Esempio di configurazione di VPN dinamiche di livello 3 con tunnel GRE multipoint

Sommario

Introduzione

In questo documento viene descritto come configurare le VPN Dynamic Layer 3 (L3) con la funzionalità tunnel GRE (Generic Routing Encapsulation) multipoint.

Prerequisiti

Requisiti

Prima di configurare le VPN L3 dinamiche con la funzionalità tunnel GRE, verificare che la VPN MPLS (Multiprotocol Label Switching) sia configurata e funzioni correttamente e che la connettività end-to-end sia stabilita per la rete IPV4.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Router Cisco serie 7206VXR (NPE-G1) con software Cisco IOS® versione 15.2(4)S3
- Cisco serie 7609-S Router con software Cisco IOS versione 12.2(33)SRE4

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.

Premesse

Le VPN dinamiche L3 con tunnel mGRE forniscono un meccanismo di trasporto L3 basato su una tecnologia di tunneling mGRE avanzata da utilizzare nelle reti IP. Il trasporto dinamico del tunneling L3 può essere utilizzato anche all'interno delle reti IP per trasportare il traffico VPN tra le reti dei provider di servizi e delle aziende e per fornire l'interoperabilità per il trasporto dei pacchetti tra le VPN IP e MPLS. Questa funzionalità supporta la RFC 2547, che definisce l'outsourcing dei servizi backbone IP per le reti aziendali.

Restrizioni per VPN L3 dinamiche con tunnel GRE

Di seguito è riportato un elenco di restrizioni che si applicano alle VPN L3 dinamiche con tunnel GRE:

- La distribuzione di una VPN MPLS con incapsulamento IP/GRE e MPLS all'interno di una singola rete non è supportata.
- Ogni router Provider Edge (PE) supporta una sola configurazione del tunnel.
- L'interfaccia VLAN sul router Cisco serie 7600 rivolta verso il core al quale deve entrare il traffico di tag tunneled non è supportata. Deve essere l'interfaccia principale o una sottointerfaccia.
- MPLS VPN over mGRE è supportato sui router Cisco serie 7600 che usano la scheda di linea ES-40 e la scheda di linea Session Initiation Protocol (SIP) 400 come schede di base.

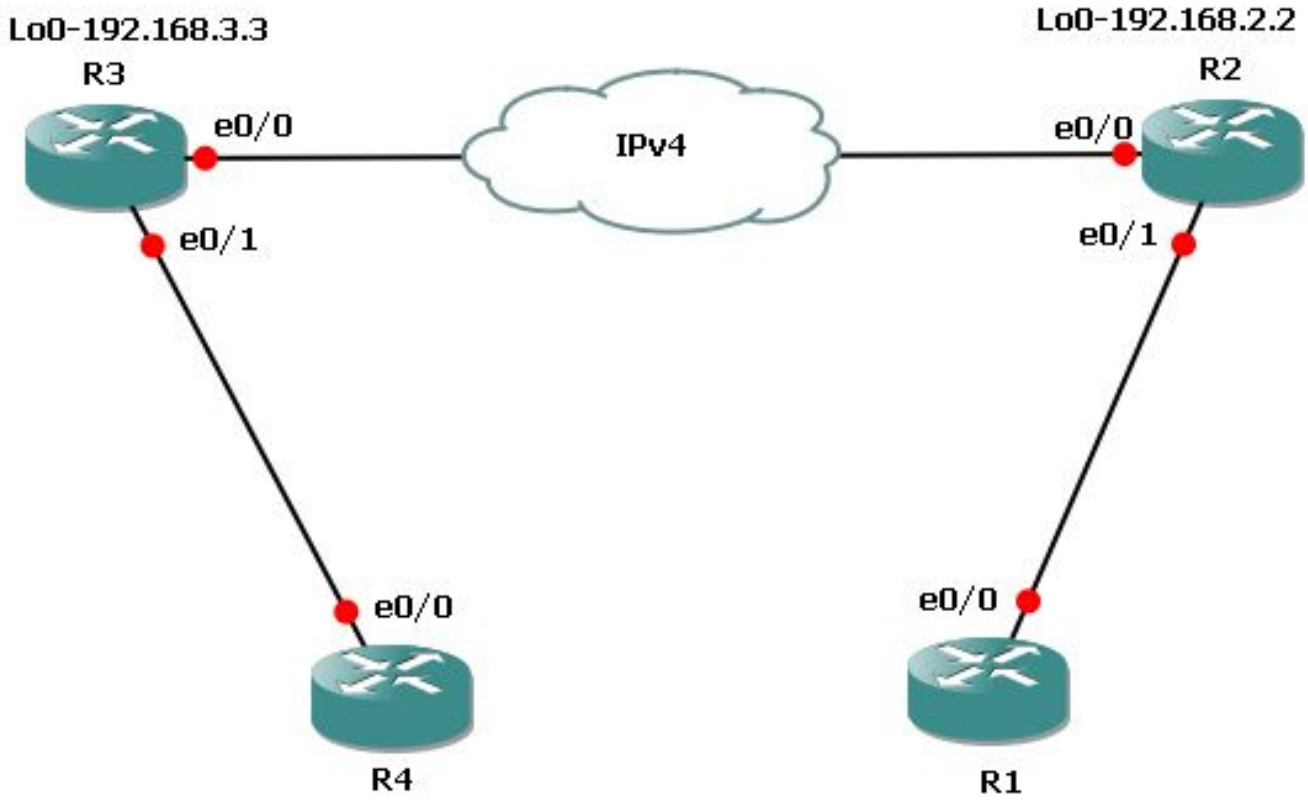
Configurazione

In questa sezione vengono descritte due configurazioni:

- VPN dinamica L3 con tunnel mGRE su rete solo IP
- VPN dinamica L3 con tunnel GRE su rete IP + MPLS

VPN L3 dinamiche con tunnel GRE su rete solo IP (non MPLS)

Esempio di rete



Configurazioni

Queste sono le configurazioni richieste sul router 3 (R3) e sul router 2 (R2).

Ecco la configurazione per R3:

```
l3vpn encapsulation ip MGRE
transport ipv4 source Loopback0

route-map MGRE-NEXT-HOP permit 10
set ip next-hop encapsulate l3vpn MGRE

router bgp 65534
 !
address-family vpnv4
neighbor 192.168.2.2 route-map MGRE-NEXT-HOP in
```

Ecco la configurazione per R2:

```
l3vpn encapsulation ip MGRE
transport ipv4 source Loopback0

route-map MGRE-NEXT-HOP permit 10
set ip next-hop encapsulate l3vpn MGRE

router bgp 65534
 !
address-family vpnv4
neighbor 192.168.3.3 route-map MGRE-NEXT-HOP in
```

Verifica

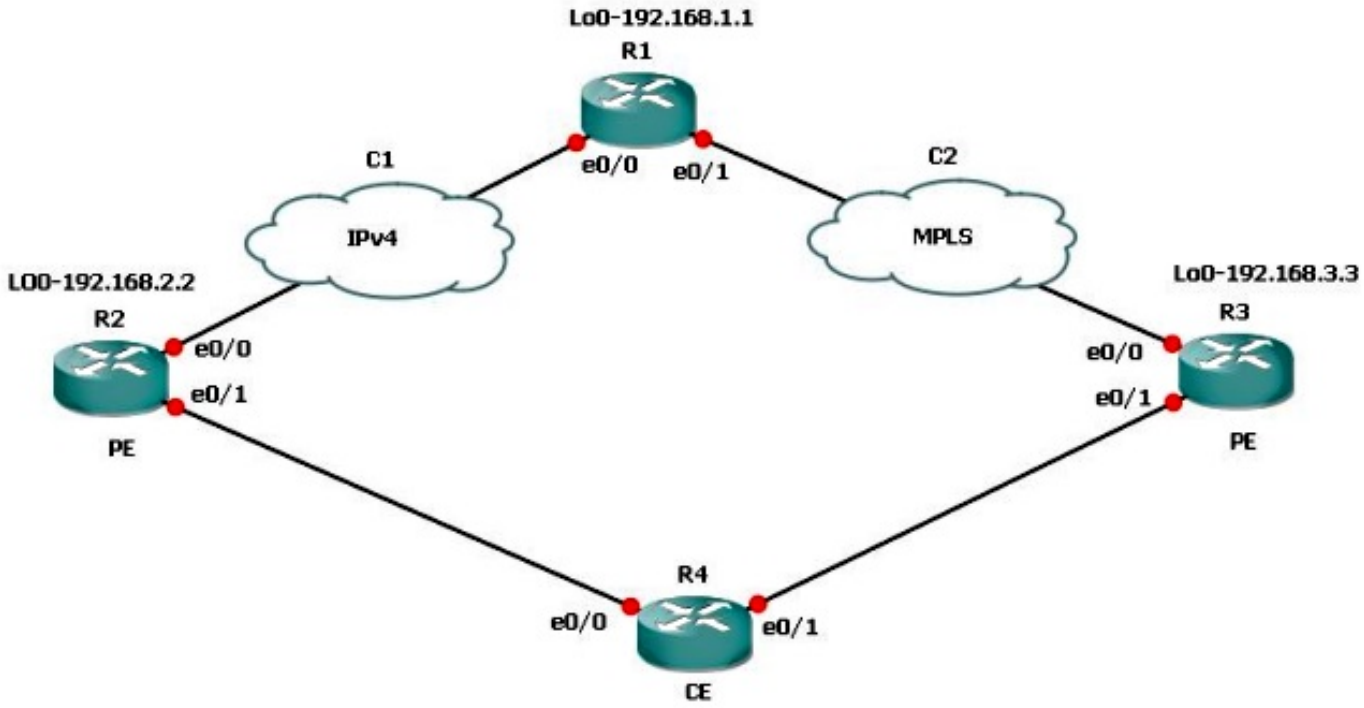
Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

```
R2#show tunnel endpoints

 Tunnel0 running in multi-GRE/IP mode

 Endpoint transport 192.168.3.3 Refcount 3 Base 0x1E8E1B74 Create Time 00:47:53
  overlay 192.168.3.3 Refcount 2 Parent 0x1E8E1B74 Create Time 00:47:53


R2#show l3vpn encapsulation ip MGRE

 Profile: MGRE
   transport ipv4 source Loopback0
   protocol gre
   payload mpls
   mtu default
 Tunnel Tunnel0 Created [OK]
 Tunnel Linestate [OK]
 Tunnel Transport Source Loopback0 [OK]


R2#show ip route vrf MGRE 172.16.3.3

Routing Table: MGRE
Routing entry for 172.16.3.3
 Known via "bgp 65534", distance 200, metric 0, type internal
 Last update from 192.168.3.3 on Tunnel0, 01:03:25 ago
 Routing Descriptor Blocks:
 * 192.168.3.3 (default), from 172.16.112.1, 01:03:25 ago, via Tunnel0 <points to tunnel
     Route metric is 0, traffic share count is 1
     AS Hops 0
     MPLS label: 17   <BGP vpnv4 label>
     MPLS Flags: MPLS Required
```

Nota: Nell'esempio precedente sono presenti solo due PE. Tuttavia, se si dispone di una rete di grandi dimensioni con più router PE, questo mGRE dinamico è molto semplice da configurare e scalare, in quanto è necessario disporre di una configurazione simile su tutti i PE e i tunnel vengono rilevati automaticamente.

VPN L3 dinamiche con tunnel GRE su rete IP + MPLS

Esempio di rete



Se si dispone di uno scenario di connessione doppia in cui una connessione è MPLS e l'altra non è MPLS, è necessario configurare mGRE su tutti i router PE interessati. Con questa topologia, è necessario configurare mGRE su tutti e tre i router PE.

Se non è stato configurato mGRE sulla connessione tra R3 e R1 - collegamento MPLS, le subnet dietro R3 non saranno in grado di comunicare con le subnet dietro R2.

R1 e R2 costruiscono endpoint del tunnel con R3 basati sul profilo VPN L3. Fare riferimento alla configurazione in questo documento se il profilo VPN L3 non è configurato, la route-map al peer Border Gateway Protocol (BGP) su R3 non viene applicata e la route-map per la VPN L3 per R3 su R1 non viene applicata.

Configurazioni

Queste sono le configurazioni richieste su R1, R2 e R3.

Ecco la configurazione di R1:

```
l3vpn encapsulation ip MGRE
transport ipv4 source Loopback0

route-map MGRE-NEXT-HOP permit 10
set ip next-hop encapsulate l3vpn MGRE

router bgp 65534
address-family vpnv4
neighbor 192.168.2.2 send-community extended
neighbor 192.168.2.2 route-map MGRE-NEXT-HOP in
neighbor 192.168.3.3 activate
```

Ecco la configurazione per R2:

```
l3vpn encapsulation ip MGRE
transport ipv4 source Loopback0

route-map MGRE-NEXT-HOP permit 10
set ip next-hop encapsulate l3vpn MGRE

router bgp 65534
address-family vpnv4
neighbor 192.168.1.1 route-map MGRE-NEXT-HOP in
neighbor 192.168.1.1 activate
```

Ecco la configurazione per R3:

```
router bgp 65534
address-family vpnv4
neighbor 192.168.1.1 activate
```

Verifica

A questo punto, è possibile eseguire il ping tra il loopback R2 1 e il loopback R3 1:

```
R2#ping vrf  MGRE  172.16.3.3 source 172.16.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.3, timeout is 2 seconds:
Packet sent with a source address of 172.16.2.2
.....
Success rate is 0 percent (0/5)


R2#show ip route vrf MGRE 172.16.3.3

Routing Table: MGRE
Routing entry for 172.16.3.3/32
 Known via "bgp 65534", distance 200, metric 0, type internal
 Last update from 192.168.3.3 on Tunnel0, 00:50:23 ago
 Routing Descriptor Blocks:
 * 192.168.3.3 (default), from 192.168.1.1, 00:50:23 ago, via Tunnel0




      pointed towards a tunnel>
     Route metric is 0, traffic share count is 1
     AS Hops 0
     MPLS label: 19
     MPLS Flags: MPLS Required


R2#show tunnel endpoints
 Tunnel1 running in multi-GRE/IP mode

 Tunnel0 running in multi-GRE/IP mode

 Endpoint transport 192.168.1.1 Refcount 3 Base 0x507665E4 Create Time 01:24:25
  overlay 192.168.1.1 Refcount 2 Parent 0x507665E4 Create Time 01:24:25
 Endpoint transport 192.168.3.3 Refcount 3 Base 0x507664D4 Create Time 00:50:51
   overlay 192.168.3.3 Refcount 2 Parent 0x507664D4 Create Time 00:50:51
```

R2 ha creato un tunnel dinamico per la versione 192.168.3.3 basato sull'hop successivo BGP per la versione 172.16.3.3.

```
R2#show ip bgp vpnv4 vrf  MGRE 172.16.3.3
BGP routing table entry for 43984:300:172.16.3.3/32, version 29
Paths: (1 available, best #1, table MGRE)
 Advertised to update-groups:
    1
 Local, imported path from 300:300:172.16.3.3/32
    192.168.3.3 (metric 3) (via Tunnel0) from 192.168.1.1 (192.168.1.1)
     Origin incomplete, metric 0, localpref 100, valid, internal, best
     Extended Community: RT:43984:300
     Originator: 192.168.3.3, Cluster list: 192.168.1.1
     mpls labels in/out nolabel/19
```

Viene verificato su R1 e crea anche endpoint tunnel per entrambi i router PE:

```
R1#show tunnel endpoints
 Tunnel1 running in multi-GRE/IP mode

 Tunnel0 running in multi-GRE/IP mode

 Endpoint transport 192.168.2.2 Refcount 3 Base 0x1E8EE7B0 Create Time 01:36:41
  overlay 192.168.2.2 Refcount 2 Parent 0x1E8EE7B0 Create Time 01:36:41
 Endpoint transport 192.168.3.3 Refcount 3 Base 0x1E8EE590 Create Time 00:59:34
  overlay 192.168.3.3 Refcount 2 Parent 0x1E8EE590 Create Time 00:59:34
```

In R3, non vengono creati endpoint del tunnel:

```
R3#show tunnel endpoints
```

Di seguito è riportato il percorso della subnet R2 da cui è stato originato il ping:

```
R3#show ip route vrf  MGRE  172.16.2.2

Routing Table: MGRE
Routing entry for 172.16.2.2/32
 Known via "bgp 65534", distance 200, metric 0, type internal
 Last update from 192.168.2.2 01:01:57 ago
 Routing Descriptor Blocks:
 * 192.168.2.2 (default), from 192.168.1.1, 01:01:57 ago
     Route metric is 0, traffic share count is 1
     AS Hops 0
     MPLS label: 17
     MPLS Flags: MPLS Required
```

Pertanto, il pacchetto viene inviato come incapsulato nel GRE verso R3. Poiché R3 non ha un tunnel, non accetta il pacchetto GRE e lo scarta.

Pertanto, è necessario configurare il GRE end-to-end su un percorso in modo che funzioni. Ecco la configurazione di mGRE su R3, che è necessaria:

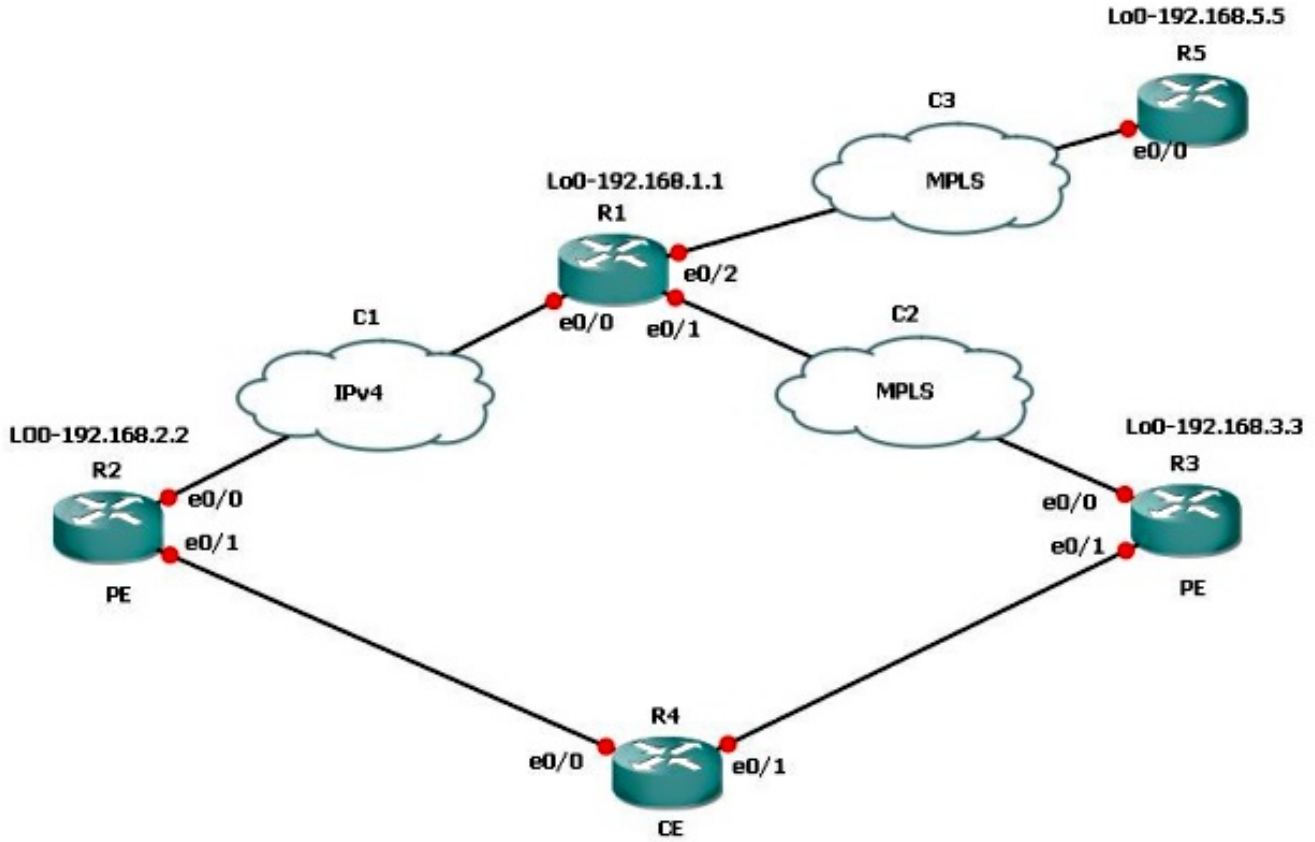
```
l3vpn encapsulation ip MGRE
transport ipv4 source Loopback0

route-map MGRE-NEXT-HOP permit 10
set ip next-hop encapsulate l3vpn MGRE
```

Non appena si crea il profilo VPN L3, vengono creati gli endpoint del tunnel e si riceve il traffico che è stato scartato in precedenza. Tuttavia, il traffico di ritorno è MPLS e non GRE finché non si applica il profilo sul peer BGP. Il traffico viene interrotto su R1 perché R1 non dispone di informazioni di etichetta per R2, che esegue solo IP.

```
R3#show tunnel endpoints
 Tunnel0 running in multi-GRE/IP mode

 Endpoint transport 192.168.1.1 Refcount 3 Base 0x2B79FBD4 Create Time 00:00:02
  overlay 192.168.1.1 Refcount 2 Parent 0x2B79FBD4 Create Time 00:00:02
 Endpoint transport 192.168.2.2 Refcount 3 Base 0x2B79FAC4 Create Time 00:00:02
  overlay 192.168.2.2 Refcount 2 Parent 0x2B79FAC4 Create Time 00:00:02


R3#show ip cef vrf  MGRE  172.16.2.2
172.16.2.2/32
 nexthop 192.168.13.1 GigabitEthernet0/0.1503 label 21 17

 router bgp 65534
address-family vpnv4
neighbor 192.168.1.1 route-map MGRE-NEXT-HOP in


R3#show ip cef vrf  MGRE  172.16.2.2
172.16.2.2/32
 nexthop 192.168.2.2 Tunnel0 label 17
```

```
R2#ping vrf  MGRE 172.16.3.3 source  172.16.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.3, timeout is 2 seconds:
Packet sent with a source address of 172.16.2.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Scenario 3



Si supponga che le subnet dietro R5, che devono comunicare con R3, non desiderino utilizzare mGRE. Quindi, è possibile usare la route-map usata per il profilo VPN L3 per impostare l'hop successivo e chiamare un prefisso-elenco e autorizzare solo i prefissi che richiedono il tunnel GRE.

Ecco la configurazione di R1:

```
route-map MGRE-NEXT-HOP permit 10
 match ip address prefix-list test
 set ip next-hop encapsulate l3vpn MGRE
route-map MGRE-NEXT-HOP permit 20
```

Èpossibile autorizzare i prefissi nel test prefix-list che richiedono il tunnel GRE e tutto il resto non ha un tunnel come interfaccia di uscita e segue il normale routing. Questa configurazione funziona perché R3 e R5 hanno connettività MPLS end-to-end.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- VPN dinamiche di livello 3 con tunnel GRE multipoint
- Documentazione e supporto tecnico – Cisco Systems