فهم إدخالات Catalyst 6500 S2T CEF

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
معلومات أساسية
الرسم التخطيطي للشبكة
تحديد إدخالات CEF عبر محركات إعادة التوجيه الموزعة
حذف إدخالات CEF
إضافة إدخال CEF
إضافة إدخالات لجداول توجيه VRF وحذفها

المقدمة

يصف هذه الوثيقة كيف cisco مادة حافزة 6500 مع مشرف Sup2T برمجية (cisco Express Forwarding) CEF مدخل يشكل على cisco ios برمجية في الخط جهاز يستعمل أن يحقق ربط forwarding.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- إعادة التوجيه السريع Cisco Express Forwarding ((CEF)
- المحولات Cisco Catalyst 6500 Series Switches
- بطاقة التحويل الموزع Cisco Distributed Forwarding Card (DFC)

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات المكونات المادية والبرامج التالية:

- بطاقة الخط Cisco Catalyst 6500 WS-X6848-GE-TX (with DFC4).
- Cisco Catalyst 6500 مع Supervisor 2T على IOS، الإصدار 15.2.1SY5

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

يتم إستخدام آلية تحويل CEF كطبقة 3 من قبل معظم محولات Cisco متعددة الطبقات.من الضروري لمهندسي الشبكات فهم كيفية عمل CEF لاستكشاف أخطاء الشبكة وإصلاحها أو فقد الحزم أو سيناريوهات تأخير الحزم بشكل يومي.

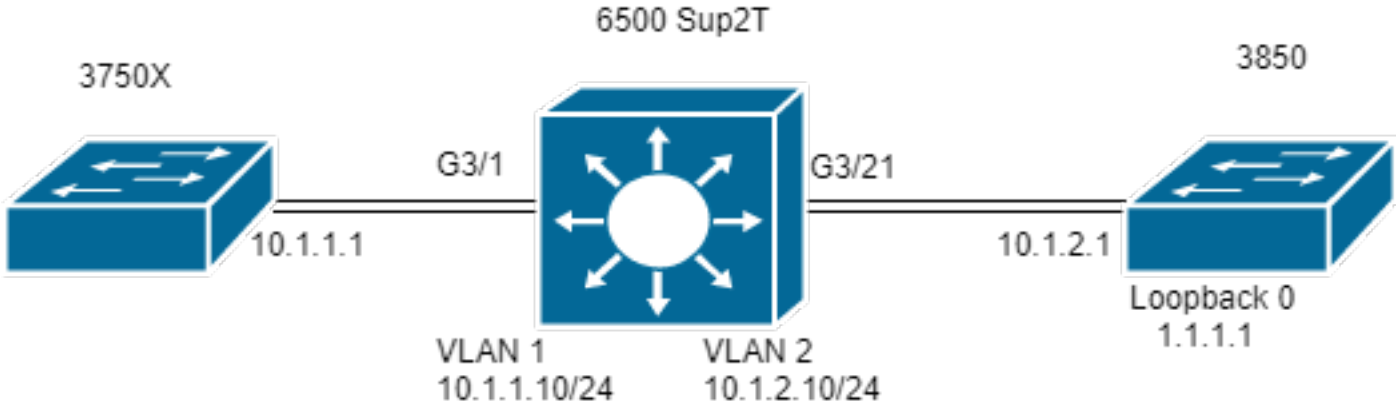
يتم نشر المشرف Sup2T في الوضع المستقل أو VSS حاليا بواسطة العديد من شبكات المؤسسات كمحول أساسي، ويجمع عمليا جميع أجهزة التوجيه أو التحويل الأخرى. وهذا يعني أيضا إعادة توجيه معظم حركة المرور بين المجالات ودخلها من أجل تسليم الحزم بنجاح إلى وجهاتها. لتحقيق ذلك، يجب أن يحتوي Sup2T على معلومات التوجيه المناسبة التي يتم التعرف عليها بشكل ثابت أو ديناميكي عبر بروتوكولات التوجيه.

في هيكل قابل للإضافة وحدات أخرى، قد توجد محركات إعادة توجيه متعددة إلى جانب محركات المشرف. تتضمن بالفعل بطاقات خط معينة (وخاصة بطاقات الجيل الجديد مثل C6800-32P10G) محرك إعادة التوجيه الخاص بها من أجل تحسين أداء تحويل الحزم، ويتم تنفيذ البحث عن إدخالات إعادة التوجيه السريع محليا وبسبب أفضل توزيع للموارد لحركة المرور التي تجمع عبر بطاقات الخط المختلفة.تعرف هذه بطاقات إعادة التوجيه الموزعة (DFCs).

قد يفشل تخصيص إدخالات إعادة التوجيه السريع (CEF) هذه المشتركة عبر جميع محركات إعادة التوجيه في الأجهزة لأسباب متعددة، من حالة عيب في البرنامج واستنفاد الموارد إلى شروط وحدة المعالجة المركزية العالية ومنع المحول من الحصول على وقت كاف لتحديث جميع الإدخالات، قد يتسبب ذلك في سلسلة من الأحداث غير المرغوب فيها.

الرسم التخطيطي للشبكة

الشبكة:




```
Switch#show module 3
---------------------- ---------------------------- Mod Ports Card Type Model Serial No. --- --
--- ---------------------------------------- ------------------ ----------- 3 48 CEF720 48 port
10/100/1000mb Ethernet WS-X6848-GE-TX SAL2003X5AH ---- ---------------------------- -------------
----- ----------- ------- ------- 3 Distributed Forwarding Card WS-F6K-DFC4-A SAL2003X5AH 1.4 Ok
```

تحديد إدخالات CEF عبر محركات إعادة التوجيه الموزعة

في المخطط، تم تثبيت محول 6506 مستقل مشرف 2T بالإضافة إلى بطاقة خط WS-6848-GE-TX مع DFC في slot 3. المضيف 3750X المتصل ببطاقة الخط من خلال المنفذ G3/1 يرسل حركة مرور إلى عنوان الاسترجاع 0 الخاص ب 3850 1.1.1.

ل هذا، يتلقى 3750X طريق ساكن استاتيكي إلى عنوان IP 1.1.1.1 من خلال الخطوة التالية 10.1.1.10 أي ال SVI من VLAN 1 في ال Sup2T مفتاح. يحتاج المحول Sup2T switch إلى توجيه حركة المرور هذه إلى المحول 3850 switch القائم في إدخال مسار ثابت ل IP 1.1.1.1/32 عبر الخطوة التالية 10.1.2.1 والتي هي الواجهة 3850 المتصلة ب Sup2T في VLAN 2.

```
MXC.CALO.3750X#show ip route | inc 1.1.1.1
S 1.1.1.1 [1/0] via 10.1.1.10
```

```
MXC.CALO.Sup2T#show ip route | inc 1.1.1.1
S 1.1.1.1 [1/0] via 10.1.2.1
```

```
CALO.MXC.3850#show ip route | inc 1.1.1.1
C 1.1.1.1 is directly connected, Loopback1
```

كن على علم بأن كلا من المحولين 3750X و 3850 يتم توصيلهما بالمحول 6500 من خلال بطاقة الخط نفسها، وذلك لتحقيق البساطة. وهذا يعني أنه يتم البحث عن حركة المرور محليا وإعادة توجيهها محليا أيضا.

تجمع الحزمة Sup2T مفتاح عبر Gi3/1، أخيرا يصل إلى محرك إعادة التوجيه (بما أن هذا هو DFC). يحلل محرك إعادة التوجيه حقل عنوان IP للوجهة في هذه الحزمة والبحث عبر إدخالات CEF المبرمجة لأفضل تطابق (القناع الأطول).

بما أن هذه بطاقة DFC، فإنها تعني أنها تحتوي على إدخالات التحكم في الوصول (CEF) الخاصة بها وللتحقق من صحتها، فمن الضروري أن يتم إرفاقها إلى بطاقة الخط باستخدام الأمر **attach [dec] أو attach switch [1-2] mod [dec]** ل VSS.

الآن، أنت موفق كنت في ال DFC رسالة، أمر **عرض منصة جاز cef** أو **أبدت منصة جاز cef vpn 0** يرجع كل CEF مدخل برمجية ل عام تحشد طاولة (VPN 0/ ما من VRF).

بما أن الهدف هو البادئة 1.1.1.1/32 أنت تستخدم الأمر **show platform hardware cef vpn 0 lookup 1.1.1.1**. يرجع الأمر أفضل تطابق للبادئة 1.1.1.1 والبادئة التي يستخدمها إعادة توجيه حركة المرور:

```
MXC.CALO.Sup2T#attach 3
Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C^C" to end this session

MXC.CALO.Sup2T-dfc3#show platform hardware cef vpn 0
Codes: decap - Decapsulation, + - Push Label
Index Prefix Adjacency
32 0.0.0.0/32 receive
33 255.255.255.255/32 receive
34 10.1.85.254/32 glean
35 10.1.85.5/32 receive
36 10.1.86.5/32 receive
[snip...]

MXC.CALO.Sup2T-dfc3#show platform hardware cef vpn 0 lookup 1.1.1.1
Codes: decap - Decapsulation, + - Push Label
Index Prefix Adjacency
262 1.1.1.1/32 Vl2 ,0c11.678b.f6f7
```

إدخال CEF هناك، تمت برمجته كنتيجة لإدخالات الثابت المبرمج في برنامج IOS عبر الأمر **ip route 1.1.1.1 255.255.255.255.10.1.2.1**.

يمكنك أيضا التحقق من أن هذا الإدخال يحصل على عمليات الوصول وأن حركة المرور تتم إعادة توجيهها مع هذا الإدخال عبر الأوامر **show platform hardware cef 1.1.1 detail** التي ترجع إدخال التجاوز:

```
MXC.CALO.Sup2T-dfc3#show platform hardware cef 1.1.1.1 detail
Codes: M - mask entry, V - value entry, A - adjacency index, NR- no_route bit
LS - load sharing count, RI - router_ip bit, DF: default bit
CP - copy_to_cpu bit, AS: dest_AS_number, DGTv - dgt_valid bit
DGT: dgt/others value

Format:IPV4 (valid class vpn prefix)
M(262 ): 1 F 2FFF 255.255.255.255
V(262 ): 1 0 0 1.1.1.1
(A:114689, LS:0, NR:0, RI:0, DF:0 CP:0 DGTv:1, DGT:0)
```

أخيرا، يظهر إدخال التجاوز كيفية إعادة كتابة الحزمة وإذا كان قد تمت إعادة كتابة حركة المرور بواسطة إدخال التجاوز هذا:

```
MXC.CALO.Sup2T-dfc3#show platform hardware cef adjacencies entry 114689 detail

RIT fields: The entry has a Layer2 Format
_____________________________________________________
|decr_ttl = YES | pipe_ttl = 0 | utos = 0
|_________________|_________________|___________________
|l2_fwd = 0 | rmac = 0 | ccc = L3_REWRITE
|_________________|_________________|___________________
|rm_null_lbl = YES| rm_last_lbl = YES| pv = 0
|_________________|_________________|___________________
|add_shim_hdr= NO | rec_findex = N/A | rec_shim_op = N/A
|_________________|_________________|___________________
|rec_dti_type = N/A | rec_data = N/A
|_____________________________________|___________________
|modify_smac = YES| modify_dmac = YES| egress_mcast = NO
|_____________________________________|___________________
|ip_to_mac = NO
|_____________________________________________________
|dest_mac = 0c11.678b.f6f7 | src_mac = d8b1.902c.9680
```

```
|_____________________________|_________________________________
|
Statistics: Packet = 642
Bytes = 75756                    <<<<
```

Dest_mac وsrc_mac هما قيمتا الاهتمام الرئيسي، والللتان تشيران إلى رؤوس L2 الجديدة التي يتم كتابتها لهذه الحزمة. غاية {upper}mac address 0c11.678b.f6f7 وه 10.1.2.1 أي ال 3850 (الخطوة التالية أن تصل إلى 1.1.1.1):

```
MXC.CALO.Sup2T#show ip arp 10.1.2.1
Protocol Address Age (min) Hardware Addr Type Interface
Internet 10.1.2.1 30 0c11.678b.f6f7 ARPA Vlan2
```

أيضا، يظهر حقل **الإحصائيات** أن حركة المرور تضرب إدخال التجاوز هذا بالفعل ويتم إعادة كتابة رؤوس L2 وفقا لذلك.

حذف إدخالات CEF

يمكن أن يساعدنا حذف إدخالات إعادة التوجيه السريع (CEF) على حذف أي إدخال قد تتم برمجته بشكل غير صحيح (على إدخال تجاوز غير صحيح على سبيل المثال) أو حتى الأغراض التدريبي. كما يوفر طريقة لتعديل مسار توجيه.

لحذف إدخال CEF، يلزمك أن تفهم أن إدخالات CEF مبرمجة بشكل تسلسلي ولها فهرس أجهزة معين، على سبيل المثال:

MXC.CALO.SUP2T-dfc3#show platform hardware cef vpn 0

الأكواد: إزالة الكبسلة، + - تسمية الدفع

```
MXC.CALO.Sup2T-dfc3#show platform hardware cef vpn 0
...
Index Prefix Adjacency 259 10.1.2.255/32 receive 260 10.1.1.1/32 Vl1 ,a0ec.f930.3f40 261
10.1.2.1/32 Vl2 ,0c11.678b.f6f7 262 1.1.1.1/32 Vl2 ,0c11.678b.f6f7    <<<< Our CEF entry of
interest has a HW index of 262.
...
```

فهرس الأجهزة هذا وهو العنصر الأكثر أهمية لحذف إدخال CEF لأنه يستخدم كمرجع. ومع ذلك، ولإجراء أي تغييرات عليه، يجب تحويله إلى معالج برنامج. يمكنك تحقيق ذلك باستخدام الأمر **cef index-conv hw_to_sw [hw index] إختبار منصة عمل الأجهزة**

```
MXC.CALO.Sup2T-dfc3#test platform hardware cef index-conv hw_to_sw 262
hw index: 262 ----> sw handle: 101
```

الآن بعد أن أصبحت تعرف مقبض البرنامج، أنت يستطيع باشرت مع ال CEF مدخل حذف مع أمر **cef v4-delete [sw handle] قناع [قناع طول] VPN [dec] إختبار منصة جهاز**

```
MXC.CALO.s2TVSS-sw2-dfc3#test platform hardware cef v4-delete 101 mask 32 vpn 0
test_ipv4_delete: done.
```

ملاحظة: قيمة طول القناع هي 32 نظرا لأنه مسار محدد للمضيف (1.1.1.1/32)

تم حذف إدخال CEF الآن:

```
MXC.CALO.Sup2T-dfc3#show platform hard cef vpn 0 1.1.1.1
Codes: decap - Decapsulation, + - Push Label
Index Prefix Adjacency
```

```
MXC.CALO.Sup2T-dfc3#show platform hard cef vpn 0
[snip...]
259 10.1.2.255/32 receive
260 10.1.1.1/32 Vl1 ,a0ec.f930.3f40
261 10.1.2.1/32 Vl2 ,0c11.678b.f6f7
```

```
288 224.0.0.0/24 receive              <<<<<<< Index 262 no longer exists in the CEF entries.
289 10.1.85.0/24 glean
```

لاحظ أنه تم تنفيذ الأمر **test platform hardware cef vpn 0** تحت موجه أمر DFC. بهذه الطريقة، تمت إزالة إدخال CEF من جدول CEF الخاص ب DFC وليس من المشرف، يجب أن تكون حريصا حقا على محرك إعادة التوجيه الذي تم إزالة الإدخالات منه.

يؤدي أي تغيير في حركة المرور إلى خطر عدم الرؤية (في حالة الاختبار المعملي)، قد يكون ذلك بسبب إصابة إدخال CEF آخر. ضع في اعتبارك أن تطابق دائما أكثر قناع دقة (أطول قناع). في هذا المختبر، تصل إلى:

```
MXC.CALO.Sup2T-dfc3#show plat hard cef vpn 0 lookup 1.1.1.1
Codes: decap - Decapsulation, + - Push Label
Index Prefix Adjacency
262048 0.0.0.0/0 glean
```

فماذا يفعل هذا الإدخال فعلا بالحزمة؟:

```
MXC.CALO.Sup2T-dfc3#show platform hardware cef adjacencies entry 262048
RIT fields: The entry has a Recirc. Format
_____________________________________________________ |decr_ttl=NO | l2_fwd=NO | ccc = 6 |
add_shim_hdr = YES |_____________|_____________|_________|_____________________ |rc_fidx=0 |
rc_shimop=1 | rc_dti_type=4 | rc_data = 0x10B
|_____________|_____________|_________________|_______________ Statistics: Packets = 2163 Bytes =
255234
```

Taken from a CPU packet capture using Catlayst 6500 NETDR tool. For NETDR capture tool details refer to: [Catalyst 6500 Series Switches Netdr Tool for CPU-Bound Packet Captures]

```
------- dump of incoming inband packet -------
l2idb Po1, l3idb Vl1, routine inband_process_rx_packet, timestamp 01:00:17.841
dbus info: src_vlan 0x1(1), src_indx 0xB40(2880), len 0x82(130)
bpdu 0, index_dir 0, flood 0, dont_lrn 0, dest_indx 0x5FA4(24484), CoS 0
cap1 0, cap2 0
78020800 00018400 0B400100 82000000 1E000464 2E000004 00000010 5FA45BDD
destmac D8.B1.90.2C.96.80, srcmac A0.EC.F9.30.3F.40, shim ethertype CCF0
earl 8 shim header IS present:
version 0, control 64(0x40), lif 1(0x1), mark_enable 1,
feature_index 0, group_id 0(0x0), acos 0(0x0),
ttl 14, dti 4, dti_value 267(0x10B)
10000028 00038080 010B
ethertype 0800
protocol ip: version 0x04, hlen 0x05, tos 0x00, totlen 100, identifier 51573
df 0, mf 0, fo 0, ttl 255, src 10.1.1.1, dst 1.1.1.1
icmp type 8, code 0


------- dump of outgoing inband packet -------
l2idb NULL, l3idb Vl2, routine etsec_tx_pak, timestamp 01:03:56.989
dbus info: src_vlan 0x2(2), src_indx 0x380(896), len 0x82(130)
bpdu 0, index_dir 0, flood 0, dont_lrn 0, dest_indx 0x0(0), CoS 0
cap1 0, cap2 0
00020000 0002A800 03800000 82000000 00000000 00000000 00000000 00000000
destmac 0C.11.67.8B.F6.F7, srcmac D8.B1.90.2C.96.80, shim ethertype CCF0
earl 8 shim header IS present:
version 0, control 0(0x0), lif 16391(0x4007), mark_enable 0,
feature_index 0, group_id 0(0x0), acos 0(0x0),
ttl 15, dti 0, dti_value 540674(0x84002)
000800E0 0003C008 4002
ethertype 0800
protocol ip: version 0x04, hlen 0x05, tos 0x00, totlen 100, identifier 50407
df 0, mf 0, fo 0, ttl 254, src 10.1.1.1, dst 1.1.1.1
icmp type 8, code 0
```

الآن، تم إعادة حساب كل حركة المرور ذات الوجهة 1.1.1.1 التي تدخل عبر بطاقة الخط 3 باستخدام رأس الرقاقة وتم تثبيتها على وحدة المعالجة المركزية. في بعض الأحيان، يدل من إدخال CEF هذا، يتم ترقية إدخال **0.0.0/0** لرواتج بتخزين **الإفتراضي** وفي الشيء نفسه تمامًا.

> **ملاحظة**: قم بتقييم إدخالات CEF التي تمت إزالتها. قد يحدث إستخدام عال لوحدة المعالجة المركزية (CPU) بسبب هذا. بشكل عام، يتم تكوين مسار افتراضي 0.0.0.0/0 ويتم إعادة توجيه حركة مرور البيانات استنادا إليه (وبسبب فقدان الحزمة).

إضافة إدخال CEF

عند إضافة إدخال CEF، في معظم الحالات، يحل أي مشكلة في البرمجة الخاطئة تتسبب في فقدان الحزمة أو تأخر الحزمة أو إستخدام عال لوحدة المعالجة المركزية. تعرف كيفية تثبيت إدخالات إعادة التوجيه السريع (CEF) في الأجهزة، ال تفرق القدرة على تصحيح الإدخال الذي تمت برمجته، وتوجيهها إلى واجهة مختلفة تمامًا أو الخطوة التالية، بشكل غير صحيح فحسب، بل أيضا عالجة أي إعادة توجيه حزم من إعادة حساب الحزمة، وتوجيهها إلى واجهة مختلفة تمامًا أو الخطوة التالية. إدخال تغيير أي أو تكوين طبق وضع القرار، مع إعادة تحميل المربع، دون إعادة حساب الحزمة، أو إلى ذلك. كل هذه الأشياء تجعل إدخال CEF المذكور في القسم السابق (كما فعلت مع إزالة إدخال CEF) أيضا. (وضع التكوين إلى دون الدخول من إضافة إجراء الكمي CEF).

أساسا، هناك حالتان هنا، عندما يكون لديك إدخال ARP صالح إلى الخطوة التالية، في هذه الحالة 10.1.2.1 وعندما لا تفعل ذلك (لأي سبب). الوضع الثاني يجبرك على إنشاء إدخال ARP صالح (عبر ARP الثابت):

الخطوة 1. هناك مدخل ARP في المفاتح ل 10.1.2.1 أي يكون الخطوة التالية ل 1.1.1.1.

```
MXC.CALO.Sup2T#show ip arp 10.1.2.1
Protocol Address Age (min) Hardware Addr Type Interface
Internet 10.1.2.1 2 0c11.678b.f6f7 ARPA Vlan2

MXC.CALO.Sup2T#show ip route | inc 1.1.1.1
S 1.1.1.1 [1/0] via 10.1.2.1
```

تتم برمجة إدخال ARP كمسار مضيف (/32) في جدول CEF:

```
MXC.CALO.Sup2T-dfc3#show plat hard cef vpn 0 look 10.1.2.1
Codes: decap - Decapsulation, + - Push Label
Index Prefix Adjacency
53 10.1.2.1/32 Vl2 ,0c11.678b.f6f7
```

And of course, there is an index for this which again will tell us how a packet should be rewritten to reach 10.1.2.1:

```
MXC.CALO.Sup2T-sw2-dfc3#show plat hard cef vpn 0 10.1.2.1 detail
[snip...]
Format:IPV4 (valid class vpn prefix)
M(53 ): 1 F 2FFF 255.255.255.255
V(53 ): 1 0 0 10.1.2.1
(A:114689, LS:0, NR:0, RI:0, DF:0 CP:0 DGTv:1, DGT:0)
```

Wait, wasn't 114689 adj entry the same used for 1.1.1.1?:

```
MXC.CALO.Sup2T-sw2-dfc3#show plat hard cef 1.1.1.1 de
[snip...]
Format:IPV4 (valid class vpn prefix)
M(54 ): 1 F 2FFF 255.255.255.255
V(54 ): 1 0 0 1.1.1.1
(A:114689, LS:0, NR:0, RI:0, DF:0 CP:0 DGTv:1, DGT:0)
```

يجب إعادة توجيه أي حزمة تحتوي على أي عنوان IP للوجهة لها نفس إرتباط البيانات في الخطوة التالية من خلال نفس الواجهة وإعادة كتابتها باستخدام نفس رؤوس L2.

على الرغم من أن هذا قد يبدو واضحا للغاية في البداية، إلا أنه في الواقع هو العنصر الأكثر أهمية لإضافة إدخال CEF، إلا أنك تحتاج إلى إخباره بكيفية إعادة كتابة الحزمة باستخدام إدخال تجاوز CEF محدد.

الخطوة 2. الآن، لنفترض أنه لا يوجد إدخال ARP تم إنشاؤه تلقائيا له، لذلك أنت تحتاج أن يخلق ARP مدخل ساكن إستاتيكي.

إلى 10.1.2.1، لذلك هو أرسلت خطوة تالية للبادئة أن يكون استعملت عنوان من الأداة أن يعرف ال MAC عنوان أن تحتاج، هذا أتمت in order to
0c11.678b.f6f7. إن هناك يكون بالفعل {upper}mac address مدخل في **العرض كام عنوان طاولة عنوان 0c11.678b.f6f7** أم يتنتج أن يكون جيد، إن لم يكن
بعد ذلك أنت تحتاج أن يخلق ساكن إستاتيكي كام مدخل:

```
MXC.CALO.Sup2T(config)#mac address-table static 0c11.678b.f6f7 vlan 2 int Gi3/21
Displaying entries from DFC switch [2] linecard [3]:

vlan mac address type learn age ports
----+----+---------------+-------+-----+----------+----------------------------
2 0c11.678b.f6f7 static No - Gi3/21
```

الخطوة 3. أخيرا، يحتاج إدخال ARP ساكن إستاتيكي أن يكون خلق تم in order to برمجت إدخال CEF:

```
MXC.CALO.Sup2T(config)#arp 10.1.2.1 0c11.678b.f6f7 arpa    <<< Static ARP configuration

MXC.CALO.Sup2T#show ip arp 10.1.2.1
Protocol Address Age (min) Hardware Addr Type Interface
Internet 10.1.2.1 - 0c11.678b.f6f7 ARPA                  <<< Now the static ARP entry is
complete

// Attaching to DFC3...
MXC.CALO.Sup2T-sw2-dfc3#show plat hard cef 10.1.2.1 detail
[snip...]
Format:IPV4 (valid class vpn prefix)
M(53 ): 1 F 2FFF 255.255.255.255
V(53 ): 1 0 0 10.1.2.1
(A:114689, LS:0, NR:0, RI:0, DF:0 CP:0 DGTv:1, DGT:0)

The ARP entry exist in CEF table for DFC3. Same Adjacency Index result as before...
```

الآن بعد أن تفهم ام تفعله إدخالات التجاوز هذه، يمكنك المتابعة أخيرا إضافة إدخال CEF. في القسم الأخير، تم حذف إدخال CEF للبادئة 1.1.1.1/32
من خلال الأمر **test platform hardware cef v4-delete**. الآن، قم بإضافة أمر آخر من خلال الأمر **إختبار منصة عمل الأجهزة cef v4-insert [prefix] [طول القناع] VPN [رقم VPN] التجاوز [فهرس التجاوز]**

للتحقق من ذلك، أستخدم الأمر **test platform hardware cef v4-insert 1.1.1 32 vpn 0 التجاوز 114689**. تمت إضافة الإدخال أمر آخر في جدول DFC CEF:

```
MXC.CALO.Sup2T-sw2-dfc3#test platform hardware cef v4-insert 1.1.1.1 32 vpn 0 adjacency 114689
test_ipv4_insert: done: sw_index = 42

MXC.CALO.Sup2T-sw2-dfc3#show plat hard cef vpn 0 1.1.1.1
Codes: decap - Decapsulation, + - Push Label
Index Prefix Adjacency
54 1.1.1.1/32 Vl2 ,0c11.678b.f6f7

Ping from the 3750X to Loopback 0 is successful and HW forwarded by 6500 DFC.

MXC.CALO.Sup2T-sw2-dfc3#show platform hard cef adj entry 114689

Index: 114689 -- Valid entry (valid = 1) --

RIT fields: The entry has a Layer2 Format
_____________________________________________________
|decr_ttl=YES | l2_fwd=NO | ccc = 4 | add_shim_hdr = NO
|_____________|____________|_________|___________________

Statistics: Packets = 684
Bytes = 80712


// Logs in 3850
CALO.MXC.385024XU#show logging [snip...] *Jan 23 05:59:56.911: ICMP: echo reply sent, src
1.1.1.1, dst 10.1.1.1, topology BASE, dscp 0 topoid 0 *Jan 23 05:59:57.378: ICMP: echo reply
```

```
sent, src 1.1.1.1, dst 10.1.1.1, topology BASE, dscp 0 topoid 0 *Jan 23 05:59:57.390: ICMP: echo
reply sent, src 1.1.1.1, dst 10.1.1.1, topology BASE, dscp 0 topoid 0
```

إضافة إدخالات لجداول توجيه VRF وحذفها

من خلال التكوين الذي تم إجراؤه من جميع الخطوات السابقة، تم فرض سلسلة **VPN 0** في أوامر **show platform hardware cef**. حتى إذا بدا غير ضروري تتم إضافة إدخالات لجدول التوجيه العام **VPN 0**، فإن هذه هي الطريقة الوحيدة لضمان أن الإدخالات تتم بشكل افتراضي بواسطة رمز VPN الأمامي. وهو CEF 1.1.1.1/32. إدخال حذفه وإضافته من جدول توجيه معين (VRFs)، من خلال المستند الذي تم إضافته وحذفه من الجدول. فمن المرجح أن توجد بيانات معينة في ذاكرة الوصول العشوائي (VRF) مختلفة (أي. 10.x.x.x) كما يمكن أن يؤدي حذف إدخال CEF وأ إضافته وأ تعديله لمعرفة فئة المورد (VRF) غير صحيح إلى إحداث تأثير سلبي.

إحذف إدخال CEF بيانات 1.1.1.1/32 ل VRF **TEST_VRF**. للحصول على وصف تفصيلي لإدخالات CEF الإضافية، ارجع إلى قسم **إضافة إدخال CEF في هذه المستند.**

in order to أضف ال VRF، غيرت SVIs في 6500 مفاتح إلى ال VRF مقترح مع أمر **ip vrf forwarding [vrf-name]** أو أخيرا أضف ال نفسه ساكن إستاتيكي في **ديناميكي TEST_VRF** طاولة:

```
MXC.CALO.Sup2T(config)#ip vrf TEST_VRF
MXC.CALO.Sup2T(config-vrf)#int vlan 1
MXC.CALO.Sup2T(config-if)#ip vrf forwarding TEST_VRF
% Interface Vlan1 IPv4 disabled and address(es) removed due to enabling VRF TEST_VRF
MXC.CALO.Sup2T(config-if)#ip add 10.1.1.10 255.255.255.0
MXC.CALO.Sup2T(config-if)#int vlan 2
MXC.CALO.Sup2T(config-if)#ip vrf forwarding TEST_VRF
% Interface Vlan2 IPv4 disabled and address(es) removed due to enabling VRF TEST_VRF
MXC.CALO.Sup2T(config-if)#ip add 10.1.2.10 255.255.255.0
MXC.CALO.Sup2T(config)#ip route vrf TEST_VRF 1.1.1.1 255.255.255.255 10.1.2.1

MXC.CALO.Sup2T#show ip vrf
Name Default RD Interfaces
TEST_VRF <not set> Vl1
Vl2
```

وتتم برمجة شبكات VRF بشكل تسلسلي أيضا. هذا كان أول VRF في المفاتح (ام من آخر) رمز تشغيل الأمر. قم بتنت 1. هذا VRF مثال سوف تكون ل رقم VPN لذلك (اقل تسلسل شكل VRF) للتحقق من صحة ذلك **show platform hardware cef vpn 1**:

```
MXC.CALO.Sup2T-sw2-dfc3#show plat hard cef vpn 1
Codes: decap - Decapsulation, + - Push Label
Index Prefix Adjacency
34 10.1.1.10/32 receive
35 10.1.1.0/32 receive
36 10.1.1.255/32 receive
38 10.1.2.10/32 receive
43 10.1.2.0/32 receive
44 10.1.2.255/32 receive
53 10.1.2.1/32 Vl2 ,0c11.678b.f6f7
54 1.1.1.1/32 Vl2 ,0c11.678b.f6f7
[snip...]
```

However, usually, switches have hundred or thousands of VRFs and just count them in the 'show ip vrf' command output would be quite difficult. In order to know which VPN number is assigned to a VRF we will run the command "show platform hardware cef vrf [VRF name] [prefix] detail", it will return the actual vpn number for that VRF:

```
Format:IPV4 (valid class vpn prefix)
M(54 ): 1  F 2FFF 255.255.255.255
V(54 ): 1  0  1    1.1.1.1                              <<<<<<<<<<< The number in red
determines the VPN this prefix belongs to.
(A:114689, LS:0, NR:0, RI:0, DF:0 CP:0 DGTv:1, DGT:0)
```

من المهم معرفة رقم VPN الفعلي وفهرس البرامج لهذا الإدخال حتى يمكنك المتابعة لحذفه أو إضافته من/إلى مثيل VRF هذا:

```
MXC.CALO.Sup2T-sw2-dfc3#test platform hardware cef index-conv hw_to_sw 54
hw index: 54 ----> sw handle: 42

MXC.CALO.Sup2T-sw2-dfc3#test platform hardware cef v4-delete 42 mask 32 vpn 1
test_ipv4_delete: done.

Result:

MXC.CALO.Sup2T-sw2-dfc3#show platform hardware cef vpn 1 lookup 1.1.1.1
Codes: decap - Decapsulation, + - Push Label
Index Prefix Adjacency
262049 0.0.0.0/0 drop

Traffic is now getting punted, and the effects are seen in the 3750X pings to 1.1.1.1:

MXC.CALO.3750X#ping 1.1.1.1 repe 5000000
Sending 5000000, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[snip...]

// Packet loss
```

ضع في الاعتبار أنه في شبكة إنتاج، يتم تعرض فقد الحزمة وتقطع الصوت أو الفيديو التالف بسبب حالة إدخالات CEF هذه. لذلك، يوصى بإجراء هذه الاختبارات في إطار الصيانة.

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 دائماً إلى المستند الإنجليزي الأصلي (الرابط متوفر).