أفضل الممارسات للمحولات من السلسلة Catalyst 4500/4000 و Catalyst 6500/6000 Series Switches التي تشغل برنامج Cisco IOS Software

المحتويات

معلومات ذات صلة

المقدمة

يزود هذا وثيقة أفضل ممارسة لمادة حفازة 6000/6500 و 4000/4500 sery مفتاح أن يركض cisco ios ® برمجية على المشرف محرك.

المادة حفازة 6000/6500 ومادة حفازة 4000/4500 sery يساند مفتاح واحد من هذا إثنان نظام تشغيل أن يركض على المشرف محرك:

- نظام التشغيل CatOS) Catalyst)
- برنامج IOS من Cisco

باستخدام نظام التشغيل CatOS، هناك الخيار لتشغيل برنامج Cisco IOS Software على بطاقات أو وحدات التوجيه التابعة مثل:

- متعدد طبقات مفتاح سمة بطاقة (MSFC) في المادة حفازة 6000/6500
- الوحدة النمطية 4232 طبقة 3 (L3) في المادة حفازة 4000/4500

في هذا الوضع، هناك سطرا أوامر للتكوين:

- سطر أوامر CatOS للتحويل
- سطر أوامر برنامج Cisco IOS Software للتوجيه

CatOS هو النظام برمجية، أي يركض على المشرف محرك. برنامج Cisco IOS Software الذي يتم تشغيله على وحدة التوجيه النمطية هو خيار يتطلب برنامج CatOS system.

بالنسبة لبرنامج Cisco IOS Software، هناك سطر أوامر واحد فقط للتكوين. في هذا الوضع، تم دمج وظائف CatOS في برنامج Cisco IOS. ينتج عن التكامل سطر أوامر واحد لكل من تكوين التوجيه والتحويل. في هذا الوضع، يكون برنامج Cisco IOS هو برنامج النظام، ويحل محل CatOS.

يتم نشر كل من أنظمة التشغيل CatOS و Cisco IOS Software في الشبكات الحساسة. يتم دعم نظام التشغيل CatOS، مع خيار برنامج Cisco IOS لبطاقات ووحدات الموجه التابعة، في سلسلة المحولات التالية:

- Catalyst 6500/6000
- Catalyst 5500/5000
- Catalyst 4500/4000

يتم دعم برنامج Cisco IOS System في سلسلة المحولات التالية:

- Catalyst 6500/6000
- Catalyst 4500/4000

أحلت الوثيقة أفضل ممارسة لمادة حفازة 4000/4500، 5000/5500، و 6000/6500 sery مفتاح يركض CatOS تشكيل وإدارة لمعلومة على CatOS لأن هذا وثيقة تغطية cisco ios نظام برمجية.

يوفر برنامج Cisco IOS System للمستخدمين بعض الميزات التالية:

- واجهة مستخدم واحدة
- نظام أساسي موحد لإدارة الشبكات
- مميزات جودة الخدمة المحسنة
- دعم التحويل الموزع

يوفر هذا المستند إرشادات تكوين نمطية. لذلك، يمكنك قراءة كل قسم بشكل مستقل وعمل تغييرات على نهج مرحلي. يفترض هذا المستند وجود فهم أساسي ومعرفة بواجهة مستخدم برنامج Cisco IOS. لا يغطي المستند

تصميم شبكة مجمع شامل.

قبل البدء

الخلفية

تمثل الحلول التي يقدمها هذا المستند سنوات من الخبرة الميدانية من مهندسي Cisco الذين يعملون مع الشبكات المعقدة والعديد من أكبر العملاء. وبالتالي، تؤكد هذه الوثيقة على عمليات التهيئة في العالم الواقعي التي تجعل الشبكات ناجحة. يقدم هذا المستند الحلول التالية:

- حلول لها، إحصائيا، أوسع تعرض في المجال، وبالتالي أقل المخاطر
- حلول بسيطة تقايض بعض المرونة بالنتائج القطعية
- الحلول التي تتسم بسهولة الإدارة وتكوينها فرق عمليات الشبكة
- حلول تعمل على تعزيز إمكانية التوفر الفائقة والاستقرار الفائق

المراجع

هناك كثير موقع مرجع للمادة حفازة 6000/6500 ومادة حفازة 4000/4500 منتوج خط على cisco.com. المراجع التي يسرد هذا القسم بها توفر عمق إضافي في الموضوعات التي يتناقش فيها هذا المستند.

راجع دعم تقنية تحويل شبكة LAN للحصول على مزيد من المعلومات حول أي من المواضيع التي يغطيها هذا المستند. توفر صفحة الدعم مستندات المنتج بالإضافة إلى مستندات أستكشاف الأخطاء وإصلاحها وتكوينها.

يوفر هذا المستند مراجع لمواد عامة على الإنترنت حتى يمكنك قراءة المزيد. ولكن المراجع الأساسية والتعليمية الجيدة الأخرى هي:

- أساسيات ISP من Cisco
- مقارنة بين Cisco Catalyst وأنظمة التشغيل Cisco IOS للمحولات من السلسلة Cisco Catalyst 6500 Series Switch
- تبديل الشبكة المحلية (LAN) من Cisco (سلسلة التطوير الاحترافي ل CCIE)
- إنشاء شبكات محولة متعددة الطبقات من Cisco
- إدارة الأداء والأعطال
- السلامة: مخطط أمان لشبكات المؤسسات
- دليل حقل Cisco: تكوين المحول Catalyst Switch

التكوين الأساسي

يناقش هذا قسم سمة أن يكون نشرت عندما أنت تستخدم الغالبية من مادة حفازة شبكة.

بروتوكولات مستوى التحكم Catalyst

يقدم هذا القسم البروتوكولات التي تعمل بين المحولات تحت العملية العادية. من المفيد أن تجد فهما أساسيا للبروتوكولات عند تناول كل قسم منها.

حركة مرور بيانات Supervisor Engine

تتطلب معظم الميزات التي يتم تمكينها في شبكة Catalyst تعاون محولين أو أكثر. لذلك، يجب أن يكون هناك تبادل متحكم به لرسائل keepalive، معلمات التكوين، وتغييرات الإدارة. سواء كانت هذه البروتوكولات خاصة من Cisco، مثل بروتوكول أستكشاف Cisco (CDP)، أو مستندة إلى المعايير، مثل IEEE 802.1D (بروتوكول الشجرة المتفرعة

[STP])، جميعها تحتوي على عناصر معينة مشتركة عند تنفيذ البروتوكولات على سلسلة Catalyst.

في إعادة توجيه الإطارات الأساسية، تنشأ إطارات بيانات المستخدم من الأنظمة الطرفية. لا يتم تغيير عنوان المصدر (SA) وعنوان الوجهة (DA) لإطارات البيانات عبر مجالات تحويل الطبقة 2 (L2). يتم ملء جداول البحث عن الذاكرة القابلة للتوجيه إلى المحتوى (CAM) على كل محرك مشرف على المحول بعملية تعلم SA. تشير الجداول إلى أي منفذ مخرج يرسل كل إطار يتم إستلامه. إذا كانت الوجهة غير معروفة أو تم توجيه الإطار إلى عنوان بث أو بث متعدد، فإن عملية تعلم العنوان غير مكتملة. عندما تكون العملية غير كاملة، يتم إعادة توجيه الإطار (فضت) إلى جميع المنافذ في شبكة VLAN هذه. يجب أن يتعرف المحول أيضا على الإطارات التي يجب تحويلها من خلال النظام والإطارات التي يجب توجيهها إلى وحدة المعالجة المركزية (CPU) للمحول نفسها. تعرف وحدة المعالجة المركزية للمحول أيضا بمعالج إدارة الشبكة (NMP).

يتم إستخدام الإدخالات الخاصة في جدول CAM لإنشاء مستوى التحكم في Catalyst. تسمى هذه الإدخالات الخاصة إدخالات النظام. يستلم مستوى التحكم حركة مرور البيانات ويوجهها إلى NMP على منفذ محول داخلي. وهكذا، باستخدام البروتوكولات ذات عناوين MAC للوجهة المعروفة، يمكن فصل حركة مرور مستوى التحكم عن حركة مرور البيانات.

تتضمن Cisco نطاقا محجوزا من Ethernet MAC وعناوين البروتوكول، كما يوضح الجدول في هذا القسم. يغطي هذا المستند كل عنوان محجوز بالتفصيل، ولكن يوفر هذا الجدول ملخصا لتوفير سهولة الاستخدام:

الميزة	نوع البروتوكول SNAP[1] HDLC[2]	غاية multicast MAC
PAgP[3]	0x0104	01-00-0c-cc-cc-cc
PVST+ و RPVST+[4]	0x010b	01-00-0c-cc-cd
جسر VLAN	0x010c	01-00-0c-cd-cd-ce
UDLD [5]	0x011	01-00-0c-cc-cc-cc
CDP	0x2000	01-00-0c-cc-cc-cc
DTP[6]	0x2004	01-00-0c-cc-cc-cc
بروتوكول STP Uplinkfast	0x200a	01-00-0c-cd-cd-cd
شجرة الامتداد IEEE 802.1D	N/A—DSAP[7] 42 SSAP[8] 42	01-80-c2-00-00-00
ISL[9]	غير متوفر	01-00-0c-00-00-00
VTP[10]	0x2003	01-00-0c-cc-cc-cc
IEEE Pause 802.3x	الطراز N/A—DSAP 81 SSAP 80	01-80-c2-00-00-00>0f

[1] SNAP = بروتوكول الوصول إلى الشبكة الفرعية.

[2] HDLC = تحكم إرتباط بيانات عالي المستوى.

[3] PAgP = بروتوكول تجميع المنفذ.

[4] PVST+ = لكل شبكة محلية ظاهرية (VLAN) الشجرة الممتدة+ و PVST = +RPVST+ السريع.

[5] UDLD = اكتشاف الروابط أحادي الإتجاه.

[6] DTP = بروتوكول التوصيل الديناميكي.

[7] DSAP = نقطة وصول خدمة الوجهة.

[8] SSAP = نقطة وصول خدمة المصدر.

[9] ISL = إرتباط بين المحولات.

[10] VTP = بروتوكول خط اتصال شبكة VLAN.

تستخدم معظم بروتوكولات التحكم من Cisco تضمين IEEE 802.3 SNAP، والذي يتضمن التحكم في الارتباط المنطقي (0xAAA03 (LLC ومعرف الهوية الفريد التنظيمي (0x0000c (UI. أنت يستطيع رأيت هذا على lan محلل تتبع.

وتفترض هذه البروتوكولات إمكانية الاتصال من نقطة إلى نقطة. لاحظ أن الاستخدام المتعمد لعناوين وجهة البث المتعدد يمكن محولين Catalyst من الاتصال بشفافية عبر محولات غير Cisco. حيث أن الأجهزة التي لا تفهم الإطارات وتعترض طريقها تقوم بإغراق الإطارات ببساطة. ومع ذلك، قد تؤدي الاتصالات من نقطة إلى عدة نقاط من خلال بيئات موردين متعددين إلى سلوك غير متناسق. بشكل عام، تجنب الاتصالات من نقطة إلى عدة نقاط من خلال بيئات موردين متعددين. تنتهي هذه البروتوكولات في موجهات الطبقة 3 وتعمل فقط داخل مجال محول. وتتلقى هذه البروتوكولات ترتيب الأولويات على بيانات المستخدم عن طريق معالجة وجدولة الدائرة المتكاملة الخاصة بالتطبيق (ASIC) عند الدخول.

والآن تتحول المناقشة إلى العلاقات الاجتماعية. تستخدم بروتوكولات المحول عنوان MAC الذي يتم أخذه من بنك للعناوين المتاحة. وتوفر وحدة توسعة المنافذ (EPROM) القائمة على الهيكل مجموعة العناوين المتاحة. قم بإصدار الأمر **show module** لعرض نطاقات العناوين المتاحة لكل وحدة نمطية لمصدر حركة المرور مثل وحدات بيانات بروتوكول بروتوكول (BPDUs STP) أو إطارات ISL. وهذه عينة من مخرجات الأمر:

```
show module<
…

Mod MAC-Address(es)                         Hw     Fw           Sw
---------------- ---------- ------ ---------------------------------------- ---
(00-01-c9-da-0c-1e to 00-01-c9-da-0c-1f 2.2    6.1(3)     6.1(1d   1
                                    00-01-c9-da-0c-1c to 00-01-c9-da-0c-1
                                   00-d0-ff-88-c8-00 to 00-d0-ff-88-cb-ff
                                .These are the MACs for sourcing traffic ---!
```

VLAN 1

VLAN 1 له أهمية خاصة في شبكات Catalyst.

عندما trunking، المادة حفازة مشرف يستعمل محرك دائما التقصير in order to VLAN، VLAN 1، حددت a number of control and إدارة بروتوكول. وتتضمن هذه البروتوكولات CDP و VTP و PAgP. شكلت كل مفتاح ميناء، أي يتضمن الداخلي sc0 قارن، افتراضيا أن يكون عضو من VLAN 1. تحمل جميع شنطة شبكة VLAN رقم 1 بشكل افتراضي.

هذه التعريفات ضرورية للمساعدة في توضيح بعض المصطلحات المستخدمة بشكل جيد في شبكات Catalyst:

- الإدارة VLAN حيث sc0 يقيم ل CatOS و منخفض نهاية مفتاح. أنت يستطيع غيرت هذا VLAN. ضع هذا في الاعتبار عند العمل البيني بين محولات CatOS و Cisco IOS.
- ال VLAN أهلي طبيعي ال VLAN إلى أي ميناء يرجع عندما هو ليس trunking. أيضا، ال VLAN أهلي طبيعي ال untagged VLAN على IEEE 802.1Q شنطة.

هناك عدة أسباب جيدة أن ينسق شبكة ويغير تصرف الميناء في VLAN 1:

- عندما يصبح القطر من شبكة VLAN 1، مثل أي شبكة VLAN أخرى، كبيرا بما يكفي ليكون خطرا على الاستقرار، وخاصة من منظور بروتوكول الشجرة المتفرعة (STP)، تحتاج إلى تقليم شبكة VLAN مرة أخرى. راجع واجهة إدارة المحول وقسم شبكة VLAN الأصلية للحصول على تفاصيل.
- أنت تحتاج إلى الحفاظ على بيانات مستوى التحكم على شبكة VLAN 1 منفصلة عن بيانات المستخدم لتبسيط أستكشاف الأخطاء وإصلاحها وزيادة دورات وحدة المعالجة المركزية (CPU) المتوفرة إلى الحد الأقصى. تجنب حلقات الطبقة 2 في شبكة VLAN 1 عندما تقوم بتصميم شبكات شبكات مجموعة متعددة الطبقات دون بروتوكول الشجرة المتفرعة (STP). in order to تفاديت الطبقة 2 أنشوطة، يمحو VLAN 1 يدويا من شنطة ميناء.

باختصار، لاحظ هذه المعلومات عن خطوط الاتصال:

- يتم دائما إعادة توجيه تحديثات CDP و VTP و PAgP على خطوط الاتصال باستخدام علامة VLAN 1. هذا هو الحالة even if VLAN 1 يتلقى يكون مسح من شنطة ولا ال VLAN أهلي طبيعي. إن يمسح أنت VLAN 1 ل مستعمل معطيات، الإجراء يتلقى ما من تأثير على التحكم مستوى حركة مرور أن يكون بعد أرسلت مع الإستعمالمن VLAN 1.
- على خط اتصال ISL، يتم إرسال حزم DTP على VLAN1. هذا هو الحالة even if VLAN 1 يتلقى يكون مسح من الشنطة ولم يعد ال VLAN أهلي طبيعي. على خط اتصال 802.1Q، يتم إرسال حزم DTP على شبكة VLAN الأصلية. هذا هو الحالة even if ال VLAN أهلي طبيعي يتلقى يكون مسحت من الشنطة.
- في PVST+، تتم إعادة توجيه وحدات بيانات بروتوكول الجسر (BPDUs) وفقا لمعيار IEEE 802.1Q دون وضع علامات على الشبكة المحلية الظاهرية (VLAN) الخاصة بالشجرة المتفرعة الشائعة 1 لإتاحة إمكانية التشغيل البيني مع الموردين الآخرين، ما لم يتم مسح شبكة VLAN 1 من خط الاتصال. هذا هو الحالة بغض النظر عن تكوين شبكة VLAN الأصلية. يتم إرسال وحدات بيانات بروتوكول الجسر (PVST (BPDUs+ من Cisco ووضع علامة عليها لجميع الشبكات المحلية الظاهرية (VLANs) الأخرى. راجع قسم بروتوكول الشجرة المتفرعة للحصول على مزيد من التفاصيل.
- 802.1s يتعدد يجسر - شجرة (BPDUs (MST دائما يرسل على VLAN 1 على كلا من ISL و 802.1Q trunks. هذا يطبق even when VLAN 1 يتلقى يكون مسح من الشنطة.
- لا يمسح أو يعجز VLAN 1 على شنطة بين MST جسر و PVST+ جسر. غير أن، في حالة تعطيل شبكة VLAN 1، يجب أن يصبح جسر MST جذر in order for all the VLANs أن يتجنب وضع جسر MST لمنافذ حدوده في حالة عدم تناسق الجذر. ارجع إلى فهم بروتوكول الشجرة المتفرعة المتعددة (802.1s) للحصول على تفاصيل.

الميزات القياسية

يركز هذا القسم من المستند على ميزات التحويل الأساسية الشائعة في أي بيئة. قم بتكوين هذه الميزات على جميع أجهزة تحويل Cisco IOS Software Catalyst في شبكة العميل.

بروتوكول خط اتصال الشبكة المحلية الظاهرية (VLAN)

الغرض

VTP مجال، أي يكون أيضا دعات VLAN إدارة مجال، شكلت من one or much يربط مفتاح عن طريق شنطة أن يتشارك ال نفسه VTP domain name. VTP مصمم للسماح للمستخدمين بإجراء تغييرات تكوين شبكة VLAN مركزيا على محول واحد أو أكثر. VTP تلقائيا يربط التغيير إلى all the آخر مفتاح في (شبكة) VTP مجال. أنت يستطيع

شكلت مفتاح أن يكون في فقط واحد VTP مجال. قبل أن يخلق أنت VLANs، حددت ال VTP أسلوب أن يكون استعملت في الشبكة.

نظرة عامة على العمليات

VTP هو بروتوكول مراسلة من الطبقة 2. VTP يدير الإضافة، الحذف، وإعادة تسمية VLANs على شبكة واسع in order to حافظت VLAN تشكيل تناسق. VTP يقلل misconfiguration وتناقضات تشكيل أن يستطيع أنتجت عدة مشكلة. تتضمن المشاكل أسماء VLAN المكررة، ومواصفات نوع VLAN غير الصحيحة، وانتهاكات الأمان.

افتراضيا، المفتاح في VTP نادل أسلوب وهو في ال ما من إدارة مجال حالة. تتغير هذه الإعدادات الافتراضية عند إستلام المحول إعلانا لمجال عبر إرتباط خط اتصال أو عند تكوين مجال إدارة.

يتصل بروتوكول VTP بين المحولات باستخدام بروتوكول MAC للبث المتعدد معروف لوجهة الإيثرنت (01-00--0c-cc cc) وبروتوكول HDLC للتوصيل من النوع 0x2003. وكما هو الحال مع البروتوكولات الأساسية الأخرى، يستخدم VTP أيضا تضمين IEEE 802.3 SNAP، والذي يتضمن 0xAAA03 LLC و 0x0000c OUI. أنت يستطيع رأيت هذا على lan محلل تتبع. لا يعمل VTP عبر منافذ غير شنطة. لذلك، لا يمكن إرسال الرسائل حتى يقوم DTP برفع خط الاتصال. VTP، in other words حمولة من isl أو 802.1Q.

تتضمن أنواع الرسائل:

- إعلانات الملخص كل 300 ثانية (ثانية)
- تعيين إعلانات فرعية وطلب إعلانات عند حدوث تغييرات
- ربط عندما VTP تقليم يكون مكنت

VTP تشكيل مراجعة رقم واحد مع كل تغيير على نادل، وينتشر هذا الجدول عبر المجال.

عند حذف شبكة VLAN، تدخل المنافذ التي كانت بمجرد عضو في شبكة VLAN حالة . بالمثل، إن يعجز مفتاح في زبون أسلوب أن يستلم ال VTP VLAN طاولة عند بدء، إما من VTP نادل أو آخر VTP زبون، كل ميناء في VLANs بخلاف التقصير VLAN 1 يكون أبطلت.

أنت يستطيع شكلت معظم مادة حفازة مفتاح أن يعمل في أي واحد من هذا VTP أسلوب:

- خادم—في وضع خادم VTP، يمكنك:خلقت VLANsتعديل شبكات VLANمحات VLANsعينت آخر تشكيل معلم، مثل VTP صيغة و VTP تقسيم، ل ال VTP كامل مجالVTP يعلن نادل عن هم VLAN تشكيل إلى آخر مفتاح في ال نفسه VTP مجال. كما تقوم خوادم VTP بمزامنة تكوين شبكة VLAN الخاصة بها مع المحولات الأخرى على أساس الإعلانات التي يتم استقبالها عبر إرتباطات خطوط الاتصال. خادم VTP هو الوضع الافتراضي.
- يتصرف عملاء VTP—العميل بنفس الطريقة التي تتصرف بها خوادم VTP. غير أنه لا يمكنك إنشاء شبكات VLAN أو تغييرها أو حذفها على عميل VTP. علاوة على ذلك، لا يتذكر العميل شبكة VLAN بعد إعادة التشغيل لأنه لا توجد معلومات شبكة VLAN مكتوبة في ذاكرة NVRAM.
- شفاف—لا تشارك مبدّلات VTP الشفافة في VTP. VTP شفاف لا يعلن مفتاح هو VLAN تشكيل ولا يزامن هو VLAN تشكيل على أساس الإعلانات المستلمة. غير أن، في VTP صيغة 2، يرسل مفتاح شفاف VTP إعلان أن المفتاح يستلم من شنطة قارن.

الميزة	الخادم	العميل	شفاف	إيقاف [1]
مصدر VTP رسالة	نعم	نعم	لا	—
يستمع إلى VTP رسالة	نعم	نعم	لا	—

خلقت VLANs	نعم	لا	نعم (المهم محليا فقط)	—
تذكر شبكات VLAN	نعم	لا	نعم (المهم محليا فقط)	—

[1] cisco ios برمجية لا يتلقى الخيار أن يعجز VTP مع إستعمال من أسلوب.

هذا الجدول هو ملخص للتكوين الأولي:

الميزة	القيمة الافتراضية
VTP domain name	فارغ (null)
vtp mode	الخادم
VTP صيغة	تم تمكين الإصدار 1
تنقية بروتوكول VTP	معطل

في VTP أسلوب شفاف، VTP يتجاهل تحديث ببساطة. أزلت ال VTP معروف multicast MAC عنوان من النظام حدبة أن يكون عادة استعملت أن ينتقي إطار تحكم ويوجههم إلى المشرف محرك. لأن البروتوكول يستعمل عنوان multicast، المفتاح في أسلوب شفاف أو آخر بائع مفتاح يفيض الإطار ببساطة إلى آخر cisco مفتاح في المجال.

VTP يتضمن صيغة 2 (VTPv2) المرونة الوظيفية أن هذا قائمة يصف. غير أن، VTPv2 ليس interoperable مع VTP صيغة 1 (VTPv1):

- دعم Token Ring
- دعم معلومات VTP غير المعروف—تقوم المحولات الآن بنشر قيم لا يمكنها تحليلها.
- الوضع الشفاف المعتمد على الإصدار—لم يعد الوضع الشفاف يتحقق من اسم المجال. وهذا يمكن دعم أكثر من مجال عبر مجال شفاف.
- نشر رقم الإصدار—إذا كان VTPv2 ممكنا على جميع المحولات، يمكن تمكين جميع المحولات مع تكوين محول واحد.

راجع فهم بروتوكول إنشاء خط اتصال شبكات VTP) VLAN) للحصول على مزيد من المعلومات.

عملية VTP في برنامج Cisco IOS

تتم كتابة تغييرات التكوين في CatOS إلى NVRAM فورا بعد إجراء تغيير. وعلى النقيض من ذلك، لا يحفظ برنامج Cisco IOS تغييرات التكوين على ذاكرة NVRAM إلا إذا قمت بإصدار الأمر VTP. **copy run start** يتطلب زبون ونادل نظام VTP تحديث من آخر VTP نادل أن يكون أنقذت فورا في NVRAM دون تدخل من المستخدم. ال VTP تحديث استوفيت متطلب في التقصير CatOS عملية، غير أن ال cisco ios برمجية تحديث نموذج يتطلب بديل تحديث عملية.

ل هذا تعديل، VLAN قدمت قاعدة معطيات داخل cisco ios برمجية لمادة حفازة 6500 كطريقة أن ينقذ فورا VTP تحديث ل VTP زبون وخوادم. في بعض الإصدارات من البرنامج، تكون قاعدة بيانات شبكة VLAN هذه في شكل ملف منفصل في ذاكرة NVRAM، يسمى ملف vlan.dat. تحقق من إصدار البرنامج الخاص بك لتحديد ما إذا كان مطلوبا إجراء عملية نسخ إحتياطي لقاعدة بيانات شبكات VLAN. أنت يستطيع شاهدت VTP/VLAN معلومة أن يكون خزنت في ال vlan.dat مبرد ل ال VTP زبون أو VTP نادل إن يصدر أنت **العرض vtp وضع** أمر.

لا يتم حفظ تكوين VTP/VLAN بالكامل في ملف تكوين بدء التشغيل في ذاكرة NVRAM عند إصدار الأمر **copy run start** على هذه الأنظمة. لا يطبق هذا إلى نظام أن يركض ك VTP شفاف. VTP نظام شفاف ينقذ ال

VTP/VLAN تشكيل كامل إلى الذو رأسمالمجازفة config مبرد في NVRAM عندما أنت تصدر **copy run start** ال أمر.

في cisco ios برمجية إطلاق أن يكون مبكر من cisco ios برمجية إطلاق 12.1(11b)E، أنت يستطيع فقط شكلت VTP و VLANs عن طريق ال VLAN قاعدة معطيات أسلوب. VLAN قاعدة معطيات أسلوب منفصل من الشامل تشكيل أسلوب. السبب ل هذا تشكيل متطلب أن، عندما أنت تشكل الأداة في VTP أسلوب نادل أو VTP أسلوب زبون، VTP مجاور يستطيع حدثت ال VLAN قاعدة معطيات ديناميكيا من خلال VTP إعلان. لا تريد نشر هذه التحديثات تلقائيا إلى التكوين. لذلك، ال VLAN لا خزنت قاعدة معطيات وال VTP معلومة في التشكيل رئيسي، غير أن يكون خزنت في NVRAM في مبرد مع الإسم vlan.dat.

يوضح هذا المثال كيفية إنشاء شبكة VLAN الخاصة بالإيثرنت في وضع قاعدة بيانات شبكات VLAN:

```
Switch#vlan database
Switch(vlan)#vlan 3
:VLAN 3 added
Name: VLAN0003
Switch(vlan)#exit
.APPLY completed
....Exiting
```

في cisco ios برمجية إطلاق 12.1(11b)E وفيما بعد، أنت يستطيع شكلت VTP و VLANs عبر VLAN قاعدة معطيات أسلوب أو من خلال الشامل تشكيل أسلوب. في VTP أسلوب نادل أو VTP أسلوب شفاف، التشكيل من VLANs بعد يحدث ال vlan.dat مبرد في ال NVRAM. ومع ذلك، لا يتم حفظ هذه الأوامر في التكوين. لذلك، لا تظهر الأوامر في التكوين الجاري تشغيله.

أحلت ال *VLAN تشكيل في شامل تشكيل أسلوب* قسم من الوثيقة بشكل VLANs ل كثير معلومة.

يوضح هذا المثال كيفية إنشاء شبكة VLAN الخاصة بالإيثرنت في وضع التكوين العام وكيفية التحقق من التكوين:

```
Switch#configure terminal
Switch(config#vtp mode transparent
.Setting device to VTP TRANSPARENT mode
Switch(config#vlan 3
Switch(config-vlan)#end
#Switch
OR
Switch#vlan database
Switch(vlan#vtp server
.Switch device to VTP SERVER mode
Switch(vlan#vlan 3
Switch(vlan#exit
.APPLY completed
....Exiting
#Switch
```

ملاحظة: ال VLAN خزنت تشكيل في ال vlan.dat مبرد، أي يكون خزنت في غير متطاير ذاكرة. in order to أنجزت نسخة إحتياطية كامل من تشكيلك، تضمنت ال vlan.dat مبرد في النسخة إحتياطية مع التشكيل. بعد ذلك، إذا كان المحول بالكامل أو وحدة Supervisor Engine (محرك المشرف) تتطلب الاستبدال، فيجب على مسؤول الشبكة تحميل كلا من هذه الملفات لاستعادة التكوين الكامل:

- ملف vlan.dat
- ملف التكوين

VTP وشبكات VLAN الموسعة

يتم إستخدام ميزة معرف النظام الموسع لتمكين تعريف شبكة VLAN الموسعة. عند تمكين معرف النظام الموسع،

فإنه يعجز تجمع عناوين MAC المستخدمة للشجرة المتفرعة للشبكة المحلية الظاهرية (VLAN)، ويترك عنوان MAC واحدا لتعريف المحول. يقدم برنامج Catalyst IOS الإصدار 12.1(EX(11b و 12.1(E(13 دعما ممتدا لمعرف النظام لمادة حفازة 6500/6000 لدعم 4096 شبكة محلية ظاهرية (VLANs) بما يتوافق مع معيار IEEE 802.1Q. قدمت هذا سمة في cisco ios برمجية إطلاق 12.1(ew(12c لمادة حفازة 4500/4000 مفتاح. يتم تنظيم شبكات VLAN هذه في نطاقات متعددة، يمكن إستخدام كل منها بشكل مختلف. استولدت بعض من هذا VLANs إلى آخر مفتاح في الشبكة عندما يستعمل أنت ال VTP. لا يتم نشر شبكات VLAN الموسعة النطاق، لذلك يجب تكوين شبكات VLAN الموسعة النطاق يدويا على كل جهاز على الشبكة. هذا موسع نظام id سمة مكافئ ل {mac address{upper خفض سمة في مادة حفازة os.

يصف هذا الجدول نطاقات VLAN:

VLANs	مدى	الاستخدام	تم النشر بواسطة VTP؟
0، 4095 م	محتفظي	لاستخدام النظام فقط. أنت يستطيع لا يرى أو يستعمل هذا VLANs.	—
1	عادي	الافتراضي من Cisco. أنت يستطيع استعمالت هذا VLAN، غير أن أنت يستطيع لا يمحو هو.	نعم
1001–2	عادي	لشبكات Ethernet VLAN. أنت يستطيع خلقت،	نعم

		استعمالت، وحذف هذا VLANs.	
10–100205	عادي	إعدادات Cisco الافتراضية لـ FDDI و Token Ring. أنت يستطيع لا يمحو VLANs 1002-1005.	نعم
40–100694	محتفظي	لشبكات Ethernet VLANs فقط.	لا

تستخدم بروتوكولات المحول عنوان MAC مأخوذ من بنك للعناوين المتاحة التي يوفرها EPROM على الهيكل كجزء من معرفات الجسر لشبكات VLAN التي تعمل تحت PVST+ و RPVST+. مادة حفازة 6500/6000 ومادة حفازة 4500/4000 مفتاح دعم إما 1024 أو 64 ماك عنوان أن يعتمد على الهيكل نوع.

لا تمكن محولات Catalyst ذات عناوين 1024 MAC معرف النظام الموسع بشكل افتراضي. يتم تخصيص عناوين MAC بشكل تسلسلي، مع تعيين عنوان MAC الأول في النطاق الذي تم تعيينه لشبكة VLAN رقم 1، وعنوان MAC الثاني في النطاق الذي تم تعيينه لشبكة VLAN رقم 2، وما إلى ذلك. هذا يمكن المفتاح أن يساند 1024 VLANs وكل VLAN يستعمل فريد جسر معين.

نوع الهيكل	عنوان الهيكل
WS-C4003-S1، WS-C4006-S2	1024

WS-C4503 و WS-C4506	641
WS-C6509-E و WS-C6509 و WS-C6509-NEB و WS-C6506-E و WS-C6506 و WS-C6009 و WS-C6006 و OSR-7609-AC و OSR-7609-DC	1024
WS-C6513، WS-C6509-NEB-A، WS-C6504-	641

E، WS-C6503-E، WS-C6503، Cisco7603، Cisco7606، Cisco7609، Cisco7613	

[1] يتيح الهيكل ذو 64 عنوانا من عناوين MAC معرف النظام الموسع بشكل افتراضي، ولا يمكن تعطيل الميزة.

راجع قسم *فهم معرف الجسر* في تكوين بروتوكول الشجرة المتفرعة (STP) و IEEE 802.1s MST للحصول على مزيد من المعلومات.

بالنسبة للمحولات من السلسلة Catalyst ذات عناوين MAC 1024، لتمكين معرف النظام الموسع، يسمح دعم 4096 شبكة محلية ظاهرية (VLANs) التي تعمل تحت مثيلات PVST+ أو 16 حالة MISTP بامتلاك معرفات فريدة دون زيادة عدد عناوين MAC المطلوبة على المحول. يقلل معرف النظام الموسع عدد عناوين MAC المطلوبة بواسطة بروتوكول الشجرة المتفرعة (STP) من عنوان واحد لكل شبكة محلية ظاهرية (VLAN) أو عنوان MISTP إلى عنوان واحد لكل محول.

يوضح هذا الشكل معرف الجسر عند عدم تمكين معرف النظام الموسع. يتكون معرف الجسر من أولوية جسر سعة 2 بايت وعنوان MAC سعة 6 بايت.

يقوم معرف النظام الموسع بتعديل جزء معرف جسر بروتوكول الشجرة المتفرعة (STP) لوحدات بيانات بروتوكول الجسر (BPDU). وينقسم حقل الأولوية الأصلي ذو 2 بايت إلى حقلين، وهما حقل أولوية جسر 4 بت وامتداد معرف النظام 12 بت الذي يسمح بترقيم شبكة VLAN من 0 إلى 4095.

عند تمكين معرف النظام الموسع على محولات Catalyst للاستفادة من شبكات VLAN ذات النطاق الموسع، يلزم تمكينه على جميع المحولات داخل مجال STP نفسه. وهذا ضروري لإبقاء حسابات جذر بروتوكول الشجرة المتفرعة (STP) ثابتة على جميع المحولات. وبمجرد تمكين معرف النظام الموسع، تصبح أولوية الجسر الرئيسي مضاعفا ل 4096 بالإضافة إلى معرف شبكة VLAN. يمكن للمحولات التي تحتوي على معرف النظام الموسع المطالبة بالجذر بشكل غير مقصود نظرا لأن لها عدة مستويات أكثر دقة في تحديد معرف الجسر الخاص بها.

بينما يوصى بالحفاظ على تكوين معرف النظام الموسع المتسق داخل مجال بروتوكول الشجرة المتفرعة (STP) نفسه، فمن غير العملي فرض معرف النظام الموسع على جميع أجهزة الشبكة عند تقديم هيكل جديد بعنوان MAC 64 إلى مجال STP. ولكن من المهم أن نفهم أنه عندما يتم تكوين نظامين بنفس أولوية الشجرة المتفرعة، فإن النظام بدون معرف النظام الموسع له أولوية أفضل للشجرة المتفرعة. أصدرت هذا أمر in order to مكنت موسع نظام id تشكيل:

Spanning-Tree Extend System-id

يتم تخصيص شبكات VLAN الداخلية بترتيب تصاعدي، بدءا من شبكة VLAN رقم 1006. من المستحسن أن يعين المستعمل VLANs أقرب إلى VLAN 4094 ممكن in order to تفاديت تعارض بين المستعمل VLANs و VLANs داخلي. أصدرت الأمر **عرض vlan إستعمال داخلي** على مفتاح in order to عرضت VLANs يعين داخليا.

```
Switch#show vlan internal usage

                                VLAN Usage
---------------------- ----
   online diag vlan0 1006
   online diag vlan1 1007
   online diag vlan2 1008
   online diag vlan3 1009
   online diag vlan4 1010
   online diag vlan5 1011
(PM vlan process (trunk tagging 1012
                Port-channel100 1013
        Control Plane Protection 1014
L3 multicast partial shortcuts for VPN 0 1015
                    vrf_0_vlan0 1016
            Egress internal vlan 1017
        Multicast VPN 0 QOS vlan 1018
IPv6 Multicast Egress multicast 1019
         GigabitEthernet5/1 1020
                   ATM7/0/0 1021
                 ATM7/0/0.1 1022
          FastEthernet3/1 1023
          FastEthernet3/2 1024
          ------deleted------
```

في IOS الأصلي، يمكن تكوين **سياسة توزيع داخلي لشبكة VLAN** بحيث يتم تخصيص شبكات VLAN الداخلية بترتيب تنازلي. معادل واجهة سطر الأوامر (CLI) لبرنامج CatOS غير مدعوم رسميا.

vlan داخلي توزيع سياسة تنازلي

[توصية تكوين Cisco]

VLANs يستطيع كنت خلقت عندما مادة حفازة 6000/6500 في VTP نادل أسلوب، even without VTP domain name. شكلت ال VTP domain name أولا، قبل أن أنت تشكل VLANs على مادة حفازة 6000/6500 مفتاح أن يركض cisco ios نظام برمجية. يحافظ التكوين في هذا الترتيب على التناسق مع محولات Catalyst الأخرى التي تعمل بنظام التشغيل CatOS.

هناك ما من توصية خاص على ما إذا أن يستعمل VTP زبون/نادل أسلوب أو VTP . يفضل بعض العملاء سهولة إدارة وضع عميل/خادم VTP، على الرغم من بعض الاعتبارات التي يلاحظها هذا القسم. الموصى به هو وجود محولين في وضع الخادم في كل مجال للتكرار، وهما عادة المحولان من طبقة التوزيع. ثبتت الإستراحة من المفتاح في المجال إلى زبون أسلوب. عندما يطبق أنت زبون/نادل أسلوب مع الإستعمالمن VTPv2، تذكرت أن أعلى مراجعة رقم يكون دائما مقبول في ال نفسه VTP مجال. إن قدمت مفتاح أن يكون شكلت في إما VTP زبون أو نادل أسلوب داخل ال VTP مجال ويتلقى أعلى مراجعة رقم من ال VTP نادل أن يتواجد، هذا overwrite ال VLAN قاعدة معطيات ضمن ال VTP مجال. إذا كان تغيير التكوين غير مقصود وتم حذف شبكات VLAN، فقد تتسبب هذه الكتابة

فوق هذا في انقطاع كبير في الشبكة. in order to ضمنت أن زبون أو نادل مفتاح دائما يتلقى تشكيل مراجعة رقم أن يكون أقل من أن نادل، غيرت الزبون VTP domain name إلى شيء آخر غير الإسم معياري، وبعد ذلك رجعت إلى القياسي. يعمل هذا الإجراء على تعيين مراجعة التكوين على العميل إلى 0.

هناك إيجابيات وسلبيات إلى ال VTP قدرة أن يجعل تغير بسهولة على شبكة. تفضل العديد من المؤسسات اتباع نهج حذر وتستخدم وضع VTP لهذه الأسباب:

- تشجع هذه الممارسة التحكم في التغيير الجيد لأنه يجب إعتبار متطلب تعديل شبكة VLAN على منفذ محول أو خط اتصال محول واحد في كل مرة.
- VTP أسلوب شفاف يحد من خطر خطأ مسؤول، مثل حذف عارض من VLAN. يمكن أن تؤثر هذه الأخطاء على المجال بأكمله.
- يمكن تنقيح شبكات VLAN من خطوط الاتصال لأسفل إلى المحولات التي لا تحتوي على منافذ في شبكة VLAN. ويؤدي ذلك إلى حدوث فيضانات في الإطارات لزيادة كفاءة عرض النطاق الترددي. كما يحتوي التشذيب اليدوي على قطر شجرة متفرعة منخفض. راجع قسم بروتوكول التوصيل الديناميكي للحصول على مزيد من المعلومات. كما يشجع تكوين شبكة VLAN لكل محول هذه الممارسة.
- هناك ما من خطر التقديم داخل الشبكة من مفتاح جديد مع أعلى VTP مراجعة رقم أن overwrite ال domain VLAN تشكيل كامل.
- cisco ios برمجية VTP أسلوب شفاف ساندت في حرم جامعي مدير 3.2، أي يكون جزء من ciscoWorks2000. الحصر سابق أن يتطلب أنت أن يتلقى على الأقل واحد نادل في VTP مجال يتلقى يكون أزلت.

أوامر VTP	التعليقات
vtp domain *name*	يتحقق بروتوكول CDP من الاسم للمساعدة في منع عمليات الكبلات بين المجالات. أسماء المجالات حساسة لحالة الأحرف.
vtp mode {server | العميل | شفاف}	يعمل VTP في أحد الأوضاع الثلاثة.
vlan *vlan_number*	يقوم هذا

	بإنشاء شبكة VLAN بالمعرف المتوفر.
switchport trunk allowed *vlan_range*	هذا أمر واجهة يمكن شنطة أن تحمل VLANs حيث يحتاج. التقصير كل VLANs.
switchport trunk pruning *vlan_range*	هذا أمر واجهة يحدد قطر بروتوكول الشجرة المتفرعة (STP) عن طريق التشذيب اليدوي، مثل خطوط الاتصال من طبقة التوزيع إلى طبقة الوصول، حيث لا توجد شبكة VLAN. بشكل افتراضي، تكون جميع

	شبكات VLAN مؤهلة للعمل كشبكات محلية ظاهرية.

خيارات أخرى

VTPv2 هو متطلب في بيئات Token Ring، حيث ينصح بشدة بوضع العميل/الخادم.

يدعو قسم توصيات التكوين من Cisco في هذا المستند إلى فوائد شبكات VLAN التشظية للحد من فيض الإطارات غير الضروري. ال **vtp يقضب** أمر VLANs تلقائيا، أي يوقف الإعصار غير فعال يفيض من إطار حيث هم لا يحتاج.

ملاحظة: على عكس التشذيب اليدوي للشبكة المحلية الظاهرية (VLAN)، لا يحد التشذيب التلقائي من قطر الشجرة الممتدة.

أنتج IEEE بنية مستندة إلى المعايير من أجل تحقيق نتائج مشابهة VTP. كعضو في بروتوكول تسجيل السمات العامة (GARP) وفقا لمعيار 802.1Q، يتيح بروتوكول التسجيل لشبكة VLAN العامة (GVRP) إمكانية التشغيل البيني لإدارة شبكة VLAN بين الموردين. مهما، GVRP خارج نطاق هذا وثيقة.

ملاحظة: لا يحتوي برنامج Cisco IOS على إمكانية وضع إيقاف تشغيل VTP، وهو يدعم VTPv1 و VTPv2 فقط مع التشذيب.

التفاوض التلقائي السريع لشبكة الإيثرنت

الغرض

تعد التفاوض التلقائي وظيفة إختيارية لمعيار الإيثرنت السريع (IEEE 802.3u FE). تتيح ميزة التفاوض التلقائي للأجهزة إمكانية تبادل المعلومات تلقائيا حول إمكانيات السرعة والإرسال ثنائي الإتجاه عبر إرتباط ما. تعمل التفاوض التلقائي في الطبقة الأولى (L1). يتم إستهداف الوظيفة عند المنافذ التي يتم تخصيصها للمناطق التي يتصل فيها المستخدمون العابرون أو الأجهزة العابرة بشبكة ما. وتتضمن الأمثلة محولات طبقة الوصول ولوحات التوزيع.

نظرة عامة على العمليات

يستخدم التفاوض التلقائي إصدارا معدلا من إختبار سلامة الارتباط لأجهزة 10BASE-T للتفاوض حول السرعة وتبادل معلمات التفاوض التلقائي الأخرى. يشير إختبار سلامة الارتباط 10BASE-T الأصلي إلى NLP. وبشار إلى الإصدار المعدل من إختبار سلامة الارتباط للوصول التلقائي إلى 100/10 ميجابت في الثانية باسم FLP (Fast Link Pulse). تتوقع أجهزة 10BASE-T تدفق نبضة كل 16 مللي ثانية (+/-8) كجزء من إختبار سلامة الارتباط. يرسل FLP الخاص بالتشغيل التلقائي 100/10 ميجابت في الثانية هذه النوبات كل 16 مللي ثانية (+/-8) مع النبضات الإضافية كل 62.5 (+/-7) ميكروثانية. تقوم النبضات الموجودة ضمن تسلسل الاندفاع بإنشاء كلمات التعليمات البرمجية التي يتم إستخدامها لتبادل التوافق بين شركاء الارتباط.

في منفذ 10BASE-T، يتم إرسال نبضة إرتباط للخارج كلما ظهرت محطة. هذه نبضة واحدة ترسل كل 16 ميللي ثانية. كما تقوم أجهزة 10BASE-T بإرسال نبضة إرتباط كل 16 مللي ثانية عندما يكون الارتباط خاملا. وتسمى أيضا نبضات الوصلات هذه بنبضات القلب أو NLP.

يرسل جهاز 100BASE-T FLP. ويطلق هذا النبض في شكل انفجار بدلا من نبض واحد. ويتم إكمال الانفجار في

غضون 2 ميللي ثانية ويتم تكراره مرة أخرى كل 16 ميللي ثانية. عند التهيئة، يرسل الجهاز رسالة FLP ذات 16 بت إلى شريك الارتباط للتفاوض على السرعة والإرسال ثنائي الإتجاه والتحكم في التدفق. يتم إرسال هذه الرسالة ذات 16 بت بشكل متكرر حتى يتم التعرف على الرسالة من قبل الشريك.

ملاحظة: وفقا لمواصفات IEEE 802.3u، لا يمكنك تكوين شريك إرتباط واحد يدويا للإرسال ثنائي الإتجاه الكامل بسرعة 100 ميجابت في الثانية مع الاستمرار في عمل التفاوض التلقائي على الإرسال ثنائي الإتجاه الكامل مع شريك الارتباط الآخر. تؤدي محاولة تكوين شريك إرتباط واحد للإرسال ثنائي الإتجاه الكامل بسرعة 100 ميجابت في الثانية وشريك الارتباط الآخر للإرسال التلقائي إلى عدم تطابق الإرسال ثنائي الإتجاه. نتائج عدم تطابق الإرسال ثنائي الإتجاه لأن أحد شركاء الارتباط التفاوض التلقائي ولا يرى أي معلمات التفاوض التلقائي من شريك الارتباط الآخر. فيتم بعد ذلك تعيين شريك الارتباط الأول افتراضيا على وضع الإرسال أحادي الإتجاه.

تدعم جميع وحدات تحويل الإيثرنت Catalyst 6500 Ethernet switching modules الإرسال أحادي الإتجاه أو الإرسال ثنائي الإتجاه الكامل بسرعة 100/10 ميجابت في الثانية. قم بإصدار الأمر **show interface capabilities** للتحقق من هذه الوظيفة على محولات Catalyst الأخرى.

ينشأ أحد أكثر أسباب مشاكل الأداء شيوعا على روابط إيثرنت بسرعة 100/10 ميجابت في الثانية عندما يعمل منفذ واحد على الارتباط بنظام الإرسال أحادي الإتجاه بينما يعمل المنفذ الآخر بنظام الإرسال ثنائي الإتجاه الكامل. يحدث هذا الموقف أحيانا عند إعادة ضبط أحد المنفذين أو كليهما على رابط ولا تؤدي عملية التفاوض التلقائي إلى نفس التكوين لكلا شريكي الارتباط. يحدث الموقف أيضا عند إعادة تكوين جانب واحد من الرابط ونسيان إعادة تكوين الجانب الآخر. يمكنك تجنب الحاجة إلى إجراء مكالمات دعم متعلقة بالأداء إذا:

- إنشاء سياسة تتطلب تكوين المنافذ للسلوك المطلوب لجميع الأجهزة غير العابرة
- فرض السياسة مع إتخاذ تدابير كافية لمراقبة التغيير

الأعراض النموذجية لتسلسل فحص زيادة الإطار (FCS)، التحقق الدوري من التكرار (CRC)، المحاذاة، أو عدادات الحزم الصغيرة على المحول.

في وضع الإرسال أحادي الإتجاه، لديك زوج واحد من التلقي وزوج واحد من أسلاك الإرسال. لا يمكن إستخدام كلا السلكين في نفس الوقت. يتعذر على الجهاز الإرسال عند وجود حزمة على جانب التلقي.

في وضع الإرسال ثنائي الإتجاه الكامل، لديك نفس زوج أسلاك الاستقبال والبث. ومع ذلك، يمكن إستخدام كليهما في نفس الوقت بسبب تعطيل وظائف "إستشعار الناقل" و"اكتشاف التصادم". يمكن أن يبث الجهاز ويستلم في نفس الوقت.

وبالتالي، يعمل اتصال أحادي الإتجاه بالإرسال ثنائي الإتجاه الكامل، ولكن هناك عدد كبير من التصادمات في جانب الإرسال أحادي الإتجاه التي ينتج عنها أداء ضعيف. يقع الإصطدام لأن الأداة أن يكون شكلت ك full-duplex يستطيع بثت في نفس الوقت أن الأداة يستلم بيانات.

تناقش الوثائق الواردة في هذه القائمة التفاوض التلقائي بالتفصيل. توضح هذه المستندات كيفية عمل التفاوض التلقائي وتناقش خيارات التكوين المختلفة:

- تكوين إيثرنت 1000Mb/100/10 التفاوض التلقائي للإرسال أحادي/مزدوج الاتجاه واستكشاف أخطائه وإصلاحها
- استكشاف أخطاء توافق محولات Cisco Catalyst Switches مع بطاقة واجهة الشبكة (NIC) وإصلاحها

من الأفكار الخاطئة الشائعة حول التفاوض التلقائي أنه من الممكن تكوين شريك إرتباط واحد يدويا للإرسال ثنائي الإتجاه الكامل بسرعة 100 ميجابت في الثانية والإصدار التلقائي إلى الإرسال ثنائي الإتجاه الكامل مع شريك الارتباط الآخر. وفي الواقع، ينتج عن محاولة القيام بهذا عدم تطابق في الإرسال ثنائي الإتجاه. وهذه نتيجة لأن أحد شركاء الارتباط التلقائي لا يرى أي معلمات التفاوض التلقائي من شريك الارتباط الآخر، كما أنه يتم تعيينه افتراضيا على وضع الإرسال أحادي الإتجاه.

تدعم معظم وحدات الإيثرنت Catalyst Ethernet modules الإرسال أحادي الإتجاه/الكامل بسرعة 100/10 ميجابت في الثانية. مهما، أنت يستطيع أكدت هذا إن يصدر أنت **العرض قارن capabilities** *mod/port* أمر.

فيفي

تحمي الإشارة إلى الأعطال الطرفية البعيدة (FEFI) الواجهات 100BASE-FX (الليفية) و Gigabit، بينما تحمي التفاوض التلقائي 100BASE-TX (النحاسية) ضد الأعطال المادية المتعلقة بالطبقة/الإشارات.

الخطأ الطرفي البعيد هو خطأ في الارتباط الذي يمكن لإحدى المحطات كشفه بينما لا يمكن للمحطة الأخرى كشفه. على سبيل المثال، سلك إرسال غير متصل. في هذا المثال، لا تزال محطة الإرسال تتلقى بيانات صالحة وتكشف عن أن الارتباط جيد عبر مراقبة تكامل الارتباط. ومع ذلك، لا يمكن لمحطة الإرسال اكتشاف أن المحطة الأخرى لا تتلقى الإرسال. بإمكان محطة 100BASE-FX التي تكتشف خطأ عن بعد كهذا تعديل الدفق الذي يتم نقله من أجل إرسال نمط بت خاص لإعلام المجاور بالخطأ عن بعد. ويشار إلى نمط بت الخاص باسم نمط FEFI. يؤدي نمط FEFI بعد ذلك إلى تشغيل إيقاف تشغيل المنفذ البعيد (errDisable). راجع قسم اكتشاف الارتباط أحادي الإتجاه في هذا المستند للحصول على مزيد من المعلومات حول حماية الأخطاء.

دعم هذه الوحدات النمطية/الأجهزة FEFI:

- مادة حفازة 6000/6500 و 4000/4500:جميع الوحدات النمطية 100BASE-FX ووحدات GE

توصية منفذ البنية الأساسية من Cisco

تعتمد إمكانية تكوين التفاوض التلقائي على الارتباطات بسرعة 100/10 ميجابت في الثانية أو سرعة الرمز الثابت والإرسال ثنائي الإتجاه في نهاية المطاف على نوع شريك الارتباط أو الجهاز الطرفي الذي قمت بتوصيله بمنفذ محول Catalyst. التفاوض التلقائي بين الأجهزة الطرفية ومحولات Catalyst يعمل بشكل جيد بشكل عام، وتكون محولات Catalyst متوافقة مع مواصفات IEEE 802.3u. مهما، عندما شبكة قارن بطاقة (nic) أو بائع لا يصادق مفتاح تماما، مشكلة يستطيع نتجت. بالإضافة إلى ذلك، يمكن أن تتسبب الميزات المتقدمة الخاصة بالمورد التي لم يتم وصفها في مواصفات IEEE 802.3u للتشغيل التلقائي 100/10 ميجابت في الثانية في عدم توافق الأجهزة ومسائل أخرى. وتتضمن هذه الأنواع من الميزات المتقدمة تكامل الكابلات ووحدة التشغيل التلقائي. يقدم هذا المستند مثالا:

- تنبيه ميداني: مشكلة في الأداء مع بطاقات واجهة الشبكة PRO/1000T من Intel المتصلة ب CAT4K/6K

في بعض الحالات، تحتاج إلى تعيين المضيف وسرعة المنفذ ووضع الإرسال ثنائي الإتجاه. بشكل عام، أكمل الخطوات الأساسية التالية لاستكشاف الأخطاء وإصلاحها:

- تأكد من تكوين التفاوض التلقائي على كلا جانبي الارتباط أو تكوين الترميز الثابت على كلا الجانبين.
- تحقق من ملاحظات الإصدار الخاصة بالتحذيرات الشائعة.
- تحقق من إصدار برنامج تشغيل بطاقة واجهة الشبكة (NIC) أو نظام التشغيل الذي تقوم بتشغيله. غالبا ما يكون أحدث برنامج تشغيل أو حزمة تصحيح مطلوبا.

كقاعدة، أستخدم أولا التفاوض التلقائي لأي نوع من أنواع شركاء الارتباط. هناك فوائد واضحة لتكوين التفاوض التلقائي للأجهزة العابرة مثل أجهزة الكمبيوتر المحمولة. يعمل التفاوض التلقائي أيضا بشكل جيد مع الأجهزة الأخرى، على سبيل المثال:

- مع الأجهزة غير العابرة مثل الخوادم ومحطات العمل الثابتة
- من محول إلى محول
- من المحول إلى الموجه

ولكن لبعض الأسباب التي يذكرها هذا القسم، قد تنشأ قضايا خاصة بالتفاوض. ارجع إلى تكوين التفاوض التلقائي للإرسال ثنائي الإتجاه الكامل/أحادي الإتجاه واستكشاف أخطاء الإيثرنت وإصلاحها بسرعة 1000/100/10 ميجابت للحصول على الخطوات الأساسية لاستكشاف الأخطاء وإصلاحها في هذه الحالات.

تعطيل التفاوض التلقائي ل:

- المنافذ التي تدعم أجهزة البنية الأساسية للشبكة مثل المحولات والموجهات
- أنظمة طرفية غير عابرة أخرى مثل الخوادم والطابعات

ترميز السرعة ووضع الإرسال ثنائي الإتجاه ترميزا ثابتا دائما لهذه المنافذ.

قم بتكوين تكوينات الارتباط هذه يدويا بسرعة 100/10 ميجابت في الثانية للسرعة والإرسال ثنائي الإتجاه الكامل، والذي عادة ما يكون بسرعة 100 ميجابت في الثانية:

- محول إلى محول
- التبديل إلى الخادم
- محول إلى موجه

إذا تم تعيين سرعة المنفذ على "تلقائي" على منفذ إيثرنت بسرعة 100/10 ميجابت في الثانية، فسيتم تعيين كل من السرعة والإرسال ثنائي الإتجاه على "تلقائي". أصدرت هذا قارن أمر in order to ثبتت الميناء إلى تلقائي:

```
Switch(config)#interface fastethernet slot/port
Switch(config-if)#speed auto
.This is the default ---!
```

قم بإصدار أوامر الواجهة هذه لتكوين السرعة والإرسال ثنائي الإتجاه:

```
Switch(config)#interface fastethernet slot/port
{Switch(config-if)#speed {10 | 100 | auto
{Switch(config-if)#duplex {full | half
```

توصيات منفذ الوصول من Cisco

يحتاج المستخدمون النهائيون والعمال كثيرو التنقل والمضيفون العابرون إلى التفاوض التلقائي لتقليل إدارة هذه الأجهزة المضيفة إلى الحد الأدنى. يمكنك جعل التفاوض التلقائي يعمل مع محولات Catalyst أيضا. غالبا ما تكون أحدث برامج تشغيل بطاقة واجهة الشبكة (NIC) مطلوبة.

أصدرت هذا أمر شامل in order to مكنت التفاوض التلقائي للسرعة للميناء:

```
Switch(config)#interface fastethernet slot/port
Switch(config-if)#speed auto
```

ملاحظة: إذا قمت بضبط سرعة المنفذ على "تلقائي" على منفذ إيثرنت بسرعة 100/10 ميجابت في الثانية، فسيتم التفاوض التلقائي على كل من السرعة والإرسال ثنائي الإتجاه. لا يمكنك تغيير وضع الإرسال ثنائي الإتجاه لمنافذ التفاوض التلقائي.

عندما لا تتوافق بطاقات واجهة الشبكة (NIC) أو محولات المورد تماما مع مواصفات IEEE 802.3u، يمكن أن ينتج عن ذلك مشاكل. بالإضافة إلى ذلك، يمكن أن تتسبب الميزات المتقدمة الخاصة بالمورد التي لم يتم وصفها في مواصفات IEEE 802.3u للتشغيل التلقائي 100/10 ميجابت في الثانية في عدم توافق الأجهزة ومسائل أخرى. وتشتمل هذه الميزات المتقدمة على سلامة الكابلات ووحدة التشغيل التلقائي.

خيارات أخرى

عندما يتم تعطيل التفاوض التلقائي بين المحولات، يمكن أيضا فقد إشارة خطأ الطبقة 1 لمشاكل معينة. استعملت طبقة 2 بروتوكول أن يزيد كشف إخفاق مثل عدواني UDLD.

لا تكشف التفاوض التلقائي هذه الحالات، حتى عند تمكين التفاوض التلقائي:

- الميناء يصبح ب التصق ولا يستلم أو يبث
- جانب واحد من الخط مرتفع لكن الجانب الآخر انخفض
- يتم توصيل كبلات الألياف بأسلاك مختلفة

لا تكشف التفاوض التلقائي هذه المشاكل لأنها ليست في الطبقة المادية. يمكن أن تؤدي المشاكل إلى حلقات

بروتوكول الشجرة المتفرعة (STP) أو الثقوب السوداء لحركة مرور البيانات.

UDLD يستطيع كشفت all the حالة و errdisable على حد سواء الميناء على الخطوة، إن UDLD يكون شكلت على كلا غاية. بهذه الطريقة، يمنع UDLD أنشوطة STP و حركة مرور ثقوب أسود.

التفاوض التلقائي لشبكة Gigabit Ethernet

الغرض

تحتوي شبكة جيجابت إيثرنت (GE) على إجراء تشغيل تلقائي أكثر شمولا من الإجراء المستخدم لإيثرنت 100/10 ميجابت في الثانية (IEEE 802.3z). باستخدام منافذ GE، يتم إستخدام التفاوض التلقائي للتبادل:

- محددات التحكم في التدفق
- معلومات الأعطال البعيدة
- معلومات الإرسال ثنائي الإتجاه**ملاحظة:** منافذ Catalyst series GE تدعم وضع الإرسال ثنائي الإتجاه الكامل فقط.

تم إستبدال IEEE 802. 3z بمواصفات IEEE 802. 3:2000. راجع اشتراك معايير الشبكات المحلية والمنطقة الحضرية + المسودات (LAN/MAN 802s) للحصول على مزيد من المعلومات.

نظرة عامة على العمليات

على عكس التفاوض التلقائي باستخدام بطاقة FE بسرعة 100/10 ميجابت في الثانية، لا يتضمن التفاوض التلقائي على سرعة المنفذ. أيضا، لا يمكنك إصدار الأمر **set port speed** لتعطيل التفاوض التلقائي. يتم تمكين تفاوض منفذ GE بشكل افتراضي، ويجب أن يكون للمنافذ الموجودة على كلا طرفي إرتباط GE الإعداد نفسه. لا يظهر الارتباط إذا تم تعيين المنافذ في كل نهاية من الارتباط بشكل غير متناسق، مما يعني أن المعلمات المتبادلة مختلفة.

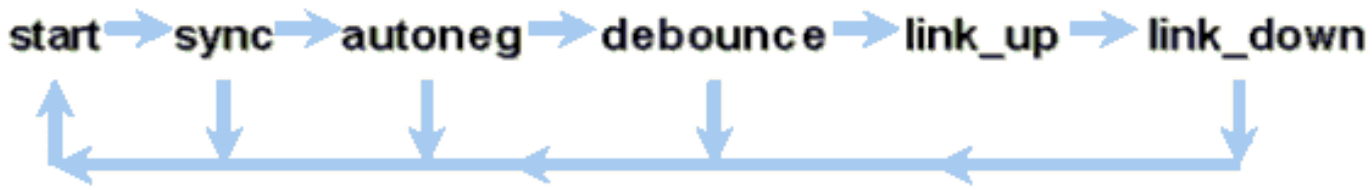
على سبيل المثال، لنفترض أن هناك جهازين، جهاز(أ) وجهاز (ب). يمكن أن يحتوي كل جهاز على التفاوض التلقائي الذي تم تمكينه أو تعطيله. هذا جدول يشتمل على عمليات تكوين محتملة، كما ينص الارتباط الخاص بها على ما يلي:

مفاوضة	تمكين B	B معطل
A ممكن	من كلا الجانبين	A down، B up
معطل	أ ب	من كلا الجانبين

في GE، يتم إجراء المزامنة والتشغيل التلقائي (في حالة تمكينها) عند بدء تشغيل الارتباط من خلال إستخدام تسلسل خاص لكلمات كود الارتباط المحجوزة.

ملاحظة: يوجد قاموس للكلمات الصحيحة، وليس كل الكلمات الممكنة صحيحة في GE.

يمكن وصف حياة اتصال GE بهذه الطريقة:



إن فقدان التزامن يعني أن جهاز MAC يكتشف الارتباط. ينطبق فقد المزامنة سواء تم تمكين التفاوض التلقائي أو تعطيله. تفقد المزامنة في ظل ظروف معينة فاشلة، مثل إستلام ثلاث كلمات غير صحيحة في تتابع. إذا إستمرت هذه الحالة لمدة 10 مللي ثانية، فسيتم تأكيد حالة فشل المزامنة ويتم تغيير الارتباط إلى حالة link_down. بعد فقدان المزامنة، يلزم وجود ثلاثة أحرف صحيحة متتابعة أخرى لإعادة التزامن. تتسبب أحداث كارثية أخرى، مثل إشارة فقدان

الاستقبال (Rx)، في حدوث حدث انسداد.

التفاوض التلقائي هو جزء من عملية الربط. عندما يكون الارتباط قيد التشغيل، يكون التفاوض التلقائي قد انتهى. ومع ذلك، لا يزال المحول يراقب حالة الارتباط. إذا تم تعطيل التفاوض التلقائي على منفذ ما، فإن مرحلة التفاوض التلقائي لم تعد خيارا.

تدعم مواصفات GE النحاسية (1000BASE-T) التفاوض التلقائي من خلال تبادل الصفحة التالية. يسمح تبادل الصفحات التالية التفاوض التلقائي لسرعات 1000/100/10 ميجابت في الثانية على المنافذ النحاسية.

ملاحظة: ومع ذلك، تنص مواصفات الألياف GE فقط على إجراء التفاوض على الإرسال ثنائي الإتجاه والتحكم في التدفق واكتشاف الأعطال عن بعد. لا تتفاوض منافذ GE الليفية على سرعة المنفذ. راجع الأقسام 28 و 37 من مواصفات IEEE 802.3-2002 للحصول على مزيد من المعلومات حول التفاوض التلقائي.

تأخير إعادة تشغيل المزامنة هي ميزة برمجية تتحكم في الوقت الإجمالي لإصدار التفاوض التلقائي. إذا لم ينجح التفاوض التلقائي خلال هذه المرة، فسيقوم البرنامج الثابت بإعادة تشغيل التفاوض التلقائي في حالة حدوث أزمة. يكون للأمر **sync-restart-delay** تأثير فقط عند تعيين التفاوض التلقائي على التمكين.

توصية منفذ البنية الأساسية من Cisco

يعد تكوين التفاوض التلقائي أمرا بالغ الأهمية في بيئة GE أكثر من أهميته في بيئة تبلغ سرعتها 100/10 ميجابت في الثانية. تعطيل التفاوض التلقائي فقط في هذه الحالات:

- على منافذ المحول التي ترتبط بأجهزة لا يمكنها دعم التفاوض
- حيث تنشأ مشكلات الاتصال من مشاكل قابلية التشغيل البيني

قم بتمكين تفاوض جيجابت على جميع الارتباطات من محول إلى محول وبشكل عام، على جميع أجهزة GE. القيمة الافتراضية على واجهات Gigabit هي التفاوض التلقائي. بعد، قم بإصدار هذا الأمر لضمان تمكين التفاوض التلقائي:

```
switch(config)#interface type slot/port
switch(config-If)#no speed
.This command sets the port to autonegotiate Gigabit parameters ---!
```

هناك إستثناء معروف عند الاتصال بموجه محول جيجابت (GSR) الذي يشغل برنامج Cisco IOS Software الذي يعد أقدم من الإصدار S(10)12.0 من برنامج Cisco IOS Software، وهو الإصدار الذي أضاف التحكم في التدفق والتشغيل التلقائي. في هذه الحالة، قم بإيقاف تشغيل هاتين الميزتين. إن لا يلتفت أنت هذا سمة، المفتاح ميناء تقارير لا يربط وال GSR يبلغ خطأ. هذا نموذج لتسلسل أوامر الواجهة:

```
flowcontrol receive off
flowcontrol send off
speed nonegotiate
```

توصيات منفذ الوصول من Cisco

ونظرا لأنه يمكن أن تختلف نقاط الوصول في الوضع Lightweight (FLPs) بين الموردين، فيجب عليك النظر في إتصالات من محول إلى خادم على أساس كل حالة على حدة. واجه عملاء Cisco بعض المشاكل مع تفاوض Gigabit على خوادم Sun و HP و IBM. اطلب من جميع الأجهزة إستخدام التفاوض التلقائي لشبكة جيجابت ما لم يذكر مورد بطاقة واجهة الشبكة (NIC) بشكل محدد خلاف ذلك.

خيارات أخرى

التحكم في التدفق هو جزء إختياري من مواصفات 802.3x. يجب أن يكون التحكم في التدفق خاضعا للتفاوض إذا

كنت تستخدمه. يمكن للأجهزة أو لا يمكن أن تكون قادرة على إرسال و/أو الاستجابة لإطار PAUSE (المعروف جيدا MAC 01-80-C2-00-00-00 0F). وقد لا توافق الأجهزة على طلب التحكم في التدفق من جالهاز الطرفي البعيد المجاور. يرسل المنفذ الذي يحتوي على مخزن إدخال مؤقت والذي يبدأ في التعبئة إطار PAUSE (إيقاف مؤقت) إلى شريك الارتباط. يقوم شريك الارتباط بإيقاف الإرسال ويحتجز أي إطارات إضافية في المخازن المؤقتة لمخرجات شريك الارتباط. لا تحل هذه الوظيفة أي مشكلة في حالة الاكتتاب الزائد. ولكن هذه الوظيفة تعمل بفعالية على زيادة سعة التخزين المؤقت للإدخال بمقدار صغير من سعة المخزن المؤقت لمخرجات الشريك طوال فترات التشغيل.

تم تصميم وظيفة PAUSE (الإيقاف المؤقت) لمنع تجاهل الإطارات المستلمة بشكل غير ضروري بواسطة الأجهزة (المحولات أو الموجهات أو المحطات الطرفية) بسبب حالات تجاوز سعة التخزين المؤقت التي تتسبب في الحمل الزائد لحركة مرور البيانات العابرة القصيرة الأجل. يمنع الجهاز تحت التحميل الزائد لحركة مرور البيانات تجاوز سعة التخزين المؤقت الداخلي عندما يرسل الجهاز إطار PAUSE (إيقاف مؤقت). يحتوي إطار PAUSE (الإيقاف المؤقت) على معلمة تشير إلى طول الوقت الذي يستغرقه شريك الإرسال ثنائي الإتجاه الكامل للانتظار قبل أن يرسل الشريك المزيد من إطارات البيانات. يتوقف الشريك الذي يستقبل إطار PAUSE (الإيقاف المؤقت) عن إرسال البيانات للفترة المحددة. عند انتهاء صلاحية المؤقت هذا، تبدأ المحطة في إرسال إطارات البيانات مرة أخرى، من المكان الذي انتهت منه المحطة.

يمكن لمحطة إصدار PAUSE (الإيقاف المؤقت) إصدار إطار PAUSE (إيقاف مؤقت) آخر يحتوي على معلمة وقت صفر. يؤدي هذا الإجراء إلى إلغاء باقي فترة الإيقاف المؤقت. لذلك، يتخطى إطار PAUSE (الإيقاف المؤقت) المستلم حديثا أي عملية PAUSE (إيقاف مؤقت) قيد التقدم حاليا. أيضا، يمكن أن تمدد المحطة التي تصدر إطار PAUSE (الإيقاف المؤقت) فترة PAUSE (الإيقاف المؤقت). تصدر المحطة إطار PAUSE (الإيقاف المؤقت) آخر يحتوي على معلمة وقت غير صفرية قبل انتهاء صلاحية فترة PAUSE (الإيقاف المؤقت الأول).

عملية PAUSE (الإيقاف المؤقت) هذه ليست رقابة على التدفق تستند إلى المعدل. العملية هي آلية إيقاف بداية بسيطة تتيح للجهاز تحت حركة مرور، والذي أرسل إطار PAUSE (الإيقاف المؤقت)، فرصة لتقليل إزدحام المخزن المؤقت الخاص به.

وأفضل إستخدام لهذه الميزة هو الارتباطات بين منافذ الوصول والمضيفين النهائيين، حيث يحتمل أن يكون المخزن المؤقت لإخراج المضيف كبيرا كالذاكرة الظاهرية. يتمتع إستخدام التحويل إلى محول بفوائد محدودة.

أصدرت هذا قارن أمر in order to ضبطت هذا على المفتاح ميناء:

```
{flowcontrol {receive | send} {off | on | desired
```

```
show port flowcontrol<
```

```
Port  Send FlowControl    Receive FlowControl   RxPause TxPause
                            admin    oper       admin    oper
------- -------     -------- --------   -------- --------  -----
      off      off        on       on           0       0   6/1
      off      off        on       on           0       0   6/2
      off      off        on       on           0       0   6/3
```

ملاحظة: تستجيب جميع وحدات Catalyst النمطية لإطار PAUSE ( ) إذا تم التفاوض بشأنه. لا تقوم بعض الوحدات النمطية (على سبيل المثال، WS-X5410 و WS-X4306) بإرسال إطارات PAUSE (الإيقاف المؤقت) أبدا، حتى إذا تفاوضت على ذلك، لأنها لا تمنع.

بروتوكول التوصيل الديناميكي

الغرض

من أجل توسيع شبكات VLAN بين الأجهزة، تقوم الشنطة مؤقتا بتعريف وتمييز (ربط محلي) إطارات الإيثرنت الأصلية. هذه العملية تمكن الإطارات من أن يتم مضاعفتها عبر رابط واحد. يضمن الإجراء أيضا أن منفصل VLAN إذاعة وأمان

مجال يكون أبقيت بين مفتاح. تحافظ جداول CAM على الإطار إلى تخطيط VLAN داخل المحولات.

نظرة عامة على العمليات

DTP هو الجيل الثاني من الارتباط بين المحولات (ISL) الديناميكي (ISL .(DISL معتمد فقط. يدعم بروتوكول DTP كلا من ISL و 802. 1Q. يضمن هذا الدعم أن المحولات في أي من نهايتي خط الاتصال تتفق على المعلمات المختلفة لإطارات الاتصال. وتتضمن هذه المعلمات ما يلي:

- نوع التضمين المكون
- شبكة VLAN الأصلية
- إمكانية إستخدام الأجهزة

يساعد دعم DTP أيضا على الحماية من غمر الإطارات المميزة بمنافذ غير شنطة، وهو ما قد يكون خطرا على الأمان. تحمي DTP من مثل هذه الفيضانات لأنها تضمن أن الموانئ وجيرانها في حالات ثابتة.

وضع التوصيل

DTP هو بروتوكول من الطبقة 2 يتفاوض مع معلمات التكوين بين منفذ المحول والجار له. يستخدم DTP عنوان MAC آخر معروف للبث المتعدد من 01-00-cc-cc-cc-0c ونوع بروتوكول SNAP من 0x2004. يصف هذا الجدول الدالة على كل من أوضاع تفاوض DTP المحتملة:

نمط	دالة	هل تم إرسال إطارات DTP؟	الحالة النهائية (المنفذ المحلي)
(مكافئ للصيغة في CatOS)	يجعل المنفذ على إستعداد لتحويل الارتباط إلى خط اتصال. يصبح الميناء شنطة ميناء إن المجاور ثبتت ميناء إلى أو أسلوب.	نعم، دوري	
(مكافئ للوضع في CatOS)	يضع المنفذ في وضع الدائم ويتفاوض على تحويل الارتباط إلى خط اتصال. يصبح الميناء شنطة ميناء المجاور even if لا يوافق ميناء إلى التغيير.	نعم، دوري	، بدون شرو ط
	يضع الميناء في وضع `trunking` دائم غير أن لا يسمح الميناء أن يلد DTP إطار.	لا	، بدون شرو ط

	أنت ينبغي يدويا شكلت الميناء مجاور كشنطة ميناء in order to خلقت شنطة خطوة. وهذا مفيد للأجهزة التي لا تدعم DTP.		
(أمر مقارنة CatOS)	يجعل المنفذ يحاول بشكل نشط تحويل الارتباط إلى إرتباط خط اتصال. يصبح الميناء شنطة ميناء إن المجاور ثبتت ميناء إلى ، ، أو auto أسلوب.	نعم، دوري	ينتهي في حالة فقط إذا كان الوض ع البعيد ، أو ، أو .
	يضع المنفذ في وضع التوصيل الدائم ويتفاوض على تحويل الارتباط إلى إرتباط غير خط اتصال. يصبح الميناء غير شنطة ميناء even if المجاور لا يوافق ميناء إلى التغيير.	لا، في حالة ثابتة، ولكن يتم إرسال المعلومات من أجل تسريع اكتشاف الطرف البعيد بعد تغيير .	trun king

ملاحظة: يمكن تعيين نوع تضمين ISL و 802.1Q أو التفاوض بشأنه.

في التكوين الافتراضي، يفترض DTP هذه الخصائص على الارتباط:

- تدعم إتصالات نقطة إلى نقطة وأجهزة Cisco منافذ خطوط اتصال 802.1Q التي تكون فقط من نقطة إلى نقطة.
- طوال تفاوض DTP، لا تشارك المنافذ في بروتوكول الشجرة المتفرعة (STP). تتم إضافة المنفذ إلى بروتوكول الشجرة المتفرعة (STP) فقط بعد أن يصبح نوع المنفذ أحد الأنواع الثلاثة التالية:وصولISL802,1qPAgP هي العملية التالية التي يتم تشغيلها قبل مشاركة المنفذ في بروتوكول الشجرة المتفرعة (STP). يتم إستخدام PAgP للتحويل التلقائي ل EtherChannel.
- VLAN 1 موجود دائما على الشنطة ميناء. إن يكون الميناء trunking في isl أسلوب، DTP ربط أرسلت على VLAN 1. إن لا يكون الميناء trunking في isl أسلوب، ال DTP يرسل ربط على ال VLAN أهلي طبيعي (ل 802.1Q trunking أو لا trunking ميناء).
- تنقل حزم DTP اسم مجال VTP، بالإضافة إلى تكوين خط الاتصال وحالة المسؤول. ال VTP domain name ينبغي طابقت in order to حصلت على شنطة فاوض أن يأتي. يتم إرسال هذه الحزم كل ثانية طوال التفاوض وكل 30 ثانية بعد التفاوض. إذا لم يكتشف منفذ ما في الوضع أو حزمة DTP في غضون 5 دقائق (كحد أدنى)، فسيتم تعيين المنفذ على أنه غير خط اتصال.

تحذير: يجب أن تفهم أن الأوضاع nonegotiate، trunk، وaccess تحدد بشكل صريح الحالة التي ينتهي فيها المنفذ. قد يؤدي التكوين السيئ إلى حالة خطيرة/غير متناسقة يكون فيها أحد الجانبين متعلقا والآخر غير مرتبط.

أحلت بشكل ISL trunking على مادة حفازة 5000/5500 و 6000/6500 عائلة مفتاح ل كثير تفصيل. أحلت trunking بين مادة حفازة 4000/4500، 5000/5500، و 6000/6500 sery مفتاح يستعمل 802.1Q عملية كبسلة مع cisco CatOS نظام برمجية ل كثير 802.1Q تفصيل.

نوع التضمين

نظرة عامة على تشغيل ISL

ISL هو بروتوكول توصيل خاص من Cisco (مخطط تضمين علامات الشبكة المحلية الظاهرية (VLAN)). وقد ظل هذا التنظيم قيد الاستخدام لسنوات عديدة. وعلى العكس من ذلك، فإن معيار 802.1Q أحدث بكثير، ولكن معيار 802.1Q هو معيار IEEE.

يقوم ISL بتضمين الإطار الأصلي بالكامل في مخطط تمييز على مستويين. وبهذه الطريقة، يعد ISL بروتوكولا للاتصال النفقي بشكل فعال، وكميزة إضافية، فإنه يحمل إطارات غير إيثرنت. يضيف ISL رأس 26 بايت و 4 FCS بايت إلى إطار الإيثرنت القياسي. تتوقع المنافذ التي تم تكوينها لتكون خط اتصال وتعالج إطارات إيثرنت الأكبر. يدعم ISL 1024 شبكة VLAN.

تنسيق الإطار - يتم تظليل علامة ISL

40 Bits	4 Bits	4 Bits	48 Bits	16 Bits	24 Bits	24 Bits	15 Bits	1 Bit	16 Bits	16 Bits
DA	Type	USER	SA	LEN	SNAP LLC	HSA	VLAN	BPDU	INDEX	Reserve
01-00-0c-00-00					AAAA03	00000C				

Encapsulated Frame	FCS
Variable length	32 bits

راجع تنسيق إطار InterSwitch و IEEE 802.1Q للحصول على مزيد من المعلومات.

802.1Q نظرة عامة على التشغيل

على الرغم من أن معيار IEEE 802.1Q يتعلق فقط بالإيثرنت، فإن المعيار يحدد أكثر بكثير من أنواع التضمين. يتضمن معيار 802.1Q، من بين بروتوكولات تسجيل السمات العامة (GARPs) الأخرى، تحسينات الشجرة المتفرعة ووضع علامات جودة الخدمة 802.1p. راجع معايير IEEE Standard Online للحصول على مزيد من المعلومات

يحافظ تنسيق إطار 802. 1Q على بروتوكولات SA و DA الخاصة بالإيثرنت الأصلية. ومع ذلك، يجب أن تتوقع المحولات الآن إستقبال الإطارات الصغيرة العملاقة، حتى على منافذ الوصول حيث يمكن للمضيفين إستخدام وضع العلامات للتعبير عن أولوية المستخدم وفقا لمعيار 802.1p لإرسال إشارات جودة الخدمة. العلامة هي 4 بايت. يبلغ حجم إطارات الإصدار الثاني من شبكة إيثرنت لشبكة 802.1Q 1522 بايت، وهو ما يعد إنجازا حققته مجموعة العمل

وفقا لمعيار IEEE 802.3ac. كما يدعم معيار 802. 1Q مساحة الترقيم لشبكة محلية ظاهرية (VLANs) بسرعة 4096.

كل إطارات البيانات التي يتم إرسالها واستقبالها هي 802.1Q ذات علامات تمييز، ماعدا إطارات البيانات تلك التي تكون على شبكة VLAN الأصلية. في هذه الحالة، هناك علامة ضمني أن يكون بناءا على المدخل مفتاح تشكيل ميناء. ترسل الإطارات على شبكة VLAN الأصلية دائما untagged ويتم إستلامها عادة untagged. على أي حال، تلك الإطارات يمكن أن يتم إستلامها بعلامات تمييز.

راجع هذه المستندات للحصول على مزيد من المعلومات:

- قابلية التشغيل البيني لشبكة VLAN
- trunking بين مادة حفازة 4000/4500، 5000/5500، و 6000/6500 sery مفتاح يستعمل 802.1q عملية كبسلة مع cisco CatOS نظام برمجية

تنسيق الإطار 802.1Q/802.1p

		Tag Header						
		TPID	TCI					
48 bits	48 bits	16 bits	3 bits	1 bit	12 bits	16 bits	Variable length	32 bits
DA	SA	TPID	Priority	CFI	VLAN ID	Length/ Type	Data with PAD	FCS
		0x8100	0 – 7	0-1	0-4095			

توصية تكوين Cisco

يتمثل أحد أساسيات تصميم Cisco في السعي لتحقيق التناسق في الشبكة حيث يكون التناسق ممكنا. تدعم جميع منتجات Catalyst الأحدث 802.1Q وبعضها فقط 802.1Q، مثل الوحدات النمطية السابقة في السلسلة Catalyst 4500/4000 و Catalyst 6500. لذلك، يجب أن تتبع جميع عمليات التنفيذ الجديدة معيار IEEE 802.1Q هذا والشبكات القديمة التي تحتاج إلى الترحيل تدريجيا من ISL.

أصدرت هذا قارن أمر in order to مكنت 802.1Q trunking على ميناء خاص:

```
#Switch(config)#interface type slot#/port
Switch(config-if)#switchport
Configure the interface as a Layer 2 port. Switch(config-if)#switchport trunk encapsulation ---!
dot1q
```

يتيح معيار IEEE للبائع إمكانية التشغيل البيني. تكون قابلية التشغيل البيني للمورد ميزة في جميع بيئات Cisco عند توفر بطاقات واجهة شبكة (NIC) وأجهزة جديدة تدعم معيار 802.1p للمضيف. على الرغم من أن كلا من تطبيقات

ISL و 802.1Q قوية، فإن معيار IEEE يتمتع في نهاية المطاف بتعرض أكبر للحقل ودعم أكبر من جهات خارجية، والذي يتضمن دعم محلل الشبكة. بالإضافة إلى ذلك، هناك إعتبار صغير يتمثل في أن معيار 802.1Q يحتوي أيضا على تكلفة كبسلة أعلى أقل من ISL.

للكمال، يخلق التمييز الضمني على VLANs أهلي طبيعي إعتبار تأمين. النقل من إطار من واحد VLAN X، VLAN، إلى آخر VLAN Y، VLAN، دون مسحاج تخديد يمكن. يمكن أن يقع الإرسال دون مسحاج تخديد إن المصدر ميناء (VLAN X) يكون في ال نفسه VLAN بما أن ال VLAN أهلي طبيعي من 802.1Q شنطة على ال نفسه مفتاح. ال workaround أن يستعمل VLAN وهمي ل ال VLAN أهلي طبيعي من الشنطة.

أصدرت هذا قارن أمر in order to خلقت VLAN كأهلي طبيعي (التقصير) ل 802.1Q trunking على ميناء خاص:

```
#Switch(config)#interface type slot#/port
Switch(config-If)#switchport trunk native vlan 999
```

ونظرا لأن جميع الأجهزة الأحدث تدعم معيار 802.1Q، فيجب أن تتبع جميع عمليات التنفيذ الجديدة معيار IEEE 802.1Q وأن تقوم بترحيل الشبكات السابقة من ISL بشكل تدريجي. حتى وقت قريب، لم تدعم العديد من وحدات Catalyst 4500/4000 ISL. لذلك، فإن 802.1Q هو الخيار الوحيد لتوصيل الإيثرنت. أحلت الإنتاج من **العرض قارن إمكانيات** أمر، **العرض ميناء capabilities** أمر ل CatOS. ونظرا لأن دعم التوصيل يتطلب الأجهزة المناسبة، فإن الوحدة التي لا تدعم معيار 802.1Q لا تدعم معيار 802.1Q على الإطلاق. لا توفر ترقية البرامج الدعم ل 802.1Q. معظم جهاز جديد للمادة حفازة 6000/6500 ومادة حفازة 4000/4500 مفتاح دعم كلا من ISL و 802.1Q.

إذا تم مسح شبكة VLAN 1 من خط اتصال، بما أن واجهة إدارة المحول وقسم شبكة VLAN الأصلية يناقش، على الرغم من عدم إرسال بيانات مستخدم أو استقبالها، فإن بروتوكول NMP يستمر في تمرير بروتوكولات التحكم على شبكة VLAN رقم 1. وتتضمن أمثلة بروتوكولات التحكم CDP و VTP.

أيضا، بما أن ال VLAN 1 يناقش قسم، VTP، CDP، و PAgP يرسل ربط دائما على VLAN 1 عندما trunking. مع الإستعمالمن 802.1Q) dot1q) عملية كبسلة، هذا تحكم إطار حددت مع VLAN 1 إن المفتاح VLAN أهلي طبيعي غيرت. إن dot1q trunking إلى مسحاج تخديد وال VLAN أهلي طبيعي غيرت على المفتاح، قارن فرعي في VLAN 1 ضروري in order to إستلمت ال tagged CDP إطار وتقديم ال cdp مجاور رؤية على المسحاج تخديد.

ملاحظة: هناك إعتبار أمان محتمل مع dot1q أن التمييز الضمني من ال VLAN أهلي طبيعي يسبب. يمكن أن يكون إرسال الإطارات من شبكة VLAN إلى أخرى دون موجه ممكنا. ارجع إلى الأسئلة المتداولة حول اكتشاف الاقتحام للحصول على مزيد من التفاصيل. ال workaround أن يستعمل VLAN id ل ال VLAN أهلي طبيعي من الشنطة أن لا يستعمل ل المستعمل منفذ. in order to حققت هذا، يترك معظم cisco زبون ببساطة VLAN 1 بما أن ال VLAN أهلي طبيعي على شنطة وعينت منفذ ميناء إلى VLANs بخلاف VLAN 1.

توصي Cisco بتكوين صريح لوضع خط الاتصال في كلا النهايتين. هذا أسلوب التقصير أسلوب. في هذا الوضع، يمكن لمشغلي الشبكة الثقة في رسائل حالة سطر الأوامر و syslog أن يكون المنفذ up و trunking. هذا أسلوب مختلف من on أسلوب، أي يستطيع جعلت ميناء يظهر فوق رغم أن المجاور يكون misconfiguration. وبالإضافة إلى ذلك، توفر الوضع فيه الاستقرار في الحالات التي لا يمكن فيها لجانب واحد من الارتباط أن يصبح شنطة أو أن يسقط حالة .

إذا تم التفاوض على نوع التضمين بين المحولات باستخدام DTP، ويتم إختيار ISL كفائز بشكل افتراضي إذا كان كلا النهايتين يدعمانه، فيجب عليك إصدار أمر الواجهة هذا لتحديد dot1q[1]:

```
switchport trunk encapsulation dot1q
```

[1] لا تدعم بعض الوحدات التي تتضمن WS-X6548-GE-TX و WS-X6148-GE-TX توصيل ISL. لا تقبل هذه الوحدات النمطية الأمر **switchport trunk encapsulation *dot1q*** .

ملاحظة: قم بإصدار الأمر **switchport mode access** من أجل تعطيل خطوط الاتصال على المنفذ. يساعد هذا التعطيل على التخلص من وقت التفاوض المهدر عند عرض منافذ المضيف.

```
Switch(config-if)#switchport host
```

خيارات أخرى

كما يستخدم تكوين عميل شائع آخر الوضع فيه في طبقة التوزيع والتكوين الافتراضي الأكثر بساطة (الوضع) في طبقة الوصول. بعض المحولات، مثل المادة حفازة cisco ios ،2900xl مسحاج تخديد، أو آخر بائع أداة، لا يساند حاليا شنطة تفاوض عبر DTP. يمكنك إستخدام وضع الإغواء لتعيين منفذ على خط الاتصال دون قيد أو شرط مع هذه الأجهزة. يمكن أن يساعد هذا الوضع في توحيد الإعدادات المشتركة في الجامعة.

توصيك Cisco التفاوض عند الاتصال بموجه Cisco IOS. وعبر الجسر، يمكن لبعض إطارات DTP التي يتم استقبالها من منفذ تم تكوينه باستخدام **خط اتصال وضع** switchport أن ترجع إلى منفذ خط الاتصال. عند إستلام إطار DTP، يحاول منفذ المحول إعادة التفاوض دون داع. in order to renegotiate، المفتاح ميناء الشنطة وبعد ذلك . إذا تم تمكين الذاتية، فإن المحول لا يرسل إطارات DTP.

```
#switch(config)#interface type slot#/port
switch(config-if)#switchport mode dynamic desirable
Configure the interface as trunking in desirable !--- mode for switch-to-switch links with ---!
multiple VLANs. !--- And... switch(config-if)#switchport mode trunk
Force the interface into trunk mode without negotiation of the trunk connection. !--- Or... ---!
switch(config-if)#switchport nonegotiate
Set trunking mode to not send DTP negotiation packets !--- for trunks to routers. ---!
switch(config-if)#switchport access vlan vlan_number
Configure a fallback VLAN for the interface. switch(config-if)#switchport trunk native vlan ---!
999
Set the native VLAN. switch(config-if)#switchport trunk allowed vlan vlan_number_or_range ---!
.Configure the VLANs that are allowed on the trunk ---!
```

بروتوكول الشجرة الممتدة

الغرض

تحافظ الشجرة المتفرعة على بيئة من الطبقة 2 خالية من الحلقة في الشبكات المحولة والجسور المكررة. بدون بروتوكول الشجرة المتفرعة (STP)، يتم تكرار الإطارات و/أو ضربها إلى أجل غير مسمى. يتسبب هذا التكرار في انهيار الشبكة لأن حركة المرور العالية تقاطع جميع الأجهزة في مجال البث.

في بعض النواحي، بروتوكول الشجرة المتفرعة (STP) هو بروتوكول مبكر تم تطويره في البداية لمواصفات الجسور القائمة على البرامج البطيئة (IEEE 802.1D). ومع ذلك، يمكن تعقيد بروتوكول الشجرة المتفرعة (STP) من أجل تنفيذه بنجاح في الشبكات المحولة الكبيرة التي تمتلك:

- كثير VLANs
- العديد من المحولات في مجال
- دعم موردين متعددين
- تحسينات IEEE الأحدث

أخذ برنامج نظام Cisco IOS بالتطورات الجديدة لبروتوكول الشجرة المتفرعة (STP). توفر معايير IEEE الجديدة التي تتضمن بروتوكول الشجرة المتفرعة (STP) السريع وفقا لمعيار 802.1w وبروتوكولات شجرة الامتداد المتعددة وفقا لمعيار 802.1s إمكانية تقارب سريعة، فضلا عن مشاركة الأحمال وتطوير مستوى التحكم. وبالإضافة إلى ذلك، توفر مميزات تحسين بروتوكول الشجرة المتفرعة (STP) مثل RootGuard، وتصفية وحدة بيانات بروتوكول الجسر (BPDU)، وحراسة وحدة بيانات بروتوكول الجسر (BPDU) من PortFast، وحماية إضافية ضد حلقات إعادة التوجيه من الطبقة 2.

نظرة عامة على تشغيل PVST+

ويتم الفوز بعملية إختيار الجسر الرئيسي لكل شبكة محلية ظاهرية (VLAN) بواسطة المحول صاحب معرف الجسر الرئيسي الأدنى (BID). العطاء هو أولوية الجسر المدمج مع المفتاح عنوان MAC.

في البداية، يتم إرسال وحدات بيانات بروتوكول الجسر (BPDUs) من جميع المحولات وتحتوي على العطاء الخاص بكل محول وتكلفة المسار للوصول إلى ذلك المحول. وهذا يمكن من تحديد الجسر الرئيسي والمسار الأقل تكلفة إلى الجذر. كما أن معلمات التكوين الإضافية التي يتم نقلها في وحدات بيانات بروتوكول الجسر (BPDUs) من الجذر تتجاوز هذه المعلمات التي تم تكوينها محليا بحيث تستخدم الشبكة بالكامل وحدات توقيت متناسقة. لكل وحدة بيانات بروتوكول الجسر (BPDU) التي يتلقاها محول من الجذر، يقوم بروتوكول Catalyst المركزي بتجهيز وحدة بيانات بروتوكول الجسر (BPDU) جديدة وإرسالها باستخدام المعلومات الجذر.

ثم تتلاقى الطبولوجيا من خلال الخطوات التالية:

1. يتم إختيار جسر رئيسي واحد لمجال الشجرة المتفرعة بأكمله.
2. يتم إختيار منفذ جذري واحد (يواجه الجسر الرئيسي) على كل جسر غير جذري.
3. يتم إختيار منفذ معين لإعادة توجيه وحدة بيانات بروتوكول الجسر (BPDU) على كل مقطع.
4. تصبح المنافذ غير المعينة قيد الحظر.

راجع هذه المستندات للحصول على مزيد من المعلومات:

- تكوين بروتوكول الشجرة المتفرعة (STP) و IEEE 802.1s MST
- فهم بروتوكول الشجرة الممتدة السريع (802.1w)

وحدات التوقيت الأساسية الافتراضية	الاسم	دالة
2 ثانية	مرحبا	التحكم في مغادرة وحدات بيانات بروتوكول الجسر (BPDU(s.
15 ثانية	تأخير إعادة التوجيه (Fwd delay)	يتحكم في طول الوقت الذي يقضيه المنفذ في حالة وحالة ويؤثر على عملية تغيير المخطط.
20 ثانية	ماكسا ج	يتحكم في طول الوقت

		الذي يحتفظ فيه المحول بالمخطط الحالي قبل أن يبحث المحول عن مسار بديل. بعد الحد الأقصى لوقت التقادم (maxAge)، يتم إعتبار BPDU قديم ويبحث المحول عن منفذ جذر جديد من المجموعة الخاصة بمنافذ الحظر. في حال عدم توفر منفذ محظور، فإن المحول يدعي أنه الجذر نفسه على المنافذ المخصصة.

توصي Cisco بعدم تغيير عدادات الوقت لأن هذا يمكن أن يؤثر سلبا على الاستقرار. لم يتم ضبط غالبية الشبكات التي يتم نشرها. وحدات توقيت بروتوكول الشجرة المتفرعة (STP) البسيطة التي يمكن الوصول إليها عبر سطر الأوامر (مثل maxage، hello-interval، وما إلى ذلك) تتكون نفسها من مجموعة معقدة من وحدات التوقيت الأخرى المفترضة والمتأصلة. لذلك، من الصعب ضبط الوقت والتفكير في كل التداعيات. علاوة على ذلك، يمكنك تقويض حماية UDLD. راجع قسم اكتشاف الروابط أحادي الإتجاه للحصول على مزيد من التفاصيل.

ملاحظة على وحدات توقيت STP:

تستند قيم مؤقت بروتوكول الشجرة المتفرعة (STP) الافتراضية إلى حساب يأخذ في الاعتبار قطر الشبكة من سبعة محولات (سبع نقلات محول من الجذر إلى حافة الشبكة)، والوقت اللازم لوحدة بيانات بروتوكول الجسر (BPDU) للتنقل من الجسر الرئيسي إلى المحولات الطرفية في الشبكة، والتي تبعد عن سبع نقلات. يقوم هذا الافتراض بحساب قيم المؤقت المقبولة لمعظم الشبكات. ولكن، يمكنك تغيير وحدات التوقيت هذه إلى قيم أكثر مثالية لزيادة سرعة أوقات التقارب عبر تغييرات مخطط الشبكة.

أنت يستطيع شكلت الجذر جسر مع الشبكة قطر ل VLAN خاص، وال وقت حسبت قيمة وفقا لذلك. cisco يوصي أن، إن ينبغي أنت جعلت تغير، فقط شكلت القطر و إختياري مرحبا وقت معلم على الجذر جسر ل ال VLAN.

```
spanning-tree vlan vlan-id [root {primary | secondary}] [diameter diameter-value [hello hello-
[[time
.This command needs to be on one line ---!
```

يقوم هذا الماكرو بتكوين جذر المحول لشبكة VLAN المحددة، وحساب قيم المؤقت الجديدة على أساس القطر ووقت مرحبا المحدد، ونشر هذه المعلومات في وحدات بيانات بروتوكول الجسر (BPDUs) الخاصة بالتكوين إلى جميع المحولات الأخرى في المخطط.

يصف القسم حالات المنافذ الجديدة وأدوار المنافذ بروتوكول الشجرة المتفرعة (STP) طراز 802.1D ويقارن بين بروتوكول الشجرة المتفرعة (STP) طراز 802.1D ومقارنته مع بروتوكول الشجرة المتفرعة (RSTP) السريع. راجع فهم بروتوكول الشجرة المتفرعة السريعة (802.1w) للحصول على مزيد من المعلومات حول RSTP.

دول المنافذ الجديدة وأدوار المنافذ

يتم تحديد الطراز 802.1D في أربع دول منافذ مختلفة:

- إصغاء
- تعلم
- معوقونا
- إعادة توجيه

راجع الجدول في قسم دول المنفذ للحصول على مزيد من المعلومات. تكون حالة المنفذ مختلطة (ما إذا كانت تمنع حركة المرور أو تعيد توجيهها)، كما هو دور المنفذ في المخطط النشط (المنفذ الجذري، المنفذ المعين، وما إلى ذلك). على سبيل المثال، من وجهة نظر عملياتية، لا يوجد فرق بين منفذ في حالة الحظر ومنفذ في حالة الاستماع. كلاهما يتجاهل إطارات ولا يتعلم عناوين MAC. ويكمن الاختلاف الحقيقي في الدور الذي تعينه الشجرة الممتدة للميناء. يمكنك افتراض أن منفذ الاستماع إما معين أو جذر وهو في طريقه إلى حالة إعادة التوجيه. لسوء الحظ، بمجرد أن يكون المنفذ في حالة إعادة توجيه، فلا توجد طريقة لاستنتاج ما إذا كان المنفذ الجذري أو المعين من حالة المنفذ. وهذا يدل على فشل هذا المصطلح القائم على الدولة. يعالج RSTP هذا إخفاق لأن RSTP يفك دور وحالة ميناء.

دول الميناء

دول المنفذ في STP 802.1D

دول الميناء	وسيلة	التوقيتات الافتراضية للحالة

		التالية
	معطل إداريا.	
	إستلام وحدات بيانات بروتوكول الجسر (BPDUs) ووقف بيانات المستخدم.	مراقبة إستقبال وحدات بيانات بروتوكول الجسر (BPDUs). انتظار لمدة 20 ثانية لانتهاء صلاحية الحد الأقصى أو التغيير الفوري في حالة اكتشاف فشل الارتباط المباشر/الم

		حالي.
	لإرسال وحدات بيانات بروتوكول الجسر (BPDUs) أو استقبالها للتحقق مما إذا كان من الضروري العودة إلى الحظر.	انتظر 15 ثانية من Fwddelay.
	يبني المخطط/جدول CAM.	انتظر 15 ثانية من Fwddelay.
	يرسل/يستلم البيانات.	

التغيير الكلي للمخطط الأساسي هو:

- 20 + 2 (15) = 50 ثانية، إذا كنت تنتظر انتهاء صلاحية العرف
- 30 ثانية لفشل الارتباط المباشر

ولم يتبق في بروتوكول الشجرة المتفرعة (RSTP) سوى ثلاث دول مرفئية، وهو ما يتوافق مع الحالات التشغيلية الثلاث المحتملة. تم دمج حالات 802.1D المعطلة والحجب والإصغاء في حالة تجاهل فريدة بقدرة 802.1w.

دولة المنفذ STP (802.1D)	حالة المنفذ RSTP (802.1w)	هل يتم تضمين المنفذ في المخطط النشط؟	هل المنفذ يعلم عناوين MAC؟
معطل	تجاهل	لا	لا
معوقونا	تجاهل	لا	لا
إصغاء	تجاهل	نعم	لا
تعلم	تعلم	نعم	نعم
إعادة توجيه	إعادة توجيه	نعم	نعم

أدوار المنفذ

الدور الآن متغير يتم تعيينه على منفذ معين. يبقى المنفذ الجذري وأدوار المنفذ المعين، لكن يتم الآن تقسيم دور منفذ الحظر إلى أدوار المنفذ الاحتياطي والبديل. تحدد خوارزمية الشجرة المتفرعة (STA) دور المنفذ على أساس وحدات بيانات بروتوكول الجسر (BPDUs). وللحفاظ على بساطة الأمور، تذكر هذا الأمر على وحدات بيانات بروتوكول الجسر (BPDUs)، حيث توجد دائما طريقة لمقارنة أي من وحدات بيانات بروتوكول الجسر (BPDUs) وتحديد ما إذا كان أحد هذه الوحدات أكثر فائدة من الآخر. ويستند هذا القرار إلى القيمة المخزنة في وحدة بيانات بروتوكول الجسر (BPDU)، وأحيانا المنفذ الذي يتم تلقي وحدة بيانات بروتوكول الجسر عليه. يوضح الجزء المتبقي من هذا الجزء النهوج العملية جدا لأدوار الميناء.

دور المنفذ الجذري

الميناء أن يستلم أفضل BPDU على جسر الجذر ميناء. هذا هو المنفذ الأقرب إلى الجسر الرئيسي من حيث تكلفة المسار. يقوم بروتوكول STA بإختيار جسر رئيسي واحد في الشبكة التي تم ربطها بالكامل (لكل شبكة محلية ظاهرية (VLAN)). الجسر الرئيسي يرسل BPDUs أن يكون مفيد أكثر من أن أي جسر آخر يستطيع أرسلت. والجسر الرئيسي هو الجسر الوحيد في الشبكة الذي لا يحتوي على منفذ جذري. وتتلقى جميع الجسور الأخرى وحدات بيانات بروتوكول الجسر (BPDUs) على منفذ واحد على الأقل.

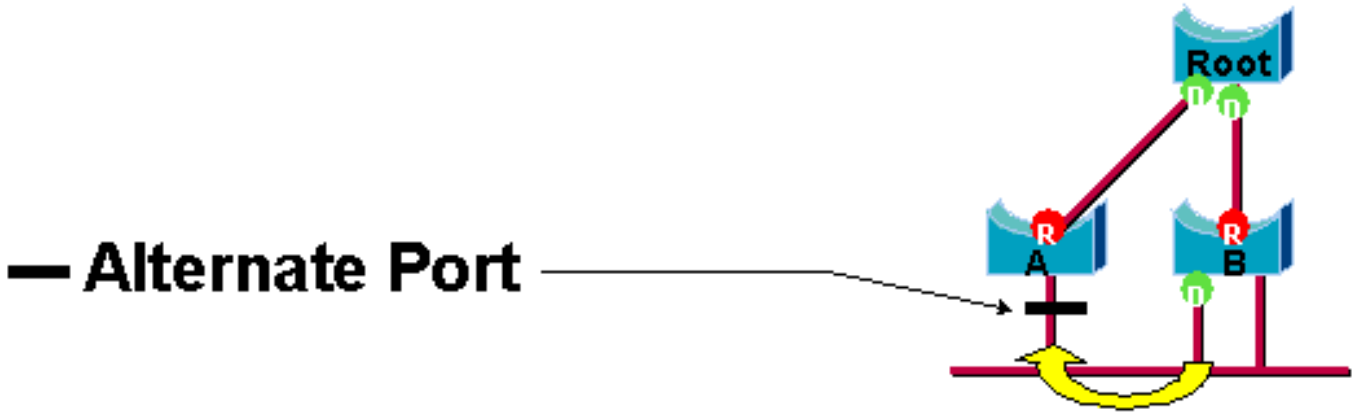
دور المنفذ المعين

عينت ميناء إن يستطيع أرسلت أفضل BPDU على القطعة أي الميناء يكون ربطت إلى. تربط الجسور 802.1D مقاطع مختلفة (مقاطع إيثرنت، على سبيل المثال) لإنشاء مجال جسر. على مقطع محدد، يمكن أن يكون هناك مسار واحد فقط باتجاه الجسر الرئيسي. إن يكون هناك إثنان ممر، هناك يجسر أنشوطة في الشبكة. تستمع جميع الجسور المتصلة بمقطع معين إلى وحدات بيانات بروتوكول الجسر (BPDU) الأخرى وتتفق على الجسر الذي يرسل أفضل وحدة بيانات بروتوكول الجسر (BPDU) كالجسر المعين للمقطع. يتم تخصيص المنفذ المطابق على ذلك الجسر.

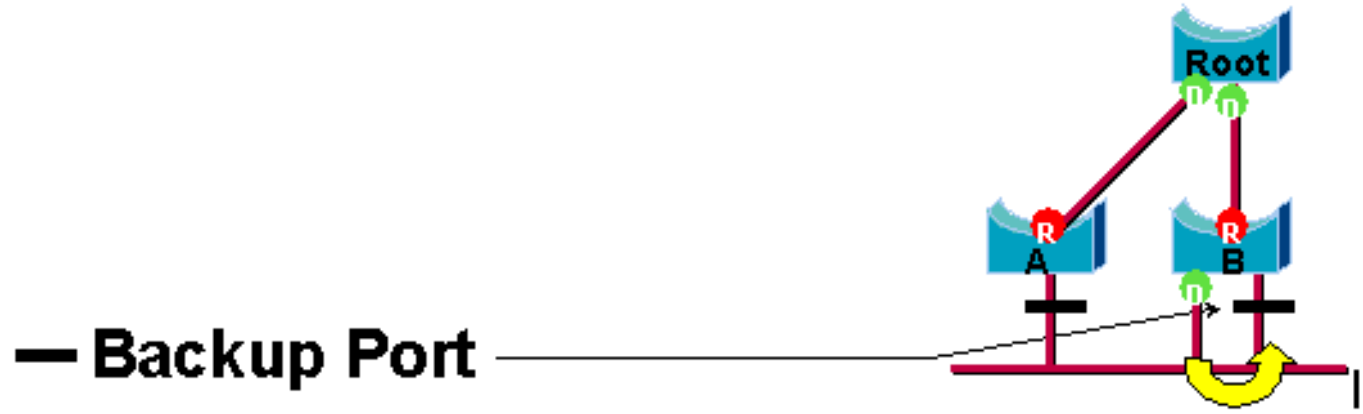
أدوار منفذ النسخ الاحتياطي والبديل

يتوافق دورا المنفذ هذين مع حالة الحظر الخاصة ب 802.1D. تعريف المنفذ المحظور هو منفذ ليس المنفذ المعين أو الجذر. يستلم ميناء محظور BPDU أكثر فائدة من ال BPDU أن هو يبعث على قطاعه. تذكرت أن ميناء يحتاج إطلاقا أن يستلم BPDUs in order to أبقيت محظور. يقدم بروتوكول الشجرة المتفرعة (RSTP) هذين الدورين لهذا الغرض.

ميناء بديل هو ميناء أن يكون منعت ب يستلم أكثر فائدة BPDUs من آخر جسر. يوضح هذا المخطط:



ميناء نسخة إحتياطية يكون ميناء أن يكون منعت ب يستلم أكثر فائدة BPDUs من ال نفسه جسر أن الميناء يكون على. يوضح هذا المخطط:



وقد تم بالفعل إجراء هذا التمييز داخليا في حدود 802.1 دال. هذه هي أساسا كيفية عمل Cisco Uplinkfast. الأساس المنطقي وراء هذا هو أن المنفذ البديل يوفر مسار بديل للجسر الرئيسي. لذلك، هذا ميناء يستطيع استبدلت الجذر ميناء إن يفشل. بطبيعة الحال، يوفر منفذ النسخ الاحتياطي اتصال متكرر لنفس المقطع ولا يمكنه ضمان اتصال بديل للجسر الرئيسي. لذلك، استثنيت النسخة الاحتياطية ميناء من مجموعة الوصلات.

ونتيجة لذلك، يقوم بروتوكول الشجرة المتفرعة (RSTP) بحساب المخطط النهائي للشجرة المتفرعة باستخدام نفس المعايير تماما مثل معيار 802.1D. لا يوجد تغيير في طريقة إستخدام أولويات المنافذ والجسر المختلفة. يتم إستخدام حظر الاسم لحالة التجاهل في تنفيذ Cisco. لا يزال الإصدار 7.1 من CatOS والإصدارات الأحدث يعرض حالات الإصغاء والتعلم، والتي توفر معلومات أكثر حول المنفذ مما يتطلبه معيار IEEE. ولكن، الميزة الجديدة هي أن هناك الآن فرق بين الدور الذي حدده البروتوكول لمنفذ ما وحالته الحالية. على سبيل المثال، هو الآن صالح تماما لمنفذ ما أن يكون عينت وحظرت في نفس الوقت. بينما يحدث هذا عادة لفترات زمنية قصيرة جدا، فإنه يعني ببساطة أن هذا المنفذ في حالة انتقالية تجاه إعادة التوجيه المعينة.

تفاعلات STP مع شبكات VLAN

هناك ثلاث طرق مختلفة لربط شبكات VLAN بالشجرة المتفرعة:

- شجرة متفرعة واحدة لجميع الشبكات المحلية الظاهرية (VLANs) أو بروتوكول الشجرة المتفرعة الشائعة (CST)، مثل IEEE 802.1D
- شجرة متفرعة لكل شبكة VLAN، أو شجرة متفرعة مشتركة، مثل Cisco PVST
- شجرة متفرعة لكل مجموعة من شبكات VLAN، أو شجرة متفرعة متعددة (MST)، مثل IEEE 802.1s

من وجهة نظر تكوين، يمكن تكوين هذه الأنواع الثلاثة من أوضاع الشجرة المتفرعة هذه من حيث إتصالها بالتفاعل مع شبكات VLAN في واحد من الأنواع الثلاثة للأوضاع:

- **PVST** — الشجرة الممتدة لكل شبكة VLAN. وهذا يطبق في الواقع الإصدار PVST+، ولكنه ملاحظ في برنامج Cisco IOS باسم PVST ببساطة.
- **Rapid-PVST** — يعمل تطور معيار 802.1D على تعزيز أوقات التقارب ودمج خصائص (802.1w Uplinkfast و BackboneFast القائمة على المعايير.
- **mst** — هذا هو المعيار 802.1s للشجرة المتفرعة لكل مجموعة من شبكات VLAN أو شبكات MST. وهذا يتضمن أيضا مكون 802.1w السريع ضمن المعيار.

تسمح الشجرة المتفرعة الأحادية لجميع شبكات VLAN بمخطط واحد نشط فقط، وبالتالي لا تسمح بموازنة الأحمال. قام بروتوكول الشجرة المتفرعة (STP) بحظر كتل المنفذ لجميع شبكات VLAN ولا يحمل أي بيانات.

تسمح شجرة متفرعة واحدة لكل شبكة محلية ظاهرية (VLAN) أو PVST+ بموازنة الأحمال ولكنها تتطلب معالجة وحدة معالجة مركزية (CPU) إضافية مع زيادة عدد شبكات VLAN.

يتيح المعيار الجديد (MST 802.1s) تعريف ما يصل إلى 16 حالة/طبولوجيا لبروتوكول الشجرة المتفرعة (STP) النشطة وتخطيط جميع شبكات VLAN لهذه المثيلات. في بيئة مجموعة نموذجية، يلزم تعريف مثالين فقط. يتيح هذا الأسلوب قياس STP إلى عدة آلاف من VLANs أثناء تمكينه من موازنة التحميل.

يتم تقديم دعم PVST السريع و MST السابق للمستوى القياسي في البرنامج Cisco IOS Software، الإصدار 12.1(11b)EX و 12.1(13)E ل Catalyst 6500. مادة حفازة 4500 مع cisco ios برمجية إطلاق 12.1(12c)ew وإطلاق متأخر دعم pre-standard MST. تتم إضافة دعم PVST السريع في برنامج Cisco IOS الإصدار 12.1(19)EW لمنصة Catalyst 4500. ال standard متوافق MST ساندت في cisco ios برمجية إطلاق 12.2(18)SXF لمادة حفازة 6500 و cisco ios برمجية إطلاق 12.2(25)sg لمادة حفازة 4500 sery مفتاح.

راجع فهم بروتوكول الشجرة المتفرعة السريعة (802.1w) وفهم بروتوكول الشجرة المتفرعة المتعددة (802.1s) للحصول على مزيد من المعلومات.

المنافذ المنطقية للشجرة الممتدة

توفر ملاحظات إصدار Catalyst 4500 و 6500 إرشادات حول عدد المنافذ المنطقية في الشجرة المتفرعة لكل محول. يساوي مجموع كل ميناء منطقي عدد شنطة على المفتاح ضرب عدد VLANs نشط على شنطة، زائد عدد الواجهات غير trunking على المفتاح. يقوم برنامج Cisco IOS software بإنشاء رسالة سجل نظام إذا تجاوز الحد الأقصى لعدد الواجهات المنطقية. ويوصى بعدم تجاوز الإرشادات الموصى بها.

يقارن هذا طاولة عدد الميناء منطقي يساند مع مختلف STP أسلوب ومشرف نوع:

المشرف	+PVST	+RPVST	MST
المشرف Catalyst 6500 Supervisor 1	إجمالي 6000[1] 1200 لكل وحدة تحويل	إجمالي 1200 1 لكل وحدة تحويل	إجمالي 30000[2] لكل وحدة تحويل
المشرف Catalyst 6500 Supervisor 2	13000[1] إجمالي 1800[2] لكل وحدة تحويل	إجمالي 10000 1800[2] لكل وحدة تحويل	إجمالي 60000[2] لكل وحدة تحويل
المشرف Catalyst 6500 Supervisor 720	إجمالي 13000 1800[2] لكل وحدة تحويل	إجمالي 10000 1800[2] لكل وحدة تحويل	إجمالي 600003[2] لكل وحدة تحويل

برنامج Catalyst 4500 Supervisor II Plus	إجمالي 1،500	إجمالي 1،500	إجمالي 25000
المشرف Catalyst 4500 Supervisor II Plus-10GE	إجمالي 1،500	إجمالي 1،500	إجمالي 25000
المشرف Catalyst 4500 Supervisor IV	إجمالي 3000	إجمالي 3000	إجمالي 50000
المشرف Catalyst 4500 Supervisor V	إجمالي 3000	إجمالي 3000	إجمالي 50000
المشرف Catalyst 4500 Supervisor V 10GE	إجمالي 3000	إجمالي 3000	إجمالي 80000

[1] يبلغ الحد الأقصى لعدد إجمالي المنافذ المنطقية المدعومة في PVST+ الأقدم من الإصدار 12.1(13)E من البرنامج Cisco IOS Software 4500.

تدعم وحدات التحويل النمطية [2] بسرعة 10 ميجابت في الثانية و 100/10 ميجابت في الثانية و 100 ميجابت في الثانية دعم 1200 واجهة منطقية كحد أقصى لكل وحدة.

[3] يبلغ الحد الأقصى لعدد إجمالي المنافذ المنطقية المدعومة في MST قبل برنامج Cisco IOS الإصدار 12.2(30000 SXA(17b.

توصية

من الصعب توفير توصية وضع الشجرة المتفرعة دون معلومات تفصيلية مثل الأجهزة والبرامج وعدد الأجهزة وعدد شبكات VLAN. بشكل عام، إذا لم يتجاوز عدد المنافذ المنطقية المخطط الإرشادي الموصى به، فإنه يوصى بوضع PVST السريع لنشر الشبكة الجديد. يعمل وضع PVST السريع على توفير تقارب سريع للشبكة دون الحاجة إلى تهيئة إضافية مثل Backbone Fast و Uplinkfast. قم بإصدار الأمر التالي لتعيين الشجرة المتفرعة في وضع Rapid-PVST:

```
spanning-tree mode rapid-pvst
```

خيارات أخرى

في شبكة تحتوي على مزيج من الأجهزة القديمة والبرامج القديمة، يوصى بوضع PVST+. قم بإصدار هذا الأمر لتعيين الشجرة المتفرعة في وضع PVST+:

```
spanning-tree mode pvst
.This is default and it shows in the configuration----
```

يوصى بوضع MST لتصميم الشبكة في كل مكان لشبكة VLAN باستخدام عدد كبير من شبكات VLAN. بالنسبة لهذه الشبكة، يمكن أن يتجاوز مجموع المنافذ المنطقية التوجيه ل PVST و Rapid-PVST. قم بإصدار هذا الأمر لتعيين الشجرة المتفرعة في وضع MST:

```
spanning-tree mode mst
```

تنسيقات BPDU

من أجل دعم معيار IEEE 802.1Q، قامت Cisco بتوسيع بروتوكول PVST الموجود لتوفير بروتوكول PVST+. يضيف PVST+ دعما للارتباطات عبر منطقة الشجرة الممتدة الأحادية IEEE 802.1Q. يتوافق PVST+ مع كل من شجرة الامتداد IEEE 802.1Q الأحادية وبروتوكولات PVST من Cisco الموجودة. وبالإضافة إلى ذلك، يضيف PVST+ آليات التحقق لضمان عدم وجود عدم تناسق تكوين معرف توصيل المنفذ وشبكة VLAN عبر المحولات. PVST+ متوافق مع التوصيل والتشغيل مع PVST، بدون متطلبات أمر أو تكوين واجهة سطر أوامر (CLI) جديدة.

فيما يلي بعض النقاط البارزة للنظرية التشغيلية لبروتوكول PVST+:

- يتم تشغيل PVST+ مع شجرة الامتداد أحادية اللون وفقا لمعيار 802. 1Q. تعمل واجهة PVST+ مع المحولات المتوافقة مع معيار 802.1Q على بروتوكول الشجرة المتفرعة (STP) الشائع من خلال توصيل عبر معيار 802.1Q. يجسر - شجرة على VLAN 1، ال VLAN أهلي طبيعي، افتراضيا. يتم إرسال وحدة بيانات بروتوكول الجسر (BPDU) واحدة مشتركة متفرعة (BPDU) أو استقبالها مع عنوان MAC لمجموعة الجسر القياسية من IEEE (01-80-c2-00-00-00، نوع البروتوكول 0x010c) عبر إرتباطات 802.1Q. يمكن جذر الشجرة المتفرعة الشائعة في منطقة الشجرة المتفرعة أحادية اللون أو PVST.
- ينفق PVST+ وحدات بيانات بروتوكول الجسر (BPDUs) الخاصة ب PVST عبر منطقة شبكة الاتصال المحلية الظاهرية (VLAN) وفقا لمعيار 802.1Q كبيانات بث متعدد. لكل شبكة VLAN على خط اتصال، يتم إرسال وحدات بيانات بروتوكول الجسر (BPDUs) باستخدام عنوان (SSTP) MAC المشترك من Cisco (01-00-0c-cc-cd) أو استقبالها. ل VLANs أن يكون مماثل إلى الميناء VLAN معين (PVID، BPDU untagged). لكل شبكات VLAN الأخرى، يتم تمييز وحدات BPDUs.
- PVST+ متوافق مع الخلف مع محول Cisco الحالي على PVST من خلال ISL trunking. يتم إرسال وحدات بيانات بروتوكول الجسر (BPDU) التي يغلف بها ISL أو استقبالها من خلال شبكات ISL، والتي تكون هي نفسها كما هو الحال مع شبكات Cisco PVST السابقة.
- يتحقق PVST+ من عدم تناسق المنفذ وشبكة VLAN. يقوم PVST+ بحظر هذه المنافذ التي تتلقى وحدات بيانات بروتوكول الجسر (BPDUs) غير المتناسقة لمنع تكرار حلقات إعادة التوجيه. يقوم PVST+ أيضا بإعلام المستخدمين عبر رسائل syslog عن أي عدم اتساق.

ملاحظة: في شبكات ISL، يتم إرسال جميع وحدات بيانات بروتوكول الجسر (BPDUs) باستخدام عنوان IEEE MAC.

توصيات تكوين Cisco

تحتوي جميع محولات Catalyst على بروتوكول الشجرة المتفرعة (STP) الممكنة بشكل افتراضي. حتى إذا أخترت تصميما لا يتضمن حلقات أنشوطة من الطبقة 2 و STP لا يمكن in order to حافظت بشكل نشط على ميناء محظور، أترك الميزة يمكن لهذه الأسباب:

- إذا كانت هناك تكرار حلقي، فإن بروتوكول الشجرة المتفرعة (STP) يمنع المشاكل التي يمكن تفاقمها بواسطة بيانات البث المتعدد والبث. فغالبا ما يتسبب سوء الترقيع أو سلك سيئ أو سبب آخر في حدوث تكرار حلقي.
- يحمي بروتوكول الشجرة المتفرعة (STP) من انهيار EtherChannel.

- يتم تكوين معظم الشبكات باستخدام بروتوكول الشجرة المتفرعة (STP)، وبالتالي، احصل على الحد الأقصى من تعرض الحقل. فالتعرض بشكل عام يعادل شفرة أكثر إستقرارا.
- يحمي بروتوكول الشجرة المتفرعة (STP) من السلوك الخاطئ لبطاقات واجهة الشبكة (NICs) مزدوجة المرفق (أو التوصيل الذي يتم تمكينه على الخوادم).
- يوجد العديد من البروتوكولات مرتبطة بشكل وثيق مع بروتوكول الشجرة المتفرعة (STP) في الرمز. الأمثلة تتضمن:PAgPتطفل بروتوكول رسائل مجموعات الإنترنت (IGMP)توصيلإذا قمت بالتشغيل دون بروتوكول الشجرة المتفرعة (STP)، فيمكنك الحصول على نتائج غير مرغوب فيها.
- أثناء انقطاع الشبكة الذي تم الإبلاغ عنه، عادة ما يقترح مهندسو Cisco أن عدم إستخدام بروتوكول الشجرة المتفرعة (STP) هو مركز الخطأ، إذا كان ذلك ممكنا على الإطلاق.

أصدرت in order to مكنت يجسر - شجرة على كل VLANs، هذا أمر عام:

```
Switch(config)#spanning-tree vlan vlan_id
Specify the VLAN that you want to modify. Switch(config)#default spanning-tree vlan vlan_id ---!
.Set spanning-tree parameters to default values ---!
```

لا تغير وحدات التوقيت، والتي يمكن أن تؤثر سلبا على الاستقرار. لم يتم ضبط غالبية الشبكات التي يتم نشرها. تعمل وحدات توقيت بروتوكول الشجرة المتفرعة (STP) البسيطة التي يمكن الوصول إليها عبر سطر الأوامر، مثل hello-interval و maxage، على مجموعة معقدة من وحدات التوقيت الأخرى المفترضة والمضمنة. لذلك، قد تواجه صعوبة إذا حاولت معايرة وحدات التوقيت والتفكير في كل التداعيات. علاوة على ذلك، يمكنك تقويض حماية UDLD.

نظريا، أبق حركة مرور المستخدم بعيدا عن إدارة VLAN. لا يطبق هذا على المادة حفازة cisco ios 6000/6500 مفتاح. ومع ذلك، يلزمك إحترام هذه التوصية على محولات Cisco IOS ومحولات CatOS الأصغر حجما التي يمكن أن يكون لها واجهة إدارة منفصلة وتحتاج إلى التكامل مع محولات Cisco IOS. خصوصا مع المعالجات الأقدم Catalyst switch، أبق الإدارة VLAN منفصل عن بيانات المستخدم in order to تفاديت مشكلة مع STP. يمكن لمحطة نهاية سيئة التصرف أن تبقي معالج Supervisor Engine مشغولا بحزم البث بحيث يمكن أن يفتقد المعالج واحدة أو أكثر من وحدات بيانات بروتوكول الجسر (BPDU). ولكن، تعمل المحولات الأحدث المزودة بوحدات معالجة مركزية (CPU) أكثر قوة وعناصر التحكم في التحكم على تخفيف هذا الاعتبار. راجع قسم واجهة إدارة المحول وشبكة VLAN الأصلية في هذا المستند للحصول على مزيد من التفاصيل.

تجنب تكرار التصميم الزائد. قد يؤدي ذلك إلى عدد كبير للغاية من منافذ الحظر وقد يؤثر سلبا على الاستقرار طويل المدى. الاحتفاظ بقطر بروتوكول الشجرة المتفرعة (STP) الإجمالي ضمن سبع نقلات. حاول التصميم إلى نموذج Cisco متعدد الطبقات حيثما كان هذا التصميم ممكنا. النموذج يتضمن:

- مجالات محولة أصغر
- مثلثات STP
- المنافذ القطعية المحظورة

التاثير ومعرفة مكان وجود وظائف الجذر والمنافذ المحظورة. قم بتوثيق هذه المعلومات على الرسم التخطيطي للمخطط. تعرف على مخطط الشجرة المتفرعة لديك، والذي يعد ضروريا لاستكشاف الأخطاء وإصلاحها. المنافذ المحظورة هي المكان الذي يبدأ فيه أستكشاف أخطاء بروتوكول الشجرة المتفرعة (STP) وإصلاحها. غالبا ما يكون سبب التغيير من الحظر إلى إعادة التوجيه هو الجزء الرئيسي من تحليل السبب الجذري. أختر التوزيع وطبقات الأساس كموقع للجذر الجذر/الثانوي لأن هذه الطبقات تعتبر أكثر أجزاء الشبكة إستقرارا. تحقق من المستوى الثالث الأمثل وغطاء بروتوكول الموجه الاحتياطي الفعال (HSRP) باستخدام مسارات إعادة توجيه البيانات من الطبقة 2.

هذا الأمر هو ماكرو يقوم بتكوين أولوية الجسر. يعين الجذر الأولوية أن تكون أقل بكثير من الافتراضي (32،768)، والثانوي يثبت الأولوية أن يكون بشكل معقول أقل من الافتراضي:

```
Switch(config)#interface type slot/port
Switch(config)#spanning-tree vlan vlan_id root primary
.Configure a switch as root for a particular VLAN ---!
```

ملاحظة: يقوم هذا الماكرو بتعيين أولوية الجذر لتكون إما:

- 8192 افتراضيا
- أولوية الجذر الحالية - 1، إذا كان هناك جسر رئيسي آخر معروف
- أولوية الجذر الحالية، إذا كان عنوان MAC الخاص بها أقل من الجذر الحالي

شذبت VLANs غير ضروري من شنطة ميناء، أي يكون تمرين ثنائي إتجاه. يحدد الإجراء قطر مصروفات معالجة بروتوكول الشجرة المتفرعة (STP) والشبكة (NMP) على أجزاء من الشبكة حيث لا تكون هناك حاجة إلى شبكات VLAN معينة. لا يزيل التشذيب التلقائي ل VTP بروتوكول الشجرة المتفرعة (STP) من خط اتصال. أنت يستطيع أيضا أزلت التقصير VLAN 1 من شنطة.

راجع مشاكل بروتوكول الشجرة المتفرعة واعتبارات التصميم ذات الصلة للحصول على معلومات إضافية.

خيارات أخرى

cisco يتلقى آخر STP بروتوكول، يدعو **VLAN-Bridge**، أن يعمل مع الإستعمالمن معروف غاية {upper}mac address من **0c-cd-cd-ce-00-01** ونوع بروتوكول 0x010c.

ويكون هذا البروتوكول مفيدا للغاية إذا كانت هناك حاجة إلى جسر البروتوكولات غير الموجهة أو القديمة بين شبكات VLAN دون تداخل مع مثيلات الشجرة المتفرعة ل IEEE التي تعمل على شبكات VLAN هذه. إذا أصبحت واجهات VLAN لحركة المرور غير العابرة محظورة لحركة مرور الطبقة 2، فإن حركة مرور الطبقة 3 التي تتجاوز الطبقة 3 يتم تنقيحها بشكل غير مقصود أيضا، وهو تأثير جانبي غير مرغوب فيه. يمكن أن يحدث هذا الانسداد للطبقة 2 بسهولة إذا شاركت واجهات شبكة VLAN لحركة المرور غير المتقاطعة في بروتوكول الشجرة المتفرعة (STP) نفسه كشبكات VLAN الخاصة ببروتوكول IP. VLAN-Bridge هو مثيل منفصل لبروتوكول الشجرة المتفرعة (STP) للبروتوكولات المتفرعة. يوفر البروتوكول مخطط منفصل يمكن معالجته دون تأثير على حركة مرور IP.

ركضت ال VLAN-bridge بروتوكول إن يتطلب جسر بين VLANs على cisco مسحاج تخديد مثل ال MSFC.

ميزة STP PortFast

أنت يستطيع استعملت PortFast in order to تجاوزت عادي يجسر - شجرة عملية على منفذ ميناء. يعمل PortFast على زيادة سرعة الاتصال بين المحطات الطرفية والخدمات التي تحتاج المحطات الطرفية إلى الاتصال بها بعد تهيئة الارتباط. يحتاج تنفيذ Microsoft DHCP أن يرى منفذ الوصول في وضع مباشرة بعد حالة الارتباط لطلب عنوان IP واستقباله. تحتاج بعض البروتوكولات، مثل تبادل حزم الشبكة البينية (IPX)/تبادل الحزم المتسلسل (SPX)، إلى رؤية منفذ الوصول في وضع مباشرة بعد حالة الارتباط لتجنب الحصول على مشكلات أقرب خادم (GNS).

راجع إستخدام أوامر PortFast والأوامر الأخرى لإصلاح حالات تأخير اتصال بدء تشغيل محطة العمل للحصول على مزيد من المعلومات.

نظرة عامة على تشغيل PortFast

يتخطى PortFast حالات `STP` العادية و و . تنقل الميزة منفذا مباشرة من إلى وضع بعد إعتبار الارتباط `up`. إذا لم يتم تمكين هذه الميزة، فإن بروتوكول الشجرة المتفرعة (STP) يتجاهل جميع بيانات المستخدم حتى يقرر أن المنفذ جاهز للنقل إلى وضع . يمكن أن تستغرق هذه العملية (2 x ForwardDelay) وقت، وهو 30 ثانية بشكل افتراضي.

يمنع وضع `PortFast` إنشاء إعلام بتغيير مخطط (STP (TCN في كل مرة تتغير فيها حالة المنفذ من إلى . TCNs عادي. ولكن هناك موجة من شبكات TCN التي تصل إلى الجسر الرئيسي قادرة على تمديد وقت التقارب بلا داع. غالبا ما تحدث موجة من النفثالينات في الصباح، عندما يقوم الأشخاص بتشغيل أجهزة الكمبيوتر الخاصة بهم.

توصية تكوين منفذ الوصول من Cisco

تعيين PortFast STP على لجميع منافذ المضيف الممكنة. كما يمكنك تعيين بروتوكول PortFast STP صريح التشغيل لارتباطات محول المحول والمنافذ غير المستخدمة.

قم بإصدار أمر الماكرو **switchport host** في وضع تكوين الواجهة لتنفيذ التكوين الموصى به لمنافذ الوصول. كما تساعد عملية التهيئة على تشغيل التفاوض التلقائي وأداء الاتصال بشكل ملحوظ:

```
#switch(config)#interface type slot#/port

switch(config-if)#switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
.This macro command modifies these functions ---!
```

ملاحظة: PortFast لا يعني أن الشجرة المتفرعة لا يتم تشغيلها على الإطلاق على المنافذ. لا تزال وحدات بيانات بروتوكول الجسر (BPDU) يتم إرسالها واستقبالها ومعالجتها. تعد الشجرة المتفرعة أمرا ضروريا للشبكة المحلية (LAN) التي تعمل بشكل كامل. ومن دون اكتشاف التكرار الحلقي ومنعه، يمكن للحلقة الحلقية إسقاط شبكة LAN بالكامل بسرعة من دون قصد.

أيضا، أعجزت trunking وقنوات لكل مضيف ميناء. كل منفذ مكنت ميناء افتراضيا ل trunking وقناة، غير أن مفتاح لا يتوقع جيران حسب تصميم على مضيف ميناء. إذا تركت هذه البروتوكولات للتفاوض، فإن التأخير اللاحق في تنشيط المنفذ يمكن أن يؤدي إلى حالات غير مرغوب فيها. لا يتم إعادة توجيه الحزم الأولية من محطات العمل، مثل طلبات DHCP و IPX.

أفضل خيار أن يشكل PortFast افتراضيا في الشامل تشكيل أسلوب مع إستعمال من هذا أمر:

```
Switch(config)#spanning-tree portfast enable
```

بعد ذلك، على أي منفذ منفذ منفذ أن يتلقى صرة أو مفتاح في فقط واحد VLAN، أعجزت ال PortFast سمة على كل قارن مع **القارن** أمر:

```
Switch(config)#interface type slot_num/port_num
Switch(config-if)#spanning-tree portfast disable
```

خيارات أخرى

يوفر حارس PortFast BPDU طريقة لمنع حلقات التكرار. يقوم حارس BPDU بنقل منفذ غير trunking إلى دولة errDisable في إستقبال BPDU على ذلك ميناء.

تحت ظروف عادية، لا يستلم أبدا أي BPDU ربط على منفذ منفذ أن يكون شكلت ل PortFast. تشير وحدة بيانات بروتوكول الجسر (BPDU) الواردة إلى تكوين غير صالح. أفضل إجراء هو إيقاف تشغيل منفذ الوصول.

يقدم برنامج Cisco IOS System أمر عام مفيد أن يمكن تلقائيا BPDU-Root-GUARD على أي ميناء أن يكون مكنت ل Uplinkfast. أستخدم هذا الأمر *دائما*. يعمل الأمر على أساس كل محول، وليس لكل منفذ.

أصدرت هذا أمر عام in order to مكنت BPDU-root-guard:

```
Switch(config)#spanning-tree portfast bpduguard default
```

يقوم فخ بروتوكول إدارة الشبكة البسيط (SNMP) أو رسالة syslog بإعلام مدير الشبكة إذا تم إسقاط المنفذ. أنت يستطيع أيضا شكلت تلقائيا إستعادة وقت ل errDisabled ميناء. راجع قسم اكتشاف الروابط أحادي الإتجاه في هذا المستند للحصول على مزيد من التفاصيل.

راجع يجسر - شجرة PortFast BPDU حارس تعزيز للحصول على مزيد من التفاصيل.

ملاحظة: تم تقديم PortFast لمنافذ خطوط الاتصال في البرنامج Cisco IOS Software، الإصدار 12.1(11b)E. تم تصميم PortFast لمنافذ خطوط الاتصال لزيادة أوقات تقارب شبكات الطبقة 3. عندما يستعمل أنت هذا سمة، تأكدت أن يعجز BPDU حارس و BPDU مرشح على قارن أساس.

Uplinkfast

الغرض

يوفر Uplinkfast تقارب STP سريعا بعد فشل الارتباط المباشر في طبقة الوصول إلى الشبكة. يعمل Uplinkfast دون تعديل بروتوكول الشجرة المتفرعة (STP). والغرض من ذلك هو تسريع وقت التقارب في ظرف معين إلى أقل من ثلاث ثوان، بدلا من التأخير النموذجي لمدة 30 ثانية. ارجع إلى فهم ميزة Cisco Uplinkfast وتكوينها.

نظرة عامة على العمليات

باستخدام نموذج تصميم Cisco متعدد الطبقات في طبقة الوصول، يتم نقل وصلة الحظر على الفور إلى حالة إذا تم فقد وصلة إعادة التوجيه. لا تنتظر الميزة حالات و.

مجموعة الوصلات هي مجموعة من المنافذ لكل شبكة VLAN يمكنك التفكير فيها كمنفذ جذري ومنفذ جذري للنسخ الاحتياطي. في الظروف العادية، تضمن منافذ الجذر الاتصال من الوصول إلى الجذر. إذا فشل اتصال الجذر الأساسي هذا لأي سبب، فيبدأ إرتباط جذر النسخ الاحتياطي في العمل على الفور، دون الحاجة إلى المرور عبر تأخير التقارب النموذجي الذي يبلغ 30 ثانية.

بما أن Uplinkfast يتخطى بشكل فعال عملية معالجة تغيير مخطط STP العادي (و)، فمن الضروري وجود آلية بديلة لإصلاح المخطط. تحتاج الآلية إلى تحديث المحولات في المجال بالمعلومات التي تفيد بأنه يمكن الوصول إلى المحطات الطرفية المحلية عبر مسار بديل. وبالتالي، فإن محول طبقة الوصول الذي يشغل Uplinkfast يقوم أيضا بتوليد إطارات لكل عنوان MAC في جدول CAM الخاص به إلى عنوان MAC معروف متعدد البث (0c-cd-cd-cd HDLC-00-01 بروتوكول 0x200a). تقوم هذه العملية بتحديث جدول CAM في جميع المحولات في المجال باستخدام الطبولوجيا الجديدة.

توصيات Cisco

cisco يوصي أن يمكن أنت Uplinkfast للوصول مفتاح مع ميناء محظور إن أنت تركض 802.1D يجسر - شجرة. لا تستخدم Uplinkfast على المحولات دون معرفة المخطط الضمنية للارتباط الجذري للنسخ الاحتياطي—وبشكل نموذجي التوزيع والمحولات الأساسية في تصميم Cisco متعدد الطبقات. بشكل عام، لا تقم بتمكين Uplinkfast على محول بأكثر من طريقتين خارج الشبكة. إذا كان المحول في بيئة وصول معقدة ولك أكثر من حظر إرتباط واحد وإعادة توجيه إرتباط واحد، فيمكنك تجنب إستخدام هذه الميزة على المحول أو إستشارة مهندس الخدمات المتقدمة لديك.

أصدرت هذا أمر عام in order to مكنت Uplinkfast:

```
Switch(config)#spanning-tree uplinkfast
```

لا يقوم هذا الأمر في برنامج Cisco IOS software تلقائيا بضبط جميع قيم أولوية الجسر على قيمة عالية. بدلا من ذلك، يقوم الأمر فقط بتغيير شبكات VLAN تلك بأولوية جسر لم يتم تغييرها يدويا إلى قيمة أخرى. بالإضافة إلى ذلك، وعلى عكس CatOS، عندما تقوم باستعادة محول تم تمكين Uplinkfast عليه، فإن الصيغة no من هذا الأمر (**no** spanning-**tree uplinkfast**) ترجع كل القيم التي تم تغييرها إلى قيمها الافتراضية. لذلك، عند إستخدام هذا الأمر، يجب عليك التحقق من الحالة الحالية لأولويات الجسر قبل وبعد لضمان تحقيق النتيجة المطلوبة.

ملاحظة: تحتاج إلى الكلمة الأساسية **all protocols** لأمر Uplinkfast عند تمكين ميزة تصفية البروتوكول. لأن CAM يسجل البروتوكول نوع وكذلك ماك و VLAN معلومة عندما بروتوكول مكنت بيصفي، Uplinkfast إطار ينبغي كنت ولدت ل كل بروتوكول على كل عنوان MAC. تشير الكلمة الأساسية **rate** إلى الحزم في الثانية من إطارات تحديث مخطط Uplinkfast. ينصح بالافتراض. أنت لا تحتاج أن يشكل Uplinkfast مع RSTP لأن الآلية تضمنت طبيعي

ومكنت تلقائيا في RSTP.

باكبون فاست

الغرض

توفر BackboneFast تقاربا سريعا من حالات فشل الارتباط غير المباشر. تعمل تقنية BackboneFast على تقليل أوقات التقارب من الإعداد الافتراضي الذي يبلغ 50 ثانية إلى 30 ثانية في العادة، وبهذه الطريقة تضيف الوظائف إلى بروتوكول الشجرة المتفرعة (STP). مرة أخرى، لا تنطبق هذه الميزة إلا عند تشغيل 802.1D. لا تقم بتكوين الميزة عند تشغيل PVST السريع أو MST (والذي يتضمن المكون السريع).

نظرة عامة على العمليات

يبدأ BackboneFast عندما يستلم منفذ جذري أو منفذ محظور على محول وحدات بيانات بروتوكول الجسر (BPDU) سفلية من الجسر المعين. يستقبل المنفذ عادة وحدات بيانات بروتوكول الجسر (BPDU) الدنيا عندما يفقد محول من الخادم الاتصال بالجذر ويبدأ في إرسال وحدات بيانات بروتوكول الجسر (BPDUs) من أجل إختيار جذر جديد. تعرف وحدة بيانات بروتوكول الجسر (BPDU) السفلية المحول على أنه كل من الجسر الرئيسي والجسر المعين.

تحت قواعد الشجرة المتفرعة العادية، يتجاهل المحول المتلقي وحدات بيانات بروتوكول الجسر (BPDUs) الأدنى لوقت الحد الأقصى الذي تم تكوينه. بشكل افتراضي، تكون العظمة 20 ثانية. ولكن مع تقنية BackboneFast، يرى المحول وحدة بيانات بروتوكول الجسر (BPDU) المتدنية المستوى كإشارة إلى التغيير المحتمل في المخطط. يستخدم المحول وحدات بيانات بروتوكول الجسر (BPDU) لاستعلام الارتباط الجذري (RLQ) لتحديد ما إذا كان لديه مسار بديل للجسر الرئيسي. تتيح إضافة بروتوكول RLQ هذا للمحول إمكانية التحقق مما إذا كان الجذر لا يزال متوفرا. يقوم RLQ بنقل منفذ محظور إلى مسبقا ويخطر المحول المعزول الذي أرسل وحدة بيانات بروتوكول الجسر (BPDU) الأدنى التي لا يزال الجذر موجودا.

فيما يلي بعض الميزات البارزة لعملية البروتوكول:

- يرسل المحول حزمة RLQ خارج المنفذ الرئيسي فقط (وهو ما يعني أن الحزمة تنتقل إلى الجذر).
- يمكن للمحول الذي يستقبل RLQ الرد إذا كان المحول الجذري، أو إذا كان هذا المحول يعرف أنه فقد الاتصال بالجذر. إذا كان المحول لا يعرف هذه الحقائق، فيجب عليه إعادة توجيه الاستعلام إلى خارج المنفذ الرئيسي الخاص به.
- إذا فقد المحول الاتصال بالجذر، فيجب على المحول الرد بالنفي على هذا الاستعلام.
- يجب إرسال الرد فقط من المنفذ الذي جاء منه الاستعلام.
- يجب أن يستجيب المحول الجذري دائما لهذا الاستعلام برد إيجابي.
- إذا تم إستلام الرد على منفذ غير جذري، فعليك بتجاهل الرد.

يمكن أن تعمل العملية على تقليل أوقات تقارب بروتوكول الشجرة المتفرعة (STP) حتى 20 ثانية لأن الحد الأقصى لا يحتاج إلى انتهاء الصلاحية. راجع فهم وتكوين Backbone Fast على محولات Catalyst للحصول على مزيد من المعلومات.

توصيات Cisco

قم بتمكين BackboneFast على جميع المحولات التي تشغل بروتوكول الشجرة المتفرعة (STP) فقط إذا كان مجال الشجرة المتفرعة بأكمله يمكنه دعم هذه الميزة. يمكنك إضافة الميزة دون مقاطعة لشبكة إنتاج.

أصدرت هذا أمر شامل in order to مكنت BackboneFast:

```
Switch(config)#spanning-tree backbonefast
```

ملاحظة: يجب تكوين هذا الأمر على المستوى العام على جميع المحولات في مجال ما. الأمر يضيف وظائف إلى

بروتوكول الشجرة المتفرعة (STP) التي تحتاج جميع المحولات إلى فهمها.

خيارات أخرى

لا يساند BackboneFast على مادة حفازة 2900xl و 3500xl مفتاح. بصفة عامة، يحتاج أنت أن يمكن BackboneFast إن المفتاح مجال يحتوي هذا مفتاح بالإضافة إلى مادة حفازة 4000/4500، 5000/5500، و 6000/6500 مفتاح. عندما تطبق BackboneFast في بيئات ذات محولات XL، تحت طوبولوجيا صارمة، أنت يستطيع مكنت السمة حيث ال xl مفتاح آخر مفتاح في خط و فقط يربط إلى لب في مكانين. لا تقم بتنفيذ هذه الميزة إذا كانت بنية محولات XL في وضع سلسلة متسلسلة.

لا تحتاج إلى تكوين BackboneFast باستخدام RSTP أو 802.1w لأن الآلية يتم تضمينها بشكل طبيعي ويتم تمكينها تلقائيا في RSTP.

حماية تكرار الشجرة الممتدة

حماية التكرار هي تحسين Cisco خاص ل STP. يحمي حماية حماية التكرار الحلقي شبكات الطبقة 2 من حلقات التكرار التي تحدث بسبب حدوث عطل في واجهة الشبكة، أو وحدة المعالجة المركزية (CPU) المشغولة، أو أي شيء يمنع إعادة التوجيه العادية لوحدات بيانات بروتوكول الجسر (BPDUs). يتم إنشاء حلقة STP عند منفذ حظر في عمليات انتقال خاطئة للمخطط المتكرر إلى حالة إعادة التوجيه. وهذا يحدث عادة لأن أحد المنافذ في مخطط متكرر ماديا (ليس بالضرورة منفذ الحظر) توقف عن تلقي وحدات بيانات بروتوكول الجسر (BPDUs).

يكون حماية التكرار الحلقي مفيدا فقط في الشبكات المحولة حيث يتم توصيل المحولات بروابط من نقطة إلى نقطة، كما هو الحال في معظم شبكات شبكات المجمعات ومركز البيانات الحديثة. والفكرة هنا هي أن الجسر المعين، على خط الاتصال من نقطة إلى نقطة، من غير الممكن أن يختفي من دون إرسال وحدات بيانات بروتوكول الجسر (BPDU) أقل درجة أو قطع الاتصال. تم إدخال ميزة "حماية حلقة بروتوكول الشجرة المتفرعة (STP)" في الإصدار E(13)12.1 من برنامج Catalyst Cisco IOS Software لمادة حفازة 6500 وبرنامج Cisco IOS الإصدار EA1(9)12.1 لمحولات Catalyst 4500 switches.

راجع تحسينات بروتوكول الشجرة المتفرعة باستخدام ميزات "حماية التكرار الحلقي" و BPDU Skew Detection للحصول على مزيد من المعلومات حول حماية التكرار الحلقي.

نظرة عامة على العمليات

حماية التكرار الحلقي للتحقق مما إذا كان منفذ جذري أو منفذ جذر بديل/إحتياطي يستلم وحدات بيانات بروتوكول الجسر (BPDUs). إن لا يستلم الميناء BPDUs، أنشوطة حارس يضع الميناء داخل دولة غير متناسق (يقيد) إلى أن هو يبدأ أن يستلم BPDUs ثانية. لا يبث ميناء في الدولة غير متناسق BPDUs. إن يستلم هذا ميناء BPDUs ثانية، الميناء (وربط) اعتبرت usable ثانية. أزلت الحلقي-متناقض شرط من الميناء، و STP يعين الميناء دولة. وبهذه الطريقة يصبح التعافي تلقائيا.

يعزل حماية التكرار الحلقي الفشل ويتيح للشجرة المتفرعة التقارب إلى مخطط ثابت دون فشل الارتباط أو الجسر. يمنع حماية التكرار الحلقي حلقات تكرار بروتوكول الشجرة المتفرعة (STP) مع سرعة إصدار STP قيد الاستخدام. لا يوجد اعتماد على بروتوكول الشجرة المتفرعة (STP) نفسه (802.1D أو 802.1w) أو عند ضبط أجهزة توقيت بروتوكول الشجرة المتفرعة (STP). ل هذا سبب، cisco يوصي أن يطبق أنت أنشوطة حارس مع UDLD في طوبولوجيا أن يعتمد على STP وحيث البرمجية يساند السمة.

عندما يقوم حماية التكرار الحلقي بحظر منفذ غير متناسق، يتم تسجيل هذه الرسالة:

```
SPANTREE-SP-2-LOOPGUARD_BLOCK: Loop guard blocking port GigabitEthernet2/1 on VLAN0010%
```

عقب إستلمت ال BPDU على ميناء في أنشوطة-متناقض STP دولة، الميناء إنتقال إلى آخر STP دولة. ووفقا لوحدة بيانات بروتوكول الجسر (BPDU) المستلمة، فإن هذا يعني أن الاسترداد يتم بشكل تلقائي، ولا يلزم أي تدخل. بعد الاسترداد، يتم تسجيل هذه الرسالة:

```
SPANTREE-SP-2-LOOPGUARD_UNBLOCK: Loop guard unblocking port GigabitEthernet2/1 on%
VLAN0010
```

التفاعل مع ميزات STP الأخرى

حماية الجذر

يفرض حماية الجذر تخصيص المنفذ دائما. يكون حماية التكرار الحلقي فعالة فقط إذا كان المنفذ هو المنفذ الرئيسي أو المنفذ البديل، مما يعني أن وظائفها حصرية بشكل متبادل. لذلك، أنشوطة حارس وجذر حارس يستطيع لا يكون مكنت على ميناء في نفس الوقت.

Uplinkfast

حماية التكرار الحلقي متوافقة مع Uplinkfast. إذا قام حماية التكرار الحلقي بوضع منفذ جذري في حالة حظر، فإن Uplinkfast يضع منفذ جذر جديد في حالة إعادة التوجيه. أيضا، لا ينتقي Uplinkfast *ميناء متناقض أنشوطة* كميناء جذري.

باكبون فاست

حماية التكرار الحلقي متوافقة مع BackboneFast. يتم تشغيل BackboneFast عن طريق إستقبال وحدة بيانات بروتوكول الجسر (BPDU) سفلية المستوى تأتي من جسر معين. لأن BPDUs يكون إستلمت من هذا خطوة، أنشوطة حارس لا يركل في. لذلك، فإن BackboneFast و حماية التكرار الحلقي متوافقان.

PortFast

يقوم PortFast بنقل منفذ ما إلى حالة إعادة التوجيه المعينة مباشرة عند الارتباط. لأن PortFast-enabled ميناء ليس جذر/بديل ميناء، أنشوطة حارس و PortFast مشترك خاص.

PAgP

يستخدم حماية التكرار الحلقي المنافذ المعروفة ب STP. لذلك، يمكن أن يستفيد حارس الحلقة من تجريد المنافذ المنطقية التي يوفرها PAgP. غير أن، in order to شكلت قناة، all the physical ميناء مجموعة في القناة ينبغي يتلقى تشكيل متوافق. يفرض PAgP تشكيل موحد من أنشوطة حارس على all the ميناء طبيعي in order to شكلت قناة. لاحظ هذا تحذير عندما يشكل أنت أنشوطة حارس على EtherChannel:

- ينتقي STP دائما أول ميناء عملياتي في القناة أن يرسل ال BPDUs. إذا أصبح ذلك الرابط أحادي الإتجاه، يمنع واقي التكرار القناة، even if آخر خطوة في القناة تعمل بشكل صحيح.
- إذا تم تجميع مجموعة من المنافذ التي تم حظرها بالفعل بواسطة واقي التكرار الحلقي معا لتكوين قناة، فإن بروتوكول الشجرة المتفرعة (STP) يفقد جميع معلومات الحالة لتلك المنافذ، ويمكن أن يصل منفذ القناة الجديد إلى حالة إعادة التوجيه باستخدام دور معين.
- إذا تم حظر قناة بواسطة حماية التكرار الحلقي وانكسرت القناة، فإن بروتوكول الشجرة المتفرعة (STP) يفقد جميع معلومات الحالة. يمكن للمنافذ المادية الفردية الوصول إلى حالة إعادة التوجيه بدور معين، حتى إذا كان أحد الروابط التي شكلت القناة أحادي الإتجاه أو أكثر.

في هاتين الحالتين الأخيرتين، هناك إمكانية حدوث تكرار حلقي حتى يكتشف UDLD الفشل. ولكن حماية التكرار الحلقي لا يمكنها الكشف عنه.

مقارنة ميزة Loop Guard و UDLD

يتداخل جزئيا بين حماية التكرار الحلقي ووظيفة UDLD، جزئيا بمعنى أن كلا منهما يحمي ضد فشل STP الذي تسببه الارتباطات أحادي الإتجاه. وتختلف هاتان السمتان في النهج المتبع إزاء المشكلة وفي الأداء الوظيفي أيضا. تحديدا، هناك خاص أحادي إتجاه إخفاق أن UDLD يعجز أن يكشف، مثل إخفاق أن يكون بسبب CPU أن لا يرسل BPDUs. وبالإضافة إلى ذلك، يمكن أن يؤدي إستخدام توقيتات STP القوية ووضع RSTP إلى تكرارات حلقية قبل أن يتمكن

UDLD من اكتشاف حالات الفشل.

لا يعمل حماية التكرار الحلقي على الارتباطات المشتركة أو في الحالات التي يكون فيها الارتباط أحادي الإتجاه منذ الارتباط. في حالة وجود إرتباط أحادي الإتجاه منذ الارتباط، لا يستقبل المنفذ وحدات بيانات بروتوكول الجسر (BPDUs) أبدا ويصبح معينا. هذا يستطيع كنت سلوك عادي، لذلك أنشوطة حارس لا يغطي هذه الحالة خاص. UDLD يوفر حماية ضد هذا سيناريو.

يزود التمكين من كلا UDLD و أنشوطة حارس أعلى مستوى حماية. ل كثير معلومة على سمة مقارنة بين أنشوطة حارس و UDLD، أحلت:

- *حماية التكرار الحلقي مقابل* قسم *اكتشاف الارتباط أحادي الإتجاه* من تحسينات بروتوكول الشجرة المتفرعة باستخدام حماية التكرار الحلقي ومميزات اكتشاف تشوه BPDU
- UDLD قسم من هذا وثيقة

توصيات Cisco

cisco يوصي أن أنت يمكن أنشوطة حارس بشكل عام على مفتاح شبكة مع أنشوطة طبيعي. أنت يستطيع مكنت أنشوطة حارس بشكل عام على كل ميناء. بشكل فعال، مكنت السمة على كل خطوة إلى نقطة. يتم اكتشاف إرتباط نقطة إلى نقطة بواسطة حالة الإرسال ثنائي الإتجاه الخاصة بالارتباط. إذا كان الإرسال ثنائي الإتجاه ممتلئا، فسيتم إعتبار الارتباط من نقطة إلى نقطة.

```
Switch(config)#spanning-tree loopguard default
```

خيارات أخرى

بالنسبة للمحولات التي لا تدعم تكوين واقي تكرار حلقي عالمي، فإن التوصية هي تمكين الميزة على جميع المنافذ الفردية، والتي تتضمن منافذ قناة المنفذ. على الرغم من أن هناك ما من فائدة إن يمكن أنت أنشوطة حارس على يعين ميناء، لا يعتبر التمكين إصدار. وبالإضافة إلى ذلك، يمكن لإعادة تقارب الشجرة المتفرعة الصالحة بالفعل تحويل منفذ محدد إلى منفذ جذري، مما يجعل الميزة مفيدة على هذا المنفذ.

```
#Switch(config)#interface type slot#/port
Switch(config-if)#spanning-tree guard loop
```

الشبكات ذات الطوبولوجيا الخالية من الحلقة ما تزال يمكن أن تستفيد من حماية التكرار الحلقي في حالة أن حلقات التكرار تم تقديمها بشكل عرضي. ولكن، يمكن أن يؤدي تمكين حماية التكرار في هذا النوع من المخطط إلى مشاكل في عزل الشبكة. إذا قمت بإنشاء مخطط خال من الحلقة وكنت ترغب في تجنب مشاكل عزل الشبكة، يمكنك تعطيل حماية التكرار الحلقي بشكل عام أو بشكل فردي. عدم تمكين حماية التكرار الحلقي على الارتباطات المشتركة.

```
Switch(config)#no spanning-tree loopguard default
.This is the global configuration ---!
```

أو

```
#Switch(config)#interface type slot#/port
Switch(config-if)#no spanning-tree guard loop
.This is the interface configuration ---!
```

حماية جذر الشجرة الممتدة

تُوفر ميزة Root Guard طريقة لفرض إدخال الجسر الرئيسي في الشبكة. يضمن واقي الجذر أن المنفذ الذي يتم تمكين واقي الجذر عليه هو المنفذ المعين. عادةً ما تكون جميع منافذ الجسر الرئيسي عبارة عن منافذ مُعينة، ما لم يتم توصيل منفذين أو أكثر للجسر الرئيسي معًا. إذا كان الجسر يستلم وحدات بيانات بروتوكول الشجرة المتفرعة

(STP) فائقة على منفذ يدعم الواقي، فإن الجسر ينقل هذا المنفذ إلى حالة STP غير متوافقة مع الجذر. إن حالة عدم اتساق الجذر هذه تساوي فعليًا حالة الاستماع (Listening State). لا تتم إعادة توجيه حركة المرور عبر هذا المنفذ. وبهذه الطريقة، يفرض Root Guard موضع الجسر الرئيسي. يتوفر حماية الجذر في الإصدار 12.1E من برنامج Cisco IOS Software السابق جدا والإصدارات الأحدث.

نظرة عامة على العمليات

حماية الجذر هي آلية مدمجة لبروتوكول الشجرة المتفرعة (STP). لا يحتوي Root Guard على مؤقت خاص به ويعتمد على إستقبال وحدات بيانات بروتوكول الجسر (BPDUs) فقط. عندما يطبق حارس جذر على ميناء، هو ينكر هذا ميناء الإمكانية أن يصبح جذر ميناء. إن يستلم من BPDU يشعل يجسر - شجرة تقارب أن يجعل يعين ميناء يصبح جذر ميناء، الميناء بعد ذلك وضعت في جذر حالة متناقض. توضح رسالة syslog هذه:

```
SPANTREE-SP-2-ROOTGUARD_BLOCK: Root guard blocking port GigabitEthernet2/1 on VLAN0010%
```

عقب توقف الميناء أن يرسل أعلى BPDUs، الميناء يكون unblocking ثانية. عبر STP، ينتقل المنفذ من حالة الاستماع (Listening State) إلى حالة التعلّم (Learning State)، وفي النهاية ينتقل إلى حالة إعادة التوجيه (Forwarding State). تظهر رسالة syslog هذه المرحلة الانتقالية:

```
SPANTREE-SP-2-ROOTGUARD_UNBLOCK: Root guard unblocking port GigabitEthernet2/1%
on VLAN0010
```

الاسترداد تلقائي. لا يلزم التدخل البشري.

لأن حماية الجذر تفرض تخصيص منفذ ما ويكون واقي التكرار فعالا فقط إذا كان المنفذ هو منفذ جذري أو منفذ بديل، فإن الوظائف تكون خاصة بالتبادل. لذلك، أنت يستطيع لا يمكن يمكن أنشوطة حارس وجذر حارس على ميناء في نفس الوقت.

راجع تحسين واقي جذر بروتوكول الشجرة المتفرعة للحصول على مزيد من المعلومات.

توصيات Cisco

توصيك Cisco بتمكين ميزة "الواقي الجذر" على المنافذ المتصلة بأجهزة الشبكة التي لا تكون تحت التحكم الإداري المباشر. استعملت in order to شكلت الجذر حارس، هذا أمر عندما أنت في قارن تشكيل أسلوب:

```
#Switch(config)#interface type slot#/port
Switch(config-if)#spanning-tree guard root
```

EtherChannel

الغرض

تتضمن EtherChannel خوارزمية توزيع الإطارات التي تضاعف الإطارات بكفاءة عبر المكون 100/10 ميجابت في الثانية أو روابط جيجابت. تتيح خوارزمية توزيع الإطارات التجميع المعكوس لقنوات متعددة في إرتباط منطقي واحد. على الرغم من أن كل نظام أساسي يختلف عن النظام الأساسي التالي في التطبيق، إلا أنه يجب عليك فهم هذه الخصائص المشتركة:

- يجب أن تكون هناك خوارزمية لمضاعفة الإطارات إحصائيا عبر قنوات متعددة. في محولات Catalyst، يكون هذا الأمر متعلقا بالأجهزة. وفيما يلي أمثلة:مادة حفازة 5000s/5500 — وجود أو عدم وجود شريحة تجميع إيثرنت (EBC) على الوحدة النمطيةمادة حفازة 6000s/6500- خوارزمية أن يستطيع قرأت أكثر في الإطار ومضروبة في عنوان IP
- هناك الخلق من قناة منطقي لذلك أن يكون مثيل وحيد من STP يستطيع كنت ركضت أو وحيد تحشد نظير

يستطيع كنت استعملت، أي يعتمد على إن هو طبقة 2 أو طبقة 3 EtherChannel.
- يوجد بروتوكول إدارة للتحقق من تناسق المعلمة في أي من طرفي الارتباط وللمساعدة في إدارة تجميع الاسترداد من فشل الارتباط أو إضافته. هذا بروتوكول يستطيع كنت PAgP أو خطوة تراكم تحكم بروتوكول (LACP).

نظرة عامة على العمليات

تشتمل EtherChannel على خوارزمية توزيع الإطارات التي تقوم بضرب الإطارات بكفاءة عبر المكون 100/10 ميجابت في الثانية، أو روابط جيجابت أو 10-جيجابت. تنشأ الاختلافات في الخوارزميات لكل نظام من قدرة كل نوع من الأجهزة على إستخلاص معلومات رأس الإطار لاتخاذ قرار التوزيع.

خوارزمية توزيع الحمل هي خيار عام لكل من بروتوكولات التحكم في القناة. يستخدم كل من PAgP و LACP خوارزمية توزيع الإطارات لأن معيار IEEE لا يتطلب أي خوارزميات توزيع معينة. ولكن، تضمن أي خوارزمية توزيع أنه عندما يتم تلقي الإطارات، فإن الخوارزمية لا تتسبب في سوء ترتيب الإطارات التي تعد جزءا من أي محادثة أو تكرار للإطارات.

يوضح هذا الجدول خوارزمية توزيع الإطارات بالتفصيل لكل نظام أساسي مدرج:

النظام الأساسي	خوارزمية موازنة حمل القناة
Catalyst 3750 Series	يوازن Catalyst 3750 الذي يعمل ببرنامج Cisco IOS Software خوارزمية تستخدم عناوين MAC أو عناوين IP، وإما مصدر الرسالة أو وجهة

	الرسالة، أو كليهما.
Catalyst 4500 Series	مادة حفازة 4500 أن يركض cisco ios برمجية موازنة خوارزمية أن يستعمل {upper}mac address، ip address، أو طبقة 4 (L4) ميناء رقم، وأي من الرسالة مصدر أو رسالة غاية، أو كلا.
Catalyst 6500/6000 Series	هناك خوارزميات تجزئة يمكن إستخ

	دامها، والتي تعتمد على أجهز ة Supervisor Engine (محر ك المش رف). التجزئ ة هي متعدد حدود من الدرج ة السابـ عة عشر ة التي تطبق في الأجه زة. في جميع الحالا ت، تأخذ التجزئ ة رقم منفذ MAC أو عنوان IP أو IP IP TCP /UDP وتطبـ ق الخوا رزمية

	لإنشاء قيمة 3 بت. تحدث هذه العملية بشكل منفصل لكل من SAs و DAs. وبعد ذلك يتم إستخدام عملية XOR مع النتائج لإنشاء قيمة 3 بت أخرى. تحدد القيمة المنفذ الذي يتم إستخدامه في القناة لإعادة توجيه الحزمة. يمكن تكوين القنوات على

	المادة حفازة 6500/600 0 بين المنافذ على أي وحدة نمطية ويمكن أن يكون حتى ثمانية منافذ.

يشير هذا طاولة التوزيع طريقة أن يكون ساندت على المختلف مادة حفازة 6000/6500 مشرف محرك نموذج. يظهر الجدول أيضا السلوك الافتراضي:

الأجهزة	الوصف	طرق التوزيع
WS-F6020a (محرك الطبقة 2) WS-F6K-PFC (محرك الطبقة 3)	محرك المشرف i ومحرك المشرف Supervisor Engine IA Supervisor Engine IA/بطاقة ميزة السياسة 1 (PFC1) فيما بعد	عناوين التحكم في الوصول للوسائط من المستوى الثاني: SA و DA و SA و DA من المستوى الثالث: SA و DA و SA و DA (الافتراضي)
WS-F6K-PFC 2	محرك المشرف II/PFC2	MAC من المستوى 2: SA؛ DA؛ SA و DA من المستوى 3 IP: SA؛ DA؛ SA و DA (الافتراضي) جلسة

		الطبقة 4: منفذ S؛ منفذ D؛ منفذ S و D
WS-F6K-PFC3A WS-F6K-PFC3B WS-F6K-PFC3BXL	محرك المشرف PFC3A/720 Supervisor Engine 720/Supervisor Engine 32/PFC3B Supervisor Engine 720/PFC3BXL	MAC من المستوى 2: SA؛ DA؛ SA و DA من المستوى 3 IP: SA؛ DA؛ SA و DA (الافتراضي) جلسة الطبقة 4: منفذ S؛ منفذ D؛ منفذ S و D

ملاحظة: باستخدام توزيع الطبقة الرابعة، تستخدم الحزمة الأولى المجزأة التوزيع من الطبقة الرابعة. تستخدم جميع الحزم التالية توزيع الطبقة 3.

ملاحظة: أحلت هذا وثيقة in order to وجدت كثير معلومة حول EtherChannel دعم على آخر منصة وكيف أن يشكل واستكشاف أخطاء EtherChannel وإصلاحها:

- يفهم EtherChannel تحميل موازنة وتكرار على مادة حفازة مفتاح
- يشكل طبقة 3 وطبقة EtherChannel 2 (مادة حفازة 6500 sery cisco ios برمجية تشكيل مرشد، 12.2SX)
- تكوين الطبقة 3 والطبقة EtherChannel 2 (دليل تكوين برنامج Catalyst 6500 Series Cisco IOS Software، الإصدار 12.1E)
- يشكل EtherChannel (مادة حفازة 4500 sery مفتاح cisco ios برمجية تشكيل مرشد، 12.2(31)sg)
- يشكل EtherChannels (مادة حفازة 3750 مفتاح برمجية تشكيل مرشد، 12.2(25)SEE)
- تكوين قناة EtherChannel بين مُبدلات Catalyst 4500/4000 و5000/5500 و6000/6500 التي تعمل ببرنامج نظام CatOS

توصيات Cisco

مادة حفازة 3750، مادة حفازة 4500، ومادة حفازة 6000/6500 sery ينجز مفتاح موازنة حمل عن طريق تجزئة على حد سواء المصدر والوجهة عنوان افتراضيا. ويوصى بذلك، مع افتراض أن IP هو البروتوكول السائد. أصدرت هذا أمر in order to ثبتت حمل موازنة:

```
port-channel load-balance src-dst-ip
!--- This is the default.
```

خيارات أخرى

على حسب تدفقات حركة المرور، أنت يستطيع استعملت طبقة 4 توزيع in order to حسنت تحميل موازنة إن غالبية الحركة مرور يكون بين ال نفسه مصدر وغاية عنوان. أنت ينبغي فهمت أن، عندما طبقة 4 شكلت توزيع، التجزئة فقط يتضمن طبقة 4 مصدر وغاية ميناء. ولا تقوم بدمج عناوين IP للطبقة 3 في خوارزمية التجزئة. أصدرت هذا أمر in order to ثبتت حمل موازنة:

```
port-channel load-balance src-dst-port
```

ملاحظة: التوزيع من الطبقة الرابعة غير قابل للتكوين على المحولات من السلسلة Catalyst 3750.

أصدرت **العرض etherChannel load-balance** أمر in order to فحصت الإطار توزيع سياسة.

حسب العتاد منصة، أنت يستطيع استعملت CLI أمر in order to حددت أي قارن في EtherChannel يرسل الحركة مرور تدفق خاص، مع الإطار توزيع سياسة كأساس.

بالنسبة لمحولات Catalyst 6500 switches، قم بإصدار الأمر **login switch عن بعد** لتسجيل الدخول عن بعد إلى وحدة تحكم معالج المحول (SP). بعد ذلك، أصدرت **الاختبار EtherChannel load-balanced قارن *port-channel* رقم {*dest_ip_add* | *source_mac_add* | *source_l4_port*] [*dest_ip_add* | *source_mac_add* | *source_l4_port*] {ip | L4port | mac}** أمر.

بالنسبة للمحولات Catalyst 3750 switches، قم بإصدار **إختبار *port-*EtherChannel load-balance interface *channel number* {ip | mac} [*source_ip_add* | *source_mac_add*] [*dest_ip_add* | *dest_mac_add*]** أمر.

بالنسبة لمادة حفازة 4500، لا يتوفر الأمر المكافئ بعد.

قيود وإرشادات تكوين EtherChannel

يتحقق EtherChannel من خصائص أيسر على كل ميناء طبيعي قبل أن يجمع هو ميناء متوافق إلى ميناء منطقي وحيد. تختلف إرشادات وقيود التكوين الخاصة بمنصات المحولات المختلفة. أكمل هذه الإرشادات والقيود لتجنب مشاكل التجميع. على سبيل المثال، إذا تم تمكين جودة الخدمة، فإن EtherChannels لا يتم تكوينها عند تجميع وحدات تحويل Catalyst 6500/6000 series مع إمكانيات جودة الخدمة المختلفة. لمادة حفازة 6500 مفتاح أن يركض cisco ios برمجية، أنت يستطيع أعجزت ال QoS ميناء سمة تدقيق على EtherChannel يجمع مع ال **ما من mls qos قناة تناسق** ميناء قارن أمر. يعرض الأمر **show interface capability *mod/port*** إمكانية منفذ جودة الخدمة (QoS) ويحدد ما إذا كانت المنافذ متوافقة.

أحلت هذا guidelines لمنصات مختلف in order to تفاديت تشكيل مشكلة:

- بشكل طبقة 3 وطبقة EtherChannel 2 (مادة حفازة 6500 sery cisco ios برمجية تشكيل مرشد، 12.2SX)
- تكوين الطبقة 3 والطبقة EtherChannel 2 (دليل تكوين برنامج Catalyst 6500 Series Cisco IOS Software، الإصدار 12.1E)
- بشكل EtherChannel (مادة حفازة 4500 sery مفتاح cisco ios برمجية تشكيل مرشد، 12.2(31)sg)
- بشكل EtherChannels (مادة حفازة 3750 مفتاح برمجية تشكيل مرشد، 12.2(25)SEE)

يعتمد العدد الأقصى من EtherChannels أن يكون ساندت أيضا على الجهاز منصة وبرمجية إطلاق. مادة حفازة 6500 يساند مفتاح أن يركض cisco ios برمجية إطلاق 12.2(18)sxe وفيما بعد حد أقصى 128 ميناء قناة قارن. تدعم إصدارات البرامج الأقدم من برنامج Cisco IOS الإصدار 12.2(18)SXE حد أقصى 64 واجهة قناة منفذ. يمكن أن يكون رقم المجموعة القابلة للتكوين من 1 إلى 256، بغض النظر عن إصدار البرنامج. مادة حفازة 4500 sery دعم مفتاح حد أقصى 64 EtherChannels. لمادة حفازة 3750 مفتاح، التوصية لا أن يشكل أكثر من 48 EtherChannels على المفتاح كومة.

حساب تكلفة منفذ الشجرة الممتدة

أنت ينبغي فهمت ال يجسر - شجرة أيسر تكلفة حساب ل EtherChannels. أنت يستطيع حسبت ال يجسر - شجرة ميناء تكلفة ل EtherChannels مع إما الأسلوب قصير أو طويل. بشكل افتراضي، يتم حساب تكلفة المنفذ في الوضع القصير.

يوضح هذا الجدول تكلفة منفذ الشجرة المتفرعة للطبقة EtherChannel 2 على أساس النطاق الترددي:

النطاق الترددي	قيمة STP القديمة	قيمة STP الطويلة الجديدة
10 ميغابت في الثانية	100	2,000,000
100 ميغابت في الثانية	19	200,000
1 جيجابت في الثانية	4	20,000
n x 1 جيجابت في الثانية	3	6660
10 جيجابت في الثانية	2	2,000
100 جيجابت في الثانية	غير متوفر	200
1 تيرابت في الثانية	غير متوفر	20
10 تيرابت في الثانية	غير متوفر	2

ملاحظة: في CatOS، ال يجسر - شجرة ميناء تكلفة ل EtherChannel يبقى نفسه بعد الميناء عضو خطوة إخفاق. في cisco ios برمجية، يتم تحديث تكلفة الميناء ل EtherChannel فورا in order to عكست الجديد يتوفر نطاق ترددي. إذا كان السلوك المرغوب هو تجنب تغييرات مخطط الشجرة المتفرعة غير الضرورية، فيمكنك تكوين تكلفة منفذ الشجرة المتفرعة بشكل ثابت باستخدام أمر ***تكلفة الشجرة المتفرعة***.

بروتوكول تجميع المنفذ (PAgP)

الغرض

PAgP هو بروتوكول إدارة يتحقق من اتساق المعلمة عند أي من طرفي الارتباط. كما يساعد PAgP القناة مع التكيف على فشل الرابط أو إضافته. فيما يلي خصائص PAgP:

- يتطلب PAgP أن ينتسب كل ميناء في القناة إلى ال نفسه VLAN أو يكون شكلت كشنطة ميناء. لأن شبكات VLAN الديناميكية يمكن أن تفرض التغيير من ميناء إلى VLAN مختلف، VLANs حركي لا يتضمن في EtherChannel مشاركة.
- عندما حزمة موجود بالفعل وتشكيل من ميناء عدلت، كل ميناء في الحزمة عدلت أن يماثل أن تشكيل. مثال على هذا التغيير تغيير في VLAN أو تغيير وضع .
- لا يقوم PAgP بتجميع المنافذ التي تعمل بسرعات مختلفة أو الإرسال ثنائي الإتجاه للمنفذ. إن غيرت سرعة ومزدوج يكون عندما حزمة يتواجد، PAgP يغير سرعة أيسر وزواج لكل ميناء في الحزمة.

نظرة عامة على العمليات

يتحكم منفذ PAgP في كل منفذ مادي (أو منطقي) فردي يتم تجميعه. يتم إستخدام عنوان MAC لمجموعة البث المتعدد نفسها التي يتم إستخدامها لحزم CDP لإرسال حزم PAgP. عنوان MAC هو 0c-cc-cc-00-01. ولكن، قيمة البروتوكول هي 0x0104. هذا ملخص لعملية البروتوكول:

- ما دام المنفذ الفعلي قيد التشغيل، يتم إرسال حزم PAgP كل ثانية أثناء الكشف، وكل 30 ثانية في حالة ثابتة.
- إذا تم إستلام حزم البيانات ولكن لا يتم إستلام حزم PAgP، فمن المفترض أن المنفذ متصل بجهاز غير قادر على PAgP.
- استمع لحزم PAgP التي تثبت أن المنفذ الفعلي لديه اتصال ثنائي الإتجاه بجهاز آخر قادر على PAgP.
- بمجرد إستلام حالتين من هذه الحزم على مجموعة من المنافذ المادية، حاول تكوين منفذ مجمع.
- إذا توقفت حزم PAgP لفترة من الزمن، فسيتم تقسيم حالة PAgP.

معالجة عادية

وتساعد هذه المفاهيم على توضيح سلوك البروتوكول:

- agport—منفذ منطقي يتكون من جميع المنافذ المادية في نفس التجميع ويمكن تحديده بواسطة SNMP ifIndex الخاص به. لا يحتوي المنفذ على منافذ غير عاملة.

- القناة—وهي تجميع يفي بمعايير التكوين. يمكن أن تحتوي القناة على منافذ غير عاملة وهي مجموعة فرعية من المنفذ. البروتوكولات، التي تتضمن بروتوكول الشجرة المتفرعة (STP) وبروتوكول الشجرة المتفرعة (VTP) ولكنها تستبعد بروتوكول CDP و DTP، يتم تشغيلها فوق PAgP عبر المنافذ. لا يمكن لأي من هذه البروتوكولات إرسال الحزم أو استقبالها حتى يقوم PAgP بإرفاق العناوين بمنفذ فعلي واحد أو أكثر.
- قدرة المجموعة- يحتوي كل منفذ ومنفذ طبيعي على معلمة تكوين تسمى . ميناء طبيعي يستطيع كنت جمعت مع أي آخر ميناء طبيعي أن يتلقى ال نفسه ، وفقط مع هذا ميناء طبيعي.
- إجراء التجميع- عندما يصل المنفذ الفعلي إلى حالة UpData أو UpPAgP، يتم إرفاق المنفذ بمنفذ مناسب. عندما يترك الميناء إما من هذا دولة آخر، الميناء فصلت من الميناء.

يوفر هذا الجدول المزيد من التفاصيل حول الحالات:

الحالة	معنى
UPdata	لم يتم تلقي حزم PAgP. يتم إرسال حزم PAgP. الميناء طبيعي هو الميناء وحيد أن يكون ربط إل

	إلى المينا. يتم تحرير مغير PAgP إلى الداخل والخارج بين المنفذ الفعلي ومنفذ الوصول.
	تم تلقي حزمة PAgP واحدة بالضبط تثبت

	وجود اتصال ثنائي الإتجاه إلى جدار واحد بالضبط. لا يتصل المنفذ المادي بأي منفذ. يتم إرسال حزم PAgP ويمكن استقبالها.
UPpaGP	ربط

هذا مينا طبيعي، مالا شتراك مع آخر مينا طبيعي إلى مينا. يتم إرسال حزم PAgP واستقبالها على المنفذ الفعلي. يتم تبديل حزم غير

	PAgP إلى الداخل والخارج بين المنفذ الفعلي ومنفذ الوصول.

يجب أن يتفق كلا طرفي الوصلتين على التجميع. يتم تحديد التجميع كأكبر مجموعة من المنافذ في المنفذ الذي ينتهي كلا المنفذين من تصريح الاتصال.

عندما يصل ميناء طبيعي إلى حالة UpPAgP، عينت الميناء إلى الميناء أن يتلقى عضو ميناء طبيعي أن يطابق من الميناء طبيعي جديد وأن يكون في BiDir أو الدولة UpPAgP. يتم نقل أي منافذ BiDir هذه إلى حالة UPgP في نفس الوقت. إن لا يوجد أي ميناء أن يتلقى يشكل ميناء معلم طبيعي أن يكون متوافق مع ال حديثا جاهز physical ميناء، الميناء عينت إلى ميناء مع معلم مناسب أن لا يتلقى ميناء طبيعي موحد.

يمكن أن تحدث مهلة PAgP على المجاور الأخير الذي يعرف على المنفذ الفعلي. أزلت الميناء أن وقت out من الميناء. في الوقت نفسه، تتم إزالة جميع المنافذ المادية على المنفذ نفسه الذي يحتوي على وحدات توقيت انتهت أيضا. وهذا يمكن السفينة التي ماتت طرفها الآخر من أن تنهار كلها مرة واحدة، بدلا من ميناء مادي واحد في كل مرة.

سلوك فاشل

في حالة فشل إرتباط موجود في قناة، يتم تحديث المنفذ ويتم تجزئة حركة المرور عبر الارتباطات التي تبقى دون فقدان. الأمثلة على هذا الفشل تشمل:

- المنفذ غير متصل
- تمت إزالة محول واجهة Gigabit (GBIC)
- الألياف مكسورة

ملاحظة: عند فشل إرتباط في قناة مع إيقاف تشغيل وحدة نمطية أو إزالتها، يمكن أن يكون السلوك مختلفا. وفقا للتعريف، تتطلب القناة منفذين حقيقيين. في حال فقد منفذ واحد من النظام في قناة ذات منفذين، فإن المنفذ المنطقي يتم مزقه ويتم إعادة تهيئة المنفذ الفعلي الأصلي فيما يتعلق بالشجرة المتفرعة. يمكن تجاهل حركة مرور البيانات حتى يسمح بروتوكول الشجرة المتفرعة (STP) للمنفذ بأن يصبح متوفرا للبيانات مرة أخرى.

هذا الاختلاف في وضعي الفشل مهم عند تخطيط صيانة الشبكة. يمكن أن يكون هناك تغيير في مخطط بروتوكول

الشجرة المتفرعة (STP) تحتاج إلى أخذه في الاعتبار عند إجراء إزالة أو إدخال وحدة نمطية عبر الإنترنت. يجب عليك إدارة كل إرتباط مادي في القناة باستخدام نظام إدارة الشبكة (NMS) لأن المنفذ يمكن أن يظل دون أية مشكلات من خلال فشل.

أتمت واحد من هذا توصيات in order to خففت غير مرغوب طبولوجيا تغير على المادة حفازة 6000/6500:

- إذا تم إستخدام منفذ واحد لكل وحدة نمطية لتكوين قناة، فاستخدم ثلاث وحدات أو أكثر (إجمالي ثلاث وحدات).
- إذا امتدت القناة عبر وحدتين، فاستخدم منفذين على كل وحدة نمطية (إجمالي أربعة).
- إن يكون إثنان ميناء قناة ضروري عبر إثنان بطاقة، يستعمل فقط المشرف محرك ميناء.

خيارات التكوين

أنت يستطيع شكلت EtherChannels في أسلوب مختلف، بما أن هذا طاولة يلخص:

نمط	الخيارات القابلة للتكوين
	PAgP ليس قيد التشغيل. الميناء قناة، regardless of the مجاور شكلت ميناء يكون. إن مجاور ميناء يكون نشط، قناة شكلت.
	التجميع تحت تحكم PAgP. يوضع المنفذ في حالة تفاوض سلبي. لا يتم إرسال حزم PAgP على الواجهة حتى يتم تلقي حزمة

	PAgP واحدة على الأقل تشير إلى أن المرسل يعمل في الوضع .
	التجميع تحت تحكم PAgP. يتم وضع المنفذ في حالة تفاوض نشطة، حيث يبدأ المنفذ المفاوضا ت مع المنافذ الأخرى عبر إرسال حزم PAgP. يتم تكوين قناة مع مجموعة منافذ أخرى في الوضع أو .
هذا التقصير على مادة حفازة fiber FE 5000/5500 و GE ميناء.	الكلمة الأساسية أو فيه. إذا لم يتم إستلام حزم بيانات على الواجهة، فلن يتم إرفاق الواجهة أبدا بمنفذ

	ولا يمكن إستخدامها للبيانات. تم توفير هذا التحقق من ثنائية الإتجاه لأجهزة Catalyst 5500/5000 المحددة لأن بعض حالات فشل الارتباط تؤدي إلى انقسام القناة. عند تمكين الوضع ، لا يسمح أبدا للمنفذ المجاور الذي يسترد بأن يعود مرة أخرى ويفصل القناة دون داع. تتوفر عملية التجميع الأكثر مرونة والتحقق المحسن من ثنائية الإتجاه بشكل افتراضي في أجهزة السلسلة Catalyst

	4500/4000 و 6/6500.000.
هذا التقصير على كل مادة حفازة 6000/6500 و 4000/4500 ميناء، as well as 5500/5000 نحاسي ميناء.	الكلمة الأساسية أو فيه. إن لا يستلم أي ربط بيانات على القارن، بعد 15 ثاني مهلة فترة، القارن ألحقت فقط إلى ميناء. وبالتالي، يمكن إستخدام الواجهة لنقل البيانات. يسمح الوضع أيضا بتشغيل القناة عندما يكون الشريك محلل أو خادم لا يرسل PAgP أبدا.

تؤثر الإعدادات / على كيفية تفاعل المنافذ مع المواقف التي تتسبب في حركة مرور موحدة الإتجاه. عندما ميناء يكون يعجز أن يبث بسبب فشل قارن طبيعي أو كبل أو ليف مكسور، الميناء مجاور يستطيع بعد كنت تركت في عملية دولة. يواصل الشريك نقل البيانات. ولكن، يتم فقد البيانات لأنه لا يمكن إستلام حركة المرور العائدة. كما يمكن أن تتكون حلقات الشجرة المتفرعة بسبب طبيعة الارتباط أحادي الإتجاه.

لبعض منافذ الألياف القدرة المرغوبة أن تجلب المنفذ إلى حالة عدم تشغيل عندما يفقد المنفذ إشارة الاستقبال (FEFI). يتسبب هذا الإجراء في أن يصبح منفذ الشريك غير عامل ويتسبب بشكل فعال في تعطل المنافذ على كلا طرفي الارتباط.

عندما تستخدم الأجهزة التي تنقل البيانات (BPDUs)، ولا يمكنك الكشف عن الشروط أحادي الإتجاه، أستخدم الوضع للسماح بأن تبقى المنافذ غير عاملة حتى تتوفر بيانات الاستلام ويتم التحقق من الارتباط ليكون ثنائي الإتجاه. الوقت الذي يستغرقه الأمر PAgP لاكتشاف إرتباط أحادي الإتجاه هو حوالي 3.5 * 30 ثانية = 105 ثانية. ثلاثين ثانية هي الوقت بين رسالتين متتاليتين ل PAgP. استعملت UDLD، أي يكون أسرع كاشف من خطوة أحادي إتجاه.

عندما تستخدم أجهزة لا ترسل أي بيانات، أستخدم الوضع . يفرض إستخدام الوضع على المنفذ أن يصبح متصلا ويعمل، بغض النظر عما إذا كانت البيانات المستلمة موجودة أم لا. وبالإضافة إلى ذلك، لتلك المنافذ التي يمكنها اكتشاف وجود شرط أحادي الإتجاه، يتم إستخدام الوضع بشكل افتراضي. أمثلة من هذا ميناء جديد منصة أن يستعمل طبقة 1 FEFI و UDLD.

أصدرت in order to منعت يقني على قارن، الأمر **no channel-group** رقم :

```
#Switch(config)#interface type slot#/port
Switch(config-if)#no channel-group 1
```

التحقق

يزود الجدول في هذا قسم خلاصة من all the يمكن PAgP يقني أسلوب سيناريو بين إثنان مباشرة يربط مفتاح A والمحول B. بعض من هذا خليط يستطيع سببت STP أن يضع الميناء على ال يقني جانب داخل `ErrDisable` دولة، لذلك هو يعني أن هذا خليط يعطل الميناء على ال يقني جانب. EtherChannel misconfiguration حارس مكنت سمة افتراضيا.

تبديل وضع القناة	وضع قناة المحول B	تبديل حالة القناة	حالة قناة المحول B
تشغيل	تشغيل	قناة (غير PAgP)	قناة (غير PAgP)
تشغيل	لم يتم التكوين	ليس قناة (errDisable)	ليس قناة
تشغيل	تلقائي	ليس قناة (errDisable)	ليس قناة
تشغيل	شيق	ليس قناة (errDisable)	ليس قناة
لم يتم التكوين	تشغيل	ليس قناة	ليس قناة (errDisable)
لم يتم التكوين	لم يتم التكوين	ليس قناة	ليس قناة
لم يتم التكوين	تلقائي	ليس قناة	ليس قناة
لم يتم التكوين	شيق	ليس قناة	ليس قناة
تلقائي	تشغيل	ليس قناة	ليس قناة (errDisable)
تلقائي	لم يتم التكوين	ليس قناة	ليس قناة
تلقائي	تلقائي	ليس قناة	ليس قناة
تلقائي	شيق	قناة PAgP	قناة PAgP
شيق	تشغيل	ليس قناة	ليس قناة
شيق	لم يتم التكوين	ليس قناة	ليس قناة
شيق	تلقائي	قناة PAgP	قناة PAgP
شيق	شيق	قناة PAgP	قناة PAgP

[توصيات تكوين قنوات Cisco من المستوى الثاني]

مكنت PAgP واستعملت إعداد من على كل EtherChannel خطوة. راجع هذا الإخراج للحصول على مزيد من المعلومات:

```
#Switch(config)#interface type slot#/port
Switch(config-if)#no ip address
This ensures that there is no IP !--- address that is assigned to the LAN port. ---!
Switch(config-if)#channel-group number mode desirable
.Specify the channel number and the PAgP mode ---!
```

دققت التشكيل بهذه الطريقة:

```
Switch#show run interface port-channel number
#Switch#show running-config interface type slot#/port
Switch#show interfaces type slot#/port# etherchannel
Switch#show etherchannel number port-channel
```

منع أخطاء تكوينات EtherChannel

أنت يستطيع misconfigure EtherChannel وأنشئ يجسر - شجرة أنشوطة. يمكن أن يتسبب سوء التكوين هذا في إرباك عملية المحول. يتضمن برنامج Cisco IOS System ميزة **config**حارس **EtherChannel** لمنع هذه المشكلة.

أصدرت هذا تشكيل أمر على كل مادة حفازة مفتاح أن يركض cisco ios برمجية كنظام برمجية:

```
Switch(config)#spanning-tree etherchannel guard misconfig
```

خيارات أخرى

عند توجيه جهازين لا يدعمان PAgP ولكنهما يدعمان LACP، تكون التوصية تمكين LACP باستخدام تكوين LACP النشط على كلا طرفي الأجهزة. راجع قسم بروتوكول التحكم في تجميع الارتباطات (LACP) في هذا المستند للحصول على مزيد من المعلومات.

عند التحويل إلى أجهزة لا تدعم PAgP أو LACP، يجب عليك ترميز القناة إلى ترميز ثابت. ينطبق هذا المتطلب على هذه الأجهزة على سبيل المثال:

- الخوادم
- مدير محلي
- مبدلات المحتوى
- الموجهات
- المحولات ذات البرامج السابقة
- مادة حفازة 2900xl/3500xl مفتاح
- مادة حفازة 8540s

أصدر الأوامر التالية:

```
#Switch(config)#interface type slot#/port
Switch(config-if)#channel-group number mode on
```

بروتوكول التحكم في تجميع الارتباطات (LACP)

LACP هو بروتوكول يسمح للمنافذ ذات الخصائص المماثلة بتكوين قناة من خلال التفاوض الديناميكي باستخدام المحولات المجاورة. PAgP هو بروتوكول خاص من Cisco يمكنك تشغيله فقط على محولات Cisco والمحولات التي يطلقها الموردون المرخصون. ولكن LACP، والذي تم تعريفه في IEEE 802.3ad، يسمح لمحولات Cisco بإدارة قناة الإيثرنت باستخدام أجهزة تطابق مواصفات 802.3ad.

يتم دعم بروتوكول التحكم في تجميع الارتباطات (LACP) مع هذه الأنظمة الأساسية والإصدارات:

- مادة حفازة 6000/6500 sery مع cisco ios برمجية إطلاق 12.1(ex(11b وفيما بعد
- مادة حفازة 4500 sery مع cisco ios برمجية إطلاق 12.1(13)ew وفيما بعد
- مادة حفازة 3750 sery مع cisco ios برمجية إطلاق 12.1(14)EA1 وفيما بعد

ولا يوجد فرق يذكر بين بروتوكول التحكم في تجميع الارتباطات (LACP) وبروتوكول الوصول إلى نقطة الخدمة (PAgP) من منظور وظيفي. يدعم كلا البروتوكولين ثمانية منافذ كحد أقصى في كل قناة، ويتم التحقق من نفس خصائص المنفذ قبل تكوين الحزمة. تتضمن خصائص المنفذ هذه:

- السرعة
- الإرسال ثنائي الاتجاه
- شبكة VLAN الأصلية ونوع التوصيل

والاختلافات الملحوظة بين بروتوكول التحكم في تجميع الارتباطات (LACP) وبروتوكول الوصول إلى الخدمات (PAgP) هي:

- يمكن تشغيل بروتوكول LACP فقط على منافذ الإرسال ثنائي الإتجاه الكامل ولا يدعم منافذ الإرسال أحادي الإتجاه.
- يدعم بروتوكول LACP منافذ الاستعداد السريع. يحاول بروتوكول LACP دائما تكوين الحد الأقصى لعدد المنافذ المتوافقة في قناة ما، حتى الحد الأقصى الذي يسمح به الجهاز (ثمانية منافذ). إذا لم يكن بروتوكول التحكم في الوصول للبنية الأساسية (LACP) قادرا على تجميع جميع المنافذ المتوافقة (على سبيل المثال، إذا كان النظام البعيد به قيود أجهزة أكثر تقييدا)، يتم وضع جميع المنافذ التي لا يمكن تضمينها بشكل نشط في القناة في حالة الاستعداد السريع ويتم إستخدامها فقط إذا فشل أحد المنافذ المستخدمة.

ملاحظة: بالنسبة للمحولات من السلسلة Catalyst 4500، يكون الحد الأقصى لعدد المنافذ التي يمكنك تعيين نفس المفتاح الإداري لها هو ثمانية. ل مادة حفازة 6500 و 3750 مفتاح أن يركض cisco ios برمجية، LACP يحاول أن يشكل العدد الأقصى من ميناء متوافق في EtherChannel، حتى الأقصى أن الجهاز يسمح (ثمانية ميناء). يمكن تكوين ثمانية منافذ إضافية كمنافذ إحتياطية فعالة.

نظرة عامة على العمليات

يتحكم بروتوكول LACP في كل منفذ مادي (أو منطقي) فردي يتم تجميعه. يتم إرسال حزم LACP باستخدام عنوان MAC لمجموعة البث المتعدد **01-80-c2-00-00-02**. قيمة النوع/الحقل هي 0x8809 مع نوع فرعي 0x01. هذا ملخص لعملية البروتوكول:

- يعتمد البروتوكول على الأجهزة للإعلان عن إمكانيات التجميع الخاصة بها ومعلومات الحالة. وترسل عمليات الإرسال على أساس منتظم ودوري على أساس كل رابط قابل للتجميع.
- ما دام المنفذ الفعلي قيد التشغيل، يتم إرسال حزم LACP كل ثانية أثناء الكشف وكل 30 ثانية في حالة ثابتة.
- يستمع الشركاء الموجودون على رابط قابل للتجميع إلى المعلومات التي يتم إرسالها داخل البروتوكول ويقررون أي إجراء أو إجراءات يجب إتخاذها.
- يتم تكوين المنافذ المتوافقة في قناة ما، حتى الحد الأقصى الذي يسمح به الجهاز (ثمانية منافذ).
- ويتم الحفاظ على التجميعات من خلال التبادل المنتظم وفي الوقت المناسب لمعلومات حديثة عن الحالة بين شركاء الارتباط. إذا تغير التكوين (بسبب فشل إرتباط، على سبيل المثال)، ينتهي وقت شركاء البروتوكول ويتخذون الإجراء المناسب استنادا إلى الحالة الجديدة للنظام.
- وبالإضافة إلى عمليات الإرسال الدورية لوحدة بيانات بروتوكول التحكم في الوصول إلى شبكة LACP (LACPDU)، إذا حدث تغيير في معلومات الحالة، يقوم البروتوكول بإحالة وحدة بيانات بروتوكول التحكم في الوصول إلى المنفذ (LACPDU) الموجهة حسب الحدث إلى الشركاء. يتخذ الشركاء في البروتوكول الإجراء المناسب استنادا إلى الحالة الجديدة للنظام.

معلمات LACP

للسماح ب LACP لتحديد ما إذا كانت مجموعة من الارتباطات متصلة بنفس النظام وإذا كانت تلك الارتباطات متوافقة من وجهة نظر التجميع، فمن الضروري أن تكون قادرا على إنشاء:

- معرف فريد عمومي لكل نظام يشارك في تجميع الارتباطات.يجب تعيين أولوية لكل نظام يقوم بتشغيل بروتوكول التحكم في الوصول للبنية الأساسية (LACP) يمكن إختيارها إما تلقائيا (بالأولوية الافتراضية التي تبلغ 32768) أو بواسطة المسؤول. يتم إستخدام أولوية النظام بشكل رئيسي بالاقتران مع عنوان MAC الخاص بالنظام لتكوين معرف النظام.
- وسيلة لتحديد مجموعة القدرات المرتبطة بكل منفذ ومع كل مجمع، كما يفهمها نظام معين.يجب أن يتم تعيين أولوية لكل منفذ في النظام إما بشكل تلقائي (مع الأولوية الافتراضية وهي 128) أو بواسطة المسؤول. يتم إستخدام الأولوية بالاقتران مع رقم المنفذ لتكوين معرف المنفذ.
- وسيلة لتحديد مجموعة تجميع روابط والمجمع المرتبط بها.يتم تلخيص قدرة المنفذ على التجميع مع منفذ آخر بواسطة معلمة عدد صحيح بسيطة 16 بت أكبر تماما من الصفر الذي يسمى المفتاح. يتم تحديد كل مفتاح على أساس عوامل مختلفة، مثل:الخصائص المادية للمنفذ، والتي تتضمن معدل البيانات، والازدواج، والنقطة إلى نقطة أو الوسيط المشتركقيود التكوين التي يتم إنشاؤها بواسطة مسؤول الشبكةيرتبط مفتاحان بكل منفذ:مفتاح إداريمفتاح عملياتييسمح المفتاح الإداري بتلاعب الإدارة بالقيم الأساسية، وبالتالي، يمكن للمستخدم إختيار هذا المفتاح. يستخدم النظام المفتاح التشغيلي لتكوين التجميعات. يتعذر على المستخدم إختيار هذا المفتاح أو تغييره مباشرة. يقال إن مجموعة المنافذ الموجودة في نظام معين والتي تشترك في نفس قيمة مفتاح التشغيل هي أعضاء في نفس مجموعة المفاتيح.

لذلك، بافتراض نظامين ومجموعة من المنافذ التي تحمل المفتاح الإداري نفسه، يحاول كل نظام تجميع المنافذ بدءا من المنفذ الذي يحظى بالأولوية العليا في النظام ذي الأولوية العليا. هذا السلوك ممكن لأن كل نظام يعرف هذه الأولويات:

- الأولوية الخاصة به، والتي قام المستخدم أو البرنامج بتعيينها
- أولوية شريكه، والتي تم اكتشافها من خلال حزم LACP

سلوك فاشل

سلوك الفشل ل LACP هو نفسه سلوك الفشل ل PAgP. إذا فشل إرتباط في قناة موجودة (على سبيل المثال، إذا تم إلغاء توصيل منفذ، أو تمت إزالة GBIC، أو تم قطع قناة ليفية)، يتم تحديث المنفذ ويتم تجزئة حركة مرور البيانات عبر الارتباطات المتبقية خلال ثانية واحدة. لا تعاني أي حركة مرور لا تتطلب إعادة التجزئة بعد الفشل (وهو حركة المرور التي تستمر في الإرسال على نفس الارتباط) من أي خسارة. تؤدي إستعادة الارتباط الفاشل إلى تشغيل تحديث آخر إلى المنفذ، ويتم تجزئة حركة مرور البيانات مرة أخرى.

خيارات التكوين

أنت يستطيع شكلت LACP EtherChannels في أسلوب مختلف، بما أن هذا طاولة يلخص:

نمط	الخيارات القابلة للتكوين
تشغيل	يتم فرض تكوين تجميع الارتباطات دون أي تفاوض على بروتوك

	ول التحكم في الوصول إلى شبكة LACP. لا يرسل المحول حزمة LACP ولا يعالج أي حزمة LACP واردة. إن يكون المجاور ميناء أسلوب نشط، قناة شكلت.
إيقاف (أو) غير مكون	لا يقني الميناء، regardless of the مجاور يكون شكلت.
خامل (افتراضي)	هذا مماثل إلى **الوضع** تلقائي في PAgP. لا يقوم المحول ببدء القناة،

	ولكنه يفهم حزم LACP الواردة. يقوم النظير (في الحالة النشطة) بتهيئة التفاوض (عن طريق إرسال حزمة LACP) التي يتلقاها المحول والتي يستجيب إليها المحول، مما يؤدي في نهاية المطاف إلى تكوين قناة التجميع مع النظير.
نشط	وهذا مماثل للوضع **المرغوب** فيه في PAgP. يقوم المحول ببدء التفاوض

	لتكوين إرتباط تجميع. يتم تكوين تجميع الارتباطات إذا كان الطرف الآخر يعمل في وضع LACP النشط أو السلبي.

يستخدم LACP مؤقت الفاصل الزمني بزمن 30 ثانية (slow_periodic_time) بعد إنشاء قنوات EtherChannels الخاصة ب LACP. يبلغ عدد الثواني التي تسبق إبطال معلومات LACPDU المستلمة عند إستخدام فترات انتهاء المهلة الطويلة (3 مرات 90 (Slow_Periodic_Time. يوصى ب UDLD ككاشف أكثر سرعة للروابط أحادي الإتجاه. لا يمكنك ضبط وحدات توقيت LACP، وعند هذه النقطة، لا يمكنك تكوين المحولات لاستخدام إرسال وحدة بيانات البروتوكول السريع (PDU) (في كل ثانية) للحفاظ على القناة بعد تكوين القناة.

التحقق

يوفر الجدول الموجود في هذا القسم ملخصا لجميع سيناريوهات وضع توجيه LACP المحتمل بين محولين متصلين مباشرة (المحول A والمحول B). بعض من هذا خليط يستطيع سببت EtherChannel حارس أن يضع الميناء على ال يقني جانب داخل الدولة EtherChannel misconfiguration .errdisable حارس مكنت سمة افتراضيا.

تبديل وضع القناة	وضع قناة المحول B	تبديل حالة القناة	حالة قناة المحول B
تشغيل	تشغيل	قناة (غير LACP)	قناة (غير LACP)
تشغيل	إيقاف	ليس قناة (errDisable)	ليس قناة
تشغيل	سلبي	ليس قناة (errDisable)	ليس قناة
تشغيل	نشط	ليس قناة (errDisable)	ليس قناة
إيقاف	إيقاف	ليس قناة	ليس قناة
إيقاف	سلبي	ليس قناة	ليس قناة
إيقاف	نشط	ليس قناة	ليس قناة
سلبي	سلبي	ليس قناة	ليس قناة
سلبي	نشط	قناة LACP	قناة LACP

نشط	نشط	قناة LACP	قناة LACP

توصيات Cisco

cisco يوصي أن يمكن أنت PAgP على قناة توصيل بين cisco مفتاح. عند توجيه جهازين لا يدعمان PAgP ولكنهما يدعمان LACP، تكون التوصية تمكين LACP باستخدام تكوين LACP النشط على كلا طرفي الأجهزة.

على مفتاح أن يركض CatOS، كل ميناء على مادة حفازة 4000/4500 ومادة حفازة 6000/6500 يستعمل PAgP قناة بروتوكول افتراضيا. in order to شكلت ميناء أن يستعمل LACP، أنت ينبغي ثبتت القناة بروتوكول على الوحدات نمطية إلى LACP. لا يمكن تشغيل LACP و PAgP على نفس الوحدة النمطية على المحولات التي تعمل بنظام التشغيل CatOS. لا ينطبق هذا القيد على المحولات التي تعمل ببرنامج Cisco IOS Software. يمكن للمحولات التي تعمل ببرنامج Cisco IOS Software دعم PAgP و LACP على الوحدة النمطية نفسها. أصدرت هذا أمر in order to ثبتت ال lacp قناة أسلوب إلى نشط وأن يعين إداري مفتاح رقم:

```
#Switch(config)#interface range type slot#/port
Switch(config-if)#channel-group admin_key mode active
```

يعرض الأمر **show etherChannel summary** خلاصة سطر واحد لكل مجموعة قناة تتضمن هذه المعلومات:

- أرقام المجموعة
- أرقام قنوات المنافذ
- حالة المنافذ
- الميناء أن يكون جزء من القناة

يعرض الأمر **show etherChannel port-channel** معلومات قناة المنفذ التفصيلية لجميع مجموعات القنوات. يتضمن الإخراج هذه المعلومات:

- حالة القناة
- البروتوكول المستخدم
- الوقت منذ تجميع المرافئ

لعرض المعلومات التفصيلية لمجموعة قنوات معينة، مع تفاصيل كل منفذ موضح بشكل منفصل، أستخدم الأمر **show etherChannel** *channel_number* detail. تتضمن مخرجات الأمر تفاصيل الشريك وتفاصيل قناة المنفذ. أحلت بشكل LACP (802.3ad) بين مادة حفازة 6000/6500 ومادة حفازة 4000/4500 ل كثير معلومة.

خيارات أخرى

مع أجهزة القناة التي لا تدعم PAgP أو LACP، يجب عليك ترميز القناة إلى برمجية. ينطبق هذا المتطلب على هذه الأجهزة:

- الخوادم
- مدير محلي
- مبدلات المحتوى
- الموجهات
- المحولات ذات البرامج القديمة
- مادة حفازة 2900xl/3500xl مفتاح
- مادة حفازة 8540s

أصدر الأوامر التالية:

```
#Switch(config)#interface range type slot#/port
Switch(config-if)#channel-group admin_key mode on
```

اكتشاف الروابط أحادي الإتجاه

الغرض

UDLD هو بروتوكول Cisco خاص وخفيف الوزن الذي تم تطويره لاكتشاف مثيلات الاتصالات أحادي الإتجاه بين الأجهزة. هناك طرق أخرى للكشف عن حالة الإرسال ثنائية الإتجاه، مثل FEFI. ولكن، هناك حالات تكون فيها آليات اكتشاف الطبقة الأولى غير كافية. يمكن أن ينتج عن هذه السيناريوهات:

- التشغيل غير المتوقع ل STP
- فيض الحزم غير الصحيح أو المفرط
- التعتيم الأسود لحركة المرور

ال UDLD يخاطب سمة هذا خطأ حالة على ليف ونحاس إثرنيت قارن:

- يراقب فعلية كبل تشكيل — يعطل أي ميناء سلكي.
- يحمي ضد خطوة أحادي إتجاه- في الكشف عن خطوة أحادي إتجاه أن يقع بسبب وسائط أو ميناء/قارن يعطل، ال يتأثر ميناء عطلت بما أن `erdisabled`. يتم إنشاء رسالة syslog المقابلة.
- علاوة على ذلك، يتحقق وضع UDLD العدواني من أن الرابط ثنائي الإتجاه الذي سبق اعتباره لا يفقد الاتصال في حالة أن الرابط يصبح غير قابل للاستخدام بسبب الازدحام. UDLD يقوم أسلوب فعال إختبار اتصال مستمر عبر الرابط. الغرض الأساسي من UDLD عدواني أسلوب أن يتحاشى الأسود يقيد حركة مرور في بعض حالات فشل أن لا يعالج ب عادي أسلوب UDLD.

راجع فهم ميزة بروتوكول اكتشاف الارتباط أحادي الإتجاه (UDLD) وتكوينها للحصول على مزيد من التفاصيل.

تحتوي الشجرة المتفرعة على تدفق BPDU أحادي الإتجاه ثابت ويمكن أن تحتوي على الإخفاقات التي يسردها هذا القسم. يمكن أن يفشل ميناء فجأة أن يبث BPDUs، أي يسبب تغير حالة STP من إلى على المجاور. بعد، أنشوطة بعد تواجدت لأن الميناء بعد يستطيع أن يستلم.

نظرة عامة على العمليات

UDLD هو بروتوكول من الطبقة 2 يعمل فوق طبقة LLC (غاية snap HDLC، 01-00-0c-cc-cc MAC بروتوكول نوع 0x0111). عندما تقوم بتشغيل UDLD مع FEFI وآليات التفاوض التلقائي من الطبقة 1، يمكنك التحقق من التكامل المادي (L1) والمنطقي (L2) للارتباط.

UDLD به أحكام للميزات والحماية أن FEFI و autonegotiation يستطيع لا ينجز. وتتضمن هذه الميزات ما يلي:

- اكتشاف معلومات الجوار وذاكرة التخزين المؤقت لها
- إيقاف عمل أي ميناء غير متصل
- اكتشاف أعطال الواجهة/المنافذ المنطقية أو الأعطال على الارتباطات التي لا تكون من نقطة إلى نقطة**ملاحظة:** عندما لا تكون الروابط من نقطة إلى نقطة، فإنها تجتاز محولات الوسائط أو المحاور.

وتستخدم الرابطة هاتين الآليتين الأساسيتين.

1. UDLD يعلم عن الجيران ويحفظ المعلومات محدثة في ذاكرة تخزين مؤقت محلي.
2. UDLD يرسل قطار من UDLD مستكشفات/صدى (مرحبا) رسالة عند الكشف عن جار جديد أو كلما طلب جار إعادة تزامن من التخزين المؤقت.

UDLD يرسل تدقيق/صدى رسالة على كل ميناء. في إستقبال ال يماثل UDLD رسالة على ميناء، كشف مرحلة والتحقق عملية أطلقت. يتم تمكين المنفذ في حالة استيفاء جميع الشروط الصالحة. يتم استيفاء الشروط إذا كان المنفذ ثنائي الإتجاه وتم توصيله بشكل صحيح. إن لا يتوفر الشرط، الميناء `errDisabled`، أي يشغل هذا syslog رسالة:

```
.UDLD-3-AGGRDISABLE: Neighbor(s) of port disappeared on bidirectional link
                                                                Port disabled
.UDLD-3-AGGRDISABLEFAIL: Neighbor(s) of port disappeared on bidirectional link
                                                        Failed to disable port
                                .UDLD-3-DISABLE: Unidirectional link detected on port disabled
.UDLD-3-DISABLEFAIL: Unidirectional link detected on port, failed to disable port
                                                .UDLD-3-SENDFAIL: Transmit failure on port
[UDLD-4-ONEWAYPATH: A unidirectional link from port to port of device [chars
                                                                .was detected
```

للحصول على قائمة كاملة من رسائل النظام حسب المرفق، والتي تتضمن أحداث UDLD، راجع رسائل UDLD (رسائل نظام Cisco IOS، المجلد 2 من 2).

بعد إنشاء خطوة وتصنيفه ك ثنائي إتجاه، UDLD يستمر أن يعلن تدقيق/صدى رسالة في تقصير فاصل من 15 ثانية.

يوفر هذا الجدول معلومات عن دول المنفذ:

دولة الميناء	تعليق
غير محدد	كشف قيد التقدم/مجاور UDLD أعجزت.
غير قابل للتطبيق	UDLD يتلقى يكون معأق.
الإغلاق	كشفت خطوة أحادي إتجاه والميناء يكون أعجزت.
ثنائي الإتجاه	تم اكتشاف إرتباط ثنائي الإتجاه.

صيانة ذاكرة التخزين المؤقت المجاورة

UDLD يرسل دوريا مرحبا تحقيق/صدى ربط على كل قارن نشط in order to حافظت على التكامل من ال UDLD مجاور ذاكرة تخزين مؤقت. عند إستلام رسالة ترحيب، يتم تخزين الرسالة مؤقتا ويتم حفظها في الذاكرة لمدة أقصاها، والتي يتم تعريفها بوقت الانتظار. عند انتهاء صلاحية وقت الاحتجاز، يكون إدخال ذاكرة التخزين المؤقت الخاص به قديما. إذا تم تلقي رسالة ترحيب جديدة خلال فترة الانتظار، فإن الرسالة الجديدة تستبدل الإدخال الأقدم ويتم إعادة تعيين وحدة توقيت فترة البقاء المقابلة.

عندما يكون UDLD يمكن قارن معأق أو كلما تمت إعادة ضبط جهاز، فإن كل إدخالات التخزين المؤقت الموجودة للواجهات التي يؤثر عليها تغيير التكوين يتم مسحها. تحافظ هذه الخلوص على سلامة ذاكرة تخزين UDLD المؤقتة. يرسل UDLD على الأقل رسالة واحد أن يبلغ الجيران شخصي بالحاجة إلى مسح ال يماثل ذاكرة تخزين مؤقت مدخل.

آلية كشف الارتداد

تشكل آلية الصدى أساس خوارزمية الكشف. عندما يعلم جهاز UDLD عن جار جديد أو يستلم طلب إعادة مزامنة من جار خارج المزامنة، يقوم الجهاز بتشغيل نافذة الكشف أو إعادة تشغيلها على جانبه من الاتصال ويرسل دفعة من رسائل الصدى في الرد. ولأن هذا السلوك لابد أن يكون متماثلا في كل الجيران، فإن مرسل صدى الصوت يتوقع أن يتلقى أصداء في الرد. إذا انتهت نافذة الكشف دون إستلام أي رسائل رد صحيحة، يعتبر الارتباط أحادي الإتجاه. من هذه النقطة، خطوة إعادة إنشاء أو ميناء إيقاف عمل عملية يستطيع كنت أطلقت. حالات شاذة أخرى نادرة يتحقق الجهاز منها:

- ألياف إرسال خلفية مجدولة (Tx) إلى موصل Rx الخاص بنفس المنفذ
- التمويلات في حالة اتصال الوسائط المشتركة البيني (على سبيل المثال، صرة أو جهاز مماثل)

وقت التقارب

in order to منعت أنشوطة STP، cisco ios برمجية إطلاق 12.1 وفيما بعد خفضت ال UDLD تقصير رسالة فاصل من 60 ثاني إلى 15 ثاني. غيرت هذا فاصل زمني in order to عطلت إرتباط أحادي إتجاه قبل أن يكون ميناء سابق محظور في 802.1D يجسر - شجرة يستطيع أن ينتقل إلى حالة إعادة توجيه. تحدد قيمة الفاصل الزمني للرسالة المعدل الذي يرسل عنده الجار إختبارات UDLD بعد مرحلة الربط أو الكشف. لا يلزم تطابق فاصل الرسالة على كلا طرفي إرتباط، رغم أن التكوين المتناسق مرغوب فيه حيثما كان ذلك ممكنا. عندما UDLD خلقت مجاور، ال يشكل رسالة فاصل أرسلت إلى المجاور، وال تعطيل فاصل ل أن نظير حسبت ك:

```
(message interval) * 3
```

وهكذا، تفتقد علاقة النظير إلى ما بعد ثلاثة إختبارات متتالية (أو مسابر). ولأن الفواصل الزمنية للرسالة مختلفة على كل جانب، فإن قيمة المهلة هذه تختلف ببساطة على كل جانب، ويتعرف جانب على الفشل بشكل أسرع.

الوقت التقريبي الضروري ل UDLD أن يكشف فشل أحادي الإتجاه من خطوة كانت مستقرة سابقا هو تقريبا:

```
message interval) + 4 seconds) * 2.5
```

هذا تقريبا 41 ثاني مع التقصير رسالة فاصل من 15 ثاني. وهذا المقدار من الوقت أقل بكثير من 50 ثانية اللازمة عادة لإعادة تقارب بروتوكول الشجرة المتفرعة (STP). إذا كانت وحدة المعالجة المركزية لبروتوكول NMP تحتوي على بعض الدورات الاحتياطية وإذا كان المستخدم يراقب مستوى إستخدامها بعناية (ممارسة جيدة)، فإن تقليل الفاصل الزمني للرسالة (حتى) إلى الحد الأدنى وهو 7 ثوان يعد أمرا مقبولا. كما يساعد تقليل الفاصل الزمني بين الرسائل على زيادة سرعة اكتشاف المشكلة بواسطة عامل هام.

ملاحظة: الحد الأدنى هو ثانية واحدة في برنامج Cisco IOS الإصدار 12.2(25)SEC.

لذلك، UDLD يفترض تبعية على التقصير يجسر - شجرة وقت. إن يكون STP ضبطت أن يتلاقى بسرعة أكبر من UDLD، فكر آلية بديلة، مثل ال STP أنشوطة حارس سمة. ضع آلية بديلة في هذه الحالة عند تنفيذ بروتوكول RSTP (802.1w))، أيضا، لأن بروتوكول الشجرة المتفرعة (RSTP) يتميز بخصائص تقارب في مللي ثانية، حسب المخطط. ل هذا مثال، استعملت أنشوطة حارس بالاقتران مع UDLD in order to زودت الأكثر حماية. يمنع حماية التكرار الحلقي حلقات تكرار بروتوكول الشجرة المتفرعة (STP) مع سرعة إصدار STP قيد الاستخدام. و UDLD يأخذ بعين الاعتبار الكشف عن الاتصالات أحادي الإتجاه على فرادى EtherChannel خطوة أو في الحالات التي BPDUs لا يتدفق على طول الإتجاه المكسور.

ملاحظة: UDLD مستقل عن STP. UDLD لا يمسك كل حالة فشل STP، مثل تلك الفشل أن يكون بسبب CPU أن لا يرسل BPDUs لوقت أن يكون أكبر من (2 * max + Fwddelay). لهذا السبب، توصي Cisco بتنفيذ UDLD بالاقتران مع حماية التكرار الحلقي في المخططات التي تعتمد على بروتوكول الشجرة المتفرعة (STP).

تحذير: احترس من إطلاق مبكر UDLD في ال 2900xl/3500xl مفتاح أن يستعمل غير تشكيل، 60 ثاني تقصير رسالة فاصل. وهي عرضة لظروف تكرار حلقي لشجرة الامتداد.

وضع UDLD العدائي

تم إنشاء UDLD العدواني من أجل معالجة تلك الحالات القليلة تحديدا التي يكون فيها إختبار مستمر للاتصال ثنائي الإتجاه ضروريا. على هذا النحو، توفر ميزة الوضع العدواني حماية محسنة ضد شروط الارتباط أحادي الإتجاه الخطيرة في هذه المواقف:

- عندما يكون فقد UDLD PDUs متماثل وكلا ينتهي وقت. في هذه الحالة، لا ميناء errdisabled.
- يتلقى جانب واحد من خطوة ميناء ب التصق (على حد سواء Tx و Rx).
- يبقى جانب واحد من الرابط مرتفع بينما الجانب الآخر من الرابط انخفض.
- تم تعطيل التفاوض التلقائي، أو آلية أخرى لاكتشاف الأعطال من الطبقة 1.
- ومن المستصوب الحد من الاعتماد على آليات المستوى 1 من نظام معلومات المؤسسات المالية الدولية.

- تحتاج إلى أقصى حماية ضد حالات فشل الارتباط أحادي الإتجاه على إرتباطات FE/GE من نقطة إلى نقطة.
وعلى وجه التحديد، عندما لا يكون الفشل مقبولا بين جارتين، يمكن إعتبار التحقيقات العدوانية في UDLD نبضات القلب، التي يضمن وجودها صحة الرابط.

الحالة الأكثر شيوعا لتنفيذ UDLD عدواني أن ينجز الموصولية تدقيق على عضو من حزمة عندما autonegotiation أو آخر طبقة 1 خطأ آلية معأق أو غير usable. وهو مفيد بشكل خاص مع إتصالات EtherChannel لأن PAgP و LACP، حتى إذا تم تمكينهما، لا يستخدمان توقيتات ترحيب منخفضة جدا في حالة مستقرة. في هذه الحالة، UDLD يتلقى سمة إضافية أن يمنع يمكن يجسر - شجرة أنشوطة.

من المهم أن تفهم أن UDLD عادي يفحص وضع خطوة أحادي إتجاه، even after خطوة يبلغ وضع ثنائي إتجاه. UDLD يعني أن يكشف طبقة 2 مشكلة أن يسبب أنشوطة STP، وتلك مشكلة عادة أحادي إتجاه (لأن BPDUs يتدفق فقط في إتجاه واحد في حالة مستقرة). لذلك، غالبا ما يكون إستخدام UDLD عادي بالاقتران مع autonegotiation وواقي التكرار (للشبكات التي تعتمد على بروتوكول الشجرة المتفرعة (STP) كافيا. مع تمكين وضع UDLD العدواني، بعد أن تكون جميع جيران المنفذ قد انتهت أعمارهم، إما في الإعلان أو في مرحلة الكشف، يعيد وضع UDLD العدواني تشغيل تسلسل الارتباط في محاولة لإعادة التزامن مع أي جيران من المحتمل أن يكونوا خارج المزامنة. إن بعد قطار سريع من رسالة (ثمانية إعادة محاولة فاشلة) الربط بعد اعتبرت غير محدد، الميناء وضعت داخل الدولة errdisable.

ملاحظة: بعض المحولات لا تدعم UDLD بقوة. حاليا، المادة حفازة 2900xl ومادة حفازة 3500xl يتلقى صلب ترميز رسالة فاصل من 60 ثاني. ولا يعتبر هذا الأمر سريعا بما فيه الكفاية للحماية من حلقات تكرار بروتوكول الشجرة المتفرعة (STP) المحتملة (مع افتراض معلمات STP الافتراضية).

الاسترداد التلقائي لارتباطات UDLD

Errdisable أعجزت إستعادة بشكل عام افتراضيا. عقب مكنت هو بشكل عام، إن يذهب ميناء داخل ال errdisable دولة، هو reenabled تلقائيا بعد زمنية محددة فاصل. التقصير وقت 300 ثاني، أي يكون عمومي مؤقت ويحفظ لكل ميناء في مفتاح. حسب البرمجية إطلاق، أنت يستطيع يدويا منعت reenable ميناء إن أنت ثبتت ال errdisable تعطيل ل أن ميناء أن يعجز مع إستعمال من ال errdisable تعطيل آلية إستعادة ل UDLD:

```
Switch(config)#errdisable recovery cause udld
```

ضع في الاعتبار إستخدام ميزة تعطيل errdisable عندما تقوم بتنفيذ وضع UDLD العدائي مع عدم وجود قدرات إدارة شبكة خارج النطاق، وخاصة في طبقة الوصول أو على أي جهاز يمكن أن يصبح معزولا من الشبكة في حالة حالة وضع errdisable.

أحلت إستعادة errdisable (مادة حفازة 6500 sery cisco ios أمر مرجع، E 12.1) ل كثير معلومة على كيف أن يشكل مهلة فترة لميناء في الدولة errdisable.

Errdisable إستعادة يستطيع كنت مهم خاصة ل UDLD في الوصول طبقة عندما المنفذ وزعت مفتاح عبر حرم جامعي بيئة وال زيارة يدوي من كل مفتاح in order to reenable كلا الوصلات يأخذ وقت كبير.

لا توصي Cisco باستعادة errdisable في مركز الشبكة لأن هناك عادة نقاط إدخال متعددة في لب، والاستعادة آلي في لب يستطيع أدت إلى مشاكل متكررة. لذلك، أنت ينبغي يدويا reenable ميناء في لب إن UDLD يعجز الميناء.

UDLD على الروابط الموجهة

لأغراض هذه المناقشة، يكون الارتباط الموجه أحد نوعي الاتصال هذين:

- نقطة إلى نقطة بين عقدتي موجه (يتم تكوينها بقناع شبكة فرعية من 30 بت)
- شبكة VLAN ذات منافذ متعددة ولكنها تدعم الاتصالات الموجهة فقط، مثل في طبولوجيا أساسية للطبقة 2 المقسمة

لكل بروتوكول توجيه العبارة الداخلية (IGRP) خصائص فريدة فيما يتعلق بكيفية معالجته لعلاقات الجوار وتقارب

المسار. يصف هذا القسم الخصائص ذات الصلة بهذه المناقشة، والتي تتعارض مع إثنين من بروتوكولات التوجيه الأكثر شيوعا التي يتم إستخدامها اليوم، وبروتوكول فتح أقصر مسار أولا (OSPF) وبروتوكول IGRP المحسن (EIGRP).

ملاحظة: ينتج عن فشل الطبقة 1 أو الطبقة 2 في أي شبكة موجهة من نقطة إلى نقطة التمهيد المباشر تقريبا لاتصال الطبقة 3. لأن المنفذ الوحيد للمحول في تلك الانتقالات إلى حالة غير متصلة على فشل الطبقة 1/الطبقة 2، فإن ميزة الواجهة auto-state تقوم بمزامنة حالات منافذ الطبقة 2 والطبقة 3 في نحو ثانيتين وتضع واجهة شبكة VLAN للطبقة 3 في حالة up/down (بروتوكول الخط قيد الإيقاف).

إذا افترضت قيمة المؤقت الافتراضية، يرسل OSPF رسائل ترحيب كل 10 ثاني وبه فاصل زمني موات مقداره 40 ثانية (4 * مرحبا). تكون وحدات التوقيت هذه متوافقة مع شبكات البث من نقطة إلى نقطة الخاصة ب OSPF. ولأن بروتوكول فتح أقصر مسار أولا (OSPF) يتطلب الاتصال ثنائي الإتجاه لتشكيل عملية تجاور، فإن زمن تجاوز الفشل الأسوأ هو 40 ثانية. وهذا صحيح حتى إذا كان فشل الطبقة 1/الطبقة 2 غير نقي على اتصال من نقطة إلى نقطة ويترك سيناريو نصف منبثق يجب أن يتعامل معه بروتوكول الطبقة 3. لأن الكشف وقت UDLD مماثل جدا إلى الكشف وقت من OSPF ميت وقت ينتهي (تقريبا 40 ثاني)، فإن مميزات التشكيل من UDLD أسلوب عادي على OSPF طبقة 3 نقطة إلى نقطة خطوة محدود.

وفي العديد من الحالات، يتلاقى EIGRP بسرعة أكبر من OSPF. ولكن من المهم ملاحظة أن الاتصال في الاتجاهين ليس شرطا لكي يتبادل الجيران معلومات التوجيه. في سيناريوهات الفشل نصف المكسوة بالخبز بشكل محدد للغاية، يكون EIGRP عرضة للاختراق الأسود لحركة المرور التي تستمر حتى يقوم حدث آخر باستجلاب المسارات من خلال الجوار كنشاط. UDLD عادي أسلوب يستطيع خففت هذا ظرف لأن هو يكشف ال unidirectional خطوة إخفاق وخطأ يعجز الميناء.

بالنسبة للاتصالات الموجهة من الطبقة 3 التي تستخدم أي بروتوكول توجيه، فإن UDLD normal لا يزال يوفر الحماية ضد المشاكل الموجودة عند تنشيط الارتباط الأولي، مثل الكبلات الفاشلة أو الأجهزة المعيبة. وبالإضافة إلى ذلك، يوفر وضع UDLD المكثف هذه المزايا على الاتصالات الموجهة من الطبقة 3:

- يمنع التعتيم الأسود غير الضروري لحركة المرور (مع حد أدنى للتوقيت مطلوب في بعض الحالات)
- يضع خطوة خطوة خطوة داخل الدولة errdisable
- يحمي ضد أنشوطة أن ينتج من طبقة EtherChannel 3 تشكيل

السلوك الافتراضي ل UDLD

UDLD معأق بشكل عام ومكنت في إستعداد على ليف ميناء افتراضيا. لأن UDLD يكون بنية بروتوكول أن يكون احتجت بين مفتاح فقط، UDLD معأق افتراضيا على ميناء نحاسي، أي يميل أن يكون استعملت للمضيف منفذ. لاحظ أن أنت ينبغي مكنت UDLD بشكل عام وعلى القارن مستوى قبل أن يستطيع الجيران حققت وضع ثنائي إتجاه. الفاصل الزمني للرسالة الافتراضية هو 15 ثانية. ولكن، يمكن أن يظهر الفاصل الزمني للرسالة الافتراضية على هيئة سبع ثوان في بعض الحالات. راجع معرف تصحيح الأخطاء من CSCea70679 Cisco (العملاء المسجلون فقط) للحصول على مزيد من المعلومات. التقصير رسالة فاصل يمكن شكلت بين سبعة و 90 ثاني، UDLD عدواني أسلوب معأق. يعمل برنامج IOS الإصدار SEC(25)12.2 من Cisco على تقليل هذا المؤقت الأدنى إلى ثانية واحدة.

توصية تكوين Cisco

في الغالبية العظمى من الحالات، cisco يوصي أن أنت يمكن UDLD أسلوب عادي على كل نقطة إلى نقطة FE/GE خطوة بين cisco مفتاح، وعينت ال UDLD رسالة فاصل إلى 15 ثاني عندما أنت تستعمل تقصير 802.1D يجسر - شجرة وقت. وبالإضافة إلى ذلك، حيث تعتمد الشبكات على بروتوكول الشجرة المتفرعة (STP) للتكرار والتقارب (مما يعني أن هناك منفذا واحدا أو أكثر في حالة حظر بروتوكول الشجرة المتفرعة (STP) في المخطط)، أستخدم UDLD بالاقتران مع الميزات والبروتوكولات المناسبة. وتتضمن هذه الميزات FEFI، والتشغيل التلقائي، وواقي التكرار، وما إلى ذلك. في العادة، إذا تم تمكين التفاوض التلقائي، فإن الوضع العدواني ليس ضروريا لأن التفاوض التلقائي يعوض عن اكتشاف الأعطال في الطبقة 1.

أصدرت واحد من هذا إثنان أمر خيار in order to مكنت UDLD:

ملاحظة: تغيرت الصياغة عبر أنظمة/إصدارات مختلفة.

-

```
udld enable
Once globally enabled, all FE and GE fiber !--- ports have UDLD enabled by default. ---!
udld port
```

أو

-

```
udld enable
The copper ports of some earlier Cisco IOS Software !--- releases can have UDLD enabled ---!
.by individual port command
```

أنت ينبغي يدويا مكنت ميناء أن يكون عطلت بسبب {unidirectional{mixed خطوة عرض. أستخدم إحدى الطريقتين التاليتين:

```
udld reset
Globally reset all interfaces that UDLD shut down. no udld port ---!
[udld port [aggressive
.Per interface, reset and reenable interfaces that UDLD shut down ---!
```

ال **errdisable إستعادة سبب udld** و **errdisable إستعادة فاصل** تشكيل أمر يستطيع كنت استعملت أن تلقائيا إستردت من ال UDLD خطأ يعجز دولة.

cisco يوصي أن يستعمل أنت فقط ال errdisable إستعادة آلية في الوصول طبقة من الشبكة، مع إستعادة وقت 20 دقيقة أو أكثر، إن الوصول طبيعي إلى المفتاح صعب. أفضل حالة هي السماح بالوقت لتثبيت الشبكة واستكشاف الأخطاء وإصلاحها، قبل إعادة المنفذ إلى الخط ويتسبب في عدم إستقرار الشبكة.

توصي Cisco بعدم إستخدام آليات الاسترداد في مركز الشبكة لأن هذا يمكن أن يتسبب في عدم الاستقرار الذي يرتبط بأحداث التقارب في كل مرة يتم فيها إعادة إرتباط معيب إلى الواجهة. التصميم المتكرر لشبكة لب يوفر مسار نسخ إحتياطي لارتباط فاشل ويتيح الوقت لدراسة أسباب فشل UDLD.

إستخدام UDLD بدون واقي حلقة STP

لطبقة 3 نقطة إلى نقطة، أو طبقة 2 خطوة حيث هناك يكون libre STP طبولوجيا (ما من ميناء حظر)، cisco يوصي أن أنت يمكن عدواني UDLD على نقطة إلى نقطة FE/GE خطوة بين cisco مفتاح. في هذه الحالة، ثبتت الرسالة فاصل إلى سبعة ثاني، و 802.1D STP يستعمل وقت افتراضي.

UDLD على EtherChannels

ما إذا STP أنشوطة حارس نشرت أو لا ينشر، UDLD عدواني أسلوب يوصى ل أي EtherChannel تشكيل، بالاقتران مع ال مرغوب قناة أسلوب. في تكوينات EtherChannel، يمكن أن يؤدي فشل في الارتباط الخاص بالقناة الذي يحمل الشجرة المتفرعة BPDUs وحركة مرور التحكم في PAgP إلى حلقات تكرار فورية بين شركاء القناة إذا أصبحت روابط القناة غير مجزأة. يعطل وضع UDLD العدائي منفذ فاشل. يمكن بعد ذلك ل PAgP (وضع القناة التلقائي/المرغوب فيها) التفاوض حول إرتباط تحكم جديد والتخلص بفعالية من إرتباط فاشل من القناة.

UDLD مع الشجرة الممتدة 802.1w

لمنع حلقات التكرار عند إستخدام إصدارات الشجرة المتفرعة الأحدث، أستخدم وضع UDLD العادي وواقي حلقة STP مع RSTPs مثل UDLD .802.1w يستطيع زودت حماية من خطوة أحادي إتجاه أثناء خطوة ربط، و STP أنشوطة حارس يستطيع منعت أنشوطة STP في حال أن الروابط أصبحت أحادي إتجاه بعد أن أسس UDLD الروابط ك ثنائي إتجاه. لأن أنت يستطيع لا يشكل UDLD أن يكون أقل من التقصير 802.1w وقت، STP أنشوطة حارس ضروري in order to منعت كليا أنشوطة في طوبولوجيا فائض.

راجع فهم ميزة بروتوكول اكتشاف الارتباط أحادي الإتجاه (UDLD) وتكوينها للحصول على مزيد من التفاصيل.

إختبار ومراقبة UDLD

UDLD ليس سهل أن يختبر دون خطأ حقيقي/مكون أحادي الإتجاه في المختبر، مثل GBIC معيب. وقد صمم البروتوكول لاكتشاف سيناريوهات فشل أقل شيوعا من تلك السيناريوهات التي تستخدم عادة في المختبر. على سبيل المثال، إن ينجز أنت إختبار بسيط مثل إلغاء توصيل واحد خيط من ليف in order to رأيت errdisable مرغوب دولة، أنت تحتاج أن يلتفت أولا طبقة autonegoation 1. وإلا، الميناء طبيعي يذهب ، أي يعيد UDLD رسالة إتصال. ينتقل النهاية البعيدة إلى حالة في UDLD عادي أسلوب، وينقل إلى دولة errdisable فقط مع الإستعمالمن UDLD عدائي أسلوب.

طريقة إختبار إضافية تحاكي فقدان PDU المجاور ل UDLD. الطريقة أن يستعمل ماك طبقة مرشح in order to منعت ال UDLD/CDP جهاز عنوان بينما أنت تسمح آخر عنوان أن يمر. بعض مفتاح لا يرسل UDLD إطار عندما الميناء يكون شكلت أن يكون يحول محلل أيسر (فسحة بين دعامتين) غاية، أي يحاكي غير مستجيب UDLD مجاور.

in order to راقبت UDLD، استعملت هذا أمر:

```
show udld gigabitethernet1/1
Interface Gi1/1
---
Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 7
Time out interval: 5
```

أيضا، من وضع التمكين في cisco ios برمجية إطلاق sxd(18)12.2 أو مفتاح متأخر، أنت يستطيع أصدرت المخفي **عرض udld جار** أمر in order to فحصت ال UDLD ذاكرة تخزين مؤقت محتويات (بالطريقة أن CDP يفعل). غالبا ما يكون مفيدا جدا مقارنة ذاكرة التخزين المؤقت ل UDLD بذاكرة التخزين المؤقت ل CDP للتحقق من وجود خطأ خاص بالبروتوكول. وعندما يتأثر بروتوكول CDP أيضا، فإنه يعني عادة أن جميع وحدات بيانات بروتوكول الجسر/وحدات بيانات بروتوكول الجسر (BPDUs) تتأثر. لذلك، تحقق أيضا من بروتوكول الشجرة المتفرعة (STP). على سبيل المثال، تحقق من تغييرات هوية الجذر الحديثة أو تغييرات وضع المنفذ الجذري/المعين.

أنت يستطيع راقبت UDLD وضع وتشكيل تناسق مع إستعمال من ال mib cisco UDLD SNMP متغير.

التبديل متعدد الطبقات

نظرة عامة

في cisco ios نظام برمجية، يتم دعم التحويل متعدد الطبقات (MLS) على المادة حفازة sery 6000/6500، داخليا فقط. هذا يعني أنه يجب تثبيت الموجه في المحول. تدعم محركات المشرف الأحدث Catalyst 6500/6000 Supervisor Engines MLS CEF، حيث يتم تنزيل جدول التوجيه إلى كل بطاقة. وهذا يتطلب أجهزة إضافية، تتضمن وجود بطاقة إعادة توجيه موزعة (DFC). لا يتم دعم DFCs في برنامج CatOS، حتى إذا أخترت إستخدام برنامج Cisco IOS Software على بطاقة الموجه. يتم دعم DFCs فقط في برنامج Cisco IOS System.

ذاكرة التخزين المؤقت MLS التي يتم إستخدامها لتمكين إحصائيات NetFlow على محولات Catalyst هي ذاكرة التخزين المؤقت المستندة إلى التدفق التي تستخدمها محولات Supervisor Engine I card و Catalyst القديمة لتمكين تحويل الطبقة 3. MLS مكنت افتراضيا على المشرف محرك 1 (أو مشرف محرك 1a) مع MSFC أو MSFC2. لا يلزم تكوين MLS إضافي لوظيفة MLS الافتراضية. يمكنك تكوين ذاكرة التخزين المؤقت MLS في أحد الأوضاع الثلاثة:

- غاية
- مصدر-غاية
- منفذ مصدر-غاية

يتم إستخدام قناع التدفق لتحديد وضع MLS للمحول. يتم إستخدام هذه البيانات لاحقا لتمكين تدفقات الطبقة 3 في محولات Supervisor Engine (محرك المشرف) المزودة بمادة حفازة. لا تستخدم الخوادم النصلية Supervisor Engine II ذاكرة التخزين المؤقت ل MLS لتبديل الحزم لأن هذه البطاقة تدعم الأجهزة CEF، وهي تقنية أكثر قابلية للتطوير. يتم الاحتفاظ بذاكرة التخزين المؤقت MLS في بطاقة Supervisor Engine II لتمكين التصدير الإحصائي NetFlow فقط. لذلك، يمكن تمكين Supervisor Engine II للتدفق الكامل إذا لزم الأمر، دون تأثير سلبي على المحول.

التكوين

يتم تطبيق وقت تقادم MLS على كافة إدخالات ذاكرة التخزين المؤقت ل MLS. يتم تطبيق قيمة زمن التقادم مباشرة على شيخوخة وضع الوجهة. أنت تقسم ال MLS شيخوخة وقت قيمة إثنان in order to استخرجت المصدر إلى غاية أسلوب شيخوخة وقت. قم بتقسيم قيمة وقت تقادم MLS على ثمانية للبحث عن وقت تقادم التدفق الكامل. قيمة وقت تقادم MLS الافتراضية هي 256 ثانية.

يمكنك تكوين وقت التقادم العادي في نطاق من 32 إلى 4092 ثانية في ثماني زيادات ثانية. يتم ضبط أي قيمة لوقت التقادم لا تكون مضاعفا لثماني ثوان إلى أقرب مضاعف من 8 ثوان. على سبيل المثال، يتم تعديل قيمة 65 إلى 64 ويتم تعديل قيمة 127 إلى 128.

يمكن أن تتسبب الأحداث الأخرى في إزالة إدخالات MLS. وتشمل هذه الأحداث ما يلي:

- تغييرات التوجيه
- تغيير في حالة الارتباطعلى سبيل المثال، إرتباط PFC معطل.

للحفاظ على حجم ذاكرة التخزين المؤقت MLS تحت 32،000 مدخل، قم بتمكين هذه المعلمات بعد إصدار الأمر **mls aging**:

```
Normal: configures the wait before aging out and deleting shortcut entries in
.the L3 table

Fast aging: configures an efficient process to age out entries created for flows that
only switch a few packets and then are never used again. The fast aging parameter uses
the time keyword value to check if at least the threshold keyword value of packets has
been switched for each flow. If a flow has not switched the threshold number of packets
.during the time interval, then the entry in the L3 table is aged out

Long: configures entries for deletion that have been up for the specified value even if
the L3 entry is in use. Long aging is used to prevent counter wraparound, which could
.cause inaccurate statistics
```

التكوين

إدخال ذاكرة التخزين المؤقت النموذجي الذي تتم إزالته هو إدخال التدفقات إلى ومن خادم اسم المجال (DNS) أو خادم TFTP الذي من المحتمل ألا يتم إستخدامه مرة أخرى بعد إنشاء الإدخال. يؤدي اكتشاف هذه الإدخالات والخروج منها إلى توفير مساحة في ذاكرة التخزين المؤقت ل MLS لحركة مرور البيانات الأخرى.

إذا كنت بحاجة إلى تمكين وقت التقادم السريع MLS، فقم بتعيين القيمة الأولية إلى 128 ثانية. إذا استمر حجم ذاكرة التخزين المؤقت MLS في النمو أكثر من 32000 إدخال، فقم بخفض الإعداد حتى يبقى حجم ذاكرة التخزين المؤقت أقل من 32000. إذا إستمرت ذاكرة التخزين المؤقت في النمو أكثر من 32000 إدخال، فقل وقت تقادم MLS العادي.

تكوين MLS الموصى به من Cisco

أترك MLS عند القيمة الافتراضية، الوجهة فقط، إلا إذا كان تصدير NetFlow مطلوبا. إذا كان NetFlow مطلوبا، فقم بتمكين التدفق الكامل ل MLS فقط على أنظمة Supervisor Engine II.

أصدرت هذا أمر in order to مكنت MLS تدفق غاية:

```
Switch(config)#mls flow ip destination
```

إطارات Jumbo

وحدة الإرسال القصوى

وحدة الإرسال القصوى (MTU) هي أكبر مخطط بيانات أو حجم حزمة بالبايت يمكن للواجهة إرساله أو إستلامه دون تجزئة الحزمة.

وفقا لمعيار IEEE 802. 3، يكون الحد الأقصى لحجم إطار شبكة إيثرنت:

- **1518 بايت** للإطارات العادية (1500 بايت بالإضافة إلى 18 بايت إضافية من رأس إيثرنت ومقطورة CRC)
- **1522 بايت** للإطارات المغلفة ب 802.1Q) 1518 بالإضافة إلى 4 بايت من التمييز)

شركة Baby Giants: تتيح ميزة Baby Giants للمحول إمكانية تمرير حزم/إعادة توجيه أكبر حجما بقليل من الحد الأقصى للنقل (MTU) عبر شبكة إيثرنت من IEEE، بدلا من الإعلان عن أن الإطارات كبيرة الحجم ومتجاهلة.

Jumbo: يعتمد تعريف حجم الإطار على البائع، لأن أحجام الإطارات ليست جزءا من معيار IEEE. الإطارات كبيرة الحجم هي إطارات أكبر من حجم إطار إيثرنت القياسي (وهو 1518 بايت، والذي يتضمن رأس الطبقة 2 وتسلسل فحص الإطارات [FCS]).

الحجم الافتراضي لوحدة الحد الأقصى للنقل (MTU) هو 9216 بايت بعد تمكين دعم الإطارات الكبيرة على المنفذ الفردي.

متى يمكن توقع حزم أكبر من 1518 بايت

in order to نقلت حركة مرور عبر شبكات يحول، تأكدت أن الحركة مرور يبث MTU لا يتجاوز أن يكون ساندت على المفتاح منصة. هناك أسباب مختلفة تدعو إلى إمكانية اقتطاع حجم وحدة الحد الأقصى للنقل (MTU) لإطارات معينة:

- **المتطلبات الخاصة بالمورد**—يمكن للتطبيقات وبعض بطاقات واجهة الشبكة (NICs) تحديد حجم MTU خارج الحجم القياسي 1500 بايت. وقد حدث هذا التغيير بسبب الدراسات التي تثبت أن زيادة حجم إطار إيثرنت يمكن أن تزيد من متوسط الإنتاجية.
- **trunking**— لحمل معلومات معرف شبكة VLAN بين المحولات أو أجهزة الشبكة الأخرى، تم إستخدام trunking لزيادة إطار الإيثرنت القياسي. واليوم، فإن الشكلين الأكثر شيوعا للربط هما:تضمين ISL الخاص من Cisco802,1q
- **Multiprotocol Label Switching (MPLS)**— بعد أن تقوم بتمكين MPLS على واجهة، MPLS له إمكانية زيادة حجم إطار الحزمة، والتي تعتمد على عدد التسميات في مكدس التسمية للحزمة MPLS-tagged. الحجم الإجمالي للتسمية هو 4 بايت. الحجم الإجمالي لمكدس تسميات هو:
  `n * 4 bytes`
  إذا تم تكوين مكدس تسميات، فإن الإطارات يمكن أن تتجاوز MTU.
- **802.1Q tunneling**—802.1Q تحتوي الحزم النفقي على علامتين 802.1Q، منها واحدة فقط في كل مرة تكون عادة مرئية للأجهزة. وبالتالي، تضيف العلامة الداخلية 4 بايت إلى قيمة MTU (حجم الحمولة).
- **تتضمن واجهة النقل العالمي (UTI)/بروتوكول الاتصال النفقي للطبقة 2 الإصدار 3 (Layer 2TPv3)**—UTI/Layer 2TPv3 بيانات الطبقة 2 التي سيتم إعادة توجيهها عبر شبكة IP. يمكن أن يزيد UTI/Layer 2TPv3 حجم الإطار الأصلي بما يصل إلى 50 بايت. يتضمن الإطار الجديد رأس IP جديد (20 بايت)،

رأس الطبقة 12) 2TPv3 بايت)، ورأس طبقة 2 جديد. تتكون حمولة الطبقة 2TPv3 من إطار الطبقة 2 الكامل، والذي يتضمن رأس الطبقة 2.

الغرض

تحويل قائم على الأجهزة فائق السرعة (1 جيجابت في الثانية و 10 جيجابت في الثانية) جعل الإطارات كبيرة الحجم حلا ملموسا للغاية لمشاكل سعة المعالجة غير المثالية. على الرغم من عدم وجود مقياس رسمي لحجم الإطار كبير الحجم، فإن القيمة الشائعة إلى حد ما التي يتم اعتمادها عادة في الحقل هي 9216 بايت (9 كيلوبايت).

إعتبار كفاءة الشبكة

يمكنك حساب كفاءة الشبكة لإعادة توجيه الحزمة إذا قمت بقسمة حجم الحمولة الخاص بها على مجموع قيمة التكاليف الإضافية وحجم الحمولة.

حتى إذا كانت زيادة كفاءة الشبكة باستخدام إطارات كبيرة الحجم متواضعة فقط، وتذهب من 94.9 في المائة (1500 بايت) إلى 99.1 في المائة (9216 بايت)، فإن مصروفات المعالجة (إستخدام وحدة المعالجة المركزية) لأجهزة الشبكة والمضيفين النهائيين تنخفض نسبيا إلى حجم الحزمة. هذا هو السبب في أن تقنيات شبكات LAN وشبكات WAN عالية الأداء تفضل أحجام الإطارات القصوى الكبيرة.

لا يمكن تحسين الأداء إلا عند إجراء عمليات نقل طويلة للبيانات. تتضمن أمثلة التطبيقات:

- الاتصال من الخادم إلى الخلف (على سبيل المثال، معاملات نظام ملفات الشبكة [NFS])
- تجميع الخوادم
- عمليات نسخ إحتياطي للبيانات عالية السرعة
- اتصال حاسوبي فائق السرعة
- عمليات نقل بيانات التطبيقات الرسومية

إعتبار أداء الشبكة

تمت دراسة أداء بروتوكول TCP عبر شبكات WAN (الإنترنت) بشكل مكثف. توضح هذه المعادلة كيف يحتوي إخراج بروتوكول TCP على حد أعلى استنادا إلى:

- الحد الأقصى لحجم المقطع (MSS)، وهو طول MTU ناقص طول رؤوس TCP/IP
- وقت الذهاب والعودة (RTT)
- فقدان الحزمة

$$Throughput \leq\sim 0.7 \times MSS / \left(RTT \times \sqrt{packet\_loss} \right)$$

وفقا لهذه الصيغة، يتناسب إخراج TCP الأقصى القابل للإنجاز بشكل مباشر مع MSS. هذا يعني أنه، مع RTT الثابت وفقدان الحزمة، يمكنك مضاعفة معدل إخراج TCP إذا قمت بمضاعفة حجم الحزمة. وبالمثل، عند إستخدام إطارات ضخمة بدلا من الإطارات سعة 1518 بايت، يمكن أن تؤدي زيادة الحجم بمقدار ستة أضعاف إلى تحسين سعة معالجة بروتوكول TCP لاتصال إيثرنت محتمل بمقدار ستة أضعاف.

نظرة عامة على العمليات

تحدد مواصفات IEEE 802.3 القياسية حجم إطار إيثرنت الأقصى **1518**. تمت إضافة الإطارات 802.1Q المغلفة، والتي يتراوح طولها بين 1519 و 1522 بايت، إلى مواصفات 802.3 في مرحلة لاحقة من خلال إضافة IEEE Std 802.3ac-1998. ويشار اليهم أحيانا في المطبوعات بصفتهم **عمالقة الاطفال**.

بشكل عام، يتم تصنيف الحزم **كإطارات عملاقة** عندما تتجاوز الحد الأقصى للطول المحدد لشبكة إيثرنت لاتصال إيثرنت معين. تعرف الحزم العملاقة أيضا **بالإطارات الضخمة**.

النقطة الرئيسية للتشويش حول الإطارات الكبيرة هي التكوين: تدعم الواجهات المختلفة الحد الأقصى لأحجام الحزم المختلفة، وفي بعض الأحيان، تتعامل مع الحزم الكبيرة بطرق مختلفة قليلا.

Catalyst 6500 Series

يحاول هذا طاولة أن يلخص ال MTU حجم أن يكون حاليا ساندت ب بطاقة مختلف على المادة حفازة 6500 منصة:

بطاقة خط	حجم MTU
افتراضي	9216 بايت
WS-X6248-RJ-45، WS-X6248a-RJ-45، WS-X6248-TEL، WS-X6248a-TEL، WS-X6348-RJ-45، WS-X6348-RJ45V، WS-X6348-RJ-21، و WX X6348-RJ21V	8092 بايت (محددة بواسطة شريحة PHY)
WS-X6148-RJ-45(V) و WS-X6148-RJ-21(V) و WS-X6148-45AF و WS-X6148-21AF	9100 بايت (100 ميجابت في الثانية) 9216 بايت (10 ميجابت في الثانية)
WS-X6516-GE-TX	8092 بايت (100 ميجابت في الثانية) 9216 بايت (10 أو 1000 ميجابت في الثانية)
WS-X6148(V)-GE-TX و WS-X6148-GE-45AF و WS-X6548(V)-GE-TX و WS-X6548-GE-45AF	1500 بايت
OSM ATM (OC12c)	9180 بايت
OSM CHOC3 و CHOC12 و CHOC48 و CT3	9216 بايت (OCx و 7673 (DS3 بايت (T1/E1)
FlexWAN	7673 بايت (9216 (CT3 T1/DS0 بايت (7673 (OC3c POS بايت (T1)
WS-X6148-GE-TX و WS-X6548-GE-TX	لا يوجد دعم

ارجع إلى تكوين تحويل الإيثرنت والإيثرنت السريع وإيثرنت جيجابت وإيثرنت 10 جيجابت للحصول على مزيد من المعلومات.

دعم الاتصال من المستويين 2 و 3 في برنامج Catalyst 6500/6000 Cisco IOS Software

يوجد دعم كبير الحجم من المستويين الثاني والثالث مع PFC/MSFC1، و PFC/MSFC2، و PFC2/MSFC2 في جميع منافذ GE التي تم تكوينها كواجهات مادية من المستويين الثاني والثالث. الدعم موجود regardless of هذا ميناء يكون trunking أو يقني. تتوفر هذه الميزة في برنامج Cisco IOS الإصدار 12.1.1E والإصدارات الأحدث.

- يتم ربط أحجام وحدة الحد الأقصى للنقل (MTU) لجميع المنافذ المادية التي تم تمكينها بواسطة Jumbo معا.

التغيير في واحد منهم يغير كل شيء. دائما ما يحتفظون بنفس حجم وحدة الحد الأقصى للنقل (MTU) للإطار كبير الحجم بعد تمكينها.

- أثناء التكوين، قم إما بتمكين جميع المنافذ في شبكة VLAN نفسها التي تم تمكينها بواسطة jumbo، أو تمكين لا شيء منها تم تمكين jumbo.
- تم تعيين حجم وحدة الحد الأقصى للنقل (MTU) للواجهة الظاهرية المحولة (SVI) (واجهة شبكة VLAN) بشكل منفصل عن المنافذ المادية MTU. لا يؤدي أي تغيير في المنافذ المادية MTU إلى تغيير حجم SVI MTU. أيضا، لا يؤثر التغيير في SVI MTU على المنافذ المادية MTU.
- بدأ دعم الإطارات الضخمة من المستويين 2 و 3 على واجهات FE في برنامج Cisco IOS الإصدار 12.1((8a EX01. يعمل الأمر **MTU 1500** على تعطيل ميزة Jumbo على FE، كما يوفر الأمر **MTU 9216** إمكانية الاتصال واسعة النطاق على بروتوكول FE. أحلت cisco بق CSCdv90450 id (يسجل زبون فقط).
- إطارات ضخمة من الطبقة 3 على واجهات VLAN مدعومة فقط على:PFC/MSFC2 (برنامج CISCO IOS الإصدار 12.1(7a)E والإصدارات الأحدث)PFC2/MSFC2 (برنامج CISCO IOS الإصدار 12.1(8a)E4 والإصدارات الأحدث)
- لا يوصى باستخدام إطارات كبيرة مع PFC/MSFC1 لواجهات VLAN (SVIs) لأن MSFC1 قد لا يكون قادرا على معالجة التجزئة حسب الرغبة.
- لا يساند أي تجزئة للحزم ضمن ال نفسه VLAN (طبقة jumbo 2).
- يتم إرسال الحزم التي تحتاج إلى التجزئة عبر شبكات VLAN/الشبكات الفرعية (طبقة jumbo 3) إلى البرنامج للتجزئة.

فهم دعم الإطارات كبيرة الحجم في Catalyst 6500/6000 برنامج Cisco IOS Software

الإطار كبير الحجم هو إطار أكبر من حجم إطار إيثرنت الافتراضي. لتمكين دعم الإطارات كبيرة الحجم، يمكنك تكوين حجم MTU أكبر من الافتراضي على واجهة منفذ أو شبكة محلية ظاهرية (VLAN)، ومع برنامج Cisco IOS الإصدار 12.1(13)E والإصدارات الأحدث، قم بتكوين حجم LAN العالمي لمنفذ MTU.

التحقق من حجم حركة المرور العابرة والموجهة في برنامج Cisco IOS Software

بطاقة خط	مدخل	مخرج
10- منافذ بسرعة 100/10 ميجابت في الثانية	تم التحقق من حجم وحدة الحد الأقصى للنقل (MTU). يقوم دعم الإطارات الكبيرة بمقارنة حجم حركة مرور البيانات بالمداخل مع حجم وحدة الحد الأقصى للنقل (MTU) لشبكة LAN العالمية عند الدخول عبر منافذ إيثرنت بسرعة 10- و 100/10- و 100 ميجابت في الثانية وشبكة LAN بسرعة 10 جيجابت التي تحتوي على حجم وحدة الحد الأقصى للنقل (MTU) غير الافتراضي الذي تم تكوينه. يسقط المنفذ حركة المرور التي تكون أكبر من حجمها.	لم يتم التحقق من حجم وحدة الحد الأقصى للنقل (MTU). منافذ تم تكوينها بحجم

		غير افتراضي لوحدة الحد الأقصى للنقل (MTU) إطارات تحتوي على حزم أكبر من 64 بايت بأي حجم. مع حجم وحدة الحد الأقصى للنقل (MTU) غير الافتراضي الذي تم تكوينه، لا تقوم منافذ شبكة محلية إيثرنت

		ت بسر عة 10 و /10 100 و 100 ميجا بت في الثانيـ ة بالبحـ ث عن إطار ات الخر وج ذات الحجـ م الزائـ د.
منافذ GE	لم يتم التحقق من حجم وحدة الحد الأقصى للنقل (MTU). تقبل المنافذ التي تم تكوينها بحجم MTU غير افتراضي الإطارات التي تحتوي على حزم أكبر من 64 بايت ولا تتحقق من إطارات الدخول ذات الحجم الزائد.	تم التحـ قق من حجـ م وحد ة الحد الأقـ صى للنقـ ل (MT U). يقار ن دعم إطار Ju mb o حجـ م حرك ة مرور

		المخرج مع المخرج lan ميناء MTU حجم عند مخرج GE و 10-GE lan ميناء أن يتلقى حجم MTU غير افتراضي يشكل. يسقط المنفذ حركة المرور التي تكون أكبر من حجمها.
منافذ شبكة إيثرنت بسرعة 10 جيجابت	تم التحقق من حجم وحدة الحد الأقصى للنقل (MTU). يسقط المنفذ حركة المرور التي تكون أكبر من حجمها.	تم التحقق من حجم

		وحدة الحد الأقصى للنقل (MTU). يسقط المنفذ حركة المرور التي تكون أكبر من حجمها.
SVI	لم يتم التحقق من حجم وحدة الحد الأقصى للنقل (MTU). لا يتحقق ال SVI من حجم الإطار على المدخل جانب.	تم التحقق من حجم وحدة الحد الأقصى للنقل (MTU). يتم التحقق من حجم MTU على جانب مخرج SVI

		.
	PFC	
جميع حركة المرور الموجهة	لحركة المرور التي يجب توجيهها، يقارن دعم الإطارات الكبيرة على PFC أحجام حركة المرور بأحجام MTU التي تم تكوينها ويوفر تحويل الطبقة 3 لحركة المرور الكبيرة بين الواجهات التي تم تكوينها بأحجام MTU الكبيرة بدرجة كافية لاستيعاب حركة المرور. بين الواجهات التي لم يتم تكوينها بأحجام MTU كبيرة بدرجة كافية: • إذا لم يتم تعيين بت عدم التجزئة (DF)، فإن PFC يرسل حركة مرور البيانات إلى MSFC in order to تمت تجزئته وتوجيه توجيهه في البرنامج. • إذا تم ضبط بت DF، فإن PFC يسقط حركة المرور.	

توصيات Cisco

إذا تم تطبيقها بشكل صحيح، فيمكن أن توفر الإطارات كبيرة الحجم إمكانية تحسين سعة معالجة TCP بمقدار ستة أضعاف لاتصال إيثرنت، مع تقليل المصاريف الإضافية المتعلقة بانقسام البيانات (بالإضافة إلى تقليل حمل وحدة المعالجة المركزية (CPU) على الأجهزة الطرفية).

يجب التأكد من عدم وجود أي جهاز في الوسط غير قادر على معالجة حجم MTU المحدد. إذا قام هذا الجهاز بتجزئة الحزم وإعادة توجيهها، فإنه يبطل العملية بالكامل. يمكن أن يؤدي هذا إلى إضافة مصروفات عامة على هذا الجهاز لتجزئة الحزم وإعادة تجميعها.

في مثل هذه الحالات، يساعد اكتشاف وحدة الحد الأقصى للنقل (MTU) لمسار IP المرسلين على العثور على الحد الأدنى لطول الحزمة المشتركة المناسب لنقل حركة المرور على كل مسار. بدلا من ذلك، يمكنك تكوين الأجهزة المضيفة واسعة النطاق المتوافقة مع الإطار مع حجم MTU الذي هو الحد الأدنى لجميع الأجهزة المدعومة في الشبكة.

يجب عليك التحقق بعناية من كل جهاز للتأكد من أنه يمكنه دعم حجم وحدة الحد الأقصى للنقل (MTU). راجع جدول دعم حجم وحدة الحد الأقصى للنقل (MTU) في هذا القسم.

يمكن تمكين دعم الإطارات الكبيرة على أنواع الواجهات التالية:

- واجهة قناة المنفذ
- SVI
- الواجهة المادية (الطبقة 2/الطبقة 3)

أنت يستطيع مكنت jumbo إطار على الميناء قناة أو القارن طبيعي أن يساهم في الميناء قناة. من المهم للغاية التأكد من أن وحدة الحد الأقصى للنقل (MTU) على جميع الواجهات المادية متشابهة. وإلا، يمكن أن ينتج عن ذلك واجهة معلقة. أنت تحتاج أن يغير ال MTU من ميناء قناة قارن لأن هو يغير ال MTU من كل عضو ميناء.

ملاحظة: إذا تعذر تغيير وحدة الحد الأقصى للنقل (MTU) لمنفذ عضو إلى القيمة الجديدة لأن منفذ العضو هو منفذ الحظر، فسيتم تعليق قناة المنفذ.

دائما تأكد من تكوين جميع الواجهات المادية في شبكة VLAN لإطارات ضخمة قبل تكوين دعم الإطارات الكبيرة على SVI. لا يتم التحقق من وحدة الحد الأقصى للنقل (MTU) للحزمة على جانب المدخل من SVI. ولكن، يتم فحصه على جانب المخرج من SVI. إذا كانت الحزمة MTU أكبر من المخرج SVI MTU، الربط مجزأة حسب برمجية (إن لم يتم تعيين بت DF)، مما ينتج عنه أداء ضعيف. يحدث تجزئة البرامج فقط لتحويل الطبقة 3. عندما تتم إعادة توجيه الحزمة إلى منفذ من الطبقة 3 أو SVI باستخدام وحدة الحد الأقصى للنقل (MTU) أصغر، يحدث تجزئة البرنامج.

يجب أن تكون وحدة الحد الأقصى للنقل (MTU) الخاصة ب SVI دائما أصغر من أصغر وحدة الحد الأقصى للنقل (MTU) بين جميع منافذ المحول في شبكة VLAN.

Catalyst 4500 Series

يتم دعم الإطارات كبيرة الحجم بشكل رئيسي على المنافذ غير القابلة للحظر لبطاقات الخط Catalyst 4500. ولمنافذ GE غير القابلة للحظر هذه إتصالات مباشرة ببنية تحويل Supervisor Engine (المحرك المشرف) وتدعم الإطارات كبيرة الحجم:

- محركات المشرفWS-X4516، WS-X4515—منفذان GBIC بارتباطين على Supervisor Engine IV أو VWS-X4516-10GE - وصلتان 10 جيجابت والوصلات الأربع ذات التصميم الصغير 1 جيجابت القابلة للتوصيل (+WS-X4013(SFP—وصلتان لشبكة إيثرنت بسرعة 1 جيجابتWS-X4013+10GE - وصلتان 10 جيجابت إيثرنت والوصلات الأربع 20 - WS-X4013+TS-GE1 منفذ SFP 1-GE
- بطاقات خطوطالوحدة النمطية WS-X4306-GB — Six-port 1000BASE-X (GBIC) GE Moduleالطراز WS-X4506-GB-T — ثماني منافذ بسرعة 1000/100/10 ميجابت في الثانية وبستة منافذ SFPالوحدة النمطية WS-X4302-GB—Two-Port 1000BASE-X (GBIC) GE Moduleمنفذا GBIC الأولان من وحدة GE لتحويل الخادم ذات 18 منفذا (WS-X4418-GB) ومنفذ GBIC من الوحدة النمطية WS-X4232-GB-RJ
- محولات ذات تكوين ثابتالطراز WS-C4948 — جميع المنافذ التي تعمل عبر شبكة إيثرنت بسرعة 1 جيجابت والبالغ عددها 48 منفذاالطراز WS-C4948-10GE — جميع المنافذ التي تعمل عبر شبكة إيثرنت بسرعة 1 جيجابت والتي يبلغ عددها 48 منفذا ومنفذي شبكة إيثرنت بسرعة 10 جيجابت

يمكنك إستخدام منافذ GE غير القابلة للحظر هذه لدعم إطارات Jumbo بسعة 9 كيلوبايت أو قمع بث الأجهزة (Supervisor Engine IV فقط). جميع بطاقات الخط الأخرى تدعم إطارات الطفل العملاقة. يمكنك إستخدام العمالقة الصغار لربط MPLS أو ل Q في كلمة المرور بحد أقصى للحمولة 1552 بايت.

ملاحظة: يزداد حجم الإطار مع علامات تمييز ISL/802.1Q.

تعد صغار العمالقة وإطارات jumbo شفافة لميزات Cisco IOS الأخرى باستخدام محركات المشرف IV و V.

ميزات أمان برنامج Cisco IOS

ميزات الأمان الأساسية

وفي وقت من الأوقات، كانت التصاميم في الحرم الجامعي تغفل كثيرا عن تدابير الأمن. ولكن، أصبح الأمان الآن جزءا أساسيا من كل شبكة من شبكات المؤسسات. عادة، يكون العميل قد أنشأ سياسة أمان بالفعل للمساعدة في تحديد الأدوات والتقنيات القابلة للتطبيق من Cisco.

الحماية الأساسية لكلمة المرور

يتم تكوين معظم أجهزة برنامج Cisco IOS software باستخدام مستويين من كلمات المرور. المستوى الأول هو وصول برنامج Telnet إلى الجهاز، والذي يعرف أيضا بوصول vty. بعد منح وصول VTY، يلزمك الحصول على حق الوصول إلى وضع التمكين أو وضع EXEC ذي الامتيازات.

تأمين وضع التمكين للمحول

تتيح كلمة مرور enable للمستخدم إمكانية الوصول الكامل إلى جهاز ما. منح كلمة مرور enable فقط للأشخاص الموثوق بهم.

```
Switch(config)#enable secret password
```

تأكد من أن كلمة المرور تطيع هذه القواعد:

- يجب أن تحتوي كلمة المرور على أحرف أبجدية ورقمية صغيرة يتراوح عددها بين واحد و 25 حرفا.
- يجب ألا تحتوي كلمة المرور على رقم كالحرف الأول.
- يمكنك إستخدام المسافات البادئة، لكنها يتم تجاهلها. يتم التعرف على المسافات الوسيطة والمتجانبة.
- التحقق من كلمة المرور حساس لحالة الأحرف. على سبيل المثال، يختلف سر كلمة المرور عن سر كلمة المرور.

ملاحظة: يستخدم الأمر **enable secret** دالة تجزئة رسالة مشفرة أحادية الإتجاه (MD5 Digest 5). إذا قمت بإصدار الأمر **show running-config**، فيمكنك رؤية كلمة المرور المشفرة هذه. إستعمال من **ال enable كلمة** أمر آخر أن يثبت ال enable كلمة. ولكن خوارزمية التشفير التي يتم إستخدامها مع الأمر **enable password** ضعيفة ويمكن عكسها بسهولة للحصول على كلمة المرور. لذلك، لا يستعمل ال **enable كلمة** أمر. أستخدم الأمر **enable secret** للحصول على أمان أفضل. راجع حقائق تشفير كلمة مرور Cisco IOS للحصول على مزيد من المعلومات.

وصول Telnet/VTY الآمن إلى المحول

بشكل افتراضي، يدعم برنامج Cisco IOS software خمس جلسات عمل Telnet نشطة. يشار إلى هذه الجلسات ب0 vty إلى 4. يمكنك تمكين هذه الخطوط للوصول. ولكن in order to مكنت login، أنت تحتاج أيضا المجموعة كلمة ل هذا خط.

```
Switch(config)#line vty 0 4
Switch(config-line)#login
Switch(config-line)#password password
```

يقوم الأمر **login** بتكوين هذه الخطوط للوصول إلى Telnet. يقوم الأمر **password** بتكوين كلمة مرور. تأكد من أن كلمة المرور تطيع هذه القواعد:

- لا يمكن أن يكون الحرف الأول رقما.
- يمكن أن تحتوي السلسلة على أي أحرف أبجدية رقمية، حتى 80 حرفا. تتضمن الحروف مسافات.
- لا يمكنك تحديد كلمة المرور بتنسيق number-space-character. يسبب الفراغ بعد الرقم مشاكل. على سبيل المثال، Hello 21 هو كلمة مرور قانونية، لكن Hello 21 ليس كلمة مرور قانونية.
- التحقق من كلمة المرور حساس لحالة الأحرف. على سبيل المثال، يختلف سر كلمة المرور عن سر كلمة المرور.

ملاحظة: باستخدام تكوين سطر vty هذا، يقوم المحول بتخزين كلمة المرور في نص واضح. إذا أصدر شخص ما الأمر **show running-config**، تكون كلمة المرور هذه مرئية. لتجنب هذه الحالة، أستخدم الأمر **service password-encryption**. يقوم الأمر بتشفير كلمة المرور بشكل فضفاض. يقوم الأمر فقط بتشفير كلمة مرور سطر vty وكلمة مرور enable التي تم تكوينها باستخدام الأمر **enable password**. يستخدم الأمر enable password الذي تم تكوينه باستخدام الأمر **enable secret** تشفيرا أقوى. والتكوين باستخدام الأمر **enable secret** هو الطريقة الموصى بها.

ملاحظة: للحصول على مزيد من المرونة في إدارة الأمان، تأكد من أن جميع أجهزة برنامج Cisco IOS software تنفذ نموذج أمان المصادقة والتفويض والمحاسبة (AAA). يمكن أن تستخدم المصادقة والتفويض والمحاسبة (AAA) قواعد بيانات محلية و RADIUS و TACACS+. راجع قسم تكوين مصادقة TACACS+ للحصول على مزيد من المعلومات.

خدمات أمان AAA

نظرة عامة على تشغيل AAA

عناصر التحكم في الوصول التي لديها إذن للوصول إلى المحول والخدمات التي يمكن لهؤلاء المستخدمين إستخدامها. توفر خدمات أمان شبكة AAA الإطار الأساسي لإعداد التحكم في الوصول على المحول لديك.

يصف هذا القسم الجوانب المختلفة ل AAA بالتفصيل:

- المصادقة—تقوم هذه العملية بالتحقق من صحة هوية المستخدم النهائي أو الجهاز المزعومة. أولا، تم تحديد الطرق المختلفة التي يمكن إستخدامها لمصادقة المستخدم. تحدد هذه الطرق نوع المصادقة المراد تنفيذها (على سبيل المثال، TACACS+ أو RADIUS). كما يتم تعريف التسلسل الذي تحاول فيه أساليب المصادقة هذه. ثم يتم تطبيق الطرق على الواجهات المناسبة، والتي تنشط المصادقة.
- التفويض- تمنح هذه العملية حقوق الوصول لمستخدم أو لمجموعات من المستخدمين أو لنظام أو عملية. يمكن لعملية AAA تنفيذ تفويض أو تفويض لمرة واحدة لكل مهمة. تحدد العملية السمات (على خادم AAA) على ما يملك المستخدم الإذن بتنفيذه. عندما يحاول المستخدم بدء خدمة، يستعلم المحول عن خادم AAA ويطلب إذنا لتخويل المستخدم. إذا وافق خادم AAA، يتم تخويل المستخدم. إذا لم يوافق خادم AAA، فلن يحصل المستخدم على إذن لتنفيذ تلك الخدمة. يمكنك إستخدام هذه العملية لتحديد إمكانية تنفيذ بعض المستخدمين لأوامر معينة فقط.
- المحاسبة - تتيح لك هذه العملية تعقب الخدمات التي يصل إليها المستخدمون ومقدار موارد الشبكة التي يستهلكها المستخدمون. عند تمكين المحاسبة، يقوم المحول بالإعلام عن نشاط المستخدم إلى خادم AAA في شكل سجلات محاسبة. وتتضمن أمثلة نشاط المستخدم الذي تم الإبلاغ عنه وقت جلسة العمل ووقت البدء والتوقف. وبعد ذلك، يمكن تحليل هذا النشاط لأغراض الإدارة أو إعداد الفواتير.

على الرغم من أن المصادقة والتفويض والمحاسبة (AAA) هي الطريقة الأساسية الموصى بها للتحكم في الوصول، إلا أن برنامج Cisco IOS يوفر ميزات إضافية للتحكم في الوصول البسيط الموجود خارج نطاق المصادقة والتفويض والمحاسبة (AAA). وتتضمن هذه الميزات الإضافية ما يلي:

- مصادقة اسم المستخدم المحلي
- مصادقة كلمة مرور السطر
- تمكين مصادقة كلمة المرور

ولكن هذه الميزات لا توفر نفس درجة التحكم في الوصول التي يمكن الحصول عليها من المصادقة والتفويض والمحاسبة (AAA).

لفهم AAA بشكل أفضل، ارجع إلى هذه المستندات:

- المصادقة والتفويض والمحاسبة (AAA)
- تكوين المصادقة والتفويض والمحاسبة (AAA) الأساسي على خادم الوصول
- مقارنة TACACS+ و RADIUS

لا تشير هذه المستندات بالضرورة إلى المحولات. ولكن مفاهيم المصادقة والتفويض والمحاسبة (AAA) التي تصفها المستندات تنطبق على المحولات.

TACACS+

الغرض

بشكل افتراضي، تكون كلمات مرور الوضع غير ذي الامتيازات وذات الامتيازات عامة. تنطبق كلمات المرور هذه على كل مستخدم يصل إلى المحول أو الموجه، إما من منفذ وحدة التحكم أو من خلال جلسة عمل على برنامج Telnet عبر الشبكة. يستغرق تنفيذ كلمات المرور هذه على أجهزة الشبكة الوقت وغير المركزي. كما يمكنك أن تواجه صعوبة في تنفيذ قيود الوصول باستخدام قوائم التحكم في الوصول (ACL) التي يمكن أن تكون عرضة لأخطاء التكوين. للتغلب على هذه المشكلات، اتبع نهجا مركزيا عند تكوين أسماء المستخدمين وكلمات المرور وسياسات الوصول على خادم مركزي. يمكن أن يكون هذا الخادم خادم التحكم في الوصول الآمن (ACS) من Cisco أو أي خادم من إنتاج جهات خارجية. تم تكوين الأجهزة لاستخدام قواعد البيانات المركزية هذه لوظائف AAA. في هذه الحالة، تكون الأجهزة هي محولات برنامج Cisco IOS Software. يمكن أن يكون البروتوكول المستخدم بين الأجهزة والخادم المركزي:

- TACACS+
- RADIUS
- Kerberos

TACACS+ هو نشر شائع في شبكات Cisco وهو بؤرة هذا القسم. يوفر TACACS+ الميزات التالية:

- المصادقة—العملية التي تعرف المستخدم وتتحقق منه. يمكن إستخدام العديد من الطرق لمصادقة مستخدم ما. ولكن الطريقة الأكثر شيوعا تتضمن مزيجا من اسم المستخدم وكلمة المرور.
- التفويض—عندما يحاول المستخدم تنفيذ أمر، يمكن للمحول التحقق من الأمر مع خادم TACACS+ لتحديد ما إذا كان المستخدم قد حصل على إذن باستخدام هذا الأمر المعين.
- المحاسبة - تسجل هذه العملية ما يقوم به المستخدم أو قام به على الجهاز.

ارجع إلى مقارنة TACACS+ و RADIUS للمقارنة بين TACACS+ و RADIUS.

نظرة عامة على العمليات

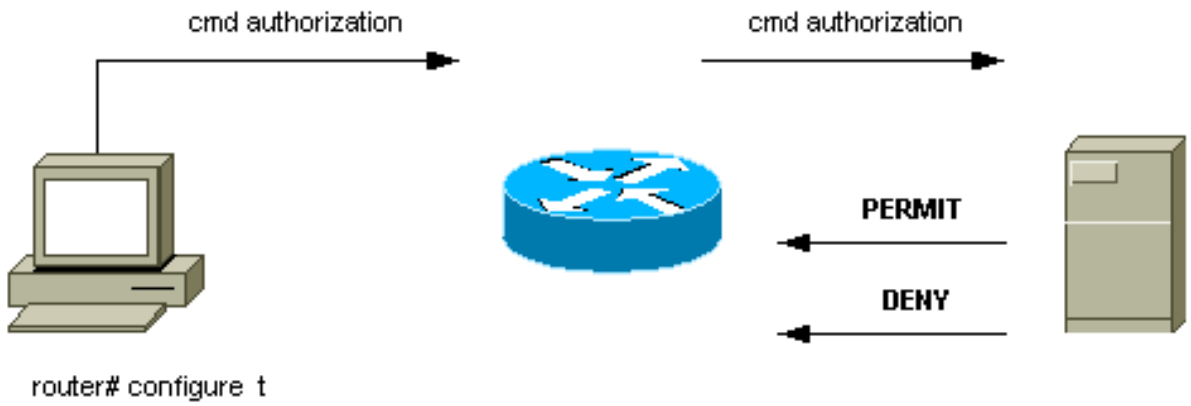
يعمل بروتوكول TACACS+ على إعادة توجيه أسماء المستخدمين وكلمات المرور إلى الخادم المركزي. يتم تشفير المعلومات عبر الشبكة باستخدام تجزئة MD5 أحادية الإتجاه. راجع RFC 1321 للحصول على مزيد من المعلومات. يستخدم TACACS+ منفذ TCP رقم 49 كبروتوكول نقل، والذي يقدم هذه الميزات عبر بروتوكول UDP:

ملاحظة: يستخدم RADIUS بروتوكول UDP.

- النقل الموجه للاتصال
- إقرار منفصل باستلام طلب (إقرار TCP [ACK])، بغض النظر عن كيفية تحميل آلية المصادقة النهائية
- الإشارة الفورية إلى تعطل الخادم (إعادة ضبط حزم [RST])

أثناء جلسة العمل، إذا كان التحقق من التفويض الإضافي ضروريا، يتحقق المحول من خلال TACACS+ لتحديد ما إذا كان المستخدم قد تم منحه إذنا لاستخدام أمر معين. توفر هذه الخطوة تحكم أكبر على الأوامر التي يمكن تنفيذها على المحول وتوفر الفصل من آلية المصادقة. باستخدام محاسبة الأوامر، يمكنك تدقيق الأوامر التي قام مستخدم معين بإصدارها بينما يتم إرفاق المستخدم بجهاز شبكة معين.

يوضح هذا المخطط عملية التخويل المعنية:



عندما يقوم المستخدم بالمصادقة على جهاز شبكة باستخدام TACACS+ في محاولة تسجيل دخول ASCII بسيطة، تحدث هذه العملية عادة:

- عند تأسيس الاتصال، يتصل المحول بالجهاز المساعد TACACS+ للحصول على موجه اسم مستخدم. يعرض المفتاح بعد ذلك الإيعاز للمستخدم. يدخل المستخدم اسم مستخدم، ويتصل المحول بالجهاز المساعد

TACACS+ للحصول على مطالبة كلمة مرور. يعرض المفتاح الكلمة رسالة حث للمستخدم، الذي يدخل كلمة مرور أن يكون أيضا أرسلت إلى ال TACACS+ daemon.

- يستقبل جهاز الشبكة أخيرا أحد هذه الاستجابات من برنامج TACACS+ الخدمي:— تتم مصادقة المستخدم ويمكن بدء الخدمة. في حالة تكوين جهاز الشبكة بحيث يتطلب تخويل، يبدأ التخويل في هذا الوقت.—فشل المستخدم في المصادقة. يتم رفض وصول المستخدم أو مطالبته بإعادة محاولة تسلسل تسجيل الدخول. تعتمد النتيجة على برنامج TACACS+.- حدث خطأ في وقت ما أثناء المصادقة. يمكن أن يكون الخطأ إما في الأداة المساعدة أو في اتصال الشبكة بين الأداة المساعدة والمحول. في حالة تلقي إستجابة ، يحاول جهاز الشبكة عادة إستخدام طريقة بديلة لمصادقة المستخدم.—تتم مطالبة المستخدم بمعلومات مصادقة إضافية.
- يجب على المستخدمين إكمال مصادقة TACACS+ بنجاح أولا قبل المتابعة إلى تفويض TACACS+.
- إذا كان تفويض TACACS+ مطلوبا، فسيتم الاتصال بالجهاز الخفي TACACS+ مرة أخرى. يرجع البرنامج الخفي TACACS+ إستجابة تفويض أو . إذا تم إرجاع إستجابة ، فستتضمن الاستجابة بيانات في شكل سمات يتم إستخدامها لتوجيه جلسة عمل EXEC أو لذلك المستخدم. يحدد هذا الأمر الأوامر التي يمكن للمستخدم الوصول إليها.

خطوات تكوين AAA الأساسية

يكون تكوين المصادقة والتفويض والمحاسبة (AAA) بسيطا نسبيا بعد فهمك للعملية الأساسية. لتكوين الأمان على موجه Cisco أو خادم الوصول باستخدام AAA، قم بتنفيذ الخطوات التالية:

1. لتمكين المصادقة والتفويض والمحاسبة (AAA)، قم بإصدار أمر التكوين العام **aaa new-model**.
```
Switch(config)#aaa new-model
```

تلميح: احفظ التكوين الخاص بك قبل تكوين أوامر AAA الخاصة بك. قم بحفظ التكوين مرة أخرى فقط بعد إكمال جميع تكوينات AAA لديك واقتناعك بأن التكوين يعمل بشكل صحيح. بعد ذلك، يمكنك إعادة تحميل المحول من أجل الاسترداد من عمليات الإغلاق غير المتوقعة (قبل حفظ التكوين)، إذا لزم الأمر.

2. إذا قررت إستخدام خادم أمان منفصل، فقم بتكوين معلمات بروتوكول الأمان مثل RADIUS أو TACACS+ أو Kerberos.
3. أستخدم الأمر **المصادقة والتفويض والمحاسبة (AAA)** لتحديد قوائم الطرق للمصادقة.
4. أستخدم الأمر **login authentication** لتطبيق قوائم الطرق على واجهة أو خط معين.
5. قم بإصدار الأمر **تفويض المصادقة والتفويض والمحاسبة (AAA)** الاختياري لتكوين التفويض.
6. قم بإصدار الأمر محاسبة **AAA** الاختيارية لتكوين المحاسبة.
7. قم بتكوين خادم AAA الخارجي لمعالجة طلبات المصادقة والتفويض من المحول.**ملاحظة:** ارجع إلى وثائق خادم AAA للحصول على مزيد من المعلومات.

تكوين مصادقة TACACS+

قم بإجراء هذه الخطوات لتكوين مصادقة TACACS+:

1. قم بإصدار الأمر **aaa new-model** في وضع التكوين العام لتمكين AAA على المحول.
2. قم بتحديد خادم TACACS+ والمفتاح المقترن.يستخدم هذا المفتاح لتشفير حركة مرور البيانات بين خادم TACACS+ والمحول. في الأمر **tacacs-server host 1.1.1.1 key mysecretkey**، يكون خادم TACACS+ في عنوان IP 1.1.1.1، ومفتاح التشفير هو mysecretkey. للتحقق من إمكانية وصول المحول إلى خادم TACACS+، ابدأ إختبار اتصال بروتوكول رسائل التحكم في الإنترنت (ICMP) من المحول.
3. قم بتحديد قائمة طرق.تحدد قائمة الطرق تسلسل آليات المصادقة لمحاولة الحصول على خدمات مختلفة. يمكن للخدمات المختلفة أن تكون، على سبيل المثال:تمكينتسجيل الدخول (للوصول إلى VTY/Telnet)**ملاحظة:** راجع قسم ميزات الأمان الأساسية في هذا المستند للحصول على معلومات حول الوصول إلى برنامج Telnet/vty.وحدة التحكميتناول هذا المثال **تسجيل الدخول** فقط. يجب تطبيق قائمة الطرق على الواجهات/الأسطر:

```
Switch(config)#aaa authentication login METHOD-LIST-LOGIN group tacacs+ line
Switch(config)#line vty 0 4
Switch(config-line)#login authentication METHOD-LIST-LOGIN
Switch(config-line)#password hard_to_guess
```

في هذا التكوين، يستخدم الأمر **مصادقة تسجيل الدخول** إلى المصادقة والتفويض والمحاسبة (AAA) اسم القائمة المركب METHOD-LIST-LOGIN ويستخدم الأسلوب TACACS+ قبل أن يستخدم سطر الطريقة. تتم مصادقة المستخدمين باستخدام خادم TACACS+ كالطريقة الأولى. إذا لم يستجب خادم TACACS+ أو يرسل رسالة خطأ، فسيتم إستخدام كلمة المرور التي تم تكوينها على السطر كطريقة ثانية. ولكن إذا رفض خادم TACACS+ المستخدم ورد برسالة رفض، فإن المصادقة والتفويض والمحاسبة (AAA) تعتبر الحركة ناجحة ولا تستخدم الطريقة الثانية.**ملاحظة:** لا يكتمل التكوين حتى تقوم بتطبيق القائمة (method-list-login) على سطر vty. قم بإصدار الأمر **login authentication method-list-login** في وضع تكوين الخط، كما يوضح المثال.**ملاحظة:** يقوم المثال بإنشاء باب خلفي عندما يكون خادم TACACS+ غير متوفر. يمكن لمسؤولي الأمان أو قد لا يمكنهم قبول تنفيذ الباب الخلفي. تأكد من أن قرار تنفيذ مثل تلك الأعمال السرية يتماشى مع السياسات الأمنية للموقع.

تكوين مصادقة RADIUS

تكوين RADIUS مطابق تقريبا لتكوين TACACS+. ما عليك سوى إستبدال كلمة RADIUS ب TACACS في التكوين. هذا عينة تشكيل RADIUS للوصول إلى منفذ COM:

```
Switch(config)#aaa new-model
Switch(config)#radius-server host 1.1.1.1 key mysecretkey
Switch(config)#aaa authentication login METHOD-LIST-LOGIN group radius line
Switch(config)#line con 0
Switch(config-line)#login authentication METHOD-LIST-LOGIN
Switch(config-line)#password hard_to_guess
```

شعارات تسجيل الدخول

قم بإنشاء لافتات الأجهزة المناسبة التي تذكر بشكل خاص الإجراءات التي يتم إتخاذها عند الوصول غير المصرح به. عدم الإعلان عن اسم الموقع أو معلومات الشبكة للمستخدمين غير المصرح لهم. وتوفر اللافتات سبل الانتصاف في حالة تعرض جهاز ما للخطر وقبض على مرتكب الجريمة. أصدرت هذا أمر in order to خلقت login راية:

```
Switch(config)#banner motd ^C
*** Unauthorized Access Prohibited ***
C^
```

الأمان المادي

تأكد من أن التفويض المناسب ضروري للوصول المادي إلى الأجهزة. احتفظ بالجهاز في مساحة مضبوطة (مغلقة). لضمان إستمرار تشغيل الشبكة وعدم تأثرها بالعوامل الضارة أو العوامل البيئية، تأكد من أن جميع المعدات:

- مصدر طاقة غير قابل للانقطاع (UPS) مناسب مزود بمصادر إحتياطية حيثما أمكن
- التحكم في درجة الحرارة (تكييف الهواء)

تذكر أنه إذا قام شخص ذو نية خبيثة بانتهاك الوصول المادي، فإن العرقلة عبر إسترداد كلمة المرور أو وسائل أخرى يكون أكثر إحتمالا.

تكوين الإدارة

مخططات الشبكة

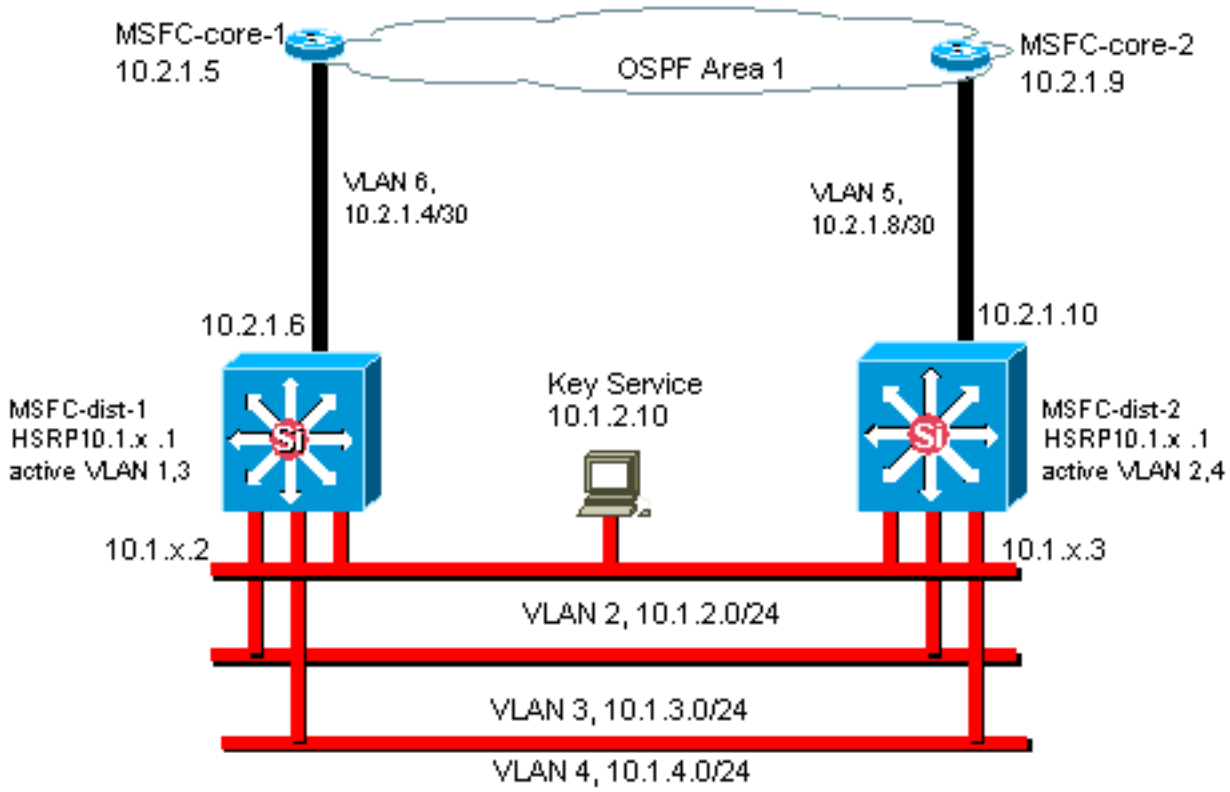
الغرض

تعد مخططات الشبكة الواضحة جزءا أساسيا من عمليات الشبكة. تصبح الرسوم البيانية بالغة الأهمية أثناء أستكشاف المشكلات وحلها، وهي الوسيلة الوحيدة الأكثر أهمية لإيصال المعلومات أثناء التصعيد إلى البائعين والشركاء أثناء انقطاع العمل. لا تستخف بالإعداد والاستعداد وإمكانية الوصول التي توفرها مخططات الشبكة.

توصية

هذه الأنواع الثلاثة من الرسوم البيانية ضرورية:

- **الرسم التخطيطي العام** — حتى بالنسبة لأكبر الشبكات، يعد الرسم التخطيطي الذي يوضح الاتصال المادي أو المنطقي من نهاية إلى نهاية أمرا مهما. غالبا، المؤسسات التي قامت بتنفيذ مستند تصميم هرمي كل طبقة على حدة. عندما تقوم بالتخطيط وحل المشكلة، فالمهم هو معرفة جيدة لكيفية إرتباط المجالات ببعضها البعض.
- **الرسم التخطيطي المادي**— يوضح هذا المخطط جميع أجهزة وكابلات المحولات والموجهات. تأكد من أن الرسم التخطيطي يلصق كل من هذه الجوانب:جذوعروابطالسرعاتمجموعات القنواتأرقام المنافذمشقوقأنواع الهيكلالبرنامجمجالات VTPالجسر الرئيسيأولوية الجسر الرئيسي للنسخ الاحتياطيعنوان MACالمنافذ المحظورة لكل شبكة VLANللحصول على وضوح أفضل، قم بتوصيل الأجهزة الداخلية مثل موجه Catalyst 6500/6000 MSFC كموجه على عصا يتم توصيلها عبر خط اتصال.
- **الرسم التخطيطي المنطقي**— يعرض هذا المخطط وظائف الطبقة 3 فقط، وهو ما يعني أنه يعرض الموجهات ككائنات وشبكات VLAN كأجزاء إيثرنت. تأكد من أن الرسم التخطيطي يسمي هذه الجوانب:عناوين IPالشبكات الفرعيةعنونة ثانويةHSRP نشطة ومستعدةالوصول إلى طبقات التوزيع الأساسيةمعلومات التوجيه



واجهة إدارة المحول وشبكة VLAN الأصلية

الغرض

يصف هذا قسم السمة ومشاكل المحتملة لاستخدام من التقصير VLAN 1. يغطي هذا قسم أيضا مشكلة ممكن عندما يركض أنت إدارة حركة مرور إلى المفتاح في ال نفسه VLAN بما أن مستعمل حركة مرور على 6000/6500 sery مفتاح.

تستخدم المعالجات الموجودة على Supervisor Engines (محركات المشرف) و MSFCs ل the Catalyst 6500/6000 series الشبكة المحلية الظاهرية (VLAN) رقم 1 لعدد من بروتوكولات التحكم والإدارة. الأمثلة تتضمن:

- بروتوكولات التحكم في المحول:وحدات بيانات بروتوكول الجسر (BPDUs) لبروتوكول STPVTPDTPCDP
- بروتوكولات الإدارة:SNMPTelnetبروتوكول طبقة الأمان (Syslog(SSH

عندما ال VLAN يكون استعملت بهذه الطريقة، هو يشار إليه بما أن ال VLAN أهلي طبيعي. التقصير مفتاح يثبت تشكيل VLAN 1 بما أن التقصير VLAN أهلي طبيعي على المادة حفازة شنطة ميناء. أنت يستطيع تركت VLAN 1 بما أن ال VLAN أهلي طبيعي. ولكن تذكر أن أي محولات تشغل برنامج Cisco IOS System في شبكتك تضع جميع الواجهات التي يتم تكوينها كمنافذ محول من الطبقة 2 للوصول إلى المنافذ في شبكة VLAN 1 بشكل افتراضي. غالبا، يستخدم محول في مكان ما في الشبكة شبكة VLAN 1 كشبكة VLAN لحركة مرور المستخدم.

المخاوف الرئيسية مع إستخدام شبكة VLAN 1 هي أن، بشكل عام، المشرف محرك NMP لا يحتاج أن يقاطع بقسم كبير من البث المتعدد أن محطة النهاية تولد. تميل تطبيقات البث المتعدد بشكل خاص إلى إرسال الكثير من البيانات بين الخوادم والعملاء. لا يحتاج Supervisor Engine (محرك المشرف) إلى رؤية هذه البيانات. إذا كانت الموارد أو المخازن المؤقتة من المشرف محرك يشغلون بالكامل بما أن المشرف محرك يستمع إلى حركة مرور غير ضرورية، المشرف محرك يستطيع فشلت أن يرى إدارة ربط أن يستطيع سببت يجسر - شجرة أنشوطة أو EtherChannel إخفاق (في أسوأ سيناريو).

يمكن أن يمنحك الأمر show interfaces *interface_type slot*/*port* counters *والأمر* show ip traffic *بعض الإشارة إلى:*

- نسبة البث إلى حركة مرور البث الأحادي
- نسبة حركة مرور IP إلى غير IP (والتي لا يتم رؤيتها عادة في شبكات VLAN الخاصة بالإدارة)

VLAN 1 علامات وتعالج معظم حركة مرور مستوى التحكم. VLAN 1 مكنت على كل شنطة افتراضيا. مع شبكات المجمعات الأكبر، أنت تحتاج أن يكون حريصا من القطر من ال VLAN 1 STP مجال. يمكن أن يؤثر عدم الاستقرار في جزء واحد من الشبكة على شبكة VLAN 1 ويمكن أن يؤثر على إستقرار مستوى التحكم واستقرار STP لجميع الشبكات المحلية الظاهرية (VLANs) الأخرى. أنت يستطيع حددت ال VLAN 1 بث من مستعمل معطيات والتشغيل من STP على قارن. ببساطة لا يشكل ال VLAN على الشنطة قارن.

لا يوقف هذا تشكيل النقل من تحكم ربط من مفتاح إلى مفتاح في VLAN 1، بما أن مع شبكة محلل. ولكن لا يتم إعادة توجيه أي بيانات، ولا يتم تشغيل بروتوكول الشجرة المتفرعة (STP) عبر هذا الارتباط. لذلك، أنت يستطيع استعملت هذا أسلوب أن يفصل VLAN 1 إلى أصغر إخفاق مجال.

ملاحظة: أنت يستطيع لا يمسح VLAN 1 من شنطة إلى مادة حفازة 2900xl/3500xlS.

حتى إذا كنت حريصا على تقييد شبكات VLAN الخاصة بالمستخدم إلى مجالات محول صغيرة نسبيا وما يقابل ذلك من حدود صغيرة للفشل/الطبقة 3، لا يزال بعض العملاء يستسلمون لإغراء معالجة شبكة VLAN الخاصة بالإدارة بشكل مختلف. يحاول هؤلاء العملاء تغطية الشبكة بالكامل باستخدام شبكة فرعية واحدة للإدارة. لا يوجد سبب فني لأن تطبيق NMS المركزي يجب أن يكون متجاورا مع الأجهزة التي يديرها التطبيق، كما أن هذا الأمر لا يعد وسيطة أمان مؤهلة. قصر قطر إدارة VLANs إلى ال نفسه يوجه مجال بنية بما أن أن المستعمل VLANs. اعتبر الإدارة خارج النطاق و/أو دعم بروتوكول طبقة الأمان (SSH) طريقة لزيادة أمان إدارة الشبكة.

خيارات أخرى

هناك اعتبارات تصميم لتوصيات Cisco هذه في بعض المخططات. على سبيل المثال، يعد التصميم متعدد الطبقات المرغوب فيه والشائع من Cisco أحد التصميمات التي تتجنب إستخدام شجرة متفرعة نشطة. بهذه الطريقة، يدعو التصميم إلى تقييد كل شبكة IP فرعية/شبكة VLAN إلى محول طبقة وصول واحدة (أو مجموعة من المحولات). في هذه التصميمات، لا يمكن تكوين أي توصيل حتى طبقة الوصول.

هل تقوم بإنشاء شبكة VLAN إدارة منفصلة ويمكن trunking لنقلها بين طبقة الوصول من الطبقة 2 وطبقات التوزيع من الطبقة 3؟ لا توجد إجابة سهلة على هذا السؤال. ضع في الاعتبار هذين الخيارين لمراجعة التصميم مع مهندس Cisco الذي تتعامل معه:

- **خيار 1**— شنطة إثنان أو ثلاثة VLANs فريد من طبقة التوزيع إلى كل مفتاح طبقة الوصول. يسمح هذا تشكيل ل بيانات VLAN، صوت VLAN، وإدارة VLAN، ومع ذلك يتلقى الفائدة أن STP يكون غير نشط. خطوة تشكيل إضافي ضروري in order to أخلت VLAN 1 من شنطة. في هذا الحل، هناك أيضا نقاط تصميم يجب مراعاتها لتجنب حركة مرور البيانات الموجهة بشكل مؤقت أثناء إسترداد الأعطال. أستخدم بروتوكول STP PortFast لشبكات الاتصال (في المستقبل) أو مزامنة الحالة التلقائية لشبكة VLAN مع إعادة توجيه بروتوكول الشجرة المتفرعة (STP).
- **خيار 2**- VLAN وحيد للبيانات والإدارة يستطيع كنت مقبول. إذا كنت تريد الاحتفاظ بواجهة sc0 منفصلة عن بيانات المستخدم، فإن أجهزة المحول الأحدث تجعل هذا السيناريو أقل من مشكلة ما كان عليه سابقا. يوفر الجهاز الأحدث ما يلي:وحدات معالجة مركزية (CPU) أكثر فعالية وعناصر تحكم مقيدة لمعدل مستوى التحكمتصميم بمجالات بث صغيرة نسبيا كما ينادي به التصميم متعدد الطبقاتفحصت in order to اتخذت قرار نهائي، البث حركة مرور profile ل ال VLAN وناقشت القدرات من المفتاح جهاز مع cisco مهندس ك. إذا كانت شبكة VLAN الإدارية تحتوي على جميع المستخدمين على محول طبقة الوصول هذا، فاستخدم عوامل تصفية إدخال IP لتأمين المحول من المستخدمين، وفقا لقسم ميزات أمان برنامج Cisco IOS software.

توصية واجهة إدارة Cisco وشبكة VLAN الأصلية

واجهة الإدارة

يمنحك برنامج Cisco IOS System خيار تكوين الواجهات كواجهات الطبقة 3 أو كمنافذ محول من الطبقة 2 في شبكة VLAN. عندما يستعمل أنت **ال switchport** أمر في cisco ios برمجية، كل مفتاح ميناء ينفذ في VLAN 1 افتراضيا. لذلك، ما لم يشكل أنت خلاف ذلك، مستعمل معطيات يستطيع أيضا تواجدت افتراضيا على VLAN 1.

جعلت الإدارة VLAN VLAN آخر من VLAN 1. أبق كل بيانات مستعمل خارج الإدارة VLAN. بدلا من ذلك، قم بتكوين واجهة loopback0 كواجهة إدارة على كل محول.

ملاحظة: إذا كنت تستخدم بروتوكول OSPF، فإن ذلك يصبح أيضا معرف موجه OSPF.

تأكد من أن واجهة الاسترجاع تحتوي على قناع شبكة فرعية 32-بت، وشكلت واجهة الاسترجاع كواجهة نقية للطبقة 3 على المحول. وفيما يلي مثال على هذا:

```
Switch(config)#interface loopback 0
Switch(config-if)#ip address 10.x.x.x 255.255.255.255
Switch(config-if)#end
#Switch
```

شبكة VLAN الأصلية

شكلت ال VLAN أهلي طبيعي أن يكون واضح VLAN وهمي أن لا يمكن على المسحاج تخديد. cisco يوصي VLAN 999 في الماضي، غير أن الخيار يكون تعسفي بحت.

أصدرت هذا قارن أمر in order to أسست VLAN كأهلي طبيعي (تقصير) ل 802.1Q trunking على ميناء خاص:

```
Switch(config)#interface type slot/port
Switch(config-if)#switchport trunk native vlan 999
```

للحصول على توصيات تكوين توصيل إضافية، راجع قسم بروتوكول التوصيل الديناميكي في هذا المستند.

الإدارة خارج النطاق

الغرض

يمكنك زيادة إمكانية إدارة الشبكة إذا قمت بإنشاء بنية أساسية منفصلة للإدارة حول شبكة الإنتاج. يتيح هذا الإعداد للأجهزة إمكانية الوصول إليها عن بعد، على الرغم من حركة المرور التي يتم تشغيلها أو أحداث مستوى التحكم التي تحدث. هذان النهجان نموذجيان:

- إدارة خارج النطاق باستخدام شبكة محلية (LAN) حصرية
- إدارة خارج النطاق مع خوادم طرفية

نظرة عامة على العمليات

يمكنك توفير كل موجه ومحول في الشبكة باستخدام واجهة إدارة إيثرنت خارج النطاق على شبكة VLAN للإدارة. أنت تشكل واحد إثرنيت ميناء على كل أداة في الإدارة VLAN وكبل هو خارج الإنتاج شبكة إلى منفصل يحول إدارة شبكة.

ملاحظة: تحتوي محولات Catalyst 4500/4000 على واجهة ME1 خاصة على Supervisor Engine (المحرك المشرف) يجب إستخدامها للإدارة خارج النطاق فقط وليس كمنفذ محول.

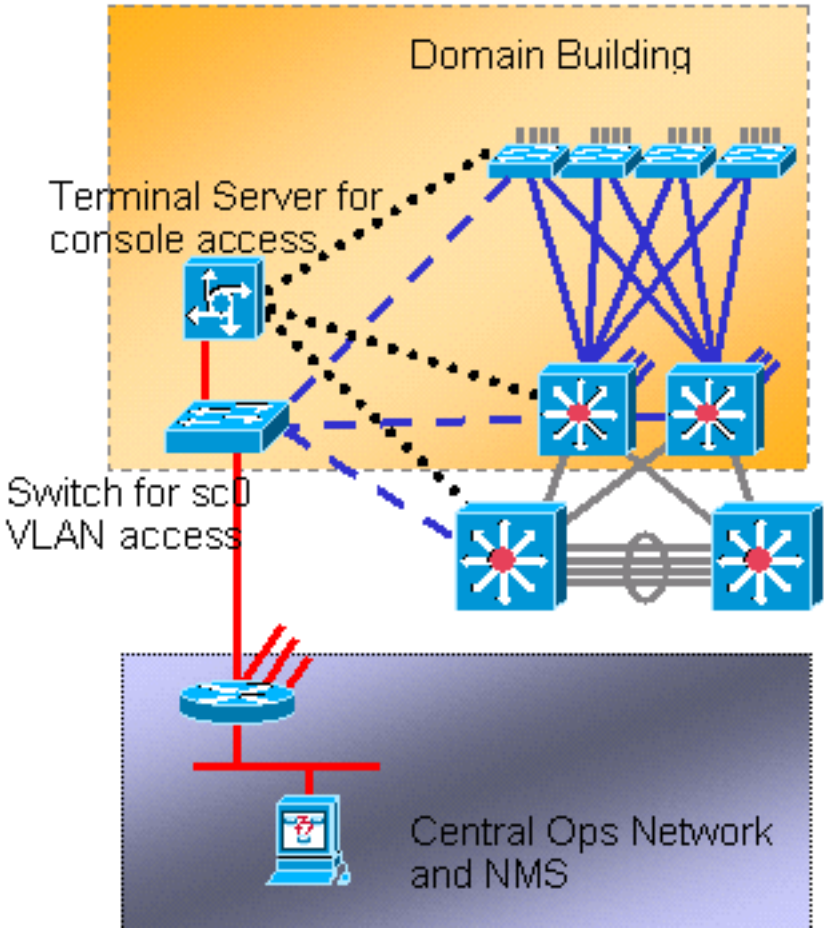
وبالإضافة إلى ذلك، يمكنك تحقيق اتصال الخادم الطرفي إذا قمت بتكوين موجه Cisco 2600 أو 3600 مع كبلات RJ-45 التسلسلية للوصول إلى منفذ وحدة التحكم لكل موجه ومحول في التخطيط. كما أن إستخدام الخادم الطرفي يجنب الحاجة إلى تكوين سيناريوهات النسخ الاحتياطي، مثل أجهزة المودم على المنافذ المساعدة لكل جهاز. يمكنك تكوين مودم واحد على المنفذ المساعد للخادم الطرفي. يوفر هذا التكوين خدمة الطلب الهاتفي للأجهزة الأخرى أثناء فشل اتصال الشبكة. راجع توصيل مودم بمنفذ وحدة التحكم في محولات Catalyst للحصول على مزيد من المعلومات.

توصية

باستخدام هذا الترتيب، يمكن إستخدام مسارين خارج النطاق لكل محول وموجه، بالإضافة إلى العديد من المسارات داخل النطاق. يتيح هذا الترتيب إمكانية إدارة عالية التوفر للشبكة. وتتمثل الفوائد فيما يلي:

- يفصل الترتيب حركة مرور الإدارة عن بيانات المستخدم.
- الإدارة عنوان في subnet منفصل، VLAN، ومفتاح للأمان.
- هناك ضمان أعلى لتقديم بيانات الإدارة أثناء حالات فشل الشبكة.
- لا يوجد شجرة متفرعة نشطة في شبكة VLAN الخاصة بالإدارة. التكرار هنا ليس أمرا بالغ الأهمية.

يوضح هذا المخطط الإدارة خارج النطاق:



تسجيل دخول النظام

الغرض

تكون رسائل syslog خاصة ب Cisco ويمكنها توفير معلومات أكثر إستجابة ودقة من SNMP القياسي. على سبيل المثال، تقوم الأنظمة الأساسية للإدارة مثل (Cisco Resource Manager Essentials (RME ومجموعة أدوات تحليل الشبكة (NATKit) بالاستخدام القوي لمعلومات syslog لتجميع تغييرات الجرد والتكوين.

توصية تكوين Cisco Syslog

تسجيل الدخول إلى النظام ممارسة عملياتية شائعة ومقبولة. يمكن أن يلتقط نظام UNIX syslog المعلومات/الأحداث على الموجه وتحليلها مثل:

- حالة الواجهة
- تنبيهات الأمان
- الظروف البيئية
- خنزير المعالجة المركزية
- أحداث أخرى

يمكن لبرنامج Cisco IOS تسجيل الدخول إلى خادم UNIX syslog. تنسيق Cisco UNIX syslog متوافق مع الإصدار 4.3 UNIX Berkeley Standard Distribution (BSD). أستخدم إعدادات سجل برنامج Cisco IOS software التالية:

- **لا توجد وحدة تحكم** في **التسجيل** — يتم إرسال جميع رسائل النظام إلى وحدة تحكم النظام بشكل افتراضي. تسجيل وحدة التحكم مهمة ذات أولوية عالية في برنامج Cisco IOS software. تم تصميم هذه الوظيفة في المقام الأول لتوفير رسائل الخطأ إلى مشغل النظام قبل فشل النظام. قم بتعطيل تسجيل وحدة التحكم في

جميع تكوينات الجهاز لتجنب الحالة التي يمكن فيها للموجه/المحول أن يعلق بينما ينتظر الجهاز إستجابة من وحدة طرفية. ولكن رسائل وحدة التحكم يمكن أن تكون مفيدة أثناء عزل المشكلات. في هذه الأمثلة، قم بتمكين تسجيل وحدة التحكم. قم بإصدار الأمر **logging console level** للحصول على المستوى المطلوب لتسجيل الرسائل. مستويات التسجيل من 0 إلى 7.

- **no logging monitor**— يقوم هذا الأمر بتعطيل تسجيل خطوط المحطة الطرفية بخلاف وحدة تحكم النظام. يمكن أن يكون تسجيل الشاشة مطلوبا (باستخدام **تصحيح أخطاء شاشة التسجيل** أو خيار أمر آخر). في هذه الحالة، قم بتمكين تسجيل المراقبة على مستوى التسجيل المحدد اللازم للنشاط. راجع عنصر **no logging console** في هذه القائمة للحصول على مزيد من المعلومات حول مستويات التسجيل.
- **التسجيل المخزن مؤقتا** 16384— يلزم إضافة الأمر **logging buffered** إلى رسائل نظام السجل في المخزن المؤقت للسجل الداخلي. المخزن المؤقت للتسجيل دائري. بمجرد تعبئة المخزن المؤقت للتسجيل، يتم الكتابة فوق الإدخالات الأقدم بواسطة الإدخالات الأحدث. حجم المخزن المؤقت للتسجيل قابل للتكوين من قبل المستخدم ويتم تحديده بالبايت. يختلف حجم المخزن المؤقت للنظام حسب النظام الأساسي. 16384 هو تقصير جيد يوفر التسجيل المناسب في معظم الحالات.
- **إعلامات ملائمة التسجيل**— يوفر هذا الأمر رسائل من مستوى الإعلام (5) إلى خادم syslog المحدد. مستوى التسجيل الافتراضي لجميع الأجهزة (وحدة التحكم والشاشة والمخزن المؤقت والفخاخ) هو تصحيح الأخطاء (المستوى 7). إذا قمت بترك مستوى تسجيل الملائمة عند 7، يتم إنتاج العديد من الرسائل الخارجية التي تمثل أهمية قليلة أو لا تمثل أي أهمية على صحة الشبكة. قم بتعيين مستوى التسجيل الافتراضي للملائمات على 5.
- **محلي7 لمرافق التسجيل** — يحدد هذا الأمر مرفق/مستوى التسجيل الافتراضي لتسلسل UNIX. قم بتكوين خادم syslog الذي يستقبل هذه الرسائل لنفس المرفق/المستوى.
- **logging host**— يعمل هذا الأمر على تعيين عنوان IP لخادم تسجيل UNIX.
- **logging source-interface loopback 0**— يعمل هذا الأمر على تعيين IP SA الافتراضي لرسائل syslog. تم ترميز SA للتسجيل ترميزا ثابتا لتسهيل تعريف المضيف الذي أرسل الرسالة.
- **تصحيح أخطاء الإعدادات المحلية لتوقيت تقديم الخدمة للطابع الزمني ل datetime show-timezone msec**—بشكل افتراضي، لا يتم ختم رسائل السجل بالوقت. يمكنك إستخدام هذا الأمر لتمكين ختم وقت رسائل السجل وتكوين ختم وقت رسائل تصحيح أخطاء النظام. يوفر ختم الوقت التوقيت النسبي للأحداث المسجلة ويحسن تصحيح الأخطاء في الوقت الفعلي. تكون هذه المعلومات مفيدة بشكل خاص عندما يرسل العملاء إخراج تصحيح الأخطاء إلى موظفي الدعم الفني للحصول على المساعدة. لتمكين ختم وقت رسائل تصحيح أخطاء النظام، أستخدم الأمر في وضع التكوين العام. يكون للأمر تأثير فقط عند تمكين تصحيح الأخطاء.

ملاحظة: بالإضافة إلى ذلك، قم بتمكين التسجيل لحالة الارتباط وحالة الحزمة على جميع واجهات جيجابت للبنية الأساسية.

يوفر برنامج Cisco IOS software آلية واحدة لتعيين المرفق ومستوى السجل لجميع رسائل النظام الموجهة إلى خادم syslog. تعيين مستوى مصيدة التسجيل إلى إعلام (المستوى 5). إذا قمت بضبط مستوى رسالة الملائمة على إعلام، فيمكنك تقليل عدد رسائل المعلومات التي يتم إعادة توجيهها إلى خادم syslog. يمكن أن يقلل هذا الإعداد بدرجة كبيرة من مقدار حركة مرور syslog على الشبكة ويمكن أن يقلل من التأثير على موارد خادم syslog.

أضفت هذا أمر إلى كل مسحاج تخديد ومفتاح أن يركض cisco ios برمجية in order to مكنت syslog رسالة:

- أوامر تكوين syslog العامة:

```
no logging console
no logging monitor
logging buffered 16384
logging trap notifications
logging facility local7
logging host-ip
logging source-interface loopback 0
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
```

- قارن syslog تشكيل أمر:

```
logging event link-status
logging event bundle-status
```

SNMP

الغرض

يمكنك إستخدام SNMP لاسترداد الإحصائيات والعدادات والجداول التي يتم تخزينها في قواعد معلومات الإدارة (MIB) الخاصة بجهاز الشبكة. يمكن أن تستخدم وحدات NMS مثل OpenView من HP المعلومات من أجل:

- إنشاء تنبيهات الوقت الحقيقي
- قياس التوفر
- إنتاج معلومات تخطيط القدرات
- المساعدة في إجراء عمليات التحقق من التكوين واستكشاف الأخطاء وإصلاحها

عملية واجهة إدارة SNMP

SNMP هو بروتوكول طبقة تطبيق يوفر تنسيق رسالة للاتصال بين مديري SNMP والوكلاء. يوفر SNMP إطارا قياسيا ولغة مشتركة لمراقبة الأجهزة وإدارتها في الشبكة.

يتكون إطار عمل SNMP من الأجزاء الثلاثة التالية:

- مدير SNMP
- وكيل SNMP
- MIB

مدير SNMP هو النظام الذي يستخدم SNMP من أجل التحكم في أنشطة مضيفي الشبكة ومراقبتها. يطلق على نظام الإدارة الأكثر شيوعا اسم NMS. يمكنك تطبيق المصطلح NMS على جهاز مخصص يتم إستخدامه لإدارة الشبكة أو التطبيقات المستخدمة على هذا الجهاز. تتوفر مجموعة متنوعة من تطبيقات إدارة الشبكة للاستخدام مع بروتوكول SNMP. تتراوح هذه التطبيقات من تطبيقات واجهة سطر الأوامر (CLI) البسيطة إلى شبكات GUI الثرية بالميزات مثل خط منتجات CiscoWorks.

يعد عميل SNMP مكون البرنامج داخل الجهاز المدار الذي يحتفظ ببيانات الجهاز ويبلغ عن هذه البيانات، حسب الضرورة، لإدارة الأنظمة. يوجد الوكيل و MIB على جهاز التوجيه (الموجه أو خادم الوصول أو المحول). لتمكين وكيل SNMP على جهاز توجيه Cisco، يجب عليك تحديد العلاقة بين المدير والوكيل.

قاعدة معلومات الإدارة (MIB) هي منطقة تخزين معلومات افتراضية لمعلومات إدارة الشبكة. تتألف قاعدة معلومات الإدارة من مجموعات من الكائنات التي تتم إدارتها. وضمن قاعدة معلومات الإدارة، توجد مجموعات من الكائنات ذات الصلة معرفة في الوحدات النمطية لقاعدة معلومات الإدارة. تتم كتابة وحدات قاعدة معلومات الإدارة (MIB) في لغة وحدة قاعدة معلومات الإدارة (MIB) لبروتوكول SNMP، كما هو محدد من خلال std 58 وRFC 2578 وRFC 2579 وRFC 2580 .

ملاحظة: يشار أيضا إلى وحدات قاعدة معلومات الإدارة (MIB) الفردية باسم قواعد معلومات الإدارة. على سبيل المثال، قاعدة معلومات الإدارة (MIB) الخاصة بمجموعة الواجهات (IF-MIB) هي وحدة قاعدة معلومات الإدارة (MIB) داخل قاعدة معلومات الإدارة (MIB) الموجودة بالنظام لديك.

يحتوي عامل SNMP على متغيرات MIB، والتي يمكن أن يطلب مدير SNMP منها عمليات الحصول على أو تعيينها أو تغييرها. يمكن للمدير الحصول على قيمة من وكيل أو تخزين قيمة في هذا الوكيل. يقوم البرنامج العميل بتجميع البيانات من قاعدة معلومات الإدارة (MIB)، وهي مستودع للمعلومات حول معلمات الجهاز وبيانات الشبكة. كما يمكن للوكيل الاستجابة لطلبات المدير للحصول على البيانات أو تعيينها.

يمكن للمدير إرسال طلبات الوكيل للحصول على قيم قاعدة معلومات الإدارة (MIB) وتعيينها. يمكن للوكيل الاستجابة لهذه الطلبات. وبغض النظر عن هذا التفاعل، يمكن للوكيل إرسال إعلامات غير مطلوبة (إختبارات أو معلومات) إلى المدير لإعلام المدير بظروف الشبكة. باستخدام بعض آليات الأمان، يمكن ل NMS إسترداد المعلومات في قواعد معلومات الإدارة (MIB) باستخدام الطلبات `get` و`next`، كما يمكن إصدار الأمر **set** لتغيير المعلمات. وبالإضافة إلى ذلك، يمكنك إعداد جهاز شبكة لإنشاء رسالة ملائمة إلى NMS للحصول على تنبيهات في الوقت الفعلي. يتم إستخدام منفذ IP UDP 161 و 162 للملائمات.

نظرة عامة على تشغيل إعلامات SNMP

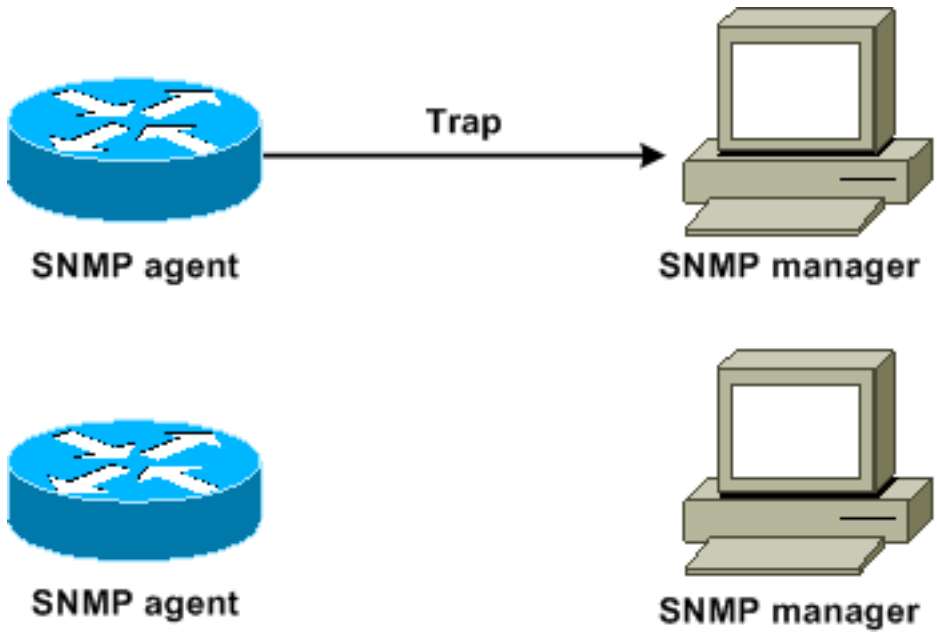
تتمثل إحدى الميزات الأساسية لبروتوكول SNMP في القدرة على إنشاء إعلامات من وكيل SNMP. لا تتطلب هذه الإعلامات طلبات ليتم إرسالها من مدير SNMP. يمكن إنشاء الإعلامات غير المرغوب فيها (غير المتزامنة) كإختبارات أو طلبات إعلام. الملائمات هي رسائل تنبه مدير SNMP إلى حالة على الشبكة. الإعلام بالطلبات (المعلومات) هي إختبارات تتضمن طلب تأكيد الاستلام من مدير SNMP. يمكن أن تشير الإعلامات إلى أحداث مهمة مثل:

- مصادقة مستخدم غير صحيحة
- إعادة التشغيل
- إغلاق اتصال
- فقدان الاتصال بالموجه المجاور
- أحداث أخرى

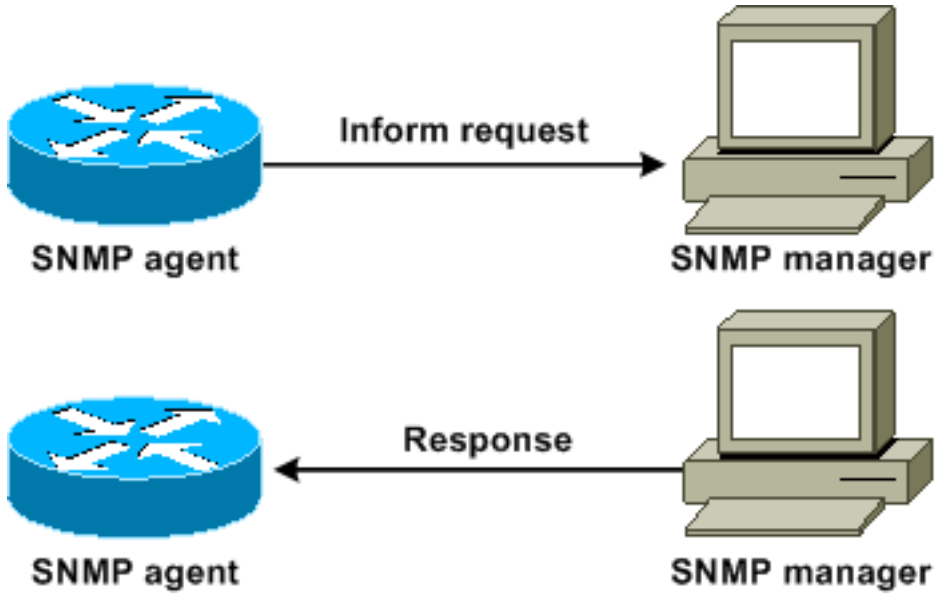
تكون الملائمات أقل موثوقية من المعلومات لأن المتلقي لا يرسل أي إقرار عندما يتلقى المتلقي مصيدة. يتعذر على المرسل تحديد ما إذا كان قد تم تلقي الملائمة أم لا. يتعرف مدير SNMP الذي يستقبل طلب إعلام على الرسالة باستخدام وحدة بيانات بروتوكول إستجابة SNMP (PDU). إذا لم يستلم المدير طلب إعلام، فلن يرسل المدير إستجابة. إذا لم يتلق المرسل أية إستجابة، فيمكن للمرسل إرسال طلب الإعلام مرة أخرى. من المرجح أن تصل المعلومات إلى الوجهة المقصودة.

ولكن غالبا ما يتم تفضيل الملائمات لأن المعلومات تستهلك المزيد من الموارد في الموجه وفي الشبكة. يتم تجاهل الملائمة بمجرد إرسالها. ولكن يجب الاحتفاظ بطلب الإعلام في الذاكرة حتى يتم تلقي الاستجابة أو انتهاء مهلة الطلب. أيضا، يتم إرسال الملائمات مرة واحدة فقط، بينما يمكن إعادة محاولة الإعلام عدة مرات. تزيد المحاولات حركة المرور وتساهم في زيادة التكاليف الإضافية على الشبكة. وبالتالي، فإن الفخاخ والطلبات المستنيرة توفر مقايضة بين الموثوقية والموارد. إذا كنت بحاجة إلى مدير SNMP لتلقي كل إعلام، فاستخدم طلبات الإعلام. ولكن إذا كانت لديك مخاوف حول حركة مرور البيانات على الشبكة أو الذاكرة الخاصة بك في الموجه ولا تحتاج إلى تلقي كل إعلام، فاستخدم الملائمات.

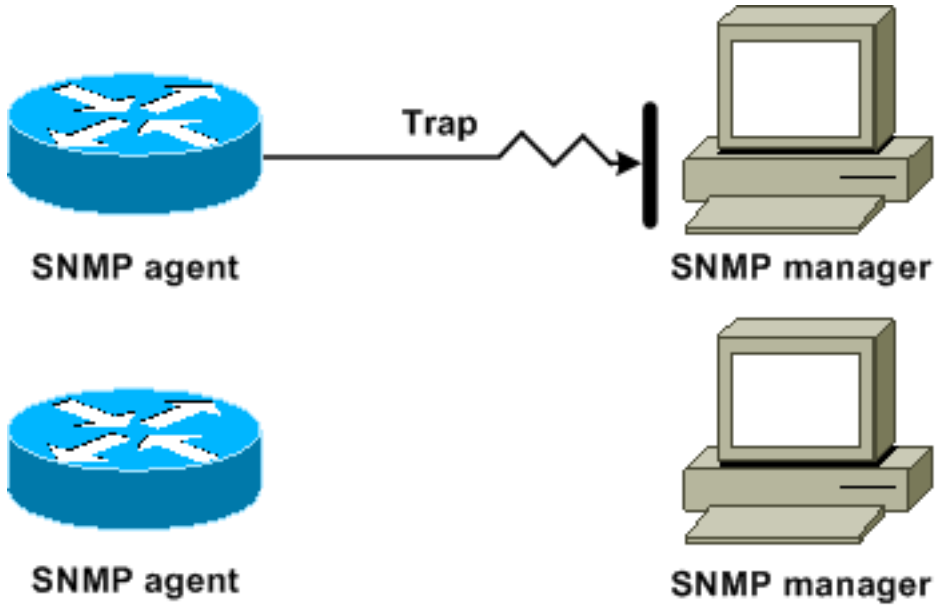
توضح هذه الرسوم البيانية الاختلافات بين الفخاخ وتقدم المعلومات حول الطلبات:



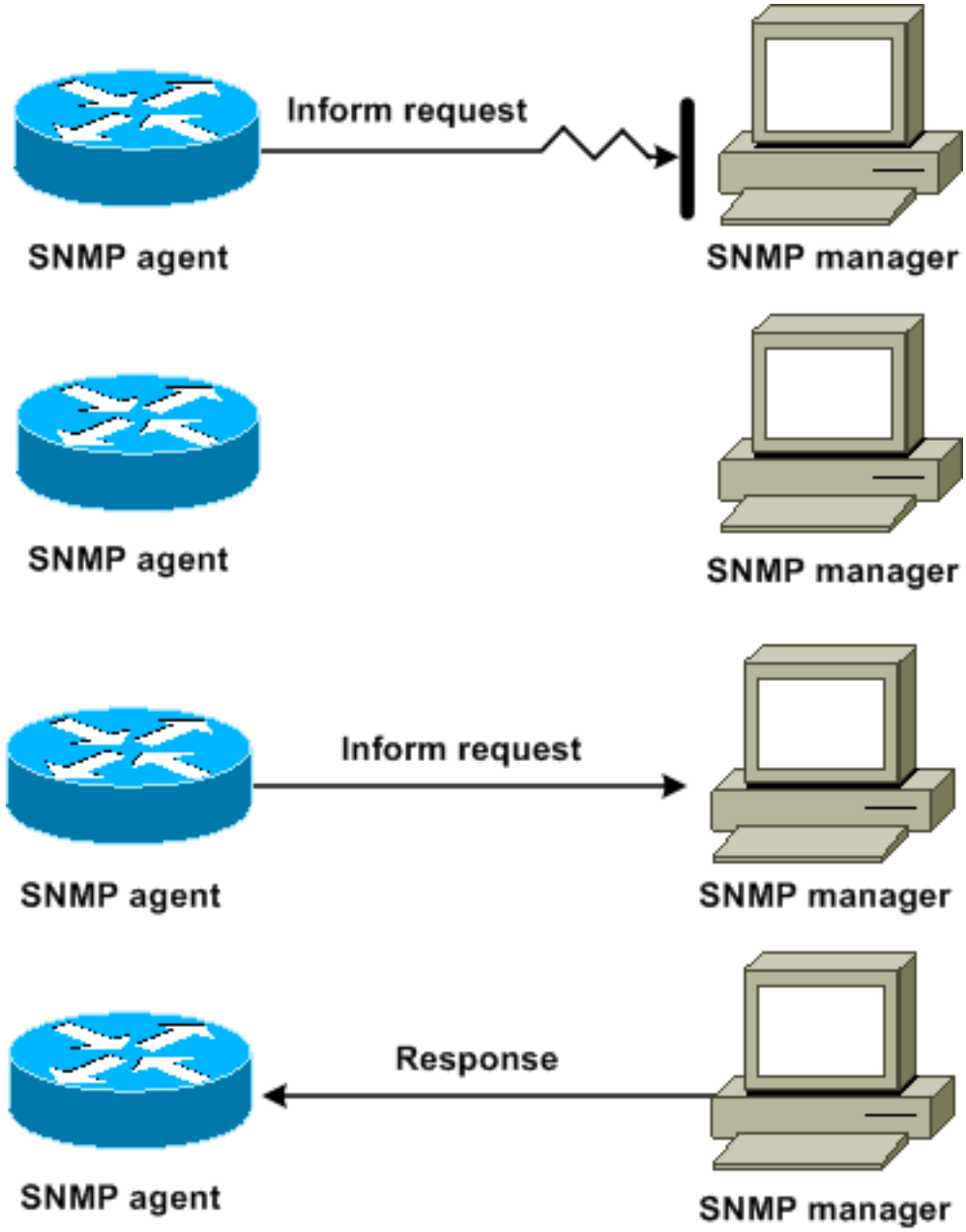
يوضح هذا المخطط كيفية إرسال موجه الوكيل بنجاح فخ إلى مدير SNMP. على الرغم من أن المدير يتلقى الملائمة، إلا أن المدير لا يرسل أي إقرار إلى الوكيل. ليس لدى العميل أي طريقة لمعرفة أن الفخ وصل إلى الوجهة.



يوضح هذا المخطط كيف يقوم موجه الوكيل بإرسال طلب إعلام بنجاح إلى المدير. عندما يستقبل المدير طلب الإعلام، يرسل المدير إستجابة إلى الوكيل. بهذه الطريقة، يعرف الوكيل أن طلب الإعلام وصل إلى الوجهة. لاحظ أنه، في هذا المثال، هناك ضعف حركة المرور. لكن الوكيل يعرف أن المدير تلقى الإخطار.



في هذا رسم بياني، يرسل الوكيل مصيدة إلى المدير، غير أن المصيدة لا تصل إلى المدير. لا يملك العميل أي طريقة لمعرفة أن الفخ لم يصل إلى الوجهة، وبالتالي لا يتم إرسال الفخ مرة أخرى. المدير لا يستلم الفخ أبدا.



في هذا الرسم التخطيطي، يرسل العميل طلب إعلام إلى المدير، ولكن طلب الإعلام لا يصل إلى المدير. نظرا لأن المدير لم يستلم طلب الإعلام، فلا يوجد رد. بعد مرور فترة من الوقت، يقوم الوكيل برد طلب الإعلام. وفي المرة الثانية، يتلقى المدير طلب الإعلام والرد عليه برد. في هذا مثال، هناك كثير حركة مرور. ولكن يصل الإعلام إلى مدير SNMP.

مرجع Cisco MIBs و RFCs

تحدد وثائق معيار RFC بشكل نموذجي وحدات قاعدة معلومات الإدارة (MIB). وتقدم وثائق مركز البحوث الحرجية إلى فرقة العمل المعنية بهندسة الإنترنت، وهي هيئة دولية معنية بالمعايير. يقوم الأفراد أو الجماعات بكتابة التقارير المرتجلة لتنظر فيها جمعية الإنترنت (ISOC) ومجتمع الإنترنت ككل. راجع الصفحة الرئيسية مجتمع الإنترنت للتعرف على عملية المعايير وأنشطة IETF. راجع الصفحة الرئيسية IETF لقراءة النص الكامل لجميع RFCs ومشروعات الإنترنت (I-DS) و STDs التي تشير إليها مستندات Cisco.

يستخدم تنفيذ SNMP من Cisco:

- تعريفات متغيرات قاعدة معلومات الإدارة (MIB) الثانية التي يصفها RFC 1213
- تعريفات إختبارات SNMP التي يصفها RFC 1215

توفر Cisco امتدادات قاعدة معلومات الإدارة الخاصة بها مع كل نظام. تتوافق قواعد معلومات الإدارة (MIB) الخاصة

بالمؤسسات من Cisco مع الإرشادات التي تصفها قواعد معلومات الإدارة (RFCs) ذات الصلة، ما لم تلاحظ الوثائق خلاف ذلك. يمكنك العثور على ملفات تعريف وحدة قاعدة معلومات الإدارة (MIB) وقائمة قواعد معلومات الإدارة (MIB) المدعومة على كل نظام أساسي من Cisco في الصفحة الرئيسية ل Cisco MIB.

إصدارات SNMP

يدعم برنامج Cisco IOS هذه الإصدارات من SNMP:

- SNMPv1 — معيار إنترنت كامل يحدده RFC 1157 . يعمل RFC 1157 على إستبدال الإصدارات السابقة التي تم نشرها باسم RFC 1067 وRFC 1098 . يرتكز الأمن على سلاسل المجتمع.
- SNMPv2c-SNMPv2c هو الإطار الإداري المستند إلى سلسلة المجتمع ل SNMPv2c .SNMPv2 (يمثل c المجتمع) هو بروتوكول إنترنت تجريبي يحدده RFC 1901 ، وRFC 1905 ، وSNMPv2c . RFC 1906 هو تحديث لعمليات البروتوكول وأنواع البيانات من SNMPv2 Classic) SNMPv2p). يستخدم SNMPv2c نموذج الأمان المستند إلى المجتمع ل SNMPv1.
- يعد SNMPv3—SNMPv3 بروتوكولا مستندا إلى المعايير قابل للتشغيل البيني يحدده RFC 2273 وRFC 2274 وRFC 2275 . يوفر SNMPv3 الوصول الآمن إلى الأجهزة باستخدام مجموعة من المصادقة وتشفير الحزم عبر الشبكة.ميزات الأمان التي يوفرها SNMPv3 هي:تكامل الرسالة—يضمن عدم التلاعب بالحزمة أثناء النقل.المصادقة—تحدد أن الرسالة من مصدر صالح.التشفير- يتعطل محتويات الحزمة، مما يمنع الاكتشاف بواسطة مصدر غير مصرح به.

يستخدم كل من SNMPv1 و SNMPv2c شكلا أمنيا مستندا إلى المجتمع. تحدد قائمة التحكم في الوصول (ACL) لعنوان IP وكلمة المرور مجتمع المديرين الذين يمكنهم الوصول إلى قاعدة معلومات الإدارة للوكيل.

يتضمن دعم SNMPv2c آلية إسترداد كميات كبيرة وإبلاغ محطات الإدارة برسائل الخطأ الأكثر تفصيلا. وتدعم آلية الاسترداد المجمع إسترداد الجداول والكميات الكبيرة من المعلومات، مما يقلل إلى أدنى حد من عدد الرحلات ذهابا وإيابا اللازمة. يتضمن دعم معالجة الأخطاء المحسن ل SNMPv2c رموز أخطاء موسعة تميز أنواع مختلفة من حالات الخطأ. يتم الإبلاغ عن هذه الشروط من خلال رمز خطأ واحد في SNMPv1. خطأ إرجاع الرموز الآن الإبلاغ عن نوع الخطأ.

يوفر SNMPv3 لكل من طرز الأمان ومستويات الأمان. نموذج الأمان هو إستراتيجية مصادقة يتم إعدادها للمستخدم والمجموعة التي يتواجد فيها المستخدم. مستوى الأمان هو مستوى الأمان المسموح به داخل نموذج الأمان. يحدد الجمع بين نموذج الأمان ومستوى الأمان آلية الأمان التي يجب إستخدامها عند معالجة حزمة SNMP.

تكوين SNMP العام

قم بإصدار هذه الأوامر على جميع محولات العميل لتمكين إدارة SNMP:

- أمر قوائم التحكم في الوصول إلى SNMP:

```
Switch(config)#access-list 98 permit ip_address
.This is the SNMP device ACL ---!
```

- أوامر SNMP العامة:

```
These are sample SNMP community strings. Switch(config)#snmp-server community RO- ---!
                                                    community ro 98
                                          snmp-server community RW-community rw 98
                                    (snmp-server contact Glen Rahn (Home Number
                                                snmp-server location text
```

توصية ملائمة SNMP

SNMP هو الأساس لإدارة الشبكة، ويتم تمكينه واستخدامه على جميع الشبكات.

يمكن أن يتصل عميل SNMP بالعديد من المدراء. ولهذا السبب، يمكنك تكوين البرنامج لدعم الاتصالات باستخدام محطة إدارة واحدة باستخدام SNMPv1، ومحطة إدارة أخرى باستخدام SNMPv2. لا يزال معظم العملاء و NMSs يستخدمون SNMPv1 و SNMPv2c لأن دعم جهاز شبكة SNMPv3 في أنظمة NMS الأساسية متأخر إلى حد ما.

قم بتمكين ملائمات SNMP لجميع الميزات قيد الاستخدام. أنت يستطيع أعجزت آخر سمة، إن يريد أنت. بعد أن تقوم بتمكين الملائمة، يمكنك إصدار الأمر **test snmp** وإعداد المعالجة المناسبة على NMS للخطأ. وتتضمن أمثلة هذه المعالجة تنبيه جهاز النداء أو منبثق.

كل الملائمات معأق افتراضيا. قم بتمكين جميع الملائمات على المحولات الأساسية، كما يوضح المثال التالي:

```
Switch(config)#snmp trap enable
Switch(config)#snmp-server trap-source loopback0
```

قم أيضا بتمكين ملائمات المنافذ للمنافذ الرئيسية، مثل روابط البنية الأساسية للموجهات والمحولات ومنافذ الخادم الأساسية. التمكين غير ضروري للمنافذ الأخرى، مثل منافذ المضيف. أصدرت هذا أمر in order to شكلت الميناء مكنت إرتباط up/down إعلام:

```
Switch(config-if)#snmp trap link-status
```

بعد ذلك، قم بتعيين الأجهزة لتلقي الفخاخ والعمل على الفخاخ بشكل مناسب. يمكنك الآن تكوين كل وجهة مصيدة كمستلم SNMPv1 أو SNMPv2 أو SNMPv3. بالنسبة لأجهزة SNMPv3، يمكن إرسال معلومات موثوقة بدلا من إختبارات UDP. هذا هو التكوين:

```
Switch(config)#snmp-server host ip_address [traps | informs] [version {1 | 2c | 3}] community-
string
This command needs to be on one line. !--- These are sample host destinations for SNMP ---!
traps and informs. snmp-server host 172.16.1.27 version 2c public
snmp-server host 172.16.1.111 version 1 public
snmp-server host 172.16.1.111 informs version 3 public
snmp-server host 172.16.1.33 public
```

توصيات إستطلاع SNMP

تأكد من أن قواعد معلومات الإدارة (MIB) هذه هي قواعد معلومات الإدارة (MIB) الأساسية التي يتم استفتاؤها أو مراقبتها في شبكات المجمعات:

ملاحظة: هذه التوصية مقدمة من الفريق الاستشاري لإدارة الشبكات من Cisco.

Object Name	Object Description	OID	Period	Max
MIB-II				
SysUpTime	system uptime in 1/100ths of seconds	1.3.6.1.2.1.1.3	5 min	< 30000
CISCO-STACK-MIB				
ChassisPs1status	Status of power supply 1	1.3.6.1.4.1.9.5.1.2.4	10 min	≠ 2
ChassisPs2Status	Status of power supply 2	1.3.6.1.4.1.9.5.1.2.7	10 min	≠ 2
ChassisFanStatus	Status of Chassis Fan	1.3.6.1.4.1.9.5.1.2.9	10 min	≠ 2
ChassisMinorAlarm	Chassis Minor Alarm Status	1.3.6.1.4.1.9.5.1.2.11	10 min	≠ 1
chassis MajorAlarm	Chassis Major Alarm Status	1.3.6.1.4.1.9.5.1.2.12	10 min	≠ 1

Object Name	Object Description	OID	Period	Max
ChassisTempAlarm	Chassis Temperature Alarm status	1.3.6.1.4.1.9.5.1.2.13	10 min	≠ 1
ModuleStatus	Operational Status of the module	1.3.6.1.4.1.9.5.1.3.1.1.10	30 min	≠ 2
CISCO-PROCESS-MIB				
CpmCPUTotal5min	The overall CPU busy percentage in the last 5 minute period. This object deprecates the avgBusy5 object from the OLD-CISCO-SYSTEM-MIB	1.3.6.1.4.1.9.9.109.1.1.1.5	5 min	
CISCO-STACK-MIB				
SysTraffic	% of bandwidth utilization for the previous polling interval	1.3.6.1.4.1.9.5.1.1.8	30 min	

Object Name	Object Description	OID	Period	Max
SysTrafficPeak	Peak traffic meter value since the last time the port counters were cleared or the system started	1.3.6.1.4.1.9.5.1.1.19	30 min	
BRIDGE-MIB				
CiscoEsStackSwitchBufferOverruns	Number of times the switch was out of buffers	1.3.6.1.4.1.9.5.14.2.1.1.17	30 min	

بروتوكول وقت الشبكة

الغرض

يقوم بروتوكول وقت الشبكة (NTP)، RFC 1305 ، بمزامنة حفظ الوقت بين مجموعة من خوادم الوقت الموزعة والعملاء. يسمح NTP بربط الأحداث عند إنشاء سجلات النظام وعند حدوث أحداث أخرى خاصة بالوقت.

نظرة عامة على العمليات

بروتوكول وقت الشبكة (NTP) الموثق وفقا لمعيار RFC 958 أولا. ولكن بروتوكول وقت الشبكة (NTP) تطور من خلال RFC 1119 (الإصدار 2 من بروتوكول وقت الشبكة). يعمل RFC 1305 الآن على تحديد بروتوكول وقت الشبكة (NTP)، والذي يوجد في إصداره الثالث.

يقوم NTP بمزامنة وقت عميل الكمبيوتر أو الخادم إلى خادم آخر أو مصدر وقت مرجعي آخر، مثل الراديو أو جهاز إستقبال القمر الصناعي أو المودم. يوفر بروتوكول وقت الشبكة (NTP) دقة العميل التي تكون عادة داخل مللي ثانية على شبكات LAN وما يصل إلى بضع عشرات من مللي ثانية على شبكات WAN، مقارنة بخادم أساسي متزامن. على سبيل المثال، يمكنك إستخدام بروتوكول وقت الشبكة (NTP) لتنسيق التوقيت العالمي المنسق (UTC) من خلال مستقبل خدمة تحديد المواقع العالمية (GPS).

تستخدم عمليات التهيئة النموذجية لبروتوكول وقت الشبكة (NTP) خوادم إحتياطية متعددة ومسارات شبكة متنوعة للحصول على دقة وموثوقية عاليتين. تتضمن بعض التكوينات المصادقة المشفرة لمنع هجمات البروتوكولات العرضية أو الضارة.

يعمل NTP عبر UDP، والذي يعمل بدوره، عبر IP. جميع إتصالات NTP تستخدم التوقيت العالمي المنسق، وهو نفس الوقت مثل توقيت جرينتش المركزي.

تتوفر حاليا عمليات تنفيذ NTP الإصدار 3 (NTPv3) و NTP الإصدار 4 (NTPv4). أحدث إصدار للبرامج التي يتم العمل عليها هو NTPv4، ولكن معيار الإنترنت الرسمي لا يزال NTPv3. وبالإضافة إلى ذلك، يقوم بعض بائعي نظم التشغيل بتخصيص تنفيذ البروتوكول.

ضمانات NTP

يحاول تنفيذ NTP أيضا تجنب المزامنة مع جهاز لا يمكن أن يكون الوقت دقيقة عليه. تقوم NTP بهذا بطريقتين:

- لا يقوم NTP بالمزامنة مع جهاز لم تتم مزامنته بنفسه.
- تقوم NTP دائما بمقارنة الوقت الذي يتم الإبلاغ عنه بواسطة العديد من الأجهزة، ولا تتم مزامنته مع جهاز يختلف الوقت عنه كثيرا عن الأجهزة الأخرى، حتى إذا كان لهذا الجهاز مستوى أدنى.

جمعيات

عادة ما تكون الاتصالات بين الأجهزة التي تشغل بروتوكول وقت الشبكة (NTP)، المعروفة باسم "الاقترانات"، مكونة بشكل ثابت. يتم إعطاء كل جهاز عناوين IP لجميع الأجهزة التي يحتاج إليها لتكوين اقترانات. يمكن حفظ الوقت بدقة من خلال تبادل رسائل NTP بين كل زوج من الأجهزة المقترنة. ولكن في بيئة شبكة LAN، يمكنك تكوين NTP لاستخدام رسائل بث IP. باستخدام هذا البديل، يمكنك تكوين الجهاز لإرسال رسائل البث أو تلقيها، ولكن يتم خفض دقة ضبط الوقت بشكل هامشي لأن تدفق المعلومات يكون في إتجاه واحد فقط.

إذا كانت الشبكة معزولة عن الإنترنت، يسمح لك تنفيذ Cisco NTP بتكوين جهاز حتى يعمل كما لو كان متزامنا مع إستخدام NTP، عندما يكون قد حدد الوقت بالفعل مع إستخدام أساليب أخرى. تتزامن أجهزة أخرى مع ذلك الجهاز باستخدام NTP.

يمكن أن يكون اقتران NTP إما:

- اقتران نظيرهذا يعني أنه يمكن لهذا النظام إما المزامنة مع النظام الآخر أو السماح للنظام الآخر بالمزامنة معه.
- اقتران خادموهذا يعني أن هذا النظام وحده هو الذي يتزامن مع النظام الآخر. لا يقوم النظام الآخر بالمزامنة مع هذا النظام.

إذا كنت ترغب في تكوين اقتران NTP بنظام آخر، فاستخدم أحد الأوامر التالية في وضع التكوين العام:

	الغرض
النظير ل *عنوان IP* NTP [normal-sync] [رقم الإصدار] [key *key-id*] [مصدر الواجهة] [أفضل]	تشكيل اقتران نظير بنظام آخر
خادم NTP *ip-address* [version *number*] [key *key-id*] [source *interface*] [أفضل]	تشكيل اقتران خادم بنظام آخر

ملاحظة: يلزم تكوين طرف واحد فقط من الاقتران. أما النظام الآخر فينشئ الاقتران تلقائيا.

الوصول إلى خوادم الوقت العام

تحتوي الشبكة الفرعية ل NTP حاليا على أكثر من 50 خادم أساسي عام يتم مزامنتها مباشرة مع UTC بواسطة الراديو أو القمر الصناعي أو المودم. عادة، لا تقوم محطات العمل والخوادم العميلة التي تحتوي على عدد صغير نسبيا من العملاء بالمزامنة مع الخوادم الأساسية. هناك حوالي 100 خادم ثانوي عام يتم مزامنتها مع الخوادم الأساسية. توفر هذه الخوادم المزامنة لإجمالي يزيد عن 100000 عميل وخوادم على الإنترنت. تحافظ صفحة خوادم NTP العامة على القوائم الحالية ويتم تحديثها بشكل متكرر.

وهناك أيضا العديد من الخوادم الخاصة الأولية والثانوية التي لا تكون عادة متاحة للجمهور. راجع مشروع بروتوكول وقت الشبكة (جامعة Delaware) للحصول على قائمة بخوادم NTP العامة ومعلومات حول كيفية إستخدامها. لا يوجد أي ضمان بأن خوادم الإنترنت العامة NTP هذه متوفرة وتنتج الوقت الصحيح. لذلك، يجب أن تتأمل في الخيارات الأخرى. على سبيل المثال، أستخدم أجهزة GPS مستقلة متنوعة متصلة مباشرة بعدد من الموجهات.

أحد الخيارات الأخرى هو إستخدام موجهات متنوعة، يتم ضبطها على هيئة أساسي Stratum 1. ولكن لا يوصى باستخدام موجه من هذا القبيل.

طبقة

يستخدم NTP إستراتيجية لوصف عدد نقلات NTP التي تبعد جهاز ما عن مصدر وقت موثوق به. يحتوي خادم الوقت Stratum 1 على ساعة ذرية أو لاسلكية متصلة مباشرة. يتلقى خادم الوقت Stratum 2 وقته من خادم وقت Stratum 1، وهكذا. يختار الجهاز الذي يشغل NTP تلقائيا، كمصدر الوقت الخاص به، الجهاز الذي يحتوي على أقل رقم إستراتيجية تم تكوينه به للاتصال من خلال NTP. وتبني هذه الاستراتيجية بفعالية شجرة ذاتية التنظيم من المتكلمين في بروتوكول وقت الشبكة.

يتجنب NTP المزامنة مع جهاز قد يكون الوقت غير دقيق عليه. راجع قسم *ضمانات NTP* في بروتوكول وقت الشبكة للحصول على تفاصيل.

علاقة نظير الخادم

- يستجيب الخادم لطلبات العميل ولكنه لا يحاول دمج أي معلومات تاريخ من مصدر وقت العميل.
- يستجيب النظير لطلبات العملاء ويحاول إستخدام طلب العميل كمرشح محتمل للحصول على مصدر وقت أفضل والمساعدة على تثبيت تردد ساعة المعالج.
- لكي تكون الأقران الحقيقيين، يجب أن يدخل كلا جانبي الاتصال في علاقة نظير، بدلا من حالة يعمل فيها أحد المستخدمين كنظير ويعمل فيها المستخدم الآخر كخادم. اطلب من النظراء تبادل المفاتيح بحيث لا يتمكن إلا المضيفون الموثوق بهم من التحدث إلى الآخرين كنظراء.
- في طلب عميل لخادم، يجيب الخادم على العميل وينسى أن العميل سأل سؤالا.
- في طلب العميل إلى نظير، يجيب الخادم على العميل. يحتفظ الخادم بمعلومات الحالة عن العميل لتعقب مدى أداء العميل للمتطلبات في الوقت المحدد وخادم الطبقة الأساسية الذي يقوم العميل بتشغيله.

يمكن لخادم NTP التعامل مع عدة آلاف من العملاء دون أي مشكلة. ولكن عندما يعالج خادم NTP أكثر من عدد قليل من العملاء (يصل إلى بضع مئات)، يكون هناك تأثير على الذاكرة على قدرة الخادم على الاحتفاظ بمعلومات الحالة. عندما يقوم خادم NTP بمعالجة أكثر من المبلغ الموصى به، يتم إستهلاك المزيد من موارد وحدة المعالجة المركزية والنطاق الترددي على المربع.

أوضاع الاتصال بخادم NTP

وهما وضعان منفصلان للاتصال بالخادم:

- وضع البث
- وضع العميل/الخادم

في وضع البث، يستمع العملاء. في وضع العميل/الخادم، يقوم العملاء باستطلاع الخادم. يمكنك إستخدام بث NTP إذا لم يكن هناك إرتباط WAN متورط بسبب سرعته. للتنقل عبر إرتباط شبكة WAN، أستخدم وضع العميل/الخادم (عن طريق الاقتراع). تم تصميم وضع البث لشبكة LAN، حيث قد يحتاج العديد من العملاء إلى إستطلاع الخادم. بدون وضع البث، يمكن أن يؤدي هذا الاستقصاء إلى توليد عدد كبير من الحزم على الشبكة. لا تتوفر بث NTP المتعدد حتى الآن في NTPv3، ولكنه متوفر في NTPv4.

وبشكل افتراضي، يتصل برنامج Cisco IOS باستخدام NTPv3. ولكن البرنامج متوافق مع الإصدارات السابقة من بروتوكول وقت الشبكة (NTP).

إستبيان

يسمح بروتوكول NTP للعميل باستعلام خادم في أي وقت.

عندما يشكل أنت أول NTP في cisco صندوق، NTP يرسل ثمانية إستفسار في تعاقب سريع في NTP_MINPOLL 16=4^2) ثانية) فاصل. يبلغ 14^2 NTP_MAXPOLL ثانية (16،384 ثانية أو 4 ساعات، 33 دقيقة، 4 ثانية). هذه الفترة الزمنية هي أطول فترة قبل إجراء إستطلاعات NTP مرة أخرى للرد. حاليا، لا تمتلك Cisco طريقة للسماح للمستخدم بفرض وقت .

يبدأ عداد إستطلاع NTP في 6^2 (64) ثانية، أو 1 دقيقة، 4 ثانية. وتزداد هذه المرة باقوى من 2، إذ يتزامن الخادمان مع بعضهما البعض، إلى 10^2. يمكنك توقع إرسال رسائل المزامنة في فترة زمنية واحدة من 64 أو 128 أو 256 أو 512 أو 1024 ثانية، وفقا لتكوين الخادم أو النظير. الفترة الزمنية الأطول بين عمليات الاقتراع حيث تصبح الساعة الحالية أكثر إستقرارا بسبب حلقات التكرار المقفلة. تقوم حلقات التكرار المقفلة بالطور بقص بلورة الساعة المحلية، حتى 1024 ثانية (17 دقيقة).

يتراوح الوقت بين 64 ثانية و 1024 ثانية كقوة مقدارها 2 (وهو ما يعادل مرة واحدة كل 64 أو 128 أو 256 أو 512 أو 1024 ثانية). يعتمد الوقت على الحلقة المقفلة مرحليا التي ترسل وتستلم الحزم. وإذا كان هناك الكثير من الارتباك في ذلك الوقت، فإن عمليات الاقتراع تحدث بشكل أكثر تكرارا. إذا كانت الساعة المرجعية دقيقة وكان اتصال الشبكة متناسقا، فإن أوقات الاستقصاء تتقارب في 1024 ثانية بين كل إستقصاء.

يتغير الفاصل الزمني لاستطلاع NTP مع تغير الاتصال بين العميل والخادم. مع اتصال أفضل، الفاصل الزمني للاستطلاع أطول. وفي هذه الحالة، يعني الاتصال الأفضل أن عميل NTP قد تلقى ثماني استجابات للطلبات الثمانية الأخيرة. ثم يتم مضاعفة الفترة الزمنية للاستطلاع. تتسبب إستجابة فائتة واحدة في تقليل الفاصل الزمني للاستطلاع إلى النصف. تبدأ فترة الاستقصاء في 64 ثانية وتنتهي إلى 1024 ثانية كحد أقصى. في أفضل الظروف، الوقت المطلوب للفاصل الزمني للاستطلاع لكي ينتقل من 64 ثانية إلى 1024 ثانية هو أكثر بقليل من ساعتين.

إذاعات

لا يتم إعادة توجيه عمليات بث NTP أبدا. إذا قمت بإصدار أمر **بث NTP**، يبدأ الموجه في إنشاء بث NTP على الواجهة التي تم تكوينه عليها.

عادة، تقوم بإصدار الأمر **ntp broadcast** لإرسال بث NTP إلى شبكة LAN لخدمة محطات العميل الطرفية والخوادم.

مزامنة الوقت

تتكون مزامنة أحد العملاء مع أحد الخوادم من عدة عمليات تبديل للحزم. كل تبادل هو زوج طلب/رد. عندما يرسل أحد العملاء طلبا، يقوم العميل بتخزين وقته المحلي داخل الحزمة المرسلة. عندما يستلم خادم الحزمة، فإنه يخزن تقديره الخاص للوقت الحالي في الحزمة، ويتم إرجاع الحزمة. عند إستلام الرد، يقوم المستلم مرة أخرى بتسجيل وقت الاستلام الخاص به لتقدير وقت سفر الحزمة.

هذا وقت فرق يستطيع كنت استعملت in order to قدرت الوقت أن كان ضروري للحزمة أن يبث من الخادم إلى الطالب. ويأخذ هذا الوقت من الرحلة المستديرة في الاعتبار لتقدير الوقت الحالي. وكلما كان وقت الرحلة الدائرية أقصر، كان تقدير الوقت الحالي أكثر دقة.

لا يتم قبول الوقت حتى يتم إجراء العديد من عمليات تبادل الحزم المتفق عليها. يتم وضع بعض القيم الأساسية في عوامل تصفية متعددة المراحل لتقدير جودة العينات. عادة، يلزم حوالي 5 دقائق لكي يقوم عميل NTP بالمزامنة مع خادم. ومن المثير للاهتمام ان ذلك يصح أيضا في الساعات المرجعية المحلية التي ليس لها تأخير على الاطلاق بحسب التعريف.

وإضافة إلى ذلك، تؤثر جودة اتصال الشبكة أيضا على الدقة النهائية. تؤثر الشبكات البطيئة والتي لا يمكن التنبؤ بها مع تأخيرات متنوعة بشكل سيئ على مزامنة الوقت.

يلزم توفر فرق زمني أقل من 128 مللي ثانية لإجراء المزامنة من قبل بروتوكول وقت الشبكة (NTP). تتراوح الدقة النموذجية على الإنترنت من 5 مللي ثانية إلى 100 مللي ثانية، وهو ما يمكن أن يختلف باختلاف حالات تأخر الشبكة.

مستويات حركة مرور NTP

النطاق الترددي الذي يستخدمه NTP هو الحد الأدنى. الفترة بين رسائل الاقتراع التي يتبادلها النظراء عادة ما ترجع إلى ما لا يزيد عن رسالة واحدة كل 17 دقيقة (1024 ثانية). مع التخطيط الدقيق، يمكنك الحفاظ على هذا داخل شبكات الموجه عبر إرتباطات شبكة WAN. أجعل عملاء NTP نظراء لخوادم NTP المحلية وليس طوال الطريق عبر شبكة WAN إلى الموجهات الأساسية في الموقع المركزي، والتي هي خوادم Stratum 2.

يستخدم عميل NTP المجمع متوسطات مقدارها 0.6 بت في الثانية (bps) لكل خادم.

توصية Cisco NTP

- توصي Cisco بأن يكون لديك خوادم وقت متعددة ومسارات شبكة متنوعة لتحقيق دقة وموثوقية عالية. تتضمن بعض التكوينات المصادقة المشفرة لمنع هجمات البروتوكولات العرضية أو الضارة.
- وفقا ل NTP، RFC حقا مصمم أن يسمح لك باستطلاع عدة وقت خادم مختلف واستخدام تحليل إحصائي معقد in order to ظهرت وقت صالح، حتى إذا كنت غير متأكد من أن جميع الخوادم التي تقوم باستطلاع هي موثوقة. تقدر NTP الأخطاء في كل الساعات. لذلك، تقوم جميع خوادم NTP بإرجاع الوقت مع تقدير للخطأ الحالي. عند إستخدام خوادم الوقت المتعددة، يريد NTP أيضا أن توافق هذه الخوادم على ذلك في بعض الوقت.
- لا يدعم تنفيذ Cisco لبروتوكول وقت الشبكة (NTP) خدمة الطبقة الأولى. لا يمكنك الاتصال بساعة راديو أو ساعة ذرية. توصي Cisco بأن يتم اشتقاق خدمة الوقت لشبكتك من خوادم NTP العامة المتوفرة على إنترنت IP.
- قم بتمكين جميع محولات العميل لإرسال طلبات الوقت اليومي بشكل منتظم إلى خادم NTP. يمكنك تكوين ما يصل إلى 10 عناوين خوادم/نظراء لكل عميل حتى يمكنك تحقيق المزامنة السريعة.
- لتقليل التكاليف الإضافية للبروتوكول، تقوم الخوادم الثانوية بتوزيع الوقت عبر بروتوكول NTP على مضيفي الشبكة المحلية المتبقين. لتحقيق الموثوقية، يمكنك تزويد الأجهزة المضيفة المحددة بساعات أقل دقة ولكنها أقل تكلفة لاستخدامها لإجراء نسخ إحتياطي في حالة فشل الخوادم الرئيسية و/أو الثانوية أو مسارات الاتصال بينها.
- NTP—**NTP update-calendar** عادة ما تغير ساعة النظام فقط. يسمح هذا الأمر ل NTP بتحديث معلومات التاريخ/الوقت على التقويم. يتم إجراء التحديث فقط في حالة مزامنة وقت NTP. وإلا، يحتفظ التقويم بوقته الخاص ولا يتأثر بتوقيت بروتوكول وقت الشبكة (NTP) أو ساعة النظام. أستخدم هذا دائما على الموجهات المتطورة.
- **تقويم الساعة صحيح**—يعلن هذا الأمر أن معلومات التقويم صحيحة ومزامنة. أستخدم هذا الخيار على مدير NTP. إذا لم يتم تكوين هذا الأمر، فإن الموجه الطرفي الذي يحتوي على التقويم لا يزال يعتقد أن وقته غير موثوق به، حتى إذا كان يحتوي على سطر NTP الرئيسي.
- أي رقم طبقة يتجاوز 15 يعتبر غير متزامن. هذا هو السبب الذي من أجله ترى الطبقة 16 في إخراج الأمر **show ntp status** على الموجهات التي تكون الساعات غير متزامنة لها. إذا تم مزامنة الأساسي مع خادم NTP عام، فتأكد من أن رقم الطبقة العليا على سطر NTP الرئيسي هو أعلى واحد أو إثنين من أعلى رقم طبقة على الخوادم العامة التي تقوم باستطلاعها.
- قام العديد من العملاء بتكوين NTP في وضع الخادم على الأنظمة الأساسية لبرنامج Cisco IOS الخاصة بهم، والتي تمت مزامنتها من العديد من موجز الويب الموثوق به من الإنترنت أو ساعة الراديو. داخليا، هناك بديل أبسط لوضع الخادم عندما تشغل عددا كبيرا من المحولات هو تمكين NTP في وضع البث على شبكة VLAN الإدارية في مجال محول. يسمح هذا آلية المادة حفازة أن يستلم ساعة من بيث رسالة. ولكن دقة ضبط الوقت تتضاءل بشكل هامشي لأن تدفق المعلومات في إتجاه واحد.
- يمكن أن يساعد إستخدام عناوين الاسترجاع كمصدر للتحديثات في التناسق أيضا. يمكنك معالجة المخاوف الأمنية بطريقتين:مع التحكم في تحديثات الخادم، والذي توصي به Ciscoعن طريق المصادقة

أوامر التكوين العام NTP

```
???? For the client: clock timezone EST -5 ---!
????? ntp source loopback 0
```

```
ntp server ip_address key 1
ntp peer ip_address
This is for a peer association. ntp authenticate ---!
ntp authentication-key 1 md5 xxxx
ntp trusted-key 1

For the server: clock timezone EST -5 ---!
clock summer-time EDT recurring 1 Sun Apr 3:00 last Sun Oct 3:00
clock calendar-valid
ntp source loopback0
ntp update-calendar

This is optional: interface vlan_id ntp broadcast ---!
This sends NTP broadcast packets. ntp broadcast client ---!
This receives NTP broadcast packets. ntp authenticate ---!
ntp authentication-key 1 md5 xxxxx
ntp trusted-key 1
ntp access-group access-list
.This provides further security, if needed ---!
```

أمر حالة NTP

```
show ntp status

Clock is synchronized, stratum 8, reference is 127.127.7.1
nominal freq is 250.0000 Hz, actual freq is 249.9974 Hz, precision is 2**18
(reference time is C6CF0C30.980CCA9D (01:34:00.593 IST Mon Sep 12 2005
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.02 msec, peer dispersion is 0.02 msec
```

هذا هو عنوان الساعة المرجعية لموجه Cisco عندما يعمل الموجه كمدير NTP. إذا لم تتم مزامنة الموجه مع أي خادم NTP، يستخدم الموجه هذا العنوان كمعرف مرجع. للحصول على تفاصيل حول التكوين والأوامر، ارجع إلى قسم *تكوين NTP* في تنفيذ إدارة النظام الأساسية.

بروتوكول أستكشاف Cisco

الغرض

يعمل بروتوكول CDP عبر الطبقة 2 (طبقة إرتباط البيانات) على جميع موجهات Cisco والجسور وخوادم الوصول والمحولات. يسمح CDP لتطبيقات إدارة الشبكة باكتشاف أجهزة Cisco المجاورة للأجهزة المعروفة بالفعل. وعلى وجه الخصوص، يمكن لتطبيقات إدارة الشبكة اكتشاف الجيران الذين يقومون بتشغيل بروتوكولات شفافة منخفضة الطبقة. باستخدام CDP، يمكن لتطبيقات إدارة الشبكة معرفة نوع الجهاز وعنوان وكيل SNMP للأجهزة المجاورة. تمكن هذه الميزة التطبيقات من إرسال استعلامات SNMP إلى الأجهزة المجاورة.

تتيح أوامر **العرض** المرتبطة بميزة CDP لمهندس الشبكة تحديد هذه المعلومات:

- الوحدة النمطية/رقم المنفذ للأجهزة الأخرى المجاورة التي تم تمكين CDP عليها
- عناوين الجهاز المجاور التالية:عنوان MACعنوان IPعنوان قناة المنفذ
- إصدار برنامج الجهاز المجاور
- هذه المعلومات حول الجهاز المجاور:السرعةالإرسال ثنائي الاتجاهvtp domainإعداد شبكة VLAN الأصلية

يسلط قسم نظرة عامة على العمليات الضوء على بعض تحسينات الإصدار 2 من بروتوكول CDP (CDPv2) على الإصدار 1 من بروتوكول CDP (CDPv1).

نظرة عامة على العمليات

يتم تشغيل CDP على جميع وسائط LAN و WAN التي تدعم SNAP.

يرسل كل جهاز مكون من CDP رسائل دورية إلى عنوان بث متعدد. يعلن كل جهاز عن عنوان واحد على الأقل يمكن للجهاز تلقي رسائل SNMP عليه. كما تحتوي الإعلانات على معلومات فترة البقاء، أو فترة الانتظار. تشير هذه المعلومات إلى طول الوقت الذي يستغرقه الجهاز المتلقي في الاحتفاظ بمعلومات بروتوكول CDP قبل تجاهلها.

يستخدم CDP تضمين SNAP مع رمز النوع 2000. على الإيثرنت، ATM، و FDDI، يتم إستخدام عنوان البث المتعدد للوجهة 0c-cc-cc-00-01. في حلقات الرمز المميز، يتم إستخدام العنوان الوظيفي c000.0800.0000. يتم إرسال إطارات CDP بشكل دوري كل دقيقة.

تحتوي رسائل CDP على رسالة واحدة أو أكثر تسمح للجهاز الوجهة بجمع معلومات وتخزينها حول كل جهاز مجاور.

يوفر هذا الجدول المعلمات التي يدعمها CDPv1:

بارامتر	النوع	الوصف
1	معرف الجهاز	اسم مضيف الجهاز أو الرقم التسلسلي للأجهزة في ASCII
2	العنوان	الطبقة 3 عنوان من القارن أن يرسل التحديث
3	معرف المنفذ	المنفذ الذي يتم إرسال تحديث CDP عليه
4	القدرات	تصف القدرات الوظيفية للجهاز بهذه الطريقة: • الـ

		وجه: 0x01 جسر SR1: • 0x04 الوحول: 0x08 (يوفر تحويل الطبقة 2 و/أو الطبقة 3

) • المضيف: 0x10 • التصفية الشرطية لبروتوكول IGMP: 0x20 • لا يقوم الجسر أو الم		

		حول بإعادة توجيه حزم تقارير GMP على الواجهة غير المعرفة.
5	الإصدار	سلسلة أحرف تحتوي على إصدار البرنامج **ملاحظة:** يعرض إخراج الأمر **show**

		version المعلومات نفسها.
6	النظام الأساسي	النظام الأساسي للأجهزة، على سبيل المثال، WS-C5000 و WS-C6009 و Cisco RSP[2]

[1] SR = source-route.

[2] RSP = معالج محول المسار.

في CDPv2، تم إدخال نوع وطول وقيم إضافية (TLVs). يدعم CDPv2 أي TLV. ولكن هذا الجدول يوفر المعاملات التي يمكن أن تكون مفيدة بشكل خاص في البيئات المحولة والتي تستخدمها برامج Catalyst.

عندما يقوم محول بتشغيل CDPv1، يقوم المحول بإسقاط إطارات CDPv2. عندما يقوم محول بتشغيل CDPv2 ويستلم إطار CDPv1 على واجهة، يبدأ المحول في إرسال إطارات CDPv1 من تلك الواجهة، بالإضافة إلى إطارات CDPv2.

بارامتر	**النوع**	**الوصف**
9	vtp domain	المجال VTP، إن يكون شكلت على الأداة
10	شبكة VLAN الأصلية	في dot1q،

		يبقى الإطارات لل VLAN أي الميناء يكون في إن الميناء ليس trunking، untagged. عادة ما يشار إليها باسم شبكة VLAN الأصلية.
11	الإرسال ثنائي الإتجاه الكامل/النصفي	يحتوي TLV هذا على إعداد الإر

		سا ل ثنائ ي الإت جاه لمنـ فذ الإر سا ل.
14	معرف Appliance vlan	يتيح التم ييز بين حر كة مرو ر Vo IP وح ركة المر ور الأخ رى من خلا ل معر ف VL AN منف صل (شب كة VL AN الم سا عد ة).
16	إستهلاك الطاقة	الح د الأق ص ى لمق دار الط

		اقة المتوقع إستهلاكه، في mW، بواسطة الجهاز المتصل.
17	MTU	وحدة الحد الأقصى للنقل (MTU) للواجهة التي يتم من خلالها إرسال إطار CDP.
18	ثقة ممتدة	يشير إلى أن المنفذ في وض

		ع الثقة المـوسعة.
19	CoS للمنافذ غير الموثوق بها	قيمة فئة الخدمة (CoS) التي يتم إستخدامها لوضع علامة على جميع الحزم التي يتم استقبالها على المنفذ غير الموثوق به لجهاز تحويل متصل.

20	SysName	اسم المجال المؤهل بالكامل للجهاز (0، إذا كان غير معروف).
25	الطاقة المطلوبة	يتم إرسالها بواسطة جهاز فائق الإمكانات للتفاوض حول مستوى طاقة مناسب.
26	الطاقة المتوفرة	تم الإرسال بواسطة مح

		ول. يتيح للجهاز القوي التفاوض وتحديد إعداد طاقة منا سب.

CDPv2/التزويد بالطاقة عبر شبكة إيثرنت

تملك بعض المحولات، مثل المادة حفازة 6000/6500 و 4000/4500، القدرة على إمداد الطاقة من خلال كبلات زوج مجدول غير محمية (UTP) إلى الأجهزة القابلة للطاقة. تساعد المعلومات التي يتم تلقيها عبر بروتوكول CDP (المعلمات 16 و 25 و 26) في تحسين إدارة طاقة المحول.

تفاعل هاتف بروتوكول الإنترنت (IP) من CDPv2/Cisco

توفر هواتف Cisco IP إمكانية الاتصال لجهاز إيثرنت متصل خارجيا بسرعة 100/10 ميجابت في الثانية. ويتم تحقيق هذا الاتصال من خلال دمج محول داخلي من الطبقة 2 يحتوي على ثلاثة منافذ داخل هاتف بروتوكول الإنترنت (IP). ويشار إلى منافذ المحول الداخلي باسم:

- P0 (جهاز هاتف بروتوكول الإنترنت الداخلي)
- P1 (منفذ خارجي بسرعة 100/10 ميجابت في الثانية)
- P2 (منفذ Mbps-100/10 خارجي يتصل بالمحول)

أنت يستطيع نقلت حركة مرور صوت على VLAN منفصل على المفتاح ميناء إن يشكل أنت dot1q منفذ شنطة ميناء. هذا VLAN إضافي يعرف بما أن (CatOS) أو الصوت (cisco ios برمجية) VLAN. ونتيجة لذلك، يمكن إرسال حركة مرور البيانات المميزة dot1q من هاتف IP على شبكة VLAN المساعدة/الصوتية، ويمكن إرسال حركة المرور غير المميزة عبر المنفذ الخارجي Mbps-100/10 من الهاتف عبر شبكة VLAN للوصول.

يمكن لمحولات Catalyst إعلام هاتف IP بمعرف شبكة VLAN الصوتية عبر CDP (المعلمة-14: appliance vlan-id TLV). ونتيجة لذلك، يقوم هاتف بروتوكول الإنترنت بوضع علامات على جميع الحزم المتعلقة ب VoIP بمعرف VLAN المناسب وأولوية 802.1p. يتم إستخدام CDP TLV هذا أيضا لتحديد ما إذا كان هاتف IP متصلا عبر معلمة معرف الجهاز.

ويمكن إستغلال هذا المفهوم عند تطوير سياسة جودة الخدمة. أنت يستطيع شكلت المادة حفازة مفتاح أن يتفاعل مع ال ip هاتف بثلاثة طرق:

- هاتف بروتوكول الإنترنت من CiscoCoS الثقة المشروطة فقط عندما يتم الكشف عن هاتف IP عبر CDP. عند اكتشاف هاتف IP عبر معلمة CDP-14، يتم تعيين حالة ثقة المنفذ على Trust CoS. إذا لم يتم اكتشاف هاتف IP، فإن المنفذ غير موثوق به.
- ثقة ممتدةيمكن أن يقوم المحول بإعلام هاتف IP عبر CDP (المعلمة-18) بالثقة في جميع الإطارات التي يتم استقبالها على منفذ الجهاز الخارجي بسرعة 100/10 ميجابت في الثانية.

- إعادة كتابة CoS للمنافذ غير الموثوق بهايمكن أن يقوم المحول بإعلام هاتف IP عبر CDP (المعلمة-19) لإعادة كتابة قيم CoS 802.1p التي يتم استقبالها على منفذ الجهاز الخارجي 100/10 ميجابت في الثانية.**ملاحظة:** بشكل افتراضي، تكون جميع حركة مرور البيانات التي يتم استقبالها على المنافذ الخارجية بسرعة 100/10 ميجابت في الثانية لهاتف IP غير موثوق بها.

ملاحظة: هذا مثال لتكوين كيفية توصيل هاتف IP غير المزود بمحول.

ملاحظة: على سبيل المثال،

```
Switch(config)#interface gigabitEthernet 2/1
Switch(config-if)#switchport mode trunk

For example use VLAN 30 for voice VLAN, and VLAN 10 for access VLAN. Switch(config- ---!
if)#switchport trunk native vlan 10
Switch(config-if)#switchport trunk allow vlan 10,30
Switch(config-if)#switchport voice vlan 30
Switch(config-if)#spanning-tree portfast trunk

And besides that enable LLDP as Non Cisco IP Phone do not use CDP. Switch(config)#lldp run ---!
```

توصية تكوين Cisco

يمكن أن تكون المعلومات التي يقدمها بروتوكول CDP مفيدة للغاية عند أستكشاف أخطاء اتصال الطبقة 2 وإصلاحها. قم بتمكين CDP على جميع الأجهزة التي تدعم تشغيله. أصدر الأوامر التالية:

- لتمكين CDP بشكل عام على المحول:

```
Switch(config)#cdp run
```

- لتمكين CDP على أساس كل منفذ:

```
#Switch(config)#interface type slot#/port
Switch(config-if)#cdp enable
```

قائمة إختيار التكوين

أوامر عامة

قم بتسجيل الدخول والتمكين وإدخال وضع التكوين العام لبدء عملية تكوين المحول.

```
Switch>enable
#Switch
Switch#configure terminal
#(Switch(Config
```

الأوامر العامة العامة (على مستوى المؤسسة)

يسرد قسم الأوامر العامة هذا الأوامر العامة التي سيتم تطبيقها على جميع المحولات في شبكة مؤسسة العميل.

يحتوي هذا التكوين على الأوامر العامة الموصى بها لإضافتها إلى التكوين الأولي. يجب أن تقوم بتغيير القيم في المخرجات قبل أن تقوم بنسخ ولصق النص في CLI. أصدرت هذا أمر in order to طبقت التشكيل شامل:

```
vtp domain domain_name
vtp mode transparent
spanning-tree portfast bpduguard
spanning-tree etherchannel guard misconfig
cdp run
no service pad
service password-encryption
enable secret password
clock timezone EST -5
clock summer-time EDT recurring 1 Sun Apr 3:00 last Sun Oct 3:00
clock calendar-valid
ip subnet-zero
ip host tftpserver your_tftp_server
ip domain-name domain_name
ip name-server name_server_ip_address
ip name-server name_server_ip_address
ip classless
no ip domain-lookup
no ip http server
no logging console
no logging monitor
logging buffered 16384
logging trap notifications
logging facility local7
logging syslog_server_ip_address
logging syslog_server_ip_address
logging source-interface loopback0
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
access-list 98 permit host_ip_address_of_primary_snmp_server
access-list 98 permit host_ip_address_of_secondary_snmp_server
snmp-server community public ro 98
snmp-server community laneng rw 98
snmp-server enable traps entity
snmp-server host host_address traps public
snmp-server host host_address traps public
banner motd ^CCCCC

,This is a proprietary system, NOT for public or personal use.  All work products
 communications, files, data or information directly or indirectly created, input
.or accessed on this system are and shall become the sole property of the company
  This system is actively monitored and accessed by the company.  By logging onto
                    .this system, the user consents to such monitoring and access

  USE OF THIS SYSTEM WITHOUT OR IN EXCESS OF THE PROPER AUTHORIZATION MAY SUBJECT
                        THE USER TO DISCIPLINE AND/OR CIVIL AND CRIMINAL PENALTIES

C^
line console 0
exec-timeout 0 0
password cisco
login
transport input none
line vty 0 4
exec-timeout 0 0
password cisco
login
length 25
clock calendar-valid
ntp server ntp_server_ip_address
ntp server ntp_server_ip_address
ntp update-calendar
```

الأوامر العامة الخاصة بكل هيكل محول

تكون الأوامر العامة في هذا القسم خاصة بكل هيكل محول يتم تثبيته في الشبكة.

متغيرات التكوين الخاصة بالهيكل

أصدرت in order to ثبتت التاريخ والوقت، هذا أمر:

```
Switch#clock set hh:mm:ss day month year
```

أصدرت in order to ثبتت الأداة مضيف إسم، هذا أمر:

```
Switch>enable
Switch#configure terminal
.Enter configuration commands, one per line.  End with CNTL/Z
Switch(config)#hostname Cat6500
```

أصدرت in order to شكلت الاسترجاع قارن للإدارة، هذا أمر:

```
CbrCat6500(config)#interface loopback 0
Cat6500(config-if)#description Cat6000 - Loopback address and Router ID
Cat6500(config-if)#ip address ip_address subnet_mask
Cat6500(config-if)#exit
```

أصدرت in order to عرضت المشرف محرك cisco ios برمجية مراجعة، هذا أمر:

```
Cbrcat6500#show version | include IOS
IOS (tm) MSFC Software (C6MSFC-DSV-M), Version 12.1(13)E9, EARLY DEPLOYMENT RELE
(ASE SOFTWARE (fc1
cat6500#
```

أصدرت in order to عرضت ال MSFC جزمة مبرد مراجعة، هذا أمر:

```
:Cat6500#dir bootflash
/:Directory of bootflash
rw- 1879040 Aug 19 2003 19:03:29 c6msfc-boot-mz.121-19.E1a- 1

bytes total (14111616 bytes free 15990784
```

لتحديد معلومات جهة اتصال خادم SNMP والموقع، قم بإصدار الأوامر التالية:

```
Cat6500(config)#snmp-server contact contact_information
Cat6500(config)#snmp-server location location_of_device
```

لنسخ تكوين بدء التشغيل من Supervisor Engine (محرك المشرف) موجود إلى Supervisor Engine (محرك المشرف) جديد، قد يحدث بعض الفقدان للتكوين، على سبيل المثال، التكوين على واجهات المشرف الموجود. توصي Cisco بنسخ التكوين إلى ملف نصي ولصقه في مقاطع في وحدة التحكم لمعرفة ما إذا كانت هناك أي مشاكل تكوين تحدث.

أوامر الواجهة

أنواع المنافذ الوظيفية من Cisco

تتم الإشارة إلى منافذ المحول في برنامج Cisco IOS software كواجهات. هناك نوعان من أوضاع الواجهة في برنامج Cisco IOS Software:

- الواجهة الموجهة للطبقة 3
- واجهة محول الطبقة 2

تشير وظيفة الواجهة إلى كيفية تكوين المنفذ لديك. يمكن أن يكون تكوين المنفذ:

- الواجهة الموجهة
- الواجهة الظاهرية المحولة (SVI)
- منفذ الوصول
- شنطة
- EtherChannel
- مزيج من هذه

يشير نوع الواجهة إلى نوع منفذ. يمكن أن يكون نوع المنفذ إما:

- في
- ge
- قناة المنفذ

تصف هذه القائمة بإيجاز وظائف واجهة برنامج Cisco IOS Software المختلفة:

- الواجهة المادية الموجهة (الافتراضية)- كل واجهة على المحول هي واجهة الطبقة 3 الموجهة بشكل افتراضي، والتي تكون مماثلة لأي موجه Cisco. يجب أن تقع الواجهة الموجهة على شبكة IP فرعية فريدة.
- Access Switch Port Interface — تستخدم هذه الوظيفة لوضع الواجهات في شبكة VLAN نفسها. يجب تحويل المنافذ من واجهة موجهة إلى واجهة محولة.
- SVI—يمكن إقران SVI بشبكة VLAN تحتوي على منافذ محول وصول للتوجيه بين شبكات VLAN. شكلت ال SVI أن يكون صحبت مع VLAN عندما أنت تريد ممر أو جسر بين منفذ مفتاح ميناء على VLANs مختلف.
- واجهة منفذ محول خط الاتصال — تستخدم هذه الوظيفة لحمل شبكات VLAN متعددة إلى جهاز آخر. يجب تحويل المنافذ من واجهة موجهة إلى منفذ محول خط اتصال.
- EtherChannel—يتم إستخدام EtherChannel لتجميع منافذ منفردة في منفذ منطقي وحيد للتكرار وتوزيع الأحمال.

توصيات نوع المنفذ الوظيفي من Cisco

أستخدم المعلومات الواردة في هذا القسم للمساعدة في تحديد المعلمات التي سيتم تطبيقها على الواجهات.

ملاحظة: أدمجت بعض الأوامر الخاصة بالواجهة حيثما أمكن ذلك.

التفاوض التلقائي

لا تستخدم التفاوض التلقائي في أي من هذه الحالات:

- للمنافذ التي تدعم أجهزة البنية الأساسية للشبكة مثل المحولات والموجهات
- بالنسبة للأنظمة الطرفية غير العابرة الأخرى مثل الخوادم والطابعات

قم بتكوين تكوينات الارتباط هذه يدويا للسرعة والإرسال ثنائي الإتجاه بسرعة 100/10 ميجابت في الثانية. ويتم إرسال

الإرسال ثنائي الإتجاه الكامل بسرعة 100 ميجابت في الثانية عادة:

- محول إلى محول إرتباط 100 ميجابت
- اتصال من محول إلى خادم بسرعة 100 ميجابت
- جهاز توجيه الارتباط 100 ميجابت من Cisco

أنت يستطيع شكلت هذا عملية إعداد بهذه الطريقة:

```
#Cat6500(config-if)#interface [type] mod#/port
Cat6500(config-if)#speed 100
Cat6500(config-if)#duplex full
```

توصي Cisco بتكوينات إرتباط بسرعة 100/10 ميجابت في الثانية للمستخدمين النهائيين. يحتاج العمال المتنقلون والمضيفون العابرون إلى التفاوض التلقائي، كما يوضح هذا المثال:

```
#Cat6500(config-if)#interface [type] mod#/port
Cat6500(config-if)#speed auto
```

القيمة الافتراضية على واجهات Gigabit هي . ولكن قم بإصدار هذه الأوامر لضمان تمكين التفاوض التلقائي. توصي Cisco بتمكين تفاوض Gigabit:

```
#Cat6500(config-if)#interface gigabitethernet mod#/port
Cat6500(config-if)#no speed
```

جذر الشجرة الممتدة

مع مراعاة تصميم الشبكة، حدد المحول الأكثر ملاءمة ليكون هو الجذر لكل شبكة محلية ظاهرية (VLAN). بشكل عام، أختر محولا قويا في وسط الشبكة. ضع الجسر الرئيسي في مركز الشبكة ثم قم بتوصيل الجسر الرئيسي مباشرة بالخوادم والموجهات. ويعمل هذا الإعداد بشكل عام على تقليل متوسط المسافة من العملاء إلى الخوادم والموجهات. راجع مشاكل بروتوكول الشجرة المتفرعة واعتبارات التصميم ذات الصلة للحصول على مزيد من المعلومات.

لفرض محول على أن يكون الجذر لشبكة VLAN مخصصة، قم بإصدار هذا الأمر:

```
Cat6500(config)#spanning-tree vlan vlan_id root primary
```

بروتوكول PortFast للشجرة الممتدة

يقوم PortFast بتجاوز عملية الشجرة المتفرعة العادية على منافذ الوصول لزيادة سرعة تأخيرات الاتصال الأولية التي تحدث عند توصيل المحطات الطرفية بمحول ما. راجع إستخدام أوامر PortFast وغيرها من الأوامر لإصلاح تأخيرات اتصال بدء تشغيل محطة العمل للحصول على مزيد من المعلومات حول PortFast.

تعيين STP PortFast على تشغيل جميع منافذ الوصول الممكنة المتصلة بمضيف واحد. وفيما يلي مثال على هذا:

```
#Cat6500(config-if)#interface [type] mod#/port
Cat6500(config-if)#spanning-tree portfast
Warning: portfast should only be enabled on ports connected to a single%
host. Connecting hubs, concentrators, switches, bridges, etc... to this
.interface  when portfast is enabled, can cause temporary bridging loops
```

```
Use with CAUTION
Portfast has been configured on FastEthernet3/1 but will only have effect%
.when the interface is in a non-trunking mode
```

اكتشاف الرابط أحادي الاتجاه (UDLD)

مكنت UDLD فقط على يربط بنية ميناء أو نحاسي إثرنيت كبل in order to راقبت التشكيل طبيعي من الكبل. أصدرت هذا أمر in order to مكنت UDLD:

```
#Cat6500(config)#interface [type] mod#/port
Cat6500(config-if)#udld enable
```

VLAN تشكيل معلومة

شكلت VLANs مع هذا أمر:

```
Cat6500(config)#vlan vlan_number
Cat6500(config-vlan)#name vlan_name
Cat6500(config-vlan)#exit
Cat6500(config)#spanning-tree vlan vlan_id
Cat6500(config)#default spanning-tree vlan vlan_id
```

كررت الأمر ل كل VLAN، وبعد ذلك خرجت. قم بإصدار هذا الأمر:

```
Cat6500(config)#exit
```

أصدرت هذا أمر in order to دققت all the VLANs:

```
Cat6500#show vlan
```

بطاقات SVIs الموجهة

قم بتكوين SVIs للتوجيه بين شبكات VLAN. أصدر الأوامر التالية:

```
Cat6500(config)#interface vlan vlan_id
Cat6500(config-if)#ip address svi_ip_address subnet_mask
Cat6500(config-if)#description interface_description
Cat6500(config-if)#no shutdown
```

كرر هذه الأوامر لكل وظيفة واجهة تحتوي على SVI موجه، ثم قم بإنهاء. قم بإصدار هذا الأمر:

```
Cat6500(config-if)#^Z
```

الواجهة المادية الأحادية الموجهة

أصدرت هذا أمر in order to شكلت التقصير يوجه طبقة 3 قارن:

```
#Cat6500(config)#interface [type] mod#/port
```

```
Cat6500(config-if)#ip address ip_address subnet_mask
Cat6500(config-if)#description interface_description
```

كرر هذه الأوامر لكل وظيفة واجهة تحتوي على واجهة مادية موجهة، ثم قم بالخروج. قم بإصدار هذا الأمر:

```
Cat6500(config-if)#^Z
```

قناة EtherChannel الموجهة (L3)

أصدرت in order to شكلت EtherChannel على طبقة 3 قارن، الأمر في هذا قسم.

شكلت منطقي ميناء قناة قارن بهذه الطريقة:

```
#_Cat6500(config)#interface port-channel port_channel_interface
Cat6500(config-if)#description port_channel_description
Cat6500(config-if)#ip address port_channel_ip_address subnet_mask
Cat6500(config-if)#no shutdown
```

أنجزت ال steps في هذا قسم للميناء أن يشكل أن قناة خاص. قم بتطبيق المعلومات المتبقية على قناة المنفذ، كما يوضح المثال التالي:

```
Cat6500(config)#interface range [type] mod/port_range
[Cat6500(config-if)#channel-group 1-64 mode [active | auto | desirable | on | passive
Cat6500(config-if)#no shutdown
Cat6500(config-if)#^Z
```

ملاحظة: بعد أن يشكل أنت EtherChannel، التشكيل أن أنت تطبق إلى القناة قارن يؤثر EtherChannel. يؤثر التكوين الذي تقوم بتطبيقه على منافذ LAN على منفذ LAN فقط حيث تقوم بتطبيق التكوين.

EtherChannel (L2) مع trunking

شكلت الطبقة 2 EtherChannel ل trunking بهذه الطريقة:

```
#_Cat6500(config)#interface port-channel port_channel_interface
Cat6500(config-if)#switchport
Cat6500(config-if)#switchport encapsulation encapsulation_type
Cat6500(config-if)#switchport trunk native vlan vlan_id
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

أنجزت ال steps في هذا قسم فقط للميناء أن يشكل أن قناة خاص.

```
Cat6500(config)#interface range [type] mod/port_range
[Cat6500(config-if)#channel-group 1-64 mode [active | auto | desirable | on | passive
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

ملاحظة: بعد أن يشكل أنت EtherChannel، التشكيل أن أنت تطبق إلى القناة قارن يؤثر EtherChannel. يؤثر التكوين الذي تقوم بتطبيقه على منافذ LAN على منفذ LAN فقط حيث تقوم بتطبيق التكوين.

دققت الخلق من كل EtherChannels و trunks. وفيما يلي مثال على هذا:

```
Cat6500#show etherchannel summary
Cat6500#show interface trunk
```

منافذ الوصول

إن القارن عمل يكون منفذ منفذ أن يكون شكلت كقارن وحيد، أصدرت هذا أمر:

```
#Cat6500(config)#interface [type] mod#/port
Cat6500(config-if)#switchport mode access
Cat6500(config-if)#switchport access vlan vlan_id
Cat6500(config-if)#exit
```

كرر هذه الأوامر لكل واجهة يلزم تكوينها كمنفذ محول من الطبقة 2.

إن المفتاح ميناء أن يكون ربطت إلى نهاية محطة، أصدرت هذا أمر:

```
Cat6500(config-if)#spanning-tree portfast
```

منفذ خط الاتصال (الواجهة المادية الفردية)

إن القارن عمل يكون شنطة ميناء أن يكون شكلت كقارن وحيد، أصدرت هذا أمر:

```
#Cat6500(config)#interface [type] mod#/port
Cat6500(config-if)#switchport
Cat6500(config-if)#switchport trunk encapsulation dot1q
Cat6500(config-if)#switchport trunk native vlan vlan_id
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

كرر هذه الأوامر لكل وظيفة واجهة يلزم تكوينها كمنفذ خط اتصال.

معلومات كلمة المرور

أصدرت هذا أمر ل كلمة معلومة:

```
Cat6500(config)#service password-encryption
Cat6500(config)#enable secret password

CbrCat6500(config)#line con 0
Cat6500(config-line)#password password

CbrCat6500(config-line)#line vty 0 4
Cat6500(config-line)#password password
Cat6500(config-line)#^Z
```

حفظ التكوين

أصدرت هذا أمر in order to أنقذت التشكيل:

```
Cat6500#copy running-config startup-config
```

ميزات البرنامج الجديدة في برنامج Cisco IOS الإصدار 12.1(13)E

راجع تكوين دعم هاتف Cisco IP للحصول على مزيد من المعلومات حول دعم هاتف IP.

راجع التعرف على التطبيق المستند إلى شبكة والتعرف على التطبيق المستند إلى شبكة للحصول على مزيد من المعلومات حول التعرف على التطبيق المستند إلى شبكة (NBAR) لمنافذ LAN.

ملاحظات:

- ال nbar ل lan ميناء ساندت في برمجية على ال MSFC2.
- يوفر PFC2 دعم الأجهزة لقوائم التحكم في الوصول (ACL) للإدخال على منافذ الشبكة المحلية (LAN) حيث تقوم بتكوين NBAR.
- عندما PFC QoS مكنت، الحركة مرور عبر lan ميناء حيث أنت تشكل NBAR يمر من خلال المدخل ومخرج قائمة انتظار وإسقاط الحد.
- عندما يتم تمكين جودة خدمة PFC، فإن MSFC2 يضبط فئة مخرج من الخدمة (CoS) تساوي أسبقية مخرج IP.
- عقب يمر حركة مرور خلال مدخل قائمة انتظار، كل حركة مرور تتم معالجتها في برمجية على ال MSFC2 على lan ميناء حيث أنت تشكل NBAR.
- يتوفر NBAR الموزع على واجهات FlexWAN مع برنامج Cisco IOS الإصدار 12.1(6)E والإصدارات الأحدث.

تتضمن تحسينات تصدير بيانات NetFlow (NDE):

- destination-source-interface وأقنعة تدفق الواجهة الكاملة
- NDE الإصدار 5 من ال PFC2
- NetFlow عينة
- خيار ملء هذه الحقول الإضافية في سجلات NDE:عنوان IP الخاص بموجه الخطوة التاليةIngress Interface SNMP IfIndexSNMP IfIndex لواجهة الخروجرقم النظام الذاتي المصدر

راجع تكوين NDE للحصول على مزيد من المعلومات حول هذه التحسينات.

وتتضمن تحسينات الميزات الأخرى ما يلي:

- بشكل UDLD
- بشكل VTP
- تكوين خدمات ذاكرة التخزين المؤقت للويب باستخدام WCCP

هذه الأوامر هي أوامر جديدة:

- **الحد الأدنى لإعادة تحميل التأخير الاحتياطي**
- **فصل الارتباط**
- **vlan داخلي توزيع سياسة {ascending | تنازلي}**
- **نظام Jumbomtu**
- **مقياس حركة المرور clear Catalyst 6000**

هذه الأوامر هي أوامر محسنة:

- **show vlan داخلي إستعمال**— تم تحسين هذا الأمر لتضمين شبكات VLAN التي تستخدمها واجهات WAN.
- **show vlan id**— تم تحسين هذا الأمر لدعم إدخال نطاق من شبكات VLAN.
- **show l2protocol-tunnel**— تم تحسين هذا الأمر لدعم إدخال معرف VLAN.

يدعم برنامج IOS الإصدار E(13)12.1 من Cisco ميزات البرامج التالية، والتي تم دعمها سابقا في برنامج Cisco IOS الإصدار EX 12.1 الإصدارات:

- تكوين قنوات EtherChannels من الطبقة 2 التي تتضمن واجهات على وحدات تحويل مختلفة مجهزة بواسطة DFCأحلت ال حللت تحذير عام في إطلاق E(13)12.1 قسم من cisco بق CSCdt27074 id (يسجل زبون فقط).
- تكرار معالج التوجيه المحسن (RPR+)ارجع إلى تكوين تكرار محرك المشرف RPR أو RPR+.**ملاحظة:** في الإصدار E(13)12.1 من البرنامج Cisco IOS Software والإصدارات الأحدث، تستبدل ميزات تكرار RPR و RPR+ إمكانية التوفر المحسن المحسن للنظام (EHSA).
- 4،096 طبقة 2 VLANsارجع إلى تكوين شبكات VLAN.**ملاحظة:** يدعم الإصدار E(13)12.1 من البرنامج Cisco IOS Software والإصدارات الأحدث تكوين واجهات 4096 من الطبقة 3 للشبكة المحلية الظاهرية (VLAN). قم بتكوين إجمالي إجمالي لا يزيد عن 2000 واجهة شبكة VLAN من الطبقة 3 ومنافذ من الطبقة 3 على MSFC2 باستخدام Supervisor Engine II أو Supervisor Engine I. قم بتكوين إجمالي إجمالي لا يزيد عن 1000 واجهة شبكة VLAN من الطبقة 3 ومنافذ من الطبقة 3 على MSFC.
- اتصال IEEE 802.1Q النفقيأحلت بشكل IEEE 802.1Q tunneling و طبقة 2 بروتوكول tunneling.
- اتصال بروتوكول IEEE 802.1Q النفقيأحلت بشكل IEEE 802.1Q tunneling و طبقة 2 بروتوكول tunneling.
- بروتوكول شجرة الامتداد المتعدد (MST) وفقا لمعيار IEEE 802.1sارجع إلى تكوين بروتوكول الشجرة المتفرعة (STP) و IEEE 802.1s MST.
- بروتوكول الشجرة المتفرعة (STP) السريع (RSTP) وفقا لمعيار IEEE 802.1wارجع إلى تكوين بروتوكول الشجرة المتفرعة (STP) و IEEE 802.1s MST.
- بروتوكول التحكم في تجميع الارتباطات (LACP) وفقا لمعيار IEEE 802.3adأحلت بشكل طبقة 3 و طبقة 2 EtherChannel.
- تصفية PortFast BPDUراجع تكوين ميزات بروتوكول الشجرة المتفرعة (STP).
- الإنشاء التلقائي لواجهات الطبقة 3 لشبكة VLAN لدعم قوائم التحكم في الوصول إلى شبكة VLAN (VACLs)راجع تكوين أمان الشبكة.
- VACL التقاط ميناء أن يستطيع كنت أي طبقة 2 إثرنيت ميناء في أي VLANراجع تكوين أمان الشبكة.
- حجم وحدة الحد الأقصى للنقل (MTU) القابل للتكوين على المنافذ الفردية من الطبقة الثالثةارجع إلى نظرة عامة على تكوين الواجهة.
- تشكيل من فسحة بين دعامتين غاية ميناء بما أن كل فسحة بين دعامتين حركة مرور يكون حددتأحلت بشكل فسحة بين دعامتين محلي وبعيد.

معلومات ذات صلة

- الأدوات والموارد - Cisco Systems
- دعم منتجات المحولات
- 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).