Telnet- of SSH-toegang tot apparaat configureren met VRF-systemen

Inhoud

Inleiding

Dit document beschrijft de configuratie van apparaattoegang met Telnet of Secure Shell (SSH) via een Virtual Routing and Forwarding (VRF)-tabel.

Achtergrondinformatie

In IP-gebaseerde computernetwerken is VRF een technologie waarmee meerdere instanties van een routeringstabel tegelijkertijd binnen dezelfde router kunnen bestaan. Omdat de routeringsinstanties onafhankelijk zijn, kunnen dezelfde of IP-adressen die elkaar overlappen zonder conflicten met elkaar worden gebruikt. De netwerkfunctionaliteit is verbeterd omdat netwerkpaden kunnen worden gesegmenteerd zonder dat hiervoor meerdere routers nodig zijn.

VRF kan in een netwerkapparaat worden geïmplementeerd door afzonderlijke routingtabellen bekend als Forwarding Information Bases (FIBâ€™s), een per routinginstantie. Een andere mogelijkheid is dat een netwerkapparaat verschillende virtuele routers kan configureren, waarbij elke router een eigen FIB heeft die niet toegankelijk is voor een andere virtuele routerinstantie op hetzelfde apparaat.

Telnet is een protocol op de toepassingslaag dat op internet of LAN (Local Area Networks) wordt gebruikt om een bidirectionele, interactieve, tekstgeoriënteerde communicatievoorziening te bieden die gebruik maakt van een virtuele terminalverbinding. De gegevens van de gebruiker worden in-band met de controleinformatie van Telnet in een byte georiënteerde gegevensverbinding met 8 bits over het Protocol van de Controle van de Transmissie (TCP) onderbroken.

SSH is een cryptografisch netwerkprotocol om netwerkservices veilig te kunnen uitvoeren via een onbeveiligd netwerk. De bekendste voorbeeldtoepassing is voor externe aanmelding bij computersystemen door gebruikers.

Wanneer deze technologieën samen worden gebruikt, creëren ze vaak verwarring. Vooral wanneer u probeert om op afstand toegang te krijgen tot een apparaat via een interface die behoort tot een niet-wereldwijde routing VRF-instantie.

Deze configuratiegids gebruikt Telnet als een vorm van beheerstoegang enkel voor verklarende doeleinden. Het concept kan ook voor SSH-toegang worden uitgebreid.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

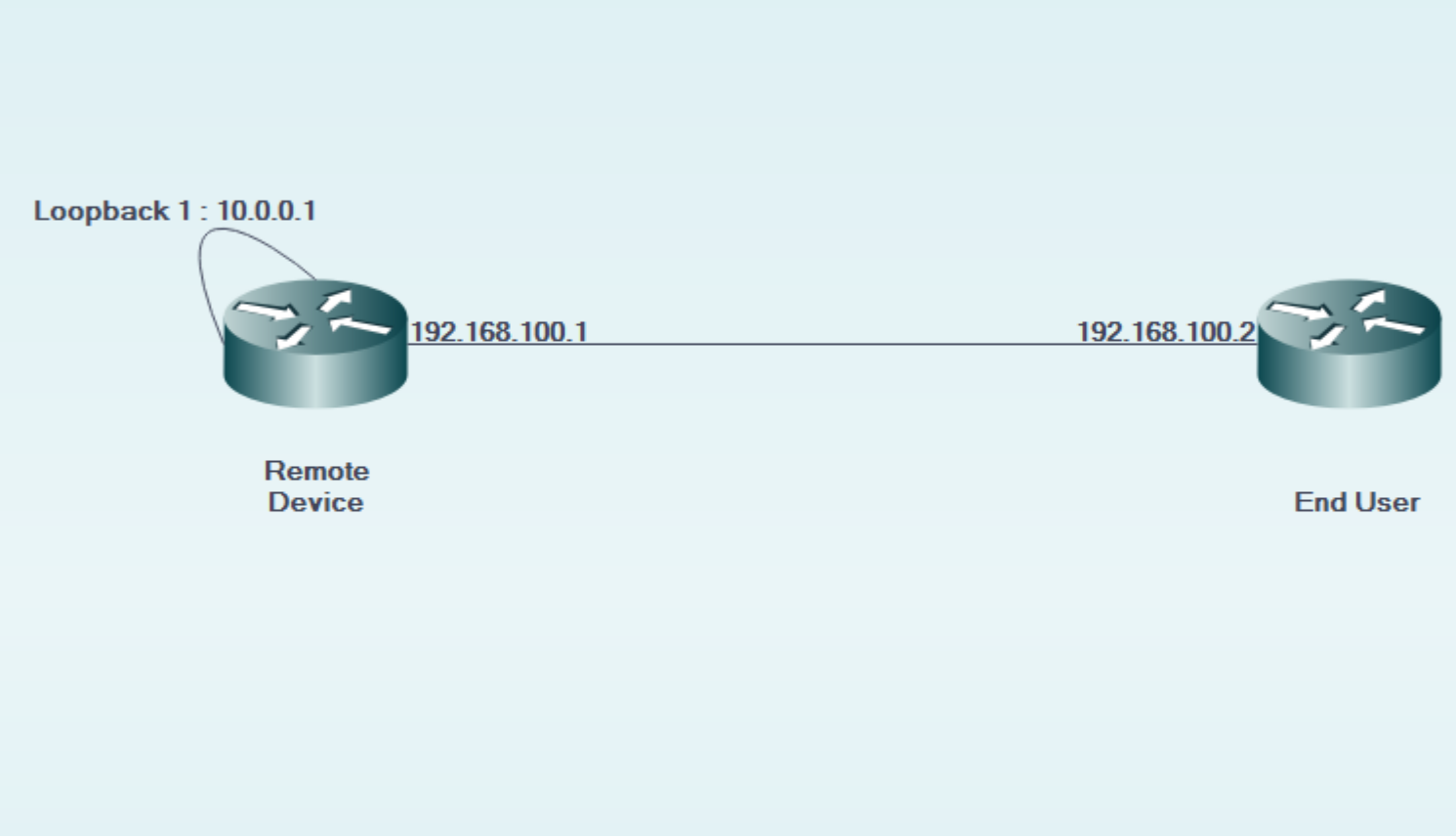
Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

> **Opmerking**: basiskennis van VRF en Telnet. Kennis van ACL wordt ook aanbevolen. De configuratie van VRF's moet op het apparaat en het platform worden ondersteund. Dit document is van toepassing op alle Cisco-routers waarop Cisco IOS® wordt uitgevoerd en waar VRF- en ACLâ€™s worden ondersteund.

Configureren

Netwerkdiagram



Configuratie

Op het afstandsapparaat:

```
!
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
!
```

Op het apparaat van de eindgebruiker:

```
!
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
!
```

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Voor de vrf-also Het sleutelwoord wordt gebruikt in de toegang-klasse van lijn vty 0 15 configuratie van het verre apparaat:

```
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 op het apparaat op afstand verhogen als de ACE-telling die overeenkomt met verhogingen.

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

Na de vrf-also het sleutelwoord wordt toegevoegd in de toegang-klasse van lijn vty 0 15, wordt telnet toegang toegelaten.

Conform het gedefinieerde gedrag accepteren Cisco IOS-apparaten standaard alle VTY-verbindingen. Als echter een toegangsklasse wordt gebruikt, wordt ervan uitgegaan dat verbindingen alleen uit de globale IP-instantie moeten komen. Als er echter een eis en wens is om verbindingen van VRF-gevallen toe te staan, gebruikt u de vrf-also sleutelwoord, samen met de bijbehorende verklaring van de toegangsklasse over het lijnconfiguratie.

```
!
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>
```

Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

Op VRF gebaseerde probleemoplossing kan soms nodig zijn. Zorg ervoor dat de betrokken interfaces allemaal in dezelfde VRF zitten en dat ze bereikbaar zijn binnen dezelfde VRF.

Ook kunnen relevante SSH- en Telnet-gerelateerde probleemoplossing nodig zijn.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.