مثال تكوين ميزة Catalyst 4500 Series Switches Wireshark

المحتويات

المقدمة

يصف هذا وثيقة كيف أن يشكل ال Wireshark سمة ل cisco مادة حفازة 4500 sery مفتاح.

المتطلبات الأساسية

المتطلبات

لاستخدام ميزة Wireshark، يجب عليك استيفاء الشروط التالية:

- يجب أن يستخدم النظام محول Cisco Catalyst 4500 Series Switch.
- يجب أن يقوم المحول بتشغيل Supervisor Engine 7-E (محرك المشرف 6 غير مدعوم في الوقت الحالي).
- يجب أن تحتوي الميزة على قاعدة IP وخدمات المؤسسة (قاعدة LAN غير مدعومة في الوقت الحالي).
- لا يمكن أن تحتوي وحدة المعالجة المركزية (CPU) للمحول على حالة إستخدام عالية، حيث إن ميزة Wireshark هي حزم معينة تستخدم وحدة المعالجة المركزية (CPU) وتنقل البرامج بشكل مكثف في عملية الالتقاط.

المكونات المستخدمة

أسست المعلومة في هذا وثيقة على cisco مادة حفازة 4500 sery مفتاح أن يركض مشرف محرك E-7.

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

أمر.

معلومات أساسية

تحتوي محولات Cisco Catalyst 4500 Series switches التي تعمل بنظام التشغيل Supervisor Engine 7-E على وظيفة مدمجة جديدة باستخدام الإصدارات 3.3(0) / 151.1 أو الأحدث من Cisco IOS XE-؟. لهذه الميزة المدمجة في Wireshark القدرة على التقاط الحزم بطريقة تستبدل الاستخدام التقليدي لمحلل منفذ المحول (SPAN) بجهاز كمبيوتر شخصي مرفق من أجل التقاط الحزم في سيناريو أستكشاف الأخطاء وإصلاحها.

التكوين

يعمل هذا القسم كدليل بداية سريعة لبدء الالتقاط. المعلومات المتوفرة عامة جدا، ويجب عليك تنفيذ إعدادات المرشحات والمخزن المؤقت حسب الحاجة للحد من الالتقاط المفرط للحزم إذا عملت في شبكة إنتاج.

أتمت هذا steps in order to شكلت ال wireshark سمة:

1. دققت أن أنت تستوفي الشرط in order to ساندت الالتقاط. (مرجع **المتطلبات** لمزيد من التفاصيل.) دخلت هذا أمر ودققت الإنتاج:

```
4500TEST#show version

Cisco IOS Software, IOS-XE Software, Catalyst 4500 L3 Switch Software
  (cat4500e-UNIVERSAL-M), Version 03.03.00.SG RELEASE SOFTWARE (fc3)

<output omitted>

'License Information for 'WS-X45-SUP7-E
License Level: entservices   Type: Permanent
Next reboot license Level: entservices

(cisco WS-C4507R+E (MPC8572) processor (revision 8
.with 2097152K/20480K bytes of memory

Processor board ID FOX1512GWG1

MPC8572 CPU at 1.5GHz, Supervisor 7

<output omitted>

4500TEST#show proc cpu history

:History information for system

888844444222222222222222333334444422222222222222255555222222
                                                          100
                                                          90
                                                          80
                                                          70
                                                          60
                                                          50
                                                          40
                                                          30
                                                          20
****                                                    **** 10
5....5.....4.....4.....3.....3.....2.....2.....1.....1.....5.....0
```

```
5    0    5    0    5    0    5    0    5    0

(CPU% per second (last 60 seconds
```

2. قبض حركة مرور في TX/RX إتجاه من ميناء **gig2/26** في هذا المثال. تخزين ملف الالتقاط على bootflash في **PCAP** تنسيق الملف للمراجعة من كمبيوتر محلي، إذا لزم الأمر:**ملاحظة**: تأكد من تنفيذ التكوين من وضع **EXEC للمستخدم**، وليس **وضع التكوين العام**.

```
4500TEST#monitor capture MYCAP interface g2/26 both
4500TEST#monitor capture file bootflash:MYCAP.pcap
4500TEST#monitor capture MYCAP match any start

.Sep 13 15:24:32.012: %BUFCAP-6-ENABLE: Capture Point MYCAP enabled*
```

3. على قبض هذا كل حركة مرور مدخل ومخرج على ميناء **ع 26/2**. هو أيضا يملأ الملف بسرعة جدا بحركة مرور غير مفيدة في حالة إنتاج، إلا إذا قمت بتعيين الإتجاه وتطبيق مرشحات الالتقاط لتضييق نطاق حركة المرور التي يتم التقاطها. دخلت هذا أمر in order to طبقت مرشح:

```
"4500TEST#monitor capture MYCAP start capture-filter "icmp
```

ملاحظة: يضمن ذلك أنك تقوم فقط بالتقاط حركة مرور بروتوكول رسائل التحكم في الإنترنت (ICMP) في ملف الالتقاط الخاص بك.

4. بمجرد أن ينتهي وقت التقاط الملف، أو يقوم بتعبئة الحصة النسبية للحجم، تتلقى هذه الرسالة:

```
:Sep 13 15:25:07.933: %BUFCAP-6-DISABLE_ASYNC*
Capture Point MYCAP disabled. Reason : Wireshark session ended
```

أدخل هذا الأمر لإيقاف الالتقاط يدويا:

```
4500TEST#monitor capture MYCAP stop
```

5. يمكنك عرض الالتقاط من واجهة سطر الأوامر. دخلت هذا أمر in order to شاهدت الربط:

```
4500TEST#show monitor capture file bootflash:MYCAP.pcap

                d3:ca:25:9c:c9 -> 01:00:0c:cc:cc:cc CDP:44 0.000000   1
                 Device ID: 4500TEST  Port ID: GigabitEthernet2/26
                e7:c1:6a:18 -> 01:80:c2:00:00:00 STP:00:19 0.166983   2
Conf. Root = 32768/1/00:19:e7:c1:6a:00  Cost = 0  Port = 0x8018
                e7:c1:6a:18 -> 01:00:0c:cc:cc:cd STP:00:19 0.166983   3
Conf. Root = 32768/1/00:19:e7:c1:6a:00  Cost = 0  Port = 0x8018
(HSRP Hello (state Standby    224.0.0.2 <- 14.1.98.2    1.067989   4
                e7:c1:6a:18 -> 01:80:c2:00:00:00 STP:00:19 2.173987   5
Conf. Root = 32768/1/00:19:e7:c1:6a:00  Cost = 0  Port = 0x8018
```

ملاحظة: يتوفر خيار التفاصيل في النهاية لعرض الحزمة بتنسيق Wireshark. أيضا، التفريغ خيار يتوفر in order to رأيت ال hex قيمة من الربط.

6. يصبح ملف الالتقاط مكبلا إذا كنت لا تستخدم Capture-Filter عندما تبدأ الالتقاط. في هذه الحالة، أستخدم خيار **show-filter** لعرض حركة مرور معينة في العرض. تريد فقط عرض حركة مرور ICMP، وليس بروتوكول موجه الاستعداد السريع (HSRP)، وبروتوكول الشجرة المتفرعة (STP)، وحركة مرور بروتوكول اكتشاف Cisco (CDP) الموضحة في الإخراج السابق. يستخدم عامل تصفية **العرض** نفس تنسيق Wireshark، لذلك يمكنك العثور على الملفات عبر الإنترنت.

```
"4500TEST#show monitor capture file bootflash:MYCAP.pcap display-filter "icmp

     ICMP Echo 172.18.108.26 <- 14.1.98.144  4.936999   17
(ping) request  (id=0x0001, seq(be/le)=0/0, ttl=255)
     ICMP Echo  14.1.98.144 <- 172.18.108.26 4.936999   18
(ping) reply    (id=0x0001, seq(be/le)=0/0, ttl=251)
     ICMP Echo 172.18.108.26 <- 14.1.98.144  4.938007   19
(ping) request  (id=0x0001, seq(be/le)=1/256, ttl=255)
     ICMP Echo  14.1.98.144 <- 172.18.108.26 4.938007   20
(ping) reply    (id=0x0001, seq(be/le)=1/256, ttl=251)
     ICMP Echo 172.18.108.26 <- 14.1.98.144  4.938998   21
(ping) request  (id=0x0001, seq(be/le)=2/512, ttl=255)
     ICMP Echo  14.1.98.144 <- 172.18.108.26 4.938998   22
```

```
(ping) reply    (id=0x0001, seq(be/le)=2/512, ttl=251)
      ICMP Echo 172.18.108.26 <- 14.1.98.144  4.938998   23
(ping) request  (id=0x0001, seq(be/le)=3/768, ttl=255)
      ICMP Echo  14.1.98.144 <- 172.18.108.26 4.940005   24
(ping) reply    (id=0x0001, seq(be/le)=3/768, ttl=251)
      ICMP Echo 172.18.108.26 <- 14.1.98.144  4.942996   25
(ping) request  (id=0x0001, seq(be/le)=4/1024, ttl=255)
      ICMP Echo  14.1.98.144 <- 172.18.108.26 4.942996   26
(ping) reply    (id=0x0001, seq(be/le)=4/1024, ttl=251)
```

7. قم بنقل الملف إلى جهاز محلي، وانظر إلى ملف PCAP كما تفعل مع أي ملف التقاط قياسي آخر. دخلت واحد من هذا أمر in order to أتمت النقل:

```
@4500TEST#copy bootflash: ftp://Username:Password
```

```
:4500TEST#copy bootflash: tftp
```

8. لتنظيف الالتقاط، قم بإزالة التكوين باستخدام الأوامر التالية:

```
4500TEST#no monitor capture MYCAP
4500TEST#show monitor capture MYCAP

<no output>

#4500TEST
```

الإعدادات الإضافية

بشكل افتراضي، حد الحجم لملف الالتقاط هو 100 حزمة، أو 60 ثانية في ملف خطي. لتغيير حد الحجم، أستخدم خيار **الحد** في صياغة التقاط الشاشة:

```
? 4500TEST#monitor cap MYCAP limit

duration       Limit total duration of capture in seconds
packet-length  Limit the packet length to capture
packets        Limit number of packets to capture
```

الحد الأقصى لحجم المخزن المؤقت هو 100 ميغابايت. يتم ضبط هذا، وكذلك إعداد المخزن المؤقت الدائري/الخطي، باستخدام هذا الأمر:

```
? 4500TEST#monitor cap MYCAP buffer

circular  circular buffer
 size      Size of buffer
```

تعد ميزة Wireshark المدمجة أداة فعالة للغاية في حالة إستخدامها بشكل صحيح. فهي توفر الوقت والموارد عند أستكشاف أخطاء الشبكة وإصلاحها. ومع ذلك، عليك توخي الحذر عند إستخدام الميزة، لأنها قد تزيد إستخدام وحدة المعالجة المركزية (CPU) في حالات حركة المرور العالية. لا تقم بتكوين الأداة مطلقا وتركها دون مراقبة.

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

نظرا لقيود الأجهزة، قد تتلقى حزم خارج الترتيب في ملف الالتقاط. وهذا يرجع إلى المخازن المؤقتة المنفصلة المستخدمة لالتقاط حزم الدخول والخروج. إذا كان لديك حزم غير مرتبة في الالتقاط الخاص بك، فقم بتعيين كلا من المخازن المؤقتة **لديك** إلى **الدخول**. هذا يمنع الربط في مخرج من المعالجة قبل المدخل ربط عندما يكون المخزن المؤقت معالج.

إذا ظهرت حزم غير مرتبة، فيوصى بتغيير التكوين من **كلا** الأمرين **إلى** الداخل على كلا الواجهات.

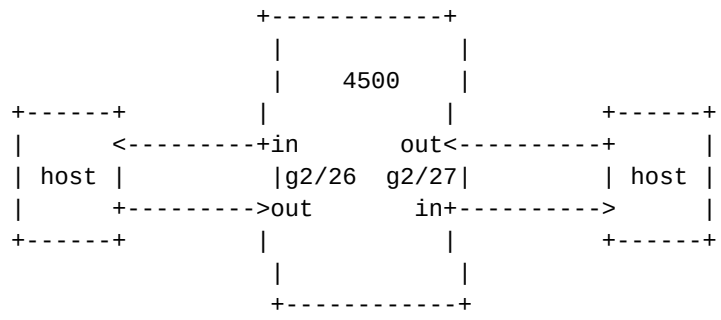
هنا الأمر السابق:

```
4500TEST#monitor capture MYCAP interface g2/26 both
```

قم بتغيير الأمر إلى ما يلي:

```
4500TEST#monitor capture MYCAP interface g2/26 in

4500TEST#monitor capture MYCAP interface g2/27 in
```



معلومات ذات صلة

- [دليل تكوين البرنامج Catalyst 4500 Series Switch Software، إصدار IOS XE 3.3.0SG و IOS 15.1(1)SG - تكوين Wireshark]
- [الدعم التقني والمستندات - Cisco Systems]

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).