مثال على تكوين ميزات أمان الطبقة الثانية في مبدلات الطبقة الثالثة من Cisco Catalyst ذات التكوين الثابت

المحتويات

المقدمة

يزود هذا وثيقة عينة تشكيل لبعض من الطبقة 2 أمن سمة، مثل أمن أيسر، DHCP يتطفل، حركي تحليل العنوان بروتوكول (ARP) تفتيش وواقي مصدر بروتوكول الإنترنت، أن يستطيع كنت طبقت على cisco مادة حفازة طبقة 3 ثابت تشكيل مفتاح.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى المحول Cisco Catalyst 3750 Series Switch مع الإصدار SEC2(25)12.2.

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.

المنتجات ذات الصلة

يمكن إستخدام هذا التكوين أيضا مع الأجهزة الصلبة التالية:

- المحولات Cisco Catalyst 3550 Series Switches
- المحولات Cisco Catalyst 3560 Series Switches
- سلسلة مبدلات Cisco Catalyst 3560-E
- سلسلة مبدلات Cisco Catalyst 3750-E

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات أساسية

وكما هو الحال مع الموجهات، فإن لكل من محولات الطبقة 2 والطبقة 3 مجموعاتها الخاصة من متطلبات أمان الشبكة. تكون المحولات عرضة للعديد من هجمات الطبقة 3 نفسها الخاصة بالموجهات. ومع ذلك، تخضع المحولات والطبقة 2 من نموذج مرجع الاتصال المتبادل بين الأنظمة المفتوحة (OSI) بشكل عام لهجمات الشبكة بطرق مختلفة. وتشمل هذه التدابير ما يلي:

- **تجاوز جدول الذاكرة القابلة للتوجيه للمحتوى (CAM)**جداول ذاكرة المحتوى القابلة للتوجيه (CAM) محدودة الحجم. إذا تم إدخال عدد كاف من الإدخالات في جدول CAM قبل انتهاء صلاحية الإدخالات الأخرى، فإن جدول CAM يتم تعبئته إلى درجة أنه لا يمكن قبول الإدخالات الجديدة. نموذجيا، يفيض متطفل الشبكة المحول بعدد كبير من عناوين التحكم في الوصول إلى الوسائط (MAC) غير الصالحة حتى يتم تعبئة جدول CAM. عندما يقع ذلك، يفيض المفتاح كل ميناء مع حركة مرور قادم لأن هو يستطيع لا يجد رقم الميناء لخاص ماك عنوان في الكومة طاولة. يعمل المحول، في جوهره، كمركز. إذا لم يحافظ الدخيل على تدفق عناوين MAC للمصدر غير الصالحة، سيقوم المحول في نهاية المطاف بنسخ إدخالات عنوان MAC القديمة من جدول CAM ويبدأ في العمل كمحول مرة أخرى. تجاوز جدول CAM يفيض حركة المرور فقط ضمن شبكة VLAN المحلية لذلك المتسلل لا يرى حركة المرور إلا داخل شبكة VLAN المحلية التي يكون هو أو هي متصلا بها.يمكن الحد من هجوم تجاوز جدول CAM من خلال تكوين أمان المنفذ على المحول. يزود هذا خيار ل إما مواصفة من ال mac عنوان على خاص مفتاح ميناء أو المواصفة من الرقم من {mac address{upper أن يستطيع كنت علمت بمفتاح ميناء. عندما كشفت عنوان MAC غير صالح على المنفذ، يمكن للمحول إما حظر عنوان MAC المسيء أو إيقاف تشغيل المنفذ. لا يمكن إدارة مواصفات عناوين MAC على منافذ المحول كحل لبيئة الإنتاج. يمكن إدارة حد عدد عناوين MAC على منفذ محول. يعد تنفيذ أمان المنفذ الديناميكي في المحول حلا أكثر قابلية للتطوير من الناحية الإدارية. لتنفيذ أمان المنفذ الديناميكي، حدد الحد الأقصى لعدد عناوين MAC التي سيتم التعرف عليها.
- **انتحال عنوان التحكم في الوصول إلى الوسائط (MAC)**تتضمن هجمات الانتحال الخاصة بالتحكم في الوصول إلى الوسائط (MAC) إستخدام عنوان MAC معروف لمضيف آخر لمحاولة تحويل الإطارات المستهدفة الموجهة للمضيف البعيد إلى مهاجم الشبكة. عندما يتم إرسال إطار واحد مع عنوان إيثرنت المصدر للمضيف الآخر، يقوم مهاجم الشبكة بالكتابة فوق إدخال جدول CAM بحيث يقوم المحول بإعادة توجيه الحزم الموجهة للمضيف إلى مهاجم الشبكة. إلى أن يرسل المضيف حركة مرور، لا يستلم هو أي حركة مرور. عندما يرسل المضيف حركة مرور، ال CAM طاولة يعاد كتابتها مرة أخرى بحيث أن هو يتحرك إلى الخلف إلى الميناء أصلي.أستخدم ميزة أمان المنفذ للحد من هجمات انتحال MAC. يوفر أمان المنفذ إمكانية تحديد عنوان MAC للنظام المتصل بمنفذ معين. هذا أيضا يزود القدرة أن يعين إجراء أن يأخذ إن أيسر أمن يقع انتهاك.
- **انتحال بروتوكول تحليل العنوان (ARP)**يتم إستخدام ARP لتعيين عنونة IP إلى عناوين MAC في مقطع شبكة

منطقة محلية حيث يقيم المضيفون من الشبكة الفرعية نفسها. عادة، يرسل المضيف طلب ARP للبث للعثور على عنوان MAC لمضيف آخر مع عنوان IP خاص، وتأتي إستجابة ARP من المضيف الذي يتطابق عنوانه مع الطلب. يقوم المضيف الطالب بعد ذلك بتخزين إستجابة ARP هذه مؤقتا. وضمن بروتوكول ARP، تم توفير حكم آخر للمضيفين لتنفيذ ردود ARP غير المرغوب فيها. تسمى ردود ARP غير المرغوب فيها GARP) ARP). يمكن إستغلال GARP بشكل خبيث من قبل المهاجم لإفساد هوية عنوان IP على مقطع الشبكة المحلية (LAN). يستخدم هذا عادة لإفساد الهوية بين جهازين مضيفين أو حركة المرور بالكامل من وإلى البوابة الافتراضية في هجوم "رجل في الوسط".عند صياغة رد ARP، يمكن لمهاجم الشبكة أن يجعل نظامه يبدو كمضيف الوجهة الذي ينشده المرسل. يتسبب رد ARP في قيام المرسل بتخزين عنوان MAC لنظام مهاجم الشبكة في ذاكرة تخزين ARP المؤقت. هذا {mac address{upper أيضا خزنت بالمفتاح في ه حدبة طاولة. بهذه الطريقة، قام مهاجم الشبكة بإدخال عنوان MAC الخاص بنظامه أو نظامها في كل من جدول CAM الخاص بالمحول وذاكرة تخزين ARP المؤقتة الخاصة بالمرسل. وهذا يسمح لمهاجم الشبكة باعتراض الإطارات الموجهة للمضيف الذي ينتحله أو تنتحله.يمكن إستخدام مؤقتات الإيقاف في قائمة تكوين الواجهة للحد من هجمات انتحال ARP عن طريق تعيين طول الوقت الذي سيبقى فيه الإدخال في ذاكرة التخزين المؤقت ل ARP. غير أن أوقات الانتظار غير كافية بحد ذاتها. يلزم تعديل وقت انتهاء صلاحية ذاكرة التخزين المؤقت ل ARP على جميع الأنظمة الطرفية بالإضافة إلى إدخالات ARP الثابتة. وهناك حل آخر يمكن إستخدامه لتخفيف العديد من أستكشاف الشبكات المستندة إلى ARP، وهو إستخدام التطفل على بروتوكول DHCP مع الفحص الديناميكي ل ARP. تحقق ميزات Catalyst هذه من حزم ARP في شبكة وتسمح باعتراض حزم ARP وتسجيلها وتجاهلها باستخدام عنوان MAC غير صالح لروابط عنوان IP.مرشحات التطفل على بروتوكول DHCP لرسائل DHCP الموثوق بها لتوفير الأمان. بعد ذلك، يتم إستخدام هذه الرسائل لإنشاء جدول ربط التطفل على بروتوكول DHCP والاحتفاظ به. يعتبر التطفل على بروتوكول DHCP رسائل DHCP التي تنشأ من أي منفذ يواجه المستخدم والذي ليس منفذ خادم DHCP غير موثوق به. من منظور التطفل على بروتوكول DHCP، يجب ألا تقوم هذه المنافذ غير الموثوقة الموجهة من قبل المستخدم بإرسال استجابات نوع خادم DHCP، مثل DHCPpoffer، أو DHCPack، أو DHCPnak. يحتوي جدول ربط التطفل على بروتوكول DHCP على عنوان MAC وعنوان IP ووقت الإيجار ونوع الربط ورقم الشبكة المحلية الظاهرية (VLAN) ومعلومات الواجهة التي تطابق الواجهات المحلية غير الموثوق بها للمحول. لا يحتوي جدول ربط التطفل على بروتوكول DHCP على معلومات حول البيئات المضيفة المتصلة بواجهة موثوق بها. الواجهة غير الموثوق بها هي واجهة تم تكوينها لتلقي الرسائل من خارج الشبكة أو جدار الحماية. الواجهة الموثوق بها هي واجهة تم تكوينها لتلقي الرسائل فقط من داخل الشبكة. يمكن أن يحتوي جدول ربط التطفل على بروتوكول DHCP على كل من عنوان MAC الديناميكي والثابت لروابط عناوين IP.يحدد الفحص الديناميكي ل ARP صحة حزمة ARP استنادا إلى عنوان MAC الصحيح لروابط عناوين IP المخزنة في قاعدة بيانات التطفل على بروتوكول DHCP. وبالإضافة إلى ذلك، يمكن أن يتحقق الفحص الديناميكي ل ARP من حزم ARP استنادا إلى قوائم التحكم في الوصول (ACL) القابلة للتكوين من قبل المستخدم. وهذا يسمح بفحص حزم ARP للمضيفين الذين يستخدمون عناوين IP التي تم تكوينها بشكل ثابت. يسمح فحص ARP الديناميكي باستخدام قوائم التحكم في الوصول إلى كل منفذ وشبكة VLAN) PACL) للحد من حزم ARP لعناوين IP المحددة لعناوين MAC معينة.

- **تجويع بروتوكول تكوين الاستضافة الديناميكية (DHCP)**يعمل هجوم DHCP للمجاعة عن طريق بث طلبات DHCP باستخدام عناوين MAC المنتحلة. إذا تم إرسال طلبات كافية، فيمكن لمهاجم الشبكة استنفاد مساحة العنوان المتاحة لخوادم DHCP لفترة من الوقت. بعد ذلك يمكن لمهاجم الشبكة إعداد خادم DHCP مخادع على نظامه أو نظامها والاستجابة لطلبات DHCP الجديدة من العملاء على الشبكة. مع وضع خادم DHCP مخادع على الشبكة، يمكن لمهاجم الشبكة توفير عناوين ومعلومات شبكة أخرى للعملاء. نظرا لأن استجابات DHCP تتضمن عادة العبارة الافتراضية ومعلومات خادم DNS، فيمكن لمهاجم الشبكة توفير نظامه الخاص كالعبارة الافتراضية وخادم DNS. وينتج عن ذلك هجوم الدخيل. ومع ذلك، لا يلزم إستخدام جميع عناوين DHCP لتقديم خادم DHCP مخادع.يمكن إستخدام الميزات الإضافية في مجموعة المحولات Catalyst من المحولات، مثل التطفل على بروتوكول DHCP، للمساعدة في الحماية من هجوم المجاعة على بروتوكول DHCP. التطفل على بروتوكول DHCP هو ميزة أمان تقوم بتصفية رسائل DHCP غير الموثوق بها وإنشاء جدول ربط التطفل على بروتوكول DHCP والاحتفاظ به. يحتوي جدول الربط على معلومات مثل عنوان MAC، عنوان IP، وقت التأجير، نوع الربط، رقم VLAN ومعلومات الواجهة التي تطابق الواجهات المحلية غير الموثوق بها للمحول. الرسائل غير الموثوق بها هي تلك التي تم تلقيها من خارج الشبكة أو جدار الحماية. واجهات المحولات غير الموثوق بها هي واجهات يتم تكوينها لتلقي مثل هذه الرسائل من خارج الشبكة أو جدار الحماية.يمكن أن توفر

ميزات محولات Catalyst الأخرى، مثل واقي مصدر بروتوكول الإنترنت، حماية إضافية ضد الهجمات مثل تجويع بروتوكول DHCP وانتحال عناوين IP. وكما هو الحال مع التطفل على بروتوكول DHCP، يتم تمكين واقي مصدر بروتوكول الإنترنت على منافذ الطبقة 2 غير الموثوق بها. يتم حظر جميع حركة مرور IP في البداية، باستثناء حزم DHCP التي يتم التقاط بياناتها بواسطة عملية التطفل على بروتوكول DHCP. ما إن يستلم زبون عنوان صالح من ال DHCP نادل، PACL طبقت إلى الميناء. يؤدي هذا إلى تقييد حركة مرور IP للعميل بعناوين IP للمصدر التي تم تكوينها في التوثيق. تتم تصفية أي حركة مرور IP أخرى ذات عنوان مصدر غير العناوين في التوثيق.

التكوين

في هذا القسم، تقدم لك معلومات تكوين أمان المنفذ وتطفل DHCP والفحص الديناميكي ل ARP ومميزات أمان أمان مصدر IP.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

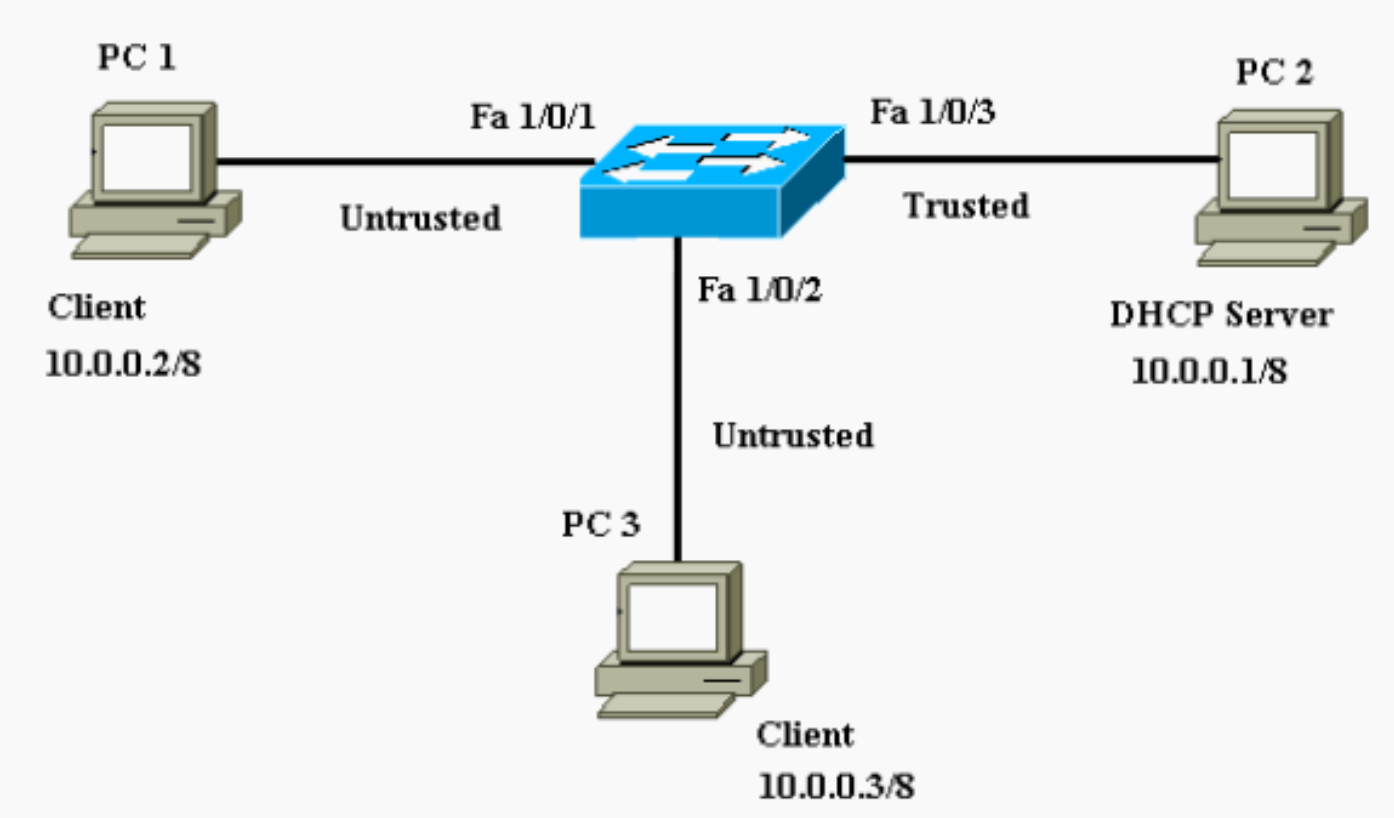
تحتوي تكوينات المحول Catalyst 3750 switch على التالي:

- أمان المنفذ
- التطفل على بروتوكول DHCP
- فحص ARP (بروتوكول تحليل العناوين) الديناميكي
- واقي مصدر بروتوكول الإنترنت

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:

- PC 1 و PC 3 هما عملاء متصلان بالمحول.
- PC 2 هو خادم DHCP متصل بالمحول.
- كل ميناء من المفتاح في ال نفسه VLAN (VLAN 1).
- تم تكوين خادم DHCP لتعيين عناوين IP إلى العملاء استنادا إلى عناوين MAC الخاصة بهم.



أمان المنفذ

أنت يستطيع استعملت الميناء أمن سمة أن يحد ويعين ماك عنوان من المحطات يسمح أن ينفذ الميناء. يؤدي هذا إلى تقييد الإدخال إلى واجهة. عندما يعين أنت يأمن {upper}mac address إلى يأمن ميناء، الميناء لا يرسل ربط مع مصدر عنوان خارج المجموعة من يعين عنوان. إن يقصر أنت الرقم من يأمن {upper}mac address إلى واحد ويعين وحيد يأمن {upper}mac address، محطة العمل يربط إلى أن ميناء يطمئن ال كامل نطاق من الميناء. إن شكلت ميناء يكون كيأمن ميناء وأقصى عدد من يؤمن ماك عنوان بلغت، عندما ال ماك عنوان من محطة أن يحاول أن ينفذ الميناء يكون مختلف من any of the يعين يؤمن ماك عنوان، أمن يقع انتهاك. أيضا، إن يحاول محطة مع يأمن {upper}mac address يشكل أو علمت على واحد يأمن ميناء أن ينفذ آخر يأمن ميناء، انتهاك يعين. افتراضيا، يعطل الميناء عندما يتجاوز العدد الأقصى من ماك عنوان آمن.

ملاحظة: عند انضمام محول Catalyst 3750 switch إلى مكدس، يستقبل المحول الجديد العناوين الآمنة التي تم تكوينها. يتم تنزيل جميع العناوين الآمنة الديناميكية بواسطة عضو المكدس الجديد من أعضاء المكدس الأخرى.

ارجع إلى إرشادات التكوين للحصول على الإرشادات حول كيفية تكوين أمان المنفذ.

هنا، يتم عرض ميزة أمان المنفذ التي تم تكوينها على واجهة FastEthernet 1/0/2. بشكل افتراضي، يكون الحد الأقصى لعدد عناوين MAC الآمنة للواجهة هو واحد. أنت يستطيع أصدرت **العرض ميناء-أمن قارن** أمر in order to دققت الميناء أمن وضع لقارن.

أمان المنفذ

```
Cat3750#show port-security interface fastEthernet 1/0/2
                  Port Security              : Disabled
               Port Status                   : Secure-down
                  Violation Mode             : Shutdown
                    Aging Time               : 0 mins
                  Aging Type                 : Absolute
                  SecureStatic Address Aging : Disabled
                        Maximum MAC Addresses      : 1
                        Total MAC Addresses        : 0
                        Configured MAC Addresses   : 0
```

```
                                Sticky MAC Addresses        : 0
                          Last Source Address:Vlan    : 0000.0000.0000:0
                                Security Violation Count    : 0
 Default port security configuration on the switch. ---!
                                                    Cat3750#conf t
   Enter configuration commands, one per line.  End with
                                                          .CNTL/Z
                          Cat3750(config)#interface fastEthernet 1/0/2
                           Cat3750(config-if)#switchport port-security
  .Command rejected: FastEthernet1/0/2 is a dynamic port
     Port security can only be configured on static ---!
           access ports or trunk ports. Cat3750(config-
                                          if)#switchport mode access
       Sets the interface switchport mode as access. ---!
                           Cat3750(config-if)#switchport port-security
            Enables port security on the interface. ---!
 Cat3750(config-if)#switchport port-security mac-address
                                                  0011.858D.9AF9
      Sets the secure MAC address for the interface. ---!
   Cat3750(config-if)#switchport port-security violation
                                                      shutdown
    Sets the violation mode to shutdown. This is the ---!
default mode. Cat3750# !--- Connected a different PC (PC
     4) to the FastEthernet 1/0/2 port !--- to verify the
     port security feature. 00:22:51: %PM-4-ERR_DISABLE:
    psecure-violation error detected on Fa1/0/2, putting
Fa1/0/2 in err-disable state 00:22:51: %PORT_SECURITY-2-
  PSECURE_VIOLATION: Security violation occurred, caused
by MAC address 0011.8565.4B75 on port FastEthernet1/0/2.
          00:22:52: %LINEPROTO-5-UPDOWN: Line protocol on
      Interface FastEthernet1/0/2, changed state to down
  00:22:53: %LINK-3-UPDOWN: Interface FastEthernet1/0/2,
  changed state to down !--- Interface shuts down when a
 security violation is detected. Cat3750#show interfaces
                                              fastEthernet 1/0/2
  FastEthernet1/0/2 is down, line protocol is down (err-
                                                    (disabled
    Output Suppressed. !--- The port is shown error- ---!
    disabled. This verifies the configuration. !--- Note:
 When a secure port is in the error-disabled state, !---
    you can bring it out of this state by entering !--- the
      errdisable recovery cause psecure-violation global
     configuration command, !--- or you can manually re-
 enable it by entering the !--- shutdown and no shutdown
                                        .interface configuration commands


 Cat3750#show port-security interface fastEthernet 1/0/2
                     Port Security              : Enabled
            Port Status                 : Secure-shutdown
                   Violation Mode             : Shutdown
                     Aging Time                 : 0 mins
                   Aging Type                 : Absolute
                   SecureStatic Address Aging : Disabled
                          Maximum MAC Addresses      : 1
                          Total MAC Addresses        : 1
                          Configured MAC Addresses   : 1
                          Sticky MAC Addresses       : 0
          Last Source Address:Vlan    : 0011.8565.4B75:1
                          Security Violation Count   : 1
```

ملاحظة: لا ينبغي تكوين عناوين MAC نفسها كعنوان MAC آمن وساكن إستاتيكي على منافذ مختلفة من المحول.

عندما يكون هاتف IP متصلا بمحول من خلال Switchport الذي تم تكوينه لشبكة VLAN الصوتية، يرسل الهاتف حزم CDP غير المميزة وحزم CDP الصوتية المميزة. إذا عنوان MAC لهاتف بروتوكول الإنترنت تم التعرف عليه على كل من PVID و VVID. إذا لم يتم تكوين العدد المناسب من العناوين الآمنة، فيمكنك الحصول على رسالة خطأ مماثلة لهذه الرسالة:

```
,PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred%
.caused by MAC address 001b.77ee.eeee on port GigabitEthernet1/0/18
:PSECURE: Assert failure: psecure_sb->info.num_addrs <= psecure_sb->max_addrs
```

أنت ينبغي ثبتت الأقصى يأمن عنوان على الميناء إلى إثنان (لهاتف IP) بالإضافة إلى العدد الأقصى من يأمن عنوان يسمح على الوصول VLAN in order to حللت هذا إصدار.

راجع تكوين أمان المنفذ للحصول على مزيد من المعلومات.

التطفل على بروتوكول DHCP

يعمل التطفل على بروتوكول DHCP كجدار حماية بين الأجهزة المضيفة غير الموثوق بها وخوادم DHCP. أنت تستخدم التطفل على بروتوكول DHCP للتمييز بين الواجهات غير الموثوق بها المتصلة بالمستخدم النهائي والواجهات الموثوق بها المتصلة بخادم DHCP أو محول آخر. عندما يستلم مفتاح ربط على قارن غير موثوق وتنسب القارن إلى VLAN أن يتلقى DHCP يتطفل يمكن، المفتاح يقارن المصدر {mac address}upper وال DHCP زبون جهاز عنوان. إن تلاءم العنوان (التقصير)، المفتاح يرسل الربط. إذا لم تتطابق العناوين، يقوم المحول بإسقاط الحزمة. يقوم المحول بإسقاط حزمة DHCP عند حدوث إحدى هذه الحالات:

- يتم تلقي حزمة من خادم DHCP، مثل DHCPpoffer، أو DHCPack، أو DHCPnak، أو حزمة DHCPwitery، من خارج الشبكة أو جدار الحماية.
- يتم تلقي حزمة على واجهة غير موثوق بها، ولا يتطابق عنوان MAC المصدر وعنوان جهاز عميل DHCP.
- يستلم المفتاح DHCPprelease أو DHCPdecline بث رسالة أن يتلقى عنوان MAC في ال DHCP snooping ملزم قاعدة معطيات، غير أن القارن معلومة في الربط قاعدة معطيات لا تلاءم القارن على أي رسالة إستلمت.
- يرسل وكيل ترحيل DHCP حزمة DHCP، والتي تتضمن عنوان IP لعامل ترحيل ليس 0.0.0.0، أو يقوم وكيل الترحيل بإعادة توجيه حزمة تتضمن معلومات الخيار-82 إلى منفذ غير موثوق به.

ارجع إلى إرشادات تكوين التطفل على بروتوكول DHCP للحصول على الإرشادات حول كيفية تكوين التطفل على بروتوكول DHCP.

ملاحظة: لكي يعمل التطفل على بروتوكول DHCP بشكل صحيح، يجب توصيل جميع خوادم DHCP بالمحول من خلال الواجهات الموثوق بها.

ملاحظة: في مكدس محول باستخدام محولات Catalyst 3750، تتم إدارة التطفل على بروتوكول DHCP على مدير المكدس. عندما ينضم محول جديد إلى المكدس، يستقبل المحول تكوين التطفل على بروتوكول DHCP من مدير المكدس. عندما يترك عضو المكدس، فإن جميع روابط التطفل على بروتوكول DHCP المرتبطة بالمحول تخرج.

ملاحظة: لضمان دقة وقت التأجير في قاعدة البيانات، توصي Cisco بتمكين NTP وتكوينه. إذا تم تكوين بروتوكول وقت الشبكة (NTP)، يقوم المحول بكتابة تغييرات الربط إلى ملف الربط فقط عندما يتم مزامنة ساعة نظام المحول مع NTP.

يمكن الحد من خوادم DHCP المخادعة بواسطة ميزات التطفل على بروتوكول DHCP. يتم إصدار الأمر **ip dhcp snooping** لتمكين DHCP بشكل عام على المحول. عندما يشكل مع التطفل على بروتوكول DHCP، فإن كل المنافذ في شبكة VLAN تكون غير موثوق بها لردود DHCP. هنا، فقط ال FastEthernet قارن 3/0/1 يربط إلى ال DHCP نادل شكلت ك موثوق.

التطفل على بروتوكول DHCP

```
Cat3750#conf t
Enter configuration commands, one per line.  End with
.CNTL/Z
Cat3750(config)#ip dhcp snooping
Enables DHCP snooping on the switch. ---!
Cat3750(config)#ip dhcp snooping vlan 1
DHCP snooping is not active until DHCP snooping is ---!
enabled on a VLAN. Cat3750(config)#no ip dhcp snooping
information option
Disable the insertion and removal of the option-82 ---!
field, if the !--- DHCP clients and the DHCP server
reside on the same IP network or subnet.
Cat3750(config)#interface fastEthernet 1/0/3
Cat3750(config-if)#ip dhcp snooping trust
Configures the interface connected to the DHCP ---!
server as trusted. Cat3750#show ip dhcp snooping
Switch DHCP snooping is enabled
:DHCP snooping is configured on following VLANs
1
Insertion of option 82 is disabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                    Trusted    Rate limit
((pps
---------------     -------     -----------------------
-
FastEthernet1/0/3            yes         unlimited
Displays the DHCP snooping configuration for the ---!
switch. Cat3750#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type
VLAN  Interface
-------  ----------  ---------------  ------------------
--------------------  ----  ------
A5:7B:F5     10.0.0.2        86391       dhcp-:00:11:85
snooping  1    FastEtheret1/0/1
00:11:85:8D:9A:F9     10.0.0.3        86313       dhcp-
snooping  1    FastEtheret1/0/2
Total number of bindings: 2
Displays the DHCP snooping binding entries for the ---!
switch. Cat3750# !--- DHCP server(s) connected to the
untrusted port will not be able !--- to assign IP
.addresses to the clients
```

راجع تكوين ميزات DHCP للحصول على مزيد من المعلومات.

فحص ARP (بروتوكول تحليل العناوين) الديناميكي

فحص ARP الديناميكي هو ميزة أمان تتحقق من حزم ARP في شبكة. وهو يعترض حزم ARP وتسجيلها ويتجاهلها باستخدام روابط عنوان IP إلى MAC غير صحيحة. هذه الإمكانية تحمي الشبكة من بعض هجمات الدخيل.

يضمن فحص ARP الديناميكي إرسال طلبات ARP واستجاباتها الصالحة فقط. ينجز المفتاح هذا نشاط:

- يعترض جميع طلبات ARP واستجاباتها على المنافذ غير الموثوق بها
- يتحقق من أن كل حزمة من هذه الحزم التي تم اعتراضها تحتوي على عنوان IP إلى MAC صالح قبل أن يقوم بتحديث ذاكرة تخزين ARP المحلية أو قبل أن يقوم بإعادة توجيه الحزمة إلى الوجهة المناسبة
- إسقاط حزم ARP غير الصالحة

يحدد الفحص الديناميكي ل ARP صحة حزمة ARP استنادا إلى روابط عنوان IP إلى MAC صالحة مخزنة في قاعدة بيانات موثوق بها، وهي قاعدة بيانات ربط التطفل على بروتوكول DHCP. يتم إنشاء قاعدة البيانات هذه بواسطة

التطفل على بروتوكول DHCP إذا تم تمكين التطفل على بروتوكول DHCP على شبكات VLAN وعلى المحول. إذا تم إستلام حزمة ARP على واجهة موثوق بها، سيقوم المحول بإعادة توجيه الحزمة دون أي عمليات تحقق. على الواجهات غير الموثوق بها، يقوم المحول بإعادة توجيه الحزمة فقط إذا كانت صحيحة.

في بيئات غير DHCP، يمكن أن يتحقق الفحص الديناميكي ل ARP من صحة حزم ARP مقابل قوائم التحكم في الوصول ل ARP التي يتم تكوينها من قبل المستخدم للمضيفين الذين لديهم عناوين IP مكونة بشكل ثابت. يمكنك إصدار أمر التكوين العام **arp access-list** من أجل تحديد قائمة التحكم في الوصول (ACL) ل ARP. تكون لقوائم التحكم في الوصول ل ARP الأولوية على الإدخالات في قاعدة بيانات ربط التطفل على بروتوكول DHCP. يستخدم المحول قوائم التحكم في الوصول (ACLs) فقط إذا قمت بإصدار أمر التكوين العام **ip arp inspection filter vlan** لتكوين قوائم التحكم في الوصول (ACLs). يقوم المحول أولا بمقارنة حزم ARP بقوائم التحكم في الوصول (ACL) ل ARP التي قام المستخدم بتكوينها. إذا رفضت قائمة التحكم في الوصول ل ARP حزمة ARP، فإن المحول ينكر أيضا الحزمة حتى إذا كان هناك ربط صالح في قاعدة البيانات التي تم إنشاؤها بواسطة التطفل على بروتوكول DHCP.

راجع إرشادات تكوين الفحص الديناميكي ل ARP للحصول على الإرشادات حول كيفية تكوين فحص ARP الديناميكي.

يتم إصدار أمر التكوين العام **ip arp inspection vlan** لتمكين الفحص الديناميكي ل ARP لكل شبكة محلية ظاهرية (VLAN). هنا، فقط يتم تكوين واجهة FastEthernet 1/0/3 المتصلة بخادم DHCP على أنها موثوق بها باستخدام الأمر **ip arp inspection** trust. يجب تمكين التطفل على بروتوكول DHCP للسماح لحزم ARP التي تحتوي على عناوين IP معينة بشكل ديناميكي. رأيت ال DHCP يتطفل قسم من هذا وثيقة ل DHCP يتطفل تشكيل معلومة.

فحص ARP (بروتوكول تحليل العناوين) الديناميكي

```
Cat3750#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Cat3750(config)#ip arp inspection vlan 1
Enables dynamic ARP inspection on the VLAN. ---!
Cat3750(config)#interface fastEthernet 1/0/3
Cat3750(config-if)#ip arp inspection trust
Configures the interface connected to the DHCP ---!
server as trusted. Cat3750#show ip arp inspection vlan 1

  Source Mac Validation      : Disabled
  Destination Mac Validation : Disabled
  IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match  Static ACL
 ---------   ---------    -------------     ----  ----------
                 Enabled          Active     1

 Vlan     ACL Logging      DHCP Logging
 ------------      -----------     ----
                Deny             Deny     1
Verifies the dynamic ARP inspection configuration. ---!
Cat3750#
```

راجع تكوين الفحص الديناميكي ل ARP للحصول على مزيد من المعلومات.

واقي مصدر بروتوكول الإنترنت

واقي مصدر بروتوكول الإنترنت هو ميزة أمان تعمل على تصفية حركة المرور استنادا إلى قاعدة بيانات ربط التطفل على بروتوكول DHCP وعلى روابط مصدر IP التي تم تكوينها يدويا لتقييد حركة مرور IP على واجهات الطبقة 2 غير

الموجهة. يمكنك إستخدام واقي مصدر بروتوكول الإنترنت لمنع هجمات حركة المرور التي تحدث عندما يحاول مضيف إستخدام عنوان IP الخاص بجاره. يمنع واقي مصدر بروتوكول الإنترنت انتحال عناوين IP/MAC.

يمكنك تمكين واقي مصدر بروتوكول الإنترنت عندما يتم تمكين التطفل على بروتوكول DHCP على واجهة غير موثوق بها. بعد تمكين واقي مصدر بروتوكول الإنترنت على واجهة، يقوم المحول بحظر جميع حركة مرور IP التي يتم استقبالها على الواجهة، باستثناء حزم DHCP التي يتم السماح بها بواسطة التطفل على بروتوكول DHCP. يتم تطبيق قائمة التحكم في الوصول (ACL) الخاصة بالمنفذ على الواجهة. تسمح قائمة التحكم في الوصول الخاصة بالمنفذ بحركة مرور IP فقط مع عنوان IP للمصدر في جدول ربط مصدر IP وترفض جميع حركات المرور الأخرى.

يحتوي جدول ربط مصدر IP على روابط تم التعرف عليها بواسطة التطفل على بروتوكول DHCP أو تم تكوينها يدويا (روابط مصدر IP الثابتة). يحتوي أحد الإدخالات في هذا الجدول على عنوان IP وعنوان MAC المقترن به ورقم شبكة VLAN المقترن به. يستخدم المحول جدول ربط مصدر IP فقط عند تمكين واقي مصدر IP.

يمكنك تكوين واقي مصدر IP باستخدام تصفية عنوان IP للمصدر، أو باستخدام تصفية عنوان IP و MAC للمصدر. عندما يتم تمكين واقي مصدر بروتوكول الإنترنت مع هذا الخيار، تتم تصفية حركة مرور IP استنادا إلى عنوان IP للمصدر. يقوم المحول بإعادة توجيه حركة مرور IP عندما يتطابق عنوان IP للمصدر مع إدخال في قاعدة بيانات ربط التطفل على بروتوكول DHCP أو ربط في جدول ربط مصدر IP. عندما يتم تمكين واقي مصدر بروتوكول الإنترنت مع هذا الخيار، تتم تصفية حركة مرور IP استنادا إلى عناوين IP و MAC للمصدر. يقوم المحول بإعادة توجيه حركة مرور البيانات فقط عندما تطابق عناوين IP و MAC للمصدر إدخالا في جدول ربط مصدر IP.

ملاحظة: يتم دعم واقي مصدر بروتوكول الإنترنت فقط على منافذ الطبقة 2، والتي تتضمن منافذ الوصول وخطوط الاتصال.

ارجع إلى إرشادات تكوين واقي مصدر بروتوكول الإنترنت للحصول على إرشادات حول كيفية تكوين واقي مصدر بروتوكول الإنترنت.

هنا، تم تكوين واقي مصدر IP مع تصفية IP للمصدر على واجهة FastEthernet 1/0/1 باستخدام الأمر **ip verify source**. عندما يتم تمكين واقي مصدر بروتوكول الإنترنت مع تصفية IP للمصدر على شبكة VLAN، يجب تمكين التطفل على بروتوكول DHCP على شبكة VLAN الخاصة بالوصول التي تنتمي إليها الواجهة. قم بإصدار الأمر **show ip verify source** للتحقق من تكوين واقي مصدر بروتوكول الإنترنت على المحول.

واقي مصدر بروتوكول الإنترنت

```
Cat3750#conf t
Enter configuration commands, one per line.  End with
.CNTL/Z
Cat3750(config)#ip dhcp snooping
Cat3750(config)#ip dhcp snooping vlan 1
See the DHCP Snooping section of this document for ---!
!--- DHCP snooping configuration information.
Cat3750(config)#interface fastEthernet 1/0/1
Cat3750(config-if)#ip verify source
Enables IP source guard with source IP filtering. ---!
Cat3750#show ip verify source
        Interface  Filter-type  Filter-mode  IP-address
                                Mac-address        Vlan
--  ---------------  -----------  -----------  ---------
                                 -----  ---------------
            Fa1/0/1    ip           active       10.0.0.2
                                                        1
        For VLAN 1, IP source guard with IP address ---!
    filtering is configured !--- on the interface and a
            binding exists on the interface. Cat3750#
```

راجع فهم واقي مصدر بروتوكول الإنترنت للحصول على مزيد من المعلومات.

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- تأمين الشبكات باستخدام شبكات VLAN الخاصة وقوائم التحكم في الوصول إلى شبكة VLAN
- دعم منتجات الشبكات المحلية (LAN)
- دعم تقنية تحويل شبكات LAN
- 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).