

# Configurazione dell'accesso Telnet o SSH al dispositivo con VRF

## Sommario

[Introduzione](#)

[Premesse](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

## Introduzione

In questo documento viene descritta la configurazione dell'accesso al dispositivo con Telnet o Secure Shell (SSH) in una tabella VRF (Virtual Routing and Forwarding).

## Premesse

Nelle reti IP, il VRF è una tecnologia che consente la coesistenza di più istanze di una tabella di routing nello stesso router contemporaneamente. Poiché le istanze di routing sono indipendenti, è possibile utilizzare gli stessi indirizzi IP o IP che si sovrappongono senza alcun conflitto tra loro. La funzionalità di rete è stata migliorata in quanto i percorsi di rete possono essere segmentati senza la necessità di più router.

Il VRF può essere implementato in un dispositivo di rete da tabelle di routing distinte, note come FIB (Forwarding Information Base), una per istanza di routing. In alternativa, un dispositivo di rete può avere la capacità di configurare router virtuali diversi, ognuno dei quali dispone di un proprio FIB non accessibile a nessun'altra istanza di router virtuale sullo stesso dispositivo.

Telnet è un protocollo a livello di applicazione utilizzato su Internet o sulle reti LAN (Local Area Network) per fornire una comunicazione bidirezionale, interattiva e orientata al testo che utilizza una connessione terminale virtuale. I dati utente vengono scambiati in banda con le informazioni di controllo Telnet in una connessione dati a 8 bit orientata ai byte su TCP (Transmission Control Protocol).

SSH è un protocollo di rete crittografico per il funzionamento sicuro dei servizi di rete su una rete non protetta. L'applicazione di esempio più nota è quella per l'accesso remoto ai computer da parte degli utenti.

Spesso, quando queste tecnologie vengono utilizzate insieme, creano confusione. Specialmente quando si cerca di accedere in remoto a un dispositivo tramite un'interfaccia che appartiene a un'istanza VRF di routing non globale.

Questa guida alla configurazione utilizza Telnet come forma di accesso alla gestione solo a scopo esplicativo. Il concetto può essere esteso anche per l'accesso SSH.

# Prerequisiti

## Requisiti

Nessun requisito specifico previsto per questo documento.

## Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

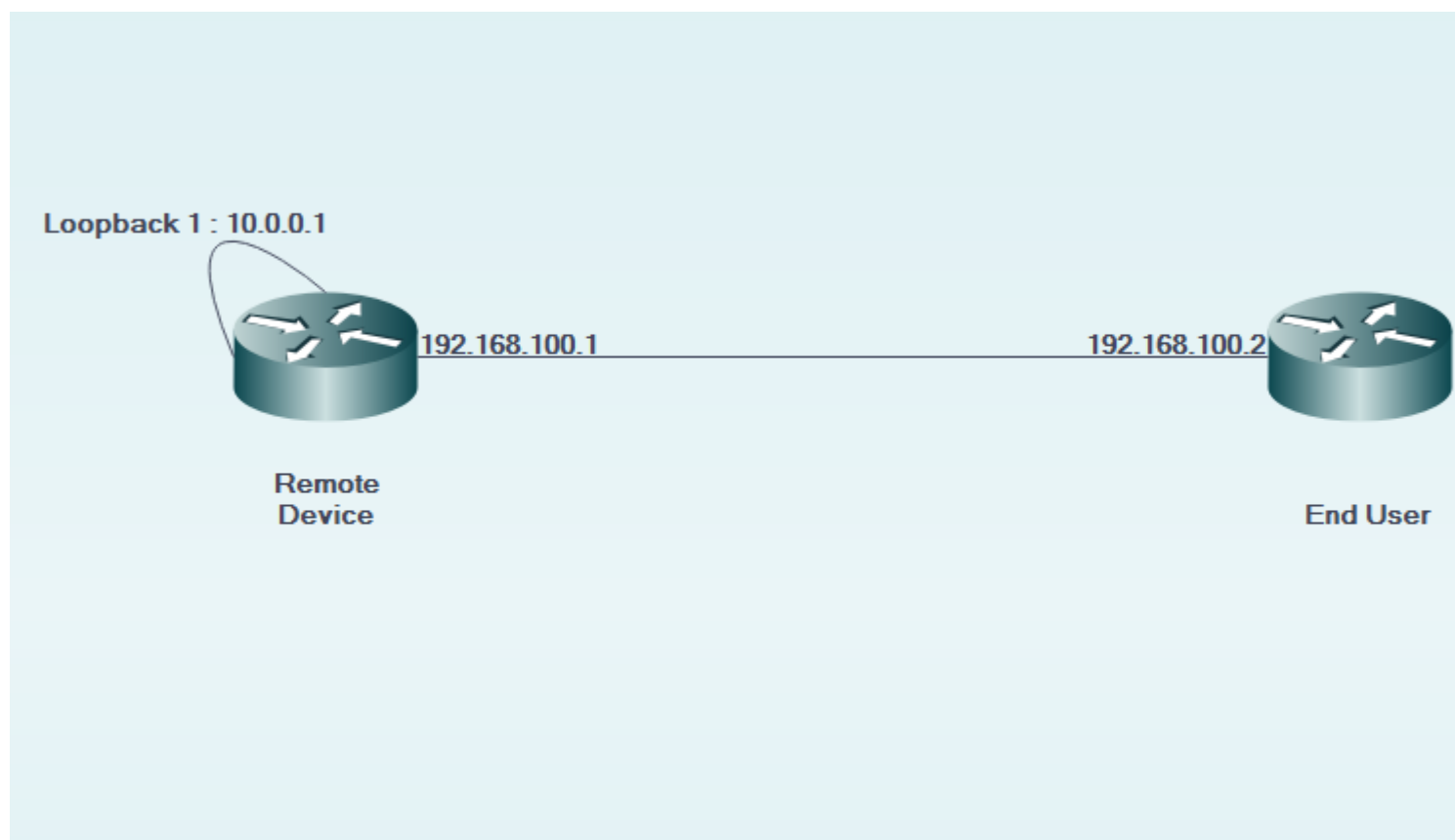
---

**Nota:** informazioni di base su VRF e Telnet. Si consiglia inoltre di conoscere gli ACL. La configurazione dei VRF deve essere supportata dal dispositivo e dalla piattaforma. Questo documento è relativo a tutti i router Cisco con Cisco IOS® e dove sono supportati i VRF e ACL.

---

# Configurazione

## Esempio di rete



## Configurazione

Sul dispositivo remoto:

```

!
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
!

```

Sul dispositivo dell'utente finale:

```

!
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
!

```

## Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Prima del vrf-also la parola chiave viene usata nella configurazione access-class della riga vty 0 15 del dispositivo remoto:

```
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
```

All'aumento del numero di voci ACE corrispondenti, aumentano i risultati del pacchetto sul dispositivo remoto.

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

Tuttavia, dopo `vrf-also` parola chiave viene aggiunta nella classe access della riga vty 0 15, l'accesso telnet è consentito.

In base al comportamento definito, i dispositivi Cisco IOS accettano tutte le connessioni VTY per impostazione predefinita. Tuttavia, se si utilizza una classe access, si presume che le connessioni debbano provenire solo dall'istanza IP globale. Tuttavia, se esiste un requisito e si desidera consentire le connessioni dalle istanze VRF, utilizzare il `vrf-also` parola chiave, insieme all'istruzione `access-class` corrispondente configurazione della linea.

```
!
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>
```

## **Risoluzione dei problemi**

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

La risoluzione dei problemi basata su VRF può essere talvolta necessaria. Verificare che le interfacce interessate siano tutte nello stesso VRF e che siano raggiungibili all'interno dello stesso VRF.

Inoltre, può essere necessaria la risoluzione dei problemi relativi a SSH e Telnet.

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).