

配置对支持 VRF 的设备的 Telnet/SSH 访问

Contents

[Introduction](#)

[背景信息](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Network Diagram](#)

[配置](#)

[Verify](#)

[Troubleshoot](#)

Introduction

本文档介绍如何配置通过虚拟路由和转发 (VRF)，实现基于 Telnet 或安全外壳 (SSH) 的设备访问。

背景信息

在基于 IP 的网络中，VRF 技术允许路由表的多个实例在同一路由器中同时存在。由于路由实例相互独立，因此可使用相同或重叠的 IP 地址，而且相互之间不会冲突。由于无需多个路由器就可以对网络路径进行分段，因此增强了网络功能。

可以通过不同的路由表（也称为转发信息库 [FIB]，每个路由实例一个路由表）在网络设备中实施 VRF。或者，同一个网络设备能够配置不同的虚拟路由器，每个虚拟路由器都有自己的 FIB，同一设备上的任何其他虚拟路由器实例都不可访问该 FIB。

Telnet 是一种在互联网或局域网上使用的应用层网络协议，通过虚拟终端连接提供面向文本的双向交互式通信。系统通过基于 8 位字节的传输控制协议 (TCP) 数据连接，在带内传输用户数据和 Telnet 控制信息。

SSH 是一种在非安全网络上用于安全运行网络服务的加密网络协议。目前已知的最佳示例应用就是用户远程登录计算机系统。

通常当这些技术一起使用时会造成混乱，尤其是当试图通过属于非全局路由 VRF 实例的接口远程接入设备的时候。

本配置指南仅出于示范目的而将 Telnet 用于管理访问。此说明对于 SSH 访问同样适用。

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

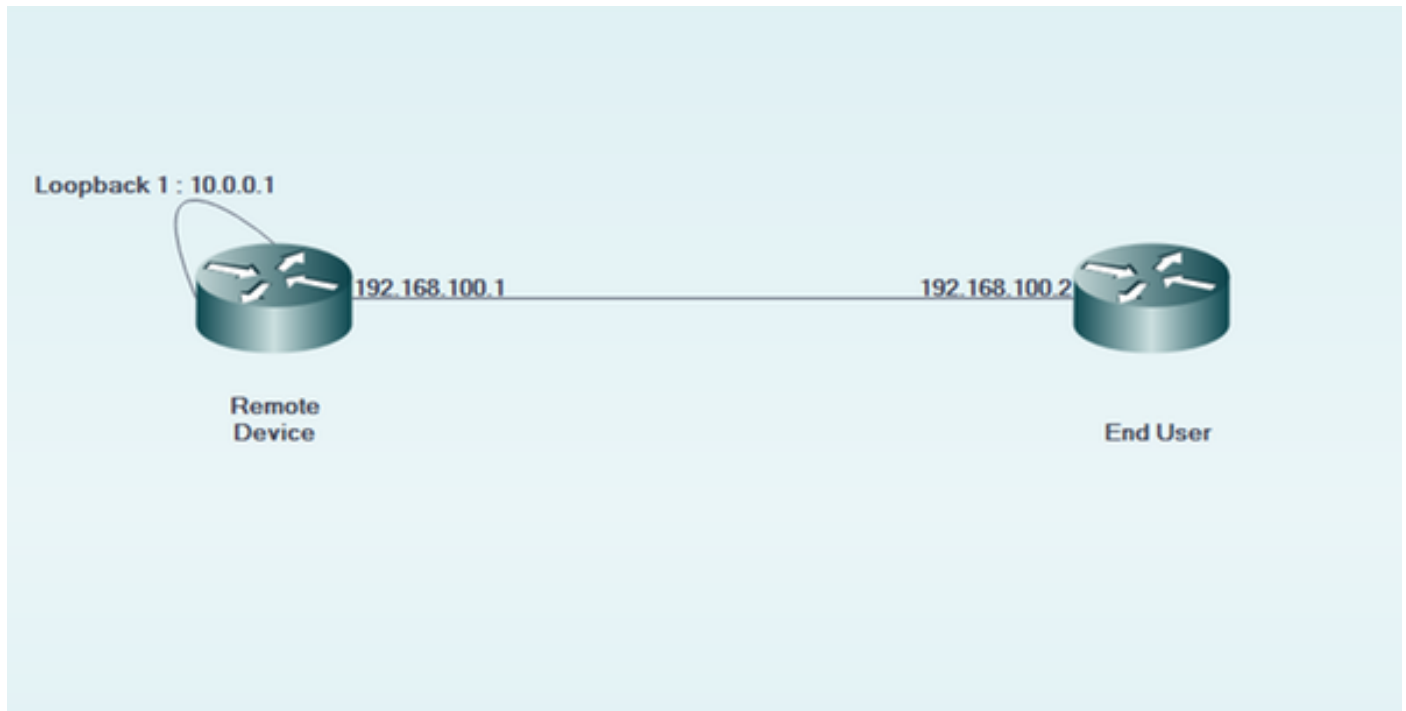
This document is not restricted to specific software and hardware versions.

Note: 了解 VRF 和 Telnet 的基础知识。还建议了解 ACL 的知识。设备和平台必须支持 VRF 配置。 IOS VRF ACL

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. 如果网络处于活动状态，请确保您了解所有命令的潜在影响。

Configure

Network Diagram



配置

远程设备端的配置：

```
!  
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  
!
```

最终用户端的配置：

```
!  
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  
!
```

Verify

使用本部分可确认配置能否正常运行。

在 vty 0 15 线路的 access-class 中使用关键字 vrf-also 之前，远程设备的配置：

```
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
```

随着相应 ACE 计数的增加，远程设备上的数据包命中数也随之上升。

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

但是，在 vty 0 15 线路的 access-class 中添加关键字 vrf-also 后，设备允许 telnet 访问。

根据定义的行为，思科 IOS 设备默认接受所有的 VTY 连接。但是，如果使用 access-class，则意味着只能允许来自全局 IP 实例的连接。但如果需要允许来自 VRF 实例的连接，则在线路配置上使用 vrf-also 关键字及相应的 access-class 语句

。

```
!  
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

本部分提供了可用于对配置进行故障排除的信息。

有时需要执行基于 VRF 的故障排除。确保连接接口都位于同一 VRF 中并且在该 VRF 中可达。

此外，可能还需要执行 SSH 和 Telnet 相关的故障排除。