

Configuración básica del router usando el Cisco Configuration Professional

Contenido

[Introducción](#)

[prerrequisitos](#)

[Componentes Utilizados](#)

[Instale al Cisco Configuration Professional](#)

[Configuración del router para ejecutar Cisco CP](#)

[Requisitos](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración de la Interfaz](#)

[Configuración de NAT](#)

[Configuración de Ruteo](#)

[Configuraciones Miceláneas](#)

[Configuración de CLI](#)

[Verificación](#)

[Troubleshooting](#)

[¿Cómo puedo cambiar el Nombre de usuario y la contraseña para el router?](#)

[Recibo un error interno cuando utilizo al Internet Explorer 8 para acceder Cisco CP. ¿Cómo resuelvo este problema?](#)

[Recibo este mensaje de error cuando intento instalar Cisco CP: "Incapaz de leer el archivo de origen. El archivo podía ser corrompido. Reinstale por favor al Cisco Configuration Professional para resolver el problema." ¿Cómo resuelvo este problema?](#)

[¿Cómo accedo los registros técnicos de Cisco CP?](#)

[El descubrimiento de enrutador tarda más tiempo que usual. ¿Cómo resuelvo este problema?](#)

[No puedo ver la página de configuración IPS en Cisco CP. ¿Cómo resuelvo este problema?](#)

[Información Relacionada](#)

[Introducción](#)

Este documento describe cómo utilizar Cisco Configuration Professional (Cisco CP) para establecer la configuración básica del router. La configuración básica del router incluye la configuración de la dirección IP, el ruteo predeterminado, los parásitos atmosféricos y el Dynamic Routing, el NATing estático y dinámico, el nombre del host, el banner, la contraseña secreta, las cuentas de usuario, y las otras opciones. Cisco CP permite que usted configure a su router en varios entornos de red, tales como Small Office Home Office (SOHO), sucursal (BO), oficina regional, y sitio central o jefaturas de la empresa, con una Interfaz de administración basado en la Web fácil de usar.

Para más información sobre el Cisco Configuration Professional, refiera a la [guía de inicio rápido del Cisco Configuration Professional](#).

prerrequisitos

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

Cisco 2811 Router con la versión del Cisco IOS ® Software 12.4(9)

Versión 2.5 de Cisco CP

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Instale al Cisco Configuration Professional

Realice estos pasos para instalar el CCP:

Descargue Cisco CP V2.5 del [centro del software de Cisco \(clientes registrados solamente\)](#) y instalelo en su PC local.

La última versión de Cisco CP se puede encontrar en el [sitio web CCP](#).

Inicie Cisco CP de su PC local a través **Start > Programs > Cisco Configuration Professional** y elija a la **comunidad** que tiene el router que usted quiere configurar.

Para descubrir el dispositivo que usted quiere configurar, resaltar al router y hacer clic el botón del **descubrimiento**.

Note: Para la información sobre los modelos y las versiones del IOS del router Cisco que son compatibles a CCPv2.5, refiera a la sección [compatible de las versiones del Cisco IOS](#).

Note: Para la información sobre los requisitos PC que ejecuta CCPv2.5, refiera a la sección de los [requisitos del sistema](#)

Configuración del router para ejecutar Cisco CP

Realice estos pasos para la configuración para ejecutar Cisco CP en un router Cisco:

Conecte con su router que usa Telnet, SSH, o a través de la consola.

Ingrese al modo de configuración global que usa este comando:

```
Router(config)#enable
```

```
Router(config)#
```

Si el HTTP y el HTTPS se habilitan y se configuran para utilizar los números del puerto no estándar, usted puede saltar este paso y utilizar simplemente el número del puerto configurado ya.

Habilite el router HTTP o al servidor HTTPS que usa estos comandos del Cisco IOS Software:

```
Router(config)# ip http server
Router(config)# ip http secure-server
Router(config)# ip http authentication local
```

Cree a un usuario con el nivel de privilegio 15:

```
Router(config)# username <username> privilege 15 password 0 <password>
```

Note: *<username>* y *<password>* del reemplace con el nombre de usuario y contraseña que usted quiere configurar. No utilice la misma contraseña para su usuario y contraseñas habilitadas.

Configure SSH y Telnet para la conexión local y el nivel de privilegio 15.

```
Router(config)# line vty 0 4
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# exit
```

(Opcional) permita al registro local para soportar la función de supervisión del registro:

```
Router(config)# logging buffered 51200 warning
```

Requisitos

Este documento asume que el router Cisco está completamente - operativo y configurado para permitir que Cisco CP realice los cambios de configuración.

Para toda la información sobre cómo comenzar a usar Cisco CP, refiera a la [introducción con el Cisco Configuration Professional](#).

Convenciones

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

Configurar

En esta sección, le presentan con la información para configurar las configuraciones básicas para un router en una red.

Note: Utilice la herramienta [Command Lookup Tool](#) ([clientes registrados solamente](#)) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Note: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son las direcciones [RFC1918](#) que se han utilizado en un entorno de laboratorio.

Configuración de la Interfaz

Realice estos pasos para configurar las interfaces de un router Cisco:

Haga clic **a casa** para ir al homepage de Cisco CP.

El homepage de Cisco CP proporciona la información tal como el hardware y software del router, de la disponibilidad de la función, y de un resumen de la configuración.

Elija la **configuración** > la **administración de la interfaz** > las **interfaces y las conexiones** > **crean la conexión** para configurar la conexión WAN para la interfaz.

Como un ejemplo, para el FastEthernet0/1, elija la opción de los **Ethernetes** y el tecleo **crea la nueva conexión**.

Note: Para otros tipos de interfaces como los **Ethernetes**, elija el tipo de interfaz respectiva y el tecleo **crea la nueva conexión** para proceder.

Haga clic **después** para proceder una vez que aparece esta interfaz:

Elija el **FastEthernet0/1** (deseado) de la opción de interfaces disponible y haga clic **después**.

Especifique la dirección IP estática con la máscara de subred correspondiente para la interfaz y haga clic en **Siguiente**.

Configure el ruteo predeterminado con los parámetros optativos tales como el IP Address de Next Hop (172.16.1.2 según el diagrama de la red) suministrado por el ISP y haga clic **después**.

Esta ventana aparece y muestra el resumen de la configuración configurado por el usuario.

Haga clic en Finish (Finalizar).

Note: La Conectividad de la configuración puede ser marcada marcando el checkbox al lado de la **prueba la Conectividad después de configurar**. Esto es una característica opcional disponible.

Esta ventana aparece y muestra el estado de salida de comando al router. De lo contrario, muestra los errores si la salida del comando falla debido a que los comandos son incompatible o las funciones no son soportadas.

Elija la **configuración > la administración de la interfaz > las interfaces y las conexiones > editan las interfaces/las conexiones** para agregar/los editan/cancelación las diversas interfaces.

Resalte la interfaz con la cual desea hacer cambios y haga clic en **Editar** si desea editar o cambiar la configuración de la interfaz. Aquí, usted puede cambiar el IP Address estático existente.

[Configuración de NAT](#)

[Configuración de NAT dinámica](#)

Realice estos pasos para configurar el NAT dinámico en un router Cisco:

Elija la **configuración > el Router> NAT > NAT básico** y haga clic el **lanzamiento la tarea seleccionada** para configurar el NATing básico.

Haga clic en Next (Siguiente).

Elija la interfaz que conecta con Internet o su ISP y elija el alcance del IP Address al cual el acceso a internet debe ser compartido. Después de elegir esta información, haga clic **después** como se muestra aquí:

Esta ventana aparece y muestra el resumen de la configuración configurado por el usuario. Haga clic en Finish (Finalizar).

La ventana Editar Configuración del NAT muestra la configuración NAT dinámica configurada con la dirección IP traducida sobrecargada (PATing). Si desea configurar la NATing dinámica con el pool de direcciones, haga clic en **Pool de Direcciones**.

Haga clic en Add (Agregar).

Aquí, la información tal como el nombre del pool y el alcance del IP Address con el netmask se proporcionan. Puede haber casos en los que la mayor parte de las direcciones en el pool se ha asignado, y el pool de dirección IP queda prácticamente agotado. Cuando ocurre esto, la PALMADITA se puede utilizar con una sola dirección IP para satisfacer los pedidos adicionales los IP Addresses. Verifique **Traducción de Dirección de Puerto (PAT)** si desea que el router use PAT cuando el pool de direcciones está próximo a agotarse. Click OK.

Haga clic en Add (Agregar).

Haga clic en **Editar**.

Elija a la **agrupación de direcciones** en el campo del tipo, proporcione el nombre a la agrupación de direcciones como **pool**, y haga clic la **AUTORIZACIÓN**.

Esta ventana muestra la configuración para la NATing dinámica con el pool de direcciones. Haga clic en **Designar Interfaces NAT**.

Utilice esta ventana para señalar las interfaces interior y exterior que usted quiere utilizar en traducciones de NAT. La NAT utiliza las designaciones internas y externas cuando interpreta las reglas de traducción, porque las traducciones se realizan desde el interior al exterior, o viceversa.

Una vez que están designadas, estas interfaces se utilizan en todas las reglas de traducción de NAT. Las interfaces designadas aparecen en la parte superior de la lista de las reglas de traducción en la ventana principal NAT.

[Configuración de NAT Estática](#)

Realice estos pasos para configurar el NAT estático en un router Cisco:

Elija la **configuración** > el **Router**> **NAT** > **editan la configuración del NAT** y el tecleo **agrega** para configurar el NATing estático.

Elija la **dirección** desde adentro a exterior o del exterior a dentro, y especifique la dirección IP interior que se traducirá debajo **traducen de la interfaz**. Para que el **traducir interconecte el** área, elija el tipo:

Elija **Dirección IP** si desea que Traducir desde Dirección se traduzca a una dirección IP definida en el campo Dirección IP.

Elija **Interfaz** si desea que **Traducir de esa Dirección** use la dirección de una interfaz en el router. **Traducir desde Dirección** es traducido a la dirección IP asignada a la interfaz que especifica en el campo Interfaz.

Haga clic en **Redireccionar Puerto** si desea incluir información de puerto para el dispositivo interno en la traducción. Esto lo habilita a utilizar la misma dirección IP pública para los dispositivos múltiples, siempre que el puerto especificado para cada dispositivo sea diferente. Debe crear una entrada para cada mapping de puerto para esta dirección Traducida a. Haga clic en **TCP** si es un número de puerto TCP y haga clic en **UDP** si es un número de puerto UDP. En el campo de Puerto Original, ingrese el número de puerto en el dispositivo interno. En el campo Puerto Traducido, ingrese el número de puerto que el router usará para esta traducción. Consulte la sección [Cómo Permitir que Internet Acceda a Dispositivos Internos](#) de [Configuración de Traducción de Dirección de Red: Introducción](#).

Esta ventana muestra la configuración estática del NATing con la redirección de puerto habilitada:

[Configuración de Ruteo](#)

[Configuración de Ruteo Estático](#)

Realice estos pasos para configurar el Static Routing en un router Cisco:

Elija los **parásitos atmosféricos de la configuración > del Router> y el Dynamic Routing** y el tecleo **agregan** para configurar el Static Routing.

Ingrese el direccionamiento de red de destino con la máscara y elija la interfaz saliente o el IP Address de Next Hop.

Esta ventana muestra la Static ruta configurada para la red de 10.1.1.0 con 172.16.1.2 como el IP Address de Next Hop:

[Configuración de Ruteo Dinámico](#)

Realice estos pasos para configurar el Dynamic Routing en un router Cisco:

Elija la **configuración > los parásitos atmosféricos y el Dynamic Routing del Router>**.

Seleccione el **RIP** y haga clic en **Editar**.

El RIP del permiso del control, elige la versión de RIP, y el haga click en Add

Especifique la Dirección de Red que se anunciará.

Click OK.

Haga clic en **Entregar** para transferir los comandos al router.

Esta ventana muestra la configuración de ruteo dinámica del RIP:

[Configuraciones Miceláneas](#)

Realice estos pasos para configurar las otras configuraciones básicas en un router Cisco:

Elija las **opciones del router de la configuración > del Router>** y el tecleo **edita** si usted quiere cambiar las propiedades del nombre de host, del Domain Name, del banner, y de la contraseña enable secret para un router.

Elija la **configuración** > el **acceso al router** > las **cuentas de usuario/visión** para agregar/editelos/cancelación las cuentas de usuario al router.

Elija la **configuración** > las **utilidades** > los **Config corrientes de la salvaguardia al PC** para salvar la configuración al NVRAM del router así como al PC y reajustar la configuración actual para omitir las configuraciones (de la fábrica).

Note: Para utilizar el CCP para restablecer el archivo de configuración salvó en un ordenador a un router o respaldo el archivo de configuración de un router a un ordenador, accede el editor de la configuración, y el tecleo que **estoy de acuerdo**. En la ventana de la configuración, elija la **configuración de la importación del PC**, y después haga clic el botón **corriente de la configuración del reemplazo**.

Configuración de CLI

Configuración del router

```
Router#show run
Building configuration...

Current configuration : 2525 bytes
! version 12.4 service timestamps debug datetime msec
service timestamps log datetime msec no service
password-encryption ! hostname Router ! boot-start-
marker boot-end-marker ! no logging buffered enable
password cisco ! no aaa new-model ! resource policy ! !
! ip cef ! ! ! !--- RSA certificate generated after you
enable the !--- ip http secure-server command.

crypto pki trustpoint TP-self-signed-2401602417
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-2401602417
  revocation-check none
  rsakeypair TP-self-signed-2401602417

crypto pki certificate chain TP-self-signed-2401602417
  certificate self-signed 01
    30820248 308201B1 A0030201 02020101 300D0609 2A864886
F70D0101 04050030
    31312F30 2D060355 04031326 494F532D 53656C66 2D536967
6E65642D 43657274
    69666963 6174652D 32343031 36303234 3137301E 170D3130
30353139 30393031
    31315A17 0D323030 31303130 30303030 305A3031 312F302D
06035504 03132649
    4F532D53 656C662D 5369676E 65642D43 65727469 66696361
74652D32 34303136
    30323431 3730819F 300D0609 2A864886 F70D0101 01050003
818D0030 81890281
    8100CD35 A3A6E322 9B6005DA A0FF26C2 8A0DC5AF 27B38F3B
DBF2BF58 D8F2655D
    31115681 EC8BC750 03FE3A25 0F79DC74 3A839496 CB9486F1
A1F5BF43 D92BA7AF
    3C72A57B D8D37799 50493588 A5A18F7F 27955AB0 AC36B560
3BE9F648 A4F6F41F
    B9E9C5E6 F9570DEB 5555FDED 9593BD00 5ABB30CD D3B9BDF
A
F570F987 651652CE
    3D310203 010001A3 70306E30 0F060355 1D130101 FF040530
```



```
030101FF 301B0603
 551D1104 14301282 10526F75 7465722E 70616D6D 692E636F
6D301F06 03551D23
 04183016 80146A0A C2100122 EFDA58AB C319820D 98256622
52C5301D 0603551D
 0E041604 146A0AC2 100122EF DA58ABC3 19820D98 25662252
C5300D06 092A8648
 86F70D01 01040500 03818100 83B0EC8C 6916178F 587E15D6
5485A043 E7BB258D
 0C9A63F2 DA18793D CACC026E BC0B9B33 F8A27B34 5BD7DD7F
FCECA34F 04662AEC
 07FD7677 A90A8D1C 49042963 C2562FEC 4EFFF17C 360BF88A
FEDC7CAA AE308F6C
 A5756C4A F574F5F3 39CE14AE BAAEC655 D5920DD0 DA76E296
B246E36E 16CFBC5A
 00974370 170BBDAD C1594013
quit
```

```
!!!!!!!!--- Create a user account named ccpccp
with all privileges.
```

```
username ccpccp privilege 15 password 0 cisco123
archive
 log config
  hidekeys
```

```
!!!!!!!--- The LAN interface configured with a
private IP address. interface FastEthernet0/0
description $ETH-LAN$ ip address 192.168.1.1
255.255.255.0 !--- Designate that traffic that
originates from behind !--- the interface is subject to
Network Address Translation (NAT). ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
```

```
!!--- This is the LAN interface configured with a
routable (public) IP address. interface FastEthernet0/1
description $ETH-WAN$ ip address 172.16.1.1
255.255.255.0 !--- Designate that this interface is the
!--- destination for traffic that has undergone NAT. ip
nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
```

```
!!!--- RIP version 2 routing is enabled. router rip
version 2 network 192.168.1.0 no auto-summary !--- This
is where the commands to enable HTTP and HTTPS are
configured. ip http server ip http authentication local
ip http secure-server !!--- This configuration is for
dynamic NAT. !
```

```
!--- Define a pool of outside IP addresses for NAT. ip
nat pool pool 10.10.10.1 10.10.10.100 netmask
255.255.255.0 !--- In order to enable NAT of the inside
source address, !--- specify that traffic from hosts
that match access list 1 !--- are NATed to the address
pool named pool1. ip nat inside source list 1 pool pool1
!!--- Access list 1 permits only 122.168.1.0 network to
be NATed. access-list 1 remark CCP_ACL Category=2
access-list 1 permit 192.168.1.0 0.0.0.255 !!--- This
```

```
configuration is for static NAT !--- In order to
translate the packets between the real IP address
10.10.10.1 with TCP !--- port 80 and the mapped IP
address 172.16.1.1 with TCP port 500. !
```

```
ip nat outside source static tcp 10.10.10.1 8080
172.16.1.1 80 extendable
! ! ! ! !--- The default route is configured and points
to 172.16.1.2. ip route 0.0.0.0 0.0.0.0 172.16.1.2 ! ! !
! control-plane ! ! ! ! ! ! ! ! ! ! line con 0 line aux
0 !--- Telnet enabled with password as cisco. line vty 0
4 password cisco transport input all line vty 5 15
password cisco transport input all ! ! ! end
```

Verificación

Elija **Configure > Interface & Connections > Edit Interface Connections > Test Connection** para evaluar la conectividad de un extremo a otro. Puede especificar la dirección IP remota final si hace clic en el botón de opción **definido por el usuario**.

Troubleshooting

La herramienta [Output Interpreter Tool \(clientes registrados solamente\)](#) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Note: Consulte [información importante en los comandos debug](#) antes de ejecutar los comandos debug.

Puede utilizar estas opciones para resolver problemas:

Elija el **Help (Ayuda) > About (Acerca de) este router** para ver a los detalles del hardware y software del router.

La opción de **ayuda** proporciona la información sobre las diversas opciones disponibles en Cisco CP para la configuración del router.

¿Cómo puedo cambiar el Nombre de usuario y la contraseña para el router?

Usted puede cambiar el nombre y la contraseña de usuario del router con Cisco CP. Complete estos pasos para cambiar el Nombre de usuario y la contraseña:

Cree una nueva cuenta de usuario temporal, y después inicie sesión a la cuenta de usuario temporal.

Cambie el Nombre de usuario y la contraseña de la cuenta de usuario principal (es decir, la cuenta de usuario del router en quien usted quiere cambiar el Nombre de usuario y la contraseña) en su Cisco CP.

Termine la sesión de la cuenta temporal, y del login a la cuenta de usuario principal.

Borre la cuenta de usuario temporal después de que usted cambie la contraseña para la cuenta principal.

[Recibo un error interno cuando utilizo al Internet Explorer 8 para acceder Cisco CP. ¿Cómo resuelvo este problema?](#)

Problema

Usted puede ser que reciba este error interno cuando usted utiliza al Internet Explorer 8 para configurar al 2800 Series Router que usa Cisco CP:

```
Error interno: [Fault= de FaultEvent [el faultString= " Send del incidente RPC falló" error
NetConnection.Call.Failed Channel.Connect.Failed del faultDetail= el " "
Client.Error.MessageSend del faultCode=": HTTP: Estatus 200: URL: cancelable=true eventPhase=2]
del bubbles=false del " incidente" del type= 'http://localhost:8600/messagebroker/amf'] el
messageId="A08846FF-E7C6-F578-7C38-61C6E94899C7"
```

La degradación de las Javas no resuelve el problema.

Solución

Este error pudo ser el resultado de un problema de la compatibilidad del buscador. El Internet Explorer 8 cambia muchos aspectos fundamentales de desarrollar las aplicaciones para el IE. Cisco recomienda que usted retrocede al Internet Explorer a la versión 7. Usted debe también desinstalar y reinstalar Cisco CP.

[Recibo este mensaje de error cuando intento instalar Cisco CP: "Incapaz de leer el archivo de origen. El archivo podía ser corrompido. Reinstale por favor al Cisco Configuration Professional para resolver el problema." ¿Cómo resuelvo este problema?](#)

Problema

Cuando usted descarga el archivo de configuración de la aplicación e intenta instalar Cisco CP, usted puede ser que reciba este error:

```
Router#show run
Building configuration...
```

```
Current configuration : 2525 bytes
! version 12.4 service timestamps debug datetime msec service timestamps log datetime msec no
service password-encryption ! hostname Router ! boot-start-marker boot-end-marker ! no logging
buffered enable password cisco ! no aaa new-model ! resource policy ! ! ! ip cef ! ! ! !--- RSA
certificate generated after you enable the !--- ip http secure-server command.
```

```
crypto pki trustpoint TP-self-signed-2401602417
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-2401602417
  revocation-check none
  rsakeypair TP-self-signed-2401602417
```

```
crypto pki certificate chain TP-self-signed-2401602417
  certificate self-signed 01
```

```
30820248 308201B1 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
69666963 6174652D 32343031 36303234 3137301E 170D3130 30353139 30393031
31315A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 34303136
30323431 3730819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
8100CD35 A3A6E322 9B6005DA A0FF26C2 8A0DC5AF 27B38F3B DBF2BF58 D8F2655D
31115681 EC8BC750 03FE3A25 0F79DC74 3A839496 CB9486F1 A1F5BF43 D92BA7AF
3C72A57B D8D37799 50493588 A5A18F7F 27955AB0 AC36B560 3BE9F648 A4F6F41F
B9E9C5E6 F9570DEB 5555FDED 9593BD00 5ABB30CD D3B9BDFA F570F987 651652CE
3D310203 010001A3 70306E30 0F060355 1D130101 FF040530 030101FF 301B0603
551D1104 14301282 10526F75 7465722E 70616D6D 692E636F 6D301F06 03551D23
04183016 80146A0A C2100122 EFDA58AB C319820D 98256622 52C5301D 0603551D
0E041604 146A0AC2 100122EF DA58ABC3 19820D98 25662252 C5300D06 092A8648
86F70D01 01040500 03818100 83B0EC8C 6916178F 587E15D6 5485A043 E7BB258D
0C9A63F2 DA18793D CACC026E BC0B9B33 F8A27B34 5BD7DD7F FCECA34F 04662AEC
07FD7677 A90A8D1C 49042963 C2562FEC 4EFFF17C 360BF88A FEDC7CAA AE308F6C
A5756C4A F574F5F3 39CE14AE BAAEC655 D5920DD0 DA76E296 B246E36E 16CFBC5A
00974370 170BBDAD C1594013
```

quit

!!!!!!!!--- Create a user account named **ccpccp** with all privileges.

```
username ccpccp privilege 15 password 0 cisco123
archive
log config
hidekeys
```

```
!!!!!!!!--- The LAN interface configured with a private IP address. interface
FastEthernet0/0 description $ETH-LAN$ ip address 192.168.1.1 255.255.255.0 !--- Designate that
traffic that originates from behind !--- the interface is subject to Network Address Translation
(NAT). ip nat inside
ip virtual-reassembly
duplex auto
speed auto
```

```
!--- This is the LAN interface configured with a routable (public) IP address. interface
FastEthernet0/1 description $ETH-WAN$ ip address 172.16.1.1 255.255.255.0 !--- Designate that
this interface is the !--- destination for traffic that has undergone NAT. ip nat outside
ip virtual-reassembly
duplex auto
speed auto
```

```
!--- RIP version 2 routing is enabled. router rip version 2 network 192.168.1.0 no auto-
summary !--- This is where the commands to enable HTTP and HTTPS are configured. ip http server
ip http authentication local ip http secure-server !!--- This configuration is for dynamic NAT.
!
```

```
!--- Define a pool of outside IP addresses for NAT. ip nat pool pool 10.10.10.1 10.10.10.100
netmask 255.255.255.0 !--- In order to enable NAT of the inside source address, !--- specify
that traffic from hosts that match access list 1 !--- are NATed to the address pool named pool1.
ip nat inside source list 1 pool pool1 !!--- Access list 1 permits only 192.168.1.0 network to
be NATed. access-list 1 remark CCP_ACL Category=2 access-list 1 permit 192.168.1.0 0.0.0.255 !
!--- This configuration is for static NAT !--- In order to translate the packets between the
real IP address 10.10.10.1 with TCP !--- port 80 and the mapped IP address 172.16.1.1 with TCP
port 500. !
```

```
ip nat outside source static tcp 10.10.10.1 8080 172.16.1.1 80 extendable
!!!!!--- The default route is configured and points to 172.16.1.2. ip route 0.0.0.0 0.0.0.0
172.16.1.2 !!!!! control-plane !!!!! line con 0 line aux 0 !--- Telnet enabled
with password as cisco. line vty 0 4 password cisco transport input all line vty 5 15 password
```

```
cisco transport input all ! ! ! end
```

Solución

Intente el siguiente para resolver esto.

Borre todos los casos de Cisco CP en su PC, y realice una descarga fresca y instalela.

Si el paso anterior no trabaja, intente descargar una diversa versión de Cisco CP.

Si el paso anterior no trabaja, entrar en contacto el [TAC de Cisco](#).

Note: Usted debe tener credenciales válidas del Usuario Cisco para entrar en contacto el TAC de Cisco.

¿Cómo accedo los registros técnicos de Cisco CP?

El tecleo **Start > Programs > Cisco Systems > Cisco Configuration Professional > recoge los datos para el soporte técnico**. Cisco CP archiva automáticamente abre una sesión archivo zip un `_ccptech.zip` Nombrado. *Realice una* búsqueda del sistema de archivo local para este archivo si no se guarda a su escritorio. Usted puede enviar estos registros técnicos a [CiscoTAC para el troubleshooting](#) adicional.

Note: Cierre todos los casos de Cisco CP para librarse de cualquier otro problema en archivar los registros.

El descubrimiento de enrutador tarda más tiempo que usual. ¿Cómo resuelvo este problema?

Problema

Una vez que se inicia Cisco CP y configuran a la comunidad, la detección del router tarda más tiempo que usual. Aquí están los registros de Cisco CP que describen el tiempo transcurrieron:

```
Router#show run
Building configuration...

Current configuration : 2525 bytes
! version 12.4 service timestamps debug datetime msec service timestamps log datetime msec no
service password-encryption ! hostname Router ! boot-start-marker boot-end-marker ! no logging
buffered enable password cisco ! no aaa new-model ! resource policy ! ! ! ip cef ! ! ! !--- RSA
certificate generated after you enable the !--- ip http secure-server command.

crypto pki trustpoint TP-self-signed-2401602417
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-2401602417
  revocation-check none
  rsakeypair TP-self-signed-2401602417

crypto pki certificate chain TP-self-signed-2401602417
  certificate self-signed 01
    30820248 308201B1 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
    31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
```

```
69666963 6174652D 32343031 36303234 3137301E 170D3130 30353139 30393031
31315A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 34303136
30323431 3730819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
8100CD35 A3A6E322 9B6005DA A0FF26C2 8A0DC5AF 27B38F3B DBF2BF58 D8F2655D
31115681 EC8BC750 03FE3A25 0F79DC74 3A839496 CB9486F1 A1F5BF43 D92BA7AF
3C72A57B D8D37799 50493588 A5A18F7F 27955AB0 AC36B560 3BE9F648 A4F6F41F
B9E9C5E6 F9570DEB 5555FDED 9593BD00 5ABB30CD D3B9BDFA F570F987 651652CE
3D310203 010001A3 70306E30 0F060355 1D130101 FF040530 030101FF 301B0603
551D1104 14301282 10526F75 7465722E 70616D6D 692E636F 6D301F06 03551D23
04183016 80146A0A C2100122 EFDA58AB C319820D 98256622 52C5301D 0603551D
0E041604 146A0AC2 100122EF DA58ABC3 19820D98 25662252 C5300D06 092A8648
86F70D01 01040500 03818100 83B0EC8C 6916178F 587E15D6 5485A043 E7BB258D
0C9A63F2 DA18793D CACC026E BC0B9B33 F8A27B34 5BD7DD7F FCECA34F 04662AEC
07FD7677 A90A8D1C 49042963 C2562FEC 4EFFF17C 360BF88A FEDC7CAA AE308F6C
A5756C4A F574F5F3 39CE14AE BAAEC655 D5920DD0 DA76E296 B246E36E 16CFBC5A
00974370 170BBDAD C1594013
quit
```

!!!!!!! *!--- Create a user account named cpcpcp with all privileges.*

```
username cpcpcp privilege 15 password 0 cisco123
archive
log config
hidekeys
```

!!!!!! *!--- The LAN interface configured with a private IP address.* interface
FastEthernet0/0 description \$ETH-LAN\$ ip address 192.168.1.1 255.255.255.0 *!--- Designate that traffic that originates from behind !--- the interface is subject to Network Address Translation (NAT).* ip nat inside
ip virtual-reassembly
duplex auto
speed auto

! *!--- This is the LAN interface configured with a routable (public) IP address.* interface
FastEthernet0/1 description \$ETH-WAN\$ ip address 172.16.1.1 255.255.255.0 *!--- Designate that this interface is the !--- destination for traffic that has undergone NAT.* ip nat outside
ip virtual-reassembly
duplex auto
speed auto

!! *!--- RIP version 2 routing is enabled.* router rip version 2 network 192.168.1.0 no auto-summary *!--- This is where the commands to enable HTTP and HTTPS are configured.* ip http server
ip http authentication local ip http secure-server ! *!--- This configuration is for dynamic NAT.*
!

!--- Define a pool of outside IP addresses for NAT. ip nat pool pool 10.10.10.1 10.10.10.100 netmask 255.255.255.0 *!--- In order to enable NAT of the inside source address, !--- specify that traffic from hosts that match access list 1 !--- are NATed to the address pool named pool1.*
ip nat inside source list 1 pool pool1 ! *!--- Access list 1 permits only 192.168.1.0 network to be NATed.* access-list 1 remark CCP_ACL Category=2 access-list 1 permit 192.168.1.0 0.0.0.255 ! *!--- This configuration is for static NAT !--- In order to translate the packets between the real IP address 10.10.10.1 with TCP !--- port 80 and the mapped IP address 172.16.1.1 with TCP port 500. !*

```
ip nat outside source static tcp 10.10.10.1 8080 172.16.1.1 80 extendable
!!!! !--- The default route is configured and points to 172.16.1.2. ip route 0.0.0.0 0.0.0.0 172.16.1.2 !!!!! control-plane !!!!! line con 0 line aux 0 !--- Telnet enabled with password as cisco. line vty 0 4 password cisco transport input all line vty 5 15 password cisco transport input all !!! end
```

Este problema ocurre con todo el Routers con independencia de su modelo y plataforma.

Además, no hay memoria o asuntos relacionados CPU en el Routers.

Solución

Verifique al modo de autenticación. Si no ocurre la autenticación localmente, después marque si hay un problema con el servidor de autenticidad. Repare cualquier problema con el servidor de autenticidad para resolver este problema.

[No puedo ver la página de configuración IPS en Cisco CP. ¿Cómo resuelvo este problema?](#)

Problema

Cuando una característica específica en la ventana de configuración no muestra cualquier cosa excepto una página en blanco, pudo haber los problemas de incompatibilidad.

Solución

Verifique estos elementos para resolver este problema:

Verifique si esa característica específica se soporta y se habilita en su modelo de router.

Verifique si sus soportes de la versión del router que ofrezcan. Las incompatibilidades de la versión del router se podían resolver con una actualización de la versión.

Verifique si el problema está con la autorización actual.

Información Relacionada

- [Guía de inicio rápido del Cisco Configuration Professional](#)
- [Páginas de Soporte de Productos de Cisco - Routers](#)
- [Página de Soporte de NAT](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)