

# VRF를 사용하여 디바이스에 대한 텔넷 또는 SSH 액세스 구성

## 목차

---

[소개](#)

[배경 정보](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[네트워크 다이어그램](#)

[설정](#)

[다음을 확인합니다.](#)

[문제 해결](#)

---

## 소개

이 문서에서는 VRF(Virtual Routing and Forwarding) 테이블에서 텔넷 또는 SSH(Secure Shell)로 디바이스 액세스를 구성하는 방법에 대해 설명합니다.

## 배경 정보

IP 기반 컴퓨터 네트워크에서 VRF는 라우팅 테이블의 여러 인스턴스가 동일한 라우터 내에서 동시에 공존할 수 있도록 하는 기술입니다. 라우팅 인스턴스는 독립적이므로 겹치는 동일한 주소 또는 IP 주소를 서로 충돌하지 않고 사용할 수 있습니다. 여러 라우터의 요구 없이 네트워크 경로를 분할할 수 있으므로 네트워크 기능이 향상됩니다.

VRF는 라우팅 인스턴스당 하나씩 FIB(Forwarding Information Base)라고 하는 개별 라우팅 테이블을 통해 네트워크 디바이스에서 구현될 수 있습니다. 또는 네트워크 디바이스에는 서로 다른 가상 라우터를 구성할 수 있는 기능이 있으며, 각 라우터에는 동일한 디바이스의 다른 가상 라우터 인스턴스에 액세스할 수 없는 자체 FIB가 있습니다.

텔넷은 인터넷 또는 LAN(Local Area Network)에서 가상 터미널 연결을 사용하는 양방향 인터랙티브 텍스트 지향 통신 기능을 제공하기 위해 사용되는 애플리케이션 레이어 프로토콜입니다. 사용자 데이터는 TCP(Transmission Control Protocol)를 통한 8비트 바이트 지향 데이터 연결에서 텔넷 제어 정보와 인밴드(in-band)로 분산됩니다.

SSH는 보안되지 않은 네트워크를 통해 네트워크 서비스를 안전하게 운영하기 위한 암호화 네트워크 프로토콜입니다. 가장 잘 알려진 응용 프로그램은 사용자가 컴퓨터 시스템에 원격으로 로그인하는 것입니다.

이러한 기술이 함께 사용될 때 종종 혼란이 야기됩니다. 특히 비전역 라우팅 VRF 인스턴스에 속하

는 인터페이스를 통해 디바이스에 원격으로 액세스하려고 시도하는 경우.

이 컨피그레이션 가이드에서는 설명을 위해 텔넷을 관리 액세스 형태로 사용합니다. SSH 액세스를 위해 이 개념을 확장할 수도 있습니다.

## 사전 요구 사항


### 요구 사항

이 문서에 대한 특정 요건이 없습니다.

### 사용되는 구성 요소

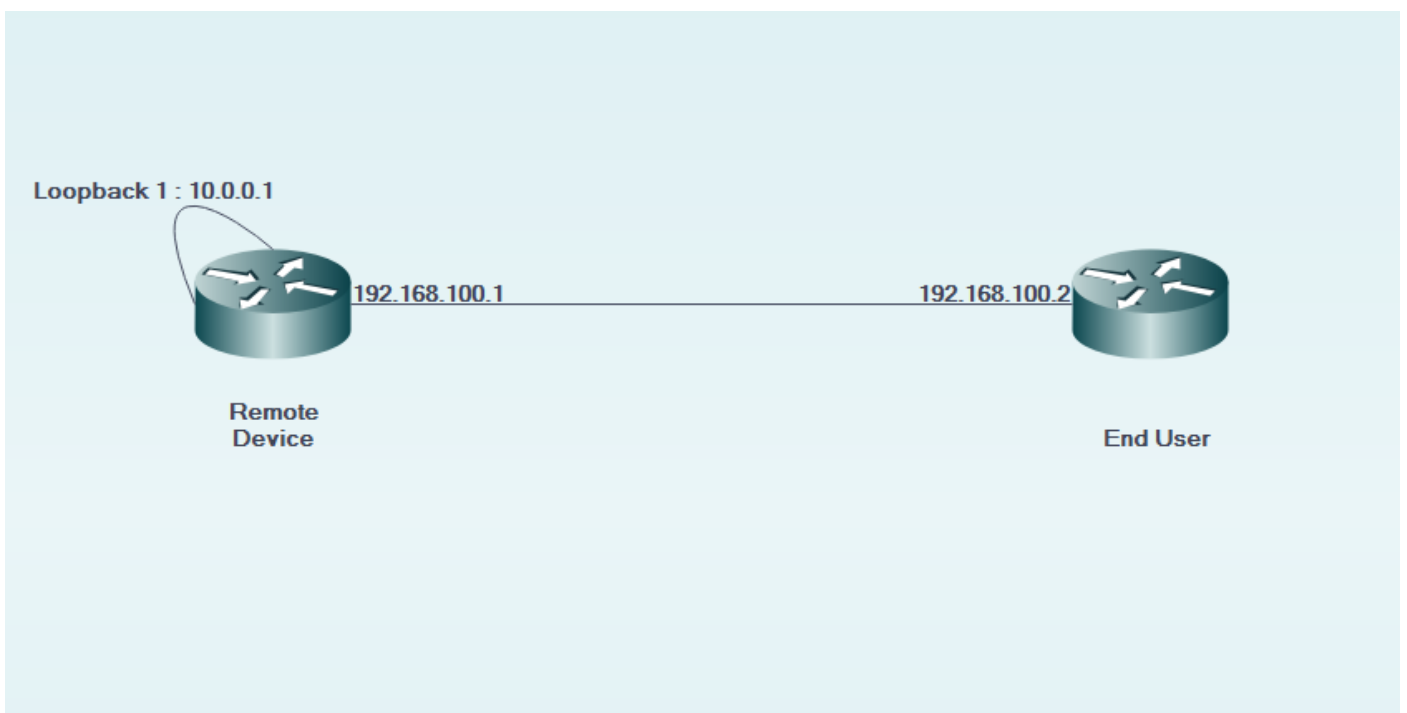
이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

 참고: VRF 및 텔넷에 대한 기본적인 이해 ACL에 대한 지식도 권장합니다. VRF 컨피그레이션은 디바이스 및 플랫폼에서 지원되어야 합니다. 이 문서는 Cisco IOS®를 실행하고 VRF 및 ACL이 지원되는 모든 Cisco 라우터에 적용됩니다.

## 구성

### 네트워크 다이어그램



## 설정

원격 디바이스에서:

```
!  
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  
!
```

최종 사용자 디바이스에서:

```
!  
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  
!
```

## 다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

공격 전 `vrf-also` 키워드는 원격 디바이스의 `line vty 0 15` 컨피그레이션의 `access-class`에 사용됩니다.

```
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
```

원격 디바이스의 패킷 적중은 해당하는 ACE 수가 증가함에 따라 증가합니다.

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

그러나 `vrf-also` 라인 `vty 0 15`의 `access-class`에 키워드가 추가되면 텔넷 액세스가 허용됩니다.

정의된 동작에 따라 Cisco IOS 디바이스는 기본적으로 모든 VTY 연결을 수락합니다. 그러나 `access-class`를 사용하는 경우 전역 IP 인스턴스에서만 연결이 도달해야 한다고 가정합니다. 그러나 VRF 인스턴스로부터의 연결을 허용해야 하는 요구 사항이 있는 경우 `vrf-also` 키워드 및 의 해당 `access-class` 문 라인 컨피그레이션

```
!
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>
```

## 문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

VRF 기반 트러블슈팅이 필요할 때도 있습니다. 관련된 인터페이스가 모두 동일한 VRF에 있고 동일한 VRF 내에서 도달 가능한지 확인합니다.

또한 관련 SSH 및 텔넷 관련 트러블슈팅이 필요할 수 있습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.