أستكشاف أخطاء MAC وإصلاحها/التكرار في محولات Cisco Catalyst Switches

المحتويات

المقدمة

المتطلبات الأساسية

- المتطلبات
- المكونات المستخدمة

معلومات أساسية

ما هو رفرفة ماك؟

إرشادات عامة لاستكشاف الأخطاء وإصلاحها

دراسة الحالة 1

- وصف المشكلة
- المخطط
- خطوات أستكشاف الأخطاء وإصلاحها
- سبب جذري
- قرار

دراسة حالة 2

- وصف المشكلة
- المخطط
- خطوات أستكشاف الأخطاء وإصلاحها
- سبب جذري
- قرار

منع

المقدمة

يصف هذا وثيقة كيف أن يتحرى ال MAC بركة/أنشوطة على cisco مادة حفازة مفتاح.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة أساسية بمفاهيم التحويل الأساسية وفهم بروتوكول الشجرة المتفرعة (STP) وميزاته على محولات Cisco Catalyst.

المكونات المستخدمة

أسست المعلومة في هذا وثيقة على cisco مادة حفازة مفتاح مع كل صيغة (هذا وثيقة ال يقيد إلى أي خاص برمجية أو جهاز صيغة).

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

يعمل هذا المستند كدليل يحدد نهجا منتظما لاستكشاف أخطاء رفرفة MAC وأ التكرار الحلقي وإصلاحها على محولات Cisco Catalyst switches. إن رفرفة/حلقات MAC هي حالات تشويش في الشبكة تنجم عن حالات عدم التناسق في جداول عناوين MAC للمحولات. والا توفر هذه الوثيقة خطوات لتحديد هذه المسائل وحلها فحسب، بل تتضمن أيضا أمثلة عملية من أجل تحسين الفهم.

ما هو رفرفة ماك؟

يظهر رفرفة MAC عندما يستلم مفتاح إطار مع ال نفس MAC مصدر عنوان غير من قارن مختلف من الواحد وه في البداية علمت وه من. هذا يسبب المفتاح أن يرفرف بين ميناء، تحديث ه {upper}mac address طوال مع القارن جديد. قد يتسبب هذا الوضع في عدم إستقرار الشبكة ويؤدي إلى حدوث مشاكل في الأداء.

في محول Cisco، يتم تسجيل رفرفة MAC بشكل خاص كرسالة مماثلة لهذه:

```
"%SW_MATM-4-MACFLAP_NOTIF: Host xxxx.xxxx.xxxx in vlan x is flapping between port (1) and port (2)"
```

في هذا المثال، ماكxxxx.xxxx.xxxxعنوان كان أول علمت على قارن ميناء (1)، بعد ذلك رأيت على قارن ميناء (2)، يسبب رفرفة ماك.

أكثر الأسباب شيوعا لاردادت MAC وه حلقة من الطبقة 2 في الشبكة، غالبا بسبب تكوين خاطئ لبروتوكول الشجرة المتفرعة (STP) أو مشاكل مع الروابط المتكررة. وقد يتضمن السبب الآخر وجود أخطاء في الأجهزة أو أخطاء البرامج أو حتى مشكلات الأمان مثل انتحال عناوين MAC.

يتضمن أستكشاف أخطاء MAC وإصلاحها غالبا تحديد أي حلقات تكرار في الشبكة وحلها، أو التحقق من تكوينات الجهاز، أو تحديث البرامج/البرامج الثابتة للجهاز.

إرشادات عامة لاستكشاف الأخطاء وإصلاحها

- التعرف على رفرفة MAC: ابحث عن السجلات الموجودة في المحول والتي تشير إلى رفرفة MAC. على سبيل المثال، في محول Cisco، تبدو رسالة السجل كما يلي:

```
%SW_MATM-4-MACFLAP_NOTIF: Host [mac_address] in vlan [vlan_id] is flapping between port [port_id_
```

- لاحظ عنوان MAC والواجهات: تعطيك رسالة السجل عنوان MAC الذي يرفرف والواجهات التي يرفرف بينها. لاحظ هذه الأشياء لأنها تساعدك في تحقيقك.
- التحقيق في الواجهات المتأثرة: أستخدم واجهة سطر الأوامر (CLI) الخاصة بالمحول للتحقق من الواجهات المعنية. يمكنك إستخدام أوامر مثلshow interfacesأوshow mac address-tableلترى أي الأجهزة تكون متصلة بالواجهات وأين يتم تعلم عنوان MAC.
- تتبع عنوان MAC الخاص بالرفرفة: MAC يتعلم من خلال X و Y. واحد ميناء يقودنا إلى حيث أن MAC يكون موصل والآخر يقودنا إلى الحلقة. أختر منفذ وابدأ العمل من خلال إستخدامshow mac address-tableالأمر على كل محول من الطبقة 2 في المسار.
- التحقق من حلقات التكرار المادية: انظر إلى مخطط الشبكة الخاصة بك لمعرفة ما إذا كانت هناك أي حلقات تكرار فعلية. يمكن أن يحدث ذلك إذا وجدت مسارات متعددة بين المحولات. إن أسست أنشوطة يكون، أنت ينبغي أعدت شكلت شبكتك in order to أزلت الأنشوطة.
- فحص بروتوكول الشجرة المتفرعة (STP): تم تصميم بروتوكول الشجرة المتفرعة (STP) لمنع حلقات التكرار في شبكتك من خلال حظر مسارات معينة. إذا تم تكوين بروتوكول الشجرة المتفرعة (STP) بشكل غير صحيح، فإنه لا يمنع حلقات التكرار كما يجب أن تكون. أستخدم أوامر مثلshow spanning-treeللتحقق من تكوين بروتوكول الشجرة المتفرعة (STP). تحقق أيضا من إعلامات تغيير المخطط (TCNs) باستخدام الأمرshow spanning-tree detail | include ieee|occur|from|is.
- التحقق من مضاعفة عناوين MAC: إذا كان لجهازين على شبكتك نفس عنوان MAC (يظهر غالبا في إعداد التوفر العالي (HA) والعديد من وحدات تحكم واجهة الشبكة أو البطاقات (NICs))، فقد يؤدي ذلك إلى رفرفة MAC. أستخدم الأمرshow mac address-tableللبحث عن عناوين MAC المكررة على شبكتك.
- تحقق من وجود أجهزة أو كبلات معيبة: قد تتسبب كبلات الشبكة أو الأجهزة المعيبة في إرسال الإطارات إلى الواجهات الخطأ، مما يؤدي إلى رفرفة MAC. تحقق من الحالة المادية للكابلات وأفكر في إستبدال الأجهزة لمعرفة ما إذا كانت المشكلة مستمرة. كما يمكن أن يتسبب رفرفة الواجهة في رفرفة MAC على المحولات.
- التحقق من أخطاء البرامج: في بعض الأحيان، يمكن أن يكون رفرفة ماك بسبب أخطاء في برنامج أجهزة الشبكة. تحقق من أداة البحث عن الأخطاء.

أداة البحث عن الأخطاء: https://bst.cloudapps.cisco.com/bugsearch

تعليمات أداة البحث عن الأخطاء:
https://www.cisco.com/c/en/us/support/web/tools/bst/bsthelp/index.html#search

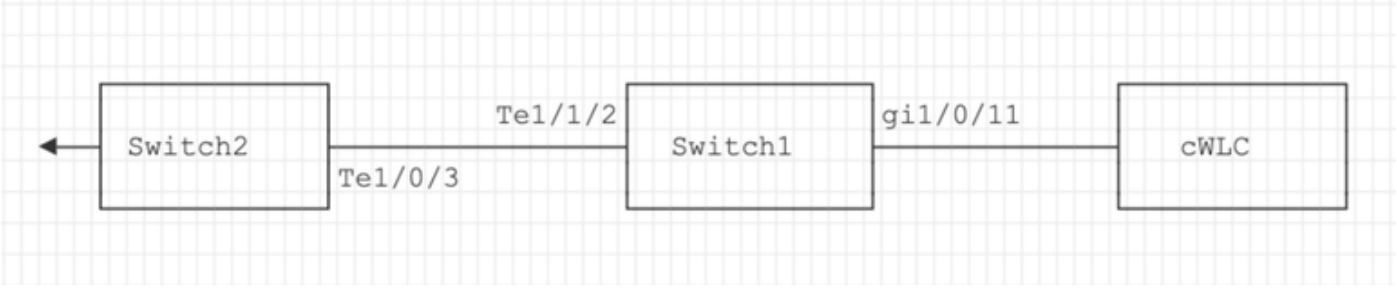
- الاتصال بدعم TAC: إذا حاولت كل شيء وكانت المشكلة لا تزال قائمة، فقد يكون الوقت قد حان للاتصال بدعم Cisco TAC. ويمكنهم تقديم المزيد من المساعدة.

دراسة الحالة 1

وصف المشكلة

تواجه وحدة التحكم في الشبكة المحلية اللاسلكية (EWLC) فقدانا للاتصال بالبوابة، وتعمل حالات إسقاط الحزم على منع نقاط الوصول (APs) من الانضمام إلى وحدة التحكم.

المخطط



خطوات أستكشاف الأخطاء وإصلاحها

تم تحديد رفرفة MAC على المحول (Switch1) المتصل بعنصر التحكم في الشبكة المحلية اللاسلكية (eWLC).

```
*Aug  5 05:52:50.750: %SW_MATM-4-MACFLAP_NOTIF: Host 0000.5e00.0101 in vlan 4 is flapping between port
*Aug  5 05:53:03.327: %SW_MATM-4-MACFLAP_NOTIF: Host 0000.5e00.0101 in vlan 4 is flapping between port
*Aug  5 05:53:21.466: %SW_MATM-4-MACFLAP_NOTIF: Host 0000.5e00.0101 in vlan 4 is flapping between port
```

تعلم MAC:

أدخل الأمرshow mac address-table address
in order to فحص ما إذا كان عنوان MAC قد تعلم على الميناء.

<#root>

```
Switch1#show mac address-table address 0000.5e00.0101

          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   4    0000.5e00.0101    DYNAMIC     Gi1/0/11


   4    0000.5e00.0101    DYNAMIC     Te1/1/2
```

تشكيل الميناء gi1/0/11 و te1/1/2:

أدخل الأمرshow running-config interface
in order to فحص القارن تشكيل.

<#root>

```
interface GigabitEthernet1/0/11
```

```
 switchport trunk native vlan 4
 switchport mode trunk
end
```

```
interface TenGigabitEthernet1/1/2
```

```
 switchport mode trunk
end
```

جيران المنافذ CDP GI1/0/11 و TE1/1/2:

أدخل الأمرshow cdp neighbors
للتحقق من تفاصيل الأجهزة المتصلة.

<#root>

```
Switch1#show cdp neighbors gi1/0/11
```

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
eWLC            Gig 1/0/11        130              R T   C9115AXI- Gig 0 < ----- eWLC Controller
```

```
Switch1#show cdp neighbors gi1/1/2
```

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Switch2

                 Ten 1/1/2         163             R S I  C9500-16X Ten 1/0/3 < ----- Uplink Switch
```

التعرف على MAC على المحول 2 (محول الوصلة):

دخلت الأمرshow mac address-table address
in order to فحصت لا مام عنوان علمت على الميناء.

<#root>

```
Switch2#show mac address-table address 0000.5E00.0101
```

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   4    0000.5e00.0101    STATIC
```

Vl4 < ----- VRRP MAC of Vlan4

```
   4    0000.5e00.0101    DYNAMIC
```

Te1/0/13 < ----- Learning from Switch1 (eWLC connected Switch)

<#root>

Switch2#show vrrp vlan 4

Vlan4 - Group 1

```
 - Address-Family IPv4
  State is MASTER
  State duration 5 days 4 hours 22 mins
  Virtual IP address is x.x.x.x
```

** Virtual MAC address is 0000.5E00.0101 < ------ VRRP MAC of Vlan4**

```
  Advertisement interval is 1000 msec
```

سبب جذري

تم التحقق من أن مع رف بروتوكول تكرار جهاز التوجيه الظاهري (VRRP) للمجموعة 2 و eWLC كانا متشابهين، مما أدى إلى إنشاء MAC الظاهري نفسه بواسطة VRRP.

قرار

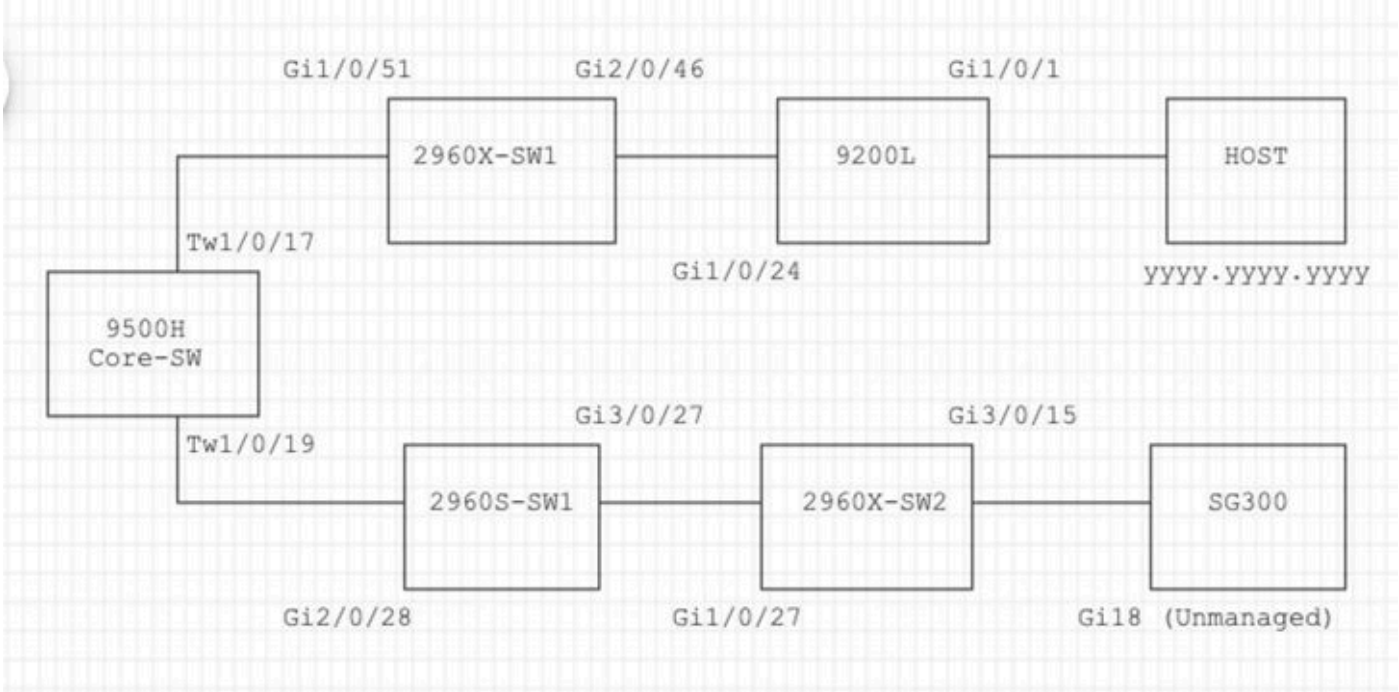
تم حل المشكلة بعد تغيير مثيل VRRP على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، والذي كان يتسبب في حدوث MAC مكرر على المجموعة مما يؤدي إلى فقد الاتصال بالبوابة وعمليات إسقاط الحزم، مما منع نقاط الوصول (APs) من الانضمام إلى وحدة التحكم.

دراسة حالة 2

وصف المشكلة

يتعذر الوصول إلى بعض الخوادم أو أنها تواجه زمن وصول/حالات سقوط كبيرة.

المخطط



خطوات أستكشاف الأخطاء وإصلاحها

1. تم ملاحظة رفرفة MAC تحدث على المحول الأساسي.

```
Nov 14 08:36:34.637: %SW_MATM-4-MACFLAP_NOTIF: Host xxxx.xxxx.xxxx in vlan 1 is flapping between port Tw
Nov 14 08:36:34.838: %SW_MATM-4-MACFLAP_NOTIF: Host yyyy.yyyy.yyyy in vlan 1 is flapping between port Tw
Nov 14 08:36:34.882: %SW_MATM-4-MACFLAP_NOTIF: Host zzzz.zzzz.zzzz in vlan 1 is flapping between port Po
```

2. إختيار عنوانyyyy.yyyy.yyyyMAC لعملية أستكشاف الأخطاء وإصلاحها.

تعلم MAC:

دخلت الأمرshow mac address-table address
in order to فحصت ال ماك عنوان علمت على المينا.

<#root>

```
Core-SW#show mac address-table address yyyy.yyyy.yyyy
```

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    yyyy.yyyy.yyyy    DYNAMIC     Twe1/0/17
```

منافذ CDP المجاورة للمنافذ 1/0/17 و 1/0/19:

أدخل الأمرshow cdp neighbors
للتحقق من تفاصيل الأجهزة المتصلة.

<#root>

Core-SW#show cdp neighbors Twe 1/0/17

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
```

2960X-SW1

Twe 1/0/17 162 S I WS-C2960X Gig 1/0/51

Core-SW#show cdp neighbors Twe 1/0/19

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
```

2960S-SW1

Twe 1/0/19 120 S I WS-C2960S Gig 2/0/28

السجلات من 2960X-SW1 المتصلة ب core-SW twe1/0/17:

يرفرف MACyyyy.yyyy.yyyyبين منفذ gi1/0/51 و gi2/0/46 (9200L).

<#root>

2960X-SW1#show mac address-table address yyyy.yyyy.yyyy

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
```

1 yyyy.yyyy.yyyy DYNAMIC Gi1/0/51

2960X-SW1#show mac address-table address yyyy.yyyy.yyyy

```
          Mac Address Table
```

```
----------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    yyyy.yyyy.yyyy DYNAMIC     Gi2/0/46
```

```
2960X-SW1#show run interface gi 1/0/51

Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet1/0/51
switchport mode trunk
end
```

```
2960X-SW1#show run interface gi 2/0/46

Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet2/0/46
switchport mode trunk
end
```

السجلات من 9200L:

(يبدو أن هذا هو المنفذ الصالح لعنوان MAC هذا.)

<#root>

```
9200L#show mac address-table address yyyy.yyyy.yyyy

          Mac Address Table
----------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    yyyy.yyyy.yyyy DYNAMIC     Gi1/0/1
```

```
9200L#show run interface gi 1/0/1

Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet1/0/1
switchport mode access
end
```

2960S-SW1 متصل ب core-sw twe1/0/19:

(يظهر أن يكون مسار تكرار حلقي.) عطلت الميناء على ال core-sw in order to خفف
الأنشطة.

ومع ذلك، كان ال يزال يجري ملاحظة ذاذ MAC على الل-الجنوب.

السجلات من 2960S-SW1:

<#root>

```
Nov 14 08:36:34.637: %SW_MATM-4-MACFLAP_NOTIF: Host xxxx.xxxx.xxxx in vlan 1 is flapping between port G
Nov 14 08:36:34.838: %SW_MATM-4-MACFLAP_NOTIF: Host yyyy.yyyy.yyyy in vlan 1 is flapping between port G
Nov 14 08:36:34.882: %SW_MATM-4-MACFLAP_NOTIF: Host zzzz.zzzz.zzzz in vlan 1 is flapping between port G
```

2960S-SW1#show run interface gi 3/0/27

```
Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet3/0/27
switchport mode trunk
end
```

2960S-SW1#show cdp neighbor gi 3/0/27

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
```

2960X-SW2

Gig 3/0/27 176 S I WS-C2960X Gig 1/0/27

السجلات من 2960X-SW2:

<#root>

2960X-SW2#show run interface gi 3/0/15

```
Building configuration...

Current configuration : 39 bytes
!
interface GigabitEthernet3/0/15
end
```

```
2960X-SW2#show cdp neighbor gi 3/0/15


Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

SG300     Gig 3/0/15        157              S I   SG300-28P gi18



2960X-SW2#config terminal


2960X-SW2(config)#interface gi 3/0/15


2960X-SW2(config-if)#shutdown
```

سبب جذري

شوهدت نقاط وصول MAC بسبب محول SG300 (غير مدار) المتصل بالشبكة.

قرار

حللت ال MAC يرفرفة إصدار ب يعطل المينا يربط إلى ال unmanaged مفتاح SG300.

منع

بروتوكول STP PortFast:

يتسبب بروتوكول STP PortFast في إدخال منفذ شبكة LAN من الطبقة 2 في حالة إعادة التوجيه على الفور، مما يؤدي إلى تجاوز حالات الاستماع والتعلم. يمنع STP PortFast إنشاء شبكات STP TCN، والتي لا تكون ذات معنى من المنافذ التي لا تستلم وحدات بيانات بروتوكول بروتوكول STP (BPDUs). تشكل STP PortFast فقط على ميناء أن يكون ربط أن ينهي مضيفا أداة أن ينهي VLANs ومن أي المينا ينبغي أبدا إستلمت STP BPDUs، مثل عمل محطة، لاند، ميناء على مسحاج تخدي أن ال يشكل أن ياسان يجسر.

حماية وحدة بيانات بروتوكول الجسر (BPDU):

يقوم واقي STP BPDU باستكمال وظائف STP PortFast. على منافذ STP PortFast-enabled، يحمي واقي STP BPDU حلقات الطبقة 2 التي ال يمكن أن يوفرها STP عندما STP PortFast يكون ممكنت. يقوم حارس STP BPDU بإيقاف تشغيل المنافذ التي تستلم BPDUs.

حماية الجذر:

يمنع الواقي الجذر المنافذ من أن تصبح منافذ جذر بروتوكول الشجرة المتفرعة (STP). أستخدم واقي جذر بروتوكول الشجرة المتفرعة (STP) لمنع المنافذ غير المناسبة من أن

تصبح منافذ جذر بروتوكول الشجرة المتفرعة (STP). مثال من ميناء غير مناسب ميناء أن يطبري إلى أداة أن يكون خارج تحكم إداري شبكة مباشرة.

حماية التكرار الحلقي:

حماية التكرار الحلقي هي تحسين خاص ب Cisco ل STP. يحمي حماية حماية التكرار الحلقي شبكات الطبقة 2 من حلقات التكرار التي تحدث عندما يمنع شيء ما إعادة التوجيه العادية (على سبيل المثال، عطل واجهة شبكة أو وحدة معالجة مركزية (CPU) مشغولة). استكمل حماية التكرار الحلقي الحماية ضد حالات فشل الارتباط أحادي الإتجاه التي يوفرها اكتشاف الارتباط أحادي الإتجاه (UDLD). يعمل حماية التكرار الحلقي على عزل الأعطال والسماح بتحويل بروتوكول الشجرة المتفرعة (STP) إلى مخطط مستقر مع إستبعاد المكون الفاشل من مخطط بروتوكول الشجرة المتفرعة (STP).

مرشح BPDU:

يؤدي ذلك إلى تعطيل بروتوكول الشجرة المتفرعة (STP). لا يتم إرسال وحدات بيانات بروتوكول الجسر (BPDU) أو معالجتها عند الاستلام. وهو شائع مع موفري الخدمة، وليس بالضرورة مع شبكات المؤسسة.

UDLD العدواني:

ال cisco مالك UDLD يراقب بروتوكول التشكيل طبيعي من الربط بين أداة وميناء أن يساند UDLD. UDLD يكشف وجود خطوة أحادي إتجاه. UDLD يستطيع عملت في إما عادي أو عدواني أسلوب. UDLD في الوضع العادي يصنف خطوة ك أحادي إتجاه إن ال يستلم UDLD ال يحتوي ربط معلومة أن يكون صحيح للأداة مجاور. بالإضافة إلى وظيفة الوضع العادي UDLD، وضع عدوانية أسلوب UDLD ميناء داخل الدولة handicapé إن العلاقة بين إثنان سابقا تزامن مجاور يستطيع ال يكون أسست من جديد.

السيطرة على العواصف:

يتم تنفيذ التحكم في عواصف حركة المرور في الأجهزة والتي تؤثر على الأداء الإجمالي للمحول. عادة، تكون المحطات الطرفية مثل أجهزة الكمبيوتر والخوادم هي مصدر حركة مرور البث التي يمكن قمعها. تتجنب المعالجة غير الضرورية لحركة مرور البث الزائدة، قم بتمكين التحكم في عواصف حركة مرور البيانات لحركة مرور البث على منافذ الوصول المتصلة بالمحطات الطرفية وعلى المنافذ المتصلة بعقد الشبكة الأساسية.

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).