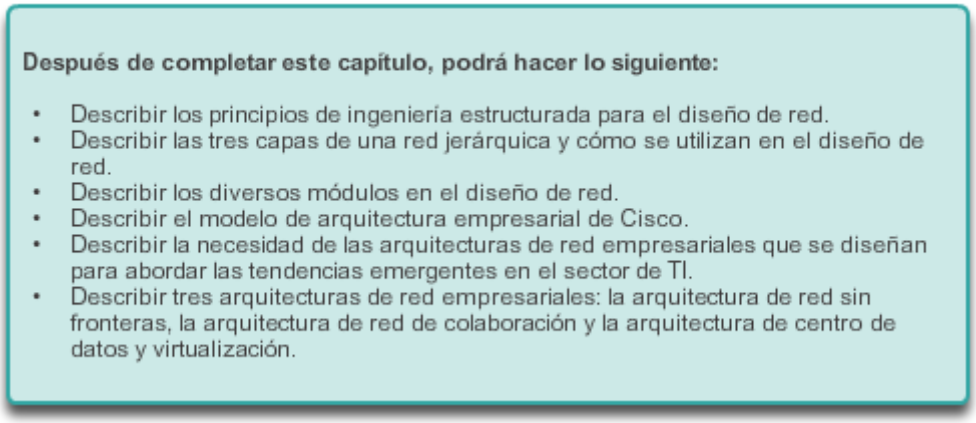
Capítulo 1: Diseño jerárquico de la red 1.0.1.1 Introducción

Las redes deben satisfacer las necesidades actuales de las organizaciones y admitir tecnologías emergentes a medida que se adoptan nuevas tecnologías. Los principios y los modelos de diseño de red pueden ayudar a un ingeniero de red a diseñar y armar una red que sea flexible, resistente y fácil de administrar.

En este capítulo, se presentan los conceptos, los principios, los modelos y las arquitecturas del diseño de red. Se abarcan los beneficios que se obtienen mediante un enfoque de diseño sistemático. También se analizan las tendencias tecnológicas emergentes que afectan la evolución de las redes.



Capítulo 1: Diseño jerárquico de la red 1.0.1.2 Actividad de clase: Jerarquía de diseño

Jerarquía de diseño

A un administrador de red se le asigna la tarea de diseñar una red ampliada para la empresa.

Después de hablar con los administradores de red de otras sucursales de la empresa, se decidió utilizar el modelo de diseño de red jerárquico de tres capas de Cisco para influir en la expansión. Este modelo se eligió debido a su influencia simple en la planificación de la red.

Las tres capas del diseño de la red ampliada incluyen lo siguiente:

- Acceso
- Distribución
- Núcleo

Actividad de clase: Jerarquía de diseño

Capítulo 1: Diseño jerárquico de la red 1.1.1.1 Requisitos de la red

Cuando se analiza el diseño de red, es útil categorizar las redes según la cantidad de dispositivos que se atienden:

- **Red pequeña:** proporciona servicios para hasta 200 dispositivos.
- **Red mediana:** proporciona servicios para 200 a 1000 dispositivos.
- **Red grande:** proporciona servicios para más de 1000 dispositivos.

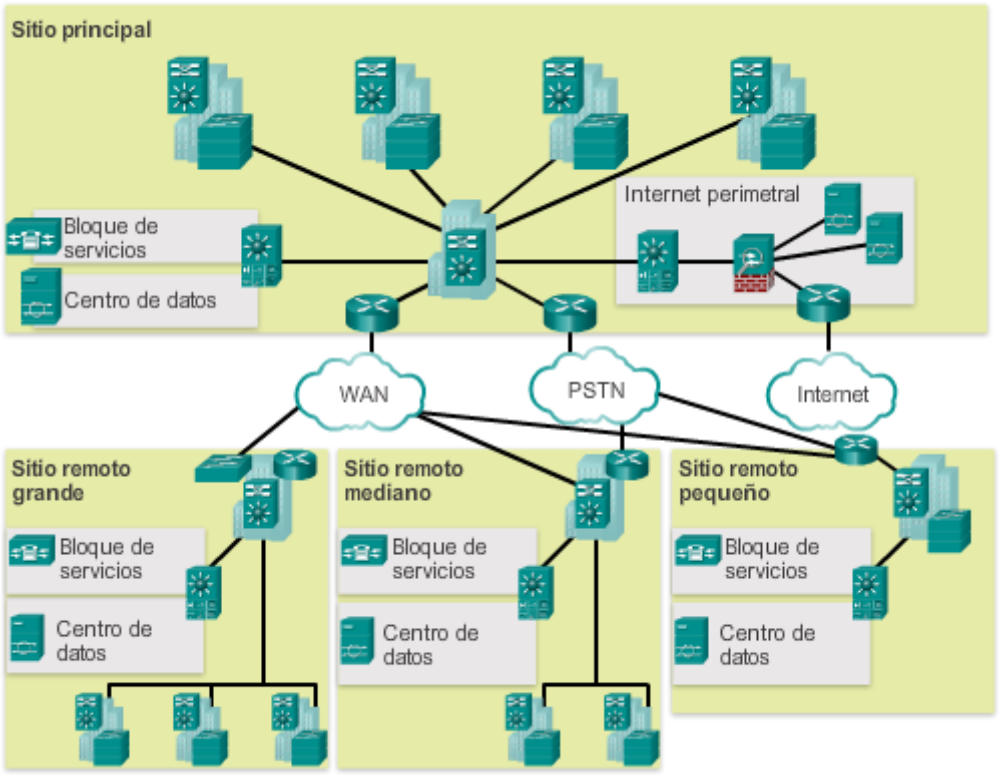
Los diseños de red varían según el tamaño y las necesidades de las organizaciones. Por ejemplo, las necesidades de infraestructura de red de una organización pequeña con menos dispositivos son menos complejas que la infraestructura de una organización grande con una cantidad importante de dispositivos y conexiones.

Existen muchas variables para tener en cuenta al diseñar una red. Tenga en cuenta el ejemplo de la ilustración. El diagrama de topología de alto nivel de ejemplo es para una red empresarial grande que consta de un campus principal que conecta sitios pequeños, medianos y grandes.

El diseño de red es un área en expansión y requiere mucho conocimiento y experiencia. El objetivo de esta sección es presentar conceptos de diseño de red ampliamente aceptados.

Nota: Cisco Certified Design Associate (CCDA®) es una certificación reconocida en el sector para los ingenieros y técnicos de diseño de red, así como para los ingenieros de soporte, que demuestran las habilidades requeridas para diseñar redes básicas de campus, de centro de datos, de seguridad, de voz e inalámbricas.

Diseño de una red empresarial grande



Capítulo 1: Diseño jerárquico de la red 1.1.1.2 Principios de ingeniería estructurada

Independientemente del tamaño o los requisitos de la red, un factor fundamental para la correcta implementación de cualquier diseño de red es seguir buenos principios de ingeniería estructurada. Estos principios incluyen lo siguiente:

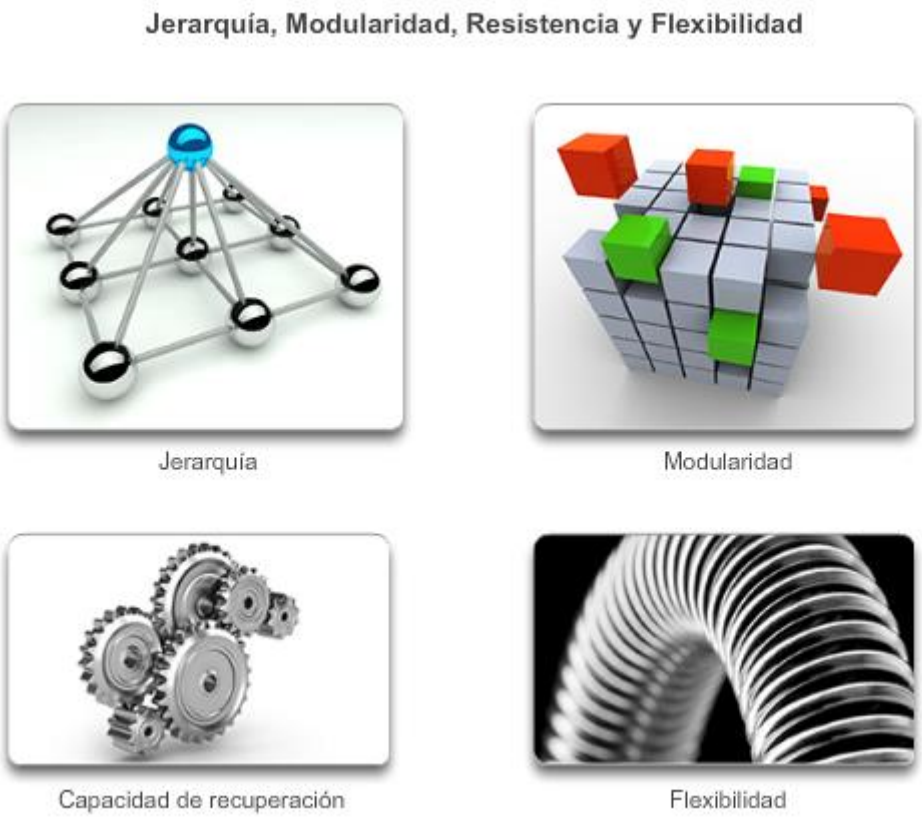
- **Jerarquía:** un modelo de red jerárquico es una herramienta útil de alto nivel para diseñar una infraestructura de red confiable. Divide el problema complejo del diseño de red en áreas más pequeñas y más fáciles de administrar.

- **Modularidad:** al separar en módulos las diversas funciones que existen en una red, esta es más fácil diseñar. Cisco identificó varios módulos, incluido el campus empresarial, el bloque de servicios, el centro de datos e Internet perimetral.

- **Resistencia:** la red debe estar disponible para que se pueda utilizar tanto en condiciones normales como anormales. Entre las condiciones normales se incluyen los flujos y los patrones de tráfico normales o esperados, así como los eventos programados, como los períodos de mantenimiento. Entre las condiciones anormales se incluyen las fallas de hardware o de software, las cargas de tráfico extremas, los patrones de tráfico poco comunes, los eventos de denegación de servicio (DoS), ya sean intencionales o involuntarios, y otros eventos imprevistos.

- **Flexibilidad:** la capacidad de modificar partes de la red, agregar nuevos servicios o aumentar la capacidad sin necesidad de realizar actualizaciones de gran importancia (es decir, reemplazar los principales dispositivos de hardware).

Para cumplir con estos objetivos fundamentales del diseño, la red se debe armar sobre la base de una arquitectura de red jerárquica que permita la flexibilidad y el crecimiento.



Capítulo 1: Diseño jerárquico de la red 1.1.2.1 Jerarquía de red

En la tecnología de redes, un diseño jerárquico implica dividir la red en capas independientes. Cada capa (o nivel) en la jerarquía proporciona funciones específicas que definen su función dentro de la red general. Esto ayuda al diseñador y al arquitecto de red a optimizar y seleccionar las características, el hardware y el software de red adecuados para llevar a cabo las funciones específicas de esa capa de red. Los modelos jerárquicos se aplican al diseño de LAN y WAN.

Un diseño típico de red LAN jerárquica de campus empresarial incluye las siguientes tres capas:

- **Capa de acceso:** proporciona acceso a la red para los grupos de trabajo y los usuarios.
- **Capa de distribución:** proporciona una conectividad basada en políticas y controla el límite entre las capas de acceso y de núcleo.
- **Capa de núcleo:** proporciona un transporte rápido entre los switches de distribución dentro del campus empresarial.

El beneficio de dividir una red plana en bloques más pequeños y fáciles de administrar es que el tráfico local sigue siendo local. Sólo el tráfico destinado a otras redes se traslada a una capa superior.

Los dispositivos de Capa 2 en una red plana brindan pocas oportunidades de controlar broadcasts o filtrar tráfico no deseado. A medida que se agregan más dispositivos y

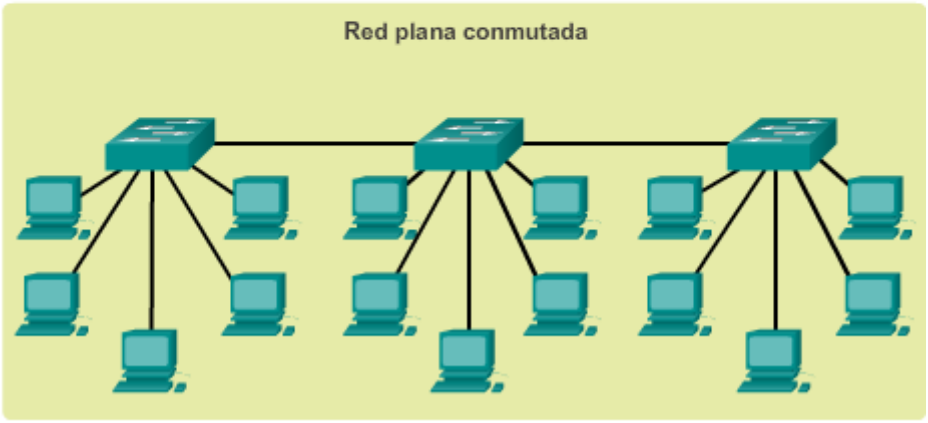
aplicaciones a una red plana, los tiempos de respuesta se degradan hasta que la red queda inutilizable.

Haga clic en Reproducir en la figura 1 para ver la transición de un diseño de red plana a un diseño de red jerárquico.

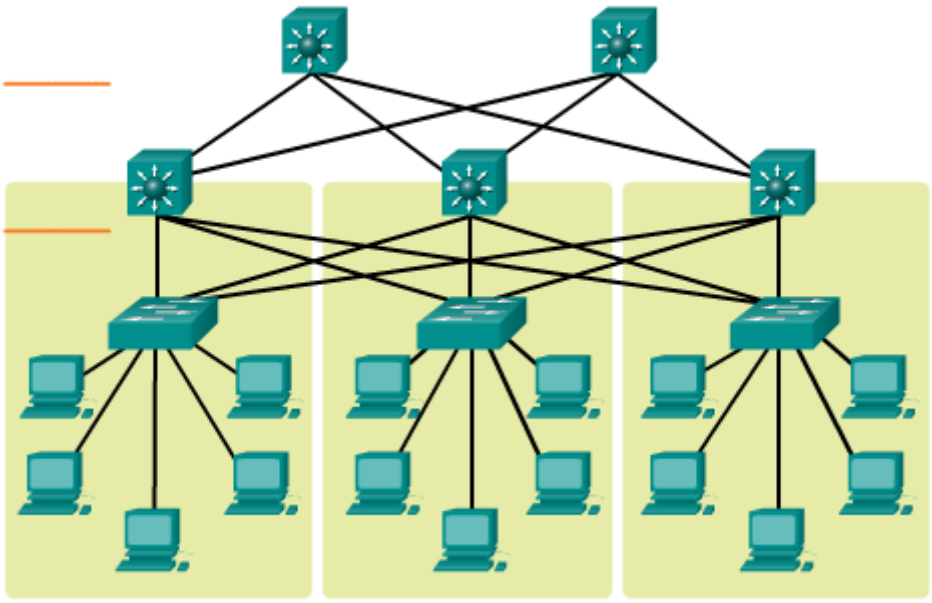
En la figura 2, se muestra otro ejemplo de diseño de red jerárquico de tres capas. Observe que cada edificio utiliza el mismo modelo de red jerárquico que incluye las capas de acceso, de distribución y de núcleo.

Nota: no existen reglas absolutas sobre la forma en que se debe armar físicamente una red de campus. Si bien es cierto que muchas redes de campus se construyen con tres niveles físicos de switches, no es un requisito estricto. En un campus más pequeño, la red puede tener dos niveles de switches en los que los elementos de núcleo y de distribución se combinan en un switch físico. Esto se denomina “diseño de núcleo contraído”.

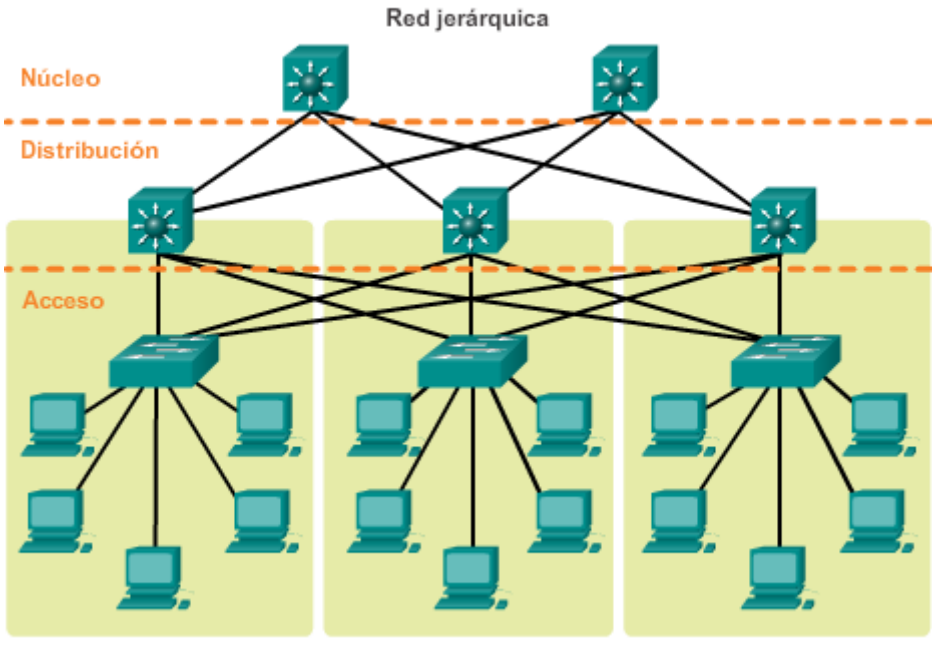
Diseño jerárquico de la red



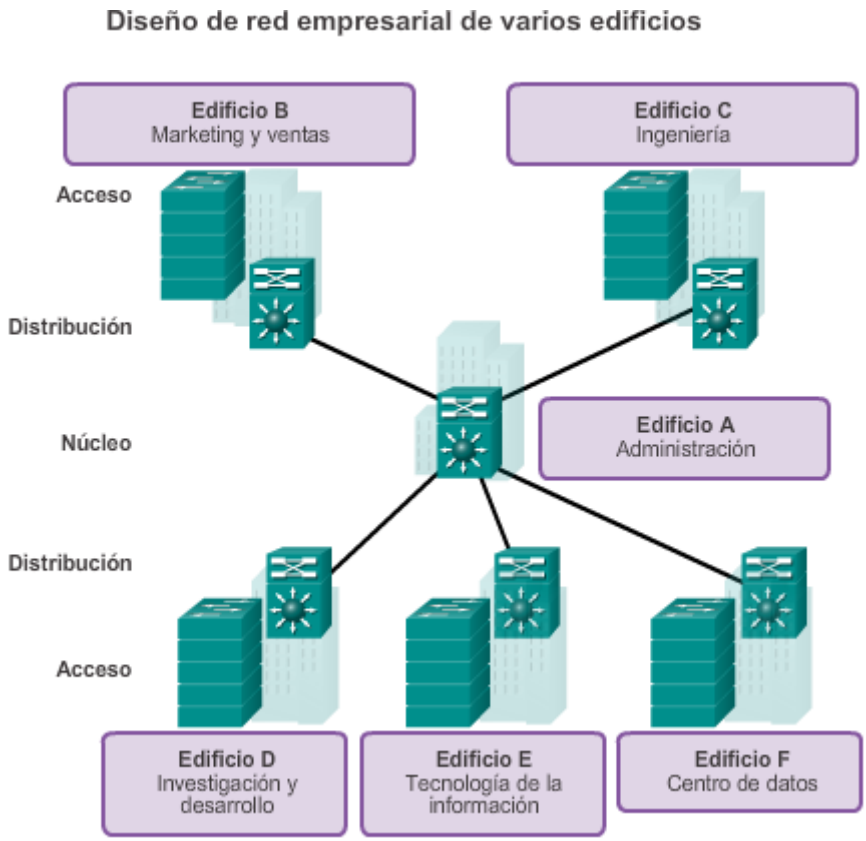
Diseño jerárquico de la red



Diseño jerárquico de la red



Tres dominios de broadcast separados



Capítulo 1: Diseño jerárquico de la red 1.1.2.2 Capa de acceso

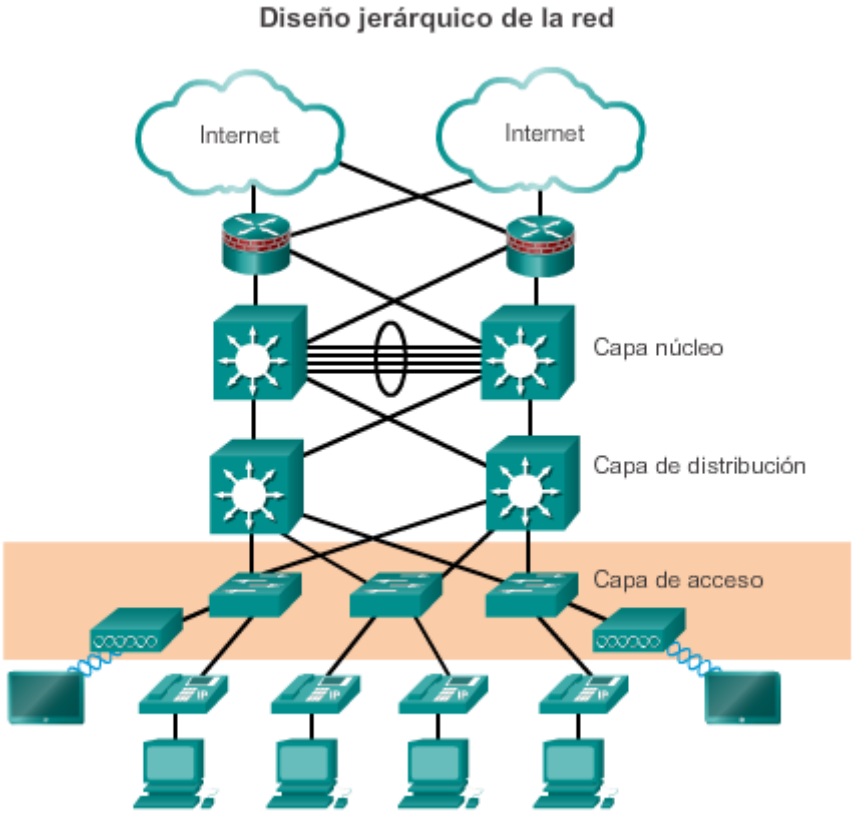
En un entorno LAN, la capa de acceso otorga acceso a la red para las terminales. En el entorno WAN, puede proporcionar acceso a la red empresarial para los trabajadores a distancia o los sitios remotos a través de conexiones WAN.

Como se muestra en la ilustración, la capa de acceso para la red de una pequeña empresa, por lo general, incorpora switches de capa 2 y puntos de acceso que proporcionan conectividad entre las estaciones de trabajo y los servidores.

La capa de acceso cumple varias funciones, incluido lo siguiente:

- Switching de capa 2
- Alta disponibilidad
- Seguridad del puerto
- Clasificación y marcación de QoS, y límites de confianza
- Inspección del protocolo de resolución de direcciones (ARP)
- Listas de control de acceso virtual (VACL)
- Árbol de expansión

- Alimentación por Ethernet y VLAN auxiliares para VoIP



Capítulo 1: Diseño jerárquico de la red 1.1.2.3 En la Capa de distribución.

La capa de distribución agrega los datos recibidos de los switches de la capa de acceso antes de que se transmitan a la capa núcleo para el enrutamiento hacia su destino final. En la ilustración, la capa de distribución es el límite entre los dominios de capa 2 y la red enrutada de capa 3.

El dispositivo de capa de distribución es el centro en los armarios de cableado. Para segmentar los grupos de trabajo y aislar los problemas de la red en un entorno de campus, se utiliza un router o un switch multicapa.

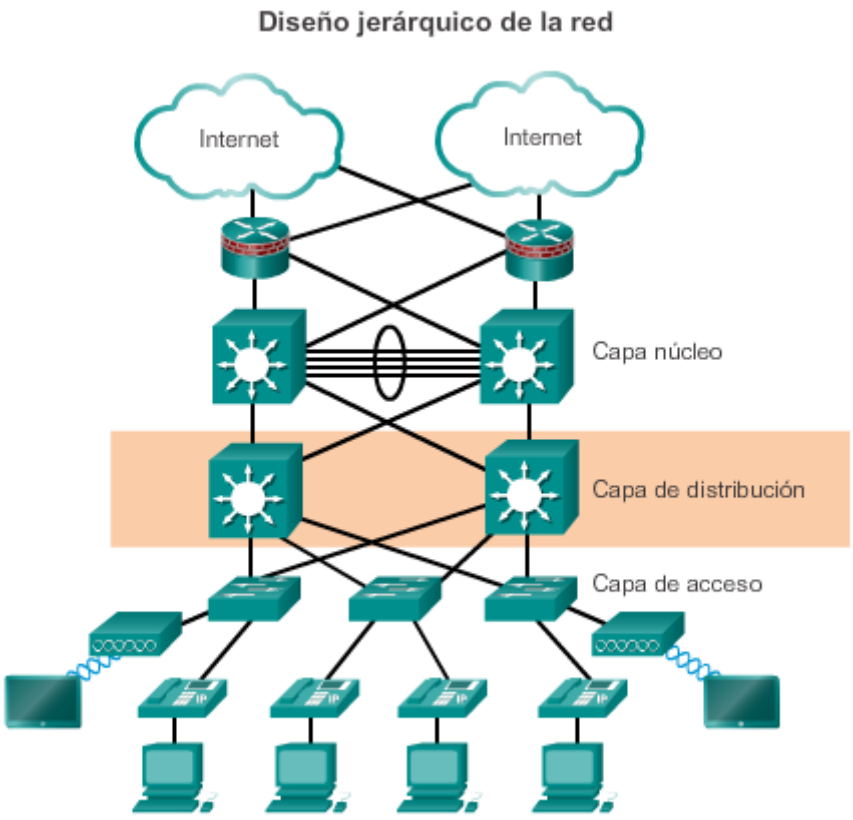
Un switch de capa de distribución puede proporcionar servicios ascendentes para muchos switches de capa de acceso.

La capa de distribución puede proporcionar lo siguiente:

- Agregación de enlaces LAN o WAN.
- Seguridad basada en políticas en forma de listas de control de acceso (ACL) y filtrado.
- Servicios de routing entre redes LAN y VLAN, y entre dominios de routing (p. ej., EIGRP a OSPF).
- Redundancia y balanceo de carga.

- Un límite para la agregación y la sumarización de rutas que se configura en las interfaces hacia la capa de núcleo.

- Control del dominio de difusión, ya que ni los routers ni los switches multicapa reenvían difusiones. El dispositivo funciona como punto de demarcación entre los dominios de difusión.



Capítulo 1: Diseño jerárquico de la red 1.1.2.4 Capa de núcleo

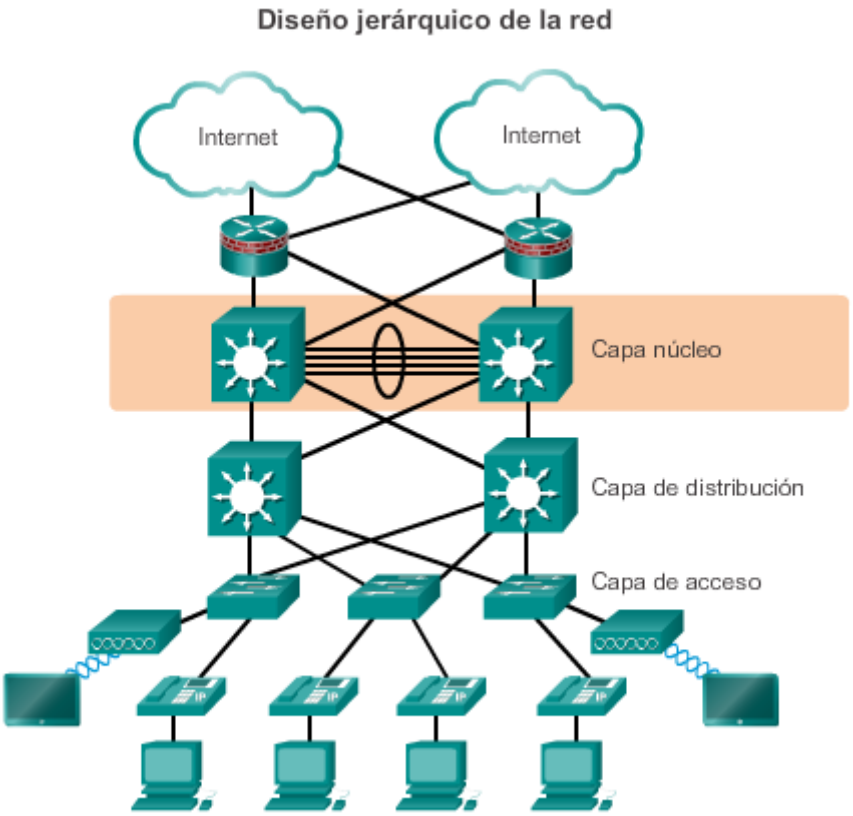
La capa de núcleo también se conoce como “backbone de red”. La capa de núcleo consta de dispositivos de red de alta velocidad, como los switches Cisco Catalyst 6500 o 6800. Estos están diseñados para conmutar paquetes lo más rápido posible e interconectar varios componentes de campus, como módulos de distribución, módulos de servicio, el centro de datos y el perímetro de la WAN.

Como se muestra en la ilustración, la capa de núcleo es fundamental para la interconectividad entre los dispositivos de capa de distribución; por ejemplo, interconecta el bloque de distribución al perímetro de la WAN y de Internet. El núcleo debe tener una alta disponibilidad y debe ser redundante. El núcleo agrega el tráfico de todos los dispositivos de la capa de distribución, por lo tanto debe poder enviar grandes cantidades de datos rápidamente.

Algunas de las consideraciones en cuanto a la capa de núcleo incluyen lo siguiente:

- Debe proporcionar switching de alta velocidad (es decir, un transporte rápido).

- Debe proporcionar confiabilidad y tolerancia a fallas.
- Debe lograr la escalabilidad mediante equipos más rápidos, no con más equipos.
- Debe evitar la manipulación de paquetes que implica una gran exigencia para la CPU a causa de la seguridad, la inspección, la clasificación de la calidad de servicio (QoS) u otros procesos.



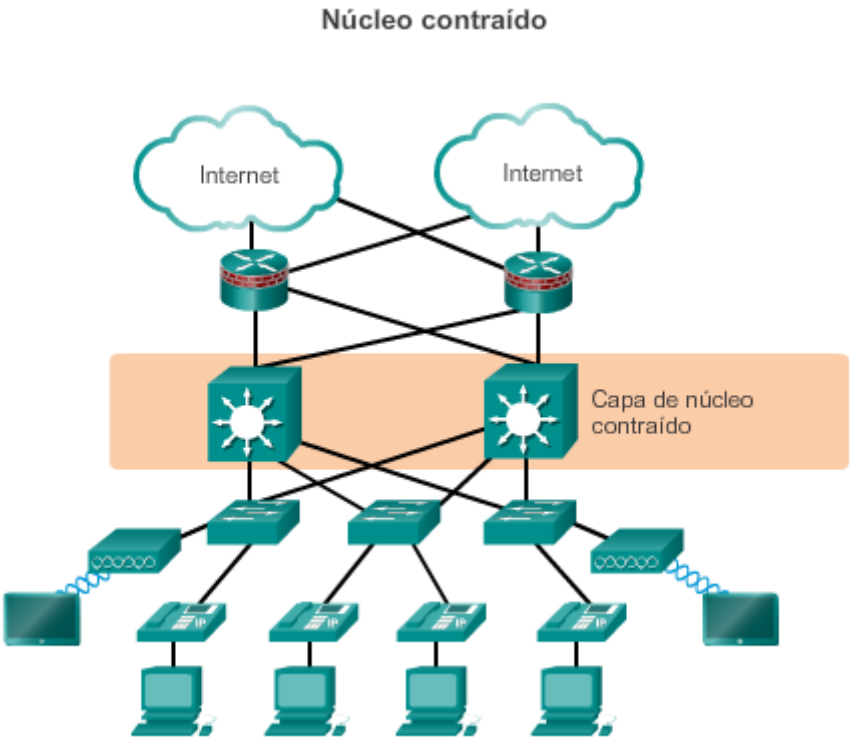
Capítulo 1: Diseño jerárquico de la red 1.1.2.5 Diseño de núcleo contraído de dos niveles

El diseño jerárquico de tres niveles maximiza el rendimiento, la disponibilidad de la red y la capacidad de escalar el diseño de red.

Sin embargo, hay muchas redes de pequeñas empresas que no crecen mucho con el tiempo. Por lo tanto, un diseño jerárquico de dos niveles en el que las capas de núcleo y de distribución se combinan en una sola capa suele ser más práctico. Existe un “núcleo contraído” cuando las funciones de la capa de distribución y de la capa de núcleo se implementan mediante un único dispositivo. La principal motivación para elegir el diseño de núcleo contraído es la reducción de costos de la red, a la vez que se mantiene la mayoría de los beneficios del modelo jerárquico de tres niveles.

En el ejemplo de la ilustración, se contrajo la funcionalidad de la capa de distribución y la capa de núcleo en dispositivos de switch multicapa.

El modelo de red jerárquico proporciona un marco modular que brinda flexibilidad al diseño de red y facilita su implementación y la resolución de problemas.



Capítulo 1: Diseño jerárquico de la red 1.1.2.6 Actividad: Identificar las características de las redes jerárquicas

Actividad: Identificar las características de las redes jerárquicas

Haga clic en el campo correspondiente para unir las características del diseño jerárquico con las capas.

	Capa de acceso	Capa de distribución	Capa de núcleo
Permite los servicios de transporte rápido entre los campus.			✓
Proporciona la admisión a la red para los usuarios y los grupos de trabajo de la red.	✓		
Proporciona conectividad y control de red basados en políticas.		✓	

Capítulo 1: Diseño jerárquico de la red 1.2.1.1 Diseño modular

Si bien el diseño de red jerárquico funciona bien dentro de la infraestructura del campus, las redes se expandieron más allá de estas fronteras. Como se muestra en la ilustración, las redes se volvieron más sofisticadas y complejas, y algunas requieren conexiones a centros de datos dedicados, que por lo general son externos. A menudo, las sucursales requieren conectividad a los backbones de campus, y los empleados necesitan poder trabajar desde sus oficinas domésticas u otras ubicaciones remotas. Debido a que la complejidad de la red para satisfacer estas demandas aumentó, se volvió necesario modificar el diseño de la red por uno que utilizara un enfoque más modular.

Un diseño de red modular separa la red en varios módulos de red funcionales, y cada uno de estos apunta a un lugar o un propósito específico en la red. Los módulos representan áreas que tienen una conectividad física o lógica diferente. Se encargan de designar dónde se llevan a cabo las diferentes funciones en la red. El enfoque modular tiene varios beneficios, incluidos los siguientes:

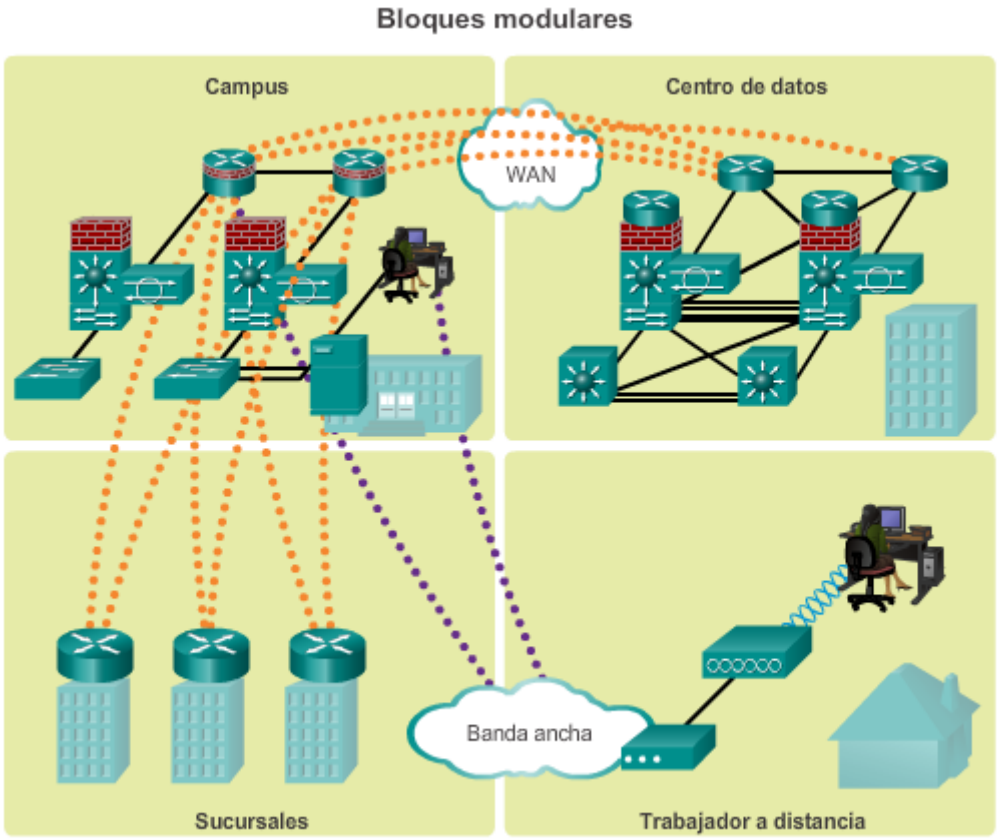
- Las fallas que ocurren dentro de un módulo se pueden aislar del resto de la red, lo que permite una detección de problemas más sencilla y una mayor disponibilidad general del sistema.

- Los cambios, las actualizaciones o la introducción de nuevos servicios de redes se pueden realizar de forma controlada y gradual, lo que permite una mayor flexibilidad en el mantenimiento y el funcionamiento de la red del campus.

- Cuando un módulo específico ya no posee la capacidad suficiente o no tiene una función o un servicio nuevos, se puede actualizar o reemplazar con otro módulo que tenga la misma función estructural en el diseño jerárquico general.

- Se puede implementar seguridad de forma modular, lo que permite un control más detallado de la seguridad.

El uso de módulos en el diseño de red brinda flexibilidad y facilita su implementación y la resolución de problemas.



Capítulo 1: Diseño jerárquico de la red 1.2.1.2 Módulos en la arquitectura empresarial

El enfoque modular aplicado al diseño de red divide aún más el diseño jerárquico de tres capas, ya que elimina bloques específicos o áreas modulares. Estos módulos básicos están conectados entre sí a través del núcleo de la red.

Los módulos de red básicos incluyen lo siguiente:

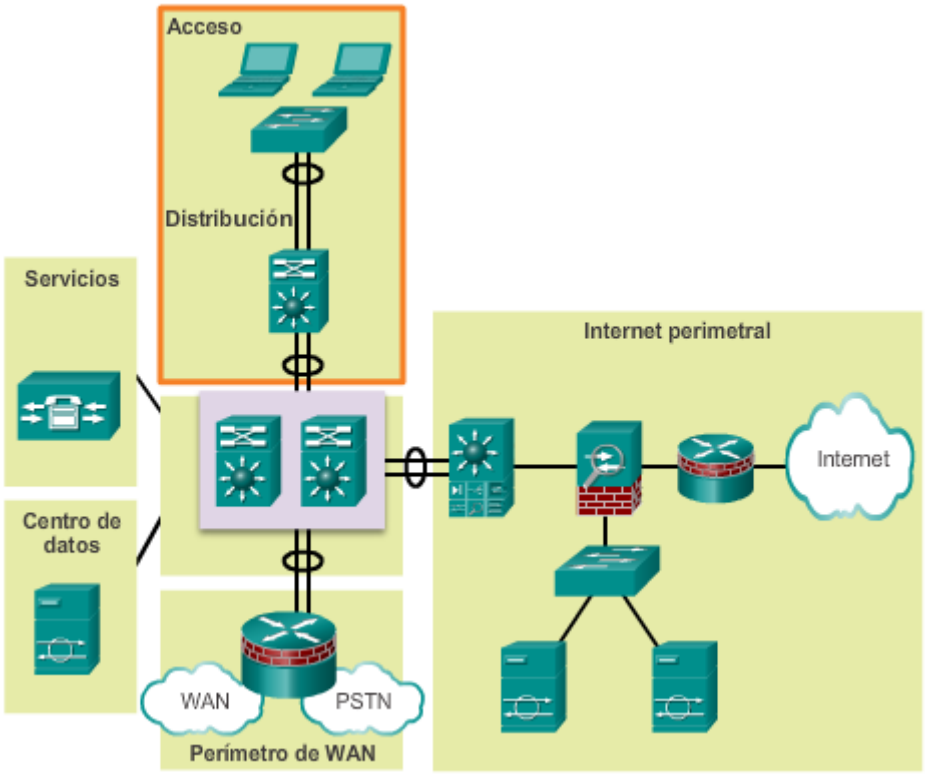
- **Acceso y distribución:** también denominado “bloque de distribución”, es el elemento más conocido y el componente fundamental del diseño de campus (figura 1).

- **Servicios:** este es un bloque genérico que se utiliza para identificar servicios como los controladores inalámbricos centralizados del protocolo de punto de acceso ligero (LWAPP), los servicios de comunicaciones unificadas, los gateways de políticas, entre otros (figura 2).

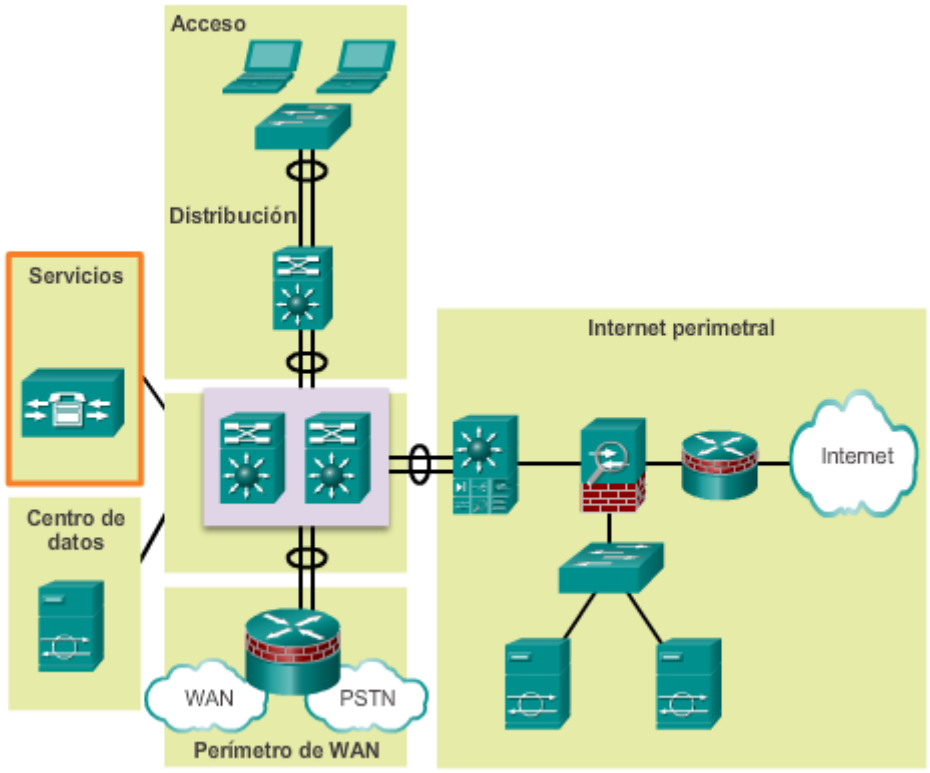
- **Centro de datos:** originalmente, se denominaba “granja de servidores”. Este bloque es responsable de administrar y mantener muchos sistemas de datos que son fundamentales para las operaciones comerciales modernas. Los empleados, los socios y los clientes confían en los datos y los recursos del centro de datos para crear, colaborar e interactuar de manera eficaz (figura 3).

- **Perímetro empresarial:** consta de Internet perimetral y del perímetro de WAN. Estos bloques ofrecen conectividad a servicios de voz, de video y de datos fuera de la empresa (figura 4).

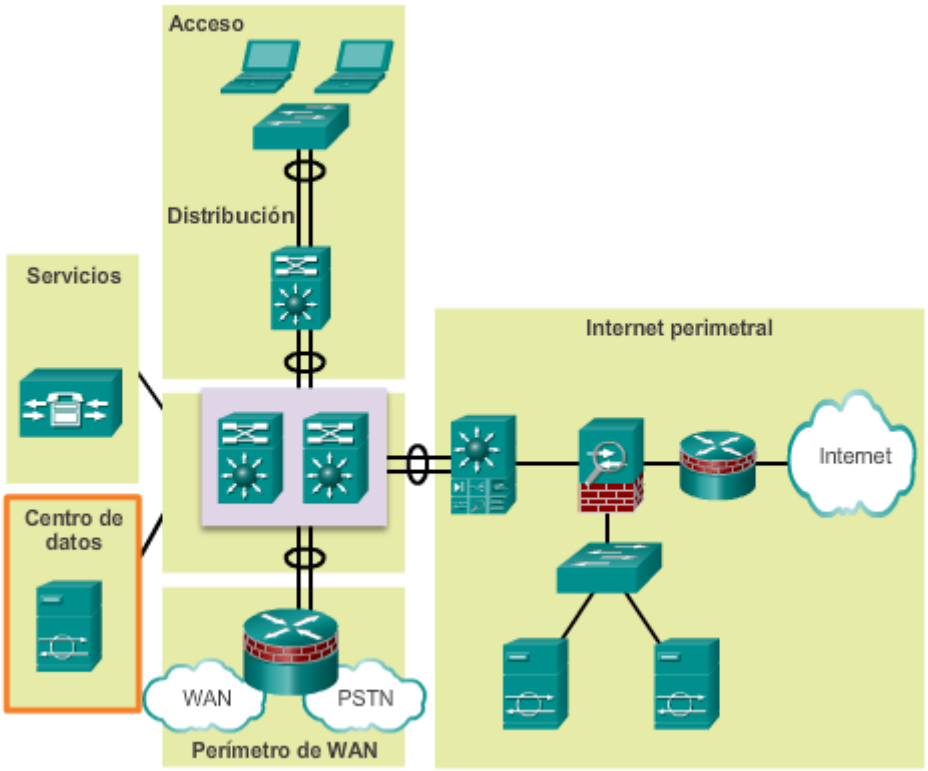
Módulo de acceso y distribución



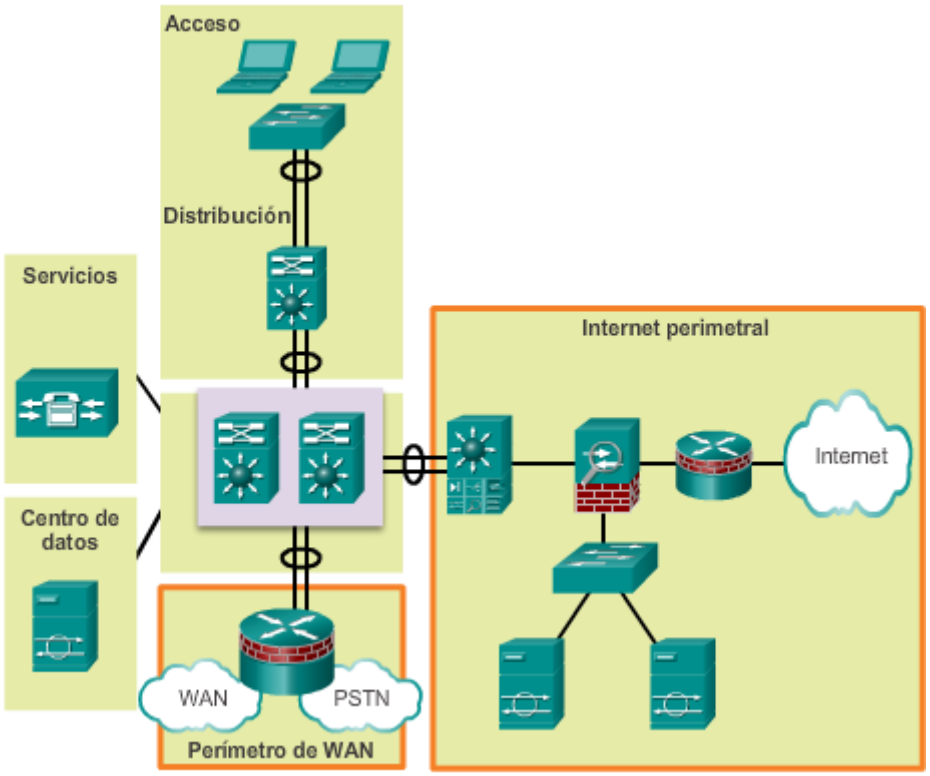
Módulo de servicios



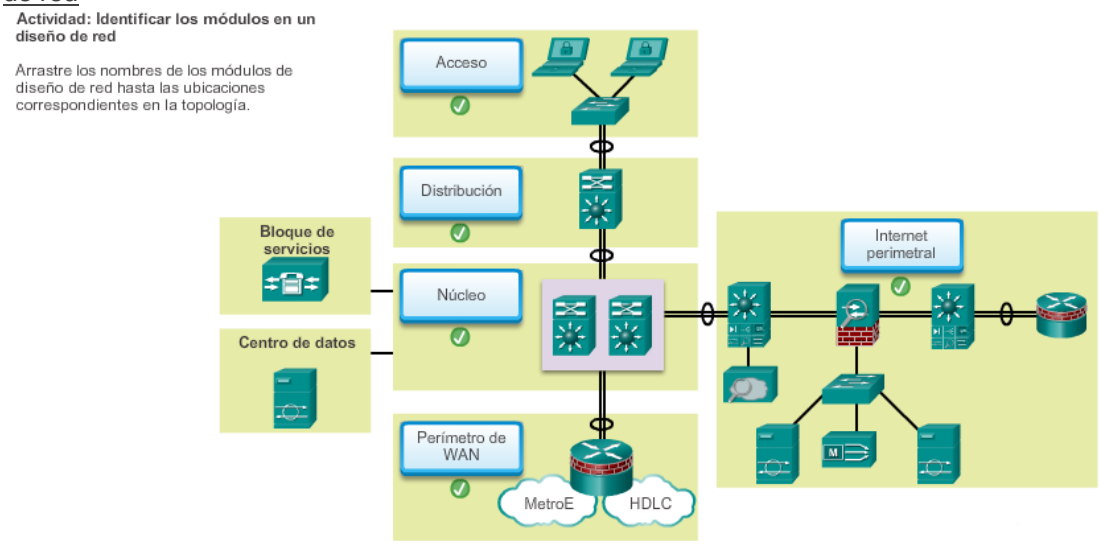
Centro de datos



Enterprise Edge



Capítulo 1: Diseño jerárquico de la red 1.2.1.3 Actividad: Identificar los módulos en un diseño de red



Capítulo 1: Diseño jerárquico de la red 1.2.2.1 Modelo de arquitectura empresarial de Cisco

Para satisfacer la necesidad de modularidad en el diseño de red, Cisco desarrolló el modelo de arquitectura empresarial de Cisco. Este modelo proporciona todos los beneficios del diseño de red jerárquico en la infraestructura del campus y facilita el diseño de redes más grandes y escalables.

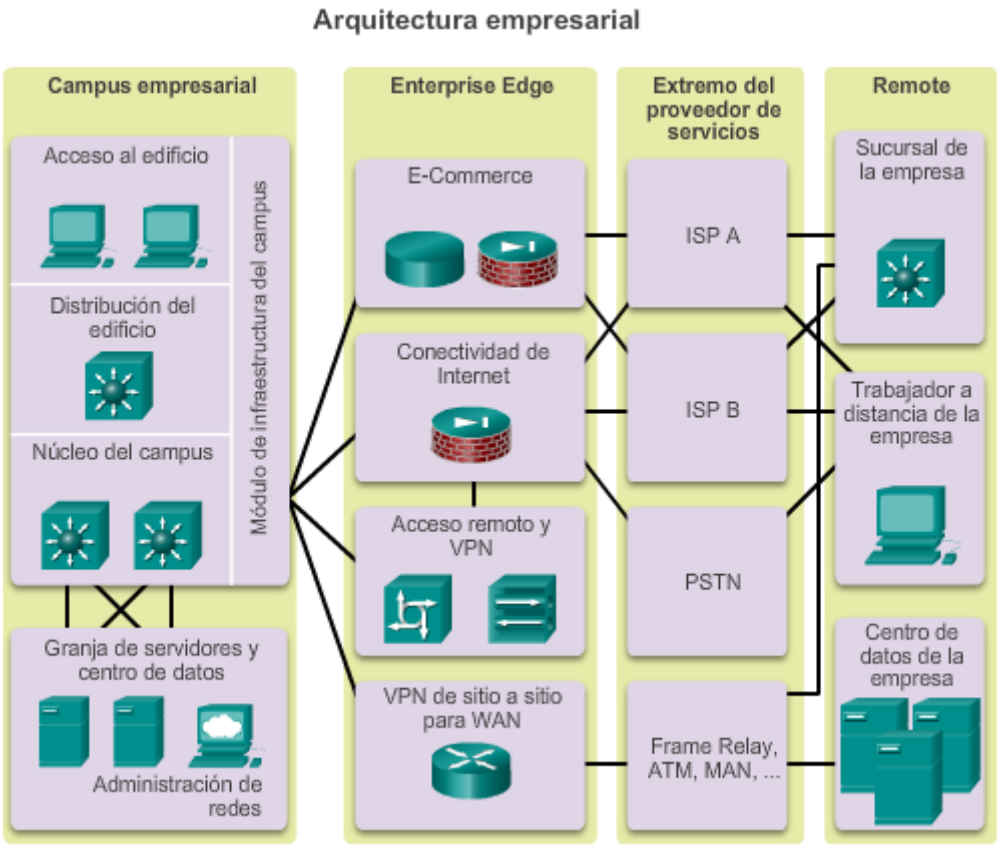
El modelo de arquitectura empresarial de Cisco separa la red empresarial en áreas funcionales que se conocen como “módulos”. La modularidad que se incorpora a la arquitectura permite que haya flexibilidad en el diseño de red y facilita su implementación y la resolución de problemas.

Como se muestra en la ilustración, los siguientes son los módulos principales de la arquitectura empresarial de Cisco:

- Campus empresarial
- Enterprise Edge
- Extremo del proveedor de servicios

Existen módulos adicionales conectados al perímetro del proveedor de servicios:

- Centro de datos de la empresa
- Sucursal de la empresa
- Trabajador a distancia de la empresa



Capítulo 1: Diseño jerárquico de la red 1.2.2.2 Campus empresarial de Cisco

Una red de campus es un edificio o un grupo de edificios conectados a una red empresarial que consta de muchas LAN. Por lo general, un campus se limita a un área geográfica fija, pero puede abarcar varios edificios vecinos, por ejemplo, un complejo industrial o el entorno de un parque industrial. Es posible que las oficinas regionales, las SOHO y los trabajadores móviles necesiten conectarse al campus central para obtener datos e información.

El módulo de campus empresarial describe los métodos recomendados para crear una red escalable, a la vez que aborda las necesidades de las operaciones comerciales del tipo de campus. La arquitectura es modular y se puede expandir fácilmente para incluir edificios o pisos de campus adicionales a medida que la empresa crece.

El módulo de campus empresarial consta de los siguientes submódulos:

- Acceso al edificio
- Distribución del edificio
- Núcleo del campus
- Centro de datos

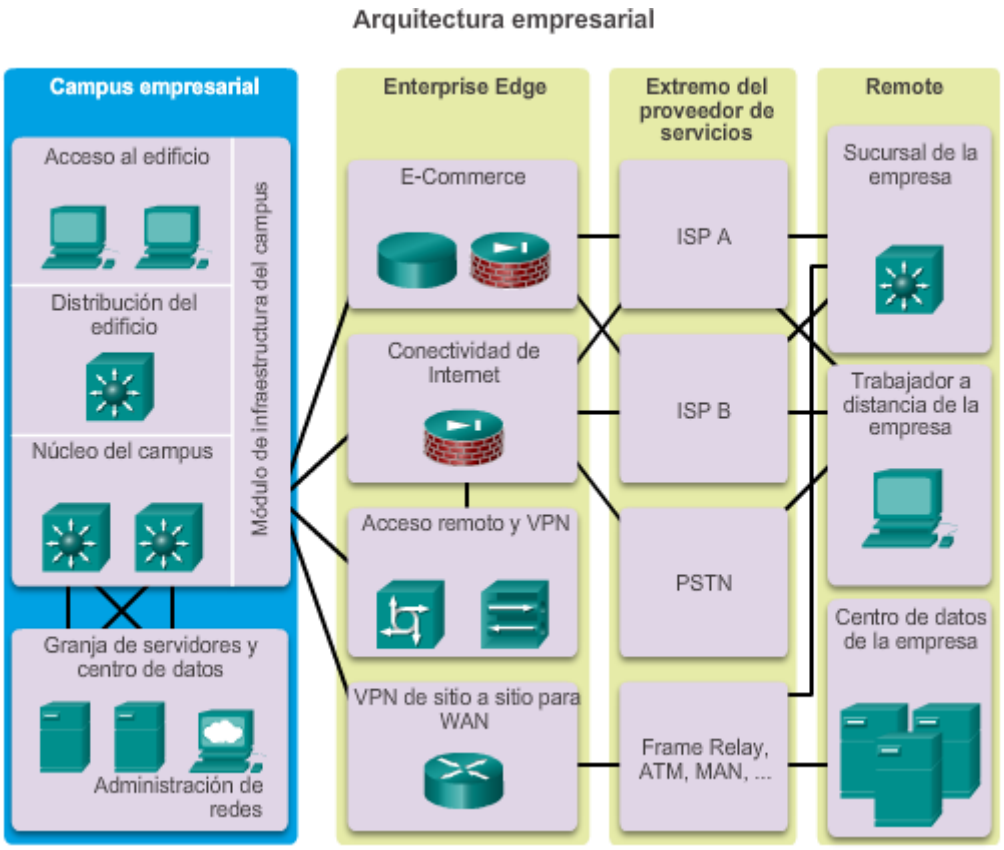
Juntos, estos submódulos realizan lo siguiente:

- Proporcionan una alta disponibilidad mediante un diseño de red jerárquico resistente.
- Integran las comunicaciones IP, la movilidad y la seguridad avanzada.
- Utilizan el tráfico de multidifusión y QoS para optimizar el tráfico de la red.
- Proporcionan una mayor seguridad y flexibilidad mediante la administración del acceso, las VLAN y las VPN con IPsec.

La arquitectura del módulo de campus empresarial proporciona a la empresa una alta disponibilidad a través de un diseño multicapa resistente, características de hardware y software redundante, y procedimientos automáticos para volver a configurar las rutas de la red cuando ocurren fallas. La seguridad integrada protege contra el impacto de gusanos, virus y otros ataques a la red, además de mitigarlo, incluso en el nivel del puerto del switch.

Un módulo de centro de datos centralizado de gran capacidad puede proporcionar recursos de servidores internos a los usuarios. Por lo general, el módulo de centro de datos también admite servicios de administración de red para la empresa, incluidos el control, el registro, la resolución de problemas y otras características comunes de administración de extremo a extremo. El submódulo de centro de datos normalmente contiene servidores de correo electrónico y corporativos internos que proporcionan servicios de aplicación, de archivo, de impresión, de correo electrónico y de sistema de nombres de dominios (DNS) a los usuarios internos.

Haga clic en el módulo de campus empresarial de la ilustración para obtener más información.



Capítulo 1: Diseño jerárquico de la red 1.2.2.3 Perímetro empresarial de Cisco

El módulo de perímetro empresarial proporciona conectividad para los servicios de voz, video y datos fuera de la empresa. A menudo, este módulo funciona como vínculo entre el módulo de campus empresarial y los otros módulos.

El módulo de perímetro empresarial consta de los siguientes submódulos:

- **Redes y servidores de comercio electrónico:** el submódulo de comercio electrónico permite que las empresas admitan aplicaciones de comercio electrónico a través de Internet. Utiliza los diseños de alta disponibilidad del módulo de centro de datos. Los dispositivos ubicados en el submódulo de comercio electrónico incluyen los servidores web, de aplicaciones y de bases de datos, el firewall y los routers de firewall, y los sistemas de prevención de intrusiones (IPS) en la red.

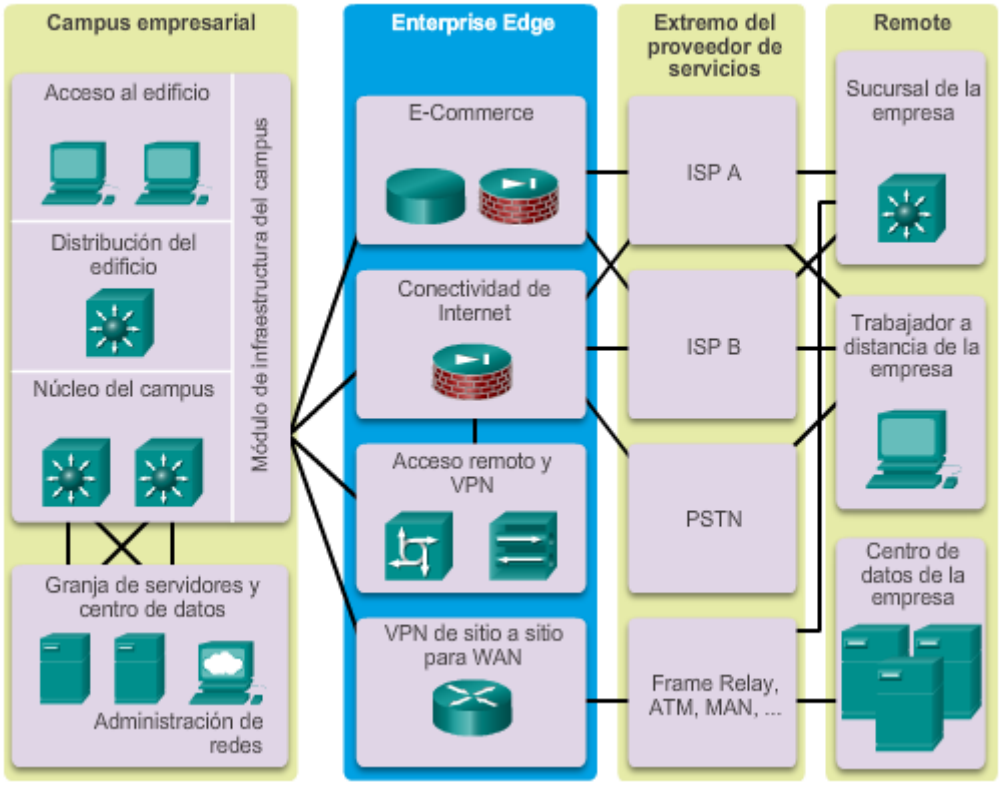
- **Conectividad a Internet y zona perimetral (DMZ):** el submódulo de Internet del perímetro empresarial proporciona a los usuarios internos una conectividad segura a los servicios de Internet, como los servidores públicos, el correo electrónico y DNS. También se proporciona la conectividad a uno o varios proveedores de servicios de Internet (ISP). Los componentes de este submódulo incluyen el firewall y los routers de firewall, los routers perimetrales de Internet, los servidores FTP y HTTP, los servidores de retransmisión de SMTP y los servidores DNS.

- **Acceso remoto y VPN:** el submódulo de acceso remoto y VPN del perímetro empresarial proporciona servicios de terminación de acceso remoto, incluida la autenticación para usuarios y sitios remotos. Los componentes de este submódulo incluyen los firewalls, los

concentradores de acceso telefónico, los dispositivos de seguridad adaptables (ASA) de Cisco y las aplicaciones de sistema de prevención de intrusiones (IPS) en la red.

- **WAN:** el submódulo WAN utiliza diversas tecnologías WAN para enrutar el tráfico entre los sitios remotos y el sitio central. Los enlaces de redes WAN empresariales incluyen tecnologías como la conmutación de etiquetas multiprotocolo (MPLS), Ethernet metropolitana, las líneas arrendadas, la red óptica síncrona (SONET) y la jerarquía digital síncrona (SDH), PPP, Frame Relay, ATM, el cable, la línea de suscriptor digital (DSL) y la tecnología inalámbrica.

Haga clic en el módulo de perímetro empresarial de la ilustración para obtener más información.



Capítulo 1: Diseño jerárquico de la red 1.2.2.4 Extremo del proveedor de servicios

Las empresas utilizan proveedores de servicios (SP) para enlazarse con otros sitios. Como se muestra en la figura 1, el módulo de perímetro del SP puede incluir lo siguiente:

- Proveedores de servicios de Internet (ISP)
- Servicios WAN, como Frame Relay, ATM y MAN
- Servicios de red pública de telefonía conmutada (PSTN)

El perímetro del SP proporciona conectividad entre el módulo de campus empresarial y los módulos remotos de centro de datos, de sucursales y de trabajadores a distancia de la empresa.

El módulo de perímetro del SP presenta las siguientes características:

- Abarca amplias áreas geográficas de manera rentable.
- Converge los servicios de voz, video y datos a través de una única red de comunicaciones IP.
- Admite QoS y acuerdos del nivel de servicio.
- Admite seguridad mediante VPN (IPsec y MPLS) a través de las WAN de capa 2 y capa 3.

Haga clic en el perímetro del proveedor de servicios en la figura 1 para obtener más información.

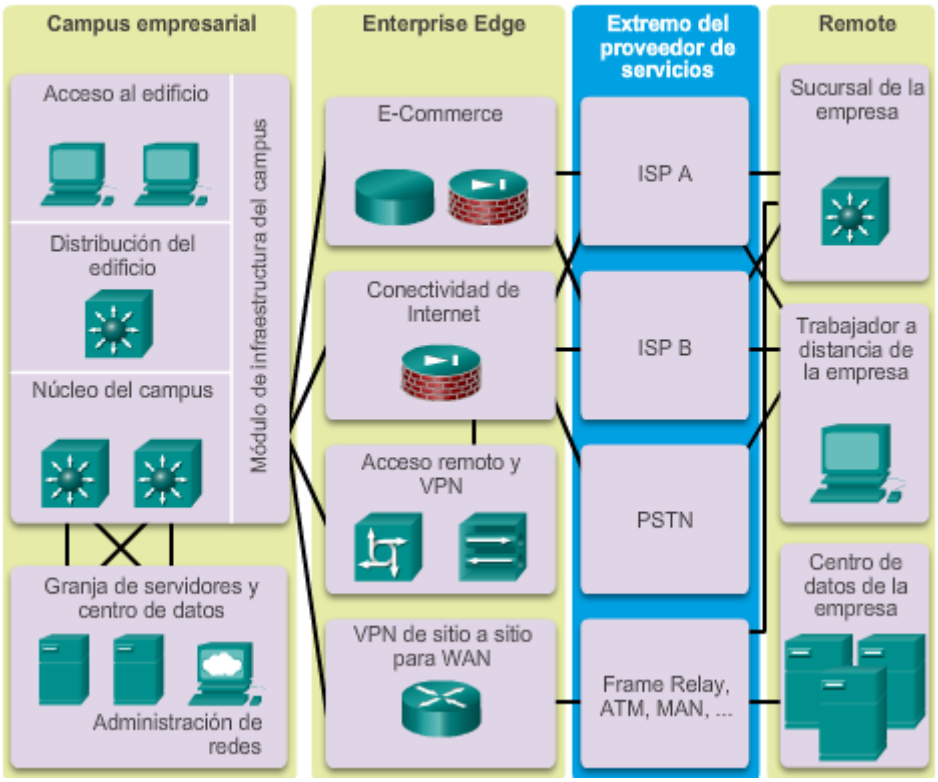
Al adquirir servicios de Internet de un ISP, se debe tener en cuenta la redundancia o la conmutación por falla. Como se muestra en la figura 2, las conexiones redundantes a un único ISP pueden incluir lo siguiente:

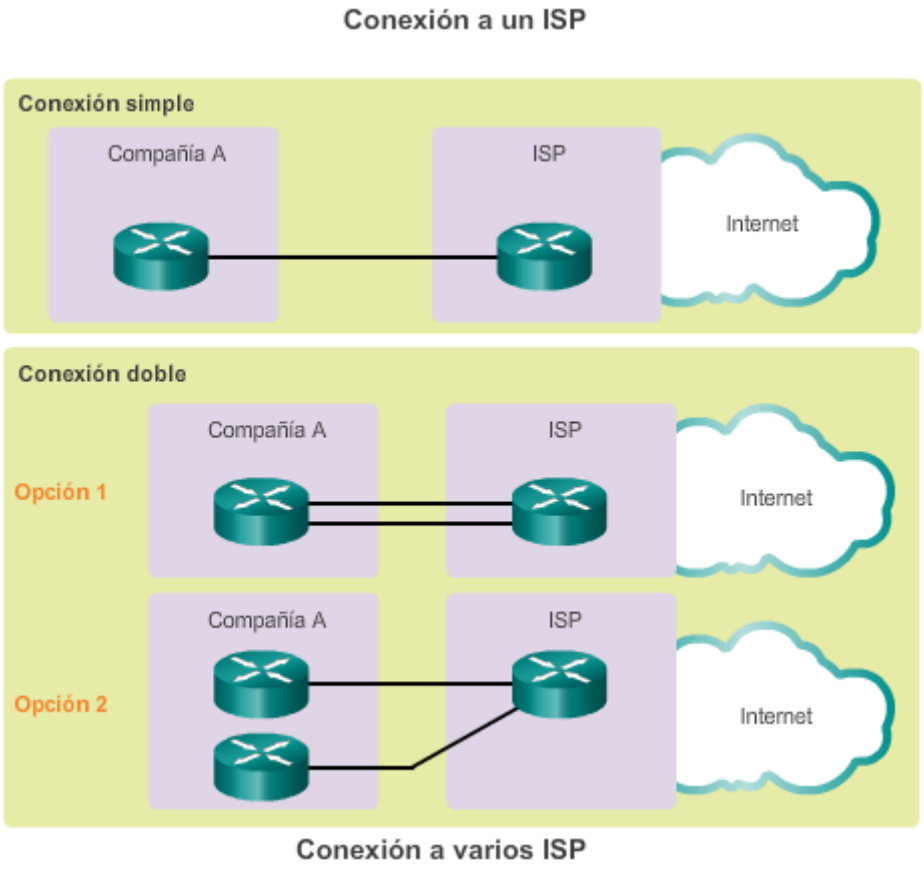
- **Conexión simple:** una única conexión a un ISP
- **Conexión doble:** dos o más conexiones a un único ISP

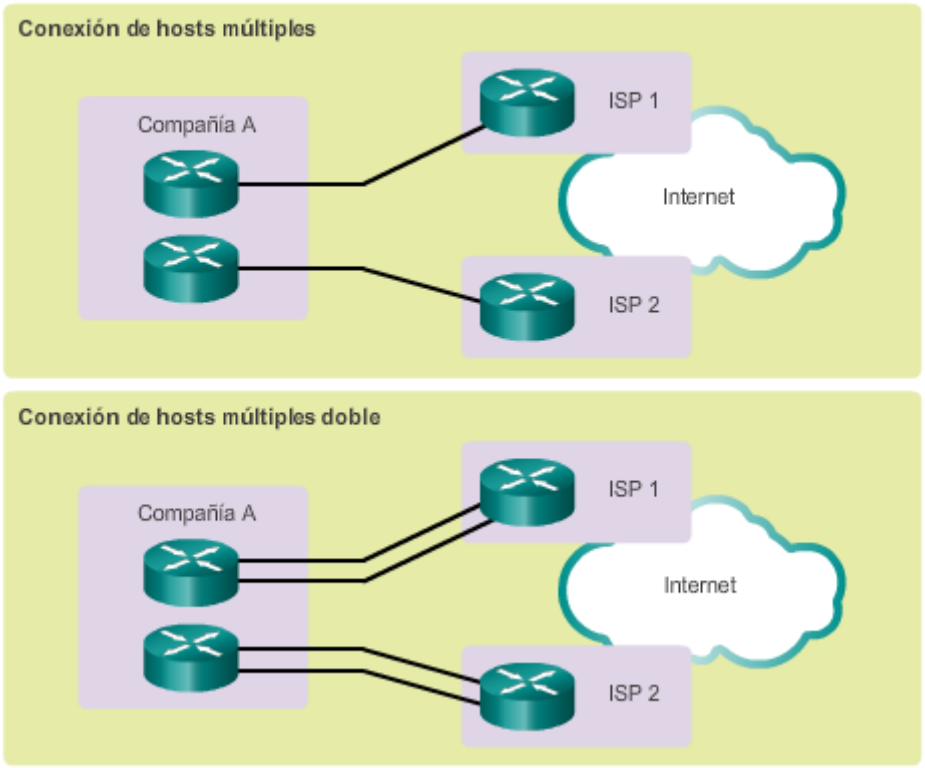
También se puede establecer la redundancia con varios ISP, como se muestra en la figura 3. Las opciones para conectarse a varios ISP incluyen lo siguiente:

- **Conexión de hosts múltiples:**conexiones a dos o más ISP
- **Conexión de hosts múltiples doble:**varias conexiones a dos o más ISP

Arquitectura empresarial







Capítulo 1: Diseño jerárquico de la red 1.2.2.5 Área funcional remota

El área funcional remota es responsable de las opciones de conectividad remota e incluye varios módulos:

Sucursal de la empresa

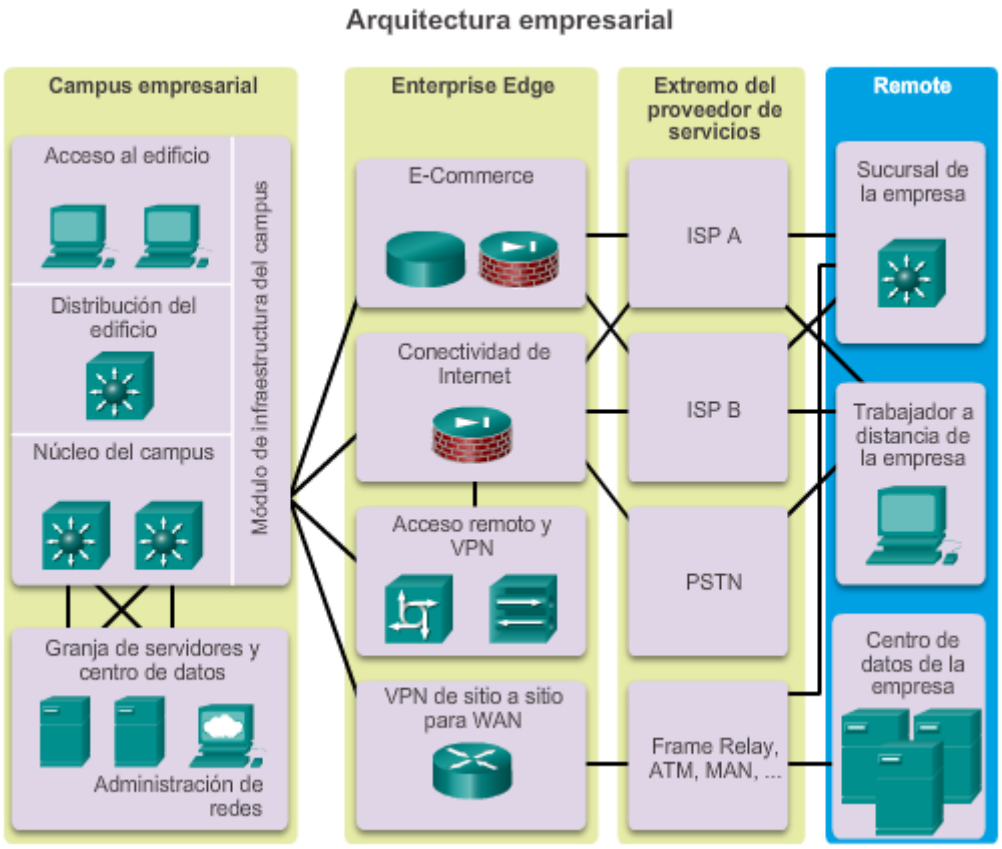
El módulo de sucursales de la empresa incluye las sucursales remotas que permiten que los empleados trabajen en ubicaciones fuera del campus. Por lo general, estas ubicaciones son las que proporcionan opciones de seguridad, telefonía y movilidad a los empleados, así como conectividad general a la red del campus y a los distintos componentes ubicados dentro del campus empresarial. El módulo de sucursales de la empresa permite que las empresas extiendan las aplicaciones y los servicios de la oficina central, como la seguridad, las Comunicaciones unificadas de Cisco y el rendimiento de las aplicaciones avanzadas, hasta las sucursales remotas. El dispositivo perimetral que conecta el sitio remoto al sitio central varía según las necesidades y el tamaño del sitio. Los sitios remotos grandes pueden utilizar switches Cisco Catalyst de tecnología avanzada, mientras que los sitios más pequeños pueden usar un router ISR G2. Estos sitios remotos dependen del perímetro del SP para proporcionar los servicios y las aplicaciones del sitio principal. En la ilustración, el módulo de sucursales de la empresa se conecta al campus empresarial principalmente mediante un enlace WAN; sin embargo, también cuenta con un enlace a Internet de respaldo. El enlace a Internet utiliza la tecnología VPN con IPsec de sitio a sitio para cifrar datos corporativos.

Trabajador a distancia de la empresa

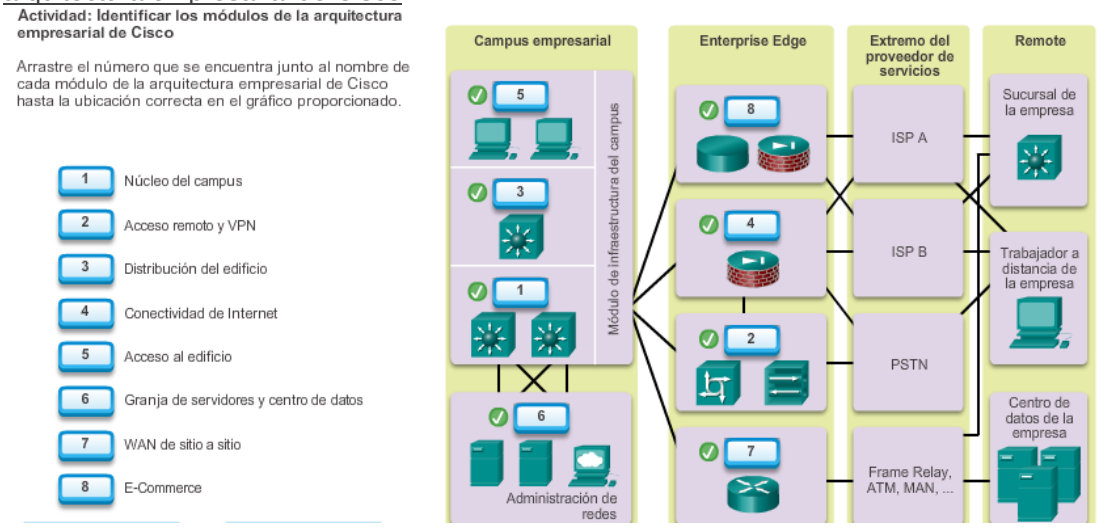
El módulo de trabajadores a distancia de la empresa se encarga de proporcionar conectividad a los empleados que trabajan desde diversas ubicaciones geográficamente dispersas, que incluyen las oficinas domésticas, los hoteles o los sitios de clientes. El módulo de trabajadores a distancia recomienda que los usuarios móviles se conecten a Internet mediante los servicios de un ISP local, como el cable módem o el módem DSL. Se pueden utilizar servicios de VPN para proteger las comunicaciones entre el trabajador móvil y el campus central. Los servicios de red de seguridad integrada y basados en identidad permiten que la empresa extienda las políticas de seguridad del campus al trabajador a distancia. El personal puede iniciar sesión en la red de manera segura a través de la VPN y acceder a las aplicaciones y los servicios autorizados desde una única plataforma rentable.

Centro de datos de la empresa

El módulo de centro de datos de la empresa es un centro de datos con las mismas opciones funcionales del centro de datos del campus, pero en una ubicación remota. Esto proporciona una capa de seguridad adicional, dado que el centro de datos externo puede proporcionar a la empresa servicios de recuperación tras un desastre y de continuidad empresarial. Los switches de tecnología avanzada, como los switches de la serie Cisco Nexus, utilizan servicios WAN rápidos como Ethernet metropolitana (MetroE) para conectar el campus empresarial al centro de datos de la empresa remoto. Los centros de datos redundantes proporcionan respaldo mediante la replicación síncrona y asíncrona de datos y aplicaciones. Además, la red y los dispositivos ofrecen balanceo de carga de servidores y aplicaciones para maximizar el rendimiento. Esta solución permite que la empresa escale sin que se produzcan cambios importantes en la infraestructura.



Capítulo 1: Diseño jerárquico de la red 1.2.2.6 Actividad: Identificar los módulos de la arquitectura empresarial de Cisco



Capítulo 1: Diseño jerárquico de la red 1.3.1.1 Desafíos de TI

Dado que las empresas se volvieron más dependientes de las redes para lograr el éxito, las arquitecturas de red evolucionaron con el correr de los años. Originalmente, los usuarios, los datos y las aplicaciones se alojaban en las instalaciones. Los usuarios solo podían acceder a

los recursos de red con computadoras que pertenecían a la empresa. La red tenía fronteras y requisitos de acceso claros. Mantener la seguridad, la productividad y los servicios era más sencillo. Hoy en día, la frontera de la red cambió, lo que presenta nuevos desafíos para los departamentos de TI. Las redes están pasando de ser un sistema de transporte únicamente de datos compuesto por dispositivos LAN conectados, a un sistema que permite conectar personas, dispositivos e información en un entorno de red convergente y con gran variedad de medios.

A medida que se lanzan al mercado nuevas tecnologías y dispositivos para usuarios finales, las empresas y los consumidores deben continuar adaptándose a este entorno en constante evolución. Existen muchas nuevas tendencias de red que continúan afectando a organizaciones y consumidores. Algunas de las tendencias principales incluyen las siguientes:

- Traiga su propio dispositivo (BYOD)
- Colaboración en línea
- Comunicación por video
- Computación en la nube

Si bien estas tendencias admiten más servicios avanzados que nunca, también presentan nuevos riesgos de seguridad que los profesionales de TI deben resolver.

Capítulo 1: Diseño jerárquico de la red 1.3.1.2 Arquitecturas empresariales emergentes

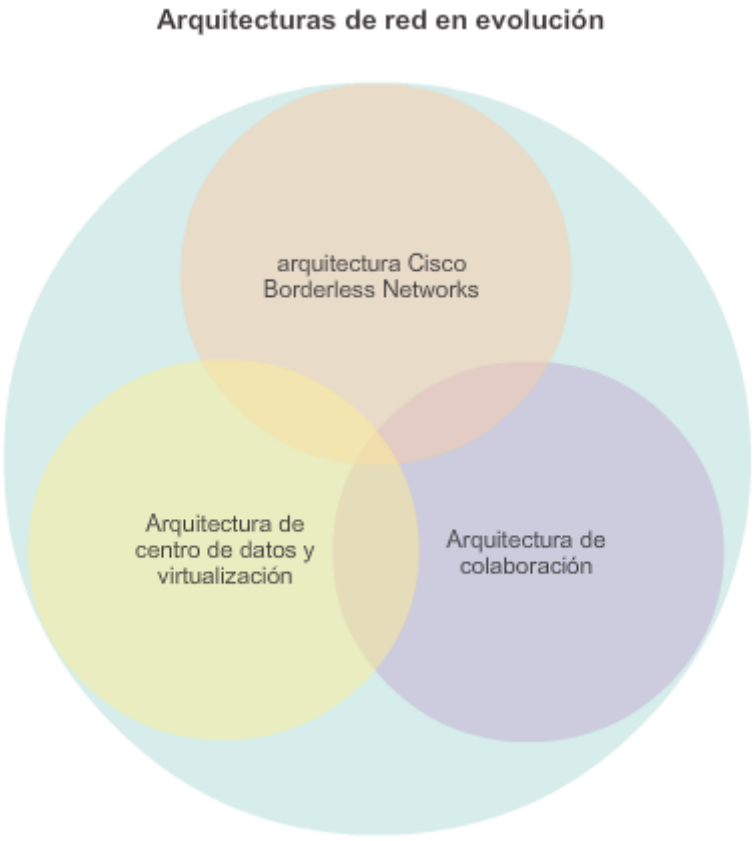
La velocidad con la que cambian los entornos de mercado y comerciales les exige a los profesionales de TI que sean más estratégicos que nunca. La evolución de los modelos empresariales genera desafíos tecnológicos complejos que los profesionales de TI deben resolver.

Para abordar estas tendencias de red emergentes, se necesitan nuevas arquitecturas de red empresariales. Estas arquitecturas deben cumplir con los principios de diseño de red establecidos en la arquitectura empresarial de Cisco, así como con las políticas y las tecnologías superpuestas que permiten que las organizaciones admitan tendencias emergentes de manera segura y fácil de administrar.

Para satisfacer esta necesidad, Cisco presentó las siguientes tres arquitecturas de red, las cuales se muestran en la ilustración:

- arquitectura Cisco Borderless Networks
- Arquitectura de colaboración
- Arquitectura de centro de datos y virtualización

Nota: las arquitecturas de red evolucionan constantemente. El objetivo de esta sección es proporcionar una introducción y una descripción general de las tendencias de arquitectura emergentes.



Capítulo 1: Diseño jerárquico de la red 1.3.2.1 Cisco Borderless Networks

La arquitectura Cisco Borderless Network es una solución de red que permite que las organizaciones y las personas se conecten de manera segura, con confianza y sin inconvenientes a la red empresarial en un entorno BYOD. Se basa en dispositivos conectados por cable, inalámbricos, de routing, de switching, de seguridad y de optimización de aplicaciones que funcionan en sintonía para ayudar a los profesionales de TI a equilibrar los exigentes desafíos comerciales y los modelos empresariales cambiantes.

No es una solución estática, sino una solución en evolución para ayudar a los profesionales de TI a desarrollar la infraestructura para proporcionar experiencias de usuario seguras, confiables y sin inconvenientes en un mundo lleno de fronteras nuevas y cambiantes.

Permite que el departamento de TI diseñe e implemente sus sistemas y políticas con eficacia en todos los dispositivos para usuarios finales que requieren conectarse a la red. Al hacerlo, proporciona un acceso seguro, confiable y sin inconvenientes a los recursos desde varios dispositivos y ubicaciones, así como a aplicaciones que pueden estar ubicadas en cualquier lugar.

Específicamente, la arquitectura Cisco Borderless Network ofrece dos conjuntos principales de servicios:

- **Servicios para terminales y usuarios sin fronteras:** como se muestra en la figura 1, los servicios para terminales y usuarios sin fronteras conectan los diversos dispositivos para proporcionar acceso a los servicios de red. Los dispositivos que se pueden conectar a la red sin fronteras van desde computadoras hasta tablet PC y smartphones. Elimina las

fronteras de ubicación y dispositivo, lo que proporciona un acceso unificado para los dispositivos conectados por cable e inalámbricos. Los servicios para terminales y usuarios definen la experiencia del usuario y permiten un rendimiento seguro, confiable y sin inconvenientes en una amplia variedad de dispositivos y entornos, como se muestra en la ilustración. Por ejemplo, la mayoría de los smartphones y las tablet PC pueden descargar y utilizar el software Cisco AnyConnect. Permite que el dispositivo establezca una conexión segura, continua y basada en políticas para lograr una experiencia de usuario sin inconvenientes.

- **Servicios de red sin fronteras:** como se muestra en la figura 2, los servicios de red sin fronteras unifican el enfoque para brindar aplicaciones de forma segura a los usuarios en un entorno de alta distribución. Conecta a los usuarios internos y remotos de manera segura y proporciona acceso a los recursos de red. El elemento fundamental para escalar el acceso seguro es una arquitectura basada en políticas que permita que los profesionales de TI implementen controles de acceso centralizados.

La arquitectura Borderless Network admite una red sumamente segura y de alto rendimiento a la que puede acceder una amplia variedad de dispositivos. Debe ser lo suficientemente flexible para que se pueda escalar y para que admita el crecimiento futuro en términos de la expansión empresarial, incluida la informática BYOD, móvil y en la nube, y debe poder admitir los crecientes requisitos de los servicios de voz y video en línea.

Servicios para terminales y usuarios sin fronteras
Los dispositivos se deben conectar de manera segura, confiable y sin inconvenientes =Cisco AnyConnect
Servicios de red sin fronteras
Seguridad: TrustSec
Movilidad: Motion
Rendimiento de las aplicaciones: App Velocity
Optimización de multimedia: Medianet
Administración de la energía: EnergyWise

Capítulo 1: Diseño jerárquico de la red 1.3.2.2 Arquitectura de colaboración

El trabajo en un entorno cooperativo contribuye al aumento de la productividad. Se utiliza la colaboración y otros tipos de groupware para reunir a las personas por distintos motivos: por ejemplo, para socializar, para trabajar juntos, para cooperar y contribuir a la producción de algo, y para innovar.

La arquitectura Cisco Collaboration ofrece una cartera de productos, aplicaciones, kits de desarrollo de software (SDK) y API. Los componentes individuales trabajan juntos para proporcionar una solución integral.

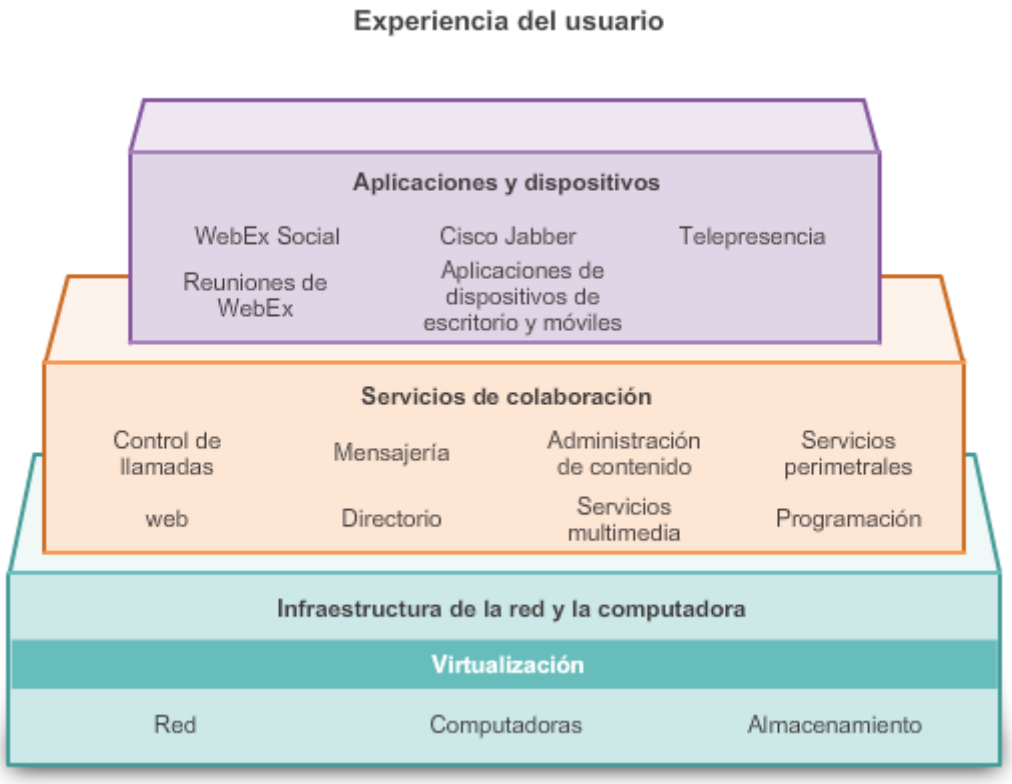
Como se muestra en la ilustración, la arquitectura de colaboración de Cisco consta de tres capas:

- **Aplicaciones y dispositivos:** esta capa contiene aplicaciones de comunicaciones unificadas y de conferencia, como Cisco WebEx Meetings, WebEx Social, Cisco Jabber y TelePresence. Las aplicaciones dentro de esta capa ayudan a que los usuarios

permanezcan conectados y mantengan la productividad. Estas aplicaciones incluyen servicios de voz, video, conferencias web, mensajería, aplicaciones móviles y software social para empresas.

- **Servicios de colaboración:** esta capa admite aplicaciones de colaboración, incluidos los servicios de presencia, ubicación, administración de sesión, administración de contactos, marcos de clientes, etiquetado y administración de políticas y seguridad.

- **Infraestructura de la red y la computadora:** esta capa permite la colaboración en cualquier momento, desde cualquier lugar, en cualquier dispositivo. Incluye máquinas virtuales, la red y el almacenamiento.



Capítulo 1: Diseño jerárquico de la red 1.3.2.3 Centro de datos y virtualización

La arquitectura de centro de datos y virtualización de Cisco se construye sobre la base de Cisco Data Center 3.0. Consta de un conjunto integral de tecnologías y servicios de virtualización que une las plataformas de red, de informática, de almacenamiento y de virtualización.

La arquitectura del centro de datos consta de tres componentes, como se muestra en la figura 1:

- **Cisco Unified Management Solutions:** las soluciones de administración simplifican y automatizan el proceso de implementación de la infraestructura y los servicios de TI con rapidez y confiabilidad empresarial. Las soluciones operan con transparencia a través de recursos físicos y virtuales en entornos de la nube.

- **Unified Fabric Solutions:** las soluciones de red flexibles prestan servicios de red a los servidores, el almacenamiento y las aplicaciones, lo que proporciona una convergencia transparente, escalabilidad e inteligencia sofisticada. Estas soluciones incluyen los switches Cisco Nexus, los switches Catalyst, Cisco Fabric Manager y el software NX-OS de Cisco.

- **Unified Computing Solutions:** el sistema de última generación del centro de datos de Cisco reúne la computación, la red, el acceso al almacenamiento y la virtualización en un sistema cohesivo diseñado para reducir el costo total de propiedad (TCO) y aumentar la agilidad comercial. El sistema Cisco Unified Computing System (Cisco UCS) está diseñado con servidores de blade, servidores montados en un rack, interconexiones de estructura y tarjetas de interfaz virtuales (VIC).

Haga clic en Reproducir en la figura 2 para ver un breve video sobre Cisco Unified Fabric.

Capítulo 1: Diseño jerárquico de la red 1.3.2.4 Expansión de la red

Estas tres arquitecturas se basan en una infraestructura de hardware y software escalable y resistente. Los componentes de la arquitectura se agrupan para formar sistemas de red que abarcan una organización desde el acceso de red hasta la nube y proporcionan a las organizaciones los servicios que necesitan.

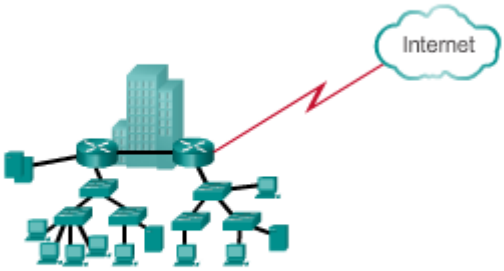
Al construir la infraestructura de red básica, las organizaciones pueden utilizar estas arquitecturas de red para ampliar la red con el tiempo mediante el agregado de características y funcionalidades a una solución integrada.

Uno de los primeros pasos para ampliar la red es expandirla de la infraestructura de campus a una red que conecte sitios remotos a través de Internet y de la WAN.

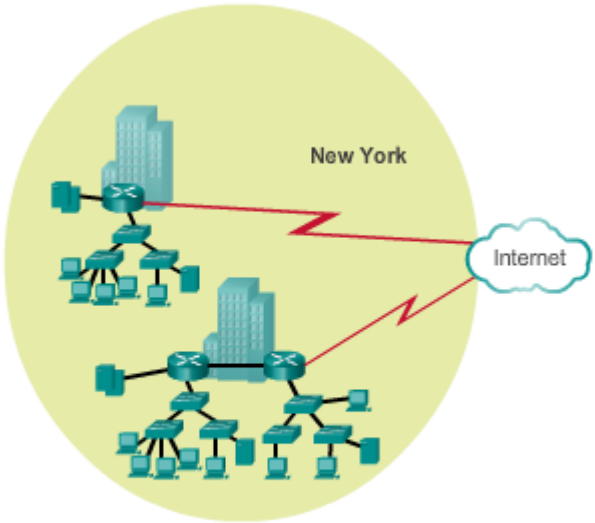
Haga clic en Reproducir en la ilustración para ver la evolución de una red a una infraestructura

Una empresa pequeña con una única ubicación.

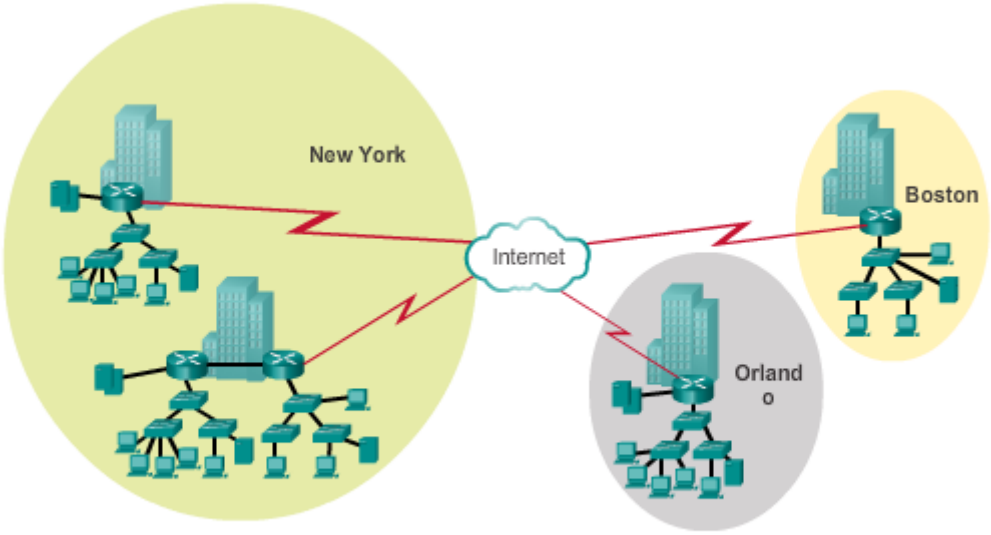
WAN.



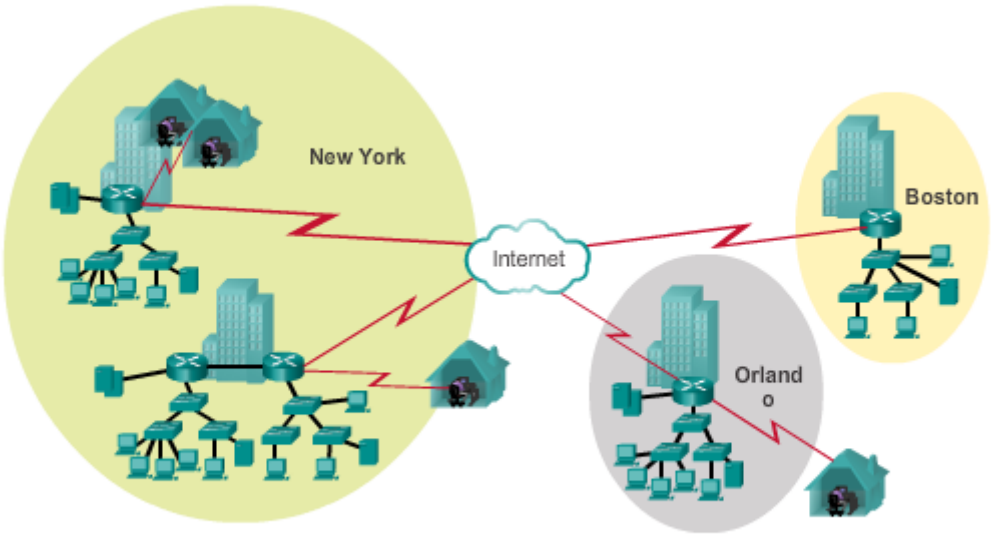
La empresa aumenta su cantidad de empleados.



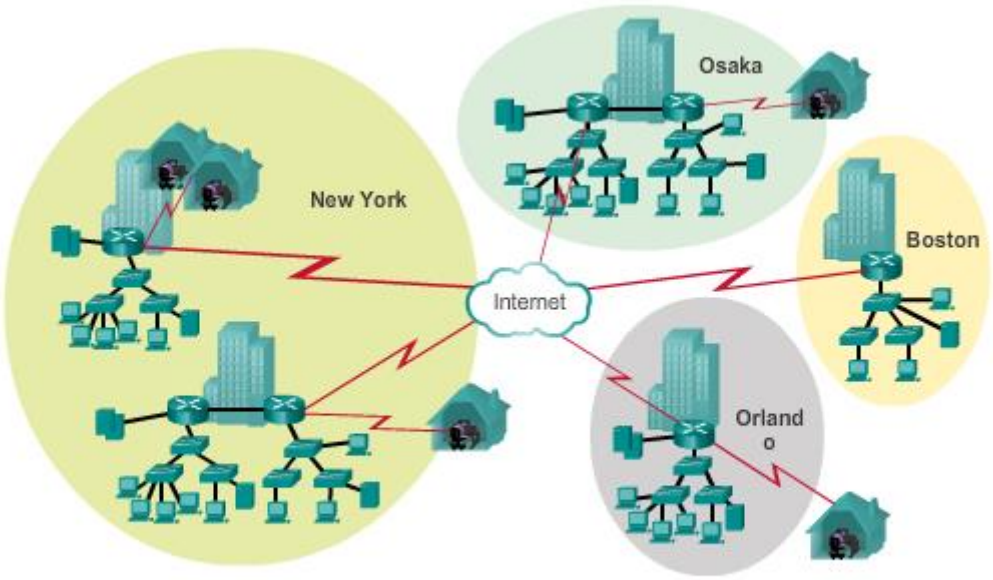
La empresa crece y crea varias sucursales en la misma ciudad.



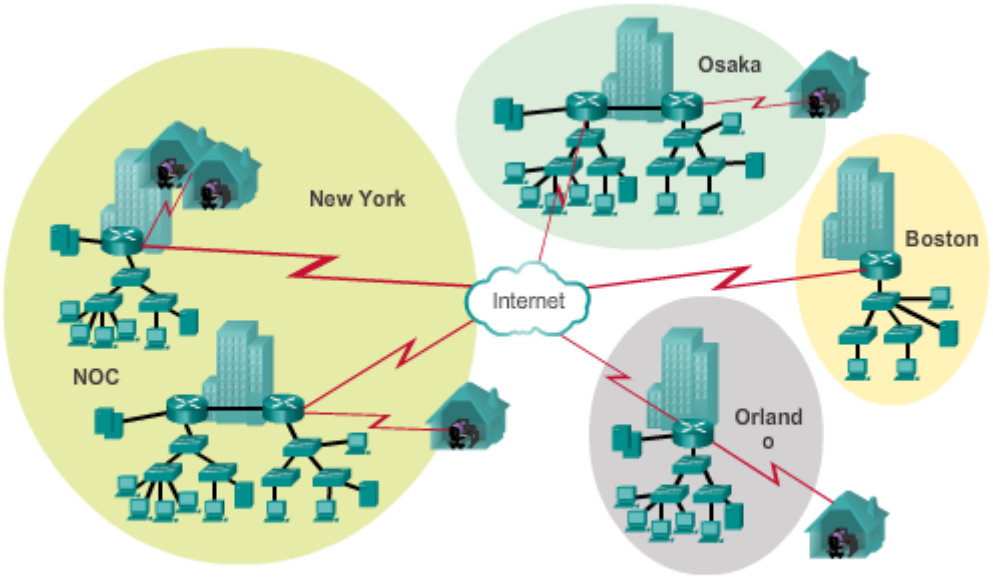
La empresa crece y se expande a varias ciudades.



La empresa contrata empleados a distancia.



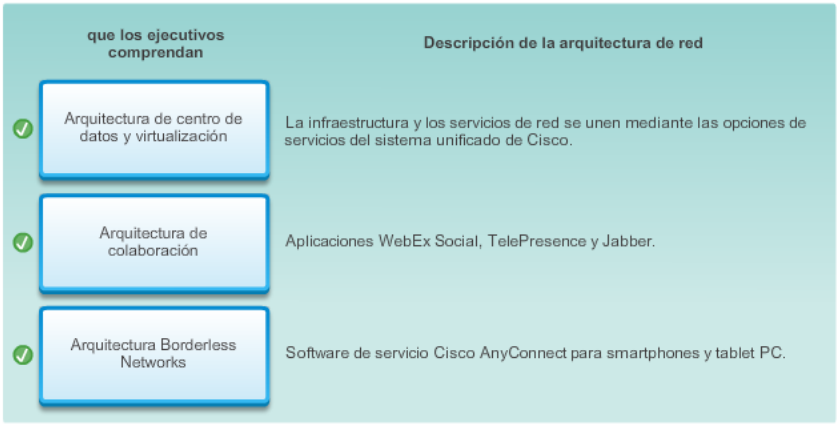
La empresa se expande a otros países.
Nota: no todas las redes empresariales son internacionales.



La empresa centraliza la administración de la red en un centro de operaciones de red (NOC, Network Operations Center).

Capítulo 1: Diseño jerárquico de la red 1.3.2.5 Actividad: Identificar la terminología de las arquitecturas de red en evolución

Actividad: Identificar la terminología de las arquitecturas de red en evolución
Arrastre los términos hasta las descripciones en la tabla.



Capítulo 1: Diseño jerárquico de la red 1.4.1.1 Actividad de clase: Innovaciones sin fronteras, en todas partes

Innovaciones sin fronteras: en todas partes

Usted es el administrador de red de su pequeña o mediana empresa. Se interesa por los servicios de red sin fronteras mientras hace planes para el futuro de la red.

Mientras planifica las políticas y los servicios de red, se da cuenta de que las redes cableadas e inalámbricas requieren capacidad de administración y un diseño de implementación.

Por consiguiente, esto lo lleva a considerar los siguientes servicios sin fronteras de Cisco como opciones posibles para su empresa:

- Seguridad: ***TrustSec***
- Movilidad: ***Motion***
- Rendimiento de las aplicaciones: ***App Velocity***
- Rendimiento multimedia: ***Medianet***
- Administración de la energía:***EnergyWise***

Actividad de clase: Innovaciones sin fronteras, en todas partes

Capítulo 1: Diseño jerárquico de la red 1.4.1.2 Packet Tracer: Desafío de integración de habilidades sobre OSPF

Esta actividad de Packet Tracer proporciona una oportunidad para revisar las habilidades obtenidas en trabajos de cursos anteriores.

Información básica/situación

Su empresa se acaba de expandir a otra ciudad y necesita ampliar su presencia a través de Internet. Su tarea consiste en llevar a cabo las actualizaciones de la red empresarial, que incluye redes dual-stack IPv4 e IPv6, así como una variedad de tecnologías de direccionamiento y routing.

Packet Tracer: Desafío de integración de habilidades sobre OSPF (instrucciones)

Packet Tracer: Desafío de integración de habilidades sobre OSPF (PKA)

Capítulo 1: Diseño jerárquico de la red 1.4.1.3 Packet Tracer: Desafío de integración de habilidades sobre EIGRP

Esta actividad de Packet Tracer proporciona una oportunidad para revisar las habilidades obtenidas en trabajos de cursos anteriores.

Información básica/situación

Usted es el nuevo técnico de red de una empresa que perdió a su técnico anterior en medio del proceso de actualización del sistema. Su tarea es completar las actualizaciones de la infraestructura de red que tiene dos ubicaciones. La mitad de la red empresarial utiliza direccionamiento IPv4 y la otra mitad utiliza direccionamiento IPv6. Además, los requisitos incluyen una variedad de tecnologías de routing y switching.

Packet Tracer: Desafío de integración de habilidades sobre EIGRP (instrucciones)

Packet Tracer: Desafío de integración de habilidades sobre EIGRP (PKA)

Capítulo 1: Diseño jerárquico de la red 1.4.1.4 Resumen

Los principios de ingeniería estructurada de un buen diseño de red incluyen jerarquía, modularidad, resistencia y flexibilidad.

Un diseño típico de red LAN jerárquica de campus empresarial incluye la capa de acceso, la capa de distribución y la capa de núcleo. En las redes empresariales más pequeñas, puede ser más práctica una jerarquía de “núcleo contraído”, en la que las funciones de capa de distribución y de capa de núcleo se implementan en un único dispositivo. Los beneficios de una

red jerárquica incluyen la escalabilidad, la redundancia, el rendimiento y la capacidad de mantenimiento.

Un diseño modular que separa las funciones de una red brinda flexibilidad y facilita la implementación y la administración. Los bloques de módulos básicos que conecta el núcleo incluyen el bloque de acceso y distribución, el de servicios, el de centro de datos y el de perímetro empresarial. Los módulos de la arquitectura empresarial de Cisco se utilizan para facilitar el diseño de redes grandes y escalables. Entre los módulos principales se incluye el de campus empresarial, el de perímetro empresarial, el de perímetro del proveedor de servicios, el de centro de datos, el de sucursales y el de trabajadores a distancia de la empresa.**Capítulo 2: Conexión a la WAN 2.0.1.1 Introducción**

Las empresas deben conectar redes LAN para proporcionar comunicación entre ellas, incluso cuando estas LAN están muy separadas entre sí. Las redes de área extensa (WAN) se usan para conectar LAN remotas. Una WAN puede proporcionar cobertura a una ciudad, un país o una región global. Las WAN son de propiedad de un proveedor de servicios, y las empresas pagan una tarifa para usar los servicios de red WAN del proveedor.

Para las WAN, se usan tecnologías diferentes que para las LAN. En este capítulo, se presentan los estándares, las tecnologías y los propósitos de WAN y se abarca la elección de las tecnologías, los servicios y los dispositivos WAN apropiados para satisfacer los requisitos comerciales cambiantes de una empresa en crecimiento.

Después de completar este capítulo, podrá hacer lo siguiente:

- Describir el propósito de una WAN.
- Describir las operaciones de WAN.
- Describir los servicios WAN disponibles.
- Comparar las diferentes tecnologías WAN privadas.
- Comparar las diferentes tecnologías WAN públicas.
- Seleccionar el protocolo y el servicio WAN adecuados para requisitos de red específicos.

Capítulo 2: Conexión a la WAN 2.0.1.2 Actividad de clase: Sucursales

Ramificaciones

Su empresa mediana abre una nueva sucursal para prestar servicios a una red basada en el cliente más amplia. Esta sucursal se centra en operaciones de red cotidianas comunes, pero también proporcionará TelePresence, conferencias web, telefonía IP, video a petición y servicios inalámbricos.

Aunque sabe que un ISP puede proporcionar los routers y switches WAN para admitir la conectividad a la red para la sucursal, prefiere utilizar su propio equipo local del cliente (CPE). Para garantizar la interoperabilidad, se utilizaron dispositivos de Cisco en las demás WAN de sucursales.

Como administrador de red de la sucursal, tiene la responsabilidad de investigar los posibles dispositivos de red que se pueden comprar y utilizar para la WAN.

Actividad de clase: Sucursales

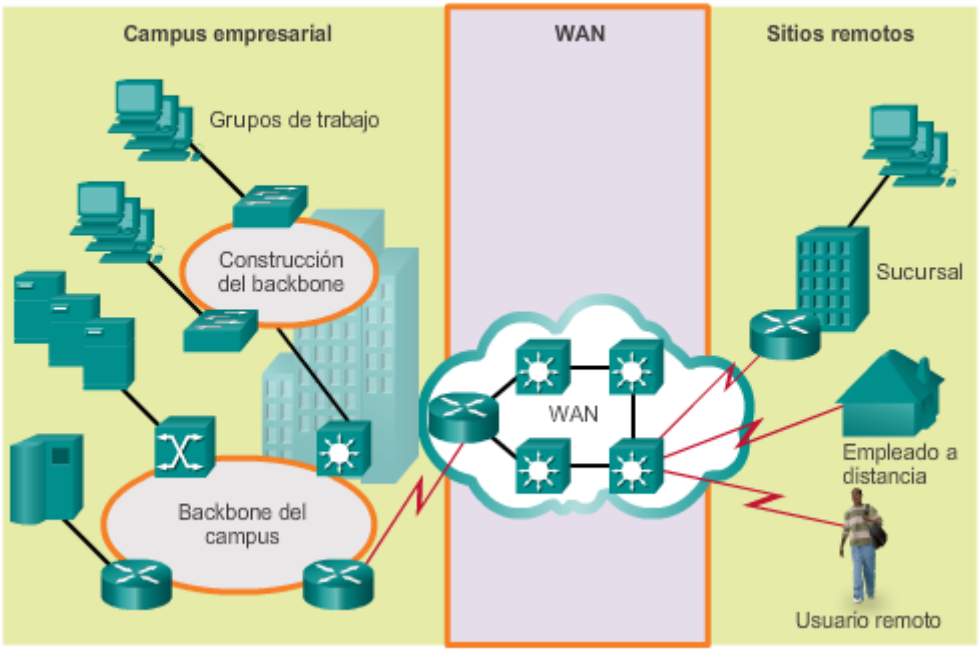
Capítulo 2: Conexión a la WAN 2.1.1.1 ¿Por qué una WAN?

Las WAN funcionan más allá del ámbito geográfico de una LAN. Como se muestra en la ilustración, las WAN se usan para interconectar la LAN de la empresa a las LAN remotas en las sucursales y las ubicaciones de los empleados a distancia.

Una WAN es de propiedad de un proveedor de servicios. Para conectarse a sitios remotos, una organización debe pagar una tarifa para usar los servicios de red del proveedor. Los proveedores de servicios WAN incluyen empresas prestadoras de servicios, como una red telefónica, una empresa de cable o un servicio satelital. Los proveedores de servicios proporcionan enlaces para interconectar los sitios remotos, con el fin de transportar datos, voz y video.

En cambio, las LAN normalmente son de propiedad de la organización y se utilizan para conectar computadoras, periféricos y otros dispositivos locales en un único edificio u otra área geográfica pequeña.

Las WAN interconectan usuarios y redes LAN



Capítulo 2: Conexión a la WAN 2.1.1.2 ¿Son necesarias las WAN?

Sin las WAN, las LAN serían una serie de redes aisladas. Las LAN proporcionan velocidad y rentabilidad para la transmisión de datos en áreas geográficas relativamente pequeñas. Sin embargo, a medida que las organizaciones se expanden, las empresas requieren capacidad de comunicación entre sitios geográficamente separados. Los siguientes son algunos ejemplos:

- Las oficinas regionales o las sucursales de una organización necesitan poder comunicarse y compartir datos con el sitio central.

- Las organizaciones necesitan compartir información con las organizaciones de los clientes. Por ejemplo, los fabricantes de software comunican regularmente información de

producto y promocional a los distribuidores que venden los productos a los usuarios finales.

- Los empleados que viajan por negocios de la empresa con frecuencia necesitan acceder a información ubicada en las redes empresariales.

Los usuarios de computadoras domésticas también necesitan enviar y recibir datos a través de distancias cada vez más grandes. Estos son algunos ejemplos:

- En la actualidad, los consumidores se comunican normalmente con los bancos, las tiendas y una variedad de proveedores de bienes y servicios a través de Internet.

- Para investigar para sus clases, los estudiantes acceden a índices de bibliotecas y publicaciones ubicados en otras partes del país y del mundo.

No se pueden conectar computadoras a través de un país, o del mundo, con cables físicos. Por lo tanto, las distintas tecnologías evolucionaron para admitir este requisito de comunicación. Internet se usa cada vez más como una alternativa económica a las WAN empresariales. Existen nuevas tecnologías disponibles para las empresas, que tienen el fin de proporcionar seguridad y privacidad a las comunicaciones y transacciones a través de Internet. Las WAN, ya sea que se usen solas o en conjunto con Internet, permiten que las organizaciones y las personas cubran sus necesidades de comunicación en un área extensa.

Capítulo 2: Conexión a la WAN 2.1.1.3 Evolución de las redes

Cada empresa es única, y la manera en que una organización crece depende de varios factores. Estos factores incluyen el tipo de productos o servicios que vende la empresa, la filosofía de administración de los propietarios y el clima económico del país en el que opera la empresa.

En tiempos de economía lenta, muchas empresas se centran en aumentar su rentabilidad por medio de mejorar la eficacia de las operaciones existentes, aumentar la productividad de los empleados y reducir los costos operativos. Establecer y administrar redes puede representar gastos de instalación y funcionamiento significativos. Para justificar un gasto tan grande, las empresas esperan que las redes funcionen en forma óptima y puedan ofrecer una variedad cada vez mayor de servicios y aplicaciones que respalden la productividad y la rentabilidad.

El ejemplo usado en este capítulo es el de una empresa ficticia llamada SPAN Ingeniería. Observe cómo cambian los requisitos de red a medida que esta pequeña empresa local se convierte en una empresa global.

Capítulo 2: Conexión a la WAN 2.1.1.4 Oficina pequeña

SPAN Ingeniería, una empresa de consultoría ambiental, desarrolló un proceso especial para convertir los residuos domésticos en electricidad y trabaja en un pequeño proyecto piloto para el gobierno municipal en su área local. La empresa, que opera desde hace cuatro años, creció y cuenta con 15 empleados: seis ingenieros, cuatro diseñadores de dibujo asistido por computadora (CAD), una recepcionista, dos socios ejecutivos y dos asistentes administrativos.

La administración de SPAN Ingeniería está trabajando para obtener contratos a gran escala una vez que el proyecto piloto demuestre de manera satisfactoria la viabilidad del proceso. Hasta entonces, la empresa debe administrar los costos cuidadosamente.

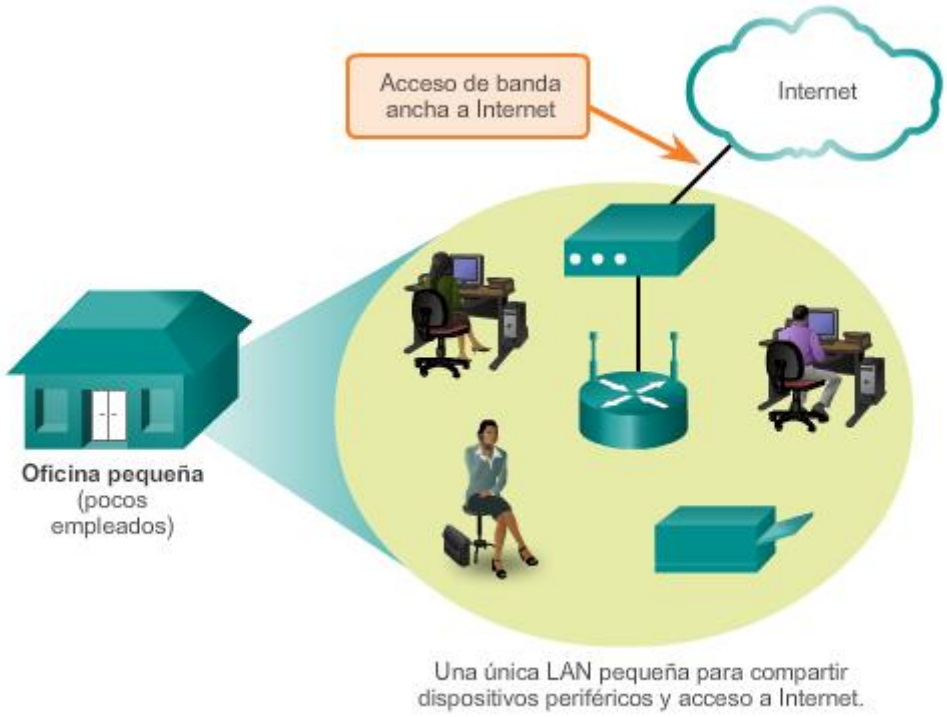
Para su pequeña oficina, SPAN Ingeniería usa una única LAN para compartir la información entre las computadoras y para compartir los periféricos, como una impresora, un trazador de gran escala (para imprimir planos de ingeniería) y máquinas de fax. Recientemente, se actualizó la LAN para que proporcione un servicio económico de voz sobre IP (VoIP), a fin de ahorrar en los costos de líneas telefónicas separadas para los empleados.

La conexión a Internet se realiza a través de un servicio de banda ancha común denominado DSL, que suministra el proveedor de servicios de telefonía local. Con tan pocos empleados, el ancho de banda no es un problema significativo.

La empresa no puede costear personal interno de soporte de TI, por lo que usa los servicios de soporte del proveedor de DSL. La empresa también usa un servicio de alojamiento web, en lugar de comprar y operar sus propios servidores FTP y de correo electrónico.

En la ilustración, se muestra un ejemplo de una oficina pequeña y su red.

Conexión de una oficina pequeña



Capítulo 2: Conexión a la WAN 2.1.1.5 Red de campus

En el transcurso de cinco años, SPAN Ingeniería crece rápidamente. Poco después de la implementación satisfactoria de la primera planta piloto, se contrató a la empresa para que diseñara e implementara una instalación de conversión de residuos a gran escala. Desde entonces, SPAN consiguió otros proyectos en las municipalidades vecinas y en otras partes del país.

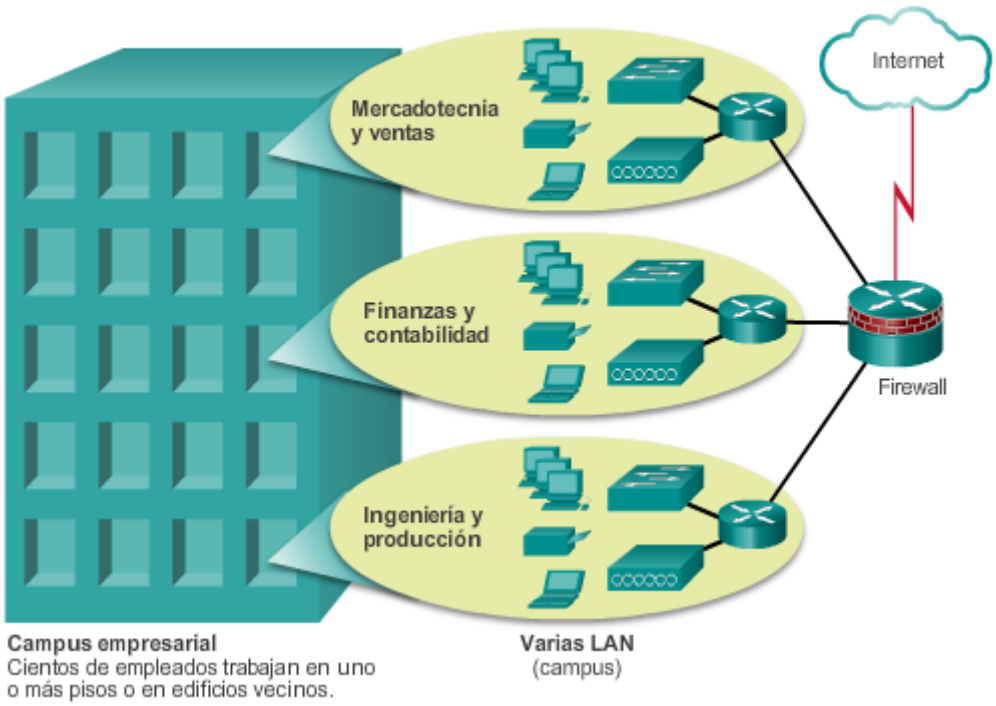
Para manejar la carga de trabajo adicional, la empresa contrató más personal y alquiló más espacio de oficina. Ahora es una pequeña a mediana empresa con varios cientos de empleados. Se desarrollan varios proyectos al mismo tiempo, y cada uno requiere un gerente de proyecto y personal de soporte. La empresa está organizada en departamentos funcionales, y cada departamento tiene su propio equipo organizativo. Para satisfacer las necesidades cada vez mayores, la empresa se mudó a varios pisos de un edificio de oficinas más grande.

A medida que la empresa se expandió, la red también creció. En lugar de una única LAN pequeña, la red ahora consta de diversas subredes, cada una destinada a un departamento diferente. Por ejemplo, todo el personal de ingeniería está en una LAN, mientras que el personal de marketing está en otra LAN diferente. Estas diversas LAN se unen para crear una red empresarial, o campus, que abarca varios pisos del edificio.

Ahora, la empresa cuenta con personal interno de TI para dar soporte y mantenimiento a la red. La red incluye servidores dedicados para correo electrónico, transferencia de datos y almacenamiento de archivos, así como aplicaciones y herramientas de productividad basadas en Web. Además, la empresa tiene una intranet para proporcionar documentos e información internos a los empleados, mientras que una extranet proporciona información de proyectos a los clientes designados.

En la ilustración, se muestra un ejemplo de la red de campus de SPAN.

Conexión de una red de campus



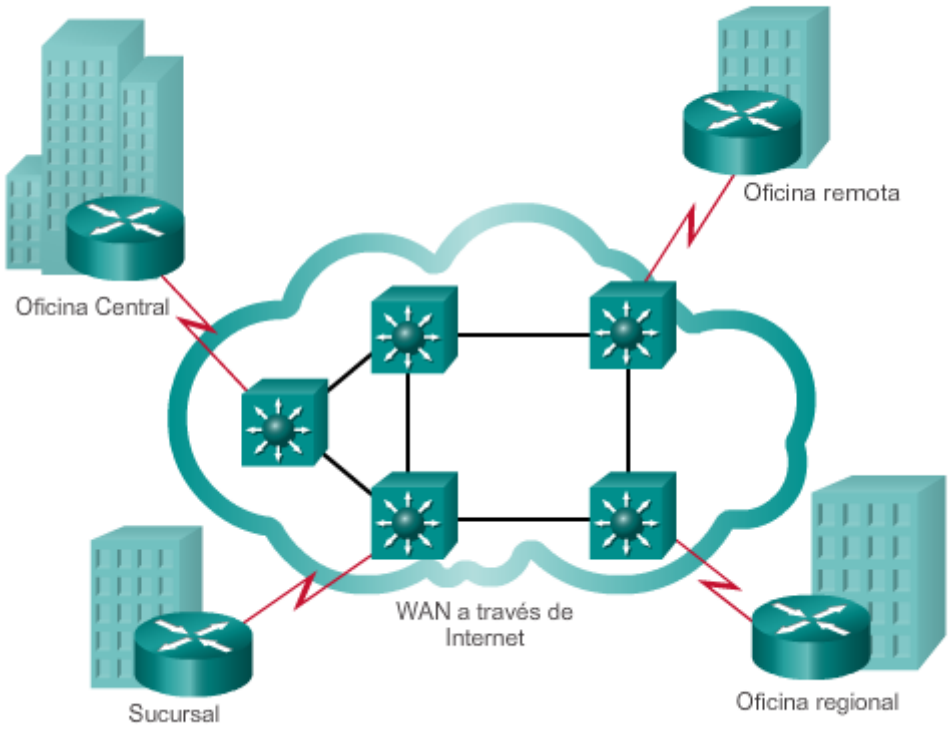
Capítulo 2: Conexión a la WAN 2.1.1.6 Redes de sucursales

SPAN Ingeniería tuvo tanto éxito con su proceso patentado que, otros seis años después, la demanda de sus servicios se incrementó enormemente. Hay nuevos proyectos en curso en varias ciudades. Para administrar estos proyectos, la empresa abrió pequeñas sucursales cercanas a los sitios de los proyectos.

Esta situación presenta nuevos desafíos para el equipo de TI. Para administrar la provisión de información y servicios en toda la empresa, SPAN Ingeniería cuenta ahora con un centro de datos, que aloja los diversos servidores y bases de datos de la empresa. Para asegurar que todas las partes de la empresa puedan acceder a los mismos servicios y las mismas aplicaciones independientemente de la ubicación de las oficinas, la empresa ahora debe implementar una WAN.

Para las sucursales que están en ciudades cercanas, la empresa decide usar líneas privadas dedicadas a través de su proveedor de servicios local. Sin embargo, para las oficinas que están ubicadas en otros países, Internet es una opción de conexión WAN atractiva. Si bien conectar oficinas a través de Internet es una opción económica, presenta problemas de seguridad y privacidad que el equipo de TI debe abordar.

Conexión de redes de sucursales



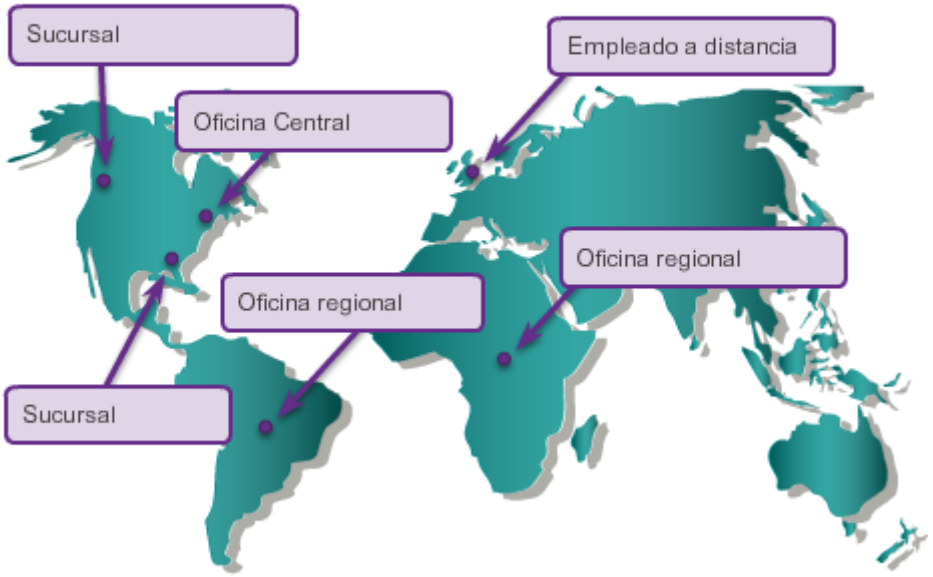
Capítulo 2: Conexión a la WAN 2.1.1.7 Red distribuida

Ahora, SPAN Ingeniería tiene 20 años de operación y cuenta con miles de empleados distribuidos en oficinas en todo el mundo, como se muestra en la figura 1. El costo de la red y los servicios relacionados implica un gasto significativo. La empresa busca proporcionar a sus empleados los mejores servicios de red con el menor costo posible. Los servicios de red optimizados permitirían que cada empleado trabaje con un porcentaje de eficiencia elevado.

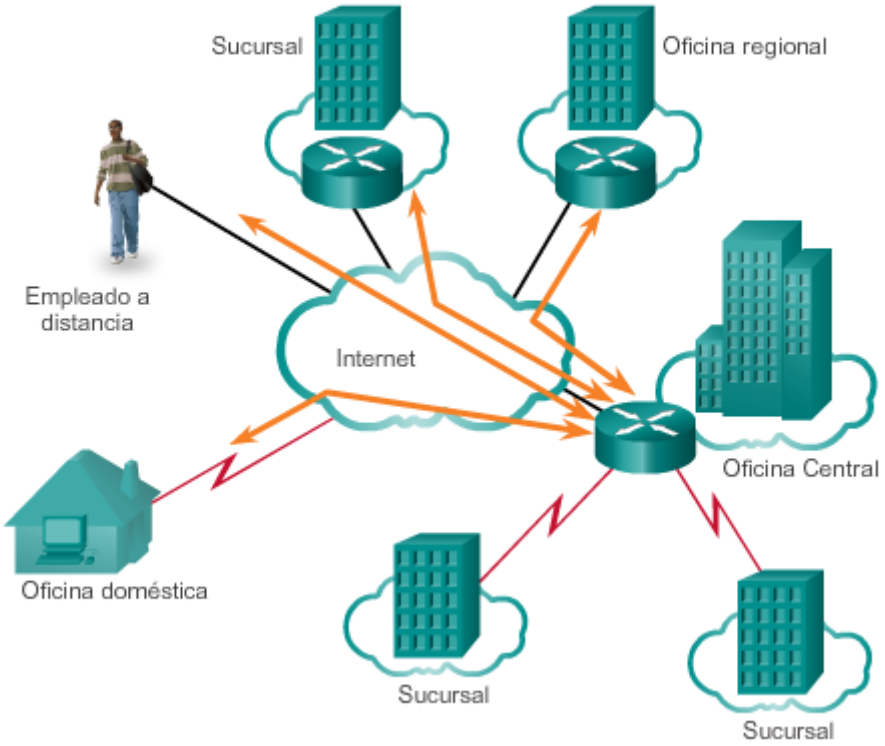
Para aumentar la rentabilidad, SPAN Ingeniería debe reducir sus gastos de operación. Reubicó algunas de sus oficinas en áreas menos costosas y también promueve el trabajo a distancia y los equipos de trabajo virtuales. Para aumentar la productividad y reducir los costos, se usan aplicaciones basadas en Web, que incluyen conferencias web, aprendizaje electrónico y herramientas de colaboración en línea. Las redes privadas virtuales (VPN) de sitio a sitio y de acceso remoto permiten que la empresa use Internet para conectarse de manera fácil y segura

con los empleados y las instalaciones en todo el mundo. Para cumplir con estos requisitos, la red debe proporcionar los servicios convergentes y la conectividad WAN de Internet segura necesarios para las personas y las oficinas y remotas, como se muestra en la figura 2.

Como se observa en este ejemplo, los requisitos de red de una empresa pueden cambiar significativamente a medida que la empresa crece con el tiempo. La distribución de empleados permite ahorrar costos de varias formas, pero pone mayores exigencias en la red. Una red no solo debe satisfacer las necesidades operativas diarias de la empresa, sino que debe ser capaz de adaptarse y crecer a medida que la empresa cambia. Los diseñadores y los administradores de red superan estos desafíos mediante la elección cuidadosa de tecnologías de red, protocolos y proveedores de servicios, y por medio de la optimización de sus redes con muchas de las técnicas y las arquitecturas de diseño de red descritas en este curso.



Conexión de una red empresarial global



Capítulo 2: Conexión a la WAN 2.1.1.8 Actividad: Identificar las topologías de WAN

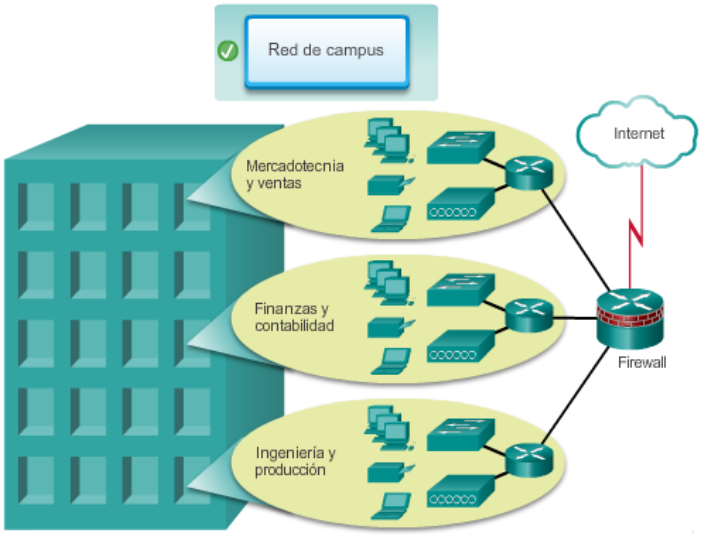
Actividad: Identificar las tecnologías WAN (parte 1)
Elija el tipo de red de tecnología WAN que mejor coincida con la descripción de la red y la ilustración. Haga clic en el botón 2 para continuar la actividad.

Descripción de la red
- Pequeña a mediana empresa
- Cientos de empleados
- Varias LAN de campus
- Personal interno de TI y de soporte de red

Red de oficina pequeña

Red de rama

Red distribuida



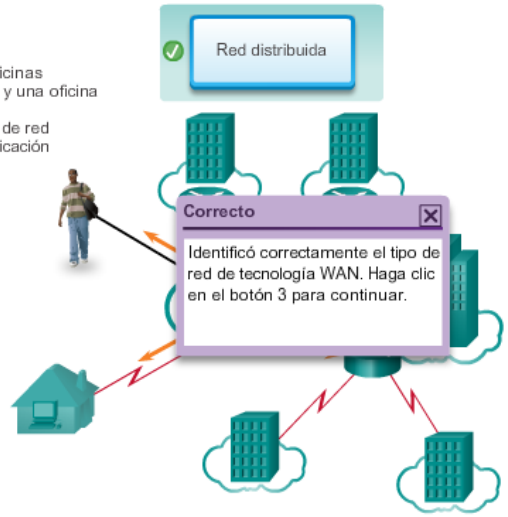
Actividad: Identificar las tecnologías WAN (parte 2)
Elija el tipo de red de tecnología WAN que mejor coincida con la descripción de la red y la ilustración. Haga clic en el botón 3 para continuar la actividad.

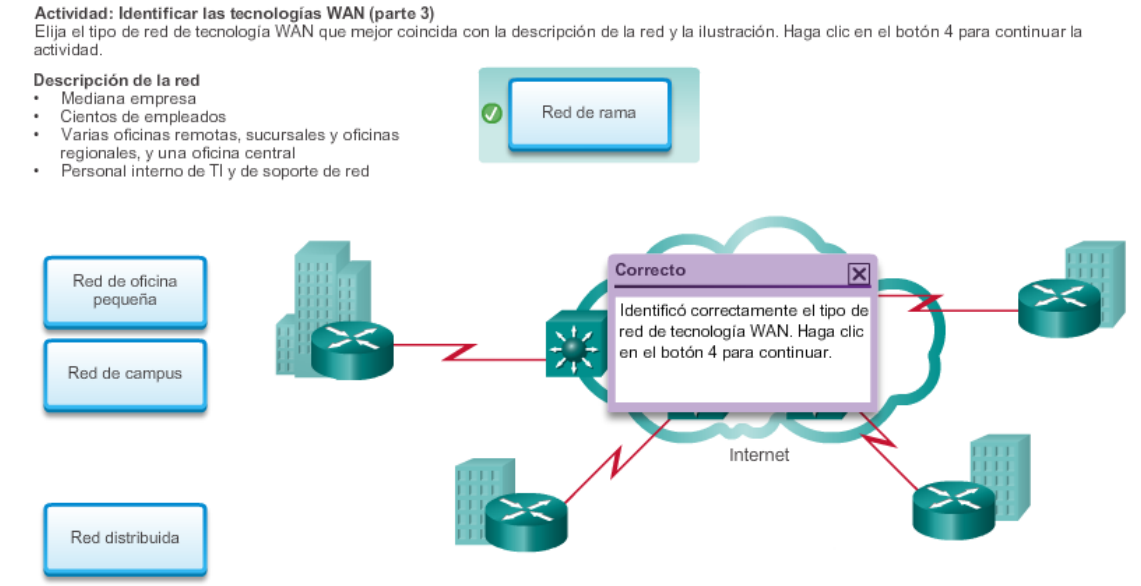
Descripción de la red
- Empresa de gran escala
- Miles de empleados
- Oficinas domésticas, sucursales, oficinas regionales, trabajadores a distancia y una oficina central
- Personal interno de TI y de soporte de red
- Red convergente y servicios de aplicación

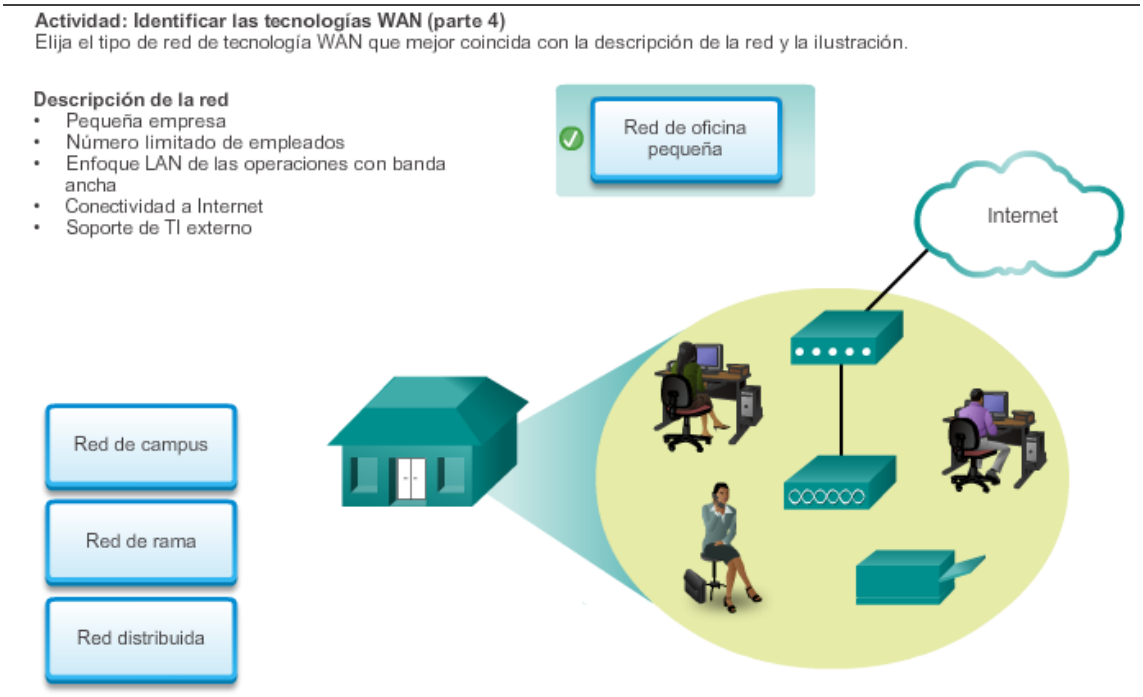
Red de oficina pequeña

Red de campus

Red de rama







Capítulo 2: Conexión a la WAN 2.1.2.1 WAN en el modelo OSI

Las operaciones WAN se centran principalmente en la capa física (capa 1 del modelo OSI) y en la capa de enlace de datos (capa 2 del modelo OSI). Los estándares de acceso WAN por lo general describen los métodos de entrega de la capa física y los requisitos de la capa de enlace de datos, incluidos el direccionamiento físico, el control del flujo y la encapsulación.

Varias autoridades reconocidas definen y administran los estándares de acceso WAN, incluidas las siguientes:

- Asociación de la Industria de Telecomunicaciones y Alianza de Industrias Electrónicas (TIA/EIA)

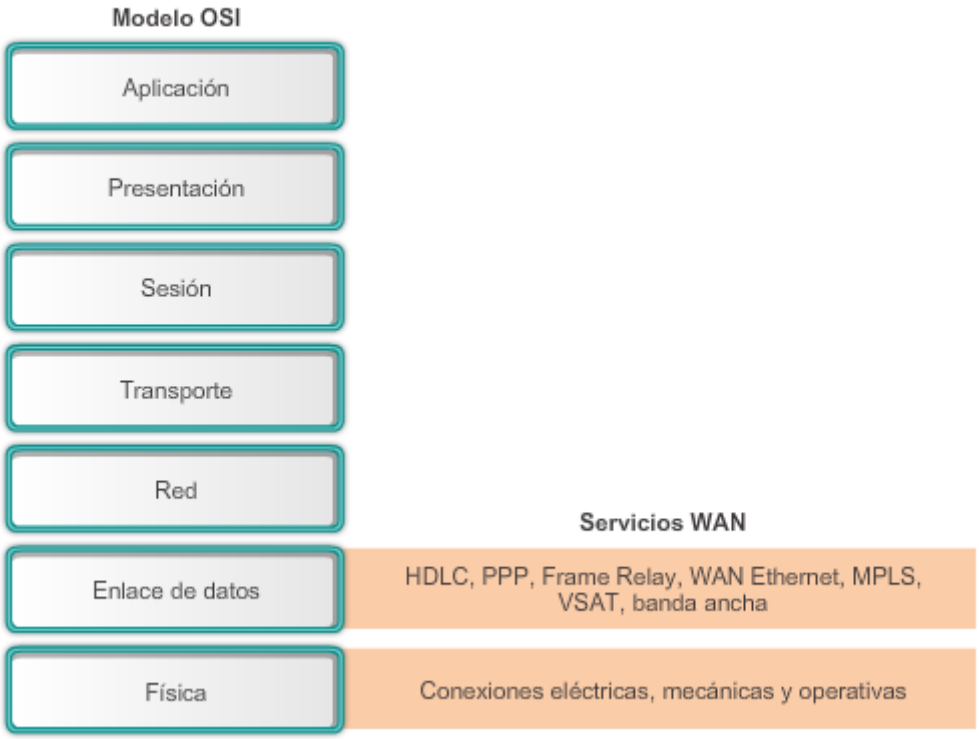
- Organización Internacional para la Estandarización (ISO)
- Instituto de Ingenieros en Electricidad y Electrónica (IEEE)

Los protocolos de capa 1 describen la manera de proporcionar conexiones eléctricas, mecánicas, operativas y funcionales a los servicios de un proveedor de servicios de comunicación.

Los protocolos de capa 2 definen la forma en que se encapsulan los datos para la transmisión a una ubicación remota, así como los mecanismos para transferir las tramas resultantes. Se usa una variedad de tecnologías diferentes, como el protocolo punto a punto (PPP), Frame Relay y ATM. Algunos de estos protocolos usan el mismo entramado básico o un subconjunto del mecanismo de control de enlace de datos de alto nivel (HDLC).

La mayoría de los enlaces WAN son punto a punto. Por este motivo, no se suele utilizar el campo de dirección de la trama de capa 2.

Las WAN operan en las capas 1 y 2



Capítulo 2: Conexión a la WAN 2.1.2.2 Terminología común de WAN

Una diferencia principal entre una WAN y una LAN es que, para usar los servicios de red de una prestadora de servicios WAN, una empresa u organización se debe suscribir a un proveedor de servicios WAN externo. Una WAN usa los enlaces de datos proporcionados por una prestadora de servicios para acceder a Internet y conectar las diferentes ubicaciones de una organización entre sí, a las ubicaciones de otras organizaciones, a los servicios externos y a los usuarios remotos.

La capa física de una WAN describe las conexiones físicas entre la red de la empresa y la red del proveedor de servicios. En la ilustración, se muestra la terminología que normalmente se usa para describir las conexiones WAN, entre otros:

- **Equipo local del cliente (CPE):**cables internos y dispositivos ubicados en el perímetro empresarial que se conectan a un enlace de una prestadora de servicios. El suscriptor es dueño del CPE o lo alquila al proveedor de servicios. En este contexto, un suscriptor es una empresa que obtiene los servicios WAN de un proveedor de servicios.

- **Equipo de comunicación de datos (DCE):** también llamado “equipo de terminación de circuito de datos”, el DCE consta de dispositivos que colocan los datos en el bucle local. Principalmente, el DCE proporciona una interfaz para conectar a los suscriptores a un enlace de comunicación en la nube WAN.

- **Equipo terminal de datos (DTE):**dispositivos del cliente que transmiten los datos desde un equipo host o la red de un cliente para la transmisión a través de la WAN. El DTE se conecta al bucle local a través del DCE.

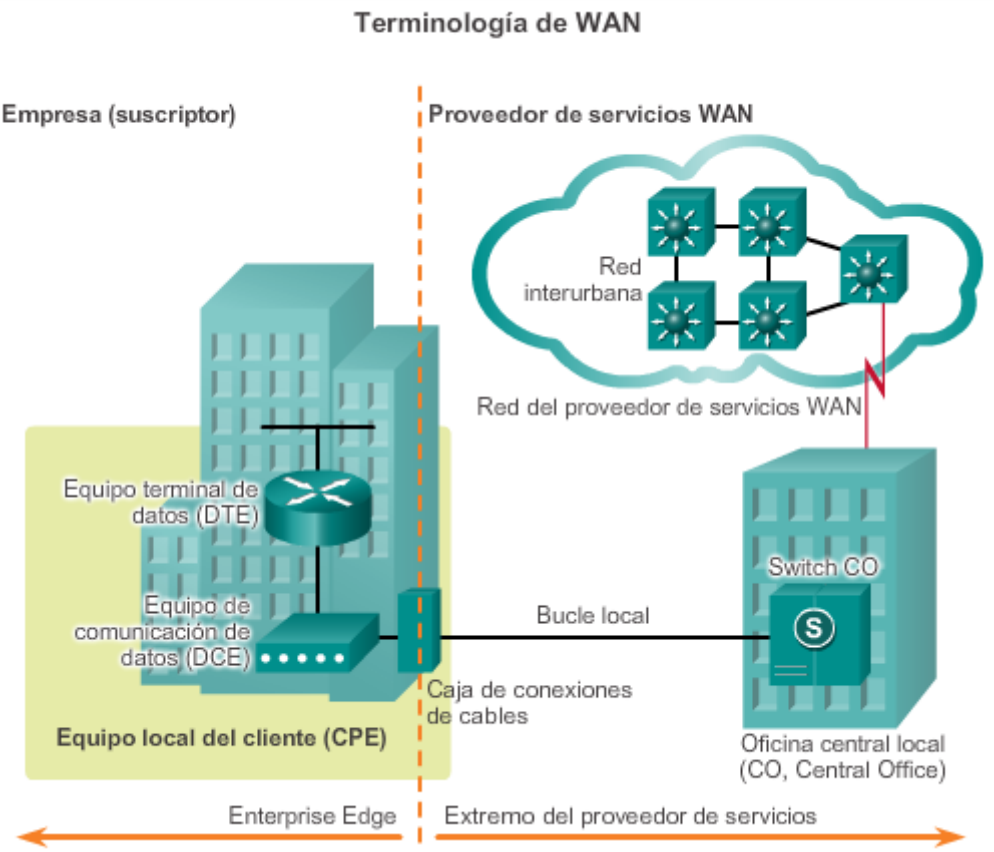
- **Punto de demarcación:** un punto establecido en un edificio o un complejo para separar el equipo del cliente del equipo del proveedor de servicios. En términos físicos, el punto de demarcación es la caja de conexiones del cableado, ubicada en las instalaciones del cliente, que conecta los cables del CPE al bucle local. Por lo general, se coloca de modo que sea de fácil acceso para un técnico. El punto de demarcación es el lugar donde la responsabilidad de la conexión pasa del usuario al proveedor de servicios. Cuando surgen problemas, es necesario determinar si el usuario o el proveedor de servicios es responsable de la resolución o la reparación.

- **Bucle local:** cable de cobre o fibra propiamente dicho que conecta el CPE a la CO del proveedor de servicios. A veces, el bucle local también se denomina “última milla”.

- **Oficina central (CO):** la CO es la instalación o el edificio del proveedor de servicios local que conecta el CPE a la red del proveedor.

- **Red interurbana:** consta de líneas de comunicación, switches, routers y otros equipos digitales, de largo alcance y de fibra óptica dentro de la red del proveedor de servicios

WAN.



Capítulo 2: Conexión a la WAN 2.1.2.3 Dispositivos WAN

Existen muchos tipos de dispositivos que son específicos de los entornos WAN, incluidos los siguientes:

- **Módem dial-up:** considerado una tecnología WAN antigua, un módem de banda de voz convierte (es decir, modula) 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 lado de la conexión, otro módem convierte nuevamente los sonidos en una señal digital (es decir, los demodula) como entrada para una computadora o una conexión de red.

- **Servidor de acceso:** concentra las comunicaciones de entrada y de salida del módem dial-up de los usuarios. Considerado una tecnología antigua; un servidor de acceso puede tener una combinación de interfaces analógicas y digitales y admitir cientos de usuarios simultáneos.

- **Módem de banda ancha:** un tipo de módem digital que se utiliza con servicio de Internet por DSL o por cable de alta velocidad. Ambos funcionan de manera similar al módem de banda de voz, pero usan mayores velocidades de transmisión y frecuencias de banda ancha.

- **CSU/DSU:** las líneas arrendadas digitales requieren una CSU y una DSU. Una CSU/DSU puede ser un dispositivo separado, como un módem, o puede ser una interfaz en un

router. La CSU proporciona terminación de la señal digital y asegura la integridad de la conexión mediante la corrección de errores y el monitoreo de la línea. La DSU convierte las tramas de línea en tramas que la LAN puede interpretar y viceversa.

- **Switch WAN:** un dispositivo de internetworking de varios puertos utilizado en las redes de los proveedores de servicios. Por lo general, estos dispositivos conmutan el tráfico, como Frame Relay o ATM, y operan en la capa 2.

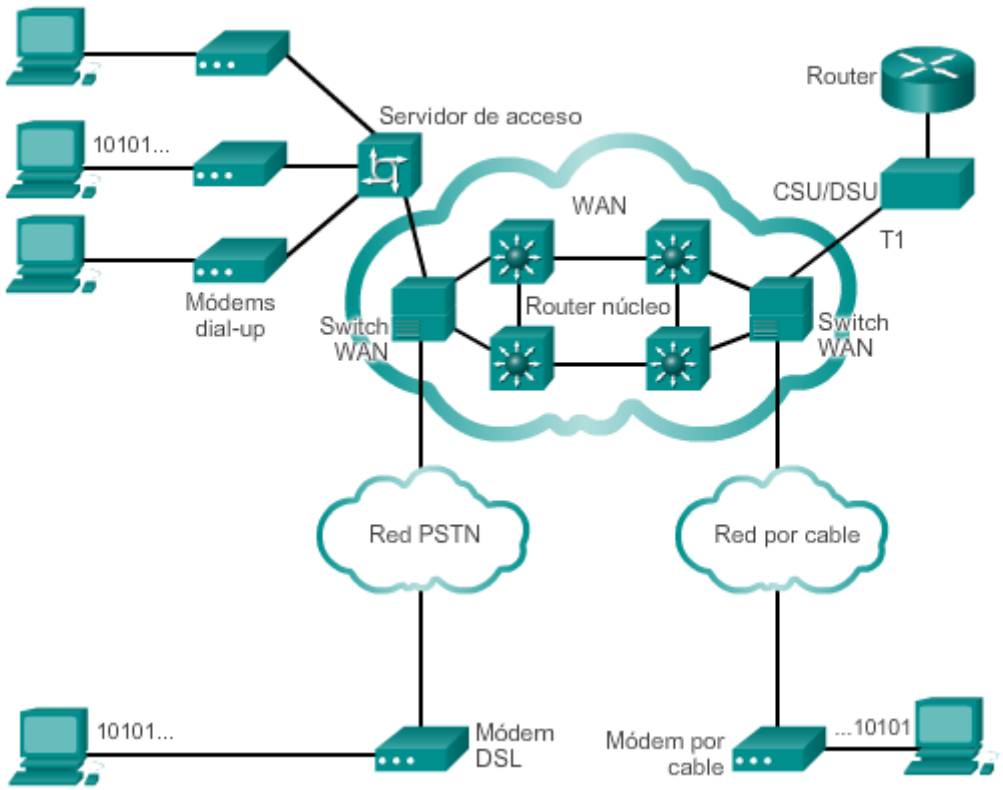
- **Router:** proporciona internetworking y puertos de interfaz de acceso WAN que se usan para conectarse a la red del proveedor de servicios. Estas interfaces pueden ser conexiones seriales, Ethernet u otras interfaces WAN. Con algunos tipos de interfaces WAN, se requiere un dispositivo externo, como una DSU/CSU o un módem (analógico, por cable o DSL) para conectar el router al proveedor de servicios local.

- **Router principal/switch multicapa:**router o switch multicapa que reside en el centro o en el backbone de la WAN, en lugar de en la periferia. Para desempeñar esta función, un router o switch multicapa debe poder admitir varias interfaces de telecomunicaciones con la mayor velocidad usada en el núcleo de la WAN. También debe poder reenviar paquetes IP a máxima velocidad en todas esas interfaces. El router o switch multicapa también debe admitir los protocolos de routing que se utilizan en el núcleo.

Nota: la lista anterior no es exhaustiva y pueden ser necesarios otros dispositivos, según la tecnología de acceso WAN elegida.

Las tecnologías WAN se conmutan por circuitos o por paquetes. El tipo de dispositivo usado depende de la tecnología WAN implementada.

Dispositivos WAN comunes



Capítulo 2: Conexión a la WAN 2.1.2.4 Conmutación de circuitos

Las red de conmutación de circuitos son aquellas que establecen un circuito (o canal) dedicado entre los nodos y las terminales antes de que los usuarios se puedan comunicar. Específicamente, la conmutación de circuitos establece una conexión virtual dedicada para voz o datos entre un emisor y un receptor en forma dinámica. Antes de que la comunicación pueda comenzar, es necesario establecer la conexión a través de la red del proveedor de servicios.

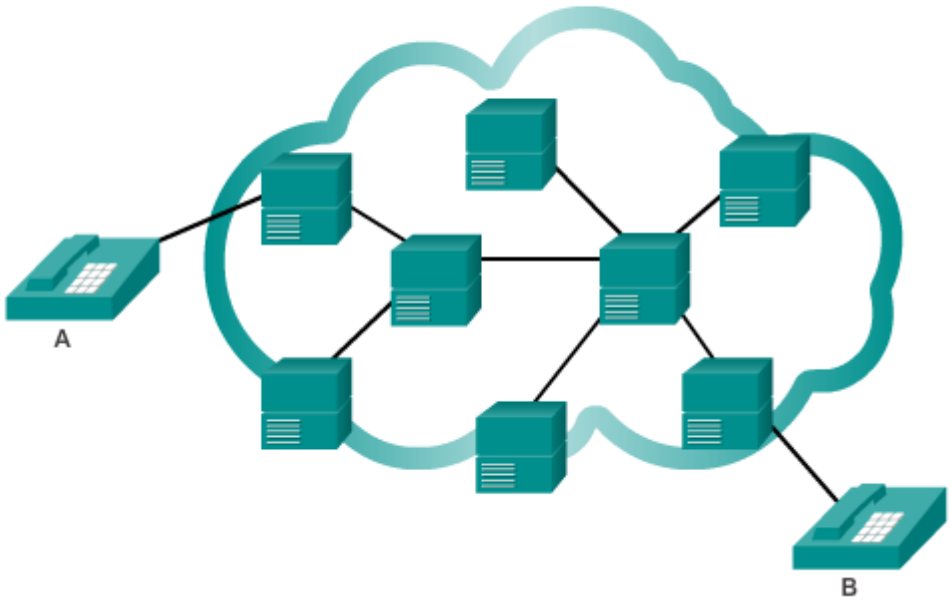
Como ejemplo, cuando un suscriptor realiza una llamada telefónica, el número marcado se usa para establecer los switches en los intercambios a lo largo de la ruta de la llamada, de modo que haya un circuito continuo desde el origen hasta el destinatario de la llamada. Debido a la operación de conmutación utilizada para establecer el circuito, el sistema telefónico se denomina “red de conmutación de circuitos”. Si los teléfonos se reemplazan por módems, el circuito de conmutación puede transportar datos informáticos.

Si el circuito transporta datos informáticos, es posible que el uso de esta capacidad fija no sea eficaz. Por ejemplo, si el circuito se utiliza para acceder a Internet, se produce una ráfaga de actividad en el circuito cuando se transfiere una página web. A esto lo podría seguir un período sin actividad, en el que el usuario lee la página, y luego otra ráfaga de actividad cuando se transfiere la página siguiente. Esta variación en el uso, entre un uso nulo y un uso máximo, es típica del tráfico de la red de computadoras. Debido a que el suscriptor tiene uso exclusivo de la asignación de la capacidad fija, los circuitos de conmutación generalmente son una manera costosa de mover datos.

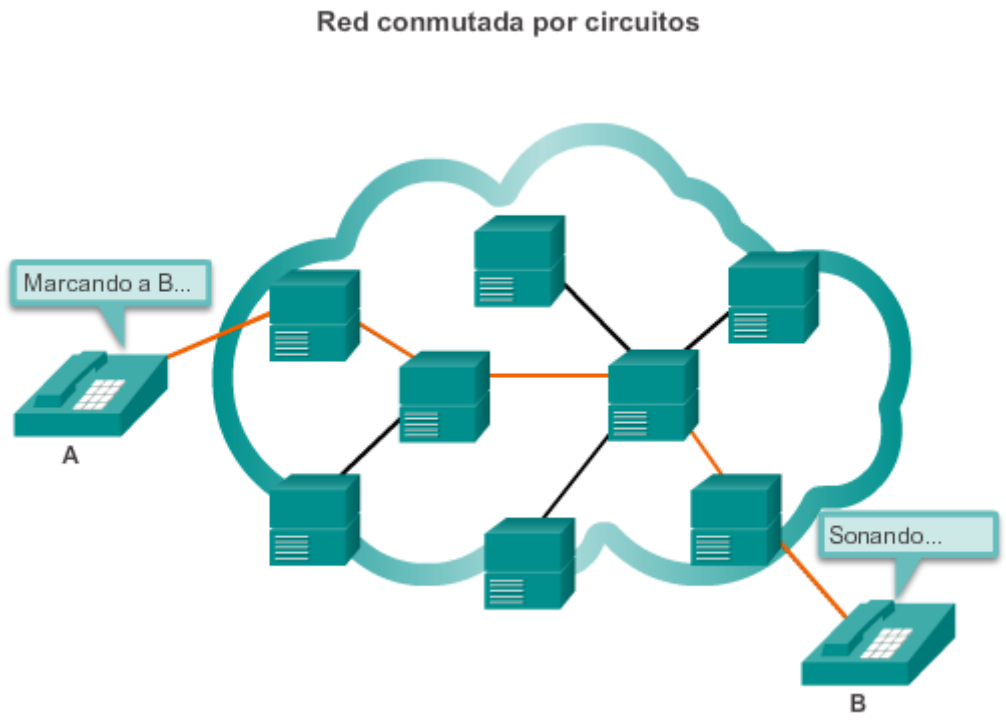
Los dos tipos más comunes de tecnologías WAN de conmutación de circuitos son la red pública de telefonía de conmutación (PSTN) y la red digital de servicios integrados (ISDN).

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

Red conmutada por circuitos



La marcación establece un circuito físico por el sistema.



La marcación establece un circuito físico por el sistema.

Capítulo 2: Conexión a la WAN 2.1.2.5 Conmutación de paquetes

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

En una red de conmutación de paquetes (PSN), los switches determinan los enlaces a través de los que se deben enviar los paquetes según la información de direccionamiento en cada paquete. Los siguientes son dos enfoques de esta determinación de enlaces:

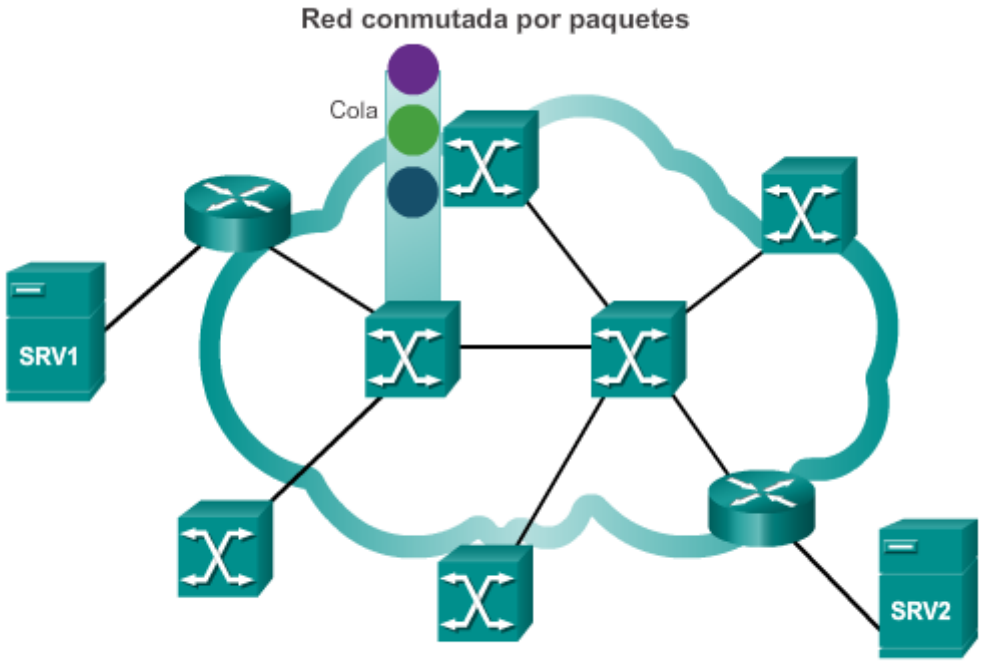
- **Sistemas sin conexión:** se debe transportar toda la información de direccionamiento en cada paquete. Cada switch debe evaluar la dirección para determinar adónde enviar el paquete. Un ejemplo de sistema sin conexión es Internet.

- **Sistemas orientados a la conexión:**la red predetermina la ruta para un paquete, y cada paquete solo tiene que transportar un identificador. El switch determina la ruta siguiente al buscar el identificador en las tablas almacenadas en la memoria. El conjunto de entradas en las tablas identifica una ruta o un circuito particular a través del sistema. Si el circuito se establece en forma temporal mientras un paquete viaja a través de él y luego se divide nuevamente, se lo denomina “circuito virtual” (VC). Un ejemplo de un sistema orientado a la conexión es Frame Relay. En el caso de Frame Relay, los identificadores utilizados se denominan “identificadores de conexión de enlace de datos” (DLCI).

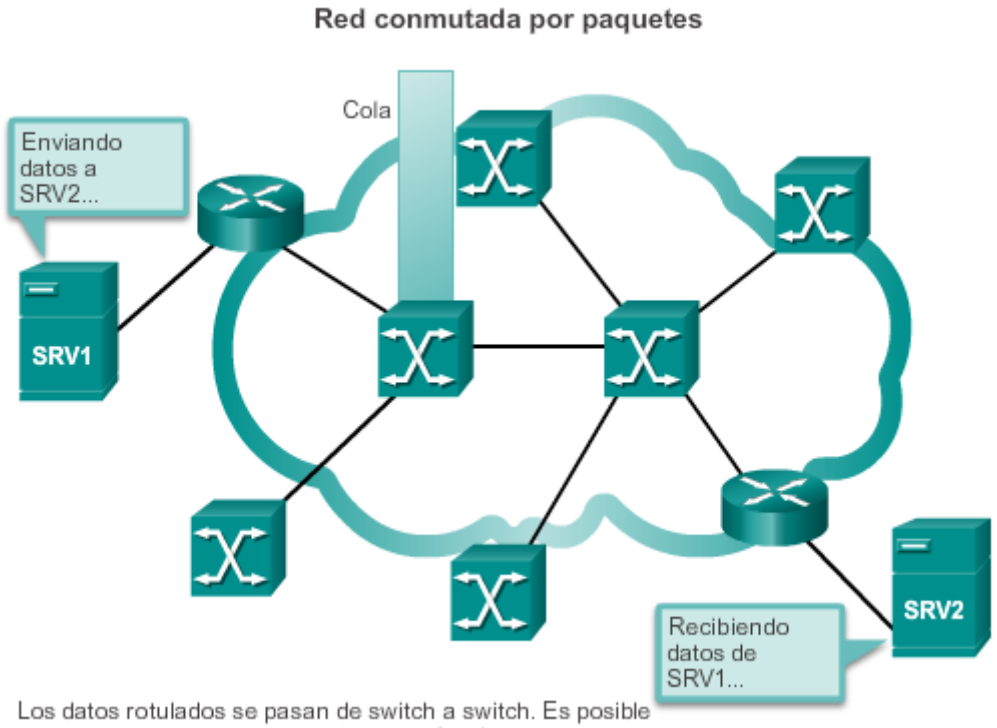
Debido a que varios usuarios comparten los enlaces internos entre los switches, el costo de la conmutación de paquetes es inferior al de la conmutación de circuitos. Sin embargo, los retrasos (latencia) y la variabilidad de retraso (vibración) son mayores en las redes de conmutación de paquetes que en las redes de conmutación de circuitos. Esto se debe a que se comparten los enlaces, y los paquetes se deben recibir por completo en un switch antes de

pasar al siguiente. A pesar de la latencia y la vibración inherentes en las redes compartidas, la tecnología moderna permite el transporte satisfactorio de las comunicaciones de voz y video en estas redes.

Haga clic en el botón Reproducir de la ilustración para ver cómo funciona la conmutación de paquetes. En la animación, SRV1 envía datos a SRV2. Una vez que el paquete atraviesa la red del proveedor de servicios, llega al segundo switch del proveedor. El paquete se agrega a la cola y se reenvía después de que se reenvíen todos los otros paquetes en la cola. Finalmente, el paquete llega a SRV2.

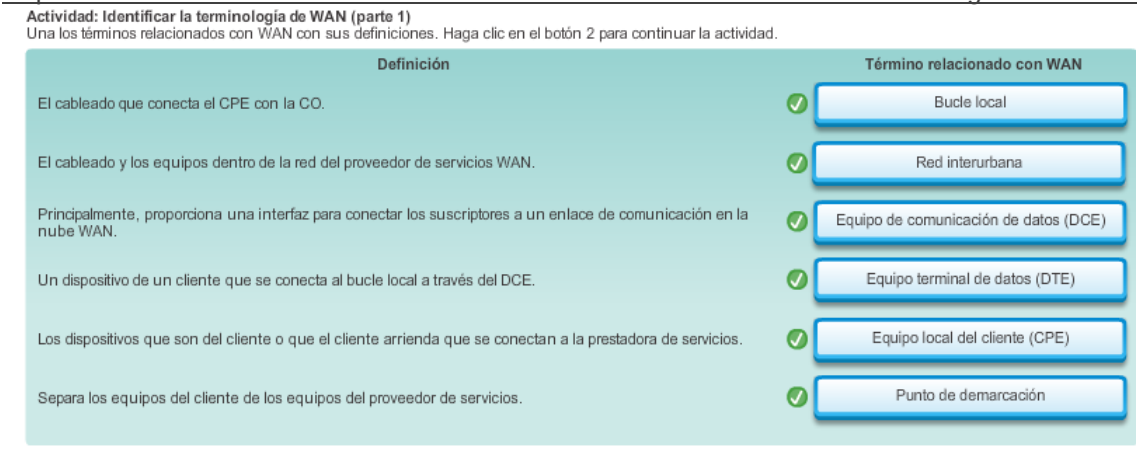


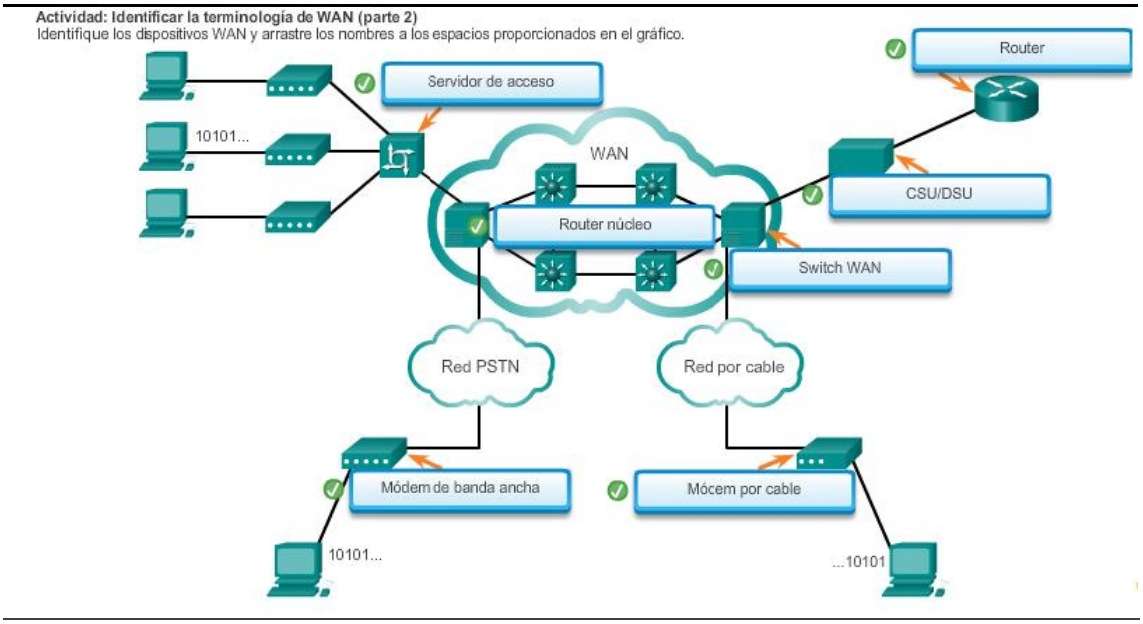
Los datos rotulados se pasan de switch a switch. Es posible que tenga que esperar su turno en un vínculo.



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

Capítulo 2: Conexión a la WAN 2.1.2.6 Actividad: Identificar la terminología de WAN





Capítulo 2: Conexión a la WAN 2.2.1.1 Opciones de conexión de enlace WAN

Existen diversas opciones de conexión de acceso WAN que los ISP pueden utilizar para conectar el bucle local al perímetro empresarial. Estas opciones de acceso WAN varían en términos de tecnología, velocidad y costo. Cada una tiene ventajas y desventajas diferentes. Familiarizarse con estas tecnologías es una parte importante del diseño de red.

Como se muestra en la figura 1, una empresa puede obtener acceso WAN a través de:

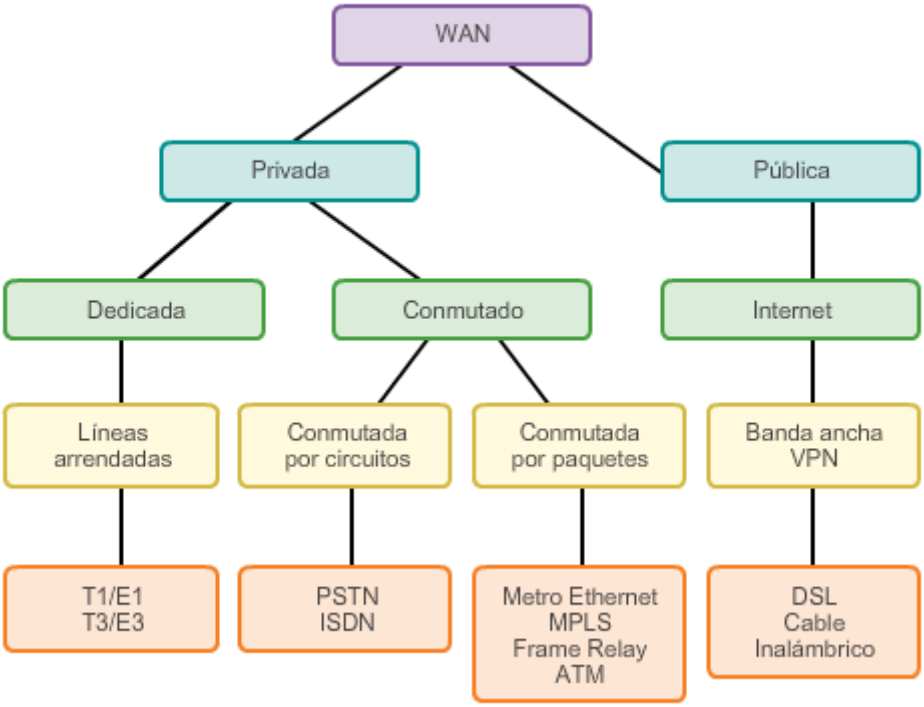
- **Infraestructura WAN privada:** los proveedores de servicios pueden ofrecer líneas arrendadas punto a punto dedicadas, enlaces de conmutación de circuitos, como PSTN o ISDN, y enlaces de conmutación de paquetes, como WAN Ethernet, ATM o Frame Relay.

- **Infraestructura WAN pública:** el proveedor de servicios puede ofrecer acceso a Internet de banda ancha mediante una línea de suscriptor digital (DSL), cable y acceso satelital. Las opciones de conexión de banda ancha normalmente se usan para conectar oficinas pequeñas y trabajadores a distancia a un sitio corporativo a través de Internet. Los datos

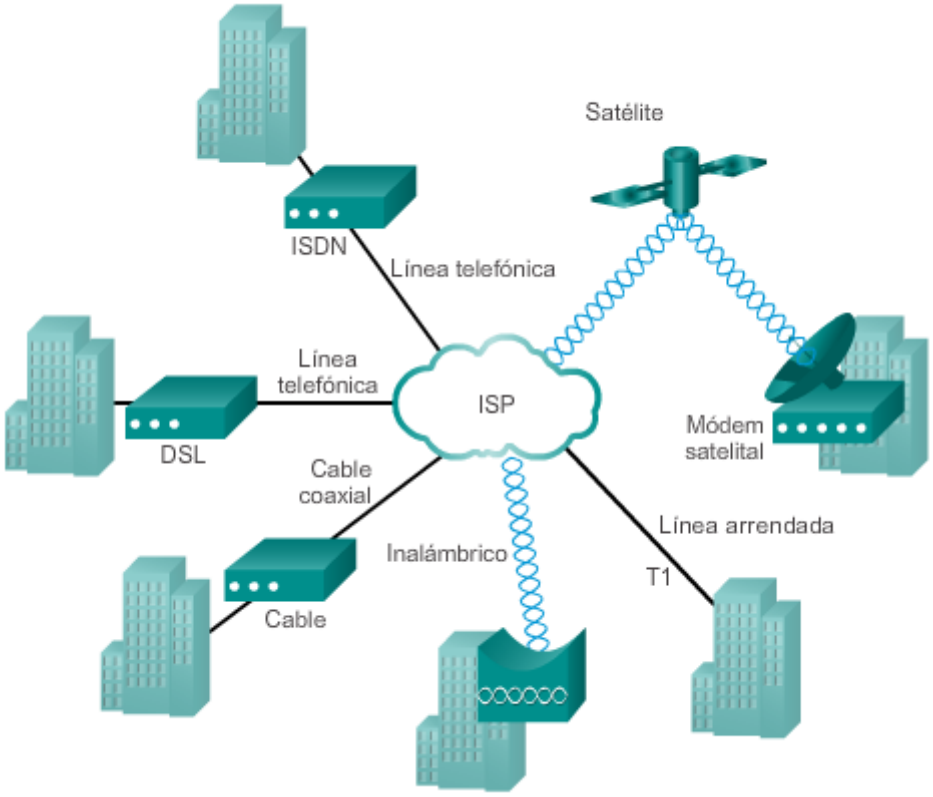
que se transmiten entre sitios corporativos a través de la infraestructura WAN pública se deben proteger mediante VPN.

En la topología de la figura 2, se muestran algunas de estas tecnologías de acceso WAN.

Opciones de acceso WAN



Tecnologías de acceso WAN



Capítulo 2: Conexión a la WAN 2.2.1.2 Infraestructura de la red del proveedor de servicios

Cuando un proveedor de servicios WAN recibe datos de un cliente en un sitio, debe reenviar los datos al sitio remoto para la entrega final al destinatario. En algunos casos, el sitio remoto se puede conectar al mismo proveedor de servicios que el sitio de origen. En otros casos, el sitio remoto se puede conectar a un ISP diferente, y el ISP de origen debe transmitir los datos al ISP conectado.

Las comunicaciones de largo alcance normalmente son esas conexiones entre ISP o entre sucursales en empresas muy grandes.

Las redes de los proveedores de servicios son complejas. Constan principalmente de medios de fibra óptica de un ancho de banda elevado, que usan el estándar de red óptica síncrona (SONET) o de jerarquía digital síncrona (SDH). Estos estándares definen cómo transferir diverso tráfico de datos, voz y video a través de fibra óptica mediante láseres o diodos emisores de luz (LED) por grandes distancias.

Nota: SONET es un estándar de ANSI con base en los Estados Unidos, mientras que SDH es un estándar de ETSI y de ITU con base en Europa. Ambos son básicamente iguales y, por lo tanto, con frecuencia se los presenta como SONET/SDH.

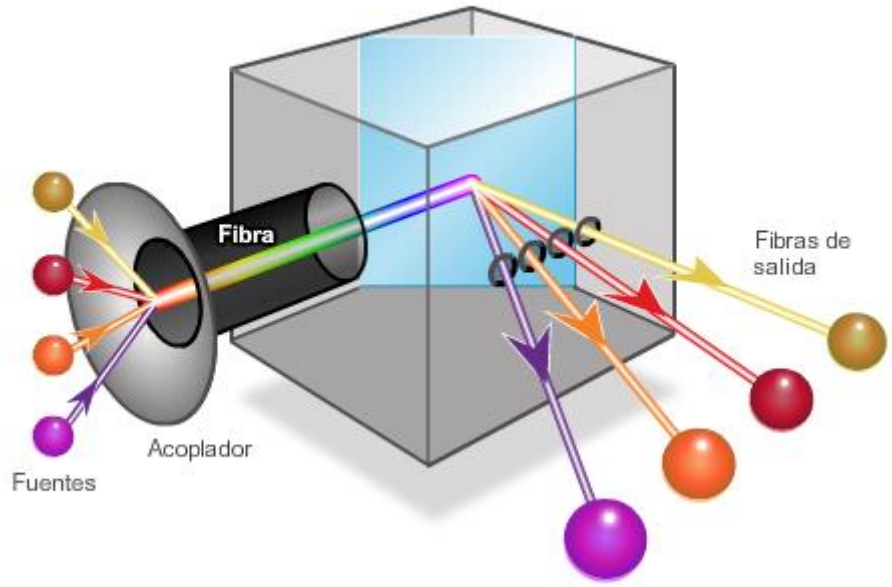
Un avance más reciente en los medios de fibra óptica para las comunicaciones de largo alcance se denomina “multiplexación por división de longitud de onda densa” (DWDM). DWDM multiplica la cantidad de ancho de banda que puede admitir un único hilo de fibra, como se muestra en la figura 1.

Específicamente, DWDM tiene las siguientes características:

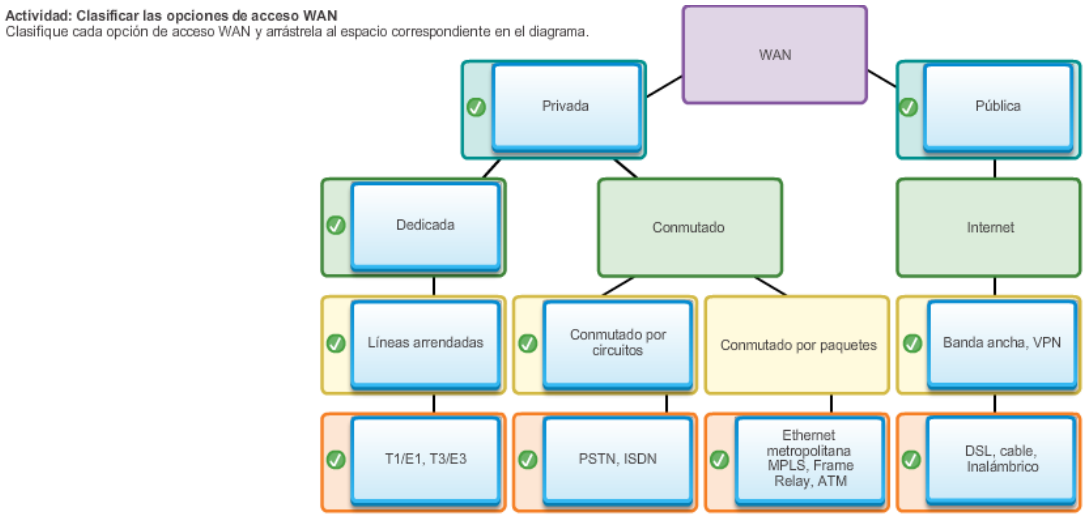
- Habilita comunicaciones bidireccionales a través de un hilo de fibra.
- Puede multiplexar más de 80 canales de datos (es decir, longitudes de onda) diferentes en una única fibra.
- Cada canal puede transportar una señal multiplexada de10 Gb/s.
- Asigna señales ópticas entrantes a longitudes de onda de luz específicas (es decir, frecuencias).
- Puede amplificar esas longitudes de onda para mejorar la intensidad de la señal.
- Admite los estándares SONET y SDH.

Los circuitos DWDM se usan en todos los sistemas de cables submarinos de comunicaciones modernos y en otros circuitos de largo alcance, como se muestra en la figura 2.

DWDM



Las redes de los proveedores de servicios usan DWDM



Capítulo 2: Conexión a la WAN 2.2.2.1 Líneas arrendadas

Cuando se requieren conexiones dedicadas permanentes, se utiliza un enlace punto a punto para proporcionar una ruta de comunicaciones WAN preestablecida desde las instalaciones del cliente hasta la red del proveedor. Por lo general, un proveedor de servicios arrienda las líneas punto a punto, que se llaman “líneas arrendadas”.

Las líneas arrendadas existen desde comienzos de los años cincuenta y, por este motivo, se las conoce con nombres diferentes como circuito arrendado, enlace serial, línea serial, enlace punto a punto y línea T1/E1 o T3/E3. El término “línea arrendada” hace referencia al hecho de que la organización paga una tarifa mensual de arrendamiento a un proveedor de servicios para usar la línea. Hay líneas arrendadas disponibles con diferentes capacidades y, generalmente, el precio se basa en el ancho de banda requerido y en la distancia entre los dos puntos conectados.

En América del Norte, los proveedores de servicios usan el sistema de portadora T para definir la capacidad de transmisión digital de un enlace serial de medios de cobre, mientras que en Europa se usa el sistema de portadora E, como se muestra en la ilustración. Por ejemplo, un enlace T1 admite 1,544 Mb/s, un E1admite 2,048 Mb/s, un T3 admite 43,7 Mb/s y una conexión E3 admite 34,368 Mb/s. Para definir la capacidad de transmisión digital de una red de fibra óptica, se utilizan las velocidades de transmisión de la portadora óptica (OC).

Las ventajas de las líneas arrendadas incluyen las siguientes:

- **Simplicidad:** los enlaces de comunicación punto a punto requieren conocimientos mínimos de instalación y mantenimiento.

- **Calidad:** los enlaces de comunicación punto a punto generalmente ofrecen una alta calidad de servicio si tienen un ancho de banda adecuado. La capacidad dedicada quita latencia o vibración entre las terminales.

- **Disponibilidad:** la disponibilidad constante es esencial para algunas aplicaciones, como el comercio electrónico. Los enlaces de comunicación punto a punto proporcionan la capacidad dedicada permanente que se necesita para VoIP o para video sobre IP.

Las desventajas de las líneas arrendadas incluyen lo siguiente:

- **Costo:** en general, los enlaces punto a punto son el tipo de acceso WAN más costoso. Cuando se usan para conectar varios sitios a través de distancias cada vez mayores, el costo de las soluciones de línea arrendada puede ser significativo. Además, cada terminal requiere una interfaz en el router, lo que aumenta los costos de los equipos.

- **Flexibilidad limitada:** el tráfico WAN suele ser variable, y las líneas arrendadas tienen una capacidad fija, de modo que el ancho de banda de la línea rara vez coincide con la necesidad de forma precisa. Por lo general, cualquier cambio en la línea arrendada requiere que el personal del ISP visite el sitio para ajustar la capacidad.

Generalmente, el protocolo de capa 2 es HDLC o PPP.

Ejemplo de topología de línea arrendada

Capítulo 2: Conexión a la WAN 2.2.2.2 Dial-up

Cuando no hay ninguna otra tecnología WAN disponible, es posible que se requiera acceso WAN por dial-up. Por ejemplo, una ubicación remota podría usar un módem y líneas telefónicas de marcado analógico para proporcionar baja capacidad y conexiones de conmutación dedicadas. Cuando se necesita realizar transferencias de datos de bajo volumen de manera intermitente, el acceso por dial-up es conveniente.

En la telefonía tradicional, se usa un cable de cobre, al que se denomina “bucle local”, para conectar el auricular del teléfono en las instalaciones del suscriptor a la CO. La señal en el bucle local durante una llamada es una señal electrónica continuamente cambiante, que es una traducción de la voz del suscriptor a una señal analógica.

Los bucles locales tradicionales pueden transportar datos informáticos binarios a través de 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 en datos binarios en el destino. Las características físicas del bucle local y su conexión a la PSTN limitan la velocidad de señal a menos de 56 kb/s.

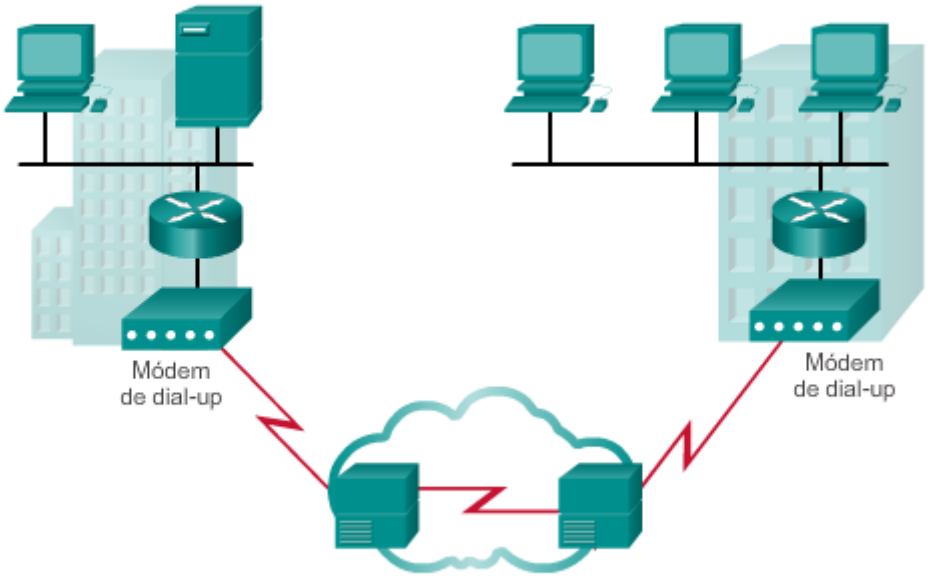
Para pequeñas empresas, estas conexiones dial-up de velocidad relativamente baja son adecuadas para el intercambio de cifras de ventas, precios, informes regulares y correos electrónicos. Usar dial-up automático a la noche o durante los fines de semana para transferir

archivos grandes y realizar copias de seguridad de datos permite aprovechar las tarifas más bajas de horas no pico (cargos interurbanos). Las tarifas dependen de la distancia entre las terminales, la hora del día y la duración de la llamada.

Las ventajas de los módems y las líneas analógicas son la simplicidad, la disponibilidad y el bajo costo de implementación. Las desventajas son las bajas velocidades de datos y un tiempo de conexión relativamente prolongado. El circuito dedicado tiene poco retraso o poca vibración para el tráfico punto a punto, pero el tráfico de voz o video no funciona correctamente en estas velocidades de bit bajas.

Nota: si bien muy pocas empresas admiten el acceso por dial-up, este sigue siendo una solución viable para áreas remotas con opciones de acceso WAN limitadas.

Ejemplo de topología dial-up



WAN armada con una conexión a petición mediante un módem y la red telefónica de voz.

Capítulo 2: Conexión a la WAN 2.2.2.3 ISDN

La red digital de servicios integrados (ISDN) es una tecnología de conmutación de circuitos que habilita al bucle local de una PSTN para transportar señales digitales, lo que da como resultado conexiones de conmutación de mayor capacidad.

ISDN cambia las conexiones internas de la PSTN para que transporte señales digitales multiplexadas por división de tiempo (TDM) en vez de señales analógicas. TDM permite que se transfieran dos o más señales, o flujos de bits, como subcanales en un canal de comunicación. Las señales parecen transferirse en forma simultánea; sin embargo, físicamente, las señales se turnan en el canal.

En la figura 1, se muestra un ejemplo de una topología de ISDN. La conexión ISDN puede requerir un adaptador de terminal (TA), que es un dispositivo utilizado para conectar las conexiones de la interfaz de velocidad básica (BRI) de ISDN a un router.

ISDN convierte el bucle local en una conexión digital TDM. Este cambio permite que el bucle local transporte las señales digitales, lo que genera conexiones de conmutación de mayor capacidad. La conexión usa canales de corriente portadora (B) de 64 kb/s para transportar voz y datos, y un canal delta (D), de señalización, para la configuración de llamadas y otros propósitos.

Existen dos tipos de interfaces de ISDN:

- **Interfaz de velocidad básica (BRI):** la BRI ISDN está diseñada para su uso en hogares y pequeñas empresas, y proporciona dos canales B de 64 kb/s y un canal D de 16 kb/s. El canal D de BRI está diseñado para propósitos de control y con frecuencia se infrautiliza, debido a que solo tiene que controlar dos canales B (figura 2).

- **Interfaz de velocidad primaria (PRI):**ISDN también está disponible para instalaciones de mayor tamaño. En América del Norte, PRI proporciona 23 canales B con 64 kb/s y un canal D con 64 kb/s para una velocidad de bits total de hasta 1,544 Mb/s. Esto incluye cierta sobrecarga adicional para la sincronización. En Europa, Australia y otras partes del mundo, PRI ISDN proporciona 30 canales B y un canal D para una velocidad de bits total de hasta 2,048 Mb/s, lo que incluye la sobrecarga para la sincronización (figura 3).

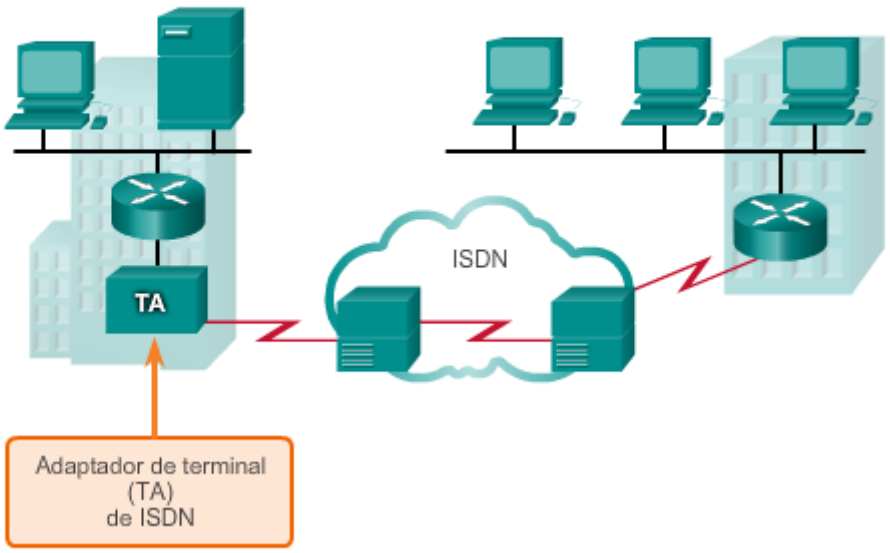
BRI tiene un tiempo de configuración de llamada inferior a un segundo, y el canal B de 64 kb/s proporciona mayor capacidad que un enlace de módem analógico. Si se requiere mayor capacidad, se puede activar un segundo canal B para proporcionar un total de 128 kb/s. Si bien es no es adecuado para video, permite varias conversaciones de voz simultáneas además del tráfico de datos.

Otra aplicación común de ISDN es proporcionar la capacidad adicional necesaria en una conexión de línea arrendada. La línea arrendada tiene el tamaño para transportar cargas de tráfico promedio, mientras que la ISDN se agrega durante períodos de picos de demanda. Si la línea arrendada falla, la ISDN también se usa como respaldo. Las tarifas de ISDN se determinan sobre la base de los canales B y son similares a las de las conexiones de voz analógicas.

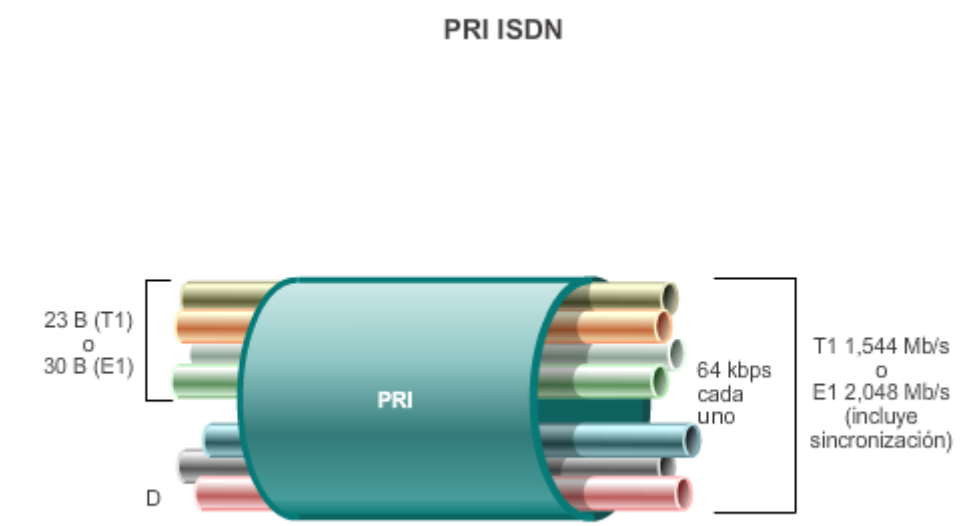
Con PRI ISDN, se pueden conectar varios canales B entre dos terminales. Esto permite videoconferencias y conexiones de datos con un ancho de banda elevado sin latencia o vibración. Sin embargo, usar varias conexiones a través de distancias largas puede ser muy costoso.

Nota: si bien ISDN sigue siendo una tecnología importante para las redes de los proveedores de servicios de telefonía, su popularidad como opción de conexión a Internet disminuyó debido a la introducción de DSL de alta velocidad y otros servicios de banda ancha.

Ejemplo de topología de ISDN



BRI RDSI



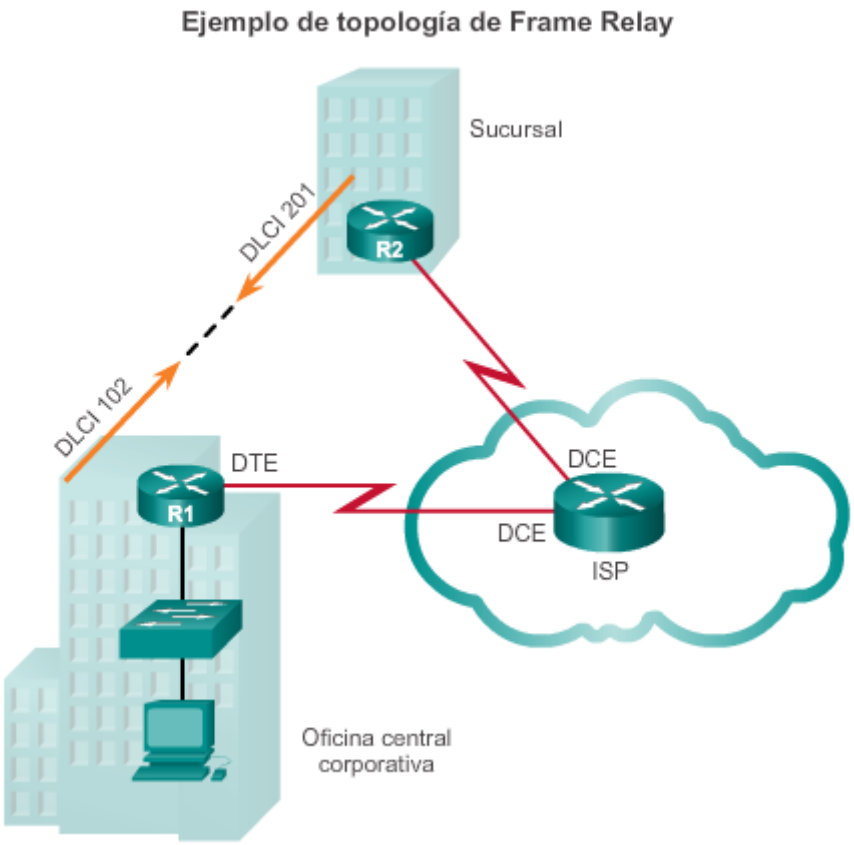
Capítulo 2: Conexión a la WAN 2.2.2.4 Frame Relay

Frame Relay es una tecnología WAN multiacceso sin difusión (NBMA) simple de capa 2 que se utiliza para interconectar las LAN de una empresa. Para conectarse a varios sitios mediante PVC, se puede usar una única interfaz de router. Los PVC se usan para transportar tráfico de voz y datos entre origen y destino y admiten velocidades de datos de hasta 4 Mb/s, si bien algunos proveedores ofrecen velocidades aun mayores.

Los routers perimetrales solo requieren una única interfaz, incluso cuando se usan varios circuitos virtuales (VC). La línea arrendada corta al perímetro de la red Frame Relay permite conexiones rentables entre las LAN ampliamente dispersas.

Frame Relay crea PVC que se identifican únicamente por un identificador de conexión de enlace de datos (DLCI). Los PVC y los DLCI aseguran la comunicación bidireccional de un dispositivo DTE a otro.

Por ejemplo, en la ilustración, el R1 usa el DLCI 102 para llegar al R2, mientras que el R2 usa el DLCI 201 para llegar al R1.



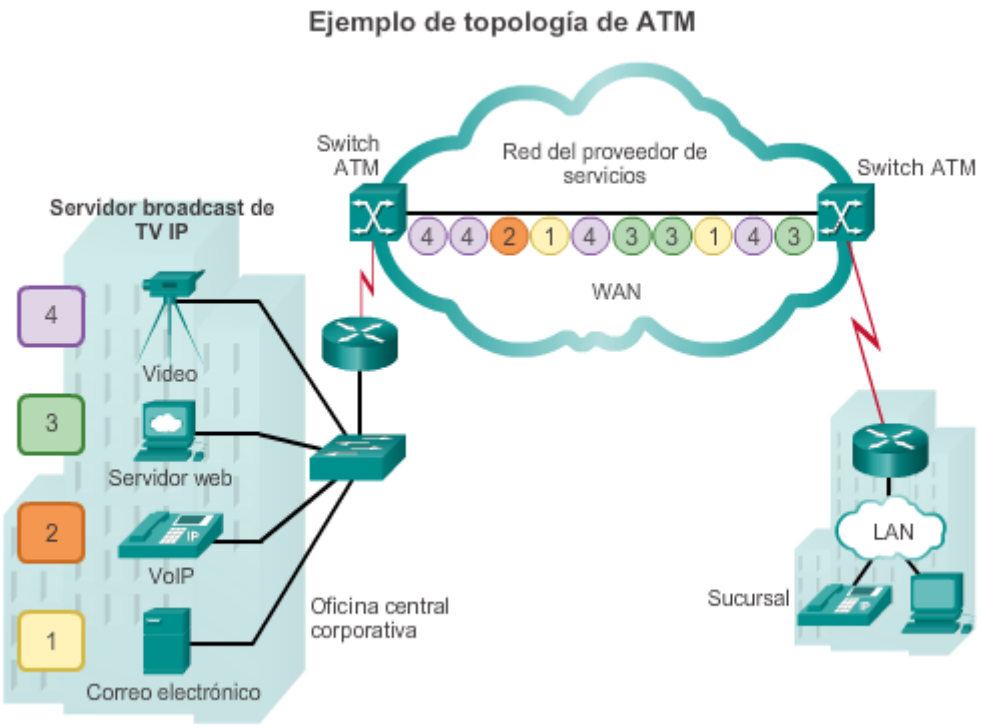
Capítulo 2: Conexión a la WAN 2.2.2.5 ATM

La tecnología del modo de transferencia asíncrona (ATM) puede transferir voz, video y datos a través de redes privadas y públicas. Se construye sobre una arquitectura basada en celdas, en vez de una arquitectura basada en 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 y de longitud fija son adecuadas para transportar tráfico de voz y video, debido a que este tipo de tráfico no admite retrasos. El tráfico de voz y video no tiene que esperar a que se transmitan paquetes de datos más grandes.

La celda ATM de 53 bytes es menos eficaz que las tramas y los paquetes más grandes de Frame Relay. Además, la celda ATM tiene por lo menos 5 bytes de sobrecarga por cada contenido de 48 bytes. Cuando la celda transporta los paquetes de capa de red segmentados, la sobrecarga es mayor debido a que el switch ATM debe poder rearmar los paquetes en el destino. Una línea ATM típica necesita casi un 20% más de ancho de banda que Frame Relay para transportar el mismo volumen de datos de capa de red.

ATM se diseñó para ser extremadamente escalable y para admitir las velocidades de enlace de T1/E1 a OC-12 (622 Mb/s) y más.

ATM ofrece PVC y SVC, si bien los PVC son más comunes con las WAN. Al igual que sucede con otras tecnologías de uso compartido, ATM permite varios VC en una única conexión de línea arrendada al perímetro de la red.



Capítulo 2: Conexión a la WAN 2.2.2.6 WAN Ethernet

Originalmente, Ethernet se desarrolló para que fuera una tecnología de acceso a LAN. Sin embargo, en aquel momento no era realmente adecuada como tecnología de acceso WAN, debido a que la longitud máxima admitida del cable era solo de hasta un kilómetro. No obstante, los estándares de Ethernet más recientes que utilizan cables de fibra óptica hicieron de Ethernet una opción de acceso WAN razonable. Por ejemplo, el estándar IEEE 1000BASE-LX admite longitudes de cable de fibra óptica de 5 km, mientras que el estándar IEEE 1000BASE-ZX admite longitudes de cable de hasta 70 km.

Ahora, los proveedores de servicios ofrecen el servicio WAN Ethernet con cableado de fibra óptica. El servicio WAN Ethernet se puede conocer con distintos nombres, incluidos Ethernet metropolitana (MetroE), Ethernet por MPLS (EoMPLS) y el servicio de LAN privada virtual (VPLS).

Los beneficios de WAN Ethernet incluyen lo siguiente:

- **Reducción de gastos y administración:** WAN Ethernet proporciona una red de conmutación de capa 2 con un ancho de banda elevado que es capaz de administrar datos, voz y video en la misma infraestructura. Esta característica aumenta el ancho de banda y elimina las conversiones costosas a otras tecnologías WAN. La tecnología permite que las empresas conecten varios sitios en un área metropolitana, entre sí y a Internet, en forma económica.

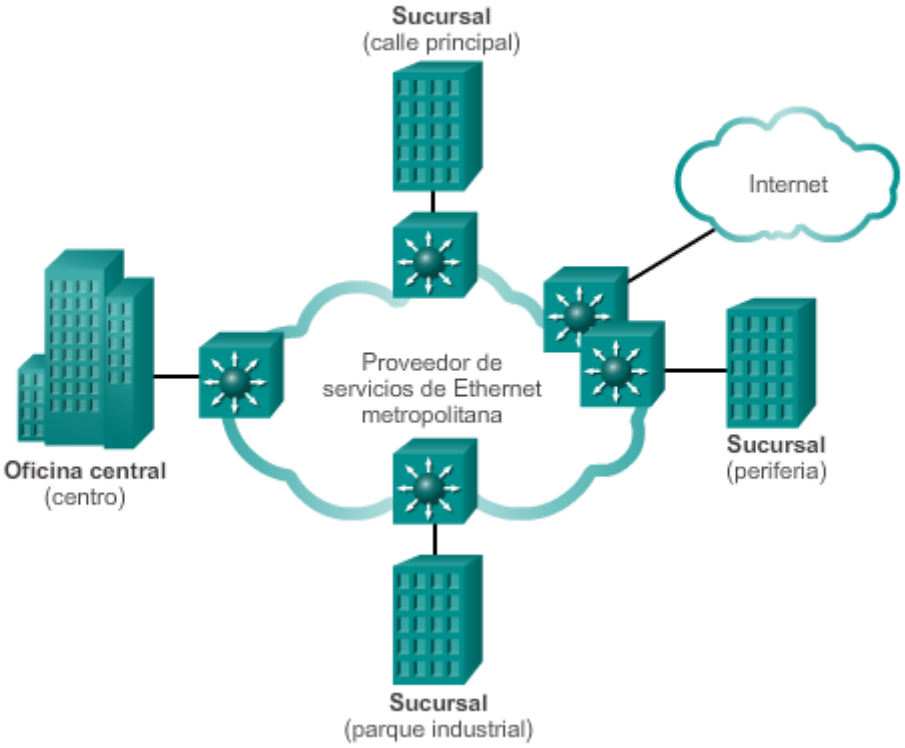
- **Fácil integración con las redes existentes:** WAN Ethernet se conecta fácilmente a las LAN Ethernet existentes, lo que reduce los costos y el tiempo de instalación.

- **Productividad mejorada de la empresa:** WAN Ethernet permite que las empresas aprovechen las aplicaciones IP para mejorar la productividad, como las comunicaciones

IP alojadas, VoIP y transmisión y difusión de video, que son difíciles de implementar en las redes TDM o Frame Relay.

Nota: las WAN Ethernet ganaron popularidad y ahora se usan comúnmente para reemplazar los tradicionales enlaces de Frame Relay y WAN ATM.

Ejemplo de topología de WAN Ethernet



Capítulo 2: Conexión a la WAN 2.2.2.7 MPLS

La conmutación de etiquetas multiprotocolo (MPLS) es una tecnología WAN multiprotocolo de alto rendimiento que dirige los datos de un router al siguiente según las etiquetas de ruta de acceso corta, en vez de las direcciones de red IP.

MPLS tiene varias características que la definen. Es multiprotocolo, lo que significa que tiene la capacidad de transportar cualquier contenido, incluido tráfico IPv4, IPv6, Ethernet, ATM, DSL y Frame Relay. Usa etiquetas que le señalan al router qué hacer con un paquete. Las etiquetas identifican las rutas entre routers distantes —en lugar de entre terminales—, y mientras MPLS enruta paquetes IPv4 e IPv6 efectivamente, todo lo demás se conmuta.

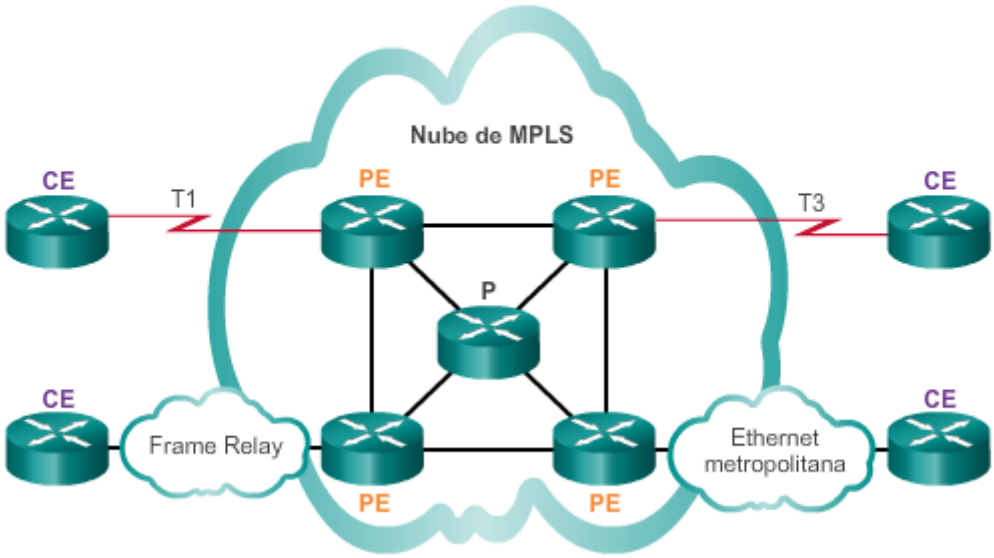
MPLS es una tecnología de proveedor de servicios. Las líneas arrendadas entregan bits entre sitios, y Frame Relay y WAN Ethernet entregan tramas entre los sitios. Sin embargo, MPLS puede entregar cualquier tipo de paquete entre sitios. MPLS puede encapsular paquetes de diversos protocolos de red. Admite una amplia variedad de tecnologías WAN, que incluyen los enlaces de portadoras T y E, Carrier Ethernet, ATM, Frame Relay y DSL.

En el ejemplo de topología de la ilustración, se muestra cómo se utiliza MPLS. Observe que los diferentes sitios se pueden conectar a la nube MPLS mediante diferentes tecnologías de

acceso. En la ilustración, CE hace referencia al perímetro del cliente, PE es el router perimetral del proveedor que agrega y quita etiquetas, y P es un router interno del proveedor que conmuta paquetes con etiquetas MPLS.

Nota: MPLS es principalmente una tecnología WAN de proveedor de servicios.

Ejemplo de topología de MPLS



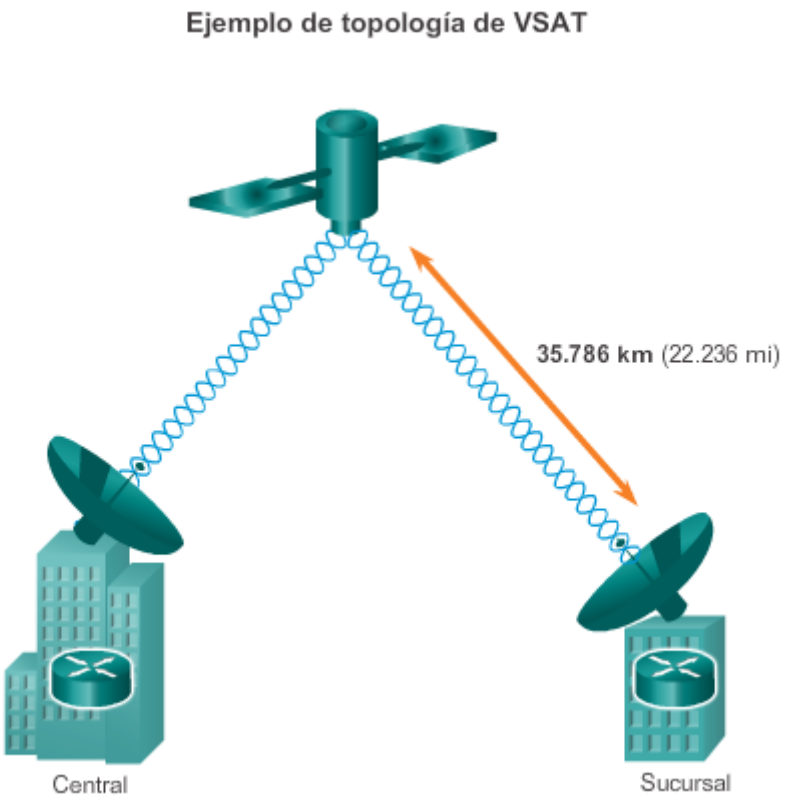
Capítulo 2: Conexión a la WAN 2.2.2.8 VSAT

En todas las tecnologías WAN privadas analizadas hasta ahora se usan medios de cobre o de fibra óptica. ¿Qué sucedería si una organización necesitara conectividad en una ubicación remota donde no hubiera proveedores de servicios que ofrecieran un servicio WAN?

Una terminal de apertura muy pequeña (VSAT) es una solución que crea una WAN privada mediante comunicaciones satelitales. Una VSAT es una pequeña antena parabólica similar a las que se usan para Internet y televisión en el hogar. Las VSAT crean una WAN privada a la vez que proporcionan conectividad a ubicaciones remotas.

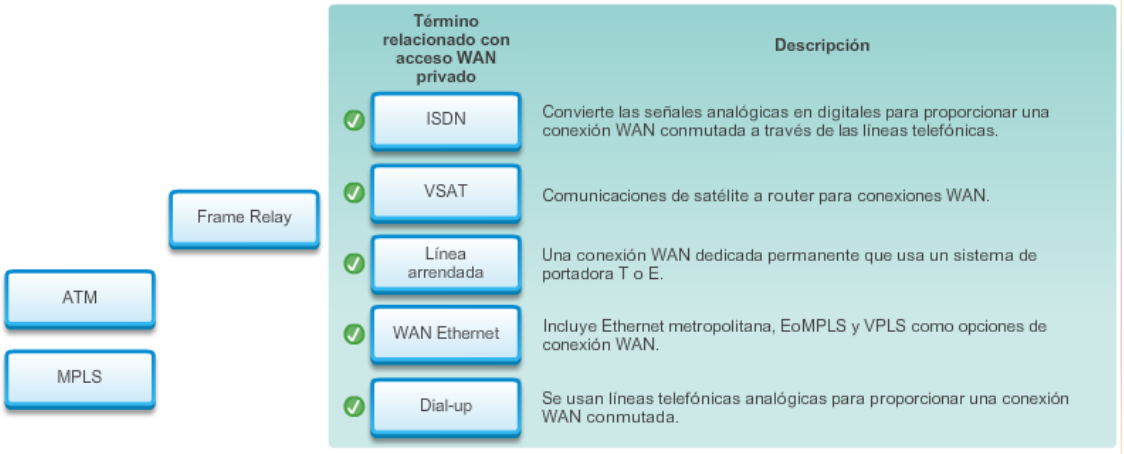
Específicamente, un router se conecta a una antena parabólica que apunta al satélite de un proveedor de servicios en una órbita geosincrónica en el espacio. Las señales deben recorrer alrededor de 35.786 km (22.236 mi) hasta el satélite y regresar.

En el ejemplo de la ilustración, se muestra una antena VSAT sobre los techos de los edificios, que se comunica con una antena parabólica a miles de kilómetros de distancia en el espacio.

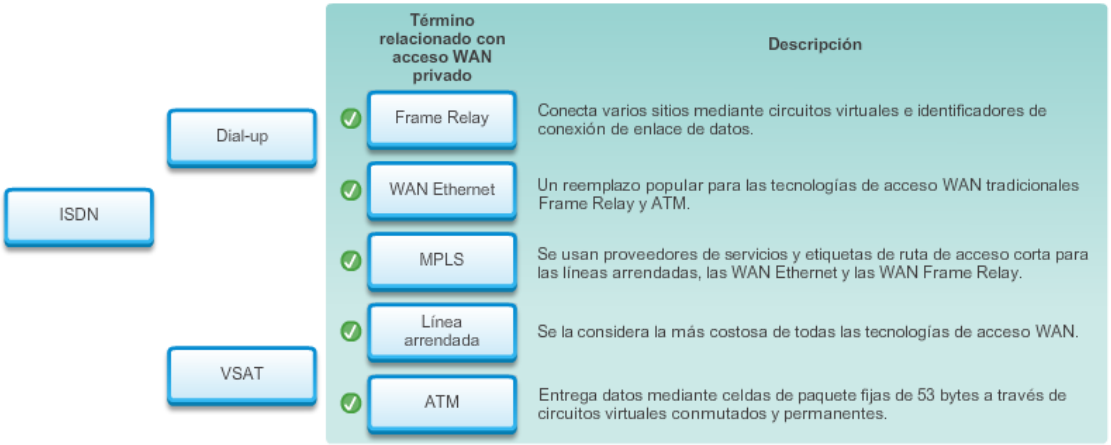


Capítulo 2: Conexión a la WAN 2.2.2.9 Actividad: Identificar la terminología de la infraestructura WAN privada

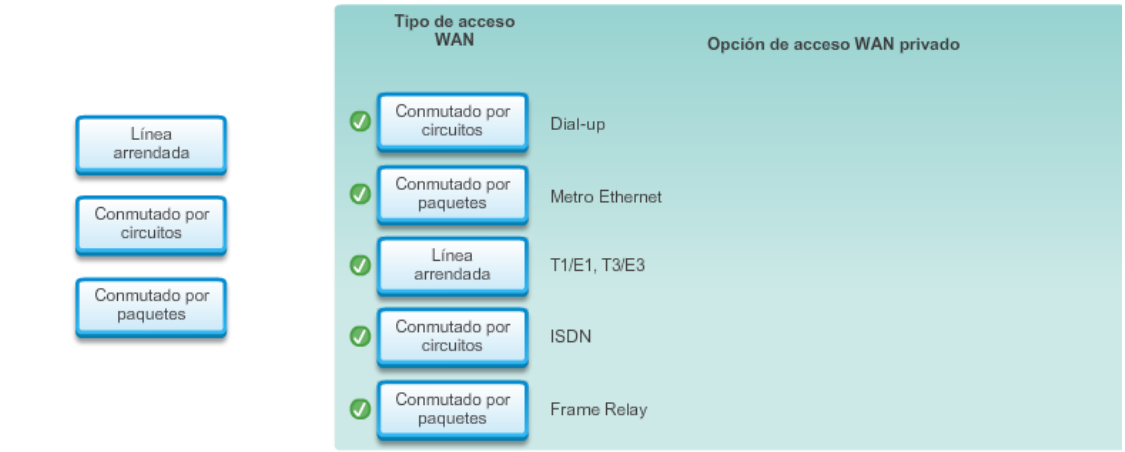
Actividad: Identificar las tecnologías de acceso WAN (parte 1)
Una cada término relacionado con acceso WAN privado con su descripción. No utilizará todas las opciones. Haga clic en el botón 2 para continuar la actividad.



Actividad: Identificar las tecnologías de acceso WAN (parte 2)
Una cada término relacionado con acceso WAN privado con su descripción. No utilizará todas las opciones. Haga clic en el botón 3 para continuar la actividad.



Actividad: Identificar las tecnologías de acceso WAN (parte 3)
Clasifique cada opción de acceso WAN privado según su tipo.



Capítulo 2: Conexión a la WAN 2.2.3.1 DSL

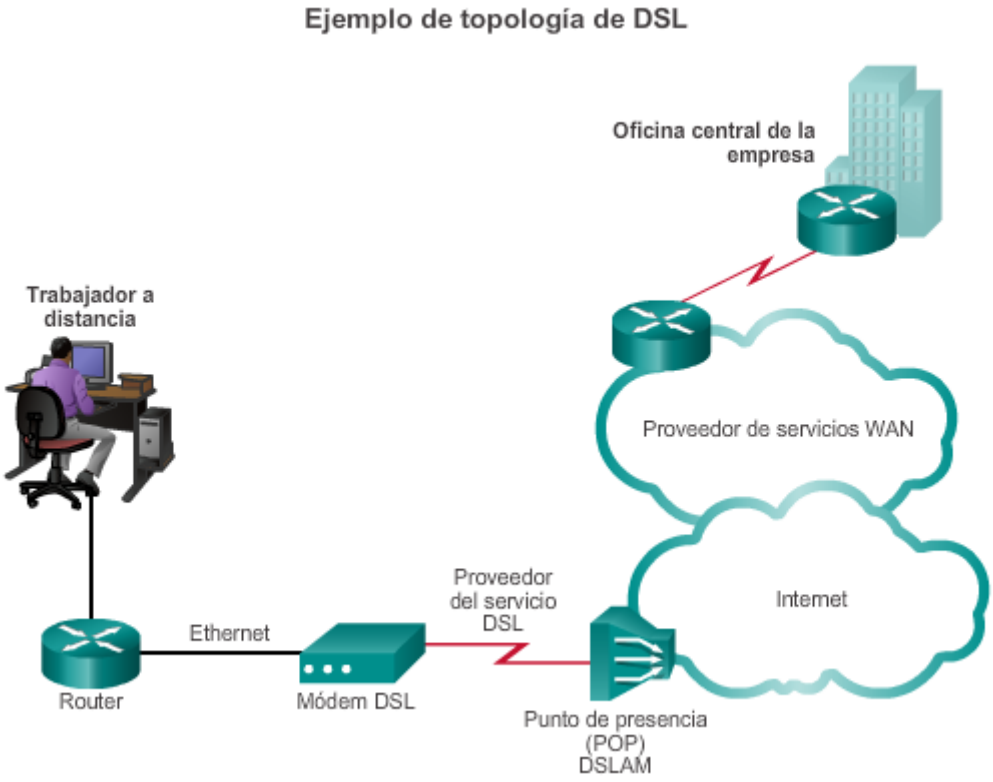
La tecnología DSL es una tecnología de conexión permanente que usa las líneas telefónicas de par trenzado existentes para transportar datos con un ancho de banda elevado y proporciona

servicios IP a los suscriptores. Un módem DSL convierte una señal de Ethernet del dispositivo de usuario en una señal DSL, que se transmite a la oficina central.

Varias líneas de suscriptor DSL se multiplexan en un único enlace de alta capacidad mediante un multiplexor de acceso DSL (DSLAM) en la ubicación del proveedor. Los DSLAM incorporan la tecnología TDM para la agregación de varias líneas de suscriptor en un único medio, generalmente una conexión T3 (DS3). Para lograr velocidades de datos rápidas, las tecnologías DSL actuales utilizan técnicas sofisticadas de codificación y modulación.

Existe una amplia variedad de tipos, estándares y estándares emergentes de DSL. En la actualidad, DSL es una opción popular para la provisión de soporte a los trabajadores en el hogar por parte de los departamentos de TI corporativos. Generalmente, un suscriptor no puede elegir conectarse a una red empresarial directamente, sino que primero se debe conectar a un ISP y, luego, se realiza una conexión IP a la empresa a través de Internet. Se generan riesgos de seguridad en este proceso, pero se pueden remediar con medidas de seguridad.

En la topología de la ilustración, se muestra un ejemplo de una conexión WAN DSL.



Capítulo 2: Conexión a la WAN 2.2.3.2 Cable

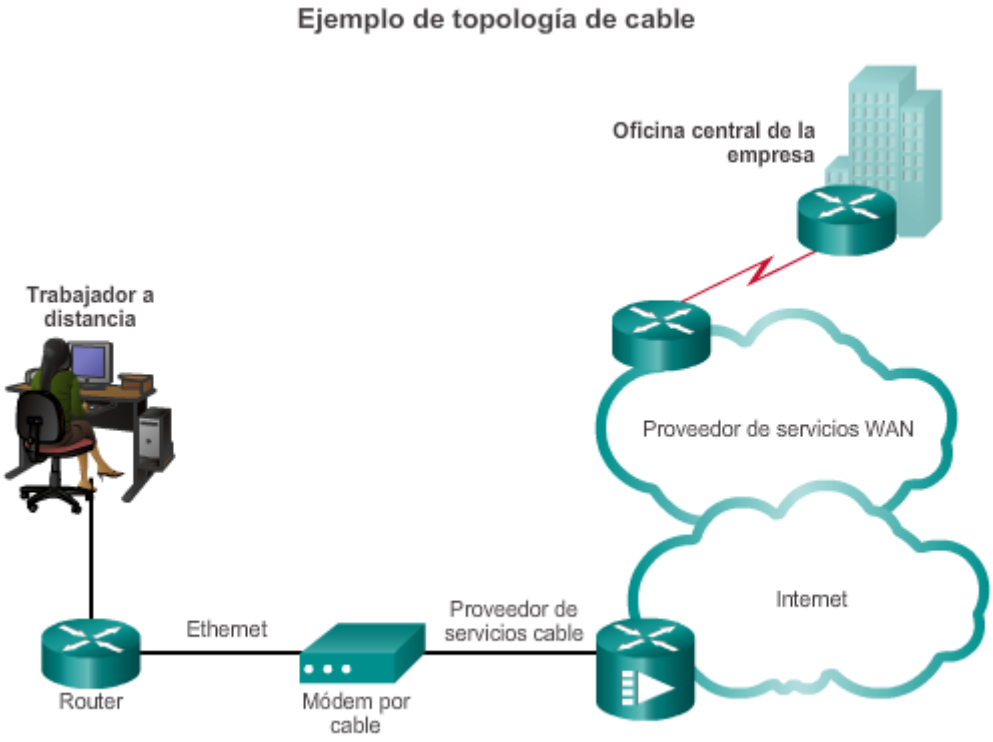
En áreas urbanas, para distribuir las señales de televisión se usa ampliamente el cable coaxial. Muchos proveedores de televisión por cable ofrecen acceso a la red. Esto permite un ancho de banda superior al del bucle local de telefonía convencional.

Los cable módems proporcionan una conexión permanente y tienen una instalación simple. Un suscriptor conecta una computadora o un router LAN al cable módem, que traduce las señales digitales por frecuencias de banda ancha que se usan para la transmisión en una red de

televisión por cable. La oficina local de televisión por cable, que se denomina “cabecera de cable”, contiene el sistema de computación y las bases de datos que se necesitan para proporcionar acceso a Internet. El componente más importante ubicado en la cabecera es el sistema de terminación de cable módem (CMTS), que envía y recibe señales digitales de cable módem en una red de cable y es necesario para proporcionar servicios de Internet a los suscriptores.

Los suscriptores de cable módem deben usar el ISP asociado con el proveedor de servicios. Todos los suscriptores locales comparten el mismo ancho de banda de cable. A medida que se unen más usuarios al servicio, es posible que el ancho de banda disponible esté por debajo de la velocidad esperada.

En la topología de la ilustración, se muestra un ejemplo de una conexión WAN por cable.



Capítulo 2: Conexión a la WAN 2.2.3.3 Inalámbrico

Para enviar y recibir datos, la tecnología inalámbrica usa el espectro de radio sin licencia. Cualquier persona que tenga un router inalámbrico y tecnología inalámbrica en el dispositivo que utilice puede acceder al espectro sin licencia.

Hasta hace poco tiempo, una limitación del acceso inalámbrico era la necesidad de estar dentro del alcance de transmisión local (normalmente, inferior a los 100 ft [30 m]) de un router inalámbrico o de un módem inalámbrico con una conexión por cable a Internet. Los siguientes avances en la tecnología inalámbrica de banda ancha están cambiando esta situación:

- **Wi-Fi municipal:** muchas ciudades comenzaron a instalar redes inalámbricas municipales. Algunas de estas redes proporcionan acceso a Internet de alta velocidad de manera gratuita o por un precio sustancialmente inferior al de otros servicios de banda

ancha. Otras son solo para uso de la administración de la ciudad y permiten que la policía, los bomberos y otros empleados municipales realicen ciertos aspectos de su trabajo de manera remota. Para conectarse a Wi-Fi municipal, por lo general un suscriptor necesita un módem inalámbrico, que proporciona una antena de radio y direccional más potentes que los adaptadores inalámbricos convencionales. La mayoría de los proveedores de servicios proporcionan los equipos necesarios de manera gratuita o por una tarifa, de manera similar a lo que sucede con los módems DSL o los cable módems.

- **WiMAX:** la interoperabilidad mundial para el acceso por microondas (WiMAX) es una tecnología nueva que acaba de comenzar a usarse. Se describe en el estándar IEEE 802.16. WiMAX proporciona un servicio de banda ancha de alta velocidad con acceso inalámbrico y proporciona una amplia cobertura como una red de telefonía celular, en vez de pequeñas zonas de cobertura inalámbrica Wi-Fi. WiMAX funciona de manera similar a Wi-Fi, pero con velocidades más altas, a través de distancias mayores y para una mayor cantidad de usuarios. Usa una red de torres WiMAX que son similares a las torres de telefonía celular. Para acceder a una red WiMAX, los suscriptores se deben suscribir a un ISP con una torre WiMAX a menos de 30 mi (48 km) de su ubicación. Para tener acceso a la estación base, también necesitan algún tipo de receptor WiMAX y un código de cifrado especial.

- **Internet satelital:** generalmente utilizado por usuarios en áreas rurales, donde no hay cable ni DSL. Una VSAT proporciona comunicaciones de datos bidireccionales (subida y descarga). La velocidad de subida es aproximadamente un décimo de la velocidad de descarga de 500 kb/s. Cable y DSL tienen velocidades de descarga mayores, pero los sistemas satelitales son unas diez veces más rápidos que un módem analógico. Para acceder a los servicios de Internet satelital, los suscriptores necesitan una antena parabólica, dos módems (uplink y downlink) y cables coaxiales entre la antena y el módem.

En la ilustración, se muestra un ejemplo de una red WiMAX.

Capítulo 2: Conexión a la WAN 2.2.3.4 Datos móviles 3G/4G

Cada vez más, el servicio celular es otra tecnología WAN inalámbrica que se usa para conectar usuarios y ubicaciones remotas donde no hay otra tecnología de acceso WAN disponible. Muchos usuarios con smartphones y tablet PC pueden usar los datos móviles para enviar correos electrónicos, navegar la Web, descargar aplicaciones y mirar videos.

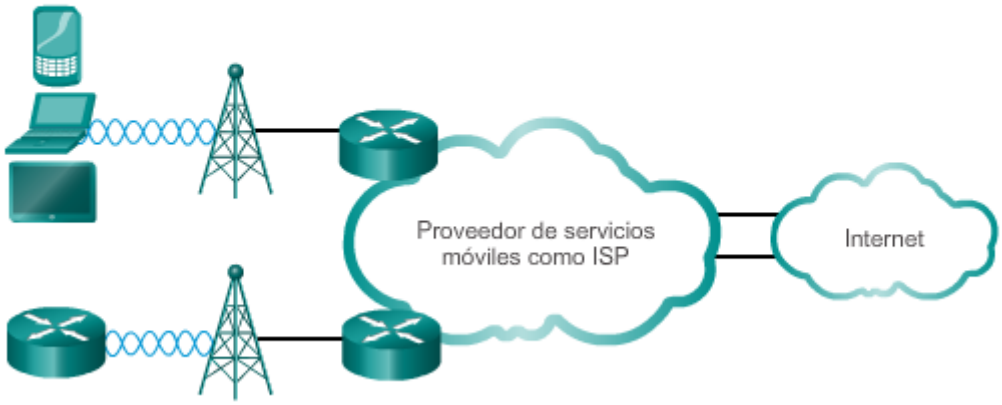
Los teléfonos, las tablet PC, las computadoras portátiles e incluso algunos routers se pueden comunicar a través de Internet mediante la tecnología de datos móviles. Estos dispositivos usan ondas de radio para comunicarse por medio de una torre de telefonía móvil. El dispositivo tiene una pequeña antena de radio, y el proveedor tiene una antena mucho más grande que se ubica en la parte superior de una torre en algún lugar a una distancia determinada del teléfono.

Algunos términos comunes de la industria de datos móviles incluyen los siguientes:

- **3G/4G inalámbrico:** abreviatura para el acceso celular de tercera y cuarta generación. Estas tecnologías admiten acceso inalámbrico a Internet.

- **Evolución a largo plazo (LTE):** hace referencia a una tecnología más reciente y más rápida, que se considera parte de la tecnología de cuarta generación (4G).

Topología inalámbrica de ejemplo



Capítulo 2: Conexión a la WAN 2.2.3.5 Tecnología VPN

Cuando un trabajador a distancia o un trabajador en una oficina remota utilizan servicios de banda ancha para acceder a la WAN corporativa a través de Internet, se generan riesgos de seguridad. Para abordar las cuestiones de seguridad, los servicios de banda ancha proporcionan capacidades para usar conexiones VPN a un servidor VPN, que por lo general se encuentra en el sitio corporativo.

Una VPN es una conexión cifrada entre redes privadas a través de una red pública, como Internet. En vez de usar una conexión dedicada de capa 2, como una línea arrendada, una VPN usa conexiones virtuales llamadas “túneles VPN”, que se enrutan a través de Internet desde la red privada de la empresa hasta el host del sitio o del empleado remoto.

Los beneficios de VPN incluyen lo siguiente:

- **Ahorro de costos:** las VPN permiten que las organizaciones usen Internet global para conectar oficinas y usuarios remotos al sitio corporativo principal, lo que elimina la necesidad de enlaces WAN dedicados y bancos de módems costosos.

- **Seguridad:** las VPN proporcionan el nivel máximo de seguridad mediante dos protocolos avanzados de cifrado y autenticación que protegen los datos del acceso no autorizado.

- **Escalabilidad:** debido a que las VPN usan la infraestructura de Internet en los ISP y los dispositivos, es fácil agregar nuevos usuarios. Las empresas pueden incrementar ampliamente la capacidad, sin agregar una infraestructura significativa.

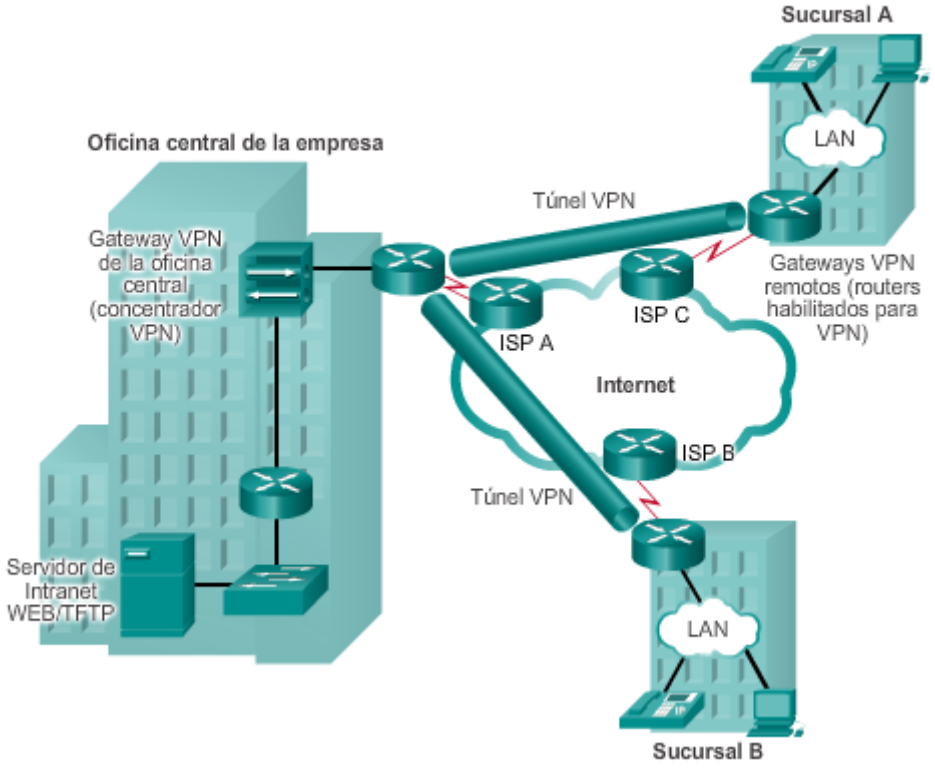
- **Compatibilidad con la tecnología de banda ancha:** los proveedores de servicios de banda ancha, como DSL y cable, admiten la tecnología VPN, de modo que los trabajadores móviles y los empleados a distancia pueden aprovechar el servicio de Internet de alta velocidad de sus hogares para acceder a las redes corporativas. Las conexiones de banda ancha de alta velocidad para uso empresarial también pueden proporcionar una solución rentable para la conexión de oficinas remotas.

Existen dos tipos de acceso a VPN:

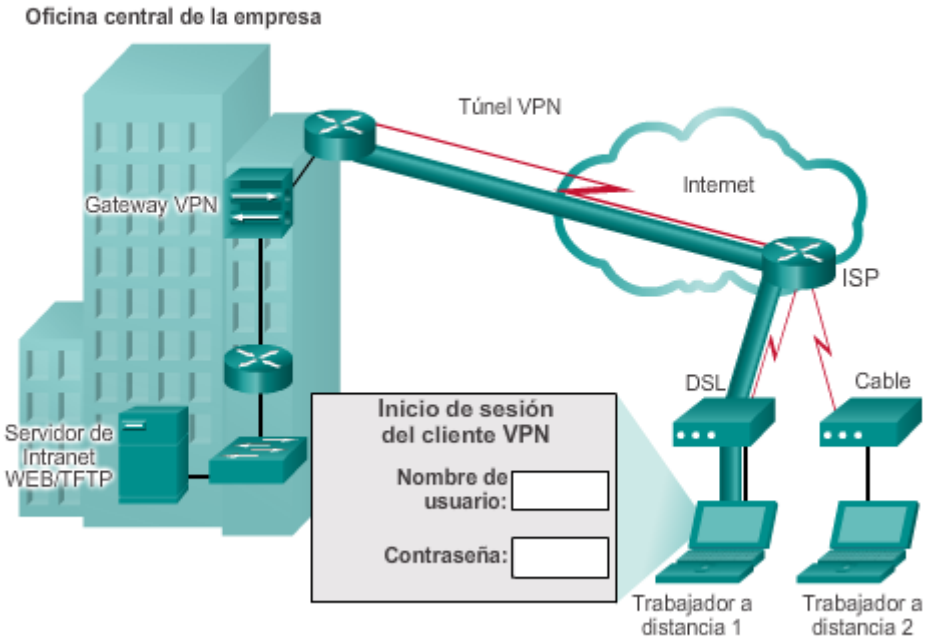
- **VPN de sitio a sitio:** las VPN de sitio a sitio conectan redes enteras entre sí; por ejemplo, pueden conectar la red de una sucursal a la red de la oficina central de la empresa, como se muestra en la figura 1. Cada sitio cuenta con un gateway VPN, como un router, un firewall, un concentrador VPN o un dispositivo de seguridad. En la ilustración, una sucursal remota utiliza una VPN de sitio a sitio para conectarse a la oficina central de la empresa.

- **VPN de acceso remoto:** las VPN de acceso remoto permiten que los hosts individuales, como los empleados a distancia, los usuarios móviles y los consumidores de extranets, accedan a la red de una empresa de manera segura a través de Internet. Por lo general, cada host (trabajador a distancia 1 y trabajador a distancia 2) tiene cargado un software de cliente VPN o usa un cliente basado en Web, como se muestra en la figura 2.

Ejemplo de topología de VPN de sitio a sitio

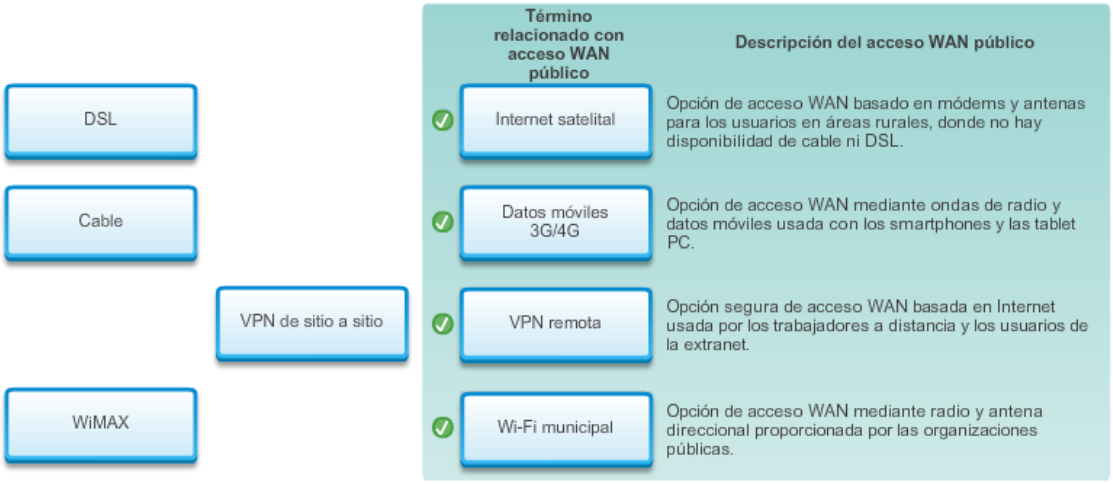


Ejemplo de topología de VPN de acceso remoto

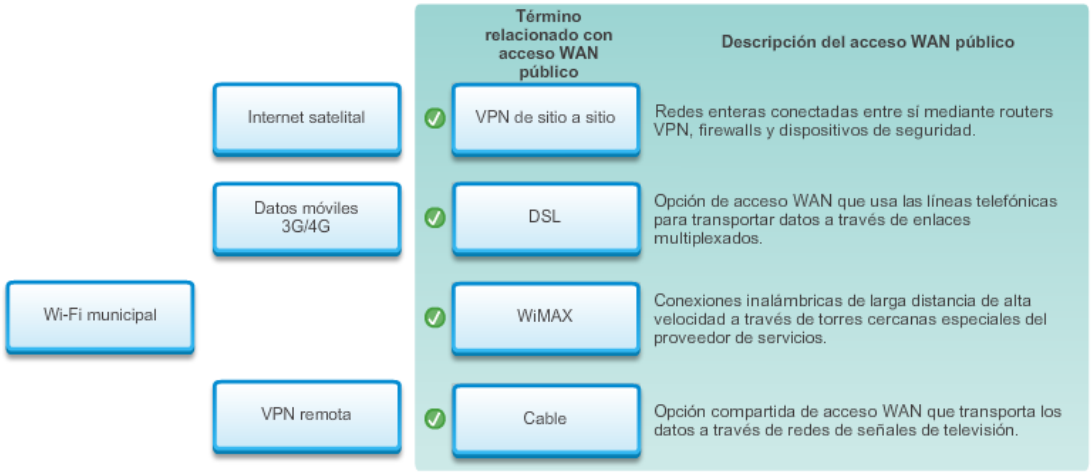


Capítulo 2: Conexión a la WAN 2.2.3.6 Actividad: Identificar la terminología de la infraestructura WAN pública

Actividad: Identificar la terminología de la infraestructura WAN pública (parte 1)
Una cada término relacionado con acceso WAN público con su descripción. Haga clic en el botón 2 para continuar la actividad.



Actividad: Identificar la terminología de la infraestructura WAN pública (parte 2)
Una cada término relacionado con acceso WAN público con su descripción.



Capítulo 2: Conexión a la WAN 2.2.4.1 Elección de una conexión de enlace WAN

Al elegir la conexión WAN apropiada, se deben tener en cuenta varios factores importantes. Para que un administrador de red decida cuál es la tecnología WAN que mejor cumple con los requisitos de una empresa específica, debe responder las siguientes preguntas:

¿Cuál es el propósito de la WAN?

Se debe tener en cuenta lo siguiente:

- ¿La empresa conectará sucursales locales en la misma área urbana, conectará sucursales remotas o realizará una conexión a una única sucursal?

- ¿Se usará la WAN para conectar a los empleados internos, los socios comerciales externos, los clientes o los tres grupos?

- ¿La empresa se conectará a los clientes, a los socios comerciales, a los empleados o a alguna combinación de los tres?

- ¿La WAN proporcionará a los usuarios autorizados un acceso limitado o total a la intranet de la empresa?

¿Cuál es el alcance geográfico?

Se debe tener en cuenta lo siguiente:

- ¿Es la WAN local, regional o global?

- ¿La WAN es de una sucursal a una sucursal, de una sucursal a varias sucursales o de varias sucursales a varias sucursales (distribuida)?

¿Cuáles son los requisitos de tráfico?

Se debe tener en cuenta lo siguiente:

- ¿Cuál es el tipo de tráfico que se debe admitir (solo datos, VoIP, video, archivos grandes, archivos de transmisión)? Esto determina los requisitos de calidad y rendimiento.

- ¿Cuál es el volumen por tipo de tráfico (voz, video o datos) que se debe admitir para cada destino? Esto determina la capacidad de ancho de banda que se necesita para la conexión WAN al ISP.

- ¿Cuál es la calidad de servicio que se requiere? Esto puede limitar las opciones. Si el tráfico es muy sensible a la latencia y a la vibración, elimine todas las opciones de conexión WAN que no pueden proporcionar la calidad requerida.

- ¿Cuáles son los requisitos de seguridad (integridad de datos, confidencialidad y seguridad)? Estos son factores importantes si el tráfico es de una naturaleza muy confidencial o si proporciona servicios esenciales, como respuesta de emergencia.

Capítulo 2: Conexión a la WAN 2.2.4.2 Elección de una conexión de enlace WAN (cont.)

Además de reunir información sobre el ámbito de la WAN, el administrador también debe determinar lo siguiente:

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

- **Para una WAN privada, ¿la conexión debe ser dedicada o de conmutación?** Las transacciones de gran volumen en tiempo real tienen requisitos especiales que podrían inclinar la elección por una línea dedicada, como el flujo de tráfico entre el centro de datos y la oficina central de la empresa. Si la empresa se conecta a una única sucursal local, se podría usar una línea arrendada dedicada. Sin embargo, esa opción se volvería muy costosa para una WAN que conecte varias oficinas. En ese caso, podría ser mejor una conexión de conmutación.

- **Para una WAN pública, ¿qué tipo de acceso a VPN se requiere?** Si el propósito de la WAN es conectar una oficina remota, una VPN de sitio a sitio puede ser la mejor opción. Para conectar a los trabajadores a distancia o a los clientes, las VPN de acceso remoto son una mejor opción. Si la WAN brinda servicio a una combinación de oficinas remotas, trabajadores a distancia y clientes autorizados, como en el caso de una empresa global con operaciones distribuidas, es posible que sea necesaria una combinación de opciones de VPN.

- **¿Qué opciones de conexión están disponibles en el ámbito?** En ciertas áreas, no todas las opciones de conexión WAN están disponibles. En este caso, se simplifica el proceso de selección, si bien la WAN resultante puede proporcionar un rendimiento inferior al óptimo. Por ejemplo, en un área rural o remota, es posible que la única opción sea VSAT o acceso celular.

- **¿Cuál es el costo de las opciones de conexión disponibles?** Según la opción elegida, la WAN puede implicar un gasto continuo significativo. Se debe analizar el costo de una opción particular según cuán bien cumpla esta con los otros requisitos. Por ejemplo, una línea arrendada dedicada es la opción más costosa, pero el gasto puede estar justificado si es fundamental proteger la transmisión de grandes volúmenes de datos en tiempo real. Para aplicaciones menos exigentes, puede ser más conveniente una opción de conmutación o de conexión a Internet menos costosa.

Según las pautas descritas anteriormente, así como las que se describen en la arquitectura empresarial de Cisco, un administrador de red debe poder elegir una conexión WAN adecuada para satisfacer los requisitos de diversas situaciones empresariales.

Capítulo 2: Conexión a la WAN 2.2.4.3 Práctica de laboratorio: Investigación de las tecnologías WAN

En esta práctica de laboratorio, cumplirá los siguientes objetivos:

- Parte 1: Investigar las tecnologías WAN dedicadas y sus proveedores

- Parte 2: Investigar un proveedor de servicios de línea arrendada dedicada en su área

Práctica de laboratorio: Investigación de las tecnologías WAN

Capítulo 2: Conexión a la WAN 2.3.1.1 Actividad de clase: Módulos de dispositivos WAN

Módulos de dispositivos WAN

En su empresa mediana, están actualizando la red. Para aprovechar al máximo el equipo que se usa actualmente, decide adquirir módulos WAN en lugar de equipos nuevos.

En todas las sucursales se utilizan ISR Cisco de las series 1900 o 2911. Actualizará estos routers en varias ubicaciones. Cada sucursal tiene sus propios requisitos de ISP para tener en cuenta.

Para actualizar los dispositivos, enfóquese en los siguientes tipos de acceso de los módulos WAN:

- Ethernet
- Banda ancha
- T1/E1 e ISDN PRI
- BRI
- Serial
- Voz y WAN de enlaces troncales T1 y E1
- LAN y WAN inalámbricas

Actividad de clase: Módulos de dispositivos WAN

Capítulo 2: Conexión a la WAN 2.3.1.2 Resumen

Una empresa puede usar las líneas privadas o la infraestructura de red pública para conexiones WAN. Una conexión de infraestructura pública puede ser una alternativa rentable para una conexión privada entre LAN, siempre que también se incluya la seguridad en la planificación.

Los estándares de acceso WAN funcionan en las capas 1 y 2 del modelo OSI, y la definición y administración de dichos estándares están a cargo de la TIA/EIA, la ISO y el IEEE. Una WAN puede ser de conmutación de circuitos o de conmutación de paquetes.

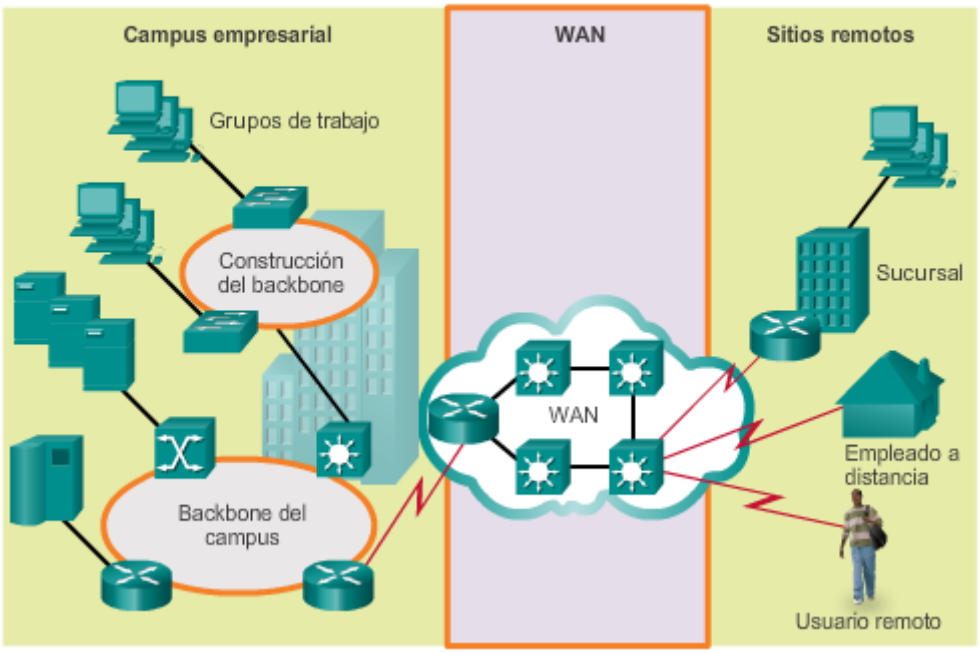
Existe terminología común que se usa para identificar los componentes físicos de las conexiones WAN y quién es responsable de qué componentes (el proveedor de servicios o el cliente).

Las redes del proveedor de servicios son complejas, y las redes troncales del proveedor de servicios constan principalmente de medios de fibra óptica de ancho de banda elevado. El dispositivo usado para la interconexión a un cliente es específico de la tecnología WAN que se implemente.

El uso de líneas arrendadas proporciona conexiones punto a punto dedicadas permanentes. El acceso por dial-up, si bien es lento, aún es viable para las áreas remotas con opciones de WAN limitadas. Otras opciones de conexión privada incluyen ISDN, Frame Relay, ATM, WAN Ethernet, MPLS y VSAT.

Las conexiones de infraestructura pública incluyen DSL, cable, tecnología inalámbrica y datos móviles 3G/4G. En las conexiones mediante infraestructura pública, se puede proporcionar seguridad con redes virtuales privadas (VPN) de acceso remoto o de sitio a sitio.

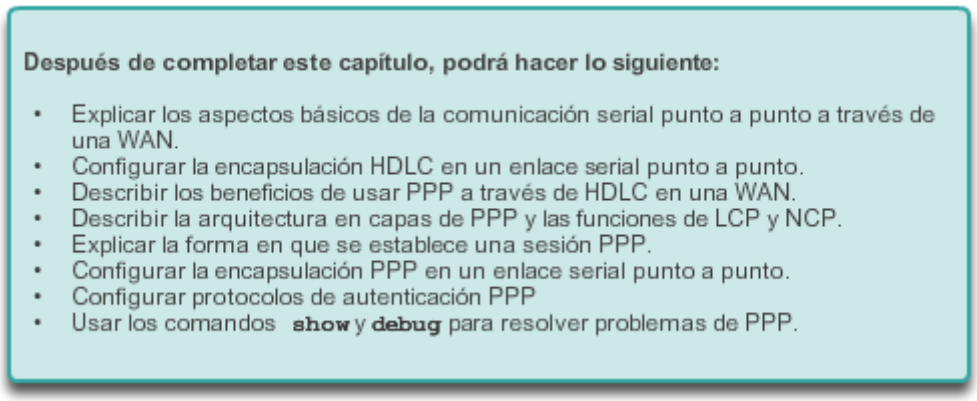
Las WAN interconectan usuarios y redes LAN



Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.0.1.1 Introducción

Uno de los tipos de conexiones WAN más comunes, especialmente en las comunicaciones de larga distancia, son las conexiones punto a punto, que también se denominan “conexiones seriales” o “de líneas arrendadas“. Debido a que, en general, estas conexiones las proporciona una empresa prestadora de servicios, como una compañía telefónica, los límites entre lo que administra la prestadora y lo que administra el cliente se deben establecer con claridad.

En este capítulo, se abarcan los términos, la tecnología y los protocolos que se utilizan en las conexiones seriales. Se presentan los protocolos punto a punto (PPP) y HDLC. PPP es un protocolo capaz de manejar la autenticación, la compresión y la detección de errores, de controlar la calidad de los enlaces, y de agrupar lógicamente varias conexiones seriales para compartir la carga.



Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.0.1.2 Actividad de clase: Persuasión de PPP

Persuasión para el uso de PPP

Su supervisor de ingeniería de red asistió recientemente a una conferencia sobre tecnología de redes en la que se abordaron los protocolos de capa 2. Él sabe que usted cuenta con equipos de Cisco en las instalaciones, pero también quiere ofrecerle seguridad y opciones y controles avanzados de TCP/IP en esos mismos equipos mediante el protocolo punto a punto (PPP).

Después de investigar el protocolo PPP, descubre que este ofrece algunas ventajas que el protocolo HDLC, que se utiliza actualmente en la red, no ofrece.

Cree una matriz donde se incluyan las ventajas y desventajas de utilizar el protocolo HDLC en comparación con el protocolo PPP. Cuando compare los dos protocolos, incluya lo siguiente:

- Facilidad de configuración
- Adaptabilidad a equipos de red no exclusivos
- Opciones de seguridad
- Uso y compresión del ancho de banda
- Consolidación del ancho de banda

Comparta el gráfico con otro estudiante o con la clase. Explique si sugeriría, o no, mostrarle la matriz al supervisor de ingeniería de red para justificar la implementación de un cambio de HDLC a PPP para la conectividad de red de capa 2.

Actividad de clase: Persuasión de PPP

Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.1.1.1 Puertos serie y paralelos

Uno de los tipos de conexiones WAN más comunes es la conexión punto a punto. Como se muestra en la figura 1, las conexiones punto a punto se utilizan para conectar redes LAN a redes WAN de un proveedor de servicios, así como para conectar segmentos LAN dentro de una red empresarial.

Una conexión punto a punto de LAN a WAN también se denomina “conexión serial” o “conexión de línea arrendada”. Esto se debe a que las líneas se arriendan de una prestadora de servicios (generalmente, una compañía telefónica) y se las dedica para que las utilice la empresa que arrienda las líneas. Las empresas pagan una conexión continua entre dos sitios remotos, y la línea está continuamente activa y disponible. Las líneas arrendadas son un tipo de acceso WAN que se usa con frecuencia y, generalmente, el precio se basa en el ancho de banda requerido y en la distancia entre los dos puntos conectados.

Es importante comprender cómo funciona la comunicación serial punto a punto a través de una línea arrendada para tener un concepto general de cómo funcionan las WAN.

Las comunicaciones a través de una conexión serial son un método de transmisión de datos en el que los bits se transmiten en forma secuencial por un único canal. Esto equivale a una tubería con un ancho suficiente para que pase de a una pelota por vez. Pueden entrar varias pelotas en la tubería, pero de a una sola, y solo tienen un punto de salida (el otro extremo de la tubería). Los puertos serie son bidireccionales y a menudo se los denomina “puertos bidireccionales” o “puertos de comunicaciones”.

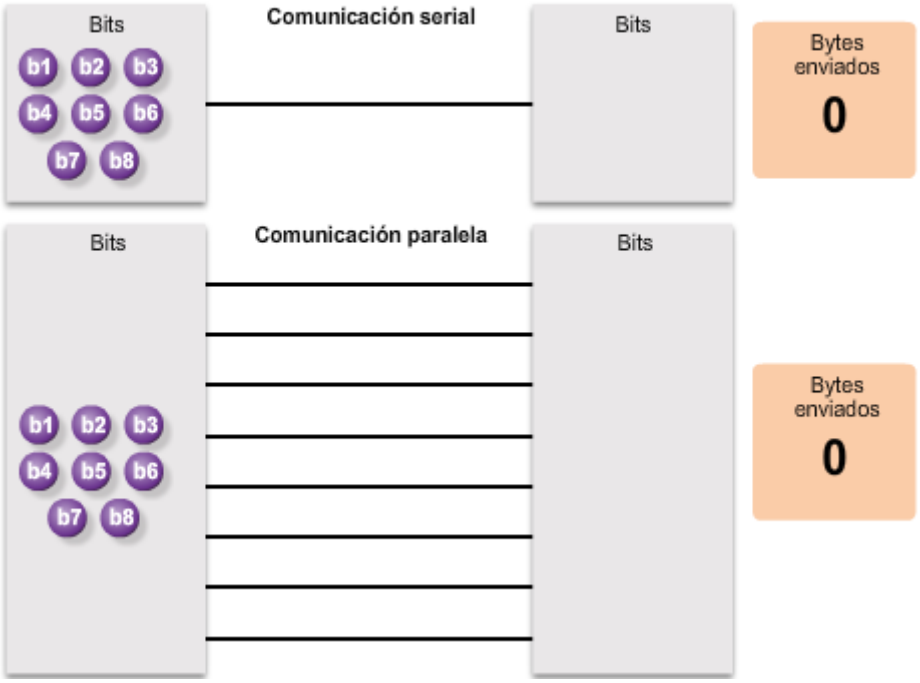
Esto es distinto de las comunicaciones paralelas, en las que los bits se pueden transmitir simultáneamente por varios cables. Como se muestra en la figura 2, en teoría, una conexión paralela transfiere datos ocho veces más rápido que una conexión serial. De acuerdo con esta teoría, una conexión paralela envía 1 byte (8 bits) en el tiempo en que una conexión serial envía un único bit. Sin embargo, las comunicaciones paralelas tienen problemas con el crosstalk a través de los cables, especialmente a medida que la longitud de estos aumenta. El sesgo de reloj también es un problema con las comunicaciones paralelas. El sesgo de reloj ocurre cuando los datos no llegan al mismo tiempo a través de los diferentes cables, lo que crea problemas de sincronización. Por último, la mayoría de las comunicaciones paralelas solo admiten un único sentido: la comunicación saliente del disco duro.

En una época, la mayoría de las computadoras incluían puertos serie y paralelos. Los puertos paralelos se utilizaban para conectar impresoras, computadoras y otros dispositivos que requerían un ancho de banda relativamente alto. Los puertos paralelos también se utilizaban entre los componentes internos. Para las comunicaciones externas, los buses serie se utilizaban principalmente para la conversión de señales. Debido a su capacidad bidireccional, la implementación de las comunicaciones seriales es mucho menos costosa. Las comunicaciones seriales usan menos hilos, cables más económicos y menos pines de los conectores.

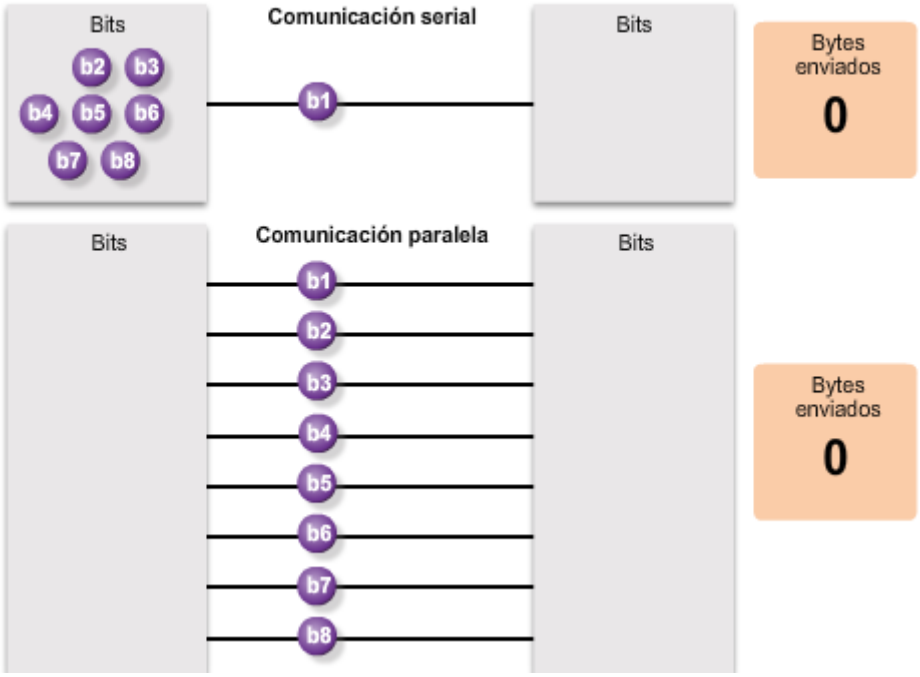
En la mayoría de las computadoras, los puertos paralelos y los puertos serie RS-232 se reemplazaron por las interfaces de bus serial universal (USB), de mayor velocidad. Sin embargo, para las comunicaciones de larga distancia, muchas WAN siguen utilizando la transmisión serial.

Conexión serial punto a punto

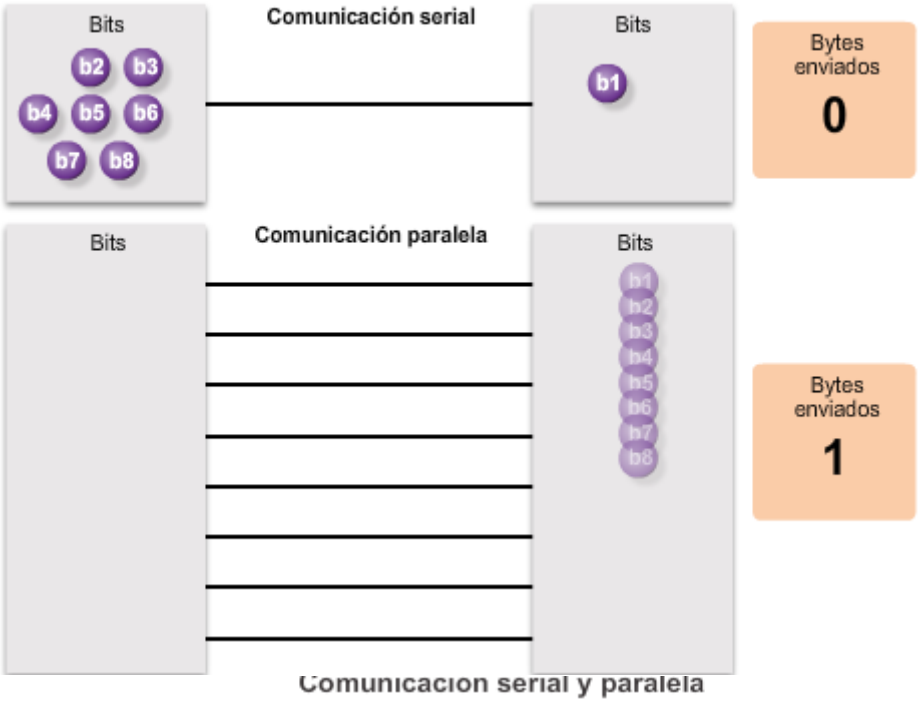
Comunicación serial y paralela



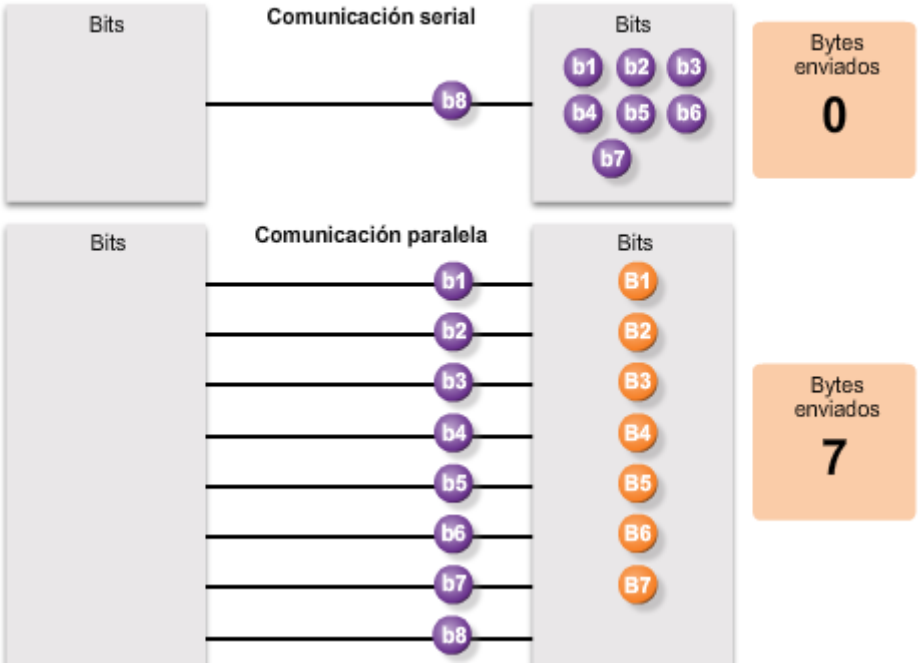
Comunicación serial y paralela

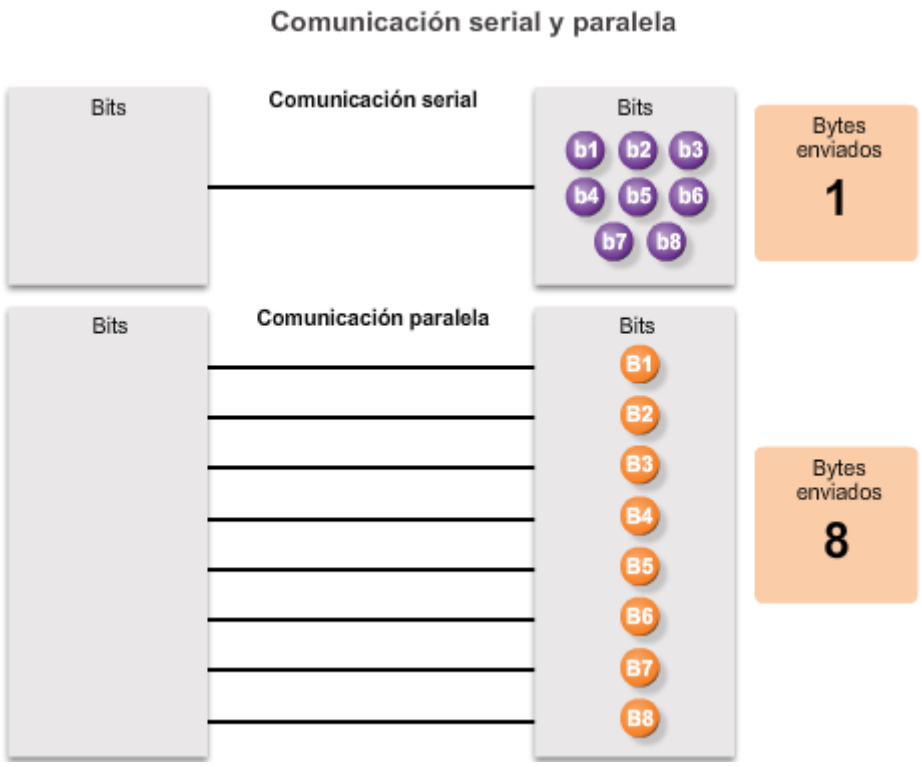


Comunicación serial y paralela



Comunicación serial y paralela





Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.1.1.2 Comunicación serial

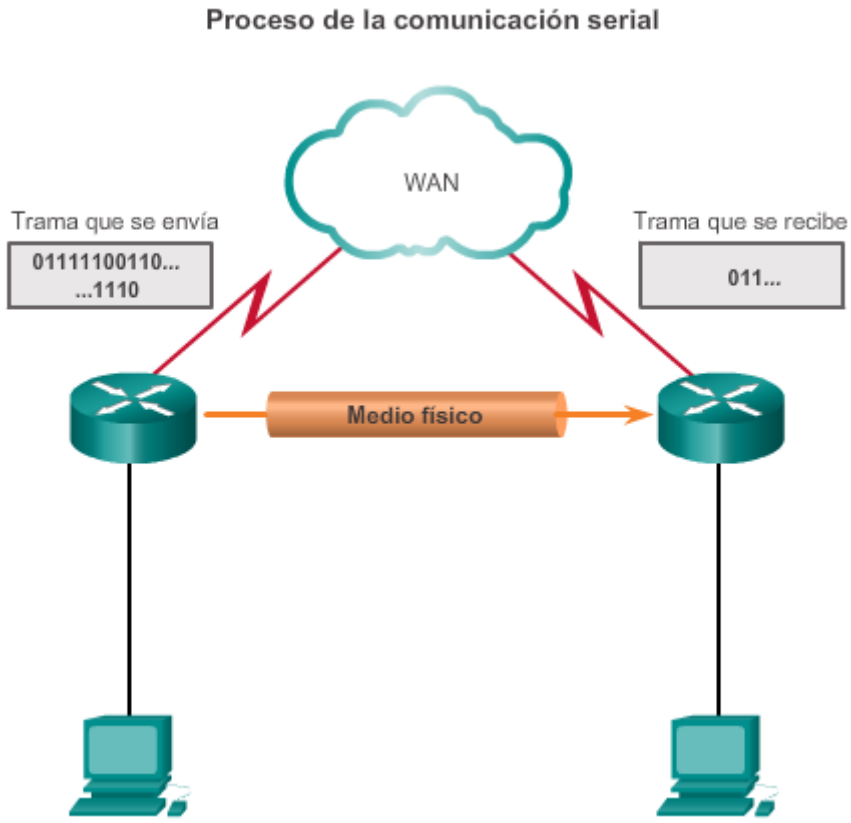
En la ilustración, se muestra una representación simple de una comunicación serial a través de una WAN. El protocolo de comunicaciones que usa el router emisor encapsula los datos. La trama encapsulada se envía a la WAN por un medio físico. Existen varias formas de atravesar la WAN, pero el router receptor usa el mismo protocolo de comunicaciones para desencapsular la trama cuando esta llega.

Existen diferentes estándares de comunicación serial, y cada una usa un método de señalización diferente. Existen tres estándares importantes de comunicación serial que afectan las conexiones de LAN a WAN:

- **RS-232:** la mayoría de los puertos serie en las computadoras personales cumplen con el estándar RS-232C o los estándares RS-422 y RS-423 más recientes. Se utilizan conectores tanto de 9 pines como de 25 pines. Un puerto serie es una interfaz de uso general que se puede utilizar para casi cualquier tipo de dispositivo, incluidos los módems, los mouses y las impresoras. Los nuevos estándares más rápidos como USB reemplazaron a estos tipos de dispositivos periféricos para las computadoras, pero muchos dispositivos de red utilizan conectores RJ-45 que cumplen con el estándar RS-232 original.

- **V.35:** este estándar de la ITU para el intercambio de datos síncrono de alta velocidad combina el ancho de banda de varios circuitos telefónicos y, en general, se usa para la comunicación de módem a multiplexor. En los EE. UU., el estándar de interfaz V.35 es el que utiliza la mayoría de los routers y las DSU que se conectan a las portadoras T1. Los cables V.35 son conjuntos seriales de alta velocidad diseñados para admitir una conectividad y velocidades de datos superiores entre los DTE y los DCE a través de líneas digitales. Se proporcionan más detalles sobre los DTE y los DCE más adelante en esta sección.

- **Interfaz serial de alta velocidad (HSSI):** una HSSI admite velocidades de transmisión de hasta 52 Mb/s. Los ingenieros usan HSSI para conectar los routers en las LAN a las WAN a través de líneas de alta velocidad, como las líneas T3. Además, los ingenieros usan HSSI para proporcionar conectividad de alta velocidad entre redes LAN mediante Token Ring o Ethernet. HSSI es una interfaz DTE/DCE desarrollada por Cisco Systems y T3 plus Networking para satisfacer la necesidad de comunicación de alta velocidad a través de enlaces WAN.



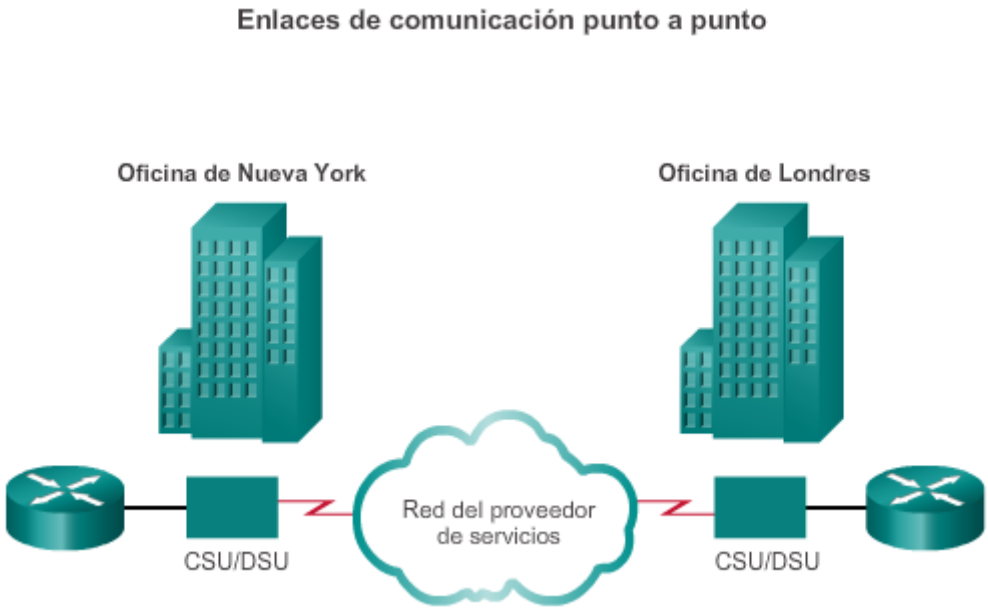
Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.1.1.3 Enlaces de comunicación punto a punto

Cuando se requieren conexiones dedicadas permanentes, se utiliza un enlace punto a punto para proporcionar una única ruta de comunicaciones WAN preestablecida desde las instalaciones del cliente hasta un destino remoto a través de la red del proveedor, como se muestra en la ilustración.

Un enlace punto a punto puede conectar dos sitios geográficamente distantes, como una oficina corporativa en Nueva York y una oficina regional en Londres. Para una línea punto a punto, la portadora dedica recursos específicos a una línea que arrienda el cliente (línea arrendada).

Nota: las conexiones punto a punto no se limitan a las conexiones por tierra. Existen cientos de miles de kilómetros de cables de fibra óptica submarinos que conectan países y continentes en todo el mundo. Una búsqueda en Internet de “mapa de cables submarinos de Internet” presenta varios mapas de cables de estas conexiones submarinas.

En general, los enlaces punto a punto son más costosos que los servicios compartidos. El costo de las soluciones de línea arrendada puede llegar a ser considerable cuando se utiliza para conectar varios sitios a través de distancias cada vez mayores. Sin embargo, hay ocasiones en las que los beneficios superan el costo de la línea arrendada. La capacidad dedicada quita latencia o vibración entre las terminales. La disponibilidad constante es fundamental para algunas aplicaciones, como VoIP o video sobre IP.



Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.1.1.4 Time-Division Multiplexing, multiplexación por división de tiempo

Con una línea arrendada, a pesar de que los clientes pagan servicios dedicados y de que se proporciona ancho de banda dedicado al cliente, la portadora sigue usando tecnologías de multiplexación dentro de la red. La multiplexación se refiere a un esquema que permite que varias señales lógicas compartan un único canal físico. Dos tipos comunes de multiplexación son la multiplexación por división de tiempo (TDM) y la multiplexación estadística por división de tiempo (STDM).

TDM

En los inicios, Bell Laboratories inventó TDM para maximizar la cantidad de tráfico de voz que se transportaba por un medio. Antes de la multiplexación, cada llamada telefónica requería su propio enlace físico. Esto era una solución costosa e imposible de escalar. TDM divide el ancho de banda de un único enlace en intervalos de tiempo separados. TDM transmite dos o más canales (flujo de datos) por el mismo enlace al asignar un intervalo de tiempo diferente para la transmisión de cada canal. En efecto, los canales se turnan para usar el enlace.

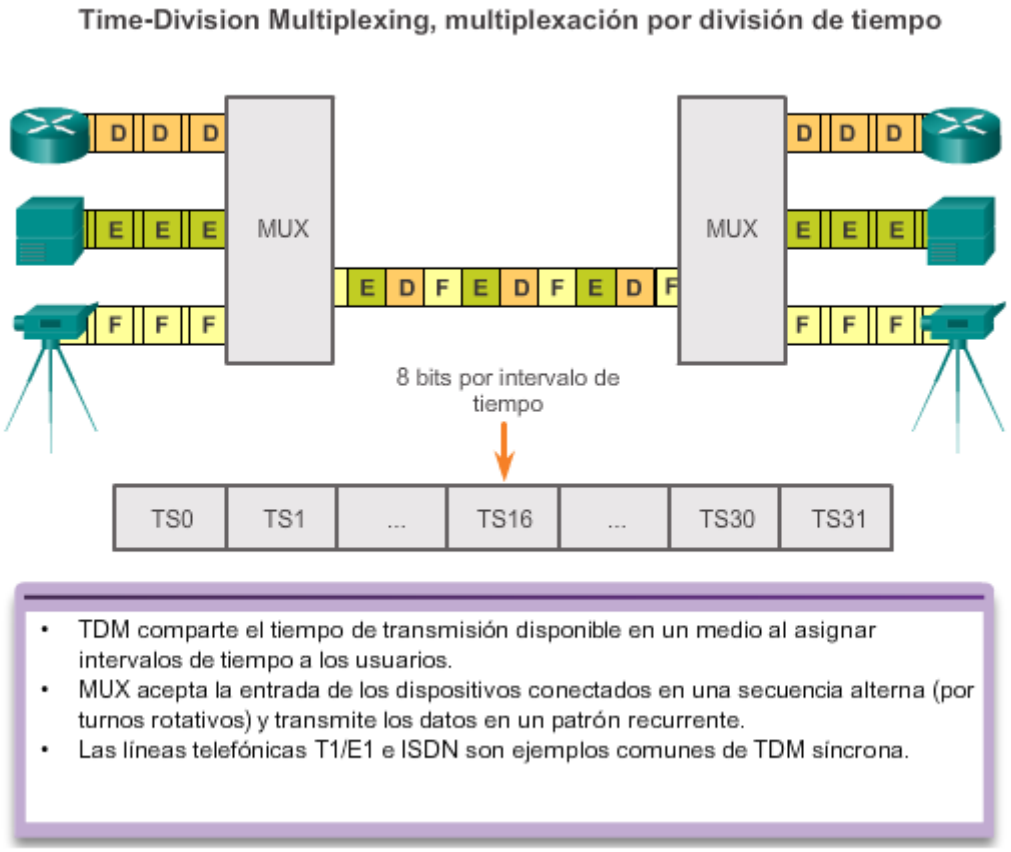
TDM es un concepto de capa física. No tiene en cuenta la naturaleza de la información que se multiplexa en el canal de salida. TDM es independiente del protocolo de capa 2 que usaron los canales de entrada.

TDM se puede explicar mediante una analogía con el tráfico de las autopistas. Para transportar el tráfico de cuatro caminos a otra ciudad, se puede enviar todo el tráfico por un carril si se atienden los caminos por igual y se sincroniza el tráfico. Si cada uno de los cuatro caminos coloca un automóvil en la autopista principal cada cuatro segundos, esta recibe un automóvil con una frecuencia de uno por segundo. Mientras la velocidad de todos los automóviles esté sincronizada, no hay colisiones. En el destino, sucede lo contrario, y los automóviles se sacan de la autopista y se colocan en los caminos locales mediante el mismo mecanismo sincrónico.

Este es el principio que se usa en TDM síncrona al enviar datos a través de un enlace. TDM aumenta la capacidad del enlace de transmisión al dividir el tiempo de transmisión en intervalos iguales más cortos, de modo que el enlace transporte los bits de varios orígenes de entrada.

En la ilustración, un multiplexor (MUX) en el transmisor acepta tres señales distintas. El MUX divide cada señal en segmentos. El MUX coloca cada segmento en un único canal insertando cada segmento en un intervalo de tiempo.

Un MUX en el extremo receptor vuelve a armar la transmisión TDM en tres flujos de datos distintos únicamente sobre la base del momento de llegada de cada bit. Una técnica denominada “entrelazado de bits” realiza un seguimiento del número y la secuencia de bits de cada transmisión específica para que se puedan volver a armar con rapidez y eficacia en la forma original de recepción. El entrelazado de bytes realiza las mismas funciones, pero debido a que hay 8 bits en cada byte, el proceso necesita un intervalo de tiempo más grande o más largo.



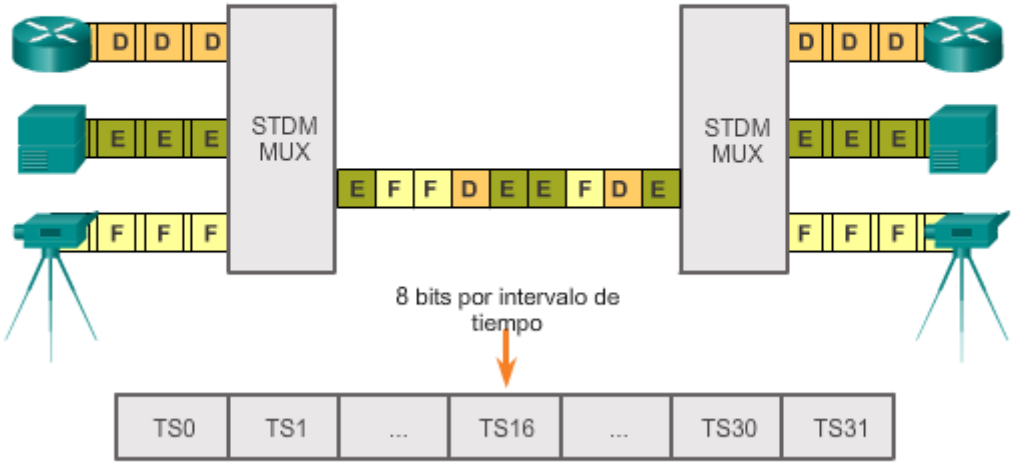
Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.1.1.5 Multiplexación estadística por división de tiempo

En otra analogía, se compara TDM con un tren con 32 vagones. Cada vagón pertenece a una empresa de carga distinta, y todos los días el tren parte con los 32 vagones conectados. Si una de las empresas tiene carga para enviar, se carga el vagón. Si la empresa no tiene nada para enviar, el vagón queda vacío, pero permanece en el tren. El envío de contenedores vacíos no es muy eficaz. TDM comparte esta ineficacia cuando el tráfico es intermitente, ya que se sigue asignando el intervalo de tiempo aun cuando el canal no tiene ningún dato para transmitir.

STDM

STDM se desarrolló para superar esta ineficacia. STDM utiliza un intervalo de tiempo variable, lo que permite que los canales compitan por cualquier espacio de intervalo libre. Emplea una memoria de búfer que almacena temporalmente los datos durante períodos de mayor tráfico. Con este esquema, STDM no pierde tiempo de la línea de alta velocidad con canales inactivos. STDM requiere que cada transmisión transporte información de identificación o un identificador de canal.

Multiplexación estadística por división de tiempo



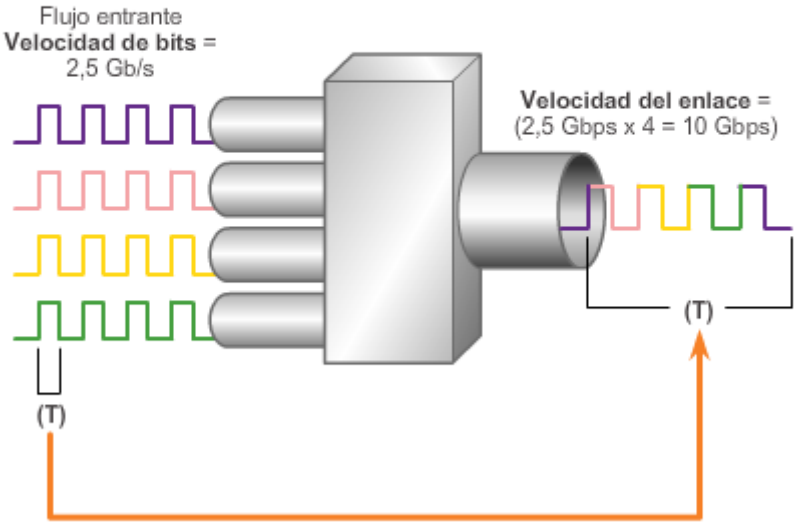
Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.1.1.6 Ejemplos de TDM

SONET y SDH

En una escala más grande, el sector de las telecomunicaciones usa el estándar de red óptica síncrona (SONET) o jerarquía digital síncrona (SDH) para el transporte óptico de datos TDM. SONET, utilizado en América del Norte, y SDH, utilizado en el resto del mundo, son dos estándares estrechamente vinculados que especifican parámetros de interfaz, velocidades, formatos de trama, métodos de multiplexación y la administración para TDM síncrona por fibra óptica.

En la ilustración, se muestra SONET, que es un ejemplo de STDM. SONET/SDH toma *n* streams de bits, los multiplexa y modula las señales ópticamente. A continuación, envía las señales mediante un dispositivo emisor de luz por fibra óptica con una velocidad de bits igual a *n* x (velocidad de bits entrantes). De esta forma, el tráfico que llega hasta el multiplexor SONET desde cuatro lugares a 2,5 Gb/s sale como un único flujo a 4 x 2,5 Gb/s o 10 Gb/s. Este principio se explica en la ilustración, en la que se muestra un aumento de la velocidad de bits por un factor de 4 en el intervalo de tiempo T.

Ejemplo de TDM: SONET



Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.1.1.7 Punto de demarcación

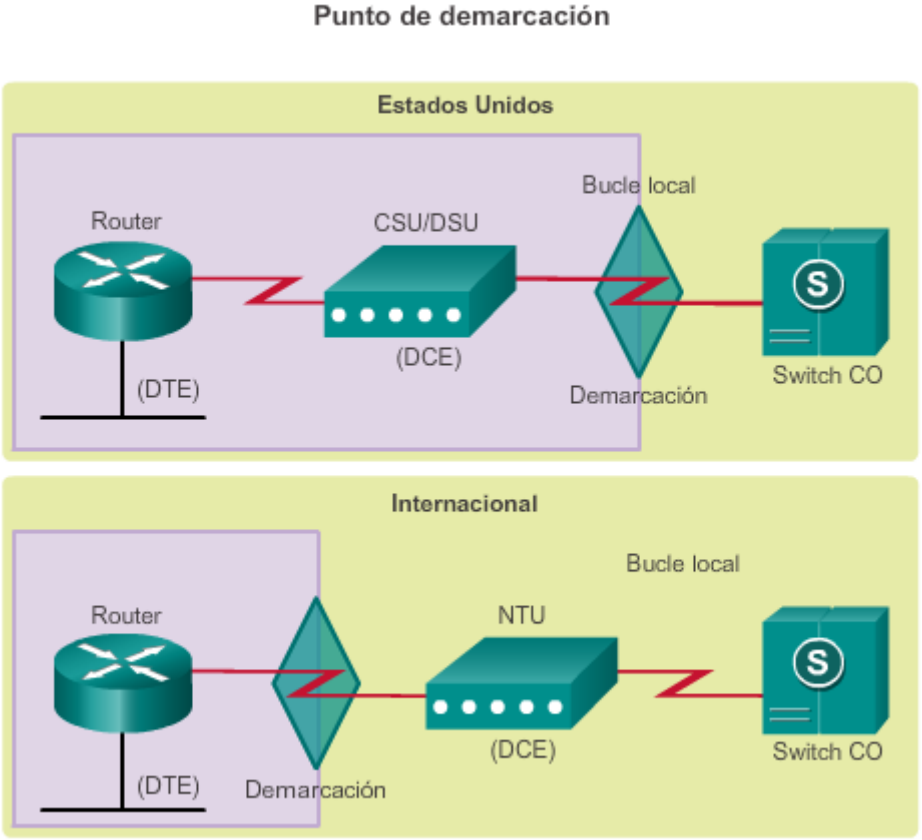
Antes de la desregulación en América del Norte y otros países, las empresas telefónicas eran propietarias del bucle local, incluidos el cableado y los equipos en las instalaciones de los clientes. El bucle local se refiere a la línea desde las instalaciones de un suscriptor telefónico hasta la oficina central de la compañía telefónica. La desregulación obligó a las empresas telefónicas a desarmar su infraestructura de bucle local para permitir que otros proveedores proporcionaran equipos y servicios. Esto llevó a la necesidad de delinear la parte de la red que pertenecía a la compañía telefónica y la parte que pertenecía al cliente. Este punto de delineación es el punto de demarcación. El punto de demarcación marca el punto en que la red se comunica con una red que pertenece a otra organización. En la terminología de la telefonía, esta es la interfaz entre el equipo local del cliente (CPE) y el equipo del proveedor de servicios de red. El punto de demarcación es aquel donde termina la responsabilidad del proveedor de servicios, como se muestra en la figura 1.

Las diferencias en los puntos de demarcación se muestran mejor mediante el uso de ISDN. En los Estados Unidos, un proveedor de servicios proporciona el bucle local en las instalaciones del cliente, y este proporciona equipos activos como la CSU/DSU, donde termina el bucle local. Esta terminación ocurre con frecuencia en un gabinete de telecomunicaciones, y el cliente es responsable de mantener, reemplazar o corregir el equipo. En otros países, el proveedor de servicios proporciona y administra la unidad de terminación red (NTU). Esto permite que el proveedor de servicios administre y resuelva problemas del bucle local de forma activa con el punto de demarcación que ocurre después de la NTU. El cliente conecta un dispositivo CPE, como un router o un dispositivo de acceso Frame Relay, a la NTU mediante una interfaz serial V.35 o RS-232.

Se requiere un puerto serial de router para cada conexión de línea arrendada. Si la red subyacente se basa en las tecnologías de portadora T o E, la línea arrendada se conecta a la red de la portadora a través de una CSU/DSU. El propósito de la CSU/DSU es proporcionar una señal de reloj a la interfaz del equipo del cliente desde la DSU y terminar los medios de

transporte canalizados de la portadora en la CSU. La CSU también proporciona funciones de diagnóstico, como la prueba de loopback.

Como se muestra en la figura 2, la mayoría de las interfaces TDM T1 o E1 en los routers actuales incluyen capacidades de CSU/DSU. No se requiere una CSU/DSU separada, ya que esta funcionalidad está integrada en la interfaz. Para configurar las operaciones de la CSU/DSU, se utilizan los comandos del IOS.



T1/E1 con CSU/DSU integrada

Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.1.1.8 DTE-DCE

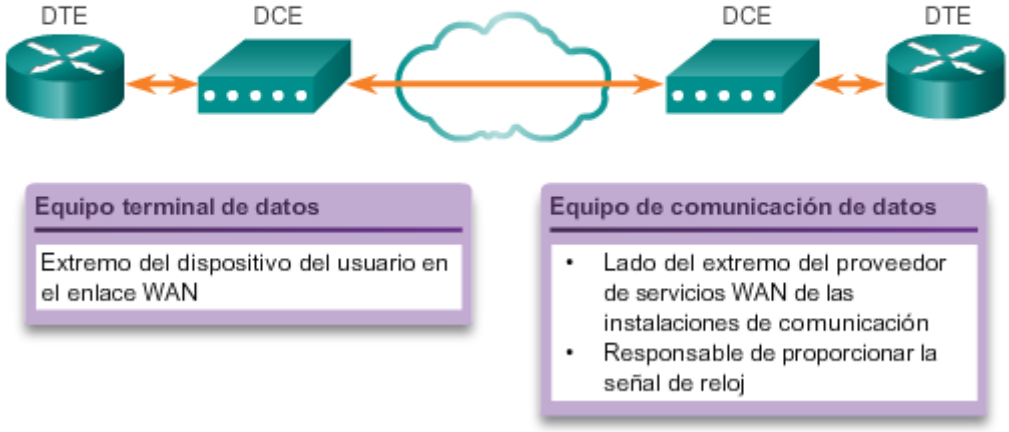
Desde el punto de vista de la conexión a la WAN, una conexión serial tiene un dispositivo DTE en un extremo y un dispositivo DCE en el otro. La conexión entre los dos dispositivos DCE es la red de transmisión del proveedor de servicios WAN, como se muestra en la ilustración. En este ejemplo:

- El CPE, que generalmente es un router, es el DTE. El DTE también podría ser una terminal, una computadora, una impresora o una máquina de fax si se conectan directamente a la red del proveedor de servicios.

- El DCE, habitualmente un módem o una CSU/DSU, es el dispositivo utilizado para convertir los datos de usuario del DTE a un formato aceptable para el enlace de transmisión del proveedor de servicios WAN. Esta señal se recibe en el DCE remoto, que vuelve a decodificar la señal en una secuencia de bits. A continuación, el DCE remoto indica esta secuencia al DTE remoto.

La Asociación de Industrias de la Electrónica (EIA) y el Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones (UIT-T) cumplieron una función importante en el desarrollo de estándares que permiten que los DTE se comuniquen con los DCE.

Conexiones WAN de DCE y DTE seriales



Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.1.1.9 Cables seriales

Originalmente, el concepto de DCE y DTE se basaba en dos tipos de equipos: el equipo terminal que generaba o recibía datos, y el equipo de comunicación que solo retransmitía datos. En el desarrollo del estándar RS-232, había motivos por los que los conectores RS-232 de 25 pines en estos dos tipos de equipos se debían conectar con cables diferentes. Estos motivos ya no son importantes, pero quedan dos tipos de cables diferentes: uno para conectar un DTE a un DCE, y otro para conectar dos DTE directamente entre sí.

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

- **Mecánica y física:** cantidad de pines y tipo de conector.
- **Eléctrica:** define los niveles de voltaje para 0 y 1.
- **Funcional:** especifica las funciones que se realizan mediante la asignación de significados a cada una de las líneas de señalización en la interfaz.
- **De procedimiento:** especifica la secuencia de eventos para transmitir datos.

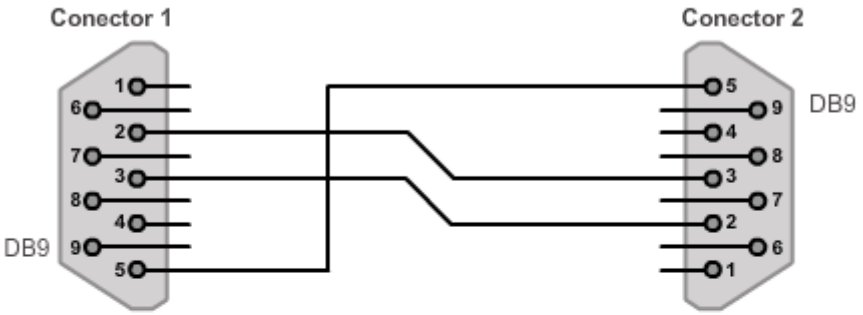
El estándar RS-232 original solo definía la conexión de los DTE con los DCE, que eran módems. Sin embargo, para conectar dos DTE, como dos computadoras o dos routers en un laboratorio, un cable especial denominado “cable de módem nulo” elimina la necesidad de un DCE. Es decir, se pueden conectar los dos dispositivos sin un módem. Un módem nulo es un método de comunicación para conectar directamente dos DTE mediante un cable serial RS-232. Con una conexión de módem nulo, las líneas de transmisión (Tx) y de recepción (Rx) se entrecruzan, como se muestra en la figura 1.

El cable para la conexión de DTE a DCE es un cable serial de transición blindado. El extremo del router del cable serial de transición blindado puede ser un conector DB-60, que se conecta al puerto DB-60 en una tarjeta de interfaz WAN serial, como se muestra en la figura 2. El otro extremo del cable serial de transición está disponible con el conector correspondiente para el estándar que se debe usar. Por lo general, el proveedor de servicios WAN o la CSU/DSU determina este tipo de cable. Los dispositivos de Cisco son compatibles con los estándares seriales EIA/TIA-232, EIA/TIA-449, V.35, X.21 y EIA/TIA-530, como los que se muestran en la figura 3.

Para admitir densidades de puertos superiores en un factor de forma más pequeño, Cisco presentó un cable serial inteligente, el cual se muestra en la figura 4. El extremo de la interfaz del router del cable serial inteligente es un conector de 26 pines que es mucho más compacto que el conector DB-60.

Al utilizar un módem nulo, las conexiones síncronas requieren una señal de reloj. Un dispositivo externo o uno de los DTE pueden generar la señal de reloj. De manera predeterminada, cuando se conecta un DTE y un DCE, el puerto serie en un router es el extremo DTE de la conexión, y generalmente una CSU/DSU o un dispositivo DCE similar proporciona la señal de reloj. Sin embargo, cuando se usa un cable módem nulo en una conexión de router a router, se debe configurar una de las interfaces seriales como el extremo DCE de modo que proporcione la señal de reloj para la conexión, como se muestra en la figura 5.

Módem nulo para conectar dos DTE

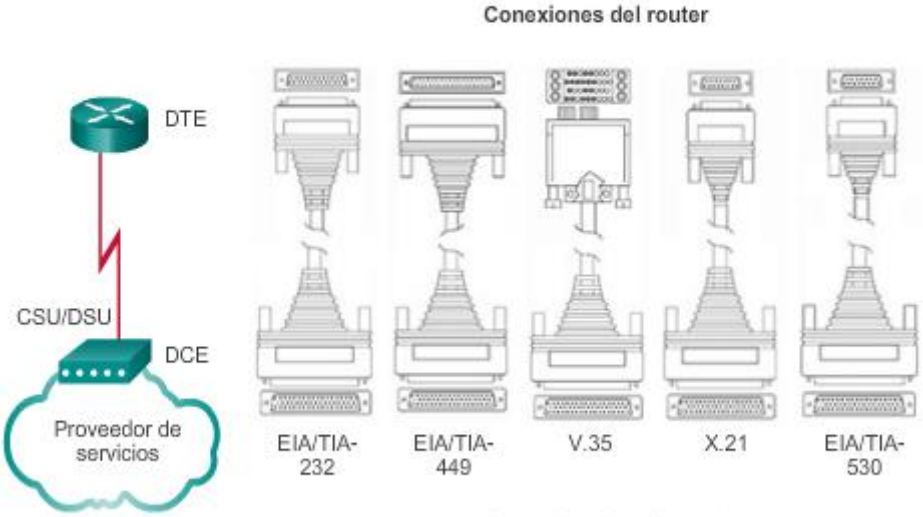


Observe los enlaces entrecruzados: del pin 2 al pin 3 y del pin 3 al pin 2

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

Conexión del router DB-60

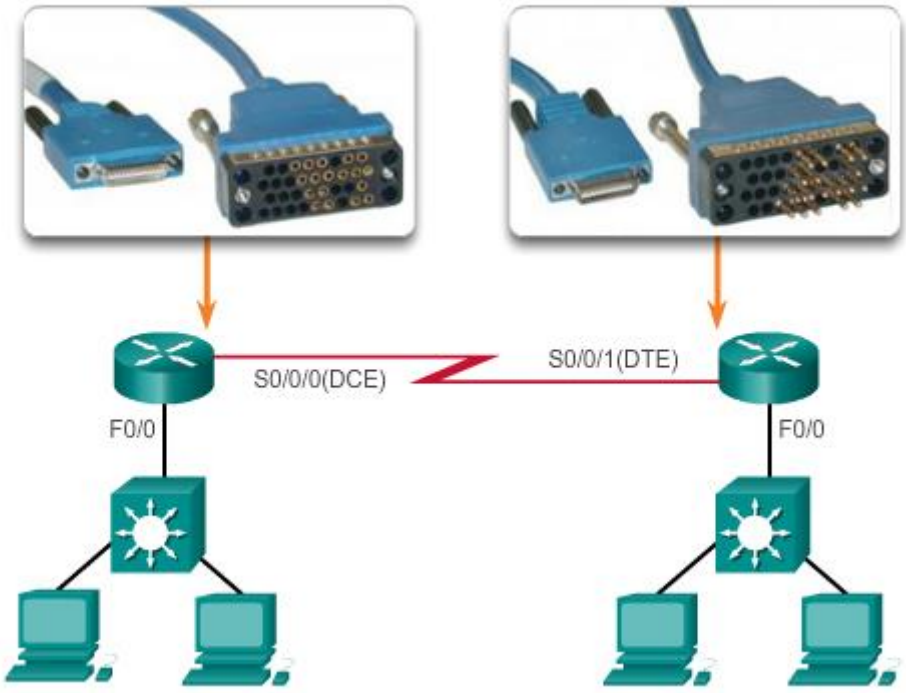
Opciones de conexión serial de WAN



Conector serial inteligente

Conector serial inteligente

Conexiones seriales WAN en el laboratorio



Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.1.1.10 Ancho de banda serial

El ancho de banda se refiere a la velocidad a la que se transfieren los datos a través del enlace de comunicación. La tecnología de portadora subyacente depende del ancho de banda disponible. Existe una diferencia en los puntos de ancho de banda entre la especificación norteamericana (portadora T) y el sistema europeo (portadora E). Las redes ópticas también utilizan otra jerarquía de ancho de banda, que también difiere entre América del Norte y Europa. En los EE. UU., la portadora óptica (OC) define los puntos de ancho de banda.

En América del Norte, el ancho de banda generalmente se expresa como un número de nivel de señal digital (DS0, DS1, etc.), el cual se refiere a la velocidad y el formato de la señal. La velocidad en línea más elemental es 64 kb/s, o DS-0, que es el ancho de banda requerido para una llamada telefónica digitalizada sin comprimir. Los anchos de banda de las conexiones seriales pueden aumentar cada vez más para satisfacer la necesidad de una transmisión más rápida. Por ejemplo, se pueden agrupar 24 DS0 para obtener una línea DS1 (también denominada “línea T1”) con una velocidad de 1,544 Mb/s. Asimismo, se pueden agrupar 28 DS1 para obtener una línea DS3 (también denominada “línea T3”) con una velocidad de 44,736 Mb/s. Hay líneas arrendadas disponibles con diferentes capacidades y, generalmente, el precio se basa en el ancho de banda requerido y en la distancia entre los dos puntos conectados.

Las velocidades de transmisión de OC son un conjunto de especificaciones estandarizadas para la transmisión de señales digitales que se transportan por redes de fibra óptica SONET. La designación utiliza OC seguida de un número entero que representa la velocidad de transmisión básica de 51,84 Mb/s. Por ejemplo, OC-1 tiene una capacidad de transmisión de

51,84 Mb/s, mientras que un medio de transmisión OC-3 sería 51,84 Mb/s por tres, o 155,52 Mb/s.

En la ilustración, se muestran los tipos de línea más comunes y la capacidad de velocidad de bits asociada de cada uno.

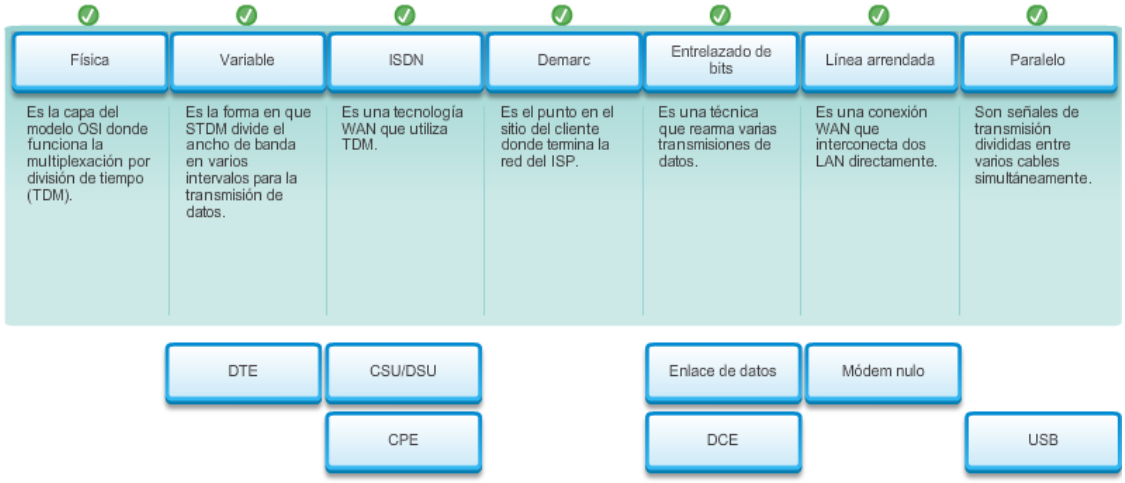
Nota: E1 (2,048 Mb/s) y E3 (34,368 Mb/s) son estándares europeos como T1 y T3, pero con anchos de banda y estructuras de trama diferentes.

Velocidades de transmisión de portadora

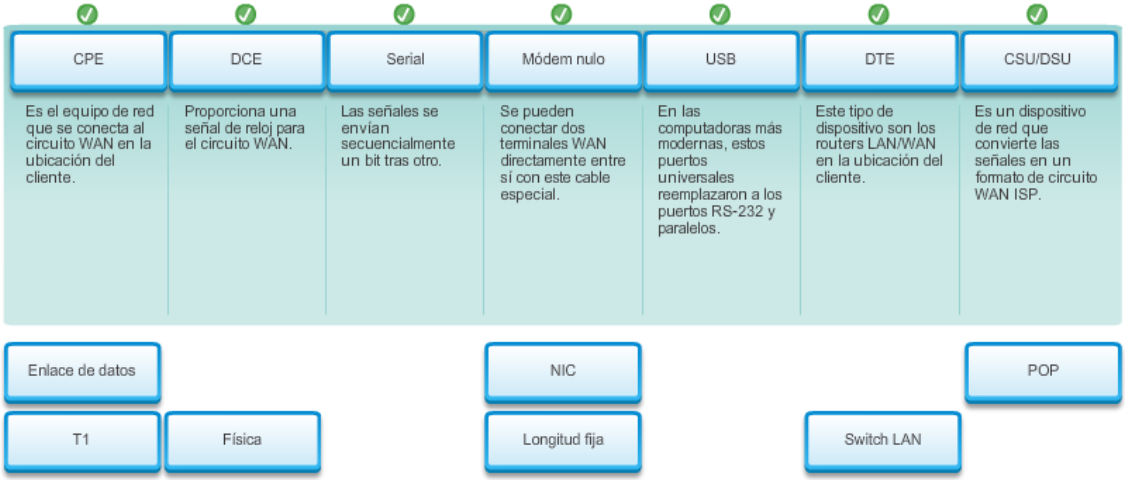
Tipo de línea	Capacidad de la velocidad de transmisión
56	56 kb/s
64	64 kb/s
T1	1,544 Mbps
E1	2,048 Mbps
J1	1,544 Mbps
E3	34,368 Mb/s
T3	44,736 Mbps
OC-1	51,84 Mb/s
OC-3	155,52 Mb/s
OC-9	466,56 Mb/s
OC-12	622,08 Mb/s
OC-18	933,12 Mb/s
OC-24	1,244 Gb/s
OC-36	1,866 Gb/s
OC-48	2,488 Gb/s
OC-96	4,976 Gb/s
OC-192	9,954 Gb/s
OC-768	39,813 Gb/s

Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.1.1.11 Actividad: Identificar la terminología relacionada con las comunicaciones seriales

Actividad: Identificar la terminología relacionada con las comunicaciones seriales (parte 1)
Arrastre el término relacionado con las comunicaciones seriales hasta la descripción correspondiente. Haga clic en el botón 2 para continuar la actividad.



Actividad: Identificar la terminología relacionada con las comunicaciones seriales (parte 2)
Arrastre el término relacionado con las comunicaciones seriales hasta la descripción correspondiente.



Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.1.2.1 Protocolos de encapsulación WAN

En cada conexión WAN, se encapsulan los datos en las tramas antes de cruzar el enlace WAN. Para asegurar que se utilice el protocolo correcto, se debe configurar el tipo de encapsulación de capa 2 correspondiente. La opción de protocolo depende de la tecnología WAN y el equipo de comunicación. En la ilustración, se muestran los protocolos WAN más comunes y dónde se utilizan. Las siguientes son descripciones breves de cada tipo de protocolo WAN:

- **HDLC:** es el tipo de encapsulación predeterminado en las conexiones punto a punto, los enlaces dedicados y las conexiones conmutadas por circuitos cuando el enlace utiliza dos dispositivos de Cisco. Ahora, HDLC es la base para PPP síncrono que usan muchos servidores para conectarse a una WAN, generalmente Internet.

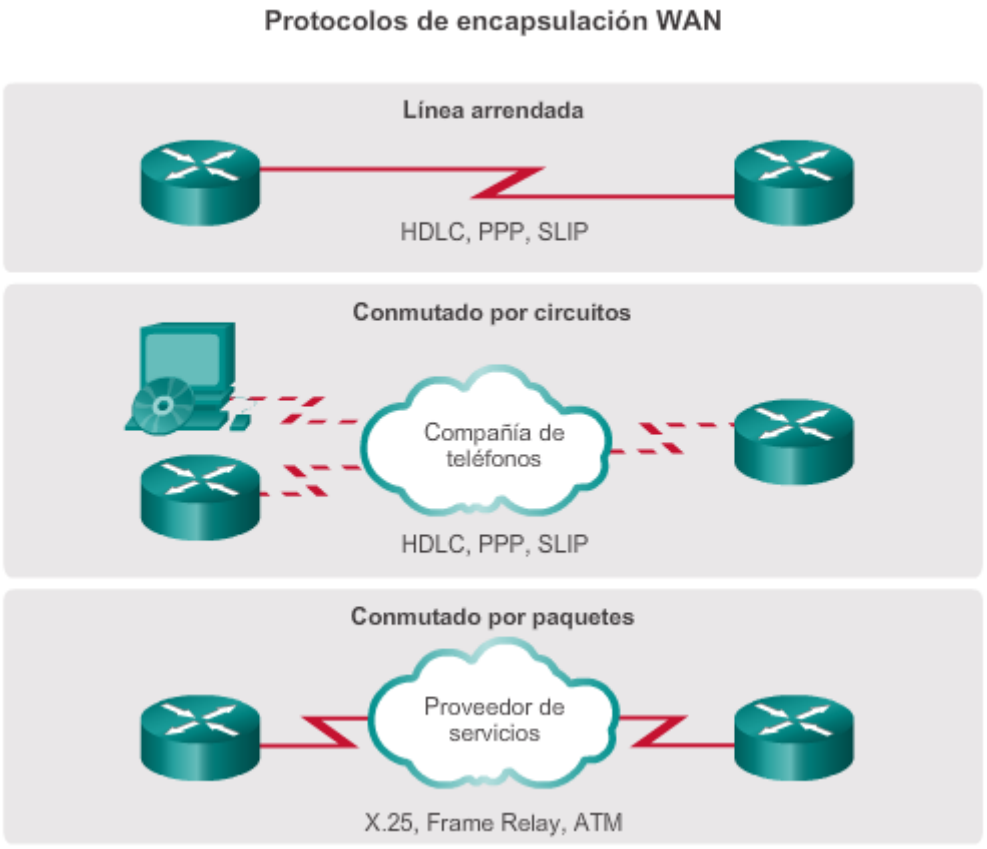
- **PPP:** proporciona conexiones de router a router y de host a red a través de circuitos síncronos y asíncronos. PPP funciona con varios protocolos de capa de red, como IPv4 e IPv6. PPP utiliza el protocolo de encapsulación HDLC, pero también tiene mecanismos de seguridad incorporados como PAP y CHAP.

- **Protocolo de Internet de línea serial (SLIP):** es un protocolo estándar para conexiones seriales punto a punto mediante TCP/IP. PPP reemplazó ampliamente al protocolo SLIP.

- **Procedimiento de acceso al enlace balanceado (LAPB) X.25:** es un estándar del UIT-T que define cómo se mantienen las conexiones entre un DTE y un DCE para el acceso remoto a terminales y las comunicaciones por computadora en las redes de datos públicas. X.25 especifica a LAPB, un protocolo de capa de enlace de datos. X.25 es un antecesor de Frame Relay.

- **Frame Relay:** es un protocolo de capa de enlace de datos conmutado y un estándar del sector que maneja varios circuitos virtuales. Frame Relay es un protocolo de última generación posterior a X.25. Frame Relay elimina algunos de los procesos prolongados (como la corrección de errores y el control del flujo) empleados en X.25.

- **ATM:** es el estándar internacional de retransmisión de celdas en el que los dispositivos envían varios tipos de servicios (como voz, video 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 las demoras en el tránsito. ATM aprovecha los medios de transmisión de alta velocidad, como E3, SONET y T3.



Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.1.2.2 Encapsulación HDLC

HDLC es un protocolo sincrónico de capa de enlace de datos orientado a bits desarrollado por la Organización Internacional para la Estandarización (ISO). El estándar actual para HDLC es ISO 13239. HDLC se desarrolló a partir del estándar de control de enlace de datos síncronos

(SDLC) propuesto en la década de los setenta. HDLC proporciona servicio orientado a la conexión y sin conexión.

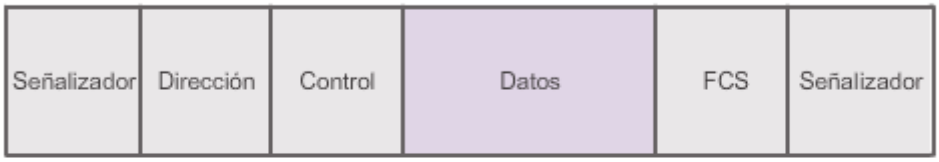
HDLC utiliza la transmisión serial síncrona, que proporciona una comunicación sin errores entre dos puntos. HDLC define una estructura de trama de capa 2 que permite el control del flujo y de errores mediante el uso de acuses de recibo. Cada trama presenta el mismo formato ya sea una trama de datos o una trama de control.

Cuando las tramas se transmiten por enlaces síncronos o asíncronos, esos enlaces no tienen ningún mecanismo para marcar ni el principio ni el fin de las tramas. Por este motivo, HDLC utiliza un delimitador de trama, o indicador, para marcar el principio y el fin de cada trama.

Cisco desarrolló una extensión del protocolo HDLC para resolver la incapacidad de proporcionar compatibilidad multiprotocolo. Si bien HDLC de Cisco (también conocido como cHDLC) es un protocolo exclusivo, Cisco permitió que muchos otros proveedores de equipos de red lo implementen. Las tramas HDLC de Cisco contienen un campo para identificar el protocolo de red que se encapsula. En la ilustración, se compara el estándar HDLC con HDLC de Cisco.

Formato de trama estándar y HDLC Cisco

HDLC estándar



Sólo admite entornos de protocolo único.

HDLC Cisco

Usa un campo de datos de protocolo para admitir entornos multiprotocolo.

Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.1.2.3 Tipos de tramas HDLC

HDLC define tres tipos de tramas, cada uno con un formato diferente de campo de control.

Señalizador

El campo Indicador inicia y termina la verificación de errores. La trama siempre comienza y termina con un campo Indicador de 8 bits. El patrón de bits es 01111110. Debido a que existe una probabilidad de que este patrón ocurra en los datos propiamente dichos, el sistema HDLC emisor siempre inserta un bit 0 después de cada cinco 1 consecutivos en el campo de datos,

de modo que en la práctica, la secuencia de indicadores solo se puede producir en los extremos de la trama. El sistema receptor elimina los bits introducidos. Cuando las tramas se transmiten en forma consecutiva, el indicador de fin de la primera trama se utiliza como indicador 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, una dirección de grupo o una dirección de difusión. Una dirección principal es un origen o un destino de comunicación, lo que elimina la necesidad de incluir la dirección de la estación principal.

Control

El campo Control utiliza tres formatos diferentes, según el tipo de trama HDLC que se use:

- **Trama de información (I):** las tramas I transportan información de capa superior y determinada información de control. Esta trama envía y recibe números de secuencia, y el bit de sondeo final (P/F) realiza el control del flujo y de errores. El número de secuencia de envío se refiere al número de la trama que se debe enviar a continuación. El número de secuencia de recepción proporciona el número de la trama que se recibe a continuación. Tanto el emisor como el receptor mantienen números de secuencia de envío y recepción. Las estaciones principales usan el bit P/F para informarles a las secundarias si requieren una respuesta inmediata. Las estaciones secundarias usan el bit P/F para informarles a las principales si la trama actual es la última en su respuesta actual.

- **Trama de supervisión (S):** las tramas S proporcionan información de control. Las tramas S pueden solicitar y suspender la transmisión, informar sobre el estado y confirmar la recepción de las tramas I. Las tramas S no tienen un campo de información.

- **Trama sin numerar (U):** las tramas U admiten funciones de control y no son secuenciales. Según la función de la trama U, el campo de control es de 1 byte o 2 bytes. Algunas tramas U tienen un campo de información.

Protocolo

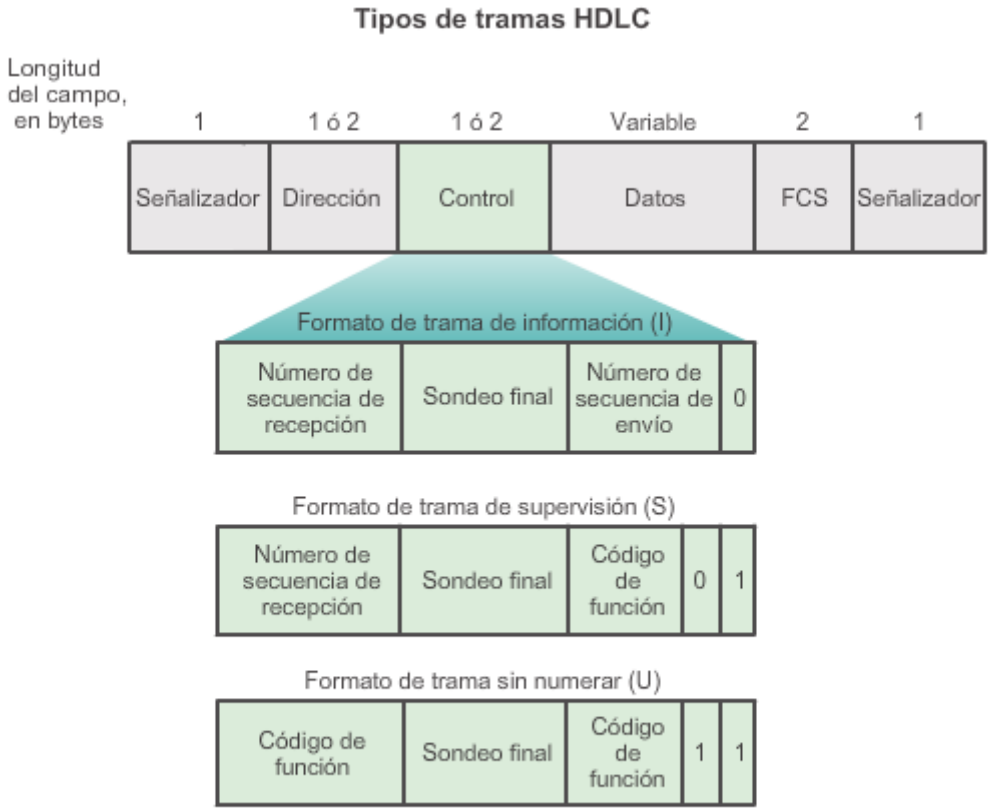
Solo se usa en HDLC de Cisco. Este campo especifica el tipo de protocolo encapsulado dentro de la trama (p. ej., 0x0800 para IP).

Datos

El campo de datos contiene una unidad de información de ruta (PIU) o información de identificación de intercambio (XID).

Secuencia de verificación de trama (FCS, Frame Check Sequence)

La FCS precede al delimitador del indicador de fin y generalmente es un resto del cálculo de la comprobación de redundancia cíclica (CRC). El cálculo de CRC se vuelve a realizar en el receptor. Si el resultado difiere del valor en la trama original, se supone que existe un error.



Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.1.2.3 Tipos de tramas HDLC

HDLC define tres tipos de tramas, cada uno con un formato diferente de campo de control.

Señalizador

El campo Indicador inicia y termina la verificación de errores. La trama siempre comienza y termina con un campo Indicador de 8 bits. El patrón de bits es 01111110. Debido a que existe una probabilidad de que este patrón ocurra en los datos propiamente dichos, el sistema HDLC emisor siempre inserta un bit 0 después de cada cinco 1 consecutivos en el campo de datos, de modo que en la práctica, la secuencia de indicadores solo se puede producir en los extremos de la trama. El sistema receptor elimina los bits introducidos. Cuando las tramas se transmiten en forma consecutiva, el indicador de fin de la primera trama se utiliza como indicador 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, una dirección de grupo o una dirección de difusión. Una dirección principal es un origen o un destino de comunicación, lo que elimina la necesidad de incluir la dirección de la estación principal.

Control

El campo Control utiliza tres formatos diferentes, según el tipo de trama HDLC que se use:

- **Trama de información (I):** las tramas I transportan información de capa superior y determinada información de control. Esta trama envía y recibe números de secuencia, y el bit de sondeo final (P/F) realiza el control del flujo y de errores. El número de secuencia de envío se refiere al número de la trama que se debe enviar a continuación. El número de secuencia de recepción proporciona el número de la trama que se recibe a continuación. Tanto el emisor como el receptor mantienen números de secuencia de envío y recepción. Las estaciones principales usan el bit P/F para informarles a las secundarias si requieren una respuesta inmediata. Las estaciones secundarias usan el bit P/F para informarles a las principales si la trama actual es la última en su respuesta actual.

- **Trama de supervisión (S):** las tramas S proporcionan información de control. Las tramas S pueden solicitar y suspender la transmisión, informar sobre el estado y confirmar la recepción de las tramas I. Las tramas S no tienen un campo de información.

- **Trama sin numerar (U):** las tramas U admiten funciones de control y no son secuenciales. Según la función de la trama U, el campo de control es de 1 byte o 2 bytes. Algunas tramas U tienen un campo de información.

Protocolo

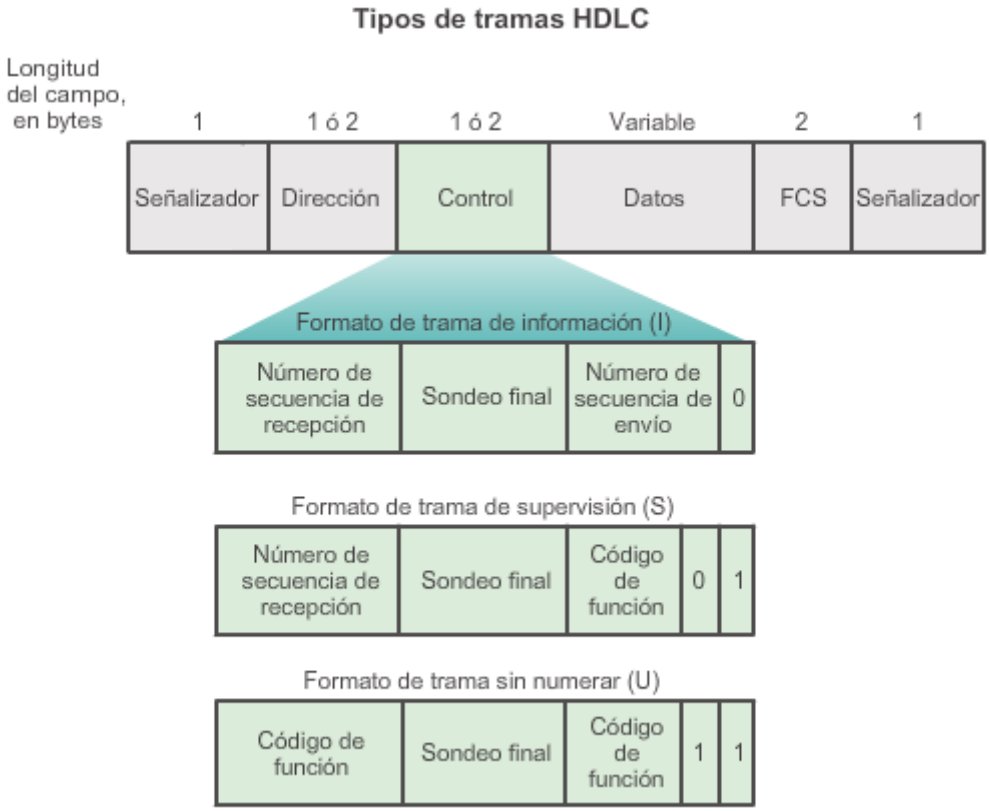
Solo se usa en HDLC de Cisco. Este campo especifica el tipo de protocolo encapsulado dentro de la trama (p. ej., 0x0800 para IP).

Datos

El campo de datos contiene una unidad de información de ruta (PIU) o información de identificación de intercambio (XID).

Secuencia de verificación de trama (FCS, Frame Check Sequence)

La FCS precede al delimitador del indicador de fin y generalmente es un resto del cálculo de la comprobación de redundancia cíclica (CRC). El cálculo de CRC se vuelve a realizar en el receptor. Si el resultado difiere del valor en la trama original, se supone que existe un error.



Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.1.2.4 Configuración de la encapsulación HDLC

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

Utilice HDLC de Cisco como protocolo punto a punto en las líneas arrendadas entre dos dispositivos de Cisco. Si conecta dispositivos que no son de Cisco, utilice PPP síncrono.

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

Como se muestra en la ilustración, se deben seguir dos pasos para volver a habilitar la encapsulación HDLC:

Paso 1. Ingrese al modo de configuración de interfaz de la interfaz serial.

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

Configuración de la encapsulación HDLC

```
Router(config)# interface s0/0/0
Router(config-if)# encapsulation hdlc
```

- Habilitación de la encapsulación HDLC.
- HDLC es la encapsulación predeterminada en las interfaces seriales.

Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.1.2.5 Resolución de problemas de una interfaz serial

El resultado del comando **show interfaces serial** muestra información específica de las interfaces seriales. Cuando se configura HDLC, debe figurar encapsulation HDLC en el resultado, como se destaca en la figura 1.Serial 0/0/0 is up, Line Protocol is up indica que la línea está activa y en funcionamiento;encapsulation HDLC indica que la encapsulación serial predeterminada (HDLC) está habilitada.

El comando **show interfaces serial**devuelve uno de seis estados posibles:

- Serial x is up, line protocol is up
- 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 está desactivado administrativamente, el protocolo de línea está desactivado

De los seis estados posibles, cinco son estados problemáticos. En la figura 2, se muestran los cinco estados problemáticos, los problemas asociados a cada estado y la forma de resolver el problema.

El comando **show controllers** es otra herramienta de diagnóstico importante para la resolución de problemas de líneas seriales, como se muestra en la figura 3. El resultado indica el estado de los canales de la interfaz y si hay un cable conectado a la interfaz o no. En la ilustración, la interfaz serial 0/0/0 tiene un cable DCE V.35 conectado. La sintaxis de los comandos varía, según la plataforma. Los routers Cisco serie 7000 utilizan una tarjeta controladora cBus para conectar enlaces seriales. Con estos routers, utilice el comando **show controllers cbus**.

Si el resultado de la interfaz eléctrica aparece como UNKNOWN en lugar de V.35, EIA/TIA-449 o algún otro tipo de interfaz eléctrica, es probable que el problema sea un cable mal conectado. También es posible que exista un problema con el cableado interno de la tarjeta. Si la interfaz eléctrica es desconocida, el resultado correspondiente para el comando **show interfaces serial** muestra que la interfaz y el protocolo de línea están inactivos.

Resolución de problemas de una interfaz serial

```
R1# show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 172.16.0.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  Last input 00:00:05, output 00:00:04, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total
  output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max
total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
```

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 ninguna señal de detección de portadora (CD), lo que significa que la CD no está activa. Se produjo un problema con el proveedor de servicios de portadora WAN, lo que significa que la línea está inactiva o no está conectada a la CSU/DSU. El cableado presenta una falla o es incorrecto. Se produjo una falla de hardware (CSU/DSU).	1. Verifique los LED en la CSU/DSU para ver si la CD está activa, o inserte una caja de interconexión en la línea a fin de verificar la señal CD. 2. Verifique que se utilice el cable y la interfaz correspondientes en la documentación de instalación del hardware. 3. Inserte una caja de interconexión y revise todos los conectores de control. 4. Comuníquese con el servicio de línea arrendada o de otra portadora para ver si existe algún problema. 5. Cambie las partes que presenten fallas. 6. Si se sospecha que el hardware del router presenta una falla, 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 keepalive. Se produjo un problema con el servicio de portadora o de línea arrendada, lo que significa que hay una línea con ruido o un switch mal configurado o con fallas. Se produjo un problema de temporización en el cable, lo que significa que no se estableció la transmisión externa del reloj serial (SCTE) en la 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	1. Coloque el módem, la CSU o la DSU en el modo de loopback local y utilice el comando **`show interfaces serial`** para determinar si el protocolo de línea se activa. Si el protocolo de línea se activa, es probable que haya un problema con el proveedor de servicios de portadora WAN o con un router remoto que presenta fallas. 2. Si parece que el problema se encuentra en el extremo remoto, repita el paso1 en el módem remoto, la CSU o DSU. 3. Verifique 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. Utilice el comando **`show controllers`** del modo EXEC para determinar qué cable se conecta a qué interfaz. 4. Habilite el comando **`debug serial interface`** del modo EXEC.

	muestra de los datos sin error, aunque se produzca un desplazamiento de fase en el cable. Una CSU/DSU remota o local ha fallado. El hardware del router, que puede ser local o remoto, ha fallado.	5. Si el protocolo de línea no se activa en el modo de loopback local y el resultado del comando **debug serial interface** del modo EXEC muestra que el contador de keepalives no aumenta, es probable que haya un problema con el hardware del router. Cambie el hardware de interfaz del router. 6. Si se activa el protocolo de línea y el contador de keepalives aumenta, el problema no está en el router local. 7. Si se sospecha que el hardware del router presenta una falla, cambie la línea serial a un puerto sin utilizar. Si la conexión se activa, la interfaz conectada anteriormente tiene un problema.
Serial x is up, line protocol is down (DCE mode)	Falta el comando de configuración de interfaz **clockrate** El dispositivo DTE no admite el modo SCTE (temporización de terminales) o no se configuró para este modo. La CSU o la DSU remota falló.	1. Agregue el comando de configuración de interfaz **clockrate** a la interfaz serial. Sintaxis: **clockrate** *bps* Descripción de la sintaxis: *bps*, frecuencia de reloj deseada en bits por segundo, 1200, 2400, 4800, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 250000, 500000, 800000, 1000000, 1300000, 2000000, 4000000 o 8000000 2. Si parece que el problema se encuentra en el extremo remoto, repita el paso1 en el módem remoto, la CSU o DSU. 3. Verifique que se utilice el cable correcto. 4. Si el protocolo de línea sigue desactivado, posiblemente haya una falla de hardware o problema de cableado. Inserte una caja de interconexión y observe los conectores. 5. Reemplace las partes dañadas, según sea necesario.
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. Utilice el comando **show running-config** del modo EXEC privilegiado para buscar entradas del comando de configuración de interfaz **loopback** . 2. Si hay una entrada del comando de configuración de interfaz **loopback** , utilice el comando de configuración de interfaz **no loopback** para eliminar el bucle. 3. Si no hay ningún comando de configuración de interfaz **loopback** , examine la CSU/DSU para determinar si se configuraron en modo loopback manual. De ser así, deshabilite el modo loopback manual. 4. Después de deshabilitar el modo loopback en la CSU/DSU, restablezca la CSU/DSU e inspeccione el estado de la línea. Si el protocolo de línea se activa, no necesita realizar ninguna otra acción. 5. Si al realizar la inspección no se puede restablecer la CSU o la DSU manualmente, comuníquese con el servicio de la línea arrendada o de otra portadora para obtener ayuda con la resolución de problemas de la línea.
Serial x is up, line protocol is down (disabled)	Se produjo un índice de error alto debido a un problema con el proveedor de servicios WAN. Se produjo un problema con el hardware de la CSU o de la DSU. El hardware del router (interfaz) es defectuoso.	1. Resuelva los problemas de la línea con un analizador serial y una caja de interconexión. Busque señales CTS y DSR que cambien de estado. 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 continúa, es probable que haya un problema con el proveedor de servicios WAN. 3. Cambie el hardware defectuoso (CSU, DSU, switch, router local o remoto).

Serial x está desactivado administrativamente, el protocolo de línea está desactivado	La configuración del router incluye el comando de configuración de interfaz **shutdown** . Existe una dirección IP duplicada.	1. Verifique la configuración del router para el comando **shutdown** . 2. Utilice el comando de configuración de interfaz **no shutdown** para eliminar el comando **shutdown** . 3. Verifique que no haya direcciones IP idénticas mediante el comando **show running-config** del modo EXEC privilegiado o el comando **show interfaces** del modo EXEC. 4. Si hay direcciones duplicadas, resuelva el conflicto mediante el cambio de una de las direcciones IP.

```
R1# show controllers serial 0/0/0
Interface Serial0/0/0
Hardware is GT96K
DCE V.35, clock rate 64000
idb at 0x66855120, driver data structure at 0x6685C93C
wic_info 0x6685CF68
Physical Port 0, SCC Num 0
MPSC Registers:
MMCR_L=0x000304C0, MMCR_H=0x00000000, MPCR=0x00000000
CHR1=0x00FE007E, CHR2=0x00000000, CHR3=0x0000064A,
CHR4=0x00000000
```

Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.1.2.6 Verificador de sintaxis:

Resolución de problemas de una interfaz serial

Resolución de problemas de una interfaz serial

Realice los pasos de la resolución de problemas según lo indicado.
El router R1 debe configurarse con los siguientes parámetros:

- **S0/0/0 es la interfaz DCE.**
- **Frecuencia de reloj establecida en 64000.**
- **Encapsulación HDLC**

Introduzca el comando show para verificar el tipo de cable conectado a S0/0/0.

```
R1# show controllers s0/0/0
Interface Serial0/0/0
Hardware is PowerQUICC MPC860
DCE V.35, clock rate 64000
idb at 0x81081AC4, driver data structure at 0x81084AC0
SCC Registers:
General [GSMR]=0x2:0x00000000, Protocol-specific [PSMR]=0x8
Events [SCCE]=0x0000, Mask [SCCM]=0x0000, Status [SCCS]=0x00
Transmit on Demand [TODR]=0x0, Data Sync [DSR]=0x7E7E
< Resultado omitido >
```

Introduzca el comando show para verificar la configuración de la encapsulación para S0/0/0.

```
R1# show interfaces s0/0/0
Serial0/0/0 is up, line protocol is down (disabled)
 Hardware es HD64570
 Internet address is 172.16.0.1/30
 MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
 reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation PPP, loopback not set, keepalive set (10 sec)
 LCP Closed
 Closed: LEXCP, BRIDGECP, IPCP, CCP, CDPCP, LLC2, BACP
 Last input never, output never, output hang never
 Last clearing of "show interface" counters never
< Resultado omitido >
```

Configure la interfaz S0/0/0 para que utilice la encapsulación predeterminada.

```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# interface s0/0/0
```

```
R1(config-if)# encapsulation hdlc
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up
```

Introduzca el comando "do show" para verificar la configuración de la encapsulación para S0/0/0.

```
R1(config-if)# do show interfaces s0/0/0
Serial0/0/0 is up, line protocol is up (connected)
 Hardware es HD64570
 Internet address is 172.16.0.1/30
 MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
 reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation HDLC, loopback not set, keepalive set (10 sec)
 Last input never, output never, output hang never
 Last clearing of "show interface" counters never
< Resultado omitido >
```

Realizó correctamente los pasos de la resolución de problemas para la interfaz serial.

Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.1.2.7 Packet Tracer: Resolución de problemas de interfaces seriales

Información básica/situación

Se le pidió que resuelva los problemas de las conexiones WAN de una compañía telefónica local (Telco). Se supone que el router Telco se debe comunicar con cuatro sitios remotos, pero ninguno de estos funciona. Aplique sus conocimientos del modelo OSI y algunas reglas generales para identificar y resolver los errores en la red.

Packet Tracer: Resolución de problemas de interfaces seriales (instrucciones)

Packet Tracer: Resolución de problemas de interfaces seriales (PKA)

Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.2.1.1 Introducción a PPP

Recuerde que HDLC es el método de encapsulación serial predeterminado al conectar dos routers Cisco. Con un campo agregado de tipo de protocolo, la versión de HDLC de Cisco es exclusiva. Por eso, HDLC de Cisco solo puede funcionar con otros dispositivos de Cisco. Sin embargo, cuando existe la necesidad de conectarse a un router que no es de Cisco, se debe usar la encapsulación PPP, como se muestra en la ilustración.

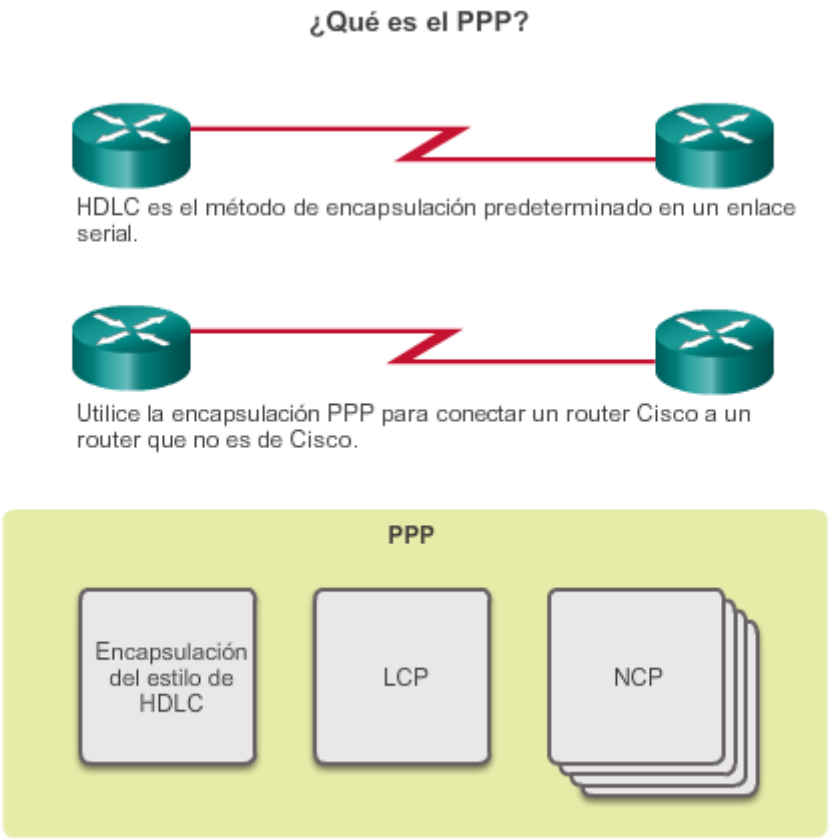
La encapsulación PPP se diseñó cuidadosamente para conservar la compatibilidad con el hardware más usado que la admite. PPP encapsula tramas de datos para transmitirlas a través de enlaces físicos de capa 2. PPP establece una conexión directa mediante cables seriales, líneas telefónicas, líneas troncales, teléfonos celulares, enlaces de radio especializados o enlaces de fibra óptica.

PPP contiene tres componentes principales:

- Entramado del estilo de HDLC para transportar paquetes multiprotocolo a través de enlaces punto a punto.

- Protocolo de control de enlace (LCP) extensible para establecer, configurar y probar la conexión de enlace de datos.

- Familia de protocolos de control de red (NCP) para establecer y configurar distintos protocolos de capa de red. PPP permite el uso simultáneo de varios protocolos de capa de red. Algunos de los NCP más comunes son el protocolo de control del protocolo de Internet (IPv4), el protocolo de control de IPv6, el protocolo de control AppleTalk, Novell IPX, el protocolo de control de Cisco Systems, el protocolo de control SNA y el protocolo de control de compresión.



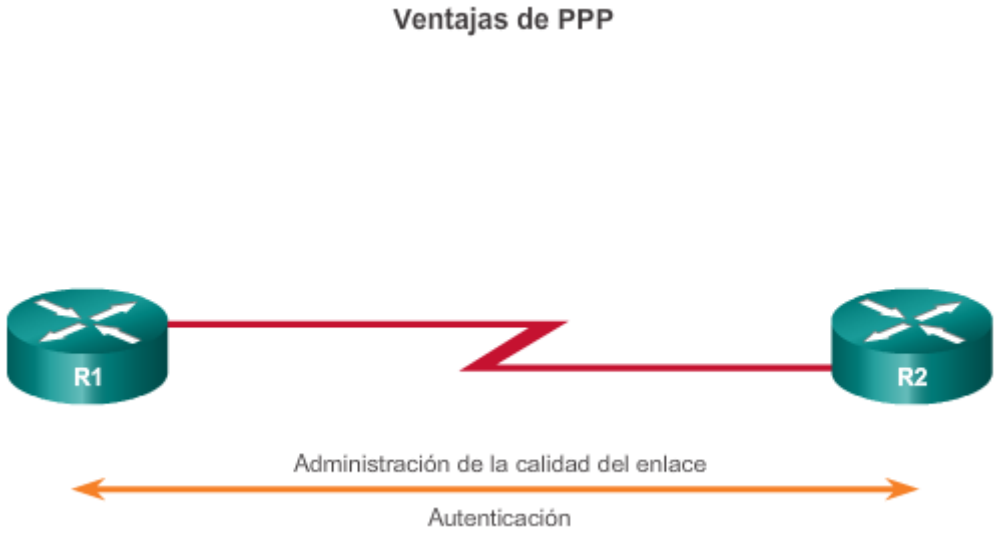
Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.2.1.2 Ventajas de PPP

PPP surgió originalmente como protocolo de encapsulación para transportar tráfico IPv4 a través de enlaces punto a punto. PPP proporciona un método estándar para transportar paquetes multiprotocolo a través de enlaces punto a punto.

El uso de PPP presenta muchas ventajas, incluido el hecho de que no es exclusivo. PPP incluye muchas funciones que no están disponibles en HDLC:

- La característica de administración de calidad del enlace, la cual se muestra en la ilustración, controla la calidad del enlace. Si se detectan demasiados errores, PPP desactiva el enlace.

- PPP admite la autenticación PAP y CHAP. Esta característica se explica y se práctica más adelante en otra sección.



Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.2.2.1 Arquitectura de capas PPP

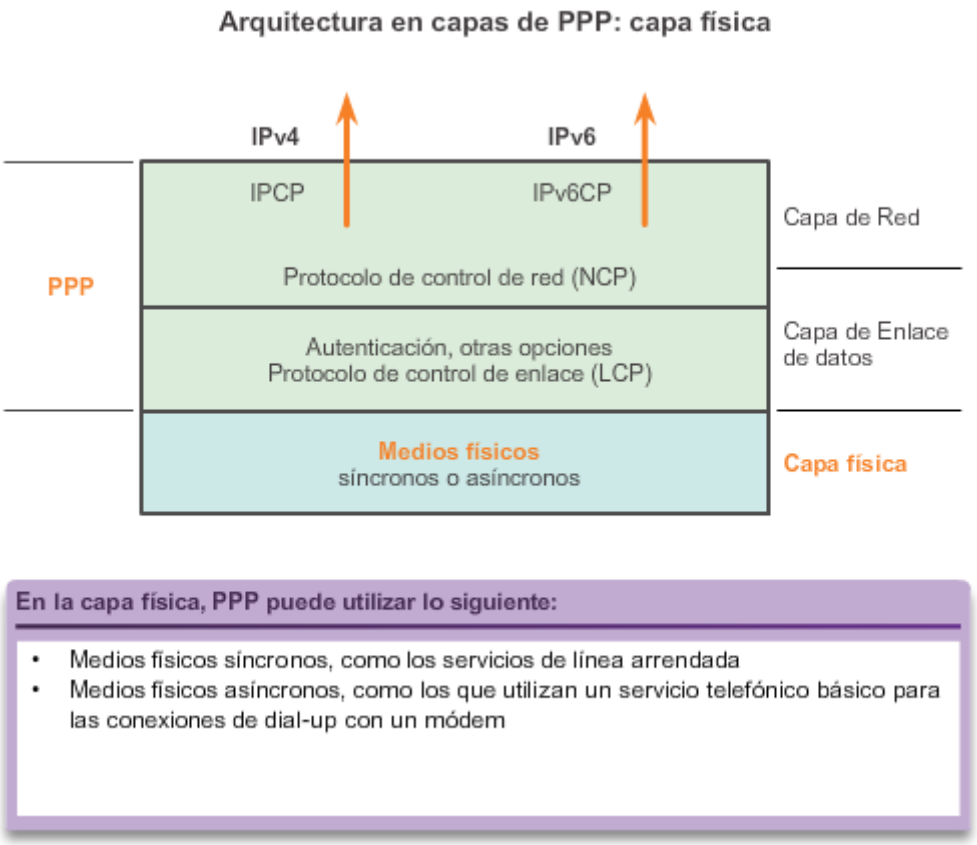
Una arquitectura en capas es un modelo, un diseño, o un plano lógico que ayuda en la comunicación de las capas que se interconectan. En la ilustración, se compara la arquitectura en capas de PPP con el modelo de interconexión de sistema abierto (OSI). PPP y OSI comparten la misma capa física, pero PPP distribuye las funciones de LCP y NCP de manera diferente.

En la capa física, puede configurar PPP en un rango de interfaces, incluidas las siguientes:

- Serial asíncrona
- Serial síncrona
- HSSI
- ISDN

PPP opera a través de cualquier interfaz DTE/DCE (RS-232-C, RS-422, RS-423 o V.35). El único requisito absoluto impuesto por PPP es un circuito full-duplex, ya sea dedicado o conmutado, que pueda funcionar en modo de bits seriales síncrono o asíncrono, transparente para las tramas de capa de enlace PPP. PPP no impone ninguna restricción con respecto a la velocidad de transmisión además de los impuestos por la interfaz DTE/DCE específica que se utiliza.

La mayor parte del trabajo que realiza PPP lo llevan a cabo LCP y los NCP en las capas de enlace de datos y de red. LCP configura la conexión PPP y sus parámetros, los NCP manejan las configuraciones de protocolo de capa superior, y LCP finaliza la conexión PPP.



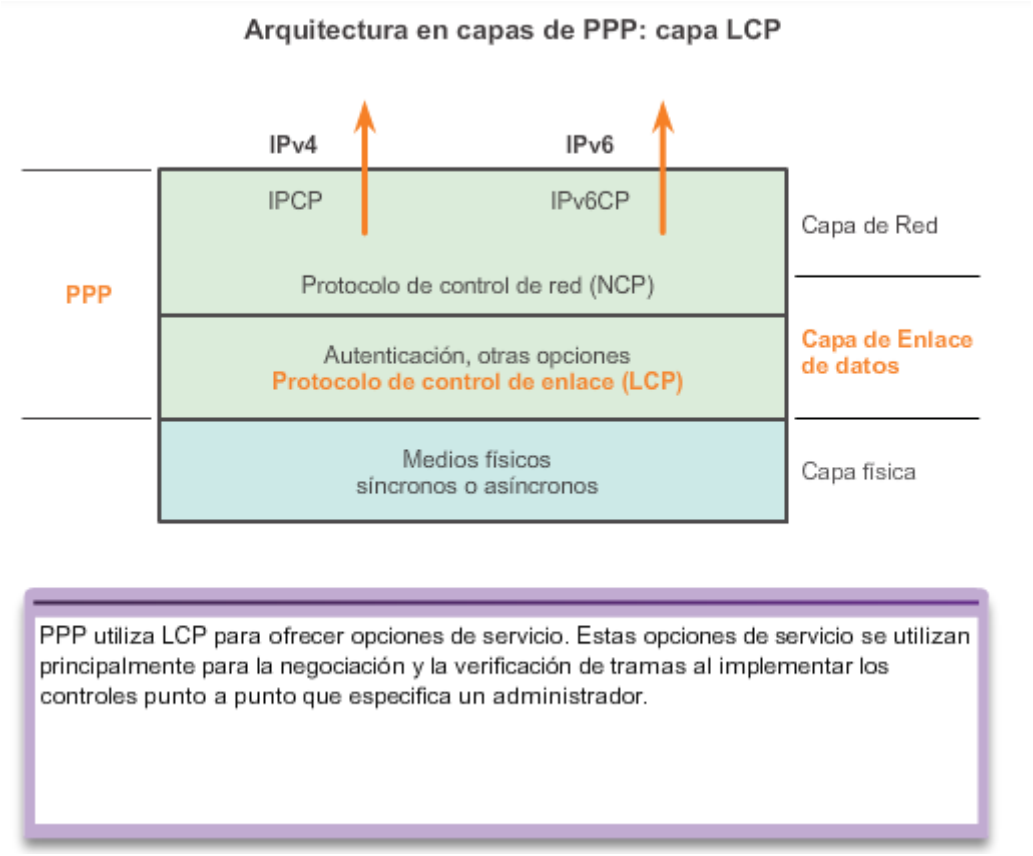
Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.2.2.2 PPP: protocolo de control de enlace (LCP)

LCP funciona dentro de la capa de enlace de datos y cumple una función en el establecimiento, la configuración y la prueba de la conexión de enlace de datos. LCP establece el enlace punto a punto. LCP también negocia y configura las opciones de control en el enlace de datos WAN, administradas por los NCP.

LCP proporciona la configuración automática de las interfaces en cada extremo, incluido lo siguiente:

- Manejo de distintos límites en el tamaño de paquete
- Detección de errores comunes de configuración
- Finalización del enlace
- Determinación de cuándo un enlace funciona correctamente o cuándo falla

Una vez establecido el enlace, PPP también usa LCP para acordar automáticamente los formatos de encapsulación, como la autenticación, la compresión y la detección de errores.

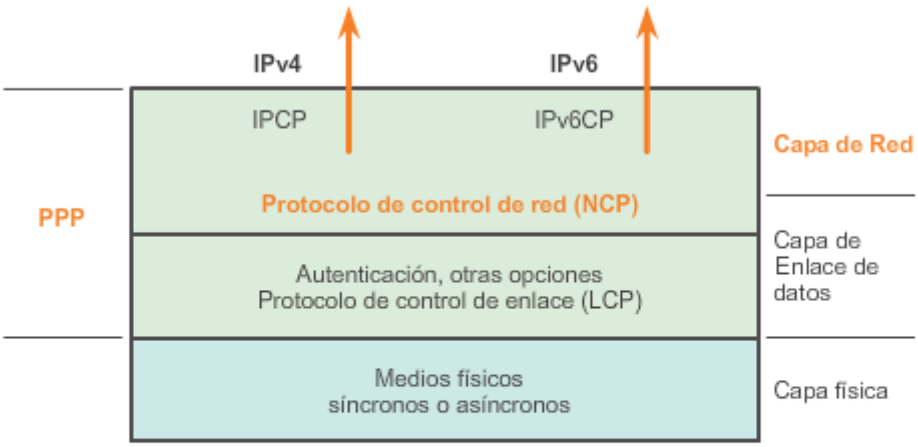


Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.2.2.3 PPP: protocolo de control de red (NCP)

PPP permite que varios protocolos de capa de red funcionen en el mismo enlace de comunicación. Para cada protocolo de capa de red que se usa, PPP utiliza un NCP separado, como se muestra en la figura 1. Por ejemplo, IPv4 utiliza el protocolo de control de IP (IPCP) e IPv6 utiliza el protocolo de control de IPv6 (IPv6CP.

Los protocolos NCP incluyen campos funcionales que contienen códigos estandarizados para indicar el protocolo de capa de red que PPP encapsula. En la figura 2, se indican los números de los campos de protocolo PPP. Cada NCP administra las necesidades específicas requeridas por sus respectivos protocolos de capa de red. Los distintos componentes NCP encapsulan y negocian las opciones para varios protocolos de capa de red.

Arquitectura PPP: capa de red



PPP utiliza NCP para negociar los protocolos de capa 3 que se utilizarán para transportar paquetes de datos. Estos protocolos proporcionan campos funcionales que contienen códigos estandarizados para indicar el tipo de protocolo de capa de red que PPP encapsula.

Campos de protocolo

Valor (en hex)	Nombre del protocolo
8021	Protocolo de control del protocolo de Internet (IPv4)
8057	Protocolo de control del protocolo de Internet versión 6 (IPv6)
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

Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.2.2.4 Estructura de la trama PPP

Las tramas PPP constan de seis campos. Las siguientes descripciones resumen los campos de las tramas PPP, que se muestran en la ilustración:

- **Indicador:** un único byte que indica el inicio y el final de una trama. El campo Señalización está formado por la secuencia binaria 01111110. En tramas PPP sucesivas sólo se usa un caracter de señalador único.

- **Dirección:** un único byte que contiene la secuencia binaria 11111111, la dirección de difusión estándar. PPP no asigna direcciones a estaciones individuales.

- **Control:** un único byte formado por la secuencia binaria 00000011, que requiere la transmisión de datos de usuario en una trama no secuencial. Esto brinda un servicio de enlace sin conexión que requiere el establecimiento de enlaces de datos o estaciones de enlaces. 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 peers PPP acuerdan realizar la compresión de los campos de control y de dirección durante la negociación LCP, el campo Dirección no se incluye.

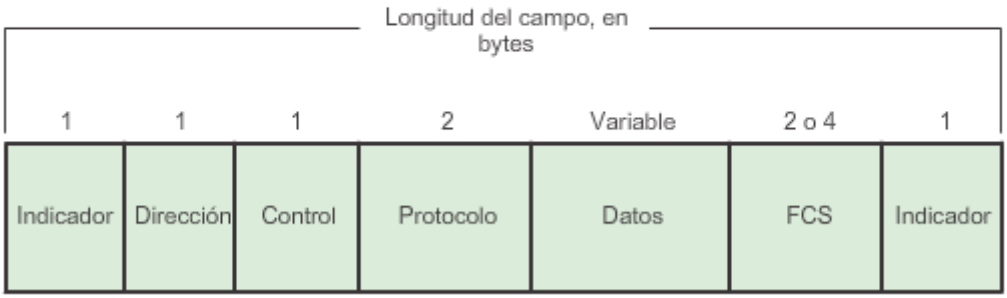
- **Protocolo:** dos bytes que identifican el protocolo encapsulado en el campo de información de la trama. El campo Protocolo de 2 bytes identifica al protocolo del contenido PPP. Si ambos peers PPP acuerdan realizar la compresión del campo de protocolo durante la negociación LCP, el campo Protocolo es de 1 byte para la identificación del protocolo en el rango de 0x00-00 a 0x00-FF. Los valores más actualizados del campo Protocolo se especifican en la Solicitud de comentarios con números asignados (RFC) más reciente.

- **Datos:** cero o más bytes que contienen el datagrama para el protocolo especificado en el campo Protocolo. Para encontrar el fin del campo de información, se debe buscar la secuencia del indicador de finalización y dejar 2 bytes para el campo FCS. La longitud máxima predeterminada del campo de información es de 1500 bytes. Mediante un acuerdo previo, con la aceptación de las implementaciones PPP se pueden usar otros valores para la longitud máxima del campo de información.

- **Secuencia de verificación de trama (FCS):** normalmente de 16 bits (2 bytes). Mediante un acuerdo previo, con la aceptación de las implementaciones PPP se puede utilizar una FCS de 32 bits (4 bytes) para una mayor detección de errores. Si el cálculo de la FCS que realiza el receptor no coincide con la FCS de la trama PPP, esta se descarta sin aviso.

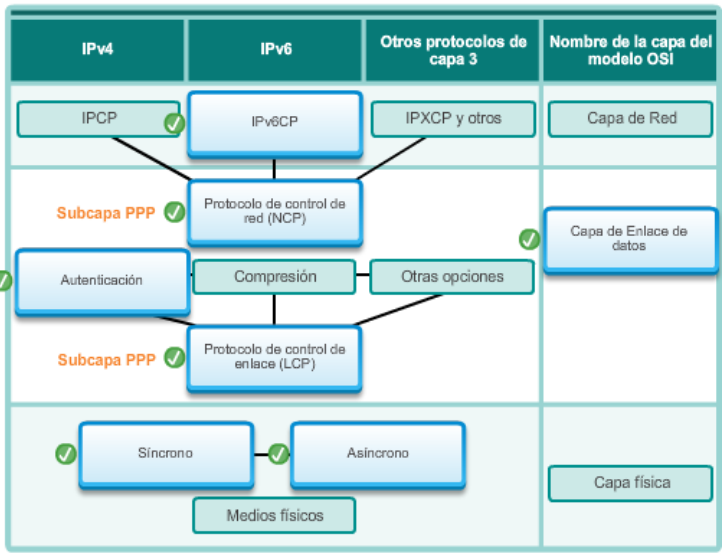
Los protocolos LCP pueden negociar modificaciones a la estructura de la trama PPP estándar. No obstante, las tramas modificadas siempre se distinguen de las tramas estándar.

Campos de la trama PPP



Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.2.2.5 Actividad: Identificar las características y las operaciones de PPP

Actividad (parte 1): Identificar las características y las operaciones de PPP
Arrastre las etiquetas de la arquitectura en capas de PPP hasta los campos correspondientes para ordenar la operación en el diagrama de arquitectura de red en capas. No utilizará todas las etiquetas. Haga clic en el botón 2 para continuar la actividad.



HDLC

Capa de Transporte

Multisíncrono

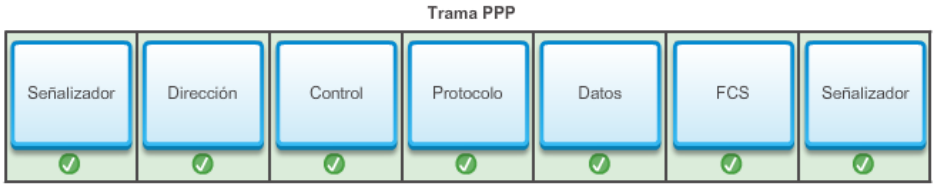
Actividad (parte 2): Identificar las funciones de LCP y NCP
Haga clic en el campo correspondiente para determinar si cada característica describe a LCP o NCP. Haga clic en el botón 3 para continuar la actividad.

Correcto

Identificó correctamente las características de LCP y NCP. Haga clic en el botón 3 para continuar.

	LCP	NCP
Negocia y configura las opciones de control en el circuito WAN.	✓	
Administra paquetes de varios protocolos de capa de red.		✓
Establece, configura y prueba la conexión de enlace de datos.	✓	
Termina el enlace.	✓	
Activa y desactiva los protocolos de capa de red.		✓
Determina si el enlace funciona correctamente.	✓	
Encapsula y negocia las opciones para IPv4, IPv6 e IPX.		✓

Actividad (parte 3): Identificar el formato de la trama PPP
Arrastre los nombres de los campos hasta los espacios correspondientes para ordenar los campos de la trama PPP en el formato estándar de dicha trama.



FCS

Dirección

Control

Datos

Señalizador

Protocolo

Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.2.3.1 Establecimiento de una sesión PPP

Hay tres fases de establecimiento de una sesión PPP, como se muestra en la ilustración:

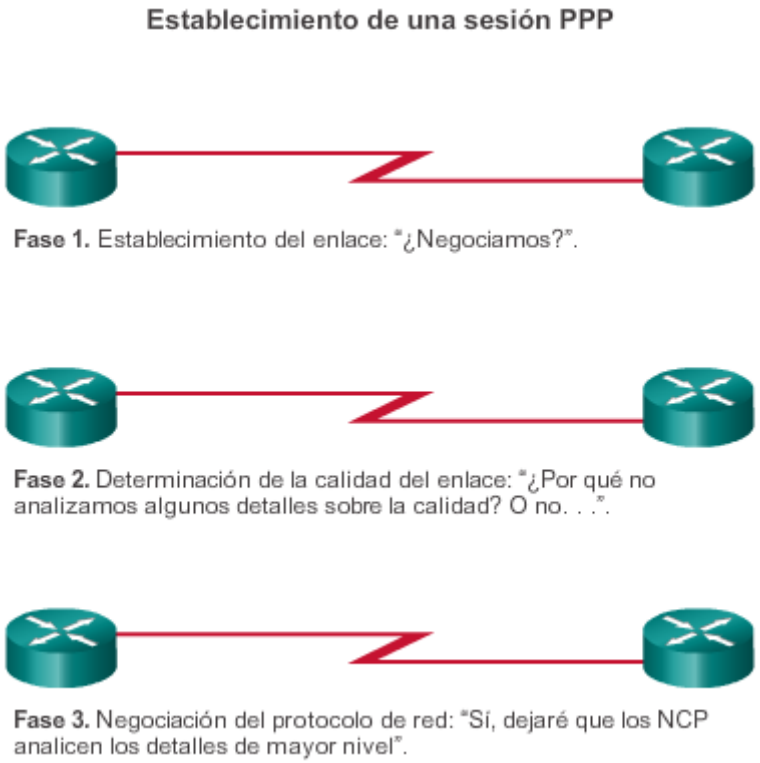
- **Fase 1, establecimiento del enlace y negociación de la configuración:**antes de que PPP intercambie cualquier datagrama de capa de red (como IP) LCP primero debe abrir la conexión y negociar las opciones de configuración. Esta fase se completa cuando el router receptor envía una trama de acuse de recibo de configuración de vuelta al router que inicia la conexión.

- **Fase 2, determinación de la calidad del enlace (optativa):** LCP prueba el enlace para determinar si la calidad de este es suficiente para activar protocolos de capa de red. LCP puede retrasar la transmisión de la información del protocolo de capa de red hasta que se complete esta fase.

- **Fase 3, negociación de la configuración del protocolo de capa de red:** una vez que LCP terminó la fase de determinación de la calidad del enlace, el protocolo NCP correspondiente puede configurar por separado los protocolos de capa de red, activarlos y desactivarlos en cualquier momento. Si LCP cierra el enlace, informa a los protocolos de 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 cierren el enlace, o hasta que ocurra algún evento externo, por ejemplo, que caduque un temporizador de inactividad o que intervenga un administrador.

LCP puede finalizar el enlace en cualquier momento. Por lo general, esto se realiza cuando uno de los routers solicita la finalización, pero puede suceder debido a un evento físico, como la pérdida de una portadora o el vencimiento de un temporizador de período inactivo.



Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.2.3.2 Funcionamiento de LCP

El funcionamiento de LCP incluye las disposiciones para el establecimiento, el mantenimiento y la finalización de enlaces. El funcionamiento de LCP utiliza tres clases de tramas LCP para lograr el trabajo de cada una de las fases de LCP:

- Las tramas de establecimiento de enlace establecen y configuran un enlace (solicitud de configuración, acuse de recibo de configuración, acuse de recibo negativo [NAK] de configuración y rechazo de configuración).

- Las tramas de mantenimiento de enlace administran y depuran un enlace (rechazo de código, rechazo de protocolo, solicitud de eco, respuesta de eco y solicitud de descarte).

- Las tramas de terminación de enlace terminan un enlace (solicitud de terminación y acuse de recibo de terminación).

Establecimiento del enlace

El establecimiento del enlace es la primera fase de una operación LCP, como se observa en la figura 1. Esta fase se debe completar correctamente antes de que se intercambie cualquier paquete de capa de red. Durante el establecimiento del enlace, LCP abre una conexión y negocia los parámetros de configuración. El proceso de establecimiento del enlace comienza cuando el dispositivo de inicio envía una trama de solicitud de configuración al respondedor. La trama de solicitud de configuración incluye una cantidad variable de opciones de configuración necesarias para configurar en el enlace.

El iniciador incluye las opciones para la forma en que desea que se cree el enlace, incluidos los parámetros de protocolo o de autenticación. El respondedor procesa la solicitud:

- Si las opciones no son aceptables o no se reconocen, el respondedor envía un mensaje de NAK de configuración o de rechazo de configuración. Si esto sucede y la negociación falla, el iniciador debe reiniciar el proceso con nuevas opciones.

- Si las opciones son aceptables, el respondedor responde con un mensaje de acuse de recibo de configuración, y el proceso pasa a la fase de autenticación. La operación del enlace se entrega a NCP.

Una vez que NCP completó todas las configuraciones necesarias, incluida la validación de la autenticación si se configuró, la línea está disponible para la transferencia de datos. Durante el intercambio de datos, LCP pasa al mantenimiento del enlace.

Mantenimiento del enlace

Durante el mantenimiento del enlace, LCP puede utilizar mensajes para proporcionar comentarios y probar el enlace, como se muestra en la figura 2.

- **Solicitud de eco, respuesta de eco y solicitud de descarte:** estas tramas se pueden utilizar para probar el enlace.

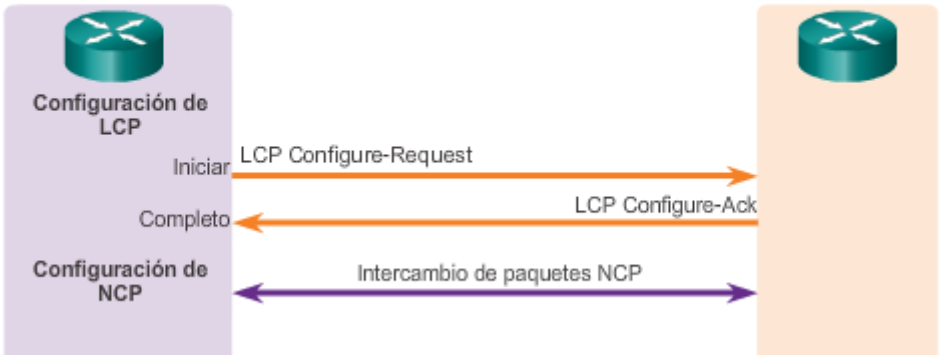
- **Rechazo de código y rechazo de protocolo:** estos tipos de tramas proporcionan comentarios cuando un dispositivo recibe una trama no válida debido a un código LCP desconocido (tipo de trama LCP) o a un identificador de protocolo defectuoso. Por ejemplo, si se recibe un paquete interpretable del peer, se envía un paquete rechazo de código en respuesta. El dispositivo emisor vuelve a enviar el paquete.

Terminación del enlace

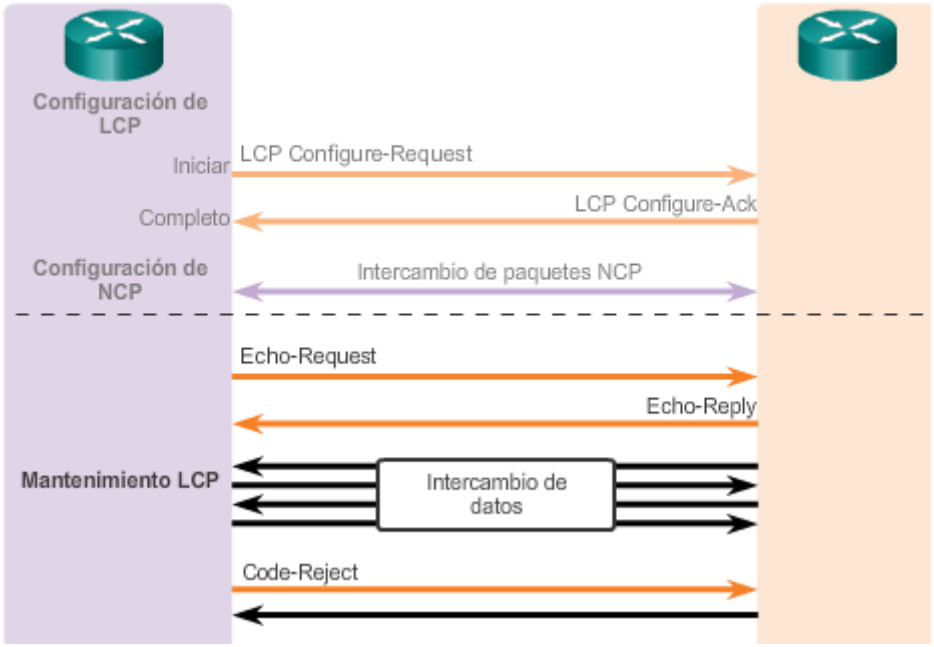
Una vez finalizada la transferencia de datos en la capa de red, LCP termina el enlace, como se muestra en la figura 3. NCP solo termina el enlace NCP y de capa de red. El enlace permanece abierto hasta que LCP lo termina. Si LCP termina el enlace antes que NCP, también se termina la sesión NCP.

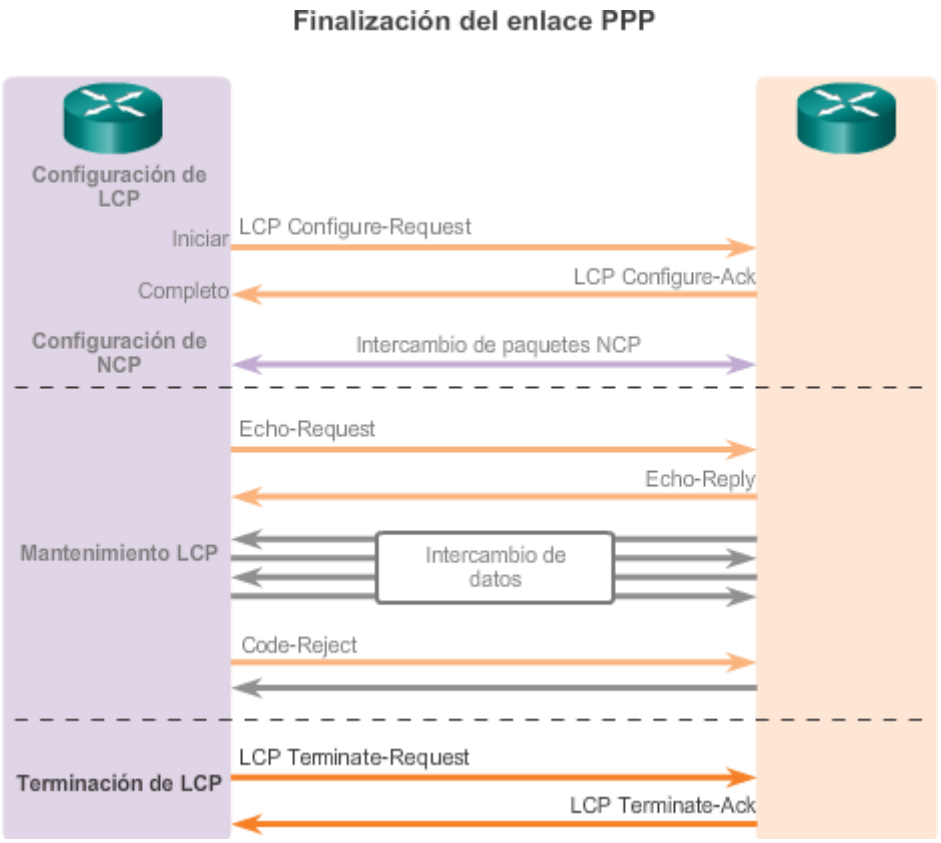
PPP puede terminar el enlace en cualquier momento. Esto podría suceder debido a la pérdida de la portadora, a un error de autenticación, a una falla de la calidad del enlace, al vencimiento de un temporizador de período inactivo o al cierre administrativo del enlace. LCP cierra el enlace mediante el intercambio de paquetes de terminación. El dispositivo que inicia la desactivación envía un mensaje de solicitud de terminación. El otro dispositivo responde con un mensaje de acuse de recibo de terminación. Una solicitud de terminación indica que el dispositivo que la envía necesita cerrar el enlace. Cuando se cierra el enlace, PPP informa a los protocolos de capa de red para que puedan tomar las medidas adecuadas.

Establecimiento del enlace PPP



Mantenimiento del enlace PPP





Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.2.3.3 Paquete LCP

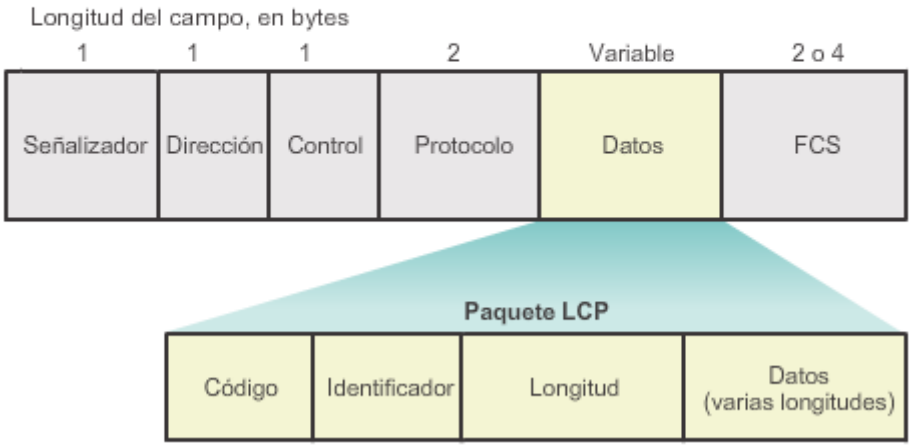
En la figura 1, se muestran los campos en un paquete LCP:

- **Código:** el campo Código tiene una longitud de 1 byte e identifica el tipo de paquete LCP.
- **Identificador:** el campo Identificador tiene una longitud de 1 byte y se usa para establecer coincidencias entre solicitudes y respuestas de paquetes.
- **Longitud:** el campo Longitud tiene una longitud de 2 bytes e indica la longitud total (incluidos todos los campos) del paquete LCP.
- **Datos:** el campo de datos consta de 0 o más bytes, según lo que indique el campo Longitud. El formato de este campo es determinado por el código.

Cada paquete LCP es un único mensaje LCP que consta de un campo Código que identifica el tipo de paquete LCP, un campo Identificador para establecer coincidencias entre solicitudes y respuestas, y un campo Longitud que indica el tamaño del paquete LCP y los datos específicos del tipo de paquete LCP.

Cada paquete LCP tiene una función específica en el intercambio de la información de configuración según el tipo de paquete. El campo Código de los paquetes LCP identifica el tipo de paquete, según la figura 2.

Códigos de paquete LCP



Campos de paquete LCP

Código LCP	Tipo de paquete LCP	Descripción
1	Solicitud de configuración	Se envía para abrir o restablecer una conexión PPP. El mensaje de solicitud de configuración contiene una lista de opciones LCP con cambios para los valores de las opciones predeterminadas.
2	Acuse de recibo de configuración	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	NAK de configuración	Se envía cuando se reconocen todas las opciones de LCP, pero los valores de algunas opciones no son aceptables. El mensaje de acuse de recibo negativo (NAK) de configuración incluye las opciones que presentan la incompatibilidad y los valores aceptables.
4	Rechazo de configuración	Enviado cuando las opciones de LCP no son reconocidas o aceptadas para la negociación. El mensaje de rechazo de configuración incluye las opciones no reconocidas o no negociables.
5	Solicitud de terminación	Se envía opcionalmente para cerrar la conexión PPP.
6	Acuse de recibo de terminación	Se envía en respuesta al mensaje de solicitud de terminación.
7	Rechazo de código	Se envía cuando se desconoce el código LCP. El mensaje de rechazo de código incluye el paquete LCP rechazado.
8	Rechazo de protocolo	Se envía cuando la trama PPP contiene una ID de protocolo desconocida. El mensaje de rechazo de protocolo incluye el paquete LCP rechazado. El mensaje de rechazo de protocolo 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	Solicitud de eco	Se envía opcionalmente para probar la conexión PPP.
10	Respuesta de eco	Se envía en respuesta a un mensaje de solicitud de eco. Los mensajes de solicitud de eco y de respuesta de eco de PPP no están relacionados con los mensajes del mismo nombre de ICMP.
11	Solicitud de descarte	Se envía opcionalmente para practicar el enlace en la dirección de salida.

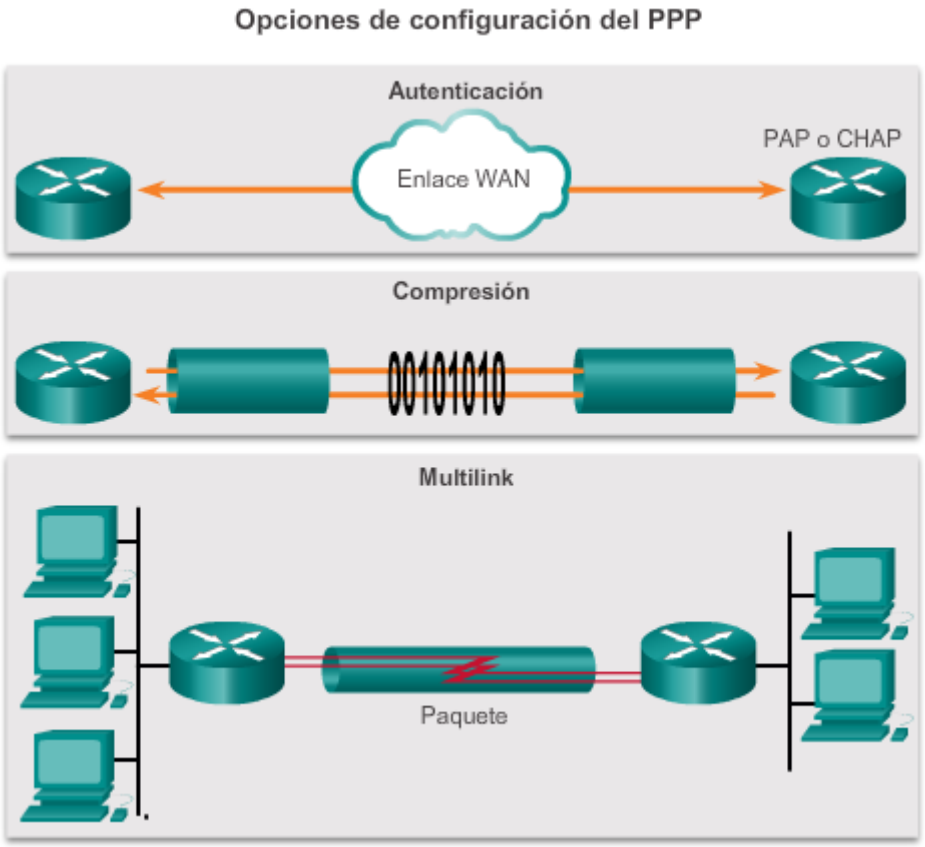
Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.2.3.4 Opciones de configuración del PPP

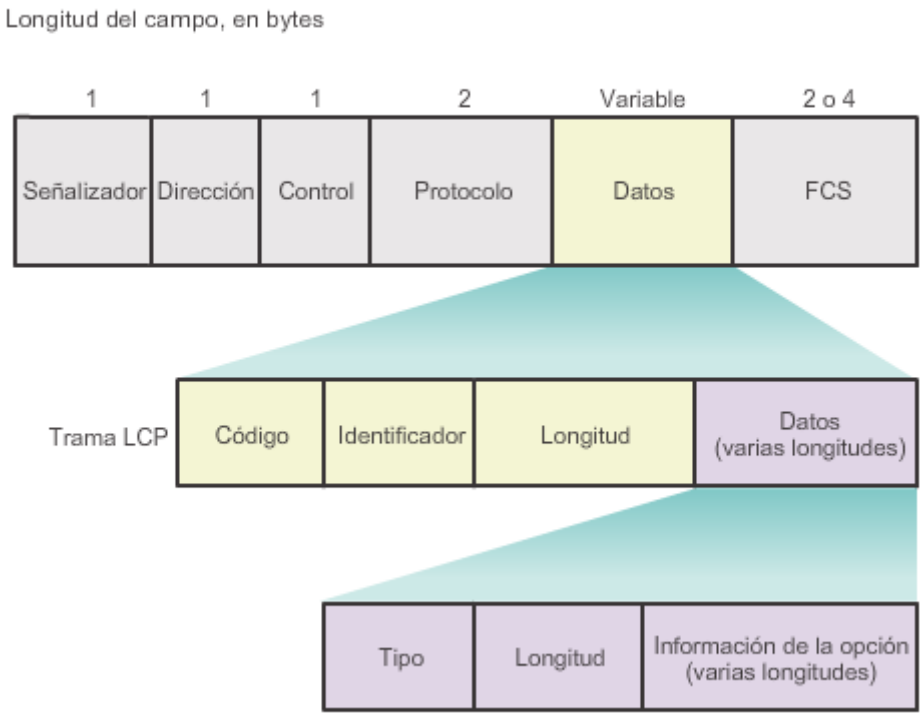
PPP se puede configurar para admitir diversas funciones optativas, como se muestra en la figura 1. Estas funciones optativas incluyen lo siguiente:

- Autenticación mediante PAP o CHAP
- Compresión mediante Stacker o Predictor
- Multienlace que combina dos o más canales para aumentar el ancho de banda WAN

Para negociar el uso de estas opciones de PPP, las tramas de establecimiento de enlace LCP incluyen información de la opción en el campo de datos de la trama LCP, como se muestra en la figura 2. Si no se incluye una opción de configuración en una trama LCP, se supone el valor predeterminado para esa opción de configuración.

Esta fase se completa cuando se envía y se recibe una trama de acuse de recibo de la configuración.





Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.2.3.5 Explicación de NCP

Proceso NCP

Una vez que se inició el enlace, LCP entrega el control al protocolo NCP correspondiente.

Si bien en los inicios se diseñó para los paquetes IP, PPP puede transportar datos de varios protocolos de capa de red mediante un enfoque modular en su implementación. El modelo modular de PPP permite que LCP configure el enlace y transfiera los detalles de un protocolo de red a un protocolo NCP específico. Cada protocolo de red tiene un NCP correspondiente, y cada NCP tiene un RFC correspondiente.

Hay NCP para IPv4, IPv6, IPX, AppleTalk y muchos otros. Los protocolos NCP usan el mismo formato de paquetes que los protocolos LCP.

Una vez que LCP configuró y autenticó el enlace básico, se invoca el protocolo NCP correspondiente para completar la configuración específica del protocolo de capa de red que se usa. Cuando NCP configuró correctamente el protocolo de capa de red, este se encuentra en estado abierto en el enlace LCP establecido. En este momento, PPP puede transportar los paquetes correspondientes del protocolo de capa de red.

Ejemplo de IPCP

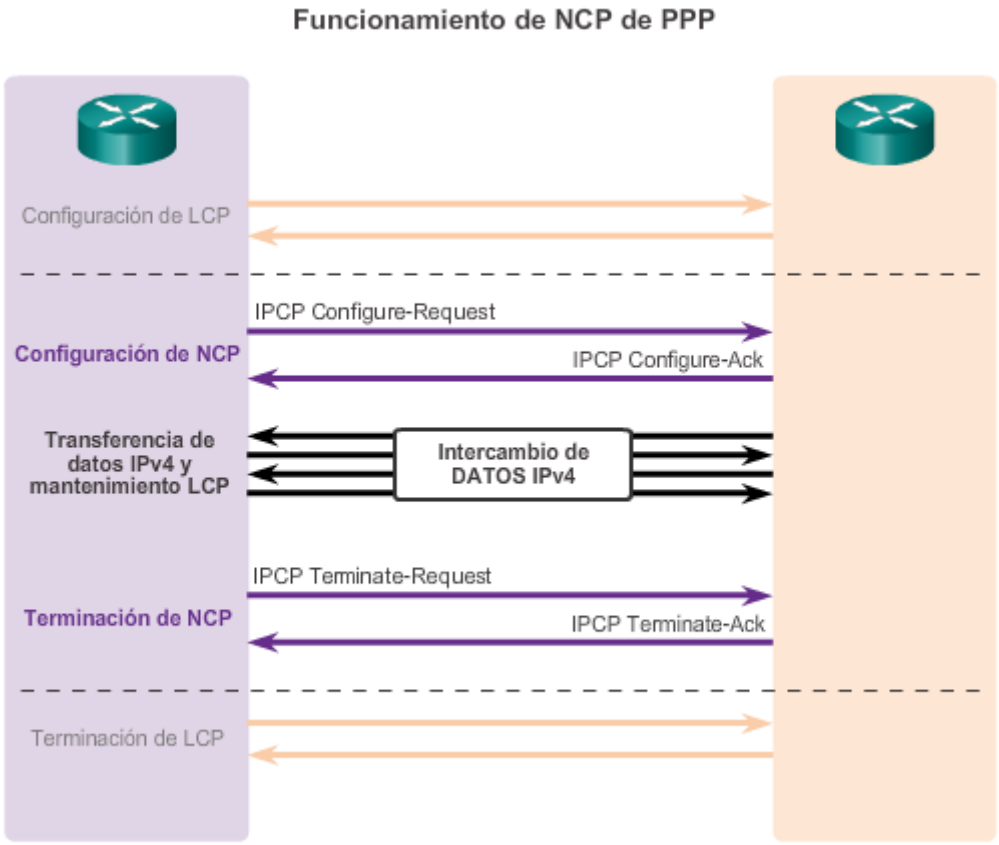
Como ejemplo de cómo funciona la capa NCP, en la ilustración se muestra la configuración NCP de IPv4, que es el protocolo de capa 3 más común. Una vez que LCP estableció el enlace, los routers intercambian mensajes IPCP para negociar opciones específicas del protocolo IPv4. IPCP es responsable de la configuración, la habilitación y la deshabilitación de los módulos IPv4 en ambos extremos del enlace. IPV6CP es un protocolo NCP con las mismas responsabilidades para IPv6.

IPCP negocia dos opciones:

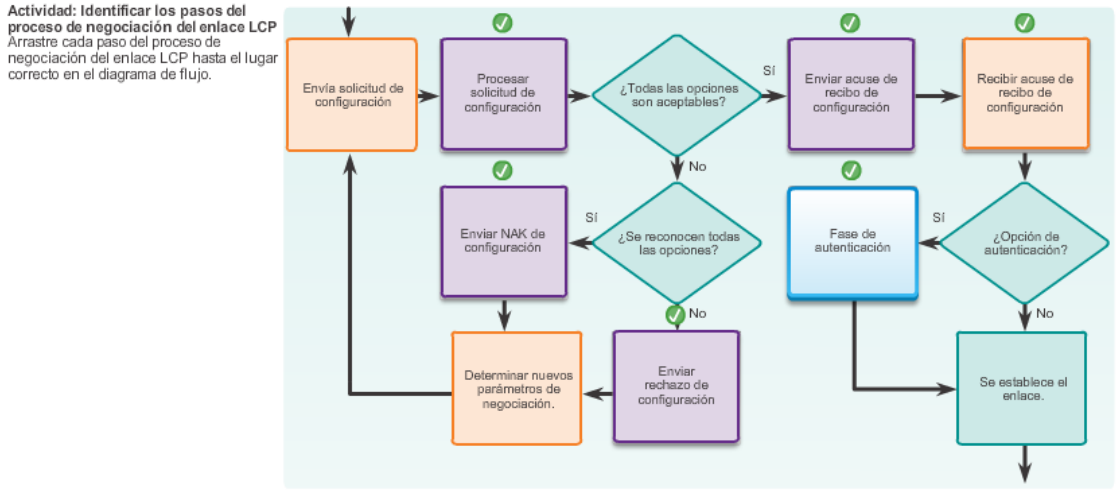
- **Compresión:** permite que los dispositivos negocien un algoritmo para comprimir encabezados TCP e IP, y ahorrar ancho de banda. La compresión de encabezados TCP/IP de Van Jacobson reduce los encabezados TCP/IP a un tamaño de hasta 3 bytes. Esto puede ser una mejora considerable en las líneas seriales lentas, en particular para el tráfico interactivo.

- **Dirección IPv4:** permite que el dispositivo de inicio especifique una dirección IPv4 para utilizar en el routing IP a través del enlace PPP, o para solicitar una dirección IPv4 para el respondedor. Antes de la llegada de las tecnologías de banda ancha como los servicios de DSL y de cable módem, los enlaces de red de dial-up normalmente usaban la opción de dirección IPv4.

Una vez que se completa el proceso NCP, el enlace pasa al estado abierto, y LCP vuelve a tomar el control en la fase de mantenimiento del enlace. El tráfico del enlace consta de cualquier combinación posible de paquetes LCP, NCP y de protocolo de capa de red. Cuando se completa la transferencia de datos, NCP termina el enlace del protocolo; LCP finaliza la conexión PPP.



Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.2.3.6 Actividad: Identificar los pasos del proceso de negociación del enlace LCP



Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.3.1.1 Opciones de configuración del PPP

En la sección anterior, se presentaron las opciones configurables de LCP para satisfacer los requisitos específicos de las conexiones WAN. PPP puede incluir las siguientes opciones de LCP:

- **Autenticación:** los routers peers intercambian mensajes de autenticación. Las dos opciones de autenticación son: el protocolo de autenticación de contraseña (PAP, Password Authentication Protocol) y el protocolo de autenticación de intercambio de señales (CHAP, Challenge Handshake Authentication Protocol).

- **Compresión:** aumenta el rendimiento eficaz en las conexiones PPP al reducir la cantidad de datos que se deben transferir en la trama 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 fallas. Las opciones de calidad y número mágico contribuyen a asegurar el establecimiento de un enlace de datos confiable y sin bucles. El campo de número mágico ayuda a detectar enlaces que se encuentran en una condición de loop back. Hasta que no se negocie correctamente la opción de configuración de número mágico, este se debe transmitir como cero. Los números mágicos se generan de forma aleatoria en cada extremo de la conexión.

- **Devolución de llamada PPP:** la devolución de llamada PPP se usa para mejorar la seguridad. Con esta opción de LCP, un router Cisco puede funcionar como cliente o servidor de devolución de llamada. El cliente realiza la llamada inicial, solicita que el servidor le devuelva la llamada y termina la comunicación inicial. El router de devolución de llamada responde la llamada inicial y se comunica con el cliente sobre la base de sus instrucciones de configuración. El comando es **ppp callback**[**accept** | **request**].

- **Multienlace:** esta alternativa proporciona balanceo de carga a través de las interfaces del router que PPP utiliza. El protocolo PPP multienlace, también conocido como MP, MPPP, MLP o multienlace, proporciona un método para propagar el tráfico a través de varios enlaces WAN físicos a la vez que proporciona la fragmentación y el rearmado de paquetes, la secuenciación adecuada, la interoperabilidad con varios proveedores y el balanceo de carga del tráfico entrante y saliente.

Cuando se configuran las opciones, se inserta el valor de campo correspondiente en el campo de opción de LCP.

Códigos de campo de opciones configurables

Nombre de la opción	Tipo de opción	Longitud de la opción	Descripción
Protocolo de autenticación	3	5 o 6	Este campo indica el protocolo de autenticación, ya sea el PAP o el CHAP.
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.
Número mágico (detección de errores)	5	6	Es un número elegido de manera aleatoria para distinguir un par y detectar las líneas de loopback.
Devolución de llamada	13 o 0x0D	3	Un indicador de 1 octeto que muestra cómo se determinan las devoluciones de llamadas.

Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.3.1.2 Comando de configuración básica de PPP

Habilitación de PPP en una interfaz

Para establecer PPP como el método de encapsulación que usa una interfaz serial, utilice el comando de configuración de interfaz **encapsulation ppp**.

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

R3# **configure terminal**

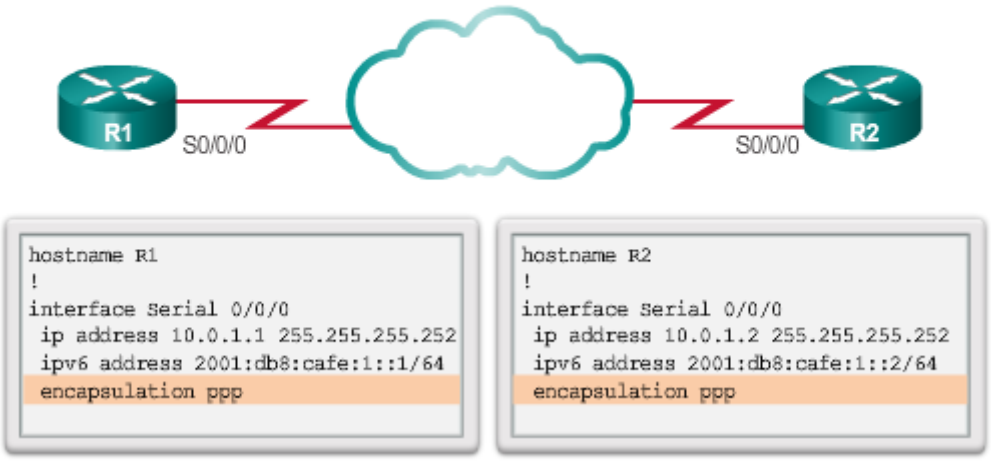
R3(config)# **interface serial 0/0/0**

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

El comando de interfaz **encapsulation ppp** no tiene ningún argumento. Recuerde que si no se configura PPP en un router Cisco, la encapsulación predeterminada para las interfaces seriales es HDLC.

En la ilustración, se muestra que los routers R1 y R2 se configuraron con una dirección IPv4 y una dirección IPv6 en las interfaces seriales. PPP es una encapsulación de capa 2 que admite varios protocolos de capa 3, incluidos IPv4 e IPv6.

Configuración básica de PPP



Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.3.1.3 Comandos de compresión de PPP

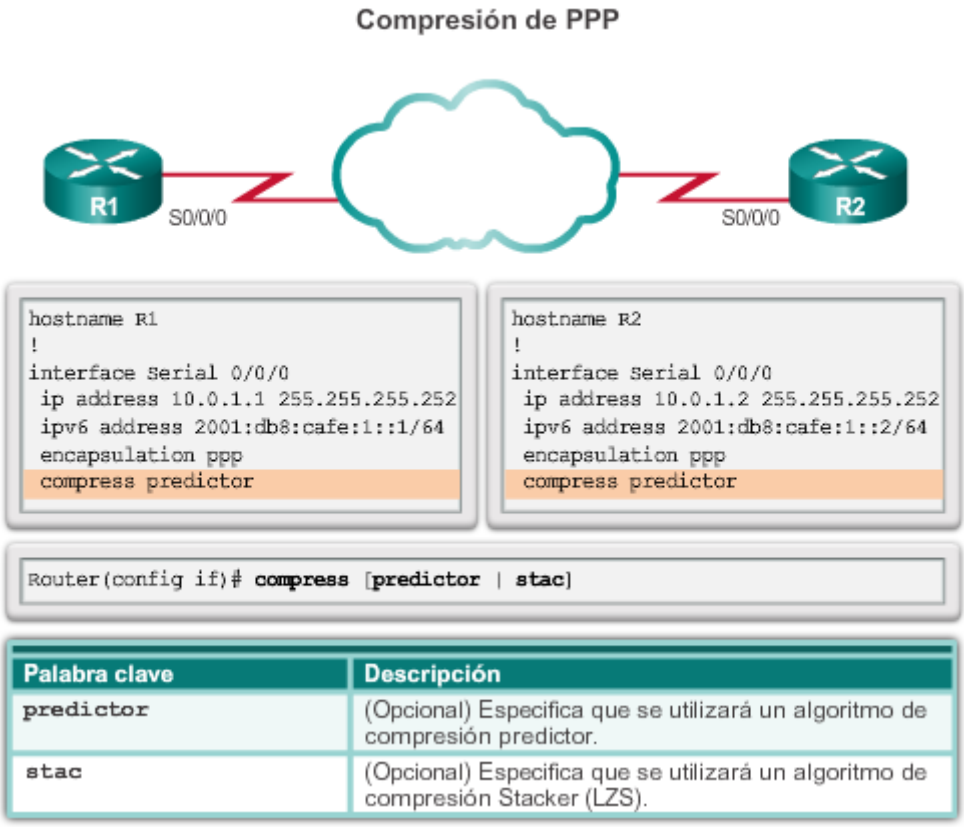
La compresión de software de punto a punto en las interfaces seriales se puede configurar después de que se habilita la encapsulación PPP. Dado que esta opción invoca un proceso de compresión de software, puede afectar el rendimiento del sistema. Si el tráfico ya consta de archivos comprimidos, como .zip, .tar, o .mpeg, no utilice esta opción. En la ilustración, se muestra la sintaxis del comando**compress**.

Para configurar la compresión a través de PPP, introduzca los siguientes comandos:

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

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

R3(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).

Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.3.1.4 Comando de control de calidad del enlace PPP

Recuerde que LCP proporciona una fase optativa de determinación de la calidad del enlace. En esta fase, LCP prueba el enlace para determinar si la calidad de este es suficiente para usar protocolos de capa 3.

El comando **ppp quality** *percentage*asegura que el enlace cumpla con el requisito de calidad establecido; de lo contrario, el enlace queda inactivo.

Los porcentajes se calculan para las direcciones entrantes y salientes. La calidad de salida se calcula comparando la cantidad total de paquetes y bytes enviados con la cantidad total de paquetes y bytes que recibe el nodo de destino. La calidad de entrada se calcula comparando la cantidad total de paquetes y bytes recibidos con la cantidad total de paquetes y bytes que envía el nodo de destino.

Si el porcentaje de la calidad del enlace no se mantiene, el enlace se considera de baja calidad y se desactiva. El control de calidad del enlace (LQM) implementa un retraso de tiempo de modo que el enlace no rebote de un lado a otro.

El siguiente ejemplo de configuración controla los datos descartados en el enlace y evita que las tramas formen bucles, como se muestra en la figura 1:

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

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

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

Utilice el comando **no ppp quality** para deshabilitar LQM.

Utilice el verificador de sintaxis de la figura 2 para configurar la encapsulación, la compresión y LQM de PPP en la interfaz Serial 0/0/1 del router R1.

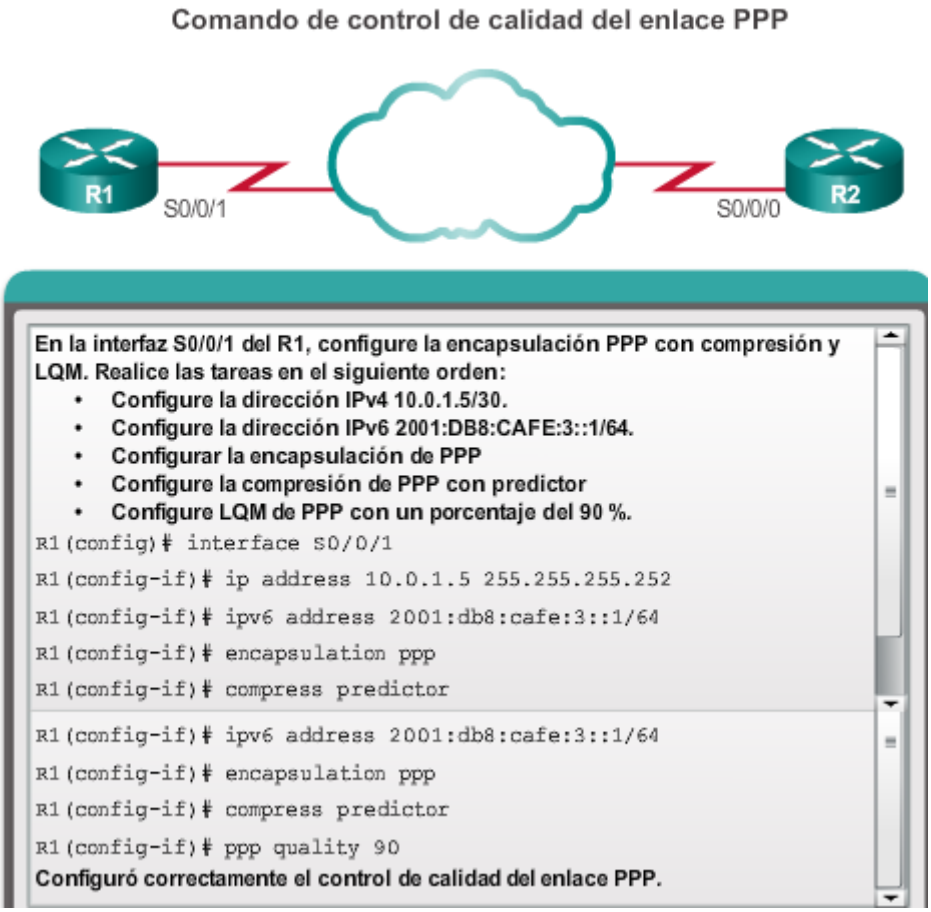
Control de calidad del enlace PPP


```
hostname R1
!
interface Serial 0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:db8:cafe:1::1/64
 encapsulation ppp
 ppp quality 80
```

```
hostname R2
!
interface Serial 0/0/0
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 encapsulation ppp
 ppp quality 80
```

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

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



Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.3.1.5 Comandos de PPP multienlace

El protocolo PPP multienlace (también conocido como MP, MPPP, MLP o multienlace) proporciona un método para propagar el tráfico a través de varios enlaces WAN físicos. Además, el protocolo PPP multienlace proporciona la fragmentación y el rearmado de paquetes, la secuenciación adecuada, la interoperabilidad con varios proveedores y el balanceo de carga del tráfico entrante y saliente.

MPPP permite fragmentar los paquetes y enviarlos simultáneamente a la misma dirección remota a través de varios enlaces punto a punto. Todos los enlaces físicos se activan en respuesta a un umbral de carga definido por el usuario. MPPP puede medir la carga solo en el tráfico entrante o solo en el tráfico saliente, pero no la carga combinada del tráfico entrante y saliente.

La configuración de MPPP requiere dos pasos, como se muestra en la ilustración.

Paso 1. Cree un grupo multienlace.

- El comando **interface multilink***number* crea la interfaz de multienlace.

- En el modo de configuración de interfaz, se asigna una dirección IP a la interfaz de multienlace. En este ejemplo, se configuran direcciones IPv4 e IPv6 en los routers R3 y R4.

- La interfaz está habilitada para el protocolo PPP multienlace.

- Se asigna un número de grupo multienlace a la interfaz.

Paso 2. Asigne las interfaces al grupo multienlace.

Cada interfaz que forma parte del grupo multienlace tiene las siguientes características:

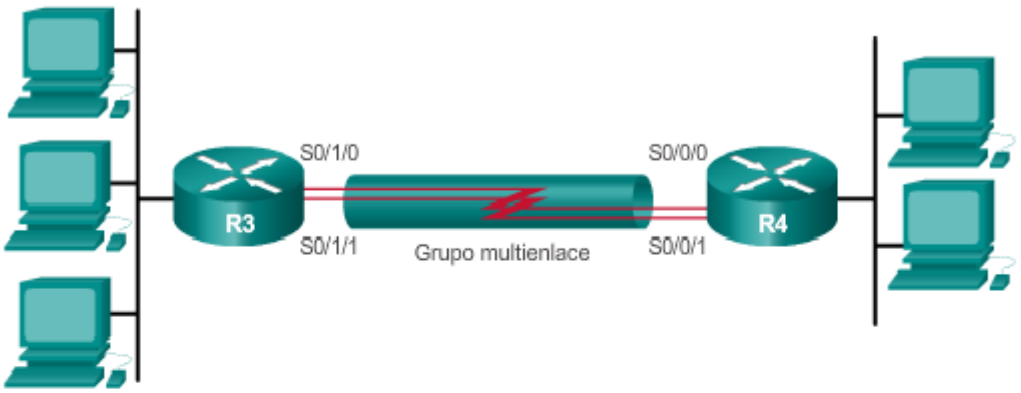
- Está habilitada para la encapsulación PPP.

- Está habilitada para el protocolo PPP multienlace.

- Está vinculada al grupo multienlace mediante el número de grupo multienlace configurado en el paso 1.

Para deshabilitar el protocolo PPP multienlace, use el comando **no ppp multilink**.

Protocolo PPP multienlace




```
hostname R3
!
interface Multilink 1
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:db8:cafe:1::1/64
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/1/0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/1/1
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
```

```
hostname R4
!
interface Multilink 1
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/0/0
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
!
interface Serial 0/0/1
 no ip address
 encapsulation ppp
 ppp multilink
 ppp multilink group 1
```

Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.3.1.6 Verificación de la configuración de PPP

Utilice el comando **show interfaces serial** para verificar la configuración de la encapsulación PPP o HDLC. El resultado del comando en la figura 1 muestra una configuración PPP.

Cuando configure HDLC, el resultado del**comando show interfaces serial**debe mostrar encapsulation HDLC. Cuando se configura PPP, también se muestran los estados de LCP y NCP. Observe que los protocolos NCP IPCP e IPV6CP están abiertos para IPv4 e IPv6, ya que el R1 y el R2 se configuraron con direcciones IPv4 e IPv6.

En la figura 2, se resumen los comandos que se usan para verificar PPP.

El comando **show ppp multilink**verifica que el protocolo PPP multienlace esté habilitado en el R3, como se muestra en la figura 3. El resultado indica la interfaz Multilink 1, los nombres de host de las terminales locales y remotas, y las interfaces seriales asignadas al grupo multienlace.

Verificación de la configuración de la encapsulación PPP serial

```
R2# show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.0.1.2/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, IPV6CP, CCP, CDPCP, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  Last input 00:00:02, output 00:00:02, output hang never
  Last clearing of "show interface" counters 01:29:06
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
```

Comandos de verificación de PPP

Comando	Descripción
show interfaces	Muestra estadísticas de todas las interfaces configuradas en el router.
show interfaces serial	Muestra información sobre una interfaz serial.
show ppp multilink	Muestra información sobre una interfaz PPP multienlace.

Verificación del protocolo PPP multienlace

```
R3# show ppp multilink

Multilink1
  Bundle name: R4
  Remote Endpoint Discriminator: [1] R4
  Local Endpoint Discriminator: [1] R3
  Bundle up for 00:01:20, total bandwidth 3088, load 1/255
  Receive buffer limit 24000 bytes, frag timeout 1000 ms
    0/0 fragments/bytes in reassembly list
    0 lost fragments, 0 reordered
    0/0 discarded fragments/bytes, 0 lost received
    0x2 received sequence, 0x2 sent sequence
  Member links: 2 active, 0 inactive (max 255, min not set)
    Se0/1/1, since 00:01:20
    Se0/1/0, since 00:01:06
No inactive multilink interfaces
R3#
```

Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.3.2.1 Protocolos de autenticación

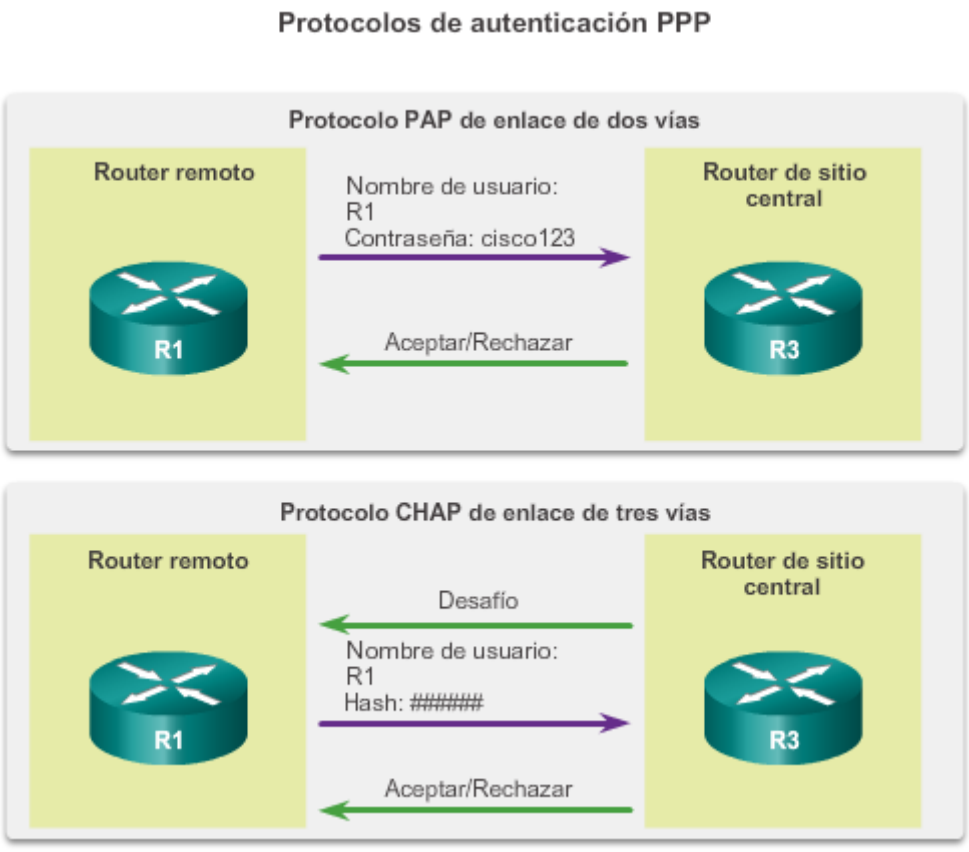
PPP

PPP define un protocolo LCP extensible que permite la negociación de un protocolo de autenticación para autenticar a los peers antes de permitir que los protocolos de capa de red transmitan por el enlace. RFC 1334 define dos protocolos para la autenticación, PAP y CHAP, los cuales se muestran en la ilustración.

PAP es un proceso bidireccional muy básico. No hay cifrado. El nombre de usuario y la contraseña se envían en texto no cifrado. Si se acepta, se permite la conexión. CHAP es más seguro que PAP. Implica un intercambio de tres vías de un secreto compartido.

La fase de autenticación de una sesión PPP es optativa. Si se utiliza, se autentica el peer después de que LCP establece el enlace y elige el protocolo de autenticación. Si se utiliza, la autenticación ocurre antes de que comience la fase de configuración del protocolo de capa de red.

Las opciones de autenticación requieren que la parte del enlace que llama introduzca la información de autenticación. Esto contribuye a asegurar que el usuario tenga permiso del administrador de red para realizar la llamada. Los routers pares intercambian mensajes de autenticación.



Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.3.2.2 Protocolo de autenticación de contraseña (PAP)

Una de las diversas características de PPP es que realiza la autenticación de capa 2 además de otras capas de autenticación, de cifrado, de control de acceso y de procedimientos de seguridad generales.

Inicio de PAP

PAP proporciona un método simple para que un nodo remoto establezca su identidad mediante un enlace bidireccional. PAP no es interactivo. Como se muestra en la figura 1, cuando se utiliza el comando **ppp authentication pap**, se envía el nombre de usuario y la contraseña como un paquete de datos LCP, en lugar de que el servidor envíe una solicitud de inicio de sesión y espere una respuesta. Una vez que PPP completa la fase de establecimiento del enlace, el nodo remoto envía repetidamente un par de nombre de usuario y contraseña a través del enlace hasta que el nodo receptor lo confirma o finaliza la conexión.

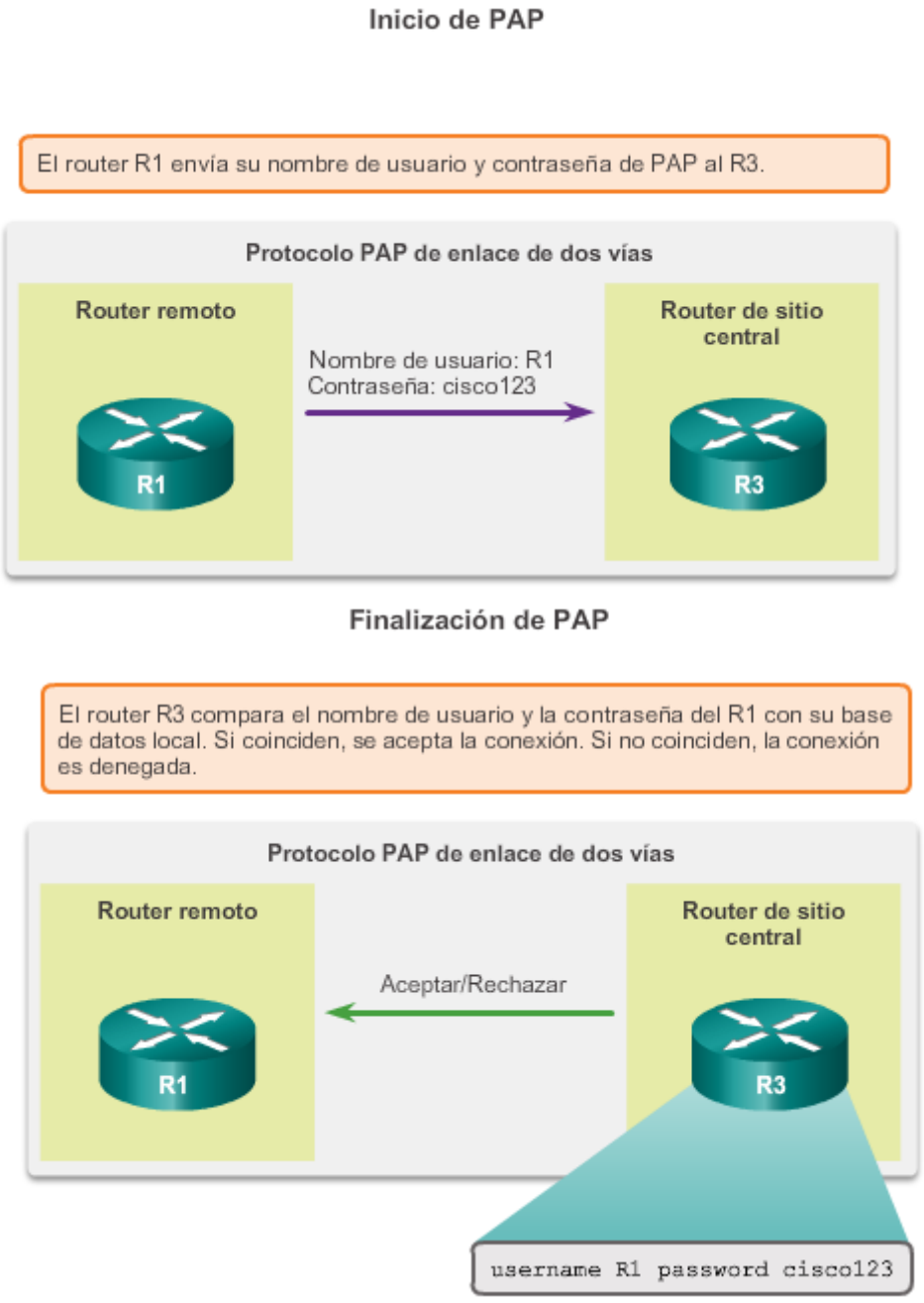
Finalización de PAP

En el nodo receptor, un servidor de autenticación que permite o deniega la conexión verifica el nombre de usuario y la contraseña. Se devuelve un mensaje de aceptación o rechazo al solicitante, como se muestra en la figura 2.

PAP no es un protocolo de autenticación seguro. Mediante PAP, las contraseñas se envían a través del enlace en texto no cifrado, y no existe protección contra los ataques de reproducción o los ataques repetidos de prueba y error. El nodo remoto tiene el control de la frecuencia y la temporización de los intentos de inicio de sesión.

No obstante, hay momentos en los que se justifica el uso de PAP. Por ejemplo, a pesar de sus limitaciones, PAP se puede utilizar en los siguientes entornos:

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



Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.3.2.3 Protocolo de autenticación de intercambio de señales (CHAP)

Una vez que se establece la autenticación con PAP, no se vuelve a autenticar. Esto deja la red vulnerable a los ataques. A diferencia de PAP, que autentica solo una vez, CHAP realiza desafíos periódicos para asegurar que el nodo remoto siga teniendo un valor de contraseña válido. El valor de contraseña varía y cambia de manera impredecible mientras existe el enlace.

Una vez completa la fase de establecimiento del enlace PPP, el router local envía un mensaje de desafío al nodo remoto, como se muestra en la figura 1.

El nodo remoto responde con un valor calculado mediante una función de hash unidireccional, que suele ser la síntesis del mensaje 5 (MD5), según la contraseña y el mensaje de desafío, como se muestra en la figura 2.

El router local compara la respuesta con su propio cálculo del valor de hash esperado. Si los valores coinciden, el nodo de inicio reconoce la autenticación, como se muestra en la figura 3. Si el valor no coincide, el nodo de inicio finaliza la conexión de inmediato.

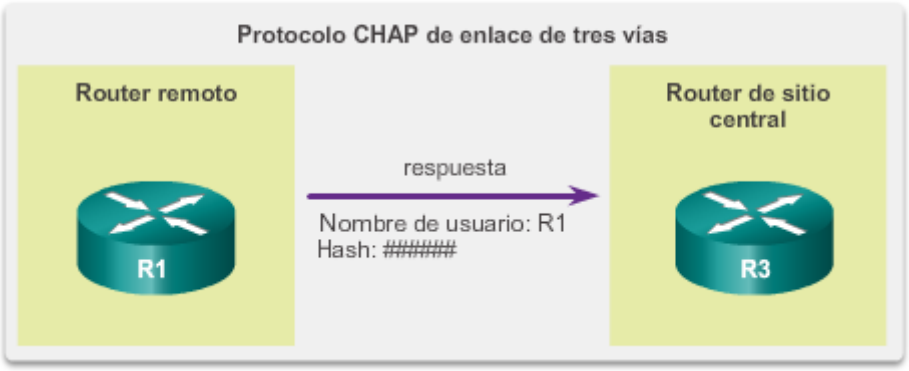
CHAP proporciona protección contra los ataques de reproducción mediante el uso de un valor de desafío variable que es exclusivo e impredecible. Como la comprobación es única y aleatoria, el valor hash resultante también es único y aleatorio. El uso de comprobaciones reiteradas limita el tiempo de exposición 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.

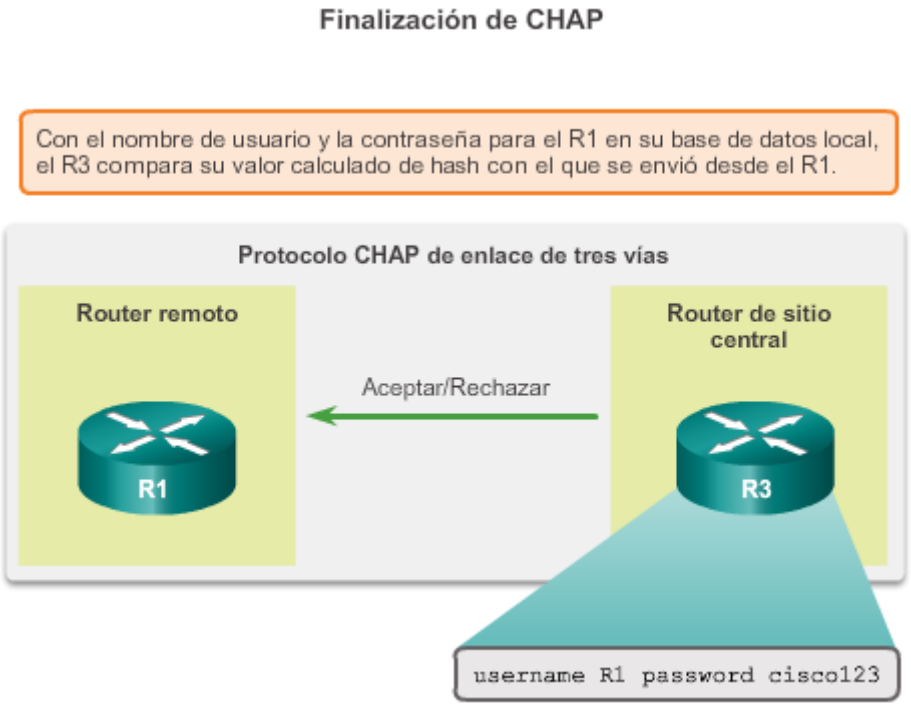
Inicio de CHAP

El router R3 inicia el protocolo de enlace de tres vías y envía un mensaje de desafío al R1.

Respuesta de CHAP

El R1 responde al desafío CHAP del R3 enviando su nombre de usuario de CHAP y un valor de hash que se basa en la contraseña de CHAP.





Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.3.2.4 Encapsulación y proceso de autenticación del PPP

El diagrama de flujo de la figura 1 se puede utilizar para ayudar a comprender el proceso de autenticación PPP al configurar este protocolo. El diagrama de flujo proporciona un ejemplo visual de las decisiones lógicas que toma PPP.

Por ejemplo, si una solicitud de PPP entrante no requiere autenticación, PPP avanza al siguiente nivel. Si una solicitud de PPP entrante requiere autenticación, se puede autenticar con la base de datos local o un servidor de seguridad. Como se muestra en el diagrama de flujo, si la autenticación es correcta, avanza al siguiente nivel; en cambio, si se produce una falla de autenticación, se desconecta y se descarta la solicitud de PPP entrante.

Siga los pasos a medida que avanza la animación de la figura 2 para ver cómo el R1 establece una conexión PPP autenticada con CHAP con el R2.

Paso 1. Primero, el R1 negocia la conexión del enlace con el router R2 mediante LCP y ambos sistemas acuerdan utilizar la autenticación CHAP durante la negociación LCP de PPP.

Paso 2. El R2 genera una ID y un número aleatorio, y los envía con su nombre de usuario como paquete de desafío CHAP al R1.

Paso 3. El R1 utiliza el nombre de usuario del desafiante (el R2) y lo compara con su base de datos local para encontrar la contraseña asociada. A continuación, el R1 genera un número de hash MD5 exclusivo usando el nombre de usuario, la ID, el número aleatorio y la contraseña secreta compartida del R2. En este ejemplo, la contraseña secreta compartida es “boardwalk”.

Paso 4. El router R1 envía la ID de desafío, el valor de hash y su nombre de usuario (R1) al R2.

Paso 5. El R2 genera su propio valor de hash mediante la ID, la contraseña secreta compartida y el número aleatorio que envió originalmente al R1.

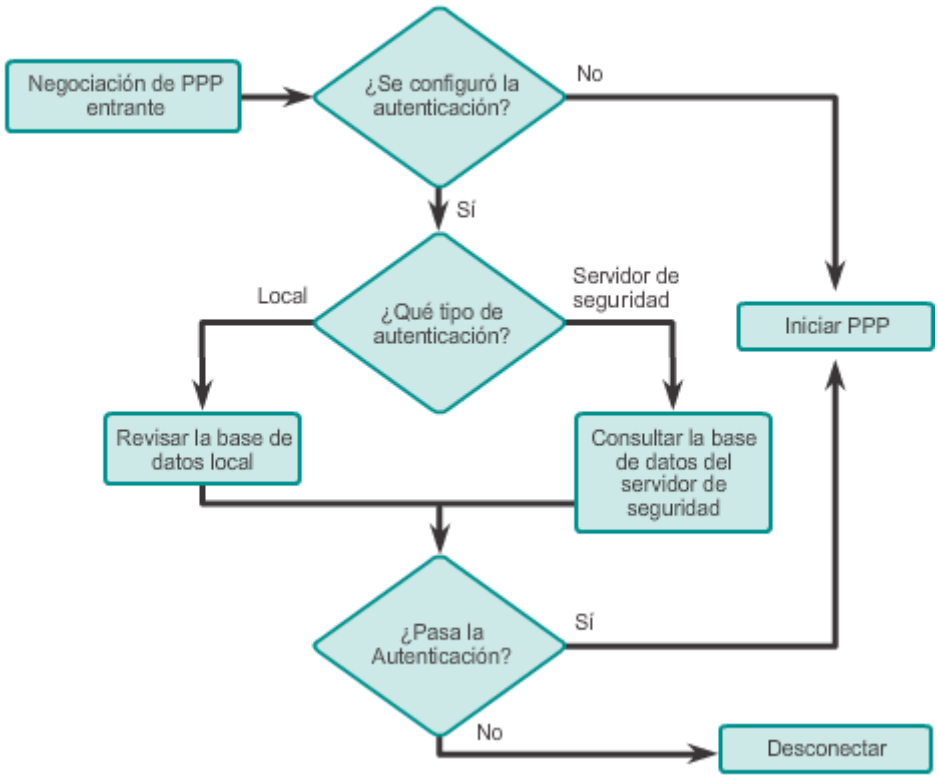
Paso 6. El R2 compara su valor de hash con el valor de hash que envió el R1. Si los valores son iguales, el R2 envía una respuesta de enlace establecido al R1.

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

- 04 = tipo de mensaje de falla CHAP
- id = se copia del paquete de respuesta
- "Authentication failure" o algún mensaje de texto similar, diseñado para ser una explicación que el usuario pueda leer

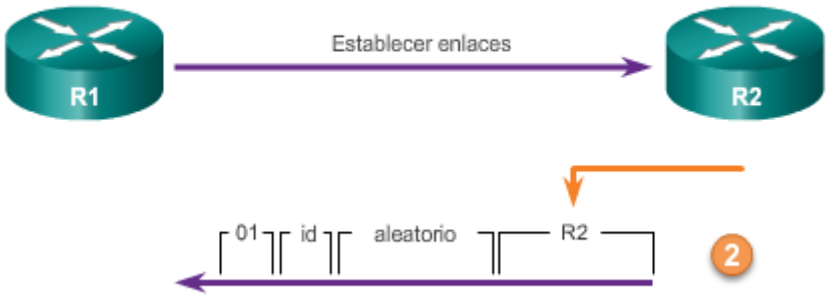
La contraseña secreta compartida debe ser idéntica en el R1 y el R2.

Encapsulación y proceso de autenticación del PPP

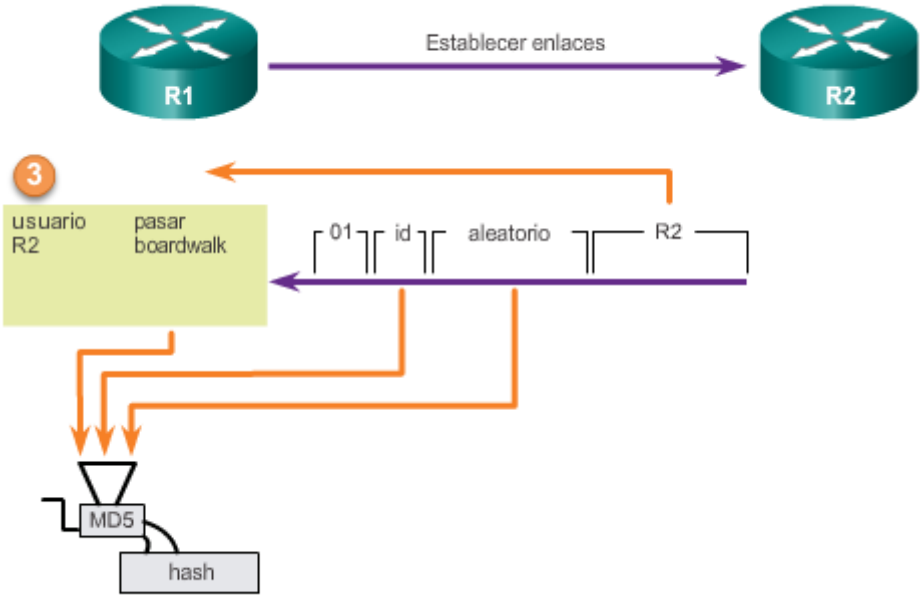


Ejemplo: proceso de autenticación de CHAP

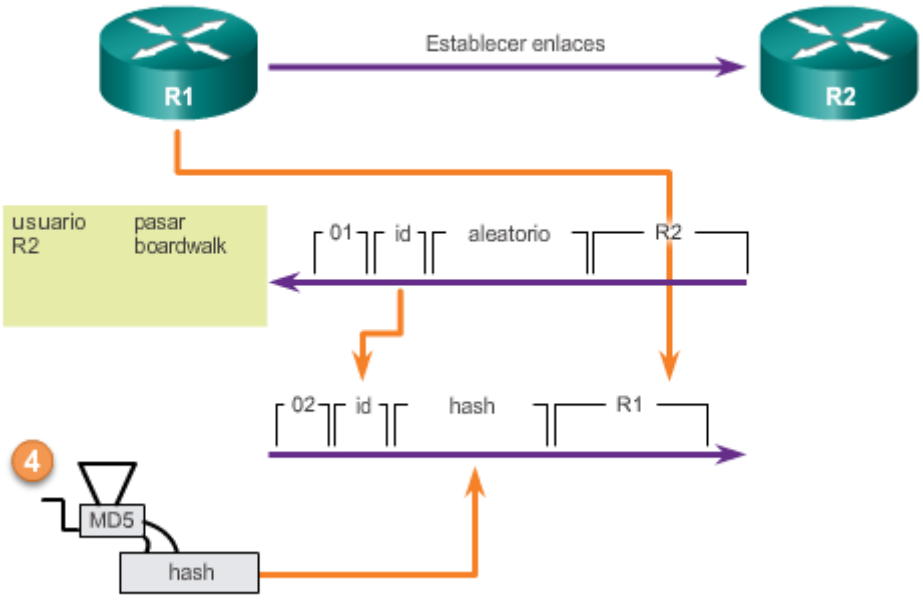
Ejemplo: proceso de autenticación de CHAP



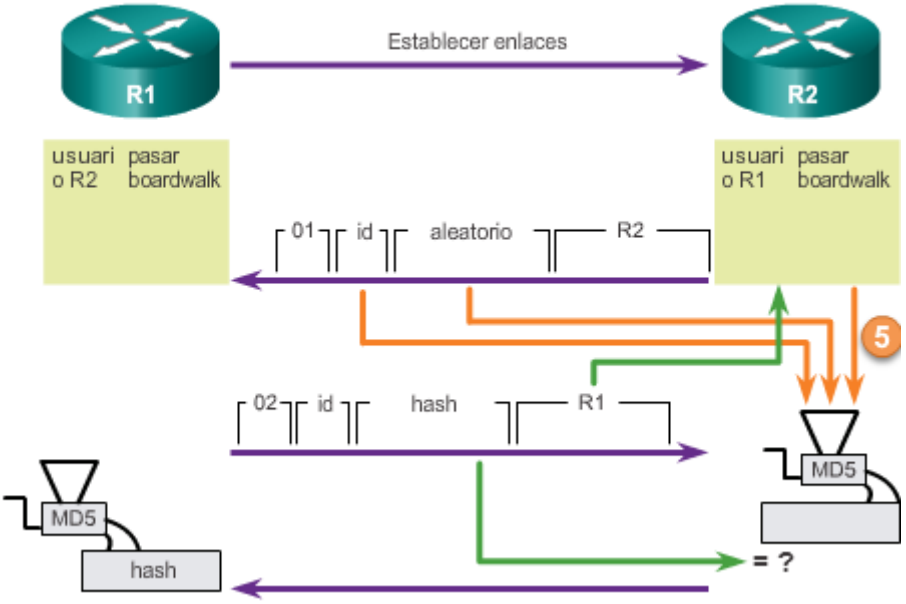
Ejemplo: proceso de autenticación de CHAP

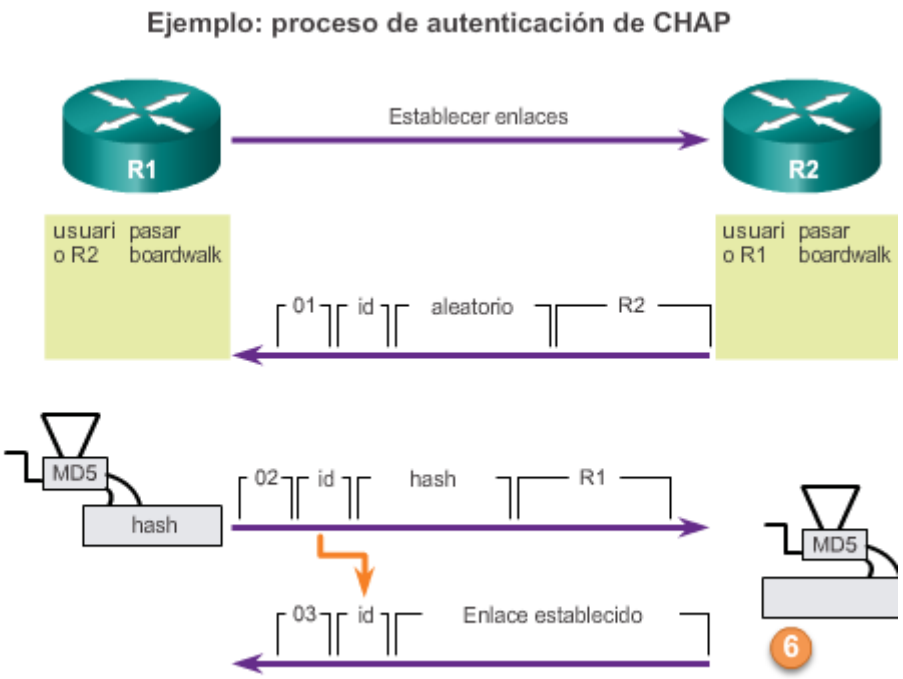


Ejemplo: proceso de autenticación de CHAP



Ejemplo: proceso de autenticación de CHAP





Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.3.2.5 Configuración de la autenticación PPP

Para especificar el orden en que se solicitan los protocolos CHAP o PAP en la interfaz, utilice el comando de configuración de interfaz **ppp authentication**, como se muestra en la ilustración. Utilice la versión **no** de este comando para deshabilitar esta autenticación.

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

- La autenticación PAP requiere que el dispositivo remoto envíe un nombre y una contraseña para compararlos con una entrada coincidente en la base de datos de nombres de usuario local o en la base de datos remota TACACS/TACACS+.

- La autenticación CHAP envía un desafío al dispositivo remoto. El dispositivo remoto debe cifrar el valor del desafío con un secreto compartido y devolver el valor cifrado y su nombre al router local en un mensaje de respuesta. El router local utiliza el nombre del dispositivo remoto para buscar el secreto correspondiente en el nombre de usuario local o la base de datos remota TACACS/TACACS+. Utiliza el secreto que buscó para cifrar el desafío original y verificar que los valores cifrados coincidan.

Nota: la autenticación, la autorización y la contabilidad (AAA)/TACACS es un servidor dedicado que se usa para autenticar usuarios. Los clientes TACACS envían una consulta a un servidor de autenticación TACACS. El servidor puede autenticar al usuario, autorizar lo que este puede hacer y hacer un seguimiento de lo que hizo.

Se puede habilitar tanto PAP como CHAP. Si ambos métodos están habilitados, se solicita el primer método especificado durante la negociación del enlace. Si el peer sugiere usar el segundo método o simplemente rechaza el primero, se debe probar con el segundo método. Algunos dispositivos remotos soportan sólo CHAP y algunos sólo PAP. El orden en que se especifican los métodos se basa en las preocupaciones sobre la capacidad del dispositivo remoto para negociar correctamente el método adecuado, así como la preocupación sobre la seguridad de la línea de datos. Los nombres de usuario y las contraseñas de PAP se envían como cadenas de texto no cifrado y se pueden interceptar y volver a utilizar. CHAP eliminó 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` (optativo)	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` (optativo)	Usado con AAA/TACACS+. Especifica el nombre de una lista de métodos de autenticación TACACS+ para usar. Si no se especifica ningún nombre de lista, el sistema utiliza el valor predeterminado. Las listas se crean con el comando **`aaa authentication ppp`** .
`default` (optativo)	Usado con AAA/TACACS+. Se crea con el comando **`aaa authentication ppp`** .
`callin`	Especifica la autenticación sólo en las llamadas entrantes (recibidas).

El procedimiento descrito en la tabla explica cómo configurar la encapsulación PPP y los protocolos de autenticación PAP y CHAP. La configuración correcta es fundamental, ya que CHAP y PAP utilizan estos parámetros para autenticar.

Configuración de la autenticación PAP

En la figura 1, se muestra un ejemplo de configuración de autenticación PAP bidireccional. Ambos routers se autentican entre sí, por lo que los comandos de autenticación PAP se reflejan. El nombre de usuario y la contraseña PAP que envía cada router deben coincidir con los especificados con el comando **username***name* **password** *password* del otro router.

PAP proporciona un método simple para que un nodo remoto establezca su identidad mediante un enlace bidireccional. Esto se realiza solo en el establecimiento del enlace inicial. El nombre de host en un router debe coincidir con el nombre de usuario que el otro router configuró para PPP. Las contraseñas también deben coincidir. Para especificar los parámetros de nombre de usuario y contraseña, utilice el siguiente comando: **ppp sent-username** *name***password** *password*.

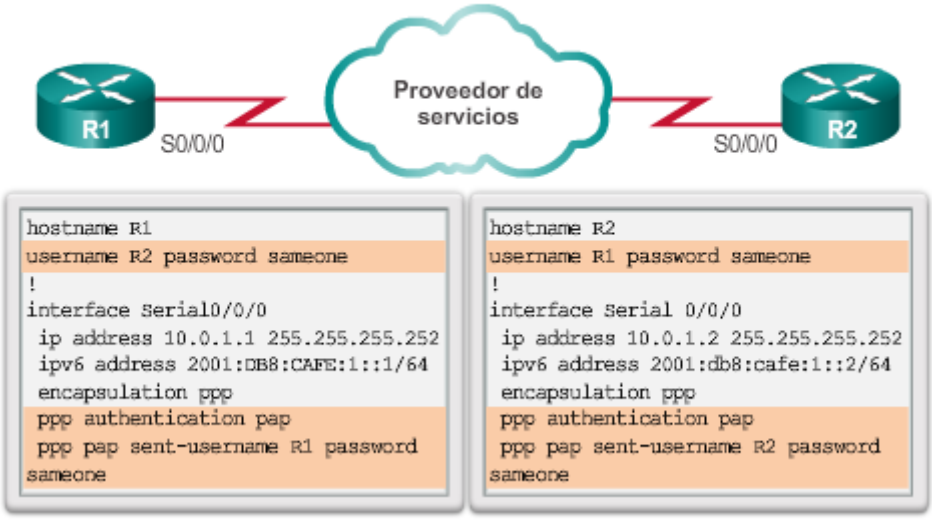
Utilice el verificador de sintaxis de la figura 2 para configurar la autenticación PPP en la interfaz serial 0/0/1 del router R1.

Configuración de la autenticación CHAP

CHAP verifica periódicamente la identidad del nodo remoto mediante un protocolo de enlace de tres vías. El nombre de host en un router debe coincidir con el nombre de usuario que configuró el otro router. Las contraseñas también deben coincidir. Esto ocurre en el establecimiento del enlace inicial y se puede repetir en cualquier momento después de que se estableció el enlace. En la figura 3, se muestra un ejemplo de una configuración CHAP.

Utilice el verificador de sintaxis de la figura 4 para configurar la autenticación CHAP en la interfaz serial 0/0/1 del router R1.

Configuración de autenticación PAP




```
hostname R1
username R2 password someone
!
interface Serial0/0/0
 ip address 10.0.1.1 255.255.255.252
 ipv6 address 2001:DB8:CAFE:1::1/64
 encapsulation ppp
 ppp authentication pap
 ppp pap sent-username R1 password
someone
```

```
hostname R2
username R1 password someone
!
interface Serial 0/0/0
 ip address 10.0.1.2 255.255.255.252
 ipv6 address 2001:db8:cafe:1::2/64
 encapsulation ppp
 ppp authentication pap
 ppp pap sent-username R2 password
someone
```

Configuración de autenticación PAP

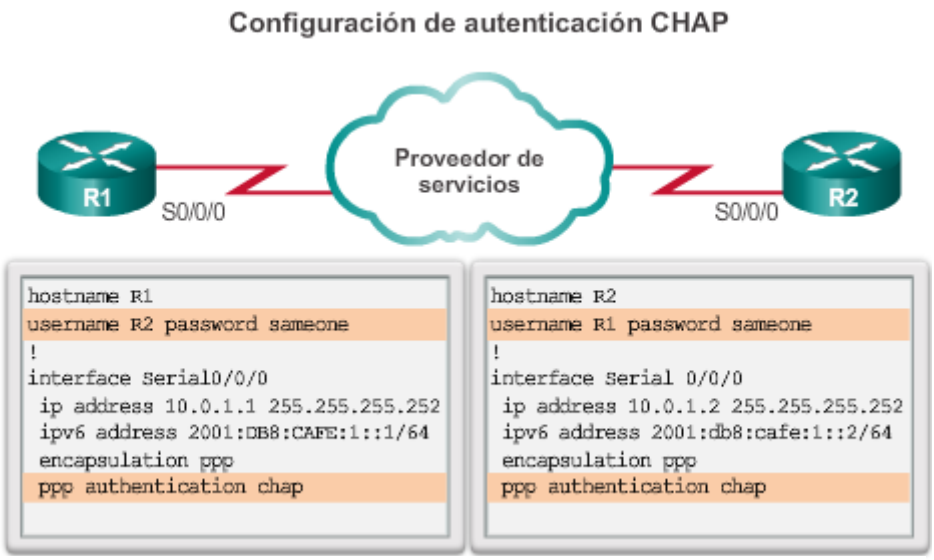
En la interfaz Serial 0/0/1 del R1, agregue los comandos para configurar la autenticación PPP mediante PAP. Realice las tareas en el siguiente orden:

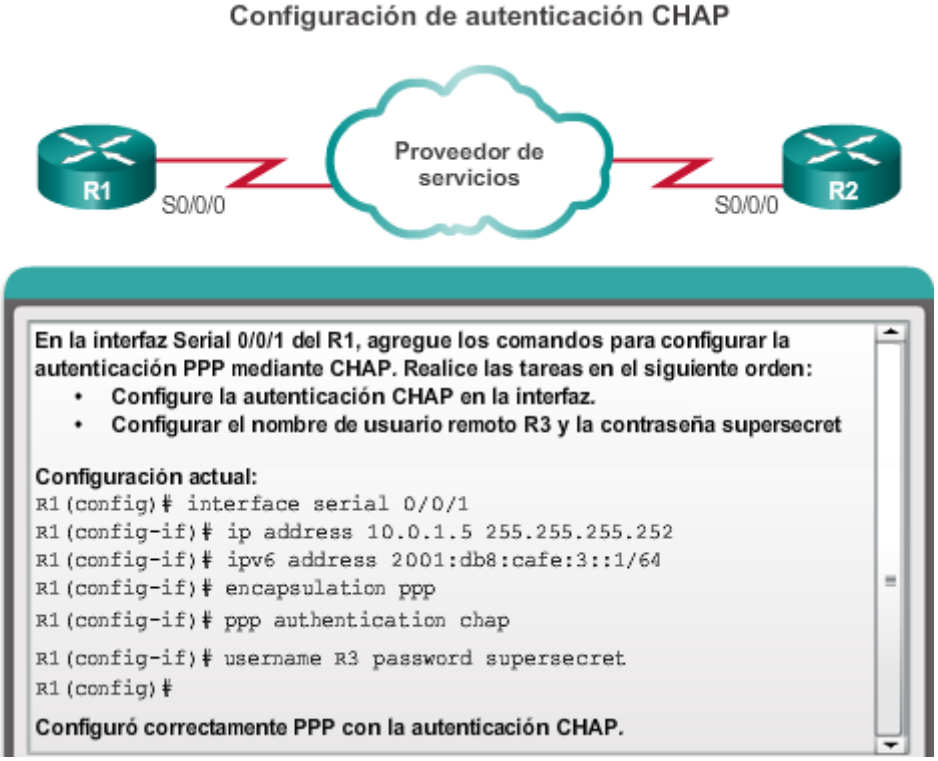
- **Configure la autenticación PAP en la interfaz.**
- **Configure el nombre de usuario local de PAP R1 y la contraseña supersecret.**
- **Configurar el nombre de usuario remoto R3 y la contraseña supersecret**

Configuración actual:

```
R1(config)# interface serial 0/0/1
R1(config-if)# ip address 10.0.1.5 255.255.255.252
R1(config-if)# ipv6 address 2001:db8:cafe:3::1/64
R1(config-if)# encapsulation ppp
R1(config-if)# ppp authentication pap
R1(config-if)# ppp pap sent-username R1 password supersecret
R1(config-if)# username R3 password supersecret
R1(config)#
```

Configuró correctamente PPP con la autenticación PAP.





Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.3.2.7 Packet Tracer: Configuración de la autenticación PAP y CHAP

Información básica/situación

En esta actividad, practicará la configuración de la encapsulación PPP en los enlaces seriales. Por último, configurará la autenticación PAP de PPP y CHAP de PPP.

Packet Tracer: Configuración de la autenticación PAP y CHAP (instrucciones)

Packet Tracer: Configuración de la autenticación PAP y CHAP (PKA)

Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.3.2.8 Práctica de laboratorio: Configuración de PPP básico con autenticación

En esta práctica de laboratorio, cumplirá los siguientes objetivos:

- Parte 1: configurar los parámetros básicos de los dispositivos
- Parte 2: Configurar la encapsulación PPP
- Parte 3: Configurar la autenticación CHAP de PPP

Práctica de laboratorio: Configuración de PPP básico con autenticación

Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.4.1.1 Resolución de problemas de la encapsulación PPP serial

Recuerde que, para la resolución de problemas, se utiliza el comando **debug**, al que se accede en el modo EXEC privilegiado de la interfaz de línea de comandos. El resultado de **debug** muestra información sobre diferentes operaciones del router, relacionada con el tráfico generado o recibido por el router, y cualquier mensaje de error. Esto puede consumir una cantidad considerable de recursos, y el router se ve obligado a aplicar el switching de procesos a los paquetes que se depuran. El comando**debug** no se debe usar como herramienta de control; en cambio, está diseñado para ser utilizado durante un período breve para la resolución de problemas.

Utilice el comando **debug ppp** para mostrar información sobre el funcionamiento de PPP. En la ilustración, se muestra la sintaxis del comando. Utilice la versión **no** de este comando para deshabilitar el resultado de la depuración.

Utilice el comando **debug ppp** cuando intente buscar lo siguiente:

- Los protocolos NCP que se admiten en cualquier extremo de una conexión PPP
- Cualquier bucle que pudiera existir en una internetwork PPP
- Los nodos que negocian conexiones PPP correctamente (o no)
- Los errores que ocurrieron en la conexión PPP
- Las causas para las fallas de la sesión CHAP
- Las causas para las fallas de la sesión PAP
- Información específica del intercambio de conexiones PPP mediante el protocolo de devolución de llamada (CBCP), que usan los clientes Microsoft

- Información de número de secuencia de paquete incorrecta donde está habilitada la compresión MPPC

debug ppp Parámetros de comandos

```
debug ppp (packet | negotiation | error | authentication |
compression | cbcp)
```

Parámetro	Uso
Paquete	Muestra los paquetes PPP enviados y recibidos. (Este comando muestra las descargas de los paquetes de bajo nivel).
negociación	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.
Autenticación	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).
Compresión	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.

Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.4.1.2 Depuración de PPP

Además del comando **debug ppp**, existen otros comandos para la resolución de problemas de una conexión PPP.

Un buen comando para usar durante la resolución de problemas de encapsulación de interfaces seriales es el comando**debug ppp packet**, como se muestra en la figura 1. En el ejemplo de la ilustración, se representan intercambios de paquetes durante el funcionamiento normal de PPP, incluido el estado LCP, los procedimientos de LQM y el número mágico LCP.

En la figura 2, se muestra el resultado del comando **debug ppp negotiation** en una negociación normal, donde ambos lados acuerdan los parámetros de NCP. En este caso, se proponen y se confirman los tipos de protocolo IPv4 e IPv6. El comando**debug ppp negotiation** permite que el administrador de red vea las transacciones de negociación PPP, identifique el problema o la etapa en que se produce el error, y desarrolle una solución. El resultado incluye la negociación LCP, la autenticación, y la negociación NCP.

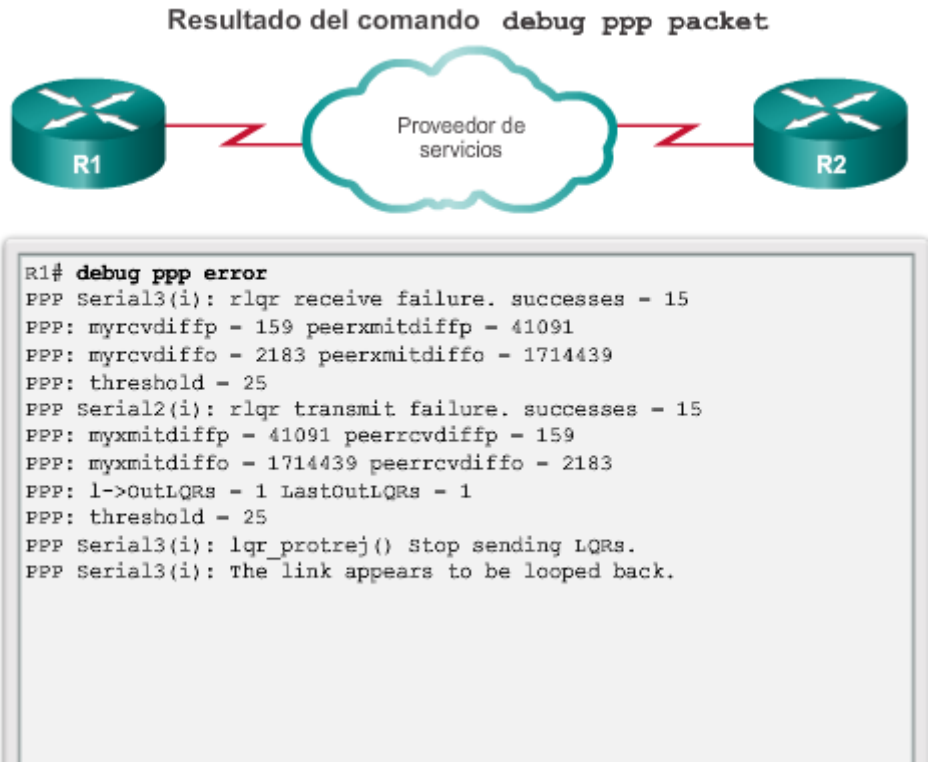
El comando **debug ppp error** se utiliza para mostrar los errores de protocolo y las estadísticas de errores con relación a la negociación y la operación de las conexiones PPP, como se muestra en la figura 3. Estos mensajes pueden aparecer cuando se habilita la opción de protocolo de calidad en una interfaz que ya ejecuta PPP.

Resultado del comando debug ppp packet


```
R1# debug ppp packet
PPP packet display debugging is on
R1#
*Apr  1 16:15:17.471: Se0/0/0 LQM: O state Open magic 0x1EFC37C3
len 48
*Apr  1 16:15:17.471: Se0/0/0 LQM:    LastOutLQRs 70
LastOutPackets/Octets 194/9735
*Apr  1 16:15:17.471: Se0/0/0 LQM:    PeerInLQRs 70
PeerInPackets/Discards/Errors/Octets 0/0/0/0
*Apr  1 16:15:17.471: Se0/0/0 LQM:    PeerOutLQRs 71
PeerOutPackets/Octets 197/9839
*Apr  1 16:15:17.487: Se0/0/0 PPP: I pkt type 0xC025,
datagramsize 52 link[ppp]
*Apr  1 16:15:17.487: Se0/0/0 LQM: I state Open magic 0xFE83D624
len 48
*Apr  1 16:15:17.487: Se0/0/0 LQM:    LastOutLQRs 71
LastOutPackets/Octets 197/9839
```

Resultado del comando debug ppp packet


```
R1# debug ppp negotiation
PPP protocol negotiation debugging is on
R1#
*Apr  1 18:42:29.831: %LINK-3-UPDOWN: Interface Serial0/0/0,
changed state to up
*Apr  1 18:42:29.831: Se0/0/0 PPP: Sending cstate UP notification
*Apr  1 18:42:29.831: Se0/0/0 PPP: Processing CstateUp message
*Apr  1 18:42:29.835: PPP: Alloc Context [66A27824]
*Apr  1 18:42:29.835: ppp2 PPP: Phase is ESTABLISHING
*Apr  1 18:42:29.835: Se0/0/0 PPP: Using default call direction
*Apr  1 18:42:29.835: Se0/0/0 PPP: Treating connection as a
dedicated line
*Apr  1 18:42:29.835: Se0/0/0 PPP: Session handle[4000002]
Session id[2]
*Apr  1 18:42:29.835: Se0/0/0 LCP: Event[OPEN]
State[Initial to Starting]
*Apr  1 18:42:29.835: Se0/0/0 LCP: O CONFREQ [Starting]
id 1 len 23
```



Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.4.1.3 Resolución de problemas de una configuración PPP con autenticación

La autenticación es una característica que se debe implementar correctamente, de lo contrario, la seguridad de la conexión serial puede verse comprometida. Siempre verifique la configuración con el comando**show interfaces serial**, de la misma forma en que lo hizo sin la autenticación.

Nota: nunca suponga que la configuración de la autenticación funciona sin probarla. La depuración permite confirmar la configuración y corregir cualquier defecto. Para depurar la autenticación PPP, utilice el comando **debug ppp authentication**.

En la ilustración, se muestra un resultado de ejemplo del comando **debug ppp authentication**. La siguiente es una interpretación del resultado:

La línea 1 indica que el router no puede autenticar en la interfaz Serial0 porque el peer no envió ningún nombre.

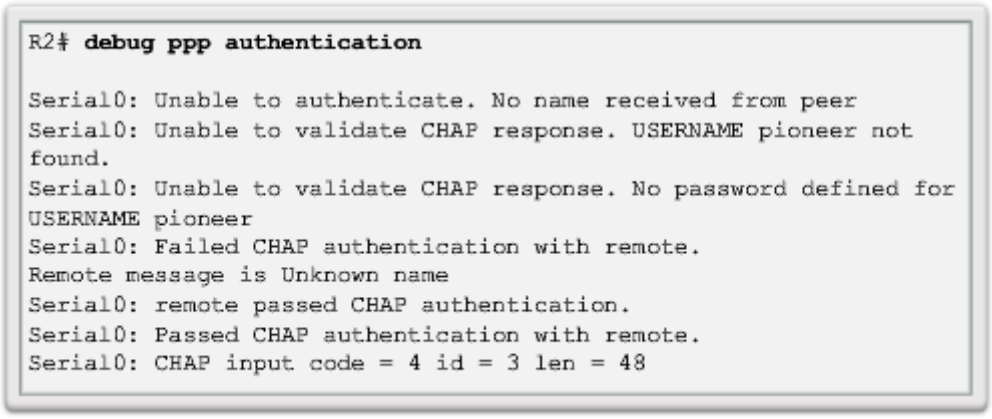
La línea 2 indica que el router no pudo validar la respuesta CHAP porque no se encontró el NOMBRE DE USUARIOpioneer.

La línea 3 indica que no se encontró ninguna contraseña para pioneer. Otras posibles respuestas en esta línea podrían ser que no se recibió ningún nombre para autenticar, que el nombre es desconocido, que no hay ningún secreto para el nombre dado, que la respuesta MD5 recibida es corta o que la comparación MD5 falló.

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

- 1, desafío
- 2, respuesta
- 3, conexión satisfactoria
- 4, falla
- id - 3 es el número de ID por formato de paquete LCP
- len - 48 es la longitud del paquete sin el encabezado

Resolución de problemas de una configuración PPP con autenticación



Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.4.1.4 Packet Tracer: Resolución de problemas de PPP con autenticación

Información básica/ Situación

Un ingeniero de redes inexperto configuró los routers de la compañía. Varios errores en la configuración han resultado en problemas de conectividad. El jefe le solicitó al usuario que resuelva y corrija los errores de configuración y que documente su trabajo. Según los conocimientos de PPP y los métodos de prueba estándar, busque y corrija los errores. Asegúrese de que todos los enlaces seriales utilicen la autenticación PPP CHAP y de que todas las redes sean alcanzables. Las contraseñas son “cisco” y “class”.

Packet Tracer: Resolución de problemas de PPP con autenticación (instrucciones)

Packet Tracer: Resolución de problemas de PPP con autenticación (PKA)

Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.4.1.5 Práctica de laboratorio: Resolución de problemas de PPP básico con autenticación

En esta práctica de laboratorio, cumplirá los siguientes objetivos:

- Parte 1: armar la red y cargar las configuraciones de los dispositivos
- Parte 2: Resolver problemas de la capa de enlace de datos
- Parte 3: Resolver problemas de la capa de red

Práctica de laboratorio: Resolución de problemas de PPP básico con autenticación

Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.5.1.1 Actividad de clase: Validación de PPP

Validación en PPP

Tres amigos que están inscritos en Cisco Networking Academy desean poner a prueba sus conocimientos acerca de la configuración de redes PPP.

Establecen un concurso en el que cada uno tiene que pasar una prueba de configuración de PPP con requisitos definidos y diversas opciones de situaciones de PPP. Cada persona elabora una situación de configuración diferente.

Al día siguiente, se reúnen y prueban la configuración de los otros con los requisitos de sus respectivas situaciones de PPP.

Actividad de clase: Validación de PPP

Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.5.1.2 Packet Tracer: desafío de integración de habilidades

Información básica/situación

Esta actividad le permite poner en práctica diversas aptitudes, incluida la configuración de VLAN, PPP con CHAP, el routing estático y predeterminado, y el uso de IPv4 e IPv6. Debido a la gran cantidad de elementos con calificación, siéntase libre para hacer clic en Check Results (Verificar resultados) y después, Assessment Items (Elementos de evaluación) para ver si introdujo correctamente un comando con calificación. Utilice las contraseñas “cisco” y “class” para acceder a los modos EXEC de la CLI para routers y switches.

Packet Tracer: Reto de habilidades de integración (instrucciones)

Packet Tracer: Reto de habilidades de integración (PKA)

Capítulo 3: Point-to-Point Connections (Conexiones PSTN) 3.5.1.3 Resumen

Las transmisiones seriales envían 1 bit por vez a través de un único canal de manera secuencial. Los puertos serie son bidireccionales. Las comunicaciones seriales síncronas requieren una señal de reloj.

En general, los enlaces punto a punto son más costosos que los servicios compartidos; sin embargo, los beneficios pueden superar los costos. La disponibilidad constante es importante para algunos protocolos, como VoIP.

SONET es un estándar de red óptica que utiliza STDM para el uso eficaz del ancho de banda. En los Estados Unidos, las velocidades de transmisión de OC son especificaciones estandarizadas para SONET.

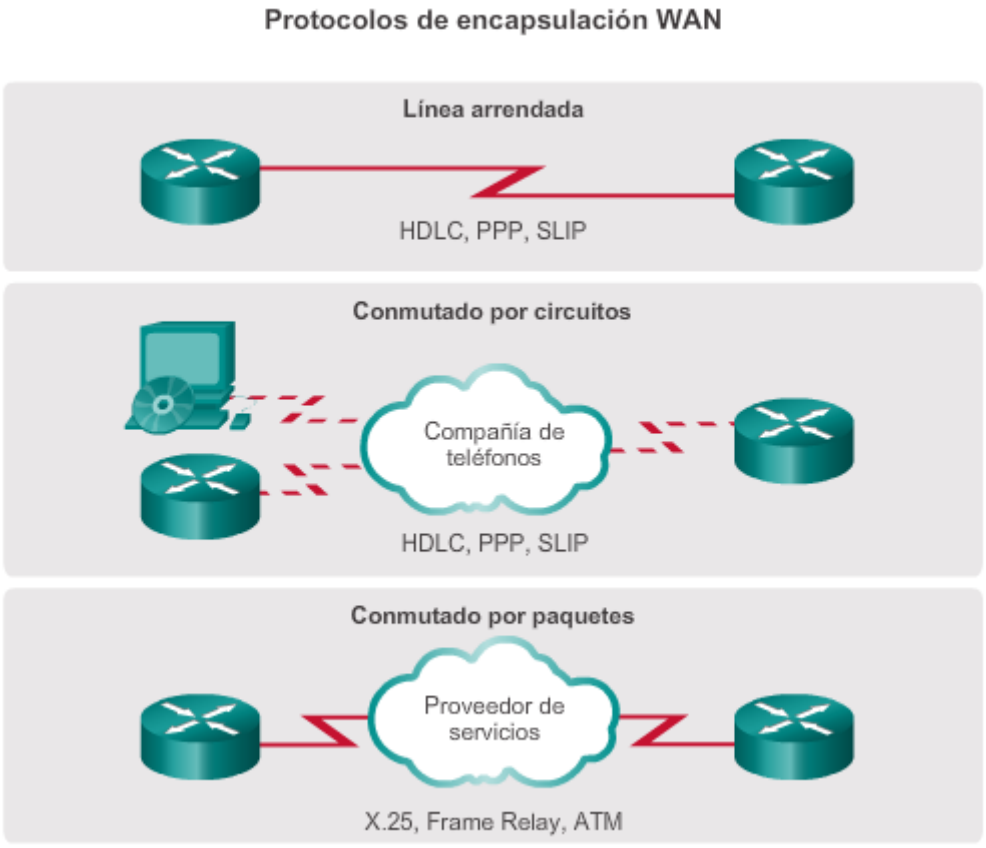
La jerarquía de ancho de banda que usan las portadoras es diferente en América del Norte (portadora T) y Europa (portadora E). En América del Norte, la velocidad en línea elemental es 64 kbps, o DS0. Para proporcionar velocidades en línea superiores, se agrupan varios DS0.

El punto de demarcación es aquel donde termina la responsabilidad del proveedor de servicios y comienza la responsabilidad del cliente. El CPE, que generalmente es un router, es el dispositivo DTE. El DCE suele ser un módem o una CSU/DSU.

Un cable de módem nulo se usa para conectar dos dispositivos DTE cruzando las líneas Tx y Rx, sin necesidad de un dispositivo DCE. Cuando se usa este cable entre los routers en un laboratorio, uno de los routers debe proporcionar la señal de reloj.

HDLC de Cisco es una extensión de protocolo sincrónico de capa de enlace de datos orientada a bits de HDLC que usan muchos proveedores para proporcionar compatibilidad multiprotocolo. Este es el método de encapsulación predeterminado que se usa en las líneas seriales síncronas de Cisco.

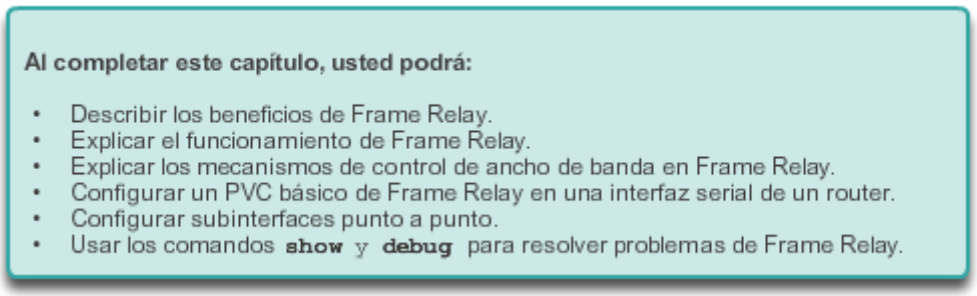
PPP síncrono se utiliza para conectarse a dispositivos que no son de Cisco, controlar la calidad del enlace, proporcionar autenticación o agrupar enlaces para el uso compartido. PPP utiliza HDLC para encapsular datagramas. LCP es el protocolo PPP que se usa para establecer, configurar, probar y finalizar la conexión de enlace de datos. LCP puede autenticar un peer mediante PAP o CHAP. El protocolo PPP usa una familia de NCP para admitir varios protocolos de capa de red simultáneamente. El protocolo PPP multienlace propaga el tráfico a través de enlaces agrupados mediante la fragmentación de paquetes y el envío simultáneo de estos fragmentos a través de varios enlaces a la misma dirección remota, donde se vuelven a armar.



Capítulo 4: Frame Relay 4.0.1.1 Introducción

Frame Relay es una alternativa a las líneas dedicadas arrendadas WAN, que son más costosas. Frame Relay es un protocolo WAN de alto rendimiento que funciona en las capas física y de enlace de datos del modelo de referencia OSI. Si bien los servicios más modernos como los de banda ancha y Ethernet metropolitana redujeron la necesidad de Frame Relay en muchas ubicaciones, Frame Relay sigue siendo una opción viable en muchos sitios de todo el mundo. Frame Relay proporciona una solución rentable para las comunicaciones entre varios sitios remotos mediante un único circuito de acceso desde cada sitio hasta el proveedor.

En este capítulo, se presentan los conceptos fundamentales de Frame Relay. También se abarcan las tareas de configuración, verificación y resolución de problemas de Frame Relay.



Capítulo 4: Frame Relay 4.0.1.2 Actividad de clase: Tecnologías WAN emergentes

Tecnologías WAN emergentes

Como administrador de red de su pequeña a mediana empresa, ya pasó de WAN de línea arrendada a conectividad de Frame Relay para la comunicación de red WAN. Usted es responsable de mantener todas las futuras actualizaciones de red al corriente.

Descubre que hay algunas opciones alternativas disponibles para la conectividad WAN para mantenerse al corriente con las tecnologías emergentes y en desarrollo. Algunos de estos programas incluyen los siguientes:

- Frame Relay
- DSL de banda ancha
- Cable módem de banda ancha
- GigaMAN
- VPN
- MPLS

Dado que desea ofrecerle a su empresa el servicio de red WAN de mejor calidad y menor costo, decide investigar, al menos, dos tecnologías emergentes y en desarrollo. Su objetivo es reunir información acerca de estas dos opciones de WAN alternativas para analizar de forma consciente los objetivos futuros de la red con su gerente comercial y con otros administradores de red.

Actividad de clase: Tecnologías WAN emergentes

Capítulo 4: Frame Relay 4.1.1.1 Introducción a la tecnología Frame Relay

Las líneas arrendadas proporcionan capacidad dedicada permanente y se utilizan mucho para armar redes WAN. Son la conexión tradicional de preferencia, pero presentan una serie de desventajas. Una desventaja es que los clientes pagan por líneas arrendadas con una capacidad fija. Sin embargo, el tráfico WAN suele variar, y parte de la capacidad queda sin utilizar. Además, cada terminal necesita una interfaz física individual en el router, lo que aumenta los costos de los equipos. Por lo general, cualquier cambio en la línea arrendada requiere que el personal de la empresa prestadora de servicios visite el sitio.

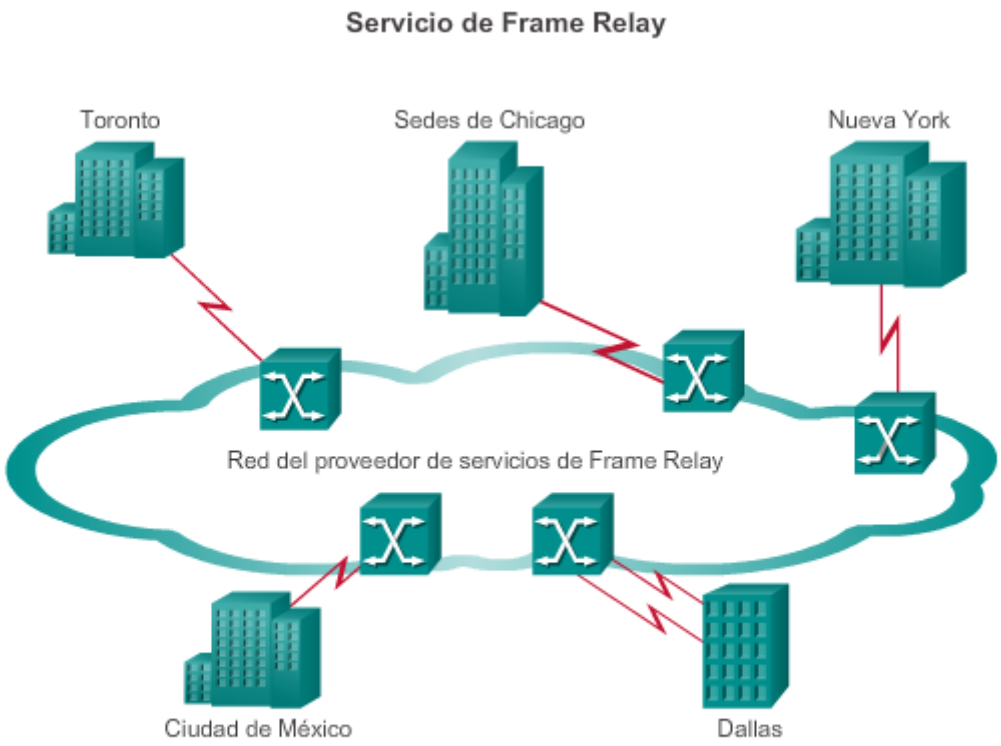
Frame Relay es un protocolo WAN de alto rendimiento que funciona en las capas física y de enlace de datos del modelo de referencia OSI. A diferencia de las líneas arrendadas, Frame Relay solo requiere un único circuito de acceso al proveedor de servicios de Frame Relay para comunicarse con otros sitios conectados al mismo proveedor. La capacidad entre dos sitios puede variar.

Eric Scace, un ingeniero de Sprint International, inventó Frame Relay como una versión más simple del protocolo X.25 para utilizarlo a través de las interfaces de red digital de servicios integrados (ISDN). En la actualidad, también se utiliza en otros tipos de interfaces de red. Cuando Sprint implementó Frame Relay en su red pública, utilizó switches StrataCom. La

adquisición de StrataCom por parte de Cisco en 1996 marcó su entrada en el mercado de las prestadoras de servicios.

Los proveedores de servicios de red implementan Frame Relay para admitir tráfico de voz y de datos entre redes LAN a través de una WAN. Cada usuario final obtiene una línea privada, o una línea arrendada, a un nodo de Frame Relay. La red Frame Relay maneja la transmisión a través de una ruta que cambia con frecuencia, transparente para todos los usuarios finales. Como se muestra en la ilustración, Frame Relay proporciona una solución para permitir comunicaciones entre varios sitios mediante un único circuito de acceso al proveedor.

Históricamente, Frame Relay se utilizó ampliamente como protocolo WAN porque era económico en comparación con las líneas arrendadas dedicadas. Además, configurar el equipo del usuario en una red Frame Relay es muy simple. Las conexiones de Frame Relay se crean configurando los routers u otros dispositivos del equipo local del cliente (CPE) para que se comuniquen con un switch Frame Relay de un proveedor de servicios. El proveedor de servicios configura el switch Frame Relay, lo que reduce al mínimo las tareas de configuración del usuario final.



Frame Relay permite las comunicaciones entre todos los sitios mediante un único circuito de acceso al proveedor.

Capítulo 4: Frame Relay 4.1.1.2 Beneficios de la tecnología WAN de Frame Rela

Con la llegada de los servicios de banda ancha como DSL y cable módem, WAN Ethernet (servicio Ethernet punto a punto a través de cable de fibra óptica), VPN y conmutación de etiquetas multiprotocolo (MPLS), Frame Relay se convirtió en una solución menos adecuada para acceder a la WAN. Sin embargo, todavía hay sitios en el mundo que confían en Frame Relay para obtener conectividad a la WAN.

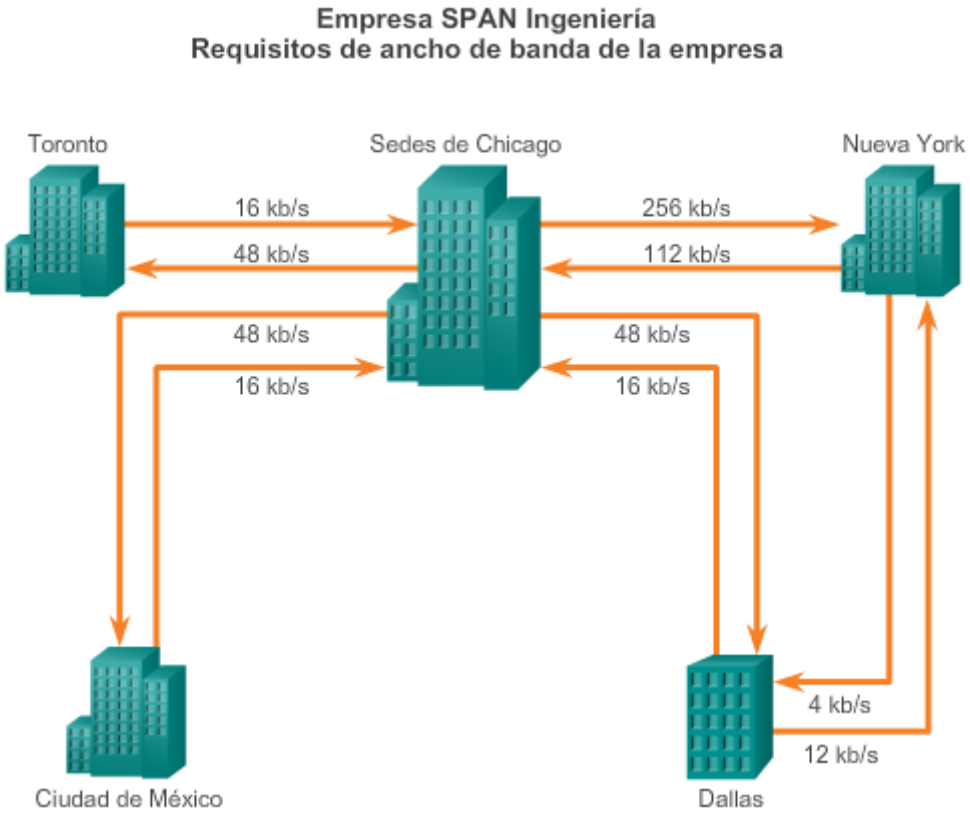
Frame Relay proporciona más ancho de banda, confiabilidad y resistencia que las líneas privadas o arrendadas.

Usar un ejemplo de una red empresarial grande ayuda a ilustrar los beneficios de utilizar una WAN de Frame Relay. En el ejemplo que se muestra en la ilustración, la empresa SPAN Ingeniería tiene cinco campus en toda América del Norte. Como la mayoría de las organizaciones, SPAN tiene diversos requisitos de ancho de banda.

Lo primero que se debe tener en cuenta es el requisito de ancho de banda de cada sitio. Al trabajar en la oficina central, la conexión de Chicago a Nueva York requiere una velocidad máxima de 256 kb/s. Otros tres sitios necesitan una velocidad máxima de 48 kb/s para conectarse a la oficina central, mientras que la conexión entre las sucursales de Nueva York y Dallas requiere solo 12 kb/s.

Antes de que Frame Relay estuviera disponible, la empresa SPAN Ingeniería arrendaba líneas dedicadas.

Nota: los valores de ancho de banda utilizados en los ejemplos de línea arrendada y Frame Relay en este capítulo no necesariamente reflejan los anchos de banda que utilizan muchos clientes en la actualidad. Los valores de ancho de banda utilizados en este capítulo son solamente con fines de comparación.



Capítulo 4: Frame Relay 4.1.1.3 Requisitos de la línea dedicada

Mediante las líneas arrendadas, cada uno de los sitios de SPAN se conecta a través de un switch en la oficina central (CO) de la compañía telefónica local por medio del bucle local, y después a través de toda la red. Los sitios de Chicago y Nueva York usan una línea dedicada

T1 (equivalente a 24 canales DS0) para conectarse al switch, mientras que otros sitios utilizan conexiones ISDN (56 kb/s), como se muestra en la ilustración. Debido a que el sitio de Dallas se conecta a Nueva York y Chicago, tiene dos líneas arrendadas localmente. Los proveedores de servicios de red proporcionan a SPAN un DS0 entre las respectivas CO, excepto la canalización más grande que conecta Chicago y Nueva York, y que tiene cuatro DS0. Los DS0 tienen precios diferentes según la región y, generalmente, se ofrecen a un precio fijo. Estas líneas son realmente dedicadas, ya que el proveedor de servicios de red reserva esa línea para uso exclusivo de SPAN. No existe el uso compartido, y SPAN paga por el circuito de extremo a extremo, independientemente de cuánto ancho de banda utiliza.

Una línea dedicada proporciona pocas oportunidades prácticas para establecer una conexión de uno a varios sin obtener más líneas del proveedor de servicios de red. En el ejemplo, casi toda la comunicación debe fluir a través de las oficinas centrales de la empresa, simplemente para reducir el costo de líneas adicionales.

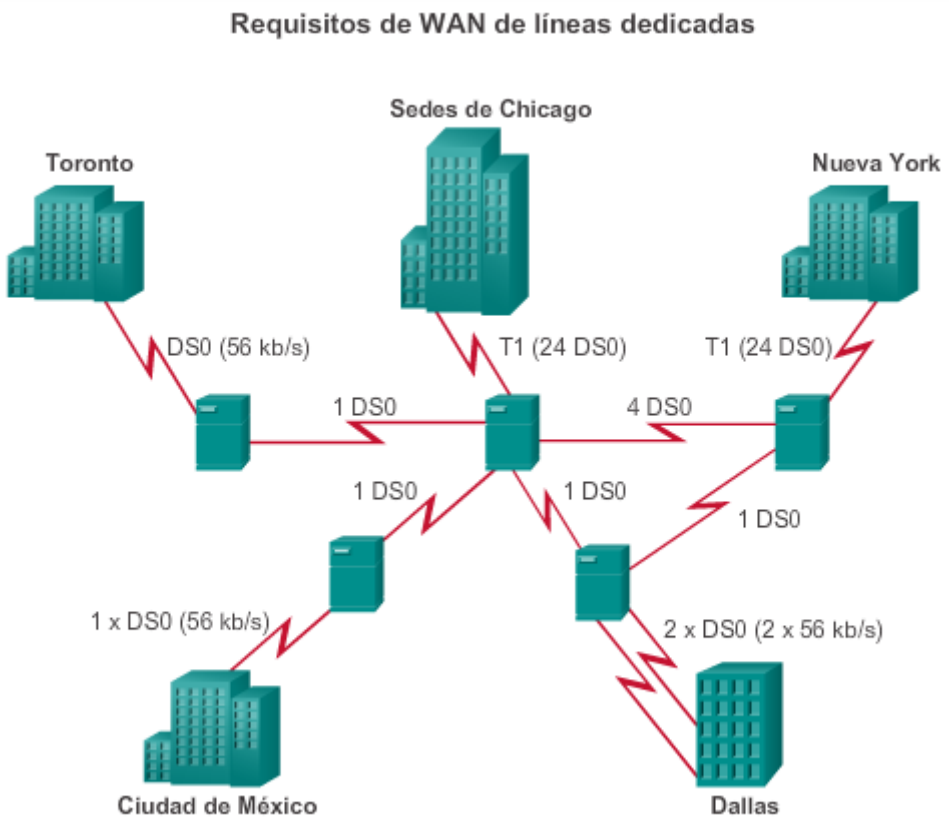
Después de un análisis más detallado de los requisitos de ancho de banda para cada sitio, se comprueba que hay una falta de eficacia:

- De los 24 canales DS0 disponibles en la conexión T1, el sitio de Chicago utiliza solo siete. Algunas prestadoras de servicios ofrecen conexiones T1 fraccionadas en incrementos de 64 kb/s, pero esto requiere un dispositivo especializado denominado “multiplexor” en el extremo del cliente para canalizar las señales. En este caso, SPAN optó por el servicio T1 completo.

- De manera similar, el sitio de Nueva York utiliza solo cinco de sus 24 DS0 disponibles.

- Debido a que Dallas debe conectarse a Chicago y Nueva York, hay dos líneas que se conectan a cada sitio a través de la CO.

El diseño de línea arrendada también limita la flexibilidad. A menos que los circuitos ya estén instalados, la conexión de nuevos sitios normalmente requiere nuevas instalaciones de circuitos, e implementarlo lleva mucho tiempo. Desde el punto de vista de la confiabilidad de la red, imagine los costos adicionales en dinero y la complejidad de agregar circuitos redundantes de repuesto.



Capítulo 4: Frame Relay 4.1.1.4 Rentabilidad y flexibilidad de Frame Relay

La red Frame Relay de SPAN utiliza circuitos virtuales permanentes (PVC), como se muestra en la ilustración. Un PVC es la ruta lógica a lo largo de un enlace Frame Relay de origen, a través de la red y a lo largo de un enlace Frame Relay de finalización hasta su destino final. Compare esto con la ruta física que utiliza una conexión dedicada. En una red con acceso mediante Frame Relay, un PVC define la ruta entre dos terminales de manera exclusiva. El concepto de circuitos virtuales (VC) se analiza en mayor detalle más adelante en esta sección.

La solución Frame Relay de SPAN proporciona flexibilidad y rentabilidad.

Rentabilidad de Frame Relay

Frame Relay es una opción más rentable por dos motivos. En primer lugar, con las líneas dedicadas, los clientes pagan por una conexión de extremo a extremo que incluye el bucle local y el enlace de red. Con Frame Relay, los clientes solo pagan por el bucle local y adquieren el ancho de banda del proveedor de servicios de red. La distancia entre los nodos no es importante. En un modelo de línea dedicada, los clientes utilizan líneas dedicadas proporcionadas en incrementos de 64 kb/s, y los clientes de Frame Relay pueden definir sus necesidades de circuito virtual con una granularidad mucho mayor, a menudo en incrementos tan pequeños como 4 kb/s.

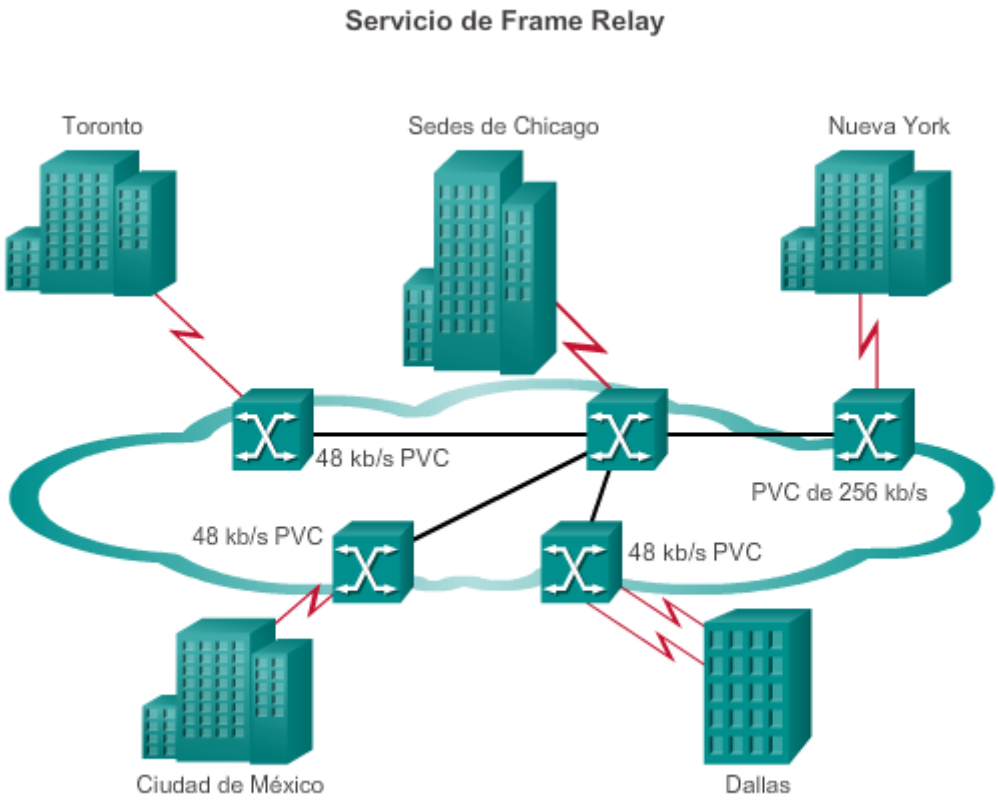
El segundo motivo de la rentabilidad de Frame Relay es que comparte el ancho de banda a través de una mayor base de clientes. Generalmente, un proveedor de servicios de red puede brindar servicio a 40 o más clientes de 56 kb/s a través de un circuito T1. El uso de líneas dedicadas requeriría más CSU/DSU (una para cada línea), así como routing y switching más

complicados. Los proveedores de servicios de red ahorran porque hay menos equipos para adquirir y mantener.

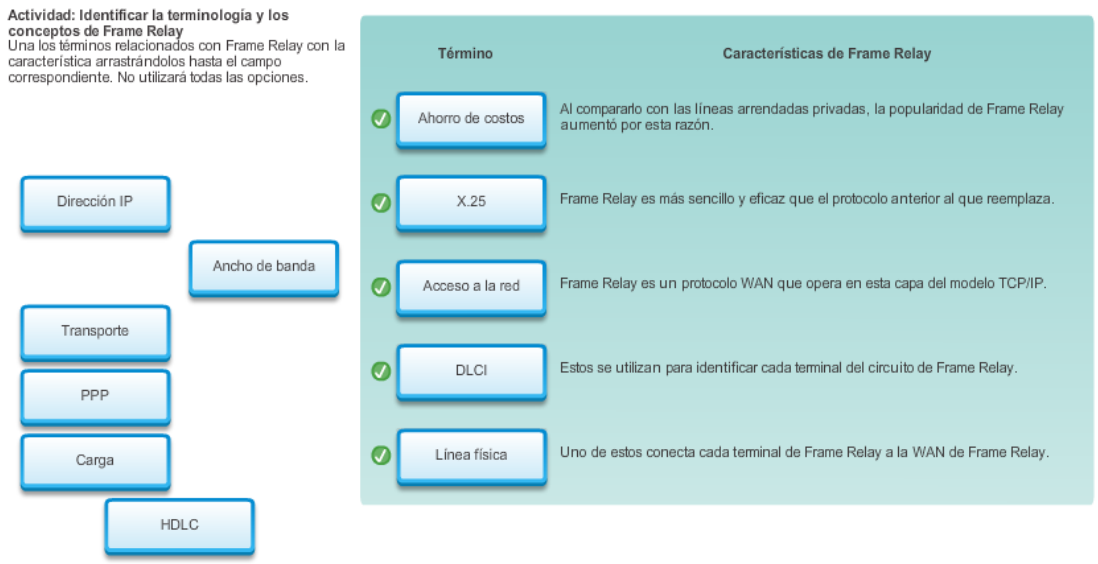
Nota: el costo puede variar considerablemente según la ubicación.

La flexibilidad de Frame Relay

Un circuito virtual proporciona una flexibilidad considerable en el diseño de red. Al analizar la ilustración, puede ver que todas las oficinas de SPAN se conectan a la nube de Frame Relay a través de sus respectivos bucles locales. Por el momento, lo que sucede en la nube realmente no es de interés. Lo único que importa es que cuando cualquier oficina de SPAN desea comunicarse con cualquier otra oficina de SPAN, todo lo que debe hacer es conectarse a un circuito virtual que conduce a la otra oficina. En Frame Relay, el extremo de cada conexión tiene un número para identificarlo denominado “identificador de conexión de enlace de datos” (DLCI). Cualquier estación puede conectarse a cualquier otra con solo indicar la dirección de esa estación y el número de DLCI de la línea que debe utilizar. 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. Imagine la misma flexibilidad mediante líneas dedicadas. No solo es difícil, sino que también requiere muchos más equipos.



Capítulo 4: Frame Relay 4.1.1.5 Actividad: Identificar la terminología y los conceptos de Frame Relay



Capítulo 4: Frame Relay 4.1.2.1 Circuitos virtuales

La conexión a través de una red Frame Relay entre dos DTE es un VC. Los circuitos son virtuales porque no hay una conexión eléctrica directa de extremo a extremo. La conexión es lógica, y los datos se transfieren de extremo a extremo sin un circuito eléctrico directo. Con los VC, Frame Relay comparte el ancho de banda entre varios usuarios, y cualquier sitio individual puede comunicarse con cualquier otro sitio individual sin utilizar varias líneas físicas dedicadas.

Hay dos formas de establecer VC:

- **Circuitos virtuales conmutados (SVC):** se establecen en forma dinámica mediante el envío de mensajes de señalización a la red (CALL SETUP, DATA TRANSFER, IDLE, CALL TERMINATION).

- **Circuitos virtuales permanentes (PVC):** los preconfigura la prestadora de servicios y, una vez establecidos, solo funcionan en los modos IDLE y DATA TRANSFER. Tenga en cuenta que, en algunas publicaciones, los PVC se denominan “VC privados”.

Nota: los PVC se implementan con más frecuencia que los SVC.

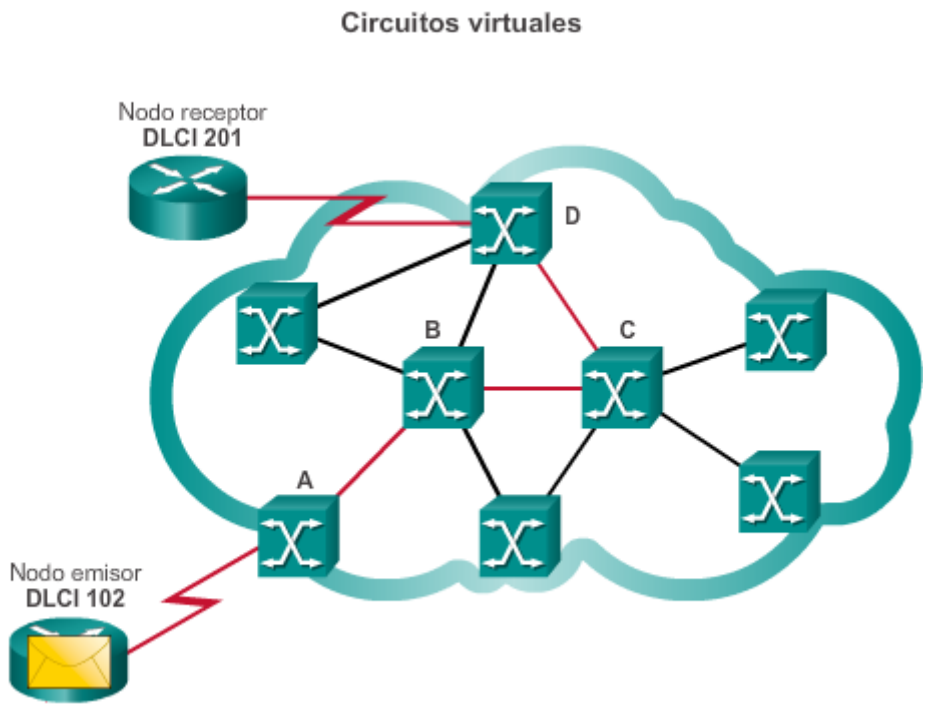
Haga clic en Reproducir en la figura 1 para ver una animación acerca de un VC entre el nodo emisor y el nodo receptor. El VC sigue la ruta A, B, C y D. Frame Relay crea un VC almacenando asignaciones de puerto de entrada a puerto de salida en la memoria de cada switch y, de esta manera, enlaza un switch con otro hasta que se identifica una ruta continua de un extremo del circuito a otro. Un VC puede pasar a través de cualquier cantidad de dispositivos intermedios (switches) ubicados dentro de la red Frame Relay.

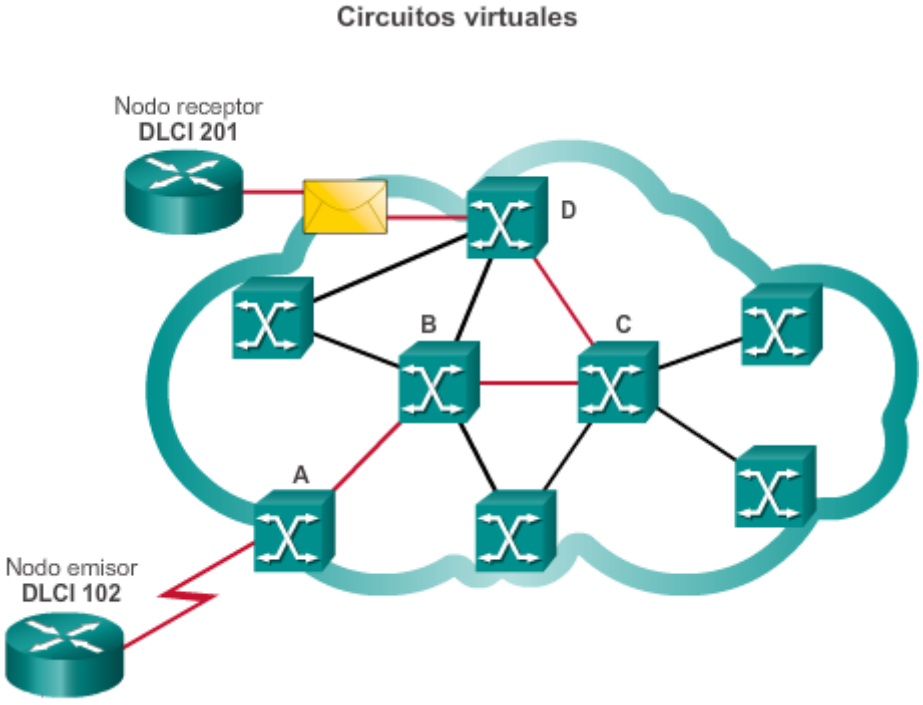
Los VC proporcionan una ruta de comunicación bidireccional desde un dispositivo hasta otro. Los VC se identifican mediante los DLCI, como se muestra en la figura 2. Por lo general, el proveedor de servicios de Frame Relay asigna los valores de DLCI. Los DLCI de Frame Relay tienen importancia local, lo que significa que los valores propiamente dichos no son exclusivos en la WAN de Frame Relay. Un DLCI identifica un VC ante el equipo en una terminal. Un DLCI no tiene importancia más allá del enlace único. Dos dispositivos conectados mediante un VC pueden utilizar un valor diferente de DLCI para referirse a la misma conexión.

Los DLCI con importancia local se convirtieron en el método principal de direccionamiento, porque se puede usar la misma dirección en varias ubicaciones diferentes y aún así referirse a diferentes conexiones. El direccionamiento local evita que un cliente se quede sin DLCI a medida que crece la red.

Haga clic en Reproducir en la figura 3. Esta es la misma red que se presentó en la ilustración anterior, pero esta vez, cuando se transfiere la trama a través de la red, Frame Relay etiqueta cada VC con un DLCI. El DLCI se almacena en el campo de dirección de cada trama transmitida para informar a la red cómo se debe enrutar la trama. El proveedor de servicios de Frame Relay asigna números de DLCI. Generalmente, los DLCI de 0 a 15 y de 1008 a 1023 están reservados. Por lo tanto, los proveedores de servicios suelen asignar los DLCI en el intervalo de 16 a 1007.

En este ejemplo, la trama utiliza el DLCI 102. Sale del router (R1) mediante 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 y VC continúa a través de la WAN hasta que la trama llegue a su destino en el DLCI 201. El DLCI se almacena en el campo de direcciones de cada trama transmitida.





Capítulo 4: Frame Relay 4.1.2.2 Circuitos virtuales múltiples

Varios VC

Frame Relay se multiplexa estadísticamente, lo que significa que solo transmite de a una trama por vez, pero pueden coexistir muchas conexiones lógicas en una única línea física. El dispositivo de acceso Frame Relay (FRAD) o el router conectado a la red Frame Relay puede tener varios VC que lo conecten a las diversas terminales. Varios VC en una única línea física

se distinguen porque cada VC tiene su propio DLCI. Recuerde que el DLCI solo tiene importancia local y puede ser diferente en cada extremo de un VC.

En la figura 1, se muestra un ejemplo de dos VC en una línea de acceso única, cada uno con su propio DLCI, que se conectan a un router (el R1).

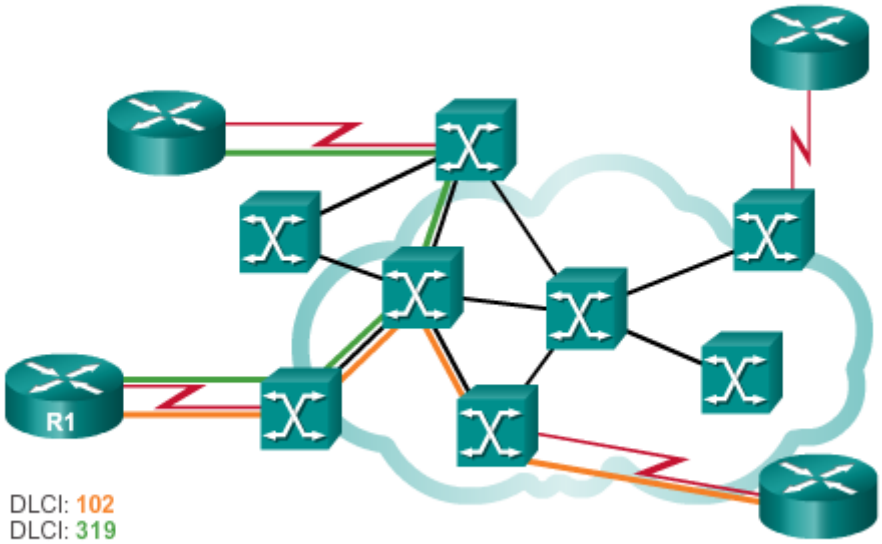
Esta capacidad suele reducir la complejidad de la red y el equipo que se requiere para conectar varios dispositivos, lo que lo hace un reemplazo muy rentable para una malla de líneas de acceso. Con esta configuración, cada terminal necesita solo una línea y una interfaz de acceso únicas. Surgen más ahorros, ya que la capacidad de la línea de acceso se basa en el requisito de ancho de banda promedio de los VC, en lugar del requisito de ancho de banda máximo.

En el ejemplo de la figura 2, la empresa SPAN Ingeniería. tiene cinco ubicaciones remotas, con la oficina central en Chicago. Chicago está conectada a la red mediante cinco VC, y cada VC tiene un DLCI. Para ver las asignaciones de los respectivos DLCI de Chicago, haga clic en la ubicación en la tabla. Observe que SPAN creció y recientemente abrió una oficina en San José. El uso de Frame Relay hizo que esta expansión fuera relativamente fácil.

Beneficios de costos de tener varios VC

Con Frame Relay, los clientes pagan por el ancho de banda que utilizan. En efecto, pagan por un puerto de Frame Relay. Cuando el cliente aumenta la cantidad de puertos, como se describió anteriormente, paga por más ancho de banda, pero no paga por más equipos, porque los puertos son virtuales. No hay cambios en la infraestructura física. Compare esto con la adquisición de más ancho de banda mediante líneas dedicadas.

Varios VC en una única línea de acceso



DLCI de SPAN Ingeniería de Chicago

Ubicación	DLCI
Nueva York	17
Toronto	18
Dallas	19
Ciudad de México	20
San José	21

Capítulo 4: Frame Relay 4.1.2.3 Encapsulación Frame Relay

Frame Relay toma paquetes de datos de un protocolo de capa de red, como IPv4 o IPv6, los encapsula como la porción de datos de una trama Frame Relay y después pasa la trama a la

capa física para la entrega en el cable. Para entender cómo funciona esto, es conveniente entender cómo se relaciona con los niveles inferiores del modelo OSI.

Frame Relay encapsula los datos para el transporte y los baja a la capa física para la entrega, como se muestra en la figura 1.

Primero, Frame Relay acepta un paquete de un protocolo de capa de red, como IPv4. A continuación, lo envuelve con un campo de dirección que contiene el DLCI y un valor de checksum. Se agregan campos de indicador para indicar el principio y el fin de la trama. Los campos de indicador marcan el comienzo y el fin de la trama, y siempre son los mismos. Los indicadores se representan como el número hexadecimal 7E o como el número binario 01111110. Una vez que se encapsula el paquete, Frame Relay pasa la trama a la capa física para el transporte.

El router CPE encapsula cada paquete de capa 3 dentro de un encabezado y un tráiler de Frame Relay antes de enviarlo a través del VC. El encabezado y el tráiler se definen en la especificación de servicios portadores para el procedimiento de acceso de enlace para Frame Relay (LAPF), ITU Q.922-A. Como se muestra en la figura 2, el encabezado de Frame Relay (campo de dirección) contiene específicamente lo siguiente:

- **DLCI:** el DLCI de 10 bits es uno de los campos más importantes del encabezado de Frame Relay. Este valor representa la conexión virtual entre el dispositivo DTE y el switch. Un DLCI exclusivo representa cada conexión virtual que se multiplexa en el canal físico. Los valores de DLCI solo tienen importancia local, lo que significa que solo son exclusivos para el canal físico en el que residen. Por lo tanto, los dispositivos de los extremos opuestos de una conexión pueden usar diferentes valores de DLCI para referirse a la misma conexión virtual.

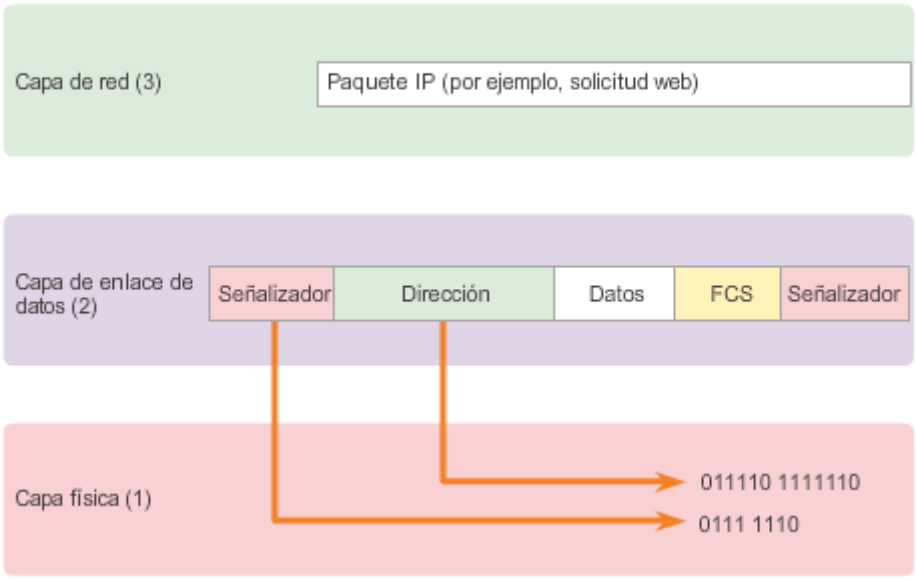
- **C/R:** es el bit que sigue al byte de DLCI más importante del campo de dirección. El bit C/R no está definido actualmente.

- **Dirección extendida (EA):** si el valor del campo EA es 1, se determina que el byte actual es el último octeto del DLCI. Si bien todas las implementaciones actuales de Frame Relay utilizan un DLCI de dos octetos, esta capacidad permite que se usen DLCI más largos en el futuro. El octavo bit de cada byte del campo Dirección indica la EA.

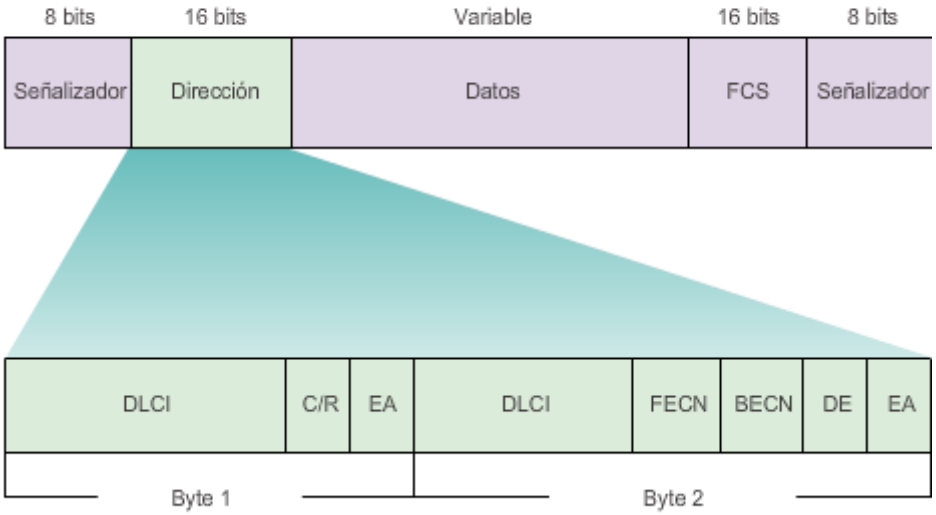
- **Control de congestión:** consta de 3 bits de notificación de congestión de Frame Relay. Estos 3 bits se denominan específicamente “bit de notificación explícita de congestión hacia delante” (FECN), “bit de notificación explícita de congestión hacia atrás” (BECN) y “bit elegible de descarte”.

Por lo general, la capa física es EIA/TIA-232, 449 o 530, V.35 o X.21. La trama Frame Relay es un subconjunto del tipo de trama HDLC; por lo tanto, se delimita con campos de indicador. El indicador de 1 byte utiliza el patrón de bits 01111110. La FCS determina si ocurrieron errores en el campo de dirección de capa 2 durante la transmisión. El nodo emisor calcula la FCS antes de la transmisión, y el resultado se inserta en el campo FCS. En el extremo distante, se calcula un segundo valor de FCS y se lo compara con la FCS en la trama. Si los resultados son iguales, se procesa la trama. Si existe una diferencia, se descarta la trama. Frame Relay no notifica el origen cuando se descarta una trama. El control de errores se reserva para las capas superiores del modelo OSI.

Encapsulación de Frame Relay y el modelo OSI



Trama Frame Relay estándar



Capítulo 4: Frame Relay 4.1.2.4 Topologías de Frame Rela

Cuando se deben conectar más de dos sitios, se debe planificar la topología o el mapa de Frame Relay de las conexiones entre los sitios. Un diseñador de red debe considerar la topología desde varios puntos de vista para comprender la red y los equipos utilizados para armarla. Las topologías completas para el diseño, la implementación, la operación y el mantenimiento incluyen mapas de descripción general, mapas de las conexiones lógicas,

mapas funcionales y mapas de direcciones que muestren el detalle de los equipos y los enlaces de canales.

Las redes Frame Relay enlazan decenas e incluso cientos de sitios en forma rentable. Si se considera que una red empresarial podría abarcar cualquier cantidad de proveedores de servicios e incluir redes de empresas adquiridas que difieren en el diseño básico, registrar las topologías puede ser un proceso muy complicado. Sin embargo, cada red o segmento de red puede verse como uno de tres tipos de topología: en estrella, malla completa o malla parcial.

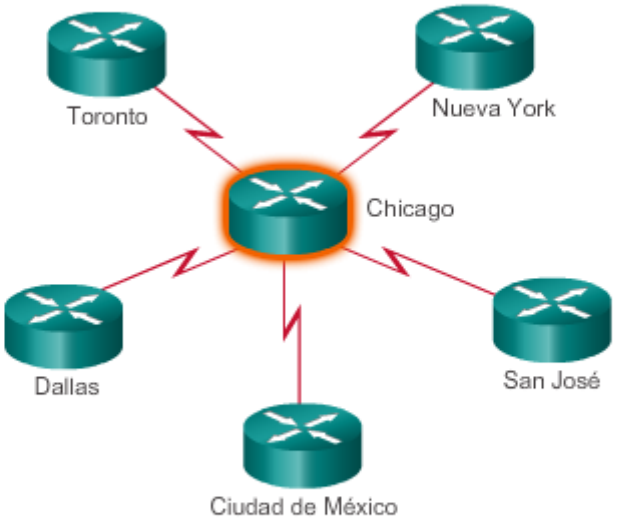
Topología en estrella (hub-and-spoke)

La topología de WAN más simple es una estrella, como la que se muestra en la figura 1. En esta topología, la empresa SPAN Ingeniería tiene un sitio central en Chicago que funciona como hub y aloja los servicios principales.

Las conexiones a cada uno de los cinco sitios remotos funcionan como spokes (que significa “rayos”). En una topología en estrella, la ubicación del hub generalmente se elige por el costo de línea arrendada más bajo. Cuando se implementa una topología en estrella con Frame Relay, cada sitio remoto tiene un enlace de acceso a la nube de Frame Relay con un único VC.

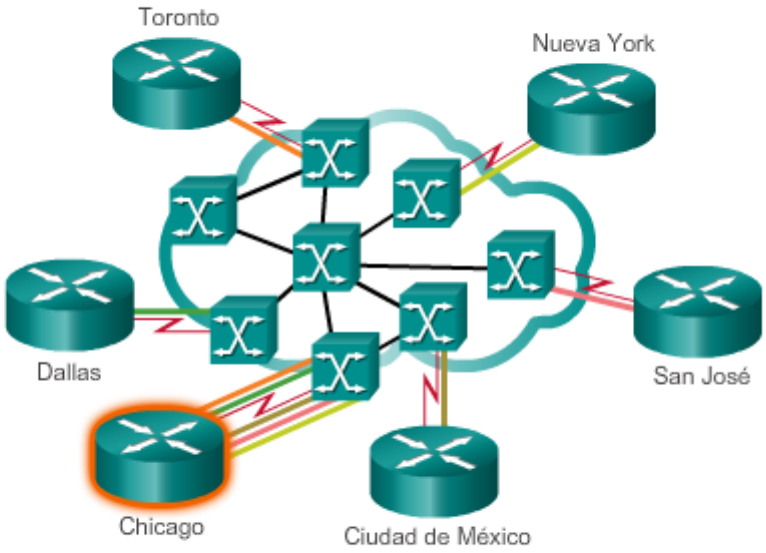
En la figura 2, se muestra la topología en estrella en el contexto de una nube de Frame Relay. El hub en Chicago tiene un enlace de acceso con varios VC, uno para cada sitio remoto. Las líneas que salen de la nube representan las conexiones del proveedor de servicios de Frame Relay y terminan en las instalaciones del cliente. En general, estas líneas tienen velocidades que van desde 56 kb/s hasta un T1 (1544 Mb/s) y más rápidas. Se asigna uno o más números de DLCI a cada terminal de la línea. Debido a que los costos de Frame Relay no se relacionan con la distancia, no es necesario que el hub esté en el centro geográfico de la red.

Topología en estrella (Hub and Spoke)



Topología en estrella: hub de Chicago con cinco enlaces físicos (spokes)

Topología en estrella Frame Relay



Hub de Chicago con un enlace físico que transporta cinco VC.

Capítulo 4: Frame Relay 4.1.2.5 Topologías de Frame Relay (cont.)

Topología de malla completa

En la figura 1, se muestra una topología de malla completa que usa líneas dedicadas. Una topología de malla completa se adapta a una situación en la que los servicios a los que se debe acceder están en distintas zonas geográficas y en la que se requiere un acceso altamente confiable a ellos. Una topología de malla completa conecta cada sitio a todos los demás. Si se utilizan interconexiones de línea arrendada, las líneas y las interfaces seriales adicionales agregan costos. En este ejemplo, se requieren 10 líneas dedicadas para interconectar cada sitio en una topología de malla completa.

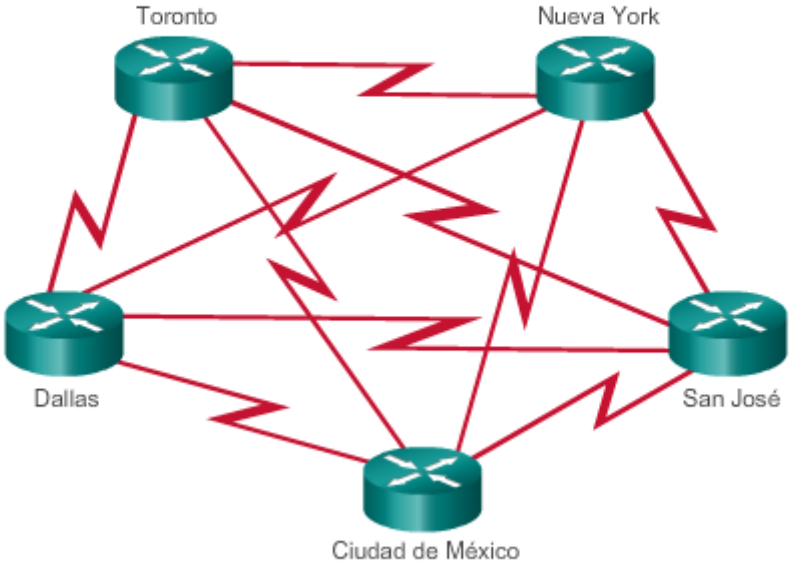
Con una malla de Frame Relay, un diseñador de red puede armar varias conexiones simplemente configurando VC adicionales en cada enlace existente, como se muestra en la figura 2. Esta actualización de software eleva la topología en estrella a una topología de malla completa sin los gastos de hardware o de líneas dedicadas adicionales. Debido a que los VC utilizan la multiplexación estadística, varios VC en un enlace de acceso usan Frame Relay mejor que los VC individuales. En la figura 2, se muestra cómo SPAN utilizó cuatro VC en cada enlace para escalar su red sin agregar nuevo hardware. Los proveedores de servicios cobran el ancho de banda adicional, pero esta solución generalmente es más rentable que usar líneas dedicadas.

Topología de malla parcial

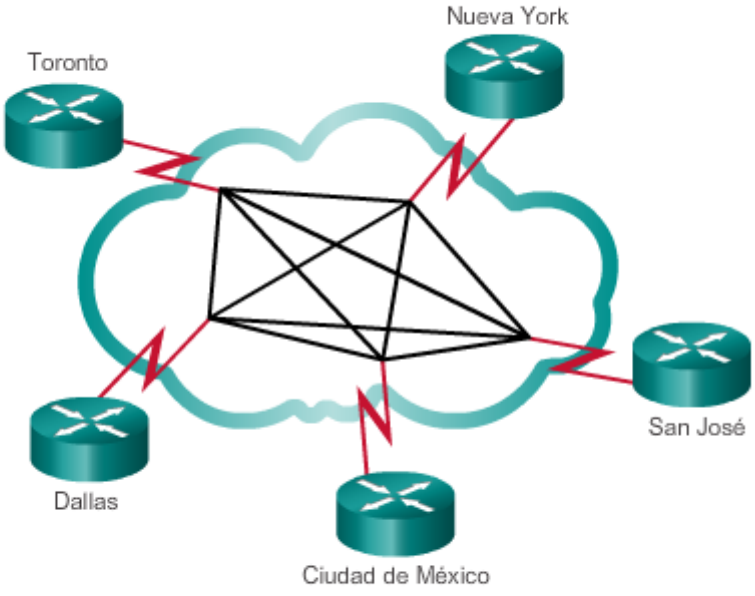
Para las redes grandes, una topología de malla completa rara vez es accesible, porque la cantidad de enlaces necesarios aumenta exponencialmente. El problema no se debe al costo del hardware, sino a que hay un límite teórico de menos de 1000 VC por enlace. En la práctica, el límite es inferior a eso.

Por este motivo, las redes más grandes se suelen configurar en una topología de malla parcial. Con la malla parcial, existen más interconexiones que las requeridas para una configuración en estrella, pero no tantas como para una malla completa. El patrón real depende de los requisitos de flujo de datos.

Topología de malla completa



Malla Frame Relay



Topología de malla: cada DTE tiene un enlace físico que transporta 4 VC.

Capítulo 4: Frame Relay 4.1.2.6 Asignación de direcciones de Frame Relay

Antes de que un router Cisco pueda transmitir datos a través de Frame Relay, necesita saber qué DLCI local se asigna a la dirección de capa 3 del destino remoto. Los routers Cisco admiten todos los protocolos de capa de red mediante Frame Relay, como IPv4, IPv6, IPX y AppleTalk. Esta asignación de dirección a DLCI se puede lograr mediante la asignación estática o dinámica. En la figura 1, se muestra un ejemplo de topología con asignación de DLCI.

ARP inverso

El protocolo de resolución de direcciones (ARP) inverso es una herramienta principal de Frame Relay. Mientras que ARP traduce direcciones IPv4 de capa 3 a direcciones MAC de capa 2, ARP inverso hace lo contrario. Las direcciones IPv4 de capa 3 correspondientes deben estar disponibles antes de que se puedan utilizar los VC.

Nota: Frame Relay para IPv6 utiliza el descubrimiento inverso de vecinos (IND) para obtener una dirección IPv6 de capa 3 a partir de un DLCI de capa 2. Un router Frame Relay envía un mensaje de solicitud IND para solicitar una dirección IPv6 de capa 3 correspondiente a una dirección DLCI de capa 2 del router Frame Relay remoto. Al mismo tiempo, el mensaje de solicitud IND proporciona la dirección DLCI de capa 2 del emisor al router Frame Relay remoto.

Asignación dinámica

La asignación dinámica de direcciones depende de ARP inverso para resolver una dirección IPv4 de capa de red de siguiente salto a un valor de DLCI local. El router Frame Relay envía solicitudes de ARP inverso en su PVC para descubrir la dirección de 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 en el servidor de acceso. El router arma y mantiene esta tabla de asignación, que contiene todas las solicitudes de ARP inverso resueltas, incluidas las entradas de asignación dinámica y estática.

En los routers Cisco, ARP inverso está habilitado de manera 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.

Asignación estática de Frame Relay

El usuario puede elegir anular la asignación dinámica de ARP inverso mediante el suministro de un mapa estático manual para la dirección de protocolo de siguiente salto a un DLCI local. Un mapa estático funciona de manera similar a ARP inverso dinámico mediante la asociación de una dirección de protocolo de siguiente salto específica a un DLCI de Frame Relay local. No se puede utilizar ARP inverso y una instrucción de asignación para el mismo DLCI y el mismo protocolo.

Un ejemplo del uso de la asignación estática de direcciones es una situación en la cual el router en el otro lado de la red Frame Relay no admite ARP inverso dinámico para un protocolo de red específico. A fin de proporcionar conectividad, se requiere una asignación estática para completar la dirección de capa de red remota a la resolución de DLCI local.

En una red Frame Relay hub-and-spoke, se da otro ejemplo. Utilice la asignación estática de direcciones en los routers spoke para proporcionar la posibilidad de conexión de spoke a spoke. Debido a que los routers spoke no tienen conectividad directa entre sí, ARP inverso dinámico no funciona entre ellos. ARP inverso dinámico depende de la presencia de una conexión punto a punto directa entre dos extremos. En este caso, ARP inverso dinámico solo

funciona entre hub y spoke, y los spokes requieren asignación estática para proporcionar la posibilidad de conexión entre sí.

Configuración de la asignación estática

El establecimiento de la asignación estática depende de las necesidades de la red. Para asignar entre una dirección de protocolo de siguiente salto y una dirección de destino DLCI, utilice este comando: **frame-relay map** *protocol protocol-addressdlci* [**broadcast**] [**ietf**] [**cisco**].

Utilice la palabra clave **ietf** cuando se conecte a un router que no es de Cisco.

La configuración del protocolo OSPF (Open Shortest Path First) se puede simplificar considerablemente agregando la palabra clave optativa **broadcast** cuando se realiza esta tarea. La palabra clave**broadcast** especifica que se permite el tráfico de difusión y multidifusión en el VC. Esta configuración permite el uso de protocolos de routing dinámico en el VC.

En la figura 2, se 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 0/0/1. La encapsulación de Frame Relay que se usa en el DLCI 102 es CISCO. Como se observa en los pasos de configuración, la asignación estática de direcciones mediante el comando **frame-relay map** permite que los usuarios seleccionen el tipo de encapsulación de Frame Relay que se utiliza por VC.

En la figura 3, se muestra el resultado del comando **show frame-relay map**. Observe que la interfaz está activa y la dirección IPv4 de destino es 10.1.1.2. El DLCI identifica la conexión que se usa para llegar a esta interfaz. Este valor se muestra en valor decimal (102), en valor hexadecimal (0x66) y en el valor que aparecería en el cable (0x1860). Esta es una entrada estática, no una entrada dinámica. El enlace utiliza la encapsulación Cisco en lugar de la encapsulación IETF.

Asignación estática de Frame Relay

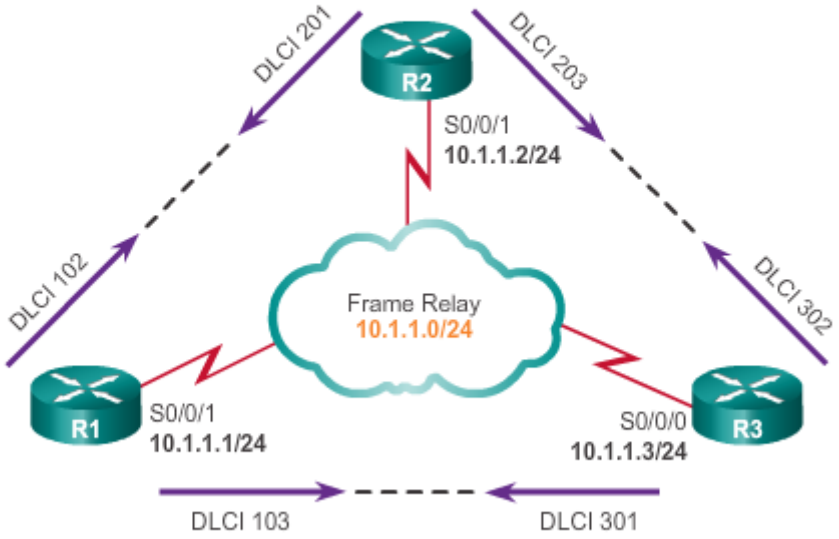


Tabla de asignación de direcciones a DLCI

```
R1(config)# interface serial 0/0/1
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# encapsulation frame-relay
R1(config-if)# no frame-relay inverse-arp
R1(config-if)# frame-relay map ip 10.1.1.2 102 broadcast
cisco
R1(config-if)# no shutdown
R1(config-if)#
*Mar 31 18:57:38.994: %LINK-3-UPDOWN: Interface Serial0/0/1,
changed state to up
R1(config-if)#
```

Asignación estática de Frame Relay

```
R1# show frame-relay map
Serial0/0/1 (up): ip 10.1.1.2 dlci 102(0x66,0x1860), static,
              broadcast,
              CISCO, status defined, active
R1#
```

Capítulo 4: Frame Relay 4.1.2.7 Interfaz de administración local (LMI)

Otro concepto importante en Frame Relay es la interfaz de administración local (LMI). El diseño de Frame Relay proporciona la transferencia de datos conmutada por paquetes con retrasos mínimos de extremo a extremo. El diseño original omite cualquier cosa que pudiera ocasionar un retraso.

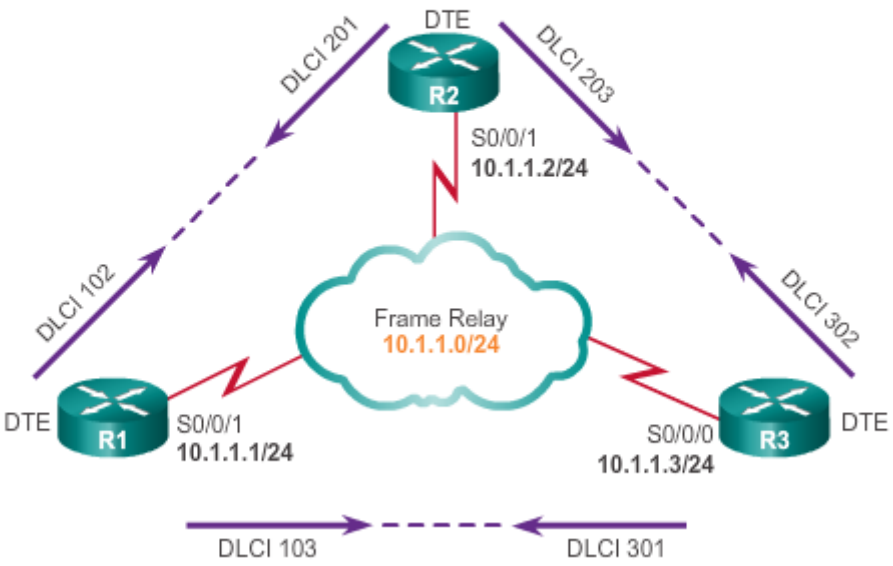
Cuando los proveedores implementaron Frame Relay como una tecnología independiente y no como un componente de ISDN, decidieron que los DTE debían adquirir dinámicamente la información sobre el estado de la red. Sin embargo, el diseño original no incluía esta característica. Un consorcio de Cisco, Digital Equipment Corporation (DEC), Northern Telecom y StrataCom amplió el protocolo Frame Relay a fin de proporcionar capacidades adicionales para los entornos complejos de internetworking. Estas ampliaciones se conocen colectivamente como la LMI.

Consulte la topología de Frame Relay de la figura 1. Básicamente, la LMI es un mecanismo keepalive que proporciona información acerca del estado de las conexiones Frame Relay entre el router (DTE) y el switch Frame Relay (DCE). Aproximadamente cada 10 segundos, la terminal sondea la red, ya sea para solicitar una respuesta muda secuencial o información del estado del 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 de FULL STATUS, incluye información sobre el estado de los DLCI que se asignan a esa línea. La terminal puede utilizar esta información para determinar si las conexiones lógicas pueden pasar datos.

En la figura 2, se muestra el resultado del comando **show frame-relay lmi**. El resultado muestra el tipo de LMI que usa la interfaz de Frame Relay y los contadores para la secuencia de intercambio del estado de LMI, incluidos los errores como los tiempos de espera de LMI.

Es fácil confundir la LMI y la encapsulación. La LMI es una definición de los mensajes que se usan entre el DTE (el R1) y el DCE (el switch Frame Relay que pertenece al proveedor de servicios). La encapsulación define los encabezados que utiliza un DTE para comunicar información al DTE en el otro extremo de un VC. Al switch y al router conectado a él les interesa utilizar el mismo LMI. Al switch no le interesa la encapsulación. A los routers terminales (DTE) sí les interesa la encapsulación.

Estadísticas de LMI



Asignación estática de Frame Relay

```
R1# show frame-relay lmi

LMI Statistics for interface Serial0/0/1 (Frame Relay DTE)
LMI TYPE = CISCO
  Invalid Unnumbered info 0Invalid Prot Disc 0
  Invalid dummy Call Ref 0Invalid Msg Type 0
  Invalid Status Message 0Invalid Lock Shift 0
  Invalid Information ID 0Invalid Report IE Len 0
  Invalid Report Request 0Invalid Keep IE Len 0
  Num Status Enq. Sent 368Num Status msgs Rcvd 369
  Num Update Status Rcvd 0Num Status Timeouts 0
  Last Full Status Req 00:00:29Last Full Status Rcvd 00:00:29
R1#
```

Capítulo 4: Frame Relay 4.1.2.8 Extensiones de LMI

Además de las funciones de transferencia de datos del protocolo Frame Relay, la especificación de Frame Relay incluye extensiones optativas de LMI. Algunas de estas extensiones son las siguientes:

- **Mensajes de estado de VC:**proporcionan información sobre la integridad del PVC mediante la comunicación y la sincronización entre dispositivos, informes periódicos sobre la existencia de nuevos PVC y la eliminación de PVC existentes. Los mensajes de estado de VC evitan que los datos se envíen a agujeros negros (PVC que ya no existen).

- **Multidifusión:** permite que un emisor transmita una única trama que se entrega a varios receptores. La multidifusión da soporte a la entrega eficaz de los mensajes de protocolo de routing y los procedimientos de resolución de direcciones que se envían típicamente a varios destinos en forma simultánea.

- **Direccionamiento global:** proporciona ID de conexiones con importancia global en lugar de importancia local, lo que permite que se usen para identificar una interfaz específica de la red Frame Relay. El direccionamiento global hace que la red Frame Relay se asemeje a una LAN en términos de direccionamiento, y los ARP se utilizan como en una LAN.

- **Control del flujo simple:** proporciona un mecanismo de control del flujo XON/XOFF que se aplica a toda la interfaz de Frame Relay. Está diseñado para los dispositivos que no pueden usar los bits de notificación de congestión (es decir, FECN y BECN) que aprovecharían las capas superiores, pero que de todas formas requieren cierto nivel de control del flujo.

La LMI se utiliza para administrar enlaces de Frame Relay. Cada mensaje de LMI se clasifica mediante un DLCI que aparece en la trama LMI. El campo DLCI de 10 bits admite 1024 ID de VC: de 0 a 1023, como se muestra en la figura 1. Las extensiones de LMI reservan algunas de estas ID de VC, lo que reduce la cantidad de VC permitidos. Los mensajes de LMI se intercambian entre el DTE y el DCE mediante estos DLCI reservados.

Existen varios tipos de LMI, y cada uno es incompatible con los demás. El tipo de LMI configurado en el router debe coincidir con el tipo que utiliza el proveedor de servicios. Los routers Cisco admiten tres tipos de LMI:

- **CISCO:** extensión original de LMI

- **ANSI:** correspondiente al estándar ANSI T1.617, anexo D

- **Q933A:** correspondiente al estándar ITU Q933, anexo A

Para mostrar la información de los mensajes de LMI y los números de DLCI asociados, use el comando **show interfaces** [*tipo número*], como se muestra en la figura 2. Cisco utiliza el DLCI 1023 para identificar los mensajes de LMI que se usan para la administración de enlaces Frame Relay.

A partir del software IOS de Cisco versión 11.2, la característica predeterminada de detección automática de LMI detecta el tipo de LMI que admite el switch Frame Relay conectado directamente. Sobre la base 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 que reconoce el switch Frame Relay. Si es necesario establecer el tipo de LMI, utilice el comando de configuración de interfaz **frame-relay lmi-type**[**cisco** | **ansi** | **q933a**]. La configuración del tipo de LMI deshabilita la característica de detección automática.

En los casos en los que un switch Frame Relay utiliza la configuración de tiempo de espera no predeterminada, también se debe configurar el intervalo de keepalive en la interfaz de Frame Relay para evitar que los mensajes de intercambio de estado expiren. Los mensajes de intercambio de estado de LMI determinan el estado de la conexión de PVC. Una incompatibilidad importante en el intervalo de keepalive en el router y el switch puede hacer que el switch declare inactivo al router. Es importante consultar al proveedor de servicios de Frame Relay para obtener información sobre cómo modificar la configuración de keepalive. De manera predeterminada, el intervalo de tiempo keepalive en las interfaces seriales de Cisco es

de 10 segundos. Puede cambiar el intervalo de keepalive con el comando de configuración de interfaz**keepalive**.

Los mensajes de estado ayudan a verificar la integridad de los enlaces lógicos y físicos. Esta información es fundamental en un entorno de routing, porque los protocolos de routing toman decisiones sobre la base de la integridad del enlace.

Como se muestra en la figura 3, los mensajes de estado de LMI son similares a la trama Frame Relay. En lugar del campo Dirección de una trama Frame Relay que se utiliza para la transmisión de datos, hay un campo DLCI de LMI. A continuación del campo DLCI están los campos Control, Discriminador de protocolo y Referencia de llamada. Estos son los mismos que en la trama de datos de Frame Relay estándar. El cuarto campo indica el tipo de mensajes de LMI e incluye uno de los tres tipos de mensajes de LMI que admite Cisco.

Identificadores LMI

Identificadores de VC	Tipos de VC
0	Administración de enlace LMI (ANSI, ITU)
1 a 15	Se reserva para uso futuro
16 a 991	Disponible para la asignación de terminal de VC
992 a 1007	Información de administración de capa2 optativa
1008 a 1018	Se reserva para uso futuro (ANSI, UIT)
1019 a 1022	Multidifusión de LMI
1023	Administración de enlace LMI (Cisco)

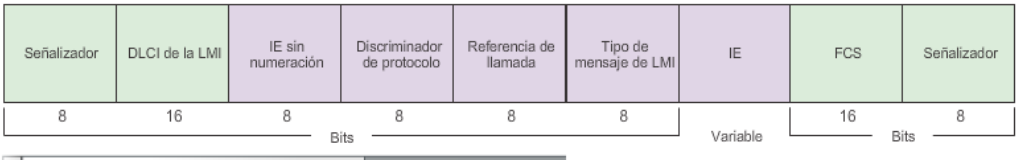
Visualización del tipo de LMI

```
R1# show interfaces serial 0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  MTU 1500 bytes, BW 1544 Kbit/sec, 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  443, LMI stat recvd 444, 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 1723/0,
interface broadcasts 1582
  Last input 00:00:01, output 00:00:01, output hang never

<resultado omitido>
```

Formato de trama LMI

La trama Frame Relay estándar es la base de una trama LMI.



Capítulo 4: Frame Relay 4.1.2.9 Uso de LMI y ARP inverso para asignar direcciones

Los mensajes de estado de LMI combinados con los mensajes de ARP inverso permiten que un router asocie direcciones de capa de red y de capa de enlace de datos.

Reproduzca la animación de la figura 1 para ver cómo comienza el proceso de LMI.

En este ejemplo, cuando el R1 se conecta a la red Frame Relay, envía un mensaje de consulta de estado de LMI a la red. La red responde con un mensaje de estado de 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 incluyen solo cambios de estado. Después de una cantidad establecida de estas respuestas abreviadas, la red envía un mensaje de estado completo.

Si el router necesita asignar los VC a direcciones de capa de red, envía un mensaje de ARP inverso en cada VC. ARP inverso funciona de manera similar a ARP en una red local Ethernet, con la excepción de que ARP inverso no transmite solicitudes por difusión. Con ARP, el dispositivo emisor conoce la dirección IP de capa 3 y envía una difusión para descubrir la dirección MAC de capa 2 de destino. Con ARP inverso, el router conoce la dirección de capa 2, que es el DLCI local, y envía una solicitud para la dirección IP de capa 3 de destino.

Funcionamiento de ARP inverso

Cuando una interfaz que admite ARP inverso se activa, inicia el protocolo ARP inverso y da formato a una solicitud de ARP inverso para el VC activo. La solicitud de ARP inverso incluye el hardware de origen, la dirección de protocolo de capa 3 de origen y la dirección conocida del hardware de destino. A continuación, rellena el campo de dirección del protocolo de capa 3 de destino solo con ceros. Encapsula el paquete para la red específica y lo envía directamente al dispositivo de destino mediante el VC.

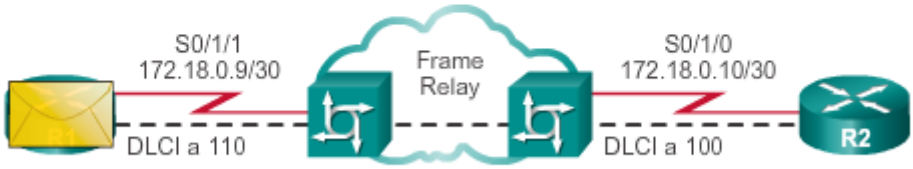
Al recibir una solicitud de ARP inverso, el dispositivo de destino utiliza la dirección del dispositivo de origen para crear su propio mapa de DLCI a capa 3. Después envía una respuesta de ARP inverso que incluye la información de su dirección de capa 3. Cuando el dispositivo de origen recibe la respuesta de ARP inverso, completa el mapa de DLCI a capa 3 con la información proporcionada.

Cuando se configura una interfaz en un router Cisco para que utilice la encapsulación de Frame Relay, ARP inverso se habilita de manera predeterminada.

Reproduzca la animación de la figura 2 para ver el funcionamiento de ARP inverso.

Formato de trama LMI

El DTE envía un mensaje de consulta de estado al DCE.

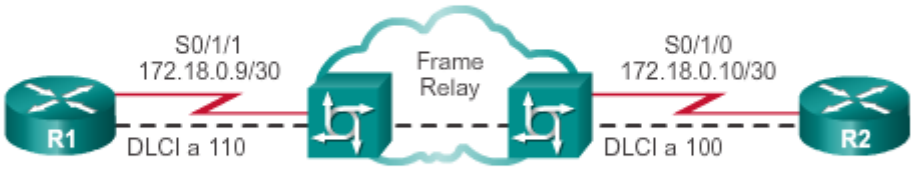


Formato de trama LMI

El DCE responde con un mensaje de estado que incluye los DLCI.

Formato de trama LMI

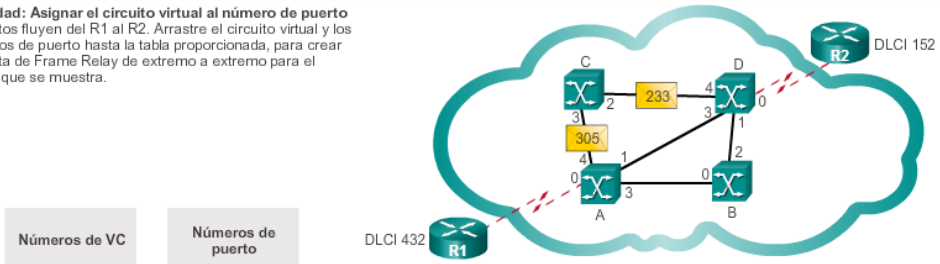
El DTE descubre sus VC.



DLCI	Estado
101	Activo
102	Activo
103	Activo
104	Activo

Capítulo 4: Frame Relay 4.1.2.10 Actividad: Asignar el circuito virtual al número de puerto

Actividad: Asignar el circuito virtual al número de puerto
Los datos fluyen del R1 al R2. Arrastre el circuito virtual y los números de puerto hasta la tabla proporcionada, para crear una ruta de Frame Relay de extremo a extremo para el tráfico que se muestra.



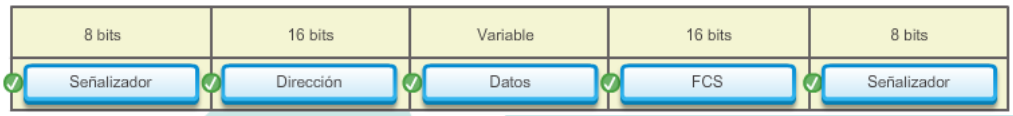
Números de VC
152
233
305
432

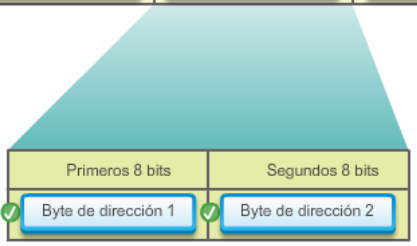
Números de puerto
0
1
2
3
4

	Ingreso		Egreso	
Tramo	VC	Puerto	VC	Puerto
A	432	0	305	4
C	305	3	233	2
D	233	4	152	0

Capítulo 4: Frame Relay 4.1.2.11 Actividad: Unir los campos de Frame Relay con la definición

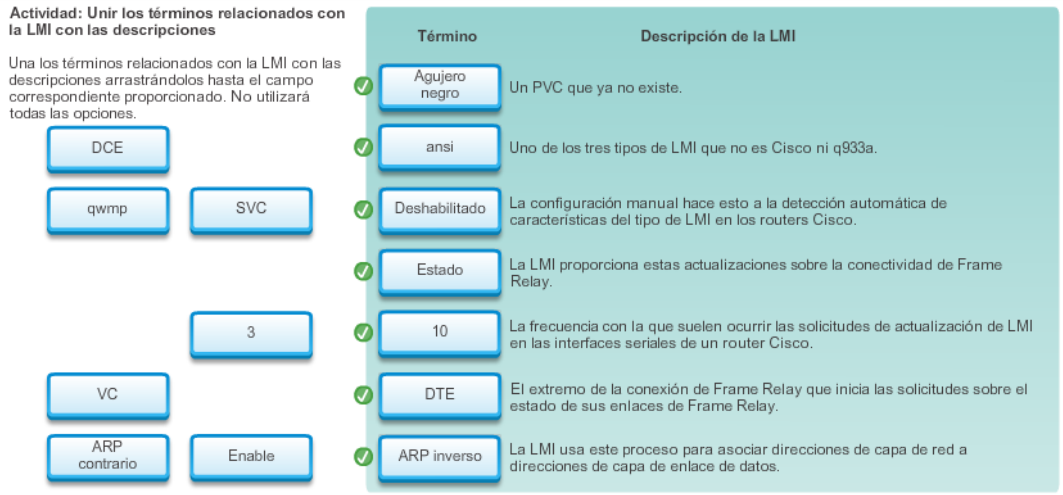
Actividad: Ordenar los campos de la trama Frame Relay
Ordene los campos de la trama Frame Relay arrastrando las etiquetas con el nombre del campo hasta el espacio correspondiente proporcionado. Algunas etiquetas se pueden usar más de una vez





Nombre de campo	Definición
Datos	Paquetes
FCS	Valor calculado para revisar errores de transmisión
Señalizador	Un valor binario numérico especial 01111110
Byte de dirección 2	Incluye valores de DLCI, FECN, BECN, DE y EA
Byte de dirección 1	Incluye valores de DLCI, C/R y EA
Dirección	Valores de control de Frame Relay

Capítulo 4: Frame Relay 4.1.2.12 Actividad: Identificar la terminología y los conceptos de LMI



Capítulo 4: Frame Relay 4.1.3.1 Velocidad de acceso y velocidad de información comprometida

Los proveedores de servicios arman las redes Frame Relay con switches muy grandes y potentes, pero los dispositivos solo ven la interfaz del switch del proveedor de servicios. En general, los clientes no están expuestos al funcionamiento interno de la red, que se puede armar con tecnologías de muy alta velocidad, como SONET o SDH.

Desde el punto de vista de un cliente, Frame Relay es una interfaz única configurada con uno o más PVC. Los clientes adquieren los servicios de Frame Relay de un proveedor de servicios. Antes de considerar cómo pagar los servicios de Frame Relay, se deben aprender algunos términos y conceptos, como los que se muestra en la ilustración:

- **Velocidad de acceso:** la velocidad de acceso se refiere a la velocidad del puerto. Desde el punto de vista de un 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 acceso es la velocidad a la que sus circuitos de acceso se unen a la red Frame Relay. Estos pueden ser de 56 kb/s, T1 (1544 Mb/s) o T1 fraccionada (un múltiplo de 56 kb/s o de 64 kb/s). Las velocidades de acceso se miden en el switch Frame Relay. No es posible enviar datos a mayor velocidad que la velocidad de acceso.

- **Velocidad de información comprometida (CIR):** los clientes negocian las CIR con los proveedores de servicios para cada PVC. La CIR es la cantidad de datos que la 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 esta se aceptan.

La CIR especifica la velocidad de datos máxima promedio que la red se compromete a entregar en condiciones normales. Al suscribirse a un servicio de Frame Relay, se especifica la velocidad de acceso local, por ejemplo, 56 kb/s o T1. Normalmente, el proveedor solicita que el cliente especifique una CIR para cada DLCI.

Si el cliente envía la información más rápido que la CIR en un DLCI determinado, la red marca algunas tramas con un bit de elegibilidad de descarte (DE). La red hace lo mejor para entregar todos los paquetes; sin embargo, descarta primero los paquetes DE si hay congestión.

Nota: muchos servicios Frame Relay económicos se basan en una CIR de cero (0). Una CIR de cero significa que cada trama es una trama DE, y la red descarta cualquier trama cuando lo necesita. El bit DE forma parte del campo de dirección en el encabezado de la trama Frame Relay.

Terminología de los servicios de Frame Relay

Término	Acceso
Velocidad de acceso	La capacidad del bucle local.
Velocidad de información suscrita (CIR, Committed Information Rate)	La capacidad a través del bucle local que garantiza el proveedor.

Capítulo 4: Frame Relay 4.1.3.2 Ejemplo de Frame Relay

Independientemente de cualquier costo de CPE, el cliente paga por tres componentes de los costos de Frame Relay siguientes:

- **Velocidad de acceso:** el costo de la línea de acceso desde el DTE hasta el DCE (del cliente al proveedor de servicios). Esta línea se cobra sobre la base de la velocidad del puerto que se negoció y se instaló.

- **PVC:** este componente de los costos se basa en los PVC. Después de establecer un PVC, el costo adicional para aumentar la CIR suele ser bajo y se puede hacer en pequeños incrementos (4 kb/s).

- **CIR:** en general, los clientes eligen una CIR inferior a la velocidad de acceso. Esto les permite aprovechar las ráfagas.

En el ejemplo de la ilustración, el cliente paga por lo siguiente:

- Una línea de acceso con una velocidad de 64 kb/s que conecta su DTE al DCE del proveedor de servicios a través del puerto serie S0/0/1.

- Dos puertos virtuales, uno a 32 kb/s y el otro a 16 kb/s.

- Una CIR de 48 kb/s a través de toda la red Frame Relay. Por lo general, es un cargo fijo y no se relaciona con la distancia.

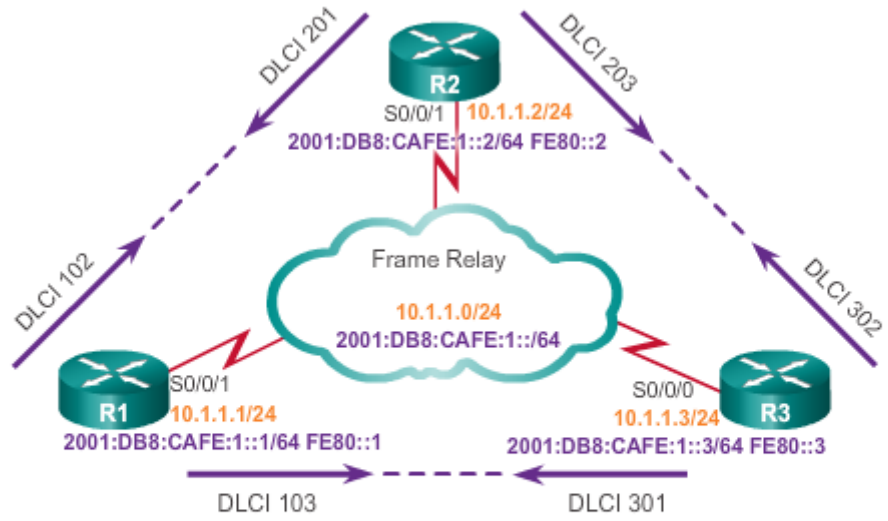
Nota: los valores de ancho de banda que se usan en este capítulo son solo con fines comparativos. No reflejan necesariamente implementaciones reales.

Sobresuscripción

En ocasiones, los proveedores de servicios venden más capacidad de la que tienen, con la suposición de que no todos exigen la capacidad que tienen permitida todo el tiempo. Esta sobresuscripción es similar a que las aerolíneas vendan más asientos de los que tienen con la expectativa de que algunos de los clientes reservados no se presenten. Debido a la

sobresuscripción, hay situaciones en las que la suma de las CIR de varios PVC a una ubicación dada es superior a la velocidad del puerto o del canal de acceso. Esto puede causar congestión y descarte de tráfico.

Cargos de Frame Relay: ejemplo



Se cobran tres componentes para el R1:	
Bucle local	64 kb/s
Dos puertos	DLCI 102 DLCI 103
CIR	48 kb/s

CIR para cada PVC:	
PVC DLCI	**CIR**
DLCI 102	32 kb/s
DLCI 103	16 kb/s
CIR total	**48 kb/s**

Capítulo 4: Frame Relay 4.1.3.3 Ráfaga

Una gran ventaja de Frame Relay es que cualquier capacidad de red que no se utilice queda a disposición de todos los clientes o se comparte con ellos, generalmente sin cargo adicional. Esto permite que los clientes excedan la CIR a modo de bonificación.

Con el ejemplo anterior, en la figura 1 se muestra que la velocidad de acceso en el puerto serie S0/0/1 del router R1 es de 64 kb/s. Esto supera la combinación de las CIR de los dos PVC. En circunstancias normales, los dos PVC no deben transmitir más de 32 kb/s y 16 kb/s, respectivamente. Mientras la cantidad de datos que envían los dos PVC no exceda la CIR, debería atravesar la red.

Debido a que los circuitos físicos de la red Frame Relay se comparten entre los suscriptores, suele haber momentos en los que hay 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 que excedan la CIR sin costo.

Las ráfagas permiten que los dispositivos que necesitan ancho de banda adicional temporalmente puedan tomarlo prestado de otros dispositivos que no lo utilizan, sin costo adicional. Por ejemplo, si el PVC 102 transfiere un archivo grande, podría usar cualquiera de los 16 kb/s que no utiliza el PVC 103. Un dispositivo puede llegar hasta la velocidad de acceso y aun así esperar que los datos pasen. La duración de una transmisión en ráfaga debe ser inferior a tres o cuatro segundos.

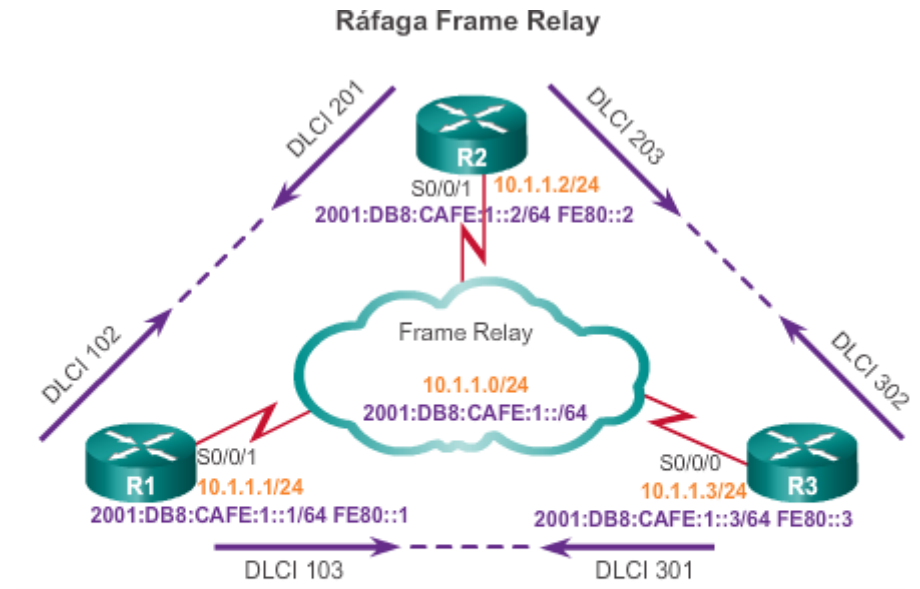
Se utilizan varios términos para describir las velocidades de ráfaga, incluidos “tamaño de ráfaga comprometida” (Bc) y “tamaño de ráfaga en exceso” (Be).

El Bc es una velocidad negociada por encima de la CIR que el cliente puede usar para transmitir durante una ráfaga breve y que representa el tráfico máximo permitido en condiciones de funcionamiento normales. Permite que el tráfico se transmita en ráfaga a velocidades más altas, tanto como el ancho de banda disponible de la red lo permita. Sin embargo, no puede exceder la velocidad de acceso del enlace. Un dispositivo puede llegar hasta el Bc y aun así esperar que los datos pasen. Si persisten las ráfagas largas, se debe adquirir una CIR más alta.

Por ejemplo, el DLCI 102 tiene una CIR de 32 kb/s con un Bc adicional de 16 kb/s para obtener un total de hasta 48 kb/s. El DLCI 103 tiene una CIR de 16 kb/s. Sin embargo, el DLCI 103 no tiene un Bc negociado; por lo tanto, la Bc se establece en 0 kb/s. Las tramas dentro de las CIR negociadas no son elegibles para descarte (DE = 0). Las tramas por encima de la CIR tienen el bit DE establecido en 1, lo que las marca como elegibles para descarte si se congestiona la red. Las tramas que se envían en el nivel de Bc se marcan como elegibles para descarte (DE) en el encabezado de la trama, pero es muy probable que se reenvíen.

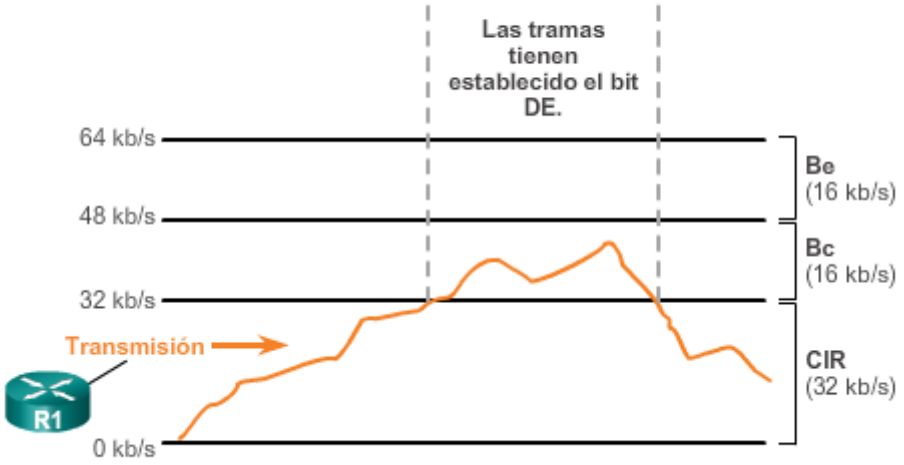
El Be describe el ancho de banda disponible por encima de la CIR hasta la velocidad de acceso del enlace. A diferencia del Bc, no se negocia. Las tramas se pueden transmitir en este nivel, pero es muy probable que se descarten.

En la figura 2, se muestra la relación entre los diversos términos relacionados con las ráfagas.



PVC DCLI	CIR (normal)	Bc (ejemplo)	Be
DCLI 102	32 kb/s	48 kb/s	16 kb/s
DCLI 103	16 kb/s	0 kb/s	48 kb/s
	Se reenvían todas las tramas.	Las tramas se reenvían, pero con la marca DE.	Lo más probable es que las tramas se descarten.

Ejemplo de ráfaga de Frame Relay



Capítulo 4: Frame Relay 4.1.3.4 Control del flujo de Frame Relay

Frame Relay reduce la sobrecarga de la red mediante la implementación de mecanismos sencillos de notificación de congestión, en lugar del control del flujo explícito por VC. Estos mecanismos de notificación de congestión son la notificación explícita de congestión hacia delante (FECN) y la notificación explícita de la congestión hacia atrás (BECN).

Para comprender los mecanismos, en la figura 1 se muestra la estructura de la trama Frame Relay estándar para su revisión. La FECN y la BECN se controlan mediante un único bit

incluido en el encabezado de la trama. Le informan al router que hay congestión y que debe detener la transmisión hasta que la condición se revierta. Cuando el DCE establece el bit BECN en 1, notifica a los dispositivos en el sentido del origen (ascendente) que hay congestión en la red. Cuando el DCE establece el bit FECN en 1, notifica a los dispositivos en el sentido del destino (descendente) que hay congestión en la red.

El encabezado de trama también contiene el bit DE, que identifica el tráfico menos importante que se puede descartar durante los períodos de congestión. Los dispositivos DTE pueden establecer el valor del bit DE en 1 para indicar que la trama tiene menos importancia que otras tramas. Cuando la red se congestiona, los dispositivos DCE descartan las tramas con el bit DE establecido en 1 antes de descartar las que no lo tienen. Esto reduce la probabilidad de que se descarten datos importantes durante los períodos de congestión.

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

- Si la trama entrante no excede el Bc, la trama se pasa.
- Si una trama entrante excede el Bc, se marca como DE.
- Si una trama entrante excede el Bc y el Be, se descarta.

Haga clic en el botón Reproducir de la animación de la figura 2 para ver cómo se usan la FECN y la BECN.

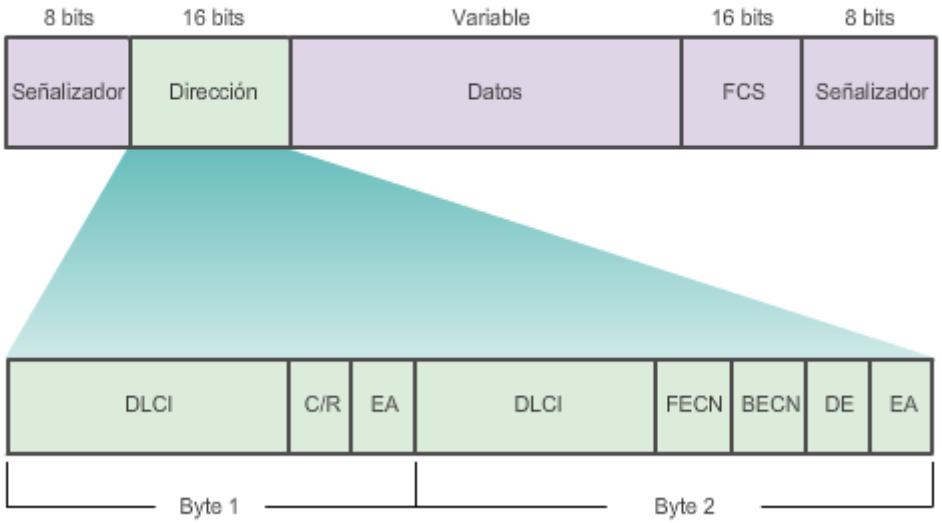
Las tramas que llegan a un switch se ponen en cola o se almacenan en búfer antes del reenvío. Como en cualquier sistema de puesta en cola, es posible que haya una acumulación excesiva de tramas en un switch. Esto genera retrasos que llevan a retransmisiones innecesarias que se producen cuando los protocolos de nivel superior no reciben un acuse de recibo en un plazo establecido. En casos graves, esto puede causar una importante caída del rendimiento de la red. Para evitar este problema, Frame Relay incorpora una característica de control del flujo.

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

- El bit FECN, que se indica con una F, se establece en cada trama que recibe el switch en el enlace congestionado.
- El bit BECN, que se indica con una B, se establece en cada trama que el switch coloca en el enlace congestionado.

Se espera que los DTE que reciben las tramas con los bits ECN establecidos busquen reducir el flujo de tramas hasta que se despeje la congestión. Si la congestión se produce en un enlace troncal interno, los DTE pueden recibir una notificación aunque no sean la causa de la congestión.

Trama Frame Relay estándar

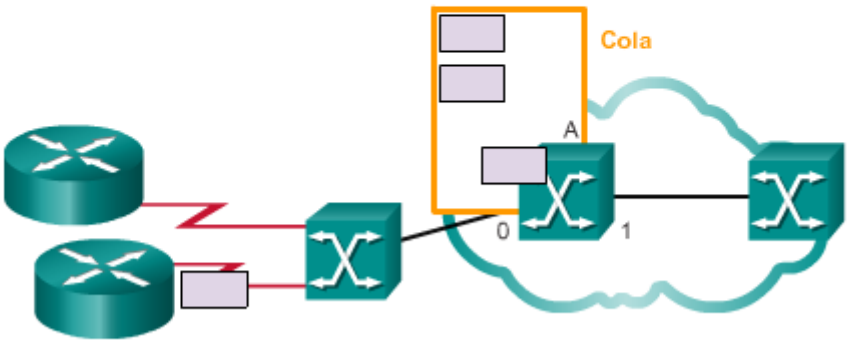


Control del ancho de banda de FR: puesta en cola

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

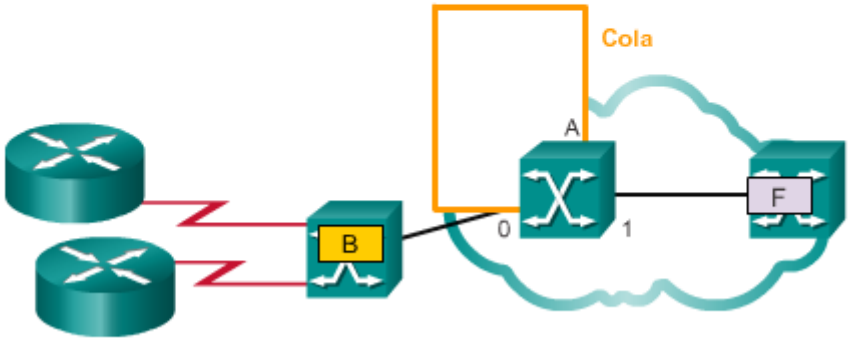
Control del ancho de banda de FR: puesta en cola

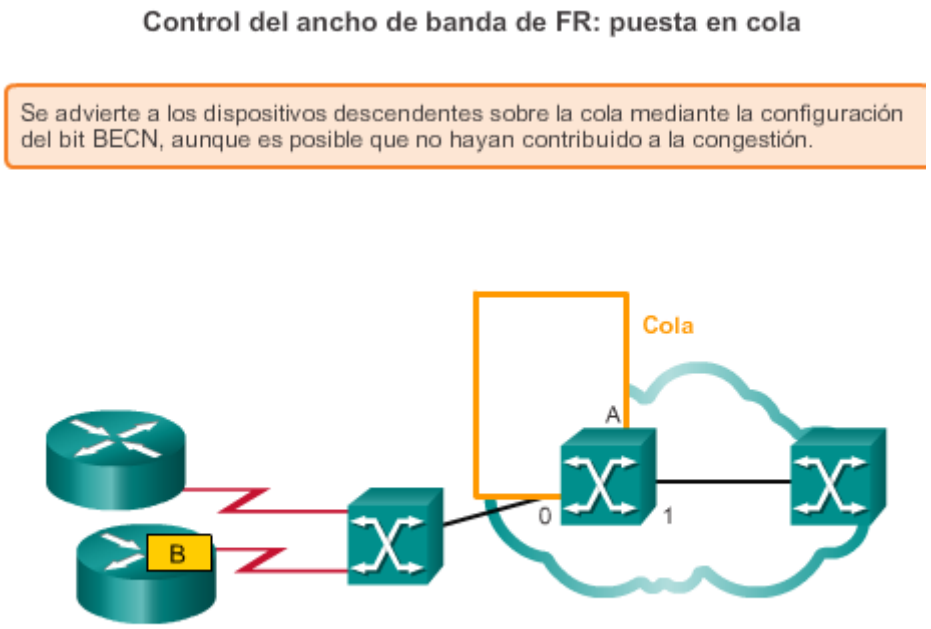
Se advierte a los dispositivos ascendentes sobre la cola mediante la configuración del bit FECN.



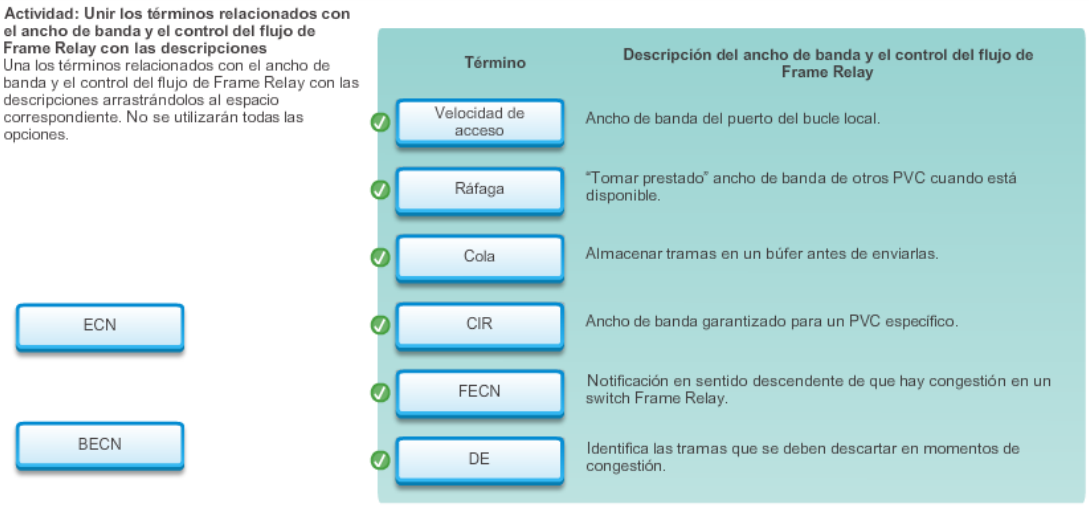
Control del ancho de banda de FR: puesta en cola

Se advierte a los dispositivos ascendentes sobre la cola mediante la configuración del bit FECN.





Capítulo 4: Frame Relay 4.1.3.5 Actividad: Identificar la terminología relacionada con ancho de banda y control del flujo de Frame Relay



Capítulo 4: Frame Relay 4.2.1.1 Comandos de configuración básica de Frame Relay

Frame Relay se configura en un router Cisco desde la interfaz de línea de comandos (CLI) del IOS de Cisco. En la figura 1, se muestran los pasos obligatorios y optativos para configurar Frame Relay.

En la figura 2, se muestra la topología de tres routers que se utiliza en esta sección, aunque el enfoque inicial se centra en el enlace Frame Relay entre el R1 y el R2, la red 10.1.1.0/24. Observe que todos los routers se configuraron con direcciones IPv4 e IPv6.

Paso 1. Establezca la dirección IP en la interfaz

En un router Cisco, Frame Relay se admite generalmente en las interfaces seriales síncronas. Utilice el comando **ip address** para establecer la dirección IPv4 de la interfaz.

En el enlace entre el R1 y el R2, se asignó la dirección 10.1.1.1/24 a S0/0/1 del R1 y la dirección IPv4 10.1.1.2/24 a S0/0/1 del R2.

Con el comando **ipv6 address**, los routers R1 y R2 también se configuraron con las siguientes direcciones IPv6:

- El R1 se configuró con la dirección IPv6 de unidifusión global 2001:DB8:CAFE:1::1/64 y la dirección link-local estática FE80::1.

- El R2 se configuró con la dirección IPv6 de unidifusión global 2001:DB8:CAFE:1::2/64 y la dirección link-local estática FE80::2.

Nota: de manera predeterminada, el IOS de Cisco utiliza EUI-64 para generar automáticamente la dirección IPv6 link-local en una interfaz. La configuración de direcciones link-local estáticas facilita recordar e identificar las direcciones link-local. Los protocolos de routing IPv6 usan las direcciones IPv6 link-local para los mensajes de routing y las direcciones de siguiente salto en la tabla de routing IPv6.

Paso 2. Configure la encapsulación

El comando de configuración de interfaz**encapsulation frame-relay** [**cisco**| **ietf**] habilita la encapsulación de Frame Relay y permite el procesamiento de Frame Relay en la interfaz admitida. Existen dos opciones de encapsulación para escoger: cisco e ietf.

- El tipo de encapsulación cisco es la encapsulación de Frame Relay predeterminada habilitada en las interfaces admitidas. Utilice esta opción si se conecta a otro router Cisco. Muchos dispositivos que no son de Cisco también admiten este tipo de encapsulación. Utiliza un encabezado de 4 bytes, con 2 bytes para identificar el DLCI y 2 bytes para identificar el tipo de paquete.

- El tipo de encapsulación ietf cumple con RFC 1490 y RFC 2427. Utilice esta opción si se conecta a un router que no es de Cisco.

Paso 3. Establezca el ancho de banda

Utilice el comando **bandwidth** para establecer el ancho de banda de la interfaz serial. Especifique el ancho de banda en kb/s. Este comando notifica al protocolo de routing que el ancho de banda se configuró estáticamente en el enlace. Los protocolos de routing EIGRP y OSPF usan el valor de ancho de banda para calcular y determinar la métrica del enlace.

Paso 4. Establezca el tipo de LMI (optativo)

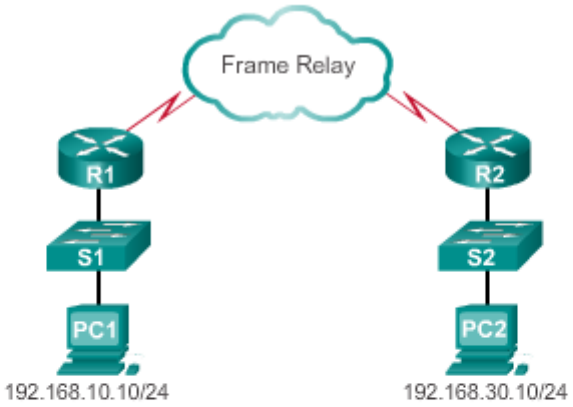
La configuración manual del tipo de LMI es optativa, ya que los routers Cisco detectan automáticamente el tipo de LMI de manera predeterminada. Recuerde que Cisco admite tres tipos de LMI: cisco, ANSI anexo D y Q933-A anexo A. El tipo de LMI predeterminado para los routers Cisco es cisco.

En la figura 3, se muestran las configuraciones del R1 y el R2 para habilitar Frame Relay.

El comando **show interfaces serial**verifica la configuración, incluida la encapsulación de capa 2 de Frame Relay y el tipo de LMI predeterminado cisco, como se muestra en la figura 4. Observe que este comando muestra la dirección IPv4, pero no incluye ninguna de las direcciones IPv6. Utilice el comando **show ipv6 interface** o el comando **show ipv6 interface brief** para verificar IPv6.

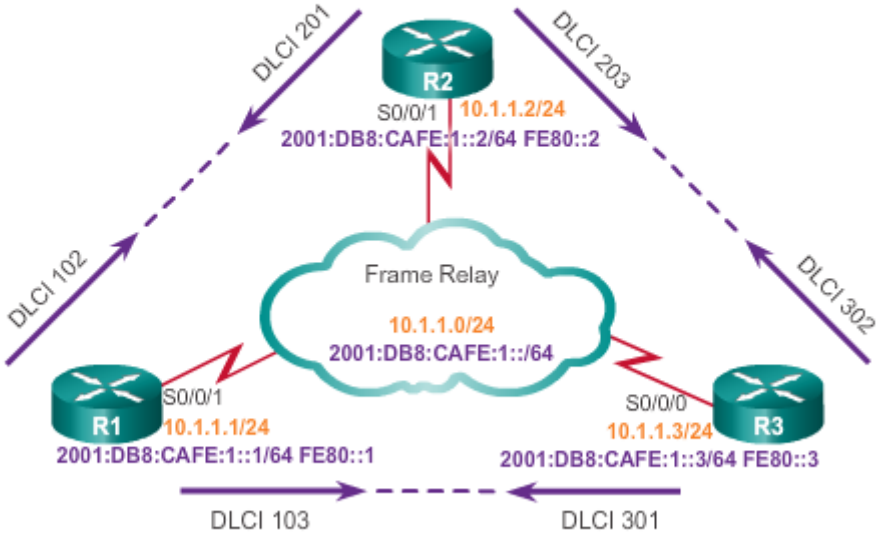
Nota: el comando **no encapsulation frame-relay** elimina la encapsulación de Frame Relay en la interfaz y devuelve la interfaz a la encapsulación HDLC predeterminada.

Tareas de configuración de Frame Relay



Tareas requeridas	Tareas opcionales
Habilitar la encapsulación de Frame Relay en una interfaz.	Configurar la LMI.
Configurar la asignación de direcciones dinámica o estática.	Configurar SVC de Frame Relay.
	Configurar el modelado del tráfico de Frame Relay.
	Personalizar Frame Relay para la red.
	Controlar y mantener las conexiones de Frame Relay.

Topología de Frame Relay



Configuración de interfaces de Frame Relay

```
R1(config)# interface Serial0/0/1
R1(config-if)# bandwidth 64
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# encapsulation frame-relay
```

```
R2(config)# interface Serial0/0/1
R2(config-if)# bandwidth 64
R2(config-if)# ip address 10.1.1.2 255.255.255.0
R2(config-if)# ipv6 address 2001:db8:cafe:1::2/64
R2(config-if)# ipv6 address fe80::2 link-local
R2(config-if)# encapsulation frame-relay
```

Verificación de la configuración Frame Relay

```
R1# show interfaces serial 0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.1.1.1/24
  MTU 1500 bytes, BW 64 Kbit/sec, 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 eng sent  481, LMI stat recvd 483, LMI upd recvd 0, DTE LMI up
  LMI eng 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 1/0, interface
  broadcasts 0
  Last input 00:00:05, output 00:00:05, output hang never
  Last clearing of "show interface" counters 01:21:27
  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 48 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
```

Capítulo 4: Frame Relay 4.2.1.2 Configuración de un mapa estático Frame Relay

Configuración de un mapa estático Frame Relay

Los routers Cisco admiten todos los protocolos de capa de red mediante Frame Relay, como IPv4, IPv6, IPX y AppleTalk. La asignación de dirección a DLCI se logra mediante la asignación de direcciones dinámica o estática.

La asignación dinámica la realiza la característica de ARP inverso. Debido a que ARP inverso está habilitado de manera predeterminada, no se requiere ningún comando adicional para configurar la asignación dinámica en una interfaz. En la figura 1, se muestra la topología que se usa para este tema.

La asignación estática se configura manualmente en un router. El establecimiento de la asignación estática depende de las necesidades de la red. Para asignar entre una dirección de protocolo de siguiente salto y una dirección de destino DLCI, utilice el comando **frame-relay map** *protocol protocol-address dlci* [**broadcast**], como se muestra en la figura 2. Observe la palabra clave**broadcast** al final del comando.

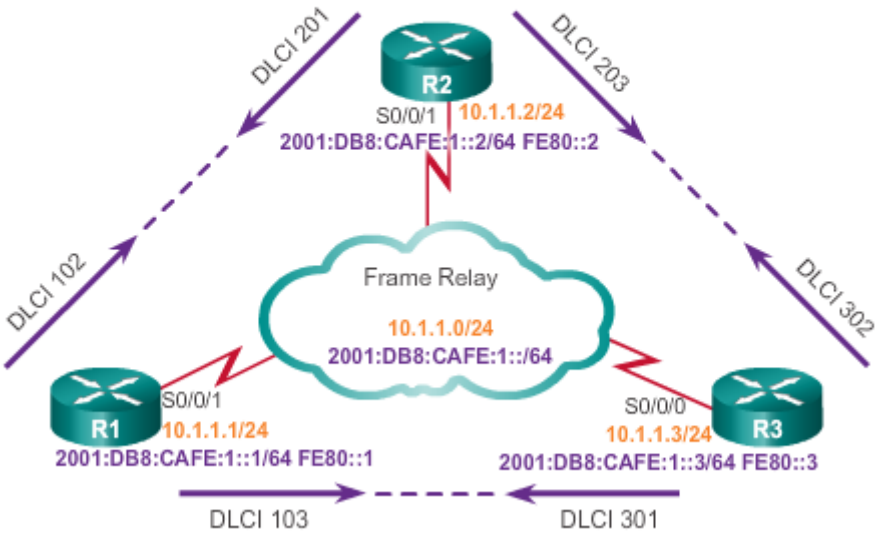
Frame Relay, ATM y X.25 son redes multiacceso sin difusión (NBMA). Las redes NBMA solo permiten la transferencia de datos de una computadora a otra a través de un VC o de un dispositivo de switching. Las redes NBMA no admiten el tráfico de multidifusión y de difusión, por lo que un paquete individual no puede llegar a todos los destinos. Esto requiere que reproduzca los paquetes manualmente a todos los destinos. El uso de la palabra clave**broadcast** es una forma simplificada de reenviar las actualizaciones de routing. La palabra clave **broadcast** permite que las difusiones y las multidifusiones de IPv4 se propaguen a todos los nodos. También permite las multidifusiones de IPv6 a través del PVC. Cuando se habilita la palabra clave, el router convierte el tráfico de difusión y de multidifusión en tráfico de unidifusión para que otros nodos reciban las actualizaciones de routing.

En la figura 3, se muestra cómo utilizar las palabras clave al configurar asignaciones de direcciones estáticas. Observe que la primera asignación de Frame Relay IPv6 a una dirección de unidifusión global no incluye la palabra clave **broadcast**. Sin embargo, la palabra clave **broadcast** se utiliza en la asignación a la dirección link-local. Los protocolos de routing IPv6 utilizan direcciones link-local para las actualizaciones de routing de multidifusión. Por lo tanto, solo el mapa de direcciones link-local requiere la palabra clave**broadcast** para reenviar paquetes de multidifusión.

En el ejemplo, se muestran solo las configuraciones para asignar los VC entre el R1 y el R2.

Nota: algunos protocolos de routing pueden requerir opciones de configuración adicionales. Por ejemplo, RIP, EIGRP y OSPF requieren configuraciones adicionales para que se los admita en las redes NBMA.

Topología de Frame Relay



Parámetros de comando

```
frame-relay map protocol protocol-address dlci [broadcast]
```

Parámetros de comando	Descripción
protocolo	Define el protocolo admitido, el puente o el control de enlace lógico: ip (IPv4), ipv6, AppleTalk, decnet, dlsw, 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 que se usa para conectarse a la dirección de protocolo remoto.
Broadcast	(Optativo) Permite las transmisiones de difusión y multidifusión a través del circuito virtual. Esto permite el uso de protocolos de enrutamiento dinámico en el VC.

Configuración para el R1 y el R2

```
R1(config)# interface Serial0/0/1
R1(config-if)# bandwidth 64
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# encapsulation frame-relay
R1(config-if)# frame-relay map ip 10.1.1.2 102 broadcast
R1(config-if)# frame-relay map ipv6 2001:DB8:CAFE:1::2 102
R1(config-if)# frame-relay map ipv6 FE80::2 102 broadcast
```

```
R2(config)# interface Serial0/0/1
R2(config-if)# bandwidth 64
R2(config-if)# ip address 10.1.1.2 255.255.255.0
R2(config-if)# ipv6 address 2001:db8:cafe:1::2/64
R2(config-if)# ipv6 address fe80::2 link-local
R2(config-if)# encapsulation frame-relay
R2(config-if)# frame-relay map ip 10.1.1.1 201 broadcast
R2(config-if)# frame-relay map ipv6 2001:DB8:CAFE:1::1 201
R2(config-if)# frame-relay map ipv6 FE80::1 201 broadcast
```

Capítulo 4: Frame Relay 4.2.1.3 Verificación de un mapa estático de Frame Relay

Para verificar la asignación de Frame Relay, utilice el comando **show frame-relay map**, como se muestra en la figura 1. Observe que hay tres asignaciones de Frame Relay. Hay una asignación para IPv4 y dos para IPv6, una para cada una de las direcciones IPv6.

Utilice el verificador de sintaxis de la figura 2 para configurar los mapas estáticos de Frame Relay del R1 al R3.

Verificación de un mapa estático de Frame Relay

```
R1# show frame-relay map
Serial0/0/1 (up): ipv6 2001:DB8:CAFE:1::2 dlci 102(0x66,0x1860),
                  static, CISCO, status defined, active
Serial0/0/1 (up): ipv6 FE80::2 dlci 102(0x66,0x1860), static,
                  broadcast, CISCO, status defined, active
Serial0/0/1 (up): ip 10.1.1.2 dlci 102(0x66,0x1860), static,
                  broadcast, CISCO, status defined, active
R1#
```

```
R2# show frame-relay map
Serial0/0/1 (up): ipv6 2001:DB8:CAFE:1::1 dlci 201(0xC9,0x3090),
                  static, CISCO, status defined, active
Serial0/0/1 (up): ipv6 FE80::1 dlci 201(0xC9,0x3090), static,
                  broadcast, CISCO, status defined, active
Serial0/0/1 (up): ip 10.1.1.1 dlci 201(0xC9,0x3090), static,
                  broadcast, CISCO, status defined, active
R2#
```

En la interfaz serial 0/0/1 del R1, configure los mapas estáticos de Frame Relay IPv4 e IPv6 para reenviar tráfico al R3. Realice las tareas en el siguiente orden:

- **Configure el mapa estático de Frame Relay IPv4.**
- **Configure el mapa estático de Frame Relay IPv6 para la dirección IPv6 de unidifusión global del R3.**
- **Configure el mapa estático IPv6 de Frame Relay para la dirección IPv6 link-local del R3.**

Configuración actual:

```
R1(config)#interface serial 0/0/1
R1(config-if)#bandwidth 64
R1(config-if)#ip address 10.1.1.1 255.255.255.0
R1(config-if)#ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)# frame-relay map ip 10.1.1.3 103 broadcast
R1(config-if)# frame-relay map ipv6 2001:db8:cafe:1::3 103
R1(config-if)# frame-relay map ipv6 fe80::3 103 broadcast
R1(config-if)#
```

Configuró correctamente un mapa estático de Frame Relay.

Capítulo 4: Frame Relay 4.2.1.4 Packet Tracer: Configuración de mapas estáticos de Frame Relay

Información básica/situación

En esta actividad, configurará dos mapas estáticos de Frame Relay en cada router para llegar a otros dos routers. Si bien el tipo LMI se detecta automáticamente en los routers, asignará el tipo de manera estática mediante la configuración manual de la LMI.

Packet Tracer: Configuración de mapas estáticos de Frame Relay (instrucciones)

Packet Tracer: Configuración de mapas estáticos de Frame Relay (PKA)

Capítulo 4: Frame Relay 4.2.2.1 Problemas de conexión

De manera predeterminada, la mayoría de las redes Frame Relay proporcionan conectividad NBMA entre sitios remotos mediante una topología hub-and-spoke. En una topología de Frame Relay NBMA, cuando se debe usar una única interfaz multipunto para interconectar varios sitios, pueden surgir problemas de conexión de las actualizaciones de routing. Con los protocolos de routing vector distancia, pueden surgir problemas de conexión de horizonte dividido, así como de reproducción de multidifusión y de difusión. Con los protocolos de routing de estado de enlace, los problemas con la elección del DR/BDR pueden ocasionar problemas de conexión.

Horizonte dividido

La regla del horizonte dividido es un mecanismo de prevención de bucles para los protocolos de routing vector distancia como EIGRP y RIP. No se aplica a los protocolos de routing de estado de enlace. La regla del horizonte dividido reduce los bucles de routing al evitar que una actualización de routing que se recibe en una interfaz se reenvíe desde la misma interfaz.

Por ejemplo, en la figura 1, que es una topología hub-and-spoke de Frame Relay, el router remoto R2 (un router spoke) envía una actualización al router de oficina central R1 (el router hub). El R1 conecta varios PVC a través de una única interfaz física. El R1 recibe la multidifusión en su interfaz física; sin embargo, el horizonte dividido no puede reenviar esa actualización de routing a través de la misma interfaz a otros routers remotos (spoke).

Nota: el horizonte dividido no es un problema si se configuró solo un PVC (una única conexión remota) en una interfaz física. Este tipo de conexión es punto a punto.

En la figura 2, se muestra un ejemplo similar con la topología de referencia que se usa en este capítulo. El R2, un router spoke, envía una actualización de routing al R1, un router hub. El R1 tiene varios PVC en una única interfaz física. La regla del horizonte dividido evita que el R1 reenvíe esa actualización de routing a través de la misma interfaz física al otro router spoke remoto (el R3).

Reproducción de multidifusión y de difusión

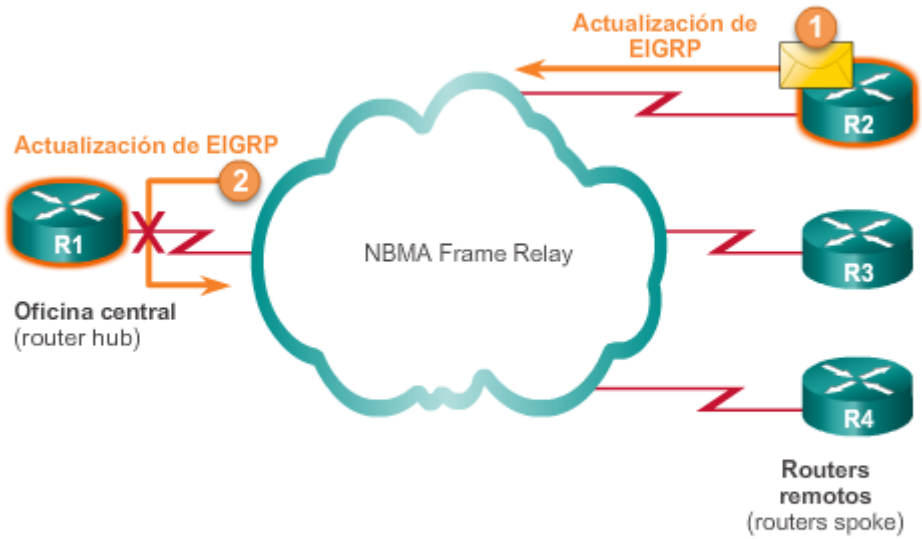
Como se muestra en la figura 3, debido al horizonte dividido, cuando un router admite las conexiones multipunto a través de una única interfaz, el router debe reproducir los paquetes de difusión y de multidifusión. En el caso de las actualizaciones de routing, las actualizaciones deben reproducirse y enviarse en cada PVC a los routers remotos. Estos paquetes reproducidos consumen ancho de banda y causan importantes variaciones de latencia en el tráfico de usuarios. La cantidad de tráfico de difusión y el número de VC que terminan en cada router se deben evaluar durante la fase de diseño de una red Frame Relay. El tráfico de sobrecarga, como las actualizaciones de routing, puede afectar la entrega de datos de usuarios

críticos, especialmente cuando la ruta de entrega contiene enlaces con ancho de banda bajo (56 kb/s).

Descubrimiento de vecinos: DR y BDR

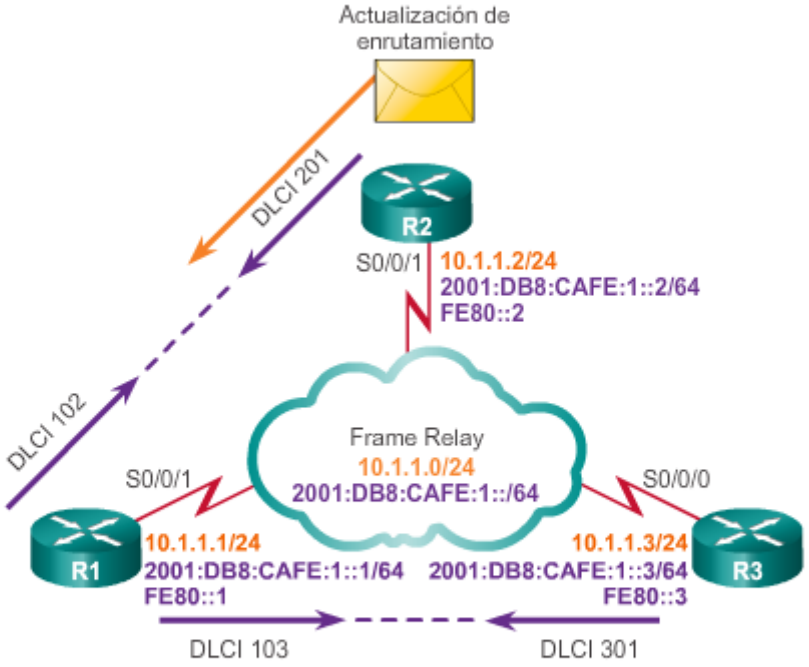
Los protocolos de routing de estado de enlace, como OSPF, no utilizan la regla del horizonte dividido para evitar los bucles. No obstante, pueden surgir problemas de conexión con el DR/BDR. En las redes NBMA, OSPF funciona en el modo de red sin difusión de manera predeterminada, y los vecinos no se descubren de forma automática. Los vecinos se pueden configurar estáticamente. Sin embargo, asegúrese de que el router hub se convierta en un DR, como se muestra en la figura 4. Recuerde que una red NBMA se comporta como Ethernet, y en Ethernet se necesita un DR para intercambiar información de routing entre todos los routers en un segmento. Por lo tanto, solo el router hub puede funcionar como DR, porque es el único router que tiene PVC con el resto de los routers.

Problema de horizonte dividido, ejemplo 1



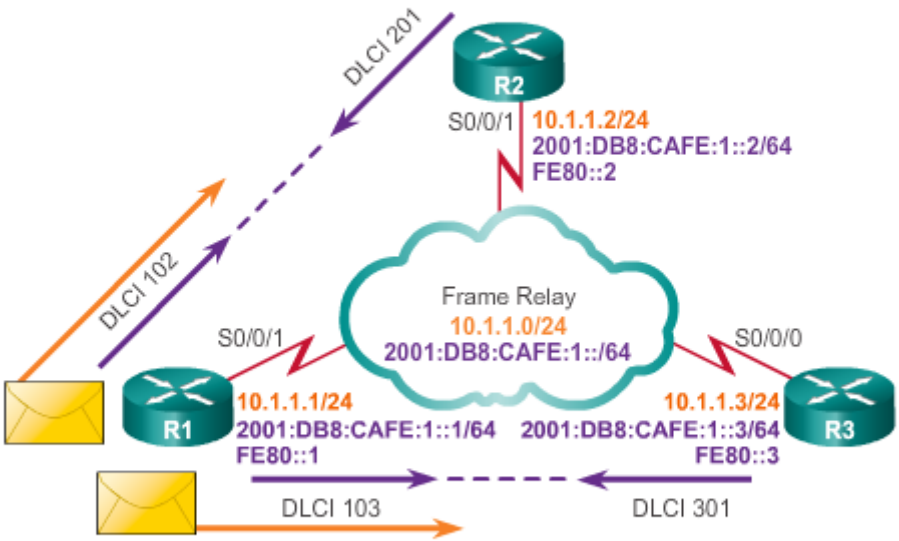
Problema: la actualización recibida en una interfaz física no se retransmite por esa misma interfaz: horizonte dividido.

Problema de horizonte dividido, ejemplo 2



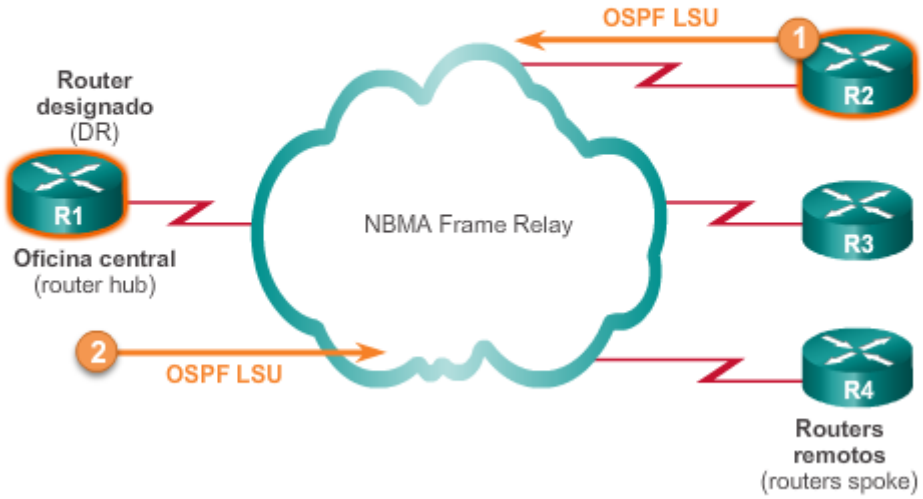
Problema: la actualización recibida en una interfaz física no se retransmite por esa misma interfaz: horizonte dividido.

Problema de horizonte dividido, ejemplo 3



Problema: se debe reproducir el tráfico de difusión para cada conexión activa.

Descubrimiento de vecinos: DR/BDR



Capítulo 4: Frame Relay 4.2.2.2 Solución de problemas relacionados a la posibilidad de conexión

Existen varias maneras de resolver el problema de conexión de routing:

- **Deshabilitar el horizonte dividido:**un método para resolver los problemas de conexión que produce el horizonte dividido puede ser desactivar el horizonte dividido. Sin embargo, deshabilitar el horizonte dividido aumenta las posibilidades de que se formen bucles de routing en la red. Además, solo IP permite deshabilitar el horizonte dividido; IPX y AppleTalk no lo permiten.

- **Topología de malla completa:** otro método es utilizar una topología de malla completa; sin embargo, esta topología aumenta los costos.

- **Subinterfaces:** en una topología hub-and-spoke de Frame Relay, el router hub se puede configurar con interfaces asignadas lógicamente denominadas “subinterfaces”.

Subinterfaces Frame Relay

Frame Relay puede dividir una interfaz física en varias interfaces virtuales denominadas “subinterfaces”, como se muestra en la figura 1. Una subinterfaz es simplemente una interfaz lógica que se asocia directamente a una interfaz física. Por lo tanto, se puede configurar una subinterfaz de Frame Relay para cada uno de los PVC que ingresan a una interfaz serial física.

Para habilitar el reenvío de las actualizaciones de routing de difusión en una red Frame Relay, puede configurar el router con subinterfaces asignadas lógicamente. Al utilizar una configuración de subinterfaz, cada VC se puede configurar como una conexión punto a punto. Una red de malla parcial se puede dividir en varias redes punto a punto más pequeñas, de malla completa. Se puede asignar una dirección de red única a cada subred punto a punto. Esto permite que cada subinterfaz funcione de manera similar a una línea arrendada. Mediante una subinterfaz de Frame Relay punto a punto, cada par de los routers punto a punto se encuentra en su propia subred. Esto permite que los paquetes recibidos en una subinterfaz se envíen por otra subinterfaz, aunque los paquetes se reenvíen por la misma interfaz física.

Las subinterfaces de Frame Relay se pueden configurar en modo punto a punto o multipunto:

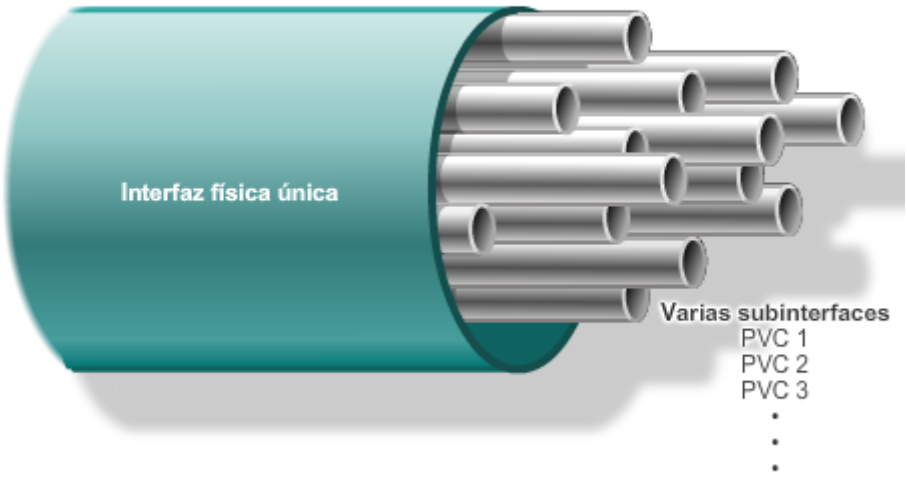
- **Punto a punto (figura 2):** una única subinterfaz punto a punto establece una conexión de PVC a otra interfaz física o subinterfaz en un router remoto. En este caso, cada par de los routers punto a punto está en su propia subred, y cada subinterfaz punto a punto tiene un único DLCI. En un entorno punto a punto, cada subinterfaz funciona como una interfaz punto a punto. Para cada VC punto a punto, hay una subred distinta. Por lo tanto, el tráfico de actualización de routing no está sujeto a la regla del horizonte dividido.

- **Multipunto (figura 3):** una única subinterfaz multipunto establece varias conexiones de PVC a varias interfaces físicas o subinterfaces en los routers remotos. Todas las interfaces que participan están en la misma subred. La subinterfaz funciona como una interfaz de Frame Relay NBMA, de modo que el tráfico de actualización de routing está sujeto a la regla del horizonte dividido. Todos los VC multipunto pertenecen a la misma subred.

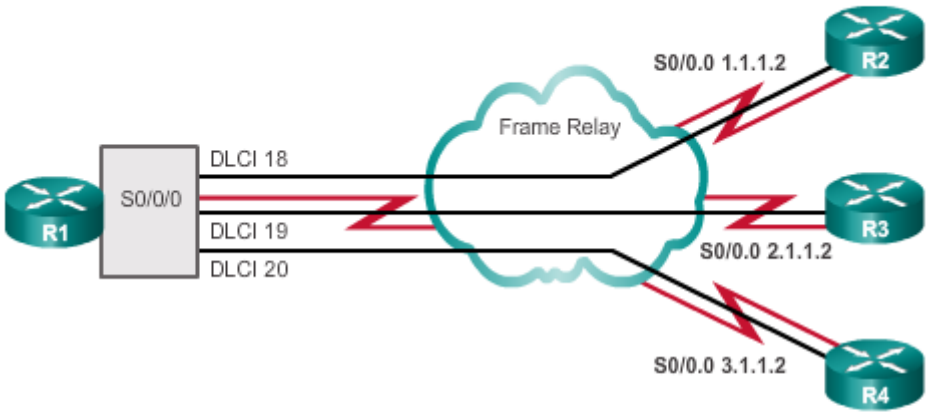
Al configurar subinterfaces, se asigna el comando **encapsulation frame-relay** a la interfaz física. Todos los demás elementos de la configuración, como la dirección de capa de red y los DLCI, se asignan a la subinterfaz.

Las configuraciones de la subinterfaz multipunto se pueden utilizar para conservar direcciones. Esto puede ser especialmente útil si no se utiliza la máscara de subred de longitud variable

(VLSM). Sin embargo, es posible que las configuraciones multipunto no funcionen correctamente, dadas las consideraciones del tráfico de difusión y el horizonte dividido. La opción de subinterfaz punto a punto se creó para evitar estos problemas.



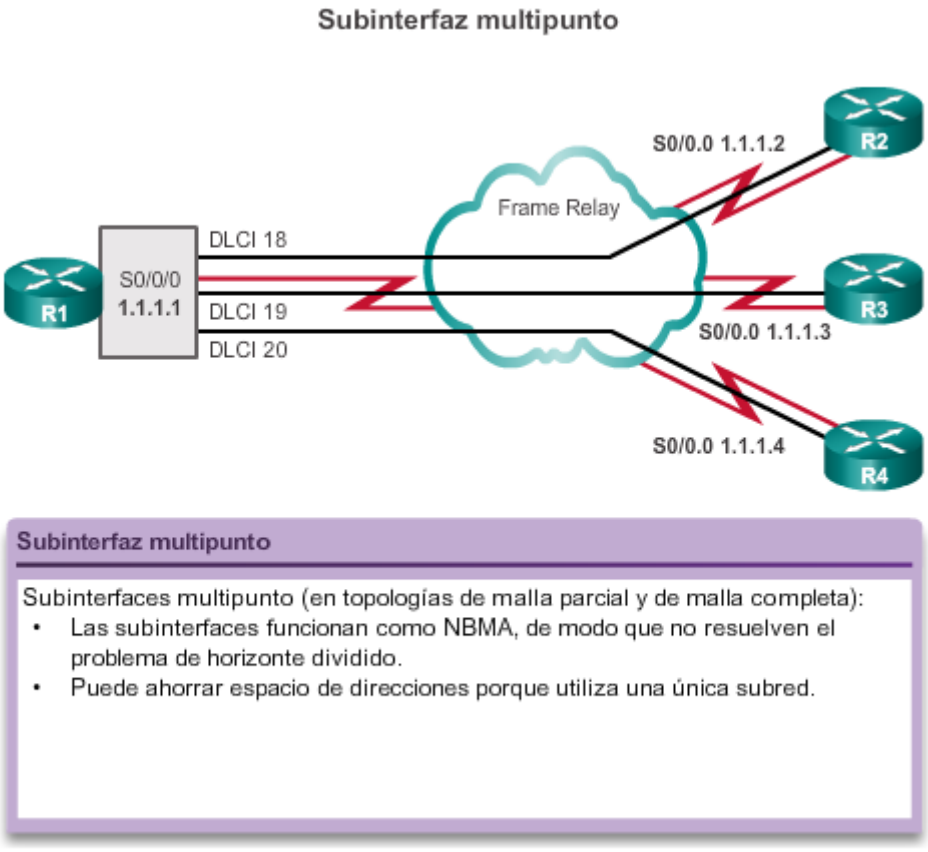
Subinterfaz punto a punto



Subinterfaz punto a punto

Subinterfaces punto a punto (en topologías hub-and-spoke):

- Las subinterfaces funcionan como líneas arrendadas.
- Cada subinterfaz punto-a-punto requiere su propia subred.



Capítulo 4: Frame Relay 4.2.2.3 Configuración de las subinterfaces punto a punto

Las subinterfaces se ocupan de las limitaciones de las redes Frame Relay al proporcionar una manera de subdividir una red Frame Relay de malla parcial en una cantidad de subredes más pequeñas de malla completa o punto a punto. A cada subred se le asigna su propio número de red y aparece ante los protocolos como si se pudiera llegar a ella mediante una interfaz diferente.

Para crear una subinterfaz, utilice el comando **interface serial** en el modo de configuración global seguido del número de puerto físico, un punto (.) y el número de subinterfaz. Para simplificar la resolución de problemas, utilice el DLCI como número de subinterfaz. También debe especificar si la interfaz es punto a multipunto o punto a punto con la palabra clave **multipoint** o**point-to-point**, ya que no hay un valor predeterminado. Estas palabras clave se definen en la figura 1.

El siguiente comando crea una subinterfaz punto a punto para el PVC 103 al R3:

R1(config-if)# **interface serial 0/0/0.103 point-to-point**

Nota: para simplificar, en esta sección solo se usan direcciones IPv4 para ilustrar las subinterfaces. Los mismos conceptos y comandos también se aplican al usar el direccionamiento IPv6.

Si la subinterfaz se configura como punto a punto, también se debe configurar el DLCI local de la subinterfaz para distinguirlo de la interfaz física. El DLCI también se requiere para las

subinterfaces multipunto con ARP inverso habilitado para IPv4. No se requiere para las subinterfaces multipunto configuradas con mapas de rutas estáticas.

El proveedor de servicios de Frame Relay asigna los números de DLCI. Estos números van del 16 al 992 y, en general, solo tienen importancia local. El intervalo varía según la LMI que se utilice.

El comando **frame-relay interface-dlci** configura el DLCI local en la subinterfaz, como se muestra en la figura 2:

R1(config-subif)# **frame-relay interface-dlci 103**

Nota: desafortunadamente, es posible que modificar la configuración de una subinterfaz de Frame Relay existente no proporcione el resultado esperado. En estas situaciones, desactive la interfaz física, realice los cambios adecuados a las subinterfaces y, a continuación, vuelva a habilitar la interfaz física. Si la configuración corregida produce resultados inesperados, es posible que deba guardar la configuración y volver a cargar el router.

Configuración de las subinterfaces punto a punto

```
router(config-if)# interface serial number.subinterface-number
[multipoint | point-to-point]
```

Parámetros del comando **interface serial**	Descripción
subinterface-number	El número de subinterfaz debe estar en el intervalo de 1 a 4294967293. El número de interfaz que precede al punto (.) debe coincidir con el número de la interfaz física a la que pertenece esta subinterfaz.
multipunto	Seleccione esta opción si todos los routers se encuentran en la misma subred.
Punto a punto	Seleccione esta opción para que cada par de routers punto a punto tengan su propia subred. Los enlaces punto a punto normalmente usan una máscara de subred 255.255.255.252

Asignación de un DLCI

```
router(config-subif)# frame-relay interface-dlci dlci-number
```

Parámetro del comando **frame-relay interface-dlci**	Descripción
dlci-number	Define el número DLCI local que se enlaza a la subinterfaz. Esta es la única forma de enlazar un DLCI derivado de LMI con una subinterfaz, ya que LMI no conoce las subinterfaces. Use el comando **frame-relay interface-dlci** solamente en las subinterfaces.

Capítulo 4: Frame Relay 4.2.2.4 Ejemplo: Configuración de las subinterfaces punto a punto

En la figura 1, se muestra la topología anterior, pero con subinterfaces punto a punto. Cada PVC es una subred distinta. Las interfaces físicas del router se dividen en subinterfaces, con cada subinterfaz en una subred distinta.

En la figura 2, el R1 tiene dos subinterfaces punto a punto. La subinterfaz s0/0/1.102 se conecta al R2, y la subinterfaz s0/0/1.103 se conecta al R3. Cada subinterfaz está en una subred diferente.

Para configurar subinterfaces en una interfaz física, se requieren los siguientes pasos:

Paso 1. Elimine 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. Configure la encapsulación de Frame Relay en la interfaz física mediante el comando **encapsulation frame-relay**.

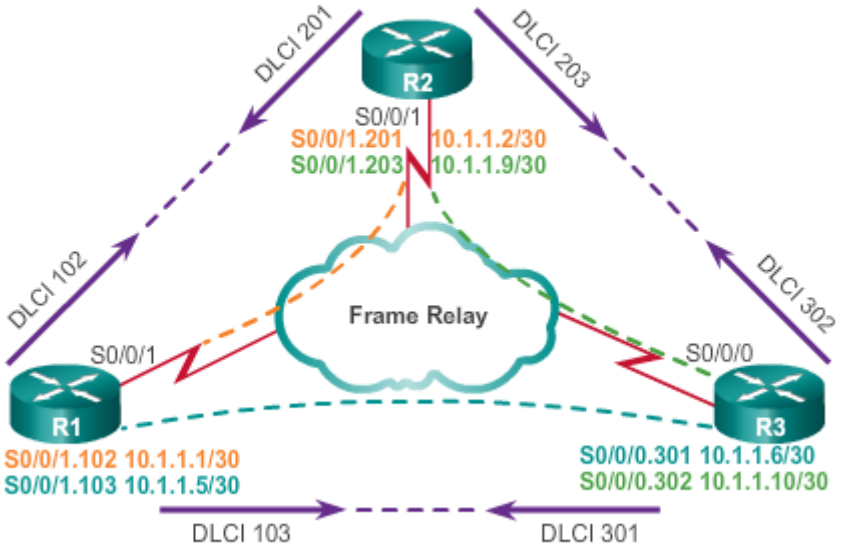
Paso 3. Cree una subinterfaz lógica para cada uno de los PVC definidos. Especifique el número de puerto, seguido de un punto (.) y el número de subinterfaz. Para simplificar la resolución de problemas, se sugiere que el número de subinterfaz coincida con el número de DLCI.

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

Paso 5. Configure el DLCI local en la subinterfaz mediante el comando **frame-relay interface-dlci**. Recuerde que el proveedor de servicios de Frame Relay asigna los números de DLCI.

Utilice el verificador de sintaxis de la figura 3 para configurar la interfaz física del router R2 en subinterfaces punto a punto con la configuración de Frame Relay correspondiente.

Topología de Frame Relay con Subinterfaces



Configuración de subinterfaces punto a punto en el R1

```
R1(config)# interface serial 0/0/1
R1(config-if)# encapsulation frame-relay
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/0/1.102 point-to-point
R1(config-subif)# ip address 10.1.1.1 255.255.255.252
R1(config-subif)# bandwidth 64
R1(config-subif)# frame-relay interface-dlci 102
R1(config-fr-dlci)# exit
R1(config-subif)# exit
R1(config)# interface serial 0/0/1.103 point-to-point
R1(config-subif)# ip address 10.1.1.5 255.255.255.252
R1(config-subif)# bandwidth 64
R1(config-subif)# frame-relay interface-dlci 103
R1(config-fr-dlci)#
```

Configuración de subinterfaces punto a punto en el R2

Configure la interfaz serial 0/0/1 del R2 con subinterfaces mediante los comandos de configuración de Frame Relay correspondientes. Realice las tareas en el orden que se indica:

- **Configure la interfaz física del R2 para la encapsulación de Frame Relay.**
- **Active la interfaz.**
- **Vuelva al modo de configuración global.**

```
R2(config)# interface Serial0/0/1
R2(config-if)# encapsulation frame-relay
R2(config-if)# no shutdown:
R2(config-if)# exit
```

Configure la subinterfaz .201 con lo siguiente:

- **Ancho de banda: 64**
- **Dirección IPv4 10.1.1.2/30**
- **DLCI de interfaz 201**
- **Volver al modo de configuración global**

```
R2(config)# interface Serial0/0/1.201 point-to-point
R2(config-subif)# bandwidth 64
R2(config-subif)# ip address 10.1.1.2 255.255.255.252
R2(config-subif)# frame-relay interface-dlci 201
R2(config-fr-dlci)# exit
```

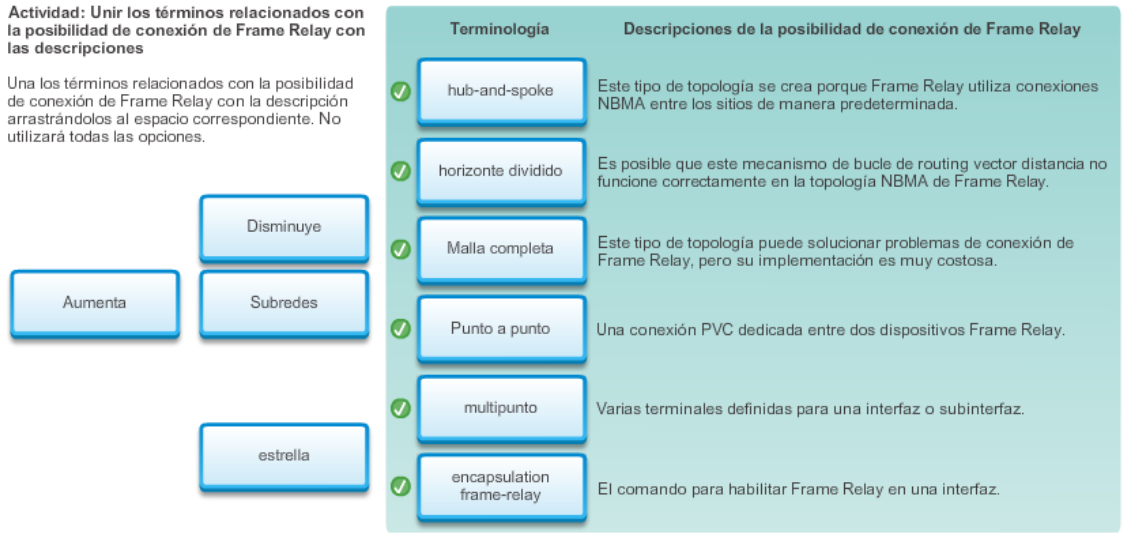
Configure la subinterfaz .203 con lo siguiente:

- **Ancho de banda: 64**
- **Dirección IPv4 10.1.1.9/30**
- **DLCI de interfaz 203**
- **Volver al modo de configuración global**

```
R2(config-subif)# interface Serial0/0/1.203 point-to-point
R2(config-subif)# bandwidth 64
R2(config-subif)# ip address 10.1.1.9 255.255.255.252
R2(config-subif)# frame-relay interface-dlci 203
R2(config-fr-dlci)# exit
R2(config-if)#
```

Configuró correctamente las subinterfaces punto a punto.

Capítulo 4: Frame Relay 4.2.2.5 Actividad: Identificar la terminología relacionada con ancho de banda y control del flujo de Frame Relay



Capítulo 4: Frame Relay 4.2.2.6 Packet Tracer: Configuración de subinterfaces punto a punto de Frame Relay

Información básica/situación

En esta actividad, configurará Frame Relay con dos subinterfaces en cada router para llegar a los otros dos routers. También configurará EIGRP y verificará la conectividad de extremo a extremo.

Packet Tracer: Configuración de subinterfaces punto a punto de Frame Relay (instrucciones)

Packet Tracer: Configuración de subinterfaces punto a punto de Frame Relay (PKA)

Capítulo 4: Frame Relay 4.2.2.7 Práctica de laboratorio: Configuración de Frame Relay y subinterfaces

En esta práctica de laboratorio, cumplirá los siguientes objetivos:

- Parte 1: armar la red y configurar los parámetros básicos de los dispositivos
- Parte 2: Configurar un switch Frame Relay
- Parte 3: Configurar los parámetros básicos de Frame Relay
- Parte 4: Resolver problemas de Frame Relay
- Parte 5: Configurar una subinterfaz Frame Relay

Práctica de laboratorio: Configuración de Frame Relay y subinterfaces

Capítulo 4: Frame Relay 4.3.1.1 Verificación del funcionamiento de Frame Relay: interfaz de Frame Relay

En general, Frame Relay es un servicio muy confiable. Sin embargo, hay momentos en los que la red funciona a niveles más bajos que lo esperado y se deben resolver los problemas. Por ejemplo, los usuarios pueden informar sobre conexiones lentas e intermitentes a través del circuito, o los circuitos pueden dejar de funcionar completamente. Independientemente del motivo, las interrupciones de la red son muy costosas en términos de pérdida de productividad. Una práctica recomendada es verificar la configuración antes de que aparezcan los problemas.

En este tema, deberá seguir los pasos de un procedimiento de verificación para asegurar que todo funcione correctamente antes de que se inicie una configuración en una red activa.

Verificación de las interfaces de Frame Relay

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

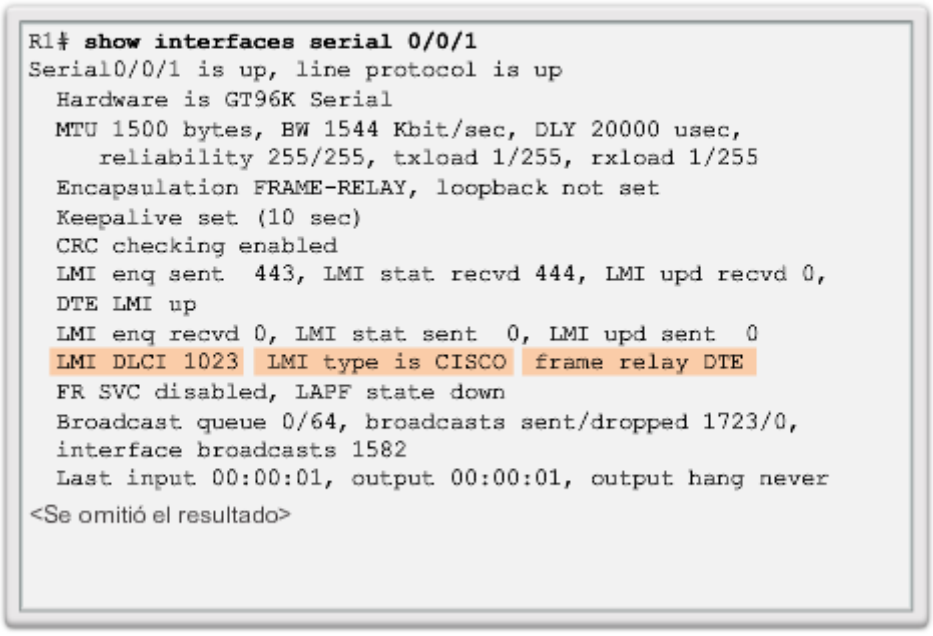
Recuerde que con Frame Relay, el router normalmente se considera un dispositivo DTE. Sin embargo, con fines de prueba, se puede configurar un router Cisco como un dispositivo DCE para simular un switch Frame Relay. En estos casos, el router se convierte en un dispositivo DCE cuando se lo configura como switch Frame Relay.

Como se muestra en la ilustración, el comando **show interfaces** muestra cómo se establece la encapsulación, junto con información útil del estado de la capa 1 y la capa 2, incluido lo siguiente:

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

El primer paso siempre es confirmar que las interfaces estén configuradas correctamente. En la ilustración, entre otras cosas, puede ver los detalles sobre la encapsulación, el DLCI en la interfaz serial configurada con Frame Relay y el DLCI utilizado para la LMI. Confirme que estos valores sean los valores esperados; de lo contrario, se pueden requerir cambios.

Verificación del funcionamiento de Frame Relay: observación de las interfaces

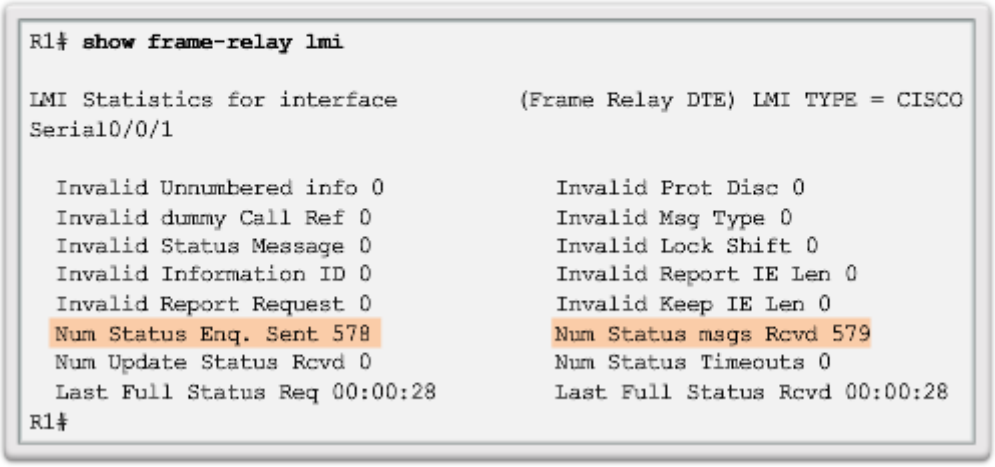


Capítulo 4: Frame Relay 4.3.1.2 Verificación del funcionamiento de Frame Relay: operaciones de LMI

El siguiente paso es analizar algunas estadísticas de LMI mediante el comando**show frame-relay lmi**. En la ilustración, se muestra un resultado de ejemplo que indica la cantidad de mensajes de estado intercambiados entre el router local y el switch Frame Relay local. Asegúrese de que los contadores entre los mensajes de estado enviados y recibidos aumenten. Esto valida que existe comunicación activa entre el DTE y el DCE.

También busque elementos Invalid distintos de cero. Esto ayuda a aislar el problema de comunicaciones de Frame Relay entre el switch de la prestadora de servicios y el router cliente.

Verificación del funcionamiento de Frame Relay: estadísticas de LMI



Capítulo 4: Frame Relay 4.3.1.3 Verificación del funcionamiento de Frame Relay: estado de PVC

En la ilustración, se muestran las estadísticas de la interfaz.

Utilice el comando **show frame-relay pvc** [**interface** *interfaz*] [*dlci*]para ver las estadísticas de tráfico y PVC. Este comando además resulta útil para ver la cantidad de paquetes de BECN y FECN que recibe el router. El estado de 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.

Después de recopilar las estadísticas, utilice el comando **clear counters** para restablecer los contadores de estadísticas. Después de borrar los contadores, espere 5 o 10 minutos antes de volver a emitir los comandos **show**. Observe cualquier error adicional. Si necesita comunicarse con la prestadora de servicios, estas estadísticas contribuyen a resolver los problemas.

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 1230          output pkts 1243         in bytes 103826
  out bytes 105929         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 1228      out bcast bytes 104952
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 01:38:29, last time pvc status changed 01:26:19
R1#
```

Capítulo 4: Frame Relay 4.3.1.4 Verificación del funcionamiento de Frame Relay: ARP inverso

Para borrar mapas de Frame Relay creados dinámicamente mediante ARP inverso, utilice el comando **clear frame-relay inarp**, como se muestra en la figura 1.

La última tarea es confirmar si el comando**frame-relay inverse-arp** resolvió una dirección IPv4 remota a un DLCI local. Utilice el comando **show frame-relay map** para mostrar las entradas de mapa actuales y la información sobre las conexiones. En la figura 2, se muestra el resultado del router R3 con una configuración de Frame Relay anterior en la interfaz física, sin el uso de subinterfaces. ARP inverso está habilitado de manera predeterminada para IPv4. Frame Relay para IPv6 utiliza el descubrimiento inverso de vecinos (IND) para obtener una dirección IPv6 de capa 3 a partir de un DLCI de capa 2.

El resultado muestra la siguiente información:

- **10.1.1.9** es la dirección IPv4 del router remoto, descubierta dinámicamente a través del proceso ARP inverso.
- **302** es el valor decimal del número de DLCI local.
- **0x12E** es la conversión hexadecimal del número de DLCI, 0x12E = decimal 302.
- **0x48E0** es el valor como aparecería en el cable debido a la forma en que se propagan los bits de DLCI en el campo de dirección de la trama Frame Relay.
- La **difusión/multidifusión** se encuentra habilitada en el PVC.
- El tipo de LMI es **cisco**.
- El PVC está en estado **activo**.

Cuando se realiza una solicitud de ARP inverso, el router actualiza su tabla de mapa con tres estados posibles de conexión LMI. Estos estados son los siguientes:

- **ACTIVE:** indica un circuito de extremo a extremo (DTE a DTE) correcto.
- **INACTIVE:** indica una conexión correcta al switch (DTE a DCE) sin que se detecte un DTE en el otro extremo del PVC. Esto puede ocurrir debido a una configuración incorrecta en el switch.
- **DELETED:** indica que el DTE está configurado para un DLCI que el switch no reconoce como válido para esa interfaz.

Verificación del funcionamiento de Frame Relay: borrado de mapas 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
Serial0/0/1.103 (up): point-to-point dlci, dlci 103(0x67,0x1870),
broadcast status defined, active
R1#
```

```
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
Serial0/0/1.203 (up): point-to-point dlci, dlci 203(0xCB,0x30B0),
broadcast status defined, active
R2#
```

Verificación del funcionamiento de Frame Relay: verificación de ARP inverso

```
R3# show frame-relay map
Serial0/0/0 (up): ip 10.1.1.9 dlci 302(0x12E,0x48E0), dynamic,
              broadcast, CISCO, status defined, active
R3#
```

Si el procedimiento de verificación indica que la configuración de Frame Relay no funciona correctamente, el paso siguiente es resolver los problemas de la configuración.

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

Observe la ilustración para examinar el resultado de un intercambio de LMI.

- **out** es un mensaje de estado de LMI que envía el router.
- **in** es un mensaje que se recibe del switch Frame Relay.
- Un mensaje **type 0** es un mensaje de estado de LMI completo.
- Un intercambio de LMI es **type 1**.
- **dlci 102, status 0x2** significa que el DLCI 102 está en estado activo.

Los valores posibles del campo de estado son los siguientes:

- **0x0:** el switch tiene este DLCI programado, pero por algún motivo no se puede usar. El motivo podría ser que posiblemente el otro extremo del PVC esté inactivo.
- **0x2:** el switch Frame Relay tiene el DLCI y todo funciona.
- **0x4:** el switch Frame Relay no tiene este DLCI programado para el router, pero estuvo programado antes en algún momento. Esto también puede deberse a que se invirtieron los DLCI en el router, o a que el proveedor de servicios eliminó el PVC en la nube de 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#
*Apr  1 14:57:43.559: Serial0/0/1(in): Status, myseq 22, pak size 29
*Apr  1 14:57:43.559: RT IE 1, length 1, type 0
*Apr  1 14:57:43.559: KA IE 3, length 2, yourseq 22, myseq 22
*Apr  1 14:57:43.559: PVC IE 0x7 , length 0x6 , dlci 102, status 0x2 , bw 0
*Apr  1 14:57:43.559: PVC IE 0x7 , length 0x6 , dlci 103, status 0x2 , bw 0
R1#
*Apr  1 14:57:53.555: Serial0/0/1(out): StEnq, myseq 23, yourseen 22, DTE up
*Apr  1 14:57:53.555: datagramstart = 0xED802AF4, datagramsize = 13
*Apr  1 14:57:53.555: FR encap = 0xFCF10309
*Apr  1 14:57:53.555: 00 75 01 01 01 03 02 17 16
*Apr  1 14:57:53.555:
*Apr  1 14:57:53.559: Serial0/0/1(in): Status, myseq 23, pak size 13
*Apr  1 14:57:53.559: RT IE 1, length 1, type 1
*Apr  1 14:57:53.559: KA IE 3, length 2, yourseq 23, myseq 23
R1# undebug all
All possible debugging has been turned off
```

Capítulo 4: Frame Relay 4.3.1.6 Práctica de laboratorio: Resolución de problemas de Frame Relay básico

En esta práctica de laboratorio, cumplirá los siguientes objetivos:

- Parte 1: armar la red y cargar las configuraciones de los dispositivos
- Parte 2: Resolver problemas de conectividad de capa 3
- Parte 3: Resolver problemas de Frame Relay

Práctica de laboratorio: Resolución de problemas de Frame Relay básico

Capítulo 4: Frame Relay 4.4.1.1 Actividad de clase: Propuesta presupuestaria de Frame Relay

Propuesta presupuestaria de Frame Relay

Se decidió que en su empresa se utilizará la tecnología Frame Relay para proporcionar conectividad de video entre la ubicación de la oficina principal y dos sucursales. Además, la empresa utilizará la nueva red para redundancia en caso de que la conectividad de la red ISP actual se interrumpa por algún motivo.

Como suele suceder con cualquier tipo de actualización de red, debe desarrollar un presupuesto para el administrador.

Después de investigar, decide utilizar este sitio web de Frame Relay para realizar el análisis de costos. Los costos que se indican en el sitio son una representación de los costos reales de ISP; solo se mencionan para ayudarlo a diseñar el análisis de costos.

Actividad de clase: Propuesta presupuestaria de Frame Relay

Capítulo 4: Frame Relay 4.4.1.2 Packet Tracer: desafío de integración de habilidades

Información básica/situación

Esta actividad le permite poner en práctica diversas aptitudes, incluida la configuración de Frame Relay, PPP con CHAP, EIGRP, routing estático y predeterminado.

Packet Tracer: Desafío de integración de habilidades (instrucciones)

Packet Tracer: Reto de habilidades de integración (PKA)

Capítulo 4: Frame Relay 4.4.1.3 Resumen

Frame Relay es una tecnología confiable de conmutación de paquetes orientada a la conexión, que se utiliza ampliamente para interconectar sitios remotos. Es más rentable que las líneas arrendadas, ya que el ancho de banda en la red del proveedor de servicios se comparte, y una terminal necesita solo un circuito físico al proveedor de circuitos para admitir varios VC. Cada VC se identifica mediante un DLCI.

Los datos de capa 3 se encapsulan en una trama Frame Relay que tiene un encabezado y un tráiler de Frame Relay. A continuación, se pasa a la capa física, que generalmente es EIA/TIA-232, 449 o 530, V.35 o X.21.

Las topologías típicas de Frame Relay incluyen la topología en estrella (hub-and-spoke), una topología de malla completa y una topología de malla parcial.

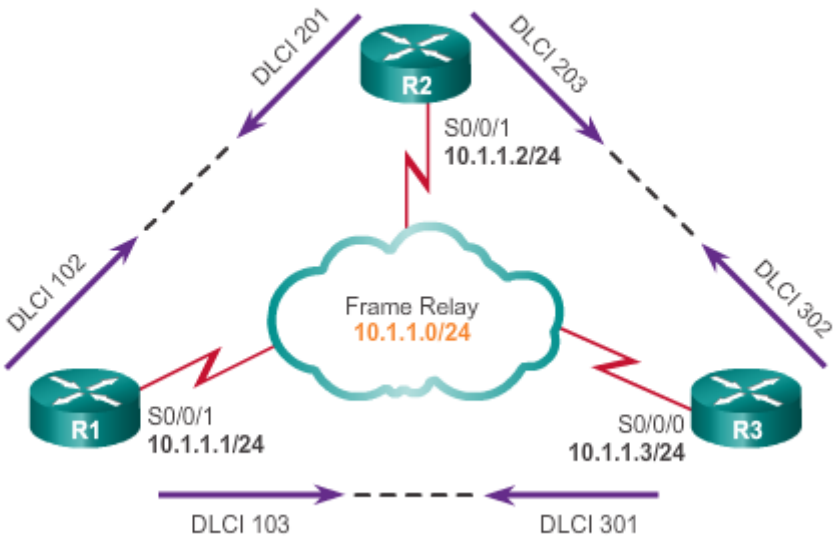
La asignación entre las direcciones DLCI de capa 2 y las direcciones de capa 3 se puede lograr dinámicamente mediante ARP inverso o mediante la configuración manual de mapas estáticos.

LMI es un protocolo para los mensajes enviados entre los dispositivos DCE y DTE para mantener la información de estado de Frame Relay entre estos dispositivos. El tipo de LMI que se configura en el router debe coincidir con el del proveedor de servicios.

El costo del circuito de Frame Relay incluye la velocidad de acceso, la cantidad de PVC y la CIR. Generalmente, se permiten algunas ráfagas por encima de la CIR sin costo adicional. Se puede negociar una velocidad Bc para proporcionar una cierta capacidad de ráfaga confiable para condiciones de corto plazo.

Frame Relay utiliza los bits BECN y FECN en el encabezado de Frame Relay para el control de congestión.

El uso de subinterfaces en las configuraciones de Frame Relay ayuda a aliviar los problemas de horizonte dividido de los protocolos de routing.

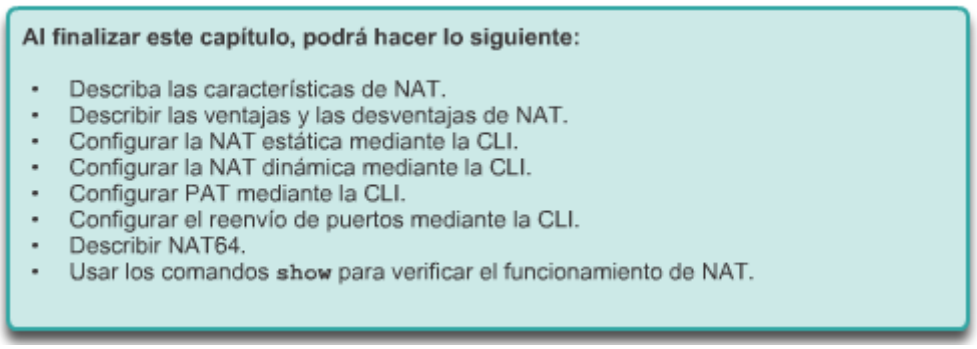


Capítulo 5: Traducción de direcciones de red para IPv4 5.0.1.1 Introducción

Todas las direcciones IPv4 públicas que se usan en Internet deben registrarse en un registro regional de Internet (RIR). Las organizaciones pueden arrendar direcciones públicas de un SP, pero solo el titular registrado de una dirección pública de Internet puede asignar esa dirección a un dispositivo de red. Sin embargo, con un máximo teórico de 4300 millones de direcciones, el espacio de direcciones IPv4 es muy limitado. Cuando Bob Kahn y Vint Cerf desarrollaron por primera vez la suite de protocolos TCP/IP que incluía IPv4 en 1981, nunca imaginaron en qué podría llegar a convertirse Internet. En aquel entonces, la computadora personal era, en la mayoría de los casos, una curiosidad para los aficionados, y todavía faltaba más de una década para la aparición de la World Wide Web.

Con la proliferación de los dispositivos informáticos personales y la llegada de la World Wide Web, pronto resultó evidente que los 4300 millones de direcciones IPv4 no serían suficientes. La solución a largo plazo era el protocolo IPv6, pero se necesitaban soluciones más inmediatas para abordar el agotamiento de direcciones. A corto plazo, el IETF implementó varias soluciones, entre las que se incluía la traducción de direcciones de red (NAT) y las direcciones IPv4 privadas definidas en RFC 1918. En este capítulo, se analiza cómo se utiliza NAT combinada con el espacio de direcciones privadas para conservar y usar de forma más eficaz las direcciones IPv4, a fin de proporcionar acceso a Internet a las redes de todos los tamaños. En este capítulo, se abarcan los siguientes temas:

- Las características, la terminología y las operaciones generales de NAT
- Los diferentes tipos de NAT, incluidas la NAT estática, la NAT dinámica y la NAT con sobrecarga
- Las ventajas y las desventajas de NAT
- La configuración, la verificación y el análisis de la NAT estática, la NAT dinámica y la NAT con sobrecarga
- La forma en que se puede usar el reenvío de puertos para acceder a los dispositivos internos desde Internet
- La resolución de problemas de NAT mediante los comandos **show** y **debug**
- La forma en que se utiliza NAT para IPv6 para traducir entre direcciones IPv6 y direcciones IPv4



Capítulo 5: Traducción de direcciones de red para IPv4 5.0.1.2 Actividad de clase: NAT conceptual

NAT conceptual

Usted trabaja para una universidad o un sistema escolar grande.

Por ser el administrador de red, muchos profesores, trabajadores administrativos y otros administradores de red necesitan su ayuda con las redes todos los días. Lo llaman durante toda la jornada laboral y debido a la cantidad de llamadas telefónicas, no puede completar sus tareas regulares de administración de red.

Debe encontrar la manera de decidir el momento para atender llamadas y las personas a quienes atender. También debe ocultar su número de teléfono para que, cuando llame a alguien, el destinatario vea otro número.

En esta situación, se describe un problema muy frecuente para la mayoría de las pequeñas y medianas empresas. Visite la página “How Network Address Translation Works”, ubicada en el siguiente enlace, para ver más información sobre la forma en que el mundo digital maneja este tipo de interrupciones de la jornada laboral.

Actividad de clase: NAT conceptual

Capítulo 5: Traducción de direcciones de red para IPv4 5.1.1.1 Espacio de direcciones IPv4 privadas

No existen suficientes direcciones IPv4 públicas para asignar una dirección única a cada dispositivo conectado a Internet. Las redes suelen implementarse mediante el uso de direcciones IPv4 privadas, según se definen en RFC 1918. En la figura 1, se muestra el rango de direcciones incluidas en RFC 1918. Es muy probable que la computadora que utiliza para ver este curso tenga asignada una dirección privada.

Estas direcciones privadas se utilizan dentro de una organización o un sitio para permitir que los dispositivos se comuniquen localmente. Sin embargo, como estas direcciones no identifican empresas u organizaciones individuales, las direcciones privadas IPv4 no se pueden enrutar a través de Internet. Para permitir que un dispositivo con una dirección IPv4 privada acceda a recursos y dispositivos fuera de la red local, primero se debe traducir la dirección privada a una dirección pública.

Como se muestra en la figura 2, NAT proporciona la traducción de direcciones privadas a direcciones públicas. Esto permite que un dispositivo con una dirección IPv4 privada acceda a recursos fuera de su red privada, como los que se encuentran en Internet. La combinación de NAT con las direcciones IPv4 privadas resultó ser un método útil para preservar las direcciones IPv4 públicas. Se puede compartir una única dirección IPv4 pública entre cientos o incluso miles de dispositivos, cada uno configurado con una dirección IPv4 privada exclusiva.

Sin NAT, el agotamiento del espacio de direcciones IPv4 habría ocurrido mucho antes del año 2000. Sin embargo, NAT presenta algunas limitaciones, las cuales se analizan más adelante en este capítulo. La solución al agotamiento del espacio de direcciones IPv4 y a las limitaciones de NAT es la transición final a IPv6.

Direcciones IPv4 privadas

Las direcciones privadas de Internet están definidas en RFC 1918:		
Clase	**Rango de direcciones internas RFC 1918**	**Prefijo CIDR**
A	10.0.0.0 a 10.255.255.255	10.0.0.0/8
B	172.16.0.0 a 172.31.255.255	172.16.0.0/12
C	192.168.0.0 a 192.168.255.255	192.168.0.0/16

Traducción entre direcciones privadas y públicas

Capítulo 5: Traducción de direcciones de red para IPv4 5.1.1.2 ¿Qué es NAT?

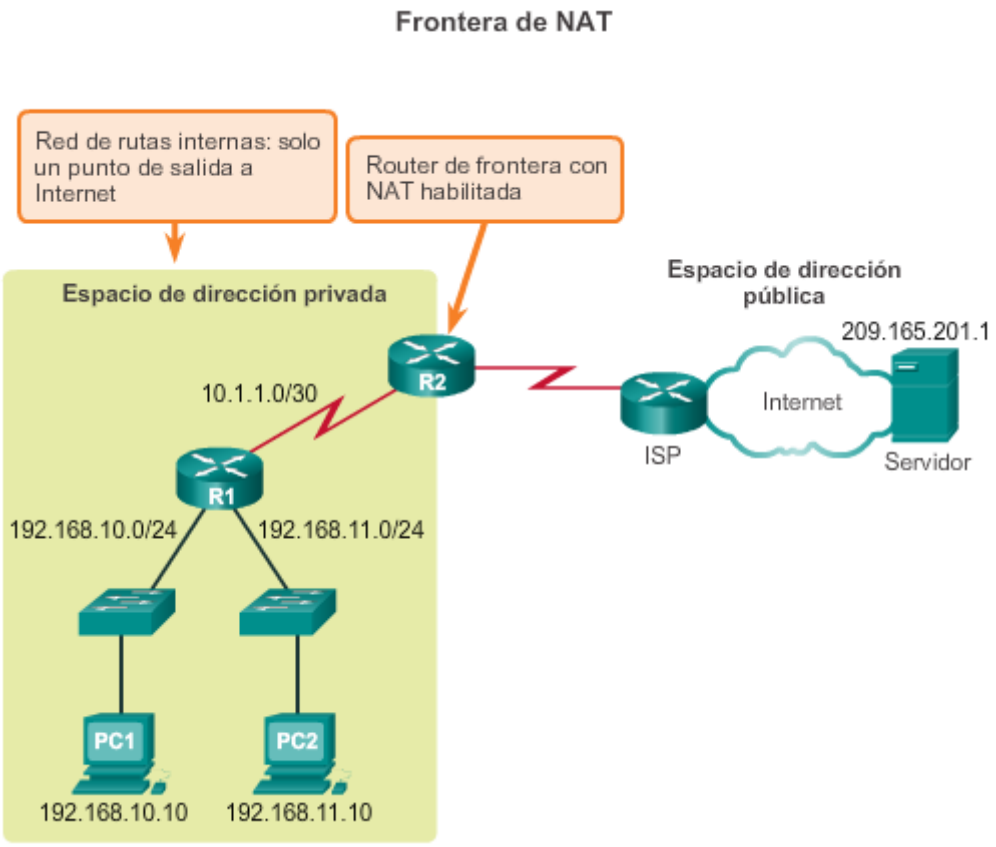
NAT tiene muchos usos, pero el principal es conservar las direcciones IPv4 públicas. Esto se logra al permitir que las redes utilicen direcciones IPv4 privadas internamente y al proporcionar la traducción a una dirección pública solo cuando sea necesario. NAT tiene el beneficio adicional de proporcionar cierto grado de privacidad y seguridad adicional a una red, ya que oculta las direcciones IPv4 internas de las redes externas.

Los routers con NAT habilitada se pueden configurar con una o más direcciones IPv4 públicas válidas. Estas direcciones públicas se conocen como “conjunto de NAT”. Cuando un dispositivo interno envía tráfico fuera de la red, el router con NAT habilitada traduce la dirección IPv4 interna del dispositivo a una dirección pública del conjunto de NAT. Para los dispositivos externos, todo el tráfico entrante y saliente de la red parece tener una dirección IPv4 pública del conjunto de direcciones proporcionado.

En general, los routers NAT funcionan en la frontera de una red de rutas internas. Una red de rutas internas es aquella que tiene una única conexión a su red vecina, una entrada hacia la red y una salida desde ella. En el ejemplo de la ilustración, el R2 es un router de frontera. Visto desde el ISP, el R2 forma una red de rutas internas.

Cuando un dispositivo dentro de la red de rutas internas desea comunicarse con un dispositivo fuera de su red, el paquete se reenvía al router de frontera. El router de frontera realiza el proceso de NAT, es decir, traduce la dirección privada interna del dispositivo a una dirección pública, externa y enrutable.

Nota: la conexión al ISP puede utilizar una dirección privada o pública compartida entre clientes. A los fines de este capítulo, se muestra una dirección pública.



Capítulo 5: Traducción de direcciones de red para IPv4 5.1.1.3 Terminología de NAT

Según la terminología de NAT, la red interna es el conjunto de redes sujetas a traducción. La red externa se refiere a todas las otras redes.

Al utilizar NAT, las direcciones IPv4 se designan de distinto modo, según si están en la red privada o en la red pública (Internet), y si el tráfico es entrante o saliente.

NAT incluye cuatro tipos de direcciones:

- Dirección local interna
- Dirección global interna

- Dirección local externa
- Dirección global externa

Al determinar qué tipo de dirección se utiliza, es importante recordar que la terminología de NAT siempre se aplica desde la perspectiva del dispositivo con la dirección traducida:

- **Dirección interna:** la dirección del dispositivo que se traduce por medio de NAT.
- **Dirección externa:** la dirección del dispositivo de destino.

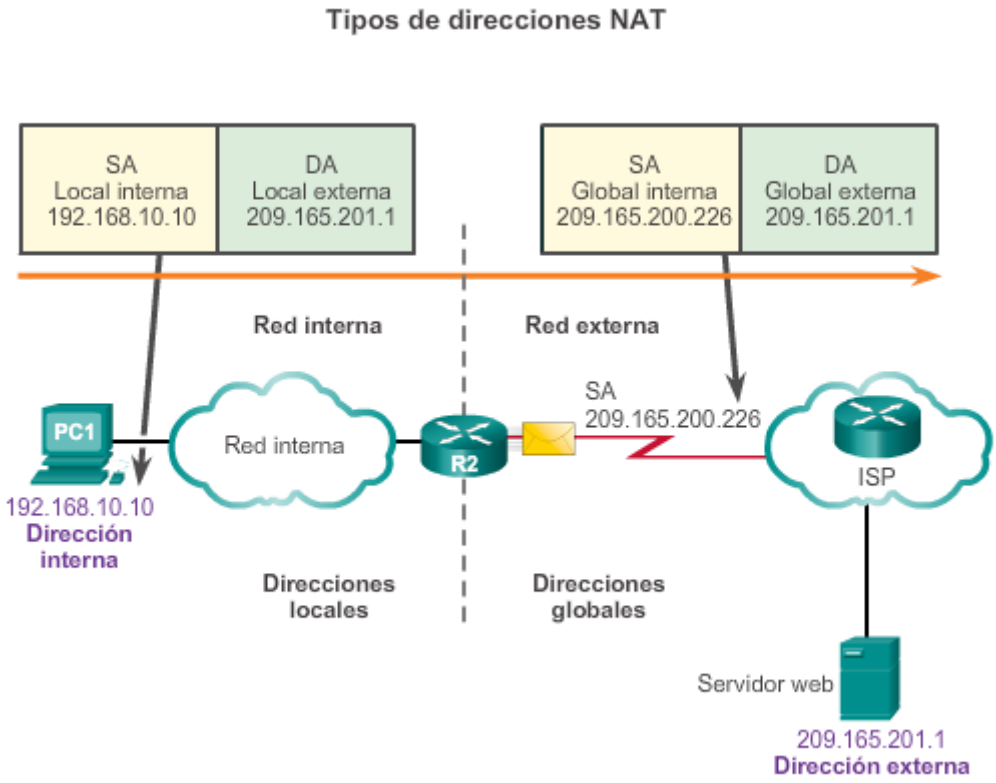
NAT también usa los conceptos de local o global con relación a las direcciones:

- **Dirección local:** cualquier dirección que aparece en la porción interna de la red.
- **Dirección global:** cualquier dirección que aparece en la porción externa de la red.

En la ilustración, la PC1 tiene la dirección local interna 192.168.10.10. Desde la perspectiva de la PC1, el servidor web tiene la dirección externa 209.165.201.1. Cuando se envían los paquetes de la PC1 a la dirección global del servidor web, la dirección local interna de la PC1 se traduce a 209.165.200.226 (dirección global interna). En general, la dirección del dispositivo externo no se traduce, ya que suele ser una dirección IPv4 pública.

Observe que la PC1 tiene distintas direcciones locales y globales, mientras que el servidor web tiene la misma dirección IPv4 pública en ambos casos. Desde la perspectiva del servidor web, el tráfico que se origina en la PC1 parece provenir de 209.165.200.226, la dirección global interna.

El router NAT, el R2 en la ilustración, es el punto de demarcación entre las redes internas y externas, así como entre las direcciones locales y globales.



Capítulo 5: Traducción de direcciones de red para IPv4 5.1.1.4 Terminología de NAT (cont.)

Los términos “interna” y “externa” se combinan con los términos “global” y “local” para hacer referencia a direcciones específicas. En la ilustración, el router R2 se configuró para proporcionar NAT. Este tiene un conjunto de direcciones públicas para asignar a los hosts internos.

- **Dirección local interna:** la dirección de origen vista desde el interior de la red. En la ilustración, la dirección IPv4 192.168.10.10 se asignó a la PC1. Esta es la dirección local interna de la PC1.

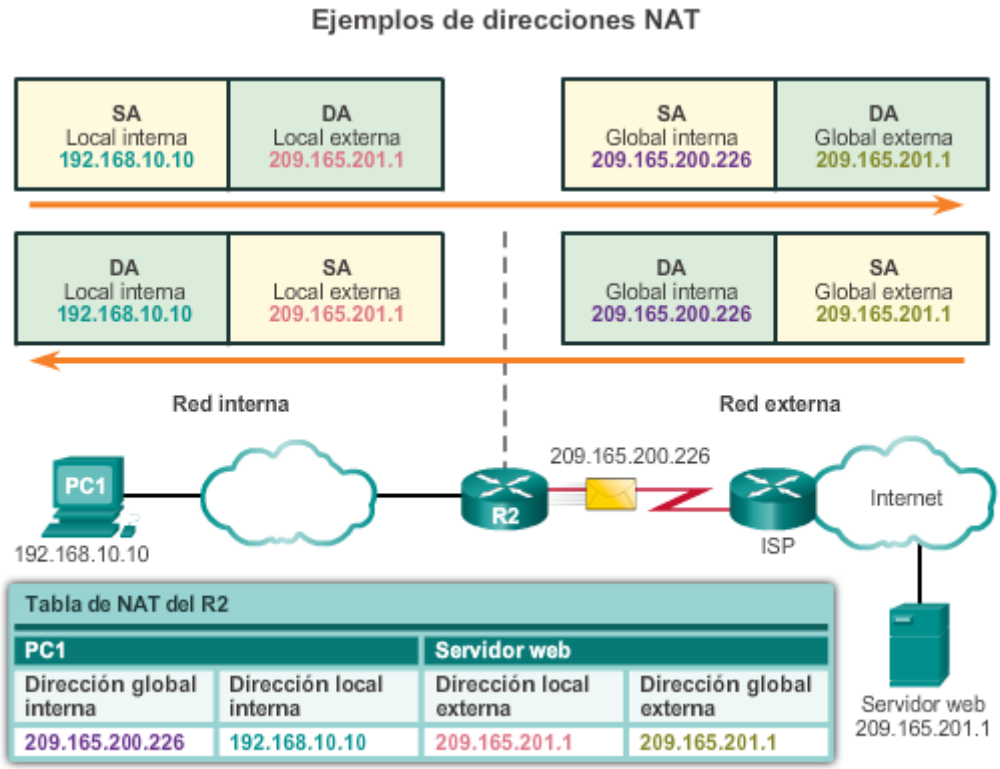
- **Dirección global interna:** la dirección de origen vista desde la red externa. En la ilustración, cuando se envía el tráfico de la PC1 al servidor web en 209.165.201.1, el R2 traduce la dirección local interna a una dirección global interna. En este caso, el R2 cambia la dirección IPv4 de origen de 192.168.10.10 a 209.165.200.226. De acuerdo con la terminología de NAT, la dirección local interna 192.168.10.10 se traduce a la dirección global interna 209.165.200.226.

- **Dirección global externa:** la dirección del destino vista desde la red externa. Es una dirección IPv4 enrutable globalmente y asignada a un host en Internet. Por ejemplo, se puede llegar al servidor web en la dirección IPv4 209.165.201.1. Por lo general, las direcciones externas globales y locales son iguales.

- **Dirección local externa:** la dirección del destino vista desde la red interna. En este ejemplo, la PC1 envía tráfico al servidor web en la dirección IPv4 209.165.201.1. Si bien es poco frecuente, esta dirección podría ser diferente de la dirección globalmente enrutable del destino.

En la ilustración, se muestra cómo se dirige el tráfico que se envía desde una computadora interna hacia un servidor web externo a través del router con NAT habilitada. También se muestra cómo se dirige y se traduce inicialmente el tráfico de retorno.

Nota: el uso de la dirección local externa excede el ámbito de este curso.



Capítulo 5: Traducción de direcciones de red para IPv4 5.1.1.5 ¿Cómo funciona NAT?

En este ejemplo, la PC1 con la dirección privada 192.168.10.10 desea comunicarse con un servidor web externo con la dirección pública 209.165.201.1.

Haga clic en el botón Reproducir de la figura para iniciar la animación.

La PC1 envía un paquete dirigido al servidor web. El R1 reenvía el paquete al R2.

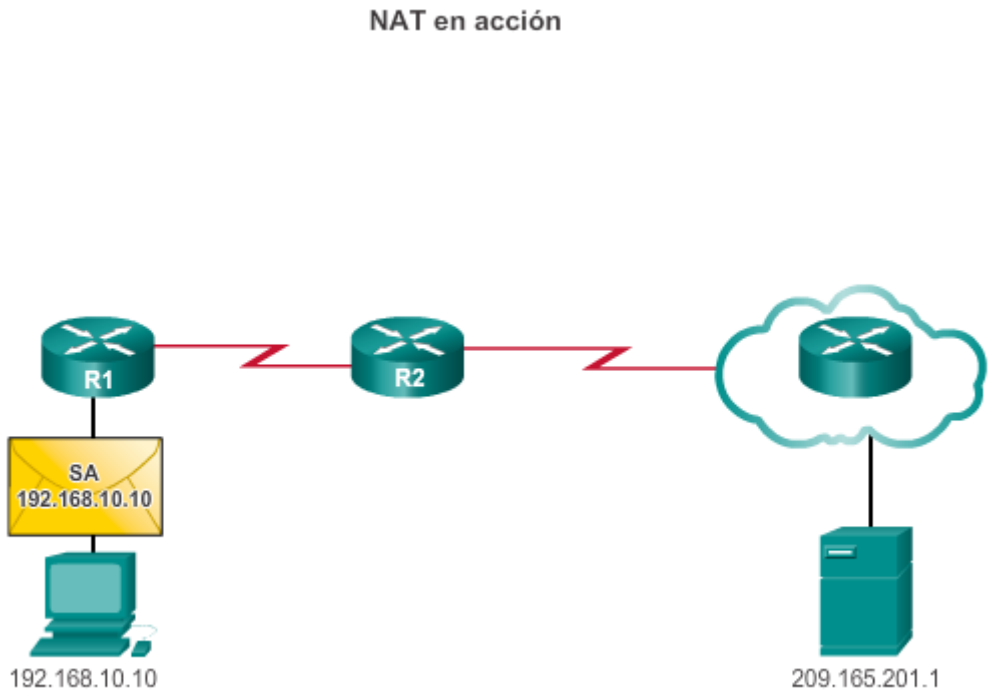
Cuando el paquete llega al R2, el router con NAT habilitada para la red, el R2 lee la dirección IPv4 de origen del paquete para determinar si este cumple con los criterios especificados para la traducción.

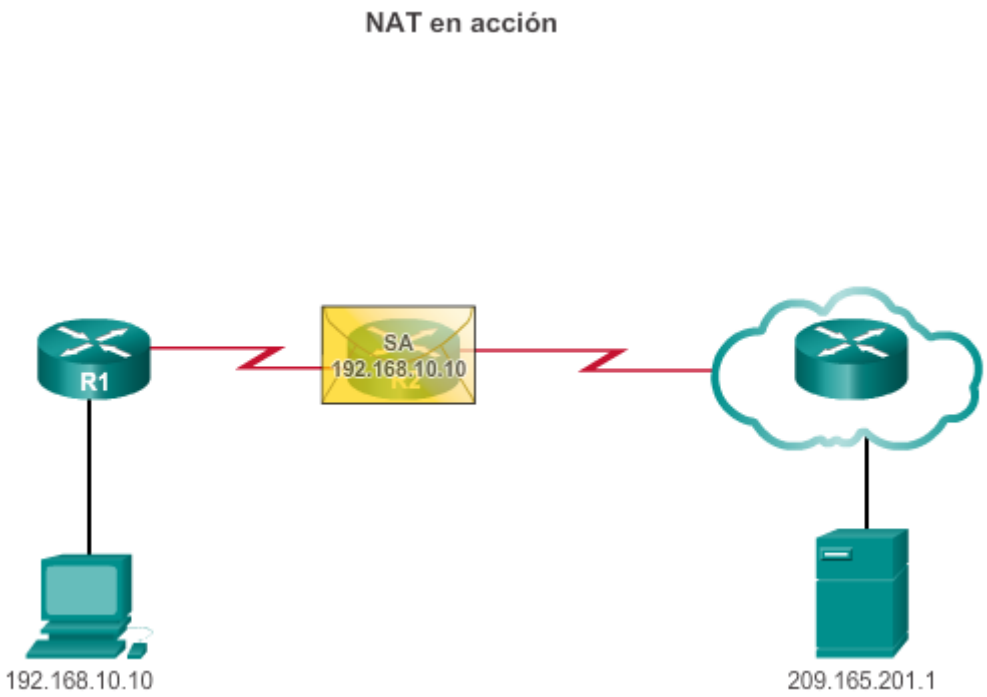
En este caso, la dirección IPv4 de origen cumple con los criterios y se traduce de 192.168.10.10 (dirección local interna) a 209.165.200.226 (dirección global interna). El R2 agrega esta asignación de dirección local a global a la tabla de NAT.

El R2 envía el paquete con la dirección de origen traducida hacia el destino.

El servidor web responde con un paquete dirigido a la dirección global interna de la PC1 (209.165.200.226).

El R2 recibe el paquete con la dirección de destino 209.165.200.226. El R2 revisa la tabla de NAT y encuentra una entrada para esta asignación. El R2 usa esta información y traduce la dirección global interna (209.165.200.226) a la dirección local interna (192.168.10.10), y el paquete se reenvía a la PC1.

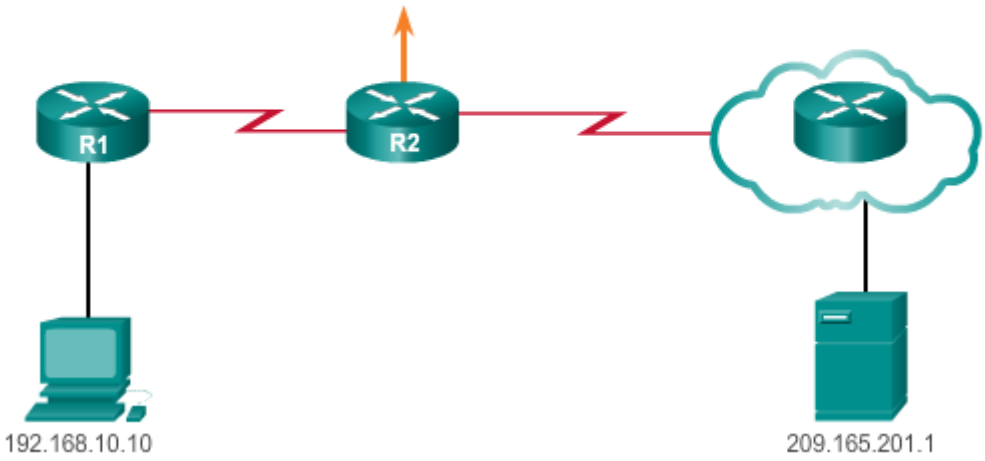




NAT en acción

Tabla NAT

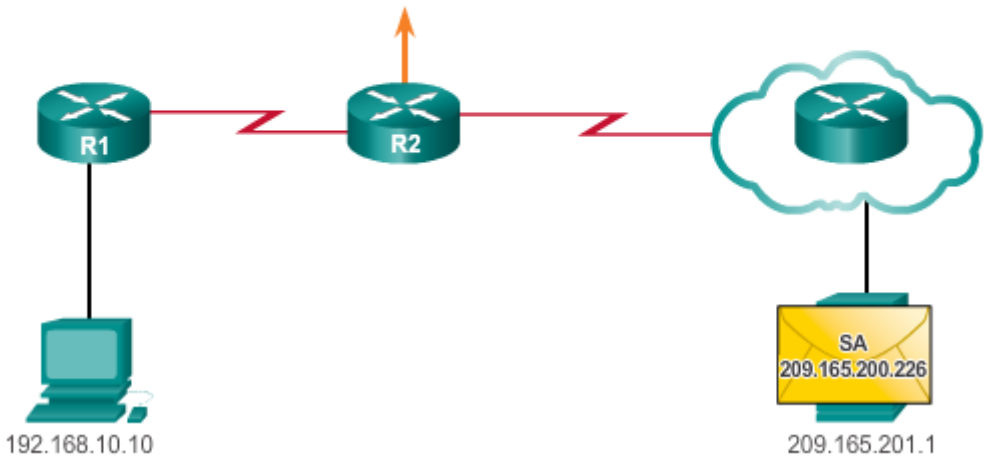
Local interna	Global interna	Local externa	Global externa
192.168.10.10	209.165.200.226	209.165.201.1	209.165.201.1



NAT en acción

Tabla NAT

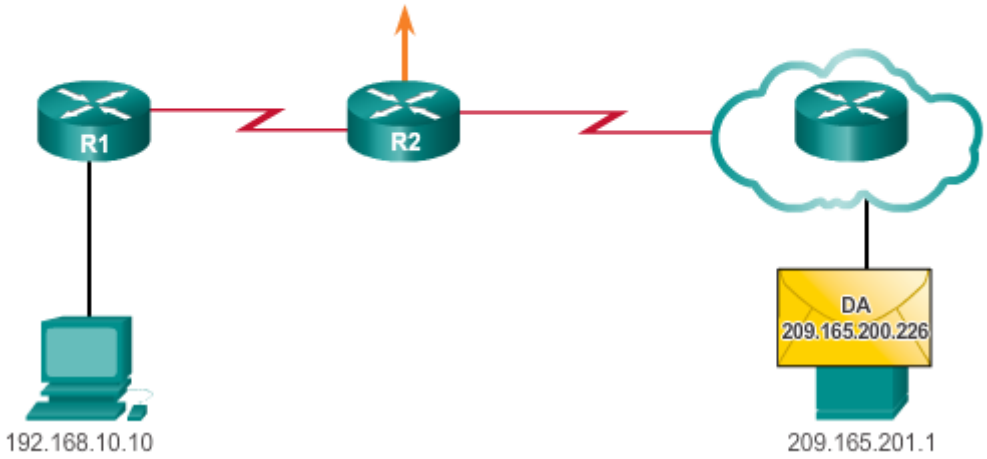
Local interna	Global interna	Local externa	Global externa
192.168.10.10	209.165.200.226	209.165.201.1	209.165.201.1



NAT en acción

Tabla NAT

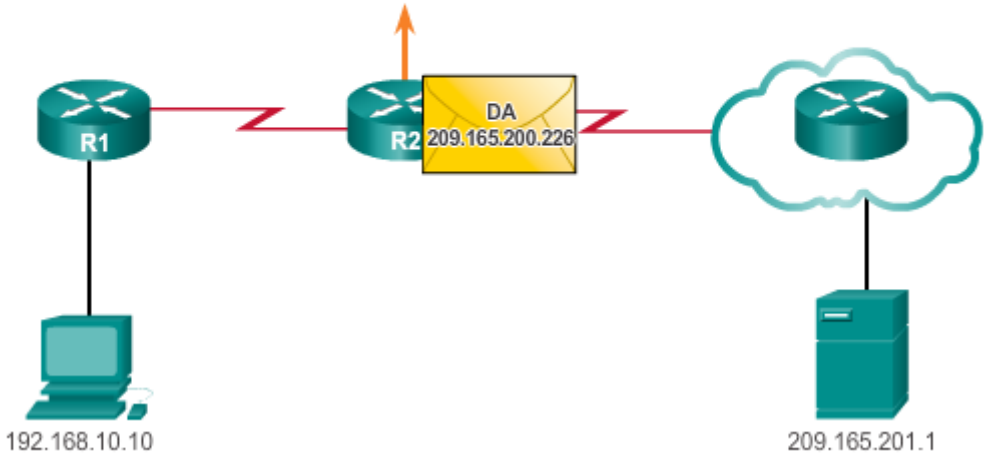
Local interna	Global interna	Local externa	Global externa
192.168.10.10	209.165.200.226	209.165.201.1	209.165.201.1



NAT en acción

Tabla NAT

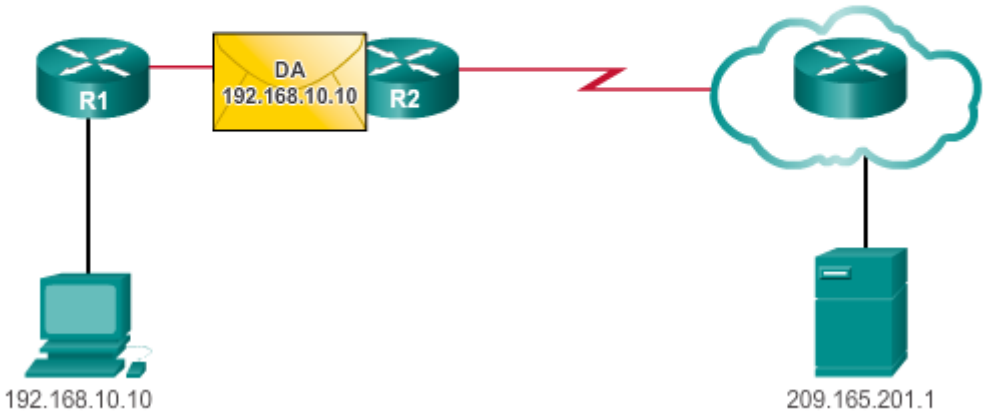
Local interna	Global interna	Local externa	Global externa
192.168.10.10	209.165.200.226	209.165.201.1	209.165.201.1



NAT en acción

Tabla NAT

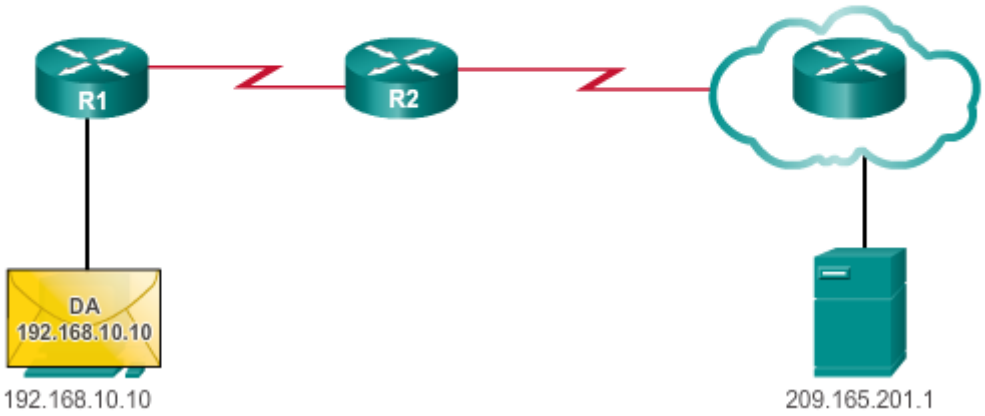
Local interna	Global interna	Local externa	Global externa
192.168.10.10	209.165.200.226	209.165.201.1	209.165.201.1



NAT en acción

Tabla NAT

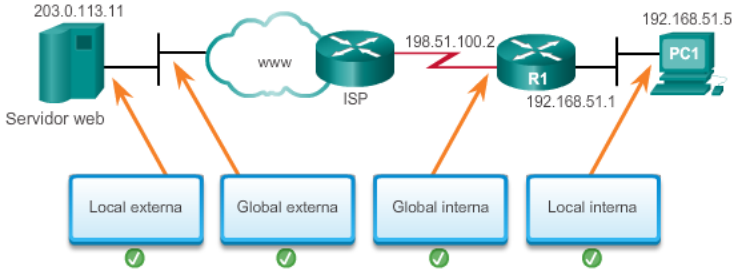
Local interna	Global interna	Local externa	Global externa
192.168.10.10	209.165.200.226	209.165.201.1	209.165.201.1



Capítulo 5: Traducción de direcciones de red para IPv4 5.1.1.6 Actividad: identificar la terminología de NAT

Actividad: Identificar la terminología de NAT

La PC1 se comunica con el servidor web a través de un router con NAT habilitada (R1). Arrastre cada tipo de dirección NAT hacia el campo correspondiente en la topología.



Capítulo 5: Traducción de direcciones de red para IPv4 5.1.2.1 NAT estática

Existen tres tipos de traducción NAT:

- **Traducción estática de direcciones (NAT estática):** asignación de direcciones uno a uno entre una dirección local y una global.
- **Traducción dinámica de direcciones (NAT dinámica):** asignación de varias direcciones a varias direcciones entre direcciones locales y globales.
- **Traducción de la dirección del puerto (PAT):** asignación de varias direcciones a una dirección entre direcciones locales y globales. Este método también se conoce como “sobrecarga” (NAT con sobrecarga).

NAT estática

La NAT estática consiste en una asignación uno a uno entre direcciones locales y globales. Estas asignaciones son configuradas por el administrador de red y se mantienen constantes.

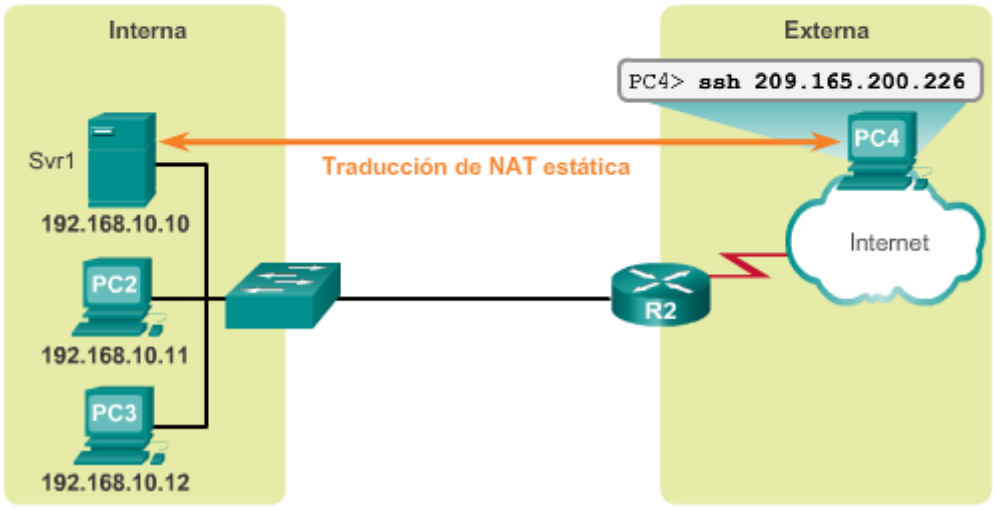
En la ilustración, el R2 se configuró con las asignaciones estáticas para las direcciones locales internas del Svr1, la PC2 y la PC3. Cuando estos dispositivos envían tráfico a Internet, sus direcciones locales internas se traducen a las direcciones globales internas configuradas. Para las redes externas, estos dispositivos tienen direcciones IPv4 públicas.

La NAT estática resulta útil, en especial para los servidores web o los dispositivos que deben tener una dirección constante que sea accesible tanto desde Internet, como desde el servidor web de una empresa. También es útil para los dispositivos a los que debe poder acceder el personal autorizado cuando no está en su lugar de trabajo, pero no el público en general en Internet. Por ejemplo, un administrador de red puede acceder a la dirección global interna del Svr1 (209.165.200.226) desde la PC4 mediante SSH. El R2 traduce esta dirección global interna a la dirección local interna y conecta la sesión del administrador al Svr1.

La NAT estática requiere que haya suficientes direcciones públicas disponibles para satisfacer la cantidad total de sesiones de usuario simultáneas.

NAT estática

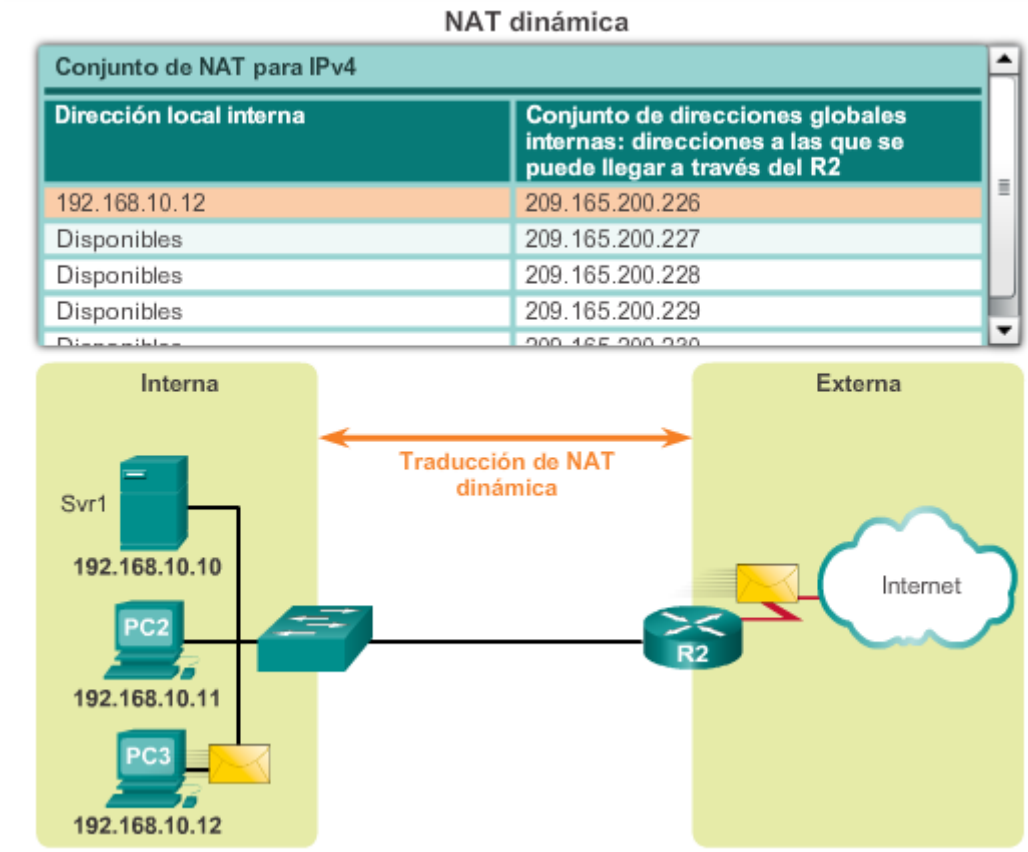
Tabla de NAT estática	
Dirección local interna	**Dirección global interna: direcciones a las que se puede llegar a través del R2**
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228



Capítulo 5: Traducción de direcciones de red para IPv4 5.1.2.2 NAT dinámica

La NAT dinámica utiliza un conjunto de direcciones públicas y las asigna según el orden de llegada. Cuando un dispositivo interno solicita acceso a una red externa, la NAT dinámica asigna una dirección IPv4 pública disponible del conjunto.

En la ilustración, la PC3 accede a Internet mediante la primera dirección disponible del conjunto de NAT dinámica. Las demás direcciones siguen disponibles para utilizarlas. Al igual que la NAT estática, la NAT dinámica requiere que haya suficientes direcciones públicas disponibles para satisfacer la cantidad total de sesiones de usuario simultáneas.



Capítulo 5: Traducción de direcciones de red para IPv4 5.1.2.3 Traducción de la dirección del puerto (PAT)

La traducción de la dirección del puerto (PAT), también conocida como “NAT con sobrecarga”, asigna varias direcciones IPv4 privadas a una única dirección IPv4 pública o a algunas direcciones. Esto es lo que hace la mayoría de los routers domésticos. El ISP asigna una dirección al router, no obstante, varios miembros del hogar pueden acceder a Internet de manera simultánea. Esta es la forma más común de NAT.

Con PAT, se pueden asignar varias direcciones a una o más direcciones, debido a que cada dirección privada también se rastrea con un número de puerto. Cuando un dispositivo inicia una sesión TCP/IP, genera un valor de puerto de origen TCP o UDP para identificar la sesión de forma exclusiva. Cuando el router NAT recibe un paquete del cliente, utiliza su número de puerto de origen para identificar de forma exclusiva la traducción NAT específica.

PAT garantiza que los dispositivos usen un número de puerto TCP distinto para cada sesión con un servidor en Internet. Cuando llega una respuesta del servidor, el número de puerto de origen, que se convierte en el número de puerto de destino en la devolución, determina a qué dispositivo el router reenvía los paquetes. El proceso de PAT también valida que los paquetes entrantes se hayan solicitado, lo que añade un grado de seguridad a la sesión.

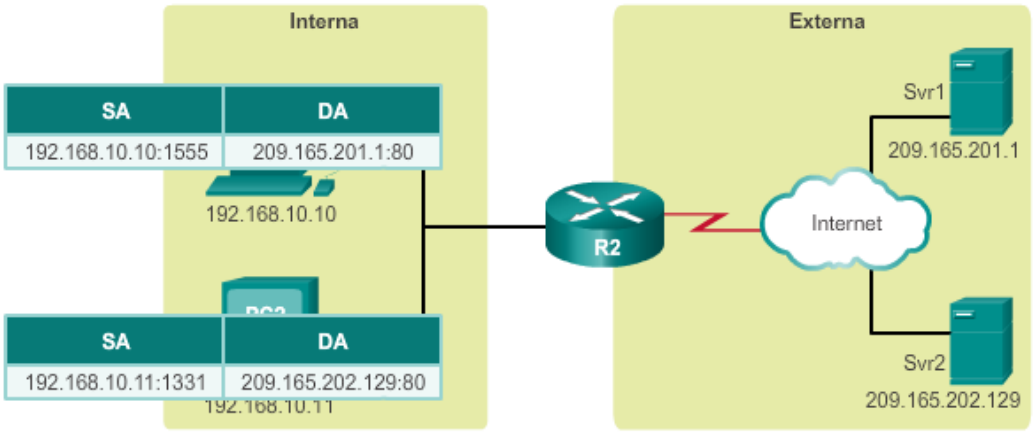
Haga clic en los botones Reproducir y Pausa de la ilustración para controlar la animación.

En la animación, se muestra el proceso de PAT. PAT agrega números de puerto de origen únicos a la dirección global interna para distinguir las traducciones.

A medida que el R2 procesa cada paquete, utiliza un número de puerto (1331 y 1555, en este ejemplo) para identificar el dispositivo en el que se originó el paquete. La dirección de origen (SA) es la dirección local interna a la que se agregó el número de puerto TCP/IP asignado. La dirección de destino (DA) es la dirección local externa a la que se agregó el número de puerto de servicio. En este ejemplo, el puerto de servicio es 80, que es HTTP.

Para la dirección de origen, el R2 traduce la dirección local interna a una dirección global interna con el número de puerto agregado. La dirección de destino no se modifica, pero ahora se la denomina “dirección IP global externa”. Cuando el servidor web responde, se invierte la ruta.

Proceso PAT



Proceso PAT

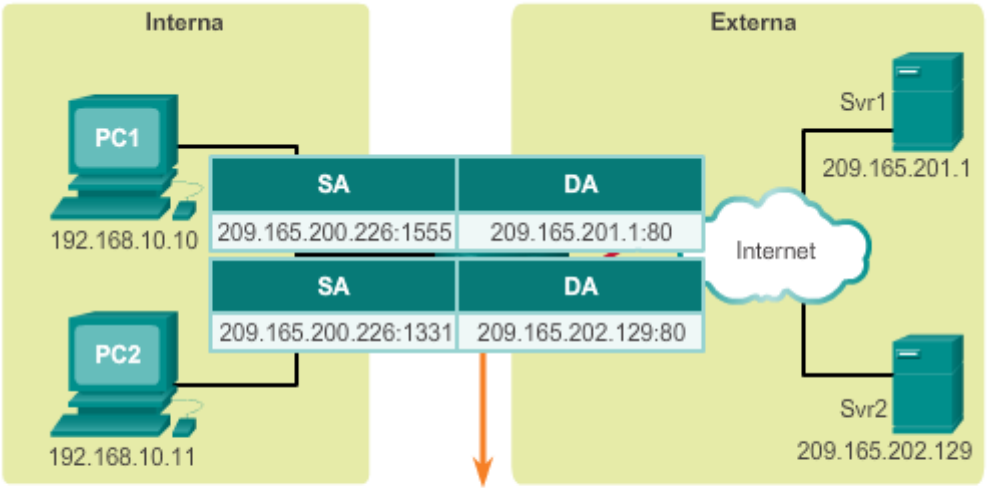


Tabla NAT con sobrecarga

Dirección IP global interna	Dirección IP local interna	Dirección IP local externa	Dirección IP global externa
209.165.200.226:1555	192.168.10.10:1555	209.165.201.1:80	209.165.201.1:80
209.165.200.226:1331	192.168.10.11:1331	209.165.202.129:80	209.165.202.129:80

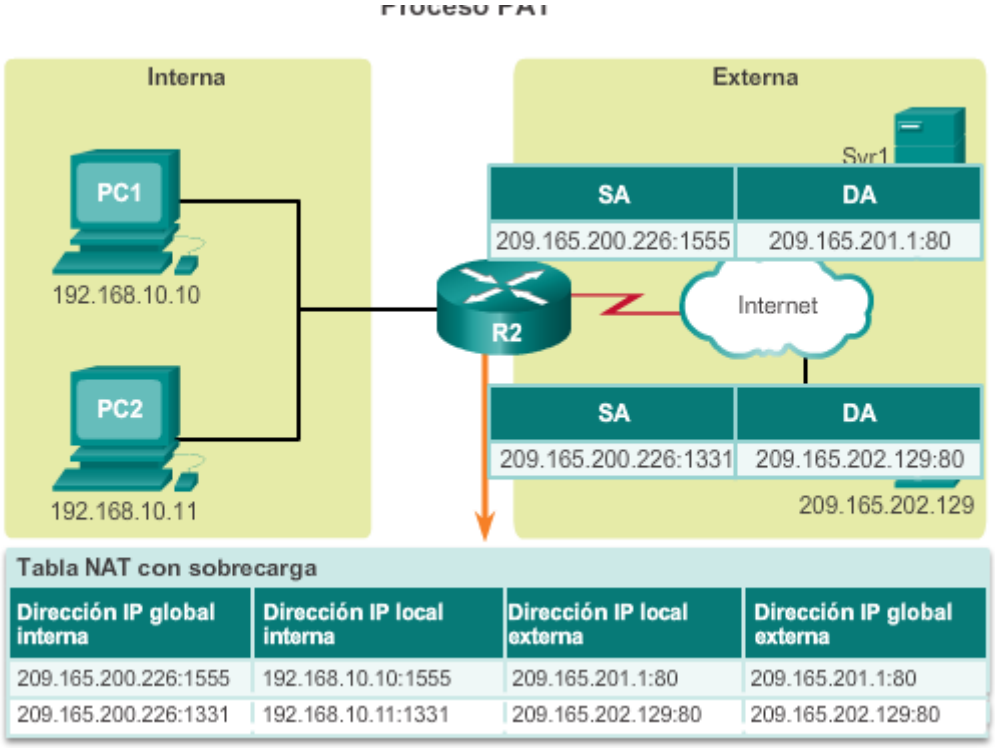


Tabla NAT con sobrecarga

Dirección IP global interna	Dirección IP local interna	Dirección IP local externa	Dirección IP global externa
209.165.200.226:1555	192.168.10.10:1555	209.165.201.1:80	209.165.201.1:80
209.165.200.226:1331	192.168.10.11:1331	209.165.202.129:80	209.165.202.129:80

Capítulo 5: Traducción de direcciones de red para IPv4 5.1.2.4 Siguiente puerto disponible

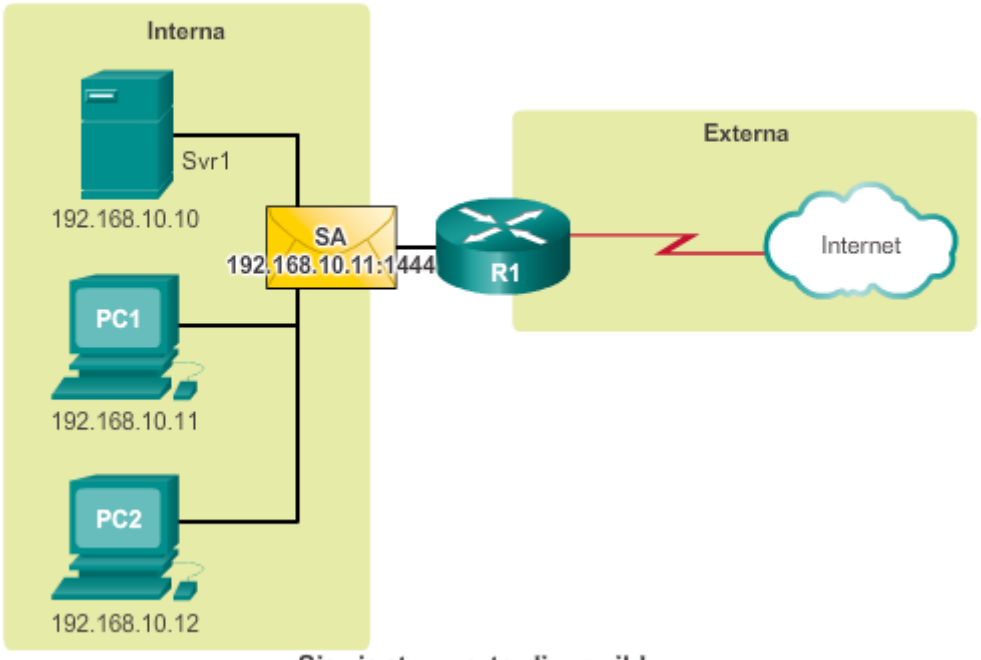
En el ejemplo anterior, los números de puerto del cliente, 1331 y 1555, no se modificaron en el router con NAT habilitada. Esta no es una situación muy probable, porque existe una gran posibilidad de que estos números de puerto ya se hayan conectado a otras sesiones activas.

PAT intenta conservar el puerto de origen inicial. Sin embargo, si el puerto de origen inicial ya está en uso, PAT asigna el primer número de puerto disponible desde el comienzo del grupo de puertos correspondiente de 0 a 511, 512 a 1023 o 1024 a 65 535. Cuando no hay más puertos disponibles y hay más de una dirección externa en el conjunto de direcciones, PAT avanza a la siguiente dirección para intentar asignar el puerto de origen inicial. Este proceso continúa hasta que no haya más direcciones IP externas o puertos disponibles.

Haga clic en el botón Reproducir de la ilustración para ver el funcionamiento de PAT.

En la animación, los hosts eligieron el mismo número de puerto 1444. Esto resulta aceptable para la dirección interna, porque los hosts tienen direcciones IP privadas únicas. Sin embargo, en el router NAT, se deben cambiar los números de puerto; de lo contrario, los paquetes de dos hosts distintos saldrían del R2 con la misma dirección de origen. En este ejemplo, PAT asignó el siguiente puerto disponible (1445) a la segunda dirección host.

Siguiente puerto disponible



Siguiente puerto disponible

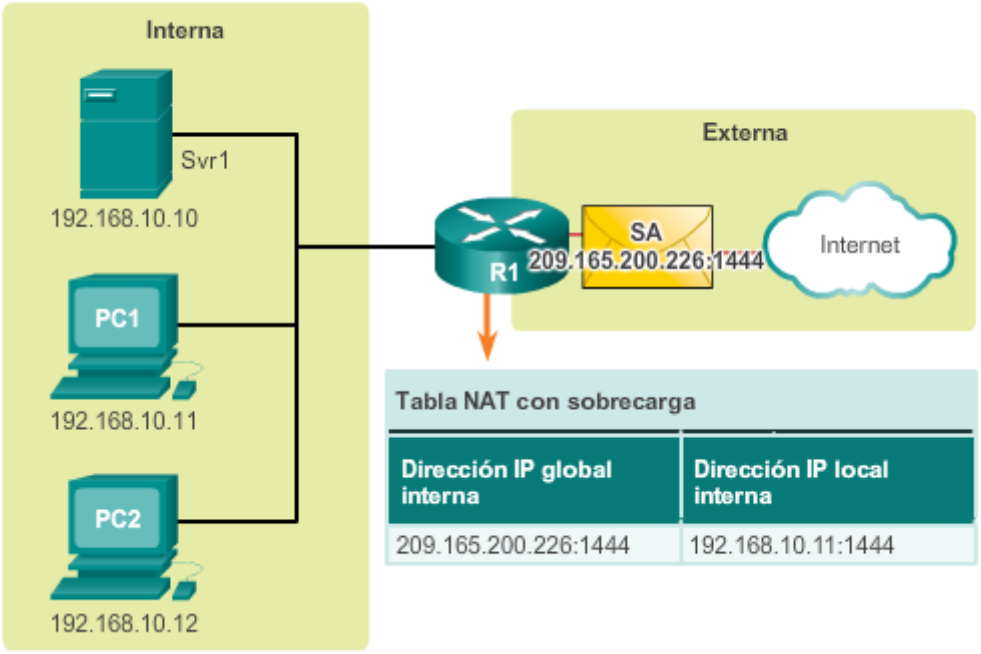


Tabla NAT con sobrecarga

Dirección IP global interna	Dirección IP local interna
209.165.200.226:1444	192.168.10.11:1444

Siguiente puerto disponible

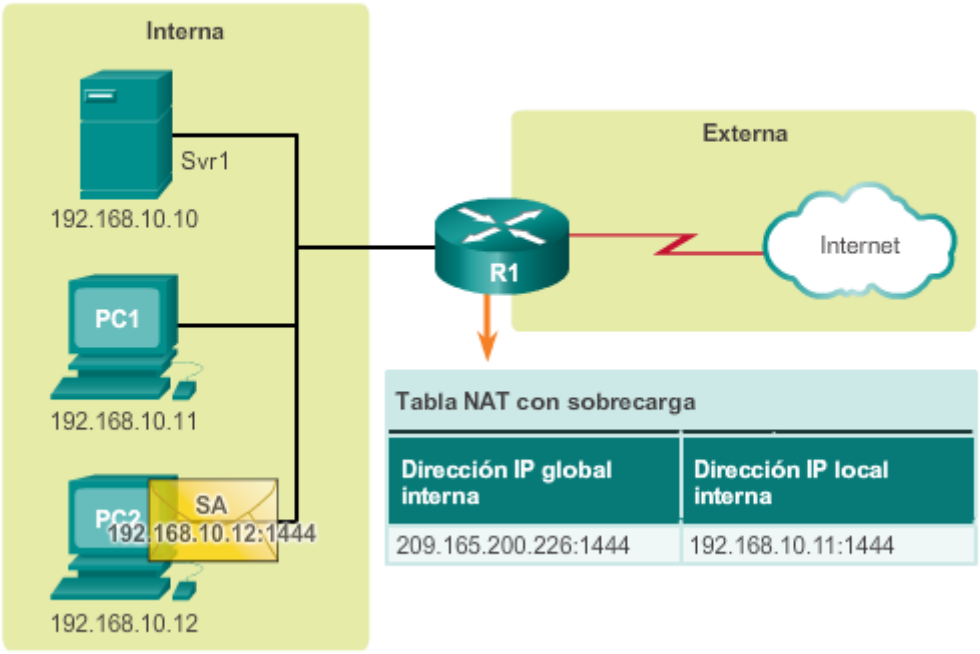


Tabla NAT con sobrecarga

Dirección IP global interna	Dirección IP local interna
209.165.200.226:1444	192.168.10.11:1444

Siguiente puerto disponible

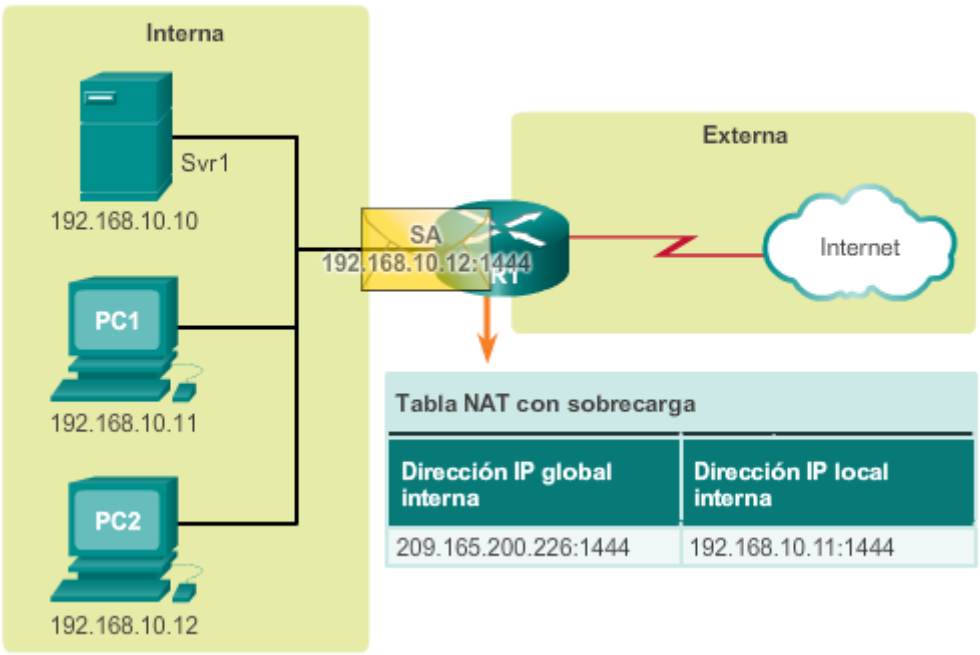
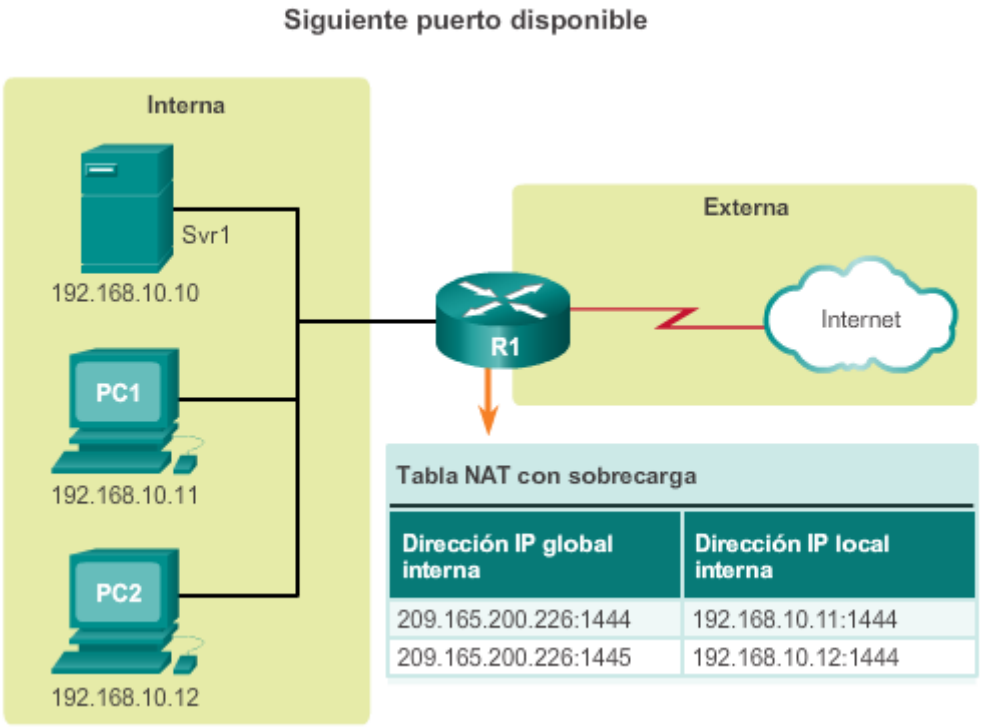
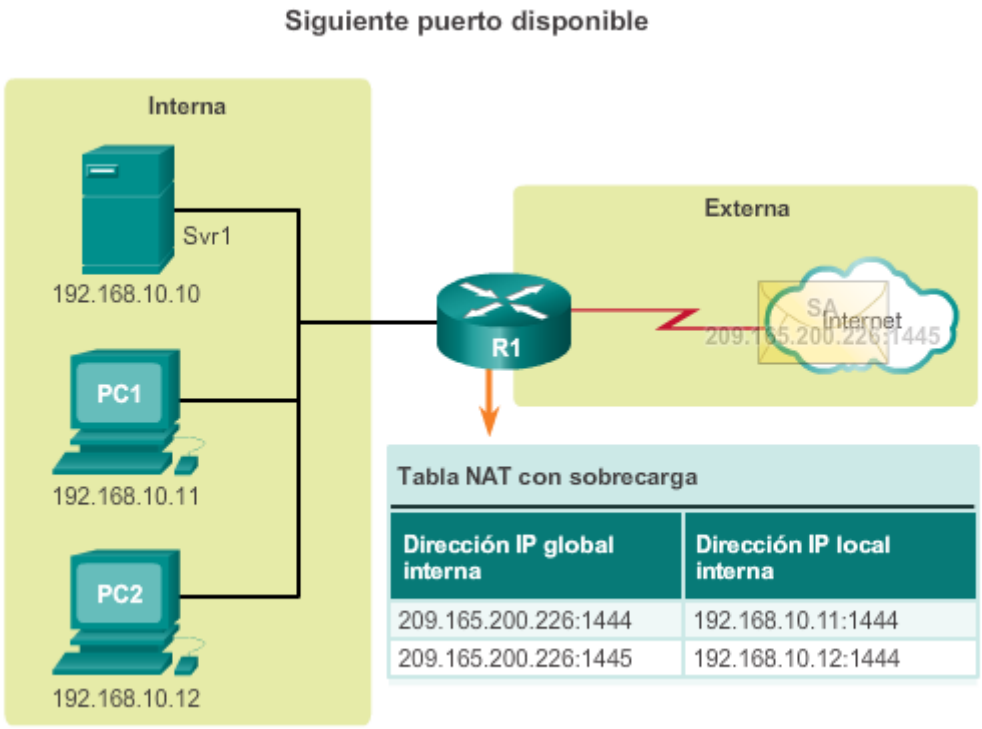


Tabla NAT con sobrecarga

Dirección IP global interna	Dirección IP local interna
209.165.200.226:1444	192.168.10.11:1444





Capítulo 5: Traducción de direcciones de red para IPv4 5.1.2.5 Comparación entre NAT y PAT

Hacer un resumen de las diferencias entre NAT y PAT contribuye a la comprensión de ambas.

Como se muestran en la ilustración, NAT traduce direcciones IPv4 en una relación de 1:1 entre direcciones IPv4 privadas y direcciones IPv4 públicas. Sin embargo, PAT modifica la dirección y el número de puerto.

NAT reenvía los paquetes entrantes a su destino interno mediante la dirección IPv4 de origen de entrada proporcionada por el host en la red pública. En general, con PAT hay solo una o muy pocas direcciones IPv4 públicamente expuestas. Los paquetes entrantes de la red pública se enrutan a sus destinos en la red privada consultando una tabla en el router NAT. Esta tabla hace un seguimiento de los pares de puertos públicos y privados. Esto se denomina "seguimiento de conexiones".

Paquetes sin segmento de capa 4

¿Qué sucede con los paquetes IPv4 que transportan datos que no son segmentos TCP o UDP? Estos paquetes no contienen un número de puerto de capa 4. PAT traduce la mayoría de los protocolos comunes transmitidos mediante IPv4 que no utilizan TCP o UDP como protocolo de la capa de transporte. El más común de ellos es ICMPv4. PAT maneja cada uno de estos tipos de protocolos de manera diferente. Por ejemplo, los mensajes de consulta, las solicitudes de eco y las respuestas de eco de ICMPv4 incluyen una ID de consulta. ICMPv4 utiliza la ID de consulta para identificar una solicitud de eco con su respectiva respuesta. La ID de consulta aumenta con cada solicitud de eco enviada. PAT utiliza la ID de consulta en lugar de un número de puerto de capa 4.

Nota: otros mensajes ICMPv4 no utilizan la ID de consulta. Estos mensajes y otros protocolos que no utilizan los números de puerto TCP o UDP varían y exceden el ámbito de este currículo.

Comparación entre NAT y PAT

NAT	
Conjunto de direcciones globales internas	**Dirección local interna**
209.165.200.226	192.168.10.10
209.165.200.227	192.168.10.11
209.165.200.228	192.168.10.12
209.165.200.229	192.168.10.13

PAT	
Dirección global interna	**Dirección local interna**
209.165.200.226:1444	192.168.10.10:1444
209.165.200.226:1445	192.168.10.11:1444
209.165.200.226:1555	192.168.10.12:1555
209.165.200.226:1556	192.168.10.13:1555

Capítulo 5: Traducción de direcciones de red para IPv4 5.1.2.6 Packet Tracer: investigación del funcionamiento de NAT

Información básica/situación

A medida que la trama se transmite a través de una red, las direcciones MAC pueden cambiar. Las direcciones IP también pueden cambiar cuando un paquete es reenviado por un dispositivo configurado con NAT. En esta actividad, investigaremos qué sucede a las direcciones IP durante el proceso de NAT.

Packet Tracer: investigación del funcionamiento de NAT (instrucciones)

Packet Tracer: investigación del funcionamiento de NAT (PKA)

Capítulo 5: Traducción de direcciones de red para IPv4 5.1.3.1 Beneficios de NAT

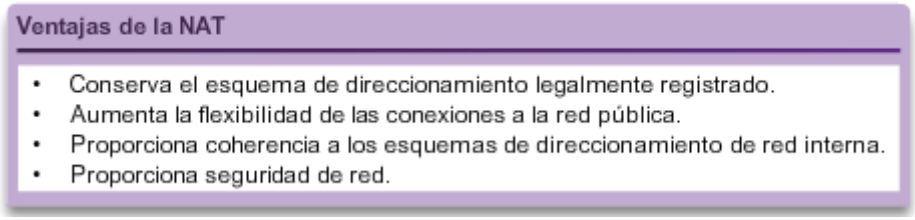
Como se resalta en la ilustración, NAT proporciona muchos beneficios, incluido lo siguiente:

- NAT conserva el esquema de direccionamiento legalmente registrado al permitir la privatización de las intranets. NAT conserva las direcciones mediante la multiplexación de aplicaciones en el nivel de puerto. Con la NAT con sobrecarga, los hosts internos pueden compartir una única dirección IPv4 pública para todas las comunicaciones externas. En este tipo de configuración, se requieren muy pocas direcciones externas para admitir varios hosts internos.

- NAT aumenta la flexibilidad de las conexiones a la red pública. Se pueden implementar varios conjuntos y conjuntos de respaldo y de equilibrio de carga para asegurar conexiones de red pública confiables.

- NAT proporciona coherencia a los esquemas de direccionamiento de red interna. Para cambiar el esquema de direcciones IPv4 públicas en una red que no utiliza direcciones IPv4 privadas ni NAT, se requiere redireccionar todos los hosts en la red existente. Los costos de redireccionamiento de hosts pueden ser considerables. NAT permite mantener el esquema de direcciones IPv4 privadas existente a la vez que facilita el cambio a un nuevo esquema de direccionamiento público. Esto significa que una organización podría cambiar los ISP sin necesidad de modificar ninguno de sus clientes internos.

- NAT proporciona seguridad de red. Debido a que las redes privadas no anuncian sus direcciones ni su topología interna, son razonablemente seguras cuando se utilizan en conjunto con NAT para obtener acceso externo controlado. Sin embargo, NAT no reemplaza a los firewalls.



Capítulo 5: Traducción de direcciones de red para IPv4 5.1.3.2 Desventajas de la NAT

Como se resalta en la ilustración, NAT presenta algunas desventajas. El hecho de que los hosts en Internet parezcan comunicarse de forma directa con el dispositivo con NAT habilitada,

en lugar de hacerlo con el host real dentro de la red privada, genera una serie de inconvenientes.

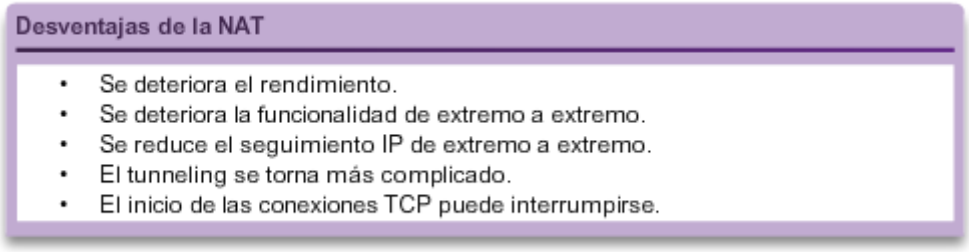
Una desventaja del uso de NAT se relaciona con el rendimiento de la red, en especial, en el caso de los protocolos en tiempo real como VoIP. NAT aumenta los retrasos de switching porque la traducción de cada dirección IPv4 dentro de los encabezados del paquete lleva tiempo. Al primer paquete siempre se aplica el switching de procesos por la ruta más lenta. El router debe revisar todos los paquetes para decidir si necesitan traducción. El router debe modificar el encabezado de IPv4 y, posiblemente, el encabezado TCP o UDP. El checksum del encabezado de IPv4, junto con el checksum de TCP o UDP, se debe volver a calcular cada vez que se realiza una traducción. Si existe una entrada de caché, el resto de los paquetes atraviesan la ruta de switching rápido; de lo contrario, también se retrasan.

Otra desventaja del uso de NAT es que se pierde el direccionamiento de extremo a extremo. Muchos protocolos y aplicaciones de Internet dependen del direccionamiento de extremo a extremo desde el origen hasta el destino. Algunas aplicaciones no funcionan con NAT. Por ejemplo, algunas aplicaciones de seguridad, como las firmas digitales, fallan porque la dirección IPv4 de origen cambia antes de llegar a destino. Las aplicaciones que utilizan direcciones físicas, en lugar de un nombre de dominio calificado, no llegan a los destinos que se traducen a través del router NAT. En ocasiones, este problema se puede evitar al implementar las asignaciones de NAT estática.

También se reduce el seguimiento IPv4 de extremo a extremo. El seguimiento de los paquetes que pasan por varios cambios de dirección a través de varios saltos de NAT se torna mucho más difícil y, en consecuencia, dificulta la resolución de problemas.

El uso de NAT también genera complicaciones para los protocolos de tunneling como IPsec, ya que NAT modifica los valores en los encabezados que interfieren en las verificaciones de integridad que realizan IPsec y otros protocolos de tunneling.

Los servicios que requieren que se inicie una conexión TCP desde la red externa, o “protocolos sin estado”, como los servicios que utilizan UDP, pueden interrumpirse. A menos que el router NAT esté configurado para admitir dichos protocolos, los paquetes entrantes no pueden llegar a su destino. Algunos protocolos pueden admitir una instancia de NAT entre los hosts participantes (por ejemplo, FTP de modo pasivo), pero fallan cuando NAT separa a ambos sistemas de Internet.



Capítulo 5: Traducción de direcciones de red para IPv4 5.2.1.1 Configuración de NAT estática

La NAT estática es una asignación uno a uno entre una dirección interna y una dirección externa. La NAT estática permite que los dispositivos externos inicien conexiones a los

dispositivos internos mediante la dirección pública asignada de forma estática. Por ejemplo, se puede asignar una dirección global interna específica a un servidor web interno de modo que se pueda acceder a este desde redes externas.

En la figura 1, se muestra una red interna que contiene un servidor web con una dirección IPv4 privada. El router R2 se configuró con NAT estática para permitir que los dispositivos en la red externa (Internet) accedan al servidor web. El cliente en la red externa accede al servidor web mediante una dirección IPv4 pública. La NAT estática traduce la dirección IPv4 pública a la dirección IPv4 privada.

Existen dos pasos básicos para configurar las traducciones NAT estáticas.

Paso 1. El primer paso consiste en crear una asignación entre la dirección local interna y las direcciones globales internas. Por ejemplo, en la figura 1, la dirección local interna 192.168.10.254 y la dirección global interna 209.165.201.5 se configuraron como traducción NAT estática.

Paso 2. Una vez configurada la asignación, las interfaces que participan en la traducción se configuran como interna o externa con respecto a NAT. En el ejemplo, la interfaz Serial 0/0/0 del R2 es una interfaz interna, y la interfaz Serial 0/1/0 es una interfaz externa.

Los paquetes que llegan hasta la interfaz interna del R2 (Serial 0/0/0) desde la dirección IPv4 local interna configurada (192.168.10.254) se traducen y, luego, se reenvían hacia la red externa. Los paquetes que llegan a la interfaz externa del R2 (Serial 0/1/0), que están dirigidos a la dirección IPv4 global interna configurada (209.165.201.5), se traducen a la dirección local interna (192.168.10.254) y, luego, se reenvían a la red interna.

En la figura 2, se describen los comandos necesarios para configurar la NAT estática.

En la figura 3, se muestran los comandos necesarios en el R2 para crear una asignación de NAT estática al servidor web en la topología de ejemplo. Con la configuración que se muestra, el R2 traduce los paquetes del servidor web con la dirección 192.168.10.254 a la dirección IPv4 pública 209.165.201.5. El cliente de Internet dirige solicitudes web a la dirección IPv4 pública 209.165.201.5. El R2 reenvía ese tráfico al servidor web en 192.168.10.254.

Utilice el verificador de sintaxis de la figura 4 para configurar una entrada de NAT estática adicional en el R2.

Topología de NAT estática

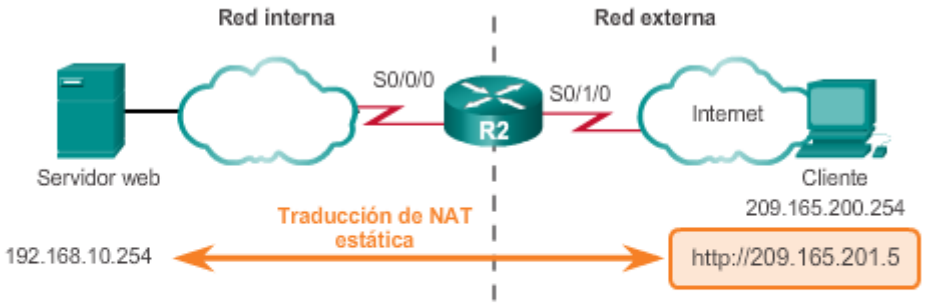


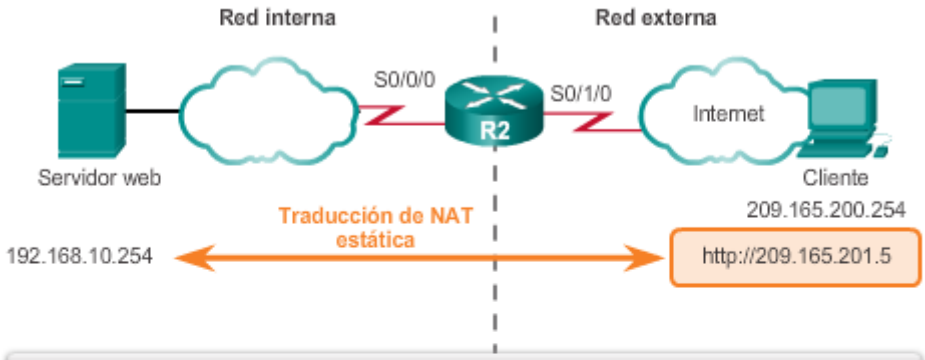
Tabla de NAT estática

Dirección global interna	Dirección local interna
209.165.201.5	192.168.10.254

Configuración de NAT estática

Revise	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 ip-local ip-global`	Introduzca el comando **`no ip nat inside source static`** del modo de configuración global para eliminar la traducción dinámica de origen.
2	Especificar la interfaz interna. `Router(config)# interface tipo número`	Introduzca el comando **`interface`**. La petición de entrada de la CLI cambia 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	Especificar la interfaz externa. `Router(config)# interface tipo número`	
6	Marque la interfaz como conectada al exterior. `Router(config-if)# ip nat outside`	

Configuración NAT estática de ejemplo

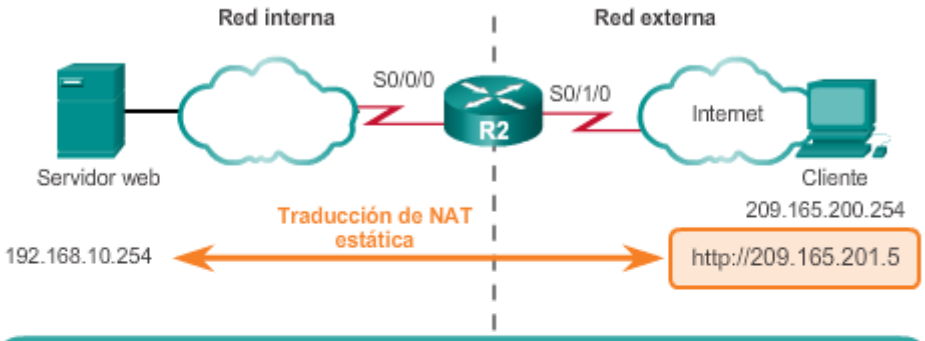



```
Establishes static translation between an inside local address and
an inside global address.
R2(config)# ip nat inside source static 192.168.10.254 209.165.201.5

R2(config)# interface Serial0/0/0
R2(config-if)# ip address 10.1.1.2 255.255.255.252
Identifies interface serial 0/0/0 as an inside NAT interface.
R2(config-if)# ip nat inside
R2(config-if)# exit

R2(config)# interface Serial0/1/0
R2(config-if)# ip address 209.165.200.225 255.255.255.224
Identifies interface serial 0/1/0 as the outside NAT interface.
R2(config-if)# ip nat outside
```

Configuración de subinterfaces punto a punto en el R2




```
Configure la traducción estática con una dirección local interna 192.168.11.99
y una dirección global interna 201.165.201.15.
R2(config)# ip nat inside source static 192.168.11.99 209.16
Configure la interfaz NAT interna adecuada.
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside
Configure la interfaz NAT externa adecuada.
R2(config)# interface Serial0/1/0
R2(config-if)# ip nat outside
Configuró correctamente la NAT estática.
```

Capítulo 5: Traducción de direcciones de red para IPv4 5.2.1.2 Análisis de NAT estática

Con la configuración anterior, en la ilustración se muestra el proceso de traducción de NAT estática entre el cliente y el servidor web. En general, las traducciones estáticas se utilizan cuando los clientes en la red externa (Internet) necesitan llegar a los servidores en la red interna.

1. El cliente desea establecer una conexión al servidor web. El cliente envía un paquete al servidor web con la dirección IPv4 pública de destino 209.165.201.5. Esta es la dirección global interna del servidor web.

2. El primer paquete que recibe del cliente en su interfaz NAT externa ocasiona que el R2 revise su tabla de NAT. Una vez que se encuentra la dirección IPv4 de destino en la tabla de NAT, se traduce.

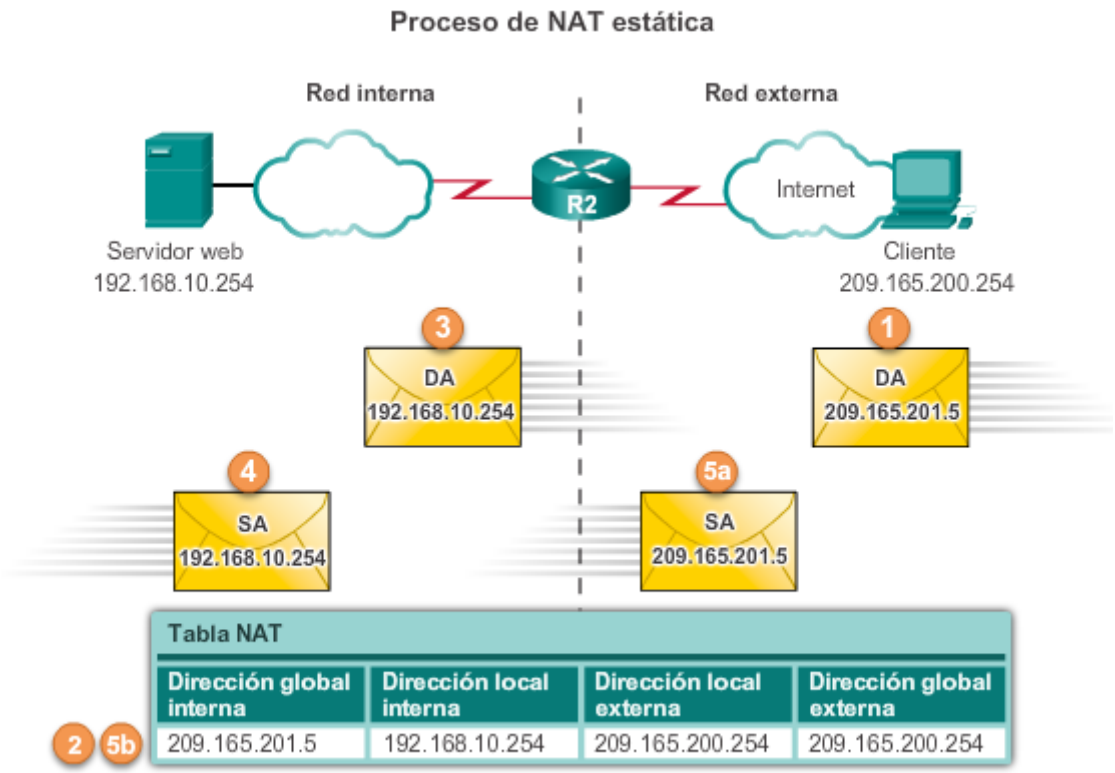
3. El R2 reemplaza la dirección global interna 209.165.201.5 por la dirección local interna 192.168.10.254. Luego, el R2 reenvía el paquete hacia el servidor web.

4. El servidor web recibe el paquete y responde al cliente con la dirección local interna, 192.168.10.254.

5a. El R2 recibe el paquete del servidor web en su interfaz NAT interna con la dirección de origen de la dirección local interna del servidor web, 192.168.10.254.

5b. El R2 busca una traducción para la dirección local interna en la tabla de NAT. La dirección se encuentra en esa tabla. El R2 traduce la dirección de origen a la dirección global interna 209.165.201.5 y reenvía el paquete por su interfaz serial 0/1/0 hacia el cliente.

6. El cliente recibe el paquete y continúa la conversación. El router NAT lleva a cabo los pasos 2 a 5b para cada paquete. El paso 6 no aparece en la ilustración.



Capítulo 5: Traducción de direcciones de red para IPv4 5.2.1.3 Verificación de NAT estática

El comando **show ip nat translations** es útil para verificar el funcionamiento de NAT. Este comando muestra las traducciones NAT activas. A diferencia de las traducciones dinámicas, las traducciones estáticas siempre figuran en la tabla de NAT. En la figura 1, se muestra el resultado de este comando con el ejemplo de configuración anterior. Debido a que el ejemplo es una configuración NAT estática, siempre figura una traducción en la tabla de NAT, independientemente de que haya comunicaciones activas. Si se emite el comando durante una sesión activa, el resultado también indica la dirección del dispositivo externo, como se muestra en la figura 1.

Otro comando útil es **show ip nat statistics**. Como se muestra en la figura 2, el comando **show ip nat statistics** muestra información sobre la cantidad total de traducciones activas, los parámetros de configuración NAT, la cantidad de direcciones en el conjunto y la cantidad de direcciones que se asignaron.

Para verificar que la traducción NAT funcione, es conveniente borrar las estadísticas de todas las traducciones anteriores con el comando **clear ip nat statistics** antes de realizar la prueba.

Antes de cualquier comunicación con el servidor web, el comando **show ip nat statistics** no muestra ningún acierto actual. Una vez que el cliente establece una sesión con el servidor web, el comando**show ip nat statistics** muestra cinco aciertos. De este modo, se verifica que se lleva a cabo la traducción de NAT estática en el R2.

Verificación de las traducciones de NAT estática

La traducción estática siempre está presente en la tabla de NAT.

```
R2# show ip nat translations
Pro Inside global  Inside local   Outside local  Outside global
--- 209.165.201.5  192.168.10.254  ---            ---
R2#
```

La traducción estática durante una sesión activa.

```
R2# show ip nat translations
Pro Inside global Inside local   Outside local    Outside global
--- 209.165.201.5 192.168.10.254 209.165.200.254  209.165.200.254
R2#
```

Verificación de las estadísticas de NAT estática

```
R2# clear ip nat statistics

R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/0/0
Hits: 0  Misses: 0
<resultado omitido>
Client PC establishes a session with the web server

R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 2, occurred 00:00:14 ago
Outside interfaces:
  Serial0/1/0
Inside interfaces:
  Serial0/0/0
Hits: 5  Misses: 0
<resultado omitido>
```

Capítulo 5: Traducción de direcciones de red para IPv4 5.2.1.4 Packet Tracer: configuración de NAT estática

Información básica/situación

En las redes IPv4 configuradas, los clientes y los servidores utilizan direcciones privadas. Para que los paquetes con direcciones privadas puedan transmitirse por Internet, deben traducirse en direcciones públicas. Los servidores a los que se puede acceder desde fuera de la organización generalmente tienen asignadas una dirección IP estática pública y una privada. En esta actividad, deberá configurar NAT estática de modo que los dispositivos externos puedan acceder al servidor interno en su dirección pública.

Packet Tracer: configuración de NAT estática (instrucciones)

Packet Tracer: configuración de NAT estática (PKA)

Capítulo 5: Traducción de direcciones de red para IPv4 5.2.2.1 Funcionamiento de NAT dinámica

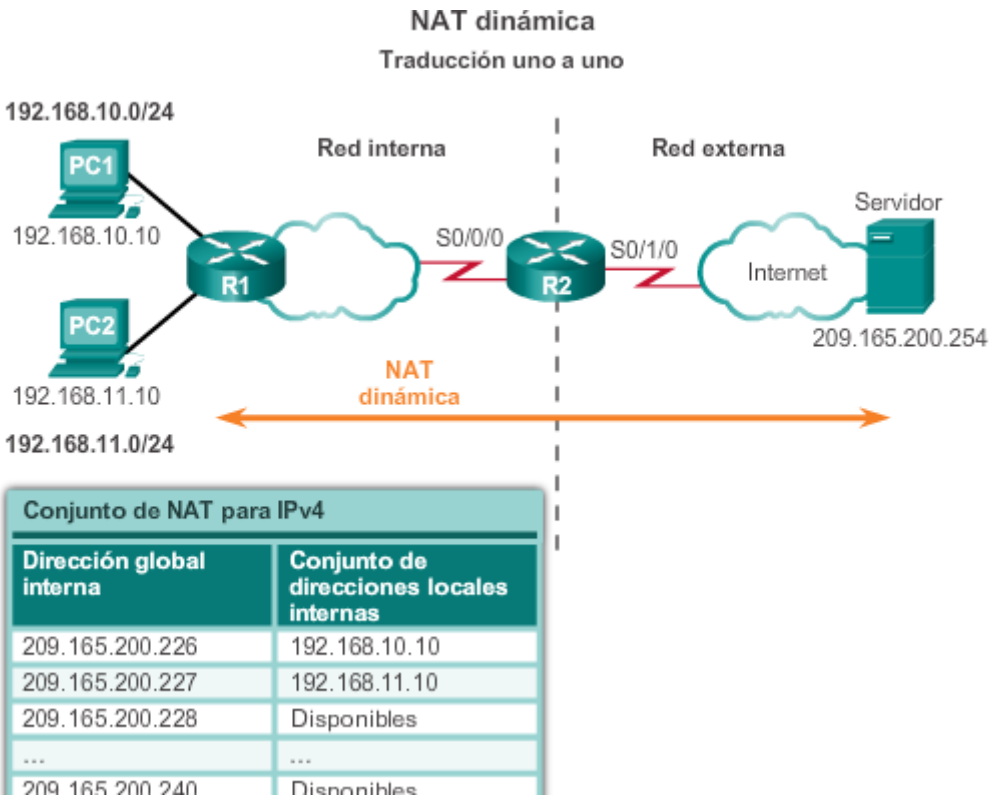
Mientras que la NAT estática proporciona una asignación permanente entre una dirección local interna y una dirección global interna, la NAT dinámica permite la asignación automática de direcciones locales internas a direcciones globales internas. Por lo general, estas direcciones globales internas son direcciones IPv4 públicas. La NAT dinámica utiliza un grupo o un conjunto de direcciones IPv4 públicas para la traducción.

Al igual que la NAT estática, la NAT dinámica requiere que se configuren las interfaces interna y externa que participan en la NAT. Sin embargo, mientras que la NAT estática crea una asignación permanente a una única dirección, la NAT dinámica utiliza un conjunto de direcciones.

Nota: la traducción entre direcciones IPv4 públicas y privadas es el uso más frecuente de NAT. No obstante, las traducciones de NAT se pueden realizar entre cualquier par de direcciones.

La topología de ejemplo que se muestra en la ilustración tiene una red interna que usa direcciones del espacio de direcciones privadas definido en RFC 1918. Hay dos LAN conectadas al router R1: 192.168.10.0/24 y 192.168.11.0/24. El router R2, es decir, el router de frontera, se configuró para NAT dinámica con un conjunto de direcciones IPv4 públicas de 209.165.200.226 a 209.165.200.240.

El conjunto de direcciones IPv4 públicas (conjunto de direcciones globales internas) se encuentra disponible para cualquier dispositivo en la red interna según el orden de llegada. Con la NAT dinámica, una única dirección interna se traduce a una única dirección externa. Con este tipo de traducción, debe haber suficientes direcciones en el conjunto para admitir a todos los dispositivos internos que necesiten acceso a la red externa al mismo tiempo. Si se utilizaron todas las direcciones del conjunto, los dispositivos deben esperar que haya una dirección disponible para poder acceder a la red externa.



Capítulo 5: Traducción de direcciones de red para IPv4 5.2.2.2 Configuración de NAT dinámica

En la figura 1, se muestran los pasos y los comandos utilizados para configurar la NAT dinámica.

Paso 1. Defina el conjunto de direcciones que se utilizará para la traducción con el comando **ip nat pool**. Por lo general, este conjunto es un grupo de direcciones públicas. Las direcciones se definen indicando la primera y la última dirección IP del conjunto. Las palabras clave **netmask**o **prefix-length** indican qué bits de la dirección pertenecen a la red y cuáles al host en el rango de direcciones.

Paso 2. Configure una ACL estándar para identificar (permitir) solo aquellas direcciones que se deben traducir. Una ACL demasiado permisiva puede generar resultados impredecibles. Recuerde que al final de cada ACL hay una instrucción implícita para **denegar todo**.

Paso 3. Conecte la ACL al conjunto. Para conectar la ACL al conjunto, se utiliza el comando **ip nat inside source list** *número-lista-acceso* **number pool** *nombre-conjunto*. El router utiliza esta configuración para determinar qué dirección (**pool**) recibe cada dispositivo (**list**).

Paso 4. Identifique qué interfaces son internas con respecto a NAT; es decir, cualquier interfaz que se conecte a la red interna.

Paso 5. Identifique qué interfaces son externas con respecto a NAT; es decir, cualquier interfaz que se conecte a la red externa.

En la figura 2, se muestra una topología y una configuración de ejemplo. Esta configuración permite la traducción para todos los hosts en la red 192.168.0.0/16, que incluye las LAN 192.168.10.0 y 192.168.11.0, cuando generan tráfico que ingresa por S0/0/0 y sale por S0/1/0.

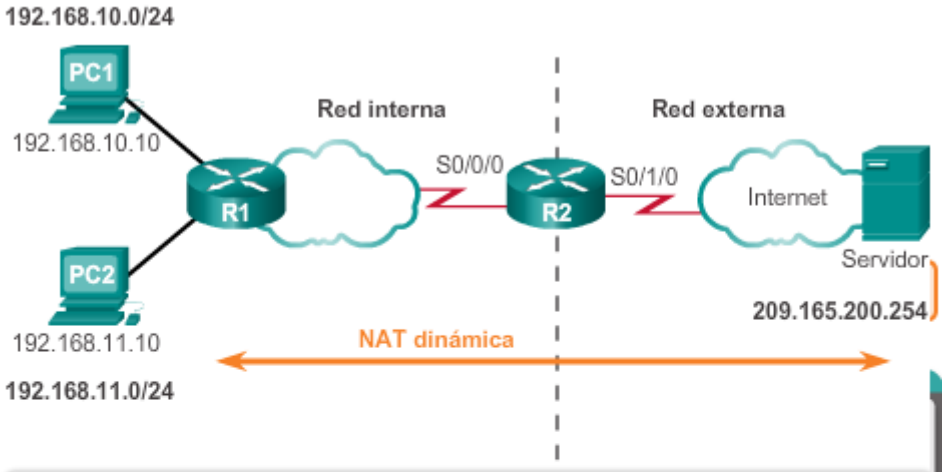
Estos hosts se traducen a una dirección disponible del conjunto en el rango de 209.165.200.226 a 209.165.200.240.

En la figura 3, se muestra la topología utilizada para la configuración del verificador de sintaxis. Utilice el verificador de sintaxis de la figura 4 para configurar la NAT dinámica en el R2.

Pasos de configuración de NAT dinámica

Pasos de configuración de NAT dinámica	
Paso 1	Definir el conjunto de direcciones globales que se debe usar para la traducción. **ip nat pool** *nombre primera-ip última-ip* {**netmask** *máscara-red*| **prefix-length** *longitud-prefijo*}
Paso 2	Configurar una lista de acceso estándar que permita las direcciones que se deben traducir. **access-list** *número-lista-acceso* **permit** *origen* [*wildcard-origen*]
Paso 3	Especificar la lista de acceso y el conjunto que se definieron en los pasos anteriores para establecer la traducción dinámica de origen. **ip nat inside source list** *número-lista-acceso* **pool** *nombre*
Paso 4	Identificar la interfaz interna. **interface** *tipo número* **ip nat inside**
Paso 5	Identificar la interfaz externa. **interface** *tipo número* **ip nat outside**

Configuración de NAT dinámica de ejemplo



Defines a pool of public IPv4 addresses under the pool name NAT-POOL1.

```
R2(config)# ip nat pool NAT-POOL1 209.165.200.226
209.165.200.240 netmask 255.255.255.224
```

Defines which addresses are eligible to be translated.

```
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

Binds NAT-POOL1 with ACL 1.

```
R2(config)# ip nat inside source list 1 pool NAT-POOL1
```

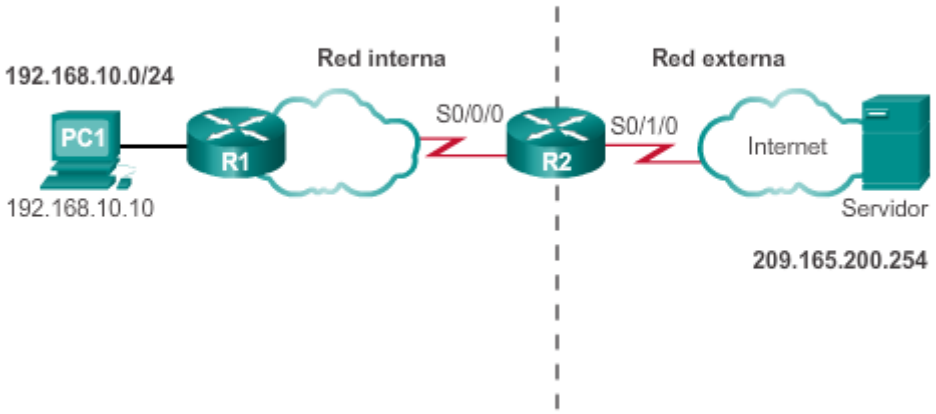
Identifies interface serial 0/0/0 as an inside NAT interface.

```
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside
```

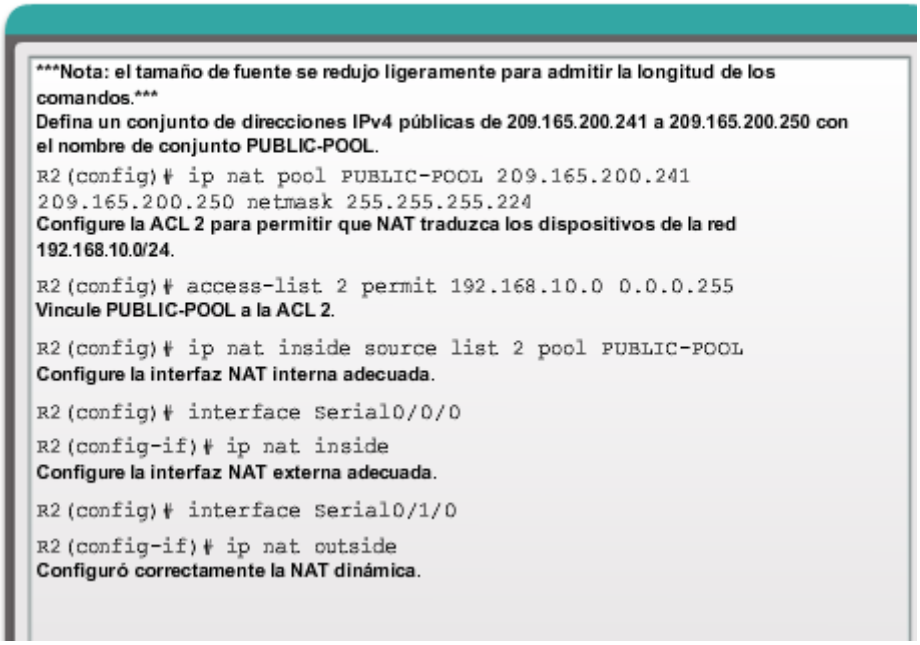
Identifies interface serial 0/1/0 as an outside NAT interface.

```
R2(config)# interface Serial0/1/0
R2(config-if)# ip nat outside
```

configurar la NAT dinámica



Configuración de NAT dinámicas



Capítulo 5: Traducción de direcciones de red para IPv4 5.2.2.3 Análisis de NAT dinámica

Con la configuración anterior, en las ilustraciones se muestra el proceso de traducción de NAT dinámica entre dos clientes y el servidor web:

En la figura 1, se muestra el flujo de tráfico desde adentro hacia fuera:

1. Los hosts con las direcciones IPv4 de origen (192.168.10.10 [PC1] y 192.168.11.10 [PC2]) envían paquetes para solicitar la conexión al servidor en la dirección IPv4 pública (209.165.200.254).

2. El R2 recibe el primer paquete del host 192.168.10.10. Debido a que este paquete se recibió en una interfaz configurada como interfaz NAT interna, el R2 verifica la configuración NAT para determinar si este paquete debe traducirse. Como la ACL permite este paquete, el R2 lo traduce. El R2 consulta su tabla de NAT. Debido a que no hay entrada de traducción para esta dirección IP, el R2 determina que la dirección de origen 192.168.10.10 se debe traducir de manera dinámica. El R2 selecciona una dirección global disponible del conjunto de direcciones dinámicas y crea una entrada de traducción, 209.165.200.226. La dirección IPv4 de origen inicial (192.168.10.10) es la dirección local interna, y la dirección traducida es la dirección global interna (209.165.200.226) en la tabla de NAT.

Para el segundo host, 192.168.11.10, el R2 repite el procedimiento, selecciona la siguiente dirección global disponible del conjunto de direcciones dinámicas y crea una segunda entrada de traducción, 209.165.200.227.

3. El R2 reemplaza la dirección de origen local interna de la PC1, 192.168.10.10, por la dirección global interna traducida 209.165.200.226 y reenvía el paquete. El mismo proceso se lleva a cabo para el paquete de la PC2 con la dirección traducida para esta computadora (209.165.200.227).

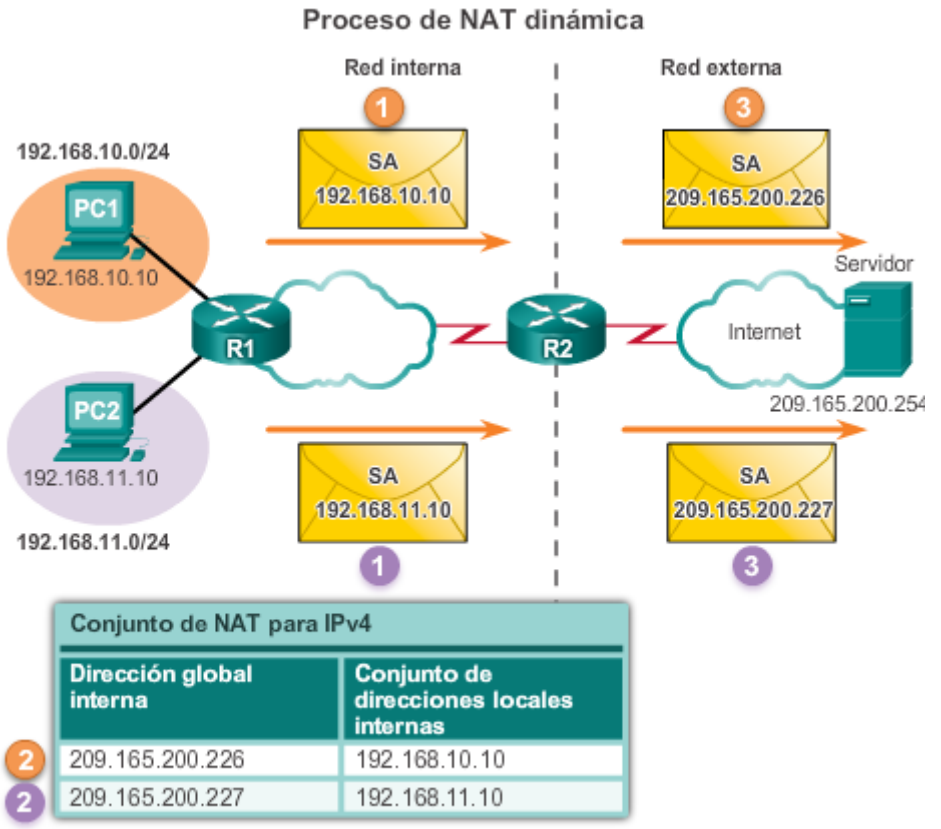
En la figura 2, se muestra el flujo de tráfico desde adentro hacia fuera:

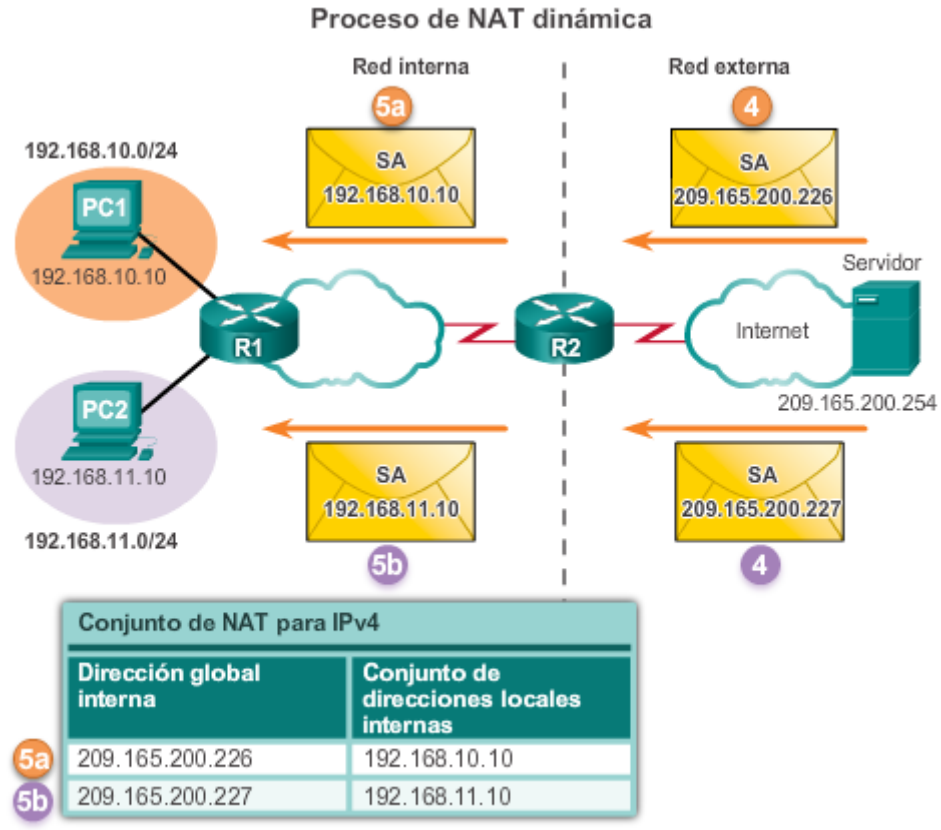
4. El servidor recibe el paquete de la PC1 y responde con la dirección IPv4 de destino 209.165.200.226. Cuando el servidor recibe el segundo paquete, responde a la PC2 con la dirección IPv4 de destino 209.165.200.227.

5a. Cuando el R2 recibe el paquete con la dirección IPv4 de destino 209.165.200.226, realiza una búsqueda en la tabla de NAT. Con la asignación de la tabla, el R2 vuelve a traducir la dirección a la dirección local interna (192.168.10.10) y reenvía el paquete hacia la PC1.

5b. Cuando el R2 recibe el paquete con la dirección IPv4 de destino 209.165.200.227, realiza una búsqueda en la tabla de NAT. Con la asignación de la tabla, el R2 vuelve a traducir la dirección a la dirección local interna (192.168.11.10) y reenvía el paquete hacia la PC2.

6. La PC1 en 192.168.10.10 y la PC2 en 192.168.11.10 reciben los paquetes y continúan la conversación. El router lleva a cabo los pasos 2 a 5 para cada paquete. (El paso 6 no aparece en las ilustraciones).


Proceso de NAT dinámica
Red interna
Red externa
192.168.10.0/24
PC1
192.168.10.10
SA
192.168.10.10
SA
209.165.200.226
Servidor
R1
R2
Internet
209.165.200.254
PC2
192.168.11.10
192.168.11.0/24
SA
192.168.11.10
SA
209.165.200.227
Conjunto de NAT para IPv4
Dirección global interna
Conjunto de direcciones locales internas
209.165.200.226
192.168.10.10
209.165.200.227
192.168.11.10


Proceso de NAT dinámica
Red interna
Red externa
192.168.10.0/24
PC1
192.168.10.10
SA
192.168.10.10
SA
209.165.200.226
Servidor
R1
R2
Internet
209.165.200.254
PC2
192.168.11.10
192.168.11.0/24
SA
192.168.11.10
SA
209.165.200.227
Conjunto de NAT para IPv4
Dirección global interna
Conjunto de direcciones locales internas
209.165.200.226
192.168.10.10
209.165.200.227
192.168.11.10

El resultado del comando **show ip nat translations** que aparece en la figura 1 muestra los detalles de las dos asignaciones de NAT anteriores. El comando muestra todas las traducciones estáticas que se configuraron y todas las traducciones dinámicas que se crearon a causa del tráfico.

Si se agrega la palabra clave **verbose**, se muestra información adicional acerca de cada traducción, incluido el tiempo transcurrido desde que se creó y se utilizó la entrada.

De manera predeterminada, a las entradas de traducción se les agota el tiempo de espera después de 24 horas, a menos que se vuelvan a configurar los temporizadores con el comando **ip nat translation timeout** *segundos-tiempo-espera*en el modo de configuración global.

Para borrar las entradas dinámicas antes de que se agote el tiempo de espera, utilice el comando **clear ip nat translation**en el modo de configuración global (figura 2). Es útil borrar las entradas dinámicas al probar la configuración NAT. Como se muestra en la tabla, este comando se puede utilizar con palabras clave y variables para controlar qué entradas se deben borrar. Se pueden borrar entradas específicas para evitar interrumpir las sesiones activas. Utilice el comando de configuración global **clear ip nat translation *** para borrar todas las traducciones de la tabla.

Nota: solo se borran de la tabla las traducciones dinámicas. Las traducciones estáticas no pueden borrarse de la tabla de traducción.

En la figura 3, el comando **show ip nat statistics** muestra la información sobre la cantidad total de traducciones activas, los parámetros de configuración NAT, la cantidad de direcciones en el conjunto y la cantidad de direcciones que se asignaron.

También puede utilizar el comando **show running-config** y buscar los comandos de NAT, ACL, interfaz o conjunto con los valores requeridos. Examínelos detenidamente y corrija cualquier error que detecte.

Verificación de NAT dinámica con `show ip nat translations`

```
R2# show ip nat translations
Pro Inside global     Inside local  Outside local Outside global
--- 209.165.200.226   192.168.10.10 ---           ---
--- 209.165.200.227   192.168.11.10 ---           ---
R2#
R2# show ip nat translations verbose
Pro Inside global     Inside local  Outside local Outside global
--- 209.165.200.226   192.168.10.10 ---           ---
    create 00:17:25, use 00:01:54 timeout:86400000, left
23:58:05, Map-Id(In): 1,
    flags:
none, use_count: 0, entry-id: 32, lc_entries: 0
--- 209.165.200.227    192.168.11.10      ---     ---
    create 00:17:22, use 00:01:51 timeout:86400000, left
23:58:08, Map-Id(In): 1,
    flags:
none, use_count: 0, entry-id: 34, lc_entries: 0
R2#
```

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 dinámica de direcciones de la tabla de traducción NAT.
clear ip nat translation inside *ip-global ip-local* [**outside** *ip-local ip-global*]	Elimina una entrada de traducción dinámica simple que contiene una traducción interna o una traducción interna y una externa.
clear ip nat translation *protocolo* **inside** *ip-global puerto-global ip-local puerto-local* [**outside** *ip-local puerto local ip-global puerto-global*]	Elimina una entrada de traducción dinámica extendida.

Verificación de NAT dinámica con **show ip nat statistics**

```
R2# clear ip nat statistics

PC1 and PC2 establish sessions with the server

R2# show ip nat statistics
Total active translations: 2 (0 static, 2 dynamic; 0 extended)
Peak translations: 6, occurred 00:27:07 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/1/0
Hits: 24  Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 4
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool NAT-POOL1 refcount 2
 pool NAT-POOL1: netmask 255.255.255.224
start 209.165.200.226 end 209.165.200.240
type generic, total addresses 15, allocated 2 (13%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
R2#
```

Capítulo 5: Traducción de direcciones de red para IPv4 5.2.2.5 Packet Tracer: configuración de NAT dinámica

En esta actividad de Packet Tracer, cumplirá los siguientes objetivos:

- Parte 1: configurar NAT dinámica
- Paso 2: verificar la implementación de NAT

Packet Tracer: configuración de NAT dinámica (instrucciones)

Packet Tracer: configuración de NAT dinámica (PKA)

Capítulo 5: Traducción de direcciones de red para IPv4 5.2.2.6 Práctica de laboratorio: configuración de NAT dinámica y estática

En esta práctica de laboratorio, cumplirá los siguientes objetivos:

- Parte 1: armar la red y verificar la conectividad
- Parte 2: configurar y verificar la NAT estática

- Parte 3: configurar y verificar la NAT dinámica

Práctica de laboratorio: configuración de NAT dinámica y estática

Capítulo 5: Traducción de direcciones de red para IPv4 5.2.3.1 Configuración de PAT: conjunto de direcciones

PAT (también denominada “NAT con sobrecarga”) conserva las direcciones del conjunto de direcciones globales internas al permitir que el router use una dirección global interna para muchas direcciones locales internas. En otras palabras, se puede utilizar una única dirección IPv4 pública para cientos, incluso miles de direcciones IPv4 privadas internas. Cuando se configura este tipo de traducción, el router mantiene suficiente información acerca de los protocolos de nivel superior, de los números de puerto TCP o UDP, por ejemplo, para volver a traducir la dirección global interna a la dirección local interna correcta. Cuando se asignan varias direcciones locales internas a una dirección global interna, los números de puerto TCP o UDP de cada host interno distinguen entre las direcciones locales.

Nota: la cantidad total de direcciones internas que se pueden traducir a una dirección externa teóricamente podría ser de hasta 65 536 por dirección IP. Sin embargo, la cantidad de direcciones internas a las que se puede asignar una única dirección IP es aproximadamente 4000.

Existen dos formas de configurar PAT, según cómo el ISP asigna las direcciones IPv4 públicas. En primer lugar, el ISP asigna más de una dirección IPv4 pública a la organización y, en segundo lugar, asigna una única dirección IPv4 pública que se requiere para que la organización se conecte al ISP.

Configuración de PAT para un conjunto de direcciones IP públicas

Si se emitió más de una dirección IPv4 pública para un sitio, estas direcciones pueden ser parte de un conjunto utilizado por PAT. Esto es similar a la NAT dinámica, con la excepción de que no existen suficientes direcciones públicas para realizar una asignación uno a uno entre direcciones internas y externas. Una gran cantidad de dispositivos comparte el pequeño conjunto de direcciones.

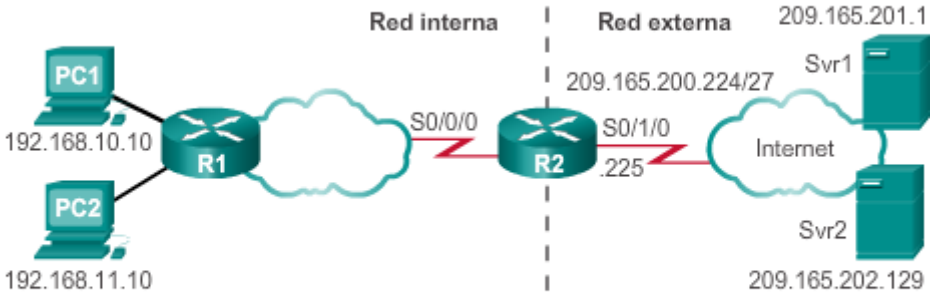
En la figura 1, se muestran los pasos para configurar PAT a fin de que utilice un conjunto de direcciones. La diferencia principal entre esta configuración y la configuración para NAT dinámica uno a uno es que se utiliza la palabra clave**overload**. La palabra clave **overload**habilita PAT.

La configuración de ejemplo que se muestra en la figura 2 establece la traducción de sobrecarga para el conjunto de NAT denominado NAT-POOL2. NAT-POOL2 contiene las direcciones de 209.165.200.226 a 209.165.200.240. Los hosts en la red 192.168.0.0/16 están sujetos a traducción. La interfaz S0/0/0 se identifica como interfaz interna, y la interfaz S0/1/0 se identifica como interfaz externa.

Utilice el verificador de sintaxis de la figura 3 para configurar PAT con un conjunto de direcciones en el R2.

Paso 1	Definir el conjunto de direcciones globales que se debe usar para la traducción de sobrecarga. **ip nat pool** *nombre primera-ip última-ip* {**netmask** *máscara-red* | **prefix-length** *longitud-prefijo*}
Paso 2	Definir una lista de acceso estándar que permita las direcciones que se deben traducir. **access-list** *número-lista-acceso* **permit** *origen* [*wildcard-origen*]
Paso 3	Especificar la lista de acceso y el conjunto que se definieron en los pasos anteriores para establecer la traducción de sobrecarga. **ip nat inside source list** *número-lista-acceso* **pool** *nombre* **overload**
Paso 4	Identificar la interfaz interna. **interface** *tipo número* **ip nat inside**
Paso 5	Identificar la interfaz externa. **interface** *tipo número* **ip nat outside**

Ejemplo de PAT con conjunto de direcciones



Defina un conjunto de direcciones IPv4 públicas con el nombre de conjunto NAT-POOL2.

```
R2(config)# ip nat pool NAT-POOL2 209.165.200.226
209.165.200.240 netmask 255.255.255.224
```

Defina las direcciones que se pueden traducir.

```
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

Vincule NAT-POOL2 a la ACL 1.

```
R2(config)# ip nat inside source list 1 pool NAT-POOL2
overload
```

Identifique la interfaz serial 0/0/0 como interfaz NAT interna.

Identifique la interfaz serial 0/0/0 como interfaz NAT interna.

```
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside
```

Identifique la interfaz serial 0/1/0 como interfaz NAT externa.

```
R2(config)# interface Serial0/1/0
R2(config-if)# ip nat outside
```

Capítulo 5: Traducción de direcciones de red para IPv4 5.2.3.2 Configuración de PAT: dirección única

Configuración de PAT para una única dirección IPv4 pública

En la figura 1, se muestra la topología de una implementación de PAT para la traducción de una única dirección IPv4 pública. En el ejemplo, todos los hosts de la red 192.168.0.0/16 (que coincide con la ACL 1) que envían tráfico a Internet a través del router R2 se traducen a la dirección IPv4 209.165.200.225 (dirección IPv4 de la interfaz S0/1/0). Los flujos de tráfico se identifican por los números de puerto en la tabla de NAT, ya que se utilizó la palabra clave **overload**.

En la figura 2, se muestran los pasos que se deben seguir para configurar PAT con una única dirección IPv4. Si solo hay una única dirección IPv4 pública disponible, la configuración de sobrecarga generalmente asigna la dirección pública a la interfaz externa que se conecta al ISP. Todas las direcciones internas se traducen a la única dirección IPv4 cuando salen de la interfaz externa.

Paso 1. Defina una ACL para permitir que se traduzca el tráfico.

Paso 2. Configure la traducción de origen con las palabras clave **interface** y**overload**. La palabra clave **interface**identifica la dirección IP de la interfaz que se debe utilizar en la traducción de las direcciones internas. La palabra clave**overload** le indica al router que realice un seguimiento de los números de puerto con cada entrada de NAT.

Paso 3. Identifique cuáles son las interfaces internas con respecto a NAT. Es decir, toda interfaz que se conecte a la red interna.

Paso 4. Identifique cuál es la interfaz externa con respecto a NAT. Esta debe ser la misma interfaz identificada en la instrucción de la traducción de origen del paso 2.

La configuración es similar a la de NAT dinámica, excepto que, en lugar de un conjunto de direcciones, se utiliza la palabra clave **interface** para identificar la dirección IPv4 externa. Por lo tanto, no se define ningún pool de NAT.

Utilice el verificador de sintaxis de la figura 3 para configurar PAT con una única dirección en el R2.

PAT con dirección única

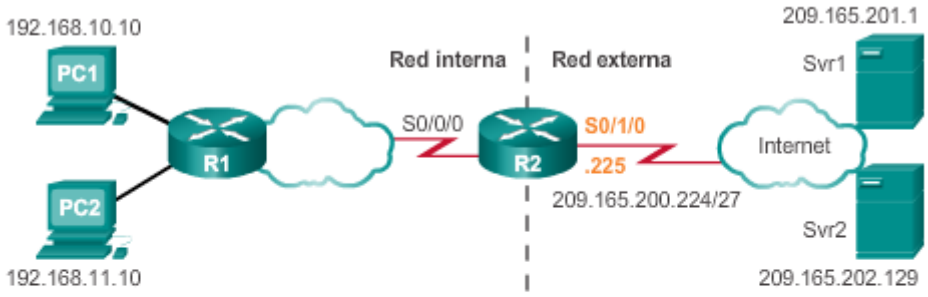
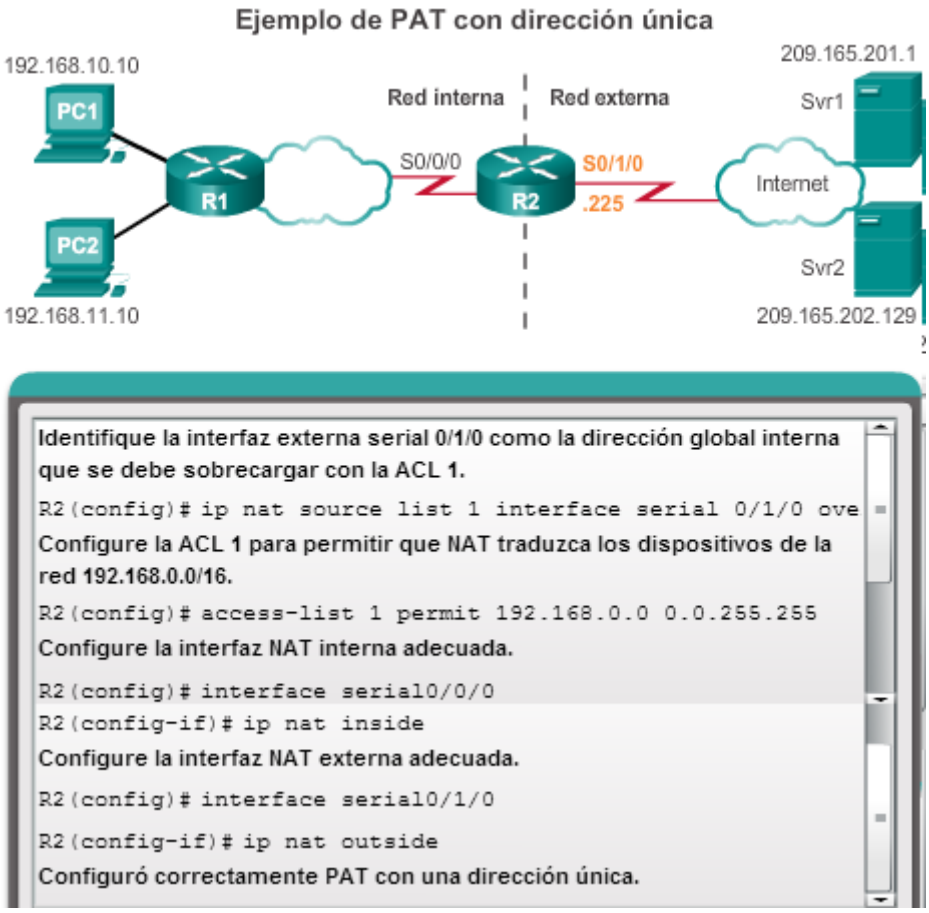


Tabla NAT

Dirección global interna	Dirección local interna	Dirección local externa	Dirección global externa
209.165.200.225:1444	192.168.10.10:1444	209.165.201.1:80	209.165.201.1:80
209.165.200.225:1445	192.168.10.11:1444	209.165.202.129:80	209.165.202.129:80

Pasos de configuración de PAT

Paso 1	Definir una lista de acceso estándar que permita las direcciones que se deben traducir. **access-list** *número-lista-acceso* **permit** *origen* [*wildcard-origen*]
Paso 2	Especificar las opciones de ACL, interfaz de salida y sobrecarga para establecer la traducción dinámica de origen. **ip nat inside source list** *número-lista-acceso* **interface** *tipo número* **overload**
Paso 3	Identifique la interfaz interna. **interface** *type number* **ip nat inside**
Paso 4	Identifique la interfaz externa. **interface** *type number* **ip nat outside**



Capítulo 5: Traducción de direcciones de red para IPv4 5.2.3.3 Análisis de PAT

El proceso de NAT con sobrecarga es el mismo, ya sea que se utilice un conjunto de direcciones o una única dirección. En el ejemplo anterior de PAT, la PC1 desea comunicarse con el servidor web Svr1 por medio de una única dirección IPv4 pública. Al mismo tiempo, otro cliente, la PC2, desea establecer una sesión similar con el servidor web Svr2. Tanto la PC1 como la PC2 se configuraron con direcciones IPv4 privadas, con el R2 habilitado para PAT.

Proceso de la computadora al servidor

1. En la figura 1, se muestra que la PC1 y la PC2 envían paquetes a los servidores Svr1 y Svr2, respectivamente. La PC1 tiene la dirección IPv4 de origen 192.168.10.10 y utiliza el puerto de origen TCP 1444. La PC2 tiene la dirección IPv4 de origen 192.168.10.11 y, por casualidad, se le asigna el mismo puerto de origen 1444.

2. El paquete de la PC1 llega primero al R2. Mediante el uso de PAT, el R2 modifica la dirección IPv4 de origen a 209.165.200.225 (dirección global interna). En la tabla de NAT, no hay ningún otro dispositivo que use el puerto 1444, de modo que PAT mantiene el mismo número de puerto. El paquete luego se reenvía hacia el Svr1 en 209.165.201.1.

3. A continuación, llega el paquete de la PC2 al R2. PAT está configurada para utilizar una única dirección IPv4 global interna para todas las traducciones, 209.165.200.225. Al igual que con el proceso de traducción para la PC1, PAT cambia la dirección IPv4 de origen de la PC2 a la dirección global interna 209.165.200.225. Sin embargo, la PC2 tiene el mismo número de

puerto de origen que una entrada actual de PAT, la traducción para la PC1. PAT aumenta el número de puerto de origen hasta que sea un valor único en su tabla. En este caso, la entrada del puerto de origen en la tabla de NAT y el paquete de la PC2 reciben el número 1445.

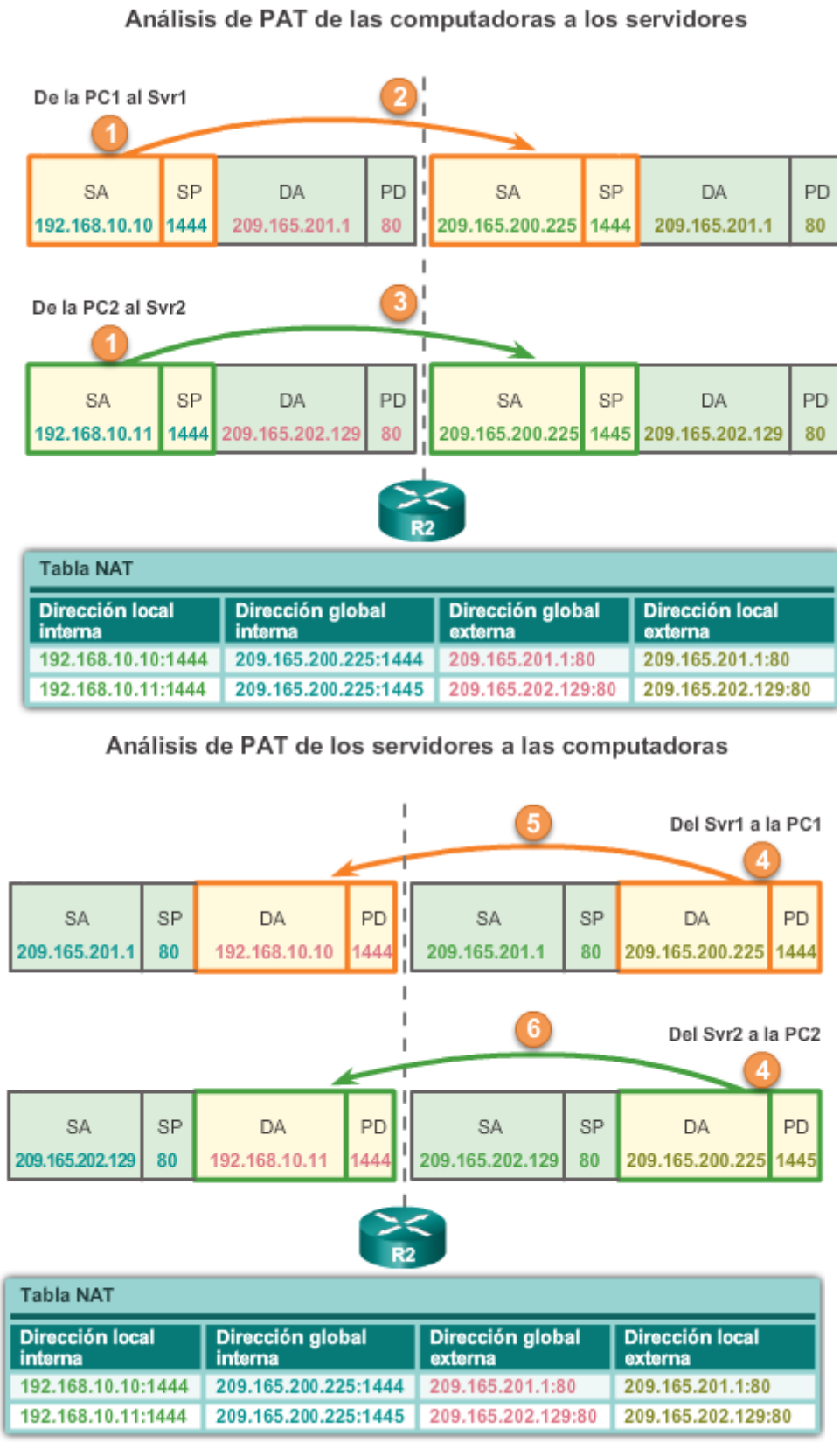
Si bien la PC1 y la PC2 usan la misma dirección traducida, la dirección global interna 209.165.200.225, y el mismo número de puerto de origen 1444, el número de puerto modificado para la PC2 (1445) hace que cada entrada en la tabla de NAT sea única. Esto se torna evidente cuando los paquetes se devuelven desde los servidores hacia los clientes.

Proceso del servidor a la computadora

4. Como se muestra en la figura 2, en un intercambio típico entre cliente y servidor, los servidores Svr1 y Svr2 responden a las solicitudes recibidas de la PC1 y la PC2, respectivamente. Los servidores usan el puerto de origen del paquete recibido como puerto de destino y la dirección de origen como dirección de destino para el tráfico de retorno. Al parecer, los servidores se comunican con el mismo host en 209.165.200.225, pero no es así.

5. A medida que llegan los paquetes, el R2 ubica una única entrada en su tabla de NAT mediante la dirección de destino y el puerto de destino de cada paquete. En el caso del paquete del Svr1, la dirección IPv4 de destino 209.165.200.225 tiene varias entradas, pero solo una con el puerto de destino 1444. Mediante la entrada de su tabla, el R2 cambia la dirección IPv4 de destino del paquete a 192.168.10.10, sin necesidad de modificar el puerto de destino. Luego, el paquete se reenvía hacia la PC1.

6. Cuando llega el paquete del Svr2, el R2 realiza una traducción similar. La dirección IPv4 de destino 209.165.200.225 vuelve a aparecer en varias entradas. Sin embargo, con el puerto de destino 1445, el R2 puede identificar una única entrada de traducción. La dirección IPv4 de destino se modifica a 192.168.10.11. En este caso, el puerto de destino también se debe volver a modificar a su valor original de 1444, que está almacenado en la tabla de NAT. Luego, el paquete se reenvía hacia la PC2.

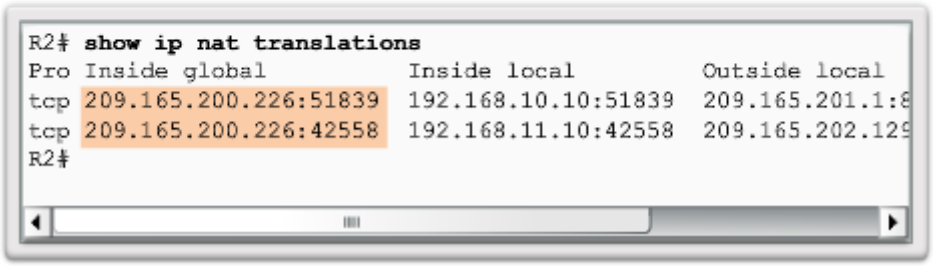

Análisis de PAT de las computadoras a los servidores
De la PC1 al Svr1
1
2
SA
192.168.10.10
SP
1444
DA
209.165.201.1
PD
80
SA
209.165.200.225
SP
1444
DA
209.165.201.1
PD
80
De la PC2 al Svr2
1
3
SA
192.168.10.11
SP
1444
DA
209.165.202.129
PD
80
SA
209.165.200.225
SP
1445
DA
209.165.202.129
PD
80
R2
Tabla NAT
Dirección local interna
Dirección global interna
Dirección global externa
Dirección local externa
192.168.10.10:1444
209.165.200.225:1444
209.165.201.1:80
209.165.201.1:80
192.168.10.11:1444
209.165.200.225:1445
209.165.202.129:80
209.165.202.129:80
Análisis de PAT de los servidores a las computadoras
5
Del Svr1 a la PC1
4
SA
209.165.201.1
SP
80
DA
192.168.10.10
PD
1444
SA
209.165.201.1
SP
80
DA
209.165.200.225
PD
1444
6
Del Svr2 a la PC2
4
SA
209.165.202.129
SP
80
DA
192.168.10.11
PD
1444
SA
209.165.202.129
SP
80
DA
209.165.200.225
PD
1445
R2
Tabla NAT
Dirección local interna
Dirección global interna
Dirección global externa
Dirección local externa
192.168.10.10:1444
209.165.200.225:1444
209.165.201.1:80
209.165.201.1:80
192.168.10.11:1444
209.165.200.225:1445
209.165.202.129:80
209.165.202.129:80

El router R2 se configuró para proporcionar PAT a los clientes de 192.168.0.0/16. Cuando los hosts internos salen del router R2 a Internet, se traducen a una dirección IPv4 del conjunto de PAT con un único número de puerto de origen.

Para verificar PAT, se usan los mismos comandos que se usan para verificar la NAT estática y dinámica, como se muestra en la figura 1. El comando **show ip nat translations** muestra las traducciones de dos hosts distintos a servidores web distintos. Observe que se asigna la misma dirección IPv4 209.165.200.226 (dirección global interna) a dos hosts internos distintos. Los números de puerto de origen en la tabla de NAT distinguen las dos transacciones.

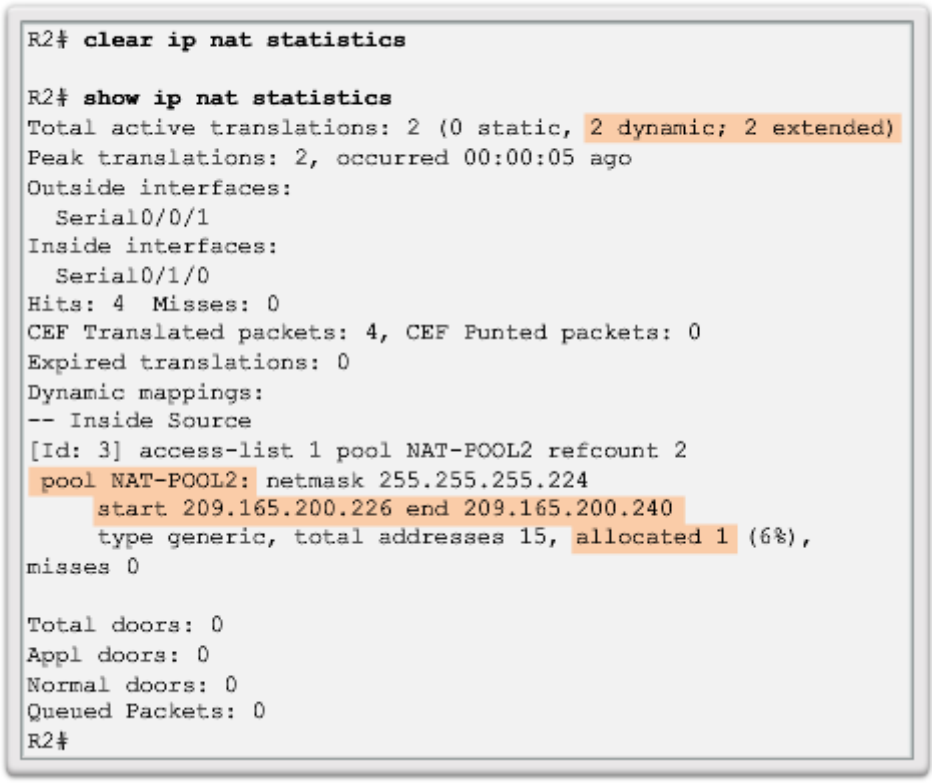
Como se muestra en la figura 2, el comando **show ip nat statistics**verifica que NAT-POOL2 haya asignado una única dirección para ambas traducciones. El resultado incluye información sobre la cantidad y el tipo de traducciones activas, los parámetros de configuración NAT, la cantidad de direcciones en el conjunto y la cantidad que se asignó.

Verificación de las traducciones PAT



```
R2# show ip nat translations
Pro Inside global          Inside local         Outside local
tcp 209.165.200.226:51839  192.168.10.10:51839  209.165.201.1:8
tcp 209.165.200.226:42558  192.168.11.10:42558  209.165.202.129
R2#
```

Verificación de las estadísticas de PAT



```
R2# clear ip nat statistics

R2# show ip nat statistics
Total active translations: 2 (0 static, 2 dynamic; 2 extended)
Peak translations: 2, occurred 00:00:05 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/1/0
Hits: 4  Misses: 0
CEF Translated packets: 4, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 3] access-list 1 pool NAT-POOL2 refcount 2
 pool NAT-POOL2: netmask 255.255.255.224
     start 209.165.200.226 end 209.165.200.240
     type generic, total addresses 15, allocated 1 (6%),
misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
R2#
```

Capítulo 5: Traducción de direcciones de red para IPv4 5.2.3.6 Packet Tracer: implementación de NAT estática y dinámica

En esta actividad de Packet Tracer, cumplirá los siguientes objetivos:

- Parte 1: configurar NAT dinámica con PAT
- Parte 2: configurar NAT estática
- Paso 3: verificar la implementación de NAT

Packet Tracer: implementación de NAT estática y dinámica (instrucciones)

Packet Tracer: implementación de NAT estática y dinámica (PKA)

Capítulo 5: Traducción de direcciones de red para IPv4 5.2.3.7 Práctica de laboratorio:

Configuración de la traducción de la dirección del puerto (PAT)

En esta práctica de laboratorio, cumplirá los siguientes objetivos:

- Parte 1: armar la red y verificar la conectividad
- Parte 2: configurar y verificar un conjunto de NAT con sobrecarga
- Parte 3: configurar y verificar PAT

Práctica de laboratorio: Configuración de la traducción de la dirección del puerto (PAT)

Capítulo 5: Traducción de direcciones de red para IPv4 5.2.4.1 Reenvío de puertos

El reenvío de puertos (a veces, denominado “tunneling”) consiste en reenviar el tráfico dirigido a un puerto de red específico desde un nodo de red hacia otro. Esta técnica permite que un usuario externo alcance un puerto en una dirección IPv4 privada (dentro de una LAN) desde el exterior a través de un router con NAT habilitada.

En general, las operaciones y los programas peer-to-peer para compartir archivos, como las aplicaciones de servidores web y los FTP salientes, requieren que los puertos de router se reenvíen o se abran para permitir que estas aplicaciones funcionen, como se muestra en la figura 1. Debido a que NAT oculta las direcciones internas, la comunicación peer-to-peer solo funciona desde adentro hacia fuera donde NAT puede asignar las solicitudes salientes a las respuestas entrantes.

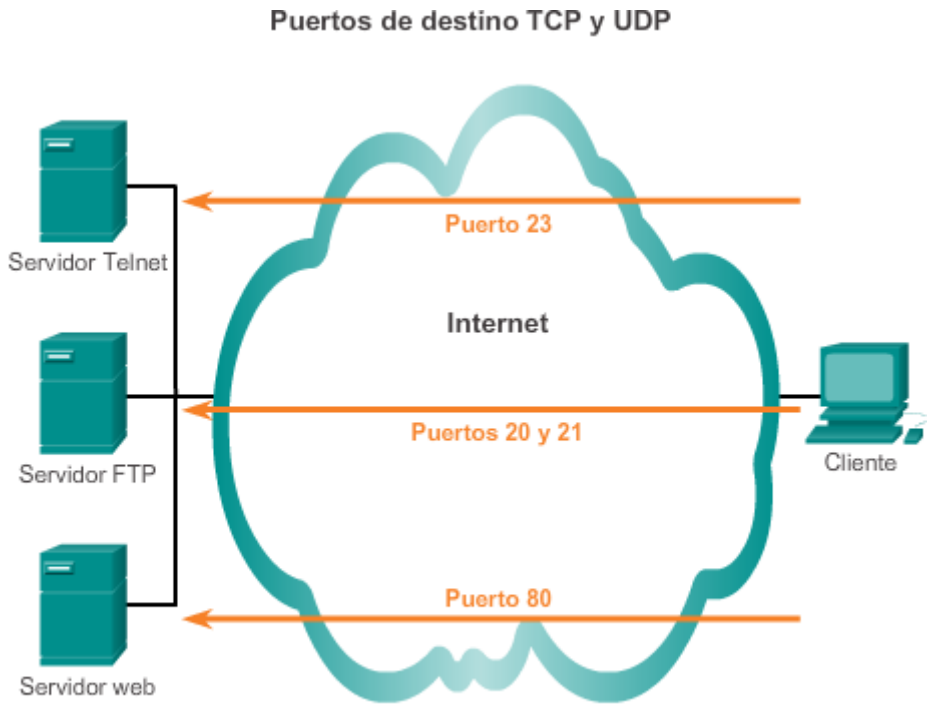
El problema es que NAT no permite las solicitudes iniciadas desde el exterior. Esta situación se puede resolver de forma manual. El reenvío de puertos se puede configurar para identificar los puertos específicos que se pueden reenviar a los hosts internos.

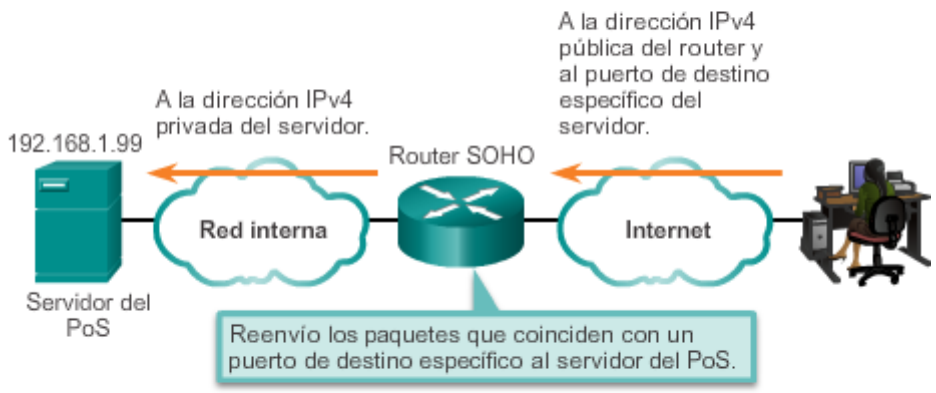
Recuerde que las aplicaciones de software de Internet interactúan con los puertos de usuario que necesitan estar abiertos o disponibles para dichas aplicaciones. Las distintas aplicaciones usan puertos diferentes. Esto hace que las aplicaciones y los routers identifiquen los servicios de red de manera predecible. Por ejemplo, HTTP funciona a través del puerto bien conocido 80. Cuando alguien introduce la dirección **http://cisco.com**, el explorador muestra el sitio web de Cisco Systems, Inc. Tenga en cuenta que no es necesario especificar el número de puerto HTTP para la solicitud de página, ya que la aplicación asume que se trata del puerto 80.

Si se requiere un número de puerto diferente, se puede agregar al URL separado por dos puntos (:). Por ejemplo, si el servidor web escuchara en el puerto 8080, el usuario escribiría**http://www.ejemplo.com:8080**.

El reenvío de puertos permite que los usuarios en Internet accedan a los servidores internos mediante el uso de la dirección de puerto de WAN del router y del número de puerto externo que coincida. En general, los servidores internos se configuran con direcciones IPv4 privadas definidas en RFC 1918. Cuando se envía una solicitud a la dirección IPv4 del puerto de WAN a través de Internet, el router reenvía la solicitud al servidor correspondiente en la LAN. Por motivos de seguridad, los routers de banda ancha no permiten que se reenvíe ninguna solicitud de redes externas a un host interno de manera predeterminada.

En la figura 2, se muestra al propietario de una pequeña empresa que utiliza un servidor del punto de venta (PoS) para hacer un seguimiento de las ventas y los inventarios en la tienda. Se puede acceder al servidor desde la tienda pero, debido a que tiene una dirección IPv4 privada, no es posible acceder a este de manera pública desde Internet. Habilitar el router local para el reenvío de puertos permitiría que el propietario acceda al servidor del punto de venta en cualquier lugar desde Internet. El reenvío de puertos en el router se configura con el número de puerto de destino y la dirección IPv4 privada del servidor del punto de venta. Para acceder al servidor, el software de cliente utilizaría la dirección IPv4 pública del router y el puerto de destino del servidor.





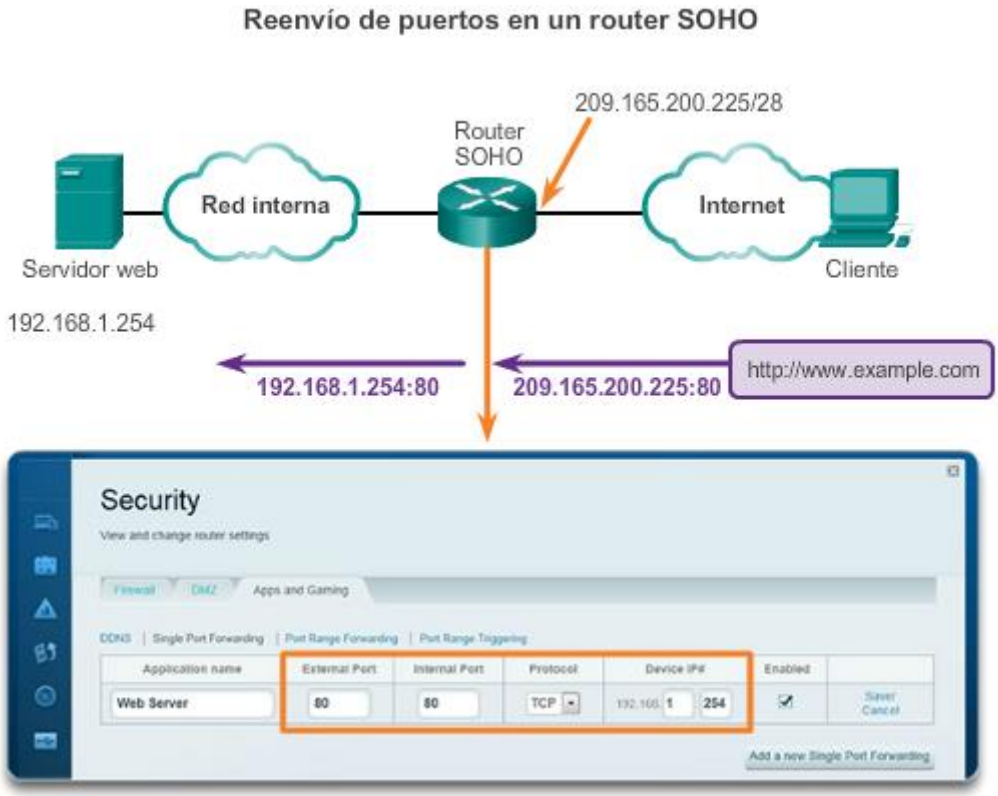
Capítulo 5: Traducción de direcciones de red para IPv4 5.2.4.2 Ejemplo de SOHO

En la ilustración, se muestra la ventana de configuración Single Port Forwarding (Reenvío de puerto único) de un router SOHO Linksys EA6500. De manera predeterminada, el reenvío de puertos no está habilitado en el router.

Si se especifica la dirección local interna a la cual se deben reenviar las solicitudes, es posible habilitar el reenvío de puertos para las aplicaciones. En la ilustración, las solicitudes de servicio HTTP que llegan a este router Linksys se reenvían al servidor web con la dirección local interna 192.168.1.254. Si la dirección IPv4 WAN externa del router SOHO es 209.165.200.225, el usuario externo puede introducir **http://www.ejemplo.com**, y el router Linksys redirige la solicitud HTTP al servidor web interno en la dirección IPv4 192.168.1.254, con el número de puerto predeterminado 80.

Se puede especificar un puerto distinto al puerto predeterminado 80. Sin embargo, el usuario externo tendría que saber el número de puerto específico que debe utilizar. Para especificar un puerto diferente, se modifica el valor del campo External Port (Puerto externo) en la ventana Single Port Forwarding (Reenvío de puerto único).

El enfoque adoptado para configurar el reenvío de puertos depende de la marca y el modelo del router de banda ancha en la red. No obstante, hay algunos pasos genéricos que se deben seguir. Si las instrucciones que suministra el ISP o las que vienen con el router no proporcionan una orientación adecuada, en el sitio webhttp://www.portforward.com se ofrecen guías para varios routers de banda ancha. Puede seguir las instrucciones para agregar o eliminar puertos según sea necesario para satisfacer las necesidades de todas las aplicaciones que desee permitir o denegar.



Capítulo 5: Traducción de direcciones de red para IPv4 5.2.4.3 Configuración de reenvío de puertos con IOS

Los comandos de IOS que se usan para implementar el reenvío de puertos son similares a los que se usan para configurar la NAT estática. Básicamente, el reenvío de puertos es una traducción de NAT estática con un número de puerto TCP o UDP específico.

En la figura 1, se muestra el comando de NAT estática que se usa para configurar el reenvío de puertos con IOS.

En la figura 2, se muestra un ejemplo de configuración del reenvío de puertos con comandos de IOS en el router R2. La dirección 192.168.10.254 es la dirección IPv4 local interna del servidor web que escucha en el puerto 80. Los usuarios acceden a este servidor web interno con la dirección IP global 209.165.200.225, una dirección IPv4 pública globalmente única. En este caso, es la dirección de la interfaz Serial 0/1/0 del R2. El puerto global se configura como 8080. Este es el puerto de destino que se utiliza junto con la dirección IPv4 global 209.165.200.225 para acceder al servidor web interno. Observe los siguientes parámetros de comando dentro de la configuración NAT:

- *ip-local* = 192.168.10.254
- *puerto-local* = 80
- *ip-global* = 209.165.200.225
- *puerto-global* = 8080

Cuando no se utiliza un número de puerto bien conocido, el cliente debe especificar el número de puerto de la aplicación.

Al igual que otros tipos de NAT, el reenvío de puertos requiere que se configuren las interfaces NAT interna y externa.

Como en el caso de la NAT estática, se puede utilizar el comando **show ip nat translations** para verificar el reenvío de puertos, como se muestra en la figura 3.

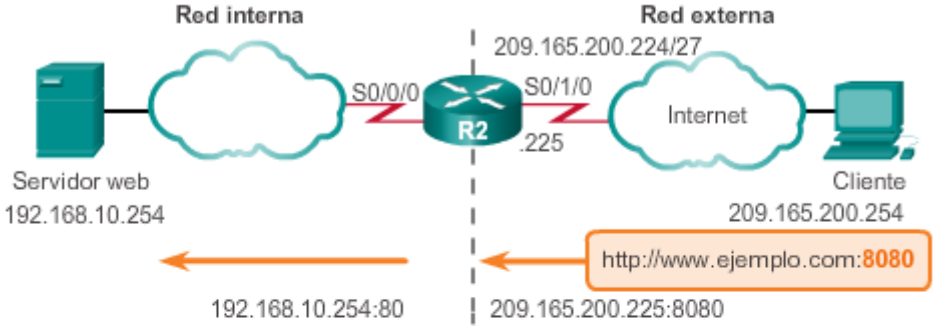
En el ejemplo, cuando el router recibe el paquete con la dirección IPv4 global interna 209.165.200.225 y un puerto TCP de destino 8080, el router realiza una búsqueda en la tabla de NAT con la dirección IPv4 de destino y el puerto de destino como claves. A continuación, el router traduce la dirección a la dirección local interna del host 192.168.10.254 y el puerto de destino 80. Luego, el R2 reenvía el paquete al servidor web. En el caso de los paquetes de retorno del servidor web al cliente, este proceso se invierte.

Reenvío de puertos con IOS

```
ip nat inside source {static {tcp | udp local-ip local-port
global-ip global-port} [extendable]
```

Parámetro	Descripción
tcp o **udp**	Indica si este es un número de puerto TCP o UDP.
ip-local	Esta es la dirección IPv4 asignada al host en la red interna, generalmente, del espacio de direcciones privadas definido en RFC 1918.
puerto-local	Establece el puerto local TCP/UDP en un rango de 1 a 65535. Este es el número de puerto en el que escucha el servidor.
ip-global	Esta es la dirección IPv4 globalmente única de un host interno. Esta es la dirección IP que utilizan los clientes externos para llegar al servidor interno.
puerto-global	Establece el puerto global TCP/UDP en un rango de 1 a 65535. Este es el número de puerto que utilizan los clientes externos para llegar al servidor interno.
extendable	La opción **extendable** se aplica de forma automática. La palabra clave **extendable** permite que el usuario configure varias traducciones estáticas ambiguas, es decir, traducciones con la misma dirección local o global. Permite que el router extienda la traducción a más de un puerto, en caso de ser necesario.

Ejemplo de reenvío de puertos con IOS



Establece la traducción estática entre una dirección local interna y un puerto local, y entre una dirección global interna y un puerto global.

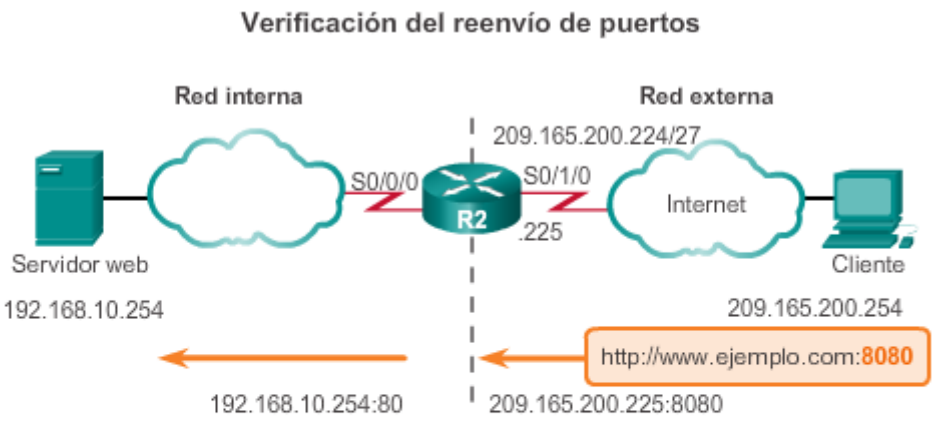
```
R2(config)# ip nat inside source static tcp 192.168.10.254 80
209.165.200.225 8080
```

Identifica la interfaz serial 0/0/0 como interfaz NAT interna.

```
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside
```

Identifica la interfaz serial 0/1/0 como interfaz NAT externa.

```
R2(config)# interface Serial0/1/0
R2(config-if)# ip nat outside
```




```
R2# show ip nat translations
Pro Inside global         Inside local       Outside local
tcp 209.165.200.225:8080 192.168.10.254:80  209.165.200.254:46
tcp 209.165.200.225:8080 192.168.10.254:80  ---
R2#
```

Capítulo 5: Traducción de direcciones de red para IPv4 5.2.4.4 Packet Tracer: configuración del reenvío de puertos en un router Linksys

Información básica/situación

Su amigo desea jugar un juego con usted en su servidor. Ambos están en sus respectivos hogares conectados a Internet. Debe configurar su router SOHO (oficinas pequeñas/domésticas) para reenviar solicitudes de HTTP a través del puerto a su servidor de modo que su amigo pueda acceder a la página web del juego.

Packet Tracer: configuración del reenvío de puertos en un router Linksys (instrucciones)

Packet Tracer: configuración del reenvío de puertos en un router Linksys (PKA)

Capítulo 5: Traducción de direcciones de red para IPv4 5.2.5.1 ¿NAT para IPv6?

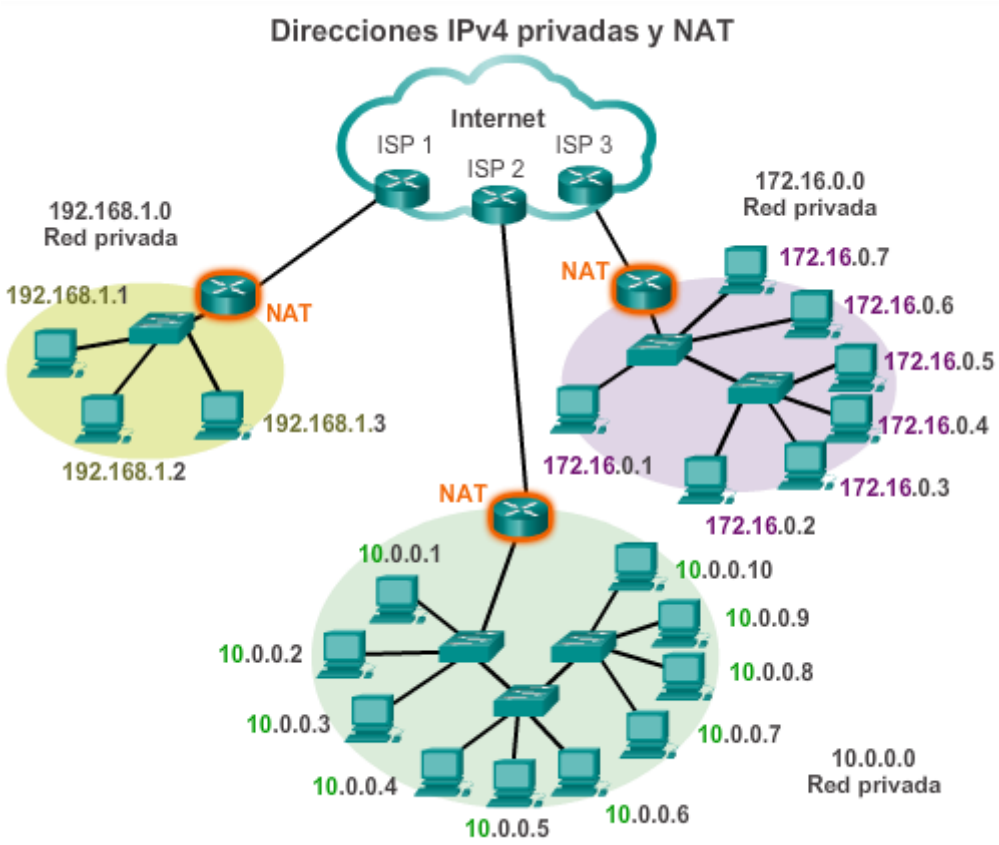
irecciones IPv4 es una prioridad para el IETF desde principios de la década de los noventa. La combinación de las direcciones IPv4 privadas definidas en RFC 1918 y de NAT cumple un papel decisivo para retrasar este agotamiento. NAT presenta desventajas considerables, y en enero de 2011, la IANA asignó sus últimas direcciones IPv4 a los RIR.

Uno de los beneficios de NAT para IPv4 que no fueron intencionales es que oculta la red privada de Internet pública, como se muestra en la ilustración. NAT tiene la ventaja de que ofrece un nivel de seguridad considerable al denegar el acceso de las computadoras que se encuentran en Internet pública a los hosts internos. Sin embargo, no debe considerarse como un sustituto de la seguridad de red adecuada, como la que proporciona un firewall.

En RFC 5902, el Consejo de Arquitectura de Internet (IAB) incluyó la siguiente cita sobre la traducción de direcciones de red IPv6:

“En general, se cree que una caja NAT proporciona un nivel de protección porque los hosts externos no pueden iniciar directamente una comunicación con los hosts detrás de una NAT. No obstante, no se deben confundir las cajas NAT con los firewalls. Como se analizó en la sección 2.2 de RFC4864, el acto de traducción en sí mismo no proporciona seguridad. La función de filtrado con estado puede proporcionar el mismo nivel de protección sin requerir una función de traducción”.

Con una dirección de 128 bits, IPv6 proporciona 340 sextillones de direcciones. Por lo tanto, el espacio de direcciones no es un problema. IPv6 se desarrolló con la intención de que la NAT para IPv4 con su traducción entre direcciones IPv4 públicas y privadas resulte innecesaria. Sin embargo, IPv6 implementa una forma de NAT. IPv6 incluye su propio espacio de direcciones IPv6 privadas y NAT, que se implementan de manera distinta de como se hace para IPv4.



Capítulo 5: Traducción de direcciones de red para IPv4 5.2.5.2 Direcciones IPv6 locales únicas

Las direcciones IPv6 locales únicas (ULA) se asemejan a las direcciones privadas en IPv4 definidas en RFC 1918, pero también existen diferencias considerables. El objetivo de las ULA es proporcionar espacio de direcciones IPv6 para las comunicaciones dentro de un sitio local, no tienen el propósito de proporcionar espacio adicional de direcciones IPv6 ni un nivel de seguridad.

Como se muestra en la ilustración, las ULA tienen el prefijo FC00::/7, lo que produce un rango de primer hexteto que va desde FC00 hasta FDFF. El bit siguiente se establece en 1 si el prefijo se asigna localmente. Es posible que en el futuro se pueda establecer en 0. Los 40 bits siguientes corresponden a una ID global seguida de una ID de subred de 16 bits. Estos primeros 64 bits se combinan para crear el prefijo de la ULA. Esto permite que los 64 bits restantes se utilicen para la ID de interfaz o, en términos de IPv4, la porción de host de la dirección.

Las direcciones locales únicas se definen en RFC 4193. Las ULA también se conocen como "direcciones IPv6 locales" (no se deben confundir con las direcciones IPv6 link-local) y tienen varias características, incluidas las siguientes:

- Permiten que los sitios se combinen o se interconecten de manera privada, sin generar conflictos entre direcciones y sin necesidad de volver a numerar las interfaces que usan estos prefijos.

- Son independientes de cualquier ISP y se pueden usar para las comunicaciones dentro de un sitio sin tener conectividad a Internet.

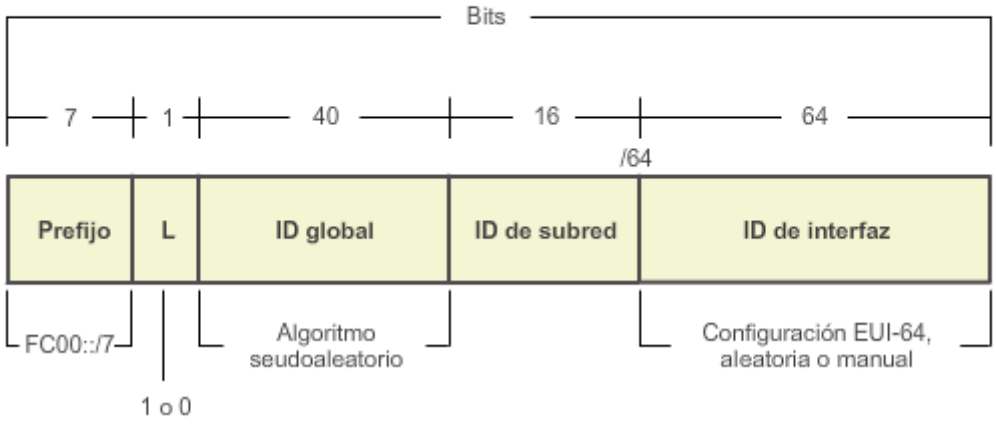
- No se pueden enrutar a través de Internet; sin embargo, si se filtran por routing o DNS, no existe conflicto con otras direcciones.

Las ULA no son tan sencillas como las direcciones definidas en RFC 1918. A diferencia de las direcciones IPv4 privadas, el IETF no tenía la intención de utilizar una forma de NAT para traducir entre las direcciones locales únicas y las direcciones IPv6 de unidifusión global.

La comunidad de Internet continúa analizando la implementación y los posibles usos de las direcciones IPv6 locales únicas. Por ejemplo, el IETF considera permitir la opción de crear el prefijo de la ULA de forma local con FC00::/8, o de que lo asigne un tercero de forma automática y que empiece con FD00::/8.

Nota: la especificación original de IPv6 asignaba el espacio de direcciones para las direcciones locales de sitio, definidas en RFC 3513. El IETF dejó en desuso las direcciones locales de sitio en RFC 3879 porque el término "sitio" resultaba algo ambiguo. Las direcciones locales de sitio tenían el rango de prefijos FEC0::/10 y todavía pueden encontrarse en documentos antiguos de IPv6.

Dirección IPv6 local única



Capítulo 5: Traducción de direcciones de red para IPv4 5.2.5.3 NAT para IPv6

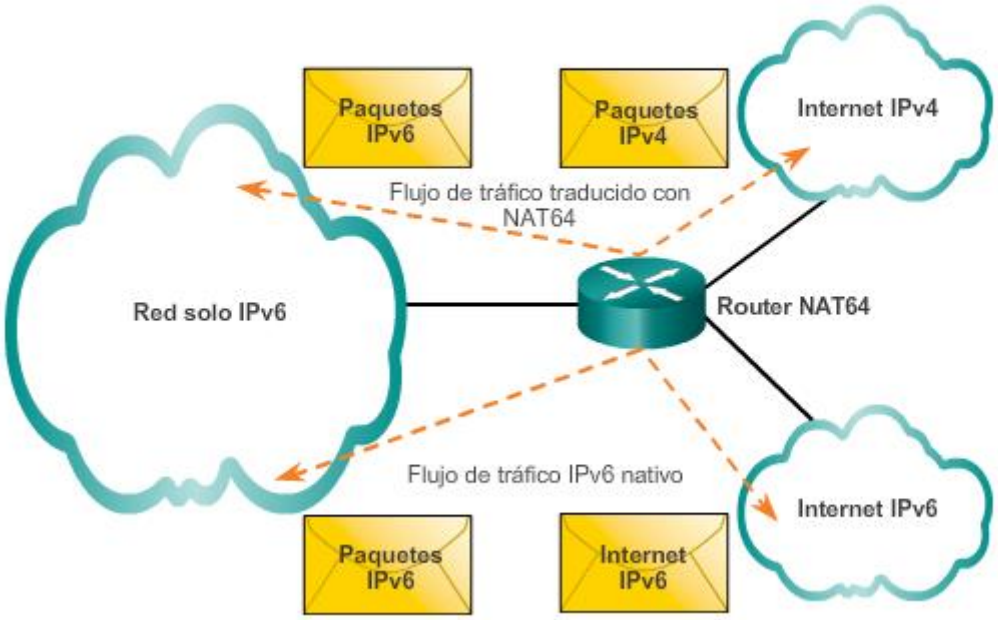
NAT para IPv6 se utiliza en un contexto muy diferente del de NAT para IPv4, como se muestra en la ilustración. Las variedades de NAT para IPv6 se usan para proporcionar acceso de manera transparente entre redes solo IPv6 y redes solo IPv4. No se utiliza como forma de traducción de IPv6 privada a IPv6 global.

Lo ideal es que IPv6 se ejecute de forma nativa siempre que sea posible. Es decir, en dispositivos IPv6 que se comunican entre sí a través de redes IPv6. No obstante, para colaborar en el cambio de IPv4 a IPv6, el IETF elaboró varias técnicas de transición que admiten una variedad de situaciones de IPv4 a IPv6, como dual-stack, tunneling y traducción.

Dual-stack es cuando los dispositivos ejecutan protocolos asociados a IPv4 y a IPv6. Tunneling para IPv6 es el proceso de encapsulación de un paquete IPv6 dentro de un paquete IPv4. Esto permite que el paquete IPv6 se transmita a través de una red solo IPv4.

La NAT para IPv6 no se debe usar como una estrategia a largo plazo, sino como un mecanismo temporal para contribuir a la migración de IPv4 a IPv6. Con el correr de los años, hubo varios tipos de NAT para IPv6, incluida la traducción de direcciones de red/traducción de protocolos (NAT-PT). El IETF dejó en desuso NAT-PT en favor de su reemplazo, NAT64. NAT64 excede el ámbito de este currículo.

NAT64



Capítulo 5: Traducción de direcciones de red para IPv4 5.3.1.1 Resolución de problemas de NAT: comandos show

En la figura 1, se muestra el R2 habilitado para PAT, que usa el rango de direcciones de 209.165.200.226 a 209.165.200.240.

Cuando hay problemas de conectividad IPv4 en un entorno NAT, suele ser difícil determinar la causa del problema. El primer paso para resolverlo es descartar que la causa sea NAT. Siga estos pasos para verificar que NAT funcione como se espera:

Paso 1. En función de la configuración, defina claramente lo que debe lograr la NAT. Esto puede revelar un problema con la configuración.

Paso 2. Verifique que las traducciones de la tabla sean correctas con el comando**show ip nat translations**.

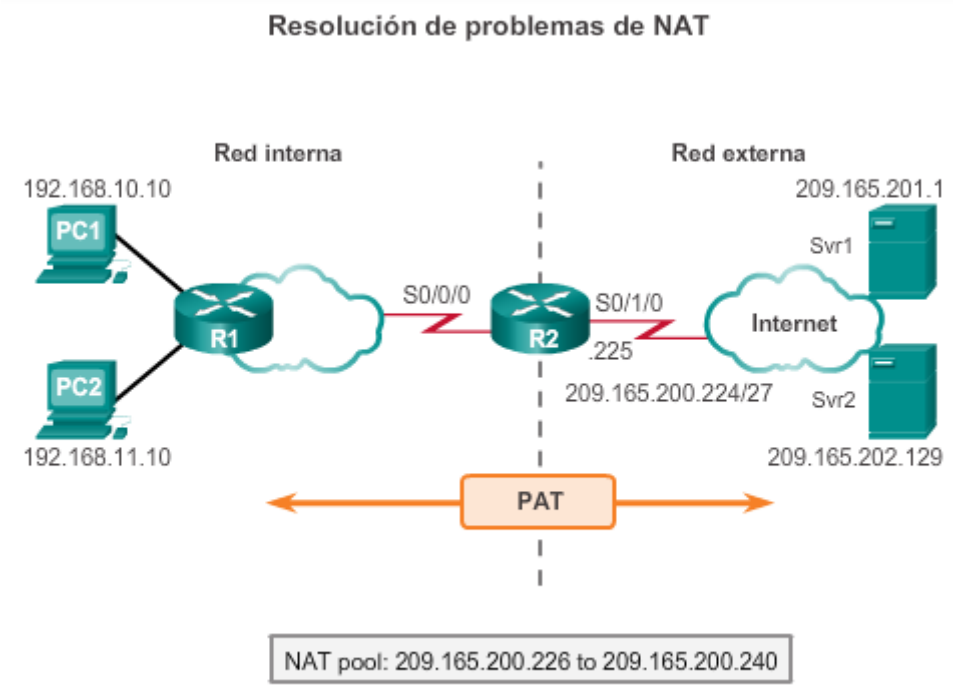
Paso 3. Utilice los comandos **clear** y**debug** para verificar que NAT funcione como se espera. Verifique si se vuelven a crear las entradas dinámicas después de borrarlas.

Paso 4. Revise en detalle lo que sucede con el paquete y verifique que los routers tengan la información de routing correcta para trasladar el paquete.

En la figura 2, se muestra el resultado de los comandos **show ip nat statistics** y **show ip nat translations**. Antes de utilizar los comandos **show**, se eliminan las estadísticas y entradas de NAT de la tabla de NAT con los comandos **clear ip nat statistics** y **clear ip nat translation ***. Una vez que el host en 192.168.10.10 accede mediante Telnet al servidor en 209.165.201.1, se

muestran las estadísticas de NAT y la tabla de NAT para verificar que NAT funcione como se espera.

En un entorno de red simple, es útil controlar las estadísticas de NAT con el comando **show ip nat statistics**. El comando **show ip nat statistics**muestra información sobre la cantidad total de traducciones activas, los parámetros de configuración NAT, la cantidad de direcciones en el conjunto y la cantidad que se asignó. Sin embargo, en un entorno NAT más complejo, con varias traducciones en curso, es posible que este comando no identifique el problema de forma clara. Es posible que se deban ejecutar los comandos **debug** en el router.




```
R2# clear ip nat statistics
R2# clear ip nat translation *
R2#
El host 192.168.10.10 accede al servidor en 209.165.201.1 mediante telnet
R2# show ip nat statistics
Total active translations: 1 (0 static, 1 dynamic; 1 extended)
Peak translations: 1, occurred 00:00:09 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/0/0
Hits: 31  Misses: 0
CEF Translated packets: 31, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 5] access-list 1 pool NAT-POOL2 refcount 1
 pool NAT-POOL2: netmask 255.255.255.224
start 209.165.200.226 end 209.165.200.240
type generic, total addresses 15, allocated 1 (6%), misses 0
<resultado omitido>
R2# show ip nat translations
Pro Inside global         Inside local         Outside local      Out.
tcp 209.165.200.226:19005 192.168.10.10:19005  209.165.201.1:23   209
R2#
```

Capítulo 5: Traducción de direcciones de red para IPv4 5.3.1.2 Resolución de problemas de NAT: comando debug

Para verificar el funcionamiento de la característica de NAT, utilice el comando**debug ip nat**, que muestra información sobre cada paquete que traduce el router. El comando **debug ip nat**

detailedgenera una descripción de cada paquete que se tiene en cuenta para traducir. Este comando también proporciona información sobre determinados errores o condiciones de excepción, como la falla para asignar una dirección global. El comando **debug ip nat detailed** genera más sobrecarga que el comando **debug ip nat**, pero puede proporcionar el detalle necesario para resolver el problema de NAT. Desactive siempre la depuración al finalizar.

En la figura 1, se muestra un resultado de ejemplo de **debug ip nat**. Este resultado muestra que el host interno (192.168.10.10) inició el tráfico hacia el host externo (209.165.201.1) y que la dirección de origen se tradujo a la dirección 209.165.200.226.

Cuando decodifique el resultado de este comando, observe los significados de los siguientes símbolos y valores:

- *** (asterisco):** el asterisco junto a NAT indica que la traducción se realiza en la ruta de switching rápido. Al primer paquete en una conversación siempre se aplica el switching de procesos, que es más lento. Si existe una entrada de caché, el resto de los paquetes atraviesan la ruta de switching rápido.

- **s=:** este símbolo se refiere a la dirección IP de origen.

- **a.b.c.d**--->**w.x.y.z:** este valor indica que la dirección de origen a.b.c.d se traduce a w.x.y.z.

- **d=:** este símbolo se refiere a la dirección IP de destino.

- **[xxxx]:** el valor entre corchetes es el número de identificación IP. Esta información puede ser útil para la depuración, ya que habilita la correlación con otros seguimientos de paquetes realizados por los analizadores de protocolos.

Nota: verifique que la ACL mencionada en la referencia de comandos de NAT permita todas las redes necesarias. En la figura 2, solo las direcciones 192.168.0.0/16 se pueden traducir. El R2 no traduce los paquetes de la red interna destinados a Internet con direcciones de origen que la ACL 1 no permita de forma explícita.

```
R2# debug ip nat
IP NAT debugging is on
R2#
*Feb 15 20:01:311.670: NAT*: s=192.168.10.10->209.165.200.226,
*Feb 15 20:01:311.682: NAT*: s=209.165.201.1, d=209.165.200.226
*Feb 15 20:01:311.698: NAT*: s=192.168.10.10->209.165.200.226,
*Feb 15 20:01:311.702: NAT*: s=192.168.10.10->209.165.200.226,
*Feb 15 20:01:311.710: NAT*: s=192.168.10.10->209.165.200.226,
*Feb 15 20:01:311.710: NAT*: s=209.165.201.1, d=209.165.200.226
*Feb 15 20:01:311.722: NAT*: s=209.165.201.1, d=209.165.200.226
*Feb 15 20:01:311.726: NAT*: s=192.168.10.10->209.165.200.226,
*Feb 15 20:01:311.730: NAT*: s=209.165.201.1, d=209.165.200.226
*Feb 15 20:01:311.734: NAT*: s=192.168.10.10->209.165.200.226,
*Feb 15 20:01:311.734: NAT*: s=209.165.201.1, d=209.165.200.226
<resultado omitido>
```

Capítulo 5: Traducción de direcciones de red para IPv4 5.3.1.3 Caso práctico

Caso práctico

En la figura 1, se muestra que los hosts de las LAN 192.168.0.0/16, la PC1 y la PC2, no pueden hacer ping a los servidores en la red externa, el Svr1 y el Svr2.

Para iniciar la resolución de problemas, utilice el comando **show ip nat translations** a fin de verificar si actualmente hay alguna traducción en la tabla de NAT. El resultado de la figura 1 muestra que no hay traducciones en la tabla.

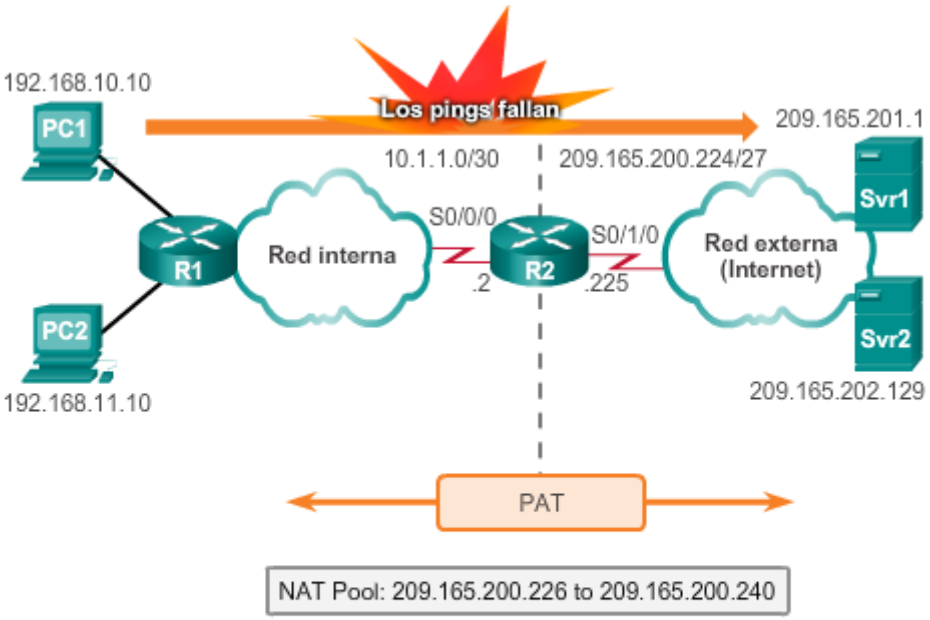
El comando **show ip nat statistics**se utiliza para determinar si se realizaron traducciones. También identifica las interfaces entre las que debe ocurrir la traducción. Como se muestra en el resultado de la figura 2, los contadores de NAT están en 0, lo que verifica que no se realizó ninguna traducción. Al comparar el resultado con la topología de la figura 1, observe que las interfaces del router están definidas de forma incorrecta como NAT interna o NAT externa. También es posible verificar una configuración incorrecta con el comando **show running-config**.

Se debe eliminar la configuración NAT actual de las interfaces antes de aplicar la configuración correcta.

Luego de definir correctamente las interfaces NAT interna y externa, otro ping de la PC1 al Svr1 falla. El uso de los comandos **show ip nat translations**y **show ip nat statistics**nuevamente verifica que no hay traducciones en curso.

Como se muestra en la figura 3, el comando **show access-lists** se utiliza para determinar si la ACL a la que hace referencia el comando NAT permite todas las redes necesarias. Al examinar el resultado, se comprueba que se utilizó una máscara de bits wildcard incorrecta en la ACL que define las direcciones que se deben traducir. La máscara wildcard solo permite la subred 192.168.0.0/24. Primero se elimina la lista de acceso y después se reconfigura con la máscara wildcard correcta.

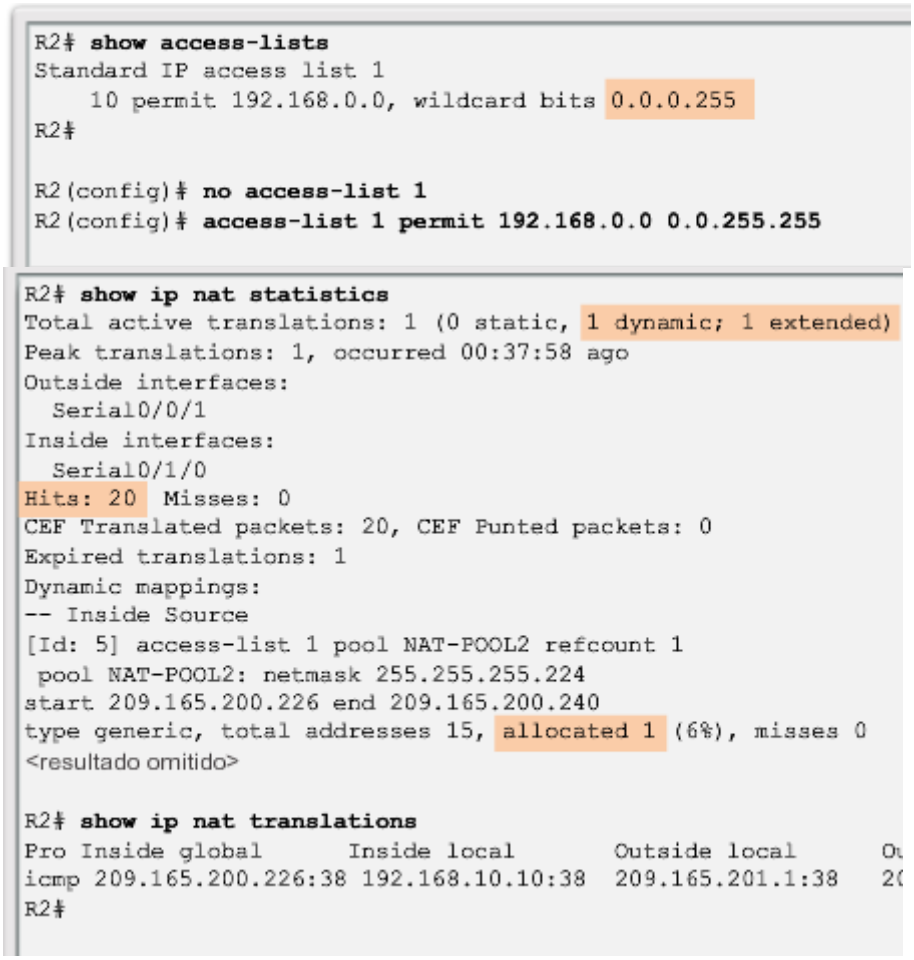
Una vez corregidas las configuraciones, se genera otro ping de la PC1 al Svr1, y esta vez el ping es correcto. Como se muestra en la figura 4, los comandos **show ip nat translations** y **show ip nat statistics** se utilizan para verificar que se produzca la traducción NAT.




```
R2# show ip nat translations
R2#
```

```
R2# show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
  Serial0/0/0
Inside interfaces:
  Serial0/1/0
Hits: 0  Misses: 0
<resultado omitido>

R2(config)# interface serial 0/0/0
R2(config-if)# no ip nat outside
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface serial 0/0/1
R2(config-if)# no ip nat inside
R2(config-if)# ip nat outside
```



Capítulo 5: Traducción de direcciones de red para IPv4 5.3.1.4 Packet Tracer: verificación y resolución de problemas de configuración NAT

Información básica/situación

Un contratista restauró una antigua configuración en un nuevo router que ejecuta NAT. Sin embargo, la red se modificó y se agregó una nueva subred después de hacer una copia de seguridad de la antigua configuración. Su trabajo es hacer que la red funcione nuevamente.

Packet Tracer: verificación y resolución de problemas de configuración NAT (instrucciones)

Packet Tracer: verificación y resolución de problemas de configuración NAT (PKA)

Capítulo 5: Traducción de direcciones de red para IPv4 5.3.1.5 Práctica de laboratorio: resolución de problemas de configuración NAT

En esta práctica de laboratorio, cumplirá los siguientes objetivos:

- Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

- Parte 2: resolver problemas de la NAT estática
- Parte 3: resolver problemas de la NAT dinámica

Práctica de laboratorio: resolución de problemas de configuración NAT

Capítulo 5: Traducción de direcciones de red para IPv4 5.4.1.1 Actividad de clase: Revisión de NAT

Revisión de NAT

La traducción de direcciones de red no se incluye actualmente en el diseño de red de su empresa. Se decidió configurar algunos dispositivos para que utilicen los servicios de NAT para conectarse al servidor de correo.

Antes de implementar la NAT real en la red, usted crea un prototipo mediante un programa de simulación de redes.

Actividad de clase: Revisión de NAT

Capítulo 5: Traducción de direcciones de red para IPv4 5.4.1.2 Packet Tracer: desafío de integración de habilidades

Información básica/situación

Esta actividad de culminación incluye muchas de las habilidades que adquirió durante este curso. Primero deberá completar la documentación de la red. De modo que debe asegurarse de tener una versión impresa de las instrucciones. Durante la implementación, configurará las VLAN, los enlaces troncales, la seguridad de puertos y el acceso remoto mediante SSH en un switch. Luego deberá implementar el routing entre redes VLAN y NAT en un router. Por último, deberá utilizar su documentación para verificar la implementación al probar la conectividad de extremo a extremo.

Packet Tracer: Desafío de integración de habilidades (instrucciones)

Packet Tracer: Desafío de integración de habilidades (PKA)

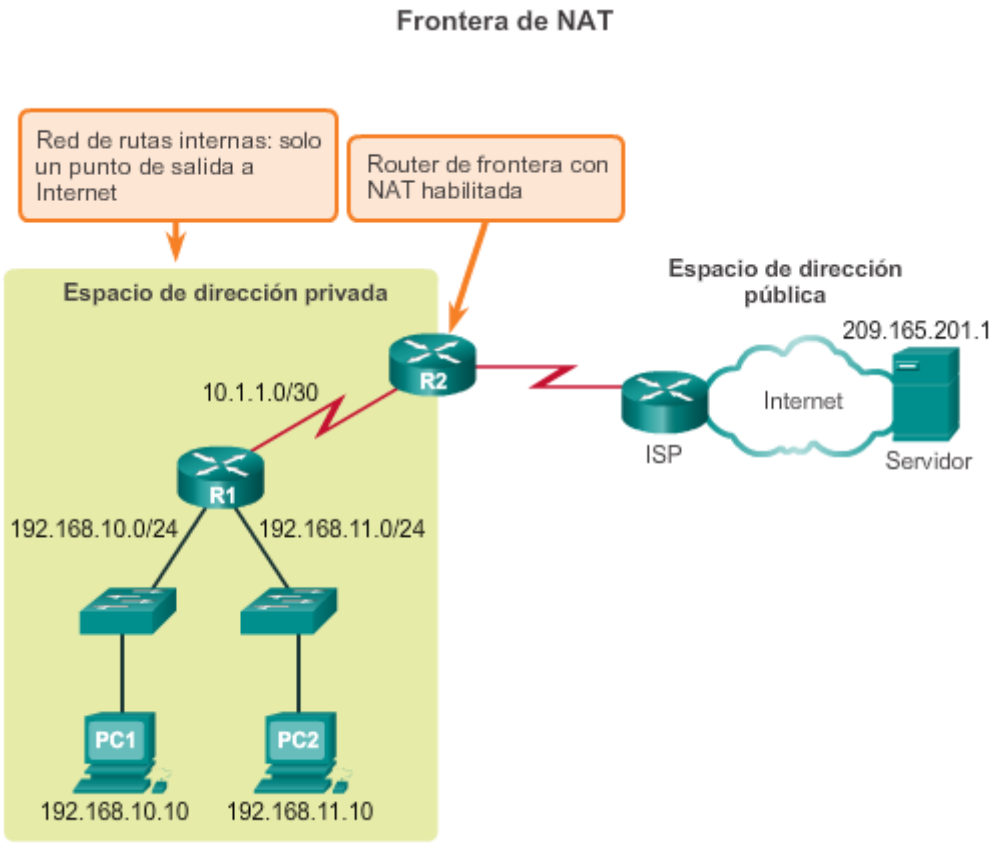
Capítulo 5: Traducción de direcciones de red para IPv4 5.4.1.3 Resumen

En este capítulo, se explicó cómo se utiliza NAT para contribuir a mitigar el agotamiento del espacio de direcciones IPv4. La NAT para IPv4 permite que los administradores de red utilicen el espacio de direcciones privadas definido en RFC 1918, a la vez que proporciona conectividad a Internet, mediante una única dirección pública o una cantidad limitada de estas.

NAT conserva el espacio de direcciones públicas y reduce la sobrecarga administrativa de forma considerable al administrar las adiciones, los movimientos y las modificaciones. NAT y PAT se pueden implementar para ahorrar espacio de direcciones públicas y armar intranets privadas seguras sin afectar la conexión al ISP. Sin embargo, NAT presenta desventajas en términos de sus efectos negativos en el rendimiento de los dispositivos, la seguridad, la movilidad y la conectividad de extremo a extremo, y se debe considerar como una implementación a corto plazo para el agotamiento de direcciones, cuya solución a largo plazo es IPv6.

En este capítulo, se analizó la NAT para IPv4, incluido lo siguiente:

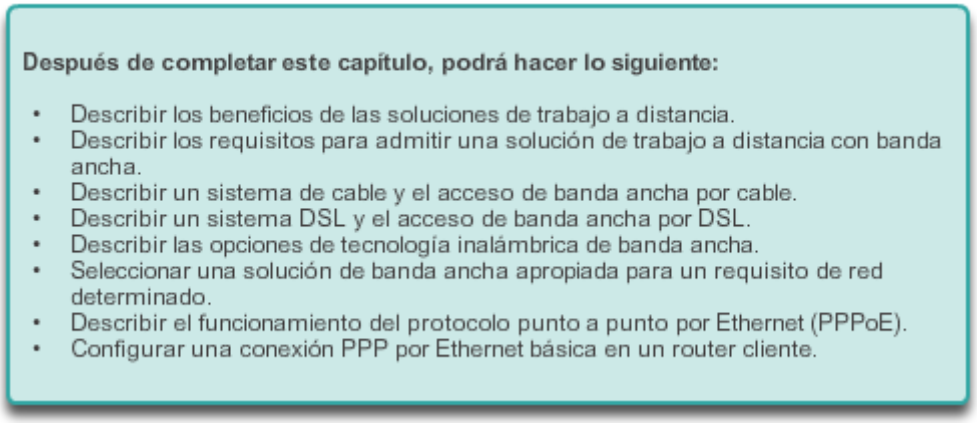
- Las características, la terminología y las operaciones generales de NAT
- Los diferentes tipos de NAT, incluidas la NAT estática, la NAT dinámica y PAT
- Las ventajas y las desventajas de NAT
- La configuración, la verificación y el análisis de la NAT estática, la NAT dinámica y PAT
- La forma en que se puede usar el reenvío de puertos para acceder a los dispositivos internos desde Internet
- La resolución de problemas de NAT mediante los comandos **show** y **debug**



Capítulo 6: Soluciones de banda ancha 6.0.1.1 Introducción

El trabajo a distancia, o el trabajo desde un lugar que no es tradicional, como el hogar, ofrece muchos beneficios al trabajador y a la empresa. Las soluciones de banda ancha proporcionan opciones de conexión de alta velocidad a ubicaciones empresariales y a Internet para estos trabajadores. Las pequeñas sucursales también pueden conectarse mediante estas mismas tecnologías.

En este capítulo, se abarcan las soluciones de banda ancha de uso frecuente, como el cable, DSL y la tecnología inalámbrica. La tecnología VPN proporciona opciones de seguridad para los datos que atraviesan estas conexiones. En este capítulo, también se analizan los factores que se deben tener en cuenta si hay más de una solución de banda ancha disponible para brindar servicios a una ubicación determinada.



Capítulo 6: Soluciones de banda ancha 6.0.1.2 Actividad de clase: Variedades de banda ancha

Variedades de banda ancha

Las oportunidades de empleo a distancia en su área local se expanden todos los días. Le ofrecieron empleo como trabajador a distancia para una empresa importante. El nuevo empleador requiere que los trabajadores a distancia tengan acceso a Internet para cumplir con sus responsabilidades laborales.

Investigue los siguientes tipos de conexión a Internet por banda ancha que están disponibles en su área geográfica:

- DSL
- Cable
- Satélite

Considere las ventajas y desventajas de cada variante de banda ancha a medida que registra su investigación, las cuales pueden incluir el costo, la velocidad, la seguridad y la facilidad de implementación o instalación.

Actividad de clase: Variedades de banda ancha

Capítulo 6: Soluciones de banda ancha 6.1.1.1 Introducción al trabajo a distancia

El trabajo a distancia consiste en trabajar fuera del lugar de trabajo tradicional, por ejemplo, desde una oficina doméstica. Los motivos para elegir el trabajo a distancia son diversos e incluyen desde cuestiones de conveniencia personal hasta permitir que los empleados tengan la oportunidad de continuar trabajando cuando están enfermos o tienen una discapacidad.

El término “trabajo a distancia” es amplio y se refiere a desempeñar una tarea mediante la conexión a un lugar de trabajo desde una ubicación remota, con ayuda de las telecomunicaciones. El trabajo a distancia se realiza de forma eficaz gracias a las conexiones a Internet de banda ancha, las redes privadas virtuales (VPN), voz sobre IP (VoIP) y las videoconferencias.

Muchas empresas modernas ofrecen oportunidades de empleo para las personas que no pueden trasladarse al trabajo todos los días o para aquellas a las que les resulta más práctico trabajar desde una oficina doméstica. Estas personas, denominadas “trabajadores a distancia”, se deben conectar a la red de la empresa para poder trabajar y compartir información desde las oficinas domésticas.

Las soluciones de banda ancha son esenciales para que el trabajo a distancia se desarrolle correctamente. En este capítulo, se detallan los beneficios del trabajo a distancia y la forma en que las soluciones de banda ancha hacen que el trabajo a distancia sea la forma más inteligente de hacer negocios.

Capítulo 6: Soluciones de banda ancha 6.1.1.2 Beneficios del trabajo a distancia para el empleador

Para las organizaciones, ofrecer un entorno de trabajo a distancia tiene muchos beneficios. Algunos de los beneficios más conocidos incluyen lo siguiente:

- **Mejora la productividad de los empleados:** en general, el trabajo a distancia permite que los empleados trabajen más y mantengan una mejor calidad de trabajo que los trabajadores limitados exclusivamente a un espacio de oficina. Según un estudio de British Telecom realizado por Gartner Group, el empleado a distancia promedio trabaja un 11% más de horas que el empleado de oficina. La empresa Bell Atlantic Corporation (ahora conocida como Verizon) indicó que 25 horas de trabajo en el hogar equivalen a 40 horas de trabajo en la oficina.

- **Reduce costos y gastos:** el costo inmobiliario es un gasto importante para muchas organizaciones. El trabajo a distancia representa menos requisitos de espacio de oficina. El ahorro en el costo inmobiliario puede equivaler entre el 10% y el 80%. Incluso un ahorro del 10% en costos inmobiliarios puede marcar la diferencia entre pérdidas y ganancias. Los ahorros adicionales incluyen calefacción, aire acondicionado, estacionamiento, iluminación, equipos e insumos de oficina, ya que todos estos costos, entre otros, disminuyen a medida que el personal comienza a trabajar a distancia.

- **Facilita la contratación y la retención:** al ofrecer flexibilidad, se puede reducir la rotación de personal hasta un 20%. Esto es un ahorro considerable, ya que el reemplazo

de personal representa un 75% del salario o más, incluso sin tener en cuenta los costos de capacitación y retención. Algunos observadores calculan que el costo de la rotación de personal llega al 250% del salario.

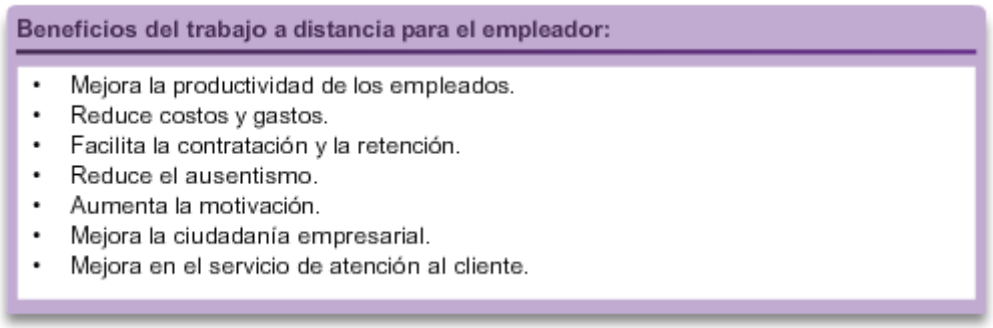
- **Reduce el ausentismo:** el trabajo a distancia puede reducir el ausentismo hasta un 80%.

- **Aumenta la motivación:** los empleadores que ofrecen la opción de trabajo a distancia a menudo se consideran empleadores que concilian la vida laboral y familiar.

- **Mejora la ciudadanía empresarial:**permitir que los empleados trabajen desde sus hogares y reducir las emisiones de transporte que generan los empleados de una empresa puede ser una parte importante del plan de una organización para lograr reducir cada vez más la emisión de dióxido de carbono y ser una empresa más ecológica. Esto puede traer muchos beneficios, incluido lo siguiente: crear oportunidades de marketing, agregar valor a los productos y servicios, abordar las inquietudes que expresan los clientes y responder a los requisitos de la cadena de abastecimiento.

- **Mejora el servicio al cliente:** si el personal no tiene que comenzar la jornada laboral trasladándose a la oficina, los clientes experimentan mejoras en los tiempos de contacto y de respuesta, lo que da lugar a grandes mejoras con respecto a la retención y la valoración de los clientes. Los clientes informan una respuesta más rápida y un mejor servicio.

Al haber mejores tiempos de respuesta, un mejor servicio al cliente, una reducción en los costos y una mayor productividad de los empleados, las empresas pueden competir mejor en mercados que cambian rápidamente. El trabajo a distancia realmente es una manera inteligente de hacer negocios.



Capítulo 6: Soluciones de banda ancha 6.1.1.3 Beneficios para la comunidad y el gobierno

El trabajo a distancia puede beneficiar a organizaciones de todos los tamaños, desde pequeñas empresas hasta grandes corporaciones. Sin embargo, esos beneficios en realidad se extienden más allá del nivel de la organización, lo que ofrece ventajas exclusivas para las entidades públicas como las comunidades e incluso los gobiernos locales y nacionales.

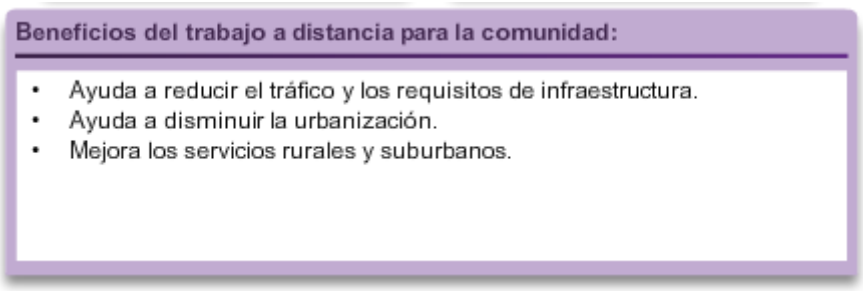
Las entidades públicas, como las comunidades y los gobiernos, son empresas que deben administrar ganancias y gastos. Deben ser tan eficaces, responsables y transparentes como sea posible, porque el dinero de los contribuyentes está en juego. Por este motivo, desde el punto de vista empresarial, todos los beneficios para los empleados y de ahorro de costos que

ofrece el trabajo a distancia se aplican a estas entidades públicas. Además, las entidades públicas se benefician del trabajo a distancia de las siguientes maneras:

- **Ayuda a reducir el tráfico y los requisitos de infraestructura:** el trabajo a distancia elimina muchos problemas contemporáneos de raíz. El tráfico es solo un ejemplo. Según un artículo del Washington Post publicado en el año 2004, los retrasos de tráfico en la región de Washington D. C. disminuyeron un 10% por cada 3% de las personas que trabajan desde el hogar. Además, el trabajo a distancia reduce los costos de infraestructura y de prestación de servicios.

- **Ayuda a disminuir la urbanización:**la urbanización se refiere al traslado de las personas desde zonas rurales hasta centros urbanos en busca de mejores condiciones y oportunidades laborales. La urbanización provoca hacinamiento y congestión. El trabajo a distancia permite que las personas puedan trabajar sin importar la ubicación física, lo que elimina la necesidad de que se tengan que mudar por causas laborales.

- **Mejora los servicios rurales y suburbanos:** el aumento en la cantidad de personas que trabajan en regiones rurales o suburbanas podría traer mejoras en los servicios de transporte público y cambios en las instalaciones minoristas locales. Hay menos probabilidades de que las oficinas de correo, los consultorios médicos, los bancos o las estaciones de servicio cierren y se muden a otro lugar. Con una respuesta más flexible, empresas más productivas y la capacidad de todas las personas para contribuir, las regiones o el país se vuelven más competitivos y atraen más empleo y desarrollo.



Capítulo 6: Soluciones de banda ancha 6.1.1.4 Beneficios individuales del trabajo a distancia

Al trabajar en forma remota, las personas también obtienen importantes beneficios, incluido lo siguiente:

- **Productividad:** más del 70% de los trabajadores a distancia informan que son mucho más productivos, lo que significa que hacen más en menos tiempo; de esta forma, se ahorra tiempo o se gana más en el mismo tiempo.

- **Flexibilidad:** los trabajadores a distancia pueden administrar mejor el momento y el lugar donde se realiza el trabajo. Cuentan con mayor flexibilidad para administrar muchos otros detalles de la vida moderna, como reparar el automóvil, evitar el tráfico durante los fines de semana largos y llevar a sus hijos al médico.

- **Ahorro de costos:** los empleados que deben trasladarse a una oficina gastan una suma importante de dinero debido a la carga de combustible y el mantenimiento del vehículo, los almuerzos, la ropa para ir a trabajar, las salidas a comer y todos los demás costos relacionados con el trabajo tradicional que se pueden reducir si se trabaja a distancia.

- **Hogar y familia:** para muchas personas, dedicar más tiempo a la familia o cuidar a parientes a cargo es uno de los principales motivos para trabajar a distancia.

Capítulo 6: Soluciones de banda ancha 6.1.1.5 Desventajas del trabajo a distancia

Si bien los beneficios del trabajo a distancia son muchos, existen algunas desventajas que también se deben tener en cuenta:

Desde el punto de vista del empleador:

- **Seguimiento del progreso de los empleados:** para algunos gerentes, puede resultar difícil hacer un seguimiento de los logros de trabajo de los empleados que trabajan a distancia. Es necesario acordar evaluaciones de control y validar el progreso de tareas de diferente manera con los empleados que trabajan desde el hogar.

- **Necesidad de implementar un nuevo estilo de administración:** los gerentes que supervisan a los empleados dentro de una oficina pueden mantener un contacto personal con todos ellos. Esto significa que, si surge un problema o hay un malentendido con las tareas asignadas, se puede llevar a cabo una reunión cara a cara no programada, lo que suele resolver el problema rápidamente. En el entorno del trabajo a distancia, los gerentes deben establecer procesos para validar la comprensión y tienen que mantenerse flexibles a las diversas necesidades de los empleados a distancia.

Desde el punto de vista de los empleados:

- **Sensación de aislamiento:** a muchas personas, trabajar desde el hogar las hace sentirse solas.

- **Conexiones más lentas:** por lo general, en las áreas residenciales y rurales no se obtiene el tipo de soporte y de servicios tecnológicos que reciben las oficinas ubicadas en centros urbanos, y estos servicios pueden ser costosos. Si se requiere un ancho de banda alto para trabajar, piense con detenimiento si la oficina doméstica es la opción adecuada.

- **Distracciones:** ya sea un vecino, un cónyuge, un niño, cortar el césped, lavar la ropa, la TV o el refrigerador, en la oficina doméstica se presentan distracciones. Además, muchas personas consideran que si se trabaja a distancia, no hay necesidad de contratar servicios de cuidado de niños, pero esto no es del todo cierto. Especialmente con los niños pequeños, a veces es importante planificar su cuidado cuando es necesario concentrarse por completo en el trabajo.

Capítulo 6: Soluciones de banda ancha 6.1.1.6 Actividad: Beneficios del trabajo a distancia

Actividad: Clasificar los beneficios del trabajo a distancia

Haga clic en la casilla que mejor represente la categoría a la que pertenece cada beneficio.

	Empleador	Gobierno/comunidad	Individuo
1. Reduce los costos de infraestructura local.		✓	
2. Puede reducir los retrasos en el tráfico regional.		✓	
3. Reduce los costos de contratación y retención.	✓		
4. Reduce los costos asociados al traslado.			✓
5. Reduce los niveles de ausentismo.	✓		
6. Atrae el empleo y el desarrollo en el ámbito local.		✓	
7. Aumenta el tiempo disponible para cuidar de las personas a cargo.			✓

Capítulo 6: Soluciones de banda ancha 6.1.2.1 Solución para el trabajador a distancia

Las organizaciones necesitan redes seguras, confiables y rentables para conectar las sedes centrales, las sucursales y los proveedores. Con el aumento en la cantidad de trabajadores a distancia, hay una creciente necesidad de las empresas de contar con formas seguras, confiables y rentables para conectar a los trabajadores a distancia a los recursos de la organización en los sitios de la LAN corporativa.

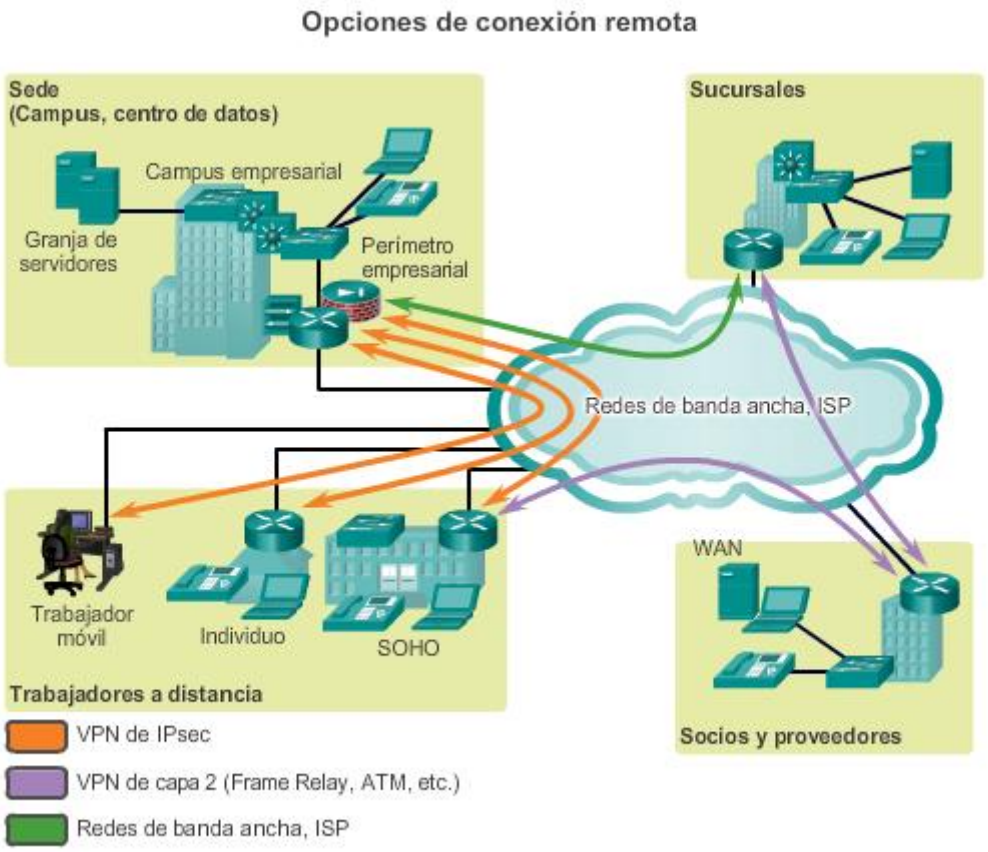
En la ilustración, se muestran topologías de conexión remota que las redes modernas utilizan para conectar ubicaciones remotas. En algunos casos, las ubicaciones remotas se conectan solo a la oficina central, mientras que en otros casos, las ubicaciones remotas se conectan a varios sitios. La sucursal que se muestra en la ilustración se conecta a la oficina central y los sitios asociados, mientras que el trabajador a distancia tiene una única conexión a la oficina central.

Existen tres tecnologías principales de conexión remota para las organizaciones que admiten servicios para trabajadores a distancia:

- **Conexiones de banda ancha:** el término “banda ancha” se refiere a los sistemas de comunicaciones avanzados capaces de proporcionar una transmisión de alta velocidad de los servicios, como datos, voz y video por Internet y otras redes. La transmisión se proporciona mediante una amplia variedad de tecnologías, como DSL, fibra hasta el hogar, sistemas de cable coaxial, tecnología inalámbrica y satelital. Las velocidades de transmisión de datos del servicio de banda ancha generalmente exceden los 200 kb/s en al menos un sentido entre el ISP y el usuario.

- **VPN con IPsec:** esta es la opción más común para los trabajadores a distancia, combinada con el acceso remoto a través de banda ancha, para establecer una VPN segura mediante Internet pública. Este tipo de conexión WAN ofrece conectividad flexible y escalable. Las conexiones de sitio a sitio pueden proporcionar una conexión remota segura, rápida y confiable a los trabajadores a distancia.

- **Tecnologías tradicionales de capa 2 de WAN privada:** estos tipos de conexión proporcionan muchas soluciones de conexión remota e incluyen tecnologías como Frame Relay, ATM y las líneas arrendadas. La seguridad de estas conexiones depende del proveedor de servicios que las proporciona.



Capítulo 6: Soluciones de banda ancha 6.1.2.2 Requisitos de conectividad de trabajadores a distancia

Independientemente de la tecnología de conexión remota que se usa para conectarse a las redes de una organización, los trabajadores a distancia requieren tanto componentes de oficina doméstica como componentes corporativos:

- **Componentes de la oficina doméstica:** los componentes requeridos en la oficina doméstica son una computadora portátil o de escritorio, acceso por banda ancha (mediante cable, DSL o tecnología inalámbrica) y un software de router o cliente VPN instalado en la computadora. Los componentes adicionales pueden incluir un punto de acceso inalámbrico. Cuando viajan, los trabajadores a distancia necesitan una conexión a Internet y un cliente VPN para conectarse a la red corporativa mediante cualquier conexión de dial-up, de red o de banda ancha disponible.

- **Componentes corporativos:** los componentes corporativos son routers con capacidad para VPN, concentradores VPN, dispositivos de seguridad multifunción y dispositivos de autenticación y administración central para la agregación y la terminación resistentes de las conexiones VPN.

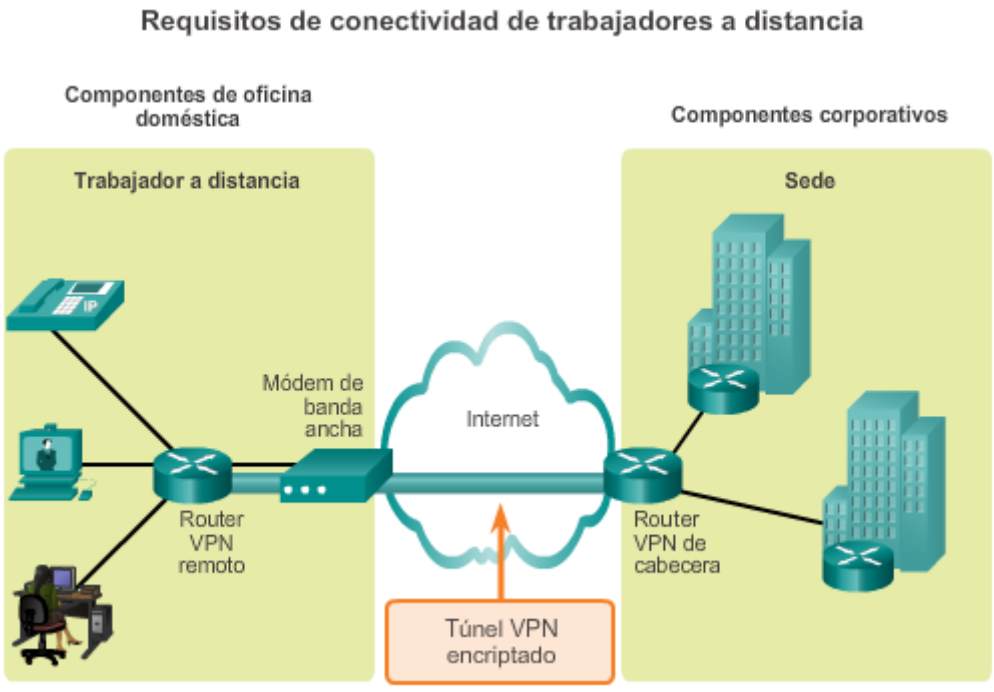
Los componentes de VoIP y videoconferencia que admiten calidad de servicio (QoS) son componentes cada vez más esenciales del kit de herramientas de los trabajadores a distancia. QoS se refiere a la capacidad de una red para proporcionar un mejor servicio al tráfico de la red

seleccionado, según los requisitos de las aplicaciones de voz y video. Para admitir VoIP y videoconferencia se deben actualizar los routers y dispositivos que admiten funcionalidad de QoS.

En la ilustración, se muestra un túnel VPN cifrado que conecta al trabajador a distancia a la red corporativa. Esta es la base principal de las conexiones seguras y confiables para los trabajadores a distancia. Una VPN es una red de datos privada que utiliza la infraestructura pública de telecomunicaciones. La seguridad de VPN mantiene la privacidad mediante un protocolo de tunneling y procedimientos de seguridad. En este curso, se presenta el protocolo de seguridad IP (IPsec) como el método preferido para construir túneles VPN seguros. A diferencia de los enfoques de seguridad anteriores que aplican seguridad en la capa de aplicación del modelo OSI, IPsec funciona en la capa de red, donde se produce el procesamiento de paquetes.

Como ya se mencionó, un túnel VPN seguro se utiliza a través de una infraestructura pública de telecomunicaciones. Esto significa que antes de iniciar un VPN, los usuarios domésticos primero deben poder conectarse a los servicios de Internet mediante alguna forma de acceso por banda ancha de alta velocidad. Las tres formas de acceso por banda ancha más comunes incluyen lo siguiente:

- Cable
- DSL
- Acceso inalámbrico de banda ancha



Capítulo 6: Soluciones de banda ancha 6.1.2.3 Actividad: Clasificar los requisitos para la conectividad del trabajador a distancia

Actividad: Clasificar los requisitos para la conectividad del trabajador a distancia

Haga clic en la casilla que mejor represente la categoría a la que pertenece cada responsabilidad de conectividad.

	Trabajador a distancia	Empresa
1. Generalmente utiliza cable o DSL para acceder a la VPN.	✓	
2. Utiliza software de cliente para acceder a la red.	✓	
3. Mantiene los dispositivos de seguridad y los concentradores VPN.		✓
4. Determina los métodos de agregación de enlaces y de terminación de VPN.		✓
5. Utiliza acceso de red mientras viaja.	✓	
6. Administra los procedimientos de autenticación de VPN.		✓

Capítulo 6: Soluciones de banda ancha 6.2.1.1 ¿Qué es un sistema de cable?

El acceso a Internet a través de una red de cable es una opción común que utilizan los trabajadores a distancia para acceder a su red empresarial. El sistema de cable utiliza un cable coaxial que transporta las señales de radiofrecuencia (RF) a través de la red. El cable coaxial es el principal medio que se utiliza para armar sistemas de TV por cable.

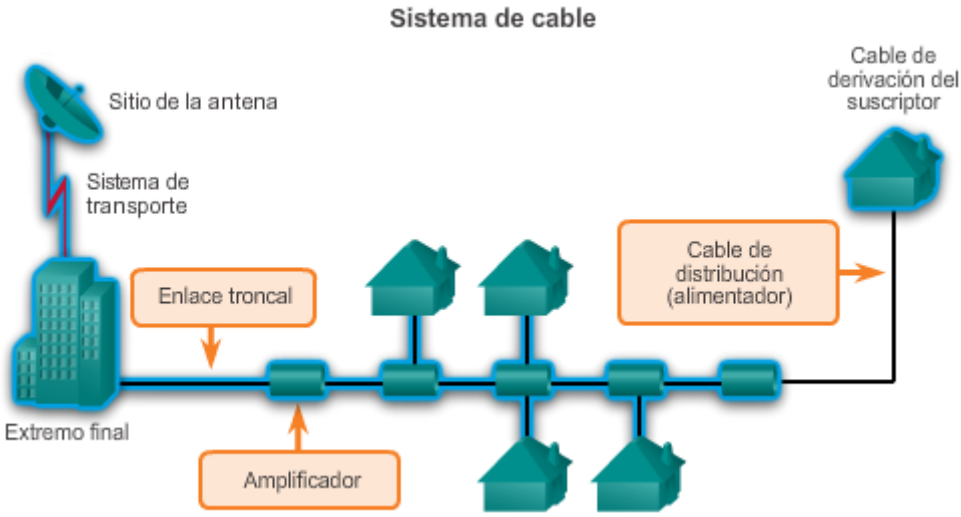
La televisión por cable comenzó en Pensilvania en el año 1948. John Walson, propietario de una tienda de electrodomésticos en un pequeño pueblo de montaña, necesitaba resolver los problemas de mala recepción por aire que experimentaban los clientes que deseaban recibir señales de televisión desde Filadelfia a través de las montañas. Walson colocó una antena en un poste de servicio público en la cima de una montaña local, lo que le permitió mostrar los televisores de su tienda con buenas señales de difusión provenientes de las tres estaciones de Filadelfia. Conectó la antena a la tienda a través de un cable y modificó los amplificadores de señal. A continuación, conectó a varios de los clientes que se encontraban en el trayecto del cable. Este fue el primer sistema de televisión por cable (CATV) en los Estados Unidos.

La empresa de Walson creció con el transcurso de los años, y se lo reconoce como el fundador de la industria de la televisión por cable. También fue el primer operador de cable en utilizar las microondas para importar las señales de estaciones de televisión distantes y el primero en utilizar el cable coaxial para mejorar la calidad de la imagen.

La mayoría de los operadores de cable utilizan antenas parabólicas para atraer las señales de televisión. Los primeros sistemas eran unidireccionales, en los que se colocaban amplificadores en cascada en serie a lo largo de la red para compensar la pérdida de señal. Estos sistemas utilizaban derivaciones para vincular señales de video desde las líneas principales hasta los hogares de los suscriptores mediante los cables de derivación.

Los sistemas de cable modernos proporcionan una comunicación bidireccional entre los suscriptores y el operador de cable. Hoy en día, los operadores de cable ofrecen servicios avanzados de telecomunicaciones a los clientes, incluidos el acceso a Internet de alta velocidad, la televisión por cable digital y el servicio telefónico residencial. Los operadores de cable suelen implementar redes de fibra coaxial híbrida (HFC) para habilitar la transmisión de datos de alta velocidad a los cable módems ubicados en una SOHO.

Haga clic en las áreas resaltadas en la ilustración para obtener más información sobre los componentes de un sistema de cable moderno típico.



Capítulo 6: Soluciones de banda ancha 6.2.1.2 Cable y espectro electromagnético

El espectro electromagnético abarca una amplia banda de frecuencias.

La frecuencia es la velocidad a la que se producen los ciclos de corriente o de voltaje. La frecuencia se calcula como la cantidad de ondas por segundo. La longitud de onda es la distancia desde el punto más alto de una onda hasta el punto más alto de la siguiente. La longitud de onda se calcula como la velocidad de propagación de la señal electromagnética dividida por su frecuencia en ciclos por segundo.

Las ondas de radio, a menudo denominadas RF, constituyen una porción del espectro electromagnético entre 1 kHz y 1 THz aproximadamente, como se indica en la ilustración. Cuando los usuarios sintonizan una radio o un televisor para buscar diferentes estaciones de radio o canales de televisión, sintonizan distintas frecuencias electromagnéticas a través de ese espectro de RF. El mismo principio se aplica al sistema de cable.

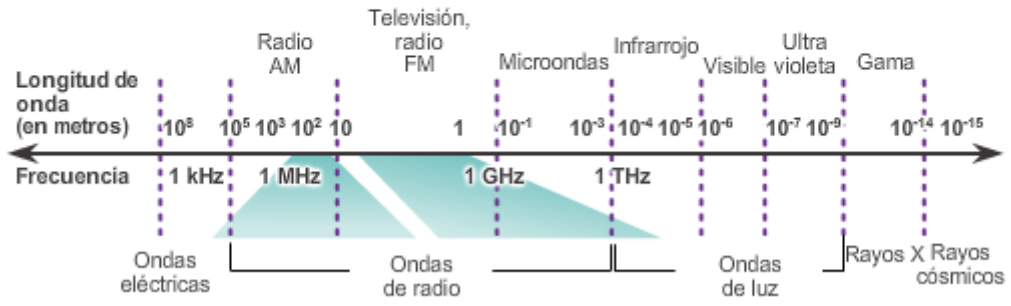
La industria de la televisión por cable utiliza una parte del espectro electromagnético de RF. Dentro del cable, hay diferentes frecuencias que transportan canales de televisión y datos. En el extremo del suscriptor, los equipos como los televisores, los reproductores de Blu-ray, los DVR y los decodificadores de HDTV sintonizan ciertas frecuencias que permiten que el usuario vea el canal o utilice un cable módem para recibir acceso a Internet de alta velocidad.

Una red de cable puede transmitir señales por el cable en cualquier sentido al mismo tiempo. Se utilizan los siguientes alcances de frecuencia:

- **Descendente:** el sentido de la transmisión de una señal de RF, como los canales de televisión y los datos, desde el origen, o la cabecera, hasta el destino, o los suscriptores. La transmisión de origen a destino se denomina “ruta de reenvío”. Las frecuencias descendentes se encuentran en la banda de 50 MHz a 860 MHz.

- **Ascendente:** el sentido de la transmisión de la señal de RF desde los suscriptores hasta la cabecera. Las frecuencias ascendentes se encuentran en la banda de 5 MHz a 42 MHz.

Espectro electromagnético del cable



Capítulo 6: Soluciones de banda ancha 6.2.1.3 DOCSIS

La especificación de interfaz para servicios de datos por cable (DOCSIS) es un estándar internacional desarrollado por CableLabs, un consorcio sin fines de lucro para la investigación y el desarrollo de tecnologías relacionadas con el cable. CableLabs prueba y certifica los dispositivos de proveedores de equipos de cable, como los cable módems y los sistemas de terminación de cable módem, y otorga la certificación y la calificación DOCSIS.

DOCSIS define los requisitos para las comunicaciones y los requisitos de la interfaz de soporte de funcionamiento para un sistema de datos por cable, y permite agregar la transferencia de datos de alta velocidad a un sistema de CATV existente. Los operadores de cable utilizan DOCSIS para proporcionar acceso a Internet a través de la infraestructura de HFC existente.

DOCSIS especifica los requisitos de las capas 1 y 2 del modelo OSI:

- **Capa física:** para las señales de datos que el operador de cable puede utilizar, DOCSIS especifica los anchos de canal, o los anchos de banda de cada canal, en 200 kHz, 400 kHz, 800 kHz, 1,6 MHz, 3,2 MHz y 6,4 MHz. DOCSIS también especifica la técnica de modulación, que es la forma en que se utiliza la señal de RF para transmitir datos digitales.

- **Capa MAC:** define un método de acceso determinista, un acceso múltiple por división de tiempo (TDMA) o un acceso múltiple por división de código síncrono (S-CDMA).

Para comprender los requisitos de la capa MAC para DOCSIS, resulta útil explicar la forma en que las diversas tecnologías de comunicación dividen el acceso a los canales. TDMA divide el acceso por tiempo. El acceso múltiple por división de frecuencia (FDMA) divide el acceso por frecuencia. El acceso múltiple por división de código (CDMA) emplea tecnología de espectro ensanchado y un esquema de codificación especial en el que se asigna un código específico a cada transmisor.

Una analogía que ilustra estos conceptos puede ser una sala que representa un canal. La sala está llena de personas que necesitan comunicarse entre sí. Es decir, cada persona necesita acceso al canal. Una solución es que las personas se turnen para hablar (división por tiempo). Otra es que cada persona hable en diferentes tonos (división por frecuencia). En CDMA, las

personas hablarían en distintos idiomas. Las personas que hablan el mismo idioma pueden entenderse, pero no pueden entender a las demás. En CDMA de radio, que se utiliza en muchas redes norteamericanas de telefonía celular, cada grupo de usuarios tiene un código compartido. Muchos de los códigos ocupan el mismo canal, pero solo los usuarios asociados a un código específico pueden entenderse. S-CDMA es una versión exclusiva de CDMA desarrollada por Terayon Corporation para la transmisión de datos a través de redes de cable coaxial. S-CDMA dispersa los datos digitales por toda una banda de frecuencia ancha y permite que varios suscriptores conectados a la red transmitan y reciban simultáneamente. S-CDMA es seguro y extremadamente resistente al ruido.

Los planes de bandas de asignación de frecuencia difieren entre los sistemas de cable de América del Norte y Europa. Euro-DOCSIS se adaptó para el uso en Europa. Las diferencias principales entre DOCSIS y Euro-DOCSIS se relacionan con los anchos de banda de los canales. Los estándares técnicos de televisión varían en todo el mundo, lo que afecta la manera en que se desarrollan las variantes de DOCSIS. Los estándares internacionales de televisión incluyen NTSC en América del Norte 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.

Capítulo 6: Soluciones de banda ancha 6.2.1.4 Componentes del cable

La prestación de servicios mediante una red de cable requiere diferentes radiofrecuencias. Las frecuencias descendentes están en la banda de 50 MHz a 860 MHz, y las frecuencias ascendentes están en la banda de 5 MHz a 42 MHz.

Se requieren dos tipos de equipos para enviar señales de módem digitales de forma ascendente y descendente en un sistema de cable:

- El sistema de terminación de cable módem (CMTS) en la cabecera del operador de cable
- Un cable módem (CM) en el extremo del suscriptor

Haga clic en los componentes resaltados en la ilustración para obtener más información sobre la forma en que cada dispositivo contribuye a la comunicación.

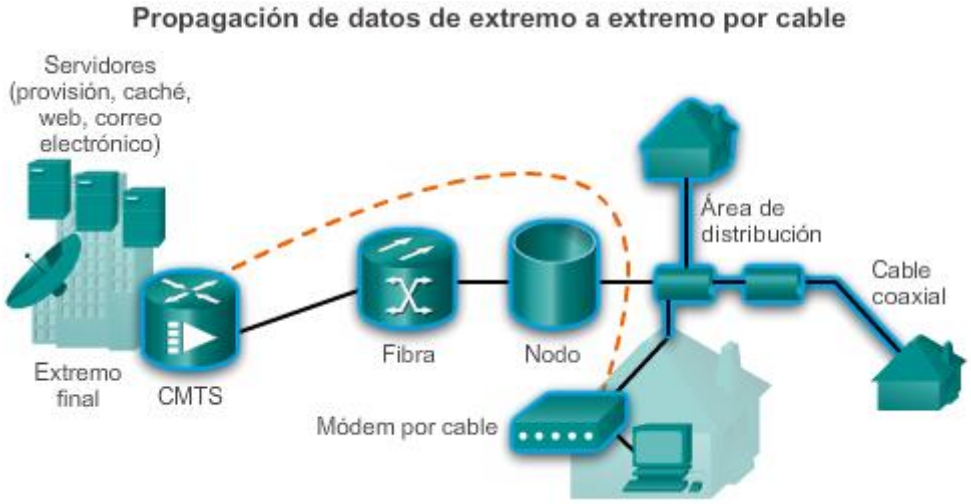
Un CMTS de cabecera se comunica con los CM ubicados en los hogares de los suscriptores. La cabecera es en realidad un router con las bases de datos para proporcionar servicios de Internet a los suscriptores del servicio de cable. La arquitectura es relativamente simple: se utiliza una red mixta óptica y coaxial en la que la fibra óptica reemplaza al cable coaxial, de ancho de banda inferior.

Una red de cables troncales de fibra óptica conecta la cabecera a los nodos donde ocurre la conversión de la señal óptica a una señal de RF. La fibra transporta el mismo contenido de banda ancha para las conexiones a Internet, el servicio telefónico y la transmisión de video que transporta el cable coaxial. Los cables de alimentación coaxial conectan el nodo a los suscriptores y transportan señales de RF.

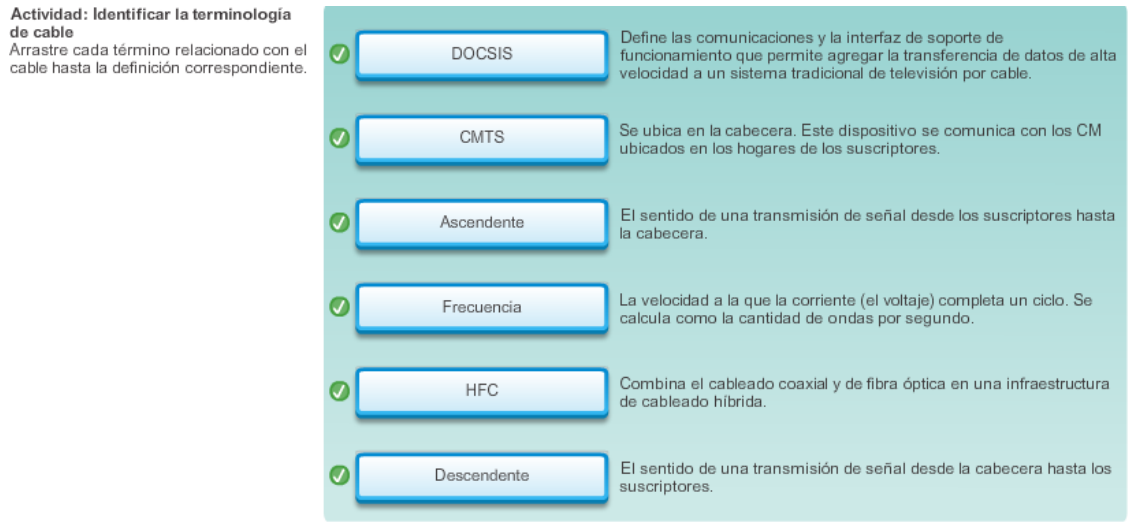
En una red HFC moderna, generalmente hay de 500 a 2000 suscriptores de servicios de datos activos conectados a un segmento de red de cable, y todos comparten el ancho de banda ascendente y descendente. El ancho de banda real para el servicio de Internet a través de una

línea de CATV puede ser de hasta 160 Mb/s descendentes con la última iteración de DOCSIS, y de hasta 120 Mb/s ascendentes.

Cuando se produce congestión por el uso elevado, el operador de cable puede agregar ancho de banda adicional para los servicios de datos mediante la asignación de un canal de televisión adicional para datos de alta velocidad. Esto puede duplicar eficazmente el ancho de banda descendente disponible para los suscriptores. Otra opción es reducir el número de suscriptores que reciben servicios de cada segmento de red. Para reducir el número de suscriptores, el operador de cable continúa subdividiendo la red al extender las conexiones de fibra óptica aún más en los vecindarios.



Capítulo 6: Soluciones de banda ancha 6.2.1.5 Actividad: Identificar la terminología de cable



Capítulo 6: Soluciones de banda ancha 6.2.2.1 ¿Qué es DSL?

DSL es un medio para proporcionar conexiones de alta velocidad a través de cables de cobre instalados. DSL es una de las soluciones clave disponibles para los trabajadores a distancia.

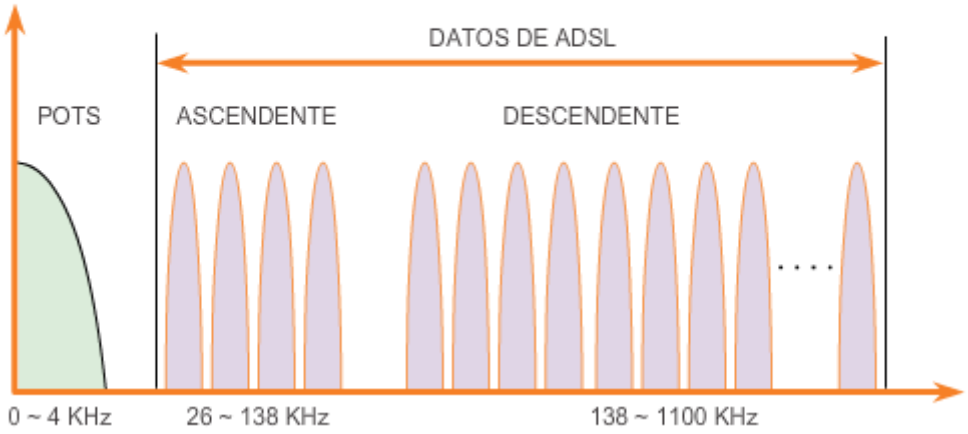
Hace varios años, Bell Labs identificó que una conversación de voz típica a través de un bucle local solo requería de 300 Hz a 3 kHz de ancho de banda. Durante muchos años, las redes telefónicas no utilizaron el ancho de banda superior a 3 kHz. Los avances tecnológicos permitieron que DSL utilizara el ancho de banda adicional desde 3 kHz hasta 1 MHz para proporcionar servicios de datos de alta velocidad mediante líneas de cobre comunes.

Como ejemplo, DSL asimétrico (ADSL) utiliza una banda de frecuencia de aproximadamente 20 kHz a 1 MHz. Afortunadamente, solo se requieren pequeños cambios en la infraestructura existente de la compañía telefónica para brindar velocidades de datos de ancho de banda elevado a los suscriptores. En la ilustración, se muestra una representación de la asignación de espacio de ancho de banda en un cable de cobre para ADSL. El área denominada POTS identifica la banda de frecuencia que utiliza el servicio de calidad telefónica. El área denominada ADSL representa el espacio de frecuencia que utilizan las señales DSL ascendentes y descendentes. El área que abarca tanto el área POTS como el área ADSL representa la totalidad de la banda de frecuencia admitida por el par de hilos de cobre.

DSL simétrico (SDSL) es otra forma de tecnología DSL. Todas las formas del servicio DSL se categorizan como ADSL o SDSL, y hay diferentes variedades de cada tipo. ADSL proporciona al usuario un ancho de banda descendente superior al ancho de banda de carga. SDSL proporciona la misma capacidad en ambas direcciones.

Las distintas variedades de DSL proporcionan diferentes anchos de banda, algunos con capacidades que exceden los 40 Mb/s. Las velocidades de transferencia dependen de la extensión real del bucle local (que conecta el suscriptor a la oficina central) y del tipo y la condición del cableado. Para lograr un servicio de ADSL satisfactorio, el bucle debe ser inferior a 3,39 mi (5,46 km).

DSL asimétrico en el espectro electromagnético



Capítulo 6: Soluciones de banda ancha 6.2.2.2 Conexiones DSL

Los proveedores de servicios implementan las conexiones DSL en el último paso de una red telefónica local, denominado “bucle local” o “última milla”. Se establece la conexión entre un par de módems en cualquiera de los extremos de un cable de cobre que se extiende entre el

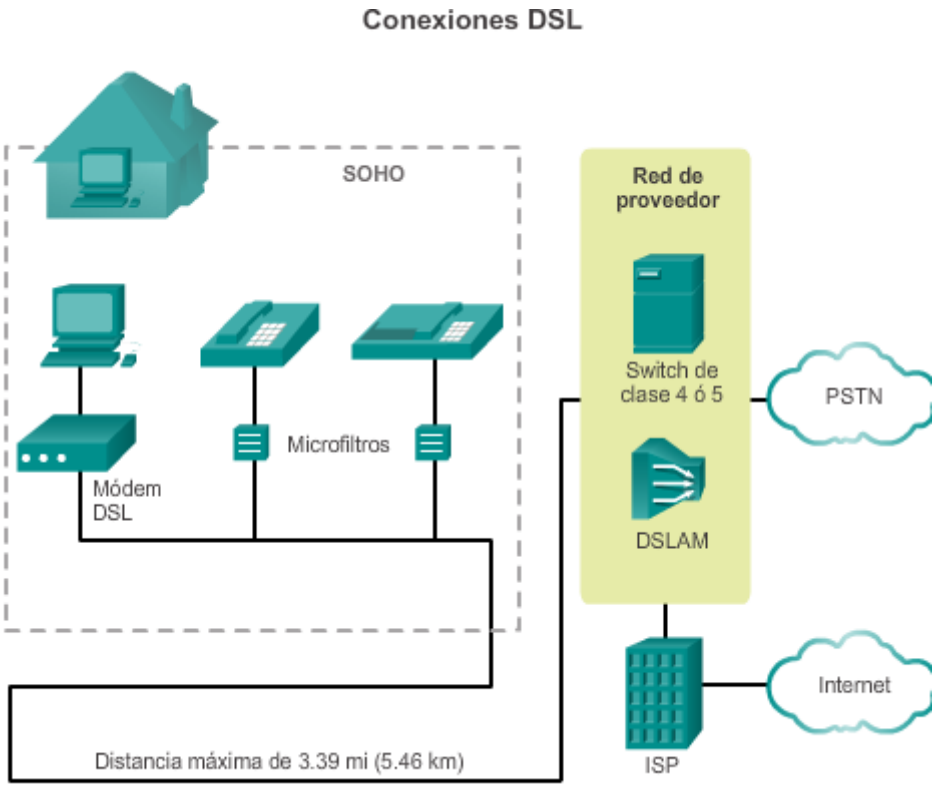
equipo local del cliente (CPE) y el multiplexor de acceso DSL (DSLAM). Un DSLAM es el dispositivo ubicado en la oficina central (CO) del proveedor y concentra las conexiones de varios suscriptores de DSL. Por lo general, un DSLAM está incorporado en un router de agregación.

En la figura 1, se muestra el equipo necesario para proporcionar una conexión DSL a una SOHO. Los dos componentes son el transceptor DSL y el DSLAM:

- **Transceptor:** conecta la computadora del trabajador a distancia al DSL. Generalmente, el transceptor es un módem DSL conectado a la computadora mediante un cable USB o Ethernet. Los transceptores DSL más modernos se pueden integrar a pequeños routers con varios puertos de switch 10/100 aptos para el uso en oficina doméstica.

- **DSLAM:** ubicado en la CO de la prestadora de servicios, el DSLAM combina las conexiones DSL individuales de los usuarios en un enlace de gran capacidad a un ISP y, por lo tanto, a Internet.

En la figura 2, se describen los routers DSL y los routers de agregación de banda ancha modernos. La ventaja que tiene DSL en comparación con la tecnología de cable es que DSL no es un medio compartido. Cada usuario tiene su propia conexión directa al DSLAM. El rendimiento no se ve afectado si se agregan usuarios, a menos que la conexión a Internet del DSLAM para el ISP o para Internet se sature.



Capítulo 6: Soluciones de banda ancha 6.2.2.3 Separación de voz y datos en ADSL

El principal beneficio de ADSL es la capacidad de proporcionar servicios de datos junto con servicios de voz POTS. Las transmisiones de las señales de voz y de datos se propagan a lo

largo del mismo par de hilos, como se muestra en la figura 1. Los circuitos de datos se descargan del switch de voz.

Cuando el proveedor de servicios coloca voz analógica y ADSL en el mismo par de hilos, las señales ADSL pueden distorsionar la transmisión de voz. Por este motivo, el proveedor divide el canal POTS del módem ADSL en las instalaciones del cliente con filtros o divisores. Esta configuración garantiza un servicio telefónico tradicional ininterrumpido incluso si falla ADSL. Si hay filtros o divisores, el usuario puede utilizar la línea telefónica y la conexión ADSL simultáneamente sin que se produzcan efectos adversos en ninguno de los servicios.

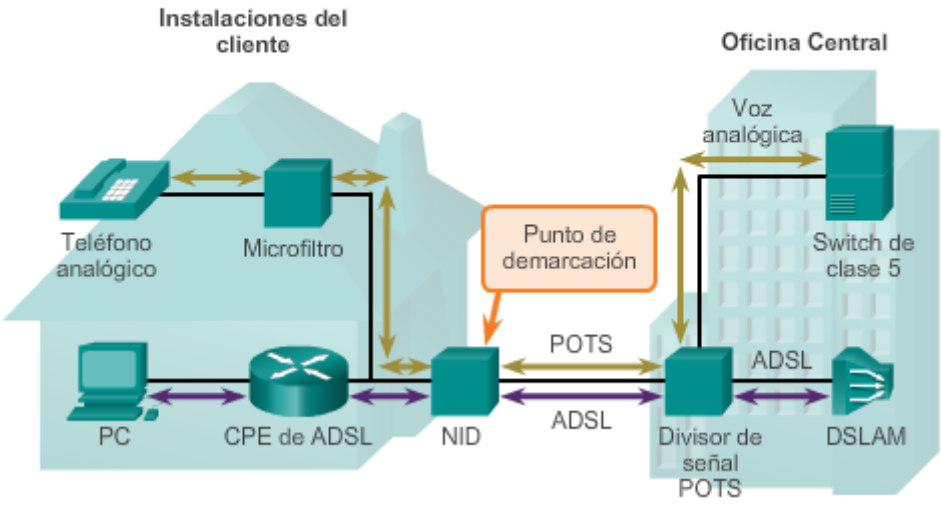
En la figura 1, se muestra el bucle local que termina en las instalaciones del cliente en el punto de demarcación. El punto de demarcación es aquel donde la línea telefónica ingresa a las instalaciones del cliente. El dispositivo que efectivamente marca el punto de demarcación es el dispositivo de interfaz de red (NID). En este punto, se puede conectar un divisor a la línea telefónica. El divisor bifurca la línea telefónica; una parte proporciona el cableado telefónico original de la casa para los teléfonos y la otra parte se conecta al módem ADSL. El divisor funciona como filtro de paso bajo, ya que solo permite que pasen las frecuencias de 0 kHz a 4 kHz desde o hacia el teléfono.

Existen dos formas de separar el servicio de ADSL del de voz en las instalaciones del cliente: mediante un microfiltro o un divisor.

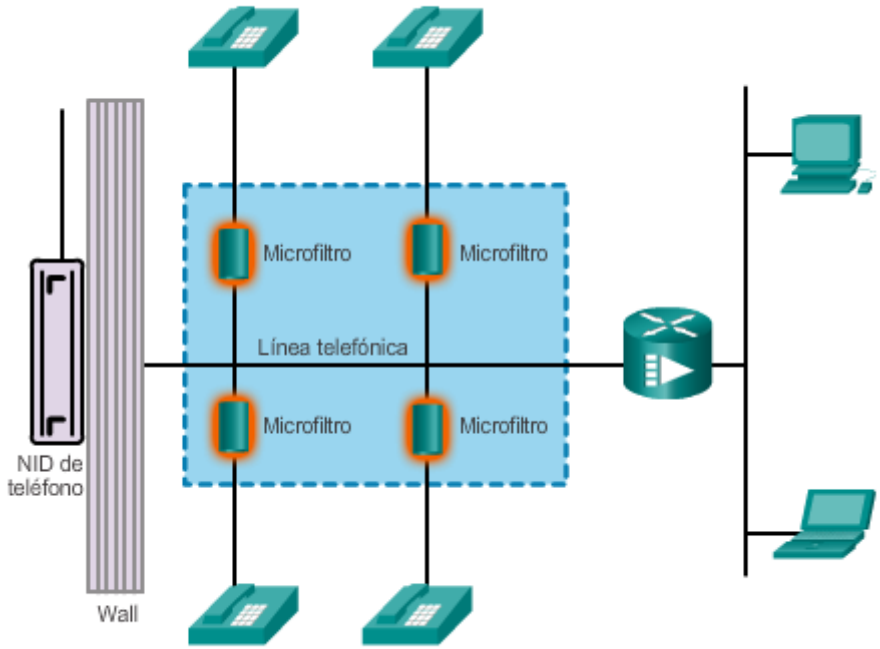
Un microfiltro es un filtro de paso bajo pasivo con dos extremos, como se muestra en la figura 2. Un extremo se conecta al teléfono y el otro extremo se conecta al conector de pared del teléfono. Haga clic en el área resaltada en la figura 2 para ver la imagen de un microfiltro. Esta solución permite que el usuario utilice cualquier conector en la casa para los servicios de voz o ADSL.

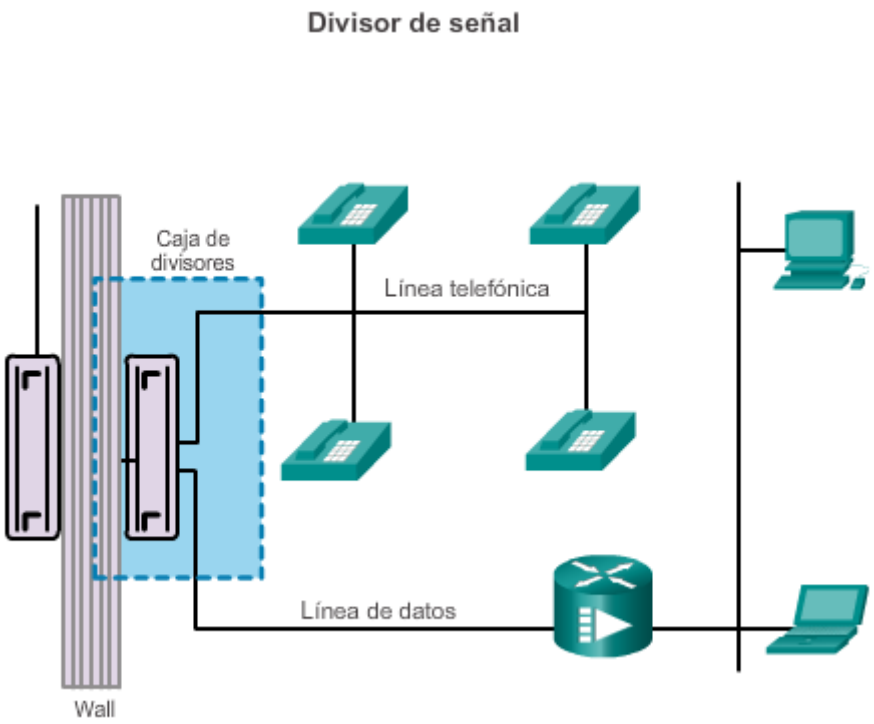
Un divisor de señal POTS, que se muestra en la figura 3, separa el tráfico DSL del tráfico POTS. El divisor de señal POTS es un dispositivo pasivo. Haga clic en el área resaltada en la figura 3 para ver el diagrama de un divisor. En caso de un corte de energía, el tráfico de voz continúa viajando hacia el switch de voz en la CO de la prestadora de servicios. Los divisores están ubicados en la CO y, en algunas implementaciones, en las instalaciones del cliente. En la CO, el divisor de señal POTS separa el tráfico de voz, destinado a las conexiones POTS, y el tráfico de datos, destinado al DSLAM. La instalación del divisor de señal POTS en el NID generalmente requiere que un técnico vaya al sitio del cliente.

Separación de voz y datos en ADSL



Microfiltros





Capítulo 6: Soluciones de banda ancha 6.2.2.4 Actividad: Identificar la terminología de DSL

Capítulo 6: Soluciones de banda ancha 6.2.3.1 Tipos de tecnologías inalámbricas de banda ancha

En lugar de la conectividad por cable y DSL, hoy en día muchos usuarios optan por la conectividad inalámbrica.

El alcance de las conexiones inalámbricas ahora incluye las redes de área personal, las LAN y las WAN. La cantidad de zonas de cobertura inalámbrica aumentó el acceso a las conexiones inalámbricas en todo el mundo. Una zona de cobertura inalámbrica es el área que cubren uno o

más puntos de acceso interconectados. Los puntos de encuentro públicos, como las cafeterías, los bares y las bibliotecas, tienen zonas de cobertura inalámbrica Wi-Fi. Si se superponen puntos de acceso, las zonas de cobertura inalámbrica pueden abarcar muchas millas cuadradas.

Los desarrollos en la tecnología inalámbrica de banda ancha aumentan la disponibilidad inalámbrica. Estos tipos de banda ancha se explican en la figura 1 e incluyen lo siguiente:

- Wi-Fi municipal (malla)
- WiMAX (Interoperabilidad mundial para el acceso por microondas)
- Datos móviles
- Internet satelital

Wi-Fi municipal

Muchos gobiernos municipales, que suelen trabajar con proveedores de servicios, implementan redes inalámbricas. Algunas de estas redes proporcionan acceso a Internet de alta velocidad sin costo o por un precio considerablemente inferior al de otros servicios de banda ancha. Otras ciudades reservan las redes Wi-Fi para uso oficial, a fin de proporcionar acceso remoto a Internet y a las redes municipales para la policía, los bomberos y los empleados de mantenimiento de espacios públicos.

La mayoría de las redes inalámbricas municipales utilizan una topología de malla en lugar de un modelo hub-and-spoke. Una malla es una serie de puntos de acceso interconectados, como se muestra en la figura 2. Cada punto de acceso está al alcance y puede comunicarse con al menos otros dos puntos de acceso. La malla cubre su área con señales de radio. Las señales viajan de un punto de acceso a otro a través de esta nube.

Una red de malla tiene varias ventajas en comparación con una zona de cobertura inalámbrica con un único router. La instalación es más fácil y puede ser más económica, dado que hay menos cables. La implementación en un área urbana grande es más rápida y confiable. Si falla un nodo, el resto de los nodos en la malla lo compensan.

WiMAX

WiMAX, que se muestra en la figura 3, es una tecnología de telecomunicaciones cuyo propósito es proporcionar datos inalámbricos a través de largas distancias de diversas maneras, desde enlaces punto a punto hasta acceso de tipo de datos móviles. WiMAX funciona a velocidades más altas, a mayores distancias y para una mayor cantidad de usuarios que Wi-Fi. Debido a la mayor velocidad (ancho de banda) y a la caída en los precios de los componentes, se predice que WiMAX pronto reemplazará las redes de malla municipales para las implementaciones inalámbricas.

Una red WiMAX consta de dos componentes principales:

- Una torre cuyo concepto es similar al de una torre de telefonía móvil. Una única torre WiMAX puede proporcionar cobertura a un área de hasta 3000 mi cuadradas (7500 km cuadrados).

- Un receptor WiMAX conectado a un puerto USB o incorporado a la computadora portátil u otro dispositivo inalámbrico.

Una estación de torre WiMAX se conecta directamente a Internet mediante una conexión de ancho de banda elevado, como una línea T3. Una torre también se puede conectar a otras torres WiMAX mediante enlaces de microondas con línea de vista. Por lo tanto, WiMAX puede proporcionar cobertura a las áreas rurales fuera del alcance de las tecnologías de DSL y de cable de última milla.

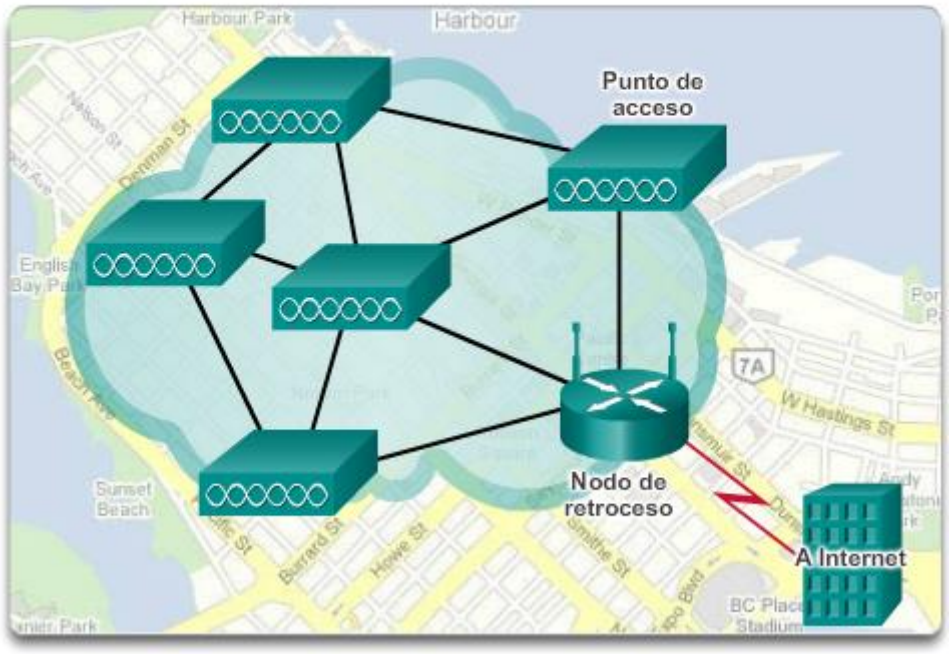
- Estándares IEEE 802.11 comúnmente denominados "Wi-Fi".
- Las implementaciones de Wi-Fi municipal utilizan una topología de malla, con un punto de acceso en cada nodo.
- Las variantes incluyen 802.11a/b/g/n/ac/ad.
- Admite velocidades de hasta 7Gb/s.

- Estándar IEEE 802.16 comúnmente denominado "WiMAX".
- Utiliza una topología de punto a multipunto para proporcionar acceso celular de banda ancha inalámbrica.
- Admite velocidades de hasta 1Gb/s.

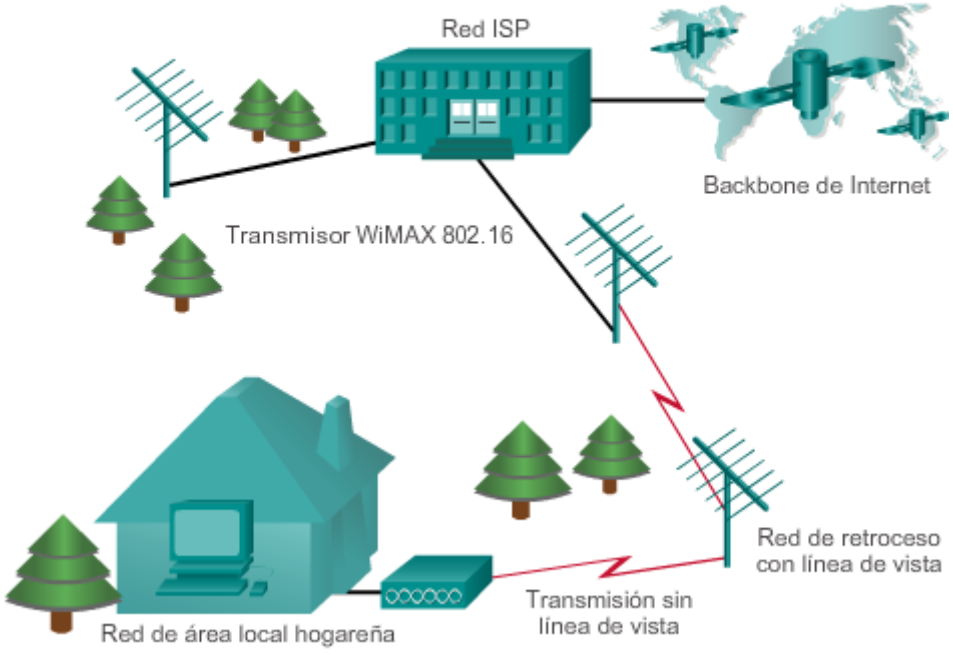
- El acceso de banda ancha móvil consta de diversos estándares que admiten velocidades de hasta 5Mb/s.
- Las variantes incluyen 2G (con GSM, CDMA o TDMA), 3G (con UMTS, CDMA2000, EDGE o HSPA+) y 4G (con WiMAX o LTE).

- La comunicación satelital se produce mediante una antena parabólica direccional alineada con un satélite GEO.
- Ideal en situaciones tales como las de áreas remotas donde no hay otro acceso inalámbrico disponible.
- Admite velocidades de descarga de hasta 10Mb/s.

Implementación de Wi-Fi municipal (malla)



Implementación de WiMax



Capítulo 6: Soluciones de banda ancha 6.2.3.2 Tipos de tecnologías inalámbricas de banda ancha (cont.)

Implementaciones de datos móviles

La banda ancha móvil se refiere al acceso a Internet inalámbrico que se entrega a través de las torres de telefonía móvil a las computadoras, los teléfonos móviles y otros dispositivos digitales mediante módems portátiles. En la figura 1, se muestra una torre de telefonía móvil utilizada en una red de banda ancha móvil.

Los teléfonos celulares usan ondas de radio para comunicarse mediante una torre de telefonía móvil cercana. El teléfono móvil tiene una pequeña antena de radio. El proveedor tiene una antena mucho más grande en la parte superior de una torre, como la que se muestra en la ilustración.

El acceso de banda ancha móvil consta de diversos estándares que admiten velocidades de hasta 5 Mb/s. Las variantes incluyen 2G (con GSM, CDMA o TDMA), 3G (con UMTS, CDMA2000, EDGE o HSPA+) y 4G (con WiMAX o LTE). La suscripción al servicio de telefonía móvil no incluye la suscripción a la banda ancha móvil necesariamente.

Tres términos comunes que se utilizan al analizar las redes de datos móviles incluyen lo siguiente:

- **Internet inalámbrica:** es un término general para los servicios de Internet de un teléfono móvil o cualquier dispositivo que utilice la misma tecnología.

- **Redes inalámbricas 2G/3G/4G:**cambios importantes en las redes inalámbricas de las compañías de telefonía móvil a través de la evolución de la segunda, la tercera y la cuarta generación de tecnologías móviles inalámbricas.

- **Evolución a largo plazo (LTE):** una tecnología más nueva y más rápida que se considera parte de la tecnología 4G.

Implementaciones satelitales

Los servicios de Internet satelital se utilizan en lugares que no cuentan con acceso a Internet basado en tierra o para instalaciones temporales que son móviles. El acceso a Internet mediante satélites está disponible en todo el mundo, incluso para proporcionar acceso a Internet a las embarcaciones en el mar, a los aviones durante el vuelo y a los vehículos en tránsito.

Existen tres maneras de conectarse a Internet mediante satélites:

- **Multidifusión unidireccional:** los sistemas de Internet satelital se utilizan para la distribución de datos, audio y video basada en multidifusión IP. Si bien la mayoría de los protocolos IP requieren una comunicación bidireccional para el contenido de Internet, incluidas las páginas web, los servicios de Internet unidireccionales basados en satélites pueden utilizarse para insertar páginas en el almacenamiento local en los sitios de usuarios finales. La interactividad bidireccional no es posible.

- **Retorno terrestre unidireccional:** los sistemas de Internet satelital utilizan el acceso por dial-up tradicional para enviar datos salientes a través de un módem y recibir descargas del satélite.

- **Internet satelital bidireccional:** envía datos de sitios remotos por el satélite a un hub, que después envía los datos a Internet. La antena parabólica en cada ubicación se debe posicionar de forma precisa para evitar la interferencia con otros satélites.

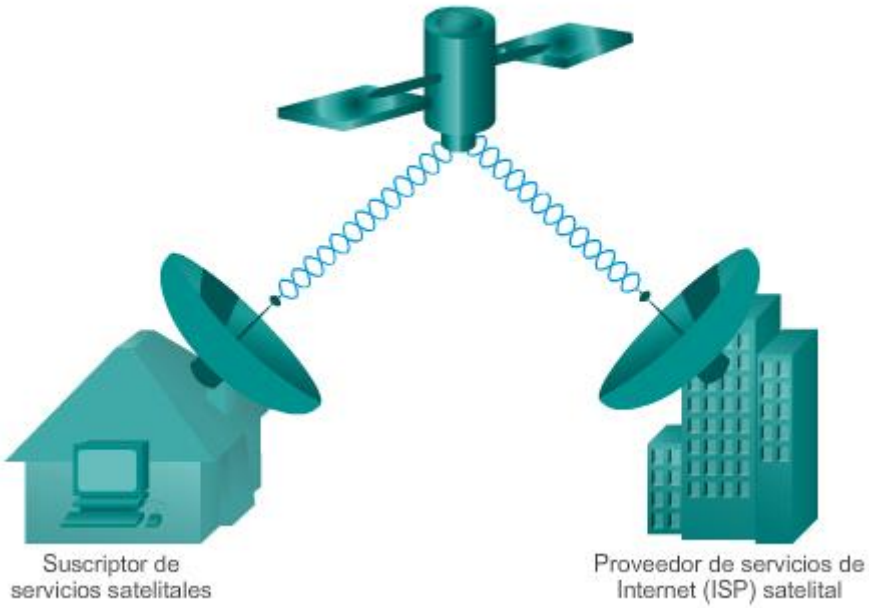
En la figura 2, se muestra un sistema de Internet satelital bidireccional. Las velocidades de subida son aproximadamente un décimo de la velocidad de descarga, que está alrededor de los 500 kb/s.

El principal requisito para la instalación es que la antena tenga una vista despejada hacia el ecuador, donde se ubica la mayoría de los satélites que están en órbita. Los árboles y las lluvias torrenciales pueden afectar la recepción de las señales.

La tecnología de Internet satelital bidireccional utiliza la tecnología de multidifusión IP, que permite que un satélite cubra hasta 5000 canales de comunicación simultáneamente. La multidifusión IP envía datos desde un punto hacia muchos puntos a la vez mediante el envío de datos en formato comprimido. La compresión reduce el tamaño de los datos y los requisitos de ancho de banda.

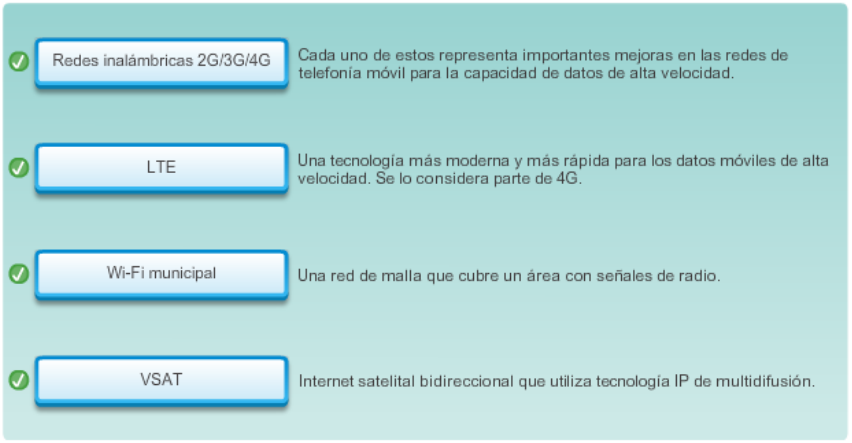
Una empresa puede crear una WAN privada mediante las comunicaciones satelitales y terminales de apertura muy pequeña (VSAT). Una VSAT es un tipo de antena parabólica similar a las que se utilizan para la televisión satelital en el hogar y, por lo general, mide alrededor de 1 m de ancho. La antena VSAT se ubica afuera, apuntando hacia un satélite específico, y se conecta a una interfaz de router especial. El router se coloca dentro del edificio. Mediante las VSAT se crea una WAN privada.

Implementación satelital bidireccional



Capítulo 6: Soluciones de banda ancha 6.2.3.3 Actividad: Identificar la terminología de tecnología inalámbrica de banda ancha

Actividad: Identificar la terminología de tecnología inalámbrica de banda ancha
Arrastre cada término relacionado con la tecnología inalámbrica de banda ancha hasta la definición correspondiente.



Capítulo 6: Soluciones de banda ancha 6.2.4.1 Comparación de las soluciones de banda ancha

Todas las soluciones de banda ancha tienen ventajas y desventajas. Lo ideal es tener un cable de fibra óptica conectado directamente a la red SOHO. En algunas ubicaciones, solo es posible una opción, como el cable o DSL. Algunas ubicaciones cuentan solamente con opciones de tecnología inalámbrica de banda ancha de conectividad a Internet.

Si hay varias soluciones de banda ancha disponibles, se debe llevar a cabo un análisis de costos y beneficios para determinar cuál es la mejor solución.

Algunos factores para tener en cuenta al tomar una decisión incluyen lo siguiente:

- **Cable:** el ancho de banda se comparte con muchos usuarios; las velocidades de datos ascendentes suelen ser lentas.
- **DSL:** el ancho de banda es limitado y se ve afectado por la distancia; la velocidad ascendente es proporcionalmente muy pequeña en comparación con la velocidad descendente.
- **Fibra hasta el hogar:** requiere la instalación de la fibra directamente en el hogar (como se muestra en la ilustración).
- **Datos móviles:** la cobertura a menudo representa un problema; incluso dentro de una SOHO, el ancho de banda es relativamente limitado.
- **Malla Wi-Fi:** la mayoría de las municipalidades no cuentan con la implementación de una red de malla; si está disponible y la SOHO está dentro del alcance, entonces es una opción viable.
- **WiMAX:** la velocidad de bits se limita a 2 Mb/s por suscriptor; el tamaño de las celdas es de 1 km a 2 km (1,25 mi).
- **Satélite:** es costoso, tiene una capacidad limitada por suscriptor, suele proporcionar acceso donde no hay posibilidad de ningún otro tipo de acceso.

Capítulo 6: Soluciones de banda ancha 6.2.4.2 Práctica de laboratorio: Investigación de las tecnologías de acceso a Internet por banda ancha

En esta práctica de laboratorio, cumplirá los siguientes objetivos:

- Parte 1: Investigar la distribución de banda ancha
- Parte 2: Investigar las opciones de acceso por banda ancha para situaciones específicas

Práctica de laboratorio: Investigación de las tecnologías de acceso a Internet por banda ancha

Capítulo 6: Soluciones de banda ancha 6.3.1.1 Motivación para el uso de PPPoE

Además de comprender las diversas tecnologías disponibles para el acceso a Internet de banda ancha, también es importante comprender el protocolo de capa de enlace de datos subyacente que utiliza el ISP para formar una conexión.

Un protocolo de capa de enlace de datos que usan generalmente los ISP es el protocolo punto a punto (PPP). PPP se puede utilizar en todos los enlaces seriales, incluidos aquellos enlaces creados con módems de dial-up analógicos e ISDN. Actualmente, es probable que el enlace que va de un usuario de dial-up a un ISP mediante módems analógicos utilice PPP. En la figura 1, se muestra una representación básica de esa conexión de dial-up analógico con PPP.

Además, los ISP suelen usar PPP como protocolo de enlace de datos a través de las conexiones de banda ancha. Esto se debe a varios motivos. En primer lugar, PPP admite la capacidad de asignar direcciones IP a los extremos remotos de un enlace PPP. Cuando PPP está habilitado, los ISP pueden utilizarlo para asignar una dirección IPv4 pública a cada cliente. Lo más importante es que PPP admite la autenticación CHAP. A menudo, los ISP prefieren utilizar CHAP para autenticar a los clientes, ya que, durante la autenticación, los ISP pueden revisar los registros contables para determinar si el cliente pagó la factura antes de permitirle conectarse a Internet.

Estas tecnologías salieron al mercado en el siguiente orden, con una compatibilidad variable para PPP:

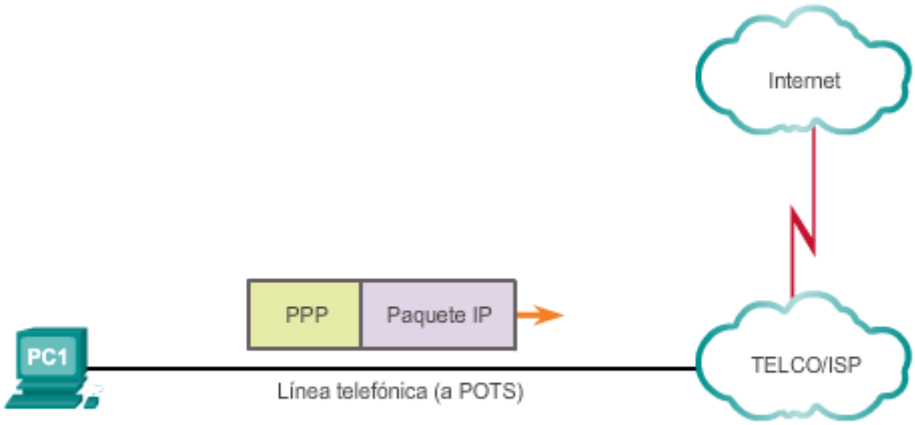
1. Módems análogos para dial-up que podían utilizar PPP y CHAP

2. ISDN para dial-up que podían utilizar PPP y CHAP

3. DSL, que no establecía un enlace punto a punto y no admitía PPP ni CHAP

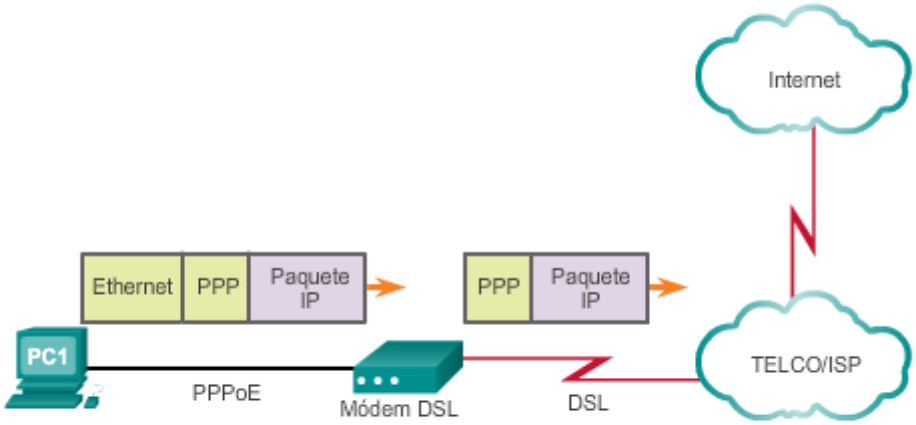
Los ISP consideran que PPP es valioso debido a las características de autenticación, contabilidad y administración de enlaces. Los clientes valoran la facilidad y la disponibilidad de la conexión Ethernet. Sin embargo, los enlaces Ethernet no admiten PPP de forma nativa. Como solución a este problema, se creó PPP por Ethernet (PPPoE). Como se muestra en la figura 2, PPPoE permite el envío de tramas PPP encapsuladas dentro de tramas de Ethernet.

Tramas PPP a través de una conexión de dial-up antigua



En una situación de dial-up antiguo, la PC1 llega a Internet a través de la nube TELCO/ISP mediante un dispositivo FAX/MÓDEM.

Tramas PPP a través de una conexión Ethernet (PPPoE)

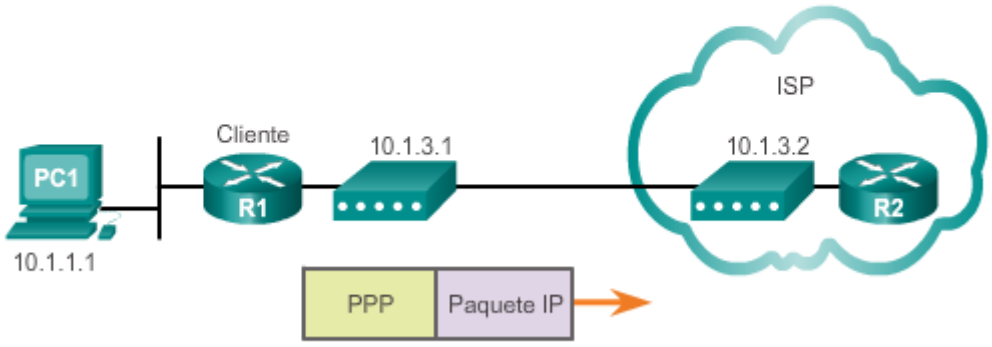


La PC1 se conecta directamente a un módem DSL. Mediante el uso del software adecuado (generalmente, un marcador o un cliente DLS que proporciona el ISP), la PC1 encapsula tramas PPP dentro de las tramas de Ethernet y las envía al módem DSL.

Capítulo 6: Soluciones de banda ancha 6.3.1.2 Conceptos de PPPoE

Como se muestra en la ilustración, el router del cliente generalmente está conectado a un módem DSL mediante un cable Ethernet. PPPoE crea un túnel PPP a través de una conexión Ethernet. Esto permite que las tramas PPP se envíen a través de un cable Ethernet hasta el ISP desde el router del cliente. El módem convierte las tramas de Ethernet en tramas PPP mediante la eliminación de los encabezados Ethernet. Después, el módem transmite estas tramas PPP en la red DSL del ISP.

Tunneling para crear un enlace PPP por Ethernet



Capítulo 6: Soluciones de banda ancha 6.3.2.1 Configuración de PPPoE

Con la capacidad de enviar y recibir tramas PPP entre los routers, el ISP puede seguir utilizando el mismo modelo de autenticación que con los módems analógicos e ISDN. Para que todo funcione, los routers cliente e ISP necesitan una configuración adicional, incluida la configuración de PPP. Para comprender la configuración, tenga en cuenta lo siguiente:

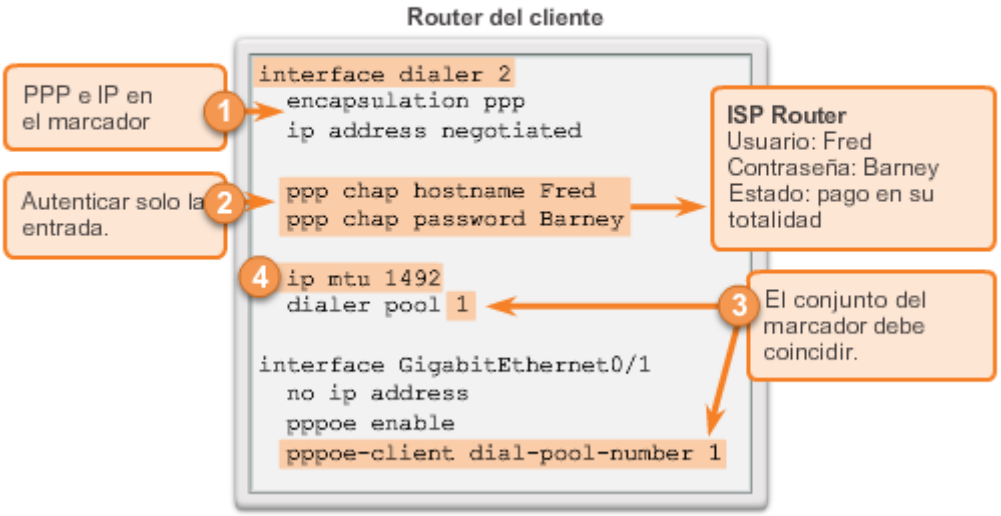
1. Para crear un túnel PPP, la configuración utiliza una interfaz de marcador. Una interfaz de marcador es una interfaz virtual. La configuración de PPPoE se ubica en la interfaz del marcador, no en la interfaz física. La interfaz del marcador se crea mediante el comando **interface dialer***número*. El cliente puede configurar una dirección IP estática, pero es más probable que el ISP le asigne automáticamente una dirección IP pública.

2. En general, la configuración de CHAP de PPP define la autenticación unidireccional; por lo tanto, el ISP autentica al cliente. El nombre de host y la contraseña configurados en el router del cliente deben coincidir con el nombre de host y la contraseña configurados en el router ISP. Observe en la ilustración que el nombre de usuario y la contraseña de CHAP coinciden con la configuración del router ISP.

3. La interfaz Ethernet física que se conecta al módem DSL se habilita con el comando **pppoe enable**, que habilita PPPoE y enlaza la interfaz física a la interfaz del marcador. La interfaz del marcador se enlaza a la interfaz Ethernet mediante los comandos **dialer pool** y**pppoe-client** con el mismo número. El número de la interfaz del marcador no tiene que coincidir con el número de conjunto del marcador.

4. Para admitir los encabezados PPPoE, la unidad máxima de transmisión (MTU) se debe establecer en 1492, en lugar del valor predeterminado 1500.

Ejemplo de configuración de PPPoE



Capítulo 6: Soluciones de banda ancha 6.3.2.2 Verificador de sintaxis: configuración de PPPoE

Configuración de PPPoE

El router ISP se configuró con los siguientes parámetros:

- Nombre de usuario: customer2222
- Contraseña: ConnectMe

Configure la interfaz virtual del marcador 5 en el siguiente orden:

- Cree la interfaz virtual del marcador 5.
- Establezca la encapsulación en PPP.
- Negocie la dirección IP del ISP.
- Reduzca la MTU a 1492 para admitir los encabezados PPP.
- Cree el conjunto del marcador 5.
- Implemente la autenticación CHAP; utilice el nombre de usuario que le proporcionó el ISP.
- Asigne la contraseña de CHAP que le proporcionó el ISP.
- Active la interfaz.

```
R1(config)# interface dialer 5
R1(config-if)# encapsulation ppp
R1(config-if)# ip address negotiated
R1(config-if)# ip mtu 1492
R1(config-if)# dialer pool 5
R1(config-if)# ppp chap hostname customer2222
R1(config-if)# ppp chap password ConnectMe
R1(config-if)# no shutdown:
*Jul 5 15:02:54.207: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Virtual-Access1, changed state to up
*Jul 5 15:02:54.207: %LINK-3-UPDOWN: Interface Virtual-Access1,
changed state to up
```

Configure la conexión DSL al ISP en GigabitEthernet 0/0 en el siguiente orden:

- Elimine cualquier dirección IP asignada.
- Habilite PPPoE.
- Configure la interfaz para que sea un cliente PPPoE con el número de conjunto del marcador creado en la interfaz del marcador.
- Active la interfaz.
- Vuelva al modo EXEC privilegiado.

```
R1(config-if)# interface GigabitEthernet 0/0
R1(config-if)# no ip address
R1(config-if)# pppoe enable
R1(config-if)# pppoe-client dial-pool-number 5
R1(config-if)# no shutdown:
*Jul 5 15:03:01.359: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/0, changed state to up
R1(config-if)# end
```

Muestre el estado resumido de la interfaz.

```
R1# show ip interface brief
Interface          IP-Address   OK?  Method  Status   Protocol
GigabitEthernet0/0 unassigned   YES  NVRAM   up       up
GigabitEthernet0/1 172.16.1.1   YES  manual  up       up
Dialer5            64.100.10.1 YES  manual  up       up
Virtual-Access1    unassigned   YES  unset   up       up
```

Configuró correctamente PPPoE en el router R1 del cliente.

Capítulo 6: Soluciones de banda ancha 6.3.2.3 Práctica de laboratorio: Configuración de un router como cliente PPPoE para la conectividad DSL

En esta práctica de laboratorio, cumplirá los siguientes objetivos:

- Parte 1: Armar la red
- Parte 2: Configurar el router ISP
- Parte 3: Configurar el router Cliente1

Práctica de laboratorio: Configuración de un router como cliente PPPoE para la conectividad DSL

Capítulo 6: Soluciones de banda ancha 6.4.1.1 Actividad de clase: Propuesta de trabajo a distancia

Propuesta de trabajo a distancia

Se acaba de adjudicar un contrato grande de diseño de marketing a su pequeña o mediana empresa. Debido a que el espacio de la oficina es limitado, se recomendó contratar trabajadores a distancia para ayudar en el contrato.

Por lo tanto, se debe diseñar un programa muy general de trabajo a distancia para la empresa, ya que se anticipa que esta crezca. A medida que se adjudiquen más contratos, revise y expanda el programa para que se ajuste a las necesidades de la empresa.

Elabore una descripción básica de la propuesta de trabajo a distancia para que la empresa la tenga en cuenta como base para un programa de trabajo a distancia.

Actividad de clase: Propuesta de trabajo a distancia

Capítulo 6: Soluciones de banda ancha 6.4.1.2 Resumen

La transmisión de banda ancha se proporciona mediante una amplia variedad de tecnologías, como la línea de suscriptor digital (DSL), la fibra hasta el hogar, los sistemas de cable coaxial, la tecnología inalámbrica y satelital. Esta transmisión requiere componentes adicionales en el extremo del hogar y en el de la empresa.

DOCSIS es un estándar de CableLabs que permite agregar transferencia de datos de alta velocidad a un sistema de CATV existente. El ancho de banda para el servicio de Internet a través de una línea de CATV puede ser de hasta 160 Mb/s descendentes con la última iteración de DOCSIS, y de hasta 120 Mb/s ascendentes, de forma simultánea. Requiere el uso de un sistema de terminación de cable módem (CMTS) en la cabecera del operador de cable y un cable módem (CM) en el extremo del suscriptor.

Los dos tipos básicos de tecnologías DSL son ADSL y DSL simétrica (SDSL). ADSL proporciona al usuario un ancho de banda descendente superior al ancho de banda de carga. SDSL proporciona la misma capacidad en ambas direcciones. DSL puede proporcionar un ancho de banda que excede los 40 Mbps. DSL requiere el uso de un DSLAM en la CO de la

prestadora de servicios y un transceptor, generalmente incorporado a un router doméstico, en el extremo del cliente.

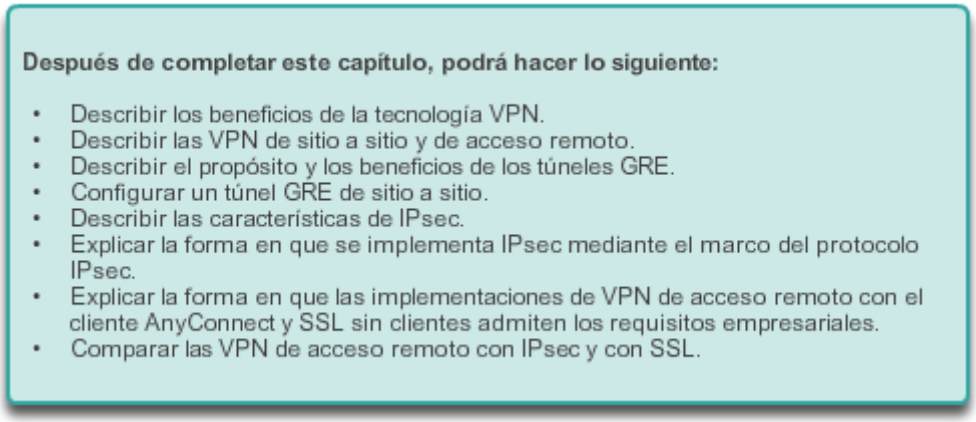
Las soluciones inalámbricas de banda ancha incluyen Wi-Fi municipal, WiMAX, datos móviles e Internet satelital. Las redes de malla de Wi-Fi municipal no se utilizan a gran escala. La velocidad de bits de WiMAX se limita a 2 Mbps por suscriptor. La cobertura de datos móviles puede ser limitada, por lo que el ancho de banda puede ser un problema. La tecnología de Internet satelital es relativamente costosa y limitada, pero puede ser el único método para proporcionar acceso.

Si hay varias conexiones de banda ancha disponibles para una ubicación determinada, se debe llevar a cabo un análisis de costos y beneficios para determinar cuál es la mejor solución. Puede ser que la mejor solución sea conectarse a varios proveedores de servicios para proporcionar redundancia y confiabilidad.

Capítulo 7: Seguridad de la conectividad Site-to-Site 7.0.1.1 Introducción

La seguridad es un motivo de preocupación cuando se utiliza Internet pública para realizar negocios. Las redes virtuales privadas (VPN) se utilizan para garantizar la seguridad de los datos a través de Internet. Una VPN se utiliza para crear un túnel privado a través de una red pública. Se puede proporcionar seguridad a los datos mediante el uso de cifrado en este túnel a través de Internet y con autenticación para proteger los datos contra el acceso no autorizado.

En este capítulo, se explican los conceptos y los procesos relacionados con las VPN, así como los beneficios de las implementaciones de VPN y los protocolos subyacentes requeridos para configurar las VPN.



Capítulo 7: Seguridad de la conectividad Site-to-Site 7.0.1.2 Actividad de clase: Resumen sobre las VPN

Resumen sobre las VPN

Una pequeña o mediana empresa crece y necesita que los clientes, los trabajadores a distancia y los empleados que se conectan por cable y de forma inalámbrica puedan acceder a la red principal desde cualquier ubicación. Como administrador de red de la empresa, usted

decidió implementar las VPN para aportar seguridad, facilitar el acceso a la red y ahorrar costos.

Su trabajo es asegurar que todos los administradores de red comiencen el proceso de planificación de VPN con el mismo conjunto de conocimientos.

Se deben investigar cuatro áreas informativas básicas de VPN, y dichas áreas se deben presentar al equipo de administración de la red:

- Definición concisa de las VPN
- Algunos datos generales sobre las VPN
- IPsec como opción de seguridad de VPN
- Formas en las que las VPN usan el tunneling

Actividad de clase: Resumen sobre las VPN

Capítulo 7: Seguridad de la conectividad Site-to-Site 7.1.1.1 Introducción a las VPN

Las organizaciones necesitan redes seguras, confiables y rentables para interconectar varias redes, por ejemplo, para permitir que las sucursales y los proveedores se conecten a la red de la oficina central de una empresa. Además, con el aumento en la cantidad de trabajadores a distancia, hay una creciente necesidad de las empresas de contar con formas seguras, confiables y rentables para que los empleados que trabajan en oficinas pequeñas y oficinas domésticas (SOHO), y en otras ubicaciones remotas se conecten a los recursos en sitios empresariales.

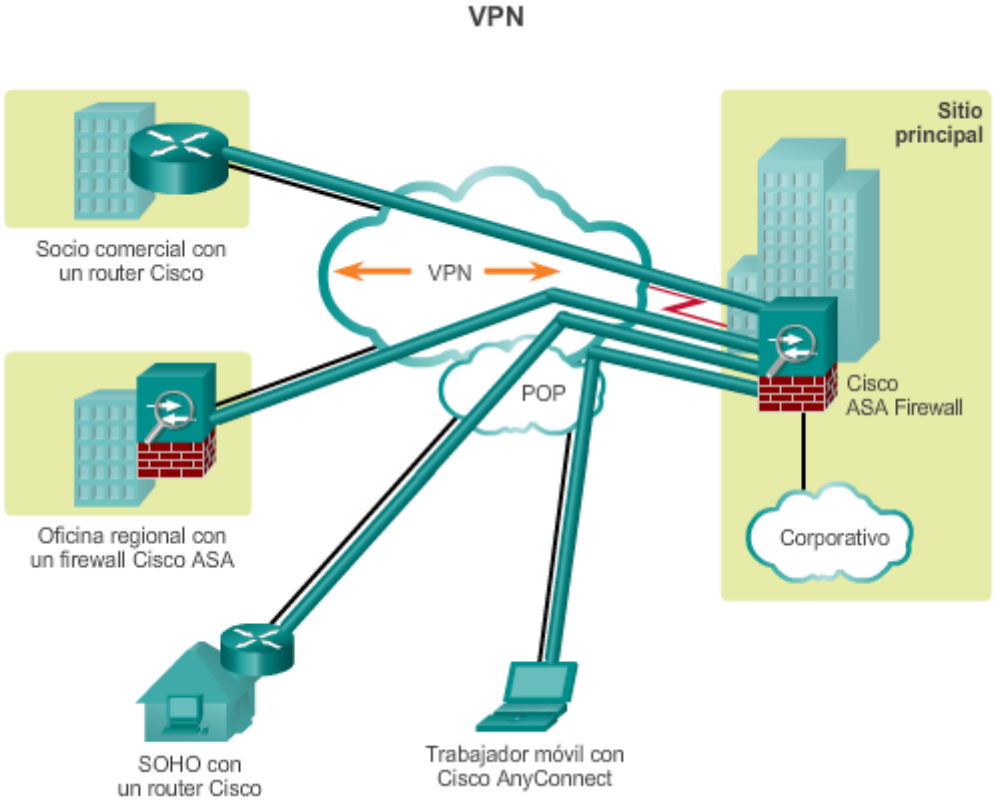
En la ilustración, se muestran las topologías que utilizan las redes modernas para conectar ubicaciones remotas. En algunos casos, las ubicaciones remotas se conectan solo a la oficina central, mientras que en otros casos, las ubicaciones remotas se conectan a sitios adicionales.

Las organizaciones utilizan las VPN para crear una conexión de red privada de extremo a extremo a través de redes externas como Internet o las extranets. El túnel elimina la barrera de distancia y permite que los usuarios remotos accedan a los recursos de red del sitio central. Una VPN es una red privada creada mediante tunneling a través de una red pública, generalmente Internet. Una VPN es un entorno de comunicaciones en el que el acceso se controla de forma estricta para permitir las conexiones de peers dentro de una comunidad de interés definida.

Las primeras VPN eran exclusivamente túneles IP que no incluían la autenticación o el cifrado de los datos. Por ejemplo, la encapsulación de routing genérico (GRE) es un protocolo de tunneling desarrollado por Cisco que puede encapsular una amplia variedad de tipos de paquetes de protocolo de capa de red dentro de los túneles IP. Esto crea un enlace virtual punto a punto a los routers Cisco en puntos remotos a través de una internetwork IP.

En la actualidad, las redes privadas virtuales generalmente se refieren a la implementación segura de VPN con cifrado, como las VPN con IPsec.

Para implementar las VPN, se necesita un gateway VPN. El gateway VPN puede ser un router, un firewall o un dispositivo de seguridad adaptable (ASA) de Cisco. Un ASA es un dispositivo de firewall independiente que combina la funcionalidad de firewall, concentrador VPN y prevención de intrusiones en una imagen de software.



Capítulo 7: Seguridad de la conectividad Site-to-Site 7.1.1.2 Beneficios de las VPN

Como se muestra en la ilustración, una VPN utiliza conexiones virtuales que se enrutan a través de Internet desde la red privada de una organización hasta el sitio remoto o el host del empleado. La información de una red privada se transporta de manera segura a través de la red pública para formar una red virtual.

Los beneficios de una VPN incluyen lo siguiente:

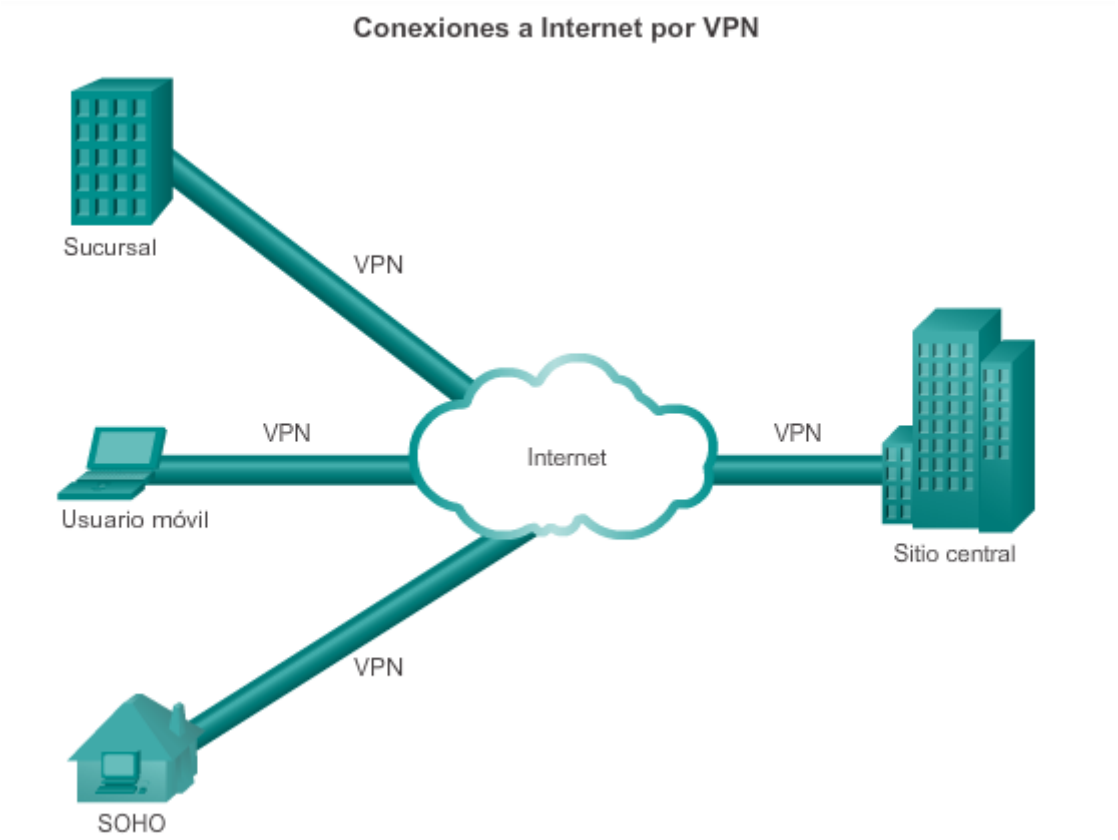
- **Ahorro de costos:** las VPN permiten que las organizaciones utilicen un transporte externo de Internet rentable para conectar oficinas remotas y usuarios remotos al sitio principal; por lo tanto, se eliminan los costosos enlaces WAN dedicados y los bancos de módem. Además, con la llegada de las tecnologías rentables de ancho de banda alto, como DSL, las organizaciones pueden utilizar VPN para reducir los costos de conectividad y, al mismo tiempo, aumentar el ancho de banda de la conexión remota.

- **Escalabilidad:** las VPN permiten que las organizaciones utilicen la infraestructura de Internet dentro de los ISP y los dispositivos, lo que facilita la tarea de agregar nuevos usuarios. Por lo tanto, las organizaciones pueden agregar una gran cantidad de capacidad sin necesidad de aumentar considerablemente la infraestructura.

- **Compatibilidad con la tecnología de banda ancha:** las redes VPN permiten que los trabajadores móviles y los empleados a distancia aprovechen la conectividad por banda

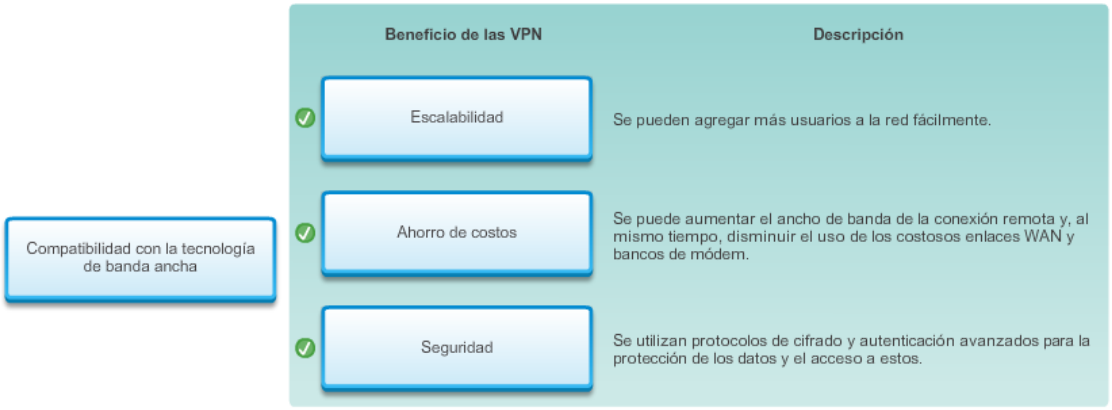
ancha de alta velocidad, como DSL y cable, para acceder a las redes de sus organizaciones. La conectividad por banda ancha proporciona flexibilidad y eficacia. Las conexiones por banda ancha de alta velocidad también proporcionan una solución rentable para conectar oficinas remotas.

- **Seguridad:** las VPN pueden incluir mecanismos de seguridad que proporcionan el máximo nivel de seguridad mediante protocolos de cifrado y autenticación avanzados que protegen los datos contra el acceso no autorizado.



Capítulo 7: Seguridad de la conectividad Site-to-Site 7.1.1.3 Actividad: Identificar los beneficios de las VPN

Actividad: Identificar los beneficios de las VPN
Una los beneficios de las VPN con las descripciones. No se utilizan todas las opciones.



Capítulo 7: Seguridad de la conectividad Site-to-Site 7.1.2.1 VPN de sitio a sitio

Existen dos tipos de redes VPN:

- Sitio a sitio
- Acceso remoto

VPN de sitio a sitio

Una VPN de sitio a sitio se crea cuando los dispositivos en ambos lados de la conexión VPN conocen la configuración de VPN con anticipación, como se muestra en la ilustración. La VPN permanece estática, y los hosts internos no saben que existe una VPN. En una VPN de sitio a sitio, los hosts terminales envían y reciben tráfico TCP/IP normal a través de un “gateway” VPN. El gateway VPN es el responsable de encapsular y cifrar el tráfico saliente para todo el tráfico de un sitio en particular. Después, el gateway VPN lo envía por un túnel VPN a través de Internet a un gateway VPN de peer en el sitio de destino. Al recibirlo, el gateway VPN de peer elimina los encabezados, descifra el contenido y transmite el paquete hacia el host de destino dentro de su red privada.

Una VPN de sitio a sitio es una extensión de una red WAN clásica. Las VPN de sitio a sitio conectan redes enteras entre sí, por ejemplo, pueden conectar la red de una sucursal a la red de la oficina central de una empresa. En el pasado, se requería una conexión de línea arrendada o de Frame Relay para conectar sitios, pero dado que en la actualidad la mayoría de las empresas tienen acceso a Internet, estas conexiones se pueden reemplazar por VPN de sitio a sitio.

VPN de sitio a sitio

Capítulo 7: Seguridad de la conectividad Site-to-Site 7.1.2.2 VPN de acceso remoto

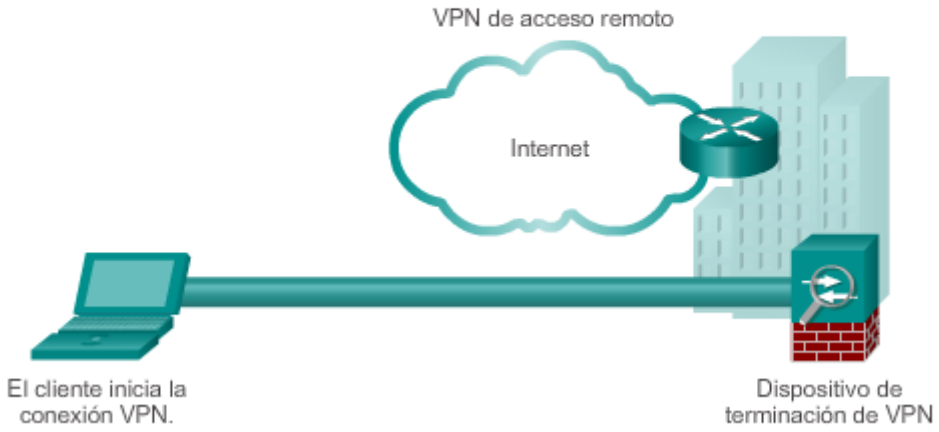
VPN de acceso remoto

Si se utiliza una VPN de sitio a sitio para conectar redes enteras, la VPN de acceso remoto admite las necesidades de los empleados a distancia, de los usuarios móviles y del tráfico de extranet de cliente a empresa. Una VPN de acceso remoto se crea cuando la información de VPN no se configura de forma estática, pero permite el intercambio dinámico de información y se puede habilitar y deshabilitar. Las VPN de acceso remoto admiten una arquitectura cliente/servidor, en la que el cliente VPN (host remoto) obtiene acceso seguro a la red empresarial mediante un dispositivo del servidor VPN en el perímetro de la red.

Las VPN de acceso remoto se utilizan para conectar hosts individuales que deben acceder a la red de su empresa de forma segura a través de Internet. La conectividad a Internet que utilizan los trabajadores a distancia suele ser una conexión por banda ancha, DSL, cable o inalámbrica, como se indica en la ilustración.

Es posible que se deba instalar un software de cliente VPN en la terminal del usuario móvil; por ejemplo, cada host puede tener el software Cisco AnyConnect Secure Mobility Client instalado. Cuando el host intenta enviar cualquier tipo de tráfico, el software Cisco AnyConnect VPN Client encapsula y cifra este tráfico. Después, los datos cifrados se envían por Internet al gateway VPN en el perímetro de la red de destino. Al recibirlos, el gateway VPN se comporta como lo hace para las VPN de sitio a sitio.

Nota: el software Cisco AnyConnect Secure Mobility Client se basa en las características que ofrecían anteriormente Cisco AnyConnect VPN Client y Cisco VPN Client para mejorar la experiencia de VPN permanente en más dispositivos portátiles basados en computadoras portátiles y smartphones. Este cliente admite IPv6.



Capítulo 7: Seguridad de la conectividad Site-to-Site 7.1.2.3 Actividad: Comparar los tipos de VPN

Actividad: Comparar los tipos de VPN
Haga clic en la casilla junto a la afirmación sobre las VPN que represente la mejor coincidencia con el tipo.

	Sitio a sitio	Acceso remoto
1. Configuración de VPN dinámica para conectarse a la red.		✓
2. Tiene el soporte de un servidor VPN para la entrada de clientes en el perímetro de la red.		✓
3. Configuración de VPN estática para conectarse a la red.	✓	
4. Tipo de VPN que utiliza la mayoría de los trabajadores a distancia, los usuarios móviles y el tráfico de la red de cliente a empresa.		✓
5. Conecta las redes de las sucursales entre sí.	✓	

Capítulo 7: Seguridad de la conectividad Site-to-Site 7.1.2.4 Packet Tracer: Configuración de VPN (optativo)

Información básica/situación

En esta actividad, configurará dos routers para admitir una VPN con IPsec de sitio a sitio para el tráfico que fluye de sus respectivas LAN. El tráfico de la VPN con IPsec pasa a través de otro router que no tiene conocimiento de la VPN. IPsec proporciona una transmisión segura de la información confidencial a través de redes sin protección, como Internet. IPsec funciona en la capa de red, por lo que protege y autentica los paquetes IP entre los dispositivos IPsec participantes (peers), como los routers Cisco.

Packet Tracer: Configuración de VPN (optativo) (instrucciones)

Packet Tracer: Configuración de VPN (optativo) (PKA)

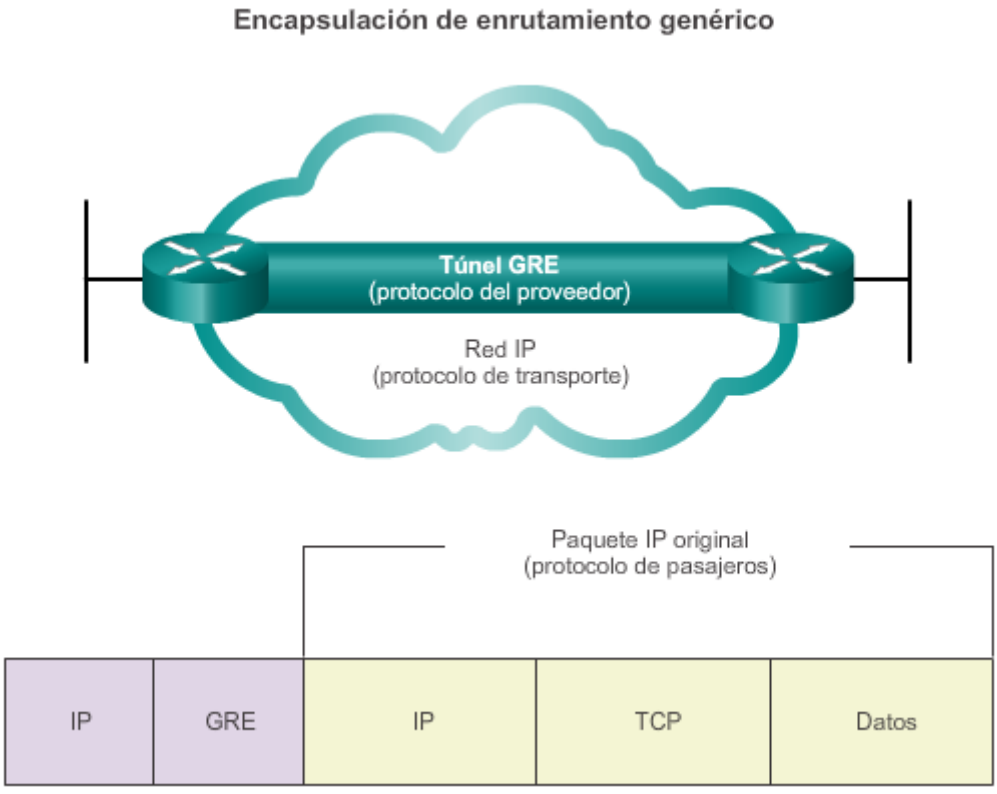
Capítulo 7: Seguridad de la conectividad Site-to-Site 7.2.1.1 Introducción a GRE

La encapsulación de routing genérico (GRE) es un ejemplo de un protocolo de tunneling de VPN de sitio a sitio básico y no seguro. GRE es un protocolo de tunneling desarrollado por Cisco que puede encapsular una amplia variedad de tipos de paquete de protocolo dentro de túneles IP. GRE crea un enlace virtual punto a punto a los routers Cisco en puntos remotos a través de una internetwork IP.

GRE está diseñada para administrar el transporte del tráfico multiprotocolo y de multidifusión IP entre dos o más sitios, que probablemente solo tengan conectividad IP. Puede encapsular varios tipos de paquete de protocolo dentro de un túnel IP.

Como se muestra en la ilustración, una interfaz de túnel admite un encabezado para cada uno de los siguientes protocolos:

- Un protocolo encapsulado (o protocolo de pasajeros), como IPv4, IPv6, AppleTalk, DECnet o IPX
- Un protocolo de encapsulación (o portadora), como GRE
- Un protocolo de entrega de transporte, como IP, que es el protocolo que transporta al protocolo encapsulado



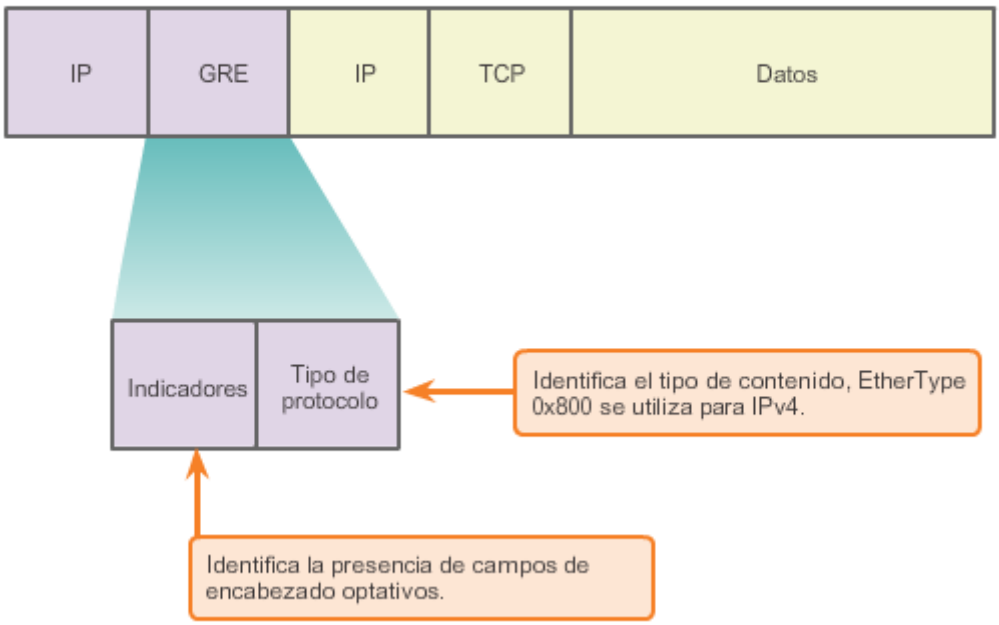
Capítulo 7: Seguridad de la conectividad Site-to-Site 7.2.1.2 Características de GRE

GRE es un protocolo de tunneling desarrollado por Cisco que puede encapsular una amplia variedad de tipos de paquete de protocolo dentro de túneles IP, lo que crea un enlace punto a punto virtual a los routers Cisco en puntos remotos a través de una internetwork IP. El tunneling IP que utiliza GRE habilita la expansión de la red a través de un entorno de backbone de protocolo único. Esto se logra mediante la conexión de subredes multiprotocolo en un entorno de backbone de protocolo único.

Las características de GRE son las siguientes:

- GRE se define como un estándar IETF (RFC 2784).
- En el encabezado IP externo, se utiliza el número 47 en el campo de protocolo para indicar que lo que sigue es un encabezado GRE.
- La encapsulación de GRE utiliza un campo de tipo de protocolo en el encabezado GRE para admitir la encapsulación de cualquier protocolo de capa 3 del modelo OSI. Los tipos de protocolo se definen en RFC 1700 como “EtherTypes”.
- GRE en sí misma no tiene estado; de manera predeterminada, no incluye ningún mecanismo de control de flujo.
- GRE no incluye ningún mecanismo de seguridad sólido para proteger su contenido.
- El encabezado GRE, junto con el encabezado de tunneling IP que se indica en la ilustración, crea por lo menos 24 bytes de sobrecarga adicional para los paquetes que se envían por túnel.

Encabezado para el encabezado de paquete encapsulado de GRE



Capítulo 7: Seguridad de la conectividad Site-to-Site 7.2.1.3 Actividad: Identificar la características de GRE

Actividad: Identificar la características de GRE
Arrastre cada etiqueta de protocolo hasta las ubicaciones funcionales de VPN en el gráfico.

Capítulo 7: Seguridad de la conectividad Site-to-Site 7.2.2.1 Configuración de túneles GRE

GRE se utiliza para crear un túnel VPN entre dos sitios, como se muestra en la figura 1. Para implementar un túnel GRE, el administrador de red primero debe descubrir las direcciones IP de las terminales. Después, se deben seguir cinco pasos para configurar un túnel GRE:

Paso 1. Cree una interfaz de túnel con el comando **interface tunnel number**.

Paso 2. Especifique la dirección IP de origen del túnel.

Paso 3. Especifique la dirección IP de destino del túnel.

Paso 4. Configure una dirección IP para la interfaz de túnel.

Paso 5. (Optativo) Especifique el modo de túnel GRE como modo de interfaz de túnel. El modo de túnel GRE es el modo predeterminado de interfaz de túnel para el software IOS de Cisco.

En el ejemplo de configuración que se muestra en la figura 2, se detalla una configuración básica de túnel GRE para el router R1.

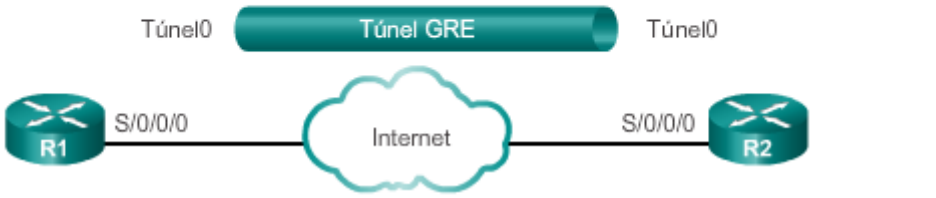
La configuración del R2 en la figura 3 refleja la configuración del R1.

La configuración mínima requiere la especificación de las direcciones de origen y destino del túnel. También se debe configurar la subred IP para proporcionar conectividad IP a través del enlace de túnel. Ambas interfaces de túnel tienen el origen del túnel establecido en la interfaz serial local S0/0/0 y el destino del túnel establecido en la interfaz serial S0/0/0 del router peer. La dirección IP se asigna a las interfaces de túnel en ambos routers. También se configuró OSPF para intercambiar rutas a través del túnel GRE.

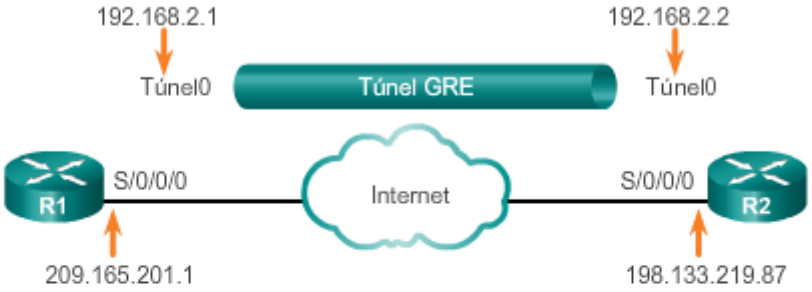
Las descripciones de los comandos individuales de túnel GRE se muestran en la figura 4.

Nota: cuando se configuran los túneles GRE, puede ser difícil recordar cuáles son las redes IP asociadas a las interfaces físicas y cuáles son las redes IP asociadas a las interfaces de túnel. Recuerde que antes de que se cree un túnel GRE, ya se configuraron las interfaces físicas. Los comandos **tunnel source** y **tunnel destination** se refieren a las direcciones IP de las interfaces físicas configuradas previamente. El comando **ip address** en las interfaces de túnel se refiere a una red IP especialmente diseñada para los propósitos del túnel GRE.

Configuración de túneles GRE



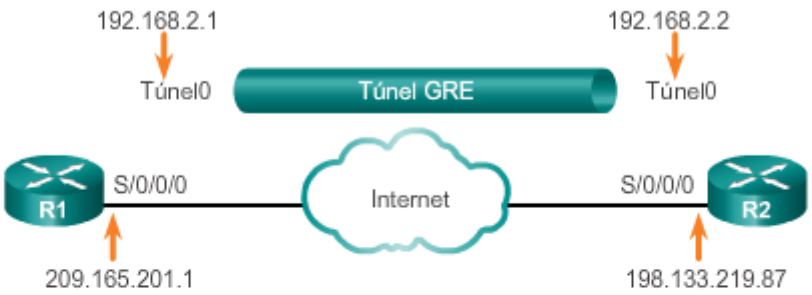
Configuración de túneles GRE



Configuración del R1:

```
R1(config)# interface Tunnel0
R1(config-if)# tunnel mode gre ip
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# tunnel source 209.165.201.1
R1(config-if)# tunnel destination 198.133.219.87
R1(config-if)# router ospf 1
R1(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

Configuración de túneles GRE



Configuración del R2:

```
R2(config)# interface Tunnel0
R2(config-if)# tunnel mode gre ip
R2(config-if)# ip address 192.168.2.2 255.255.255.0
R2(config-if)# tunnel source 198.133.219.87
R2(config-if)# tunnel destination 209.165.201.1
R2(config-if)# router ospf 1
R2(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

Comandos de túnel GRE

Comando	Descripción
tunnel mode gre ip	Especifica que el modo de la interfaz de túnel es GRE por IP.
tunnel source *dirección_ip*	Especifica la dirección de origen del túnel.
tunnel destination *dirección_ip*	Especifica la dirección de destino del túnel.
ip address *dirección_ip máscara*	Especifica la dirección IP de la interfaz de túnel.

Capítulo 7: Seguridad de la conectividad Site-to-Site 7.2.2.2 Verificación del túnel GRE

Existen varios comandos que se pueden utilizar para controlar los túneles GRE y resolver los problemas relacionados. Para determinar si la interfaz de túnel está activa o inactiva, utilice el comando **show ip interface brief**, el cual se muestra en la figura 1.

Para verificar el estado de un túnel GRE, utilice el comando **show interface tunnel**. El protocolo de línea en una interfaz de túnel GRE permanece activo mientras haya una ruta al destino del túnel. Antes de implementar un túnel GRE, la conectividad IP ya debe estar operativa entre las direcciones IP de las interfaces físicas en extremos opuestos del túnel GRE potencial. El protocolo de transporte de túnel se muestra en el resultado, que también aparece en la figura 1.

Si también se configuró OSPF para intercambiar rutas a través del túnel GRE, verifique que se haya establecido una adyacencia OSPF a través de la interfaz de túnel con el comando **show ip ospf neighbor**. En la figura 2, observe que la dirección de interconexión para el vecino OSPF está en la red IP creada para el túnel GRE.

En la figura 3, utilice el verificador de sintaxis para configurar y verificar un túnel GRE en el R2 seguido del R1.

GRE se considera una VPN porque es una red privada que se crea con tunneling a través de una red pública. Mediante la encapsulación, un túnel GRE crea un enlace virtual punto a punto a los routers Cisco en puntos remotos a través de una internetwork IP. Las ventajas de GRE son que se puede utilizar para canalizar el tráfico que no es IP a través de una red IP, lo que permite la expansión de la red mediante la conexión de subredes multiprotocolo en un entorno de backbone de protocolo único. Además, GRE admite el tunneling de multidifusión IP. Esto significa que se pueden utilizar los protocolos de routing a través del túnel, lo que habilita el intercambio dinámico de información de routing en la red virtual. Por último, es habitual crear túneles GRE IPv6 a través de IPv4, donde IPv6 es el protocolo encapsulado e IPv4 es el protocolo de transporte. En el futuro, es probable que estas funciones se inviertan cuando IPv6 pase a cumplir la función de protocolo IP estándar.

Sin embargo, GRE no proporciona cifrado ni ningún otro mecanismo de seguridad. Por lo tanto, los datos que se envían a través de un túnel GRE no son seguros. Si se necesita una comunicación de datos segura, se deben configurar redes VPN con IPsec o SSL.

Verificar que la interfaz de tunel esté activa

```
R1# show ip interface brief | include Tunnel
Tunnel0                192.168.2.1     YES manual up        up
```

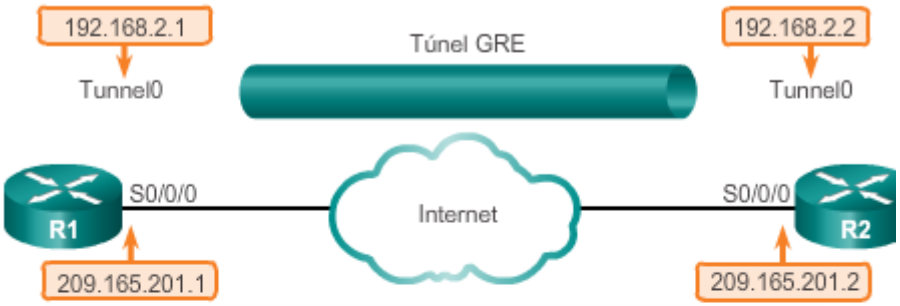
```
R1# show interface Tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.2.1/24
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 209.165.201.1, destination 209.165.201.2
  Tunnel protocol/transport GRE/IP
<se omite el resultado>
```

Verificar la adyacencia de OSPF a través del tunel GRE

```
R1# show ip ospf neighbor

Neighbor ID     Pri State      Dead Time   Address         Interface
209.165.201.2   0   FULL/  -   00:00:37    192.168.2.2     Tunnel0
```

Configurar y verificar GRE



Configurar R2 con los siguientes pasos:

- **Crear interfaz de túnel 0.**
- **Configurar modo de túnel a GRE con IP como protocolo de entrega.**
- **Asignar la dirección IP 192.168.2.2/24.**
- **Configurar la fuente del túnel como 209.165.201.2.**
- **Configurar el destino del túnel como 209.165.201.1.**
- **Configurar OSPF con la Id. del proceso 1.**
- **Anunciar la red 192.168.2.0/24 para el área 0.**

```
R2(config)# interface tunnel 0
R2(config-if)# tunnel mode gre ip
R2(config-if)# ip address 192.168.2.2 255.255.255.0
R2(config-if)# tunnel source 209.165.201.2
R2(config-if)# tunnel destination 209.165.201.1
R2(config-if)# router ospf 1
R2(config-router)#  network 192.168.2.0 0.0.0.255 area 0
```

Configurar R1 con los siguientes pasos:

- Crear interfaz de túnel 0.
- Configurar modo de túnel a GRE con IP como protocolo de entrega.
- Asignar la dirección IP 192.168.2.1/24.
- Configurar la fuente del túnel como 209.165.201.1.
- Configurar el destino del túnel como 209.165.201.2.
- Configurar OSPF con la Id. del proceso 1.
- Anunciar la red 192.168.2.0/24 para el área 0.

```
R1(config)# interface tunnel 0
R1(config-if)# tunnel mode gre ip
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# tunnel source 209.165.201.1
R1(config-if)# tunnel destination 209.165.201.2
R1(config-if)# router ospf 1
R1(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

Vuelva directamente al modo EXEC privilegiado. Muestre la lista breve de interfaces filtradas para que incluyan la palabra "Túnel".

```
R1(config-router)# end
R1# show ip interface brief | incluir túnel
Tunnel0              192.168.2.1     YES manual up       up
```

Mostrar la información de interfaz de túnel 0.

```
R1# show interface Tunnel 0
Tunnel0 está activo, el protocolo de línea está activo
 Hardware es túnel
 La dirección de Internet es 192.168.2.1/24
 MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
 fiabilidad 255/255, txload 1/255, rxload 1/255
 Encapsulación TUNNEL, bucle invertido no configurado
 Keepalive no configurado
 Fuente de túnel 209.165.201.1, destino 209.165.201.2
 Protocolo de túnel/transporte GRE/IP
 Clave inhabilitada, secuencia inhabilitada
 Suma de verificación de paquetes inhabilitada
 Túnel TTL 255, Fast tunneling activado
 Transporte de túnel MTU 1476 bytes
 Ancho de banda de transmisión de túnel 8000 (kbps)
 Ancho de banda de recepción de túnel 8000 (kbps)
 Última entrada 00:00:07, salida 00:00:09, salida hang never
 Última explicación de contadores "show interface" 00:34:58
 Cola de entrada: 0/75/0/0 (size/max/drops/flushes); Total
output
   drops: 0
 Queueing strategy: fifo
 Output queue: 0/0 (size/max)
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
 161 packets input, 16704 bytes, 0 no buffer
 Received 0 broadcasts (0 IP multicasts)
 0 runts, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 178 packets output, 18316 bytes, 0 underruns
 0 output errors, 0 collisions, 0 interface resets
 0 unknown protocol drops
 0 output buffer failures, 0 output buffers swapped out
```

Muestre los vecinos de OSPF.

```
R1# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
209.165.201.2   0     FULL/  -        00:00:36    192.168.2.2     Tunnel0
```

You successfully configured and verified GRE.

Capítulo 7: Seguridad de la conectividad Site-to-Site 7.2.2.3 Packet Tracer: configuración de GRE

Información básica/situación

Usted es el administrador de red de una empresa que desea configurar un túnel GRE a una oficina remota. Ambas redes están configuradas localmente y solo necesitan que se configure el túnel.

Packet Tracer: Configuración de GRE (instrucciones)

Packet Tracer: Configuración de GRE (PKA)

Capítulo 7: Seguridad de la conectividad Site-to-Site 7.2.2.4 Packet Tracer: Resolución de problemas de GRE

Información básica/situación

Se contrató a un administrador de red principiante para configurar un túnel GRE entre dos sitios, pero no pudo completar la tarea. Se le solicita a usted corregir los errores de configuración en la red de la empresa.

Packet Tracer: Resolución de problemas de GRE (instrucciones)

Packet Tracer: Resolución de problemas de GRE (PKA)

Capítulo 7: Seguridad de la conectividad Site-to-Site 7.2.2.5 Práctica de laboratorio: Configuración de un túnel VPN GRE de punto a punto

En esta práctica de laboratorio, cumplirá los siguientes objetivos:

- Parte 1: configurar los parámetros básicos de los dispositivos
- Parte 2: Configurar un túnel GRE
- Parte 3: Habilitar el routing por el túnel GRE

Práctica de laboratorio: Configuración de un túnel VPN GRE de punto a punto

Capítulo 7: Seguridad de la conectividad Site-to-Site 7.3.1.1 IPsec

Las VPN con IPsec ofrecen conectividad flexible y escalable. Las conexiones de sitio a sitio pueden proporcionar una conexión remota segura, rápida y confiable. Con una VPN con IPsec, la información de una red privada se transporta de manera segura a través de una red pública. Esto forma una red virtual en lugar de usar una conexión dedicada de capa 2, como se muestra en la ilustración. Para que siga siendo privado, el tráfico se cifra a fin de mantener la confidencialidad de los datos.

IPsec es un estándar IETF que define la forma en que se puede configurar una VPN de manera segura mediante el protocolo de Internet.

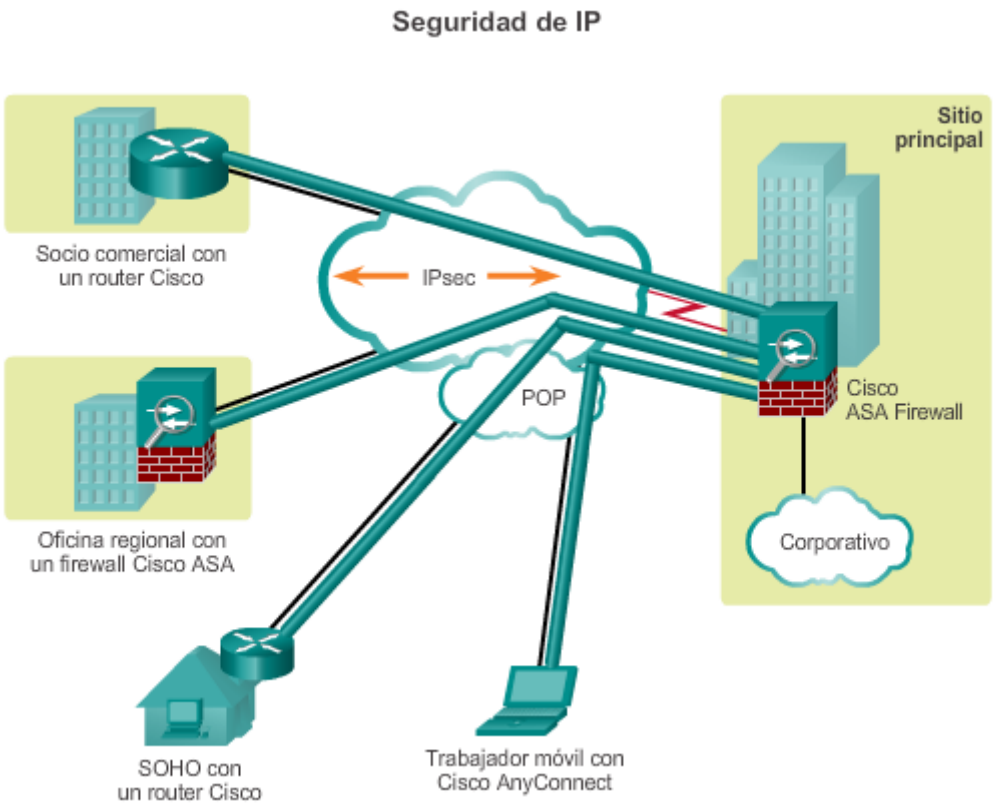
IPsec es un marco de estándares abiertos que detalla las reglas para las comunicaciones seguras. IPSec no se limita a ningún tipo específico de cifrado, autenticación, algoritmo de seguridad ni tecnología de creación de claves. En realidad, IPsec depende de algoritmos existentes para implementar comunicaciones seguras. IPsec permite que se implementen nuevos y mejores algoritmos sin modificar los estándares existentes de IPsec.

IPsec funciona en la capa de red, por lo que protege y autentica los paquetes IP entre los dispositivos IPsec participantes, también conocidos como “peers”. IPsec protege una ruta entre un par de gateways, un par de hosts o un gateway y un host. Como resultado, IPsec puede proteger prácticamente todo el tráfico de una aplicación, dado que la protección se puede implementar desde la capa 4 hasta la capa 7.

Todas las implementaciones de IPsec tienen un encabezado de capa 3 de texto no cifrado, de modo que no hay problemas de routing. IPsec funciona en todos los protocolos de capa 2, como Ethernet, ATM o Frame Relay.

Las características de IPsec se pueden resumir de la siguiente manera:

- IPsec es un marco de estándares abiertos que no depende de algoritmos.
- IPsec proporciona confidencialidad e integridad de datos, y autenticación del origen.
- IPsec funciona en la capa de red, por lo que protege y autentica paquetes IP.



Capítulo 7: Seguridad de la conectividad Site-to-Site 7.3.1.2 Servicios de seguridad IPsec

Los servicios de seguridad IPsec proporcionan cuatro funciones fundamentales, las cuales se muestran en la ilustración:

- **Confidencialidad (cifrado):** en una implementación de VPN, los datos privados se transfieren a través de una red pública. Por este motivo, la confidencialidad de los datos es fundamental. Esto se puede lograr mediante el cifrado de los datos antes de transmitirlos a través de la red. Este es el proceso de tomar todos los datos que una computadora envía a otra y codificarlos de una manera que solo la otra computadora pueda decodificar. Si se intercepta la comunicación, el pirata informático no puede leer los datos. IPsec proporciona características de seguridad mejoradas, como algoritmos de cifrado seguros.

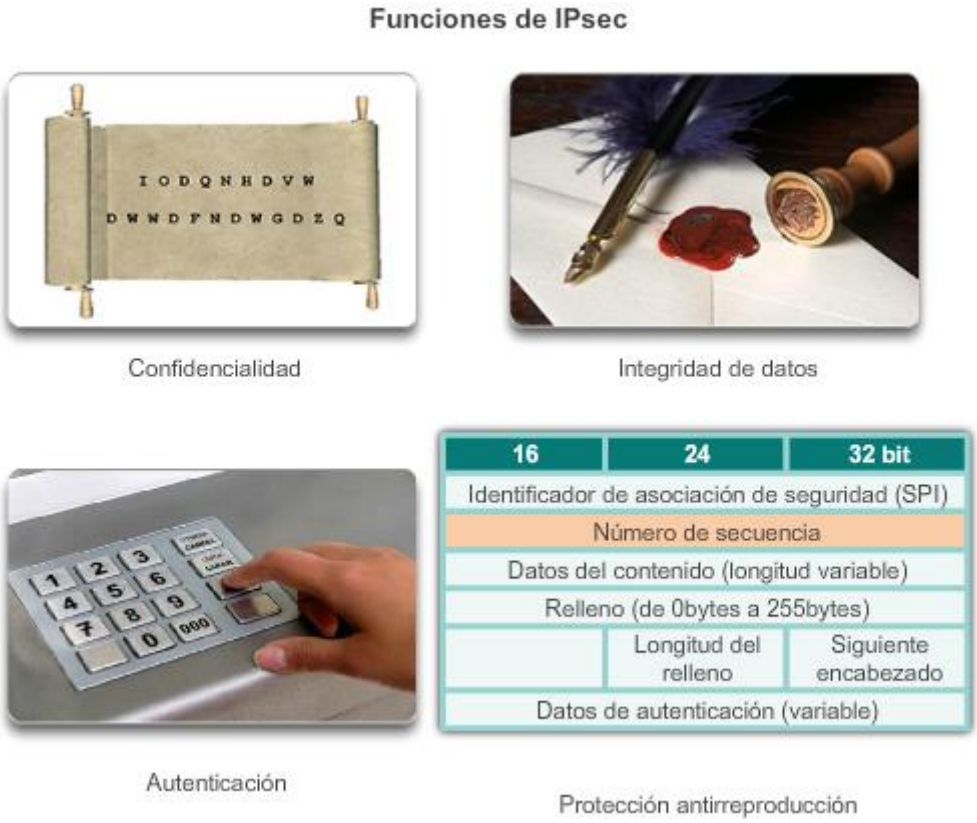
- **Integridad de datos:** el receptor puede verificar que los datos se hayan transmitido a través de Internet sin sufrir ningún tipo de modificaciones ni alteraciones. Si bien es importante que los datos a través de una red pública estén cifrados, también es importante verificar que no se hayan modificado cuando estaban en tránsito. IPsec cuenta con un mecanismo para asegurarse de que la porción cifrada del paquete, o todo el encabezado y la porción de datos del paquete, no se haya modificado. IPsec asegura la integridad de los datos mediante checksums, que es una comprobación de redundancia simple. Si se detecta una alteración, el paquete se descarta.

- **Autenticación:** verifica la identidad del origen de los datos que se envían. Esto es necesario para la protección contra distintos ataques que dependen de la suplantación de identidad del emisor. La autenticación asegura que se cree una conexión con el compañero de comunicación deseado. El receptor puede autenticar el origen del paquete

mediante la certificación del origen de la información. IPsec utiliza el intercambio de claves de Internet (IKE) para autenticar a los usuarios y dispositivos que pueden llevar a cabo la comunicación de manera independiente. IKE utiliza varios tipos de autenticación, por ejemplo, nombre de usuario y contraseña, contraseña por única vez, biometría, clave previamente compartida (PSK) y certificados digitales.

- **Protección antirreproducción:** es la capacidad de detectar y rechazar los paquetes reproducidos, y ayuda a prevenir la suplantación de identidad. La protección antirreproducción verifica que cada paquete sea único y no esté duplicado. Los paquetes IPsec se protegen mediante la comparación del número de secuencia de los paquetes recibidos con una ventana deslizante en el host de destino o el gateway de seguridad. Se considera que un paquete que tiene un número de secuencia anterior a la ventana deslizante tiene un retraso o está duplicado. Los paquetes duplicados y con retraso se descartan.

El acrónimo CIA se suele utilizar para ayudar a recordar las iniciales de estas tres funciones: confidencialidad, integridad y autenticación.



Capítulo 7: Seguridad de la conectividad Site-to-Site 7.3.2.1 Confidencialidad con cifrado

Confidencialidad

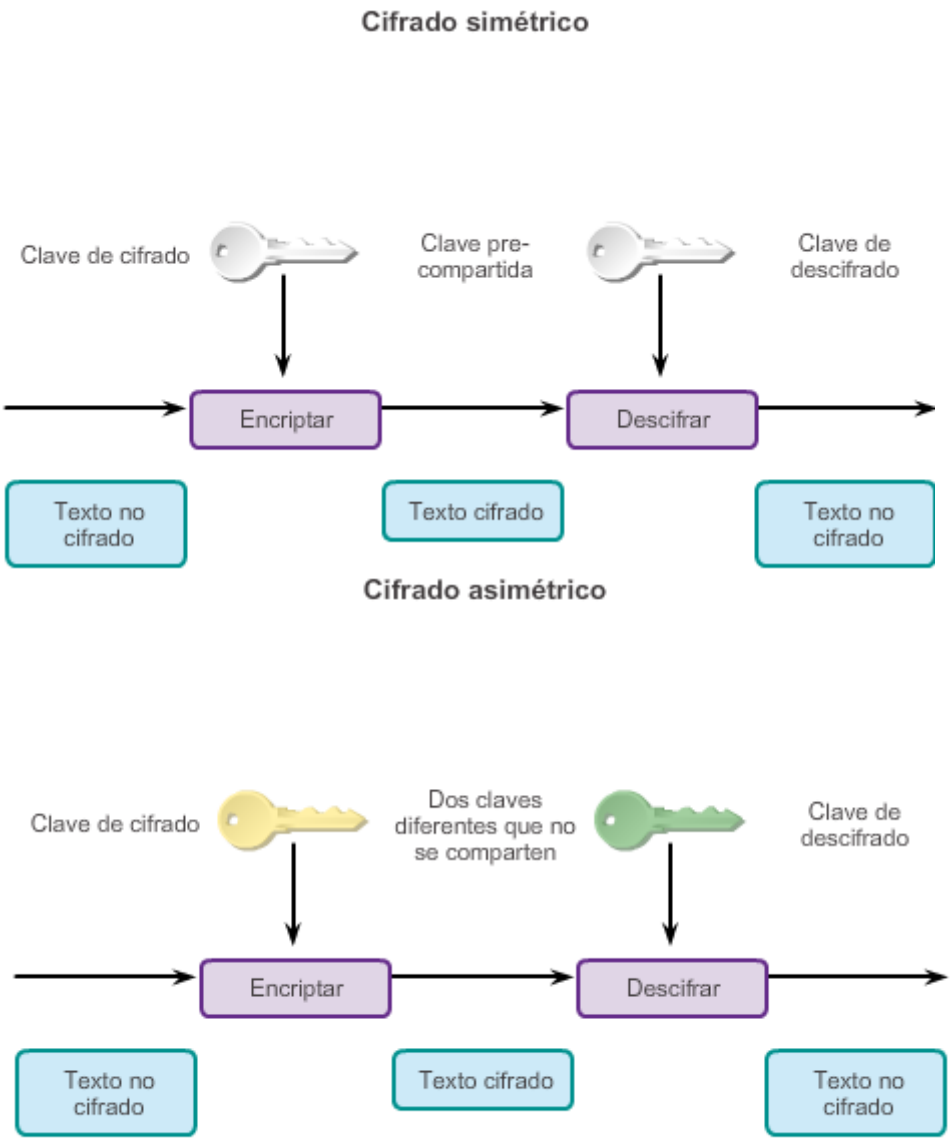
El tráfico VPN se mantiene confidencial con el cifrado. Los datos de texto no cifrado que se transportan a través de Internet pueden interceptarse y leerse. Cifre la fecha para que se mantenga privada. El cifrado digital de los datos hace que estos sean ilegibles hasta que el receptor autorizado los descifre.

Para que la comunicación cifrada funcione, el emisor y el receptor deben conocer las reglas que se utilizan para transformar el mensaje original a su forma cifrada. Las reglas se basan en algoritmos y claves asociadas. En el contexto del cifrado, un algoritmo es una secuencia matemática de pasos que combina un mensaje, texto, dígitos o las tres cosas con una cadena de dígitos denominada “clave”. El resultado es una cadena de cifrado ilegible. El algoritmo de cifrado también especifica cómo se descifra un mensaje cifrado. El descifrado es extremadamente difícil o imposible sin la clave correcta.

En la ilustración, Gail desea enviar una transferencia electrónica de fondos (EFT) a Jeremías a través de Internet. En el extremo local, el documento se combina con una clave y se procesa con un algoritmo de cifrado. El resultado es un texto cifrado. El texto cifrado se envía a través de Internet. En el extremo remoto, el mensaje se vuelve a combinar con una clave y se devuelve a través del algoritmo de cifrado. El resultado es el documento financiero original.

La confidencialidad se logra con el cifrado del tráfico mientras viaja por una VPN. El grado de seguridad depende de la longitud de la clave del algoritmo de cifrado y la sofisticación del algoritmo. Si un pirata informático intenta descifrar la clave mediante un ataque por fuerza bruta, la cantidad de intentos posibles es una función de la longitud de la clave. El tiempo para procesar todas las posibilidades es una función de la potencia de la computadora del dispositivo atacante. Cuanto más corta sea la clave, más fácil será descifrarla. Por ejemplo, una computadora relativamente sofisticada puede tardar aproximadamente un año para descifrar una clave de 64 bits, mientras que descifrar una clave de 128 bits puede llevarle de 10 a 19 años.

Capítulo 7: Seguridad de la conectividad Site-to-Site 7.3.2.2 Algoritmos de cifrado



Capítulo 7: Seguridad de la conectividad Site-to-Site 7.3.2.3 Intercambio de claves de Diffie-Hellman

Integridad de datos

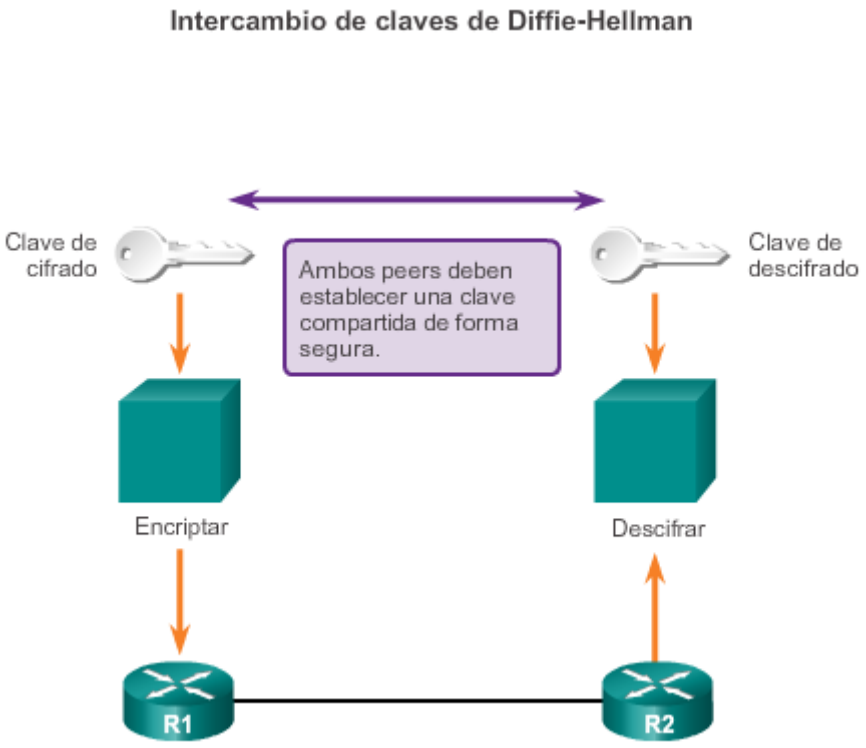
Diffie-Hellman (DH) no es un mecanismo de cifrado y no se suele utilizar para cifrar datos. En cambio, es un método para intercambiar con seguridad las claves que cifran datos. Los algoritmos (DH) permiten que dos partes establezcan la clave secreta compartida que usan el cifrado y los algoritmos de hash.

DH, presentado por Whitfield Diffie y Martin Hellman en 1976, fue el primer sistema en utilizar la clave pública o las claves criptográficas asimétricas. En la actualidad, DH forma parte del estándar IPsec. Además, un protocolo denominado OAKLEY utiliza un algoritmo DH. OAKLEY

es un protocolo utilizado por el protocolo IKE, que forma parte del marco general denominado “protocolo de administración de claves y de asociación de seguridad de Internet”.

Los algoritmos de cifrado, como DES, 3DES y AES, así como los algoritmos de hash MD5 y SHA-1, requieren una clave secreta compartida simétrica para realizar el cifrado y el descifrado. ¿Cómo obtienen la clave secreta compartida los dispositivos de cifrado y descifrado? El método más sencillo de intercambio de claves es un método de intercambio de clave pública entre dispositivos de cifrado y descifrado.

El algoritmo DH especifica un método de intercambio de clave pública que proporciona una manera para que dos peers establezcan una clave secreta compartida que solo ellos conozcan, aunque se comuniquen a través de un canal inseguro. Como todos los algoritmos criptográficos, el intercambio de claves DH se basa en una secuencia matemática de pasos.



Capítulo 7: Seguridad de la conectividad Site-to-Site 7.3.2.4 Integridad con los algoritmos de hash

Los algoritmos de hash manejan la integridad y la autenticación del tráfico VPN. Los hashes proporcionan integridad y autenticación de datos al asegurar que las personas no autorizadas no alteren los mensajes transmitidos. Un hash, también denominado “síntesis del mensaje”, es un número que se genera a partir de una cadena de texto. El hash es más corto que el texto en sí. Se genera mediante el uso de una fórmula, de tal manera que es muy poco probable que otro texto produzca el mismo valor de hash.

El emisor original genera un hash del mensaje y lo envía con el mensaje propiamente dicho. El destinatario analiza el mensaje y el hash, produce otro hash a partir del mensaje recibido y

compara ambos hashes. Si son iguales, el destinatario puede estar lo suficientemente seguro de la integridad del mensaje original.

En la ilustración, Gail le envió a Alex un EFT de USD 100. Jeremías interceptó y alteró este EFT para mostrarse como el destinatario y que la cantidad sea USD 1000. En este caso, si se utilizara un algoritmo de integridad de datos, los hashes no coincidirían, y la transacción no sería válida.

Los datos VPN se transportan por Internet pública. Como se muestra, existe la posibilidad de que se intercepten y se modifiquen estos datos. Para protegerlos contra esta amenaza, los hosts pueden agregar un hash al mensaje. Si el hash transmitido coincide con el hash recibido, se preservó la integridad del mensaje. Sin embargo, si no hay una coincidencia, el mensaje se alteró.

Las VPN utilizan un código de autenticación de mensajes para verificar la integridad y la autenticidad de un mensaje, sin utilizar ningún mecanismo adicional.

El código de autenticación de mensajes basado en hash (HMAC) es un mecanismo para la autenticación de mensajes mediante funciones de hash. Un HMAC con clave es un algoritmo de integridad de datos que garantiza la integridad de un mensaje. Un HMAC tiene dos parámetros: una entrada de mensaje y una clave secreta que solo conocen el autor del mensaje y los destinatarios previstos. El emisor del mensaje utiliza una función HMAC para producir un valor (el código de autenticación de mensajes) que se forma mediante la compresión de la clave secreta y la entrada de mensaje. El código de autenticación de mensajes se envía junto con el mensaje. El receptor calcula el código de autenticación de mensajes en el mensaje recibido con la misma clave y la misma función HMAC que utilizó el emisor. A continuación, el receptor compara el resultado que se calculó con el código de autenticación de mensajes que se recibió. Si los dos valores coinciden, el mensaje se recibió correctamente y el receptor se asegura de que el emisor forma parte de la comunidad de usuarios que comparten la clave. La fortaleza criptográfica del HMAC depende de la fortaleza criptográfica de la función de hash subyacente, del tamaño y la calidad de la clave, y del tamaño de la longitud del resultado del hash en bits.

Hay dos algoritmos HMAC comunes:

- **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 procesan con el algoritmo de hash HMAC-MD5. El resultado es un hash de 128 bit. El hash se adjunta al mensaje original y se envía al extremo remoto.

- **SHA:** 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 procesan con el algoritmo de hash HMAC-SHA1. El resultado es un hash de 160 bits. El hash se adjunta al mensaje original y se envía al extremo remoto.

Nota: el IOS de Cisco también admite implementaciones de SHA de 256 bits, 384 bits y 512 bits.

Capítulo 7: Seguridad de la conectividad Site-to-Site 7.3.2.5 Autenticación IPsec

Autenticación

Las VPN con IPsec admiten la autenticación. Al realizar negocios a larga distancia, es necesario saber quién está del otro lado del teléfono, del correo electrónico o del fax. Lo mismo sucede con las redes VPN. El dispositivo en el otro extremo del túnel VPN se debe autenticar para que la ruta de comunicación se considere segura, como se indica en la ilustración. Existen dos métodos de autenticación de peers:

- **PSK:** es una clave secreta que se comparte entre las dos partes que utilizan un canal seguro antes de que se necesite utilizarla. Las claves previamente compartidas (PSK) utilizan algoritmos criptográficos de clave simétrica. Se introduce una PSK en cada peer de forma manual y se la utiliza para autenticar el peer. En cada extremo, la PSK se combina con otra información para formar la clave de autenticación.

- **Firmas RSA:** se intercambian certificados digitales para autenticar los peers. El dispositivo local deriva un hash y lo cifra con su clave privada. El hash cifrado, o la firma digital, se vincula al mensaje y se reenvía hacia el extremo remoto. En el extremo remoto, se descifra el hash cifrado con la clave pública del extremo local. Si el hash descifrado coincide con el hash recalculado, la firma es genuina.

IPsec utiliza RSA (sistema criptográfico de claves públicas) para la autenticación en el contexto de IKE. El método de firmas RSA utiliza una configuración de firma digital en la que cada dispositivo firma un conjunto de datos de forma digital y lo envía a la otra parte. Las firmas RSA usan una entidad de certificación (CA) para generar un certificado digital de identidad exclusiva que se asigna a cada peer para la autenticación. El certificado digital de identidad tiene una función similar a la de una PSK, pero proporciona una seguridad mucho más sólida. Las personas que originan una sesión IKE y que responden a ella con firmas RSA envían su propio valor de ID, su certificado digital de identidad y un valor de firma RSA que consta de una serie de valores IKE, cifrados con el método de cifrado IKE negociado (como AES).

El algoritmo de firma digital (DSA) es otra opción para la autenticación.

Capítulo 7: Seguridad de la conectividad Site-to-Site 7.3.2.6 Marco del protocolo IPsec

Como se mencionó anteriormente, el marco del protocolo IPSec describe la mensajería para proteger las comunicaciones, pero depende de los algoritmos existentes.

En la figura 1, se describen dos protocolos IPSec principales:

- **Encabezado de autenticación (AH):**AH es el protocolo que se debe utilizar cuando no se requiere o no se permite la confidencialidad. Proporciona la autenticación y la integridad de datos para los paquetes IP que se transmiten entre dos sistemas. Sin embargo, AH no proporciona la confidencialidad (el cifrado) de datos de los paquetes. Todo el texto se transporta como texto no cifrado. Cuando se utiliza solo, el protocolo AH proporciona una protección poco eficaz.

- **Contenido de seguridad encapsulado (ESP):** es un protocolo de seguridad que proporciona confidencialidad y autenticación mediante el cifrado del paquete IP. El cifrado de paquetes IP oculta los datos y las identidades del origen y el destino. ESP autentica el paquete IP y el encabezado ESP internos. La autenticación proporciona la autenticación del origen de los datos y la integridad de los datos. Si bien el cifrado y la autenticación son optativos en ESP, se debe seleccionar, como mínimo, uno de ellos.

En la figura 2, se muestran los componentes de la configuración de IPSec. Se deben seleccionar cuatro componentes básicos del marco de IPsec.

- **Protocolo del marco de IPsec:** al configurar un gateway IPsec para proporcionar servicios de seguridad, se debe seleccionar un protocolo IPsec. Las opciones son una combinación de ESP y AH. En realidad, las opciones de ESP o ESP+AH casi siempre se seleccionan porque AH en sí mismo no proporciona el cifrado, como se muestra en la figura 3.

- **Confidencialidad (si se implementa IPsec con ESP):** el algoritmo de cifrado elegido se debe ajustar al nivel deseado de seguridad (DES, 3DES o AES). Se recomienda AES, ya que AES-GCM proporciona la mayor seguridad.

- **Integridad:** garantiza que el contenido no se haya alterado en tránsito. Se implementa mediante el uso de algoritmos de hash. Entre las opciones se incluye MD5 y SHA.

- **Autenticación:** representa la forma en que se autentican los dispositivos en cualquiera de los extremos del túnel VPN. Los dos métodos son PSK o RSA.

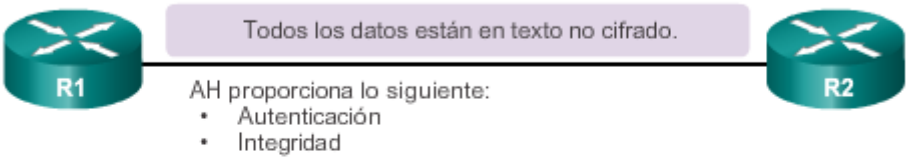
- **Grupo de algoritmos DH:** representa la forma en que se establece una clave secreta compartida entre los peers. Existen varias opciones, pero DH24 proporciona la mayor seguridad.

La combinación de estos componentes es la que proporciona las opciones de confidencialidad, integridad y autenticación para las VPN con IPsec.

Nota: en esta sección, se presentó IPsec para proporcionar una comprensión de cómo IPsec protege los túneles VPN. La configuración de VPN con IPsec excede el ámbito de este curso.

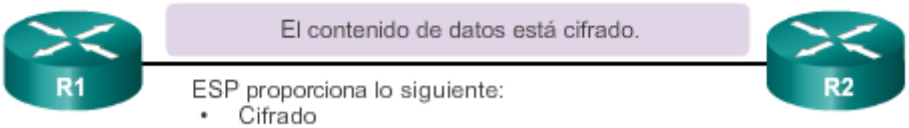
Marco del protocolo IPsec

Encabezado de autenticación



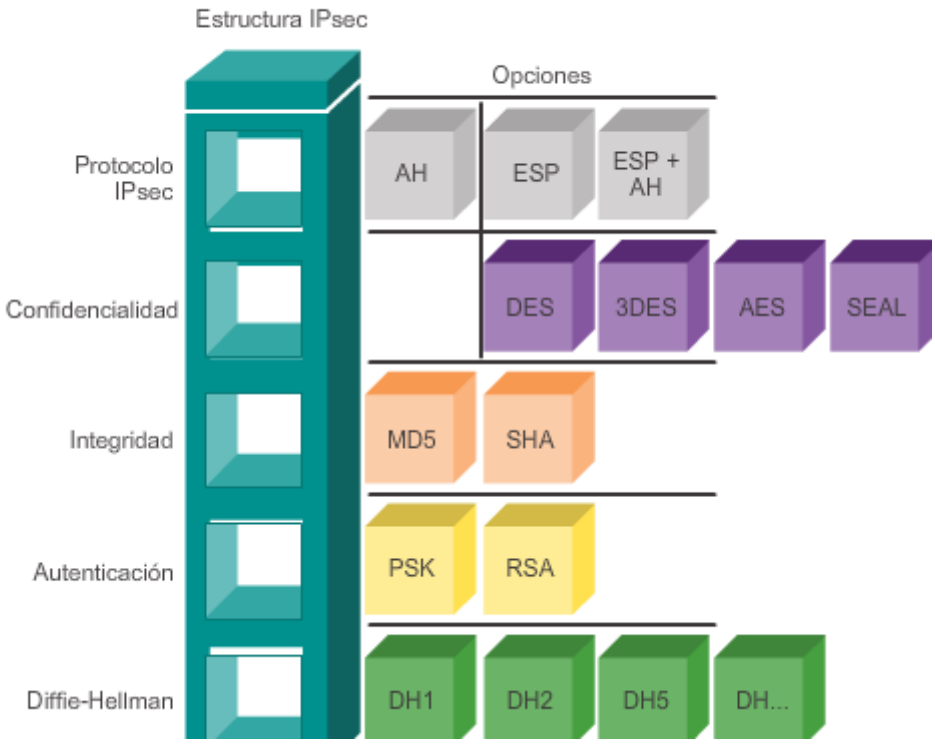
AH proporciona lo siguiente:
- Autenticación
- Integridad

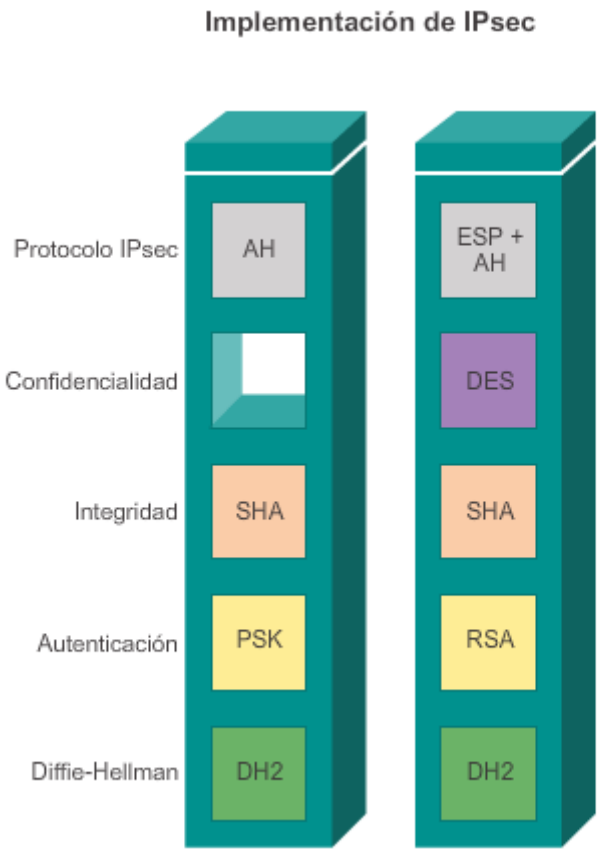
Contenido de seguridad encapsulado



ESP proporciona lo siguiente:
- Cifrado
- Autenticación
- Integridad

Marco del protocolo IPsec

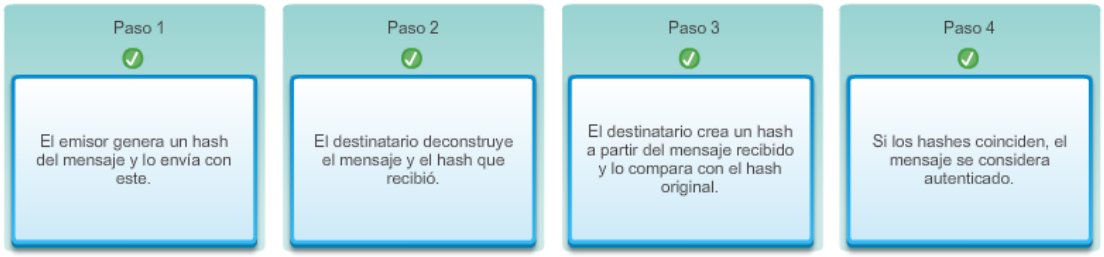




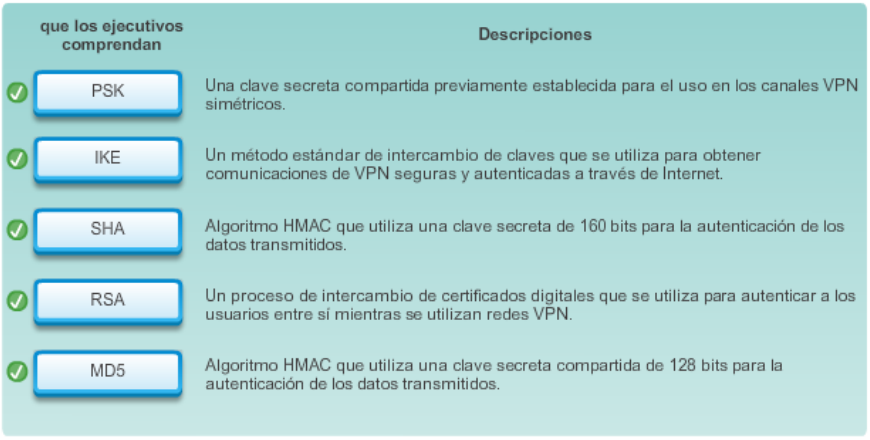
Capítulo 7: Seguridad de la conectividad Site-to-Site 7.3.2.7 Actividad: Identificar la terminología y los conceptos de IPsec

Actividad (parte 1): Identificar los algoritmos de cifrado IPsec
Arrastre la clasificación (simétrica o asimétrica) hasta el término o el concepto de cifrado correspondiente. Haga clic en el botón 2 para continuar la actividad.

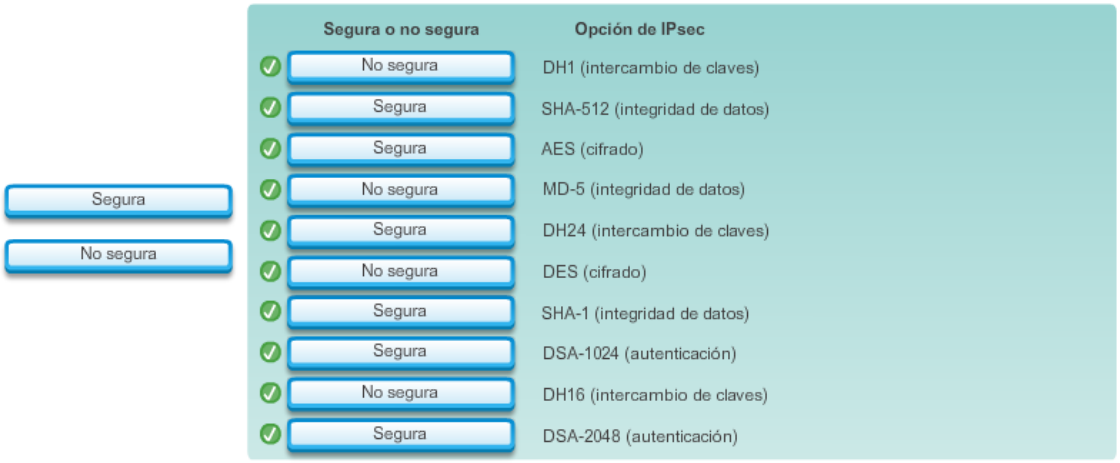
Actividad (parte 2): Identificar los pasos de la autenticación
Coloque los pasos del procedimiento de autenticación IPsec en el orden correcto para mostrar el proceso de autenticación e integridad de datos. Haga clic en el botón 3 para continuar la actividad.



Actividad (parte 3): Identificar la terminología de la autenticación y la integridad de datos
Una los términos relacionados con la autenticación y la integridad de datos con la descripción correspondiente. Haga clic en el botón 4 para continuar la actividad.



Actividad (parte 4): Identificar las opciones de seguridad de IPsec
Identifique cada opción de IPsec como configuración segura o no segura del protocolo IPsec.



Capítulo 7: Seguridad de la conectividad Site-to-Site 7.3.2.8 Packet Tracer: Configuración de GRE por IPsec (optativo)

Información básica/situación

Usted es el administrador de red de una empresa que desea configurar un túnel GRE por IPsec a una oficina remota. Todas las redes están configuradas localmente y solo necesitan que se configure el túnel y el cifrado.

Packet Tracer: Configuración de GRE por IPsec (optativo) (instrucciones)

Packet Tracer: Configuración de GRE por IPsec (optativo) (PKA)

Capítulo 7: Seguridad de la conectividad Site-to-Site 7.4.1.1 Tipos de VPN de acceso remoto

Las VPN se convirtieron en la solución lógica para la conectividad de acceso remoto por muchos motivos. Las VPN proporcionan comunicaciones seguras con derechos de acceso

hechos a la medida de los usuarios individuales, como empleados, contratistas y socios. También aumentan la productividad mediante la extensión de la red y las aplicaciones empresariales de forma segura, a la vez que reducen los costos de comunicación y aumentan la flexibilidad.

Básicamente, con la tecnología VPN, los empleados pueden llevar la oficina con ellos, incluido el acceso al correo electrónico y las aplicaciones de red. Las VPN también permiten que los contratistas y socios tengan acceso limitado a los servidores, a las páginas web o a los archivos específicos requeridos. Este acceso de red les permite contribuir a la productividad de la empresa sin comprometer la seguridad de la red.

Existen dos métodos principales para implementar VPN de acceso remoto:

- Capa de sockets seguros (SSL)
- Seguridad IP (IPsec)

El tipo de método VPN implementado se basa en los requisitos de acceso de los usuarios y en los procesos de TI de la organización.

Tanto la tecnología de VPN con SSL como la de VPN con IPsec ofrecen acceso a prácticamente cualquier aplicación o recurso de red. Las VPN con SSL ofrecen características como una fácil conectividad desde las computadoras de escritorio que no administra la empresa, un escaso o nulo mantenimiento del software de escritorio y portales web personalizados por el usuario al iniciar sesión.

Capítulo 7: Seguridad de la conectividad Site-to-Site 7.4.1.2 VPN con SSL de Cisco

VPN con SSL del IOS de Cisco es la primera solución de VPN con SSL basada en routers del sector. Ofrece conectividad desde cualquier ubicación, no solo desde los recursos administrados por las empresas, sino también desde las computadoras de los empleados, las computadoras de escritorio de los contratistas o de los socios de negocios, y los quioscos de Internet.

El protocolo SSL admite diversos algoritmos criptográficos para las operaciones, como la autenticación del servidor y el cliente entre sí, la transmisión de certificados y el establecimiento de claves de sesión. Las soluciones de VPN con SSL de Cisco se pueden personalizar para empresas de cualquier tamaño. Estas soluciones ofrecen muchas características y ventajas de conectividad de acceso remoto, incluido lo siguiente:

- Acceso total a la red, sin clientes y basado en Web, sin software de escritorio instalado previamente. Esto facilita el acceso remoto personalizado según los requisitos de usuario y de seguridad, y minimiza los costos de soporte de escritorio.
- Protección contra virus, gusanos, spyware y piratas informáticos en una conexión VPN mediante la integración de la seguridad de la red y de las terminales en la plataforma VPN con SSL de Cisco. Esto reduce los costos y la complejidad de la administración, ya que elimina la necesidad de contar con equipos de seguridad e infraestructura de administración adicionales.

- Uso de un único dispositivo tanto para VPN con SSL como para VPN con IPsec. Esto reduce los costos y la complejidad de la administración, ya que facilita servicios VPN sólidos de acceso remoto y de sitio a sitio desde una única plataforma con administración unificada.

VPN con SSL del IOS de Cisco es una tecnología que proporciona acceso remoto mediante un navegador web y el cifrado SSL nativo del navegador web. Alternativamente, puede proporcionar acceso remoto mediante el software Cisco AnyConnect Secure Mobility Client.

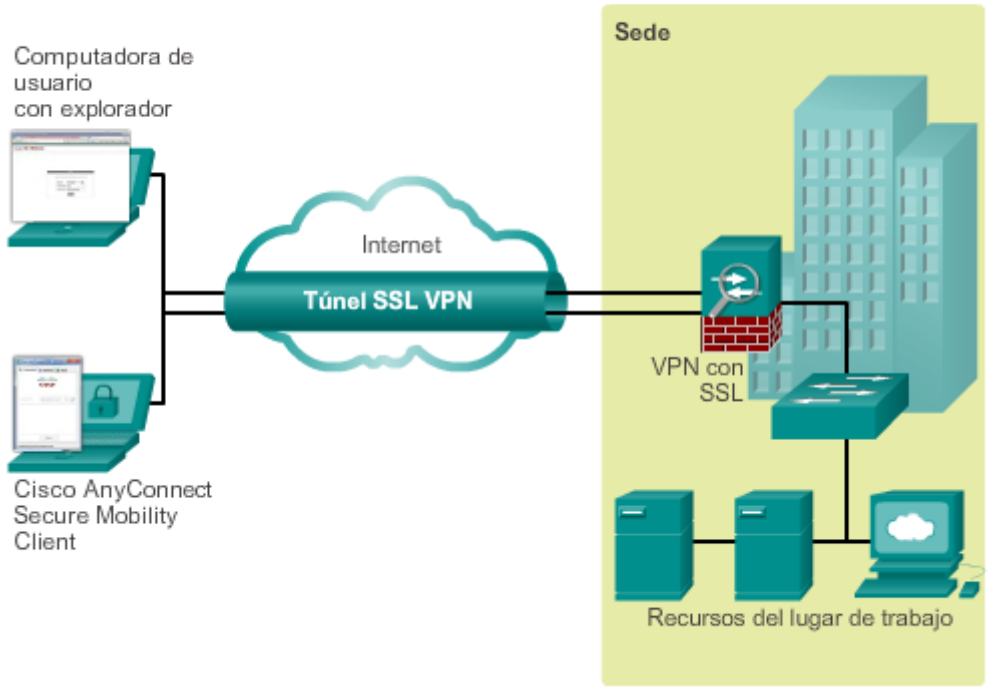
Cisco ASA proporciona dos modos principales de implementación que se encuentran en las soluciones de VPN con SSL de Cisco, como se muestra en la ilustración:

- **Cisco AnyConnect Secure Mobility Client con SSL:** requiere el cliente Cisco AnyConnect.

- **Cisco Secure Mobility Clientless SSL VPN:** requiere un explorador de Internet.

Cisco ASA se debe configurar para admitir la conexión VPN con SSL.

Soluciones VPN con SSL de Cisco



Capítulo 7: Seguridad de la conectividad Site-to-Site 7.4.1.3 Soluciones VPN con SSL de Cisco

Cisco AnyConnect Secure Mobility Client con SSL

Las VPN con SSL basadas en el cliente proporcionan acceso total de red del estilo de LAN para los usuarios autenticados. Sin embargo, los dispositivos remotos requieren la instalación de una aplicación cliente, como el cliente Cisco VPN o el más reciente AnyConnect, en el dispositivo para usuarios finales.

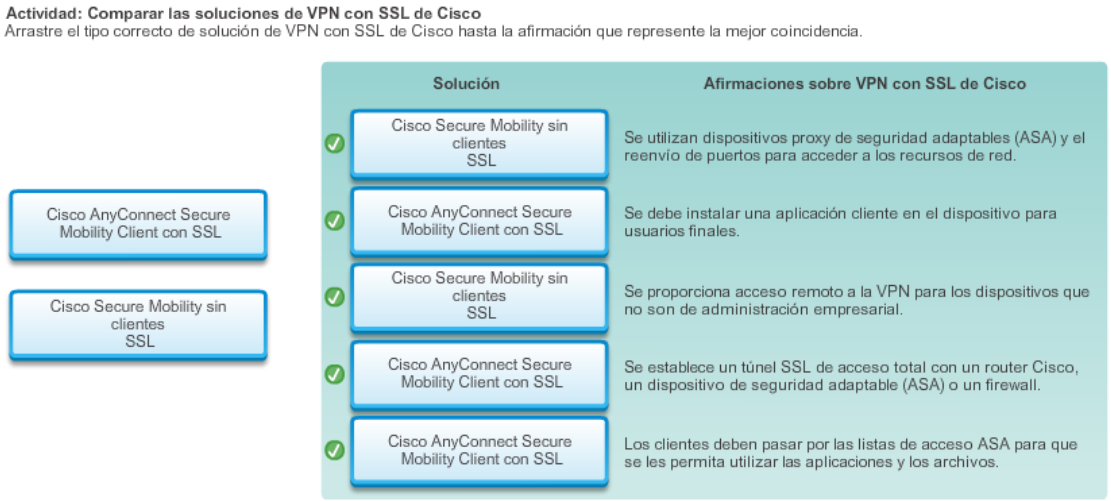
En un Cisco ASA básico configurado para el tunneling completo y una solución de VPN con SSL de acceso remoto, los usuarios remotos utilizan Cisco AnyConnect Secure Mobility Client, que se muestra en la figura 1, para establecer un túnel SSL con Cisco ASA. Después de que Cisco ASA establece la VPN con el usuario remoto, este usuario puede reenviar tráfico IP por el túnel SSL. Cisco AnyConnect Secure Mobility Client crea una interfaz de red virtual para proporcionar esta funcionalidad. El cliente puede utilizar cualquier aplicación para acceder a cualquier recurso, sujeto a las reglas de acceso, detrás del gateway VPN de Cisco ASA.

VPN con SSL de Cisco Secure Mobility sin clientes

El modelo de implementación de VPN con SSL sin clientes permite que las empresas proporcionen acceso a los recursos corporativos incluso cuando la empresa no administra el dispositivo remoto. En este modelo de implementación, Cisco ASA se usa como dispositivo proxy de los recursos en red. Proporciona una interfaz de portal web para que los dispositivos remotos naveguen la red mediante capacidades de reenvío de puertos.

En una solución de VPN con SSL básica sin clientes de Cisco ASA, los usuarios remotos utilizan un navegador web estándar para establecer una sesión SSL con Cisco ASA, como se muestra en la figura 2. Cisco ASA presenta al usuario un portal web por el que puede acceder a los recursos internos. En la solución básica sin clientes, el usuario puede acceder solo a algunos servicios, como las aplicaciones web internas y los recursos de intercambio de archivos basados en el explorador, como se muestra en la figura 3.

Capítulo 7: Seguridad de la conectividad Site-to-Site 7.4.1.4 Actividad: Comparar las soluciones de VPN con SSL de Cisco



Capítulo 7: Seguridad de la conectividad Site-to-Site 7.4.2.1 Acceso remoto a IPsec

Muchas aplicaciones requieren la seguridad de una conexión VPN de acceso remoto con IPsec para autenticar y cifrar datos. Cuando se implementan VPN para trabajadores a distancia y sucursales pequeñas, la facilidad de implementación es fundamental si los recursos técnicos no están disponibles para la configuración de VPN en un router del sitio remoto.

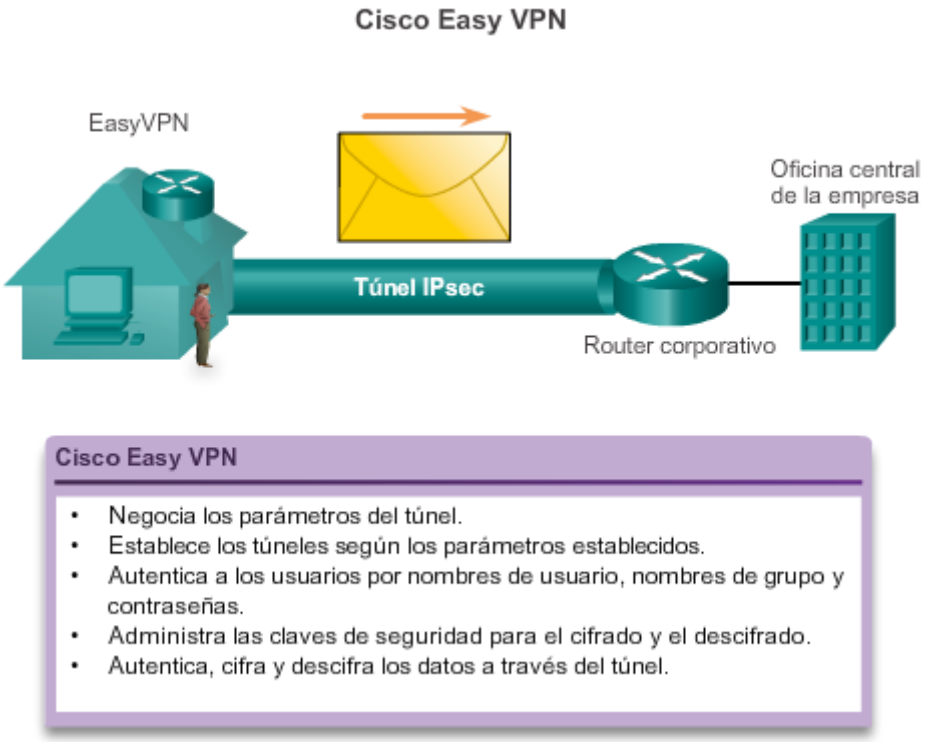
La característica de la solución Cisco Easy VPN ofrece flexibilidad, escalabilidad y facilidad de uso para las VPN con IPsec de sitio a sitio y de acceso remoto. La solución Cisco Easy VPN consta de tres componentes:

- **Cisco Easy VPN Server:** es un router con IOS de Cisco o un firewall Cisco ASA que funciona como terminal de cabecera de la VPN en las VPN de sitio a sitio o de acceso remoto.

- **Cisco Easy VPN Remote:** es un router con IOS de Cisco o un firewall Cisco ASA que funciona como cliente VPN remoto.

- **Cisco VPN Client:** una aplicación compatible en una computadora que se utiliza para acceder a un servidor Cisco VPN.

El uso de Cisco Easy VPN Server permite que los trabajadores móviles y a distancia que utilizan un cliente VPN en sus computadoras o que utilizan Cisco Easy VPN Remote en un router perimetral puedan crear túneles IPsec seguros para acceder a la intranet de la oficina central, como se muestra en la ilustración.



Capítulo 7: Seguridad de la conectividad Site-to-Site 7.4.2.2 Cisco Easy VPN Server e Easy VPN Remote

Cisco Easy VPN Server

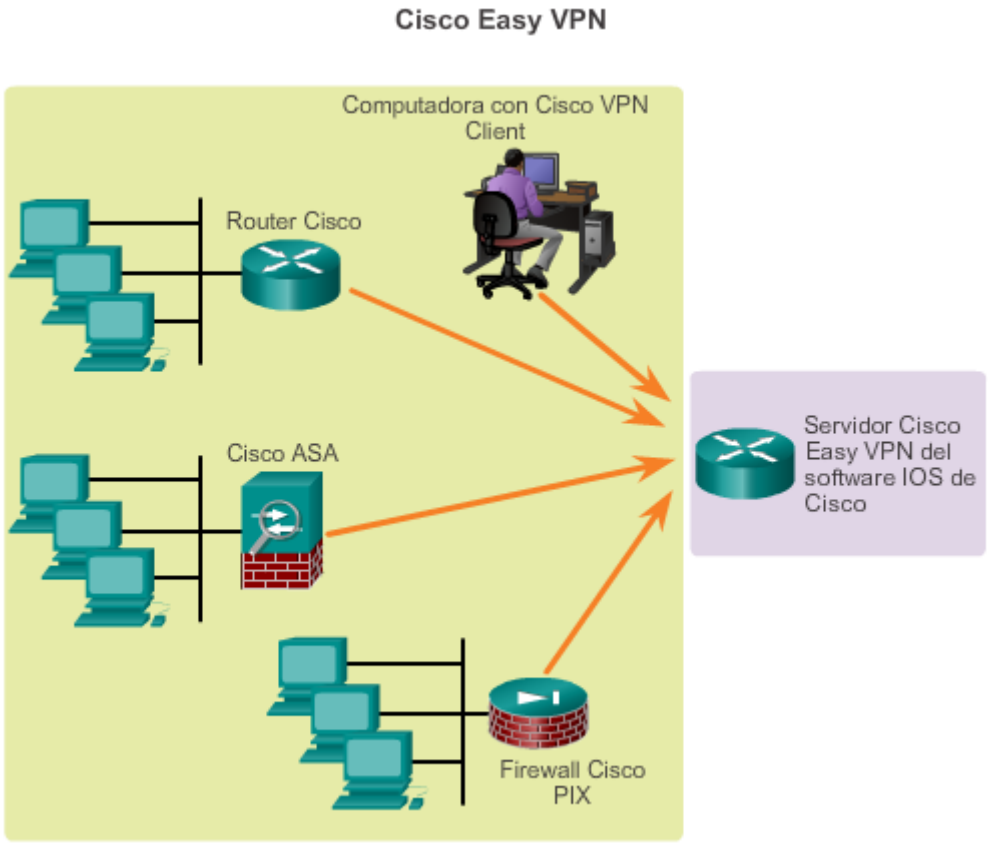
Cisco Easy VPN Server permite que los trabajadores móviles y a distancia que utilizan un software de cliente VPN en sus computadoras puedan crear túneles IPsec seguros para acceder a la intranet de la oficina central donde se ubican datos y aplicaciones fundamentales.

Permite que los routers con IOS de Cisco y los firewalls Cisco ASA funcionen como terminales de cabecera de las VPN de sitio a sitio o de acceso remoto. Los dispositivos de oficina remota utilizan la característica Cisco Easy VPN Remote o la aplicación Cisco VPN Client para conectarse al servidor, que después inserta las políticas de seguridad definidas en el dispositivo VPN remoto. Esto asegura que esas conexiones cuenten con las políticas actualizadas antes de que se establezca la conexión.

Cisco Easy VPN Remote

Cisco Easy VPN Remote permite que los clientes de software o los routers con IOS de Cisco funcionen como clientes VPN remotos. Estos dispositivos pueden recibir las políticas de seguridad de Cisco Easy VPN Server, lo que minimiza los requisitos de configuración de VPN en la ubicación remota. Esta solución rentable es ideal para oficinas remotas con poco soporte de TI o para implementaciones de equipo local del cliente (CPE) a gran escala donde es poco práctico configurar varios dispositivos remotos de forma individual.

En la ilustración, se muestran tres dispositivos de red con Easy VPN Remote habilitado, todos conectados a Easy VPN Server para obtener los parámetros de configuración.



Capítulo 7: Seguridad de la conectividad Site-to-Site 7.4.2.3 Cisco Easy VPN Client

Cliente Cisco VPN

La herramienta Cisco VPN Client es fácil de implementar y de utilizar. Permite que las organizaciones establezcan túneles VPN de extremo a extremo cifrados para proporcionar una conectividad segura a los empleados móviles o los trabajadores a distancia.

Para iniciar una conexión IPsec mediante Cisco VPN Client, todo lo que debe hacer el usuario es abrir la ventana de Cisco VPN Client, la cual se muestra en la figura 1. La aplicación Cisco VPN Client indica los sitios disponibles configurados previamente. El usuario hace doble clic en un sitio para seleccionarlo, y el cliente VPN inicia la conexión IPsec. En el cuadro de diálogo de autenticación del usuario, se autentica al usuario con un nombre de usuario y una contraseña, como se muestra en la figura 2. Después de la autenticación, Cisco VPN Client muestra el estado conectado.

La mayoría de los parámetros de VPN se definen en Easy VPN Server del IOS de Cisco para simplificar la implementación. Después de que un cliente remoto inicia una conexión de túnel VPN, Cisco Easy VPN Server inserta las políticas de IPSec en el cliente, lo que minimiza los requisitos de configuración en la ubicación remota.

Esta solución simple y altamente escalable es ideal para implementaciones de acceso remoto a gran escala donde es poco práctico configurar las políticas para varias computadoras remotas de forma individual. Además, esta arquitectura asegura que esas conexiones cuenten con las políticas de seguridad actualizadas y elimina los costos operativos asociados al mantenimiento de un método coherente de administración de políticas y claves.

Nota: la configuración de Cisco VPN Client excede el ámbito de este curso. Visite el sitio www.cisco.com para obtener más información.

Capítulo 7: Seguridad de la conectividad Site-to-Site 7.4.2.4 Comparación de IPsec y SSL

Tanto la tecnología de VPN con SSL como la de IPsec ofrecen acceso a prácticamente cualquier aplicación o recurso de red, como se muestra en la ilustración. Las VPN con SSL ofrecen características como una fácil conectividad desde las computadoras de escritorio que no administra la empresa, un escaso o nulo mantenimiento del software de escritorio y portales web personalizados por el usuario al iniciar sesión.

IPsec supera a SSL en muchas formas importantes:

- La cantidad de aplicaciones que admite
- La solidez del cifrado
- La solidez de la autenticación
- La seguridad general

Cuando la seguridad representa un problema, IPsec es la mejor opción. Si el soporte y la facilidad de implementación son los principales problemas, considere utilizar SSL.

IPsec y las VPN con SSL se complementan porque resuelven diferentes problemas. Según las necesidades, una organización puede implementar una o ambas. Este enfoque complementario permite que un único dispositivo, como un router ISR o un dispositivo de firewall ASA, pueda satisfacer todos los requisitos de los usuarios de acceso remoto. Si bien muchas soluciones ofrecen IPsec o SSL, las soluciones de VPN de acceso remoto de Cisco ofrecen ambas tecnologías integradas en una única plataforma con administración unificada. Si se ofrece tanto la tecnología IPsec como SSL, las organizaciones pueden personalizar su VPN de acceso remoto sin ningún hardware adicional ni complejidad de administración.

Comparación de IPsec y SSL

	SSL	IPsec
Aplicaciones	Aplicaciones habilitadas para Web, uso compartido de archivos, correo electrónico	Todas las aplicaciones basadas en IP
Cifrado	**Moderado a seguro** Longitudes de clave de 40bits a 256bits	**Seguro** Longitudes de clave de 56bits a 256bits
Autenticación	**Moderada** Autenticación unidireccional o bidireccional	**Segura** Autenticación bidireccional mediante secretos compartidos o certificados digitales
Complejidad de conexión	**Baja** Solo se requiere un navegador web.	**Media** Puede resultar difícil para usuarios sin conocimientos técnicos.
Opciones de conexión	Cualquier dispositivo se puede conectar.	Solo se pueden conectar dispositivos específicos con una configuración específica.

Capítulo 7: Seguridad de la conectividad Site-to-Site 7.4.2.5 Actividad: Identificar la características de acceso remoto

Actividad: Identificar las características del acceso remoto por IPsec y SSL

Clasifique las características de acceso remoto con SSL o IPsec.

Capítulo 7: Seguridad de la conectividad Site-to-Site 7.5.1.1 Actividad de clase: Diseño de la planificación de VPN

Diseño de planificación VPN

Su pequeña o mediana empresa recibió algunos contratos nuevos recientemente. Esto aumentó la necesidad de contratar trabajadores a distancia y servicios externos para la carga

de trabajo. Los proveedores y clientes de los nuevos contratos también necesitan acceso a la red a medida que progresan los proyectos.

Como administrador de red de la empresa, usted reconoce que se deben incorporar VPN como parte de la estrategia de red para admitir un acceso seguro para los trabajadores a distancia, los empleados y los proveedores o clientes.

A fin de preparar la implementación de las VPN en la red, elabora una lista de comprobación de planificación para presentarla en la siguiente reunión del departamento.

Actividad de clase: Diseño de la planificación de VPN

Capítulo 7: Seguridad de la conectividad Site-to-Site 7.5.1.2 Packet Tracer: desafío de integración de habilidades

Información básica/situación

Esta actividad le permite poner en práctica una variedad de habilidades, incluida la configuración de Frame Relay, PPP con CHAP, NAT con sobrecarga (PAT) y túneles GRE. Los routers están parcialmente configurados.

Packet Tracer: Desafío de integración de habilidades (instrucciones)

Packet Tracer: Desafío de integración de habilidades (PKA)

Capítulo 7: Seguridad de la conectividad Site-to-Site 7.5.1.3 Resumen

Las VPN se utilizan para crear una conexión segura de red privada de extremo a extremo a través de redes externas, como Internet. Una VPN de sitio a sitio utiliza un dispositivo de gateway VPN en el límite de ambos sitios. Los hosts terminales desconocen la VPN y no cuentan con software de soporte adicional.

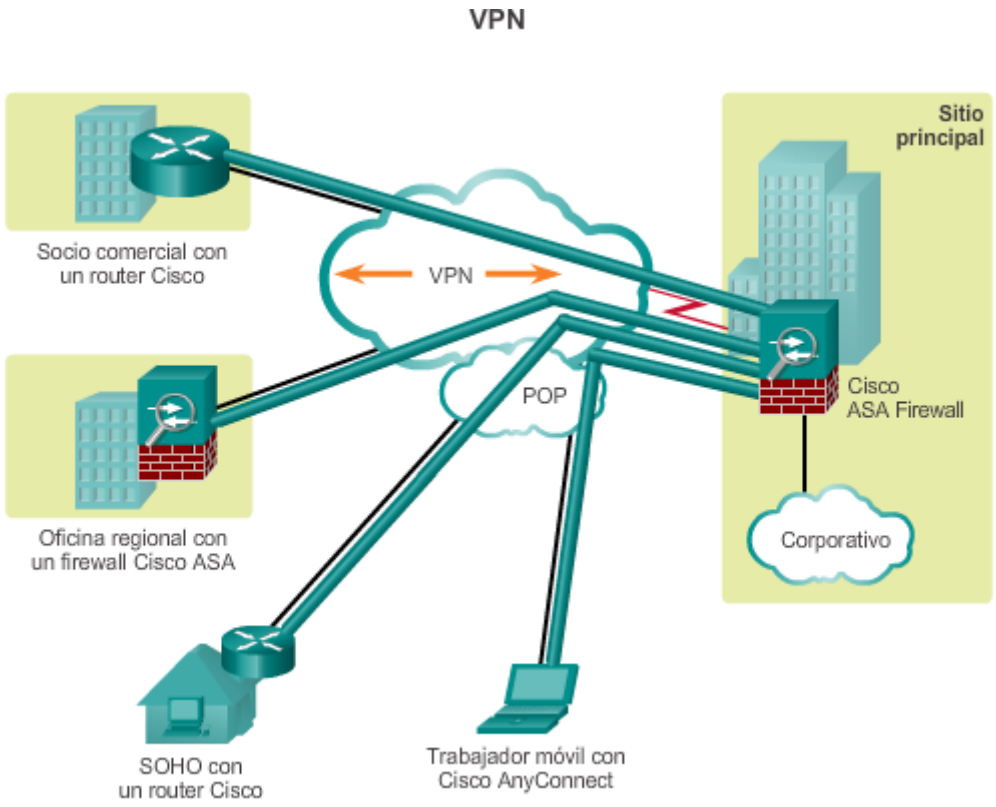
Una VPN de acceso remoto requiere que se instale un software en el dispositivo host individual que accede a la red desde una ubicación remota. Los dos tipos de VPN de acceso remoto son SSL e IPsec. La tecnología SSL puede proporcionar acceso remoto mediante el navegador web de un cliente y el cifrado SSL nativo del navegador. Mediante el uso del software Cisco AnyConnect en el cliente, los usuarios pueden obtener acceso total de red del estilo de LAN con SSL.

GRE es un protocolo de tunneling de VPN de sitio a sitio básico no seguro que puede encapsular una amplia variedad de tipos de paquete de protocolo dentro de túneles IP, lo que permite que una organización entregue otros protocolos mediante una WAN basada en IP. En la actualidad, se utiliza principalmente para entregar tráfico de multidifusión IP o IPv6 a través de una conexión IPv4 de solo unidifusión.

IPsec, un estándar IETF, es un túnel seguro que funciona en la capa 3 del modelo OSI que puede proteger y autenticar paquetes IP entre peers IPsec. Puede proporcionar confidencialidad mediante el cifrado, la integridad de datos, la autenticación y la protección

antirreproducción. La integridad de datos se proporciona mediante un algoritmo de hash, como MD5 o SHA. El método de autenticación de peers PSK o RSA proporciona la autenticación.

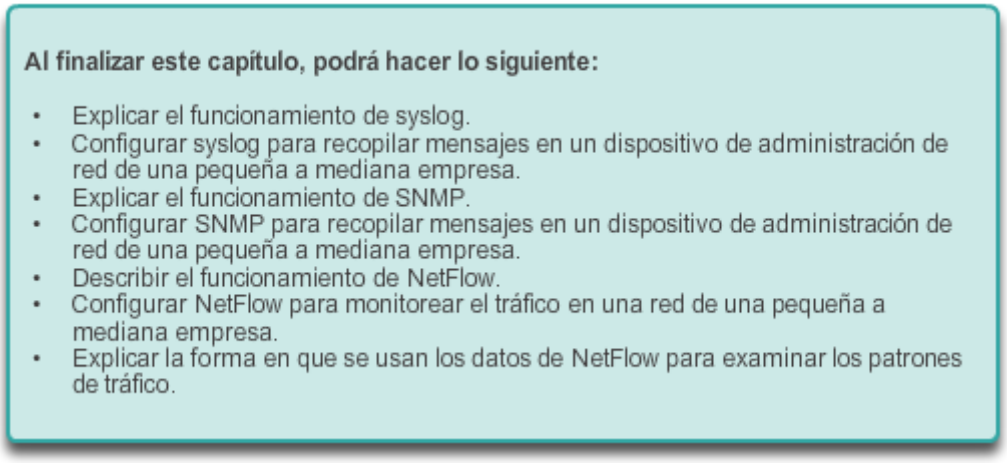
El nivel de confidencialidad que proporciona el cifrado depende del algoritmo utilizado y la longitud de la clave. El cifrado puede ser simétrico o asimétrico. DH es un método que se utiliza para intercambiar de forma segura las claves para cifrar datos.



Capítulo 8: Supervisión de la red 8.0.1.1 Introducción

Supervisar una red en funcionamiento puede proporcionar información a un administrador de red para administrar la red de forma proactiva e informar estadísticas de uso de la red a otros. La actividad de los enlaces, las tasas de error y el estado de los enlaces son algunos de los factores que contribuyen a que un administrador de red determine el estado y el uso de una red. Recopilar y revisar esta información en el transcurso del tiempo permite que un administrador de red vea y proyecte el crecimiento, y puede contribuir a que el administrador detecte y reemplace una parte defectuosa antes de que falle por completo.

En este capítulo, se abarcan tres protocolos que puede usar un administrador de red para controlar la red. Syslog, SNMP y NetFlow son protocolos populares con diferentes puntos fuertes y débiles. Juntos proporcionan un buen conjunto de herramientas para comprender qué sucede en una red. El protocolo NTP se utiliza para sincronizar la hora a través de los dispositivos, lo cual es especialmente importante al intentar comparar los archivos de registro de distintos dispositivos.



Capítulo 8: Supervisión de la red 8.0.1.2 Actividad de clase: Desarrollo del mantenimiento de red

Desarrollo de mantenimiento de la red

Actualmente, no hay políticas o procedimientos formales para registrar los problemas que se experimentan en la red de su empresa. Además, cuando ocurren problemas de red, debe probar varios métodos para encontrar las causas, y este enfoque lleva tiempo.

Usted sabe que debe de existir una mejor manera de resolver estos problemas. Decide crear un plan de mantenimiento de red para conservar los registros de reparación e identificar las causas de los errores en la red.

Actividad de clase: Desarrollo del mantenimiento de red

Capítulo 8: Supervisión de la red 8.1.1.1 Introducción a syslog

Cuando ocurren ciertos eventos en una red, los dispositivos de red tienen mecanismos de confianza para notificar mensajes detallados del sistema al administrador. Estos mensajes pueden ser importantes o no. Los administradores de red tienen una variedad de opciones para almacenar, interpretar y mostrar estos mensajes, así como para recibir esos mensajes que podrían tener el mayor impacto en la infraestructura de la red.

El método más común para acceder a los mensajes del sistema que proporcionan los dispositivos de red es utilizar un protocolo denominado “syslog”.

El término “syslog” se utiliza para describir un estándar. También se utiliza para describir el protocolo desarrollado para ese estándar. El protocolo syslog se desarrolló para los sistemas UNIX en la década de los ochenta, pero la IETF lo registró por primera vez como RFC 3164 en 2001. Syslog usa el puerto UDP 514 para enviar mensajes de notificación de eventos a través de redes IP a recopiladores de mensajes de eventos, como se muestra en la ilustración.

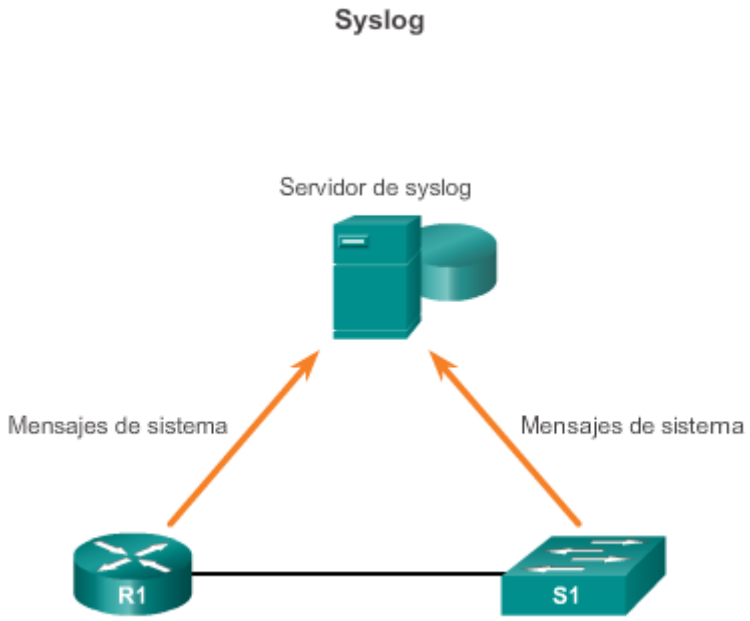
Muchos dispositivos de red admiten syslog, incluidos routers, switches, servidores de aplicación, firewalls y otros dispositivos de red. El protocolo syslog permite que los dispositivos

de red envíen los mensajes del sistema a servidores de syslog a través de la red. Es posible armar una red especial fuera de banda (OOB) para este propósito.

Existen varios paquetes de software diferentes de servidores de syslog para Windows y UNIX. Muchos de ellos son freeware.

El servicio de registro de syslog proporciona tres funciones principales:

- La capacidad de recopilar información de registro para el control y la resolución de problemas
- La capacidad de seleccionar el tipo de información de registro que se captura
- La capacidad de especificar los destinos de los mensajes de syslog capturados



Capítulo 8: Supervisión de la red 8.1.1.2 Funcionamiento de syslog

En los dispositivos de red Cisco, el protocolo syslog comienza enviando los mensajes del sistema y el resultado del comando **debug** a un proceso de registro local interno del dispositivo. La forma en que el proceso de registro administra estos mensajes y resultados se basa en las configuraciones del dispositivo. Por ejemplo, los mensajes de syslog se pueden enviar a través de la red a un servidor de syslog externo. Estos mensajes se pueden recuperar sin necesidad de acceder al dispositivo propiamente dicho. Los resultados y los mensajes de registro almacenados en el servidor externo se pueden incluir en varios informes para facilitar la lectura.

Por otra parte, los mensajes de syslog se pueden enviar a un búfer interno. Los mensajes enviados al búfer interno solo se pueden ver mediante la CLI del dispositivo.

Por último, el administrador de red puede especificar que solo se envíen determinados tipos de mensajes del sistema a varios destinos. Por ejemplo, se puede configurar el dispositivo para

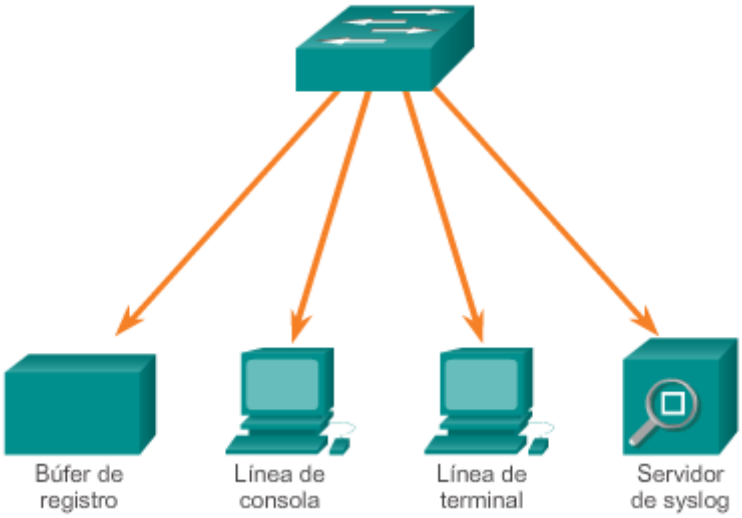
que reenvíe todos los mensajes del sistema a un servidor de syslog externo. Sin embargo, los mensajes del nivel de depuración se reenvían al búfer interno, y solo el administrador puede acceder a ellos desde la CLI.

Como se muestra en la ilustración, los destinos comunes para los mensajes de syslog incluyen lo siguiente:

- Búfer de registro (RAM dentro de un router o switch)
- Línea de consola
- Línea de terminal
- Servidor de syslog

Es posible controlar los mensajes del sistema de manera remota viendo los registros en un servidor de syslog o accediendo al dispositivo mediante Telnet, SSH o a través del puerto de consola.

Opciones de destino de mensajes de syslog



Capítulo 8: Supervisión de la red 8.1.1.3 Formato de los mensajes de syslog

Los dispositivos de Cisco generan mensajes de syslog como resultado de los eventos de red. Cada mensaje de syslog contiene un nivel de gravedad y una instalación.

Cuanto más bajos son los números de nivel, más fundamentales son las alarmas de syslog. El nivel de gravedad de los mensajes se puede establecer para controlar dónde se muestra cada tipo de mensaje (es decir, en la consola o los otros destinos). En la figura 1, se muestra la lista completa de los niveles de syslog.

Cada nivel de syslog tiene su propio significado:

- **Nivel de advertencia, nivel de emergencia:** estos son mensajes de error sobre software o hardware que funciona mal; estos tipos de mensajes significan que la funcionalidad del dispositivo se ve afectada. La gravedad del problema determina el nivel real de syslog que se aplica.

- **Nivel de depuración:** este nivel indica que los mensajes son resultados que se generan a partir de la emisión de varios comandos **debug**.

- **Nivel de notificación:** el nivel de notificación solo proporciona información, la funcionalidad del dispositivo no se ve afectada. Los mensajes de interfaz activa o inactiva, o de reinicio del sistema se muestran en el nivel de notificación.

Además de especificar la gravedad, los mensajes de syslog también contienen información sobre la instalación. Las instalaciones de syslog son identificadores de servicios que identifican y categorizan los datos de estado del sistema para informar los mensajes de error y de eventos. Las opciones de instalación de registro disponibles son específicas del dispositivo de red. Por ejemplo, los switches Cisco de la serie 2960 que ejecutan el IOS de Cisco versión 15.0(2) y los routers Cisco 1941 que ejecutan el IOS de Cisco versión 15.2(4) admiten 24 opciones de instalación que se categorizan en 12 tipos de instalación.

Algunas instalaciones comunes de mensajes de syslog que se informan en los routers con IOS de Cisco incluyen lo siguiente:

- IP

- Protocolo OSPF

- Sistema operativo SYS

- Seguridad IP (IPsec)

- IP de interfaz (IF)

De manera predeterminada, el formato de los mensajes de syslog en el software IOS de Cisco es el siguiente:

seq no: timestamp: %facility-severity-MNEMONIC: description

Los campos incluidos en el mensaje de syslog del software IOS de Cisco se explican en la figura 2.

Por ejemplo, el resultado de ejemplo de un switch Cisco para un enlace EtherChannel que cambia al estado activo es el siguiente:

00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up

Aquí la instalación es LINK, y el nivel de gravedad es 3, con la MNEMOTÉCNICA UPDOWN.

Los mensajes más comunes son los de enlace activo y enlace inactivo, y los mensajes que produce un dispositivo cuando sale del modo de configuración. Si se configura el registro de ACL, el dispositivo genera mensajes de syslog cuando los paquetes coinciden con una condición de parámetros.

Nivel de gravedad de syslog

Nombre de la gravedad	Nivel de gravedad	Explicación
Emergencia	Nivel 0	El sistema no se puede usar.
Alerta	Nivel 1	Se necesita una acción inmediata.
Crítico	Nivel 2	Condición crítica.
Error	Nivel 3	Condición de error.
Advertencia	Nivel 4	Condición de advertencia.
Notificación	Nivel 5	Condición normal pero importante.
informativo	Nivel 6	Mensaje informativo.
Depuración	Nivel 7	Mensaje de depuración.

Formato de los mensajes de syslog

Campo	Explicación
seq no	Marca los mensajes de registro con un número de secuencia solamente si se configuró el comando de configuración global`service sequence-numbers`
timestamp	Fecha y hora del mensaje o del evento, aparece solamente si se configuró el comando de configuración global `service timestamps`.
facility	La instalación a la que se refiere el mensaje.
severity	Código de un único digito entre 0 y 7 que indica la gravedad del mensaje.
MNEMONIC	Cadena de texto que describe el mensaje de forma exclusiva.
descripción	Cadena de texto que contiene información detallada sobre el evento que se informa.

Capítulo 8: Supervisión de la red 8.1.1.4 Marca de hora del servicio

Los mensajes de registro se pueden marcar con la hora, y se puede establecer la dirección de origen de los mensajes de syslog. Esto mejora la depuración y la administración en tiempo real.

Cuando se introduce el comando del modo de configuración global **service timestamps log uptime**, se muestra la cantidad de tiempo que transcurrió desde la última vez que se arrancó el switch en los eventos registrados. Una versión más útil de este comando aplica la palabra clave**datetime** en lugar de la palabra clave**uptime**; esto hace que cada evento registrado muestre la fecha y la hora asociadas al evento.

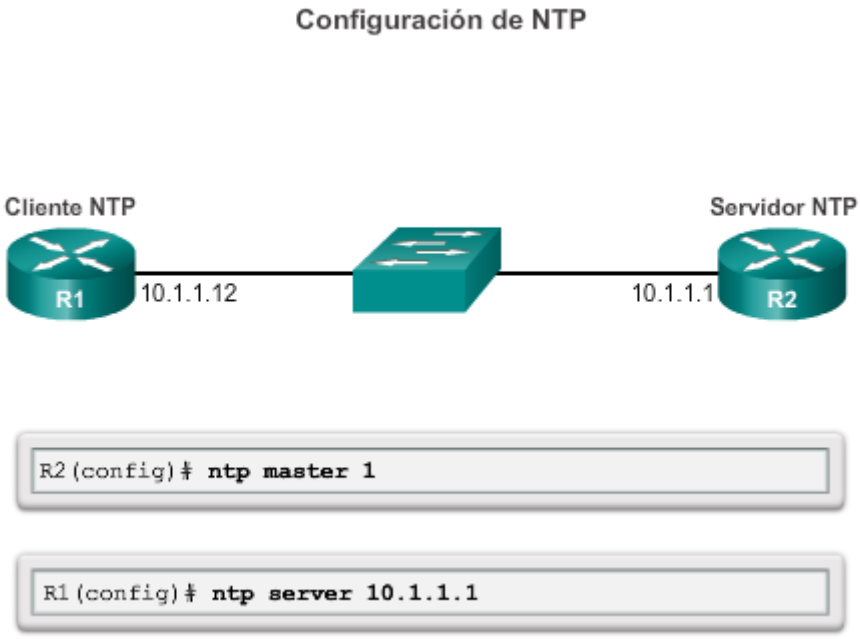
Cuando se utiliza la palabra clave**datetime**, se debe establecer el reloj en el dispositivo de red. Esto se puede lograr de dos maneras:

- Configuración manual mediante el comando **clock set**
- Configuración automática mediante el protocolo NTP

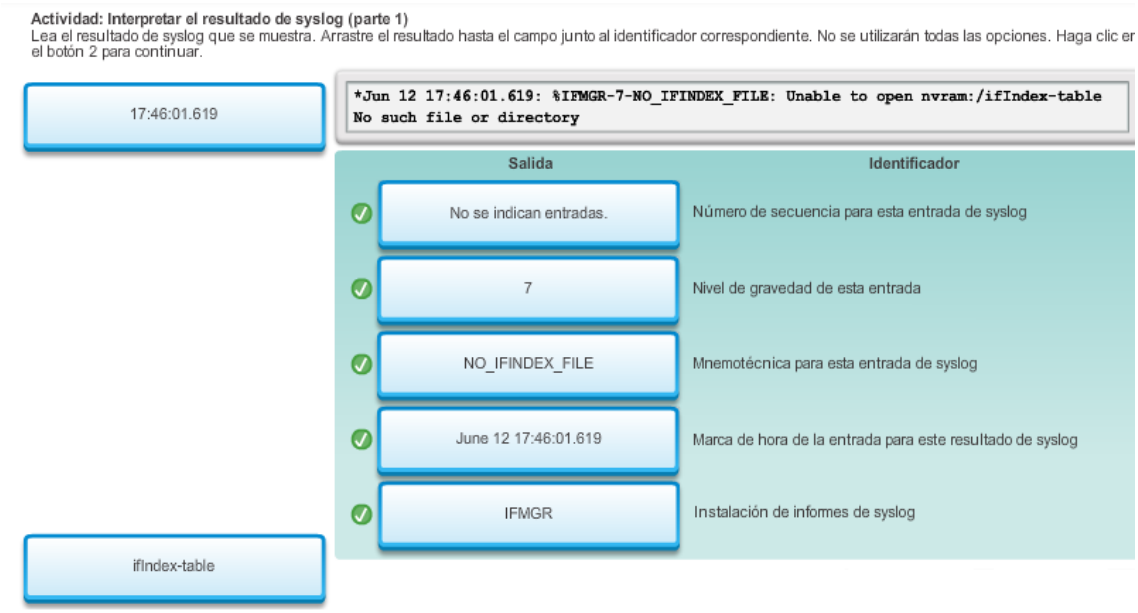
Recuerde que NTP es un protocolo que se utiliza para permitir que los dispositivos de red sincronicen la configuración de la hora con un servidor NTP.

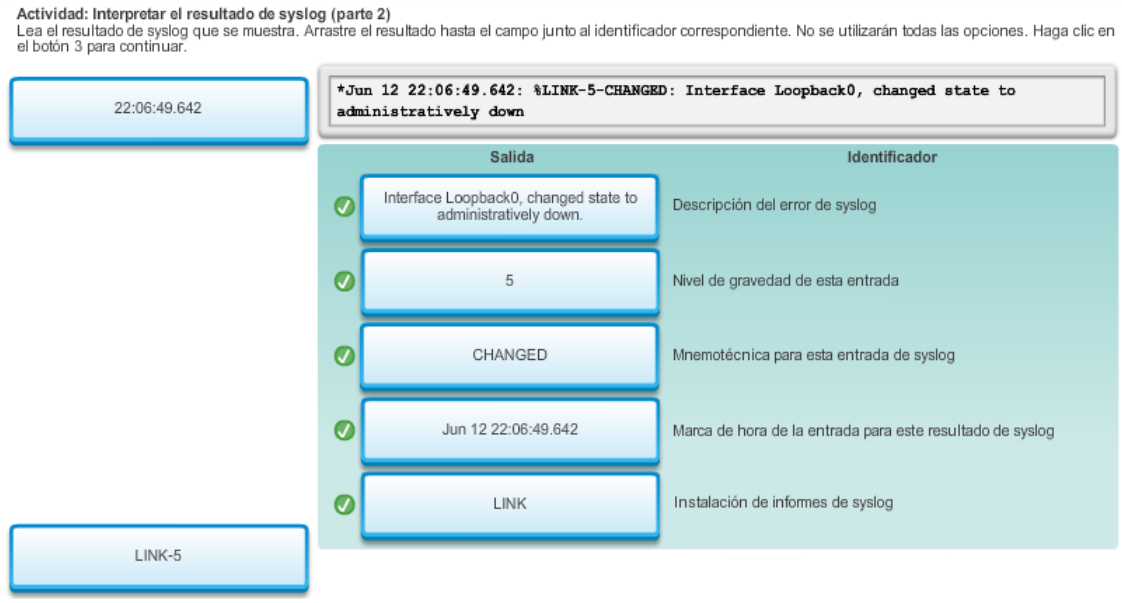
Para permitir que un servidor horario NTP sincronice el reloj del software, use el comando **ntp server** *dirección-IP*del modo de configuración global. En la ilustración, se muestra un ejemplo de configuración. El R1 está configurado como cliente NTP, mientras que el router R2 funciona como servidor NTP autoritativo. Un dispositivo de red se puede configurar como servidor NTP, para que los otros dispositivos sincronicen fuera de su hora, o como cliente NTP.

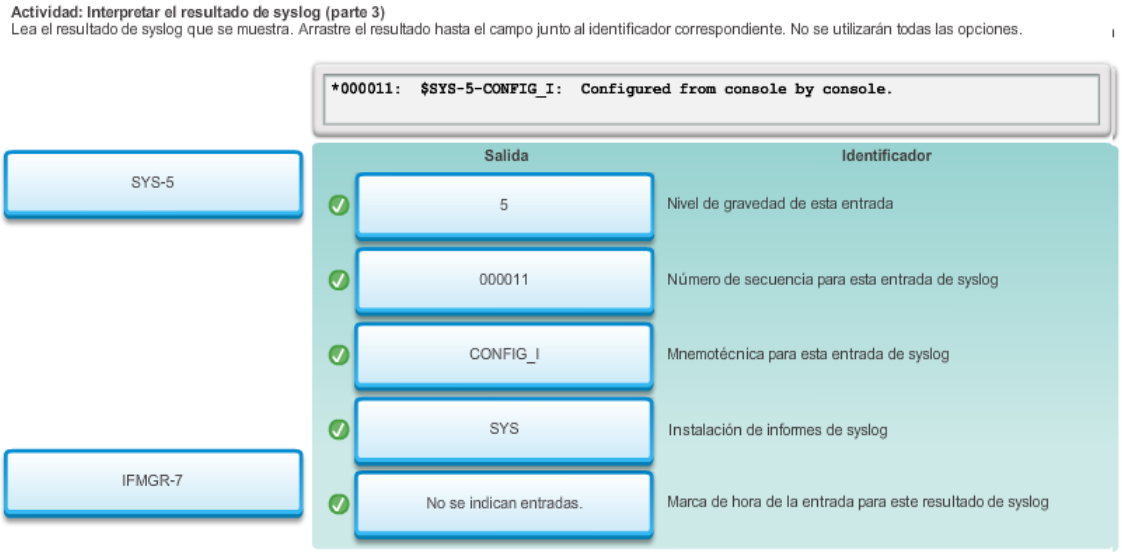
Para el resto del capítulo, se supone que se estableció el reloj y se configuró el comando **service timestamps log datetime** en todos los dispositivos.



Capítulo 8: Supervisión de la red 8.1.1.5 Actividad: Interpretar el resultado de syslog







Capítulo 8: Supervisión de la red 8.1.2.1 Servidor de syslog

Para ver los mensajes de syslog, se debe instalar un servidor de syslog en una estación de trabajo en la red. Hay varias versiones de freeware y shareware de syslog, así como versiones empresariales para comprar. En la figura 1, se muestra una versión de evaluación del daemon de syslog Kiwi en una máquina con Windows 7.

El servidor de syslog proporciona una interfaz relativamente fácil de usar para ver el resultado de syslog. El servidor analiza el resultado y coloca los mensajes en columnas predefinidas para interpretarlos con facilidad. Si se configuran las marcas de hora en el dispositivo de red que origina los mensajes de syslog, se muestra la fecha y hora de cada mensaje en el resultado del servidor de syslog, como se muestra en la figura 2.

Los administradores de red pueden navegar fácilmente a través de una gran cantidad de datos que se recopilan en un servidor de syslog. Una ventaja de ver los mensajes de syslog en un servidor de syslog es la capacidad de realizar búsquedas granulares a través de los datos.

Además, un administrador de red puede eliminar rápidamente de la base de datos los mensajes de syslog que no son importantes.

Capítulo 8: Supervisión de la red 8.1.2.2 Registro predeterminado

De forma predeterminada, los routers y switches de Cisco envían mensajes de registro a la consola para todos los niveles de gravedad. En algunas versiones del IOS, el dispositivo también almacena en búfer los mensajes de registro de manera predeterminada. Para habilitar estas dos configuraciones, utilice los comandos de configuración global **logging console** y**logging buffered**, respectivamente.

El comando **show logging** muestra la configuración predeterminada del servicio de registro en un router Cisco, como se muestra en la ilustración. En las primeras líneas del resultado, se proporciona información sobre el proceso de registro, y al final del resultado se indican los mensajes de registro.

En la primera línea resaltada, se indica que este router se registra en la consola y se incluyen mensajes de depuración. Esto en realidad significa que todos los mensajes del nivel de depuración, así como cualquier mensaje de nivel inferior (como los mensajes del nivel de notificación), se registran en la consola. El resultado también indica que se registraron 32 de estos mensajes.

En la segunda línea resaltada, se indica que este router se registra en un búfer interno. Dado que en este router se habilitó el registro en un búfer interno, el comando**show logging** también indica los mensajes en ese búfer. Puede ver algunos de los mensajes del sistema que se registraron al final del resultado.

Configuración predeterminada del servicio de registro

```
R1# show logging
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0
flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

    Console logging: level debugging, 32 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 32 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

    Trap logging: level informational, 34 message lines logged
        Logging Source-Interface:       VRF Name:

Log Buffer (8192 bytes):

*Jan  2 00:00:02.527: %LICENSE-6-EULA_ACCEPT_ALL: The Right to Use End User
```

Capítulo 8: Supervisión de la red 8.1.2.3 Comandos de router y switch para los clientes syslog

Existen tres pasos para configurar el router para que envíe los mensajes del sistema a un servidor de syslog donde se puedan almacenar, filtrar y analizar:

Paso 1. Configure el nombre del host de destino o la dirección IP del servidor de syslog en el modo de configuración global:

R1(config)# **logging 192.168.1.3**

Paso 2. Controle los mensajes que se envían al servidor de syslog con el comando del modo de configuración global**logging trap** *nivel*. Por ejemplo, para limitar los mensajes a los niveles 4 e inferiores (0 a 4), utilice uno de los dos comandos equivalentes:

R1(config)# **logging trap 4**

R1(config)# **logging trap warning**

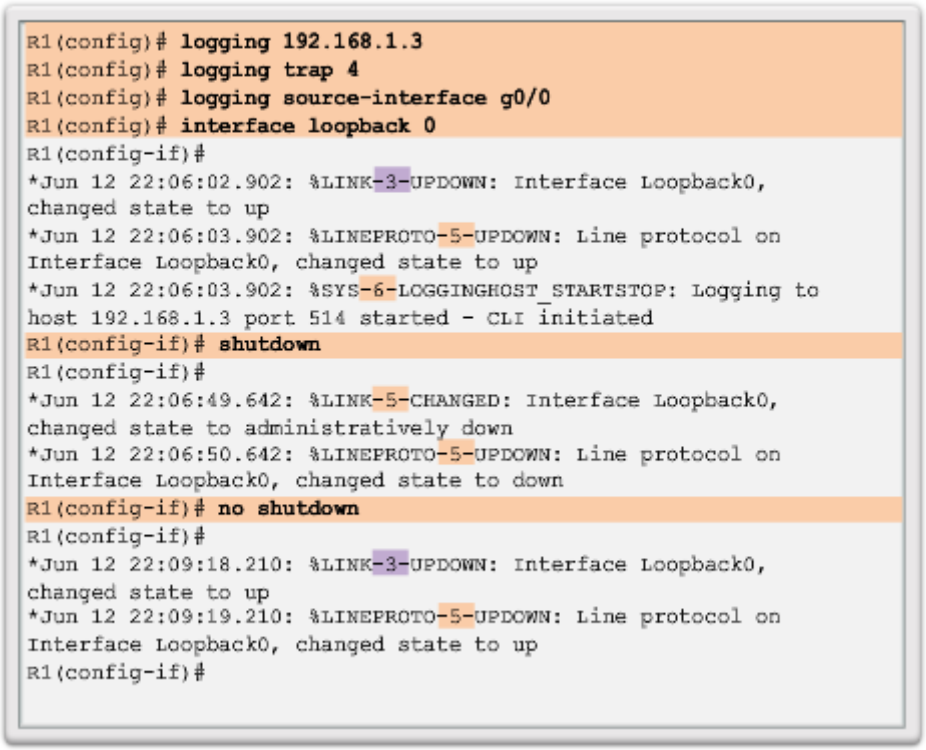
Paso 3. De manera optativa, configure la interfaz de origen con el comando del modo de configuración global **logging source-interface** *tipo-interfaz número interfaz*. Esto especifica que los paquetes de syslog incluyen la dirección IPv4 o IPv6 de una interfaz específica, independientemente de la interfaz que use el paquete para salir del router. Por ejemplo, para establecer la interfaz de origen en g0/0, utilice el siguiente comando:

R1(config)# **logging source-interface g0/0**

En la figura 1, el R1 se configuró para enviar mensajes de registro de los niveles 4 e inferiores al servidor de syslog en 192.168.1.3. La interfaz de origen se estableció en la interfaz G0/0. Se crea una interfaz loopback, se desactiva y se vuelve a activar. El resultado de la consola refleja estas acciones.

Como se muestra en la figura 2, se configuró el servidor de syslog Tftpd32 en una máquina con Windows 7 con la dirección IP 192.168.1.3. Como puede observar, los únicos mensajes que aparecen en el servidor de syslog son aquellos con un nivel de gravedad de 4 o menos (más graves). Los mensajes con un nivel de gravedad de 5 o más (menos graves) aparecen en el resultado de la consola del router, pero no aparecen en el resultado del servidor de syslog, porque el comando **logging trap** limita los mensajes de syslog que se envían al servidor de syslog según el nivel de gravedad.

Configuración de syslog



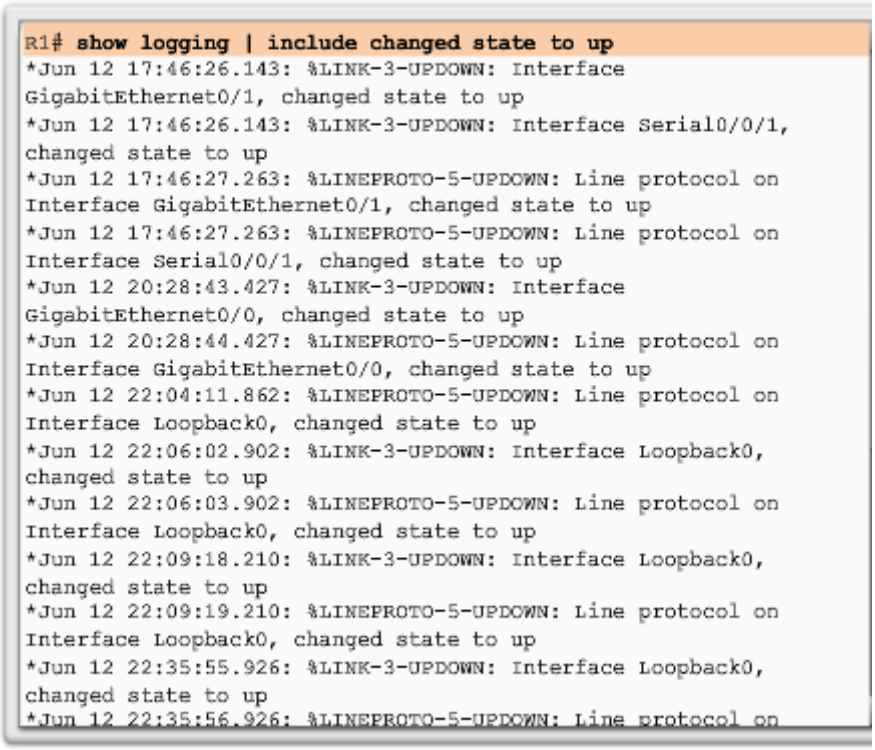
Capítulo 8: Supervisión de la red 8.1.2.4 Verificación de syslog

Puede utilizar el comando **show logging**para ver cualquier mensaje que se registre. Cuando el búfer de registro es grande, es conveniente utilizar la opción de la barra vertical (|) con el comando **show logging**. La opción de la barra vertical permite que el administrador indique específicamente qué mensajes se deben mostrar.

Por ejemplo, mediante la emisión del comando **show logging** | **include changed state to up**, la cual se muestra en la figura 1, se asegura que solo se muestren las notificaciones de interfaz en las que se indica “changed state to up”.

En la figura 1, también se muestra que mediante la emisión del comando **show logging** | **begin June 12 22:35** se muestra el contenido del búfer de registro que ocurrió el 12 de junio o después de esta fecha.

Verificación de syslog



Capítulo 8: Supervisión de la red 8.1.2.5 Packet Tracer: Configuración de syslog y NTP

Información básica/situación

En esta actividad, habilitará y usará los servicios de syslog y NTP para que el administrador de red pueda monitorear la red de forma más eficaz.

Packet Tracer: Configuración de syslog y NTP (instrucciones)

Packet Tracer: Configuración de syslog y NTP (PKA)

Capítulo 8: Supervisión de la red 8.1.2.6 Práctica de laboratorio: Configuración de syslog y NTP

En esta práctica de laboratorio, cumplirá los siguientes objetivos:

- Parte 1: configurar los parámetros básicos de los dispositivos
- Parte 2: configurar NTP
- Parte 3: Configurar syslog

Práctica de laboratorio: Configuración de syslog y NTP

Capítulo 8: Supervisión de la red 8.2.1.1 Introducción a SNMP

Protocolo simple de administración de red (SNMP)

SNMP se desarrolló para permitir que los administradores puedan administrar los nodos, como los servidores, las estaciones de trabajo, los routers, los switches y los dispositivos de seguridad, en una red IP. Permite que los administradores de red administren el rendimiento de la red, detecten y resuelvan problemas de red, y planifiquen el crecimiento de la red.

SNMP es un protocolo de capa de aplicación que proporciona un formato de mensaje para la comunicación entre administradores y agentes El sistema SNMP consta de tres elementos:

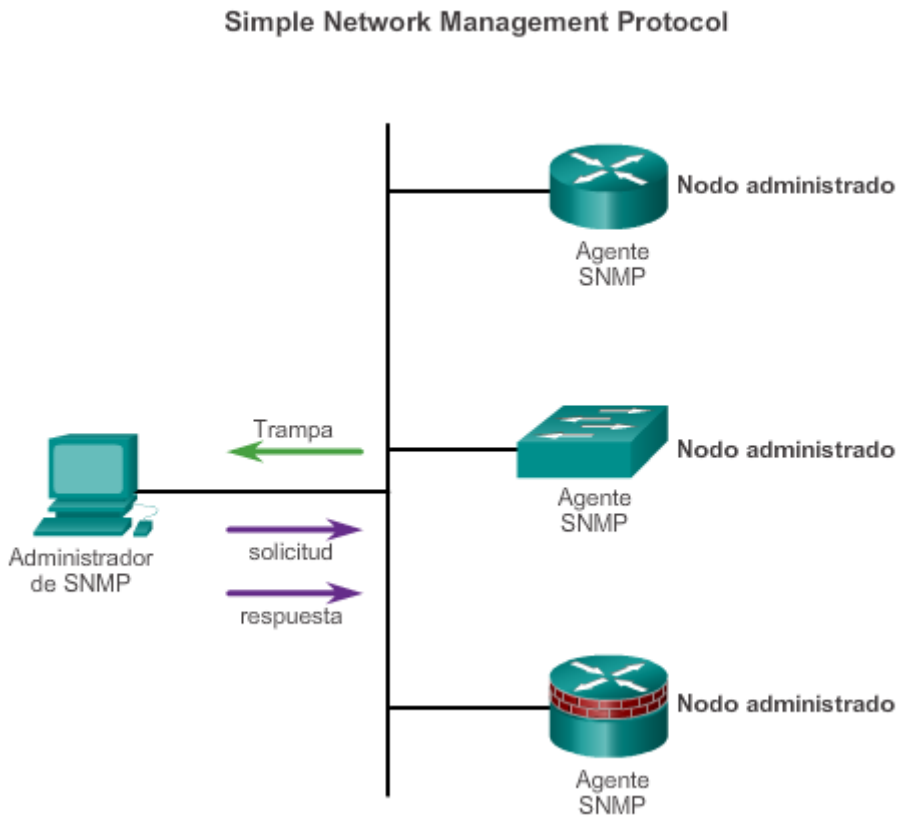
- Administrador de SNMP
- Agentes SNMP (nodo administrado)
- base de información de administración (MIB)

Para configurar SNMP en un dispositivo de red, primero es necesario definir la relación entre el administrador y el agente.

El administrador de SNMP forma parte de un sistema de administración de red (NMS). El administrador de SNMP ejecuta software de administración SNMP. Como se muestra en la ilustración, el administrador de SNMP puede recopilar información de un agente SNMP mediante una acción “get” y puede cambiar la configuración en un agente mediante la acción “set”. Además, los agentes SNMP pueden reenviar información directamente a un NMS mediante “traps”.

El agente SNMP y la MIB residen en los clientes de dispositivo de red. Los dispositivos de red que se deben administrar, como los switches, los routers, los servidores, los firewalls y las estaciones de trabajo, cuentan con un módulo de software de agente SMNP. Las MIB almacenan datos sobre el funcionamiento del dispositivo y están diseñadas para estar disponibles para los usuarios remotos autenticados. El agente SNMP es responsable de proporcionar acceso a la MIB local que refleja los recursos y la actividad de los objetos.

SNMP define cómo se intercambia la información de administración entre las aplicaciones de administración de red y los agentes de administración. SNMP utiliza el número de puerto UDP 162 para recuperar y enviar la información de administración.



Capítulo 8: Supervisión de la red 8.2.1.2 Funcionamiento de SNMP

Los agentes SNMP que residen en los dispositivos administrados recopilan y almacenan información sobre los dispositivos y su funcionamiento. El agente almacena esta información localmente en la MIB. El administrador SNMP luego usa el agente SNMP para tener acceso a la información dentro de la MIB.

Existen dos solicitudes principales de administrador de SNMP: get y set. NMS usa una solicitud get para solicitar datos al dispositivo. NMS usa una solicitud establecida para cambiar las variables de configuración en el dispositivo del agente. Una solicitud set también puede iniciar acciones dentro de un dispositivo. Por ejemplo, una solicitud set puede hacer que un router se reinicie, que envíe o que reciba un archivo de configuración. El administrador de SNMP utiliza las acciones de las solicitudes get y set para realizar las operaciones descritas en la tabla de la figura 1.

El agente SNMP responde a las solicitudes del administrador de SNMP de la siguiente manera:

- **Obtener una variable de MIB:** el agente SNMP realiza esta función en respuesta a una PDU de solicitud get de NMS. El agente recupera el valor de la variable de MIB solicitada y responde a NMS con ese valor.

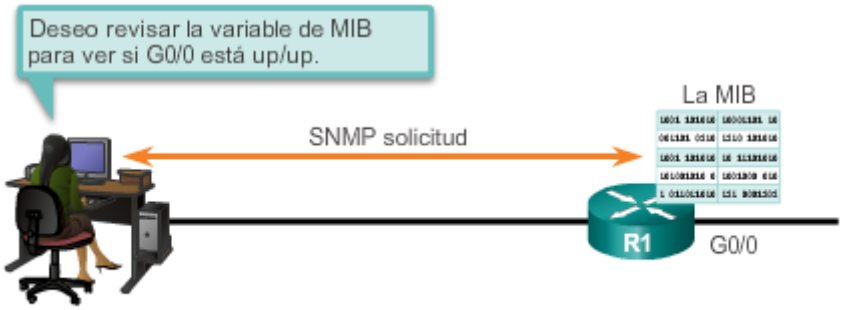
- **Establecer una variable de MIB:** el agente SNMP realiza esta función en respuesta a una PDU de solicitud set de NMS. El agente SNMP cambia el valor de la variable de MIB por el valor que especifica NMS. La respuesta del agente SNMP a una solicitud set incluye la nueva configuración en el dispositivo.

En la figura 2, se muestra el uso de una solicitud get de SNMP para determinar si la interfaz G0/0 está up/up (activa/activa).

Operaciones de SNMP

Operación	Descripción
`get-request`	Recupera un valor de una variable específica.
`get-next-request`	Recupera un valor de una variable dentro de una tabla; el administrador de SNMP no necesita saber el nombre exacto de la variable. Se realiza una búsqueda secuencial para encontrar la variable necesaria dentro de una tabla.
`get-bulk-request`	Recupera grandes bloques de datos, como varias filas en una tabla, que de otra manera requerirían la transmisión de muchos bloques pequeños de datos. (Solo funciona con SNMPv2 o más reciente).
`get-response`	Responde a una operación `get-request`, `get-next-request` y `set-request` que envió NMS.
`set-request`	Almacena un valor en una variable específica.

Solicitud get de SNMP



Capítulo 8: Supervisión de la red 8.2.1.3 Traps del agente SNMP

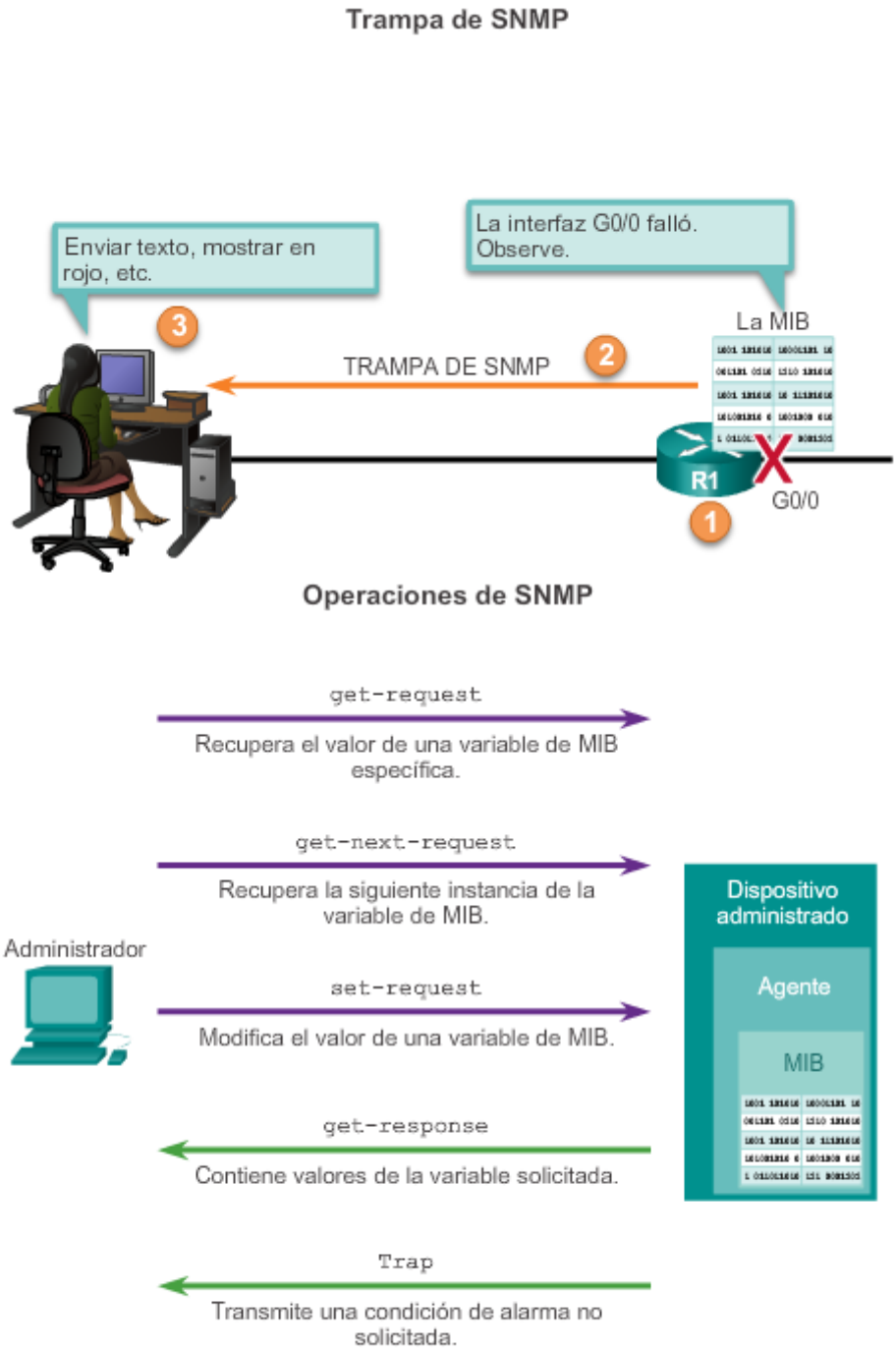
NMS sondea periódicamente a los agentes SNMP que residen en los dispositivos administrados para solicitar datos a los dispositivos mediante la solicitud get. Con este proceso, una aplicación de administración de red puede recopilar información para controlar cargas de tráfico y verificar las configuraciones de los dispositivos administrados. La información se puede mostrar a través de la GUI de NMS. Se pueden calcular los promedios, los mínimos o los máximos, representar los datos gráficamente o establecer umbrales para activar un proceso de notificación cuando se exceden los umbrales. Por ejemplo, NMS puede controlar el uso de CPU de un router Cisco. El administrador de SNMP prueba el valor periódicamente y presenta esta información en un gráfico a fin de que el administrador de red la utilice para crear una línea de base.

El sondeo periódico de SNMP tiene desventajas. En primer lugar, existe un retraso entre el momento en el que ocurre un evento y el momento en el que NMS lo advierte (mediante el sondeo). En segundo lugar, existe un nivel de equilibrio entre la frecuencia del sondeo y el uso del ancho de banda.

Para mitigar estas desventajas, es posible que los agentes SNMP generen y envíen traps para informarle a NMS sobre ciertos eventos de inmediato. Las traps son mensajes no solicitados que alertan al administrador de SNMP sobre una condición o un evento en la red. Algunos ejemplos de las condiciones de trap incluyen, entre otros, la autenticación incorrecta de usuarios, los reinicios, el estado del enlace (activo o inactivo), el seguimiento de direcciones MAC, el cierre de una conexión TCP, la pérdida de conexión a un vecino u otros eventos importantes. Las notificaciones de trap reducen los recursos de red y de agente al eliminar la necesidad de algunas de las solicitudes de sondeo de SNMP.

En la figura 1, se muestra el uso de una trap de SNMP para alertar al administrador de red que la interfaz G0/0 falló. El software de NMS puede enviar un mensaje de texto al administrador de red, mostrar una ventana emergente en el software de NMS o mostrar el ícono del router en color rojo en la GUI de NMS.

El intercambio de todos los mensajes de SNMP se muestra en la figura 2.



Capítulo 8: Supervisión de la red 8.2.1.4 Versiones de SNMP

Existen varias versiones de SNMP, incluidas las siguientes:

- **SNMPv1:** el protocolo simple de administración de red, un estándar de Internet completo, se define en RFC 1157.

- **SNMPv2c:** se define en las RFC 1901 a 1908; utiliza el marco administrativo basado en cadenas de comunidad.

- **SNMPv3:** protocolo interoperable basado en estándares definido originalmente en las RFC 2273 a 2275; proporciona acceso seguro mediante la autenticación y el cifrado de paquetes a través de la red. Incluye estas características de seguridad: integridad del mensaje para asegurar que no se alteró un paquete en tránsito, autenticación para determinar que el mensaje proviene de un origen válido, y cifrado para evitar que un origen no autorizado lea el contenido de un mensaje.

Todas las versiones usan administradores de SNMP, agentes SNMP y MIB. El software IOS de Cisco admite las tres versiones mencionadas anteriormente. La versión 1 es una solución antigua y no se suele encontrar en las redes actuales; por lo tanto, este curso se centra en las versiones 2c y 3.

SNMPv1 y SNMPv2c usan una forma de seguridad basada en comunidades. Una ACL y una contraseña definen la comunidad de administradores que pueden acceder a la MIB del agente.

A diferencia de SNMPv1, SNMPv2c incluye un mecanismo de recuperación masiva e informes de mensajes de error más detallados para las estaciones de administración. El mecanismo de recuperación masiva recupera tablas y grandes cantidades de información, lo que minimiza la cantidad de idas y vueltas requeridas. El manejo de errores mejorado de SNMPv2c incluye códigos de error ampliados que distinguen diferentes tipos de condiciones de error. Estas condiciones se informan mediante un único código de error en SNMPv1. Los códigos de devolución de error en SNMPv2c incluyen el tipo de error.

Nota: SNMPv1 y SNMPv2c ofrecen características de seguridad mínima. Específicamente, SNMPv1 y SNMPv2c no pueden autenticar el origen de un mensaje de administración ni proporcionar cifrado. La descripción más actualizada de SNMPv3 se encuentra en las RFC 3410 a 3415. Agrega métodos para garantizar la transmisión segura de datos importantes entre los dispositivos administrados.

SNMPv3 proporciona tanto modelos como niveles de seguridad. Un modelo de seguridad es una estrategia de autenticación configurada para un usuario y el grupo dentro del que reside el usuario. Un nivel de seguridad es el nivel de seguridad permitido dentro de un modelo de seguridad. La combinación del nivel de seguridad y el modelo de seguridad determina qué mecanismo de seguridad se utiliza al manejar un paquete SNMP. Los modelos de seguridad disponibles son SNMPv1, SNMPv2c y SNMPv3.

En la ilustración, se identifican las características de las distintas combinaciones de modelos y niveles de seguridad.

Un administrador de red debe configurar el agente SNMP para que use la versión de SNMP que admite la estación de administración. Debido a que un agente puede comunicarse con varios administradores de SNMP, es posible configurar el software para admitir comunicaciones mediante SNMPv1, SNMPv2c o SNMPv3.

Modelos y niveles de seguridad de SNMP

Modelo	Nivel	Autenticación	Cifrado	Resultado
SNMPv1	noAuthNoPriv	Cadena de comunidad	No	Usa una coincidencia de cadena de comunidad para la autenticación.
SNMPv2c	noAuthNoPriv	Cadena de comunidad	No	Usa una coincidencia de cadena de comunidad para la autenticación.
SNMPv3	noAuthNoPriv	Nombre de usuario	No	Usa una coincidencia de nombre de usuario para la autenticación (una mejora con respecto a SNMPv2c).
SNMPv3	authNoPriv	Algoritmo de síntesis del mensaje 5 (MD5) o algoritmo hash seguro (SHA)	No	Proporciona autenticación basada en los algoritmos HMAC-MD5 o HMAC-SHA.
SNMPv3	authPriv (requiere la imagen del software criptográfico)	MD5 o SHA	Estándar de cifrado de datos (DES) o estándar de cifrado avanzado (AES)	Proporciona autenticación basada en los algoritmos HMAC-MD5 o HMAC-SHA. Permite especificar el modelo de seguridad basado en usuarios (USM) con estos algoritmos de cifrado: • Cifrado DES de 56bits, además de autenticación basada en el estándar CBC-DES (DES-56). • Cifrado 3DES de 168bits • Cifrado AES de 128bits, 192bits o 256bits

Capítulo 8: Supervisión de la red 8.2.1.5 Cadenas de comunidad

Para que SNMP funcione, NMS debe tener acceso a la MIB. Para asegurar que las solicitudes de acceso sean válidas, debe haber cierta forma de autenticación.

SNMPv1 y SNMPv2c usan cadenas de comunidad que controlan el acceso a la MIB. Las cadenas de comunidad son contraseñas de texto no cifrado. Las cadenas de la comunidad de SNMP autentican el acceso a los objetos MIB.

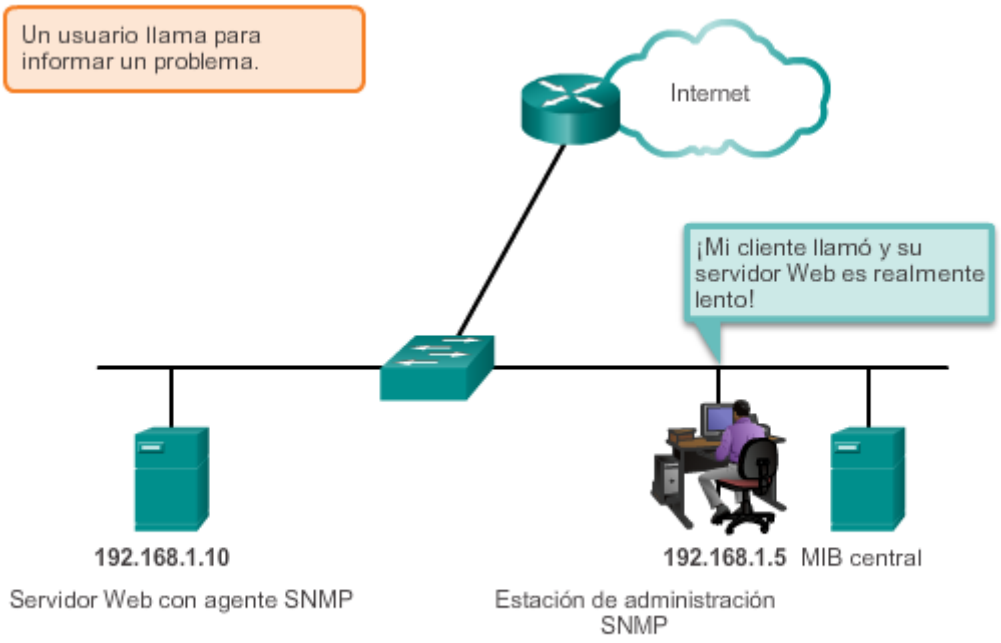
Existen dos tipos de cadenas de comunidad:

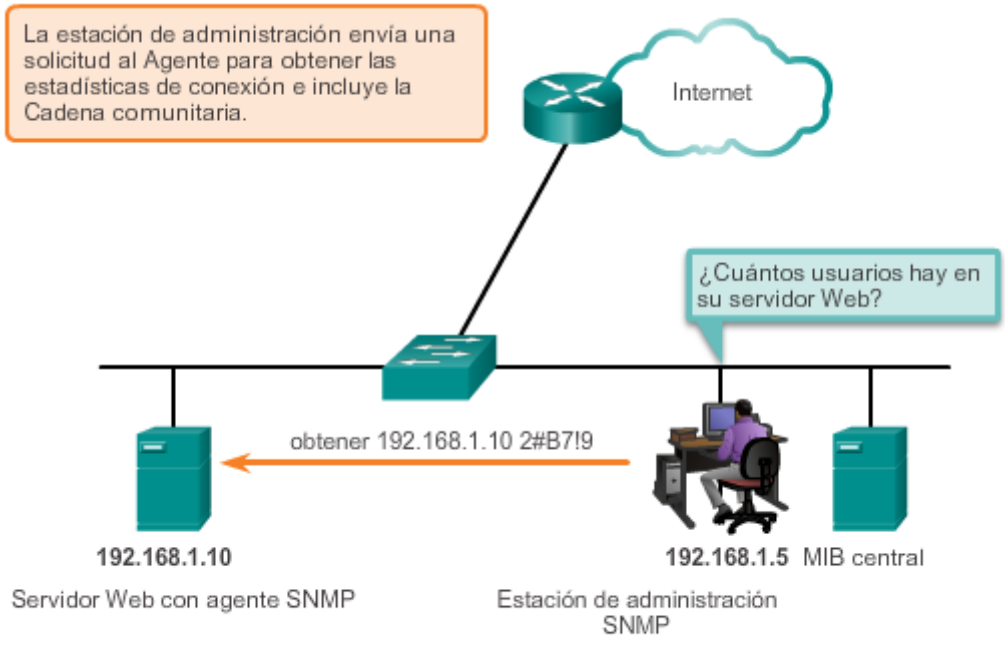
- **Solo lectura (ro):** proporciona acceso a las variables de MIB, pero no permite realizar cambios a estas variables, solo leerlas. Debido a que la seguridad es mínima en la versión 2c, muchas organizaciones usan SNMPv2c en modo de solo lectura.

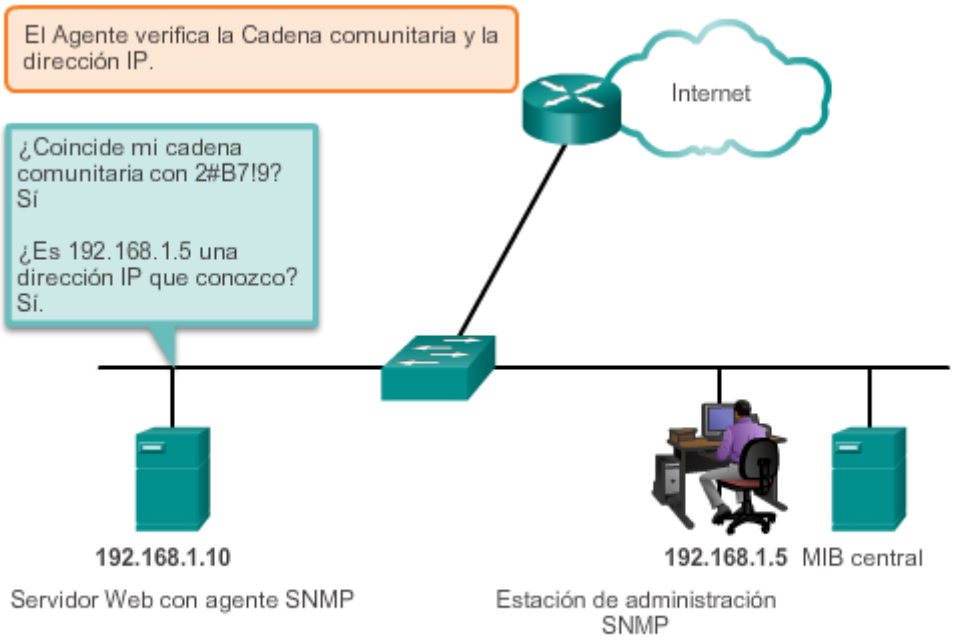
- **Lectura y escritura (rw):** proporciona acceso de lectura y escritura a todos los objetos de la MIB.

Para ver o establecer variables de MIB, el usuario debe especificar la cadena de comunidad correspondiente para el acceso de lectura o escritura. Reproduzca la animación de la ilustración para ver cómo funciona SNMP con la cadena de comunidad.

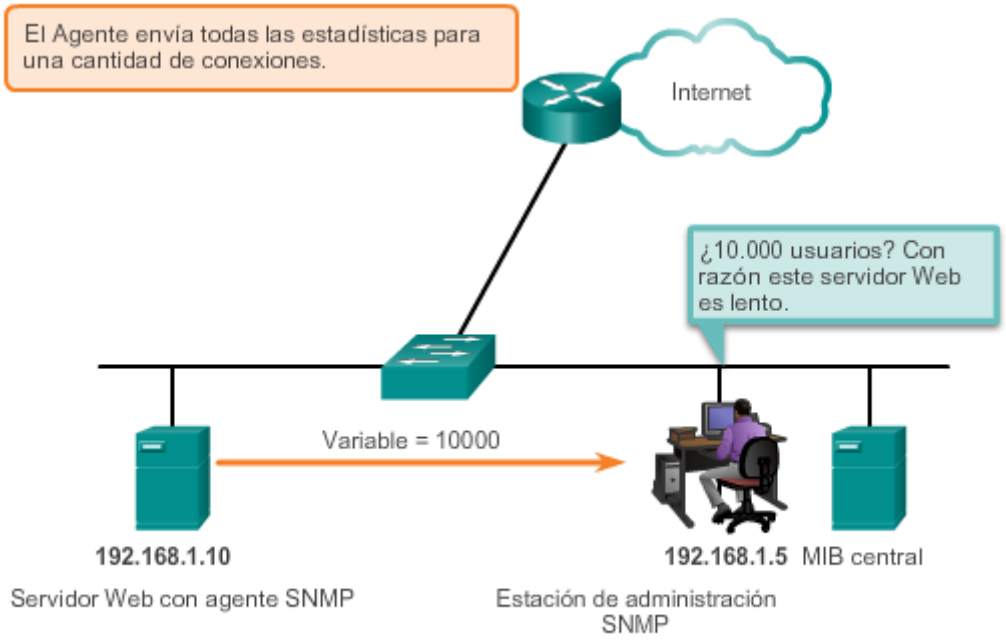
Nota: las contraseñas de texto no cifrado no se consideran un mecanismo de seguridad. Esto se debe a que las contraseñas de texto no cifrado son sumamente vulnerables a los ataques man-in-the-middle (intermediario), en los que se ven comprometidas a través de la captura de paquetes.



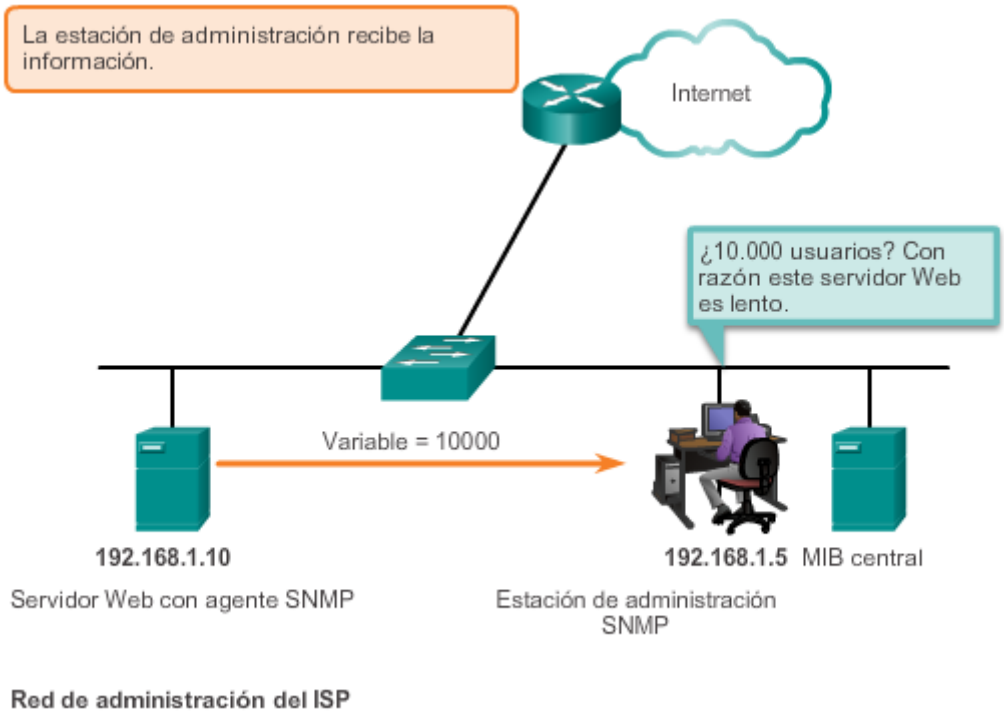




Red de administración del ISP



Red de administración del ISP



Capítulo 8: Supervisión de la red 8.2.1.6 ID de objetos de la base de información de administración

La MIB organiza variables de manera jerárquica. Las variables de MIB permiten que el software de administración controle el dispositivo de red. Formalmente, la MIB define cada variable como una ID de objeto (OID). Las OID identifican de forma exclusiva los objetos administrados en la jerarquía de la MIB. La MIB organiza las OID según estándares RFC en una jerarquía de OID, que se suele mostrar como un árbol.

El árbol de la MIB para un dispositivo determinado incluye algunas ramas con variables comunes a varios dispositivos de red y algunas ramas con variables específicas de ese dispositivo o proveedor.

Las RFC definen algunas variables públicas comunes. La mayoría de los dispositivos implementan estas variables de MIB. Además, los proveedores de equipos de redes, como Cisco, pueden definir sus propias ramas privadas del árbol para admitir las nuevas variables específicas de sus dispositivos. En la ilustración 1, se muestran partes de la estructura de MIB definida por Cisco Systems, Inc. Observe que la OID se puede describir en palabras o números para buscar una variable específica en el árbol. Las OID que pertenecen a Cisco, como se muestra en la figura 1, se numeran de la siguiente manera: .iso (1).org (3).dod (6).internet (1).private (4).enterprises (1).cisco (9). Esto se muestra como 1.3.6.1.4.1.9.

Dado que la CPU es uno de los recursos clave, se debe medir de manera continua. Las estadísticas de CPU deben recopilarse en NMS y se deben representar gráficamente. La observación del uso de la CPU durante un período extendido permite que el administrador establezca una línea de base aproximada para el uso de la CPU. Los valores de umbral se pueden establecer en relación con esta línea de base. Cuando el uso de la CPU supera este umbral, se envían notificaciones. Una herramienta de representación gráfica de SNMP puede

sondear de forma periódica a los agentes SNMP, como un router, y representar gráficamente los valores recopilados. En la figura 2, se muestran ejemplos de 5 minutos de uso de la CPU por parte de un router durante un período de unas semanas.

Los datos se recuperan mediante la utilidad snmpget, que se emite en NMS. Mediante la utilidad snmpget, se pueden obtener valores manualmente para calcular el promedio de porcentaje de ocupación de la CPU. La utilidad snmpget requiere que se establezca la versión de SNMP, la comunidad correcta, la dirección IP del dispositivo de red que se debe consultar y el número de OID. En la figura 3, se demuestra el uso de la utilidad de freeware snmpget, que permite la recuperación rápida de información de la MIB.

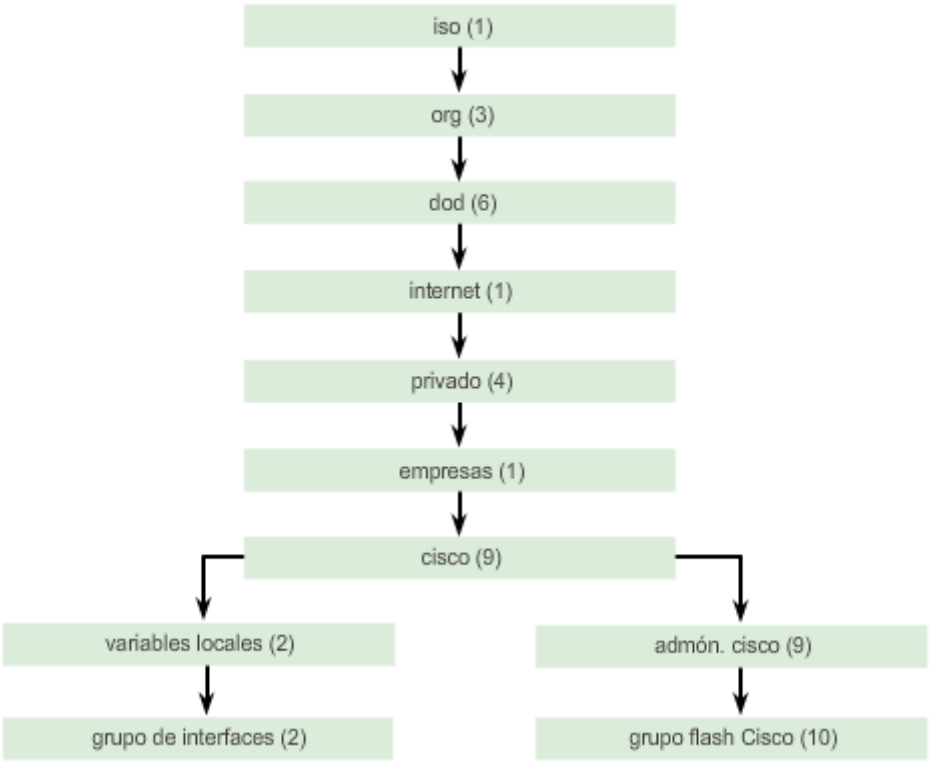
En la figura 3, se muestra un comando bastante largo con varios parámetros, incluido lo siguiente:

- -v2c: versión de SNMP
- -c community contraseña de SNMP, denominada “cadena de comunidad”
- 10.250.250.14: dirección IP del dispositivo monitoreado
- 1.3.6.1.4.1.9.2.1.58.0: OID de la variable de MIB

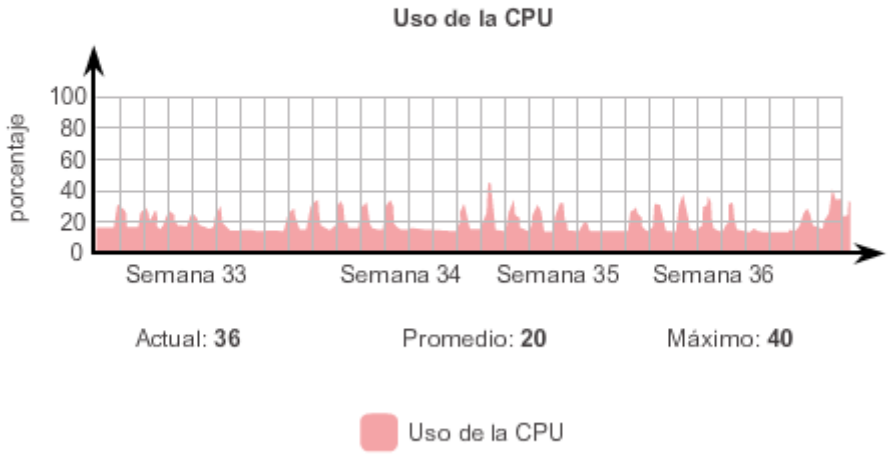
En la última línea, se muestra la respuesta. El resultado muestra una versión abreviada de la variable de MIB. A continuación, indica el valor real en la ubicación de la MIB. En este caso, el promedio cambiante exponencial de 5 minutos del porcentaje de ocupación de la CPU es del 11%. La utilidad proporciona cierta información sobre los mecanismos básicos de funcionamiento de SNMP. Sin embargo, trabajar con nombres de variables de MIB largos como 1.3.6.1.4.1.9.2.1.58.0 puede ser problemático para el usuario promedio. Generalmente, el personal de operaciones de red utiliza un producto de administración de red con una GUI fácil de usar, con el nombre completo de la variable de datos de MIB transparente para el usuario.

El sitio web de Cisco SNMP Navigator permite que un administrador de red investigue detalles de un OID en particular. En la figura 4, se muestra un ejemplo asociado a un cambio de configuración en un switch Cisco 2960.

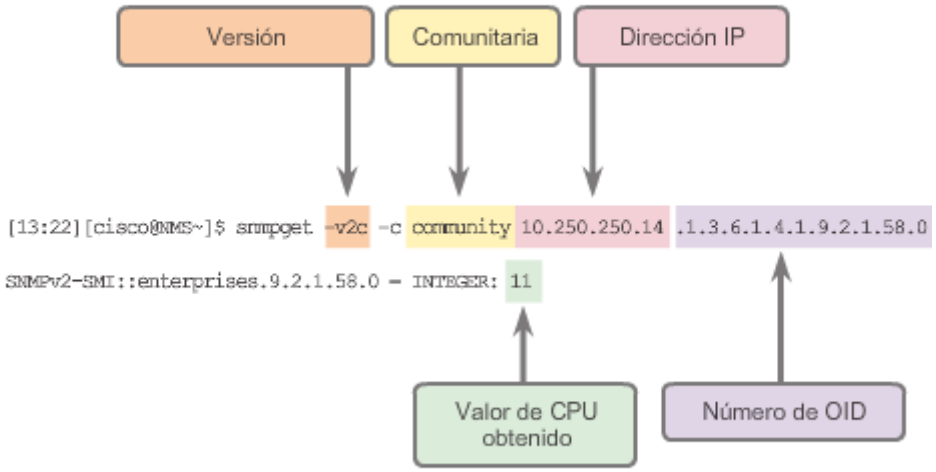
ID de objetos de la base de información de administración



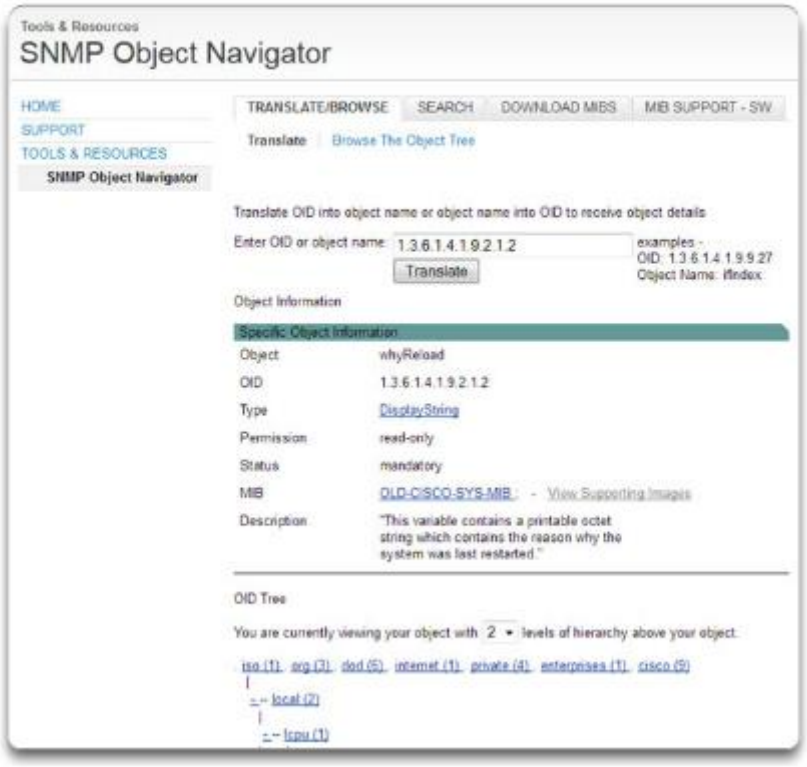
Herramienta de representación gráfica de SNMP



Utilidad snmpget



Cisco SNMP Navigator



Capítulo 8: Supervisión de la red 8.2.1.7 Actividad: Identificar las características de las versiones de SNMP

Actividad: Identificar las características de las versiones de SNMP

Haga clic en el campo correspondiente para clasificar cada característica de SNMP como versión 2c, versión 3 o ambas.

	Versión 2c	Versión 3	Ambos
Autentica el origen de los mensajes de administración.		✓	
Proporciona servicios para los modelos de seguridad.			✓
No puede proporcionar mensajes cifrados de administración.	✓		
Lo admite el software IOS de Cisco.			✓
Proporciona servicios para modelos y niveles de seguridad.		✓	
Incluye códigos de error expandidos con los tipos.	✓		
Utiliza formas de seguridad basadas en comunidad.	✓		
Se utiliza para la interoperabilidad e incluye informes de integridad del mensaje.		✓	

Capítulo 8: Supervisión de la red 8.2.1.8 Práctica de laboratorio: Investigación del software de supervisión de red

En esta práctica de laboratorio, cumplirá los siguientes objetivos:

- Parte 1: Evaluar su comprensión del monitoreo de red
- Parte 2: Investigar las herramientas de monitoreo de red
- Parte 3: Seleccionar una herramienta de monitoreo de red

Práctica de laboratorio: Investigación del software de supervisión de red

Capítulo 8: Supervisión de la red 8.2.2.1 Pasos para configurar SNMP

Un administrador de red puede configurar SNMPv2 para obtener información de red de los dispositivos de red. Como se muestra en la ilustración, todos los pasos básicos para configurar SNMP se realizan en el modo de configuración global.

Paso 1. (Obligatorio) Configure la cadena de comunidad y el nivel de acceso (solo lectura o lectura y escritura) mediante el comando **snmp-server community***cadena* **ro** | **rw**.

Paso 2. (Optativo) Registre la ubicación del dispositivo mediante el comando **snmp-server location** *texto*.

Paso 3. (Optativo) Registre el contacto del sistema mediante el comando **snmp-server contact** *texto*.

Paso 4. (Optativo) Restrinja el acceso de SNMP a los hosts NMS (administradores de SNMP) que autoriza una ACL: defina la ACL y, a continuación, nombre la ACL con el comando **snmp-server community***cadena número-o-nombre-lista-acceso*. Este comando se puede utilizar para especificar la cadena de comunidad y para restringir el acceso de SNMP a través de las

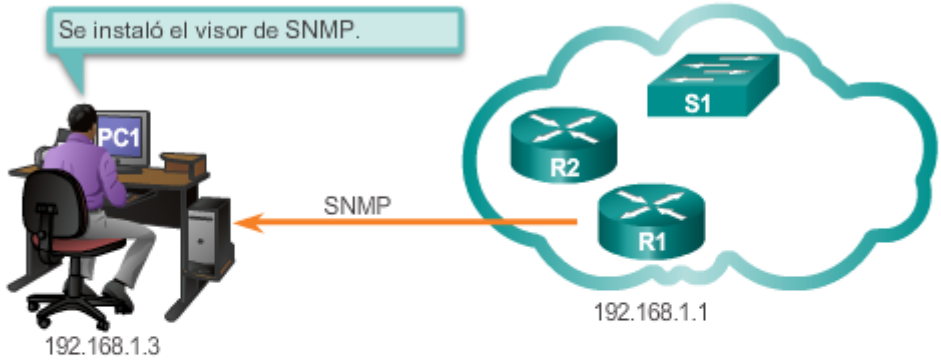
ACL. Los pasos 1 y 4 pueden combinarse en un paso, si lo desea; el dispositivo de red de Cisco combina los dos comandos en uno si se introducen por separado.

Paso 5. (Optativo) Especifique el destinatario de las operaciones de trap de SNMP con el comando **snmp-server host** *id-host* [**version** {**1** | **2c** |**3** [**auth** | **noauth** | **priv**]}]*cadena-comunidad*. De manera predeterminada, no se define ningún administrador de traps.

Paso 6. (Optativo) Habilite las traps en un agente SNMP con el comando **snmp-server enable traps** *tipos-notificación*. Si no se especifica ningún tipo de notificación de traps en este comando, entonces se envían todos los tipos de trap. Es necesario el uso reiterado de este comando si se desea un subconjunto determinado de tipos de trap.

Nota: de manera predeterminada, SNMP no tiene ninguna trap configurada. Sin este comando, los administradores de SNMP deben realizar sondeos para obtener toda la información importante.

La configuración admite el administrador de SNMP




```
R1(config)# snmp-server community batonaug ro SNMP_ACL
R1(config)# snmp-server location NOC_SNMP_MANAGER
R1(config)# snmp-server contact Wayne World
R1(config)# snmp-server host 192.168.1.3 version 2c batonaug
R1(config)# snmp-server enable traps
R1(config)# ip access-list standard SNMP_ACL
R1(config-std-nacl)# permit 192.168.1.3
```

Capítulo 8: Supervisión de la red 8.2.2.2 Verificación de la configuración de SNMP

Existen varias soluciones de software para ver el resultado de SNMP. Para nuestros fines, el servidor de syslog Kiwi muestra los mensajes de SNMP asociados a las traps de SNMP.

La PC1 y el R1 están configurados para demostrar el resultado en un administrador de SNMP en relación con las traps de SNMP.

Como se muestra en la figura 1, se asignó la dirección IP 192.168.1.3/24 a la PC1. El servidor de syslog Kiwi está instalado en la PC1.

Después de que se configura el R1, cada vez que ocurre un evento que califique como trap, se envían traps de SNMP al administrador de SNMP. Por ejemplo, si se activa una interfaz, se envía una trap al servidor. Los cambios de configuración en el router también activan el envío de traps de SNMP al administrador de SNMP. Se puede ver una lista de más de 60 tipos de notificación de traps con el comando**snmp-server enable traps ?** . En la configuración del R1, no se especifica ningún tipo de notificación de trap en el comando **snmp-server enable traps***tipos-notificación*, de modo que se envían todas las traps.

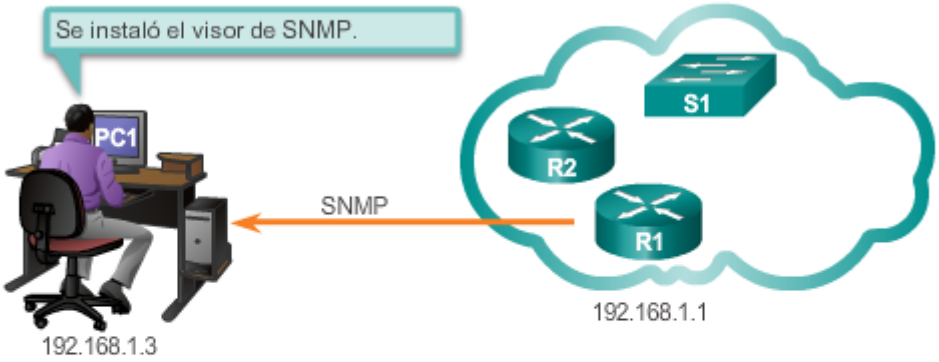
En la figura 2, se activó una casilla de verificación en el menú **Setup**(Configuración) para indicar que el administrador de red desea que el software del administrador de SNMP escuche para detectar las traps de SNMP en el puerto UDP 162.

En la figura 3, la fila superior del resultado de trap de SNMP que se muestra indica que el estado de la interfaz GigabitEthernet0/0 cambió a up (activo). Además, cada vez que se pasa del modo EXEC privilegiado al modo de configuración global, el administrador de SNMP recibe una trap, como se muestra en la fila resaltada.

Para verificar la configuración SNMP, utilice cualquier variante del comando **show snmp** del modo EXEC privilegiado. El comando más útil es simplemente el comando **show snmp**, ya que muestra la información que suele ser de interés al examinar la configuración SNMP. A menos que haya una configuración SNMPv3 involucrada, la mayoría de las otras opciones de comandos solo muestran partes seleccionadas del resultado del comando **show snmp**. En la figura 4, se proporciona un ejemplo del resultado de**show snmp**.

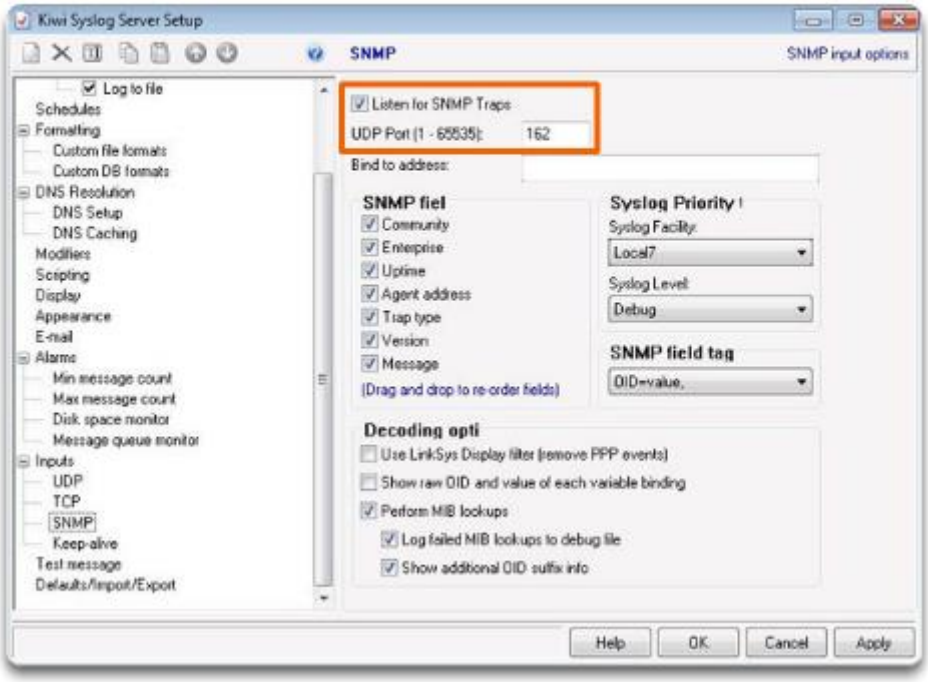
El resultado del comando **show snmp** no muestra información relacionada con la cadena de comunidad SNMP o, si corresponde, con la ACL asociada. En la figura 5, se muestra la información de la cadena de comunidad SNMP y de la ACL mediante el comando **show snmp community**.

La configuración admite el administrador de SNMP




```
R1(config)# snmp-server community batonaug ro SNMP_ACL
R1(config)# snmp-server location NOC_SNMP_MANAGER
R1(config)# snmp-server contact Wayne World
R1(config)# snmp-server host 192.168.1.3 version 2c batonaug
R1(config)# snmp-server enable traps
R1(config)# ip access-list standard SNMP_ACL
R1(config-std-nacl)# permit 192.168.1.3
```

Configuración del administrador de SNMP

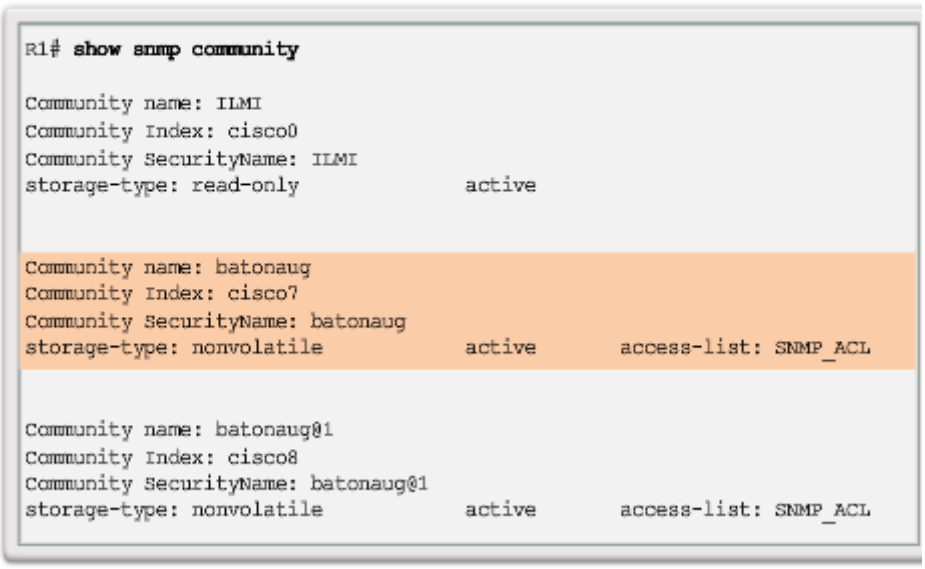


Visualización de mensajes del administrador de SNMP

Verificación de la configuración de SNMP

```
R1# show snmp
Chassis: FTX1636848Z
Contact: Wayne World
Location: NOC_SNMP_MANAGER
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
    0 Input queue packet drops (Maximum queue size 1000)
19 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    19 Trap PDUs
SNMP Dispatcher:
   queue 0/75 (current/max), 0 dropped
SNMP Engine:
   queue 0/1000 (current/max), 0 dropped
```

Servicio de comunidad SNMP



Capítulo 8: Supervisión de la red 8.2.2.3 Prácticas recomendadas de seguridad

Si bien SNMP es muy útil para el monitoreo y la resolución de problemas, como se muestra en la ilustración, también puede crear vulnerabilidades de seguridad. Por este motivo, antes de implementar SNMP, tenga en cuenta las prácticas recomendadas de seguridad.

SNMPv1 y SNMPv2c dependen de las cadenas de comunidad SNMP en texto no cifrado para autenticar el acceso a los objetos de la MIB. Estas cadenas de comunidad, al igual que todas las contraseñas, se deben elegir cuidadosamente para asegurar que no sean demasiado fáciles de descifrar. Además, las cadenas de comunidad se deben cambiar a intervalos regulares y de acuerdo con las políticas de seguridad de la red. Por ejemplo, se deben cambiar las cadenas cuando un administrador de red cambia de función o deja la empresa. Si SNMP se utiliza solo para monitorear los dispositivos, use comunidades de solo lectura.

Asegúrese de que los mensajes de SNMP no se propaguen más allá de las consolas de administración. Se deben usar ACL para evitar que los mensajes de SNMP se envíen más allá de los dispositivos requeridos. También se deben usar ACL en los dispositivos monitoreados para limitar el acceso solamente a los sistemas de administración.

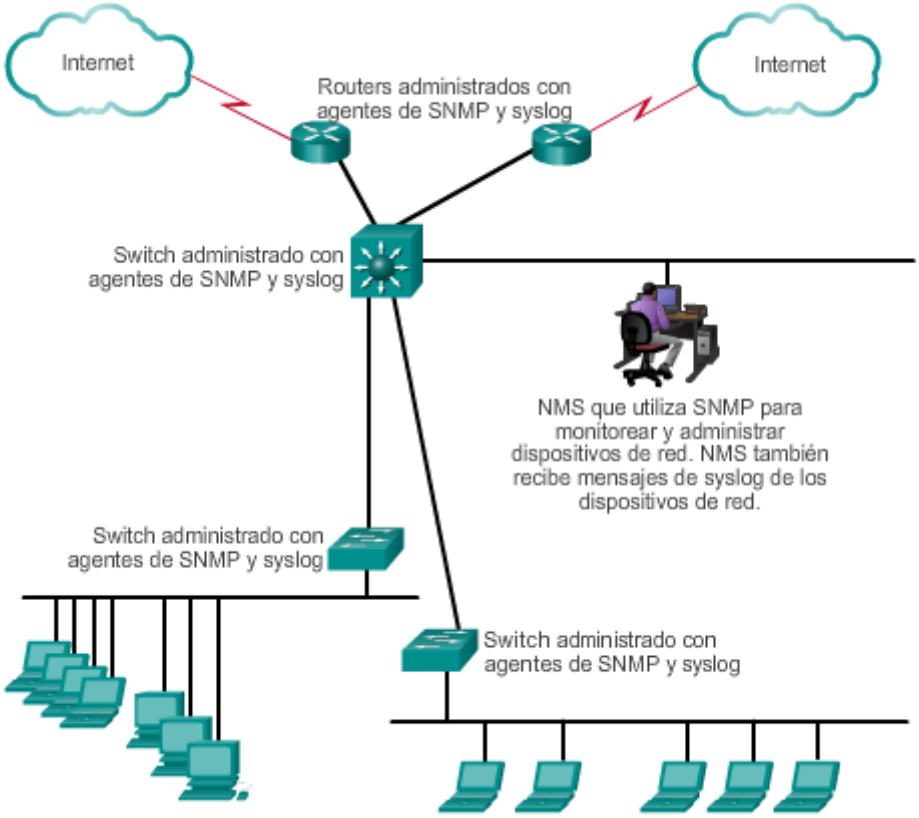
Se recomienda SNMPv3 porque proporciona autenticación y cifrado de seguridad. Existen otros comandos del modo de configuración global que puede implementar un administrador de red para aprovechar la autenticación y el cifrado en SNMPv3:

- El comando **snmp-server group***nombre-grupo* {**v1** | **v2c** | **v3**{**auth** | **noauth** | **priv**}} crea un nuevo grupo SNMP en el dispositivo.

- El comando **snmp-server user***nombre-usuario nombre-grupo***v3** [**encrypted**] [**auth** {**md5** |**sha**} contraseña-aut]

[***priv***{**des** | **3des** | **aes** {**128** | **192**| **256**}} contraseña-priv] se usa para agregar un nuevo usuario al grupo SNMP especificado en el comando **snmp-server group***nombre-grupo*.

Nota: la configuración de SNMPv3 excede el ámbito de los currículos de CCNA.



Capítulo 8: Supervisión de la red 8.2.2.4 Práctica de laboratorio: configuración de SNMP

En esta práctica de laboratorio, cumplirá los siguientes objetivos:

- Parte 1: armar la red y configurar los parámetros básicos de los dispositivos
- Parte 2: Configurar un administrador de SNMP y agentes SNMP
- Parte 3: Convertir los códigos OID con Cisco SNMP Object Navigator

Práctica de laboratorio: configuración de SNMP

Capítulo 8: Supervisión de la red 8.3.1.1 Introducción a NetFlow

NetFlow es una tecnología del IOS de Cisco que proporciona estadísticas sobre los paquetes que fluyen a través de un switch multicapa o un router Cisco. NetFlow es el estándar para recopilar datos operativos IP de las redes IP.

Históricamente, la tecnología NetFlow se desarrolló porque los profesionales de redes necesitaban un método simple y eficaz para realizar un seguimiento de los flujos TCP/IP en la red, y SNMP no era suficiente para estos fines. Mientras que SNMP intenta proporcionar una amplia variedad de características y opciones de administración de red, NetFlow se centra en proporcionar estadísticas sobre los paquetes IP que fluyen a través de los dispositivos de red.

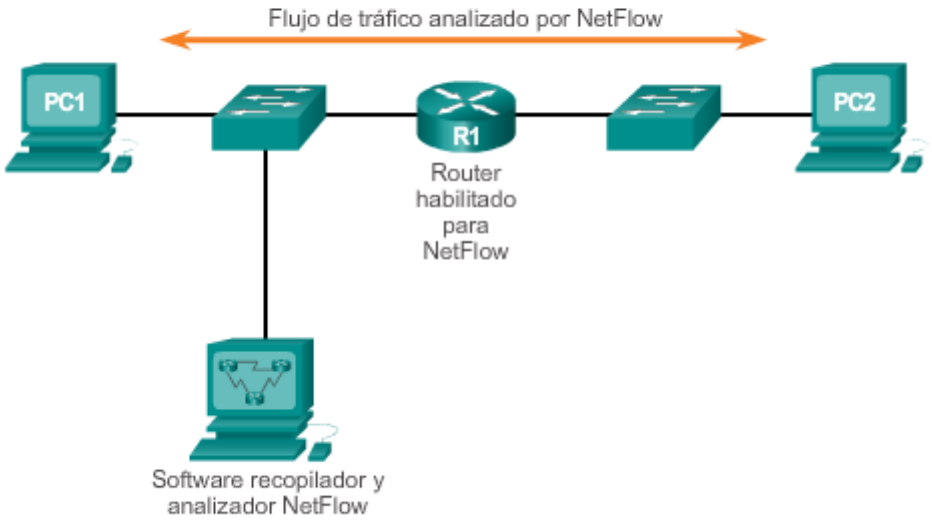
NetFlow proporciona datos para habilitar el monitoreo de red y de seguridad, la planificación de red, el análisis de tráfico para incluir la identificación de los cuellos de botella de la red y la contabilidad de IP para fines de facturación. Por ejemplo, en la ilustración, la PC1 se conecta a la PC2 mediante una aplicación como HTTPS. NetFlow puede monitorear la conexión de esa aplicación mediante el seguimiento de los conteos de bytes y de paquetes para el flujo de esa aplicación individual. A continuación, inserta las estadísticas en un servidor externo denominado “recopilador NetFlow”.

NetFlow se convirtió en un estándar de monitoreo y ahora se admite ampliamente en el sector de la tecnología de redes.

Flexible NetFlow es la tecnología NetFlow más reciente. Flexible NetFlow mejora el “NetFlow original” al agregar la capacidad de personalizar los parámetros de análisis de tráfico según los requisitos específicos de un administrador de red. Flexible NetFlow facilita la creación de configuraciones más complejas para el análisis de tráfico y la exportación de datos mediante componentes de configuración reutilizables.

Flexible Netflow usa el formato de exportación de la versión 9. La característica distintiva del formato de exportación de la versión 9 de NetFlow es que se basa en plantillas. Las plantillas proporcionan un diseño extensible al formato de registro, una característica que permite mejoras futuras a los servicios de NetFlow sin necesidad de realizar cambios simultáneos al formato básico del registro de flujo. Es importante tener en cuenta que muchos comandos útiles de Flexible NetFlow se presentaron con la versión 15.1 del IOS de Cisco.

NetFlow en la red



Capítulo 8: Supervisión de la red 8.3.1.2 Comprensión de NetFlow

Existen muchos usos posibles de las estadísticas que proporciona NetFlow; sin embargo, la mayoría de las organizaciones utilizan NetFlow para algunos o la totalidad de los importantes propósitos de la recolección de datos, entre ellos:

- Medir quién utiliza qué recursos de red y con qué propósito.
- Contabilizar y cobrar según el nivel de uso de los recursos.
- Usar la información medida para planificar la red con más eficacia, de modo que la implementación y la asignación de recursos estén bien alineadas con los requisitos del cliente.
- Usar la información para estructurar y personalizar mejor el conjunto de aplicaciones y servicios disponibles, a fin de satisfacer las necesidades de los usuarios y los requisitos de atención al cliente.

Al comparar la funcionalidad de SNMP con NetFlow, una analogía para SNMP podría ser el software de control remoto para un vehículo automático, mientras que una analogía para NetFlow sería una factura telefónica simple pero detallada. Los registros telefónicos proporcionan estadísticas agregadas llamada por llamada que permiten que quienes pagan la factura rastreen llamadas largas, frecuentes o que no se deberían haber realizado.

A diferencia de SNMP, NetFlow utiliza un modelo “basado en inserción”. El recopilador simplemente escucha el tráfico de NetFlow, y los dispositivos de red se encargan de enviar los datos de NetFlow al recopilador, sobre la base de los cambios en su memoria caché de flujo. Otra diferencia entre NetFlow y SNMP es que NetFlow recopila solamente las estadísticas de tráfico, como se muestra en la ilustración, mientras que SNMP también puede recopilar muchos otros indicadores de rendimiento, como errores de interfaz, uso de CPU y de la memoria. Por otra parte, las estadísticas de tráfico recopiladas con NetFlow tienen una granularidad mucho mayor que las estadísticas de tráfico que se pueden recopilar con SNMP.

Nota: no confunda el propósito y los resultados de NetFlow con los del hardware y el software de captura de paquetes. Mientras que las capturas de paquetes registran toda la información posible que sale de un dispositivo de red o que ingresa a este para un análisis posterior, NetFlow identifica información estadística específica.

Cuando Cisco creó NetFlow, dos criterios clave orientaron su creación:

- NetFlow debe ser totalmente transparente para las aplicaciones y los dispositivos en la red.
- No debe ser necesario que se admita y se ejecute NetFlow en todos los dispositivos en la red para que funcione.

Lograr estos criterios de diseño aseguró que NetFlow fuera muy fácil de implementar en las redes modernas más complejas.

Nota: si bien NetFlow es fácil de implementar y transparente para la red, consume memoria adicional en el dispositivo de Cisco, porque almacena información de registro en la caché del

dispositivo. El tamaño predeterminado de esta caché varía según la plataforma, y el administrador puede ajustar este valor.

Capítulo 8: Supervisión de la red 8.3.1.3 Flujos de red

NetFlow analiza las comunicaciones TCP/IP para mantener un registro estadístico mediante el concepto de flujo. Un flujo es una secuencia unidireccional de paquetes entre un sistema específico de origen y un destino específico. En la ilustración, se demuestra el concepto de flujo.

Para NetFlow, que se basa en TCP/IP, las direcciones IP de capa de red y los números de puerto de origen y destino de capa de transporte definen el origen y el destino.

Existen varias generaciones de la tecnología NetFlow que proporcionan mayor sofisticación para definir los flujos de tráfico, pero “NetFlow original” distinguía los flujos mediante una combinación de siete campos. Si el valor de uno de estos campos difería del de otro paquete, se podía determinar con seguridad que los paquetes provenían de flujos diferentes:

- Dirección IP de origen
- Dirección IP de destino
- Número de puerto de origen
- Número de puerto de destino
- Tipo de protocolo de capa 3
- Marca de tipo de servicio (ToS)
- Interfaz lógica de entrada

Los primeros cuatro campos que usa NetFlow para identificar un flujo se deberían conocer. Las direcciones IP de origen y destino, más los puertos de origen y destino, identifican la conexión entre la aplicación de origen y destino. El tipo de protocolo de capa 3 identifica el tipo de encabezado que sigue al encabezado IP (generalmente TCP o UDP, pero otras opciones incluyen ICMP). El byte ToS en el encabezado de IPv4 contiene información sobre cómo los dispositivos deben aplicar las reglas de calidad de servicio (QoS) a los paquetes en ese flujo.

Flexible NetFlow admite más opciones con registros de datos de flujo. Flexible NetFlow permite que un administrador defina los registros para una caché de control de flujo mediante la especificación de los campos optativos y obligatorios definidos por el usuario para personalizar la recolección de datos, a fin de que se adapte a requisitos específicos. Cuando se definen registros para una caché de control de flujo de Flexible NetFlow, se los denomina “registros definidos por el usuario”. Los valores en los campos optativos se agregan a los flujos para proporcionar información adicional sobre el tráfico en los flujos. Un cambio en el valor de un campo optativo no crea un nuevo flujo.

Capítulo 8: Supervisión de la red 8.3.1.4 Actividad: Comparar SNMP y NetFlow

Actividad:Comparar SNMP y NetFlow
Haga clic en el campo correspondiente para clasificar cada característica de las herramientas de monitoreo de red como SNMP o NetFlow.

	SNMP	NetFlow
1. Los errores de interfaz, el uso de la CPU y el uso de la memoria no se registran.		✓
2. Se utiliza una base de información de administración (MIB) para registrar los eventos monitoreados en la red.	✓	
3. Recopila datos IP para registrar quién usó recursos de red, y con qué propósito se utilizaron esos recursos.		✓
4. Los agentes pueden enviar traps a un sistema de administración de red cuando se producen los eventos definidos.	✓	
5. El acceso a la MIB se controla por medio de la configuración de cadenas de comunidad.	✓	
6. Se utiliza un servidor externo (recopilador) para registrar los cambios en la caché monitoreados en la red IP.		✓

Capítulo 8: Supervisión de la red 8.3.2.1 Configuración de NetFlow

Para implementar NetFlow en un router, siga estos pasos:

Paso 1. Configure la captura de datos de NetFlow: NetFlow captura datos de los paquetes entrantes y salientes.

Paso 2. Configure la exportación de datos de NetFlow: se debe especificar la dirección IP y el nombre de host del recopilador NetFlow, así como el puerto UDP al que escucha el recopilador NetFlow.

Paso 3. Verifique NetFlow, su funcionamiento y sus estadísticas:después de configurar NetFlow, se pueden analizar los datos exportados en una estación de trabajo que ejecute una aplicación como NetFlow Traffic Analyzer de SolarWinds, Scrutinizer de Plixer o NetFlow Collector de Cisco (NFC). Como mínimo, se puede depender del resultado de varios comandos **show** en el router mismo.

Algunas consideraciones de configuración de NetFlow incluyen lo siguiente:

- Los routers Cisco más modernos, como la serie ISR G2, admiten NetFlow y Flexible NetFlow.
- Los switches Cisco más modernos, como los de la serie 3560-X, admiten Flexible NetFlow; sin embargo, algunos switches Cisco, como los de la serie Cisco 2960, no admiten NetFlow o Flexible NetFlow.
- NetFlow consume memoria adicional. Si un dispositivo de red de Cisco tiene restricciones de memoria, se puede establecer previamente el tamaño de la caché de NetFlow, de modo que contenga una menor cantidad de entradas. El tamaño predeterminado de la caché depende de la plataforma.
- Los requisitos de software de NetFlow para el recopilador NetFlow varían. Por ejemplo, el software de NetFlow Scrutinizer en un host de Windows requiere 4 GB de RAM y 50 GB de espacio de unidad.

Nota: el enfoque se centra en la configuración de un router Cisco con NetFlow original (denominado simplemente “NetFlow” en los documentos de Cisco). La configuración de Flexible NetFlow excede el ámbito de este curso.

Un flujo de NetFlow es unidireccional. Esto significa que una conexión de usuario a una aplicación existe como dos flujos de NetFlow, uno para cada sentido. Para definir los datos que se deben capturar para NetFlow en el modo de configuración de interfaz:

- Capture los datos de NetFlow para controlar los paquetes entrantes en la interfaz mediante el comando **ip flow ingress**.

- Capture los datos de NetFlow para controlar los paquetes salientes en la interfaz mediante el comando **ip flow egress**.

Para habilitar el envío de los datos de NetFlow al recopilador NetFlow, se deben configurar varios elementos en el modo de configuración global del router:

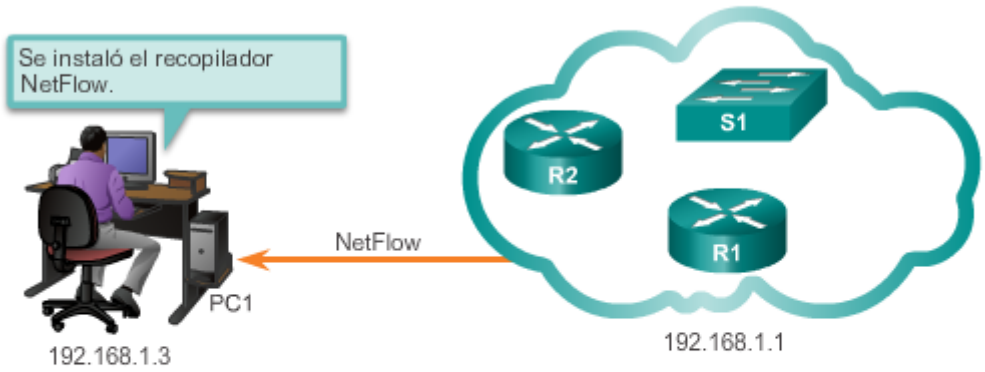
- **Dirección IP y número de puerto UDP del recopilador NetFlow:** utilice el comando **ip flow-export destination** *dirección-ip puerto-udp*. De manera predeterminada, el recopilador tiene uno o más puertos para la captura de datos de NetFlow. El software permite que el administrador especifique qué puertos se deben aceptar para la captura de datos de NetFlow. Algunos puertos UDP comunes que se asignan son los puertos 99, 2055 y 9996.

- **(Optativo) La versión de NetFlow que se debe seguir para dar formato a los registros de NetFlow que se envían al recopilador:** utilice el comando **ip flow-export version** *versión*. NetFlow exporta los datos en UDP en uno de cinco formatos (1, 5, 7, 8 y 9). La versión 9 es el formato de exportación de datos más versátil, pero no es compatible con las versiones anteriores. La versión 1 es la predeterminada si no se especifica la versión 5. La versión 1 solo debe usarse cuando es la única versión del formato de exportación de datos de NetFlow que admite el software del recopilador NetFlow.

- **(Optativo) Interfaz de origen que se debe usar como origen de los paquetes enviados al recopilador:**utilice el comando **ip flow-export source** *tiponúmero*.

En la ilustración, se muestra una configuración básica de NetFlow. El router R1 tiene la dirección IP 192.168.1.1 en la interfaz G0/1. El recopilador NetFlow tiene la dirección IP 192.168.1.3 y se configuró para capturar los datos en el puerto UDP 2055. Se controla el tráfico que entra y sale por G0/1. Los datos de NetFlow se envían en el formato de la versión 5.

Configuración de un router con NetFlow




```
R1(config)# interface GigabitEthernet 0/1
R1(config-if)# ip flow ingress
R1(config-if)# ip flow egress
R1(config-if)# exit
R1(config)# ip flow-export destination 192.168.1.3 2055
R1(config)# ip flow-export version 5
```

Capítulo 8: Supervisión de la red 8.3.2.2 Verificación de NetFlow

Una vez que se verificó que NetFlow funciona correctamente, puede comenzar la recolección de datos en el recopilador NetFlow. La verificación de NetFlow se realiza con un examen de la información almacenada en el recopilador NetFlow. Como mínimo, revise la caché local de NetFlow en un router para asegurarse de que el router esté recopilando los datos.

NetFlow se configuró en el router R1 de la siguiente manera:

- Dirección IP 192.168.1.1/24 en G0/1
- NetFlow controla el tráfico entrante y saliente.
- Recopilador de NetFlow en 192.168.1.3/24
- Puerto de captura de UDP 2055 de NetFlow
- Formato de exportación de NetFlow versión 5

Para mostrar un resumen de las estadísticas de contabilidad de NetFlow, así como el protocolo que utiliza el mayor volumen de tráfico, y ver entre qué hosts fluye este tráfico, utilice el comando **show ip cache flow** en el modo EXEC del usuario o el modo EXEC privilegiado. Este comando se introduce en el R1 para verificar la configuración de NetFlow, como se ve en la figura 1. El resultado del comando detalla qué protocolo utiliza el mayor volumen del tráfico y entre qué hosts fluye este tráfico. En la tabla de la figura 1, se describen los campos importantes que se muestran en las líneas de la caché de switching de flujo de la visualización.

El resultado en la parte superior de la visualización confirma que el router está recopilando datos. La primera entrada resaltada indica que NetFlow controla un conteo de 178 617 paquetes. El final del resultado muestra estadísticas acerca de tres flujos, la que está resaltada corresponde a una conexión HTTPS activa entre el recopilador NetFlow y el R1. También muestra el puerto de origen (SrcP) y el puerto de destino (DstP) en sistema hexadecimal.

Nota: el valor hexadecimal 01BB equivale al valor decimal 443, el puerto TCP bien conocido para HTTPS.

En la figura 2, se describen los campos importantes en las líneas de la caché de switching de flujo del resultado del comando **show ip cache flow**.

En la figura 3, se describen los campos importantes en la actividad según las líneas de protocolo del resultado del comando**show ip cache flow**.

En la figura 4, se describen los campos importantes en las líneas de registro de NetFlow del resultado del comando **show ip cache flow**.

Si bien el resultado del comando **show ip cache flow** confirma que el router está recopilando datos, para asegurarse de que NetFlow se configuró en las interfaces y en las direcciones correctas, utilice el comando **show ip flow interface**, como se muestra en la figura 5.

Para revisar la configuración de los parámetros de exportación, utilice el comando **show ip flow export**, que se muestra en la figura 5. En la primera línea resaltada, se muestra que NetFlow está habilitado con el formato de exportación de la versión 5. En las últimas líneas resaltadas en la figura 5, se muestra que se exportaron 1764 flujos en forma de 532 datagramas UDP al recopilador NetFlow en 192.168.1.3 a través del puerto 2055.

Verificación de la configuración de NetFlow

```
R1# show ip cache flow
IP packet size distribution (178617 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .002 .080 .008 .005 .001 .000 .001 .001 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .895 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  5 active, 4091 inactive, 1573 added
  18467 ager polls, 0 flow alloc failures
  Active flows timeout in 1 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
  5 active, 1019 inactive, 1569 added, 1569 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol       Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------       Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet         3       0.0         3    50      0.0       1.0      15.0
TCP-WWW          245       0.0         6    93      0.0       0.3       2.4
TCP-other        529       0.0        27    57      0.2       0.7       6.2
UDP-other        328       0.0         6   107      0.0       2.4      15.3
ICMP             711       0.0       226  1261      2.4       0.2      15.4
```

Descriptores de la caché de switch del comando `show ip cache flow`

Campo	Descripción
bytes	Cantidad de bytes de memoria que utiliza la caché de NetFlow.
active	Cantidad de flujos activos en la caché de NetFlow en el momento en que se introdujo este comando.
inactive	Cantidad de búfer de flujo que se asignan en la caché de NetFlow, pero que actualmente no se asignaron a un flujo específico en el momento en que se introdujo este comando.

Descriptores del resultado de protocolo del comando `show ip cache flow`

Operación	Descripción
`Protocolo`	Protocolo IP y número de puerto bien conocido.
`Total Flows`	Cantidad de flujos en la caché para este protocolo desde la última vez que se borraron las estadísticas.
`Flows/Sec`	Cantidad promedio de flujos para este protocolo por segundo; equivale a la cantidad total de flujos dividida por la cantidad de segundos de este período de resumen.
`Packets/Flow`	Cantidad promedio de paquetes para los flujos de este protocolo; equivale a la cantidad total de paquetes para este protocolo dividida por la cantidad de flujos para este protocolo durante este período de resumen.
`Bytes/Pkt`	Cantidad promedio de bytes para los paquetes de este protocolo; equivale a la cantidad total de bytes para este protocolo dividida por la cantidad total de paquetes para este protocolo durante este período de resumen.
`Packets/Sec`	Cantidad promedio de paquetes para este protocolo por segundo; equivale a la cantidad total de paquetes para este protocolo dividida por la cantidad total de segundos de este período de resumen.
`Active(Sec)/Flow`	Cantidad de segundos desde el primer paquete hasta el último paquete de un flujo que caducó dividida por la cantidad total de flujos para este protocolo durante este período de resumen.
`Idle(Sec)/Flow`	Cantidad de segundos observados desde el último paquete de cada flujo que no caducó para este protocolo hasta el momento en que se introdujo el comando **`show ip cache verbose flow`** dividida por la cantidad total de flujos para este protocolo durante este período de resumen.

Descriptores del registro de NetFlow del comando `show ip cache flow`

Operación	Descripción
`SrcIf`	Interfaz en la que se recibió el paquete.
`SrcIPaddress`	Dirección IP del dispositivo que transmitió el paquete.
`DstIf`	Interfaz desde la que se transmitió el paquete; si inmediatamente después del campo DstIf figura un asterisco (*), el flujo que se muestra es un flujo saliente.
`DstIPaddress`	Dirección IP del dispositivo de destino.
`Pr`	Número de puerto "bien conocido" del protocolo IP en formato hexadecimal.
`SrcP`	El número de puerto de protocolo de origen en sistema hexadecimal.
`DstP`	El número de puerto de protocolo de destino en sistema hexadecimal.
`Packets`	Cantidad de paquetes conmutados a través de este flujo.

Verificación de la configuración de NetFlow

```
R1# show ip flow interface
GigabitEthernet0/1
  ip flow ingress
  ip flow egress
```

```
R1# show ip flow export
Flow export v5 is enabled for main cache
  Export source and destination details :
  VRF ID : Default
    Destination(1)  192.168.1.3 (2055)
  Version 5 flow records
  1764 flows exported in 532 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
```

Capítulo 8: Supervisión de la red 8.3.3.1 Identificación de las funciones del recopilador NetFlow

Un recopilador NetFlow es un host que ejecuta software de aplicación. Este software se especializa en el manejo de los datos de NetFlow sin procesar. Este recopilador se puede configurar para recibir información de NetFlow de varios dispositivos de red. Los recopiladores NetFlow agregan y organizan datos de NetFlow según lo que indica el administrador de red dentro de las limitaciones del software.

En un recopilador NetFlow, los datos de NetFlow se escriben en una unidad a intervalos especificados. El administrador puede ejecutar varios esquemas o subprocesos de recolección simultáneamente. Por ejemplo, se pueden almacenar distintos cortes de datos para admitir la comparación entre la planificación y la facturación; un recopilador NetFlow puede producir fácilmente los esquemas de agregación adecuados.

En la figura 1, se muestra un recopilador NetFlow que escucha de manera pasiva los datagramas de NetFlow exportados. Una aplicación de recopilador NetFlow proporciona una solución de alto rendimiento, fácil de usar y escalable para ajustar el consumo de datos de exportación de NetFlow de varios dispositivos. El uso que le da una organización varía, pero el propósito suele ser admitir los flujos fundamentales asociados a las aplicaciones de consumidores. Estos incluyen la contabilidad, la facturación y la planificación y el monitoreo de red.

Existen varios recopiladores NetFlow en el mercado. Estas herramientas permiten el análisis del tráfico en la red al mostrar los hosts principales (o los más activos), las aplicaciones más usadas y otros medios de medir los datos de tráfico, como se muestra en la figura 2. Un recopilador NetFlow muestra los tipos de tráfico (web, correo, FTP, peer-to-peer, etc.) en la red, así como los dispositivos que envían y reciben la mayoría del tráfico. La recolección de datos proporciona a un administrador de red datos sobre los principales emisores, hosts y oyentes.

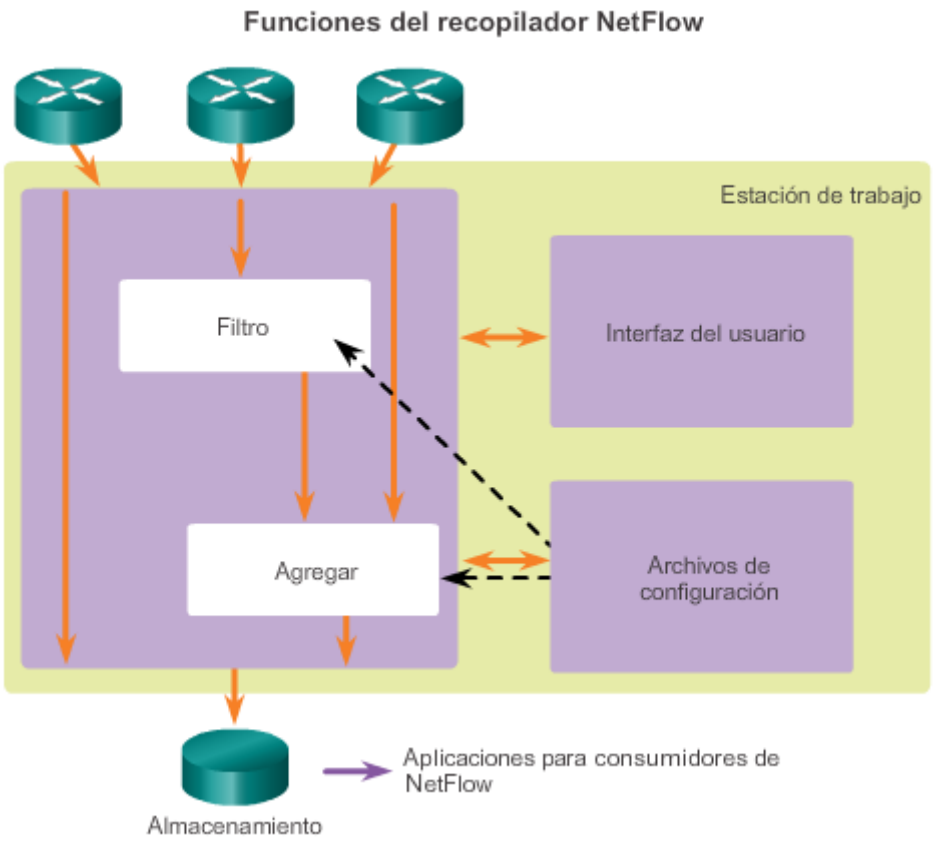
Dado que los datos se preservan con el tiempo, el análisis posterior del tráfico de la red puede determinar tendencias de uso de la red.

Sobre la base del uso de analizadores NetFlow, un administrador de red puede identificar lo siguiente:

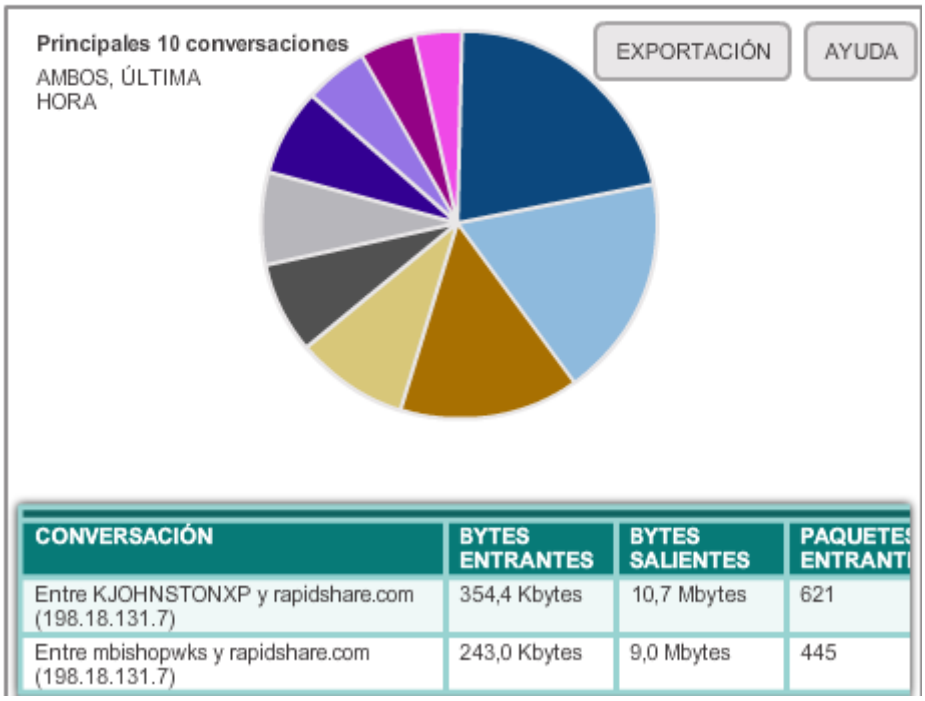
- Quiénes son los principales emisores y con quién hablan.
- Qué sitios web se visitan regularmente y qué se descarga.
- Quién genera la mayor parte del tráfico.
- Si hay suficiente ancho de banda para admitir actividad esencial.
- Quién monopoliza el ancho de banda.

La cantidad de información que puede analizar un recopilador NetFlow varía según la versión de NetFlow que se utilice, ya que los distintos formatos de exportación de NetFlow constan de distintos tipos de registro de NetFlow. Un registro de NetFlow contiene información específica sobre el tráfico real que constituye un flujo de NetFlow.

Un recopilador NetFlow proporciona la visualización y el análisis en tiempo real de los datos de flujo registrados y agregados. Se pueden especificar los routers y los switches admitidos, así como el esquema de agregación y el intervalo de tiempo para almacenar datos antes del siguiente análisis periódico. Los datos se pueden clasificar y visualizar de una manera que sea útil para los usuarios: gráficos de barras, gráficos circulares o histogramas de los informes clasificados. Después se pueden exportar los datos a hojas de cálculo, como las de Microsoft Excel, para obtener análisis, tendencias e informes más detallados.



Emisores principales del recopilador NetFlow



Capítulo 8: Supervisión de la red 8.3.3.2 Análisis de NetFlow con un recopilador NetFlow

Plixer International desarrolló el software analizador NetFlow Scrutinizer. Scrutinizer es una de muchas opciones para capturar y analizar datos de NetFlow en un recopilador NetFlow.

Recuerde la configuración del tema anterior:

- Dirección IP 192.168.1.1/24 en G0/1
- Se controla el tráfico entrante y saliente para NetFlow.
- Recopilador de NetFlow en 192.168.1.3/24
- Puerto de captura de UDP 2055 de NetFlow
- Formato de exportación de NetFlow versión 5

Se instaló el software Scrutinizer en el recopilador NetFlow en 192.168.1.3/24.

En la figura 1, se muestra la interfaz del software al abrir la aplicación Scrutinizer.

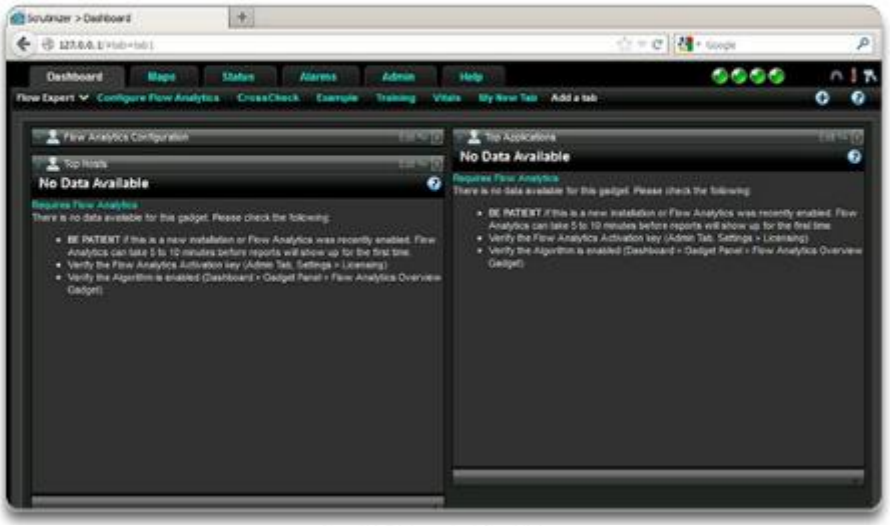
En la figura 2, se muestra el resultado de hacer clic en la ficha Status (Estado) una vez que se ejecuta la aplicación. El software muestra un mensaje: Flows detected, please wait while Scrutinizer prepares the initial reports (Se detectaron flujos, espere mientras Scrutinizer prepara los informes iniciales).

En la figura 3, se muestra la pantalla Status después de unos minutos. El router R1 se configuró con el nombre de dominio cisco.com.

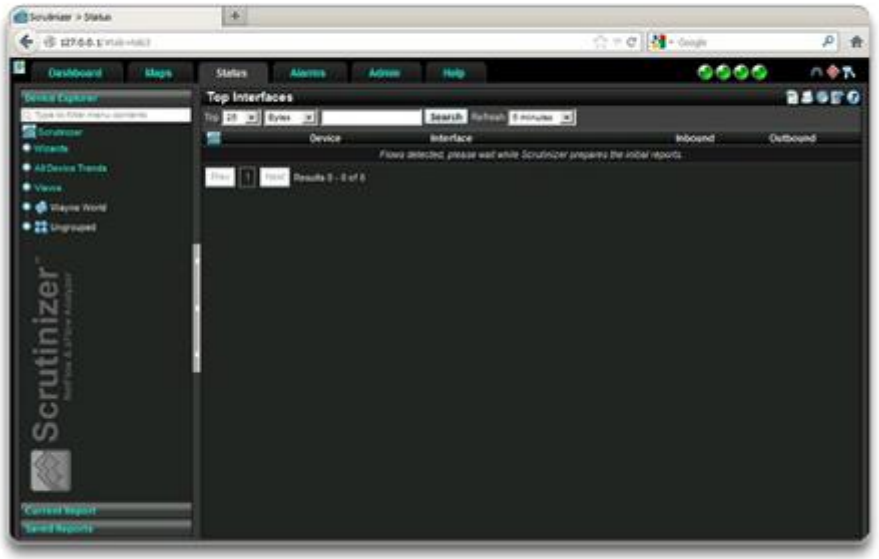
La configuración SNMP de la sección anterior sigue activa en el R1. El software Scrutinizer se configuró con la comunidad SNMP *batonaug* en la ficha **Admin Settings** (Configuración de administración). Cuando se hace clic en el enlace SNMP de R1.cisco.com en el panel izquierdo, se muestra la visualización de la figura 4. Esto muestra un análisis de tráfico básico para el R1 comunicado al recopilador NetFlow mediante SNMPv2c. Multi Router Traffic Grapher (MRTG) es el software gratuito que utilizan muchos administradores de red para el análisis de tráfico básico. La aplicación Scrutinizer integra MRTG, que produce los gráficos de la figura 4. El gráfico superior refleja el tráfico entrante y el gráfico inferior refleja el tráfico saliente de la interfaz G0/1 en el R1.

Por último, en la figura 5, la ficha**Dashboard** (Tablero) muestra los datos de NetFlow que se informan para Top Hosts (Hosts principales) y Top Applications (Aplicaciones principales). El software Scrutinizer tiene disponibles decenas de estos gadgets para mostrar diversas categorizaciones de datos. En la figura 5, el host principal es el R1, con la mayor cantidad de tráfico entre el R1 y el recopilador NetFlow. La aplicación principal es HTTPS, seguida de SNMP, HTTP, SSH, ICMP y NetBIOS.

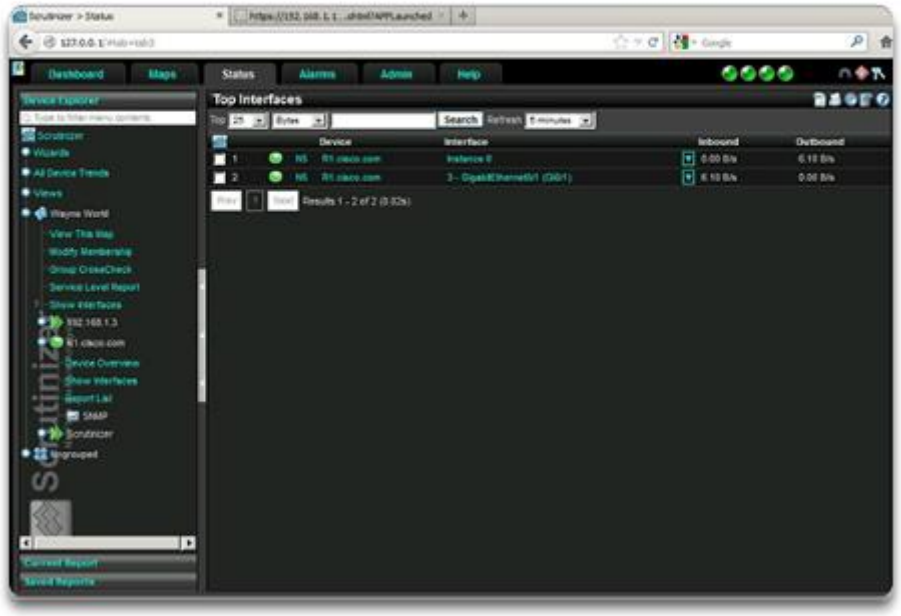
Análisis de NetFlow



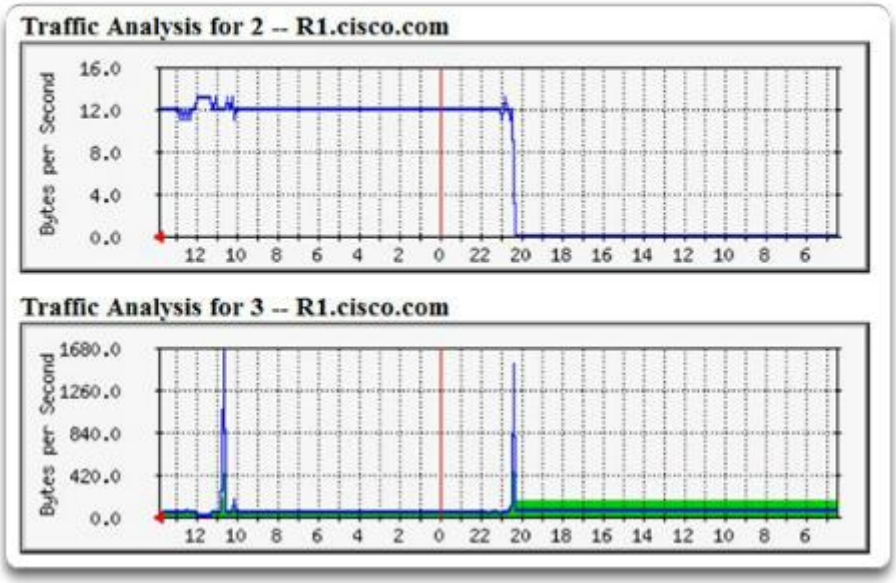
Análisis de NetFlow



Análisis de NetFlow



Análisis de NetFlow



Análisis de NetFlow

Capítulo 8: Supervisión de la red 8.3.3.3 Práctica de laboratorio: Recopilación y análisis de datos de NetFlow

En esta práctica de laboratorio, cumplirá los siguientes objetivos:

- Parte 1: armar la red y configurar los parámetros básicos de los dispositivos
- Parte 2: Configurar NetFlow en un router
- Parte 3: Analizar NetFlow mediante la CLI
- Parte 4: Explorar el software recopilador y analizador NetFlow

Práctica de laboratorio: Recopilación y análisis de datos de NetFlow

Capítulo 8: Supervisión de la red 8.4.1.1 Actividad de clase: Caja de herramientas de un administrador de red para el monitoreo

Caja de herramientas de un administrador de red para el monitoreo

Como administrador de red de una pequeña o mediana empresa, acaba de comenzar con el monitoreo de red mediante CLI en los routers, los switches y los servidores de la empresa.

Decide crear una lista situacional en la que explica cuándo usar cada método. Los métodos de monitoreo de red que se deben incluir son los siguientes:

- Syslog
- SNMP
- NetFlow

Actividad de clase: Caja de herramientas de un administrador de red para el monitoreo

Capítulo 8: Supervisión de la red 8.4.1.2 Resumen

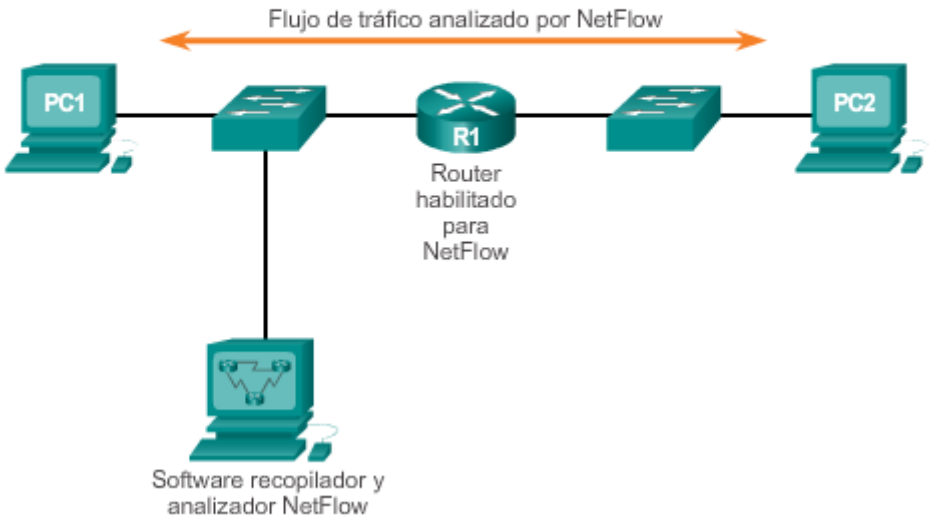
El tiempo en los dispositivos de red Cisco se puede sincronizar mediante NTP.

Los dispositivos de red Cisco pueden registrar mensajes de syslog en un búfer interno, en la consola, en una línea terminal o en un servidor de syslog externo. Un administrador de red puede configurar qué tipos de mensajes se deben recopilar y dónde enviar los mensajes marcados con la hora.

El protocolo SNMP tiene tres elementos: el administrador, el agente y la MIB. El administrador de SNMP reside en NMS, mientras que el agente y la MIB se encuentran en los dispositivos cliente. El administrador de SNMP puede sondear a los dispositivos cliente para obtener información, o puede utilizar un mensaje de trap que le indica a un cliente que debe informar inmediatamente si llega a determinado umbral. SNMP también se puede utilizar para cambiar la configuración de un dispositivo. SNMPv3 es la versión recomendada porque proporciona seguridad. SNMP es una herramienta de administración remota integral y potente. Casi todos los elementos disponibles en un comando **show** están disponibles mediante SNMP.

La tecnología del IOS de Cisco NetFlow es el estándar para recopilar datos operativos IP de las redes IP. NetFlow mide con eficacia cuáles son los recursos de red que se utilizan y con qué propósitos. NetFlow usa los campos del encabezado para distinguir los flujos de datos. NetFlow es una tecnología de “inserción”, en la que el dispositivo cliente inicia el envío de datos a un servidor configurado.

NetFlow en la red



Capítulo 9: Resolución de problemas de red 9.0.1.1 Introducción

Si una red o una parte de una red queda fuera de servicio, esto puede tener un impacto negativo importante en la empresa. Cuando ocurren problemas en la red, los administradores deben usar un enfoque sistemático de resolución de problemas a fin de que la red vuelva a funcionar completamente lo antes posible.

La capacidad de un administrador de red para resolver problemas de red de manera rápida y eficaz es una de las habilidades más buscadas en TI. Las empresas necesitan personas con habilidades sólidas de resolución de problemas de red, y la única forma de obtener estas habilidades es a través de la experiencia práctica y el uso de métodos sistemáticos de resolución de problemas.

En este capítulo, se describe la documentación de red que se debe mantener así como los procedimientos, los métodos y las herramientas generales de resolución de problemas. También se analizan los síntomas y las causas típicos en distintas capas del modelo OSI. En este capítulo, también se incluye información sobre la resolución de problemas de rutas y ACL.

Al finalizar este capítulo, podrá hacer lo siguiente:

- Explicar la forma en que se elabora y se utiliza la documentación de red para resolver problemas de red.
- Describir el proceso general de resolución de problemas.
- Comparar los métodos de resolución de problemas que usan un enfoque sistemático, en capas.
- Describir las herramientas de resolución de problemas que se utilizan para recolectar y analizar síntomas de los problemas de red.
- Determinar los síntomas y las causas de los problemas de red mediante un modelo en capas.
- Resolver problemas de una red mediante un modelo en capas.

Capítulo 9: Resolución de problemas de red 9.0.1.2 Actividad de clase: Falla de la red

Falla de la red

Acaba de mudarse a una nueva oficina, y la red es muy pequeña. Después de un largo fin de semana dedicado a configurar la nueva red, advierte que esta no funciona correctamente.

Algunos dispositivos no tienen acceso entre ellos y algunos no pueden acceder al router que se conecta al ISP.

Su responsabilidad consiste en llevar a cabo la resolución y la reparación de problemas. Para identificar las posibles áreas de resolución de problemas, decide comenzar con los comandos básicos.

Actividad de clase: Falla de la red

Capítulo 9: Resolución de problemas de red 9.1.1.1 Documentación de la red

Para que los administradores de red puedan monitorear y resolver problemas de red, deben tener un conjunto completo de documentación de red precisa y actual. Esta documentación incluye:

- Archivos de configuración, incluidos los de la red y los del sistema final
- Diagramas de topología física y lógica
- Un nivel de rendimiento de línea de base

La documentación de red permite que los administradores de red diagnostiquen y corrijan de manera eficaz los problemas de la red, según el diseño y el rendimiento esperado de la red en condiciones de operación normales. Toda la información de la documentación de red se debe conservar en una única ubicación, ya sea en forma impresa o en la red, en un servidor protegido. Debe realizarse una copia de seguridad del registro, la que se debe conservar en una ubicación diferente.

Archivos de configuración de red

Los archivos de configuración de red contienen registros precisos y actualizados del hardware y el software usados en una red. En los archivos de configuración de la red, debe existir una tabla para cada dispositivo de red utilizado con toda la información relevante sobre ese dispositivo. En la figura 1, se muestran ejemplos de tablas de configuración de red para dos routers. En la figura 2, se muestra una tabla similar para un switch LAN.

La información que se podría reunir en una tabla de dispositivo incluye lo siguiente:

- Tipo de dispositivo, designación de modelo
- Nombre de la imagen del IOS
- Nombre de host de red del dispositivo
- Ubicación del dispositivo (edificio, piso, sala, rack, panel)
- En caso de dispositivo modular, todos los tipos de módulos y en qué ranura de módulo se ubican
- Direcciones de la capa de enlace de datos
- Direcciones de la capa de red
- Cualquier información adicional importante sobre los aspectos físicos del dispositivo

Archivos de configuración del sistema final

Los archivos de configuración del sistema final se centran en el hardware y el software usados en los dispositivos del sistema final, como servidores, consolas de administración de red y estaciones de trabajo de los usuarios. Un sistema final configurado incorrectamente puede tener un impacto negativo en el rendimiento general de una red. Por este motivo, para resolver problemas, puede ser muy útil tener un registro de línea de base de muestra del hardware y del software usado en los dispositivos incluido en el registro del sistema final, como se muestra en la figura 3.

Para resolver problemas, se podría registrar la siguiente información en la tabla de configuración del sistema final:

- Nombre del dispositivo (propósito)
- Sistema operativo y versión
- Direcciones IPv4 e IPv6
- Máscara de subred y longitud de prefijo
- Gateway predeterminado, servidor DNS y direcciones del servidor WINS
- Cualquier aplicación de red de ancho de banda elevado que se ejecute en el sistema final

Registro del router

Nombre y modelo del dispositivo	Nombre de interfaz	Dirección MAC	Dirección IPv4	Direcciones IPv6	Protocolos de enrutamiento IP
R1, Cisco 1941, c1900-universalk9-mz.SPA.152-4.M1	G0/0	0007.8580.a159	192.168.10.1 /24	2001:db8:cafe:10::1/64 fe80::1	EIGRPv4 10 EIGRPv6 20
	G0/1	0007.8580.a160	192.168.11.1 /24	2001:db8:cafe:11::1/64 fe80::1	EIGRPv4 10 EIGRPv6 20
	S0/0/0	No aplicable	10.1.1.1/30	2001:db8:acad:20::1/64 fe80::	EIGRPv4 10 EIGRPv6 20
	S0/0/1	No aplicable	Ninguno	Ninguno	Ninguno
R2, Cisco 1941, c1900-universalk9-mz.SPA.152-4.M1	S0/0/0	No aplicable	10.1.1.2/30	2001:db8:acad:20::2/64 fe80::2	EIGRPv4 10 EIGRPv6 20

Registro del switch

Nombre del switch, modelo, direcciones IP de administración	Puerto	Velocidad	Duplex	STP	Puerto Fast	Estado troncal	EtherChannel L2 o L3	VLAN	Tecla
S1, Cisco WS-2960-24TT, 192.168.10.2/24, 2001:db6:acad:99::2, c2960-lanbasek9-mz.150-2.SE	F0/1	100	Automático	Reenviar	No	On	Ninguno	1	Conecta con R1
	F0/2	100	Automático	Reenviar	Sí	No	Ninguno	1	Conecta con PC1
	F0/3								No conectado

Registro del sistema final

Nombre del dispositivo, propósito	Sistema operativo	Dirección MAC	Dirección IP
PC2	Windows 8	5475.D08E.9AD8	192.168.11.10 /24
			2001:DB8:ACAD:11:5075:D0FF:FE8E:9AD8/64
SRV1	Linux	000C.D991.A138	192.168.20.254 /24
			2001:DB8:ACAD:4::100/64

Capítulo 9: Resolución de problemas de red 9.1.1.2 Diagramas de topología de la red

Diagramas de topología de la red

Los diagramas de topología de la red mantienen un registro de la ubicación, la función y el estado de los dispositivos en la red. Hay dos tipos de diagramas de topología de la red: la topología física y la topología lógica.

Topología física

Una topología física de la red muestra la distribución física de los dispositivos conectados a la red. Para resolver problemas de la capa física, es necesario conocer la forma en que los dispositivos están conectados físicamente. La información registrada en el diagrama generalmente incluye:

- Tipo de dispositivo
- Modelo y fabricante

- Versión del sistema operativo
- Tipo de cable e identificador
- Especificación del cable
- Tipo de conector
- Extremos de cables

En la figura 1, se muestra un ejemplo de un diagrama de topología física de la red.

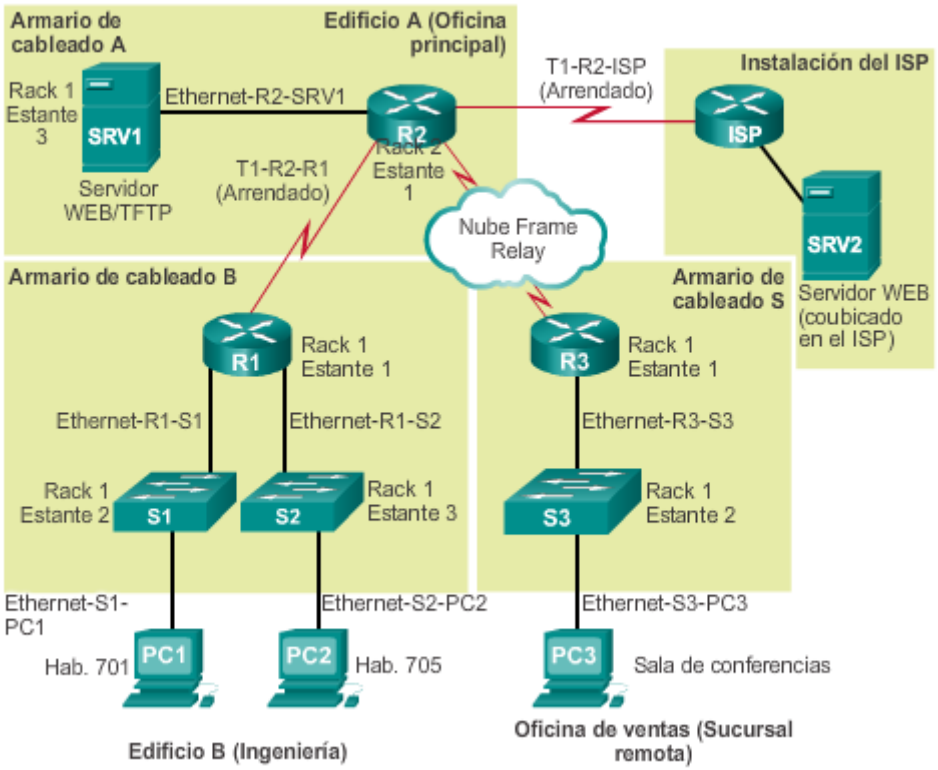
Topología lógica

La topología lógica de la red ilustra la forma en que los dispositivos se conectan a la red de manera lógica, es decir, cómo los dispositivos transfieren datos a través de la red al comunicarse con otros dispositivos. Los símbolos se usan para representar los elementos de la red, como routers, servidores, hosts, concentradores VPN y dispositivos de seguridad. De manera adicional, se pueden mostrar conexiones entre varios sitios, pero no representan ubicaciones físicas reales. La información registrada en un diagrama de red lógico puede incluir lo siguiente:

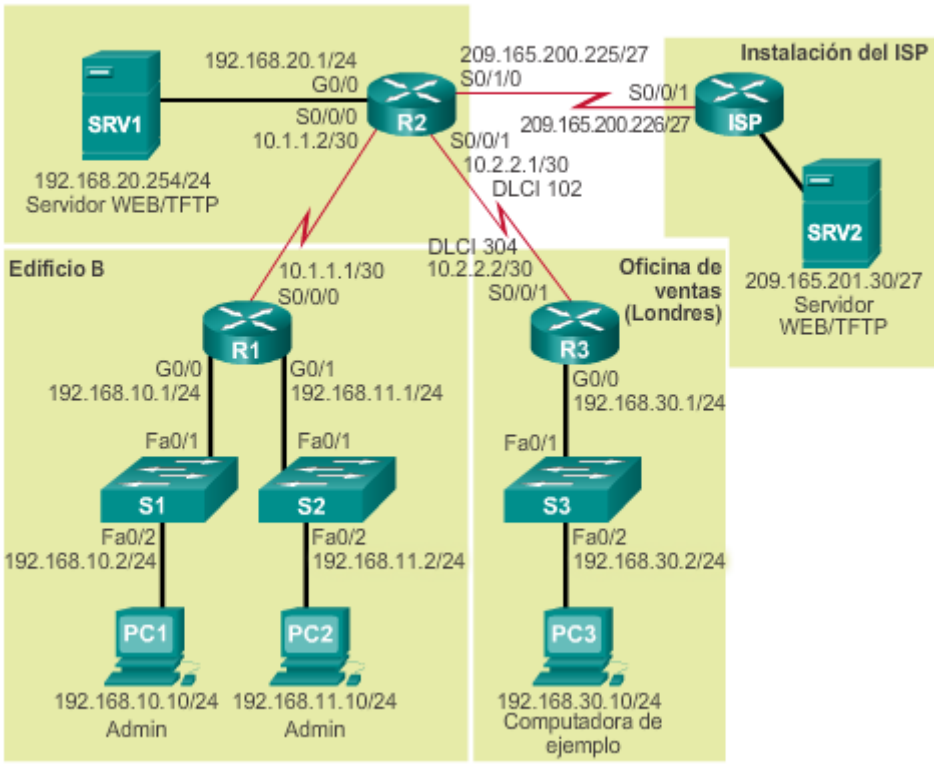
- Identificadores de dispositivos
- Dirección IP y longitudes de prefijos
- Identificadores de interfaz
- Tipo de conexión
- DLCI para circuitos virtuales
- VPN de sitio a sitio
- Protocolos de routing
- Rutas estáticas
- Protocolos de enlace de datos
- Tecnologías WAN utilizadas

En la figura 2, se muestra un ejemplo de topología lógica de red IPv4. Si bien las direcciones IPv6 también se podrían mostrar en la misma topología, puede resultar más claro crear un diagrama separado de topología lógica de red IPv6.

Topología física de la red



Topología lógica de red IPv4



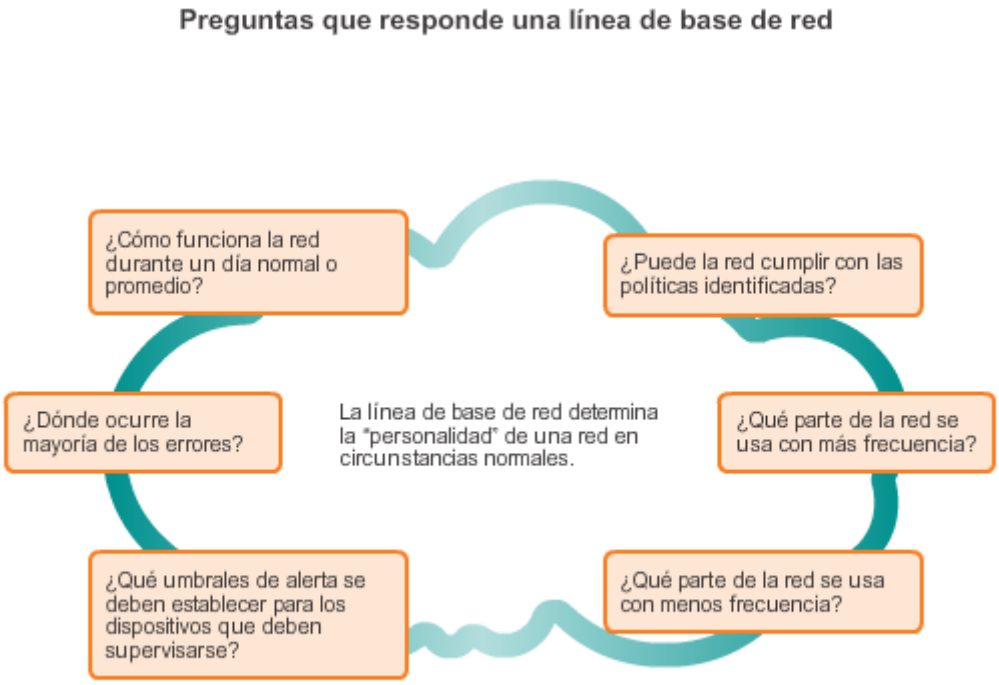
Capítulo 9: Resolución de problemas de red 9.1.1.3 Establecimiento de una línea de base de red

Nivel de rendimiento de línea de base

El propósito de la supervisión de la red es vigilar el rendimiento de la red en comparación con una línea de base predeterminada. Para establecer el rendimiento normal de una red o un sistema, se usa una línea de base. Para establecer una línea de base de rendimiento de la red, es necesario reunir datos sobre el rendimiento de los puertos y los dispositivos que son esenciales para el funcionamiento de la red. En la ilustración, se muestran varias preguntas que se responden mediante una línea de base.

Medir el rendimiento y la disponibilidad iniciales de los dispositivos y enlaces de red fundamentales permite que un administrador de red determine la diferencia entre un comportamiento anormal y un rendimiento correcto de la red, a medida que esta crece o cambian los patrones de tráfico. Una línea de base también proporciona información sobre si el diseño actual de la red puede satisfacer los requisitos comerciales. Sin una línea de base, no existe ningún estándar para medir la naturaleza óptima de los niveles de tráfico y congestión de la red.

Un análisis después de establecer una línea de base inicial también tiende a revelar problemas ocultos. Los datos reunidos muestran la verdadera naturaleza de la congestión, o la congestión potencial, en una red. También puede revelar las áreas de la red que están infrautilizadas y, con bastante frecuencia, puede originar esfuerzos para rediseñar la red sobre la base de las observaciones de calidad y capacidad.



Capítulo 9: Resolución de problemas de red 9.1.1.4 Establecimiento de una línea de base de red (cont.)

Es importante planificar cuidadosamente la línea de base de rendimiento de la red inicial, ya que establece el marco para medir los efectos de los cambios de la red y los esfuerzos posteriores para resolver problemas.

Para planificar la primera línea de base, siga estos pasos:

Paso 1. Determine qué tipos de datos se deben reunir.

Al establecer la línea de base inicial, comience por seleccionar algunas variables que representen a las políticas definidas. Si se seleccionan demasiados puntos de datos, la cantidad de datos puede ser abrumadora, lo que dificulta el análisis de los datos reunidos. Comience de manera simple y realice ajustes a lo largo del proceso. Para comenzar, algunas medidas útiles son el uso de interfaz y el uso de CPU. En la figura 1, se muestran capturas de pantalla de los datos de uso de CPU, según los muestra el software de servicios de aplicaciones de área amplia (WAAS) de Cisco.

Paso 2. Identifique los dispositivos y los puertos de interés.

Use la topología de la red para identificar aquellos dispositivos y puertos para los que se deben medir los datos de rendimiento. Los dispositivos y los puertos de interés incluyen:

- Puertos de dispositivos de red que se conectan a otros dispositivos de red
- Servidores

- Usuarios principales
- Cualquier otro elemento que se considere fundamental para las operaciones

Un diagrama de topología lógica de la red puede ser útil en la identificación de los dispositivos y los puertos principales que se van a supervisar. Por ejemplo, en la figura 2, el administrador de red resaltó los dispositivos y los puertos de interés que se supervisarán durante la prueba de la línea de base. Los dispositivos de interés incluyen la PC1 (la terminal de administración) y el SRV1 (el servidor web/TFTP). Los puertos de interés incluyen aquellos puertos en los routers R1, R2 y R3 que se conectan a otros routers o a los switches y, en el R2, el puerto que se conecta al SRV1 (G0/0).

Al reducir la lista de puertos que se sondean, los resultados son concisos, y se minimiza la carga de administración de la red. Recuerde que una interfaz en un router o un switch puede ser una interfaz virtual, como una interfaz virtual de switch (SVI).

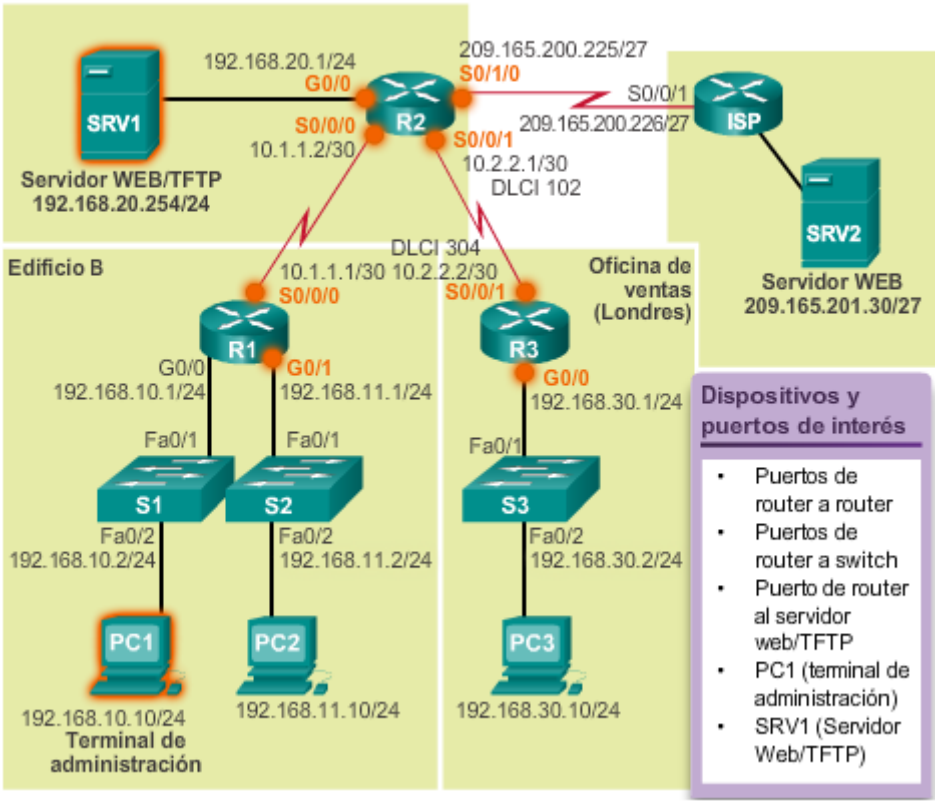
Paso 3. Determine la duración de la línea de base.

Para establecer una imagen típica de la red, la duración y la información de la línea de base que se reúne deben ser suficientes. Es importante que se monitoreen las tendencias diarias del tráfico de la red. También es importante monitorear las tendencias que se producen durante un período más prolongado, como semanas o meses. Por este motivo, al capturar datos para su análisis, el período especificado debe tener, como mínimo, una duración de siete días.

En la figura 3, se muestran ejemplos de varias capturas de pantalla de las tendencias del uso de CPU obtenidas durante un día, una semana, un mes o un año. En este ejemplo, observe que las tendencias de la semana de trabajo son demasiado cortas para revelar el pico de uso recurrente que se produce el sábado por la noche, cada fin de semana, cuando una operación de copia de seguridad de la base de datos consume ancho de banda de la red. Este patrón recurrente se revela en la tendencia mensual. Una tendencia anual, como la que se muestra en el ejemplo, puede ser demasiado prolongada para proporcionar detalles significativos sobre el rendimiento de línea de base. Sin embargo, puede ayudar a identificar patrones a largo plazo que se deben analizar en profundidad. Generalmente, las líneas de base no se deben extender durante más de seis semanas, salvo que se deban medir tendencias específicas a largo plazo. Por lo general, una línea de base de dos a cuatro semanas es adecuada.

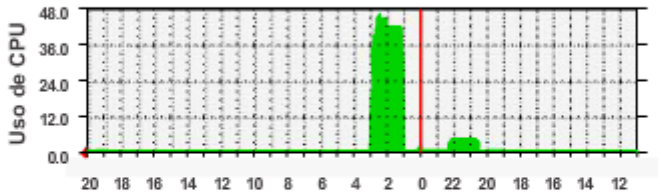
Las mediciones de una línea de base no se deben realizar durante momentos de patrones de tráfico únicos, dado que los datos proporcionarían una representación imprecisa de las operaciones normales de la red. El análisis de línea de base de la red se debe realizar periódicamente. De manera rotativa, realice un análisis anual de toda la red o analice la línea de base de diferentes secciones de la red. Para entender la forma en que el crecimiento y otros cambios afectan la red, el análisis se debe realizar periódicamente.

Planificación de la primera línea de base



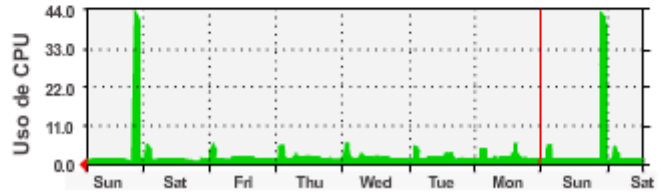
Tendencias de los datos

Gráfico diario (promedio de cinco minutos)



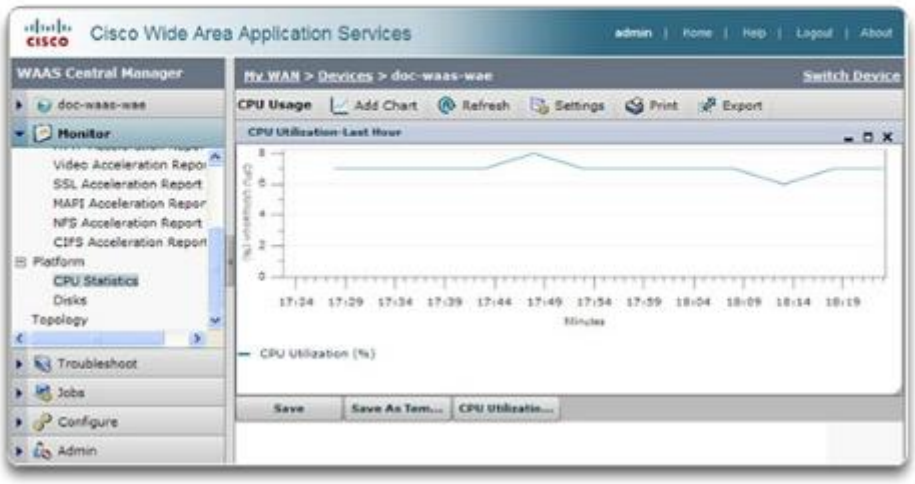
Carga máxima: **46%** Carga promedio: **3%** Carga actual: **1%**

Gráfico semanal (promedio de dos horas)



Carga máxima: **43%** Carga promedio: **2%** Carga actual: **1%**

Recolección de datos



Capítulo 9: Resolución de problemas de red 9.1.1.5 Medición de los datos

Al documentar la red, con frecuencia es necesario reunir información directamente de los routers y los switches. Los comandos obvios y útiles para la documentación de red incluyen **ping**,**traceroute** y **telnet**, así como los siguientes comandos **show**:

- Los comandos **show ip interface brief** y **show ipv6 interface brief** se usan para mostrar el estado activo o inactivo y la dirección IP de todas las interfaces en un dispositivo.

- Los comandos **show ip route** y**show ipv6 route** se usan para mostrar la tabla de routing de un router a fin de detectar los vecinos conectados directamente, los dispositivos remotos adicionales (a través de las rutas detectadas) y los protocolos de routing que se configuraron.

- El comando **show cdp neighbor detail** se usa para obtener información detallada sobre los dispositivos vecinos Cisco conectados directamente.

En la figura 1, se indican algunos de los comandos más comunes del IOS de Cisco que se usan para la recolección de datos.

La recolección manual de datos mediante los comandos **show** en dispositivos de red individuales puede tomar muchísimo tiempo y no es una solución escalable. Por esa razón, la recolección manual de datos se debe reservar para las redes más pequeñas o aquellas que se limitan a los dispositivos de red esenciales. Para diseños de red más simples, en las tareas de línea de base por lo general se combinan la recolección manual de datos con inspectores de protocolos de red simples.

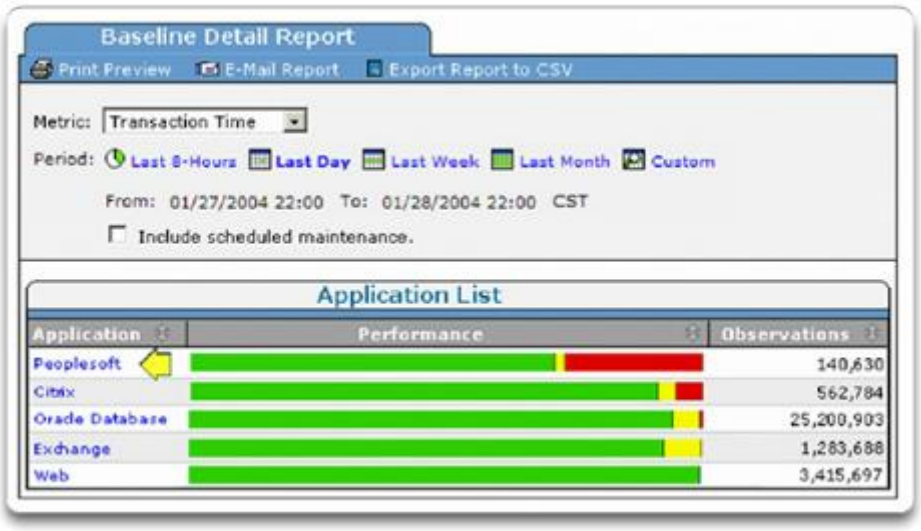
Con frecuencia, para establecer la línea de base de redes grandes y complejas se utiliza un software de administración de red sofisticado. Por ejemplo, como se muestra en la figura 2, el módulo SuperAgent de Fluke Network permite que los administradores creen y revisen informes automáticamente mediante la característica de líneas de base inteligentes. Esta característica compara los niveles de rendimiento actuales con observaciones históricas y

puede identificar automáticamente los problemas de rendimiento y las aplicaciones que no proporcionan los niveles de servicio esperados.

Establecer una línea de base inicial o realizar un análisis de monitoreo del rendimiento puede requerir muchas horas o muchos días para reflejar el rendimiento de la red con precisión. Con frecuencia, el software de administración de red o los inspectores y analizadores de protocolos se ejecutan continuamente a lo largo del proceso de recolección de datos.

Comandos para la recolección de datos

Comando	Descripción
show version	Muestra el tiempo de actividad, información sobre la versión del software y del hardware del dispositivo.
show ip interface [*brief*] **show ipv6 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 interfaces [*interface_type interface_num*]	Muestra la salida detallada de cada interfaz. Para mostrar el resultado detallado de una sola interfaz, incluya el tipo y el número de interfaz en el comando (por ejemplo, gigabitethernet 0/0).
show ip route **show ipv6 route**	Muestra el contenido de la tabla de enrutamiento.
show arp **show ipv6 neighbors**	Muestra el contenido de la tabla ARP (IPv4) y la tabla de vecinos (IPv6).
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	Este comando es útil para recopilar una gran cantidad de información sobre el dispositivo para propósitos de resolución de problemas. Ejecuta varios comandos **show** que se pueden proporcionar a los representantes de soporte técnico al informar un problema.
show ip cache flow	Muestra un resumen de las estadísticas de contabilidad de NetFlow.



Capítulo 9: Resolución de problemas de red 9.1.1.6 Actividad: Identificar los beneficios de establecer una línea de base de red

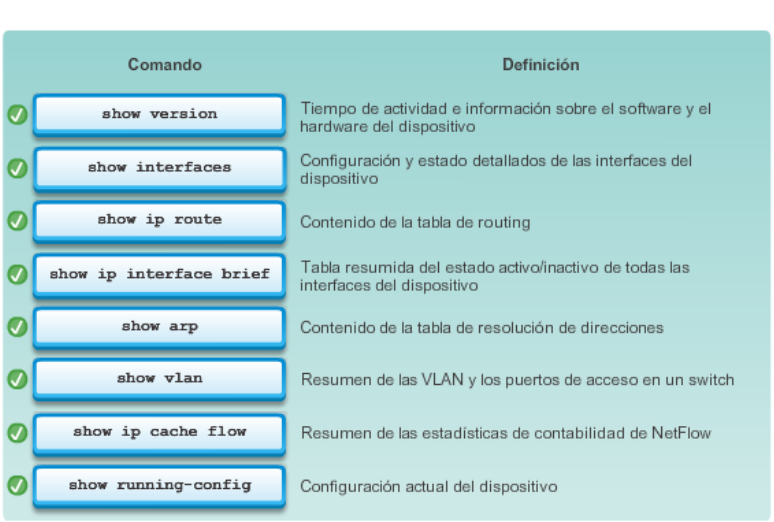
Actividad: Identificar los beneficios de establecer una línea de base de red

Indique cuáles de las afirmaciones que se incluyen a continuación son beneficios de establecer una línea de base de red.

	Beneficios	No es un beneficio
Identificar dónde se producen la mayoría de los errores.	✓	
Ubicar las áreas de la red que se usan con mayor frecuencia.	✓	
Habilitar servicios de transporte rápido entre los campus.		✓
Combinar dos capas de diseño jerárquico.		✓
Investigar si la red puede cumplir con las políticas y los requisitos de uso identificados.	✓	
Identificar las partes de la red que se usan con menos frecuencia.	✓	
Establecer los patrones y las cargas de tráfico para un día normal o promedio.	✓	

Capítulo 9: Resolución de problemas de red 9.1.1.7 Actividad: Identificar los comandos usados para medir datos

Actividad: Medir los datos de rendimiento de la red
Una cada comando relacionado con el rendimiento de la red con su definición.



.

Capítulo 9: Resolución de problemas de red 9.1.1.8 Packet Tracer: Desafío de resolución de problemas sobre la documentación de la red

Información básica/situación

En esta actividad, se abarcan los pasos que se deben seguir para detectar una red principalmente mediante el uso de los comandos **telnet**, **show cdp neighbors detail** y **show ip route**. Esta es la parte 1 de una actividad que consta de dos partes. La parte 2 es Packet Tracer: Desafío de resolución de problemas sobre el uso del registro para resolver problemas, que se presenta más adelante en este capítulo.

La topología que ve cuando abre la actividad de Packet Tracer no muestra todos los detalles de la red. Los detalles se ocultaron mediante la función de clúster de Packet Tracer. La infraestructura de la red se contrajo, y la topología en el archivo muestra solo las terminales. Su tarea consiste en usar sus conocimientos sobre comandos de detección y redes para obtener información acerca de la topología de la red completa y registrarla.

Packet Tracer: Desafío de resolución de problemas sobre la documentación de la red (instrucciones)

Packet Tracer: Desafío de resolución de problemas sobre la documentación de la red (PKA)

Capítulo 9: Resolución de problemas de red 9.1.2.1 Procedimientos generales de resolución de problemas

La resolución de problemas ocupa gran parte del tiempo de los administradores de red y del personal de soporte. Al trabajar en un entorno de producción, el uso de técnicas eficaces de resolución de problemas reduce el tiempo total dedicado a esta tarea. Hay tres etapas principales en el proceso de resolución de problemas:

Etapa 1. Recolección de síntomas: la resolución de problemas comienza con la recolección y el registro de los síntomas de la red, los sistemas finales y los usuarios. Además, el administrador de red determina qué componentes de la red se vieron afectados y de qué forma cambió la funcionalidad de la red en comparación con la línea de base. Los síntomas pueden aparecer de distintas maneras, que incluyen alertas del sistema de administración de red, mensajes de la consola y quejas de los usuarios. Mientras se recolectan los síntomas, es importante que el administrador de red realice preguntas e investigue el problema para restringirlo a una variedad de posibilidades más reducida. Por ejemplo, ¿el problema se limita a un único dispositivo, un grupo de dispositivos, una subred completa o una red de dispositivos?

Etapa 2. Aislamiento del problema: el aislamiento es el proceso mediante el que se eliminan variables hasta que se identifica como la causa a un único problema o a un conjunto de problemas relacionados. Para realizar esto, el administrador de red examina las características de los problemas en las capas lógicas de la red para poder seleccionar la causa más probable. En esta etapa, el administrador de red puede recopilar y registrar más síntomas, según las características que se identifiquen.

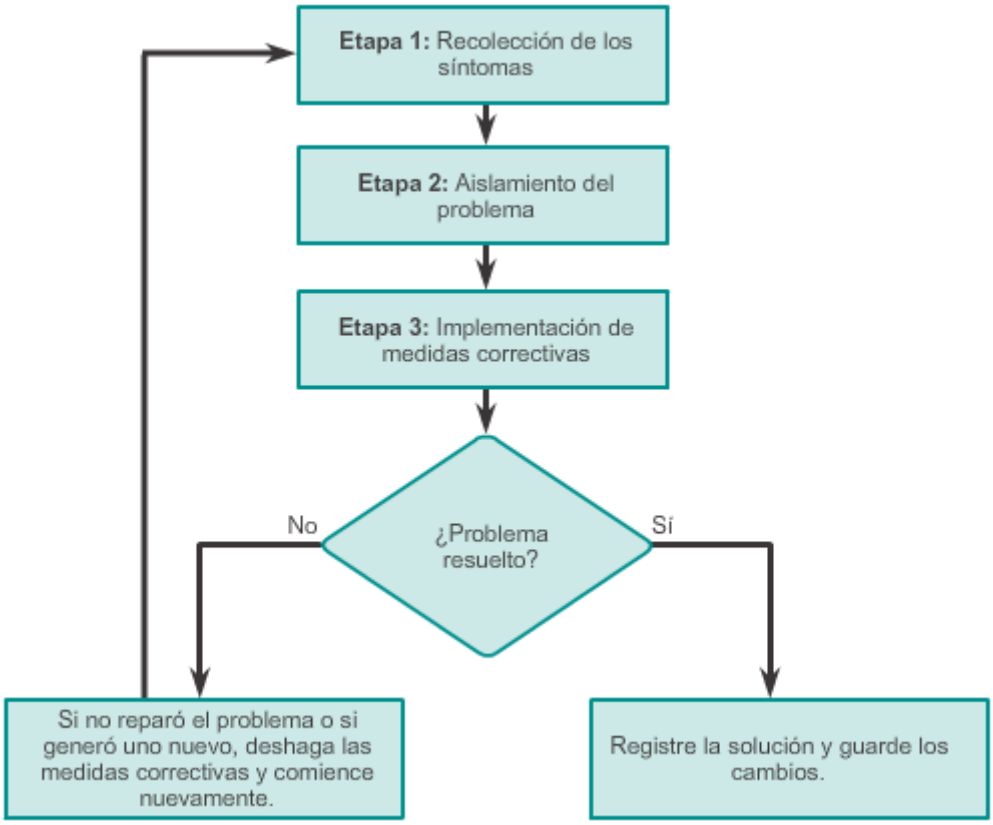
Etapa 3. Implementación de la medida correctiva: una vez que se identificó la causa del problema, el administrador de red trabaja para corregir el problema mediante la implementación, la puesta a prueba y el registro de posibles soluciones. Después de encontrar el problema y determinar una solución, es posible que el administrador de red deba decidir si la solución se puede implementar inmediatamente o si se debe posponer. Esto depende del impacto de los cambios en los usuarios y en la red. La gravedad del problema se debe ponderar en comparación con el impacto de la solución. Por ejemplo, si un servidor o un router fundamentales deben permanecer sin conexión durante una cantidad significativa de tiempo, tal vez sea mejor esperar hasta el final del día de trabajo para implementar la solución. A veces, se puede crear una solución alternativa hasta que se resuelva el problema real. Por lo general, esto forma parte de los procedimientos de control de cambios de una red.

Si la medida correctiva no soluciona el problema o genera otro nuevo, se registra la solución probada, se eliminan los cambios y el administrador de red vuelve a recolectar síntomas y a aislar el problema.

Estas etapas no son mutuamente excluyentes. En cualquier parte del proceso, es posible que sea necesario volver a las etapas anteriores. Por ejemplo, es posible que el administrador de red necesite recolectar más síntomas mientras aísla un problema. Además, cuando se intenta corregir un problema, se puede generar otro. En este caso, se deben eliminar los cambios y comenzar la resolución de problemas nuevamente.

Para cada etapa, se debe establecer una política de resolución de problemas que incluya procedimientos de control de cambios. Una política proporciona una forma coherente de llevar a cabo cada etapa. Parte de la política debe incluir el registro de cada dato importante.

Nota: comunique que el problema se resolvió a los usuarios y a cualquier persona involucrada en el proceso de resolución de problemas. La solución se debe informar a los otros miembros del equipo de TI. El registro adecuado de la causa y la solución ayudan a otros técnicos de soporte a prevenir y resolver problemas similares en el futuro.



Capítulo 9: Resolución de problemas de red 9.1.2.2 Recolección de síntomas

Al recolectar síntomas, es importante que el administrador reúna datos y evidencia para eliminar de manera progresiva posibles causas y, finalmente, identificar la causa raíz del problema. Al analizar la información, el administrador de red formula una hipótesis para proponer posibles causas y soluciones y, al mismo tiempo, eliminar otras.

Existen cinco pasos en la recolección de información:

Paso 1. Recolectar información: para formar una definición del problema, recolecte la información en las solicitudes de soporte y de los usuarios o los sistemas finales afectados por el problema.

Paso 2. Determinar a quién corresponde:si el problema está dentro del ámbito de control de la organización, continúe con la etapa siguiente. Si el problema está fuera del límite de control de la organización (por ejemplo, pérdida de conectividad a Internet fuera del sistema autónomo), comuníquese con un administrador del sistema externo antes de recolectar más síntomas de la red.

Paso 3. Reducir el ámbito: determine si el problema está en la capa de 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 equipo es la causa más probable.

Paso 4. Recolectar síntomas de los dispositivos sospechosos: mediante un método de resolución de problemas en capas, recolecte los síntomas del hardware y el software de los

dispositivos sospechosos. Comience por la posibilidad más probable y use sus conocimientos y experiencia para determinar si es más probable que el problema sea de configuración del hardware o del software.

Paso 5. Registrar los síntomas: a veces, el problema se puede resolver sobre la base de los síntomas registrados. De lo contrario, inicie la etapa de aislamiento del proceso general de resolución de problemas.

Para recolectar síntomas de la red, use los comandos del IOS de Cisco y otras herramientas, por ejemplo:

- **ping, traceroute** y **telnet**(comandos)
- **show** y **debug** (comandos)
- Capturas de paquetes
- Registros de dispositivos

En la tabla de la ilustración, se describen los comandos comunes del IOS de Cisco usados para recolectar los síntomas de un problema de red.

Nota: si bien el comando **debug** es una herramienta importante para recolectar síntomas, genera una gran cantidad de tráfico de mensajes de la consola y puede afectar considerablemente el rendimiento de un dispositivo de red. Si la depuración con el comando **debug** se debe realizar durante el horario de trabajo normal, advierta a los usuarios de la red que se está realizando un esfuerzo para resolver problemas y que el rendimiento de la red se puede ver afectado. Al terminar, recuerde deshabilitar la depuración.

Comandos para recolectar 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 de 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 **show ipv6 interface brief**	Muestra un resumen del estado de todas las interfaces en un dispositivo.
show ip route **show ipv6 route**	Muestra las tablas de routing IPv4 e IPv6 actuales, que contienen las rutas a todos los destinos de red conocidos.
show running-config	Muestra el contenido del archivo de configuración en ejecución en el momento.
[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.

Capítulo 9: Resolución de problemas de red 9.1.2.3 Preguntas a usuarios finales

En muchos casos, un usuario final informa del problema. Con frecuencia, la información puede ser vaga o confusa, por ejemplo, “la red está inactiva” o “no puedo acceder a mi correo electrónico”. En estos casos, el problema se debe definir mejor. Esto puede requerir hacer preguntas a los usuarios finales.

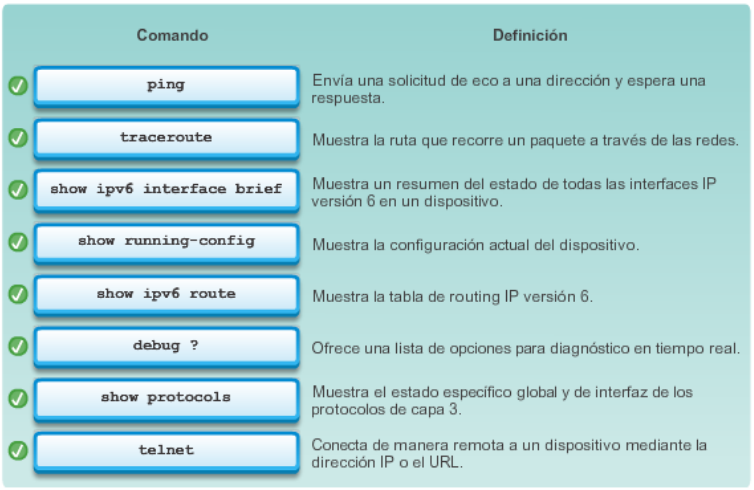
Al preguntarles a los usuarios finales acerca del problema de red que tal vez experimenten, use técnicas de interrogación eficaces. Esto lo ayudará a obtener la información necesaria para registrar los síntomas de un problema. En la tabla de la ilustración, se proporcionan algunas pautas y ejemplos de preguntas 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?

Capítulo 9: Resolución de problemas de red 9.1.2.4 Actividad: Identificar los comandos para recolectar síntomas

Actividad: Recolectar síntomas de un problema de red
Una cada uno de los comandos usados para recolectar información sobre problemas de red con su definición.



Capítulo 9: Resolución de problemas de red 9.1.3.1 Uso de modelos en capas para la resolución de problemas

Una vez que se recopilan todos los síntomas, y si no se identifica una solución, el administrador de red compara las características del problema con las capas lógicas de la red para aislar y resolver el problema.

Los modelos lógicos de tecnología de redes, como los modelos OSI y TCP/IP, dividen la funcionalidad de la red en capas modulares. Cuando se realiza la resolución de problemas, se pueden aplicar estos modelos en capas 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 según lo esperado, el técnico observa las áreas en otra capa que podrían estar causando el problema.

Modelo de referencia OSI

El modelo de referencia OSI proporciona un lenguaje común para los administradores de red y se usa frecuentemente para resolver problemas de red. Por lo general, los problemas se describen en términos de una determinada capa del modelo OSI.

El modelo de referencia OSI describe la forma en que la información de una aplicación de software en una computadora se desplaza a través de un medio de red hasta una aplicación de software en otra computadora.

Las capas superiores (de 5 a 7) del modelo OSI se ocupan de los problemas de aplicación y, generalmente, se implementan solo en el software. La capa de aplicación es la más cercana al usuario final. Los usuarios y los procesos de la capa de aplicación interactúan con las aplicaciones de software que contienen un componente de comunicaciones.

Las capas inferiores (de 1 a 4) del modelo OSI se ocupan de los problemas de transporte de datos. Las capas 3 y 4 por lo general se implementan solo en el 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 físico de red, como el cableado de la red, y es responsable de colocar efectivamente la información en el medio.

En la figura 1, se muestran algunos dispositivos comunes y las capas del modelo OSI que se deben examinar durante el proceso de resolución de problemas de cada dispositivo. Observe que los routers y los switches multicapa se muestran en la capa 4, la capa de transporte. Si bien los routers y los switches multicapa generalmente toman decisiones de reenvío en la capa 3, se pueden usar las ACL en esos dispositivos para tomar decisiones de filtrado con la información de la capa 4.

Modelo TCP/IP

Similar al modelo de red OSI, el modelo de red TCP/IP también divide la arquitectura de red en capas modulares. En la figura 2, se muestra la relación entre el modelo de red TCP/IP y las capas del modelo de red OSI. Esta es una asignación estrecha que permite que la suite de protocolos TCP/IP se comunique correctamente con muchas tecnologías de red.

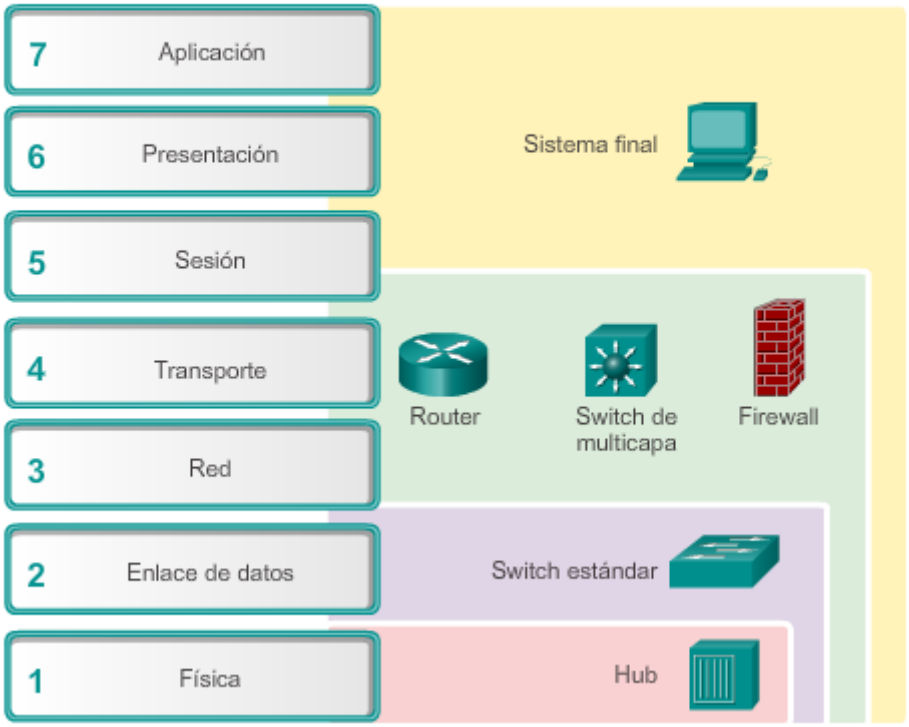
La capa de aplicación en la suite TCP/IP combina las funciones de las tres capas del modelo OSI: sesión, presentación y aplicación. La capa de aplicación proporciona comunicación entre aplicaciones tales como FTP, HTTP y SMTP en hosts separados.

Las capas de transporte de TCP/IP y de OSI se corresponden directamente en cuanto a su función. La capa de transporte es responsable del intercambio de segmentos entre dispositivos en una red TCP/IP.

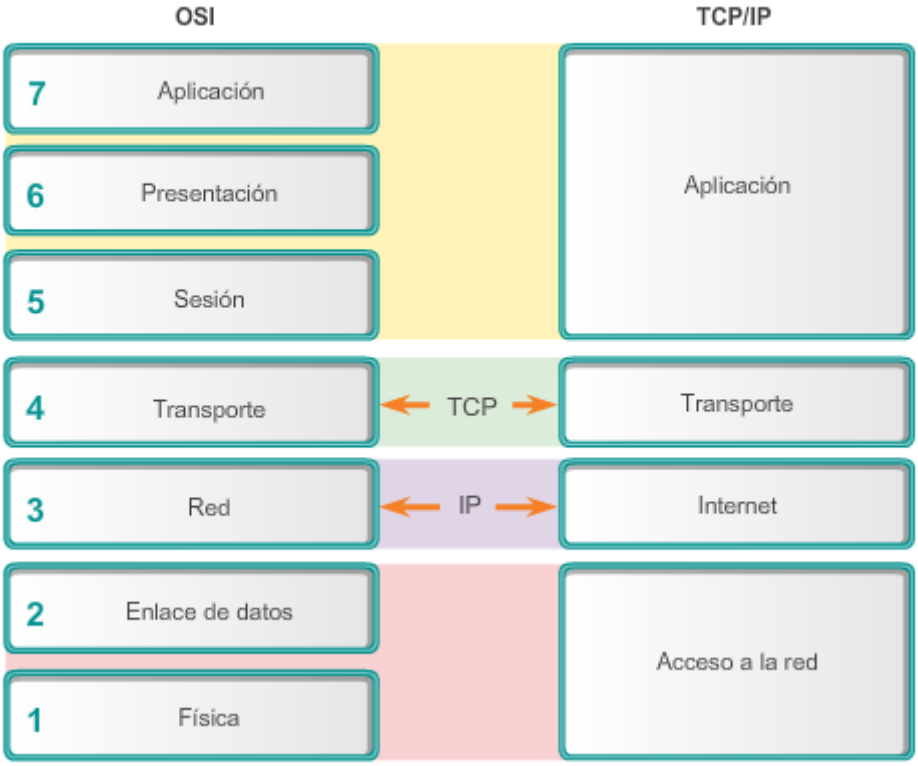
La capa de Internet de TCP/IP se relaciona con la capa de red del modelo OSI. La capa de Internet es responsable de colocar los mensajes en un formato fijo para que los dispositivos los administren.

La capa de acceso a Internet de TCP/IP corresponde a las capas física y de enlace de datos de OSI. La capa de acceso a la red se comunica directamente con los medios de red y proporciona una interfaz entre la arquitectura de la red y la capa de Internet.

Modelo de referencia OSI



Comparación del modelo OSI y el modelo TCP/IP



Mediante los modelos en capas, existen tres métodos principales para resolver problemas de red:

- Ascendente
- Descendente
- Divide y vencerás

Cada método tiene sus ventajas y desventajas. En este tema, se describen los tres métodos y se proporcionan pautas para elegir el mejor método para una situación específica.

Método de resolución de problemas ascendente

En la resolución de problemas ascendente, se comienza por los componentes físicos de la red y se atraviesan las capas del modelo OSI de manera ascendente hasta que se identifica la causa del problema, como se muestra en la figura 1. La resolución de problemas ascendente es un buen método para usar cuando se sospecha que el problema es físico. La mayoría de los problemas de red residen en los niveles inferiores, de modo que, con frecuencia, la implementación del método ascendente es eficaz.

La desventaja del método de resolución de problemas ascendente es que requiere que revise cada dispositivo e interfaz en la red hasta que detecte la posible causa del problema. Recuerde que se debe registrar cada conclusión y cada posibilidad, de modo que es posible que haya mucho papeleo asociado a este enfoque. Otro desafío es determinar qué dispositivos se deben examinar primero.

Método de resolución de problemas descendente

En la figura 2, la resolución de problemas descendente comienza por las aplicaciones de usuario final y atraviesa las capas del modelo OSI de manera descendente hasta que se identifica la causa del problema. Antes de abordar las partes más específicas de la red, se prueban las aplicaciones de usuario final de un sistema final. Use este método para los problemas más simples o cuando crea que el problema está en un software.

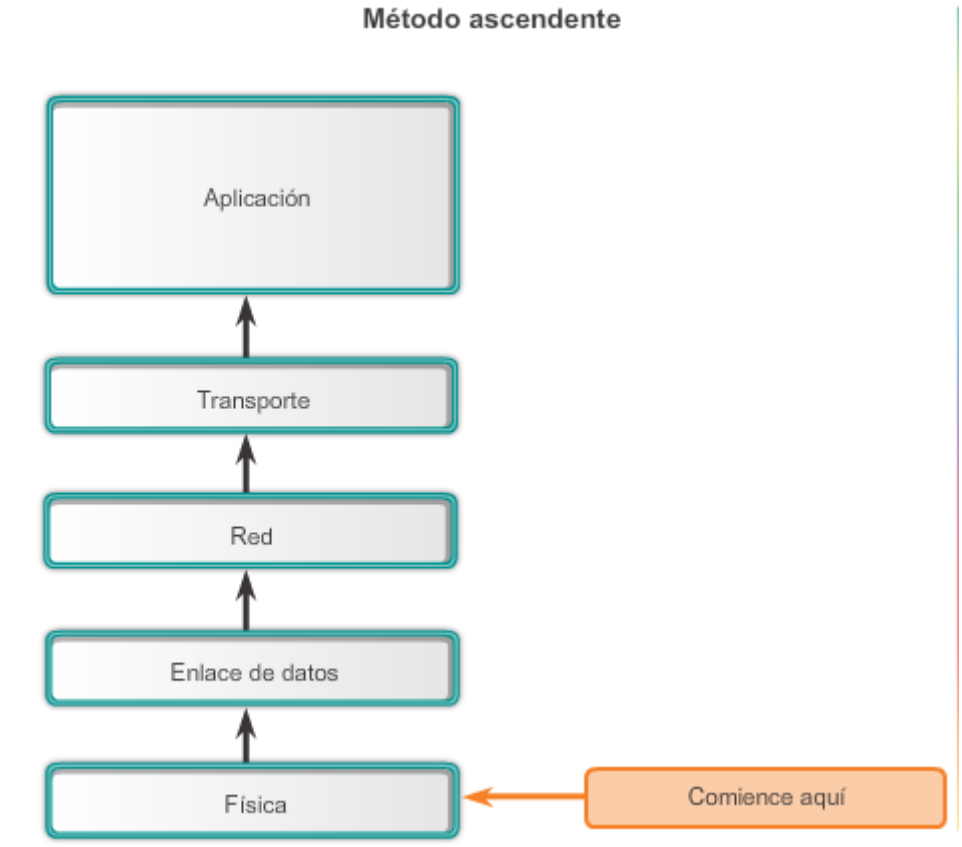
La desventaja del enfoque descendente es que requiere que se revise cada aplicación de red hasta que se detecte la posible causa del problema. Se debe registrar cada conclusión y cada posibilidad. El desafío es determinar qué aplicación se debe examinar primero.

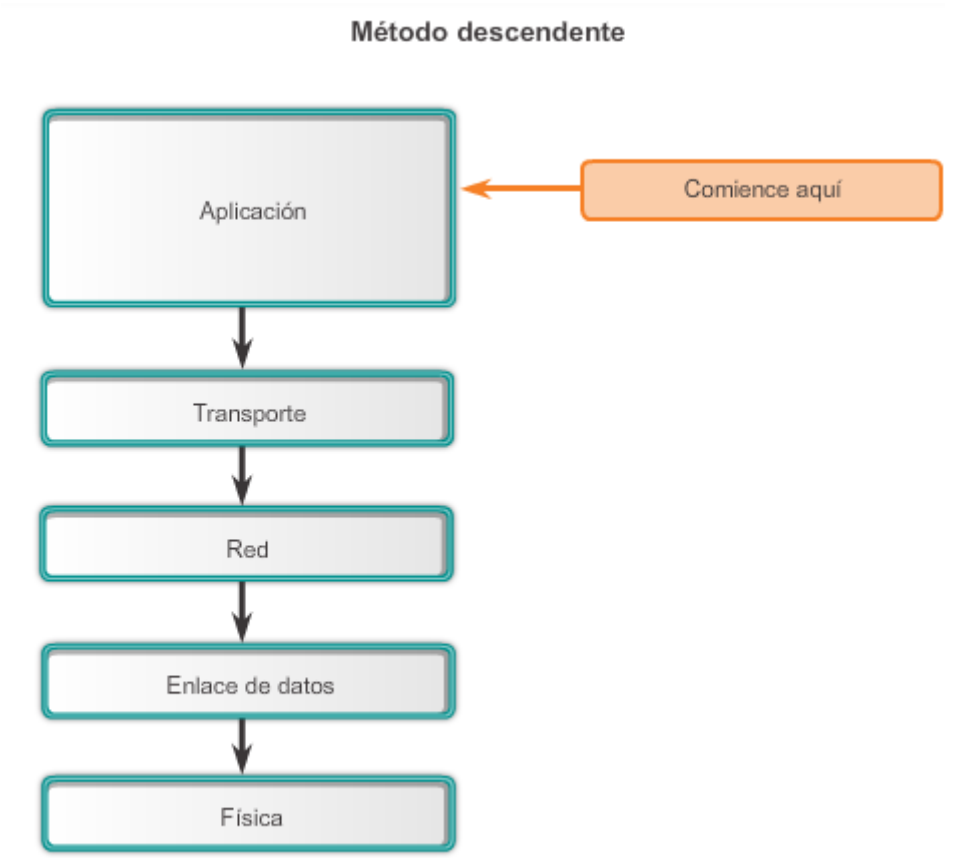
Método de resolución de problemas divide y vencerás

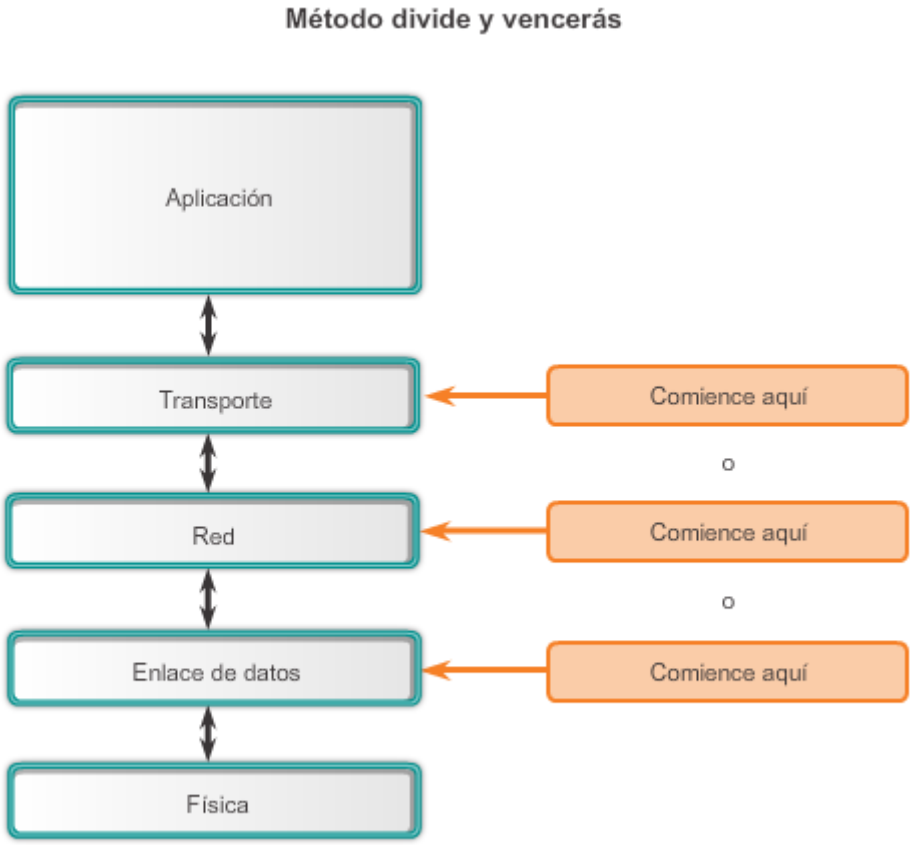
En la figura 3, se muestra el enfoque divide y vencerás para resolver un problema de red. El administrador de red selecciona una capa y hace pruebas en ambos sentidos desde esa capa.

En el método de resolución de problemas divide y vencerás, comienza por reunir las experiencias que el usuario tiene del problema, documenta los síntomas y, después, con esa información, hace una deducción fundamentada sobre la capa del modelo OSI en la que se debe comenzar la investigación. Cuando se verifica que una capa funciona correctamente, se puede suponer que las capas por debajo de ella funcionan. El administrador puede trabajar en las capas del modelo OSI en sentido ascendente. Si una capa del modelo OSI no funciona correctamente, el administrador puede trabajar en el modelo de capas OSI de manera descendente.

Por ejemplo, si los usuarios no pueden acceder al servidor web, pero pueden hacer ping al servidor, entonces el problema se encuentra por encima de la capa 3. Si el ping al servidor falla, es probable que el problema esté en una capa inferior del modelo OSI.


Método ascendente
Aplicación
Transporte
Red
Enlace de datos
Física
Comience aquí


Método descendente
Aplicación
Comience aquí
Transporte
Red
Enlace de datos
Física



Capítulo 9: Resolución de problemas de red 9.1.3.3 Métodos de resolución de problemas

(cont.)

Además del enfoque sistemático de resolución de problemas en capas, también existen otros enfoques menos estructurados.

Un enfoque de resolución de problemas se basa en una deducción fundamentada del administrador de red, según los síntomas del problema. Los administradores de red experimentados implementan este método con mayor éxito porque se apoyan en sus amplios conocimientos y experiencia para aislar y resolver problemas de red con determinación. En el caso de un administrador de red menos experimentado, es muy posible que este método sea más parecido a una resolución de problemas fortuita.

Otro método consiste en comparar una situación de funcionamiento con una en la que no hay funcionamiento y detectar las diferencias significativas, que incluyen:

- Configuraciones
- Versiones de software
- Propiedades del hardware y de otros dispositivos

Si bien este método puede proporcionar una solución que funcione, no revela con claridad la causa del problema. Este método puede ser útil cuando al administrador de red le falta un área de conocimientos o cuando es necesario resolver el problema rápidamente. Después de que se implementa la corrección, el administrador de red puede continuar la investigación para determinar la causa real del problema.

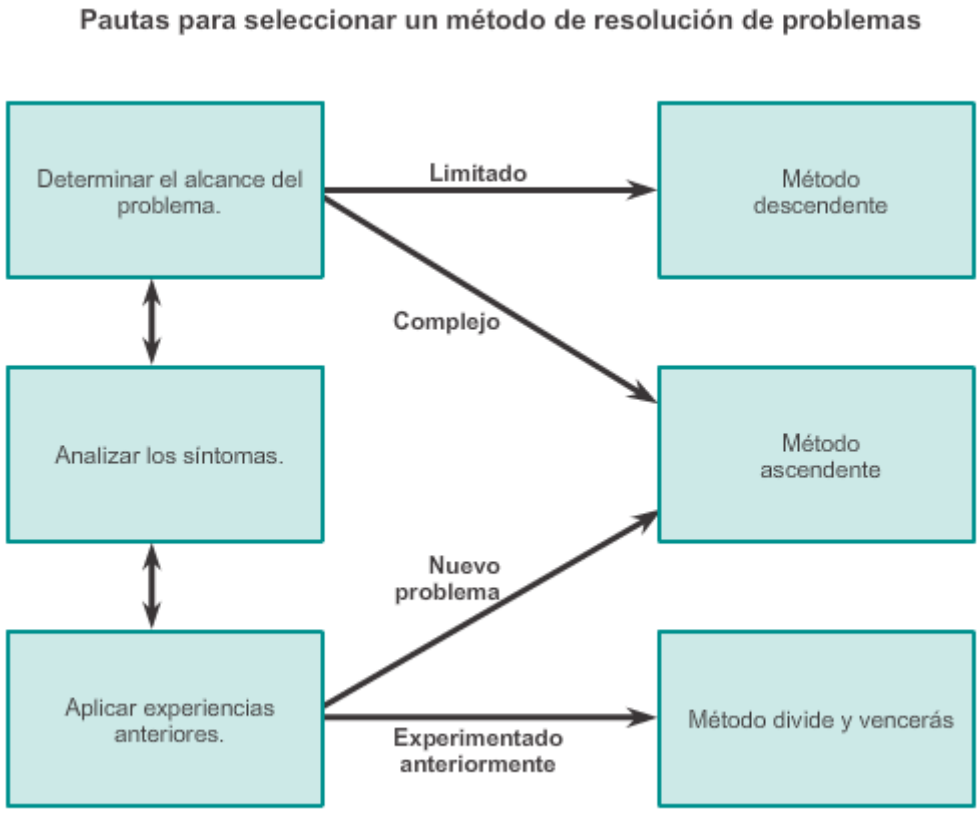
La sustitución es otra metodología rápida de resolución de problemas, que implica cambiar el dispositivo problemático por uno que se sepa que funciona. Si se corrige el problema, el administrador de red sabe que el problema está en el dispositivo que quitó. Si el problema permanece, la causa puede estar en cualquier otro lugar. En situaciones específicas, este puede ser un método ideal para la resolución rápida de un problema, por ejemplo, cuando queda inactivo un único punto de error crítico, como un router de frontera. En vez de resolver el problema, puede resultar más beneficioso reemplazar el dispositivo y restaurar el servicio.

Capítulo 9: Resolución de problemas de red 9.1.3.4 Pautas para seleccionar un método de resolución de problemas

Para resolver rápidamente los problemas de una red, tómese el tiempo para seleccionar el método más eficaz de resolución de problemas de red. En la ilustración, se muestra este proceso.

El siguiente es un ejemplo de cómo elegir un método de resolución de problemas según un problema específico:

Dos routers IP no intercambian información de routing. La última vez que ocurrió este tipo de problema se trató de un problema de protocolo. Por lo tanto, elija el método de resolución de problemas divide y vencerás. Un análisis revela que hay conectividad entre los routers. Comience el proceso de resolución de problemas en la capa física o de enlace de datos. Confirme la conectividad y comience a probar las funciones asociadas con TCP/IP en la capa superior siguiente del modelo OSI, es decir, la capa de red.



Capítulo 9: Resolución de problemas de red 9.1.3.5 Actividad: Métodos de resolución de problemas

Actividad: Métodos de resolución de problemas
Seleccione cuál de las afirmaciones que se incluyen a continuación se asocia a cada uno de los métodos de resolución de problemas.

	Ascendente	Descendente	Divide y vencerás	Prueba y error	Detección de las diferencias	Sustitución
Comienza por una deducción fundamentada sobre en qué capa del modelo OSI se debe iniciar la resolución de problemas.			✓			
Se usa cuando se sospecha que el problema es una falla de cableado o de un dispositivo.	✓					
Se usa para problemas que es probable que abarquen la configuración del software.		✓				
Usa una deducción de resolución de problemas basada en la experiencia para investigar una causa posible.				✓		
Cambia el dispositivo problemático por un dispositivo que se sepa que funciona.						✓
Compara una situación de funcionamiento con una en la que no hay funcionamiento para buscar las diferencias significativas.					✓	

Capítulo 9: Resolución de problemas de red 9.2.1.1 Herramientas para la solución de problemas de software

Para facilitar la resolución de problemas, hay disponible una amplia variedad de herramientas de hardware y software. Estas herramientas se pueden usar para recolectar y analizar los síntomas de los problemas de red. Con frecuencia, proporcionan funciones de monitoreo y generación de informes que se pueden usar para establecer la línea de base de red.

Algunas herramientas para la solución de problemas de software incluyen las siguientes:

Herramientas del sistema de administración de red (NMS)

Las herramientas del sistema de administración de red (NMS) incluyen herramientas de monitoreo en el nivel de los dispositivos, de configuración y de administración de fallas. En la figura 1, se muestra un ejemplo del software NMS “WhatsUp Gold”. Estas herramientas se pueden usar para investigar y corregir los problemas de red. El software de supervisión de red muestra de manera gráfica una vista física de los dispositivos de red, lo que permite a los administradores supervisar los dispositivos remotos sin revisarlos físicamente. El software de administración de dispositivos proporciona datos dinámicos sobre el estado, las estadísticas y la información de configuración de productos conmutados. Algunas otras herramientas de administración de red que se usan frecuentemente son CiscoView, HPBTO Software (antes OpenView) y SolarWinds.

Base de conocimientos

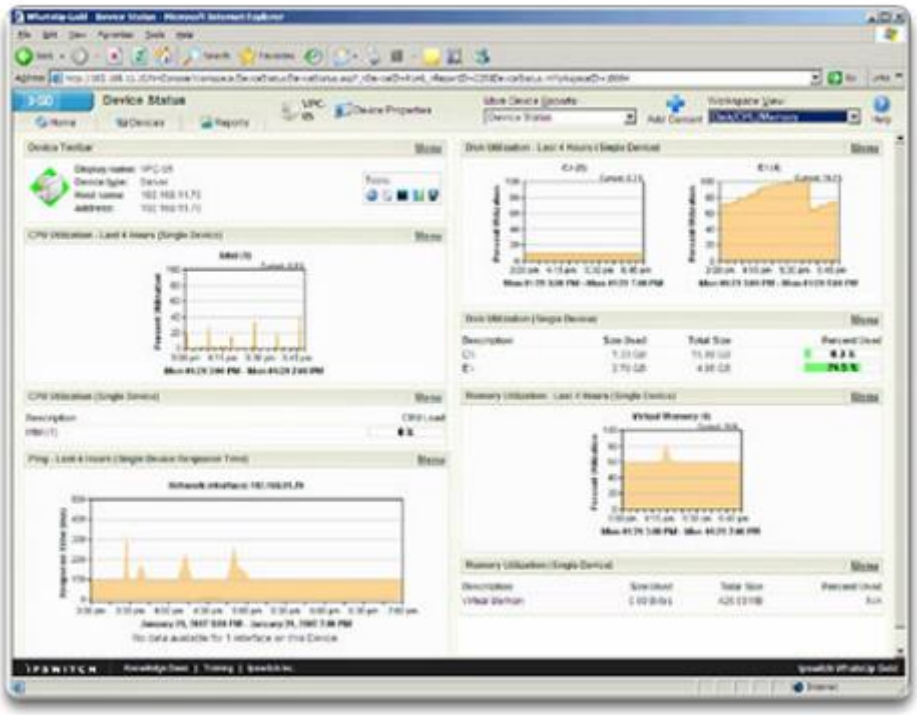
Las bases de conocimientos en línea de los proveedores de dispositivos de red se volvieron fuentes de información indispensables. Cuando las bases de conocimientos de los proveedores se combinan con motores de búsqueda de Internet como Google, los administradores de red tienen acceso a una vasta fuente de información fundada en la experiencia.

En la figura 2, se muestra la página **Tools & Resources** (Herramientas y recursos) de Cisco, que se encuentra enhttp://www.cisco.com. Esta es una herramienta gratuita que proporciona información sobre el hardware y el software relacionados con Cisco. Incluye procedimientos de resolución de problemas, guías de implementación y notas de producto originales sobre la mayoría de los aspectos de la tecnología de red.

Herramientas de línea de base

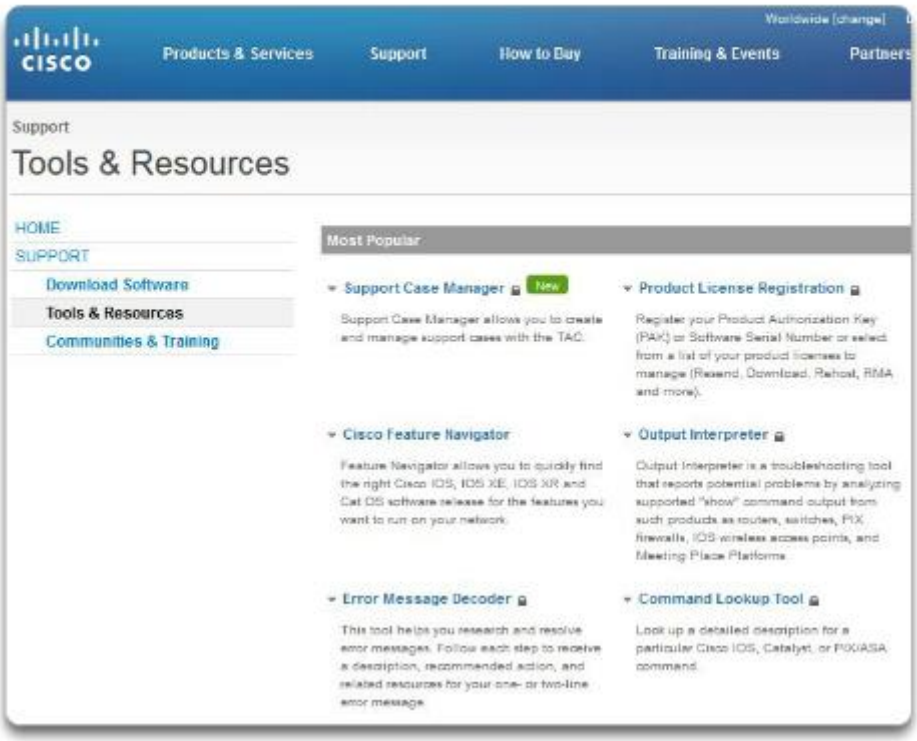
Hay numerosas herramientas disponibles para automatizar la documentación de red y el proceso de línea de base. Estas herramientas están disponibles para los sistemas operativos Windows, Linux y AUX. En la figura 3, se muestra una captura de pantalla de los softwares SolarWinds LANsurveyor y CyberGauge. Las herramientas de establecimiento de línea de base ayudan con las tareas de registro frecuentes. Por ejemplo, pueden generar diagramas de red, ayudar a conservar actualizado el registro del software y el hardware de una red y ayudar a medir de forma rentable la línea de base de uso de ancho de banda de la red.

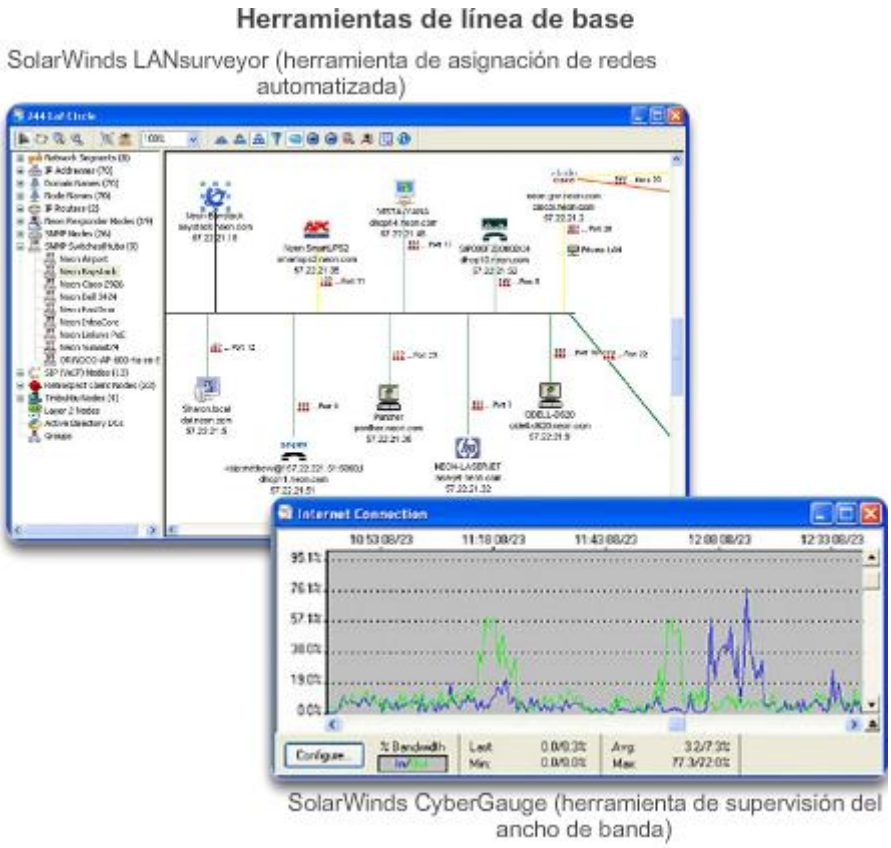
Sistema de administración de red



Pantalla de estado de dispositivos del NMS "WhatsUp Gold"

Herramientas y recursos





Capítulo 9: Resolución de problemas de red 9.2.1.2 Herramientas para la solución de problemas de software (cont.)

Analizadores de protocolos basados en host

Un analizador de protocolos decodifica las diversas capas del protocolo en una trama registrada y presenta esa información en un formato relativamente fácil de usar. En la ilustración, se muestra una captura de pantalla del analizador de protocolos Wireshark. Los analizadores de protocolos muestran información sobre los componentes físicos, los enlaces de datos y el protocolo, así como descripciones para cada trama. La mayoría de los analizadores de protocolos pueden filtrar el tráfico que cumple con ciertos criterios, por ejemplo, se puede captar todo el tráfico hacia y desde un dispositivo determinado. Los analizadores de protocolos como Wireshark pueden ayudar a resolver problemas de rendimiento de la red. Es importante tener un buen nivel de conocimiento sobre cómo usar el analizador de protocolos y TCP/IP. Para adquirir más conocimientos y habilidades relacionados con el uso de Wireshark, un excelente recurso eshttp://www.wiresharkbook.com.

Captura de paquetes integrada del IOS de Cisco

La captura de paquetes integrada (EPC) del IOS de Cisco constituye una potente herramienta de rastreo y resolución de problemas. Esta característica permite que los administradores de red capturen los paquetes IPv4 e IPv6 que circulan hacia y desde un router Cisco, así como a través de él. La característica EPC del IOS de Cisco se usa principalmente en situaciones de

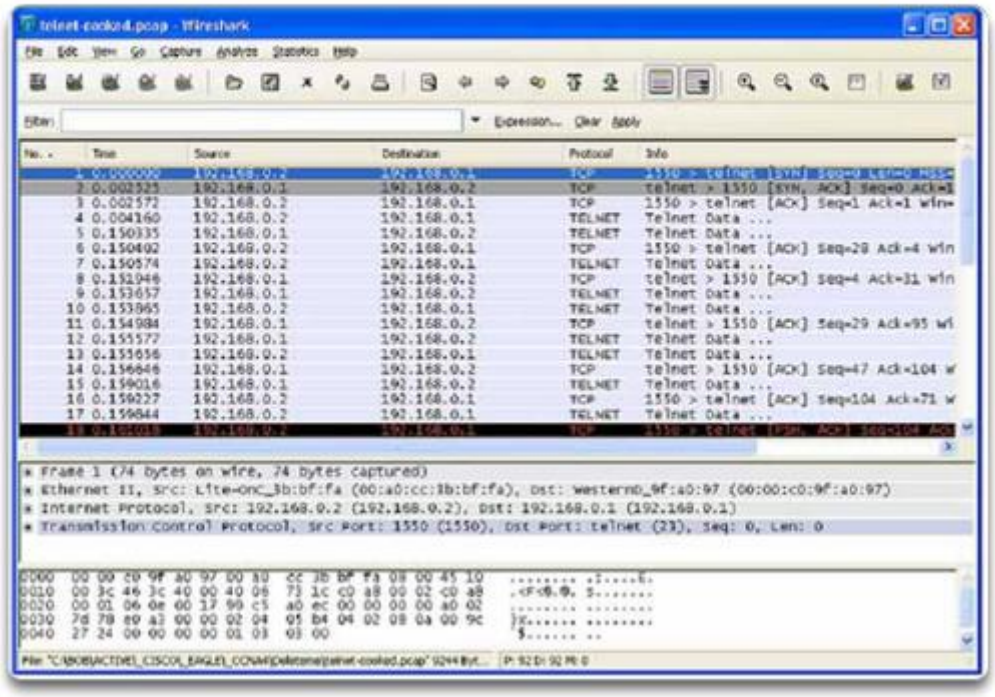
resolución de problemas en las que es útil ver los datos que se envían desde o hacia el dispositivo de red, o a través de él.

Por ejemplo, el personal de soporte técnico necesita establecer por qué un dispositivo determinado no puede acceder a la red o a alguna aplicación. Para detectar el problema, es probable que sea necesario realizar capturas de los paquetes de datos IP y examinarlos. Otro ejemplo consistiría en determinar la firma del atacante en una amenaza de red o una infracción de seguridad del sistema de servidores. EPC del IOS de Cisco puede ayudar a capturar los paquetes que circulan hacia la red en el origen o en el perímetro.

EPC del IOS de Cisco es útil siempre que se puede usar un analizador de protocolos de red para depurar un problema pero no resulta práctico instalar un dispositivo tal.

Para obtener más información sobre el uso y la configuración de EPC de Cisco, consulte la Guía de configuración de la captura de paquetes integrada.

Analizador de protocolos Wireshark



Capítulo 9: Resolución de problemas de red 9.2.1.3 Herramientas para la solución de problemas de hardware

Algunas herramientas para la solución de problemas de hardware incluyen las siguientes:

- **Módulo de análisis de redes:** como se muestra en la figura 1, se puede instalar un módulo de análisis de redes (NAM) en los switches Cisco Catalyst de la serie 6500 y los routers Cisco de la serie 7600. Los NAM proporcionan 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 los recursos de red fundamentales. Además, el NAM puede capturar y decodificar paquetes y rastrear los tiempos de respuesta para localizar un problema de aplicación en la red o el servidor.

- **Multímetros digitales:** los multímetros digitales (DMM), por ejemplo, el Fluke 179 que se muestra en la figura 2, son instrumentos de prueba que se usan para medir directamente los valores eléctricos de voltaje, corriente y resistencia. En la resolución de problemas de red, la mayoría de las pruebas multimedia implican revisar los niveles de voltaje de la fuente de alimentación y verificar que los dispositivos de red reciban energía.

- **Comprobadores de cables:** son dispositivos de mano especializados que están diseñados para probar los diversos tipos de cables de comunicación de datos. En la figura 3, se muestran dos comprobadores de cables Fluke diferentes. Los comprobadores de cables se pueden usar para detectar hilos dañados, hilos cruzados, conexiones en cortocircuito y pares de conexiones incorrectos. Estos dispositivos pueden ser económicos comprobadores de continuidad, comprobadores de cables de datos de precio moderado o costosos reflectómetros de dominio de tiempo (TDR). Los TDR se usan para identificar la distancia a una ruptura en un cable. Estos dispositivos envían señales a lo largo del cable y esperan a que estas se reflejen. El tiempo entre el envío y la recepción de la señal se convierte en una medida de distancia. Normalmente, la función de TDR viene incluida en los comprobadores de cables de datos. Los TDR que se usan para probar los cables de fibra óptica se conocen como “reflectómetros ópticos de dominio de tiempo” (OTDR).

- **Analizadores de cables:** los analizadores de cables, como el analizador de cable Fluke DTX que se muestra en la figura 4, son dispositivos de mano con varias funciones que se usan para probar y para certificar los cables de cobre y fibra para los diferentes servicios y estándares. Las herramientas más sofisticadas incluyen un diagnóstico avanzado de resolución de problemas que mide la distancia al defecto de rendimiento (NEXT, RL), identifica las acciones correctivas y muestra gráficamente el comportamiento de crosstalk e impedancia. Los analizadores de cables también suelen incluir software basado en computadora. Después de que se recolectan los datos de campo, el dispositivo de mano puede subir los datos para crear informes actualizados.

- **Analizadores de red portátiles:** los dispositivos portátiles, como Fluke OptiView en la figura 5, se usan para resolver problemas en redes conmutadas y VLAN. Al conectar el analizador de red en cualquier parte de la red, un ingeniero de red puede ver el puerto de switch al que se conecta el dispositivo, así como el uso promedio y el uso pico. El analizador también se puede usar para conocer la configuración de la VLAN, identificar los participantes principales de la red, analizar el tráfico de la red y ver los detalles de la interfaz. Para un análisis y una resolución de problemas más profundos, el dispositivo conectarse a una computadora que tenga instalado un software de supervisión de red.

Capítulo 9: Resolución de problemas de red 9.2.1.4 Resolución de problemas con un servidor de syslog

Syslog es un protocolo simple que un dispositivo IP, conocido como “cliente syslog”, usa para enviar mensajes de registro basados en texto a otro dispositivo IP, el servidor de syslog. Actualmente, Syslog se define en RFC 5424.

Implementar una instalación de registro es una parte importante de la seguridad y la resolución de problemas de red. Los dispositivos de Cisco pueden registrar información relacionada con cambios de configuración, infracciones de ACL, estado de interfaces y muchos otros tipos de eventos. Los dispositivos de Cisco pueden enviar mensajes de registro a varias instalaciones. Los mensajes de eventos se pueden enviar a uno o varios de los siguientes componentes:

- **Consola:** el registro de la consola está activado de manera predeterminada. Los mensajes se registran en la consola y se pueden ver al modificar o probar el router o el switch mediante el software de emulación de terminal, mientras se esté conectado al puerto de consola del router.

- **Líneas de las terminales:** las sesiones de EXEC habilitadas se pueden configurar para recibir mensajes de registro en cualquiera de las líneas de las terminales. De manera similar al registro de la consola, el router no almacena este tipo de registro y, por lo tanto, solo es valioso para el usuario en esa línea.

- **Registro almacenado en búfer:** este registro es un poco más útil como herramienta de resolución de problemas porque los mensajes de registro se almacenan en la memoria durante cierto tiempo. Sin embargo, cuando se reinicia el dispositivo, se borran los mensajes de registro.

- **Traps de SNMP:** ciertos umbrales se pueden configurar previamente en los routers y otros dispositivos. El router puede procesar los eventos de router, como superar un umbral, y reenviarlos como traps de SNMP a un servidor SNMP externo. Las traps de SNMP son una instalación de registro de seguridad viable, pero requieren la configuración y el mantenimiento de un sistema SNMP.

- **Syslog:** los routers y los switches Cisco se pueden configurar para reenviar mensajes de registro a un servicio de syslog externo. Este servicio puede residir en cualquier número de servidores o estaciones de trabajo, incluidos los sistemas basados en Microsoft Windows y Linux. Syslog es la instalación de registro de mensajes más popular, ya que proporciona capacidades de almacenamiento de registro a largo plazo y una ubicación central para todos los mensajes del router.

Los mensajes de registro del IOS de Cisco se ubican en uno de ocho niveles, como se muestra en la figura 1. Cuanto menor es el número del nivel, mayor es el nivel de gravedad. De manera predeterminada, todos los mensajes del nivel 0 al 7 se registran en la consola. Si bien la capacidad para ver los registros en un servidor central de syslog es útil para resolver problemas, examinar una gran cantidad de datos puede ser una tarea abrumadora. El comando**logging trap** *level* limita los mensajes registrados en el servidor de syslog según la gravedad. El nivel es el nombre o el número del *level* de gravedad. Solo se registran los mensajes iguales o numéricamente inferiores al *level*especificado.

En el ejemplo de la figura 2, los mensajes de sistema del nivel 0 (emergencias) al 5 (notificaciones) se envían al servidor de syslog en 209.165.200.225.

Niveles de gravedad

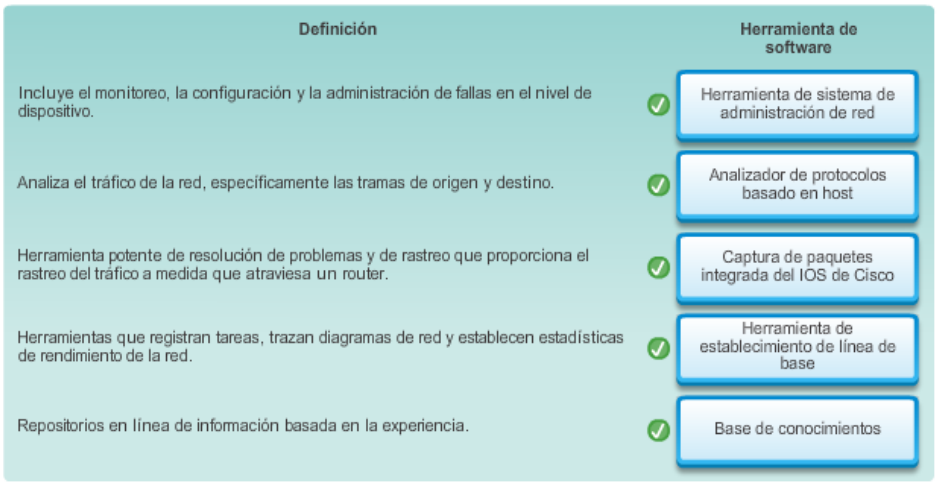
	Nivel	Palabra clave	Descripción	Definición
Nivel más alto	0	emergencias	No se puede utilizar el sistema.	LOG_EMERG
	1	alertas	Se necesita una acción inmediata.	LOG_ALERT
	2	crítico	Existen condiciones críticas.	LOG_CRIT
	3	errores	Existen condiciones de error.	LOG_ERR
	4	advertencias:	Existen condiciones de advertencia.	LOG_WARNING
	5	notificaciones	Condición normal pero importante.	LOG_NOTICE
	6	informativo	Solo mensajes informativos.	LOG_INFO
Nivel más bajo	7	depuración	Mensajes de depuración	LOG_DEBUG

Limitación de los mensajes enviados al servidor de syslog

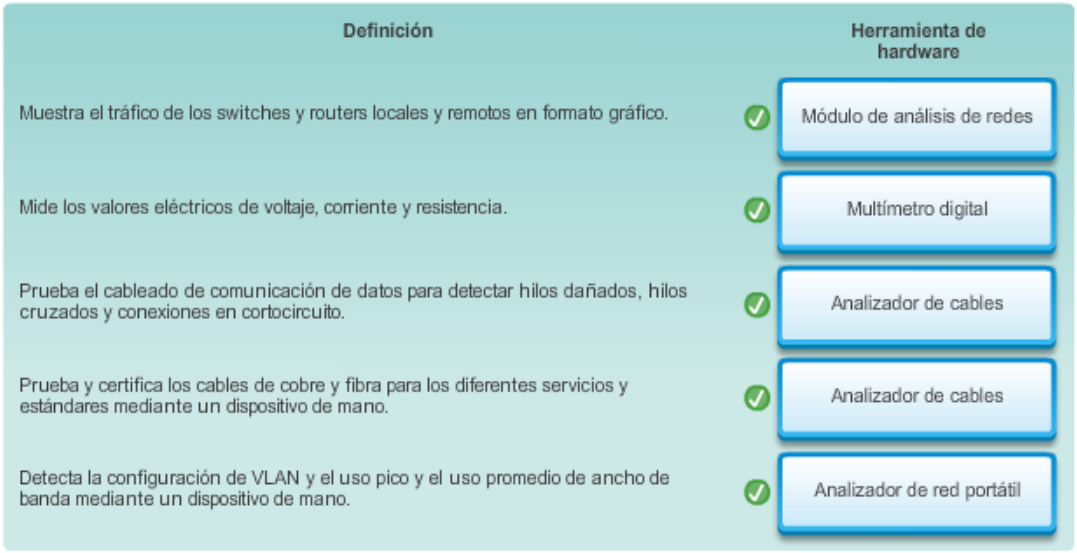
```
R1(config)# logging host 209.165.200.225
R1(config)# logging trap notifications
R1(config)# logging on
```

Capítulo 9: Resolución de problemas de red 9.2.1.5 Actividad: Identificar herramientas comunes de resolución de problemas

Actividad: Herramientas para la solución de problemas de software (parte 1)
Una cada herramienta para la solución de problemas de software con su definición. Haga clic en el botón 2 para continuar la actividad.



Actividad: Herramientas para la solución de problemas de hardware (parte 2)
Una cada herramienta para la solución de problemas de hardware con su definición.



Capítulo 9: Resolución de problemas de red 9.2.2.1 Resolución de problemas de la capa física

La capa física transmite bits desde una computadora a otra y regula la transmisión de un flujo de bits a través del medio físico. La capa física es la única con propiedades físicamente tangibles, como cables, tarjetas y antenas.

Los problemas en una red con frecuencia se presentan como problemas de rendimiento. Los problemas de rendimiento indican que existe una diferencia entre el comportamiento esperado y el comportamiento observado y que el sistema no funciona como se podría esperar razonablemente. Las fallas y las condiciones por debajo del nivel óptimo en la capa física no solo presentan inconvenientes para los usuarios sino que pueden afectar la productividad de toda la empresa. Las redes en las que se dan estos tipos de condiciones por lo general se desactivan. Dado que las capas superiores del modelo OSI dependen de la capa física para

funcionar, el administrador de red debe tener la capacidad de aislar y corregir los problemas en esta capa de manera eficaz.

Los síntomas frecuentes de los problemas de red en la capa física incluyen los siguientes:

- **Rendimiento inferior a la línea de base:** las razones más frecuentes de un rendimiento lento o deficiente incluyen servidores sobrecargados o con alimentación insuficiente, configuraciones de router o switch inadecuadas, congestión del tráfico en un enlace de baja capacidad y pérdida crónica de tramas.

- **Pérdida de la conectividad:** si un cable o un dispositivo fallan, el síntoma más evidente es una pérdida de la conectividad entre los dispositivos que se comunican a través de ese enlace o con el dispositivo o la interfaz que presenta la falla. Esto se indica por medio de una simple prueba de ping. La pérdida intermitente de la conectividad puede indicar una conexión floja u oxidada.

- **Cuellos de botella o congestión de la red:** si un router, una interfaz o un cable fallan, es probable que los protocolos de routing redirijan el tráfico hacia otras rutas que no estén diseñadas para transportar la capacidad adicional. Esto puede provocar congestión o cuellos de botella en esas partes de la red.

- **Tasas de uso de CPU elevadas:** las tasas de uso de CPU elevadas son un síntoma de que un dispositivo, como un router, un switch o un servidor, funciona en el límite admitido por su diseño o lo supera. Si no se aborda rápidamente, la sobrecarga de CPU puede ocasionar que un dispositivo falle o se desactive.

- **Mensajes de error de la consola:** los mensajes de error que se muestran en la consola de un dispositivo indican un problema de la capa física.

Los incidentes que comúnmente causan problemas de red en la capa física incluyen los siguientes:

- **Problemas relacionados con la alimentación:** estos son el motivo principal de una falla de la red. Además, debe revisarse el funcionamiento de los ventiladores y asegurarse de que los orificios de entrada y salida de ventilación del bastidor no estén obstruidos. Si en otras unidades cercanas también se produce una pérdida de potencia, considere la posibilidad de que haya un corte de energía en la fuente de alimentación principal.

- **Fallas de hardware:** las tarjetas de interfaz de red (NIC) defectuosas pueden ser la causa de errores de transmisión de la red debido a colisiones tardías, tramas cortas y jabber. Con frecuencia, “jabber” se define como la condición en la que un dispositivo de red transmite continuamente datos aleatorios, sin sentido, a la red. Otras causas probables de jabber son archivos de controlador de la NIC defectuosos o dañados, cables defectuosos o problemas de conexión a tierra.

- **Fallas del cableado:** se pueden corregir numerosos problemas simplemente por medio de volver a asentar cables que se desconectaron de manera parcial. Al realizar una inspección física, busque cables dañados, tipos de cables inadecuados y RJ-45 con engarces deficientes. Los cables sospechosos se deben probar o cambiar por un cable que se sepa que funcione.

- **Atenuación:** la atenuación puede ocurrir cuando la longitud de un cable supera el límite de diseño para los medios o cuando hay una conexión deficiente que se debe a un cable

flojo o a contactos sucios u oxidados. Si la atenuación es grave, el dispositivo receptor no siempre puede distinguir entre sí los bits que componen el flujo correctamente.

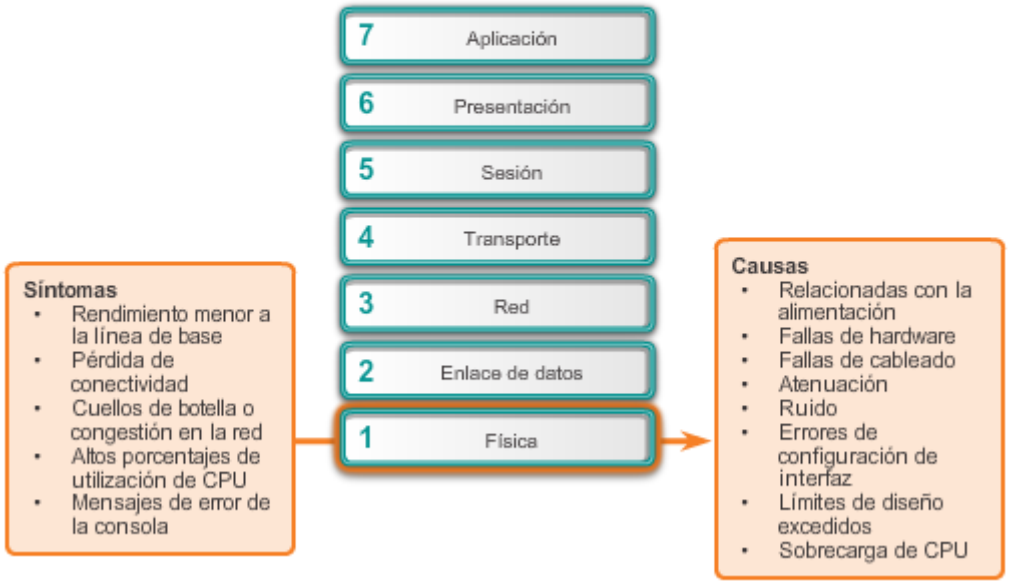
- **Ruido:** la interferencia electromagnética (EMI) local se conoce comúnmente como “ruido”. El ruido se puede generar a partir de muchas fuentes, como estaciones de radio FM, radio de la policía, seguridad de edificios, aviónica para aterrizaje automático, crosstalk (ruido inducido por otros cables en la misma ruta o por cables adyacentes), cables eléctricos cercanos, dispositivos con motores eléctricos grandes o cualquier elemento que cuente con un transmisor más potente que el de un teléfono celular.

- **Errores de configuración de la interfaz:** muchos elementos se pueden configurar incorrectamente en una interfaz y ocasionar que se desactive, por ejemplo, una frecuencia de reloj incorrecta, un origen de reloj incorrecto y que la interfaz no esté encendida. Esto provoca la pérdida de la conectividad a los segmentos de red conectados.

- **Límites de diseño excedidos:** un componente puede operar de manera deficiente en la capa física porque se usa a una tasa promedio superior a la que está configurado para funcionar. Al resolver este tipo de problema, es evidente que los recursos del dispositivo funcionan a la capacidad máxima, o cerca de ella, y hay un aumento en el número de errores de interfaz.

- **Sobrecarga de CPU:** los síntomas incluyen procesos con porcentajes elevados de uso de CPU, descartes de la cola de entrada, rendimiento lento, lentitud o falta de respuesta de los servicios de router como Telnet y ping o falta de actualizaciones de routing. Una de las causas de sobrecarga de CPU en un router es un volumen de tráfico elevado. Si algunas interfaces están regularmente sobrecargadas con tráfico, considere rediseñar el flujo de tráfico en la red o actualizar el hardware.

Síntomas y causas de la capa física



Capítulo 9: Resolución de problemas de red 9.2.2.2 Resolución de problemas de la capa de enlace de datos

La resolución de problemas de capa 2 puede ser un proceso desafiante. La configuración y el funcionamiento de estos protocolos son fundamentales para crear redes con ajustes precisos y en condiciones de funcionamiento. Los problemas de capa 2 causan síntomas específicos que, al reconocerse, ayudan a identificar el problema rápidamente.

Los síntomas frecuentes de los problemas de red en la capa de enlace de datos incluyen los siguientes:

- **Falta de funcionalidad o conectividad en la capa de red o en las capas superiores:** algunos problemas de capa 2 pueden detener el intercambio de tramas a través de un enlace, mientras que otros solo provocan un deterioro del rendimiento de la red.

- **Funcionamiento de la red por debajo de los niveles de rendimiento de línea de base:** en una red, pueden ocurrir dos tipos de funcionamiento deficiente en la capa 2. En primer lugar, que las tramas elijan una ruta deficiente al destino, pero lleguen. En este caso, la red podría experimentar un uso de ancho de banda elevado en enlaces que no deberían tener ese nivel de tráfico. En segundo lugar, que se descarten algunas tramas. Estos problemas se pueden identificar mediante las estadísticas del contador de errores y los mensajes de error de la consola en el switch o el router. En un entorno Ethernet, un ping extendido o continuo también revela si se descartan tramas.

- **Difusiones excesivas:** los sistemas operativos usan difusiones y multidifusiones ampliamente para detectar los servicios de red y otros hosts. Por lo general, las difusiones excesivas son el resultado de una de las siguientes situaciones: aplicaciones programadas o configuradas incorrectamente, grandes dominios de difusión de capa 2 o problemas de red subyacentes, como bucles de STP o rutas inestables.

- **Mensajes de la consola:** a veces, un router reconoce que se produjo un problema de capa 2 y envía mensajes de alerta a la consola. Generalmente, un router hace esto cuando detecta un problema con la interpretación de las tramas entrantes (problemas de encapsulación o entramado) o cuando se esperan keepalives pero no llegan. El mensaje de la consola más común que indica que existe un problema de Capa 2 es un mensaje que indica que el protocolo de línea está desactivado.

Los problemas en la capa de enlace de datos que con frecuencia provocan problemas de conectividad o rendimiento de la red incluyen los siguientes:

- **Errores de encapsulación:** un error de encapsulación ocurre porque los bits que el emisor coloca en un campo determinado no son los que el receptor espera ver. Esta condición se produce cuando la encapsulación en un extremo de un enlace WAN está configurada de manera diferente de la encapsulación que se usa en el otro extremo.

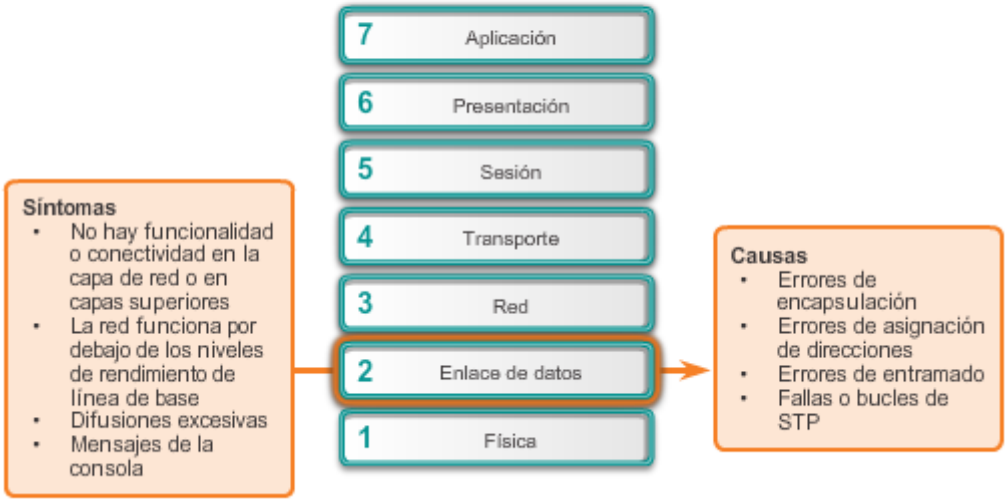
- **Errores de asignación de direcciones:** en las topologías, como punto a multipunto, Frame Relay o Ethernet de difusión, es fundamental darle a la trama una dirección de destino de capa 2 correcta. Esto asegura su llegada al destino correcto. Para lograr esto, el dispositivo de red debe encontrar la coincidencia entre una dirección de destino de

capa 3 y la dirección de capa 2 correcta mediante mapas estáticos o dinámicos. En un entorno dinámico, la asignación de información de capa 2 y capa 3 puede fallar debido a que los dispositivos pueden estar configurados de manera específica para no responder a las solicitudes de ARP o de ARP inverso, a que la información de capa 2 y capa 3 almacenada en caché puede haber cambiado físicamente o a que se reciben respuestas de ARP no válidas debido a una configuración incorrecta o un ataque de seguridad.

- **Errores de entramado:** las tramas generalmente operan en grupos de bytes de 8 bits. Cuando una trama no termina en un límite de bytes de 8 bits, se produce un error de entramado. Cuando sucede esto, el receptor puede tener problemas para determinar dónde termina una trama y dónde comienza la otra. Un número excesivo de tramas no válidas puede impedir el intercambio de keepalives válidos. Los errores de entramado pueden ser el resultado de una línea serial ruidosa, un cable diseñado de manera incorrecta (demasiado largo o blindado en forma inadecuada) o un reloj de línea de unidad de servicio de canal (CSU) configurado de manera incorrecta.

- **Fallas o bucles de STP:** el objetivo del protocolo de árbol de expansión (STP) es convertir 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 el reenvío de bucles, que se produce cuando no se bloquean puertos en una topología redundante y el tráfico se reenvía en círculos indefinidamente, lo que implica una saturación excesiva provocada por una tasa elevada de cambios en la topología STP. En una red configurada correctamente, un cambio de topología debería ser un evento inusual. Cuando un enlace entre dos switches se activa o se desactiva, llegado el momento se produce un cambio de topología cuando el estado de STP del puerto cambia por hacia reenvío o desde reenvío. Sin embargo, cuando un puerto es inestable (oscila entre los estados activo y inactivo), provoca cambios de topología repetitivos y saturación, u ocasiona la convergencia lenta o reiterada de STP. Esto puede ser el resultado de una incompatibilidad entre la topología real y la topología registrada, un error de configuración, como una configuración incoherente de los temporizadores de STP, una sobrecarga de CPU de switch durante la convergencia o un defecto de software.

Síntomas y causas de la capa de enlace de datos



Capítulo 9: Resolución de problemas de red 9.2.2.3 Resolución de problemas de la capa de red

Los problemas de la capa de red incluyen cualquier problema que comprenda a un protocolo de capa 3, ya sea un protocolo de routing (como IPv4 o IPv6) o un protocolo de routing (como EIGRP, OSPF, entre otros).

Los síntomas frecuentes de los problemas de red en la capa de red incluyen los siguientes:

- **Falla de red:** una falla de red se produce cuando esta no funciona o funciona parcialmente, lo que afecta a todos los usuarios y a todas las aplicaciones en la red. Los usuarios y los administradores de red normalmente detectan estas fallas en seguida, las que sin dudas son fundamentales para la productividad de la empresa.

- **Rendimiento por debajo del nivel óptimo:** los problemas de optimización de la red por lo general comprenden a un subconjunto de usuarios, aplicaciones, destinos o un determinado tipo de tráfico. Es difícil detectar los problemas de optimización, y es incluso más difícil aislarlos y diagnosticarlos. Esto generalmente se debe a que estos problemas abarcan varias capas o, incluso, al equipo host. Puede llevar tiempo determinar que el problema se encuentra en la capa de red.

En la mayoría de las redes, se usan rutas estáticas junto con protocolos de routing dinámico. La configuración incorrecta de las rutas estáticas puede provocar un routing deficiente. En algunos casos, las rutas estáticas configuradas incorrectamente pueden generar bucles de routing que hacen que algunas partes de la red se vuelvan inalcanzables.

La resolución de problemas de protocolos de routing dinámico requiere una comprensión profunda de cómo funciona el protocolo de routing específico. Algunos problemas son comunes a todos los protocolos de routing, mientras que otros son específicos de un protocolo de routing particular.

No existe una única plantilla para resolver problemas de capa 3. Los problemas de routing se resuelven con un proceso metódico, por medio de una serie de comandos para aislar y diagnosticar el problema.

Las siguientes son algunas áreas que se deben explorar al diagnosticar un posible problema que involucre protocolos de routing:

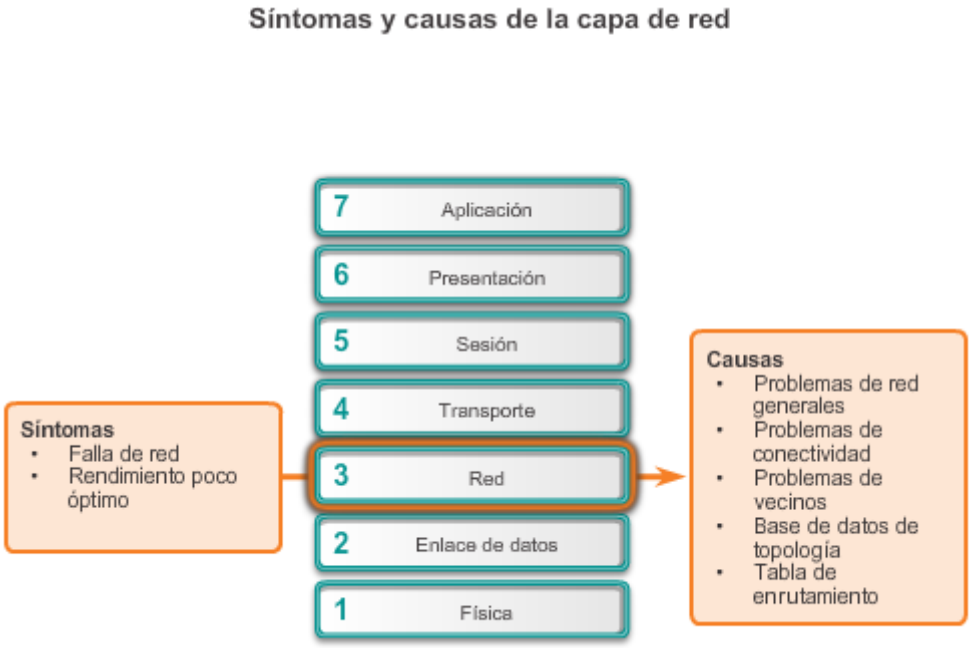
- **Problemas de red generales:** con frecuencia, un cambio en la topología, como un enlace inactivo, puede tener efectos en otras áreas de la red que tal vez no sean evidentes en ese momento. Esto puede implicar instalar nuevas rutas, estáticas o dinámicas, o eliminar otras. Determine si algún elemento de la red cambió de manera reciente y si hay alguna persona trabajando en la infraestructura de la red en ese momento.

- **Problemas de conectividad:** revise si existe algún problema de conectividad o en los equipos, incluidos problemas de alimentación como cortes de energía y problemas ambientales (por ejemplo, recalentamiento). También revise si hay problemas de capa 1, como problemas de cableado, puertos defectuosos y problemas del ISP.

- **Problemas de vecinos:** si el protocolo de routing establece una adyacencia con un vecino, revise si hay algún problema con los routers en lo que respecta a la formación de adyacencias de vecinos.

- **Base de datos de topología:** si el protocolo de routing usa una tabla o base de datos de topología, revíselas para ver si existe algo inesperado, como entradas faltantes o imprevistas.

- **Tabla de routing:** revise la tabla de routing para ver si existe algo inesperado, como rutas faltantes o imprevistas. Use los comandos **debug**para ver las actualizaciones de routing y el mantenimiento de la tabla de routing.



Capítulo 9: Resolución de problemas de red 9.2.2.4 Resolución de problemas de la capa de transporte: ACL

Los problemas de red pueden surgir a partir de problemas de la capa de transporte en el router, especialmente en el perímetro de la red, donde se examina y se modifica el tráfico. Dos de las tecnologías de capa de transporte que se implementan con más frecuencia son las listas de control de acceso (ACL) y la traducción de direcciones de red (NAT), que se muestran en la figura 1.

La mayoría de los problemas frecuentes con las ACL se debe a una configuración incorrecta, como se muestra en la figura 2. Los problemas con las ACL pueden provocar fallas en sistemas que, por lo demás, funcionan correctamente. Comúnmente, las configuraciones incorrectas ocurren en varias áreas:

- **Selección del flujo de tráfico:** la configuración incorrecta del router más frecuente es aplicar la ACL al tráfico incorrecto. El tráfico se define por la interfaz del router a través de la que viaja y el sentido en el que viaja. Para que funcione de manera adecuada, se debe aplicar la ACL a la interfaz correcta y se debe seleccionar el sentido de tráfico apropiado.

- **Orden de entradas de control de acceso:** el orden de las entradas en una ACL debe ir de lo específico a lo general. Si bien una ACL puede tener una entrada para permitir

específicamente un flujo de tráfico en particular, los paquetes nunca coincidirán con esa entrada si una entrada anterior en la lista ya los rechazó. Si el router ejecuta las ACL y la NAT, es importante el orden en que se aplica cada una de estas tecnologías a un flujo de tráfico. La ACL de entrada procesa el tráfico entrante antes de que lo procese la NAT de afuera hacia dentro. La ACL de salida procesa el tráfico saliente después de que lo procesa la NAT de adentro hacia fuera.

- **Instrucción implícita de denegar todo el tráfico:** cuando no se requiere un nivel de seguridad elevado en la ACL, este elemento implícito de control de acceso puede ser la causa de una configuración incorrecta de la ACL.

- **Direcciones y máscaras wildcard IPv4:** las máscaras wildcard IPv4 complejas proporcionan mejoras importantes en términos de eficiencia, pero están más sujetas a errores de configuración. Un ejemplo de una máscara wildcard compleja consiste en usar la dirección IPv4 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 10.0.32.0.

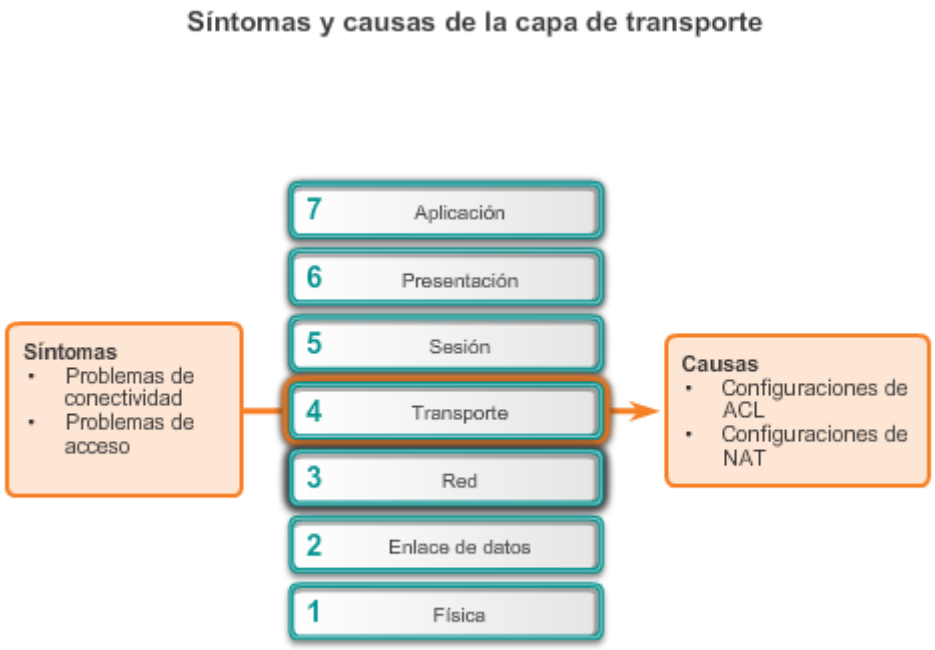
- **Selección del protocolo de la capa de transporte:** al configurar las ACL, es importante que se especifiquen solo los protocolos de la capa de transporte correctos. Cuando no están seguros de si un flujo de tráfico determinado usa un puerto TCP o un puerto UDP, muchos administradores de red configuran ambos. Especificar ambos puertos provoca una abertura a través del firewall, lo que posibilita a los intrusos un camino dentro la red. También introduce un elemento adicional en la ACL, de modo que el procesamiento de esta toma más tiempo, lo que imprime mayor latencia a las comunicaciones de la red.

- **Puertos de origen y destino:**controlar el tráfico entre dos hosts de manera adecuada requiere elementos simétricos de control de acceso para las ACL de entrada y de salida. La información de dirección y de puerto del tráfico generado por un host que responde es el reflejo de la información de dirección y puerto del tráfico generado por el host de origen.

- **Uso de la palabra claveestablished:** la palabra clave**established** aumenta la seguridad que se proporciona mediante una ACL. Sin embargo, si la palabra clave se aplica incorrectamente, pueden tener lugar resultados imprevistos.

- **Protocolos poco frecuentes:** las ACL configuradas incorrectamente suelen causar problemas en protocolos distintos de TCP y UDP. Los protocolos poco frecuentes que están ganando popularidad son VPN y los protocolos de cifrado.

La palabra clave **log** es un comando útil para ver la operación de las ACL en las entradas de ACL. Esta palabra clave le ordena al router que coloque una entrada en el registro del sistema cada vez que haya una coincidencia con esa condición de entrada. El evento registrado incluye los detalles del paquete que coincidió con el elemento de la ACL. La palabra clave **log**es especialmente útil para resolver problemas y también proporciona información sobre los intentos de intrusión que la ACL bloquea.



Capítulo 9: Resolución de problemas de red 9.2.2.5 Resolución de problemas de la capa de transporte: NAT para IPv4

Existen varios problemas con la NAT, como la falta de interacción con servicios como DHCP y tunneling. Estos pueden incluir la configuración incorrecta de la NAT interna, la NAT externa o la ACL. Otros problemas incluyen interoperabilidad con otras tecnologías de red, especialmente con aquellas que contienen o derivan información de direccionamiento de red del host en el paquete. Algunas de estas tecnologías incluyen las siguientes:

- **BOOTP y DHCP:** ambos protocolos administran la asignación automática de direcciones IPv4 a los clientes. Recuerde que el primer paquete que un nuevo cliente envía es un paquete IPv4 de difusión de solicitud de DHCP. El paquete de solicitud de DHCP tiene la dirección IPv4 de origen 0.0.0.0. Debido a que la NAT requiere direcciones IPv4 de origen y de destino válidas, BOOTP y DHCP pueden tener dificultades para operar a través de un router que ejecuta una NAT estática o dinámica. La configuración de la característica de aplicación auxiliar IPv4 puede contribuir a la resolución de este problema.

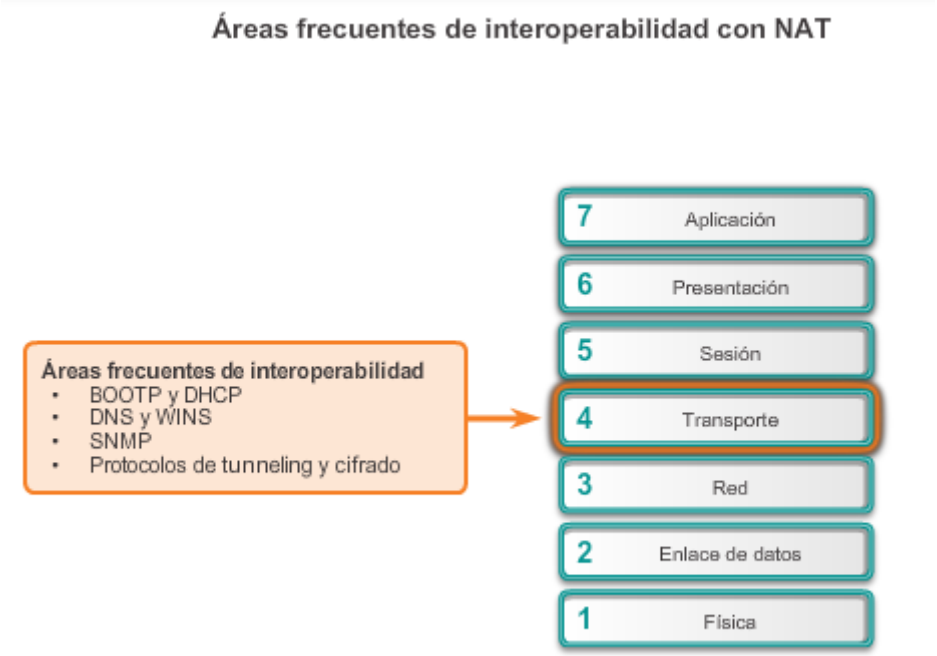
- **DNS y WINS:** debido a que un router que ejecuta una NAT dinámica cambia la relación entre las direcciones internas y externas periódicamente, a medida que las entradas de la tabla se vencen y se vuelven a crear, un servidor DNS o WINS fuera del router NAT no tiene una representación precisa de la red dentro del router. La configuración de la característica de aplicación auxiliar IPv4 puede contribuir a la resolución de este problema.

- **SNMP:** de manera similar a los paquetes DNS, la NAT no puede alterar la información de direccionamiento almacenada en el contenido de datos del paquete. Debido a esto, es posible que una estación de administración SNMP en un lado de un router NAT no pueda comunicarse con los agentes SNMP del otro lado del router NAT. La configuración de la

característica de aplicación auxiliar IPv4 puede contribuir a la resolución de este problema.

- **Protocolos de cifrado y tunneling:**los protocolos de cifrado y tunneling suelen requerir que el tráfico se origine en un puerto UDP o TCP específico o usan 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 routing genérico usados por las implementaciones de VPN.

Nota: el router puede reenviar DHCPv6 de un cliente IPv6 mediante el comando **ipv6 dhcp relay**.



Capítulo 9: Resolución de problemas de red 9.2.2.6 Resolución de problemas de la capa de aplicación

La mayoría de los protocolos de la capa de aplicación proporcionan servicios para los usuarios. Los protocolos de la capa de aplicación normalmente se usan para la administración de red, la transferencia de archivos, los servicios de archivos distribuidos, la emulación de terminal y el correo electrónico. Con frecuencia, se agregan nuevos servicios para usuarios, como VPN y VoIP.

En la ilustración, se muestran los protocolos de capa de aplicación de TCP/IP más conocidos e implementados, que incluyen los siguientes:

- **SSH/Telnet:** permite a los usuarios establecer conexiones de sesión de terminal a los hosts remotos.

- **HTTP:** admite el intercambio de texto, gráficos, sonido, video y otros archivos multimedia en la Web.

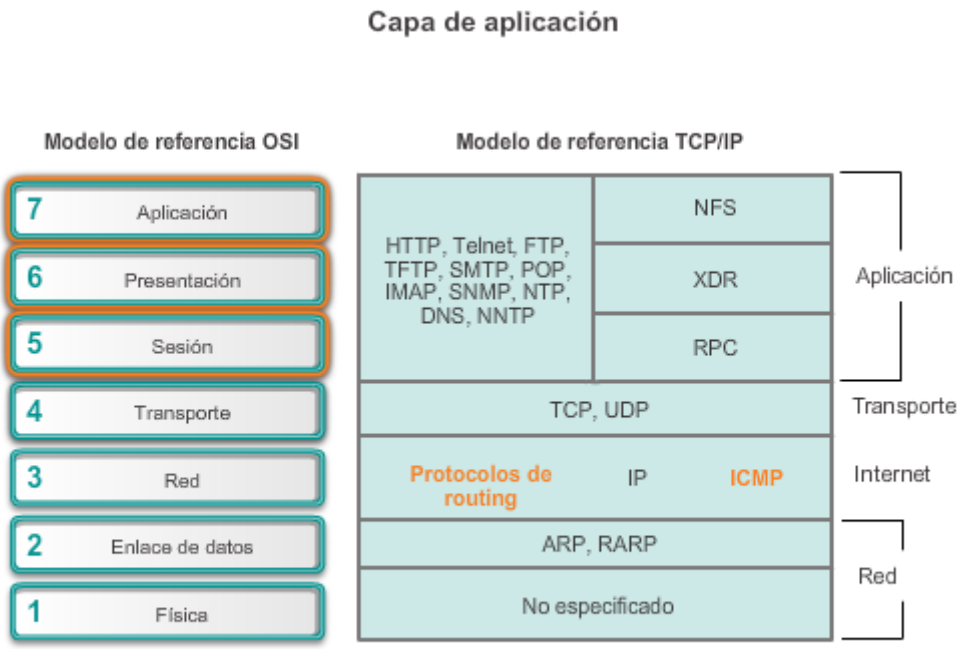
- **FTP:** realiza transferencias interactivas de archivos entre los hosts.
- **TFTP:** realiza transferencias interactivas básicas de archivos, generalmente, entre hosts y dispositivos de red.
- **SMTP:** admite servicios básicos de entrega de mensajes.
- **POP:** conecta a los servidores de correo electrónico y descarga correo electrónico.
- **Protocolo simple de administración de red (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):**habilita las computadoras para montar unidades en hosts remotos y operarlas como si fueran unidades locales. Desarrollado originalmente por Sun Microsystems, se combina con otros dos protocolos de capa de aplicación, la representación externa de datos (XDR) y la llamada a procedimiento remoto (RPC), para permitir un acceso transparente a los recursos de la red remota.

Los tipos de síntomas y causas dependen de la aplicación real propiamente dicha.

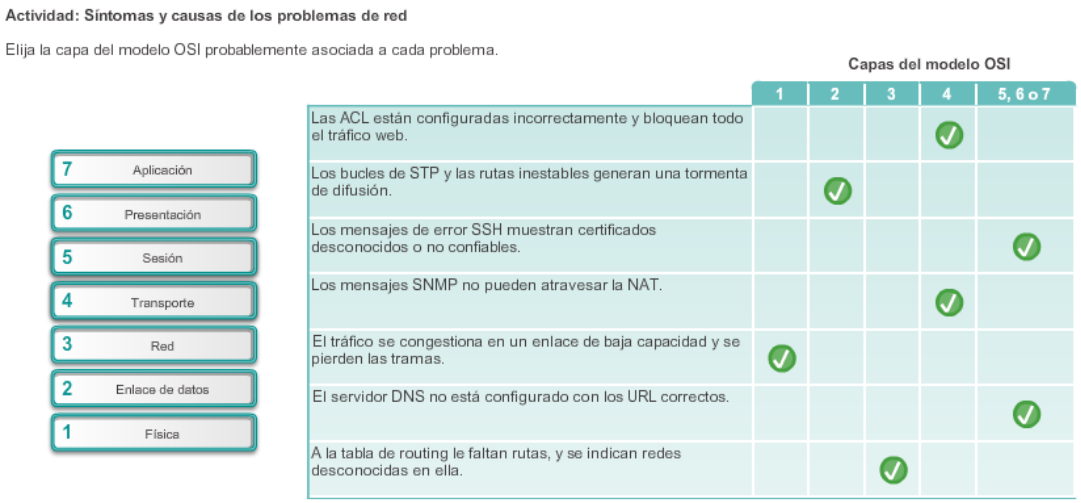
Los problemas de la capa de aplicación impiden la provisión de servicios a los programas de aplicación. Cuando la capa física, la capa de enlace de datos, la capa de red y la capa de transporte funcionan, un problema en la capa de aplicación puede tener como consecuencia recursos inalcanzables o inutilizables. Es posible que, teniendo una conectividad de red plena, la aplicación simplemente no pueda proporcionar datos.

Otro tipo de problema en la capa de aplicación ocurre cuando las capas física, de enlace de datos, de red y de transporte funcionan, pero la transferencia de datos y las solicitudes de servicios de red de un único servicio o aplicación de red no cumplen con las expectativas normales de un usuario.

Un problema en la capa de aplicación puede hacer que los usuarios se quejen de que, al transferir datos o solicitar servicios de red, la red o la aplicación específica con la que trabajan está inactiva o más lenta de lo normal.



Capítulo 9: Resolución de problemas de red 9.2.2.7 Actividad: Identificar la capa del modelo OSI asociada a un problema de red



Capítulo 9: Resolución de problemas de red 9.2.3.1 Componentes de la resolución de problemas de conectividad de extremo a extremo

Diagnosticar y resolver problemas es una aptitud esencial para los administradores de red. No existe una única receta para la resolución de problemas, y un problema en particular se puede diagnosticar de muchas maneras diferentes. Sin embargo, al emplear un enfoque estructurado

para el proceso de resolución de problemas, un administrador puede reducir el tiempo que tarda en diagnosticar y resolver un problema.

En este tema, se usa la siguiente situación. El host cliente PC1 no puede acceder a las aplicaciones en el servidor SRV1 o el servidor SRV2. En la ilustración, se muestra la topología de esta red. Para crear su dirección IPv6 de unidifusión global, la PC1 usa SLAAC con EUI-64. Para crear la ID de interfaz, EUI-64 usa la dirección MAC de Ethernet, inserta FFFE en el medio e invierte el séptimo bit.

Cuando no hay conectividad de extremo a extremo y el administrador elige resolver problemas con un enfoque ascendente, estos son los pasos frecuentes que el administrador puede seguir:

Paso 1. Revisar la conectividad física en el punto donde se detiene la comunicación de red. Esto incluye los cables y el hardware. El problema podría estar relacionado con un cable o una interfaz defectuosos o con un componente de hardware defectuoso o configurado incorrectamente.

Paso 2. Revisar las incompatibilidades de dúplex.

Paso 3. Revisar el direccionamiento de las capas de enlace de datos y de red en la red local. Esto incluye las tablas ARP de IPv4, las tablas de vecinos IPv6, las tablas de direcciones MAC y las asignaciones de VLAN.

Paso 4. Verificar que el gateway predeterminado sea correcto.

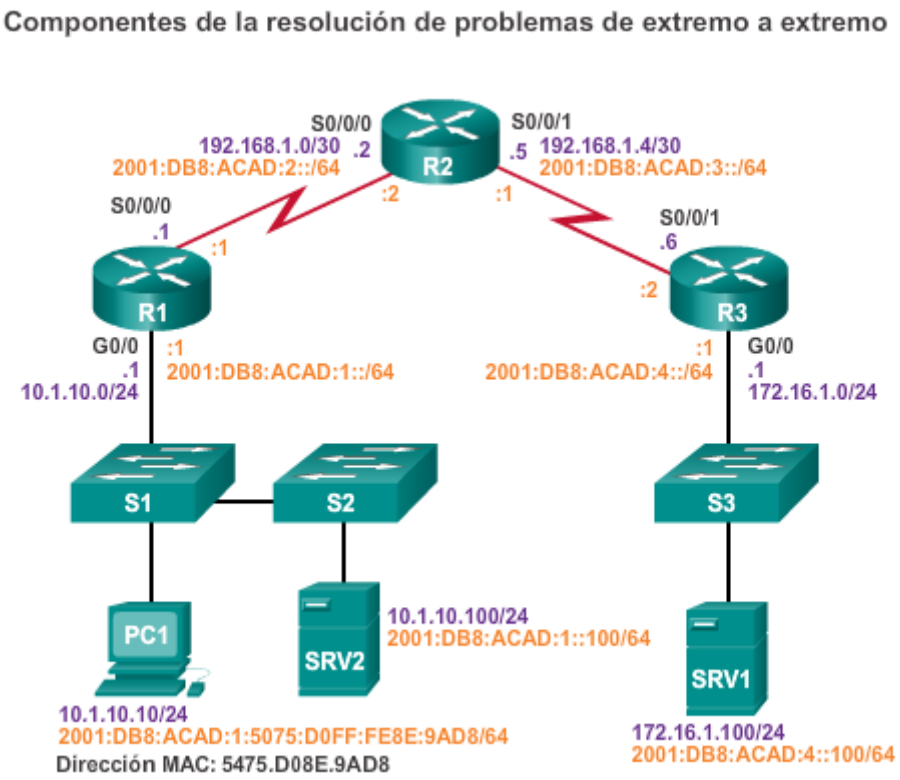
Paso 5. Asegurarse de que los dispositivos determinen la ruta correcta del origen al destino. Si es necesario, se debe manipular la información de routing.

Paso 6. Verificar que la capa de transporte funcione correctamente. También se puede usar Telnet desde la línea de comandos para probar las conexiones de la capa de transporte.

Paso 7. Verificar que no haya ACL que bloqueen el tráfico.

Paso 8. Asegurarse de que la configuración del DNS sea correcta. Debe haber un servidor DNS accesible.

El resultado de este proceso es una conectividad de extremo a extremo en condiciones de funcionamiento. Si se siguieron todos los pasos sin obtener resolución alguna, es posible que el administrador de red desee repetir los pasos anteriores o elevar el problema a un administrador más experimentado.



Capítulo 9: Resolución de problemas de red 9.2.3.2 Problema de conectividad de extremo a

extremo que inicia la resolución de problemas

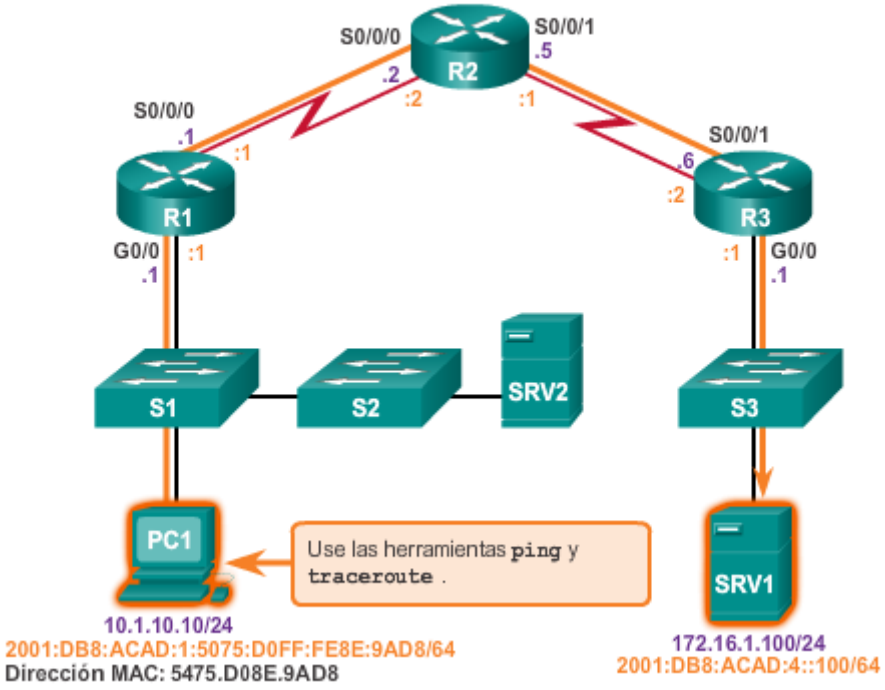
Generalmente, lo que da inicio a un esfuerzo de resolución de problemas es la detección de un problema con la conectividad de extremo a extremo. Dos de las utilidades más comunes que se utilizan para verificar un problema con la conectividad de extremo a extremo son**ping** y **traceroute**, que se muestran en la figura 1.

Es probable que ping sea la utilidad de prueba de conectividad más popular en el ámbito de la tecnología de redes y siempre formó parte del software IOS de Cisco. Esta herramienta envía solicitudes de respuesta desde una dirección host especificada. El comando **ping** usa un protocolo de capa 3 que forma parte de la suite TCP/IP llamada ICMP. Ping usa la solicitud de eco ICMP y los paquetes de respuesta de eco ICMP. Si el host en la dirección especificada recibe la solicitud de eco ICMP, responde con un paquete de respuesta de eco ICMP. Se puede usar ping para verificar la conectividad de extremo a extremo tanto en IPv4 como en IPv6. En la figura 2, se muestra un ping satisfactorio de la PC1 al SRV1, en la dirección 172.16.1.100.

El comando **traceroute** en la figura 3 muestra la ruta que los paquetes IPv4 toman para llegar al destino. De manera similar a lo que sucede con el comando**ping**, se puede usar el comando**traceroute** del IOS de Cisco para IPv4 e IPv6. El comando **tracert** se usa con el sistema operativo Windows. El rastreo genera una lista de saltos, direcciones IP de router y la dirección IP de destino final a las que se llega correctamente a través de la ruta. Esta lista proporciona información importante sobre la verificación y la resolución de problemas. Si los datos llegan al destino, el rastreo indica la interfaz de cada router de la ruta. Si los datos fallan en algún salto de la ruta, se conoce la dirección del último router que respondió al rastreo. Esta dirección es un indicio de dónde se encuentran el problema o las restricciones de seguridad.

Según lo indicado, al proporcionar la dirección IPv6 como dirección de destino, las utilidades ping y traceroute se pueden usar para probar y diagnosticar la conectividad IPv6 de extremo a extremo. Al usarlas, las utilidades del IOS de Cisco reconocen si la dirección en cuestión es IPv4 o IPv6 y usan el protocolo apropiado para probar la conectividad. En la figura 4, se muestran los comandos **ping** y**traceroute** en el router R1 que se usa para probar la conectividad IPv6.

Verificación de la conectividad de extremo a extremo



Ping IPv4 correcto de la PC1 al SRV1

```
PC1> ping 172.16.1.100
Pinging 172.16.1.100 with 32 bytes of data:
Reply from 172.16.1.100: bytes=32 time=8ms TTL=254
Reply from 172.16.1.100: bytes=32 time=1ms TTL=254
Reply from 172.16.1.100: bytes=32 time=1ms TTL=254
Reply from 172.16.1.100: bytes=32 time=1ms TTL=254
Ping statistics for 172.16.1.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round-trip times in milliseconds:
Minimum = 1ms, Maximum = 8ms, Average = 2ms
```

Tracert IPv4 correcto de la PC1 al SRV1

```
C:\Windows\system32> tracert 172.16.1.100
Tracing route to 172.16.1.100 over a maximum of 30 hops
1    1 ms    <1 ms    <1 ms    10.1.10.1
2    2 ms     2 ms     1 ms    192.168.1.2
3    2 ms     2 ms     1 ms    192.168.1.6
4    2 ms     2 ms     1 ms    172.16.1.100
Trace complete.
```

Ping y traceroute IPv6 correctos del R1 al SRV1

```
R1# ping 2001:db8:acad:4::100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:4::100,
timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
56/56/56 ms
R1# traceroute 2001:db8:acad:4::100
Type escape sequence to abort.
Tracing the route to 2001:DB8:ACAD:4::100

  1 2001:DB8:ACAD:2::2 20 msec 20 msec 20 msec
  2 2001:DB8:ACAD:3::2 44 msec 40 msec 40 msec
R1#
```

Capítulo 9: Resolución de problemas de red 9.2.3.3 Paso 1: Verificar la capa física

Todos los dispositivos de red son sistemas de computación especializados. Como mínimo, estos dispositivos constan de una CPU, RAM y espacio de almacenamiento, que permiten que el dispositivo arranque y ejecute el sistema operativo y las interfaces. Esto permite la recepción y la transmisión del tráfico de la red. Cuando un administrador de red determina que existe un problema en un dispositivo determinado y que el problema puede estar relacionado con el hardware, vale la pena verificar el funcionamiento de estos componentes genéricos. Los comandos del IOS de Cisco usados con más frecuencia son **show processes cpu**, **show memory** y **show interfaces**. En este tema, se analiza el comando **show interfaces**.

Al resolver problemas relacionados con el rendimiento en los que se sospecha que el hardware es el culpable, se puede usar el comando **show interfaces** para verificar las interfaces que atraviesa el tráfico.

En el resultado del comando **show interfaces** en la ilustración, se indican varias estadísticas importantes que se pueden revisar:

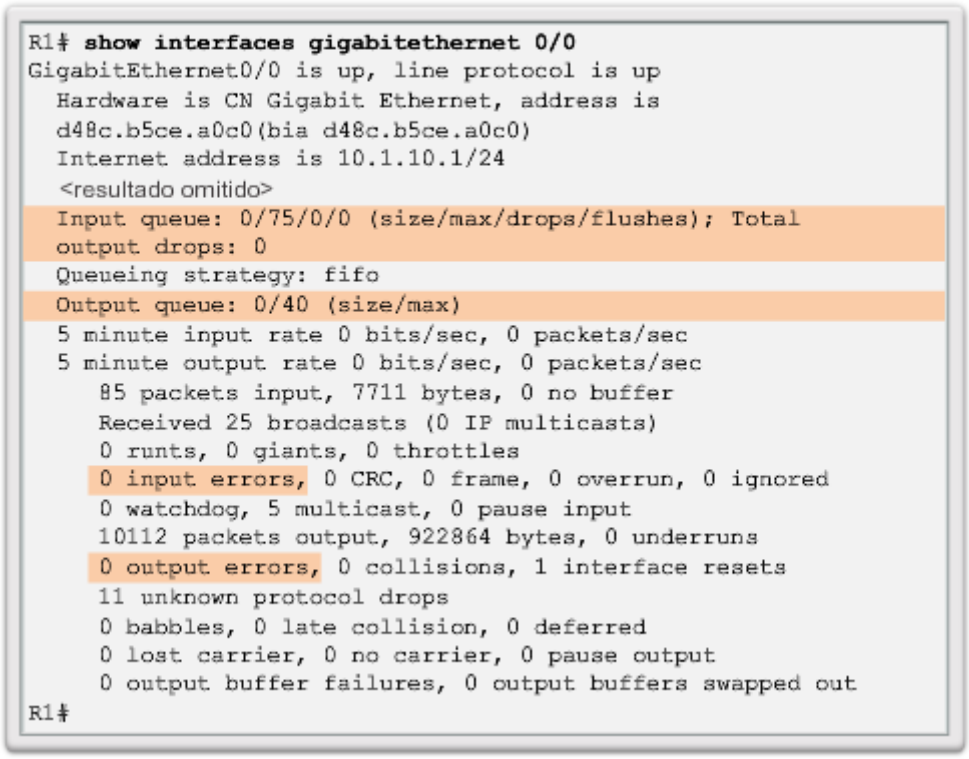
- **Descartes de la cola de entrada:** los descartes de la cola de entrada (y los contadores ignorados y de limitación relacionados) indican que, en algún momento, se entregó al router más tráfico del que podía procesar. Esto no indica necesariamente un problema. Podría ser normal durante los picos de tráfico. Sin embargo, podría ser una indicación de que la CPU no puede procesar los paquetes a tiempo, por lo que, si este número es permanentemente alto, vale la pena tratar de detectar en qué momentos aumentan estos contadores y cómo se relaciona eso con el uso de CPU.

- **Descartes de la cola de salida:** los descartes de la cola de salida indican que se descartaron paquetes debido a la congestión en la interfaz. Es normal ver descartes de salida en cualquier punto donde la agregación de tráfico de entrada es superior al tráfico de salida. Durante los picos de tráfico, si el tráfico se entrega a la interfaz más rápidamente de que lo que se puede enviar, se descartan paquetes. Sin embargo, incluso si esto se considera un comportamiento normal, provoca el descarte de paquetes y retrasos en la cola, de modo que es posible que las aplicaciones afectadas por esas situaciones, como VoIP, tengan problemas de rendimiento. La observación sistemática de descartes de salida puede indicar que es necesario implementar un mecanismo de cola avanzado para proporcionar una buena QoS para cada aplicación.

- **Errores de entrada:** los errores de entrada (input errors) indican errores que se experimentan durante la recepción de la trama, como errores de CRC. Una cantidad elevada de errores de CRC podría indicar problemas de cableado, problemas de hardware de interfaz o, en una red basada en Ethernet, incompatibilidades de dúplex.

- **Errores de salida:** los errores de salida (output errors) indican errores durante la transmisión de una trama, por ejemplo, colisiones. En la actualidad, en la mayoría de las redes basadas en Ethernet, la transmisión full-duplex es la norma y la transmisión half-duplex es la excepción. En la transmisión full-duplex, no pueden ocurrir colisiones en las operaciones; por lo tanto, las colisiones (especialmente las colisiones tardías) indican con frecuencia incompatibilidades de dúplex.

Análisis de las estadísticas de entrada y de salida en el R1



```
R1# show interfaces gigabitethernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is
  d48c.b5ce.a0c0(bia d48c.b5ce.a0c0)
  Internet address is 10.1.10.1/24
   <resultado omitido>
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total
  output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     85 packets input, 7711 bytes, 0 no buffer
     Received 25 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 5 multicast, 0 pause input
     10112 packets output, 922864 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     11 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
R1#
```

Capítulo 9: Resolución de problemas de red 9.2.3.4 Paso 2: Revisar las incompatibilidades de dúplex

Otra causa común de los errores de interfaz es un modo de dúplex incompatible entre los dos extremos de un enlace Ethernet. Actualmente, en numerosas redes basadas en Ethernet, las conexiones punto a punto son la norma, y el uso de hubs y la operación half-duplex asociadas se están volviendo menos frecuentes. Esto significa que, en la actualidad, la mayoría de los enlaces Ethernet operan en modo full-duplex y que, si bien se consideraba que las colisiones eran normales en un enlace Ethernet, hoy en día las colisiones suelen indicar que la negociación de dúplex falló y que el enlace no opera en el modo de dúplex correcto.

El estándar Gigabit Ethernet IEEE 802.3ab exige el uso de la autonegociación para velocidad y dúplex. Además, si bien no es estrictamente obligatorio, casi todas las NIC Fast Ethernet también usan la autonegociación de manera predeterminada. En la actualidad, la práctica recomendada es la autonegociación para velocidad y dúplex. En la figura 1, se indican las pautas para la configuración de dúplex.

Sin embargo, si la negociación de dúplex falla por algún motivo, podría ser necesario establecer la velocidad y el dúplex manualmente en ambos extremos. Por lo general, esto conllevaría configurar el modo dúplex en full-duplex en ambos extremos de la conexión. Sin embargo, si esto no funciona, es preferible ejecutar half-duplex en ambos extremos a experimentar una incompatibilidad de dúplex.

Ejemplo de resolución de problemas

El administrador de red tuvo que agregar usuarios adicionales a la red de la situación anterior. Para incorporar a estos nuevos usuarios, el administrador de red instaló un segundo switch y lo conectó al primero. Poco después de que se agregó el S2 a la red, los usuarios en ambos switches comenzaron a experimentar importantes problemas de rendimiento al conectarse con los dispositivos en el otro switch, como se muestra en la figura 2.

El administrador de red observa un mensaje de la consola en el switch S2:

*Mar 1 00:45:08.756: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet0/20 (not half duplex), with Switch FastEthernet0/20 (half duplex).

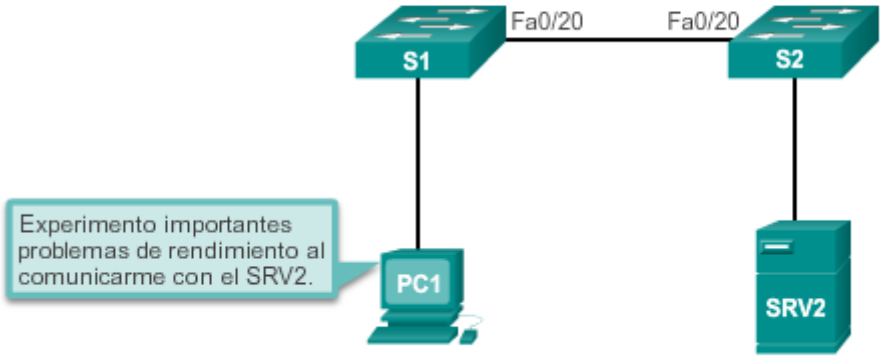
Mediante el comando **show interfaces fa 0/20**, el administrador de red examina la interfaz en el S1 usada para conectarse al S2 y observa que está establecida en full-duplex, como se muestra en la figura 3. Ahora, el administrador de red examina el otro lado de la conexión: el puerto en el S2. En la figura 4, se muestra que este lado de la conexión se configuró como half-duplex. El administrador de red corrige la configuración y la establece en **duplex auto**, para que el dúplex se negocie automáticamente. Debido a que el puerto en el S1 se establece en full-duplex, el S2 también usa full-duplex.

Los usuarios informan que ya no existe ningún problema de rendimiento.

Pautas de configuración de dúplex:

- Los enlaces Ethernet de punto a punto siempre se deben ejecutar en modo full-duplex.
- Half-duplex ya no es frecuente y se utiliza principalmente si se usan hubs.
- Se recomienda la autonegociación de velocidad y dúplex.
- Si la autonegociación no funciona, establezca manualmente la velocidad y el dúplex en ambos extremos.
- La presencia de half-duplex en ambos extremos funciona mejor que una incompatibilidad de dúplex.

Incompatibilidad de dúplex



Funcionamiento del puerto del S1 en full-duplex

```
S1# show interface fa 0/20
FastEthernet0/20 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0cd9.96e8.8a01 (bia
  0cd9.96e8.8a01)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, Auto-speed, media type is 10/100BaseTX
<resultado omitido>
```

Funcionamiento del puerto del S2 en half-duplex

```
S2# show interface fa 0/20
FastEthernet0/20 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0cd9.96d2.4001 (bia
  0cd9.96d2.4001)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, Auto-speed, media type is 10/100BaseTX
<resultado omitido>
Switch(config)# interface fa 0/20
Switch(config-if)# duplex auto
Switch(config-if)#
```

Capítulo 9: Resolución de problemas de red 9.2.3.5 Paso 3: Verificar el direccionamiento de capa 2 y capa 3 en la red local

Al resolver problemas de conectividad de extremo a extremo, es útil verificar las asignaciones entre las direcciones IP de destino y las direcciones Ethernet de capa 2 en segmentos individuales. En IPv4, ARP proporciona esta funcionalidad. En IPv6, la funcionalidad de ARP se reemplaza por el proceso de detección de vecinos e ICMPv6. La tabla de vecinos almacena en caché las direcciones IPv6 y sus direcciones físicas de Ethernet (MAC) resueltas.

Tabla ARP de IPv4

El comando **arp** de Windows muestra y modifica las entradas en la caché ARP que se usan para almacenar las direcciones IPv4 y sus direcciones físicas de Ethernet (MAC) resueltas. Como se muestra en la figura 1, el comando **arp** de Windows enumera todos los dispositivos que actualmente están en la caché ARP. La información que se muestra para cada dispositivo incluye la dirección IPv4, la dirección física (MAC) y el tipo de direccionamiento (estático o dinámico).

Si el administrador de red desea volver a llenar la caché con información actualizada, se puede borrar la caché mediante el comando **arp -d** de Windows.

Nota: los comandos **arp** en Linux y MAC OS X tienen una sintaxis similar.

Tabla de vecinos de IPv6

Como se muestra en la figura 2, el comando **netsh interface ipv6 show neighbor** de Windows enumera todos los dispositivos que actualmente están en la tabla de vecinos. La información que se muestra para cada dispositivo incluye la dirección IPv6, la dirección física (MAC) y el tipo de direccionamiento. Al examinar la tabla de vecinos, el administrador de red puede verificar que las direcciones IPv6 de destino se asignen a las direcciones Ethernet correctas. Las direcciones IPv6 link-local se configuraron manualmente en todas las interfaces del R1 como FE80::1. De manera similar, se configuró el R2 con la dirección link-local FE80::2 en sus interfaces, y se configuró el R3 con la dirección link-local FE80::3 en sus interfaces. Recuerde que las direcciones link-local solo tienen que ser exclusivas en el enlace o la red.

Nota: en los sistemas operativos Linux y MAC OS X, se puede mostrar la tabla de vecinos mediante el comando **ip neigh show**.

En la figura 3, se muestra un ejemplo de la tabla de vecinos en un router con IOS de Cisco mediante el comando **show ipv6 neighbors**.

Nota: los estados de los vecinos en IPv6 son más complejos que los estados de la tabla ARP en IPv4. RFC 4861 contiene información adicional.

Tabla de direcciones MAC del switch

Un switch reenvía una trama solamente al puerto donde se conecta el destino. Para hacer esto, el switch consulta su tabla de direcciones MAC. La tabla de direcciones MAC indica la dirección MAC conectada a cada puerto. Use el comando **show mac address-table** para visualizar la tabla de direcciones MAC en el switch. En la figura 4, se muestra un ejemplo del switch local de la PC1. Recuerde que la tabla de direcciones MAC de un switch solo contiene información de capa 2, que incluye la dirección MAC de Ethernet y el número de puerto. No se incluye información de dirección IP.

Asignación de red VLAN

Al resolver problemas de conectividad de extremo a extremo, otro problema que se debe considerar es la asignación de VLAN. En una red conmutada, cada puerto en un switch pertenece a una VLAN. Cada VLAN se considera una red lógica independiente, y los paquetes destinados a las estaciones que no pertenecen a la VLAN se deben reenviar a través de un dispositivo que admita el routing. Si un host en una VLAN envía una trama de Ethernet de difusión, como una solicitud de ARP, todos los hosts en la misma VLAN reciben la trama, mientras que los hosts en otras VLAN no la reciben. Incluso si dos hosts están en la misma red IP, no se podrán comunicar si están conectados a puertos asignados a dos VLAN separadas.

Además, si se elimina la VLAN a la que pertenece el puerto, este queda inactivo. Ninguno de los hosts conectados a los puertos que pertenecen a la VLAN que se eliminó se puede comunicar con el resto de la red. Los comandos como **show vlan** se pueden usar para validar las asignaciones de VLAN en un switch.

Ejemplo de resolución de problemas

Consulte la topología en la figura 5. Para mejorar la administración de los cables en el armario de cableado, se reorganizaron los cables que se conectan al S1. Casi inmediatamente después de hacerlo, los usuarios comenzaron a llamar al soporte técnico con el comentario de que ya no tenían posibilidad de conexión a los dispositivos fuera de su propia red. Un examen de la tabla ARP de la PC1 mediante el comando **arp** de Windows muestra que la tabla ARP ya no contiene una entrada para el gateway predeterminado 10.1.10.1, como se muestra en la figura 6. No hubo cambios de configuración en el router, de modo que la resolución de problemas se centra en el S1.

Tabla ARP en la PC1

```
PC1> arp -a
Interface: 10.1.10.100 --- 0xd
Internet         Address Physical    Address Type
10.1.10.1        d4-8c-b5-ce-a0-c0   dynamic
224.0.0.22       01-00-5e-00-00-16   static
224.0.0.252      01-00-5e-00-00-fc   static
255.255.255.255  ff-ff-ff-ff-ff-ff   static
```

Tabla de vecinos en la PC1

```
PC1> netsh interface ipv6 show neighbor
Interface 13: LAB
Internet Address              Physical Address    Type
----------------------        ----------------    -------
fe80::9c5a:e957:a865:bde9     00-0c-29-36-fd-f7   Stale
fe80::1                       d4-8c-b5-ce-a0-c0   Reachable (Router)
ff02::2                       33-33-00-00-00-02   Permanent
ff02::16                      33-33-00-00-00-16   Permanent
ff02::1:2                     33-33-00-01-00-02   Permanent
ff02::1:3                     33-33-00-01-00-03   Permanent
ff02::1:ff05:f9fb             33-33-ff-05-f9-fb   Permanent
ff02::1:ffce:a0c0             33-33-ff-ce-a0-c0   Permanent
ff02::1:ff65:bde9             33-33-ff-65-bd-e9   Permanent
ff02::1:ff67:bae4             33-33-ff-67-ba-e4   Permanent
```

Tabla de vecinos en el R1

```
R1# show ipv6 neighbors
IPv6 Address                              Age Link-layer Addr State Interface
FE80::21E:7AFF:FE79:7A81                    8 001e.7a79.7a81  STALE  Gi0/0
2001:DB8:ACAD:1:5075:D0FF:FE8E:9AD8         0 5475.d08e.9ad8  REACH  Gi0/0
```

Tabla de direcciones MAC en el switch LAN local

```
S1# show mac address-table
             Mac Address Table
-------------------------------------------
Vlan     Mac Address         Type      Ports
All      0100.0ccc.cccc      STATIC    CPU
All      0100.0ccc.cccd      STATIC    CPU
 10      d48c.b5ce.a0c0      DYNAMIC   Fa0/4
 10      000f.34f9.9201      DYNAMIC   Fa0/5
 10      5475.d08e.9ad8      DYNAMIC   Fa0/13
Total Mac Addresses for this criterion: 5
```

La PC1 está conectada a Fa0/13 del S1, dentro de la VLAN 10.

Ejemplo de resolución de problemas

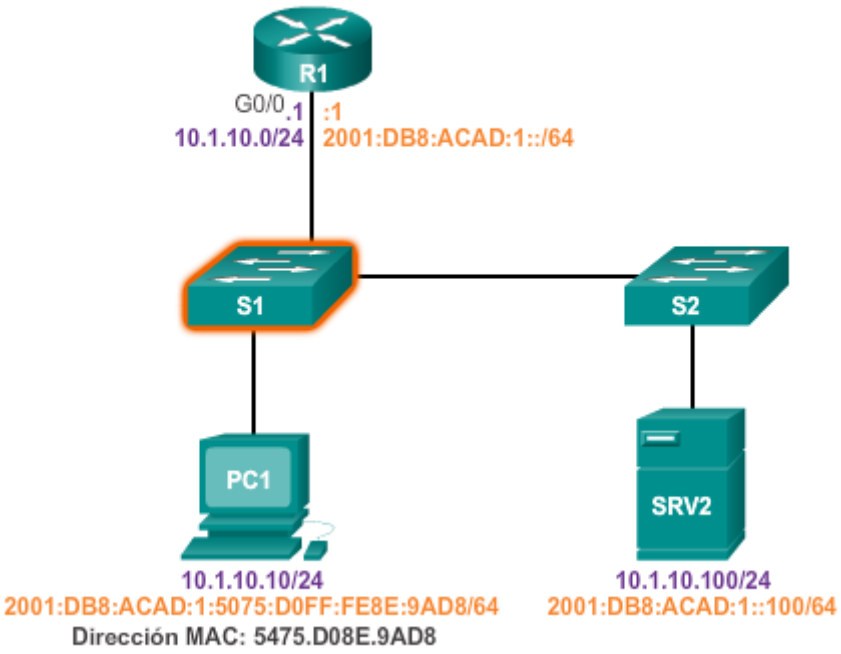


Tabla ARP en la PC1

```
PC1> arp -a
Interface: 10.1.10.100 --- 0xd
Internet    Address Physical Address Type
224.0.0.22    01-00-5e-00-00-16 static
224.0.0.252    01-00-5e-00-00-fc static
255.255.255.255     ff-ff-ff-ff-ff-ff static
```

La PC1 no tiene una entrada para el gateway predeterminado, 10.1.10.1.

La tabla de direcciones MAC revela una VLAN incorrecta para Fa0/1

```
S1# show mac address-table
             Mac Address Table
-------------------------------------------
Vlan      Mac Address          Type      Ports
All       0100.0ccc.cccc       STATIC    CPU
All       0100.0ccc.cccd       STATIC    CPU
   1      d48c.b5ce.a0c0       DYNAMIC   Fa0/1
  10      000f.34f9.9201       DYNAMIC   Fa0/5
  10      5475.d08e.9ad8       DYNAMIC   Fa0/13
Total Mac Addresses for this criterion: 5
```

R1

PC1

Configuración de la VLAN correcta

```
S1(config)# interface fa 0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config-if)#
```

Tabla de direcciones MAC en el switch LAN local

```
S1# show mac address-table
             Mac Address Table
-------------------------------------------
Vlan      Mac Address          Type      Ports
All       0100.0ccc.cccc       STATIC    CPU
All       0100.0ccc.cccd       STATIC    CPU
  10      d48c.b5ce.a0c0       DYNAMIC   Fa0/1
  10      000f.34f9.9201       DYNAMIC   Fa0/5
  10      5475.d08e.9ad8       DYNAMIC   Fa0/13
Total Mac Addresses for this criterion: 5
```

R1

PC1

Capítulo 9: Resolución de problemas de red 9.2.3.6 Paso 4: Verificar el gateway

predeterminado

Si no hay una ruta detallada en el router o si el host está configurado con el gateway predeterminado incorrecto, la comunicación entre dos terminales en redes distintas no funciona. En la figura 1, se muestra que la PC1 usa el R1 como gateway predeterminado. De manera similar, el R1 usa al R2 como gateway predeterminado o como gateway de último recurso.

Si un host necesita acceso a recursos que se encuentran más allá de la red local, se debe configurar el gateway predeterminado. El gateway predeterminado es el primer router en la ruta a los destinos que se encuentran más allá de la red local.

Ejemplo de resolución de problemas 1

En la figura 2, se muestran el comando**show ip route** del IOS de Cisco y el comando **route print** de Windows para verificar la presencia del gateway predeterminado IPv4.

En este ejemplo, el router R1 tiene el gateway predeterminado correcto, que es la dirección IPv4 del router R2. Sin embargo, la PC1 tiene el gateway predeterminado incorrecto. La PC1 debería tener el gateway predeterminado 10.1.10.1 del router R1. Si la información de direccionamiento IPv4 se configuró en forma manual en la PC1, esto se debe configurar manualmente. Si la información de direccionamiento IPv4 se obtuvo automáticamente de un servidor de DHCPv4, se debe examinar la configuración en el servidor de DHCP. Por lo general, un problema de configuración en un servidor de DHCP puede ser detectado por varios clientes.

Ejemplo de resolución de problemas 2

En IPv6, el gateway predeterminado se puede configurar manualmente o mediante la configuración automática sin estado (SLAAC) o DHCPv6. Con SLAAC, el router anuncia el gateway predeterminado a los hosts mediante los mensajes de anuncio de router (RA) ICMPv6. El gateway predeterminado en el mensaje RA es la dirección IPv6 link-local de una interfaz del router. Si el gateway predeterminado se configura manualmente en el host, lo que es muy poco probable, se puede establecer el gateway predeterminado en la dirección IPv6 global o en la dirección IPv6 link-local.

Como se muestra en la figura 3, el comando **show ipv6 route** del IOS de Cisco muestra la ruta predeterminada IPv6 en el R1, y el comando **ipconfig** de Windows se usa para verificar la presencia del gateway predeterminado IPv6.

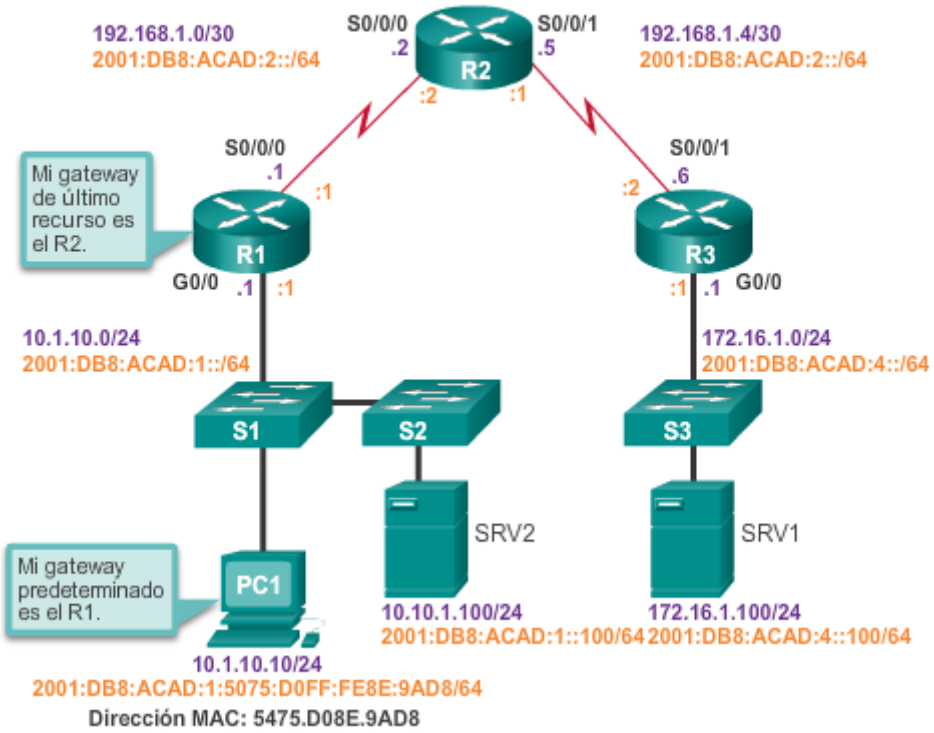
El R1 tiene una ruta predeterminada a través del router R2, pero observe que el comando **ipconfig** revela la ausencia de una dirección IPv6 de unidifusión global y un gateway predeterminado IPv6. La PC1 está habilitada para IPv6 debido a que tiene una dirección IPv6 link-local. El dispositivo crea automáticamente la dirección link-local. Al revisar la documentación de red, el administrador de red confirma que los hosts en esta LAN deberían recibir la información de dirección IPv6 del router que usa SLAAC.

Nota: en este ejemplo, otros dispositivos que usen SLAAC en la misma LAN también experimentarían el mismo problema al recibir la información de dirección IPv6.

Mediante el comando **show ipv6 interface GigabitEthernet 0/0** en la figura 4, se puede observar que, si bien la interfaz tiene una dirección IPv6, no forma parte del grupo de multidifusión de todos los routers IPv6, FF02::2. Esto significa que el router no envía mensajes RA ICMPv6 por esta interfaz. En la figura 5, el R1 se habilita como router IPv6 mediante el comando **ipv6 unicast-routing**. Ahora, el comando **show ipv6 interface GigabitEthernet 0/0**revela que el R1 forma parte de FF02::2, el grupo de multidifusión de todos los routers IPv6.

Para verificar que la PC1 tenga establecido el gateway predeterminado, use el comando**ipconfig** en una computadora con Microsoft Windows o el comando**ifconfig** en los sistemas operativos Linux y Mac OS X. En la figura 6, la PC1 tiene una dirección IPv6 de unidifusión global y un gateway predeterminado IPv6. El gateway predeterminado se establece en la dirección link-local del router R1, FE80::1.

Identificación de la ruta actual y la ruta deseada



Verificación del gateway predeterminado IPv4

```
R1# show ip route
<resultado omitido>

Gateway of last resort is 192.168.1.2 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.1.2
```

```
C:\Windows\system32> route print
<resultado omitido>

Network Destination   Netmask     Gateway      Interface     Metric
          0.0.0.0     0.0.0.0     10.1.10.2    10.1.10.100       11
```

Gateway predeterminado IPv6 faltante

```
R1# show ipv6 route
<resultado omitido>

S   ::/0 [1/0]
     via 2001:DB8:ACAD:2::2
```

```
C:\Windows\system32> ipconfig
Windows IP Configuration
   Connection-specific DNS Suffix . :
   Link-local IPv6 Address . . . . . :
fe80::5075:d0ff:fe8e:9ad8%13
   IPv4 Address. . . . . . . . . . . : 10.1.1.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.1.10.1
```

R1 configurado como router IPv6

```
R1# show ipv6 interface GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:1::1, subnet is 2001:DB8:ACAD:1::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF00:1
<resultado omitido>
```

R1 configurado como router IPv6

```
R1(config)# ipv6 unicast-routing
R1(config)# end
R1# show ipv6 interface GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:1::1, subnet is 2001:DB8:ACAD:1::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
<resultado omitido>
```

Verificación del gateway predeterminado IPv6

```
PC1> ipconfig
Windows IP Configuration
 Connection-specific DNS Suffix :
 IPv6 Address. . . . . . . . . . :
2001:db8:acad:1:5075:d0ff:fe8e:9ad8
 Link-local IPv6 Address . . . . : fe80::5075:d0ff:fe8e:9ad8%13
 IPv4 Address. . . . . . . . . . : 10.1.1.100
 Subnet Mask . . . . . . . . . . : 255.255.255.0
 Default Gateway . . . . . . . . : fe80::1
                                   10.1.10.1
```

Capítulo 9: Resolución de problemas de red 9.2.3.7 Paso 5: Verificar la ruta correcta

Resolución de problemas de la capa de red

Al resolver problemas, con frecuencia es necesario verificar la ruta hacia la red de destino. En la figura 1, se muestra la topología de referencia que indica la ruta deseada para los paquetes de la PC1 al SRV1.

En la figura 2, se usa el comando **show ip route** para examinar la tabla de routing IPv4.

Las tablas de routing IPv4 e IPv6 se pueden llenar con los siguientes métodos:

- Redes conectadas directamente
- Host local o rutas locales
- Rutas estáticas
- Rutas dinámicas
- Rutas predeterminadas

El proceso de reenvío de paquetes IPv4 e IPv6 se basa en la coincidencia más larga de bits o de prefijos. El proceso de la tabla de routing intenta reenviar el paquete mediante una entrada en la tabla de routing con el máximo número de bits coincidentes en el extremo izquierdo. La longitud de prefijo de la ruta indica el número de bits coincidentes.

En la figura 3, se muestra una situación similar con IPv6. Para verificar que la ruta IPv6 actual coincide con la ruta deseada para llegar a los destinos, use el comando**show ipv6 route** en el router para examinar la tabla de routing. Después de examinar la tabla de routing IPv6, el R1 tiene una ruta a 2001:DB8:ACAD:4::/64 mediante el R2 en FE80::2.

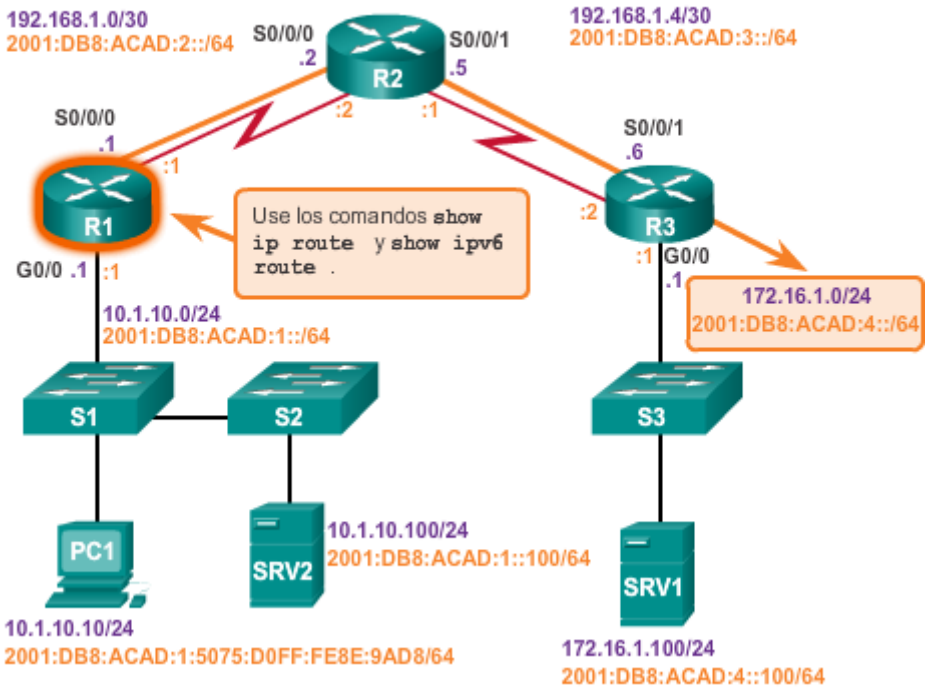
La siguiente lista, junto con la figura 4, describe el proceso de las tablas de routing IPv4 e IPv6. Si la dirección de destino en un paquete:

- No coincide con una entrada en la tabla de routing, se usa la ruta predeterminada. Si no hay una ruta predeterminada que esté configurada, se descarta el paquete.
- Coincide con una única entrada en la tabla de routing, el paquete se reenvía a través de la interfaz definida en esta ruta.
- Coincide con más de una entrada en la tabla de routing y las entradas de routing tienen la misma longitud de prefijo, los paquetes para este destino se pueden distribuir entre las rutas definidas en la tabla de routing.
- Coincide con más de una entrada en la tabla de routing y las entradas de routing tienen longitudes de prefijo diferentes, los paquetes para este destino se reenvían por la interfaz que está asociada a la ruta que tiene la coincidencia de prefijos más larga.

Ejemplo de resolución de problemas

Los dispositivos no se pueden conectar al servidor SRV1 en 172.16.1.100. Mediante el comando **show ip route**, el administrador debe revisar si existe una entrada de routing en la red 172.16.1.0/24. Si la tabla de routing no tiene una ruta específica a la red del SRV1, el administrador de red debe revisar la existencia de una entrada de ruta resumida o predeterminada en el sentido de la red 172.16.1.0/24. Si no existe ninguna entrada, es posible que el problema esté relacionado con el routing y que el administrador deba verificar que la red esté incluida dentro de la configuración del protocolo de routing dinámico o que deba agregar una ruta estática.

Identificación de la ruta actual y la ruta deseada



Análisis de la tabla de routing IPv4 en el R1

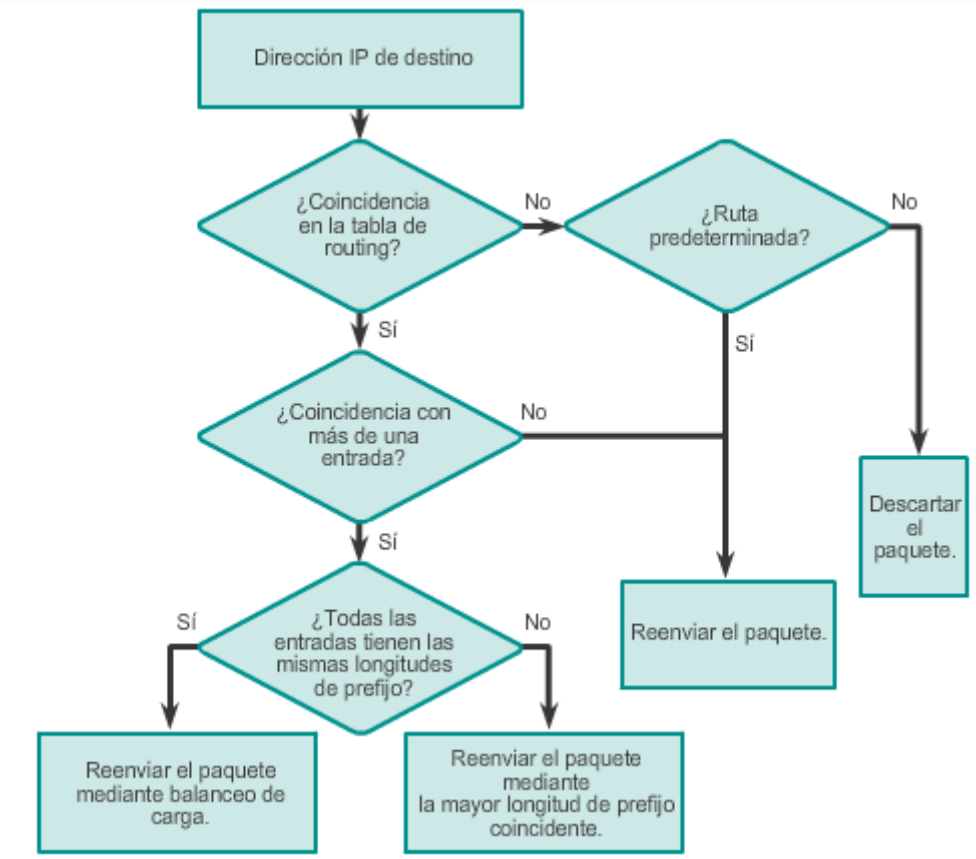
```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile
       B - BGP, D - EIGRP, EX - EIGRP external, O - OSPF
       IA - OSPF inter area, N1 - OSPF NSSA external type 1
       N2 - OSPF NSSA external type 2, E1 - OSPF external type 1
       E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary
       L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default
       U - per-user static route, o - ODR
       P - periodic downloaded static route, H - NHRP l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.1.2 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.1.2
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.10.0/24 is directly connected, GigabitEthernet0/0
L        10.1.10.1/32 is directly connected, GigabitEthernet0/0
      172.16.0.0/24 is subnetted, 1 subnets
D        172.16.1.0 [90/41024256] via 192.168.1.2, 05:32:46,
         Serial0/0/0
      192.168.1.0/24 is variably subnetted, 3 subnets, 2 masks
C        192.168.1.0/30 is directly connected, Serial0/0/0
L        192.168.1.1/32 is directly connected, Serial0/0/0
D        192.168.1.4/30 [90/41024000] via 192.168.1.2, 05:32:46,
         Serial0/0/0
R1#
```

Análisis de la tabla de routing IPv6 en el R1

```
R1# show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static
       U - Per-user Static route, B - BGP, R - RIP
       I1 - ISIS L1, I2 - ISIS L2, A - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2
S   ::/0 [1/0]
     via 2001:DB8:ACAD:2::2
C   2001:DB8:ACAD:1::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
     via GigabitEthernet0/0, receive
C   2001:DB8:ACAD:2::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
     via Serial0/0/0, receive
D   2001:DB8:ACAD:3::/64 [90/41024000]
     via FE80::2, Serial0/0/0
D   2001:DB8:ACAD:4::/64 [90/41024256]
     via FE80::2, Serial0/0/0
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```



Resolución de problemas de la capa de transporte

Si la capa de red parece funcionar como se esperaba, pero los usuarios aún no pueden acceder a los recursos, el administrador de red debe comenzar a resolver problemas en las capas superiores. Dos de los problemas más frecuentes que afectan la conectividad de la capa de transporte incluyen las configuraciones de ACL y de NAT. Una herramienta frecuente para probar la funcionalidad de la capa de transporte es la utilidad Telnet.

Precaución: si bien se puede usar Telnet para probar la capa de transporte, por motivos de seguridad se debe usar SSH para administrar y configurar los dispositivos en forma remota.

Un administrador de red trabaja en la resolución de un problema en el que una persona no puede enviar correo electrónico a través de un servidor SMTP determinado. El administrador hace ping al servidor, y este responde. Esto significa que la capa de red y todas las capas inferiores a esta entre el usuario y el servidor están en condiciones de funcionamiento. El administrador sabe que el problema está en la capa 4 o en las capas superiores y que debe comenzar a resolver problemas en esas capas.

Si bien la aplicación del servidor telnet se ejecuta en su propio número de puerto bien conocido 23, y los clientes Telnet se conectan a este puerto de manera predeterminada, se puede especificar un número de puerto diferente en el cliente para conectarse a cualquier puerto TCP que se deba probar. Esto indica si la conexión se acepta (como se indica mediante la palabra “Open” [Abierta] en el resultado), se rechaza o si excede el tiempo de espera. A partir de cualquiera de estas respuestas, se pueden obtener otras conclusiones relacionadas con la conectividad. En ciertas aplicaciones, si usan un protocolo de sesión basado en ASCII (incluso pueden mostrar un aviso de la aplicación), es posible desencadenar algunas respuestas desde el servidor al escribir ciertas palabras clave, como con SMTP, FTP y HTTP.

Dada la situación anterior, el administrador accede mediante Telnet al servidor HQ desde la PC1, a través de IPv6, y la sesión Telnet es correcta, como se muestra en la figura 1. En la figura 2, el administrador intenta acceder mediante Telnet al mismo servidor, a través del puerto 80. En el resultado, se verifica que la capa de transporte se conecta correctamente de la PC1 a HQ. Sin embargo, el servidor no acepta conexiones en el puerto 80.

En el ejemplo de la figura 3, se muestra una conexión Telnet correcta del R1 al R3, a través de IPv6. En la figura 4, se observa un intento similar de acceder mediante Telnet a través del puerto 80. Una vez más, en el resultado se verifica una conexión correcta de la capa de transporte, pero el R3 rechaza la conexión mediante el puerto 80.

Conexión Telnet correcta a través de IPv4

```
PC1> telnet 2001:DB8:172:16::100
HQ#
```

Prueba de la capa de transporte a través de IPv4 mediante el puerto 80 (HTTP)

```
PC1> telnet 2001:DB8:172:16::100 80
HTTP/1.1 400 Bad Request
Date: Wed, 26 Sep 2012 07:27:10 GMT
Server: cisco-IOS
Accept-Ranges: none
400 Bad Request
Connection to host lost.
```

Conexión Telnet correcta a través de IPv6

```
R1# telnet 2001:db8:acad:3::2
Trying 2001:DB8:ACAD:3::2 ... Open

User Access Verification

Password:
R3>
```

Prueba de la capa de transporte a través de IPv6 mediante el puerto 80 (HTTP)

```
R1# telnet 2001:db8:acad:3::2 80
Trying 2001:DB8:ACAD:3::2, 80 ...
% Connection refused by remote host

R1#
```

Capítulo 9: Resolución de problemas de red 9.2.3.9 Paso 7: Verificar las ACL

En los routers, puede haber ACL configuradas que prohíben a los protocolos atravesar la interfaz en sentido entrante o saliente.

Use el comando **show ip access-lists** para visualizar el contenido de todas las ACL de IPv4 y el comando **show ipv6 access-list** para visualizar el contenido de todas las ACL de IPv6 configuradas en un router. Como una opción de este comando, se puede visualizar una ACL específica al introducir el nombre o el número de la ACL. Los comandos **show ip interfaces** y **show ipv6 interfaces** muestran la información de interfaz IPv4 e IPv6 que indica hay alguna ACL de IP establecida en la interfaz.

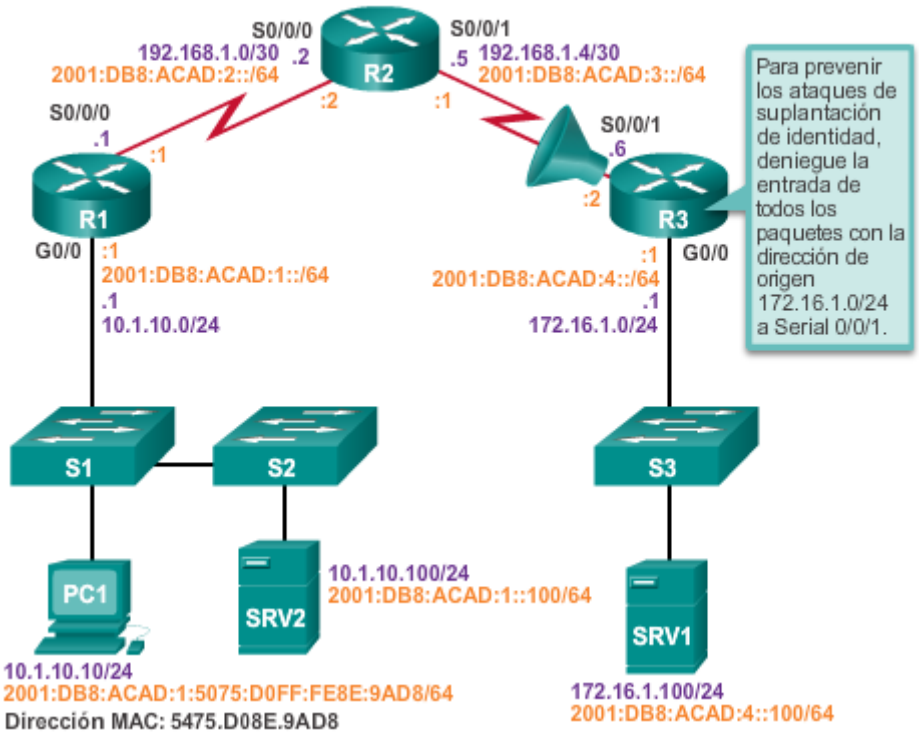
Ejemplo de resolución de problemas

Para prevenir los ataques de suplantación de identidad, el administrador de red decidió implementar una ACL para evitar que los dispositivos con la dirección de red de origen 172.16.1.0/24 ingresen a la interfaz de entrada S0/0/1 en el R3, como se muestra en la figura 1. Se debe permitir el resto del tráfico IP.

Sin embargo, poco después de implementar la ACL, los usuarios en la red 10.1.10.0/24 no podían conectarse a los dispositivos en la red 172.16.1.0/24, incluido el SRV1. Como se ve en la figura 2, el comando**show ip access-lists** muestra que la ACL está configurada correctamente. Sin embargo, el comando **show ip interfaces serial 0/0/1** revela que la ACL nunca se aplicó a la interfaz de entrada s0/0/1. Una investigación más profunda revela que la ACL se aplicó accidentalmente a la interfaz G0/0, lo que bloqueó todo el tráfico saliente de la red 172.16.1.0/24.

Después de colocar de manera correcta la ACL de IPv4 en la interfaz de entrada s0/0/1, como se muestra en la figura 3, los dispositivos se pueden conectar correctamente al servidor.

Problemas de ACL



Visualización de ACL y colocación de ACL en el R1

```
R3# show ip access-lists
Extended IP access list 100
    deny ip 172.16.1.0 0.0.0.255 any (3 match(es))
    permit ip any any

R3# show ip interface Serial 0/0/1 | include access list
   Outgoing access list is not set
   Inbound access list is not set

R3# show ip interface gigabitethernet 0/0 | include access list
   Outgoing access list is not set
   Inbound  access list is 100
```

Cambio de colocación de ACL

```
R3(config)# interface gigabitethernet 0/0
R3(config-if)# no ip access-group 100 in
R3(config-if)# interface serial 0/0/1
R3(config-if)# ip access-group 100 in
```

Capítulo 9: Resolución de problemas de red 9.2.3.10 Paso 8: Verificar DNS

El protocolo DNS controla el DNS, una base de datos distribuida mediante la cual se pueden asignar nombres de host a las direcciones IP. Cuando configura el DNS en el dispositivo, puede reemplazar el nombre de host por la dirección IP con todos los comandos IP, como **ping** o**telnet**.

Para visualizar la información de configuración de DNS en el switch o el router, utilice el comando **show running-config**. Cuando no hay instalado un servidor DNS, es posible introducir asignaciones de nombres a direcciones IP directamente en la configuración del switch o del router. Use el comando **ip host**para introducir una asignación de nombre a dirección IPv4 en el switch o el router. El comando **ipv6 host** se usa para realizar las mismas asignaciones en IPv6. En la figura 1, se demuestran estos comandos. Dado que los números de red IPv6 son largos y difíciles de recordar, el DNS es incluso más importante para IPv6 que para IPv4.

Para visualizar la información de asignación de nombre a dirección IP en una computadora con Windows, use el comando **nslookup**.

Ejemplo de resolución de problemas

El resultado de la figura 2 indica que el cliente no pudo llegar al servidor DNS o que el servicio DNS en 10.1.1.1 no funcionaba. En este momento, la resolución de problemas se debe centrar en las comunicaciones con el servidor DNS o en verificar que el servidor DNS funcione correctamente.

Para visualizar la información de configuración de DNS en una computadora con Microsoft Windows, use el comando**nslookup**. Debe haber un DNS configurado para IPv4, para IPv6 o para ambos. El DNS puede proporcionar direcciones IPv4 e IPv6 al mismo tiempo, independientemente del protocolo que se use para acceder al servidor DNS.

Debido a que los nombres de dominio y el DNS son un componente fundamental para acceder a los servidores en una red, muchas veces el usuario piensa que “la red está inactiva” cuando, en realidad, el problema se encuentra en el servidor DNS.

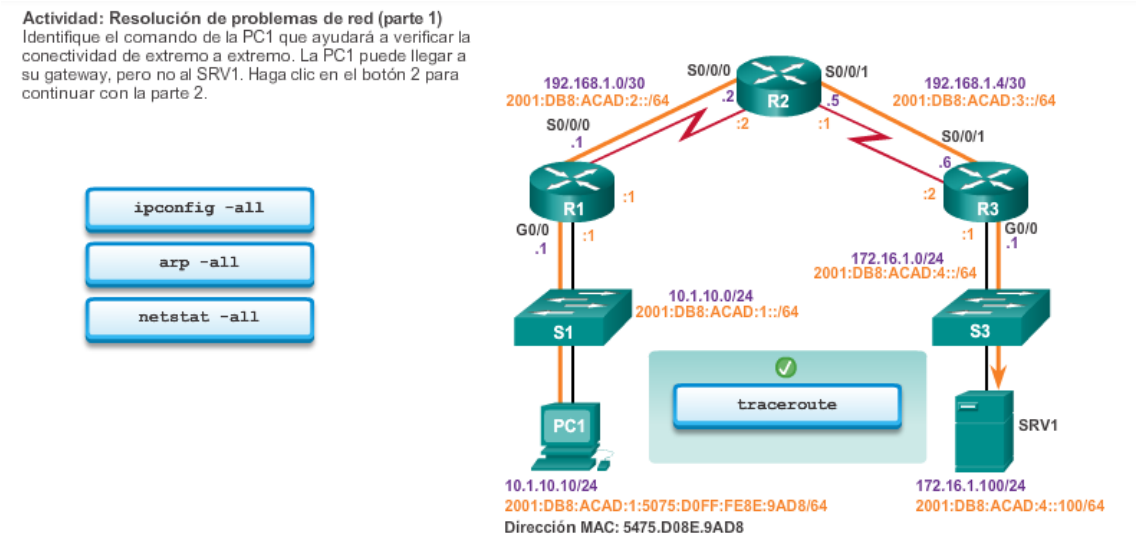
Creación de asignaciones de nombre a dirección IP

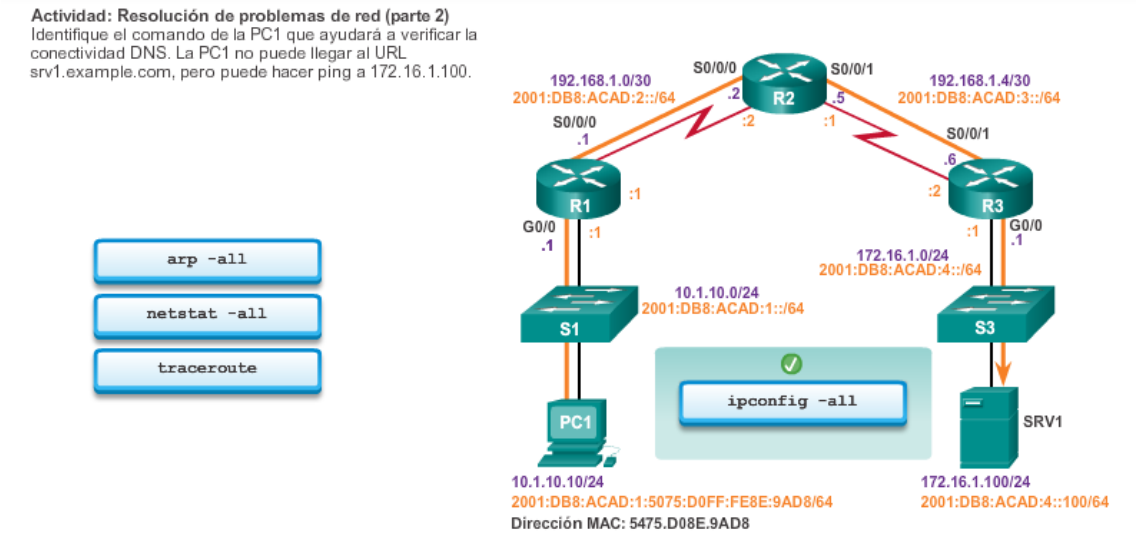
```
R1(config)# ip host ipv4-server 172.16.1.100
R1(config)# exit
R1# ping ipv4-server
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.100,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5),
round-trip min/avg/max = 52/56/64 ms
R1#
R1# conf t
R1(config)# ipv6 host ipv6-server 2001:db8:acad:4::100
R1(config)# exit
R1# ping ipv6-server
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:4::100,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5),
round-trip min/avg/max = 52/54/56 ms
R1#
```

Imposibilidad de llegar al servidor DNS

```
PC1> nslookup Server
*** Request to 10.1.1.1 timed-out
```

Capítulo 9: Resolución de problemas de red 9.2.3.11 Actividad: Identificar los comandos para resolver un problema de red





Capítulo 9: Resolución de problemas de red 9.2.3.12 Packet Tracer: Resolución de problemas de redes empresariales 1

Información básica/situación

En esta actividad, se usa una variedad de tecnologías con las que se encontró durante sus estudios de CCNA, entre ellas, la tecnología VLAN, STP, el routing, el routing entre VLAN, DHCP, NAT, PPP y Frame Relay. Su tarea consiste en revisar los requisitos, aislar y resolver cualquier problema, y después registrar los pasos que siguió para verificar los requisitos.

Packet Tracer: Resolución de problemas de redes empresariales 1 (instrucciones)

Packet Tracer: Resolución de problemas de redes empresariales 1 (PKA)

Capítulo 9: Resolución de problemas de red 9.2.3.13 Packet Tracer: Resolución de problemas de redes empresariales 2

Información básica/situación

En esta actividad, se usan configuraciones de IPv6, incluidas DHCPv6, EIGRPv6 y el routing IPv6 predeterminado. Su tarea consiste en revisar los requisitos, aislar y resolver cualquier problema, y después registrar los pasos que siguió para verificar los requisitos.

Packet Tracer: Resolución de problemas de redes empresariales 2 (instrucciones)

Packet Tracer: Resolución de problemas de redes empresariales 2 (PKA)

Capítulo 9: Resolución de problemas de red 9.2.3.14 Packet Tracer: Resolución de problemas de redes empresariales 3

Información básica/situación

En esta actividad, se usa una variedad de tecnologías con las que se encontró durante sus estudios de CCNA, entre ellas, el routing, la seguridad de puertos, EtherChannel, DHCP, NAT, PPP y Frame Relay. Su tarea consiste en revisar los requisitos, aislar y resolver cualquier problema, y después registrar los pasos que siguió para verificar los requisitos.

Packet Tracer: Resolución de problemas de redes empresariales 3 (instrucciones)

Packet Tracer: Resolución de problemas de redes empresariales 3 (PKA)

Capítulo 9: Resolución de problemas de red 9.2.3.15 Packet Tracer: Desafío de resolución de problemas sobre el uso del registro para resolver problemas

Información básica/situación

Esta es la parte 2 de una actividad que consta de dos partes. La parte 1 es Packet Tracer: Desafío de resolución de problemas sobre la documentación de la red, que debe haber completado anteriormente en el capítulo. En la parte 2, usará sus habilidades de resolución de problemas y el registro de la parte 1 para resolver los problemas de conectividad entre las computadoras.

Packet Tracer: Desafío de resolución de problemas sobre el uso del registro para resolver problemas (instrucciones)

Packet Tracer: Desafío de resolución de problemas sobre el uso del registro para resolver problemas (PKA)

Capítulo 9: Resolución de problemas de red 9.3.1.1 Actividad de clase: Elaboración del registro

Elaboración del registro

Como administrador de red de una pequeña empresa, desea implementar un sistema de registro para usar en la resolución de problemas de red.

Después de pensar mucho, decide recopilar información simple de documentación de red en un archivo que se utilizará cuando surjan problemas de red. También sabe que si la empresa crece en el futuro, se puede usar este archivo para exportar la información a un sistema de software de red computarizado.

Para comenzar el proceso de documentación de red, incluye lo siguiente:

- Un diagrama físico de la red de su pequeña empresa.
- Un diagrama lógico de la red de su pequeña empresa.
- Información de configuración de red para los dispositivos importantes, incluidos routers y switches.

Actividad de clase: Elaboración del registro

Capítulo 9: Resolución de problemas de red 9.3.1.2 Resumen

Para que los administradores de red puedan monitorear y resolver problemas en una red, deben tener un conjunto completo de documentación de red precisa y actual que incluya los archivos de configuración, diagramas de topología física y lógica y un nivel de rendimiento de línea de base.

Las tres etapas principales en la resolución de problemas son la recolección de síntomas, el aislamiento del problema y la corrección del problema. A veces, es necesario implementar temporalmente una solución alternativa al problema. Si la medida correctiva deseada no soluciona el problema, se debe eliminar el cambio. El administrador de red debe registrar todos los pasos del proceso. Para cada etapa, se debe establecer una política de resolución de problemas que incluya procedimientos de control de cambios. Una vez que se resuelve el problema, es importante comunicárselo a los usuarios, a cualquier persona que participe en el proceso de resolución de problemas y a los otros miembros del equipo de TI.

El modelo OSI o el modelo TCP/IP se puede aplicar a un problema de red. Los administradores de red pueden usar el método ascendente, el método descendente o el método divide y vencerás. Otros métodos menos estructurados incluyen prueba y error, detección de las diferencias y sustitución.

Las herramientas de software comunes que pueden ayudar con la resolución de problemas incluyen herramientas de administración de red del sistema, bases de conocimientos, herramientas de línea de base, analizadores de protocolo basados en host y EPC del IOS de Cisco. Las herramientas para la solución de problemas de hardware incluyen NAM, multímetros digitales, comprobadores de cables, analizadores de cables y analizadores de red portátiles. La

información de registro del IOS de Cisco también se puede usar para identificar problemas potenciales.

Existen síntomas y problemas característicos de la capa física, la capa de enlace de datos, la capa de red, la capa de transporte y la capa de aplicación que el administrador de red debe reconocer. Es posible que el administrador necesite prestar especial atención a la conectividad física, los gateways predeterminados, las tablas de direcciones MAC, la NAT y la información de routing.

Pautas para seleccionar un método de resolución de problemas