

通過點選將Google雲互聯配置為使用Cisco SD-WAN的傳輸

目錄

[簡介](#)

[背景資訊](#)

[問題](#)

[解決方案](#)

[設計概述](#)

[解決方案詳細資訊](#)

[步驟1.準備](#)

[步驟2.使用適用於多雲工作流的雲onRamp建立思科雲網關](#)

[步驟3.在GCP控制檯中新增合作夥伴互連連線](#)

[步驟4.在Cisco vManage中使用Cloud onRamp互連建立DC連線](#)

[步驟5.配置DC路由器以通過Internet和GCP雲互聯建立隧道](#)

[驗證](#)

[DC兆埠SD-WAN路由器配置](#)

簡介

本檔案介紹如何使用Google [Cloud Interconnect](#)作為軟體定義廣域網(SD-WAN)傳輸。

背景資訊

在Google雲平台(GCP)上工作負荷的企業客戶使用雲[互聯](#)來實現資料中心或中心連線。同時，公共Internet連線也非常常見於資料中心，並用作與其他地點的SD-WAN連線的基礎。本文介紹GCP雲互聯如何用作Cisco SD-WAN的基礎。

這非常類似於描述適用於AWS的同一解決方案。

將GCP雲互聯僅作為思科SD-WAN的另一個傳輸方式的主要優勢是，能夠在包括GCP雲互聯在內的所有傳輸上使用SD-WAN策略。客戶可以建立SD-WAN應用感知策略，通過GCP雲互聯路由關鍵應用，並在SLA違規時通過公共網際網路重新路由。

問題

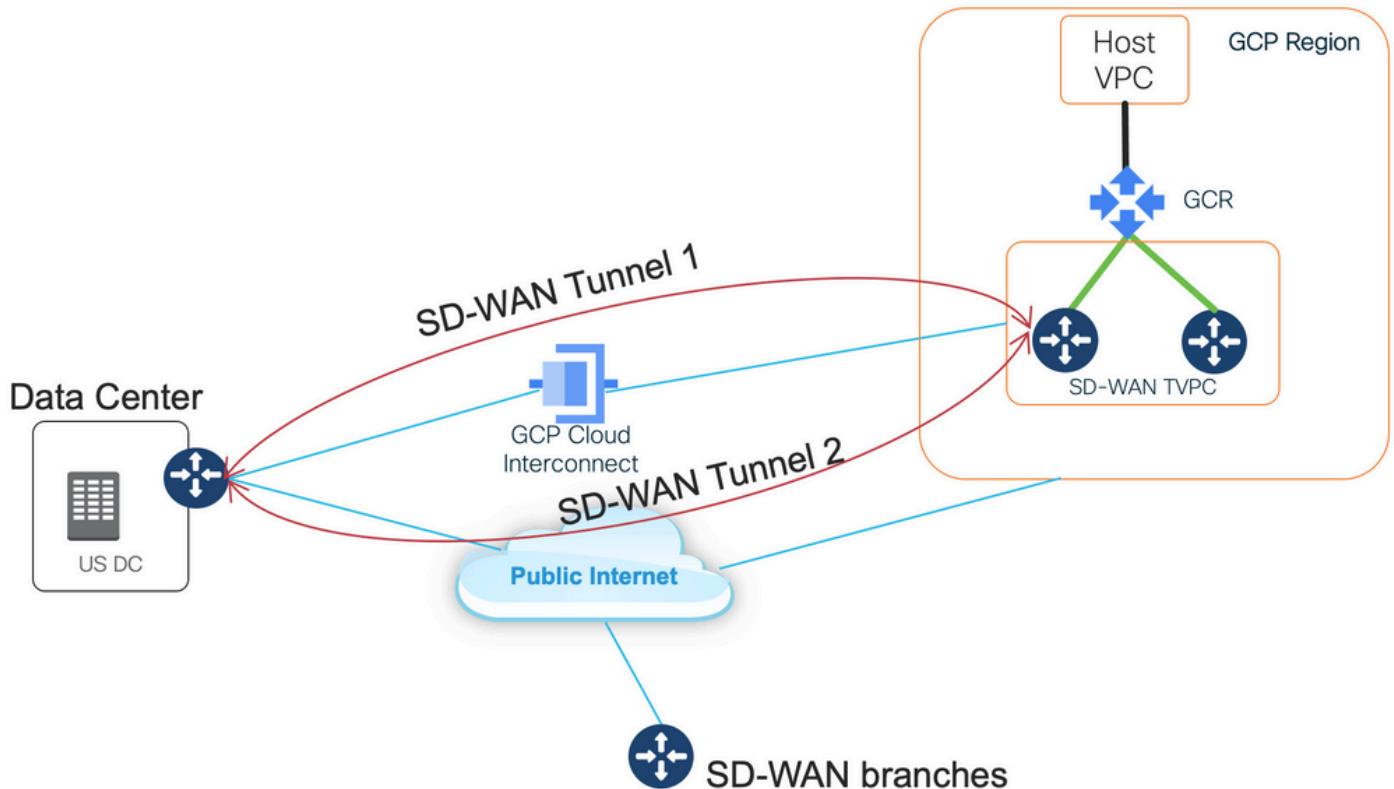
GCP雲互聯不提供本地SD-WAN功能。企業SD-WAN客戶的典型問題包括：

- 「是否可以使用GCP雲互聯作為Cisco SD-WAN的基礎」？
- 「How can I interconnect GCP Cloud Interconnect and Cisco SD-WAN ? (如何將GCP雲互聯與Cisco SD-WAN互聯 ?) 」
- 「如何建立可恢復、安全且可擴展的解決方案」？

解決方案

設計概述

關鍵設計點是資料中心通過GCP雲互聯連線到由Cloud onRamp為多雲調配建立的Cisco SD路由器，如下圖所示。



此解決方案的優勢包括：

- 完全自動：適用於多雲自動化的Cisco Cloud onRamp可用於部署具有兩個SD-WAN路由器的SD-WAN傳輸VPC。主機VPC可以作為Cloud onRamp的一部分被發現，只需點選一下即可對映到SD-WAN網路。
- 使用GCP的完整SD-WAN雲互連：GCP雲互聯只是另一個SD-WAN傳輸。所有SD-WAN功能（如應用感知策略、加密等）都可原生用於通過GCP雲互連的SD-WAN隧道上。

請注意，此解決方案的可擴充性與C8000V在GCP上的效能是一致的。有關GCP上的C8000v效能的詳細資訊，請參閱[SalesConnect](#)。

解決方案詳細資訊

瞭解此解決方案的關鍵點是SD-WAN顏色。請注意，GCP SD-WAN路由器將具有**private color private2**用於網際網路連線以及通過互聯進行連線，SD-WAN隧道將通過網際網路使用公共IP地址形成，SD-WAN隧道將通過使用私有IP地址的互聯電路建立到DC/站點(Site)。這意味著，資料中心路由器（業務網際網路顏色）將通過具有公共IP地址的Internet和通過專用IP的Private color與GCP SD-WAN路由器（private2顏色）建立連線。

有關SD-WAN顏色的通用資訊：

傳輸定位器(TLOC)指由SD-WAN路由器連線到底層網路的WAN傳輸(VPN 0)介面。每個TLOC通過SD-WAN路由器的系統IP地址、WAN介面的顏色以及傳輸封裝（GRE或IPsec）的組合進行唯一標

識。思科重疊管理協定(OMP)用於在SD-WAN路由器之間分發TLOC (也稱為TLOC路由)、SD-WAN重疊字首 (也稱為OMP路由) 和其他資訊。SD-WAN路由器知道如何通過TLOC路由相互連線並建立IPsec VPN隧道。

SD-WAN路由器和/或控制器 (vManage、vSmart或vBond) 可能位於網路中的網路地址轉換(NAT)裝置之後。當SD-WAN路由器向vBond控制器進行身份驗證時，vBond控制器將在交換過程中獲取SD-WAN路由器的專用IP地址/埠號以及公共IP地址/埠號設定。vBond控制器充當NAT(STUN)伺服器的會話遍歷實用程式，允許SD-WAN路由器發現其WAN傳輸介面的對映和/或轉換IP地址和埠號。

在SD-WAN路由器上，每個WAN傳輸都與一個公共和專用IP地址對相關聯。私有IP地址被視為前NAT地址。這是分配給SD-WAN路由器的WAN介面的IP地址。雖然這被視為私有IP地址，但此IP地址可以是公開可路由IP地址空間的一部分，也可以是IETF RFC 1918非公開可路由IP地址空間的一部分。公有IP地址被視為後NAT地址。當SD-WAN路由器最初與vBond伺服器進行通訊和身份驗證時，vBond伺服器會檢測到這種情況。公有IP地址也可以是公開可路由IP地址空間的一部分，也可以是IETF RFC 1918非公開可路由IP地址空間的一部分。在沒有NAT的情況下，SD-WAN傳輸介面的公有IP地址和私有IP地址相同。

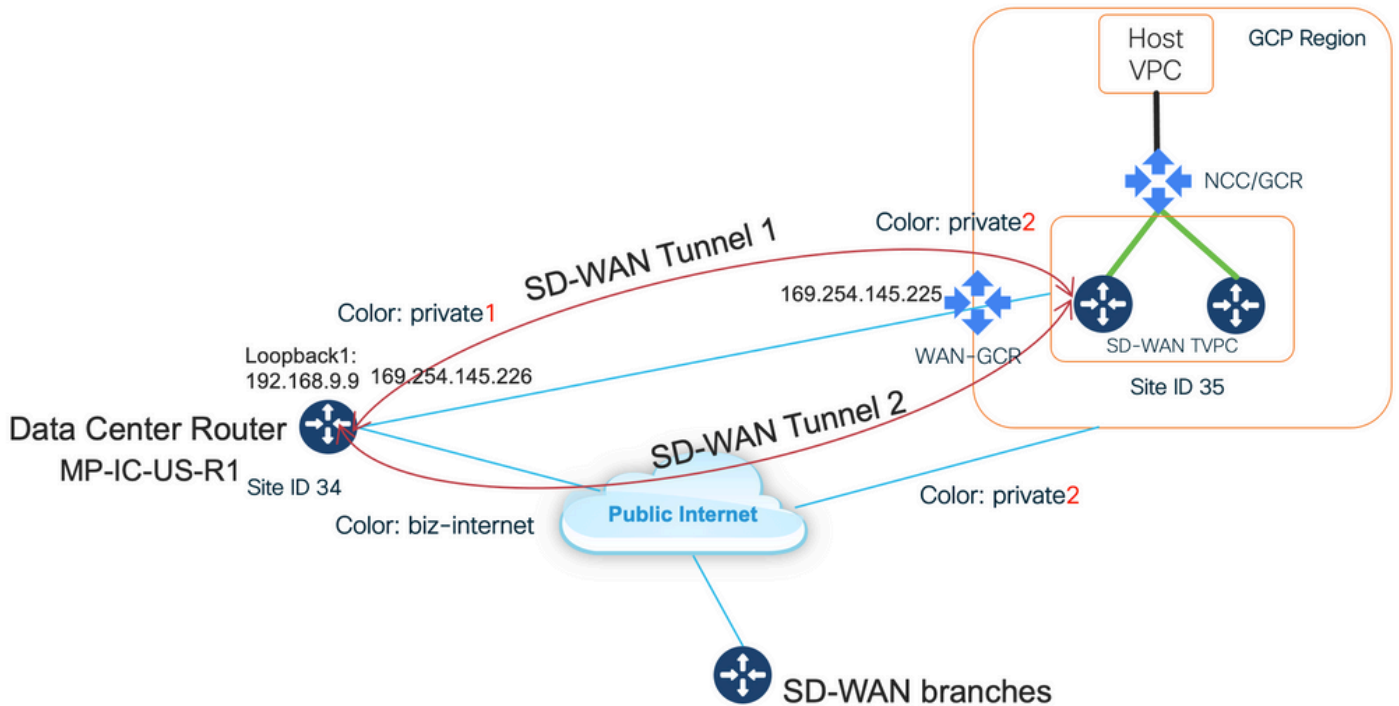
TLOC顏色是靜態定義的關鍵字，用於標識每個SD-WAN路由器上的各個WAN傳輸。給定SD-WAN路由器上的每個WAN傳輸都必須具有唯一的顏色。顏色還用於標識單個WAN傳輸是公共傳輸還是專用傳輸。城域乙太網、Mpls和private1、private2、private3、private4、private5和private6顏色被視為專用顏色。它們用於私有網路或沒有NAT的位置。顏色為3g、biz-internet、藍色、銅色、custom1、custom2、custom3、default、gold、green、lte、public-internet、紅色和銀色被視為公共顏色。它們旨在用於公共網路或具有廣域網傳輸介面的公共IP地址的地方 (本地或通過NAT)。

顏色指示在通過控制和資料平面進行通訊時使用私有IP地址或公有IP地址。當兩台SD-WAN路由器嘗試相互通訊時 (都使用帶專用顏色的WAN傳輸介面)，兩端將嘗試連線到遠端路由器的專用IP地址。如果一端或兩端使用公共顏色，則兩端將嘗試連線到遠端路由器的公共IP地址。當兩台裝置的Site ID相同時，則是一個例外。如果站點ID相同，但顏色為公用，則使用私有IP地址進行通訊。對於嘗試與位於同一站點的vManage或vSmart控制器通訊的SD-WAN路由器，可能會發生這種情況。請注意，預設情況下，SD-WAN路由器在擁有相同的站點ID時不會在彼此之間建立IPsec VPN隧道。

這是資料中心路由器的輸出，其中顯示兩個通過Internet的隧道 (彩色業務網際網路) 和兩個通過GCP雲互聯 (彩色專用1) 到兩個SD-WAN路由器的隧道。有關詳細資訊，請參閱附件中的完整DC路由器配置。

```
MP-IC-US-R1#sh sdwan bfd sessions
SOURCE TLOC REMOTE TLOC DST PUBLIC DST PUBLIC DETECT TX
SYSTEM IP SITE ID STATE COLOR COLOR SOURCE IP IP PORT ENCAP MULTIPLIER INTERVAL(msec UPTIME
TRANSITIONS
-----
-----
-----
35.35.35.2 35 up biz-internet private2 162.43.150.15 35.212.162.72 12347 ipsec 7 1000 10
4:02:55:32 0
35.35.35.1 35 up biz-internet private2 162.43.150.15 35.212.232.51 12347 ipsec 7 1000 10
4:02:55:32 0
35.35.35.1 35 up private1 private2 192.168.9.9 10.35.0.2 12347 ipsec 7 1000 10 0:00:00:16 0
35.35.35.2 35 up private1 private2 192.168.9.9 10.35.0.3 12347 ipsec 7 1000 10 0:00:00:16 0
...
MP-IC-US-R1#
```

此圖說明了用於驗證解決方案的IP地址和SD-WAN顏色的拓撲詳細資訊。



所用軟體：

- 執行CCO版本20.7.1.1的SD-WAN控制器
- 資料中心路由器模擬使用運行17.06.01a的C8000v，通過vManage Cloud onRamp進行調配，用於與巨型埠互連
- GCP中的兩台SD-WAN路由器：運行17.06.01a的C8000v，通過適用於多雲的vManage Cloud onRamp進行調配

步驟1.準備

確保Cisco vManage已定義工作正常的GCP帳戶，並且正確配置了Cloud onRamp全域性設定。

另請在vManage中定義互聯合作夥伴帳戶。在此部落格中，MegaPort用作互連合作夥伴，因此您可以定義相應的帳戶和全域性設定。

步驟2.使用適用於多雲工作流的雲onRamp建立思科雲網關

這是一個簡單的過程：選擇兩台SD-WAN裝置，連線預設GCP模板，部署。有關詳細資訊，請參閱[Cloud onRamp for Multicloud文檔](#)。

步驟3.在GCP控制檯中新增合作夥伴互連連線

使用GCP分步配置工作流(Hybrid Connectivity > Interconnect)建立與選定合作夥伴 (在此部落格中)的合作夥伴互聯連線 — 使用MegaPort，如下圖所示。

Hybrid Connectivity

VPN

Interconnect

Cloud Routers

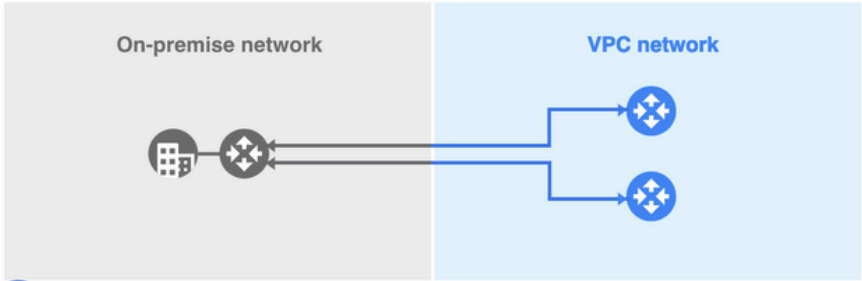
Network Connectivity Center

← Add VLAN attachment

Choose an interconnect type that fits your networking needs:

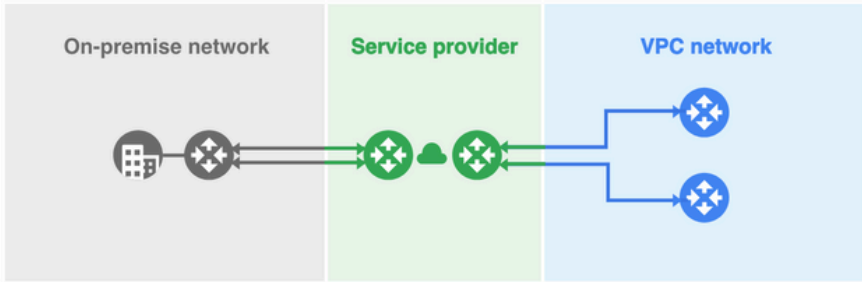
Interconnect type

Dedicated Interconnect connection Connect your on-premises network to your Google Cloud VPC network by connecting a new fiber to your equipment. [Learn more](#)



The diagram shows an 'On-premise network' on the left with a server and a router icon. Two blue lines connect this router to two blue router icons in a 'VPC network' on the right.

Partner Interconnect connection Connect your on-premises network to your Google Cloud VPC network through a connection from a supported service provider. [Learn more](#) or [check supported service providers](#)



The diagram shows an 'On-premise network' on the left with a server and a router icon. A green line connects this router to a green router icon in a 'Service provider' box in the middle. Another green line connects the service provider router to a green router icon in a 'VPC network' on the right. Two blue lines then connect the VPC network router to two blue router icons in the VPC network.

CONTINUE CANCEL

請選擇我已有服務提供商的選項。

為便於演示，使用建立單VLAN選項時沒有冗餘。

選擇正確的網路名稱，該名稱之前由Cloud onRamp for Multicloud工作流程建立。在VLAN部分下，您可以建立新的GCR路由器並定義VLAN的名稱，稍後將在Cloud onRamp Interconnect部分中顯示。

此影象反映了所提到的所有點。

Hybrid Connectivity

VPN

Interconnect

Cloud Routers

Network Connectivity Center

Add Partner VLAN attachment

✓ Check your connection
2 **Add VLAN attachments**
3 Connect to your VPC networks

A VLAN attachment allows you to access your VPC network by adding a VLAN to your existing service provider connection. [Learn more](#)

Redundancy

Creating a redundant pair of VLANs is recommended to increase availability. If you don't need redundancy or an SLA, you can create a single VLAN attachment (and make it redundant later). [Learn more about redundancy](#)

Create a redundant pair of VLAN attachments (recommended)
 Add a redundant VLAN to an existing VLAN
 Create a single VLAN (no redundancy)

Network *
wan-mc-demo-npitaev

Region *
us-west1 (Oregon) ?

Region is permanent

VLAN

Cloud Router *
gcp-gcr-ic-r1 ?

VLAN attachment name *
test-vlan-name ?

Lowercase letters, numbers, hyphens allowed

Description
VLAN for Megaport

Maximum transmission unit (MTU) *
1440

基本上，完成步驟3。之後，您只需獲取BGP配置，並根據互連提供商使用的內容建立連線。在這種情況下，使用Megaport進行測試。但是，您可以使用任何型別的互連，可以通過Megaport、Equinix或MSP。

步驟4.在Cisco vManage中使用Cloud onRamp互連建立DC連線

與AWS部落格類似，將Cisco Cloud onRamp Interconnect工作流程與Megaport結合使用，建立資料中心路由器並將其用於GCP雲互連。請注意，此處使用Megaport只是為了進行測試，如果您已經設定了資料中心，則無需使用Megaport。

在Cisco vManage中，選擇一個免費的SD-WAN路由器，附加預設CoR Megaport模板，並使用CoR Interconnect工作流程將其部署為Megaport中的Cisco Cloud Gateway。

在Megaport中的Cisco SD-WAN路由器處於活動狀態後，請使用CoR Interconnect工作流程建立連線，如下圖所示。

Cisco vManage Select Resource Group Configuration · Cloud onRamp for Multicloud

Cloud OnRamp For Multicloud > Interconnect Connectivity > Add Connection

Interconnect Gateway MP-IC-GW-US1

1 Destination 2 Primary MP-IC-GW-US1 3 Details 4 Summary

DESTINATION

Destination Type: Cloud
 Cloud Service Provider: Google Cloud
 Google Account: GCP-rpitsev
 Redundancy: Disable
 Google Cloud Interconnect Attachment: us-west1:gcp-gcr-ic-r1:gcr-megaport-vlan

DETAILS

Settings: Auto-generated
 Segment: 10

PRIMARY

Peering Location: San Jose (sjc-zone2-6) - San Jose - CA - USA
 Connection Name: MP-GCP-SJ-Peering
 Bandwidth(Mbps): 50

Connection Name : MP-GCP-SJ-Peering

Cancel Back Save

步驟5.配置DC路由器以通過Internet和GCP雲互聯建立隧道

將SD-WAN Megaport路由器設定為CLI模式，並將配置從服務端移至VPN0。由於GCP使用169.254.x.y IP地址，因此您可以在DC路由器上建立Loopback1介面，並將其用於通過GCP雲互聯進行的SD-WAN通訊。

以下是DC路由器配置的相關部分。

```
interface Loopback1
no shutdown
ip address 192.168.9.9 255.255.255.255
!
!
interface Tunnel2
ip unnumbered Loopback1
tunnel source Loopback1
tunnel mode sdwan
!
!
interface GigabitEthernet1.215
encapsulation dot1Q 215
ip address 169.254.145.226 255.255.255.248
ip mtu 1440
!
!
router bgp 64513
bgp log-neighbor-changes
neighbor 169.254.145.225 remote-as 16550
neighbor 169.254.145.225 description MP-GCP-SJ-Peering
neighbor 169.254.145.225 ebgp-multihop 4
!
address-family ipv4
network 192.168.9.9 mask 255.255.255.255
neighbor 169.254.145.225 activate
neighbor 169.254.145.225 send-community both
exit-address-family
!
```

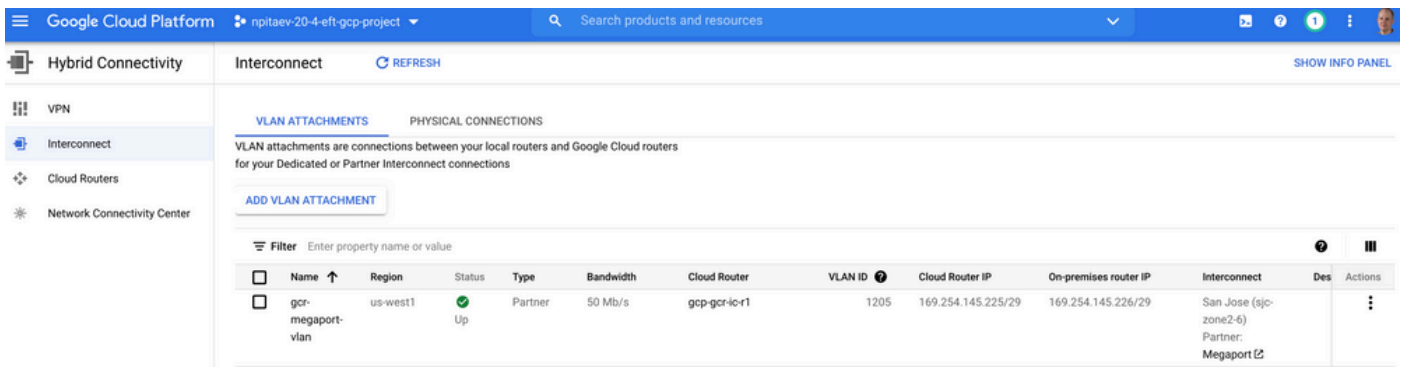


```
!
sdwan
interface Loopback1
tunnel-interface
encapsulation ipsec preference 100 weight 1
color private1
max-control-connections 0
allow-service all
!
```

請參閱本文檔後面部分中的完整DC路由器配置。

驗證

GCP雲互連狀態：



實施雲互連的資料中心路由器和WAN GCR之間的BGP連線：

```
MP-IC-US-R1#sh ip ro bgp
...
10.0.0.0/27 is subnetted, 1 subnets
B 10.35.0.0 [20/100] via 169.254.145.225, 01:25:26
MP-IC-US-R1#
```

DC兆埠SD-WAN路由器配置

```
MP-IC-US-R1#sh sdwan bfd sessions
SOURCE TLOC REMOTE TLOC DST PUBLIC DST PUBLIC DETECT TX
SYSTEM IP SITE ID STATE COLOR COLOR SOURCE IP IP PORT ENCAP MULTIPLIER INTERVAL(msec UPTIME
TRANSITIONS
-----
-----
10.12.1.11 12 up biz-internet public-internet 162.43.150.15 13.55.49.253 12426 ipsec 7 1000 10
4:02:55:32 0
35.35.35.2 35 up biz-internet private2 162.43.150.15 35.212.162.72 12347 ipsec 7 1000 10
4:02:55:32 0
35.35.35.1 35 up biz-internet private2 162.43.150.15 35.212.232.51 12347 ipsec 7 1000 10
4:02:55:32 0
61.61.61.61 61 down biz-internet biz-internet 162.43.150.15 162.43.145.3 12427 ipsec 7 1000 NA 0
61.61.61.61 61 down biz-internet private1 162.43.150.15 198.18.0.5 12367 ipsec 7 1000 NA 0
35.35.35.1 35 up private1 private2 192.168.9.9 10.35.0.2 12347 ipsec 7 1000 10 0:00:00:16 0
35.35.35.2 35 up private1 private2 192.168.9.9 10.35.0.3 12347 ipsec 7 1000 10 0:00:00:16 0
10.12.1.11 12 down private1 public-internet 192.168.9.9 13.55.49.253 12426 ipsec 7 1000 NA 0
61.61.61.61 61 down private1 biz-internet 192.168.9.9 162.43.145.3 12427 ipsec 7 1000 NA 0
61.61.61.61 61 down private1 private1 192.168.9.9 198.18.0.5 12367 ipsec 7 1000 NA 0
```



```
MP-IC-US-R1#sh ip ro bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
&- replicated local route overrides by connected
```

```
Gateway of last resort is 162.43.150.14 to network 0.0.0.0
```

```
10.0.0.0/27 is subnetted, 1 subnets
B 10.35.0.0 [20/100] via 169.254.145.225, 00:03:17
```

```
MP-IC-US-R1#
```

```
MP-IC-US-R1#sh sdwa
```

```
MP-IC-US-R1#sh sdwan runn
```

```
MP-IC-US-R1#sh sdwan running-config
system
```

```
location "55 South Market Street, San Jose, CA -95113, USA"
```

```
gps-location latitude 37.33413
```

```
gps-location longitude -121.8916
```

```
system-ip 34.34.34.1
```

```
overlay-id 1
```

```
site-id 34
```

```
port-offset 1
```

```
control-session-pps 300
```

```
admin-tech-on-failure
```

```
sp-organization-name MC-Demo-npitaev
```

```
organization-name MC-Demo-npitaev
```

```
port-hop
```

```
track-transport
```

```
track-default-gateway
```

```
console-baud-rate 19200
```

```
no on-demand enable
```

```
on-demand idle-timeout 10
```

```
vbond 54.188.241.123 port 12346
```

```
!
```

```
service tcp-keepalives-in
```

```
service tcp-keepalives-out
```

```
no service tcp-small-servers
```

```
no service udp-small-servers
```

```
hostname MP-IC-US-R1
```

```
username admin privilege 15 secret 9
```

```
$9$3V6L3V6L2VUI2k$ysPnXOdg8RLj9KgMdmfHdSHkdaMmiHzGaUpcqH6pfTo
```

```
vrf definition 10
```

```
rd 1:10
```

```
address-family ipv4
```

```
route-target export 64513:10
```

```
route-target import 64513:10
```

```
exit-address-family
```

```
!
```

```
address-family ipv6
```

```
exit-address-family
```

```
!
```

```
!
```

```
ip arp proxy disable
```

```
no ip finger
```

```
no ip rcmd rcp-enable
```

```
no ip rcmd rsh-enable
```

```
no ip dhcp use class
ip bootp server
no ip source-route
no ip http server
no ip http secure-server
ip nat settings central-policy
cdp run
interface GigabitEthernet1
no shutdown
arp timeout 1200
ip address dhcp client-id GigabitEthernet1
no ip redirects
ip dhcp client default-router distance 1
ip mtu 1500
load-interval 30
mtu 1500
negotiation auto
exit
interface GigabitEthernet1.215
no shutdown
encapsulation dot1Q 215
ip address 169.254.145.226 255.255.255.248
no ip redirects
ip mtu 1440
exit
interface Loopback1
no shutdown
ip address 192.168.9.9 255.255.255.255
exit
interface Tunnel1
no shutdown
ip unnumbered GigabitEthernet1
no ip redirects
ipv6 unnumbered GigabitEthernet1
no ipv6 redirects
tunnel source GigabitEthernet1
tunnel mode sdwan
exit
interface Tunnel2
no shutdown
ip unnumbered Loopback1
no ip redirects
ipv6 unnumbered Loopback1
no ipv6 redirects
tunnel source Loopback1
tunnel mode sdwan
exit
clock timezone UTC 0 0
logging persistent size 104857600 filesize 10485760
no logging monitor
logging buffered 512000
logging console
aaa authentication login default local
aaa authorization exec default local
aaa server radius dynamic-author
!
router bgp 64513
bgp log-neighbor-changes
neighbor 169.254.145.225 remote-as 16550
neighbor 169.254.145.225 description MP-GCP-SJ-Peering
neighbor 169.254.145.225 ebgp-multihop 4
address-family ipv4 unicast
neighbor 169.254.145.225 activate
neighbor 169.254.145.225 send-community both
```

```
network 192.168.9.9 mask 255.255.255.255
exit-address-family
!
timers bgp 60 180
!
snmp-server ifindex persist
line aux 0
stopbits 1
!
line con 0
speed 19200
stopbits 1
!
line vty 0 4
transport input ssh
!
line vty 5 80
transport input ssh
!
lldp run
nat64 translation timeout tcp 3600
nat64 translation timeout udp 300
sdwan
interface GigabitEthernet1
tunnel-interface
encapsulation ipsec weight 1
no border
color biz-internet
no last-resort-circuit
no low-bandwidth-link
no vbond-as-stun-server
vmanage-connection-preference 5
port-hop
carrier default
nat-refresh-interval 5
hello-interval 1000
hello-tolerance 12
allow-service all
no allow-service bgp
allow-service dhcp
allow-service dns
allow-service icmp
allow-service sshd
no allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
allow-service https
no allow-service snmp
no allow-service bfd
exit
exit
interface Loopback1
tunnel-interface
encapsulation ipsec preference 100 weight 1
color privatel
max-control-connections 0
allow-service all
no allow-service bgp
allow-service dhcp
allow-service dns
allow-service icmp
no allow-service sshd
no allow-service netconf
```

```
no allow-service ntp
no allow-service ospf
no allow-service stun
allow-service https
no allow-service snmp
no allow-service bfd
exit
exit
appqoe
no tcptopt enable
no dreopt enable
!
omp
no shutdown
send-path-limit 4
ecmp-limit 4
graceful-restart
no as-dot-notation
timers
holdtime 60
advertisement-interval 1
graceful-restart-timer 43200
eor-timer 300
exit
address-family ipv4
advertise bgp
advertise connected
advertise static
!
address-family ipv6
advertise bgp
advertise connected
advertise static
!
!
!
licensing config enable false
licensing config privacy hostname false
licensing config privacy version false
licensing config utility utility-enable false
bfd color lte
hello-interval 1000
no pmtu-discovery
multiplier 1
!
bfd default-dscp 48
bfd app-route multiplier 2
bfd app-route poll-interval 123400
security
ipsec
rekey 86400
replay-window 512
!
!
sslproxy
no enable
rsa-key-modulus 2048
certificate-lifetime 730
eckey-type P256
ca-tp-label PROXY-SIGNING-CA
settings expired-certificate drop
settings untrusted-certificate drop
settings unknown-status drop
settings certificate-revocation-check none
```

```
settings unsupported-protocol-versions drop
settings unsupported-cipher-suites drop
settings failure-mode close
settings minimum-tls-ver TLSv1
dual-side optimization enable
!
```

```
MP-IC-US-R1#
MP-IC-US-R1#
MP-IC-US-R1#
MP-IC-US-R1#sh run
Building configuration...
```

```
Current configuration : 4628 bytes
!
! Last configuration change at 19:42:11 UTC Tue Jan 25 2022 by admin
!
version 17.6
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
! Call-home is enabled by Smart-Licensing.
service call-home
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
platform console virtual
!
hostname MP-IC-US-R1
!
boot-start-marker
boot-end-marker
!
!
vrf definition 10
rd 1:10
!
address-family ipv4
route-target export 64513:10
route-target import 64513:10
exit-address-family
!
address-family ipv6
exit-address-family
!
vrf definition 65528
!
address-family ipv4
exit-address-family
!
logging buffered 512000
logging persistent size 104857600 filesize 10485760
no logging monitor
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization exec default local
!
!
!
```

```
!  
aaa server radius dynamic-author  
!  
aaa session-id common  
fhrp version vrrp v3  
ip arp proxy disable  
!  
!  
!  
!  
!  
!  
ip bootp server  
no ip dhcp use class  
!  
!  
no login on-success log  
ipv6 unicast-routing  
!  
!  
!  
!  
!  
!  
subscriber templating  
!  
!  
!  
!  
!  
!  
multilink bundle-name authenticated  
!  
!  
!  
!  
!  
!  
!  
crypto pki trustpoint TP-self-signed-1238782368  
enrollment selfsigned  
subject-name cn=IOS-Self-Signed-Certificate-1238782368  
revocation-check none  
rsa-keypair TP-self-signed-1238782368  
!  
crypto pki trustpoint SLA-TrustPoint  
enrollment pkcs12  
revocation-check crl  
!  
!  
crypto pki certificate chain TP-self-signed-1238782368  
crypto pki certificate chain SLA-TrustPoint  
!  
!  
!  
!  
!  
!
```



```
tunnel mode sdwan
!
interface GigabitEthernet1
ip dhcp client default-router distance 1
ip address dhcp client-id GigabitEthernet1
no ip redirects
load-interval 30
negotiation auto
arp timeout 1200
!
interface GigabitEthernet1.215
encapsulation dot1Q 215
ip address 169.254.145.226 255.255.255.248
no ip redirects
ip mtu 1440
arp timeout 1200
!
router omp
!
router bgp 64513
bgp log-neighbor-changes
neighbor 169.254.145.225 remote-as 16550
neighbor 169.254.145.225 description MP-GCP-SJ-Peering
neighbor 169.254.145.225 ebgp-multihop 4
!
address-family ipv4
network 192.168.9.9 mask 255.255.255.255
neighbor 169.254.145.225 activate
neighbor 169.254.145.225 send-community both
exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ip nat settings central-policy
ip nat route vrf 65528 0.0.0.0 0.0.0.0 global
no ip nat service H225
no ip nat service ras
no ip nat service rtsp udp
no ip nat service rtsp tcp
no ip nat service netbios-ns tcp
no ip nat service netbios-ns udp
no ip nat service netbios-ssn
no ip nat service netbios-dgm
no ip nat service ldap
no ip nat service sunrpc udp
no ip nat service sunrpc tcp
no ip nat service msrpc tcp
no ip nat service tftp
no ip nat service rcmd
no ip nat service pptp
no ip ftp passive
ip scp server enable
!
!
!
!
!
!
!
!
!
control-plane
!
```

```
!  
mgcp behavior rsip-range tgcp-only  
mgcp behavior comedia-role none  
mgcp behavior comedia-check-media-src disable  
mgcp behavior comedia-sdp-force disable  
!  
mgcp profile default  
!  
!  
!  
!  
!  
line con 0  
stopbits 1  
speed 19200  
line aux 0  
line vty 0 4  
transport input ssh  
line vty 5 80  
transport input ssh  
!  
nat64 translation timeout udp 300  
nat64 translation timeout tcp 3600  
call-home  
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com  
! the email address configured in Cisco Smart License Portal will be used as contact email  
address to send SCH notifications.  
contact-email-addr sch-smart-licensing@cisco.com  
profile "CiscoTAC-1"  
active  
destination transport-method http  
!  
!  
!  
!  
!  
!  
netconf-yang  
netconf-yang feature candidate-datastore  
end  
  
MP-IC-US-R1#  
MP-IC-US-R1#  
MP-IC-US-R1#sh ver  
Cisco IOS XE Software, Version 17.06.01a  
Cisco IOS Software [Bengaluru], Virtual XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version  
17.6.1a, RELEASE SOFTWARE (fc2)  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2021 by Cisco Systems, Inc.  
Compiled Sat 21-Aug-21 03:20 by mcpre
```

Cisco IOS-XE software, Copyright (c) 2005-2021 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.

ROM: IOS-XE ROMMON

MP-IC-US-R1 uptime is 4 days, 3 hours, 2 minutes
Uptime for this control processor is 4 days, 3 hours, 3 minutes
System returned to ROM by reload
System image file is "bootflash:packages.conf"
Last reload reason: factory-reset

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wvl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

Technology Package License Information:
Controller-managed

The current throughput level is 250000 kbps

Smart Licensing Status: Registration Not Applicable/Not Applicable

cisco C8000V (VXE) processor (revision VXE) with 2028465K/3075K bytes of memory.
Processor board ID 9SRWHHH66II
Router operating mode: Controller-Managed
1 Gigabit Ethernet interface
32768K bytes of non-volatile configuration memory.
3965112K bytes of physical memory.
11526144K bytes of virtual hard disk at bootflash:.

Configuration register is 0x2102

MP-IC-US-R1#