Configure Telnet or SSH Access to Device with VRFs

Contents

Introduction

Background Information

Prerequisites

- Requirements
- Components Used

Configure

- Network Diagram
- Configuration

Verify

Troubleshoot

Introduction

This document describes the configuration of device access with Telnet or Secure Shell (SSH) across a Virtual Routing and Forwarding (VRF) table.

Background Information

In IP-based computer networks, VRF is a technology that allows multiple instances of a routing table to co-exist within the same router at the same time.

Because the routing instances are independent, the same or IP addresses that overlap can be used without any conflict with each other.

Network functionality is improved because network paths can be segmented without the requirement of multiple routers.

VRF can be implemented in a network device by distinct routing tables known as Forwarding Information Bases (FIBs), one per routing instance.

Alternatively, a network device can have the ability to configure different virtual routers, where each one has its own FIB that is not accessible to any other virtual router instance on the same device.

Telnet is an application layer protocol used on the Internet or local area networks (LAN) to provide a bi-directional, interactive, text-oriented communication facility that uses a virtual terminal connection.

User data is interspersed in-band with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP).

SSH is a cryptographic network protocol to operate network services securely over an unsecured network. The best known example application is for remote log in to computer systems by users.

Often when these technologies are used together, they create confusion. Especially when remotely accessing

a device through an interface that belongs to a non-global routing VRF instance.

This configuration guide uses Telnet as a form of management access just for explanatory purposes. The concept can be extended for SSH access too.

Prerequisites

Requirements

Basic understanding of VRFs and Telnet. Knowledge of ACL is also recommended.

Configuration of VRFs must be supported on the device and platform.

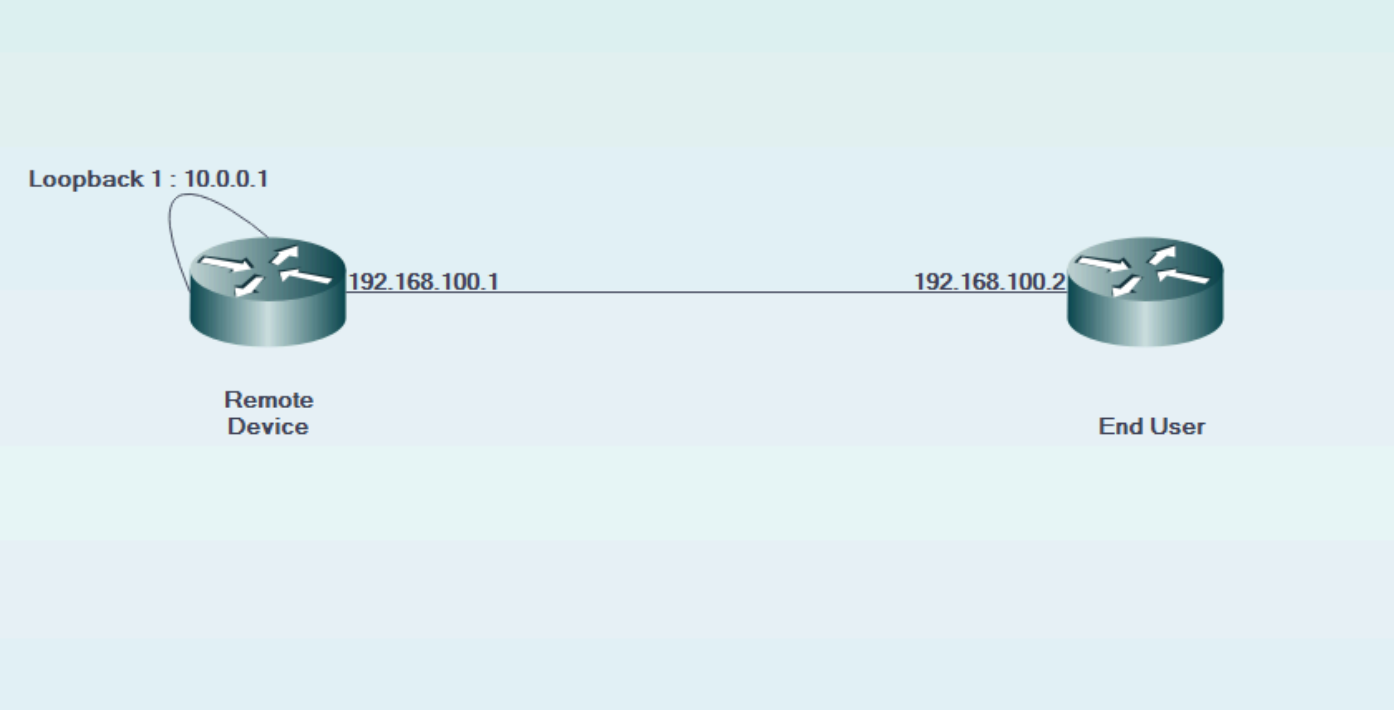
Components Used

This document applies to all Cisco routers that run Cisco IOS® and where VRFs and ACLs are supported.

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. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram



Configuration

On the remote device:

```
!
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
!
```

On the end user device:

```
!
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

Use this section in order to confirm that your configuration works properly.

Before the vrf-also keyword is used in the access-class of line vty 0 15 configuration of the remote device:

```
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
```

Packet hits on the remote device increase as the ACE count that corresponds increases.

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

However, after the vrf-also keyword is added in the access-class of line vty 0 15, telnet access is permitted.

As per the defined behavior, Cisco IOS devices accept all VTY connections by default.

However, if an access-class is used, the assumption is that connections must arrive only from the global IP instance.

If there is a requirement and desire to allow connections from VRF instances, use the vrf-also keyword, along with the corresponding access-class statement on the line configuration.

```
!
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

Ensure that the concerned interfaces are all in the same VRF and they have reachability within the same VRF.