REPORTE DE LECTURA

NOBRE DEL LIBRO:
ICND1-OFFICIAL-CERT-GUIDE-THIRD-EDITION

NOMBRE DEL PROFESOR:
ISMAEL JIMÉNEZ SÁNCHEZ

*

NOMBRE DEL ALUMNO:
BRAYAN ALEXIS MAAS CANCHE

Capítulo 7 Conmutación de LAN Ethernet

Conceptos de conmutación LAN

La conmutación LAN es un tipo de conmutación en la que los paquetes de datos se transfieren de un ordenador a otro a través de la red LAN. La tecnología de conmutación LAN es vital para el diseño de la red, ya que permite que el tráfico sólo se envíe a los lugares que se necesitan. La primera parte de esta sección analiza brevemente por qué se crearon los conmutadores. A continuación, esta sección explica las tres funciones principales de un interruptor, además de algunos otros detalles.

La gente desarrolló aplicaciones para aprovechar el ancho de banda de la LAN. Se agregaron más dispositivos a cada Ethernet. Eventualmente, toda una red se congestionó. Los dispositivos en la misma Ethernet no podían enviar (colectivamente) más de 10 Mbps de tráfico porque todos compartían los 10 Mbps de ancho de banda. Además, el aumento en los volúmenes de tráfico aumentó el número de colisiones. Mucho antes de que la utilización general de Ethernet se acercara a los 10 Mbps, Ethernet comenzó a sufrir debido a las crecientes colisiones.

La parte superior de la figura muestra una red 10BASE-T antes de agregar un puente y la parte inferior muestra la red después de haber la segmentario utilizando un puente. El puente crea dos separados dominios de colisión. Los marcos de Fred pueden colisionar con los de Barney, pero no pueden colisionar con los de Wilma o Betty.

Si un segmento LAN está ocupado y el puente necesita reenviar una trama al segmento ocupado, el puente simplemente almacena la trama (mantiene la trama en la memoria) hasta que el segmento ya no está ocupado. Reducir las colisiones, y suponiendo que no haya cambios significativos en la cantidad de dispositivos o la carga en la red, mejora en gran medida el rendimiento de la red.

En pocas palabras este tipo de conceptos muestra como esta conectado a un conmutador todas las interfaces que están ejecutando a 100 Mbps y con 4 dominios de colisión.

Lógica de conmutación

En última instancia, la función de un conmutador de LAN es reenviar tramas de Ethernet. Para lograr ese objetivo, los conmutadores usan lógica: lógica basada en la dirección MAC de origen y destino en el encabezado Ethernet de cada trama. Para ayudarlo a apreciar cómo funcionan los conmutadores, primero se requiere una revisión de las direcciones Ethernet.

El IEEE define tres categorías generales de direcciones MAC de Ethernet:

- Direcciones de unidifusión: Direcciones MAC que identifican una sola tarjeta de interfaz LAN.

- Direcciones de difusión: Una trama enviada con una dirección de destino de la dirección de transmisión (FFFF.FFFF.FFFF) implica que todos los dispositivos de la LAN deben recibir y procesar la trama.

- Direcciones de multidifusión: Las direcciones MAC de multidifusión se utilizan para permitir que un subconjunto dinámico de dispositivos en una LAN se comunique.

Cómo aprenden los switches las direcciones MAC

La segunda función principal de un conmutador es aprender las direcciones MAC y las interfaces para colocarlas en su tabla de direcciones. Con una tabla de direcciones MAC completa y precisa, el conmutador puede tomar decisiones precisas de reenvío y filtrado.

A continuación vamos enseñar Como se muestra en la figura, después de que Fred envía su primera trama (etiquetada como “1”) a Barney, el conmutador agrega una entrada para 0200.1111.1111, la dirección MAC de Fred, asociada con la interfaz

Fa0/1. Cuando Barney responde en el paso 2, el conmutador agrega una segunda entrada, esta para 0200.2222.2222, la dirección MAC de Barney, junto con la interfaz Fa0/2, que es la interfaz en la que el conmutador recibió la trama. El aprendizaje siempre ocurre mirando la dirección MAC de origen en el marco.

El interruptor reenvía el primer cuadro fuera de Fa0/2, Fa0/3 y Fa0/4, aunque 0200.2222.2222 (Barney) solo está fuera de Fa0/2. El conmutador no reenvía la trama hacia fuera Fa0/1, porque un conmutador nunca reenvía una trama por el mismo interfaz en la que llegó. Cuando Barney responde a Fred, el conmutador agrega correctamente una entrada para 0200.2222.2222 (Fa0/2) a su tabla de direcciones. Las tramas posteriores enviadas a la dirección de destino 0200.2222.2222 ya no necesitarán enviarse Fa0/3 y Fa0/4, solo se reenviarán Fa0/2.

Larry envía una sola trama de unidifusión a la dirección MAC de Bob, pero Bob está apagado, por lo que ninguno de los conmutadores ha aprendido todavía la dirección MAC de Bob. La dirección MAC de Bob sería una dirección unidifusión desconocida en este momento.

De esta manera se muestra que una sola trama, enviada por Larry a Bob, se repite para siempre porque la red tiene redundancia pero no STP.

Los switches utilizan la lógica de capa 2 y examinan el encabezado del enlace de datos de Ethernet para elegir cómo procesar las tramas. En particular, los switches toman decisiones para reenviar y filtrar tramas, aprender direcciones

MAC y usar STP para evitar bucles, de la siguiente manera:

Paso 1 Cambia las tramas de reenvío en función de la dirección de destino:

a. Si la dirección de destino es un unicast de difusión, multidifusión o destino desconocido (un unicast que no figura en la tabla MAC), el switch inunda la trama.

b. Si la dirección de destino es una dirección de unidifusión conocida (una dirección de unidifusión que se encuentra en la tabla MAC):

i. Si la interfaz de salida que aparece en la tabla de direcciones MAC es diferente de la interfaz en la que se recibió la trama, el conmutador reenvía la trama por la interfaz de salida.

ii. Si la interfaz de salida es la misma que la interfaz en la que se recibió la trama, el conmutador filtra la trama, lo que significa que el conmutador simplemente ignora la trama y no la reenvía.

Paso 2 Los switches utilizan la siguiente lógica para aprender las entradas de la tabla de direcciones MAC:

a. Para cada trama recibida, examine la dirección MAC de origen y observe la interfaz desde la que se recibió la trama.

b. Si aún no están en la tabla, agregue la dirección y la interfaz, configurando el temporizador de inactividad en 0.

C. Si ya está en la tabla, restablezca el temporizador de inactividad para la entrada a 0.

Paso 3 Los conmutadores utilizan STP para evitar bucles al bloquear algunas interfaces, lo que significa que no envían ni reciben tramas.

Dominios de colisión y dominios de difusión

Al crear cualquier LAN Ethernet, utiliza algún tipo de dispositivo de red, generalmente conmutadores en la actualidad, algunos enrutadores y posiblemente algunos concentradores. Las diferentes partes de una LAN Ethernet pueden comportarse de manera diferente, en términos de funcionamiento y rendimiento, según los tipos de dispositivos que se utilicen.

Dominios de colisión

Un dominio de colisión es un segmento de una red de computadores, conectado a un mismo medio de transmisión, donde es posible que las tramas puedan "colisionar" (interferir) con otros. Estas colisiones se dan particularmente en el protocolo de red Ethernet.

A medida que aumenta el número de nodos que pueden transmitir en un segmento de red, aumentan las posibilidades de que dos de ellos transmitan a la vez. Esta transmisión simultánea ocasiona una interferencia entre las señales de ambos nodos, que se conoce como colisión. Conforme aumenta el número de colisiones disminuye el rendimiento de la red.

Para revisar el concepto central, la Figura 7-8 ilustra los dominios de colisión.

Dominios de difusión

broadcast domain El dominio de difusión es el conjunto de todos los dispositivos que reciben tramas de broadcast que se originan en cualquier dispositivo del conjunto. Los conjuntos de

broadcast generalmente están limitados por enrutadores, dado que los routers no envían tramas de broadcast.

Si bien los switches filtran la mayoría de las tramas según las direcciones MAC, no hacen lo mismo con las tramas de broadcast. Para que otros switches de la LAN obtengan tramas de broadcast, estas deben ser reenviadas por switches. Una serie de switches interconectados forman un dominio de broadcast simple. Solo una entidad de capa 3, como un router o una LAN virtual (VLAN), puede detener un dominio de difusión de capa 3. Los routers y las VLAN se utilizan para segmentar los dominios de colisión y de broadcast.

Cuando un switch recibe una trama de broadcast, la reenvía a cada uno de sus puertos excepto al puerto entrante en el que el switch recibió esa trama. Cada dispositivo conectado reconoce la trama de broadcast y la procesa. Esto provoca una disminución en la eficacia (ineficiencia) de la red dado que el ancho de banda se utiliza para propagar el tráfico de broadcast.

El impacto de los dominios de colisión y transmisión en el diseño de LAN

Al diseñar una LAN, debe tener en cuenta las compensaciones al elegir la cantidad de dispositivos en cada dominio de colisión y dominio de transmisión. Primero, considere los dispositivos en un solo dominio de colisión por un momento. Para un único dominio de colisión:

- Los dispositivos comparten el ancho de banda disponible.

- Los dispositivos pueden usar ese ancho de banda de manera ineficiente debido a los efectos de las colisiones, particularmente bajo una mayor utilización.

LAN virtuales (VLAN)

La mayoría de las redes empresariales de hoy utilizan el concepto de LAN virtuales (VLAN).

Antes de comprender las VLAN, debe tener una comprensión muy específica de la definición de una LAN. Aunque puede pensar y definir el término "LAN" desde muchas perspectivas, una perspectiva en particular lo ayudará a comprender las VLAN:

Una LAN consta de todos los dispositivos en el mismo dominio de transmisión.

Sin VLAN, un conmutador considera que todas las interfaces del conmutador están en el mismo dominio de difusión.

Las siguientes dos figuras comparan dos LAN con el fin de explicar un poco más sobre las VLAN. Primero, antes de que existieran las VLAN, si un diseño especificaba dos dominios de transmisión separados, se usarían dos conmutadores, uno para cada dominio de transmisión, como se muestra en la Figura 7-10. La Figura 7-11 muestra los mismos dos dominios de difusión que en la Figura 7-10, ahora implementados como dos VLAN diferentes en un solo conmutador.

Terminología de diseño de LAN de campus

El términoLAN del campusse refiere a la LAN creada para soportar edificios más grandes, o varios edificios en cierta proximidad entre sí. Por ejemplo, una empresa podría arrendar espacio de oficinas en varios edificios en el mismo parque de oficinas. Luego, los ingenieros de redes pueden construir una LAN de campus que incluya conmutadores en cada edificio, además de enlaces Ethernet entre los conmutadores de los edificios, para crear una LAN de campus más grande.

Por ejemplo, la gran mayoría de las PC que ya están instaladas en redes hoy en día tienen NIC 10/100, y muchas PC nuevas hoy en día tienen NIC 10/100/1000 integradas en la PC. Suponiendo que se haya instalado el cableado adecuado, una NIC 10/100/1000 puede usar la negociación automática para usar 10BASE-T (10 Mbps), 100BASE-TX (100 Mbps) o 1000BASE-T (1000 Mbps o 1 Gbps) Ethernet, cada uno usando el mismo cable UTP.

Medios LAN Ethernet y longitudes de cable

Al diseñar una LAN de campus, un ingeniero debe considerar la longitud de cada tramo de cable y luego encontrar el mejor tipo de Ethernet y el tipo de cableado que admita esa longitud de cable. Por ejemplo, si una empresa alquila espacio en cinco edificios en el mismo parque de oficinas, el ingeniero debe calcular la longitud que deben tener los cables entre los edificios y luego elegir el tipo correcto de Ethernet.

Los tres tipos más comunes de Ethernet en la actualidad (10BASE-T, 100BASE-TX y 1000BASE-T) tienen la misma restricción de cable de 100 metros, pero usan cables ligeramente diferentes. La EIA/TIA define los estándares de cableado de Ethernet, incluida la calidad del cable. Cada estándar de

Ethernet que utiliza cableado UTP enumera una categoría de calidad de cableado como la categoría mínima que admite el estándar.

Capítulo 8: Funcionamiento de los conmutadores LAN de Cisco

Acceso a la CLI del conmutador Cisco Catalyst 2960

Cisco usa el mismo concepto de acinterfaz de línea de comandos (CLI) con sus productos de enrutador y la mayoría de sus productos de conmutador Catalyst LAN. La CLI es una interfaz basada en texto en la que el usuario, generalmente un ingeniero de redes, ingresa un comando de texto y presiona Enter. Presionando Entrar envía el comando al interruptor, que le dice al

dispositivo que haga algo. El conmutador hace lo que dice el comando y, en algunos casos, el conmutador responde con algunos mensajes que indican los resultados del comando.

Dentro de la marca Cisco Catalyst de conmutadores LAN, Cisco produce una amplia variedad de series o familias de conmutadores. Cada serie de interruptores incluye varios modelos específicos de interruptores que tienen características similares, compensaciones similares de precio versus rendimiento y componentes internos similares.

Cisco se refiere a los conectores físicos de un switch comointerfacesopuertos. Cada interfaz tiene un número en el estilo.X/y, dóndeXyyson dos números diferentes. En un 2960, el número antes de / siempre es 0. La primera interfaz 10/100 en un 2960 se numera a partir de 0/1, la segunda es 0/2 y así sucesivamente. Las interfaces también tienen nombres; por ejemplo, “interfaz FastEthernet 0/1” es la primera de las interfaces 10/100. Cualquier interfaz compatible con Gigabit se denominaría interfaz "GigabitEthernet". Por ejemplo, la primera interfaz 10/100/1000 en un 2960 sería "interfaz gigabitethernet 0/1”.

La figura 8-1 muestra una fotografía de la serie de switches 2960 de Cisco. Cada interruptor es un modelo específico diferente de interruptor dentro de la serie 2960.

Cisco admite dos tipos principales de sistemas operativos de switch:Sistema operativo interredes(IOS) y

Sistema operativo catalizador (sistema operativo Cat). La mayoría de las series de conmutadores Cisco

Catalyst en la actualidad solo ejecutan Cisco IOS, pero por algunas razones históricas, algunos de los conmutadores Cisco LAN de gama alta admiten tanto Cisco IOS como Cat OS.

Acceso a la CLI de Cisco IOS

El software Cisco IOS para switches Catalyst implementa y controla la lógica y las funciones realizadas por un switch Cisco. Además de controlar el rendimiento y el comportamiento del switch, Cisco IOS también define una interfaz para humanos llamada CLI. La CLI de Cisco IOS permite al usuario utilizar un programa de emulación de terminal, que acepta el texto introducido por el usuario. Cuando el usuario presiona Enter, el emulador de terminal envía ese texto al conmutador.

Se puede acceder a la CLI del switch a través de tres métodos populares: la consola, Telnet y Secure Shell (SSH). Dos de estos métodos (Telnet y SSH) utilizan la red IP en la que reside el conmutador para llegar al conmutador. La consola es un puerto físico creado específicamente para permitir el acceso a la CLI. La Figura 8-3 muestra las opciones.

Acceso a la CLI con Telnet y SSH

La aplicación TCP/IP Telnet permite que un emulador de terminal se comunique con un dispositivo, al igual que sucede con un emulador en una PC conectada a la consola. Sin embargo, Telnet usa una red

IP para enviar y recibir los datos, en lugar de un cable especializado y un puerto físico en el dispositivo. Los protocolos de aplicación Telnet llaman al emulador de terminal un cliente Telnety el dispositivo que escucha los comandos y responde a ellos unservidor telnet. Telnet es un protocolo de capa de aplicación basado en TCP que utiliza el conocido puerto 23.

Cubierta segura (SSH) hace las mismas cosas básicas que Telnet, pero de una manera más segura mediante el uso de cifrado. Al igual que el modelo Telnet, el software de cliente SSH incluye un emulador de terminal y la capacidad de enviar y recibir datos mediante IP. Al igual que Telnet, SSH usa TCP, mientras usa el conocido puerto 22 en lugar del 23 de Telnet. Al igual que con Telnet, el servidor SSH (en el conmutador) recibe el texto de cada cliente SSH, procesa el texto como un comando y envía los mensajes de vuelta al cliente.

Seguridad de contraseña para acceso CLI

De forma predeterminada, un conmutador Cisco es muy seguro siempre que esté bloqueado dentro de una habitación. De forma predeterminada, un conmutador solo permite el acceso a la consola, pero no permite el acceso a Telnet o SSH. Desde la consola, puede obtener acceso completo a todos los comandos de cambio y, si así lo desea, puede detener todas las funciones del interruptor. Sin embargo, el acceso a la consola requiere acceso físico al conmutador, por lo que es razonable permitir el acceso a la consola para los conmutadores recién extraídos de las cajas de envío.

Modos de usuario y activación (privilegiados)

Los tres métodos de acceso a la CLI cubiertos hasta ahora (consola, Telnet y SSH) colocan al usuario en un área de la CLI llamada modo EXEC del usuario. Modo EXEC de usuario, a veces también llamado modo de usuario, permite al usuario mirar alrededor pero no romper nada.

Cisco IOS admite un modo EXEC más potente llamadopermitirModo (también conocido como privilegiado modo oEXEC privilegiadomodo). El modo de habilitación se llama así porque elpermitir El comando se utiliza para llegar a este modo, como se muestra en la Figura 8-6.

Funciones de ayuda de la CLI y comandos básicos

La Tabla 8-4 resume las opciones de ayuda de recuperación de comandos disponibles en la CLI.

La Tabla 8-5 enumera los comandos utilizados para manipular los comandos ingresados previamente a cualquier comando.

Configuración del software Cisco IOS

Debe comprender cómo configurar un conmutador Cisco para tener éxito en el examen y en trabajos de redes reales. Esta sección cubre los procesos básicos de configuración, incluido el concepto de un archivo de configuración y las ubicaciones en las que se pueden almacenar los archivos de configuración.

Las configuraciones de otro modo para la CLI de Cisco, muy similar al modo de usuario y al modo privilegiado. El modo de usuario le permite emitir comandos no disruptivos y muestra cierta información.

Los comandos ingresados en el modo de configuración actualizan el archivo de configuración activo. Estos cambios en la configuración ocurren inmediatamente cada vez que presiona la tecla enter al final de un comando. ¡Tenga cuidado cuando ingrese un comando de configuración!

Cuando comienza a practicar con CLI con equipo real, la navegación entre los modos puede volverse natural. Por ahora, considere el Ejemplo 8-1, que muestra lo siguiente:

- Pasar del modo de habilitación al modo de configuración global mediante el configure terminal EXEC comando

- Usando el comando hostname Fred configuración global para configurar el nombre del conmutador

- Pasar del modo de configuración global al modo de configuración de línea de consola (usando el comando line console 0)

- Establecer la contraseña simple de la consola hope (utilizando password hope subcomando de línea)

- Pasar del modo de configuración de consola al modo de configuración de interfaz

(Usando el comando interface)

- Configurando la velocidad a 100 Mbps para la interfaz Fa0/1 (usando speed 100 subcomando de interfaz)

- Pasar del modo de configuración de interfaz al modo de configuración global

(Usando el comando exit)

Copiar y borrar archivos de configuración

Para poder realizar el copiado de una configuración de un archivo de inicio, en donde se sobrescribe el archivo se debe de usar el comando copy running-config

Startup-config, esto hace que se sobrescribe el archivo de configuración de inicio actual con lo que está actualmente en el archivo de configuración en ejecución. copy comando se puede utilizar para copiar archivos en un conmutador, generalmente un archivo de configuración o una nueva versión del software Cisco IOS. El método más básico para mover archivos de configuración dentro y fuera de un switch es usar el Copy Comando para copiar archivos entre RAM o NVRAM en un conmutador y un servidor TFTP. Los archivos se pueden copiar entre cualquier par, como se muestra en la Figura 8-9.

Configuración inicial (Setup Mode)

El software Cisco IOS admite dos métodos principales para dar a un switch una configuración básica inicial: el modo de configuración, que ya se trató en este capítulo, y el modo de instalación. El modo de configuración lleva al administrador del conmutador a una configuración básica del conmutador mediante preguntas que solicitan al administrador los parámetros de configuración básicos.

La figura 8-10 y el ejemplo 8-3 describen el proceso utilizado por el modo de configuración. El modo de configuración se usa con mayor frecuencia cuando se inicia el conmutador y no tiene configuración en la NVRAM. También puede ingresar al modo de configuración usando el setup comando desde el modo privilegiado.

La configuración se comporta como se muestra en el ejemplo 8-3, independientemente de si se llegó a la configuración arrancando con una NVRAM vacía o si la setup Se utilizó el comando EXEC privilegiado.

Primero, el conmutador le pregunta si desea ingresar al cuadro de diálogo de configuración inicial. Respondiendo y o yes se pone en modo de configuración.

Cuando haya terminado de responder las preguntas de configuración, el conmutador le pedirá que elija una de tres opciones:

0: No guarde nada de esta configuración y vaya al símbolo del sistema CLI.

1: No guarde nada de esta configuración, pero comience de nuevo en el modo de configuración.

2: Guarde la configuración tanto en la configuración de inicio como en la configuración en ejecución, y vaya a la línea de comandos de la CLI. También puede abortar el proceso de configuración antes de responder a todas las preguntas y llegar a un mensaje de CLI, presionando Ctrl-C.

Capítulo 9

Ethernet Switch Configuración

Muchos switches Cisco Catalyst utilizan la misma interfaz de línea de comandos del software Cisco IOS (CLI) como enrutadores Cisco. Además de tener la misma apariencia, los interruptores y los enrutadores a veces admiten exactamente la misma configuración y muestran los comandos. Además, como se mencionó en el Capítulo 8, algunos de los mismos comandos y procesos que se muestran para Cisco

Los interruptores funcionan de la misma manera para los enrutadores Cisco.

Este capítulo explica una amplia variedad de elementos configurables en los switches de Cisco. algunos temas son relativamente importantes, como la configuración de usuarios y contraseñas para que cualquier el acceso remoto a un conmutador es seguro. Algunos temas son relativamente poco importantes, pero útiles, como

como la capacidad de asignar una descripción de texto a una interfaz con fines de documentación.

Sin embargo, este capítulo contiene la mayoría de los temas de configuración del switch para este libro, con la excepción de los comandos de configuración de Cisco Discovery Protocol (CDP) en Capítulo 10.

Protección de la CLI del conmutador

Para llegar al modo de habilitación de un interruptor, un usuario debe llegar al modo de usuario desde la consola o desde una sesión Telnet o SSH y, a continuación, utilice el comando enable. con defecto

ajustes de configuración, un usuario en la consola no necesita proporcionar una contraseña para llegar modo de usuario o modo de habilitación. La razón es que cualquier persona con acceso físico al conmutador o la consola del enrutador podría restablecer las contraseñas en menos de 5 minutos usando la contraseña procedimientos de recuperación que publica Cisco. Por lo tanto, los enrutadores y los conmutadores están predeterminados para permitir que el acceso de usuario de la consola para habilitar el modo para alcanzar el modo de activación desde un vty (Telnet o SSH), el conmutador debe configurarse con varios artículos:

- Una dirección IP
- Seguridad de inicio de sesión en las líneas vty
- Una contraseña de habilitación

La mayoría de los ingenieros de redes querrán poder establecer una conexión Telnet o SSH para cada conmutador, por lo que tiene sentido configurar los conmutadores para permitir un acceso seguro. Además, aunque alguien con acceso físico al conmutador puede usar el proceso de recuperación de contraseña para obtener acceso al conmutador, todavía tiene sentido configurar la seguridad incluso para el acceso desde la consola.

Esta sección examina la mayoría de los detalles de configuración relacionados con el acceso al modo de activación en un conmutador o enrutador. El único tema clave que no se cubre aquí es la configuración de la dirección IP, que se trata más adelante en este capítulo en la sección "Configuración de la dirección IP del conmutador".

En particular, esta sección cubre los siguientes temas:

- Seguridad de contraseña simple para la consola y acceso Telnet
- Shell seguro (SSH)
- Cifrado de contraseña
- Habilitar contraseña de modo

Configuración de seguridad de contraseña simple

Un ingeniero puede acceder al modo de usuario en un conmutador o enrutador de Cisco desde la consola o a través de Telnet o SSH. De manera predeterminada, los conmutadores y enrutadores permiten que un usuario de la consola acceda de inmediato modo de usuario después de iniciar sesión, sin necesidad de contraseña. Con la configuración predeterminada, los usuarios de Telnet son rechazados cuando intentan acceder al conmutador, porque aún no se ha introducido una contraseña vty. configurado. Independientemente de estos valores predeterminados, tiene sentido proteger el modo de usuario con contraseña para usuarios de consola, Telnet y SSH.

Configuración de nombres de usuario y Secure Shell (SSH)

Telnet envía todos los datos, incluidas todas las contraseñas ingresadas por el usuario, como texto claro. el seguro La aplicación Shell (SSH) proporciona la misma función que Telnet, mostrando una terminal ventana del emulador y permitir que el usuario se conecte de forma remota a la CLI de otro host.

Sin embargo, SSH encripta los datos enviados entre el cliente SSH y el servidor SSH, haciendo SSH es el método preferido para el inicio de sesión remoto en conmutadores y enrutadores en la actualidad.

Para agregar soporte para inicio de sesión SSH a un conmutador o enrutador de Cisco, el conmutador necesita varios comandos de configuración. Por ejemplo, SSH requiere que el usuario proporcione un nombre de usuario y contraseña en lugar de solo una contraseña. Por lo tanto, el interruptor debe reconfigurarse para usar uno de dos métodos de autenticación de usuario que requieren tanto un nombre de usuario como una contraseña: un método con los usuarios y contraseñas configuradas en el switch, y el otro con el nombre de usuario y contraseñas configurados en un servidor externo llamado Autenticación, Servidor de Autorización y Contabilidad (AAA). (Este libro cubre la configuración usando nombres de usuario/contraseñas configuradas localmente). La Figura 9-1 muestra un diagrama de la configuración y proceso necesarios para admitir SSH

El ejemplo muestra un comentario resaltado en gris justo antes de los comandos de configuración en cada paso. Además, tenga en cuenta la clave pública creada por el conmutador, que aparece en la parte resaltada de la salida del comando show crypto key mypubkey rsa. Cada cliente SSH necesita un copia de esta clave, ya sea agregando esta clave a la configuración del cliente SSH de antemano, o al permitir que el conmutador envíe esta clave pública al cliente cuando el cliente SSH se conecta por primera vez a el interruptor

Cifrado de contraseña

Varios de los comandos de configuración utilizados para configurar contraseñas almacenan las contraseñas en texto claro en el archivo de configuración en ejecución, al menos de forma predeterminada. En particular, las contraseñas simples configurado en la consola y lineas vty, con el comando contraseña, más la contraseña

en el comando de nombre de usuario, se almacenan todos en texto sin cifrar de forma predeterminada. (El secreto de habilitación El comando oculta automáticamente el valor de la contraseña).

Para evitar la vulnerabilidad de la contraseña en una versión impresa del archivo de configuración, o en una copia de seguridad del archivo de configuración almacenado en un servidor, puede cifrar o codificar las contraseñas mediante el comando de configuración global service password-encryption. El presencia o ausencia del comando de configuración global service password-encryption dicta si las contraseñas están encriptadas de la siguiente manera:

1. Cuando se configura el comando de cifrado de contraseña de servicio, todas las consolas, vty, y las contraseñas de comando de nombre de usuario se cifran inmediatamente.
2. Si el comando de cifrado de contraseña del servicio ya se configuró, cualquier
3. los cambios en estas contraseñas están encriptados.
4. Si más tarde se utiliza el comando de cifrado de contraseña sin servicio, las contraseñas permanecen encriptados, hasta que se cambien, momento en el cual se muestran en texto sin cifrar.

Las dos contraseñas del modo de activación

El comando enable lo mueve del modo EXEC de usuario (con un aviso de nombre de host>) a

modo EXEC privilegiado (con un mensaje de hostname#). Se puede configurar un enrutador o conmutador solicitar una contraseña para acceder al modo de activación de acuerdo con las siguientes reglas:

1. Si se utiliza el comando de configuración global enable password actual-password,
2. define la contraseña requerida cuando se usa el comando enable EXEC. esta contraseña
3. aparece como texto no cifrado en el archivo de configuración de forma predeterminada.
4. Si se utiliza el comando de configuración global enable secret actual-password, define la contraseña requerida cuando se usa el comando enable EXEC. Esta contraseña está en la lista como un valor hash MD5 oculto en el archivo de configuración.
5. Si se utilizan ambos comandos, la contraseña establecida en el comando enable secret define que contraseña se requiere

Cuando se configura el comando enable secret, el enrutador o conmutador oculta automáticamente la contraseña. Si bien a veces se menciona que está encriptado, el secreto de habilitación la contraseña en realidad no está encriptada. En su lugar, IOS aplica una función matemática a la contraseña, denominada hash Message Digest 5 (MD5), que almacena los resultados de la fórmula en el archivo de configuración. IOS hace referencia a este estilo de codificación de la contraseña como tipo 5 en la salida en el ejemplo 9-4. Tenga en cuenta que la codificación MD5 es mucho más segura que el cifrado se utiliza para otras contraseñas con el comando service password-encryption. El ejemplo muestra la creación del comando enable secret, su formato y su eliminación.

Configuración de consola y vty

Esta sección cubre algunos ajustes de configuración pequeños que afectan el comportamiento de la CLI conexión desde la consola y/o vty (Telnet y SSH). pancartas Los enrutadores y conmutadores de Cisco pueden mostrar una variedad de pancartas dependiendo de qué enrutador o cambiar el administrador está haciendo. Un banner es simplemente un texto que aparece en la pantalla para el usuario Puede configurar un enrutador o conmutador para mostrar varios banners, algunos antes inicio de sesión y algo después. La Tabla 9-2 enumera los tres banners más populares y su uso típico

El comando de configuración global banner se puede utilizar para configurar los tres tipos de estos pancartas En cada caso, el tipo de banner aparece como el primer parámetro, siendo MOTD la opción predeterminada. El primer carácter que no está en blanco después del tipo de banner se llama comienzo carácter delimitador. El texto del banner puede abarcar varias líneas, con el usuario CLI presionando Introduzca al final de cada línea. La CLI sabe que el banner se configuró tan pronto a medida que el usuario ingresa el mismo carácter delimitador nuevamente.

Los comandos logging synchronous y exec-timeout

La consola recibe automáticamente copias de todos los mensajes de syslog no solicitados en un conmutador o enrutador; esa función no se puede desactivar. La idea es que si el conmutador o enrutador necesita informar el administrador de la red alguna información importante y posiblemente urgente, el administrador puede estar en la consola y puede notar el mensaje. Normalmente un interruptor o El enrutador pone estos mensajes de syslog en la pantalla de la

consola en cualquier momento, incluso en medio de un comando que está ingresando, o en medio de la salida de un programa dominio.

También puede hacer que usar la consola o las líneas vty sea más conveniente configurando un tiempo de espera de inactividad en la consola o vty. De forma predeterminada, el conmutador o enrutador automáticamente desconecta a los usuarios después de 5 minutos de inactividad, tanto para los usuarios de la consola como para los usuarios que se conectan a líneas vty mediante Telnet o SSH. Cuando configura el exec-timeout minutos segundos subcomando de línea, se le puede indicar al conmutador o enrutador un temporizador de inactividad diferente. Además, si tú establezca el tiempo de espera en 0 minutos y 0 segundos, el enrutador nunca agota el tiempo de espera de la consola conexión. El ejemplo 9-6 muestra la sintaxis de estos dos comandos

Configuración y funcionamiento del conmutador LAN

Uno de los hechos más convenientes sobre la configuración del conmutador LAN es que los conmutadores Cisco trabajar sin ninguna configuración. Los switches Cisco se envían de fábrica con todas las interfaces habilitado (una configuración predeterminada de no apagado) y con la negociación automática habilitada para puertos que se ejecutan a varias velocidades y configuraciones dúplex (una configuración predeterminada de dúplex automático) y velocidad automática). Todo lo que tiene que hacer es conectar los cables Ethernet y enchufar la alimentación cable a una toma de corriente, y el interruptor está listo para funcionar: aprender direcciones MAC, hacer decisiones de reenvío/filtrado, e incluso usar STP por defecto

La segunda mitad de este capítulo continúa con la cobertura de la configuración del switch, principalmente cubriendo características que se aplican solo a conmutadores y no a enrutadores. En particular, esta sección cubre lo siguiente:

1. Cambiar la configuración de IP
2. Configuración de interfaz (incluyendo velocidad y dúplex)
3. seguridad portuaria
4. Configuración de VLAN
5. Protección de las interfaces de conmutador no utilizadas

Configuración de la dirección IP del conmutador

Para permitir el acceso Telnet o SSH al conmutador, para permitir otros protocolos de gestión basados en IP como el Protocolo simple de administración de redes (SNMP) para funcionar según lo previsto, o para permitir acceso al conmutador mediante herramientas gráficas como Cisco Device Manager (CDM), el conmutador necesita una dirección IP. Los switches no necesitan una dirección IP para poder reenviar Ethernet marcos La necesidad de una dirección IP es simplemente para admitir el tráfico de administración de gastos generales, como iniciar sesión en el interruptor.

Un conmutador basado en IOS configura su dirección IP y máscara en una interfaz virtual especial llamada la interfaz VLAN1. Esta interfaz juega el mismo papel que una interfaz Ethernet en una PC.

En efecto, la interfaz VLAN 1 de un conmutador proporciona al conmutador una interfaz en la VLAN predeterminada utilizado en todos los puertos del conmutador, es decir, VLAN 1. Los siguientes pasos enumeran los comandos

utilizado para configurar IP en un conmutador:

Paso 1 Ingrese al modo de configuración de VLAN 1 mediante la configuración global de la interfaz vlan 1 comando (desde cualquier modo de configuración).

Paso 2 Asigne una dirección IP y una máscara usando la máscara de dirección IP de la dirección IP

subcomando de interfaz.

Paso 3 Habilite la interfaz VLAN 1 usando la interfaz sin apagado subcomando

Paso 4 Agregue el comando global ip default-gateway ip-address para configurar el puerta de enlace predeterminada.

De particular interés, este ejemplo muestra cómo habilitar cualquier interfaz, interfaces VLAN incluido. Para habilitar administrativamente una interfaz en un conmutador o enrutador, utilice el no subcomando de interfaz de apagado. Para deshabilitar administrativamente una interfaz, usaría el subcomando de la interfaz de apagado. Los mensajes que se muestran en el Ejemplo 9-7, inmediatamente después del comando no shutdown, hay mensajes de syslog generados por el conmutador que indican que el interruptor efectivamente habilitó la interfaz.

Para que el conmutador actúe como un cliente DHCP para descubrir su dirección IP, máscara y puerta de enlace predeterminada, aún necesita configurarlo. Utiliza los mismos pasos que para la configuración estática, con el siguientes diferencias en los pasos 2 y 4:

Paso 2: use el comando dhcp de dirección IP, en lugar de la máscara de dirección IP de dirección IP comando, en la interfaz VLAN 1

Paso 4: No configure el comando global ip default-gateway.

El ejemplo 9-8 muestra un ejemplo de configuración de un conmutador para usar DHCP para adquirir una IP

Finalmente, la salida del comando show interface vlan 1, que se muestra al final del Ejemplo 9-8, enumera dos detalles muy importantes relacionados con el direccionamiento IP del conmutador. Primero, este comando show enumera el estado de la interfaz de la interfaz VLAN 1, en este caso, "activa y activa". Si la VLAN 1 la interfaz no está activa, el conmutador no puede usar su dirección IP para enviar y recibir tráfico. Notablemente, si olvida ejecutar el comando no shutdown, la interfaz VLAN 1 permanece en su estado de apagado predeterminado y aparece como "administrativamente inactivo" en el comando show producción. En segundo lugar, tenga en cuenta que la salida enumera la dirección IP de la interfaz en la tercera línea de la producción. Si el conmutador no logra adquirir una dirección IP con DHCP, la salida en su lugar listaría el hecho de que la dirección (con suerte) será adquirida por DHCP. Tan pronto como una dirección tiene sido

alquilado mediante DHCP, la salida del comando se parece al Ejemplo 9-8. Sin embargo, nada en la salida del comando show interface vlan 1 menciona que la dirección es configurada estáticamente o arrendada por DHCP.

Configuración de interfaces de conmutador

IOS usa el término interfaz para referirse a los puertos físicos que se usan para reenviar datos hacia y desde otros dispositivos. Cada interfaz puede configurarse con varios ajustes, cada uno de los cuales puede diferir de interfaz a interfaz.

IOS utiliza subcomandos de la interfaz para configurar estos ajustes. Por ejemplo, las interfaces pueden ser configurado para usar los subcomandos de interfaz de velocidad y dúplex para configurar esos ajustes estáticamente, o una interfaz puede usar la negociación automática (el valor predeterminado). El ejemplo 9-9 muestra cómo configurar el dúplex y la velocidad, así como el comando de descripción, que es simplemente un texto descripción de lo que hace una interfaz

Seguridad Portuaria

Si el ingeniero de redes sabe qué dispositivos deben cablearse y conectarse a un determinado interfaz en un conmutador, el ingeniero puede usar la seguridad del puerto para restringir esa interfaz para que solo los dispositivos esperados pueden usarlo. Esto reduce la exposición a algunos tipos de ataques en que el atacante conecta una computadora portátil a la toma de pared que se conecta a un puerto de conmutador que ha sido configurado para usar la seguridad del puerto. Cuando ese dispositivo inapropiado intenta enviar tramas a la interfaz del conmutador, el conmutador puede emitir mensajes informativos, descartar tramas desde ese dispositivo, o incluso descartar marcos de todos los dispositivos apagando efectivamente el interfaz.

La configuración de la seguridad del puerto implica varios pasos. Básicamente, debe hacer que el puerto sea un puerto de acceso, lo que significa que el puerto no está realizando ningún enlace troncal de VLAN. Entonces necesitas habilite la seguridad del puerto y luego configure las direcciones MAC reales de los dispositivos autorizados para usar ese puerto. La siguiente lista describe los pasos, incluidos los comandos de configuración usado:

Paso 1 Convierta la interfaz del conmutador en una interfaz de acceso utilizando el modo de acceso del puerto del conmutador subcomando de interfaz.

Paso 2 Habilite la seguridad del puerto mediante la interfaz de seguridad del puerto switchport subcomando

Paso 3 (Opcional) Especifique el número máximo de direcciones MAC permitidas asociado con la interfaz usando el switchport port-security subcomando de interfaz de número máximo. (Predeterminado a una MAC DIRECCIÓN.)

Paso 4 (Opcional) Defina la acción a realizar cuando se recibe una trama de una Dirección MAC distinta de las direcciones definidas mediante el puerto de conmutación violación de seguridad portuaria {proteger | restringir | apagar} interfaz subcomando (La acción predeterminada es cerrar el puerto).

Paso 5A Especifique las direcciones MAC permitidas para enviar tramas a esta interfaz utilizando la dirección mac de la dirección mac de la seguridad del puerto switchport dominio. Use el comando varias veces para definir más de uno

Dirección MAC.

Paso 5B Alternativamente, en lugar del Paso 5A, use el proceso de "aprendizaje persistente" para aprenda y configure dinámicamente las direcciones MAC de los hosts conectados mediante la configuración del subcomando switchport port-security mac address sticky interface.

Configuración de VLAN

Las interfaces de switch de Cisco se consideran interfaces de acceso o interfaces troncales. Por definición, las interfaces de acceso envían y reciben tramas solo en una sola VLAN, llamada acceder a la VLAN. Las interfaces de enlace troncal envían y reciben tráfico en varias VLAN. El concepto y la configuración para el enlace troncal VLAN está más allá del alcance de este libro, pero se trata en detalles en la Guía de certificación oficial CCNA ICND2 640-816, Capítulos 1 y 3. Este libro se centra en la configuración de VLAN para las interfaces de acceso, que por definición deben asignarse a una sola VLAN

Para que un switch de Cisco reenvíe tramas en interfaces de acceso en una VLAN particular, el switch debe configurarse para creer que la VLAN existe. Además, el interruptor debe tener uno más interfaces de acceso asignadas a la VLAN. De manera predeterminada, los switches de Cisco ya tienen VLAN 1 configurada y todas las interfaces predeterminadas para ser asignadas a VLAN 1. Sin embargo, para agregar otra VLAN y asigne interfaces de acceso para estar en esa VLAN, puede seguir estos pasos

Paso 1 Para configurar una nueva VLAN:

a. Desde el modo de configuración, use el comando de configuración global vlan vlan-id para crear la VLAN y mover al usuario al modo de configuración de VLAN.

b. (Opcional) Utilice el subcomando name name VLAN para enumerar un nombre para el VLAN. Si no está configurado, el nombre de VLAN es VLANZZZZ, donde ZZZZ es el ID de VLAN decimal de cuatro dígitos.

Paso 2 Para configurar una VLAN para cada interfaz de acceso:

a. Use el comando de interfaz para pasar al modo de configuración de interfaz para cada interfaz deseada.

b. Utilice el subcomando de la interfaz switchport access vlan id-number para especificar el número de VLAN asociado con esa interfaz.

C. (Opcional) Para deshabilitar el enlace troncal para que el conmutador no decida dinámicamente use enlace troncal en la interfaz, y seguirá siendo una interfaz de acceso, use el subcomando de interfaz de acceso de modo switchport

El ejemplo comienza con el comando show vlan brief que confirma la configuración predeterminada de cinco VLAN no eliminables (VLAN 1 y 1002–1005), con todas las interfaces asignadas a VLAN 1. En particular, tenga en cuenta que este conmutador 2960 tiene 24 puertos Fast Ethernet (Fa0/1–Fa0/24) y dos puertos Gigabit Ethernet (Gi0/1 y Gi0/2), todos los cuales aparecen como asignados a la VLAN 1.

Después del primer comando show vlan brief, el ejemplo muestra la configuración completa proceso. La configuración muestra la creación de la VLAN 2, denominada "Freds-vlan", y la asignación de interfaces Fa0/13 y Fa0/14 a VLAN 2. Tenga en cuenta en particular que el ejemplo utiliza el comando de rango de interfaz, lo que hace que la interfaz switchport access vlan 2 subcomando que se aplicará a ambas interfaces en el rango, como se confirma en el show salida del comando running-config al final del ejemplo

Protección de las interfaces de conmutador no utilizadas

Cisco eligió originalmente los ajustes de configuración de interfaz predeterminados en los switches de Cisco para que las interfaces funcionen sin ninguna configuración abierta. Las interfaces negocian automáticamente la velocidad y el dúplex, y cada interfaz comienza en una habilitada (sin apagado), con todas las interfaces asignadas a la VLAN 1. Además, cada los valores predeterminados de la interfaz son negociar el uso de funciones de VLAN denominadas enlace troncal de VLAN y VLAN Trunking Protocol (VTP), que se tratan con más detalle en el Capítulo 2 de CCNA ICND2 640-816 Guía de certificación oficial.

Las buenas intenciones de Cisco para la operación “plug and play” tienen un efecto secundario desafortunado en que los valores predeterminados exponen los conmutadores a algunas amenazas de seguridad. Por lo tanto, para cualquier actualmente sin usar cambiar las interfaces, Cisco hace algunas recomendaciones generales para anular el valor predeterminado configuración de la interfaz para hacer que los puertos no utilizados sean más seguros. Las recomendaciones para no utilizados interfaces son las siguientes:

- Inhabilite administrativamente la interfaz mediante el subcomando de interfaz de apagado.
- Evite el enlace troncal de VLAN y el VTP haciendo que el puerto sea una interfaz no troncal mediante el subcomando de interfaz de acceso de modo switchport.
- Asigne el puerto a una VLAN no utilizada mediante el número de VLAN de acceso al puerto del conmutador subcomando de interfaz.

Francamente, si simplemente apaga la interfaz, la exposición a la seguridad desaparece, pero el otro dos tareas previenen cualquier problema inmediato si alguien más viene y habilita el interfaz mediante la configuración de un comando sin apagado.

Capítulo 10

Este capítulo tiene dos objetivos principales. Primero, cubre los temas restantes orientados a Ethernet para este libro, específicamente, algunos de los comandos y conceptos relacionados con la verificación de que un LAN Ethernet conmutada funciona.

Si la red no funciona, este capítulo sugiere herramientas que puede utilizar para averiguar por qué. Además, este capítulo sugiere algunos métodos de solución de problemas y prácticas que podrían mejorar sus habilidades de solución de problemas.

Aunque la resolución de problemas Los procesos explicados en este libro no se prueban directamente en los exámenes, pueden ayudarlo prepárese para responder correctamente algunas de las preguntas más difíciles del examen. "¿Ya sé esto?" Prueba El "¿Ya sé esto?" prueba le permite evaluar si debe leer el capítulo completo.

Si no falla más de una de estas ocho preguntas de autoevaluación, usted Es posible que desee pasar a la sección "Tareas de preparación para el examen". La Tabla 10-1 enumera los encabezados principales de este capítulo y la sección "¿Ya lo sé?" preguntas del examen que cubren el material en esas secciones. Esto le ayuda a evaluar su conocimiento de estas áreas específicas. Las respuestas a "¿Ya lo sé?" cuestionario aparecen en el Apéndice A.

Este capítulo contiene la primera cobertura específica de temas relacionados con la verificación y solución de problemas. La verificación se refiere al proceso de examinar una red para confirmar que está funcionando según lo diseñado.

La solución de problemas se refiere a examinar la red para determinar qué está causando un problema en particular para que pueda solucionarse. Como se mencionó en la Introducción de este libro, a lo largo de los años, los exámenes CCNA se han haciendo más y más preguntas relacionadas con la verificación y la solución de problemas.

Cada uno de estas preguntas suelen utilizar una topología única. Por lo general, requieren que presente una solicitud conocimiento de redes a problemas únicos, en lugar de simplemente estar listo para responder preguntas sobre listas de hechos que has memorizado. (Para más información y perspectivas sobre estos tipos de preguntas de examen, regrese a la Introducción de este libro, en la sección titulada “Formato de los Exámenes CCNA.”) Para ayudarlo a prepararse para responder preguntas que requieren habilidades de solución de problemas, este libro y la Guía de certificación oficial CCNA ICND2 640-816 dedica varios capítulos, además de secciones de otros capítulos, a la verificación y solución de problemas.

Este capítulo es el primero de este tipo en cualquiera de los dos libros, por lo que este capítulo comienza con algunas perspectivas sobre la solución de problemas de redes. Después de esta cobertura, el capítulo examina tres temas principales relacionados con solución de problemas de redes creadas con conmutadores LAN.

Preguntas de Sim atacante

Las preguntas de Sim proporcionan una descripción de texto de una red, un diagrama de red y software que simula la red. Independientemente de los detalles, las preguntas de simulación se pueden reducir a la siguiente: “La red no está funcionando completamente, así que complete la configuración o encuentre un problema con la configuración existente y arréglelo”. En definitiva, la solución a un sim.

La pregunta es, por definición, un cambio de configuración. Un plan de ataque para estos problemas es utilizar un proceso de solución de problemas más formalizado en el que examina cada paso en cómo se reenvían los datos desde el host de envío al anfitrión de destino.

Sin embargo, los estudios y la experiencia muestran que cuando los ingenieros piensan que la configuración puede tener un problema, el primer paso para la solución de problemas es observar los diversos Archivos de configuración. Para encontrar y resolver preguntas Sim en el examen, comparando rápidamente la configuración del enrutador y/o interruptor a lo que recuerda sobre la configuración normal necesario (según el texto de la pregunta) podría ser todo lo que necesita.

preguntas de simlet

Las preguntas de Simlet pueden obligar al examinado a interpretar el significado de varios espectáculos y Comandos de depuración. Es posible que las preguntas de Simlet no le digan la contraseña de habilitación, por lo que no puede incluso mirar la configuración, eliminando la opción de simplemente mirar la configuración para encontrar la causa raíz de un problema. En ese caso, el texto de la pregunta normalmente indica los detalles del escenario, lo que requiere que recuerdes o encuentres los comandos de show correctos, úsalos, y luego interpretar la salida. Además, debido a que es posible que las preguntas de simlet no le permitan cambiar la configuración, no recibe la respuesta positiva de que su respuesta es correcta.

Por ejemplo, una pregunta de simlet puede mostrar un diagrama de una LAN conmutada, indicando que PC1 puede hacer ping a PC2 pero no a PC3. Deberá recordar los comandos show correctos para usar (o tómese el tiempo para encontrar los comandos usando la tecla ?) para encontrar la causa raíz del problema. Puede utilizar varios enfoques diferentes para atacar este tipo de problemas; no hay una sola manera es necesariamente mejor que otro. El primer paso es pensar en lo que debería ocurrir normalmente. en la red, basado en cualquier diagrama de red e información en la pregunta. Entonces, muchas personas comienzan probando los comandos show (que recuerdan) que de alguna manera son relacionado con la pregunta. El texto de la pregunta probablemente da algunas pistas sobre el área del problema. Por ejemplo, quizás el problema esté relacionado con la seguridad del puerto. Muchas personas simplemente prueban el

comandos que saben que están relacionados con ese tema, como show port-security, solo para ver si la respuesta salta a la vista, y ese es un plan de ataque razonable. Este plan utiliza el sentido común y la intuición hasta cierto punto, y puede funcionar bien y rápidamente. Si la respuesta no se vuelve obvia cuando miras los comandos más obvios, un un enfoque más organizado puede ser

útil. Los capítulos de resolución de problemas de este libro y grandes secciones de solución de problemas de otros capítulos, revise la tecnología y sugiera una solución más enfoque organizado para cada tema—enfoques que pueden ser útiles cuando la respuesta no se vuelve rápidamente evidentes.

Preguntas de respuestas múltiples

Al igual que los simlets, las preguntas de opción múltiple pueden obligar al examinado a interpretar el significado de varios comandos show y debug. Las preguntas de opción múltiple podrían simplemente enumerar la salida de algunos comandos, junto con una figura, y le pedirá que identifique lo que sucedería. Por ejemplo, una pregunta de opción múltiple podría mostrar la tabla de direcciones mac show Comando dinámico que enumera las entradas de la tabla MAC aprendidas dinámicamente de un conmutador.

La pregunta puede requerir que prediga cómo ese interruptor reenviaría un marco enviado por un dispositivo, destinado a otro dispositivo.

Esto requeriría que aplicara los conceptos de Cambio de LAN a la salida que se muestra en el comando. Las preguntas de opción múltiple que enumeran la salida de los comandos show y debug requieren gran parte del mismo pensamiento que las preguntas de simlet. Al igual que con las preguntas de simlet, el primer paso para algunas preguntas de opción múltiple es pensar en lo que debería ocurrir normalmente en la red, en función de cualquier diagrama de red e información en la pregunta.

A continuación, compare la información del texto de la pregunta, incluida la salida del comando de muestra, para ver si confirma que la red funciona normalmente, o si hay un problema. (La red podría estar funcionando correctamente, y la pregunta está diseñada para confirmar que sabe por qué un comando en particular confirma que una parte particular de la red está funcionando bien).

La gran diferencia en este caso, sin embargo, es que las preguntas de opción múltiple no requieren que recuerdes los comandos usar. La salida del comando se proporciona en la pregunta o no.

Aprobar las preguntas con un proceso organizado de solución de problemas

Si la respuesta a una pregunta de simulación, simlet o de opción múltiple no es obvia después de usar el opciones más obvias y más rápidas que acabamos de discutir, necesita implementar un y proceso de pensamiento organizado. Este proceso más organizado bien puede ser lo que un típico haría un ingeniero de redes cuando se enfrentara a problemas más complejos del mundo real

Desafortunadamente, los exámenes están cronometrados y pensando en el problema con más detalle. requiere más tiempo.

Al pensar en el proceso de solución de problemas mientras se prepara para el examen, puede estar mejor preparados para atacar problemas en el examen. Con ese fin, este libro incluye

muchos procesos de solución de problemas sugeridos. Los procesos de solución de problemas no son fines hasta mismos, por lo que no necesita memorizarlos para los exámenes. Son una herramienta de aprendizaje, con el objetivo final de ayudarte a encontrar correcta y rápidamente las respuestas a las más preguntas desafiantes en los exámenes

Esta sección ofrece una descripción general de un proceso general de solución de problemas. A medida que avanzas A lo largo de este libro, el proceso se mencionará de vez en cuando en relación con otras áreas tecnológicas, como el enrutamiento IP. Los tres pasos principales en la organización de este libro proceso de solución de problemas son los siguientes:

- Paso 1 Análisis/predicción del funcionamiento normal: Prediga los detalles de lo que debería suceder si la red está funcionando correctamente, según la documentación, la configuración, y mostrar y depurar la salida del comando.
- Paso 2 Aislamiento del problema: determine qué tan lejos a lo largo de la ruta esperada trama/paquete va antes de que no se pueda reenviar más, de nuevo basado en la documentación, la configuración y la salida del comando show y debug.
- Paso 3 Análisis de causa raíz: identificar las causas subyacentes de los problemas identificadas en el paso anterior—específicamente, las causas que tienen una acción específica con la que se puede solucionar el problema

Seguir este proceso requiere una amplia variedad de habilidades aprendidas. Necesitas recordar la teoría de cómo deberían funcionar las redes, así como también cómo interpretar el resultado del comando show eso confirma cómo se comportan actualmente los dispositivos. Este proceso requiere el uso de herramientas de prueba, como ping y traceroute, para aislar el problema. Finalmente, este enfoque requiere la capacidad de pensar en términos generales acerca de todo lo que podría afectar a un solo componente.

Por ejemplo, imagine una LAN simple con dos conmutadores conectados entre sí y dos PC (PC1 y PC2), cada una conectada a uno de los conmutadores. Originalmente, PC1 podía hacer ping a PC2 con éxito, pero el ping ahora falla. Puede examinar la documentación, así como mostrar la salida del comando, para confirmar la topología de la red y predecir su funcionamiento normal comportamiento basado en su conocimiento de la conmutación de LAN.

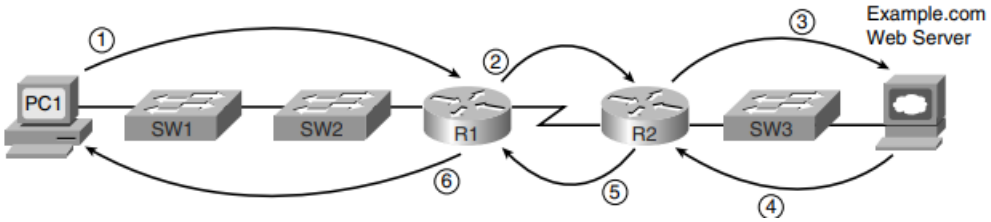
Como resultado, podría predecir dónde debe fluir una trama enviada por PC1 a PC2. Para aislar el problema, puede buscar en el cambie las tablas MAC para confirmar las interfaces a través de las cuales se debe reenviar la trama, posiblemente luego encuentre que la interfaz conectada a PC2 ha fallado. Sin embargo, sabiendo que la interfaz ha fallado no identifica la causa raíz del problema.

Entonces lo harías entonces necesita ampliar su pensamiento a todas y cada una de las razones por las que una interfaz puede fallar, desde un cable desenchufado, a interferencias eléctricas, a la seguridad del puerto desactivando la interfaz. Espectáculo Los comandos pueden confirmar que una causa raíz específica es el problema, o al menos dar algunas pistas sobre la causa raíz

Aislamiento de problemas en la capa 3 y luego en las capas 1 y 2

Antes de pasar a los temas específicos sobre la solución de problemas de LAN Ethernet, es útil considere el panorama general. Hoy en día, la mayoría de las soluciones de problemas en las redes IP reales comienzan con lo que el usuario final ve y experimenta. A partir de ahí, el análisis generalmente avanza rápidamente. a un examen de qué tan bien está funcionando la Capa 3. Por ejemplo, imagina que el usuario de PC1 en la Figura 10-1 generalmente puede conectarse al servidor web a la derecha ingresando www.example.com en el navegador web de PC1, pero la conexión al servidor web actualmente falla El usuario llama a la mesa de ayuda y el problema se asigna a un ingeniero de redes

Figure 10-1 *Layer 3 Problem Isolation*



Después de conocer el problema, el ingeniero puede trabajar para confirmar que PC1 puede resolver el nombre de host (www.example.com) en la dirección IP correcta. En ese punto, la capa 3 IP proceso de aislamiento del problema puede continuar, para determinar cuál de los seis pasos de enrutamiento se muestra en la figura ha fallado. Los pasos de enrutamiento que se muestran en la Figura 10-1 son los siguientes

- Paso 1 PC1 envía el paquete a su puerta de enlace predeterminada (R1) porque la IP de destino la dirección está en una subred diferente.
- Paso 2 R1 reenvía el paquete a R2 según la tabla de enrutamiento de R1.
- Paso 3 R2 reenvía el paquete al servidor web según la tabla de enrutamiento de R2.
- Paso 4 El servidor web envía un paquete de vuelta a la PC1 basado en la web configuración de la puerta de enlace predeterminada del servidor (R2).
- Paso 5 R2 reenvía el paquete destinado a PC1 reenviando el paquete a R1 según la tabla de enrutamiento de R2.
- Paso 6 R1 reenvía el paquete a PC1 según la tabla de enrutamiento de R1

El Capítulo 21, "Resolución de problemas de enrutamiento IP", examina este proceso con mucho más detalle. Por ahora, considere lo que sucede si el proceso de aislamiento de problemas de Capa 3 descubre que El paso 1, 3, 4 o 6 es el paso que falla. Aislar aún más el problema requeriría más Análisis de capa 3. Sin embargo, en algún momento, todos los problemas potenciales en la capa 3 podrían ser descartado, por lo que el siguiente paso de aislamiento del problema sería averiguar por qué las capas 1 y 2 los detalles en ese paso de enrutamiento no funcionan.

Por ejemplo, imagine que el análisis de la Capa 3 determinó que PC1 ni siquiera puede enviar un paquete a su puerta de enlace predeterminada (R1), lo que significa que el Paso 1 en la Figura 10-1 falla. para seguir aislar el problema y encontrar las causas raíz, el ingeniero tendría que determinar la siguiente:

• La dirección MAC de PC1 y de la interfaz LAN de R1

• Las interfaces de conmutador utilizadas en SW1 y SW2

• El estado de la interfaz de cada interfaz

• El comportamiento de reenvío esperado de una trama enviada por PC1 a R1 como la dirección MAC de destino

Al recopilar y analizar estos hechos, lo más probable es que el ingeniero pueda aislar el problema causa raíz y solucionarlo.

Resolución de problemas tal como se trata en este libro

Este libro tiene tres capítulos o secciones principales de solución de problemas, además de algunas secciones de solución de problemas intercaladas en otros capítulos. La cobertura principal es la siguiente:

- Capítulo 10, “Resolución de problemas del conmutador Ethernet”
- Capítulo 21, “Resoluciónón de problemas de enrutamiento IP”
- Capítulo 23, “Configuraciónón WAN”

Esencialmente, el Capítulo 21 cubre el análisis de problemas relacionados con la Capa 3, como generalmente se muestra en la Figura 10-1. Este capítulo cubre algunos de los detalles de cómo atacar los problemas como tan pronto como sepa que el problema puede estar relacionado con una LAN. El capítulo 23 cubre el paso de solución de problemas en los casos en que el problema podría estar relacionado con un enlace WAN

Estos tres capítulos de resolución de problemas dedican algo de tiempo a los aspectos más formales. Proceso de solución de problemas, sino como un medio para un fin, centrándose en la predicción normal comportamiento, aislar los problemas y determinar la causa raíz. El objetivo

final es ayudarte. conocer las herramientas, conceptos, comandos de configuración y cómo analizar una red basada en Mostrar comandos para resolver un problema.

Si tiene tanto este libro como la Guía de certificación oficial CCNA ICND2 640-816, el ICND2 El libro proporciona aún más detalles sobre la resolución de problemas y cómo utilizar un sistema más formalizado. proceso de solución de problemas, si es necesario. La razón para poner más detalles en el libro ICND2 es que para cuando llegue a los temas de resolución de problemas de ese libro, habrá completó todos los materiales de nivel CCNA para un área de tecnología en particular. Porque La solución de problemas requiere la interpretación de una amplia gama de conceptos, configuraciones y salida de comando, los capítulos/secciones de solución de problemas del libro ICND2 se encuentran al final de cada tema principal, resumiendo los materiales importantes y ayudando a mostrar cómo los temas están interrelacionados

El resto de este capítulo examina tres temas principales, cada uno de los cuales tiene algo que ver con al menos uno de los tres componentes principales del proceso de solución de problemas formalizado:

- Cisco Discovery Protocolo (CDP): se utiliza para confirmar la documentación y aprender sobre la topología de la red, para predecir el funcionamiento normal de la red.
- Examen del estado de la interfaz: las interfaces deben estar en un estado de funcionamiento antes de que un conmutador reenviar fotogramas en la interfaz. Debe determinar si una interfaz está funcionando, como, así como determinar las posibles causas raíz de una interfaz de conmutador fallida.
- Analizar dónde se reenviarán los marcos: debe saber cómo analizar una la tabla de direcciones MAC del switch y cómo predecir cómo un switch reenviará un marco particular

Verificación de la topología de red con Cisco Protocolo de descubrimiento

El Cisco Discovery Protocolo (CDP) patentado descubre información básica sobre enrutadores y conmutadores vecinos sin necesidad de conocer las contraseñas de los dispositivos vecinos. Para descubrir información los enrutadores y conmutadores envían mensajes CDP cada una de sus interfaces. Los mensajes esencialmente anuncian información sobre el dispositivo. que envió el mensaje CDP. Los dispositivos que admiten CDP aprenden información sobre otros al escuchando los anuncios enviados por otros dispositivos.

Desde una perspectiva de solución de problemas, CDP se puede utilizar para confirmar o corregir el problema. documentación que se muestra en un diagrama de red, o incluso descubrir los dispositivos e interfaces utilizado en una red. Confirmación de que la red está realmente cableada

para coincidir con la red diagrama es un buen paso a seguir antes de intentar predecir el flujo normal de datos en una red.

En los medios que admiten multidifusión en la capa de enlace de datos, CDP utiliza tramas de multidifusión; en otro multimedia, CDP envía una copia de la actualización de CDP a cualquier dirección de enlace de datos conocida. Así que cualquiera Dispositivo compatible con CDP que comparte un medio físico con otro dispositivo compatible con CDP puede aprender sobre el otro dispositivo.

CDP descubre varios detalles útiles de los dispositivos vecinos de Cisco:

- Identificador del dispositivo: por lo general, el nombre de host
- Lista de direcciones: direcciones de red y enlace de datos
- Interfaz local: la interfaz en el enrutador o conmutador que emite el comando show cdp con la que se descubrió al vecino
- Identificador de puerto: Texto que identifica el puerto utilizado por el dispositivo vecino para enviar Mensajes CDP al dispositivo local
- lista de capacidades: informaciónón sobre qué tipo de dispositivo es (por ejemplo, un enrutador o un cambiar)
- Plataforma: el modelo y el nivel de sistema operativo que se ejecuta en el dispositivo

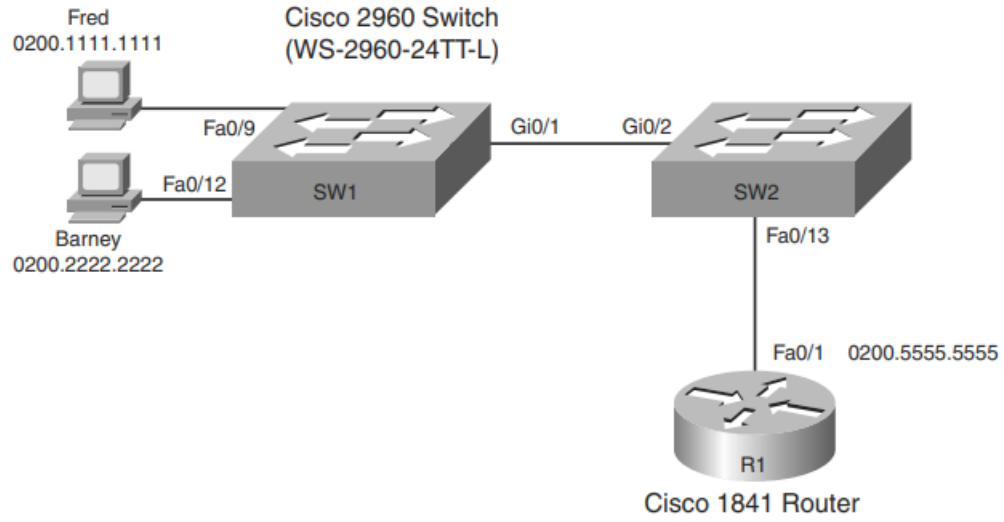
Command	Description
show cdp neighbors [*type number*]	Lists one summary line of information about each neighbor, or just the neighbor found on a specific interface if an interface was listed.
show cdp neighbors detail	Lists one large set (approximately 15 lines) of information, one set for every neighbor.
show cdp entry *name*	Lists the same information as the **show cdp neighbors detail** command, but only for the named neighbor (case-sensitive).

Al igual que muchas funciones de conmutadores y enrutadores que están habilitadas de forma predeterminada, CDP en realidad crea una exposición de seguridad cuando está habilitado. Para evitar la posibilidad de permitir que un atacante aprenda detalles sobre cada interruptor, CDP se puede desactivar fácilmente. Cisco recomienda que CDP sea deshabilitado en todas las interfaces que no tienen una necesidad específica para ello. Las interfaces más probables necesitan usar CDP son interfaces conectadas a otros enrutadores y conmutadores de Cisco y interfaces conectadas a teléfonos IP de Cisco. De lo contrario, CDP se puede deshabilitar por interfaz utilizando de interfaz no cdp enable. (El subcomando cdp enable interface vuelve a habilitar CDP). Alternativamente, el comando global no cdp run deshabilita CDP para todo el switch, con el comando cdp run global volviendo a habilitar CDP globalmente.

La figura 10-2 muestra una red pequeña con dos conmutadores, un enrutador y un par de PC.

El ejemplo 10-1 muestra los comandos show enumerados en la tabla 10-2, así como varios comandos que enumeran información sobre CDP en sí, en lugar de sobre dispositivos vecinos.

Figure 10-2 *Small Network Used in CDP Examples*



Example 10-1 **show cdp** *Command Examples: SW2*

```
SW2#show cdp ?
  entry      Information for specific neighbor entry
  interface  CDP interface status and configuration
  neighbors  CDP neighbor entries
  traffic    CDP statistics
  |          Output modifiers
  <cr>
! Next, the show cdp neighbors command lists SW2's local interface, and both R1's
! and SW1's interfaces  (in the "port" column), along with other details.
!
SW2#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID           Local Intrfce         Holdtme   Capability    Platform   Port ID
SW1                 Gig 0/2               173            S I      WS-C2960-2Gig 0/1
R1                  Fas 0/13              139          R S I      1841       Fas 0/1
SW2#show cdp neighbors detail
-------------------------
Device ID: SW1
Entry address(es):
Platform: cisco WS-C2960-24TT-L,  Capabilities: Switch IGMP
Interface: GigabitEthernet0/2,  Port ID (outgoing port): GigabitEthernet0/1
Holdtime : 167 sec
```

continues

Example 10-1 **show cdp** *Command Examples: SW2 (Continued)*

```
Version :
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(25)SEE2, RELEASE
  SOFTWARE (fc1)
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 28-Jul-06 11:57 by yenanh

advertisement version: 2
Protocol Hello:  OUI=0x00000C, Protocol ID=0x0112; payload len=27,
  value=00000000FFFFFFFF010221FF000
0000000000019E86A6F80FF0000
VTP Management Domain: 'fred'
Native VLAN: 1
Duplex: full
Management address(es):
! The info for router R1 follows.
-------------------------
Device ID: R1
Entry address(es):
  IP address: 10.1.1.1
Platform: Cisco 1841,  Capabilities: Router Switch IGMP
Interface: FastEthernet0/13,  Port ID (outgoing port): FastEthernet0/1
Holdtime : 131 sec

Version :
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(9)T, RELEASE
  SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 16-Jun-06 21:26 by prod_rel_team

advertisement version: 2
VTP Management Domain: ''
Duplex: full
Management address(es):
!
! Note that the show cdp entry R1 command repeats the same information shown in
! the show cdp neighbors detail command, but just for R1.
SW2#show cdp entry R1
-------------------------
Device ID: R1
Entry address(es):
  IP address: 10.1.1.1
Platform: Cisco 1841,  Capabilities: Router Switch IGMP
Interface: FastEthernet0/13,  Port ID (outgoing port): FastEthernet0/1
Holdtime : 176 sec
```

Example 10-1 show cdp *Command Examples: SW2 (Continued)*

```
Version :
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(9)T, RELEASE
  SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 16-Jun-06 21:26 by prod_rel_team

advertisement version: 2
VTP Management Domain: ''
Duplex: full
Management address(es):
SW2#show cdp
Global CDP information:
    Sending CDP packets every 60 seconds
    Sending a holdtime value of 180 seconds
    Sending CDPv2 advertisements is  enabled
SW2#show cdp interfaces
FastEthernet0/1 is administratively down, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
FastEthernet0/2 is administratively down, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
!
! Lines omitted for brevity
!
SW2#show cdp traffic
CDP counters :
    Total packets output: 54, Input: 49
    Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
    No memory: 0, Invalid packet: 0, Fragmented: 0
    CDP version 1 advertisements output: 0, Input: 0
    CDP version 2 advertisements output: 54, Input: 49
```

Un poco más de la primera mitad del ejemplo muestra una comparación de la salida de los tres comandos listados en la Tabla 10-2. El comando show cdp neighbors lista una línea por vecino, pero con muchos detalles clave como la interfaz del dispositivo local utilizada para conectarse a al vecino y la interfaz del dispositivo vecino (bajo el encabezado Puerto). Por ejemplo, El comando show cdp neighbors de SW2 muestra una entrada para SW1, con la interfaz local de SW2 de SW2 es GIO/2, y la interfaz de SW1 es GIO/1 (consulte la Figura 10-2 como referencia). La salida de show cdp neighbors también muestra la plataforma, por lo que si conoce la línea de productos Cisco hasta cierto punto, sabrá el modelo específico de SW1. Cisco, sabrá el modelo específico del router o switch vecino. Así, incluso usando esta información básica, puede construir una figura como la Figura 10-2 o confirmar que los detalles de la figura son correctos. los detalles de la figura son correctos

Tómese un momento para examinar la salida del comando show cdp neighbors detail y los comandos show cdp entre R1 en el Ejemplo 10-1. Ambos comandos proporcionan exactamente los mismos mensajes, con el primero suministrando la información para todos los vecinos, en lugar de

para un vecino a la vez. un vecino a la vez. Note que la salida de estos dos comandos lista detalles adicionales, como el nombre completo del modelo de switch (WS-2960-24TT-L) y la dirección IP configurada en el router 1841. (Si se hubiera configurado la dirección IP de SW1, también se mostraría). aparecido).

La parte inferior del Ejemplo 10-1 enumera la salida de muestra de algunos del show cdp comandos que identifican información sobre cómo funciona CDP. Estos comandos no enumeren cualquier información sobre los vecinos. La Tabla 10-3 enumera estos comandos y su propósito para referencia fácil

Table 10-3 *Commands Used to Verify CDP Operations*

Command	Description
show cdp	States whether CDP is enabled globally, and lists the default update and holdtime timers.
show cdp interface [*type number*]	States whether CDP is enabled on each interface, or a single interface if the interface is listed, and states update and holdtime timers on those interfaces.
show cdp traffic	Lists global statistics for the number of CDP advertisements sent and received.

Análisis del estado de la interfaz de capa 1 y 2

Una interfaz de switch de Cisco debe estar en un estado de funcionamiento antes de que el switch procese los marcos recibidos en la interfaz o enviar tramas fuera de la interfaz. Además, la interfaz podría estar en un estado de funcionamiento, pero es posible que sigan ocurriendo problemas intermitentes. Entonces, un poco El paso obvio de solución de problemas es examinar el estado de la interfaz, asegurarse de que cada interfaz esté funcionando, y también verifique que no ocurran problemas intermitentes. Esta sección examina los comandos show que puede usar para determinar el estado de cada interfaz, las razones por las cuales una interfaz podría no estar funcionando y algunos problemas que pueden ocurrir incluso cuando las interfaces están en un estado de trabajo.

Problemas comunes de la capa 1 en las interfaces de trabajo

Algunos problemas de la capa 1 impiden que una interfaz de conmutador llegue a la conexión (arriba/arriba) estado. Sin embargo, cuando la interfaz alcanza el estado de conexión, el conmutador intenta utilizar el interfaz y mantener varios contadores de interfaz. Estos contadores de interfaz pueden ayudar a identificar problemas que pueden ocurrir, aunque la interfaz esté en estado de conexión. Esta sección explica algunos de los conceptos relacionados y algunos de los problemas más comunes.

Primero, considere un par de razones comunes por las que las tramas de Ethernet experimentan errores durante transmisión. Cuando una trama Ethernet pasa por un cable UTP, la señal eléctrica puede encontrar problemas. El cable podría dañarse, por ejemplo, si se encuentra debajo de una alfombra. Si la silla del usuario sigue aplastando el cable, eventualmente la señal eléctrica puede

degradarse. Además, existen muchas fuentes de interferencia electromagnética (EMI); por ejemplo, un cable de alimentación eléctrica cercano puede causar EMI. EMI puede cambiar la señal eléctrica en el cable de ethernet

Capitulo 11

LAN inalámbricas

Hasta ahora, este libro ha dedicado mucha atención a las LAN Ethernet (con cable). Aunque ellos son de vital importancia, otro estilo de LAN, las LAN inalámbricas (WLAN), ocupa un lugar particularmente papel importante en el suministro de acceso a la red a los usuarios finales. En particular, las WLAN permiten que el usuario para comunicarse a través de la red sin necesidad de cables, lo que permite móviles dispositivos al tiempo que elimina el gasto y el esfuerzo involucrados en el tendido de cables. Este capítulo examina los conceptos básicos, estándares, instalación y opciones de seguridad para algunos de las tecnologías WLAN más comunes en la actualidad

Como recordatorio, si está siguiendo el plan de lectura opcional enumerado en la Introducción a este libro, pasará al Capítulo 1 de la Guía de certificación oficial CCNA ICND2 640-816 siguiendo este capítulo.

"¿Ya sé esto?" Prueba

prueba le permite evaluar si debe leer el capítulo completo. Si no falla más de una de estas nueve preguntas de autoevaluación, usted Es posible que desee pasar a la sección "Tareas de preparación para el examen". La Tabla 11-1 enumera los los encabezados principales de este capítulo y la sección "¿Ya lo sé?" preguntas del examen que cubren el material en esas secciones. Esto le ayuda a evaluar su conocimiento de estas áreas específicas. Las respuestas a "¿Ya lo sé?" cuestionario aparecen en el Apéndice A.

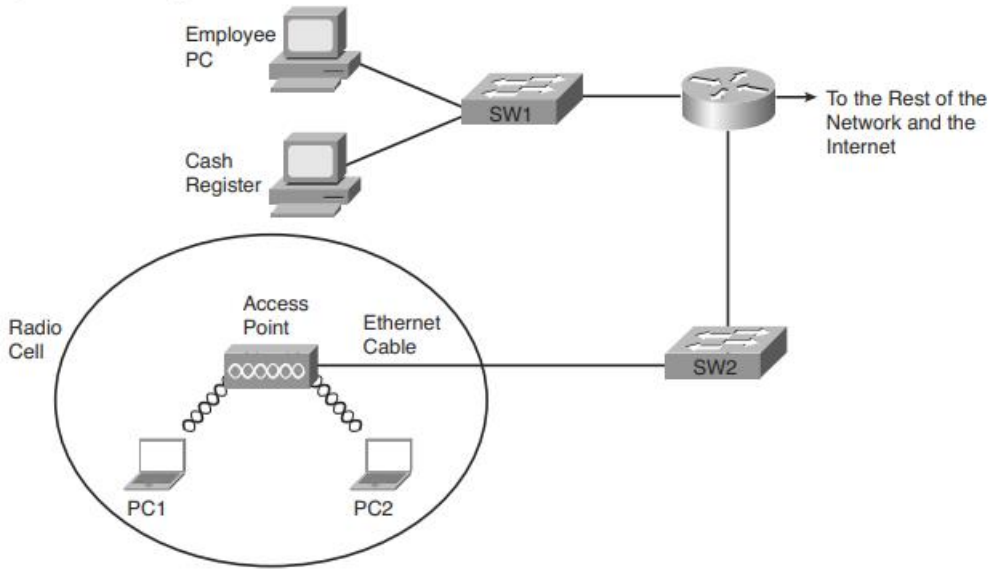
Temas de la Fundación

Este capítulo examina los conceptos básicos de las WLAN. En particular, la primera sección introduce los conceptos, protocolos y estándares utilizados por muchos de los WLAN más comunes instalaciones hoy. A continuación, el capítulo examina algunos pasos básicos de instalación. el ultimo mayor sección analiza la seguridad WLAN, que es particularmente importante porque las señales WLAN son mucho más susceptibles de ser interceptados por un atacante que las LAN Ethernet.

Conceptos de LAN inalámbrica

Mucha gente usa WLAN regularmente hoy en día. Las ventas de PC continúan con una tendencia hacia más ventas de computadoras portátiles versus computadoras de escritorio, en parte para respaldar una fuerza laboral más móvil. ordenador personal los usuarios necesitan conectarse a cualquier red que estén cerca, ya sea en el trabajo, en casa, en un hotel, o en una cafetería o librería. Y la proliferación de tabletas y otros dispositivos que todos se conectan a través de WLAN, todos conspiran para impulsar el crecimiento de las WLAN en la actualidad. Para, Por ejemplo, la figura 11-1 muestra el diseño de una LAN en una librería minorista. La librería proporciona acceso gratuito a Internet a través de WLAN y también admite los dispositivos de la librería a través de una LAN cableada.

Figure 11-1 *Sample WLAN at a Bookstore*



Las computadoras portátiles de los clientes con capacidad inalámbrica se comunican con un dispositivo WLAN llamado acceso punto (AP). El AP utiliza comunicaciones inalámbricas para enviar y recibir tramas con el Clientes WLAN (los portátiles). El AP también se conecta a la misma LAN Ethernet que los propios dispositivos de la librería, lo que permite tanto a los clientes como a los empleados comunicarse con otros sitios.

Esta sección comienza el capítulo explicando los conceptos básicos de las WLAN, comenzando con una comparación de similitudes entre Ethernet LAN y WLAN. El resto de la sección luego explora algunas de las principales diferencias.

Comparaciones con LAN Ethernet

Las WLAN son similares a las LAN Ethernet en muchos aspectos, el más importante es que Las WLAN permiten que se produzcan comunicaciones entre dispositivos. El IEEE define estándares para ambos, utilizando la familia IEEE 802.3 para LAN Ethernet y la familia 802.11 para WLAN.

Ambos estándares definen un formato de marco con un encabezado y un tráiler, con el encabezado que incluye un campo de dirección MAC de origen y de destino, cada uno de 6 bytes

de longitud. Ambos definen reglas acerca de cómo los dispositivos deben determinar cuándo deben enviar marcos y cuándo no debe

La mayor diferencia entre los dos radica en el hecho de que las WLAN usan energía radiada ondas, generalmente llamadas ondas de radio, para transmitir datos, mientras que Ethernet utiliza señales que fluyen a través de un cable (o luz en un cableado óptico). Las ondas de radio atraviesan el espacio, así que técnicamente no hay necesidad de ningún medio de transmisión física. De hecho, la presencia de materia, en particular, paredes, objetos metálicos y otras obstrucciones, se interpone en el camino de las señales de radio inalámbricas

También existen varias otras diferencias, principalmente como un efecto secundario del uso de la conexión inalámbrica en lugar de de alambres, Por ejemplo, el Capítulo 7, "Conceptos de conmutación LAN Ethernet", explica cómo Ethernet puede admitir comunicación full-duplex (FDX) si un conmutador se conecta a un solo dispositivo. Esto elimina la necesidad de controlar el acceso al enlace utilizando la detección de portadora múltiple. detección de colisión de acceso (CSMA/CD). Con inalámbrico, si más de un dispositivo a la vez envía ondas de radio en el mismo espacio a la misma frecuencia, ninguna señal es inteligible, por lo que se debe utilizar un mecanismo semidúplex (HDX). Para arbitrar el uso de la frecuencia, las WLAN utilizan el algoritmo de detección de portadora de acceso múltiple con prevención de colisiones (CSMA/CA) para aplicar la lógica HDX y evitar tantas colisiones como sea posible.

Estándares de LAN inalámbrica

El IEEE define los estándares LAN como parte del comité 802.11. Esta sección enumera los detalles básicos de cada uno de los cuatro estándares WLAN 802.11 diferentes: 802.11a, 802.11b, 802.11g y 802.11n. Cuatro organizaciones tienen un gran impacto en los estándares utilizados para las LAN inalámbricas hoy. La Tabla 11-2 enumera estas organizaciones y describe sus roles.

Table 11-2 *Organizations That Set or Influence WLAN Standards*

Organization	Standardization Role
ITU-R	Worldwide standardization of communications that use radiated energy, particularly managing the assignment of frequencies
IEEE	Standardization of wireless LANs (802.11)
Wi-Fi Alliance	An industry consortium that encourages interoperability of products that implement WLAN standards through their Wi-Fi certified program
Federal Communications Commission (FCC)	The U.S. government agency that regulates the usage of various communications frequencies in the U.S.

De las organizaciones enumeradas en esta tabla, el IEEE desarrolla los estándares específicos para los diferentes tipos de WLAN que se utilizan en la actualidad. Estas normas deben tener en cuenta las elecciones de frecuencia hechas por las diferentes agencias reguladoras a nivel mundial, tales como la FCC en los EE. UU. y el ITU-R, que en última instancia está controlado por los Estados Unidos Naciones (ONU)

El IEEE introdujo los estándares WLAN con la creación de la ratificación de 1997 de la estándar 802.11. Este estándar original no tenía una letra de sufijo, mientras que WLAN posterior las normas lo hacen. Esta lógica de denominación, sin letra de sufijo en el primer estándar, seguida de otros estándares con una letra de sufijo, es como el estándar Ethernet IEEE original. Ese estándar era 802.3, con estándares posteriores más avanzados que tienen un sufijo, como 802.3u para Fast Ethernet.

El estándar 802.11 original ha sido reemplazado por estándares más avanzados. Con el fin de ratificación, los estándares son 802.11b, 802.11a, 802.11g y 802.11n. Tabla 11-3 listas algunos puntos clave sobre las normas actualmente ratificadas.

Table 11-3 *WLAN Standards*

Key Topic

Feature	802.11a	802.11b	802.11g	802.11n
Year ratified	1999	1999	2003	2009
Maximum speed using DSSS	—	11 Mbps	11 Mbps	—
Maximum speed using OFDM	54 Mbps	—	54 Mbps	150 Mbps
Frequency band	5 GHz	2.4 GHz	2.4 GHz	Both
Non-overlapping Channels	23	3	3	9*

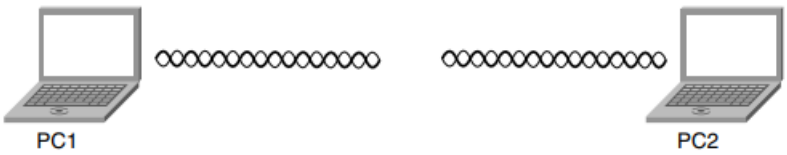
*Assumes 40 MHz channels

Esta tabla enumera un par de funciones que aún no se han definido pero que se describen más adelante.

en este capítulo. Modos de LAN inalámbrica 802.11

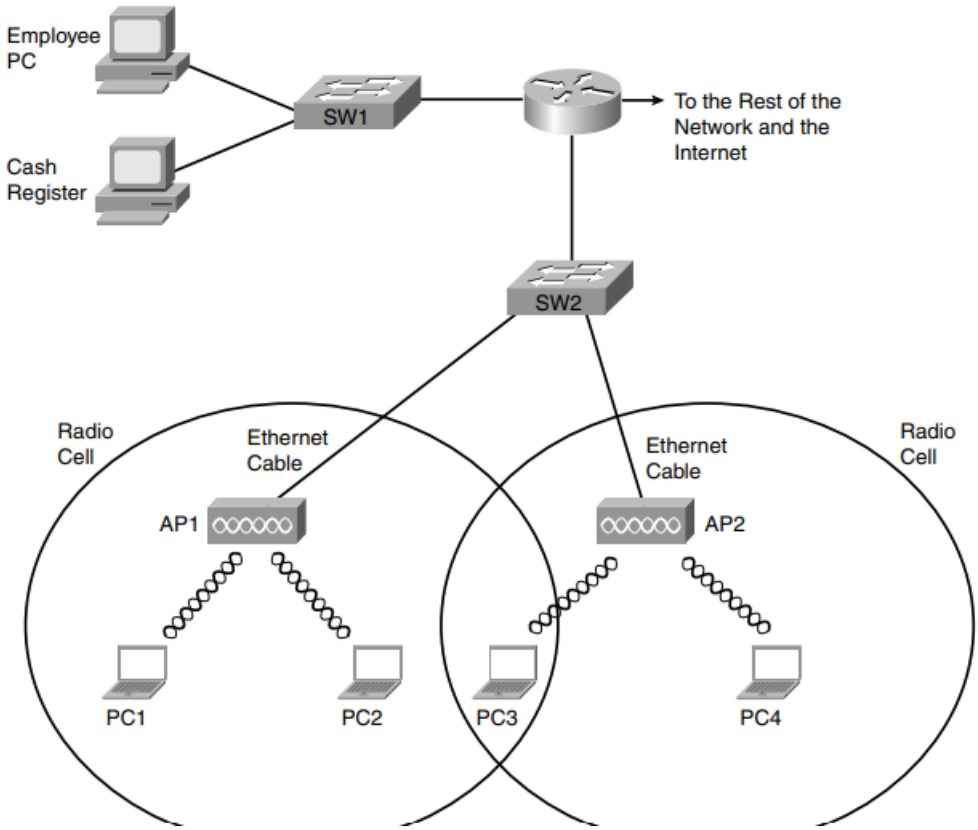
Las WLAN pueden usar uno de dos modos: modo ad hoc o modo de infraestructura. con ad-hoc modo, un dispositivo inalámbrico quiere comunicarse solo con uno o algunos otros dispositivos directamente, generalmente por un corto período de tiempo. En estos casos, los dispositivos envían tramas WLAN directamente entre sí, como se muestra en la Figura 11-2.

Figure 11-2 *Ad Hoc WLAN*



En el modo de infraestructura, cada dispositivo se comunica con un AP, y el AP se conecta a través de Ethernet cableada al resto de la infraestructura de la red. El modo de infraestructura permite que el Dispositivos WLAN para comunicarse con servidores e Internet en una red cableada existente, como se muestra anteriormente en la Figura 11-1

El modo de infraestructura admite dos conjuntos de servicios, denominados conjuntos de servicios. El primero, llamado Conjunto de servicios básicos (BSS), utiliza un solo AP para crear la LAN inalámbrica, como se muestra en Figura 11-1. El otro, llamado conjunto de servicios extendidos (ESS), utiliza más de un AP, a menudo con celdas superpuestas para permitir la itinerancia en un área más grande, como se muestra en la Figura 11-3.



Las ESS WLAN permiten el roaming, lo que significa que los usuarios pueden moverse dentro del área de cobertura y permanecer conectado a la misma WLAN. Como resultado, el usuario no necesita cambiar direcciones IP. Todo lo que el dispositivo tiene que hacer es detectar cuando las señales de radio del los AP actuales se están debilitando; encontrar un AP nuevo y mejor con una señal más fuerte o mejor; y empieza a usar el nuevo AP

Table 11-4 *Different WLAN Modes and Names*

Key Topic

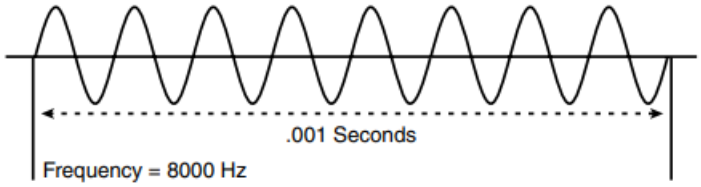
Mode	Service Set Name	Description
Ad hoc	Independent Basic Service Set (IBSS)	Allows two devices to communicate directly. No AP is needed.
Infrastructure (one AP)	Basic Service Set (BSS)	A single wireless LAN created with an AP and all devices that associate with that AP.
Infrastructure (more than one AP)	Extended Service Set (ESS)	Multiple APs create one wireless LAN, allowing roaming and a larger coverage area.

Transmisiones inalámbricas (capa 1)

Las WLAN transmiten datos en la Capa 1 enviando y recibiendo ondas de radio. La WLAN las tarjetas de interfaz de red (NIC), los puntos de acceso y otros dispositivos WLAN utilizan una radio y su antena para enviar y recibir las ondas de radio, haciendo pequeños cambios en las ondas para codificar datos. Aunque los detalles difieren significativamente en comparación con Ethernet, la idea de codificar datos cambiando la señal de energía que fluye a través de un medio es la misma idea que Ethernet codificación Al igual que la electricidad en cables de cobre y la luz en cables ópticos, las ondas de radio WLAN tienen una señal repetitiva que se puede graficar con el tiempo, como se muestra en la figura 11-4.

Cuando graficada, la curva muestra una forma de onda periódica repetitiva, con una frecuencia (el número de veces que la forma de onda se repite por segundo), amplitud (la altura de la forma de onda, que representa la fuerza de la señal) y la fase (el punto particular en la forma de onda repetitiva). De estos ítems, la frecuencia, medida en hercios (Hz), es el más importante en las discusiones de WLAN

Figure 11-4 *Graph of an 8-KHz Signal*



Muchos dispositivos electrónicos irradian energía a distintas frecuencias, algunas relacionadas con el funcionamiento del dispositivo. (por ejemplo, una LAN inalámbrica o un teléfono inalámbrico). En otros casos, la radiación la energía es un efecto secundario. Por ejemplo, los televisores emiten algo de energía radiada. Para prevenir

la energía radiada por un dispositivo de interrupción con otros dispositivos, el gobierno nacional agencias, regulan y supervisan los rangos de frecuencia que se pueden utilizar dentro de ese país. Por ejemplo, la Comisión Federal de Comunicaciones (FCC) de los EE. UU. regula el espectro electromagnético de frecuencias.

La FCC u otras agencias reguladoras nacionales especifican algunos rangos de frecuencias, llamados bandas de frecuencia. Por ejemplo, en los EE. UU., las estaciones de radio FM y AM deben registrarse con la FCC para usar un rango particular (banda) de frecuencias. Una emisora de radio accede a transmitir su señal de radio en o por debajo de un nivel de potencia particular para que otras estaciones de radio en otros las ciudades pueden usar la misma banda de frecuencia. Sin

embargo, sólo esa estación de radio puede usar una banda de frecuencia particular en una ubicación particular

Una banda de frecuencia se llama así porque en realidad es un rango de frecuencias consecutivas. Una La estación de radio FM necesita alrededor de 200 kilohercios (KHz) de frecuencia para enviar una señal de radio. señal. Cuando la estación solicita una frecuencia de la FCC, la FCC asigna una base frecuencia, con 100 KHz de ancho de banda a ambos lados de la frecuencia base. Por ejemplo, una estación de radio FM que anuncia algo como "Los grandes éxitos están en 96.5 FM" significa que la señal base es de 96,5 megahercios (MHz), con el transmisor de radio utilizando la frecuencia banda entre 96,4 MHz y 96,6 MHz, para un ancho de banda total de 0,2 MHz, o 200 KHz

Cuanto más amplio sea el rango de frecuencias en una banda de frecuencia, mayor será la cantidad de información que se puede enviar en esa banda de frecuencia. Por ejemplo, una señal de radio necesita aproximadamente 200 KHz (0,2 MHz) de ancho de banda, mientras que una señal de transmisión de TV, que contiene mucha más información debido al contenido de video, requiere aproximadamente 4.5 MHz

La FCC y las agencias equivalentes en otros países otorgan licencias para algunas bandas de frecuencia, dejando algunas bandas de frecuencia sin licencia. Las bandas con licencia se utilizan para muchos propósitos; el más comunes son la radio AM y FM, la radio de ultra alta frecuencia (UHF) (por ejemplo, para comunicaciones del departamento de policía) y teléfonos móviles.

Las frecuencias sin licencia pueden ser utilizado por todo tipo de dispositivos; sin embargo, los dispositivos aún deben cumplir con las reglas establecidas por la agencia reguladora.

En particular, un dispositivo que usa una banda sin licencia debe usar energía niveles en o por debajo de un ajuste particular. De lo contrario, el dispositivo podría interferir demasiado con otros dispositivos que comparten esa banda sin licencia. Por ejemplo, sucede que los hornos de microondas irradian energía en la banda sin licencia de 2,4 gigahercios (GHz) como efecto secundario de cocinar alimentos. Esa misma banda sin licencia es utilizada por algunos estándares de WLAN y por muchos inalámbricos. teléfonos En algunos casos, no puede escuchar a alguien en el teléfono o navegar por Internet usando una WLAN cuando alguien está calentando la cena

La FCC define tres bandas de frecuencia sin licencia. Las bandas están referenciadas por una frecuencia particular en la banda, aunque por definición, una banda de frecuencia es un rango de frecuencias La Tabla 11-5 enumera las bandas de frecuencia que importan hasta cierto punto para WLAN comunicaciones

Table 11-5 *FCC Unlicensed Frequency Bands of Interest*

Frequency Range	Name	Sample Devices
900 MHz	Industrial, Scientific, Medical (ISM)	Older cordless telephones
2.4 GHz	ISM	Newer cordless phones and 802.11, 802.11b, 802.11g, 802.11n WLANs
5 GHz	Unlicensed National Information Infrastructure (U-NII)	Newer cordless phones and 802.11a, 802.11n WLANs

Codificación inalámbrica y canales DSSS no superpuestos

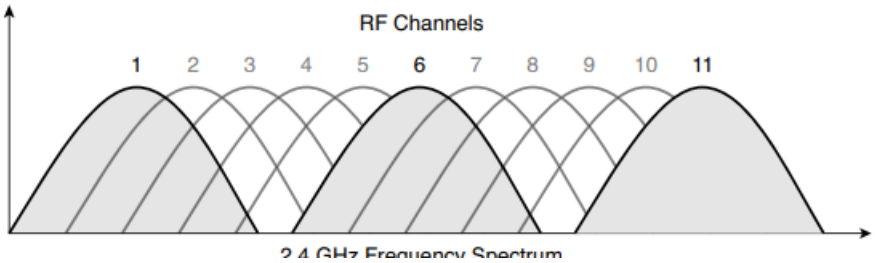
Cuando un NIC o AP WLAN envía datos, puede modular (cambiar) la señal de radio. frecuencia, amplitud y fase para codificar un 0 o 1 binario. Los detalles de esa codificación son más allá del alcance de este libro. Sin embargo, es importante conocer los nombres de tres generales clases de codificación, en parte porque el tipo de codificación requiere cierta planificación y previsión para algunas WLAN

El espectro ensanchado por salto de frecuencia (FHSS) utiliza todas las frecuencias de la banda, saltando a diferentes. Mediante el uso de frecuencias ligeramente diferentes para transmisiones consecutivas, con suerte, un dispositivo puede evitar la interferencia de otros dispositivos que usan la misma banda sin licencia, logrando enviar datos en algunas frecuencias. El 802.11 original Los estándares WLAN usaban FHSS, pero los estándares actuales (802.11a, 802.11b y 802.11g) no

Direct Sequence Spread Spectrum (DSSS) siguió como la siguiente clase general de codificación tipo para WLAN. Diseñado para usar en la banda sin licencia de 2,4 GHz, DSSS usa uno de varios canales o frecuencias independientes. Esta banda tiene un ancho de banda de 82 MHz, con un rango de 2.402 GHz a 2.483 GHz. Según lo regulado por la FCC, esta banda puede tener 11 diferentes canales DSSS superpuestos, como se muestra en la Figura 11-5

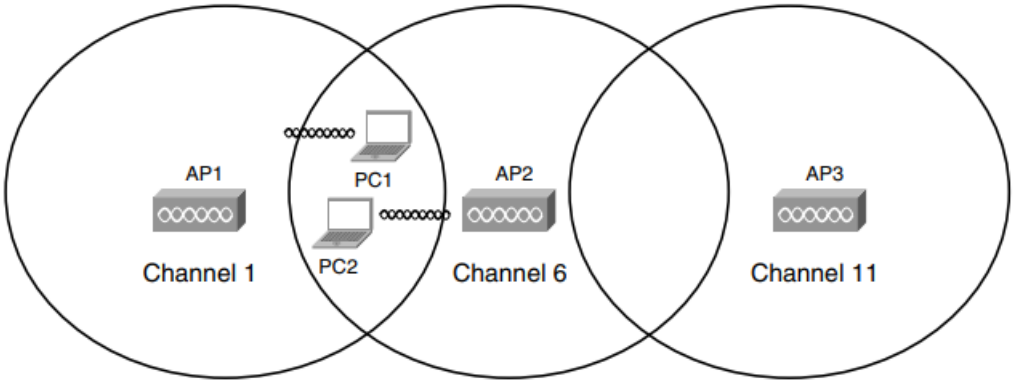
Aunque muchos de los canales que se muestran en la figura se superponen, tres de los canales (el canal en el extremo izquierdo y extremo derecho, y el canal en el centro) no se superponen, por lo que no se impacten entre sí. Estos canales (canales 1, 6 y 11) se pueden utilizar en el mismo espacio para las comunicaciones WLAN y no interferirán entre sí.

Figure 11-5 *Eleven Overlapping DSSS Channels at 2.4 GHz*



La importancia de los canales DSSS que no se superponen es que cuando diseña un ESS WLAN (más de un AP), los AP con áreas de cobertura superpuestas deben configurarse para usar diferentes canales que no se superponen. La figura 11-6 muestra la idea

Figure 11-6 *Using Nonoverlapping DSSS 2.4-GHz Channels in an ESS WLAN*



En este diseño, los dispositivos en un BSS (dispositivos que se comunican a través de un AP) pueden enviar al mismo tiempo que los otros dos BSS y no interfieren entre sí, porque cada uno usa las frecuencias ligeramente diferentes de los canales que no se superponen. Por ejemplo, PC1 y PC2 podría sentarse uno al lado del otro y comunicarse con dos puntos de acceso diferentes usando dos diferentes canales al mismo tiempo. Este diseño es típico de las WLAN 802.11b, con cada celda funcionando a una velocidad de datos máxima de 11 Mbps. Con los canales no superpuestos, cada BSS semidúplex puede ejecutarse a 11 Mbps, para un ancho de banda acumulativo de 33 Mbps en este caso. Este ancho de banda acumulativo se denomina capacidad de la WLAN.

La última de las tres categorías de codificación para WLAN se denomina frecuencia ortogonal. Multiplexación por división (OFDM). Al igual que DSSS, las WLAN que usan OFDM pueden usar múltiples canales no superpuestos. La Tabla 11-6 resume los puntos clave y los nombres de las principales tres opciones de codificación.

Table 11-6 *Encoding Classes and IEEE Standard WLANs*

Name of Encoding Class	What It Is Used By
Frequency Hopping Spread Spectrum (FHSS)	802.11
Direct Sequence Spread Spectrum (DSSS)	802.11b, 802.11g
Orthogonal Frequency Division Multiplexing (OFDM)	802.11a, 802.11g, and 802.11n

La última de las tres categorías de codificación para WLAN se denomina frecuencia ortogonal.

Multiplexación por división (OFDM). Al igual que DSSS, las WLAN que usan OFDM pueden usar múltiples canales no superpuestos. La Tabla 11-6 resume los puntos clave y los nombres de las principales tres opciones de codificación.

Área de cobertura, velocidad y capacidad

Un área de cobertura WLAN es el espacio en el que dos dispositivos WLAN pueden enviar con éxito datos. El área de cobertura creada por un AP en particular depende de muchos factores, varios de los cuales que se explican en esta sección.

Primero, la potencia de transmisión por un AP o NIC WLAN no puede exceder un nivel particular basado en las regulaciones de las agencias reguladoras como la FCC. La FCC limita la transmisión poder para garantizar la equidad en las bandas sin licencia. Por ejemplo, si dos vecinos compraron AP de Linksys y colóquelos en sus hogares para crear una WLAN, los productos se ajustarían

a las regulaciones de la FCC. Sin embargo, si una persona comprara e instalar antenas de alta ganancia para su AP, y excedió en gran medida las regulaciones de la FCC, podría obtener un área de cobertura mucho más amplia: tal vez incluso en todo el vecindario. Sin embargo, podría impedir que la otra persona AP no funcione en absoluto debido a la interferencia del AP dominado.

Los materiales y las ubicaciones de los materiales cerca del AP también afectan el área de cobertura de un AP. Por ejemplo, colocar el AP cerca de un gran archivador de metal aumenta los reflejos y dispersión, que reduce el área de cobertura. Ciertamente, la construcción de hormigón con varillas de acero reduce el área de cobertura en un típico edificio de oficinas moderno. De hecho, cuando un edificio El diseño significa que se producirán interferencias en algunas áreas, los AP pueden usar diferentes tipos de antenas que cambian la forma del área de cobertura de un círculo a alguna otra forma.

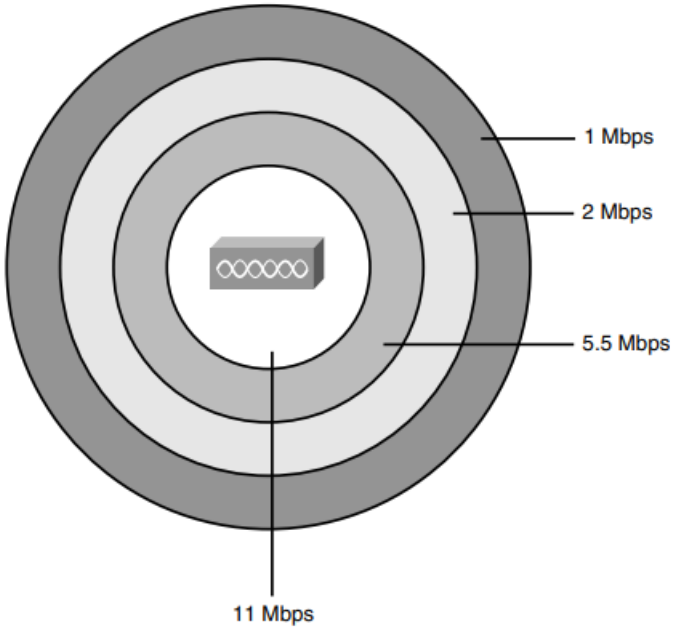
Resulta que las señales inalámbricas más débiles no pueden pasar datos a velocidades más altas, pero pueden pasar datos a velocidades más bajas. Por lo tanto, los estándares de WLAN admiten la idea de múltiples velocidades. Un dispositivo cerca del AP puede tener una señal fuerte, por lo que puede transmitir y recibir datos con el AP en tasas más altas. Un dispositivo en el borde del área de cobertura, donde las señales son débiles, aún puede poder enviar y recibir datos, aunque a una velocidad más lenta. La figura 11-7 muestra la idea de un área de cobertura, con velocidades variables, para un BSS IEEE 802.11b.

Las principales formas de aumentar el tamaño del área de cobertura de un AP son mediante el uso de antenas y aumentar la potencia de la señal transmitida. Por ejemplo, puede aumentar la ganancia de la antena, que es la potencia añadida a la señal de radio por la antena. Para duplicar el área de cobertura, la ganancia de la antena debe incrementarse para cuadriplicar la ganancia original. A pesar de esto es útil, la potencia de salida (EIRP) aún debe estar dentro de las reglas de la FCC (en los EE. UU.).

El tamaño real del área de cobertura depende de una gran cantidad de factores que están más allá el alcance de este libro. Algunos de los factores incluyen la banda de frecuencia utilizada por el estándar WLAN, las obstrucciones entre y cerca de los dispositivos WLAN, la interferencia de otras fuentes de energía de RF, las antenas utilizadas tanto en los clientes como en los puntos de acceso, y las opciones utilizadas por DSSS y OFDM al codificar datos por aire. Generalmente hablando

Estándares de WLAN que usan frecuencias más altas (estándares de banda U-NII 802.11a y 802.11n) puede enviar datos más rápido, pero con el precio de áreas de cobertura más pequeñas. Sin embargo, tenga en cuenta que El 802.11n más nuevo afirma admitir un área de cobertura más amplia que todos los estándares anteriores. A cubrir todo el espacio requerido, un ESS que usa frecuencias más altas requeriría más Puntos de acceso, lo que aumenta el costo de la implementación de WLAN

Figure 11-7 *Coverage Area and Speed*



La Tabla 11-7 enumera los principales estándares IEEE WLAN que habían sido ratificados en el momento en que este libro fue publicado, la velocidad máxima y el número de canales no superpuestos.

Table 11-7 *WLAN Speed and Frequency Reference*

IEEE Standard	Max Stream Data Rate (Mbps)	Frequency	Nonoverlapping Channels
802.11b	11	2.4 GHz	3
802.11a	54	5 GHz	23
802.11g	54	2.4 GHz	3
802.11n	72.2	5 GHz	21
802.11n*	150	5 GHz	9

Acceso a los medios (capa 2)

Las LAN Ethernet comenzaron su vida utilizando un medio compartido (un cable coaxial), lo que significa que solo un dispositivo podría enviar datos a la vez. Para controlar el acceso a este medio semidúplex (HDX), Ethernet definió el uso del algoritmo CSMA/CD. A medida que Ethernet avanzaba con estándares continuamente mejorados, comenzó a usar interruptores, con un dispositivo cableado a cada switch port, permitiendo el uso de full dúplex (FDX). Con FDX, no pueden ocurrir colisiones, por lo que el algoritmo CSMA/CD está deshabilitado.

La solución al problema de acceso a los medios con las WLAN es utilizar la detección múltiple de la portadora. Algoritmo de acceso con prevención de colisiones (CSMA/CA). La parte de prevención de colisiones minimiza la posibilidad estadística de que se produzcan colisiones.

Sin embargo, CSMA/CA no prevenir colisiones, por lo que los estándares WLAN deben tener un proceso para tratar las colisiones cuando ocurren. Porque el dispositivo de envío no puede saber si su trama transmitida colisionó con otro cuadro, todos los estándares requieren un reconocimiento de cada cuadro. Cada dispositivo WLAN escucha el reconocimiento, que debe ocurrir inmediatamente después de la se envía el marco. Si no se recibe acuse de recibo, el dispositivo emisor asume que la trama se perdió o colisionó, y vuelve a enviar el marco.

La siguiente lista resume los puntos clave sobre el algoritmo CSMA/CA, omitiendo algunos de los detalles en aras de la claridad:

- Paso 1 Escuche para asegurarse de que el medio (espacio) no esté ocupado (actualmente no hay ondas de radio). siendo recibido en las frecuencias a ser utilizadas).
- Paso 2 Establezca un temporizador de espera aleatorio antes de enviar un marco para reducir estadísticamente la posibilidad de que todos los dispositivos intenten enviar al mismo tiempo.
- Paso 3 Cuando haya pasado el temporizador aleatorio, vuelva a escuchar para asegurarse de que el medio no está ocupado. Si no es así, envíe el marco. ptg6885603 Implementación de WLAN 321
- Paso 4 Después de que se haya enviado la trama completa, espere un reconocimiento.
- Paso 5 Si no se recibe confirmación, vuelva a enviar la trama mediante CSMA/CA lógica esperar el momento adecuado para enviar de nuevo. Esto concluye la breve introducción

a los conceptos de LAN inalámbrica. A continuación, este capítulo cubre los conceptos básicos de lo que debe hacer al instalar una nueva LAN inalámbrica.

Lista de verificación de implementación de LAN inalámbrica

La siguiente lista de verificación básica puede ayudar a guiar la instalación de una nueva WLAN BSS:

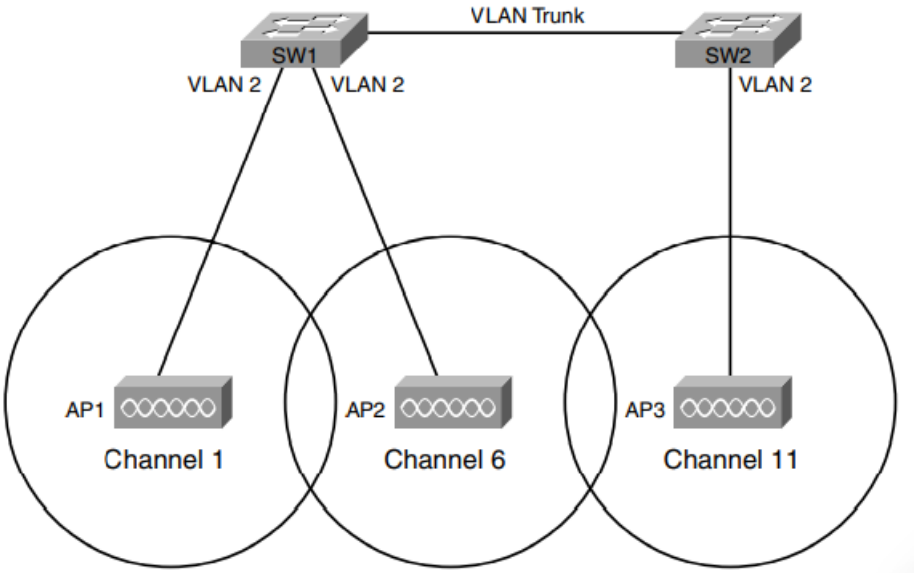
- Paso 1 Verifique que la red cableada existente funcione, incluidos los servicios DHCP, VLAN, y conectividad a Internet.
- Paso 2 Instale el AP y configure/verifique su conectividad a la red cableada, incluyendo la dirección IP, la máscara y la puerta de enlace predeterminada del AP.
- Paso 3 Configure y verifique la configuración inalámbrica del AP, incluido el conjunto de servicios Identificador (SSID), pero sin seguridad.
- Paso 4 Instale y configure un cliente inalámbrico (por ejemplo, una computadora portátil), nuevamente sin seguridad
- Paso 5 Verifique que la WLAN funcione desde la computadora portátil.
- Paso 6 Configure la seguridad inalámbrica en el AP y el cliente.
- Paso 7 Verifique que la WLAN funcione nuevamente, en presencia de la seguridad características.

Paso 1: verificar la red cableada existente

La mayoría de los otros capítulos de este libro explican los detalles de cómo entender, planificar, diseñar e implementar los conmutadores y enrutadores que crean el resto de la red, de modo que No es necesario repetir esos detalles aquí. Sin embargo, puede ser útil considerar un par de elementos relacionados con la prueba de una red cableada existente antes de conectar una nueva WLAN.

En primer lugar, el puerto del conmutador Ethernet al que se conecta el puerto Ethernet del punto de acceso suele ser un cambiar el puerto de acceso, lo que significa que está asignado a una VLAN en particular. Además, en un ESS diseño con varios puntos de acceso, todos los puertos del conmutador Ethernet a los que se conectan los puntos de acceso deben estar en la misma VLAN. La Figura 11-8 muestra un diseño ESS típico para una WLAN, con la VLAN identificaciones enumeradas.

Figure 11-8 *ESS WLAN with All APs in Ethernet VLAN 2*



Para probar la red existente, simplemente puede conectar una NIC Ethernet de una computadora portátil a la misma Cable Ethernet que se usará para el AP. Si la computadora portátil puede adquirir una dirección IP, máscara, y otra información usando DHCP, y comunicarse con otros hosts, el cable existente la red está lista para aceptar el AP.

Paso 2: Instale y configure los detalles IP y cableados del AP

Al igual que un conmutador Ethernet, los puntos de acceso inalámbricos funcionan en la capa 2 y no necesitan una dirección IP para realizar sus funciones principales.

Sin embargo, al igual que un conmutador Ethernet en una empresa La red debe tener una dirección IP para que pueda administrarse fácilmente, los AP implementados en una La red empresarial también debe tener una dirección IP. Los detalles de configuración de IP en un AP son los mismos elementos que se necesitan en un conmutador Ethernet, como cubierto en la sección "Configuración de la dirección IP del conmutador" en el Capítulo 9, "Conmutador Ethernet Configuración." En particular, el AP necesita una dirección IP, máscara de subred, puerta de enlace predeterminada Dirección IP y posiblemente la dirección IP de un servidor DNS.

El AP utiliza un cable Ethernet directo para conectarse al conmutador LAN. Aunque cualquiera La interfaz Speed Ethernet funciona, cuando se usan velocidades WLAN más rápidas, usando un Fast Ethernet La interfaz en un conmutador ayuda a mejorar el rendimiento general.

Paso 3: Configure los detalles de WLAN del AP

La mayoría de las veces, los puntos de acceso WLAN se pueden instalar sin configuración y funcionan. Para Por ejemplo, muchos hogares tienen puntos de acceso inalámbricos para consumidores instalados, conectados a una conexión a Internet de alta velocidad. A menudo, el AP, el enrutador y la conexión por cable terminan en el mismo dispositivo, como el enrutador de banda ancha inalámbrico A+G de doble banda de Linksys. (Linksys es una división de Cisco Systems que fabrica y distribuye dispositivos de redes de consumo).

Muchas personas simplemente compran estos dispositivos, conectan la alimentación y los cables apropiados para el cableado parte de la conexión, y deje la configuración predeterminada de WLAN, y el AP funciona.

Paso 4: Instale y configure un cliente inalámbrico

Un cliente inalámbrico es cualquier dispositivo inalámbrico que se asocia con un AP para usar una WLAN. Ser un cliente WLAN, el dispositivo simplemente necesita una NIC WLAN que admita la misma WLAN estándar como el AP. La NIC incluye una radio, que puede sintonizar las frecuencias utilizadas por los estándares WLAN admitidos y una antena. Por ejemplo, computadora portátil los fabricantes suelen integrar una NIC WLAN en cada computadora portátil, y luego puede usar una laptop para asociar con un AP y enviar tramas

El AP tiene varios ajustes de configuración necesarios, pero es posible que el cliente no necesite nada configurado. Por lo general, los clientes de forma predeterminada no tienen habilitada ninguna seguridad. cuando el cliente comienza a funcionar, intenta descubrir todos los AP escuchando en todos los canales de frecuencia para el Estándares WLAN que admite de forma predeterminada. Por ejemplo, si un cliente estuviera usando la WLAN como se muestra en la Figura 11-6, con tres AP, cada uno usando un canal diferente, el cliente podría realmente descubra los tres puntos de acceso. El cliente entonces usaría el AP desde el cual el cliente recibe la señal más fuerte. Además, el cliente aprende el SSID del AP, eliminando nuevamente la necesidad de cualquier configuración de cliente

Paso 5: Verifique que la WLAN funcione desde el cliente

El primer paso para verificar el correcto funcionamiento del primer cliente WLAN es verificar si el el cliente puede acceder a los mismos hosts utilizados para la prueba en el paso 1 de este proceso de instalación. (La conexión Ethernet cableada de la computadora portátil debe desconectarse para que la computadora portátil use solo su conexión WLAN). En este punto, si la computadora portátil puede obtener una respuesta de otro host, como hacer ping o navegar por una página web en un servidor web, la WLAN al menos funciona.

Si esta prueba no funciona, se podrían realizar una amplia variedad de tareas. Algunas de las tareas se relacionan con el trabajo que a menudo se realiza en las etapas de planificación, generalmente llamado estudio del sitio. Durante una encuesta del sitio inalámbrico, los ingenieros recorren el sitio en busca de una nueva WLAN, en busca de un buen punto de acceso ubicaciones,

transmitiendo y probando la intensidad de la señal en todo el sitio. En esa misma línea de pensando, si el nuevo cliente no puede comunicarse, puede verificar lo siguiente:

- ¿Está el AP en el centro del área en la que residen los clientes?
- ¿Está el punto de acceso o el cliente justo al lado de una gran cantidad de metal?
- ¿Está el AP o el cliente cerca de una fuente de interferencia, como un horno de microondas o un juego? ¿sistema?
- ¿El área de cobertura del AP es lo suficientemente amplia para llegar al cliente?

Seguridad de LAN inalámbrica

Todas las redes de hoy en día necesitan una buena seguridad, pero las WLAN tienen una seguridad única requisitos En esta sección se examinan algunas de las necesidades de seguridad de las WLAN y la progresión y maduración de las opciones de seguridad WLAN. También habla de cómo configurar las funciones de seguridad

Problemas de seguridad de WLAN

Las WLAN introducen una serie de vulnerabilidades que no existen para las LAN Ethernet cableadas. Algunas de estas vulnerabilidades dan a los hackers la oportunidad de causar daño robando información, accediendo a hosts en la parte cableada de la red, o impidiendo el servicio a través de un ataque de denegación de servicio (DoS). Otras vulnerabilidades pueden ser causadas por una buena intención, pero empleado desinformado que instala un AP sin la aprobación del departamento de TI, con Sin seguridad. Esto permitiría que cualquier persona obtenga acceso al resto de la red de la empresa.

La progresión de los estándares de seguridad WLAN

Los estándares de WLAN han progresado a lo largo de los años en respuesta a la creciente necesidad de seguridad y debido a algunos problemas en el primer estándar de seguridad de WLAN. Este La sección examina cuatro conjuntos significativos de estándares de seguridad WLAN en orden cronológico, describiendo sus problemas y soluciones

El estándar de seguridad inicial para las WLAN, denominado Privacidad equivalente por cable (WEP), tenía muchos problemas. Los otros tres estándares cubiertos aquí representan una progresión de estándares cuyo objetivo en parte era solucionar los problemas creados por WEP. en cronológico Cisco primero abordó el problema con algunas soluciones propietarias. luego el wifi Alliance, una asociación de la industria, ayudó a solucionar el problema definiendo una estrategia para toda la industria. estándar.

Finalmente, el IEEE completó el trabajo en un estándar público oficial, 802.11i. La Tabla 11-9 enumera estos cuatro principales estándares de seguridad WLAN

Table 11-9 *WLAN Security Standards*

Name	Year	Who Defined It
Wired Equivalent Privacy (WEP)	1997	IEEE
The interim Cisco solution while awaiting 802.11i	2001	Cisco, IEEE 802.1x Extensible Authentication Protocol (EAP)
Wi-Fi Protected Access (WPA)	2003	Wi-Fi Alliance
802.11i (WPA2)	2004	IEEE

La palabra estándar se usa de manera bastante vaga en este capítulo cuando se hace referencia a la seguridad de WLAN. Algunos de los estándares son verdaderos estándares abiertos de un organismo de estándares, a saber, el IEEE. Algunos de los estándares provienen de Wi-Fi Alliance, lo que los convierte en la industria de facto.

estándares, Además, Cisco creó varias soluciones provisorias propietarias para sus productos, haciendo que el uso de la palabra sea más exagerado. Sin embargo, todos estos estándares ayudaron mejorar la seguridad WEP original, por lo que el texto analizará más de cerca cada estándar.

Acceso Wi-Fi Protegido (WPA)

La solución de Cisco a las dificultades de WEP incluía protocolos propietarios, así como Estándar IEEE 802.1x. Después de que Cisco integró sus estándares de seguridad WLAN patentados en los AP de Cisco, Wi-Fi Alliance creó un estándar de seguridad WLAN de múltiples proveedores. En el Al mismo tiempo, el IEEE estaba trabajando en el futuro estándar de seguridad WLAN oficial del IEEE, 802.11i, pero la industria WLAN necesitaba una solución más rápida que esperar en el IEEE estándar. Entonces, la alianza Wi-Fi tomó el trabajo actual en progreso en el comité 802.11i, hizo algunas suposiciones y predicciones, y definió un estándar industrial de facto. El Wi-Fi Alliance luego realizó su tarea normal de certificar los productos de los proveedores en cuanto a si cumplieron con este nuevo estándar de la industria, llamándolo Wi-Fi Protected Access (WPA)

IEEE 802.11i y WPA-2

El IEEE ratificó el estándar 802.11i en 2005; llegaron especificaciones adicionales relacionadas más tarde. Al igual que la solución patentada de Cisco y el estándar de la industria WPA de Wi-Fi Alliance, 802.11i incluye intercambio dinámico de claves, encriptación mucho más fuerte y autenticación de usuario. Sin embargo, los detalles difieren lo suficiente como para que 802.11i no sea compatible con versiones anteriores de ninguno de los dos. WPA o los protocolos exclusivos de Cisco.

Una mejora particularmente importante sobre los estándares provisionales de Cisco y WPA es la inclusión del Estándar de Cifrado Avanzado (AES) en 802.11i. AES proporciona aún mejor cifrado que los estándares provisionales de Cisco y WPA, con claves más largas y muchos más algoritmos de cifrado seguro.