# طبقت BGP EVPN DHCP طبقة 2 ترحيل على مدة حفازة 9000 sery مفتاح

## المحتويات


المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

معلومات أساسية

تفاصيل المستند

سلوك ترحيل L2

المصطلح

التكوين (نشر CGW القياسي)

الرسم التخطيطي للشبكة

تفاصيل مفتاح L2 VTEP (الطرفي)

تفاصيل مفتاح VTEP (CGW) من L3

L2VTEP

CGW

التحقق من الصحة (نشر CGW القياسي)

حالة العارة (قرو)

FED MATM (قرو)

MAC المحلي (قرو)

تكوين DHCP للتطفل على بروتوكول (القرو و CGW)

التكوين (عزل جزئي مجمع)

الرسم التخطيطي للشبكة

تفاصيل مفتاح L2 VTEP (الطرفي)

تفاصيل مفتاح VTEP (CGW) من L3

CGW

التحقق من الصحة (عزل جزئي مجمع)

حالة العارة (قرو)

FED MATM (قرو)

MAC المحلي (قرو)

تكوين DHCP للتطفل على بروتوكول (القرو و CGW)

استكشاف الأخطاء وإصلاحها (أي عون CGW)

تصحيح أخطاء التطفل على بروتوكول DHCP (الطرفي)

تصحيح أخطاء التطفل على بروتوكول DHCP (CGW)

حزم التقاط

حالات عميل التطفل على بروتوكول DHCP

تصحيح الأخطاء الإضافية

معلومات ذات صلة

# المقدمة

يصف هذا المستند كيفية تكوين ميزة ترحيل EVPN VxLAN DHCP L2 والتحقق منها واستكشاف أخطائها وإصلاحها.

# المتطلبات الأساسية

## المتطلبات

- يتم إستخدام هذه الميزة في أي نشر من نوع CGW حيث يتم إستخدام DHCP
- في حالة تنفيذ التجزئة المحمية، يرجى مراجعة هذه المستندات
  - تنفيذ سياسة توجيه BGP EVPN على محولات Catalyst 9000 Series Switches
  - تنفيذ تجزئة تغشية BGP EVPN المحمية على محولات Catalyst 9000 Series Switches

## المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS® XE 17.12.1 والإصدارات الأحدث

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

# معلومات أساسية

## تفاصيل المستند

يمكن إستخدام هذا المستند لأي نشر ل CGW حيث يلزم نقل DHCP من ورقة بدون SVI نحو البوابة المركزية.

- إذا لم تكن تستخدم التجزئة المحمية، فاستخدم قسم المستند حيث يتم الإعلان عن SVI في البنية

إذا كنت تقوم بتنفيذ تجزئة محمية، فإن هذا المستند هو الجزء 2 من 3 مستندات مترابطة:

- يغطي المستند 1:تنفيذ سياسة توجيه BGP EVPN على محولات Catalyst 9000 Series Switches كيفية التحكم في حركة مرور BGP BUM في التغشية، ويجب تكوينها أولا
- المستند 2:تنفيذ تقسيم التغشية المحمية عبر بروتوكول BGP EVPN على محولات Catalyst 9000 Series Switches يعتمد على تصميم التغشية والسياسة الخاصة بالمستند 1، يصف تنفيذ الكلمة الأساسية 'protected'.

- الوثيقة 3: هذا المستند. ينبغي على أعلى الوثيقتين الأخيرتين وصف طريقة تنفيذ ترحيل DHCP باستخدام منشورات الطبقة 2 فقط و CGW

## سلوك ترحيل L2

| IPv4 | فيضان الوصول | فيضان البث | تطفل | مرحل |
|---|---|---|---|---|
| • الخيار الفرعي للخيار 82: (1) يتم تعميم معرف دائرة الوكيل (vni-mod-port) باستخدام التطفل على بروتوكول DHCP<br>• يمكن للمرء تحديد جانب الوصول باستخدام تكوين ثقة DHCP<br><br>* النموذج الموصى به | نعم | لا | نعم | نعم |
| • الخيار الفرعي للخيار 82: (1) يتم تعميم معرف دائرة الوكيل (vlan-mod-port) باستخدام التطفل على بروتوكول DHCP | نعم | نعم | لا | نعم |
| • الخيار الفرعي للخيار 82: (1) يتم تعميم معرف دائرة الوكيل (vni-mod-port) باستخدام التطفل على بروتوكول DHCP<br>• يمكن للمرء تحديد جانب الوصول باستخدام تكوين ثقة DHCP | نعم | لا | نعم | لا |
| IPv6 | فيضان الوصول | فيضان البث | تطفل | مرحل |
| • الخيار الفرعي للخيار 82: (1) يتم تعميم معرف دائرة الوكيل (vni-mod-port) باستخدام التطفل على بروتوكول DHCP<br>• يمكن للمرء تحديد جانب الوصول باستخدام تكوين ثقة DHCP | نعم | نعم | نعم | نعم |
| • الخيار الفرعي للخيار 82: (1) يتم تعميم معرف دائرة الوكيل (vlan-mod-port) باستخدام التطفل على بروتوكول DHCP | نعم | نعم | لا | نعم |
| • الخيار الفرعي للخيار 82: (1) يتم تعميم معرف دائرة الوكيل (vni-mod-port) باستخدام التطفل على | نعم | نعم | نعم | لا |

| | | | | |
|---|---|---|---|---|
| | | | | برووتوكول DHCP<br>• يمكن للمرء تحديد جانب الوصول باستخدام تكوين ثقة DHCP |
| ال | ال | نعم | نعم | |

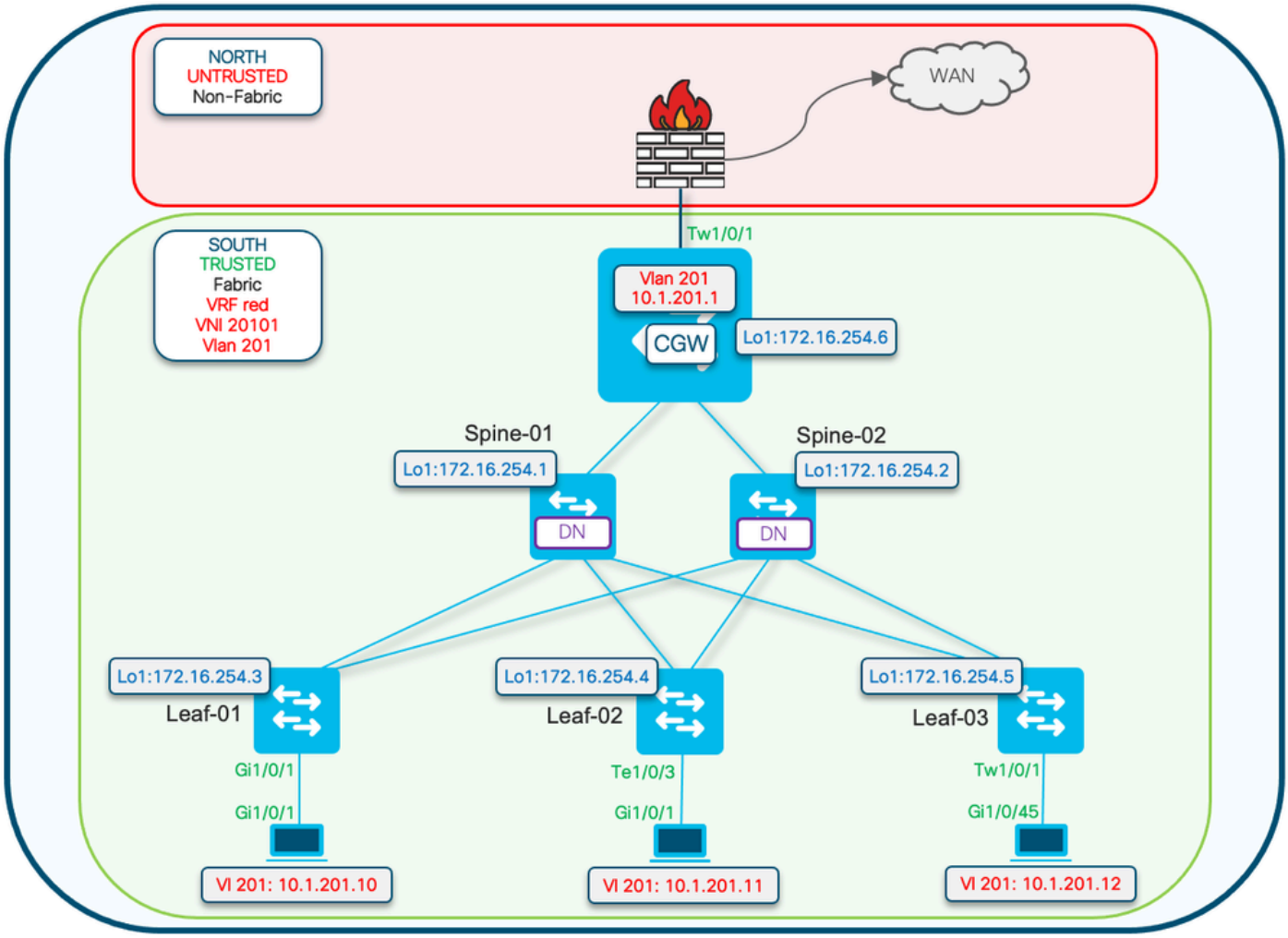
# المصطلح

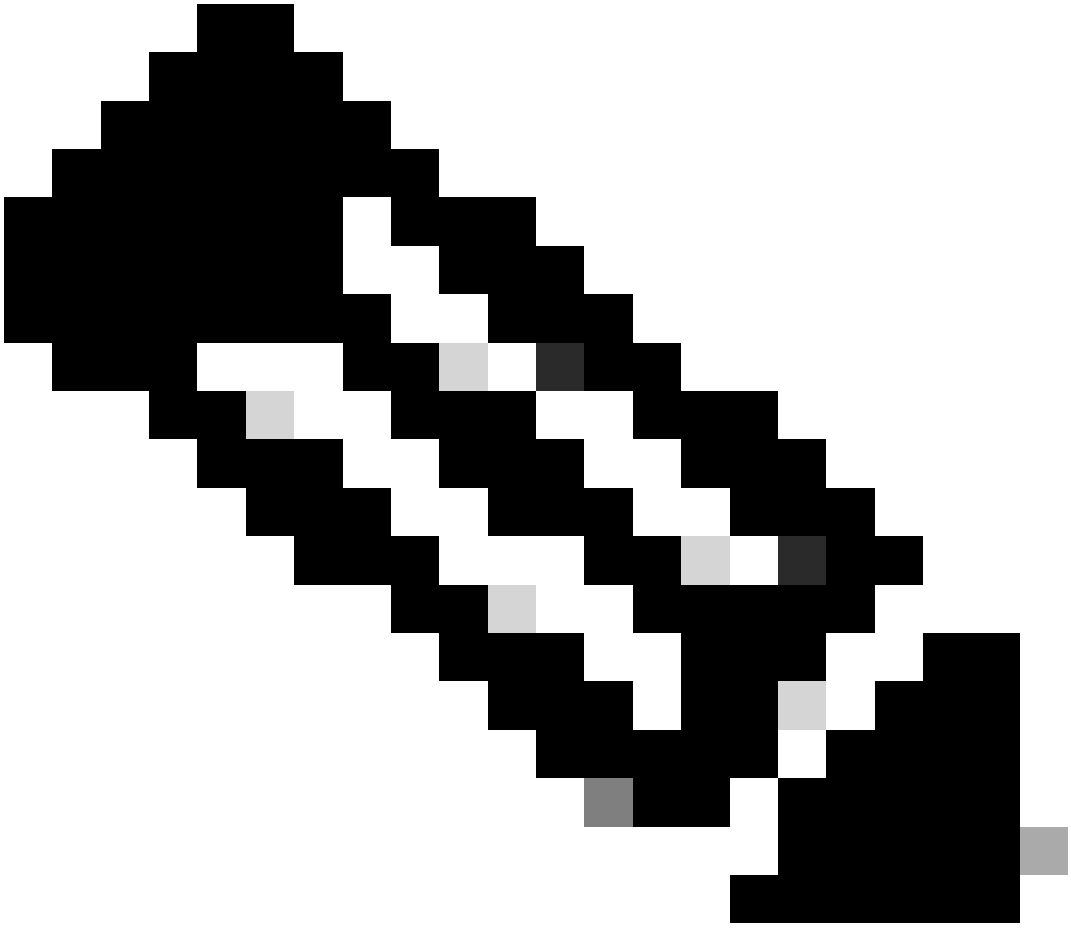
| | | |
|---|---|---|
| VRF | إعادة توجيه التوجيه الظاهري | تحديد مجال توجيه من الطبقة 3 يتم فصله عن مجال توجيه VRF آخر ومجال توجيه IPv4/IPv6 العام |
| أف | عائلة العناوين | يحدد أي نوع من البادئات ومعالج BGP لمعلومات التوجيه |
| ك | نظام ذاتي | مجموعة من بادئات IP الموجهة عبر الإنترنت التي تنتمي إلى شبكة أو مجموعة من الشبكات التي تتم إدارتها والتحكم فيها والإشراف عليها بواسطة كيان أو مؤسسة واحدة |
| EVPN | شبكة إيثرنت الخاصة الظاهرية | الملحق الذي يسمح BGP بنقل معلومات MAC من الطبقة 2 والطبقة 3 IP وهو EVPN ويستخدم برووتوكول العبارة الحدودية متعدد البروتوكولات (MP-BGP) كبروتوكول لتوزيع معلومات قابلية الوصول التي تتعلق بشبكة VXLAN المغاطة. |
| Vxlan | شبكة LAN الموسعة الظاهرية (شبكة المنطقة المحلية) | تم تصميم شبكة VXLAN للتغلب على القيود المتأصلة في برووتوكول الشجرة المتفرعة (STP). من المقترح إستخدام معيار IETF [RFC 7348] لتوفير خدمات شبكة إيثرنت من شبكات VLAN الموسعة الظاهرية المحلية (VLANs)، ولكن مع قدر أكبر من المرونة. ووظيفيا، وهو برووتوكول تضمين MAC في UDP الذي يعمل كتغشية افتراضية على شبكة أساسية من الطبقة 3. |
| CGW | بوابة مركزية | وتنفيذ EVPN حيث البوابة SVI ليست على كل ورقة. وبدلا من ذلك، يتم تنفيذ جميع التوجيه بواسطة ورقة معينة باستخدام IRB غير المتماثل (التوجيه والجسر المدمجين) |
| ديفيغ | البوابة الافتراضية | تمت إضافة سمة مجتمع BGP الموسعة إلى بادئة MAC/IP عبر الأمر "default-gateway advertising enable" ضمن قسم التكوين 'l2vpn evpn'. |

| | | |
|---|---|---|
| IMET (RT3) | علامة إيثرنت للبث المتعدد شاملة (المسار) | يسمى أيضا مسار BGP النوع 3. يتم إستخدام نوع المسار هذا في EVPN لتقديم حركة مرور BUM (البث / مجهول unicast / multicast) بين VTEPs. |
| الطراز RT2 | نوع المسار 2 | بادئة BGP MAC أو MAC/IP التي تمثل MAC المضيف أو البوابة MAC-IP |
| EVPN Mgr | مدير EVPN | عنصر الإدارة المركزية لمختلف المكونات الأخرى (مثال: التعلم من نظام المعلومات المستقل والإشارات إلى قاعدة معلومات الإدارة (RIB)) |
| SIF | ميزة الأمان المتكاملة للمحول | جدول تتبع المضيف اللاأدرية الذي يستخدمه EVPN للتعرف على المضيفين المحليين الموجودين على وقة ما |
| L2RIB | قاعدة معلومات التوجيه من المستوى الثاني | في المكون الوسيط لإدارة التفاعلات بين BGP، EVPN Mgr، L2FIB |
| أطعمتما | محرك إعادة التوجيه | برامج طبقة ASIC (الأجهزة) |
| مطم | مدير جدول عناوين MAC | IOS MATM: جدول البرامج الذي يقوم بتثبيت العناوين المحلية و طقف<br>FED MATM: جدول الأجهزة الذي يقوم بتثبيت العناوين المحلية والبعيدة التي تم التعرف عليها من مستوى التحكم، وهو جزء من مستوى إعادة توجيه الأجهزة |

# التكوين (نشر CGW القياسي)

الرسم التخطيطي للشبكة


NORTH
UNTRUSTED
Non-Fabric
WAN
SOUTH
TRUSTED
Fabric
VRF red
VNI 20101
Vlan 201
Tw1/0/1
Vlan 201
10.1.201.1
CGW
Lo1:172.16.254.6
Spine-01
Lo1:172.16.254.1
DN
Spine-02
Lo1:172.16.254.2
DN
Lo1:172.16.254.3
Leaf-01
Gi1/0/1
Gi1/0/1
Vl 201: 10.1.201.10
Lo1:172.16.254.4
Leaf-02
Te1/0/3
Gi1/0/1
Vl 201: 10.1.201.11
Lo1:172.16.254.5
Leaf-03
Tw1/0/1
Gi1/0/45
Vl 201: 10.1.201.12



ملاحظة: يغطي هذا القسم عملية نشر CGW قياسية دون إستخدام الميزة المحمية.

- يتم عرض تصحيح الأخطاء التي تظهر تبادل حزم DHCP DORA فقط في مثال المقطع المحمي

## تفاصيل مفتاح L2 VTEP (الطرفي)

تأتي حزمة الطلب من العميل

- أستخدم GW الافتراضي MAC المعلن عنه من CGW.
- إذا كان هناك أكثر من GW سيتم إستخدام أول GW mac.
- تحويل MAC للبث الخارجي (بدء العميل: D و R في DORA) إلى GW MAC أحادي البث وإعادة التوجيه إلى CGW

يضيف التطفل على بروتوكول DHCP: الخيار 82 suboptions: circuit and RID

(يتم إستخدام RID بواسطة معالجة PKT للاستجابة على CGW)

(يقوم بإعلام CGW بأنه ليس محليا ولترحيل البنية مرة أخرى إلى L2VTEP)

<#root>

```
Option: (82) Agent Information Option
        Length: 24
        Option 82 Suboption: (1) Agent Circuit ID
            Length: 12
            Agent Circuit ID: 010a00080000277501010000

        Option 82 Suboption: (2) Agent Remote ID

            Length: 8
          Agent Remote ID:
          000

682c7bf88700 <-- switch base mac 682c.7bf8.8700 (from 'show switch')
```

- تم تلقي PKTS إستجابة من CGW عبر نفق vxlan.
- خيار شرائط الورقة 82.
- إضافة إدخالات ربط باستخدام واجهة مصدر العميل. (vxlan-mod-port يعطي العميل مصدر قارن).
- تم إعادة توجيه حزمة الاستجابة إلى العميل.

## تفاصيل مفتاح VTEP (CGW) من L3

- تمكين التطفل على بروتوكول DHCP
- تمكين ترحيل DHCP في SVI
- تم تلقي الطلب من L2VTEP، وتم إعطاؤه للترحيل
- يضيف الترحيل خيارات فرعية أخرى للخيار 82 (gi، تجاوز الخادم، وهكذا) ويرسل إلى خادم DHCP.
- تأتي إستجابة DHCP من خادم DHCP أولا إلى مكون الترحيل.
- بعد أن يجرد ترحيل معلومات الخيار 82 (عنوان gi، تجاوز الخادم، وهكذا) يتم تمرير الحزمة إلى مكون التطفل على بروتوكول DHCP.
- يتحقق مكون التطفل من RID (معرف الموجه) وإذا لم يكن محليا الى يزيل الخيار 82 subopton 1 و 2.

- تتم إعادة توجيه حزمة ترحيل البنية (نظرا لأن RID ليس محليا) مباشرة إلى العميل البعيد.
- يستخدم Mac العميل ويدخل الجسر. يقوم الجهاز بالبحث عن عناوين التحكم في الوصول للوسائط الخاصة بالعميل وإعادة توجيه الحزمة ذات تضمين الشبكة المحلية الظاهرية (VXLAN) إلى L2VTEP الأصلي.

## L2VTEP

تكوين مثيل EVPN

```
<#root>

Leaf-01#

show run | beg l2vpn evpn instance 201


l2vpn evpn instance 201 vlan-based
 encapsulation vxlan
 replication-type ingress
```

تمكين التطفل على بروتوكول DHCP

```
<#root>

Leaf-01#

show run | sec dhcp snoop


ip dhcp snooping vlan 101,

201


ip dhcp snooping
```

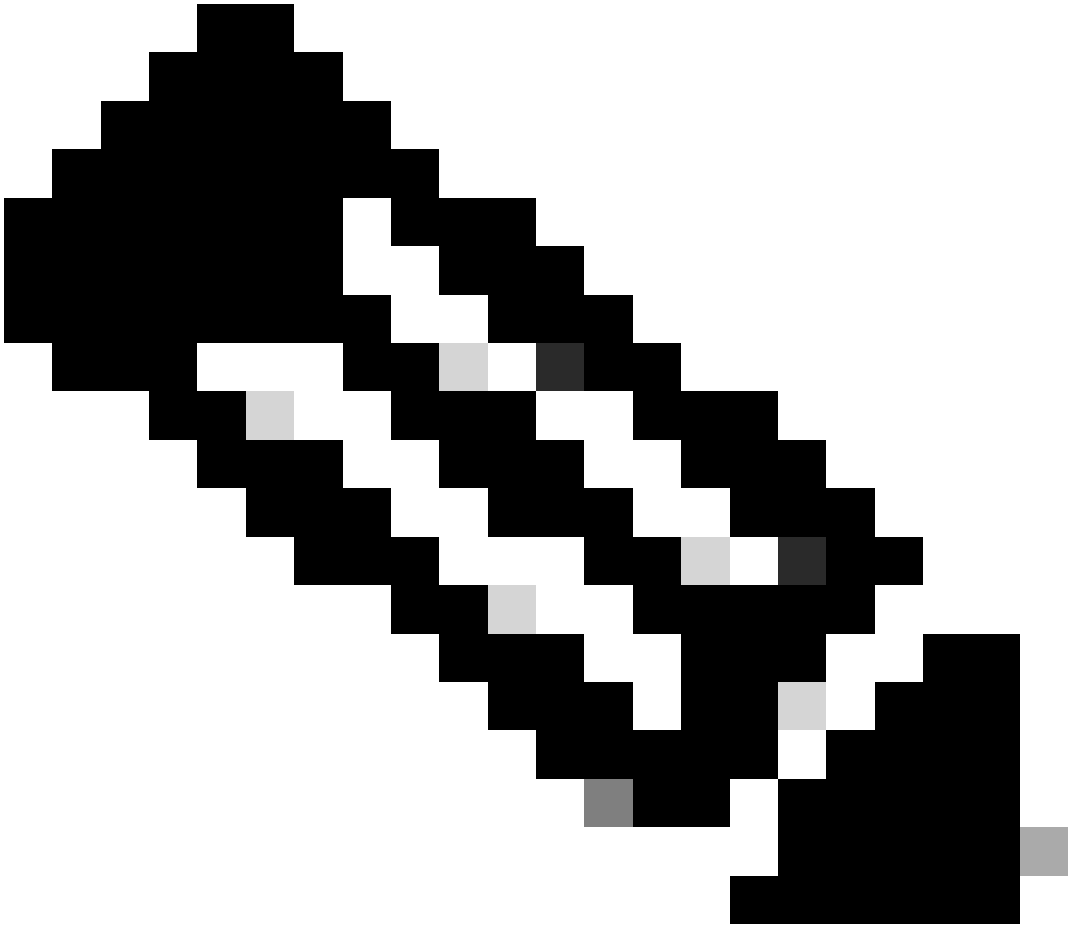
## CGW

تكوين مثيل EVPN

```
<#root>

Border#

sh run | s l2vpn evpn instance 201
```

```
l2vpn evpn instance 201 vlan-based
 encapsulation vxlan
 replication-type ingress

default-gateway advertise enable  <-- Enable to add BGP DEF GW ext. community attribute
```

---



ملاحظة: تعد السمة DEF GW أمرا بالغ الأهمية لترحيل L2 لمعرفة من الذي يجب تغليف حزمة DHCP وإرسالها إلى.

---

تمكين التطفل على بروتوكول DHCP

<#root>

```
Border#

sh run | s dhcp snoop
```

```
ip dhcp snooping vlan 101,
201

ip dhcp snooping
```

تأكد من أن ترحيل DHCP يحتوي على التكوين الصحيح لمعالجة الخيارات الإضافية

```
<#root>

Border#
sh run int vl 201

Building configuration...

interface Vlan201
 mac-address 0000.beef.cafe
 vrf forwarding red
 ip dhcp relay information option vpn-id  <-- Ensure the vrf info is passed to the server


ip dhcp relay source-interface Loopback0 <-- Sets the relay source interface to the loopback

 ip address 10.1.201.1 255.255.255.0

ip helper-address global 10.1.33.33      <-- In this scenario the DHCP server is in the global routing t
```

# التحقق من الصحة (نشر CGW القياسي)

## بادئة العبارة (ورقة)

```
<#root>

Leaf-01#
sh bgp l2vpn evpn route-type 2 0 0000.beef.cafe 10.1.201.1

BGP routing table entry for [2][172.16.255.3:201][0][48][0000BEEFCAFE][32][10.1.201.1]/24, version 8964
Paths: (1 available, best #1,
table evi_201
)
<-- In the EVI context for the segment
```

```
Not advertised to any peer
Refresh Epoch 3
Local, imported path from [2][172.16.255.6:201][0][48][0000BEEFCAFE][32][10.1.201.1]/24 (global)
  172.16.255.6 (metric 30) (via default) from 172.16.255.1 (172.16.255.1)
    Origin incomplete, metric 0, localpref 100, valid, internal, best
    EVPN ESI: 00000000000000000000,
```

**Label1 20101 <-- Correct segment ID**

```
    Extended Community: RT:65001:201 ENCAP:8
```

**EVPN DEF GW:0:0 <-- GW attribute added indicating this is GW prefix which L2 Relay uses**

**Originator: 172.16.255.6**

```
, Cluster list: 172.16.255.1
```

**<-- Learned from the Border (CGW)**

```
    rx pathid: 0, tx pathid: 0x0
    Updated on Nov 14 2023 16:06:40 UTC
```

## FED MATM (ةقرو)

### <#root>

```
Leaf-01#
```

**show platform software fed switch active matm macTable vlan 201**

```
VLAN   MAC                 Type  Seq#    EC_Bi  Flags  machandle          siHandle           riHandl
-------------------------------------------------------------------------------------------------
201    0006.f601.cd42       0x1   32436      0      0  0x71e058dc3368      0x71e058655018      0x0

201    0006.f601.cd01       0x1   32437      0      0  0x71e058dae308      0x71e058655018      0x0
```

**201 0000.beef.cafe 0x5000001**

```
       0      0     64  0x71e059177138      0x71e058eeb418      0x71e058df81f8      0x0
```

**VTEP 172.16.255.6 adj_id 1371**

**No**

**<--- The GW MAC shows learnt via the Border Leaf Loopback with the right flags**

```
Total Mac number of addresses:: 3
Summary:
```

```
Total number of secure addresses:: 0
Total number of drop addresses:: 0
Total number of lisp local addresses:: 0

Total number of lisp remote addresses:: 1          <---


*a_time=aging_time(secs)  *e_time=total_elapsed_time(secs)
Type:

MAT_DYNAMIC_ADDR           0x1

  MAT_STATIC_ADDR            0x2  MAT_CPU_ADDR               0x4  MAT_DISCARD_ADDR           0x8
MAT_ALL_VLANS              0x10  MAT_NO_FORWARD            0x20  MAT_IPMULT_ADDR           0x40  MAT_RES
MAT_DO_NOT_AGE            0x100  MAT_SECURE_ADDR          0x200  MAT_NO_PORT              0x400  MAT_DRO
MAT_DUP_ADDR             0x1000  MAT_NULL_DESTINATION    0x2000  MAT_DOT1X_ADDR          0x4000  MAT_ROU
MAT_WIRELESS_ADDR       0x10000  MAT_SECURE_CFG_ADDR    0x20000  MAT_OPQ_DATA_PRESENT   0x40000  MAT_WIR
MAT_DLR_ADDR           0x100000  MAT_MRP_ADDR          0x200000  MAT_MSRP_ADDR         0x400000  MAT_LIS

MAT_LISP_REMOTE_ADDR 0x1000000

  MAT_VPLS_ADDR        0x2000000

MAT_LISP_GW_ADDR     0x4000000                                  <-- these 3 values added = 0x5000001 (not
```

## MAC المحلي (ورقة)

```
<#root>

Leaf-01#

show switch


Switch/Stack Mac Address : 682c.7bf8.8700 - Local Mac Address
Mac persistency wait time: Indefinite
                                             H/W   Current
Switch#   Role    Mac Address     Priority Version  State
-----------------------------------------------------------------------------------
*1       Active

682c.7bf8.8700

     1      V01     Ready

<--- Use to validate the Agent ID in DHCP Option 82
```

## التطفل على بروتوكول DHCP (الورقة و CGW)

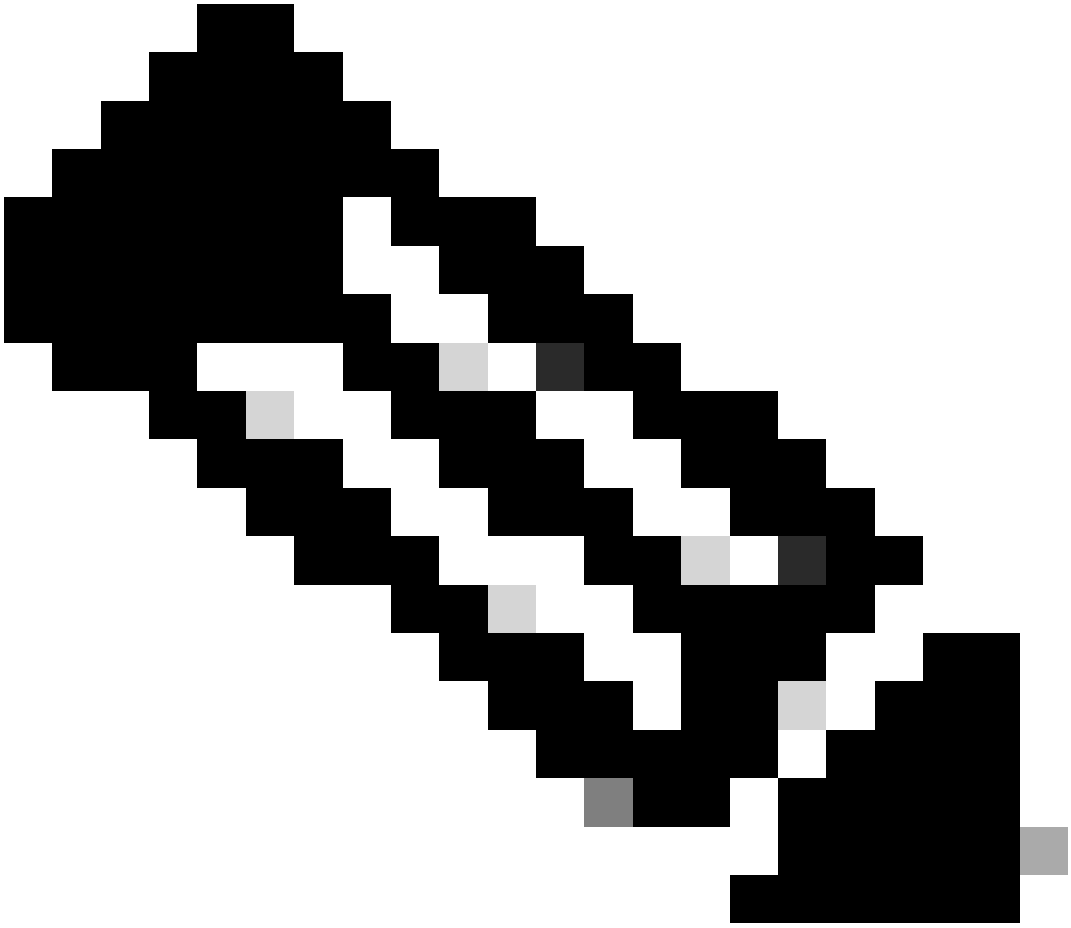
```
<#root>

Leaf-01#

show ip dhcp snooping
```

```
Switch DHCP snooping is enabled


Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
101,201

DHCP snooping is operational on following VLANs:


101,201



Insertion of option 82 is enabled
circuit-id default format: vlan-mod-port
remote-id: 682c.7bf8.8700 (MAC)          <--- Leaf-01 adds the switch MAC to Option 82 to indicate to CG



CGW#

show ip dhcp snooping


Switch DHCP snooping is enabled


Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
101,201

DHCP snooping is operational on following VLANs:


101,201
```

# التكوين (عزل جزئي محمي)

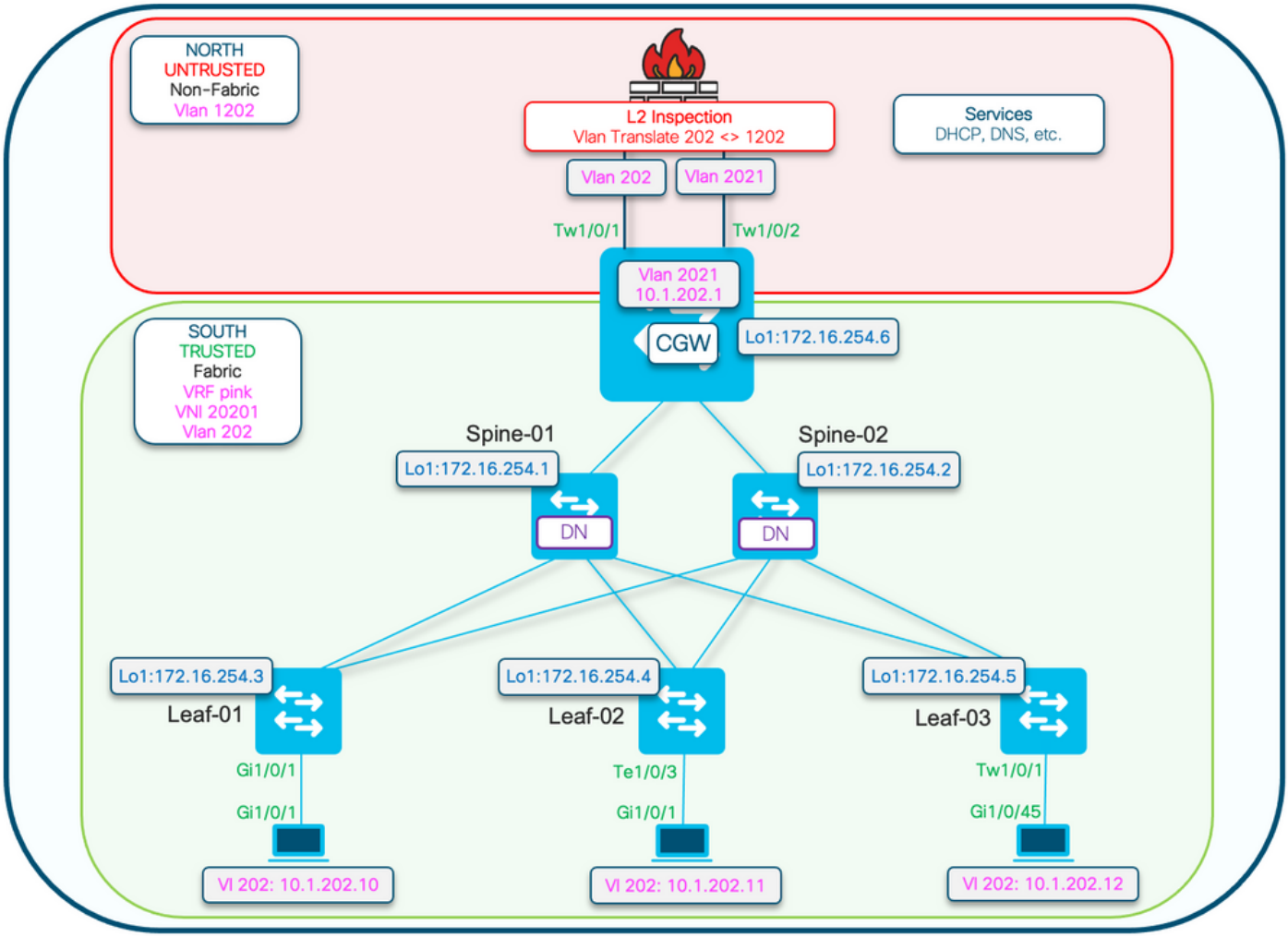
يعتمد التطفل على بروتوكول DHCP على مسار العبارة الافتراضية من CGW لتعلم البوابة MAC لإعادة توجيه حزم DHCP إلى.

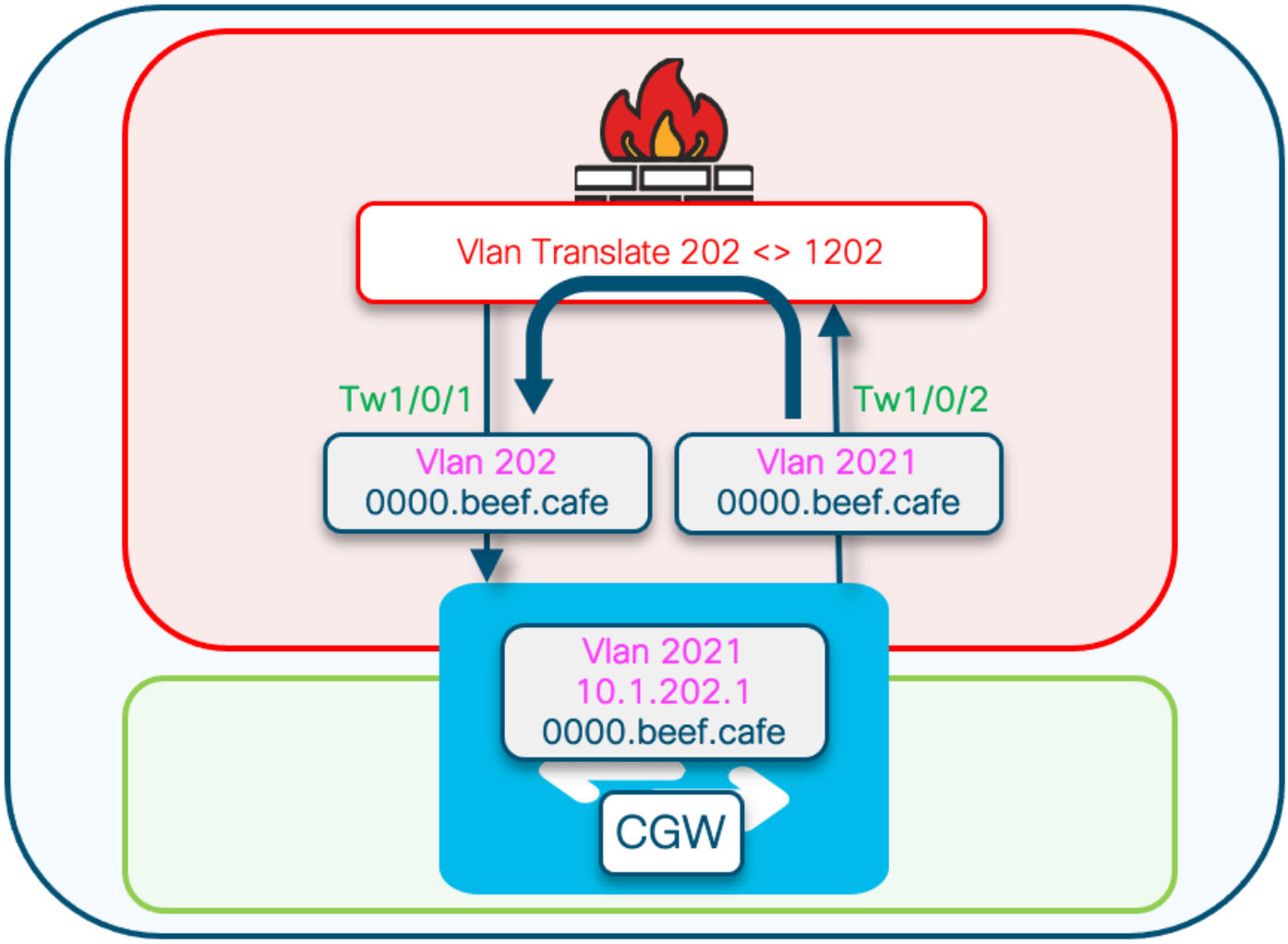
- عند إستخدام التصميم المعزول جزئيا مع البوابة الخارجية، يلزم وجود تكوينات إضافية على CGW للإعلان عن MAC-IP RT2 باستخدام سمة البوابة الافتراضية (DEF GW).



ملاحظة: يعمل هذا القسم أيضا على وصف تنفيذ مقطع محمي معزول تماما، يستخدم أيضا GW معلن عنه في البنية (مقابل GW خارج البنية).

## الرسم التخطيطي للشبكة


NORTH
UNTRUSTED
Non-Fabric
Vlan 1202
L2 Inspection
Vlan Translate 202 <> 1202
Services
DHCP, DNS, etc.
Vlan 202
Vlan 2021
Tw1/0/1
Tw1/0/2
Vlan 2021
10.1.202.1
CGW
Lo1:172.16.254.6
SOUTH
TRUSTED
Fabric
VRF pink
VNI 20201
Vlan 202
Spine-01
Lo1:172.16.254.1
DN
Spine-02
Lo1:172.16.254.2
DN
Lo1:172.16.254.3
Leaf-01
Lo1:172.16.254.4
Leaf-02
Lo1:172.16.254.5
Leaf-03
Gi1/0/1
Gi1/0/1
Te1/0/3
Gi1/0/1
Tw1/0/1
Gi1/0/45
Vl 202: 10.1.202.10
Vl 202: 10.1.202.11
Vl 202: 10.1.202.12




## تفاصيل مفتاح L2 VTEP (الطرفي)

تأتي حزمة الطلب من العميل

- أستخدم GW الافتراضي MAC المعلن عنه من CGW.
- إذا كان هناك أكثر من GW سيتم إستخدام أول GW mac.
- تحويل MAC للبث الخارجي (بدء العميل: D و R في DORA) إلى GW MAC أحادي البث وإعادة التوجيه إلى CGW

يضيف التطفل على بروتوكول DHCP: الخيار 82 suboptions: circuit and RID

(يتم إستخدام RID بواسطة معالجة PKT للاستجابة على CGW)

(يقوم بإعلام CGW بأنه ليس محليا ولترحيل البنية مرة أخرى إلى L2VTEP)

<#root>

```
Option: (82) Agent Information Option
        Length: 24
        Option 82 Suboption: (1) Agent Circuit ID
            Length: 12
            Agent Circuit ID: 010a00080000277501010000

        Option 82 Suboption: (2) Agent Remote ID

            Length: 8
          Agent Remote ID:
          000

682c7bf88700 <-- switch base mac 682c.7bf8.8700 (from 'show switch')
```

- تم تلقي PKTS إستجابة من CGW عبر نفق vxlan.
- خيار شرائط الورقة 82.
- إضافة إدخالات ربط باستخدام واجهة مصدر العميل. (vxlan-mod-port يعطي العميل مصدر قارن).
- تم إعادة توجيه حزمة الاستجابة إلى العميل.

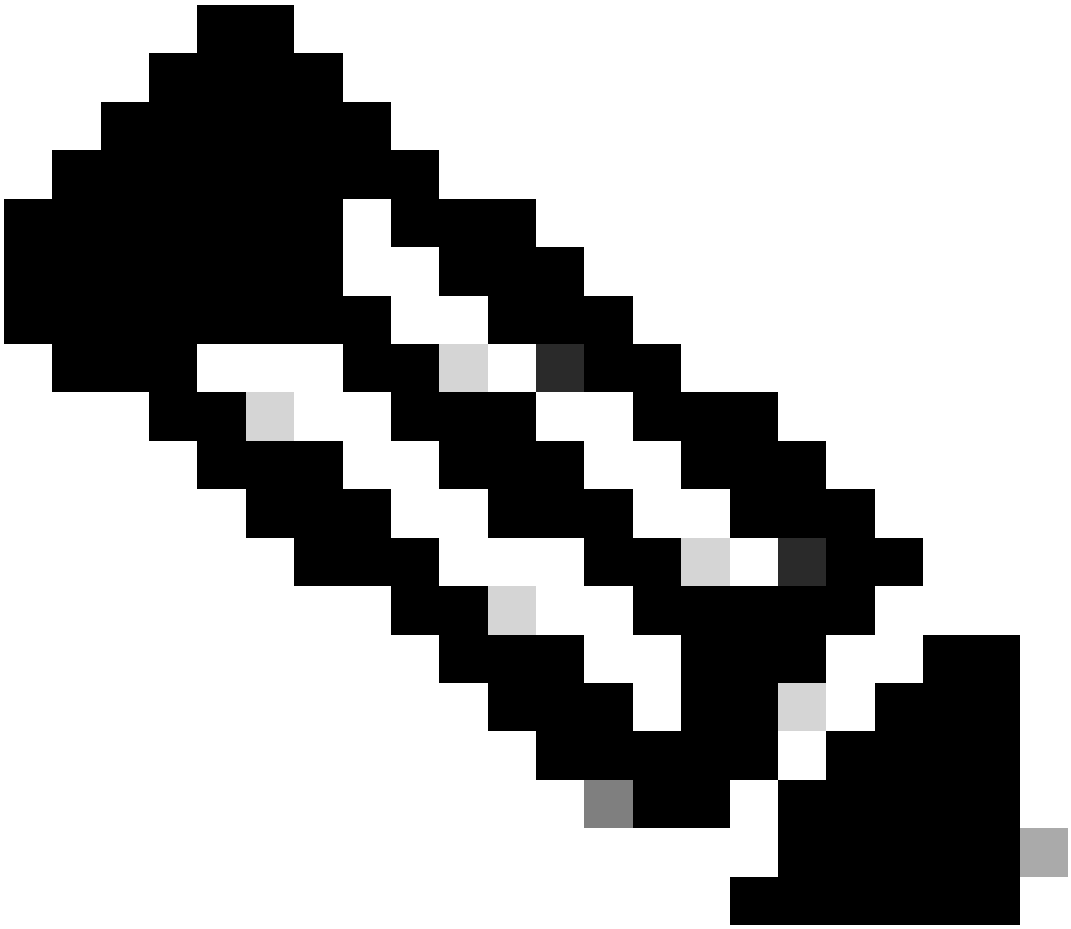
## تفاصيل مفتاح VTEP (CGW) من L3

- تمكين التطفل على بروتوكول DHCP
- تمكين ترحيل DHCP في SVI
- تم تلقي الطلب من L2VTEP، وتم إعطاؤه للترحيل
- يضيف الترحيل خيارات فرعية أخرى للخيار 82 (gi، تجاوز الخادم، وهكذا) ويرسل إلى خادم DHCP.
- تأتي إستجابة DHCP من خادم DHCP أولا إلى مكون الترحيل.
- بعد أن يجرد ترحيل معلومات الخيار 82 (عنوان gi، تجاوز الخادم، وهكذا) يتم تمرير الحزمة إلى مكون التطفل على بروتوكول DHCP.
- يتحقق مكون التطفل من RID (معرف الموجه) وإذا لم يكن محليا الى يزيل الخيار 82 subopton 1 و 2.
- تتم إعادة توجيه حزمة ترحيل البنية (نظرا لأن RID ليس محليا) مباشرة إلى العميل البعيد.
- يستخدم Mac العميل ويدخل الجسر. يقوم الجهاز بالبحث عن عناوين التحكم في الوصول للوسائط الخاصة بالعميل وإعادة توجيه الحزمة ذات تضمين الشبكة المحلية الظاهرية (VXLAN) إلى L2VTEP الأصلي.

الخطوات المطلوبة لدعم ترحيل DHCP L2:

1. تمكين التعلم المحلي لـ IP
2. إنشاء سياسة باستخدام تجميع معطل
3. إرفاق إلى عبارة خارجية VLANs/VLANs
4. إضافة إدخالات ثابتة في جدول تعقب الأجهزة للعبارة الخارجية mac-ip
5. قم بإنشاء خريطة مسار BGP لمطابقة بادئات RT2 MAC-IP وتعيين مجتمع البوابة الافتراضي الموسع
6. تطبيق خريطة المسار على جيران عاكس مسار BGP
7. تأكد من أن ترحيل DHCP يحتوي على التكوين الصحيح لمعالجة الخيار الإضافي
8. شكلت DHCP يتطفل على بناء VLAN والـ خارجي GW VLAN

---



ملاحظة: لا يلزم إجراء أي تغييرات في التكوين على أوراق الوصول لدعم ترحيل DHCP L2 باستخدام البوابة الخارجية.

---

## CGW

### تمكين التعلم المحلي ل IP

```
<#root>

CGW#

show running-config | beg l2vpn evpn instance 202

l2vpn evpn instance 202 vlan-based
 encapsulation vxlan
 replication-type ingress

 ip local-learning enable


<-- to advertise RT-2 with default gateway EC, ip local-learning must be enabled on the CGW.


    Use additional device-tracking policy shown in the next output to prevent MAC-IP binding flapping wh

 multicast advertise enable

<--- There is no default-gateway advertise enable cli here, as the SVI (Vlan 2021) used by this segment
```

### إنشاء سياسة باستخدام تجميع معطل

```
<#root>

device-tracking policy dt-no-glean <-- Configure device tracking policy to prevent MAC-IP flapping

 security-level glean
 no protocol ndp
 no protocol dhcp6
 no protocol arp
 no protocol dhcp4
```

### إرفاق إلى إيفي العبارة الخارجية/شبكات VLAN

```
<#root>

CGW#

show running-config | sec vlan config

vlan configuration 202
 member evpn-instance 202 vni 20201

 device-tracking attach-policy dt-no-glean <-- apply the new device tracking policy to the vlan configur
```

إضافة إدخالات ثابتة في جدول تعقب الأجهزة للعبارة الخارجية mac-ip

<#root>

```
device-tracking binding vlan 202 10.1.202.1 interface TwentyFiveGigE1/0/1 0000.beef.cafe
```

**<-- All static entries in device tracking table should be for external gateway mac-ip's.**

**If there is any other static entry in device tracking table, match ip/ipv6 configurations in route m**

قم بإنشاء خريطة مسار BGP لمطابقة بادئات RT2 MAC-IP وتعيين مجتمع البوابة الافتراضي الموسع

<#root>

```
route-map CGW_DEF_GW permit 10
```

**match evpn route-type 2-mac-ip <-- match RT2 type MAC-IP**

**set extcommunity default-gw <-- Set Default-gateway (DEF GW 0:0) extended community**

```
route-map CGW_DEF_GW permit 20
```

تطبيق خريطة المسار على جيران عاكس مسار BGP

<#root>

```
CGW#
```

**sh run | sec router bgp**

```
address-family l2vpn evpn
 neighbor 172.16.255.1 activate
 neighbor 172.16.255.1 send-community both
 neighbor 172.16.255.1
```

**route-map CGW_DEF_GW out <-- Sets the DEF GW Community when it advertises MAC-IP type RT2 to the RR**

```
 neighbor 172.16.255.2 activate
 neighbor 172.16.255.2 send-community both
 neighbor 172.16.255.2
```

**route-map CGW_DEF_GW out <-- Sets the DEF GW Community when it advertises MAC-IP type RT2 to the RR**

تأكد من أن ترحيل DHCP يحتوي على التكوين الصحيح لمعالجة الخيارات الإضافية

```
<#root>

CGW#

show run int vl 2021

Building configuration...

Current configuration : 315 bytes
!
interface Vlan2021
 mac-address 0000.beef.cafe
 vrf forwarding pink

 ip dhcp relay information option vpn-id   <-- Ensure the vrf info is passed to the server
 ip dhcp relay source-interface Loopback0  <-- sets the relay source interface to the loopback

 ip address 10.1.202.1 255.255.255.0

 ip helper-address global 10.1.33.33       <-- In this scenario the next hop to the DHCP server is in th

 no ip redirects
 ip local-proxy-arp
 ip route-cache same-interface
 no autostate
```

تأكد من أن DHCP يتطفل على بانء VLANs والخارجي GW VLAN

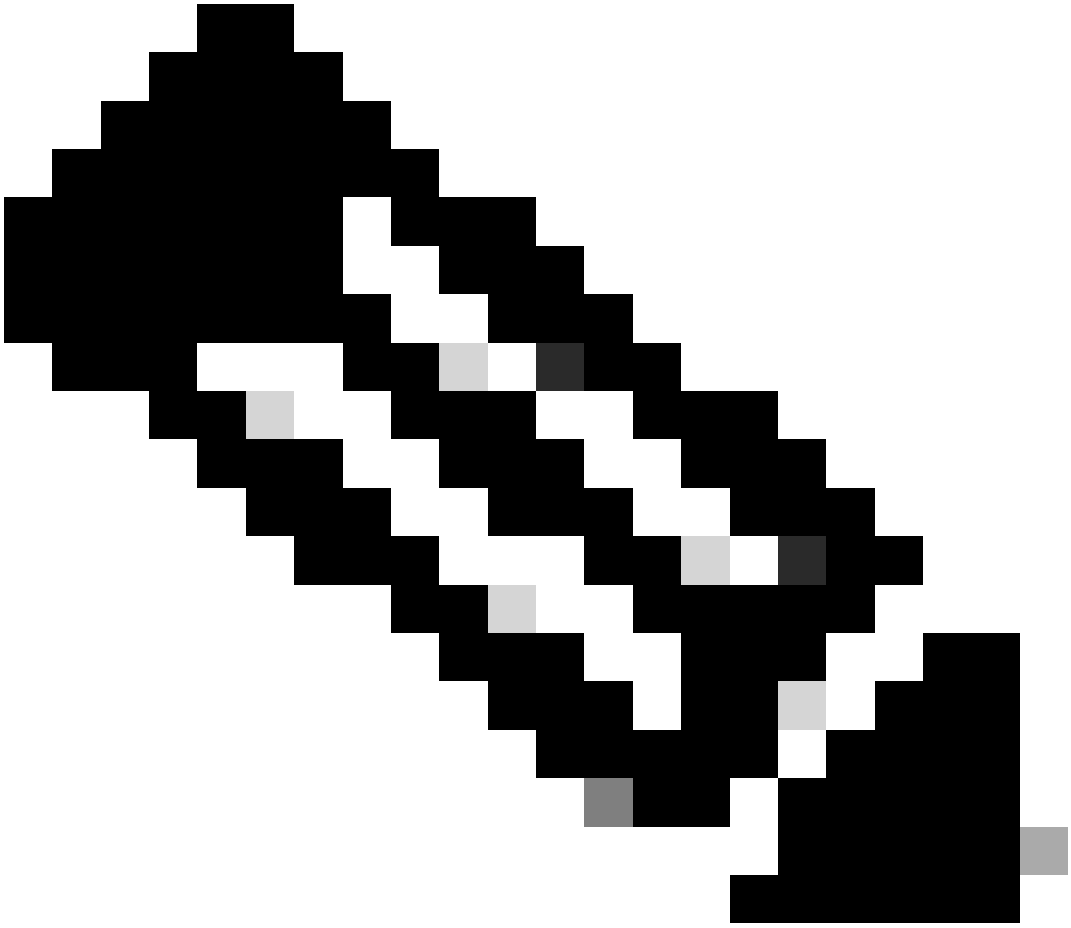
```
<#root>

Leaf01#

sh run | s dhcp snoop

ip dhcp snooping vlan 202
ip dhcp snooping

CGW#

sh run | s dhcp snoop

ip dhcp snooping vlan 202,2021  <-- snooping is required in both the fabric vlan and the external GW vla

ip dhcp snooping
```

تأكد من أن التوصيل إلى خادم DHCP موثوق به على CGW

```
<#root>

CGW#

sh run int tw 1/0/1
```

```
interface TwentyFiveGigE1/0/1
 switchport trunk allowed vlan 202
 switchport mode trunk

 ip dhcp snooping trust

end

CGW#

sh run int tw 1/0/2


interface TwentyFiveGigE1/0/2
 switchport trunk allowed vlan 33,2021
 switchport mode trunk

 ip dhcp snooping trust

end
```

---



ملاحظة: نظرا للطريقة التي يتم بها وضع الخادم على ثقة جهاز جدار الحماية تم

---

تكوينها على كل الربطين اللذين يواجهان هذا الجهاز. في الرسم التخطيطي الذي تم تكبيره، يمكنك أن ترى أن العرض يصل إلى كل من tw1/0/1 و tw1/0/2 في هذا التصميم.

# التحقق من الصحة (عزل جزئي محمي)

## بادئة العبارة (ورقة)

<#root>

Leaf01#

**show bgp l2vpn evpn route-type 2 0 0000.beef.cafe 10.1.202.1**

BGP routing table entry for [2][172.16.254.3:202][0][48][0000BEEFCAFE][32][10.1.202.1]/24, version 3411
Paths: (1 available, best #1, table evi_202)
  Not advertised to any peer
  Refresh Epoch 2
  Local, imported path from [2][172.16.254.6:202][0][48][0000BEEFCAFE][32][10.1.202.1]/24 (global)
    172.16.254.6 (metric 3) (via default) from 172.16.255.1 (172.16.255.1)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      EVPN ESI: 00000000000000000000, Label1 20201
      Extended Community: RT:65001:202 ENCAP:8

**EVPN DEF GW:0:0 <-- GW attribute added indicating this is GW prefix which L2 Relay uses**

      Originator: 172.16.255.6, Cluster list: 172.16.255.1
      rx pathid: 0, tx pathid: 0x0
      Updated on Sep 19 2023 19:57:25 UTC

## FED MATM (ورقة)

تأكد من تثبيت الورقة ل CGW Remote MAC في الجهاز

<#root>

Leaf01#

**show platform software fed switch active matm macTable vlan 202**

VLAN MAC Type Seq# EC_Bi Flags machandle siHandle riHandl
---
202 0006.f601.cd01 0x1 1093 0 0 0x71e05918f138 0x71e05917a1a8 0x0

202 0006.f601.cd44 0x1 14309 0 0 0x71e058cdc208 0x71e05917a1a8 0x0

**202**

**0000.beef.cafe 0x5000001**

```
       0      0     64  0x71e058ee5d88      0x71e059195f88      0x71e059171678      0x0
```

**<--- The GW MAC shows learnt via the Border Leaf Loopback**

```
Total Mac number of addresses:: 3
Summary:
Total number of secure addresses:: 0
Total number of drop addresses:: 0
Total number of lisp local addresses:: 0
Total number of lisp remote addresses:: 1
*a_time=aging_time(secs)  *e_time=total_elapsed_time(secs)
Type:
```

**MAT_DYNAMIC_ADDR 0x1**

```
  MAT_STATIC_ADDR            0x2  MAT_CPU_ADDR               0x4  MAT_DISCARD_ADDR           0x8
MAT_ALL_VLANS              0x10  MAT_NO_FORWARD            0x20  MAT_IPMULT_ADDR           0x40  MAT_RES
MAT_DO_NOT_AGE            0x100  MAT_SECURE_ADDR          0x200  MAT_NO_PORT              0x400  MAT_DRO
MAT_DUP_ADDR             0x1000  MAT_NULL_DESTINATION    0x2000  MAT_DOT1X_ADDR          0x4000  MAT_ROU
MAT_WIRELESS_ADDR       0x10000  MAT_SECURE_CFG_ADDR    0x20000  MAT_OPQ_DATA_PRESENT   0x40000  MAT_WIR
MAT_DLR_ADDR           0x100000  MAT_MRP_ADDR          0x200000  MAT_MSRP_ADDR         0x400000  MAT_LIS
```

**MAT_LISP_REMOTE_ADDR 0x1000000**

```
  MAT_VPLS_ADDR
```

**0x2000000  MAT_LISP_GW_ADDR     0x4000000**

**<-- these 3 values added = 0x5000001 (note that 0x4000000 = GW type address**

## MAC المحلي (ورقة)

<#root>

```
Leaf01#
```

**show switch**

```
Switch/Stack Mac Address : 682c.7bf8.8700 - Local Mac Address
Mac persistency wait time: Indefinite
                                             H/W   Current
Switch#   Role    Mac Address     Priority Version  State
------------------------------------------------------------------------------------------
*1       Active
```

**682c.7bf8.8700**

```
     1      V01     Ready
```

**<-- this is the MAC that will be added to DHCP Agent Remote ID**

## التطفل على بروتوكول DHCP (الورقة و CGW)

أكدت أن DHCP مكنت يتطفل على الورقة في القماش VLAN

<#root>

Leaf01#

**show ip dhcp snooping**

Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
202

**DHCP snooping is operational on following VLANs:  <-- Snooping on in the Fabric Vlan 202**

<...snip...>

**Insertion of option 82 is enabled**
**   circuit-id default format: vlan-mod-port**
**   remote-id: 682c.7bf8.8700 (MAC)  <--- Remote ID (RID) inserted by Leaf to DHCP packets**

<...snip...>

تأكد من تمكين التطفل على بروتوكول DHCP على CGW في شبكات VLAN الخاصة بالبنية والبوابة الخارجية

<#root>

CGW#

**show ip dhcp snooping**

Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
202,2021

**DHCP snooping is operational on following VLANs:  <-- Snooping on in the Fabric and External GW Vlans 202,2021**

<...snip...>

DHCP snooping trust/rate is configured on the following Interfaces:

Interface  Trusted  Allow option  Rate limit (pps)
---  ---  ---  ---

**TwentyFiveGigE1/0/1**

yes  yes  unlimited

**<-- Trust set on ports the OFFER arrives on**

Interface  Trusted  Allow option  Rate limit (pps)
---  ---  ---  ---
  Custom circuit-ids:

**TwentyFiveGigE1/0/2**

yes  yes  unlimited

**<-- Trust set on ports the OFFER arrives on**

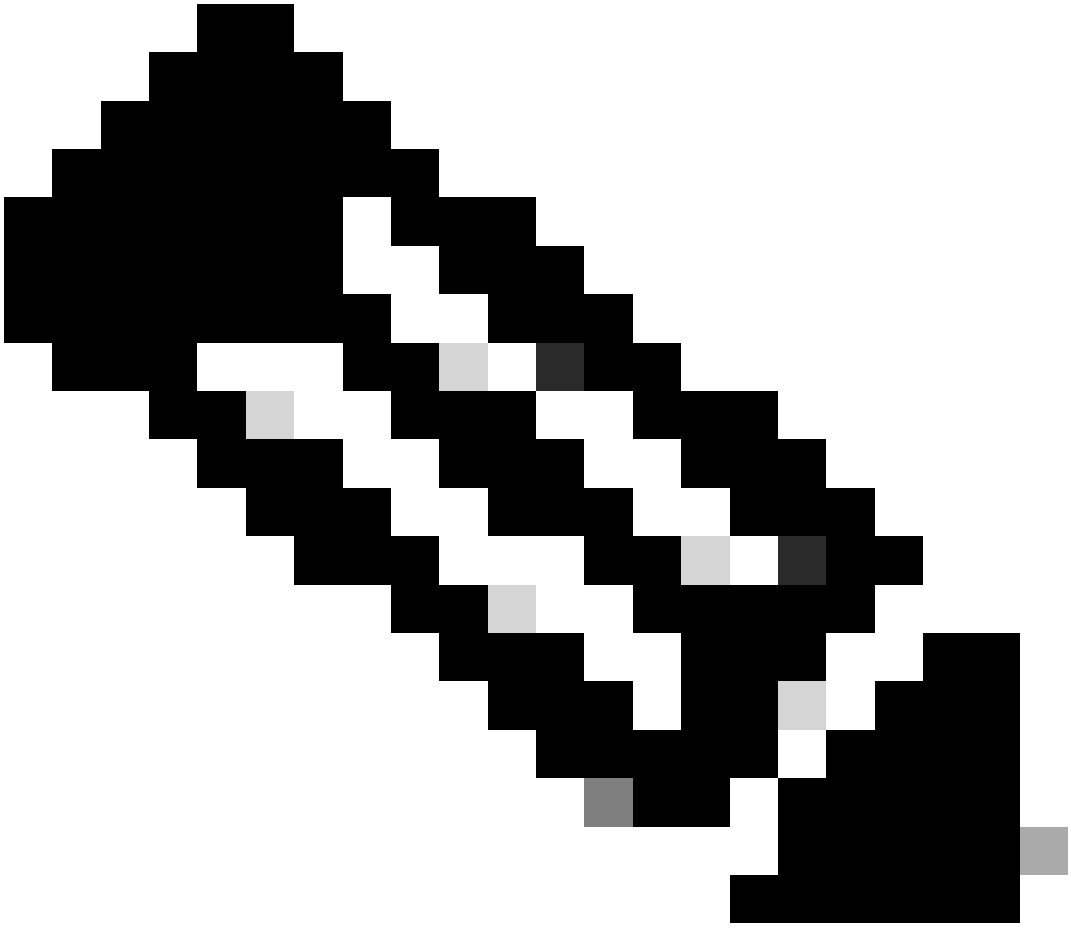
```
  Custom circuit-ids:
```

تأكيد إنشاء ربط التطفل على بروتوكول DHCP

```
<#root>

Leaf01#

show ip dhcp snooping binding

MacAddress


IpAddress

        Lease(sec)  Type           VLAN

Interface

------------------  ---------------  ----------  -------------  ----  --------------------
00:06:F6:01:CD:43

10.1.202.10

      34261       dhcp-snooping   202

GigabitEthernet1/0/1  <-- DHCP Snooping has created the binding

Total number of bindings: 1
```

## استكشاف الأخطاء وإصلاحها (أي نوع CGW)

يعد تصحيح الأخطاء مفيدا لإظهار كيفية معالجة عمليات التطفل على بروتوكول DHCP وترحيل L2 لحزم DHCP.



ملاحظة: يمكن إستخدام هذه الأخطاء لأي نوع من النشر يستخدم CGW مع ترحيل DCHP L2.

## تصحيح أخطاء التطفل على بروتوكول DHCP (الطرفي)

تصحيح أخطاء التطفل لتأكيد معالجة الحزمة

<#root>

Leaf01#

**debug ip dhcp snooping packet**

DHCP Snooping Packet debugging is on

Leaf01#

**show debugging**

DHCP Snooping packet debugging is on

ابدأ المضيف محاولة عنوان DHCP

- لهذا المستند تم إجراء إيقاف/عدم إيقاف SVI الذي يتم معالجته عبر DHCP لتشغيل تبادل DORA
- بالنسبة لمضيف Windows، يمكنك تنفيذ ipconfig /release > ipconfig /renew

تجميع تصحيح الأخطاء من show logging أو من نافذة المحطة الطرفية

DHCP لوكوتوكول برو اكتشاف

يتم ملاحظة الاكتشاف قادما من المنفذ المقابل للمضيف

```
<#root>

*Sep 19 20:16:31.164:

DHCP_SNOOPING: received new DHCP packet from input interface (GigabitEthernet1/0/1)  <-- host facing por


*Sep 19 20:16:31.177:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPDISCOVER, input interface: Gi1/0/1

, MAC da: ffff.ffff.ffff,

MAC sa: 0006.f601.cd43

, IP da: 255.255.255.255, IP sa: 0.0.0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.
*Sep 19 20:16:31.177: DHCP_SNOOPING: add relay information option.
*Sep 19 20:16:31.177:

DHCP_SNOOPING: Encoding opt82 CID in vlan-mod-port format         <-- Option 82 encoding


*Sep 19 20:16:31.177: DHCP_SNOOPING:VxLAN : vlan_id 202 VNI 20201 mod 1 port 1
*Sep 19 20:16:31.177:

DHCP_SNOOPING: Encoding opt82 RID in MAC address format           <-- Encoding the switch Remote ID (loc

*Sep 19 20:16:31.177: DHCP_SNOOPING: binary dump of relay info option, length: 26 data:
0x52 0x18 0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0 0x2 0x8 0x0 0x6

0x68 0x2C 0x7B 0xF8 0x87 0x0  <-- the switch local MAC 682c.7bf8.8700

*Sep 19 20:16:31.177: DHCPS BRIDGE PAK: vlan=202 platform_flags=1
*Sep 19 20:16:31.177: DHCP_SNOOPING: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flo
*Sep 19 20:16:31.177:

DHCP_SNOOPING: L2RELAY: sent unicast packet to default gw: 0000.beef.cafe vlan 0 src intf GigabitEtherne
```

DHCP عرض

يظهر العرض قادما من واجهة نفق البنية

```
<#root>
```

```
*Sep 19 20:16:33.180:

DHCP_SNOOPING: received new DHCP packet from input interface (Tunnel0)

*Sep 19 20:16:33.194:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPOFFER, input interface: Tu0, MAC da: 0006.f601

, IP da: 255.255.255.255, IP sa: 10.1.202.1, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 10.1.202.18, DHCP siadd
*Sep 19 20:16:33.194: DHCP_SNOOPING: binary dump of option 82, length: 26 data:
0x52 0x18 0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0 0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8
*Sep 19 20:16:33.194: DHCP_SNOOPING: binary dump of extracted circuit id, length: 14 data:
0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0
*Sep 19 20:16:33.194: DHCP_SNOOPING: binary dump of extracted remote id, length: 10 data:
0x2 0x8 0x0 0x6

0x68 0x2C 0x7B 0xF8 0x87 0x0                                    <-- the switch local MAC 682c.7bf8.8700

*Sep 19 20:16:33.194:  actual_fmt_cid OPT82_FMT_CID_VXLAN_MOD_PORT_INTF global_opt82_fmt_rid OPT82_FMT_
*Sep 19 20:16:33.194: dhcp_snooping_platform_is_local_dhcp_packet: VXLAN-MOD-PORT opt82 vni 20201, vlan
*Sep 19 20:16:33.194:

DHCP_SNOOPING: opt82 data indicates local packet      <-- switch found its own RID in Option 82 paramete


*Sep 19 20:16:33.194: DHCP_SNOOPING: remove relay information option.
*Sep 19 20:16:33.194: DHCP_SNOOPING opt82_fmt_cid_intf OPT82_FMT_CID_VXLAN_MOD_PORT_INTF opt82_fmt_cid_
*Sep 19 20:16:33.194:

DHCP_SNOOPING: VxLAN vlan_id 202 VNI 20201 mod 1 port 1

*Sep 19 20:16:33.194:

DHCP_SNOOPING: mod 1 port 1 idb Gi1/0/1 found for 0006.f601.cd43

*Sep 19 20:16:33.194: DHCP_SNOOPING: calling forward_dhcp_reply
*Sep 19 20:16:33.194: platform lookup dest vlan for input_if: Tunnel0, is  tunnel, if_output: NULL, if_
*Sep 19 20:16:33.194: DHCP_SNOOPING opt82_fmt_cid_intf OPT82_FMT_CID_VXLAN_MOD_PORT_INTF opt82_fmt_cid_
*Sep 19 20:16:33.194: DHCP_SNOOPING: VxLAN vlan_id 202 VNI 20201 mod 1 port 1
*Sep 19 20:16:33.194: DHCP_SNOOPING: mod 1 port 1 idb Gi1/0/1 found for 0006.f601.cd43
*Sep 19 20:16:33.194: DHCP_SNOOPING: vlan 202 after pvlan check
*Sep 19 20:16:33.207:

DHCP_SNOOPING: direct forward dhcp replyto output port: GigabitEthernet1/0/1.  <-- sending packet to hos
```

طلب DHCP

رأيت طلب من المضيف يواجه ميناء

<#root>

```
*Sep 19 20:16:33.209:

DHCP_SNOOPING: received new DHCP packet from input interface (GigabitEthernet1/0/1)


*Sep 19 20:16:33.222:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPREQUEST

, input interface: Gi1/0/1, MAC da: ffff.ffff.ffff, MAC sa: 0006.f601.cd43, IP da: 255.255.255.255, IP
```

```
*Sep 19 20:16:33.222: DHCP_SNOOPING: add relay information option.
*Sep 19 20:16:33.222: DHCP_SNOOPING: Encoding opt82 CID in vlan-mod-port format
*Sep 19 20:16:33.222: DHCP_SNOOPING:VxLAN : vlan_id 202 VNI 20201 mod 1 port 1
*Sep 19 20:16:33.222: DHCP_SNOOPING: Encoding opt82 RID in MAC address format
*Sep 19 20:16:33.222: DHCP_SNOOPING: binary dump of relay info option, length: 26 data:
0x52 0x18 0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0 0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8
*Sep 19 20:16:33.222: DHCPS BRIDGE PAK: vlan=202 platform_flags=1
*Sep 19 20:16:33.222: DHCP_SNOOPING: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flo
*Sep 19 20:16:33.222:

DHCP_SNOOPING: L2RELAY: sent unicast packet to default gw: 0000.beef.cafe vlan 0 src intf GigabitEtherne
```

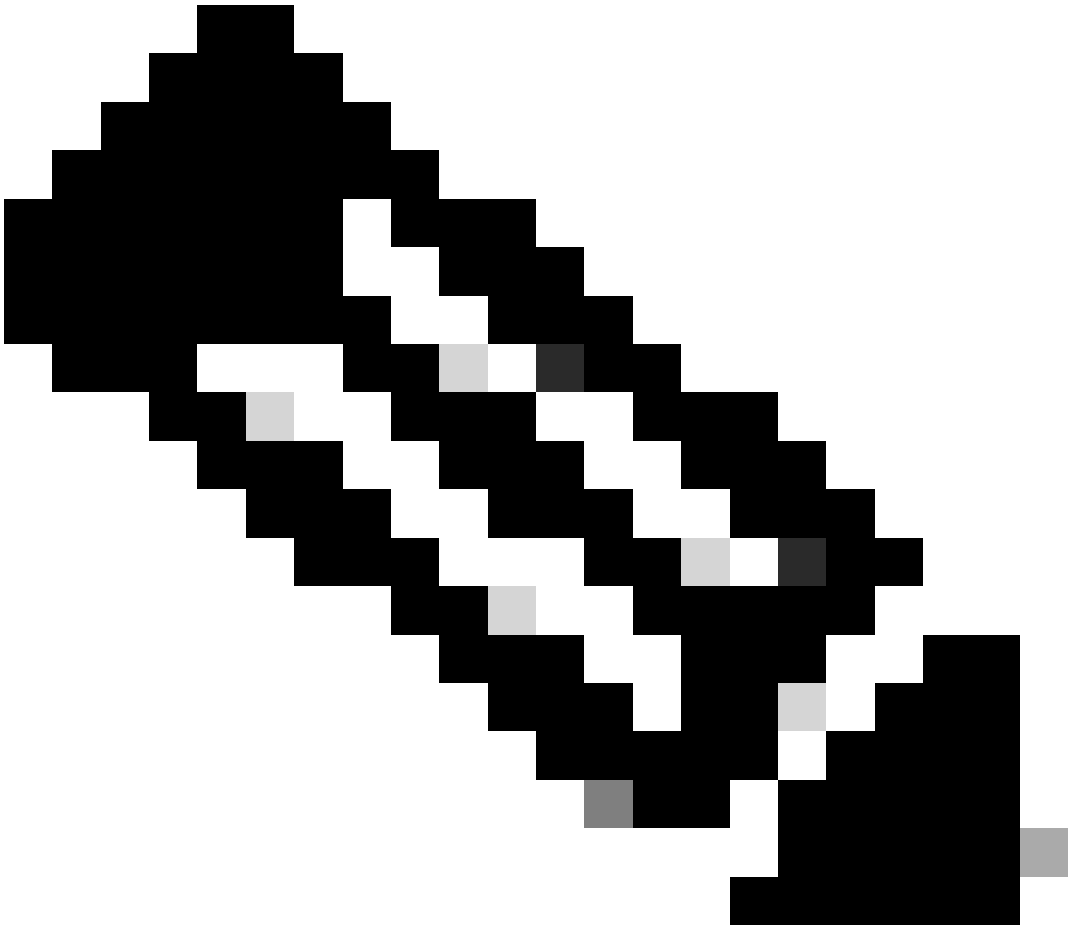
## DHCP ACK

"آك" ظهر قادما من واجهة "نفق القماش"

```
<#root>

*Sep 19 20:16:33.225:

DHCP_SNOOPING: received new DHCP packet from input interface (Tunnel0)

*Sep 19 20:16:33.238:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPACK, input interface: Tu0, MAC da: 0006.f601.c

, IP da: 255.255.255.255, IP sa: 10.1.202.1, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 10.1.202.10, DHCP siadd
*Sep 19 20:16:33.238: DHCP_SNOOPING: binary dump of option 82, length: 26 data:
0x52 0x18 0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0 0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8
*Sep 19 20:16:33.239: DHCP_SNOOPING: binary dump of extracted circuit id, length: 14 data:
0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0
*Sep 19 20:16:33.239: DHCP_SNOOPING: binary dump of extracted remote id, length: 10 data:
0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8 0x87 0x0
*Sep 19 20:16:33.239:  actual_fmt_cid OPT82_FMT_CID_VXLAN_MOD_PORT_INTF global_opt82_fmt_rid OPT82_FMT_
*Sep 19 20:16:33.239: dhcp_snooping_platform_is_local_dhcp_packet: VXLAN-MOD-PORT opt82 vni 20201, vlan_
*Sep 19 20:16:33.239:

DHCP_SNOOPING: opt82 data indicates local packet

*Sep 19 20:16:33.239:

dhcp_snooping_platform_is_local_dhcp_packet: VXLAN-MOD-PORT opt82 vni 20201, vlan_id 202

*Sep 19 20:16:33.239: DHCP_SNOOPING: opt82 data indicates local packet
*Sep 19 20:16:33.239: DHCP_SNOOPING opt82_fmt_cid_intf OPT82_FMT_CID_VXLAN_MOD_PORT_INTF opt82_fmt_cid_
*Sep 19 20:16:33.239: DHCP_SNOOPING: VxLAN vlan_id 202 VNI 20201 mod 1 port 1
*Sep 19 20:16:33.239:

DHCP_SNOOPING: mod 1 port 1 idb Gi1/0/1 found for 0006.f601.cd43

*Sep 19 20:16:33.239: DHCP_SNOOPING: Reroute dhcp pak, message type: DHCPACK
*Sep 19 20:16:33.239: DHCP_SNOOPING: remove relay information option.
*Sep 19 20:16:33.239: DHCP_SNOOPING opt82_fmt_cid_intf OPT82_FMT_CID_VXLAN_MOD_PORT_INTF opt82_fmt_cid_
*Sep 19 20:16:33.239: DHCP_SNOOPING: VxLAN vlan_id 202 VNI 20201 mod 1 port 1
*Sep 19 20:16:33.239: DHCP_SNOOPING: mod 1 port 1 idb Gi1/0/1 found for 0006.f601.cd43
*Sep 19 20:16:33.239: DHCP_SNOOPING: calling forward_dhcp_reply
*Sep 19 20:16:33.239: platform lookup dest vlan for input_if: Tunnel0, is  tunnel, if_output: NULL, if_
*Sep 19 20:16:33.239: DHCP_SNOOPING opt82_fmt_cid_intf OPT82_FMT_CID_VXLAN_MOD_PORT_INTF opt82_fmt_cid_
*Sep 19 20:16:33.239: DHCP_SNOOPING: VxLAN vlan_id 202 VNI 20201 mod 1 port 1
*Sep 19 20:16:33.239: DHCP_SNOOPING: mod 1 port 1 idb Gi1/0/1 found for 0006.f601.cd43
*Sep 19 20:16:33.239: DHCP_SNOOPING: vlan 202 after pvlan check
```

```
*Sep 19 20:16:33.252:
DHCP_SNOOPING: direct forward dhcp replyto output port: GigabitEthernet1/0/1.
```

---



ملاحظة: هذه الأخطاء تم قصها. يقومون بإنشاء تفريغ ذاكرة للحزمة، ولكن هذا التعليق التوضيحي لهذا الجزء من نتيجة تصحيح الأخطاء يقع خارج نطاق المستند.

---

## تصحيح أخطاء التطفل على بروتوكول DHCP (CGW)

اكتشاف بروتوكول DHCP

بسبب كيفية إرسال الحزمة واستقبالها مرة أخرى على CGW (معبأ عند جدار الحماية) يتم إطلاق تصحيح الأخطاء مرتين

وصول من البنية على واجهة النفق وإرسال الطرازين 1/0/1 إلى جدار الحماية في شبكة VLAN الليفية 202

<#root>

*Apr 16 14:37:43.890:

**DHCP_SNOOPING: received new DHCP packet from input interface (Tunnel0)  <-- Discover sent from Leaf01 a**

*Apr 16 14:37:43.901: DHCP_SNOOPING: process new DHCP packet, message type: DHCPDISCOVER, input interfa
*Apr 16 14:37:43.901: DHCPS BRIDGE PAK: vlan=202 platform_flags=1
*Apr 16 14:37:43.901:

**DHCP_SNOOPING: bridge packet send packet to port: TwentyFiveGigE1/0/1, pak_vlan 202. <-- Sent to Firewal**

وصول من جدار الحماية على TW 1/0/2 في شبكة VLAN رقم 2021 للإساله إلى مساعد SVI إلى
خادم DHCP

<#root>

*Apr 16 14:37:43.901:

**DHCP_SNOOPING: received new DHCP packet from input interface (TwentyFiveGigE1/0/2) <-- Firewall sends di**

*Apr 16 14:37:43.911: DHCP_SNOOPING: process new DHCP packet, message type: DHCPDISCOVER, input interfa
*Apr 16 14:37:43.911:

**DHCPS BRIDGE PAK: vlan=2021 platform_flags=1      <-- Vlan discover seen is now 2021**

*Apr 16 14:37:43.911:

**DHCP_SNOOPING: Packet destined to SVI Mac:0000.beef.cafe**

*Apr 16 14:37:43.911:

**DHCP_SNOOPING: bridge packet send packet to cpu port: Vlan2021.  <-- Packet punted to CPU for handling b**

عرض DHCP

يصل من خادم DHCP مرة أخرى إلى SVI 2021 حيث يتم تكوين المساعد وإعادة توجيهه إلى جدار
الحماية

<#root>

*Apr 16 14:37:45.913:

**DHCP_SNOOPING: received new DHCP packet from input interface (Vlan2021)  <-- Arriving from the DHCP serv**

*Apr 16 14:37:45.923:

**DHCP_SNOOPING: process new DHCP packet, message type: DHCPOFFER, input interface: Vl2021**

, MAC da: ffff.ffff.ffff, MAC sa: 0000.beef.cafe, IP da: 255.255.255.255, IP sa: 10.1.202.1, DHCP ciadd

```
*Apr 16 14:37:45.923: DHCP_SNOOPING: binary dump of option 82, length: 26 data:
0x52 0x18 0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0 0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8
*Apr 16 14:37:45.924: DHCP_SNOOPING: binary dump of extracted circuit id, length: 14 data:
0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0
*Apr 16 14:37:45.924: DHCP_SNOOPING: binary dump of extracted remote id, length: 10 data:
0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8 0x87 0x0
*Apr 16 14:37:45.924: actual_fmt_cid OPT82_FMT_CID_VXLAN_MOD_PORT_INTF global_opt82_fmt_rid OPT82_FMT_R
*Apr 16 14:37:45.924: dhcp_snooping_platform_is_local_dhcp_packet: VXLAN-MOD-PORT opt82 vni 20201, vlan
*Apr 16 14:37:45.924:

DHCP_SNOOPING: opt82 data indicates not a local packet


*Apr 16 14:37:45.924: DHCP_SNOOPING: can't parse option 82 data of the message,it is either in wrong fo

<-- This is expected even in working scenario (disregard it)


*Apr 16 14:37:45.924: DHCP_SNOOPING: calling forward_dhcp_reply
*Apr 16 14:37:45.924: platform lookup dest vlan for input_if: Vlan2021, is NOT tunnel, if_output: Vlan2
*Apr 16 14:37:45.924: DHCP_SNOOPING: vlan 2021 after pvlan check
*Apr 16 14:37:45.934:

DHCP_SNOOPING: direct forward dhcp replyto output port: TwentyFiveGigE1/0/2. <-- sending back toward the
```

يصل من جدار الحماية في شبكة VLAN الليفية ويرسل من CGW إلى القناة الليفية
باتجاه الورقة

<#root>

```
*Apr 16 14:37:45.934:

DHCP_SNOOPING: received new DHCP packet from input interface (TwentyFiveGigE1/0/1)


*Apr 16 14:37:45.944:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPOFFER, input interface: Twe1/0/1

, MAC da: ffff.ffff.ffff, MAC sa: 0000.beef.cafe, IP da: 255.255.255.255, IP sa: 10.1.202.1, DHCP ciadd
*Apr 16 14:37:45.944: DHCP_SNOOPING: binary dump of option 82, length: 26 data:
0x52 0x18 0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0 0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8
*Apr 16 14:37:45.944: DHCP_SNOOPING: binary dump of extracted circuit id, length: 14 data:
0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0
*Apr 16 14:37:45.944: DHCP_SNOOPING: binary dump of extracted remote id, length: 10 data:
0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8 0x87 0x0
*Apr 16 14:37:45.944: actual_fmt_cid OPT82_FMT_CID_VXLAN_MOD_PORT_INTF global_opt82_fmt_rid OPT82_FMT_R
*Apr 16 14:37:45.944: dhcp_snooping_platform_is_local_dhcp_packet: VXLAN-MOD-PORT opt82 vni 20201, vlan
*Apr 16 14:37:45.945:

DHCP_SNOOPING: opt82 data indicates not a local packet


*Apr 16 14:37:45.945: DHCP_SNOOPING: EVPN enabled Ex GW:fabric relay can't parse option 82 data of the
*Apr 16 14:37:45.945: DHCP_SNOOPING: client address lookup failed to locate client interface, retry loo
*Apr 16 14:37:45.945: DHCP_SNOOPING: lookup packet destination port failed to get mat entry for mac: 00
*Apr 16 14:37:45.945:

DHCP_SNOOPING: L2RELAY: Ex GW unicast bridge packet to fabric: vlan id 202 from Twe1/0/1  <-- L2 RELAY f
```

طلب DHCP

<#root>

*Apr 16 14:37:45.967:

**DHCP_SNOOPING: received new DHCP packet from input interface (Tunnel0)**

*Apr 16 14:37:45.978:

**DHCP_SNOOPING: process new DHCP packet, message type: DHCPREQUEST**

, input interface: Tu0, MAC da: 0000.beef.cafe, MAC sa: 0006.f601.cd43, IP da: 255.255.255.255, IP sa:
*Apr 16 14:37:45.978: DHCPS BRIDGE PAK: vlan=202 platform_flags=1
*Apr 16 14:37:45.978:

**DHCP_SNOOPING: bridge packet send packet to port: TwentyFiveGigE1/0/1, pak_vlan 202. <-- Send toward Fir**

<#root>

*Apr 16 14:37:45.978:

**DHCP_SNOOPING: received new DHCP packet from input interface (TwentyFiveGigE1/0/2) <-- Receive from Fire**

*Apr 16 14:37:45.989:

**DHCP_SNOOPING: process new DHCP packet, message type: DHCPREQUEST**

, input interface: Twe1/0/2, MAC da: 0000.beef.cafe, MAC sa: 0006.f601.cd43, IP da: 255.255.255.255, IP
*Apr 16 14:37:45.989: DHCPS BRIDGE PAK: vlan=2021 platform_flags=1
*Apr 16 14:37:45.989: DHCP_SNOOPING: Packet destined to SVI Mac:0000.beef.cafe
*Apr 16 14:37:45.989:

**DHCP_SNOOPING: bridge packet send packet to cpu port: Vlan2021.  <-- Punt to CPU / DHCP helper**

DHCP ACK

<#root>

*Apr 16 14:37:45.990:

**DHCP_SNOOPING: received new DHCP packet from input interface (Vlan2021)  <-- Packet back to SVI from DHC**

*Apr 16 14:37:46.000:

**DHCP_SNOOPING: process new DHCP packet, message type: DHCPACK, input interface: Vl2021**

, MAC da: ffff.ffff.ffff, MAC sa: 0000.beef.cafe, IP da: 255.255.255.255, IP sa: 10.1.202.1, DHCP ciadd
*Apr 16 14:37:46.000: DHCP_SNOOPING: binary dump of option 82, length: 26 data:
0x52 0x18 0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0 0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8

```
*Apr 16 14:37:46.000: DHCP_SNOOPING: binary dump of extracted circuit id, length: 14 data:
0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0
*Apr 16 14:37:46.000: DHCP_SNOOPING: binary dump of extracted remote id, length: 10 data:
0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8 0x87 0x0
*Apr 16 14:37:46.001: actual_fmt_cid OPT82_FMT_CID_VXLAN_MOD_PORT_INTF global_opt82_fmt_rid OPT82_FMT_R
*Apr 16 14:37:46.001: dhcp_snooping_platform_is_local_dhcp_packet: VXLAN-MOD-PORT opt82 vni 20201, vlan
*Apr 16 14:37:46.001:
```

**DHCP_SNOOPING: opt82 data indicates not a local packet  <-- found this is coming from Leaf01 RID**

```
*Apr 16 14:37:46.001: DHCP_SNOOPING: can't parse option 82 data of the message,it is either in wrong fo
*Apr 16 14:37:46.001: DHCP_SNOOPING: calling forward_dhcp_reply
*Apr 16 14:37:46.001: platform lookup dest vlan for input_if: Vlan2021, is NOT tunnel, if_output: Vlan2
*Apr 16 14:37:46.001: DHCP_SNOOPING: vlan 2021 after pvlan check
*Apr 16 14:37:46.011:
```

**DHCP_SNOOPING: direct forward dhcp replyto output port: TwentyFiveGigE1/0/2.  <-- Send to Firewall**

<#root>

```
*Apr 16 14:37:46.011:
```

**DHCP_SNOOPING: received new DHCP packet from input interface (TwentyFiveGigE1/0/1)  <-- Coming back in f**

```
*Apr 16 14:37:46.022:
```

**DHCP_SNOOPING: process new DHCP packet, message type: DHCPACK, input interface: Twe1/0/1,**

```
 MAC da: ffff.ffff.ffff, MAC sa: 0000.beef.cafe, IP da: 255.255.255.255, IP sa: 10.1.202.1, DHCP ciaddr
*Apr 16 14:37:46.022: DHCP_SNOOPING: binary dump of option 82, length: 26 data:
0x52 0x18 0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0 0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8
*Apr 16 14:37:46.022: DHCP_SNOOPING: binary dump of extracted circuit id, length: 14 data:
0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0
*Apr 16 14:37:46.022: DHCP_SNOOPING: binary dump of extracted remote id, length: 10 data:
0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8 0x87 0x0
*Apr 16 14:37:46.022: actual_fmt_cid OPT82_FMT_CID_VXLAN_MOD_PORT_INTF global_opt82_fmt_rid OPT82_FMT_R
*Apr 16 14:37:46.022: dhcp_snooping_platform_is_local_dhcp_packet: VXLAN-MOD-PORT opt82 vni 20201, vlan
*Apr 16 14:37:46.022:
```

**DHCP_SNOOPING: opt82 data indicates not a local packet**

```
*Apr 16 14:37:46.022: DHCP_SNOOPING: EVPN enabled Ex GW:fabric relay can't parse option 82 data of the
*Apr 16 14:37:46.022: DHCP_SNOOPING: client address lookup failed to locate client interface, retry loo
*Apr 16 14:37:46.022: DHCP_SNOOPING: lookup packet destination port failed to get mat entry for mac: 00
*Apr 16 14:37:46.022: DHCP_SNOOPING: can't find client's destination port, packet is assumed to be not
*Apr 16 14:37:46.022: DHCP_SNOOPING: client address lookup failed to locate client interface, retry loo
*Apr 16 14:37:46.022: DHCP_SNOOPING: lookup packet destination port failed to get mat entry for mac: 00
*Apr 16 14:37:46.022:
```

**DHCP_SNOOPING: L2RELAY: Ex GW unicast bridge packet to fabric: vlan id 202 from Twe1/0/1  <-- Send packe**

## التقاط مدمج

أستخدم EPC لتأكيد صحة تبادل حزم DHCP والمعلومات

- يتم إظهار ذلك من منظور CGW، ولكن يمكن تكرار العملية على الوحدة الطرفية للتحقق من تبادل الحزمة
- يبدي هذا مثال لـ discover بما أن العملية والتحليل هما نفسهما لـ الآخر DHCP ربط

تحقق من الطريق إلى وقهة الاسترجاع

<#root>

CGW#

**show ip route 172.16.254.3**

```
Routing entry for 172.16.254.3/32
  Known via "ospf 1", distance 110, metric 3, type intra area
  Last update from 172.16.1.25 on TwentyFiveGigE1/0/47, 2w6d ago
  Routing Descriptor Blocks:
  * 172.16.1.29, from 172.16.255.3, 2w6d ago,
```

**via TwentyFiveGigE1/0/48**

```
      Route metric is 3, traffic share count is 1
    172.16.1.25, from 172.16.255.3, 2w6d ago,
```

**via TwentyFiveGigE1/0/47**

```
      Route metric is 3, traffic share count is 1
```

قم بتكوين الالتقاط للتشغيل على الارتباطات التي تواجه الوقهة 01

```
monitor capture 1 interface TwentyFiveGigE1/0/47 BOTH
monitor capture 1 interface TwentyFiveGigE1/0/48 BOTH
monitor capture 1 match any
monitor capture 1 buffer size 100
monitor capture 1 limit pps 1000
```

بدء الالتقاط، قم بتشغيل المضيف لطلب عنوان IP لـ DHCP، ووقف الالتقاط

<#root>

```
monitor capture 1 start
  (have the host request dhcp ip)
monitor capture 1 stop
```

عرض نتيجة الالتقاط بدءا من اكتشاف DHCP (انتبه إلى معرف الحركة لتأكيد أن هذا وه حدث DORA نفسه)

<#root>

**CGW#**

**show monitor cap 1 buff brief | i DHCP**

**16**

**12.737135 0.0.0.0 -> 255.255.255.255 DHCP 434**

**DHCP Discover**

**-**

**Transaction ID 0x78b <-- Discover starts at Frame 16 with all same transaction ID**

**18 14.740041 10.1.202.1 -> 255.255.255.255 DHCP 438 DHCP**

**Offer**

**- Transaction ID**

**0x78b**

**19 14.742741 0.0.0.0 -> 255.255.255.255 DHCP 452 DHCP**

**Request**

**- Transaction ID**

**0x78b**

**20 14.745646 10.1.202.1 -> 255.255.255.255 DHCP 438 DHCP**

**ACK**

**- Transaction ID**

**0x78b**

<#root>

**CGW#**

**sh mon cap 1 buff detailed | b Frame 16**

**Frame 16:**

**434 bytes on wire (3472 bits), 434 bytes captured (3472 bits) on interface /tmp/epc_ws/wif_to_ts_pipe,**
**[Protocols in frame: eth:ethertype:ip:udp:vxlan:eth:ethertype:ip:udp:dhcp]**
**Ethernet II,**

**Src: dc:77:4c:8a:6d:7f**

**(dc:77:4c:8a:6d:7f),**

**Dst: 10:f9:20:2e:9f:82**

**(10:f9:20:2e:9f:82)**

**<-- Underlay Interface MACs**

**Type: IPv4 (0x0800)**
**Internet Protocol Version 4,**

**Src: 172.16.254.3, Dst: 172.16.254.6**

User Datagram Protocol, Src Port: 65281,

Dst Port: 4789 <-- VXLAN Port

Virtual eXtensible Local Area Network
VXLAN Network Identifier

(VNI): 20201 <-- Correct VNI / Segment

Reserved: 0
Ethernet II,

Src: 00:06:f6:01:cd:43

(00:06:f6:01:cd:43),

Dst: 00:00:be:ef:ca:fe

(00:00:be:ef:ca:fe)

<-- Inner Packet destined to CGW MAC

Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol,

Src Port: 68, Dst Port: 67 <-- DHCP ports

Dynamic Host Configuration Protocol (Discover) <-- DHCP Discover Packet

Client MAC address: 00:06:f6:01:cd:43

(00:06:f6:01:cd:43)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP

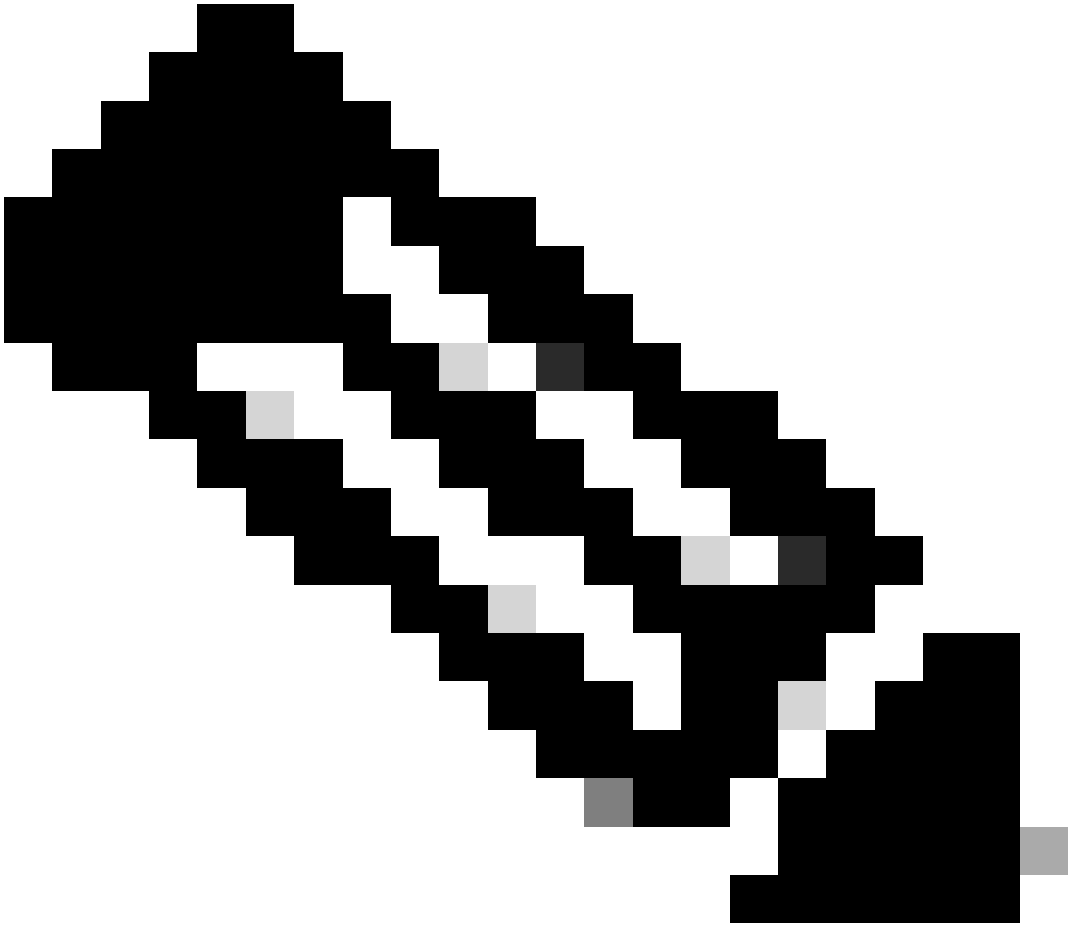
Option: (53) DHCP Message Type (Discover)

Length: 1
DHCP: Discover (1)
Option: (57) Maximum DHCP Message Size
Length: 2
Maximum DHCP Message Size: 1152
Option: (61) Client identifier
Length: 27
Type: 0
Client Identifier: cisco-0006.f601.cd43-Vl202
Option: (12) Host Name
Length: 17

Host Name: 9300-HOST-3750X-2

Option: (55) Parameter Request List
Length: 8
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
Parameter Request List Item: (3) Router

```
        Parameter Request List Item: (33) Static Route
        Parameter Request List Item: (150) TFTP Server Address
        Parameter Request List Item: (43) Vendor-Specific Information
    Option: (60) Vendor class identifier
        Length: 8
        Vendor class identifier: ciscopnp


Option: (82) Agent Information Option

        Length: 24
        Option 82 Suboption: (1) Agent Circuit ID
            Length: 12
            Agent Circuit ID: 010a000800004ee901010000


Option 82 Suboption: (2) Agent Remote ID

            Length: 8


Agent Remote ID:

000

6682c7bf88700  <-- switch base mac 682c.7bf8.8700 (from 'show switch')

    Option: (255) End
        Option End: 255
```



ملاحظة: يمكن إستخدام أداة الالتقاط على أي أوراق أو CGW لتحديد النقطة الأخيرة التي يشتبه في أن جزء من تبادل DHCP DORA بها فشل.

---

التحقق من إحصائيات التطفل الأخطاء

<#root>

```
Leaf01#

show ip dhcp snooping statistics detail

 Packets Processed by DHCP Snooping                  = 1288


Packets Dropped Because

   IDB not known                                     = 0
   Queue full                                        = 0
   Interface is in errdisabled                       = 0
   Rate limit exceeded                               = 0
   Received on untrusted ports                       = 0
```

```
   Nonzero giaddr                                  = 0
   Source mac not equal to chaddr                  = 0
   No binding entry                                = 0
   Insertion of opt82 fail                         = 0
   Unknown packet                                  = 0
   Interface Down                                  = 0
   Unknown output interface                        = 0
   Misdirected Packets                             = 0
   Packets with Invalid Size                       = 0
   Packets with Invalid Option                     = 0

<-- Look for any drop counter that is actively incrementing when the issue is seen.
```

التحقق من مسار التنصت للتطفل على بروتوكول DHCP

- CoPP هو المكون الرئيسي الذي يقوم بإسقاط الحزم في مسار الحزم

<#root>

```
Leaf01#

show platform hardware switch active qos queue stats internal cpu policer

                         CPU Queue Statistics
============================================================================================
                                           (default) (set)     Queue        Queue
QId

PlcIdx

  Queue Name                Enabled   Rate     Rate      Drop(Bytes)

Drop(Frames)

--------------------------------------------------------------------------------------------
17

6


DHCP Snooping

               Yes     400       400      0

 0


              CPU Queue Policer Statistics
=============================================================================

Policer

    Policer Accept   Policer Accept  Policer Drop  Policer Drop

Index

         Bytes          Frames        Bytes          Frames
-----------------------------------------------------------------
```

```
6          472723           1288            0             0
```

أمر آخر مفيد جدا لتحديد مكان حدوث طوفان محتمل في الحزم هو "show platform software fed switch active punt rate interfaces"

- وهذا مفيد للغاية للعثور على واجهة مصدر حيث تحدث الفيضانات والتي تعمل على إزدحام مسار الحزم وتؤثر على حركة المرور الشرعية المرتبطة بوحدة المعالجة المركزية (CPU)

<#root>

```
Leaf01#

show platform software fed switch active punt rates interfaces

Punt Rate on Interfaces Statistics

Packets per second averaged over 10 seconds, 1 min and 5 mins
================================================================================================
                               |           |  Recv |  Recv |  Recv |  Drop |  Drop  |  Drop

<-- Receive and drop rates for this port

 Interface Name              |  IF_ID    |  10s  |  1min |  5min |  10s  |  1min  |  5min
================================================================================================


GigabitEthernet1/0/1          0x0000000a

       2       2       2       0       0       0

<-- the port and its IF-ID which can be used in the next command


------------------------------------------------------------------------------------------------
```

<#root>

```
Leaf01#

show platform software fed switch active punt rates interfaces 0xa  <-- From previous command (omit the

Punt Rate on Single Interfaces Statistics


Interface : GigabitEthernet1/0/1 [if_id: 0xA]


  Received                         Dropped
  --------                         -------
   Total          : 8032546          Total           : 0
   10 sec average : 2                10 sec average  : 0
    1 min average : 2                 1 min average  : 0
    5 min average : 2                 5 min average  : 0


Per CPUQ punt stats on the interface
```

```
 (rate averaged over 10s interval)
=================================================================================
 Q  |          Queue                  |  Recv   |  Recv  |  Drop  |  Drop  |
 no |          Name                   |  Total  |  Rate  |  Total |  Rate  |
=================================================================================
 17

 CPU_Q_DHCP_SNOOPING

                 1216        0        0        0
<...snip...>
```

## حالات عميل التطفل على بروتوكول DHCP

الحظ تبادل رسائل DHCP باستخدام هذه الأمر. يمكن تشغيل ذلك على كل من Leaf أو CGW لرؤية تتبع الحدث

<#root>

Leaf01#

**show platform dhcpsnooping client stats 0006.F601.CD43**

DHCPSN: DHCP snooping server
DHCPD: DHCP protocol daemen
L2FWD: Transmit Packet to driver in L2 format
FWD: Transmit Packet to driver

**(B): Dhcp message's response expected as 'B'roadcast**
**(U): Dhcp message's response expected as 'U'nicast**

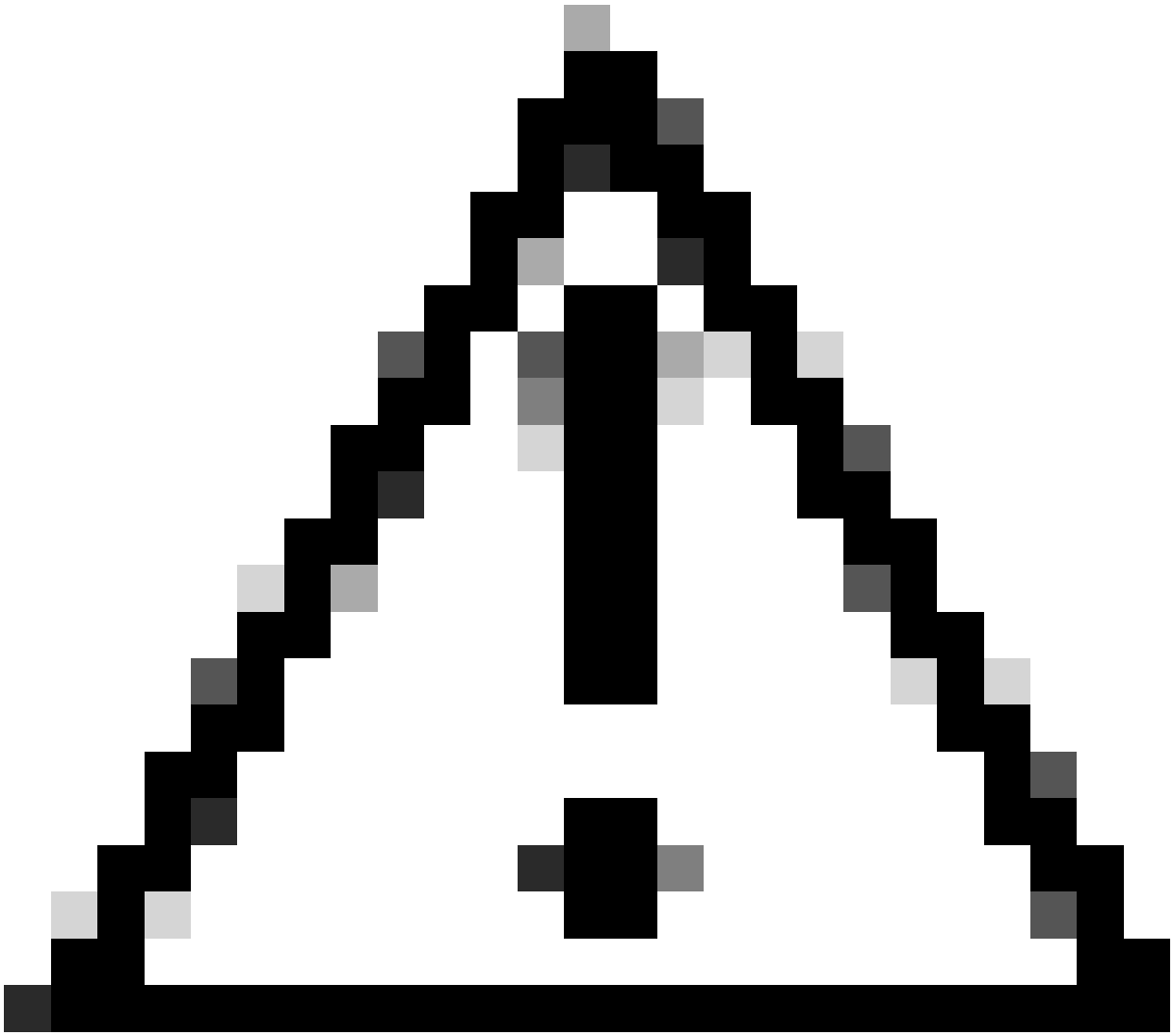
**Packet Trace for client MAC 0006.F601.CD43:**

```
Timestamp                Destination MAC  Destination Ip  VLAN  Message       Handler:Action
------------------------ ---------------- --------------- ----  ------------ ----------------
2023/09/28 14:53:59.866  FFFF.FFFF.FFFF   255.255.255.255 202  DHCPDISCOVER(B) PUNT:RECEIVED
2023/09/28 14:53:59.866  FFFF.FFFF.FFFF   255.255.255.255 202  DHCPDISCOVER(B) PUNT:TO_DHCPSN
2023/09/28 14:53:59.867  FFFF.FFFF.FFFF   255.255.255.255 202  DHCPDISCOVER(B) BRIDGE:RECEIVED
2023/09/28 14:53:59.867  0000.BEEF.CAFE   255.255.255.255 202  DHCPDISCOVER(B) L2INJECT:TO_FWD
2023/09/28 14:53:59.867  FFFF.FFFF.FFFF   255.255.255.255 202  DHCPDISCOVER(B) BRIDGE:TO_INJECT
2023/09/28 14:53:59.867  FFFF.FFFF.FFFF   255.255.255.255 202  DHCPDISCOVER(B) L2INJECT:TO_FWD
2023/09/28 14:54:01.871  0006.F601.CD43   255.255.255.255 202  DHCPOFFER(B)    PUNT:RECEIVED
2023/09/28 14:54:01.871  0006.F601.CD43   255.255.255.255 202  DHCPOFFER(B)    PUNT:TO_DHCPSN
2023/09/28 14:54:01.874  FFFF.FFFF.FFFF   255.255.255.255 202  DHCPREQUEST(B)  PUNT:RECEIVED
2023/09/28 14:54:01.874  FFFF.FFFF.FFFF   255.255.255.255 202  DHCPREQUEST(B)  PUNT:TO_DHCPSN
2023/09/28 14:54:01.874  FFFF.FFFF.FFFF   255.255.255.255 202  DHCPREQUEST(B)  BRIDGE:RECEIVED
2023/09/28 14:54:01.874  0000.BEEF.CAFE   255.255.255.255 202  DHCPREQUEST(B)  L2INJECT:TO_FWD
2023/09/28 14:54:01.874  FFFF.FFFF.FFFF   255.255.255.255 202  DHCPREQUEST(B)  BRIDGE:TO_INJECT
2023/09/28 14:54:01.874  FFFF.FFFF.FFFF   255.255.255.255 202  DHCPREQUEST(B)  L2INJECT:TO_FWD
2023/09/28 14:54:01.877  0006.F601.CD43   255.255.255.255 202  DHCPACK(B)      PUNT:RECEIVED
2023/09/28 14:54:01.877  0006.F601.CD43   255.255.255.255 202  DHCPACK(B)      PUNT:TO_DHCPSN
```

## تصحيح الأخطاء الإضافية

```
debug ip dhcp server packet detail
debug ip dhcp server packet
debug ip dhcp server events
debug ip dhcp snooping packet
debug dhcp detail
```

---



تحذير: توخ الحذر عند تشغيل تصحيح الأخطاء!

---

## معلومات ذات صلة

- تنفيذ سياسة توجيه BGP EVPN على محولات Catalyst 9000 Series Switches
- تنفيذ تجزئة تغشية BGP EVPN المحمية على محولات Catalyst 9000 Series Switches
- تشغيل التطفل على بروتوكول DHCP واستكشاف أخطائه وإصلاحها على محولات Catalyst 9000 Switches

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).