Hasta este punto en el curso, hemos considerado los servicios que una red de datos puede proporcionar a la red humana, hemos examinado las características de cada capa del modelo OSI y las operaciones de los protocolos TCP/IP y observamos en detalle Ethernet, una tecnología LAN universal. El siguiente paso consiste en aprender cómo reunir estos elementos para formar una red que funcione y se pueda mantener.

La mayoría de las empresas son pequeñas empresas. Por lo tanto, es de esperarse que la mayoría de las redes sean redes pequeñas.

En las redes pequeñas, el diseño de la red suele ser simple. La cantidad y el tipo de dispositivos en la red se reducen considerablemente en comparación con una red más grande. En general, las topologías de red para las redes pequeñas constan de un único router y uno o más switches. Las redes pequeñas también pueden tener puntos de acceso inalámbrico (posiblemente incorporados al router) y teléfonos IP. En cuanto a la conexión a Internet, las redes pequeñas normalmente tienen una única conexión WAN proporcionada por una conexión DSL, por cable o Ethernet.

La administración de una red pequeña requiere muchas de las mismas habilidades necesarias para administrar redes más grandes. La mayor parte del trabajo se centra en el mantenimiento y la resolución de problemas de equipos existentes, así como en la protección de los dispositivos y de la información de la red. La administración de las redes pequeñas está a cargo de un empleado de la compañía o de una persona contratada por esta, según el tamaño de la empresa y el tipo de actividad que realice.

En la ilustración, se muestra la típica red de una pequeña empresa.

Para cumplir con los requisitos de los usuarios, incluso las redes pequeñas requieren planificación y diseño. La planificación asegura que se consideren debidamente todos los requisitos, factores de costo y opciones de implementación.

Una de las primeras consideraciones de diseño al implementar 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**

Generalmente, el costo es uno de los factores más importantes al seleccionar equipos para la red de una pequeña empresa. 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 la consideración del costo es la cantidad de redundancia que se debe incorporar a la red; esto incluye los dispositivos, los puertos por dispositivo y el cableado de cobre o fibra óptica.

**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 preguntas que se deben hacer incluyen las siguientes: “¿Pedimos los puertos suficientes para satisfacer las necesidades actuales o tenemos en cuenta los requisitos de crecimiento?”, “¿necesitamos una mezcla de velocidades UTP?” y “¿necesitamos puertos UTP y de fibra?”.

Las PC más modernas tienen NIC de 1 Gbps incorporadas. Algunos servidores y estaciones de trabajo ya vienen con puertos de 10 Gbps 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. La mayoría de estos dispositivos incluyen una cantidad básica de puertos fijos además de ranuras de expansión. Existen switches con puertos adicionales especiales para uplinks de alta velocidad optativos. Asimismo, se debe tener el cuidado de seleccionar las interfaces y los módulos adecuados para los medios específicos, ya que los routers pueden utilizarse para conectar diferentes cantidades y tipos de redes. Las preguntas que se deben tener en cuenta incluyen las siguientes: “¿Pedimos dispositivos con módulos que se puedan actualizar?” y “¿qué tipos de interfaces WAN se requieren en los routers (si son necesarias)?”.

**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
* QoS
* VoIP
* Conmutación de Capa 3
* NAT
* DHCP

Los routers pueden ser costosos según las interfaces y las características necesarias. Los módulos adicionales, como la fibra óptica, aumentan el costo de los dispositivos de red.

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. Incluso en una red pequeña, la asignación de direcciones dentro de la red no debe ser aleatoria. En lugar de esto, se debe planificar, registrar y mantener un esquema de direccionamiento IP basado en el tipo de dispositivo que recibe 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 entre los rangos 50 y 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.

Haga clic en los botones de la ilustración para ver el método de asignación.

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. 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.

Cuanto más pequeña es la red, menor es la posibilidad de que la redundancia de los equipos sea accesible. Por lo tanto, un método frecuente para incorporar redundancia consiste en el uso de conexiones de switch redundantes entre varios switches en la red, y entre switches y routers.

Además, los servidores suelen tener varios puertos de NIC que habilitan conexiones redundantes a uno o más switches. En las redes pequeñas, los servidores generalmente se implementan como servidores Web, servidores de archivos o servidores de correo electrónico.

Por lo general, las redes pequeñas proporcionan un único punto de salida a Internet a través de uno o más gateways predeterminados. Con un router en la topología, la única redundancia en términos de rutas de capa 3 se obtiene utilizando más de una interfaz Ethernet interna en el router. Sin embargo, si el router falla, toda la red pierde la conectividad a Internet. Por este motivo, puede ser recomendable para las pequeñas empresas contratar una cuenta con una opción de menor costo a un segundo proveedor de servicios a modo de respaldo.

Los usuarios esperan un acceso inmediato a sus correos electrónicos y a los archivos que están compartiendo o actualizando. Para contribuir al aseguramiento de esta disponibilidad, el diseñador de la red debe llevar a cabo los siguientes pasos:

**Paso 1.** Aportar seguridad a los servidores de archivos y de correo en una ubicación centralizada.

**Paso 2.** Proteger la ubicación contra el acceso no autorizado mediante la implementación de medidas de seguridad lógica y física.

**Paso 3.** Crear redundancia en la granja de servidores para asegurar que no se pierdan los archivos si falla un dispositivo.

**Paso 4.** Configurar rutas redundantes a los servidores.

Además, en las redes modernas suelen utilizarse alguna forma de video o voz sobre IP para comunicarse con los clientes y los socios comerciales. Este tipo de red convergente se implementa como solución integrada o como forma adicional de datos sin procesar superpuestos en la red IP. 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 video, 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. Las clases de tráfico pueden ser tan específicas como las siguientes:

* Transferencia de archivos
* Correo electrónico
* Voz
* Video
* Mensajería
* Transaccional

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.

La utilidad de las redes depende de las aplicaciones que se encuentren en ellas. Como se muestra en la ilustración, dentro de la capa de aplicación 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 exploradores 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 video, 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.

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 incluyen los siguientes:

* DNS
* Telnet
* IMAP, SMTP, POP (correo electrónico)
* DHCP
* HTTP
* FTP

Haga clic en los servidores de la ilustración para ver una descripción breve de los servicios de red que proporciona cada uno.

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

Además de los protocolos de red comunes que se describieron anteriormente, las empresas modernas, incluso las pequeñas, suelen utilizar aplicaciones en tiempo real para comunicarse con los clientes y los socios. Si bien es posible que una compañía pequeña no pueda justificar el costo de una solución Cisco Telepresence para empresas, existen otras aplicaciones en tiempo real, como se muestra en la figura 1, que son accesibles y justificables para las pequeñas empresas. En comparación con otros tipos de datos, las aplicaciones en tiempo real requieren más planificación y servicios dedicados para asegurar la entrega prioritaria del tráfico de voz y de video. Esto significa que 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. En la figura 2, se muestran elementos de una red pequeña que admiten aplicaciones en tiempo real.

**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. El cableado que puede admitir transmisiones en gigabits debe ser capaz de transportar el tráfico generado sin necesitar ningún cambio en la infraestructura. Los switches más antiguos quizás no admitan alimentación por Ethernet (PoE). El cableado obsoleto quizás no admita los requisitos de ancho de banda. Los switches y el cableado necesitarán ser actualizados para admitir estas aplicaciones.

**VoIP**

VoIP se implementa en organizaciones que todavía utilizan teléfonos tradicionales. VoIP utiliza routers con capacidades de voz. Estos routers convierten la voz analógica de señales telefónicas tradicionales en paquetes IP. 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. Las soluciones de video y voz sobre IP para pequeñas empresas pueden consistir, por ejemplo, en Skype y en las versiones no empresariales de Cisco WebEx.

**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. En la actualidad, existen numerosos proveedores que ofrecen soluciones de telefonía IP dedicada para redes pequeñas.

**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.

El crecimiento es un proceso natural para muchas pequeñas empresas, y sus redes deben crecer en consecuencia. El administrador de una red pequeña trabajará de forma reactiva o proactiva, según la mentalidad de los directores de la compañía, que a menudo incluyen al administrador de red. 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 compañía.

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.

Para admitir y ampliar una red pequeña, se necesita estar familiarizado con los protocolos y las aplicaciones de red que se ejecutan en ella. Si bien en entornos de redes pequeñas los administradores tienen más tiempo para analizar individualmente el uso de la red por parte de cada dispositivo, se recomienda un enfoque más integral con algún tipo de analizador de protocolos basado en software o hardware.

Como se muestra en la ilustración, los analizadores de protocolos permiten que los profesionales de red recopilen información estadística sobre los flujos de tráfico en una red rápidamente.

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, el 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 porque parte del tráfico es local en un segmento en particular.

La información recopilada por el analizador de protocolos se analiza 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.

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:

* OS y versión del OS
* 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. Por ejemplo, es posible que algunos empleados utilicen recursos externos, como los medios sociales, para posicionar mejor una compañía en términos de marketing. Cuando estos empleados comenzaron a trabajar para la compañía, es posible que no le hayan dado tanta importancia a la publicidad basada en Internet. Este cambio en la utilización de recursos puede requerir que el administrador de red cambie la asignación de los recursos de red en consecuencia.

Es responsabilidad del administrador de red realizar un seguimiento de los requisitos de utilización y de flujo de tráfico de la red, e implementar modificaciones en la red para optimizar la productividad de los empleados a medida que la red y la empresa crecen.

Ya sean redes conectadas por cable o inalámbricas, las redes de computadoras son cada vez más fundamentales para las actividades cotidianas. Tanto las personas como las organizaciones dependen de las PC y las redes. Las intrusiones de personas no autorizadas pueden causar interrupciones costosas en la red y pérdidas de trabajo. Los ataques a una red pueden ser devastadores y pueden causar pérdida de tiempo y de dinero debido a los daños o robos de información o de activos importantes.

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
* Robo de identidad
* Pérdida o manipulación de datos
* Interrupción del servicio

Haga clic en las imágenes de la ilustración para obtener más información.

Incluso en las redes pequeñas, se deben tener en cuenta las amenazas y vulnerabilidades de seguridad al planificar una implementación de red.

Cuando se piensa en seguridad de red, o incluso en seguridad informática, es posible que se piense en atacantes que explotan las vulnerabilidades de software. Una vulnerabilidad igualmente importante es la seguridad física de los dispositivos, como se muestra en la ilustración. Si los recursos de red están expuestos a riesgos físicos, un atacante puede denegar el uso de dichos recursos.

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

Algunos de estos problemas se deben abordar en las políticas de la organización. Algunos de ellos dependen de una buena dirección y administración de la organización.

Tres factores de seguridad de red son la vulnerabilidad, las amenazas y los ataques.

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.

Las amenazas incluyen a las personas interesadas en aprovechar cada debilidad de seguridad y capacitadas para hacerlo. Es de esperarse que estas personas busquen continuamente nuevas vulnerabilidades y debilidades de seguridad.

Las amenazas se llevan a cabo con una variedad de herramientas, secuencias de comandos y programas para iniciar ataques contra las redes y los dispositivos de red. 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.

Todas estas vulnerabilidades o debilidades pueden dar origen a diversos ataques, incluidos los ataques de código malintencionado y los ataques de red.

Los ataques de código malintencionado incluyen diversos tipos de programas de PC que se crearon con la intención de causar pérdida de datos o daños a estos. Los tres tipos principales de ataques de código malintencionado son los virus, los caballos de Troya y los gusanos.

Un virus es un tipo de software malintencionado que se asocia a otro programa para ejecutar una función no deseada específica en una estación de trabajo. Un ejemplo es un programa que se asocia a command.com (el intérprete principal para los sistemas Windows), elimina determinados archivos e infecta cualquier otra versión de command.com que pueda encontrar.

Un caballo de Troya solo se diferencia en que toda la aplicación se creó con el fin de que aparente ser otra cosa, cuando en realidad es una herramienta de ataque. Un ejemplo de un caballo de Troya es una aplicación de software que ejecuta un juego simple en una estación de trabajo. Mientras el usuario se entretiene con el juego, el caballo de Troya envía una copia de sí mismo por correo electrónico a cada dirección de la libreta de direcciones del usuario. Los demás usuarios reciben el juego y lo utilizan, por lo que el caballo de Troya se propaga a las direcciones de cada libreta de direcciones.

En general, los virus requieren un mecanismo de entrega, un vector, como un archivo zip o algún otro archivo ejecutable adjunto a un correo electrónico, para transportar el código del virus de un sistema a otro. El elemento clave que distingue a un gusano de PC de un virus de computadora es que se requiere interacción humana para facilitar la propagación de un virus.

Los gusanos son programas autónomos que atacan un sistema e intentan explotar una vulnerabilidad específica del objetivo. Una vez que logra explotar dicha vulnerabilidad, el gusano copia su programa del host atacante al sistema atacado recientemente para volver a iniciar el ciclo. La anatomía de un ataque de gusano es la siguiente:

* **Vulnerabilidad habilitadora:** el gusano se instala mediante la explotación de las vulnerabilidades conocidas de los sistemas, como usuarios finales ingenuos que abren archivos adjuntos ejecutables sin verificar en los correos electrónicos.
* **Mecanismo de propagación:** después de obtener acceso a un host, el gusano se copia a dicho host y luego selecciona nuevos objetivos.
* **Contenido:** una vez que se infectó un host con el gusano, el atacante tiene acceso al host, a menudo como usuario privilegiado. Los atacantes pueden utilizar una vulnerabilidad local para elevar su nivel de privilegio al de administrador.

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 no autorizadas 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.

**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.

Haga clic en cada tipo de herramienta de ataque de reconocimiento para ver una animación del ataque.

**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. Uno de los tipos de ataques de acceso más comunes es el ataque a contraseñas. Los ataques a contraseñas se pueden implementar con programas detectores de paquetes para obtener cuentas de usuario y contraseñas que se transmiten como texto no cifrado. Los ataques a contraseñas también pueden referirse a los intentos repetidos de inicio de sesión en un recurso compartido, como un servidor o un router, para identificar una cuenta de usuario, una contraseña o ambas. Estos intentos repetidos se denominan “ataques por diccionario” o “ataques de fuerza bruta”.

Haga clic en los botones de la ilustración para ver ejemplos de ataques de acceso.

**Denegación de servicio**

Los ataques 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.

Haga clic en los botones de la ilustración para ver ejemplos de ataques de Dos y DDos.

Los softwares antivirus pueden detectar la mayoría de los virus y muchas aplicaciones de caballo de Troya, y evitar que se propaguen en la red. Los softwares antivirus se pueden implementar en el nivel de usuario y en el nivel de red.

Mantenerse actualizado con los últimos avances en estos tipos de ataques también puede contribuir a una defensa más eficaz contra ellos. A medida que se publican nuevas aplicaciones de virus y troyanos, las empresas deben mantenerse al día con actualizaciones a las versiones más recientes de los softwares antivirus.

La mitigación de ataques de gusanos requiere la diligencia del personal de administración de redes y sistemas. Los siguientes son los pasos recomendados para mitigar ataques de gusanos:

* **Contención:** contenga la propagación del gusano dentro de la red. Divida en secciones las partes no infectadas de la red.
* **Inoculación:** comience a aplicar parches a todos los sistemas y, si es posible, examine en busca de sistemas vulnerables.
* **Cuarentena:** realice un seguimiento de todas las máquinas infectadas dentro de la red. Desconecte o quite las máquinas infectadas de la red o bloquéelas.
* **Tratamiento:** limpie todos los sistemas infectados y aplíqueles parches. Es posible que algunos gusanos requieran la reinstalación completa del sistema central para limpiar el sistema.

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. Esto resulta difícil con los sistemas de usuario no controlados en la red local. 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, como el que se muestra en la ilustración. Todo parche que no esté aplicado en un host se descarga automáticamente del servidor de parches y se instala sin que intervenga el usuario.

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 observar las acciones que realizan mientras acceden a la red (contabilizar). AAA proporciona un mayor grado de escalabilidad que los comandos de autenticación de EXEC privilegiado, consola, puertos auxiliares y VTY.

**Autenticación**

Los usuarios y administradores deben probar que son quienes dicen ser. La autenticación se puede establecer utilizando combinaciones de nombre de usuario y contraseña, preguntas de desafío y respuesta, tarjetas token y otros métodos. Por ejemplo: “Soy el usuario ‘estudiante’. Conozco la contraseña para probar que soy el usuario ‘estudiante’”.

En redes pequeñas, se suele utilizar la autenticación local. Con la autenticación local, cada dispositivo mantiene su propia base de datos de combinaciones de nombre de usuario y contraseña. Sin embargo, cuando hay más de unas pocas cuentas de usuario en la base de datos de un dispositivo local, administrar dichas cuentas puede resultar complejo. Además, a medida que la red crece y se le agregan más dispositivos, la autenticación local se hace difícil de mantener y no se puede escalar. Por ejemplo, si hay 100 dispositivos de red, se deben agregar todas las cuentas de usuario a los 100 dispositivos.

En el caso de redes más grandes, una solución más escalable es la autenticación externa. La autenticación externa permite autenticar a todos los usuarios a través de un servidor de red externo. Las dos opciones más populares para la autenticación externa de usuarios son RADIUS y TACACS+:

* RADIUS es un estándar abierto con poco uso de memoria y recursos de la CPU. Lo utilizan una variedad de dispositivos de red, como switches, routers y dispositivos inalámbricos.
* TACACS+ es un mecanismo de seguridad que habilita servicios modulares de autenticación, autorización y contabilidad. Utiliza un demonio TACACS+ que se ejecuta en un servidor de seguridad.

**Autorización**

Una vez autenticado el usuario, los servicios de autorización determinan a qué recursos puede acceder el usuario y qué operaciones está habilitado para realizar. Un ejemplo es “El usuario ‘estudiante’ puede acceder al servidor host XYZ mediante Telnet únicamente”.

**Contabilidad**

La contabilidad registra lo que hace el usuario, incluidos los elementos a los que accede, la cantidad de tiempo que accede al recurso y todos los cambios que se realizaron. La contabilidad realiza un seguimiento de la forma en que se utilizan los recursos de red. Un ejemplo es “El usuario ‘estudiante" accedió al servidor host XYZ mediante Telnet durante 15 minutos”.

El concepto de AAA es similar al uso de una tarjeta de crédito. La tarjeta de crédito identifica quién la puede utilizar y cuánto puede gastar ese usuario, y lleva un registro de los elementos en los que el usuario gastó dinero, como se muestra en la ilustración.

Además de proteger las computadoras y servidores individuales conectados a la red, es importante controlar el tráfico de entrada y de salida de la red.

El firewall es una de las herramientas de seguridad más eficaces disponibles para la protección de los usuarios internos de la red contra amenazas externas. El firewall reside entre dos o más redes y controla el tráfico entre ellas, además de evitar el acceso no autorizado. 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 de paquetes con estado (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. Además, los firewalls suelen llevar a cabo la traducción de direcciones de red (NAT). La NAT traduce una dirección o un grupo de direcciones IP internas a una dirección IP pública y externa que se envía a través de la red. Esto permite ocultar las direcciones IP internas de los usuarios externos.

Los productos de firewall vienen en distintos formatos, como se muestra en la ilustración.

* **Firewalls basados en aplicaciones:** un firewall basado en una aplicación es un firewall incorporado en un dispositivo de hardware dedicado, conocido como una aplicación de seguridad.
* **Firewalls basados en servidor:** un firewall basado en servidor consta de una aplicación de firewall que se ejecuta en un sistema operativo de red (NOS), como UNIX o Windows.
* **Firewalls integrados:** un firewall integrado se implementa mediante la adición de funcionalidades de firewall a un dispositivo existente, como un router.
* **Firewalls personales:** los firewalls personales residen en las computadoras host y no están diseñados para implementaciones LAN. Pueden estar disponibles de manera predeterminada en el OS o pueden provenir de un proveedor externo.

Una red es apenas tan segura como su enlace más débil. Las amenazas destacadas que más se analizan en los medios de comunicación son las amenazas externas, como los gusanos de Internet y los ataques DoS. Pero la protección de la red interna es tan importante como la protección del perímetro de una red. La red interna consta de terminales de red, algunas de las cuales se muestran en la ilustración. Una terminal, o un host, es un sistema de computación o un dispositivo individual que actúa como cliente de red. Las terminales comunes son computadoras portátiles, computadoras de escritorio, servidores, smartphones y tablet PC. Si los usuarios no aplican seguridad a los dispositivos terminales, ninguna precaución de seguridad garantizará una red segura.

La seguridad de los dispositivos terminales es uno de los trabajos más desafiantes para un administrador de red, ya que incluye a la naturaleza humana. Las compañías deben aplicar políticas bien documentadas, y los empleados deben estar al tanto de estas reglas. Se debe capacitar a los empleados sobre el uso correcto de la red. En general, estas políticas incluyen el uso de software antivirus y la prevención de intrusión de hosts. Las soluciones más integrales de seguridad de terminales dependen del control de acceso a la red.

La seguridad de terminales también requiere la protección de los dispositivos de capa 2 en la infraestructura de la red, a fin de evitar ataques de capa 2, como los ataques de suplantación de direcciones MAC, los de desbordamiento de la tabla de direcciones MAC y los ataques de saturación de LAN. Esto se conoce como “mitigación de ataques”.

Una parte de la seguridad de la red consiste en proteger los dispositivos propiamente dichos, incluidos los dispositivos finales y los intermediarios, como los dispositivos de red.

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, como se describe en la ilustración. 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.

Se deben actualizar todos los dispositivos con parches de seguridad a medida que estén disponibles. A menudo, los dispositivos enviados por el fabricante pasaron cierto tiempo en un depósito y no tienen los parches más actualizados instalados. Antes de la implementación, es importante actualizar cualquier software e instalar los parches de seguridad.

Para proteger los dispositivos de red, es importante utilizar contraseñas seguras. Las pautas estándar que se deben seguir son las siguientes:

* Utilice una longitud de contraseña de, al menos, ocho caracteres y preferentemente de diez caracteres o más. Cuanto más larga sea, mejor será la contraseña.
* Cree contraseñas complejas. Incluya una combinación de letras mayúsculas y minúsculas, números, símbolos y espacios, si están permitidos.
* Evite las contraseñas basadas en la repetición, las palabras comunes de diccionario, las secuencias de letras o números, los nombres de usuario, los nombres de parientes o mascotas, información biográfica (como fechas de nacimiento), números de identificación, nombres de antepasados u otra información fácilmente identificable.
* Escriba una contraseña con errores de ortografía a propósito. Por ejemplo, Smith = Smyth = 5mYth, o Seguridad = 5egur1dad.
* Cambie las contraseñas con frecuencia. Si se pone en riesgo una contraseña sin saberlo, se limitan las oportunidades para que el atacante la utilice.
* No anote las contraseñas ni las deje en lugares obvios, por ejemplo, en el escritorio o el monitor.

En la ilustración, se muestran ejemplos de contraseñas seguras y no seguras.

En los routers Cisco, se ignoran los espacios iniciales para las contraseñas, pero no se ignoran los espacios que le siguen al primer carácter. Por lo tanto, un método para crear una contraseña segura es utilizar la barra espaciadora en la contraseña y crear una frase compuesta de muchas palabras. Esto se denomina “frase de contraseña”. Una frase de contraseña suele ser más fácil de recordar que una contraseña simple. Además, es más larga y más difícil de descifrar.

Los administradores deben asegurarse de que se utilicen contraseñas seguras en toda la red. Una forma de lograr esto es utilizar las mismas herramientas de ataque por “fuerza bruta” que utilizan los atacantes como método para verificar la seguridad de la contraseña.

Al implementar dispositivos, es importante seguir todas las pautas de seguridad establecidas por la organización. Esto incluye la denominación de dispositivos de tal manera que facilite las tareas de registro y seguimiento, pero que también mantenga algún tipo de seguridad. No se recomienda proporcionar demasiada información sobre el uso del dispositivo en el nombre de host. Existen muchas otras medidas básicas de seguridad que se deben implementar.

**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 la encriptación de todas las contraseñas sin encriptar.

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.

**Mensajes**

Los mensajes de aviso son similares a los avisos de prohibición de entrada. Son importantes para poder demandar en un tribunal a cualquiera que acceda al sistema de forma inapropiada. Asegúrese de que los mensajes de aviso cumplan con las políticas de seguridad de la organización.

Router(config)# **banner motd #message#**

**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.

Router(config)# **line vty 0 4**

Router(config-vty)# **exec-timeout 10**

Este comando desconecta a los usuarios después de 10 minutos.

**Acceso remoto mediante SSH**

El antiguo protocolo para administrar dispositivos de manera remota es Telnet. Telnet no es seguro. Los datos contenidos en un paquete Telnet se transmiten sin encriptar. Mediante una herramienta como Wireshark, es posible que alguien detecte una sesión de Telnet y obtenga información de contraseñas. 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***nombre-de-dominio* en el modo de configuración global.

**Paso 2.** Se deben generar claves secretas unidireccionales para que un router encripte el tráfico SSH. La clave es precisamente lo que se utiliza para encriptar y descifrar datos. Para crear una clave de encriptación, utilice el comando **crypto key generate rsa general-keys modulus***tamaño-del-módulo* en el modo de configuración global. El significado específico de las distintas partes de este comando es complejo y excede el ámbito de este curso, pero de momento, simplemente tenga en cuenta que el módulo determina el tamaño de la clave y se puede configurar con un valor de 360 a 2048 bits. Cuanto más grande es el módulo, más segura es la clave, pero más se tarda en encriptar y descifrar la información. La longitud mínima de módulo recomendada es de 1024 bits.

Router(config)# **crypto key generate rsa general-keys modulus 1024**

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

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

Ahora se puede acceder al servicio SSH del router mediante un software de cliente SSH.

Una vez que se implementa la red, el administrador debe poder probar la conectividad de red para asegurarse de que funcione correctamente. Además, se recomienda que el administrador de red realice un registro de la red.

**El comando ping**

El comando **ping** es una manera eficaz de probar la conectividad. Por lo general, a esta prueba se la conoce como “prueba del stack de protocolos”, porque el comando**ping** va desde la capa 3 del modelo OSI hasta la capa 2 y, luego, hasta la capa 1. Este comando utiliza el protocolo ICMP para verificar la conectividad.

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.

El comando **ping** proporciona un método para probar el stack de protocolos y la configuración de direcciones IPv4 en un host, así como para probar la conectividad a los hosts de destino local o remoto, como se muestra en la ilustración. Existen herramientas adicionales que pueden proporcionar más información que el **ping**, como Telnet o Trace, las cuales serán analizadas luego en mayor profundidad.

**Indicadores de ping IOS**

Un ping emitido desde el IOS tiene como resultado una de varias indicaciones para cada eco ICMP enviado. Los indicadores más comunes son:

* **!** : indica la recepción de un mensaje de respuesta de eco ICMP.
* **.** : indica que se agotó el tiempo mientras se esperaba un mensaje de respuesta de eco ICMP.
* **U**: se recibió un mensaje ICMP inalcanzable.

El signo “**!**” (signo de exclamación) indica que el ping se completó correctamente y verifica la conectividad de capa 3.

El "**.**" (punto) puede indicar problemas en la comunicación. 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.

La “**U**” indica que un router de la ruta no contaba con una ruta hacia la dirección de destino o que se bloqueó la solicitud de ping y se respondió con un mensaje de ICMP de destino inalcanzable.

**Prueba de loopback**

El comando **ping** se utiliza para verificar la configuración IP interna en el host local. Recuerde que esta prueba se realiza utilizando el comando **ping** en una dirección reservada denominada “dirección de loopback” (127.0.0.1). Esto verifica que el stack de protocolos funcione correctamente desde la capa de red hasta la capa física y viceversa, sin colocar realmente una señal en los medios.

**Los comandos**ping se introducen en una línea de comandos.

Utilice la siguiente sintaxis para hacer ping a la dirección de loopback:

C:\> **ping 127.0.0.1**

La respuesta de este comando se parecería a ésta:

Respuesta desde 127.0.0.1: bytes=32 tiempo<1ms TTL=128

Respuesta desde 127.0.0.1: bytes=32 tiempo<1ms TTL=128

Respuesta desde 127.0.0.1: bytes=32 tiempo<1ms TTL=128

Respuesta desde 127.0.0.1: bytes=32 tiempo<1ms TTL=128

Estadísticas de ping para 127.0.0.1:

Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),

Tiempo aproximado de ida y vuelta en milisegundos:

Mínimo = 0ms, Máximo = 0ms, Media = 0ms

El resultado indica que se enviaron cuatro paquetes de prueba de 32 bytes desde el host 127.0.0.1 y se devolvieron a este en un tiempo de menos de 1 ms. TTL son las siglas de tiempo de vida, que define la cantidad de saltos que le restan al paquete ping antes de que se descarte.

Cisco IOS ofrece un modo “extendido” del comando ping. Se ingresa a este modo escribiendo “ping” (sin las comillas) en el modo EXEC privilegiado, sin una dirección IP de destino. Luego, se presenta una serie de peticiones de entrada, como se muestra en el siguiente ejemplo. Al presionar Intro se aceptan los valores predeterminados indicados. El siguiente 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 de forma remota (desde el R2) que el R1 tenga la ruta 10.1.1.0/24 en su tabla de enrutamiento.

R2#**ping**

Protocol [ip]:

Target IP address:**192.168.10.1**

Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]:**y**

Source address or interface:**10.1.1.1**

Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]:

Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 36/97/132 ms

Al ingresar un período de tiempo de espera más prolongado que el predeterminado, se podrán detectar posibles problemas de latencia. Si la prueba de ping es exitosa con un valor superior, existe una conexión entre los hosts, pero es posible que haya un problema de latencia en la red.

Tenga en cuenta que introducir “y” en la petición de entrada “Extended commands” (Comandos extendidos) proporciona más opciones que resultar útiles para la resolución de problemas.

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. Una línea de base es un proceso para estudiar la red en intervalos regulares a fin de asegurar que la red funciona según su diseño. Una línea de base de red es más que un simple informe que detalla el estado de la red en determinado momento. 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 que deriva de los comandos de la red puede aportar 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 otro comando relevante. Estos archivos de texto pueden tener grabada la fecha y la hora y pueden guardarse en un archivo para su posterior recuperación.

Un uso eficaz de la información almacenada consiste en comparar los resultados en el transcurso del tiempo (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.

No bastan las palabras para destacar la importancia de crear documentación. La verificación de la conectividad de host a host, los problemas de latencia y las resoluciones de problemas identificados puede ayudar a un administrador de red a mantener el funcionamiento más eficiente posible de la red.

Las redes corporativas deben tener líneas de base 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, solo se abarcan algunas técnicas básicas y se analiza el propósito de las líneas de base.

Las prácticas recomendadas para los procesos de línea de base se pueden encontrar [aquí](http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a008014fb3b.shtml)  .

La captura del resultado del comando **ping** también se puede completar desde la petición de entrada del IOS, como se muestra en la figura 4.

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 Windows, utilice **tracert**. Cuando lleve a cabo el rastreo desde la CLI de un router, utilice **traceroute**, como se muestra en la figura 1.

Al igual que los comandos **ping**, los comandos **trace** se introducen en la línea de comandos y llevan una dirección IP como argumento.

Aquí, sobre la base de que el comando se emite desde un equipo Windows, se utiliza la forma **tracert**:

C:\> **tracert 10.1.0.2**

Traza a 10.1.0.2 sobre caminos de 30 saltos como máximo

1 2 ms 2 ms 2 ms 10.0.0.254

2 \* \* \* Tiempo de espera agotado.

3 \* \* \* Tiempo de espera agotado.

4 ^C

La única respuesta correcta fue la del gateway del router A. El tiempo de espera para las solicitudes de trace se agotó, lo que significa que el router de siguiente salto no respondió. Los resultados del comando trace indican que la falla entonces se encuentra en la internetwork más allá de la LAN.

La captura del resultado del comando traceroute también se puede realizar desde la petición de entrada del router, como se muestra en la figura 2.

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.

Se puede mostrar el estado de casi todos los procesos o funciones del router mediante un comando **show**. Algunos de los comandos show más conocidos son:

* **show running-config** (figura 1).
* **show interfaces** (figura 2).
* **show arp** (figura 3).
* **show ip route** (figura 4).
* **show protocols** (figura 5)
* **show version** (figura 6)

Haga clic en los botones de la ilustración para obtener más información sobre los comandos **show**.

Una vez que se carga el archivo de configuración de inicio y el router arranca correctamente, se puede utilizar el comando **show version** para verificar y resolver los problemas de algunos de los componentes básicos de hardware y software que se utilizan durante el proceso de arranque. El resultado del comando **show version**incluye lo siguiente:

* La versión del software Cisco IOS que se está utilizando.
* La versión del software bootstrap del sistema almacenado en la memoria ROM que se utilizó inicialmente para arrancar el router.
* El nombre de archivo completo de la imagen IOS de Cisco y dónde lo colocó el programa bootstrap.
* El tipo de CPU del router y la cantidad de RAM. Es posible que resulte necesario actualizar la cantidad de RAM cuando se actualice el software Cisco IOS.
* La cantidad y el tipo de las interfases físicas del router.
* La cantidad de NVRAM. La NVRAM se utiliza para almacenar el archivo startup-config.
* La cantidad de memoria flash del router. Es posible que resulte necesario actualizar la cantidad de flash cuando se actualice el software Cisco IOS.
* El valor configurado actualmente del registro de configuración del software en formato hexadecimal.

Haga clic en Reproducir en la ilustración para ver una animación sobre la manera de identificar estas características del resultado de show version.

El registro de configuración le dice al router cómo iniciarse. Por ejemplo, la configuración predeterminada de fábrica para el registro de configuración es 0x2102. Este valor indica que el router intenta cargar una imagen del software Cisco IOS desde la memoria flash y carga el archivo de configuración de inicio desde la NVRAM. Es posible cambiar el registro de configuración y, por ende, cambiar dónde busca el router la imagen IOS de Cisco y el archivo de configuración de inicio durante el proceso de arranque. Si hay un segundo valor entre paréntesis se implica el valor del registro de configuración que se debe utilizar durante la siguiente recarga del router.

Haga clic en el ícono de Nota en la esquina inferior derecha de la ilustración para obtener más detalles sobre el registro de configuración.

En un switch, el comando **show version** muestra información acerca de la versión de software cargada actualmente, junto con información del hardware y del dispositivo. Algunos de los datos que muestra este comando son los siguientes:

* **Versión del software:** versión del software IOS.
* **Versión de bootstrap:** versión de bootstrap.
* **Tiempo de actividad del sistema:** tiempo transcurrido desde la última vez que se reinició.
* **Información de reinicio del sistema:** método de reinicio (por ejemplo, apagado y encendido, colapso).
* **Nombre de la imagen del software:** nombre del archivo de IOS.
* **Plataforma de switch y tipo de procesador**: número de modelo y tipo de procesador.
* **Tipo de memoria (compartida/principal)**: memoria RAM del procesador principal y almacenamiento en búfer de E/S de paquetes compartidos.
* **Interfaces de hardware:** interfaces disponibles en el switch.
* **Registro de configuración:** establece especificaciones de arranque, la configuración de velocidad de la consola y parámetros relacionados.

En la ilustración, se muestra un ejemplo del resultado típico del comando **show version** que se muestra en un switch.

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 un equipo Windows.

Una herramienta para analizar la dirección MAC de una PC es **ipconfig /all**. Observe que, en la figura 2, la dirección MAC de la PC ahora aparece junto con varios detalles relacionados con el direccionamiento de capa 3 del dispositivo. Intente utilizar este comando.

Además, se puede identificar el fabricante de la interfaz de red en la PC mediante la porción de OUI de la dirección MAC. Esto se puede investigar en Internet.

El servicio del cliente DNS en las PC de Windows optimiza el rendimiento de la resolución de nombres DNS almacenando previamente los nombres resueltos en la memoria. El comando **ipconfig /displaydns** muestra todas las entradas DNS en caché en un sistema de computación Windows.

El comando **arp** permite crear, editar y mostrar las asignaciones de direcciones físicas a direcciones IPv4 conocidas. El comando **arp** se ejecuta desde el símbolo del sistema de Windows.

Para ejecutar un comando **arp**, introduzca lo siguiente en el símbolo del sistema de un host:

C:\host1> **arp -a**

Como se muestra en la ilustración, 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 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.

Examine el resultado de los comandos **show cdp neighbors** de la figura 1, con la topología de la figura 2. Observe que R3 ha recopilado información detallada acerca de R2 y el switch conectado a la interfaz Fast Ethernet de R3.

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, ethernet0
* **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. El CDP revelará la dirección IP del vecino, independientemente de si puede hacer ping en el 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** ayuda a determinar si uno de los vecinos con CDP tiene un error de configuración IP.

En situaciones de detección de redes, la dirección IP del vecino con CDP suele ser la única información necesaria para conectarse a ese dispositivo mediante Telnet.

Por razones obvias, CDP puede suponer un riesgo para la seguridad. 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**.

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.

En la figura 2, haga clic en el botón R1. 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.

Según el resultado, la interfaz FastEthernet0/0 tiene la dirección IP 192.168.254.254. En las últimas dos columnas de esta línea, se muestra el estado de la capa 1 y de la capa 2 de esta interfaz. El valor **up** (activo) en la columna Status (Estado) muestra que esa interfaz opera en la capa 1. El valor **up** en la columna Protocol (Protocolo) indica que el protocolo de capa 2 funciona.

Observe también que la interfaz Serial 0/0/1 no se habilitó. Esto lo indica el valor **administratively down** (administrativamente inactiva) en la columna Status.

Como en cualquier dispositivo final, es posible verificar la conectividad de capa 3 con los comandos **ping** y **traceroute**. En este ejemplo, tanto el comando**ping**como el comando**trace**muestran una conectividad satisfactoria.

**Verificación de las interfaces del switch**

En la figura 2, haga clic en el botón S1. El comando **show ip interface brief** también se puede utilizar para verificar el estado de las interfaces del switch. La dirección IP para el switch se aplica a una interfaz VLAN. En este caso, la interfaz Vlan1 recibió la dirección IP 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 a ella 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.

También se puede probar la conectividad de capa 3 en el switch con los comandos **show ip interface brief** y **traceroute**. En este ejemplo, tanto el comando**ping**como el comando**trace**muestran una conectividad satisfactoria.

Es importante tener en cuenta que no se requiere ninguna dirección IP para que un switch cumpla su función de reenvío de tramas en la capa 2. Se necesita una dirección IP solo si se administra el switch a través de la red mediante Telnet o SSH. Si el administrador de red planea conectarse al switch de forma remota desde una ubicación fuera de la red LAN local, también se debe configurar un gateway predeterminado.

Además de implementar y proteger una red pequeña, el administrador de red también debe administrar los archivos de configuración. La administración de los archivos de configuración es importante para la realización de copias de seguridad y la recuperación en caso de falla del dispositivo.

El sistema de archivos de Cisco IOS (IFS) proporciona una única interfaz a todos los sistemas de archivos que utiliza un router, incluidos los siguientes:

* Sistemas de archivos de memoria flash
* Sistemas de archivos de red (TFTP y FTP)
* Cualquier otra terminal para leer o escribir datos, como la memoria NVRAM, la configuración en ejecución y la memoria ROM, entre otras

Con Cisco IFS, se pueden ver y clasificar todos los archivos (imagen, archivo de texto, etcétera), incluidos los archivos en servidores remotos. Por ejemplo, es posible ver un archivo de configuración en un servidor remoto para verificar que sea el archivo de configuración correcto antes de cargarlo en el router.

Cisco IFS permite que el administrador se desplace por distintos directorios, enumere los archivos en uno de ellos y cree subdirectorios en la memoria flash o en un disco. Los directorios disponibles dependen del dispositivo.

En la figura 1, se muestra el resultado del comando **show file systems**. En este ejemplo, enumera todos los sistemas de archivos disponibles en un router Cisco 1941. Este comando proporciona información útil, como la cantidad de memoria disponible y libre, el tipo de sistema de archivos y los permisos. Los permisos incluyen solo lectura (ro), solo escritura (wo) y lectura y escritura (rw), los cuales se muestran en la columna Flags (Indicadores) del resultado del comando.

Si bien se enumeran varios sistemas de archivos, nos enfocaremos en los sistemas de archivos TFTP, flash y NVRAM.

Observe que el sistema de archivos flash también tiene un asterisco que lo precede. Esto indica que el sistema de archivos predeterminado actual es flash. El IOS de arranque está ubicado en la memoria flash; por lo tanto, se agrega el símbolo de almohadilla (#) a la entrada de flash para indicar que es un disco de arranque.

**El sistema de archivos flash**

En la figura 2, se muestra el contenido del sistema de archivos predeterminado actual, que en este caso es flash, tal como indicaba el asterisco que precedía la entrada en la ilustración anterior. Hay varios archivos ubicados en la memoria flash, pero el de mayor interés específicamente es el último de la lista: se trata del nombre del archivo de imagen de Cisco IOS actual que se ejecuta en la memoria RAM.

**El sistema de archivos NVRAM**

Para ver el contenido de la memoria NVRAM, se debe cambiar el sistema de archivos predeterminado actual con el comando **cd** (cambiar directorio), como se muestra en la figura 3. El comando **pwd** (directorio de trabajo actual) verifica que estemos viendo el directorio NVRAM. Finalmente, el comando **dir** (directorio) enumera el contenido de la memoria NVRAM. Si bien se enumeran varios archivos de configuración, el de mayor interés específicamente es el archivo de configuración de inicio.

Con el sistema de archivos flash del switch Cisco 2960, se pueden copiar los archivos de configuración y archivar (subir y descargar) imágenes de software.

El comando para ver los sistemas de archivos en un switch Catalyst es el mismo que se utiliza en los routers Cisco: **show file systems**, como se muestra en la ilustración.

Los switches y routers Cisco admiten muchos comandos UNIX básicos: **cd** para cambiar a un sistema de archivos o un directorio, **dir** para mostrar los directorios en un sistema de archivos y **pwd** para mostrar el directorio de trabajo.

**Copia de seguridad de las configuraciones con captura de texto (Tera Term)**

Los archivos de configuración se pueden guardar o archivar en un archivo de texto mediante Tera Term.

Como se muestra en la figura, los pasos son:

**Paso 1.** En el menú File, haga clic en **Log**.

**Paso 2.** Elija la ubicación para guardar el archivo. Tera Term comenzará a capturar texto.

**Paso 3.** Una vez que comienza la captura, ejecute el comando **show running-config** o **show startup-config** en la petición de entrada de EXEC privilegiado. El texto que aparece en la ventana de la terminal se colocará en el archivo elegido.

**Paso 4.** Cuando la captura haya finalizado, seleccione **Close** (Cerrar) en la ventana Log (Registro) de TeraTerm.

**Paso 5.** Observe el archivo para verificar que no esté dañado.

**Restauración de las configuraciones de texto**

Una configuración se puede copiar de un archivo a un dispositivo. Cuando se copia desde un archivo de texto y se pega en la ventana de una terminal, el IOS ejecuta cada línea del texto de configuración como si fuera un comando. Esto significa que el archivo necesitará edición para asegurar que las contraseñas encriptadas estén en forma de texto y que se eliminen los mensajes de IOS y el texto de no comando, como "--More--". Este proceso se analiza en la práctica de laboratorio.

A su vez, en la CLI, el dispositivo debe establecerse en el modo de configuración global para recibir los comandos del archivo de texto que se pegan en la ventana de la terminal.

Cuando se usa Tera Term, los pasos son los siguientes:

**Paso 1.** En el menú File (Archivo), haga clic en **Send** (Enviar) para enviar el archivo.

**Paso 2.** Ubique el archivo que debe copiar en el dispositivo y haga clic en **Open**.

**Paso 3.** Tera Term pegará el archivo en el dispositivo.

El texto en el archivo estará aplicado como comandos en la CLI y pasará a ser la configuración en ejecución en el dispositivo. Éste es un método conveniente para configurar manualmente un router.

**Copia de seguridad de las configuraciones mediante TFTP**

Las copias de los archivos de configuración se deben almacenar como archivos de copia de seguridad en caso de que se produzca un problema. Los archivos de configuración se pueden almacenar en un servidor de protocolo trivial de transferencia de archivos (TFTP) o en una unidad USB. Un archivo de configuración también tendría que incluirse en la documentación de red.

Para guardar la configuración en ejecución o la configuración de inicio en un servidor TFTP, utilice el comando **copy running-config tftp** o **copy startup-config tftp**, como se muestra en la ilustración. Siga estos pasos para realizar una copia de seguridad de la configuración en ejecución en un servidor TFTP:

**Paso 1.** Introduzca el comando **copy running-config tftp**.

**Paso 2.** Ingrese la dirección IP del host en el cual se almacenará el archivo de configuración.

**Paso 3.** Ingrese el nombre que se asignará al archivo de configuración.

**Paso 4.** Presione Intro para confirmar cada elección.

**Restauración de las configuraciones mediante TFTP**

Para restaurar la configuración en ejecución o la configuración de inicio desde un servidor TFTP, utilice el comando **copy tftp running-config** o **copy tftp startup-config**. Siga estos pasos para restaurar la configuración en ejecución desde un servidor TFTP:

**Paso 1.** Introduzca el comando **copy tftp running-config**.

**Paso 2.** Introduzca la dirección IP del host en el que está almacenado el archivo de configuración.

**Paso 3.** Ingrese el nombre que se asignará al archivo de configuración.

**Paso 4.** Presione Intro para confirmar cada elección.

La característica de almacenamiento de bus serial universal (USB) habilita a determinados modelos de routers Cisco para que admitan unidades flash USB. La característica flash USB proporciona una capacidad de almacenamiento secundario optativa y un dispositivo de arranque adicional. Las imágenes, las configuraciones y demás archivos se pueden copiar en la memoria flash USB Cisco y desde esta con la misma confiabilidad con la que se almacenan y se recuperan archivos con una tarjeta Compact Flash. Además, los routers de servicios integrados modulares pueden arrancar con cualquier imagen del software Cisco IOS guardada en la memoria flash USB.

Los módulos de memoria flash USB Cisco están disponibles en versiones de 64 MB, 128 MB y 256 MB.

Para ser compatible con un router Cisco, una unidad flash USB debe tener formato FAT16. De lo contrario, el comando show file systems muestra un error que indica que el sistema de archivos es incompatible.

A continuación, se presenta un ejemplo del uso del comando dir en un sistema de archivos USB:

**Router# dir usbflash0:**

**Directory of usbflash0:/**

**1 -rw- 30125020 Dec 22 2032 05:31:32 +00:00 c3825-entservicesk9-mz.123-14.T**

**63158272 bytes total (33033216 bytes free)**

Lo ideal es que la memoria flash USB pueda contener varias copias de las configuraciones de Cisco IOS y varias configuraciones del router. La memoria flash USB permite que un administrador mueva y copie fácilmente esos archivos y configuraciones de IOS de un router a otro. En numerosas ocasiones, el proceso de copiado puede ser mucho más rápido que a través de una LAN o una WAN. Tenga en cuenta que es posible que el IOS no reconozca el tamaño correcto de la memoria flash USB, pero eso no significa necesariamente que la memoria flash no sea compatible. Además, los puertos USB de un router generalmente son USB 2.0, como los que se muestran en la ilustración.

**Copia de seguridad de las configuraciones mediante una unidad flash USB**

Al realizar copias de seguridad en un puerto USB, se recomienda emitir el comando **show file systems** para verificar que la unidad USB esté presente y confirmar el nombre, como se muestra en la figura 1.

A continuación, utilice el comando **copy run usbflash0:/** para copiar el archivo de configuración a la unidad flash USB. Asegúrese de utilizar el nombre de la unidad flash tal como se indica en el sistema de archivos. La barra es optativa, pero indica el directorio raíz de la unidad flash USB.

El IOS le solicitará el nombre de archivo. Si el archivo ya existe en la unidad flash USB, el router solicitará la confirmación de sobrescritura, como se ve en la figura 2.

Utilice el comando **dir** para ver el archivo en la unidad USB, y el comando **more** para ver el contenido, como se muestra en la figura 3.

**Restauración de las configuraciones mediante una unidad flash USB**

Para volver a copiar el archivo, se deberá editar el archivo USB R1-Config con un editor de texto para transformarlo en un archivo de configuración válido; de lo contrario, hay muchas entradas que son comandos no válidos y no aparecerá ninguna interfaz.

R1# **copy usbflash0:/R1-Config running-config**

Destination filename [running-config]?

El uso de redes no se limita a las pequeñas empresas y a las grandes organizaciones.

Otro entorno en el que cada vez se aprovecha más la tecnología de red es el hogar. Las redes domésticas se utilizan para proporcionar conectividad y uso compartido de Internet entre varios sistemas de computación personales y computadoras portátiles en el hogar. También permiten que las personas aprovechen diversos servicios, como el uso compartido de una impresora de red, el almacenamiento centralizado de fotos, música y películas en un dispositivo de almacenamiento conectado a la red (NAS) y el acceso de otros dispositivos para usuarios finales, como tablet PC, teléfonos celulares e incluso electrodomésticos, como un televisor, a servicios de Internet.

Una red doméstica es muy similar a la red de una pequeña empresa. Sin embargo, la mayoría de las redes domésticas y muchas redes de pequeñas empresas no requieren dispositivos de gran volumen, como routers y switches dedicados. Los dispositivos de menor escala son suficientes, siempre que proporcionen la misma funcionalidad de enrutamiento y conmutación. Por este motivo, muchas redes domésticas y de pequeñas empresas utilizan el servicio de un dispositivo multifunción.

A los fines de este curso, los dispositivos multifunción se denominarán routers integrados.

Un router integrado es como tener varios dispositivos diferentes conectados entre sí. Por ejemplo: la conexión entre el switch y el router sigue existiendo, pero se produce internamente. Cuando se reenvía un paquete desde un dispositivo hacia otro en la misma red local, el switch integrado reenvía automáticamente el paquete al dispositivo de destino. No obstante, si se reenvía un paquete a un dispositivo en una red remota, el switch integrado reenvía el paquete a la conexión del router interno. Luego, el router interno determina cuál es el mejor camino y reenvía el paquete en consecuencia.

La mayoría de los routers integrados ofrecen tanto capacidades de conmutación por cable como conectividad inalámbrica y sirven como punto de acceso (AP) en la red inalámbrica, como el que se muestra en la figura 1. La conectividad inalámbrica es una forma popular, flexible y rentable de que los hogares y las empresas proporcionen servicios de red a los dispositivos finales.

En las figuras 2 y 3, se enumeran algunas ventajas y consideraciones comunes respecto del uso de la tecnología inalámbrica.

Además de admitir el enrutamiento, la conmutación y la conectividad inalámbrica, un router integrado puede ofrecer muchas funciones adicionales, las cuales incluyen: servicio de DHCP, un firewall e, incluso, servicios de almacenamiento conectado a la red.

Los routers integrados pueden ser desde dispositivos pequeños, diseñados para aplicaciones de oficinas hogareñas y pequeñas empresas, hasta dispositivos más eficaces, que se pueden usar en sucursales de empresas.

Un ejemplo de este tipo de router integrado es un router inalámbrico Linksys, como el que se muestra en la ilustración. Este tipo de routers integrados tienen un diseño simple y, por lo general, no tiene componentes independientes, lo que reduce el costo del dispositivo. Sin embargo, si se produce una falla, no es posible reemplazar componentes individuales dañados. De este modo, crean un único punto de falla y no están optimizados para ninguna función en particular.

Otro ejemplo de router integrado es el router de servicio integrado (ISR) de Cisco. La familia de productos ISR de Cisco ofrece una amplia gama de productos, entre ellos los dispositivos diseñados para entornos de oficinas pequeñas y hogareñas o para redes más grandes. Muchos de los ISR ofrecen modularidad y tienen componentes individuales para cada función, por ejemplo un componente de switch y un componente de router. Esto permite agregar, reemplazar y actualizar componentes individuales según sea necesario.

Todos los routers integrados permiten opciones de configuración básicas como contraseñas y direcciones IP, y opciones de configuración de DHCP, que son las mismas independientemente de si el dispositivo se utiliza para conectar hosts por cable o inalámbricos. No obstante, si se utiliza la funcionalidad inalámbrica, se necesitan parámetros de configuración adicionales, como la configuración del modo inalámbrico, el SSID y el canal inalámbrico.

**Modo inalámbrico**

El modo inalámbrico se refiere a la configuración del estándar inalámbrico IEEE 802.11 que utilizará la red. Existen cuatro enmiendas al estándar IEEE 802.11, que describen distintas características para las comunicaciones inalámbricas; estas son 802.11a, 802.11b, 802.11g y 802.11n. En la figura 1, se muestra más información sobre cada estándar.

La mayoría de los routers inalámbricos integrados son compatibles con las versiones 802.11b, 802.11g y 802.11n. Las tres tecnologías son compatibles, pero todos los dispositivos en la red deben funcionar en el mismo estándar común a todos los dispositivos. Por ejemplo: si un router 802.11n está conectado a una computadora portátil con 802.11n, la red funciona en un estándar 802.11n. Sin embargo, si se agrega una impresora inalámbrica 802.11b a la red, el router y la computadora portátil revierten al estándar 802.11b, que es más lento, para todas las comunicaciones. Por lo tanto, mantener dispositivos inalámbricos más antiguos en la red provoca que toda la red funcione más despacio. Es importante tener esto en cuenta al decidir si se mantienen dispositivos inalámbricos más antiguos o no.

**Identificador de conjunto de servicios (SSID)**

Puede haber muchas otras redes inalámbricas en su zona. Es importante que los dispositivos inalámbricos se conecten a la red WLAN correcta. Esto se realiza mediante un identificador del servicio (SSID, Service Set Identifier).

El SSID es un nombre alfanumérico que distingue mayúsculas de minúsculas para su red inalámbrica doméstica. El nombre puede tener hasta 32 caracteres de longitud. El SSID se utiliza para comunicar a los dispositivos inalámbricos a qué WLAN pertenecen y con qué otros dispositivos pueden comunicarse. Independientemente del tipo de instalación WLAN, todos los dispositivos inalámbricos en una WLAN pueden configurarse con el mismo SSID a fin de poder realizar la comunicación.

**Canal inalámbrico**

Los canales se crean al dividir el espectro de RF disponible. Cada canal puede transportar una conversación diferente. Esto es similar a la manera en que los distintos canales de televisión se transmiten por un único medio. Varios AP pueden funcionar muy cerca unos de otros siempre que utilicen diferentes canales para la comunicación.

Antes de conectar el AP a la red o al ISP, se deben planificar y configurar las medidas de seguridad.

Como se muestra en la figura 1, algunas de las medidas de seguridad más básicas incluyen lo siguiente:

* Modificación de los valores predeterminados para el SSID, los nombres de usuario y las contraseñas
* Desactivación de la transmisión del SSID
* Configuración de la encriptación mediante WEP o WPA

La encriptación es el proceso de transformar datos de manera que, aunque sean interceptados, queden inutilizables.

**Protocolo de equivalencia por cable (WEP, Wired Equivalency Protocol)**

El protocolo WEP es una característica de seguridad avanzada que encripta el tráfico de la red a medida que este se desplaza por el aire. WEP utiliza claves preconfiguradas para encriptar y descifrar datos, como se muestra en la figura 2.

Una clave WEP se introduce como una cadena de números y letras, y generalmente consta de 64 ó 128 bits. En algunos casos, el WEP admite también claves de 256 bits. Para simplificar la creación y la introducción de estas claves, muchos dispositivos incluyen la opción por contraseña. La opción por contraseña es una manera fácil de recordar la palabra o frase usada para generar automáticamente una clave.

A fin de que el WEP funcione, el AP (y cualquier otro dispositivo inalámbrico que tenga habilitado el acceso a la red) deberá tener la misma clave WEP introducida. Sin esta clave, los dispositivos no podrán comprender las transmisiones inalámbricas.

WEP tiene puntos débiles, por ejemplo, el uso de una clave estática en todos los dispositivos con WEP habilitado. Existen aplicaciones disponibles que los atacantes pueden utilizar para descubrir la clave WEP. Estas aplicaciones se encuentran disponibles fácilmente en Internet. Una vez que el atacante ha extraído la clave, tiene acceso completo a toda la información transmitida.

Una manera de superar este punto débil es cambiar la clave frecuentemente. Otra manera es usar una forma de encriptación más avanzada y segura, conocida como acceso protegido Wi-Fi (WPA, Wi-Fi Protected Access).

**Acceso protegido Wi-Fi (WPA)**

El WPA también utiliza claves de encriptación de 64 a 256 bits. Sin embargo, el WPA, a diferencia del WEP, genera nuevas claves dinámicas cada vez que un cliente establece una conexión con el AP. Por esta razón el WPA se considera más seguro que el WEP, ya que es mucho más difícil de decodificar.

Existen varias implementaciones de seguridad más que se pueden configurar en un AP inalámbrico, incluidos el filtrado de direcciones MAC, la autenticación y el filtrado de tráfico. Sin embargo, estas implementaciones de seguridad exceden el ámbito de este curso.

Un router inalámbrico Linksys es un dispositivo común utilizado en redes domésticas y de pequeñas empresas. En este curso, se utilizará para demostrar las configuraciones básicas de un router integrado. Un dispositivo Linksys típico ofrece cuatro puertos Ethernet para conectividad por cable y, además, actúa como punto de acceso inalámbrico. El dispositivo Linksys también funciona como servidor de DHCP y miniservidor Web que admite una interfaz gráfica de usuario (GUI) basada en Web.

**Acceso a un router Linksys y configuración**

Para acceder inicialmente al router, conecte un cable de una PC a uno de los puertos Ethernet para LAN del router, como se muestra en la ilustración. Una vez establecida la conexión por cable, el dispositivo que se conecta obtendrá automáticamente la información de direccionamiento IP del router integrado, incluida una dirección de gateway predeterminado. La dirección de gateway predeterminado es la dirección IP del dispositivo Linksys. Revise la configuración de la red de computadoras con el comando**ipconfig /all** para obtener esta dirección. Ahora puede escribir esa dirección IP en un explorador Web de la PC para acceder a la GUI de configuración basada en Web.

El dispositivo Linksys tiene una configuración predeterminada que habilita servicios de conmutación y de enrutamiento básico. También está configurado de manera predeterminada como servidor de DHCP. Las tareas de configuración básica, como el cambio del nombre de usuario y contraseña predeterminados, de la dirección IP predeterminada de Linksys e, incluso, de los rangos predeterminados de direcciones IP de DHCP, se deben realizar antes de que se conecte el AP a una red activa.

Para habilitar la conectividad inalámbrica, se debe configurar el modo inalámbrico, el SSID, el canal de RF y cualquier mecanismo de encriptación de seguridad deseado.

Primero, seleccione el modo inalámbrico correcto, como se muestra en la ilustración. Al seleccionar el modo, o el estándar inalámbrico, cada modo incluye una sobrecarga determinada. Si todos los dispositivos en la red utilizan el mismo estándar, seleccionar el modo asociado a ese estándar limita la cantidad de sobrecarga que se genera. También aumenta la seguridad, dado que no permite que se conecten dispositivos con estándares diferentes. No obstante, si necesitan acceder a la red dispositivos que utilizan estándares diferentes, se debe seleccionar el modo mixto. El rendimiento de la red disminuirá debido a la sobrecarga adicional ocasionada por admitir todos los modos.

A continuación, establezca el SSID. Todos los dispositivos que deseen participar en la WLAN deben tener el mismo SSID. Por cuestiones de seguridad, se debe modificar el SSID predeterminado. Para permitir que los clientes detecten la WLAN fácilmente, se transmite el SSID de manera predeterminada. Se puede deshabilitar la característica de transmisión del SSID. Si no se transmite el SSID, los clientes inalámbricos necesitarán configurar este valor manualmente.

El canal de RF utilizado para el router integrado se debe elegir teniendo en cuenta las demás redes inalámbricas que se encuentren alrededor.

Las redes inalámbricas adyacentes deben utilizar canales que no se superpongan, a fin de optimizar el rendimiento. La mayoría de los puntos de acceso ahora ofrecen una opción para permitir que el router localice automáticamente el canal menos congestionado.

Por último, seleccione el mecanismo de encriptación que prefiera e introduzca una clave o una frase de contraseña.

**Configuración de un cliente inalámbrico**

Un host inalámbrico, o cliente, se define como cualquier dispositivo que contenga un software de cliente inalámbrico y una NIC inalámbrica. Este software cliente le permite al hardware participar en la WLAN. Los dispositivos incluyen algunos smartphones, computadoras portátiles y de escritorio, impresoras, televisores, sistemas de juego y tablet PC.

Para que un cliente inalámbrico se conecte a la WLAN, las opciones de configuración del cliente deben coincidir con las del router inalámbrico. Esto incluye el SSID, la configuración de seguridad y la información del canal (si este se configuró manualmente). Esta configuración se especifica en el software de cliente.

El software cliente inalámbrico utilizado puede estar integrado por software al sistema operativo del dispositivo o puede ser un software de utilidad inalámbrica, independiente y que se puede descargar, diseñado específicamente para interactuar con la NIC inalámbrica.

Una vez que se configure el software cliente, verifique el enlace entre el cliente y el AP.

Abra la pantalla de información del enlace inalámbrico para ver datos como la velocidad de datos de la conexión, el estado de la conexión y el canal inalámbrico utilizado, como se muestra en la ilustración. Si está disponible, la característica Información de enlace muestra la potencia de señal y la calidad de la señal inalámbrica actuales.

Además de verificar el estado de la conexión inalámbrica, verifique que los datos realmente puedan transmitirse. Una de las pruebas más comunes para verificar si la transmisión de datos se realiza correctamente es la prueba de ping. Si el ping se realiza correctamente se puede realizar la transmisión de datos.

Para cumplir con los requisitos de los usuarios, incluso las redes pequeñas requieren planificación y diseño, como se muestra en la ilustración. La planificación asegura que se consideren debidamente todos los requisitos, factores de costo y opciones de implementación. La confiabilidad, la escalabilidad y la disponibilidad son partes importantes del diseño de una red.

Para admitir y ampliar una red pequeña, se necesita estar familiarizado con los protocolos y las aplicaciones de red que se ejecutan en ella. Los analizadores de protocolos permiten que los profesionales de red recopilen información estadística sobre los flujos de tráfico en una red rápidamente. La información recopilada por el analizador de protocolos se analiza de acuerdo con el origen y el destino del tráfico, y con el tipo de tráfico que se envía. Los técnicos de red pueden utilizar este análisis para tomar decisiones acerca de cómo administrar el tráfico de manera más eficiente. Los protocolos de red comunes incluyen DNS, Telnet, SMTP, POP, DHCP, HTTP y FTP.

Es necesario tener en cuenta las amenazas y vulnerabilidades de seguridad al planificar la implementación de una red. Se deben proteger todos los dispositivos de red. Esto incluye routers, switches, dispositivos para usuarios finales e, incluso, dispositivos de seguridad. Se deben proteger las redes contra softwares malintencionados, como virus, caballos de Troya y gusanos. Los softwares antivirus pueden detectar la mayoría de los virus y muchas aplicaciones de caballo de Troya, y evitar que se propaguen en la red. 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.

También se deben proteger las redes contra los ataques de red. Los ataques de red se pueden clasificar en tres categorías principales: de reconocimiento, de acceso y por denegación de servicio. Existen varias maneras de proteger la red contra los ataques de red.

* 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 observar las acciones que realizan mientras acceden a la red (contabilizar).
* El firewall es una de las herramientas de seguridad más eficaces disponibles para la protección de los usuarios internos de la red contra amenazas externas. El firewall reside entre dos o más redes y controla el tráfico entre ellas, además de evitar el acceso no autorizado.
* Para proteger los dispositivos de red, es importante utilizar contraseñas seguras. Además, al acceder a los dispositivos de red de forma remota, se recomienda habilitar SSH en vez del protocolo Telnet, que no es seguro.

Una vez que se implementó la red, el administrador debe poder supervisar y mantener la conectividad de red. Existen varios comandos para este fin. Para probar la conectividad de red a destinos locales y remotos, se suelen utilizar comandos como **ping, telnet** y **traceroute**.

En los dispositivos Cisco IOS, se puede utilizar el comando **show version** para verificar y resolver problemas de algunos de los componentes básicos de hardware y software que se utilizan durante el proceso de arranque. Para ver información de todas las interfaces de red en un router, se utiliza el comando **show ip interface**. También se puede utilizar el comando **show ip interface brief** para ver un resultado más abreviado que el del comando **show ip interface**. 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.

Los archivos de configuración de Cisco IOS como startup-config o running-config se deben archivar. Estos archivos pueden guardarse en un archivo de texto o almacenarse en un servidor TFTP. Algunos modelos de routers también tienen un puerto USB, y se puede crear la copia de seguridad de un archivo en una unidad USB. Si es necesario, esos archivos se pueden copiar en el router o switch desde el servidor TFTP o la unidad USB.

El uso de redes no se limita a las pequeñas empresas y a las grandes organizaciones. Otro entorno en el que cada vez se aprovecha más la tecnología de red es el hogar. Una red doméstica es muy similar a la red de una pequeña empresa. Sin embargo, la mayoría de las redes domésticas (y muchas redes de pequeñas empresas) no requieren dispositivos de gran volumen, como routers y switches dedicados. En lugar de esto, la mayoría de las redes domésticas utilizan un único dispositivo multifunción. A los fines de este curso, los dispositivos multifunción se denominarán routers integrados. La mayoría de los routers integrados ofrecen tanto capacidades de conmutación por cable como conectividad inalámbrica y sirven como punto de acceso (AP) en la red inalámbrica. Para habilitar la conectividad inalámbrica, se debe configurar el modo inalámbrico, el SSID, el canal de RF y cualquier mecanismo de encriptación de seguridad deseado.