente, el router se ha reiniciado y ya no puede cargar un IOS. Ahora está cargando el indicador de ROMmon predeterminado. Mientrasse encuentra en este estado, el router R1 necesita recuperar el IOS que se había copiado anteriormente en el servidor TFTP conectado a R2. En esta situación, el servidor TFTP se conecta directamente al router R1. Una vez realizados los preparativos con el servidor TFTP, lleve a cabo el siguiente procedimiento.

Paso 1. Conecte los dispositivos.

- Conecte la PC del administrador del sistema al puerto de consola del router afectado.
- Conecte el servidor TFTP al primer puerto Ethernet del router. En la figura, R1 es un router Cisco 1841; por lo tanto, el puerto es Fa0/0. Active el servidor TFTP y configúrelo con la dirección IP estática 192.168.1.1/24.

Paso 2. Inicie el router y defina las variables de ROMmon.

Dado que el router no tiene una imagen del IOS de Cisco válida, el router arranca automáticamente en el modo ROMmon. Hay muy pocos comandos disponibles en el modo ROMmon. Puede verlos al escribir**?** en el indicador de comando rommon>.

Debe escribir todas las variables que se enumeran en la figura. Cuando escribe las variables de ROMmon, tenga en cuenta lo siguiente:

- Los nombres de variables hacen distinción entre mayúsculas y minúsculas.
- No incluya ningún espacio antes o después del símbolo =.
- Cuando sea posible, use un editor de texto para cortar y pegar las variables en la ventana de terminal. Debe escribir la línea completa correctamente.
- Las teclas de navegación no funcionan.

Ahora, el router R1 debe estar configurado con los valores adecuados para conectarse al servidor TFTP. La sintaxis de los comandos de ROMmon es esencial. Si bien las direcciones IP, la máscara de subred y el nombre de la imagen de la figura son sólo ejemplos, es esencial respetar la sintaxis que se muestra al configurar el router. Tenga en cuenta que las variables reales cambian según su configuración.

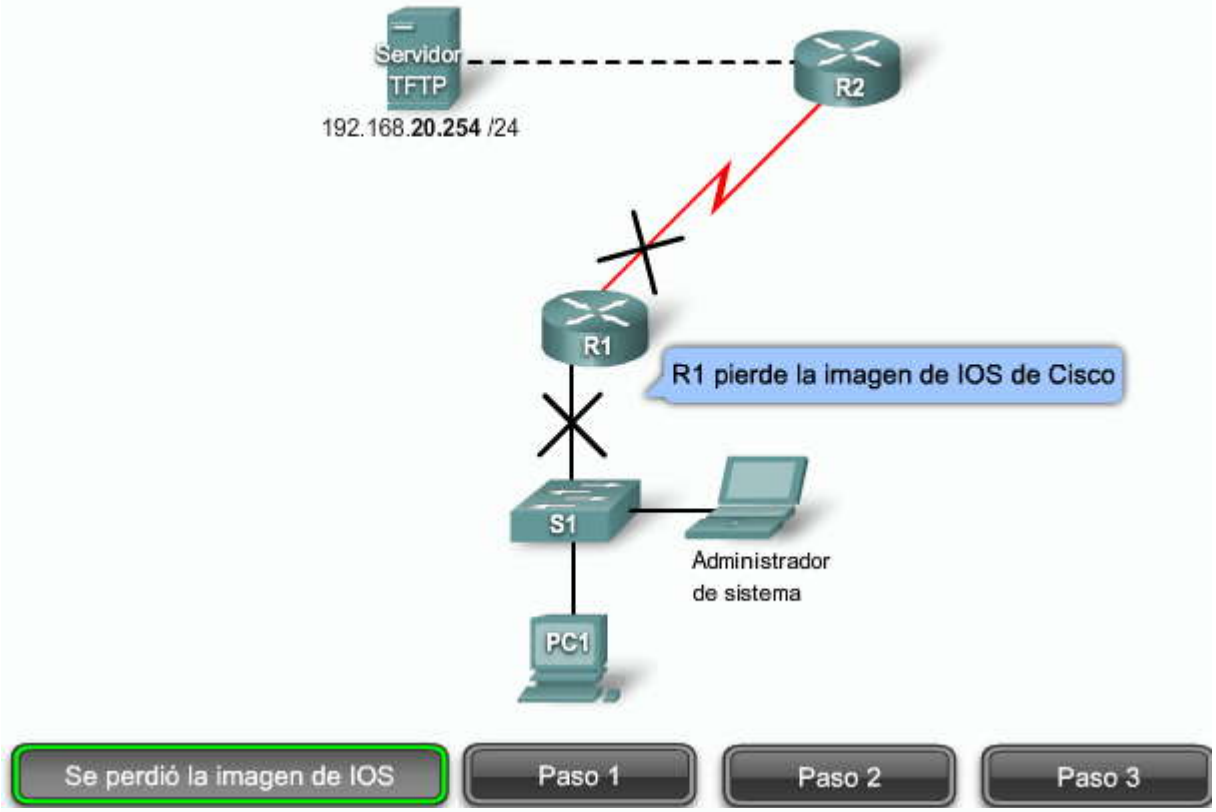
Cuando haya escrito las variables, continúe con el paso siguiente.

Paso 3. Introduzca el comando **tftpdnld** en el indicador de ROMmon.

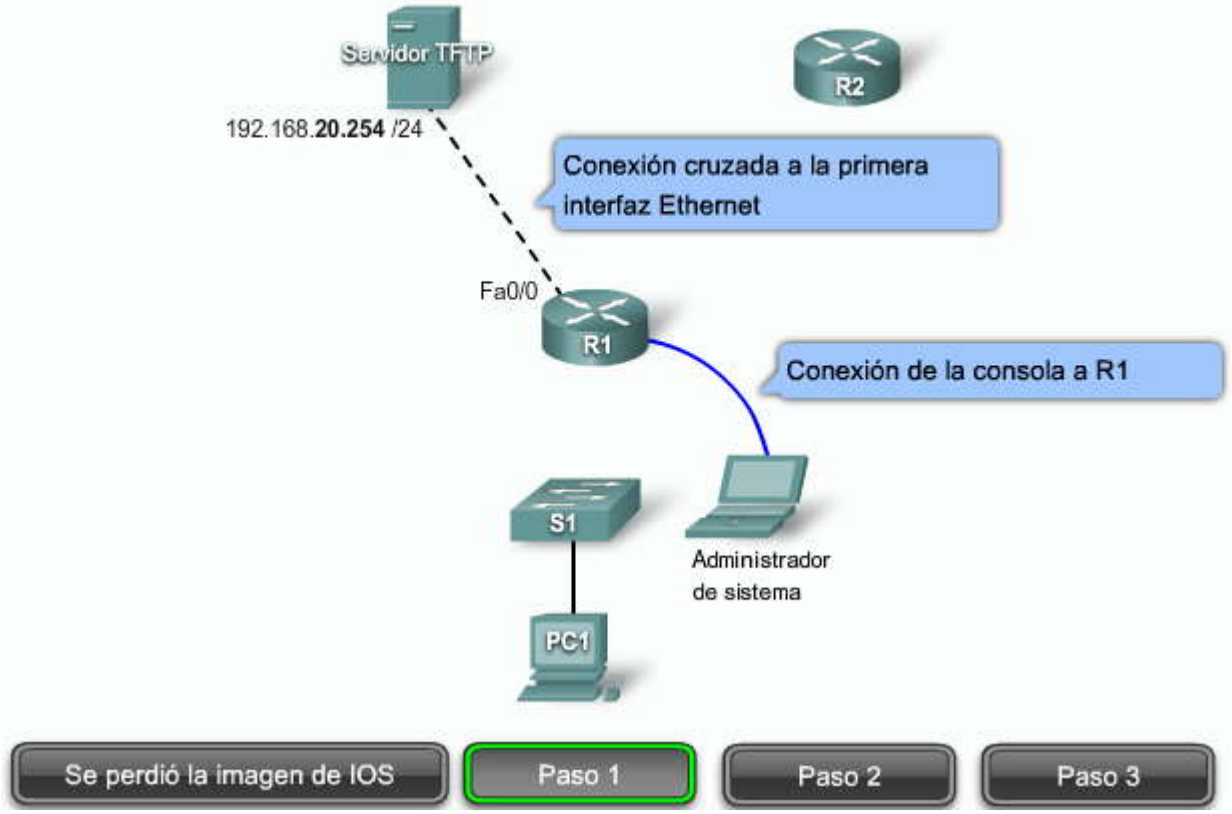
El comando muestra las variables de entorno necesarias y advierte que se borran todos los datosexistentes en la memoria flash. Escriba **y** para seguir y presione **Intro**. El router intenta conectarse al servidor TFTP para comenzar la descarga. Cuando esté conectado, la descarga comienza según lo indicado por las marcas del signo de exclamación (!). Cada! indica que el router ha recibido un segmento UDP.

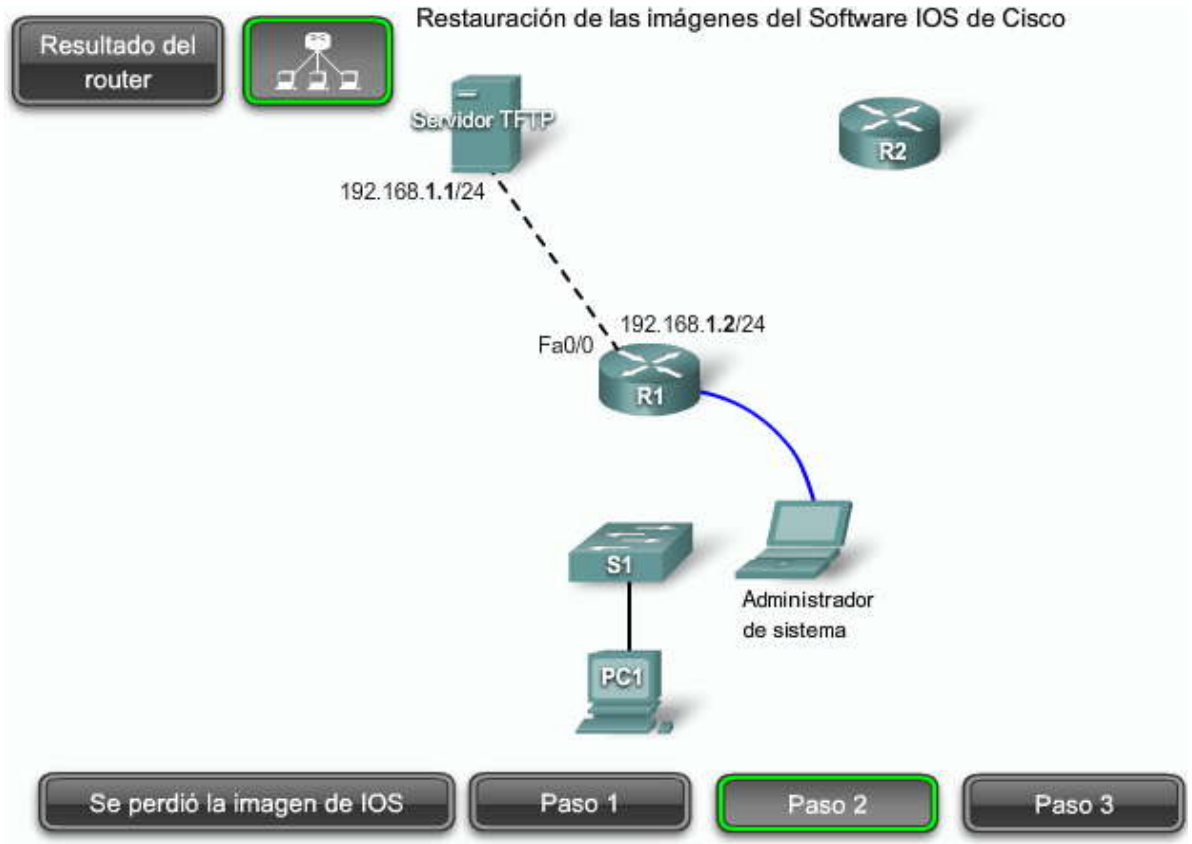
Puede utilizar el comando **reset** para volver a cargar el router con la nueva imagen del IOS de Cisco.

Restauración de las imágenes del Software IOS de Cisco

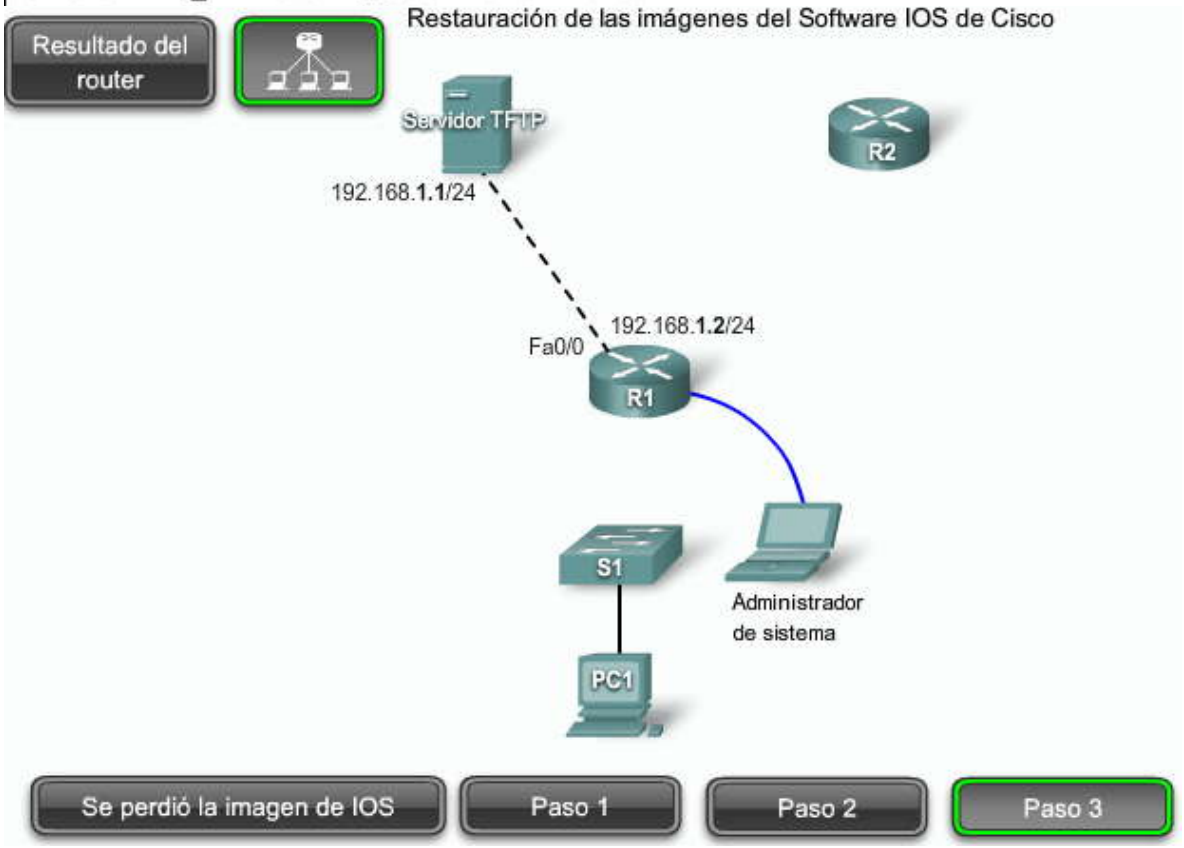


Restauración de las imágenes del Software IOS de Cisco






```
rommon1> IP_ADDRESS=192.168.1.2
rommon2> IP_SUBNET_MASK=255.255.255.0
rommon3> DEFAULT_GATEWAY=192.168.1.1
rommon4> TFTP_SERVER=192.168.1.1
rommon5> TFTP_FILE=c1841-ipbase-mz.123-14.T7.bin
```



Uso de xmodem para restaurar una imagen del IOS

Usar el comando **tftpdnld** es una forma muy rápida de copiar el archivo de imagen. Otro método para restaurar una imagen del IOS de Cisco en un router es utilizar Xmodem. Sin embargo, la transferencia del archivo se logra mediante el cable de la consola y, por lo tanto, es muy lenta en comparación con el comando **tftpdnld**.

Si se pierde la imagen del IOS de Cisco, el router cambia al modo ROMmon cuando arranca. ROMmon es compatible con Xmodem. Con esa capacidad, el router puede comunicarse con una aplicación de emulación de terminal, como HyperTerminal, en la PC del administrador del sistema. Un administrador del sistema que tiene una copia de la imagen del IOS de Cisco en una PC puede restaurarla al router estableciendo una conexión de consola entre la PC y el router, y ejecutando Xmodem desde HyperTerminal.

Los pasos que sigue el administrador se muestran en la figura.

Paso 1. Conecte la PC del administrador del sistema al puerto de consola del router afectado. Abra una sesión de emulación de terminal entre el router R1 y la PC del administrador del sistema.

Paso 2. Inicie el router y emita el comando **xmodem** en el indicador de ROMmon.

La sintaxis del comando es **xmodem** [**-cyr**] [*nombre de archivo*]. La opción cyr varía según la configuración. Por ejemplo, **-c** especifica CRC-16, **y** especifica el protocolo Ymodem y **r** copia la imagen a la memoria RAM. Filename es el nombre del archivo que se debe transferir.

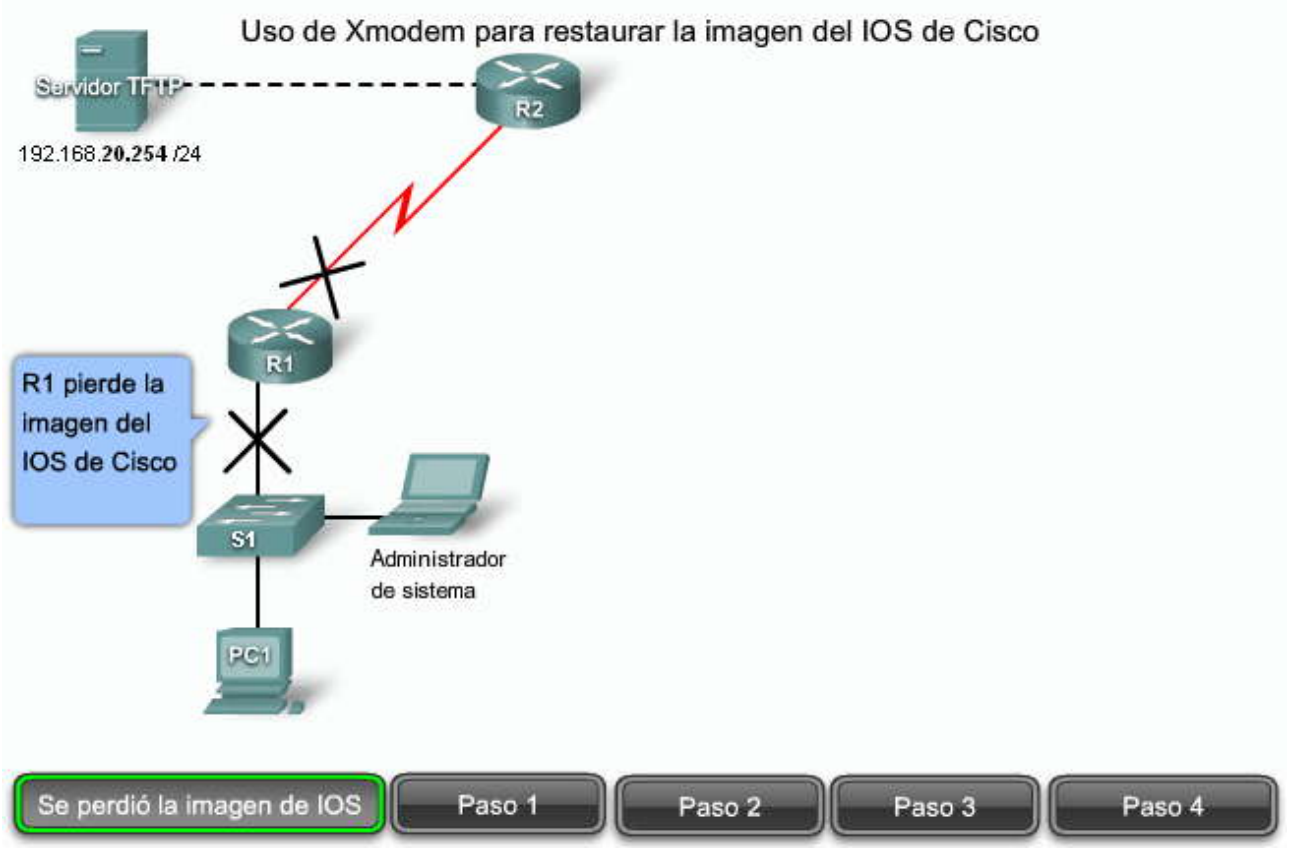
Acepte todas las solicitudes cuando se le indique, como se muestra en la figura.

Paso 3. La figura muestra el proceso para enviar un archivo mediante HyperTerminal. En este caso, seleccione **Transfer > Send File**.

Paso 4. Explore la ubicación de la imagen del IOS de Cisco que desea transferir y elija el protocolo Xmodem. Haga clic en **Send**. Aparece un cuadro de diálogo en donde se muestra el estado de la descarga. El host y el router comienzan a transferir la información después de varios segundos.

Cuando comienza la descarga, los campos Paquete y Transcurrido aumentan. Preste atención al indicador del tiempo restante estimado. El tiempo de descarga podría mejorarse drásticamente si modifica la velocidad de la conexión de HyperTerminal y del router de 9600 bps a 115 000 bps.

Cuando finaliza la transferencia, el router se vuelve a cargar automáticamente con el nuevo IOS de Cisco.

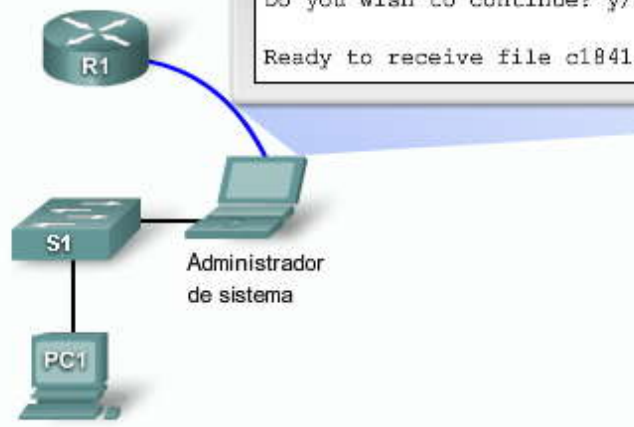


Uso de Xmodem para restaurar la imagen del IOS de Cisco

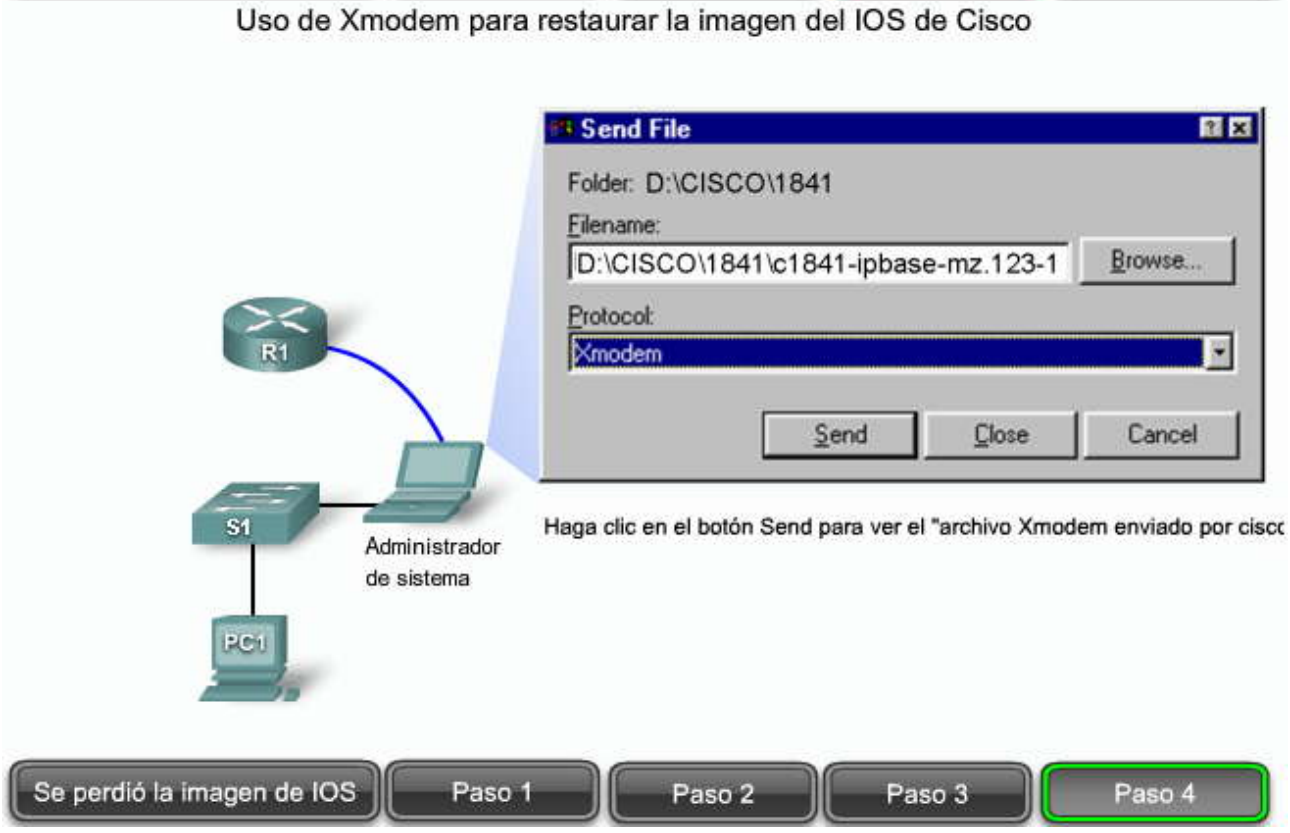
Se perdió la imagen de IOS | Paso 1 | Paso 2 | Paso 3 | Paso 4

Uso de Xmodem para restaurar la imagen del IOS de Cisco

```
rommon1>xmodem -c c1841-ipbase-mz.123-14.T7.bin
Do not start the sending program yet...
device does not contain a valid magic number
dir: cannot open device "flash:"

WARNING: All existing data in bootflash will be lost!
Invoke this application only for disaster recovery.
Do you wish to continue? y/n  [n]:y <CR>

Ready to receive file c1841-ipbase-mz.123-14.T7.bin
```



Se perdió la imagen de IOS | Paso 1 | Paso 2 | Paso 3 | Paso 4



4.5.6 Resolución de problemas de las configuraciones del IOS de Cisco

Comandos para la resolución de problemas del IOS de Cisco

Cuando tiene una imagen válida del IOS de Cisco ejecutándose en todos los routers de la red y tiene copias de seguridad de todas las configuraciones, puede ajustar manualmente las configuraciones de los dispositivos individuales para mejorar el rendimiento de éstos en la red.

Dos comandos que se usan frecuentemente en la administración de redes cotidiana son **show** y **debug**. La diferencia entre ambos es significativa. Un comando **show** enumera los parámetros configurados y sus valores. El comando **debug** le permite realizar un seguimiento de la ejecución de un proceso. Use el comando **show** para verificar las configuraciones. Use el comando **debug** para identificar los flujos de tráfico a través de las interfaces y los procesos del router.

La figura resume las características de los comandos **show** y **debug**. El mejor momento para conocer los resultados generados por estos comandos es cuando la red funciona a la perfección. De esta manera, puede reconocer qué falta o cuáles son los errores al utilizar los comandos para resolver los problemas de una red.

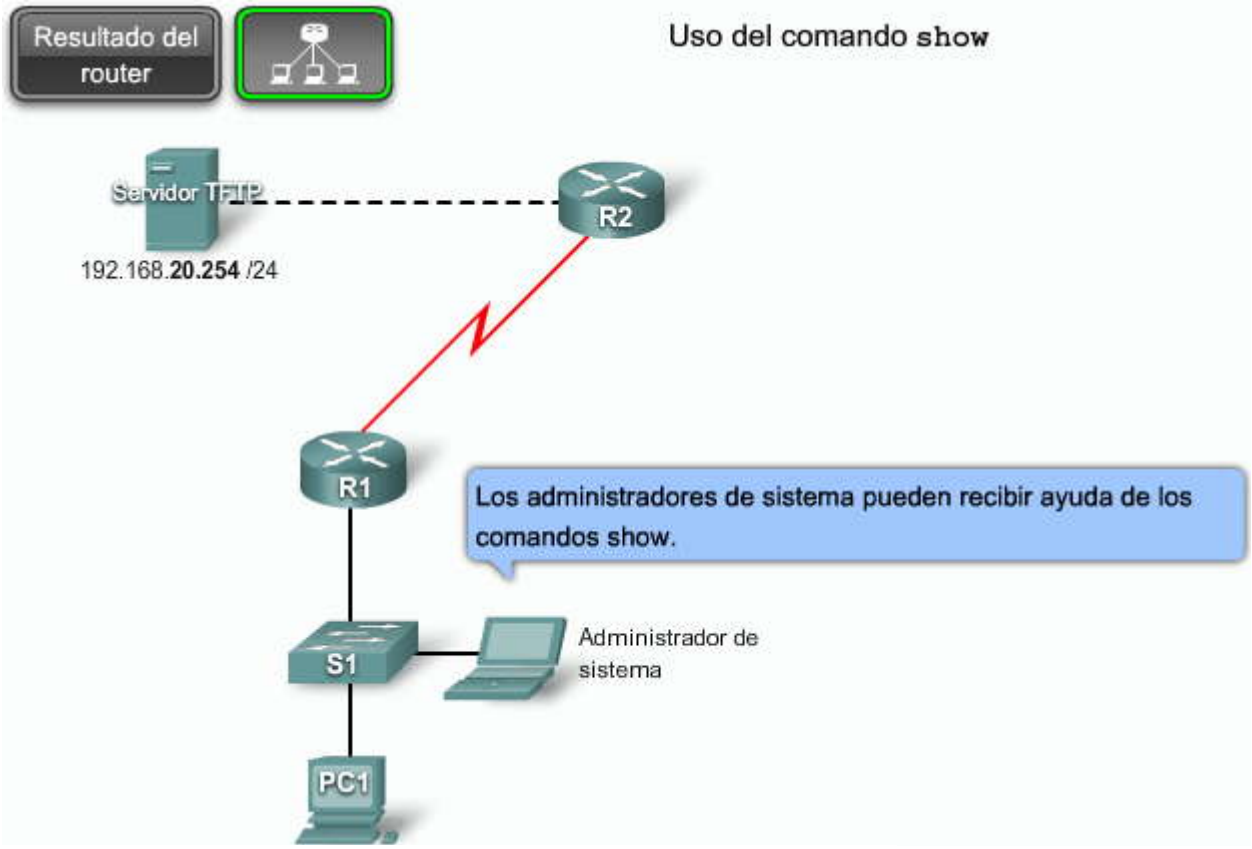
Comandos para la resolución de problemas del IOS de Cisco

	show	debug
Característica de procesamiento	Estática	Dinámica
Proceso de carga	Baja sobrecarga	Alta sobrecarga
Uso principal	Recopilar hechos	Observar los procesos

Uso del comando show

El comando **show** muestra información estática. Use los comandos **show** al compilar hechos para aislar los problemas de una internetwork, incluidos los problemas con interfaces, nodos, medios, servidores, clientes o aplicaciones. También puede utilizarlo con frecuencia para confirmar la implementación de las modificaciones de la configuración.

El ejemplo de la figura proporciona una muestra de los resultados del comando **show protocols**. La guía de comandos del IOS de Cisco enumera 1463 comandos **show**. Cuando se encuentre en la ventana de comandos, escriba **show ?** para obtener una lista de los comandos **show** disponibles para el nivel y el modo en que está operando.




```
R1#show protocols
Global values:
  Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
FastEthernet0/1 is administratively down, line protocol is down
Serial0/0/0 is up, line protocol is up
  Internet address is 10.1.1.1/30
Vlan1 is administratively down, line protocol is down
```

Uso del comando debug

Cuando configura un router, los comandos que ingresa inician muchos más procesos que los que ve en la línea de código simple. Por lo tanto, un seguimiento de las configuraciones escritas línea por línea no revela todas las posibilidades de error.

En cambio, necesita alguna manera de capturar datos desde el dispositivo a medida que se inicia cada paso de un proceso en ejecución.

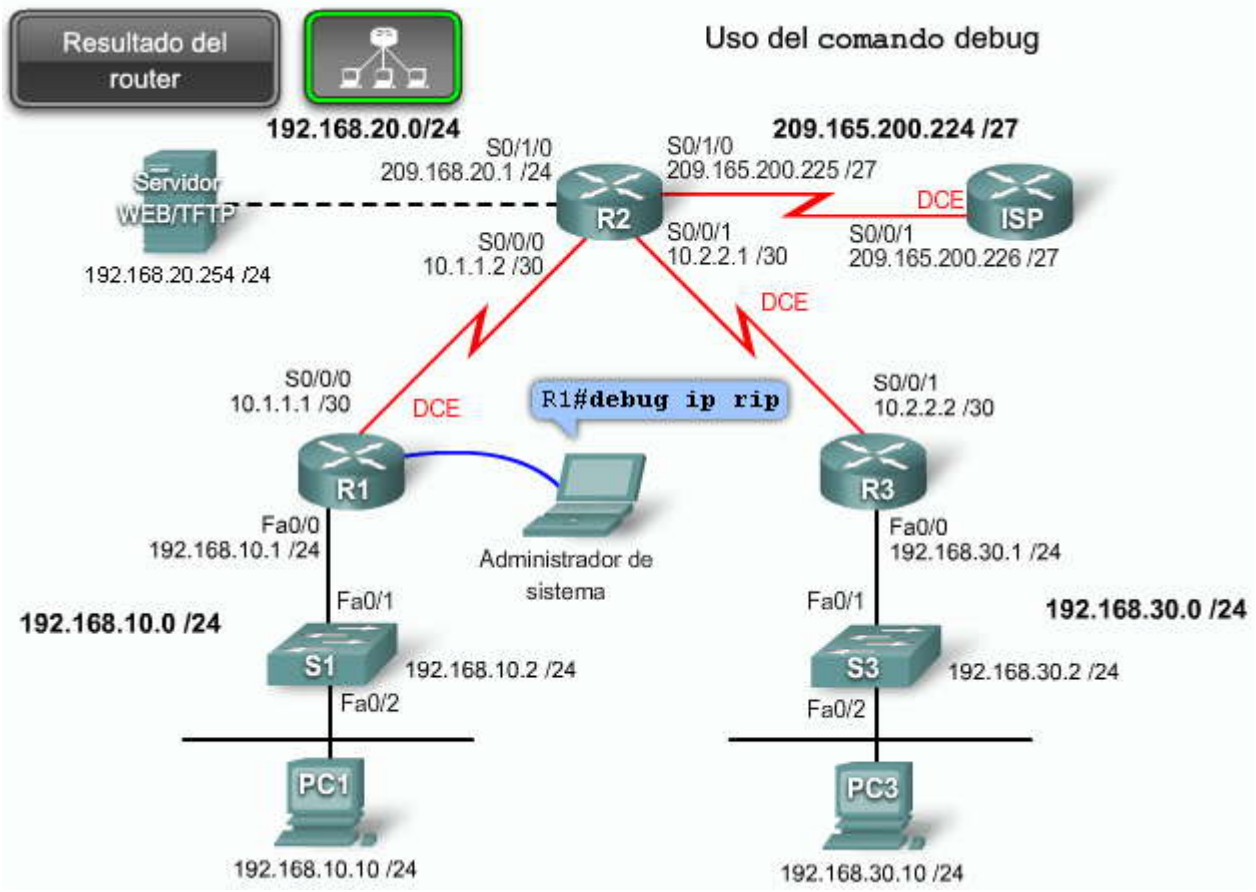
De forma predeterminada, el servidor de red envía el resultado desde los comandos **debug** y los mensajes de error del sistema a la consola. Recuerde que puede redireccionar los resultados del comando debug a un servidor syslog.

Nota: Al resultado de la depuración se le asigna una alta prioridad en la cola del proceso de la CPU y, por lo tanto, puede interferir con los procesos de producción normales de una red. Por este motivo, use los comandos **debug** durante las horas de tranquilidad y sólo para resolver problemas específicos.

El comando **debug** muestra los sucesos y datos dinámicos. Use **debug** para verificar el flujo del tráfico del protocolo, a fin de detectar problemas, defectos del protocolo o configuraciones erróneas. El comando **debug** proporciona un flujo de información acerca del tráfico que se ve (o no se ve) en una interfaz, mensajes de error generados por los nodos de una red, paquetes de diagnóstico específicos del protocolo y otros datos útiles para el diagnóstico de fallas. Use los comandos **debug** cuando las operaciones del router o de la red deban verse para determinar si los eventos o los paquetes funcionan correctamente.

Todos los comandos **debug** se introducen en el modo EXEC privilegiado y la mayoría de los comandos **debug** no toman argumentos. Para enumerar y ver una breve descripción de todas las opciones de los comandos de depuración, introduzca el comando **debug ?** en el modo EXEC privilegiado.

Precaución: Es importante desactivar la depuración cuando haya terminado su resolución de problemas. La mejor manera de asegurarse de que no haya operaciones de depuración prolongadas en ejecución es utilizar el comando **no debug all**.



```
R1#debug ip rip
RIP protocol debugging is on
R1#RIP: sending  v1 update to 255.255.255.255 via FastEthernet0/0 (192.168.10.1)
RIP: build update entries
      network 10.0.0.0 metric 1
      network 192.168.20.0 metric 2
      network 192.168.30.0 metric 3
      network 209.165.200.0 metric 2
RIP: sending  v1 update to 255.255.255.255 via Serial0/0/0 (10.1.1.1)
RIP: build update entries
      network 192.168.10.0 metric 1
RIP: received v1 update from 10.1.1.2 on Serial0/0/0
      10.2.2.0 in 1 hops
      192.168.20.0 in 1 hops (output omitted)
no debug all
All possible debugging has been turned off
```

Consideraciones para utilizar el comando debug

Una cosa es utilizar los comandos **debug** para solucionar los problemas de una red de laboratorio que no tiene tráfico de aplicaciones para usuarios finales. Otra cosa es utilizar los comandos **debug** en una red de producción de la cual los usuarios dependen para el flujo de datos. Sin las precauciones adecuadas, el impacto de un comando **debug** centrado en sentido amplio podría empeorar las cosas.

Con el uso adecuado, selectivo y temporario de los comandos **debug**, puede obtener información potencialmente útil sin la necesidad de un analizador de protocolos u otra herramienta de terceros.

Otras consideraciones para utilizar los comandos **debug** son las siguientes:

- Cuando la información que necesita del comando **debug** se interpreta y la depuración (y todo otro valor de configuración relacionado, si corresponde) finaliza, el router puede reanudar su conmutación más rápida. Se puede reanudar la resolución de problemas, crear un plan de acción mejor encaminado y resolver el problema de la red.
- Tenga en cuenta que los comandos **debug** pueden generar demasiados datos de poca utilidad para un problema específico. Normalmente, el conocimiento del protocolo o de bs protocolos que se están depurando es necesario para interpretar correctamente los resultados de **debug**.
- Cuando utilice las herramientas de resolución de problemas de **debug**, tenga en cuenta que los formatos de los resultados varían con cada protocolo. Algunas generan una única línea de resultados por paquete, otras generan varias líneas de resultados por paquete. Algunos comandos **debug** generan grandes cantidades de resultados; otros sólo generan resultados ocasionales. Algunos generan líneas de texto y otros generan información en el formato de los campos.

Consideraciones para tener en cuenta al usar el comando **debug**

Consideraciones a tener en cuenta al usar el comando debug
• **debug** tiene prioridad en la CPU. Planifique detalladamente el uso de **debug**.
• **debug** puede ayudar a resolver problemas persistentes, lo que supera la importancia del efecto que aporta al rendimiento de la red.
• **debug** puede generar demasiada salida. Determine sus objetivos antes de comenzar.
• Los diferentes debugs generan diferentes formatos de salida. No se deje sorprender.
• Planifique el uso del comando **debug**. Utilícelo con mucho cuidado.

Comandos relacionados con el comando debug

Para utilizar las herramientas de depuración de manera eficaz, debe tener en cuenta lo siguiente:

- El impacto que tiene una herramienta de resolución de problemas en el rendimiento del router
- Un uso más selectivo y centrado de la herramienta de diagnóstico
- Cómo minimizar el impacto de la resolución de problemas en otros procesos que compiten por recursos en el dispositivo de red
- Cómo detener la herramienta de resolución de problemas cuando el diagnóstico se completó, a fin de que el router pueda reanudar su conmutación más eficiente

Los siguientes comandos pueden ayudarlo a optimizar el uso eficiente del comando **debug**:

- El comando **service timestamps** se utiliza para agregar una marca horaria a un comando debug o mensaje de registro. Esta característica puede proporcionar información valiosa acerca del momento en que se suscitaron los elementos de la depuración y la duración del tiempo transcurrido entre los sucesos.
- El comando **show processes** muestra el uso de la CPU para cada proceso. Estos datos pueden influir en las decisiones relativas al uso de un comando debug si indican que el sistema de producción ya se utiliza demasiado para agregar un comando debug.
- El comando **no debug all** desactiva todos los comandos debug. Este comando puede liberar recursos del sistema después de finalizar la depuración.
- El comando **terminal monitor** muestra los resultados de la depuración y los mensajes de error del sistema para el terminal y la sesión actuales. Cuando hace Telnet a un dispositivo y se emite un comando **debug**, no se ven resultados a menos que se introduzca este comando.

Comandos relacionados con el comando debug

```
R1(config)# service timestamps debug datetime msec
```

- Agrega una marca horaria a un debug o a un mensaje de registro

```
R1# show processes
```

- Muestra el uso del CPU en cada proceso

```
R1# no debug all
```

- Inhabilita todos los comandos debug

```
R1# terminal monitor
```

- Muestra el resultado de debug en la versión actual vty

4.5.7 Recuperación de una contraseña de router perdida

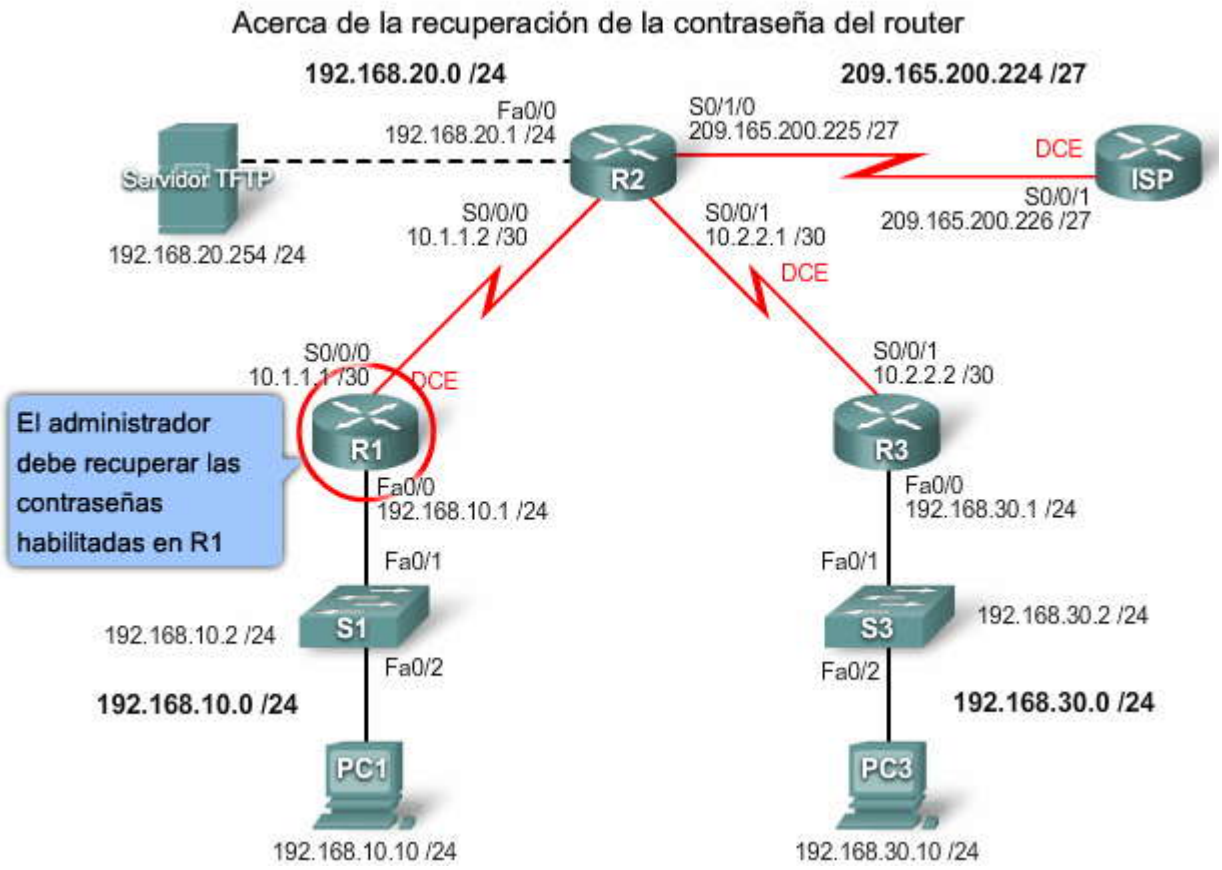
Acerca de la recuperación de contraseñas

¿Alguna vez olvidó la contraseña de un router? Tal vez no, pero en algún momento de su profesión, puede esperar que alguien la olvide y tendrá que recuperarla.

Lo primero que debe saber acerca de la recuperación de contraseñas es que, por razones de seguridad , necesita acceso físico al router. Conecte su PC al router a través de un cable de consola.

Las contraseñas enable y enable secret protegen el acceso a los modos EXEC privilegiado y de configuración. La contraseña enable se puede recuperar, pero la contraseña enable secret de enable está encriptada y debe reemplazarse con una nueva contraseña.

El registro de configuración es un concepto que conocerá más detalladamente a medida que avance en sus estudios. El registro de configuración es similar a la configuración del BIOS de su PC, que controla el proceso de arranque. Entre otras cosas, el BIOS le indica a la PC desde qué disco duro debe arrancar. En un router, un registro de configuración, representado por un valor hexadecimal único, le indica al router qué pasos específicos debe seguir cuando se enciende. Los registros de configuración tienen muchos usos y, probablemente, la recuperación de contraseñas esel más frecuente.



Procedimiento de recuperación de contraseña del router

Para recuperar la contraseña de un router, siga estos pasos:

Prepare el dispositivo

Paso 1. Conéctelo al puerto de consola.

Paso 2. Si perdió la contraseña enable, todavía tendrá acceso al modo EXEC de usuario. Escriba el comando **show version** cuando aparezca la indicación y guarde los parámetros de registro de configuración.

R>#**show version**
<show command output omitted>
El registro de configuración es 0x2102
R1>

Generalmente, el registro de configuración se define en 0x2102 ó 0x102. Si ya no puede obtener acceso al router (debido a que perdió la contraseña TACACS o de conexión), puede suponer con seguridad que su registro de configuración está definido en 0x2102.

Paso 3. Use el interruptor de alimentación para apagar el router y, a continuación, vuelva a encender el router.

Paso 4. Presione Pausa en el teclado del terminal dentro de los 60 segundos desde el encendido para colocar el router dentro de ROMmon.

Haga clic en Ignorar inicio en la figura.

Paso 5. Escriba **confreg 0x2142** en la ventana rommon 1>. Esto hace que el router ignore la configuración de inicio donde se almacena la contraseña enable olvidada.

Paso 6. Escriba **reset** en la ventana rommon 2>. El router se reinicia, pero ignora la configuración guardada.

Paso 7. Escriba **no** después de cada pregunta de configuración, o presione **Ctrl-C** para saltear el procedimiento de configuración inicial.

Paso 8. Escriba **enable** cuando aparezca el indicador Router>. Esto lo coloca en el modo enable y debe poder ver el indicador Router#.

Haga clic en Acceder a NVRAM en la figura.

Paso 9. Escriba **copy startup-config running-config** para copiar la NVRAM en la memoria. Tenga cuidado. No escriba **copy running-config startup-config** porque borra su configuración de inicio.

Paso 10. Escriba **show running-config**. En esta configuración, el comando **shutdown** aparece debajo de todas las interfaces, porque todas están actualmente cerradas. Lo que es más importante, ahora puede ver las contraseñas (contraseña enable, enable secret, vty, contraseñas de consola) ya sea en formato encriptado o no encriptado. Puede volver a usar las contraseñas sin encriptar. Debe cambiar las contraseñas encriptadas por una nueva contraseña.

Haga clic en Restablecer contraseñas en la figura.

Paso 11. Escriba **configure terminal**. Aparece la ventana hostname(config)#.

Paso 12. Escriba **enable secret** *password* para modificar la contraseña enable secret. Por ejemplo:

R1(config)# **enable secret cisco**

Paso 13. Emita el comando **no shutdown** en cada interfaz que desee utilizar. Puede emitir un comando **show ip interface brief** para confirmar que la configuración de su interfaz sea correcta. Cada interfaz que desee utilizar debe mostrar activado activado.

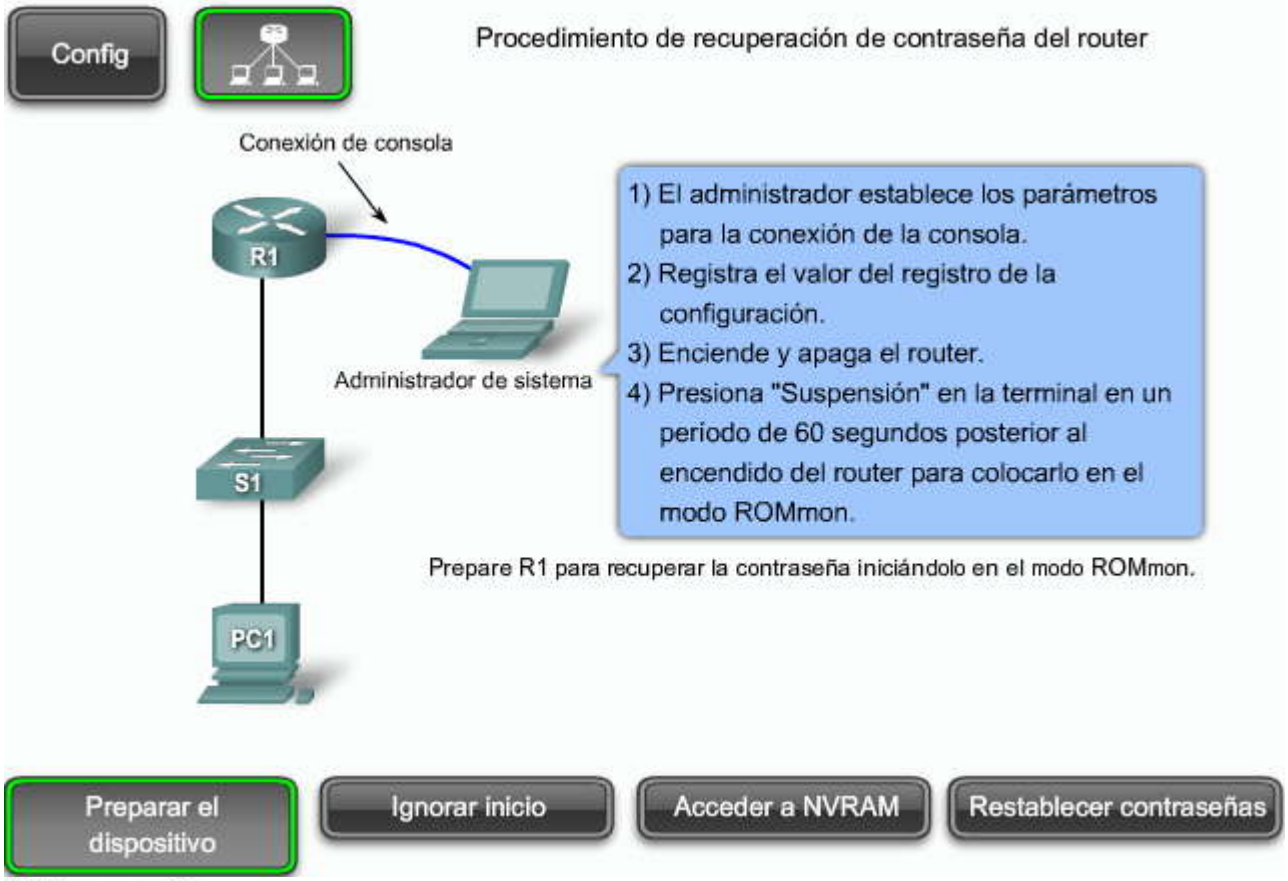
Paso 14. Escriba **config-register** *configuration_register_setting*. *configuration_register_setting* es el valor que registró en el Paso 2 ó 0x2102 . Por ejemplo:

R1(config)#**config-register 0x2102**

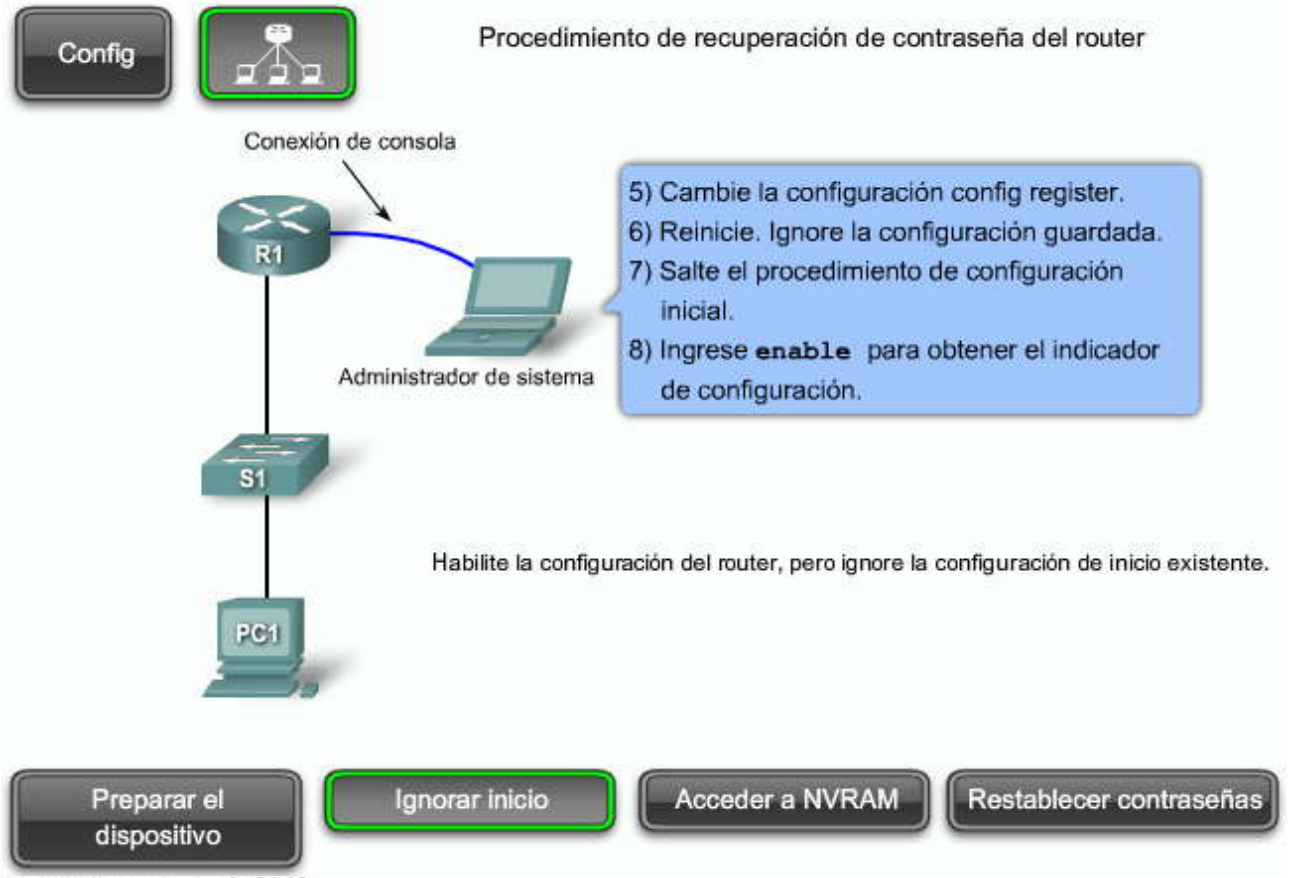
Paso 15. Presione **Ctrl-Z** o escriba **end** para abandonar el modo de configuración. Aparece la ventana hostname#.

Paso 16. Escriba **copy running-config startup-config** para realizar los cambios.

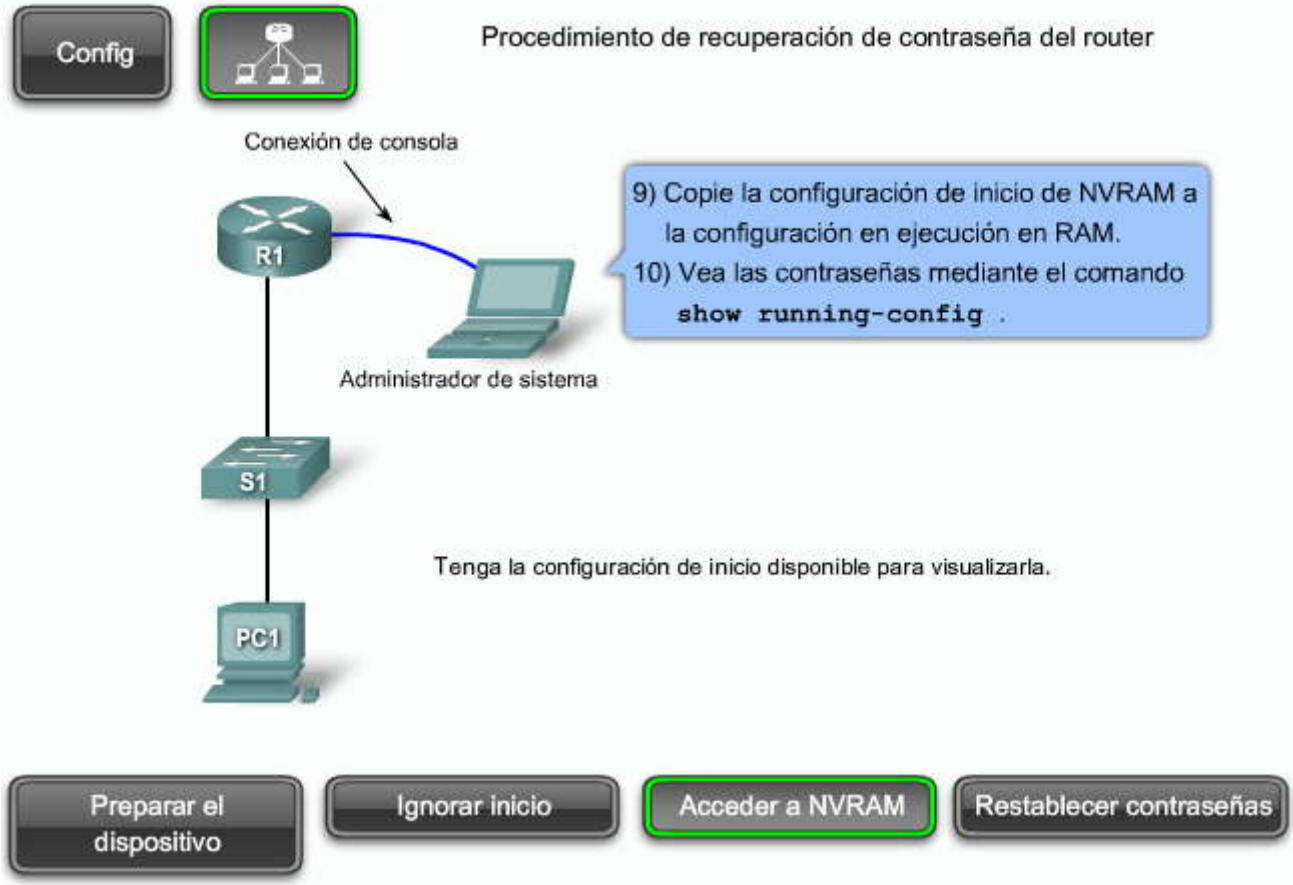
Ha finalizado la recuperación de contraseñas. Al introducir el comando **show version** confirma que el router utilizará los parámetros del registro de configuración establecidos la próxima vez que se reinicie.



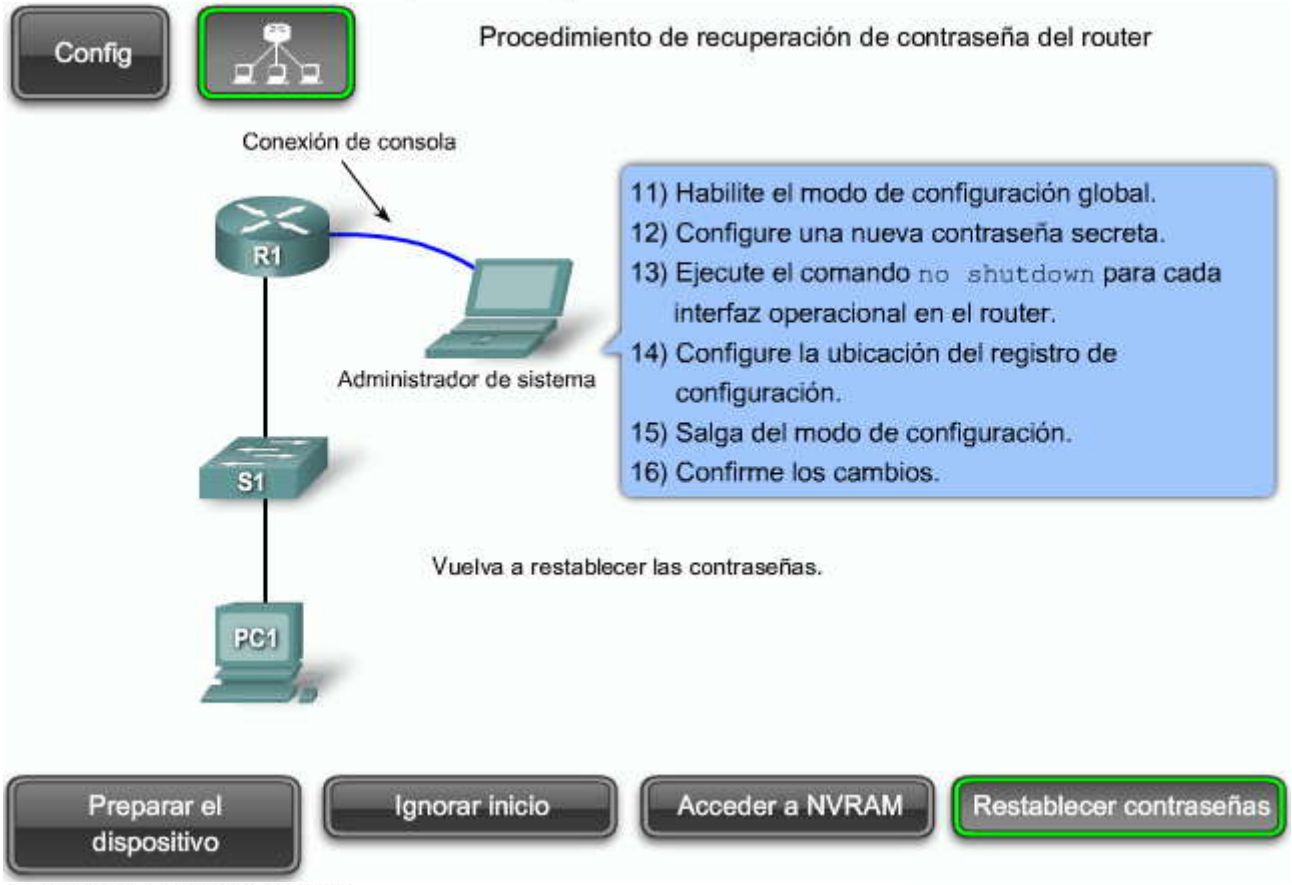

```
R1#show version
Cisco IOS Software, 1841 Software (C1841-IPBASE-M), Version
12.3(14)T7, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.

<output omitted>

Configuration register is 0x2102
R1#
ROMMON1>
```




```
rommon1>confreg 0x2142
rommon2>reset
<output omitted - type "no" to each question>
router>enable
Router#
```



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

Current configuration : 381 bytes
!
version 12.3
no service password-encryption
!
hostname Router
!
!
enable secret 5 $1$d4ST$lweSfykZWWGhId75QBzMo.
```




```
Router#configure terminal
Router(config)#enable secret cisco
Router(config)#interface serial 0/0/1
Router(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
Router(config-if)#exit
Router(config)#interface FastEthernet 0/0
Router(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
Router(config-if)#exit
Router(config)#config-register 0x2102
Router(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console
Router#copy running-config startup-config
Router#
```

CAPITULO V – “ACL ”

5 ACL

5.0 Introducción

5.0.1 Introducción

La seguridad de la red es un tema muy amplio y una buena parte de él va más allá del alcance de este curso. No obstante, una de las capacidades más importantes que un administrador de red necesita es el dominio de las listas de control de acceso (ACL). Los administradores utilizan las ACL para detener el tráfico o permitir sólo el tráfico específico y, al mismo tiempo, para detener el resto del tráfico en sus redes. Este capítulo brinda la oportunidad de desarrollar su dominio de las ACL con una serie de lecciones, actividades y prácticas de laboratorio.

Los diseñadores de red utilizan firewalls para proteger las redes contra el uso no autorizado. Los firewalls son soluciones de hardware o software que hacen cumplir las políticas de seguridad de la red. Es como la cerradura de la puerta de la habitación de un edificio. La cerradura sólo permite que ingresen los usuarios autorizados con una llave o tarjeta de acceso. Del mismo modo, los firewalls filtran el ingreso a la red de los paquetes no autorizados o potencialmente peligrosos. En un router Cisco, puede configurar un simple firewall que proporcione capacidades básicas de filtrado de tráfico mediante las ACL.

Una ACL es una lista secuencial de sentencias de permiso o denegación que se aplican a direcciones o protocolos de capa superior. Las ACL brindan una manera poderosa de controlar el tráfico de entrada o de salida de la red. Puede configurar las ACL para todos los protocolos de red enrutados.

El motivo más importante para configurar las ACL es brindar seguridad a la red. En este capítulo, se explica cómo utilizar las ACL estándar y extendidas como parte de una solución de seguridad y se enseña a configurarlas en un router Cisco. Se incluyen sugerencias, consideraciones, recomendaciones y pautas generales sobre el uso de las ACL.

En este capítulo, aprenderá a:

- Explicar cómo se utilizan las ACL para proteger una red de sucursal de mediana empresa, incluido el concepto de filtrado de paquetes, el propósito de las ACL, cómo se utilizan para controlar el acceso y los tipos de ACL de Cisco.
- Configurar las ACL estándar en una red de sucursal de mediana empresa, incluida la definición de los criterios de filtrado, la configuración de las ACL estándar para filtrar el tráfico y su aplicación a las interfaces del router.
- Configurar las ACL extendidas en una red de sucursal de mediana empresa, incluida la configuración de las ACL extendidas y denominadas, la configuración de filtros, la verificación, la supervisión y la resolución de problemas de las ACL extendidas.
- Describir las ACL complejas en una red de sucursal de mediana empresa, incluida la configuración de ACL dinámicas, reflexivas y basadas en tiempo, la verificación y resolución de problemas de las ACL complejas y la explicación de las claves relevantes.

5.1 Cómo utilizar las ACL para la protección de redes

5.1.1 Una conversación TCP

Las ACL le permiten controlar el tráfico de entrada y de salida de la red. Este control puede ser tan simple como permitir o denegar los hosts o direcciones de red. Sin embargo, las ACL también pueden configurarse para controlar el tráfico de red según el puerto TCP que se utiliza. Para comprender cómo funciona una ACL con TCP, observemos el diálogo durante una conversación TCP cuando descarga una página Web a su equipo.

Cuando solicita datos de un servidor Web, IP se encarga de la comunicación entre la PC y el servidor. TCP se encarga de la comunicación entre su navegador Web (aplicación) y el software de servidor de red. Cuando envía un correo electrónico, visita una página Web o descarga un archivo, TCP es el responsable de desglosar los datos en paquetes para IP, antes de enviarlos, y de integrar los datos de los paquetes al recibirlos. El proceso de TCP es muy similar a una conversación, donde dos nodos de una red aceptan transferir datos entre sí.

Recuerde que TCP ofrece un servicio orientado a la conexión, confiable y de stream de bytes. El término "orientado a la conexión" significa que las dos aplicaciones que utilizan TCP deben establecer una conexión TCP entre sí antes de intercambiar datos. TCP es un protocolo full-duplex, que significa que cada conexión TCP admite un par de streams de bytes, y cada stream fluye en una dirección. TCP incluye un mecanismo de control de flujo para cada stream de bytes que permite al receptor limitar la cantidad de datos que el transmisor puede enviar. TCP también implementa un mecanismo de control de congestión.

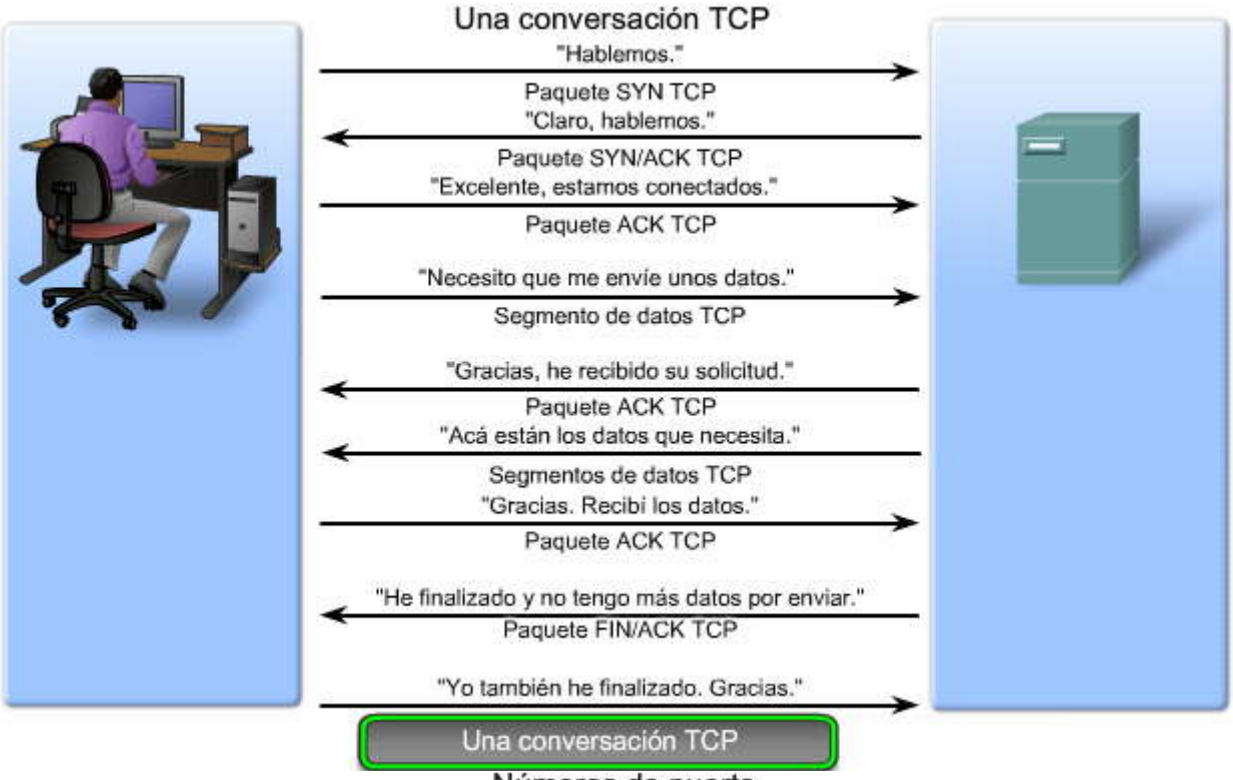
Haga clic en el botón Reproducir que se muestra en la figura para ver la animación.

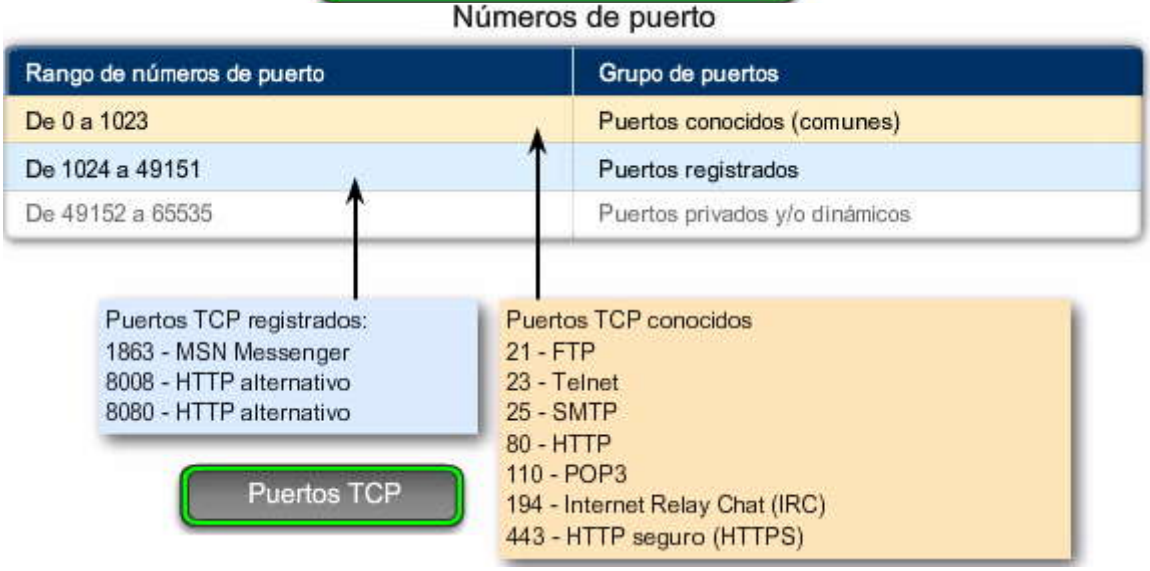
La animación muestra cómo se lleva a cabo una conversación TCP/IP. Los paquetes TCP se marcan con señalizadores que indican su finalidad. SYN inicia (sincroniza) la sesión; ACK es un acuse de recibo de que se recibió el paquete esperado, y FIN finaliza la sesión. SYN/ACK acusa recibo de que la transferencia se sincronizó. Los segmentos de datos TCP incluyen el protocolo de nivel superior necesario para orientar los datos de la aplicación hacia la aplicación correcta.

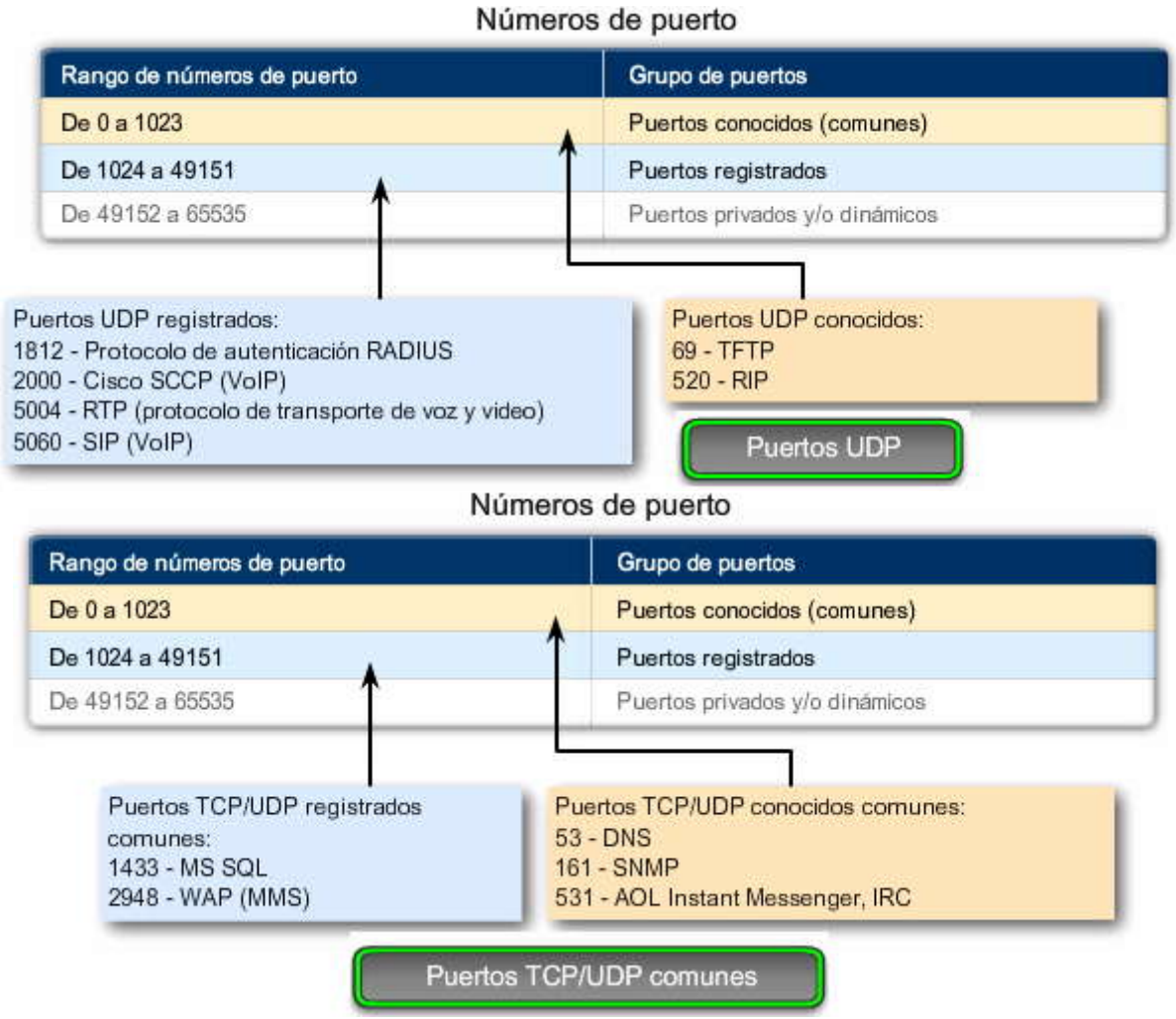
Haga clic en el botón Números de puerto TCP/UDP que se muestra en la figura.

El segmento de datos TCP identifica, además, el puerto que coincide con el servicio solicitado. Por ejemplo, HTTP es puerto 80, SMTP es puerto 25 y FTP es puerto 20 y puerto 21. La figura muestra ejemplos de puertos UDP y TCP.

Haga clic en los botones de la figura para explorar los puertos TCP/UDP.







5.1.2 Filtrado de paquetes

El filtrado de paquetes, a veces denominado filtrado estático de paquetes, controla el acceso a la red, analiza los paquetes de entrada y de salida, y permite o bloquea su ingreso según un criterio establecido.

Un router actúa como filtro de paquetes cuando reenvía o deniega paquetes según las reglas de filtrado. Cuando un paquete llega al router de filtrado de paquetes, éste extrae determinada información del encabezado del paquete y toma decisiones según las reglas de filtrado, ya sea autorizar el ingreso del paquete o descartarlo. El filtrado de paquetes actúa en la capa de red del modelo de interconexión de sistema abierto (OSI, Open Systems Interconnection) o en la capa Internet de TCP/IP.

Como dispositivo de Capa 3, un router de filtrado de paquetes utiliza reglas para determinar la autorización o denegación del tráfico según las direcciones IP de origen y de destino, el puerto origen y el puerto destino, y el protocolo del paquete. Estas reglas se definen mediante las listas de control de acceso o ACL.

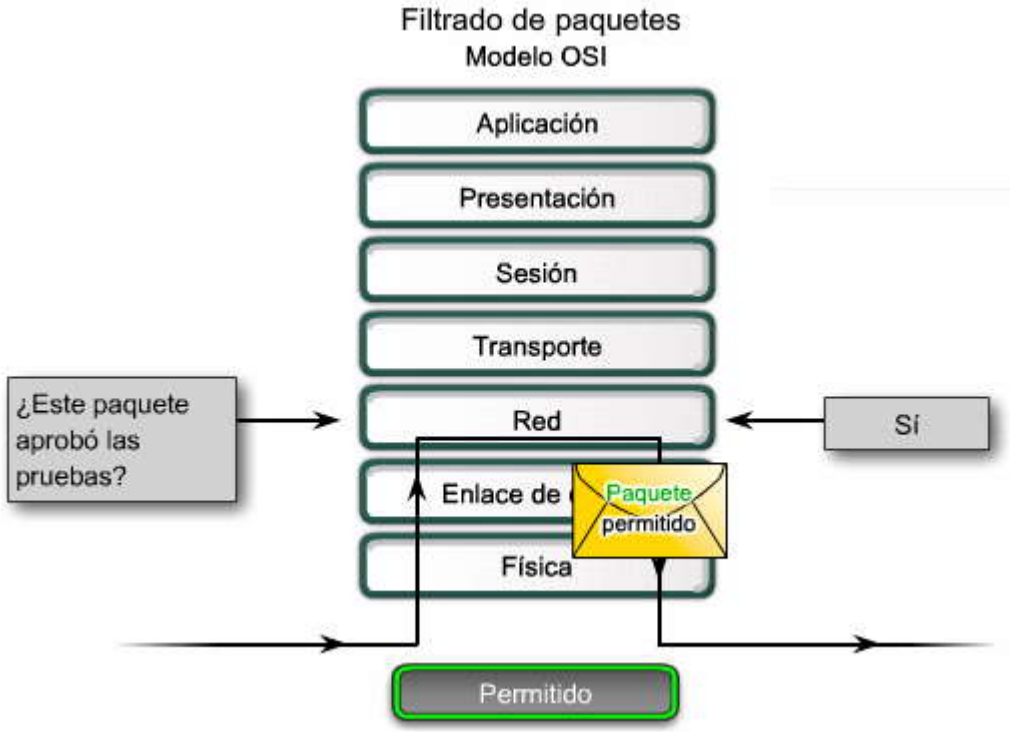
Recuerde que una ACL es una lista secuencial de sentencias de permiso o denegación que se aplican a direcciones IP o protocolos de capa superior. La ACL puede extraer la siguiente información del encabezado del paquete, probarla respecto de las reglas y decidir si "permitir" o "denegar" el ingreso según los siguientes criterios:

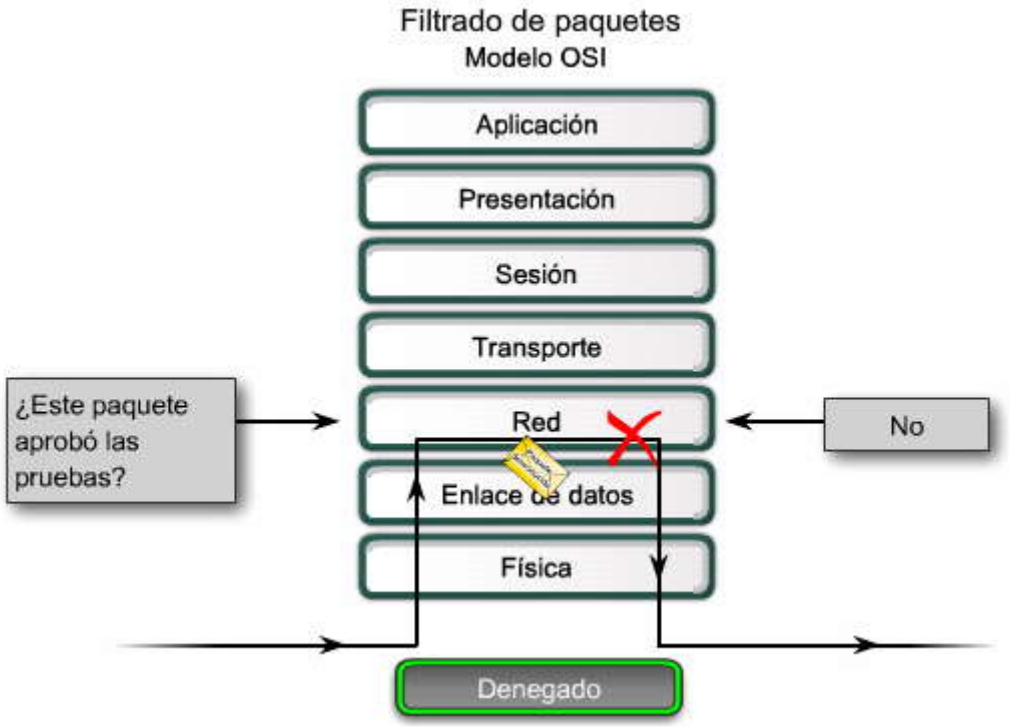
- Dirección IP de origen
- Dirección IP de destino
- Tipo de mensaje ICMP

La ACL también puede extraer información de las capas superiores y probarla respecto de las reglas. La información de las capas superiores incluye:

- Puerto TCP/UDP de origen
- Puerto TCP/UDP de destino

Haga clic en los botones de la figura para obtener un panorama general sobre la manera en la que una ACL permite o deniega el paquete. Si bien las animaciones muestran el filtrado de paquetes en la Capa 3, debe aclararse que el filtrado puede tomar lugar también en la Capa 4.





Ejemplo de filtrado de paquetes

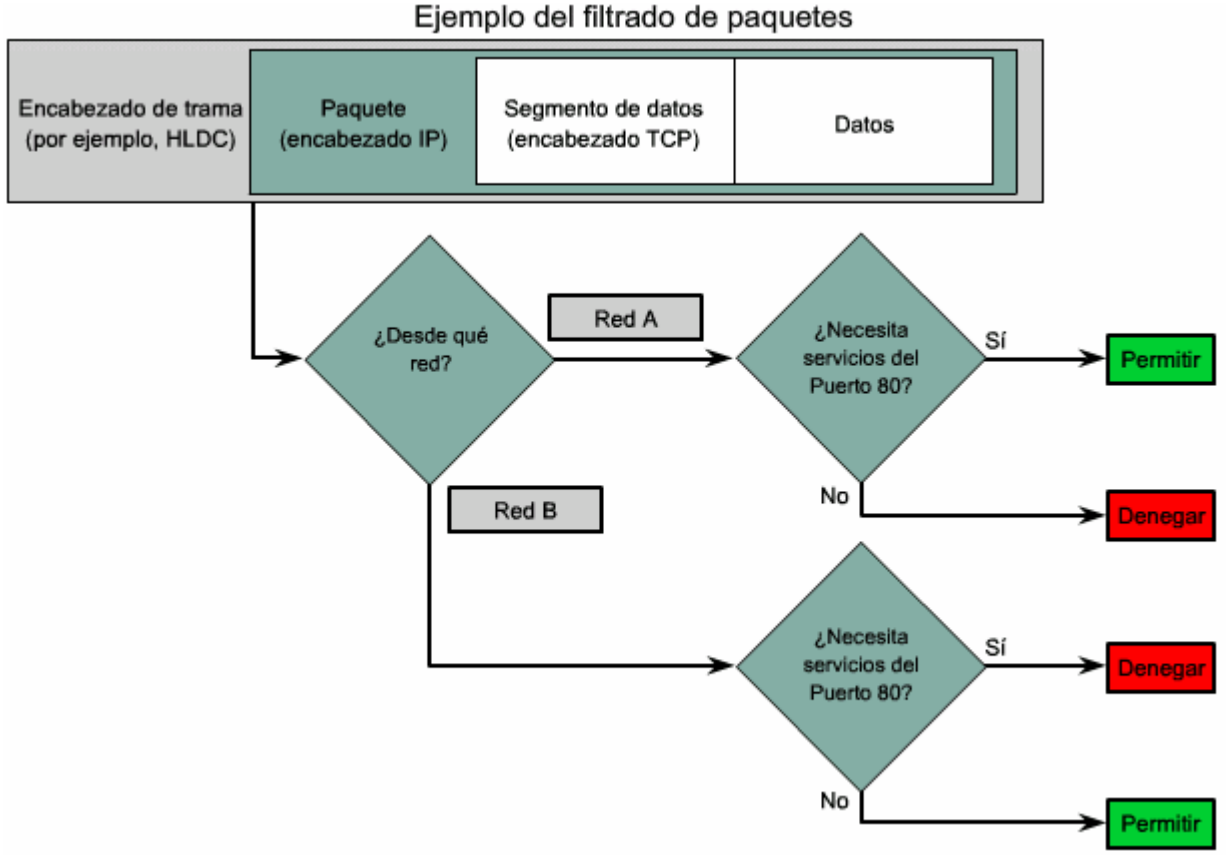
Para comprender el concepto de cómo el router utiliza el filtrado de paquetes, imagine a un guardia ubicado delante de una puerta cerrada. Las instrucciones del guardia son permitir el ingreso sólo a las personas que aparezcan en una lista. El guardia filtra las personas según el criterio de la lista de nombres autorizados.

Por ejemplo, puede decir: "Sólo permitir el acceso Web a usuarios de la red A. Denegar el acceso Web a usuario de la red B, pero permitirles los otros accesos". Consulte la figura a fin de analizar la ruta de decisión que utiliza el filtro de paquetes para realizar esta tarea.

Para esta situación, el filtro de paquetes observa cada paquete de la siguiente manera:

- Si el paquete tiene el señalizador TCP SYN de la red A y utiliza el puerto 80, está autorizado a ingresar. Se deniega todo otro acceso a esos usuarios.
- Si el paquete tiene el señalizador TCP SYN de la red B y utiliza el puerto 80, no puede ingresar. Sin embargo, se le permiten todos los demás accesos.

Éste es sólo un ejemplo. El usuario puede configurar varias reglas para luego permitir o denegar otros servicios a determinados usuarios. También puede filtrar paquetes a nivel de puerto con una ACL extendida, que se incluye en la Sección 3.



5.1.3 ¿Qué es una ACL?

La ACL es una configuración de router que controla si un router permite o deniega paquetes según el criterio encontrado en el encabezado del paquete. Las ACL son unos de los objetos más comúnmente utilizados en el software IOS de Cisco. Las ACL también se utilizan para seleccionar los tipos de tráfico por analizar, reenviar o procesar de otras maneras.

Como cada paquete llega a través de una interfaz con una ACL asociada, la ACL se revisa de arriba a abajo, una línea a la vez, y se busca un patrón que coincida con el paquete entrante. La ACL hace cumplir una o más políticas de seguridad corporativas al aplicar una regla de permiso o denegación para determinar el destino del paquete. Es posible configurar las ACL para controlar el acceso a una red o subred.

De manera predeterminada, un router no tiene ninguna ACL configurada y, por lo tanto, no filtra el tráfico. El tráfico que ingresa al router es enrutado según la tabla de enrutamiento. Si no utiliza una ACL en el router, todos los paquetes que pueden enrutarse a través del router lo atraviesan hacia el próximo segmento de la red.

A continuación, le presentamos pautas para el uso de las ACL:

- Utilice las ACL en routers firewall entre su red interna y su red externa, como Internet.
- Utilice las ACL en un router situado entre dos partes de la red a fin de controlar el tráfico que entra o sale de una parte específica de su red interna.
- Configure las ACL en routers de borde situados en los extremos de la red. Esto proporciona un búfer muy básico desde la red externa, o entre un área menos controlada y un área más sensible de su red.
- Configure las ACL para cada protocolo de red configurado en las interfaces del router de borde. Puede configurar las ACL en una interfaz para filtrar el tráfico entrante, saliente o ambos.

Haga clic en el botón Las ACL en un router que muestra la figura.

Las tres P

Puede recordar una regla general para aplicar las ACL en un router mediante las tres P. Puede configurar una ACL por protocolo, por dirección y por interfaz.

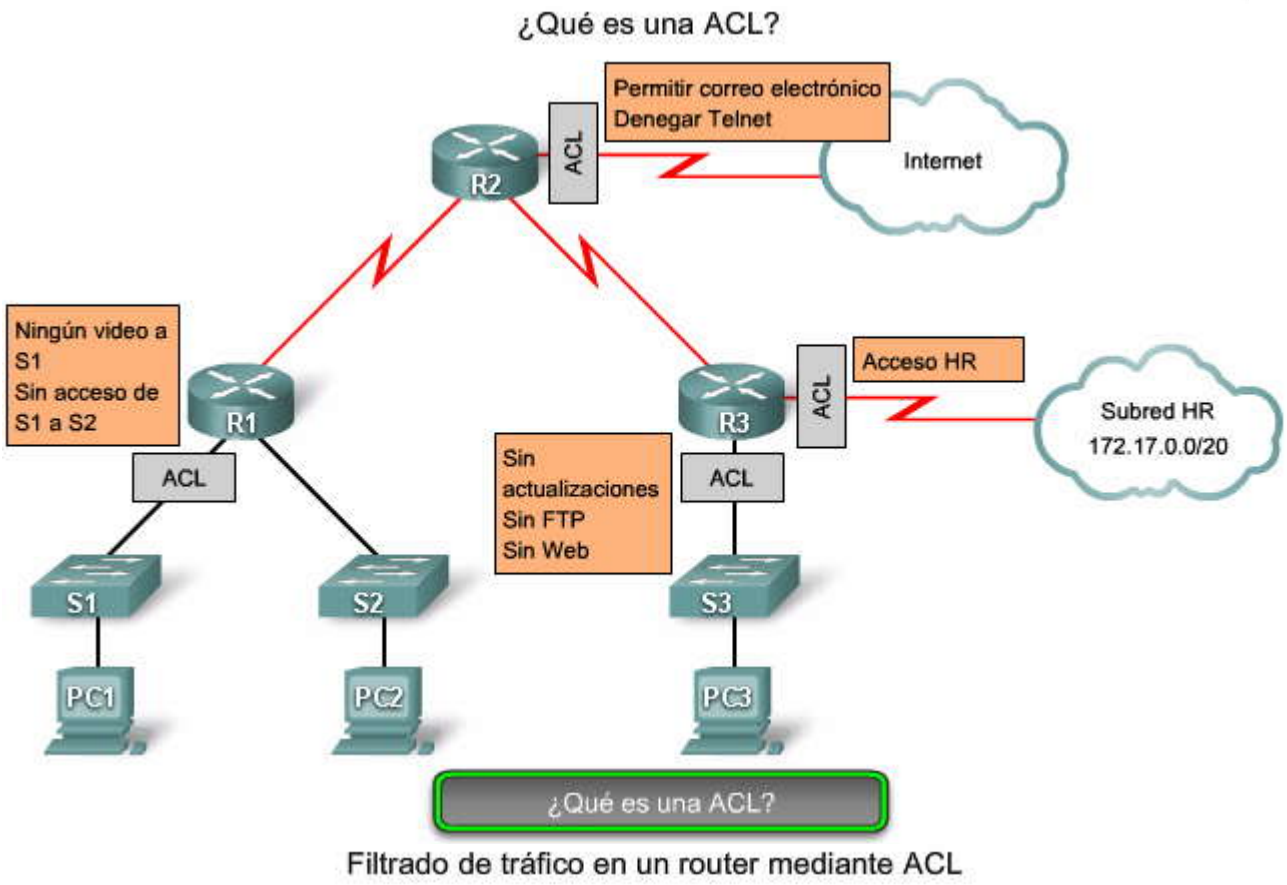
- **Una ACL por protocolo**: para controlar el flujo de tráfico de una interfaz, se debe definir una ACL para cada protocolo habilitado en la interfaz.
- **Una ACL por dirección**: las ACL controlan el tráfico en una dirección a la vez de una interfaz. Deben crearse dos ACL por separado para controlar el tráfico entrante y saliente.
- **Una ACL por interfaz**: las ACL controlan el tráfico para una interfaz, por ejemplo, Fast Ethernet 0/0.

Escribir una ACL puede ser una tarea desafiante y compleja. Cada interfaz puede tener varios protocolos y direcciones definidos. El router del ejemplo tiene dos interfaces configuradas para IP: AppleTalk e IPX. Es probable que este router necesite 12 ACL por separado, una ACL para cada protocolo, multiplicada por dos por cada dirección y por dos por la cantidad de puertos.

Las ACL realizan las siguientes tareas:

- Limitar el tráfico de red para mejorar el rendimiento de ésta. Por ejemplo, si la política corporativa no permite el tráfico de video en la red, pueden configurarse y aplicarse las ACL que bloquean el tráfico de video. Esto reduce considerablemente la carga de la red y aumenta su rendimiento.
- Brindar control de flujo de tráfico. Las ACL pueden restringir el envío de las actualizaciones de enrutamiento. Si no se necesitan actualizaciones debido a las condiciones de la red, se preserva el ancho de banda.
- Proporcionar un nivel básico de seguridad para el acceso a la red. Las ACL pueden permitir que un host acceda a una parte de la red y evitar que otro acceda a la misma área. Por ejemplo, el acceso a la red de Recursos Humanos puede restringirse a determinados usuarios.
- Se debe decidir qué tipos de tráfico enviar o bloquear en las interfaces del router. Por ejemplo, una ACL puede permitir el tráfico de correo electrónico, pero bloquear todo el tráfico de Telnet.
- Controlar las áreas de la red a las que puede acceder un cliente.
- Analizar los hosts para permitir o denegar su acceso a los servicios de red. Las ACL pueden permitir o denegar el acceso de un usuario a tipos de archivos, como FTP o HTTP.

Las ACL inspeccionan los paquetes de la red según un criterio, como dirección de origen, de destino, protocolos y números de puerto. Además de permitir o denegar el tráfico, una ACL puede clasificar el tráfico para darle prioridad en la línea. Esta capacidad es similar a tener un pase VIP para un concierto o evento deportivo. El pase VIP le da a determinados invitados privilegios que no se ofrecen al público en general, como el ingreso a áreas restringidas y asientos en el palco.



Filtrado de tráfico en un router mediante ACL

Con dos interfaces y tres protocolos en ejecución, este router puede tener una cantidad total de 12 ACL distintas aplicadas.

Las tres P para utilizar ACL

Sólo puede tener una ACL por protocolo, por interfaz y por dirección:

- Una ACL por protocolo (por ejemplo, IP o IPX)
- Una ACL por interfaz (por ejemplo, FastEthernet0/0)
- Una ACL por dirección (es decir, ENTRADA o SALIDA)

Las ACL en un router

5.1.4 Funcionamiento de las ACL

Cómo funcionan las ACL

Las listas de acceso definen el conjunto de reglas que proporcionan control adicional para los paquetes que ingresan a las interfaces de entrada, paquetes que pasan a través del router y paquetes que salen de las interfaces de salida del router. Las ACL no actúan sobre paquetes que se originan en el mismo router.

Las ACL se configuran para ser aplicadas al tráfico entrante o saliente.

- **ACL de entrada**: los paquetes entrantes se procesan antes de ser enrutados a la interfaz de salida. Una ACL de entrada es eficaz porque guarda la carga de búsquedas de enrutamiento si el paquete se descarta. Si el paquete está autorizado por las pruebas, luego se procesa para el enrutamiento.
- **ACL de salida**: los paquetes entrantes se enrutan a la interfaz de salida y luego son procesados a través de la ACL de salida.

Las sentencias de la ACL operan en orden secuencial. Comparan los paquetes con la ACL, de arriba hacia abajo, una sentencia a la vez.

La figura muestra la lógica para una ACL de entrada. Si coinciden un encabezado de paquete y una sentencia de ACL, se omite el resto de las sentencias de la lista y el paquete tiene permitido pasar o no, según la sentencia coincidente. Si el encabezado del paquete no coincide con una sentencia de ACL, el paquete se prueba según la siguiente sentencia de la lista. Este proceso de coincidencia continúa hasta el final de la lista.

Una sentencia implícita final cubre todos los paquetes para los cuales las condiciones no resultan verdaderas. Esta última prueba coincide con todos los demás paquetes y produce una "denegación" del paquete. En lugar de salir o entrar a una interfaz, el router descarta todos los paquetes restantes. La última sentencia generalmente se denomina "implicit deny any statement" (denegar implícitamente una sentencia) o "deny all traffic" (denegar todo el tráfico). Debido a esta sentencia, una ACL debe contar con, al menos, una sentencia de permiso; de lo contrario, la ACL bloquea todo el tráfico.

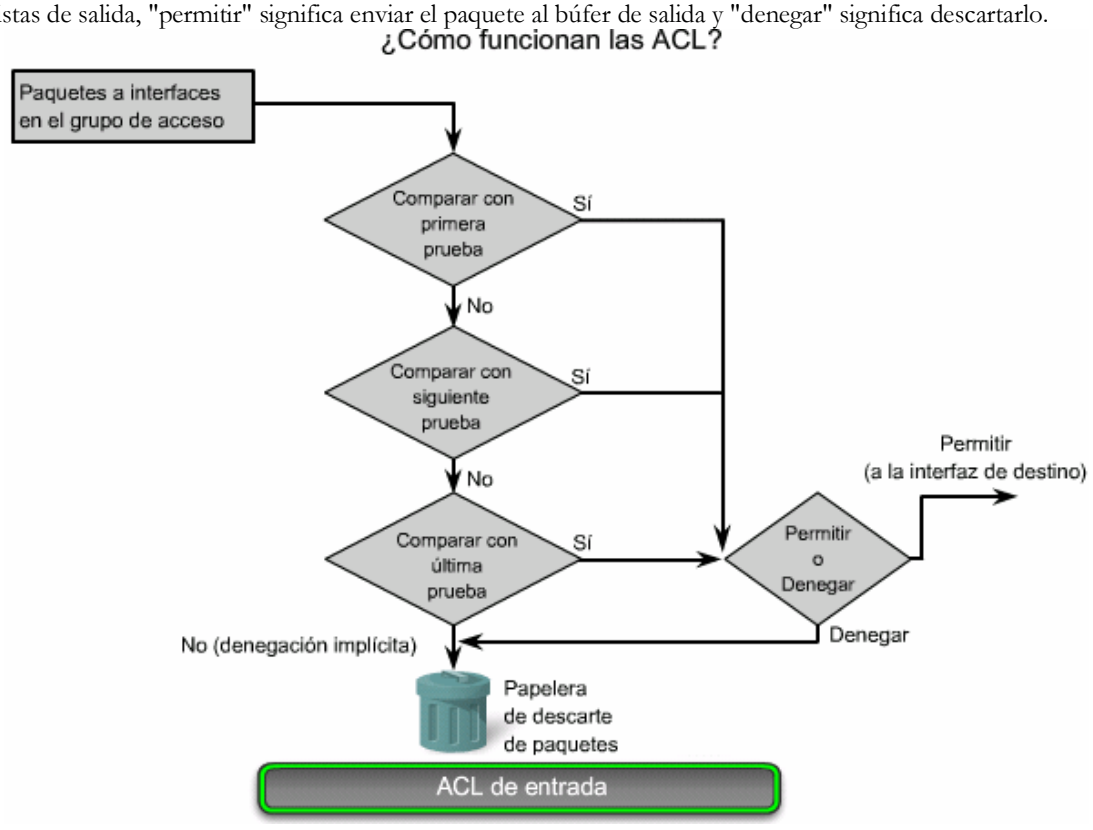
Puede aplicar una ACL a varias interfaces. Sin embargo, sólo puede haber una ACL por protocolo, por dirección y por interfaz.

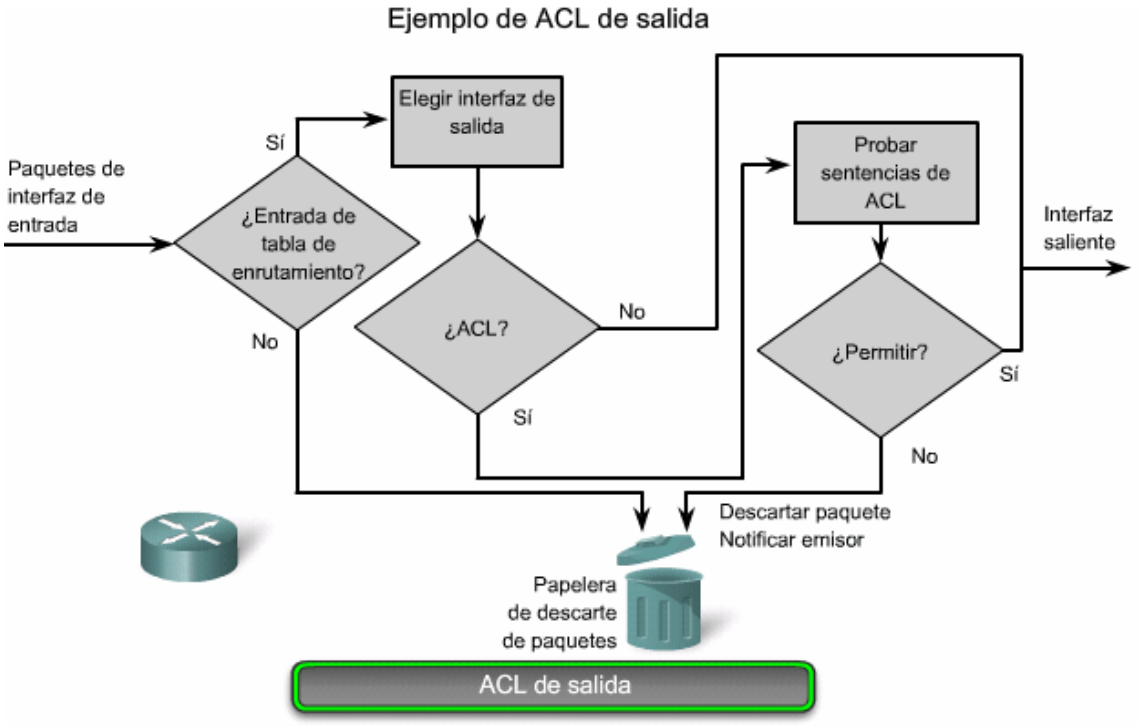
Haga clic en el botón ACL de salida que se muestra en la figura.

La figura muestra la lógica para una ACL de salida. Antes de reenviar un paquete a una interfaz de salida, el router verifica la tabla de enrutamiento para ver si el paquete es enrutable. Si no lo es, se descarta. A continuación, el router verifica si la interfaz de salida se agrupa a una ACL. Si la interfaz de salida no se agrupa a una ACL, el paquete puede enviarse al búfer de salida. Algunos ejemplos del funcionamiento de las ACL de salida son los siguientes.

- Si la interfaz de salida no se agrupa a una ACL de salida, el paquete se envía directamente a la interfaz de salida.
- Si la interfaz de salida se agrupa a una ACL de salida, el paquete no se envía a una interfaz de salida hasta probarlo según la combinación de sentencias de ACL asociadas a la interfaz. De acuerdo con el resultado de las pruebas realizadas por la ACL, el paquete se puede permitir o denegar.

Para las listas de salida, "permitir" significa enviar el paquete al búfer de salida y "denegar" significa descartarlo.





Las ACL y el enrutamiento, y los procesos de las ACL en un router

La figura muestra la lógica de enrutamiento y los procesos de las ACL en un router. Cuando un paquete llega a la interfaz del router, el proceso del router es el mismo se utilicen o no las ACL. A medida que una trama ingresa a una interfaz, el router verifica si la dirección de destino de Capa 2 concuerda con la propia o si es una trama de broadcast.

Si se acepta la dirección de la trama, la información de la trama se elimina y el router busca una ACL en la interfaz de entrada. Si existe una ACL, entonces se verifica si el paquete cumple o no las condiciones de la lista.

Si el paquete coincide con la sentencia, se acepta o se rechaza. Si se acepta el paquete en la interfaz, se lo compara con las entradas de la tabla de enrutamiento para determinar la interfaz destino y conmutarlo a aquella interfaz.

A continuación, el router verifica si la interfaz de destino tiene una ACL. Si existe una ACL, entonces se verifica si el paquete cumple o no las condiciones de la lista.

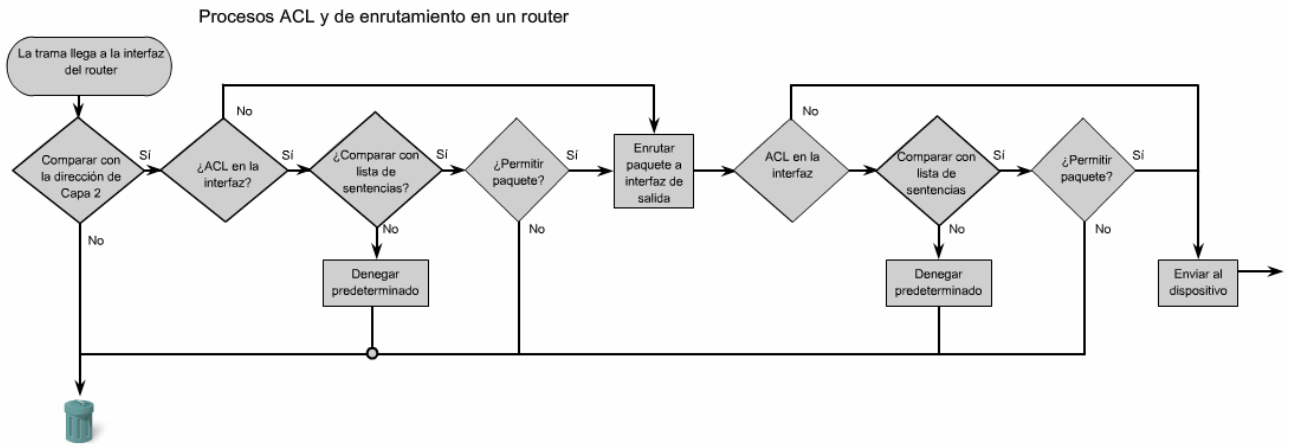
Si el paquete coincide con la sentencia, se acepta o se rechaza.

Si no hay ACL o se acepta el paquete, el paquete se encapsula en el nuevo protocolo de Capa 2 y se envía por la interfaz hacia el dispositivo siguiente.

La sentencia de criterios implícita "Deny All Traffic" (Denegar todo el tráfico)

Al final de cada lista de acceso, se encuentra la sentencia de criterios implícita "deny all traffic". Algunas veces se denomina "implicit deny any" (denegar implícitamente todo el tráfico). Por lo tanto, si un paquete no coincide con ninguna de las entradas de la ACL, se bloquea automáticamente. La sentencia implícita "deny all traffic" (denegar todo el tráfico) es el comportamiento predeterminado de las ACL y no puede modificarse.

Hay una advertencia clave relacionada con el comportamiento "deny all" (denegar todo): para la mayoría de los protocolos, si define una lista de acceso de entrada para el filtrado del tráfico, debe incluir sentencias de criterios de lista de acceso explícitas, a fin de permitir las actualizaciones de enrutamiento. Si no lo hace, puede, de hecho, perder la comunicación desde la interfaz cuando la sentencia implícita "deny all traffic" (denegar todo el tráfico) bloquea las actualizaciones de enrutamiento al final de la lista de acceso.



5.1.5 Tipos de ACL de Cisco

Hay dos tipos de ACL Cisco: estándar y extendidas.

ACL estándar

Las ACL estándar le permiten autorizar o denegar el tráfico desde las direcciones IP de origen. No importan el destino del paquete ni los puertos involucrados. El ejemplo permite todo el tráfico desde la red 192.168.30.0/24. Debido a la sentencia implícita "deny any" (denegar todo) al final, todo el otro tráfico se bloquea con esta ACL. Las ACL estándar se crean en el modo de configuración global.

Haga clic en el botón ACL extendidas que se muestra en la figura.

ACL extendidas

Las ACL extendidas filtran los paquetes IP en función de varios atributos, por ejemplo: tipo de protocolo, direcciones IP de origen, direcciones IP de destino, puertos TCP o UDP de origen, puertos TCP o UDP de destino e información opcional de tipo de protocolo para una mejor disparidad de control. En la figura, la ACL 103 permite el tráfico que se origina desde cualquier dirección en la red 192.168.30.0/24 hacia cualquier puerto 80 de host de destino (HTTP). Las ACL extendidas se crean en el modo de configuración global.

Los comandos para las ACL se explican en los próximos temas.

Tipos de ACL de Cisco

Las ACL estándar filtran paquetes IP solamente según la dirección de origen.

```
access-list 10 permit 192.168.30.0 0.0.0.255
```

Las ACL extendidas filtran paquetes IP según diferentes atributos, entre ellos los siguientes:

- Direcciones IP de origen y de destino
- Puertos TCP y UDP de origen y de destino
- Tipo de protocolo (IP, ICMP, UDP, TCP o número de protocolo)

```
access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
```

5.1.6 ¿Cómo funciona una ACL estándar?

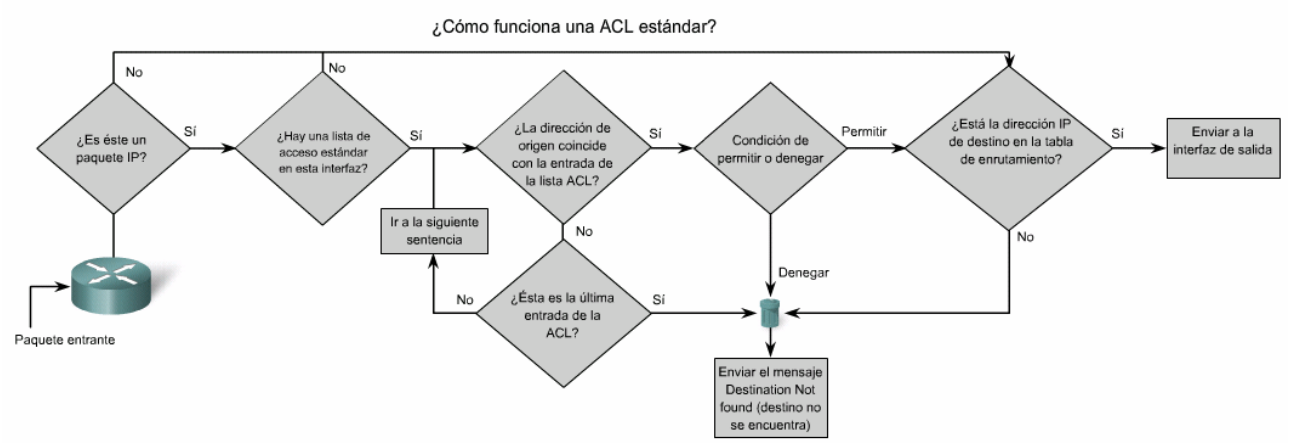
La ACL estándar es una colección secuencial de condiciones de permiso o denegación que aplican a las direcciones IP. No se incluyen el destino del paquete ni los puertos involucrados.

En la figura, aparece el proceso de decisión. El software IOS de Cisco prueba las direcciones una a una con las condiciones. La primera coincidencia determina si el software acepta o rechaza la dirección. El orden de las condiciones es muy importante, ya que el software detiene las condiciones de prueba luego de la primera coincidencia. Si no coinciden ningunas de las condiciones, se rechaza la dirección.

Las dos tareas principales involucradas al utilizar las ACL son:

Paso 1. Crear una lista de acceso que especifique un número o nombre de lista de acceso y las condiciones de acceso.

Paso 2. Aplicar la ACL a las interfaces o líneas de terminal.

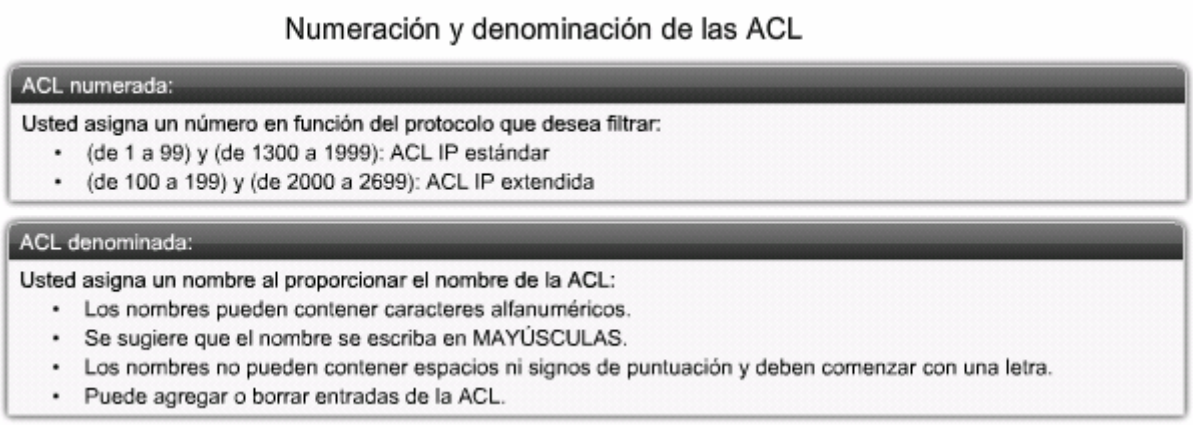


5.1.7 Numeración y denominación de las ACL

Utilizar ACL numeradas es un método eficaz para determinar el tipo de ACL en redes más pequeñas con más tráfico definido de manera homogénea. Sin embargo, un número no le informa el propósito de la ACL. Por ello, si se parte del IOS de Cisco Versión 11.2, puede utilizar un nombre para identificar una ACL de Cisco.

La figura resume la regla para especificar las ACL numeradas y las ACL denominadas.

En cuanto a las ACL, si se pregunta por qué se saltean los números del 200 al1299, la respuesta es porque esos números son utilizados por otros protocolos. Este curso se centra sólo en las ACL IP. Por ejemplo, los números del 600 al 699 son utilizados por AppleTalk y los números del 800 al 899 por IPX.



5.1.8 Dónde ubicar las ACL

La ubicación adecuada de las ACL para filtrar el tráfico no deseado proporciona un funcionamiento más eficiente de la red. Las ACL pueden actuar como firewalls para filtrar paquetes y eliminar el tráfico no deseado. El lugar donde ubique las ACL puede reducir el tráfico innecesario. Por ejemplo, el tráfico que se deniega en un destino remoto no debe usar los recursos de la red en el camino hacia ese destino.

Todas las ACL deben ubicarse donde más repercutan sobre la eficacia. Las reglas básicas son:

- Ubicar las ACL extendidas lo más cerca posible del origen del tráfico denegado. De esta manera, el tráfico no deseado se filtra sin atravesar la infraestructura de red.
- Como las ACL estándar no especifican las direcciones de destino, colóquelas lo más cerca del destino posible.

Consideremos un ejemplo de dónde colocar las ACL en nuestra red. La ubicación de la interfaz y la red depende de lo que desee que realice la ACL.

En la figura, el administrador desea que el tráfico que se origina en la red 192.168.10.0/24 no ingrese a la red 192.168.30.0/24. Una ACL en la interfaz de salida de R1 deniega a R1 la posibilidad de enviar tráfico a otros lugares. La solución es colocar una ACL estándar en la interfaz de entrada de R3 para detener todo el tráfico desde la dirección de origen 192.168.10.0/24. Una ACL estándar cumple con los requerimientos porque sólo se centra en las direcciones IP de origen.

Haga clic en el botón ACL extendida que se muestra en la figura.

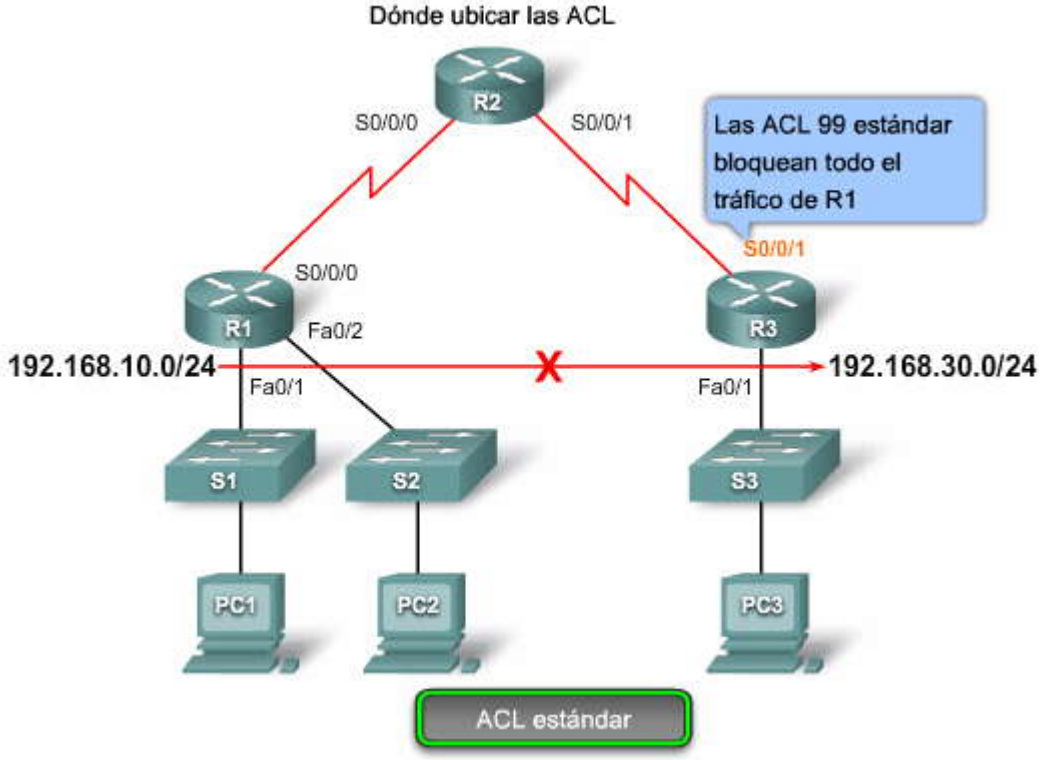
Considere que los administradores sólo pueden colocar las ACL en los dispositivos que ellos controlan. Por lo tanto, su ubicación debe determinarse según la extensión del control del administrador de red. En esta figura, el administrador de las redes 192.168.10.0/24 y 192.168.11.0/24 (designadas en este ejemplo Diez y Once, respectivamente) desea denegar el tráfico Telnet y FTP desde Once a la red 192.168.30.0/24 (Treinta en este ejemplo). Al mismo tiempo, se debe permitir todo el tráfico restante desde Diez.

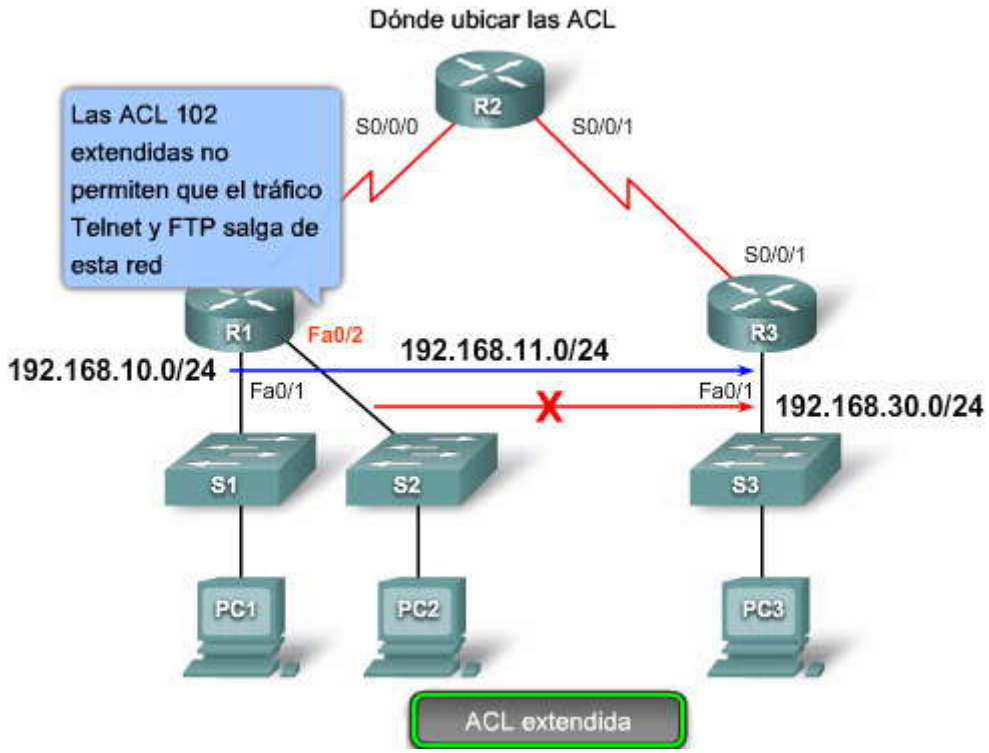
Hay varias maneras de realizar esta tarea. Una ACL extendida en R3 que bloquea el tráfico Telnet y FTP desde Once podría realizar la tarea, pero el administrador no controla R3. Esa solución sigue permitiendo, además, que el tráfico no deseado atraviese toda la red, sólo para bloquearlo en el destino. Esto afecta la eficacia general de la red.

Una solución es utilizar una ACL extendida de salida que especifique las direcciones de origen y de destino (Diez y Treinta respectivamente), y diga "El tráfico Telnet y FTP desde Diez no puede llegar hasta Treinta." Coloque esta ACL extendida en el puerto de salida S0/0/0 de R1.

Una desventaja de esta solución es que el tráfico desde Once también está sujeto a cierto procesamiento de la ACL, incluso si se permite el tráfico Telnet y FTP.

La mejor solución es acercarse al origen y colocar una ACL extendida en la interfaz de entrada Fa0/2 de R1. Esto garantiza que los paquetes desde Diez no ingresen a R1 y que luego no puedan atravesar hacia Once ni incluso ingresar a R2 o R3. Aún se permite el tráfico con otras direcciones y puertos de destino hacia R1.





5.1.9 Pautas generales para la creación de las ACL

Mejores prácticas de las ACL

Utilizar las ACL requiere atención al detalle y un gran cuidado. Los errores pueden ser costosos en lo que respecta a tiempo de inactividad, tareas de resolución de problemas y un servicio de red deficiente. Antes de comenzar a configurar una ACL, se requiere una planificación básica. La figura presenta pautas que conforman la base de la lista de mejores prácticas de una ACL.

Mejores prácticas de las ACL

Pautas	Beneficios
Fundamente sus ACL según las políticas de seguridad de la organización.	Esto asegurará la implementación de las pautas de seguridad de la organización.
Prepare una descripción de lo que desea que realicen las ACL.	Esto lo ayudará a evitar posibles problemas de acceso generados de manera inadvertida.
Utilice un editor de textos para crear, editar y guardar las ACL.	Esto lo ayudará a crear una biblioteca de ACL reutilizables.
Pruebe sus ACL en una red de desarrollo antes de implementarlas en una red de producción.	Esto lo ayudará a evitar errores costosos.

Funcionamiento de las ACL

Una lista de control de acceso (ACL, Access Control List) es un guión de configuración de router que controla si un router _____ o _____ paquetes según el criterio descrito en el encabezado del paquete.	✓ permit ✓ deny
Las ACL generalmente se utilizan en routers _____ ubicados entre su red interna y su red externa.	✓ firewall
Un router con tres interfaces activas y dos protocolos de red (IP y IPX) puede tener tantas ACL _____ activas como necesite.	✓ doce
Para las ACL de entrada, los paquetes entrantes se procesan _____ son enrutados a una interfaz de salida.	✓ antes
Para las ACL de salida, los paquetes entrantes se procesan _____ son enrutados a una interfaz de salida.	✓ después
Al final de cada lista de acceso se encuentra una sentencia de criterios implícita _____ todo el tráfico. Por eso, si un paquete no coincide con ninguna de las sentencias de criterios, el paquete será _____	✓ deny ✓ bloqueado

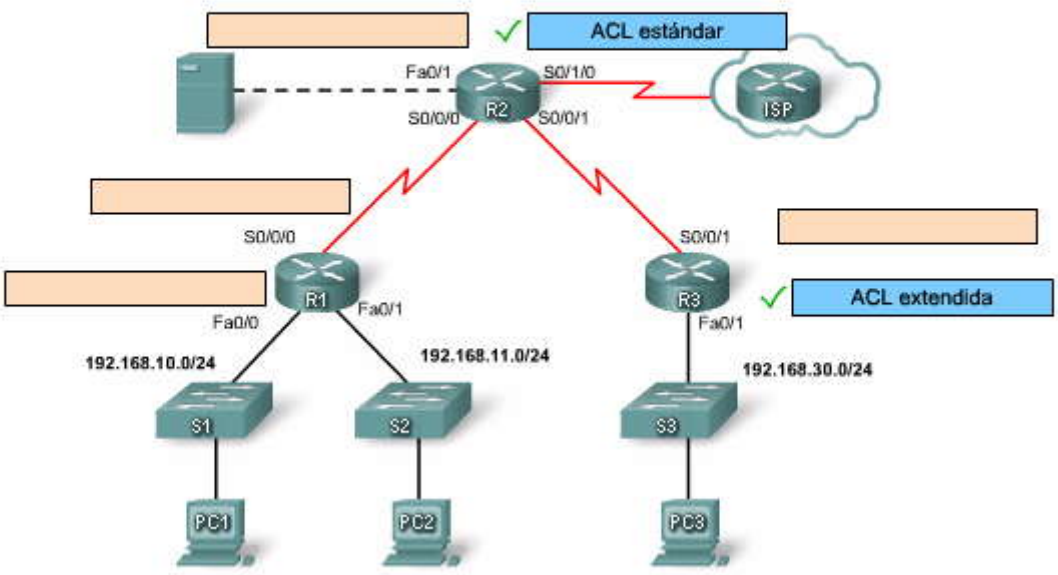
ACL estándar y extendidas

	Estándar	Extendida
Puede filtrar tráfico según la dirección IP de origen	✓	✓
Puede filtrar tráfico según la dirección IP de destino		✓
Puede filtrar tráfico según el tipo de protocolo		✓
Utiliza los números del 1 al 99	✓	
Utiliza los números del 100 al 199		✓
Utiliza los números del 1300 al 1999	✓	
Puede utilizar un nombre en lugar de un número	✓	✓

Colocación de las ACL

Política de red No. 1: Utilice una ACL estándar para que la red 192.168.10.0/24 no acceda a Internet a través de un ISP.

Política de red No. 2: Utilice una ACL extendida para que la red 192.168.30.0/24 no acceda al servidor Web/TFTP.



5.2 Configuración de las ACL estándar

5.2.1 Cómo ingresar sentencias de criterios

Antes de comenzar a configurar una ACL estándar, revisaremos conceptos importantes sobre las ACL que abarcamos en la Sección 1.

Recuerde que cuando el tráfico ingresa al router, se lo compara con las sentencias de ACL en función del orden de las entradas en el router. El router continúa procesando las sentencias de ACL hasta lograr una coincidencia. Por ello, debe colocar la ACL más utilizada al principio de la lista. Si no se encuentran coincidencias cuando el router llega al final de la lista, el tráfico es denegado porque las ACL tienen una sentencia de denegación implícita para todo el tráfico que no cumple con los criterios de prueba. Una ACL de una única entrada con sólo una entrada de denegación llega a denegar todo el tráfico. Debe tener al menos una sentencia de permiso en una ACL o se bloquea todo el tráfico.

Por ejemplo, las dos ACL (101 y 102) de la figura tienen el mismo efecto. La red 192.168.10.0 puede acceder a la red 192.168.30 mientras que 192.168.11.0 no puede.

ACL 101

```
access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
```

ACL 102

```
access-list 102 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 102 deny ip any any
```

5.2.2 Configuración de las ACL estándar

Lógica de las ACL estándar

En la figura, se revisan las direcciones de origen de los paquetes que ingresan a Fa0/0:

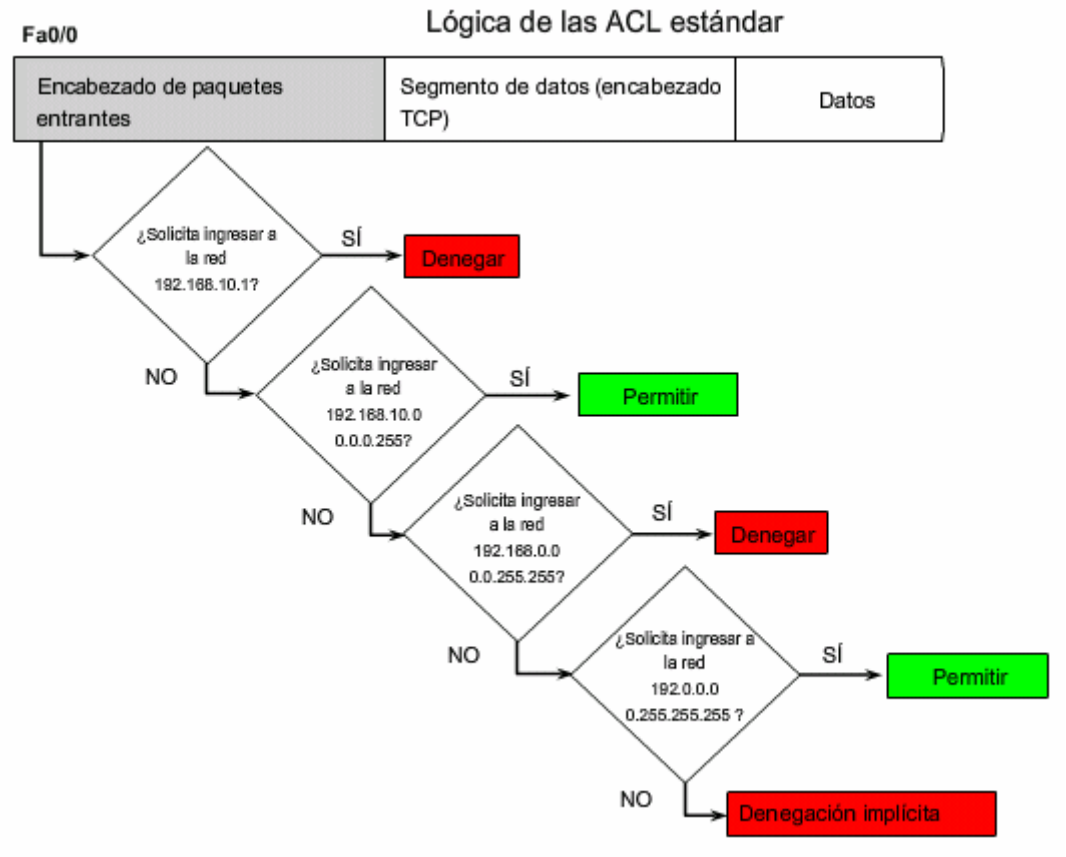
access-list 2 deny 192.168.10.1

access-list 2 permit 192.168.10.0 0.0.0.255

access-list 2 deny 192.168.0.0 0.0.255.255

access-list 2 permit 192.0.0.0 0.255.255.255

Si los paquetes tienen permiso, se enrutan a través del router hacia una interfaz de salida. Si se les niega d permiso, se los descarta en la interfaz de entrada.



Configuración de las ACL estándar

Para configurar las ACL estándar numeradas en un router Cisco, primero debe crear la ACL estándar y, luego, activarla en una interfaz.

El comando de configuración global **access-list** define una ACL estándar con un número entre 1 y 99. El software IOS de Cisco Versión 12.0.1 extendió el rango y permite desde 1300 a 1999 para brindar un máximo de 798 ACL estándar posibles. Estos números adicionales son denominados ACL IP expandidos.

La sintaxis completa del comando ACL estándar es:

Router(config)#**access-list** *número-de-lista-de-acceso* **deny permit remark** *origen* [*wildcard origen*] [**log**]

La figura muestra una explicación detallada de la sintaxis para una ACL estándar.

Por ejemplo, para crear una ACL numerada nombrada **10** que permita la red 192.168.10.0 /24, debe ingresar:

R1(config)# **access-list 10 permit 192.168.10.0**

Haga clic en el botón Eliminar ACL que se muestra en la figura.

La forma **no** de este comando elimina la ACL estándar. En la figura, el resultado del comando **show access-list** muestra las ACL actuales configuradas en el router R1.

Para eliminar la ACL, se utiliza el comando de configuración global **no access-list**. La ejecución del comando **show access-list** confirma que la lista de acceso 10 ha sido eliminada.

Haga clic en el botón Observaciones que se muestra en la figura.

Por lo general, los administradores crean las ACL y comprenden plenamente el propósito de cada sentencia dentro de la ACL. Sin embargo, cuando se vuelve a revisar una ACL más adelante, puede no ser tan evidente como antes.

La palabra clave **remark** se utiliza para la documentación y facilita considerablemente la comprensión de las listas de acceso. Cada observación está limitada a 100 caracteres. Si bien es bastante simple, la ACL de la figura se utiliza como ejemplo. Al revisar la ACL en la configuración, se muestra también la observación.

El siguiente tema explica cómo utilizar la máscara wildcard para identificar redes y hosts específicos.

Sintaxis de comando de la ACL estándar `lista-de-acceso`

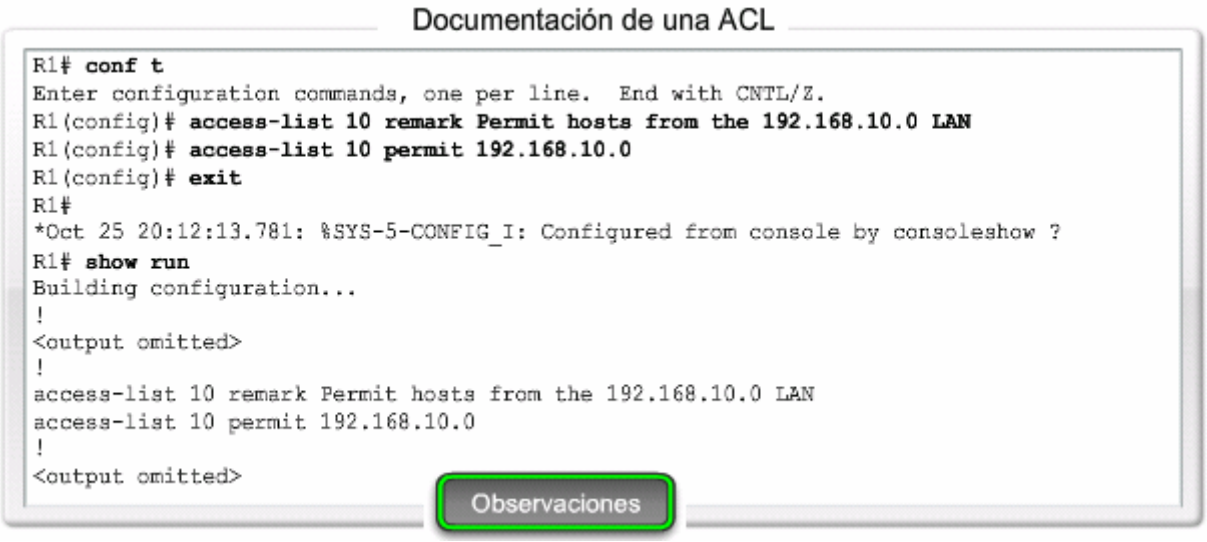
Parámetro	Descripción
número-de-lista-de-acceso	Número de una ACL. Es un número decimal del 1 al 99 o del 1300 al 1999 (para las ACL estándar).
deny	Deniega el acceso si las condiciones concuerdan.
permit	Permite el acceso si las condiciones concuerdan.
remark	Agregue un comentario sobre las entradas en la lista de acceso IP para facilitar la comprensión y el análisis de la lista.
origen	Número de la red o del host desde el que se envía el paquete. Hay dos maneras de especificar el *origen*: • Utilice una cantidad de 32 bits en formato decimal punteado de cuatro partes. • Utilice la palabra clave **any** como abreviatura para un *origen* y la *wildcard de origen* de 0.0.0.0 255.255.255.55.
wildcard origen	(Opcional) Los bits wildcard para aplicar al origen. Hay dos formas de especificar la wildcard de origen: • Utilice una cantidad de 32 bits en formato decimal punteado de cuatro partes. Coloque los unos en las posiciones de bits que desea ignorar. • Utilice la palabra clave **any** como abreviatura para un *origen* y una *wildcard de origen* de 0.0.0.0 255.255.255.55.
log	(Opcional) Genera un mensaje de registro informativo en la consola acerca del paquete que coincide con la entrada. (El nivel de mensajes generados en la consola se controla con el comando **logging console**.) El mensaje incluye el número de ACL, si el paquete está permitido o denegado, la dirección de origen y la cantidad de paquetes. El mensaje se genera para el primer paquete que coincida y, luego, a intervalos de cinco minutos, incluida la cantidad de paquetes permitidos o denegados en el intervalo de cinco minutos anterior.

Sintaxis de las ACL estándar

Eliminación de una ACL

```
R1# show access-list
Standard IP access list 10
    10 permit 192.168.10.0
R1#
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# no access-list 10
R1(config)# exit
R1#
*Oct 25 19:59:41.142: %SYS-5-CONFIG_I: Configured from console by console
R1# show access-list

R1#
```

Eliminar ACL



5.2.3 Máscara wildcard de las ACL

Máscaras wildcard

Las sentencias de las ACL incluyen máscaras, también denominadas máscaras wildcard. Una máscara wildcard es una secuencia de dígitos binarios que le indican al router qué partes del número de subred observar. Aunque las máscaras wildcard no tienen una relación funcional con las máscaras de subred, sí proporcionan una función similar. La máscara determina qué parte de la dirección IP de origen y destino aplicar a la concordancia de direcciones. Los números 1 y 0 de la máscara identifican cómo considerar los bits de direcciones IP correspondientes. Sin embargo, se utilizan con distintos propósitos y siguen distintas reglas.

Las máscaras wildcard y máscaras de subred tienen una longitud de 32 bits y utilizan unos (1) y ceros (0) binarios. Las máscaras de subred utilizan unos y ceros binarios para identificar la red, subred y porción de host de una dirección IP. Las máscaras wildcard utilizan unos y ceros binarios para filtrar direcciones IP individuales o en grupo para permitir o denegar el acceso a recursos según la dirección IP. Al configurar cuidadosamente las máscaras wildcard, puede permitir o denegar una o varias direcciones IP.

Las máscaras wildcard y máscaras de subred difieren en la forma en la que concuerdan sus unos y ceros binarios. Las máscaras wildcard utilizan las siguientes reglas para hacer coincidir sus unos y ceros binarios.

- Bit 0 de máscara wildcard: hacer coincidir el valor de bits correspondiente de la dirección
- Bit 1 de máscara wildcard: ignorar el valor de bits correspondiente de la dirección

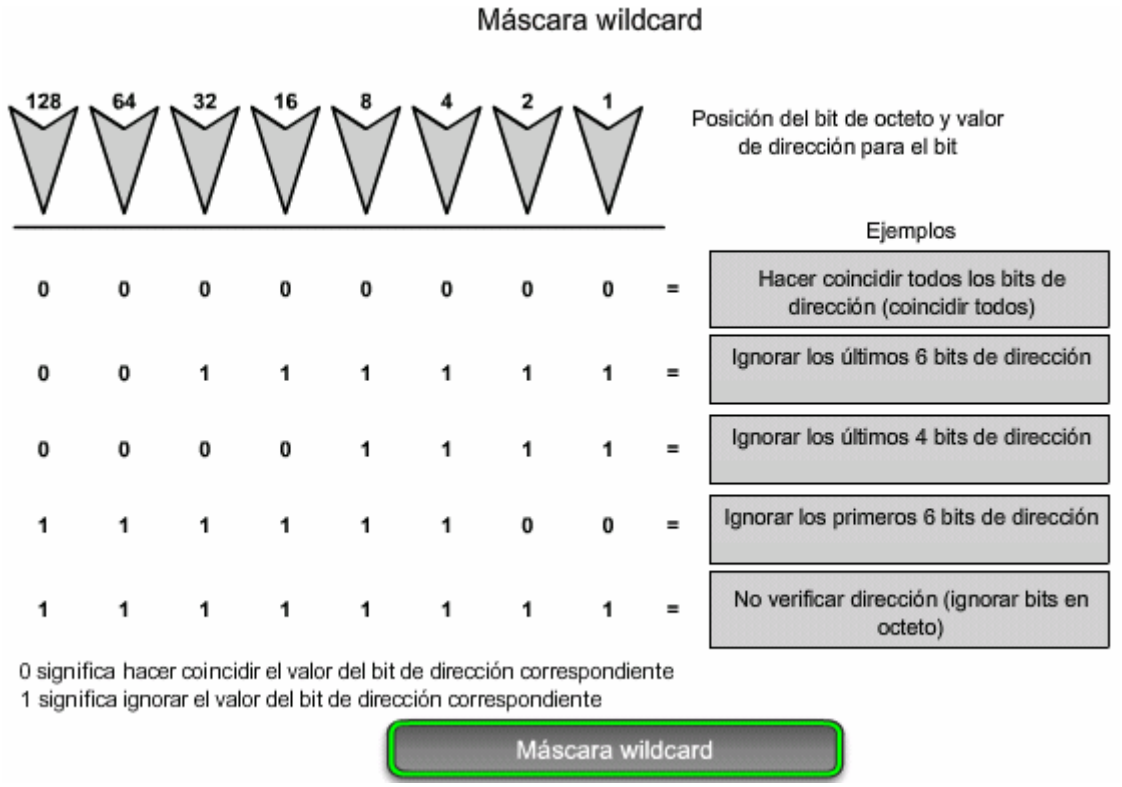
La figura muestra la forma en la que las diferentes máscaras wildcard filtran direcciones IP. Como puede observar en el ejemplo, recuerde que el 0 binario representa una coincidencia, y el 1 binario, ignorar.

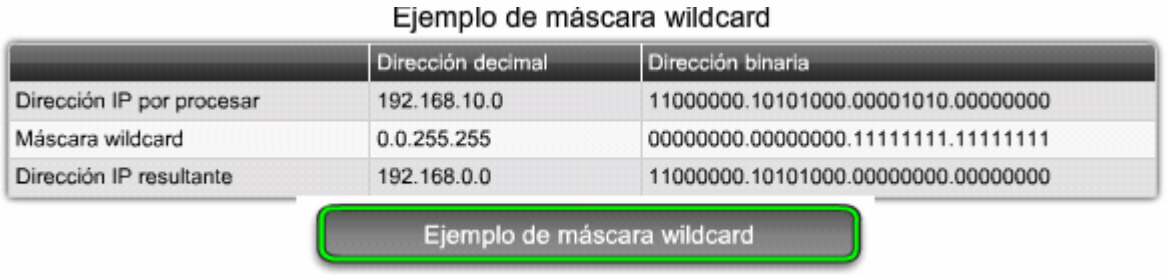
Nota: Las máscaras wildcard generalmente son denominadas máscaras inversas. El motivo es que, a diferencia de una máscara de subred cuyo 1 binario representa una coincidencia y el 0 binario la falta de coincidencia, lo inverso es verdadero.

Haga clic en el botón Ejemplo de máscara wildcard en la figura.

Uso de la máscara wildcard

La tabla de la figura muestra los resultados de aplicar una máscara wildcard 0.0.255.255 a una dirección IP de 32 bits. Recuerde que un 0 binario indica un valor coincidente.





Máscaras wildcard para hacer coincidir subredes IP

Calcular la máscara wildcard puede ser un tanto confuso al principio. La figura proporciona tres ejemplos de máscaras wildcard.

En el primer ejemplo, la máscara wildcard indica que cada bit de la dirección IP 192.168.1.1 debe coincidir en forma exacta. La máscara wildcard es equivalente a la máscara de subred 255.255.255.255.

En el segundo ejemplo, la máscara wildcard indica que todo coincide. La máscara wildcard es equivalente a la máscara de subred 0.0.0.0.

En el tercer ejemplo, la máscara wildcard indica que coincide cualquier host dentro de la red 192.168.1.0 /24. La máscara wildcard es equivalente a la máscara de subred 255.255.255.0.

Estos ejemplos eran bastante sencillos. Sin embargo, el cálculo de las máscaras wildcard puede ser un poco más complicado.

Haga clic en el botón Máscara wildcard 2 que se muestra en la figura.

Los dos ejemplos de la figura son más complicados que los últimos tres que se mostraron. En el ejemplo 1, los primeros dos octetos y los primeros cuatro bits del tercer octeto deben coincidir de manera exacta. Los últimos cuatro bits deltercer octeto y el último octeto pueden ser cualquier número válido. Esto da como resultado una máscara que verifica de 192.168.16.0 a 192.168.31.0.

El ejemplo 2 muestra una máscara wildcard que coincide con los primeros dos octetos y el bit más insignificante del tercero. El último octeto y los primeros siete bits del tercer octeto pueden ser cualquier número válido. El resultado es una máscara que permite o deniega todos los hosts desde subredes impares de la red principal 192.168.0.0.

Calcular máscaras wildcard puede ser complicado, pero puede hacerlo fácilmente restando la máscara de subred de 255.255.255.255.

Haga clic en el botón Ejemplo 1 que se muestra en la figura.

Por ejemplo, supongamos que desea permitir el acceso a todos los usuarios de lared 192.168.3.0. Si la máscara de subred es 255.255.255.0, puede tomar 255.255.255.255 y restar de la máscara de subred 255.255.255.0 o como se muestra en la figura. La solución genera la máscara wildcard 0.0.0.255.

Haga clic en el botón Ejemplo 2 que se muestra en la figura.

Supongamos que desea permitir el acceso a la red a los 14 usuarios de la subred 192.168.3.32 /28. La máscara de subred para la subred IP es 255.255.255.240; tome 255.255.255.255 y reste de la máscara de subred 255.255.255.240. Esta vez la solución genera la máscara wildcard 0.0.0.15.

Haga clic en el botón Ejemplo 3 que se muestra en la figura.

En este tercer ejemplo, supongamos que desea hacer coincidir sólo las redes 192.168.10.0 y 192.168.11.0. Nuevamente, tome 255.255.255.255 y reste la máscara de subred regular que, en este caso, es 255.255.252.0. El resultado es 0.0.3.255.

Puede obtener el mismo resultado con las siguientes dos sentencias:

R1(config)# **access-list 10 permit 192.168.10.0**

R1(config)# **access-list 10 permit 192.168.11.0**

Es más eficaz configurar la máscara wildcard de la siguiente manera:

R1(config)# **access-list 10 permit 192.168.10.0 0.0.3.255**

No parece ser más eficaz, pero considere hacer coincidir la red 192.168.16.0 a 192.168.31.0 de la siguiente manera:

R1(config)# **access-list 10 permit 192.168.16.0**
R1(config)# **access-list 10 permit 192.168.17.0**
R1(config)# **access-list 10 permit 192.168.18.0**
R1(config)# **access-list 10 permit 192.168.19.0**
R1(config)# **access-list 10 permit 192.168.20.0**
R1(config)# **access-list 10 permit 192.168.21.0**
R1(config)# **access-list 10 permit 192.168.22.0**
R1(config)# **access-list 10 permit 192.168.23.0**
R1(config)# **access-list 10 permit 192.168.24.0**
R1(config)# **access-list 10 permit 192.168.25.0**
R1(config)# **access-list 10 permit 192.168.26.0**
R1(config)# **access-list 10 permit 192.168.27.0**
R1(config)# **access-list 10 permit 192.168.28.0**
R1(config)# **access-list 10 permit 192.168.29.0**
R1(config)# **access-list 10 permit 192.168.30.0**
R1(config)# **access-list 10 permit 192.168.31.0**

Puede ver que es más eficiente al configurar la siguiente máscara wildcard:

R1(config)# **access-list 10 permit 192.168.16.0 0.0.15.255**

Ejemplos de máscara wildcard

	Decimal	Binario
Dirección IP	192.168.1.1	11000000.10101000.00000001 .00000001
Máscara wildcard	0.0.0.0.	00000000.00000000.00000000.00000000
Resultado	192.168.1.1	11000000.10101000.00000001 .00000001

	Decimal	Binario
Dirección IP	192.168.1.1	11000000.10101000.00000001 .00000001
Máscara wildcard	255.255.255.255	11111111.11111111.11111111.11111111
Resultado	0.0.0.0	00000000.00000000.00000000.00000000

	Decimal	Binario
Dirección IP	192.168.1.1	11000000.10101000.00000001 .00000001
Máscara wildcard	0.0.0.255	00000000.00000000.00000000.11111111
Resultado	192.168.1.0	11000000.10101000.00000001.00000000

Máscara wildcard 1

Ejemplos de máscara wildcard

	Decimal	Binario
Dirección IP	0.0.15.255	11000000.10101000.00010000.00000000
Máscara wildcard	0.0.0.255	00000000.00000000.00001111.11111111
Rango de resultados	De 192.168.16.0 a 192.168.31.0	De 11000000.10101000.00010000.00000000 a 11000000.10101000.00011111.00000000

	Decimal	Binario
Dirección IP	192.168.1.0	11000000.10101000.00000001 .00000000
Máscara wildcard	0.0.254.255	00000000.00000000.11111110.11111111
Resultado	192.168.1.0	11000000.10101000.00000001.00000000
	Todas las subredes con número impar en la red principal 192.168.0.0	

Máscara wildcard 2

Cálculo de máscara wildcard: 1

255.255.255.255
- 255.255.255.000
000.000.000.255

Ejemplo 1

Cálculo de máscara wildcard: 2

255.255.255.255
- 255.255.255.240
000.000.000.015

Ejemplo 2

Cálculo de máscara wildcard: 3

255.255.255.255
- 255.255.252.000
000.000.003.255

Ejemplo 3

Palabras clave de la máscara de bits wildcard

Trabajar con representaciones decimales de bits wildcard binarios puede ser una tarea muy tediosa. Para simplificarla, las palabras clave **host** y **any** ayudan a identificar los usos más comunes de las máscaras wildcard. Con estas palabras clave no necesita ingresar las máscaras wildcard al identificar un host o red específicos. También facilitan la lectura de una ACL al proporcionar pistas visuales en cuanto al origen o destino del criterio.

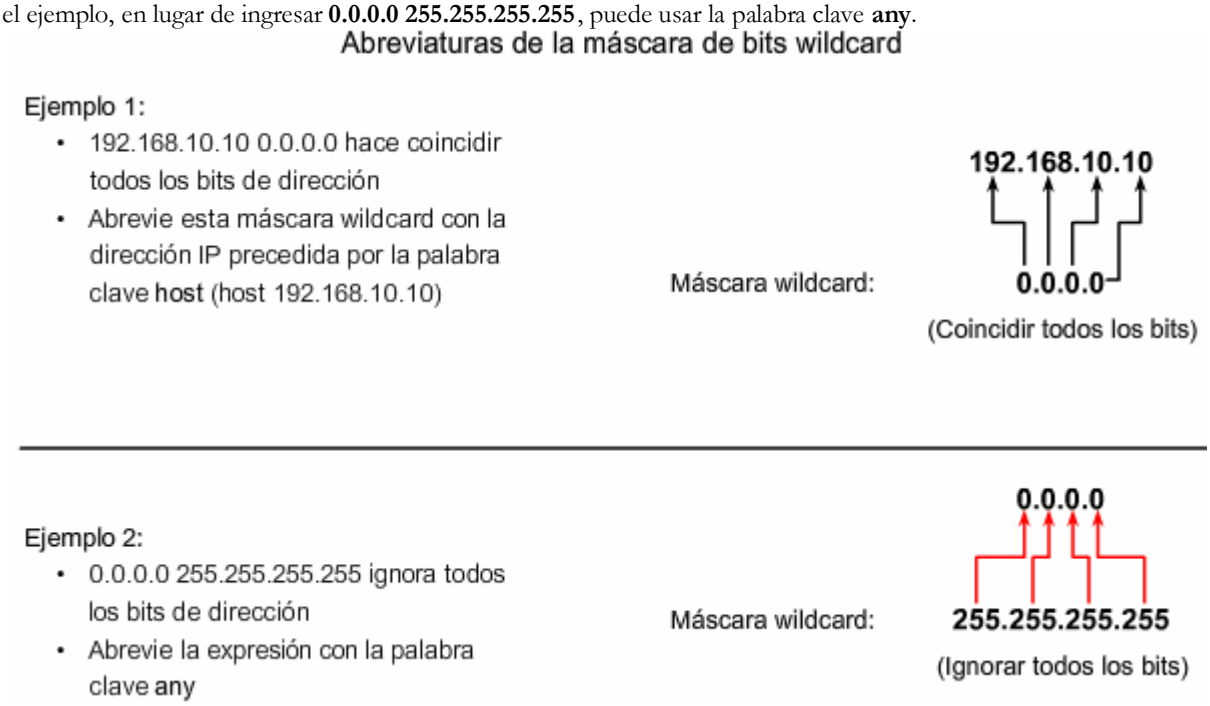
- La opción **host** reemplaza la máscara 0.0.0.0. Esta máscara indica que todos los bits de direcciones IP deben coincidir o que sólo un host coincide.
- La opción **any** reemplaza la dirección IP y la máscara 255.255.255.255. Esta máscara indica que debe ignorarse toda la dirección IP o que deben aceptarse todas las direcciones.

Ejemplo 1: Proceso de las máscaras wildcard con una única dirección IP

En el ejemplo, en lugar de ingresar **192.168.10.10 0.0.0.0**, puede utilizar **host 192.168.10.10**.

Ejemplo 2: Proceso de las máscaras wildcard con una dirección IP que coincide con todas

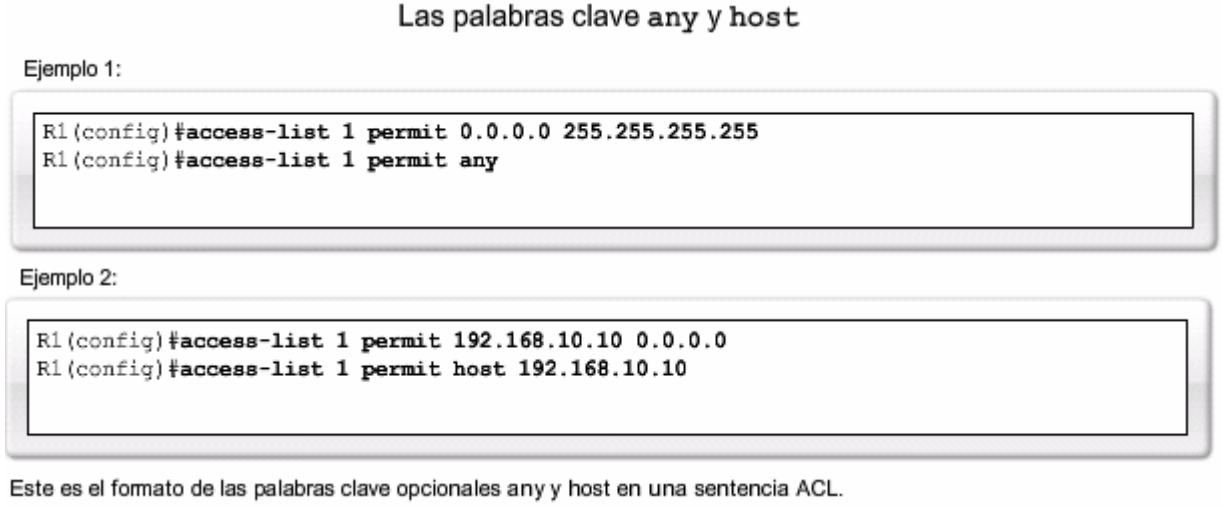
En el ejemplo, en lugar de ingresar **0.0.0.0 255.255.255.255**, puede usar la palabra clave **any**.



Palabras clave any y host

En la figura tenemos dos ejemplos. El Ejemplo 1 muestra cómo utilizar la opción **any** para reemplazar 0.0.0.0 por la dirección IP con máscara wildcard de 255.255.255.255.

El Ejemplo 2 muestra cómo utilizar la opción **host** para reemplazar la máscara wildcard.



5.2.4 Cómo aplicar las ACL estándar a las interfaces

Procedimientos de configuración de las ACL estándar

Luego de configurar una ACL estándar, se la vincula a una interfaz con el comando **ip access-group**:

Router(config-if)#**ip access-group** {*número de lista de acceso* | *nombre de lista de acceso*} {**in** | **out**}

Para eliminar una ACL de una interfaz, primero ingrese el comando **no ip access-group** en la interfaz y luego el comando global **no access-list** para eliminar toda la ACL.

En la figura aparecen los pasos y la sintaxis para configurar y aplicar una ACL estándar numerada en un router.

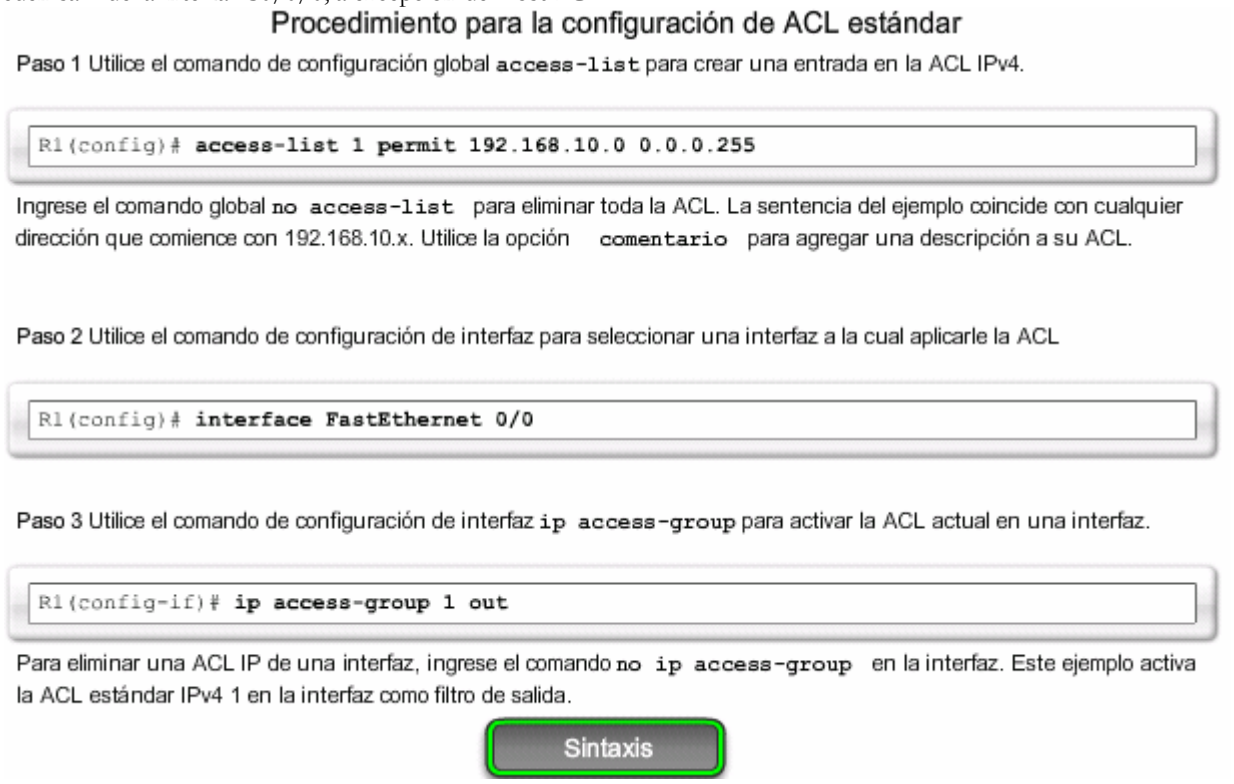
Haga clic en el botón Ejemplo 1 que aparece en la figura para obtener un ejemplo de una ACL que permite una única red.

Esta ACL sólo permite que el tráfico de la red de origen 192.168.10.0 sea enviado por la interfaz S0/0/0. Se bloquea el tráfico de las demás redes, excepto la 192.168.10.0.

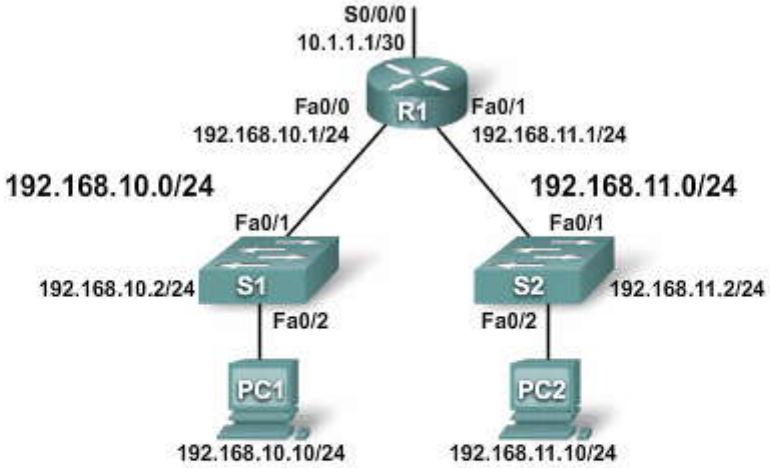
La primera línea identifica la ACL como lista de acceso 1. Permite el tráfico que coincide con los parámetros seleccionados. En este caso, la dirección IP y la máscara wildcard que identifica la red de origen es 192.168.10.0 0.0.0.255. Recuerde que existe la sentencia implícita y oculta "deny all", equivalente a agregar la línea **access-list 1 deny 0.0.0.0 255.255.255.255**.

El comando de configuración de interfaz **ip access-group 1 out** vincula y adjunta la ACL 1 a la interfaz Serial 0/0/0 como filtro de salida.

Por ello, la ACL 1 sólo permite hosts de la red 192.168.10.0 /24 para salir del router R1. Deniega cualquier otra red, incluso la 192.168.11.0.
Haga clic en el botón Ejemplo 2 que aparece en la figura para obtener un ejemplo de una ACL que deniega un host específico.
Esta ACL reemplaza el ejemplo anterior, pero además bloquea el tráfico de una dirección específica. El primer comando borra la versión anterior de la ACL 1. La siguiente sentencia de ACL deniega el host PC1 ubicado en 192.168.10.10. Está permitido cualquier otro host de la red 192.168.10.0 /24. Nuevamente, la sentencia implícita de denegación coincide con cualquier otra red.
Nuevamente se aplica la ACL a la interfaz S0/0/0 en dirección saliente.
Haga clic en el botón Ejemplo 3 que aparece en la figura para obtener un ejemplo de una ACL que deniega una subred específica.
Esta ACL reemplaza el ejemplo anterior pero aún bloquea tráfico del equipo host PC1. Permite, además, que todo el tráfico de LAN salga del router R1.
Los primeros dos comandos son los mismos que el ejemplo anterior. El primer comando borra la versión anterior de la ACL 1 y la siguiente sentencia de ACL deniega el host PC1 ubicado en 192.168.10.10.
La tercera línea es nueva y permite todos los hosts de las redes 192.168.x.x /16. Ahora, esto significa que todos los hosts de la red 192.168.10.0 /24 sí coinciden, pero ahora también coinciden los hosts de la red 192.168.11.0.
Nuevamente se aplica la ACL a la interfaz S0/0/0 en dirección saliente. Por ello, las dos LAN conectadas al router R1 pueden salir de la interfaz S0/0/0, a excepción del host PC1.



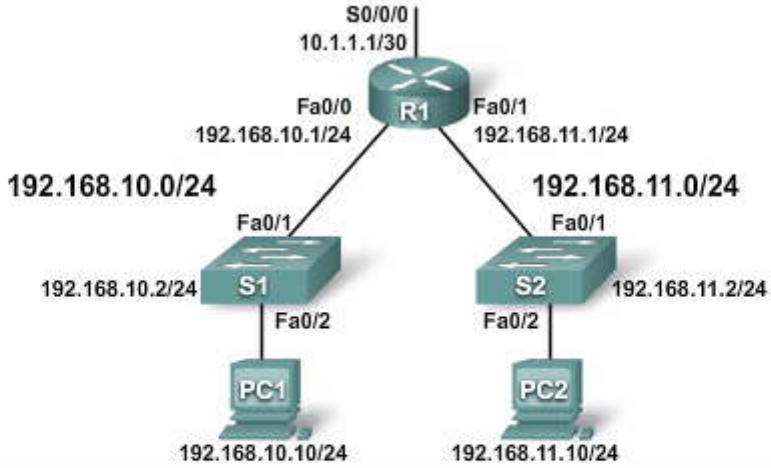
ACL estándar para permitir mi red solamente




```
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# interface S0/0/0
R1(config-if)# ip access-group 1 out
```

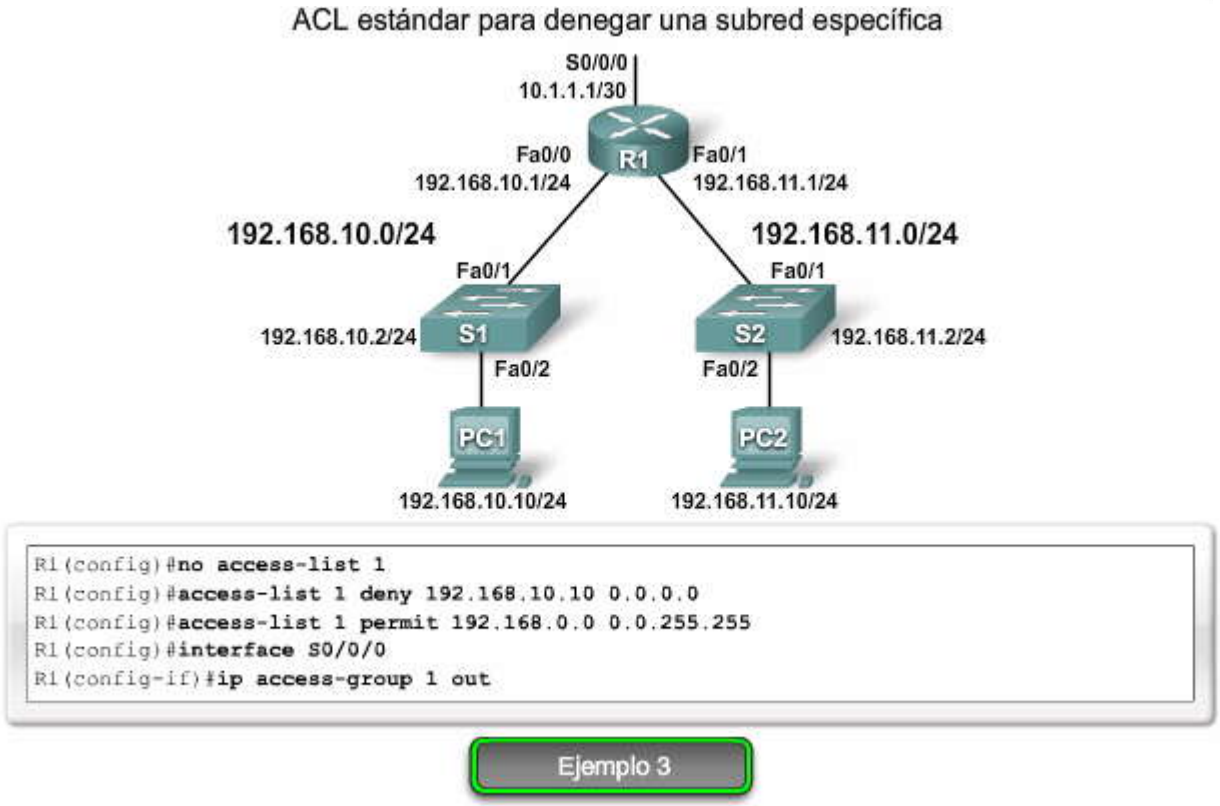
Ejemplo 1

ACL estándar para denegar un host específico




```
R1(config)#no access-list 1
R1(config)#access-list 1 deny 192.168.10.10 0.0.0.0
R1(config)#access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)#interface S0/0/0
R1(config-if)#ip access-group 1 out
```

Ejemplo 2



Uso de las ACL para controlar el acceso VTY

Cisco recomienda utilizar SSH para conexiones administrativas a routers y switches. Si la imagen del software IOS de Cisco en su router no admite SSH, puede mejorar parcialmente la seguridad de las líneas administrativas restringiendo el acceso VTY. Restringir el acceso VTY es una técnica que le permite definir qué direcciones IP tienen acceso Telnet al proceso EXEC del router. Puede controlar la estación de trabajo o red administrativa que administra su router con una ACL y una sentencia **access-class** a sus líneas VTY. También puede utilizar esta técnica con SSH para mejorar más la seguridad del acceso administrativo.

El comando **access-class** del modo de configuración de línea restringe las conexiones entrantes y salientes entre una VTY particular (en un dispositivo Cisco) y las direcciones de una lista de acceso.

Las listas de acceso extendidas y estándar se aplican a paquetes que viajan a través de un router. No están diseñadas para bloquear paquetes que se originan dentro del router. De forma predeterminada, la ACL Telnet extendida de salida no impide las sesiones Telnet iniciadas por el router.

Filtrar el tráfico de Telnet generalmente es una función de una ACL IP extendida, porque filtra un protocolo de nivel superior. Sin embargo, como usted utiliza el comando **access-class** para filtrar sesiones de Telnet entrantes y salientes mediante direcciones de origen y para aplicar filtros a las líneas VTY, puede utilizar las sentencias de ACL estándar para controlar el acceso VTY.

La sintaxis del comando access-class es:

access-class*access-list-number* {**in** [**vrf-also**] | **out**}

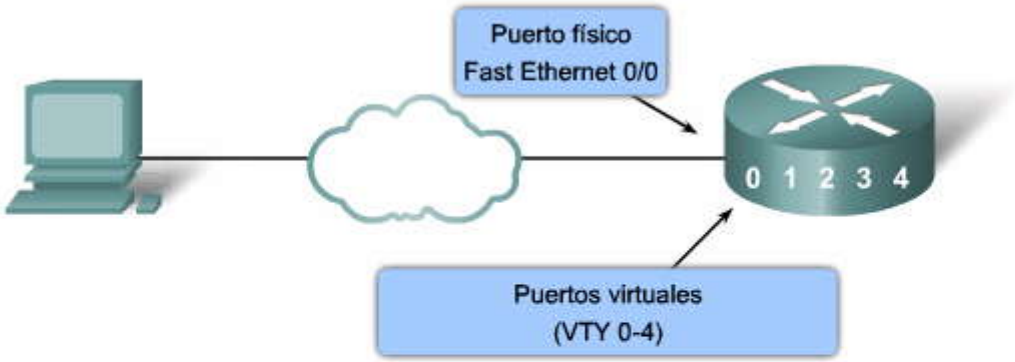
El parámetro **in** restringe las conexiones entrantes entre un dispositivo Cisco particular y las direcciones de la lista de acceso, mientras que el parámetro **out** restringe las conexiones salientes entre un dispositivo Cisco particular y las direcciones de la lista de acceso.

En la figura se muestra un ejemplo donde se permite VTY 0 y 4. Por ejemplo, la ACL de la figura se configura para permitir el acceso de las redes 192.168.10.0 y 192.168.11.0 a las VTY 0 - 4. Todas las demás redes no tienen acceso a las VTY.

Cuando configure las listas de acceso en las VTY, tenga en consideración lo siguiente:

- Sólo se pueden aplicar listas de acceso numeradas a las VTY.
- Deben establecerse las mismas restricciones en todas las VTY porque un usuario puede intentar conectarse a cualquiera de ellas.

ACL estándar para controlar el acceso de terminales virtuales




```
R1(config)#access-list 21 permit 192.168.10.0 0.0.0.255
R1(config)#access-list 21 permit 192.168.11.0 0.0.0.255
R1(config)#access-list 21 deny any

R1(config)#line vty 0 4
R1(config-line)#login
R1(config-line)#password secret
R1(config-line)#access-class 21 in
```

5.2.5 Edición de ACL numeradas

Edición de las ACL numeradas

Al configurar una ACL, se agregan sentencias en el orden en el que se ingresan al final de la ACL. Sin embargo, no hay una función de edición incorporada que le permita editar un cambio en la ACL. No puede insertar o borrar líneas de manera selectiva.

Es muy recomendable crear una ACL en un editor de texto, como el Bloc de notas de Microsoft. Esto le permite crear o editar una ACL y luego pegarla en el router. En el caso de una ACL existente, puede usar el comando **show running-config** para visualizar la ACL, copiarla y pegarla en el editor de texto, hacer los cambios necesarios y volver a cargarla.

Por ejemplo, supongamos que la dirección IP del host de la figura fue ingresada incorrectamente. En lugar del host 192.168.10.100, debería haberse ingresado 192.168.10.11. A continuación, le mostramos los pasos que se deben seguir para editar y corregir la ACL 20:

Paso 1. Visualice la ACL ingresando el comando **show running-config**. El ejemplo de la figura utiliza la palabra clave **include** para visualizar sólo las sentencias de la ACL.

Paso 2. Resalte la ACL, cópiela y luego péguela en el Bloc de notas de Microsoft. Edite la lista como sea necesario. Cuando visualice correctamente la ACL en el Bloc de notas de Microsoft, resáltela y cópiela.

Paso 3. En el modo de configuración global, deshabilite la lista de acceso con el comando **no access-list 20**. De lo contrario, se agregan las nuevas sentencias a la ACL actual. Luego pegue la nueva ACL en la configuración del router.

Se debe aclarar que al utilizar el comando **no access-list**, ninguna ACL protege su red. Tenga en cuenta, además, que si comete un error en la nueva lista, debe deshabilitarla y solucionar el problema. En ese caso, una vez más su red no contará con una ACL durante el proceso de corrección.

Edición de ACL numeradas

Paso 1

```
R1#show running-config | include access-list
access-list 20 permit 192.168.10.100
access-list 20 deny   192.168.10.0 0.0.0.255
```

Paso 2

```
access-list 20 permit 192.168.10.11
access-list 20 deny 192.168.10.0 0.0.0.255
```

Paso 3

```
R1#conf t
Enter configuration commands, one per line. End with
CTRL/Z.
R1(config)#no access-list 20
R1(config)#access-list 20 permit   192.168.10.100
R1(config)#access-list 20 deny 192.168.10.0 0.0.0.255
```

Comentarios en las ACL

Puede usar la palabra clave **remark** para incluir comentarios (observaciones) sobre entradas en cualquier ACL IP estándar o extendida. Las observaciones facilitan la comprensión y el análisis de la ACL. Cada línea de observación está limitada a 100 caracteres.

La observación puede ir antes o después de una sentencia **permit** o **deny**. Debe ser consecuente con la ubicación de las observaciones para que quede claro qué observación describe qué sentencia **permit** o **deny**. Por ejemplo, sería confuso tener algunas observaciones antes de la sentencia **permit** o **deny** asociada y algunas después.

Para incluir un comentario en una ACL IP numerada estándar o extendida, use el comando de configuración global **access-list** *nuúmero de lista de acceso* **remark** *comentario*. Para eliminar la observación, utilice la forma **no** de este comando.

En el primer ejemplo, la ACL estándar permite el acceso a la estación de trabajo que pertenece a Jones y deniega el acceso a la estación de trabajo que pertenece a Smith.

Para una entrada en una ACL nombrada, use el comando de configuración **remark access-list**. Para eliminar la observación, utilice la forma **no** de este comando. El segundo ejemplo muestra una ACL extendida nombrada. Recuerde de la definición anterior de las ACL extendidas que se utilizan para controlar números de puerto y servicios específicos. En el segundo ejemplo, la observación indica que la subred de Jones no tiene permitido utilizar Telnet saliente.

Comentarios sobre las ACL

Ejemplo 1:

```
Router(config)# access-list 1 remark Permit only Jones workstation through
Router(config)# access-list 1 permit 192.168.10.13
Router(config)# access-list 1 remark Do not allow Smith through
Router(config)# access-list 1 deny 1 192.168.10.14
```

Ejemplo 2:

```
Router(config)# ip access-list extended TELNETTING
Router(config-ext-nacl)# remark Do not allow Jones workstation to Telnet
Router(config-ext-nacl)# deny tcp host 192.168.10.13 any eq telnet
```

5.2.6 Creación de ACL estándar nombradas

Asignar un nombre a una ACL facilita la comprensión de su función. Por ejemplo, una ACL que deniega FTP puede denominarse NO_FTP. Al identificar una ACL con un nombre en lugar de un número, el modo de configuración y la sintaxis del comando son un tanto diferentes.

La figura muestra los pasos para crear una ACL estándar nombrada.

Paso 1. Desde el modo de configuración global, use el comando **ip access-list** para crear una ACL nombrada. Los nombres de las ACL son alfanuméricos, deben ser únicos y no deben comenzar con un número.

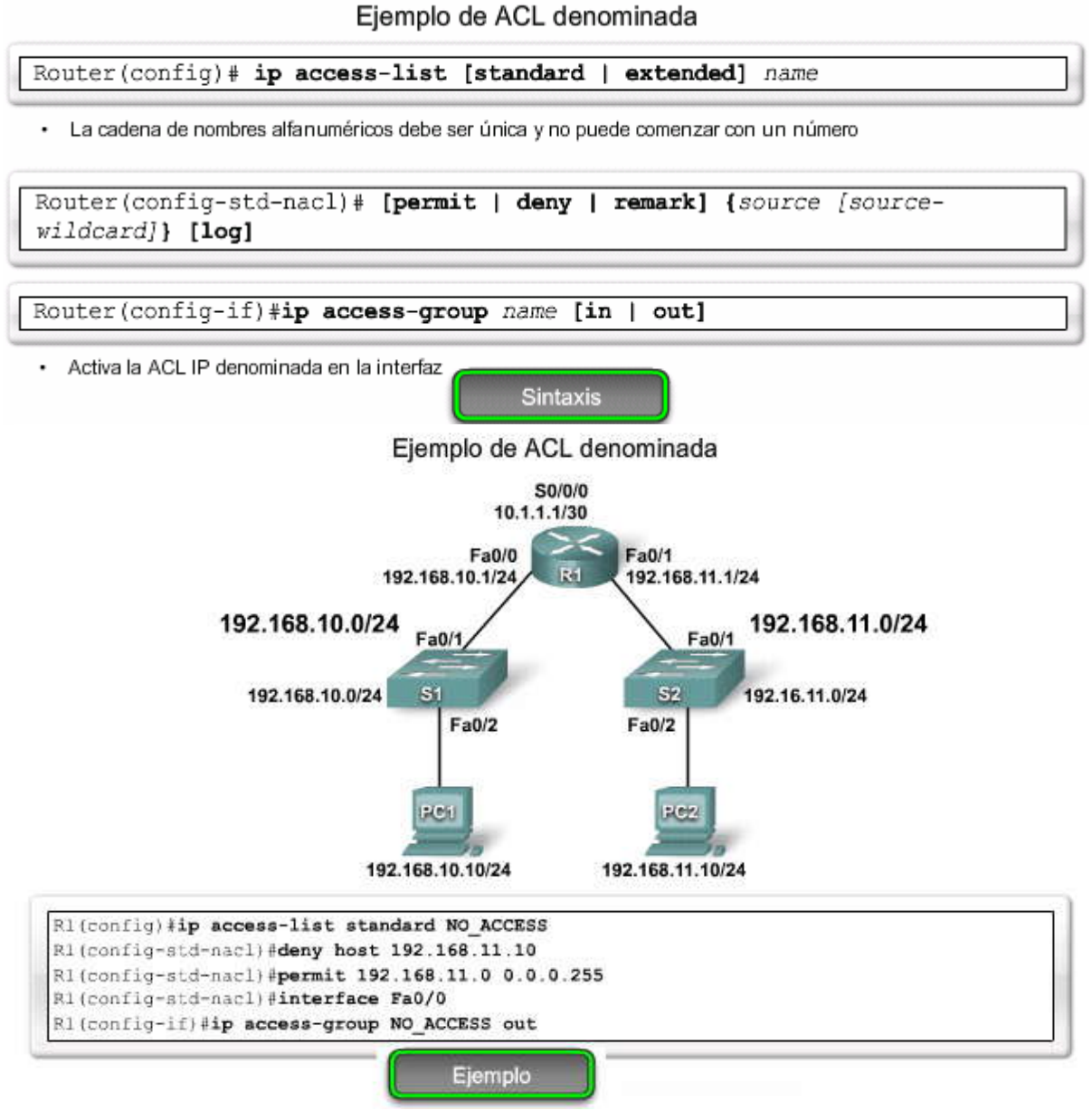
Paso 2. Desde el modo de configuración de una ACL nombrada, use las sentencias **permit** o **deny** para especificar una o más condiciones que determinen si se envía o descarta un paquete.

Paso 3. Regrese al modo EXEC privilegiado con el comando **end**.

Haga clic en el botón Ejemplo que se muestra en la figura.

En la figura, el resultado en pantalla muestra los comandos utilizados para configurar una ACL estándar nombrada en el router R1, la interfaz Fa0/0 que deniega el acceso del host 192.168.11.10 a la red 192.168.10.0.

No necesita que los nombres de las ACL estén en mayúsculas, pero se destacan al visualizar el resultado de running-config.



5.2.7 Monitoreo y verificación de ACL

Al finalizar la configuración de una ACL, use los comandos **show** del IOS de Cisco para verificar la configuración. En la figura, el ejemplo de la parte superior muestra la sintaxis del IOS de Cisco para visualizar los contenidos de todas las ACL. El ejemplo de la parte inferior muestra el resultado del comando **show access-lists** en el router R1. Los nombres en mayúscula de las ACL, SALES y ENG, se destacan en el resultado que se muestra en la pantalla.

Recuerde por qué comenzó a configurar las ACL en primer lugar: deseaba implementar las políticas de seguridad de su organización. Ahora que comprobó que las ACL se configuraron como pretendía, el siguiente paso es confirmar que funcionen según lo planeado.

Las pautas analizadas al principio de esta sección sugieren que configure las ACL en una red de prueba y, luego, las implemente en la red de producción. Si bien el análisis sobre cómo preparar una situación de prueba de las ACL no está dentro del alcance de este curso, debe saber que confirmar que las ACL funcionen según lo planeado puede ser un proceso complejo y lento.

Supervisión de sentencias de ACL

```
R1# show access-lists { access-list-number|name }
```

```
R1# show access-lists
Standard IP access list SALES
    10 deny   10.1.1.0 0.0.0.255
    20 permit 10.3.3.1
    30 permit 10.4.4.1
    40 permit 10.5.5.1
Extended IP access list ENG
    10 permit tcp host 192.168.10.2 any eq telnet (25 matches)
    20 permit tcp host 192.168.10.2 any eq ftp
    30 permit tcp host 192.168.10.2 any eq ftp-data
```

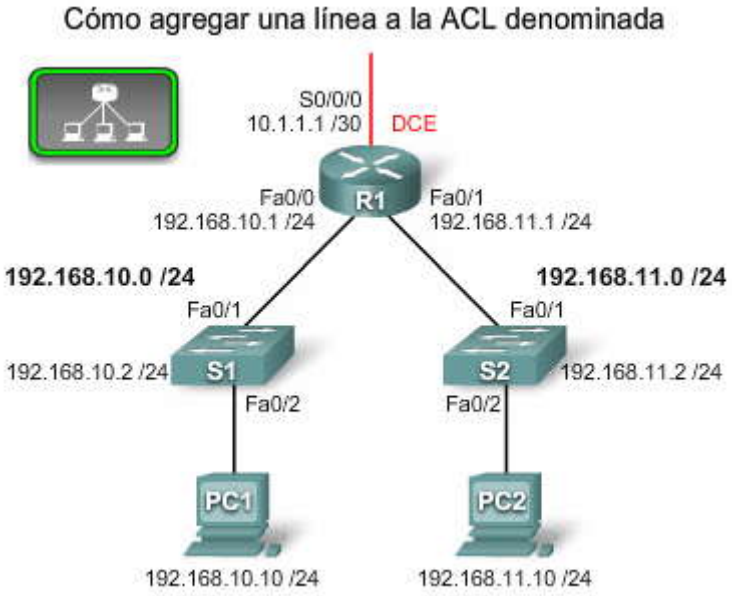
5.2.8 Edición de las ACL nombradas

Las ACL nombradas tienen una gran ventaja sobre las ACL numeradas porque son más fáciles de editar. A partir del software IOS de Cisco versión 12.3, las ACL IP nombradas le permiten borrar entradas individuales en una ACL específica. Puede usar secuencias de números para insertar sentencias en cualquier parte de la ACL nombrada. Si utiliza una versión anterior del software IOS de Cisco, puede agregar sentencias sólo al final de la ACL nombrada. Como puede borrar entradas individuales, puede modificar su ACL sin necesidad de borrar y luego reconfigurar toda la ACL.

El ejemplo de la figura muestra una ACL aplicada a la interfaz S0/0/0 de R1. Restringió el acceso al servidor Web. Si observamos este ejemplo, puede ver dos elementos que aún no se incluyeron en este curso:

Haga clic en el botón Resultados del router de la figura.

- En el primer resultado del comando **show**, puede ver que la ACL con el nombre WEBSERVER tiene tres líneas numeradas que indican las reglas de acceso para el servidor Web.
- Para otorgar acceso a otra estación de trabajo de la lista sólo debe ingresar una línea numerada. En el ejemplo, se agrega la estación de trabajo con la dirección IP 192.168.10.15.
- El último resultado del comando **show** verifica que la nueva estación de trabajo tenga acceso.



Cómo agregar una línea a la ACL denominada

```
R1# show access-lists
Standard IP access list WEBSERVER
    10 permit 192.168.10.11
    20 deny   192.168.10.0, wildcard bits 0.0.0.255
    30 deny   192.168.11.0, wildcard bits 0.0.0.255
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ip access-list standard WEBSERVER
R1(config-std-nacl)# 15 permit host 192.168.11.10
R1(config-std-nacl)# end
R1#
*Nov  1 19:20:57.591: %SYS-5-CONFIG_I: Configured from console by console
R1# sho access-lists
Standard IP access list WEBSERVER
    10 permit 192.168.10.11
    15 permit 192.168.11.10
    20 deny   192.168.10.0, wildcard bits 0.0.0.255
    30 deny   192.168.11.0, wildcard bits 0.0.0.255
R1#
```

Resultado del router

Las ACL estándar son configuraciones de router que controlan si un router permite o deniega paquetes según la dirección de origen. Esta actividad se concentra en definir los criterios de filtrado, configurar las ACL estándar, aplicar las ACL a las interfaces del router y verificar y probar la implementación de las ACL.

Se proporcionan instrucciones detalladas dentro de la actividad y en el siguiente enlace al PDF.

Instrucciones de la actividad (PDF)

Haga clic en el icono de Packet Tracer para obtener más detalles.
Desplegar medios visuales

5.3 Configuración de las ACL extendidas

5.3.1 ACL extendidas

Prueba de paquetes con ACL extendidas

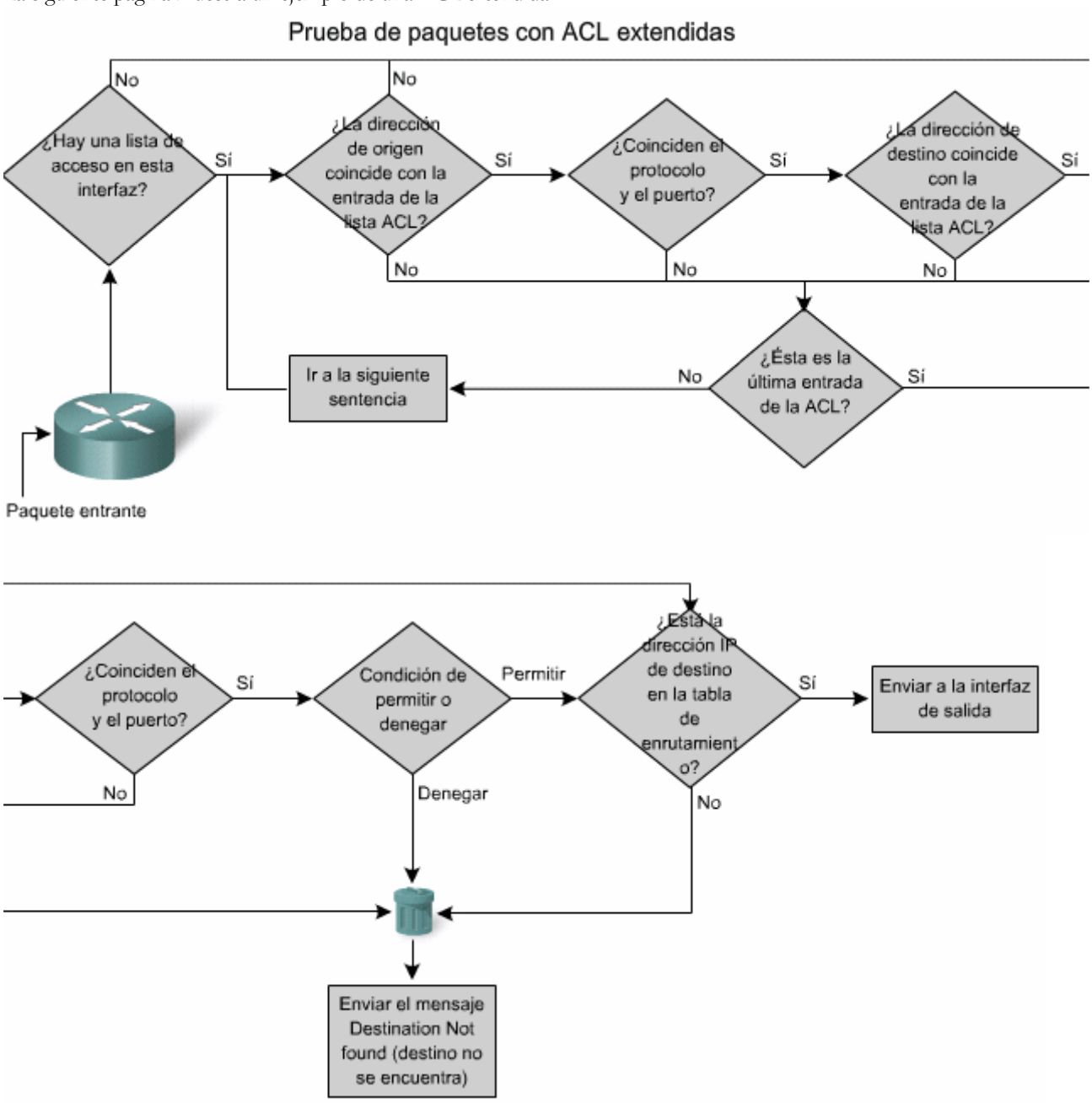
Para lograr un control más preciso del filtrado del tráfico, puede usar ACL extendidas numeradas del 100 al 199 y del 2000 al 2699, lo que ofrece un total de 799 ACL extendidas posibles. A las ACL extendidas también se les puede asignar un nombre.

Las ACL extendidas se utilizan con más frecuencia que las ACL estándar porque proporcionan un mayor control y, por lo tanto, complementan su solución de seguridad. Al igual que las ACL estándar, las extendidas verifican la dirección de origen

del paquete, pero también verifican la dirección de destino, los protocolos y los números de puerto (o servicios). Esto ofrece un criterio más amplio sobre el cual fundamentar la ACL. Por ejemplo, una ACL extendida puede permitir de manera simultánea el tráfico de correo electrónico de una red a un destino específico y, a la vez, denegar la transferencia de archivos y la navegación Web.

La figura muestra la ruta de decisión lógica utilizada por una ACL extendida creada para filtrar direcciones de origen y de destino, números de puerto y protocolo. En este ejemplo, la ACL filtra primero la dirección de origen, luego el puerto y el protocolo de origen. Luego filtra la dirección de destino; posteriormente, el puerto y el protocolo de destino y toma una decisión final de permiso o denegación.

Recuerde que las entradas de las ACL se procesan una después de la otra, por lo que la decisión 'No' no necesariamente significa 'Denegar'. Mientras recorre la ruta de decisión lógica, observe que 'No' significa seguir hasta la siguiente entrada hasta probar todas las entradas. Una vez que se hayan procesado todas las entradas, se toma la decisión final de 'Permitir' o 'Denegar'.
La siguiente página muestra un ejemplo de una ACL extendida.



Prueba de puertos y servicios

La posibilidad de filtrar protocolos y números de puerto le permite crear ACL extendidas muy específicas. Mediante el número de puerto adecuado, puede especificar una aplicación al configurar el número de puerto o el nombre de un puerto bien conocido.

La figura muestra algunos ejemplos de la forma en la que el administrador especifica un número de puerto TCP o UDP colocándolo al final de la sentencia de la ACL extendida. Pueden utilizarse operaciones lógicas, como igual (eq), desigual (neq), mayor que (gt) y menor que (lt).

Haga clic en el botón Números de puerto que se muestra en la figura.

La figura muestra cómo generar una lista de números de puerto y palabras clave que puede utilizar al crear una ACL con el comando **R1(config)#access-list 101 permit tcp any eq ?**.

5.3.2 Configuración de las ACL extendidas

Los procedimientos para configurar las ACL extendidas son los mismos que para las ACL estándar: primero crea la ACL extendida y luego la activa en una interfaz. Sin embargo, la sintaxis y los parámetros del comando tienen más complejidades para admitir las funciones adicionales de las ACL extendidas.

La figura muestra la sintaxis de comando común para las ACL extendidas. El campo de desplazamiento proporciona detalles de las palabras clave y los parámetros. A medida que avance este capitulo, encontrará explicaciones y ejemplos que le permitirán entender mejor.

Haga clic en el botón Configuración de ACL extendidas que se muestra en la figura.

La figura muestra un ejemplo de cómo se puede crear una ACL extendida específica para las necesidades de su red. En este ejemplo, el administrador de red debe restringir el acceso a Internet para permitir sólo la navegación Web. La ACL 103 se aplica al tráfico que sale de la red 192.168.10.0, y la ACL 104 al tráfico que ingresa a la red.

La ACL 103 cumple con la primera parte del requisito. Permite el tráfico que ingresa de cualquier dirección en la red 192.168.10.0 para dirigirse a cualquier destino, sujeto a la limitación que el tráfico se dirige solo a los puertos 80 (HTTP) y 443 (HTTPS).

La naturaleza de HTTP requiere que el tráfico regrese a la red, pero el administrador de red desea restringirlo a intercambios HTTP desde los sitios Web solicitados. La solución de seguridad debe denegar cualquier otro tráfico que ingrese a la red. La ACL 104 lo hace bloqueando el tráfico entrante, a excepción de las conexiones establecidas. HTTP establece conexiones a partir de la solicitud original y luego mediante el intercambio de mensajes ACK, FIN y SYN.

Observe que el ejemplo utiliza el parámetro **established**.

Este parámetro permite respuestas al tráfico que se origina desde la red 192.168.10.0 /24 a la interfaz de entrada s0/0/0. Se produce una coincidencia si el datagrama TCP tiene ajustados los bits ACK o reset (RST) que indican que el paquete pertenece a una conexión existente. Sin el parámetro **established** en la sentencia de ACL, los clientes pueden enviar tráfico a un servidor Web, pero no lo reciben de ese servidor.

Configuración de ACL extendidas

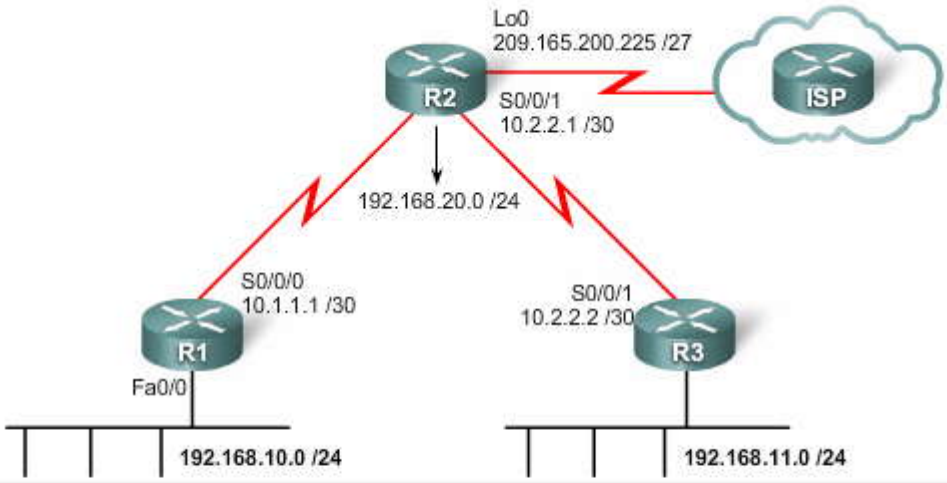
access-list *access-list-number* {deny | permit | remark} *protocol source* [*source-wildcard*] [operator *operand*] [port *port-number or name*] *destination* [*destination-wildcard*][operator operand] [port *port-number or name*][established]

Parámetro	Descripción
access-list-number	Identifica la lista de acceso con un número en el rango entre 100 y 199 (para una ACL IP extendida) y entre 2000 y 2699 (para una ACL IP expandida).
deny	Deniega el acceso si las condiciones concuerdan.
permit	Permite el acceso si las condiciones concuerdan.
remark	Indica si esta entrada permite o bloquea la dirección especificada. También puede utilizarse para ingresar un comentario.
protocol	Nombre o número de un protocolo de Internet. Algunas de las palabras clave más comunes son **icmp**, **ip**, **tcp** o **udp**. Para que haya coincidencia con cualquier protocolo de Internet (como ICMP, TCP y UDP), se usa la palabra clave **ip**.
source	Número de la red o del host desde el que se envía un paquete.
source-wildcard	Bits de wildcard para aplicar al origen.
destination	Número de la red o del host al que se envía un paquete.
destination-wildcard	Bits de wildcard para aplicar al destino.
operator	(Opcional) Compara los puertos de origen y de destino. Algunos de los operandos posibles son **lt** (menor que), **gt** (mayor que), **eq** (igual), **neq** (desigual) y **range** (rango incluido).
port	(Opcional) El número decimal o nombre de un puerto TCP o UDP.
established	(Opcional) Sólo para el protocolo TCP: indica una conexión establecida.

Desplácese por esta ventana para ver toda la sintaxis del comando.

Comandos

Configuración de ACL extendidas




```
R1(config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config)#access-list 104 permit tcp any 192.168.10.0 0.0.0.255 established
```

ACL103 permite solicitudes a los puertos 80 y 443

ACL104 permite respuestas de HTTP y SHTTP establecidas

Configuración de ACL extendidas

5.3.3 Cómo aplicar las ACL extendidas a las interfaces

Aprendamos cómo configurar una lista de acceso extendida a partir del ejemplo anterior. Recuerde que deseamos permitir a los usuarios navegar en sitios Web seguros y no seguros. Primero considere si el tráfico que desea filtrar es entrante o saliente. Intentar acceder a sitos Web de Internet implica la salida de tráfico. Recibir correos electrónicos de Internet implica la entrada de tráfico a la empresa. Sin embargo, al considerar cómo aplicar una ACL a una interfaz, el ingreso y la salida tienen significados diferentes, según el punto de vista.

En el ejemplo de la figura, R1 tiene dos interfaces. Tiene un puerto serial, S0/0/0, y uno Fast Ethernet, Fa0/0. El tráfico entrante de Internet ingresa a la interfaz S0/0/0, pero sale de la interfaz Fa0/0 para llegar a PC1. El ejemplo aplica la ACL a la interfaz serial en ambas direcciones.

Haga clic en el botón Denegar FTP que se muestra en la figura.

Es un ejemplo de denegación de tráfico FTP desde la subred 192.168.11.0 hacia la subred 192.168.10.0, pero permite todo el otro tráfico. Observe el uso de máscaras wildcard y la sentencia explícita "deny all". Recuerde que FTP requiere puertos 20 y 21, por eso necesita especificar **eq 20** y **eq 21** para denegar FTP.

En el caso de las ACL extendidas, puede elegir utilizar números de puerto como se muestra en el ejemplo o denominar un puerto bien conocido. En un ejemplo anterior de una ACL extendida, las sentencias se redactaron de la siguiente manera:

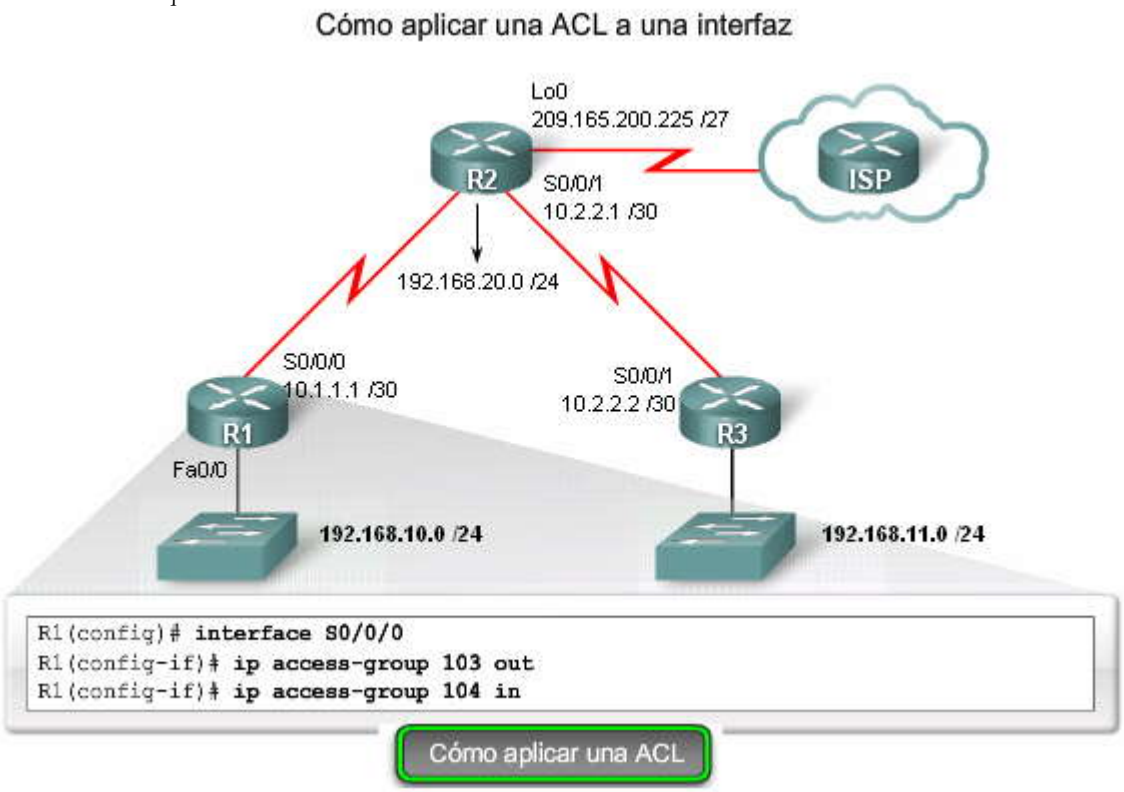
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp

access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp-data

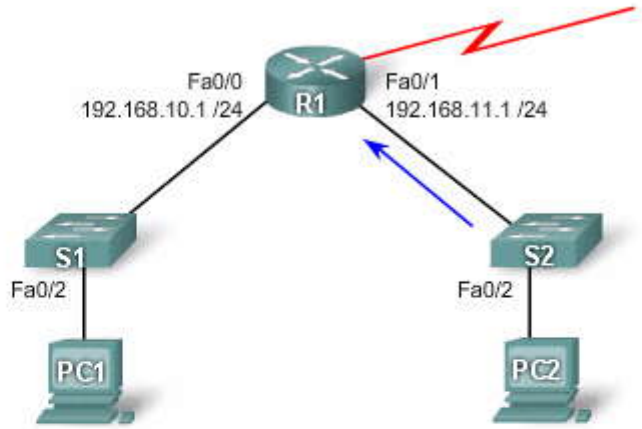
Observe que para FTP es preciso mencionar **ftp** y **ftp-data**.

Haga clic en el botón Denegar Telnet que se muestra en la figura.

Este ejemplo deniega el tráfico de Telnet desde 192.168.11.0 hacia la interfaz Fa0/0, pero permite todo el otro tráfico IP de cualquier otro origen a cualquier destino desde la interfaz Fa0/0. Observe el uso de la palabra clave **any** que significa desde cualquier lado hacia cualquier lado.



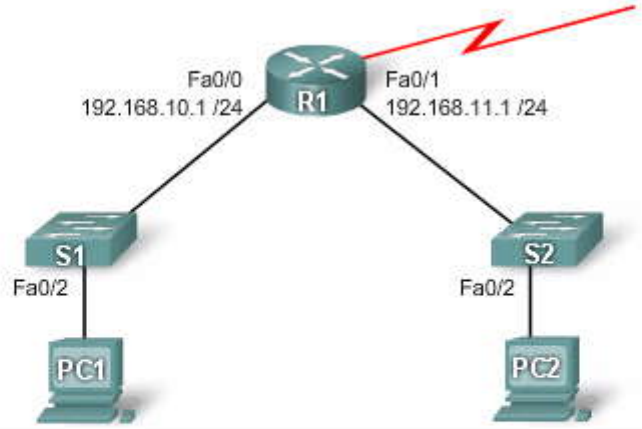
ACL extendidas para denegar FTP de las subredes




```
R1(config)# access-list 101 deny tcp 192.168.11.0 0.0.0.255 192.168.10.0
0.0.0.255 eq 21
R1(config)# access-list 101 deny tcp 192.168.11.0 0.0.0.255 192.168.10.0
0.0.0.255 eq 20
R1(config)# access-list 101 permit ip any any
R1(config)# interface Fa0/1
R1(config-if)# ip access-group 101 in
```

Denegar FTP

ACL extendidas para denegar sólo Telnet de las subredes




```
R1(config)#access-list 101 deny tcp 192.168.11.0 0.0.0.255  any eq 23
R1(config)#access-list 101 permit ip any any

R1(config)# interface Fa0/0
R1(config-if)#ip access-group 101 out
```

Denegar Telnet

5.3.4 Creación de las ACL extendidas nombradas

Puede crear ACL extendidas nombradas básicamente de la misma manera que crea las ACL estándar nombradas. Los comandos para crear una ACL nombrada son diferentes según sies estándar o extendida.

Desde el modo EXEC privilegiado, siga estos pasos para crear una ACL extendida con nombres.

Paso 1. Desde el modo de configuración global, use el comando **ip access-list extended** *nombre* para definir una ACL extendida nombrada.

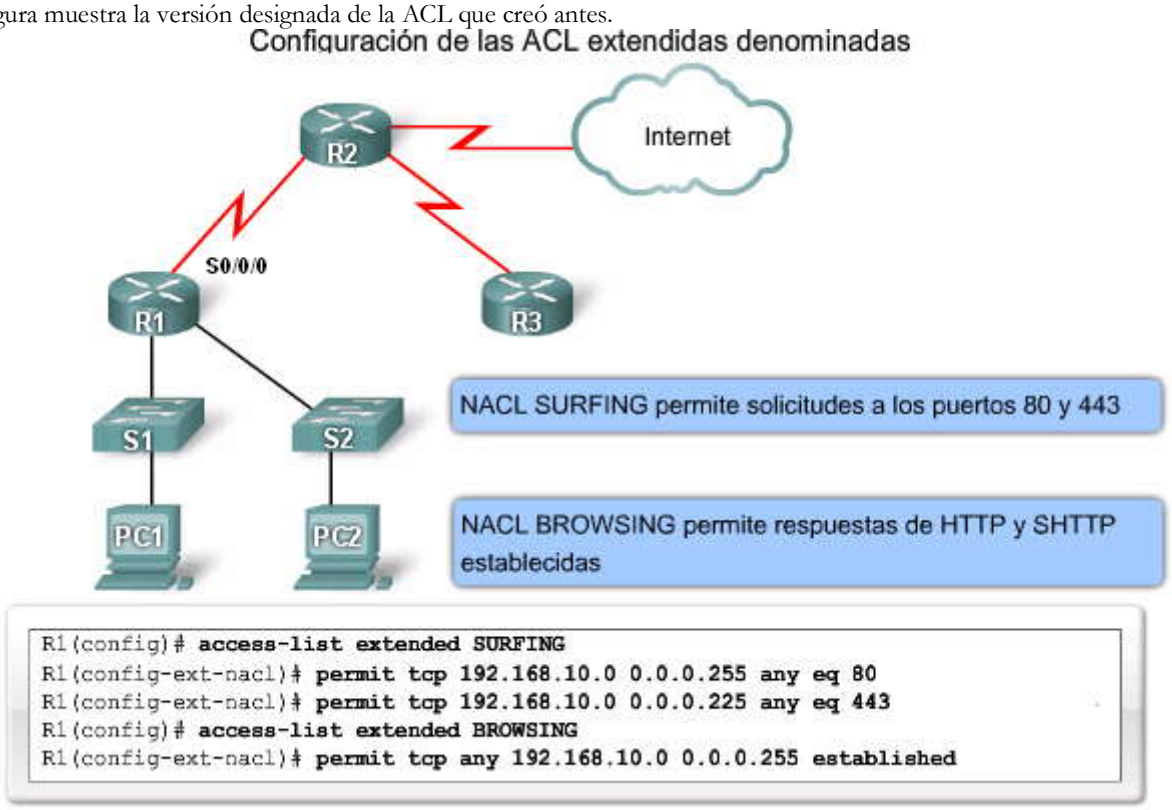
Paso 2. En el modo de configuración de ACL nombrada, especifique las condiciones que desea permitir o denegar.

Paso 3. Regrese al modo EXEC privilegiado y verifique su ACL con el comando **show access-lists** [*número* | *nombre*].

Paso 4. Como opción y paso recomendado, guarde sus entradas en el archivo de configuración con el comando **copy running-config startup-config**.

Para eliminar una ACL extendida nombrada, use el comando de configuración global **no ip access-list extended** *nombre*.

La figura muestra la versión designada de la ACL que creó antes.



Las ACL nombradas son guiones de configuración de router que controlan si un router permite o deniega paquetes según la dirección de origen y de destino, y los protocolos y puertos. Las ACL extendidas brindan unamayor flexibilidad y disparidad que las ACL estándar. Esta actividad se concentra en definir los criterios de filtrado, configurar las ACL extendidas, aplicar las ACL a las interfaces del router y verificar y probar la implementación de las ACL.
Se proporcionan instrucciones detalladas dentro de la actividad y en el siguiente enlace al PDF.
Instrucciones de la actividad (PDF)
Haga clic en el icono de Packet Tracer para obtener más detalles.
Desplegar medios visuales

5.4 Configuración de ACL complejas

5.4.1 ¿Qué son las ACL complejas?

Tipos de ACL complejas

Las ACL estándar y extendidas pueden ser la base de las ACL complejas que brindan mayor funcionalidad. La tabla de la figura resume las tres categorías de ACL complejas.

Tipos de ACL complejas

ACL complejas	Descripción
ACL dinámicas (de bloqueo)	Los usuarios que deseen atravesar el router son bloqueados hasta que utilizan Telnet para conectarse al router y son autenticados.
ACL reflexivas	Permiten el tráfico saliente y limitan el tráfico entrante como respuesta a sesiones que se originan dentro del router.
ACL basadas en tiempo	Permiten el control de acceso según la hora del día y la semana.

5.4.2 ACL dinámicas

¿Qué son las ACL dinámicas?

El bloqueo es una característica de seguridad de filtrado de tráfico que utiliza ACL dinámicas, a veces denominadas ACL de bloqueo. Está disponible sólo para tráfico IP. Las ACL dinámicas dependen de la conectividad Telnet, de la autenticación (local o remota) y de las ACL extendidas.

La configuración de las ACL dinámicas comienza con la aplicación de una ACL extendida para bloquear tráfico que atraviesa de router. Los usuarios que deseen atravesar el router son bloqueados por la ACL extendida hasta que utilizan Telnet para conectarse al router y ser autenticados. En ese momento, se interrumpe la conexión a Telnet, y se agrega una ACL dinámica de única entrada a la ACL extendida existente. Esta entrada permite el tráfico por un período determinado; es posible que se produzcan errores por inactividad y superación del tiempo de espera.

Cuándo utilizar las ACL dinámicas

Las siguientes son algunas razones comunes para utilizar ACL dinámicas:

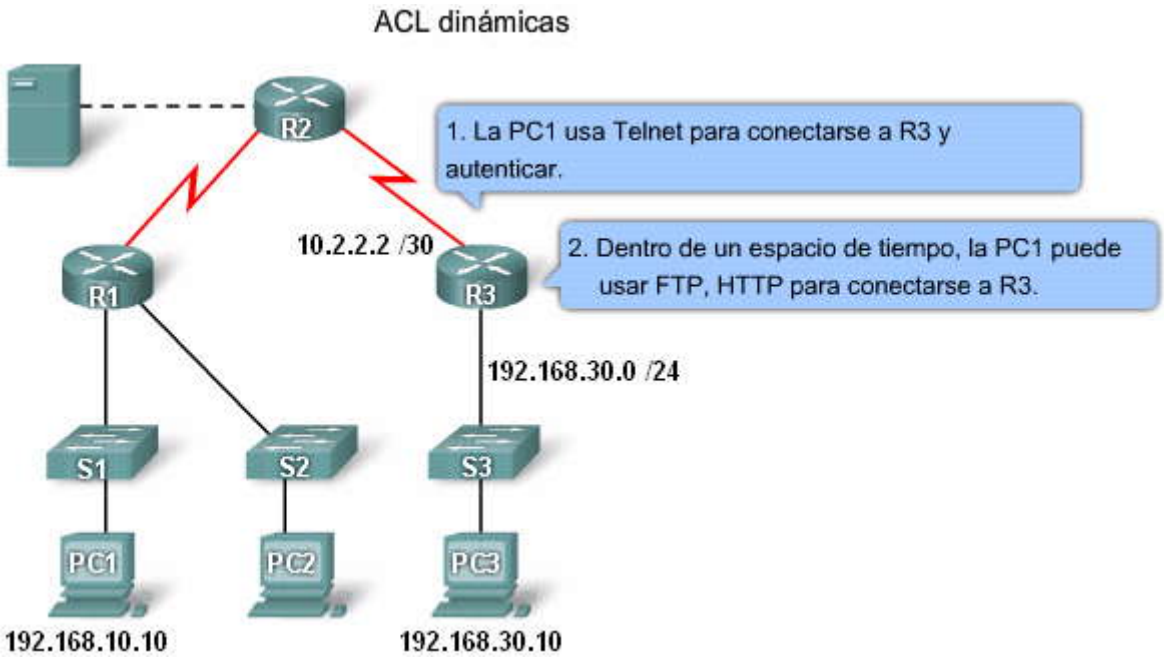
- Cuando desea un usuario remoto o grupo de usuarios remotos específico para acceder al host dentro de la red, conectándose desde sus hosts remotos a través de Internet. El bloqueo autentica al usuario y luego permite el acceso limitado a través de su router firewall para un host o subred por un período limitado.
- Cuando desea que un subconjunto de hosts de una red local acceda a un host de una red remota protegida por un firewall. Con el bloqueo, puede permitir el acceso al host remoto sólo a los conjuntos de hosts locales que desee. El bloqueo requiere que los usuarios se autentiquen a través de AAA, servidor TACACS+ u otro servidor de seguridad, antes de que permita a sus hosts el acceso a los hosts remotos.

Beneficios de las ACL dinámicas

Las ACL dinámicas tienen los siguientes beneficios de seguridad comparadas con las ACL estándar y estáticas extendidas:

- Uso de un mecanismo de desafío para autenticar los usuarios individuales
- Administración simplificada en internetworks más grandes
- En muchos casos, reducción de la cantidad de procesamiento de un router necesario para las ACL
- Reducción de la oportunidad de intromisiones a la red por parte de piratas informáticos
- Creación de acceso dinámico al usuario a través de un firewall, sin comprometer otras restricciones de seguridad configuradas

En la figura, el usuario de PC1 es un administrador que requiere acceso de puerta trasera a la red 192.168.30.0 /24 ubicada en el router R3. Se configuró una ACL dinámica para permitir el acceso FTP y HTTP al router R3 sólo por tiempo limitado.

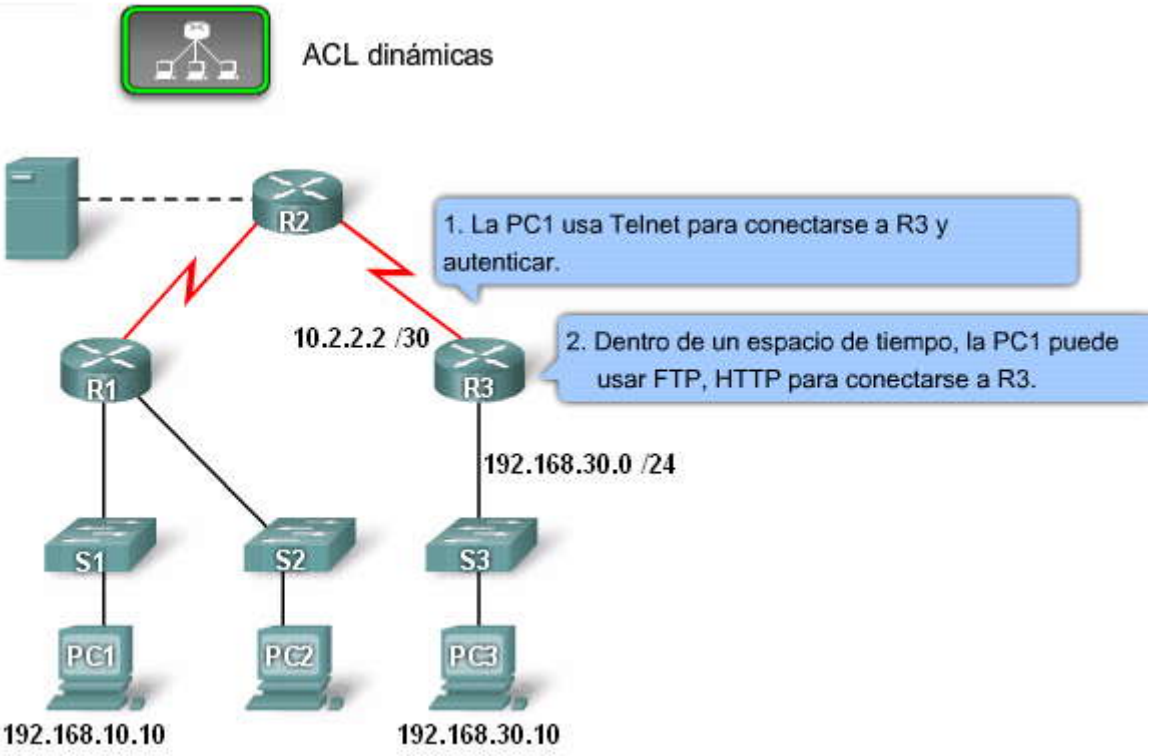


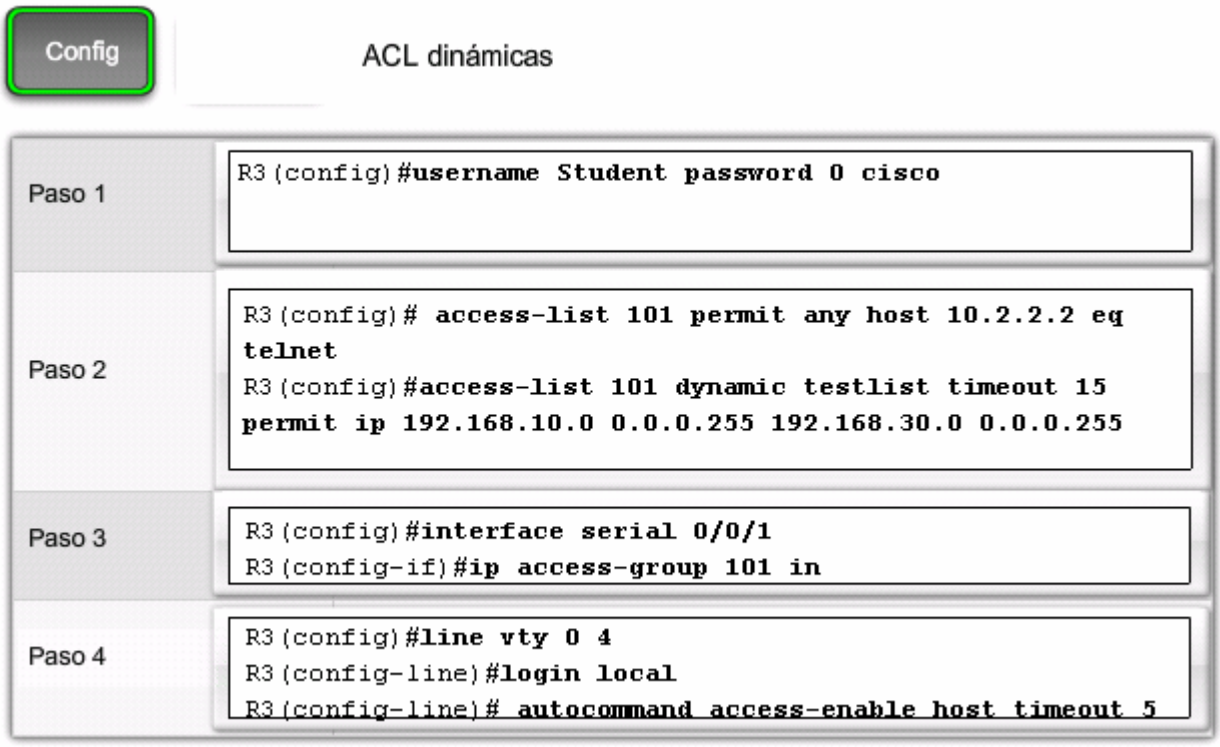
Ejemplos de ACL dinámicas

Considere un requerimiento para que un administrador de red en PC1 obtenga acceso periódico a la red (192.168.30.0 /24) a través del router R3. Para facilitar este requerimiento, se configura una ACL dinámica en la interfaz serial S0/0/1 del router R3.

Si bien la descripción detallada de la configuración de una ACL dinámica está fuera del alcance de este curso, es útil revisar los pasos de configuración.
Haga clic en el botón Config de la figura para ver un ejemplo de configuración de ACL dinámica.

Pase el cursor del mouse sobre cada Paso que se muestra en la figura para revisar los pasos de configuración de las ACL dinámicas.





5.4.3 ACL reflexivas

¿Qué son las ACL reflexivas?

Las ACL reflexivas obligan al tráfico de respuesta del destino, de un reciente paquete saliente conocido, a dirigirse al origen de ese paquete saliente. Esto aporta un mayor control del tráfico que se permite ingresar a la red e incrementa las capacidades de las listas de acceso extendidas.

Los administradores de red utilizan las ACL reflexivas para permitir el tráfico IP en sesiones que se originan en su red y, al mismo tiempo, denegar el tráfico IP en sesiones que se originan fuera de la red. Estas ACL permiten que el router administre el tráfico de sesión en forma dinámica. El router examina el tráfico saliente y, cuando ve una conexión, agrega una entrada a una ACL temporal para permitir la devolución de respuestas. Las ACL reflexivas contienen sólo entradas temporales. Estas entradas se crean automáticamente cuando se inicia una nueva sesión IP (con un paquete saliente, por ejemplo) y las entradas se eliminan automáticamente cuando finaliza la sesión.

Las ACL reflexivas proporcionan una forma más exacta de filtrado de sesión que una ACL extendida que utiliza el parámetro **established** presentado anteriormente. Si bien son similares en cuanto al concepto del parámetro **established**, las ACL reflexivas también funcionan para UDP e ICMP, que no tienen bits ACK ni RST. La opción **established** tampoco funciona con aplicaciones que alteran de forma dinámica el puerto de origen para el tráfico de sesión. La sentencia **permit established** sólo verifica los bits ACK y RST, no la dirección de origen ni la de destino.

Las ACL reflexivas no se aplican directamente a una interfaz, están "anidadas" dentro de una ACL IP extendida nombrada que se aplica a la interfaz.

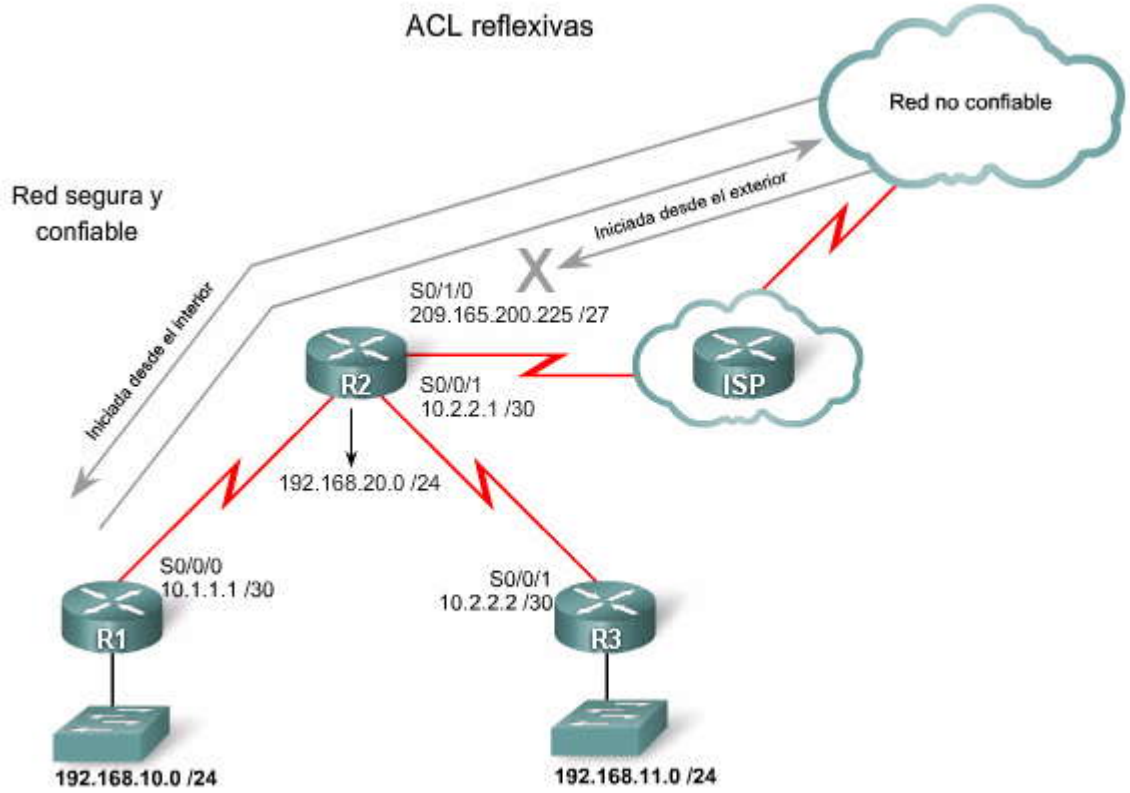
Las ACL reflexivas sólo pueden definirse con ACL IP extendidas nombradas. No pueden definirse con ACL numeradas ni estándar nombradas ni con otras ACL protocolo. Las ACL reflexivas pueden utilizarse con otras ACL estándar y extendidas estáticas.

Beneficios de las ACL reflexivas

Las ACL reflexivas tienen los siguientes beneficios:

- Ayudan a proteger la red de piratas informáticos y pueden incluirse en un firewall.
- Proporcionan un nivel de seguridad contra ataques de suplantación de identidad y de denegación de servicios. Las ACL reflexivas son mucho más resistentes a los ataques de suplantación de identidad porque deben coincidir más criterios de filtro antes de dejar ingresar un paquete. Por ejemplo, se verifican las direcciones de origen y de destino y los números de puerto, no solamente los bits ACK y RST.

- Son fáciles de utilizar y, comparadas con las ACL básicas, proporcionan un mayor control de los paquetes que ingresan a la red.



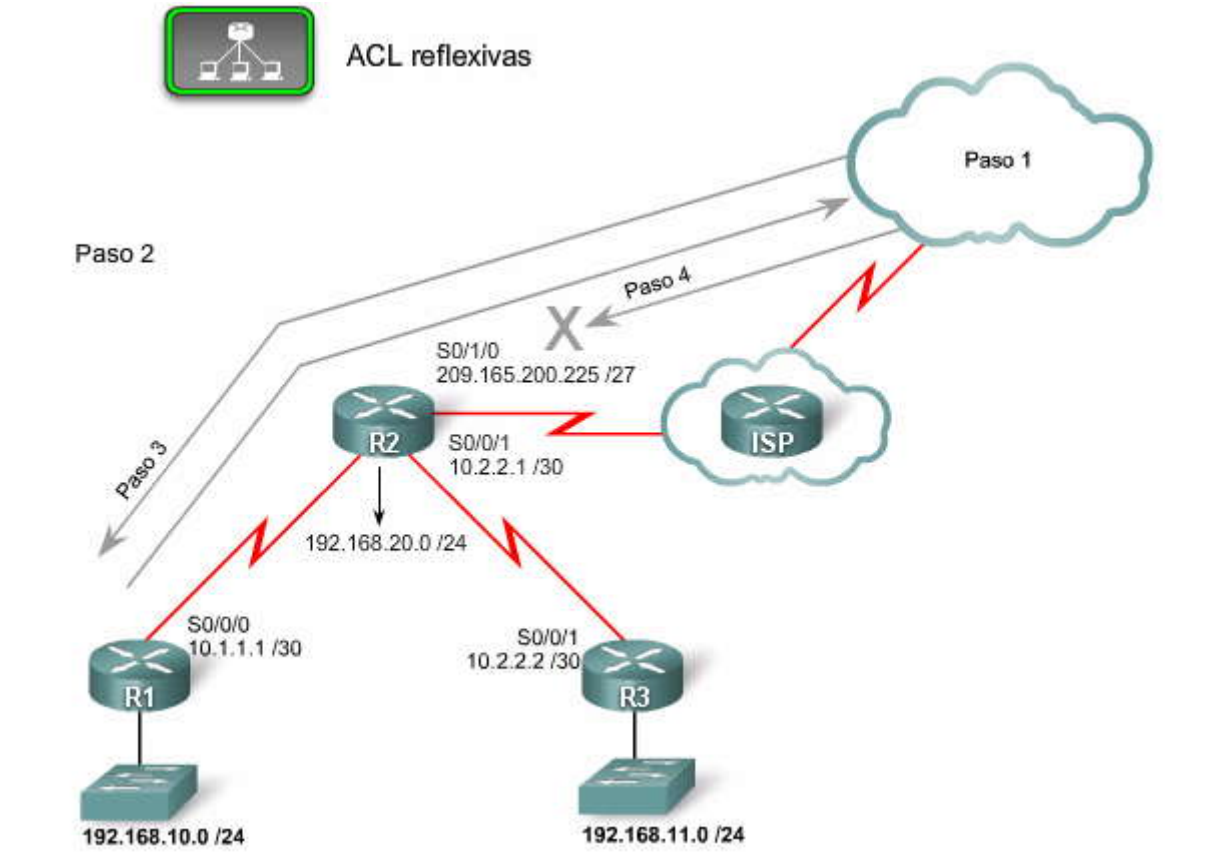
Ejemplo de ACL reflexivas

La figura muestra un ejemplo donde un administrador necesita una ACL reflexiva que permita tráfico ICMP entrante y saliente, y que permita sólo el tráfico TCP que se inició desde el interior de la red. Supongamos que todo el otro trafico será denegado. La ACL reflexiva se aplica a la interfaz de salida de R2.

Haga clic en el botón Config de la figura.

Si bien la configuración completa de las ACL reflexivas está fuera del alcance de este curso, la figura muestra un ejemplo de los pasos necesarios para configurar una ACL reflexiva.

Pase el cursor del mouse sobre cada Paso que se muestra en la figura para revisar los pasos de configuración de las ACL reflexivas.



Config — ACL reflexivas

Paso 1

```
R2(config)#ip access-list extended OUTBOUNDFILTERS
R2(config-ext-nacl)# permit tcp 192.168.0.0 0.0.255.255 any
reflect TCPTRAFFIC
R2(config-ext-nacl)# permit icmp 192.168.0.0 0.0.255.255 any
reflect ICMPTRAFFIC
```

Paso 2

```
R2(config)#ip access-list extended INBOUNDFILTERS
R2(config-ext-nacl)# evaluate TCPTRAFFIC
R2(config-ext-nacl)# evaluate ICMPTRAFFIC
```

Paso 3

```
R2(config)#interface S0/1/0
R2(config-if)#ip access-group INBOUNDFILTERS in
R2(config-if)#ip access-group OUTBOUNDFILTERS out
```

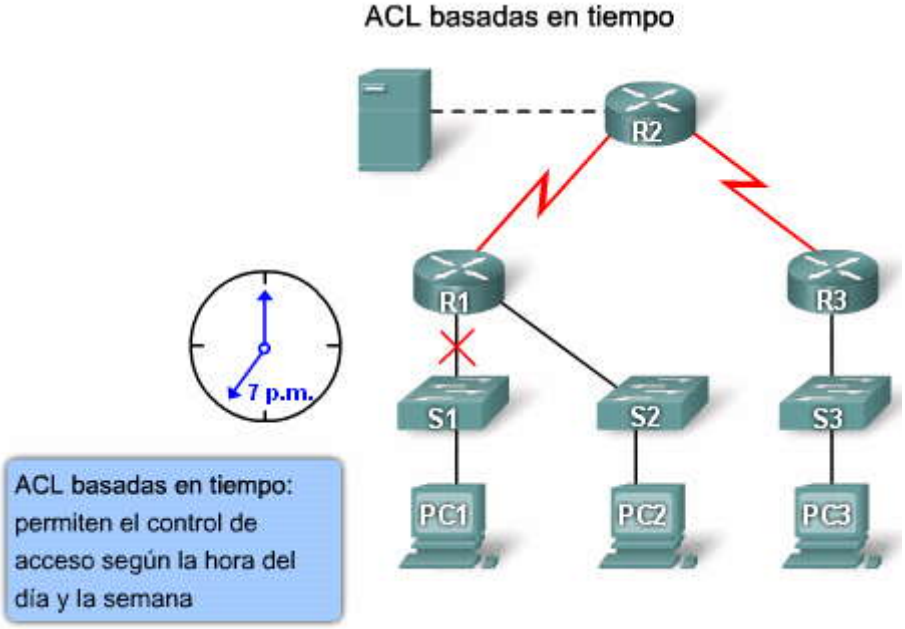
5.4.4 ACL basadas en el tiempo

¿Qué son las ACL basadas en el tiempo?

La ACL basada en el tiempo es similar en función a la ACL extendida, pero admite control de acceso basado en el tiempo. Para implementar las ACL basadas en el tiempo, debe crear un rango horario que defina la hora específica del día y la semana. Debe identificar el rango de tiempo con un nombre y, luego, remitirse a él mediante una función. Las restricciones temporales son impuestas en la misma función.

Las ACL basadas en el tiempo tienen muchos beneficios.

- Ofrecen al administrador de red más control de los permisos y denegaciones de acceso a los recursos.
- Permiten a los administradores de red controlar los mensajes de registro. Las entradas de las ACL pueden registrar el tráfico en determinados momentos del día, pero no de forma permanente. De esta manera, los administradores pueden simplemente denegar el acceso, sin tener que analizar los diferentes registros que se generan durante las horas pico.



Ejemplo de ACL basadas en tiempo

Si bien los detalles de la configuración completa de las ACL basadas en tiempo están fuera del alcance de este curso, el siguiente ejemplo muestra los pasos necesarios. En el ejemplo, se permite una conexión Telnet desde la red interna hacia la red externa los lunes, miércoles y viernes durante el horario comercial.

Haga clic en el botón Config de la figura.

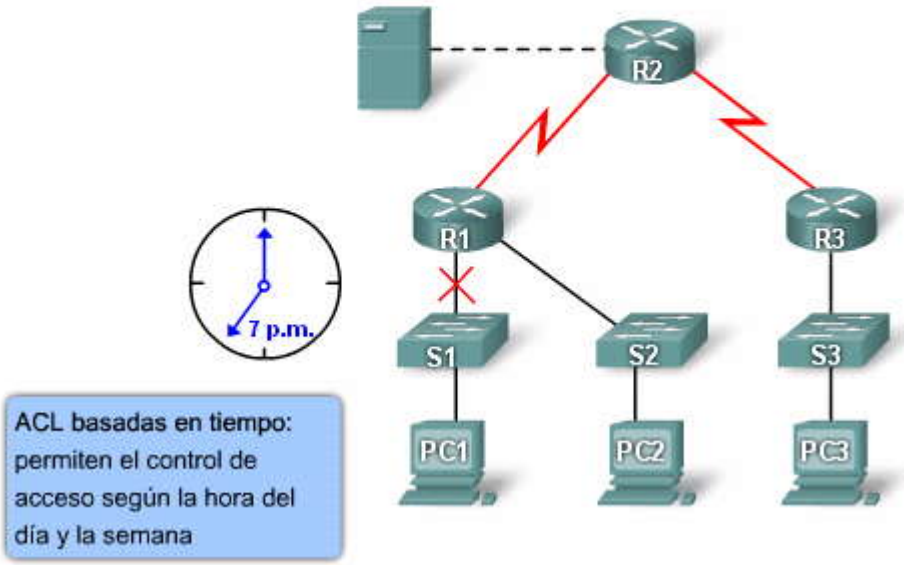
Paso 1. Defina el rango de tiempo para implementar la ACL y darle el nombre EVERYOTHERDAY, en este caso.

Paso 2. Aplique el rango de tiempo a la ACL.

Paso 3. Aplique la ACL a la interfaz.

El rango de tiempo depende del reloj del sistema del router. La característica funciona mejor con la sincronización del protocolo de hora de red (NTP), pero puede utilizarse el reloj del router.

ACL basadas en tiempo



Config

ACL basadas en tiempo

Paso 1	R1(config)#**time-range EVERYOTHERDAY** R1(config-time-range)#**periodic Monday Wednesday Friday 8:00 to 17:00**
Paso 2	R1(config)#**access-list 101 permit tcp 192.168.10.0 0.0.0.255 any eq telnet time-range EVERYOTHERDAY**
Paso 3	R1(config)#**interface s0/0/0** R1(config-if)#**ip access-group 101 out**

5.4.5 Resolución de problemas relacionados con los errores comunes de las ACL

El uso de los comandos **show** descritos anteriormente revela la mayoría de los errores más comunes de las ACL antes de que causen problemas en su red. Afortunadamente, el usuario utiliza un buen procedimiento de prueba para proteger su red de errores durante la etapa de desarrollo de la implementación de las ACL.

Cuando observe una ACL, compárela con las reglas que aprendió sobre la creación correcta de ACL. La mayoría de los errores se produce porque se omiten las reglas básicas. De hecho, los errores más comunes suceden al ingresar las sentencias de ACL en el orden incorrecto y sin aplicar un criterio adecuado de las reglas.

Observemos una serie de problemas comunes y sus soluciones. Haga clic en cada ejemplo mientras lee las explicaciones.

Haga clic en el botón Error 1 que se muestra en la figura.

El host 192.168.10.10 no tiene conectividad con 192.168.30.12. ¿Puede ver el error en el resultado del comando **show access-lists**?

Solución: observe el orden de las sentencias de ACL. El host 192.168.10.10 no tiene conectividad con 192.168.30.12 por el orden de la regla 10 de la lista de acceso. Debido a que el router procesa las ACL de arriba hacia abajo, la sentencia 10 deniega el host 192.168.10.10 y la sentencia 20 no llega a procesarse. Las sentencias 10 y 20 deben aparecer invertidas. La última línea permite todo el otro tráfico que no sea TCP que esté clasificado como IP (ICMP, UDP, etc.).

Haga clic en el botón Error 2 que se muestra en la figura.

La red 192.168.10.0 /24 no puede usar TFTP para conectarse a la red 192.168.30.0 /24. ¿Puede ver el error en el resultado del comando **show access-lists**?

Solución: la red 192.168.10.0 /24 no puede usar TFTP para conectarse a la red 192.168.30.0 /24 porque TFTP utiliza el protocolo de transporte UDP. La sentencia 30 de la lista de acceso 120 permite el resto del tráfico TCP. Como TFTP utiliza UDP, está implícitamente denegado. La sentencia 30 debe ser **ip any any**.

Esta ACL funciona si se aplica a Fa0/0 de R1 o a S0/0/1 de R3, o a S0/0/0 o a R2 en dirección entrante. Sin embargo, según la regla que indica ubicar las ACL extendidas lo más cerca del origen, la mejor opción es en Fa0/0 de R1 porque permite que el tráfico no deseado se filtre sin atravesar la infraestructura de la red.

Haga clic en el botón Error 3 que se muestra en la figura.

La red 192.168.10.0 /24 puede usar Telnet para conectarse a 192.168.30.0 /24, pero no se permite esta conexión. Analice el resultado del comando **show access-lists** e intente encontrar una solución. ¿Dónde aplicaría esta ACL?

Solución: la red 192.168.10.0 /24 puede usar Telnet para conectarse a la red 192.168.30.0 /24 porque el número de puerto Telnet en la sentencia 10 de la lista de acceso 130 aparece en la ubicación incorrecta. La sentencia 10 actualmente deniega cualquier origen con un número de puerto igual al de Telnet que intente establecer una conexión a cualquier dirección IP. Si desea denegar el tráfico Telnet que ingresa a S0, debe denegar el número de puerto de destino igual al de Telnet, por ejemplo, **deny tcp any any eq telnet**.

Haga clic en el botón Error 4 que se muestra en la figura.

El host 192.168.10.10 puede usar Telnet para conectarse a 192.168.30.12, pero no se permite esta conexión. Analice el resultado del comando **show access-lists**.

Solución: el host 192.168.10.10 puede usar Telnet para conectarse a 192.168.30.12 porque no hay reglas que denieguen el host 192.168.10.10 o su red como el origen. La sentencia 10 de la lista de acceso 140 deniega la interfaz del router desde donde parte el tráfico. Sin embargo, como estos paquetes parten del router, tienen una dirección de origen de 192.168.10.10 y no la dirección de la interfaz del router.

Como la solución para el Error 2, esta ACL debe aplicarse a Fa0/0 de R1 en dirección entrante.

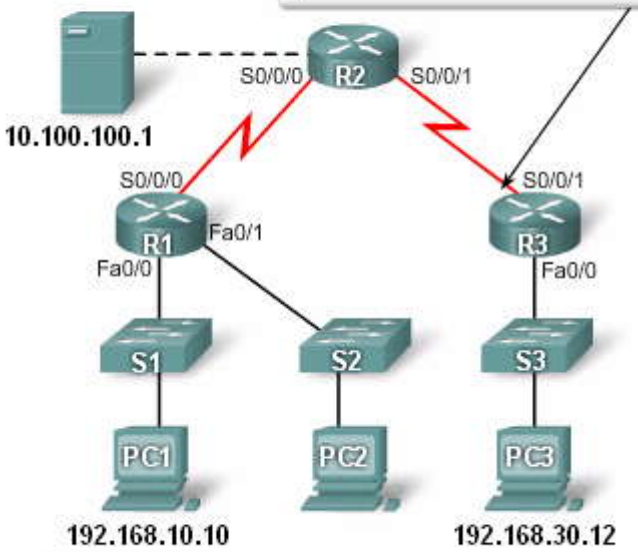
Haga clic en el botón Error 5 que se muestra en la figura.

El host 192.168.30.12 puede usar Telnet para conectarse a 192.168.10.10, pero no se permite esta conexión. Observe el resultado del comando **show access-lists** y encuentre el error.

Solución: el host 192.168.30.12 puede usar Telnet para conectarse a 192.168.10.10 por la dirección en la que se aplica la lista de acceso 150 a la interfaz S0/0. La sentencia 10 deniega la dirección de origen de 192.168.30.12, pero esa dirección sólo sería el origen si el tráfico fuera saliente y no entrante en la interfaz S0/0.

Resolución de problemas relacionados con los errores comunes de las ACL

```
# show access-lists 110
Extended IP access list 110
    10 deny tcp 192.168.10.0 0.0.0.255 any
    20 permit tcp 192.168.10.0 0.0.0.255 any eq telnet
    30 permit ip any any
```

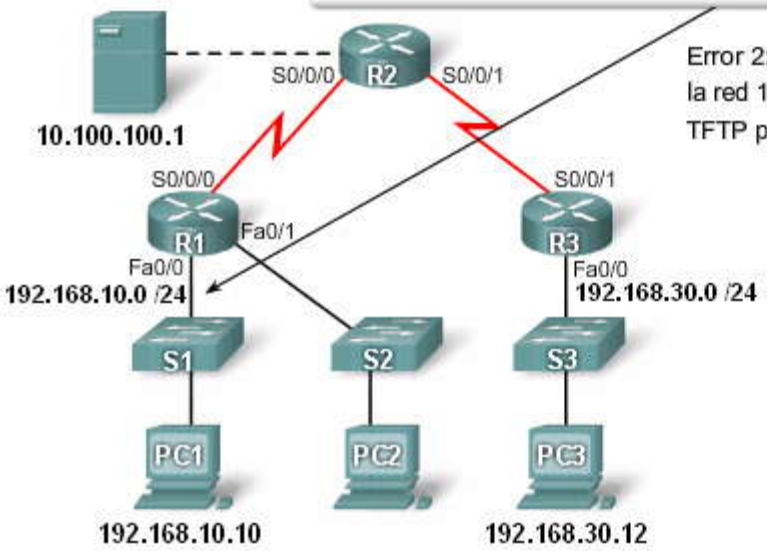


Error 1:
el host 192.168.10.10 no tiene conectividad con 192.168.30.12

Error No. 1

Resolución de problemas relacionados con los errores comunes de las ACL

```
# show access-lists 120
Extended IP access list 120
    10 deny tcp 192.168.10.0 0.0.255.255 any eq telnet
    20 deny tcp 192.168.10.0 0.0.0.255 host 10.100.100.1 eq smtp
    30 permit tcp any any
```

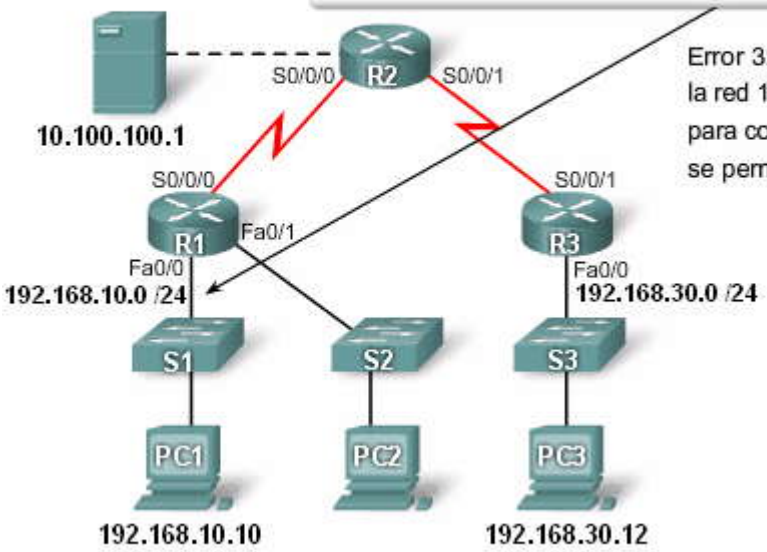


Error 2:
la red 192.168.10.0 /24 no puede usar TFTP para conectarse a 192.168.30.0 /24.

Error No. 2

Resolución de problemas relacionados con los errores comunes de las ACL

```
# show access-lists 130
Extended IP access list 130
    10 deny tcp any eq telnet any
    20 deny tcp 192.168.1.0 0.0.0.255 host 192.168.30.0 eq smtp
    30 permit ip any any
```

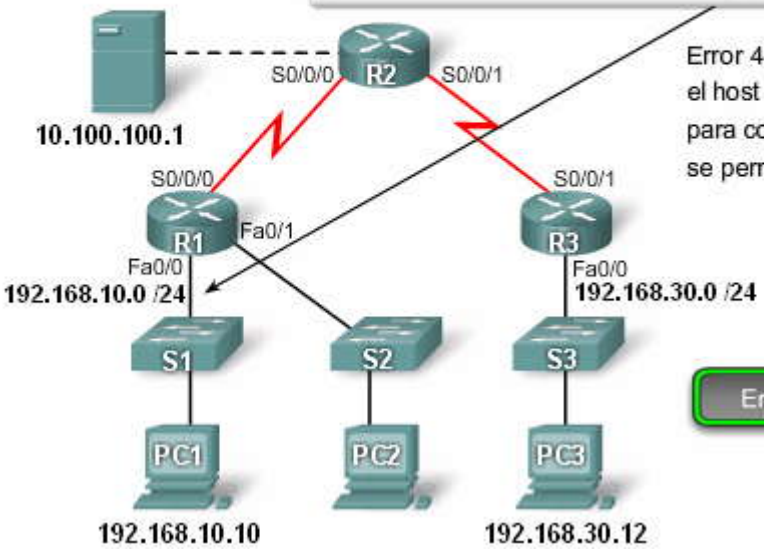


Error 3:
la red 192.168.10.0 /24 puede usar Telnet para conectarse a 192.168.30.0 /24, pero no se permitirá esta conexión.

Error No. 3

Resolución de problemas relacionados con los errores comunes de las ACL

```
# show access-lists 140
Extended IP access list 140
10 deny tcp host 192.168.10.1 any eq telnet
   20 deny tcp 192.168.1.0 0.0.0.255 host 10.100.100.1 eq smtp
   30 permit ip any any
```

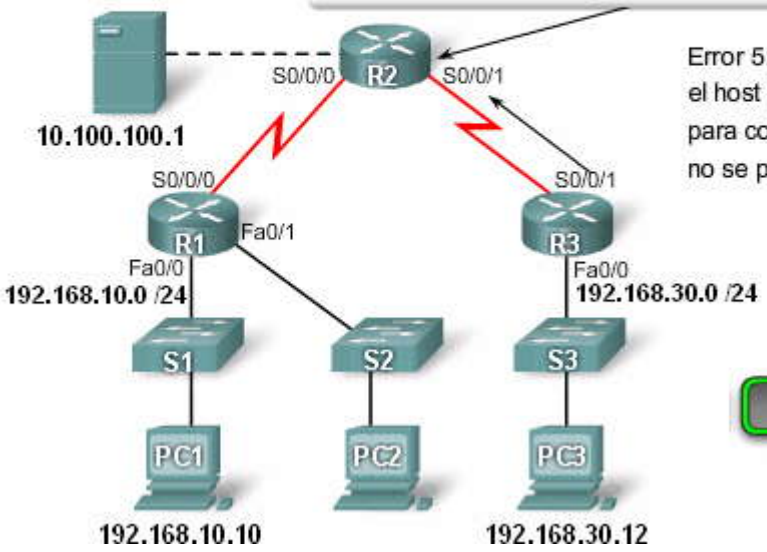


Error 4:
el host 192.168.10.10 puede usar Telnet para conectarse a 192.168.30.12, pero no se permitirá esta conexión.

Error No. 4

Resolución de problemas relacionados con los errores comunes de las ACL

```
# show access-lists 150
Extended IP access list 150
    10 deny tcp host 192.168.30.12 any eq telnet
    20 permit ip any any
```



Error 5:
el host 192.168.30.12 puede usar Telnet para conectarse a 192.168.10.10, pero no se permitirá esta conexión.

Error No. 5

Actividad

Complete los siguientes pasos para que Hannah acceda al servidor TFTP a través de una ACL dinámica.

Paso 1: Configure una contraseña que Hannah pueda usar al conectarse mediante Telnet con R2

Paso 2: Configure una ACL dinámica denominada LETMEIN para permitir el acceso de la dirección IP de Hannah.

Paso 3: Aplique LETMEIN a la interfaz S0/0/0

Paso 4: Configure las líneas de Telnet para el inicio de sesión y autocommand timeout.

Arrastre y coloque estas partes del comando para completar la configuración de las ACL dinámicas que aparece arriba.


```
R2(config)#  username hannah password itsasecret
R2(config)#  access-list 101 permit tcp  host 192.168.10.10  host 10.1.1.2
             eq telnet
R2(config)#  access-list 101 dynamic LETMEIN  timeout 90  permit ip
             host 192.168.10.10  host 192.168.20.254
R2(config)#  interface s0/0/0
R2(config-if)#  ip access-group 101 in
R2(config-if)#  line vty 0 5
R2(config-line)#  login local
R2(config-line)#  autocommand access-enable host timeout 2
R2(config-line)#end
```

Actividad

Una ACL dinámica es una característica del IOS que permite a los usuarios abrir un agujero temporal en una ACL existente.

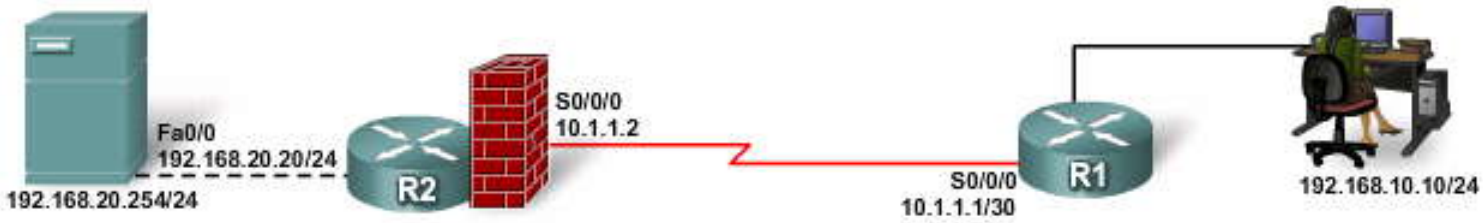
Primero el usuario se conecta al router mediante Telnet y se autentica.

Si logra hacerlo con éxito, la sesión de Telnet finaliza y se crea el agujero.

Una vez que lo abre, el usuario tiene acceso a los servicios que de otra manera estarían denegados.

La inactividad o superación del tiempo de espera puede configurarse en el router.

En este ejemplo, Hannah abrirá un agujero en el firewall de R2. Arrastre y coloque los pasos en la secuencia correcta.



Coloque estos pasos en el orden correcto arriba.

1. Abra la sesión de Telnet desde 192.168.10.10
2. Nombre de usuario y contraseña
3. Usuario: hannah; contraseña: itsasecret
4. hannah es un usuario válido
5. Cierre la sesión de Telnet
6. ¡El agujero en el firewall ya está abierto!
7. Permita 192.168.10.10 a cualquier IP hasta superar el tiempo de espera

Actividad 1

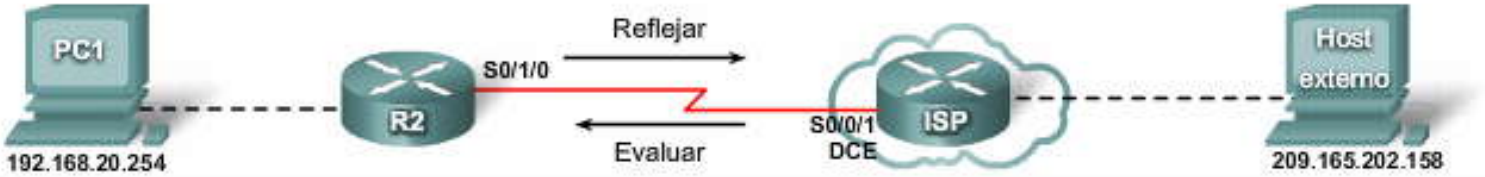
Actividad

Las ACL reflexivas generan una nueva entrada temporal que permite que el tráfico ingrese a su red si el tráfico es parte de una sesión iniciada por un origen interno.

El método de la ACL reflexiva es mucho más resistente a los ataques de suplantación de identidad porque deben coincidir más criterios de filtrado antes de permitir el ingreso de un paquete.

Las ACL reflexivas pueden filtrar tráfico IP independientemente de que el tráfico utilice TCP, UDP o cualquier otro protocolo de Internet. Se verifican las direcciones de origen y de destino y los números de puerto.

Utilice las opciones de las ACL extendidas denominadas **reflect** y **evaluate** para configurar una ACL reflexiva.




```
R2(config)#ip access-list extended FILTER_OUT
R2(config-ext-nacl)# [permit ip any any] [reflect GOODGUYS]
R2(config-ext-nacl)#exit
R2(config)#ip access-list extended FILTER_IN
R2(config-ext-nacl)# [evaluate] [GOODGUYS]
R2(config-ext-nacl)#exit
R2(config)#interface s0/1/0
R2(config-if)# [ip access-group FILTER_OUT] out
R2(config-if)# [ip access-group FILTER_IN] in
```

Arrastre y coloque estas partes del comando para completar la configuración de las ACL reflexivas que aparece arriba.

Actividad

Las ACL basadas en tiempo son similares a las ACL extendidas en cuanto a su función, pero permiten el control de acceso basado en el tiempo.

Para implementar las ACL basadas en tiempo, usted crea un rango de tiempo que defina el tiempo específico del día y la semana.

Usted identifica el rango de tiempo con un nombre y luego se remite a él mediante una ACL denominada.

Configure R2 para bloquear la salida del tráfico Web a Internet durante el horario comercial de 7:00 a.m. a 6:00 p.m. (18:00) durante la semana.

El tráfico saliente a Internet es denegado durante el horario comercial.

```
R2(config)#                 time-range NO_WEB
R2(config-time-range)#      días de la semana periódicos de 7:00 a 18:00
R2(config-ext-nacl)#exit
R2(config)#                 ip access-list extended WEB_ACCESS
R2(config-ext-nacl)#        deny tcp any any eq 80        time-range NO_WEB
R2(config-ext-nacl)#        permit ip any any
R2(config-ext-nacl)#exit
R2(config)#interface s0/1/0
R2(config-if)#              ip access-group WEB_ACCESS out
```

Arrastre y coloque estas partes del comando para completar la configuración de las ACL basadas en tiempo que aparece arriba.

CAPITULO VI – "Servicios de trabajadores a distancia"

6.0 Introducción del capítulo

6.0.1 Introducción del capítulo

El trabajo a distancia significa trabajar lejos de un lugar de trabajo tradicional, a menudo desde una oficina doméstica. Los motivos para la elección del trabajo a distancia son variados e incluyen todo, desde la conveniencia personal hasta las oportunidades que se les otorgan a los empleados con lesiones o discapacidades de seguir trabajando durante los períodos de convalecencia.

El trabajo a distancia es un término amplio que hace referencia a realizar un trabajo mediante la conexión al lugar de trabajo desde una ubicación remota, con la ayuda de las telecomunicaciones. El trabajo a distancia eficaz es posible debido a conexiones de Internet de banda ancha, redes privadas virtuales (VPN) y tecnologías más avanzadas, incluidas Voz sobre IP (VoIP) y videoconferencias. El trabajo a distancia permite ahorrar dinero que de otro modo se gasta en viajes, infraestructura y soporte de instalaciones.

Las empresas modernas emplean a quienes no pueden trasladarse al trabajo todos los días o para quienes es más práctico trabajar desde una oficina doméstica. Estas personas, denominadas trabajadores a distancia, deben conectarse a la red de la empresa para poder trabajar desde sus oficinas domésticas.

Este capítulo explica cómo las organizaciones pueden brindar conexiones de red remotas confiables, rápidas y seguras para los trabajadores a distancia.

En este capítulo, aprenderá a:

- Describir los requisitos empresariales para proporcionar servicios de trabajadores a distancia, incluidas las diferencias entre las infraestructuras de red privada y pública.
- Describir los requisitos de trabajo a distancia y la arquitectura recomendada para proporcionar servicios de trabajo a distancia.
- Explicar cómo los servicios de banda ancha extienden las redes empresariales mediante DSL, cable y la tecnología inalámbrica.
- Describir la importancia de la tecnología VPN, incluido su rol y sus beneficios para empresas y trabajadores a distancia.
- Describir cómo la tecnología VPN se puede utilizar para proporcionar a una red empresarial servicios seguros de trabajo a distancia.

6.1 Requisitos comerciales para los servicios de trabajo a distancia

6.1.1 Los requisitos comerciales para los servicios de trabajo a distancia

Cada vez más empresas consideran beneficioso tener trabajadores a distancia. Con los avances en las tecnologías de conexiones de banda ancha e inalámbricas, el trabajo lejos de la oficina ya no presenta los mismos desafíos que en el pasado. Los empleados pueden trabajar de manera remota casi como si estuvieran en el despacho o la oficina de al lado. Las organizaciones pueden distribuir de manera rentable aplicaciones de datos, voz, video y en tiempo real a través de una conexión de red común que alcance a todos los empleados, sin importar cuán lejos o separados estén.

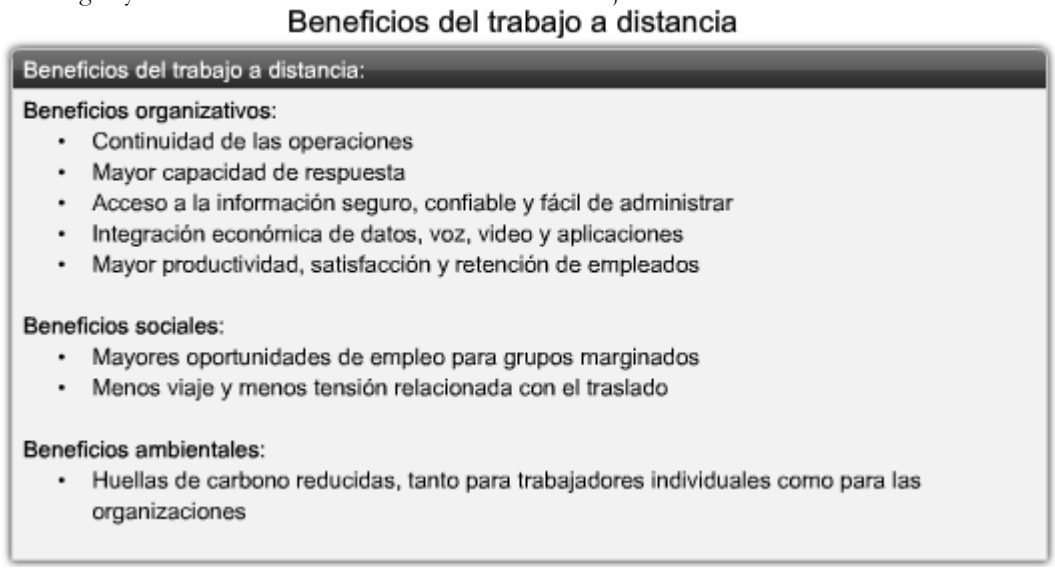
Las ventajas del trabajo a distancia se extienden mucho más allá de la habilidad de las empresas para obtener ganancias. El trabajo a distancia afecta la estructura social de las sociedades y puede tener efectos positivos en el medioambiente.

Para las operaciones comerciales de todos los días, es una ventaja poder mantener la continuidad en casode que el clima, la congestión del tráfico, los desastres naturales u otros eventos impredecibles les impidan a los empleados llegar al lugar de trabajo. En una escala más amplia, la habilidad de las empresas para proporcionar un aumento en el servicio a través de zonas horarias y los límites internacionales se mejora notablemente por medio de los trabajadores a distancia. Las soluciones de contratación y subcontratación de terceros son más fáciles de implementar y administrar.

Desde una perspectiva social, las opciones de trabajo a distancia aumentan las oportunidades de empleo para varios grupos; entre ellos, padres con hijos pequeños, discapacitados y personas que viven en áreas lejanas. Los trabajadores a distancia disfrutan de más tiempo de calidad con su familia, menos estrés generado por los viajes y, en general, proporcionan a sus empleadores una mayor productividad, satisfacción y retención. En la época de cambios climáticos, el trabajo a distancia representa otra manera en la que las personas pueden reducir la cantidad de dióxido de carbono.

Cuando se diseñan las arquitecturas de redes que admiten una solución de trabajo a distancia, los diseñadores deben lograr un equilibrio entre los requisitos de la organización de seguridad, administración de infraestructura, escalabilidad y viabilidad económica, y las necesidades prácticas de los trabajadores a distancia de facilidad de uso, velocidades de conexión y fiabilidad del servicio.

Para permitir que las empresas y los trabajadores a distancia funcionen de manera eficaz, debemos equilibrar la selección de tecnologías y diseñar cuidadosamente los servicios de trabajo a distancia.



6.1.2 La solución del trabajador a distancia

Las organizaciones necesitan redes seguras, confiables y rentables para conectar sedes corporativas, sucursales y proveedores. Con el aumento en la cantidad de trabajadores a distancia, las empresas tienen una creciente necesidad de maneras seguras, confiables y rentables de conectar a las personas que trabajan en pequeñas oficinas y oficinas domésticas (SOHO) y otras ubicaciones remotas, con los recursos existentes en las oficinas corporativas.

La figura muestra las topologías de las conexiones remotas que usan las redes modernas para conectar las ubicaciones remotas. En algunos casos, las ubicaciones remotas sólo se conectan a las sedes, mientras que en otros, las ubicaciones remotas se conectan a varios lugares. La sucursal que aparece en la figura se conecta a la sede central y las oficinas de los socios, mientras que el trabajador a distancia tiene una sola conexión a la sede central.

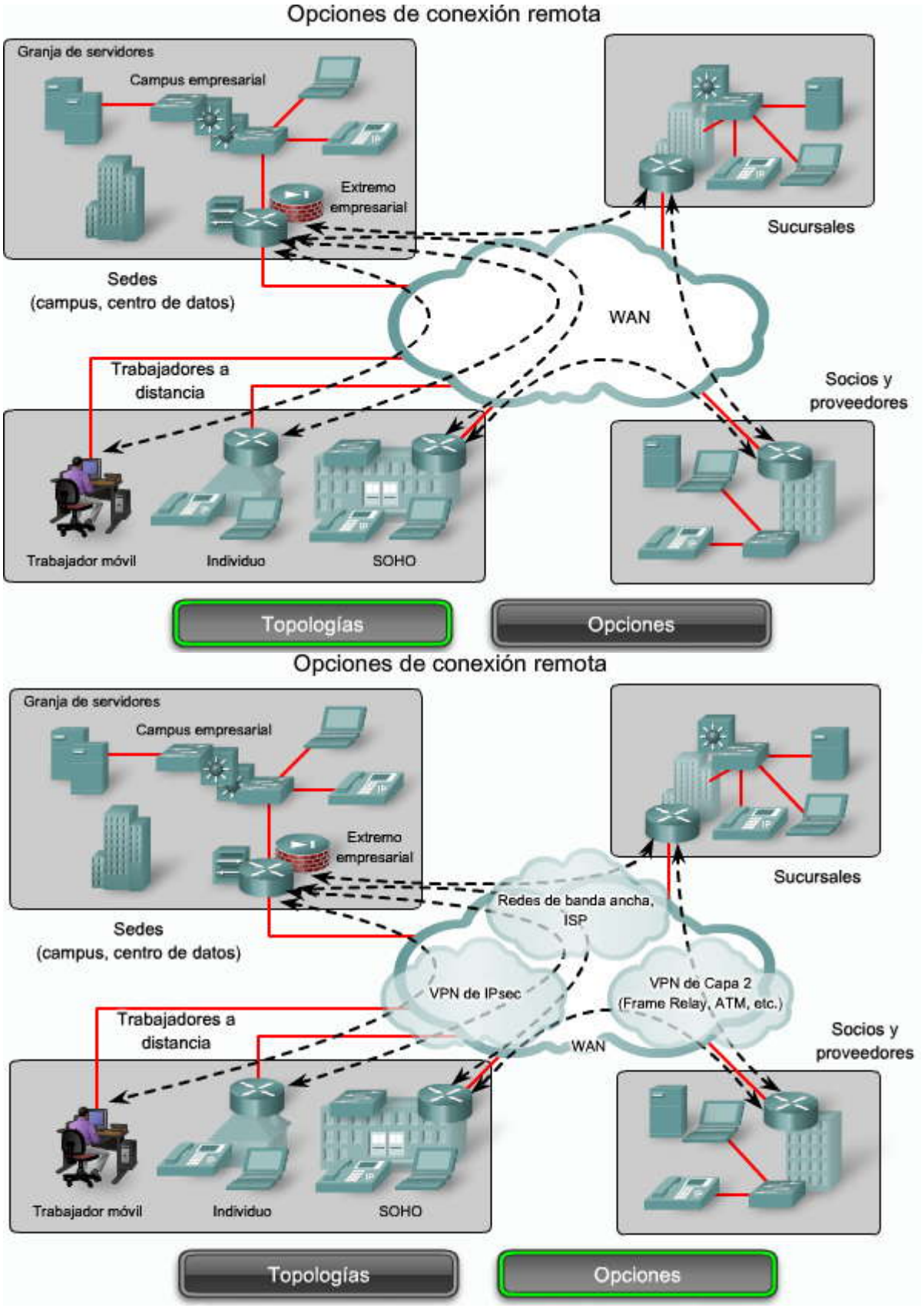
Haga clic en el botón Opciones de la figura.

La figura muestra tres tecnologías de conexiones remotas disponibles para organizaciones a fin de admitir los servicios de trabajadores a distancia:

- Las tecnologías de Capa 2 de WAN privada tradicionales, que incluyen Frame Relay, ATM y líneas alquiladas, proporcionan muchas soluciones para conexiones remotas. La seguridad de estas conexiones depende del proveedor del servicio.
- Las redes privadas virtuales (VPN) con IPSec ofrecen conectividad flexible y escalable.
- Las conexiones de sitio a sitio pueden brindar una conexión remota confiable, rápida y segura para los trabajadores a distancia. Ésta es la opción mas frecuente para los trabajadores a distancia, combinada con el acceso remoto por banda ancha, para obtener una VPN segura a través de Internet pública. (Un medio de conectividad menos confiable que usa Internet es la conexión de acceso telefónico.)

El término banda ancha hace referencia a los sistemas avanzados de comunicaciones capaces de proporcionar una transmisión de servicios de alta velocidad como datos, voz y video, a través de Internet y otras redes. Un amplio rango de tecnologías proporciona la transmisión, incluida la línea de suscriptor digital (DSL) y el cable de fibra óptica, el cable coaxial, la tecnología inalámbrica y de satélite. Las velocidades de transmisión de datos del servicio de banda ancha, en general, superan los 200 kilobits por segundo (kbps), en al menos una dirección: descendente (desde Internet a la computadora del usuario) o ascendente (desde la computadora del usuario a Internet).

Este capítulo describe cómo funciona cada una de estas tecnologías y presenta algunos de los pasos necesarios para garantizar que las conexiones del trabajador a distancia estén seguras.



Para conectarse efectivamente a las redes de la organización, los trabajadores a distancia necesitan dos conjuntos de componentes clave: componentes de la oficina doméstica y componentes corporativos. La opción de incorporar componentes de telefonía IP se está volviendo más común debido a que los proveedores extienden los servicios de banda ancha a más áreas. Pronto, los componentes de voz sobre IP (VoIP) y videoconferencias serán parte esperada de las herramientas de los trabajadores a distancia.

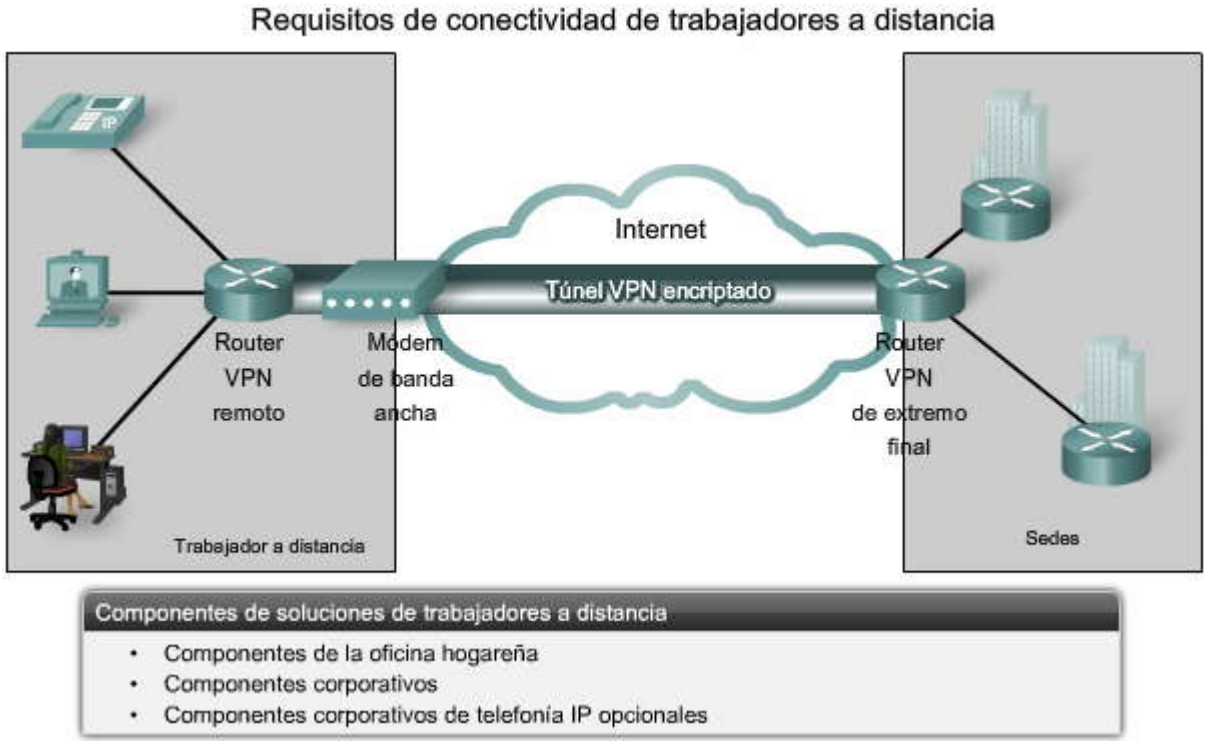
Como se muestra en la figura, el trabajo a distancia requiere de los siguientes componentes:

- Componentes de la oficina doméstica: los componentes de la oficina doméstica requeridos son una laptop o PC, acceso a banda ancha (cable o DSL) y un router VPN o software diente de VPN instalado en la computadora. Algunos componentes adicionales podrían incluir un punto de acceso inalámbrico. Durante los viajes, los trabajadores a distancia necesitan una conexión a Internet y un cliente VPN para conectarse a la red corporativa por medio de cualquier conexión de banda ancha, red o acceso telefónico disponible.
- Componentes corporativos: los componentes corporativos son routers con capacidad de VPN, concentradores VPN, aplicaciones de seguridad de varias funciones, autenticación y dispositivos de administración central para la unificación y la terminación flexibles de las conexiones VPN.

En general, la provisión de asistencia técnica para VoIP y videoconferencia requiere actualizaciones de estos componentes. Los routers necesitan la funcionalidad de calidad de servicio (QoS). La calidad de servicio se refiere a la capacidad de una red de proporcionar un mejor servicio para el tráfico de la red seleccionado, como lo requieren las aplicaciones de voz y video. El análisis detallado de la calidad de servicio (QoS) no se encuentra dentro del alcance de este curso.

La figura muestra un túnel VPN encriptado que conecta al trabajador a distancia con la red corporativa. Éste es el centro de las conexiones seguras y confiables del trabajador a distancia. La VPN es una red privada de datos que usa la infraestructura pública de telecomunicaciones. La seguridad de la VPN mantiene la privacidad mediante un protocolo de tunneling y procedimientos de seguridad.

Este curso presenta el protocolo IPSec (Seguridad IP) como el enfoque elegido para la construcción de túneles VPN seguros. A diferencia de los enfoques anteriores de seguridad que aplican la seguridad en la capa de aplicación del modelo de Interconexión de sistema abierto (OSI), IPSec funciona en la red o en la capa de procesamiento de paquetes.



6.2 Servicios de banda ancha

6.2.1 Conexión a la WAN de los trabajadores a distancia

Los trabajadores a distancia, a menudo, usan distintas aplicaciones (por ejemplo, correo electrónico, aplicaciones Web, aplicaciones críticas, colaboración en tiempo real, voz, video y videoconferencias) que requieren una conexión de un ancho de banda elevado. La elección de la tecnología de red de acceso y la necesidad de garantizar el ancho de banda adecuado son las primeras consideraciones que deben tenerse en cuenta cuando se conecta a los trabajadores a distancia.

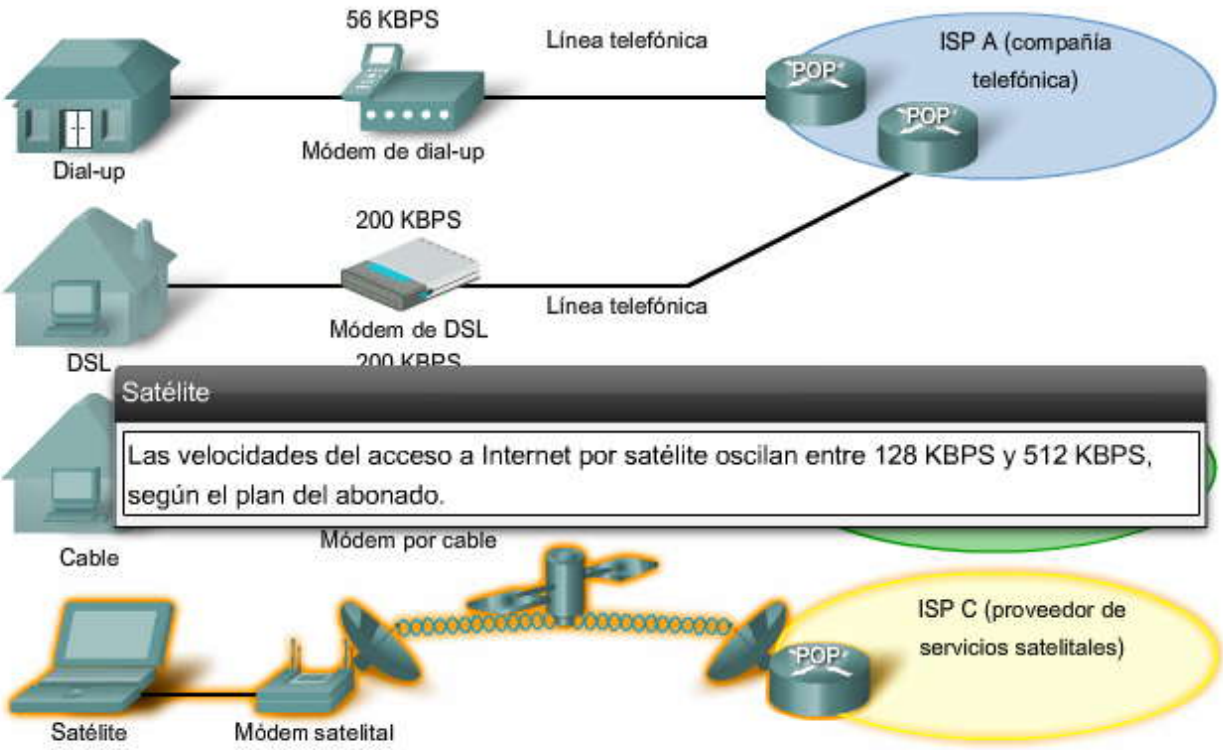
El cable residencial, DSL y el acceso inalámbrico de banda ancha son tres opciones que proporcionan un ancho de banda elevado a los trabajadores a distancia. El ancho de banda bajo proporcionado por una conexión dial-up por módem no es suficiente, aunque resulta útil para el acceso móvil cuando se está de viaje. Una conexión dial-up por módem sólo debe considerarse cuando no hay otras opciones disponibles.

Para acceder a Internet, los trabajadores a distancia necesitan una conexión con un ISP. Los ISP ofrecen varias opciones de conexión. Los métodos principales de conexión que utilizan los usuarios domésticos y de pequeñas empresas son los siguientes:

- **Acceso dial-up**: opción económica que utiliza cualquier línea telefónica y un módem. Para conectarse al ISP, el usuario llama al número telefónico de acceso del ISP. Dial-up es la opción más lenta de conexión y, generalmente, los trabajadores móviles la utilizan en zonas donde no están disponibles opciones de conexión de mayor velocidad.
- **DSL**: generalmente, es más costoso que el dial-up, pero ofrece una conexión más rápida. El DSL también utiliza líneas telefónicas, pero a diferencia del acceso dial-up, el DSL proporciona una conexión continua a Internet. La opción de DSL emplea un módem especial de alta velocidad que separa la señal de DSL de la señal telefónica y proporciona una conexión Ethernet a una computadora host o LAN.
- **Módem por cable**: los proveedores del servicio de televisión por cable ofrecen esta opción. La señal de Internet es transportada en el mismo cable coaxial que suministra televisión por cable. Un módem por cable especial separa la señal de Internet de las otras señales transportadas en el cable y proporciona una conexión Ethernet a una computadora host o LAN.
- **Satélite**: los proveedores del servicio de satélite ofrecen esta opción. La computadora se conecta a través de Ethernet a un módem satelital que transmite señales de radio al punto de presencia (POP) más cercano dentro de la red satelital.

En esta sección, aprende de qué manera los servicios de banda ancha, como DSL, cable y acceso inalámbrico de banda ancha, extienden las redes empresariales para permitir el acceso de los trabajadores a distancia.

Conexión a la WAN de los trabajadores a distancia



Coloque el cursor sobre cada tipo de conexión para obtener más información.

6.2.2 Cable

El acceso a Internet a través de una red de cable es una opción frecuente usada por los trabajadores a distancia para acceder a la red empresarial. El sistema de cable usa un cable coaxial que transporta las señales de radiofrecuencia (RF) a través de la red. El cable coaxial es el medio principal usado para construir sistemas de televisión por cable.

La televisión por cable surgió por primera vez en Pensilvania en 1948. John Walson, el dueño de una tienda de electrodomésticos de una pequeña ciudad en las montañas, necesitaba resolver los problemas de la mala recepción por aire que experimentaban los clientes, quienes intentaban recibir la señal de televisión desde Filadelfia a través de las montañas. Walson construyó una antena en un poste de la empresa de servicios públicos ubicado en la cima de una montaña local, que le permitió mostrar los televisores en su tienda con transmisiones potentes que llegaban desde tres estaciones de Filadelfia. Conectó la antena a su tienda de electrodomésticos a través de un cable y un amplificador de señal modificado. Luego,

conectó a varios de sus clientes ubicados a lo largo del recorrido del cable. Éste fue el primer sistema de televisión por antena comunitario (CATV) de los Estados Unidos.

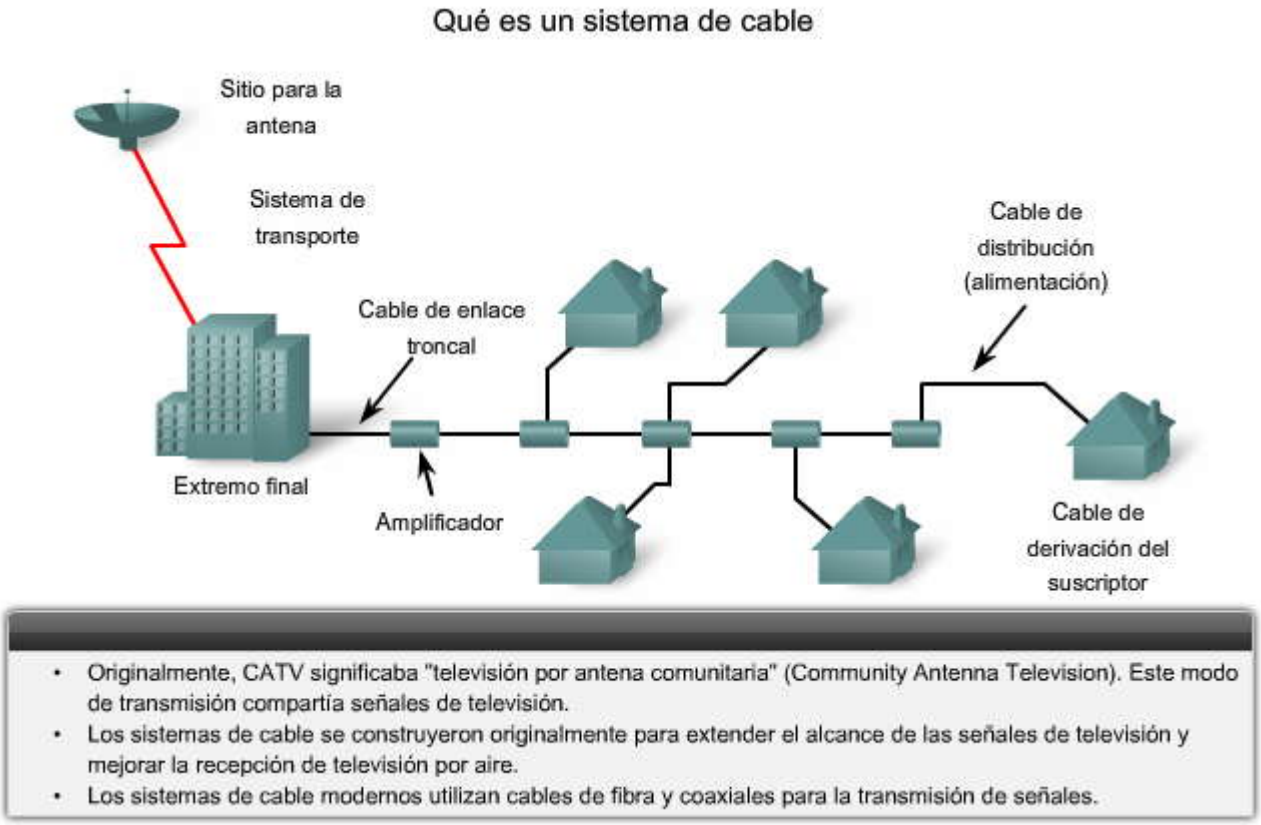
La empresa de Walson creció con los años y a él se lo reconoce como el fundador de la televisión por cable. También, fue el primer operador de cable en usar microondas para importar estaciones de televisión distantes, el primero en usar el cable coaxial para mejorar la calidad de la imagen y el primero en distribuir la programación de la televisión con programación por pago.

La mayor parte de los operadores de cable usan antenas parabólicas para recopilar señales televisivas. Las primeros sistemas eran unidireccionales, con varios amplificadores ubicados en series a lo largo de la red para compensar la pérdida de la señal. Estos sistemas usaban conexiones intermedias para conectar las señales de video del tronco principal a los hogares de los abonados, a través de cables de derivación.

Los sistemas de cable modernos proporcionan una comunicación bidireccional entre los abonados y el operador de cable. Los operadores de cable ofrecen ahora servicios de telecomunicaciones avanzados a los clientes que incluyen acceso a Internet de alta velocidad, televisión digital por cable y servicio de telefonía residencial. Los operadores de cable en general implementan redes de fibra coaxial híbrida (HFC) para permitir la transmisión de datos a alta velocidad a los módems por cable ubicados en las pequeñas oficinas y oficinas domésticas.

La figura muestra los componentes de un típico sistema de cable moderno.

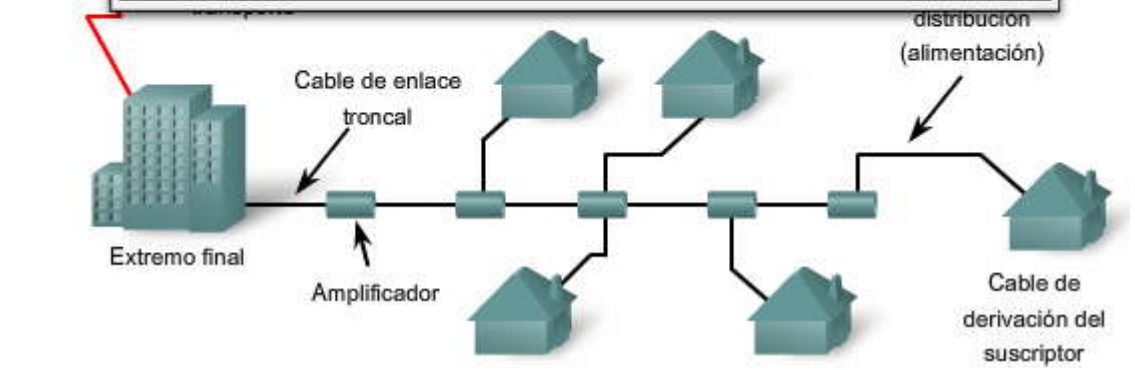
Coloque el cursor sobre cada componente de la figura para ver una descripción de lo que hace.



- Originalmente, CATV significaba "televisión por antena comunitaria" (Community Antenna Television). Este modo de transmisión compartía señales de televisión.
- Los sistemas de cable se construyeron originalmente para extender el alcance de las señales de televisión y mejorar la recepción de televisión por aire.
- Los sistemas de cable modernos utilizan cables de fibra y coaxiales para la transmisión de señales.

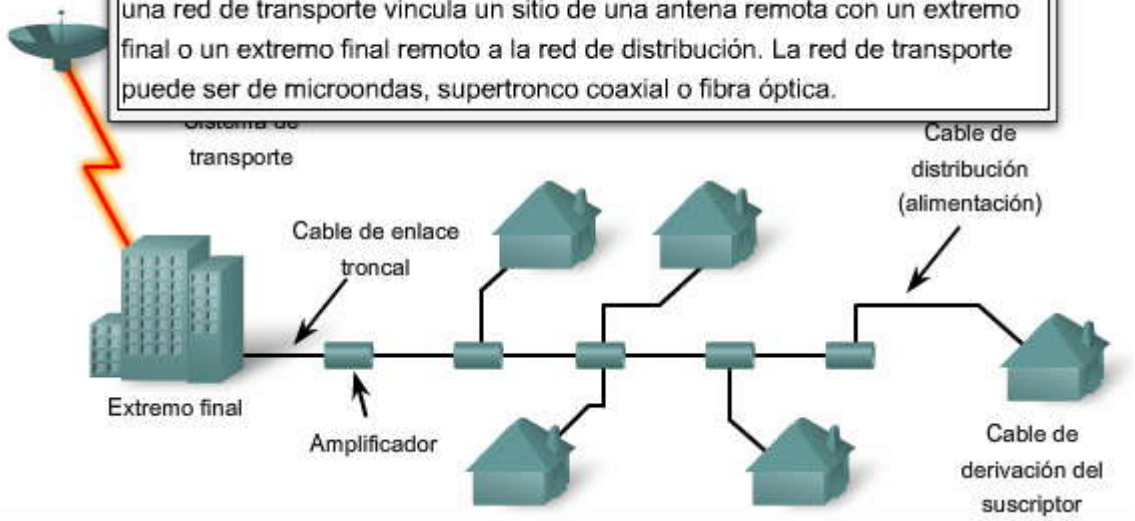
Sitio para la antena:

la ubicación de un sitio para la antena se elige con el fin de obtener una recepción óptima por aire, por satélite y por señales punto a punto. Las antenas receptoras y parabólicas principales se ubican en el sitio de la antena.



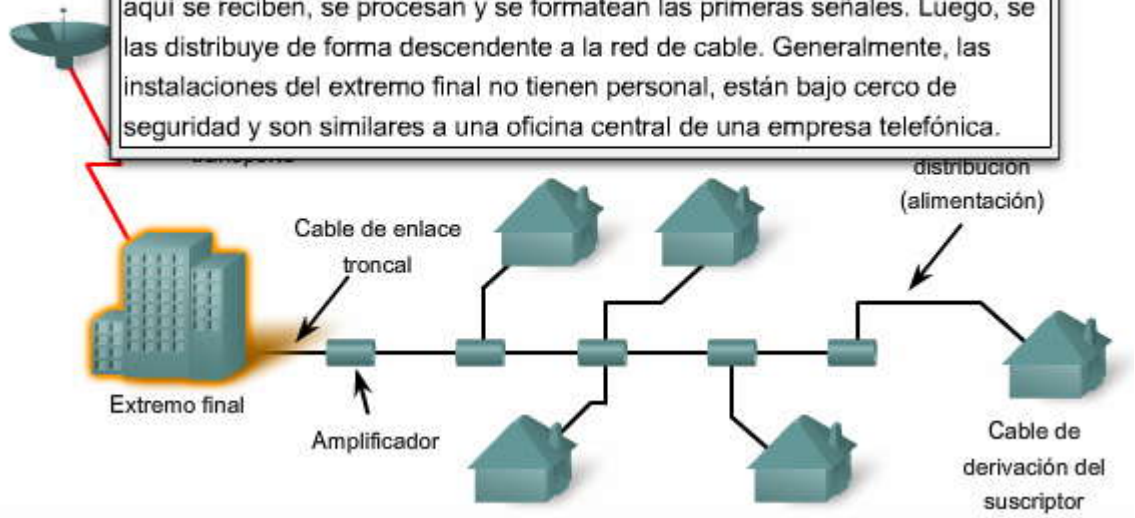
Red de transporte:

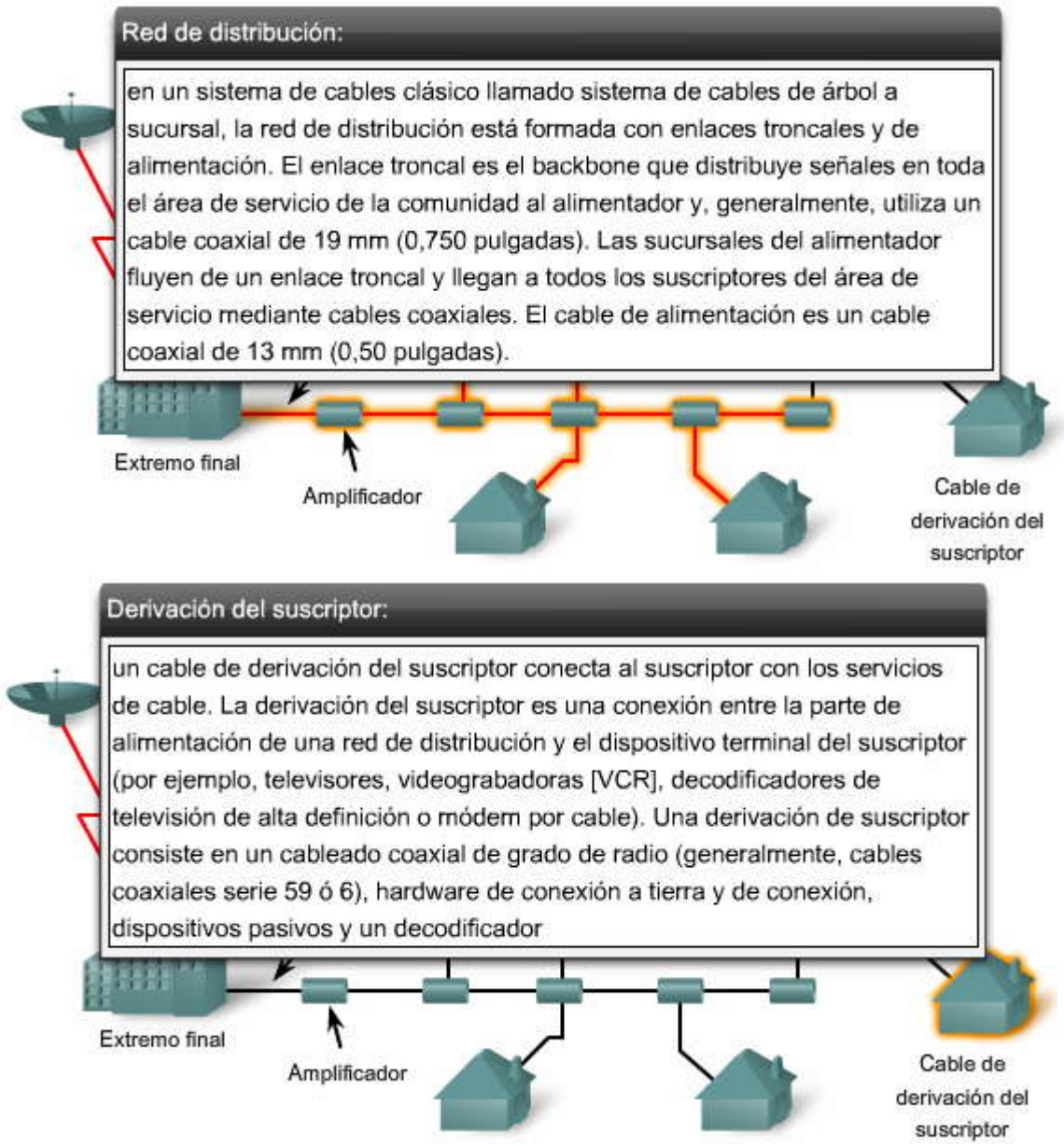
una red de transporte vincula un sitio de una antena remota con un extremo final o un extremo final remoto a la red de distribución. La red de transporte puede ser de microondas, supertronco coaxial o fibra óptica.



Extremo final:

aquí se reciben, se procesan y se formatean las primeras señales. Luego, se las distribuye de forma descendente a la red de cable. Generalmente, las instalaciones del extremo final no tienen personal, están bajo cerco de seguridad y son similares a una oficina central de una empresa telefónica.





El espectro electromagnético incluye un amplio rango de frecuencias.

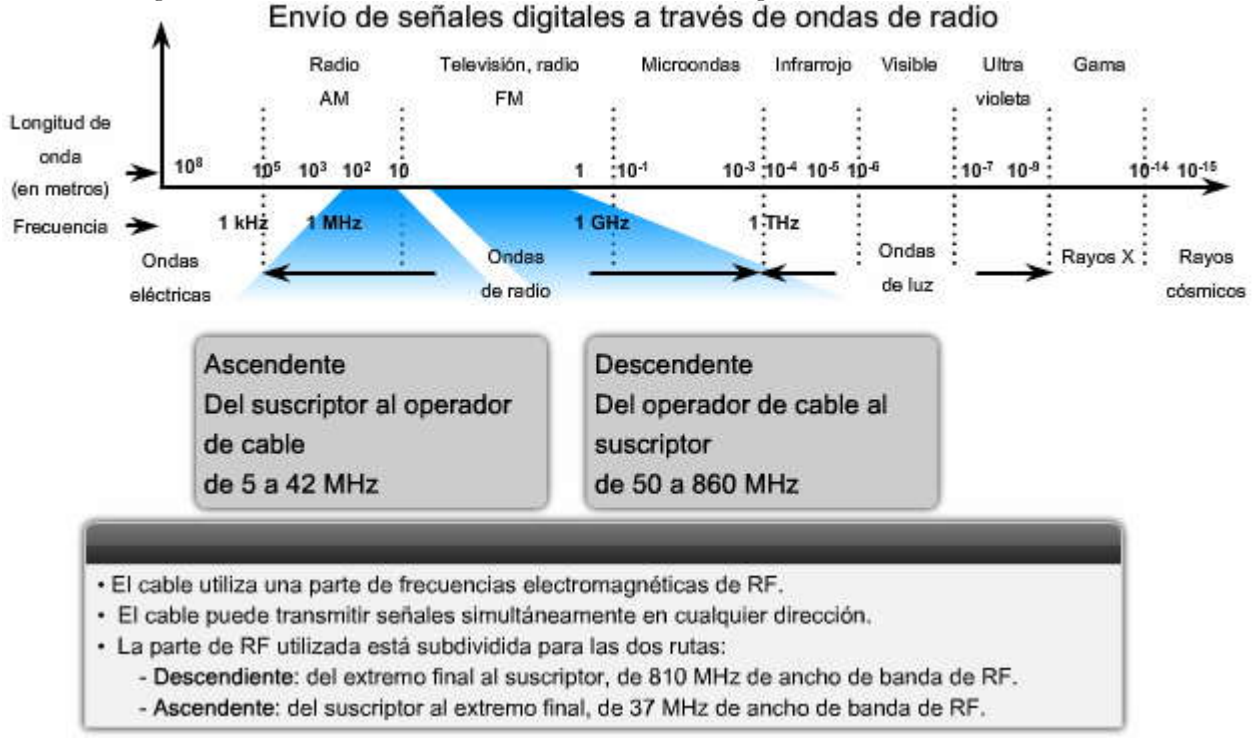
La frecuencia es la velocidad a la cual ocurren los ciclos de corriente (o voltaje), computados como la cantidad de "ondas" por segundo. La longitud de onda es la velocidad de propagación de la señal electromagnética dividida por su frecuencia en ciclos por segundo.

Las ondas de radio, generalmente denominadas RF, constituyen una parte del espectro electromagnético entre 1 kilohercio (kHz) hasta 1 terahercio, aproximadamente. Cuando los usuarios sintonizan una radio o televisor para buscar distintas estaciones de radio o canales de televisión, están sintonizando diferentes frecuencias electromagnéticas a través del espectro de la RF. El mismo principio se aplica al sistema por cable.

La industria de la televisión por cable usa una parte del espectro electromagnético de RF. Dentro del cable, frecuencias diferentes llevan datos y canales de televisión. En el extremo del suscriptor, los equipos, tales como televisores, videograbadoras y decodificadores de televisión de alta definición, sintonizan ciertas frecuencias que permiten que el usuario vea el canal o, si se usa un módem por cable, que reciba acceso a Internet de alta velocidad.

Una red por cable es capaz de transmitir señales en el cable en cualquier dirección al mismo tiempo. Se utiliza el siguiente ámbito de frecuencia:

- **Descendente**: la dirección de una transmisión de señal de RF (datos y canales de televisión) desde el origen (cabecera) hacia el destino (suscriptores). La transmisión desde el origen hacia el destino se denomina ruta de envío. Las frecuencias descendentes se encuentran en el rango de 50 a 860 megahercios (MHz).
- **Ascendente**: la dirección de una transmisión de señal de RF desde los suscriptores hacia la cabecera o la ruta inversa o de regreso. Las frecuencias ascendentes se encuentran en el rango de 5 a 42 MHz.



La especificación sobre interfaz del servicio de datos por cable (DOCSIS) es un estándar internacional desarrollado por CableLabs, un consorcio sin fines de lucro dedicado a la investigación y el desarrollo de las tecnologías relacionadas con el cable. CableLabs prueba y certifica dispositivos de proveedores de equipos de cable, como módems por cable y sistemas de terminación de módems de cable, y otorga el estado calificado o certificado por DOCSIS.

DOCSIS define los requisitos de interfaz de soporte de operaciones y comunicaciones para el sistema de datos por cable y permite la incorporación de transferencia de datos de alta velocidad a un sistema CATV existente. Los operadores de cable emplean DOCSIS para proporcionar acceso a Internet por la infraestructura existente de fibra coaxial híbrida (HFC). DOCSIS especifica los requisitos de Capa 1 y Capa 2 del modelo OSI:

- **Capa física**: para las señales de datos que el operador de cable puede usar, DOCSIS especifica los anchos de canales (anchos de banda de cada canal) como 200 kHz, 400 kHz, 800 kHz, 1,6 MHz, 3,2 MHz y 6,4 MHz. DOCSIS también especifica las técnicas de modulación (la manera de usar señales de RF para transmitir los datos digitales).
- **Capa Mac**: define un método de acceso determinista, acceso múltiple por división temporal (TDMA) o el método de acceso múltiple por división de código síncrono (S-CDMA).

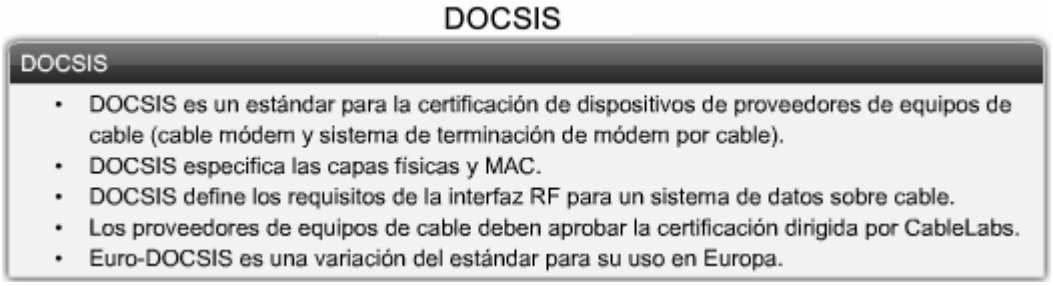
Para comprender los requisitos de capa MAC para DOCSIS, es útil una explicación de cómo varias tecnologías de comunicación dividen el acceso al canal. El TDMA divide el acceso por tiempo. El acceso múltiple de división por frecuencia (FDMA) divide el acceso por frecuencia. El acceso múltiple por división de código (CDMA) emplea una tecnología de espectro disperso y un esquema de codificación especial en el que se asigna un código específico a cada transmisor.

Una analogía que ilustra estos conceptos comienza con una sala que representa un canal. La sala está llena de personas que necesitan hablar entre ellas, en otras palabras, necesitan acceso al canal. Una solución es que las personas se turnen para hablar (división por tiempo). Otra es que cada persona hable en tonos diferentes (división por frecuencia). En CDMA, hablarían diferentes idiomas. Las personas que hablan el mismo idioma pueden entenderse entre ellas, pero el resto no. En CDMA de radio usado por las redes de teléfonos móviles de Norteamérica, cada grupo de usuarios tiene un código compartido. Muchos códigos ocupan el mismo canal, pero sólo los usuarios asociados con un código particular pueden entenderse entre ellos. S-CDMA es una versión propietaria de CDMA desarrollada por Terayon Corporation para la transmisión de datos a través de redes de cable coaxial. S-CDMA dispersa datos digitales arriba y abajo de una banda de frecuencia amplia y permite que varios suscriptores conectados a la red trasmitan y reciban de forma simultánea. S-CDMA es seguro y extremadamente resistente al ruido.

Los planes para las bandas de asignación de frecuencias difieren entre los sistemas de cable europeos y norteamericanos. Euro-DOCSIS está adaptado para su uso en Europa. Las diferencias principales entre DOCSIS y Euro-DOCSIS se relacionan con los anchos de banda del canal. Los estándares técnicos de televisión varían en el mundo, lo que afecta cómo se desarrollan las variantes de DOCSIS. Los estándares de televisión internacionales incluyen NTSC en Norteamérica y partes de Japón; PAL en la mayor parte de Europa, Asia, África, Australia, Brasil y Argentina; y SECAM en Francia y algunos países de Europa del Este.

En los siguientes sitios Web obtendrá más información:

- Acerca de DOCSIS: http://www.cablemodem.com/specifications
- Acerca de Euro-DOCSIS: http://eurocablelabs.com



Página 4:
La provisión de servicios a través de una red por cable requiere distintas frecuencias de radio. Las frecuencias descendentes están en el rango de 50 a 860 MHz y las frecuencias ascendentes están en el rango de 5 a 42 MHz.

Se requieren dos tipos de equipos para enviar señales de módem digitales ascendentes y descendentes en un sistema por cable:

- Sistema de terminación de módems de cable (CMTS) en la cabecera del operador de cable
- Módem por cable (CM) en el extremo del suscriptor

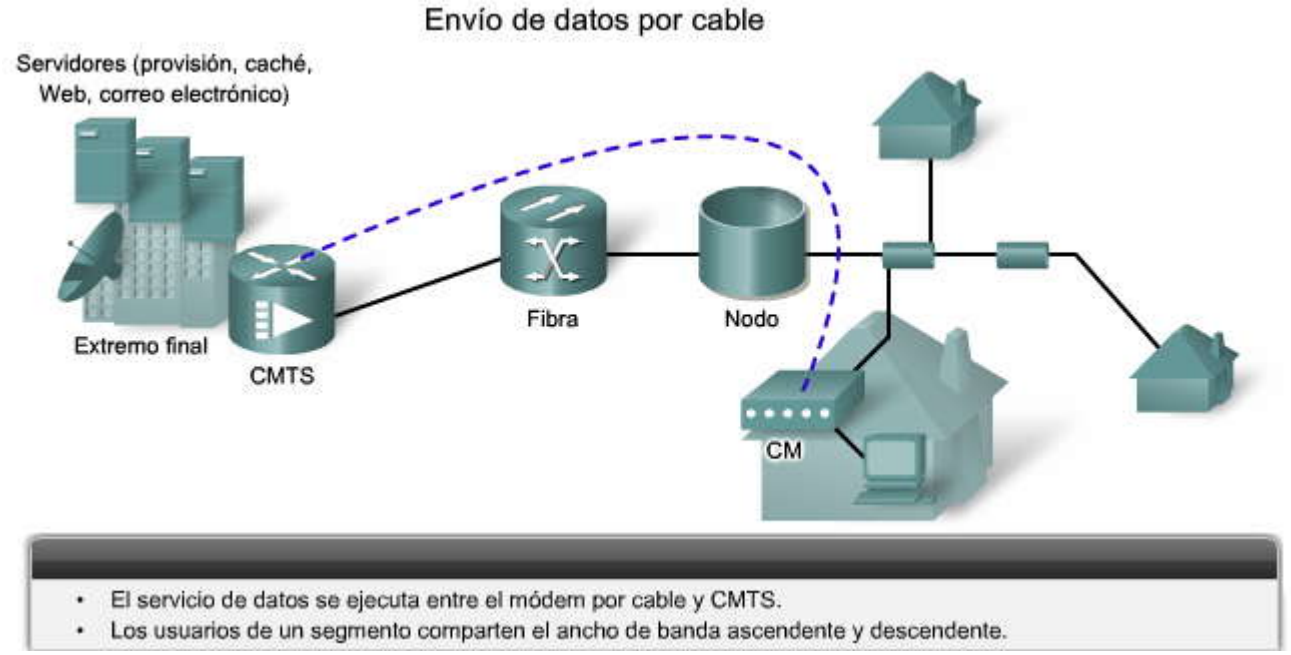
Coloque el cursor sobre los componentes de la figura y observe la función de cada uno.

Un CMTS de cabecera se comunica con los CM ubicados en los hogares de los suscriptores. La cabecera es, en realidad, un router con bases de datos para proporcionar servicios de Internet a los abonados de cable. La arquitectura es relativamente simple y usa una red coaxial óptica combinada, en la cual la fibra óptica reemplaza el coaxial de ancho de banda menor.

Una malla de cables troncales de fibra conecta la cabecera a los nodos donde ocurre la conversión de señales ópticas en señales de RF. La fibra transporta el mismo contenido de banda ancha para conexiones de Internet, servicios telefónicos y streaming video que el cable coaxial. Los cables de alimentación coaxial se originan en el nodo que transporta las señales de RF a los suscriptores.

En una red HFC moderna, en general, se conectan entre 500 y 2000 suscriptores de datos activos a un segmento de red por cable y todos comparten el ancho de banda ascendente y descendente. El ancho de banda real para el servicio de Internet a través de una línea de CATV puede ser de hasta 27 Mbps en la ruta de descarga al suscriptor y de 2.5 Mbps de ancho de banda aproximado en la ruta de carga. Basado en la arquitectura de red por cable, las prácticas de provisión del operador de cable y la carga de tráfico, un abonado individual generalmente puede obtener una velocidad de acceso de 256 kbps a 6 Mbps.

Cuando el uso elevado causa congestión, el operador de cable puede agregar un ancho de banda adicional para los servicios de datos mediante la asignación de un canal de televisión adicional para los datos de alta velocidad. Esta incorporación puede duplicar de manera efectiva el ancho de banda descendente disponible para los suscriptores. Otra opción es reducir la cantidad de suscriptores a los que cada segmento de red presta servicios. Para reducir la cantidad de suscriptores, el operador de cable subdivide aún más la red mediante la colocación de conexiones de fibra óptica más cerca y dentro de los barrios.



6.2.3 DSL

DSL es una forma de proveer conexiones de alta velocidad mediante cables de cobre instalados. En esta sección, analizamos DSL como una de las soluciones clave disponibles para el trabajador a distancia.

Hace varios años, los laboratorios de Bell identificaron que una conversación de voz común por un bucle local solamente requería un ancho de banda de 300 Hz a 3 kHz. Durante varios años, las redes telefónicas no usaron un ancho de banda superior a 3 kHz. Los avances en tecnología permitieron que DSL use el ancho de banda adicional desde 3 kHz up hasta 1 MHz para proporcionar servicios de datos de alta velocidad mediante las líneas de cobre comunes.

Como ejemplo, DSL asimétrica (ADSL) usa un rango de frecuencia de 20 kHz a 1 MHz aproximadamente. Por suerte, sólo se requieren cambios relativamente pequeños en la infraestructura existente de las empresas telefónicas para ofrecer velocidades de datos de ancho de banda elevado a los suscriptores. La figura muestra una representación de la asignación del espacio de ancho de banda en un cable de cobre para ADSL. El área de color azul identifica el rango de frecuencia usado por el servicio telefónico de grado de voz, el cual se denomina en general servicio telefónico analógico (POTS). Los demás espacios en colores representan el espacio de frecuencia usado por las señales DSL ascendentes y descendentes.

Existen dos tipos básicos de tecnología DSL: la asimétrica (ADSL) y la simétrica (SDSL). Todas las formas de servicio DSL se pueden clasificar como ADSL o SDSL y existen muchas variedades de cada tipo. ADSL brinda un mayor ancho de banda descendente al usuario que el ancho de banda de carga. SDSL ofrece la misma capacidad en ambas direcciones.

Los distintos tipos de DSL brindan diferentes anchos de banda, algunos con capacidades que exceden aquellas de la línea alquilada T1 o E1. La velocidad de transferencia depende de la longitud real del bucle local y del tipo y la condición de su cableado. Para obtener un servicio satisfactorio, el bucle debe ser menor a 5,5 kilómetros (3,5 millas).

Los proveedores de servicio implementan conexiones DSL en el último paso de una red telefónica local, lo que se denomina bucle local o última milla. Se instala la conexión entre un par de módems ubicados en cualquier extremo de un cable de cobre que se extiende entre el equipo local del cliente (CPE) y el multiplexor de acceso DSL (DSLAM). El DSLAM es el dispositivo ubicado en la oficina central (CO) del proveedor, que concentra las conexiones desde los distintos suscriptores DSL.

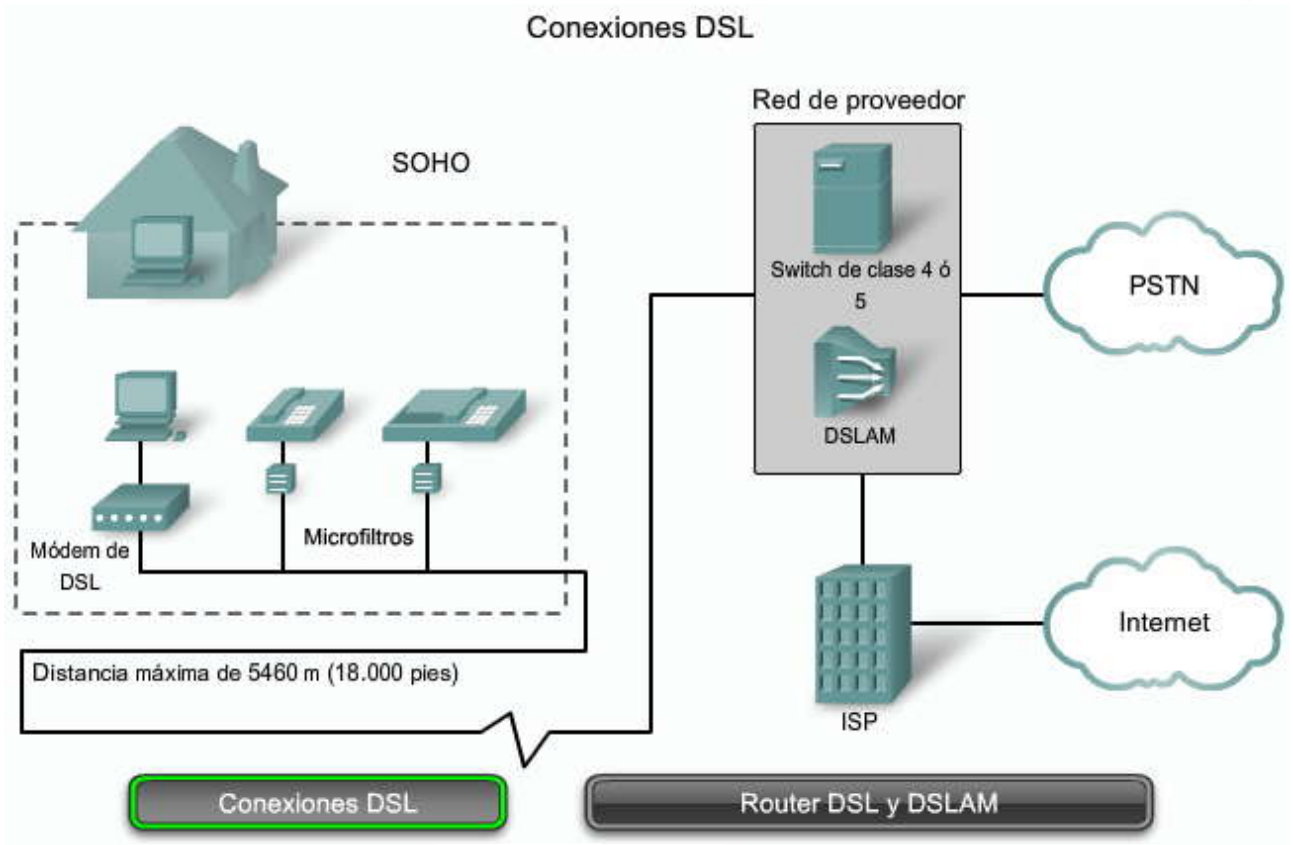
Haga clic en el botón Conexiones DSL de la figura.

La figura muestra el equipo clave necesario para brindar una conexión DSL a una oficina pequeña u oficina doméstica. Los dos componentes clave son el transceptor DSL y el DSLAM:

- Transceptor: conecta la computadora del trabajador a distancia con el DSL. Generalmente, el transceptor es un módem DSL conectado a la computadora mediante un cable USB o Ethernet. Los transceptores DSL más nuevos pueden integrarse en routers pequeños con varios puertos de switch 10/100 para que usen las oficinas pequeñas.
- **DSLAM**: ubicado en la oficina central de la empresa de telecomunicaciones, el DSLAM combina conexiones DSL individuales de los usuarios en un enlace de alta capacidad al ISP y, por lo tanto, a Internet.

Haga clic en el botón Router DSL y DSLAM de la figura.

La ventaja que tiene DSL sobre la tecnología por cable es que no es un medio compartido. Cada usuario tiene una conexión directa separada al DSLAM. La incorporación de usuarios no afecta el rendimiento, a menos que la conexión de Internet DSLAM al ISP o Internet se sature.



La mayor ventaja de ADSL es la habilidad de proporcionar servicios de datos junto con servicios de voz POTS.

Cuando el proveedor del servicio coloca voz analógica y ADSL en el mismo cable, divide el canal POTS desde el módem ADSL por medio de filtros o divisores de señal. Esta configuración garantiza el servicio telefónico normal sin interrupciones, aun si ocurre una falla en el ADSL. Cuando los filtros o divisores de señalestán en su lugar, el usuario puede usar la línea de teléfono y la conexión ADSL al mismo tiempo, sin afectar ninguno de los servicios.

Las señales ADSL distorsionan la transmisión de voz y se dividen o filtran en las instalaciones del cliente. Hay dos maneras de separar ADSL de la voz en las instalaciones del cliente: mediante un microfiltro o un divisor de señal.

Un microfiltro es un filtro de paso bajo con dos extremos. Un extremo se conecta al teléfono y el otro al jack de pared. Esta solución elimina la necesidad de que un técnico visite las instalaciones y permite que el usuario use cualquier jack de la casa para el servicio de voz o ADSL.

Los divisores de señal POTS separan el tráfico DSL del tráfico POTS. El divisor de señal POTS es un dispositivo pasivo. Si se produjera un corte de energía eléctrica, el tráfico de voz aún se desplazaría al switch de voz en la oficina central de la empresa de telecomunicaciones. Los divisores de señal se ubican en la oficina central y, en algunas implementaciones,en las instalaciones del cliente. En la oficina central, el divisor de señal POTS separa el tráfico de voz, destinado para las conexiones POTS, y el tráfico de datos destinado para DSLAM.

La figura muestra el bucle local que termina en las instalaciones del cliente en el punto de demarcación. El dispositivo real es el dispositivo de interfaz de red (NID). Este punto es, generalmente, donde la línea telefónica ingresa a las instalaciones del cliente. En este punto, puede colocarse un divisor de señal en la línea telefónica. El divisor de señal desvía la línea telefónica; una parte proporciona el cableado telefónico de la casa original para los teléfonos y la otraparte se conecta al módem ADSL. El divisor de señal actúa como un filtro de paso bajo y solamente permite que las frecuencias de 0 a 4 kHz pasen al teléfono o desde él. La instalación del divisor de señal POTS en el NID en general significa que un técnico debe ir a las instalaciones del cliente.

Debido al servicio de asistencia técnica y mano de obra adicionales, hoy en día, la mayor parte de las instalaciones domésticas usa microfiltros, como se muestra en la figura. El uso de microfiltros también ofrece la ventaja de proporcionar una conectividad mayor a través del hogar. Debido a que el divisor de señal POTS separa las señales de voz y ADSL en el NID, generalmente, hay una sola toma ADSL disponible en la casa.

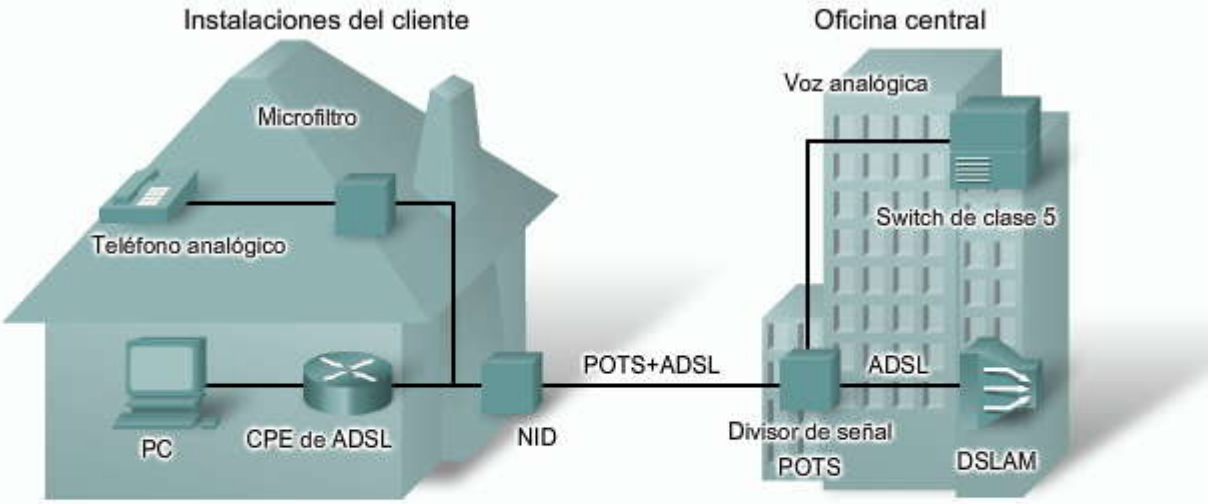
Haga clic en el botón Microfiltro que aparece en la figura.

La figura muestra un diseño DSL típico de oficinas pequeñas u oficinas domésticas mediante microfiltros. En esta solución, el usuario puede instalar microfiltros de línea interna en cada teléfono, o instalar microfiltros montados en lapared en vez de jacks de teléfono comunes. Si coloca el cursor sobre los microfiltros que aparecen en el gráfico, se muestran las fotografías de los productos Cisco.

Haga clic en el botón Divisor de señal de la figura.

Si el proveedor de servicio hubiera instalado un divisor de señal, éste se ubicaría entre el NID y el sistema interno de distribución telefónica. Un cable iría directamente al módem DSL y el otro transportaría la señal DSL a los teléfonos. Si coloca el cursor sobre la caja de divisores de señal que se encuentra en el gráfico, se muestra un esquema de cableado frecuente.

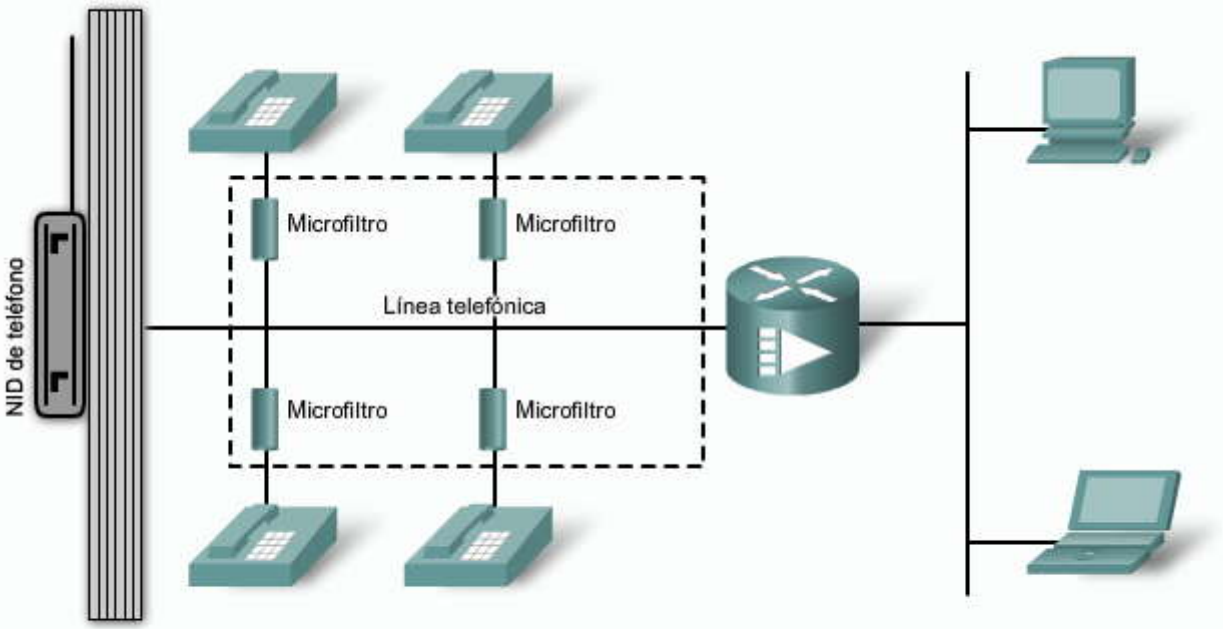
Separación de datos de voz en conexiones ADSL



- Una función clave de ADSL es la coexistencia con POTS.
- La transmisión de señales de voz y datos se realiza en el mismo par de cables.
- Los circuitos de datos se descargan del switch de voz.

ADSL | Microfiltro | Divisor de señal

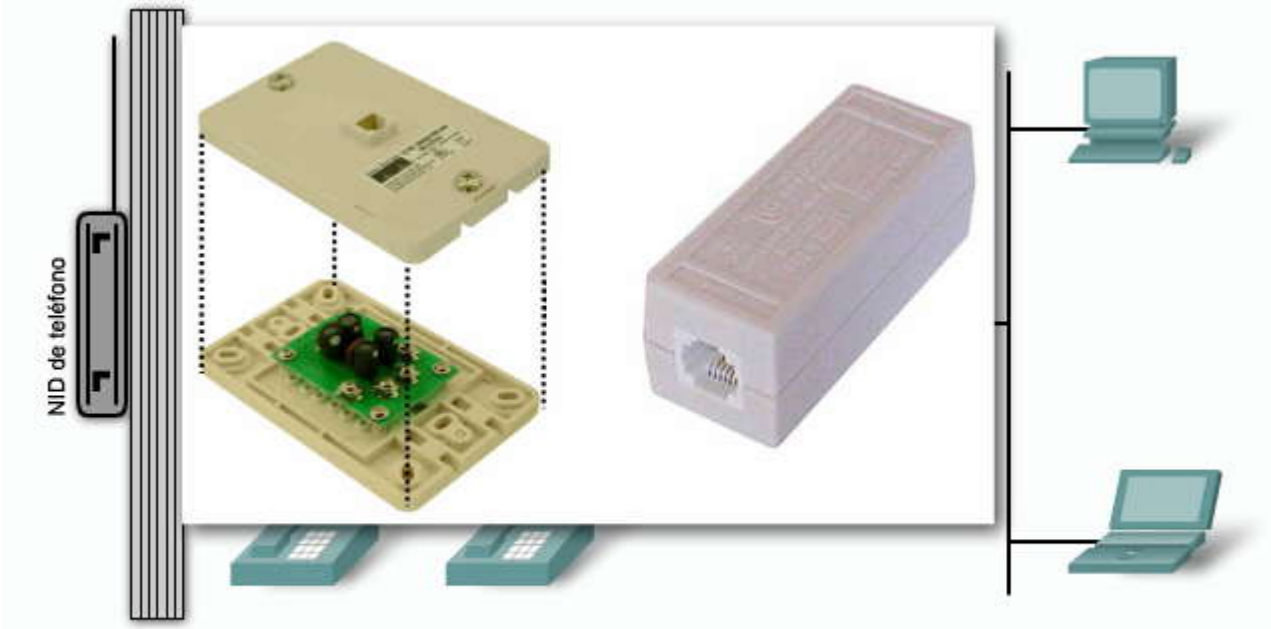
Microfiltros EZ-DSL Cisco



Coloque el cursor sobre los microfiltros para obtener ejemplos de microfiltros de línea interna y montados en la pared.

ADSL | Microfiltro | Divisor de señal

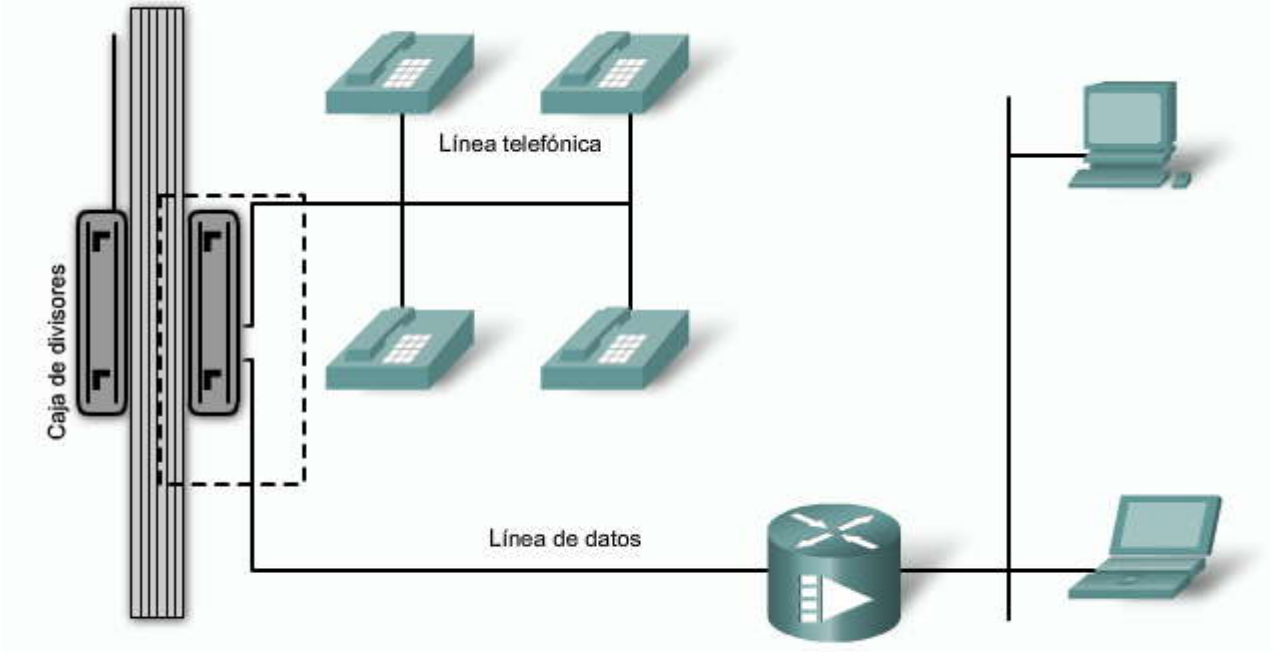
Microfiltros EZ-DSL Cisco



Coloque el cursor sobre los microfiltros para obtener ejemplos de microfiltros de línea interna y montados en la pared.

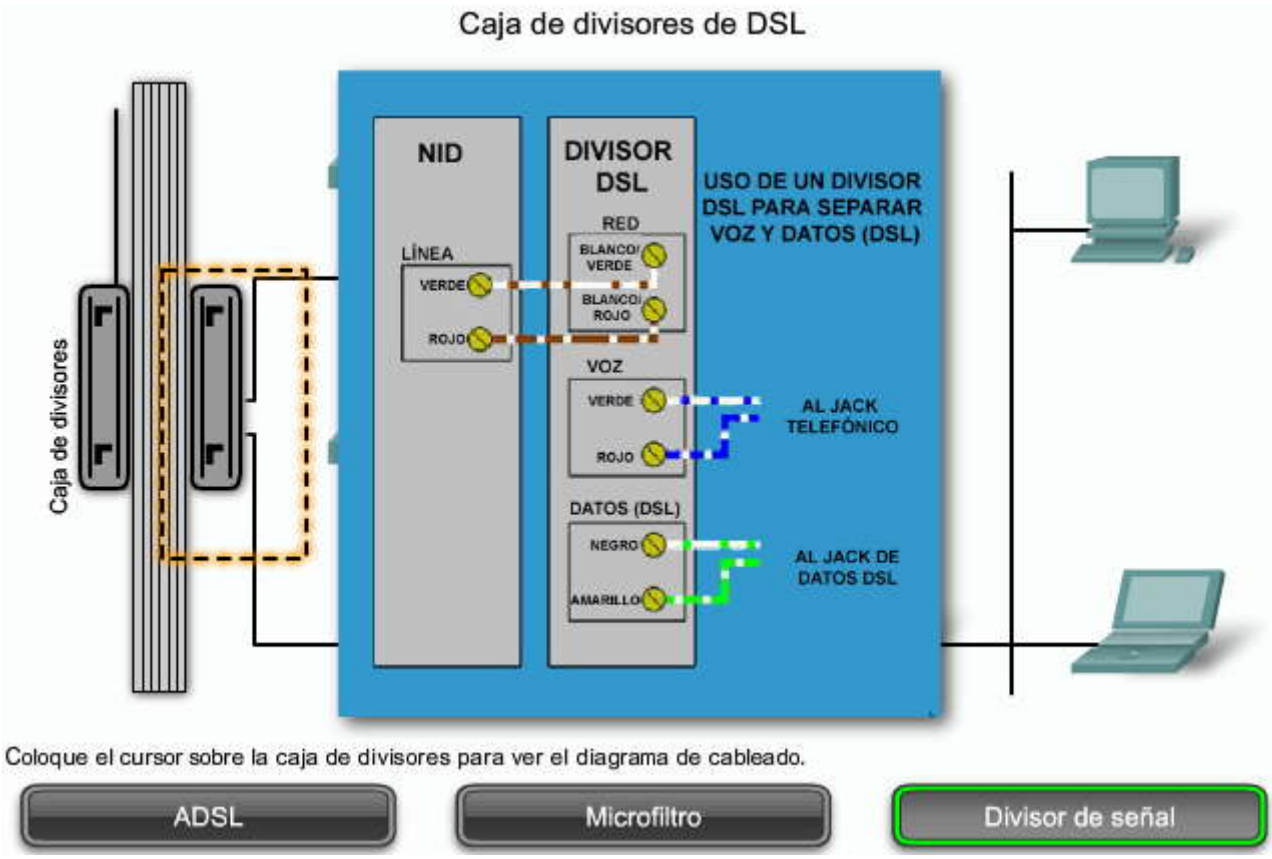
ADSL | Microfiltro | Divisor de señal

Caja de divisores de DSL



Coloque el cursor sobre la caja de divisores para ver el diagrama de cableado.

ADSL | Microfiltro | Divisor de señal



6.2.4 Conexión inalámbrica de banda ancha

El acceso de banda ancha por ADSL o cable proporciona conexiones más rápidas a los trabajadores a distancia que el servicio dial-up; sin embargo, hasta hace poco, los equipos de las oficinas pequeñas y domésticas debían conectarse a un módem o router por un cable Cat 5 (Ethernet). Las conexiones de red inalámbricas, o Wi-Fi (del inglés, Wireless Fidelity), han mejorado esa situación no sólo para las oficinas pequeñas u oficinas domésticas, sino también en los campus empresariales.

Mediante los estándares de networking 802.11, los datos se desplazan de un lugar a otro en ondas de radio. Lo que hace que el networking 802.11 sea relativamente fácil de implementar es que usa el espectro de radio sin licencia para enviar y recibir datos. La mayoría de las transmisiones de televisión y radio están reguladas por el gobierno, y se necesita licencia para poder usarlas.

A partir de 2007, los fabricantes de computadoras comenzaron a incorporar adaptadores de red inalámbrica en la mayoría de los equipos portátiles. Como el precio de los conjuntos de chip para Wi-Fi sigue disminuyendo, se está convirtiendo en una opción de networking muy económica también para las PC.

Las ventajas de Wi-Fi se extienden más allá del hecho de no tener que usar o instalar conexiones de red por cable. Las conexiones de red inalámbricas proporcionan movilidad. Las conexiones inalámbricas proporcionan unamayor flexibilidad y productividad al trabajador a distancia.

Hasta hace poco, una limitación importante de acceso inalámbrico había sido la necesidad de estar dentro de un rango de transmisión local (en general menor a 30,5 metros) de un router inalámbrico o punto de acceso inalámbrico que tiene una conexión con cable a Internet. Una vez que el trabajador abandonaba la oficina o el hogar, el acceso inalámbrico no se encontraba fácilmente disponible.

Sin embargo, con los avances tecnológicos, se ha extendido el alcance de las conexiones inalámbricas. El concepto de puntos de conexión ha aumentado el acceso a las conexiones inalámbricas en el mundo. Un punto de conexión es el área cubierta por uno o más puntos de acceso interconectados. Los lugares de reuniones públicas, como cafeterías, parques y bibliotecas, han creado puntos de conexión Wi-Fi con la esperanza de aumentar el negocio. Mediante la superposición de puntos de acceso, los puntos de conexión pueden cubrir muchos metros cuadrados.

Los desarrollos recientes en la tecnología de conexión inalámbrica de banda ancha están aumentando la disponibilidad inalámbrica. Entre otros, se encuentran los siguientes:

- Wi-Fi municipal
- WiMAX
- Internet satelital

Los gobiernos municipales también se han unido a la revolución Wi-Fi. A menudo, junto con los proveedores de servicios, las ciudades están implementando redes inalámbricas municipales. Algunas de estas redes proporcionan acceso a Internet de alta velocidad sin costo o por un precio mucho menor al de los demás servicios de banda ancha. Otras ciudades reservan las redes Wi-Fi para uso oficial y proporcionan acceso remoto a Internet y a las redes del municipio a la policía, los bomberos y los trabajadores municipales.

Haga clic en el botón Router único de la figura.

La figura muestra una implementación doméstica típica mediante un único router inalámbrico. Esta implementación usa el modelo hub-and-spoke. Si ocurre una falla en el único router inalámbrico, se pierde la conectividad. Use el mouse para colocar el cursor sobre el cuadro de texto.

Haga clic en el botón Malla de la figura.

La mayor parte de las redes inalámbricas municipales usa una topología de malla en vez del modelo hub-and-spoke. Una malla es una serie de puntos de acceso (transmisores de radio) como aparece en la figura. Cada punto de acceso está dentro del rango y puede comunicarse con al menos otros dos puntos de acceso. La malla cubre su área con señales de radio. Las señales se desplazan desde un punto de acceso a otro, a través de esta nube.

Una red en malla tiene varias ventajas en comparación con los puntos de conexión de router único. La instalación es más fácil y puede ser más económica porque hay menos cables. Es más rápida la implementación sobre un área urbana grande. Desde el punto de vista operativo, es más confiable. Si ocurre una falla en un nodo, los restantes de la malla lo compensan.

Haga clic en el botón WiMAX de la figura.

WiMAX (Interoperatividad mundial para el acceso por microondas) es una tecnología de telecomunicaciones que tiene como objetivo la provisión de datos inalámbricos sobre una gran distancia de diferentes maneras, desde enlaces punto a punto hasta el acceso completo de tipo celular móvil. WiMAX funciona a velocidades mayores, sobre distancias más grandes y para una cantidad de usuarios superior que Wi-Fi. Debido a su velocidad mayor (ancho de banda) y a la reducción de los precios de los componentes, se predice que WiMAX pronto reemplazará las redes en malla municipales por las implementaciones inalámbricas.

Una red WiMAX consta de dos componentes principales:

- Una torre conceptualmente similar a una torre de telefonía celular. Una sola torre WiMAX puede brindar cobertura a un área de 7500 kilómetros cuadrados, aproximadamente, o 3000 millas cuadradas.
- Un receptor WiMAX similar en tamaño y forma a una tarjeta PCMCIA o se incorpora a una laptop o a otro dispositivo inalámbrico.

Una estación de torre WiMAX se conecta directamente a Internet mediante una conexión de ancho de banda elevado (por ejemplo, una línea T3). Una torre también puede conectarse a otras torres WiMAX mediante enlaces de microondas de línea de visión. Por lo tanto, WiMAX puede proporcionar cobertura a las áreas rurales situadas fuera del alcance del cable de "última milla" y de las tecnologías DSL.

Haga clic en el botón Satélite de la figura.

Los servicios de Internet satelital se usan en lugares donde no está disponible el acceso a Internet terrestre o en instalaciones temporarias que están en continuo movimiento. El acceso a Internet por medio de satélites se encuentra disponible mundialmente, incluso para los barcos en el mar, los aviones durante el vuelo y los vehículos que viajan por tierra.

Hay tres formas de conectarse a Internet por medio de satélites: multicast unidireccional, retorno terrestre unidireccional y bidireccional.

- Los sistemas de Internet satelital multicast unidireccional se usan para la distribución de video, audio y datos basados en IP multicast . Aunque la mayoría de los protocolos IP requieren una comunicación bidireccional, para el contenido de Internet, incluidas las páginas Web, los servicios de Internet satelital unidireccional pueden ser páginas enviadas al almacenamiento local en los sitios del usuario final por medio de Internet satelital. No es posible la interactividad total.
- Los sistemas de Internet satelital de retorno terrestre unidireccional usan el acceso tradicional dial-up para enviar datos salientes a través de un módem o recibir descargas desde el satélite.
- Los sistemas de Internet satelital bidireccional envían datos desde lugares remotos a través del satélite a un hub, el cual luego envía los datos a Internet. Las antenas parabólicas de cada lugar necesitan una ubicación precisa para evitar interferencias con otros satélites.

La figura muestra un sistema de Internet satelital bidireccional. Las velocidades de carga son alrededor de un décimo de las velocidades de descarga, lo que está en un rango de 500 kbps.

El requisito clave de instalación es que la antena tenga una vista clara hacia el Ecuador, donde se encuentra la mayoría de los satélites. Los árboles y las lluvias copiosas pueden afectar la recepción de las señales.

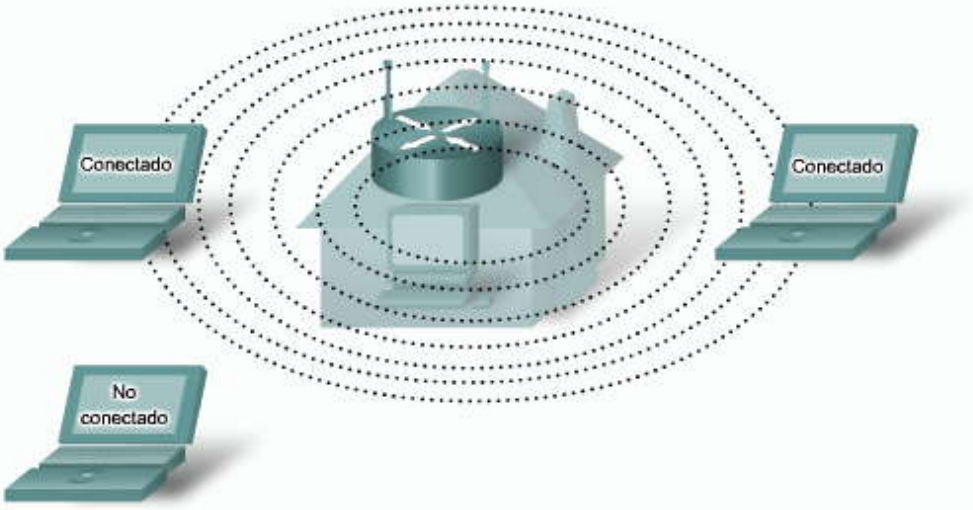
El sistema de Internet satelital bidireccional usa tecnología multicast IP, la cual permite que un satélite brinde servicios a 5000 canales de comunicación de manera simultánea. IP Multicast envía datos desde un punto a varios puntos al mismo tiempo mediante el envío de datos en un formato comprimido. La compresión reduce el tamaño de los datos y del ancho de banda.

Tipos de acceso inalámbrico de banda ancha

- Wi-Fi municipal
- WiMAX
- Internet satelital

Tipos | Router único | Malla | WiMAX | Satélite

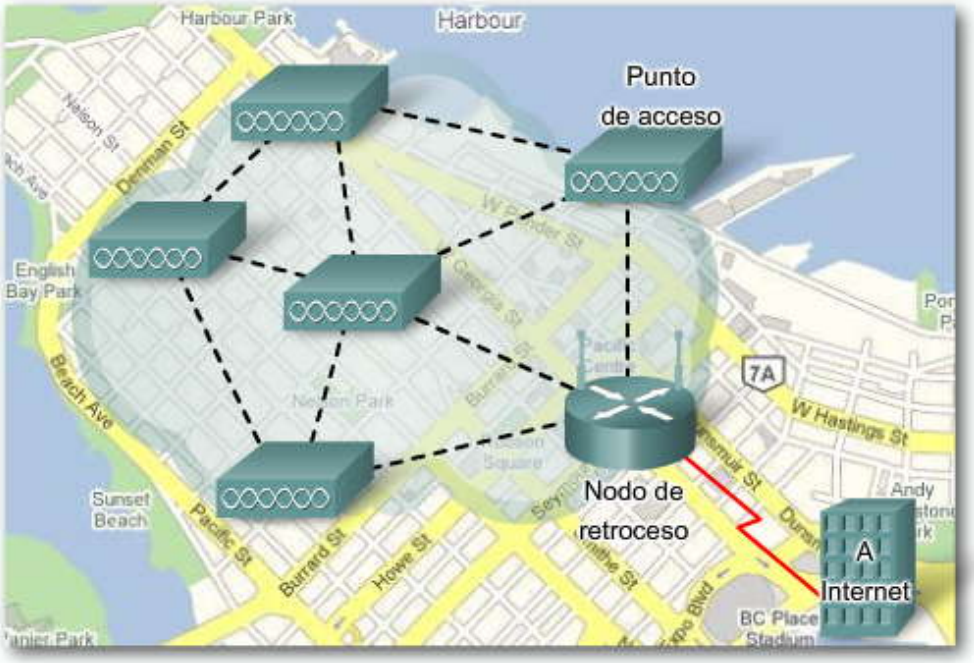
Router inalámbrico único



En una situación normal, se conectan todas las PC dentro del alcance. Pero, ¿si el router no funciona?
(Haga clic para obtener más información)

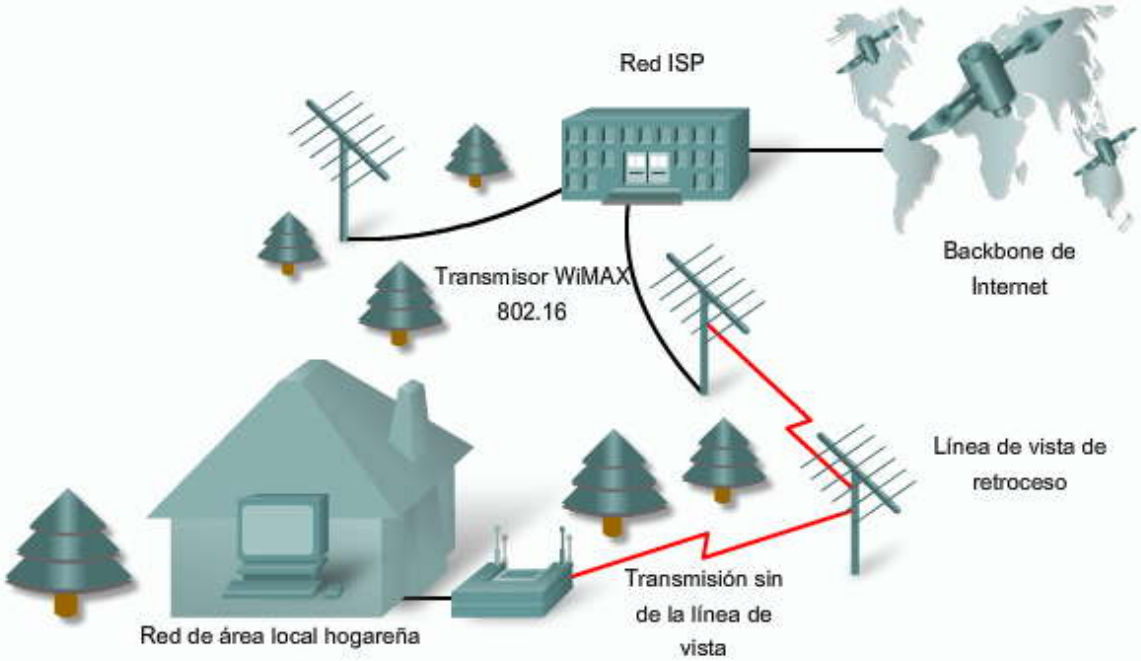
Tipos | Router único | Malla | WiMAX | Satélite

Red municipal de Wi-Fi con malla

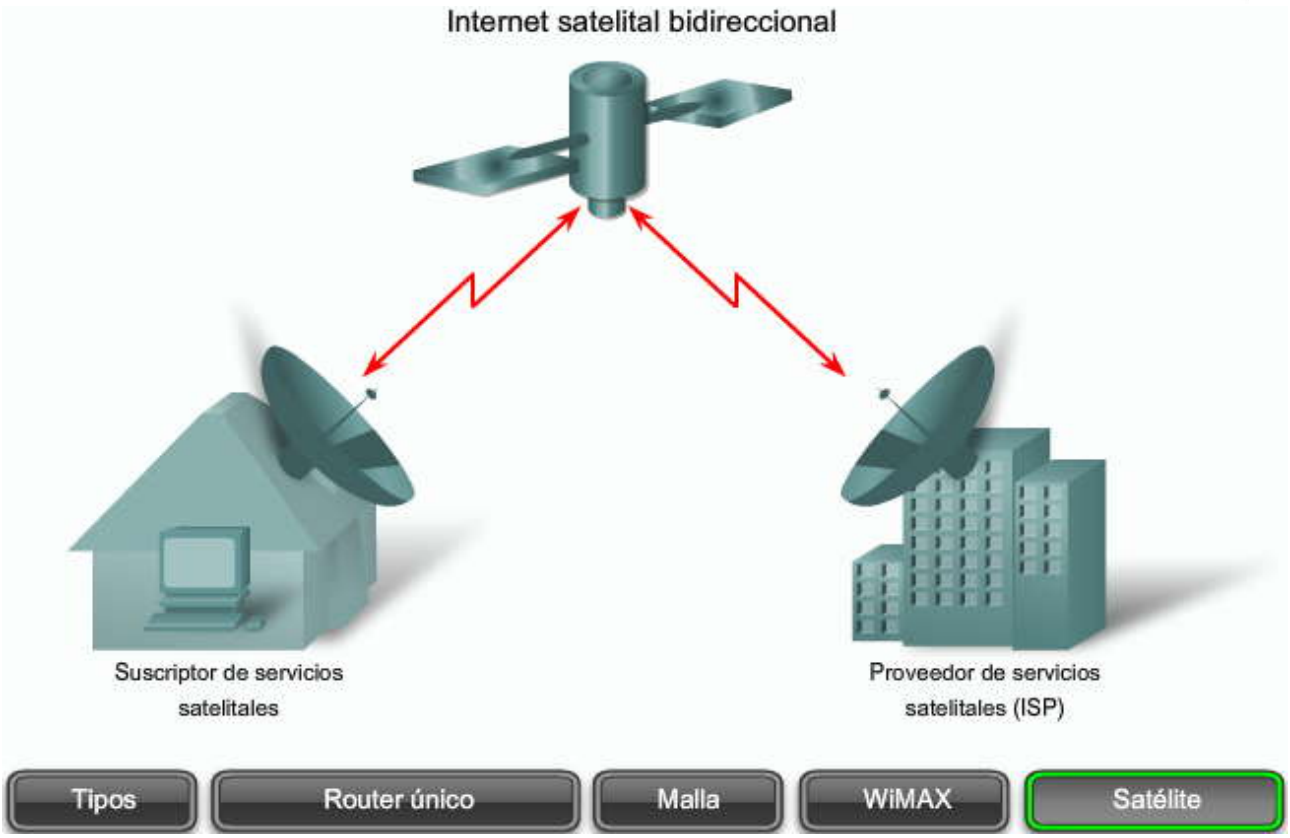


Tipos | Router único | Malla | WiMAX | Satélite

WiMAX



Tipos | Router único | Malla | WiMAX | Satélite



Las conexiones de redes inalámbricas cumplen con un rango de estándares que usan los routers y los receptores para comunicarse entre sí. Los estándares más frecuentes se incluyen en el estándar IEEE 802.11 para redes de área local inalámbrica (WLAN), el cual direcciona las bandas de espectro público (sin licencia) de 5 GHz y 2,4 GHz.

Los términos 802.11 y Wi-Fi se usan de manera intercambiable, pero no es correcto. Wi-Fi es una certificación de interoperatividad de la industria que se basa en un subconjunto de 802.11. La especificación Wi-Fi apareció porque la demanda del mercado llevó a que Wi-Fi Alliance comenzara con la certificación de productos antes de que se completaran las modificaciones al estándar 802.11. Desde ese momento, el estándar 802.11 ha alcanzado y superado a Wi-Fi.

Desde el punto de vista de los trabajadores a distancia, los enfoques de acceso más populares a la conectividad son aquellos definidos por los protocolos IEEE 802.11b y IEEE 802.11g. En un principio, la seguridad era intencionalmente débil en estos protocolos debido a los requisitos de exportación restrictivos de varios gobiernos. El estándar más reciente, 802.11n, es una modificación propuesta que se basa en los estándares 802.11 anteriores por medio de la incorporación de entrada múltiple, salida múltiple (MIMO).

El estándar 802.16 (o WiMAX) permite transmisiones de hasta 70 Mbps y tiene un rango de hasta 50 km (30 millas). Puede funcionar en bandas con licencia o sin licencia del espectro desde 2 hasta 6 GHz.

Página 4:
En esta actividad, debe demostrar su capacidad para incorporar conexiones y dispositivos de banda ancha a Packet Tracer. Aunque no puede configurar DSL y los módems por cable, puede simular la conectividad de extremo a extremo con los dispositivos del trabajador a distancia.
Se proporcionan instrucciones detalladas dentro de la actividad y en el siguiente enlace al PDF.
Instrucciones de la actividad (PDF)

6.3 Tecnología VPN

6.3.1 Las redes VPN y sus beneficios

Internet es una red IP de acceso público en todo el mundo. Debido a su amplia proliferación global, se ha convertido en una manera atractiva de interconectar sitios remotos. Sin embargo, el hecho de que sea una infraestructura pública conlleva riesgos de seguridad para las empresas y sus redes internas. Afortunadamente, la tecnología VPN permite que las organizaciones creen redes privadas en la infraestructura de Internet pública que mantienen la confidencialidad y la seguridad.

Las organizaciones usan las redes VPN para proporcionar una infraestructura WAN virtual que conecta sucursales,oficinas domésticas, oficinas de socios comerciales y trabajadores a distancia a toda la red corporativa o a parte de ella. Para que permanezca privado, el tráfico está encriptado. En vez de usar una conexión de Capa 2 exclusiva, como una línea alquilada, la VPN usa conexiones virtuales que se enrutan a través de Internet.

Anteriormente en este curso, se presentó una analogía que incluía la obtención de entradas preferenciales para un espectáculo en un estadio. Una ampliación de esa analogía ayuda a explicar cómo funciona la VPN. Imagine el estadio como un lugar público, al igual que Internet es un lugar público. Cuando el espectáculo termina, el público abandona el estadio a través de los pasillos y las puertas, se empuja y abre paso a lo largo del camino. Los robos menores son amenazas que deben soportarse.

Tenga en cuenta cómo salen los actores. Su comitiva une los brazos y forma cordones entre la gente y protege a las celebridades de los empujones. De hecho, estos cordones forman túneles. Las celebridades se trasladan a través de túneles hacia las limusinas que los llevan protegidos a sus destinos. Esta sección describe cómo funcionan las VPN de una manera muy parecida; agrupan datos y los desplazan de manera segura a través de Internet por túneles protectores. Comprender la tecnología VPN es esencial para poder implementar servicios seguros para trabajadores a distancia en las redes empresariales.

Analogía: Cada LAN es una isla
Usaremos otra analogía para ilustrar el concepto de la VPN desde un punto de vista diferente. Imagine que vive en una isla en un gran océano. Hay miles de otras islas alrededor, algunas cerca y otras lejos. La manera normal de viajar es tomar el transbordador desde su isla a cualquier otra que desee visitar. El viaje en el transbordador significa que casi no tiene privacidad. Otra persona puede observar todo lo que haga.

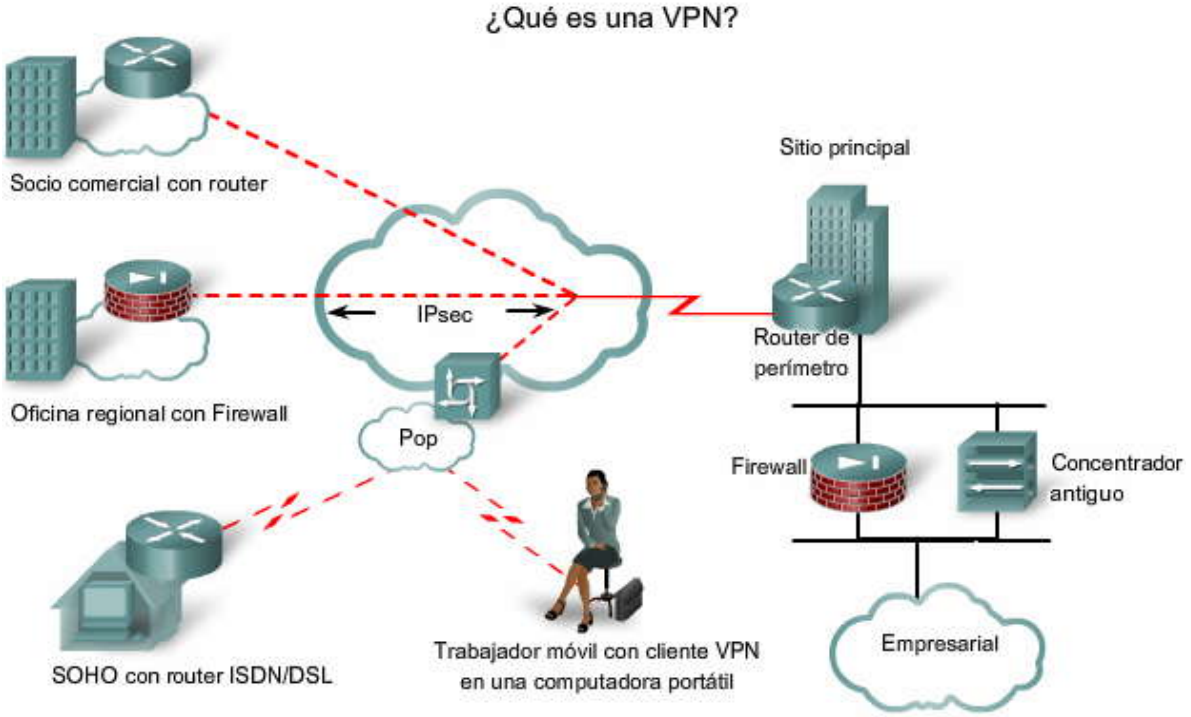
Suponga que cada isla representa una LAN privada y que el océano es Internet. Cuando viaja en el transbordador, es similar a cuando se conecta a un servidor Web o a otro dispositivo a través de Internet. No tiene control sobre los cables ni routers que forman Internet, de igual manera que no tiene control sobre el resto de las personas que viajan en el transbordador. Esto lo vuelve vulnerable a los problemas de seguridad si intenta conectarse entre dos redes privadas por medio de un recurso público.

Su isla decide construir un puente a otra isla para que sea un medio más fácil, seguro y directo para que las personas viajen entre ellas. Es caro construir y mantener el puente, aunque la isla a la que se está conectando es muy cercana. Pero la necesidad de una ruta segura y confiable es tan grande que decide hacerlo de todos modos. Su isla quisiera conectarse a una segunda isla que queda mucho más lejos, pero decide que es demasiado caro.

Esta situación es muy similar a tener una línea alquilada. Los puentes (líneas alquiladas) están separados del océano (Internet), pero aun así pueden conectar las islas (redes LAN). Muchas empresas han elegido esta ruta debido a la necesidad de seguridad y fiabilidad para la conexión de sus oficinas remotas. Sin embargo, si las oficinas están muy lejos, el costo puede ser demasiado alto, igual que intentar construir un puente que cubra una gran distancia.

Entonces ¿cómo encaja una VPN en esta analogía? Podríamos darle a cada habitante de las islas su propio submarino con estas propiedades:
- Veloz
- Fácil de llevar con usted donde sea que vaya
- Permite ocultarse por completo de otros botes o submarinos
- Confiable
- Cuesta poco agregar submarinos adicionales a la flota una vez que se compró el primero

Aunque están viajando en el océano junto con más tráfico, los habitantes de nuestras dos islas podrían viajar entre ellas cuando lo deseen con privacidad y seguridad. Esencialmente, así funciona la VPN. Cada miembro remoto de la red puede comunicarse de manera segura y confiable a través de Internet como medio para conectarse a la LAN privada. La VPN puede desarrollarse para alojar más usuarios y ubicaciones diferentes de manera mucho más fácil que una línea alquilada. De hecho, la escalabilidad es una ventaja principal que tienen las VPN sobre las líneas alquiladas comunes. A diferencia de las líneas alquiladas, donde aumenta el costo en proporción a las distancias en cuestión, las ubicaciones geográficas de cada oficina tienen poca importancia en la creación de una VPN.

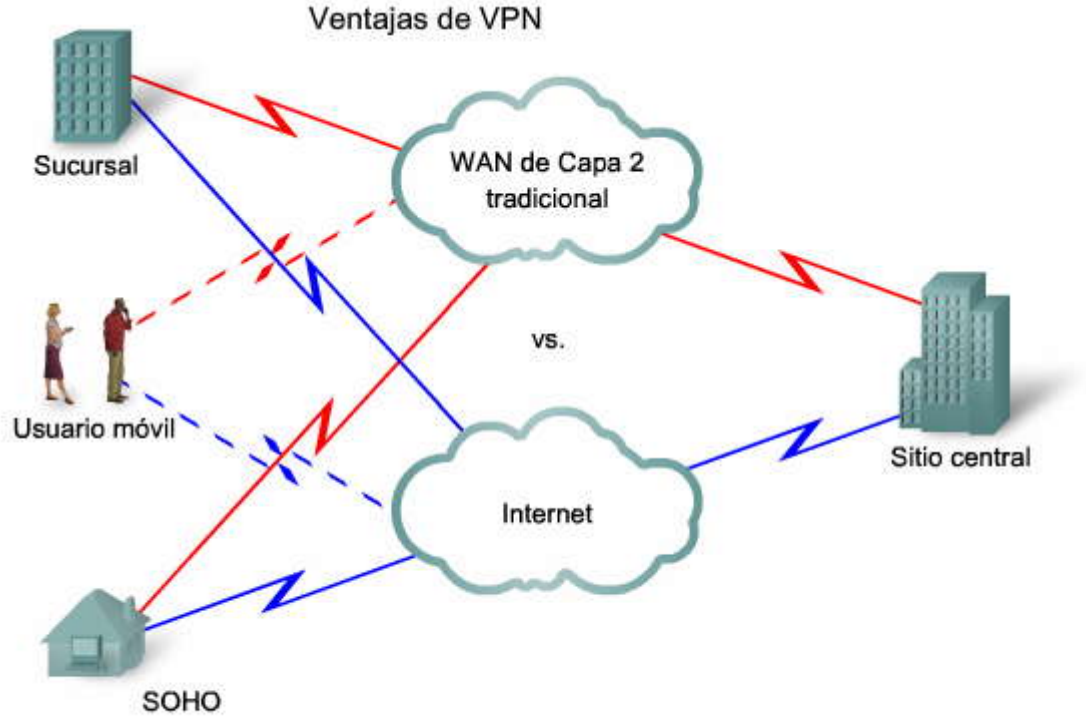


- Virtual: la información dentro de una red privada se transporta por una red pública.
- Privada: el tráfico está encriptado para que los datos sean confidenciales.

Las organizaciones que usan las VPN se benefician con el aumento en la flexibilidad y la productividad. Los sitios remotos y los trabajadores a distancia pueden conectarse de manera segura a la red corporativa desde casi cualquier lugar. Los datos de la VPN están encriptados y ninguna persona que no esté autorizada puede descifrarlos. Las VPN traen a los hosts remotos dentro del firewall y les brindan casi los mismos niveles de acceso a los dispositivos de red como si estuvieran en una oficina corporativa.

La figura muestra las líneas alquiladas en rojo. Las líneas azules representan las conexiones de VPN. Tenga en cuenta estos beneficios al usar las VPN:

- **Económicos**: las organizaciones pueden usar transporte de Internet de terceros y económico para conectar oficinas y usuarios remotos al sitio corporativo principal. Esto elimina los enlaces WAN exclusivos y caros, y los bancos de módems. Mediante el uso de banda ancha, las VPN reducen los costos de conectividad mientras aumenta el ancho de banda de las conexiones remotas.
- **Seguridad**: los protocolos de autenticación y encriptación avanzados protegen los datos contra el acceso no autorizado.
- **Escalabilidad**: las VPN usan la infraestructura de Internet dentro de los ISP y las empresas de telecomunicaciones, y es más fácil para las organizaciones agregar usuarios nuevos. Las organizaciones, grandes y pequeñas, pueden agregar grandes cantidades de capacidad sin incorporar una infraestructura significativa.



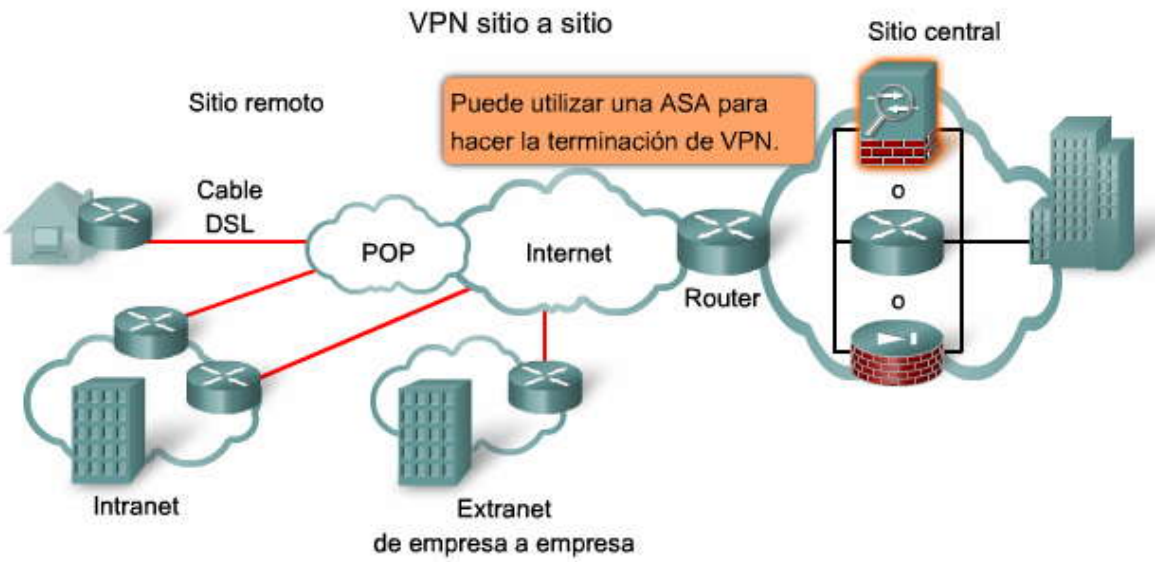
Si se los compara con las opciones de línea alquilada, las ventajas de VPN incluyen ahorro de costos, más seguridad y mayor escalabilidad.

6.3.2 Tipos de VPN

Las organizaciones usan las VPN de sitio a sitio para conectar ubicaciones remotas, tal como se usa una línea alquilada o conexión Frame Relay. Debido a que la mayoría de las organizaciones ahora tiene acceso a Internet, es lógico aprovechar los beneficios de las VPN de sitio a sitio. Como se muestra en la figura, las VPN de sitio a sitio también admiten intranets de la empresa y extranets de los socios comerciales.

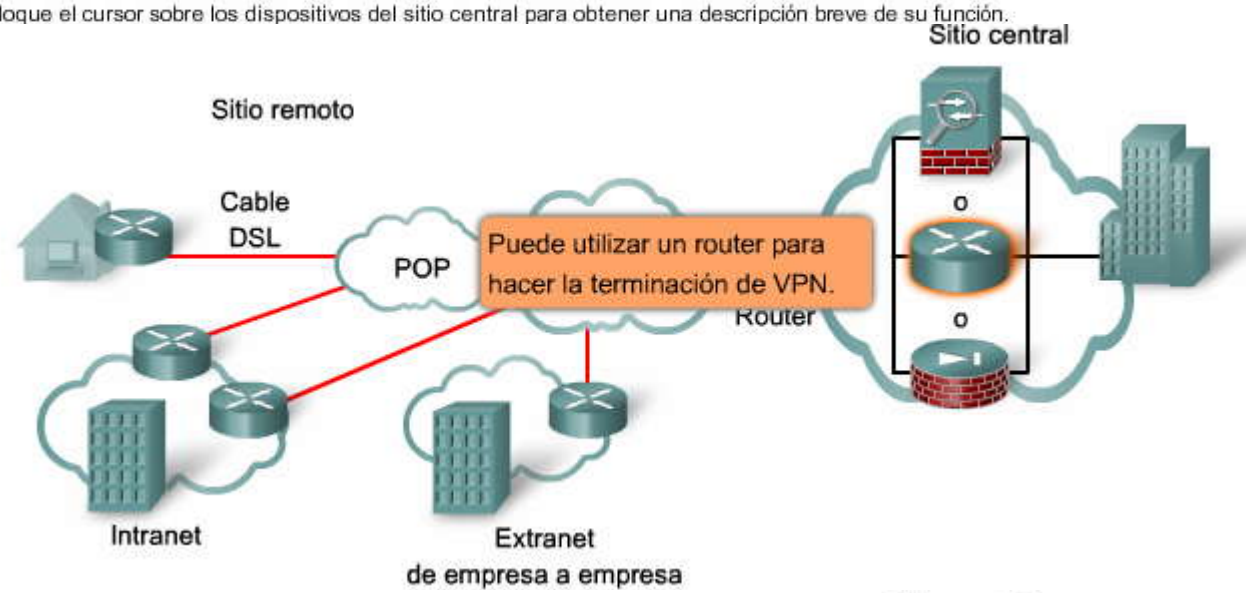
De hecho, una VPN de sitio a sitio es una extensión de una networking WAN clásica. Las VPN de sitio a sitio conectan redes enteras entre ellas. Por ejemplo, pueden conectar la red de una sucursal a la red de la sede central corporativa.

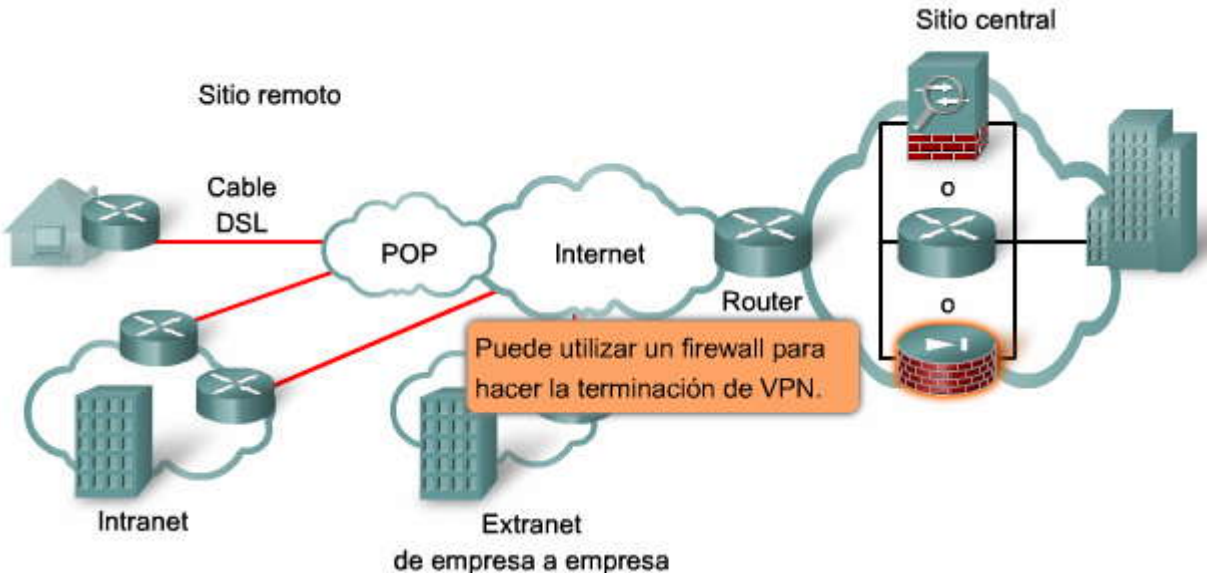
En una VPN de sitio a sitio, los hosts envían y reciben tráfico TCP/IP a través de un gateway VPN, el cual podría ser un router, una aplicación firewall PIX o una aplicación de seguridad adaptable (ASA). El gateway VPN es responsable de la encapsulación y encriptación del tráfico saliente para todo el tráfico desde un sitio particular y de su envío a través de un túnel VPN por Internet a un gateway VPN par en el sitio objetivo. Al recibirlo, el gateway VPN par elimina los encabezados, descifra el contenido y retransmite el paquete hacia el host objetivo dentro de su red privada.



Las VPN de sitio a sitio son extensiones de la WAN clásica.

Coloque el cursor sobre los dispositivos del sitio central para obtener una descripción breve de su función.

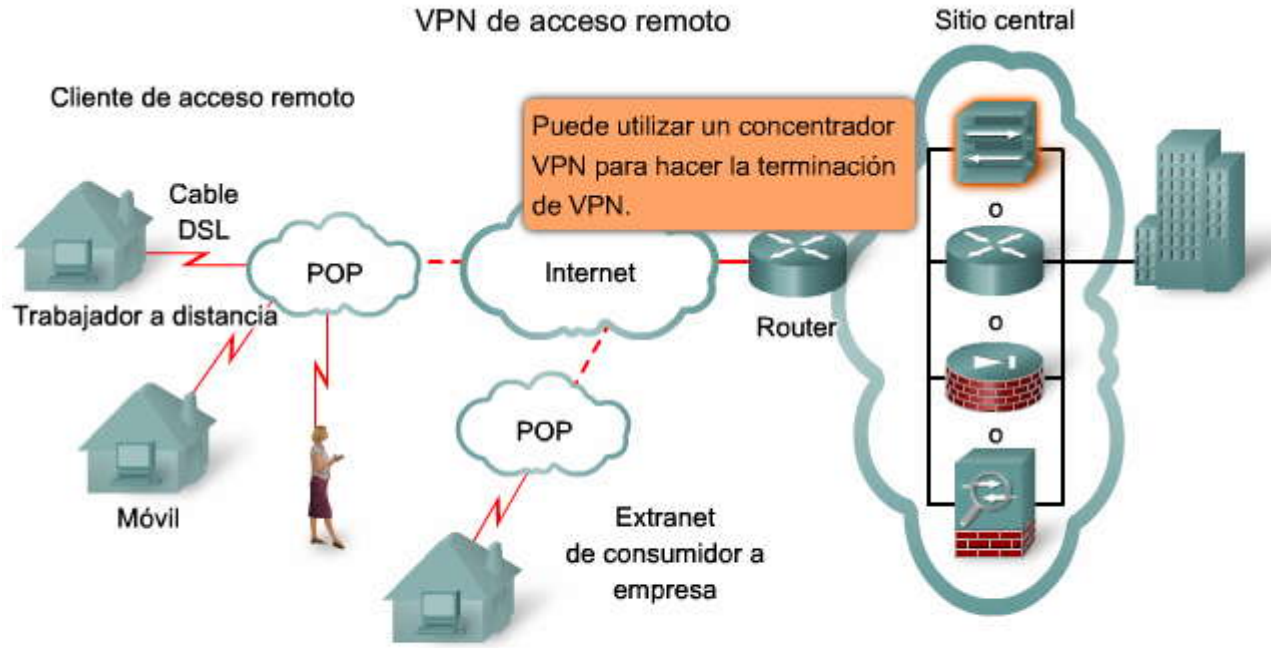




Los usuarios móviles y trabajadores a distancia usan mucho las VPN de acceso remoto. En el pasado, las empresas admitían usuarios remotos con redes dial-up. En general, esto implicaba una llamada de larga distancia y los costos correspondientes para lograr el acceso a la empresa.

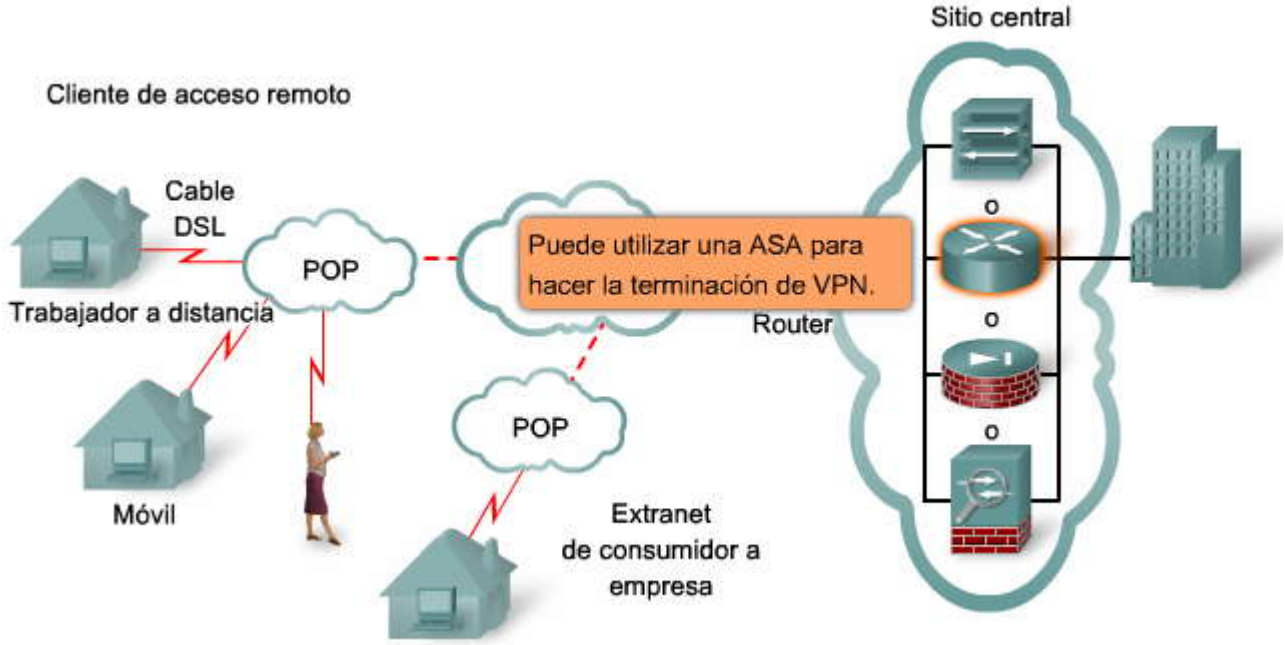
La mayoría de los trabajadores a distancia ahora tienen acceso a Internet desde sus hogares y pueden establecer VPN remotas por medio de las conexiones de banda ancha. De manera similar, un trabajador móvil puede realizar una llamada local a un ISP local para lograr el acceso a la empresa a través de Internet. De hecho, esto marca un avance de evolución en las redes dial-up. Las VPN de acceso remoto pueden admitir las necesidades de los trabajadores a distancia, los usuarios móviles, además de las extranets de consumidores a empresas.

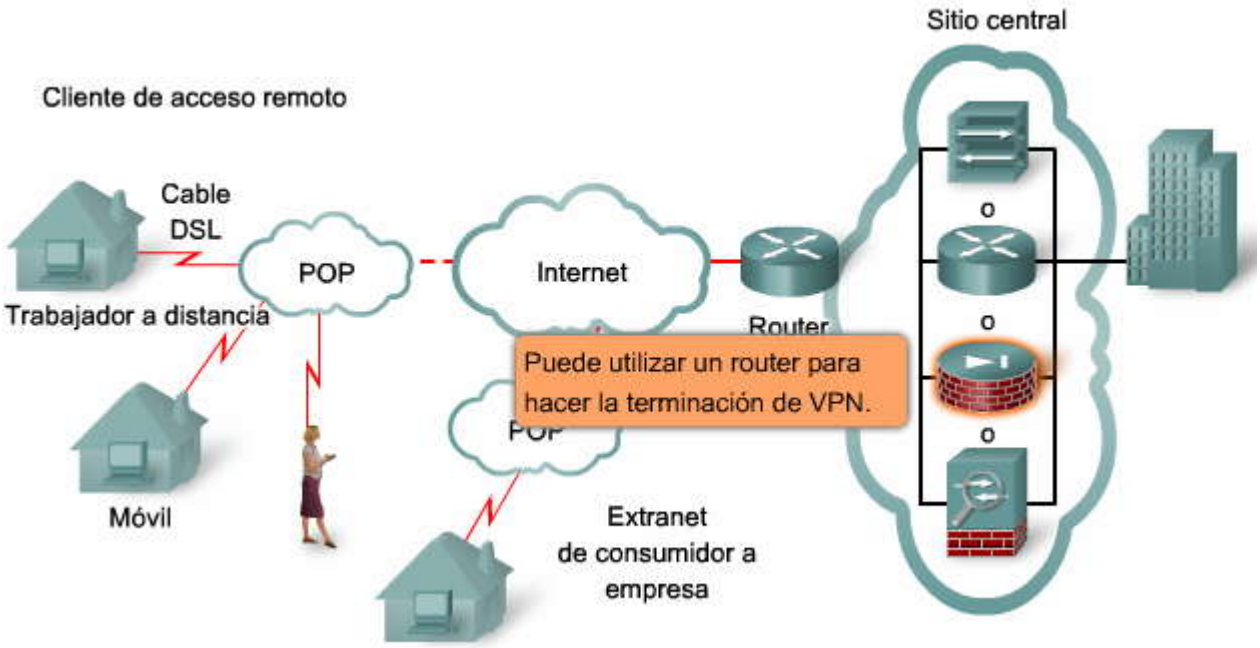
En una VPN de acceso remoto, cada host en general tiene software cliente de VPN. Cuando el host intenta enviar tráfico, el software cliente de VPN encapsula y encripta ese tráfico antes del envío a través de Internet hacia el gateway VPN en el borde de la red objetivo. Al recibirlo, el gateway VPN maneja los datos de la misma manera en que lo haría con los datos de una VPN de sitio a sitio.

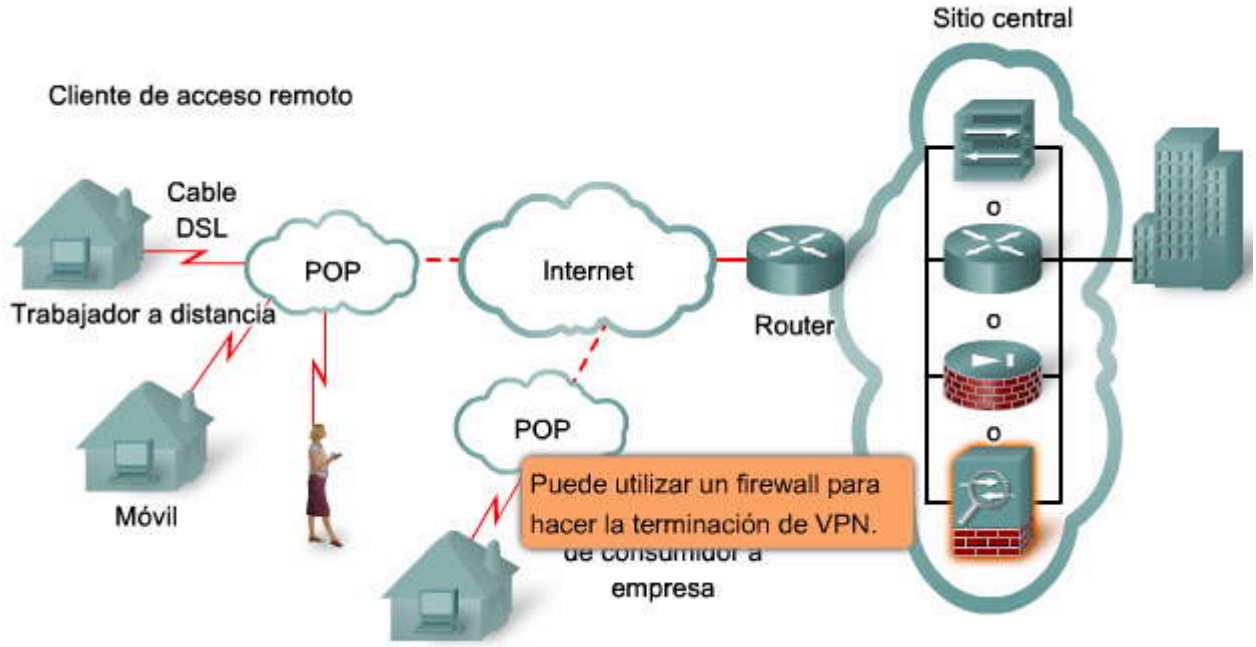


Las VPN de acceso remoto marcan un paso en la evolución de las redes ISDN y dial-up.

Coloque el cursor sobre los dispositivos del sitio central para obtener una descripción breve de su función.







6.3.3 Componentes de la VPN

La VPN crea una red privada a través de una infraestructura de red pública, mientras mantiene la confidencialidad y la seguridad. Las VPN usan protocolos de tunneling criptográficos para brindar protección contra detectores de paquetes, autenticación de emisores e integración de mensajes.

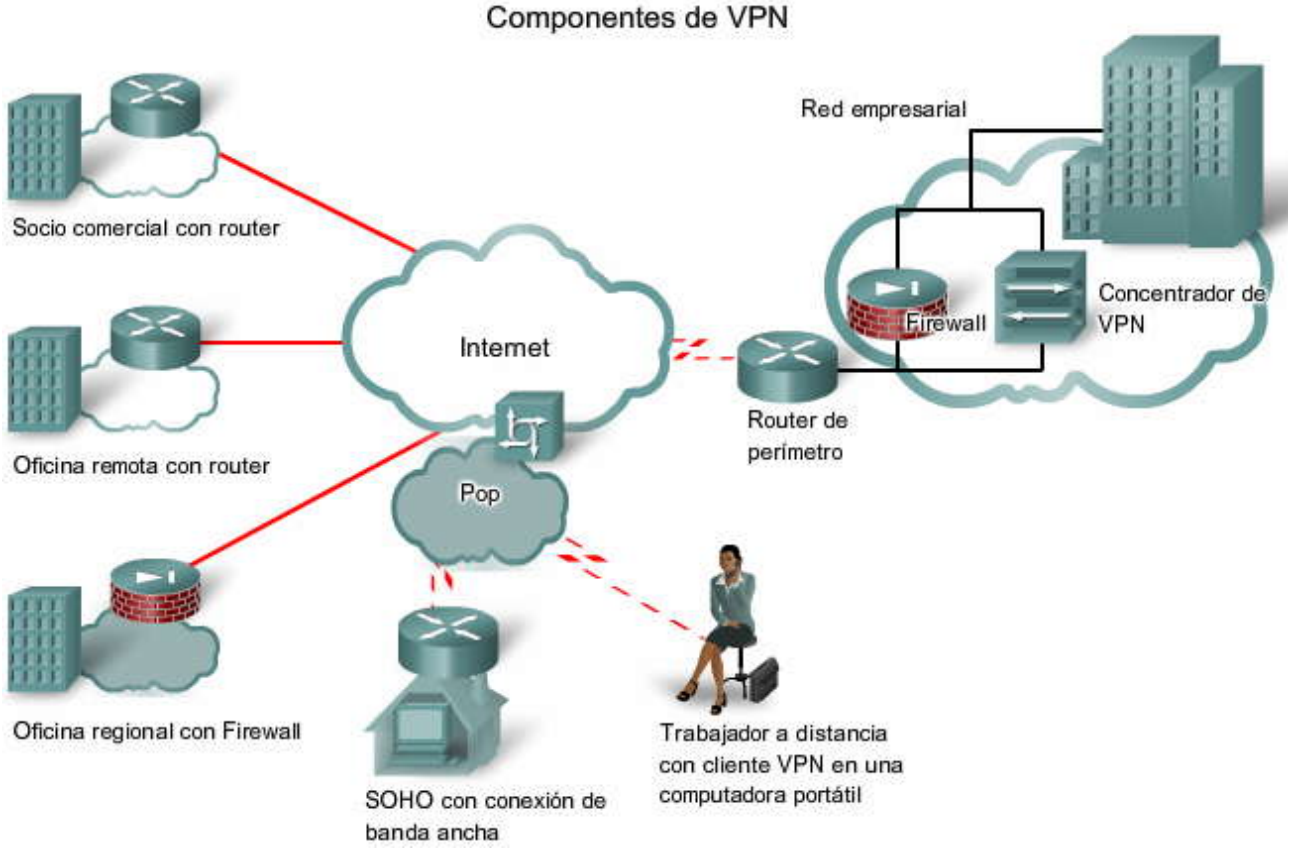
La figura muestra una topología de VPN típica. Los componentes necesarios para establecer esta VPN incluyen lo siguiente:

- Una red existente con servidores y estaciones de trabajo
- Una conexión a Internet
- Gateways VPN, como routers, firewalls, concentradores VPN y ASA, que actúan como extremos para establecer, administrar y controlar las conexiones VPN
- Software adecuado para crear y administrar túneles VPN

La clave de la eficacia de la VPN es la seguridad. Las VPN protegen los datos mediante encapsulación o encriptación. La mayoría de las VPN puede hacer las dos cosas.

- La encapsulación también se denomina tunneling, porque transmite datos de manera transparente de red a red a través de una infraestructura de red compartida.
- La encriptación codifica los datos en un formato diferente mediante una clave secreta. La decodificación vuelve los datos encriptados al formato original sin encriptar.

La encapsulación y la encriptación se analizan con detalle más adelante durante este curso.



6.3.4 Características de las VPN seguras

Las VPN utilizan técnicas de encriptación avanzada y tunneling para permitir que las conexiones de red privadas de extremo a extremo que establezcan las organizaciones a través de Internet sean seguras.

Las bases de una VPN segura son la confidencialidad, la integridad de datos y la autenticación:

- **Confidencialidad de datos**: una cuestión de seguridad que suele despertar preocupación es la protección de datos contra personas que puedan ver o escuchar subrepticiamente información confidencial. La confidencialidad de datos, que es una función de diseño, tiene el objetivo de proteger los contenidos de los mensajescontra la intercepción de fuentes no autenticadas o no autorizadas. Las VPN logran esta confidencialidad mediante mecanismos de encapsulación y encriptación.
- **Integridad de datos**: los receptores no tienen control sobre la ruta por la que han viajado los datos y, por lo tanto, no saben si alguien ha visto o ha manejado los datos mientras viajaban por Internet. Siempre existe la posibilidad de que los datos hayan sido modificados. La integridad de datos garantiza que no se realicen cambios indebidos ni alteraciones en los datos mientras viajan desde el origen al destino. Generalmente, las VPN utilizan hashes para garantizar la integridad de los datos. El hash es como una checksum o un sello (pero más robusto) que garantiza que nadie haya leído el contenido. Enel próximo tema se incluye la explicación de los hashes.
- **Autenticación**: la autenticación garantiza que el mensaje provenga de un origen auténtico y se dirija a un destino auténtico. La identificación de usuarios brinda al usuario la seguridad de que la persona con quien se comunica es quien cree que es. Las VPN pueden utilizar contraseñas, certificados digitales, tarjetas inteligentes y biométricas para establecer la identidad de las partes ubicadas en el otro extremo de la red.

Características de VPN seguras

Característica	Propósito
Confidencialidad de datos	Protege los datos contra personas que puedan ver o escuchar subrepticiamente información confidencial (spoofing).
Integridad de datos	Garantiza que no se realicen cambios indebidos ni alteraciones en los datos.
Autenticación	Garantiza que sólo ingresen en la red emisores y dispositivos autorizados.

La confidencialidad de datos y la integridad de datos dependen de la encriptación y la encapsulación

6.3.5 Tunneling de VPN

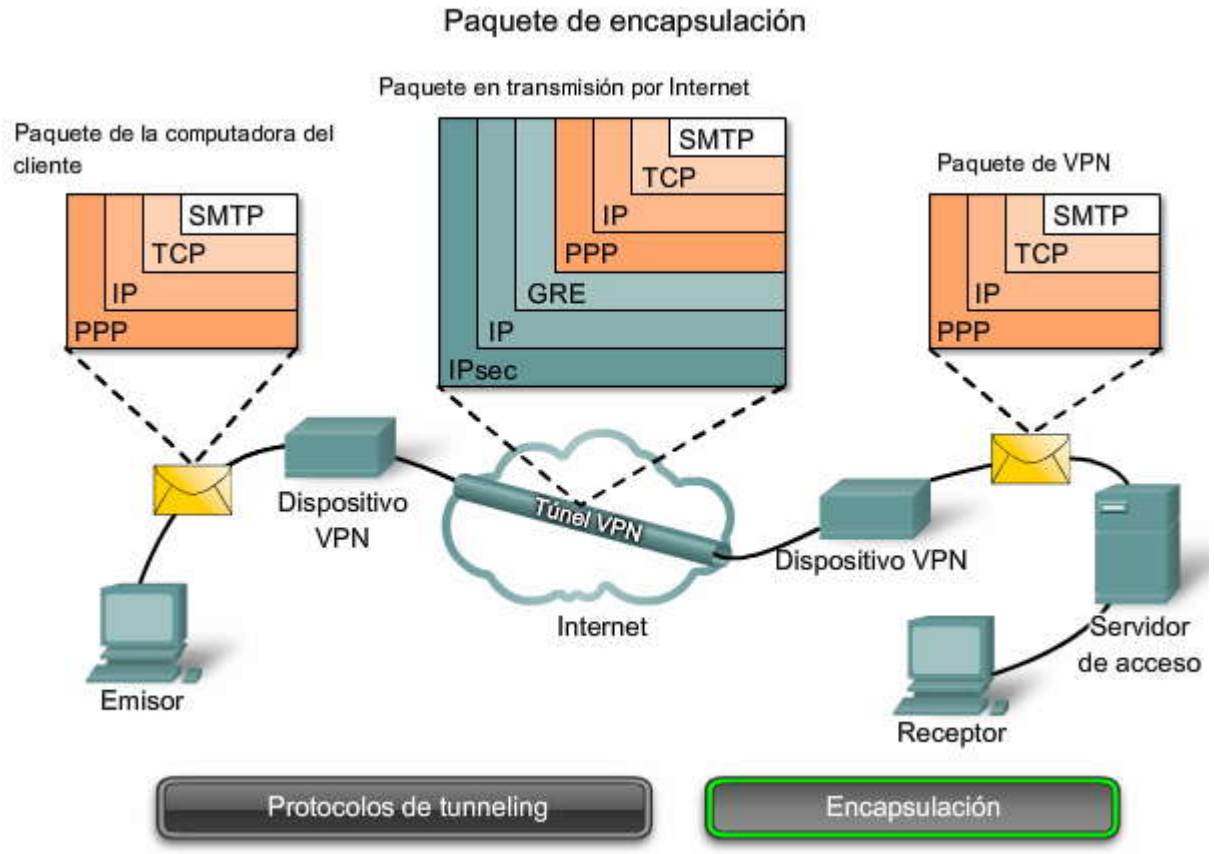
La incorporación de capacidades de confidencialidad de datos adecuadas en una VPN garantiza que sólo los orígenes y los destinos indicados sean capaces de interpretar los contenidos del mensaje original.

El tunneling permite el uso de redes públicas como Internet para transportar datos para usuarios, siempre que los usuarios tengan acceso a una red privada. El tunneling encapsula un paquete entero dentro de otro paquete y envía por una red el nuevo paquete compuesto. Esta figura contiene una lista de las tres clases de protocolos que utiliza el tunneling.

Para ilustrar el concepto de tunneling y las clases de protocolos de tunneling, veamos un ejemplo de un envío de una tarjeta navideña por correo tradicional. La tarjeta navideña tiene un mensaje adentro. La tarjeta es el protocolo pasajero. El emisor coloca la tarjeta dentro de un sobre (protocolo de encapsulación) y escribe las direcciones correctas. Luego, deposita el sobre en el buzón de correo para que sea entregado. El sistema postal (protocolo portador) busca y entrega el sobre en el buzón del receptor. Los dos extremos del sistema portador son las "interfaces del túnel". El receptor quita la tarjeta navideña (extrae el protocolo pasajero) y lee el mensaje.

Haga clic en el botón Encapsulación de la figura para ver una ilustración del proceso de encapsulación.

Esta figura muestra un mensaje de correo electrónico que viaja por Internet a través de una conexión VPN. PPP transmite el mensaje al dispositivo VPN, donde el mensaje se encapsula dentro de un paquete de Encapsulamiento de enrutamiento genérico (GRE). El GRE es un protocolo de tunneling desarrollado por Cisco Systems que puede encapsular una amplia variedad de tipos de paquetes de protocolo dentro de túneles IP, lo que crea un enlace virtual punto a punto con los routers Cisco en puntos remotos, a través de una internetwork IP. En la figura, el direccionamiento del paquete de origen y de destino externo se asigna a "interfaces del túnel" y se hace enrutable a través de la red. Una vez que el paquete compuesto llega a la interfaz del túnel de destino, se extrae el paquete interno.

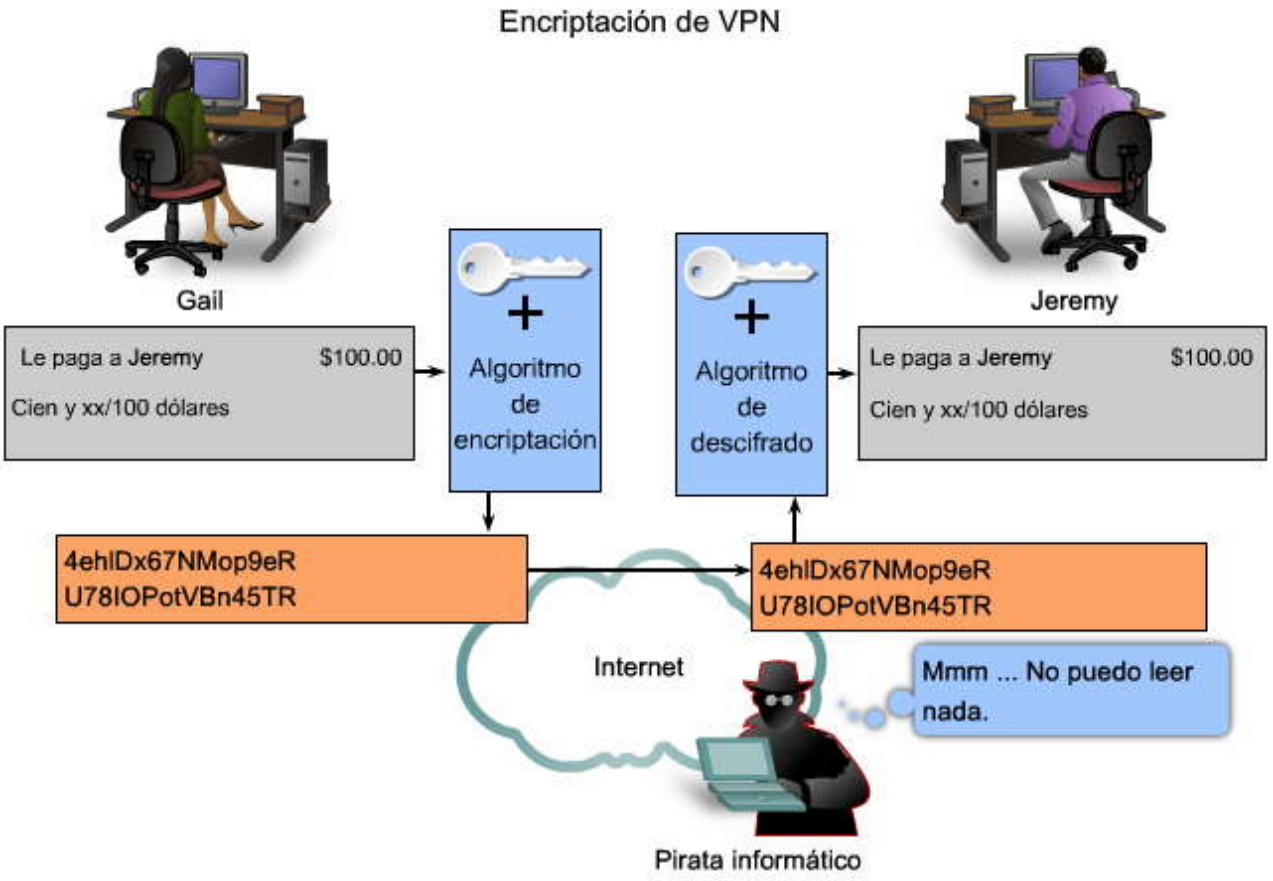


6.3.6 Integridad de datos de la VPN

Si por Internet pública se transporta texto sin formato, puede ser interceptado y leído. Para mantener la privacidad de los datos, es necesario encriptarlos. La encriptación VPN encripta los datos y los vuelve ilegibles para los receptores no autorizados.

Para que la encriptación funcione, tanto el emisor como el receptor deben conocer las reglas que se utilizan para transformar el mensaje original en la versión codificada. Las reglas de encriptación de la VPN incluyen un algoritmo y una clave. Un algoritmo es una función matemática que combina mensaje, texto, dígitos o los tres con una clave. El resultado es una cadena de cifrado ilegible. El descifrado es extremadamente difícil o imposible sin la clave correcta.

En el ejemplo, Gail desea enviar un documento de finanzas a Jeremy por Internet. Gail y Jeremy han acordado previamente una clave secreta compartida. En el extremo de Gail, el software de cliente de la VPN combina el documento con la clave secreta compartida y lo pasa por un algoritmo de encriptación. El resultado es un textocifrado indescifrable. El texto cifrado se envía mediante un túnel de la VPN o por Internet. En el otro extremo, el mensaje se vuelve a combinar con la misma clave secreta compartida y se lo procesa con el mismo algoritmo de encriptación. El resultado esel documento de finanzas original, que ahora es legible para Jeremy.



El grado de seguridad que proporciona un algoritmo de encriptación depende de la longitud de la clave. Para cualquier longitud de clave, el tiempo que lleva el procesamiento de todas las posibilidades de descifrar texto cifrado es una función de la potencia de cómputo del equipo. Por lo tanto, cuanto más corta sea la clave, más fácil será romperla; pero, a su vez, más fácil pasar el mensaje.

Algunos de los algoritmos de encriptación más comunes y la longitud de claves que se utilizan son los siguientes:

- **Algoritmo Estándar de cifrado de datos (DES)**: DES, desarrollado por IBM, utiliza una clave de 56 bits para garantizar una encriptación de alto rendimiento. El DES es un sistema de encriptación de clave simétrica. Las claves simétricas y asimétricas se explican más adelante.
- **Algoritmo Triple DES (3DES)**: una variante más reciente del DES que realiza la encriptación con una clave, descifra con otra clave y realiza la encriptación por última vez con otra clave también diferente. 3DES le proporciona mucha más fuerza al proceso de encriptación.
- **Estándar de encriptación avanzada (AES)**: el Instituto Nacional de Normas y Tecnología (NIST) adoptó el AES para reemplazar la encriptación DES en los dispositivos criptográficos. AES proporciona más seguridad que DES y es más eficaz en cuanto a su cálculo que 3DES. AES ofrece tres tipos de longitudes de clave: claves de 128, 192 y 256 bits.
- **Rivest, Shamir y Adleman (RSA)**: sistema de encriptación de clave asimétrica. Las claves utilizan una longitud de bits de 512, 768, 1024 o superior.

Encriptación simétrica

Los algoritmos de encriptación como DES y 3DES requieren que una clave secreta compartida realice la encriptación y el descifrado. Los dos equipos deben conocer la clave para decodificar la información. Con la encriptación de clave simétrica, también llamada encriptación de clave secreta, cada equipo encripta la información antes de enviarla por la red al otro equipo. La encriptación de clave simétrica requiere el conocimiento de los equipos que se comunicarán para poder configurar la misma clave en cada uno.

Por ejemplo, un emisor crea un mensaje codificado en el cual cada letra se sustituye con la letra que se encuentra dos posiciones adelante en el alfabeto; "A" se convierte en "C" y "B" se convierte en "D" y así sucesivamente. En este caso, la palabra SECRETO se convierte en UGETGVQ. El emisor le ha informado al receptor que la clave secreta es "saltear 2". Cuando el receptor recibe el mensaje UGETGVQ, su equipo decodifica el mensaje al calcular las dos letras anteriores a las

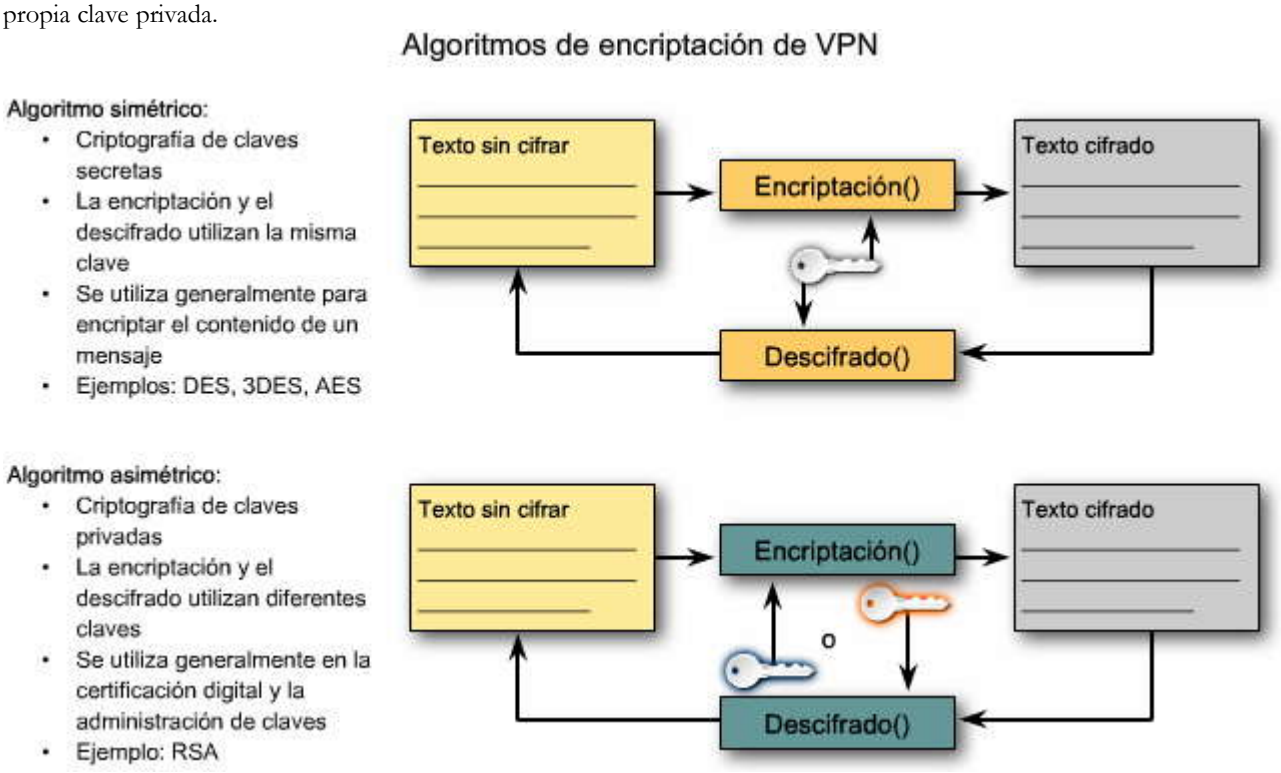
del mensaje y llega al código SECRETO. Cualquier otra persona que vea el mensaje sólo verá el mensaje cifrado, que parece una frase sin sentido a menos que la persona conozca la clave secreta.

La pregunta es, ¿cómo el dispositivo de encriptación y el de descifrado tienen la misma clave secreta compartida? Puede utilizar el correo electrónico, un mensajero o un correo de 24 horas para enviar las claves secretas compartidas a los administradores de los dispositivos. Otro método más fácil y más seguro es la encriptación asimétrica.

Encriptación asimétrica

La encriptación asimétrica utiliza diferentes claves para la encriptación y el descifrado. El conocimiento de una de las claves no es suficiente para que un pirata informático deduzca la segunda clave y decodifique la información. Una clave realiza la encriptación del mensaje y otra, el descifrado. No es posible realizar ambos con la misma clave.

La encriptación de clave pública es una variante de la encriptación asimétrica que utiliza una combinación de una clave privada y una pública. El receptor le da una clave pública a cualquier emisor con quien desee comunicarse el receptor. El emisor utiliza una clave privada junto con la clave pública del receptor para encriptar el mensaje. Además, el emisor debe compartir la clave pública con el receptor. Para descifrar un mensaje, el receptor utiliza la clave pública del emisor y su propia clave privada.



Los hashes contribuyen a la autenticación y la integridad de los datos, ya que garantizan que personas no autorizadas no alteren los mensajes transmitidos. Un hash, también denominado message digest, es un número generado a partir de una cadena de texto. El hash es menor que el texto. Se genera mediante una fórmula, de forma tal que es extremadamente improbable que otro texto produzca el mismo valor de hash.

El emisor original genera un hash del mensaje y lo envía junto con el mensaje mismo. El receptor descifra el mensaje y el hash, produce otro hash a partir del mensaje recibido y compara bs dos hashes. Si son iguales, puede estar seguro de que la integridad del mensaje no ha sido afectada.

En la figura, alguien está intentando enviarle a Jeremy un cheque por 100 dólares. En el extremo remoto, Alex Jones (probablemente un delincuente) está intentando cobrar el cheque en efectivo por 1000 dólares. El cheque fue alterado a medida que avanzaba mediante Internet. Se cambiaron el receptor y el monto en dólares. En este caso, si se hubiera utilizado el algoritmo de integridad de datos, los hashes no habrían coincidido y la transacción no habría tenido validez.

Los datos de la VPN se transportan por Internet pública. Tal como se mostró, hay posibilidades de que estos datos sean interceptados y modificados. Como protección frente a esta amenaza, los hosts pueden agregarle un hash al mensaje. Si el hash transmitido coincide con el recibido, significa que se ha preservado la integridad del mensaje. Sin embargo, si no coinciden, el mensaje ha sido alterado.

Las VPN utilizan un código de autenticación de mensajes para verificar la integridad y la autenticidad de un mensaje, sin utilizar mecanismos adicionales. Un código de autenticación de mensajes de hash (HMAC) en clave es un algoritmo de integridad de datos que garantiza la integridad del mensaje.

El HMAC tiene dos parámetros: un mensaje de entrada y una clave secreta que sólo conocen el creador del mensaje y los receptores adecuados. El emisor del mensaje utiliza una función HMAC para producir un valor (el código de autenticación del mensaje) que se forma al condensar la clave secreta y el mensaje de entrada. El código de autenticación del mensaje se envía junto con el mensaje. El receptor calcula el código de autenticación del mensaje en el mensaje recibido con la misma clave y la misma función HMAC que utilizó el emisor y compara los resultados calculados con el código de autenticación del mensaje. Si los dos valores coinciden, el mensaje se ha recibido correctamente y el receptor está seguro de que el emisor es un miembro de la comunidad de usuarios que comparten la clave. La fuerza criptográfica de HMAC depende de la fuerza criptográfica de la función hash subyacente en cuanto al tamaño y a la calidad de la clave, y en el tamaño de la longitud del resultado de hash en bits.

Hay dos algoritmos HMAC comunes:

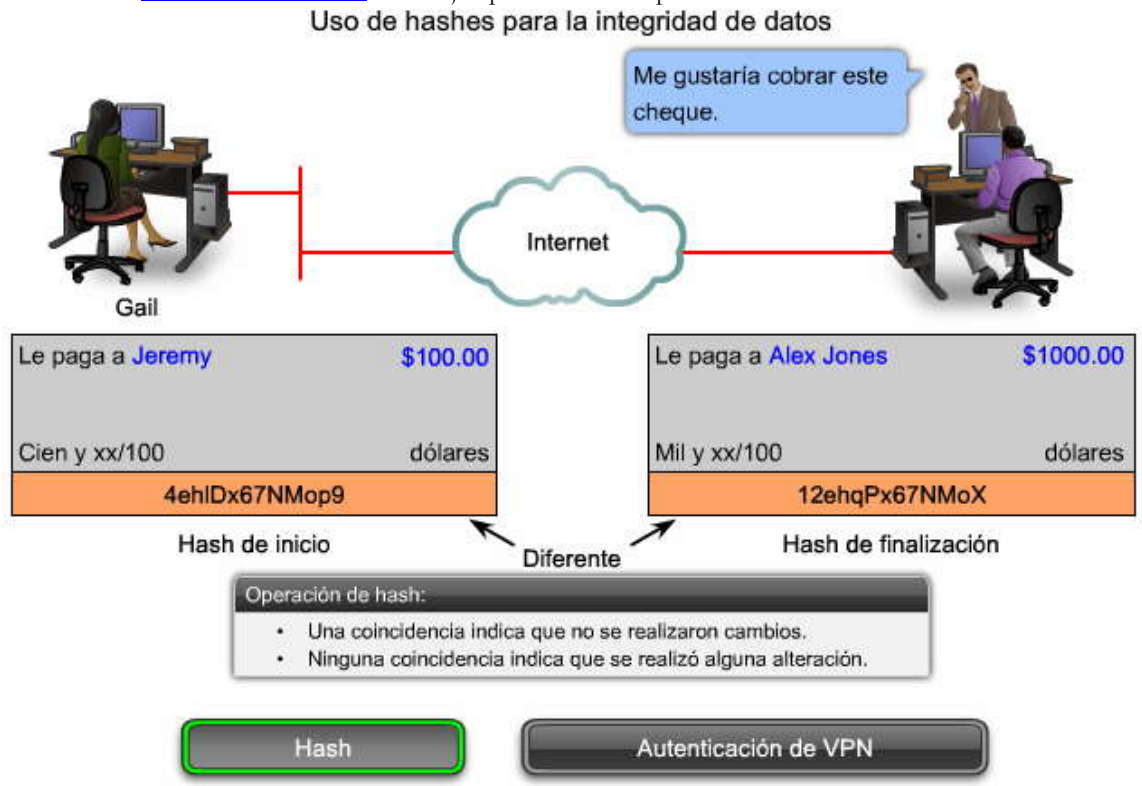
- **Message Digest 5 (MD5)**: utiliza una clave secreta compartida de 128 bits. El mensaje de longitud variable y la clave secreta compartida de 128 bits se combinan y se ejecutan mediante el algoritmo de hash HMAC-MD5. El resultado es un hash de 128 bits. El hash se agrega al mensaje original y se envía al extremo remoto.
- **Algoritmo de hash seguro 1 (SHA-1)**: utiliza una clave secreta de 160 bits. El mensaje de longitud variable y la clave secreta compartida de 160 bits se combinan y se ejecutan mediante el algoritmo de hash HMAC-SHA-1. El resultado es un hash de 160 bits. El hash se agrega al mensaje original y se envía al extremo remoto.

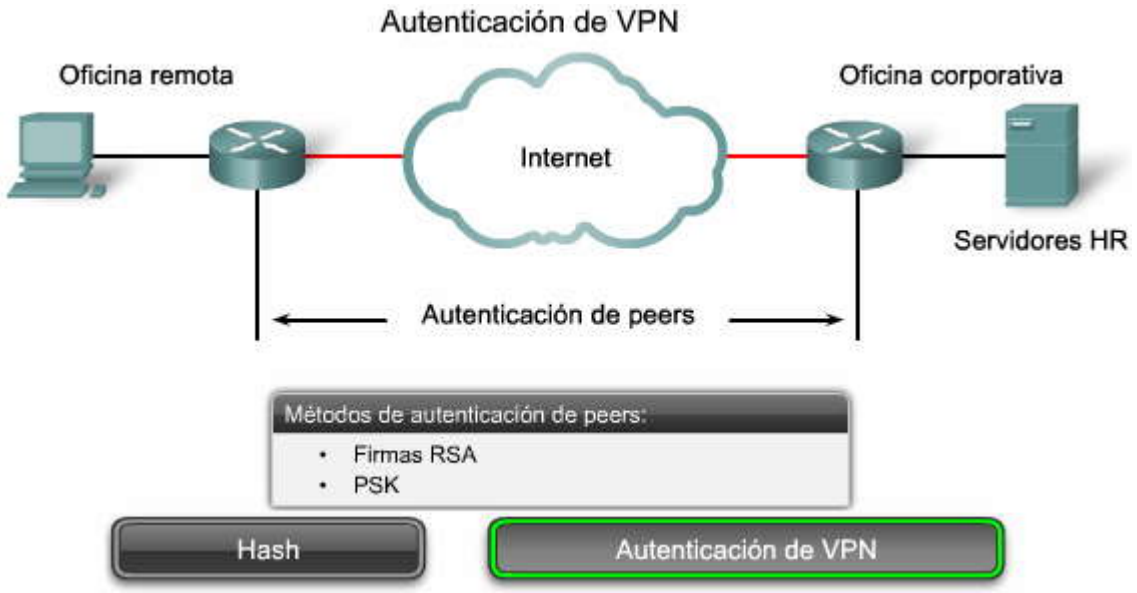
Haga clic en el botón Autenticación de VPN de la figura.

Cuando se realizan negocios a larga distancia, es necesario saber quién está del otro lado del teléfono, correo electrónico o fax. Lo mismo sucede con las redes VPN. Se debe autenticar el dispositivo ubicado en el otro extremo del túnel de la VPN antes de que la ruta de comunicación se considere segura. Hay dos métodos pares de autenticación:

- **Clave compartida previamente (PSK)**: una clave secreta compartida entre dos partes que utilizan un canal seguro antes de que deba ser utilizado. Las PSK utilizan algoritmos criptográficos de clave simétrica. Una PSK se especifica en cada par manualmente y se utiliza para autenticar al par. En cada extremo, la PSK se combina con otra información para formar la clave de autenticación.
- **Firma RSA**: utiliza el intercambio de certificados digitales para autenticar los pares. El dispositivo local deriva un hash y lo encripta con su clave privada. El hash encriptado (firma digital) se adjunta al mensaje y se envía al extremo remoto. En el extremo remoto, el hash encriptado se descifra mediante la clave pública del extremo local. Si el hash descifrado coincide con el hash recalculado, la firma es verdadera.

Observe una demostración de RSA como ejemplo de una encriptación RSA.





6.3.7 Protocolos de seguridad IPsec

El IPsec es un conjunto de protocolos para la seguridad de las comunicaciones IP que proporciona encriptación, integridad y autenticación. IPsec ingresa el mensaje necesario para proteger las comunicaciones VPN, pero se basa en algoritmos existentes.

Existen dos protocolos de estructura IPsec.

- **Encabezado de autenticación (AH)**: se utiliza cuando no se requiere o no se permite la confidencialidad. AH proporciona la autenticación y la integridad de datos para paquetes IP intercambiados entre dos sistemas. Verifica que cualquier mensaje intercambiado de R1 a R3 no haya sido modificado en el camino. También verifica que el origen de los datos sea R1 o R2. AH no proporciona la confidencialidad de datos (encriptación) de los paquetes. Si se loutiliza solo, el protocolo AH proporciona poca protección. Por lo tanto, se lo utiliza junto con el protocolo ESP para brindar las funciones de seguridad de la encriptación de los datos y el alerta contra alteraciones.
- **Contenido de seguridad encapsulado (ESP)**: proporciona confidencialidad y autenticación mediante la encriptación del paquete IP. La encriptación del paquete IP oculta los datos y las identidades de origen y de destino. ESP autentica el paquete IP interno y el encabezado ESP. La autenticación proporciona autenticación del origen de datos e integridad de datos. Aunque tanto la encriptación como la autenticación son opcionales en ESP, debe seleccionar una como mínimo.

Haga clic en el botón Estructura IPsec de la figura.

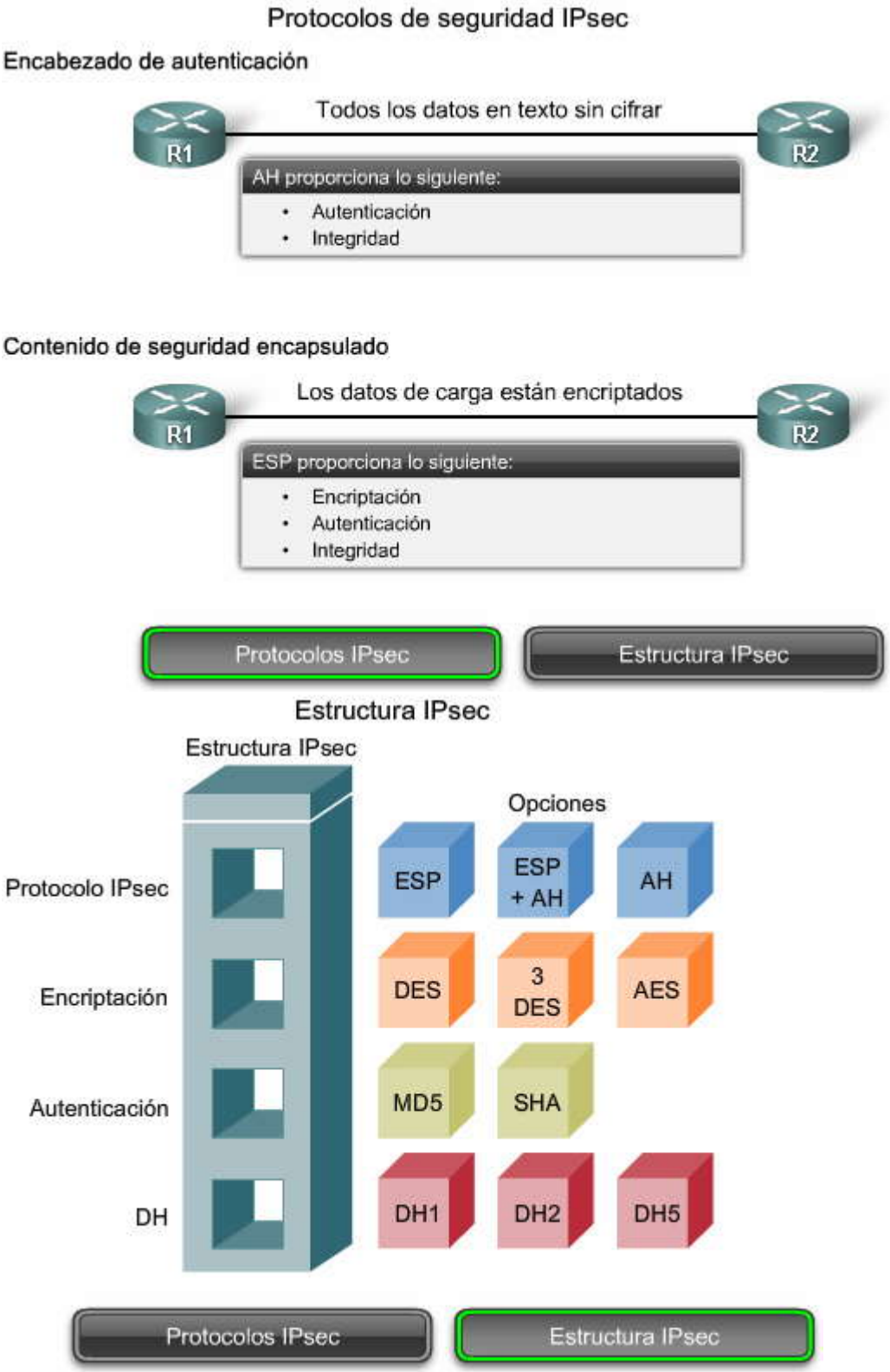
IPsec se basa en algoritmos existentes para implementar la encriptación, la autenticación y el intercambio de claves. Algunos de los algoritmos estándar que utiliza IPsec son:

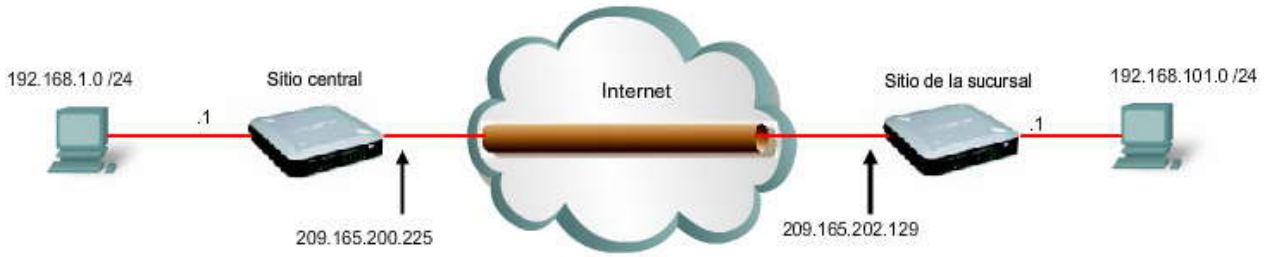
- DES: encripta y descifra los datos del paquete.
- 3DES: proporciona una fuerza de encriptación importante superior al DES de 56 bits.
- AES: proporciona un rendimiento más rápido y una encriptación más fuerte según la longitud de la clave utilizada.
- MD5: autentica datos de paquetes con una clave secreta compartida de 128 bits.
- SHA-1: autentica datos de paquetes con una clave secreta compartida de 160 bits.
- DH; permite que dos partes establezcan una clave secreta compartida mediante la encriptación y los algoritmos de hash, como DES y MD5, sobre un canal de comunicaciones no seguro.

La figura muestra cómo se configura IPsec. IPsec proporciona la estructura y el administrador elige los algoritmos utilizados para implementar los servicios de seguridad dentro de esa estructura. Existen cuatro apartados de estructura IPsec que deben completarse.

- Cuando configura un gateway de IPsec para proporcionar servicios de seguridad, primero elija un protocolo IPsec. Las opciones son ESP o ESP con AH.
- El segundo apartado es un algoritmo de encriptación si IPsec se implementa con ESP. Seleccione el algoritmo de encriptación adecuado para el nivel de seguridad deseado: DES, 3DES o AES.

- El tercer apartado es la autenticación. Seleccione un algoritmo de autenticación para proporcionar la integridad de los datos: MD5 o SHA.
- El último apartado es el grupo de algoritmos Diffie-Hellman (DH). Establece que los pares compartan la información de clave. Seleccione el grupo que desea utilizar: DH1 o DH2.





En esta actividad, se proporciona un simulacro de una pequeña compañía que ha establecido conectividad a Internet con dos routers tipo comercial Linksys WRVS4400N. Uno está ubicado en el sitio central y el otro en el sitio de la sucursal. Les gustaría acceder a recursos entre los sitios, pero les preocupa que el tráfico de Internet no sea seguro. Para atender esta preocupación, se les ha sugerido que implementen una VPN sitio a sitio. Una VPN permitiría que el sitio de la sucursal se conectara al sitio central de forma segura creando un túnel de VPN que encriptaría y descifraría datos.

Con respecto a la topología, utilizará la herramienta de configuración web del router Linksys para configurar los parámetros y habilitar una VPN llamada **Sitio a sitio** con autenticación MD5, encriptación 3DES y una clave precompartida de **cisco123**.

Situación | Central | Sucursal

IPsec VPN

Select Tunnel Entry: --new-- | Delete | Summary

IPsec VPN Tunnel: (•) Enable ( ) Disable

Tunnel Name: Site-to-Site

Local Security Group:

Local Security Group Type: Subnet

IP Address: 192.168.1.0

255 . 255 . 255 . 0

Remote Security Group:

Remote Security Group Type: Subnet

IP Address: 192.168.101.0

Subnet Mask: 255 . 255 . 255 . 0

Remote Security Gateway:

Remote Security Gateway Type: IP Addr.

IP Address: 209.165.202.129

Key Management:

Key Exchange Method: Auto.(IKE)

Encryption: 3DES

Authentication: MD5

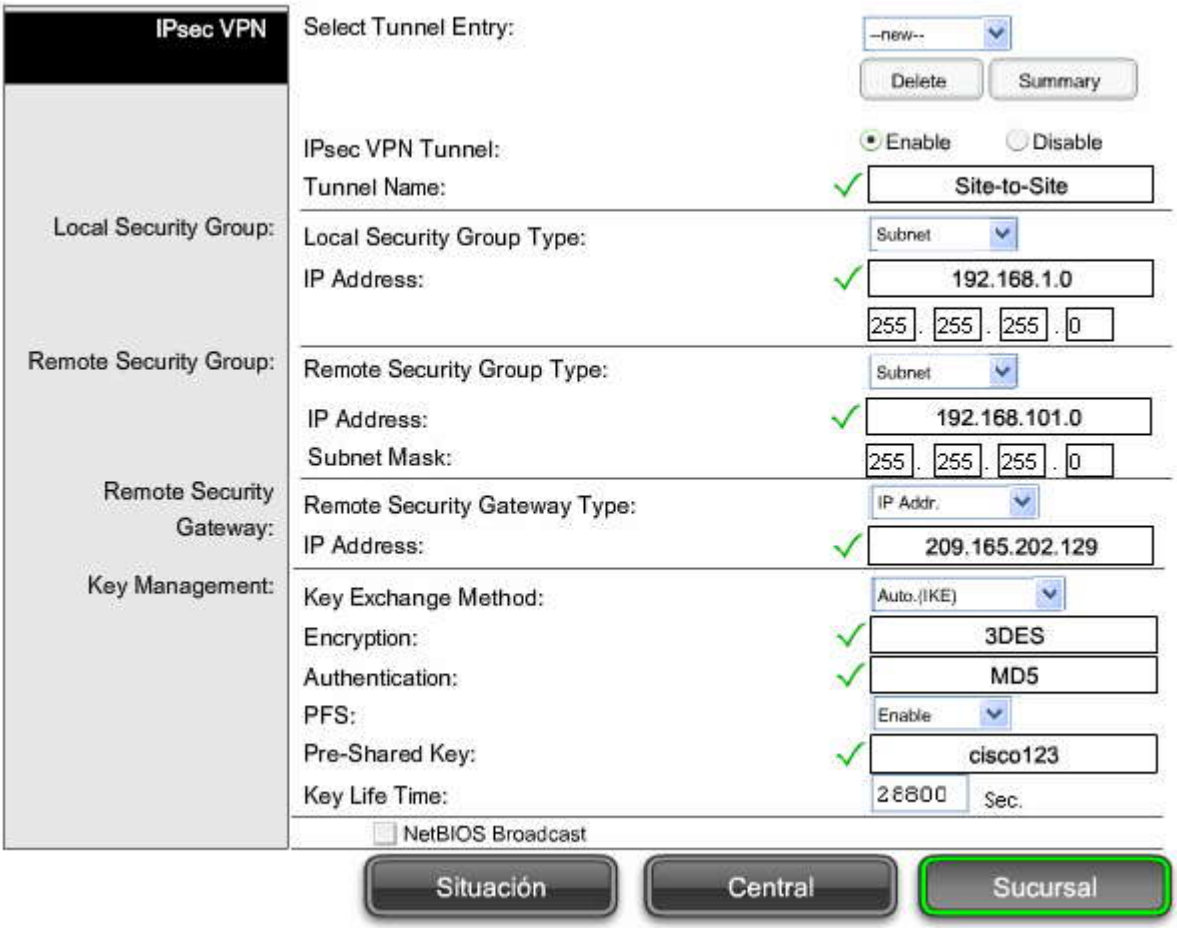
PFS: Enable

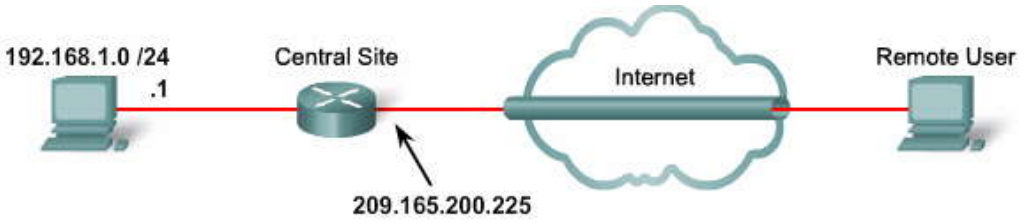
Pre-Shared Key: cisco123

Key Life Time: 28800 Sec

[ ] NetBIOS Broadcast

Situación | Central | Sucursal





Una compañía pequeña ha establecido conectividad a Internet con un router de clase comercial Linksys WRVS4400N en su sitio central. Les gustaría proporcionar acceso remoto para seleccionar usuarios de otras ubicaciones, pero les preocupa que el tráfico de Internet no sea seguro. Para atender esta preocupación, se les ha sugerido que implemente una VPN de acceso remoto que les permitirá a los trabajadores a distancia acceder de forma segura a la red del sitio central. Con el software cliente de Linksys QuickVPN, los trabajadores remotos podrían conectarse y establecer una conexión de VPN de acceso remoto que encripte y descifre datos.

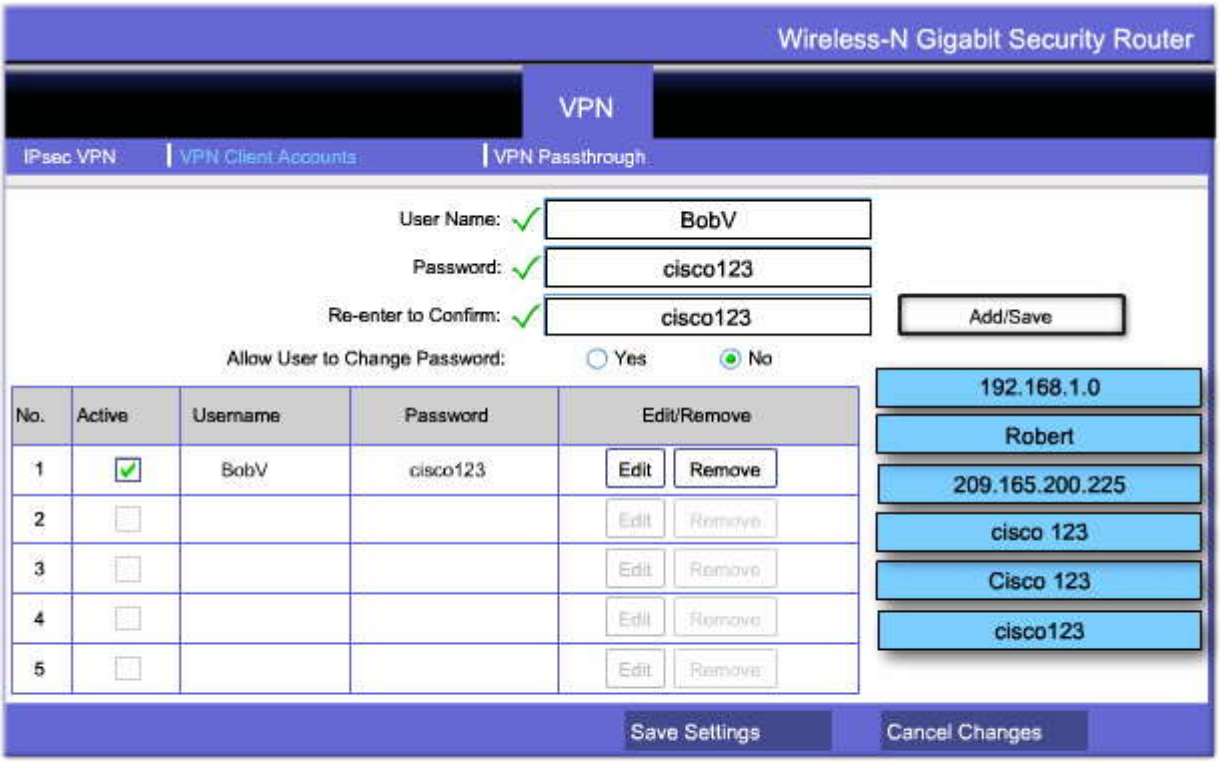
Con respecto a la topología, utilizará una herramienta de configuración web del router Linksys para configurar los parámetros de VPN remota y configurar una cuenta de usuario. El nombre del usuario es BobV y su contraseña es cisco123.

Después, Bob iniciará una conexión de VPN remota con router del sitio central utilizando el software cliente de Linksys QuickVPN. El nombre del perfil debe ser Sitio central y se debe indicar el nombre de usuario, la contraseña y la dirección IP correctos.

Situación | Central | Remota

Actividad

Arrastre y coloque la variable de VPN adecuada en el campo correcto y haga clic en Add/Save.



Situación | Central | Remota

Actividad

Arrastre y coloque la variable de VPN adecuada en el campo correcto y haga clic en Connect.

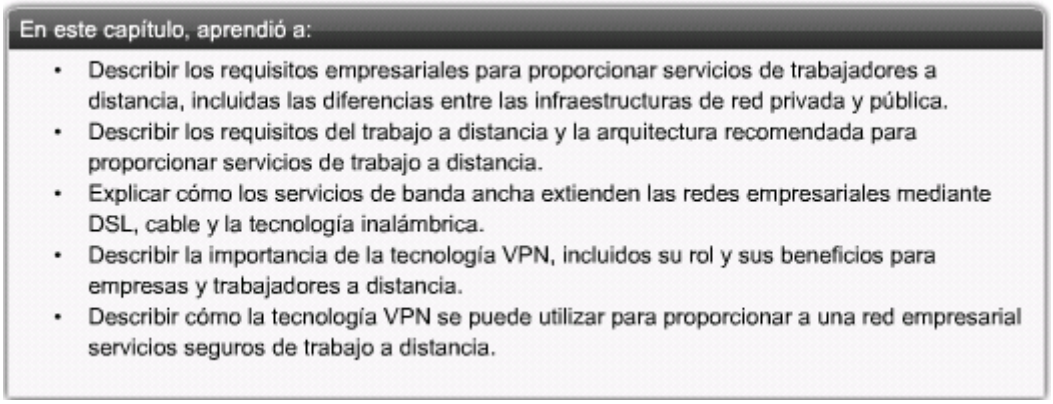
User
Central Site
192.168.1.0
209.165.200.225
BobV
Cisco123
Cisco1233
192.168.1.1
Cisco 123
Branch Site
Robert
cisco 123
cisco123

Situación | Central | Remota

6.4 Resumen del capítulo

6.4.1 Resumen del capítulo

En este capítulo aprendió la importancia cada vez mayor de los trabajadores a distancia. Puede describir los requisitos de una organización para proporcionar servicios de trabajadores a distancia, según las necesidades de los propios trabajadores a distancia y lo que debe otorgarles la organización: conectividad confiable y rentable. Entre las formas elegidas para conectar trabajadores a distancia, puede describir cómo usar los servicios de banda ancha como DSL, cable y tecnología inalámbrica. Además, sabe cómo se puede utilizar la tecnología VPN para proporcionar servicios de trabajo a distancia seguros en organizaciones; incluso conoce la importancia, los beneficios, el papel y el impacto de la tecnología VPN y los tipos de acceso, componentes, tunneling y encriptación.



CAPITULO VII – "Servicios de direccionamiento IP "

7.0 Introducción del capítulo

7.0.1 Introducción

Internet y las tecnologías de IP han crecido con rapidez. Una de las razones de este crecimiento es en parte la flexibilidad del diseño original. Sin embargo, ese diseño no anticipó la popularidad de Internet con la demanda resultante de direcciones IP. Por ejemplo, cada host y cada dispositivo conectado a Internet requiere una dirección IP versión 4 (IPv4) única. A causa del enorme crecimiento, la cantidad de direcciones IP disponibles se está acabando con rapidez.

Para poder compensar esta falta de direcciones IP, se desarrollaron diferentes soluciones a cortoplazo. Dos de estas soluciones a corto plazo son las direcciones privadas y la traducción de direcciones de red (NAT, Network Address Translation).

Normalmente un host interno recibe su dirección IP, máscara de subred, dirección IP del gateway predeterminado, dirección IP del servidor DNS y otra información de un servidor de protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol). En lugar de proporcionar a los hosts internos direcciones IP de Internet válidas, el servidor de DHCP normalmente proporcionas direcciones IP de un conjunto de direcciones privado. El problema es que puede ocurrir que estos hosts necesiten direcciones IP válidas para poder tener acceso a los recursos de Internet. Aquí es donde entra en juego NAT.

NAT permite a los hosts de red internos tomar prestada una dirección IP de Internet legítima al conectarse a los recursos de Internet. Cuando el tráfico solicitado regresa, la dirección IP legítima se libera y vuelve a estar disponible para la siguiente solicitud de Internet que haga un host interno. Al usar NAT, los administradores de red sólo necesitan una o algunas direcciones IP para que el router proporcione a los hosts, en lugar de una dirección IP única para cada cliente que se une a la red. Si bien este método no parece ser eficaz, en realidad sí lo es, porque el tráfico de los hosts se traslada con mucha rapidez.

Si bien las direcciones privadas con DHCP y NAT han colaborado para reducir la necesidad de direcciones IP, se estima que para el año 2010 se agotarán las direcciones IPv4 únicas. Por este motivo, a mediados de la década del 90, el IETF solicitó propuestas para un nuevo esquema de direccionamiento IP. Así recibió la respuesta del grupo IP de próxima generación (IPng, IP Next Generation). Para 1996, el IETF comenzó a publicar una serie de RFC que definen el IPv6.

La principal característica del IPv6 que impulsa su adopción en la actualidad es el mayor espacio de direcciones: las direcciones IPv6 tienen 128 bits en comparación con los 32 bits de IPv4.

Este capítulo describe cómo implementar DHCP, NAT e IPv6 en redes empresariales.

Al completar este capítulo, usted podrá:

- Configurar DHCP en una red de sucursal de empresa. Esto incluye poder explicar las características y los beneficios de DHCP, las diferencias entre BOOTP y DHCP, el funcionamiento de DHCP y configurar, verificar y resolver problemas de DHCP.
- Configurar NAT en un router Cisco. Esto incluye explicar las características y el funcionamiento clave de NAT y la sobrecarga de NAT, explicar las ventajas y desventajas de NAT, configurar NAT y la sobrecarga de NAT para conservar el espacio de dirección IP en una red, configurar el reenvío de puertos y verificar y resolver problemas de las configuraciones NAT.
- Configurar la nueva generación de RIP (RIPng) para usar IPv6. Esto incluye explicar cómo IPv6 soluciona cualquier problema de eliminación de direcciones IP, explicar cómo asignar direcciones IPv6, describir las estrategias de transición para implementar IPv6 y configurar, verificar y resolver problemas de RIPng para IPv6.

7.1 DHCP

7.1.1 Introducción a DHCP

¿Qué es DHCP?

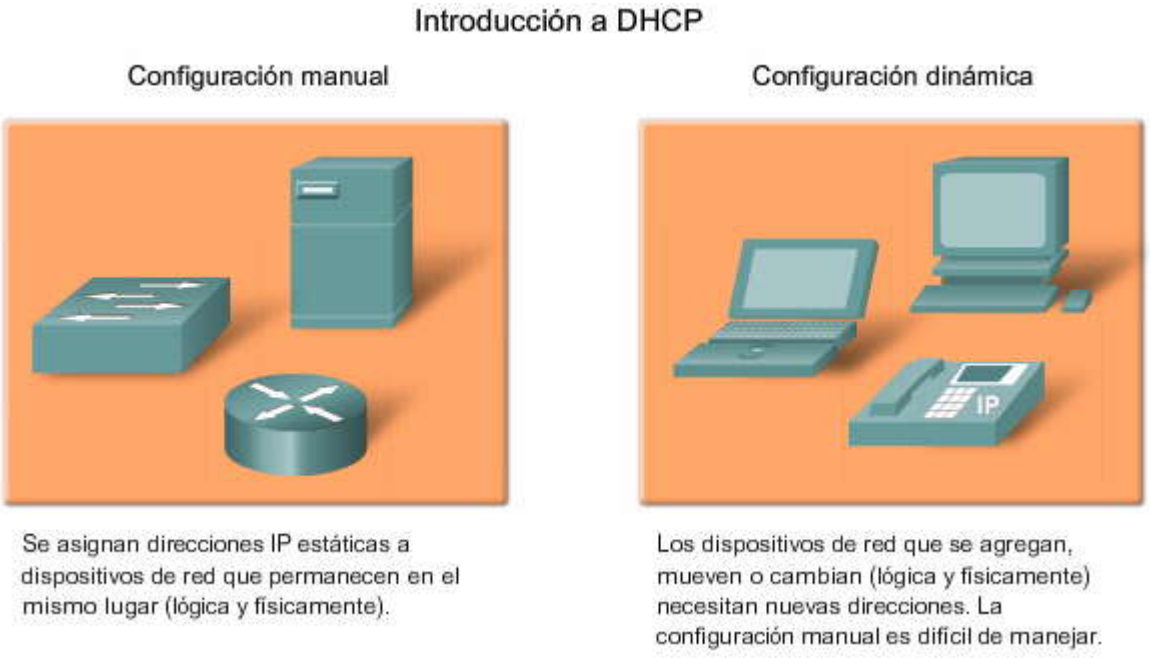
Cada dispositivo que se conecta a una red necesita una dirección IP. Los administradores de red asignan direcciones IP estáticas a los routers, los servidores y otros dispositivos de red que es poco probable que cambien de ubicación (física y lógica). Los administradores ingresan las direcciones IP estáticas de manera manual al configurar los dispositivos que se

conectarán a la red. Las direcciones estáticas también permiten a los administradores administrar esos dispositivos de manera remota.

Sin embargo, las computadoras de una organización con frecuencia cambian de ubicación, tanto física como lógica. Los administradores no pueden asignar nuevas direcciones IP cada vez que un empleado se muda a otra oficina o cubículo. Los clientes de escritorio no requieren direcciones estáticas. Por el contrario, una estación de trabajo puede utilizar cualquier dirección perteneciente a un rango de direcciones. Este rango se encuentra por lo general dentro de una subred IP. Una estación de trabajo perteneciente a una subred específica puede recibir cualquier dirección perteneciente a un rango especificado. Otros elementos, como la máscara de subred, el gateway predeterminado y el servidor del sistema de nombres de dominios (DNS, Domain Name System) reciben un valor que es común para esa subred o toda la red administrada. Por ejemplo, todos los hosts dentro de la misma subred reciben diferentes direcciones IP de host, pero reciben la misma máscara de subred y la misma dirección IP de gateway predeterminado.

Recuerde que en CCNA Exploration: Aspectos básicos de redes DHCP hace que el proceso de asignación de nuevas direcciones IP sea casi transparente. DHCP asigna direcciones IP y otra información de configuración de la red de manera dinámica. Como los clientes de escritorio por lo general conforman la mayoría de los nodos de red, DHCP es una herramienta muy útil y que ahorra tiempo a los administradores de red. RFC 2131 describe DHCP.

Los administradores en general prefieren que los servidores de red ofrezcan servicios DHCP porque estas soluciones facilitan el crecimiento y la administración. Sin embargo, en una sucursal pequeña o una ubicación SOHO, se puede configurar un router Cisco para brindar proporcionar DHCP sin necesidad de contar con un servidor dedicado y caro. Un conjunto de funciones de IOS de Cisco, llamado Easy IP, permite ofrecer un servidor de DHCP opcional con todas las funciones.



7.1.2 Funcionamiento de DHCP

Funcionamiento de DHCP

La asignación de direcciones IP a los clientes es la tarea más fundamental que realiza un servidor de DHCP. DHCP incluye tres mecanismos diferentes para la asignación de direcciones a fin de proporcionar flexibilidad al momento de asignar direcciones IP:

- **Asignación manual:** El administrador asigna una dirección IP asignada previamente al cliente y DHCP sólo comunica la dirección IP al dispositivo.
- **Asignación automática:** DHCP asigna automáticamente una dirección IP estática permanente a un dispositivo; la dirección es seleccionada de un conjunto de direcciones disponibles. No hay arrendamiento y la dirección se asigna permanentemente al dispositivo.
- **Asignación dinámica:** DHCP asigna automáticamente una dirección IP dinámica, o arrendada, tomada de un grupo de direcciones IP por un período limitado seleccionado por el servidor o hasta que el cliente informe al servidor de DHCP que ya no necesita la dirección.

Esta sección se centra en la asignación dinámica.

DHCP funciona en un modo de cliente/servidor y opera como cualquier otra relación cliente/servidor. Cuando una PC se conecta a un servidor de DHCP, el servidor asigna o arrienda una dirección IP a esa PC. La PC se conecta a la red con esa dirección IP arrendada hasta que el arrendamiento vence. El host debe comunicarse periódicamente con el servidor de DHCP para extender el arrendamiento. Este mecanismo de arrendamiento garantiza que si se traslada o apaga un host, éste no bloquee direcciones que no necesita. El servidor de DHCP devuelve estas direcciones al conjunto de direcciones y las vuelve a asignar según sea necesario.

Haga clic en el botón Descubrir que se muestra en la figura.

Cuando el cliente inicia sesión o desea unirse a una red de alguna otra manera, realiza cuatro pasos para obtener un arrendamiento. En el primer paso, el cliente envía un mensaje DHCPDISCOVER en forma de broadcast. El mensaje DHCPDISCOVER detecta servidores de DHCP en la red. Como el host no tiene información de IP válida, utiliza las direcciones de broadcast L2 y L3 para comunicarse con el servidor.

Haga clic en el botón Ofrecer que se muestra en la figura.

Cuando el servidor de DHCP recibe un mensaje DHCDISCOVER, busca una dirección IP disponible para arrendar, crea una entrada ARP que incluye la dirección MAC del host solicitante y la dirección IP arrendada, y transmite una oferta vinculante con un mensaje DHCPOFFER. El mensaje DHCPOFFER se envía como unicast mediante la dirección MAC L2 del servidor como dirección de origen y la dirección L2 del cliente como destino.

Nota: En determinadas circunstancias, el intercambio de mensajes DHCP del servidor puede enviarse como broadcast y no unicast.

Haga clic en el botón Solicitar que se muestra en la figura.

Cuando el cliente recibe el mensaje DHCPOFFER del servidor, responde con un mensaje DHCPREQUEST. Este mensaje tiene dos propósitos: el origen del arrendamiento y la verificación de la renovación del arrendamiento. Cuando se utiliza como origen del arrendamiento, el mensaje DHCPREQUEST del cliente solicita que la información de IP se verifique justo después de haber sido asignada. El mensaje proporciona una verificación de errores para asegurarse de que la asignación siga siendo válida. El mensaje DHCPREQUEST también actúa como aviso de aceptación vinculante para el servidor seleccionado y como rechazo implícito para los demás servidores que puedan haber enviado al host una oferta vinculante.

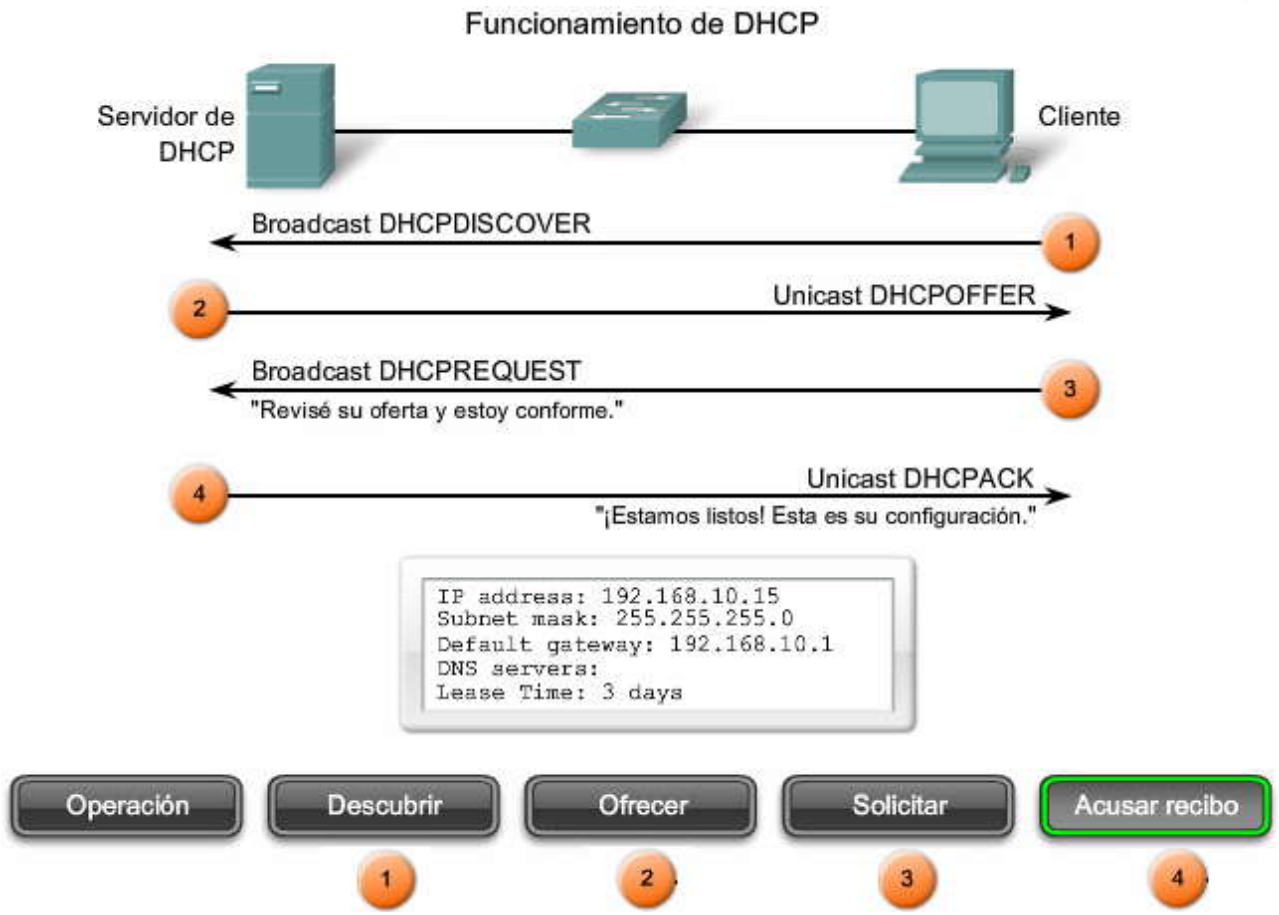
Muchas redes empresariales utilizan varios servidores de DHCP. El mensaje DHCPREQUEST se envía en forma de broadcast para informar a este servidor de DHCP y a los demás servidores de DHCP acerca de la oferta aceptada.

Haga clic en el botón Acusar recibo que se muestra en la figura.

Al recibir el mensaje DHCPREQUEST, el servidor verifica la información de arrendamiento, crea una nueva entrada ARP para el arrendamiento del cliente y responde con un mensaje DHCPACK unicast. El mensaje DHCPACK es una reproducción del mensaje DHCPOFFER, excepto por un cambio en el campo del tipo de mensaje. Cuando el cliente recibe el mensaje DHCPACK, registra la información de la configuración y realiza una búsqueda ARP para la dirección asignada. Si no recibe una respuesta, sabe que la dirección IP es válida y comienza a utilizarla como propia.

Los clientes arriendan la información de los servidores por un período definido administrativamente. Los administradores configuran los servidores de DHCP para que los arrendamientos expiren una vez transcurridos ciertos intervalos. La mayoría de los ISP y las redes grandes utilizan duraciones de arrendamiento predeterminadas de hasta tres días. Cuando el período de arrendamiento finaliza, el cliente debe pedir otra dirección, aunque en general, se le reasigna la misma dirección.

El mensaje DHCPREQUEST también se encarga del proceso DHCP dinámico. La información de IP enviada en el mensaje DHCPOFFER puede haber sido ofrecida a otro cliente durante la asignación dinámica. Cada servidor de DHCP crea conjuntos de direcciones IP y parámetros asociados. Los conjuntos están dedicados a subredes IP lógicasindividuales. Estos conjuntos permiten que varios servidores de DHCP respondan y que los clientes IP sean móviles. Si varios servidores responden, el cliente puede elegir sólo una de las ofertas.



7.1.3 BOOTP y DHCP

BOOTP y DHCP

El protocolo Bootstrap (BOOTP), definido en RFC 951, es el predecesor del protocolo DHCP y comparte con éste algunas características funcionales. BOOTP es una manera de descargar configuraciones de dirección e inicio para estaciones de trabajo sin disco. Una estación de trabajo sin disco no tiene unidad de disco duro ni sistema operativo. Por ejemplo, muchos sistemas de cajas registradoras automatizadas de los supermercados son estaciones de trabajo sin disco. Tanto DHCP como BOOTP se basan en la relación cliente/servidor y utilizan los puertos UDP 67 y 68. Estos puertos todavía se conocen como puertos BOOTP.

DHCP y BOOTP tienen dos componentes, como se muestra en la figura. El servidor es un host con dirección IP estática que asigna, distribuye y administra las asignaciones de IP y los datos de configuración. Cada asignación (IP y datos de configuración) se almacena en el servidor en un conjunto de datos llamado asignación. El cliente es algún dispositivo que utilice DHCP como método de obtención de direccionamiento IP o soporte de información de configuración.

Para comprender las diferencias funcionales entre BOOTP y DHCP, tenga en cuenta los cuatro parámetros básicos de IP necesarios para conectarse a una red:

- Dirección IP
- Dirección de gateway
- Máscara de subred
- Dirección de servidor DNS

Existen tres diferencias principales entre DHCP y BOOTP:

- La diferencia principal es que BOOTP se diseñó para la configuración previa manual de la información del host en una base de datos del servidor, mientras que DHCP permite la asignación dinámica de direcciones y configuraciones de red a hosts recientemente conectados. Cuando un cliente BOOTP solicita una dirección IP, el servidor BOOTP busca una entrada que coincida con la dirección MAC del cliente en una tabla predefinida. Si la entrada existe, la dirección IP

correspondiente a esa entrada se envía al cliente. Esto significa que el enlace entre las direcciones MAC e IP se tiene que haber configurado previamente en el servidor BOOTP.

- DHCP permite la recuperación y la reasignación de direcciones de red a través de un mecanismo de arrendamiento. Específicamente, DHCP define mecanismos por medio de los cuales se puede asignar una dirección IPa los clientes por un período de tiempo de arrendamiento determinado. Este período de arrendamiento permite la reasignación de la dirección IP a otro cliente más tarde, o que el cliente reciba otra asignación si se cambia a otra subred. Además, los clientes pueden renovar los arrendamientos y mantener la misma dirección IP. BOOTP no utiliza arrendamientos. Sus clientes tienen direcciones IP reservadas que no se pueden asignar a ningún otro host.
- BOOT proporciona una cantidad limitada de información a un host. DHCP proporciona parámetros de configuración IP adicionales, por ejemplo WINS y nombre de dominio.

BOOTP	DHCP
Mapeos estáticos	Mapeos dinámicos
Asignación permanente	Alquiler
Sólo admite cuatro parámetros de configuración	Admite más de 20 parámetros de configuración

Formato del mensaje DHCP

Los desarrolladores de DHCP necesitaban mantener la compatibilidad con BOOTP, de manera que utilizaron el mismo formato de mensaje que usa BOOTP. Sin embargo, como DHCP tiene más funcionalidades que BOOTP, se agregó el campo de opciones de DHCP. Al comunicarse con clientes BOOTP más antiguos se omite el campo de opciones de DHCP.

La figura muestra el formato de un mensaje DHCP. Los campos son los siguientes:

- **Código de operación (OP, Operation Code)**: especifica el tipo general de mensaje. Si el valor es 1, indica que se trata de un mensaje de solicitud; si el valor es 2, se trata de un mensaje de respuesta.
- **Tipo de hardware**: identifica el tipo de hardware utilizado en la red. Por ejemplo, 1 es Ethernet, 15' es Frame Relay y 20 es una línea serial. Se utilizan los mismos códigos que en los mensajes de ARP.
- **Longitud de la dirección de hardware**: 8 bits para especificar la longitud de la dirección.
- **Saltos**: el cliente asigna a este parámetro un valor de 0 antes de transmitir una solicitud. Los agentes de relay lo utilizan para controlar el reenvío de los mensajes de DHCP.
- **Identificador de transacción**: identificación de 32 bits generada por el cliente para poder equiparar la solicitud con las respuestas recibidas de los servidores de DHCP.
- **Segundos**: cantidad de segundos transcurridos desde que el cliente comenzó a intentar adquirir o renovar un arrendamiento. Los servidores de DHCP ocupados utilizan este número para establecer un orden de prioridad de respuesta cuando hay varias solicitudes de clientes todavía pendientes.
- **Señaladores**: se utiliza sólo uno de los 16 bits, que es el señalador de broadcast. Un cliente que no conoce su dirección IP cuando envía la solicitud, asigna el valor 1 al señalador. Este valor indica al servidor de DHCP o agente de relay que recibe la solicitud que debe enviar la respuesta como broadcast.
- **Dirección IP del cliente**: el cliente coloca su propia dirección IP en este campo únicamente si tiene una dirección IP válida mientras se encuentra en el estado de enlace; de lo contrario, asigna el valor 0 al campo. El cliente sólo utiliza este campo cuando su dirección es válida y puede utilizarse, no durante el proceso de adquisición de una dirección.
- **Su dirección IP**: dirección IP que el servidor asigna al cliente.
- **Dirección IP del servidor**: dirección del servidor que el cliente debe utilizar para el siguiente paso en el proceso bootstrap, que puede ser el servidor que envía esta respuesta o no. El servidor de envío siempre incluye su propia dirección IP en un campo especial, llamado Opción de DHCP del identificador de servidor.
- **Dirección IP del gateway**: enruta los mensajes de DHCP cuando participan agentes relay DHCP. La dirección del gateway permite las comunicaciones de solicitudes y respuestas DHCP entre un cliente y un servidor que se encuentran en subredes o redes diferentes.
- **Dirección del hardware del cliente**: especifica la capa física del cliente.

- **Nombre del servidor**: el servidor que envía un mensaje DHCPOFFER o DHCPACK puede, de manera opcional, colocar su nombre en este campo. Puede tratarse de un apodo de textosimple o un nombre de dominio DNS, por ejemplo, dhcpserver.netacad.net.
- **Nombre de archivo de inicio**: el cliente utiliza este campo de manera opcional para solicitar un tipo específico de archivo de inicio en un mensaje DHCPDISCOVER. Utilizado por un servidor en un mensaje DHCPOFFER para especificar por completo un nombre de archivo y directorio de archivo de inicio.
- **Opciones**: alberga las opciones de DHCP, que incluyen varios parámetros necesarios para el funcionamiento básico de DHCP. La longitud de este campo es variable. Tanto el cliente como el servidor pueden utilizar este campo.

Formato del mensaje DHCP

8	16	24	32
Código OP (1)	Tipo de hardware (1)	Longitud de dirección de hardware (1)	Saltos (1)
Identificador de transacción			
Segundos: 2 bytes		Señaladores: 2 bytes	
Dirección IP del cliente (CIADDR, Client IP Address): 4 bytes			
Su dirección IP (YIADDR, Your IP Address): 4 bytes			
Dirección IP de servidor (SIADDR, Server IP Address): 4 bytes			
Dirección IP del gateway (GIADDR, Gateway IP Address): 4 bytes			
Dirección de hardware del cliente (CHADDR, Client Hardware Address): 16 bytes			
Nombre del servidor (SNAME, Server name): 64 bytes			
Nombre de archivo: 128 bytes			
Opciones DHCP: variable			

Métodos de oferta y descubrimiento de DHCP

Estos valores proporcionan información detallada sobre el contenido del paquete de los mensajes de oferta y descubrimiento de DHCP.

Cuando un cliente desea conectarse a la red, solicita valores de direccionamiento al servidor de DHCP de la red. Si el cliente está configurado para recibir su configuración IP de manera dinámica, transmite un mensaje DHCPDISCOVER a través de su subred física local al iniciar sesión o cuando detecta una conexión de red activa. Como el cliente no tiene manera de saber a qué subred pertenece, el mensaje DHCPDISCOVER se transmite como broadcast (dirección IP de destino 255.255.255.255). El cliente no tiene una dirección IP configurada, de manera que se utiliza la dirección IP de origen 0.0.0.0. Como se puede ver en la figura, la dirección IP del cliente (CIADDR), la dirección del gateway predeterminado (GIADDR) y la máscara de subred están marcadas con signos de pregunta.

Haga clic en el botón Oferta de DHCP que se muestra en la figura.

El servidor de DHCP administra la asignación de las direcciones IP y responde a las solicitudes de configuración de los clientes.

Cuando el servidor de DHCP recibe el mensaje DHCPDISCOVER, responde con un mensaje DHCPOFFER. Este mensaje contiene la información de configuración inicial para el cliente, incluida la dirección MAC del cliente, seguida de la dirección IP que ofrece el servidor, la máscara de subred, la duración del arrendamiento y la dirección IP del servidor de DHCP que hace la oferta. La máscara de subred y el gateway predeterminado se especifican en el campo de opciones, la máscara de subred y las opciones de router, respectivamente. El mensaje DHCPOFFER se puede configurar de manera que incluya otra información, por ejemplo, el tiempo de renovación del arrendamiento, el servidor del nombre de dominio y el servicio de nombres NetBIOS (servicio de nombres para Internet de Microsoft Windows [Microsoft WINS, Microsoft Windows Internet Name Service]).

El servidor determina la configuración en función de la dirección del hardware del cliente según se especifica en el campo CHADDR.

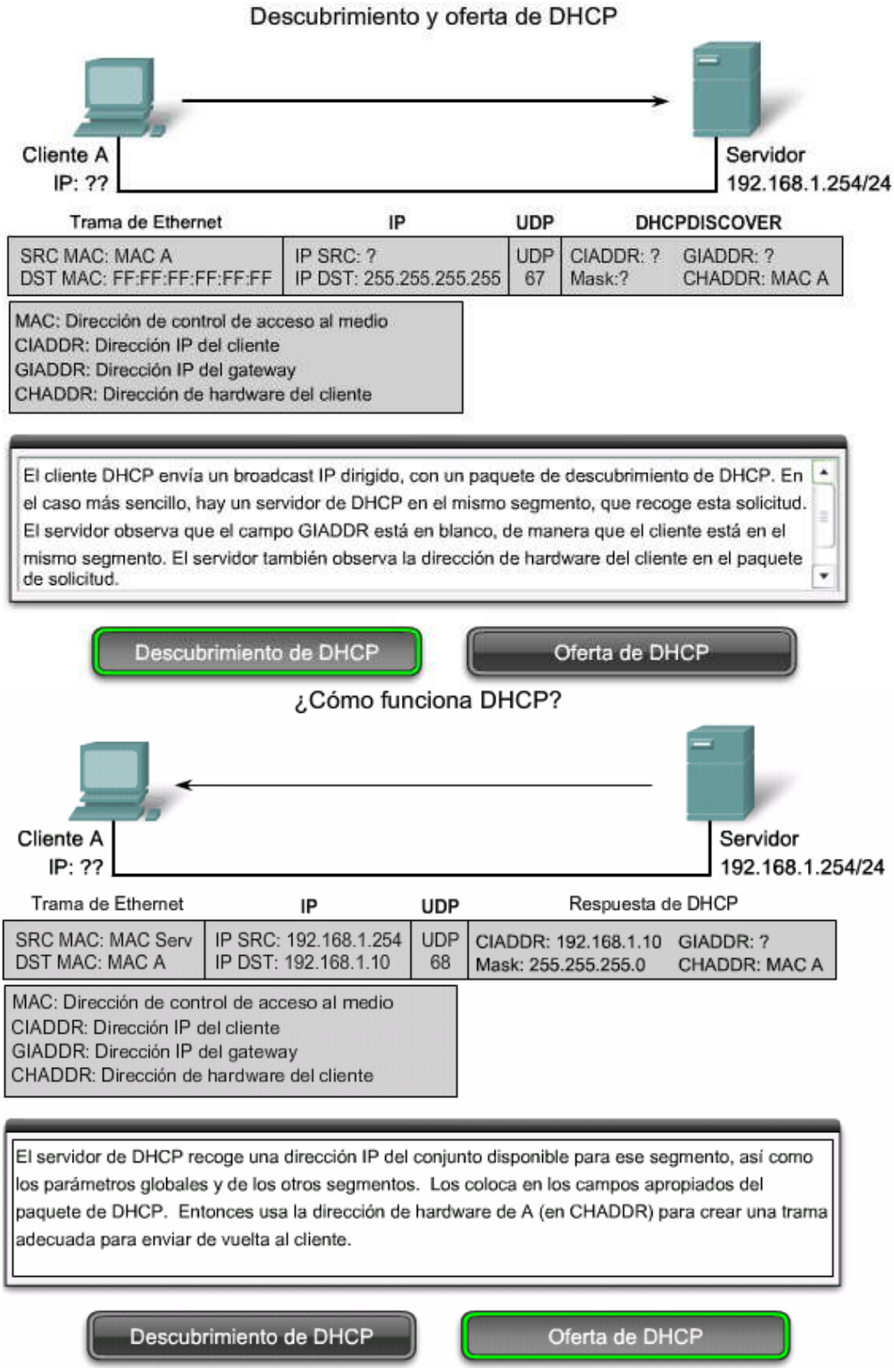
Como se muestra en el diagrama, el servidor de DHCP ha respondido al mensaje DHCPDISCOVER con la asignación de valores a CIADDR y la máscara de subred.

Los administradores configuran los servidores de DHCP para asignar direcciones de conjuntos predefinidos. La mayoría de los servidores de DHCP también permiten que el administrador defina de forma específica cuáles direcciones MAC de cliente se pueden servir y asignarles cada vez la misma dirección IP de forma automática.

DHCP utiliza el protocolo de datagramas de usuario (UDP, User Datagram Protocol) como su protocolo de transporte. El cliente envía mensajes al servidor en el puerto 67. El servidor envía mensajes al cliente en el puerto 68.

El cliente y el servidor acusan recibo de los mensajes y el proceso finaliza. El cliente establece el CIADDR sólo cuando un host se encuentra en el estado de enlace, lo que significa que el cliente ha confirmado la dirección IP y la está utilizando.

Para obtener más información acerca de DHCP, consulte "Servidor de DHCP de IOS de Cisco" en: http://www.cisco.com/en/US/docs/ios/12_0t/12_0t1/feature/guide/Easyip2.html.



7.1.4 Configuración de un servidor de DHCP

Configuración de un servidor de DHCP

Los routers Cisco que ejecutan el software IOS de Cisco son plenamente compatibles para actuar como servidores de DHCP. El servidor de DHCP que ejecuta IOS de Cisco administra direcciones IP de conjuntos de direcciones especificados en el router y las asigna a los clientes de DHCP.

Los pasos para configurar un router como servidor de DHCP son los siguientes:

Paso 1. Definición de un rango de direcciones que DHCP no debe asignar. Normalmente estas direcciones son las direcciones estáticas reservadas para la interfaz del router, la dirección IP de administración del switch, los servidores y las impresoras de red locales.

Paso 2. Creación del pool de DHCP con el comando **ip dhcp pool**.

Paso 3. Configuración de los parámetros específicos del pool.

Una mejor práctica consiste en configurar las direcciones excluidas en un modo de configuración global antes de crear el pool de DHCP. Esto garantiza que DHCP no asigne direcciones reservadas por accidente.

Es necesario especificar las direcciones IP que el servidor de DHCP no debe asignar a los clientes. Normalmente, algunas direcciones IP pertenecen a dispositivos estáticos de la red, por ejemplo, servidores o impresoras. DHCP no debe asignar estas direcciones IP a otros dispositivos. Una mejor práctica consiste en configurar las direcciones excluidas en un modo de configuración global antes de crear el pool de DHCP. Esto garantiza que DHCP no asigne direcciones reservadas por accidente. Para excluir direcciones específicas, utilice el comando **ip dhcp excluded-address**.

Haga clic en el botón Pool de DHCP que se muestra en la figura.

La configuración de un servidor de DHCP implica la definición de un conjunto de direcciones para asignar. El comando **ip dhcp pool** crea un conjunto con el nombre especificado y coloca el router en el modo de configuración de DHCP, que se identifica con la identificación Router(dhcp-config)#.

Haga clic en el botón Tareas de DHCP que se muestra en la figura.

Esta figura enumera las tareas que se deben realizar para completar la configuración del pool de DHCP. Algunas son opcionales, pero otras son obligatorias.

Debe configurar las direcciones disponibles y especificar el número de red de subred y la máscara del conjunto de direcciones de DHCP. Use la sentencia **network** para definir el rango de direcciones disponibles.

También debe utilizar el comando **default-router** para definir el gateway predeterminado o el router que deben utilizar los clientes. Normalmente, el gateway es la interfaz LAN del router. Se requiere una dirección, pero puede incluir hasta ocho direcciones.

Los siguientes comandos del pool de DHCP se consideran opcionales. Por ejemplo, puede configurar la dirección IP del servidor DNS que está disponible para un cliente DHCP con el comando **dns-server**. Para configurarlo se necesita una dirección, pero es posible incluir hasta ocho.

Otros parámetros incluyen la configuración de la duración del arrendamiento de DHCP. La configuración predeterminada es un día, pero puede utilizar el comando **lease** para modificarla. También puede configurar un servidor NetBIOS WINS que está disponible para un cliente DHCPde Microsoft. Este tipo de servidores normalmente se configura en un entorno que admite clientes anteriores a Windows 2000. Como la mayoría de las instalaciones ahora tienen clientes con sistemas operativos Windows más recientes, este parámetro no suele ser necesario.

Haga clic en el botón Ejemplo de DHCP que se muestra en la figura.

Esta figura muestra una configuración modelo con parámetros de DHCP básicos configurados en el router R1.

Desactivación de DHCP

El servidor de DHCP se habilita de forma predeterminada en las versiones del software IOS de Cisco que lo admiten. Para desactivar el servicio, utilice el comando **no service dhcp**. Utilice el comando de configuración global **service dhcp** para

volver a activar el proceso del servidor de DHCP. La habilitación del servicio no tiene efecto si no se configuran los parámetros.

Paso 1 de la configuración de DHCP: Exclusión de direcciones IP

```
R1(config)#ip dhcp excluded-address low-address [high-address]
```

```
R1(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)#ip dhcp excluded-address 192.168.10.254
```

Direcciones excluidas | Pool de DHCP | Tareas de DHCP | Ejemplo de DHCP

Paso 2 de la configuración de DHCP: Configuración de un pool de DHCP

```
R1(config)#ip dhcp pool pool-name
```

```
R1(config)#ip dhcp pool LAN-POOL-1
R1(dhcp-config)#
```

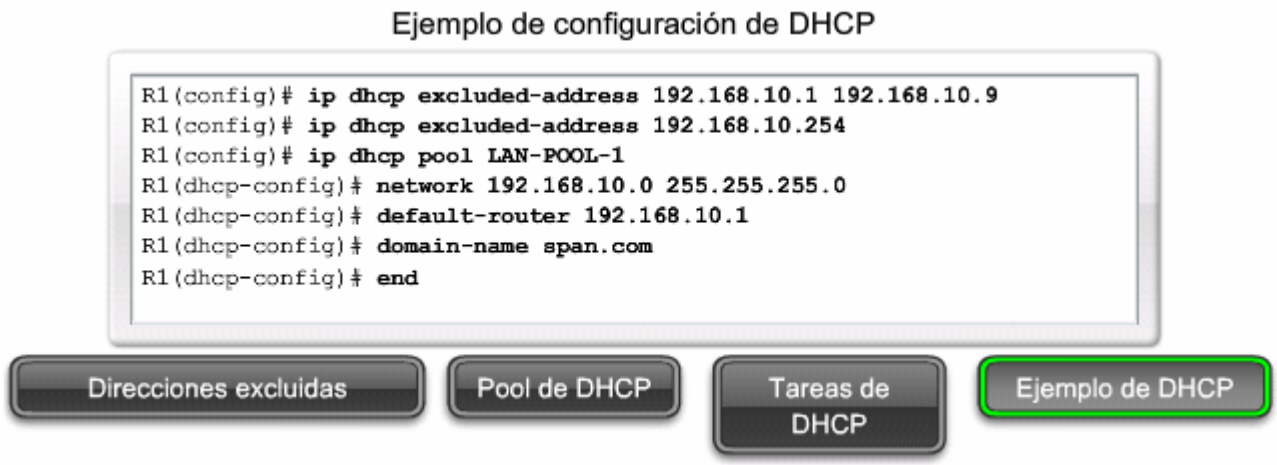
Direcciones excluidas | Pool de DHCP | Tareas de DHCP | Ejemplo de DHCP

Paso 3 de la configuración de DHCP: Tareas específicas

Tareas requeridas	Comando
Definir el conjunto de direcciones	`network network-number [mask | /prefix-length]`
Definir el router o gateway predeterminado	`default-router address [address2...address8]`

Tareas opcionales	Comando
Definir un servidor DNS.	`dns-server address [address2...address8]`
Definir el nombre de dominio	`domain-name domain`
Definir la duración del arrendamiento de DHCP	`lease {days [hours] [minutes] | infinite}`
Definir el servidor NetBIOS WINS	`netbios-name-server address [address2...address8]`

Direcciones excluidas | Pool de DHCP | Tareas de DHCP | Ejemplo de DHCP



Verificación de DHCP

En la figura se ilustra cómo se puede configurar un router Cisco para proporcionar servicios de DHCP. La PC1 no está encendida y, por lo tanto, no tiene una dirección IP.

El router R1 se configuró con los siguientes comandos:

ip dhcp excluded-address 192.168.10.1 192.168.10.9
ip dhcp excluded-address 192.168.10.254
ip dhcp pool LAN-POOL-1
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
domain-name span.com

Para verificar el funcionamiento de DHCP, utilice el comando **show ip dhcp binding**. Este comando muestra una lista de todas las asignaciones de direcciones IP a direcciones MAC que proporcionó el servicio de DHCP.

Para verificar que el router esté recibiendo o enviando los mensajes, utilice el comando de estadísticas **show ip dhcp server**. Este comando muestra información numérica acerca de la cantidad de mensajes de DHCP que se envían y reciben.

Haga clic en el botón DHCP-1 que se muestra en la figura.

Como puede observar en la figura, actualmente no hay asignaciones y no se muestran estadísticas.

Ahora, supongamos que la PC1 se enciende y completa el proceso de inicio.

Haga clic en el botón DHCP-2 que se muestra en la figura.

Observe que la información de asignación ahora muestra que la dirección IP 192.168.10.10 está vinculada a una dirección MAC. Las estadísticas también muestran que hay actividad de DHCPDISCOVER, DHCPREQUEST, DHCPOFFER y DHCPACK.

Haga clic en el botón Cliente DHCP que se muestra en la figura.

El comando **ipconfig /all** muestra los parámetros de TCP/IP configurados en la PC1. Como la PC1 se conectó al segmento de red 192.168.10.0 /24, recibió automáticamente una dirección IP, un sufijo DNS y un gateway predeterminado de ese conjunto. No es necesario configurar la interfaz DHCP. Si una PC se conecta a un segmento de red que tiene un pool de DHCP disponible, puede obtener una dirección IP automáticamente.

Entonces ¿cómo hace la PC2 para recibir una dirección IP? El router R1 tendría que estar configurado para proporcionar un pool de DHCP 192.168.11.0 /24 de la siguiente manera:

ip dhcp excluded-address 192.168.11.1 192.168.11.9
ip dhcp excluded-address 192.168.11.254
ip dhcp pool LAN-POOL-2
network 192.168.11.0 255.255.255.0

default-router 192.168.11.1
domain-name span.com

Una vez que la PC2 haya completado su proceso de inicio, recibe una dirección IP para el segmento de red al que se conectó.

Haga clic en el botón Verificación de DHCP-3 que se muestra en la figura.

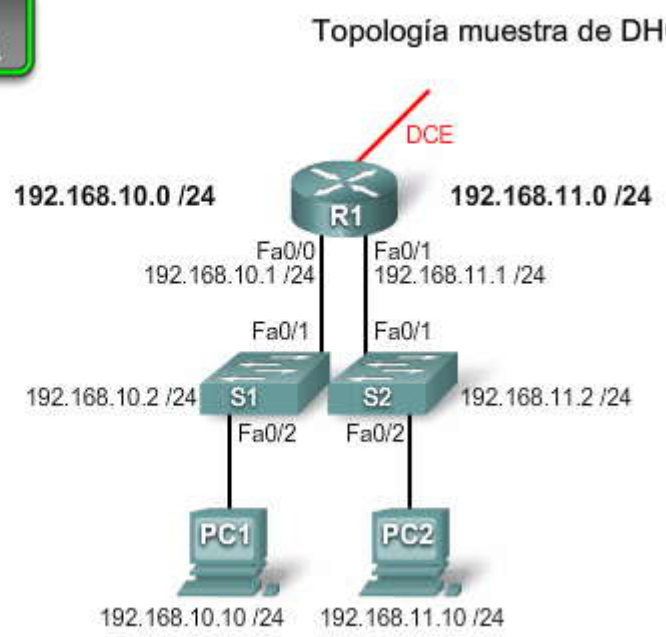
Observe que las asignaciones DHCP ahora indican que hay dos hosts que recibieron direcciones IP. Las estadísticas de DHCP también muestran el intercambio de mensajes de DHCP.

Otro comando útil para ver varios pools es el comando **show ip dhcp pool**.

Haga clic en el botón Pools de DHCP que se muestra en la figura.

Este comando resume la información del pool de DHCP.

Resultado del router



DHCP-1

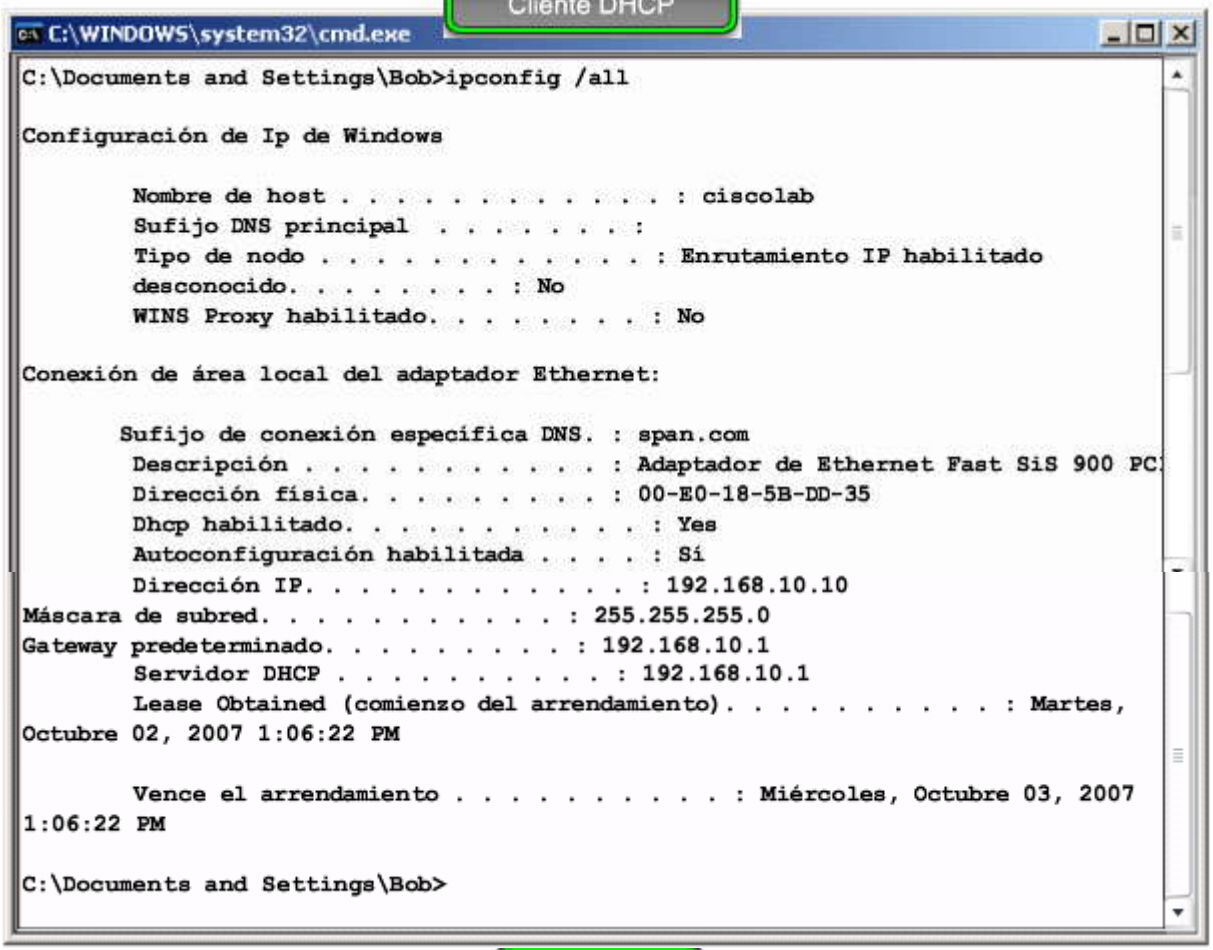
```
R1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name

R1#show ip dhcp server statistics
Memory usage         23543
Address pools        1
Database agents      0
Automatic bindings   0
Manual bindings      0
Expired bindings     0
Malformed messages   0
Secure arp entries   0
```

```
Message             Received
BOOTREQUEST         0
DHCPDISCOVER        0
DHCPREQUEST         0
DHCPDECLINE         0
DHCPRELEASE         0
DHCPINFORM          0

Message             Sent
BOOTREPLY           0
DHCPOFFER           0
DHCPACK             0
DHCPNAK             0
R1#
```

DHCP-2

```
R1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.10.10       0100.e018.5bdd.35       Oct 03 2007 05:05 PM    Automatic

R1#show ip dhcp server statistics
Memory usage        23786
Address pools       1
Database agents     0
Automatic bindings  1
Manual bindings     0
Expired bindings    0
Malformed messages  0
Secure arp entries  0

Message             Received
BOOTREQUEST         0
DHCPDISCOVER        6
DHCPREQUEST         1
DHCPDECLINE         0
DHCPRELEASE         0
DHCPINFORM          0

Message             Sent
BOOTREPLY           0
DHCPOFFER           1
DHCPACK             1
DHCPNAK             0
R1#
```

Cliente DHCP



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Bob>ipconfig /all

Configuración de Ip de Windows

        Nombre de host . . . . . . . . . . . . : ciscolab
        Sufijo DNS principal  . . . . . . . . :
        Tipo de nodo . . . . . . . . . . . . . : Enrutamiento IP habilitado
        desconocido. . . . . . . . . : No
        WINS Proxy habilitado. . . . . . . . : No

Conexión de área local del adaptador Ethernet:

       Sufijo de conexión específica DNS. : span.com
        Descripción . . . . . . . . . . . . : Adaptador de Ethernet Fast SiS 900 PC
        Dirección física. . . . . . . . . . : 00-E0-18-5B-DD-35
        Dhcp habilitado. . . . . . . . . . . : Yes
        Autoconfiguración habilitada . . . . : Sí
        Dirección IP. . . . . . . . . . . . . : 192.168.10.10
Máscara de subred. . . . . . . . . . . : 255.255.255.0
Gateway predeterminado. . . . . . . . . : 192.168.10.1
        Servidor DHCP . . . . . . . . . . . : 192.168.10.1
        Lease Obtained (comienzo del arrendamiento). . . . . . . . . . . : Martes,
Octubre 02, 2007 1:06:22 PM

        Vence el arrendamiento . . . . . . . . . . . : Miércoles, Octubre 03, 2007
1:06:22 PM

C:\Documents and Settings\Bob>
```

DHCP-3

```
R1#sho ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.10.10       0100.e018.5bdd.35       Oct 03 2007 06:14 PM    Automatic
192.168.11.10       0100.b0d0.d817.e6       Oct 03 2007 06:18 PM    Automatic


R1#sho ip dhcp server statistics
Memory usage         25307
Address pools        2
Database agents      0
Automatic bindings   2
Manual bindings      0
Expired bindings     0
Malformed messages   0
Secure arp entries   0
```

```
Message             Received
BOOTREQUEST         0
DHCPDISCOVER        8
DHCPREQUEST         3
DHCPDECLINE         0
DHCPRELEASE         0
DHCPINFORM          0

Message             Sent
BOOTREPLY           0
DHCPOFFER           3
DHCPACK             3
DHCPNAK             0
R1#
```

pool de DHCP

```
R1#show ip dhcp pool

Pool LAN-POOL-1 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                  Leased addresses
 192.168.10.11        192.168.10.1     - 192.168.10.254    1

Pool LAN-POOL-2 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                  Leased addresses
 192.168.11.11        192.168.11.1     - 192.168.11.254    1
R1#
```

7.1.5 Configuración del cliente DHCP

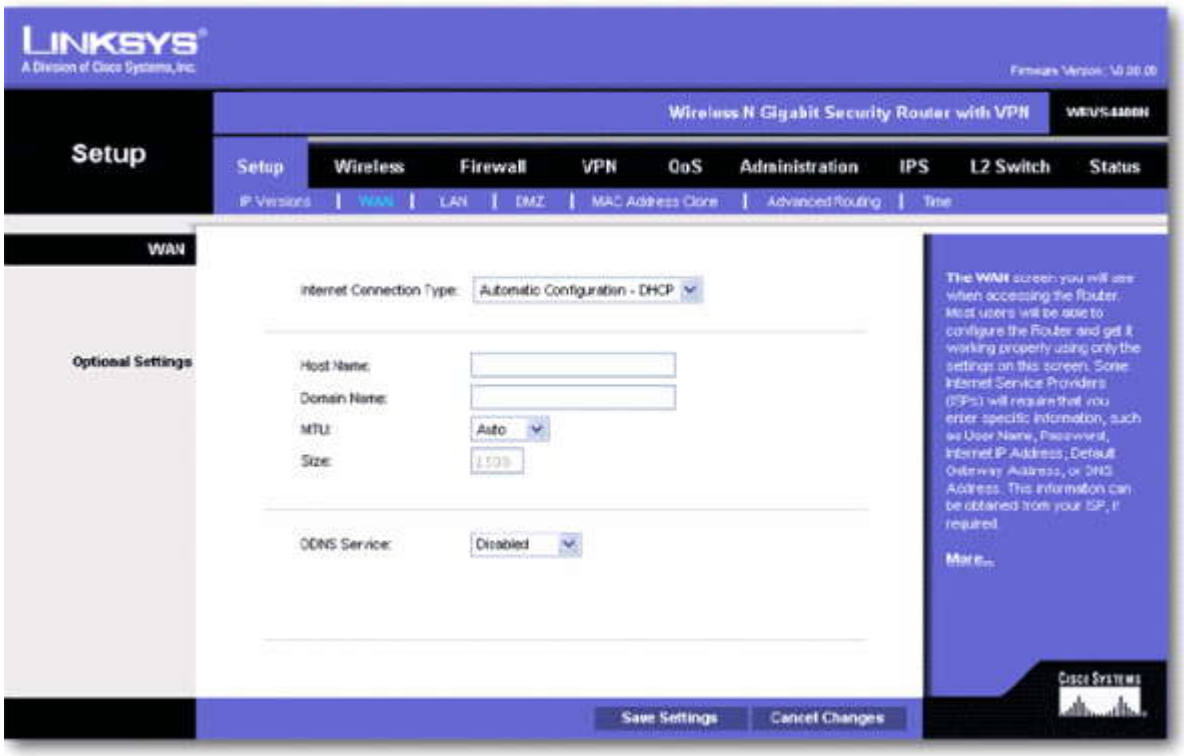
Configuración del cliente DHCP

Normalmente, los routers de ancho de banda reducido para uso doméstico, como los routers Linksys, se pueden configurar para que se conecten a un ISP a través de un módem DSL o un módem por cable. En la mayoría de los casos, los routers domésticos pequeños se configuran para adquirir direcciones IP de manera automática de los ISP. Por ejemplo, la figura muestra la página de configuración de WAN predeterminada para un router Linksys WRVS4400N. Observe que el tipo de conexión a Internet está definido como Configuración automática: DHCP. Esto significa que cuando el router está conectado a un módem por cable, por ejemplo, actúa como cliente DHCP y solicita una dirección IP al ISP.

A veces, es necesario configurar los routers Cisco en entornos de SOHO y sucursales de manera similar. El método utilizado depende del ISP. Sin embargo, en la configuración más simple se utiliza la interfaz Ethernet para conectarsea un módem por cable. Para configurar una interfaz Ethernet como cliente DHCP, se debe configurar el comando**ip address dhcp**.
Haga clic en el botón Cliente DHCP que se muestra en la figura.

En la figura, suponga que se ha configurado un ISP para proporcionar direcciones IP del rango 209.165.201.0 / 27 a clientes selectos. El resultado confirma la dirección asignada.

Conexión WAN de Linksys



Router Linksys | Cliente DHCP

Configuración del cliente DHCP


```
SOHO(config)# interface fa0/0
SOHO(config-if)# ip address dhcp
SOHO(config-if)# no shut
SOHO(config-if)#
*Oct  2 17:57:36.027: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/0 assigned
 DHCP address 209.165.201.12, mask 255.255.255.224, hostname SOHO

SOHO# show ip int fa0/0
FastEthernet0/0 is up, line protocol is up
  Internet address is 209.165.201.12/27
  Broadcast address is 255.255.255.255
  Address determined by DHCP from host 209.165.201.1
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled

<Output omitted>
```

Router Linksys | Cliente DHCP

¿Qué es el relay DHCP?

En una red jerárquica compleja, los servidores empresariales normalmente están contenidos en una granja de servidores. Estos servidores pueden proporcionar servicios de DHCP, DNS, TFTP y FTP para los clientes. El problema es que los clientes de red normalmente no están en la misma subred que esos servidores. Por lo tanto, los clientes deben localizar a los servidores para poder utilizar los servicios, lo que con frecuencia hacen mediante mensajes broadcast.

En la figura, la PC1 está intentado adquirir una dirección IP del servidor de DHCP ubicado en 192.168.11.5. En esta situación, el router R1 no está configurado como servidor de DHCP.

Haga clic en el botón Problema de host que se muestra en la figura.

En la figura, la PC1 está intentando renovar su dirección IP. Para hacerlo, se ejecuta el comando **ipconfig /release**. Observe que se libera la dirección IP y que la dirección actual es 0.0.0.0. A continuación, se ejecuta el comando **ipconfig /renew**. Esto hace que el host envíe el mensaje broadcast DHCPDISCOVER. Sin embargo, la PC1 no puede localizar al servidor de DHCP. ¿Qué sucede cuando el servidor y el cliente se encuentran separados por un router y, por lo tanto, no están en el mismo segmento de red? Recuerde, los routers no reenvían mensajes broadcast.

Nota: Ciertos clientes de Windows tienen una función llamada direccionamiento automático de IP privada (APIPA, Automatic Private IP Addressing). Con esta función, una computadora Windows puede asignarse automáticamente una dirección IP en el rango 169.254.x.x si el servidor de DHCP no está disponible o no existe en la red.

Para empeorar las cosas aún más, DHCP no es el único servicio crítico que utiliza broadcasts. Por ejemplo, los routers Cisco y otros dispositivos pueden utilizar broadcasts para localizar servidores TFTP o un servidor de autenticación, como un servidor TACACS.

Como solución a este problema, el administrador puede agregar servidores de DHCP en todas las subredes. Sin embargo, la ejecución de estos servicios en varias computadoras genera costos y gastos administrativos.

Una solución más simple es configurar la función dirección de ayudante de IOS de Cisco en los routers y switches participantes. Esta solución permite a los routers reenviar broadcasts DHCP a los servidores de DHCP. Cuando un router reenvía solicitudes de parámetros y asignación de direcciones, actúa como agente relay DHCP.

Por ejemplo, la PC1 enviaría una solicitud por broadcast para localizar un servidor de DHCP. Si el router R1 estuviera configurado como agente relay DHCP, interceptaría esta solicitud y la reenviaría al servidor de DHCP que se encuentra en la subred 192.168.11.0.

Para configurar el router R1 como agente relay DHCP, debe configurar la interfaz más cercana al cliente con el comando de configuración de interfaz **ip helper-address**. Este comando transfiere solicitudes de broadcast de servicios clave a una dirección configurada. Configure la dirección IP de helper en la interfaz que recibe el broadcast.

Haga clic en el botón Configuración de relay que se muestra en la figura.

El router R1 ahora está configurado como agente relay DHCP. Acepta solicitudes de broadcast para el servicio de DHCP y después las reenvía como unicast a la dirección IP 192.168.11.5.

Haga clic en el botón Renovación de host que se muestra en la figura.

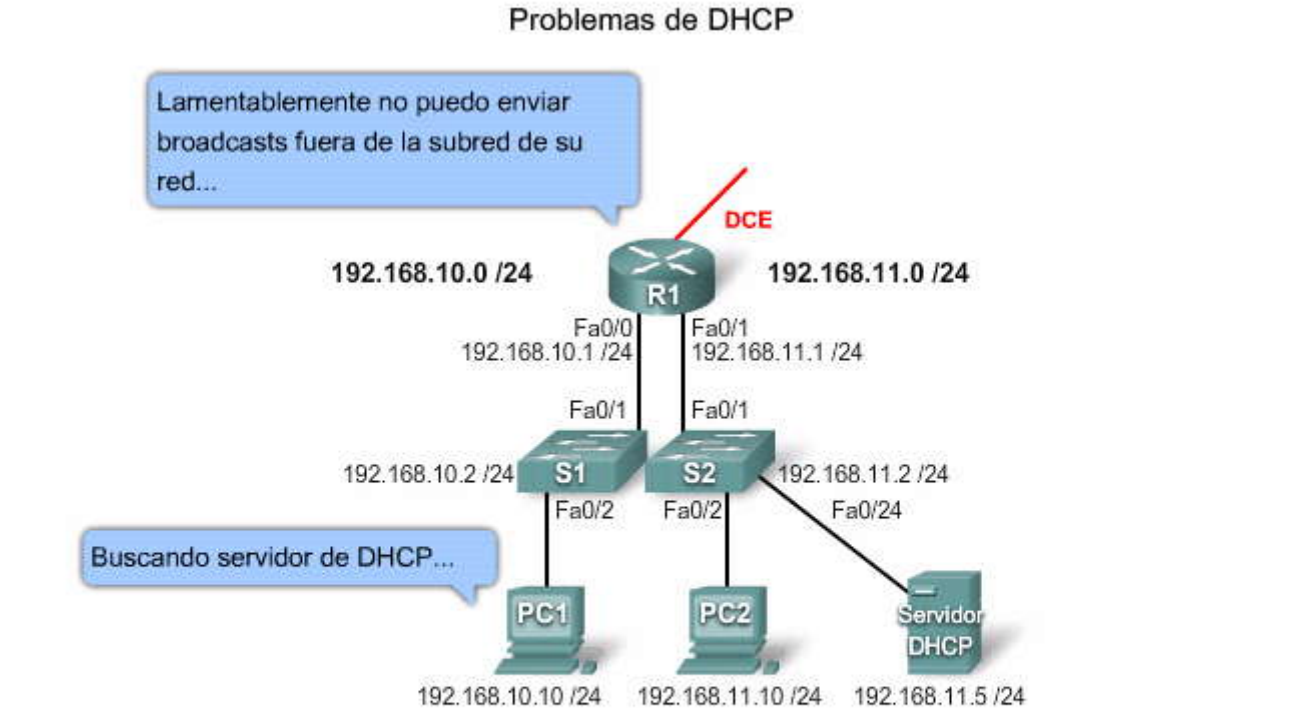
Como puede ver, la PC1 ahora puede adquirir una dirección IP del servidor de DHCP.

DHCP no es el único servicio para el que se puede configurar el router como relay. De forma predeterminada, el comando **ip helper-address** envía los siguientes ocho servicios de UDP:

- Puerto 37: Tiempo
- Puerto 49: TACACS
- Puerto 53: DNS
- Puerto 67: Cliente DHCP/BOOTP
- Puerto 68: Servidor de DHCP/BOOTP
- Puerto 69: TFTP
- Puerto 137: Servicio de nombres NetBIOS

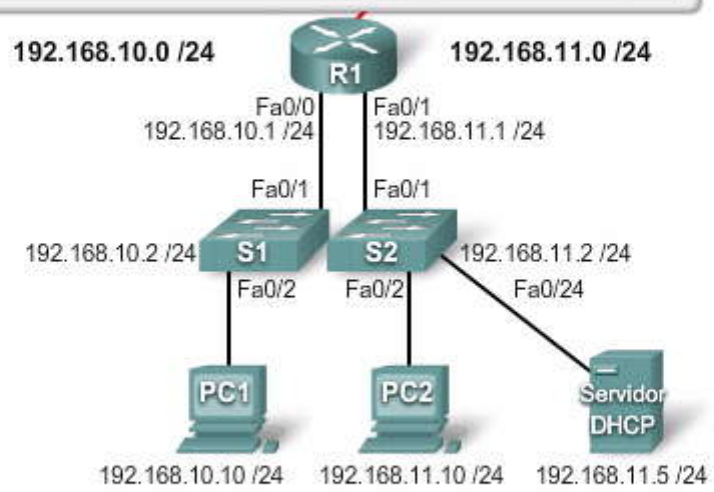
- Puerto 138: Servicio de datagrama NetBIOS)

Para especificar puertos adicionales, use el comando **ip forward-protocol** y especifique exactamente qué tipos de paquetes broadcast desea reenviar.



Relay DHCP

```
R1# config t
R1(config)# interface Fa0/0
R1(config-if)# ip helper-address 192.168.11.5
R1(config-if)# end
```



Problema de DHCP | Problema de host | Configuración de relay | Renovación de host

Relay DHCP

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ipconfig /release

Configuración IP de Windows

Conexión de área local del adaptador Ethernet:

        Sufijo de conexión específica DNS. :
              Dirección IP. . . . . . . . . . . . : 0.0.0.0
              Máscara de subred: . . . . . . . . . . : 0.0.0.0
        Gateway predeterminado. . . . . . . . . :

C:\Documents and Settings\Administrator>ipconfig /renew

Configuración IP de Windows

Conexión de área local del adaptador Ethernet:

        Sufijo de conexión específica DNS. :
              Dirección IP. . . . . . . . . . . . : 192.168.10.11
              Máscara de subred: . . . . . . . . . . : 255.255.255.0
              Gateway predeterminado. . . . . . . . . : 192.168.10.1

C:\Documents and Settings\Administrator>
```

Problema de DHCP | Problema de host | Configuración de relay | Renovación de host

7.1.7 Configuración de un servidor de DHCP con SDM

Configuración de un servidor de DHCP con SDM

Los routers Cisco también se pueden configurar como servidor de DHCP con SDM. En este ejemplo, el router R1 se configurará como servidor de DHCP en las interfaces Fa0/0 y Fa0/1.

Haga clic en el botón Tareas de DHCP que se muestra en la figura.

La función del servidor de DHCP se habilita en la sección Tareas adicionales de la ficha Configuración. Desde la lista de tareas, haga clic en la carpeta DHCP y seleccione **Pools de DHCP** para agregar un nuevo pool. Haga clic en **Agregar** para crear un nuevo pool de DHCP.

Haga clic en el botón Agregar Conjunto que se muestra en la figura.

La ventana Agregar pool de DHCP contiene las opciones que necesita para configurar el conjunto de direcciones IP de DHCP. Las direcciones IP que asigna el servidor de DHCP se extraen de un conjunto común. Para configurar el conjunto, especifique las direcciones IP final y de inicio del rango.

El SDM de Cisco configura el router para excluir automáticamente la dirección IP de la interfaz LAN del conjunto. No debe utilizar la dirección IP de la red ni la de la subred ni la dirección de broadcast de la red en el rango de direcciones que especifique.

Si necesita excluir otras direcciones IP del rango de direcciones, puede ajustar las direcciones IP final y de inicio. Por ejemplo, si necesita excluir las direcciones IP de 192.168.10.1 a 192.168.10.9, configuraría la dirección IP de inicio como 192.168.10.10. De esta manera el router comienza a asignar direcciones a partir de 192.168.10.10.

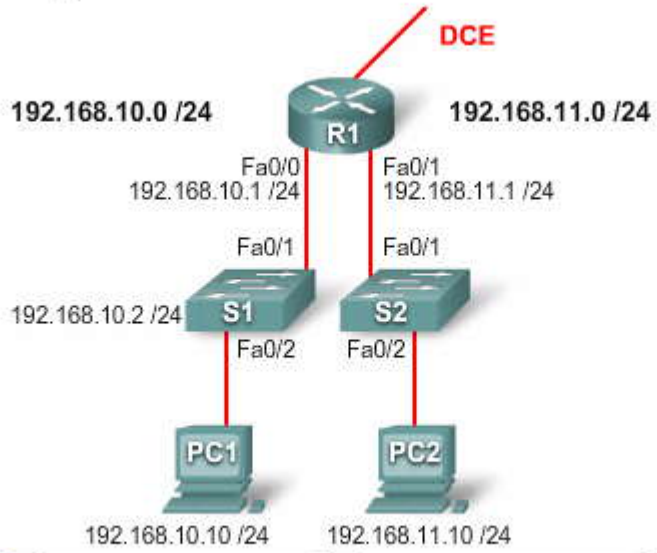
Las otras opciones disponibles son:

- **Servidor DNS 1 y servidor DNS 2**: el servidor DNS normalmente es un servidor que establece la correlación entre el nombre de un dispositivo y la dirección IP correspondiente. Si configuró un servidor DNS para la red, ingrese la dirección IP del servidor en este campo. Si hay un servidor DNS adicional en la red, puede ingresar la dirección IP de ese servidor en este campo.
- **Servidor WINS 1 y servidor WINS 2**: recuerde que la configuración WINS normalmente se utiliza en entornos que admiten clientes anteriores a Windows 2000.
- **Importar todas las opciones de DHCP a la base de datos del servidor de DHCP**: permite importar las opciones de DHCP de un servidor de un nivel superior. Normalmente se utiliza en combinación con un servidor de DHCP de Internet. Esta opción le permite obtener información de un nivel más alto sin necesidad de configurarla para este conjunto.

Haga clic en el botón Conjuntos de DHCP que se muestra en la figura.

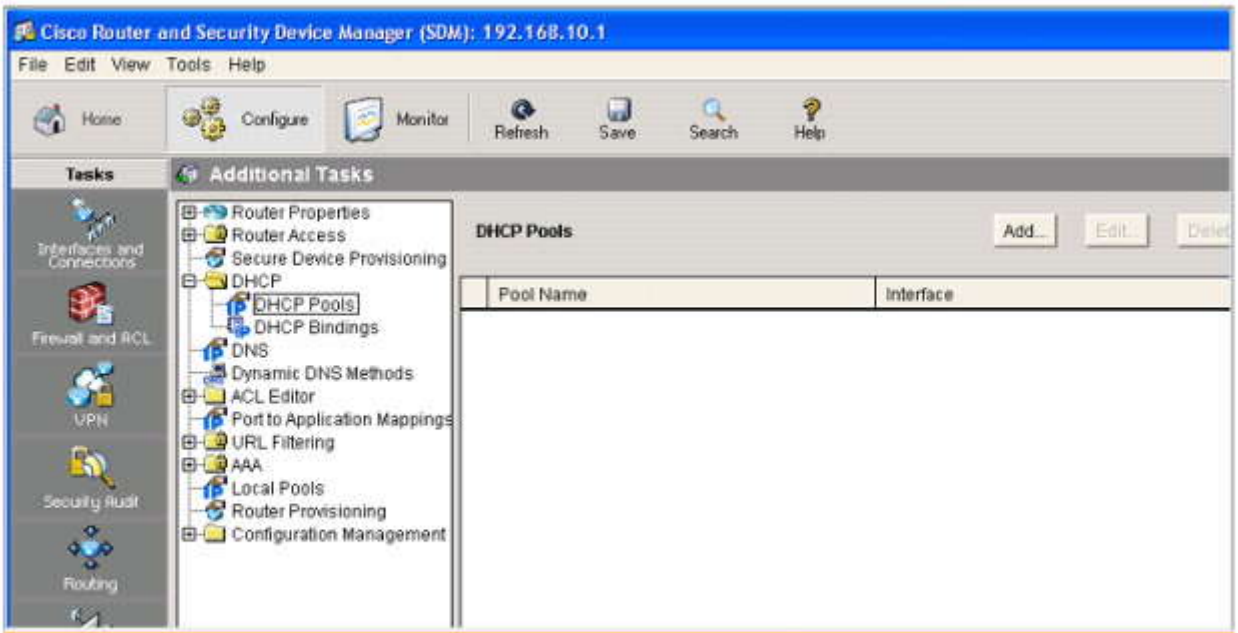
Esta pantalla le brinda un resumen de los pools configurados en el router. En este ejemplo se configuraron dos pools, uno para cada interfaz Fast Ethernet del router R1.

Configuración de un cliente DHCP con SDM



Topología de SDM | Tareas de DHCP | Agregar conjunto | Conjuntos de DHCP

Tareas de DHCP



Haga clic y arrastre la imagen para ver los detalles.

Topología de SDM | Tareas de DHCP | Agregar conjunto | Conjuntos de DHCP

7.1.8 Resolución de problemas de DHCP

Resolución de problemas relacionados con la configuración de DHCP

Pueden surgir problemas de DHCP por una variedad de motivos, por ejemplo, defectos de software en sistemas operativos, controladores NIC o agentes relay DHCP/BOOTP, pero los más comunes son ocasionados por problemas de configuración. Debido a la cantidad de áreas potencialmente problemáticas, se requiere un enfoque sistemático para la resolución de problemas.

Tarea 1 de la resolución de problemas: Solucione los conflictos de direcciones IP

Un arrendamiento de dirección IP puede expirar mientras el cliente todavía está conectado a la red. Si el cliente no renueva el arrendamiento, el servidor de DHCP puede reasignar la dirección IP a otro cliente. Cuando el cliente se reinicia, solicita una dirección IP. Si el servidor de DHCP no responde con rapidez, el cliente utiliza la última dirección IP. Así surge una situación en la que dos clientes utilizan la misma dirección IP, lo que crea un conflicto.

El comando de conflictos **show ip dhcp** muestra todos los conflictos de direcciones registrados por el servidor de DHCP. El servidor utiliza el comando **ping** para detectar conflictos. El cliente utiliza el protocolo de resolución de direcciones (ARP, Address Resolution Protocol) para detectar clientes. Si se detecta un conflicto de direcciones, la dirección se elimina del conjunto y no se asigna hasta que un administrador resuelva el conflicto.

Este ejemplo muestra el método y la hora de detección para todas las direcciones IP que el servidor de DHCP ha ofrecido y que tienen conflictos con otros dispositivos.

R2# **show ip dhcp conflict**

Método de detección de la dirección IP Hora de detección

192.168.1.32 Ping Feb 16 2007 12:28 PM

192.168.1.64 ARP gratuito Feb 23 2007 08:12 AM

Tarea 2 de la resolución de problemas: Verifique la conectividad física

Primero utilice el **comando de interfaz***show interface* para confirmar que la interfaz del router que está actuando como gateway predeterminado para el cliente esté funcionando bien. Si el estado de la interfaz es diferente de activo, el puerto no deja pasar el tráfico, incluidas las solicitudes de los clientes DHCP.

Tarea 3 de la resolución de problemas: Pruebe la conectividad de la red mediante la configuración de una estación de trabajo cliente con dirección IP estática

Al resolver cualquier problema de DHCP, verifique la conectividad de la red mediante la configuración de una dirección IP estática en una estación de trabajo cliente. Si la estación de trabajo no puede conectarse con los recursos de la red a través de una dirección IP configurada estáticamente, la causa raíz del problema no es DHCP. En este punto, se necesita resolverel problema de conectividad de la red.

Tarea 4 de la resolución de problemas: Verifique la configuración de los puertos del switch (STP Portfast y otros comandos)

Si el cliente DHCP no puede obtener una dirección IP del servidor de DHCP al iniciar, intente obtener una dirección IP del servidor de DHCP forzando manualmente al cliente a enviar una solicitud de DHCP.

Si hay un switch entre el cliente y el servidor de DHCP, verifique que el puerto tenga la opción STP PortFast activada y la opción de enlace troncal y canales desactivada. La configuración predeterminada consiste en que PortFast esté desactivado y la opción de enlace troncal y canales esté en el modo automático, si corresponde. Estos cambios de configuración resuelven los problemas más comunes de clientes DHCP que ocurren con la instalación inicial de un switch Catalyst. Repase CCNA Exploration: Conmutación de LAN y redes inalámbricas como ayuda para resolver este problema.

Tarea 5 de la resolución de problemas: Distinga si los clientes DHCP obtienen la dirección IP en la misma subred o VLAN que el servidor de DHCP

Es importante distinguir si DHCP está funcionando correctamente cuando el cliente está en la misma subred o VLAN que el servidor de DHCP. Si DHCP está funcionando bien, el problema puede residir en el agente relay DHCP/BOOTP. Si el problema persiste aún después de probar DHCP en la misma subred o VLAN que el servidor de DHCP, el problema puede ser el servidor de DHCP.

Resolución de problemas de configuraciones de DHCP

Resolución de problemas de DHCP	
Tarea 1 de la resolución de problemas:	Solucionar los conflictos de direcciones IP
Tarea 2 de la resolución de problemas:	Verificar la conectividad física
Tarea 3 de la resolución de problemas:	Probar la conectividad de red mediante la configuración de la estación de trabajo cliente con una dirección IP estática
Tarea 4 de la resolución de problemas:	Verificar la configuración de puerto de switch (con STP Portfast y otros comandos)
Tarea 5 de la resolución de problemas:	Distinguir si los clientes DHCP obtienen direcciones IP en la misma subred o VLAN que el servidor de DHCP

Verifique la configuración de relay del router DHCP/BOOTP

Cuando el servidor de DHCP se encuentra en una LAN separada del cliente, la interfaz del router con la que se conecta el cliente debe estar configurada para retransmitir solicitudes de DHCP. Esto se logra mediante la configuración de la dirección IP de helper. Si la dirección IP de helper no está bien configurada, las solicitudes de DHCP del cliente no se reenvían al servidor de DHCP.

Siga estos pasos para verificar la configuración del router:

Paso 1. Verifique que el comando **ip helper-address** esté configurado en la interfaz correcta. Debe estar presente en la interfaz de entrada de la LAN que contiene las estaciones de trabajo clientes DHCP y debe estar dirigido al servidor de DHCP correcto. En la figura, el resultado del comando **show running-config** verifica que la dirección IP de relay DHCP hace referencia a la dirección IP del servidor de DHCP 192.168.11.5.

Paso 2. Verifique que el comando de configuración global **no service dhcp** no se haya configurado. Este comando desactiva el servidor de DHCP y las funciones de relay en el router. El comando **service dhcp** no aparece en la configuración porque es la configuración predeterminada.

Verificación de relay DHCP

```
R1#show running-config

<Output omitted>
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 ip helper-address 192.168.11.5
 duplex auto
 speed auto
!
<Output omitted>
```

Verifique que el router esté recibiendo las solicitudes de DHCP mediante los comandos debug.

En los routers configurados como servidores de DHCP, el proceso DHCP falla si el router no recibe solicitudes del cliente. Como tarea de resolución de problemas, verifique que el router esté recibiendo las solicitudes de DHCP del cliente. Este paso de la resolución de problemas incluye la configuración de una lista de control de acceso para el resultado de la depuración. La lista de control de acceso de depuración no es intrusiva para el router.

En el modo de configuración global, cree la siguiente lista de control de acceso:

access-list 100 permit ip host 0.0.0.0 host 255.255.255.255

Comience la depuración con ACL 100 como parámetro de definición. En modo exec, introduzca el siguiente comando **debug**:

debug ip packet detail 100

El resultado que se muestra en la figura indica que el router está recibiendo las solicitudes de DHCP del cliente. La dirección IP de origen es 0.0.0.0 porque el cliente todavía no tiene una dirección IP. La dirección de destino es 255.255.255.255 porque el mensaje de descubrimiento de DHCP enviado por el cliente es un broadcast. Los puertos UDP de origen y destino, 68 y 67, son los puertos que DHCP utiliza normalmente.

Este resultado sólo muestra un resumen del paquete, pero no el paquete en sí. Por lo tanto, no es posible determinar si el paquete es correcto. No obstante, el router recibió un paquete broadcast con la dirección IP y los puertos UDP de origen y destino que son correctos para DHCP.

Verifique que el router esté recibiendo y reenviando las solicitudes de DHCP mediante el comando debug ip dhcp server packet.

El comando **debug ip dhcp server events** es útil para resolver problemas de funcionamiento de DHCP. Este comando informa sucesos del servidor, por ejemplo, asignaciones de direcciones y actualizaciones de bases de datos. También se utiliza para decodificar recepciones y transmisiones de DHCP.

Depuración de DHCP con los comandos debug del router

```
R2# access-list 100 permit ip host 0.0.0.0 host 255.255.255.255
R2# debug ip packet detail 100
IP packet debugging is on (detailed) for access list 100
R2#
00:16:46: IP: s=0.0.0.0 (Ethernet4/0), d=255.255.255.255, len 604, rcvd 2
00:16:46: UDP src=68, dst=67
00:16:46: IP: s=0.0.0.0 (Ethernet4/0), d=255.255.255.255, len 604, rcvd 2
00:16:46: UDP src=68, dst=67
```

DHCP asigna direcciones IP y otra información de configuración de la red de manera dinámica. Los routers Cisco pueden utilizar el conjunto de funciones de IOS de Cisco, que se llama Easy IP, como servidor de DHCP opcional con todas las funciones. Easy IP arrienda las configuraciones por 24 horas de forma predeterminada. En esta actividad, configurará los servicios de DHCP en dos routers y probará la configuración.
Se proporcionan instrucciones detalladas dentro de la actividad y en el siguiente enlace al PDF.
Instrucciones de las actividades (PDF)

7.2 Escalamiento de redes con NAT

7.2.1 Direccionamiento IP público y privado

Todas las direcciones de Internet públicas deben registrarse en un registro de Internet regional (RIR, Regional Internet Registry). Las organizaciones pueden arrendar direcciones públicas a través de un ISP. Sólo el titular registrado de una dirección de Internet pública puede asignar esa dirección a un dispositivo de red.

Tal vez haya notado que todos los ejemplos de este curso utilizan una cantidad algo restringida de direcciones IP. Tal vez también haya notado la similitud entre estos números y los números que utilizó en una red pequeña para ver la configuración de las páginas Web de muchas marcas de impresoras, routers DSL y por cable y otros periféricos. Son direcciones de Internet privadas reservadas que se toman de los tres bloques que se muestran en la figura. Estas direcciones son sólo para el uso particular de la red interna. Los paquetes que contienen estas direcciones no se enrutan a través de Internet y se conocen como direcciones no enrutables. RFC 1918 proporciona información detallada.

A diferencia de las direcciones IP públicas, las direcciones IP privadas son un bloque reservado de números y cualquiera las puede utilizar. Eso quiere decir que dos redes, o dos millones de redes, pueden utilizar las mismas direcciones privadas. Para evitar conflictos de direccionamiento, los routers nunca deben enrutar direcciones IP privadas. Para proteger la estructura de direcciones de Internet públicas, los ISP normalmente configuran los routers de borde para impedir que el tráfico con direcciones privadas se reenvíe a través de Internet.

Al proporcionar más espacio de direcciones de lo que la mayoría de las organizaciones pueden obtener a través de un RIR, el direccionamiento privado brinda a las empresas una flexibilidad considerable en materia de diseño de red. Esto permite implementar esquemas de direccionamiento convenientes desde un punto de vista funcional y administrativo, además de facilitar el crecimiento.

Sin embargo, como no es posible enrutar direcciones privadas a través de Internet, y como no hay suficientes direcciones públicas como para permitir a las organizaciones que proporcionen una a cada uno de sus hosts, las redes necesitan un

mecanismo para traducir las direcciones privadas en direcciones públicas en el extremo de la red y que funcione en ambas direcciones. Sin un sistema de traducción, los hosts privados que se encuentran detrás de un router en la red de una organización no pueden conectarse con otros hosts privados que se encuentran en otras organizaciones a través de Internet.

La traducción de direcciones de red (NAT, Network Address Translation) proporciona este mecanismo. Antes del desarrollo de NAT, un host con dirección privada no podía acceder a Internet. Con NAT, las empresas individuales pueden direccionar algunos o todos sus hosts con direcciones privadas y utilizar NAT para proporcionar acceso a Internet.

Para obtener un análisis más detallado del desarrollo del sistema RIR, consulte el artículo de Cisco Internet Protocol Journal en http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_4-4/regional_internet_registries.html.

Direcciones de Internet públicas y privadas

Las direcciones públicas de Internet son reguladas por cinco registros americanos de números de Internet (RIR, Regional Internet Registries):

- ARIN
- RIPE
- APNIC
- LACNIC
- AfriNIC

Las direcciones privadas de Internet están definidas en RFC 1918:

Clase	Rango de direcciones internas RFC 1918	Prefijo CIDR
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

7.2.2 ¿Qué es NAT?

¿Qué es NAT?

NAT es como el recepcionista de una oficina grande. Imagine que le indica al recepcionista que no le pase ninguna llamada a menos que se lo solicite. Más tarde, llama a un posible cliente y le deja un mensaje para que le devuelva el llamado. A continuación, le informa al recepcionista que está esperando una llamada de este cliente y le solicita que le pasela llamada a su teléfono.

El cliente llama al número principal de la oficina, que es el único número que el cliente conoce. Cuando el cliente informa al recepcionista a quién está buscando, el recepcionista se fija en una tabla de búsqueda que indica cuáles el número de extensión de su oficina. El recepcionista sabe que el usuario había solicitado esta llamada, de manera que la reenvía a su extensión.

Entonces, mientras que el servidor de DHCP asigna direcciones IP dinámicas a los dispositivos que se encuentran dentro de la red, los routers habilitados para NAT retienen una o varias direcciones IP de Internet válidas fuera de la red. Cuando el cliente envía paquetes fuera de la red, NAT traduce la dirección IP interna del cliente a una dirección externa. Para los usuarios externos, todo el tráfico que entra a la red y sale de ella tiene la misma dirección IP o proviene del mismo conjunto de direcciones.

NAT tiene muchos usos, pero la utilidad clave es el ahorro de direcciones IP al permitir que las redes utilicen direcciones IP privadas. NAT traduce direcciones internas, privadas y no enrutables a direcciones públicas enrutables. NAT tiene el beneficio adicional de agregar un nivel de privacidad y seguridad a una red porque oculta las direcciones IP internas de las redes externas.

Un dispositivo que ejecuta NAT generalmente opera en la frontera de una red de conexión única. En nuestro ejemplo, R2 es el router de borde. Una red de conexión única es una red que posee una sola conexión a su red vecina. Como se ve en el ISP, R2 forma una red de conexión única.

Cuando un host perteneciente a una red de conexión única, por ejemplo, la PC1, la PC2 o la PC 3, desea transmitir información a un host externo, el paquete se envía a R2, el router del gateway de borde. R2 realiza el proceso de NAT y traduce así la dirección privada interna del host a una dirección pública, externa y enrutable.

En la terminología de NAT, la red interna es el conjunto de redes que está sujeto a traducción. La red externa se refiere a todas las otras direcciones. Las direcciones IP tienen diferentes designaciones según se encuentren en la red privada o en la red pública (Internet) y el tráfico sea entrante o saliente.

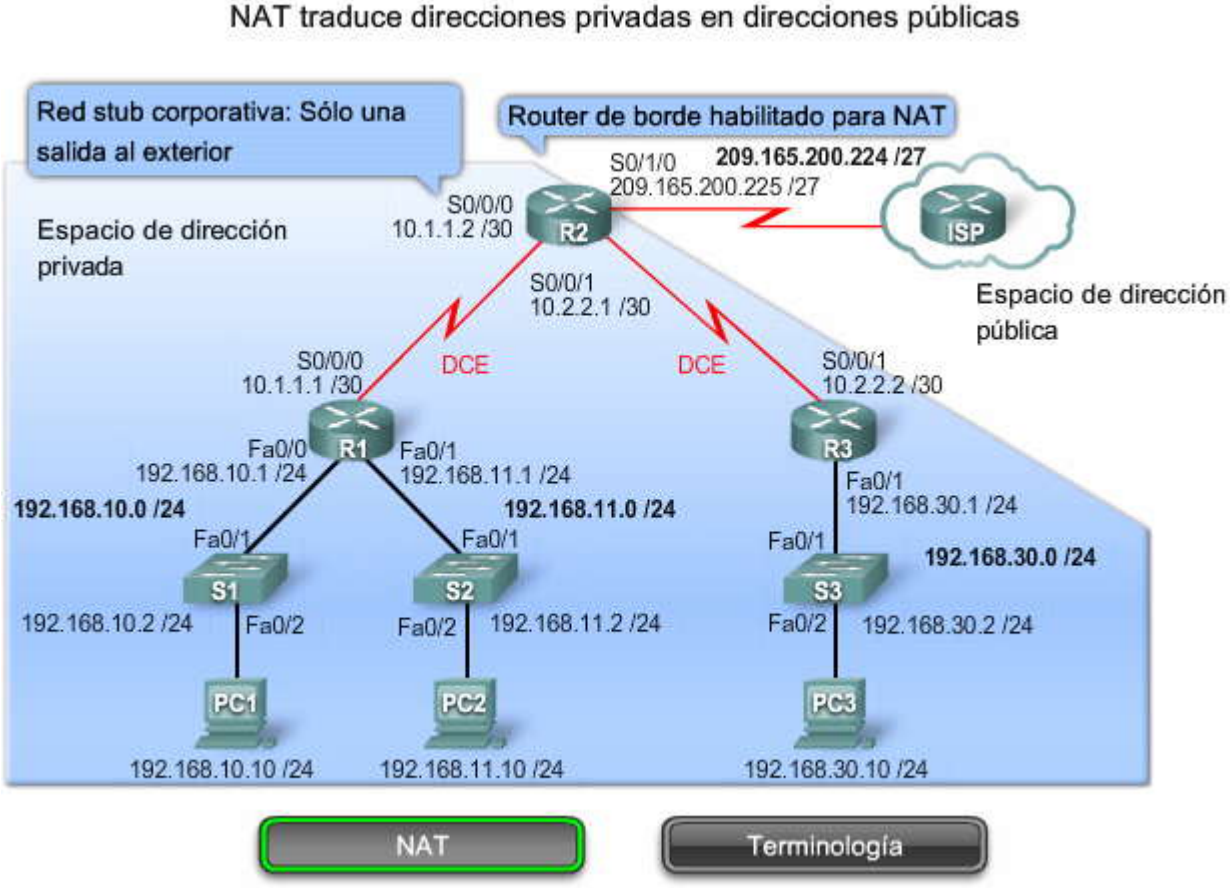
Haga clic en el botón Terminología de NAT que se muestra en la figura.

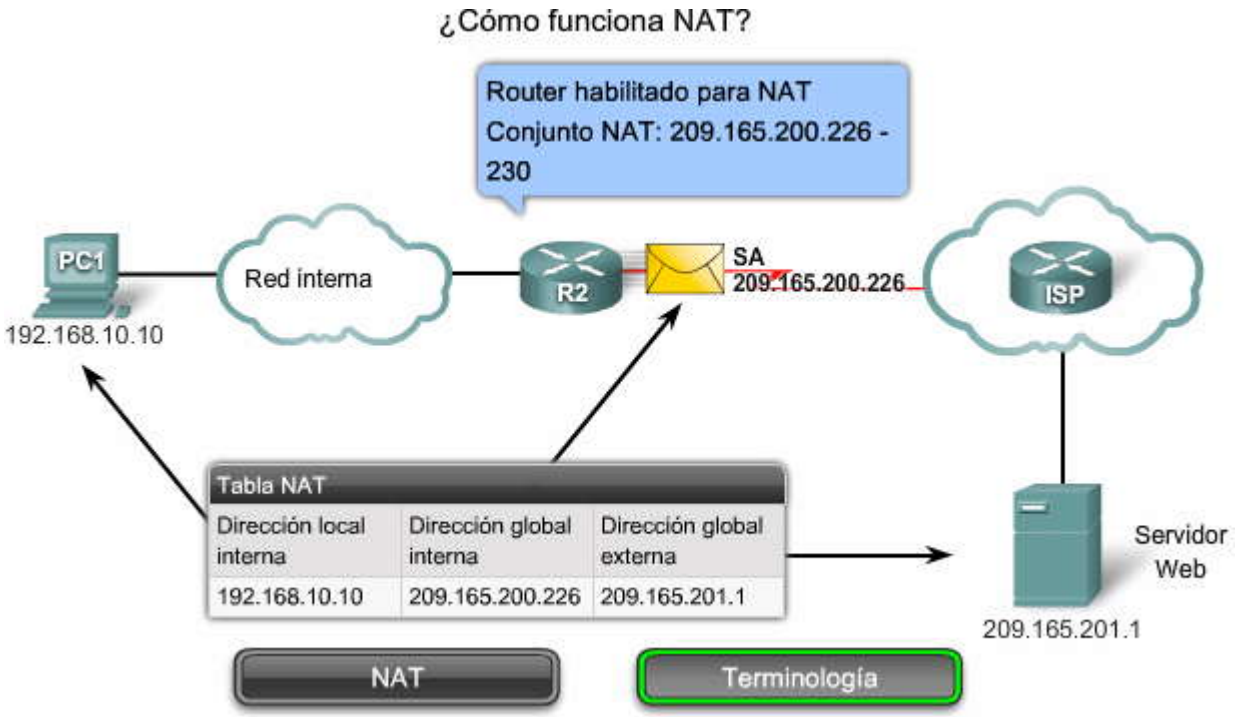
La figura muestra cómo hacer referencia a las interfaces al configurar NAT. Supongamos que el router R2 se configuró para proporcionar funciones de NAT. Tiene un conjunto de direcciones disponibles públicamente para arrendar a los hosts internos. Esta sección usa los siguientes términos al hablar sobre NAT:

- **Dirección local interna**: normalmente no es una dirección IP asignada por un RIR o un proveedor de servicios; lo más probable es que sea una dirección RFC 1918 privada. En la figura, la dirección IP 192.168.10.10 está asignada al host PC1 dentro de la red.
- **Dirección global interna**: dirección pública válida que se asigna al host interno cuando sale del router NAT. Cuando el tráfico de la PC1 está dirigido al servidor Web 209.165.201.1, el router R2 debe traducir la dirección. En este caso, la dirección IP 209.165.200.226 se utiliza como dirección global interna para la PC1.
- **Dirección global externa**: dirección IP a la que se puede acceder y que fue asignada a un host en Internet. Por ejemplo, se puede acceder al servidor Web en la dirección IP 209.165.201.1.
- **Dirección local externa**: dirección IP local asignada a un host en la red externa. En la mayoría de las situaciones, esta dirección es idéntica a la dirección global externa de ese dispositivo externo.

Nota: En este curso, haremos referencia a la dirección local interna, la dirección global interna y la dirección global externa. El uso de la dirección local externa está fuera del ámbito de este curso.

El "interior" de una configuración NAT no es sinónimo de las direcciones privadas según la definición de RFC 1918. Las direcciones a las que llamamos "no enrutables" no siempre son no enrutables. Un administrador puede configurar cualquier router para que pase el tráfico a través de subredes privadas. Sin embargo, si intentan pasar al ISP un paquete destinado a una dirección privada, el ISP lo descarta. No enrutable significa que no se puede enrutar a través de Internet.





¿Cómo funciona NAT?

En este ejemplo, un host interno (192.168.10.10) desea comunicarse con un servidor Web externo (209.165.200.1). Envía un paquete a R2, el gateway de borde configurado con NAT para la red.

Use los controles de la figura para comenzar la animación.

R2 lee la dirección IP de destino del paquete y controla que el paquete cumpla los criterios especificados para la traducción. R2 tiene una ACL que identifica la red interna como hosts válidos para la traducción. Por lo tanto, traduce una dirección IP local interna a una dirección IP global interna, que en este caso es 209.165.200.226. Almacena esta asignación de la dirección local a global en la tabla NAT.

Después el router envía el paquete a su destino. Cuando el servidor Web responde, el paquete regresa a la dirección global de R2 (209.165.200.226).

R2 consulta su tabla NAT y ve que se trata de una dirección IP que había traducido con anterioridad. Por lo tanto, traduce la dirección global interna a la dirección local interna y el paquete se envía a la PC1 a la dirección IP 192.168.10.10. Si no encuentra una asignación, el paquete se descarta.

Asignación dinámica y asignación estática

Hay dos tipos de traducción NAT: dinámica y estática.

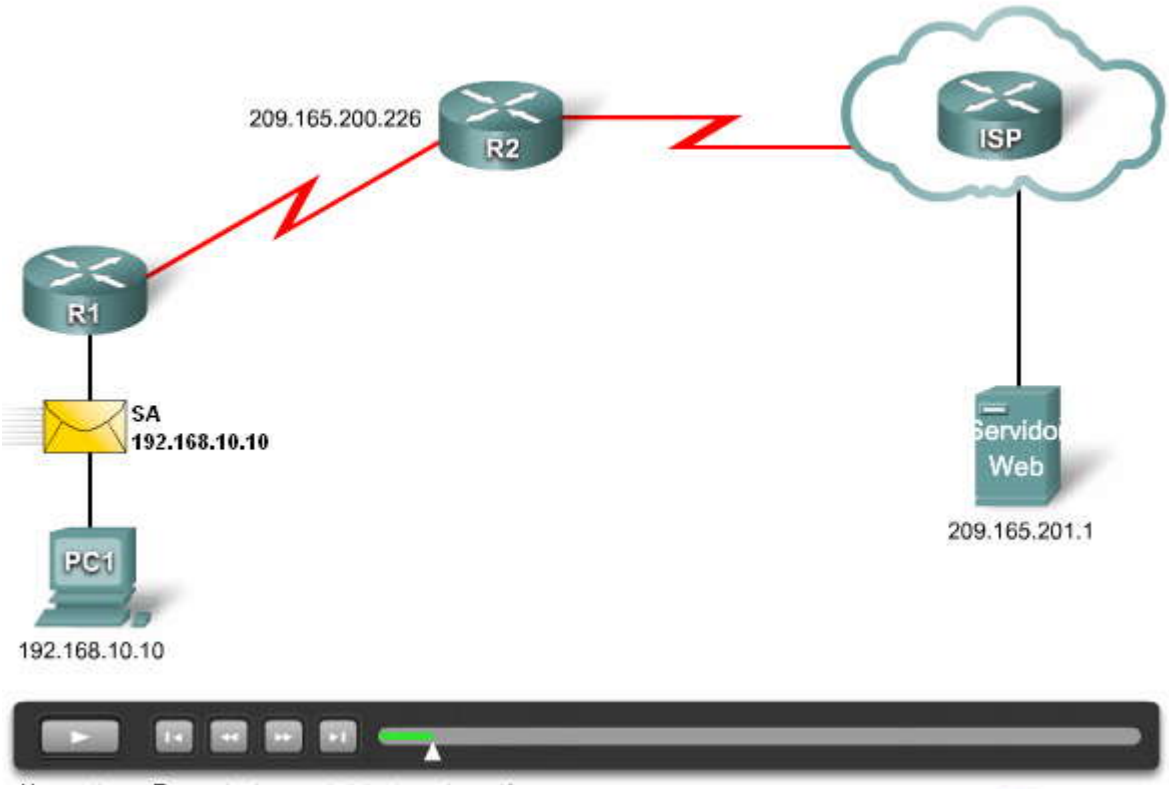
La traducción NAT dinámica usa un conjunto de direcciones públicas y las asigna en orden de llegada. Cuando un host con una dirección IP privada solicita acceso a Internet, la traducción NAT dinámica elije una dirección IP del conjunto de direcciones que no esté siendo utilizada por otro host. Éste es el tipo de asignación que hemos descrito hasta ahora.

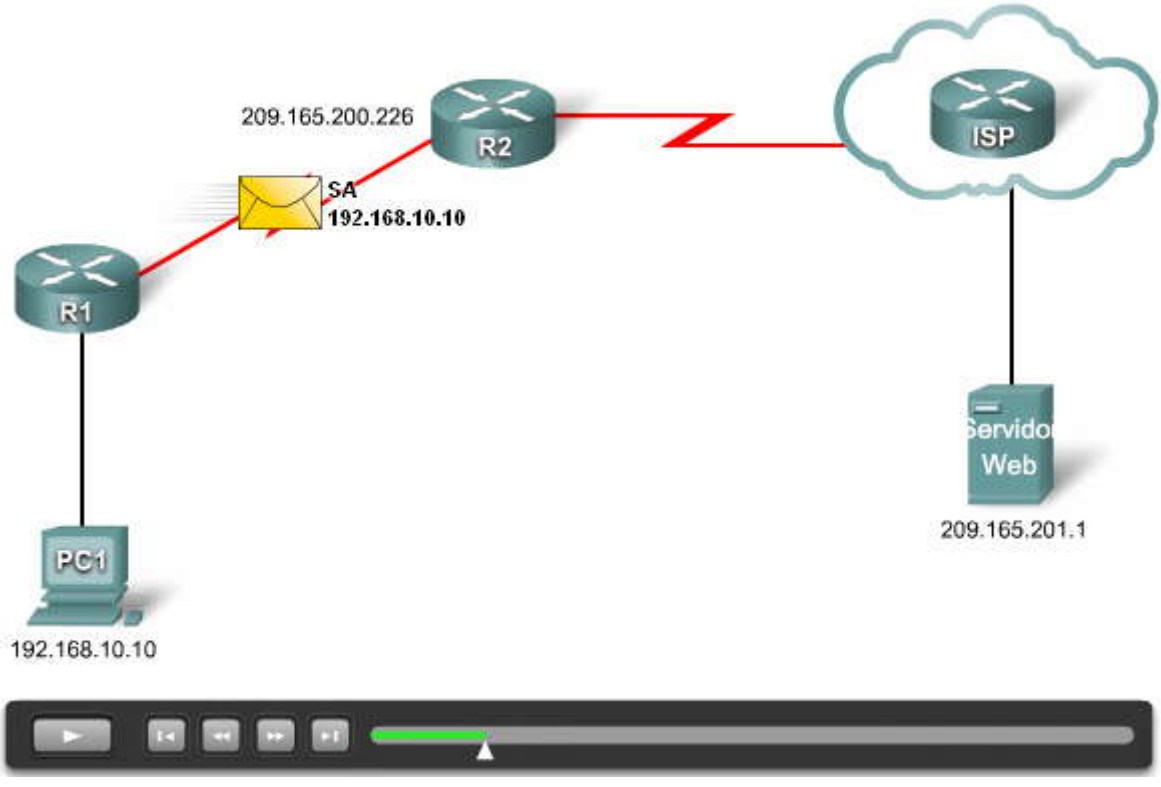
La traducción NAT estática utiliza un sistema de asignación de uno a uno entre las direcciones locales y las globales, y estas asignaciones son constantes. La traducción NAT estática resulta particularmente útil para los servidores Web o los hosts que necesitan tener una dirección uniforme a la que se pueda tener acceso desde Internet. Estoshosts internos pueden ser servidores de empresas o dispositivos de networking.

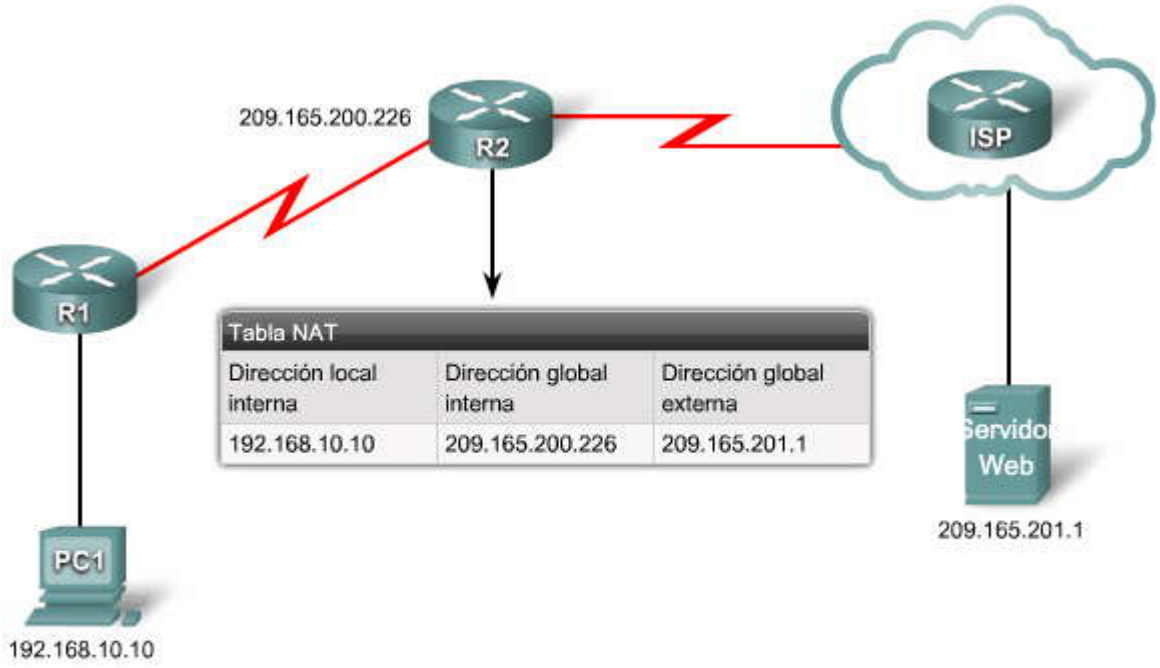
Tanto la traducción NAT estática como la dinámica necesitan que haya una cantidad suficiente de direcciones públicas disponibles para cubrir la cantidad total de sesiones de usuario simultáneas.

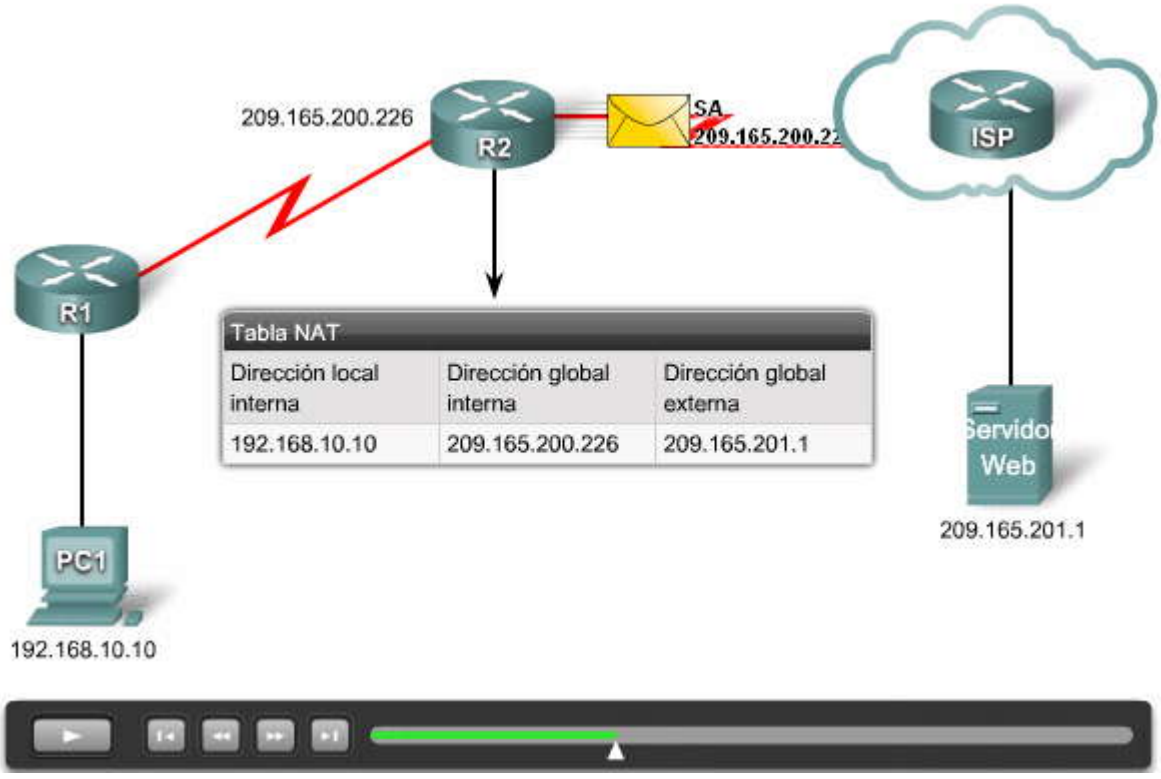
Si desea ver el funcionamiento de la traducción NAT dinámica desde otra perspectiva, vaya a http://www.cisco.com/warp/public/556/nat.swf.

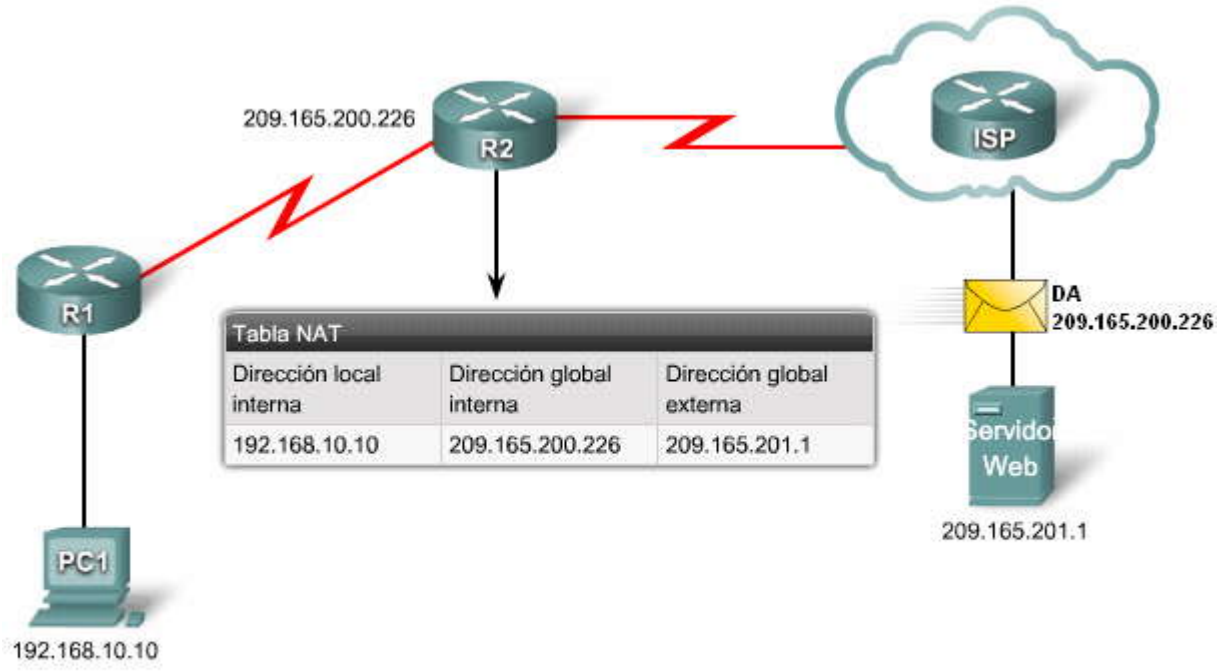
¿Cómo funciona NAT?

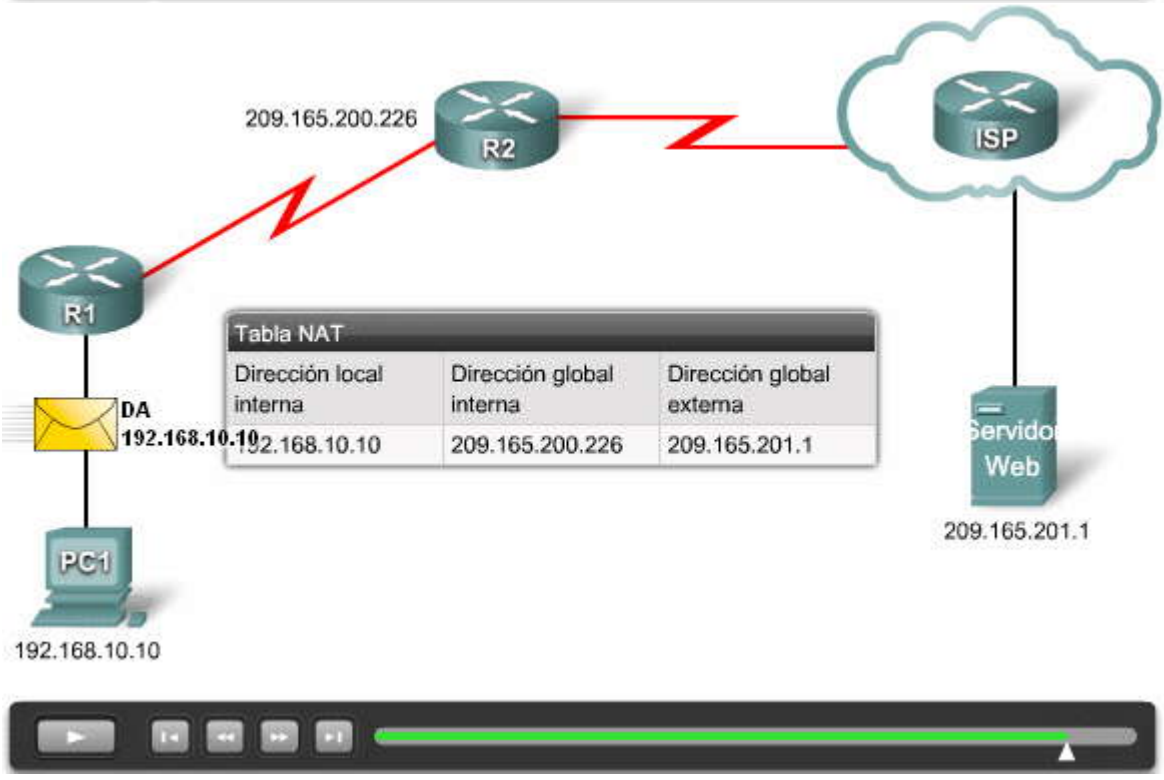





209.165.200.226
R2
ISP
R1
Tabla NAT
Dirección local interna
Dirección global interna
Dirección global externa
192.168.10.10
209.165.200.226
209.165.201.1
Web
209.165.201.1
PC1
192.168.10.10


209.165.200.226
R2
SA
ISP
R1
Tabla NAT
Dirección local interna
Dirección global interna
Dirección global externa
192.168.10.10
209.165.200.226
209.165.201.1
Web
209.165.201.1
PC1
192.168.10.10





Sobrecarga de NAT

La sobrecarga de NAT (a veces llamada Traducción de la dirección del puerto, [PAT, Port Address Translation]) asigna varias direcciones IP privadas a una única dirección IP pública o a un grupo pequeño de direcciones IP públicas. Es lo que hacen la mayoría de los routers. El ISP asigna una dirección al router doméstico, y varios integrantes de la familia pueden navegar por Internet de manera simultánea.

Con la sobrecarga de NAT, es posible asignar varias direcciones a una o sólo algunas direcciones porque cada dirección privada también se identifica por un número de puerto. Cuando un cliente abre una sesión TCP/IP, el router NAT asigna

un número de puerto a la dirección de origen correspondiente. La sobrecarga de NAT asegura que los clientes utilicen un número de puerto TCP diferente para cada sesión de cliente con un servidor en Internet. Cuando se recibe una respuesta del servidor, el número de puerto de origen, que pasa a ser el número de puerto de destino en la respuesta, determina a qué cliente se enrutan los paquetes. Además valida que los paquetes entrantes fueron solicitados, lo que agrega seguridad a la sesión.

Haga clic en los controles para iniciar la animación o hacer una pausa.

La animación ilustra el proceso. La sobrecarga de NAT utiliza números únicos de puerto origen en la dirección IP global interna para distinguir entre las traducciones. A medida que NAT procesa cada paquete, utiliza un número de puerto (en este ejemplo, 1331 y 1555) para identificar al cliente desde donde se originó el paquete. La dirección de origen (SA, Source Address) es la dirección IP local interna con el número de puerto TCP/IP asignado adjuntado a ella. La dirección de destino (DA, Destination Address) es la dirección IP local externa con el número de puerto del servicio adjuntado a ella, en este caso el puerto 80: HTTP.

En el router del gateway de borde (R2), la sobrecarga de NAT cambia la SA por la dirección IP global del cliente, nuevamente con el número de puerto adjuntado a ella. La DA es la misma dirección, pero ahora hace referencia a la dirección IP global externa. Cuando el servidor Web responde, se sigue la misma ruta pero en sentido inverso.

Los números de puerto se codifican en 16 bits. En teoría, la cantidad total de direcciones internas que se pueden traducir a una dirección externa podría ser de hasta 65 536 por dirección IP. Sin embargo, en realidad, la cantidad de direcciones internas que se pueden asignar a una única dirección IP es de aproximadamente 4000.

Haga clic en el botón Siguiente puerto disponible que se muestra en la figura.

En el ejemplo anterior, los números de los puertos de cliente de las dos SA, 1331 y 1555, no cambian en el gateway de borde. No es muy probable que se presente esta situación porque existe una alta probabilidad de que esos números ya hayan sido adjuntados a otras sesiones en desarrollo.

La sobrecarga de NAT intenta conservar el puerto de origen original. Sin embargo, si este puerto origen está en uso, la sobrecarga de NAT asigna el primer número de puerto disponible, desde el principio del grupo de puertos correspondiente 0-511, 512-1023, ó 1024-65535. Cuando no hay más puertos disponibles y hay más de una dirección IP externa configurada, la sobrecarga de NAT utiliza la próxima dirección IP para tratar de asignar nuevamente el puerto de origen original. Este proceso continúa hasta que no haya puertos ni direcciones IP externas disponibles.

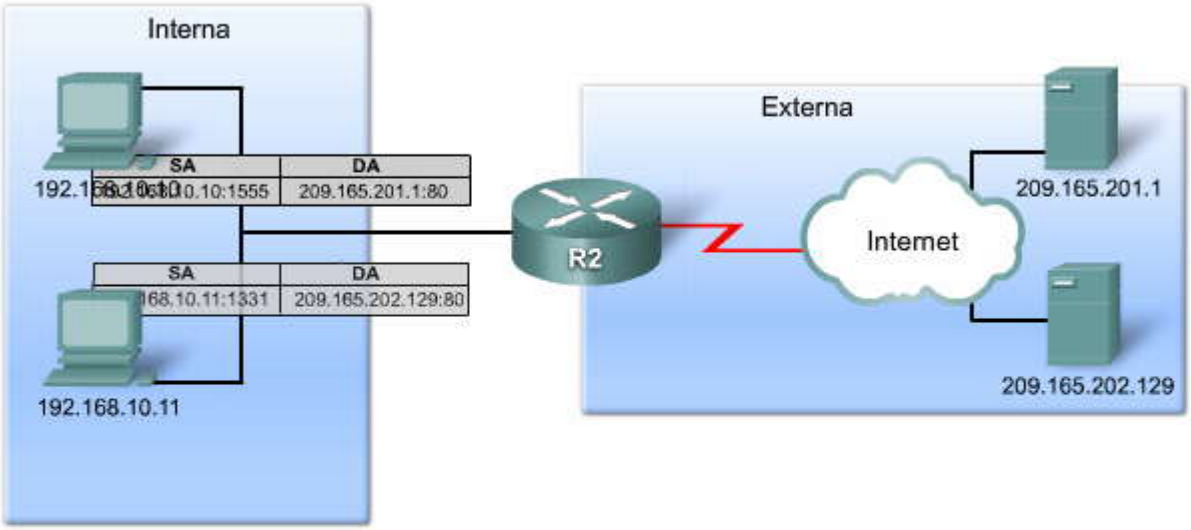
En la figura, los dos hosts han elegido el mismo número de puerto, 1444. Esto es aceptable para la drección interna, porque ambos tienen direcciones IP privadas únicas. Sin embargo, en el gateway de borde, los números de los puertos deben cambiarse; de lo contrario, dos paquetes de los dos hosts saldrían de R2 con la misma dirección de origen. La sobrecarga de NAT ha asignado a la segunda dirección el primer número de puerto disponible, que en este caso es 1445.

Diferencias entre NAT y la sobrecarga de NAT

Un resumen de las diferencias entre NAT y la sobrecarga de NAT lo ayudará a comprender mejor este tema. NAT generalmente sólo traduce direcciones IP en una correspondencia de 1:1 entre direcciones IP expuestas públicamente y direcciones IP privadas. La sobrecarga de NAT modifica la dirección IP privada y el número de puerto del emisor. La sobrecarga de NAT elije los números de puerto que ven los hosts de la red pública.

NAT enruta los paquetes entrantes hasta el destino interno mediante la consulta a la dirección IP de origen entrante dada por el host de la red pública. Con la sobrecarga de NAT, en general sólo hay una o algunas direcciones IP expuestas públicamente. Los paquetes entrantes de la red pública se enrutan a sus destinos de la red privada mediante la consulta a una tabla del dispositivo de la sobrecarga de NAT que lleva un control de los pares de puertos públicos y privados. Esto se denomina seguimiento de la conexión.

Sobrecarga de NAT



Haga clic en Reproducir para iniciar la animación.

Proceso NAT | Siguiente puerto disponible

Sobrecarga de NAT

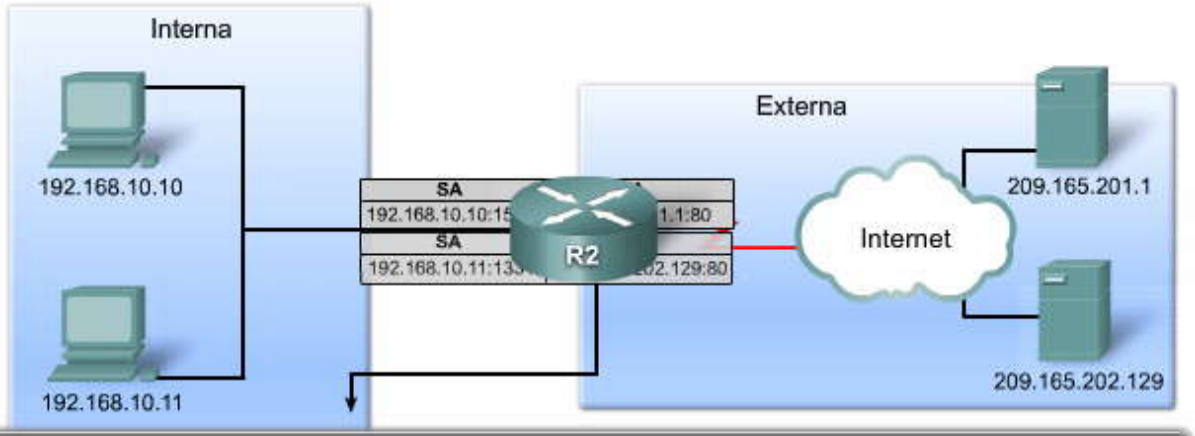


Tabla NAT con sobrecarga			
Dirección IP local interna	Dirección IP global interna	Dirección IP global externa	Dirección IP local externa
192.168.10.10:1555	209.165.200.226:1555	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1331	209.165.200.226:1331	209.165.202.129:80	209.165.202.129:80

Haga clic en Reproducir para iniciar la animación.

Proceso NAT | Siguiente puerto disponible

Sobrecarga de NAT

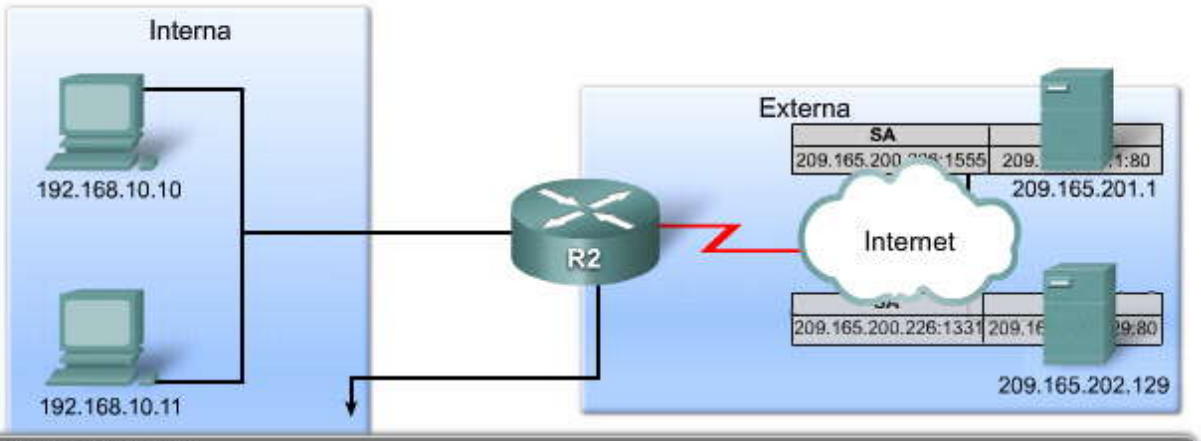
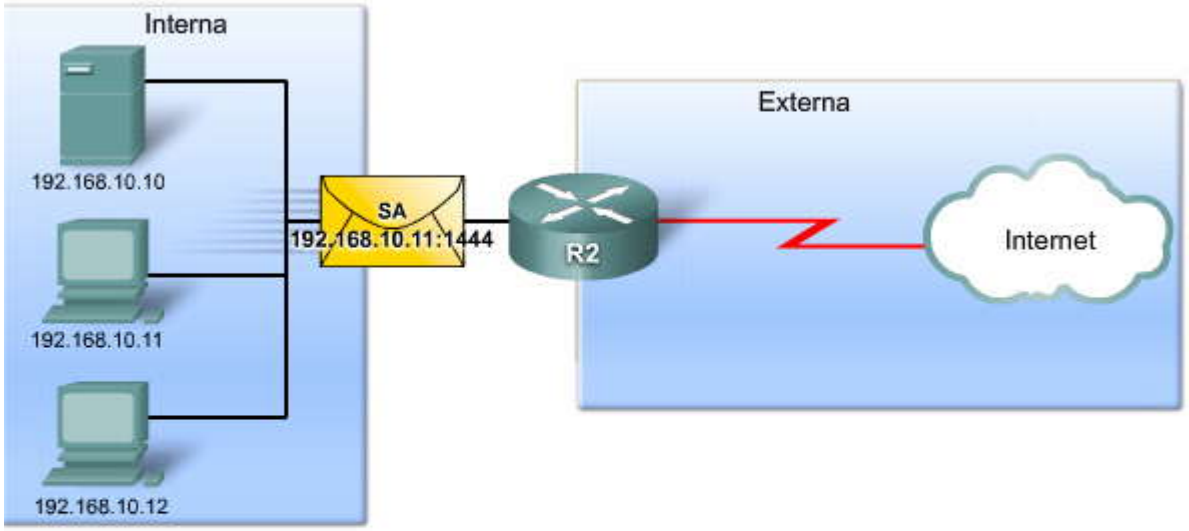


Tabla NAT con sobrecarga			
Dirección IP local interna	Dirección IP global interna	Dirección IP global externa	Dirección IP local externa
192.168.10.10:1555 192.168.10.11:1331	209.165.200.226:1555 209.165.200.226:1331	209.165.201.1:80 209.165.202.129:80	209.165.201.1:80 209.165.202.129:80

Haga clic en Reproducir para iniciar la animación.

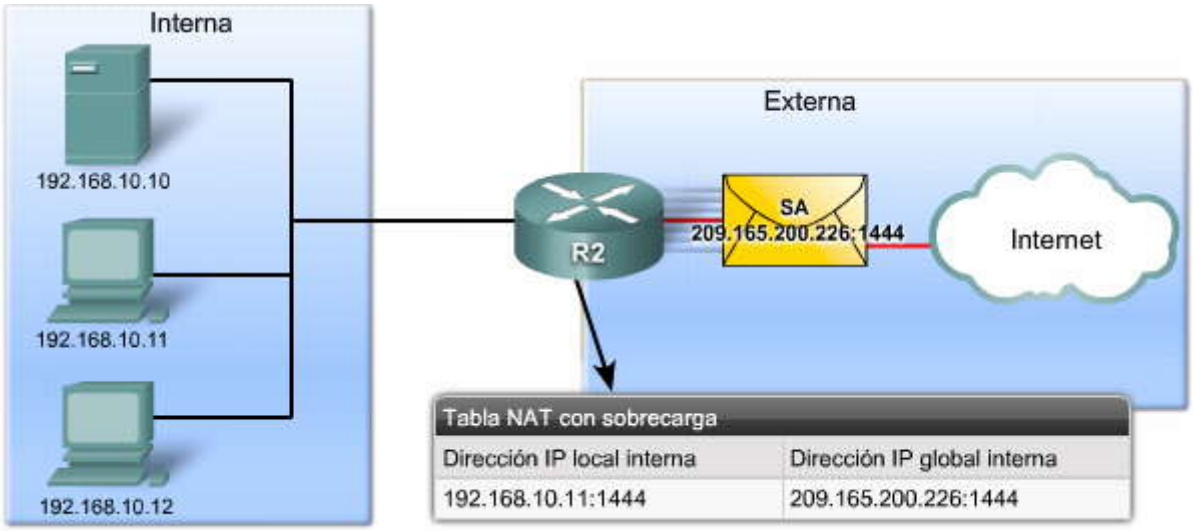
Proceso NAT | Siguiente puerto disponible

Sobrecarga de NAT



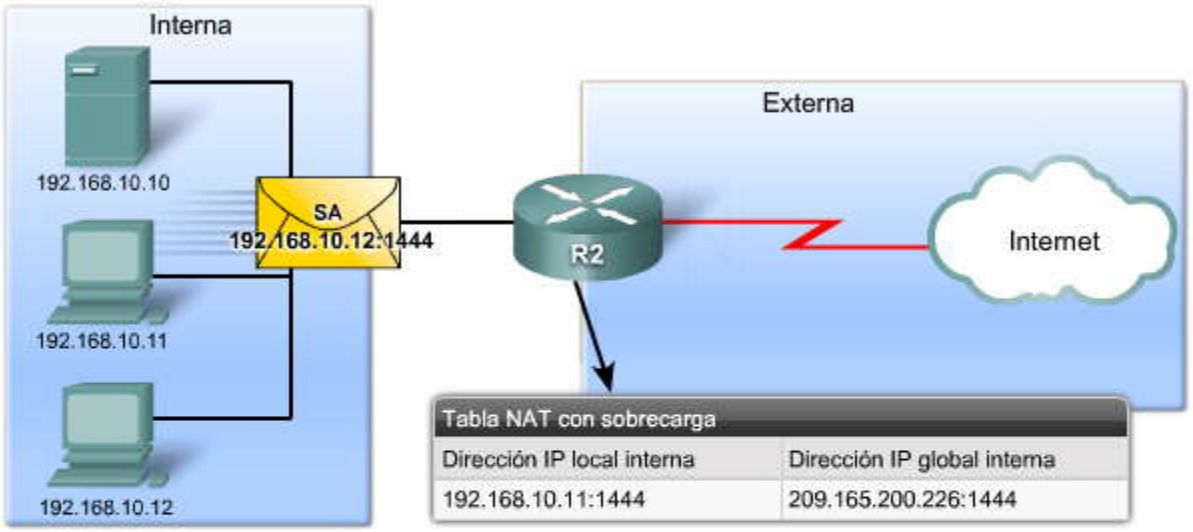
Haga clic en Reproducir para iniciar la animación.

Proceso NAT | Siguiente puerto disponible



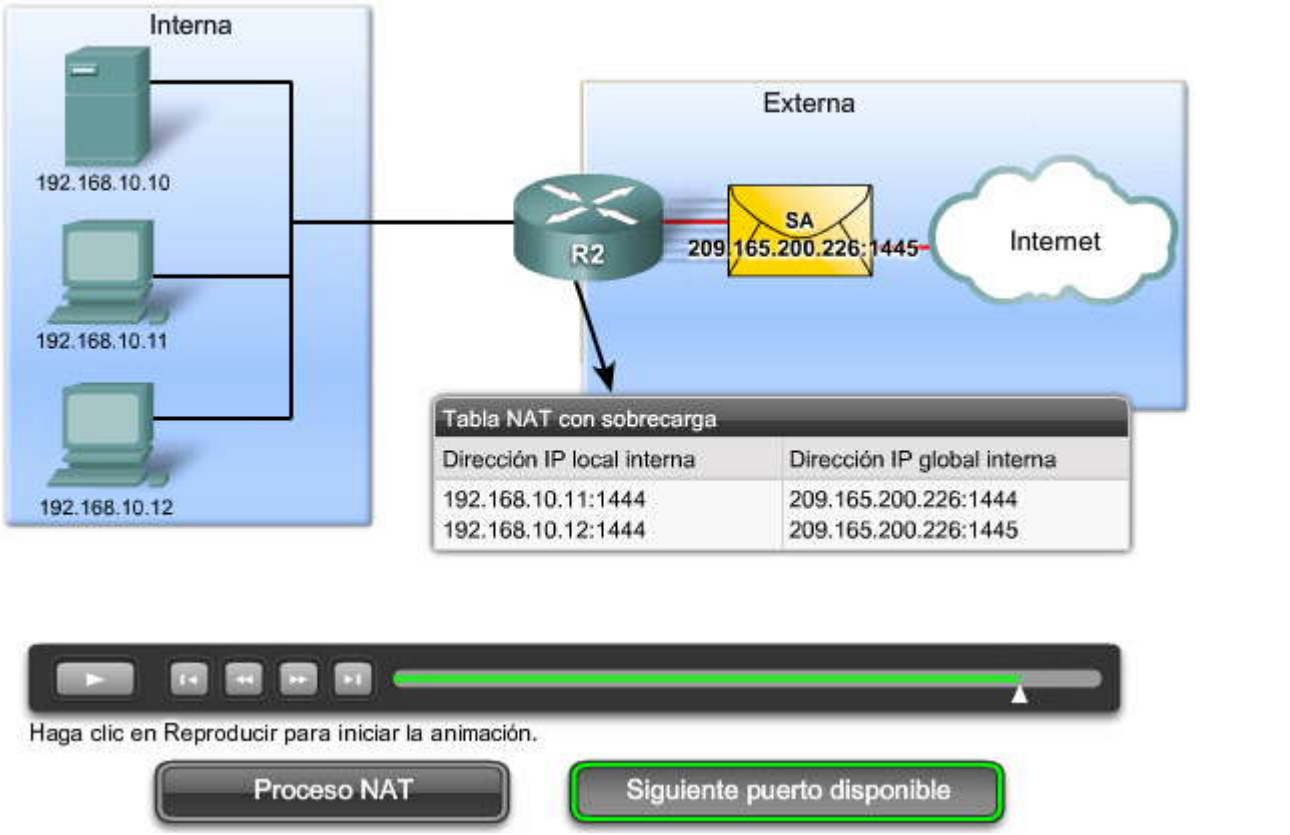
Haga clic en Reproducir para iniciar la animación.

Proceso NAT | Siguiente puerto disponible



Haga clic en Reproducir para iniciar la animación.

Proceso NAT | Siguiente puerto disponible



7.2.3 Ventajas y desventajas del uso de NAT

Ventajas y desventajas del uso de NAT

NAT proporciona muchos beneficios y ventajas. Sin embargo, el uso de NAT tiene algunas desventajas, entre ellas, la incompatibilidad con algunos tipos de tráfico.

Entre los beneficios del uso de NAT se encuentran los siguientes:

- NAT conserva el esquema de direccionamiento legalmente registrado, lo que permite la privatización de redes internas. NAT conserva las direcciones mediante la multiplexación a nivel de puerto de la aplicación. Con la sobrecarga de NAT, los hosts internos pueden compartir una sola dirección IP pública para toda comunicación externa. En este tipo de configuración, se requieren muy pocas direcciones externas para admitir muchos hosts internos.
- NAT aumenta la flexibilidad de las conexiones con la red pública. Se pueden implementar varios conjuntos, conjuntos de respaldo y de balanceo de carga para asegurar que las conexiones de red pública sean confiables.
- NAT proporciona uniformidad en los esquemas de direccionamiento internos de red. En una red sin direcciones IP privadas y NAT, cambiar de direcciones IP públicas requiere la renumeración de todos los hosts en la red existente. El costo de renumerar los host puede ser elevado. NAT permite que permanezca el esquema existente, al mismo tiempo que admite un nuevo sistema de direccionamiento público. Esto significa que una organización puede cambiar de ISP y notener que cambiar ninguno de sus clientes internos.
- NAT proporciona seguridad de red. Debido a que las redes privadas no publicitan sus direcciones o topología interna, éstas son razonablemente seguras cuando se las utiliza en conjunto con NAT para tenerun acceso externo controlado. Sin embargo, NAT no reemplaza los firewalls.

No obstante, NAT tiene algunas desventajas. El hecho de que los hosts de Internet parezcan comunicarse directamente con el dispositivo NAT en lugar de hacerlo con el verdadero host perteneciente a la red privada crea una serie de problemas. En teoría, una única dirección IP globalmente única puede representar a muchos hosts con direcciones privadas. Esto tiene ventajas desde el punto de vista de la privacidad y la seguridad, pero en la práctica hay desventajas.

La primera desventaja es que el rendimiento se ve afectado. NAT aumenta los retrasos en la conmutación porque la traducción de cada dirección IP dentro de los encabezados del paquete lleva tiempo. El primer paquete es de conmutación de procesos, lo que significa que siempre va por la ruta más lenta. El router tiene que inspeccionar cada paquete para decidir

si es necesario traducirlo. El router debe modificar el encabezado IP, y posiblemente el encabezado TCP o UDP también: Los paquetes restantes van por la ruta de conmutación rápida si hay una entrada de caché; en el caso contrario, también sufren retrasos.

Muchos protocolos y aplicaciones de Internet dependen de que la funcionalidad se aplique de extremo a extremo y que los paquetes se reenvíen sin modificaciones desde el origen al destino. Al cambiar las direcciones de extremo a extremo, NAT impide el funcionamiento de algunas aplicaciones que utilizan direccionamiento IP. Por ejemplo, algunas aplicaciones de seguridad, como ser las firmas digitales, fallan porque la dirección IP de origen cambia. Las aplicaciones que utilizan las direcciones físicas en vez de un nombre de dominio calificado no llegan a los destinos que se traducen en el router NAT. Algunas veces, este problema puede evitarse implementando asignaciones NAT estáticas.

También se pierde la capacidad de rastreo de extremo a extremo. Se hace mucho más difícil rastrear paquetes que sufren varios cambios en la dirección del paquete al atravesar múltiples saltos NAT, lo que dificulta la resolución de problemas. Por otra parte, los piratas informáticos que deseen determinar la fuente del paquete, descubrirán que es muy difícil rastrear u obtener la dirección origen o destino original.

El uso de NAT también complica el funcionamiento de los protocolos de tunneling, por ejemplo IPsec, porque NAT modifica valores de los encabezados e interfiere así con los controles de integridad que ejecutan IPsec y otros protocolos de tunneling.

Los servicios que requieren el inicio de conexiones TCP desde el exterior de la red, o protocolos sin estado como los que usan UDP, pueden verse interrumpidos. A menos que el router NAT haga un esfuerzo específico para admitir estos protocolos, los paquetes entrantes no pueden llegar a destino. Algunos protocolos pueden acomodar una instancia de NAT entre hosts participantes (por ejemplo, FTP en modo pasivo), pero fallan cuando los dos sistemas están separados de Internet por NAT.

Ventajas y desventajas de NAT

Ventajas de NAT
• Conserva el esquema de direccionamiento legalmente registrado
• Aumenta la flexibilidad de las conexiones con la red pública.
• Brinda regularidad para esquemas de direccionamiento de redes internas.
• Brinda seguridad de red
Desventajas de NAT
• Disminuye el rendimiento
• Disminuye la funcionalidad de extremo a extremo
• Se pierde la capacidad de rastreo IP de extremo a extremo
• El tunneling es más complicado
• Puede interrumpirse el inicio de conexiones TCP
• Las arquitecturas deben reconstruirse para adaptarse a los cambios

7.2.4 Configuración de NAT estática

NAT estática

Recuerde que la asignación NAT estática es una asignación uno a uno entre una dirección interna y una dirección externa. La NAT estática permite conexiones iniciadas por dispositivos externos dirigidas a dispositivos internos. Por ejemplo, puede asignar una dirección global interna a una dirección local interna específica que está asignada al servidor Web.

La configuración de las traducciones NAT estáticas es una tarea simple. Debe definir las direcciones que desea traducir y a continuación configurar NAT en las interfaces correspondientes. Los paquetes que llegan a una interfaz interna provenientes de la dirección IP identificada se someten al proceso de traducción. Los paquetes que llegan a una interfaz externa dirigidos a la dirección IP identificada se someten al proceso de traducción.

La figura explica los comandos para los pasos. Las traducciones estáticas se introducen directamente en la configuración. A diferencia de las traducciones dinámicas, estas traducciones siempre están en la tabla NAT.

Haga clic en el botón Ejemplo en la figura.

La figura es una configuración NAT estática simple aplicada a ambas interfaces. El router siempre traduce los paquetes provenientes del host interno de la red con la dirección privada de 192.168.10.254 a una dirección externa de

209.165.200.254. El host de Internet dirige las solicitudes Web a la dirección IP pública 209.165.200.254 y el router R2 siempre reenvía ese tráfico al servidor a la dirección 192.168.10.254.

Configuración de NAT estática

Paso	Acción	Notas
1	Se establece la traducción estática entre una dirección local interna y una dirección global interna. `Router(config)#ip nat inside source static local-ip global-ip`	Ingrese el comando global **no ip nat inside source** para eliminar la traducción estática de origen.
2	Especifique la interfaz interna. `Router(config)#interface type number`	Ingrese el comando **interface**. El indicador de CLI cambiará de `(config)#` a `(config-if)#`.
3	Marque la interfaz como conectada al interior. `Router(config-if)#ip nat inside`	
4	Salga del modo de configuración de interfaz. `Router(config-if)# exit`	
5	Especifique la interfaz externa. `Router(config)#interface type number`	
6	Marque la interfaz como conectada al exterior. `Router(config-if)#ip nat outside`	

Comandos | Ejemplo

Configuración de NAT estática


```
ip nat inside source static 192.168.10.254 209.165.200.254
!–Establishes static translation between an inside local address and an inside global address.
interface serial 0/0/0
ip nat inside
!—Identifies Serial 0/0/0 as an inside NAT interface.
interface serial 0/1/0
ip nat outside
!—Identifies Serial 0/1/0 as an outside NAT interface.
```

Con esta configuración, 192.168.10.254 siempre se traducirá a 209.165.200.254

Comandos | Ejemplo

7.2.5 Configuración de NAT dinámica

Configuración de NAT dinámica

Mientras que la NAT estática proporciona una asignación permanente entre una dirección interna y una dirección pública específica, la NAT dinámica asigna direcciones IP privadas a direcciones públicas. Estas direcciones IP públicas provienen de un conjunto de NAT. La configuración NAT dinámica difiere de la NAT estática, pero también tiene algunas similitudes. Como la NAT estática, requiere que la configuración identifique cada interfaz como interfaz interna o externa. Sin embargo, en lugar de crear una asignación estática a una única dirección IP, se utiliza un conjunto de direcciones globales internas.

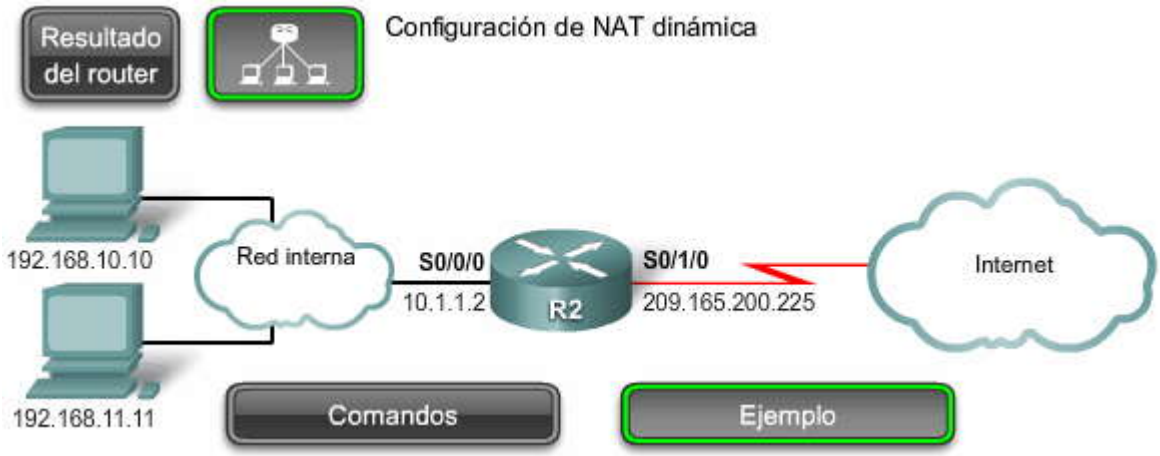
Haga clic en el botón Comandos en la figura para ver los pasos de la configuración de NAT dinámica.

Para configurar NAT dinámica, necesita una ACL que permita sólo las direcciones que se traducirán. Al desarrollar la ACL, recuerde que hay una opción implícita "denegar todo" al final de cada ACL. Una ACL que es demasiado permisiva puede

desencadenar resultados impredecibles. Cisco no recomienda configurar listas de control de acceso con el comando **permit any** si los comandos NAT se refieren a esas listas. El uso de **permit any** puede hacer que NAT consuma demasiados recursos de los routers, lo que puede provocar problemas en la red.

Haga clic en el botón Ejemplo en la figura.

La configuración permite la traducción para todos los hosts de las redes 192.168.10.0 y 192.168.11.0 cuando generan tráfico que entra por S0/0/0 y sale por S0/1/0. Estos hosts se traducen a una dirección disponible del rango 209.165.200.226 a 209.165.200.240.



Configuración de NAT dinámica

Paso	Acción	Notas
1	Defina un conjunto de direcciones globales para asignar según sea necesario. `Router(config)#ip nat pool name start-ip end-ip {netmask netmask|prefix-length prefix-length}`	Ingrese el comando global `no ip nat pool name` para eliminar el conjunto de direcciones globales.
2	Defina una lista de acceso estándar que permita las direcciones que se deben traducir. `Router(config)#access-list access-list-number permit source [source-wildcard]`	Ingrese el comando global `no access-list access-list-number` para eliminar la lista de acceso.
3	Establezca la traducción dinámica de origen; para hacerlo, especifique la lista de acceso definida en el paso anterior. `Router(config)#ip nat inside source list access-list-number pool name`	Ingrese el comando global `no ip nat inside source` para eliminar la traducción dinámica de origen.
4	Especifique la interfaz interna. `Router(config)#interface type number`	Ingrese el comando `interface`. El indicador de CLI cambiará de `(config)#` a `(config-if)#`.
5	Marque la interfaz como conectada al interior. `Router(config-if)#ip nat inside`	
6	Especifique la interfaz externa. `Router(config)#interface type number`	
7	Marque la interfaz como conectada al exterior. `Router(config-if)#ip nat outside`	
8	Salga del modo de configuración de interfaz. `Router(config-if)# exit`	

Comandos Ejemplo

7.2.6 Configuración de la sobrecarga de NAT

Configuración de la sobrecarga de NAT para una única dirección IP pública

Hay dos maneras posibles de configurar la sobrecarga, según la manera en la que el ISP asigne las direcciones IP públicas. En el primero de los casos, el ISP asigna una dirección IP pública a la organización, mientras que en el segundo, asigna más de una dirección IP pública.

La figura muestra los pasos a seguir para configurar la sobrecarga de NAT con una única dirección IP. Con una única dirección IP pública, la configuración con sobrecarga normalmente asigna esa dirección pública a la interfaz externa que se conecta con el ISP. Todas las direcciones internas se traducen a la única dirección IP al abandonar la interfaz externa.

Haga clic en el botón Comandos en la figura para ver los pasos de la configuración de la sobrecarga de NAT.

La configuración es similar a la de NAT dinámica, excepto que en lugar de haber un conjunto de direcciones,se utiliza la palabra clave **interface** para identificar la dirección IP externa. Esto significa que no se define un conjunto de NAT. La palabra clave **overload** permite el agregar el número de puerto a la traducción.

Haga clic en el botón Ejemplo en la figura.

Este ejemplo muestra cómo se configura la sobrecarga de NAT. En el ejemplo, todos los hosts de la red 192.168.0.0 /16 (que coinciden con ACL 1) que envían tráfico a Internet a través del router R2 se traducen a la dirección IP 209.165.200.225 (interfaz S0/1/0 dirección IP). Los flujos de tráfico se identifican por los números de los puertos porque se utilizó la palabra clave **overload**.

Ejemplo de configuración de sobrecarga de NAT

Paso	Acción	Notas
1	Defina una lista de acceso estándar que permita las direcciones que se deben traducir. `Router(config)#access-list acl-number permit source [source-wildcard]`	Ingrese el comando global **`no access-list`** *`access-list-number`* para eliminar la lista de acceso.
2	Establezca la traducción dinámica de origen; para hacerlo, especifique la lista de acceso definida en el paso anterior. `Router(config)#ip nat inside source list acl-number interface interface overload`	Ingrese el comando global **`no ip nat inside source`** para eliminar la traducción dinámica de origen. La palabra clave de sobrecarga habilita PAT.

3	Especifique la interfaz interna.
	`Router(config)#interface type number`
	`Router(config-if)#ip nat inside`
		Ingrese el comando **`interface`**. El indicador de CLI cambiará de `(config)#` a `(config-if)#`.

4	Especifique la interfaz externa.
	`Router(config-if)#interface type number`
	`Router(config-if)#ip nat outside`	

Comandos Ejemplo

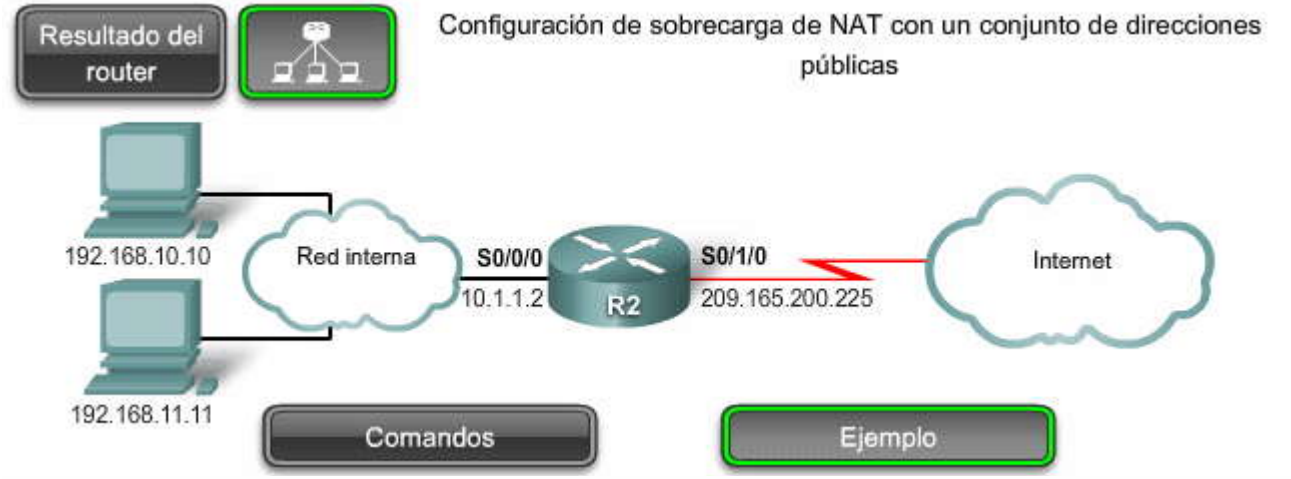
Configuración de la sobrecarga de NAT para un conjunto de direcciones IP públicas

En las situaciones en las que el ISP proporciona más de una dirección IP pública, la sobrecarga de NAT se configura para usar un conjunto de direcciones. La diferencia principal entre esta configuración y la configuración NAT dinámica uno a uno es que se utiliza la palabra clave **overload**. Recuerde que la palabra clave **overload** posibilita la traducción de la dirección del puerto.

Haga clic en el botón Comandos que se muestra en la figura para ver los pasos de la configuración de la sobrecarga de NAT con un conjunto de direcciones.

Haga clic en el botón Ejemplo en la figura.

En este ejemplo, la configuración establece la traducción con sobrecarga para el conjunto de NAT NAT-POOL2. El conjunto de NAT contiene las direcciones 209.165.200.226 a 209.165.200.240 y se traduce con PAT. Los hosts de la red 192.168.0.0 /16 se someten al proceso de traducción. Finalmente, se identifican las interfaces internas y externas.



Configuración de sobrecarga de NAT con un conjunto de direcciones públicas

Paso	Acción	Notas
1	Defina una lista de acceso estándar que permita las direcciones que se deben traducir. `Router(config)#access-list acl-number permit source [source-wildcard]`	Ingrese el comando global `no access-list access-list-number` para eliminar la lista de acceso.
2	Especifique la dirección global, como un conjunto, que se usará para la sobrecarga. `Router(config)#ip nat pool name start-ip end-ip {netmask netmask | prefix-length prefix-length}.`	
3	Establezca la traducción de sobrecarga. `Router {config} #ip nat inside source list acl-number pool name overload.`	

4	Especifique la interfaz interna.
	`Router(config)#interface type number`
	`Router(config-if)#ip nat inside`
		Ingrese el comando `interface`. El indicador de CLI cambiará de `(config)#` a `(config-if)#`.

5	Especifique la interfaz externa.
	`Router(config-if)#interface type number`
	`Router(config-if)#ip nat outside`	

Comandos Ejemplo

7.2.7 Configuración de reenvío de puertos

Reenvío de puertos

El reenvío de puertos (a veces conocido como tunneling) es el acto de reenviar un puerto de la red de un nodo de la red a otro. Esta técnica puede permitir a un usuario externo alcanzar un puerto de una dirección IP privada (perteneciente a una LAN) desde el exterior a través de un router habilitado para NAT.

Normalmente, los programas para compartir archivos y operaciones clave entre peers, por ejemplo, servidor Web y FTP de salida, requieren que los puertos del router se reenvíen o abran para permitir el funcionamiento de estas aplicaciones. Como NAT oculta las direcciones internas, las conexiones entre peers funcionan solamente desde el interior hacia afuera, ya que NAT puede asignar las solicitudes de salida contra las respuestas entrantes.

El problema es que NAT no permite las solicitudes iniciadas desde el exterior. Esta situación se puede resolver con intervención manual. El reenvío de puertos le permite identificar puertos específicos que se pueden reenviar a hosts internos.

Recuerde que las aplicaciones de software de Internet interactúan con los puertos de los usuarios que deben estar abiertos o disponibles para esas aplicaciones. Diferentes aplicaciones utilizan diferentes puertos. Por ejemplo, Telnet utiliza el puerto 23, FTP utiliza los puertos 20 y 21, HTTP el puerto 80 y SMTP el puerto 25. Esto hace que las aplicaciones y los routers puedan predecir e identificar los servicios de red. Por ejemplo, HTTP opera a través del puerto conocido 80. Al escribir la dirección http://cisco.com, el explorador muestra el sitio Web de Cisco Systems, Inc. Observeque no es necesario especificar el número de puerto de HTTP para las solicitudes de páginas porque la aplicación supone que es el puerto 80.

Configuración de reenvío de puertos

El reenvío de puertos permite a los usuarios de Internet tener acceso a servidores internos mediante el uso de la dirección del puerto WAN y el número de puerto externo correspondiente. Cuando los usuarios envían este tipo de solicitudes a la dirección del puerto WAN a través de Internet, el router reenvía las solicitudes a los servidores correspondientes de la LAN. Por cuestiones de seguridad, los routers de banda ancha no permiten, de forma predeterminada, el reenvío de ninguna solicitud de red externa a un host interno.

Por ejemplo, la figura muestra la ventana de reenvío de un único puerto de un router SOHO Linksys WVRS4400N para empresas. El reenvío de puertos no está configurado.

Haga clic en el botón Ejemplo de reenvío de puertos que se muestra en la figura.

Se puede habilitar el reenvío de puertos para aplicaciones y especificar la dirección local interna a la que se deben reenviar las solicitudes. Por ejemplo, en la figura, las solicitudes de servicio HTTP que llegan a este router Linksys ahora se reenvían al servidor Web que tiene la dirección local interna 192.168.1.254. Si la dirección IP WAN externa del router SOHO es 209.165.200.158, el usuario externo podría escribir http://209.165.202.158 y el router Linksys redireccionaría la solicitud HTTP al servidor Web interno que tiene la dirección IP 192.168.1.254 a través del número de puerto predeterminado 80.

Se podría especificar un puerto que no sea el puerto predeterminado 80. Sin embargo, el usuario externo debería saber qué número específico de puerto utilizar.

El enfoque que se siga para configurar el reenvío de puertos depende de la marca y el modelo del router de banda ancha que utilice la red. No obstante, hay algunos pasos generales que se deben seguir. Si las instrucciones proporcionadas por el ISP o incluidas con el router no proporcionan una orientación adecuada, el sitio Web www.portforward.com brinda guías para varios routers de banda ancha. Puede seguir las instrucciones para agregar o eliminar puertos según sea necesario para satisfacer las necesidades de las aplicaciones que desee permitir o denegar.

Reenvío de puertos

Reenvío de puertos

7.2.8 Verificación y resolución de problemas de configuraciones NAT

Verificación de NAT y de la sobrecarga de NAT

Es importante verificar el funcionamiento de NAT. Hay varios comandos de router útiles para ver y eliminar traducciones NAT. Este tema explica cómo verificar el funcionamiento de NAT con las herramientas disponibles en los routers Cisco.

Uno de los comandos más útiles para verificar el funcionamiento de NAT es el comando **show ip nat translations**. Antes de usar los comandos **show** para verificar NAT, debe eliminar todas las entradas de traducción dinámica que pueda haber, porque las traducciones de direcciones dinámicas, de forma predeterminada, expiran y se eliminan de la tabla de traducción NAT después de un período sin utilizarse.

En la figura, el router R2 se configuró para proporcionar la sobrecarga de NAT a los clientes 192.168.0.0 /16. Cuando los hosts internos salen a Internet a través del router R2, se traducen a la dirección IP de la interfaz serial con un número de puerto de origen único.

Supongamos que los dos hosts de la red interna se conectan a servicios Web de Internet.

Haga clic en el botón Traducciones NAT que se muestra en la figura.

Observe que el resultado del comando **show ip nat translations** muestra los detalles de las dos asignaciones NAT. Si agrega **verbose** al comando, se muestra información adicional acerca de cada traducción, incluida la antigüedad y el uso de la entrada.

El comando muestra todas las traducciones estáticas que se configuraron y todas las traducciones dinámicas que creó el tráfico. Cada traducción se identifica por protocolo además de las direcciones internas y externas locales y globales.
Haga clic en el botón Estadísticas de NAT que se muestra en la figura.

El comando **show ip nat statistics** muestra información acerca de la cantidad total de traducciones activas, los parámetros de configuración de NAT, la cantidad de direcciones que hay en el conjunto y la cantidad de direcciones que se asignaron.

En la figura, los hosts iniciaron tráfico Web y tráfico ICMP.

Otra alternativa es utilizar el comando **show run** y buscar los comandos de NAT, lista de control de acceso, interfaz o conjunto con los valores requeridos. Examínelos atentamente y corrija los errores que observe.

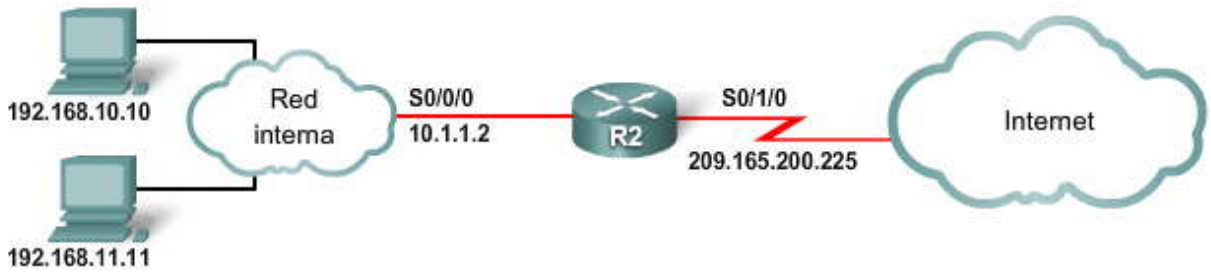
De forma predeterminada, las entradas de traducción expiran después de 24 horas a menos que se haya modificado la configuración de los temporizadores con el comando **ip nat translation timeout***timeout_ seconds* en el modo de configuración global.
Haga clic en el botón NAT eliminada que se muestra en la figura.

A veces resulta útil eliminar las entradas dinámicas antes de que se cumpla el tiempo predeterminado. Esto es particularmente válido cuando se está probando la configuración de NAT. Para eliminar las entradas dinámicas antes de que hayan expirado, use el comando global **clear ip nat translation**.

La tabla de la figura muestra las diferentes maneras en las que se pueden eliminar traducciones NAT. Puede indicar de manera muy específica qué traducciones eliminar o puede eliminar todas las traducciones de la tabla con el comando global **clear ip nat translation ***, como se muestra en el ejemplo.

Sólo se eliminan las traducciones dinámicas de la tabla. Las traducciones estáticas no se pueden eliminar de la tabla de traducciones.

Ejemplo de configuración de sobrecarga de NAT




```
access-list 1 permit 192.168.0.0 0.0.255.255
ip nat inside source list 1 interface serial 0/1/0 overload
interface serial 0/0/0
  ip nat inside
interface serial 0/1/0
  ip nat outside
```

Sobrecarga de NAT | Traducciones NAT | Estadísticas NAT | NAT eliminada

Ejemplo de traducciones NAT

```
R2#show ip nat translations
Pro Inside global          Inside local          Outside local         Outside global
tcp 209.165.200.225:16642  192.168.10.10:16642   209.165.200.254:80    209.165.200.254:80
tcp 209.165.200.225:62452  192.168.11.10:62452   209.165.200.254:80    209.165.200.254:80

R2#show ip nat translations verbose
Pro Inside global          Inside local          Outside local         Outside global
tcp 209.165.200.225:16642  192.168.10.10:16642   209.165.200.254:80    209.165.200.254:80
    create 00:01:45, use 00:01:43 timeout:86400000, left 23:58:16, Map-Id(In): 1,
    flags:
extended, use_count: 0, entry-id: 4, lc_entries: 0
tcp 209.165.200.225:62452  192.168.11.10:62452   209.165.200.254:80    209.165.200.254:80
    create 00:00:37, use 00:00:35 timeout:86400000, left 23:59:24, Map-Id(In): 1,
    flags:
extended, use_count: 0, entry-id: 5, lc_entries: 0
R2#
```

Sobrecarga de NAT | Traducciones NAT | Estadísticas NAT | NAT eliminada

Ejemplo de traducciones NAT

```
R2#show ip nat translations
Pro Inside global          Inside local          Outside local         Outside global
icmp 209.165.200.225:3     192.168.10.10:3       209.165.200.254:3     209.165.200.254:3
tcp  209.165.200.225:11679 192.168.10.10:11679   209.165.200.254:80    209.165.200.254:80
icmp 209.165.200.225:0     192.168.11.10:0       209.165.200.254:0     209.165.200.254:0
tcp  209.165.200.225:14462 192.168.11.10:14462   209.165.200.254:80    209.165.200.254:80

R2#show ip nat statistics
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Outside interfaces:
  Serial0/1/0
Inside interfaces:
  Serial0/0/0, Serial0/0/1
Hits: 173  Misses: 9
CEF Translated packets: 182, CEF Punted packets: 0
Expired translations: 6
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 interface Serial0/1/0 refcount 3
Queued Packets: 0
R2#
```

Sobrecarga de NAT | Traducciones NAT | **Estadísticas NAT** | NAT eliminada

Despejar traducciones NAT

```
R2#clear ip nat translation *
R2#show ip nat translations

R2#
```

Comando	Descripción
clear ip nat translation *	Elimina todas las entradas de traducción de direcciones dinámicas de la tabla de traducción NAT
clear ip nat translation inside *global-ip local-ip* [**outside** *local-ip global-ip*]	Elimina una simple entrada de traducción dinámica que contiene una traducción interna o ambas traducciones, interna y externa
clear ip nat translation *protocol* **inside** *global-ip global-port local-ip local-port* [**outside** *local-ip local-port global-ip global-port*]	Elimina una entrada ampliada de traducción dinámica

Sobrecarga de NAT | Traducciones NAT | Estadísticas NAT | **NAT eliminada**

Resolución de problemas de configuración de NAT y de la sobrecarga de NAT

Cuando tiene problemas de conectividad IP en un entorno NAT, muchas veces resulta difícil determinar la causa del problema. El primer paso para resolver el problema es descartar que la causa sea la NAT. Siga estos pasos para verificar que la NAT esté funcionando según lo esperado:

Paso 1. Según la configuración, defina con claridad lo que la NAT debe lograr. De esta manera puede detectar si hay problemas con la configuración.

Paso 2. Verifique que haya traducciones correctas en la tabla de traducciones con el comando **show ip nat translations**.

Paso 3. Use los comandos **clear** y **debug** para verificar que la NAT esté operando correctamente. Verifique si después de eliminar las entradas dinámicas se vuelven a crear.

Paso 4. Revise detalladamente lo que le está pasando al paquete y verifique que los routers tengan la información de enrutamiento correcta para enviar el paquete.

Utilice el comando **debug ip nat** para verificar el funcionamiento de la NAT mediante la visualización de la información de cada paquete que el router traduce. El comando **debug ip nat detailed** genera una descripción de cada paquete considerado para su traducción. Este comando también muestra información sobre ciertos errores o condiciones de excepción, como la imposibilidad de asignar una dirección global.

La figura muestra un resultado modelo de **debug ip nat**. En el resultado se puede ver que el host interno 192.168.10.10 inició tráfico hacia el host externo 209.165.200.254 y que se tradujo a la dirección 209.165.200.225.

Al decodificar el resultado de la depuración, observe lo que indican los siguientes símbolos y valores:

- *****: el asterisco que se encuentra al lado de la NAT indica que la traducción se está realizando en la ruta de conmutación rápida. El primer paquete de una conversación siempre es de conmutación de procesos, lo que significa que es más lento. Los otros paquetes se envían por la ruta de conmutación rápida, si existe una entrada de caché.
- **s=**: hace referencia a la dirección IP de origen.
- **a.b.c.d--->w.x.y.z**: indica que la dirección de origen a.b.c.d se traduce a w.x.y.z.
- **d=**: hace referencia a la dirección IP de destino.
- **[xxxx]**: el valor entre corchetes corresponde al número de identificación IP. Esta información puede ser útil para la depuración porque permite establecer una correlación con otros rastreos de paquetes de analizadores de protocolos.

Puede ver las siguientes demostraciones acerca de la verificación y la resolución de problemas de NAT en estos sitios:

Estudio de caso en animación Flash: se puede hacer ping al host, pero no telnet: se trata de una animación Flash que dura siete minutos y muestra por qué un dispositivo puede hacer ping a un host pero no puede hacer telnet: http://www.cisco.com/warp/public/556/index.swf.

Estudio de caso en animación Flash: no se puede hacer ping después de NAT: se trata de una animación Flash que dura diez minutos y muestra por qué un dispositivo no puede hacer ping más allá del punto de NAT: http://www.cisco.com/warp/public/556/TS_NATcase2/index.swf.

Depurar traducciones NAT

```
R2# debug ip nat
IP NAT debugging is on
R2#
*Oct  6 19:55:31.579: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14434]
*Oct  6 19:55:31.595: NAT*: s=209.165.200.254, d=209.165.200.225->192.168.10.10 [6334]
*Oct  6 19:55:31.611: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14435]
*Oct  6 19:55:31.619: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14436]
*Oct  6 19:55:31.627: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14437]
*Oct  6 19:55:31.631: NAT*: s=209.165.200.254, d=209.165.200.225->192.168.10.10 [6335]
*Oct  6 19:55:31.643: NAT*: s=209.165.200.254, d=209.165.200.225->192.168.10.10 [6336]
*Oct  6 19:55:31.647: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14438]
*Oct  6 19:55:31.651: NAT*: s=209.165.200.254, d=209.165.200.225->192.168.10.10 [6337]
*Oct  6 19:55:31.655: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14439]
*Oct  6 19:55:31.659: NAT*: s=209.165.200.254, d=209.165.200.225->192.168.10.10 [6338]

<Output omitted>
```

La NAT traduce direcciones internas, privadas y no enrutables a direcciones públicas enrutables. La NAT tiene el beneficio adicional de proporcionar un nivel de privacidad y seguridad a la red porque oculta las direcciones IP internas de las redes externas. En esta actividad, configurará NAT dinámica y estática.
Se proporcionan instrucciones detalladas dentro de la actividad y en el siguiente enlace al PDF.
Instrucciones de las actividades (PDF)

7.3 IPv6

7.3.1 Motivos para utilizar IPv6

Por qué se necesita más espacio de direcciones

Para comprender los problemas de direccionamiento IP que enfrentan los administradores de red en la actualidad, hay que tener en cuenta que el espacio de direcciones de IPv4 proporciona aproximadamente 4294 967 296 direcciones únicas. De éstas, sólo es posible asignar 3700 millones de direcciones porque el sistema de direccionamiento IPv4 separa las direcciones en clases y reserva direcciones para multicast, pruebas y otros usos específicos.

A partir de cifras muy recientes dadas a conocer en enero de 2007, aproximadamente 2400 millones de las direcciones IPv4 disponibles ya están asignadas a usuarios finales o ISP. Esto deja unas 1300 millones de direcciones disponibles del espacio de direcciones IPv4. Si bien parece ser una cifra importante, el espacio de direcciones IPv4 se está agotando.

Haga clic en el botón Reproducir que se muestra en la figura para ver con qué rapidez ocurrió esto en los últimos 14 años.

En la última década, la comunidad de Internet ha analizado el problema del agotamiento de las direcciones IPv4 y se han publicado enormes cantidades de informes. Algunos de ellos predicen que las direcciones IPv4 se agotarán para el año 2010, otros dicen que esto no ocurrirá hasta el 2013.

Haga clic en el botón Reducción que se muestra en la figura para ver cómo se está encogiendo el espacio de direcciones disponibles.

El crecimiento de Internet, acompañado por una capacidad informática en crecimiento, ha extendido el alcance de las aplicaciones basadas en IP.

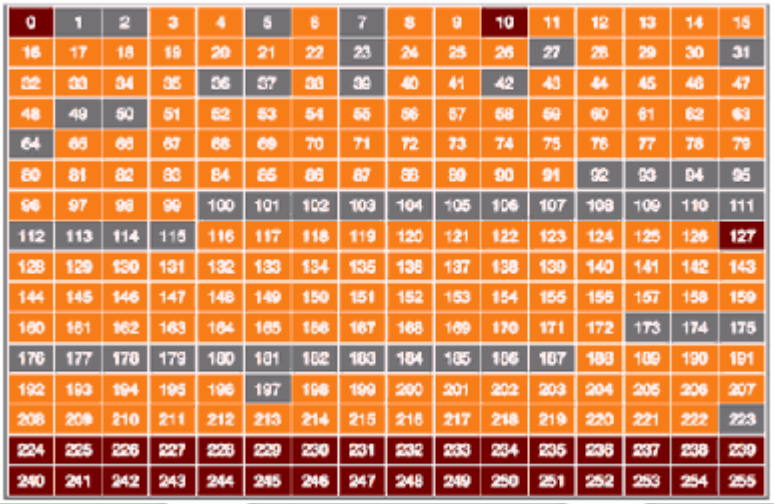
Haga clic en el botón ¿Por qué IPv6? que se muestra en la figura y considere los hechos que están forzando la adopción de IPv6.

El conjunto de números se está reduciendo por los siguientes motivos:

- **Crecimiento de la población**: la población de Internet está creciendo. En noviembre de 2005, Cisco estimó que había aproximadamente 973 millones de usuarios. Desde entonces, esta cifra se ha duplicado. Además, los usuarios permanecen conectados durante más tiempo, lo que hace que reserven direcciones IP durante períodos más prolongados y se comuniquen con una cantidad creciente de peers cada día.
- **Usuarios móviles**: la industria ha colocado más de mil millones de teléfonos móviles. Se han vendido más de 20 millones de dispositivos móviles habilitados para IP, incluidos los asistentes digitales personales (PDA, Personal Digital Assistants), pen tablets, blocs de notas y lectores de código de barras. Cada día se conectan más dispositivos habilitados para IP. Los teléfonos antiguos no necesitaban direcciones IP, pero los nuevos sí las necesitan.
- **Transporte**: para el año 2008 habrá más de mil millones de automóviles. Los modelos más recientes están habilitados para IP, para permitir el monitoreo remoto y proporcionar mantenimiento y asistencia con rapidez. Lufthansa ya brinda conectividad a Internet en sus vuelos. Más empresas de transporte, incluido el transporte marítimo, proporcionarán servicios similares.
- **Productos electrónicos para los consumidores**: los dispositivos para el hogar permiten la supervisión remota mediante la tecnología IP. Las grabadoras de video digital (DVR, Digital Video Recorders) que descargan y actualizan guías de programas de Internet son un ejemplo. Las redes domésticas pueden conectar estos dispositivos.

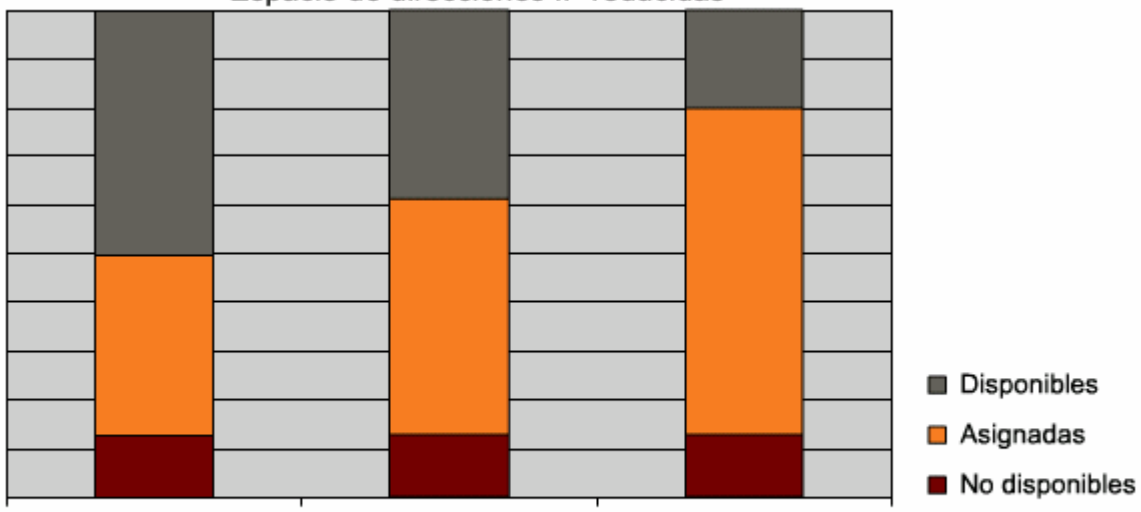
Bloques de direcciones IP asignadas

Bloques asignados: 2007

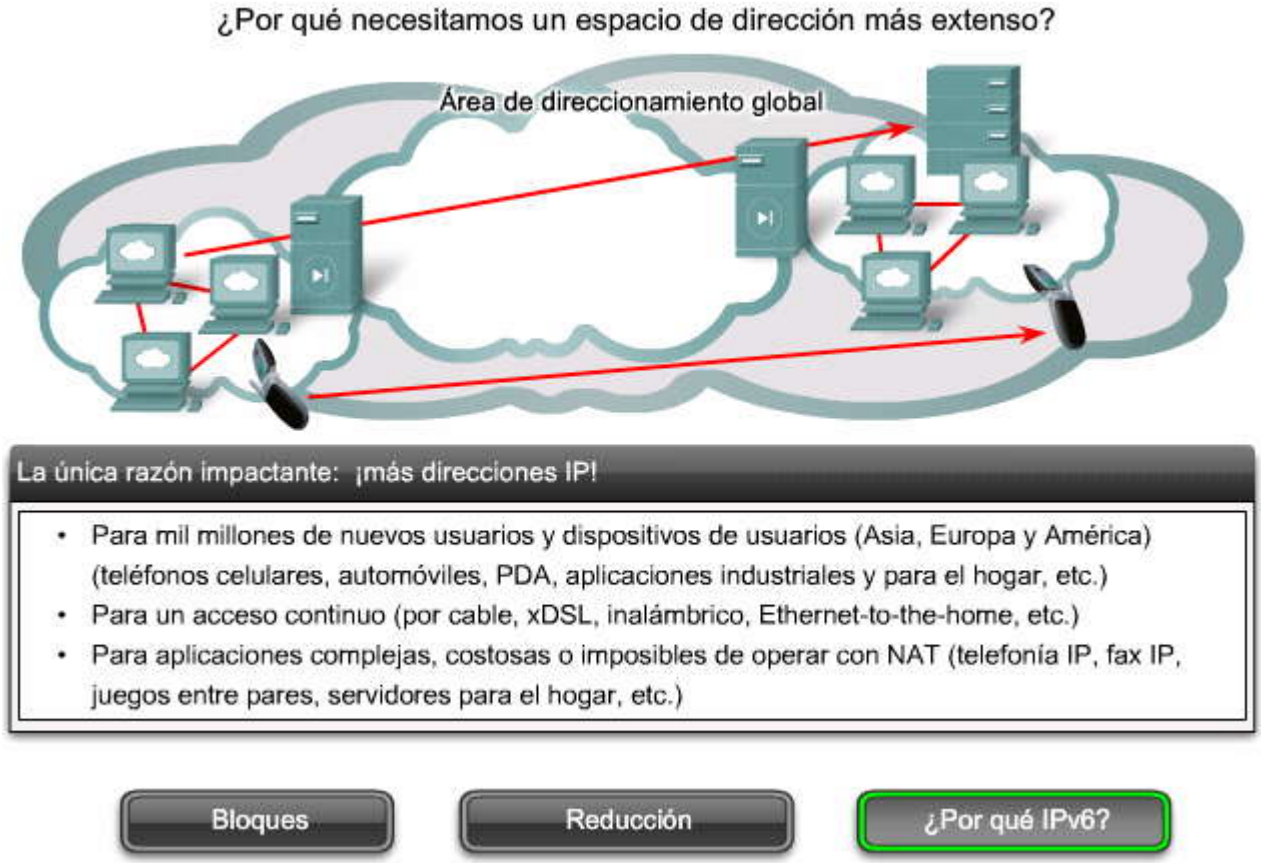


Bloques | Reducción | ¿Por qué IPv6?

Espacio de direcciones IP reducidas



Bloques | Reducción | ¿Por qué IPv6?



Motivos para usar IPv6

El movimiento para pasar de IPv4 a IPv6 ya comenzó, en particular en Europa, Japón y la región del Pacífico asiático.Estas áreas están agotando las direcciones IPv4 que tienen asignadas, lo que hace que IPv6 sea más atractivo y necesario. Japón comenzó el cambio oficialmente en el año 2000, cuando el gobierno japonés exigió la incorporación de IPv6 y estableció una fecha límite en el año 2005 para actualizar los sistemas existentes de todas las empresas del sector público. Corea, China y Malasia han lanzado iniciativas similares.

En el año 2002, el grupo de trabajo de IPv6 de la Comunidad Europea estableció una alianza estratégica para fomentar la adopción de IPv6 en todo el mundo. Se creó también el grupo de trabajo de IPv6 de América del Norte para comprometer a los mercados de América del Norte a que adopten IPv6. Los primeros avances importantes en América del Norte provienen del Departamento de Defensa (DoD, Department of Defense) de EE. UU. Con vistas a futuro y conociendo las ventajas de los dispositivos habilitados para IP, el DoD exigió ya en el año 2003 que todos los equipos que se adquirieran a partir de esa fecha no sólo estuvieran habilitados para IP sino que además fueran compatibles con IPv6. De hecho, todos los organismos del gobierno de EE. UU. deben comenzar a usar IPv6 en sus redes centrales para el año 2008 y están trabajando para cumplir con esta fecha límite.

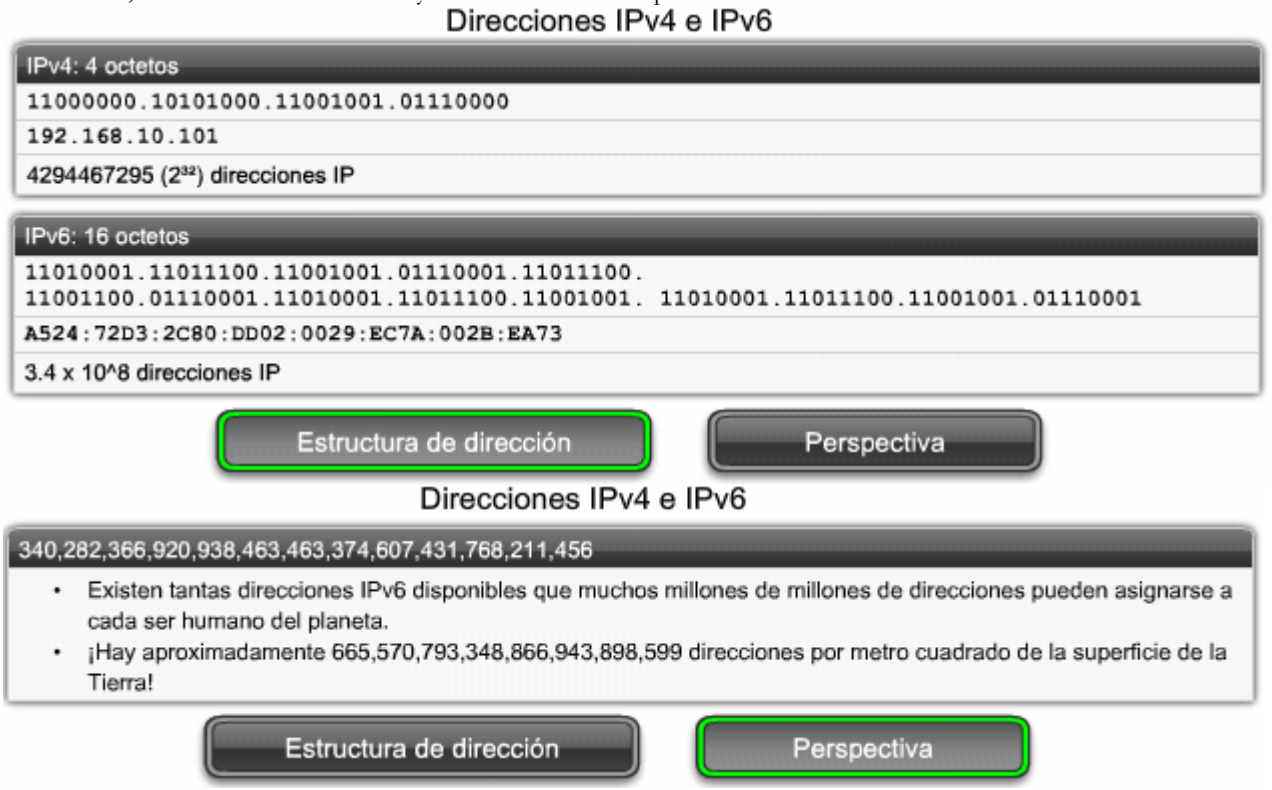
La posibilidad de expandir las redes para exigencias futuras requiere un suministro ilimitado de direcciones IP y una mayor movilidad que no se pueden satisfacer sólo con DHCP y NAT. IPv6 satisface los requisitos cada vez más complejos del direccionamiento jerárquico que IPv4 no proporciona.

Dada la enorme base instalada de IPv4 en todo el mundo, no es difícil apreciar que la transición de IPv4 a IPv6 es un desafío. Sin embargo, hay una variedad de técnicas, entre ellas una opción de configuración automática, para facilitar la transición. El mecanismo de transición que debe utilizar depende de las necesidades de su red.

La figura compara las representaciones binarias y alfanuméricas de las direcciones IPv4 e IPv6. Una dirección IPv6 es un valor binario de 128 bits, que se puede mostrar como 32 dígitos hexadecimales. IPv6 debería proporcionar una cantidad de direcciones suficiente para las necesidades de crecimiento futuras de Internet durante muchos años más. La cantidad de direcciones IPv6 disponibles permiten asignar a cada persona del planeta un espacio de direcciones de Internet equivalente al espacio total de IPv4.

Haga clic en el botón Perspectiva que se muestra en la figura.

¿Y qué ocurrió con IPv5? IPv5 se utilizó para definir un protocolo de transmisión en tiempo real experimental. Para evitar confusiones, se decidió no utilizar IPv5 y llamar IPv6 al nuevo protocolo IP.



IPv6 no existiría si no fuera por el agotamiento evidente de las direcciones IPv4 disponibles. Sin embargo, más allá del mayor espacio de direcciones IP, el desarrollo de IPv6 presentó oportunidades para aplicar lo aprendido a partir de las limitaciones de IPv4 y crear así un protocolo con funciones nuevas y mejoradas.

La mayor simplicidad de la arquitectura de encabezados y el funcionamiento del protocolo significa que se reducen los gastos operativos. Las funciones de seguridad incorporadas posibilitan prácticas de seguridad más sencillas que muchas redes actuales necesitan. Sin embargo, tal vez la mejora más importante ofrecida por IPv6 son las funciones de configuración automática de direcciones que ofrece.

Internet está evolucionando con rapidez de un conjunto de dispositivos estacionarios a una red fluida de dispositivos móviles. IPv6 permite a los dispositivos móviles adquirir direcciones y pasar de una dirección a otra con rapidez a medida que se conectan a diferentes redes externas, sin necesidad de contar con un agente externo. (Un agente externo es un router que puede funcionar como punto de conexión para un dispositivo móvil cuando éste hace roaming desde la red propia a una red externa).

La configuración automática de direcciones también significa que la conectividad en red plug-and-play es más sólida. La configuración automática admite consumidores que pueden tener una combinación indistinta de computadoras, impresoras, cámaras digitales, radios digitales, teléfonos IP, dispositivos del hogar habilitados para Internet y juguetes robóticos conectados a las redes domésticas. Muchos fabricantes ya integran IPv6 en sus productos.

Muchas de las mejoras que ofrece IPv6 se explican en esta sección, entre ellas:

- Direccionamiento IP mejorado
- Encabezado simplificado
- Movilidad y seguridad
- Intensidad de transición

Direccionamiento IP mejorado

Un espacio de direcciones más grande ofrece varias mejoras, entre ellas:

- Más posibilidad de conexión y flexibilidad global.
- Mejor agrupación de los prefijos IP anunciados en las tablas de enrutamiento.

- Hosts con múltiples conexiones. La multiconexión es una técnica para aumentar la confiabilidad de la conexión a Internet de una red IP. Con IPv6, un host puede tener varias direcciones IP a través de un enlace ascendente físico. Por ejemplo, un host puede conectarse a varios ISP.
- Configuración automática que puede incluir direcciones de capa de enlace de datos en el espacio de la dirección.
- Más opciones plug-and-play para más dispositivos.
- Redireccionamiento de extremo a extremo de público a privado sin traducción de direcciones. Esto hace que las redes entre peers (P2P) sea más funcional y fácil de implementar.
- Mecanismos simplificados para renumeración y modificación de direcciones.

Haga clic en el botón Encabezado simple que se muestra en la figura.

La figura compara la estructura de encabezado simplificada de IPv6 con la del encabezado de IPv4. El encabezado de IPv4 tiene 20 octetos y 12 campos de encabezado básicos, seguidos por un campo de opciones y una sección de datos (normalmente el segmento de la capa de transporte). El encabezado de IPv6 tiene 40 octetos, tres campos de encabezado de IPv4 básicos y cinco campos de encabezado adicionales.

El encabezado simplificado de IPv6 ofrece varias ventajas con respecto a IPv4:

- Mayor eficacia de enrutamiento para obtener mejor rendimiento y más escalabilidad de velocidad de reenvío.
- Ausencia de broadcasts, de manera que no existe peligro potencial de tormentas de broadcasts.
- No hay necesidad de procesar checksums.
- Mecanismos de encabezado de extensión más simples y eficaces.
- Rótulos de flujo en función del procesamiento de flujo sin necesidad de abrir el paquete interno de transporte para identificar los diferentes flujos de tráfico.

Mayor movilidad y seguridad

La movilidad y la seguridad ayudan a asegurar el cumplimiento con las funciones de los estándares de IP móvil y seguridad de IP (IPsec). La movilidad permite a las personas que tienen dispositivos de red móviles, muchos de ellos con conectividad inalámbrica, conectarse a diferentes redes.

- El estándar de IP móvil del IETF está disponible tanto para IPv4 como IPv6. El estándar permite que los dispositivos móviles puedan desplazarse sin que se generen interrupciones en las conexiones de red establecidas. Los dispositivos móviles utilizan una dirección propia y una dirección de respaldo para lograr esta movilidad. Con IPv4, estas direcciones se configuran de manera manual. Con IPv6 las configuraciones son dinámicas, lo que hace que los dispositivos habilitados para IPv6 tengan movilidad incorporada.
- IPsec está disponible tanto para IPv4 como IPv6. Aunque las funciones son básicamente idénticas para los dos entornos, IPsec es obligatorio en IPv6, lo que hace que Internet IPv6 sea más segura.

Intensidad de transición

IPv4 no desaparecerá de la noche a la mañana. En realidad, coexistirá durante un tiempo con IPv6 y será reemplazado gradualmente por éste. Por este motivo, IPv6 incluye técnicas de migración que abarcan cada caso de actualización de IPv4 concebible. Sin embargo, muchas de estas técnicas fueron en última instancia rechazadas por la comunidad tecnológica.

En la actualidad hay tres enfoques principales:

- Stack doble
- Tunneling 6a4
- NAT-PT, tunneling ISATAP y tunneling Teredo (métodos de último recurso)

Algunos de estos enfoques se describen en mayor detalle más adelante en este capítulo.

El consejo actual para hacer la transición a IPv6 se trata de "usar stack doble cuando pueda y tunneling cuando no tenga otra opción".

Representación de dirección IPv6

Dirección IP mejorada:
- Posibilidad de conexión y flexibilidad global
- Agregación
- Multiconexión
- Autoconfiguración
- Plug-and-play
- De extremo a extremo sin NAT
- Renumeración

Movilidad y seguridad:
- IP móvil que cumple con RFC
- IPsec obligatorio (o nativo) para IPv6

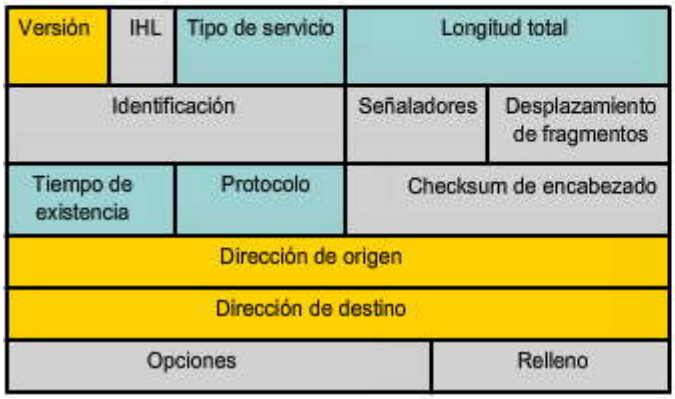
Encabezado simple:
- Eficiencia de enrutamiento
- Escalabilidad de rendimiento y velocidad de reenvío
- Sin broadcasts
- Sin checksums
- Encabezados con extensión
- Identificador de flujo

Intensidad de transición:
- Stack doble
- 6to4 y túnel manual
- Traducción

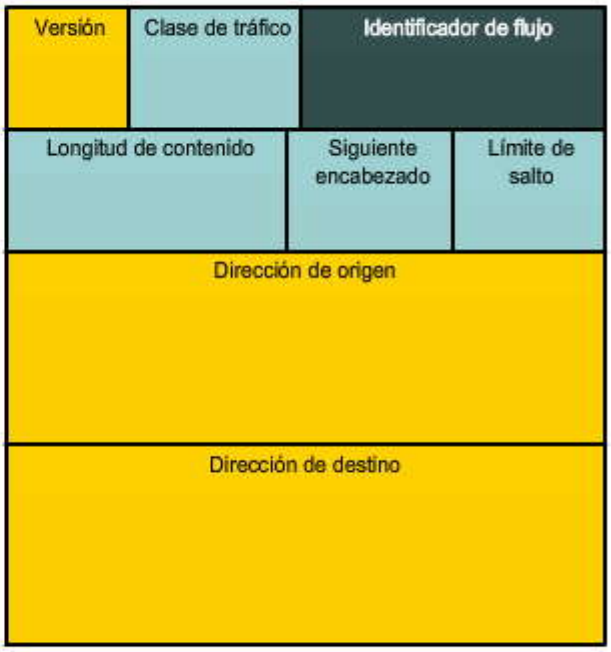
Características avanzadas | Encabezado simple

Encabezados IPv4 e IPv6

Encabezado IPv4



Encabezado IPv6



Leyenda

- Se conservan los nombres de campo de IPv4 a IPv6
- No se conservan los campos en IPv6
- Cambian el nombre y la posición en IPv6
- Nuevo campo en IPv6

Características avanzadas | Encabezado simple

Representación de direcciones IPv6

Las direcciones IPv4 conocidas tienen 32 bits representados como una serie de cuatro campos de 8 bits separados por puntos. Sin embargo, las direcciones IPv6 de 128 bits son más largas y necesitan una representación diferente a causa de su tamaño. Las direcciones IPv6 utilizan dos puntos (:) para separar entradas en una serie hexadecimal de 16 bits.

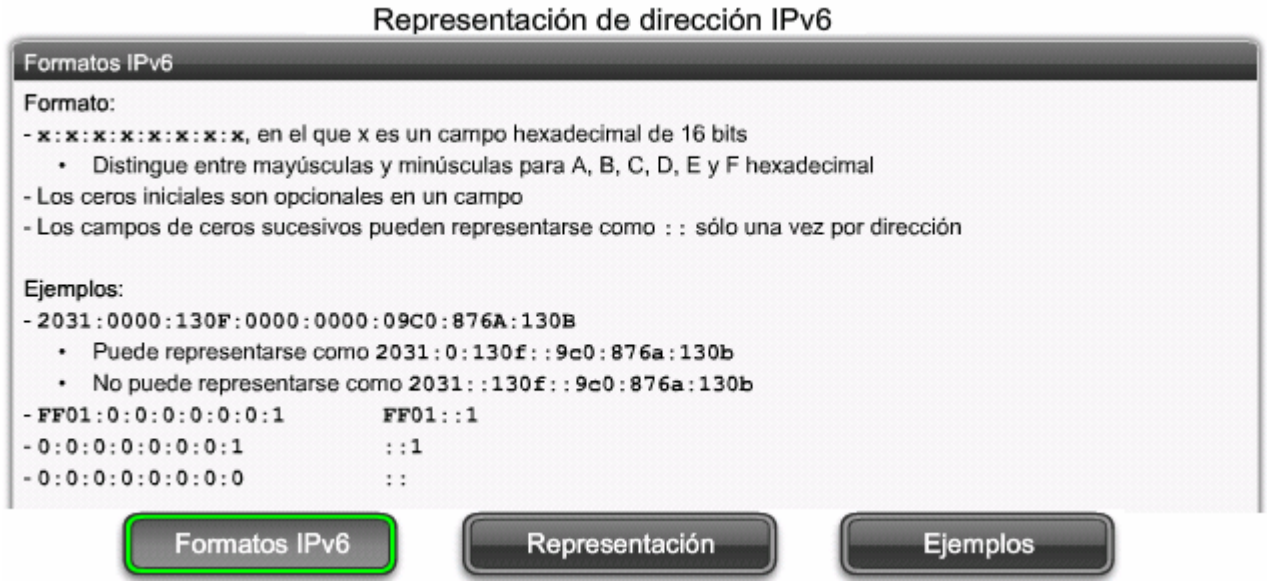
Haga clic en el botón Representación que se muestra en la figura.

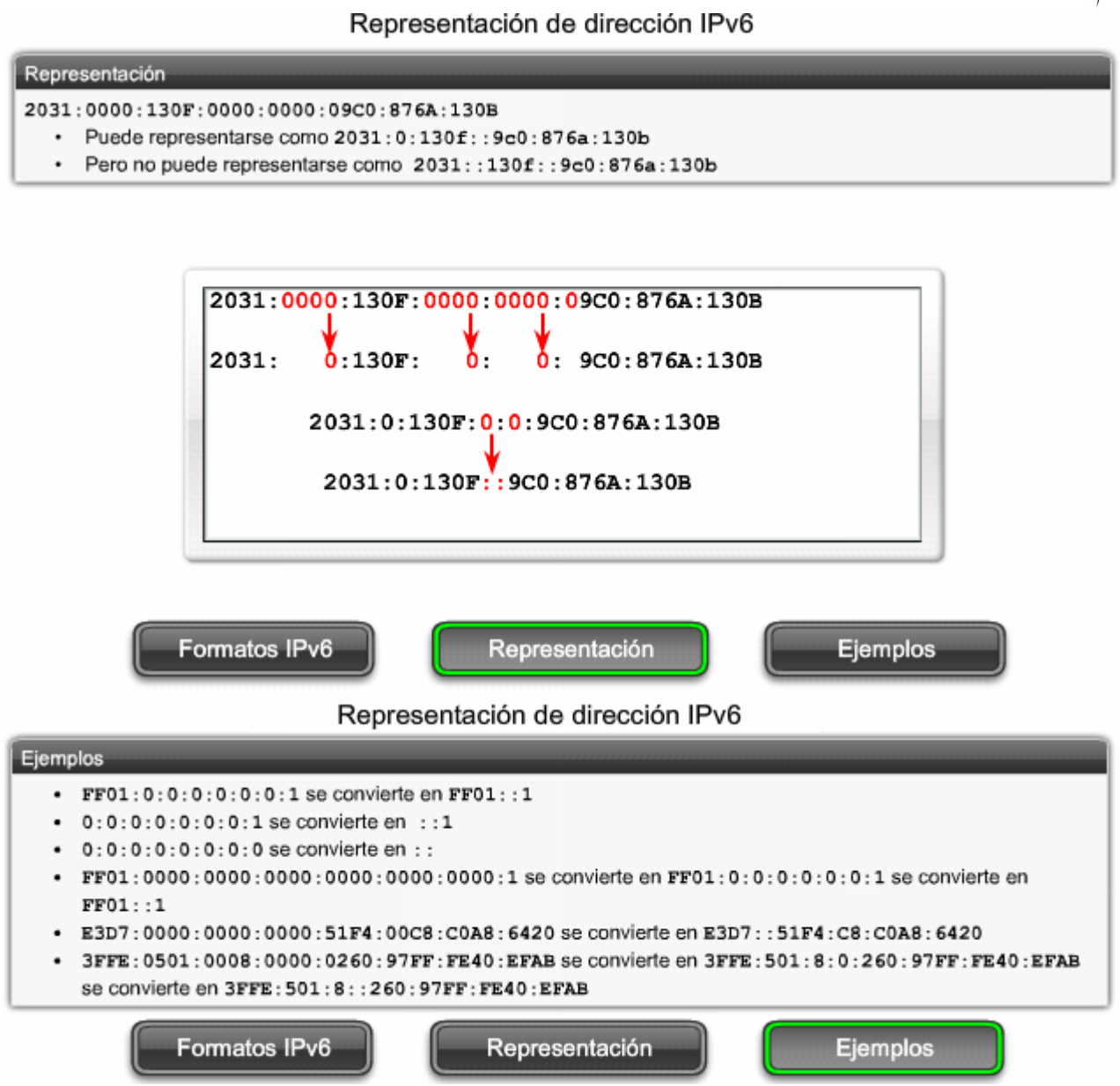
La figura muestra la dirección **2031:0000:130F:0000:0000:09C0:876A:130B**. IPv6 no requiere una notación de cadena de dirección explícita. La figura muestra cómo acortar la dirección mediante la aplicación de las siguientes pautas:

- Los ceros iniciales de los campos son opcionales. Por ejemplo, el campo 09C0 es igual a 9C0 y el campo 0000 es igual a 0. De manera que 2031:**0000**:130F:0000:0000:**09C0**:876A:130B puede escribirse como 2031:**0**:130F:0000:0000:**9C0**:876A:130B.
- Los campos sucesivos de ceros pueden representarse con doble dos puntos "::". Sin embargo, este método de abreviación sólo puede utilizarse una vez en una dirección. Por ejemplo 2031:0:130F:**0000**:**0000**:9C0:876A:130B puede escribirse como 2031:0:130F::9C0:876A:130B.
- Una dirección no especificada se escribe "::" porque sólo contiene ceros.

El uso de la notación "::" reduce en gran medida el tamaño de la mayoría de las direcciones que se muestran. Un analizador de direcciones identifica la cantidad de ceros faltantes mediante la separación de dos partes de una dirección y la adición de ceros hasta completar los 128 bits.

Haga clic en el botón Ejemplos que se muestra en la figura para ver más ejemplos.





Dirección unicast global de IPv6

IPv6 tiene un formato de direcciones que permite la agrupación ascendente hasta llegar finalmente al ISP. Las direcciones unicast globales normalmente están compuestas por un prefijo de enrutamiento global de 48 bits y un ID de subred de 16 bits. Las organizaciones individuales pueden utilizar un campo de subred de 16 bits para crear su propia jerarquía de direccionamiento local. Este campo permite a la organización utilizar hasta 65.535 subredes individuales.

En la parte superior de la figura se puede observar cómo se agrega una jerarquía adicional al prefijo de enrutamiento global de 48 bits con el prefijo del registro, el prefijo del ISP y el prefijo del sitio.

La dirección unicast global actual asignada por IANA utiliza el rango de direcciones que comienzan con el valor binario 001 (2000::/3), que es 1/8 del espacio de la dirección IPv6 y es el bloque más grande de direcciones asignadas. IANA está asignando espacio de direcciones IPv6 en los rangos de 2001::/16 a los cinco registros RIR (ARIN, RIPE, APNIC, LACNIC y AfriNIC).

Para obtener más información, consulte RFC 3587, el formato de dirección unicast global de IPv6, que reemplaza a RFC 2374.

Direcciones reservadas

IETF reserva una parte del espacio de direcciones de IPv6 para diferentes usos, tanto presentes como futuros. Las direcciones reservadas representan 1 de 256 partes del espacio total de direcciones de IPv6. Algunos de los otros tipos de direcciones IPv6 provienen de este bloque.

Direcciones privadas

Se separó un bloque de direcciones IPv6 para direcciones privadas, igual que lo que se hizo con IPv4. Estas direcciones privadas son locales solamente en un enlace o sitio en particular y, por lo tanto, nunca se enrutan fuera de la red de una empresa particular. Las direcciones privadas tienen un primer valor de octeto de "FE" en la notación hexadecimal y el siguiente dígito hexadecimal es un valor de 8 a F.

Estas direcciones se subdividen en dos tipos, según su ámbito.

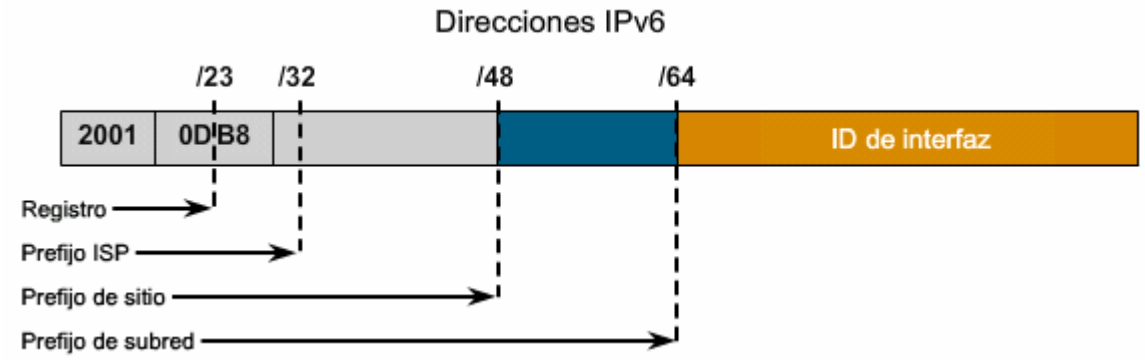
- Las **direcciones locales de un sitio** son direcciones similares a la asignación de direcciones para Internets privadas de RFC 1918 en IPv4. El ámbito de estas direcciones es un sitio o una organización completa. Sin embargo, el uso de direcciones locales de un sitio es problemático y RFC 3879 lo desaprueba desde 2003. En notación hexadecimal, las direcciones locales de un sitio comienzan con "FE" y el tercer dígito hexadecimal está entre "C" y "F". Es así como estas direcciones comienzan con "FEC", "FED", "FEE" o "FEF".
- Las **direcciones unicast de enlace local** son nuevas dentro del concepto de direccionamiento con IP en la capa de red. Estas direcciones tienen un ámbito más pequeño que las direcciones locales de un sitio, ya que hacen referencia solamente a un enlace físico en particular (red física). Los routers directamente no reenvían datagramas con direcciones link-local, ni siquiera dentro de la organización. Sólo se utilizan para comunicaciones en un segmento en particular de la red física. Se utilizan para comunicaciones de enlace, por ejemplo, configuración automática de direcciones, detección de vecinos y detección de routers. Muchos protocolos de enrutamiento IPv6 también utilizan direcciones link-local. En notación hexadecimal, las direcciones link-local comienzan con "FE" y el tercer dígito hexadecimal es un valor entre "8" y "B". Así es como estas direcciones comienzan con "FE8", "FE9", "FEA" o "FEB".

Dirección de loopback

Igual que en IPv4, se hizo una reserva de una dirección especial de loop back IPv6 para hacer pruebas: los datagramas que se envían a esta dirección regresan al dispositivo emisor y forman así un bucle de retorno o "loopback". Sin embargo, en IPv6 hay sólo una dirección y no todo un bloque para esta función. La dirección de loopback es 0:0:0:0:0:0:0:1, que normalmente se expresa mediante la compresión de ceros como "::1".

Dirección no especificada

En IPv4, una dirección IP compuesta únicamente por ceros tiene un significado especial: hace referencia al mismo host y se utiliza cuando un dispositivo no conoce su propia dirección. En IPv6, este concepto se formalizó y la dirección compuesta únicamente por ceros (0:0:0:0:0:0:0:0) se denomina dirección "no especificada". Normalmente se utiliza en el campo de origen de un datagrama que envía un dispositivo que desea configurar su dirección IP. Es posible aplicar compresión de direcciones en esta dirección, lo que la convierte simplemente en "::".



Administración de direcciones IPv6

Las direcciones IPv6 utilizan identificadores de interfaz para identificar las interfaces de un enlace. Considérelos como la porción de host de una dirección IPv6. Los identificadores de la interfaz deben ser únicos en un vínculo específico. Los identificadores de la interfaz siempre tienen 64 bits y se pueden derivar dinámicamente de una dirección de Capa 2 (MAC).

Puede asignar un ID de dirección IPv6 de manera estática o dinámica:

- Asignación estática con un ID de interfaz manual
- Asignación estática con un ID de interfaz EUI-64
- Autoconfiguración sin estado
- DHCP para IPv6 (DHCPv6)

Asignación de ID de interfaz manual

Una manera de asignar estáticamente una dirección IPv6 a un dispositivo consiste en asignar manualmente tanto el prefijo (red) como la porción del ID de la interfaz (host) de la dirección IPv6. Para configurar una dirección IPv6 en una interfaz de un router Cisco, use el comando **ipv6 address** *ipv6-address/prefix-length* en el modo de configuración de la interfaz. El siguiente ejemplo muestra la asignación de una dirección IPv6 a la interfaz de un router Cisco:

RouterX(config-if)#**ipv6 address 2001:DB8:2222:7272::72/64**

Asignación de ID de interfaz EUI-64

Otra manera de asignar una dirección IPv6 consiste en configurar la porción del prefijo (red) de la dirección IPv6 y derivar la porción del ID de la interfaz (host) de la dirección MAC de Capa 2 del dispositivo, que se conoce como ID de la interfaz EUI-64.

Haga clic en el botón EUI-64 que se muestra en la figura.

El estándar EUI-64 explica cómo extender las direcciones MAC de 48 a 64 bits mediante la inserción de la porción 0xFFFE de 16 bits en el medio en el bit 24 de la dirección MAC para crear un identificador de interfaz único de 64 bits.

Para configurar una dirección IPv6 en una interfaz de un router Cisco y habilitar el procesamiento de IPv6 con EUI-64 en esa interfaz, use el comando **ipv6 address***ipv6-prefix/prefix-length***eui-64** en el modo de configuración de la interfaz. El siguiente ejemplo muestra la asignación de una dirección EUI-64 a la interfaz de un router Cisco:

RouterX(config-if)#**ipv6 address 2001:DB8:2222:7272::/64 eui-64**

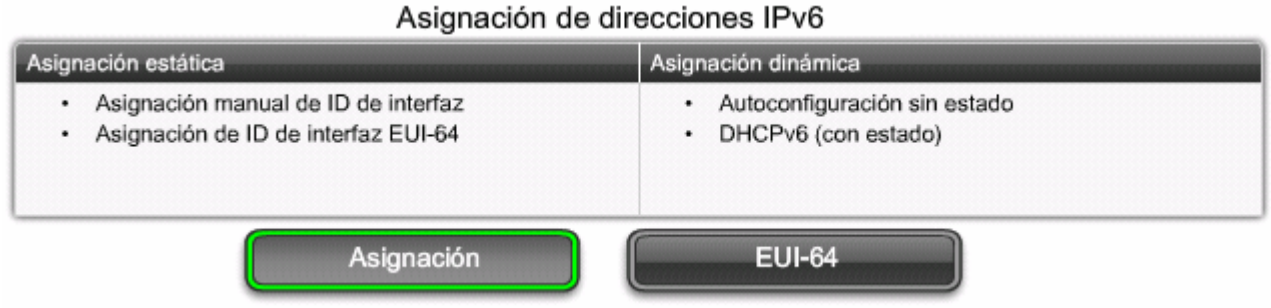
Configuración automática sin estado

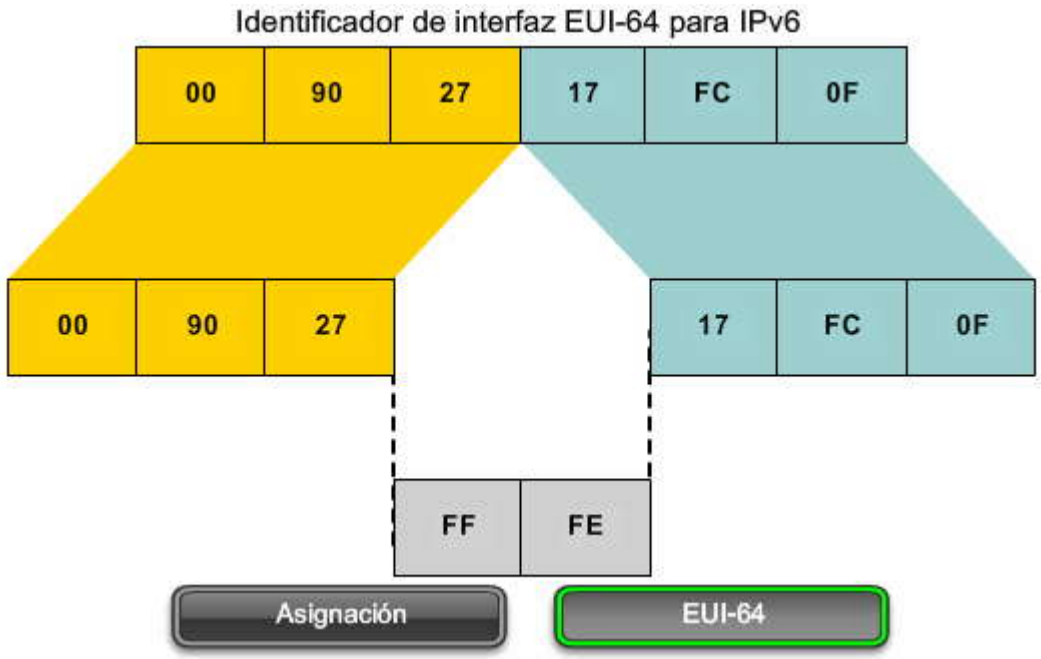
La configuración automática, como su nombre lo indica, configura automáticamente la dirección IPv6. En IPv6 se supone que los dispositivos que no son PC, así como las terminales de computadoras, están conectados a la red. El mecanismo de configuración automática se introdujo para permitir networking plug-and-play de estos dispositivos a fin de lograr la reducción de los gastos administrativos.

DHCPv6 (con estado)

DHCPv6 permite que los servidores de DHCP pasen parámetros de configuración, por ejemplo, direcciones de red IPv6, a nodos IPv6. Ofrece la capacidad de asignación automática de direcciones de red reutilizables y mayor flexibilidad de configuración. Este protocolo es una contraparte con estado de la configuración automática sin estado de direcciones IPv6 (RFC 2462) y se puede utilizar por separado o de manera concurrente con la configuración automática de direcciones IPv6 sin estado para obtener parámetros de configuración.

Para obtener más información acerca de la asignación de direcciones IPv6, visite el siguiente sitio: http://www.netbsd.org/docs/network/ipv6/.





7.3.3 Estrategias de transición a IPv6

Estrategias de transición a IPv6

La transición de IPv4 no requiere que las actualizaciones de todos los nodos sean simultáneas. Hay muchos mecanismos de transición que permiten una integración fluida de IPv4 e IPv6. Hay otros mecanismos que permiten que los nodos IPv4 se comuniquen con nodos IPv6. Para diferentes situaciones se requieren diferentes estrategias. La figura muestra la riqueza de las estrategias de transición disponibles.

Recuerde el consejo: "Use stack doble cuando pueda y tunneling cuando no tenga otra opción". Estos dos métodos son las técnicas más comunes de transición de IPv4 a IPv6.

Stack doble

El método de stack doble es un método de integración en el que un nodo tiene implementación y conectividad para redes IPv4 e IPv6. Es la opción recomendada y requiere que se ejecuten IPv4 e IPv6 simultáneamente. El router y los switches se configuran para admitir ambos protocolos; el protocolo preferido es IPv6.

Tunneling

La segunda técnica de transición más importante es el tunneling. Existen varias técnicas de tunneling, entre ellas:

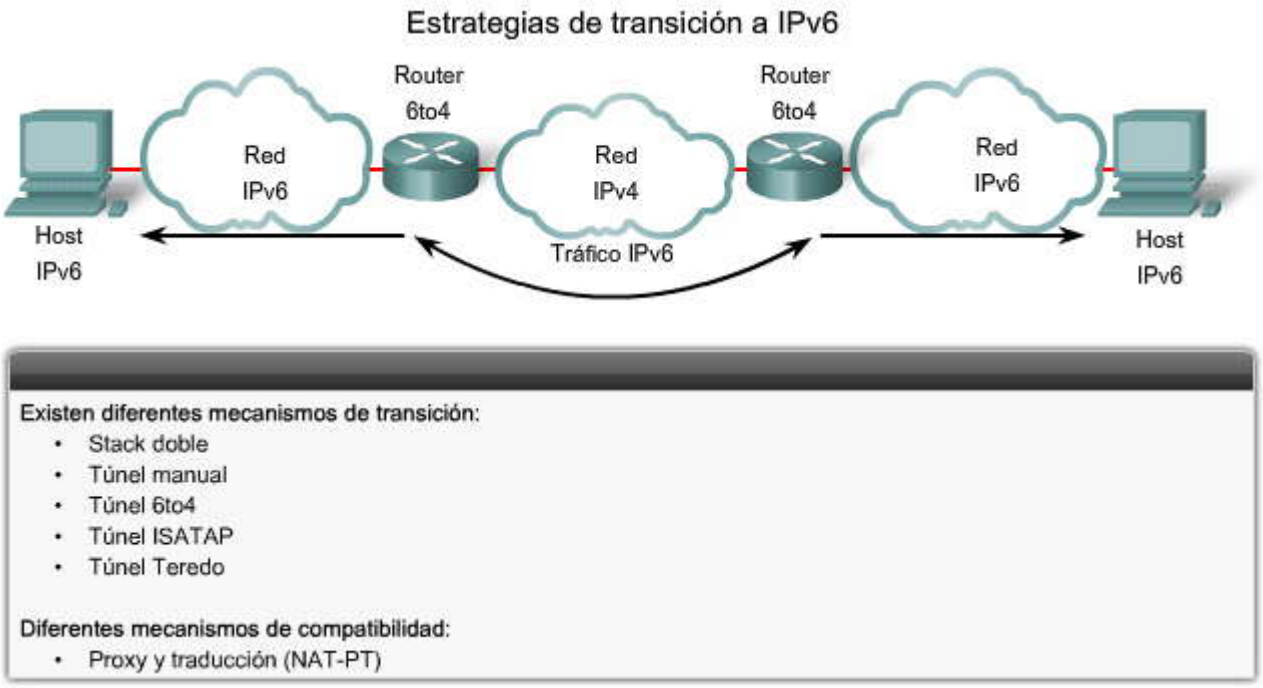
- Tunneling manual de IPv6 sobre IPv4: un paquete de IPv6 se encapsula dentro del protocolo IPv4. Este método requiere routers de stack doble.
- Tunneling dinámico 6to4: establece automáticamente la conexión de islas de IPv6 a través de la red IPv4, normalmente Internet. Aplica dinámicamente un prefijo IPv6 válido y único a cada isla de IPv6, lo que posibilita la implementación rápida de IPv6 en una red corporativa sin recuperación de direcciones de los ISP o los registros.

Otras técnicas de tunneling menos utilizadas y que están más allá del ámbito de este cursoincluyen:

- Tunneling del protocolo de direccionamiento automático de túnel dentro de un sitio (ISATAP, Intra-Site Automatic Tunnel Addressing Protocol): mecanismo de tunneling de capa superior automática que utiliza la red IPv4 subyacente como capa de enlace para IPv6. Los túneles del ISATAP permiten que los hosts de stack doble individuales IPv4 o IPv6 de un sitio se comuniquen con otros hosts similares a través de un enlace virtual y creen así una red IPv6 mediante la infraestructura IPv4.
- Tunneling Teredo: tecnología de transición a IPv6 que proporciona tunneling automático de host a host en lugar de tunneling de gateway. Este enfoque transmite tráfico IPv6 unicast si hay hosts de stack doble (hosts que ejecutan tanto IPv6 como IPv4) detrás de una o varias NAT IPv4.

Traducción de protocolos NAT (NAT-Protocol Translation, NAT-PT)

Cisco IOS Release 12.3(2)T y posteriores (con el conjunto de funciones apropiado) también incluyen NAT-PT entre IPv6 e IPv4. Esta traducción permite la comunicación directa entre hosts que utilizan versiones diferentes del protocolo IP. Estas traducciones son más complejas que IPv4 NAT. En este momento, esta técnica de traducción es la opción menos favorable y debe utilizarse como último recurso.



7.3.4 Stack doble del IOS de Cisco

Stack doble del IOS de Cisco

El método de stack doble es un método de integración que permite que un nodo tenga conectividad con redes IPv4 e IPv6 de manera simultánea. Cada nodo tiene dos stacks de protocolos con la configuración en la misma interfaz o en varias interfaces.

El enfoque de stack doble para la integración de IPv6, en el que los nodos tienen stacks de IPv4 e IPv6, será uno de los métodos de integración más comúnmente utilizados. Un nodo de stack doble elige qué stack utilizar en función de la dirección de destino del paquete. Un nodo de stack doble debe preferir utilizar IPv6 cuando esté disponible. Las aplicaciones antiguas que sólo admiten IPv4 siguen funcionando igual que antes. Las aplicaciones nuevas y las modificadas aprovechan las dos capas IP.

Se ha definido una nueva interfaz de programación de aplicaciones (API, Application Programming Interface) para admitir direcciones y solicitudes DNS de IPv4 e IPv6. Una API facilita el intercambio de mensajes o datos entre dos o más aplicaciones de software diferentes. Un ejemplo de API es la interfaz virtual entre dos funciones de software, por ejemplo, un procesador de textos y una hoja de cálculo. La API se integra en las aplicaciones de software para traducir IPv4 a IPv6 y viceversa mediante la aplicación del mecanismo de conversión IP. Las aplicaciones nuevas pueden utilizar tanto IPv4 como IPv6.

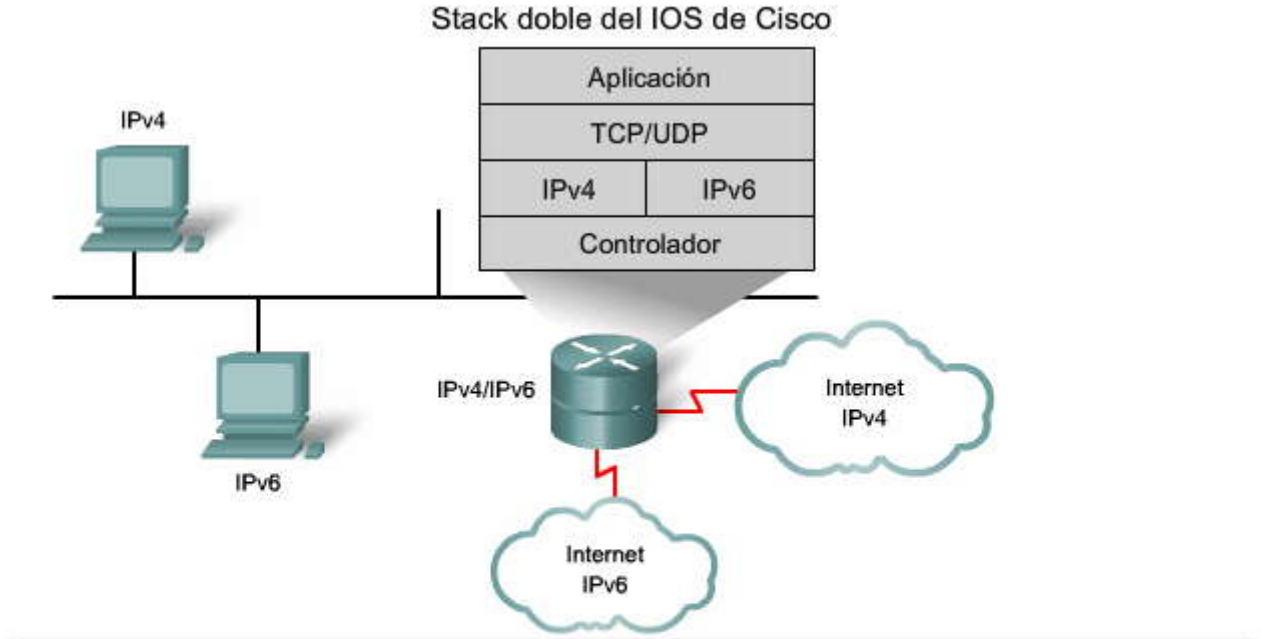
La experiencia en la conversión de aplicaciones IPv4 a IPv6 sugiere que para la mayoría de las aplicaciones hay un cambio mínimo en algunos lugares puntuales del código fuente. Esta técnica es conocida y se ha aplicado en el pasado para otras transiciones de protocolo. Permite la actualización gradual de las aplicaciones, una por una, a IPv6.

Haga clic en el botón Configuración de interfaz IPv6 que se muestra en la figura.

Cisco IOS Release 12.2(2)T y posteriores (con el conjunto de funciones apropiado) ya admiten IPv6. Tan pronto como configure IPv4 básico e IPv6 en la interfaz, la interfaz es de stack doble y reenvía el tráfico IPv4 e IPv6 en esa interfaz. Observe que se configuró una dirección IPv4 y una dirección IPv6.

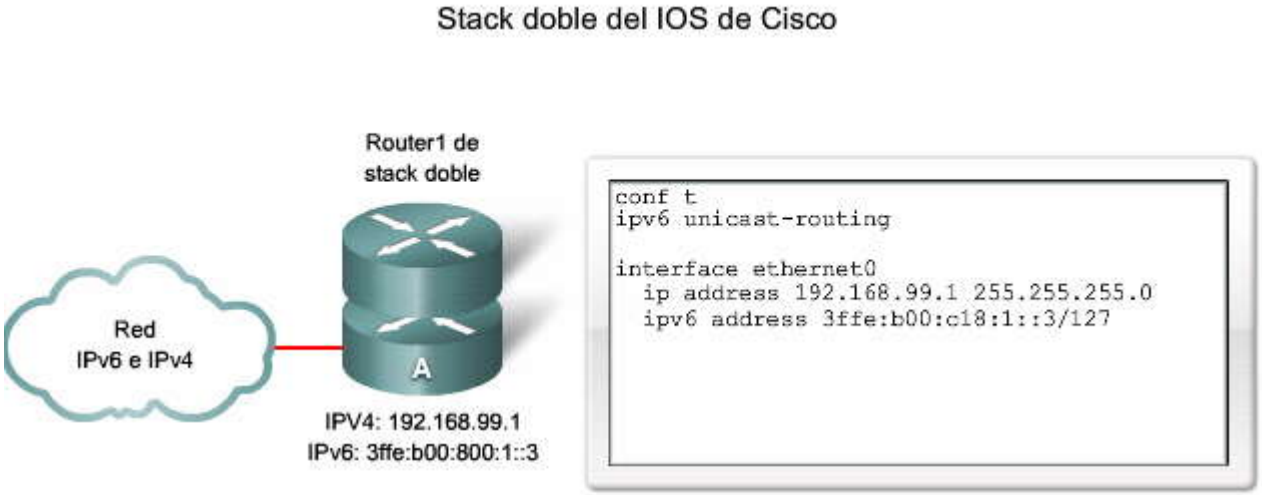
El uso de IPv6 en un router IOS de Cisco requiere el uso del comando de configuración global **ipv6 unicast-routing**. Este comando habilita el reenvío de datagramas IPv6.

Debe configurar todas las interfaces que reenvían tráfico IPv6 con una dirección IPv6 mediante el comando de interfaz **ipv6 address***IPv6-address* [/*prefix length*].



Stack doble es un método de integración en el que un nodo se implementa y conecta a una red IPv4 e IPv6.

Stack doble | Configuración de interfaz IPv6



Cuando en una interfaz se configuran tanto IPv4 como IPv6, la interfaz se considera de stack doble.

Stack doble | Configuración de interfaz IPv6

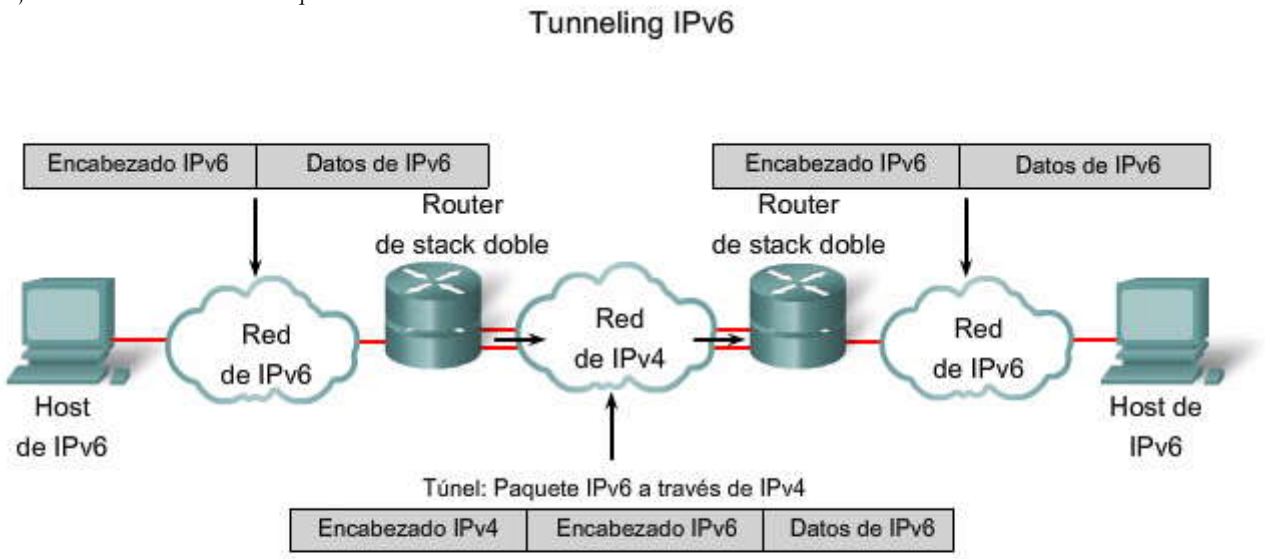
7.3.5 Tunneling IPv6

Tunneling IPv6

El tunneling es un método de integración en el que un paquete IPv6 se encapsula dentro de otro protocolo, por ejemplo, IPv4. Este método permite la conexión de islas de IPv6 sin necesidad de convertir las redes intermediarias a IPv6. Cuando se utiliza IPv4 para encapsular el paquete IPv6, se especifica el tipo de protocolo 41 en el encabezado de IPv4 y el paquete incluye un encabezado de IPv4 de 20 bytes sin opciones y un encabezado y contenido de IPv6. También requiere routers de stack doble.

El tunneling presenta estos dos problemas. La unidad máxima de transmisión (MTU, Maximum Transmission Unit) se reduce 20 octetos si el encabezado de IPv4 no contiene ningún campo opcional. Además, los problemas de las redes que utilizan tunneling normalmente son difíciles de resolver.

El tunneling es una técnica de integración y transición intermedia, y no debe considerarse como una solución definitiva. El objetivo final debe ser una arquitectura IPv6 nativa.



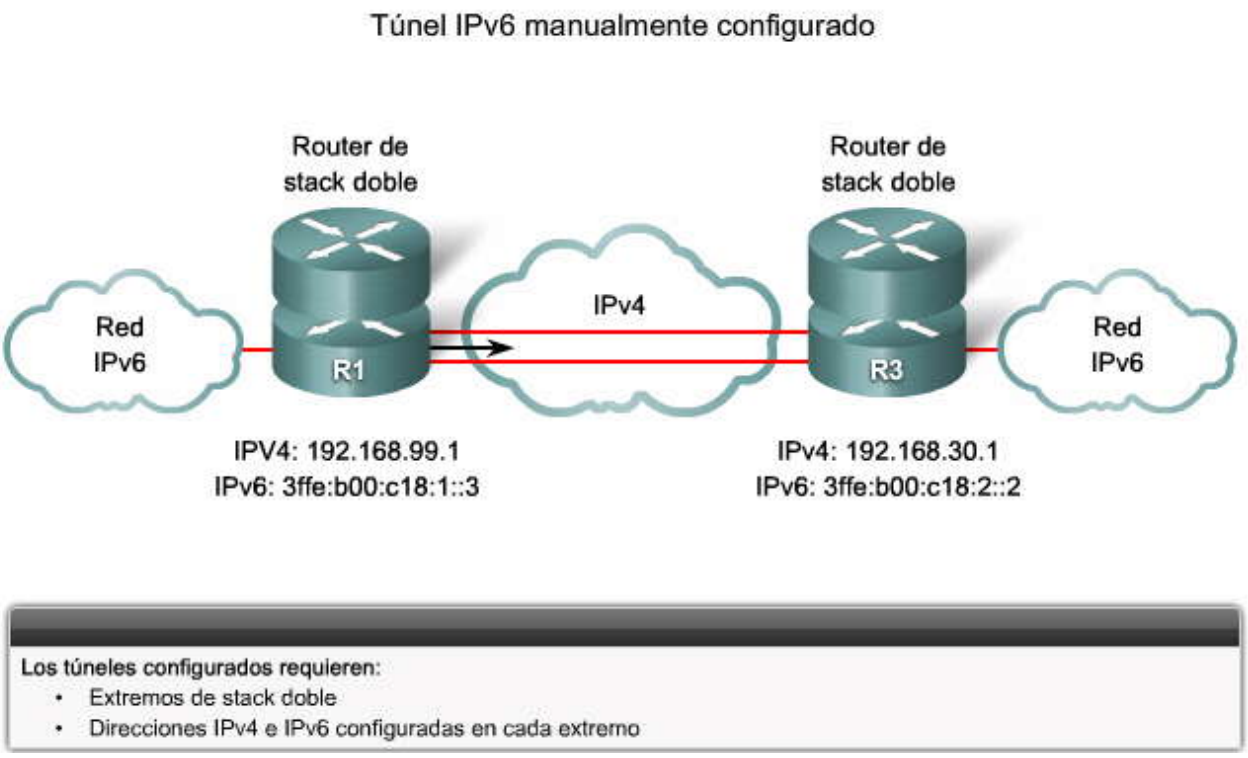
El tunneling es un método de integración en el que un paquete IPv6 se encapsula dentro de otro protocolo, como IPv4. Este método de encapsulación es IPv4:

- Incluye un encabezado IPv4 de 20 bytes sin opciones y un encabezado y contenido de IPv6
- Requiere routers de stack doble

Túnel IPv6 configurado manualmente

Un túnel configurado en forma manual equivale a un enlace permanente entre dos dominios IPv6 sobre un enlace troncal IPv4. El uso principal es para conexiones estables que requieren comunicación segura periódica entre dos routers de borde, entre un sistema final y un router de borde o para conexión con redes IPv6 remotas. Los routers de borde deben ser de stack doble y la configuración no puede cambiar dinámicamente a medida que cambian las necesidades de la red y de enrutamiento.

Los administradores configuran una dirección IPv6 estática de manera manual en una interfaz de túnel y asignan las direcciones IPv4 estáticas configuradas manualmente al origen y al destino del túnel. El host o el router de cada extremo de un túnel configurado debe admitir stacks de protocolos IPv4 e IPv6. Los túneles configurados manualmente pueden establecerse entre dos routers de borde o entre un router de borde y un host.



7.3.6 Consideraciones de enrutamiento con IPv6

Configuraciones de enrutamiento con IPv6

Al igual que el enrutamiento entre dominios sin clase (CIDR, Classless Interdomain Routing) de IPv4, IPv6 utiliza un enrutamiento de concordancia de prefijo más largo. IPv6 utiliza versiones modificadas de la mayoría de los protocolos de enrutamiento comunes para administrar las direcciones IPv6 más largas y las diferentes estructuras de encabezado.

Los espacios de dirección más grandes permiten asignaciones de direcciones grandes a los ISP y las organizaciones. Un ISP agrupa todos los prefijos de sus clientes en un único prefijo y lo anuncia en Internet IPv6. El mayor espacio de direcciones es suficiente para permitir a las organizaciones definir un único prefijo para toda su red.

¿Pero cómo se ve afectado el rendimiento del router con esto? Un breve resumen del funcionamiento de un router en una red será útil para mostrar cómo IPv6 afecta el enrutamiento. Conceptualmente, un router tiene tres áreas funcionales:

- El plano de control administra la interacción del router con los demás elementos de la red y proporciona la información necesaria para tomar decisiones y controlar el funcionamiento general del router. Este plano ejecuta procesos, tales como protocolos de enrutamiento y administración de red. Estas funciones en general son complejas.
- El plano de datos administra el reenvío de paquetes de una interfaz física o lógica a otra. Utiliza diferentes mecanismos de conmutación, por ejemplo, la conmutación de procesos y el envío express de Cisco (CEF, Cisco Express Forwarding) en routers con el software IOS de Cisco.
- Los servicios mejorados incluyen funciones avanzadas que se aplican al reenviar datos, por ejemplo, filtrado de paquetes, calidad de servicio (QoS, Quality Of Service), encriptación, traducción y contabilidad.

IPv6 presenta nuevos desafíos específicos para cada una de estas funciones.

Plano de control de IPv6

Al habilitar IPv6 en un router se inicia el proceso operativo del plano de control específicamente para IPv6. Las características del protocolo definen el rendimiento de estos procesos y la cantidad de recursos necesarios para operarlos:

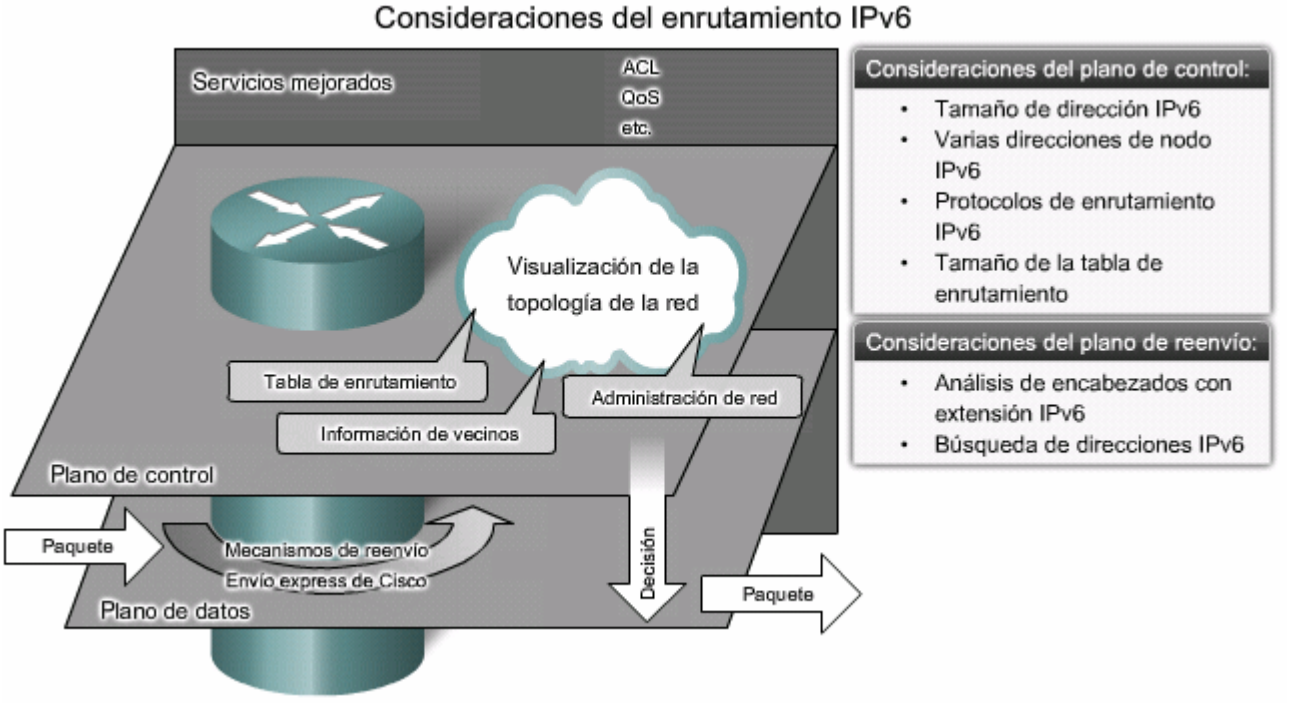
- **Tamaño de la dirección IPv6**: el tamaño de la dirección afecta las funciones de procesamiento de la información de un router. Los sistemas que utilizan una estructura de memoria, bus o CPU de 64 bits pueden transmitir una dirección IPv4 de origen y destino en un único ciclo de procesamiento. Para IPv6, las direcciones de origen y destino requieren dos ciclos cada una, o sea cuatro ciclos, para procesar la información de las direcciones de origen y destino. Como resultado, los routers que utilizan exclusivamente procesamiento de software probablemente tengan un rendimiento más lento que en un entorno IPv4.

- **Varias direcciones de nodos IPv6**: como los nodos IPv6 pueden usar varias direcciones unicast IPv6, el consumo de memoria caché para la detección de vecinos puede verse afectado.
- **Protocolos de enrutamiento IPv6**: los protocolos de enrutamiento IPv6 son similares a sus contrapartes IPv4, pero como un prefijo IPv6 es cuatro veces más grande que un prefijo IPv4, las actualizaciones de enrutamiento deben transportar más información.
- **Tamaño de la tabla de enrutamiento**: el mayor espacio de dirección IPv6 genera redes más grandes y hace que aumente mucho el tamaño de Internet. Esto hace que se necesiten tablas de enrutamiento más grandes y más requisitos de memoria para su funcionamiento.

Plano de datos IPv6

El plano de datos reenvía paquetes IP en función de las decisiones tomadas por el plano de control. El motor de reenvío analiza la información relevante del paquete IP y hace una búsqueda para establecer una equivalencia entre la información analizada y las políticas de reenvío definidas por el plano de control. IPv6 afecta el rendimiento de las funciones de análisis y búsqueda:

- **Análisis de los encabezados de extensión IPv6**: las aplicaciones, incluido IPv6 móvil, con frecuencia utilizan información de la dirección IPv6 en los encabezados de extensión, lo que hace que aumenten de tamaño. Estos campos adicionales requieren procesamiento adicional. Por ejemplo, un router que utiliza ACL para filtrar información de Capa 4 necesita aplicar las ACL tanto a los paquetes que tienen encabezados de extensión como a los que no los tienen. Si la longitud del encabezado de extensión excede la longitud fija del registro de hardware del router, la conmutación por hardware genera un error y los paquetes pueden ser derivados a conmutación por software o descartados. Esto afecta seriamente el rendimiento de reenvío del router.
- **Búsqueda de direcciones IPv6**: IPv6 realiza una búsqueda en los paquetes que ingresan al router para encontrar la interfaz de salida correcta. En IPv4, el proceso de decisión de reenvío analiza una dirección de destino de 32 bits. En IPv6, la decisión de reenvío puede requerir el análisis de una dirección de destino de 128 bits. La mayoría de los routers actuales realizan búsquedas mediante un circuito integrado de aplicación específica (ASIC, Application-Specific Integrated Circuit) con una configuración fija que realiza las funciones para las que fue diseñado originalmente: IPv4. Nuevamente, esto puede dar como resultado que los paquetes sean derivados a un procesamiento por software que es más lento o que sean descartados por completo.



Protocolo de enrutamiento RIPNg

Las rutas de IPv6 usan los mismos protocolos y las mismas técnicas que IPv4. Si bien las direcciones son más largas, los protocolos utilizados en el enrutamiento IPv6 son simplemente extensiones lógicas de los protocolos utilizados en IPv4.

RFC 2080 define el protocolo de información de routing de siguiente generación (RIPng, Routing Information Protocol Next Generation) como un protocolo de enrutamiento simple basado en RIP. RIPng no es ni más ni menos potente que

RIP, pero proporciona una manera sencilla de crear una red IPv6 sin necesidad de crear un nuevo protocolo de enrutamiento.

RIPng es un protocolo de enrutamiento vector distancia con un límite de 15 saltos que usa Actualizaciones de envenenamiento en reversa y horizonte dividido para evitar routing loops. Su simplicidad proviene del hecho de que no requiere ningún conocimiento global de la red. Sólo los routers vecinos intercambian mensajes locales.

RIPng incluye las siguientes características:

- Basado en IPv4 RIP versión 2 (RIPv2) y es similar a RIPv2
- Usa IPv6 para el transporte
- Incluye el prefijo IPv6 y la dirección IPv6 del siguiente salto
- Usa el grupo multicast FF02::9 como dirección de destino para las actualizaciones de RIP (similar a la función de broadcast que realiza RIP en IPv4)
- Envía actualizaciones por el puerto UDP 521
- Es compatible con Cisco IOS Release 12.2(2)T y posteriores

En implementaciones de stack doble, se necesitan RIP y RIPng.

Protocolo de enrutamiento RIPng

Características similares a IPv4:
- Vector distancia, radio de 15 saltos, horizonte dividido y envenenamiento en reversa
- Basado en RIPv2

Características actualizadas para IPv6:
- Prefijo IPv6, dirección IPv6 de siguiente salto
- Utiliza el grupo multicast FF02::9, el grupo multicast all-rip-routers, como la dirección de destino para las actualizaciones RIP
- Usa IPv6 para transporte
- RIPng designado

7.3.7 Configuración de direcciones IPv6

Habilitación de IPv6 en routers Cisco

Hay dos pasos básicos para activar IPv6 en un router. Primero, debe activar el reenvío de tráfico IPv6 en el router y, a continuación, debe configurar cada una de las interfaces que requiere IPv6.

De forma predeterminada, el reenvío de tráfico IPv6 está deshabilitado en los routers Cisco. Para activarlo entre interfaces, debe configurar el comando global **ipv6 unicast-routing**.

El comando **ipv6 address** puede configurar una dirección IPv6 global. La dirección link-local se configura automáticamente cuando se asigna una dirección a la interfaz. Debe especificar la dirección IPv6 completa de 128 bits o debe especificar el uso de un prefijo de 64 bits con la opción **eui-64**.

Habilitación de IPv6 en routers Cisco

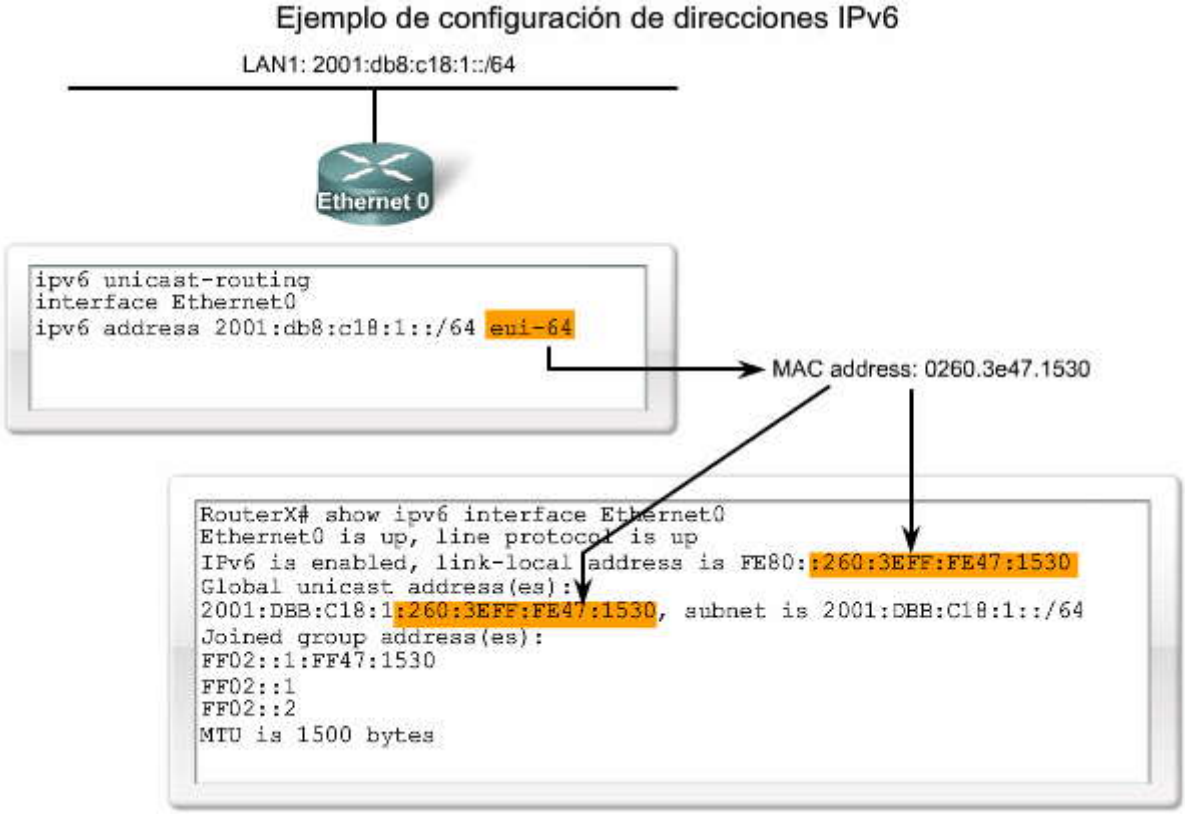
Comando	Propósito
`RouterX(config)# ipv6 unicast-routing`	Habilita el reenvío de tráfico IPv6
`RouterX(config-if)# ipv6 address ipv6prefix/prefix-length eui-64`	Configura las direcciones IPv6 de la interfaz

Ejemplo de configuración de dirección IPv6

Puede especificar la dirección IPv6 por completo o calcular el identificador del host (los 64 bits del extremo derecho) a partir del identificador EUI-64 de la interfaz. En el ejemplo, la dirección IPv6 de la interfaz se configuró con el formato EUI-64.

De manera alternativa, puede especificar la dirección IPv6 completa de la interfaz de un router con el comando **ipv6 address** *ipv6-address/prefix-length* en el modo de configuración de la interfaz.

La configuración de una dirección IPv6 en una interfaz configura automáticamente la dirección link-local para esa interfaz.



Resolución de nombres IPv6 de IOS de Cisco

Hay dos maneras de realizar la resolución de nombres desde el proceso de software IOS de Cisco:

- Definición de un nombre estático para una dirección IPv6 mediante el comando **ipv6 host name** [*port*] *ipv6-address1* [*ipv6-address2...ipv6-address4*]. Puede definir hasta cuatro direcciones IPv6 para un nombre de host. La opción del puerto hace referencia al puerto Telnet que se utilizará para el host asociado.
- Especificación del servidor DNS utilizado por el router con el comando **ip name-server** *address*. La dirección puede ser IPv4 o IPv6. Con este comando puede especificar hasta seis servidores DNS.

Resolución de nombres del IOS de Cisco para IPv6

Dos formas de efectuar la resolución de nombres del IOS de Cisco para IPv6:

Comando	Propósito
RouterX(config)# **ipv6 host** *name* [*port*] *ipv6addr* [{*ipv6addr*} ...] RouterX(config)# **ipv6 host router1 3ffe:b00:ffff:b::1**	Define un nombre estático para direcciones IPv6
RouterX(config)#**ip name-server** *address* RouterX(config)#**ip name-server 3ffe:b00:ffff:1::10**	Configura un servidor o servidores DNS para consultar

7.3.8 Configuración de RIPng con IPv6

Configuración de RIPng con IPv6

Al configurar los protocolos de enrutamiento admitidos en IPv6, debe crear el proceso de enrutamiento, habilitar el proceso de enrutamiento en las interfaces y personalizar el protocolo de enrutamiento para su red en particular.

Antes de configurar el router para que ejecute IPv6 RIP, habilite IPv6 de manera global con el comando de configuración global **ipv6 unicast-routing** y habilite IPv6 en las interfaces en las que haya que habilitar IPv6 RIP.

Para habilitar el enrutamiento RIPng en el router, use el comando de configuración global **ipv6 router rip** *name*. El parámetro *name* identifica el proceso RIP. Este nombre de proceso se utiliza más adelante al configurar RIPng en las interfaces participantes.

Para RIPng, en lugar de utilizar el comando **network** para identificar qué interfaces deben ejecutar RIPng, se utiliza el comando **ipv6 rip** *name* **enable** en el modo de configuración de la interfaz para habilitar RIPng en una interfaz. El parámetro *name* debe coincidir con el mismo parámetro en el comando **ipv6 router rip**.

La habilitación dinámica de RIP en una interfaz crea un proceso de "router rip" si es necesario.

Configuración de RIPng para IPv6

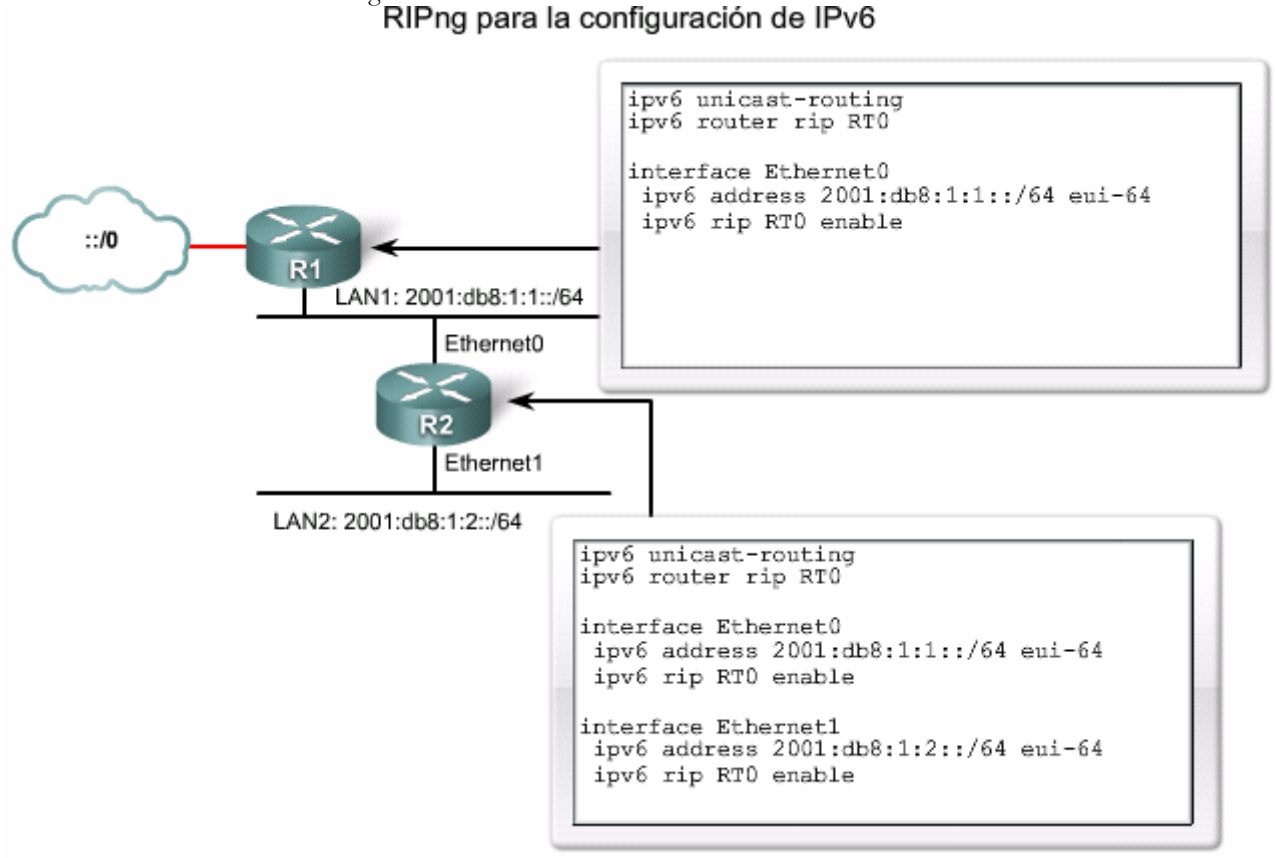
Comando	Propósito
`RouterX(config)#ipv6 router rip name`	Crea e ingresa al modo de configuración de router RIP.
`RouterX(config-if)#ipv6 rip name enable`	Configura RIP en una interfaz.

Ejemplo: RIPng para la configuración de IPv6

El ejemplo muestra una red de dos routers. El router R1 está conectado a la red predeterminada. Tanto en el router R2 como en el router R1, el nombre RT0 identifica el proceso RIPng. RIPng está habilitado en la primera interfaz Ethernet del router R1 mediante el comando **ipv6 rip RT0 enable**. El router R2 muestra que RIPng está habilitado en ambas interfaces Ethernet mediante el comando **ipv6 rip RT0 enable**.

Esta configuración permite que las interfaces Ethernet 1 del router R2 y Ethernet 0 de ambos routers intercambien información de enrutamiento RIPng.

RIPng para la configuración de IPv6



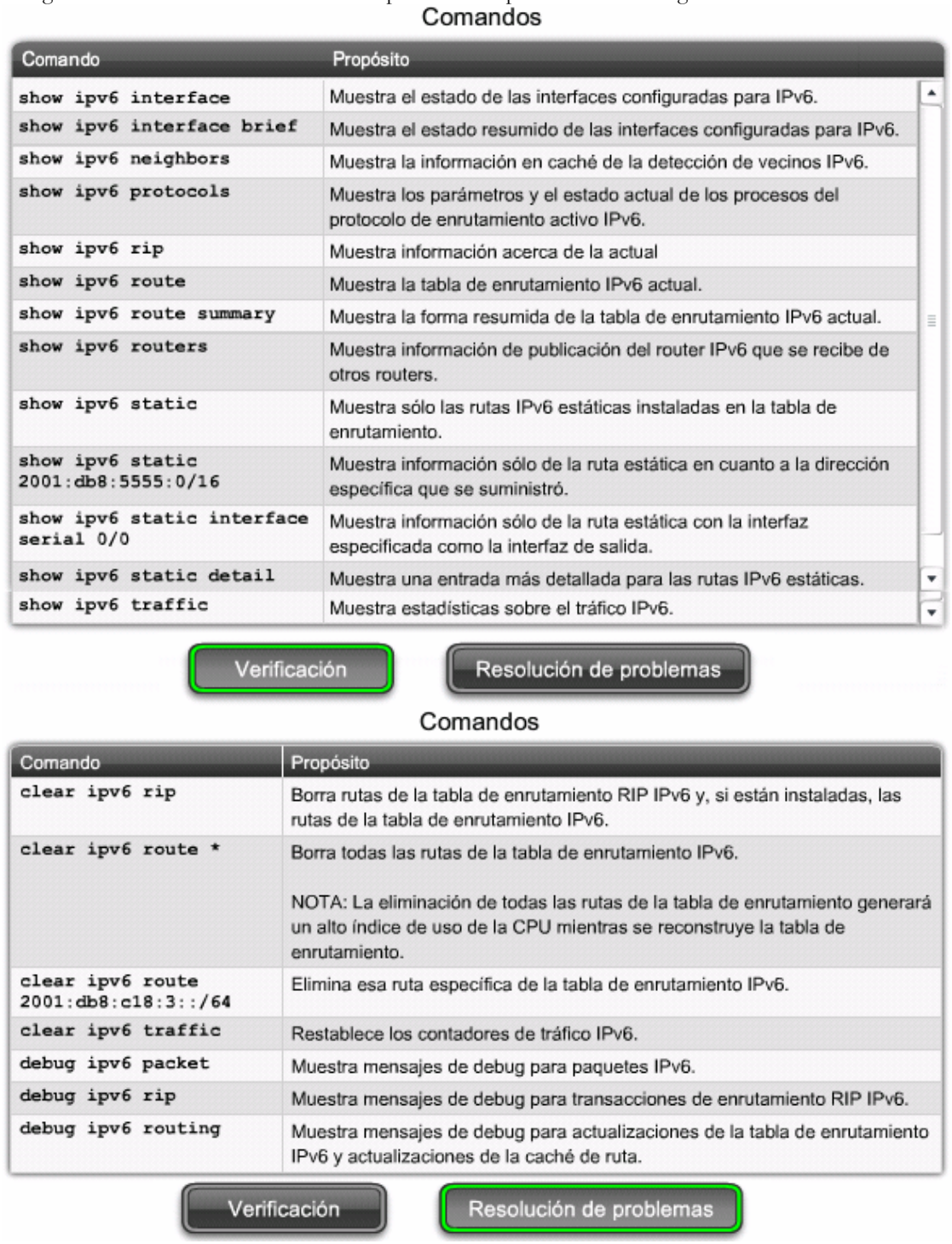
Verificación y resolución de problemas de RPIng para IPv6

Después de configurar RIPng, es necesario hacer una verificación. La figura enumera los diferentes comandos que puede utilizar.

Haga clic en el botón Resolución de problemas que se muestra en la figura.

Si durante la verificación detecta que RIPng no está funcionando bien, debe resolver el problema.

La figura enumera los comandos utilizados para resolver problemas de RIPng.



CAPITULO VIII – "Resolución de problemas de red"

8.0 Introducción del capítulo

8.0.1 Introducción del capítulo

Una vez que una red está en funcionamiento, los administradores deben supervisar su funcionamiento para mantener la productividad de la organización. De vez en cuando, pueden ocurrir interrupciones en la red. En algunos casos, son planificadas y su impacto sobre la organización se maneja fácilmente. En otros, no son planificadas y su impacto sobre la organización puede ser grave. En el caso de que ocurra una interrupción inesperada de la red, los administradores deben poder resolver el problema y hacer que la red vuelva a su producción total. En este capítulo, aprenderá un proceso sistemático para la solución de problemas cuando ocurren interrupciones en la red.

Al completar este capítulo, usted podrá:

- Establecer y documentar una línea de base de red.
- Describir las diversas metodologías de resolución de problemas y herramientas correspondientes.
- Describir los problemas frecuentes que surgen durante la implementación de WAN.
- Identificar y resolver problemas comunes de implementación de redes empresariales mediante la aplicación de un enfoque de un modelo dividido en capas.

8.1 Establecimiento de la línea de base de rendimiento de la red

8.1.1 Documentación de la red

Documentación de la red

Para diagnosticar y corregir de manera eficaz problemas de la red, un ingeniero de red debe saber cómo se ha diseñado una red y cuál es el rendimiento esperado para dicha red en condiciones normales de funcionamiento. Esta información se denomina línea de base de red y se registra en la documentación, por ejemplo, en las tablas de configuración y los diagramas de topología.

La documentación de configuración de la red proporciona un diagrama lógico de la red e información detallada acerca de cada componente. Esta información debe mantenerse en una ubicación única, ya sea como una copia impresa o en la red en un sitio Web protegido. La documentación de la red debe incluir estos componentes:

- Tabla de configuración de la red
- Tabla de configuración del sistema final
- Diagrama de topología de la red

Tabla de configuración de la red

Contiene registros actualizados y precisos del hardware y software usados en una red. La tabla de configuración de la red debe proporcionar al ingeniero de red toda la información necesaria para identificar y corregir la falla de la red.

Haga clic en el botón Documentación de router y switch en la figura.

La tabla de la figura ilustra el conjunto de datos que debe incluirse para todos los componentes:

- Tipo de dispositivo, designación del modelo
- Nombre de la imagen del IOS
- Nombre de host de la red del dispositivo
- Ubicación del dispositivo (edificio, piso, sala, bastidor, panel)
- Si es un dispositivo modular, incluya todos los tipos de módulos y en qué ranura del módulo se ubican.
- Direcciones de capa de enlace de datos
- Direcciones de capa de red
- Cualquier información importante adicional acerca de los aspectos físicos del dispositivo

Haga clic en el botón Documentación del sistema final en la figura.

Tabla de configuración del sistema final

Contiene registros de línea de base del hardware y software usados en los dispositivos del sistemafinal, tales como servidores, consolas de administración de la red y estaciones de trabajo de escritorio. La configuración incorrecta del sistema final puede tener un impacto negativo sobre el rendimiento general de una red.

Para la resolución de problemas, debe documentarse la siguiente información:

- Nombre del dispositivo (objetivo)
- Sistema operativo y versión
- Dirección IP
- Máscara de subred
- Direcciones de gateway predeterminado, servidor DNS y servidor WINS
- Todas las aplicaciones de red de ancho de banda elevado que ejecuta el sistema final

Haga clic en el botón Diagrama de topología de la red en la figura.

Diagrama de topología de la red

Representación gráfica de una red que ilustra cómo se conecta cada dispositivo en una red y su arquitectura lógica. Un diagrama de topología comparte muchos componentes con la tabla de configuración de la red. Cada dispositivo de red debe representarse en el diagrama con una notación coherente o un símbolo gráfico. Además, cada conexión lógica y física debe representarse mediante una línea simple u otro símbolo adecuado. Los protocolos de enrutamiento también pueden mostrarse.

Como mínimo, el diagrama de topología debe incluir:

- Símbolos para todos los dispositivos y cómo se conectan

Números y tipos de interfaz

- Direcciones IP
- Máscaras de subred

Documentación de la red

Nombre y modelo del dispositivo	Nombre de interfaz	Dirección MAC	Dirección IP/máscara de subred	Protocolos de enrutamiento IP
R1, Cisco 2611XM	fa0/0	0007 .8580.a159	192.168.10.1 /24	EIGRP 10
	fa0/1	0007 .8580.a160	192.168.11.1 /24	EIGRP 10
	s0/0/0	--- ---	10.1.1.1/30	OSPF
	s0/0/1	--- ---	No conectado	
R2, Cisco 2611XM	fa0/0	0007 .8580.a159	192.168.20.1 /24	EIGRP 10

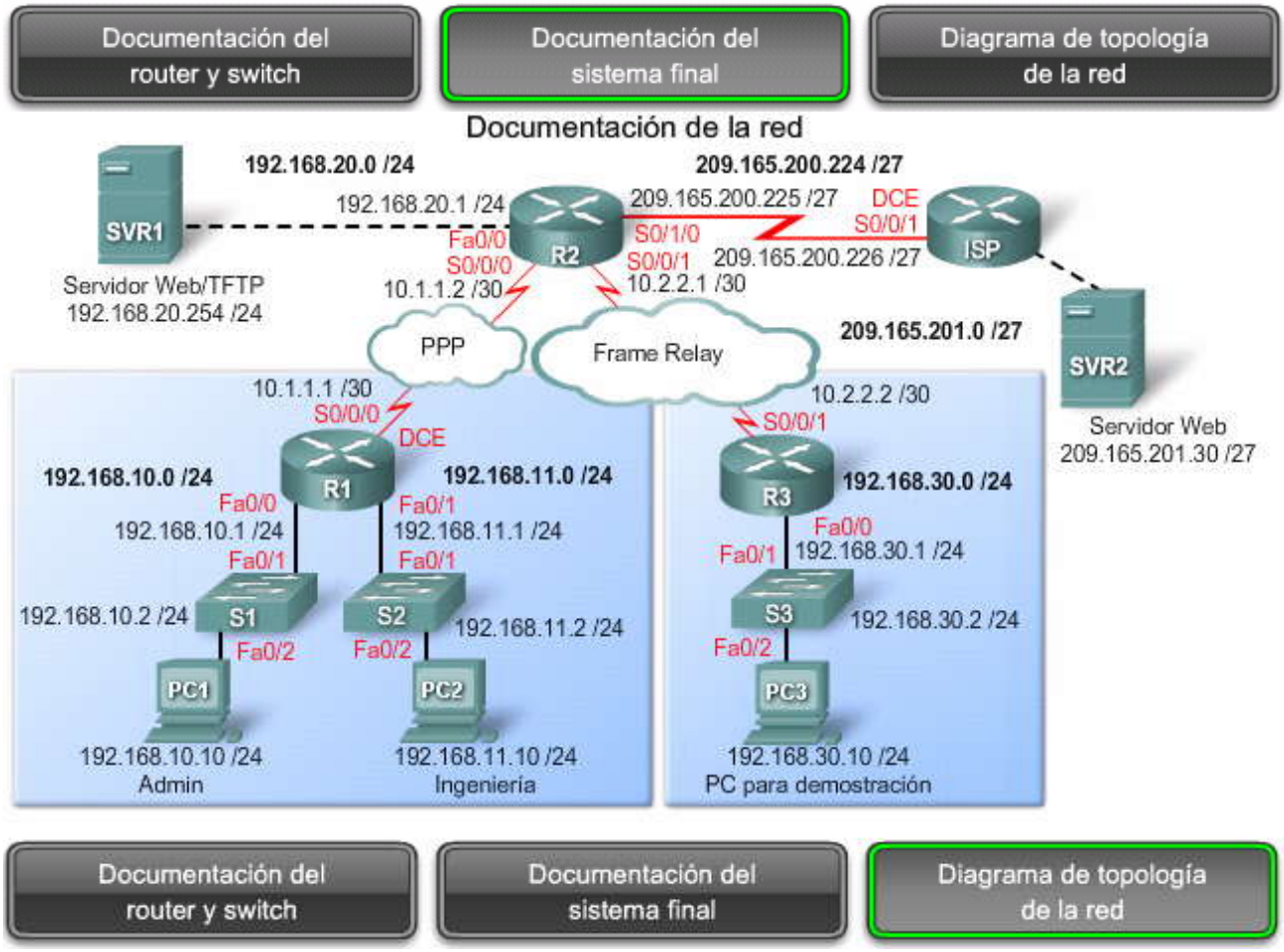
Nombre del switch, modelo, dirección IP de administración	Nombre del puerto	Velocidad	Duplex	Estado STP (Reenviar /Bloquear)	Puerto rápido (Sí/No)	Estado troncal	Canal Ether (L2 o L3)	Clave
S1, Cisco WS-C3550-24-SMI, 192.168.10.2 /24	fa0/1	100	Automático	Reenviar	No	On	L2	Conecta con R1
	fa0/2	100	Automático	Reenviar	No	On	L2	Conecta con PC1
	fa0/3							No conectado
	fa0/4							No conectado

Documentación del router y switch | Documentación del sistema final | Diagrama de topología de la red

Haga clic para ver los distintos tipos de documentación de red

Documentación de la red

Nombre del dispositivo (objetivo)	Sistema operativo/ versión	Dirección IP/máscara de subred	Dirección de gateway predeterminado	Dirección del servidor DNS	Dirección del servidor WINS	Aplicaciones de red	Aplicaciones de ancho de banda elevado
SRV1 (Servidor Web/TFTP)	UNIX	192.168.20.254 /24	192.168.20.1 /24	192.168.20.1 /24		HTTP FTP	-
SRV2 (servidor Web) coubicado en ISP	UNIX	209.165.201.30 /27	209.165.201.1 /27	209.165.201.1 /27		HTTP	-
PC1 (terminal de administración)	UNIX	192.168.10.10 /24	192.168.10.1 /24	192.168.10.1 /24		FTP Telnet	VoIP
PC2 (PC del usuario: Ingeniería)	Windows XP Pro SP2	192.168.11.10 /24	192.168.11.1 /24	192.168.11.1 /24		HTTP FTP	VoIP
PC3 (PC para demostración: Marketing)	Windows XP Pro SP2	192.168.30.10 /24	192.168.30.1 /24	192.168.30.1 /24		HTTP	Streaming Video VoIP



8.1.2 Documentación de la red

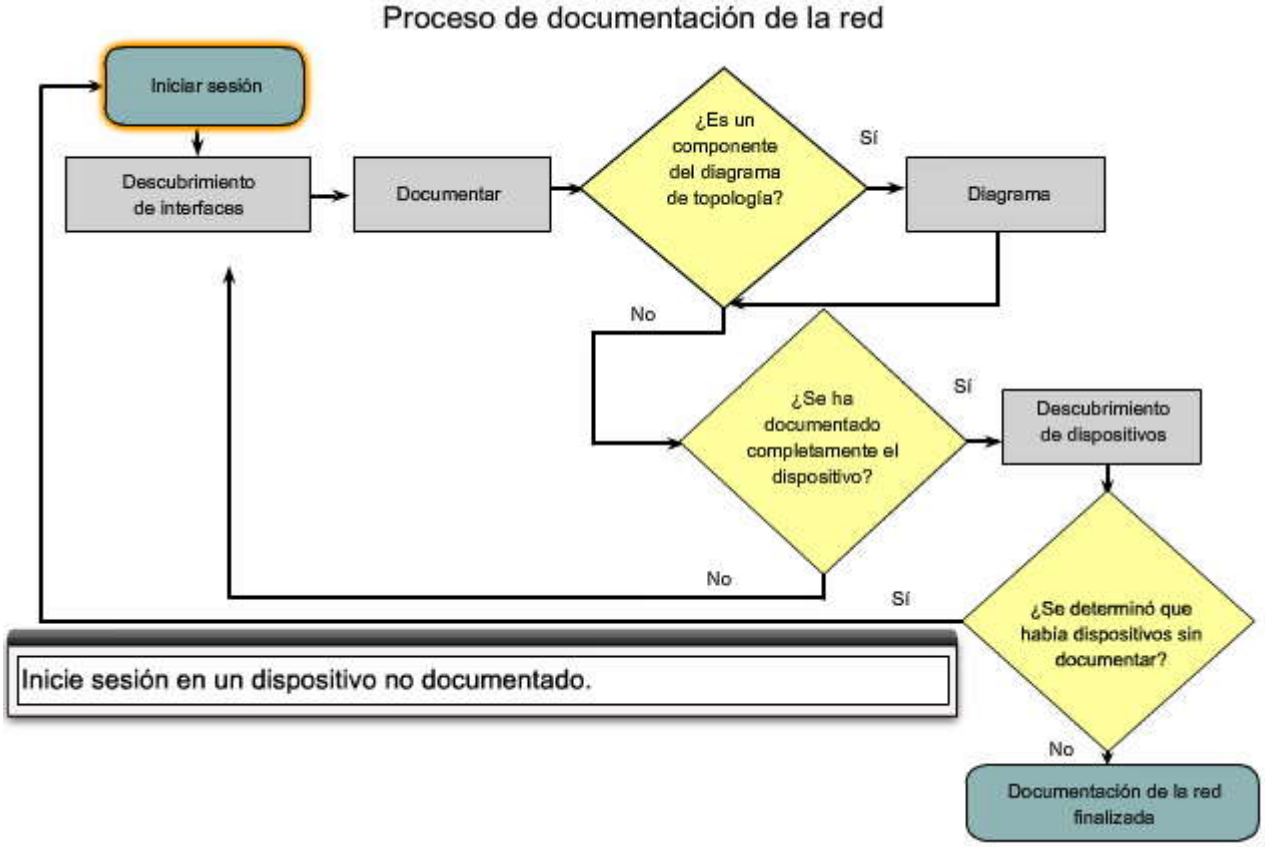
Proceso de documentación de la red

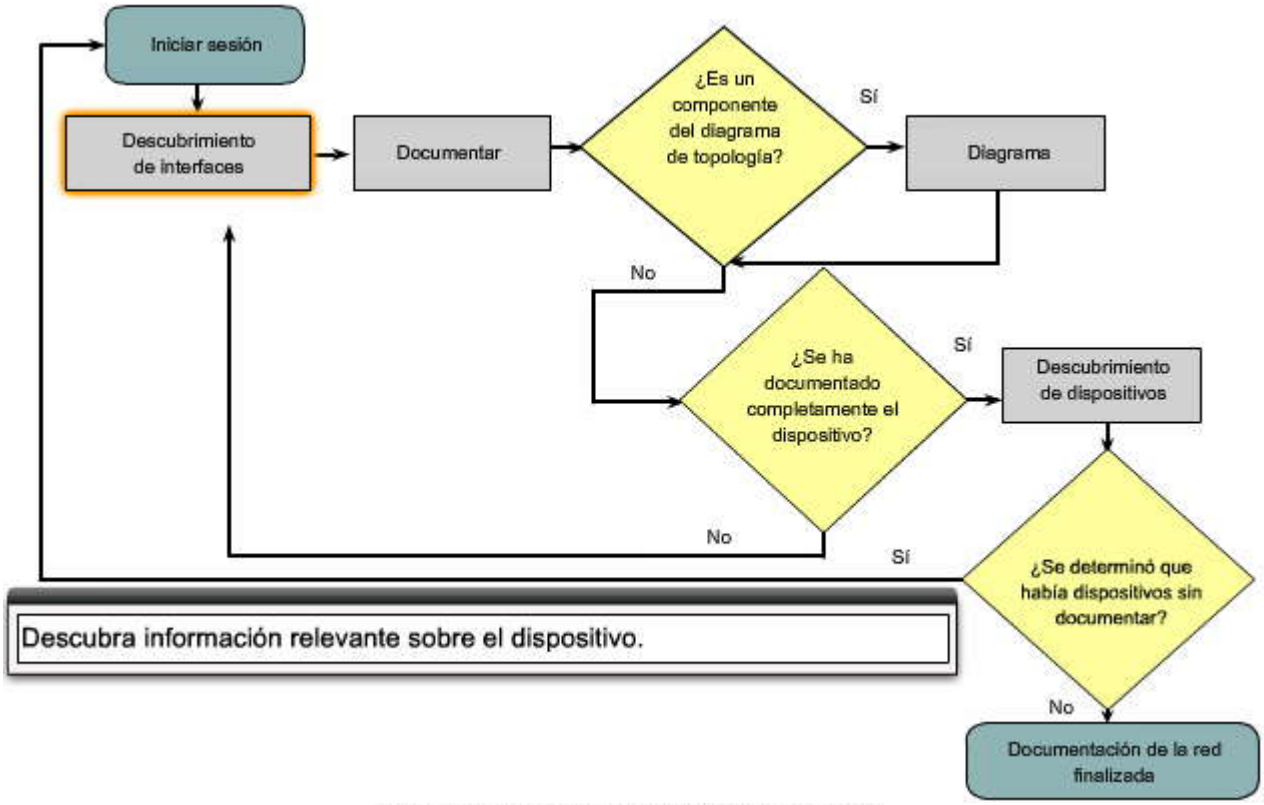
La figura muestra el proceso de documentación de la red.

Coloque el cursor sobre cada etapa en la figura para obtener más información sobre el proceso.

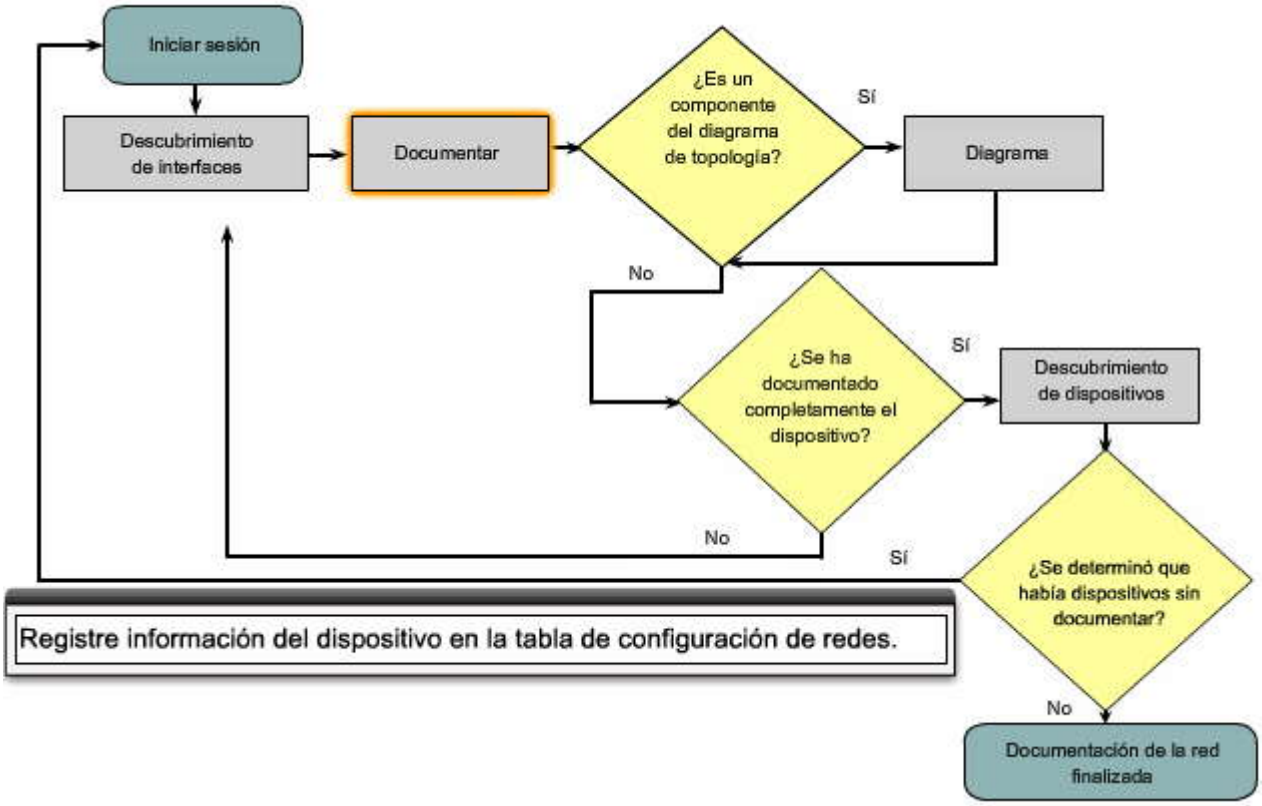
Al documentar la red, puede ser necesario recopilar información directamente de routers y switches. Los comandos útiles para el proceso de documentación de la red incluyen:

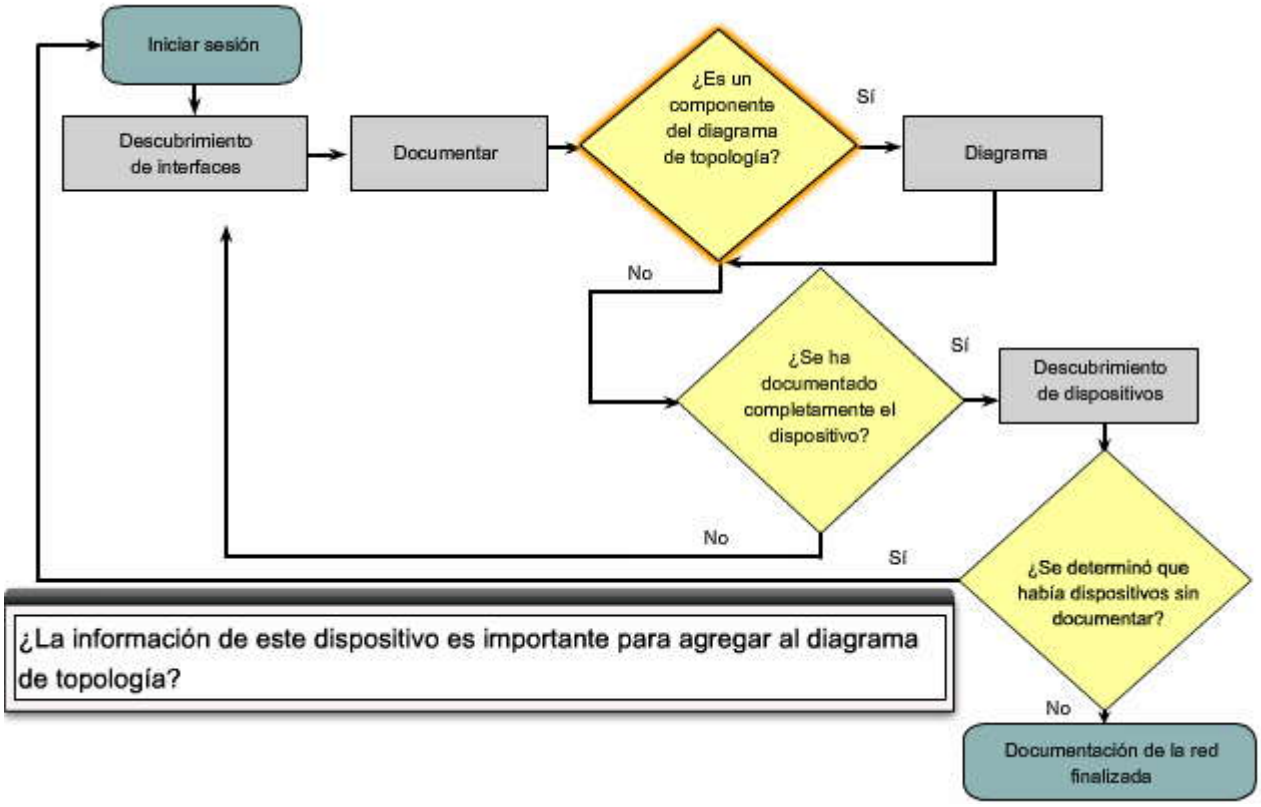
- El comando **ping**, que se usa para probar la conectividad con los dispositivos vecinos antes de conectarse a ellos. Al hacer ping a otras PC en la red también se inicia el proceso de descubrimiento automático de direcciones MAC.
- El comando **telnet**, que se usa para conectarse de manera remota a un dispositivo para obtener accesoa la información de configuración.
- El comando **show ip interface brief**, que se usa para mostrar el estado activo o no activo y la dirección IP de todas las interfaces en un dispositivo.
- El comando **show ip route**, que se usa para mostrar la tabla de enrutamiento en un router para conocer los vecinos conectados directamente, más dispositivos remotos (a través de las rutas conocidas) y los protocolos de enrutamiento que se han configurado.
- El comando **show cdp neighbor detail**, que se usa para obtener información detallada acerca de los dispositivos vecinos Cisco conectados en forma directa.

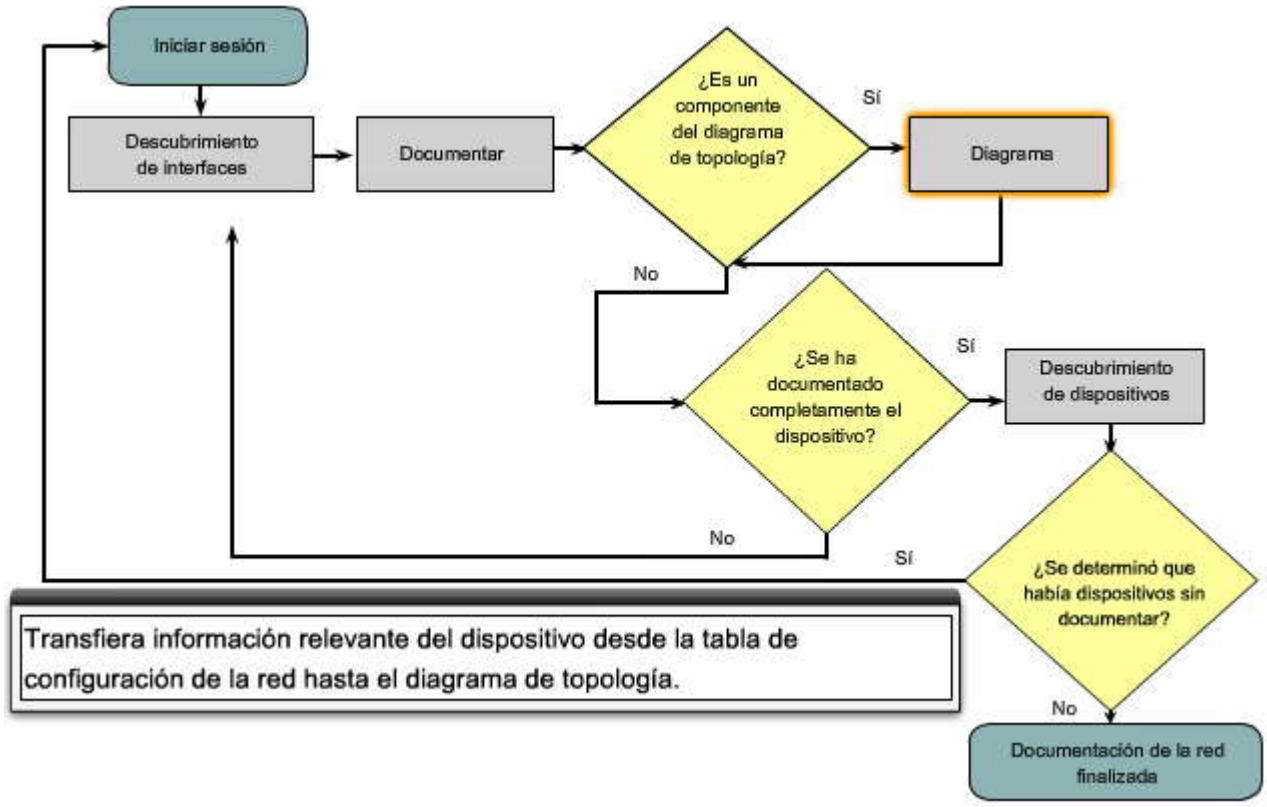


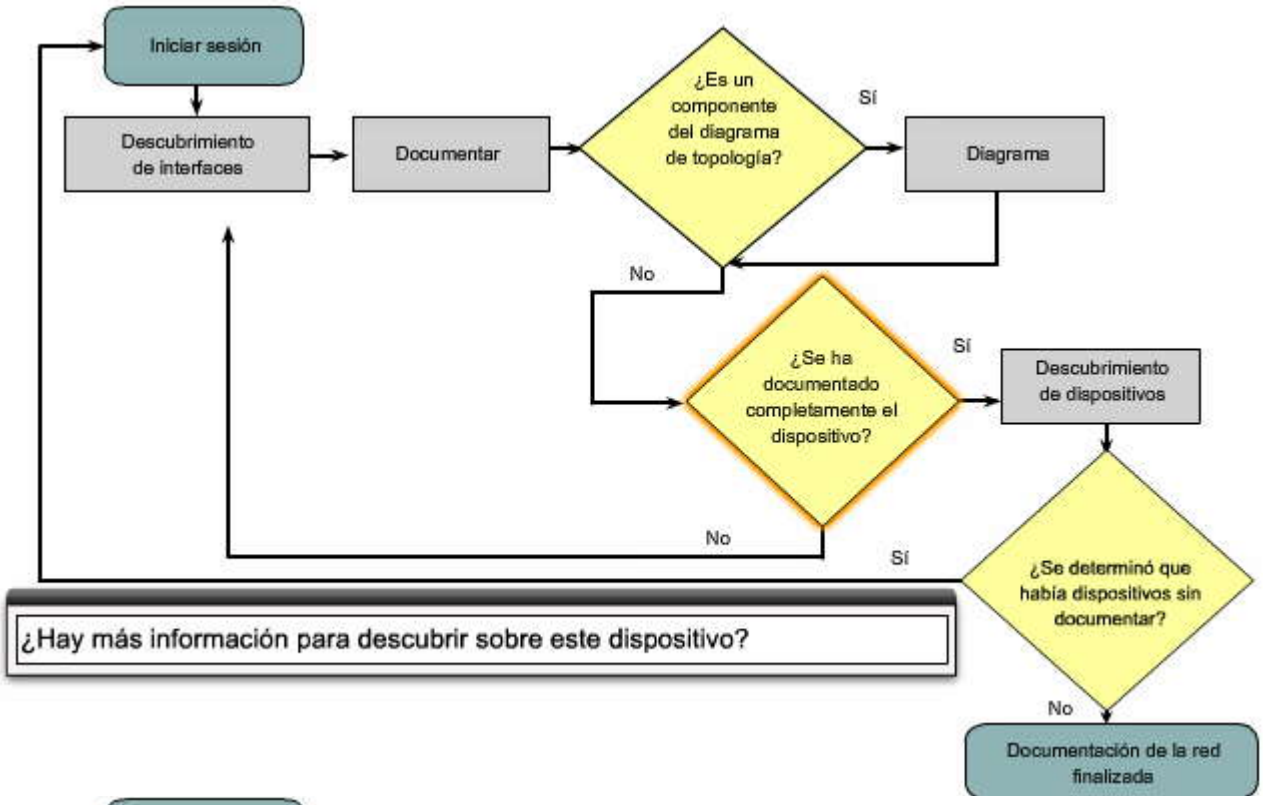


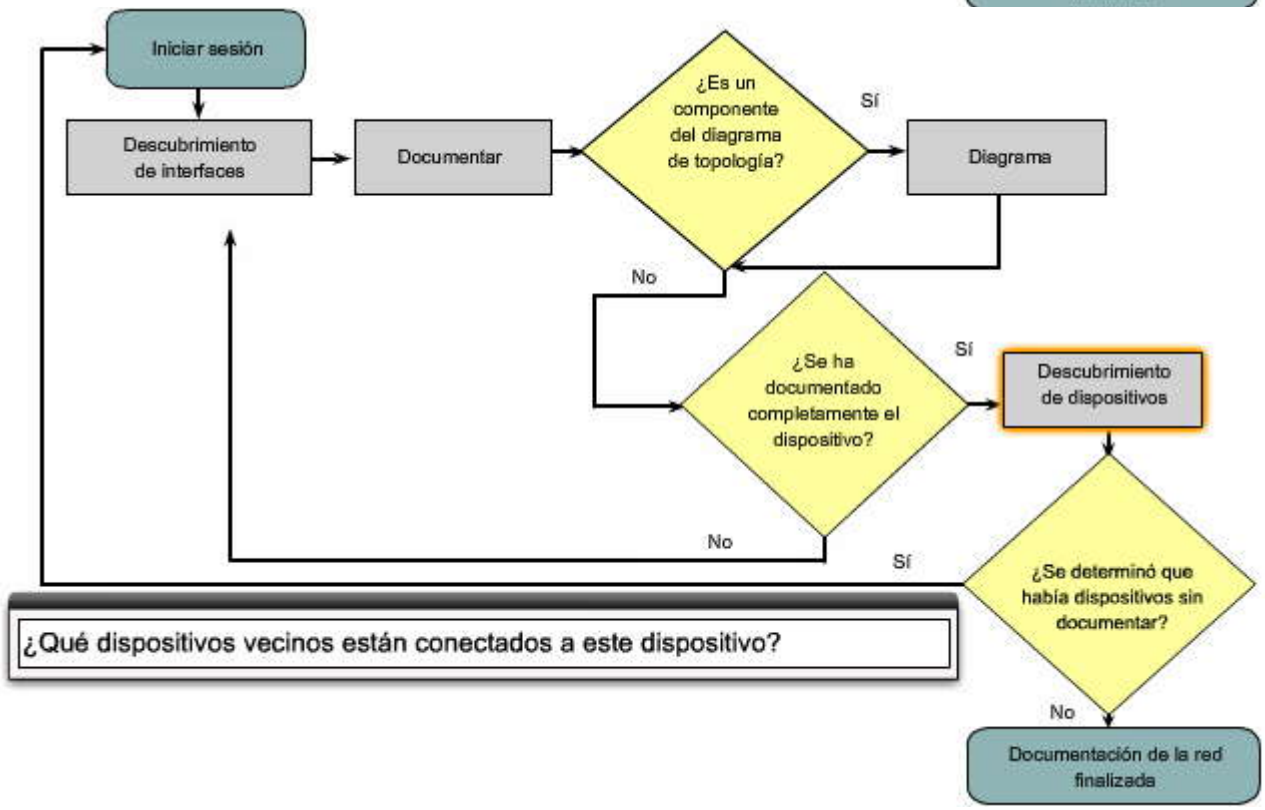
Proceso de documentación de la red

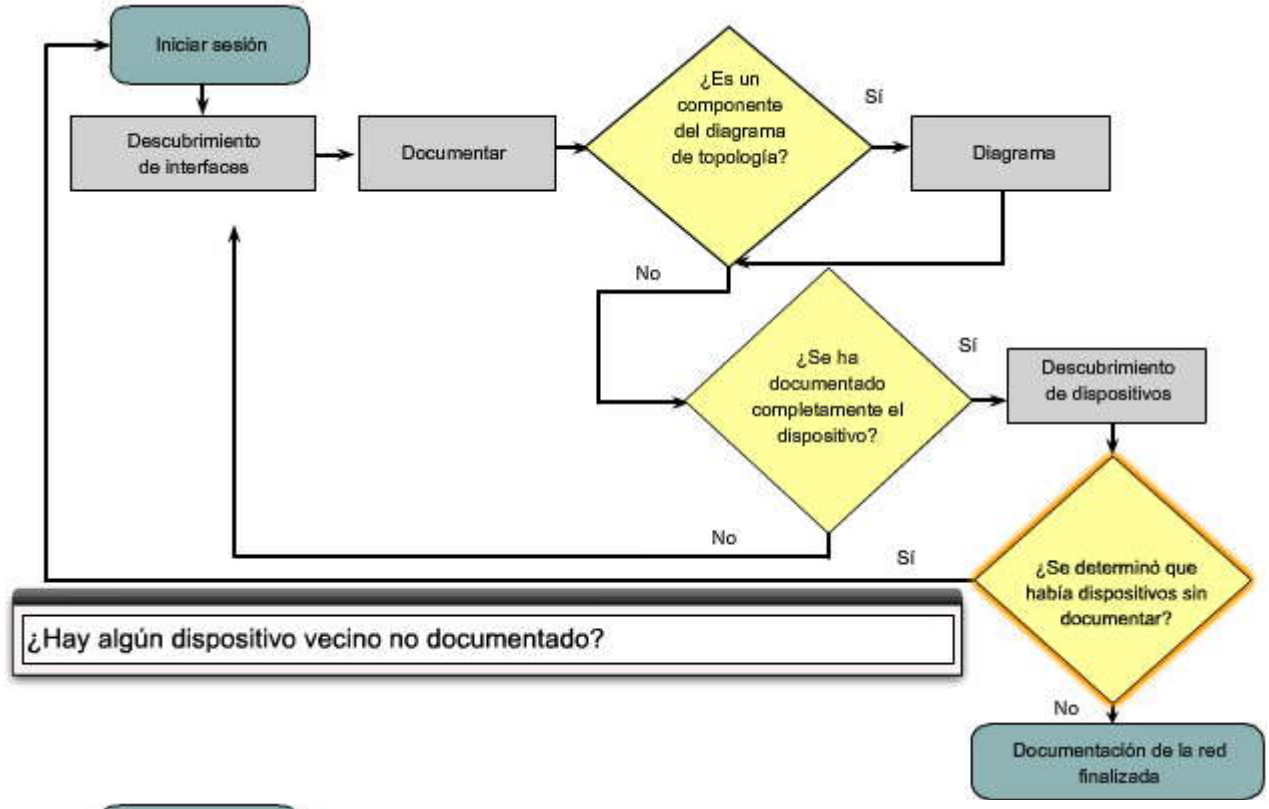


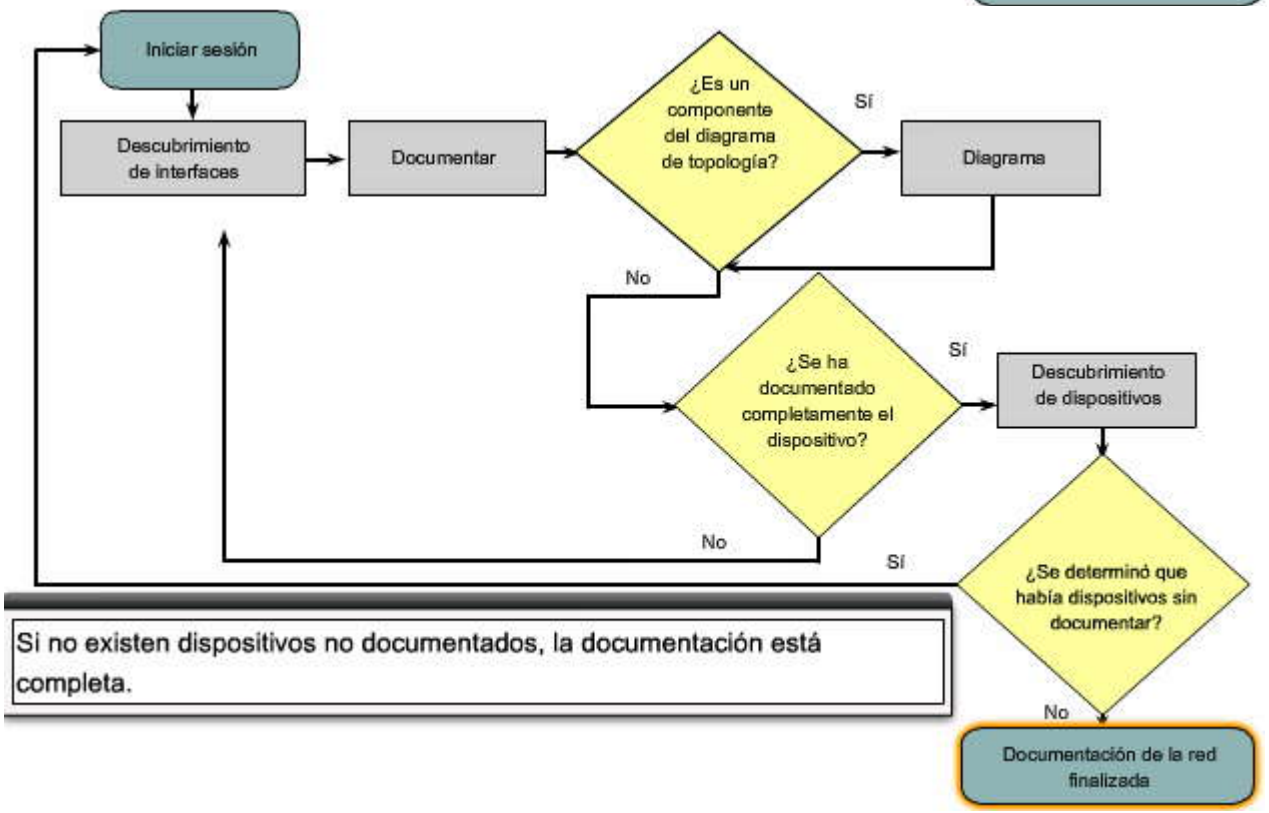

Iniciar sesión
Descubrimiento de interfaces
Documentar
¿Es un componente del diagrama de topología?
Sí
Diagrama
No
¿Se ha documentado completamente el dispositivo?
Sí
Descubrimiento de dispositivos
No
¿Se determinó que había dispositivos sin documentar?
Sí
No
Documentación de la red finalizada
¿La información de este dispositivo es importante para agregar al diagrama de topología?


Iniciar sesión
Descubrimiento de interfaces
Documentar
¿Es un componente del diagrama de topología?
Sí
Diagrama
No
¿Se ha documentado completamente el dispositivo?
Sí
Descubrimiento de dispositivos
No
¿Se determinó que había dispositivos sin documentar?
Sí
No
Documentación de la red finalizada
Transfiera información relevante del dispositivo desde la tabla de configuración de la red hasta el diagrama de topología.


Iniciar sesión
Descubrimiento de interfaces
Documentar
¿Es un componente del diagrama de topología?
Sí
Diagrama
No
¿Se ha documentado completamente el dispositivo?
Sí
Descubrimiento de dispositivos
No
¿Se determinó que había dispositivos sin documentar?
Sí
¿Hay más información para descubrir sobre este dispositivo?
No
Documentación de la red finalizada


Iniciar sesión
Descubrimiento de interfaces
Documentar
¿Es un componente del diagrama de topología?
Sí
Diagrama
No
¿Se ha documentado completamente el dispositivo?
Sí
Descubrimiento de dispositivos
No
¿Se determinó que había dispositivos sin documentar?
Sí
¿Qué dispositivos vecinos están conectados a este dispositivo?
No
Documentación de la red finalizada





Esta actividad cubre los pasos necesarios para descubrir una red mediante el uso, principalmente, de los comandos**telnet**, **show cdp neighbors detail** y **show ip route**. Ésta es la Parte I de una actividad que consta de dos partes.

La topología que se observa cuando se abre la actividad de Packet Tracer no muestra todos los detalles de la red. Se han ocultado los detalles por medio de la función de grupo de Packet Tracer. Se ha colapsado la infraestructura de la red, y la topología en el archivo muestra sólo los dispositivos finales. Su tarea consiste en usar su conocimiento sobre comandos de networking y descubrimiento para obtener más información sobre la topología de la red completa y documentarla.

Se proporcionan instrucciones detalladas dentro de la actividad y en el siguiente enlace al PDF.
Instrucciones de las actividades (PDF)

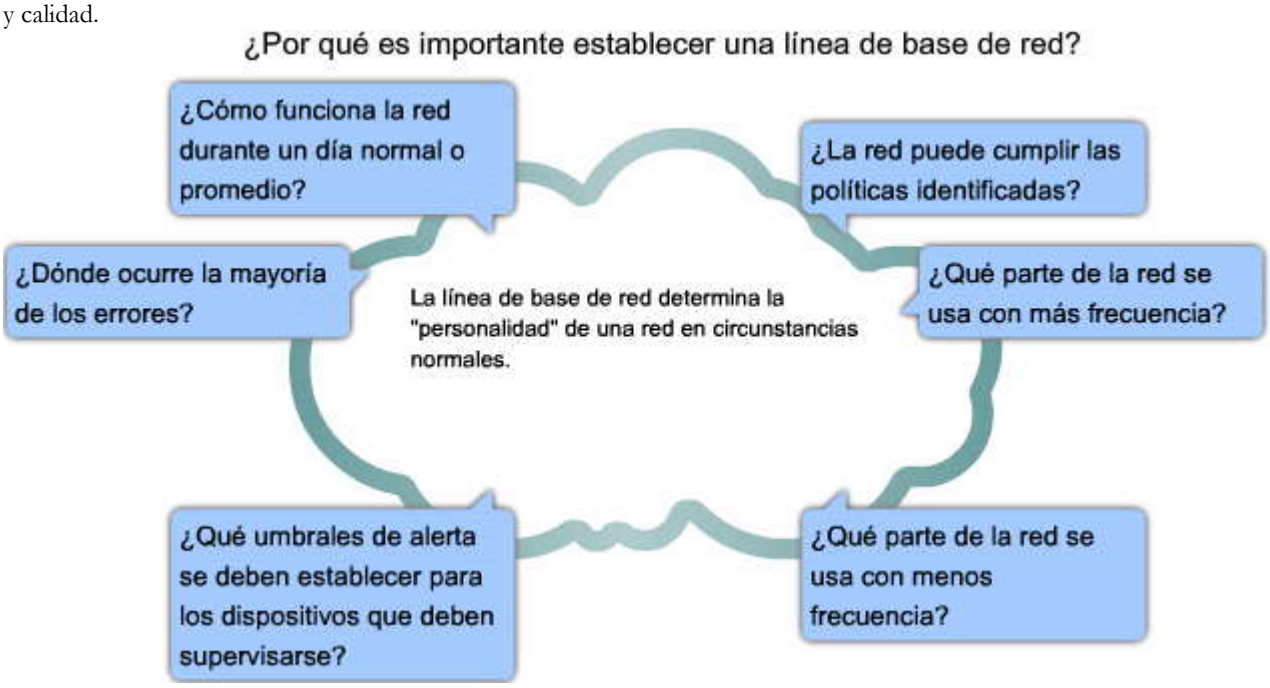
8.1.3 ¿Por qué es importante establecer una línea de base de red?

El establecimiento de una línea de base de rendimiento de la red implica la recopilación de datos clave del rendimiento de los puertos y los dispositivos que son esenciales para el funcionamiento de la red. Esta información ayuda a determinar la "personalidad" de la red y proporciona respuestas a las siguientes preguntas:

- ¿Cómo funciona la red durante un día normal o promedio?
- ¿Dónde se encuentran las áreas utilizadas en exceso y las áreas utilizadas insuficientemente?
- ¿Dónde ocurre la mayoría de los errores?
- ¿Qué niveles hay que establecer para los dispositivos que deben supervisarse?
- ¿La red puede proporcionar las políticas identificadas?

La medición del rendimiento inicial y la disponibilidad de los enlaces y dispositivos de red críticos permiten que el administrador de red establezca la diferencia entre el comportamiento anormal y el rendimiento adecuado de la reda medida que la red crece o cambian los patrones de tráfico. La línea de base también permite establecer si el diseño de red actual puede proporcionar las políticas necesarias. Sin una línea de base, no existe un estándar para medir el estado óptimo de los niveles de tráfico y congestión de la red.

Además, el análisis posterior a una línea de base inicial suele revelar problemas ocultos. Los datos recopilados revelan la naturaleza verdadera de la congestión o la posible congestión en una red. También puederevelar las áreas de una red que no se están utilizando suficientemente y, con frecuencia, puede llevar al rediseño de la red según las observaciones de capacidad y calidad.



8.1.4 Pasos para establecer una línea de base de red

Planificación de la primera línea de base

Debido a que la línea de base de rendimiento de la red inicial prepara el camino para medir los efectos de los cambios en la red y los posteriores esfuerzos de resolución de problemas, es importante planificarla cuidadosamente. Aquí sepresentan los pasos recomendados para la planificación de la primera línea de base:

Paso 1. Determinar los tipos de datos que deben recopilarse

Cuando realice la línea de base inicial, comience con la selección de algunas variables que representen las políticas definidas. Si se seleccionan demasiados puntos de datos, la cantidad de datos puede ser abrumadora y, por lo tanto, dificultar el análisis de los datos recopilados. Comience con un diseño simple y realice ajustes a medida que avanza. En general, algunas buenas

medidas iniciales son la utilización de interfaces y CPU. La figura muestra algunas capturas de pantalla de los datos de utilización de interfaces y CPU, como los muestra un sistema de administración de red de Fluke Networks.

Haga clic en el botón Dispositivos y puertos de interés en la figura.

Paso 2. Identificar los dispositivos y puertos de interés

El próximo paso es la identificación de los dispositivos y puertos clave cuyos datos de rendimiento deben medirse. Los dispositivos y puertos de interés incluyen:

- Puertos de dispositivos de red que se conectan a otros dispositivos de red
- Servidores
- Usuarios clave
- Cualquier otro elemento que se considere fundamental para las operaciones.

En la topología que se muestra en la figura, el administrador de red ha destacado los dispositivos y puertos de interés que se supervisarán durante la prueba de línea de base. Los dispositivos de interés incluyen los routers R1, R2 y R3, PC1 (terminal de administración) y SRV1 (el servidor Web/TFTP). Los puertos de interés incluyen los puertos en R1, R2 y R3 que se conectan a los otros routers o switches y, en el router R2, el puerto que se conecta a SRV1 (Fa0/0).

Al reducir los puertos sondeados, los resultados son concisos y se minimiza la carga de administración de la red. Recuerde que una interfaz en un router o switch puede ser una interfaz virtual, tal como una interfaz virtual de switch (SVI).

Este paso es más fácil si se han configurado los campos de descripción de puertos del dispositivo de forma que indiquen qué elemento se conecta al puerto. Por ejemplo, para un puerto de router que se conecta al switch de distribución en el grupo de trabajo Ingeniería, se podría configurar la descripción "Switch de distribución de LAN de Ingeniería".

Haga clic en el botón Determinar la duración de línea de base en la figura.

Paso 3. Determinar la duración de la línea de base

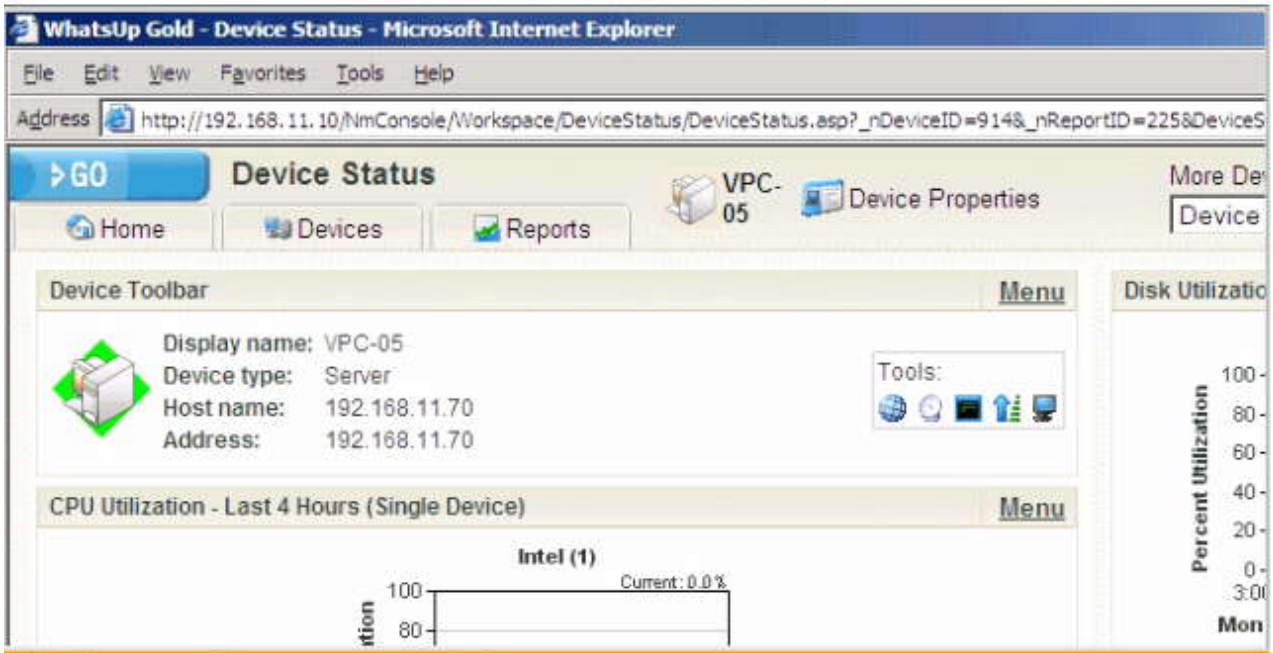
Es importante que la duración y la información de la línea de base recopilada sean suficientes para establecer una imagen típica de la red. Este período debe ser de al menos siete días a fin de capturar cualquier tendencia diaria o semanal. Las tendencias semanales son tan importantes como las tendencias por horas o días.

La figura muestra ejemplos de varias capturas de pantalla de las tendencias de utilización de CPU obtenidas durante un período diario, semanal, mensual y anual. Las tendencias de la semana laboral son demasiado escasas para reflejar de manera precisa la naturaleza recurrente de los picos de utilización que ocurren durante el fin de semana, los sábados a la tarde, cuando una importante operación de copia de seguridad de base de datos consume ancho de banda de la red. Este patrón recurrente se muestra en la tendencia mensual. La tendencia anual presentada en el ejemplo es de una duración demasiado extensa para proporcionar detalles de rendimiento significativos para la línea de base. Una línea de base no debe durar más de seis semanas, a menos que deban medirse tendencias específicas a largo plazo. En general, una línea de base de dos a cuatro semanas resulta adecuada.

No se debe realizar una medición de línea de base durante momentos de patrones de tráfico no habituales, ya que los datos proporcionarían una imagen inexacta de las operaciones normales de la red. Se obtendría una medición inexacta del rendimiento de la red si realizara una medición de línea de base durante un día inhábil o durante un mes en el cual la mayor parte de la empresa está de vacaciones.

El análisis de la línea de base de la red debe realizarse de manera regular. Realice un análisis anual de toda la red o establezca líneas de base de diferentes secciones de la red de forma rotativa. Debe realizarse el análisis regularmente para comprender cómo el crecimiento y otros cambios afectan a la red.

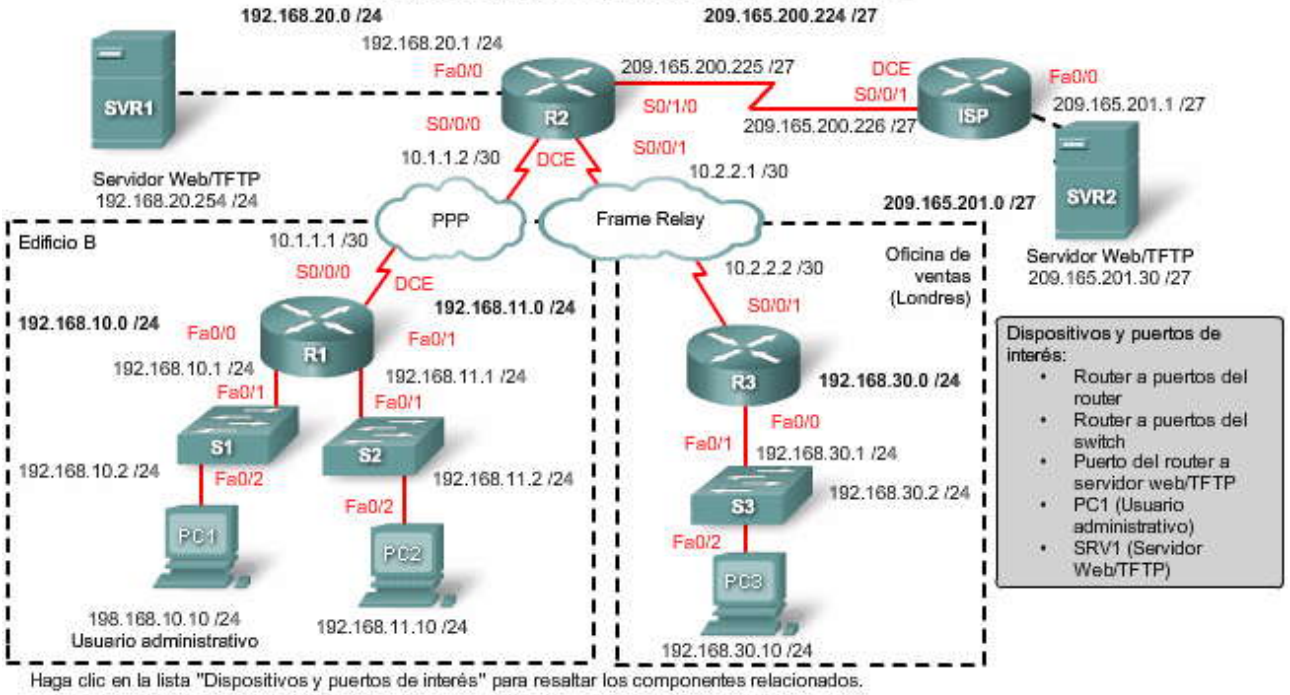
Planificación de la primera línea de base



Haga clic y arrastre la imagen para ver los detalles.

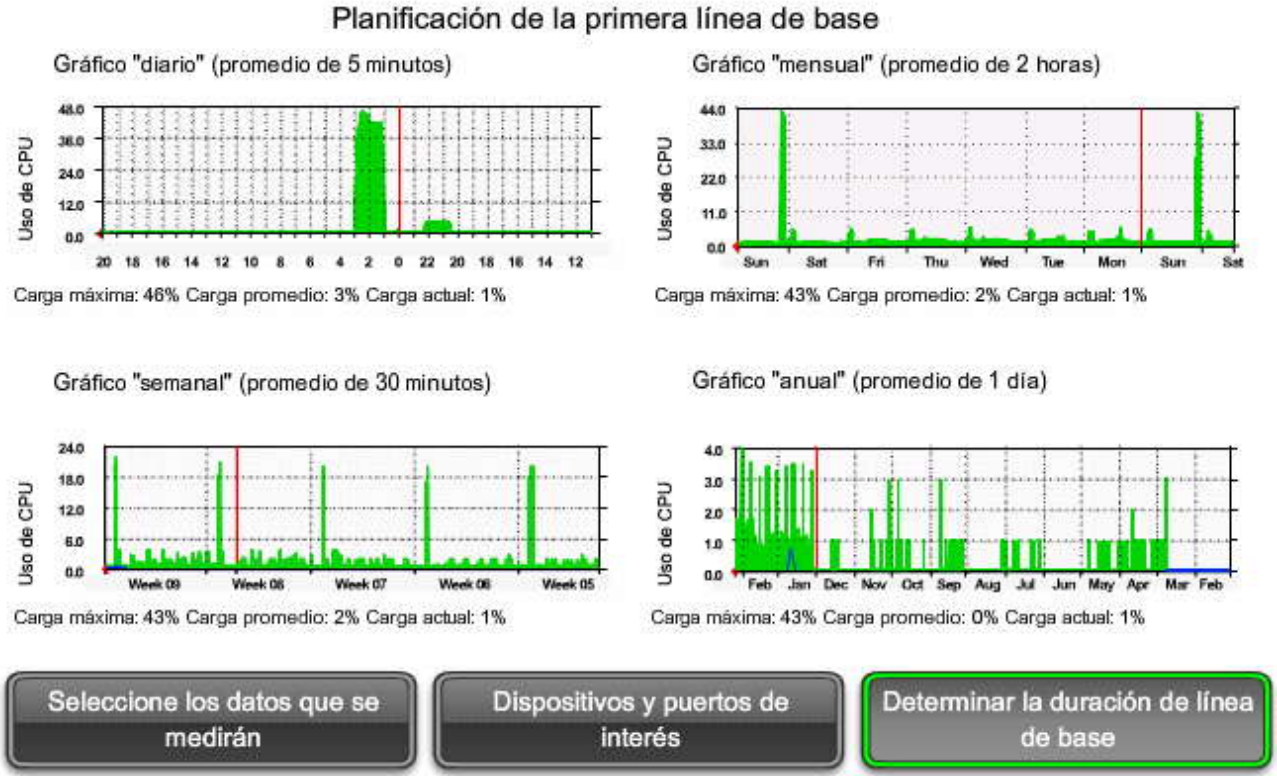
Seleccione los datos que se medirán | Dispositivos y puertos de interés | Determinar la duración de línea de base

Planificación de la primera línea de base



Haga clic en la lista "Dispositivos y puertos de interés" para resaltar los componentes relacionados.

Seleccione los datos que se medirán | Dispositivos y puertos de interés | Determinar la duración de línea de base



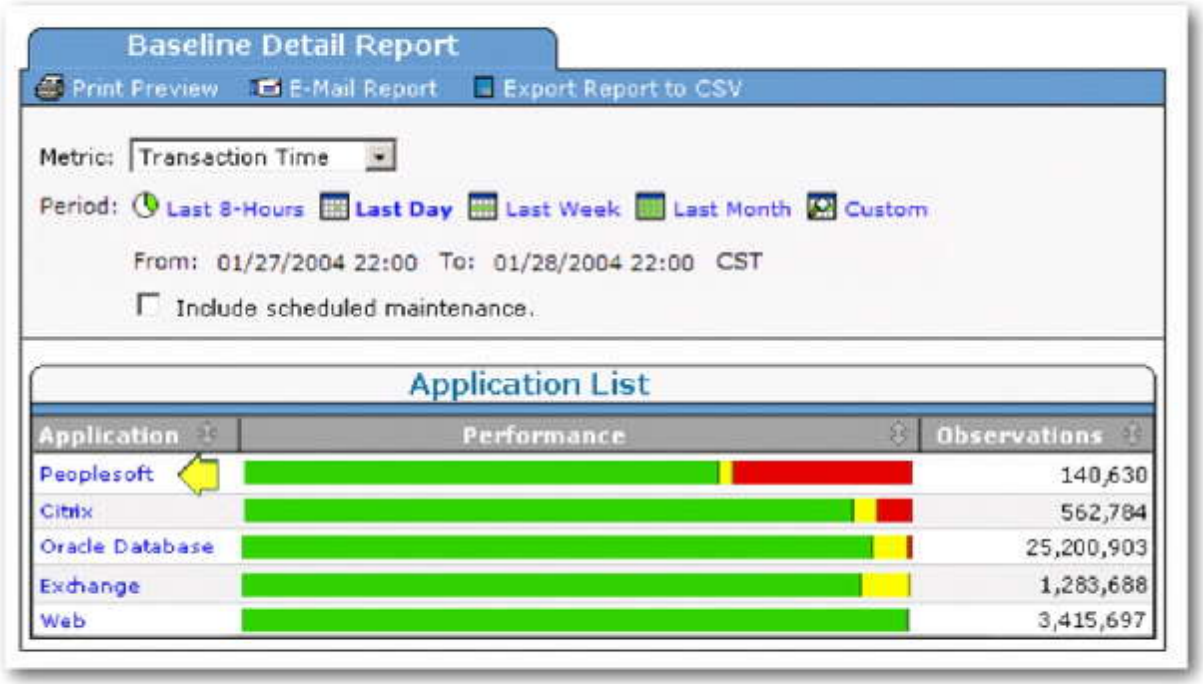
Medición de los datos de rendimiento de la red

En general, se usa software de administración de redes sofisticado para evaluar redes grandes y complejas. Por ejempb, el módulo SuperAgent de Fluke Networks permite a los administradores crear y revisar informes automáticamente mediante una función de líneas de base inteligentes. Esta función compara los niveles de rendimiento actuales con las observaciones anteriores y puede identificar automáticamente problemas de rendimiento y aplicaciones que no proporcionan los niveles de servicio esperados.

Haga clic en el botón Comandos manuales en la figura.

En redes más simples, las tareas de establecimiento de línea de base pueden requerir una combinación de recopilación de datos manual e inspectores de protocolos de red simples. La determinación de una línea de base inicial o la realización de un análisis de supervisión de rendimiento puede demorar varias horas o días para reflejar de manera precisa el rendimiento de la red. El software de administración de red o los inspectores de protocolos y programas detectores pueden ejecutarse continuamente durante el proceso de recopilación de datos. La recopilación manual mediante los comandos **show** en dispositivos de red individuales consume mucho tiempo y debe limitarse a los dispositivos de red críticos.

Medición de los datos de rendimiento de la red



Recopilación automatizada de datos Comandos manuales

Medición de los datos de rendimiento de la red

Comando	Descripción
show version	Muestra el tiempo de actividad, información sobre la versión del software y del hardware del dispositivo.
show ip interface [brief]	Muestra todas las opciones de configuración establecidas en una interfaz. Use la palabra clave **brief** para mostrar sólo el estado de actividad/inactividad de las interfaces IP y de la dirección IP de cada una de ellas.
show interface *[interface_type interface_num]*	Muestra la salida detallada de cada interfaz. Para mostrar la salida detallada de una única interfaz solamente, incluya el tipo y el número de interfaz en el comando (por ejemplo, ethernet 0/0).
show ip route	Muestra el contenido de la tabla de enrutamiento.
show arp	Muestra el contenido de la tabla ARP.
show running-config	Muestra la configuración actual.
show port	Muestra el estado de los puertos en un switch.
show vlan	Muestra el estado de las VLAN en un switch.
show tech-support	Ejecuta otros comandos show y proporciona muchas páginas de salida detalladas, diseñadas para enviarse a soporte técnico. También son útiles por otros motivos.

Recopilación automatizada de datos Comandos manuales

8.2 Herramientas y metodologías de resolución de problemas

8.2.1 Enfoque general para la resolución de problemas

Los ingenieros y administradores de red y el personal de soporte saben que la resolución de problemas es el proceso que consume el mayor porcentaje de su tiempo. El uso de técnicas eficaces para la resolución de problemas reduce el tiempo total de resolución cuando se trabaja en un entorno de producción.

Dos enfoques opuestos para resolver problemas casi siempre terminan en desilusión, retraso o fracaso. En un extremo, está el enfoque teórico o de científico espacial. En el otro extremo, está el enfoque poco prácticoo de cavernícola.

El científico espacial analiza la situación una y otra vez hasta identificar la causa exacta en la raíz del problema y corregirla con precisión quirúrgica. Mientras que este proceso es claramente confiable, pocas empresas pueden permitirse tener sus redes inactivas durante las horas o los días que puede demorar este análisis exhaustivo.

El primer instinto del cavernícola es comenzar a intercambiar tarjetas, cables, hardware y software hasta que, milagrosamente, la red empiece a funcionar de nuevo. Esto no significa que la red funcione adecuadamente, sólo que está en funcionamiento. Si bien este enfoque puede lograr un cambio más rápido en los síntomas, no es muy confiable y es posible que la causa raíz del problema siga presente.

Dado que los dos enfoques son extremos, el mejor enfoque es un punto intermedio que combine elementos de ambos. Es importante analizar la red completa en vez de en partes. Un enfoque sistemático minimiza la confusión y reduce el tiempo que se desperdicia en prueba y error.

8.2.2 Uso de modelos en capas para la resolución de problemas

Comparación de modelos en capas OSI y TCP/IP

Los modelos de networking lógicos, como los modelos OSI y TCP/IP, separan la funcionalidad de red en capas de módulos. Cuando se realiza la resolución de problemas, estos modelos en capas pueden aplicarse a la red física para aislar los problemas de la red. Por ejemplo, si los síntomas sugieren un problema de conexión física, el técnico de red puede concentrarse en la resolución de problemas del circuito que funciona en la capa física. Si ese circuito funciona adecuadamente, el técnico observa las áreas de otra capa que podrían causar el problema.

Modelo de referencia OSI

El modelo OSI proporciona un lenguaje común para los ingenieros de red y se usa con frecuencia en la resolución de problemas de redes. Típicamente, los problemas se describen en términos de las capas de un modelo OSI dado.

El modelo de referencia OSI describe cómo la información de una aplicación de software en una computadora se desplaza a través de una red a una aplicación de software en otra computadora.

Las capas superiores del modelo OSI (5 a 7) se ocupan de los problemas de las aplicaciones y generalmente se implementan sólo en software. La capa de aplicación es la capa más cercana al usuario final. Los procesos de la capa de usuario y de aplicación interactúan con las aplicaciones de software que contienen un componente de comunicaciones.

Las capas inferiores (1 a 4) del modelo OSI manejan los problemas relacionados con el transporte de datos. Las capas 3 y 4 se implementan, generalmente, sólo en software. La capa física (capa 1) y la capa de enlace de datos (capa 2) se implementan en el hardware y el software. La capa física es la más cercana al medio de red físico, como el cableado de red, y es responsable de la transmisión real de la información en el medio.

Modelo TCP/IP

De manera similar al modelo de networking OSI, el modelo TCP/IP también divide la arquitectura de red en capas de módulos. La figura muestra la correspondencia del modelo de networking TCP/IP con las capas del modelo de networking OSI. Esta asignación cercana permite que el conjunto de protocolos TCP/IP se comunique satisfactoriamente con tantas tecnologías de networking.

La capa de aplicación en el conjunto de aplicaciones TCP/IP combina, de hecho, las funciones de las tres capas del modelo OSI: sesión, presentación y aplicación. La capa de aplicación proporciona comunicación entre aplicaciones tales como FTP, HTTP y SMTP en hosts separados.

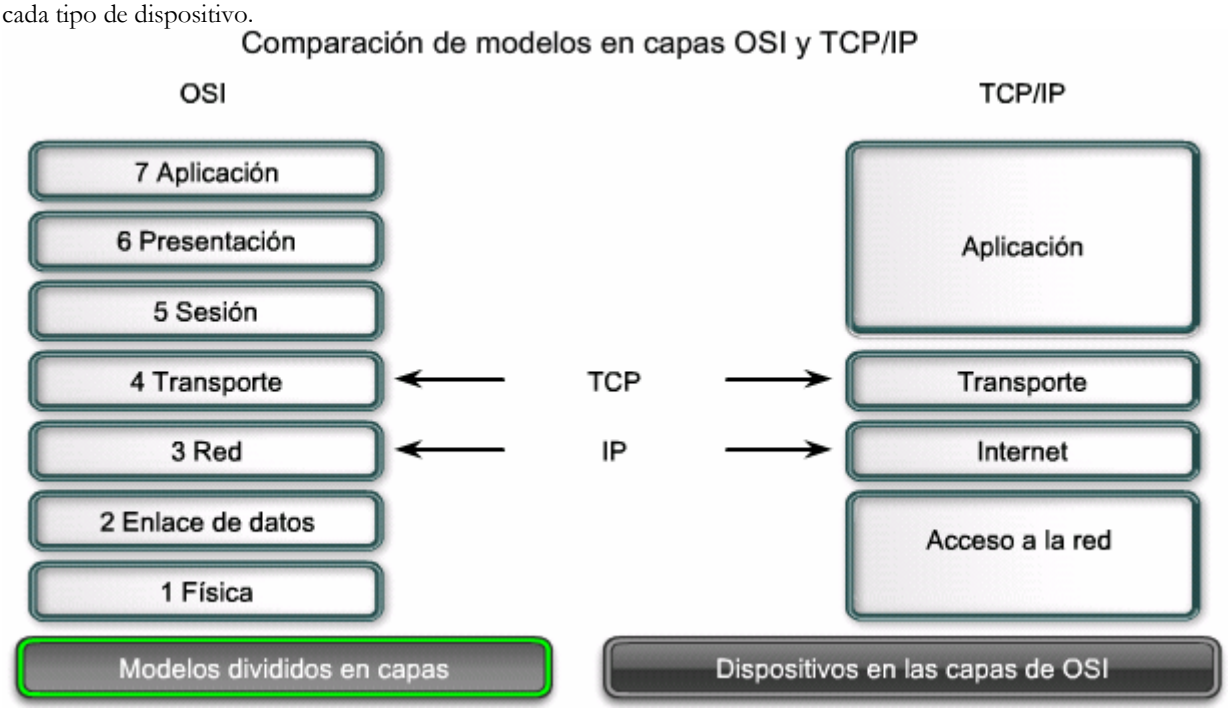
Las capas de transporte de TCP/IP y OSI se corresponden directamente en cuanto a la función. La capa de transporte es responsable del intercambio de segmentos entre dispositivos en una red TCP/IP.

La capa de Internet de TCP/IP se relaciona con la capa de red del modelo OSI. La capa de Internet es responsable de la ubicación de mensajes en un formato fijo que permita que los dispositivos los manejen.

La capa de acceso de red de TCP/IP corresponde a las capas física y de enlace de datos del modelo OSI. La capa de acceso de red se comunica directamente con los medios de red y proporciona una interfaz entre la arquitectura de la red y la capa de Internet.

Haga clic en el botón Dispositivos en las capas de OSI en la figura.

Coloque el cursor sobre cada dispositivo para ver qué capas de OSI se necesitan, en general, para resolver problemas de cada tipo de dispositivo.



Haga coincidir los dispositivos con la capa de OSI

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


Router


Firewall


Switch de multicapa


Switch estándar


Hub


Sistema final

Haga clic en cada dispositivo para ver las capas que son posibles objetivos de la resolución de problemas.

Modelos divididos en capas | Dispositivos en las capas de OSI

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


Router

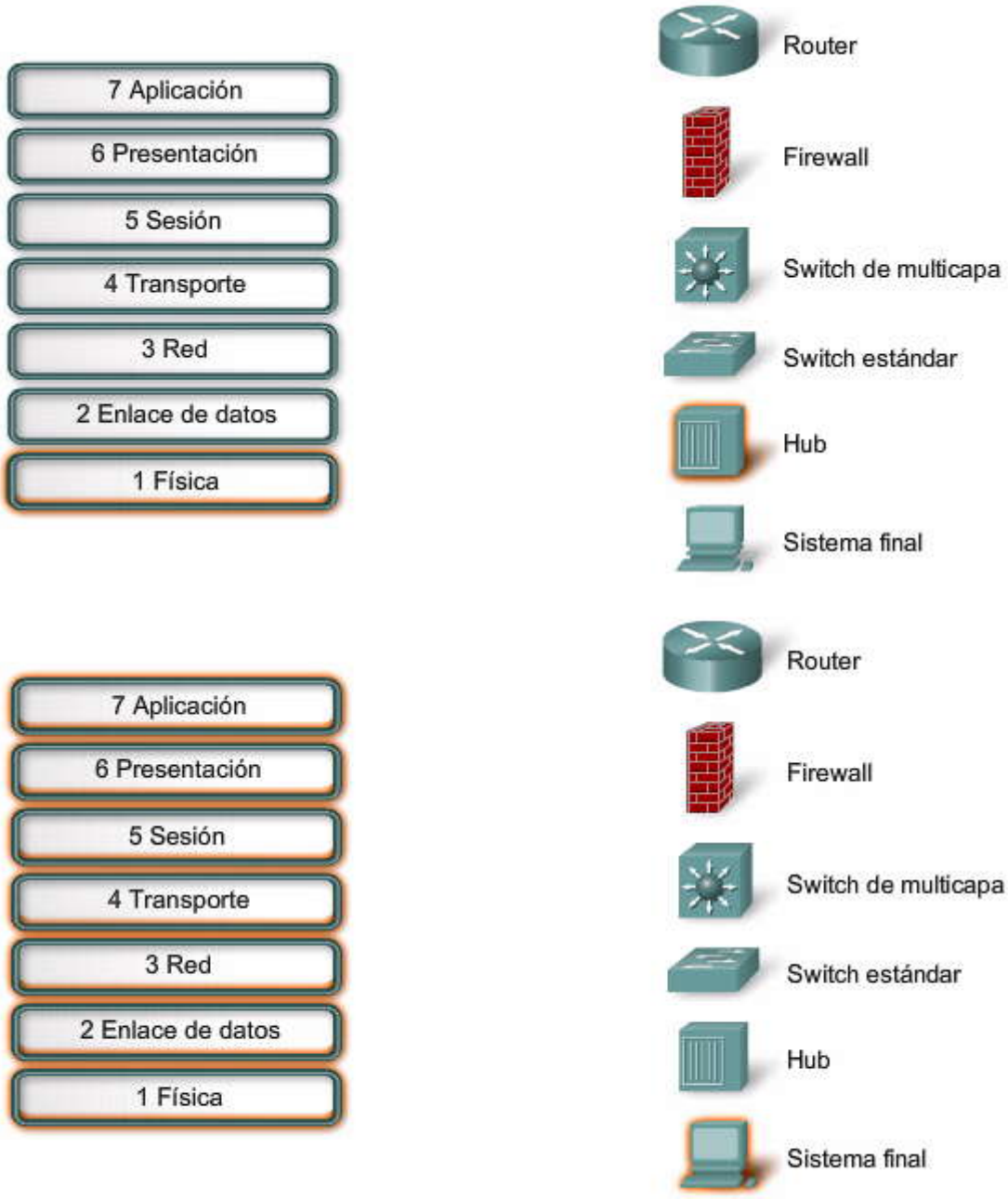

Firewall


Switch de multicapa


Switch estándar


Hub


Sistema final



8.2.3 Procedimientos generales de resolución de problemas

Las etapas del proceso general de resolución de problemas son las siguientes:

- **Etapa 1. Recopilación de síntomas**: la resolución de problemas comienza con el proceso de recopilación y documentación de los síntomas de la red, los sistemas finales y los usuarios. Además, el administrador de red determina cuáles componentes de la red se vieron afectados y cómo cambió la funcionalidad de la red en comparación con la línea de base. Los síntomas pueden aparecer en varias formas diferentes, incluso en alertas del sistema de administración de redes, mensajes de la consola y quejas de usuarios.

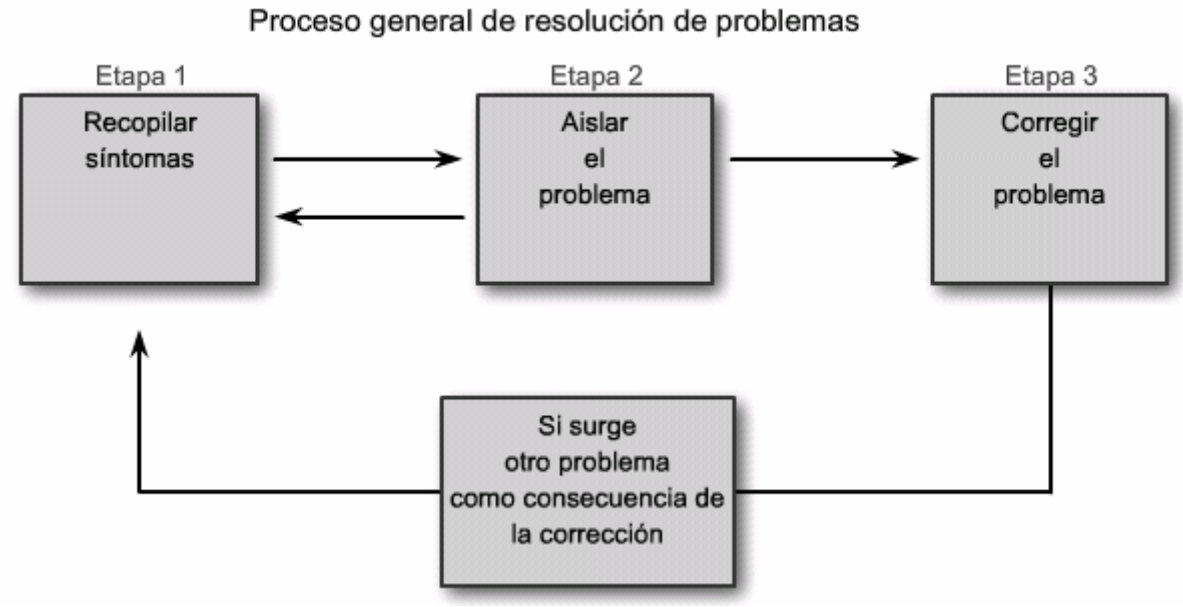
Mientras se recopila información sobre los síntomas, deben realizarse preguntas para reducir el problema a un rango menor de posibilidades.

- **Etapa 2. Aislamiento del problema**: el problema no se aísla realmente hasta que se identifica un solo problema o un conjunto de problemas relacionados. Para esto, el administrador de red examina las características de los problemas en las capas lógicas de la red de manera que pueda seleccionarse la causa más probable. En esta etapa, el administrador de red puede recopilar y documentar más síntomas según las características del problema que se identifiquen.

- **Etapa 3. Corrección del problema**: una vez que se identificó y aisló la causa del problema, el administrador de red trabaja para corregir el problema mediante la implementación, prueba y documentación de una solución. Si el administrador de red determina que la acción correctiva ha generado otro problema, se documenta el intento de solución, se eliminan los cambios y el administrador de red vuelve a recopilar síntomas y a aislar el problema.

Estas etapas no se excluyen mutuamente. En cualquier momento del proceso, puede ser necesario volver a las etapas anteriores. Por ejemplo, es posible que sea necesario recopilar más síntomas mientras se aísla el problema. Además, cuando se intenta corregir un problema, podría crearse otro problema no identificado. Como resultado, sería necesario recopilar síntomas, aislar y corregir el nuevo problema.

Debe establecerse una política de resolución de problemas para cada etapa. Una política proporciona una manera sistemática para llevar a cabo cada etapa. Parte de la política debe incluir la documentación de toda la información importante.



8.2.4 Métodos de resolución de problemas

Métodos de resolución de problemas

Hay tres métodos principales para resolver problemas en las redes:

- Ascendente
- Descendente
- Divide y vencerás

Cada enfoque tiene sus ventajas y desventajas. Este tema describe los tres métodos y proporciona pautas para la selección del mejor método para una situación específica.

Método ascendente de resolución de problemas

En la resolución de problemas ascendente, se comienza con los componentes físicos de la red y se asciende por las capas del modelo OSI hasta que se logra identificar la causa del problema. La resolución de problemas ascendente es un buen enfoque cuando se sospecha que el problema es físico. La mayor parte de los problemas de networking se encuentra en los niveles inferiores; por este motivo, la implementación del enfoque ascendente a menudo tiene resultados efectivos. La figura muestra el enfoque ascendente para resolver problemas.

La desventaja del enfoque ascendente para la resolución de problemas es que requiere la revisión de cada dispositivo e interfaz de la red hasta que se descubra la posible causa del problema. Recuerde que debe documentarse cada conclusión y posibilidad, por lo que este enfoque puede implicar mucho trabajo administrativo. Un desafío mayor es determinar qué dispositivos examinar primero.

Haga clic en el botón Método descendente en la figura.
Método descendente de resolución de problemas

En la resolución de problemas descendente, se comienza con las aplicaciones de usuario final y se desciende por las capas del modelo OSI hasta que se logra identificar la causa del problema. Las aplicaciones de usuario final de un sistema final se prueban antes de abordar las elementos de networking más específicos. Use este enfoque paraproblemas más simples o cuando crea que el problema corresponde a un elemento de software.

La desventaja del enfoque descendente es que requiere la revisión de cada aplicación de red hasta que se descubra la posible causa del problema. Cada conclusión o posibilidad debe documentarse, y el desafío es determinar qué aplicación se examinará primero.

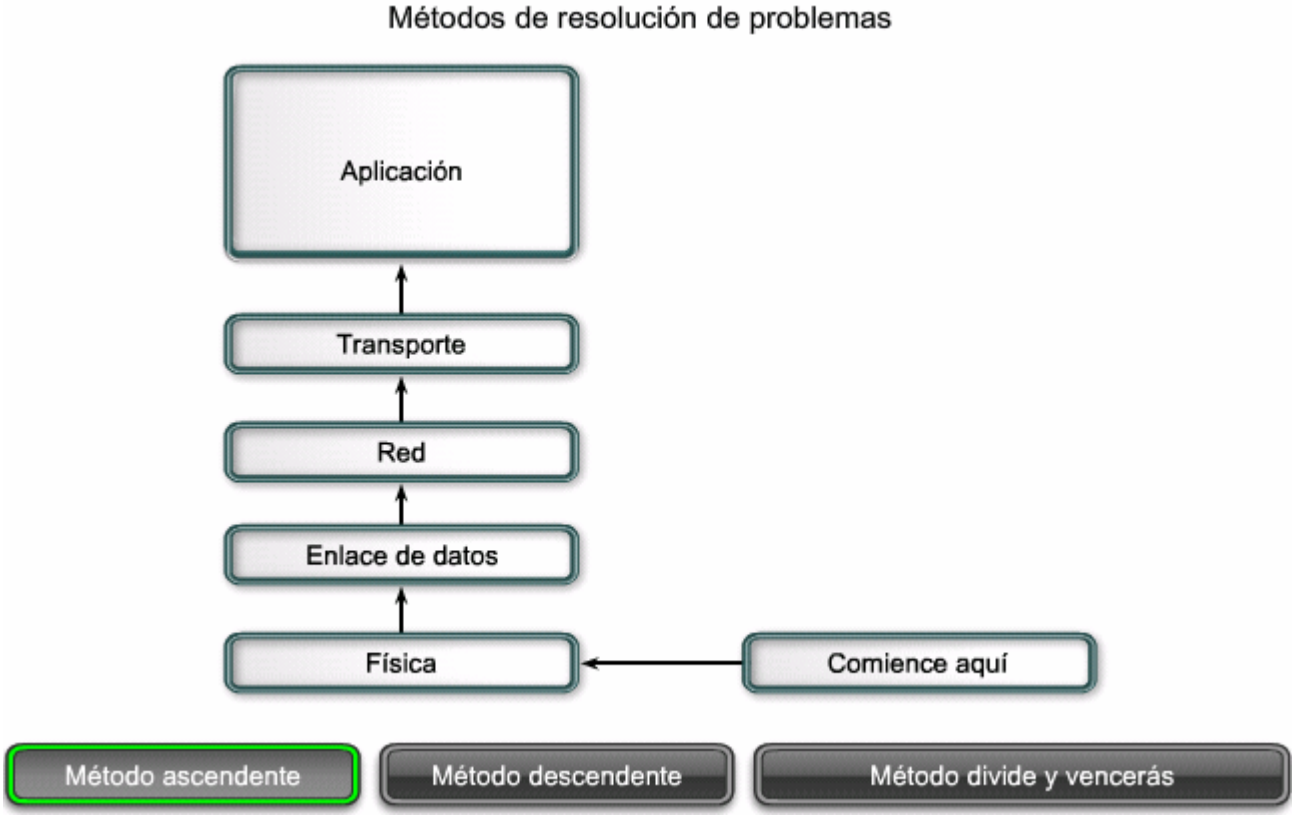
Haga clic en el botón Método divide y vencerás en la figura.

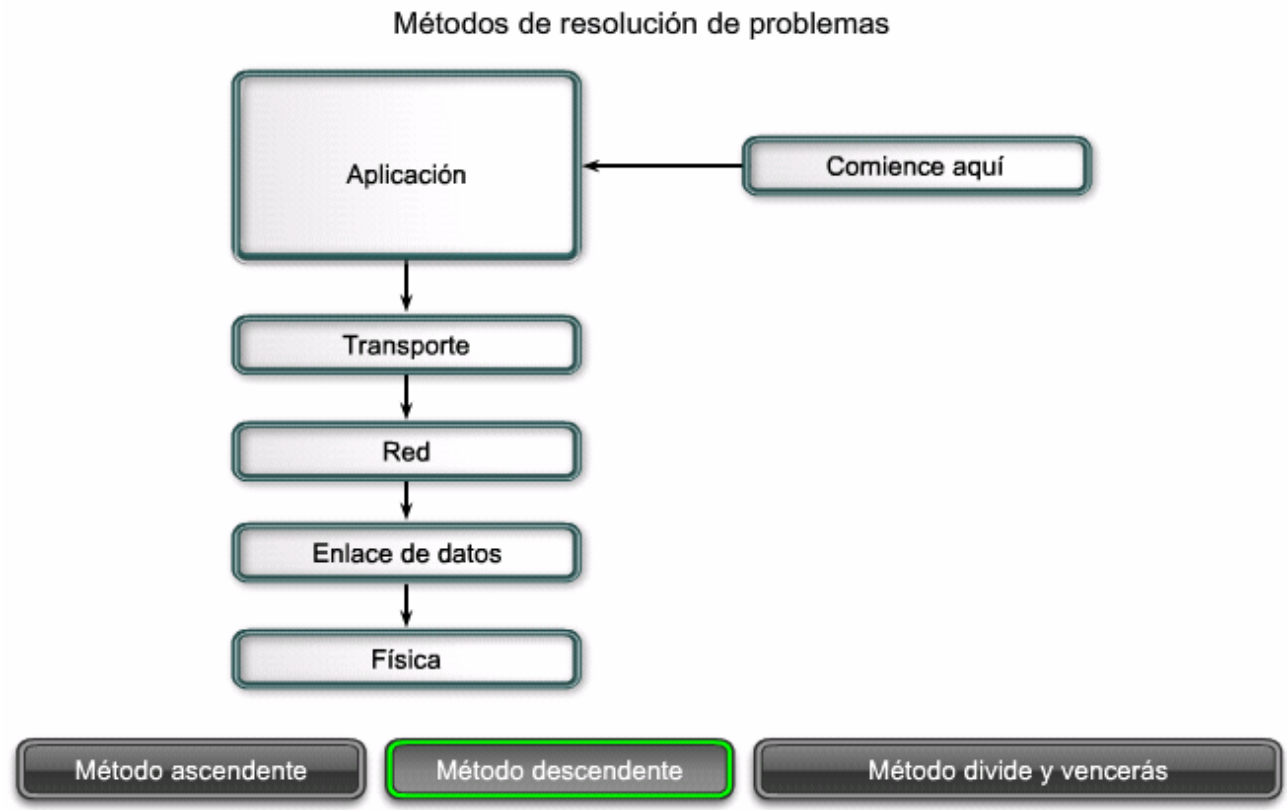
Método de resolución de problemas divide y vencerás

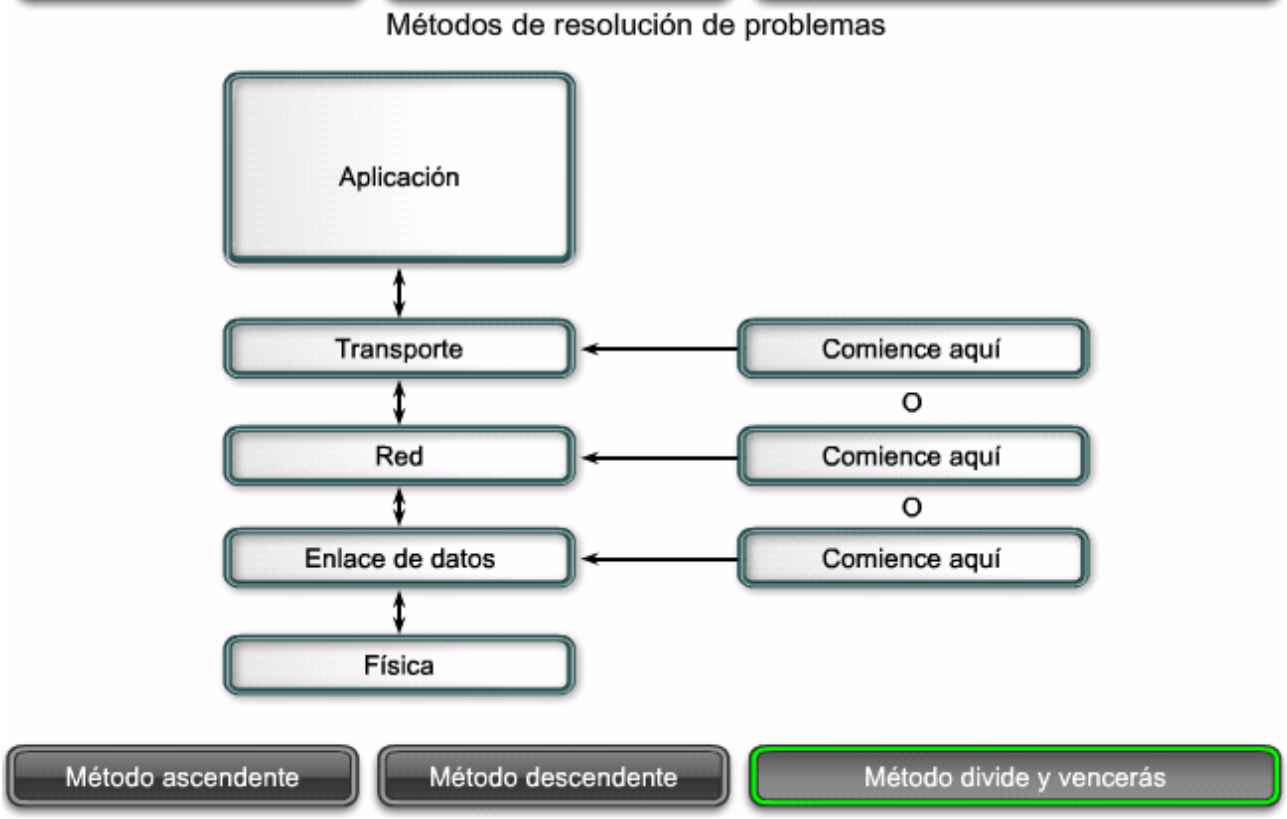
Cuando se aplica el enfoque divide y vencerás para solucionar un problema de red, se selecciona una capa y se realizan pruebas en las dos direcciones desde la capa inicial.

En la resolución de problemas con el método divide y vencerás, se comienza por recopilar la experiencia del usuario acerca del problema, documentar los síntomas y, luego, con esa información, realizar una suposición informada sobre en cuál capa de OSI se comenzará la investigación. Una vez que se verifica que una capa funciona correctamente, se supone que las capas debajo de esa están funcionando y se sigue con las capas de OSI superiores. Si una capa de OSI no funciona correctamente, es necesario desplazarse en sentido descendente por el modelo de capa OSI.

Por ejemplo, si los usuarios no pueden acceder al servidor Web y es posible hacer ping al servidor, se sabe que el problema está por encima de la capa 3. Si no se puede hacer ping al servidor, se sabe que el problema está en una capa de OSI inferior.





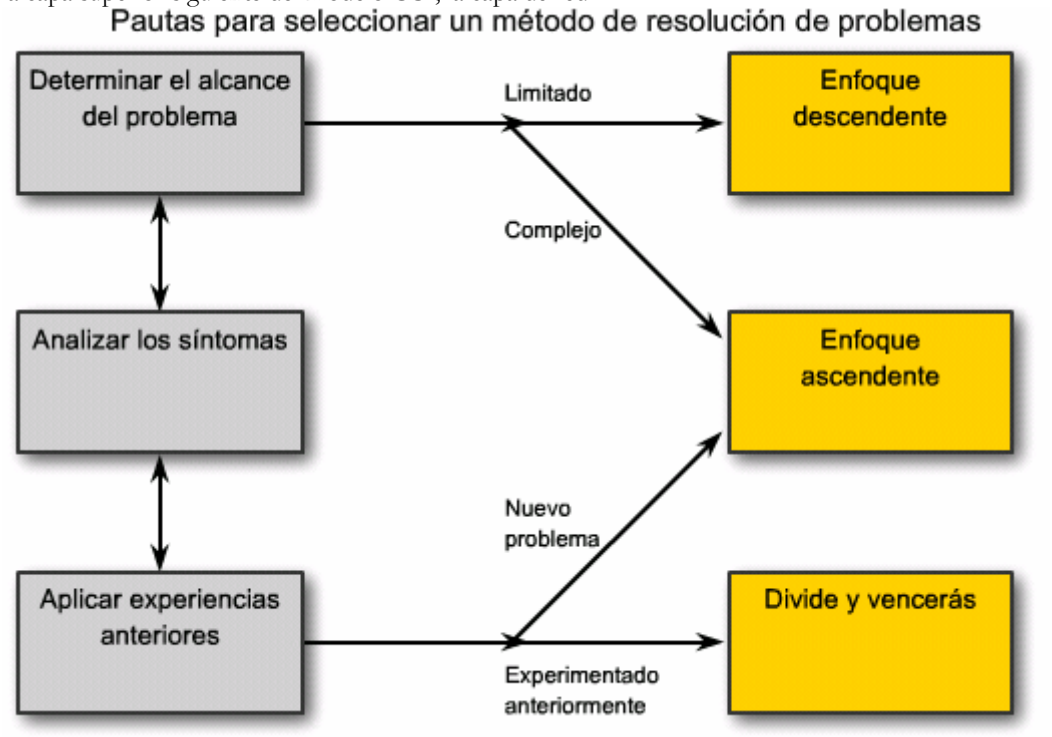


Pautas para seleccionar un método de resolución de problemas

Para resolver rápidamente problemas de red, dedique un tiempo a seleccionar el método más eficaz para la resolución de problemas. Examine la figura. Use el proceso que se muestra en la figura como ayuda para seleccionar el método más eficaz para la resolución de problemas.

Aquí se presenta un ejemplo de cómo se seleccionaría un método para la resolución de un problema específico. Dos routers IP no están intercambiando información de enrutamiento. La última vez que ocurrió este tipo de problema, fue debido a un

problema de protocolo. Por lo tanto, se selecciona el método divide y vencerás para la resolución de problemas. El análisis muestra que hay conectividad entre los routers, por lo que se comienzan los esfuerzos de resolución de problemas en la capa física o de enlace de datos, se confirma la conectividad y se empieza la prueba de las funciones relacionadas con TCP/IP en la capa superior siguiente del modelo OSI, la capa de red.



8.2.5 Recopilación de síntomas

Recopilación de síntomas

Para determinar el alcance del problema, recopile (y documente) los síntomas. La figura muestra el diagrama de flujo de este proceso. A continuación, se describe brevemente cada paso de este proceso:

Paso 1. Análisis de los síntomas actuales: se analizan los síntomas recopilados de los informes de problemas, usuarios o sistemas finales afectados por el problema a fin de obtener una definición de éste.

Paso 2. Determinación de propiedad: si el problema se encuentra dentro de su sistema, puede pasar a la etapa siguiente. Si el problema está fuera de los límites bajo su control, por ejemplo, la pérdida de conectividad a Internet fuera del sistema autónomo, debe comunicarse con un administrador para el sistema externo antes de recopilar síntomas adicionales de la red.

Paso 3. Reducción del alcance: se debe determinar si el problema está en la capa núcleo, de distribución o de acceso de la red. En la capa identificada, analice los síntomas existentes y use su conocimiento de la topología de la red para determinar qué elementos de equipamiento son la causa más probable.

Paso 4. Recopilación de síntomas de dispositivos sospechosos: mediante un enfoque de resolución de problemas en capas, se recopilan síntomas del hardware y software de los dispositivos sospechosos. Comience con la posibilidad más probable y use el conocimiento y la experiencia para determinar si es más probable que el problema sea de configuración de hardware o software.

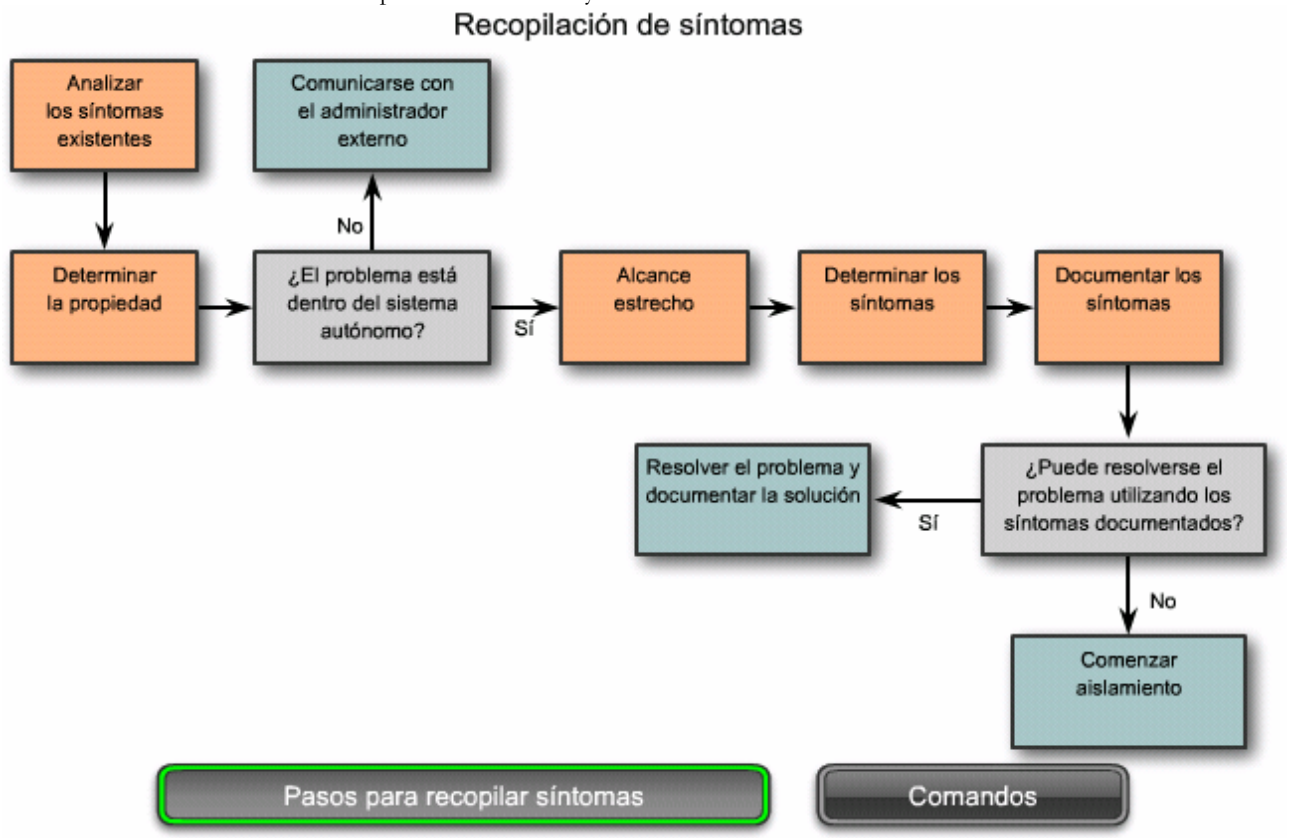
Paso 5. Documentación de síntomas: a veces, el problema puede resolverse utilizando los síntomas documentados. En caso contrario, se comienza con la etapa de aislamiento del proceso general de resolución de problemas.

Haga clic en el botón Comandos que aparece en la figura.

Use los comandos del IOS de Cisco para recopilar síntomas acerca de la red. La tabla de la figura describe los comandos comunes del IOS de Cisco que pueden usarse como ayuda para recopilar los síntomas de un problema de red.

Aunque el comando **debug** es una herramienta importante para recopilar síntomas, genera una gran cantidad de tráfico de mensajes de consola y puede afectar significativamente el rendimiento de un dispositivo de red. Asegúrese de advertir a los

usuarios de la red que se está realizando un intento de resolución de problemas y que el rendimiento de la red puede verse afectado. Recuerde deshabilitar la depuración cuando haya terminado.



Recopilación de síntomas

Comando	Descripción
ping *{host | ip-address}*	Envía un paquete de solicitud de eco a una dirección y espera una respuesta. La variable *host | ip-address* es el alias IP o la dirección IP del sistema objetivo.
traceroute *{destination}*	Identifica la ruta que recorre un paquete a través de las redes. La variable de destino es el nombre de host o la dirección IP del sistema objetivo.
telnet *{host | ip-address}*	Se conecta con una dirección IP usando la aplicación Telnet.
show ip interface brief	Muestra un resumen del estado de todas las interfaces en un dispositivo.
show ip route	Muestra el estado actual de la tabla de enrutamiento IP.
show running-config interface	Muestra el contenido del archivo de configuración actualmente en ejecución para una interfaz en particular.
[no] debug ?	Muestra una lista de opciones para habilitar o deshabilitar eventos de depuración en un dispositivo.
show protocols	Muestra los protocolos configurados y muestra el estado global y específico por interfaz de cualquier protocolo de Capa 3 configurado.

Pasos para recopilar síntomas | Comandos

Preguntas a usuarios finales

Cuando formule preguntas a usuarios finales acerca de un problema de red que pueden estar experimentando, use técnicas de interrogación efectivas. De esta manera, obtendrá la información necesaria para documentar de forma eficaz los síntomas de un problema La tabla de la figura proporciona algunas pautas y preguntas de ejemplo para los usuarios finales.

Preguntas a usuarios finales

Pautas	Preguntas de ejemplo para los usuarios finales
Hacer preguntas pertinentes al problema.	¿Qué no funciona?
Utilizar cada pregunta como un medio para eliminar o descubrir posibles problemas.	¿Están relacionados los aspectos que funcionan con aquellos que no lo hacen?
Hablar sobre los aspectos técnicos de forma que el usuario pueda comprender.	¿El aspecto que no funciona funcionó alguna vez?
Preguntar al usuario cuándo advirtió el problema por primera vez.	¿Cuándo se advirtió el problema por primera vez?
¿Sucedió algo inusual desde la última vez que funcionó?	¿Qué se ha modificado desde la última vez que funcionó?
Pedir al usuario que realice la recreación del problema, si es posible.	¿Puede reproducir el problema?
Determinar la secuencia de eventos que se produjeron antes de que ocurriera el problema.	¿Cuándo se produjo el problema exactamente?

8.2.6 Herramientas de resolución de problemas

Herramientas de resolución de problemas de software

Existe una gran variedad de herramientas de software y hardware disponibles para facilitar la resolución de problemas. Estas herramientas pueden emplearse para recopilar y analizar los síntomas de los problemas de red y, a menudo, proporcionan funciones de supervisión y generación de informes que pueden usarse para establecer la línea de base de la red.

Herramientas de NMS

Las herramientas del sistema de administración de red (NMS) incluyen herramientas de supervisión, configuración y administración de fallas de los dispositivos. La figura muestra una pantalla de ejemplo del software de NMS What's Up Gold. Estas herramientas pueden usarse para investigar y corregir problemas de red. El software de supervisión de redes presenta de manera gráfica una vista física de los dispositivos de la red y permite que los administradores de red supervisen los dispositivos remotos sin necesidad de revisarlos físicamente. El software de administración de dispositivos proporciona el estado dinámico, estadísticas e información de configuración de los productos conmutados. Algunos ejemplos de herramientas de administración de redes usadas con frecuencia son CiscoView, HP Openview, Solar Winds y What's Up Gold.

Haga clic en el botón Base de conocimientos en la figura para ver un ejemplo de un sitio Web de base de conocimientos.

Bases de conocimientos

Las bases de conocimientos en línea de los proveedores de dispositivos de red se han convertido en fuentes indispensables de información. Cuando las bases de conocimientos de los proveedores se combinan con motores de búsqueda de Internet, como Google, el administrador de red tiene acceso a un amplio conjunto de información basada en experiencias.

La figura muestra la página **Herramientas y recursos** de Cisco, que se encuentra en http://www.cisco.com. Ésta es una herramienta gratuita que proporciona información sobre hardware y software relacionado con Cisco. Contiene procedimientos de resolución de problemas, guías de implementación e informes originales acerca de la mayoría de los aspectos de la tecnología de networking.

Haga clic en el botón Herramientas de línea de base en la figura para ver algunos ejemplos de herramientas para establecer líneas de base.

Herramientas de línea de base

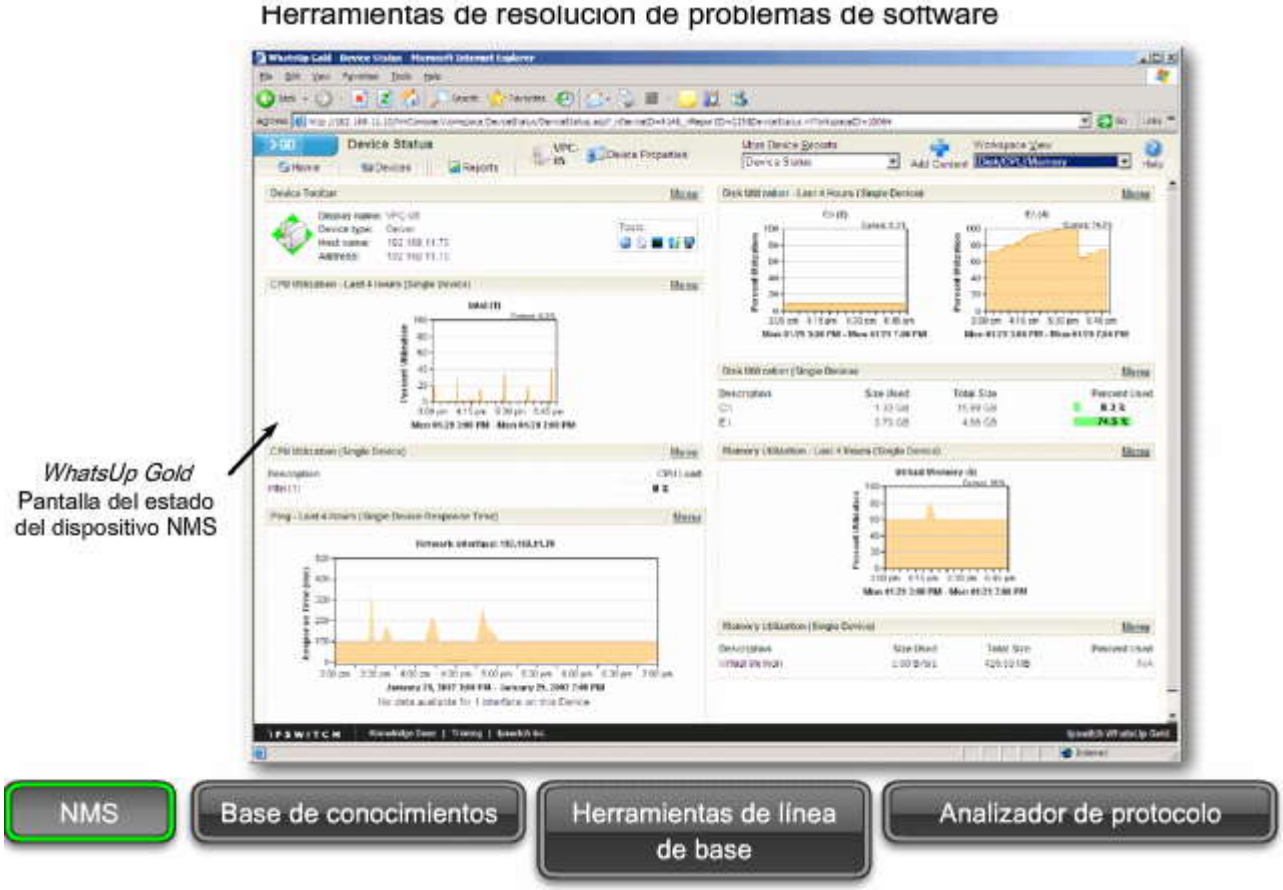
Están disponibles muchas herramientas para la automatización del proceso de creación de líneas de base y documentación de la red. Estas herramientas están disponibles para los sistemas operativos Windows,Linux y AUX. La figura muestra una captura de pantalla de las aplicaciones de software SolarWinds LANsurveyor y CyberGauge. Las herramientas de línea de base ofrecen ayuda con tareas frecuentes de documentación de línea de base. Por ejemplo, pueden servircomo ayuda para

dibujar diagramas de red, mantener actualizada la documentación de software y hardware de la red y medir de manera rentable el uso de ancho de banda de línea de base.

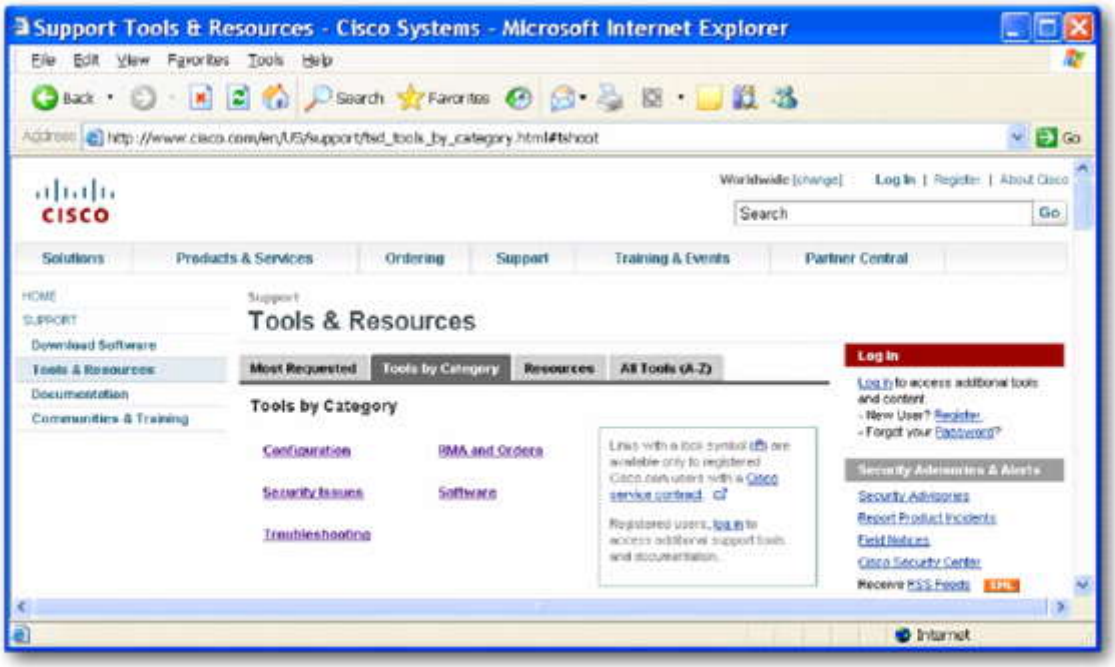
Haga clic en el botón Analizador de protocolo en la figura para ver un ejemplo de una aplicación de analizador de protocolo típica.

Analizadores de protocolo

Un analizador de protocolo decodifica las distintas capas de protocolo en una trama registrada y presenta esta información en un formato relativamente fácil de usar. La figura muestra una captura de pantalla del analizador de protocolo Wireshark. La información que muestra el analizador de protocolo incluye datos de la capa física, de enlace de datos y de protocolo, y las descripciones para cada trama. La mayoría de los analizadores de protocolo pueden filtrar el tráfico que cumple con ciertos criterios de manera que, por ejemplo, pueda capturarse todo el tráfico desde un dispositivo particular y hacia éste.

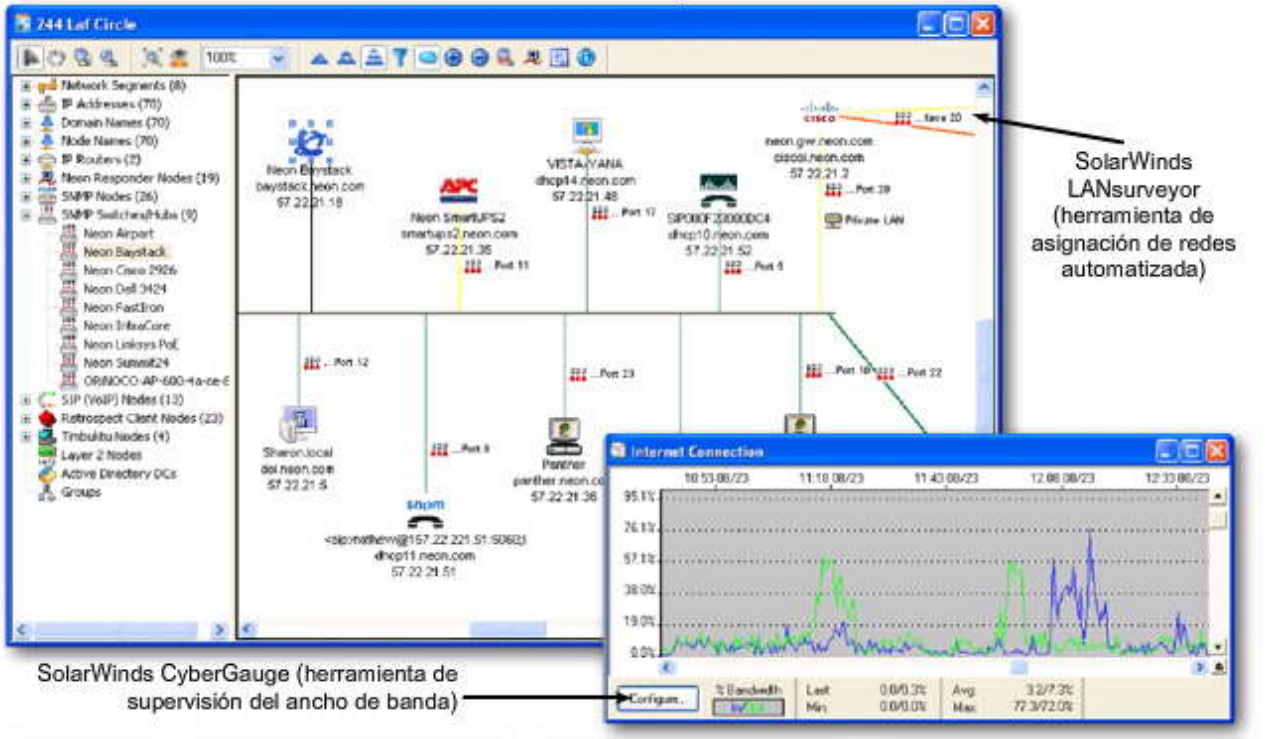


Herramientas de resolucion de problemas de software

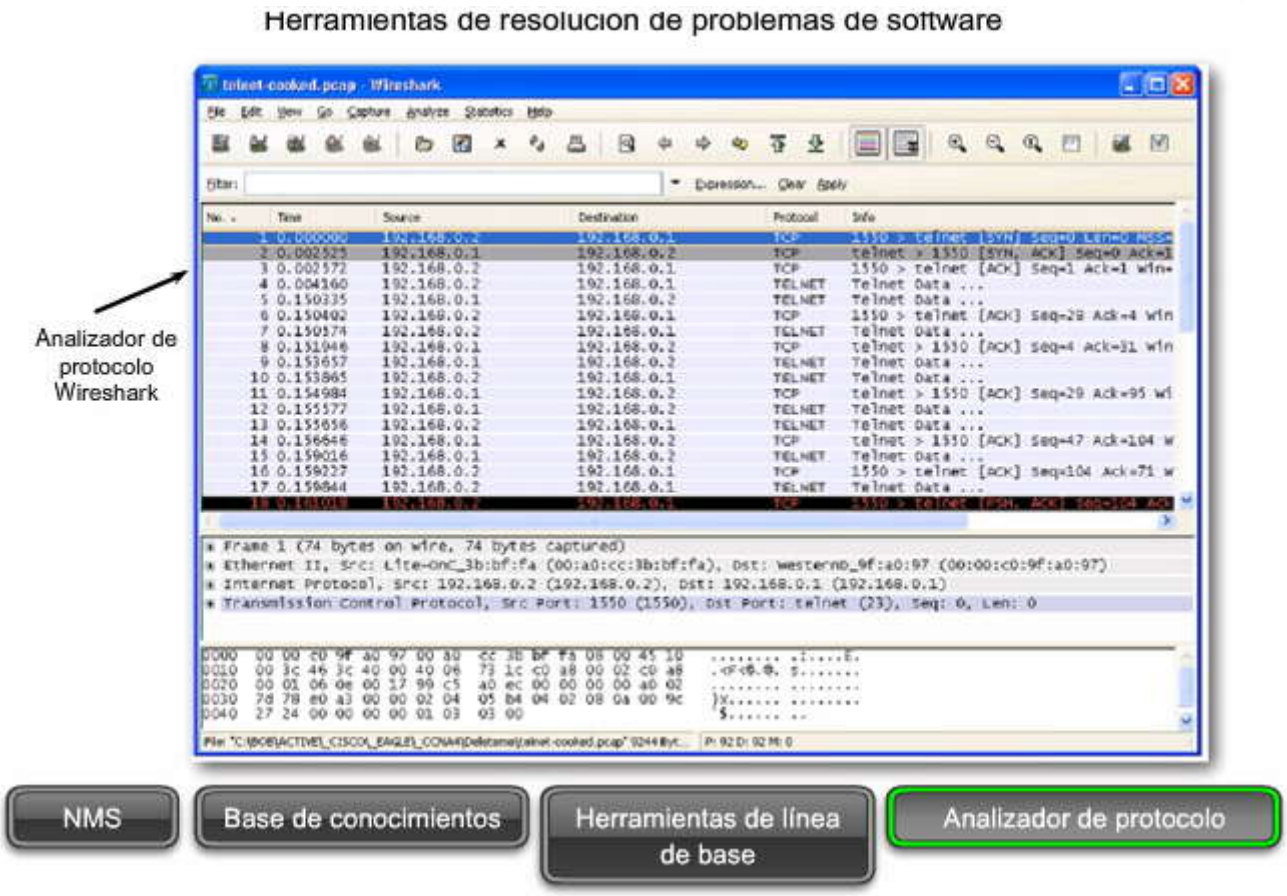


NMS | Base de conocimientos | Herramientas de línea de base | Analizador de protocolo

Herramientas de resolucion de problemas de software



NMS | Base de conocimientos | Herramientas de línea de base | Analizador de protocolo



Herramientas de resolución de problemas de hardware

Haga clic en los botones de la figura para ver ejemplos de diversas herramientas de resolución de problemas de hardware.

Módulo de análisis de red

Es posible instalar un módulo de análisis de red (NAM) en los switches de la serie Cisco Catalyst 6500 y en los routers de la serie Cisco 7600 a fin de obtener una representación gráfica del tráfico desde los switches y routers locales y remotos. El NAM es una interfaz integrada basada en el explorador que genera informes sobre el tráfico que consume recursos críticos de la red. Además, el NAM puede capturar y decodificar paquetes y rastrear los tiempos de respuesta para detectar un problema de aplicación en la red o el servidor.

Multímetros digitales

Los multímetros digitales (DMM) son instrumentos de prueba que se usan para medir directamente valores eléctricos de voltaje, corriente y resistencia. En la resolución de problemas de red, la mayoría de las pruebas multimedia incluyen la verificación de los niveles de voltaje de la fuente de energía y la comprobación de que los dispositivos de red están recibiendo energía.

Probadores de cable

Los probadores de cable son dispositivos de mano especializados diseñados para probar los distintos tipos de cableado para la comunicación de datos. Los probadores de cable pueden usarse para detectar cables dañados o cruzados, conexiones en corto y conexiones asignadas incorrectamente. Estos dispositivos pueden ser probadores de continuidad económicos, probadores de cable de datos no demasiado caros o reflectómetros de dominio de tiempo (TDR) caros.

Los TDR se usan para establecer la distancia hasta una ruptura en un cable. Estos dispositivos envían señales a lo largo del cable y esperan a que éstas se reflejen. El tiempo entre el envío de la señal y su devolución se convierte a una medida de distancia. La función del TDR en general se incluye en los probadores de cable de datos. Los TDR que se usan para probar los cables de fibra óptica se denominan reflectómetros ópticos de dominio de tiempo (OTDR).

Analizadores de red

Los analizadores de cable son dispositivos de mano multifuncionales que se usan para probar y certificar los cables de cobre y fibra para diferentes servicios y estándares. Las herramientas más sofisticadas incluyen el diagnóstico avanzado para resolución de problemas, que permite medir la distancia al defecto de rendimiento (NEXT, RL), identificar las acciones correctivas y mostrar gráficamente el comportamiento de crosstalk y de impedancia. Los analizadores de cable también incluyen, en general, software de PC. Una vez que se recopilan los datos de campo, el dispositivo de mano puede cargar los datos y permite crear informes actualizados y precisos.

Analizadores de red portátiles

Dispositivos portátiles que se usan para la resolución de problemas en redes conmutadas y VLAN. Mediante la conexión del analizador de red en cualquier lugar de la red, un ingeniero de red puede ver el puerto del switch al cual está conectado el dispositivo y la utilización máxima y promedio. También puede usarse el analizador para detectar la configuración de VLAN, identificar los principales sistemas de comunicación de red, analizar el tráfico de red y ver detalles de la interfaz. El dispositivo puede, generalmente, mostrar los resultados en una PC con software de supervisión de redes instalado a fin de permitir el análisis detallado y la resolución de problemas.

Herramientas de resolución de problemas de hardware

Aplicación basada en la Web que muestra los datos del analizador de tráfico NAM

Módulo NAM para un Catalyst 6500

NAM | DMM | Analizador de red | Analizador de red | Analizador de red

Herramientas de resolución de problemas de hardware

Multímetro digital Fluke 179

NAM | DMM | Analizador de red | Analizador de red | Analizador de red

Herramientas de resolución de problemas de hardware

Fluke Networks LinkRunner Pro Tester

Fluke Networks CableIQ Qualification Tester

NAM | DMM | Analizador de red | Analizador de red | Analizador de red

Herramientas de resolución de problemas de hardware

Analizador de cables Fluke Networks DTX

NAM | DMM | Analizador de red | **Analizador de red** | Analizador de red

Herramientas de resolución de problemas de hardware

Analizador de red integrado Fluke Networks OptiView™ Serie III

NAM | DMM | Analizador de red | Analizador de red | **Analizador de red**

Actividad de investigación

Los siguientes son enlaces a varias herramientas de resolución de problemas.

Herramientas de software

Sistemas de administración de redes:

http://www.ipswitch.com/products/whatsup/index.asp?t=demo

http://www.solarwinds.com/products/network_toolsaspx

Herramientas de línea de base:

http://www.networkuptime.com/tools/enterprise/

Bases de conocimientos:

http://www.cisco.com

Analizadores de protocolo:

http://www.flukenetworks.com/fnet/en-us/products/OptiView+Protocol+Expert/

Herramientas de hardware

Módulo analizador de red (NAM) de Cisco:

http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_software/3.5/user/guide/user.html

Probadores de cable:

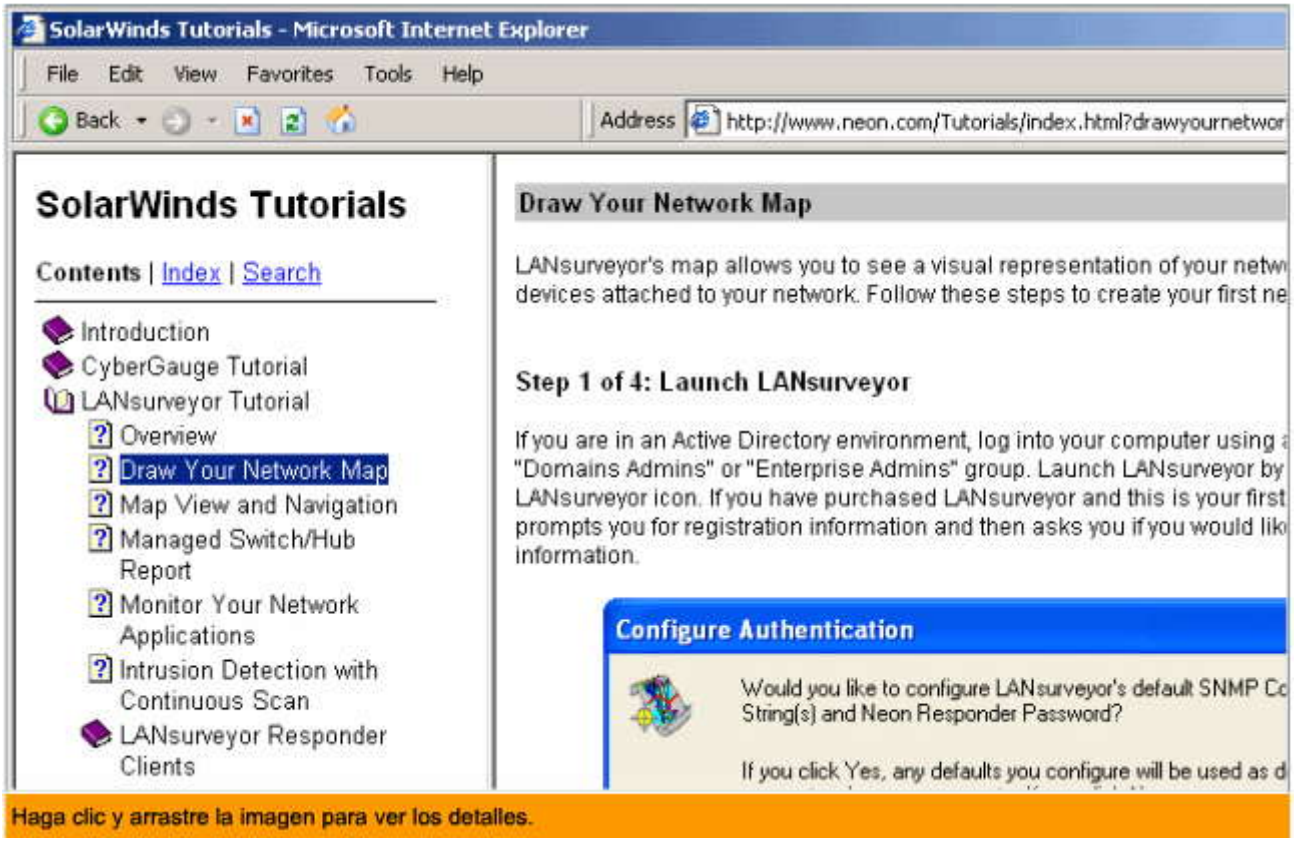
http://www.flukenetworks.com/fnet/en-us/products/CableIQ+Qualification+Tester/Demo.htm

Analizadores de cable:

http://www.flukenetworks.com/fnet/en-us/products/DTX+CableAnalyzer+Series/Demo.htm

Analizadores de red:

http://www.flukenetworks.com/fnet/en-us/products/OptiView+Series+III+Integrated+Network+Analyzer/Demos.htm



8.3 Problemas frecuentes en la implementación de WAN

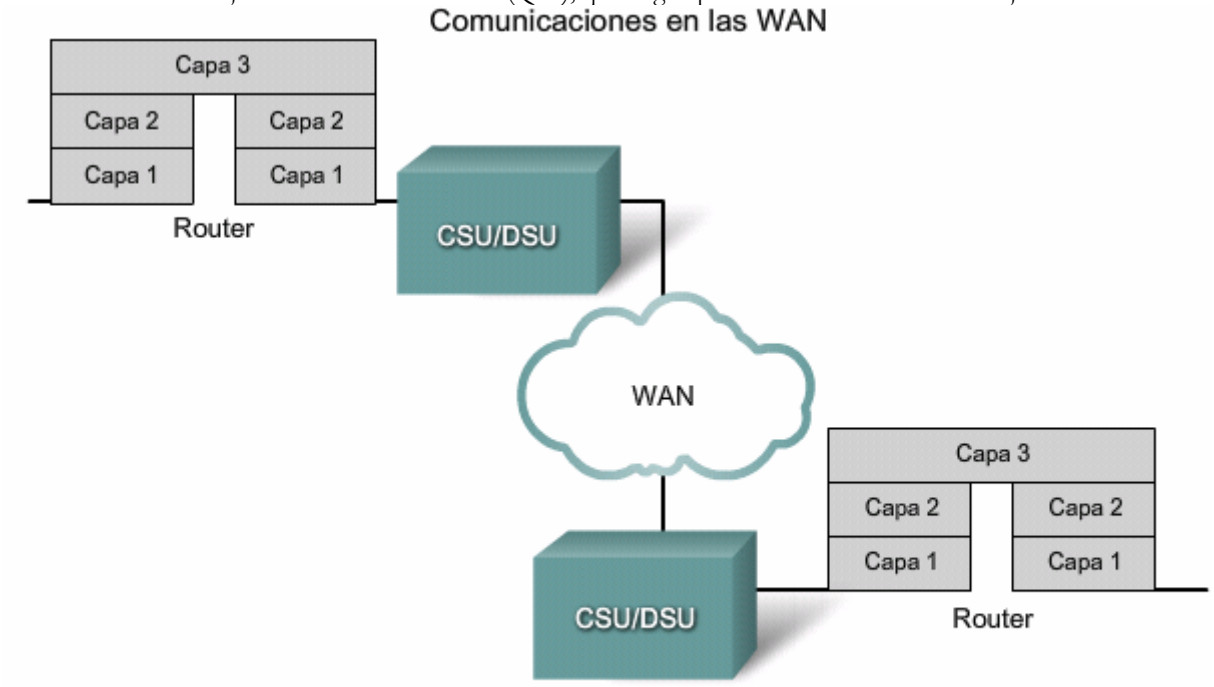
8.3.1 Comunicaciones en las WAN

Un proveedor de comunicaciones o una empresa de comunicaciones común, en general, es dueño de los enlaces de datos que componen una WAN. Los enlaces están disponibles a los suscriptores por una tarifa y se utilizan para interconectar las LAN o conectar redes remotas. La velocidad de transmisión de datos en una WAN (ancho de banda) es mucho menor al ancho de banda común de una LAN. Los costos de provisión de enlace son el elemento más caro, por lo tanto, la implementación de WAN debe buscar proveer un máximo de ancho de bandaa un costo aceptable. Con la presión por parte de los usuarios para obtener mayor acceso al servicio a velocidades más altas y la presión de los administradores para contener los costos, el determinar la configuración óptima de una WAN no es una tarea fácil.

Las WAN transportan varios tipos de tráfico, tales como datos, voz y video. El diseño seleccionado debe ofrecer capacidad adecuada y tiempos de tránsito que cumplan con las necesidades de las empresas. Entre las especificaciones, el diseño debe tener en cuenta la topología de las conexiones entre varias ubicaciones, la naturaleza de aquellas conexiones y la capacidad del ancho de banda.

Las WAN más antiguas a menudo consistían de enlaces de datos directamente conectados a computadoras centrales remotas. En la actualidad, las WAN conectan las LAN que están geográficamente separadas. Las tecnologías WAN funcionan en las tres capas inferiores del modelo de referencia OSI, las estaciones de usuarios finales, servidores y routers se comunican a través de las LAN, y los enlaces de datos WAN terminan en los routers locales.

Los routers determinan la ruta más adecuada hacia el destino de los datos a partir de los encabezados de la capa de red y transfieren los paquetes a la conexión de enlace de datos indicada para su envío en la conexión física. Los routers pueden también ofrecer manejo de la calidad de servicio (QoS), que asigna prioridades a los diferentes flujos de tráfico.



Las tecnologías WAN operan en las 3 capas inferiores del modelo OSI.

8.3.2 Pasos en el diseño de las WAN

Las empresas instalan conectividad WAN para satisfacer los requisitos comerciales estratégicos del traspaso de datos entre sucursales externas. Puesto que la conectividad WAN es importante para la empresa y es cara, se debe diseñar la WAN de manera sistemática. Esta figura muestra los pasos para el diseño de una WAN.

Cada vez que se considere hacer una modificación a una WAN existente, se deben seguir estos pasos. Sin embargo, debido a que muchas WAN han evolucionado con el tiempo, es posible que no se hayan considerado muchas de las pautas aquí presentadas. Las modificaciones a las WAN pueden surgir de la expansión de los servidores WAN de la empresa o de la inclusión de nuevas prácticas de trabajo y métodos comerciales.

Éstos son los pasos para el diseño o la modificación de una WAN:

Paso 1. Ubicar las LAN: establezca los puntos finales de origen y destino que se conectarán a través de la WAN.

Paso 2. Analizar el tráfico: conozca qué tipo de tráfico de datos debe transportarse, su origen y su destino. Las WAN transportan varios tipos de tráfico con requisitos variables en términos de ancho de banda, latencia y fluctuación de fase. Para cada par de puntos finales y para cada tipo de tráfico, se necesita información sobre las distintas características del tráfico.

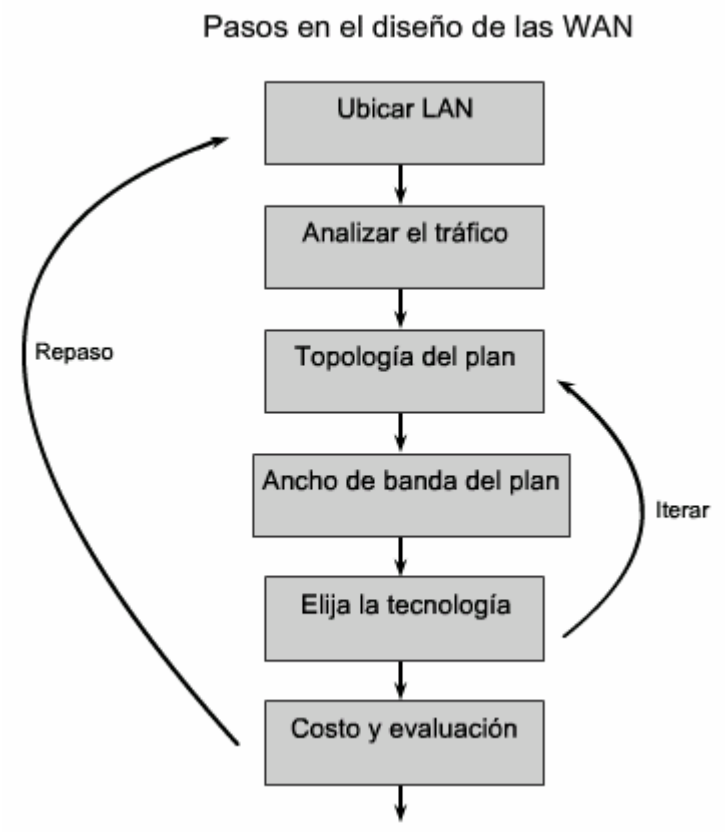
Paso 3. Planificar la topología: las cuestiones geográficas y los requisitos, como la disponibilidad, tendrán influencia en la topología. Un alto requisito de disponibilidad requiere de enlaces adicionales que ofrezcan rutas de datos alternativas y balanceo de carga.

Paso 4. Calcular el ancho de banda necesario: el tráfico en los enlaces puede tener distintos requisitos de latencia y fluctuación.

Paso 5. Seleccionar la tecnología de WAN: se deben seleccionar las tecnologías de enlace adecuadas.

Paso 6. Evaluar los costos: cuando todos los requisitos se hayan establecido, los costos de instalación y operación de la WAN se pueden determinar y comparar con la necesidad comercial que llevó a la implementación de WAN.

Como se muestra en la figura, las pasos de diseño que se describen aquí no representan un proceso lineal. Es posible que sea necesario repetir estos pasos varias veces antes de finalizar el diseño. Para mantener el rendimiento óptimo de la WAN, son necesarias la supervisión y reevaluación continuas.



8.3.3 Consideraciones sobre el tráfico de WAN

La tabla en la figura muestra la gran variedad de tipos de tráfico y los diferentes requisitos de ancho de banda, latencia y fluctuación que deben transportar los enlaces WAN.

Para determinar las condiciones del flujo de tráfico y la temporización de un enlace WAN, se deben analizar las características del tráfico específicas para cada LAN conectada a la WAN. Es posible que para determinar las características del tráfico se deba consultar a los usuarios de la red y evaluar sus necesidades.

Consideraciones sobre el tráfico de WAN

Tipos de tráfico

Tráfico	Latencia	Fluctuación de fase	Ancho de banda
Voz	Bajo	Bajo	Medio
Datos de transacción (por ejemplo, SNA)	Medio	Medio	Medio
Mensajería (correo electrónico)	Alto	Alto	Alto
Transferencia de archivos	Alto	Alto	Alto
Datos en lote	Alto	Alto	Alto
Administración de red	Alto	Alto	Bajo
Videoconferencia	Bajo	Bajo	Alto

Características de tráfico

Característica	Descripción
Conectividad y flujos de volumen	¿Hacia dónde fluye este tráfico y qué cantidad de tráfico fluye allí?
Datos de cliente/servidor	¿Qué clase de tráfico fluye entre el cliente y el servidor?
Tolerancia a la latencia, incluyendo la longitud y la variabilidad	¿Pueden los usuarios tolerar retrasos? ¿Cuántos y con qué frecuencia?
Tolerancia a la disponibilidad de la red	¿Qué importancia tiene la disponibilidad de la red para los usuarios de esta LAN? ¿Pueden tolerar interrupciones de WAN o su trabajo se detendría por completo?
Tolerancia al porcentaje de errores	¿El tráfico es ruidoso?
Prioridad	¿Este tráfico tiene prioridad en relación con otro tráfico? Por ejemplo, los mensajes de administración de la red deben tener una prioridad más alta que el correo electrónico.
Tipo de protocolo	¿Qué tipos de protocolo operan dentro de la red?
Longitud promedio de los paquetes	¿Cuál es el tamaño promedio de los paquetes que se transmiten?

8.3.4 Consideraciones sobre la topología de WAN

Luego de establecer las características del tráfico y los puntos finales de la LAN, el paso siguiente en la implementación de una WAN es diseñar una topología adecuada. El diseño de una topología de WAN consiste básicamente en lo siguiente:

Seleccionar un diseño o patrón de interconexión para los enlaces entre las diferentes ubicaciones

Seleccionar las tecnologías para que esos enlaces cumplan las necesidades de la empresa a un costo razonable

Haga clic en los botones de la figura para ver un ejemplo de cada tipo de topología de WAN.

Muchas WAN utilizan una topología en forma de estrella. A medida que la empresa crece y se agregan nuevas sucursales, éstas se conectan con la oficina central y producen una topología en forma de estrella. Algunas veces se establece una conexión cruzada con los puntos finales de la estrella y se crea, así, una topología en malla o en malla parcial. Esto posibilita muchas combinaciones de interconexión. Al diseñar, reevaluar o modificar una WAN, se debe seleccionar una topología que cumpla con los requisitos de diseño.

Al seleccionar un diseño, se deben tener en cuenta varios factores. Más enlaces aumentan el costo de los servicios de red, pero la existencia de varias rutas entre los destinos aumenta la confiabilidad. La incorporación de más dispositivos a la ruta de datos aumenta la latencia y disminuye la confiabilidad. Por lo general, cada paquete debe recibirse por completo en un nodo, antes de que se envíe al siguiente.

Haga clic en el botón Jerárquica en la figura.

Cuando deben unirse muchas ubicaciones, se recomienda una solución jerárquica. Por ejemplo, imagine una empresa que opera en todos los países de la Unión Europea y que tiene una sucursal en cada ciudad con una población superior a los

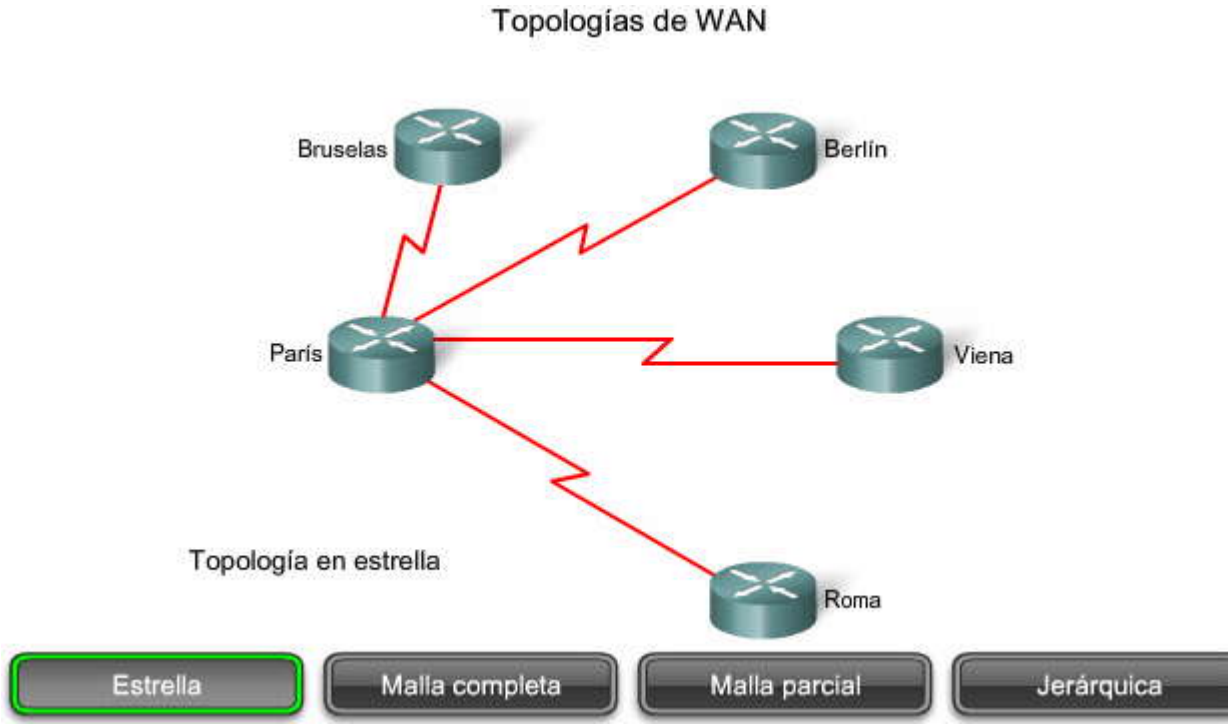
10.000 habitantes. Cada sucursal tiene una LAN, y la empresa ha decidido interconectar las sucursales. Claramente, no es posible implementar una red en malla, ya que serían necesarios cientos de miles de enlaces.

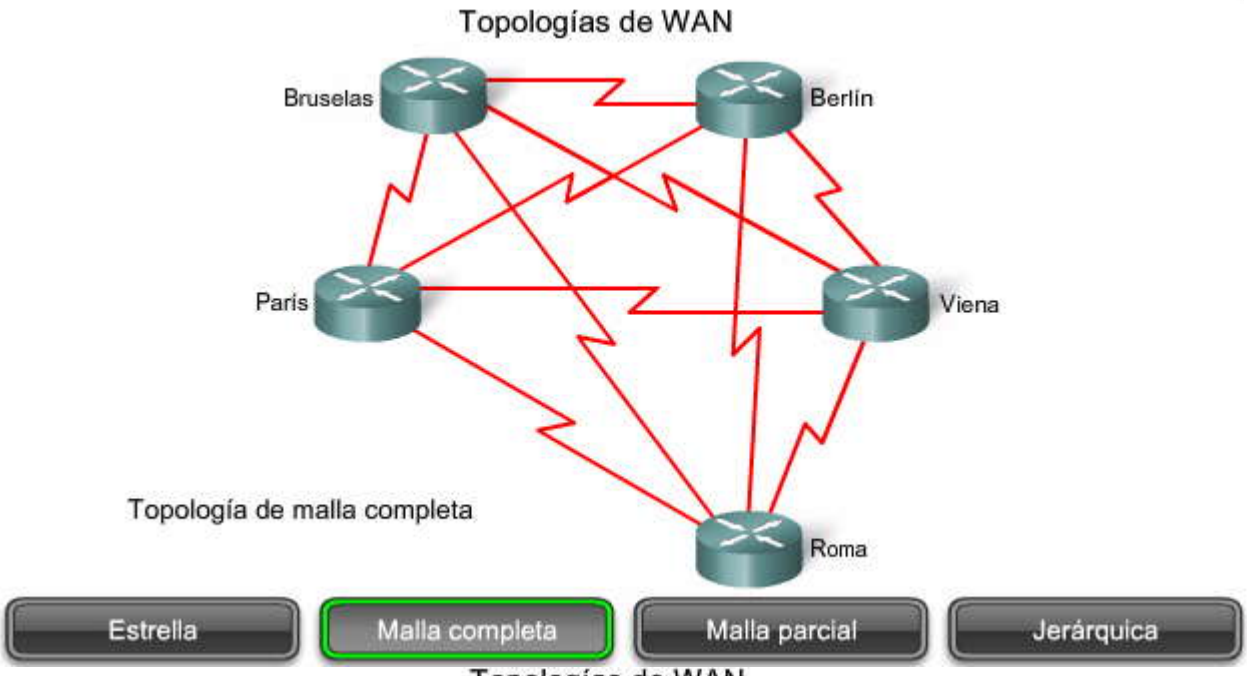
La respuesta es implementar una topología jerárquica. Se agrupan las LAN ubicadas en cada área y se las interconecta para formar una región; luego, se interconectan las regiones para formar el núcleo de la WAN. El área puede basarse en la cantidad de ubicaciones que se deben conectar, con un límite máximo entre 30 y 50. El área tendría una topología en estrella, con los hubs de las estrellas conectados para formar la región. Las regiones pueden ser geográficas y conectar entre tres y diez áreas, y el hub de cada región puede tener un enlace punto a punto.

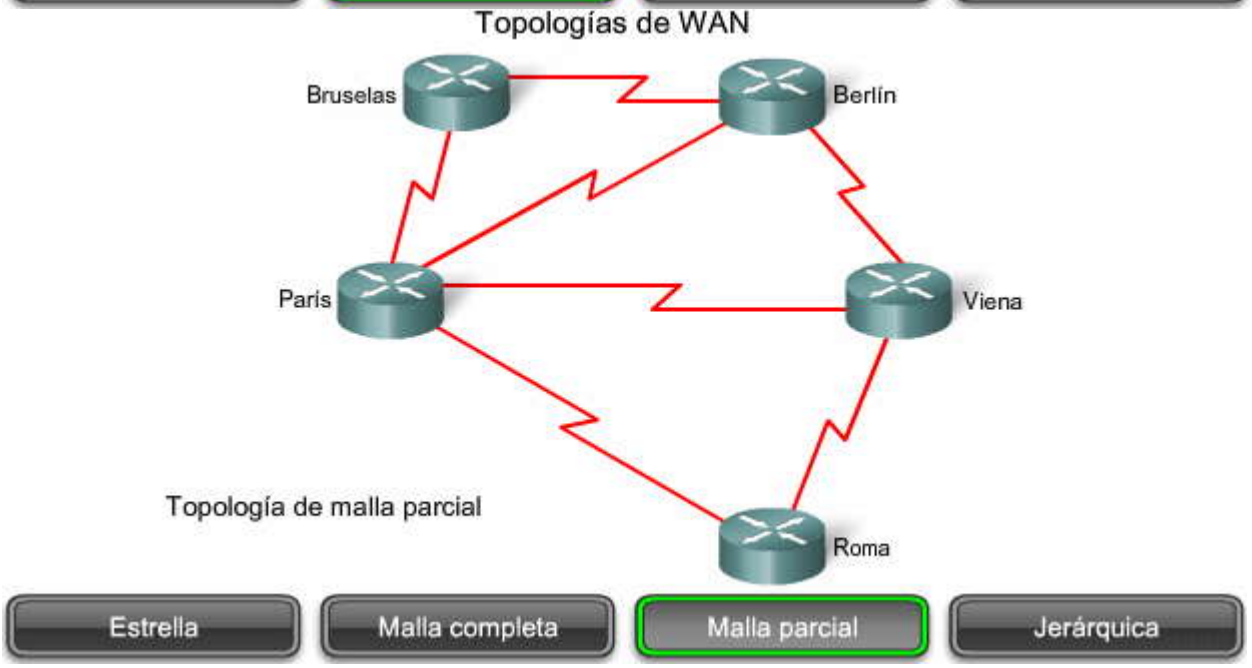
Una jerarquía de tres capas a menudo es útil cuando el tráfico de red refleja la estructura de las sucursales de la empresa y se divide en regiones, áreas y sucursales. También es útil cuando hay un servicio central al que todas las sucursales deben tener acceso, pero los niveles de tráfico son insuficientes para justificar la conexión directa de la sucursal al servicio.

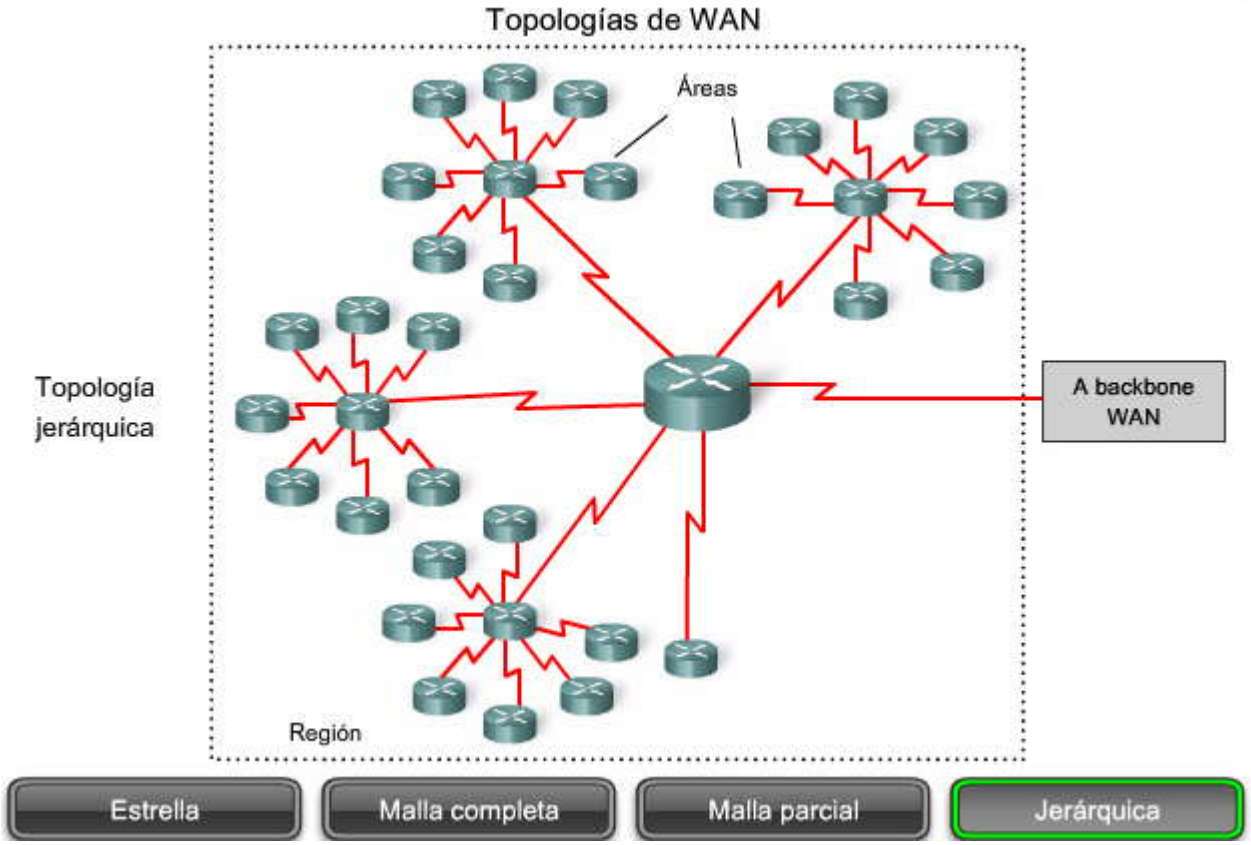
La LAN del centro del área puede tener servidores que provean servicio local y del área. Según los volúmenes y tipos de tráfico, las conexiones de acceso pueden ser dial-up, arrendadas o de Frame Relay. El Frame Relay facilita el enmallado para redundancia sin requerir conexiones físicas adicionales. Los enlaces de distribución pueden ser de Frame Relay o ATM, y el núcleo de la red puede ser ATM o de línea arrendada.

Al planear redes más sencillas, aún se debe considerar una topología jerárquica ya que ofrece una mejor escalabilidad de la red. El hub en el centro del modelo de dos capas es también un núcleo, pero no tiene otros routers núcleo conectados a él. De la misma forma, en una solución de una sola capa, el hub del área funciona como hub regional y como hub núcleo. Esto permite un crecimiento rápido y fácil en un futuro, ya que se puede reproducir el diseño básico para agregar nuevas áreas de servicio.




Topologías de WAN
Bruselas
Berlín
París
Viena
Roma
Topología de malla completa
Estrella
Malla completa
Malla parcial
Jerárquica


Topologías de WAN
Bruselas
Berlín
París
Viena
Roma
Topología de malla parcial
Estrella
Malla completa
Malla parcial
Jerárquica



Tecnologías de conexión WAN

Una WAN privada típica utiliza una combinación de tecnologías que se eligen, en general, según el tipo y el volumen del tráfico. ISDN, DSL, Frame Relay o las líneas arrendadas se utilizan para conectar sucursales individuales en una sola área. Frame Relay, ATM o las líneas arrendadas se utilizan para conectar áreas externas nuevamente al backbone. ATM o las líneas arrendadas forman el backbone de la WAN. Las tecnologías que requieren el establecimiento de una conexión antes de transmitir los datos, como el servicio telefónico básico, ISDN o X.25, no son adecuadas para las WAN que requieren un tiempo de respuesta rápido o baja latencia.

Las diferentes partes de la empresa pueden conectarse de forma directa por medio de líneas arrendadas o pueden conectarse con un enlace de acceso al punto de presencia más cercano (POP) de una red compartida. Frame Relay y ATM son ejemplos de redes compartidas. En general, las líneas arrendadas son más caras que los enlaces de acceso, pero están disponibles en casi cualquier ancho de banda y proporcionan fluctuación y latencia muy bajas.

Las redes ATM y Frame Relay transportan el tráfico de varios clientes en los mismos enlaces internos. La empresa no tiene control sobre el número de enlaces o saltos que los datos deben atravesar en la red compartida. No puede controlar el tiempo que los datos deben esperar en cada nodo antes de pasar al enlace siguiente. Esta incertidumbreen la latencia y la fluctuación hace que estas tecnologías no sean adecuadas para algunos tipos de tráfico de red. Sin embargo, los costos reducidos de una red compartida con frecuencia pueden compensar las desventajas que éstas tienen. Dado que varios clientes comparten el enlace, el costo de cada uno es, en general, menor al costo de un enlace directo de la misma capacidad.

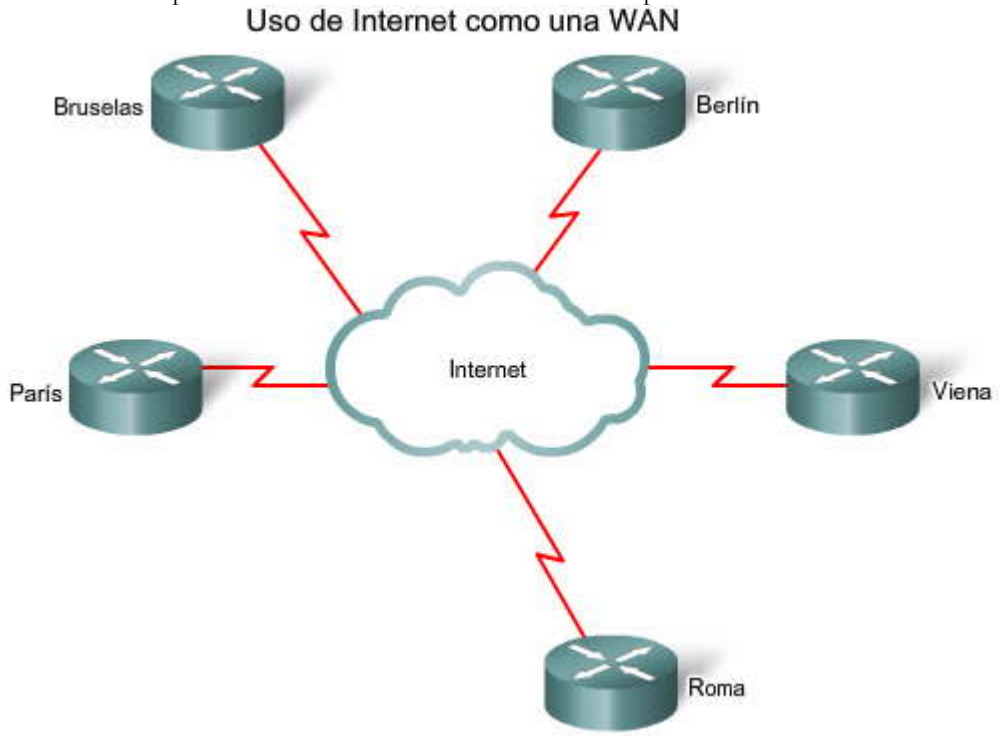
Aunque ATM es una red compartida, se diseñó para producir latencia y fluctuación mínimas a través de enlaces internos de alta velocidad que envían unidades de datos fácilmente administrables que se denominan celdas. Las celdas ATM tienen una longitud fija de 53 bytes, 48 bytes de datos y 5 bytes de encabezado. ATM se usa con frecuencia en el transporte de tráfico sensible a las demoras.

Frame Relay también se puede utilizar para el transporte de tráfico sensible a las demoras, y con frecuencia utiliza mecanismos QoS para dar prioridad a los datos más sensibles.

Tecnologías de conexión WAN

Tecnología	Carga	Velocidad de bits común	Otras
Línea arrendada	Distancia, capacidad	hasta 45 Mb/s (E3/T3)	Capacidad fija permanente
Teléfono básico	Distancia, tiempo	33-56 kb/s	Marcación, conexión lenta
ISDN	Distancia, tiempo	64 ó 128 kb/s hasta 2 Mb/s, PRI	Marcación, conexión lenta
X.25	Volumen	hasta 48 kb/s	Capacidad fija conmutada
ATM	Capacidad	hasta 155 kb/s	Capacidad variable permanente
Frame Relay	Capacidad	hasta 1,5 Mb/s	Capacidad variable permanente
DSL	Suscripción mensual	hasta 3 Mb/s	Siempre en Internet compartida
Metro Ethernet	Suscripción mensual	hasta 500 Mb/s	Alcance geográfico limitado

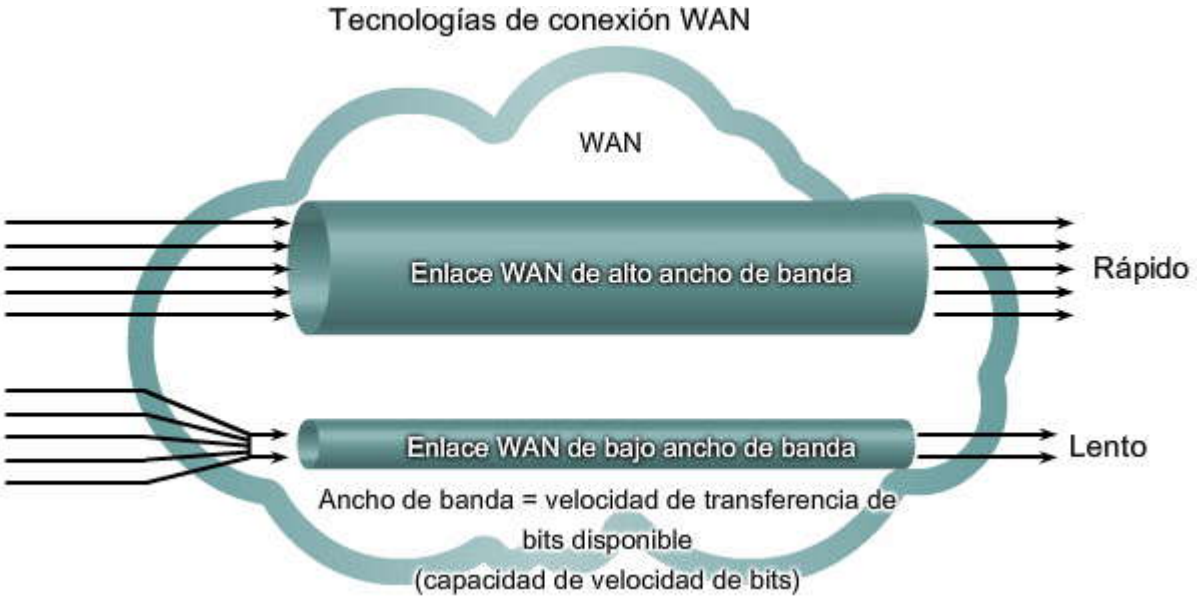
Muchas WAN de empresas están conectadas a Internet. Aunque Internet puede acarrear problemas de seguridad, es también una alternativa para el tráfico entre sucursales. Parte del tráfico que se debe considerar durante el diseño va o viene por Internet. Las implementaciones frecuentes incluyen conectar cada red de la empresaa un ISP diferente o conectar todas las redes de la empresa a un solo ISP desde una conexión de capa núcleo.



8.3.5 Consideraciones sobre el ancho de banda de WAN

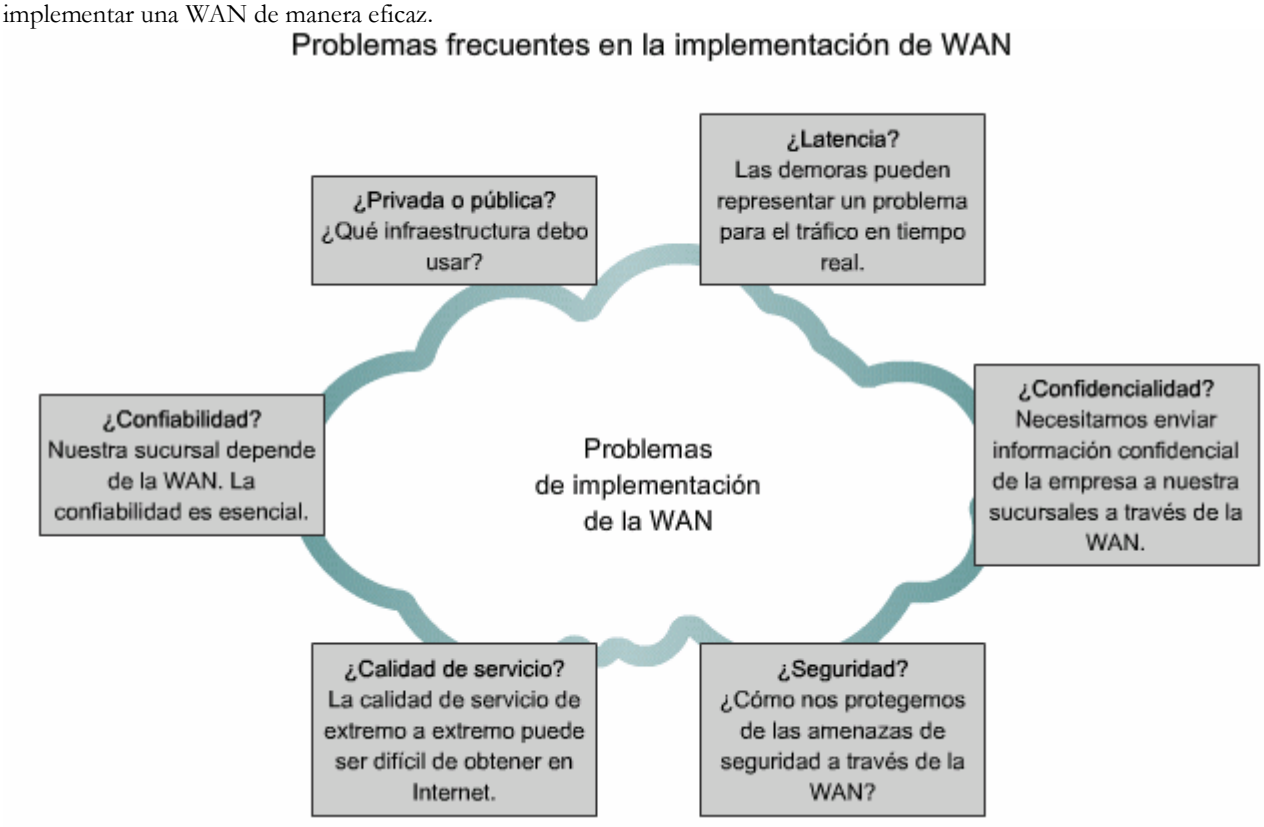
Recuerde que una red soporta las necesidades comerciales de una empresa. Muchas empresasdependen de la transferencia de datos a alta velocidad entre ubicaciones remotas. Como consecuencia, un ancho de banda más elevado es fundamental, porque permite que se transmitan más datos en un momento dado. Cuando el ancho de banda no es adecuado, la competencia entre los distintos tipos de tráfico causa un aumento en los tiempos de respuesta, lo que reduce la productividad de los empleados y hace más lentos los procesos comerciales críticos basados en la Web.

La figura muestra cómo se clasifican los enlaces WAN, generalmente, en alta velocidad o baja velocidad.



8.3.6 Problemas frecuentes en la implementación de WAN

La figura resume los problemas frecuentes en la implementación de WAN y las preguntas que deben responderse antes de implementar una WAN de manera eficaz.



8.3.7 Estudio de caso: resolución de problemas de WAN desde la perspectiva de un ISP

El gráfico ilustra las preguntas típicas que debe realizar el personal de soporte técnico de un ISP a un cliente que llama en busca de asistencia.

Una parte significativa de las llamadas de soporte que recibe un ISP se refieren a la lentitud de la red. Para resolver este problema eficazmente, se deben aislar los componentes individuales y probar cada uno como se indica a continuación:

Host de PC individual: una gran cantidad de aplicaciones de usuario abiertas en la PC al mismo tiempo puede ser la causa de la lentitud que se le atribuye a la red. Las herramientas como el Administrador de tareas en una PC con Windows pueden ser útiles para determinar la utilización de CPU.

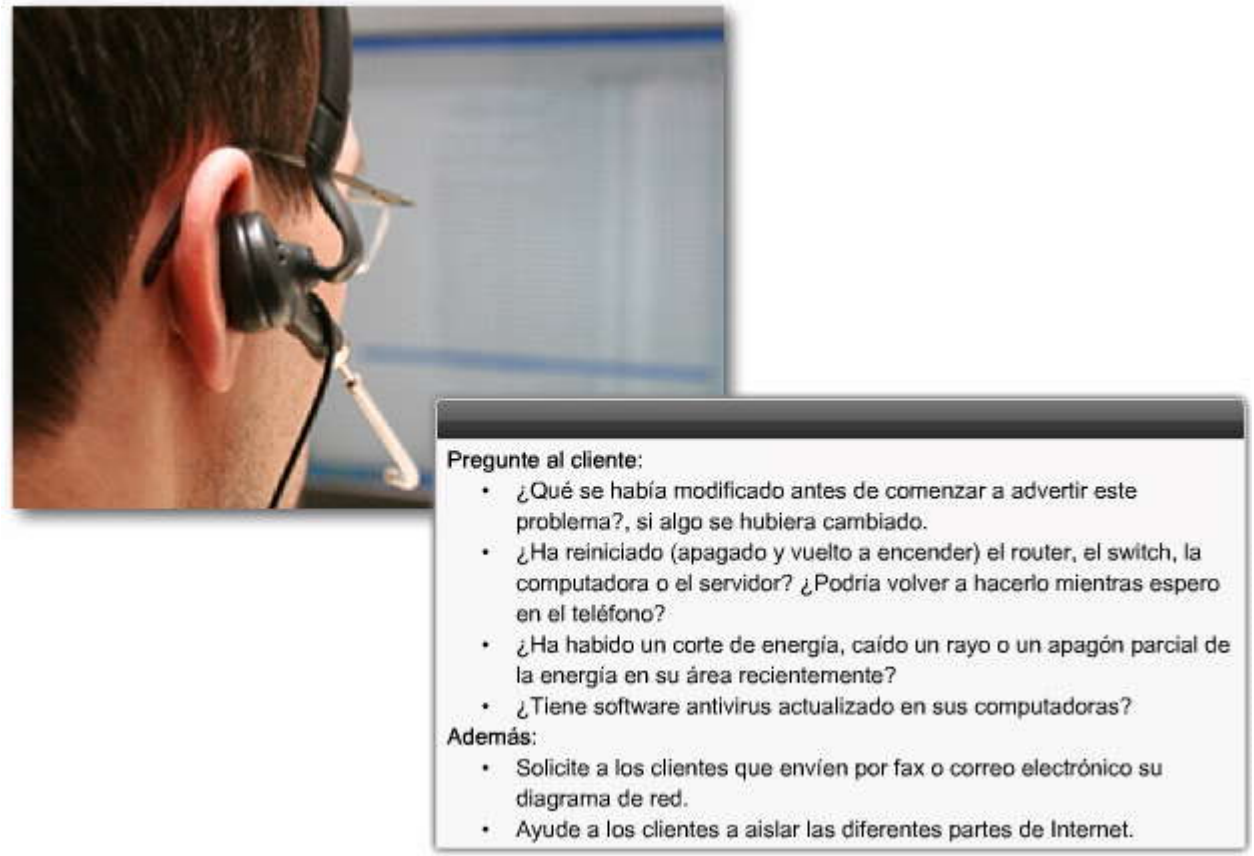
LAN : si el cliente tiene software de supervisión de redes en su LAN, el administrador de red debe poder indicar si el ancho de banda de la LAN alcanza con frecuencia una utilización del 100%. Éste es un problema que la empresa cliente debería resolver internamente. Por este motivo es tan importante establecer una línea de base de red y realizar una supervisión constante.

Enlace desde el punto extremo de la red del usuario hasta el punto extremo del ISP: pruebe el enlace desde el router extremo del cliente hasta el router extremo del ISP pidiéndole al cliente que se conecte a su router y envíe cien pings de 1500 bytes (pings de esfuerzo) a la dirección IP del router extremo del ISP. Este problema no es algo que pueda arreglar el cliente, es responsabilidad del ISP hacer que el proveedor de enlaces lo solucione.

Backbone del ISP: el representante de servicio al cliente del ISP puede ejecutar pings de esfuerzo desde el router extremo del ISP hasta el router extremo del cliente. También pueden ejecutarse pings de esfuerzo a través de cada enlace que atraviesa el tráfico del cliente. Mediante el aislamiento y la prueba de cada enlace, el ISP puede determinar qué enlace está causando el problema.

Acceso al servidor: en algunos casos, la lentitud que se atribuye a la red puede estar causada por la congestión del servidor. Este problema es el más difícil de diagnosticar y debe ser la última opción que se considera, luego de que todas las demás opciones se hayan descartado.

Estudio de caso: Resolución de problemas desde la perspectiva de un ISP



En esta actividad, usted junto con otro estudiante construirá la red que se muestra en el diagrama de topología. Configurarán NAT, DHCP y OSPF, y luego verificarán la conectividad. Cuando la red funcione completamente, un estudiante introducirá varios errores. Luego, el otro estudiante usará las técnicas de resolución de problemas para aislar y resolver el problema. A continuación, los estudiantes invertirán los roles y repetirán el proceso. Esta actividad puede realizarse en equipos reales o con Packet Tracer.

8.4 Resolución de problemas de red

8.4.1 Interpretación de diagramas de red para identificar problemas

Es casi imposible resolver cualquier tipo de problema de conectividad de la red sin un diagrama de red que muestre direcciones IP, rutas IP, dispositivos como firewalls y switches, y demás. En general, tanto las topologías lógicas y como las físicas ayudan en la resolución de problemas.

Diagrama de red físico

Un diagrama de red físico muestra el diseño físico de los dispositivos conectados a la red. Es necesario saber cómo están conectados físicamente los dispositivos para resolver problemas en la capa física, como problemas de cableado o hardware. La información registrada en el diagrama generalmente incluye lo siguiente:

- Tipo de dispositivo
- Modelo y fabricante
- Versión del sistema operativo
- Tipo de cable e identificador
- Especificación del cable
- Tipo de conector
- Extremos de cableado

La figura muestra un ejemplo de diagrama de red físico que proporciona información sobre la ubicación física de los dispositivos de red, los tipos de cableado entre ellos y los números de identificación de los cables. Esta información se usaría, principalmente, para resolver problemas físicos de los dispositivos o el cableado. Además del diagrama de red físico, algunos administradores también incluyen fotografías reales de sus armarios de cableado como parte de la documentación de la red.

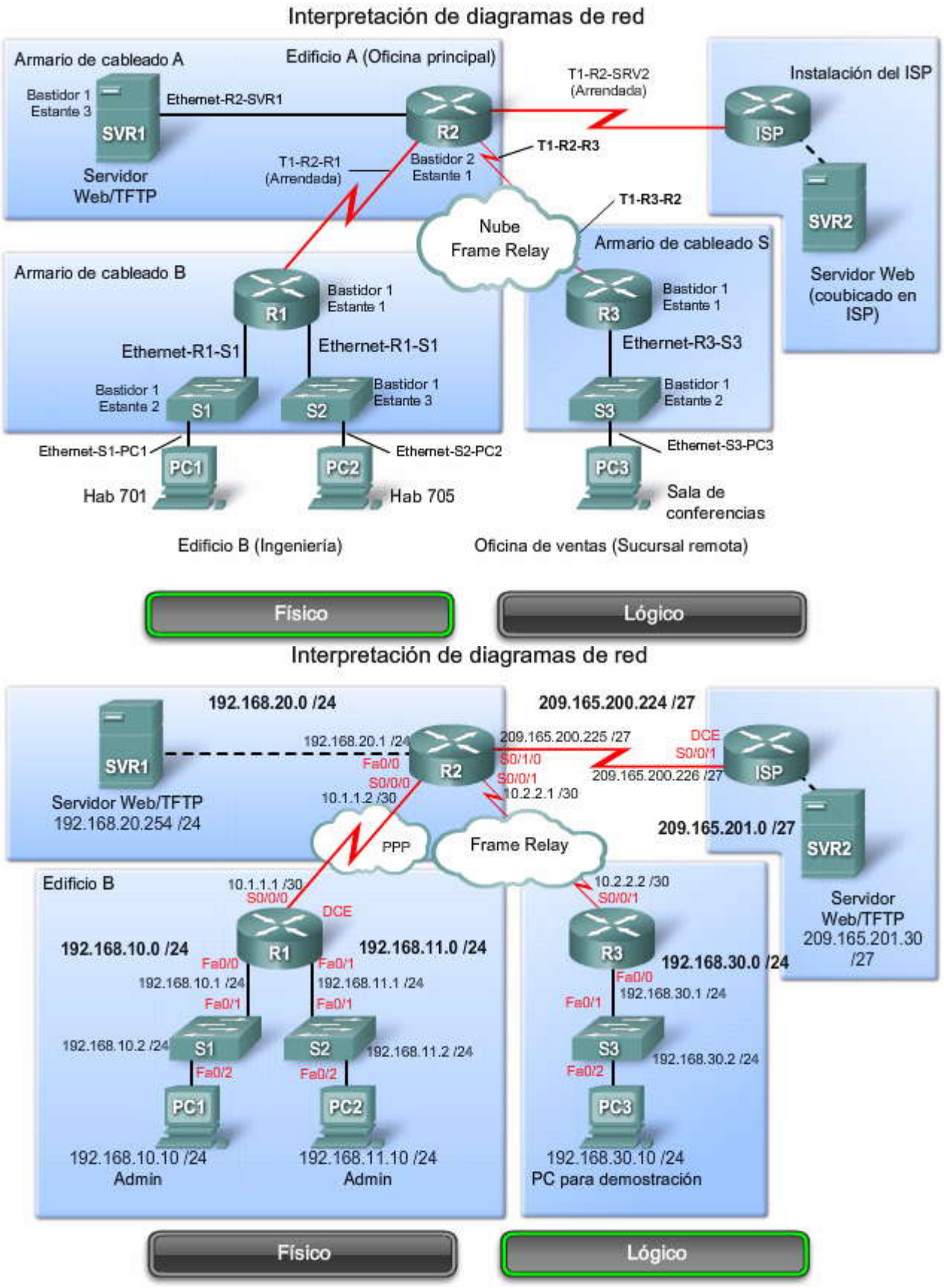
Diagrama de red lógico

Un diagrama de red lógico muestra cómo se transfieren los datos en la red. Se usan símbolos para representar elementos de la red, como routers, servidores, hubs, hosts, concentradores VPN y dispositivos de seguridad. La información registrada en el diagrama de red lógico puede incluir lo siguiente:

- Identificadores de dispositivos
- Subred y dirección IP
- Identificadores de interfaz
- Tipo de conexión
- DLCI para circuitos virtuales
- VPN de sitio a sitio
- Protocolos de enrutamiento
- Rutas estáticas
- Protocolos de enlace de datos
- Tecnologías WAN usadas

Haga clic en el botón Lógico de la figura para ver un ejemplo de un diagrama de red lógico.

La figura muestra la misma red, pero esta vez proporciona información lógica, como direcciones IP de dispositivos específicos, números de red, números de puertos, tipos de señal y asignaciones DCE para los enlaces seriales. Esta información puede usarse para resolver problemas en todas las capas de OSI.



8.4.2 Resolución de problemas de la capa física

Síntomas de los problemas de capa física

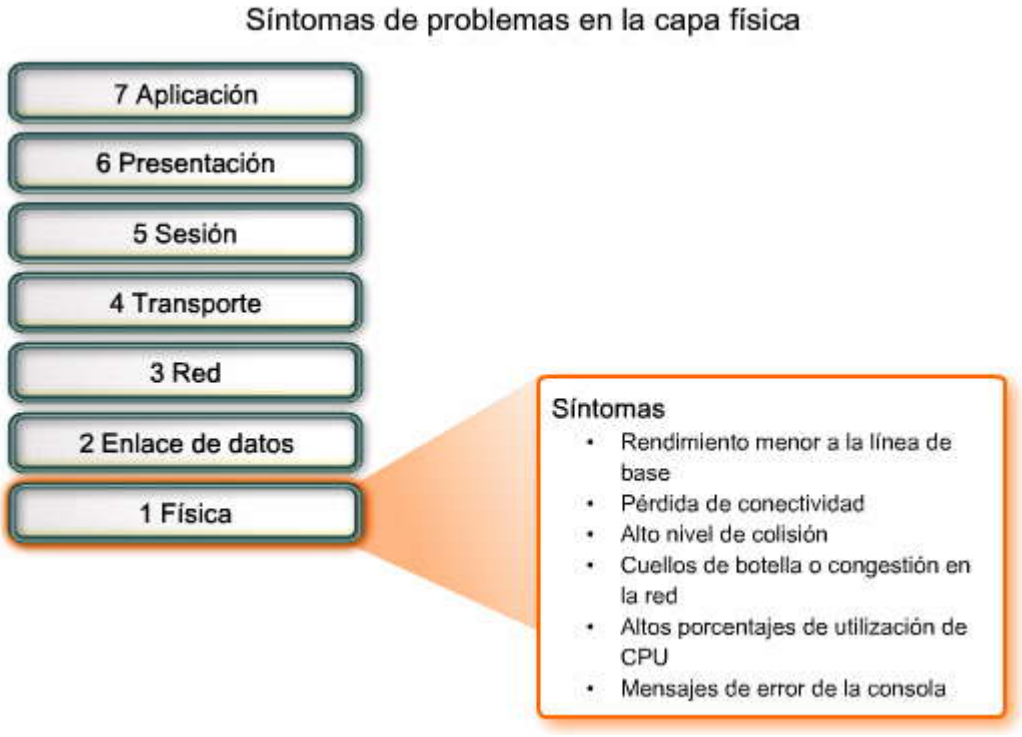
La capa física transmite bits de una computadora a otra y regula la transmisión de un streamde bits a través del medio físico. La capa física es la única capa con propiedades físicamente tangibles, como cables, tarjetas y antenas.

Las fallas y las condiciones subóptimas en la capa física no sólo molestan a los usuarios sino que también pueden afectar la productividad de toda la empresa. Las redes que experimentan estos tipos de condiciones, en general, se detienen completamente. Debido a que las capas superiores del modelo OSI dependen de la capa física para funcionar, un técnico de redes debe tener la habilidad para aislar y corregir los problemas en esta capa de manera eficaz.

Un problema de la capa física ocurre cuando las propiedades físicas de la conexión están por debajo del estándar y causan, así, que los datos se transfieran a una velocidad consistentemente menor a la velocidad del flujo de datos establecidos en la línea de base. Si hay un problema con funcionamiento subóptimo en la capa física, la red puede funcionar, pero el rendimiento es significativamente o intermitentemente menor al nivel especificado en la línea de base.

Los síntomas frecuentes de los problemas de la red en la capa física incluyen:

- **Rendimiento menor a la línea de base**: si el rendimiento no resulta satisfactorio en ningún momento, el problema probablemente esté relacionado con una mala configuración, capacidad inadecuada en algún punto u otro problema del sistema. Si el rendimiento varía y no es siempre insatisfactorio, el problema probablemente esté relacionado con una condición de error o esté siendo afectado por tráfico desde otros orígenes. Las razones más frecuentes para el rendimiento lento o inadecuado incluyen la sobrecarga o la falta de potencia de los servidores, configuraciones de switch o router inadecuadas, congestión de tráfico en un enlace de baja capacidad y pérdida crónica de trama.
- **Pérdida de conectividad**: si un cable o dispositivo falla, el síntoma más obvio es la pérdida de conectividad entre los dispositivos que se comunican a través de ese enlace o con la interfaz o el dispositivo fallado, lo cual puede indicarse mediante una simple prueba de ping. La pérdida intermitente de conectividad podría indicar una conexión floja u oxidada.
- **Altos conteos de colisión**: los problemas de dominio de colisiones afectan al medio local e interrumpen las comunicaciones con dispositivos de infraestructura de capa 2 y capa 3, servicios o servidores locales. Las colisiones son normalmente un problema más significativo en los medios compartidos que en los puertos de switch. Los conteos de colisiones promedio en los medios compartidos, generalmente, deben ser inferiores al 5%, aunque este número sea conservador. Asegúrese de que las determinaciones se basan en el promedio y no en los picos en las colisiones. En general, los problemas causados por colisiones pueden rastrearse a un solo origen. Puede ser un cable inadecuado en una sola estación, un cable uplink inadecuado en un hub o un puerto de un hub, o un enlace expuesto a ruido eléctrico externo. Una fuente de ruido cerca de un cable o hub puede causar colisiones, aun cuando no hay tráfico evidente para causarlas. Si las colisiones empeoran de forma directamente proporcional al nivel de tráfico, si la cantidad de colisiones alcanza el 100% o si no hay nada de tráfico correcto, el sistema de cable puede haber fallado.
- **Cuellos de botella o congestión en la red**: si un router, una interfaz o un cable falla, los protocolos de enrutamiento pueden redireccionar el tráfico hacia otras rutas que no están diseñadas para transportar la capacidad extra. Esto puede causar congestión o cuellos de botella en aquellas partes de la red.
- **Altos porcentajes de utilización de CPU**: los altos porcentajes de utilización de CPU representan un síntoma de que un dispositivo, como un router, switch o servidor, está funcionando en los límites de su diseño o los está superando. Si no se resuelve rápidamente, la sobrecarga de CPU puede hacer que un dispositivo falle o se desactive.
- **Mensajes de error de la consola**: los mensajes de error informados en la consola del dispositivo indican un problema en la capa física.



Causas de los problemas de capa física

Los temas que suelen causar problemas de red en la capa física incluyen los siguientes:

Relacionados con la energía

Los problemas de energía son una de las principales razones de fallas en las redes. La energía CA principal pasa a un módulo transformador CC o CA interno o externo dentro de un dispositivo. El transformador proporciona la corriente CC modulada correctamente que permite alimentar circuitos de dispositivos, conectores, puertos y ventiladores usados para el enfriamiento de dispositivos. Si se sospecha la existencia de un problema relacionado con la energía, a menudo se lleva a cabo una inspección física del módulo de energía. Verifique el funcionamiento de los ventiladores y asegúrese de que las ventilaciones de entrada y salida del chasis estén libres de obstrucciones. Si otras unidades cercanas también se han apagado, puede existir una falla de energía en la fuente de energía principal.

Fallas de hardware

Las tarjetas de interfaz de red (NIC) con fallas pueden causar errores de transmisión de red debido a colisiones tardías, tramas cortas y jabber. El jabber se define en general como la condición en la cual un dispositivo de red transmite continuamente datos sin sentido y al azar a través de la red. Otras causas posibles del jabber son los archivos de los controladores de NIC dañados o fallados, el cableado incorrecto o los problemas de conexión a tierra.

Fallas de cableado

Muchos problemas pueden corregirse, simplemente, al reacomodar los cables que se han desconectado parcialmente. Cuando se realiza una inspección física, deben buscarse cables dañados, tipos incorrectos de cables y RJ-45 mal engarzados. Los cables sospechados deben probarse o intercambiarse por un cable de funcionamiento comprobado.

Busque cables cruzados que se usan de manera inadecuada o puertos de hub o switch configurados incorrectamente como cruzados. Los cables de par dividido funcionan mal o no funcionan, según la velocidad de Ethernet usada, la longitud del segmento dividido y la distancia hasta el otro extremo.

Los problemas con los cables de fibra óptica pueden estar causados por conectores sucios, acodamientos excesivamente ajustados y conexiones RX/TX intercambiadas cuando se polarizan.

Los problemas con el cable coaxial a menudo ocurren en los conectores. Cuando el conductor del centro en el extremo del cable coaxial no está derecho o no posee la longitud correcta, no se logra una conexión adecuada.

Atenuación

Un stream de bits atenuado se produce cuando la amplitud de los bits se reduce al desplazarse por un cable. Si la atenuación es grave, el dispositivo receptor no siempre puede distinguir de manera satisfactoria los bits del componente del stream. Esto da lugar a una transmisión confusa y hace que el dispositivo receptor solicite al emisor la retransmisión del tráfico perdido. La atenuación puede causarse si la longitud de un cable supera el límite de diseño para los medios (por ejemplo, un cable Ethernet está limitado a 100 metros [328 pies] para un buen rendimiento) o cuando existe una mala conexión debido a un cable flojo o a contactos oxidados o sucios.

Ruido

La interferencia electromagnética (EMI) local con frecuencia se denomina ruido. Hay cuatro tipos de ruidos que son los más importantes para las redes de datos:

- El ruido de impulso causado por fluctuaciones de voltaje o picos de tensión inducidos en el cableado.
- El ruido aleatorio (blanco) generado por varias fuentes, como estaciones de radio FM, radios de policía, seguridad de edificios y el aterrizaje automático de aviones.
- El acoplamiento de crosstalk se produce cuando el ruido es inducido por otros cables en la misma ruta.
- La paradiafonía, o crosstalk de extremo cercano (NEXT), es el ruido originado por el crosstalk desde otros cables adyacentes o el ruido de cables eléctricos cercanos, dispositivos con motores eléctricos grandes o cualquier elemento que incluya un trasmisor más potente que un teléfono celular.

Errores de configuración de interfaz

Muchas opciones pueden configurarse incorrectamente en una interfaz y hacer que ésta deje de funcionar, lo cual causa una pérdida de la conectividad con los segmentos de red conectados. Los ejemplos de errores de configuración que afectan la capa física incluyen:

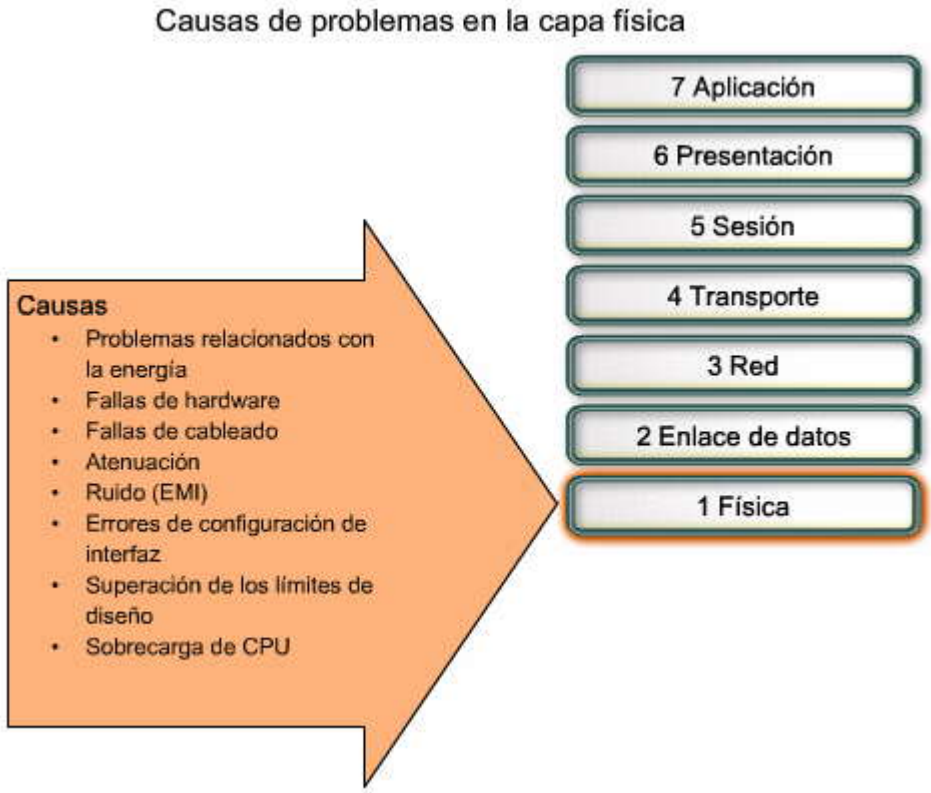
- Enlaces seriales reconfigurados como asíncronos en vez de síncronos
- Frecuencia de reloj incorrecta
- Fuente de reloj incorrecta
- Interfaz no activada

Superación de los límites de diseño

Un componente puede estar funcionando en condiciones subóptimas en la capa física porque se lo está utilizando a una velocidad promedio superior a la que debe funcionar según su configuración. Cuando se resuelve este tipo de problema, resulta evidente que los recursos para el dispositivo están funcionando a la capacidad máxima, o cerca de ella, y que se produce un aumento en la cantidad de errores de interfaz.

Sobrecarga de CPU

Los síntomas incluyen procesos con porcentajes altos de utilización de CPU, caídas en la cola de entrada, rendimiento lento, servicios de router, como Telnet y ping, que responden con lentitud o no responden, o falta de actualizaciones de enrutamiento. Una de las causas de la sobrecarga de CPU en un router es el tráfico elevado. Si algunas interfaces están habitualmente sobrecargadas con tráfico, considere la posibilidad de rediseñar el flujo de tráfico en la red o actualizar el hardware.



Para aislar problemas en las capas físicas haga lo siguiente:

Buscar conexiones o cables inadecuados

Verifique la correcta conexión del cable proveniente de la interfaz de origen y su buen estado. El probador de cables podría revelar la existencia de un cable abierto. Por ejemplo, en la figura, el probador Fluke CableIQ reveló que los cables 7 y 8 presentan una falla. Cuando dude acerca de la integridad de un cable, cambie los cables sospechados por un cable en buen funcionamiento. Si duda acerca de la conexión, quite el cable, realice una inspección física del cable y la interfaz y, luego, vuelva a colocar el cable. Use un probador de cables con los jacks de pared sospechosos para asegurarse de que el jack esté conectado correctamente.

Verificar que el estándar de cableado correcto se cumple en toda la red

Verifique que se está usando el cable adecuado. Puede ser necesario un cable cruzado para las conexiones directas entre algunos dispositivos. Compruebe que el cable esté conectado correctamente.Por ejemplo, en la figura, el medidor Fluke CableIQ ha detectado que, aunque un cable era correcto para Fast Ethernet, no admitía 1000BASE-T porque los cables 7 y 8 no estaban conectados adecuadamente. Estos cables no se necesitan para Fast Ethernet, perosí se necesitan en Gigabit Ethernet.

Verificar que el cableado de los dispositivos sea correcto

Compruebe que todos los cables estén conectados a sus puertos o interfaces adecuados. Asegúrese que todas las conexiones cruzadas estén conectadas adecuadamente a la ubicación correcta. Es en este momento cuando tener un armario de cableado organizado y prolijo ahorra una gran cantidad de tiempo.

Verificar las configuraciones de interfaz adecuadas

Compruebe que todos los puertos de switch estén configurados en la VLAN correcta y que las configuraciones de spanning tree, velocidad y dúplex sean correctas. Confirme que los puertos e interfaces activos no estén desactivados.

Comprobar las estadísticas operativas y los índices de error de datos

Use los comandos **show** de Cisco para comprobar las estadísticas, como errores de colisión, de entrada y de salida. Las características de estas estadísticas varían según los protocolos usados en la red.

8.4.3 Resolución de problemas de la capa de enlace de datos

Síntomas de los problemas en la capa de enlace de datos

La resolución de problemas en la capa 2 puede ser un proceso desafiante. La configuración y el funcionamiento de estos protocolos son críticos para la creación de una red funcional y ajustada correctamente.

Los problemas en la capa de enlace de datos causan síntomas comunes que ayudan a identificar los inconvenientes de la capa 2. El reconocimiento de estos síntomas ayuda a reducir la cantidad de causas posibles. Los síntomas frecuentes de los problemas de la red en la capa de enlace de datos incluyen:

Falta de funcionalidad o conectividad en la capa de red o en capas superiores

Algunos problemas de la capa 2 pueden detener el intercambio de tramas a través de un enlace, mientras que otros sólo empeoran el rendimiento de la red.

Funcionamiento de la red por debajo de los niveles de rendimiento de la línea de base

Hay dos tipos diferentes de funcionamiento de capa 2 subóptimo que pueden ocurrir en la red:

- Las tramas toman una ruta ilógica a su destino, pero llegan. Un ejemplo de un problema que podría causar que las tramas tomen una ruta subóptima es una topología de spanning-tree de capa 2 mal diseñada. En este caso, la red podría experimentar un uso de ancho de banda elevado en enlaces que no deberían tener ese nivel de tráfico.
- Algunas tramas se descartan. Estos problemas pueden identificarse a través de las estadísticas de los contadores de errores y los mensajes de error de la consola que aparecen en el switch o router. En un entorno Ethernet, un ping extendido o continuo también revela si se están descartando tramas.

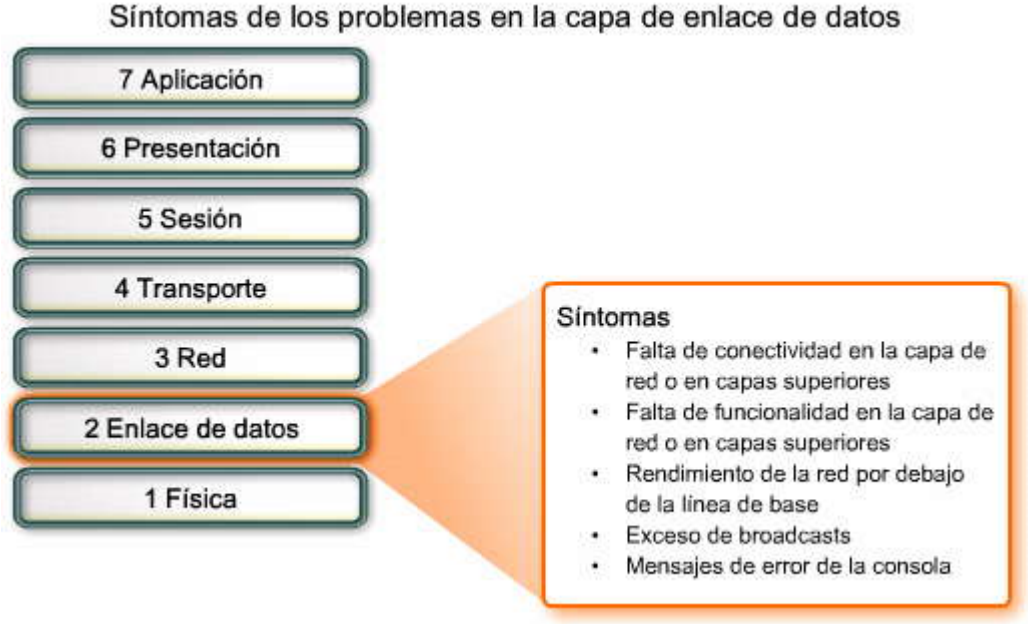
Exceso de broadcasts

Los sistemas operativos modernos usan broadcasts de manera frecuente para detectar servicios de red y otros hosts. Donde se observa un exceso de broadcasts, es importante identificar el origen de tales broadcasts. En general, el exceso de broadcasts es ocasionado por una de las siguientes situaciones:

- Aplicaciones mal configuradas o programadas
- Grandes dominios de broadcast de capa 2
- Problemas de red subyacentes, como bucles STP o rutas sacudidas.

Mensajes de consola

En algunos casos, un router reconoce que ha ocurrido un problema de capa 2 y envía mensajes de alerta a la consola. En general, un router hace esto cuando detecta un problema en la interpretación de tramas entrantes (problemas de encapsulación o entramado) o cuando se esperan mensajes de actividad, pero éstos no llegan. El mensaje de consola más frecuente que indica un problema de capa 2 es un mensaje de inactividad del protocolo de línea.



Causas de los problemas de la capa de enlace de datos

Las condiciones en la capa de enlace de datos que, en general, causan problemas de rendimiento o conectividad en la red incluyen las siguientes:

Errores de encapsulación

Un error de encapsulación se produce porque los bits que el emisor ubica en un campo determinado no son lo que el receptor espera ver. Esta condición ocurre cuando la encapsulación en un extremo de un enlace WAN se configura de manera diferente a la encapsulación usada en el otro extremo.

Errores de asignación de direcciones

En las topologías, como punto a multipunto, Frame Relay o Ethernet de broadcast, es esencial que se asigne a la trama una dirección de destino de capa 2 adecuada. Esto garantiza su llegada al destino correcto. Para lograrlo, el dispositivo de red debe hacer coincidir una dirección de capa 3 de destino con la dirección de capa 2 correcta mediante mapas dinámicos o estáticos.

Cuando se usan asignaciones estáticas en Frame Relay, una asignación incorrecta es un error frecuente. Pueden producirse errores de configuración simples por una discordancia de la información de direccionamiento de capa 2 y capa 3.

En un entorno dinámico, la asignación de la información de capa 2 y capa 3 puede fallar por las siguientes razones:

- Es posible que los dispositivos se hayan configurado específicamente para no responder a solicitudes de ARP o ARP inverso.
- La información de capa 2 y capa 3 que se almacena en caché puede haberse modificado físicamente.
- Se reciben respuestas de ARP no válidas debido a un error de configuración o un ataque de seguridad.

Errores de entramado

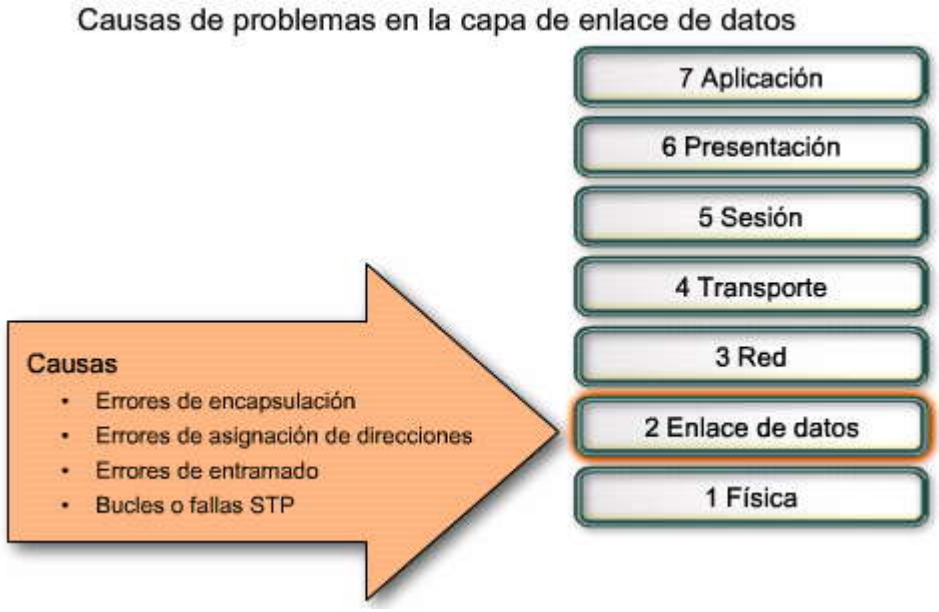
Las tramas, en general, funcionan en grupos de bytes de 8 bits. Un error de entramado ocurre cuando una trama no termina en un límite de byte de 8 bits. Cuando esto sucede, el receptor puede tener problemas para determinar dónde termina una trama y dónde comienza la trama siguiente. Según la gravedad del problema de entramado, la interfaz puede interpretar algunas de las tramas. Una cantidad excesiva de tramas no válidas puede impedir el intercambio de mensajes de actividad válidos.

Los errores de entramado pueden deberse a una línea serial con ruido, un cable mal diseñado (demasiado largo o blindado inadecuadamente) o un reloj de línea de la unidad de servicio de canal (CSU) configurado incorrectamente.

Bucles o fallas STP

El objetivo del protocolo spanning tree (STP) es resolver una topología física redundante en una topología de árbol mediante el bloqueo de los puertos redundantes. La mayoría de los problemas de STP se relacionan con estos temas:

- El reenvío de bucles que ocurre cuando no se bloquea ningún puerto de una topología redundante y cuando se reenvía el tráfico en círculos de manera indefinida. Cuando comienza el reenvío de bucles, generalmente se congestionan los enlaces de menor ancho de banda a lo largo de la ruta. Si todos los enlaces tienen el mismo ancho de banda, todos los enlaces se congestionan. Esta congestión causa la pérdida de paquetes y desactiva la red en el dominio afectado de capa 2.
- Exceso de flooding debido a un alto índice de cambios en la topología de STP. La función del mecanismo de cambios en la topología es corregir las tablas de reenvío de capa 2 cuando cambia la topología de reenvío. Esto es necesario para evitar las interrupciones en la conectividad porque, luego de un cambio en la topología, algunas direcciones MAC a las que antes era posible acceder mediante puertos específicos podrían volverse accesibles a través de puertos diferentes. En una red correctamente configurada, un cambio en la topología debería ser un episodio excepcional. Cuando un enlace en un puerto de switch se activa o desactiva, ocurre un cambio en la topología cuando el estado de STP del puerto está pasando al estado de reenviar o saliendo de ese estado. Sin embargo, cuando un puerto es inestable (oscila entre los estados activo e inactivo) causa flooding y cambios de topología repetitivos.
- La convergencia o reconvergencia de STP lenta, que puede ser causada por una discordancia entre la topología real y la documentada, un error de configuración, tal como un configuración inconsistente de los temporizadores de STP, sobrecarga de CPU del switch durante la convergencia o un defecto de software.



Resolución de problemas de capa 2: PPP

La dificultad para resolver problemas de tecnologías de capa 2, como PPP y Frame Relay, es la falta de disponibilidad de herramientas de resolución de problemas frecuentes de capa 3, como ping, para utilizar como ayuda, excepto para la identificación redes inactivas. Solamente a través de una comprensión integral de los protocolos y su funcionamiento puede un técnico de redes seleccionar la metodología adecuada de resolución de problemas y los comandos de IOS de Cisco para resolver el problema de manera eficaz.

La mayoría de los problemas que ocurren con PPP incluyen la negociación de enlaces. Los pasos para la resolución de problemas de PPP son los siguientes:

Paso 1. Verificar que se usa la encapsulación adecuada en los dos extremos mediante el comando **show interfaces serial**. En la figura para el paso 1, el resultado del comando muestra que R2 se ha configurado incorrectamente para usar la encapsulación HDLC.

Paso 2. Confirmar que las negociaciones del protocolo de control de enlace (LCP) se realizaron correctamente; para ello, revise el resultado para el mensaje de LCP abierto.

Haga clic en el botón Paso 2 de la figura.

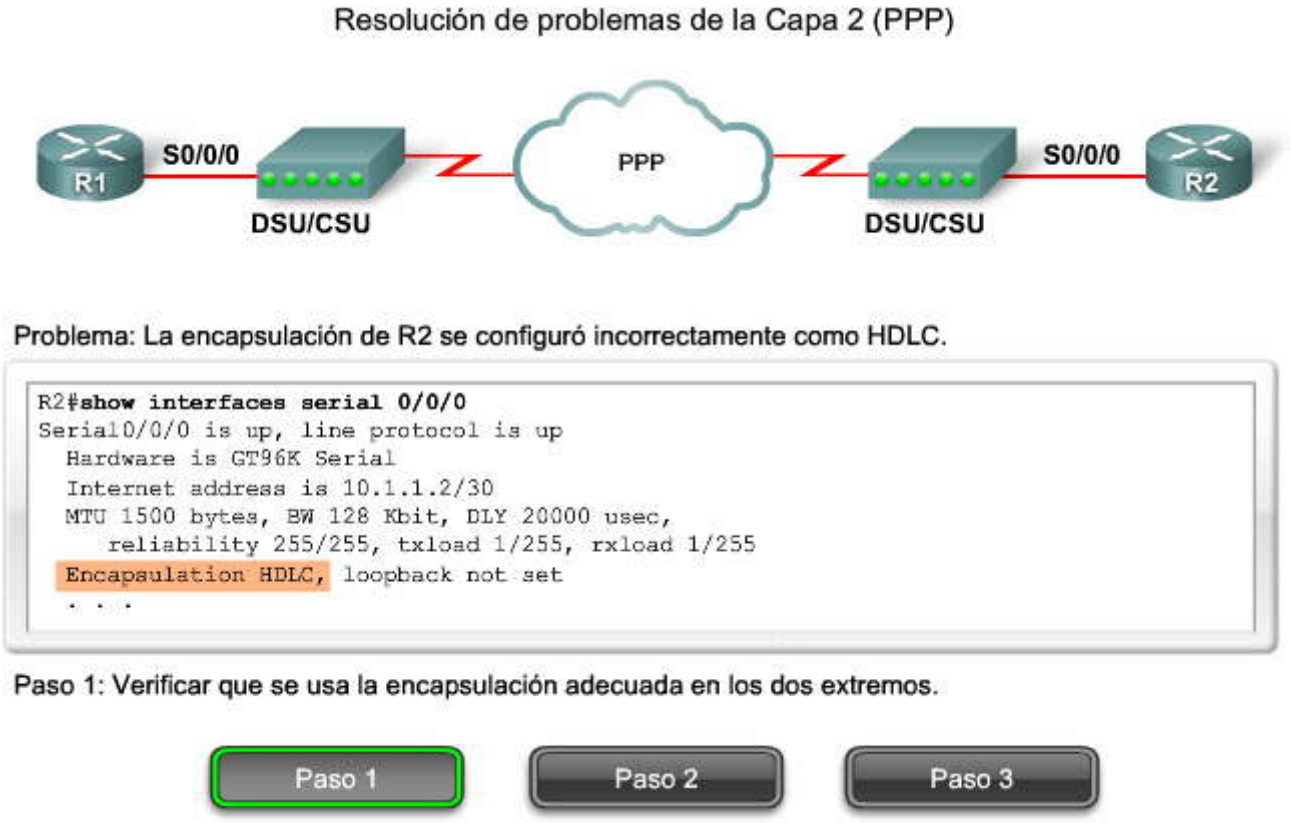
En la figura, la encapsulación en R2 se ha cambiado por PPP. El resultado del comando **show interfaces serial** muestra el mensaje de LCP abierto, el cual indica que las negociaciones de LCP fueron satisfactorias.

Paso 3. Verificar la autenticación en ambos lados del enlace mediante el comando **debug ppp authentication**.

Haga clic en el botón Paso 3 de la figura.

En la figura, el resultado del comando **debug ppp authentication** muestra que R1 no puede autenticar R2 mediante CHAP, porque el nombre de usuario y la contraseña para R2 no se han configurado en R1.

Consulte el capítulo 2, "PPP", para obtener más detalles sobre la resolución de problemas en implementaciones de PPP.



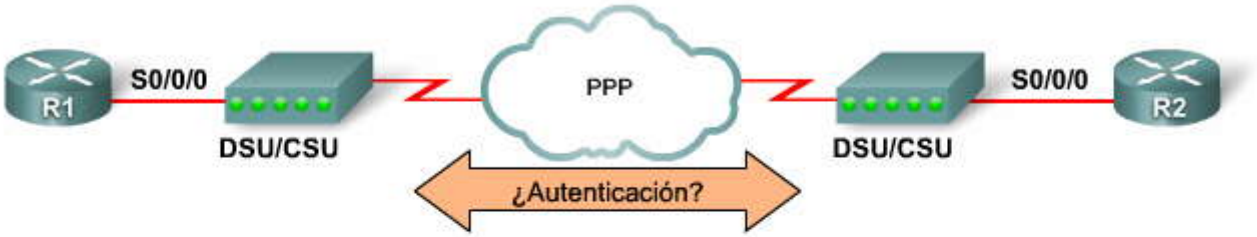
Resolución de problemas de la Capa 2 (PPP)

La encapsulación de R2 se corrigió a PPP. LCP Open muestra que las negociaciones de LCP fueron satisfactorias.

```
R2#show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.1.1.2/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
```

Paso 2: Confirmar que las negociaciones del protocolo de control de enlace (LCP) se realizaron correctamente.

Resolución de problemas de la Capa 2 (PPP)



Problema: La autenticación CHAP se configuró incorrectamente en R1.

```
R1# debug ppp authentication
Serial0: Unable to authenticate. No name received from peer
Serial0: Unable to validate CHAP response. USERNAME R2 not found.
Serial0: Unable to validate CHAP response. No password defined for USERNAME R2
Serial0: Failed CHAP authentication with remote.
Remote message is Unknown name
. . .
```

Paso 3: Verificar la autenticación en ambos lados del enlace.

Resolución de problemas de capa 2: Frame Relay

La resolución de problemas de red de Frame Relay puede dividirse en cuatro pasos:

Paso 1. Verificar la conexión física entre la CSU/unidad de servicios de datos (DSU) y el router. En la figura, las conexiones físicas entre los routers R1 y R2 y sus CSU/DSU correspondientes pueden verificarse mediante un probador de cables y la

comprobación de que todos los LED de estado en la unidad CSU/DSU estén en cdor verde. En la figura, algunas de las luces de estado para la CSU/DSU en R3 están en rojo, lo que indica un posible problema de conectividad entre la CSU/DSU y el router R3.

Paso 2. Utilizar el comando **show frame-relay lmi** para verificar que el router y el proveedor de Frame Relay estén intercambiando información LMI de manera adecuada.

Haga clic en el botón Paso 2 de la figura.

En la figura, el resultado del comando **show frame-relay lmi** en R2 muestra que no hay errores ni mensajes perdidos. Esto indica que R2 y el switch del proveedor de Frame Relay están intercambiando información LMI de manera adecuada.

Paso 3. Utilizar el comando **show frame-relay pvc** para verificar que el estado de PVC sea activo.

Haga clic en el botón Paso 3 de la figura.

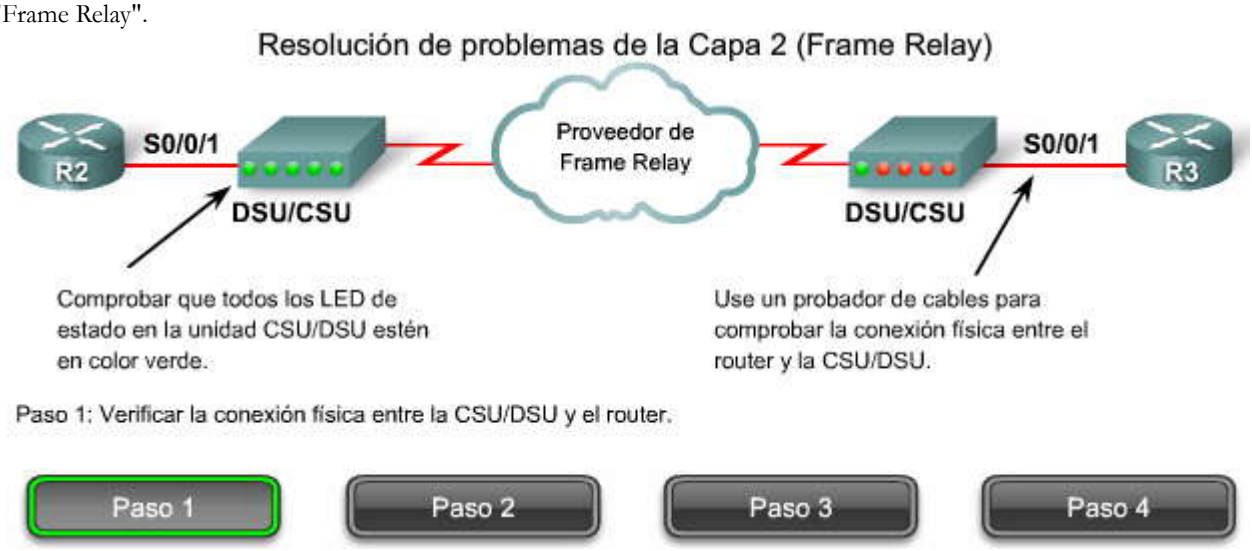
En la figura, el resultado del comando **show frame-relay pvc** en R2 verifica que el estado PVC es activo.

Paso 4. Utilizar el comando **show interfaces serial** para verificar que la encapsulación de Frame Relay coincida en los dos routers.

Haga clic en el botón Paso 4 de la figura.

En la figura, el resultado del comando **show interfaces serial** en los routers R2 y R3 muestra que hay una discordancia de encapsulación entre ellos. R3 se ha configurado incorrectamente para usar la encapsulación HDLC en vez de Frame Rday.

Para obtener más detalles sobre la resolución de problemas de las implementaciones de Frame Relay, consulte el capítulo 3, "Frame Relay".



Resolución de problemas de la Capa 2 (Frame Relay)


```
R2#show frame-relay lmi
LMI Statistics for interface Serial0/0/1 (Frame Relay DTE) LMI TYPE = CISCO
  Invalid Unnumbered info 0          Invalid Prot Disc 0
  Invalid dummy Call Ref 0           Invalid Msg Type 0
  Invalid Status Message 0           Invalid Lock Shift 0
  Invalid Information ID 0           Invalid Report IE Len 0
  Invalid Report Request 0           Invalid Keep IE Len 0
  Num Status Enq. Sent 76            Num Status msgs Rcvd 76
  Num Update Status Rcvd 0           Num Status Timeouts 0
  Last Full Status Req 00:00:48      Last Full Status Rcvd 00:00:48
```

Sin errores

Solicitudes de estado = mensajes de estado recibidos

Paso 2: Verificar el correcto intercambio de información de LMI entre cada router y el switch FR.

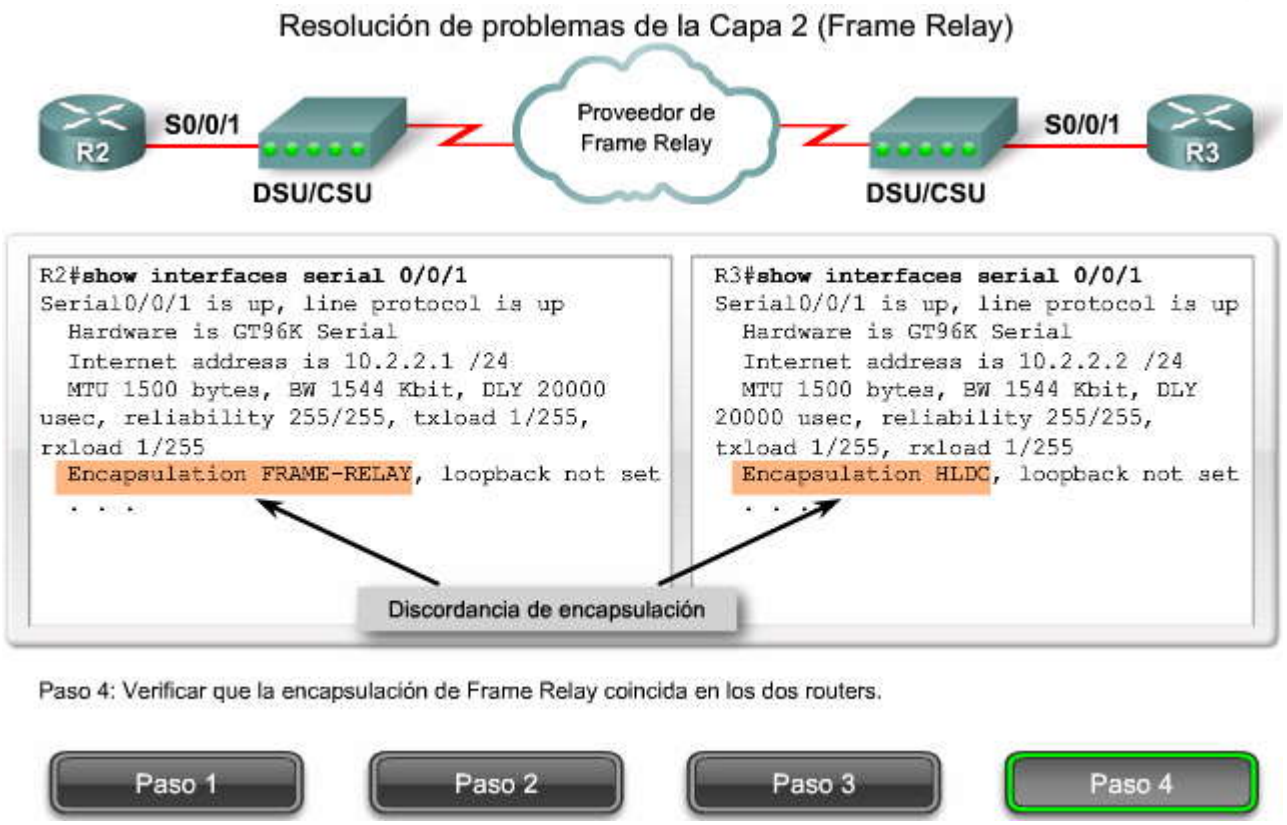
Paso 1 | **Paso 2** | Paso 3 | Paso 4

Resolución de problemas de la Capa 2 (Frame Relay)


```
R2#show frame-relay pvc 201
PVC Statistics for interface Serial0/0/1 (Frame Relay DTE)
DLCI = 201, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE = Serial0/0/1.201
  input pkts 11              output pkts 8              in bytes 3619
  out bytes 2624             dropped pkts 0             in pkts dropped 0
  out pkts dropped 0                  out bytes dropped 0
  in FECN pkts 0             in BECN pkts 0             out FECN pkts 0
  out BECN pkts 0            in DE pkts 0               out DE pkts 0
  out bcast pkts 8           out bcast bytes 2624
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 00:08:23, last time pvc status changed 00:08:23
```

Paso 3: Verificar que el estado de PVC sea activo.

Paso 1 | Paso 2 | **Paso 3** | Paso 4



Resolución de problemas de capa 2: Bucles STP

Si sospecha que un bucle STP está causando un problema de capa 2, verifique si se está ejecutando el protocolo spanning tree en cada uno de los switches. Un switch sólo debe tener desactivado STP si no es parte de una topología de bucle física. Para verificar el funcionamiento de STP, use el comando **show spanning-tree** en cada switch. Si descubre que STP no está funcionando, puede activarlo mediante el comando **spanning-tree** *vlan ID*.

Use estos pasos para resolver problemas de reenvío de bucles:

Paso 1. Identificar que esté ocurriendo un bucle STP.

Cuando se ha desarrollado un bucle de reenvío en la red, éstos son los síntomas frecuentes:

- Pérdida de conectividad hacia, desde y a través de las regiones afectadas de la red
- Nivel elevado de uso de la CPU en routers que están conectados a los segmentos o VLAN afectados
- Nivel elevado de uso de enlaces (a menudo 100%)
- Nivel elevado de uso de backplane del switch (en comparación con el uso de la línea de base)
- Mensajes Syslog que indican que los paquetes hacen un recorrido en bucle en la red (por ejemplo, mensajes con direcciones IP duplicadas del protocolo Hot Standby Router Protocol)
- Mensajes Syslog que indican un reaprendizaje constante de direcciones o mensajes inestables de direcciones MAC
- Cada vez más caídas de productividad en muchas interfaces

Paso 2. Descubrir la topología (alcance) del bucle.

La prioridad más alta es detener el bucle y restaurar el funcionamiento de la red. Para detener el bucle, debe conocer qué puertos están involucrados. Observe los puertos con el nivel de utilización de enlaces más elevado (paquetes por segundo), El comando **show interface** muestra la utilización de cada interfaz. Asegúrese de registrar esta información antes de continuar con el paso siguiente. De lo contrario, más tarde podría ser difícil determinar la causa del bucle.

Paso 3. Interrumpir el bucle.

Desactive o desconecte los puertos comprometidos, uno por vez. Luego de deshabilitar o desconectar cada puerto, verifique si la utilización del backplane del switch volvió al nivel normal. Documente los descubrimientos. Tenga en cuenta que es posible que algunos puertos no sostengan d bucle, sino que inunden el tráfico que llega con el bucle. Cuando se deshabilitan los puertos con flooding, sólo se reduce levemente la utilización de backplane, pero no se detiene el bucle.

Paso 4. Descubrir y solucionar la causa del bucle.

Determinar el motivo por el que comenzó el bucle es, a menudo, la parte más difícil del proceso, porque las razones pueden variar. También es difícil formalizar un procedimiento exacto que funcione en todos los casos. Primero, investigue el diagrama de topología para buscar una ruta redundante.

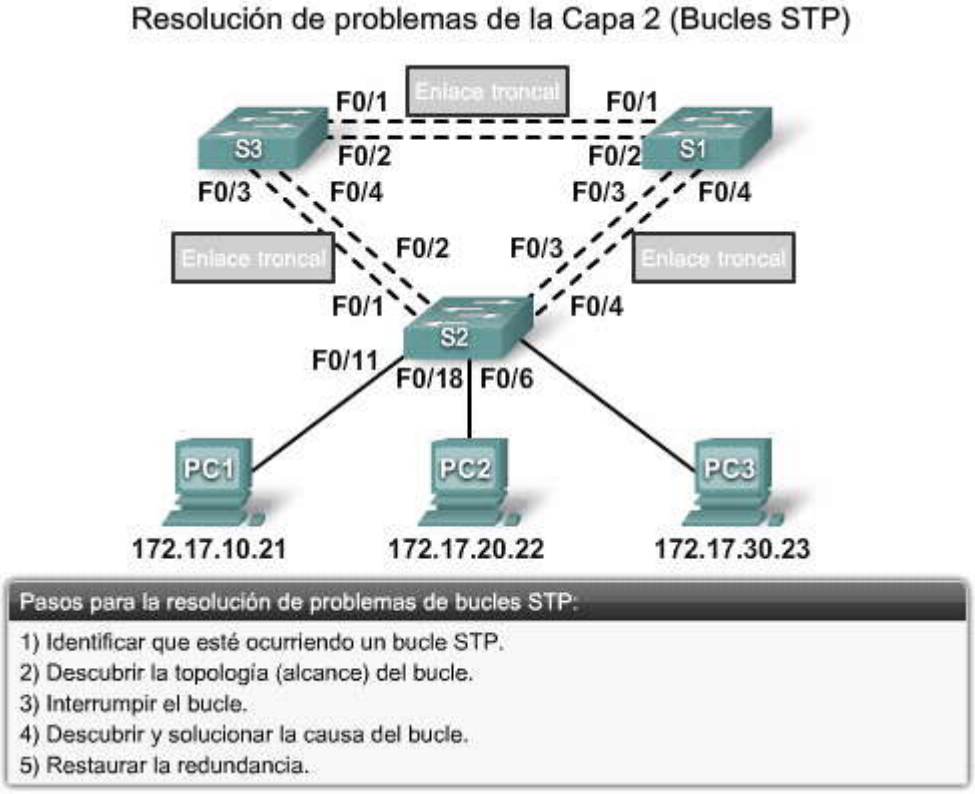
Para cada switch de la ruta redundante, compruebe lo siguiente:

- ¿Conoce el switch la raíz STP correcta?
- ¿El puerto raíz está correctamente identificado?
- ¿Se reciben regularmente las unidades de datos del protocolo de puente (BPDU) en el puerto raíz y en los puertos que se supone que deben bloquearse?
- ¿Se envían frecuentemente las BPDU en los puertos designados que no son puertos raíz?

Paso 5. Restaurar la redundancia.

Una vez encontrado el dispositivo o enlace que está causando el bucle y resuelto el problema, restaure los enlaces redundantes que se desconectaron.

Sólo se ha tratado brevemente el tema de la resolución de problemas de bucles STP. La resolución de problemas de bucles y otros problemas de STP es compleja, y su análisis detallado se encuentra fuera del alcance de este curso. Sin embargo, si desea obtener más información sobre la resolución de problemas de STP, se encuentra disponible una excelente nota técnica en: http://cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a0080136673.shtml#troubleshoot.

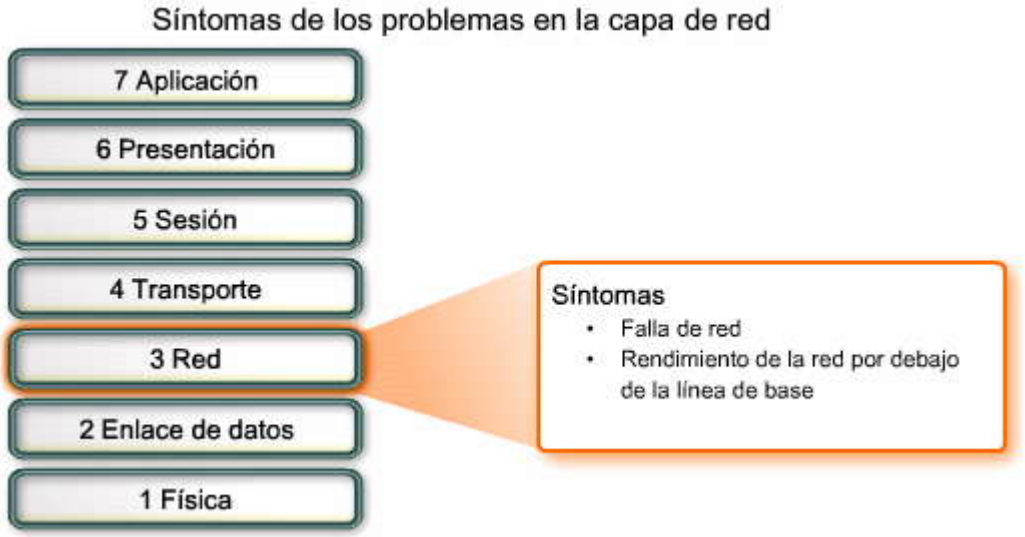


8.4.4 Resolución de problemas de la capa de red

Síntomas de los problemas de la capa de red

Los problemas de la capa de red incluyen todos los problemas que implican un protocolo de capa 3, tanto protocolos enrutados como de enrutamiento. Este tema se enfoca principalmente en los protocolos de enrutamiento IP.

Los problemas de la capa de red pueden causar fallas en la red o un rendimiento subóptimo. Una falla en la red ocurre cuando la red casi no funciona o deja de funcionar por completo, lo cual afecta a todos los usuarios y las aplicaciones que usan la red. En general, los usuarios y los administradores de red notan rápidamente estas fallas que, por supuesto, son críticas para la productividad de una empresa. Los problemas de optimización de la red suelen implicar un subconjunto de usuarios, aplicaciones, destinos o un tipo particular de tráfico. Los problemas de optimización en general pueden ser más difíciles de detectar y aún más complicados para aislar y diagnosticar porque, a menudo, incluyen varias capas o hasta la computadora host. Llegar a determinar que el problema es un problema de capa de red puede demorar tiempo.



Resolución de problemas de capa 3

En la mayoría de las redes, las rutas estáticas se usan en combinación con protocolos de enrutamiento dinámico. La configuración incorrecta de las rutas estáticas puede llevar a un enrutamiento no óptimo y,en algunos casos, puede crear bucles de enrutamiento o hacer que partes de la red se vuelvan inalcanzables.

La resolución de problemas de protocolos de enrutamiento dinámico requiere una comprensión integral del funcionamiento del protocolo de enrutamiento específico. Algunos problemas son comunes a todos los protocolos de enrutamiento, mientras que otros son específicos de un protocolo de enrutamiento individual.

No hay una plantilla única para resolver problemas de capa 3. Los problemas de enrutamientose resuelven con un proceso metódico, mediante una serie de comandos para aislar y diagnosticar el problema.

A continuación, se presentan algunas áreas que deben explorarse al diagnosticar un posible problema con los protocolos de enrutamiento:

Problemas de red generales

A menudo, un cambio en la topología, como un enlace desactivado, puede también tener impacto sobre otras áreas de la red que podrían no resultar evidentes en ese momento. Esto puede incluir la instalación de nuevas rutas, estáticas o dinámicas, la eliminación de otras rutas, etc.

Algunos aspectos que se deben considerar son los siguientes:

- ¿Se realizó alguna modificación en la red recientemente?
- ¿Actualmente hay algún usuario trabajando en la infraestructura de la red?

Problemas de conectividad

Busque problemas con los equipos y problemas de conectividad, incluso problemas de energía, como interrupciones o problemas ambientales, como el recalentamiento. También compruebe si hay problemas de capa 1, como problemas de cableado, puertos incorrectos o problemas de ISP.

Problemas de vecinos

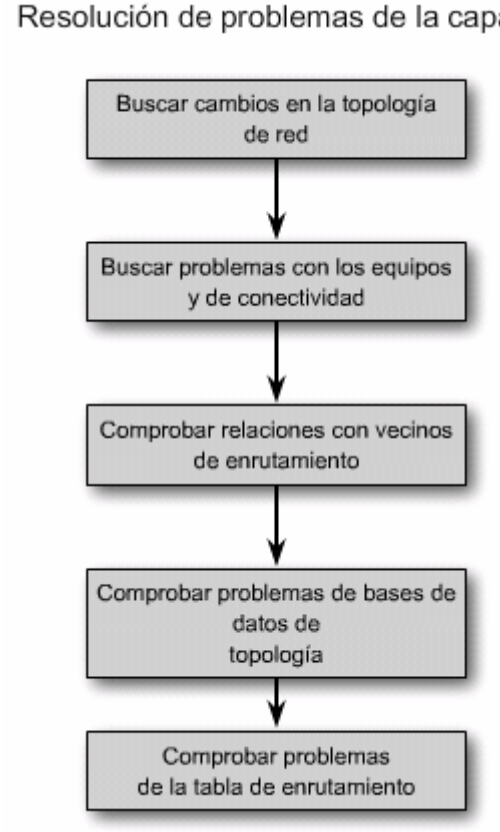
Si el protocolo de enrutamiento establece una adyacencia con un vecino, compruebe si hay problemas con los routers que forman las relaciones de vecinos.

Base de datos de topología

Si el protocolo de enrutamiento usa una tabla o una base de datos de topología, comprueba si aparece algún elemento inesperado en la tabla, como entradas faltantes o inesperadas.

Tabla de enrutamiento

Verifique si hay elementos inesperados en la tabla de enrutamiento, como rutas faltantes o inesperadas. Use los comandos **debug** para ver las actualizaciones de enrutamiento y el mantenimiento de la tabla de enrutamiento.



8.4.5 Resolución de problemas de la capa de transporte

Problemas frecuentes de listas de acceso

Los problemas de red pueden surgir de problemas de la capa de transporte en el router, especialmente en el borde de la red donde las tecnologías de seguridad examinan y modifican el tráfico. En este tema, se analizan dos de las tecnologías de seguridad de la capa de transporte que se implementan con mayor frecuencia: las listas de control de acceso (ACL) y la traducción de direcciones de red (NAT).

Haga clic en el botón Problemas de listas de acceso en la figura.

La configuración incorrecta causa los problemas más frecuentes de las ACL. Existen ocho áreas donde se producen con frecuencia configuraciones incorrectas:

Selección del flujo de tráfico

La configuración incorrecta del router más frecuente es la aplicación de la ACL al tráfico erróneo. El tráfico se define por la interfaz del router a través de la cual el tráfico se desplaza y por la dirección en la cual se desplaza este tráfico. Para que funcione de manera adecuada, una ACL debe aplicarse a la interfaz correcta y debe seleccionarse la dirección correcta del tráfico.

Orden de los elementos de control de acceso

Los elementos de una ACL deben ordenarse de los más específicos a los generales. Aunque una ACL incluya un elemento para permitir específicamente un flujo de tráfico particular, los paquetes nunca coincidirán con ese elemento si otro elemento anterior de la lista los deniega.

Deny all implícito

En una situación donde no se requiere un alto nivel de seguridad en la ACL, no incluir este elemento de control de acceso implícito puede ser la causa de una configuración incorrecta de la ACL.

Direcciones y máscaras wildcard

Si el router ejecuta ACL y NAT, el orden en el cual se aplica cada una de estas tecnologías a un flujo de tráfico es importante:

- La ACL entrante procesa el tráfico entrante antes de que sea procesado por la NAT de afuera hacia adentro.
- La ACL saliente procesa el tráfico saliente después de que es procesado por la NAT de adentro hacia afuera.

Las máscaras wildcard complejas proporcionan mejoras notables en la eficacia, pero son más propensas a errores de configuración. Un ejemplo de máscara wildcard compleja es utilizar la dirección 10.0.32.0 y la máscara wildcard 0.0.32.15 para seleccionar las primeras 15 direcciones host en la red 10.0.0.0 o en la red 10.0.32.0.

Selección del protocolo de la capa de transporte

Cuando se configuran las ACL, es importante que sólo se especifiquen los protocolos de capa de transporte correctos. Muchos ingenieros de redes, cuando dudan acerca de si un flujo de tráfico particular usa un puerto TCP o un puerto UDP, configuran los dos. La especificación de ambos puertos abre un agujero en el firewall y posiblemente otorga acceso a los intrusos hacia la red. También introduce un elemento adicional en la ACL, por lo que el procesamiento de la ACL demora más y, así, se agrega más latencia a las comunicaciones de red.

Puertos de origen y destino

El control adecuado del tráfico entre dos hosts requiere elementos de control de acceso simétrico para las ACL de entrada y de salida. La información del puerto y la dirección para el tráfico generado por un host que responde es el reflejo de la información del puerto y la dirección para el tráfico generado por el host que inicia la transmisión.

Uso de la palabra clave established

La palabra clave **established** aumenta la seguridad provista por una ACL. Sin embargo, si se aplica la palabra clave a una ACL saliente, pueden obtenerse resultados inesperados.

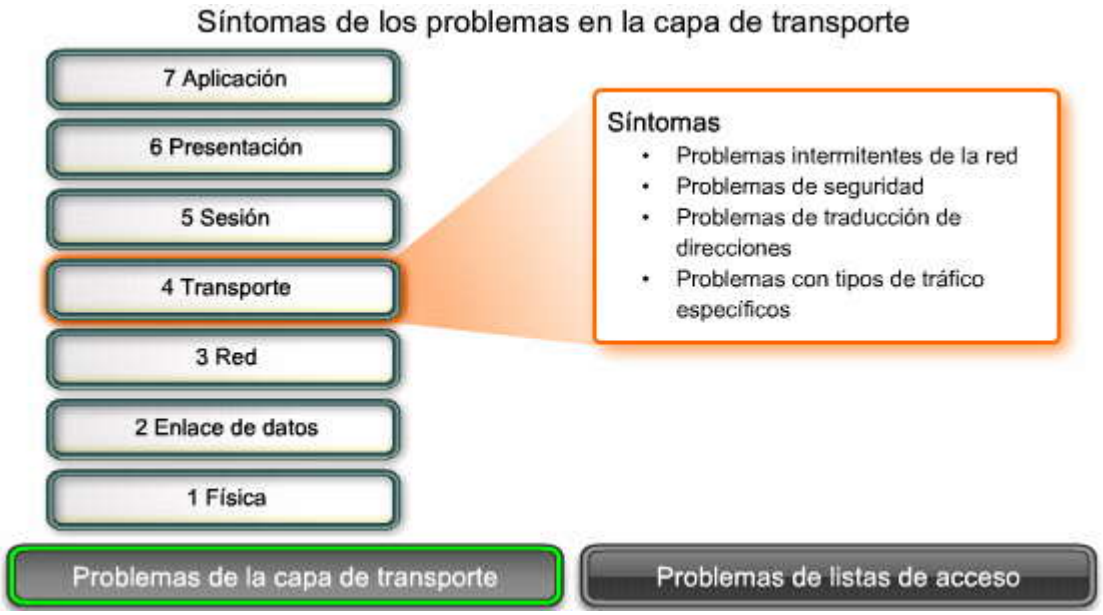
Protocolos poco frecuentes

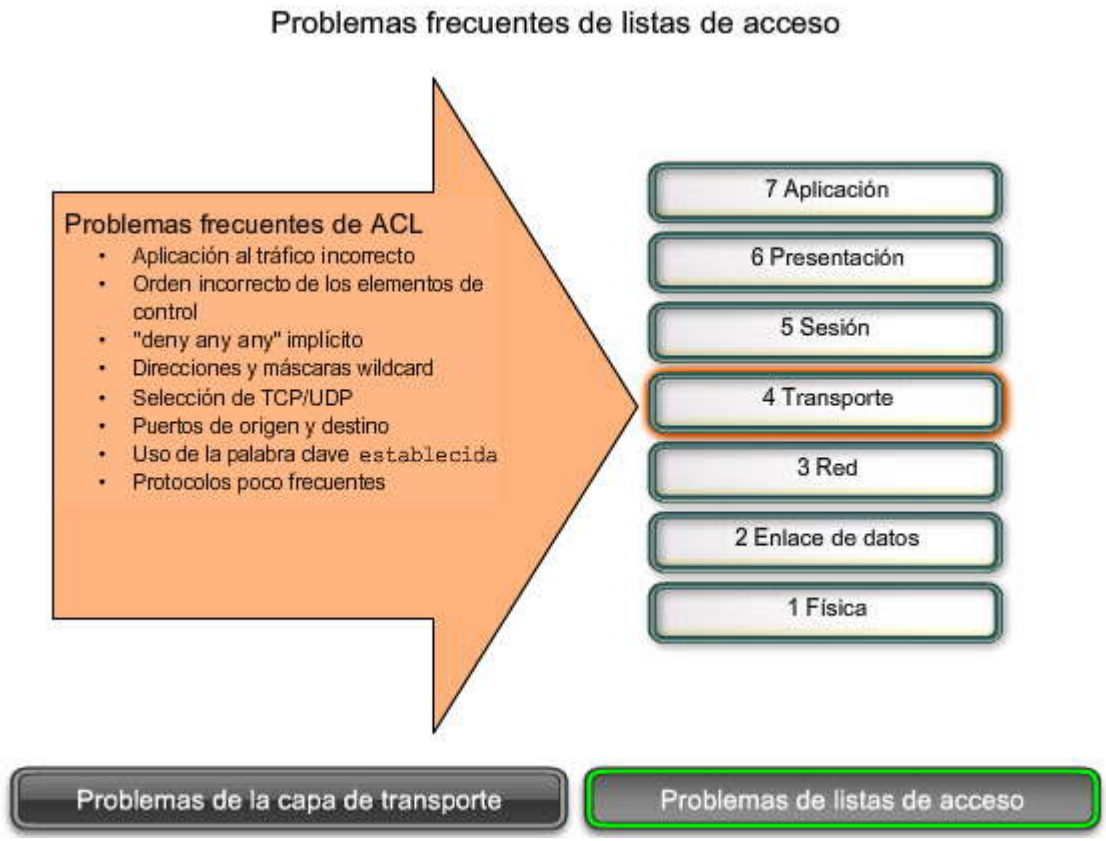
A menudo, las ACL configuradas incorrectamente causan problemas con los protocolos menos frecuentes que TCP y UDP. Los protocolos poco frecuentes que están aumentando su popularidad son VPN y los protocolos de encriptación.

Resolución de problemas de las listas de control de acceso

Un comando útil para observar el funcionamiento de la ACL es la palabra clave **log** en las entradas de ACL. Esta palabra clave le indica al router que coloque una entrada en el registro del sistema cuando hay una coincidencia con esa condición de entrada. El evento registrado incluye detalles del paquete que coincidió con el elemento de la ACL.

La palabra clave **log** es especialmente útil para la resolución de problemas y, además, proporciona información sobre los intentos de intrusión bloqueados por la ACL.





Problemas frecuentes de NAT

El mayor problema de las tecnologías de NAT es la interoperatividad con otras tecnologías de red, en especial con aquellas que contienen o derivan información de direccionamiento de red del host en el paquete. Entre estas tecnologías se incluyen:

- **BOOTP y DHCP**: ambos protocolos administran la asignación automática de direcciones IP a clientes. Recuerde que el primer paquete que envía un cliente nuevo es un paquete IP de broadcast de solicitud de DHCP. El paquete de solicitud de DHCP tiene la dirección IP de origen 0.0.0.0. Como la NAT requiere una dirección IP de origen y de destino válidas, puede haber problemas con el funcionamiento de BOOTP y DHCP sobre un router que ejecuta NAT estática o dinámica. La configuración de la función auxiliar de IP puede ayudar a resolver este problema.
- **DNS y WINS**: dado que un router que ejecuta NAT dinámica cambia la relación entre las direcciones internas y externas regularmente a medida que las entradas de la tabla vencen y se recrean, un servidor DNS o WINS fuera del router

NAT no tiene una representación exacta de la red dentro del router. La configuración de la función auxiliar de IP puede ayudar a resolver este problema.

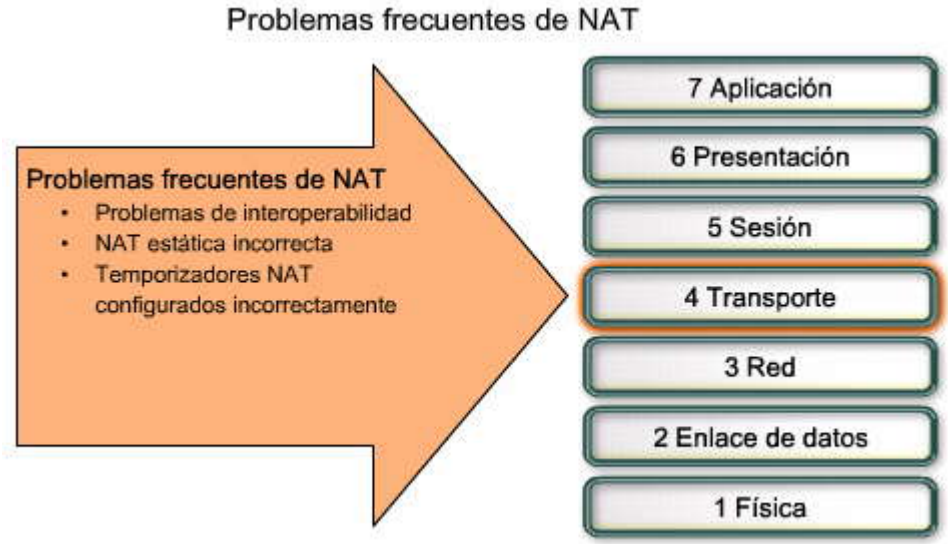
- **SNMP**: de forma similar a los paquetes DNS, NAT no puede modificar la información de direccionamiento almacenada en el contenido de datos del paquete. Por este motivo, es posible que una estación de administración de SNMP en un lado de un router NAT no pueda ponerse en contacto con los agentes SNMP del otro lado del router NAT. La configuración de la función auxiliar de IP puede ayudar a resolver este problema.
- **Protocolos de tunneling y encriptación**: los protocolos de tunneling y encriptación a menudo requieren que el tráfico se origine desde un puerto UDP o TCP específico o que se use un protocolo en la capa de transporte que la NAT no puede procesar. Por ejemplo, la NAT no puede procesar los protocolos de tunneling IPsec y los protocolos de encapsulación de enrutamiento genéricos que usan las implementaciones de VPN.

Si los protocolos de tunneling y encriptación deben ejecutarse a través de un router NAT, el administrador de red puede crear una entrada de NAT estática para el puerto necesario para una sola dirección IP dentro del router NAT.

Uno de los errores de configuración de NAT más frecuente es el olvido de que la NAT afecta tanto al tráfico entrante como al saliente. Un administrador de redes sin experiencia podría configurar una entrada de NAT estática para redireccionar el tráfico entrante a un host de respaldo interno específico. Esta sentencia de NAT estática también cambia la dirección de origen del tráfico desde ese host y, posiblemente, cause comportamientos inesperados e indeseados o un funcionamiento subóptimo.

Los temporizadores configurados de manera incorrecta también pueden causar comportamiento inesperado en la red y funcionamiento subóptimo de la NAT dinámica. Si los temporizadores de NAT son demasiado cortos, las entradas en la tabla NAT pueden vencer antes de que se reciban las respuestas y, por lo tanto, se descartan los paquetes. La pérdida de paquetes genera retransmisiones que consumen más ancho de banda. Si los temporizadores son demasiado largos, las entradas pueden permanecer más tiempo del necesario en la tabla NAT y consumir las conexiones disponibles. En las redes ocupadas, esto puede causar problemas de memoria en el router, y es posible que los hosts no puedan establecer conexiones si la tabla NAT dinámica está completa.

Consulte el capítulo 7, "Servicios de direccionamiento IP", para obtener más detalles sobre la resolución de problemas de configuración de NAT.



8.4.6 Resolución de problemas de la capa de aplicación

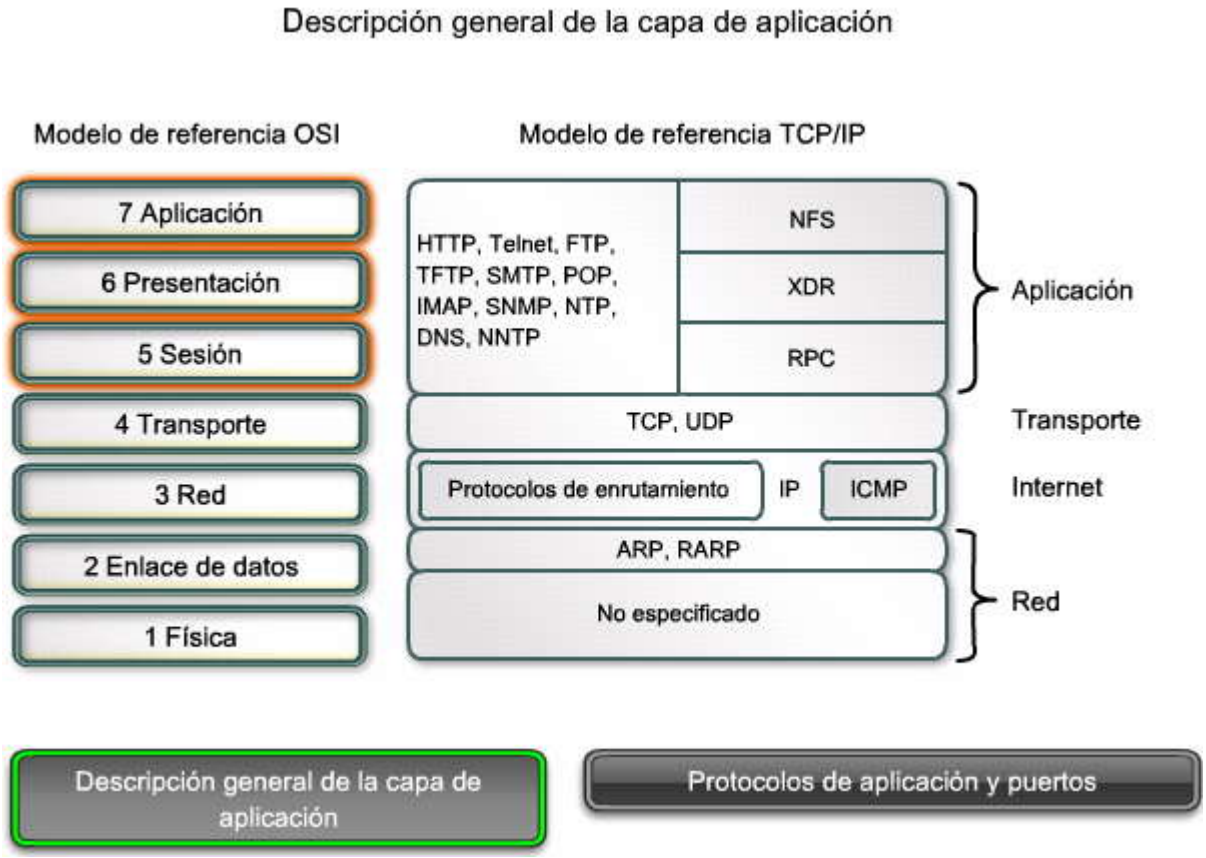
Descripción general de la capa de aplicación

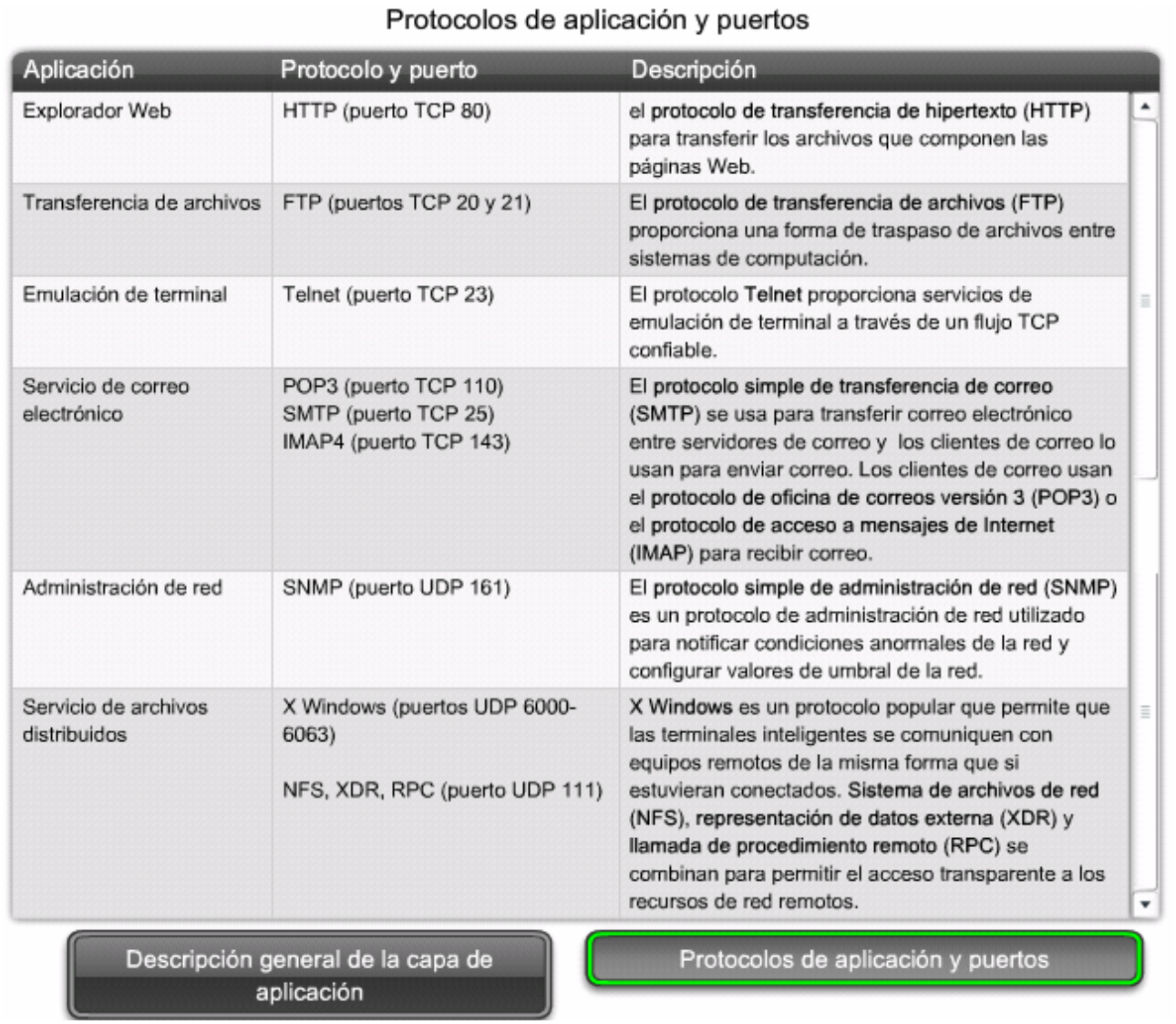
La mayor parte de los protocolos de la capa de aplicación proporciona servicios a los usuarios. Los protocolos de la capa de aplicación se usan en general para administración de la red, la transferencia de archivos, los servicios de archivos distribuidos, la emulación de terminal y el correo electrónico. Sin embargo, a menudo se agregan nuevos servicios de usuario, como VPN, VoIP, etc.

Entre los protocolos de capa de aplicación TCP/IP que más se conocen e implementan se incluyen:

- **Telnet**: permite a los usuarios establecer conexiones de sesión de terminal con hosts remotos.
- **HTTP**: admite el intercambio de texto, imágenes gráficas, sonido, video y otros archivos multimedia en la Web.
- **FTP**: realiza transferencias interactivas de archivos entre hosts.
- **TFTP**: realiza transferencias interactivas básicas de archivos entre hosts y dispositivos de red.
- **SMTP**: brinda soporte para los servicios básicos de envío de mensajes.
- **POP**: se conecta con servidores de correo y descarga correo electrónico.
- **Protocolo de administración de red simple (SNMP)**: recopila información de administración de los dispositivos de red.
- **DNS**: asigna direcciones IP a los nombres asignados a los dispositivos de red.
- **Sistema de archivos de red (NFS)**: permite a las computadoras montar unidades en hosts remotos y manejarlas como si fueran unidades locales. Desarrollado originalmente por Sun Microsystems, se combina con otros dos protocolos de capa de aplicación, representación de datos externa (XDR) y llamada de procedimiento remoto (RPC) para permitir el acceso transparente a los recursos de red remotos.

Haga clic en el botón Protocolos de aplicación y puertos de la figura para ver una lista de los protocolos de aplicación y los puertos asociados.





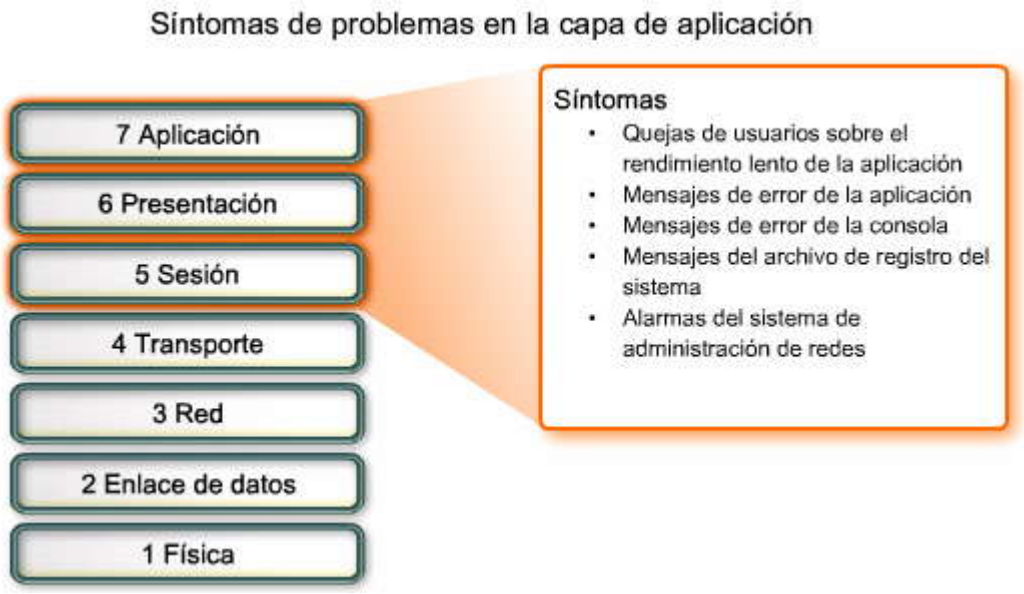
Síntomas de los problemas de la capa de aplicación

Los problemas de la capa de aplicación impiden que se proporcionen servicios a los programas de aplicación. Un problema en la capa de aplicación puede hacer que los recursos se vuelvan inutilizables o inalcanzables cuando las capas física, de enlace de datos, de red y de transporte están en funcionamiento. Es posible tener conectividad de red completa, pero la aplicación simplemente no puede proporcionar datos.

Otro tipo de problema en la capa de aplicación ocurre cuando las capas física, de enlacede datos, de red y de transporte están en funcionamiento, pero la transferencia de datos y las solicitudes de servicios de red de un solo servicio de red o aplicación no cumplen las expectativas normales de un usuario.

Un problema en la capa de aplicación puede originar quejas de los usuarios porque la red o la aplicación particular con la que están trabajando funciona más lento de lo normal cuando se transfieren datos o se solicitan servicios de red.

La figura muestra algunos de los síntomas posibles delos problemas de la capa de aplicación.



Resolución de problemas de la capa de aplicación

El mismo proceso de resolución de problemas general que se usa para aislar problemas en las capas inferiores puede usarse para aislar problemas en la capa de aplicación. Los conceptos son los mismos, pero el enfoque tecnológico ha cambiado para incluir aspectos como conexiones rechazadas o con el tiempo de espera agotado, listas de acceso y problemas de DNS.

Los pasos para la resolución de problemas de la capa de aplicación son los siguientes:

Paso 1. Hacer ping al gateway predeterminado.

Si se realiza adecuadamente, los servicios de capa 1 y capa 2 están funcionando correctamente.

Paso 2. Verificar la conectividad de extremo a extremo.

Use un ping extendido si intenta hacer ping desde un router Cisco. Si se realiza adecuadamente, la capa 3 está funcionando correctamente. Si las capas 1 a 3 funcionan correctamente, el problema debe estar en una capa superior.

Paso 3. Verificar el funcionamiento de la NAT y las listas de acceso.

Para resolver problemas en las listas de control de acceso, realice los siguientes pasos:

- Use el comando **show access-list**. ¿Existen ACL que podrían estar deteniendo el tráfico? Observe cuáles listas de acceso tienen coincidencias.
- Borre los contadores de la lista de acceso con el comando **clear access-list counters** e intente establecer una conexión nuevamente.
- Verifique los contadores de la lista de acceso. ¿Alguno aumentó? ¿Deben aumentar?

Para resolver problemas de NAT, realice los siguientes pasos:

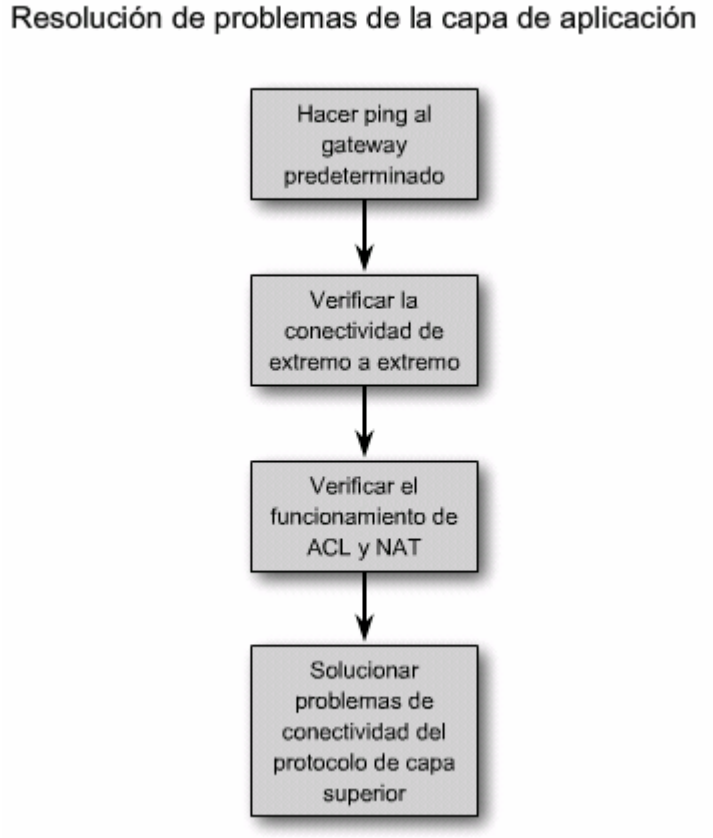
- Use el comando **show ip nat translations**. ¿Existen traducciones? ¿Las traducciones son las esperadas?
- Borre las traducciones NAT con el comando **clear ip nat translation *** e intente acceder al recurso externo nuevamente.
- Use el comando **debug ip nat** y examine el resultado.
- Observe el archivo de configuración en ejecución. ¿Los comandos **ip nat inside** e **ip nat outside** están ubicados en las interfaces correctas? ¿El conjunto de NAT está configurado correctamente? ¿La ACL está identificandolos hosts de manera correcta?

Si las ACL y la NAT están funcionando de la manera esperada, el problema debe estar en una capa superior.

Paso 4. Solucionar problemas de conectividad del protocolo de capa superior.

Aunque haya conectividad IP entre un origen y un destino, aún pueden existir problemas para un protocolo de capa superior específico, como FTP, HTTP o Telnet. Estos protocolos se ejecutan sobre el transporte IP básico, pero están sujetos a problemas específicos de cada protocolo relacionados con filtros de paquetes y firewalls. Es posible que todas las funciones, excepto el correo, funcionen entre un origen y un destino dados.

La resolución de un problema de conectividad del protocolo de capa superior requiere la comprensión del proceso del protocolo. En general, esta información se encuentra en la RFC más reciente para el protocolo o en la página Web del desarrollador.



Corrección de problemas de la capa de aplicación

Los pasos para la corrección de problemas de la capa de aplicación son los siguientes:

Paso 1: Hacer una copia de seguridad. Antes de continuar, asegúrese de que se haya guardado una configuración válida para todos los dispositivos cuya configuración pueda modificarse. Esto permite la recuperación a un estado inicial conocido

Paso 2: Hacer un cambio en la configuración inicial del hardware o software. Si la corrección requiere más de un cambio, haga sólo un cambio por vez.

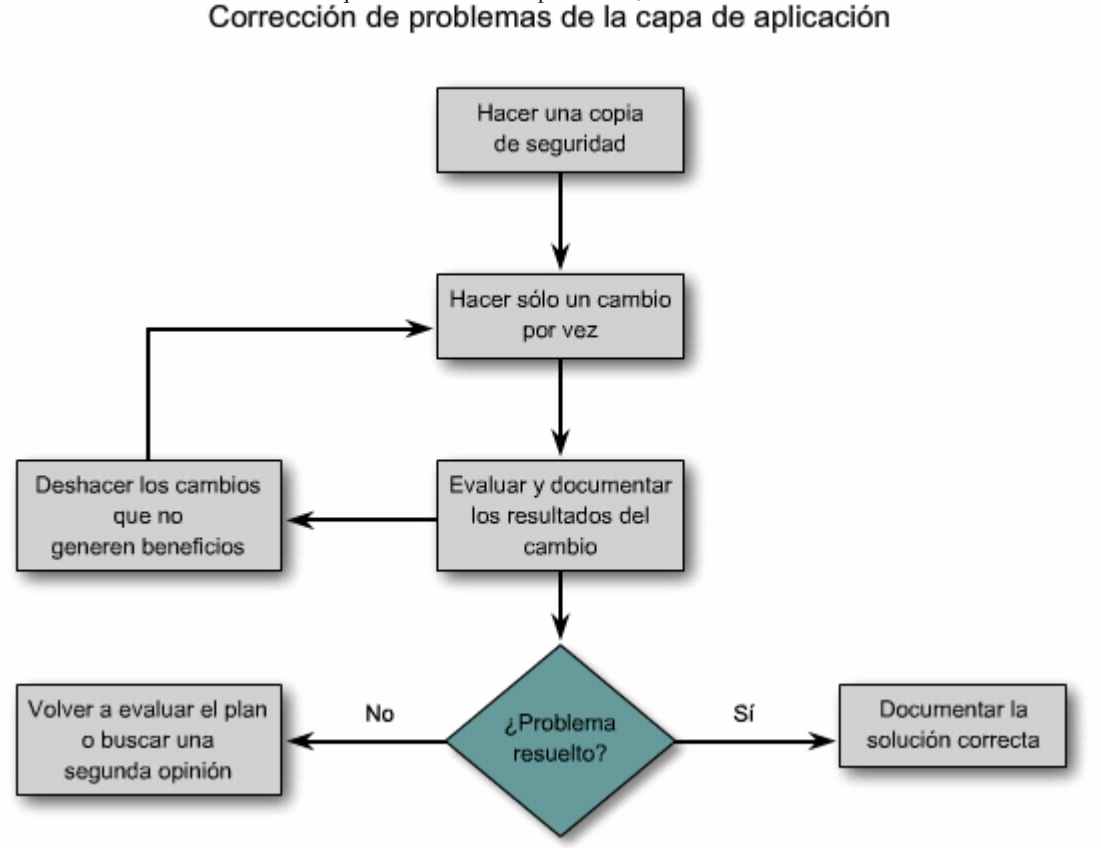
Paso 3: Evaluar y documentar cada cambio y sus resultados. Si los resultados de alguno de los pasos para la resolución de problemas no son satisfactorios, deben deshacerse los cambios inmediatamente. Si el problema es intermitente, aguarde para ver si el problema vuelve a ocurrir antes de evaluar el efecto de algún cambio.

Paso 4: Determinar si el cambio resuelve el problema. Verifique que el cambio realmente resuelve el problema sin introducir nuevos problemas. La red debe volver al funcionamiento de línea de base y no deben presentarse síntomas nuevos o antiguos. Si el problema no se resuelve, deben deshacerse todos los cambios. Si se descubren problemas nuevos o adicionales, modifique el plan de corrección.

Paso 5: Detenerse cuando se resuelva el problema. Deje de hacer cambios cuando parezca que el problema original está resuelto.

Paso 6: De ser necesario, solicitar la ayuda de recursos externos. Puede ser un compañero de trabajo, un consultor o el Centro de asistencia técnica (TAC) de Cisco. En algunas ocasiones, puede ser necesario un volcado de memoria, el cual genera un resultado que puede analizar un especialista de Cisco Systems.

Paso 7: Documentar. Una vez que se soluciona el problema, debe documentarse la solución.



Para completar satisfactoriamente esta actividad, se necesita la documentación final de la Actividad PT 8.1.2: Descubrimiento y documentación de redes, que completó anteriormente en este capítulo. Esta documentación debe tener un diagrama de topología y una tabla de direccionamiento precisos. Si no tiene esta documentación, solicite a su instructor las versiones exactas.
Se proporcionan instrucciones detalladas dentro de la actividad y en el siguiente enlace al PDF.
Instrucciones de las actividades (PDF)