

Modulo 1

1.0.1 ¿Por qué debería tomar este módulo?

¡Bienvenido a Redes en la actualidad!

¡Felicitaciones! Este módulo lo inicia en su camino hacia una carrera exitosa en Tecnología de la Información al brindarle una comprensión fundamental de la creación, operación y mantenimiento de redes. Como ventaja, puede sumergirse en simulaciones de red usando Packet Tracer. ¡Le prometemos que realmente lo disfrutará!

1.0.2 ¿Qué aprenderé en este módulo?

Título del módulo: Las redes en la actualidad

Objetivos del módulo: Explique los avances en las tecnologías de red modernas.

1.0.4 Vídeo - Introducción a Cisco Packet Tracer

Packet Tracer es una herramienta que permite simular redes reales. Proporciona tres menús principales:

- Puede agregar dispositivos y conectarlos a través de cables o inalámbricos.
- Puede seleccionar, eliminar, inspeccionar, etiquetar y agrupar componentes dentro de la red.
- Puede administrar su red abriendo una red existente o de muestra, guardando la red actual y modificando su perfil de usuario o preferencias.

Si ha utilizado algún programa, como un procesador de textos o una hoja de cálculo, ya está familiarizado con los comandos del menú Archivo ubicados en la barra de menús superior. Los comandos Abrir, Guardar, Guardar como y Salir funcionan como lo harían con cualquier programa, pero hay dos comandos especiales para Packet Tracer.

El comando Open Samples mostrará un directorio de ejemplos preconstruidos de características y configuraciones de varios dispositivos de red e Internet de las cosas incluidos en Packet Tracer.

El comando Salir y cerrar sesión eliminará la información de registro de esta copia de Packet Tracer y requerirá que el siguiente usuario de esta copia de Packet Tracer realice el procedimiento de inicio de sesión de nuevo.

Haga clic en Reproducir en el vídeo para aprender a utilizar los menús y a crear su primera red Packet Tracer

1.0.5 Packet Tracer - Exploración de Modo Lógico y Físico

El modelo de red de esta actividad Packet Tracer Physical Mode (PTPM) incorpora muchas de las tecnologías que puede dominar en los cursos de Cisco Networking Academy. y representa

una versión simplificada de la forma en que podría verse una red de pequeña o mediana empresa.

La mayoría de los dispositivos de la sucursal de Seward y del Centro de Datos de Warrenton ya están implementados y configurados. Usted acaba de ser contratado para revisar los dispositivos y redes implementados. No es importante que comprenda todo lo que vea y haga en esta actividad. Siéntase libre de explorar la red por usted mismo. Si desea hacerlo de manera más sistemática, siga estos pasos. Responda las preguntas lo mejor que pueda.

1.1.1 Las redes nos conectan

Entre todos los elementos esenciales para la existencia humana, la necesidad de interactuar está justo después de la necesidad de sustentar la vida. La comunicación es casi tan importante para nosotros como el aire, el agua, los alimentos y un lugar para vivir.

En el mundo actual, estamos conectados como nunca antes gracias al uso de redes. Las personas que tienen alguna idea pueden comunicarse de manera instantánea con otras personas para hacer esas ideas realidad. Las noticias y los descubrimientos se conocen en todo el mundo en cuestión de segundos. Incluso, las personas pueden conectarse y jugar con amigos que estén del otro lado del océano y en otros continentes.

1.1.2 Video - La experiencia de aprendizaje en Cisco Networking Academy

Los cambiadores del mundo no nacen. Se hacen. Desde 1997, Cisco Networking Academy ha estado trabajando hacia un único objetivo: la educación y el desarrollo de habilidades de la próxima generación de talentos necesarios para la economía digital.

Haga clic en Jugar para ver cómo Cisco Networking Academy para aprender cómo usamos la tecnología para hacer del mundo un lugar mejor.

1.1.3 No hay límites

Los avances en tecnologías de red son, quizá, los agentes de cambio más significativos en el mundo actual. Gracias a estos avances, podemos crear un mundo en el que las fronteras nacionales, las distancias geográficas y las limitaciones físicas se vuelven menos importantes y se convierten en obstáculos cada vez más fáciles de sortear.

Internet cambió la manera en la que se producen las interacciones sociales, comerciales, políticas y personales. La naturaleza inmediata de las comunicaciones en Internet alienta la formación de comunidades mundiales. Estas comunidades permiten una interacción social que no depende de la ubicación ni de la zona horaria.

La creación de comunidades en línea para el intercambio de ideas e información tiene el potencial de aumentar las oportunidades de productividad en todo el planeta.

La creación de la nube nos permite almacenar documentos e imágenes y acceder a ellos en cualquier lugar y en cualquier momento. Así que ya sea que estemos en un tren, en un parque o en la cima de una montaña, podemos acceder sin problemas a nuestros datos y aplicaciones desde cualquier dispositivo.

1.2.1 Roles de host

Si desea formar parte de una comunidad en línea global, su computadora, tableta o teléfono inteligente primero deben estar conectados a una red. Esa red debe estar conectada a Internet. En este tema se describen las partes de una red. ¡Vea si reconoce estos componentes en su propia red de hogar o escuela!

Todas las computadoras que están conectadas a una red y participan directamente en la comunicación de la red se clasifican como hosts. Los hosts se pueden llamar dispositivos finales. Algunos hosts también se llaman clientes. Sin embargo, el término hosts se refiere específicamente a los dispositivos de la red a los que se asigna un número para fines de comunicación. Este número identifica el host dentro de una red determinada. Este número se denomina dirección de protocolo de Internet (IP). Una dirección IP identifica el host y la red a la que está conectado el host.

Los servidores son computadoras con software que les permite proporcionar información, como correo electrónico o páginas web, a otros dispositivos finales de la red. Cada servicio requiere un software de servidor independiente. Por ejemplo, para proporcionar servicios web a la red, un servidor requiere un software de servidor web. Una computadora con software de servidor puede proporcionar servicios simultáneamente a muchos clientes diferentes.

Como se mencionó anteriormente, los clientes son un tipo de host. Los clientes disponen de software para solicitar y mostrar la información obtenida del servidor, como se muestra en la figura.

Un navegador web, como Chrome o Firefox, es un ejemplo de software de cliente. Una única PC también puede ejecutar varios tipos de software de cliente. Por ejemplo, un usuario puede consultar el correo electrónico y ver una página web mientras envía mensajes instantáneos y escucha una transmisión de audio. La tabla enumera tres tipos comunes de software de servidor.

Tipo	Descripción
Correo electrónico	El servidor de correo electrónico ejecuta el software del servidor de correo electrónico. Los clientes usan cliente de correo software, como Microsoft Outlook, para acceder al correo electrónico en el servidor.
Web	El servidor web ejecuta software de servidor web. Los clientes utilizan software de navegador, como Windows Internet Explorer, para acceder a páginas web en el servidor.
Archivo	El servidor de archivos almacena archivos de usuario y empresariales en una ubicación central. Los dispositivos cliente acceden a estos archivos con software cliente como Explorador de archivos de Windows

1.2.2 Entre pares

El software de cliente y servidor generalmente se ejecuta en computadoras separadas, pero también es posible usar una computadora para ambos roles al mismo tiempo. En pequeñas empresas y hogares, muchas PC funcionan como servidores y clientes en la red. Este tipo de red se denomina red entre pares.

Las ventajas de las redes entre pares:

- *Fácil de configurar*
- *Menos complejo*
- *Menor costo porque es posible que no se necesiten dispositivos de red ni servidores dedicados.*
- *Se pueden utilizar para tareas sencillas como transferir archivos y compartir impresoras*

Las desventajas de las redes entre pares:

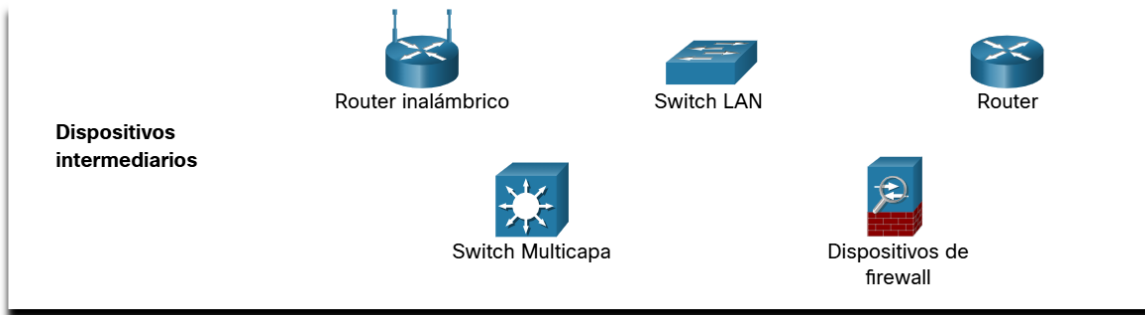
- *La administración no está centralizada*
- *No son tan seguras*
- *No son escalables*
- *Todos los dispositivos pueden funcionar como clientes y como servidores, lo que puede lentificar el rendimiento*

. 1.2.3 Dispositivos finales

- Los dispositivos de red con los que las personas están más familiarizadas se denominan dispositivos finales. Para distinguir un dispositivo final de otro, cada dispositivo final de una red tiene una dirección. Cuando un dispositivo final inicia la comunicación, utiliza la dirección del dispositivo final de destino para especificar dónde entregar el mensaje.
- Un terminal es el origen o el destino de un mensaje transmitido a través de la red.
- Haga clic en el botón Reproducir de la figura para ver una animación del flujo de datos por una red.

. 1.2.4 Dispositivos intermediarios

- Los dispositivos intermedios conectan los dispositivos finales individuales a la red. Pueden conectar múltiples redes individuales para formar una red interna. Los dispositivos intermedios proporcionan conectividad y garantizan el flujo de datos en toda la red.
- Los dispositivos intermedios usan la dirección del dispositivo final de destino, junto con información sobre las interconexiones de la red, para determinar la ruta que los mensajes deben tomar a través de la red. En la figura, se muestran algunos ejemplos de los dispositivos intermediarios más comunes y una lista de funciones.



Un dispositivo de red intermediario puede admitir algunas de estas funciones o todas ellas:

- *Regenerar y retransmitir señales de comunicación*
- *Conservar información acerca de las rutas que existen a través de la red y de internetwork*
- *Notificar a otros dispositivos los errores y las fallas de comunicación*
- *Dirigir los datos a lo largo de rutas alternativas cuando hay una falla en el enlace*
- *Clasificar y dirigir mensajes de acuerdo a las prioridades*
- *Permitir o denegar el flujo de datos de acuerdo a los parámetros de seguridad*

Nota: No se muestra un concentrador Ethernet. Un hub de Ethernet también se conoce como repetidor multipuerto. Los repetidores regeneran y retransmiten las señales de comunicación. Observe que todos los dispositivos intermedios realizan la función de repetidor .

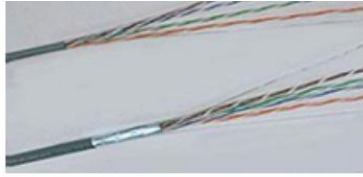
1.2.5 Medios de red

La comunicación se transmite a través de una red en los medios. El medio proporciona el canal por el cual viaja el mensaje desde el origen hasta el destino.

Las redes modernas utilizan principalmente tres tipos de medios para interconectar dispositivos, como se muestra en la figura:

- **Hilos metálicos dentro de cables** - Los datos se codifican en impulsos eléctricos.
- **Fibras de vidrio o plástico (cable de fibra óptica)** - Los datos se codifican como pulsos de luz.
- **Transmisión inalámbrica** - Los datos se codifican a través de la modulación de frecuencias específicas de ondas electromagnéticas.

Cobre



Fibra óptica



Tecnología inalámbrica



1.3.1 Representaciones de red

Los arquitectos y administradores de redes deben poder mostrar el aspecto que tendrán sus redes. Necesitan poder ver fácilmente qué componentes se conectan a otros componentes, dónde se ubicarán y cómo se conectarán. Los diagramas de redes a menudo usan símbolos, como los que se muestran en la figura, para representar los diferentes dispositivos y conexiones que forman una red.

Un diagrama proporciona una manera fácil de comprender cómo se conectan los dispositivos en una red grande. Este tipo de representación de una red se denomina diagrama de topología. La capacidad de reconocer las representaciones lógicas de los componentes físicos de red es fundamental para poder visualizar la organización y el funcionamiento de una red.

Además de estas representaciones, se utiliza una terminología especializada para describir cómo cada uno de estos dispositivos y medios se conectan entre sí:

- **Tarjeta de interfaz de red (Network Interface Card) (NIC)** - Una NIC conecta físicamente el dispositivo final a la red.
- **Puerto físico** - Un conector o conexión en un dispositivo de red donde se conectan los medios a un terminal u otro dispositivo de red.
- **Interfaz** - Puertos especializados en un dispositivo de red que se conecta a redes individuales. Debido a que los routers conectan redes, los puertos en un router se denominan interfaces de red.

Nota: Los términos puerto e interfaz con frecuencia se utilizan en forma indistinta.

1.3.2 Diagramas de topología

Los diagramas de topología son documentación obligatoria para cualquier persona que trabaje con una red. Estos diagramas proporcionan un mapa visual que muestra cómo está conectada la red. Hay dos tipos de diagramas de topología, físicos y lógicos.

Diagramas de topologías físicas

Los diagramas de topología física ilustran la ubicación física de los dispositivos intermedios y la instalación del cable, como se muestra en la figura. Puede ver que las habitaciones en las que se encuentran estos dispositivos están etiquetadas en esta topología física.

Diagramas de topologías lógicas

Los diagramas de topología lógica ilustran los dispositivos, los puertos y el esquema de direccionamiento de la red, como se muestra en la figura. Puede ver qué dispositivos finales están conectados a qué dispositivos intermediarios y qué medios se están utilizando.

Las topologías que se muestran en los diagramas físicos y lógicos son adecuadas para su nivel de comprensión en este punto del curso. Utilice Internet para buscar “diagramas de topología de red” y ver algunos ejemplos más complejos. Si agrega la palabra “Cisco” a su frase de búsqueda, encontrará muchas topologías que usan íconos similares a los que ha visto en estas figuras.

1.4.1 Redes de muchos tamaños

Ahora que está familiarizado con los componentes que componen las redes y sus representaciones en topologías físicas y lógicas, está listo para aprender acerca de los diferentes tipos de redes.

Hay redes de todo tamaño. Pueden ir desde redes simples, compuestas por dos PC, hasta redes que conectan millones de dispositivos.

Las redes domésticas sencillas le permiten compartir recursos, como impresoras, documentos, imágenes y música, entre unos pocos dispositivos finales locales.

Las redes de oficinas pequeñas y oficinas domésticas (SOHO) permiten a las personas trabajar desde casa o desde una oficina remota. Muchos trabajadores independientes utilizan este tipo de redes para anunciar y vender productos, pedir suministros y comunicarse con los clientes.

Las empresas y las grandes organizaciones usan redes para proporcionar consolidación, almacenamiento y acceso a la información en los servidores de red. Las redes proporcionan correo electrónico, mensajería instantánea y colaboración entre empleados. Muchas organizaciones usan la conexión de su red a Internet para proporcionar productos y servicios a los clientes.

Internet es la red más extensa que existe. De hecho, el término Internet significa “red de redes”. Es una colección de redes privadas y públicas interconectadas.

En pequeñas empresas y hogares, muchas PC funcionan como servidores y clientes en la red. Este tipo de red se denomina red entre pares.

Redes domésticas pequeñas

Las redes domésticas pequeñas conectan algunas computadoras entre sí y a Internet.

Redes domésticas/de oficinas pequeñas

La red SOHO permite que las computadoras en una oficina hogareña o remota se conecten a una red corporativa o accedan a recursos compartidos centralizados.

Redes medianas a grandes

Las redes medianas a grandes, como las que se utilizan en corporaciones y escuelas, pueden tener muchas ubicaciones con cientos o miles de hosts interconectados.

Redes mundiales

Internet es una red de redes que conecta cientos de millones de computadoras en todo el mundo.

1.4.2 LAN y WAN

Las infraestructuras de red pueden variar en gran medida en términos de:

- El tamaño del área que abarcan.
- La cantidad de usuarios conectados.
- La cantidad y los tipos de servicios disponibles.
- El área de responsabilidad

Los dos tipos más comunes de infraestructuras de red son las redes de área local (LAN) y las redes de área amplia (WAN). Una LAN es una infraestructura de red que proporciona acceso a usuarios y dispositivos finales en un área geográfica

pequeña. Normalmente, una LAN se utiliza en un departamento dentro de una empresa, un hogar o una red de pequeñas empresas. Una WAN es una infraestructura de red que proporciona acceso a otras redes en un área geográfica amplia, que generalmente es propiedad y está administrada por una corporación más grande o un proveedor de servicios de telecomunicaciones. La figura muestra las LAN conectadas a una WAN.

LAN

Una LAN es una infraestructura de la red que abarca un área geográfica pequeña. Las LANs tienen características específicas:

- Las LANs interconectan terminales en un área limitada, como una casa, un lugar de estudios, un edificio de oficinas o un campus.
- Por lo general, la administración de las LAN está a cargo de una única organización o persona. El control administrativo se aplica a nivel de red y rige las políticas de seguridad y control de acceso.
- Las LANs proporcionan ancho de banda de alta velocidad a dispositivos finales internos y dispositivos intermedios, como se muestra en la figura.

Una red que sirve a una casa, un edificio pequeño o un campus pequeño se considera una LAN.

Redes WAN

La figura muestra una WAN que interconecta dos LAN. Una WAN es una infraestructura de la red que abarca un área geográfica extensa. Las WAN generalmente son administradas por proveedores de servicios (SP) o proveedores de servicios de Internet (ISP).

Las WANs tienen características específicas:

- Las WAN interconectan LAN a través de áreas geográficas extensas, por ejemplo, entre ciudades, estados, provincias, países o continentes.
- Por lo general, la administración de las WAN está a cargo de varios proveedores de servicios.
- Normalmente, las WAN proporcionan enlaces de velocidad más lenta entre redes LAN.
-

1.4.3 El Internet

- Internet es una colección global de redes interconectadas (internetworks o internet para abreviar). En la figura se muestra una forma de ver a la Internet como una colección de LAN y WAN interconectadas.

- Algunos de los ejemplos de LAN están conectados entre sí a través de una conexión WAN. Las WAN están conectadas entre sí. WANs can connect through copper wires, fiber-optic cables, and wireless transmissions (not shown).
- Internet no pertenece a una persona o un grupo. Garantizar una comunicación efectiva en esta infraestructura heterogénea requiere la aplicación de estándares y tecnologías uniformes, y comúnmente reconocidas, así como también la cooperación de muchas agencias de administración de redes. Hay organizaciones que se desarrollaron para ayudar a mantener la estructura y la estandarización de los protocolos y procesos de Internet. Entre estas organizaciones, se encuentran el Grupo de trabajo de ingeniería de Internet (IETF), la Corporación de Internet para la Asignación de Nombres y Números (ICANN) y el Consejo de Arquitectura de Internet (IAB), entre muchas otras.

1.4.4 Intranets y Extranets

Hay otros dos términos que son similares al término internet: intranet y extranet.

El término intranet se utiliza para referirse a la conexión privada de LAN y WAN que pertenecen a una organización. Una intranet está diseñada para que solo puedan acceder a ella los miembros y empleados de la organización, u otras personas autorizadas.

Es posible que una organización utilice una extranet para proporcionar acceso seguro a las personas que trabajan para otra organización, pero requieren datos de la empresa. Aquí hay algunos ejemplos de extranets:

- Una empresa que proporciona acceso a proveedores y contratistas externos.
- Un hospital que proporciona un sistema de reservas a los médicos para que puedan hacer citas para sus pacientes.
- Una secretaría de educación local que proporciona información sobre presupuesto y personal a las escuelas del distrito.

La figura ilustra los niveles de acceso que los diferentes grupos tienen a una intranet de la empresa, a una extranet de la empresa y a Internet.

1.5.1 Tecnologías de acceso a Internet

Por lo tanto, ahora tiene una comprensión básica de lo que forma una red y los diferentes tipos de redes. Pero, ¿cómo se conecta realmente a los usuarios y

organizaciones a Internet? Como habrás adivinado, hay muchas maneras diferentes de hacer esto.

Los usuarios domésticos, los trabajadores remotos y las oficinas pequeñas generalmente requieren una conexión a un ISP para acceder a Internet. Las opciones de conexión varían mucho entre los ISP y las ubicaciones geográficas. Sin embargo, las opciones más utilizadas incluyen banda ancha por cable, banda ancha por línea de suscriptor digital (DSL), redes WAN inalámbricas y servicios móviles.

Las organizaciones generalmente necesitan acceso a otros sitios corporativos, así como a Internet. Para admitir servicios empresariales, como telefonía IP, videoconferencias y el almacenamiento en centros de datos, se requieren conexiones rápidas. Los SPs ofrecen interconexiones de clase empresarial. Los servicios de nivel empresarial más comunes son DSL empresarial, líneas arrendadas y red Metro Ethernet.

1.5.2 Conexiones a Internet domésticas y de oficinas pequeñas

En la figura, se muestran opciones de conexión comunes para los usuarios de oficinas pequeñas y oficinas en el hogar, que incluyen las siguientes:

- **Cable** - Típicamente ofrecido por los proveedores de servicios de televisión por cable, la señal de datos de Internet se transmite en el mismo cable que ofrece la televisión por cable. Proporciona un gran ancho de banda, alta disponibilidad y una conexión a Internet siempre activa.
- **DSL** - Las líneas de suscriptor digital también proporcionan un gran ancho de banda, alta disponibilidad y una conexión permanente a Internet. DSL se transporta por la línea de teléfono. En general los usuarios de oficinas en el hogar o pequeñas se conectan mediante una línea de suscriptor digital asimétrica (ADSL), esto implica que la velocidad de descarga es mayor que la velocidad de carga.
- **Celular** - El acceso a internet celular utiliza una red de telefonía celular para conectarse. En cualquier lugar donde tenga cobertura de telefonía móvil, puede tener acceso a Internet. El rendimiento está limitado por las capacidades del teléfono y la torre celular a la que está conectado.
- **Satelital** - La disponibilidad de acceso a internet satelital es un beneficio en aquellas áreas que de otra manera no tendrían conectividad a internet. Las antenas parabólicas requieren una línea de vista despejada al satélite.
- **Telefonía por Dial-up** - Es una opción de bajo costo que funciona con cualquier línea telefónica y un módem. El ancho de banda que proporciona una conexión por módem, conexión por dial-up es bajo y, por lo general, no es suficiente para transferencias de datos masivas, si bien es útil para acceso móvil durante viajes.

La oferta de opciones de conexión varía según la ubicación geográfica y la disponibilidad de proveedores de servicios.

1.5.3 Conexiones a Internet empresariales

Las opciones de conexión corporativas difieren de las opciones que tienen los usuarios domésticos. Es posible que las empresas requieran un ancho de banda mayor y dedicado, además de servicios administrados. Las opciones de conexión disponibles varían según el tipo de proveedores de servicios que haya en las cercanías.

La figura ilustra las opciones de conexión comunes para las empresas.

- **Líneas arrendadas dedicadas** - Las líneas arrendadas son circuitos reservados dentro de la red del proveedor de servicios que conectan oficinas separadas geográficamente para redes privadas de voz y / o datos. Los circuitos se alquilan a una tasa mensual o anual.
- **Metro Ethernet** - Esto a veces se conoce como Ethernet WAN. En este módulo, nos referiremos a él como Metro Ethernet. Metro ethernet extienden la tecnología de acceso LAN a la WAN. Ethernet es una tecnología LAN que analizaremos en un capítulo más adelante.
- **DSL empresarial** - El servicio de DSL empresarial está disponible en diversos formatos. Una opción muy utilizada es la línea de suscriptor digital simétrica (SDSL), que es similar a la versión de DSL para el consumidor, pero proporciona las mismas velocidades de subida y descarga.
- **Satelital** - El servicio satelital puede proporcionar una conexión cuando una solución por cable no está disponible.

Las opciones de conexión varían según la ubicación geográfica y la disponibilidad del proveedor de servicios.

1.5.4 La red convergente

Redes separadas tradicionales

Piense en una escuela construida hace cuarenta años. En ese entonces, las aulas contaban con conexiones por cable para la red de datos, la red telefónica y la red de vídeo para los televisores. Estas redes separadas no pueden comunicarse entre sí. Cada red utilizaba tecnologías diferentes para transportar la señal de comunicación. Cada red tenía su propio conjunto de reglas y estándares para asegurar una comunicación satisfactoria. Múltiples servicios se ejecutaron en múltiples redes.

Redes convergentes

Hoy, las redes separadas de datos, telefonía y vídeo están convergiendo. A diferencia de las redes dedicadas, las redes convergentes pueden transmitir datos, voz y vídeo entre muchos tipos diferentes de dispositivos en la misma infraestructura de red. Esta infraestructura de red

utiliza el mismo conjunto de reglas, acuerdos y estándares de implementación. Las redes de datos convergentes transportan servicios múltiples en una red.

1.6.1 Arquitectura de red

¿Alguna vez ha estado ocupado trabajando en línea, sólo para tener «Internet se cae»? Como ya sabes, Internet no se cayó, acabas de perder tu conexión con él. Es muy frustrante. Con tantas personas en el mundo que dependen del acceso a la red para trabajar y aprender, es imperativo que las redes sean confiables. En este contexto, la fiabilidad significa más que su conexión a Internet. Este tema se centra en los cuatro aspectos de la fiabilidad de la red.

La función de la red cambió de una red únicamente de datos a un sistema que permite conectar personas, dispositivos e información en un entorno de red convergente y con gran variedad de medios. Para que las redes funcionen eficazmente y crezcan en este tipo de entorno, se deben crear sobre la base de una arquitectura de red estándar.

Las redes también admiten una amplia gama de aplicaciones y servicios. Deben operar sobre muchos tipos diferentes de cables y dispositivos, que conforman la infraestructura física. En este contexto, el término arquitectura de red, se refiere a las tecnologías que dan soporte a la infraestructura y a los servicios y las reglas, o protocolos, programados que trasladan los datos a través de la red.

A medida que las redes evolucionan, hemos aprendido que hay cuatro características básicas que los arquitectos de redes deben abordar para cumplir con las expectativas del usuario:

- Tolerancia a fallas
- Escalabilidad
- Calidad de servicio (QoS)
- Seguridad

• 1.6.2 Tolerancia a fallas

- Una red tolerante a fallas es aquella que limita la cantidad de dispositivos afectados durante una falla. Está construido para permitir una recuperación rápida cuando se produce una falla de este tipo. Estas redes dependen de varias rutas entre el origen y el destino del mensaje. Si falla una ruta, los mensajes se pueden enviar inmediatamente por otro enlace. El hecho de que haya varias rutas que conducen a un destino se denomina redundancia.
- La implementación de una red de packet-switched es una forma en que las redes confiables proporcionan redundancia. La conmutación de paquetes

divide el tráfico en paquetes que se enrutan a través de una red compartida. Un solo mensaje, como un correo electrónico o una transmisión de vídeo, se divide en múltiples bloques de mensajes, llamados paquetes. Cada paquete tiene la información de dirección necesaria del origen y el destino del mensaje. Los routers dentro de la red cambian los paquetes según la condición de la red en ese momento. Esto significa que todos los paquetes en un mismo mensaje pueden tomar distintas rutas para llegar a destino. En la figura, el usuario no se da cuenta y no se ve afectado por el cambio dinámico de rutas que hace el router cuando falla un enlace.

-

• 1.6.3 Escalabilidad

- Una red escalable se expande rápidamente para admitir nuevos usuarios y aplicaciones. Lo hace sin degradar el rendimiento de los servicios a los que están accediendo los usuarios existentes. En la figura, se muestra cómo puede agregarse una red nueva a una red existente con facilidad. Además, las redes son escalables porque los diseñadores siguen los estándares y protocolos aceptados. Esto permite a los proveedores de software y hardware centrarse en mejorar los productos y servicios sin tener que diseñar un nuevo conjunto de reglas para operar dentro de la red.

• 1.6.4 Calidad de servicio

- La calidad de servicio (QoS) es un requisito cada vez más importante para las redes hoy en día. Las nuevas aplicaciones disponibles para los usuarios en internetworks, como las transmisiones de voz y de vídeo en vivo generan expectativas más altas sobre la calidad de los servicios que se proporcionan. ¿Alguna vez intentó mirar un vídeo con interrupciones y pausas constantes? A medida que el contenido de datos, voz y vídeo sigue convergiendo en la misma red, QoS se convierte en un mecanismo principal para administrar la congestión y garantizar el envío confiable de contenido a todos los usuarios.
- La congestión se produce cuando la demanda de ancho de banda excede la cantidad disponible. El ancho de banda de la red es la medida de la cantidad de bits que se pueden transmitir en un segundo, es decir, bits por segundo (bps). Cuando se producen intentos de comunicaciones simultáneas a través de la red, la demanda de ancho de banda puede exceder su disponibilidad, lo que provoca congestión en la red.
- Cuando el volumen de tráfico es mayor de lo que se puede transportar en la red, los dispositivos colocan los paquetes en cola en la memoria hasta que haya recursos disponibles para transmitirlos. En la figura, un usuario solicita una página web y otro está realizando una llamada telefónica. Con una política de QoS, el router puede administrar el flujo de datos y el tráfico de voz, dando prioridad a las comunicaciones de voz si la red se congestiona.

1.6.5 Seguridad de la red

La infraestructura de red, los servicios y los datos contenidos en los dispositivos conectados a la red son activos comerciales y personales muy importantes. Los administradores de red deben abordar dos tipos de problemas de seguridad de red: seguridad de la infraestructura de red y seguridad de la información.

Asegurar la infraestructura de red incluye asegurar físicamente los dispositivos que proporcionan conectividad de red y evitar el acceso no autorizado al software de administración que reside en ellos, como se muestra en la figura.

Los administradores de red también deben proteger la información contenida en los paquetes que se transmiten a través de la red y la información almacenada en los dispositivos conectados a la red. Para alcanzar los objetivos de seguridad de la red, hay tres requisitos principales

- **Confidencialidad** - La confidencialidad de los datos se refiere a que solamente los destinatarios deseados y autorizados pueden acceder a los datos y leerlos.
- **Integridad** - Integridad de datos significa tener la seguridad de que la información no se va a alterar en la transmisión, del origen al destino.
- **Disponibilidad** - Significa tener la seguridad de acceder en forma confiable y oportuna a los servicios de datos para usuarios autorizados.

1.7.1 Tendencias recientes

Ahora sabe mucho sobre las redes, de qué están hechas, cómo nos conectan y qué se necesita para mantenerlas confiables. Pero las redes, como todo lo demás, continúan cambiando. Hay algunas tendencias en la creación de redes que usted, como estudiante de NetaCAD, debería conocer.

A medida que se lanzan al mercado nuevas tecnologías y dispositivos para usuarios finales, las empresas y los consumidores deben continuar adaptándose a este entorno en constante evolución. Existen varias tendencias de redes que afectan a organizaciones y consumidores:

- Traiga su propio dispositivo (BYOD)
- Colaboración en línea
- Comunicaciones de video
- Computación en la nube
-

• **1.7.2 Traiga su propio dispositivo (BYOD)**

- El concepto de cualquier dispositivo, para cualquier contenido, de cualquier manera, es una tendencia global importante que requiere cambios significativos en la forma en que usamos los dispositivos y los conectamos de manera segura a las redes. Esto se llama Traiga su propio dispositivo (BYOD).
- BYOD permite a los usuarios finales la libertad de usar herramientas personales para acceder a la información y comunicarse a través de una red de negocios o campus. Con el crecimiento de los dispositivos de consumo y la caída relacionada en el costo, los empleados y estudiantes pueden tener dispositivos avanzados de computación y redes para uso personal. Estos incluyen computadoras portátiles, tabletas, teléfonos inteligentes y lectores electrónicos. Estos pueden ser comprados por la compañía o la escuela, comprados por el individuo, o ambos.
- BYOD significa que se puede usar cualquier dispositivo, de cualquier persona, en cualquier lugar.

• **1.7.3 Colaboración en línea**

- Las personas quieren conectarse a la red no solo para acceder a aplicaciones de datos, sino también para colaborar entre sí. La colaboración se define como “el acto de trabajar con otras personas en un proyecto conjunto”. Las herramientas de colaboración, como Cisco Webex que se muestra en la figura, brindan a los empleados, estudiantes, profesores, clientes y asociados una forma de conectarse, interactuar y lograr sus objetivos de forma inmediata.

- La Colaboración es una prioridad crítica y estratégica que las organizaciones están utilizando para seguir siendo competitivas. La colaboración también es una prioridad en la educación. Los estudiantes necesitan colaborar para ayudarse mutuamente con el aprendizaje, para desarrollar las habilidades de trabajo en equipo que se utilizan en la fuerza laboral y para trabajar juntos en proyectos en equipo.
- Cisco Webex Teams es una herramienta de colaboración multifuncional que le permite enviar mensajes instantáneos a una o más personas, publicar imágenes y publicar videos y enlaces. Cada equipo 'espacio' mantiene un historial de todo lo que se publica allí.
-

• **1.7.4 Comunicaciones de video**

- Otra faceta de las redes que es crítica para el esfuerzo de comunicación y colaboración es el video. El video se usa para comunicaciones,

colaboración y entretenimiento. Las videollamadas se realizan desde y hacia cualquier persona con conexión a Internet, independientemente de dónde se encuentren.

- La videoconferencia es una herramienta poderosa para comunicarse con otros, tanto local como globalmente. A medida que las organizaciones se extienden más allá de los límites geográficos y culturales, el vídeo se convierte en un requisito crítico para una colaboración eficaz.

• 1.7.5 Vídeo - Cisco Webex para Huddles

- Haga clic en Reproducir en la figura para ver cómo se incorpora Cisco Webex en la vida cotidiana y los negocios.

1.7.6 Computación en la nube

La informática en la nube es una de las formas en que accedemos y almacenamos datos. La computación en la nube nos permite almacenar archivos personales, incluso hacer copias de seguridad de una unidad completa en servidores a través de Internet. Se puede acceder a aplicaciones como procesamiento de texto y edición de fotos usando la nube.

Para las empresas, la computación en la nube amplía las capacidades de TI sin requerir inversión en nueva infraestructura, capacitación de personal nuevo o licencias de software nuevo. Estos servicios están disponibles a petición y se proporcionan de forma económica a cualquier dispositivo en cualquier lugar del mundo, sin comprometer la seguridad ni el funcionamiento.

La computación en la nube es posible gracias a los centros de datos. Los centros de datos son instalaciones utilizadas para alojar sistemas informáticos y componentes asociados. Un centro de datos puede ocupar una habitación de un edificio, uno o más pisos o un edificio completo del tamaño de un almacén. Por lo general, la creación y el mantenimiento de centros de datos son muy costosos. Por esta razón, solo las grandes organizaciones utilizan centros de datos privados creados para alojar sus datos y proporcionar servicios a los usuarios. Las organizaciones más pequeñas que no pueden mantener su propio centro de datos privado pueden reducir el costo total de propiedad mediante el arrendamiento de servicios de servidor y almacenamiento a una organización de centro de datos más grande en la nube.

Por motivos de seguridad, fiabilidad y tolerancia a fallos, los proveedores de nube suelen almacenar datos en centros de datos distribuidos. En lugar de almacenar todos los datos de una persona u organización en un centro de datos, se almacenan en varios centros de datos en diferentes ubicaciones.

Existen cuatro tipos principales de nubes: nubes públicas, nubes privadas, nubes híbridas y nubes comunitarias, como se muestra en la tabla.

Cloud Types

Tipo de nube	Descripción
Nubes públicas	Se realizan aplicaciones y servicios basados en la nube ofrecidos en una nube pública disponible para la población en general. Los servicios pueden ser gratuitos o se ofrecen en un modelo de pago por uso, como pagar por el almacenamiento en línea. El público la nube utiliza Internet para proporcionar servicios.
Nubes privadas	Las aplicaciones y servicios basados en la nube que se ofrecen en una nube privada son diseñada para una organización o una entidad específica, como el gobierno. A la nube privada se puede configurar utilizando el red, aunque esto puede ser costoso de construir y mantener. Una privada nube también puede ser administrada por una organización externa con acceso estricto seguridad.
Nubes híbridas	Una nube híbrida se compone de dos o más nubes (por ejemplo: parte privada, parte pública), donde cada parte sigue siendo un objeto distinto, pero ambos son conectados usando una única arquitectura. Individuos en una nube híbrida sería capaz de tener grados de acceso a diversos servicios basados en derechos de acceso
Nubes comunitarias	Una nube comunitaria se crea para la utilización exclusiva de entidades u organizaciones. Las diferencias entre nubes públicas y las comunitarias son las necesidades funcionales que han sido personalizadas para la comunidad. Por ejemplo, las organizaciones de servicios de salud deben cumplir las políticas y leyes (por ejemplo, la HIPAA) que requieren una autenticación y una confidencialidad especiales. Las nubes comunitarias son utilizadas por múltiples organizaciones que tienen necesidades e inquietudes similares. Las nubes comunitarias son similares a un entorno de nube pública, pero con el establecimiento de niveles de seguridad, la privacidad e incluso el cumplimiento reglamentario de una nube privada.

1.7.7 Tendencias tecnológicas en el hogar

Las tendencias de las redes no solo afectan la forma en que nos comunicamos en el trabajo y en la escuela, sino que también cambian muchos aspectos del hogar. Las nuevas tendencias del hogar incluyen la “tecnología del hogar inteligente”.

La tecnología inteligente para el hogar se integra en los electrodomésticos de todos los días, que luego pueden conectarse con otros dispositivos para hacer que los electrodomésticos sean más "inteligentes" o automatizados. Por ejemplo, puede preparar la comida y colocarla en el horno para cocinar antes de salir de la casa por el día. Usted programa su horno inteligente para la comida que desea que cocine. También estaría conectado a su "calendario de eventos" para poder determinar a qué hora debería estar disponible para comer y ajustar las horas de inicio y la duración de la cocción en consecuencia. Incluso podría ajustar el tiempo y la temperatura de cocción sobre la base de los cambios en su agenda. Además, una conexión de teléfono inteligente o tableta le permite conectarse directamente al horno para realizar los ajustes que desee. Cuando la comida está lista, el horno

envía un mensaje de alerta a usted (o a alguien que especifique) de que la comida está terminada y se calienta.

La tecnología de hogar inteligente se está desarrollando actualmente para todas las habitaciones dentro de una casa. La tecnología inteligente para el hogar se volverá más común a medida que se expandan las redes domésticas y la tecnología de Internet de alta velocidad.

1.7.8 Redes powerline

Las redes Powerline para redes domésticas utilizan el cableado eléctrico existente para conectar dispositivos, como se muestra en la figura.

Mediante un adaptador estándar de línea eléctrica, los dispositivos pueden conectarse a la LAN donde haya un tomacorriente. No es necesario instalar cables de datos, y se utiliza poca o ninguna electricidad adicional. Mediante el uso de los mismos cables que transmiten electricidad, la red de línea de alimentación envía información mediante el envío de datos en ciertas frecuencias.

La red Powerline es especialmente útil cuando los puntos de acceso inalámbrico no pueden llegar a todos los dispositivos en el hogar. La red Powerline no es un sustituto del cableado dedicado en redes de datos. Sin embargo, es una alternativa cuando los cables de red de datos o las comunicaciones inalámbricas no son posibles o efectivas.

1.7.9 Banda ancha inalámbrica

En muchas áreas donde el cable y el DSL no están disponibles, es posible que la conexión inalámbrica se utilice para conectarse a Internet.

Proveedor de servicios de Internet inalámbrico

El proveedor de servicios de Internet inalámbrico (WISP) es un ISP que conecta a los suscriptores a un punto de acceso designado o una zona activa mediante tecnologías inalámbricas similares a las que se encuentran en las redes de área local inalámbrica (WLAN). Los WISP se encuentran con mayor frecuencia en entornos rurales donde los servicios de cable o DSL no están disponibles.

Aunque se puede instalar una torre de transmisión separada para la antena, típicamente la antena está unida a una estructura elevada existente, como una torre de agua o una torre de radio. Se instala una pequeña antena en el techo del suscriptor, al alcance del transmisor del WISP. La unidad de acceso del suscriptor se conecta a la red conectada por cable dentro del hogar. Desde la perspectiva del usuario doméstico, la configuración no es muy diferente de la de DSL o el servicio

de cable. La diferencia principal es que la conexión del hogar al ISP es inalámbrica, en lugar de establecerse mediante un cable físico.

Servicio de banda ancha inalámbrica

Otra solución inalámbrica para los hogares y las pequeñas empresas es la banda ancha inalámbrica, como se muestra en la figura.

Esta solución utiliza la misma tecnología celular que un teléfono inteligente. Se instala una antena fuera del hogar, que proporciona conectividad inalámbrica o por cable a los dispositivos en el hogar. En muchas zonas, la banda ancha inalámbrica doméstica compite directamente con los servicios de DSL y cable.

1.8.1 Amenazas de seguridad

Sin duda, ha escuchado o leído noticias sobre la violación de la red de una empresa, lo que brinda a los atacantes acceso a la información personal de miles de clientes. Por esta razón, la seguridad de la red siempre va a ser una prioridad de los administradores.

La seguridad de la red es una parte integral de la red informática, independientemente de si la red está en un hogar con una sola conexión a Internet o es una corporación con miles de usuarios. La seguridad de la red debe tener en cuenta el entorno, así como las herramientas y requisitos de la red. Debe ser capaz de proteger los datos al tiempo que permite la calidad de servicio que los usuarios esperan de la red.

Asegurar una red implica protocolos, tecnologías, dispositivos, herramientas y técnicas para proteger los datos y mitigar las amenazas. Los vectores de amenazas pueden ser externos o internos. Muchas amenazas de seguridad de redes externas se originan hoy en Internet.

Existen varias amenazas externas comunes a las redes:

- **Virus, gusanos y caballos de Troya** - Estos contienen software malicioso o código que se ejecuta en un dispositivo de usuario.
- **Spyware y adware** - Estos son tipos de software que se instalan en el dispositivo de un usuario. El software recopila en secreto información sobre el usuario.
- **Ataques de día cero** - También llamados ataques de hora cero, se producen el primer día que se conoce una vulnerabilidad
- **Amenazas de Atacantes** - una persona malintencionada ataca dispositivos de usuario o recursos de red.

- **Ataques por denegación de servicio** - Estos ataques ralentizan o bloquean las aplicaciones y procesos en un dispositivo de red.
- **Intercepción y robo de datos** - Este ataque captura información privada de la red de una organización.
- **Robo de identidad** - Este ataque roba las credenciales de inicio de sesión de un usuario para acceder a datos privados.

También es importante tener en cuenta las amenazas internas. Se llevaron a cabo numerosos estudios que muestran que las violaciones de datos más comunes suceden a causa de los usuarios internos de la red. Esto se puede atribuir a dispositivos perdidos o robados o al mal uso accidental por parte de los empleados, y dentro del entorno comercial, incluso a empleados maliciosos. Con las estrategias de BYOD en desarrollo, los datos corporativos son mucho más vulnerables. Por lo tanto, al desarrollar una política de seguridad, es importante abordar las amenazas de seguridad internas y externas, como se muestra en la figura.

1.8.2 Soluciones de seguridad

No hay una solución única que pueda proteger una red contra la variedad de amenazas que existen. Por este motivo, la seguridad debe implementarse en varias capas, y debe utilizarse más de una solución de seguridad. Si un componente de seguridad no puede identificar y proteger la red, otros pueden tener éxito.

En general, la implementación de seguridad de las redes domésticas es muy básica. Por lo general, lo implementa en los dispositivos finales, así como en el punto de conexión a Internet, e incluso puede confiar en los servicios contratados por el ISP.

Estos son los componentes básicos de seguridad para una red doméstica o de oficina pequeña:

- **Antivirus y antispyware** - Estas aplicaciones ayudan a proteger los dispositivos finales para que no se infecten con software malicioso.
- **Filtrado de Firewall** - El filtrado de firewall bloquea el acceso no autorizado dentro y fuera de la red. Esto puede incluir un sistema de firewall ejecutado en un host que se implemente para impedir el acceso no autorizado al terminal o un servicio de filtrado básico en el router doméstico para impedir el acceso no autorizado del mundo exterior a la red.

Por otra parte, la implementación de seguridad de la red en redes de las empresas normalmente consiste en la integración de numerosos componentes a la red para controlar y filtrar el tráfico. Lo ideal es que todos los componentes funcionen

juntos, lo que minimiza la necesidad de mantenimiento y aumenta la seguridad. Las redes más grandes y las redes corporativas utilizan filtros antivirus, antispyware y firewall, pero también tienen otros requisitos de seguridad:

- **Sistemas de firewall dedicados** - Estos proporcionan capacidades de firewall más avanzadas que pueden filtrar grandes cantidades de tráfico con más granularidad.
- **Listas de control de acceso (ACL)** - Estos filtran aún más el acceso y el reenvío de tráfico en función de las direcciones IP y las aplicaciones.
- **Sistemas de prevención de intrusiones (IPS)** - Estos identifican amenazas de rápida propagación, como ataques de día cero o de hora cero.
- **Redes Privadas Virtuales (VPN)** - Estos proporcionan acceso seguro a una organización para trabajadores remotos.

Los requisitos de seguridad de la red deben tener en cuenta el entorno, así como las diversas aplicaciones y los requisitos informáticos. Tanto el entorno doméstico como el empresarial deben poder proteger sus datos y, al mismo tiempo, permitir la calidad de servicio que los usuarios esperan de cada tecnología. Además, la solución de seguridad implementada debe poder adaptarse a las crecientes tendencias de red, en constante cambio.

El estudio de las amenazas de seguridad de red y de las técnicas de mitigación comienza con una comprensión clara de la infraestructura de switching y routing subyacente utilizada para organizar los servicios de red.

1.9.1 CCNA

Como estudiante de NetaCAD, es posible que ya tenga una carrera en TI o que siga preparándose para prepararse para su carrera profesional. En cualquier caso, es bueno conocer las habilidades necesarias para adaptarse a los tipos de trabajos que están disponibles en TI.

La función y las competencias necesarias de los ingenieros de redes están en desarrollo y son más necesarias que nunca. La certificación Cisco Certified Network Associate (CCNA) demuestra que usted tiene conocimiento de las tecnologías fundamentales y asegura que se mantenga relevante con los conjuntos de habilidades necesarios para la adopción de tecnologías de próxima generación.

Un CCNA consolidado y actualizado para ingenieros de redes consta de tres cursos y un examen que cubre los temas fundamentales para todas las tecnologías de red. El nuevo CCNA se enfoca en temas de seguridad y

fundamentos de IP junto con programación inalámbrica, virtualización, automatización y red.

Existen nuevas certificaciones DevNet a nivel asociado, especializado y profesional, para validar sus habilidades de desarrollo de software.

Existen opciones de certificación especializadas para validar sus habilidades de acuerdo con su rol e intereses laborales. Esto incluye la certificación Cisco Enterprise Advanced Infrastructure Specialist.

Puede empezar donde quiera. No hay requisitos previos para comenzar a obtener su certificación de nivel asociado, especialista, profesional o experto. Los créditos de educación continua para la recertificación y el desarrollo continuo ya están disponibles para el CCNA.

1.9.2 Empleos de redes

Su certificación CCNA lo preparará para una variedad de puestos de trabajo en el mercado actual. En www.netacad.com puede hacer clic en el menú Carreras y, a continuación, seleccionar Oportunidades de empleo. Puede encontrar oportunidades de empleo donde vive utilizando el nuevo programa, el Talent Bridge Matching Engine. Busque trabajos con Cisco y con asociados y distribuidores de Cisco que necesiten estudiantes y graduados de Cisco Networking Academy.

También puede buscar empleos de TI usando motores de búsqueda online como Indeed, Glassdoor y Monster. Utilice términos de búsqueda como TI, administrador de red, arquitectos de red y administrador de sistemas informáticos. También puede buscar utilizando el término Cisco CCNA.

1.9.3 Laboratorio - Investigue las oportunidades de trabajo en redes y TI

En esta práctica de laboratorio se cumplirán los siguientes objetivos:

- Parte 1: Buscar oportunidades laborales
- Parte 2: Reflexionar sobre la investigación

Lab - Investigue las oportunidades de trabajo en TI y redes. Objetivos • Buscar oportunidades laborales Información básica/situación Los empleos en el área de tecnología de la información (TI) y redes de computación continúan creciendo. La mayoría de los empleadores requieren cierta forma de certificación estándar del sector, título u otras calificaciones de sus posibles empleados, en particular de aquellos que cuentan con

limitada experiencia. La certificación Cisco CCNA es una certificación de nivel inicial conocida y establecida sobre redes, respetada en el sector. Existen más niveles y tipos de certificaciones de Cisco que se pueden obtener, y cada una de ellas puede mejorar las oportunidades laborales, así como la escala salarial. En esta práctica de laboratorio, realizará cierta búsqueda laboral orientada en la web, para descubrir qué tipos de empleos relacionados con TI y redes de computación se encuentran disponibles, qué tipo de aptitudes y certificaciones necesitará y las escalas salariales asociadas con los diversos puestos.

Recursos necesarios • Dispositivo con acceso a Internet Instrucciones Utilizará un navegador web para visitar los sitios web populares de listados de trabajos, como monster.com y salary.com. Paso 1: Abra un navegador web y acceda a un sitio web de bolsa de trabajo. En la barra de direcciones URL, escriba <http://monster.com> y presione Intro. Nota: Para listados de trabajo fuera de los EE. UU., Use el siguiente enlace para buscar su país:

<http://www.monster.com/geo/siteselection/> Paso 2: Busque trabajos relacionados con redes.

a. Escriba la palabra Network Administrator en el cuadro Keyword or Title. Haga clic en Find Jobs para continuar. b. Observe los resultados de la búsqueda. Ahora, enfoque la búsqueda agregando términos a la búsqueda de administrador de redes. Pruebe con términos como Cisco CCNA, CCNP, CCNA Security, CCNA Voice, etc. c. Ahora intente refinar la búsqueda agregando ubicaciones geográficas diferentes. ¿Encontró empleos en las ubicaciones que introdujo? Escriba sus respuestas aquí. d. Intente buscar en un sitio web diferente. Vaya a <http://www.salary.com> y haga clic en el botón de la barra de menú de Búsqueda de empleo.

Nota: Para listados de salarios fuera de los EE. UU., use el siguiente enlace para buscar su país: <http://www.payscale.com/rccountries.aspx> © 2013 - 2020 Cisco y/o sus filiales. Todos los derechos reservados. Información pública de Cisco www.netacad.com Página 1 de 2 Lab

- Investigue las oportunidades de trabajo en TI y redes e. Agregue un término de búsqueda, como Information Technology al título del trabajo o a la palabra clave y haga clic en Get my salary estimate. f. Tenga en cuenta la gran cantidad de resultados de búsqueda coincidentes. Seleccione un puesto que le interese. Haga clic en SHOW MY SALARY ESTIMATE RESULTS. g. Dedique cierto tiempo a buscar empleos y observar los resultados de las búsquedas. Tome nota de las aptitudes requeridas para los distintos puestos y de la escala salarial inicial.

Preguntas de reflexión Responda las siguientes preguntas según los resultados de su investigación. 1. ¿Qué puestos buscó? Escriba sus respuestas aquí. 2. ¿Qué aptitudes o certificaciones se requerían? Escriba sus respuestas aquí. 3. ¿Encontró empleos que anteriormente no sabía que existían? Si la respuesta es afirmativa, ¿cuáles fueron? Escriba sus respuestas aquí. 4. ¿Encontró empleos que le interesan? Si la respuesta es afirmativa, ¿cuáles son y qué aptitudes o certificaciones requieren? Escriba sus respuestas aquí.

1.10.1 ¿Qué aprendí en este módulo?

Las redes afectan nuestras vidas

En el mundo actual, estamos conectados como nunca antes gracias al uso de redes. Las personas que tienen alguna idea pueden comunicarse de manera instantánea con otras personas para hacer esas ideas realidad. La creación de comunidades en línea para el intercambio de ideas e información tiene el potencial de aumentar las oportunidades de productividad en todo el planeta. La creación de la nube nos permite almacenar documentos e imágenes y acceder a ellos en cualquier lugar y en cualquier momento.

Componentes de red

Todas las computadoras que están conectadas a una red y participan directamente en la comunicación de la red se clasifican como hosts. Los hosts se pueden llamar dispositivos finales. Algunos hosts también se llaman clientes. Muchas computadoras funcionan como servidores y clientes en la red. Este tipo de red se denomina red entre pares. Un terminal es el origen o el destino de un mensaje transmitido a través de la red. Estos dispositivos conectan los terminales individuales a la red y pueden conectar varias redes individuales para formar una internetwork. Los dispositivos intermedios usan la dirección del dispositivo final de destino, junto con información sobre las interconexiones de la red, para determinar la ruta que los mensajes deben tomar a través de la red. El medio proporciona el canal por el cual viaja el mensaje desde el origen hasta el destino.

Representaciones y topología de red

Los diagramas de redes a menudo usan símbolos para representar los diferentes dispositivos y conexiones que forman una red. Un diagrama proporciona una manera fácil de comprender cómo se conectan los dispositivos en una red grande. Este tipo de representación de una red se denomina diagrama de topología. Los diagramas de topología física ilustran la ubicación física de los dispositivos intermedios y la instalación de cables. Los diagramas de topología lógica ilustran dispositivos, puertos y el esquema de direccionamiento de la red.

Tipos comunes de redes

Las redes domésticas pequeñas conectan algunas computadoras entre sí y a Internet. La red de oficina pequeña / oficina doméstica (SOHO) permite que las computadoras de una oficina doméstica o remota se conecten a una red corporativa o accedan a recursos centralizados y compartidos. Las redes medianas a grandes, como las que se utilizan en corporaciones y escuelas, pueden tener muchas ubicaciones con cientos o miles de hosts interconectados. Internet es una red de redes que conecta cientos de millones de computadoras en todo el mundo. Los dos tipos más comunes de infraestructuras de red son las redes de área local (LAN) y las redes de área amplia (WAN). Una LAN es una infraestructura de la red que abarca un área geográfica pequeña. Una WAN es una infraestructura de la red que abarca un área geográfica extensa. Intranet se refiere a una conexión privada de LAN y WAN que pertenece a una organización. Es posible que una organización utilice una extranet para proporcionar acceso

seguro a las personas que trabajan para otra organización, pero requieren datos de la empresa.

Conexiones a Internet

Las conexiones a Internet de SOHO incluyen cable, DSL, celular, satélite y telefonía por Dial-up. Las conexiones a Internet de negocios incluyen Línea dedicada arrendada, Metro Ethernet, Business DSL y Satélite. Las opciones de conexión varían según la ubicación geográfica y la disponibilidad del proveedor de servicios. Las utilizan diferentes tecnologías, reglas y estándares. Las redes convergentes entregan datos, voz y video entre muchos tipos diferentes de dispositivos a través de la misma infraestructura de red. Esta infraestructura de red utiliza el mismo conjunto de reglas, acuerdos y estándares de implementación. Packet Tracer es un programa de software flexible que le permite utilizar representaciones de red y teorías para construir modelos de red y explorar LAN y WAN relativamente complejas.

Redes confiables

En este contexto, el término arquitectura de red, se refiere a las tecnologías que dan soporte a la infraestructura y a los servicios y las reglas, o protocolos, programados que trasladan los datos a través de la red. A medida que evolucionan las redes, hemos aprendido que hay cuatro características básicas que los arquitectos de redes deben abordar para satisfacer las expectativas de los usuarios: tolerancia a fallos, escalabilidad, calidad de servicio (QoS) y seguridad. Una red tolerante a fallas es aquella que limita la cantidad de dispositivos afectados durante una falla. El hecho de que haya varias rutas que conducen a un destino se denomina redundancia. Una red escalable se expande rápidamente para admitir nuevos usuarios y aplicaciones. Las redes son escalables porque los diseñadores siguen los estándares y protocolos aceptados. QoS es un mecanismo principal para gestionar la congestión y garantizar la entrega confiable de contenido a todos los usuarios. Los administradores de red deben abordar dos tipos de problemas de seguridad de red: seguridad de la infraestructura de red y seguridad de la información. Para alcanzar los objetivos de seguridad de red, existen tres requisitos principales: Confidencialidad, Integridad y Disponibilidad.

Tendencias de red

Existen varias tendencias de redes recientes que afectan a las organizaciones y a los consumidores: Traiga su propio dispositivo (BYOD), colaboración en línea, comunicaciones de video y computación en la nube. BYOD significa que se puede usar cualquier dispositivo, de cualquier persona, en cualquier lugar. Las herramientas de colaboración, como Cisco WebEx, brindan a los empleados, estudiantes, maestros, clientes y socios una forma de conectarse, interactuar y alcanzar sus objetivos al instante. El video se usa para comunicaciones, colaboración y entretenimiento. Las videollamadas se realizan desde y hacia cualquier persona con conexión a Internet, independientemente de dónde se

encuentren. La computación en la nube nos permite almacenar archivos personales, incluso hacer copias de seguridad de una unidad completa en servidores a través de Internet. Se puede acceder a aplicaciones como procesamiento de texto y edición de fotos usando la nube. Existen cuatro tipos principales de nubes: nubes públicas, nubes privadas, nubes híbridas y nubes personalizadas. La tecnología de hogar inteligente se está desarrollando actualmente para todas las habitaciones dentro de una casa. La tecnología inteligente para el hogar se volverá más común a medida que se expandan las redes domésticas y la tecnología de Internet de alta velocidad. Mediante el uso de los mismos cables que transmiten electricidad, la red de línea de alimentación envía información mediante el envío de datos en ciertas frecuencias. El proveedor de servicios de Internet inalámbrico (WISP) es un ISP que conecta a los suscriptores a un punto de acceso designado o una zona activa mediante tecnologías inalámbricas similares a las que se encuentran en las redes de área local inalámbrica (WLAN).

Network Security

Existen varias amenazas externas comunes a las redes:

- Virus, gusanos y caballos de Troya
- Spyware y adware
- Ataques de día cero
- Amenazas de Atacantes
- Ataques por denegación de servicio
- Intercepción y robo de datos
- Robo de identidad

Estos son los componentes básicos de seguridad para una red doméstica o de oficina pequeña:

- Antivirus y antispymware
- Filtrado de firewall

Las redes más grandes y las redes corporativas utilizan filtros antivirus, antispymware y firewall, pero también tienen otros requisitos de seguridad:

- Sistemas de firewall exclusivos
- Listas de control de acceso (ACL)
- Sistemas de prevención de intrusiones (IPS)
- Redes privadas virtuales (VPN)

El profesional de TI

La certificación Cisco Certified Network Associate (CCNA) demuestra que usted tiene conocimiento de las tecnologías fundamentales y asegura que se mantenga

relevante con los conjuntos de habilidades necesarios para la adopción de tecnologías de próxima generación. Su certificación CCNA lo preparará para una variedad de puestos de trabajo en el mercado actual. En www.netacad.com puede hacer clic en el menú Carreras y, a continuación, seleccionar Oportunidades de empleo. Puede encontrar oportunidades de empleo donde vive utilizando el nuevo programa, el Talent Bridge Matching Engine. Busque trabajos con Cisco y con asociados y distribuidores de Cisco que necesiten estudiantes y graduados de Cisco Networking Academy.