

Configuración del Acceso Telnet o SSH al Dispositivo con VRFs

Contenido

[Introducción](#)

[Antecedentes](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe la configuración del acceso del dispositivo con Telnet o Secure Shell (SSH) a través de una tabla de reenvío y routing virtual (VRF).

Antecedentes

En las redes de computadoras basadas en IP, el VRF es una tecnología que permite que coexistan varias instancias de una tabla de routing en el mismo router, al mismo tiempo. Debido a que las instancias de ruteo son independientes, se pueden utilizar las mismas direcciones IP o IP que se superponen sin ningún conflicto entre sí. Hay una mejora en la funcionalidad de la red, porque se pueden segmentar las rutas de red sin necesidad de que haya muchos routers.

VRF se puede implementar en un dispositivo de red mediante distintas tablas de routing conocidas como bases de información de reenvío (FIB), una por instancia de routing. Alternativamente, un dispositivo de red puede tener la capacidad de configurar diferentes routers virtuales, donde cada uno tiene su propia FIB que no es accesible para ninguna otra instancia de router virtual en el mismo dispositivo.

Telnet es un protocolo de capa de aplicación que se utiliza en Internet o en redes de área local (LAN) para proporcionar una función de comunicación bidireccional, interactiva y orientada a texto que utiliza una conexión de terminal virtual. Los datos de usuario se intercalan dentro de la banda con la información de control de Telnet en una conexión de datos orientada a bytes de 8 bits en el Protocolo de control de transmisión (TCP).

SSH es un protocolo de red criptográfico para operar los servicios de red de forma segura a través de una red no segura. La aplicación de ejemplo más conocida es para que los usuarios inicien sesión de forma remota en los sistemas informáticos.

A menudo, cuando estas tecnologías se utilizan juntas, crean confusión. Especialmente cuando intenta acceder remotamente a un dispositivo a través de una interfaz que pertenece a una instancia VRF de ruteo no global.

Esta guía de configuración utiliza Telnet como una forma de acceso a la administración solo para fines explicativos. El concepto también se puede ampliar para el acceso SSH.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

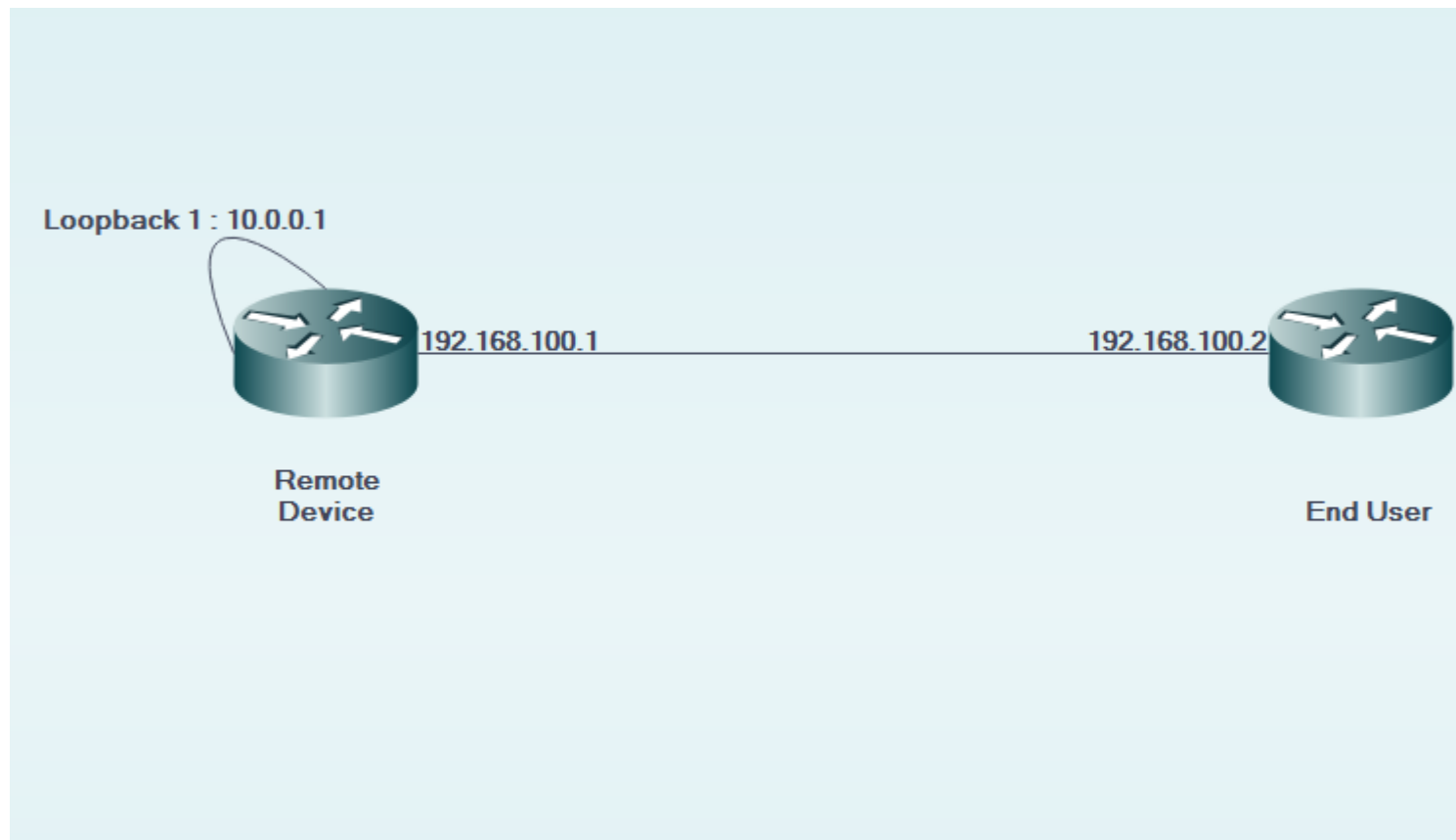
Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Nota: Comprensión básica de VRF y Telnet. También se recomienda tener conocimientos de ACL. La configuración de VRF debe ser compatible con el dispositivo y la plataforma. Este documento se aplica a todos los routers de Cisco que ejecutan Cisco IOS® y donde se soportan VRF y ACL.

Configurar

Diagrama de la red



Configuración

En el dispositivo remoto:

```
!  
interface GigabitEthernet0/0  
  description LINK TO END USER  
  ip vrf forwarding MGMT  
  ip address 192.168.100.1 255.255.255.252  
  duplex auto  
  speed auto  
!  
  
!  
interface Loopback1  
  description LOOPBACK TO TELNET INTO FOR MANAGEMENT ACCESS  
  ip vrf forwarding MGMT  
  ip address 10.0.0.1 255.255.255.255  
!  
  
!  
line vty 0 4  
  access-class 8 in  
  password cisco  
  login  
  transport input all  
line vty 5 15  
  access-class 8 in  
  password cisco  
  login  
  transport input all  
!
```

En el dispositivo del usuario final:

```
!  
interface GigabitEthernet0/0  
  description LINK TO REMOTE SITE  
  ip vrf forwarding MGMT  
  ip address 192.168.100.2 255.255.255.252  
  duplex auto  
  speed auto  
!
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Antes del `vrf-also` se utiliza en la configuración de la clase de acceso de la línea vty 0 15 del dispositivo remoto:

```
EndUser#ping vrf MGMT ip 10.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

```
EndUser#telnet 10.0.0.1 /vrf MGMT
Trying 10.0.0.1 ...
% Connection refused by remote host
```

Las llegadas del paquete al dispositivo remoto aumentan a medida que aumenta el recuento ACE correspondiente.

```
RemoteSite#show ip access-lists 8
Standard IP access list 8
 10 permit 192.168.100.2 log (3 matches)
```

Sin embargo, después del `vrf-also` se agrega en la clase de acceso de la línea vty 0 15, se permite el acceso telnet.

Según el comportamiento definido, los dispositivos Cisco IOS aceptan todas las conexiones VTY de forma predeterminada. Sin embargo, si se utiliza una clase de acceso, se supone que las conexiones deben llegar solo desde la instancia IP global. Sin embargo, si existe un requisito y el deseo de permitir conexiones desde instancias VRF, utilice el comando `vrf-also` junto con la instrucción `access-class` correspondiente en el configuración de la línea.

```
!
line vty 0 4
  access-class 8 in vrf-also
  password cisco
  login
  transport input all
line vty 5 15
  access-class 8 in vrf-also
  password cisco
  login
  transport input all
!
```

```
EndUser#ping vrf MGMT ip 10.0.0.1
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

```
EndUser#telnet 10.0.0.1 /vrf MGMT  
Trying 10.0.0.1 ... Open
```

```
User Access Verification
```

```
Password:  
RemoteSite>
```

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

La resolución de problemas basada en VRF puede ser necesaria en ocasiones. Asegúrese de que las interfaces afectadas estén todas en el mismo VRF y que tengan disponibilidad dentro del mismo VRF.

Además, puede ser necesario resolver problemas relacionados con SSH y Telnet.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).