# Preguntas frecuentes sobre el router

## Objetivo

Este documento tiene como objetivo responder preguntas comunes sobre las capacidades y funciones que se encuentran en un router Cisco, así como sobre cómo y cuándo utilizarlas. Si está interesado en contenido de video, vea nuestra lista de reproducción de video haciendo click aquí.

## Dispositivos aplicables

- Serie RV100
- Serie RV200
- Serie RV300

## Table Of Contents

## 1. ¿Qué son las reglas de acceso?

Las reglas de control de acceso son reglas que obligan a que el tráfico específico se envíe a y desde determinados usuarios de una red. Las reglas de acceso se pueden configurar para que estén en vigor todo el tiempo o en función de una programación definida. Mientras que una regla de acceso se puede configurar en un router o un switch, se configura en función de varios criterios para permitir o denegar el acceso a algunos o todos los recursos de la red.

## 2. ¿Cuáles son las opciones 66, 67 y 150 para el servidor TFTP?

Un servidor TFTP permite a un administrador almacenar, recuperar y descargar archivos de configuración para dispositivos en una red. Un servidor de protocolo de configuración dinámica de host (DHCP) alquila y distribuye direcciones IP a los dispositivos de la red. Cuando se inicia un dispositivo y no se configura previamente una dirección IPv4 o IPv6 y una dirección IP del servidor TFTP, el dispositivo enviará una solicitud al servidor DHCP con las opciones 66, 67 y 150. Estas opciones son solicitudes al servidor DHCP para obtener información sobre el servidor TFTP.

- La opción DHCP 150 es propiedad de Cisco. Proporciona las direcciones IP en una lista de servidores TFTP. El equivalente estándar del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) es la opción 66.
- La opción DHCP 66 proporciona la dirección IP o el nombre de host de un único servidor TFTP.
- La opción DHCP 67 proporciona el nombre del archivo de inicio para el servidor TFTP.

## 3. ¿Cuáles son las diferencias entre la ejecución en modo de router y el modo de gateway?

Hay dos modos en los que el router puede funcionar: el modo de router y el modo de gateway. El modo de router es el modo operativo que desactiva la traducción de direcciones de red (NAT) en el dispositivo y se utiliza para conectar más de un router y varias redes. Esto se utiliza mejor en entornos de red de área extensa.

El modo de puerta de enlace es el modo recomendado si el router aloja una conexión de red directamente a Internet. NAT se ejecuta cuando se habilita el modo de gateway, lo que significa que tomará una sola dirección IP WAN y tendrá un bloque completo de direcciones IP LAN.

## 4. ¿Qué son los registros de sistemas?

Los registros del sistema (Syslog) son registros de eventos de red. En caso de que el sistema funcione mal, puede recuperar los registros para diagnosticar el problema del sistema. Los registros son herramientas importantes que se utilizan para comprender cómo funciona una red para ejecutar el sistema sin problemas y evitar fallos. Son útiles para la gestión de redes, la resolución de problemas y la supervisión.

## 5. ¿Qué son los modos DHCP?

El protocolo de configuración dinámica de host (DHCP) tiene dos modos: DHCP Server (Servidor DHCP) y DHCP Relay (Retransmisión DHCP). Un servidor DHCP asigna automáticamente las direcciones IP disponibles a un cliente DHCP o host de la red. El servidor DHCP y el cliente DHCP deben estar conectados al mismo link de red. En redes más grandes donde los clientes y los servidores no están en la misma subred física, cada link de red contiene uno o más agentes de relé DHCP. Un agente de relé DHCP puede ser un router. Cuando un cliente envía al router una solicitud de DHCP, el router lo reenviará al servidor DHCP solicitando proporcionar una dirección IP para el cliente. El servidor DHCP envía su respuesta al router y luego el router la reenviará al cliente. El router y el servidor DHCP no necesitan estar en la misma subred para funcionar. El router actúa como enlace entre el cliente y el servidor DHCP.

## 6. ¿Qué es 3G/4G?

Se trata del tipo de tecnología para la banda ancha móvil o la Internet inalámbrica a la que se puede acceder a través de teléfonos móviles o de módems portátiles. La letra G representa a la generación. La tecnología 4G es una de las más recientes y una de las más rápidas de hoy después de Long Term Evolution (LTE). Algunos routers VPN de Cisco le permiten compartir la conexión a Internet desde dongles USB 3G/4G compatibles que se pueden conectar a ella para que funcionen como conmutación por fallo en caso de que el principal proveedor de servicios de Internet (ISP) se interrumpa o se ralentice.

## 7. ¿Qué es un generador de certificados y cuándo lo utilizaría?

Un certificado digital certifica la propiedad de una clave pública por el sujeto designado del certificado. Esto permite que las partes que confían en ellas dependan de las firmas o afirmaciones hechas por la clave privada que corresponde a la clave pública certificada. Un router puede generar un certificado autofirmado, un certificado creado por el administrador de la red. También puede enviar solicitudes a las autoridades de certificación (CA) para solicitar un certificado de identidad digital. Es importante disponer de certificados legítimos de aplicaciones de terceros.

## 8. ¿Qué es un firewall y cuándo lo utilizaría?

El objetivo principal de un firewall es controlar el tráfico de red entrante y saliente mediante el análisis de los paquetes de datos y la determinación de si se debe permitir o no, en función de un conjunto de reglas predeterminado. Un router se considera un firewall de hardware sólido debido a las funciones que permiten el filtrado de datos entrantes. Un firewall de red crea un puente entre una red interna que se supone es segura y de confianza y otra red, normalmente una red interna externa como Internet que se supone no es segura ni fiable.

## 9. ¿Qué es un certificado IPSec de confianza?

La seguridad de protocolo de Internet (IPSec) genera una comunicación segura, autenticada y fiable a través de redes IP. Se utiliza en el intercambio de datos de generación y autenticación de claves, protocolo de establecimiento de claves, algoritmo de cifrado o mecanismo de autenticación de autenticación segura y validación de transacciones en línea con certificados de Secure Socket Layer (SSL). En el RV320, puede agregar un máximo de 50 certificados autofirmados o autorizados por CA de terceros. Estos certificados se pueden exportar a un ordenador o dispositivo USB y se importan para que los utilice un cliente o administrador.

## 10. ¿Qué es un certificado SSL de confianza?

Los certificados se utilizan para verificar la identidad del usuario en un equipo o en Internet y para mejorar una conversación privada o segura. Secure Sockets Layer (SSL) es la tecnología de seguridad estándar para crear un enlace cifrado entre un servidor web y un navegador. Estos certificados se pueden exportar a un ordenador o dispositivo USB y se importan para que los utilice un cliente o administrador.

## 11. ¿Qué es VPN de cliente a gateway?

La red privada virtual (VPN) de cliente a gateway permite al usuario conectar de forma remota diferentes sucursales de su empresa situadas en diferentes zonas geográficas para transmitir y recibir los datos entre las zonas de forma más segura. Normalmente, un usuario tendría instalado un software cliente VPN como Cisco AnyConnect Secure Mobility Client en un equipo, iniciaría sesión con las credenciales necesarias y se conectaría a un router o gateway remoto.

**Nota:** Ha habido actualizaciones sobre los requisitos de licencia para la serie RV340, comenzando con la versión 1.0.3.15 en adelante. Para obtener más información sobre esto, haga clic aquí.

## 12. ¿Qué es el filtrado de contenido?

El filtrado de contenido es una función que permite al administrador bloquear sitios web designados no deseados. El filtrado de contenido puede bloquear la lista y permitir el acceso a la lista de sitios web según las palabras clave y los localizadores uniformes de recursos (URL). Un administrador puede aplicar una programación al filtrado de contenido según cuándo debe estar activo.

Consulte el glosario para obtener información adicional.

## 13. ¿Qué es CoS?

La clase de servicio (CoS) es una forma de gestionar el tráfico a través de una red mediante la asignación de una prioridad sobre otros tipos de tráfico. Se utiliza para asignar niveles de prioridad a los encabezados de trama Ethernet del tráfico de red y sólo se aplica a los links troncales. Al diferenciar el tráfico, el CoS permite controlar y priorizar los paquetes de datos preferidos para la transmisión en caso de que la red experimente problemas como congestión o retraso. Puede asignar la configuración de prioridad de CoS a la cola de reenvío de tráfico en un router.

## 14. ¿Qué es la opción 82 de DHCP?

El relé DHCP es una función incluida en el router que permite la comunicación DHCP entre hosts y servidores DHCP remotos que no están en la misma red. La opción 82 es una opción de información de agente de relé DHCP que permite a un agente de relé DHCP incluir información sobre sí mismo cuando reenvía paquetes DHCP originados por el cliente a un servidor DHCP. El servidor DHCP puede utilizar esta información para implementar el direccionamiento IP u otras políticas de asignación de parámetros. Su identificación exhaustiva de la conexión añade seguridad al proceso DHCP.

## 15. ¿Qué es DHCP?

El protocolo de configuración dinámica de host (DHCP) es un protocolo de configuración de red

que configura automáticamente las direcciones IP de los dispositivos de una red para que se puedan conectar entre sí en lugar de asignar manualmente una dirección IP a un dispositivo.

## 16. ¿Qué es DMZ y cuándo debería usarla?

Una zona desmilitarizada (DMZ) es una subred abierta al público pero que se encuentra detrás del firewall. Una DMZ permite redirigir los paquetes que entran en el puerto WAN a una dirección IP específica de la LAN. Puede configurar reglas de firewall para permitir el acceso a servicios y puertos específicos en la DMZ tanto desde la LAN como desde la WAN. En caso de ataque a cualquiera de los nodos DMZ, la LAN no es necesariamente vulnerable. Se recomienda colocar hosts que deban estar expuestos a la WAN (como servidores web o de correo electrónico) en la red DMZ.

## 17. ¿Qué es DSCP?

El punto de código de servicios diferenciados (DSCP) se utiliza para clasificar el tráfico de red y asignar diferentes niveles de servicio a los paquetes marcándolos con códigos DSCP en el campo de encabezado IP. La configuración de DSCP dictará cómo se asignan los valores de DSCP a la calidad del servicio (QoS), que es un método para administrar los niveles de prioridad del tráfico en una red. A través de DSCP, el router puede utilizar los bits de prioridad en el octeto Tipo de servicio (ToS) para priorizar el tráfico sobre QoS en la capa 3.

## 18. ¿Qué es DNS dinámico?

El sistema dinámico de nombres de dominio (DNS) es un método para actualizar automáticamente un servidor de nombres en el DNS, a menudo en tiempo real, con la configuración DDNS activa de sus nombres de host configurados, direcciones u otra información. Este servicio asigna un nombre de dominio fijo a una dirección IP WAN dinámica, de modo que pueda alojar su propia Web, FTP u otro tipo de servidor TCP/IP en su LAN. El router utiliza DDNS a través de una cuenta DDNS basada en Web. Si la dirección IP de WAN del router cambia, la función DDNS notificará el cambio al servidor DDNS. A continuación, el servidor DDNS actualizará la configuración para incluir la nueva dirección IP WAN. Esto es útil si la dirección IP de la WAN del router a menudo cambia. Se debe crear una cuenta DDNS en uno de los sitios web proporcionados para utilizar la función DDNS del router.

## 19. ¿Qué es la VPN de puerta de enlace a puerta de enlace? ¿Cuándo lo usaría?

Una conexión VPN de gateway a gateway permite que dos routers se conecten de forma segura entre sí y que un cliente en un extremo aparezca lógicamente como si formaran parte de la red en el otro extremo. Esto permite compartir datos y recursos de forma más sencilla y segura a través de Internet. La configuración se debe realizar en ambos routers para habilitar una VPN de gateway a gateway.

## 20. ¿Qué son los enlaces IP y MAC? ¿Cuándo lo usaría?

El enlace de direcciones IP y MAC es un proceso que enlaza una dirección IP a una dirección MAC y viceversa. Si el router recibe paquetes con la misma dirección IP pero una dirección MAC diferente, descarta los paquetes. Ayuda a evitar la suplantación de IP y mejora la seguridad de la red, ya que no permite que un usuario cambie las direcciones IP de los dispositivos. La dirección IP del host de origen y la dirección MAC del tráfico deben coincidir siempre para poder acceder a la red. Si el router recibe paquetes con la misma dirección IP pero una dirección MAC diferente, descarta los paquetes.

## 21. ¿Qué es el balance de carga y cuándo lo utilizaría?

El balanceo de carga permite que un router aproveche las mejores trayectorias múltiples hacia un destino determinado. Es inherente al proceso de reenvío en el router y se activa automáticamente si la tabla de ruteo tiene varias trayectorias a un destino. La configuración del balanceo de carga en el router ayuda a lograr una utilización adecuada de los recursos, maximizar el rendimiento, el tiempo de respuesta y, principalmente, evitar la sobrecarga ya que distribuye la carga de trabajo entre varios ordenadores, enlaces de red y otros recursos.

## 22. ¿Qué es la clonación de la dirección MAC y cuándo la necesitaría?

El clon de dirección MAC es la forma más sencilla de duplicar la copia exacta de la dirección MAC de un dispositivo a otro dispositivo, como un router. A veces, los ISP le piden que registre una dirección MAC del router para autenticar el dispositivo. Una dirección MAC es un código hexadecimal de 12 dígitos dado a cada pieza de hardware para que pueda identificarse de forma única. Si ya ha registrado otra dirección MAC con el ISP, se puede utilizar un clon de dirección MAC para clonar esa dirección en el nuevo router. De esta manera, no tendrá que ponerse en contacto con el ISP para cambiar la dirección MAC registrada anteriormente, lo que reduce el coste y el tiempo de mantenimiento.

## 23. ¿Qué es una NAT uno a uno y cuándo tendría que usarla?

La traducción de direcciones de red (NAT) uno a uno crea una relación que asigna una dirección IP de WAN válida a direcciones IP de LAN que la NAT oculta de la WAN (Internet). Esto protege los dispositivos LAN de detección y ataque. En el router, puede asignar una única dirección IP privada (dirección IP de LAN) a una única dirección IP pública (dirección IP de WAN) o a un intervalo de direcciones IP privadas a un intervalo de direcciones IP públicas.

## 24. ¿Qué es la complejidad de las contraseñas y por qué me beneficia?

La complejidad de la contraseña es una función de un dispositivo de red que exige un mínimo de complejidad de contraseña para los cambios de contraseña. Esto es beneficioso para todos los tipos de redes. Las contraseñas con complejidad se pueden configurar para que venzan después de un tiempo especificado.

## 25. ¿Qué es la traducción de direcciones de puerto (PAT) y cuándo la necesitaría?

Se trata de una función que permite asignar varios dispositivos dentro de una red privada o local a una única dirección IP pública. PAT se utiliza para conservar direcciones IP. Es una extensión de la traducción de direcciones de red (NAT). PAT también se conoce como portación, sobrecarga de puertos, NAT multiplexada a nivel de puerto y NAT de dirección única.

## 26. ¿Qué es el reenvío de puertos y cuándo debería utilizarlo?

Port Forwarding es una función que se utiliza para pasar datos a un dispositivo específico dentro de una LAN privada. Para ello, asigna el tráfico de los puertos elegidos del dispositivo a los puertos correspondientes de la red. El router es compatible con esta función que permite al ordenador dirigir de forma eficaz el tráfico donde sea necesario para mejorar el rendimiento y las características de equilibrio de red. El reenvío de puertos debe utilizarse sólo cuando sea necesario, ya que esto supone un riesgo para la seguridad debido a que un puerto configurado siempre está abierto.

## 27. ¿Qué es la duplicación de puertos?

La duplicación de puertos es un método utilizado para supervisar el tráfico de red. Con la duplicación de puertos, las copias de los paquetes entrantes y salientes en los puertos (puertos de origen) de un dispositivo de red se reenvían a otro puerto (puerto de destino) en el que se estudian los paquetes.

## 28. ¿Qué es Port Triggering y cuándo debería utilizarlo?

El desencadenado de puertos es similar al reenvío de puertos, excepto que es más seguro porque los puertos entrantes no están abiertos todo el tiempo. Los puertos permanecen cerrados hasta que se activan, lo que limita la posibilidad de acceso a puertos no deseados. El desencadenado de puertos es un método de reenvío dinámico de puertos. Cuando un host conectado al router abre un puerto de activación configurado en una regla de activación de intervalo de puertos, el router reenvía los puertos configurados al host. Una vez que el host cierra el puerto activado, el router cierra los puertos reenviados. Cualquier ordenador de una red puede utilizar la configuración de desencadenado de puertos, ya que no requiere una dirección IP interna para reenviar los puertos entrantes, a diferencia de lo que ocurre con el reenvío de puertos.

## 29. ¿Qué es el servidor PPTP? ¿Cuándo lo usaría? ¿Cómo lo prepararía?

El protocolo de túnel punto a punto (PPTP) es un protocolo de red utilizado para implementar túneles VPN entre redes públicas. Los servidores PPTP también se conocen como servidores de Virtual Private Dialup Network (VPDN). PPTP utiliza un canal de control sobre el protocolo de control de transmisión (TCP) y un túnel de encapsulación de routing genérico (GRE) que funciona para encapsular los paquetes PPP. Se pueden habilitar hasta 25 túneles VPN PPTP para los usuarios que ejecutan un software cliente PPTP. La implementación PPTP más común es con las familias de productos de Microsoft Windows e implementa diferentes niveles de autenticación y cifrado de forma nativa como características estándar de la pila PPTP de Windows. PPTP es preferible a otros protocolos porque es más rápido y tiene la capacidad de trabajar con dispositivos móviles. Como referencia, haga clic aquí para obtener una idea sobre cómo configurarlo.

## 30. ¿Qué es QoS?

La calidad del servicio (QoS) se utiliza principalmente para mejorar el rendimiento de la red y para proporcionar los servicios deseados a los usuarios. Prioriza el flujo de tráfico en función del tipo de tráfico. La QoS se puede aplicar al tráfico con prioridad para aplicaciones sensibles a la latencia (como voz o vídeo) y para controlar el impacto del tráfico que no distingue la latencia (como las transferencias de datos masivas).

## 31. ¿Qué es RIPv1? RIPv2?

Routing Information Protocol (RIP) es un protocolo de vector de distancia que utilizan los routers para intercambiar información de routing. RIP utiliza el conteo de saltos como su métrica de ruteo. RIP evita que los loops de ruteo continúen indefinidamente al implementar un límite en el número de saltos permitidos en una trayectoria desde el origen a un destino. El conteo máximo de saltos para RIP es 15, lo que limita el tamaño de red que puede soportar. Esta es la razón por la que se desarrolló el RIPv2. A diferencia del RIPv1 con clase, RIPv2 es un protocolo de ruteo sin clase que incluye las máscaras de subred cuando envía sus actualizaciones de ruteo.

El resumen de las rutas en RIPv2 mejora la escalabilidad y la eficiencia en las redes grandes. El

resumen de las direcciones IP significa que no hay entrada para las rutas secundarias (rutas creadas para cualquier combinación de las direcciones IP individuales contenidas en una dirección de resumen) en la tabla de ruteo RIP, lo que reduce el tamaño de la tabla y permite que el router maneje más rutas.

## 32. ¿Qué es Smart Link Backup?

Smart Link Backup es una función que permite al usuario configurar una segunda WAN en caso de que falle la primera o el enlace principal. Esta función se utiliza para garantizar que la comunicación entre la WAN y el dispositivo sea siempre continua. Esta función se encuentra en routers con conexiones WAN duales.

## 33. ¿Qué es SSL VPN? ¿Cuándo lo usaría?

Una red privada virtual (SSL VPN) de capa de sockets seguros, también conocida como WebVPN, es una tecnología que proporciona funciones VPN de acceso remoto mediante la función SSL integrada en un explorador web moderno. Esto no requiere que instale un cliente VPN en el dispositivo del cliente. SSL VPN permite a los usuarios desde cualquier ubicación con conexión a Internet iniciar un navegador web para establecer conexiones VPN de acceso remoto, lo que promete mejoras en la productividad y en la disponibilidad, así como una mayor reducción de los costes de TI para el soporte y el software del cliente VPN.

## 34. ¿Qué es VPN Passthrough (Paso a través de VPN)?

VPN Passthrough (Paso a través de VPN) es una forma de conectar dos redes seguras a través de Internet. Esto se utiliza para permitir que el tráfico VPN generado a partir de los clientes VPN conectados al router pase a través de Internet y permita que la conexión VPN se realice correctamente.

## 35. ¿Qué es VPN?

Una red privada virtual (VPN) es una conexión segura establecida dentro de una red o entre redes mediante la creación de un túnel. Las VPN sirven para aislar el tráfico entre hosts y redes especificados del tráfico de redes y hosts no autorizados. Las VPN son beneficiosas para las empresas de tal forma que son altamente escalables, simplifican la topología de red y mejoran la productividad al reducir el tiempo de desplazamiento y el coste para los usuarios remotos.

## 36. ¿Por qué cambiaría los valores de la máscara de subred?

Una subred es una parte de una red que comparte una dirección de subred determinada. Una máscara de subred es una combinación de 32 bits utilizada para describir qué parte de una dirección de red se refiere a la subred y qué parte se refiere al host. Un administrador puede querer cambiar los valores de la máscara de subred en caso de que un host no pueda comunicarse con la red. Las máscaras de subred también se pueden cambiar en caso de que un administrador desee aumentar el número de hosts en una subred sin tener que realizar ningún cambio físico.