Configurar o acesso Telnet ou SSH para o dispositivo com VRFs

Contents

Introduction

Este documento descreve a configuração de acesso de dispositivo com Telnet ou Secure Shell (SSH) através de uma tabela Virtual Routing and Forwarding (VRF).

Informações de Apoio

Nas redes de computador baseadas em IP, o VRF é a tecnologia que permite que várias instâncias de uma tabela de roteamento coexistam em um mesmo roteador ao mesmo tempo. Como as instâncias de roteamento são independentes, os mesmos endereços IP ou os endereços IP que se sobrepõem podem ser usados sem nenhum conflito entre si. A funcionalidade da rede é aprimorada porque os caminhos de rede podem ser segmentados sem a necessidade de vários roteadores.

O VRF pode ser implementado em um dispositivo de rede por tabelas de roteamento distintas conhecidas como Bases de Informações de Encaminhamento (FIBs), uma por instância de roteamento. Como alternativa, um dispositivo de rede pode ter a capacidade de configurar roteadores virtuais diferentes, onde cada um tem seu próprio FIB que não está acessível a qualquer outra instância de roteador virtual no mesmo dispositivo.

O Telnet é um protocolo da camada de aplicação usado na Internet ou em redes locais (LAN) para fornecer uma instalação de comunicação bidirecional, interativa e orientada a texto que usa uma conexão de terminal virtual. Os dados do usuário estão intercalados em banda com as informações de controle de Telnet em uma conexão de dados orientada por bytes de 8 bits no protocolo TCP (Transmission Control Protocol).

O SSH é um protocolo de rede criptográfico para operar serviços de rede com segurança em uma rede não segura. O aplicativo de exemplo mais conhecido é para login remoto em sistemas de computador por usuários.

Muitas vezes, quando essas tecnologias são usadas juntas, elas criam confusão. Especialmente quando você tenta acessar remotamente um dispositivo através de uma interface que pertence a uma instância VRF de roteamento não global.

Este guia de configuração usa o Telnet como uma forma de acesso de gerenciamento apenas para fins explicativos. O conceito pode ser estendido também para o acesso ao SSH.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

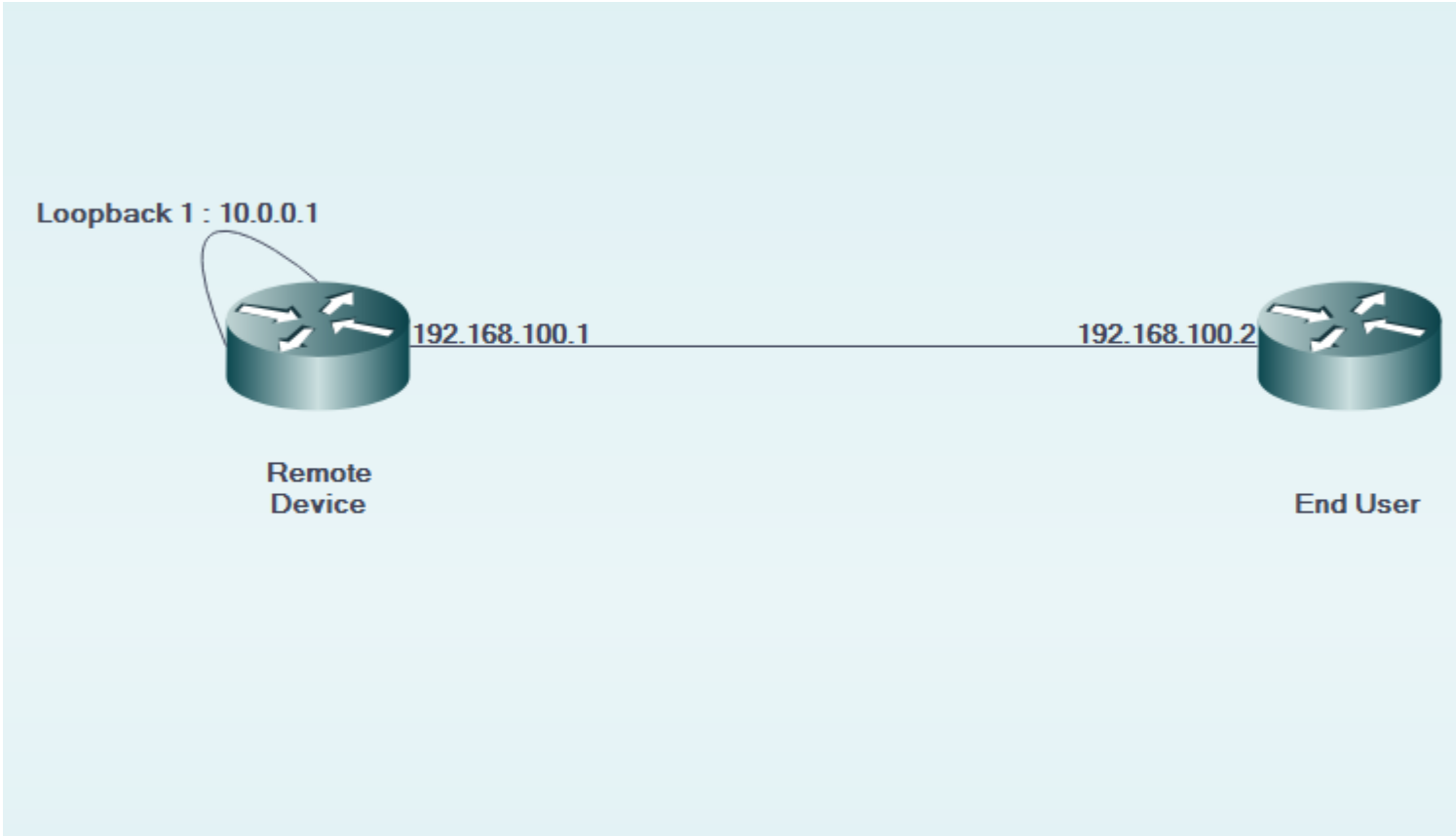
Este documento não se restringe a versões de software e hardware específicas.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

> **Observação**: entendimento básico de VRFs e Telnet. Recomenda-se também o conhecimento de ACL. A configuração de VRFs deve ser suportada no dispositivo e na plataforma. Este documento se aplica a todos os roteadores Cisco que executam o Cisco IOS® e onde VRFs e ACLs são suportados.

Configurar

Diagrama de Rede



Configuração

No 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
!
```

No dispositivo do usuário 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
!
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Antes da vrf-also palavra-chave é usada na configuração access-class of line vty 0 15 do 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
```

Os acessos ao pacote no dispositivo remoto aumentam à medida que a contagem ACE correspondente aumenta.

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

No entanto, após a vrf-also for adicionada na classe de acesso da linha vty 0 15, o acesso telnet será permitido.

De acordo com o comportamento definido, os dispositivos Cisco IOS aceitam todas as conexões VTY por padrão. Contudo, se um access-class for usado, supõe-se que as conexões devem chegar apenas na instância IP global . No entanto, se houver um requisito e desejo de permitir conexões de instâncias VRF, use o comando vrf-also palavra-chave, juntamente com a instrução access-class correspondente no configuração de linha.

```
!
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

Esta seção disponibiliza informações para a solução de problemas de configuração.

Às vezes, a solução de problemas baseada em VRF pode ser necessária. Assegure que todas as interfaces em questão estejam no mesmo VRF e tenham acessibilidade no mesmo VRF.

Além disso, a solução de problemas relacionada a SSH e Telnet pode ser necessária.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.