

Konfiguration von Telnet- oder SSH-Zugriff auf das Gerät mit VRFs

Inhalt

[Einleitung](#)

[Hintergrundinformationen](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfiguration](#)

[Überprüfung](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird die Konfiguration des Gerätezugriffs mit Telnet oder Secure Shell (SSH) über eine VRF-Tabelle (Virtual Routing and Forwarding) beschrieben.

Hintergrundinformationen

In IP-basierten Computernetzwerken ist VRF eine Technologie, die es ermöglicht, dass mehrere Instanzen einer Routing-Tabelle gleichzeitig im gleichen Router vorhanden sind. Da die Routing-Instanzen unabhängig sind, können dieselben Adressen oder IP-Adressen, die sich überschneiden, ohne Konflikte miteinander verwendet werden. Die Netzwerkfunktionen wurden verbessert, da Netzwerkpfade segmentiert werden können, ohne dass mehrere Router erforderlich sind.

VRF kann in einem Netzwerkgerät durch verschiedene Routing-Tabellen implementiert werden, die als "Forwarding Information Bases (FIBs)" bezeichnet werden und jeweils eine pro Routing-Instanz umfassen. Alternativ kann ein Netzwerkgerät verschiedene virtuelle Router konfigurieren, wobei jeder einzelne über eine eigene FIB verfügt, auf die keine andere virtuelle Router-Instanz auf demselben Gerät zugreifen kann.

Telnet ist ein Protokoll auf Anwendungsebene, das im Internet oder in LANs (Local Area Networks) verwendet wird, um eine bidirektionale, interaktive, textorientierte Kommunikationseinrichtung bereitzustellen, die eine virtuelle Terminalverbindung verwendet. Benutzerdaten werden in einer 8-Bit-Byte-orientierten Datenverbindung über das Transmission Control Protocol (TCP) in Band mit Telnet-Steuerinformationen durchgesetzt.

SSH ist ein kryptografisches Netzwerkprotokoll, das Netzwerkdienste sicher über ein ungesichertes Netzwerk betreibt. Die bekannteste Beispielanwendung ist die Remote-Anmeldung von Benutzern bei Computersystemen.

Werden diese Technologien gemeinsam genutzt, führt dies häufig zu Verwirrung. Dies gilt insbesondere, wenn Sie versuchen, über eine Schnittstelle, die zu einer nicht globalen Routing-VRF-Instanz gehört, per Fernzugriff auf ein Gerät zuzugreifen.

In diesem Konfigurationsleitfaden wird Telnet nur zu erläuternden Zwecken als Form des Verwaltungszugriffs verwendet. Das Konzept kann auch für den SSH-Zugang erweitert werden.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

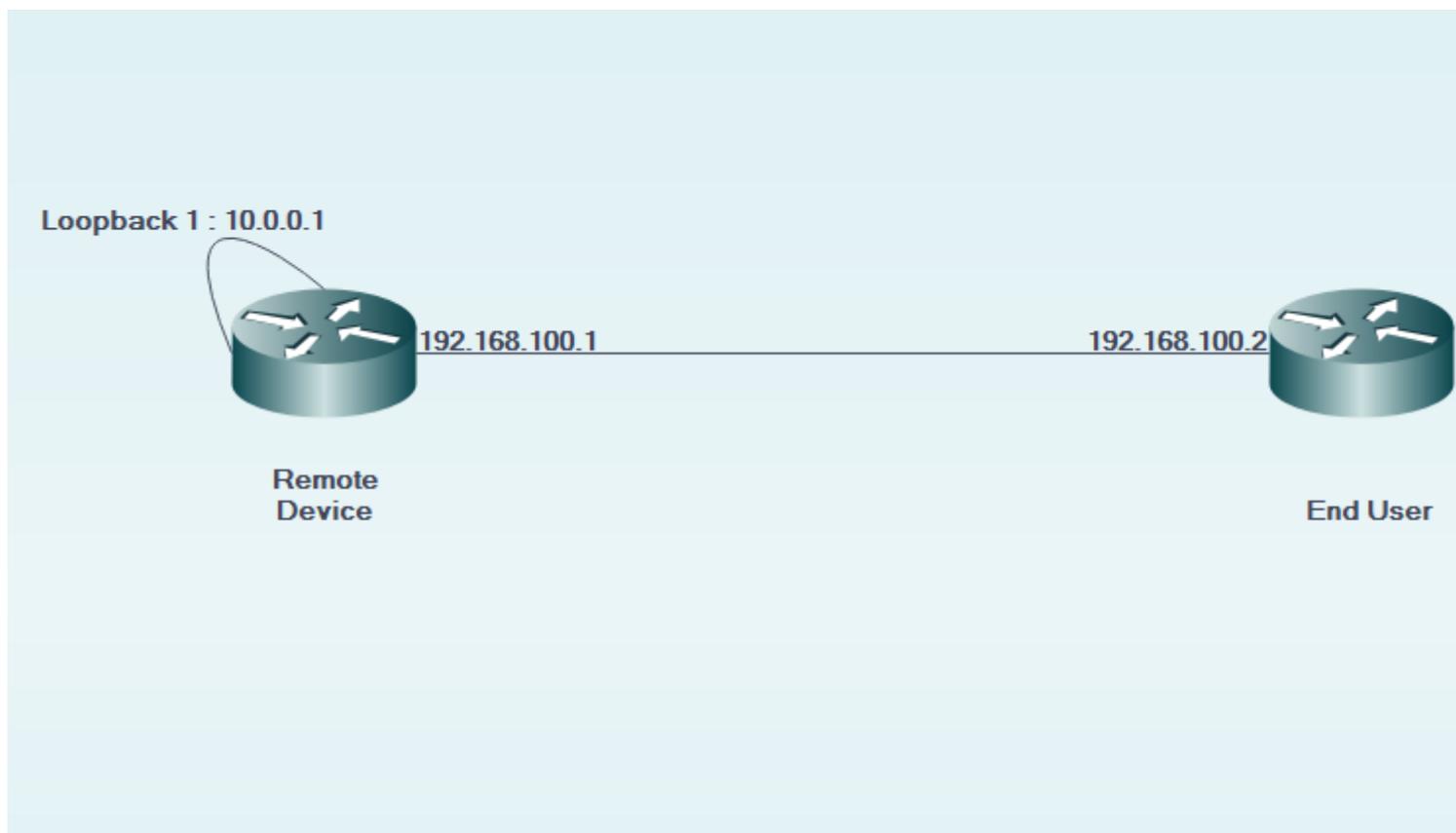
Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hinweis: Grundlegendes Verständnis von VRFs und Telnet. Außerdem sollten Sie sich mit ACL vertraut machen. Die Konfiguration von VRFs muss auf dem Gerät und der Plattform unterstützt werden. Dieses Dokument gilt für alle Cisco Router, auf denen Cisco IOS® ausgeführt wird und auf denen VRFs und ACLs unterstützt werden.

Konfigurieren

Netzwerkdigramm



Konfiguration

Auf dem Remote-Gerät:

```
!  
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  
!
```

Auf dem Endbenutzergerät:

```
!  
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  
!
```

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Vor dem `vrf-also` Das Schlüsselwort wird in der Zugriffsklasse der Konfiguration der Leitung `vty 0 15` des Remote-Geräts verwendet:

```
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
```

Die Anzahl der Paketzugriffe auf das Remote-Gerät nimmt mit der entsprechenden Anzahl von ACEs zu.

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

Nach der `vrf-also` -Schlüsselwort in der Zugriffsklasse der Zeile `vty 0 15` hinzugefügt wird, ist der Telnet-Zugriff zulässig.

Gemäß dem definierten Verhalten akzeptieren Cisco IOS-Geräte standardmäßig alle VTY-Verbindungen. Bei Verwendung einer Zugriffsklasse wird jedoch davon ausgegangen, dass Verbindungen nur von der globalen IP-Instanz ankommen. Wenn jedoch Verbindungen von VRF-Instanzen zugelassen werden sollen, verwenden Sie den `vrf-also` -Schlüsselwort zusammen mit der entsprechenden `access-class`-Anweisung auf der Leitungskonfiguration.

```
!
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>
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Eine VRF-basierte Fehlerbehebung kann zeitweise erforderlich sein. Stellen Sie sicher, dass sich alle betroffenen Schnittstellen in derselben VRF-Instanz befinden und dass sie innerhalb derselben VRF-Instanz erreichbar sind.

Darüber hinaus kann eine entsprechende Fehlerbehebung in Bezug auf SSH und Telnet erforderlich sein.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.