

## Guía 5 de estudio de CCENT

### Sección 9.5 Resolución de problemas en los servicios de la Capa 4 y la Capa superior

A medida que trabaja en esta sección sobre resolución de problemas, puede revisar el material necesario para prepararse para obtener una certificación CCENT. Para obtener una certificación CCENT, debe aprobar el examen 640-822 ICND1. Estas guías de estudio proporcionan un método para organizar su revisión de acuerdo a los objetivos del examen ICND1.

#### Protocolos y servicios de red

**Objetivo:** Describir aplicaciones de red comunes, incluyendo las aplicaciones Web

Capítulos de revisión de **CCNA Discovery: Networking para el hogar y pequeñas empresas:**

**Servicios de red:** en este capítulo se describen las aplicaciones comunes de clientes/servidor de la red. Este capítulo proporciona el protocolo que se utiliza, el puerto asignado a la aplicación y la información sobre la funcionalidad del cliente para cada aplicación de red. Asegúrese de memorizar el puerto TCP o UDP predeterminado asignado a cada aplicación, ya que es importante para la resolución de problemas y para crear las listas de filtros del firewall.

Capítulos de revisión de **CCNA Discovery: Trabajar en una pequeña o mediana empresa o ISP:**

**Servicios del SP:** la sección Servicios y protocolos analiza los diferentes servicios de la capa de aplicación que brinda el ISP y contiene información sobre los distintos protocolos que se utilizan para proporcionar estos servicios. Hay más detalles en esta sección que en el material de Discovery 1 sobre el funcionamiento de los servicios de FTP y correo electrónico.

**Responsabilidad del Proveedor de servicios de Internet (ISP, Internet Service Provider):** los métodos para asegurar los protocolos de la capa de aplicación comunes se describen en el tema **Encriptación de datos**.

**Objetivo:** Resolución de problemas del funcionamiento del DNS

Capítulos de revisión de **CCNA Discovery: Networking para el hogar y pequeñas empresas:**

**Servicios de red:** el funcionamiento del Sistema de nombres de dominios se describe en el tema **Sistema de nombres de dominio (DNS)**. Sin la resolución DNS exitosa de un nombre de dominio o URL, no se produce ninguna comunicación. Ponga atención a qué debe estar en buen funcionamiento para que se produzca la resolución del nombre. 1. Debe haber una dirección de servidor DNS correctamente configurada en el host, configurada en forma manual o a través de DHCP, 2. El servidor DNS debe estar accesible desde el host y 3. El servidor DNS se debe configurar para resolver el nombre de host de destino específico para una dirección IP válida. Practique cómo utilizar nslookup para verificar que el DNS esté funcionando correctamente en la red.

**Resolución de problemas de la red:** el tema **Resolución de problemas con Nslookup** describe cómo interpretar el resultado del comando nslookup en una PC de Windows.

Capítulos de revisión de **CCNA Discovery: Trabajar en una pequeña o mediana empresa o ISP:**

**Servicios del SP:** la sección **Sistema de nombres de dominios** proporciona información detallada sobre la estructura de un sistema DNS y los diferentes componentes que deben funcionar correctamente para que la resolución del nombre sea exitosa. Las fallas del DNS provocan la falla de todas las aplicaciones de usuario final que dependen de una resolución de nombre. Es importante verificar siempre la disponibilidad y la funcionalidad del DNS cuando los usuarios informan la falla de múltiples aplicaciones de la red.

**Objetivo:** Describir el impacto de las aplicaciones (Voz sobre IP y Video sobre IP) en una red

Capítulos de revisión de **CCNA Discovery: Networking para el hogar y pequeñas empresas:**

**Servicios de red:** en la sección **Cientes, servidores y su interacción**, el tema **Protocolos de transporte TCP y UDP** explica por qué el TCP no es una buena elección para la transmisión de tráfico de voz y de video por la red. El tema **Cientes y servidores de voz** describe la funcionalidad de la telefonía IP de Internet.

Capítulos de revisión de **CCNA Discovery: Trabajar en una pequeña o mediana empresa o ISP:**

**Servicios del SP:** las diferentes características de TCP y UDP se describen en el tema **Protocolos de la capa de transporte** dentro de la sección **Protocolos que admiten los servicios del ISP**.

**Actividades prácticas:**

1. Cree una tabla que enumere todas las aplicaciones comunes de Internet y de la red. Para cada aplicación, escriba el protocolo, la asignación de puerto predeterminado y si la aplicación utiliza o no TCP o UDP. En algunos casos, tales como voz o video, es probable que no se reconozca el puerto.

Ejemplo:

| Aplicación                    | Protocolo de aplicación | Puerto | Protocolo de transporte |
|-------------------------------|-------------------------|--------|-------------------------|
| Explorador Web                | http                    | 80     | TCP                     |
| Búsqueda de nombre de dominio | Dns                     | 53     | TCP y UDP               |

2. Identifique todas las aplicaciones del cliente que están instaladas en su computadora. Determine a qué tipo de servidor se conecta cada una para obtener información.
3. Utilice el comando netstat para ver cuántas conexiones TCP se inician cuándo observa una página Web o envía un correo electrónico.

## Prácticas y dispositivos de seguridad de la red

**Objetivo:** Describir las crecientes amenazas actuales de seguridad de la red y la necesidad de implementar una política de seguridad integral para mitigarlas

Capítulos de revisión de **CCNA Discovery: Networking para el hogar y pequeñas empresas:**

**Seguridad básica:** las primeras tres secciones en este capítulo describen las amenazas, los métodos de ataque y los requisitos de las políticas de seguridad para redes domésticas y de pequeñas empresas. El tema **Medidas de seguridad comunes** explica la necesidad de una política de seguridad integral y qué debería contemplar la política. Asegúrese de revisar el material que se encuentra en el gráfico interactivo relacionado con dicho tema.

Capítulos de revisión de **CCNA Discovery: Trabajar en una pequeña o mediana empresa o ISP:**

**Responsabilidad del Proveedor de servicios de Internet (ISP, Internet Service Provider):** los ataques de denegación de servicio se describen en el tema **Listas de acceso y filtrado de puertos**. Las medidas a tomar para mitigar las amenazas a los dispositivos host se encuentran en el tema **Seguridad del host**.

**Objetivo:** Explicar los métodos generales para mitigar las amenazas de seguridad comunes en los dispositivos de red, en los hosts y en las aplicaciones

Capítulos de revisión de **CCNA Discovery: Networking para el hogar y pequeñas empresas:**

**Seguridad básica:** la sección **Política de seguridad** de este capítulo describe las medidas de seguridad recomendadas que se deben tomar para evitar muchos ataques maliciosos o no deseados en los hosts o en la red. Ponga atención al tipo de medida preventiva que se indica para qué tipo de ataque.

Capítulos de revisión de **CCNA Discovery: Trabajar en una pequeña o mediana empresa o ISP:**

**Responsabilidad del Proveedor de servicios de Internet (ISP, Internet Service Provider):** la primera sección de este capítulo, **Consideraciones de seguridad del ISP**, se enfoca en las mejores prácticas de seguridad y en los problemas de seguridad comunes que enfrentan los ISP y sus clientes.

**Objetivo:** Describir las funciones de las aplicaciones comunes de seguridad y las aplicaciones en general.

Capítulos de revisión de **CCNA Discovery: Networking para el hogar y pequeñas empresas:**

**Seguridad básica:** los firewall y el filtrado de puertos se presentan en la sección **Uso de firewalls**. Se enumeran los diferentes métodos que utilizan los firewalls para determinar qué tráfico se permite o se deniega. La animación en el tema **Uso de firewalls** ejemplifica el concepto de las zonas de seguridad diferentes. Este tema también incluye una práctica de laboratorio para practicar la configuración de los parámetros del firewall.

Capítulos de revisión de **CCNA Discovery: Trabajar en una pequeña o mediana empresa o ISP:**

**Responsabilidad del Proveedor de servicios de Internet (ISP, Internet Service Provider):** la sección **Herramientas de seguridad** describe los distintos tipos de tecnologías de seguridad que se utilizan en las redes y los tipos de amenazas contra los que cada una protege. Garantizar la seguridad de una red es una de las tareas más importantes que realiza un técnico o ingeniero de redes. Asegúrese de que puede comprender la función de cada tipo de medida de seguridad a detalle. Los tipos de medidas de seguridad necesarias para asegurar las LAN inalámbricas se analizan en el tema **Seguridad inalámbrica**.

**Objetivo:** Describir las prácticas de seguridad recomendadas, incluyendo los pasos iniciales para asegurar los dispositivos de red

Capítulos de revisión de **CCNA Discovery: Networking para el hogar y pequeñas empresas:**

**Tecnologías inalámbricas:** la sección *Consideraciones de seguridad en una LAN inalámbrica* contiene información sobre cómo proteger un punto de acceso inalámbrico.

Capítulos de revisión de **CCNA Discovery: Trabajar en una pequeña o mediana empresa o ISP:**

**Configuración de dispositivos de red:** el tema *Configuración básica* en *Configuración de un router con la CLI del IOS* describe cómo establecer las contraseñas para obtener acceso a los modos usuario y privilegiado. También incluye los comandos para permitir el acceso Telnet al dispositivo y establecer las contraseñas de inicio de acceso VTY (Telnet). Se recomienda encriptar todas las contraseñas en un dispositivo con la función de servicio password-encryption. Los comandos para establecer las contraseñas y mensajes son los mismos en un switch Cisco que en un router ISR. Las medidas de seguridad adicionales en un switch se describen en el tema *Conexión del switch de la LAN al router*.

#### Actividades prácticas:

1. Elabore una lista de verificación para establecer la seguridad básica de los principales dispositivos de networking. Router, switch, punto de acceso inalámbrico integrado. Practique la configuración de la seguridad básica en cada uno de los dispositivos.
2. Cree una tabla de las principales tecnologías de seguridad de la red: firewalls, listas de acceso, IPS, IDS, servicios de registro, autenticación, autorización y métodos de encriptación. Describa la función de cada tecnología y contra qué amenazas protege cada una. Indique qué tecnologías tienen base en el host y cuáles se implementan en los dispositivos o aparatos de red.

Ejemplo:

| Tecnología de seguridad | Función   | Protección contra amenaza   | Basada en host | Basada en la red |
|-------------------------|---|---|----------------|------------------|
| Listas de acceso        | Filtra el tráfico según la dirección o puerto de origen o destino.                  | Evita que el tráfico no deseado ingrese a la red o al proceso del host.                                   | Sí             | Sí               |
| Protección contra virus | Identifica software malicioso según el patrón de tráfico o de contenido del archivo | Evita que el software malicioso provoque daño a los archivos host o que se produzca un exceso de tráfico. | Sí             | No               |

3. Enumero los temas que se deben incluir en la política de seguridad.
4. Enumere las mejores prácticas para proteger redes y hosts.