Detección, administración y mantenimiento de dispositivos

CDP: Descripción general

Cisco Discovery Protocol (CDP) es un protocolo de Capa 2 patentado de Cisco que se utiliza para recopilar información sobre los dispositivos Cisco que comparten el mismo enlace de datos. El CDP es independiente de los medios y del protocolo y se ejecuta en todos los dispositivos Cisco, como routers, switches y servidores de acceso.

El dispositivo envía anuncios CDP periódicos a los dispositivos conectados, tal como se muestra en la figura. Estos mensajes comparten información sobre el tipo de dispositivo que se descubre, el nombre de los dispositivos, y la cantidad y el tipo de interfaces.

Debido a que la mayoría de los dispositivos de red se conectan a otros dispositivos, el CDP puede ayudar a tomar decisiones de diseño, solucionar problemas, y realizar cambios en el equipo. El CDP se puede utilizar como herramienta de análisis de redes para conocer información sobre los dispositivos vecinos. Esta información recopilada del CDP puede ayudar a crear una topología lógica de una red cuando falta documentación o detalles.

Configuración y verificación del CDP

Para los dispositivos Cisco, el CDP está habilitado de manera predeterminada. Por motivos de seguridad, puede ser conveniente deshabilitar el CDP en un dispositivo de red de manera global, o por interfaz. Con el CDP, un atacante puede recolectar información valiosa sobre el diseño de la red, como direcciones IP, versiones de IOS, y tipos de dispositivos.

Para verificar el estado de CDP y mostrar información sobre CDP, ingrese el comando **show cdp**.

Para habilitar el CDP globalmente para todas las interfaces admitidas en el dispositivo, ingrese **cdp run** en el modo de configuración global. CDP se puede deshabilitar para todas las interfaces del dispositivo con el comando **no cdp run**, en el modo de configuración global.

Para deshabilitar CDP en una interfaz específica, como la que entra en contacto con un ISP, ingrese **no cdp enable** en el modo de configuración de la interfaz. El CDP aún se encuentra habilitado en el dispositivo; sin embargo, no se enviarán más mensajes a la interfaz. Para volver a habilitar CDP en la interfaz específica, ingrese **cdp enable**.

Para verificar el estado de CDP y mostrar una lista de sus componentes adyacentes, utilice el comando **show cdp neighbors**, en el modo EXEC con privilegios. El comando **show cdp neighbors** muestra información importante sobre los componentes adyacentes de CDP. Actualmente, este dispositivo no tiene ningún componente adyacente porque no está conectado físicamente a ningún otro dispositivo, tal como lo indican los resultados del comando **show cdp neighbors**.

Detección de dispositivos con CDP

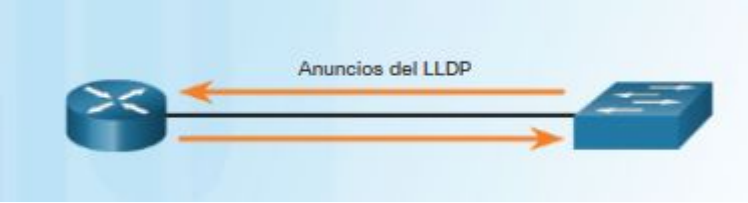
Con el CDP habilitado en la red, el comando **show cdp neighbors** se puede utilizar para determinar el diseño de la red.

Por ejemplo, considere la falta de documentación en la topología de la Figura 1. No hay información disponible relacionada con el resto de la red. El comando **show cdp neighbors** proporciona información útil sobre cada dispositivo adyacente CDP, como los siguientes datos:

- **Identificadores de dispositivos** - El nombre de host del dispositivo adyacente (S1).
- **Identificador de puerto** - El nombre de los puertos local y remoto (Gig 0/1 y Fas 0/5, respectivamente).
- **Lista de funcionalidades** - Indica si el dispositivo es un router o un switch (S para switch; I para IGMP está más allá del ámbito de este curso).
- **Plataforma** - La plataforma de hardware del dispositivo (WS-C2960 para el switch Cisco 2960).

LLDP: Descripción general

Los dispositivos Cisco también admiten el Protocolo de detección de capa de enlace (LLDP), que es un protocolo neutro de detección de componentes adyacentes similar a CDP. El LLDP funciona con los dispositivos de red, como routers, switches, y puntos de acceso inalámbrico LAN. Este protocolo informa su identidad y capacidades a otros dispositivos y recibe información de un dispositivo físicamente conectado de capa 2.



Configuración y verificación del LLDP

En algunos dispositivos, el LLDP podría estar activado de manera predeterminada. Para habilitar LLDP a nivel global en un dispositivo de red Cisco, ingrese el comando **lldp run** en el modo de configuración global. Para deshabilitar el LLDP, ingrese el comando **no lldp run** en el modo de configuración global.

Para verificar que LLDP ya se haya habilitado en el dispositivo, ingrese el comando **show lldp** en el modo EXEC con privilegios.

```
Switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# lldp run
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# lldp transmit
Switch(config-if)# lldp receive
Switch# show lldp

Global LLDP Information:
    Status: ACTIVE
    LLDP advertisements are sent every 30 seconds
    LLDP hold time advertised is 120 seconds
    LLDP interface reinitialisation delay is 2 seconds
```

Detección de dispositivos con LLDP

Con LLDP habilitado, se pueden detectar los componentes adyacentes al dispositivo mediante el comando **show lldp neighbors**. El administrador de redes solo sabe que el S1 está conectado a dos dispositivos. Si utiliza el comando **show lldp neighbors**, el administrador de redes detecta que S1 tiene un router y un switch como componentes adyacentes.

Configuración del reloj del sistema

El reloj de software de un router o un switch se inicia cuando arranca el sistema y es de donde el sistema extrae la hora. Es importante sincronizar la hora en todos los dispositivos de la red porque todos los aspectos de administración, seguridad, solución de problemas, y planificación de redes requieren una marca de hora precisa. Cuando no se sincroniza la hora entre los dispositivos, será imposible determinar el orden de los eventos y la causa de un evento.

Generalmente, las configuraciones de fecha y hora en un router o un switch se pueden configurar de una de las siguientes maneras:

- Configure manualmente la fecha y hora, tal como se muestra en la figura.
- Configurar protocolo de tiempo de red (NTP)

A medida que una red crece, se hace difícil garantizar que todos los dispositivos de infraestructura operen con una hora sincronizada. Incluso en un entorno de red más pequeño, el método manual no es lo ideal. ¿Cómo obtener una fecha y una marca de hora precisas si se reinicia un router?

Una mejor solución es configurar el NTP en la red. Este protocolo permite que los routers de la red sincronicen sus ajustes de hora con un servidor NTP. Si un grupo de clientes NTP obtiene información de fecha y hora de un único origen, tendrá ajustes de hora más consistentes. Cuando se implementa NTP en la red, se lo puede configurar para sincronizarse con un reloj maestro privado o se puede sincronizar con un servidor NTP disponible públicamente en Internet.
NTP utiliza el puerto 123 de UDP y se documenta en RFC 1305.

Funcionamiento de NTP

Las redes NTP utilizan un sistema jerárquico de fuentes horarias. Cada nivel en este sistema jerárquico se denomina estrato. El nivel de estrato se define como la cantidad de saltos desde fuente autorizada. La hora sincronización se distribuye en la red mediante el protocolo NTP. En la figura muestra una red NTP modelo.
Servidores NTP dispuestos en tres niveles que muestran los tres estratos. El estrato 1 está conectado a relojes del estrato 0.

Estrato 0

Una red NTP obtiene la hora de fuentes horarias autorizadas. Estas fuentes autorizadas, conocidas como dispositivos de estrato 0, son dispositivos de cronometraje de alta precisión que son presuntamente precisos y con poco o ningún retraso asociado con los mismos. Los dispositivos del estrato 0 están representados por el reloj en la figura.

Estrato 1

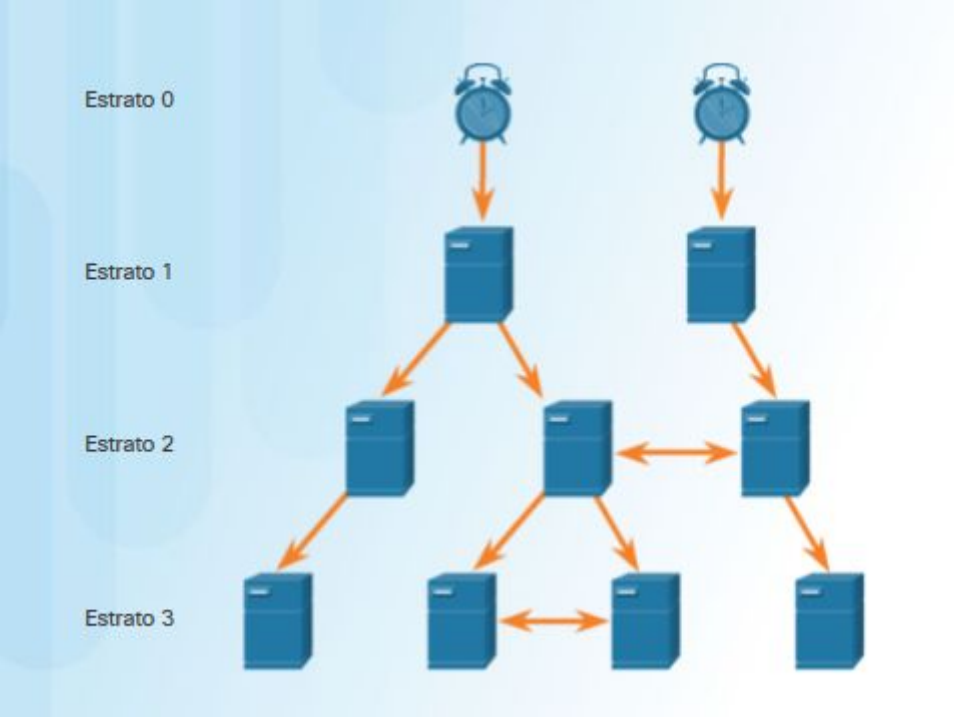
Los dispositivos del estrato 1 están conectados directamente a las fuentes horarias válidas. Actúan como el estándar horario de la red principal.

Estrato 2 y más bajos

Los servidores del estrato 2 están conectados a dispositivos del estrato 1 a través de conexiones de red. Los dispositivos del estrato 2, como clientes de NTP, sincroniza su horario con los paquetes NTP desde servidores del estrato 1. Podrían también actuar como servidores para dispositivos del estrato 3.

Los números más bajos de estratos indican que el servidor está más cerca de la fuente horaria autorizada que los números de estrato más altos. Cuanto mayor sea el número de estrato, menor es el nivel del estrato. El recuento de saltos máximo es 15. El estrato 16, el nivel de estrato inferior, indica que un dispositivo no está sincronizado.

Los servidores horarios en el mismo nivel de estrato pueden configurarse para actuar como un par con otros servidores horarios en el mismo nivel de estratos para la verificación o la copia de respaldo del horario.



Introducción a syslog

Cuando ocurren ciertos eventos en una red, los dispositivos de red tienen mecanismos de confianza para notificar mensajes detallados del sistema al administrador. Estos mensajes pueden ser importantes o no. Los administradores de red tienen una variedad de opciones para almacenar, interpretar y mostrar estos mensajes, así como para recibir esos mensajes que podrían tener el mayor impacto en la infraestructura de la red.
El método más común para acceder a los mensajes del sistema es utilizar un protocolo denominado syslog.

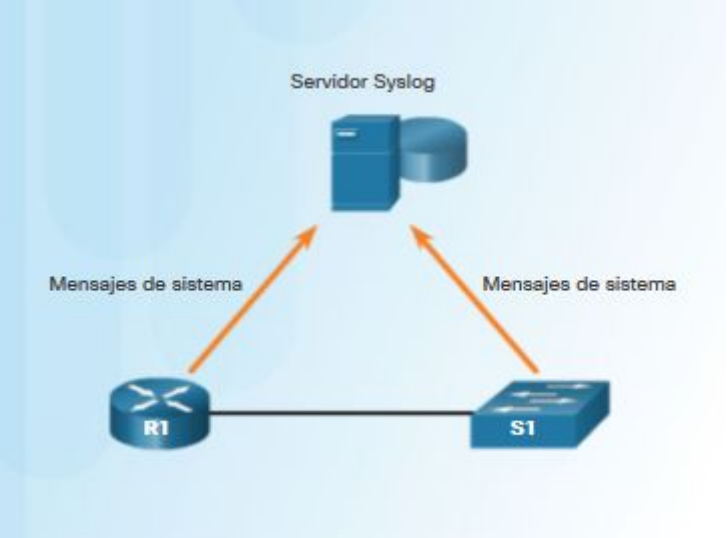
El término “syslog” se utiliza para describir un estándar. También se utiliza para describir el protocolo desarrollado para ese estándar. El protocolo syslog se desarrolló para los sistemas UNIX en la década de los ochenta, pero la IETF lo registró por primera vez como RFC 3164 en 2001. Syslog usa el puerto UDP 514 para enviar mensajes de notificación de eventos a través de redes IP a recopiladores de mensajes de eventos, como se muestra en la ilustración.

Muchos dispositivos de red admiten syslog, incluidos routers, switches, servidores de aplicación, firewalls y otros dispositivos de red. El protocolo syslog permite que los dispositivos de red envíen los mensajes del sistema a servidores de syslog a través de la red.

Existen varios paquetes de software diferentes de servidores de syslog para Windows y UNIX. Muchos de ellos son freeware.

El servicio de registro de syslog proporciona tres funciones principales:

- La capacidad de recopilar información de registro para el control y la resolución de problemas
- La capacidad de seleccionar el tipo de información de registro que se captura
- La capacidad de especificar los destinos de los mensajes de syslog capturados



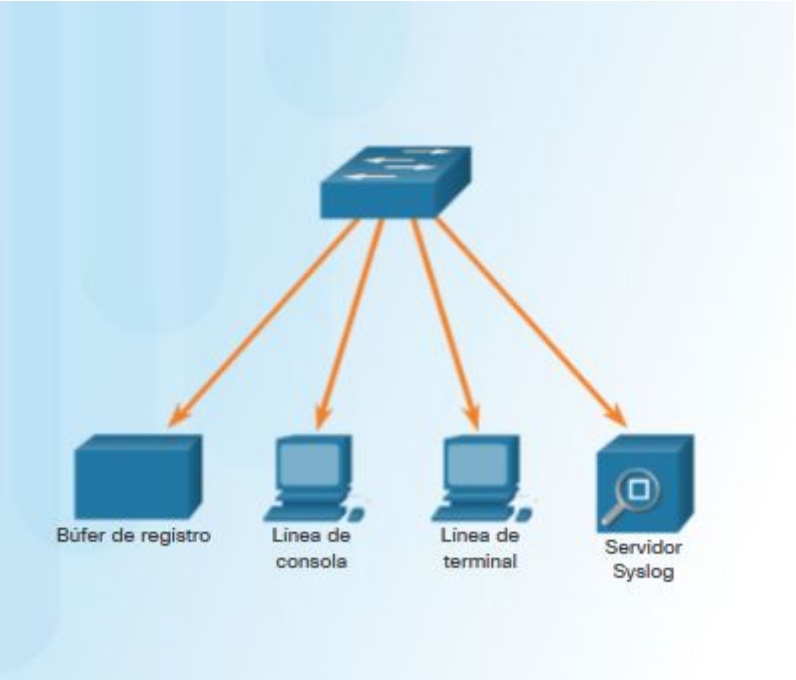
Funcionamiento de syslog

En los dispositivos de red Cisco, el protocolo syslog comienza enviando los mensajes del sistema y el resultado del comando **debug** a un proceso de registro local interno del dispositivo. La forma en que el proceso de registro administra estos mensajes y resultados se basa en las configuraciones del dispositivo.

Por ejemplo, los mensajes de syslog se pueden enviar a través de la red a un servidor de syslog externo. Estos mensajes se pueden recuperar sin necesidad de acceder al dispositivo propiamente dicho. Los resultados y los mensajes de registro almacenados en el servidor externo se pueden incluir en varios informes para facilitar la lectura.

Por otra parte, los mensajes de syslog se pueden enviar a un búfer interno. Los mensajes enviados al búfer interno solo se pueden ver mediante la CLI del dispositivo.

Por último, el administrador de red puede especificar que solo se envíen determinados tipos de mensajes del sistema a varios destinos. Por ejemplo, se puede configurar el dispositivo para que reenvíe todos los mensajes del sistema a un servidor de syslog externo. Sin embargo, los mensajes del nivel de depuración se reenvían al búfer interno, y solo el administrador puede acceder a ellos desde la CLI.



Formato de mensaje de Syslog

Los dispositivos de Cisco generan mensajes de syslog como resultado de los eventos de red. Cada mensaje de syslog contiene un nivel de gravedad y una instalación.

Cada nivel de syslog tiene su propio significado:

- **Nivel de advertencia 4 - Nivel de emergencia 0**: Estos mensajes son mensajes de error sobre desperfectos de software o hardware; indican que la funcionalidad del dispositivo está afectada. La gravedad del problema determina el nivel real de syslog que se aplica.
- **Nivel de notificación 5**: El nivel de notificaciones es para eventos normales, pero significativos. Por ejemplo: las transiciones para activar o desactivar interfaces y los mensajes para reiniciar el sistema se muestran en el nivel de notificaciones.
- **Nivel informativo 6**: Un mensaje informativo normal que no afecta la funcionalidad del dispositivo. Por ejemplo: cuando un dispositivo Cisco está arrancando, se podría

ver el siguiente mensaje informativo: %LICENSE-6-EULA_ACCEPT_ALL: The Right to Use End User License Agreement is accepted.

- **Nivel de depuración 7**: Este nivel indica que los mensajes son generados como salida a partir de la ejecución de diversos comandos **debug** (de depuración).

Además de especificar la gravedad, los mensajes de syslog también contienen información sobre la instalación. Las instalaciones de syslog son identificadores de servicios que identifican y categorizan los datos de estado del sistema para informar los mensajes de error y de eventos. Las opciones de instalación de registro disponibles son específicas del dispositivo de red. Por ejemplo, los switches Cisco de la serie 2960 que ejecutan el IOS de Cisco versión 15.0(2) y los routers Cisco 1941 que ejecutan el IOS de Cisco versión 15.2(4) admiten 24 opciones de instalación que se categorizan en 12 tipos de instalación.

Algunas instalaciones comunes de mensajes de syslog que se informan en los routers con IOS de Cisco incluyen lo siguiente:

- IP
- Protocolo OSPF
- Sistema operativo SYS
- Seguridad IP (IPsec)
- IP de interfaz (IF)

De manera predeterminada, el formato de los mensajes de syslog en el software IOS de Cisco es el siguiente:
seq no: timestamp: %facility-severity-MNEMONIC: description

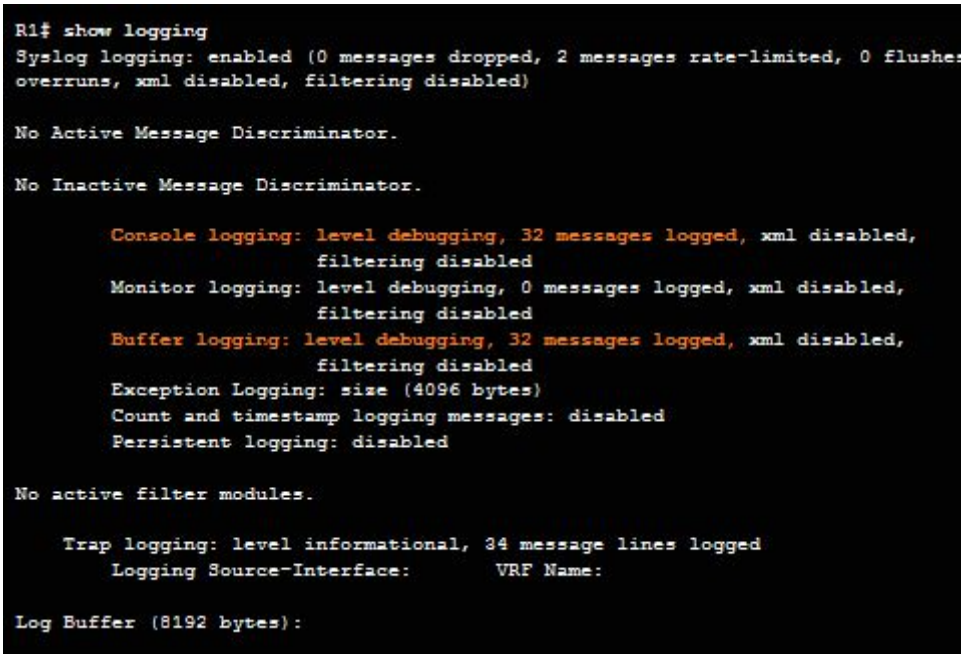
Registro predeterminado

De manera predeterminada, los routers y switches de Cisco envían mensajes de registro a la consola para todos los niveles de gravedad. En algunas versiones del IOS, el dispositivo también almacena en búfer los mensajes de registro de manera predeterminada. Para habilitar estas dos configuraciones, utilice los comandos de configuración global **logging console** y **logging buffered**, respectivamente.

El comando **show logging** muestra la configuración predeterminada del servicio de registro en un router Cisco, como se muestra en la ilustración. En las primeras líneas del resultado, se proporciona información sobre el proceso de registro, y al final del resultado se indican los mensajes de registro.

En la primera línea resaltada, se indica que este router se registra en la consola y se incluyen mensajes de depuración. Esto en realidad significa que todos los mensajes del nivel de depuración, así como cualquier mensaje de nivel inferior (como los mensajes del nivel de notificación), se registran en la consola. En la mayoría de los routers Cisco IOS, el nivel de gravedad predeterminado es 7: depuración. El resultado también indica que se registraron 32 de estos mensajes.

En la segunda línea resaltada, se indica que este router se registra en un búfer interno. Dado que en este router se habilitó el registro en un búfer interno, el comando **show logging** también indica los mensajes en ese búfer. Puede ver algunos de los mensajes del sistema que se registraron al final del resultado.



Comandos de router y switch para los clientes syslog

Existen tres pasos para configurar el router para que envíe los mensajes del sistema a un servidor de syslog donde se puedan almacenar, filtrar y analizar:

Paso 1: En el modo de configuración global, utilice el comando **logging** paraconfigurar el nombre de host del destino o la dirección IPv4 del syslog.

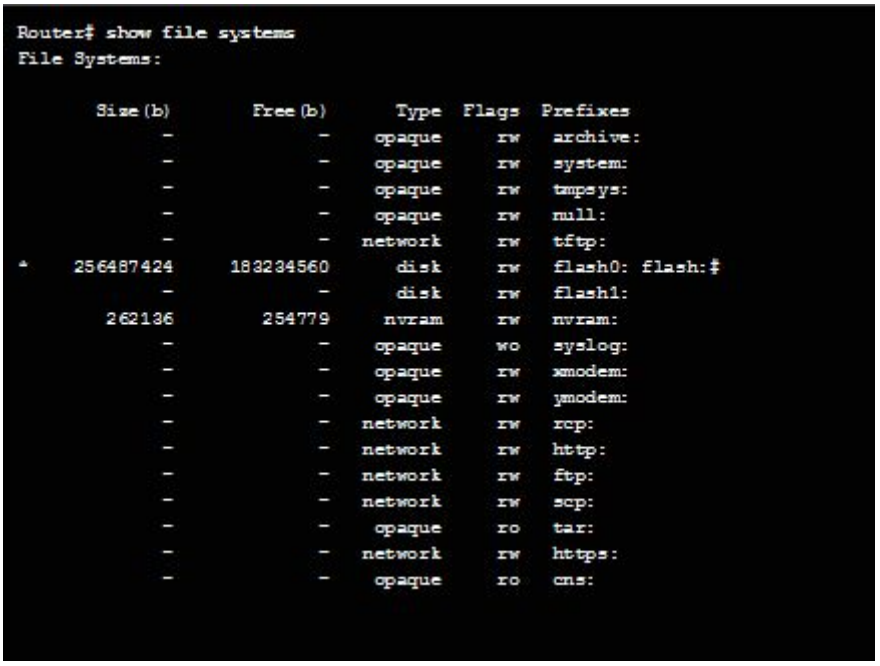
Paso 2: Controle los mensajes que se enviarán al servidor syslog con el comando **logging trap** *level* en el modo de configuración global. Por ejemplo, para limitar los mensajes a los niveles 4 e inferiores (0 a 4), utilice uno de los dos comandos equivalentes.

Paso 3: Opcionalmente, configure la interfaz de origen con el comando **logging source-interface**. *tipo-interfaz número-interfaz* comando global configuration mode. Esto especifica que los paquetes de syslog incluyen la dirección IPv4 o IPv6 de una interfaz específica, independientemente de la interfaz que use el paquete para salir del router.

```
R1(config)# logging 192.168.1.3
R1(config)# logging trap 4
R1(config)# logging source-interface g0/0
R1(config)# interface loopback 0
R1(config-if)#
*Jun 12 22:06:02.902: %LINK-3-UPDOWN: Interface Loopback0, changed state to up
*Jun 12 22:06:03.902: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up
*Jun 12 22:06:03.902: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.3
port 514 started - CLI initiated
R1(config-if)# shutdown
R1(config-if)#
*Jun 12 22:06:49.642: %LINK-5-CHANGED: Interface Loopback0, changed state to
administratively down
*Jun 12 22:06:50.642: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to down
R1(config-if)# no shutdown
R1(config-if)#
*Jun 12 22:09:18.210: %LINK-3-UPDOWN: Interface Loopback0, changed state to up
*Jun 12 22:09:19.210: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up
R1(config-if)#
```

Sistemas de archivos del router

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

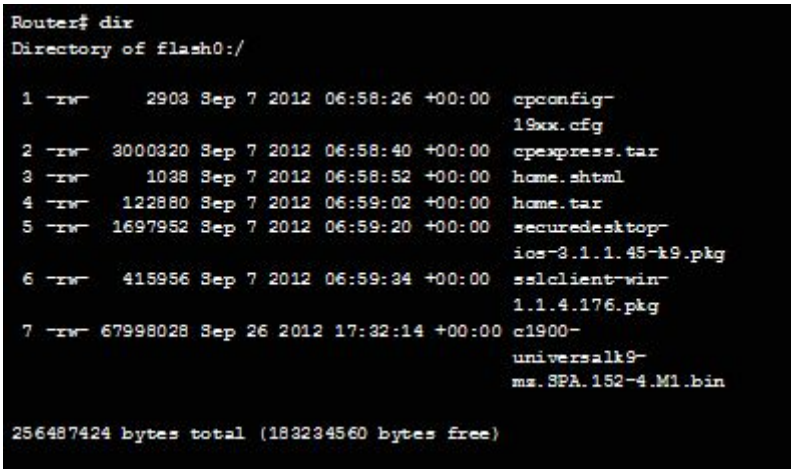


La figura 1 muestra el resultado del comando **show file systems**, que enumera todos los sistemas de archivos disponibles en un router Cisco 1941. Este comando proporciona información útil, como la cantidad de memoria disponible y libre, el tipo de sistema de archivos y los permisos. Los permisos incluyen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

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

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

El sistema de archivos flash



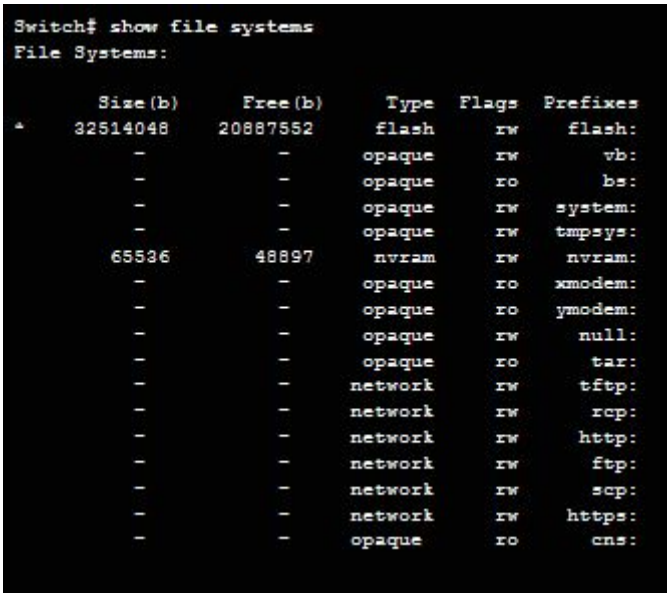
En la Figura 2 se muestra la salida del comando **dir** (directorio). Como flash es el sistema de archivos predeterminado, el comando **dir** enumera el contenido de flash. Varios archivos están ubicados en la memoria flash, pero el de mayor interés específicamente es el último de la lista. se trata del nombre del archivo de imagen de Cisco IOS actual que se ejecuta en la memoria RAM.

El sistema de archivos NVRAM

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

Sistemas de archivos del switch

Con el sistema de archivos flash del switch Cisco 2960, se pueden copiar los archivos de configuración y archivar (subir y descargar) imágenes de software.
El comando para ver los sistemas de archivos en un switch Catalyst es el mismo que se utiliza en los routers Cisco: **show file systems**, como se muestra en la ilustración.



Creación de copias de respaldo y restauración mediante archivos de texto

Copia de respaldo de las configuraciones con captura de texto (Tera Term)

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

Como se muestra en la figura, los pasos son:

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

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

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

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

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

Restauración de las configuraciones de texto

Una configuración se puede copiar de un archivo a un dispositivo. Cuando se copia desde un archivo de texto y se pega en la ventana de una terminal, el IOS ejecuta cada línea del texto de configuración como si fuera un comando. Esto significa que el archivo necesitará edición para asegurar que las contraseñas cifradas estén en forma de texto y que se eliminen los

mensajes de IOS y el texto de no comando, como "--More--". Este proceso se analiza en la práctica de laboratorio.

A su vez, en la CLI, el dispositivo debe establecerse en el modo de configuración global para recibir los comandos del archivo de texto que se pegan en la ventana de la terminal.
Cuando se usa Tera Term, los pasos son los siguientes:

Paso 1: En el menú File (Archivo), haga clic en **Send** (Enviar) para enviar el archivo.
Paso 2. Ubique el archivo que debe copiar en el dispositivo y haga clic en **Open**.
Paso 3. Tera Term pegará el archivo en el dispositivo.

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

Creación de copias de respaldo y restauración de TFTP

Copia de respaldo de las configuraciones mediante TFTP

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

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

Paso 1: Ingrese el comando **copy running-config tftp**.
Paso 2. Introduzca la dirección IP del host en el cual se almacenará el archivo de configuración.
Paso 3. Introduzca el nombre que se asignará al archivo de configuración.
Paso 4. Presione Intro para confirmar cada elección.
Restauración de las configuraciones mediante TFTP

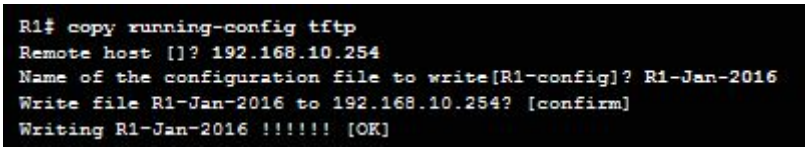
Para restaurar la configuración en ejecución o la configuración de inicio desde un servidor TFTP, utilice el comando **copy tftp running-config** o **copy tftp startup-config**. Siga estos pasos para restaurar la configuración en ejecución desde un servidor TFTP:

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

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

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

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



Recuperación de contraseñas

Las contraseñas de los dispositivos se utilizan para evitar el acceso no autorizado. Las contraseñas encriptadas, como las contraseñas generadas mediante "enable secret", se deben reemplazar después de su recuperación. De acuerdo con el dispositivo, el procedimiento detallado para la recuperación de contraseñas varía; sin embargo, todos los procedimientos de recuperación de contraseñas siguen el mismo principio:

Paso 1: Ingresar en el modo ROMMON.

Paso 2. Cambiar el registro de configuración a 0x2142 para ignorar el archivo de configuración de inicio.

Paso 3. Realizar los cambios necesarios en el archivo original de configuración de inicio.

Paso 4: Guardar la configuración nueva.

Para la recuperación de contraseñas, se requiere el acceso a la consola del dispositivo a través de un terminal o el software emulador de terminal en una PC. Las configuraciones de terminal para acceder al dispositivo son:

- 9600 velocidades en baudios
- Sin paridad
- 8 bits de datos
- 1 bit de parada
- Sin control del flujo

Con el acceso a la consola, el usuario puede acceder al modo ROMMON mediante una secuencia de interrupción durante el proceso de arranque o eliminando la memoria flash externa cuando el dispositivo está apagado.

El software ROMMON admite algunos comandos básicos, como **confreg**. El comando **confreg 0x2142** permite que el usuario defina el registro de configuración en 0x2142. Con el registro de configuración en 0x2142, el dispositivo ignorará el archivo de configuración de inicio durante el arranque.

El archivo de configuración de inicio es donde se almacenan las contraseñas olvidadas. Después de configurar el registro de configuración en 0x2142, escriba **reset** en la petición de entrada para reiniciar el dispositivo. Introduzca la secuencia de interrupción mientras el dispositivo esté reiniciando y descomprimiendo el IOS. En la Figura 1 se muestra la salida del terminal de un router 1941 en modo ROMMON después de usar una secuencia de interrupción durante el proceso de arranque.

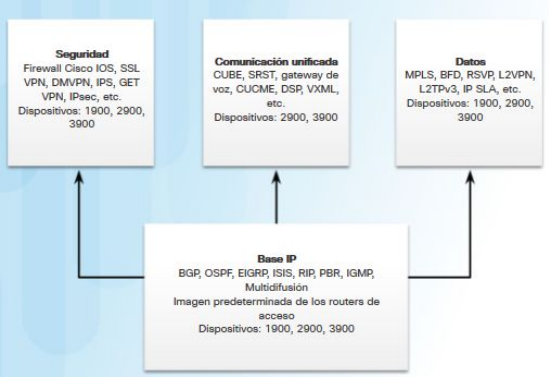
Paquetes de imagen de sistema del IOS 15

Las series de routers de servicios integrados Cisco de segunda generación (ISR G2) 1900, 2900 y 3900 admiten servicios a petición mediante el uso de licencias de software. El proceso de Servicios a petición permite que los clientes logren ahorros operativos mediante la facilidad de pedido y administración del software. Cuando se realiza un pedido de una nueva plataforma de ISR G2 de Cisco, el router se envía con una imagen única y universal del software IOS de Cisco, y se utiliza una licencia para habilitar los paquetes de conjuntos de características específicos

Existen dos tipos de imágenes universales admitidas en ISR G2:

- **Imágenes universales con la designación "universalk9" en el nombre de la imagen** - Esta imagen universal ofrece todas las funciones del software Cisco IOS, incluidas sólidas características de criptografía de carga útil como IPsec VPN, SSL VPN y Secure Unified Communications.
- **Imágenes universales con la designación "universalk9_npe" en el nombre de la imagen** - La fuerte imposición de las capacidades de cifrado proporcionadas por Cisco Software Activation satisface los requisitos para la exportación de funcionalidades de cifrado. Sin embargo, algunos países tienen requisitos de importación que exigen que la plataforma no admita ninguna funcionalidad de criptografía segura, como la criptografía del contenido. Para satisfacer los requisitos de importación de dichos países, la imagen universal npe no admite ningún cifrado del contenido seguro.

Con los dispositivos ISR G2, se facilitó la selección de la imagen del IOS, debido a que se incluyen todas las características dentro de la imagen universal. Las características se activan mediante licencias. Cada dispositivo se envía con imagen universal. Los paquetes de tecnología IP Base, Datos, UC (Comunicaciones unificadas) y SEC (Seguridad) se habilitan en la imagen universal mediante las claves de licencia de Cisco Software Activation. Cada clave de licencia es exclusiva de un dispositivo en particular y se obtiene de Cisco al proporcionar la ID del producto, el número de serie del router y una clave de activación del producto (PAK). Cisco proporciona la PAK en el momento de la compra del software. IP Base se instala de manera predeterminada.



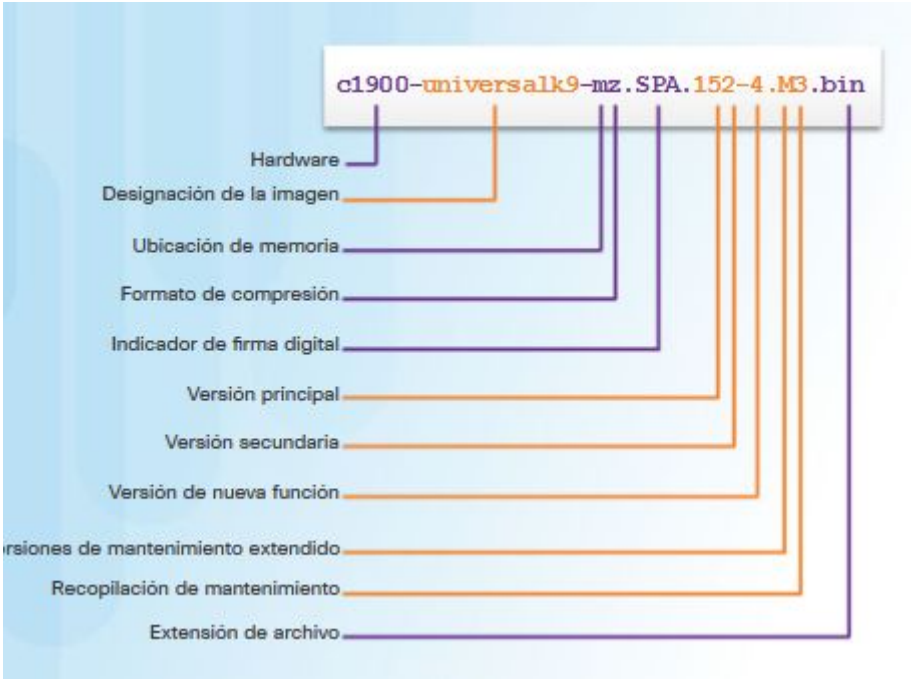
Nombres de archivo de imagen del IOS

Al seleccionar o actualizar un router con IOS de Cisco, es importante elegir la imagen del IOS adecuada con el conjunto de características y la versión correctos. El archivo de imagen de Cisco IOS se basa en una convención de nomenclatura especial. El nombre del archivo de imagen de Cisco IOS contiene varias partes, cada una con un significado específico. Es importante comprender esta convención de nomenclatura al actualizar y seleccionar un software IOS de Cisco.

```
R1# show flash0:
-# - --length-- -----date/time------ path

8   68831808   Apr 2 2013 21:29:58 +00:00 c1900-universalk9-mz.SPA.152-4.M3.bin

182394880 bytes available (74092544 bytes used)

R1#
```

Como se muestra en la figura 1, el comando **show flash** muestra los archivos almacenados en la memoria flash, incluso los archivos de imagen de sistema.

En la figura 2, se ilustran las distintas partes de un archivo de imagen de sistema del IOS 15 en un dispositivo ISR G2:



- **Nombre de la imagen (c1900):** identifica la plataforma en la que se ejecuta la imagen. En este ejemplo, la plataforma es un router Cisco 1900.
- **universalk9:** especifica la designación de la imagen. Las dos designaciones para un ISR G2 son universalk9 y universalk9_npe. Universalk9_npe no contiene cifrado seguro y está pensado para países con restricciones de cifrado. Las características se controlan mediante licencias y pueden dividirse en cuatro paquetes de tecnología. Estos son IP Base, Seguridad, Comunicaciones unificadas y Datos.
- **mz:** Indica dónde se ejecuta la imagen y si el archivo está comprimido. En este ejemplo, mz indica que el archivo se ejecuta desde la RAM y que está comprimido.
- **SPA:** indica que el archivo está firmado digitalmente por Cisco.
- **152-4.M3:** especifica el formato del nombre del archivo para la imagen 15.2(4)M3. Esta es la versión del IOS, que incluye los números de la versión principal, de la versión secundaria, de la versión de mantenimiento y de la recopilación de mantenimiento. La M indica que se trata de una versión de mantenimiento extendido.
- **bin:** La extensión del archivo. Esta extensión indica que este archivo es un archivo ejecutable binario.

La designación más común para ubicación de memoria y formato de compresión es mz. La primera letra indica la ubicación donde se ejecuta la imagen en el router. Las ubicaciones pueden incluir las siguientes:

- **f:** flash
- **m:** RAM
- **r:** ROM
- **l:** Reubicable

El formato de compresión puede ser z para zip o x para mzip. La compresión de archivos es un método que utiliza Cisco para comprimir algunas imágenes ejecutadas desde la RAM que es eficaz para reducir el tamaño de la imagen. Se autodescomprime, de modo que cuando la imagen se carga en la RAM para ejecutarse, la primera acción es la descompresión.

Nota: las convenciones de nomenclatura, el significado de los campos, el contenido de la imagen y otros detalles del software IOS de Cisco están sujetos a cambios.

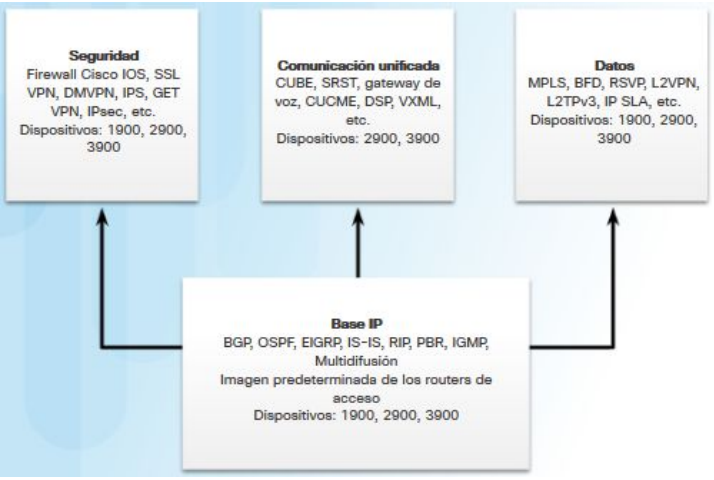
Requisitos de memoria

En la mayoría de los routers Cisco, incluso en los routers de servicios integrados, el IOS se almacena en la memoria CompactFlash como una imagen comprimida y se carga en la DRAM durante el arranque. Las imágenes de la versión 15.0 del software IOS de Cisco disponibles para los ISR Cisco 1900 y 2900 requieren 256 MB de memoria flash y 512 MB de memoria RAM. El ISR 3900 requiere 256 MB de memoria flash y 1 GB de RAM. Esto no incluye herramientas de administración adicionales, como Cisco Configuration Professional (Cisco CP). Para obtener detalles completos, consulte la ficha técnica del producto para el router específico.

Aspectos generales del proceso de otorgamiento de licencias

A partir de Cisco IOS Software versión 15.0, Cisco modificó el proceso para habilitar nuevas tecnologías en los conjuntos de características de IOS. La versión 15.0 del software IOS de Cisco incorpora conjuntos de características interplataforma para simplificar el proceso de selección de imágenes. Lo hace proporcionando funciones similares a través de los límites de las plataformas. Cada dispositivo se envía con la misma imagen universal. Los paquetes de tecnología se habilitan en la imagen universal mediante claves de licencia de Cisco Software Activation. La característica Cisco IOS Software Activation permite que el usuario habilite características con licencia y registre licencias. La característica Cisco IOS Software

Activation es un conjunto de procesos y componentes que se utilizan para activar los conjuntos de características del software IOS de Cisco mediante la obtención y validación de licencias del software de Cisco.



En la figura 1, se muestran los paquetes de tecnología disponibles:

- IP Base
- Datos
- Comunicaciones unificadas (UC)
- Seguridad (SEC)

Licencias de paquetes de tecnología

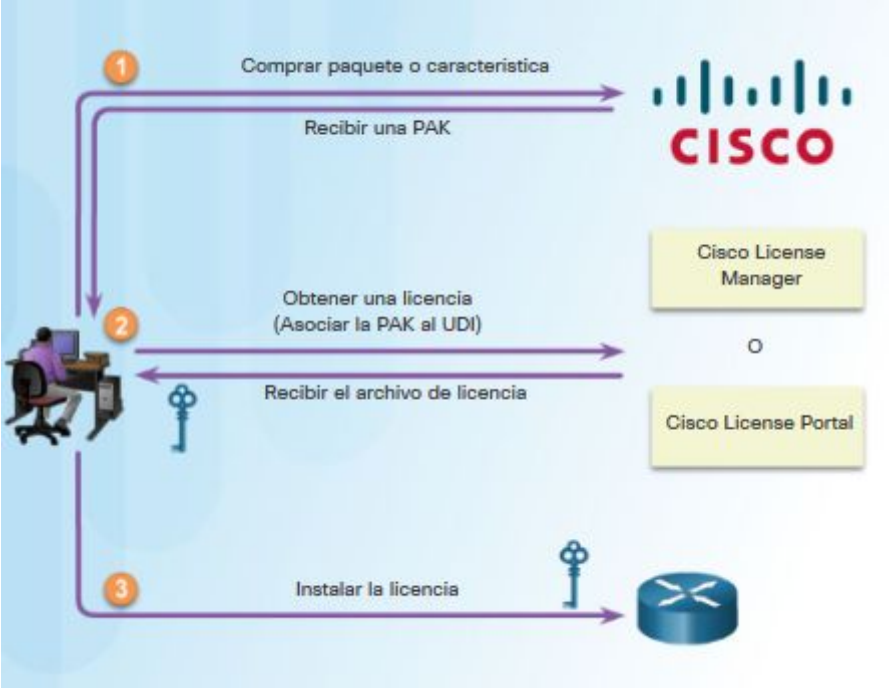
Las licencias de paquetes de tecnología se admiten en plataformas ISR G2 de Cisco (routers Cisco de las series 1900, 2900 y 3900). La imagen universal del IOS de Cisco contiene todos los paquetes y características en una imagen. Cada paquete es un conjunto de características específicas de la tecnología. Se pueden activar varias licencias de paquetes de tecnología en las plataformas ISR Cisco de las series 1900, 2900 y 3900.

Nota: utilice el comando **show license feature** para ver las licencias de paquetes de tecnología y las licencias de características admitidas en el router.

Proceso de obtención de licencias

Cuando se envía un router nuevo, vienen preinstaladas la imagen del software y las licencias permanentes correspondientes para los paquetes y características especificadas por el cliente.

El router también viene con la licencia de evaluación, conocida como licencia temporal, para la mayoría de los paquetes y características admitidas en el router especificado. Esto permite que los clientes prueben una nueva característica o un nuevo paquete de software mediante la activación de una licencia de evaluación específica. Si los clientes desean activar de forma permanente una característica o un paquete de software en el router, deben obtener una licencia de software nueva.



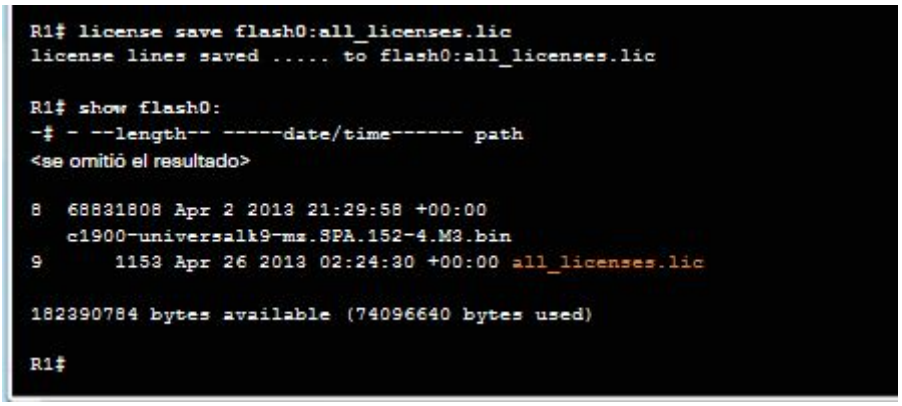
Realización de copias de respaldo de la licencia

El comando **license save** se utiliza para copiar todas las licencias en un dispositivo y almacenarlas en un formato requerido por la ubicación de almacenamiento especificada. Las licencias guardadas se restablecen mediante el comando **license install**.

El comando para realizar una copia de seguridad de las licencias en un dispositivo es el siguiente:

Router# **license save** *archivo-sys://lic-ubicación*
Utilice el comando **show flash0:** para verificar que las licencias se hayan guardado.

La ubicación de almacenamiento de licencias puede ser un directorio o un URL que corresponda a un sistema de archivos. Utilice el comando **?** para ver las ubicaciones de almacenamiento que admite un dispositivo.



Desinstalación de la licencia

Para borrar una licencia permanente activa de los routers Cisco de las series 1900, 2900 y 3900, realice los siguientes pasos:

Paso 1: Deshabilite el paquete de tecnología.

- Deshabilite la licencia activa mediante el comando:

Router(config)# **license boot module** *nombre-módulo* **technology-package** *nombre-paquete* **disable**

- Vuelva a cargar el router mediante el comando **reload**. Se requiere volver a cargarlo para que el paquete de software esté inactivo.

Paso 2: Borre la licencia.

- Borre la licencia de paquete de tecnología del almacenamiento de licencias.

Router# **license clear** *nombre-característica*

- Borre el comando **license boot module** que se usó para deshabilitar la licencia activa:

Router(config)# **no license boot module** *nombre-módulo* **technology-package** *nombre-paquete* **disable**

Nota: algunas licencias, como las licencias incorporadas, no pueden borrarse. Solo se eliminan las licencias que se agregaron mediante el comando **license install**. Las licencias de evaluación no se eliminan.