Configuracion de ROUTERS CISCO

Índice

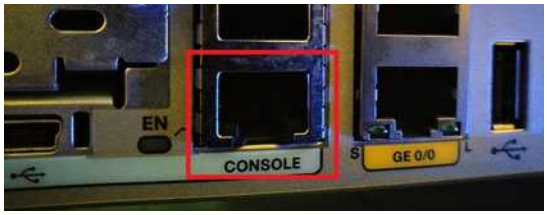
Conexión y modos del dispositivo

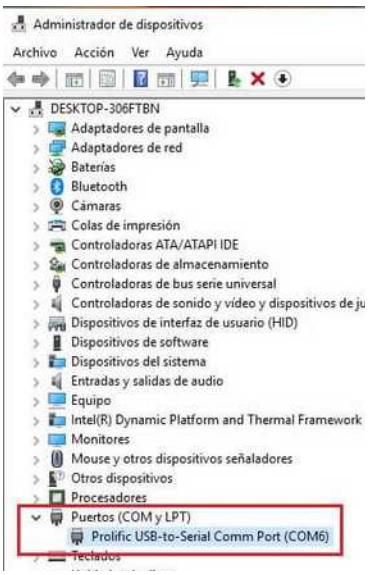
IOS es el S.O de Cisco se maneja fundamentalmente por comandos. Sin embargo, cuando encendemos un switch/router por primera vez, no es posible acceder a ese sistema. Necesitamos proporcionar una configuración inicial. Y para ello, usaremos casi con toda seguridad el cable de consola.

El cable de consola es un cable propio de Cisco y por un lado usa una conexión propia de Cisco y en el otro extremos puede ser:

- USB (hoy en día lo más probable)
- RS-232 (aún muy utilizado, pero está cayendo en desuso)
- RJ-45 (depende del dispositivo)

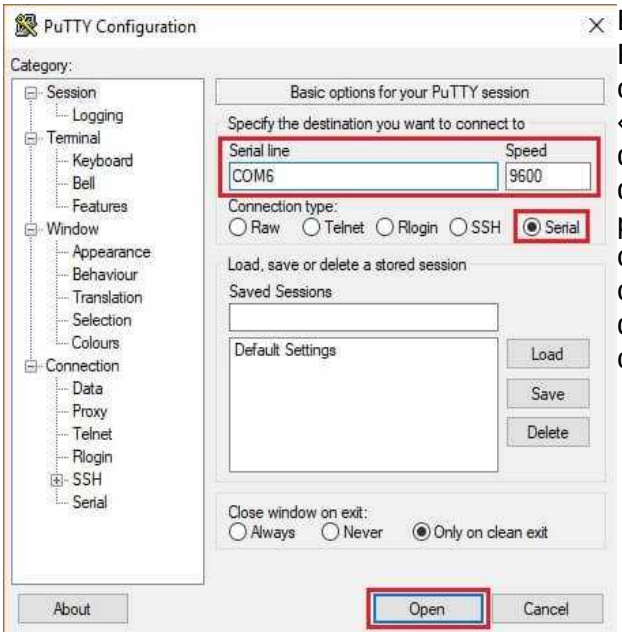
Si nuestro PC no tiene conexión DB9/RS232 vamos a necesitar algún tipo de conversor de DB9/RS232 a USB y bajar los drivers de aquí https://www.youtube.com/watch?v=jIRRsIgfHU8





Una vez todo conectado como el esquema y el router alimentado, nos iremos al PC y suponiendo que

tenemos Windows 10, haremos 'click' con el botón derecho del ratón en el menú de inicio y nos iremos a "Administrador de dispositivos": En la nueva ventana nos iremos al apartado "Puertos (COM y LPT)" y dentro buscaremos el cable USB-Serial, pero sobre todo nos fijaremos el puerto COM que aparece entre paréntesis. En nuestro caso el "COM6".



Este puerto es el que usaremos para conectarnos. Para acceder al sistema operativo necesitaremos un ordenador en el que haya algún programa de tipo «Terminal». Este programa enviará los datos directamente al dispositivo (sin direcciones de origen ni de destino ni nada). Para ello bastará con abrir un programa que nos permita establecer una conexión por consola. Usraemos PuTTY. Así que lo abriremos y lo configuraremos de la siguiente manera: Es vital saber qué velocidades acepta el dispositivo al que nos conectamos. En el caso Cisco, es casi sin excepción:

- Velocidad: 9600 bits por segundo.
- Tamaño de los caracteres de datos: 8 bits.
- Paridad. Es un mecanismo de comprobación de comprobación de errores. Los dispositivos Cisco no usan paridad.
- Bits de stop. En Cisco se usa 1 bits de stop.
- Control de flujo/velocidad. No se usará ninguno.

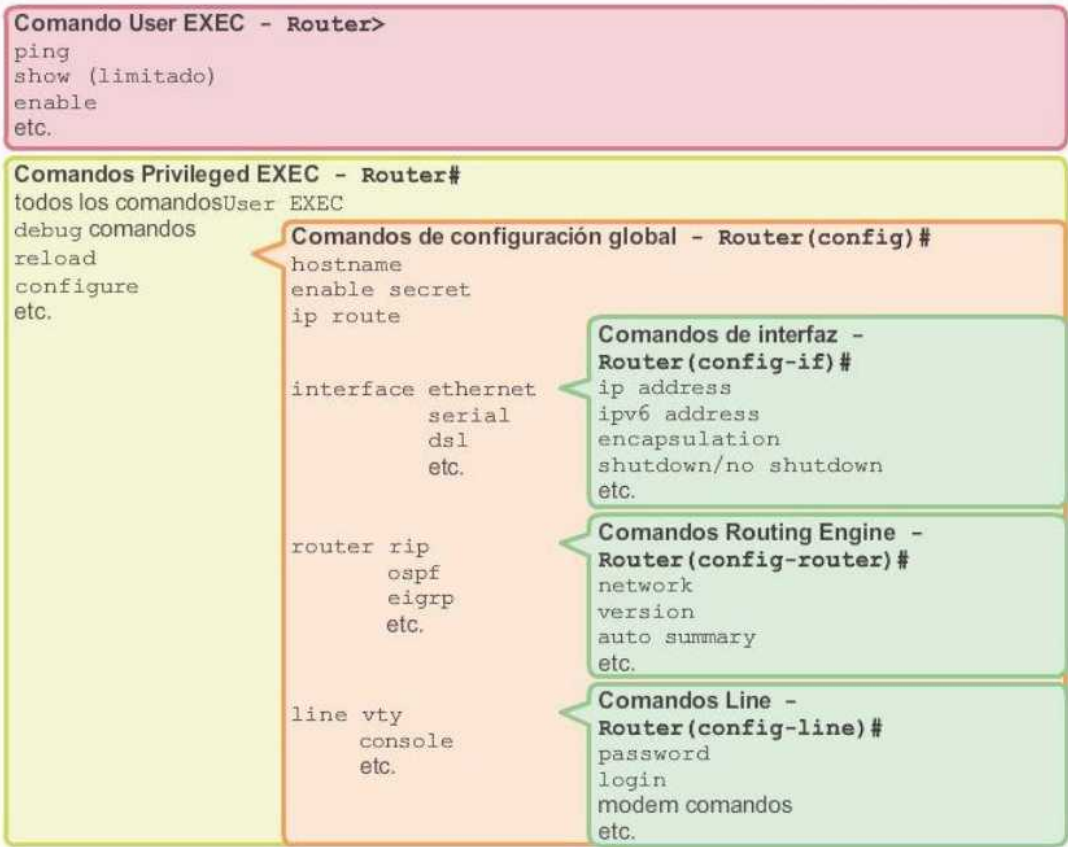
En ocasiones se puede ver algo como 96008N1N. Esto significa «9600 bits/seg», «8 bits de datos», «No paridad», «1 bit de stop» y «No control de flujo».

Una vez que tenemos acceso al sistema operativo, debemos recordar que IOS es un sistema operativo modal.

El sistema operativo arranca en modo usuario. En ese modo lo único que se suele poder hacer es «visualizar», pero no «cambiar» ni «configurar». En suma, se usa el comando **show**

Para pasar al modo «privilegiado» se usa el comando **enable**. Lo normal es que dicho modo tenga una clave. Para volver al modo usuario podemos usar **disable**.

Para pasar al modo «configuración» se usa **configure terminal** desde el modo privilegiado.



El modo usuario

En este modo solo se pueden usar unos pocos comandos show. Por ejemplo:

`show interfaces` muestra la información de todos los interfaces.
`show interfaces Fastethernet 0/1` muestra solo la tarjeta 0/1

Modo privilegiado

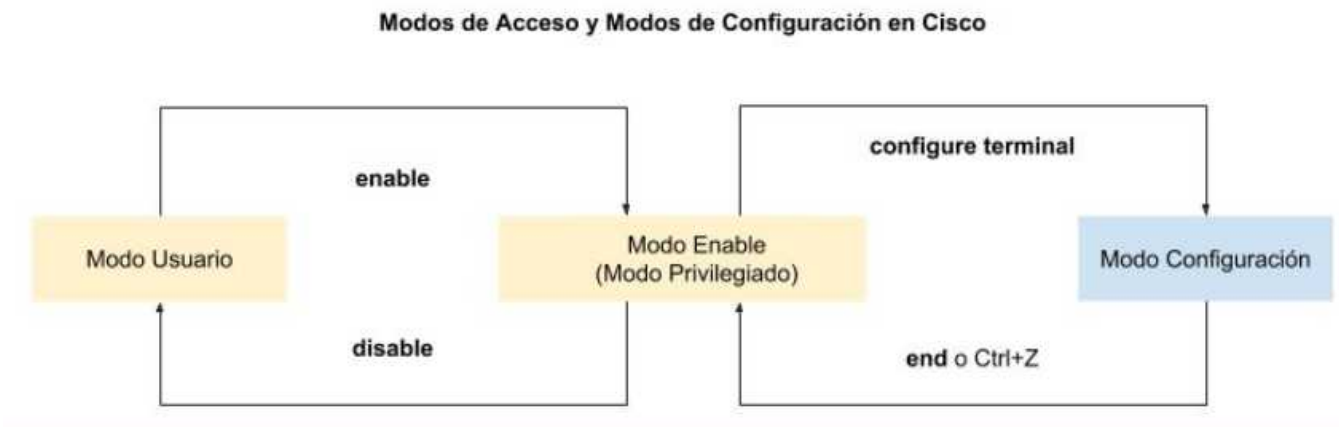
Comandos muy típicos:

`show running-config` muestra la configuración en RAM.
`show startup-config` muestra la configuración de arranque.
`show version` muestra información de versión del sistema operativo, número de serie y dirección MAC base (la que usa el switch para comunicarse con otros por ejemplo)
`copy running-config startup-config`. Graba la configuración actual del switch

clock	Comprobación de la fecha y la hora del sistema
ip interface brief	Para ver el estado de las interfaces
interfaces	Muestra información detallada de cada interfaz
logging	Comprueba el estado del registro *syslog*
mac-address-table	Visualiza la tabla MAC
privilege	Para ver el nivel de privilegio del *switch*
running-config	Muestra la configuración actual del dispositivo
sessions	Monitoriza las conexiones remotas activas
spanning-tree	Visualiza la configuración STP del *switch*
terminal	Muestra los parámetros de configuración del terminal
version	Visualiza los parámetros de estado HW y SW del dispositivo
vlan	Comprueba la configuración de las VLAN del *switch*

Modo de configuración global:

`hostname <nombre>`



Los Routers CISCO

Los routers tienen acceso a cuatro tipos de memoria: RAM, ROM, NVRAM y flash.

Memoria	Volátil/no volátil	Almacena
RAM	Volátil	• IOS en ejecución • Archivo de configuración en ejecución • Enrutamiento de IP y tablas ARP • Buffer de paquetes
ROM	No volátil	• Instrucciones de arranque • Software básico de diagnóstico • IOS limitado
NVRAM	No volátil	• Archivo de configuración de inicio
Flash	No volátil	• IOS (Sistema operativo de internetworking) • Otros archivos de sistema

La **RAM** se utiliza para almacenar diversas aplicaciones y procesos, incluido lo siguiente:

Cisco IOS: el IOS se copia en la RAM durante el arranque.

Archivo de configuración en ejecución o **running-config**: este es el archivo de configuración que almacena los comandos de configuración que el router utiliza actualmente..

Tabla de enrutamiento IP: este archivo almacena información sobre las redes conectadas directamente y remotas. Se utiliza para determinar el mejor camino para reenviar paquetes.

Caché ARP: esta caché contiene la asignación de direcciones IPv4 a direcciones MAC y es similar a la caché de protocolo de resolución de direcciones (ARP) de una PC. La caché ARP se utiliza en routers que tienen interfaces LAN, como interfaces Ethernet.

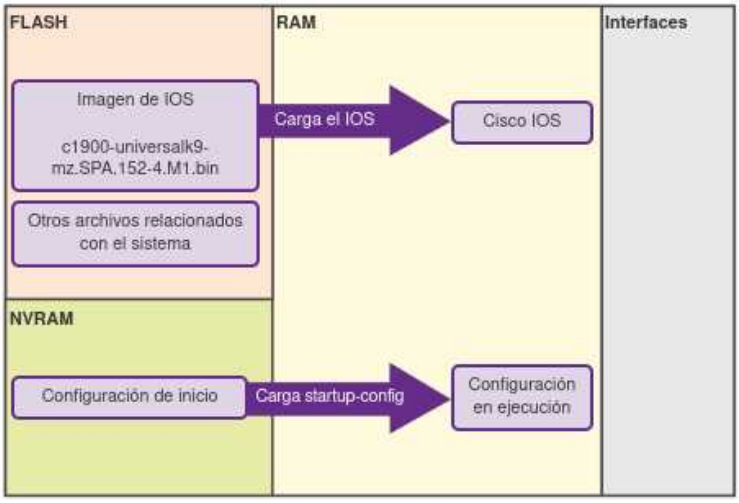
Búfer de paquetes: los paquetes se almacenan temporalmente en un búfer cuando se reciben en una interfaz o antes de salir por una.

Los routers Cisco usan la memoria **ROM** para almacenar lo siguiente:

Instrucciones de arranque: proporcionan las instrucciones de inicio.

Software de diagnóstico básico: realiza el autodiagnóstico al encender (POST) de todos los componentes.

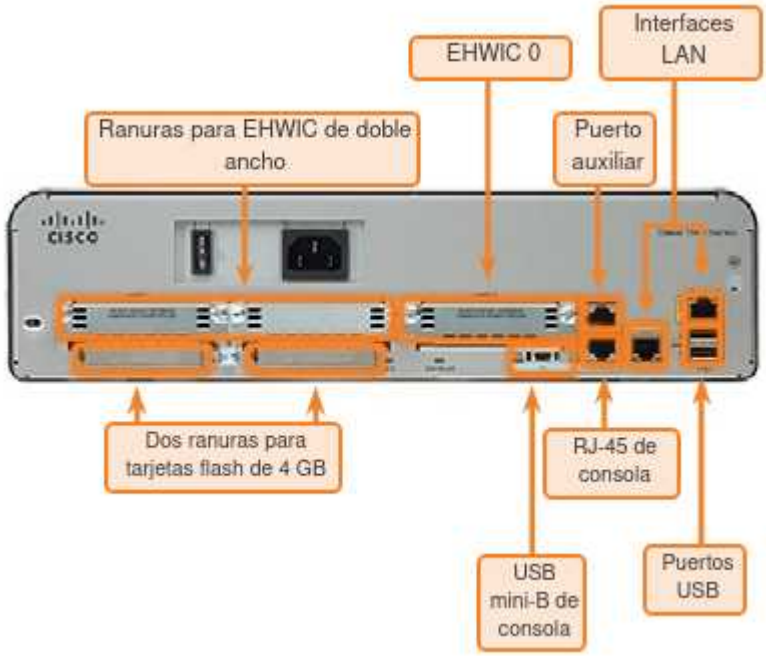
IOS limitado: proporciona una versión limitada de respaldo del OS, en caso de que el router no pueda cargar el IOS con todas las funciones.



El Cisco IOS usa la **NVRAM** como almacenamiento permanente para el archivo de configuración de inicio (**startup-config**). Al igual que la ROM, la NVRAM no pierde el contenido cuando se apaga el dispositivo.

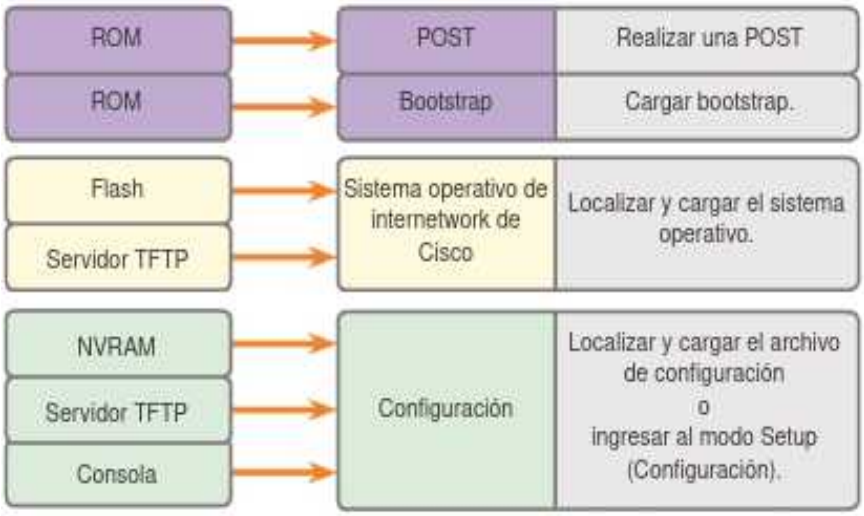
La memoria flash es memoria de PC no volátil que se utiliza como almacenamiento permanente para el IOS y otros archivos relacionados con el sistema. El IOS se copia de la memoria flash a la RAM durante el proceso de arranque.

Ranuras de un router



Ranuras para tarjetas de interfaz WAN de alta velocidad mejoradas (EHWIC): dos ranuras que proporcionan modularidad y flexibilidad al permitir que el router admita distintos tipos de módulos de interfaz, incluidos serial, línea de suscriptor digital (DSL), puerto de switch y tecnología inalámbrica.

Proceso de arranque



La prueba de Autodiagnóstico al encender (**POST**, Power-On Self Test) es un proceso común que ocurre en casi todas las computadoras durante el arranque. El proceso de POST se utiliza para probar el hardware del router. Cuando se enciende el router, el software en el chip de la ROM ejecuta el POST. Durante este autodiagnóstico, el router ejecuta desde la ROM diagnósticos de varios componentes de hardware, incluidos la CPU, la RAM y la NVRAM. Una vez finalizado el POST, el router ejecuta el programa bootstrap.

Después del POST, el programa **bootstrap** se copia de la ROM a la RAM. Una vez en la RAM, la CPU ejecuta las instrucciones del programa bootstrap. La tarea principal del programa bootstrap es ubicar al Cisco IOS y cargarlo en la RAM.

Por lo general, el IOS se almacena en la memoria flash y se copia en la RAM para que lo ejecute la CPU. Durante la autodescompresión del archivo de imagen de IOS, se muestra una cadena de símbolos de almohadilla (#).

Si la imagen de IOS no se encuentra en la memoria flash, el router puede buscarla con un servidor TFTP. Si no se puede localizar una imagen de IOS completa, se copia una versión reducida del IOS de la ROM a la RAM. Esta versión del IOS se usa para ayudar a diagnosticar cualquier problema y puede usarse para cargar una versión completa del IOS en la RAM.

A continuación, el programa bootstrap busca el archivo de configuración de inicio (también conocido como "**startup-config**") en la NVRAM. El archivo contiene los parámetros y comandos de configuración guardados anteriormente. Si existe, se copia en la RAM como archivo de configuración en ejecución o "**running-config**". El archivo running-config contiene direcciones de interfaz, inicia los procesos de enrutamiento, configura las contraseñas del router y define otras características del dispositivo.

Si el archivo startup-config no existe en la NVRAM, el router puede buscar un servidor de protocolo trivial de transferencia de archivos (TFTP). Si el router detecta que tiene un enlace activo a otro router configurado, envía un broadcast en busca de un archivo de configuración a través del enlace activo.

Si no se encuentra un servidor TFTP, el router muestra la petición de entrada del modo Setup. El modo Setup consiste en una serie de preguntas que solicitan al usuario información de configuración básica. El modo Setup no tiene como fin utilizarse para ingresar a configuraciones complejas del router y los administradores de red normalmente no lo usan.

Configuración Routers

Dejando al margen la configuración del router desde la interfaz gráfica y centrándose en la configuración utilizando comandos Cisco, es necesario conocer los diferentes modos de configuración desde la consola, que son los siguientes:

1. Modo EXEC del usuario. Para un análisis limitado del router. Indicador del sistema:

    Router>

2. Modo EXEC privilegiado. Permite el análisis detallado, la depuración y prueba y la manipulación de archivos. Indicador del sistema:

    Router> enable

    Router#

3. Modo de configuración GLOBAL. Habilita los comandos de configuración simples. Indicador del sistema:

    Router# configure terminal

    Router (config)#

4. Modo de configuración del router. Para el acceso a los protocolos de encaminamiento. Indicador del sistema:

    Router (config)# router [bgp/eigrp/ospf/rip/]

    Router (config-router) #

5. Modo de configuración de interfaz. Para la configuración de los parámetros TCP/IP. Indicador del sistema:

    Router (config)# interface FastEthernet 0/1

    Router (config-if)#

6. Modo de configuración de subinterfaz. Para la configuración de parámetros TCP/IP de interfaces lógicas. Indicador del sistema:

    Router (config)# interface FastEthernet 0/1.1

    Router (config-subif)#

Configuración de contraseñas

Se puede poner contraseña a un montón de elementos:

- Contraseña al cable de consola.
- Contraseña de administrador para el modo privilegiado.
- Contraseña al telnet.
- Contraseña SSH.
- Contraseña al puerto auxiliar.

Para poner contraseña a la conexión por cable de consola:

```
Router>enable
Router#configure terminal
Router(config)#line console 0
Router(config-line)#password sesamo1234
Router(config-line)#login
```

Para poner una clave al modo de administrador:

```
Router>enable
Router#configure terminal
Router(config)#enable secret Admin1234!
Router(config)#exit
Router#copy running-config startup-config
Router#reload
Router(config)#service password-encryption
```

El comando Cisco fue durante mucho tiempo «enable password» y de hecho **el comando sigue funcionando**. Sin embargo, `enable password` guarda las claves en la memoria **SIN CIFRAR**.

Poner service password-encryption y enable password es necesario

Acceso por Telnet

Para poner contraseña a Telnet el procedimiento es bastante parecido a lo ya visto:

```
#Nos convertimos en administrador
      Router>enable
#Pasamos al modo de configuración global
      Router#configure terminal
#Seleccionamos las conexiones
      Router(config)#line vty 0 15
#Ponemos una clave de acceso a estas conexiones
      Router(config)# password clave1234!
#Con esto se exigirá el uso de la clave
      Router(config)# login
```

Acceso por SSH

Shell seguro (SSH) es un protocolo que proporciona una conexión de administración segura (cifrada) a un dispositivo remoto. SSH debe reemplazar a Telnet para las conexiones de administración. Telnet es un protocolo más antiguo que usa la transmisión no segura de texto no cifrado de la autenticación de inicio de sesión (nombre de usuario y contraseña) y de los datos transmitidos entre los dispositivos que se comunican. SSH proporciona seguridad para las conexiones remotas mediante el cifrado seguro cuando se autentica un dispositivo (nombre de usuario y contraseña) y también para los datos transmitidos entre los dispositivos que se comunican. SHH se asigna al puerto TCP 22. Telnet se asigna al puerto TCP 23.

Paso 1. Verificar la compatibilidad con SSH

Use el comando **show ip ssh** para verificar que el switch admita SSH. Si el switch no ejecuta un IOS que admita características criptográficas, este comando no se reconoce.

Paso 2. Configurar el dominio IP

Configure el nombre de dominio IP de la red mediante el comando **ip domain-name nombre-de-dominio** del modo de configuración global. Configurar claves públicas de un nodo

Los comandos serían estos para configurar las claves públicas de un nodo:

```
ip domain-name midominio.com
```

Paso 3. Generar pares de claves RSA

```
crypto key generate rsa general-keys modulus 2048
```

```
S1# configure terminal
S1(config)# ip domain-name cisco.com
S1(config)# crypto key generate rsa
The name for the keys will be: S1.cisco.com
...
How many bits in the modulus [512]: 1024
...
S1(config)# username admin password ccna
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config)# end
```

No todas las versiones del IOS utilizan la versión 2 de SSH de manera predeterminada, y la versión 1 de SSH tiene fallas de seguridad conocidas. Para configurar la versión 2 de SSH, emita el comando ip ssh version 2 del modo de configuración global. La creación de un par de claves RSA habilita SSH automáticamente. Use el comando crypto key generate rsa del modo de configuración global para habilitar el servidor SSH en el switch y generar un par de claves RSA. Al crear claves RSA, se solicita al administrador que introduzca una longitud de módulo. Cisco recomienda un tamaño de módulo mínimo de 1024 bits. Una longitud de módulo mayor es más segura, pero se tarda más.

Para eliminar el par de claves RSA, use el comando crypto key zeroize rsa del modo de configuración global. Después de eliminarse el par de claves RSA, el servidor SSH se deshabilita automáticamente.

Paso 4. Configurar la autenticación de usuario

El servidor SSH puede autenticar a los usuarios localmente o con un servidor de autenticación. Para usar el método de autenticación local, cree un nombre de usuario y una contraseña con el comando del modo de configuración global **username nombre-de-usuario secret contraseña**. En el ejemplo, se asignó la contraseña ccna al usuario admin.

Paso 5. Configurar las líneas vty

Habilita el protocolo SSH en las líneas vty mediante el comando transport input ssh del modo de configuración de línea. Esta configuración evita las conexiones que no son SSH (como Telnet) y limita al router a que acepte solo las conexiones SSH. Usa el comando line **vty** del modo de configuración global y, luego, el comando **login local** del modo de configuración de línea para requerir la autenticación local de las conexiones SSH mediante la base de datos de nombres de usuarios locales.

Paso 6. Habilitar la versión 2 de SSH.

De manera predeterminada, SSH admite las versiones 1 y 2. Si se admiten ambas versiones, en el resultado de show ip ssh se muestra que se admite la versión 1.99. La versión 1 tiene vulnerabilidades conocidas. Por esta razón, se recomienda habilitar únicamente la versión 2. Habilita la versión de SSH mediante el comando de configuración global **ip ssh version 2.**

Configuración inicial

```
Router>enable
Router#configure terminal
Enter configuration
commands, one per line.
End with CNTL/Z.
Router(config)#hostname R1
R1(config)#
```

Entramos en modo privilegiado y luego en modo configuración global.
Establecemos el nombre del router

```
R1(config)#enable secret class
R1(config)#
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
R1(config)#service password-encryption
R1(config)#
```

Establecemos una password para el modo privilegiado y otra para la entrada por consola.

Establecemos una password para la entrada por linea externa (telnet o ssh)

```
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Guardamos la configuración

Configuración de las interfaces

Para que los routers sean accesibles, se deben configurar sus interfaces poniendo su dirección IP

```
R1(config)#
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#description Link to LAN-10
R1(config-if)#no shutdown
```

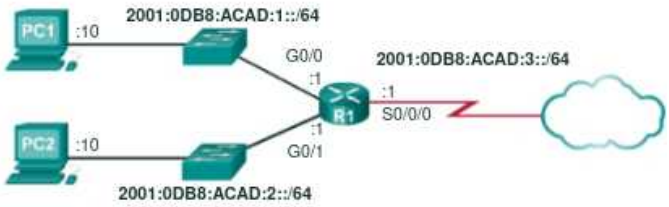
show ip interface brief. Se muestran todas las interfaces, sus direcciones IP y su estado actual. Las interfaces configuradas y conectadas deben mostrar el valor “up” (conectado) en Status (Estado) y en Protocol (Protocolo). Cualquier otro valor indicaría un problema con la configuración o el cableado.

show ip route : muestra el contenido de la tabla de enrutamiento IPv4 almacenada en la RAM.
Para que un dispositivo final se comunique a través de la red, se debe configurar con la información de dirección IP correcta, incluida la dirección de **gateway predeterminado**. El gateway predeterminado se utiliza solo cuando el host desea enviar un paquete a un dispositivo en otra red. Por lo general, la dirección de gateway predeterminado es la dirección de la interfaz del router asociada a la red local del host. Si bien no importa qué dirección se configura realmente en la interfaz del router, la dirección IP del dispositivo host y la dirección de la interfaz del router deben estar en la misma red.

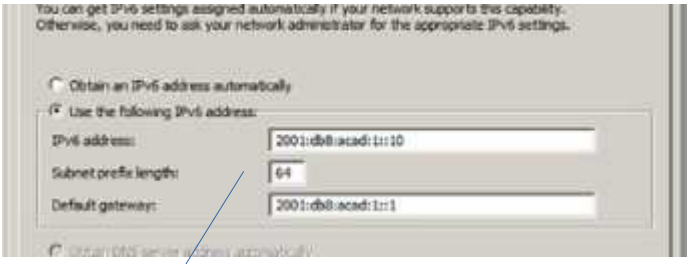
La mayoría de los comandos de configuración y verificación IPv6 de Cisco IOS son similares a sus equivalentes de IPv4. En muchos casos, la única diferencia es el uso de ipv6 en lugar de ip dentro de los comandos.
Para habilitar un router como router IPV6 hay que utilizar el comando **ipv6 unicast-routing**

Configurar dirección unicast global

El comando interface que se utiliza para configurar una dirección IPv6 unicast global en una interfaz es **ipv6 address dirección_ipv6/duración de prefijo**. No hay un espacio entre dirección ipv6 y duración de prefijo.




```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ipv6 address 2001:db8:acad:2::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ipv6 address 2001:db8:acad:3::1/64
R1(config-if)#clock rate 56000
R1(config-if)#no shutdown
```



Configuración del host

Configuración de las tres interfaces del router

Configurar link-local manual

```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ipv6 address fe80::1 ?
  link-local  Use link-local address

R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#
```

La dirección link-local FE80::1 se utiliza para que sea posible reconocer fácilmente que pertenece al router R1. Se configura la misma dirección IPv6 link-local en todas las interfaces de R1. Se puede configurar FE80::1 en cada enlace, debido a que solamente tiene que ser única en ese enlace.

De manera similar a R1, el router R2 se configuraría con FE80::2 como la dirección IPv6 link-local en todas sus interfaces.

Enrutamiento estático

R1(config)# **ip route <red destino> <mascara> <ip del siguiente salto>**

R1(config)# **ip route 0.0.0.0 0.0.0.0 <ip del router por defecto>**

ACL

Mostrar las ACL

router# **show access-lists**

Definir una ACL

standard : **access-list numeroACL {permit | deny} origen [Wildcard-origen]**

Extendida : **access-list numeroACL {permit | deny} protocolo origen [Wildcard-origen] destino [Wildcard-destino] [operación] [puerto destino] [established]**

ejemplos:

access-list 10 permit 192.168.32.0 0.0.7.255

Borrar una ACL

no access-list acl-number {permit | deny} origen [Wildcard-origen]
no access-list acl-number
Ojo! Borrarmos la ACL entera!

Aplicar una ACL a una interfaz

ip access-group <acl-number | nombre> {in | out}

ejemplos:

Router(config)# **interface Fastethernet 0/2**
Router(config-if)# **ip access-group 1 out**

Dejar de aplicar una ACL

ip access-group {acl-number | nombre} {in | out}

Edición avanzada

ip access-list {standard | extended} {numero | nombre}