

في ا ه ا ح ا ل ص ا و ة ي ئ ا ق ل ل ت ل ا R P ا ط ا خ ا ف ا ش ك ت س ا Cisco ن م SD-WAN د د ع ت م ل ا ث ب ل ا ر ش ن

ت ا ي و ت ح م ل ا

[ة م د ق م ل ا](#)

[ة ي س ا س ا ت ا م و ل ع م](#)

[ا ي ج و ل و ب و ط ل ا ط ا خ م](#)

[Cisco ن م SD-WAN د د ع ت م ل ا ث ب ل ا ر ش ن ت ا ر ا ب ت ع ا](#)

[ت ا ط ا ح ا ل م](#)

[ق ن ك م م ل ا ل و ل ح ل ا](#)

[ب ا ر ق ل ا](#)

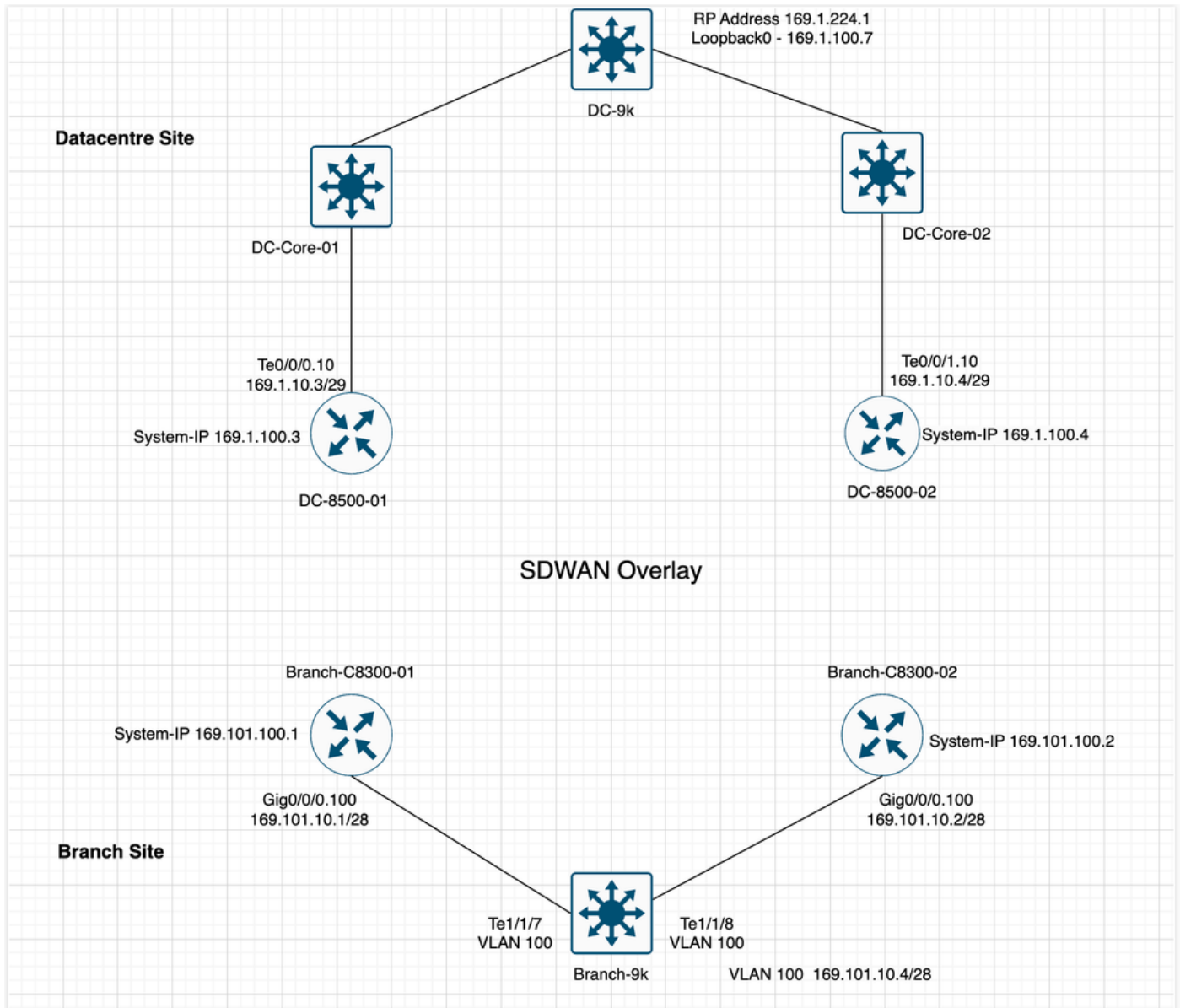
ة م د ق م ل ا

ة ط ق ن) Auto-RP ن ي ي ع ت م ل ع ت ي ف ي و ن ا ث ل ا ع ر ف ل ا ه ج و م ل ش ف ب ب س د ن ت س م ل ا ا ذ ه ح ض و ي
ة ل ك ش م ل ا ل ح ل ت ا و ط خ ر ف و ي و (ء ا ق ت ل ل ا ل ا

ة ي س ا س ا ت ا م و ل ع م

ة ف ر ع م ي س ا س ا ل ا SD-WAN ه ج و م ل ن ك م ي ، SD-WAN ع ر ف ع ق و م ي ف ج و د ز م د ح ه ج و م د ا د ع ا ي ف
م ل ا ذ ا . ك ل ذ ي ل ع ي و ن ا ث ل ا SD-WAN ه ج و م ف ر ع ت ي ا ل ا م ن ي ب ي ئ ا ق ل ل ت ل ا R P ن ي ي ع ت ل ئ ا س ر
ل و ك و ت و ر ب ل ا ن ع ل ق ت س م ل ا د د ع ت م ل ا ث ب ل ل ه ج و م ك ه ب ا خ ت ن ا م ت ي ذ ل ا SD-WAN ه ج و م ف ر ع ت ي
ي ق ل ت ت ن ل ع ر ف ل ا ي ف م د ا خ ل ا ن م ت ا ن ا ي ب ل ا ق ف د ت ت ا ل و ح م ن ا ف ، Auto-RP ن ي ي ع ت ي ل ع (PIM)
ت ا ن ي ي ع ت ل ا ه ذ ه ا ض ي ا .

ا ي ج و ل و ب و ط ل ا ط ا خ م



- يوتحت Branch-C8300-01 و Branch-C8300-02 SD-WAN عرفال عقوم في ،ططخمل اذه في
 مداخل لى لى Branch-9k لوحمل عم (OSPF) "الوأ راسم رصقأ حتف" راوجل القطنم لى
 10، غلبت OSPF فلكتب يسىئرل هجومال C8300-01 عرفال هجومال دعي VRF/VPN 10.
 15، غلبت Branch-C8300-02 يونال هجومال في OSPF فلكت نأ نىح في
- حاتفم اذه لى لى ليكشلتل انه RP. وه تانايبل زكرم عقوم في DC-9k لوحمل ربتعي

```
ip pim rp-address 169.1.224.1 override
ip pim autorp listener
ip pim send-rp-announce Loopback1 scope 30 group-list RP-Groups
ip pim send-rp-discovery Loopback0 scope 30
ip pim ssm range PIM-SSM-Range
```

```
dc1-9k-01#sh ip access-lists RP-Groups
Standard IP access list RP-Groups
 30 permit 239.1.0.0, wildcard bits 0.0.255.255
```

Cisco SD-WAN ددعتم ال ثبل رشن تارابتعا

- زكرم عقوم ةزهجأ ىلع ركرم ال ةدقعو ددعتم ال ثبل او ءاقت الال ةطقن نيوكت كنكمي .يعرف ال عقوم ال ةزهجأ ىلع ركرم ال نيوكت كنكمي ال .طقف تانايب ال
- زكرم ب ةصاخ ال LAN ةكبش بناج ىلع حشرم ال RP و نييعت ال ليك و رشن كنكمي .تانايب ال
- Cisco Auto-RP عضو وليطعت بجي . PIM BSR عم اعم Cisco Auto-RP دجاوتي نأ كنكمي ال SPT-only عضو م ادختساب
- cisco لك ،عقوم هسفن ال ي ف ةادأ cisco IOS XE Catalyst SD-WAN ناثا تنأ ىقلى تي نأ نأ رورم ال ةكرحل ةلثامتم ةخسنك تللكش نوكي نأ جاتحي ةادأ IOS XE Catalyst SD-WAN .قفدت ي
- RP حشرم نيوكتل اهم ادختسا كنكمي ي تي ال ةهجاو ال عاونأ نم ديدع ال نم دحاو وه عاجرتسا ال

تاظحال

- ةوطخل (هجوم) لبقتسم ال ةياهن نم أدبت نأ بجي ،ددعتم ال ثبل تاقفدت عبتت دنع هجوم وه Branch-9k ،انه .(ىلوالا ةوطخل هجوم) ردصم ال ةياهن ىل لقتنتو (ةريخأ ال LHR). ةريخأ ال ةوطخل
- AutoRP. نييعت ىقلى تي لوحم ال نكي مل ،عرف ال بناج ىلع هديدت دنع

```
Branch-9k#sh ip pim rp mapping
PIM Group-to-RP Mappings
```

```
Branch-9k#
```

لوحم ال ىلع PIM تانايبوكت:

```
Branch-9k#sh run | in pim
ip pim sparse-mode
ip pim sparse-mode
ip pim sparse-mode
ip pim autorp listener
ip pim ssm range PIM-SSM-Range
Branch-9k#
```

- ،عرف ال تاهجوم ىلع (MFIB) ددعتم ال ثبل هي جوت ةداعا تامولعم ةدعاق نم ققحت ال دنع ةعومجم ال AutoRP مدختسي . RP ةهجاو حي قنت مت ، 01 يعرف ال هجوم ال ىلع هنأ ظحول show جارخا ي ف RP ةهجاو ال F ةمالع ي نييعت متي مل . RP تامولعم نع نالعالل 224.0.1.40 02 عرف ال هجوم ىلع F ةمالع نييعت مت . 01 يعرف ال هجوم ال نم ip pim mfib

<#root>

Branch-C8300-01#sh ip mfib vrf 10 224.0.1.40

Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
ET - Data Rate Exceeds Threshold, K - Keepalive
DDE - Data Driven Event, HW - Hardware Installed
ME - MoFRR ECMP entry, MNE - MoFRR Non-ECMP entry, MP - MFIB
MoFRR Primary, RP - MRIB MoFRR Primary, P - MoFRR Primary
MS - MoFRR Entry in Sync, MC - MoFRR entry in MoFRR Client,
e - Encap helper tunnel flag.

I/O Item Flags: IC - Internal Copy, NP - Not platform switched,
NS - Negate Signalling, SP - Signal Present,
A - Accept, F - Forward, RA - MRIB Accept, RF - MRIB Forward,
MA - MFIB Accept, A2 - Accept backup,
RA2 - MRIB Accept backup, MA2 - MFIB Accept backup

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second

Other counts: Total/RPF failed/Other drops

I/O Item Counts: HW Pkt Count/FS Pkt Count/PS Pkt Count Egress Rate in pps
VRF 10

(* ,224.0.1.40) Flags: C HW

SW Forwarding: 0/0/0/0, Other: 0/0/0

HW Forwarding: 0/0/0/0, Other: 1741/1741/0

Lspvif0, LSM/0, RPF-ID: *, Flags: F NS

Pkts: 0/0/0 Rate: 0 pps

GigabitEthernet0/0/0.100 Flags: F IC NS

Pkts: 0/0/0 Rate: 0 pps

(169.1.10.3,224.0.1.40) Flags: HW

SW Forwarding: 0/0/0/0, Other: 0/0/0

HW Forwarding: 0/0/0/0, Other: 29642/29642/0

Lspvif0, LSM/0, RPF-ID: *, Flags: A

GigabitEthernet0/0/0.100 Flags: IC

(169.1.10.4,224.0.1.40) Flags: HW

SW Forwarding: 0/0/0/0, Other: 0/0/0

HW Forwarding: 0/0/0/0, Other: 29939/29939/0

Lspvif0, LSM/0, RPF-ID: *, Flags: A NS

GigabitEthernet0/0/0.100 Flags: IC

(169.1.20.2,224.0.1.40) Flags: HW

SW Forwarding: 0/0/0/0, Other: 0/0/0

HW Forwarding: 0/0/0/0, Other: 47783/47783/0

Lspvif0, LSM/0, RPF-ID: *, Flags: A

GigabitEthernet0/0/0.100 Flags: IC

(169.1.20.6,224.0.1.40) Flags: HW

SW Forwarding: 0/0/0/0, Other: 0/0/0

HW Forwarding: 0/0/0/0, Other: 47720/47720/0

Lspvif0, LSM/0, RPF-ID: *, Flags: A

GigabitEthernet0/0/0.100 Flags: IC

(169.1.20.10,224.0.1.40) Flags: HW

SW Forwarding: 0/0/0/0, Other: 0/0/0

HW Forwarding: 0/0/0/0, Other: 47784/47784/0

Lspvif0, LSM/0, RPF-ID: *, Flags: A

GigabitEthernet0/0/0.100 Flags: IC

(169.1.20.14,224.0.1.40) Flags: HW

SW Forwarding: 0/0/0/0, Other: 0/0/0

HW Forwarding: 0/0/0/0, Other: 47724/47724/0

Lspvif0, LSM/0, RPF-ID: *, Flags: A

GigabitEthernet0/0/0.100 Flags: IC

(169.1.100.7,224.0.1.40) Flags: HW

SW Forwarding: 0/0/0/0, Other: 0/0/0

HW Forwarding: 0/0/0/0, Other: 60088/60088/0

Lspvif0, LSM/0, RPF-ID: *, Flags: A

GigabitEthernet0/0/0.100 Flags: IC

(169.2.20.2,224.0.1.40) Flags: HW

```
SW Forwarding: 0/0/0/0, Other: 0/0/0
HW Forwarding: 0/0/0/0, Other: 47680/47680/0
Lspvif0, LSM/0, RPF-ID: *, Flags: A
GigabitEthernet0/0/0.100 Flags: IC
(169.2.20.6,224.0.1.40) Flags: HW
SW Forwarding: 0/0/0/0, Other: 0/0/0
HW Forwarding: 0/0/0/0, Other: 47640/47640/0
Lspvif0, LSM/0, RPF-ID: *, Flags: A
GigabitEthernet0/0/0.100 Flags: IC
Branch-C8300-01#
```

```
Branch-C8300-02#sh ip mfib vrf 10 224.0.1.40
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
ET - Data Rate Exceeds Threshold, K - Keepalive
DDE - Data Driven Event, HW - Hardware Installed
ME - MoFRR ECMP entry, MNE - MoFRR Non-ECMP entry, MP - MFIB
MoFRR Primary, RP - MRIB MoFRR Primary, P - MoFRR Primary
MS - MoFRR Entry in Sync, MC - MoFRR entry in MoFRR Client,
e - Encap helper tunnel flag.
I/O Item Flags: IC - Internal Copy, NP - Not platform switched,
NS - Negate Signalling, SP - Signal Present,
A - Accept, F - Forward, RA - MRIB Accept, RF - MRIB Forward,
MA - MFIB Accept, A2 - Accept backup,
RA2 - MRIB Accept backup, MA2 - MFIB Accept backup
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
I/O Item Counts: HW Pkt Count/FS Pkt Count/PS Pkt Count Egress Rate in pps
VRF 10
```

```
(* ,224.0.1.40) Flags: C HW
SW Forwarding: 0/0/0/0, Other: 0/0/0
HW Forwarding: 0/0/0/0, Other: 10549/10549/0
Lspvif0, LSM/0, RPF-ID: *, Flags: F NS
Pkts: 0/0/0 Rate: 0 pps
GigabitEthernet0/0/0.100 Flags: F IC NS
Pkts: 0/0/0 Rate: 0 pps
```

(169.1.10.3,224.0.1.40) Flags: HW

SW Forwarding: 0/0/0/0, Other: 0/0/0

HW Forwarding: 0/0/0/0, Other: 0/0/0

Lspvif0, LSM/0, RPF-ID: *, Flags: A NS

GigabitEthernet0/0/0.100 Flags: F IC NS <==

Pkts: 0/0/0 Rate: 0 pps

(169.1.10.4,224.0.1.40) Flags: HW

SW Forwarding: 0/0/0/0, Other: 0/0/0

HW Forwarding: 0/0/0/0, Other: 0/0/0

Lspvif0, LSM/0, RPF-ID: *, Flags: A NS

GigabitEthernet0/0/0.100 Flags: F IC NS <==

Pkts: 0/0/0 Rate: 0 pps

(169.1.20.2,224.0.1.40) Flags: HW
SW Forwarding: 0/0/0/0, Other: 0/0/0
HW Forwarding: 0/0/0/0, Other: 0/0/0
Lspvif0, LSM/0, RPF-ID: *, Flags: A
GigabitEthernet0/0/0.100 Flags: F IC NS
Pkts: 0/0/0 Rate: 0 pps

(169.1.20.6,224.0.1.40) Flags: HW
SW Forwarding: 0/0/0/0, Other: 0/0/0
HW Forwarding: 0/0/0/0, Other: 0/0/0
Lspvif0, LSM/0, RPF-ID: *, Flags: A
GigabitEthernet0/0/0.100 Flags: F IC NS
Pkts: 0/0/0 Rate: 0 pps

(169.1.20.10,224.0.1.40) Flags: HW
SW Forwarding: 0/0/0/0, Other: 0/0/0
HW Forwarding: 0/0/0/0, Other: 0/0/0
Lspvif0, LSM/0, RPF-ID: *, Flags: A NS
GigabitEthernet0/0/0.100 Flags: F IC NS
Pkts: 0/0/0 Rate: 0 pps

(169.1.20.14,224.0.1.40) Flags: HW
SW Forwarding: 0/0/0/0, Other: 0/0/0
HW Forwarding: 0/0/0/0, Other: 0/0/0
Lspvif0, LSM/0, RPF-ID: *, Flags: A NS
GigabitEthernet0/0/0.100 Flags: F IC NS
Pkts: 0/0/0 Rate: 0 pps

(169.2.20.2,224.0.1.40) Flags: HW
SW Forwarding: 0/0/0/0, Other: 0/0/0
HW Forwarding: 0/0/0/0, Other: 0/0/0
Lspvif0, LSM/0, RPF-ID: *, Flags: A
GigabitEthernet0/0/0.100 Flags: F IC NS
Pkts: 0/0/0 Rate: 0 pps

(169.2.20.6,224.0.1.40) Flags: HW
SW Forwarding: 0/0/0/0, Other: 0/0/0
HW Forwarding: 0/0/0/0, Other: 0/0/0
Lspvif0, LSM/0, RPF-ID: *, Flags: A
GigabitEthernet0/0/0.100 Flags: F IC NS
Pkts: 0/0/0 Rate: 0 pps

Branch-C8300-02#

ل نې عمال هجومال وه Branch-C8300-02 هجومال نأ ل اهنې يعت متي تي ال F عمال ع ريشت
هسفن ثبل لاجم في PIM ل قرواجم ل لودل نوكت امدن ع. ددعتم ل ثبل رورم كرحلو و AutoRP
IP ناونع ل عأ بحاص هجومال رايتخا متي. PIM Assert OrderDer/Specified OrderDer رايتخا متي
اذه في (نې لثام تم سايقم ل او (AD) Active Directory ناك). ددحم هجوم/ PIM دي كأت هجومك
1: يعرف ل هجوم ل اب قنراقم ل عأ IP ناونع ل ع 2 يعرف ل هجوم ل يوتحي، وي رانې س ل

```
Branch-C8300-01#sh run interface Gi0/0/0.100
Building configuration...
Current configuration : 336 bytes
!
interface GigabitEthernet0/0/0.100
 description OSPF peering interface1
 encapsulation dot1Q 100
 vrf forwarding 10
 ip address 169.101.10.1 255.255.255.240
 no ip redirects
 ip pim sparse-mode
 ip nbar protocol-discovery
 ip ospf network broadcast
 ip ospf dead-interval 40
 ip ospf 10 area 0
 ip ospf cost 10
 arp timeout 1200
end
```

```
Branch-C8300-02#sh run interface Gi0/0/0.100
Building configuration...
Current configuration : 336 bytes
!
interface GigabitEthernet0/0/0.100
 description OSPF peering interface1
 encapsulation dot1Q 100
 vrf forwarding 10
 ip address 169.101.10.2 255.255.255.240
 no ip redirects
 ip pim sparse-mode
 ip nbar protocol-discovery
 ip ospf network broadcast
 ip ospf dead-interval 40
 ip ospf 10 area 0
 ip ospf cost 15
 arp timeout 1200
end
```

- نكي مل 02 عرفال هجوم نكلو، AutoRP لئاسر ريقلتي ناك 01 عرفال هجوم نأة طحال م مت لئاسر ريقلتي AutoRP:

```
Branch-C8300-01#sh ip pim vrf 10 rp mapping
PIM Group-to-RP Mappings
Group(s) 239.195.0.0/16
  RP 10.125.125.1 (?), v2v1
    Info source: 169.254.100.9 (?), elected via Auto-RP
    Uptime: 1w0d, expires: 00:02:31
Branch-C8300-01#
```

```
Branch-C8300-02#sh ip pim vrf 10 rp mapping
PIM Group-to-RP Mappings
```

- ال يلاتلابو S,G، بيذشت متي، ديكاتلاب زئافال نوكي ال 01 يعرفال هجومال نا امب
يتح، 02 يعرفال هجومال يلعو، ليزننل لوجم ال AutoRP نييعت هيحوت ةداعإ هنكمي
هيحوت ةداعإ هنكمي الو، AutoRP نييعت ةلاسر ملعتي مل هنإف، هجومك هنيعت مت ولو
ةلاسر يلع فرعتال متي مل اذامل وه نآلا لاؤسلالو. اتانايبال قفدت لوجم ال AutoRP
02 يعرفال هجومال ةطساوب ةيئاقللل RP.
- (DC) لاجملاب مكحتال ةدحو دودح تاهجوم نم AutoRP نييعت يلع عرفال تاهجوم فرعتت
RP نييعتال ليكوددحي. نييعت ءالكوو ةفاضل تادحوك DC ل SD-WAN تاهجوم لمعت
ددعتال ثبلال نم ةنيعم ةعومجمل حشرمال
- ةمالع دوجو ةطحال م تمتو MFIB نم ققحتال مت، رمتسمل رايتلل SD-WAN هجوم يلع
S,G: لاخلال اهنيعت مت هيحوت ةداعإ

<#root>

DC-8500-01#sh ip mfib vrf 10 224.0.1.40

Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
ET - Data Rate Exceeds Threshold, K - Keepalive
DDE - Data Driven Event, HW - Hardware Installed
ME - MoFRR ECMP entry, MNE - MoFRR Non-ECMP entry, MP - MFIB
MoFRR Primary, RP - MRIB MoFRR Primary, P - MoFRR Primary
MS - MoFRR Entry in Sync, MC - MoFRR entry in MoFRR Client,
e - Encap helper tunnel flag.

I/O Item Flags: IC - Internal Copy, NP - Not platform switched,
NS - Negate Signalling, SP - Signal Present,
A - Accept, F - Forward, RA - MRIB Accept, RF - MRIB Forward,
MA - MFIB Accept, A2 - Accept backup,
RA2 - MRIB Accept backup, MA2 - MFIB Accept backup

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second

Other counts: Total/RPF failed/Other drops

I/O Item Counts: HW Pkt Count/FS Pkt Count/PS Pkt Count Egress Rate in pps

VRF 10

(*,224.0.1.40) Flags: C HW

SW Forwarding: 0/0/0/0, Other: 0/0/0

HW Forwarding: 0/0/0/0, Other: 294/294/0

TenGigabitEthernet0/0/0.10 Flags: F IC NS

Pkts: 0/0/0 Rate: 0 pps

Lspvif0, LSM/1, RPF-ID: *, Flags: F NS

Pkts: 0/0/0 Rate: 0 pps

(169.1.10.4,224.0.1.40) Flags: HW

SW Forwarding: 0/0/0/0, Other: 0/0/0

HW Forwarding: 0/0/0/0, Other: 0/0/0

TenGigabitEthernet0/0/0.10 Flags: A IC

Lspvif0, LSM/1, RPF-ID: *, Flags: F

Pkts: 0/0/0 Rate: 0 pps

(169.1.20.2,224.0.1.40) Flags: HW

SW Forwarding: 0/0/0/0, Other: 0/0/0

HW Forwarding: 0/0/0/0, Other: 0/0/0

TenGigabitEthernet0/0/0.10 Flags: A IC

Lspvif0, LSM/1, RPF-ID: *, Flags: F

Pkts: 0/0/0 Rate: 0 pps

(169.1.20.6,224.0.1.40) Flags: HW

SW Forwarding: 0/0/0/0, Other: 0/0/0

```
HW Forwarding: 0/0/0/0, Other: 0/0/0
TenGigabitEthernet0/0/0.10 Flags: A IC
Lspvif0, LSM/1, RPF-ID: *, Flags: F
Pkts: 0/0/0 Rate: 0 pps
(169.1.20.10,224.0.1.40) Flags: HW
SW Forwarding: 0/0/0/0, Other: 0/0/0
HW Forwarding: 0/0/0/0, Other: 0/0/0
TenGigabitEthernet0/0/0.10 Flags: A IC
Lspvif0, LSM/1, RPF-ID: *, Flags: F
Pkts: 0/0/0 Rate: 0 pps
(169.1.20.14,224.0.1.40) Flags: HW
SW Forwarding: 0/0/0/0, Other: 0/0/0
HW Forwarding: 0/0/0/0, Other: 0/0/0
TenGigabitEthernet0/0/0.10 Flags: A IC
Lspvif0, LSM/1, RPF-ID: *, Flags: F
Pkts: 0/0/0 Rate: 0 pps
(169.1.100.7,224.0.1.40) Flags: HW
```

SW Forwarding: 0/0/0/0, Other: 0/0/0

HW Forwarding: 0/0/0/0, Other: 0/0/0

TenGigabitEthernet0/0/0.10 Flags: A IC

Lspvif0, LSM/1, RPF-ID: *, Flags: F <==

Pkts: 0/0/0 Rate: 0 pps

```
(169.2.20.2,224.0.1.40) Flags: HW
SW Forwarding: 0/0/0/0, Other: 0/0/0
HW Forwarding: 0/0/0/0, Other: 0/0/0
TenGigabitEthernet0/0/0.10 Flags: A IC
Lspvif0, LSM/1, RPF-ID: *, Flags: F
Pkts: 0/0/0 Rate: 0 pps
(169.2.20.6,224.0.1.40) Flags: HW
SW Forwarding: 0/0/0/0, Other: 0/0/0
HW Forwarding: 0/0/0/0, Other: 0/0/0
TenGigabitEthernet0/0/0.10 Flags: A IC
Lspvif0, LSM/1, RPF-ID: *, Flags: F
Pkts: 0/0/0 Rate: 0 pps
```

ةطقن ي (P2MP) طاقنن لةدعت م لةطقن نم قفن لثم ةيره اظلل قفنن لةهجاو وه LSPVIF0
دعت م لثب ل ف LSPVIF0 قفن مادختس ل متي .ةديعب ةدعت م ةياهن طاقن ل لةدحاو ةياهن
SD-WAN. SD-WAN ةيشغت لالخن نم مزحل لاسر ل لريشي لذل يره اظلل قفنن ل وه LSPVIF0

```
DC-8500-01#sh interfaces Lspvif0
Lspvif0 is up, line protocol is up
Hardware is
```

```

Interface is unnumbered. Using address of SD-WAN-system-intf (169.1.100.3)
MTU 17892 bytes, BW 10000000 Kbit/sec, DLY 5000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation LOOPBACK, loopback not set
Keepalive set (10 sec)
Last input never, output 00:00:10, output hang never
Last clearing of "show interface" counters never
Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
    3 packets input, 210 bytes, 0 no buffer
    Received 0 broadcasts (3 IP multicasts)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    1628856 packets output, 71967520 bytes, 0 underruns
    Output 0 broadcasts (1289488 IP multicasts)
    0 output errors, 0 collisions, 0 interface resets
    0 unknown protocol drops
    0 output buffer failures, 0 output buffers swapped out

```

Lspvif0. قفنب ةقفرملا لثامملا خسنلا ةمئاق ىلإ MFIB جارخا يف LSM/1 ري شي

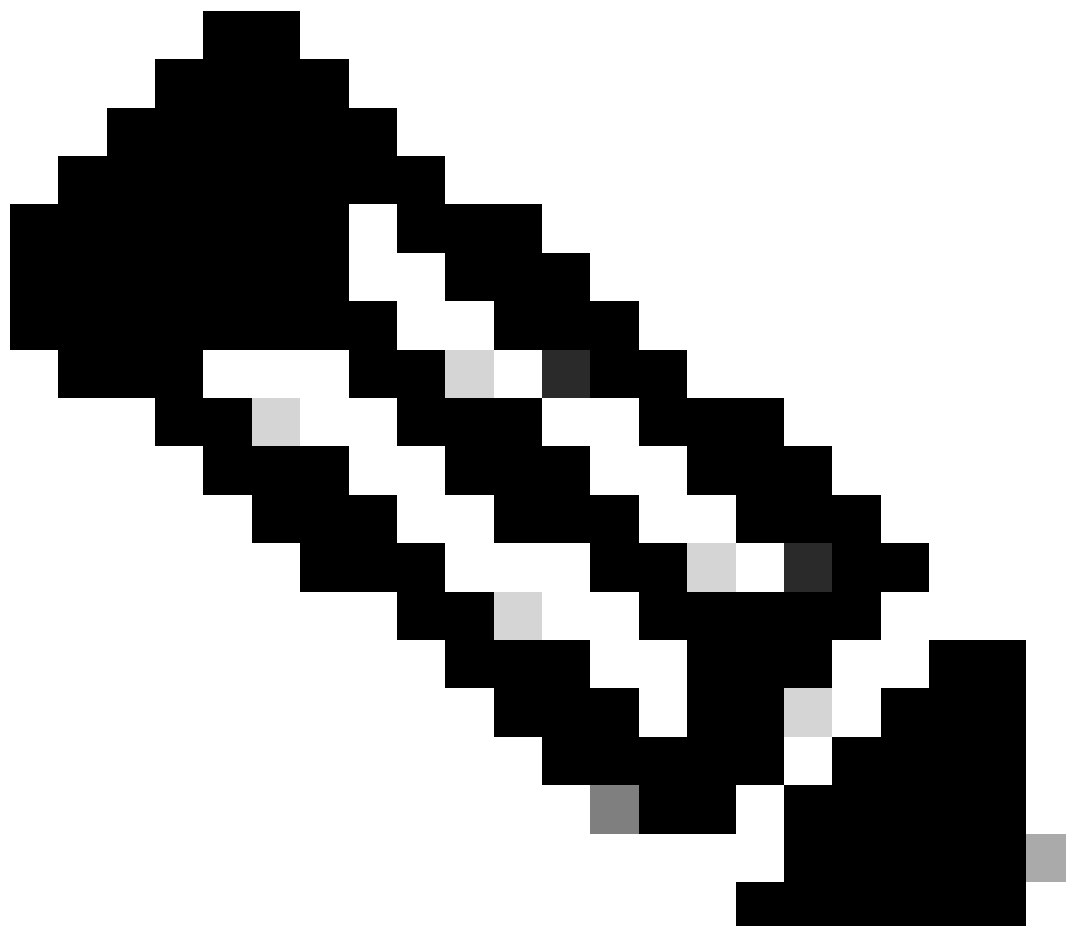
ملعتب رمتسملا رايتلا هجوم موقى Cisco نم SD-WAN ددعتمل ثبل ميمصتلا اقو
 (OMP) ةيشغتلا ةرادا لوكوتورب لال خ نم اهيلي ل PIM نيكمت مت يتلا ةيعرفلا تاهجوملا
 خسنلا ةمئاق ىلإ ةيعرفلا تاهجوملا هذبه صاخلا IP-ماظنلا لوكوتورب ةفاضإ متيو
 لثامملا.

```

DC-8500-01#sh SD-WAN omp multicast-auto-discover
Code:
C -> chosen
I -> installed
Red -> redistributed
Rej -> rejected
L -> looped
R -> resolved
S -> stale
Ext -> extranet
Stg -> staged
IA -> On-demand inactive
Inv -> invalid
BR-R -> border-router reoriginated
TGW-R -> transport-gateway reoriginated

```

ADDRESS FAMILY	TENANT	VPN	SOURCE ORIGINATOR	FROM PEER	STATUS
ipv4	0	10	169.1.100.3	0.0.0.0	C,Red,R
	0	10	169.1.100.4	2.2.2.1	Inv,U
				2.2.2.2	Inv,U
	0	10	169.101.100.1	2.2.2.1	C,R
				2.2.2.2	C,I,R
	0	10	169.101.100.2	2.2.2.1	C,R
				2.2.2.2	C,I,R



SD- ق فن لال خ نم عورفل تاهجوم الى DC هجوم نم AutoRP مزح لاسرا متيس :ةظحال م
AutoRP مزح نيمضتب (DC) رشابم الرايتال هجوم موقيس .(تانايبال ةحول) WAN BFD
عرفل تاهجوم الى هيجوت ةداعاو IPsec ق فن الى

- مت هنا الى ريشت اهناف ،DC هجوم MFIB في هيجوتال ةداعا تامال ع ةعومجم ىرت امदन ع
موقتسو ةيعرفل تاهجوملاب صاخال ماظنلل IPS ل لثامتمال خسنال ةمئاق عاشنإ
ةمئاق في .لثامتمال خسنال ةمئاق الى ادانتسا ددعتمال ثبال رورم ةكرح هيجوت ةداعاب
رمأل جرخم يلي اميفو .عورفل تاهجوم نم لكل تالخال ةيؤر كنكمي ،لثامتمال خسنال
ل:لثامتمال خسنال ةمئاقب صاخال

```
DC-8500-01#sh mvpn replication lsm-id 1
Repl ID : 1FFFFFF LSM ID : 1 Uptime : 1w3d
Path Set ID : 25
Replication branches: 2
IR (169.101.100.1)
Uptime : 1w3d Refcount : 2
Remote Label : 1006
IR (169.101.100.2)
```

Uptime : 1w3d Refcount : 2
Remote Label : 1004

- إذا لم يتم ققحت، لثامت الما خسننل عمئاق يف (IPS) ةشاشنل لخد ليدبتل ماطن دوجو درجمب ةرشابم الريغ ةيلغشنتل ةباحسنل ةئيپ هيچوت ةداعل ةلسلس/ةلسلس عاشننل مت طقف رشابم الريغ OCE رفوتي، يلاتل جارخلال يف ىرت امك. ددحمل عرفال هچومل (OCE) 01. يعرفال هچوملل

```
DC-8500-01#sh platform software SD-WAN f0 next-hop indirect all
Show SD-WAN next-hop oce all :
```

```
OCE ID: 0xf8000d9f, OCE Type: SD-WAN_NH_INDIRECT
Indirect: client_handle 0x5649f38aaa80, ppe addr 418b02c0
nhobj_type: SD-WAN_NH_LOCAL_SLA_CLASS, nhobj_handle: 0xf80805cf
label: 1006, dst_vpn: 10, nexthop sys_ip: 169.101.100.1, sla_class: 1
```

امدنع اهؤاشننل مت يتي لةيلخلادل هيچوتل ةداعل ةلسلس يه ةرشابم الريغ OCE ةلسلس ميمصتل اقفو اذه. صاخال عرفال هچوم نم يداحأل ثبل تاراسم رشابم الرايتل هچوم ملعتي هيچوت ةداعل يداحأل ثبل هيچوت ةدايزب ددعتمل ثبل موقيس ثيح، SD-WAN ددعتمل ثبل ددعتمل ثبل RP تامولعم.

02 عرفال هچوم ىللى AutoRP نييغت هيچوت ةداعل DC هچوم هيچوت ةداعل مدع عارو ببسنل لثمتي يعرفال هچوملل سيل نكلو، طقف 01 يعرفال هچوملل هؤاشننل مت رشابم الريغ OCE نأ يف موقيس، ةصلال يذ يعرفال هچوملل لةيلخلادل هيچوتل ةداعل ةلسلس عاشننل دنع طقف 02. اذه عرفال هچوم ىللى AutoRP نييغت هيچوت ةداعل DC هچوم.

- يف يداحأل ثبلل تاراسم ي (DC) لوصولال يف مكحتل ةدحو هچوم نمضتي مل هنأل ارظن ةداعل ةلسلس نإف، 02 يعرفال هچوملل نم اهملعت مت (RIB) هيچوتل تامولعم ةداعل 02. يعرفال هچوملل ىلع اهميمصت متي مل هيچوتل

```
DC-8500-01#sh ip route vrf 10 omp
```

Routing Table: 10

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 169.1.10.1 to network 0.0.0.0

```
m 169.101.0.0/16 [251/0] via 169.101.100.1, 2w0d, SD-WAN-system-intf
```

DC-8500-01#

- مت يذال راسم لال تي بـثـتـ مـتـي مـل OMP لوكوتـورب تاراسـمـل يـلـالـالـا جـارـخـإـلـا يـفـ يـرتـ اـمـك DC هـجـوم نـم RIB 10 هـجـوم يـلـع 02 يـعـرـفـال هـجـومـل نـم هـمـلـعـت

DC-8500-01#sh SD-WAN omp routes 169.101.0.0/16

Code:

C -> chosen

I -> installed

Red -> redistributed

Rej -> rejected

L -> looped

R -> resolved

S -> stale

Ext -> extranet

Inv -> invalid

Stg -> staged

IA -> On-demand inactive

U -> TLOC unresolved

BR-R -> border-router reoriginated

TGW-R -> transport-gateway reoriginated

TENANT	VPN	PREFIX	FROM PEER	PATH ID	LABEL	STATUS	ATTRIBUTE TYPE	TLOC IP
0	10	169.101.0.0/16	2.2.2.1	15	1004	R	installed	169.101.100.1
			2.2.2.1	19	1006	C,I,R	installed	169.101.100.1
			2.2.2.2	16	1004	R	installed	169.101.100.1
			2.2.2.2	21	1006	C,R	installed	169.101.100.1

DC-8500-01#

نأ وه RIB يـلـإ يـونـاـثـل هـجـومـل نـم اـهـمـلـعـت مـت يـتـل تاراسـمـل تـي بـثـت مـدـع عـارـو بـبـسـلـا حـتـف لوكوتـوربـل ةـيـلـلـع ةـفـلـكـت يـلـع يـوتـحـت يـونـاـثـل هـجـومـل نـم اـهـمـلـعـت مـت يـتـل تاراسـمـلـا يـسـيـئـرـل هـجـومـلـا بـ ةـنـراقـم (OSPF) الـأ راسـم رصـقـأ

<#root>

DC-8500-01#sh SD-WAN omp routes 169.101.0.0/16 detail

omp route entries for tenant-id 0 vpn 10 route 169.101.0.0/16

RECEIVED FROM:
peer 2.2.2.1
path-id 15
label 1004
status R
loss-reason origin-metric

lost-to-peer 2.2.2.1
lost-to-path-id 19

Attributes:

originator 169.101.100.2
type installed
tloc 169.101.100.2, public-internet, ipsec
ultimate-tloc not set
domain-id not set
overlay-id 1
site-id 10
preference not set
affinity-group None
region-id None
region-path not set
route-reoriginator not set
tag not set
origin-proto OSPF-external-1

origin-metric 35

as-path not set
community not set
unknown-attr-len not set

RECEIVED FROM:

peer 2.2.2.1
path-id 19
label 1006
status C,I,R
loss-reason not set
lost-to-peer not set
lost-to-path-id not set

Attributes:

originator 169.101.100.1
type installed
tloc 169.101.100.1, biz-internet, ipsec
ultimate-tloc not set
domain-id not set
overlay-id 1
site-id 10
preference not set
affinity-group None
region-id None
region-path not set
route-reoriginator not set
tag not set
origin-proto OSPF-external-1

origin-metric 30

as-path not set
community not set
unknown-attr-len not set

RECEIVED FROM:

peer 2.2.2.2
path-id 16
label 1004
status R
loss-reason origin-metric
lost-to-peer 2.2.2.2
lost-to-path-id 21

Attributes:

originator 169.101.100.2
type installed

```

tloc          169.101.100.2, public-internet, ipsec
ultimate-tloc not set
domain-id     not set
overlay-id    1
site-id       10
preference    not set
affinity-group None
region-id     None
region-path   not set
route-reoriginator not set
tag           not set
origin-proto  OSPF-external-1

origin-metric 35

as-path       not set
community     not set
unknown-attr-len not set
RECEIVED FROM:
peer          2.2.2.2
path-id       21
label         1006
status        C,R
loss-reason   not set
lost-to-peer  not set
lost-to-path-id not set
Attributes:
originator    169.101.100.1
type          installed
tloc          169.101.100.1, biz-internet, ipsec
ultimate-tloc not set
domain-id     not set
overlay-id    1
site-id       10
preference    not set
affinity-group None
region-id     None
region-path   not set
route-reoriginator not set
tag           not set
origin-proto  OSPF-external-1

origin-metric 30

as-path       not set
community     not set
unknown-attr-len not set
DC-8500-01#

```

- ىلع (OSPF) الؤا راسم رصقأ حتف لوكتورب تاراسم ىوس عيزوت متي مل هنا امك
OMP تانيوكت يلي امي ف. عورفال تاهجوم ىلع (OMP) الؤا راسم رصقأ حتف لوكتورب
يوناث يعرف هجوم نم:

<#root>

```

omp
no shutdown

```

```

overlay-as          65376
send-path-limit     16
ecmp-limit          16
graceful-restart
no as-dot-notation
timers
  holdtime           60
  advertisement-interval 1
  graceful-restart-timer 43200
  eor-timer           300
exit
address-family ipv4 vrf 10

```

advertise ospf external

```

<==
!
address-family ipv6
  advertise connected
  advertise static

```

ةنكمملا لولحل

1. OMP لالځ نم ةئدابلا نع نالعالاو 02 عرفلا هجوم ىلع عاجرتسا ةهجاو نيوكت كنكمي DC. هجوم ىلإ

```

Branch-C8300-02#sh run interface Lo0
Building configuration...

```

```

Current configuration : 151 bytes
!
interface Loopback0
  description Management loopback
  vrf forwarding 10
  ip address 169.101.100.2 255.255.255.255
  no ip redirects
  ip mtu 1500
end

```

ةلصتملا تاراسملا نع نالعالال 02 عرفلا هجوم ىلع OMP تانيوكت:

<#root>

```

omp
no shutdown
overlay-as          65376
send-path-limit     16
ecmp-limit          16
graceful-restart
no as-dot-notation
timers
  holdtime           60
  advertisement-interval 1

```

```
graceful-restart-timer 43200
eor-timer 300
exit
address-family ipv4 vrf 10

advertise ospf external
```

```
advertise connected
```

```
<==
!
address-family ipv6
advertise connected
advertise static
!
!
```

02: عرفال هجوم ىلع هم لعت مت يذال AutoRP طي طخت ةدهاشم كنكمي نآلا

```
Branch-C8300-02# sh ip pim vrf 10 rp mapping
PIM Group-to-RP Mappings
```

```
Group(s) 239.195.0.0/16
RP 10.125.125.1 (?), v2v1
Info source: 169.1.10.4 (terin.net.afrihost.co.za), elected via Auto-RP
Uptime: 00:02:18, expires: 00:02:47
Branch-C8300-02#
```

اضياي عرفال لوحم ىلع هم لعت مت يذال AutoRP طي طخت ةدهاشم كنكمي، لثملابو

```
Branch-9k#sh ip pim rp mapping
PIM Group-to-RP Mappings
```

```
Group(s) 239.195.0.0/16
RP 10.125.125.1 (?), v2v1
Info source: 169.254.100.9 (?), elected via Auto-RP
Uptime: 00:03:36, expires: 00:02:46
Acl: RP-Region-Ent-Sites, Static-Override
RP: 10.125.125.1 (?)
```

(DC)، رشابم الرايتال هجوم ىلع رشابم الرايغ OCE/هيجوت ةداعا ةلسلس جارخا صحف دنع
ةيوناثلاو ةيساسأل ةي عرفال تاهجومال نم لك ل IP ماطن ل تال اخدا ىلع يوتحت امناف

<#root>

```
DC-8500-01#sh platform software SD-WAN f0 next-hop indirect all
Show SD-WAN next-hop oce all :
```

```
OCE ID: 0xf80009bf, OCE Type: SD-WAN_NH_INDIRECT
Indirect: client_handle 0x5649f389fbc0, ppe addr 418b05c0
  nhobj_type: SD-WAN_NH_LOCAL_SLA_CLASS, nhobj_handle: 0xf808044f
  label: 1006, dst_vpn: 10,
```

```
  nexthop sys_ip: 169.101.100.1
```

```
, sla_class: 1
```

```
OCE ID: 0xf80009df, OCE Type: SD-WAN_NH_INDIRECT
Indirect: client_handle 0x5649f38a11f0, ppe addr 418b06d0
  nhobj_type: SD-WAN_NH_LOCAL_SLA_CLASS, nhobj_handle: 0xf808045f
  label: 1004, dst_vpn: 10,
```

```
  nexthop sys_ip: 169.101.100.2
```

```
, sla_class: 1
```

تبكړاضي 02 دي د خت چا حسم عرف نم تملع تائ داب ي ق ل تي RIB دي د خت چا حسم DC ى رت ن آل

<#root>

DC-8500-01#sh ip route vrf 10 omp

Routing Table: 10

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 169.1.10.1 to network 0.0.0.0

```
169.101.0.0/16 is variably subnetted, 3 subnets, 3 masks
m      169.101.0.0/16 [251/0] via 169.101.100.1, 13:59:47, SD-WAN-system-intf
m      169.101.10.0/28
        [251/0] via 169.101.100.2, 00:07:50,
```

SD-WAN-system-intf

```
m      169.101.100.2/32
        [251/0] via 169.101.100.2, 00:07:50,
```

SD-WAN-system-intf

2. نيو كټ ب مق (LAN) ةي لحم ل ؤكبش ل ل و ح م ب ؤل ص ت م ل ةي عرف ل ت ا ه ج و م ل ة ه ج ا و ي ل ع
م ا د خ ت س ا ب . ي و ن ا ث ل ه ج و م ل ن ا و ن ع ب ؤ ن ر ا ق م ي س ا س ا ل ا ي عرف ل ه ج و م ل ي ل ع ي ل ع ا IP ن ا و ن ع
ي ل ا ل ا ب و ، ا ص ص خ م ا د ر و م ن ي ع م ل ي عرف ل ه ج و م ل ح ب ص ي ف و س ، ا ذ ه ي س ا س ا ل ا عرف ل ه ج و م

يعرف ال هجوم ال نأ شح لوحم ال ال AutoRP تامولعم هيجوت ةداعإ ىلع ارداق نوكيس
AutoRP تامولعم ملعت دق يسيسئرل.

رارقلا

تاهجوم ال عيجم نأل ،كلذ نم دكأتل بجي ،Cisco SD-WAN ربع ددعتم ال ثبل ذيفنت ءانثأ
يداحأل ثبل ةئداب نالعب موقت (ةيوناثلاو ةيساسأل تاهجوم ال كلذ ي ف امب) ةديعب ال
ثبل هيجوت SD-WAN ددعتم ال ثبل لغتسي . OMP لالخ نم RP ال برقا SD-WAN هجوم
ثبل لكحتل ىوتسم تامولعم لاسرال ةبولطم ال هيجوتل ةداعإ ةلسلس ءانبل يداحأل
ددعتم ال.

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا