

CAPÍTULO 11. CREE UNA RED PEQUEÑA

11.1.1.2 Selección de dispositivos para redes pequeñas

Una de las primeras consideraciones de diseño cuando se implementa una red pequeña es el tipo de dispositivos intermediarios que se utilizarán para dar soporte a la red. Al elegir el tipo de dispositivos intermediarios, se deben tener en cuenta varios factores, como se muestra en la ilustración.

Costo

El costo de un switch o un router se determina sobre la base de sus capacidades y características. La capacidad del dispositivo incluye la cantidad y los tipos de puertos disponibles, además de la velocidad de backplane. Otros factores que afectan el costo son las capacidades de administración de red, las tecnologías de seguridad incorporadas y las tecnologías de conmutación avanzadas optativas. También se debe tener en cuenta el costo del tendido de cable necesario para conectar cada dispositivo de la red. Otro elemento clave que afecta las consideraciones de costos es la cantidad de redundancia que se debe incorporar en la red.

Velocidad y tipos de puertos e interfaces

Elegir la cantidad y el tipo de puertos en un router o un switch es una decisión fundamental. Las PC más modernas tienen NIC de 1 Gb/s incorporadas. Algunos servidores y estaciones de trabajo ya vienen con puertos de 10 Gb/s incorporados. Si bien es más costoso, elegir dispositivos de capa 2 que puedan admitir velocidades mayores permite que la red evolucione sin reemplazar los dispositivos centrales.

Capacidad de expansión

Los dispositivos de red incluyen configuraciones físicas modulares y fijas. Las configuraciones fijas tienen un tipo y una cantidad específica de puertos o interfaces. Los dispositivos modulares tienen ranuras de expansión que proporcionan la flexibilidad necesaria para agregar nuevos módulos a medida que aumentan los requisitos. Existen switches con puertos adicionales para uplinks de alta velocidad. Se pueden utilizar routers para conectar diferentes tipos de redes. Se debe tener precaución al seleccionar las interfaces y los módulos adecuados para los medios específicos.

Características y servicios de los sistemas operativos

Según la versión del sistema operativo, los dispositivos de red pueden admitir determinados servicios y características, por ejemplo:

- Seguridad
- Calidad de servicio (QoS)
- Voz sobre IP (VOIP)
- Conmutación de Capa 3
- Traducción de direcciones de red (NAT)
- Protocolo de configuración dinámica de host (DHCP)

11.1.1.3 Direccionamiento IP para redes pequeñas

Al implementar una red pequeña, es necesario planificar el espacio de direccionamiento IP. Todos los hosts dentro de una internetwork deben tener una dirección exclusiva. Se debe planificar, registrar y mantener un esquema de asignación de direcciones IP basado en los tipos de dispositivos que reciben la dirección.

Los siguientes son ejemplos de diferentes tipos de dispositivos que afectan el diseño de IP:

- Dispositivos finales para usuarios
- Servidores y periféricos
- Hosts a los que se accede desde Internet
- Dispositivos intermediarios

La planificación y el registro del esquema de direccionamiento IP ayudan al administrador a realizar un seguimiento de los tipos de dispositivos. Por ejemplo, si se asigna una dirección de host en el rango 50 a 100 a todos los servidores, resulta fácil identificar el tráfico de servidores por dirección IP. Esto puede resultar muy útil al llevar a cabo la resolución de problemas de tráfico de la red mediante un analizador de protocolos.

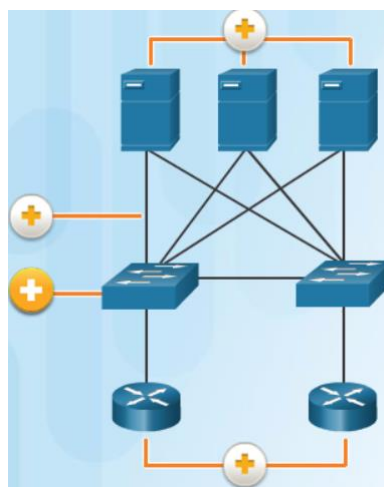
Además, los administradores pueden controlar mejor el acceso a los recursos de la red sobre la base de las direcciones IP cuando se utiliza un esquema de direccionamiento IP determinista. Esto puede ser especialmente importante para los hosts que proporcionan recursos a la red interna y la red externa. Los servidores Web o los servidores de e-commerce cumplen dicha función. Si las direcciones para estos recursos no son planificadas y documentadas, no es posible controlar fácilmente la seguridad y accesibilidad de los dispositivos. Si se asigna una dirección aleatoria a un servidor, resulta difícil bloquear el acceso a esta dirección, y es posible que los clientes no puedan localizar ese recurso.

Cada uno de estos diferentes tipos de dispositivos debería asignarse a un bloque lógico de direcciones dentro del rango de direcciones de la red.

11.1.1.4 Redundancia en redes pequeñas

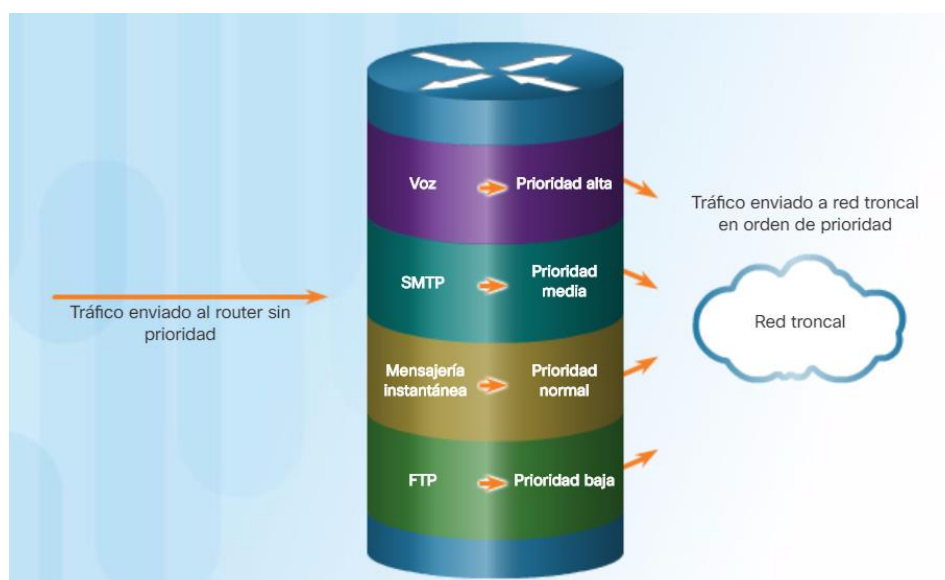
Otra parte importante del diseño de red es la confiabilidad. Incluso las pequeñas empresas, con frecuencia, dependen en gran medida de la red para su operación comercial. Una falla en la red puede tener consecuencias muy costosas. Para mantener un alto grado de confiabilidad, se requiere redundancia en el diseño de red. La redundancia ayuda a eliminar puntos de error únicos. Existen muchas formas de obtener redundancia en una red. La redundancia se puede obtener mediante la instalación de equipos duplicados, pero también se puede obtener al suministrar enlaces de red duplicados en áreas fundamentales, como se muestra en la ilustración.

Por lo general, las redes pequeñas proporcionan un único punto de salida a Internet a través de uno o más gateways predeterminados. Si el router falla, toda la red pierde la conectividad a Internet. Por este motivo, puede ser recomendable para las pequeñas empresas contratar a un segundo proveedor de servicios a modo de respaldo.



11.1.1.5 Administración del tráfico

El administrador de red debe tener en cuenta los diversos tipos de tráfico y su tratamiento en el diseño de la red. Los routers y switches en una red pequeña se deben configurar para admitir el tráfico en tiempo real, como voz y vídeo, de forma independiente del tráfico de otros datos. De hecho, un buen diseño de red clasifica el tráfico cuidadosamente según la prioridad, como se muestra en la ilustración. En definitiva, el objetivo de un buen diseño de red, incluso para una red pequeña, es aumentar la productividad de los empleados y reducir el tiempo de inactividad de la red.



11.1.2.1 Aplicaciones comunes

La utilidad de las redes depende de las aplicaciones que se encuentren en ellas. Hay dos formas de procesos o programas de software que proporcionan acceso a la red: las aplicaciones de red y los servicios de la capa de aplicación.

Aplicaciones de red

Las aplicaciones son los programas de software que se utilizan para comunicarse a través de la red. Algunas aplicaciones de usuario final reconocen la red, lo que significa que implementan los protocolos de la capa de aplicación y pueden comunicarse directamente con las capas inferiores del stack de protocolos. Los clientes de correo electrónico y los navegadores web son ejemplos de este tipo de aplicaciones.

Servicios de la capa de aplicación

Otros programas pueden necesitar la asistencia de los servicios de la capa de aplicación para utilizar recursos de red, como la transferencia de archivos o la administración de las colas de impresión en la red. Si bien el empleado no se da cuenta, estos servicios son los programas que interactúan con la red y preparan los datos para la transferencia. Los distintos tipos de datos, ya sean de texto, gráficos o vídeo, requieren distintos servicios de red para asegurar que estén correctamente preparados para que los procesen las funciones que se encuentran en las capas inferiores del modelo OSI.

Cada servicio de red o aplicación utiliza protocolos que definen los estándares y los formatos de datos que se deben utilizar. Sin protocolos, la red de datos no tendría una manera común de formatear y direccionar los datos. Es necesario familiarizarse con los protocolos subyacentes que rigen la operación de los diferentes servicios de red para entender su función.

Utilice el Administrador de tareas para ver las aplicaciones, los procesos y los servicios en ejecución en una PC Windows.

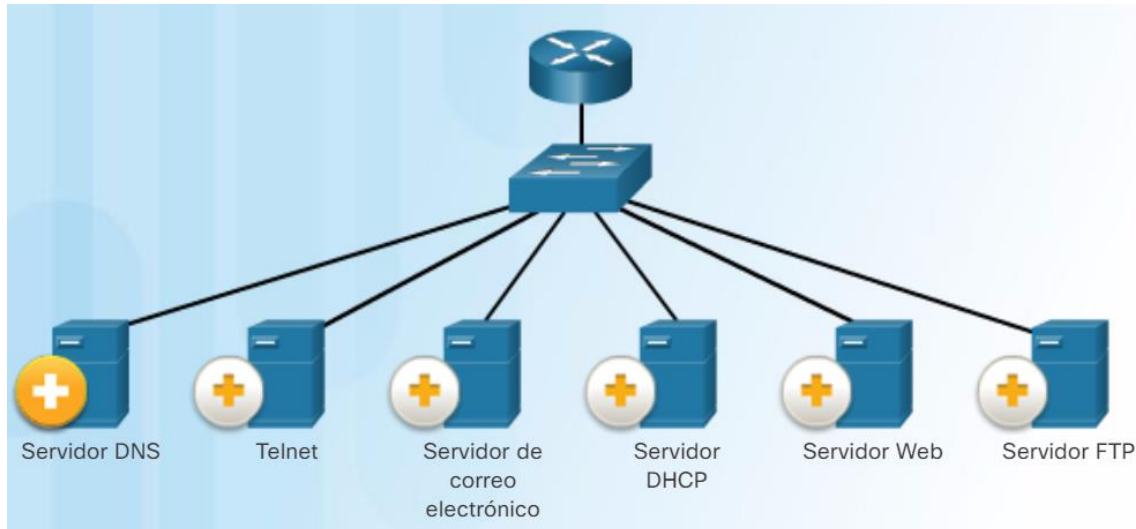
11.1.2.2 Protocolos comunes

La mayor parte del trabajo de un técnico, ya sea en una red pequeña o una red grande, está relacionada de alguna manera con los protocolos de red. Los protocolos de red admiten los servicios y aplicaciones que usan los empleados en una red pequeña. Los protocolos de red comunes se muestran en la figura. Haga clic en cada servidor para obtener una breve descripción.

Estos protocolos de red conforman el conjunto de herramientas fundamental de los profesionales de red. Cada uno de estos protocolos de red define lo siguiente:

- Procesos en cualquier extremo de una sesión de comunicación.
- Tipos de mensajes.
- La sintaxis de los mensajes
- Significado de los campos informativos.
- Cómo se envían los mensajes y la respuesta esperada.
- Interacción con la capa inferior siguiente.

Muchas empresas establecieron una política de utilización de versiones seguras de estos protocolos, siempre que sea posible. Estos protocolos son HTTPS, SFTP y SSH.



- **Servidor DNS:** sistema de nombres de dominio (DNS): Servicio que brinda la dirección IP de un sitio web o el nombre de dominio para que un host pueda conectarse a él.
- **Telnet:** servicio que permite a los administradores iniciar sesión en un host desde una ubicación remota y controlarlo como si estuviesen conectados de manera local.
- **Servidor de correo electrónico:**
 - Utiliza el protocolo simple de transferencia de correo (SMTP), el protocolo de oficina de correo (POP3) o el protocolo de acceso a mensajes de Internet (IMAP).
 - Se usa para enviar correos electrónicos de clientes a servidores a través de Internet.
 - Los receptores están identificados con el formato usuario@xyz.
- **Servidor Protocolo de configuración dinámica de host (DHCP):** servicio que asigna a los clientes una dirección IP, una máscara de subred, una puerta de enlace predeterminada y otros datos.
- **Servidor Web:**
 - Se usa para transferir entre clientes web y servidores web.
 - Se accede a la mayoría de las páginas web con el protocolo de transferencia de hipertexto (HTTP).
- **Servidor Protocolo de transferencia de archivos (FTP):** servicio que permite descargar y subir archivos entre clientes y el servidor.

11.1.2.3 Aplicaciones de voz y vídeo

El administrador de red debe asegurarse de que se instalen los equipos adecuados en la red y que se configuren los dispositivos de red para asegurar la entrega según las prioridades.

Infraestructura

Para admitir las aplicaciones en tiempo real propuestas y existentes, la infraestructura debe adaptarse a las características de cada tipo de tráfico. El diseñador de red debe determinar si los switches y el cableado existentes pueden admitir el tráfico que se agregará a la red.

VoIP

Los dispositivos VoIP convierten la entrada analógica en paquetes IP digitales. Los dispositivos pueden ser un adaptador de teléfono analógico (ATA) conectado entre un teléfono analógico tradicional y un switch Ethernet. Una vez que las señales se convierten en paquetes IP, el router envía dichos paquetes entre las ubicaciones correspondientes. VoIP es mucho más económico que una solución de telefonía IP integrada, pero la calidad de las comunicaciones no cumple con los mismos estándares.

Telefonía IP

En la telefonía IP, el teléfono IP propiamente dicho realiza la conversión de voz a IP. En las redes con solución de telefonía IP integrada, no se requieren routers con capacidades de voz. Los teléfonos IP utilizan un servidor dedicado para el control y la señalización de llamadas.

Aplicaciones en tiempo real

Para transportar streaming media de manera eficaz, la red debe ser capaz de admitir aplicaciones que requieran entrega dependiente del factor tiempo. El Protocolo de transporte en tiempo real (RTP, Real-Time Transport Protocol) y el Protocolo de control de transporte en tiempo real (RTCP, Real-Time Transport Control Protocol) admiten este requisito.

RTP y RTCP habilitan el control y la escalabilidad de los recursos de red al permitir la incorporación de mecanismos de calidad de servicio (QoS). Estos mecanismos de QoS proporcionan herramientas valiosas para minimizar problemas de latencia en aplicaciones de streaming en tiempo real.

11.1.3.1 Crecimiento de las pequeñas redes

El crecimiento es un proceso natural para muchas pequeñas empresas, y sus redes deben crecer en consecuencia. En forma ideal, el administrador de red tiene un plazo suficiente para tomar decisiones inteligentes acerca del crecimiento de la red con relación al crecimiento de la empresa.

Para escalar una red, se requieren varios elementos:

- **Documentación de la red:** topología física y lógica.
- **Inventario de dispositivos:** lista de dispositivos que utilizan o conforman la red.
- **Presupuesto:** presupuesto de TI detallado, incluido el presupuesto de adquisición de equipos para el año fiscal.
- **Análisis de tráfico:** se deben registrar los protocolos, las aplicaciones, los servicios y sus respectivos requisitos de tráfico.

Estos elementos se utilizan para fundamentar la toma de decisiones que acompaña el escalamiento de una red pequeña.

11.1.3.2 Análisis de protocolos

Al intentar determinar cómo administrar el tráfico de la red, en especial a medida que esta crece, es importante comprender el tipo de tráfico que atraviesa la red y el flujo de tráfico actual. Si se desconocen los tipos de tráfico, un analizador de protocolos ayuda a identificar el tráfico y su origen.

Para determinar patrones de flujo de tráfico, es importante:

- Capturar tráfico en horas de uso pico para obtener una buena representación de los diferentes tipos de tráfico.
- Realizar la captura en diferentes segmentos de la red; parte del tráfico será local en un segmento en particular.

La información recopilada por el analizador de protocolos se evalúa de acuerdo con el origen y el destino del tráfico, y con el tipo de tráfico que se envía. Este análisis puede utilizarse para tomar decisiones acerca de cómo administrar el tráfico de manera más eficiente. Para hacerlo, se pueden reducir los flujos de tráfico innecesarios o modificar completamente los patrones de flujo mediante el traslado de un servidor, por ejemplo.

En ocasiones, simplemente reubicar un servidor o un servicio en otro segmento de red mejora el rendimiento de la red y permite adaptarse a las necesidades del tráfico creciente. Otras veces, la optimización del rendimiento de la red requiere el rediseño y la intervención de la red principal.

11.1.3.3 Utilización de la red por parte de los empleados

Además de comprender las tendencias cambiantes del tráfico, los administradores de red también deben ser conscientes de cómo cambia el uso de la red. Como se muestra en la ilustración, los administradores de redes pequeñas tienen la capacidad de obtener “instantáneas” de TI en persona del uso de aplicaciones por parte de los empleados para una porción considerable de la fuerza laboral a través del tiempo. Generalmente, estas instantáneas incluyen la siguiente información:

- SO y versión del SO
- Aplicaciones Non-Network
- Aplicaciones de red
- Uso de CPU
- Utilización de unidades
- Utilización de RAM

El registro de instantáneas de los empleados en una red pequeña durante un período determinado resulta muy útil para informar al administrador de red sobre la evolución de los requisitos de los protocolos y los flujos de tráfico relacionados. Un cambio en la utilización de recursos puede requerir que el administrador de red ajuste la asignación de los recursos de red en consecuencia.

11.2.1.1 Tipos de amenazas

Los intrusos pueden acceder a una red a través de vulnerabilidades de software, ataques de hardware o descifrando el nombre de usuario y la contraseña de alguien. Por lo general, a los intrusos que obtienen acceso mediante la modificación del software o la explotación de las vulnerabilidades del software se los denomina piratas informáticos.

Una vez que un pirata informático obtiene acceso a la red, pueden surgir cuatro tipos de amenazas:

- Robo de información.
- Pérdida y manipulación de datos.
- Robo de identidad.
- Interrupción del servicio.

11.2.1.2 Seguridad física

Las cuatro clases de amenazas físicas son las siguientes:

- **Amenazas de hardware:** daño físico a servidores, routers, switches, planta de cableado y estaciones de trabajo
- **Amenazas ambientales:** extremos de temperatura (demasiado calor o demasiado frío) o extremos de humedad (demasiado húmedo o demasiado seco)
- **Amenazas eléctricas:** picos de voltaje, suministro de voltaje insuficiente (apagones parciales), alimentación sin acondicionamiento (ruido) y caída total de la alimentación
- **Amenazas de mantenimiento:** manejo deficiente de componentes eléctricos clave (descarga electrostática), falta de repuestos críticos, cableado y etiquetado deficientes

11.2.1.3 Tipos de vulnerabilidades

La vulnerabilidad es el grado de debilidad inherente a cada red y dispositivo. Esto incluye routers, switches, computadoras de escritorio, servidores e, incluso, dispositivos de seguridad. Por lo general, los dispositivos de red que sufren ataques son las terminales, como los servidores y las computadoras de escritorio.

Existen tres vulnerabilidades o debilidades principales:

- Tecnológicas, como las que se muestran en la figura 1.
- De configuración, como las que se muestran en la figura 2.
- De política de seguridad, como las que se muestran en la figura 3.

Debilidades de la seguridad de red

Debilidad del protocolo TCP/IP

- El protocolo de transferencia de hipertexto (HTTP), el protocolo de transferencia de archivos (FTP) y el protocolo de mensajes de control de Internet (ICMP) son inseguros por naturaleza.
- El protocolo simple de administración de redes (SNMP) y el protocolo simple de transferencia de correo (SMTP) se relacionan con la estructura intrínsecamente insegura sobre la que se diseñó TCP.

Debilidad de los sistemas operativos

- Cada sistema operativo tiene problemas de seguridad que se deben resolver.
- UNIX, Linux, Mac OS, Mac OS X, Windows Server 2012, Windows 7, Windows 8
- Están registrados en los archivos del Computer Emergency Response Team (CERT) en <http://www.cert.org>.

Debilidad de los equipos de red

Los diversos tipos de equipos de red, como routers, firewalls y switches, tienen debilidades de seguridad que deben identificarse y evitarse. Sus debilidades incluyen la protección de contraseñas, la falta de autenticación, los protocolos de routing y los agujeros de firewall.

Debilidad en la configuración	Cómo se aprovecha la debilidad
Cuentas de usuario no seguras	La información de la cuenta de usuario se puede transmitir de manera insegura a través de la red. Esto expone nombres de usuario y contraseñas a los curiosos.
Cuentas del sistema con contraseñas fáciles de adivinar	Este problema común se debe a la elección de contraseñas de usuario deficientes y fáciles de adivinar.
Servicios de Internet mal configurados	Un problema común es activar JavaScript en los navegadores web, lo que permite ataques mediante scripts hostiles cuando se accede a sitios no confiables. Otras posibles fuentes de debilidades incluyen los servicios de terminal mal configurados, FTP o los servidores web (p. ej., Microsoft Internet Information Services (IIS), servidor HTTP Apache).
Configuraciones predeterminadas no seguras dentro de productos	Muchos productos tienen configuraciones predeterminadas que habilitan los agujeros de seguridad.
Equipos de red mal configurados	Las malas configuraciones del propio equipo pueden causar problemas de seguridad importantes. Por ejemplo, las listas de acceso mal configuradas, los protocolos de routing o las cadenas comunitarias SNMP pueden abrir enormes agujeros de seguridad.

Debilidad en las políticas	Cómo se aprovecha la debilidad
Falta de políticas de seguridad por escrito	Una política no escrita no se puede aplicar sistemáticamente ni se puede hacer cumplir.
Política	Las batallas políticas y las luchas territoriales pueden dificultar la implementación de una política de seguridad sistemática.
Falta de continuidad de autenticación	Las contraseñas mal elegidas, las contraseñas fáciles de decodificar o las contraseñas predeterminadas pueden permitir el acceso no autorizado a la red.
Controles de acceso lógico no aplicados	El monitoreo y la auditoría inadecuados permiten que los ataques y el uso no autorizado continúen. Esto hace que la empresa desperdicie recursos. Esto puede ocasionar acciones legales o despidos de los técnicos de TI, de la administración de TI o hasta de los directores de la empresa que permiten que estas condiciones no seguras persistan.
La instalación de software y hardware y los cambios no respetan la política	Los cambios no autorizados que se realizan en la topología de la red o la instalación de aplicaciones no aprobadas crean agujeros de seguridad.
No existe plan de recuperación tras un desastre	La falta de un plan de recuperación tras un desastre produce caos, pánico y confusión cuando alguien ataca la empresa.

11.2.2.1 Tipos de malware

El malware (código malicioso) es la abreviatura de software malicioso. Se trata de código o software que está específicamente diseñado para dañar, alterar, robar o infligir acciones “malas” o ilegítimas en los datos, hosts o redes. Los virus, gusanos y caballos de Troya son tipos de malware.

Virus

Un virus informático es un tipo de malware que se propaga mediante la inserción de una copia de sí mismo en otro programa, del que pasa a formar parte. Se propaga de una computadora a otra, dejando infecciones a medida que viaja. Los virus pueden variar en gravedad, desde provocar efectos ligeramente molestos hasta dañar datos o programas y causar condiciones de denegación de servicio (DoS). Casi todos los virus se adjuntan a un archivo ejecutable, lo que significa que el virus puede existir en un sistema pero no estará activo ni será capaz de propagarse hasta que un usuario ejecute o abra el archivo o programa host malicioso.

Cuando se ejecuta el código del host, el código viral se ejecuta también. Por lo general, el programa anfitrión sigue funcionando después de ser infectado por el virus. Sin embargo, algunos virus sobrescriben otros programas con copias de sí mismos, lo que destruye el programa host por completo. Los virus se propagan cuando el software o el documento al que están unidos se transfiere de una computadora a otra a través de la red, un disco, adjuntos de correo electrónico infectados o al compartir archivos.

Gusanos

Los gusanos informáticos son similares a los virus en que se replican en copias funcionales de sí mismos y pueden causar el mismo tipo de daño. A diferencia de los virus, que requieren la propagación de un archivo host infectado, los gusanos son software independiente y no requieren de un programa host ni de la ayuda humana para propagarse. Un gusano no necesita unirse a un programa para infectar un host y entrar en una computadora a través de una vulnerabilidad en el sistema. Los gusanos se aprovechan de las características del sistema para viajar a través de la red sin ayuda.

Caballos de Troya

Un caballo de Troya es otro tipo de malware que lleva el nombre del caballo de madera que los griegos utilizaron para infiltrarse en Troya. Es una pieza de software dañino que parece legítimo. Los usuarios suelen ser engañados para cargarlo y ejecutarlo en sus sistemas. Después de que se active, puede lograr una variedad de ataques contra el anfitrión, desde irritar al usuario (haciendo aparecer ventanas o cambiando de escritorios) hasta dañar el host (eliminación de archivos, robo de datos, o activación y difusión de otros tipos de malware, como virus).

Los caballos de Troya también son conocidos por crear puertas traseras para que usuarios maliciosos puedan acceder al sistema. A diferencia de los virus y gusanos, los caballos de Troya no se reproducen al infectar otros archivos, ni se autorepican. Los caballos de Troya se deben distribuir a través de las interacciones con el usuario, tales como abrir un adjunto de correo electrónico o descargar y ejecutar un archivo desde internet.

11.2.2.2 Ataques de reconocimiento

Además de los ataques de código malintencionado, es posible que las redes sean presa de diversos ataques de red. Los ataques de red pueden clasificarse en tres categorías principales:

- **Ataques de reconocimiento:** detección y esquematización de sistemas, servicios o vulnerabilidades.
- **Ataques de acceso:** manipulación no autorizada de datos, de accesos al sistema o de privilegios de usuario.
- **Denegación de servicio:** consisten en desactivar o dañar redes, sistemas o servicios.

Para los ataques de reconocimiento, los atacantes externos pueden utilizar herramientas de Internet, como las utilidades **nslookup** y **whois**, para determinar fácilmente el espacio de direcciones IP asignado a una empresa o a una entidad determinada. Una vez que se determina el espacio de direcciones IP, un atacante puede hacer ping a las direcciones IP públicamente disponibles para identificar las direcciones que están activas.

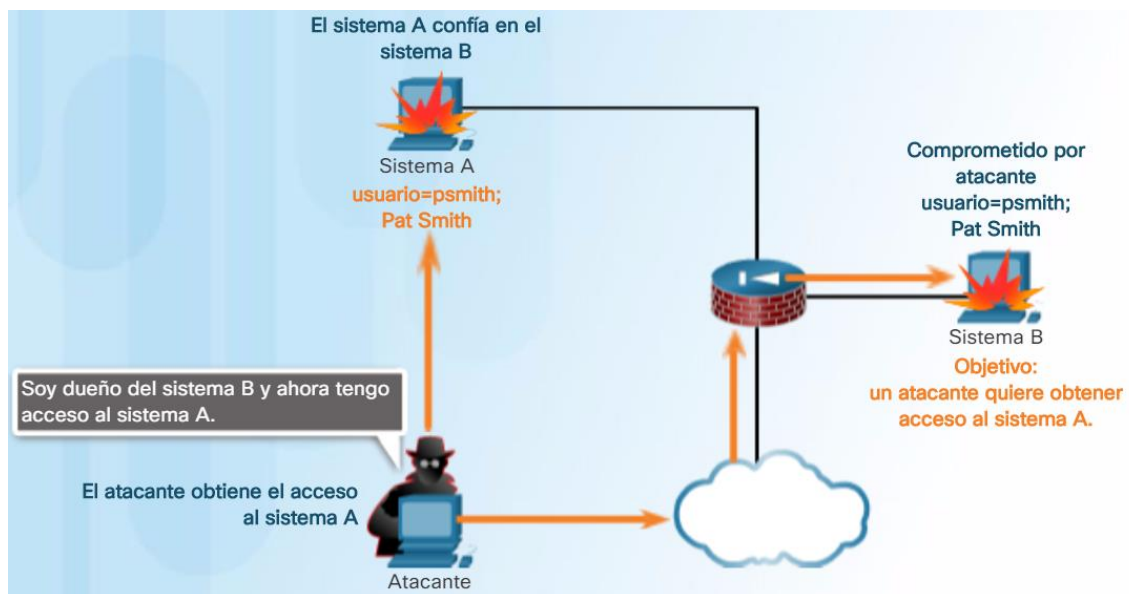
Para contribuir a la automatización de este paso, un atacante puede utilizar una herramienta de barrido de ping, como *fping* o *gping*, que hace ping sistemáticamente a todas las direcciones de red en un rango o una subred determinados. Esto es similar a revisar una sección de una guía telefónica y llamar a cada número para ver quién atiende.

11.2.2.3 Ataques con acceso

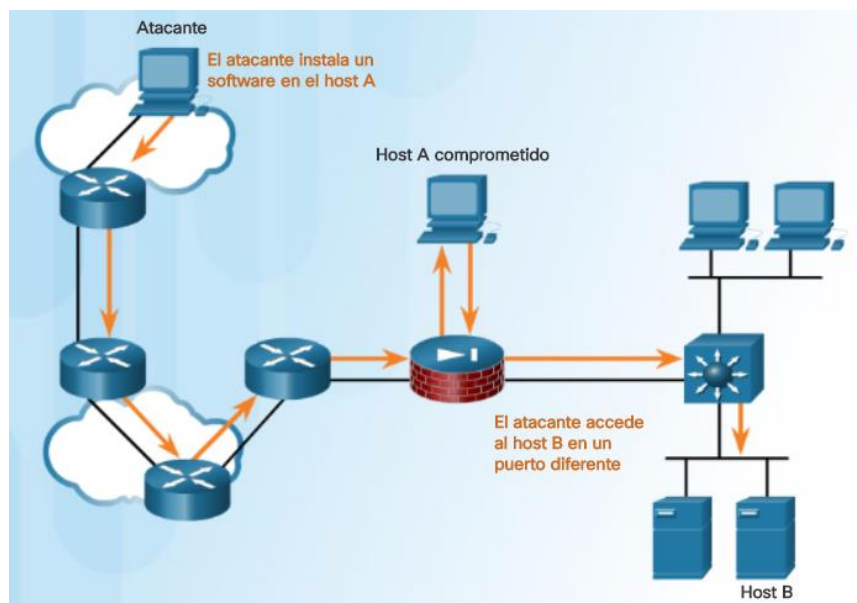
Los ataques de acceso explotan las vulnerabilidades conocidas de los servicios de autenticación, los servicios FTP y los servicios Web para obtener acceso a las cuentas Web, a las bases de datos confidenciales y demás información confidencial. Un ataque de acceso permite que una persona obtenga acceso no autorizado a información que no tiene derecho a ver. Los ataques de acceso pueden clasificarse en cuatro tipos:

- Ataques de contraseña
- Explotación de confianza (figura 1)
- Redireccionamiento de puertos (figura 2)
- Man-in-the-middle (intermediario) (figura 3)

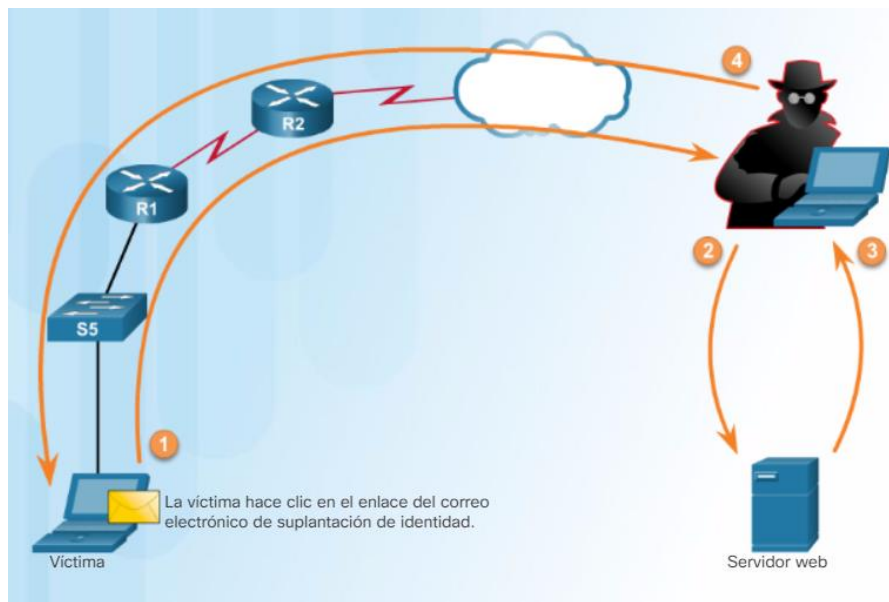
Explotación de confianza



Redireccionamiento de puertos



Man in the middle



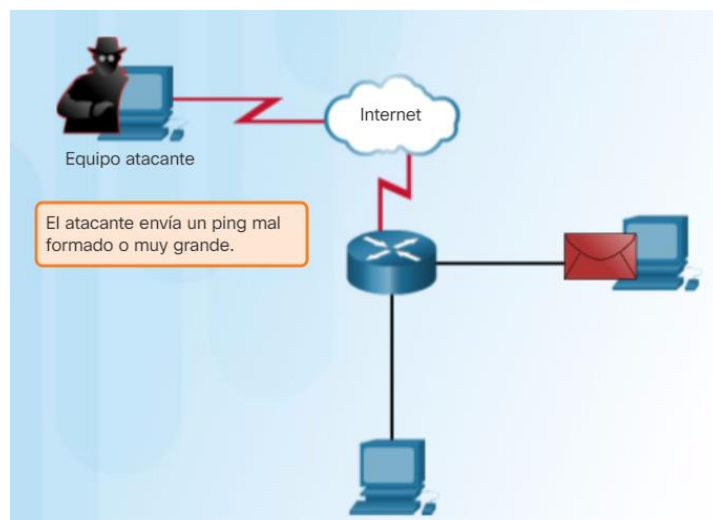
11.2.2.4 Ataques por denegación de servicio

Los ataques por denegación de servicio (DoS) son la forma de ataque más conocida y también están entre los más difíciles de eliminar. Incluso dentro de la comunidad de atacantes, los ataques DoS se consideran triviales y están mal vistos, ya que requieren muy poco esfuerzo de ejecución. Sin embargo, debido a la facilidad de implementación y a los daños potencialmente considerables, los administradores de seguridad deben prestar especial atención a los ataques DoS.

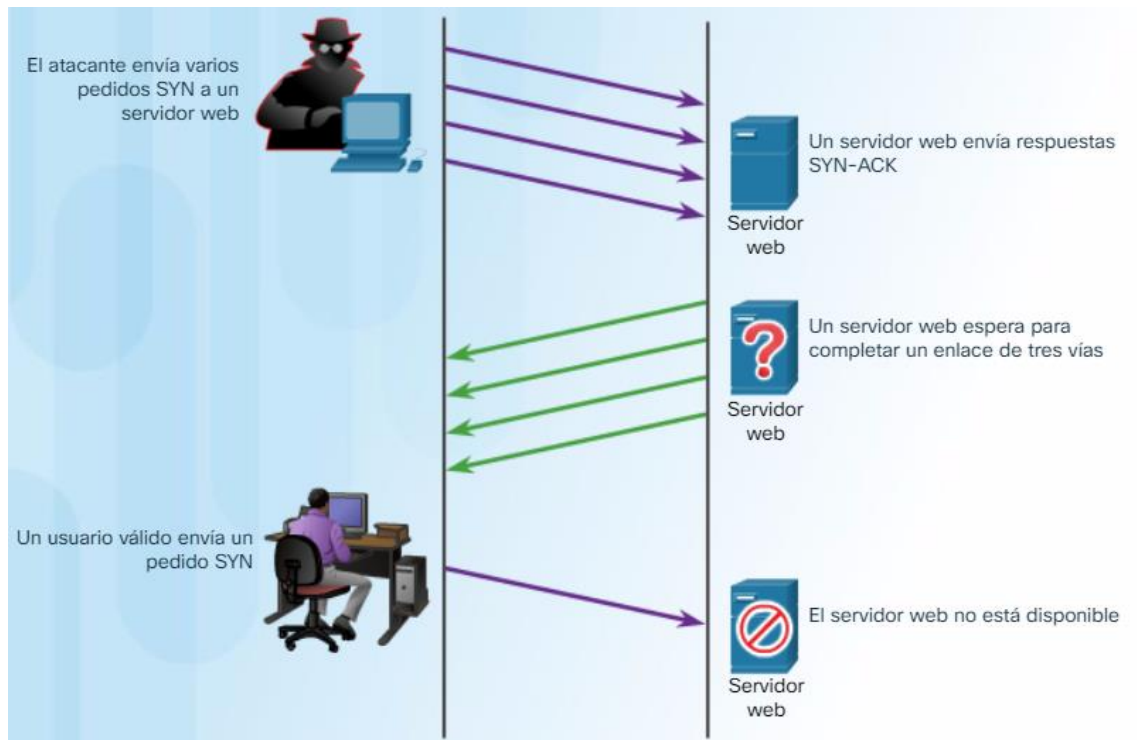
Los ataques DoS tienen muchas formas. Fundamentalmente, evitan que las personas autorizadas utilicen un servicio mediante el consumo de recursos del sistema.

Para prevenir los ataques de DoS es importante estar al día con las actualizaciones de seguridad más recientes de los sistemas operativos y las aplicaciones. Por ejemplo, el ping de la muerte ya no es una amenaza debido a que las actualizaciones de los sistemas operativos han corregido la vulnerabilidad que atacaba.

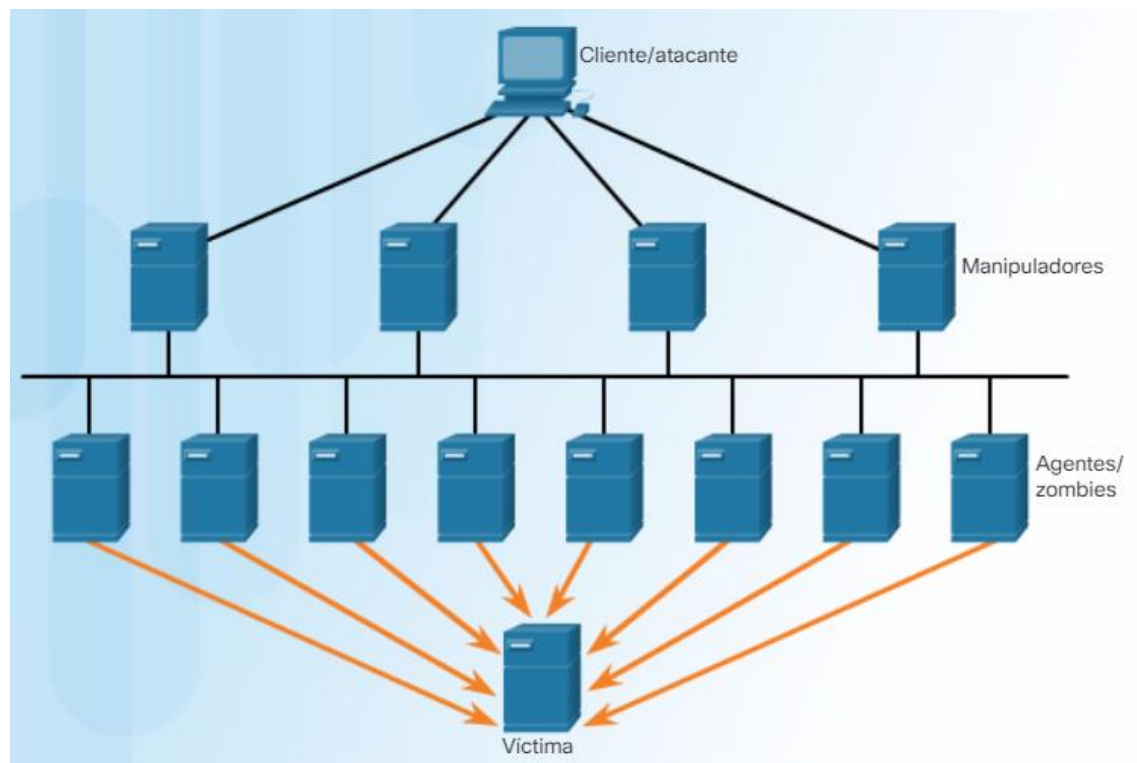
Ping de la muerte

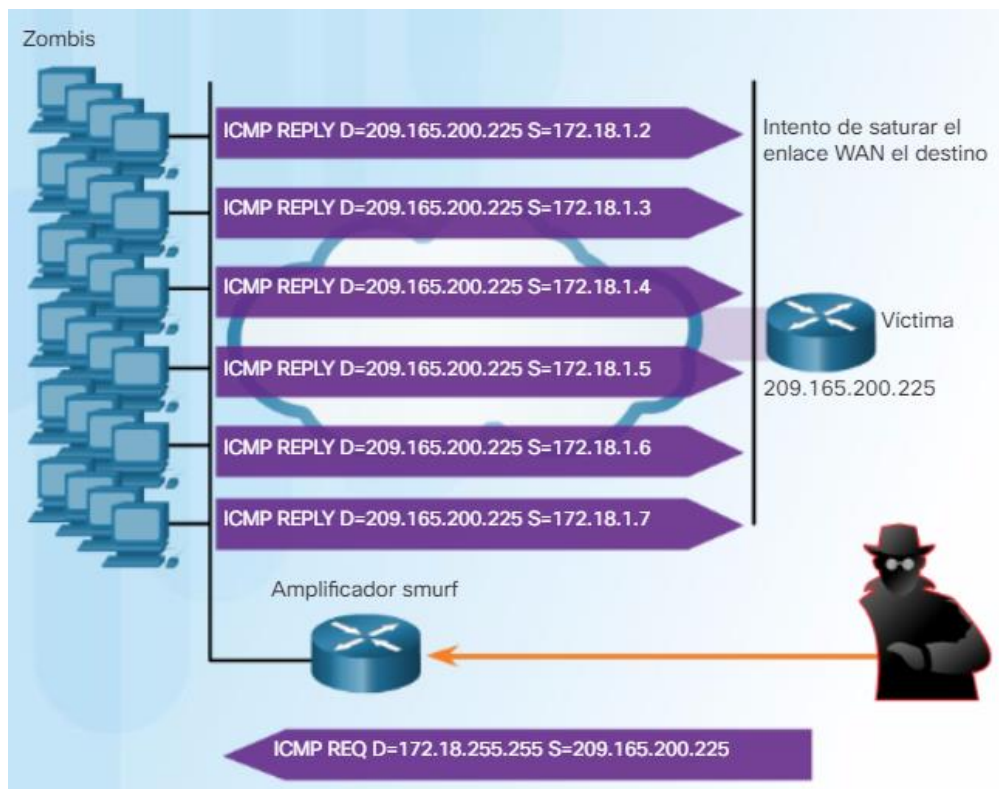


Saturación de SYN



DDos





Ataque Smurf

11.2.3.1 Copias de respaldo, actualizaciones y parches

La manera más eficaz de mitigar un ataque de gusanos consiste en descargar las actualizaciones de seguridad del proveedor del sistema operativo y aplicar parches a todos los sistemas vulnerables. La administración de numerosos sistemas implica la creación de una imagen de software estándar (sistema operativo y aplicaciones acreditadas cuyo uso esté autorizado en los sistemas cliente) que se implementa en los sistemas nuevos o actualizados. Sin embargo, los requisitos de seguridad cambian, y es posible que se deban instalar parches de seguridad actualizados en los sistemas que ya están implementados.

Una solución para la administración de parches críticos de seguridad es crear un servidor central de parches con el que deban comunicarse todos los sistemas después de un período establecido. Todo parche que no esté aplicado en un host se descarga automáticamente del servidor de parches y se instala sin que intervenga el usuario.

11.2.3.2 Autenticación, autorización y registro (Authentication, Authorization and Accounting)

Los servicios de seguridad de red de autenticación, autorización y contabilidad (AAA o “triple A”) proporcionan el marco principal para configurar el control de acceso en dispositivos de red. AAA es un modo de controlar quién tiene permitido acceder a una red (autenticar), controlar lo que las personas pueden hacer mientras se encuentran allí (autorizar) y qué acciones realizan mientras acceden a la red (contabilizar).

11.2.3.3 Firewalls

El firewall es una de las herramientas de seguridad más eficaces disponibles para la protección de los usuarios contra amenazas externas. Los firewalls de red residen entre dos o más redes, controlan el tráfico entre ellas y evitan el acceso no autorizado. Los firewalls basados en el host, o firewalls personales, se instalan en los sistemas finales. Los productos de firewall usan diferentes técnicas para determinar qué acceso permitir y qué acceso denegar en una red. Estas técnicas son las siguientes:

- **Filtrado de paquetes:** evita o permite el acceso según las direcciones IP o MAC.
- **Filtrado de aplicaciones:** evita o permite el acceso de tipos específicos de aplicaciones según los números de puerto.
- **Filtrado de URL:** evita o permite el acceso a sitios Web según palabras clave o URL específicos.
- **Inspección activa de estado de paquetes (SPI):** los paquetes entrantes deben constituir respuestas legítimas a solicitudes de los hosts internos. Los paquetes no solicitados son bloqueados, a menos que se permitan específicamente. La SPI también puede incluir la capacidad de reconocer y filtrar tipos específicos de ataques, como los ataques por denegación de servicio (DoS).

Los productos de firewall pueden admitir una o más de estas capacidades de filtrado:

- **Aplicaciones de seguridad de Cisco:** los dispositivos firewall dedicados son computadores especializados que no tienen periféricos ni disco duro. Los firewalls basados en aplicaciones pueden inspeccionar el tráfico con mayor rapidez y son menos propensos a sufrir fallos.
- **Router inalámbrico Linksys firewall integrado:** la mayoría de los routers domésticos integrados tienen capacidades de firewall básicas que admiten filtro de sitios web, aplicaciones y paquetes. Los routers más especializados que ejecutan sistemas operativos especiales como el Sistema Operativo de Internetwork de Cisco (IOS) también tienen capacidades de firewall que se pueden configurar.
- **Firewall basado en servidor:** Aplicaciones de firewall que generalmente proporcionan una solución que combina un firewall SPI y control de acceso basado en direcciones IP o aplicaciones. Los firewalls basados en servidor pueden ser menos seguros que los firewalls dedicados basados en aplicaciones debido a las debilidades de seguridad del OS de uso general.
- **Firewall personal:** Firewalls del lado cliente que normalmente filtran con SPI. El usuario puede tener que decidir si desea permitir la conexión de ciertas aplicaciones o puede definir una lista de excepciones automáticas. Con frecuencia los firewalls personales se utilizan cuando un dispositivo de host se conecta directamente a un módem ISP. Si no están bien configurados pueden interferir en el acceso a Internet. No se recomienda utilizar más de un firewall personal a la vez porque puede haber conflicto entre ellos.

11.2.4.1 Descripción general de seguridad de los dispositivos

Cuando se instala un nuevo sistema operativo en un dispositivo, la configuración de seguridad está establecida en los valores predeterminados. En la mayoría de los casos, ese nivel de seguridad es insuficiente. En los routers Cisco, se puede utilizar la característica Cisco AutoSecure para proteger el sistema. Además, existen algunos pasos simples que se deben seguir y que se aplican a la mayoría de los sistemas operativos:

- Se deben cambiar de inmediato los nombres de usuario y las contraseñas predeterminados.
- Se debe restringir el acceso a los recursos del sistema solamente a las personas que están autorizadas a utilizar dichos recursos.
- Siempre que sea posible, se deben desactivar y desinstalar todos los servicios y las aplicaciones innecesarios.

A menudo, los dispositivos enviados por el fabricante pasaron cierto tiempo en un depósito y no tienen los parches más actualizados instalados. Es importante actualizar todo el software e instalar todos los parches de seguridad antes de la implementación.

11.2.4.3 Prácticas de seguridad básicas

Seguridad adicional de contraseñas

Las contraseñas seguras resultan útiles en la medida en que sean secretas. Se pueden tomar diversas medidas para asegurar que las contraseñas sigan siendo secretas. Mediante el comando de configuración global **service password-encryption**, se evita que las personas no autorizadas vean las contraseñas como texto no cifrado en el archivo de configuración, como se muestra en la ilustración. Este comando provoca el cifrado de todas las contraseñas sin cifrar.

Además, para asegurar que todas las contraseñas configuradas tengan una longitud mínima específica, utilice el comando **security passwords min-length** del modo de configuración global.

Otra forma en la que los piratas informáticos descubren las contraseñas es simplemente mediante ataques de fuerza bruta, es decir, probando varias contraseñas hasta que una funcione. Es posible evitar este tipo de ataques si se bloquean los intentos de inicio de sesión en el dispositivo cuando se produce una determinada cantidad de errores en un lapso específico.

Router(config)# login block-for 120 attempts 3 within 60

Este comando bloquea los intentos de inicio de sesión durante 120 segundos si hay tres intentos de inicio de sesión fallidos en 60 segundos.

Exec Timeout

Otra recomendación es configurar tiempos de espera de ejecución. Al configurar el tiempo de espera de ejecución, le ordena al dispositivo Cisco que desconecte automáticamente a los usuarios en una línea después de que hayan estado inactivos durante el valor de tiempo de espera de ejecución. Los tiempos de espera de ejecución se pueden configurar en los puertos de consola, VTY y auxiliares con el comando **exec-timeout** en el modo de configuración de línea.

```
Router(config)# line vty 0 4
```

```
Router(config-line)# exec-timeout 10
```

Este comando configura el dispositivo para desconectar a los usuarios inactivos después de 10 minutos.

```
Router(config)# service password-encryption
Router(config)# security password min-length 8
Router(config)# login block-for 120 attempts 3 within 60
Router(config)# line vty 0 4
Router(config-line)# exec-timeout 10
Router(config-line)# end
Router# show running-config
- more -
!
line vty 0 4
 password 7 03095A0F034F38435B49150A1819
 exec-timeout 10
 login
```

11.2.4.4 Activar SSH

Telnet no es seguro. Los datos contenidos en un paquete Telnet se transmiten sin cifrar. Por este motivo, se recomienda especialmente habilitar SSH en los dispositivos para obtener un método de acceso remoto seguro. Es posible configurar un dispositivo Cisco para que admita SSH mediante cuatro pasos, como se muestra en la ilustración.

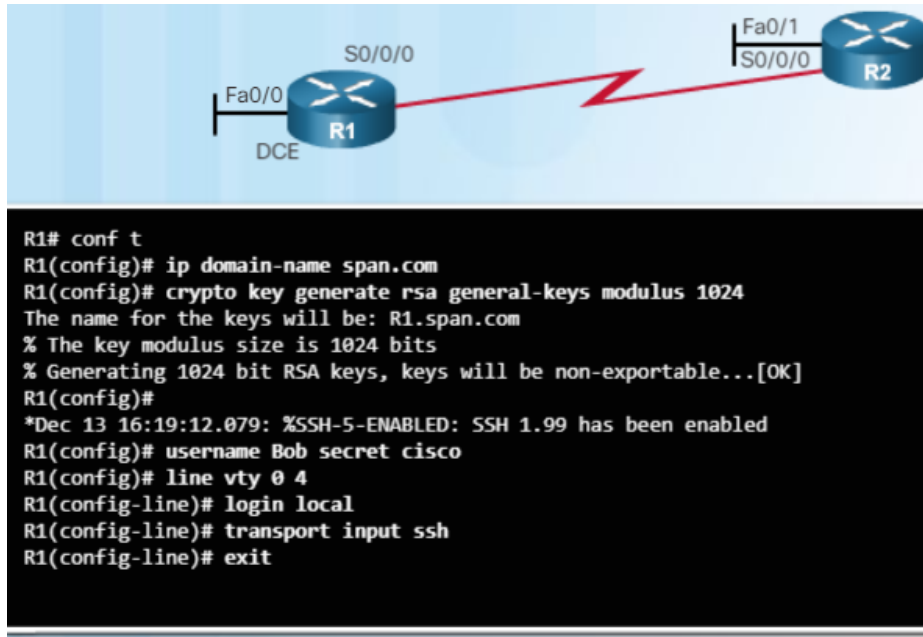
Paso 1. Asegúrese de que el router tenga un nombre de host exclusivo y configure el nombre de dominio IP de la red mediante el comando **ip domain-name** en el modo de configuración global.

Paso 2. Se deben generar claves secretas unidireccionales para que un router cifre el tráfico SSH. Para generar la clave SSH, utilice el comando **crypto key generate rsa general-keys** en el modo de configuración global. El significado específico de las diferentes partes de este comando es complejo y excede el ámbito de este curso. Observe que el módulo determina el tamaño de la clave y se puede configurar de 360 a 2048 bits. Cuanto más grande es el módulo, más segura es la clave, pero más se tarda en cifrar y descifrar la información. La longitud mínima de módulo recomendada es de 1024 bits.

Paso 3. Cree una entrada de nombre de usuario en la base de datos local mediante el comando de configuración global **username**.

Paso 4. Habilite las sesiones SSH entrantes mediante los comandos de línea vty **login local** y **transport input ssh**.

Ahora
puede



se

- Paso 1: Configurar el nombre de dominio IP.
- Paso 2: Generar claves secretas unidireccionales.
- Paso 3: Verificar o crear una entrada de base de datos local.
- Paso 4: Habilitar las sesiones SSH entrantes por VTY.

acceder remotamente al router solo con SSH.

11.3.1.1 Interpretación de los resultados de ping

El comando **ping** es una manera eficaz de probar la conectividad. El comando **ping** utiliza el protocolo de mensajes de control de Internet (ICMP) y verifica la conectividad de la capa 3. El

comando **ping** no siempre identifica la naturaleza de un problema, pero puede contribuir a identificar su origen, un primer paso importante en la resolución de problemas de una falla de red.

Indicadores de ping IOS

Un ping emitido desde el IOS tiene como resultado una de varias indicaciones para cada solicitud de eco ICMP que se envió. Los indicadores más comunes son los siguientes:

- **!** - indica la recepción de un mensaje de respuesta de eco ICMP, como se muestra en la figura 1.
- **.** : indica que se agotó el tiempo mientras se esperaba un mensaje de respuesta de eco ICMP.
- **U**: se recibió un mensaje ICMP inalcanzable.

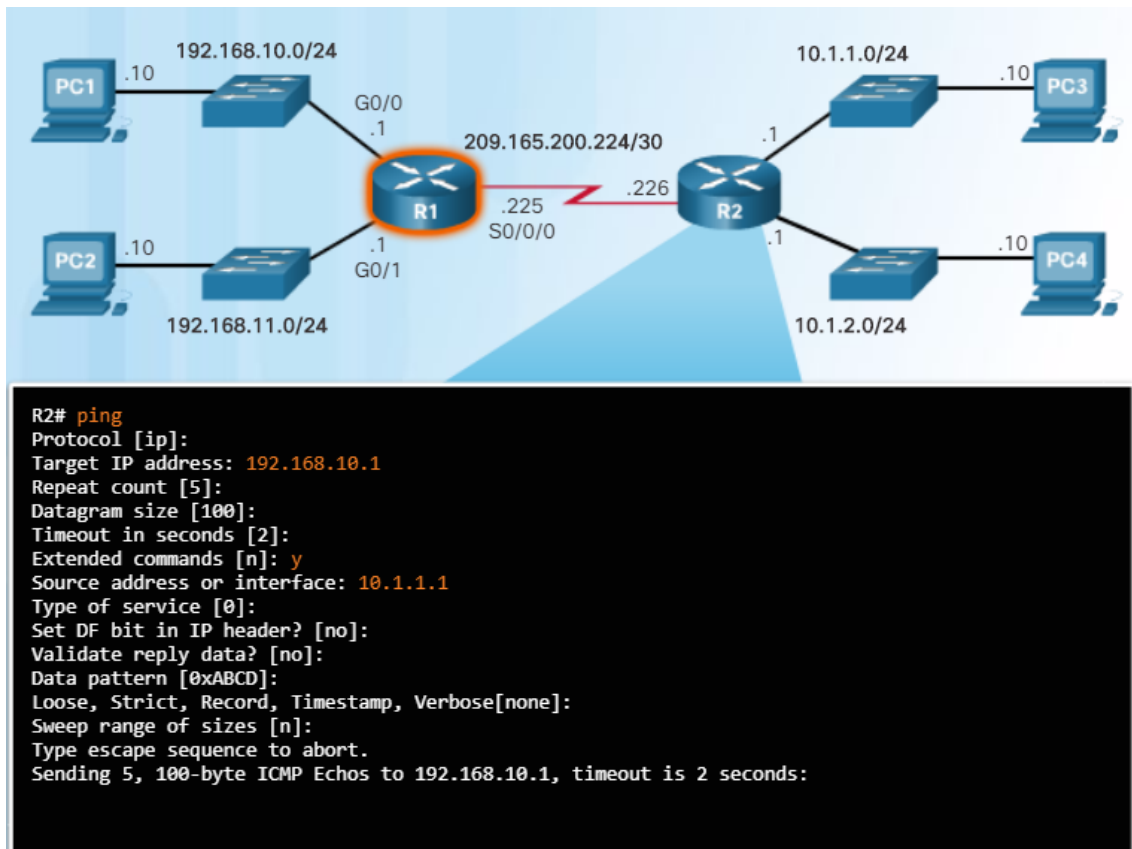
El **"."** (punto) puede señalar que se produjo un problema de conectividad en alguna parte de la ruta. También puede indicar que un router de la ruta no contaba con una ruta hacia el destino y no envió un mensaje de ICMP de destino inalcanzable. También puede señalar que el ping fue bloqueado por la seguridad del dispositivo. Cuando se envía un ping en una LAN Ethernet, es habitual que se agote el tiempo de espera del primer pedido de eco si se requiere el proceso ARP.

La **"U"** indica que un router a lo largo de la ruta respondió con un mensaje ICMP inalcanzable. O bien el router no contaba con una ruta hacia la dirección de destino o se bloqueó la solicitud de ping.

11.3.1.2 Ping extendido

Cisco IOS ofrece un modo "extendido" del comando **ping**. Se ingresa a este modo escribiendo **ping** en el modo EXEC privilegiado, sin una dirección IP de destino. Como se muestra en la figura, a continuación se presenta una serie de peticiones de entrada. Al presionar **Intro** se aceptan los valores predeterminados indicados. El ejemplo muestra cómo forzar que la dirección de origen para un ping sea 10.1.1.1 (observe el R2 en la ilustración); la dirección de origen para un ping estándar sería 209.165.200.226. De esta manera, el administrador de red puede verificar desde el R2 que el R1 tenga la ruta a 10.1.1.0/24.

Nota: El comando **ping ipv6** se utiliza para pings extendidos IPv6.



11.3.1.3 Línea de base de red

Una de las herramientas más efectivas para controlar y resolver problemas relacionados con el rendimiento de la red es establecer una línea de base de red. La creación de una línea de base efectiva del rendimiento de la red se logra con el tiempo. La medición del rendimiento en distintos momentos (figuras 1 y 2) y con distintas cargas ayuda a tener una idea más precisa del rendimiento general de la red.

El resultado derivado de los comandos network aporta datos a la línea de base de red.

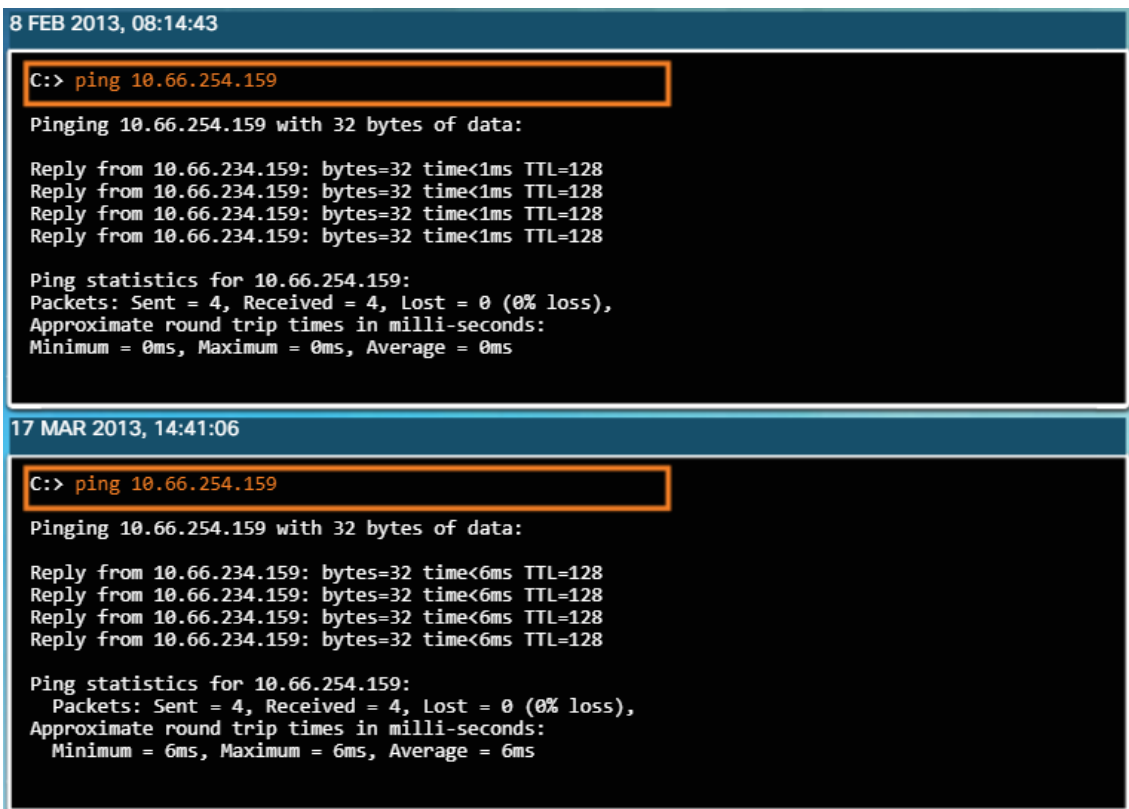
Un método para iniciar una línea de base es copiar y pegar en un archivo de texto los resultados de los comandos **ping**, **trace** u otros comandos relevantes. Estos archivos de texto pueden tener

grabada la fecha y la hora y pueden guardarse en un archivo para su posterior recuperación y comparación (figura 3). Entre los elementos que se deben considerar se encuentran los mensajes de error y los tiempos de respuesta de host a host. Si se observa un aumento considerable de los tiempos de respuesta, es posible que exista un problema de latencia para considerar.

Las redes corporativas deben tener líneas de bases extensas; más extensas de lo que podemos describir en este curso. Existen herramientas de software a nivel profesional para almacenar y mantener información de línea de base. En este curso, se cubren algunas técnicas básicas y se analiza el propósito de las líneas de base.

11.3.2.1 Interpretación de los mensajes de rastreo

Un rastreo proporciona una lista de saltos cuando un paquete se enruta a través de una red. La forma del comando depende de dónde se emita el comando. Cuando lleve a cabo el rastreo desde un equipo con Windows, utilice **tracert**. Cuando lleve a cabo el rastreo desde la CLI de un



```
8 FEB 2013, 08:14:43
C:> ping 10.66.254.159

Pinging 10.66.254.159 with 32 bytes of data:

Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128

Ping statistics for 10.66.254.159:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

17 MAR 2013, 14:41:06
C:> ping 10.66.254.159

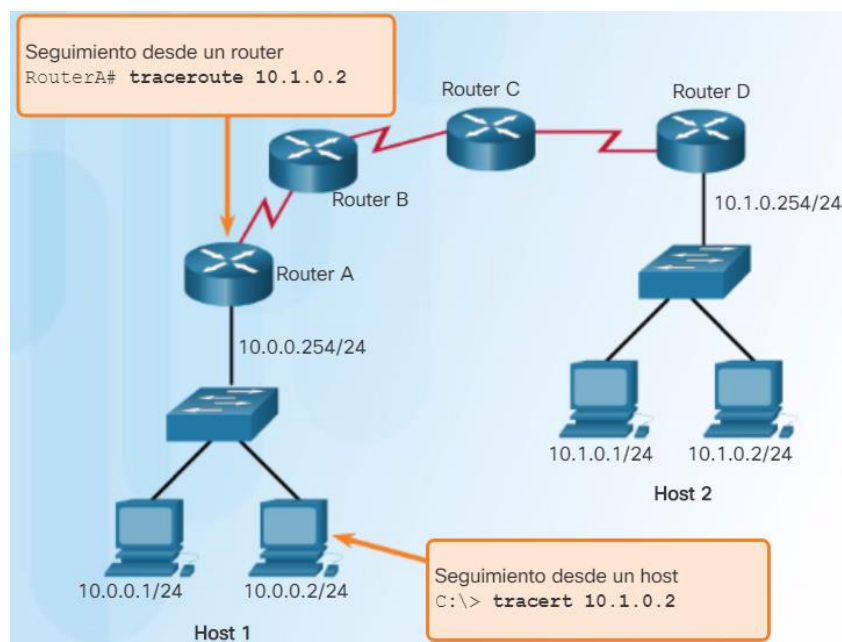
Pinging 10.66.254.159 with 32 bytes of data:

Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128

Ping statistics for 10.66.254.159:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 6ms, Average = 6ms
```

router, utilice **traceroute**, como se muestra en la figura 1.

La figura 2 muestra un ejemplo de respuesta del comando **tracert** introducido en el Host 1 para rastrear la ruta hasta el Host 2. La única respuesta satisfactoria provino del gateway en el Router A. Las solicitudes de rastreo al siguiente salto expiraron, lo cual significa que el siguiente router de salto no respondió. Los resultados del rastreo indican que, o bien hay una falla en la interconexión de redes fuera de la LAN o que esos routers se configuraron para no responder a las solicitudes de eco que se utilizan en el rastreo.



```
C:\> tracert 10.1.0.2
Tracing route to 10.1.0.2 over a maximum of 30 hops
 1  2 ms  2 ms  2 ms  10.0.0.254
 2  * * * Request timed out.
 3  * * * Request timed out.
 4  ^C
C:\>
```

11.3.2.2 Comando extended traceroute

Diseñado como variante del comando **tracert**, el comando **tracert** extendido permite que el administrador ajuste los parámetros relacionados con el funcionamiento del comando. Esto es útil para solucionar problemas de bucles de routing, determinar el router de siguiente salto, o ayudar a determinar dónde los paquetes son descartados por un router o denegados.

por un firewall. Si bien el comando **ping** extendido se puede utilizar para determinar el tipo de problema de conectividad, el comando **tracert** extendido es útil para localizar el problema.

El mensaje de error de tiempo superado de ICMP indica que un router en la ruta ha visto y ha descartado el paquete. El mensaje de error de destino inalcanzable de ICMP indica que un router recibió el paquete, pero lo descartó porque no podía enviarse. Al igual que ping, tracert utiliza solicitudes de eco ICMP y respuestas de eco. Si expira el temporizador ICMP antes de que se reciba una respuesta de eco ICMP, el resultado del comando **tracert** muestra un asterisco (*).

En IOS, el comando tracert extendido finaliza en cualquiera de los siguientes casos:

- El destino responde con una respuesta de eco ICMP
- El usuario interrumpe el seguimiento con la secuencia de escape

Nota: En IOS, puede invocar esta secuencia de escape presionando **Ctrl+Shift+6**. En Windows, la secuencia de escape se invoca presionando **Ctrl+C**.

Para utilizar el comando tracert **extendido**, solo debe escribir **tracert**, sin introducir ningún parámetro, y presionar **ENTER**. IOS lo guiará en las opciones de comando presentando varios indicadores relacionados con la configuración de todos los parámetros diferentes. En la Figura 1, se muestran las opciones de **tracert** extendido y sus respectivas descripciones.

Aunque el comando **tracert** de Windows permite introducir varios parámetros, no es guiado y se debe ejecutar a través de opciones en la línea de comandos. En la Figura 2, se muestran las opciones disponibles para **tracert** en Windows.

Opción	Descripción
Protocol [ip]:	Indicadores para un protocolo admitido. El predeterminado es IPv4
Target IP address:	Debe ingresar un nombre de host o una dirección IPv4. No hay predeterminado.
Source address:	La interfaz o la dirección IPv4 del router para utilizarla como dirección de origen para los sondeos. El router habitualmente elige la dirección IPv4 de la interfaz saliente que va a utilizar.
Numeric display [n]:	De manera predeterminada hay una pantalla simbólica y una numérica; sin embargo, puede eliminar la pantalla simbólica.
Timeout in seconds [3]:	Cantidad de segundos de espera para una respuesta a un paquete de sondeo. El valor predeterminado es 3 de segundos.
Probe count [3]:	La cantidad de sondeos a enviar en cada nivel de TTL. El valor predeterminado es 3.
Minimum Time to Live [1]:	El valor TTL para los primeros sondeos. El valor predeterminado es 1, pero puede estar configurado en un valor más alto para evitar mostrar saltos conocidos.
Maximum Time to Live [30]:	El valor TTL más grande que pueda utilizarse. De manera predeterminada, es 30. El comando traceroute finaliza cuando se llega al destino o se alcanza este valor.
Port Number [33434]:	El puerto de destino utilizado por los mensajes del sondeo UDP. De manera predeterminada, es 33434.
Loose, Strict, Record, Timestamp, Verbose [none]:	Opciones de encabezado IP. Puede especificar cualquier combinación. El comando traceroute emite peticiones para los campos obligatorios. Observe que el comando traceroute colocará las opciones solicitadas en cada sondeo; sin embargo, no hay garantía de que todos los routers (o nodos finales) procesarán las opciones.

```
C:\> tracert
Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
              [-R] [-S srcaddr] [-4] [-6] target_name
Options:
  -d          Do not resolve addresses to hostnames.
  -h maximum_hops  Maximum number of hops to search for target.
  -j host-list  Loose source route along host-list (IPv4-only).
  -w timeout    Wait timeout milliseconds for each reply.
  -R          Trace round-trip path (IPv6-only).
  -S srcaddr    Source address to use (IPv6-only).
  -4          Force using IPv4.
  -6          Force using IPv6.
C:\>
```

11.3.3.1 Repaso de comandos show comunes

Los comandos **show** de la CLI de Cisco IOS muestran información importante sobre la configuración y el funcionamiento del dispositivo.

Los técnicos de red utilizan los comandos **show** con frecuencia para ver los archivos de configuración, revisar el estado de los procesos y las interfaces del dispositivo, y verificar el estado de funcionamiento del dispositivo. Los comandos **show** están disponibles independientemente de si el dispositivo se configuró utilizando la CLI o Cisco Configuration Professional.

Mediante un comando **show** se puede mostrar el estado de casi todo proceso o función del router. Algunos de los comandos **show** más conocidos son:

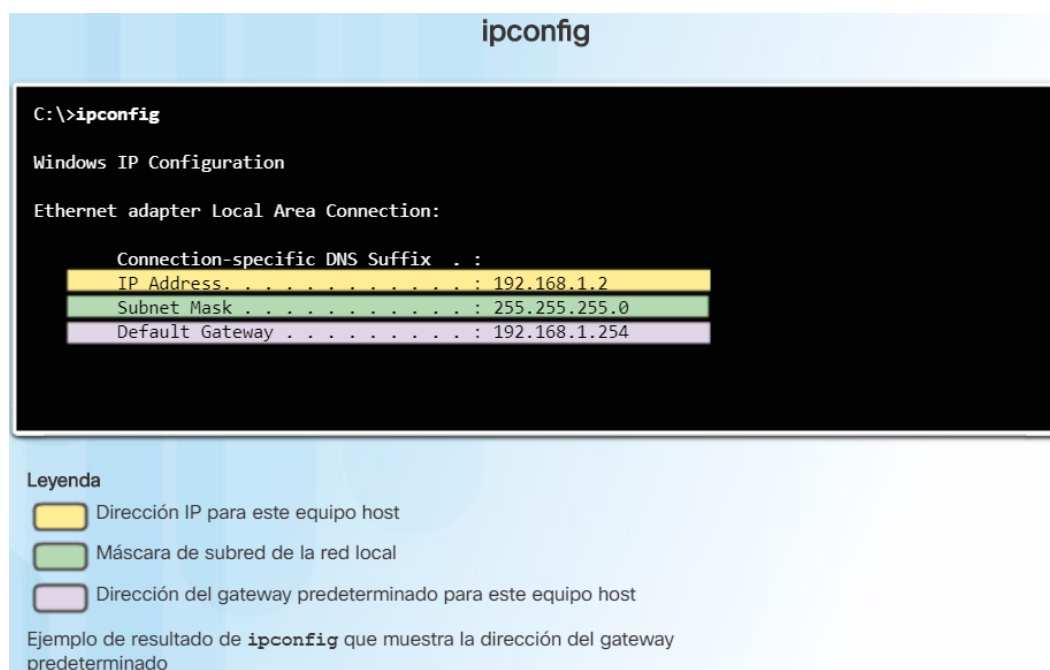
- **show running-config**
- **show interfaces**
- **show arp**
- **show ip route**
- **show protocols**
- **show version**

11.3.4.1 El comando ipconfig

Como se muestra en la figura 1, la dirección IP del gateway predeterminado de un host se puede ver emitiendo el comando **ipconfig** en la línea de comandos de una computadora Windows.

Como se muestra en la Figura 2, utilice el comando **ipconfig /all** para ver la dirección MAC junto con varios detalles relacionados con la asignación de direcciones de capa 3 del dispositivo.

El servicio del cliente DNS en PC con Windows también optimiza el rendimiento de la resolución de nombres DNS al almacenar en la memoria los nombres resueltos previamente. Como se muestra en la Figura 3, el comando **ipconfig /displaydns** muestra todas las entradas DNS en caché en un sistema informático Windows.



```
C:\>ipconfig /all
Ethernet adapter Network Connection:
    Connection-specific DNS Suffix: example.com
    Description . . . . . : Intel(R)
    PRO/Wireless 3945ABG Network Connection
    Physical Address. . . . . : 00-18-DE-C7-F3-FB
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 10.2.3.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.2.3.254
    DHCP Server . . . . . : 10.2.3.69
    DNS Servers . . . . . : 192.168.226.120
    Lease Obtained. . . . . : Thursday, May 03,
                             2007 3:47:51 PM
    Lease Expires . . . . . : Friday, May 04,
                             2007 6:57:11 AM

C:\>
```

```
C:\> ipconfig /displaydns

Windows IP Configuration

    cisco-tags.cisco.com
    -----
    Record Name . . . . . : cisco-tags.cisco.com
    Record Type . . . . . : 1
    Time To Live . . . . . : 44024
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . . : 72.163.10.10

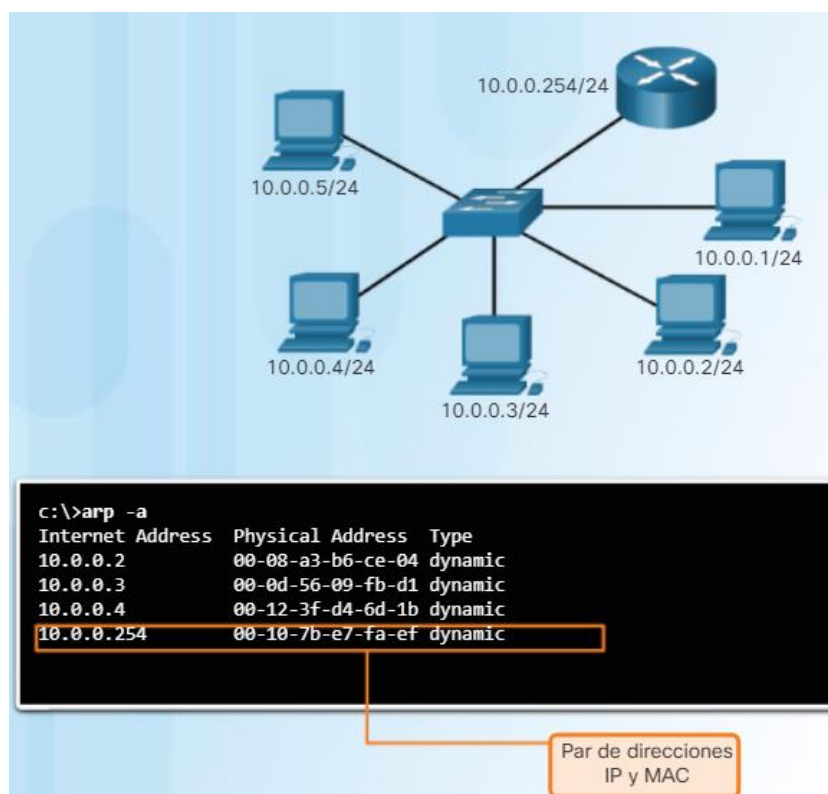
<se omitió el resultado>
```

11.3.4.2 El comando ARP

El comando **arp** se ejecuta desde el símbolo del sistema de Windows, como se muestra en la figura. El comando **arp -a** enumera todos los dispositivos que se encuentran actualmente en la caché ARP del host, lo cual incluye la dirección IPv4, la dirección física y el tipo de direccionamiento (estático/dinámico) para cada dispositivo.

Se puede borrar la caché mediante el comando **arp -d*** en caso de que el administrador de red desee volver a llenarla con información actualizada.

Nota: La caché de ARP solo contiene información de los dispositivos a los que se accedió recientemente. Para asegurar que la caché ARP esté cargada, haga ping a un dispositivo de manera tal que tenga una entrada en la tabla ARP.



11.3.4.3 El comando **show cdp neighbors**

Existen otros comandos IOS que son útiles. Por ejemplo, Cisco Discovery Protocol (CDP) es un protocolo exclusivo de Cisco que se ejecuta en la capa de enlace de datos. Debido a que el protocolo CDP funciona en la capa de enlace de datos, es posible que dos o más dispositivos de red Cisco (como routers que admiten distintos protocolos de la capa de red) obtengan información de los demás incluso si no hay conectividad de capa 3.

Cuando arranca un dispositivo Cisco, el CDP se inicia de manera predeterminada. CDP descubre automáticamente los dispositivos Cisco vecinos que ejecutan ese protocolo, independientemente de los protocolos o los conjuntos de aplicaciones de capa 3 en ejecución. El CDP intercambia información del hardware y software del dispositivo con sus vecinos CDP conectados directamente.

El CDP brinda la siguiente información acerca de cada dispositivo vecino de CDP:

- **Identificadores de dispositivos:** por ejemplo, el nombre host configurado de un switch.
- **Lista de direcciones:** hasta una dirección de capa de red para cada protocolo admitido.
- **Identificador de puerto:** el nombre del puerto local y remoto en forma de una cadena de caracteres ASCII, como por ejemplo, FastEthernet 0/0.
- **Lista de capacidades:** por ejemplo, si el dispositivo es un router o un switch
- **Plataforma:** plataforma de hardware del dispositivo; por ejemplo, un router Cisco serie 1841.

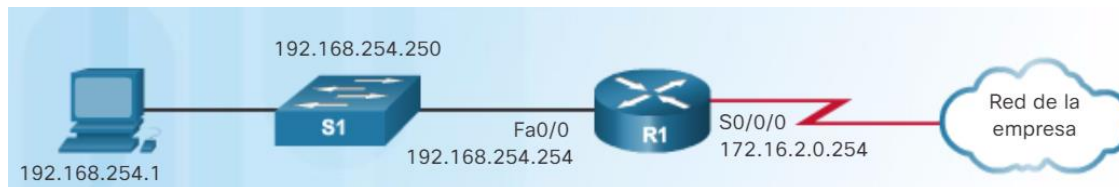
El comando **show cdp neighbors detail** muestra la dirección IP de un dispositivo vecino. CDP revelará la dirección IP del vecino, independientemente de que se pueda hacer ping en ese vecino o no. Este comando es muy útil cuando dos routers Cisco no pueden enrutarse a través de su enlace de datos compartido. El comando **show cdp neighbors detail** lo ayudará a determinar si uno de los vecinos de CDP tiene un error de configuración IP.

Pese a que CDP es útil, también puede ser un riesgo de seguridad, ya que puede proporcionar a los atacantes información útil sobre la infraestructura de la red. Por ejemplo, de manera predeterminada muchas versiones de IOS envían anuncios de CDP por todos los puertos habilitados. Sin embargo, las prácticas recomendadas sugieren que CDP debe habilitarse solamente en las interfaces que se conectan a otros dispositivos Cisco de infraestructura. Los anuncios de CDP se deben deshabilitar en los puertos para el usuario.

Debido a que algunas versiones de IOS envían publicaciones CDP de manera predeterminada, es importante que sepa cómo deshabilitar el CDP. Para desactivar CDP globalmente, utilice el comando de configuración global **no cdp run**. Para desactivar CDP en una interfaz, utilice el comando de interfaz **no cdp enable**.

11.3.4.4 El comando show ip interface brief

De la misma manera que los comandos y las utilidades se utilizan para verificar la configuración de un host, los comandos se pueden utilizar para verificar las interfaces de los dispositivos intermediarios. Cisco IOS proporciona comandos para verificar el funcionamiento de interfaces de router y switch.



Verificación de interfaces del router

Uno de los comandos más utilizados es el comando **show ip interface brief**. Este comando proporciona un resultado más abreviado que el comando **show ip interface**. Proporciona un resumen de la información clave para todas las interfaces de red de un router.

En la figura 1, se muestra la topología que se utiliza en este ejemplo.

El resultado de **show ip interface brief** muestra todas las interfaces del router, la dirección IP asignada a cada interfaz (si las hubiera) y el estado de funcionamiento de la interfaz.

```
R1# show ip interface brief
Interface          IP-Address      OK? Method Status        Protocol
FastEthernet0/0    192.168.254.254 YES NVRAM    up            up
FastEthernet0/1    unassigned      YES unset    down          down
Serial0/0/0        172.16.0.254   YES NVRAM    up            up
Serial0/0/1        unassigned      YES unset    administratively down
```

Verificación de las interfaces del switch

El comando **show ip interface brief** también se puede utilizar para verificar el estado de las interfaces del switch. La interfaz VLAN1 recibió la dirección IPv4 192.168.254.250 y está habilitada y en funcionamiento.

El resultado también muestra que la interfaz FastEthernet0/1 está inactiva. Esto indica que no hay ningún dispositivo conectado a la interfaz o que el dispositivo que está conectado tiene una interfaz de red que no funciona.

Por otro lado, el resultado muestra que las interfaces FastEthernet0/2 y FastEthernet0/3 funcionan. Esto lo indica el valor up en las columnas Status y Protocol.

```
S1# show ip interface brief
Interface          IP-Address      OK? Method Status        Protocol
Vlan1              192.168.254.250 YES manual    up            up
FastEthernet0/1    unassigned      YES unset    down          up
FastEthernet0/2    unassigned      YES unset    up            up
FastEthernet0/3    unassigned      YES unset    up            up
```

11.3.5.1 Comando debug

Los procesos, protocolos, mecanismos y eventos de IOS generan mensajes para comunicar su estado. Estos mensajes pueden proporcionar información valiosa cuando hay que solucionar problemas o verificar las operaciones del sistema. El comando **debug** de IOS permite que el administrador muestre estos mensajes en tiempo real para su análisis. Es una herramienta muy importante para supervisar eventos en un dispositivo Cisco IOS.

Todos los comandos **debug** se introducen en el modo EXEC privilegiado. Cisco IOS permite limitar el resultado de **debug** para incluir solo la característica o la subcaracterística relevante. Esto es importante porque se le asigna alta prioridad al resultado de depuración en el proceso de CPU y puede hacer que el sistema no se pueda utilizar. Por este motivo, use los comandos **debug** solo para solucionar problemas específicos. Para supervisar el estado de mensajes de ICMP en un router Cisco, utilice **debug ip icmp**.

Para acceder a una breve descripción de todas las opciones del comando de depuración, utilice el comando **debug ?** en modo EXEC con privilegios, en la línea de comandos.

Para desactivar una característica de depuración específica, agregue la palabra clave **no** delante del comando **debug**:

```
Router# no debug ip icmp
```

Alternativamente, puede ingresar la forma **undebug** del comando en modo EXEC privilegiado:

```
Router# undebug ip icmp
```

Para desactivar todos los comandos debug activos de inmediato, utilice el comando **undebug all**:

```
Router# undebug all
```

Algunos comandos debug, como **debug all** y **debug ip packet**, generan una importante cantidad de resultados y usan una gran porción de recursos del sistema. El router estaría tan ocupado mostrando mensajes de depuración que no tendría suficiente potencia de procesamiento para realizar las funciones de red, o incluso escuchar los comandos para desactivar la depuración. Por este motivo, no se recomienda y se debe evitar utilizar estas opciones de comando.

11.3.5.2 Comando terminal monitor

Las conexiones para otorgar acceso a la interfaz de línea de comandos de IOS se pueden establecer de forma local o remota.

Las conexiones locales requieren acceso físico al router o switch; por lo tanto, se requiere una conexión de cable. Esta conexión se establece generalmente mediante la conexión de una PC al puerto de consola del router o del switch mediante un cable de sustitución. En este curso, nos referimos a una conexión local como conexión de consola.

Las conexiones remotas se establecen a través de la red; por lo tanto, requieren un protocolo de red como IP. No se requiere acceso físico directo para las sesiones remotas. SSH y Telnet son dos protocolos de conexión comunes utilizados para las sesiones remotas. En este curso, usamos el protocolo cuando hablamos de una conexión remota específica, como una conexión Telnet o una conexión SSH.

Aunque los mensajes de registro de IOS se envían a la consola de manera predeterminada, estos mismos mensajes de registro no se envían a las líneas virtuales de manera predeterminada. Debido a que los mensajes de depuración son mensajes de registro, este comportamiento evita que los mensajes se muestren en las líneas VTY.

Para mostrar los mensajes de registro en una terminal (consola virtual), utilice el comando modo EXEC privilegiado **terminal monitor**. Para detener los mensajes de registro en una terminal, utilice el comando modo EXEC privilegiado **terminal no monitor**.

11.4.1.1 Enfoques básicos para la solución de problemas

Una metodología de solución de problemas común y eficaz se basa en el método científico, y se puede dividir en los seis pasos importantes que se muestran en la ilustración.

Para evaluar el problema, determine cuántos dispositivos de la red lo tienen. Si existe un problema con un dispositivo de la red, inicie el proceso de solución de problemas en ese dispositivo. Si existe un problema con todos los dispositivos de la red, inicie el proceso de solución de problemas en el dispositivo donde se conectan todos los otros dispositivos. Debe desarrollar un método lógico y coherente para diagnosticar problemas de red mediante la eliminación de un problema por vez.

Paso	Título	Descripción
1	Identificación del problema	El primer paso del proceso de solución de problemas consiste en identificar el problema. Aunque se pueden usar herramientas en este paso, una conversación con el usuario suele ser muy útil.
2	Establecer una teoría de causas probables	Después de hablar con el usuario e identificar el problema, puede probar y establecer una teoría de causas probables. Este paso generalmente permite ver más causas probables del problema.
3	Poner a prueba la teoría para determinar la causa	Según las causas probables, pruebe sus teorías para determinar cuál es la causa del problema. El técnico aplica a menudo un procedimiento rápido para probar y ver si resuelve el problema. Si el problema no se corrige con un procedimiento rápido, quizá deba continuar investigando el problema para establecer la causa exacta.
4	Establecer un plan de acción para resolver el problema e implementar la solución	Una vez que haya determinado la causa exacta del problema, establezca un plan de acción para resolver el problema e implementar la solución.
5	Verificar la funcionalidad total del sistema e implementar medidas preventivas	Una vez que haya corregido el problema, verifique la funcionalidad total y, si corresponde, implemente medidas preventivas.
6	Registrar hallazgos, acciones y resultados	El último paso del proceso de solución de problemas consiste en registrar los hallazgos, las acciones y los resultados. Esto es muy importante para referencia futura.

11.4.1.3 Verificación y supervisión de la solución

Cisco IOS incluye herramientas eficaces para la solución de problemas y la verificación. Cuando se ha solucionado el problema y se ha implementado la solución, es importante verificar el funcionamiento del sistema. Las herramientas de verificación incluyen los comandos **ping**, **traceroute** y **show**. El comando **ping** se utiliza para verificar si la conectividad de la red es satisfactoria.

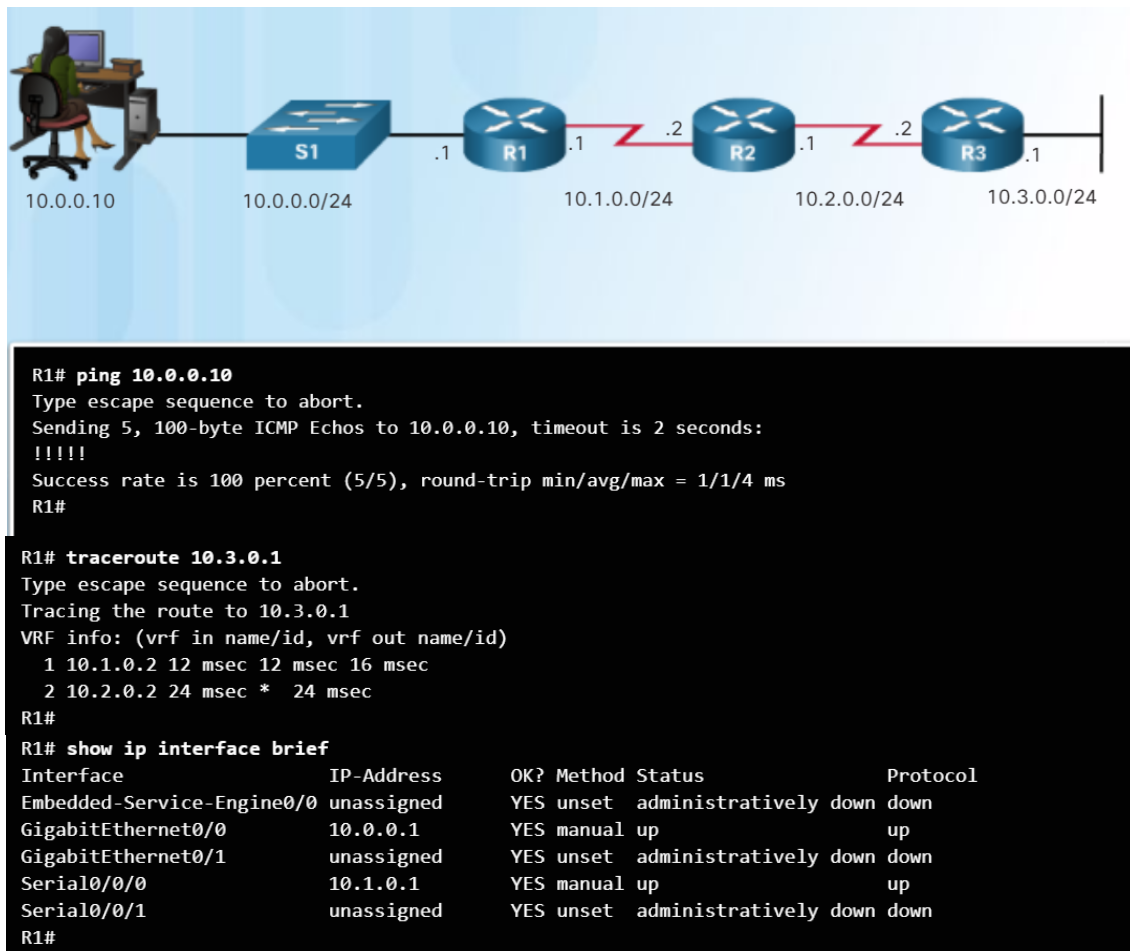
Si un **ping** se completa con éxito, como se muestra en la Figura 1, puede darse por seguro que los paquetes están llegando desde el origen hasta el destino.

Nota: Un **ping** fallido no suele proporcionar suficiente información para llegar a una conclusión. Puede ser el resultado de una ACL o de un firewall que bloqueaba los paquetes ICMP, o bien el dispositivo de destino puede estar configurado para no responder los pings. Un ping fallido generalmente indica que se requiere investigación adicional.

El comando **traceroute**, como se muestra en la Figura 2.2, es útil para mostrar la ruta que los paquetes utilizan para llegar a un destino. Aunque el resultado del comando **ping** muestra si un paquete llegó al destino, el resultado del comando **traceroute** muestra qué ruta tomó para llegar allí, o dónde el paquete fue interrumpido a lo largo de la ruta.

Los comandos **show** de Cisco IOS son algunas de las herramientas de corrección y verificación más útiles para solucionar problemas. Al aprovechar una gran variedad de opciones y de subopciones, el comando **show** puede utilizarse para filtrar y mostrar información sobre prácticamente cualquier aspecto específico de IOS.

En la Figura 3, se muestra el resultado del comando **show ip interface brief**. Observe que las dos interfaces configuradas con las direcciones IPv4 están en “up” y “up”. Estas interfaces pueden enviar y recibir tráfico. Las otras tres interfaces no tienen ningún direccionamiento IPv4 y están desactivadas.



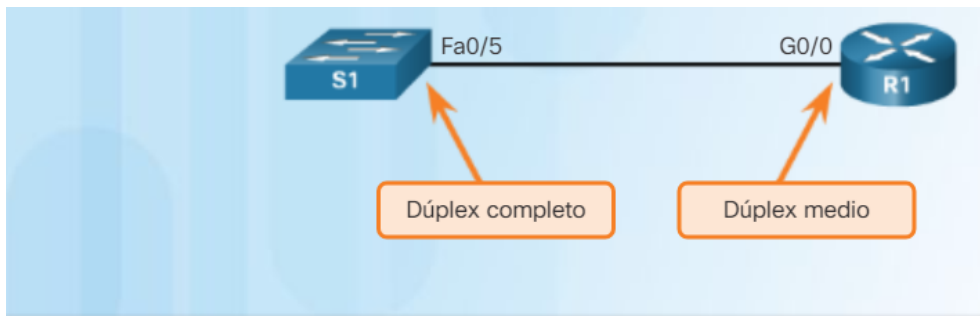
11.4.2.2 Incompatibilidad de dúplex

Las discordancias de dúplex pueden ser difíciles de resolver mientras se produce la comunicación entre dispositivos. Es posible que no sean evidentes, incluso si se usan herramientas como ping. Los pequeños paquetes individuales no puedan revelar un problema de discordancia de dúplex. Una sesión de terminal que envía los datos lentamente (en ráfagas muy cortas) también podría comunicar con éxito a través de una discordancia de dúplex. Aun cuando cualquier extremo de la conexión intente enviar una cantidad significativa de datos y el rendimiento del enlace caiga considerablemente, la causa puede no ser fácilmente evidente debido a que la red está operativa de otra manera.

CDP, el protocolo exclusivo de Cisco, puede detectar fácilmente una discordancia de dúplex entre dos dispositivos Cisco. Vea la topología y los mensajes de registro en la Figura 1, donde la interfaz G0/0 en R1 se ha configurado de forma errónea para funcionar en modo semidúplex. El CDP muestra los mensajes de registro del enlace con la discordancia de dúplex. Los mensajes también contienen los nombres de los dispositivos y los puertos involucrados en la discordancia de dúplex, lo cual facilita mucho identificar y solucionar el problema.

Nota: Debido a que estos son mensajes de registro, de manera predeterminada se muestran únicamente en una sesión de consola. Estos mensajes puede verse en una conexión remota solo si se habilita el comando terminal monitor.

En la Figura 2, se muestra que la interfaz S1 se configuró correctamente para la operación de dúplex completo. En la Figura 3, se muestra que la configuración semidúplex en R1 causó el problema.



```
S1#
*Mar 1 01:01:03.858: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on
FastEthernet0/5 (not half duplex), with R1 GigabitEthernet0/0 (half duplex).
*Mar 1 01:01:04.856: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on
FastEthernet0/5 (not half duplex), with R1 GigabitEthernet0/0 (half duplex).
*Mar 1 01:01:05.855: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on
FastEthernet0/5 (not half duplex), with R1 GigabitEthernet0/0 (half duplex).
S1#
```

```
S1# show interfaces fastethernet 0/5
FastEthernet0/5 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 0cd9.96e2.3d05 (bia 0cd9.96e2.3d05)
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)
Full-duplex, Auto-speed, media type is 10/100BaseTX
input flow-control is off, output flow-control is unsupported
<se omitió el resultado>
```

```
R1# show interfaces gigabitethernet 0/0
GigabitEthernet0/0 is up, line protocol is up
Hardware is CN Gigabit Ethernet, address is fc99.4775.c3e0 (bia
fc99.4775.c3e0)
Internet address is 10.0.0.1/24
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, 100Mbps, media type is RJ45
output flow-control is unsupported, input flow-control is unsupported
<se omitió el resultado>
```

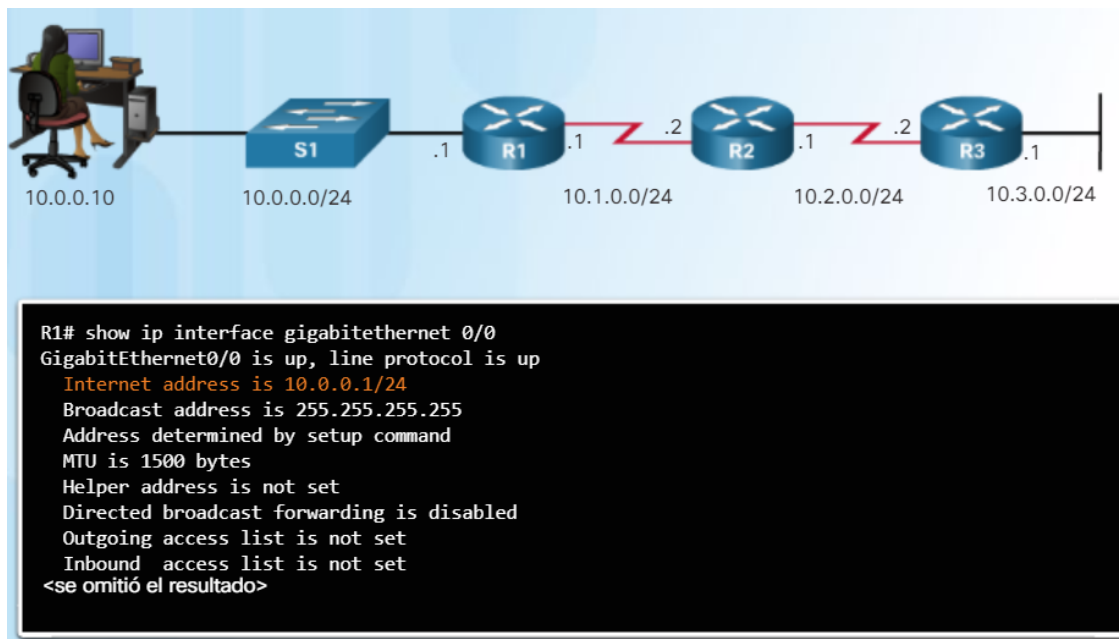
11.4.3.1 Problemas de asignación de direcciones IP en dispositivos IOS

Los problemas relacionados con la dirección IP probablemente evitarán la comunicación de los dispositivos de redes remotas. Debido a que las direcciones IP son jerárquicas, cualquier dirección IP asignada a un dispositivo de red debe adaptarse al rango de direcciones de esa red. Las direcciones IP asignadas incorrectamente crean una variedad de problemas, incluso conflictos de direcciones IP y problemas de routing.

Dos causas comunes de asignación incorrecta de IPv4 son los errores manuales de asignación o los problemas relacionados con DHCP.

Los administradores de redes tienen que asignar a menudo las direcciones IP manualmente a los dispositivos como servidores y routers. Si se genera un error durante la asignación, es muy probable que ocurran problemas de comunicación con el dispositivo.

En un dispositivo IOS, utilice los comandos **show ip interface** o **show ip interface brief** para comprobar qué direcciones IPv4 se asignan a las interfaces de red. En la ilustración, se muestra el resultado del comando **show ip interface** emitido en R1. Observe que el resultado muestra la información de IPv4 (capa 3 de OSI), mientras que el comando **show interfaces** mencionado anteriormente muestra los detalles físicos y del enlace de datos de una interfaz.



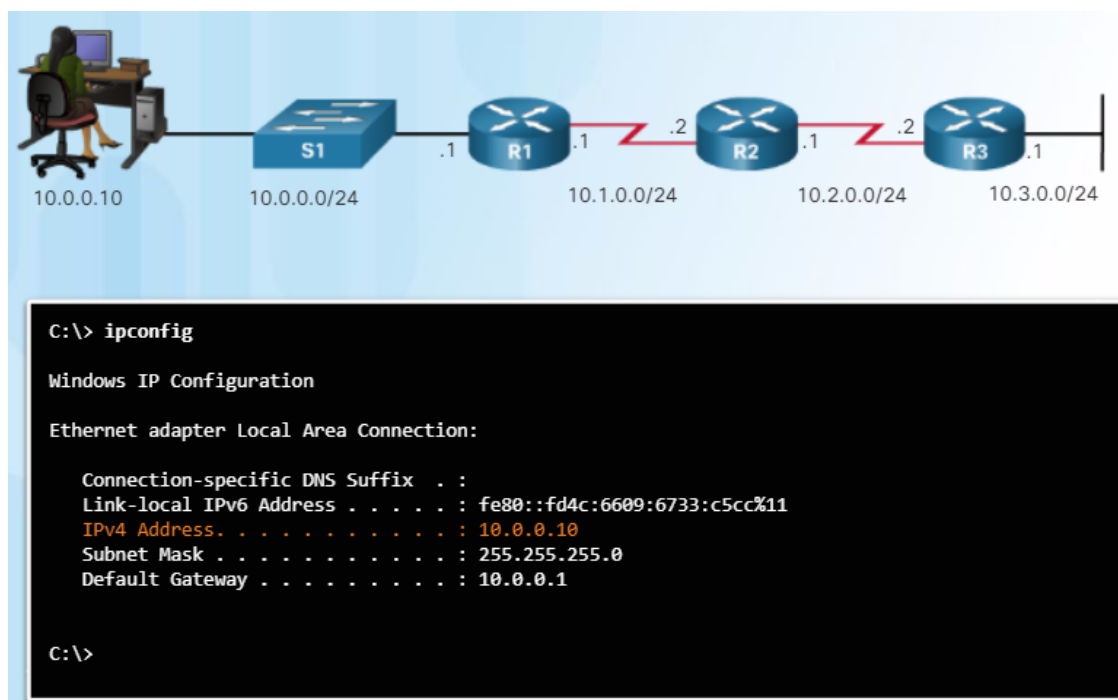
11.4.3.2 Problemas de asignación de direcciones IP en terminales

En las máquinas con Windows, cuando el dispositivo no puede comunicarse con un servidor DHCP, Windows asigna automáticamente una dirección que pertenezca al rango 169.254.0.0/16. Este proceso se diseñó para facilitar la comunicación dentro de la red local. Piense que Windows dice: “Utilizaré esta dirección del rango 169.254.0.0/16 porque no pude obtener ninguna otra dirección”. A menudo, una computadora con rango 169.254.0.0/16 no podrá comunicarse con otros dispositivos en la red porque es probable que dichos dispositivos no pertenezcan a la red 169.254.0.0/16. Esta situación indica un problema de asignación automática de direcciones IPv4 que debe solucionarse.

Nota: Otros sistemas operativos, como Linux y OS X, no asignarán una dirección IPv4 a la interfaz de red si falla la comunicación con un servidor DHCP.

La mayoría de los terminales se configuran para confiar en un servidor DHCP para la asignación automática de direcciones IPv4. Si el dispositivo no puede comunicarse con el servidor DHCP, el servidor no puede asignar una dirección IPv4 para la red específica y el dispositivo no podrá comunicarse.

Para comprobar las direcciones IP asignadas a una computadora con Windows, utilice el comando **ipconfig**, como se muestra en la ilustración.



11.4.3.3 Problemas con el gateway predeterminado

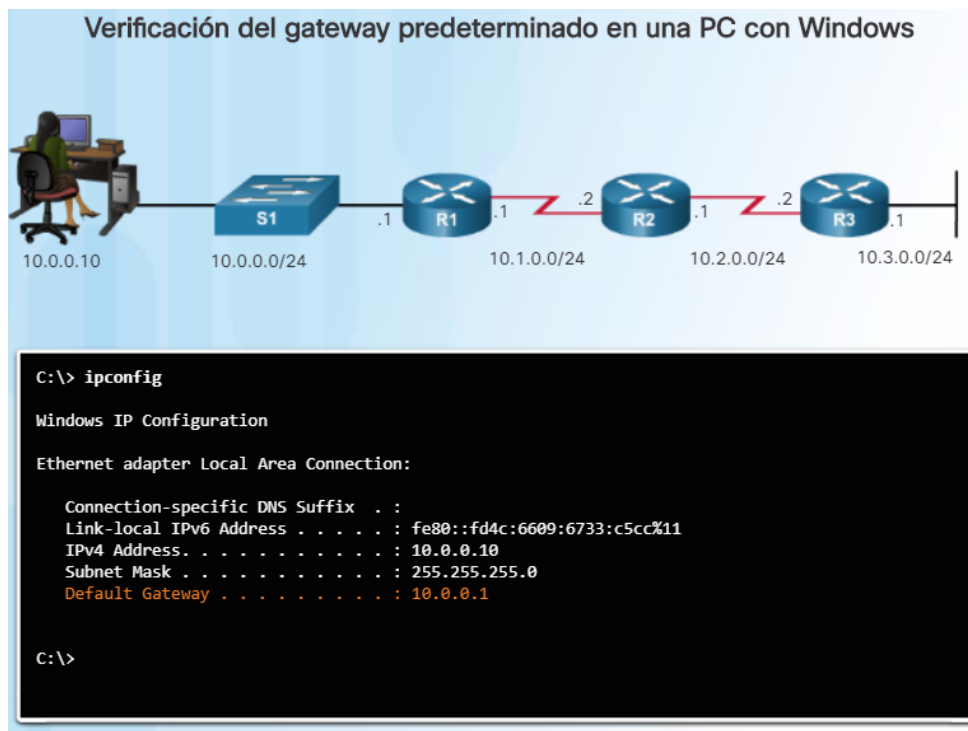
El gateway predeterminado para un terminal es el dispositivo de red más cercano que puede reenviar tráfico a otras redes. Si un dispositivo tiene una dirección de gateway predeterminado incorrecta o inexistente, no podrá comunicarse con los dispositivos de las redes remotas. Dado que el gateway predeterminado es la ruta a las redes remotas, su dirección debe pertenecer a la misma red que el terminal.

La dirección del gateway predeterminado se puede configurar u obtener manualmente de un servidor DHCP. Como sucede con los problemas de asignación de direcciones IPv4, los problemas del gateway predeterminado pueden estar relacionados con la configuración incorrecta (en el caso de la asignación manual) o problemas de DHCP (si está en uso la asignación automática).

Para resolver los problemas de un gateway predeterminado mal configurado, asegúrese de que el dispositivo tenga configurado el gateway predeterminado correcto. Si la dirección predeterminada fue configurada manualmente pero es incorrecta, simplemente reemplácela por la dirección apropiada. Si la dirección de gateway predeterminado fue configurada automáticamente, asegúrese de que el dispositivo pueda comunicarse correctamente con el servidor DHCP. También es importante verificar que se configuraron la dirección IPv4 y la máscara de subred correspondientes en la interfaz del router y que la interfaz esté activa.

Para verificar el gateway predeterminado en las computadoras con Windows, utilice el comando **ipconfig** como se muestra en la Figura 1.

En un router, use el comando **show ip route** para mostrar la tabla de routing y comprobar que se ha establecido el gateway predeterminado, conocido como ruta predeterminada. Se usa esta ruta cuando la dirección de destino del paquete no coincide con ninguna otra ruta en la tabla de routing. En la Figura 2, se muestra que R2 es la ruta predeterminada para R1, mientras que el resultado de los comandos **show ip route** muestra que el gateway predeterminado se configuró con una ruta predeterminada de 10.1.0.2.





11.4.3.4 Solución de problemas de DNS

El Servicio de Nombres de Dominio (DNS) es un servicio automatizado que hace coincidir los nombres, como `www.cisco.com`, con la dirección IP. Aunque la resolución de DNS no es fundamental para la comunicación del dispositivo, es muy importante para el usuario final.

Es común que los usuarios relacionen erróneamente el funcionamiento de un enlace de Internet con la disponibilidad del servicio DNS. Las quejas de los usuarios como “la red está inactiva” o “Internet está inactiva” se deben a menudo a un servidor DNS al que no se puede acceder. Aunque los servicios de routing de paquetes y cualquier otro tipo de servicios de red estén todavía operativos, los errores de DNS generalmente llevan al usuario a la conclusión incorrecta. Si un usuario escribe un nombre de dominio como `www.cisco.com` en un navegador web y no se puede acceder al servidor DNS, el nombre no será traducido a una dirección IP y la página web no se mostrará.

Las direcciones del servidor DNS pueden asignarse de manera manual o automática. Los administradores de redes a menudo son responsables de asignar manualmente las direcciones del servidor DNS en servidores y otros dispositivos, mientras que el DHCP se usa para asignar automáticamente las direcciones del servidor DNS a los clientes.

Si bien es común que las empresas y las organizaciones administren sus propios servidores DNS, cualquier servidor DNS accesible puede utilizarse para solucionar nombres. Los usuarios de oficinas pequeñas y oficinas en el hogar con frecuencia dependen del servidor DNS que mantiene su ISP para la resolución de nombres. Los servidores DNS mantenidos por un ISP son asignados a los clientes de SOHO mediante DHCP. Por ejemplo, Google mantiene un servidor DNS público que puede ser utilizado por cualquier persona y es muy útil para realizar pruebas. La dirección IPv4 del servidor DNS público de Google es 8.8.8.8 y 2001:4860:4860::8888 para su dirección IPv6 DNS.

Use el comando **ipconfig /all**, como se muestra en la Figura 1, para verificar qué servidor DNS utiliza la computadora con Windows.

El comando **nslookup** es otra herramienta útil para la solución de problemas de DNS para PC. Con **nslookup** un usuario puede configurar manualmente las consultas de DNS y analizar la respuesta de DNS. En la Figura 2, se muestra el resultado de **nslookup** al realizar una consulta para **www.cisco.com**.

```
C:\> ipconfig /all

Ethernet adapter Local Area Connection:
<se omitió parte del resultado>
    Connection-specific DNS Suffix . . : 
    Description . . . . . : Realtek PCIe GBE Family Controller
    Physical Address. . . . . : F0-4D-A2-DD-A7-B2
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::449f:c2:de06:ebad%10(Preferred)
    IPv4 Address. . . . . : 10.0.0.10(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Monday, November 09, 2015 7:49:48 PM
    Lease Expires . . . . . : Thursday, November 19, 2015 7:49:51 AM
    Default Gateway . . . . . : 10.0.0.1
    DHCP Server . . . . . : 10.0.0.1
    DNS Servers . . . . . : 8.8.8.8
    NetBIOS over Tcpip. . . . . : Enabled
```

```
C:\> nslookup
Default Server: dns-cac-lb-01.rr.com
Address: 209.18.47.61

> cisco.com
Server: dns-cac-lb-01.rr.com
Address: 209.18.47.61

Non-authoritative answer:
Name: cisco.com
Addresses: 2001:420:1101:1::a
           72.163.4.161

> quit

C:\>
```