# 運行CatOS配置和管理的Catalyst 4500/4000、5500/5000和6500/6000系列交換機的最佳實踐

## 目錄

# 簡介

本檔案將討論網路中Cisco Catalyst系列交換器的實作，尤其是Catalyst 4500/4000、5500/5000和6500/6000平台。假設您正在運行Catalyst OS(CatOS)通用部署軟體6.4(3)或更高版本，則會討論配置和命令。雖然介紹了一些設計注意事項，但本文檔並未涵蓋整個園區設計。

# 必要條件

## 需求

本檔案假定已熟悉Catalyst 6500系列命令參考7.6。

雖然整個檔案都提供了供進一步閱讀的公共線上材料的參考，但這些參考是其他基礎和教育參考：

- Cisco ISP基本版 — 每個ISP都應考慮的基本IOS功能。
- 思科網路監控和事件關聯指南
- 千兆校園網設計 — 原則與架構
- Cisco SAFE:企業網路的安全藍圖

## 採用元件

本文件所述內容不限於特定軟體和硬體版本。

## 慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

## 背景資訊

這些解決方案體現了思科工程師多年來的現場經驗，這些工程師為我們許多最大的客戶和複雜網路工作。因此，本文檔重點介紹使網路成功的真實配置。本文提供以下解決方案：

- 從統計學上講，這些解決辦法在實地照射最廣泛，因此風險最低。
- 簡單的解決方案，以一定的靈活性換取確定的結果。
- 易於管理和由網路運營團隊配置的解決方案。
- 提高高可用性和高穩定性的解決方案。

本檔案分為以下四個部分：

- 基本配置 — 大多數網路使用的功能，例如生成樹協定(STP)和中繼。
- 管理配置 — 設計注意事項，以及使用簡單網路管理協定(SNMP)、遠端監控(RMON)、系統日誌、思科發現協定(CDP)和網路時間協定(NTP)進行系統和事件監控。
- 安全配置 — 密碼、埠安全、物理安全以及使用TACACS+的身份驗證。
- 配置核對清單 — 建議配置模板的摘要。

# 基本配置

本節將討論大多數Catalyst網路所部署的功能。

## Catalyst控制平面通訊協定

本節介紹在正常操作下交換機之間運行的協定。對這些協定的基本瞭解有助於瞭解每個部分。

### 管理引擎流量

在Catalyst網路中啟用的大多數功能需要兩台或多台交換機配合使用，因此必須存在保持連線消息、配置引數和管理更改的受控交換。無論這些協定是Cisco專有協定（如CDP）還是基於標準的(如IEEE 802.1d(STP))，在Catalyst系列上實施時，都存在某些共同的元素。

在基本幀轉發中，使用者資料幀源自終端系統，它們的源地址和目的地址不會在整個第2層(L2)交換域中更改。每個交換機Supervisor Engine上的內容可定址儲存器(CAM)查詢表由源地址學習過程填充，並指明哪個出口埠必須轉發接收的每個幀。如果地址學習過程不完整（目標未知或幀將發往廣播或組播地址），則會從該VLAN中的所有埠轉發（泛洪）。

交換機還必須識別哪些幀將通過系統交換，哪些幀必須直接傳送到交換機CPU本身（也稱為網路管理處理器[NMP]）。

Catalyst控制平面是使用CAM表中名為**system entries**的特殊條目建立的，目的是在內部交換機埠上接收流量並將其定向到NMP。因此，通過將協定與已知的目標MAC地址結合使用，可以將控制平面流量與資料流量分離。在交換機上發出show CAM system命令以確認這一點，如下所示：

```
>show cam system

* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry
VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  -----------------    -----  -------------------------------------------
1     00-d0-ff-88-cb-ff  #          1/3
!--- NMP internal port. 1 01-00-0c-cc-cc-cc # 1/3 !--- CDP and so on. 1 01-00-0c-cc-cc-cd # 1/3
!--- Cisco STP. 1 01-80-c2-00-00-00 # 1/3 !--- IEEE STP. 1 01-80-c2-00-00-01 # 1/3 !--- IEEE
flow control. 1 00-03-6b-51-e1-82 R# 15/1 !--- Multilayer Switch Feature Card (MSFC) router. ...
```

思科具有保留的乙太網MAC地址和協定地址範圍，如圖所示。本文檔稍後將介紹每個選項。不過，為方便起見，該表格提供了彙總資訊。

| 功能 | SNAP HDLC協定型別 | 目的地多點傳送MAC |
|---|---|---|
| 連線埠彙總通訊協定(PAgP) | 0x0104 | 01-00-0c-cc-cc-cc |
| 生成樹PVSTP+ | 0x010b | 01-00-0c-cc-cc-cd |
| VLAN橋接器 | 0x010c | 01-00-0c-cd-cd-ce |
| 單向連結偵測(UDLD) | 0x0111 | 01-00-0c-cc-cc-cc |
| 思科探索通訊協定 | 0x2000 | 01-00-0c-cc-cc-cc |
| 動態Trunk(DTP) | 0x2004 | 01-00-0c-cc-cc-cc |
| STP上行鏈路快速 | 0x200a | 01-00-0c-cd-cd-cd |
| IEEE生成樹802.1d | 不適用 — DSAP 42 SSAP 42 | 01-80-c2-00-00-00 |
| 交換器間連結(ISL) | 不適用 | 01-00-0c-00-00-00 |

| | | |
|---|---|---|
| VLAN主幹(VTP) | 0x2003 | 01-00-0c-cc-cc-cc |
| IEEE暫停，802.3x | 不適用 — DSAP 81 SSAP 80 | 01-80-C2-00-00-00>0F |

大多數Cisco控制協定使用IEEE 802.3 SNAP封裝，包括**LLC 0xAAAA03、OUI 0x00000C**，可以在LAN分析器跟蹤中看到。這些協定的其他常見屬性包括：

- 這些協定採用點對點連線。請注意，慎重使用組播目標地址可使兩個Catalyst在非Cisco交換機上透明通訊，因為不瞭解並攔截幀的裝置只會泛洪它們。但是，通過多供應商環境的點對多點連線可能會導致不一致的行為，通常必須加以避免。
- 這些通訊協定終止於第3層(L3)路由器；它們僅在交換機域內運行。
- 這些協定通過輸入特定應用積體電路(ASIC)處理和排程接收優先於使用者資料的優先順序。

引入控制協定目標地址後，還必須描述源地址以保持完整性。交換機協定使用從機箱上EPROM提供的可用地址組獲取的MAC地址。發出show module命令，以顯示每個模組在來源流量(例如STP橋接器通訊協定資料單元(BPDU)或ISL訊框)時可用的位址範圍。

```
>show module

...
Mod MAC-Address(es)                         Hw     Fw          Sw
--- --------------------------------------- ------ ----------  -----------------
1   00-01-c9-da-0c-1e to 00-01-c9-da-0c-1f 2.2    6.1(3)      6.1(1d)
    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
!--- MACs for sourcing traffic. ... VLAN 1
```

## VLAN 1

VLAN 1在Catalyst網路中具有特殊意義。

Catalyst Supervisor Engine在中繼時總是使用預設VLAN(VLAN 1)來標籤許多控制和管理協定，例如CDP、VTP和PAgP。預設情況下，所有埠（包括內部sc0介面）都配置為VLAN 1的成員。預設情況下，所有中繼都承載VLAN 1，而在5.4之前的CatOS軟體版本中，無法阻止VLAN 1中的使用者資料。

為了幫助澄清Catalyst網路中一些常用的術語，需要以下定義：

- sc0所在的管理VLAN;此VLAN可以更改。
- 本徵VLAN定義為埠在不中繼時返回的VLAN，並且是802.1Q中繼上的未標籤VLAN。預設情況下，VLAN 1是本徵VLAN。
- 若要變更本徵VLAN，請發出set vlan *vlan-id mod/port*指令。**注意：**在將VLAN設定為中繼的本徵VLAN之前，請先建立VLAN。

以下是調整網路和變更VLAN 1中連線埠行為的幾個良好理由：

- 當VLAN 1的直徑像任何其他VLAN一樣大到足以對穩定性造成風險時（尤其是從STP的角度而言），需要將其修回。本檔案的頻內管理一節將對此進行詳細討論。
- VLAN 1上的控制平面資料必須與使用者資料分開，以簡化故障排除並最大化可用CPU週期。
- 如果設計多層園區網路時沒有STP，則必須避免VLAN 1中的L2環路；如果存在多個VLAN和IP子網，則接入層仍然需要建立中繼。為此，請手動清除TRUNK埠中的VLAN 1。

總之，請注意有關中繼的以下資訊：

- **CDP、VTP和PAgP更新**始終在具有VLAN 1標籤的中繼上轉發。即使VLAN 1從中繼中清除且不是本徵VLAN，情況也會如此。如果清除VLAN 1中的使用者資料，則不會影響仍使用VLAN 1傳送的控制平面流量。
- 在ISL主幹上，DTP資料包在VLAN1上傳送。即使VLAN 1從主幹中清除並且不再是本徵VLAN，情況也是如此。在802.1Q中繼上，DTP資料包在本徵VLAN上傳送。即使從主幹中清除原生VLAN，也會如此。
- 在PVST+中，除非從中繼中清除**VLAN 1，否則802.1Q IEEE BPDU**會在公共生成樹VLAN 1上無標籤轉發，以便與其他供應商進行互操作。無論本徵VLAN配置如何，情況都是如此。**Cisco PVST+ BPDU會為**所有其他VLAN傳送和標籤。如需更多詳細資訊，請參閱本檔案的生成樹通訊協定一節。
- 802.1s多生成樹(MST)BPDU始終在ISL和802.1Q中繼的VLAN 1上傳送。即使從TRUNK中清除VLAN 1也是如此。
- 請勿在MST網橋和PVST+網橋之間的中繼上清除或禁用VLAN 1。但是，在VLAN 1被禁用的情況下，MST網橋必須成為根橋，以便所有VLAN避免MST網橋將其邊界埠置於根不一致狀態。如需詳細資訊，請參閱瞭解多生成樹通訊協定(802.1s)。

### 建議

若要使VLAN處於**up/up**狀態，且沒有客戶端或主機連線到該VLAN(VLAN)，您需要至少有一個物理裝置連線到該VLAN。否則，VLAN會處於**up/down狀**態。目前，當交換器中沒有用於VLAN的活動連線埠時，沒有用於將VLAN介面**up/up**的命令。

如果您不想連線裝置，請用環回插頭連線到該VLAN的任何埠。或者，嘗試使用交叉纜線，將同一交換器上該VLAN中的兩個連線埠連結在一起。此方法會強制連線埠開啟。如需詳細資訊，請參閱T1/56K線路的回送測試的回送插頭一節。

當一個網路是服務提供商的多宿主網路時，該網路充當兩個服務提供商之間的中轉網路。如果資料包中接收的VLAN號在從服務提供商傳送到其他服務提供商時需要轉換或更改，建議使用QinQ功能轉換VLAN號。

## VLAN Trunk通訊協定

建立VLAN之前，請確定要用於網路的VTP模式。VTP允許在一台或多台交換機上集中更改VLAN配置。這些更改會自動傳播到域中的所有其它交換機。

### 操作概述

VTP是維護VLAN配置一致性的第2層消息協定。VTP可在整個網路範圍內管理VLAN的新增、刪除和重新命名。VTP最大限度地減少了可能引起許多問題的錯誤配置和配置不一致問題，例如VLAN名稱重複、VLAN型別規格不正確和安全違規。VLAN資料庫是一個二進位制檔案，與配置檔案分開儲存在VTP伺服器的NVRAM中。

VTP協定使用乙太網目標組播MAC地址(**01-00-0c-cc-cc-cc**)和SNAP HDLC協定型別Ox2003在交換機之間通訊。它無法在非中繼埠上工作（VTP是ISL或802.1Q的負載），因此在DTP使中繼聯機之前無法傳送消息。

消息型別包括每五分鐘的總結通告、子集通告和請求通告（發生更改時），以及啟用VTP修剪時加入。VTP配置修訂版號隨著伺服器上的每次更改遞增1，然後該修訂版號會在域中傳播新表。

如果刪除了VLAN，則曾經是該VLAN成員的埠將置於非活動狀態。同樣，如果處於客戶端模式的交

換機在啟動時無法接收VTP VLAN表（從VTP伺服器或其他VTP客戶端），則除預設VLAN 1外，VLAN中的所有埠都會被停用。

下表提供了各種VTP模式的功能比較摘要：

| 功能 | 伺服器 | 使用者端 | 透明 | 關閉[1] |
|---|---|---|---|---|
| 源VTP消息 | 是 | 是 | 否 | 否 |
| 收聽VTP消息 | 是 | 是 | 否 | 否 |
| 轉發VTP消息 | 是 | 是 | 是 | 否 |
| 建立VLAN | 是 | 否 | 是（僅限本地有效） | 是（僅限本地有效） |
| 記住VLAN | 是 | 否 | 是（僅限本地有效） | 是（僅限本地有效） |

在VTP `transparent`模式下，VTP更新會被忽略（VTP組播MAC地址會從系統CAM中刪除，系統CAM通常用於拾取控制幀並將其引導至Supervisor引擎）。 由於協定使用組播地址，處於透明模式的交換機（或其他供應商交換機）只需將幀泛洪到域中的其他Cisco交換機。

[1] CatOS軟體7.1版引入了使用off模式停用VTP的項。在VTP `off`模式下，交換機的行為方式與VTP `transparent`模式非常相似，不同之處在於`off`模式也會抑制VTP更新的轉發。

下表概述了初始配置：

| 功能 | 預設值 |
|---|---|
| VTP域名 | 空 |
| VTP模式 | 伺服器 |
| VTP版本 | 版本1已啟用 |
| VTP口令 | 無 |
| VTP修剪 | 已禁用 |

VTP第2版(VTPv2)具備此功能的靈活性。但是無法與VTP第1版(VTPv1)互操作：

- 權杖環支援
- 無法識別的VTP資訊支援；現在，交換機會傳播無法解析的值。
- 版本相關的透明模式；模式不再檢查域名。這樣可支援透明域中的多個域。
- 版本號傳播；如果所有交換機都支援VTPv2，則可以通過配置一台交換機來啟用所有交換機。

如需詳細資訊，請參閱瞭解和設定VLAN中繼線通訊協定(VTP)。

## VTP版本3

CatOS軟體版本8.1引入了對VTP版本3(VTPv3)的支援。VTPv3提供現有版本的增強功能。這些增強功能允許：

- 支援延伸型VLAN

- 支援建立和通告專用VLAN
- 支援VLAN例項和MST對映傳播例項（CatOS版本8.3支援）
- 改進的伺服器身份驗證
- 防止將「錯誤」資料庫意外插入VTP域
- 與VTPv1和VTPv2互動
- 能夠基於每個埠進行配置

VTPv3實施與早期版本的主要區別之一是引入了VTP主伺服器。理想情況下，如果VTPv3域未進行分割槽，則該域中只能有一個主伺服器。您對VTP域所做的任何更改都必須在VTP主伺服器上執行，以便傳播到VTP域。VTPv3域內可以有多個伺服器，也稱為輔助伺服器。當交換機配置為伺服器時，預設情況下交換機將成為輔助伺服器。輔助伺服器可以儲存域的配置，但無法修改配置。從交換機成功接管後，從屬伺服器可以成為主伺服器。

運行VTPv3的交換機只接受修訂版號比當前主伺服器更高的VTP資料庫。此程式與VTPv1和VTPv2明顯不同，後者是交換機始終接受來自同一域中鄰居的上級配置。VTPv3的這一更改提供了保護。使用更高的VTP修訂版號引入網路的新交換機不能覆蓋整個域的VLAN配置。

VTPv3還引入了對VTP處理口令的增強功能。如果使用隱藏密碼配置選項將密碼配置為「隱藏」，則會出現以下專案：

- 密碼在配置中不會以純文字檔案顯示。密碼的機密十六進位制格式儲存在配置中。
- 如果嘗試將交換機配置為主伺服器，系統會提示您輸入密碼。如果您的密碼與加密密碼匹配，則交換機將成為主伺服器，從而允許您配置域。

**注意：**必須注意的是，只有在需要修改任何例項的VTP配置時，才需要主伺服器。VTP域可以在沒有活動主伺服器的情況下運行，因為輔助伺服器可以確保配置在重新載入後的永續性。主伺服器狀態因以下原因而退出：

- 交換機重新載入
- 活動管理引擎和冗餘管理引擎之間的高可用性切換
- 從其他伺服器執行接管操作
- 模式配置的更改
- 任何VTP域配置更改，例如：版本域名域密碼

VTPv3還允許交換機參與多個VTP例項。在這種情況下，同一台交換機既可以是某個例項的VTP伺服器，也可以是另一個例項的客戶端，因為VTP模式特定於不同的VTP例項。例如，當交換器設定為VLAN例項的伺服器模式時，交換器可以為MST例項在模式下運作。

在與VTPv1和VTPv2的互動方面，所有版本的VTP的預設行為都是，早期版本的VTP只會丟棄新版本的更新。除非VTPv1和VTPv2交換機處於模式，否則所有VTPv3更新都會被丟棄。另一方面，VTPv3交換機在主幹上收到舊式VTPv1或VTPv2幀後，會將資料庫更新的縮小版本傳遞給VTPv1和VTPv2交換機。但是，此資訊交換是單向的，因為VTPv3交換機不接受來自VTPv1和VTPv2交換機的更新。在中繼連線上，VTPv3交換機繼續傳送縮減更新以及完整的VTPv3更新，以通過中繼埠滿足VTPv2和VTPv3鄰居的存在。

為了為擴展VLAN提供VTPv3支援，VTP為每個VLAN分配70位元組的VLAN資料庫格式將更改。該更改僅允許對非預設值進行編碼，而不允許為傳統協定傳送未修改欄位。由於此更改，4K VLAN支援是結果VLAN資料庫的大小。

## 建議

對於使用VTP客戶端/伺服器模式還是VTP沒有特定建議。儘管稍後會提到一些注意事項，但有些客VTP client/server模式的易管理性。建議在每個域中配置兩台模式交換機以實現冗餘，通常為兩台

分佈層交換機。域中的其餘交換機必須設定為client模式。在使用VTPv2實施/模式時，請注意同一VTP域中始終接受更高的修訂版號。如果配置為VTP client或server模式的交換機被引入到VTP域中，且其修訂版號高於現有的VTP伺服器，則這會覆蓋VTP域中的VLAN資料庫。如果無意更改了配置，並且刪除了VLAN，則覆蓋可能會導致網路中斷。為了確保client或server交換機的配置修訂版號始終低於伺服器的修訂版號，請將客戶端VTP域名更改為標準名稱以外的名稱。然後恢復為標準。此操作將客戶端上的配置修訂版設定為0。

VTP在網路中輕鬆進行更改的能力有優缺點。許多企業青睞VTP透明模式的方法，原因如下：

- 它鼓勵良好的更改控制實踐，因為要在交換機或中繼埠上修改VLAN的要求必須被視為一次只能修改一台交換機。
- 它可以限制影響整個域的管理員錯誤的風險，如意外刪除VLAN。
- 如果網路引入的新交換機的VTP修訂版號較高，則不會覆蓋整個域VLAN配置。
- 它鼓勵將VLAN從運行的中繼修剪到該VLAN中沒有埠的交換機。這使得幀泛洪更加節省頻寬。手動修剪也很有用，因為它減小了生成樹直徑(請參閱本文檔的DTP部分)。 在埠通道中繼上修剪未使用的VLAN之前，請確保任何連線到IP電話的埠都配置為具有語音VLAN的接入埠。
- CatOS 6.x和CatOS 7.x（編號為1025到4094）中的擴展VLAN範圍只能以這種方式配置。有關詳細資訊，請參閱本文檔的擴展VLAN和MAC地址減少部分。
- Cisco Works 2000的Campus Manager 3.1支援VTP transparent模式。VTP域中至少需要一台伺服器的舊限制已刪除。

| **VTP命令示例** | **意見** |
|---|---|
| set vtp domain *name* password *x* | CDP會檢查名稱，以幫助檢查域之間的纜線連線錯誤。簡單的密碼有助於防止意外更改。貼上時請注意區分大小寫的名稱或空格。 |
| set vtp mode transparent | |
| set vlan *vlan number* name *name* | 每個在VLAN中有埠的交換機。 |
| set trun | 允許中繼在需要時承載VLAN — 預設值為所有VLAN。 |

| | |
|---|---|
| k *mod/port vlan range* | |
| clear trunk *mod/port vlan range* | 通過手動修剪來限制STP直徑，例如從分佈層到接入層（VLAN不存在）的中繼上。 |

**註：使**用**set**命令指定VLAN只會新增VLAN，而不會清除它們。例如，set trunk x/y 1-10 命令不會將允許清單僅設定為VLAN 1-10。發出clear trunk x/y 11-1005 命令可達到預期結果。

雖然權杖環交換不在本檔案的範圍之內，但請注意，不建議對TR-ISL網路使用VTP `transparent` 模式。權杖環交換的基礎是整個網域形成一個分散式的多埠網橋，因此每台交換器都必須具有相同的VLAN資訊。

## 其他選項

令牌環環境中需要VTPv2，強烈建議使用/伺服器模式。

VTPv3能夠實施更嚴格的身份驗證和配置修訂控制。VTPv3本質上提供與VTPv1/VTPv2透明模式相同的功能級別，但安全性更到增強。此外，VTPv3與舊版VTP部分相容。

本文主張修剪VLAN以減少不必要的幀泛洪的優點。set vtp pruning enable 命令會自動修剪VLAN，從而停止不需要幀的無效泛洪。與手動VLAN修剪不同，自動修剪不會限制生成樹直徑。

從CatOS 5.1,Catalyst交換機可以將大於1000的802.1Q VLAN編號對映到ISL VLAN編號。在CatOS 6.x中，根據IEEE 802.1Q標準，Catalyst 6500/6000交換機支援4096個VLAN。這些VLAN分為以下三個範圍，其中只有一部分會傳播到使用VTP的網路中的其他交換機：

- 正常範圍的VLAN:1–1001
- 擴展範圍VLAN:1025-4094（只能由VTPv3傳播）
- 保留範圍的VLAN:0、1002—1024、4095

IEEE已經制定了基於標準的體系結構，以便實現與VTP類似的結果。作為802.1Q通用屬性註冊協定(GARP)的成員，通用VLAN註冊協定(GVRP)允許供應商之間的VLAN管理互通性，但不在本文檔的討論範圍之內。

**注意**：CatOS 7.x引入了將VTP設定為off模式項，該模式非常類似於。但是，交換機不會轉發VTP幀。當中繼到您的管理控制之外的交換機時，在某些設計中此功能很有用。

## 擴展VLAN和MAC地址減少

MAC地址縮減功能支援擴展範圍的VLAN標識。啟用MAC地址縮減功能會禁用用於VLAN生成樹的MAC地址池，並保留單個MAC地址。此MAC地址標識交換機。CatOS軟體版本6.1(1)引入對

Catalyst 6500/6000和Catalyst 4500/4000交換器的MAC位址縮減支援，以符合IEEE 802.1Q標準支援4096 VLAN。

## 操作概述

交換器通訊協定使用從機箱上的EPROM提供的可用位址群組取得的MAC位址，該位址作為在PVST+下執行的VLAN的橋接器識別符的一部分。Catalyst 6500/6000和Catalyst 4500/4000交換器支援1024或64個MAC位址，取決於機箱型別。

預設情況下，具有1024個MAC地址的Catalyst交換機不會啟用MAC地址減少。MAC地址按順序分配。範圍中的第一個MAC地址分配給VLAN 1。範圍中的第二個MAC地址分配給VLAN 2，以此類推。這樣，交換機就可以使用唯一的網橋識別符號支援每個VLAN中的1024個VLAN。

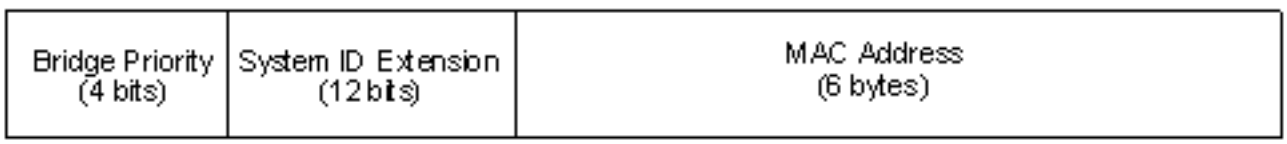
| **機箱型別** | **機箱地址** |
|---|---|
| WS-C4003-S1、WS-C4006-S2 | 1024 |
| WS-C4503、WS-C4506 | 641 |
| WS-C6509-E、WS-C6509、WS-C6509-NEB、WS-C6506-E、WS-C6506、WS-C6009、WS-C6006、OSR-7609-AC、OSR-7609-DC | 1024 |
| WS-C6513、WS-C6509-NEB-A、WS-C6504-E、WS-C6503-E、WS-C6503、CISCO7603、CISCO7606、CISCO7609、CISCO7613 | 641 |

[1]具有64個MAC地址的交換機預設啟用MAC地址減少，該功能無法禁用。

對於具有1024個MAC地址的Catalyst系列交換機，啟用MAC地址縮減功能可支援在PVST+或16個多例項STP(MISTP)例項下運行的4096個VLAN具有唯一識別符號，而不會增加交換機上所需的MAC地址數量。MAC地址縮減將STP所需的MAC地址數量從每個VLAN或MISTP例項一個減少到每台交換機一個。

下圖顯示未啟用網橋識別符號MAC地址縮減。網橋識別符號由2位元組的網橋優先順序和6位元組的MAC地址組成：


MAC地址縮減會修改BPDU的STP網橋識別符號部分。原始2位元組優先順序欄位被拆分為兩個欄位。此拆分導致4位橋接器優先順序欄位和12位系統ID擴展，允許VLAN編號從0到4095。




當您在Catalyst交換機上啟用MAC地址縮減以利用擴展範圍VLAN時，請在同一STP域內的所有交換

機上啟用MAC地址縮減。要使所有交換機上的STP根計算保持一致，必須執行此步驟。啟用MAC地址縮減後，根網橋優先順序將變為4096與VLAN ID的倍數。未減少MAC地址的交換機可能會無意中宣告根，因為這些交換機在選擇網橋ID時具有更細的粒度。

## 配置指南

設定延伸的VLAN範圍時，必須遵循特定原則。交換機可以從擴展範圍分配一個VLAN塊用於內部用途。例如，交換機可以為路由埠或Flex WAN模組分配VLAN。VLAN塊的分配始終從VLAN 1006開始，然後開始。如果您的VLAN在Flex WAN模組要求的範圍內，則不會分配所有所需的VLAN，因為從未從使用者VLAN區域分配這些VLAN。在交換器上發出show vlan 命令或show vlan summary命令，以顯示使用者指定的和內部VLAN。

```
>show vlan summary

Current Internal Vlan Allocation Policy - Ascending

Vlan status    Count  Vlans
-------------  -----  -----------------------------------------
VTP Active         7   1,17,174,1002-1005

Internal           7   1006-1011,1016
!--- These are internal VLANs. >show vlan
---- -------------------------------- --------- ------- --------

1    default                          active    7       4/1-48


!--- Output suppressed. 1006 Online Diagnostic Vlan1 active 0 internal 1007 Online Diagnostic
Vlan2 active 0 internal 1008 Online Diagnostic Vlan3 active 0 internal 1009 Voice Internal Vlan
active 0 internal 1010 Dtp Vlan active 0 internal 1011 Private Vlan Internal Vlan suspend 0
internal 1016 Online SP-RP Ping Vlan active 0 internal !--- These are internal VLANs.
```

此外，在使用擴展範圍VLAN之前，必須刪除任何現有的802.1Q到ISL對映。此外，在低於VTPv3的版本中，必須使用VTP透明模式在每台交換機上靜態配置VLAN。如需詳細資訊，請參閱設定VLAN的*延伸範圍VLAN設定指南*一節。

**注意：**在低於軟體版本8.1(1)的軟體中，無法為擴展範圍VLAN配置VLAN名稱。此功能與任何VTP版本或模式無關。

## 建議

嘗試在同一個STP域內保持一致的MAC地址縮減配置。但是，如果將64個MAC地址的新機箱引入到STP域，則在所有網路裝置上實施MAC地址縮減可能是不切實際的。具有64個MAC地址的交換機預設啟用MAC地址減少，該功能無法禁用。瞭解當兩個系統配置了相同的生成樹優先順序時，不減少MAC地址的系統具有更好的生成樹優先順序。發出以下命令可啟用或停用MAC位址減少：

```
set spantree macreduction enable | disable
```

內部VLAN的分配按升序排列，從VLAN 1006開始。將使用者VLAN分配到VLAN 4094附近，以避免使用者VLAN與內部VLAN發生衝突。使用執行Cisco IOS®系統軟體的Catalyst 6500交換器，您可以按降序設定內部VLAN分配。CatOS軟體的等效命令列介面(CLI)不受正式支援。

## 自動交涉

## 乙太網路/快速乙太網路

自動交涉是IEEE快速乙太網路(FE)標準(802.3u)的可選功能，此功能可讓裝置透過連結自動交換有關**速度和**雙工**功能**的資訊。自動協商在第1層(L1)運行，以臨時使用者(例如PC)連**接到網**絡的接入層埠為目標。

## 操作概述

導致10/100 Mbps乙太網路連結上的效能問題的最常見原因，是連結上的一個連線埠以半雙工執行，而另一個連線埠以全雙工執行。當連結上的一個或兩個連線埠重設，且自動交涉流程不會造成兩個連結夥伴具有相同的設定時，可能會發生這種情況。當管理員重新配置鏈路的一端，但忘記重新配置另一端時，也會發生這種情況。此問題的典型症狀是交換機上的幀校驗序列(FCS)、循環冗餘校驗(CRC)、對齊或殘存計數器增加。

這些文檔中詳細討論了自動協商。這些檔案中包含有關自動交涉運作方式和組態選項的說明。

- 設定和疑難排解乙太網路10/100 Mb半/全雙工自動交涉功能
- 疑難排解 Cisco Catalyst 交換器與 NIC 的相容性問題

有關自動交涉的常見誤解是，可以將一個連結夥伴手動設定為100 Mbps全雙工，並與另一個連結夥伴自動交涉為全雙工。實際上，嘗試這樣做會導致雙工不相符。這是因為一個連結夥伴自動交涉、從另一個連結夥伴看不到任何自動交涉引數，而且預設為半雙工。

大多數Catalyst乙太網路模組支援10/100 Mbps和半/全雙工，但show port capabilities *mod/port* 命令可確認這點。

## FEFI

遠端故障指示(FEFI)可保護100BASE-FX（光纖）和千兆位介面，而自動協商可保護100BASE-TX（銅纜）免受物理層/信令相關故障的影響。

**遠端故障**是一個站可以偵測到而另一個站無法偵測到的連結錯誤，例如已中斷連線的TX電線。在此示例中，傳送站仍然可以接收有效資料，並通過link-integrity-monitor檢測鏈路是否正常。它不會檢測到其它站沒有收到它的傳輸。檢測到此類遠端故障的100BASE-FX站可以修改其傳輸的IDLE流以傳送特殊位元模式（稱為FEFI IDLE模式）來通知鄰居遠端故障；fefi-IDLE模式隨後會觸發遠端埠關閉（錯誤禁用）。 有關故障保護的詳細資訊，請參閱本文檔的UDLD部分。

此硬體和以下模組支援FEFI:

- Catalyst 5500/5000:WS-X5201R、WS-X5305、WS-X5236、WS-X5237、WS-U5538和WS-U5539
- Catalyst 6500/6000和4500/4000:所有100BASE-FX模組和GE模組

## 建議

是否在10/100連結上設定自動交涉，或是設定為硬碼速度和雙工，最終取決於您連線到Catalyst交換器連線埠的連結夥伴或終端裝置的型別。終端裝置和Catalyst交換器之間的自動交涉一般運作良好，Catalyst交換器符合IEEE 802.3u規範。但是，如果NIC或供應商交換機不能完全符合，則可能會出現問題。硬體不相容和其他問題也會因為廠商專屬的進階功能（例如自動極性或纜線完整性）而產生，而IEEE 802.3u規範未就10/100 Mbps自動交涉進行說明。請參閱現場通知：例如，連線到CAT4K/6K的英特爾Pro/1000T NIC的效能問題。

預計某些情況下會要求設定主機、埠速度和雙工。一般來說，請遵循以下基本故障排除步驟：

- 確保在鏈路的兩端都配置了自動協商或者在兩端都配置了硬編碼。
- 檢視CatOS發行版本註釋以瞭解常見警告。
- 驗證正在運行的NIC驅動程式或作業系統的版本，因為通常需要最新的驅動程式或修補程式。

通常，嘗試首先對任何型別的連結夥伴使用自動協商。為筆記型電腦等臨時裝置配置自動協商功能具有明顯的優勢。理想情況下，自動協商還可與非臨時裝置（如伺服器和固定工作站）或交換機到交換機及交換機到路由器（交換機 — 路由器）很好地合作。由於上述某些原因，可能會出現談判問題。在這些情況下，請按照提供的TAC連結中概述的基本故障排除步驟操作。

如果在10/100 Mbps乙太網路連線埠上將連線埠速度設定為，則速度和雙工都會自動交涉。發出此命令，將連線埠設定為自動：

```
set port speed port range auto
!--- This is the default.
```

如果對連線埠進行硬式編碼，請發出以下組態命令：

```
set port speed port range 10 | 100 set port duplex port range full | half
```

在CatOS 8.3及更新版本中，思科已匯入可選**auto-10-100**關鍵字。在支援速度為10/100/1000 Mbps但不需要自動協商至1000 Mbps的連線埠上使用**auto-10-100**關鍵字。若使用**auto-10-100**關鍵字，則連線埠的運作方式與速度設定為自動的10/100-Mbps連線埠的運作方式**相同**。速度和雙工的交涉僅針對10/100-Mbps連線埠，而1000-Mbps速度不會參與交涉。

```
set port speed port_range auto-10-100
```

### 其他選項

當交換機之間不使用自動協商時，L1故障指示也會因為某些問題而丟失。使用L2協定來增強故障檢測(如主動UDLD)很有用。

## Gigabit乙太網路

Gigabit乙太網路(GE)具有自動交涉程式(IEEE 802.3z)，比10/100 Mbps乙太網路更廣泛，並用於交換流量控制引數、遠端故障資訊和雙工資訊（即使Catalyst系列GE連線埠僅支援全雙工模式）。

**註：**802.3z已被IEEE 802.3:2000規範取代。請參閱IEEE標準On Line LAN/MAN標準訂用：存檔 以瞭解詳細資訊。

### 操作概述

GE埠協商預設啟用，GE鏈路兩端的埠必須具有相同的設定。與FE不同，如果鏈路兩端的埠上的自動協商設定不同，GE鏈路將不會啟動。但是，禁用自動交涉的連線埠建立連結所需的唯一條件是來自遠端的有效Gigabit訊號。此行為與遠端自動交涉組態無關。例如，假設有兩個裝置：A和B。每台裝置皆可啟用或停用自動交涉。下表列出可能的設定和各自的連結狀態：

| 交涉 | B已啟用 | B已禁用 |
|---|---|---|
| **已啟用** | 邊都上 | A down, B up |
| **已禁用** | A up,B down | 邊都上 |

在GE中，同步和自動協商（如果啟用）在鏈路啟動時通過使用保留鏈路代碼字的特殊序列來執行。

**注意**：存在有效詞典並且並非所有可能的詞在GE中都有效。

GE連線的壽命可以用以下方式描述：


失去同步意味著MAC檢測到鏈路關閉。無論是否啟用或停用自動交涉，都會遺失同步。在某些失敗的情況下，例如連續收到三個無效字，同步將會丟失。如果此情況持續10毫秒，則會斷言「同步失敗」情況，並將鏈路更改為link_down狀態。在同步丟失後，需要另外三個連續的有效空閒才能重新同步。其他災難性事件(例如接收丟失(Rx)訊號)會導致連結關閉事件。

自動協商是連結過程的一部分。當連結開啟時，自動交涉即告結束。但是，交換機仍會監視鏈路的狀態。如果連線埠上停用自動交涉，則「自動交涉」階段將不再可行。

GE銅纜規範(1000BASE-T)支援通過下一頁交換進行自動協商。Next Page Exchange允許在銅纜埠上進行10/100/1000 Mbps速度的自動協商。

**注意**：GE光纖規範僅對雙工、流量控制和遠端故障檢測協商做出規定。GE光纖埠不協商埠速度。如需自動交涉的詳細資訊，請參閱IEEE 802.3-2002規範第 28和37節。

同步重新啟動延遲是一種控制總自動協商時間的軟體功能。如果自動協商在此時間內未成功，韌體將重新啟動自動協商，以防出現死鎖。set port sync-restart-delay 命令僅在自動協商設定為enable時才生效。

## 建議

在GE環境中，啟用自動協商比10/100環境中重要得多。事實上，只有在連線到無法支援交涉的裝置或連線問題源自互通性的交換器連線埠上，才能停用自動交涉。思科建議在所有交換機到交換機鏈路上（通常是所有GE裝置）啟用（預設）Gigabit協商。發出以下命令以啟用自動交涉：

```
set port negotiation port range enable
!--- This is the default.
```

一個已知的例外情況是，連線到執行Cisco IOS軟體版本12.0(10)S之前（該版本增加了流量控制和自動交涉）的Gigabit交換器路由器(GSR)時。在這種情況下，關閉這兩個功能，或者交換機埠報告，而GSR報告錯誤。以下是命令序列範例：

```
set port flowcontrol receive port range off set port flowcontrol send port range off set port
negotiation port range disable
```

必須逐個檢視交換機到伺服器的連線。思科客戶在Sun、HP和IBM伺服器上遇到千兆位協商問題。

## 其他選項

流量控制是802.3x規範的可選部分，若使用，必須透過交涉。裝置可以或不能傳送和/或響應PAUSE幀(公認的MAC 01-80-C2-00-00-00 0F)。 此外，它們不能同意遠端鄰居的流量控制請求。具有輸入緩衝區的連線埠正在填滿，會向其連結夥伴傳送一個PAUSE訊框，這樣會停止傳輸，並在連結夥伴輸出緩衝區中保留任何其他訊框。這不會解決任何穩態超訂用問題，但實際上使輸入緩衝區在突發期間比夥伴輸出緩衝區大一些部分。

此功能最適用於存取連線埠和終端主機之間的連結，其中主機輸出緩衝區可能與其虛擬記憶體一樣大。使用交換機到交換機的好處有限。

發出以下命令，以在交換器連線埠上控制此情況：

```
set port flowcontrol mod/port receive | send off |on | desired
```

```
>show port flowcontrol

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

**注意：如**果協商，所有Catalyst模組響應暫停幀。某些模組（例如WS-X5410、WS-X4306）不會傳送PAUSE訊框，即使它們協商傳送，因為它們是無封鎖的。

# 動態Trunk協定

## 封裝型別

中繼通過臨時識別和標籤（本地鏈路）原始乙太網幀來擴展裝置之間的VLAN，從而使它們能夠在單個鏈路上多路複用。這也確保交換機之間維護單獨的VLAN廣播域和安全域。CAM表維護交換機內部的幀到VLAN對映。

幾種型別的L2介質都支援中繼，包括ATM LANE、FDDI 802.10和乙太網，但此處只顯示後者。

## ISL操作概述

Cisco專有標識或標籤方案ISL已使用多年。802.1Q IEEE標準也可用。

通過將原始幀完全封裝在兩級標籤方案中，ISL有效地成為隧道協定，並具有攜帶非乙太網幀的額外優點。它將一個26位元組的報頭和4位元組的FCS新增到標準乙太網幀 — 較大的乙太網幀應該由配置為中繼的埠處理。ISL支援1024個VLAN。

### ISL幀格式

| 40位 | 4位 | 4位 | 48位 | 16位 | 24位 | 24位 | 15位 | 位 | 16位 | 16位 | 可變長度 | 32位 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 目標地址 | 類型 | 使用者 | SA | LEN | 快照LLC | HSA | VLAN | BPDU | 索引 | 儲備 | 封裝的幀 | FCS |
| 01-00-0c-00-00 | | | | | AAAA03 | 00000C | | | | | | |

有關詳細資訊，請參閱InterSwitch鏈路和IEEE 802.1Q幀格式。

## 802.1Q操作概述

IEEE 802.1Q標準規定的封裝型別遠不止於封裝型別，包括生成樹增強功能、GARP（請參閱本文檔的VTP部分）和802.1p服務品質(QoS)標籤。

802.1Q幀格式保留了原始乙太網源地址和目的地址，但交換機現在必須預期收到小巨型幀，即使在主機可以使用標籤來表示802.1p使用者優先順序以進行QoS信令的接入埠上也是如此。標籤是4位元組，因此802.1Q乙太網v2幀是1522位元組，這是IEEE 802.3ac工作組的成果。802.1Q還支援4096 VLAN的編號空間。

除了本徵VLAN上的資料幀之外（根據入口交換機埠配置，存在隱式標籤），所有傳輸和接收的資料幀都具有802.1Q標籤。 本徵VLAN上的幀始終以未標籤的方式傳輸，通常以未標籤的方式接收。但是，它們也可以被接收並標籤。

有關詳細資訊，請參閱通過IEEE 802.10實現VLAN標準化和獲取IEEE 802 。

### 802.1Q/801.1p幀格式

| | | 標籤標題 | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | TPID | TCI | | | | | |
| 48位 | 48位 | 16位 | 3位 | 1位 | 12位 | 16位 | 可變長度 | 32位 |
| DA | SA | TPID | 優先順序機制 | CFI | VLAN ID | 長度/型別 | 使用PAD的資料 | FCS |
| | | 0x8100 | 0 - 7 | 0-1 | 0-4095 | | | |

## 建議

由於所有較新的硬體都支援802.1Q(某些硬體僅支援802.1Q，如Catalyst 4500/4000系列和CSS 11000)，思科建議所有新的實施都遵循IEEE 802.1Q標準，並且舊網路逐步從ISL遷移。

IEEE標準允許廠商互通性。這在所有思科環境中都很有利，因為支援主機802.1p的新網絡卡和裝置已可用。雖然ISL和802.1Q實施均已成熟，但IEEE標準最終將擁有更大的現場曝光度和更大的第三

方支援，例如網路分析器支援。與ISL相比，802.1Q的封裝開銷較低，這也是802.1Q的次要優勢。

由於使用DTP在交換機之間協商封裝型別，如果兩端都支援ISL，則預設情況下會選擇ISL作為獲勝者，因此有必要發出以下命令以指定dot1q:

```
set trunk mod/port mode dot1q
```

如果如本文帶內管理一節所述，將VLAN 1從中繼中清除，儘管沒有傳輸或接收使用者資料，但NMP仍繼續在VLAN 1上傳遞控制協定，例如CDP和VTP。

此外，如本檔案的VLAN 1一節所述，建立中繼時，CDP、VTP和PAgP封包一律在VLAN 1上傳送。使用dot1q封裝時，如果交換機的本徵VLAN發生更改，這些控制幀將使用VLAN 1進行標籤。如果啟用了到路由器的dot1q中繼，並且交換機上的本地VLAN發生了更改，則需要VLAN 1中的子介面來接收標籤的CDP幀，並在路由器上提供CDP鄰居可見性。

**注意：**由於本徵VLAN的隱式標籤可能將幀從一個VLAN傳送到另一個VLAN而沒有路由器，因此dot1q存在潛在的安全問題。請參閱VLAN實施中存在漏洞？ 瞭解更多詳情。因應措施是將VLAN ID用於TRUNK的本地VLAN，而不用於終端使用者訪問。大多數Cisco客戶將VLAN 1保留為主幹上的本徵VLAN，並將接入埠分配給VLAN 1以外的VLAN，以便輕鬆實現這一點。

## 中繼模式

DTP是第二代動態ISL(DISL)，之所以存在，是為了確保傳送ISL或802.1Q幀時涉及的不同引數（如配置的封裝型別、本徵VLAN和硬體功能）由中繼任一端的交換機商定。這還有助於確保埠及其鄰居處於一致狀態，從而防止非中繼埠泛洪已標籤的幀，這是一種潛在嚴重的安全風險。

## 操作概述

DTP是在交換機埠與其鄰居之間協商配置引數的L2協定。它使用另一個組播MAC地址(**01-00-0c-cc-cc-cc**)和SNAP協定型別0x2004。下表彙總了配置模式：

| **模式** | **功能** | **傳輸的DTP幀** | **最終狀態（本地埠）** |
|---|---|---|---|
| | 使埠願意將鏈路轉換為中繼。如果相鄰埠設定為`on`或`desirable`模式，則該埠會成為中繼埠。 | 是的，定期的。 | 中繼 |
| | 使埠進入永久中繼模式，並協商將鏈路轉換為中繼。即使鄰近連線埠不同意變更，連線埠也會成為主干連線埠。 | 是的，定期的。 | 中繼，無**條件地**。 |
| Nonego | 使埠進入永久中繼模式，但阻止埠生成DTP幀。您必須手動將相鄰埠配置為中繼埠以建立中繼鏈路。這對於不支援DTP的裝置很有用。 | 否 | 中繼，無**條件地**。 |

| | | | |
|---|---|---|---|
| tiate | | | |
| Desirable | 使埠主動嘗試將鏈路轉換為中繼鏈路。如果相鄰連線埠設定為on、desirable或auto模式，則連線埠會成為主干連線埠。 | 是的，定期的。 | 只有在遠端模式為on、auto或desirable時，它才會處於中繼狀態。 |
| Off | 使埠進入永久非中繼模式，並協商將鏈路轉換為非中繼鏈路。即使鄰近連線埠不同意變更，連線埠也會變成非主干連線埠。 | 在穩定狀態下為no，但在從on發生更改後傳送通知以加快遠端端。 | 非中繼 |

以下是協定的一些要點：

- DTP採用點對點連線，思科裝置僅支援點對點的802.1Q中繼埠。
- 在DTP交涉期間，連線埠不參與STP。只有在埠成為三種DTP型別（接入、ISL或802.1Q）之一後，該埠才會新增到STP。否則，在連線埠參與STP之前，下一個執行的程式將是PAgP（如果已設定）。
- 如果埠在ISL模式下為主幹模式，則DTP資料包在VLAN 1上傳送，否則（對於802.1Q主幹或非主幹埠）在本地VLAN上傳送。
- 在desirable模式下，DTP資料包傳輸**VTP域名**（必須匹配才能啟動協商的中繼），以及中繼配置和**admin status**。
- 在協商過程中，消息每秒傳送一次，之後每30秒傳送一次。
- 請務必瞭解on、nonegotiate和off模式明確指定連線埠結束時的狀態。錯誤配置可能會導致危險/不一致狀態，其中一端是中繼而另一端不是。
- 處於on、auto或desirable模式的埠會定期傳送DTP幀。如果處於或desirable模式的埠在五分鐘內看不到DTP資料包，則將其設定為非中繼。

有關ISL的詳細資訊，請參閱在Catalyst 5500/5000和6500/6000系列交換機上配置ISL中繼。如需802.1Q的詳細資訊，請參閱使用802.1Q封裝和Cisco CatOS系統軟體的Catalyst 4500/4000、5500/5000和6500/6000系列交換器之間的主幹。

## 建議

思科建議在兩端使用desirable的明確中繼配置。在此模式下，網路操作員可以信任系統日誌和命令列狀態消息，即埠已啟動且處於中繼狀態，這與on模式不同，後者即使鄰居配置錯誤也可能使埠處於啟動狀態。此外，desirable mode trunk在鏈路的一端無法成為trunk或丟棄trunk狀態時提供穩定性。發出以下命令以設定desirable模式：

```
set trunk mod/port desirable ISL | dot1q
```

**注意**：在所有非TRUNK埠上將中繼設定為off。這樣有助於在啟用主機埠時消除浪費的協商時間。使用set port host 命令時也會執行此命令；有關詳細資訊，請參閱STP部分。發出此命令，以停用一系列連線埠上的主幹：

```
set trunk port range off
!--- Ports are not trunking; part of the set port host command.
```

### 其他選項

另一種常見客戶配置僅在分佈層使用desirable模式，在接入層使用最簡單的預設配置(auto模式)。

某些交換器（例如Catalyst 2900XL、Cisco IOS路由器或其他廠商裝置）目前不支援透過DTP的中繼交涉。您可以在Catalyst 4500/4000、5500/5000和6500/6000交換器上使用nonegotiate模式，將連線埠設定為無條件與這些裝置進行中繼，這有助於在整個園區實現通用設定上的標準化。此外，還可以實施nonegotiate模式以減少「整體」鏈路初始化時間。

**注意**：通道模式和STP配置等因素也會影響初始化時間。

發出以下命令以設定nonegotiate模式：

```
set trunk mod/port nonegotiate ISL | dot1q
```

Cisco建議在連線到Cisco IOS路由器時，使用nonegotiate，因為執行橋接時，從on模式接收的某些DTP訊框可以返回主干連線埠。收到DTP幀後，交換機埠會嘗試重新協商（或使中繼線關閉和開啟），這是不必要的。如果啟用nonegotiate，交換機將不傳送DTP幀。

## 生成樹通訊協定

### 基本注意事項

生成樹通訊協定(STP)在備援交換和橋接網路中維護無回圈的第2層環境。如果沒有STP，幀將無限循環和/或成倍增加，這將導致網路崩潰，因為廣播域中的所有裝置都會被高流量持續中斷。

雖然在某些方面，STP是最初針對基於軟體的緩慢橋接規範(IEEE 802.1d)開發的成熟協定，但在具有許多VLAN、域中有許多交換機、多供應商支援和較新IEEE增強功能的大型交換網路中實施良好可能會非常複雜。

為了供將來參考，CatOS 6.x繼續採用新的STP開發，例如MISTP、環路防護、根防護和BPDU到達時間偏差檢測。此外，CatOS 7.x中還提供了進一步的標準化協定，例如IEEE 802.1s共用生成樹和IEEE 802.1w快速收斂生成樹。

### 操作概述

具有最低根網橋識別符號(BID)的交換機贏得每個VLAN的根網橋選舉。 BID是與交換機MAC地址組合在一起的網橋優先順序。

最初，BPDU從所有交換機傳送，包含每台交換機的BID以及到達該交換機的路徑開銷。這樣就可以確定根網橋和到根的最低開銷路徑。BPDU中從根承載的其他配置引數會覆蓋那些本地配置的引數，以便整個網路使用一致的計時器。

然後，拓撲通過以下步驟收斂：

1. 為整個生成樹域選擇一個根網橋。
2. 在每個非根網橋上選擇一個根埠（面向根網橋）。
3. 為每個網段上的BPDU轉發選擇指定埠。
4. 非指定埠將阻塞。

如需詳細資訊，請參閱設定生成樹。

| 基本計時器預設值（秒） | 名稱 | 功能 |
|---|---|---|
| 2 | Hello | 控制BPDU的傳送。 |
| 15 | (Fwddelay) | 控制埠處於偵聽和學習狀態所花費的時間，並影響拓撲更改過程（請參見下一節）。 |
| 20 | Maxage | 控制交換機在查詢替代路徑之前保持當前拓撲的時間。在Maxage秒過後，BPDU會被視為已過時，因此交換機將從阻塞埠池中查詢新的根埠。如果沒有可用的阻塞埠，則它聲稱是指定埠上的根埠。 |

| 埠狀態 | 含義 | 到下一個狀態的預設計時 |
|---|---|---|
| | 管理性關閉。 | 不適用 |
| | 接收BPDU並停止使用者資料。 | 監控BPDU的接收。等待20秒以等待Maxage過期，或者在檢測到直接/本地鏈路故障時立即更改。 |
| | 傳送或接收BPDU以檢查是否需要返回阻塞狀態。 | Fwddelay計時器（等待15秒） |

| | | |
|---|---|---|
| | 構建拓撲/CAM表。 | Fwddelay計時器（等待15秒） |
| | 傳送/接收資料。 | |
| | **基本拓撲更改總數：** | **20 + 2(15)= 50秒（等待Maxage過期），或者30秒等待直接鏈路故障** |

STP中的兩種BPDU是配置BPDU和拓撲更改通知(TCN)BPDU。

## 配置BPDU流

配置BPDU源自根網橋上每個埠的每個hello間隔，然後流向所有枝葉交換機，以保持生成樹的狀態。在穩定狀態下，BPDU流是單向的：根埠和阻塞埠僅接收配置BPDU，而指定埠僅傳送配置BPDU。

對於交換機從根收到的每個BPDU，Catalyst中心NMP會處理一個新的BPDU並將其傳送出去，其中包含根資訊。換句話說，如果根網橋丟失或到根網橋的所有路徑都丟失，則會停止接收BPDU（直到maxage計時器開始重新選擇）。

## TCN BPDU流

TCN BPDU源自枝葉交換機，當在生成樹中檢測到拓撲更改時，TCN BPDU會流向根網橋。根埠僅傳送TCN，而指定埠僅接收TCN。

TCN BPDU向根橋傳送，並在每個步驟得到確認，因此這是一個可靠的機制。到達根網橋後，根網橋會通過為`maxage + fwddelay`時間（預設情況下為35秒）設定TCN標誌來通知配置BPDU發生了更改，從而向整個域發出警報。 這會導致所有交換機將其正常CAM老化時間從5分鐘（預設值）更改為`fwddelay`（預設值15秒）指定的時間間隔。 有關詳細資訊，請參閱瞭解生成樹協定拓撲更改。

## 生成樹模式

將VLAN與生成樹關聯有三種不同的方法：

- 適用於所有VLAN的單個生成樹或單生成樹協定，例如IEEE 802.1Q
- 每個VLAN的生成樹或共用生成樹，例如Cisco PVST
- 每個VLAN集的生成樹或多個生成樹，例如Cisco MISTP和IEEE 802.1s

所有VLAN的單一生成樹僅允許一個活動拓撲，因此不能進行負載均衡。STP阻塞的埠阻塞所有VLAN並且不傳輸資料。

每個VLAN有一個生成樹允許負載平衡，但隨著VLAN數量的增加，需要更多的BPDU CPU處理。CatOS版本說明針對每台交換機的生成樹中建議的邏輯埠數量提供指導。例如，Catalyst 6500/6000 Supervisor Engine 1公式如下：

埠數+（中繼數*中繼上的VLAN數）< 4000

Cisco MISTP和新的802.1s標準僅允許定義兩個活動STP例項/拓撲，並將所有VLAN對映到這兩個樹中的任意一個。此技術允許STP在啟用負載平衡的同時擴展到數千個VLAN。

## BPDU格式

為了支援IEEE 802.1Q標準，通過新增對跨IEEE 802.1Q單生成樹區域的隧道的支援，將現有的Cisco STP實施擴展為PVST+。因此，PVST+與IEEE 802.1Q MST和Cisco PVST協定相容，無需額外的命令或配置。此外，PVST+新增了驗證機制，以確保交換機之間的埠中繼和VLAN ID配置不不一致。

以下是PVST+協定的一些操作要點：

- PVST+通過802.1Q中繼的所謂通用生成樹(CST)，與802.1Q單生成樹互操作。CST始終位於VLAN 1上，因此需要在中繼上啟用此VLAN才能與其他供應商進行互操作。將CST BPDU傳輸到IEEE標準網橋組（MAC地址01-80-c2-00-00-00、DSAP 42、SSAP 42），且始終未標籤。為了完整地說明，BPDU的並行集也會傳輸到VLAN 1的Cisco共用生成樹MAC地址。
- PVST+通過802.1Q VLAN區域將PVST BPDU作為組播資料隧道。Cisco共用生成樹BPDU會傳輸到中繼上每個VLAN的MAC地址01-00-0c-cc-cc-cd（SNAP HDLC協定型別0x010b）。BPDU在本徵VLAN上未標籤，並為所有其他VLAN標籤。
- PVST+檢查埠和VLAN不一致。PVST+會阻塞那些接收不一致BPDU的埠，以防止轉發環路。它還通過系統日誌消息通知使用者任何配置不匹配。
- PVST+與ISL中繼上運行PVST的現有思科交換機向後相容。ISL封裝的BPDU仍然使用IEEE MAC地址傳輸或接收。換句話說，每個BPDU型別都是本地鏈路；沒有翻譯問題。

## 建議

所有Catalyst交換機預設啟用STP。即使所選擇的設計不包括L2環路，以使STP在主動維護阻塞埠方面未啟用，也建議這樣做。

```
set spantree enable all
!--- This is the default.
```

Cisco建議基於以下原因保持啟用STP:

- 如果存在環路（由錯誤修補、纜線不良等引起），STP可防止多點傳送和廣播資料對網路造成不利影響。
- 防止EtherChannel故障。
- 大多數網路都配置了STP，這最大程度地提高了現場風險。更多的曝光一般等同於穩定的代碼。
- 防止雙連線的NIC行為不當（或在伺服器上啟用橋接）。
- 許多協定（例如PAgP、IGMP監聽和中繼）的軟體與STP密切相關。不使用STP運行會導致不理想的結果。

**請勿更改計時器，因為這會對穩定性產生負面影響。**部署的大多數網路未進行調整。可通過命令列訪問的簡單STP計時器（如hello-interval和Maxage）本身由一組複雜的其他假定和內部計時器組成，因此很難調整計時器並考慮所有影響。此外，還有破壞UDLD保護的危險。

**理想情況下，將使用者流量限制在管理VLAN之外。**尤其是對於較舊的Catalyst交換機處理器，最好通過將管理VLAN與使用者資料分隔開來，避免STP出現問題。一個行為不當的終端站可能會使Supervisor Engine處理器忙於廣播資料包，以致錯過一個或多個BPDU。但是，具有更強大的CPU和節流控制的較新交換機可緩解這種顧慮。有關詳細資訊，請參閱本文檔的帶內管理部分。

**請勿過度設計冗餘。**這可能會導致故障排除噩夢 — 阻塞埠過多，對長期穩定性產生不利影響。**將SPT總直徑保持在七跳以下。**儘可能嘗試設計思科多層模型，使其具有更小的交換域、STP三角形和確定性阻塞埠(如Gigabit Campus Network Design - Principles and Architecture中所述)。

**影響和瞭解根功能和阻塞埠所在的位置，並在拓撲圖中記錄它們**。阻塞埠是STP故障排除開始的地方 — 導致這些埠從阻塞變為轉發的原因通常是根本原因分析的關鍵部分。**選擇分佈層和核心層作為根/次根的位置，因**為這些層被認為是網路最穩定的部分。檢查使用第2層資料轉發路徑的最佳第3層和HSRP重疊。此命令是配置網橋優先順序的宏；root設定它比預設設定低很多(32768)，而root secondary設定它比預設設定合理更低：

```
set spantree root secondary vlan range
```

**注意：此宏將根優先順序設定為8192(預設情況**下)、當前根優先順序減去1（如果知道另一個根網橋）或當前根優先順序（如果其MAC地址低於當前根）。

**從中繼埠修剪不必要的VLAN**（雙向練習）。 這限制了在不需要特定VLAN的網路部分上STP和NMP處理開銷的直徑。VTP自動修剪不會從中繼中刪除STP。如需詳細資訊，請參閱本檔案的VTP一節。也可使用CatOS 5.4及更高版本從中繼中刪除預設VLAN 1。

如需其他資訊，請參閱跨距樹狀目錄通訊協定問題和相關設計注意事項。

## 其他選項

Cisco有另一個稱為**VLAN-bridge的STP**。此協定使用目標MAC地址**01-00-0c-cd-cd-ce**和協定型別0x010c運行。

如果需要在VLAN之間橋接不可路由或傳統協定，而不影響這些VLAN上運行的IEEE生成樹例項，則此功能非常有用。如果非橋接流量的VLAN介面被第2層流量阻塞（如果它們與IP VLAN參與同一個STP，則很容易發生這種情況），則重疊的第3層流量也會在不經意間被剪除 — 這是有害的副作用。因此，VLAN網橋是橋接協定的STP的獨立例項，它提供了可以操縱而不影響IP流量的獨立拓撲。

如果思科路由器（例如MSFC）上的VLAN之間需要橋接，則思科建議運行VLAN網橋。

## PortFast

PortFast用於繞過存取連線埠上的正常跨距樹狀目錄作業，以加快終端站與其連結初始化後需要連線的服務之間的連線。在某些協定（例如IPX/SPX）上，在鏈路狀態恢復後立即檢視處於轉發模式的接入埠非常重要，這樣可以避免GNS問題。

有關詳細資訊，請參閱使用Portfast和其他命令修復工作站啟動連線延遲。

## 操作概述

在已知鏈路運行後，PortFast通過將埠從`blocking`直接移動到`forwarding`模式，跳過STP的正常和狀態。如果未啟用此功能，則STP會丟棄所有使用者資料，直到它確定埠已準備好移動到模式。這可能需要2倍的`ForwardDelay`時間（預設情況下共30秒）。

PortFast模式還可防止每次埠狀態從`learning`更改為`forwarding`時生成STP TCN。TCN本身並不是問題，但如果一波TCN到達根網橋（通常是在人們開啟PC的早晨），就會不必要地延長收斂時間。

STP PortFast在多播CGMP和Catalyst 5500/5000 MLS網路中都特別重要。這些環境中的TCN可能導致靜態CGMP CAM表條目老化，從而導致組播資料包丟失，直到下一個IGMP報告，和/或刷新MLS快取條目，然後需要重新生成這些條目，並可能導致路由器CPU峰值，具體取決於快取的大小

。（Catalyst 6500/6000 MLS實作和從IGMP窺探瞭解到的多點傳播專案不會受到影響。）

## 建議

Cisco建議為所有活動主機埠啟用STP PortFast，並為交換機鏈路和未使用的埠禁用STP PortFast。

還必須禁用所有主機埠的中繼和通道化。預設情況下，每個接入埠都啟用中繼和通道化，但主機埠上的設計並不要求交換機鄰居。如果讓這些協定去協商，埠啟用的後續延遲可能會導致不理想的情況，即來自工作站的初始資料包（如DHCP請求）不會被轉發。

CatOS 5.2引入了宏命令set port host port range ，該命令為接入埠實施此配置，並顯著幫助自動協商和連線效能：

```
set port host port range
!--- Macro command for these commands: set spantree portfast port range enable set trunk port
range off set port channel port range mode off
```

**注意**：PortFast並不表示這些連線埠上完全沒有執行跨距數狀目錄。BPDU仍會被傳送、接收和處理。

## 其他選項

PortFast BPDU防護提供了一種防止回圈的方法，當非主干連線埠在連線埠上收到BPDU時，可以將其移至errdisable狀態。

在為PortFast配置的接入埠上永遠不能收到BPDU資料包，因為主機埠不能連線到交換機。如果觀察到BPDU，則表明配置無效並可能危險，需要管理操作。啟用BPDU防護功能後，生成樹會關閉接收BPDU的PortFast配置的介面，而不是將其置於STP阻狀態。

此命令針對每台交換機運行，而不是針對每個埠，如下所示：

```
set spantree portfast bpdu-guard enable
```

如果連線埠關閉，網路管理員會收到SNMP設陷或系統日誌訊息的通知。也可以為已錯誤停用的連線埠設定自動復原時間。如需詳細資訊，請參閱本檔案的UDLD一節。如需詳細資訊，請參閱跨距樹狀目錄Portfast BPDU防護增強功能。

**注意**：CatOS 7.x中引入了中繼埠的PortFast，對早期版本的中繼埠沒有影響。中繼埠的PortFast旨在增加L3網路的收斂時間。為了補充此功能，CatOS 7.x還引入了按埠配置PortFast BPDU防護的可能性。

## UplinkFast

UplinkFast在網路接入層發生直接鏈路故障後提供快速STP收斂。它不會修改STP，其目的是將特定環境下的收斂時間加速到少於3秒，而不是典型的30秒延遲。如需詳細資訊，請參閱瞭解和設定思科上行鏈路快速功能。

## 操作概述

在接入層使用Cisco多層設計模型，如果轉發上行鏈路丟失，阻塞上行鏈路會立即移動到forwarding狀態，而無需等待和狀態。

上行鏈路組是每個VLAN的一組埠，可以將其視為根埠和備用根埠。在正常情況下，根埠可確保從訪問到根的連線。如果此主根連線由於任何原因而失敗，備份根鏈路將立即啟動，而無需經過典型的30秒收斂延遲。

由於這實際上會繞過正常的STP拓撲更改處理過程(和)，因此需要替代拓撲更正機制來更新域中本地終端站可通過替代路徑到達的交換機。運行UplinkFast的接入層交換機還會為其CAM中的每個MAC地址生成幀到組播MAC地址（01-00-0c-cd-cd-cd，HDLC協定0x200a），以使用新拓撲更新域中所有交換機的CAM表。

## 建議

思科建議為具有阻塞埠的交換機（通常在接入層）啟用UplinkFast。如果沒有備用根鏈路的隱含拓撲知識，請勿在交換機上使用 — 通常是Cisco多層設計中的分佈層交換機和核心層交換機。它可以在不中斷生產網路的情況下新增。發出以下命令以啟用UplinkFast:

```
set spantree uplinkfast enable
```

此命令還將**bridge priority**設定為高，以最大程度地降低成為根網橋的風險，將**port priority**設定為高，以最大程度地降低成為指定埠（該埠會中斷功能）的風險。恢復已啟用UplinkFast的交換機時，必須禁用該功能，使用「clear uplink」清除上行鏈路資料庫，並手動恢復網橋優先順序。

**注意：**啟用協議過濾功能時，需要UplinkFast命令的**all protocols關鍵字。**當啟用協定過濾時，CAM會記錄協定型別以及MAC和VLAN資訊，因此需要為每個MAC地址上的每個協定生成UplinkFast幀。**rate**關鍵字指示uplinkfast拓撲更新幀的每秒資料包數。建議使用預設值。您無需使用快速STP(RSTP)或IEEE 802.1w來配置BackboneFast，因為此機制在RSTP中原生包含並自動啟用。

## BackboneFast

BackboneFast可從間接鏈路故障中快速收斂。通過向STP新增功能，收斂時間通常可以從預設的50秒縮短到30秒。

## 操作概述

當交換機上的根埠或阻塞埠從其指定網橋接收到下級BPDU時，會啟動此機制。當下游交換機失去與根的連線，並開始傳送自己的BPDU以選擇新的根時，會發生這種情況。**次級BPDU**將交換機同時標識為根網橋和指定網橋。

在正常生成樹規則下，接收交換機在配置的最大老化時間內（預設情況下為20秒）忽略下級BPDU。但是，使用BackboneFast時，交換機將下級BPDU視為拓撲可能已更改的訊號，並嘗試使用根鏈路查詢(RLQ)BPDU來確定它是否具有到根網橋的備用路徑。此協定新增允許交換機檢查根是否仍然可用，在更短的時間內將移動到，並通知傳送次級BPDU的隔離交換機根仍然可用。

以下是協定操作的一些要點：

- 交換機只從根埠（即向根網橋）傳輸RLQ資料包。

- 接收RLQ的交換機可以回覆，如果它是根交換機，或者它知道它已失去與根的連線。如果不知道這些事實，則必須將查詢從根埠轉發出去。
- 如果交換機已失去與根的連線，則必須以否定形式回覆此查詢。
- 回覆必須僅從查詢來自的埠發出。
- 根交換機必須始終以肯定應答響應此查詢。
- 如果在非根埠上收到回覆，則丟棄該回覆。

因此，STP收斂時間最多可以縮短20秒，因為maxage不需要過期。

如需詳細資訊，請參閱瞭解和設定Catalyst交換器上的Backbone Fast。

## 建議

Cisco建議在運行STP的所有交換機上啟用BackboneFast。它可以在不中斷生產網路的情況下新增。發出以下命令以啟用BackboneFast:

```
set spantree backbonefast enable
```

**注意**：需要在域中的所有交換機上配置此全域性級別命令，因為它會為所有交換機需要瞭解的STP協定新增功能。

## 其他選項

2900XL和3500s不支援BackboneFast。如果交換器網域中除了Catalyst 4500/4000、5500/5000和6500/6000交換器之外還包含這些交換器，則不能啟用該功能。

您無需使用RSTP或IEEE 802.1w配置BackboneFast，因為此機制是原生包括在RSTP中並自動啟用的。

## 跨距樹狀目錄回圈防護

環路防護是Cisco專有的針對STP的最佳化。環路防護可保護L2網路免受以下原因導致的環路的影響：

- 網路介面出現故障
- 繁忙的CPU
- 任何阻止BPDU正常轉發的事物

當冗餘拓撲中的阻塞埠錯誤地轉換到轉發狀態時，就會發生STP環路。這種轉換通常是因為物理冗餘拓撲中的一個埠（不一定是阻塞埠）停止接收BPDU。

環路防護僅在交換機通過點對點鏈路連線的交換網路中才有用。大多數現代園區和資料中心網路都是這類網路。在點對點鏈路上，除非指定網橋傳送下級BPDU或關閉鏈路，否則該網橋無法消失。適用於Catalyst 4000和Catalyst 5000平台的CatOS版本6.2(1)和適用於Catalyst 6000平台的6.2(2)中引入了STP環路防護功能。

有關環路防護的詳細資訊，請參閱使用環路防護和BPDU遲滯檢測功能的生成樹協定增強功能。

## 操作概述

環路防護檢查以確定根埠或備用/備用根埠是否收到BPDU。如果埠沒有接收BPDU，環路防護會將埠置於不一致狀態（阻塞），直到埠再次開始接收BPDU。處於不一致狀態的埠不會傳輸BPDU。如果此類埠再次收到BPDU，則埠（和鏈路）再次被視為可行。從埠中刪除環路不一致條件，STP將確定埠狀態，因為此類恢復是自動進行的。

環路防護隔離故障，使生成樹收斂到穩定的拓撲而沒有出現故障的鏈路或網橋。環路防護可防止STP環路以正在使用的STP版本的速度運行。不依賴STP本身（802.1d或802.1w）或調整STP計時器的時間。出於這些原因，在依賴STP且軟體支援這些功能的拓撲中，結合使用UDLD實施環路防護。

當環路防護阻塞不一致的埠時，將記錄以下消息：

```
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated
in VLAN 77. Moved to root-inconsistent state.
```

當處於環路不一致STP狀態的埠收到BPDU時，該埠會轉換到另一個STP狀態。根據收到的BPDU，恢復是自動的，無需干預。恢復後，將記錄此消息。

```
SPANTREE-2-LOOPGUARDUNBLOCK: port 3/2 restored in vlan 3.
```

## 與其他STP功能的互動

- **根防護**根防護會強制始終指定埠。僅當埠是根埠或備用埠時，環路防護才有效。這些功能相互排斥。不能同時在埠上啟用環路防護和根防護。
- **UplinkFast**環路防護與UplinkFast相容。如果環路防護將根埠置於阻塞狀態，UplinkFast會將新的根埠置於轉發狀態。此外，UplinkFast不會選擇環路不一致的埠作為根埠。
- **BackboneFast**環路防護與BackboneFast相容。接收來自指定網橋的下級BPDU會觸發BackboneFast。由於從該鏈路接收BPDU，因此不會啟用環路防護，因此BackboneFast和環路防護是相容的。
- **PortFast**連線後，PortFast會立即將埠轉換為轉發指定狀態。由於啟用PortFast的連線埠不能是根或替代連線埠，因此環路防護和PortFast是互斥的。
- **PAgP**環路防護使用STP已知的埠。因此，環路防護可以利用PAgP提供的邏輯埠抽象。但是，為了形成通道，在通道中分組的所有物理埠都必須具有相容的配置。PAgP在所有物理埠上強制實施環路防護的統一配置以形成通道。**注意：**在EtherChannel上配置環路防護時，以下是注意事項：STP始終選擇通道中的第一個運行埠來傳送BPDU。如果該鏈路變為單向鏈路，則環路防護會阻塞該通道，即使該通道中的其它鏈路工作正常。如果已被環路防護阻塞的埠被組合在一起以形成通道，STP將丟失這些埠的所有狀態資訊。新通道連線埠可以達到具有指定角色的轉送狀態。如果通道被環路防護阻塞並且通道中斷，STP將丟失所有狀態資訊。即使形成通道的一個或多個鏈路是單向的，單個物理埠也可以達到指定角色的轉發狀態。在此清單的最後兩種情況下，在UDLD偵測到失敗之前，可能會產生回圈。但是環路防護無法檢測到環路。

## 環路防護和UDLD功能比較

環路防護功能和UDLD功能部分重疊。這兩種方法均可防止單向鏈路導致的STP故障。但這兩個功能在解決問題的方法和功能上有所不同。具體來說，UDLD無法檢測某些單向故障，例如由不傳送BPDU的CPU導致的故障。此外，使用積極的STP計時器和RSTP模式可能會在UDLD檢測到故障之前導致環路。

環路防護在共用鏈路上或在鏈路自鏈路連線後為單向鏈路的情況下不起作用。如果連結自連結以來是單向的，則連線埠永遠不會收到BPDU且會成為指定連線埠。此行為可能是正常的，因此環路防

護不包含此特定情況。UDLD確實針對這種情況提供保護。

啟用UDLD和環路防護以提供最高級別的保護。有關環路防護和UDLD功能比較，請參閱使用環路防護和BPDU遲滯檢測功能的生成樹協定增強功能的*環路防護與單向鏈路檢測*部分。

## 建議

思科建議在有物理環路的交換機網路上全域性啟用環路防護。在Catalyst軟體版本7.1(1)和更新版本中，可以在所有連線埠上全域啟用回圈防護。實際上，所有點對點鏈路都啟用了此功能。鏈路的雙工狀態檢測點對點鏈路。如果雙工為全雙工，則鏈路視為點對點。發出以下命令以啟用全域性環路防護：

```
set spantree global-default loopguard enable
```

## 其他選項

對於不支援全域性環路防護配置的交換機，請在包括埠通道埠的所有單個埠上啟用該功能。雖然在指定埠上啟用環路防護沒有任何好處，但此啟用並不是問題。此外，有效的跨距樹狀目錄重新收斂實際上會將指定連線埠轉變成根連線埠，因此該功能在此連線埠上非常有用。發出以下命令以啟用回圈防護：

```
set spantree guard loop mod/port
```

如果意外引入環路，採用無環路拓撲的網路仍能受益於環路防護。但是，在此類拓撲中啟用環路防護可能會導致網路隔離問題。為了構建無環路拓撲並避免網路隔離問題，請發出以下命令以全域性或單獨禁用環路防護。請勿在共用鏈路上啟用環路防護。

- ```
  set spantree global-default loopguard disable
  !--- This is the global default.
  ```
  或
- ```
  set spantree guard none mod/port
  !--- This is the default port configuration.
  ```

## 生成樹根防護

根防護功能提供了一種在網路中實施根網橋放置的方法。根防護確保啟用根防護的埠是指定埠。通常，根網橋埠都是指定埠，除非根網橋的兩個或多個埠連線在一起。如果網橋在啟用根防護的埠上收到上級STP BPDU，則網橋會將此埠移至根不一致STP狀態。這種根不一致狀態實際上等於偵聽狀態。沒有流量通過此埠轉發。通過這種方式，根防護將強制實施根網橋的位置。適用於Catalyst 29xx、4500/4000、5500/5000和6500/6000的CatOS軟體版本6.1.1和更新版本提供根防護。

## 操作概述

根防護是STP內建機制。根防護沒有自己的計時器，它只依賴於BPDU的接收。對埠應用根防護時

，根防護不允許埠成為根埠。如果BPDU的接收觸發了使指定埠成為根埠的生成樹收斂，則該埠將進入根不一致狀態。此系統日誌消息顯示操作：

```
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated
in VLAN 77. Moved to root-inconsistent state
```

連線埠停止傳送上級BPDU後，連線埠會再次解除封鎖。通過STP，埠從偵聽狀態轉換到學習狀態，最終轉換為轉發狀態。恢復是自動的，無需人為干預。以下系統日誌消息提供示例：

```
%SPANTREE-2-ROOTGUARDUNBLOCK: Port 1/1 restored in VLAN 77
```

根保護強制指定埠，並且環路保護僅在埠是根埠或備用埠時才有效。因此，這兩個功能是互斥的。不能同時在埠上啟用環路防護和根防護。

如需詳細資訊，請參閱跨距樹狀目錄通訊協定根防護增強功能。

### 建議

思科建議您在連線到不受直接管理控制的網路裝置的埠上啟用根防護功能。若要設定根防護，請發出以下命令：

**set spantree guard root** *mod/port*

## 乙太通道

EtherChannel技術可將多個通道（在Catalyst 6500/6000上最多八個）反向多工到單一邏輯連結中。雖然每個平台在實施上與下一個平台不同，但瞭解常見要求非常重要：

- 多通道統計複用幀的一種演算法
- 建立邏輯埠，以便運行單個STP例項
- 通道管理通訊協定，例如PAgP或連結彙總控制通訊協定(LACP)

### 訊框多工

EtherChannel包含幀分配演算法，可高效地將幀多路複用到元件10/100或Gigabit鏈路上。每個平台的演算法差異源於每種硬體提取幀頭資訊以便做出分配決策的能力。

負載分配演算法是兩種通道控制協定的全域性選項。PAgP和LACP使用幀分配演算法，因為IEEE標準不要求任何特定的分配演算法。但是，任何分發演算法都確保在收到幀時，該演算法不會引起作為任何給定會話一部分的幀的錯誤排序或幀的重複。

**注意：**必須考慮以下資訊：

- Catalyst 6500/6000比Catalyst 5500/5000具有更新的交換硬體，且能夠以線速讀取IP第4層(L4)資訊，以便作出比簡單的MAC L2資訊更智慧的多工決策。
- Catalyst 5500/5000功能取決於模組上是否存在乙太網路捆綁晶片(EBC)。show port capabilities *mod/port* 命令會確認每個連線埠可以執行的功能。

請參閱下表，其中詳細說明了所列每個平台的幀分配演算法：

| 平台 | 通道負載平衡演演算法 |
| --- | --- |
| Catalyst 5500/5000系列 | 具有必要模組的Catalyst 5500/5000允許每個FEC[1]存在二到四個連結，雖然這些連結必須位於同一個模組上。源和目的MAC地址對確定選擇用於幀轉發的鏈路。對源MAC地址和目的MAC地址的最低有效兩位執行X-OR操作。此操作會產生以下四種結果之一：(0 0)、(0 1)、(1 0)或(1 1)。 每個值都指向FEC捆綁包中的連結。對於雙埠快速EtherChannel，在X-OR操作中僅使用一個位。當來源/目的地配對中的一個位址為常數時，可能會發生這種情況。例如，目標可以是伺服器，甚至更可能的是路由器。在這種情況下，由於源地址始終不同，因此會看到統計負載平衡。 |
| Catalyst 4500/4000系列 | Catalyst 4500/4000 EtherChannel根據每個訊框的來源和目的地MAC位址的低位元，在通道（單一模組上）中的連結上分散訊框。與Catalyst 5500/5000相比，此演演算法更多涉及並使用了MAC DA（位元組3、5、6）、SA（位元組3、5、6）、輸入連線埠和VLAN ID這些欄位的確定性雜湊方式。幀分配方法不可配置。 |
| Catalyst 6500 | 有兩種可能的雜湊演算法，具體取決於Supervisor Engine硬體。雜湊是在硬體中實現的十七次多項式，在任何情況下，它都取MAC地址、IP地址或IP TCP/UDP2埠號，並應用演算法生成三位值。對於源地址和目標地址，此操作將分別執行。然後將結果進行XORd生成另一個三位值，用於確定通道中的哪個埠用於轉發資料包。Catalyst 6500/6000上的通道可在任何模組的連線埠之間形成，最多可以有8個連線埠。 |

| | |
|---|---|
| /6000系列 | |

[1] FEC =快速EtherChannel

[2] UDP =使用者資料包協定

下表說明各種Catalyst 6500/6000 Supervisor引擎型號所支援的分佈方法及其預設行為。

| 硬體 | 說明 | 分佈方法 |
|---|---|---|
| WS-F6020（L2引擎） | 早期監督器引擎1 | L2 MAC:SA;DA;SA和DA |
| WS-F6020A（L2引擎）WS-F6K-PFC（L3引擎） | 更高版本的Supervisor引擎1和Supervisor引擎1A/PFC1 | L2 MAC:SA;DA;SA和DA第3層IP:SA;DA;SA和DA（預設） |
| WS-F6K-PFC2 | Supervisor引擎2/PFC2（需要CatOS 6.x） | L2 MAC:SA;DA;SA和DA第3層IP:SA;DA;SA和DA（預設）第4層會話：S埠；D埠；S & D埠（預設） |
| WS-F6K-PFC3BXL WS-F6K-PFC3B WS-F6K-PFC3A | Supervisor Engine 720/PFC3A（需要CatOS 8.1.x）Supervisor Engine 720/Supervisor Engine 32/PFC3B（需要CatOS 8.4.x）Supervisor Engine 720/PFC3BXL（需要CatOS 8.3.x） | L2 MAC:SA;DA;SA和DA第3層IP:SA;DA;SA和DA（預設）第4層會話：S埠；D埠；S & D埠IP-VLAN-L4會話：SA & VLAN & S埠；DA & VLAN & D埠；SA & DA & VLAN & S埠和D埠 |

**注意：**使用L4分發時，第一個分段的資料包使用L4分發。所有後續資料包都使用L3分發。

有關其他平台上的EtherChannel支援以及如何配置和排除這些平台的問題的詳細資訊，請參閱以下文檔：

- 瞭解 Catalyst 交換器上的 EtherChannel 負載平衡和備援

- 在執行 CatOS 系統軟體的 Catalyst 4500/4000、5500/5000 和 6500/6000 交換器之間設定乙太通道。
- 在 Catalyst 6500/6000 和 Catalyst 4500/4000 之間設定 LACP (802.3ad)
- 配置第3層和第2層EtherChannel

## 建議

Catalyst 6500/6000系列交換器預設會依照IP位址執行負載平衡。在CatOS 5.5中建議這樣做，假設IP為主要協定。發出以下命令以設定負載平衡：

```
set port channel all distribution ip both
!--- This is the default.
```

在大多數網路中，通過L2 MAC地址分配的Catalyst 4500/4000和5500/5000系列幀是可接受的。但是，如果只有兩台主裝置通過通道進行通訊（因為SMAC和DMAC是常數），則同一鏈路將用於所有流量。 這通常是伺服器備份和其他大型檔案傳輸的問題，或者兩台路由器之間的中轉網段的問題。

雖然邏輯聚合埠(agport)可以由SNMP作為單獨的例項進行管理，並且收集了聚合吞吐量統計資訊，但Cisco仍建議您分別管理每個物理介面，以便檢查幀分發機制的工作方式以及是否實現了統計負載均衡。

在CatOS 6.x中，與使用show counters mod/port 命令或CatOS 5.x中的show mac *mod/port* 命令檢查各個連線埠計數器相比，新命令show channel traffic 命令可以更輕鬆地顯示百分比分佈統計資訊。在CatOS 6.x中，還可以使用另一個新命令show channel hash 命令，根據分發模式檢查將選擇哪個埠作為某些地址和/或埠號的傳出埠。適用於LACP通道的等效命令是show lacp-channel traffic 命令和show lacp-channel hash 命令。

## 其他選項

如果Catalyst 4500/4000或Catalyst 5500/5000基於MAC的演算法的相對限製出現問題，並且沒有實現良好的統計負載平衡，可以採取以下步驟：

- 單點部署Catalyst 6500/6000交換器
- 通過交換（例如，從多個FE埠交換到一個GE埠，或從多個GE埠交換到一個10 GE埠）增加頻寬，而不進行通道化
- 重新定址具有大量流量的終端站對
- 為高頻寬裝置調配專用鏈路/VLAN

## EtherChannel設定原則和限制

EtherChannel在將相容埠聚合到單個邏輯埠之前，會驗證所有物理埠上的埠屬性。配置准則和限制因交換機平台而異。請遵循指南以避免繫結問題。例如，如果啟用QoS，當捆綁具有不同QoS功能的Catalyst 6500/6000系列交換模組時，不會形成EtherChannel。在Cisco IOS軟體中，可以使用no mls qos channel-consistency port-channel interface命令停用EtherChannel繫結上的QoS連線埠屬性檢查。CatOS中沒有用於禁用QoS埠屬性檢查的等效命令。您可以發出show port capability *mod*/*port* 命令以顯示QoS連線埠功能並確定連線埠是否相容。

針對不同平台遵循以下准則，以避免配置問題：

- 設定EtherChannel(Catalyst 6500/6000)的*EtherChannel組態准則*一節
- 設定快速EtherChannel和Gigabit EtherChannel(Catalyst 4500/4000)的*EtherChannel設定指南和限制*一節
- 設定快速EtherChannel和Gigabit EtherChannel(Catalyst 5000)的*EtherChannel設定指南和限制*一節

**註**：Catalyst 4000支援的最大埠通道數為126。在軟體版本6.2(1)及更低版本中，六插槽和九插槽Catalyst 6500系列交換機最多支援128個EtherChannel。在軟體版本6.2(2)和更新版本中，跨距樹狀目錄功能會處理連線埠ID。因此，對於6或9插槽機箱，支援的最大EtherChannel數量為126，對於13插槽機箱，為63。

## 連線埠彙總通訊協定

PAgP是一種管理協定，可在鏈路兩端檢查引數一致性，並幫助通道適應鏈路故障或鏈路新增。請注意以下有關PAgP的事實：

- PAgP要求通道中的所有埠屬於同一個VLAN或配置為中繼埠。（由於動態VLAN可以強制將埠更改為不同的VLAN，因此它們不包括在EtherChannel參與中。）
- 當套件組合已存在且修改一個連線埠的組態（例如變更VLAN或主幹模式）時，將會修改套件組合中的所有連線埠以與該組態相符。
- PAgP不對以不同速度或埠雙工運行的埠進行分組。如果存在捆綁包時更改了速度和雙工，PAgP將更改捆綁包中所有埠的埠速度和雙工。

## 操作概述

PAgP埠控制每個要分組的物理（或邏輯）埠。PAgP資料包使用與CDP資料包相同的組播組MAC地址**01-00-0c-cc-cc-cc**傳送。協定值為0x0104。以下是協定操作的摘要：

- 只要物理埠處於up狀態，PAgP資料包就會在檢測期間每秒傳輸一次，在穩定狀態下則每30秒傳輸一次。
- 協定偵聽證明物理埠與另一個支援PAgP的裝置具有雙向連線的PAgP資料包。
- 如果接收到資料包但沒有PAgP資料包，則假定埠連線到不支援PAgP的裝置。
- 當一組物理埠上收到兩個PAgP資料包後，它會嘗試形成聚合埠。
- 如果PAgP資料包停止一段時間，則PAgP狀態將。

## 正常處理

必須定義以下概念來幫助理解協定行為：

- **Agport** — 由同一聚合中的所有物理埠組成的邏輯埠，可以通過其自己的SNMP ifIndex對其進行標識。因此，agport不包含非運行埠。
- **通道** — 滿足形成條件的聚合；因此，它可能包含非運行埠（agports是通道的子集）。 包括STP和VTP在內的協定（不包括CDP和DTP）在agport上運行在PAgP之上。在PAgP將其agport連線到一個或多個物理埠之前，這些協定都不能傳送或接收資料包。
- **組功能** — 每個物理埠和agport都具有一個稱為group-capability的配置引數。若且唯若物理埠具有相同的組功能時，該物理埠才能與另一個物理埠聚合。
- **聚合過**程 — 當物理埠達到UpData或UpPAgP態時，會將其連線到適當的agport。當它離開其中任一狀態進入另一狀態時，它將從agport分離。

下表給出了狀態和建立過程的定義：

| 狀態 | 含義 |
| --- | --- |
| UpData | 未收到PAgP資料包。傳送PAgP資料包。實體連線埠是唯一連線到其agport的連線埠。非PAgP資料包在物理埠和agport之間傳入和傳出。 |
| BiDir | 只收到一個PAgP資料包，證明存在與僅一個鄰居的雙向連線。物理埠未連線到任何agport。PAgP資料包傳送後可以接收。 |
| UpPAgP | 此物理埠（可能與其他物理埠關聯）連線到agport。物理埠上傳送和接收PAgP資料包。非PAgP資料包在物理埠和agport之間傳入和傳出。 |

兩個連線的兩端必須就分組內容達成一致，分組被定義為連線兩端所允許的agport中最大的埠組。

當實體連線埠達到UpPAgP狀態時，會將其指派給擁有成員實體連線埠的agport，該成員實體連線埠與新實體連線埠的群組功能相符，且處於BiDir或UpPAgP狀態。(任何此類BiDir埠將同時移動到UpPAgP狀態。) 如果不存在其構成物理埠引數與新就緒物理埠相容的agport，則將其分配給具有適當引數的無關聯物理埠的agport。

PAgP超時可能發生在物理埠上已知的最後一個鄰居。埠超時從agport中刪除。同時，同一代理埠上計時器也超時的所有物理埠都將被刪除。這樣，可以同時拆下另一端已失效的agport，而不是一次拆下一個物理埠。

## 失敗時的行為

如果現有通道中的連結失敗（例如連線埠拔出、Gigabit Interface Converter [GBIC]移除或光纖中斷），則會更新agport，並在一秒內將流量雜湊到其餘連結上。在故障發生後不需要重新雜湊的任何流量（繼續在同一鏈路上傳送的流量）不會受到任何損失。恢復故障鏈路會觸發對agport的另一次更新，流量將再次雜湊。

**注意：**當某個通道中的鏈路由於斷電或模組被移除而發生故障時，其行為可能會有所不同。根據定義，一個通道需要有兩個物理埠。如果系統在兩個埠通道中丟失了一個埠，則邏輯埠會關閉，並且原始物理埠會根據生成樹重新初始化。這表示流量可能會被丟棄，直到STP允許埠再次對資料可用。

Catalyst 6500/6000上的此規則有例外情況。在低於CatOS 6.3的版本中，如果通道僅由模組1和模組2上的連線埠組成，則在模組移除期間，agport閉。

規劃網路維護時，兩種故障模式的差異非常重要，因為在執行模組的線上刪除或插入時，可以考慮使用STP TCN。如上所述，使用NMS管理通道中的每條物理鏈路非常重要，因為agport可以不受故障干擾。

為了減輕Catalyst 6500/6000上不需要的拓撲更改，建議採取以下步驟：

- 如果每個模組使用一個埠形成通道，則必須使用三個或更多個模組（總共三個或更多個埠）。
- 如果通道跨兩個模組，則必須使用每個模組上的兩個埠（共四個埠）。

- 如果兩個卡之間需要雙埠通道，則僅使用Supervisor Engine埠。
- 升級到CatOS 6.3，該作業系統可處理模組刪除，無需重新計算跨模組拆分的通道。

## 組態選項

EtherChannel可以按不同的模式配置，如下表所示：

| 模式 | 可設定選項 |
|---|---|
| | PAgP未運行。無論鄰居連線埠的設定方式如何，連線埠都會進行通道化。如果相鄰埠模式為on，則會形成通道。 |
| Off | 無論鄰居是如何配置的，埠都不會進行通道化。 |
| | 聚合由PAgP協定控制。將連線埠置於被動交涉態，且不會在介面上傳送PAgP封包，直到至少收到一個PAgP封包指出傳送者正在理想模式作。 |
| Desirable | 聚合由PAgP協定控制。將埠置於活動狀態，在該狀態下，埠通過傳送PAgP資料包啟動與其他埠的協商。在desirable或auto模式下與另一個埠組形成通道。 |
| （Catalyst 5500/5000光纖FE和GE埠上的預設值） | auto或desirable模式關鍵字。如果介面上未收到資料包，則介面從未連線到agport，並且不能用於資料。此雙向檢查是針對特定的Catalyst 5500/5000硬體提供的，因為某些連結失敗會導致通道分離。由於模式已啟用，因此絕不會允許復原的鄰居連線埠重新開機並將通道不必要地分隔開。Catalyst 4500/4000和6500/6000系列硬體中預設存在更靈活的繫結和改進的雙向性檢查。 |
| （所有Catalyst 6500/6000和4500/4000埠以及5500/5000銅纜埠的預設設定） | auto或desirable模式關鍵字。如果在介面上未接收到資料分組，在15秒超時週期之後，該介面將自己連線到agport，因此可以用於資料傳輸。夥伴可以是從不傳送PAgP的分析器或伺服器時，靜默模式還允許通道操作。 |

silent/non-silent設定會影響埠對導致單向流量的情況作出反應的方式，或者影響它們實現故障轉移的方式。當連線埠無法傳輸時（例如，因為實體子層[PHY]發生故障或光纖或纜線中斷），仍然可以讓鄰近連線埠處於使用中的狀態。合作夥伴繼續傳輸資料，但由於無法接收返回流量，資料丟

失。由於連結的單向性質，也可能形成跨距樹狀目錄回圈。

某些光纖連線埠具有所需的功能，可在連線埠遺失其接收訊號(FEFI)時使其進入非營運狀態。 這會導致夥伴埠進入非運行狀態，並有效地導致鏈路兩端的埠關閉。

使用傳輸資料（如BPDU）且無法檢測單向條件的裝置時，必須使用non-silent模式，以允許埠保持非運行狀態，直到出現接收資料並且鏈路被驗證為雙向。PAgP檢測單向鏈路的時間大約為3.5 * 30秒= 105秒，其中30秒是兩個連續PAgP消息之間的時間。建議使用UDLD作為單向連結的更快速偵測器。

使用不傳輸任何資料的裝置時，必用靜默模式。這樣可強制連線埠成為連線且可操作的，而不管所接收的資料是否存在。此外，對於那些可以檢測存在單向條件的埠（例如使用L1 FEFI和UDLD的較新平台），預設使用靜默模式。

## 驗證

下表總結了兩台直連交換器（交換器A和交換器B）之間所有可能的PAgP通道模式案例。 其中某些組合可能會導致STP將通道化端的連線埠置於errdisable狀態（即某些組合會關閉通道化端的連線埠）。

| Switch-A通道模式 | Switch-B通道模式 | 通道狀態 |
|---|---|---|
| | | 道（非PAgP） |
| | Off | Not Channel(誤停用) |
| | | Not Channel(誤停用) |
| | Desirable | Not Channel(誤停用) |
| Off | | Not Channel(誤停用) |
| Off | Off | |
| Off | | |
| Off | Desirable | |
| | | Not Channel(誤停用) |
| | Off | |
| | | |
| | Desirable | PAgP |
| Desirable | | Not Channel（錯誤停用） |
| Desirable | Off | |
| Desirable | | PAgP |
| Desirable | Desirable | PAgP |

## 建議

思科建議在所有交換機到交換機通道連線上啟用PAgP，避免使on模式。優選的方法是在鏈路兩端設定desirable模式。其他建議是在Catalyst 6500/6000和4500/4000交換器上將silent/non-silent關鍵字保留為預設值 — silent，而在Catalyst 5500/5000光纖連線埠上保留non-silent。

如本檔案中所述，在所有其他連線埠上關閉通道化的明確組態有助於快速資料轉送。必須避免在不用於通道化的埠上等待PAgP超時的最長15秒，尤其是因為該埠隨後被傳遞到STP，而STP本身可能需要30秒才能允許資料轉發，另外DTP可能需要5秒的時間總計50秒。本檔案STP一節將詳細討論 set port host 命令。

```
set port channel port range mode desirable

set port channel port range mode off
!--- Ports not channeled; part of the set port hostcommand.
```

此命令為通道分**配一個管理**組編號，使用show channel group 命令即可看到。如果需要，可以通過管理員編號管理向同一個agport新增和刪除通道化的埠。

## 其他選項

對於在接入層具有最小管理模式的客戶，另一種常見配置是在分佈層和核心層將模式設定為 desirable，並將接入層交換機保留為預設配置。

當通道傳輸到不支援PAgP的裝置時，需要對該通道進行硬。這適用於伺服器、本機導向器、內容交換器、路由器、使用舊軟體的交換器、Catalyst XL交換器和Catalyst 8540等裝置。發出以下命令：

```
set port channel port range mode on
```

CatOS 7.x中提供的新802.3ad IEEE LACP標準長期來看可能會取代PAgP，因為它帶來了跨平台和供應商互操作性的好處。

## 連結彙總控制通訊協定

LACP是一種協定，允許具有類似特性的埠通過與相鄰交換機進行動態協商來形成通道。PAgP是思科專有協定，只能運行在思科交換機和授權供應商發佈的交換機上。但是，LACP（在IEEE 802.3ad中定義）允許思科交換機管理符合802.3ad規範的裝置的乙太網通道。CatOS 7.x軟體版本引入了LACP支援。

從功能角度看，LACP和PAgP之間差別很小。兩個通訊協定在每個通道中最多支援八個連線埠，並在套件組合形成之前檢查相同的連線埠屬性。這些埠屬性包括：

- 速度
- 雙工
- 本徵VLAN
- 中繼型別

LACP與PAgP的顯著區別是：

- LACP只能在全雙工埠上運行，而LACP不支援半雙工埠。
- LACP支援熱備用埠。LACP始終嘗試配置通道中最大數量的相容埠，最多為硬體允許的最大數量（八個埠）。 如果LACP無法聚合所有相容埠，則所有不能主動包含在通道中的埠將進入熱備用狀態，並僅在其中一個已使用的埠出現故障時才使用。LACP無法聚合所有相容埠的情況的一個示例是，遠端系統具有更嚴格的硬體限制。

**注意：**在CatOS中，可以分配相同管理金鑰的最大埠數是8。在Cisco IOS軟體中，LACP會嘗試設定EtherChannel中相容連線埠的最大數量，最多為硬體允許的最大數量（八個連線埠）。 另外8個埠可配置為熱備用埠。

## 操作概述

LACP控制要捆綁的每個單獨的物理（或邏輯）埠。使用組播組MAC地址01-80-c2-00-00-02傳送LACP資料包。型別/欄位值為0x8809，子型別為0x01。以下是協定操作的摘要：

- 該協定依靠裝置通告其聚合功能和狀態資訊。在每條「可聚合」鏈路上定期傳送這些傳輸。
- 只要物理埠處於開啟狀態，LACP資料包就會在檢測期間每秒傳輸一次，在穩定狀態下每隔30秒傳輸一次。
- 「可聚合」鏈路上的合作夥伴將偵聽協定內傳送的資訊，並決定採取何種措施。
- 在通道中配置的相容埠數最多為硬體允許的最大數量（八個埠）。
- 通過鏈路合作夥伴之間定期、及時地交換最新狀態資訊來維護聚合。如果配置發生更改（例如，由於鏈路故障），協定夥伴將超時並根據系統的新狀態採取適當的操作。
- 除了定期LACP資料單元(LACPDU)傳輸之外，如果狀態資訊發生改變，協定向夥伴傳輸事件驅動的LACPDU。協定合作夥伴根據系統的新狀態採取相應措施。

## LACP引數

為了允許LACP確定一組鏈路是否連線到同一系統，以及從聚合的角度看這些鏈路是否相容，必須能夠建立以下引數：

- 參與鏈路聚合的每個系統的全域性唯一識別符號必須為運行LACP的每個系統分配一個優先順序，該優先順序可以自動選擇，也可以由管理員選擇。預設系統優先順序為32768。系統優先順序主要與系統的MAC地址結合使用，以形成系統識別符號。
- 識別與每個埠和每個聚合器關聯的一組功能的方法，因為給定系統理解這些功能系統中的每個埠都必須自動或由管理員分配優先順序。預設值為128。優先順序與埠號一起使用以形成埠識別符號。
- 一種鏈路聚合組及其關聯聚合器的標識方法埠與另一個埠聚合的能力由一個嚴格大於零的簡單16位整數引數來總結。此引數稱為「key」。 各個金鑰由不同的因素決定，例如：埠物理特性，包括：資料速率重複性點對點或共用介質網路管理員建立的配置約束每個連線埠有兩個相關的金鑰：管理鍵 — 此鍵允許由管理操作鍵值。使用者可以選擇此金鑰。操作鍵 — 系統使用此鍵形成聚合。使用者不能選擇或直接更改此金鑰。系統中共用相同操作金鑰值的埠集被稱為同一金鑰組的成員。

如果您有兩個系統和一組具有相同管理金鑰的埠，則每個系統都會嘗試聚合這些埠。每個系統都從最高優先順序系統中具有最高優先順序的連線埠開始。此行為是可能的，因為每個系統都知道自己的優先順序（使用者或系統已經分配了該優先順序）以及通過LACP資料包發現的合作夥伴優先順序。

## 失敗時的行為

LACP的故障行為與PAgP的行為相同。如果現有通道中的鏈路發生故障，則會更新agport並在一秒鐘內通過其餘鏈路對流量進行雜湊。連結失敗的原因可能有以下以及其他原因：

- 連線埠已拔出
- 刪除GBIC

- 光纖已損壞
- 硬體故障（介面或模組）

在故障發生後不需要重新雜湊的任何流量（繼續在同一鏈路上傳送的流量）不會受到任何損失。恢復故障鏈路會觸發對agport的另一次更新，流量將再次雜湊。

## 組態選項

可以在不同的模式下配置LACP EtherChannel，如下表總結：

| 模式 | 可設定選項 |
|---|---|
| | 強制形成鏈路聚合而不進行任何LACP協商。交換機既不傳送LACP資料包，也不處理任何傳入的LACP資料包。如果相鄰埠模式為on，則會形成通道。 |
| off | 無論鄰居是如何配置的，埠都不會進行通道化。 |
| | 這類似於PAgP中的auto模式。交換機不會啟動通道，但能夠瞭解傳入的LACP資料包。對等體(處於active狀態)通過發出LACP資料包來發起協商。交換器接收並回覆封包，最終與對等點建立聚合通道。 |
| active | 這類似於PAgP中的desirable模式。交換器會啟動交涉，以便形成aglink。如果另一端在LACP主動或模式下運行，則會形成鏈路聚合。 |

## 驗證（LACP和LACP）

本節中的表格總結了兩台直接連線的交換機（交換機A和交換機B）之間所有可能的LACP通道模式方案。 其中某些組合可能導致STP將通道化端的連線埠置於狀態。這表示某些組合會關閉通道化端的連線埠。

| Switch-A通道模式 | Switch-B通道模式 | 交換機A通道狀態 | 交換機B的通道狀態 |
|---|---|---|---|
| | | 道（非LACP） | 道（非LACP） |
| | Off | Not Channel(誤停用) | |
| | | Not Channel(誤停用) | |
| | Active | Not Channel(誤停用) | |
| Off | Off | | |

| | | | |
|---|---|---|---|
| Off | | | |
| Off | Active | | |
| | | | |
| | Active | LACP | LACP |
| Active | Active | LACP | LACP |

## 驗證（LACP和PAgP）

本節中的表格總結了兩台直接連線的交換機（交換機A和交換機B）之間所有可能的LACP到PAgP通道模式方案。 其中某些組合可能導致STP將通道化端的連線埠置於狀態。這表示某些組合會關閉通道化端的連線埠。

| Switch-A通道模式 | Switch-B通道模式 | 交換機A通道狀態 | 交換機B的通道狀態 |
|---|---|---|---|
| | | 道（非LACP） | 道（非PAgP） |
| | Off | Not Channel(誤停用) | |
| | | Not Channel(誤停用) | |
| | Desirable | Not Channel(誤停用) | |
| Off | | | Not Channel(誤停用) |
| Off | Off | | |
| Off | | | |
| Off | Desirable | | |
| | | | Not Channel(誤停用) |
| | Off | | |
| | | | |
| | Desirable | | |
| Active | | | Not Channel(誤停用) |
| Active | Off | | |
| Active | | | |
| Active | Desirable | | |

## 建議

思科建議您對思科交換機之間的通道連線啟用PAgP。當您連線到不支援PAgP但支援LACP的裝置時，請通過在裝置的兩端配置`LACP active`來啟用LACP。如果任一端裝置不支援LACP或PAgP，則需要將通道硬編碼為`on`。

- **set channelprotocol lacp** *module*

  在執行CatOS的交換器上，Catalyst 4500/4000和Catalyst 6500/6000上的所有連線埠預設均使用通道通訊協定PAgP，因此不會執行LACP。為了配置埠以使用LACP，您需要將模組上的通

道協定設定為LACP。LACP和PAgP無法在運行CatOS的交換機上的同一模組上運行。

- **set port lacp-channel** *port_range admin-key*

  在LACP資料包中交換**admin key**（管理金鑰）引數。通道僅形成在具有相同管理金鑰的連線埠之間。set port lacp-channel *port_range* admin-key 命令可為通道分配管理金鑰編號。show lacp-channel group 命令會顯示編號。**set port lacp-channel** *port_range* admin-key 命令可為埠範圍中的所有埠分配相同的管理金鑰。如果沒有配置特定金鑰，則隨機分配管理金鑰。然後，如果需要，可以參考admin金鑰，以便管理向同一個agport新增和刪除通道化的埠。

- **set port lacp-channel** *port_range* **mode active**

  **set port lacp-channel** *port_range* mode active命令將一組先前分配了相同管理金鑰的埠的通道模式更改為active。

此外，在建立LACP EtherChannel後，LACP會使用30秒間隔計時器(Slow_Periodic_Time)。使用長超時(3 x Slow_Periodic_Time)使收到的LACPDU資訊失效之前的秒數為90。使用UDLD，它是單向鏈路的更快速檢測器。您無法調整LACP計時器，而且現在您無法將交換機配置為使用快速PDU傳輸（每秒一次），以便在通道形成後保持通道。

### 其他選項

如果在接入層具有最小管理模式，則常見配置是在分佈層和核心層將模式設定為active。將接入層交換機保留為預設配置。

## 單向連結偵測

UDLD是思科專有的輕量型通訊協定，專為偵測裝置之間的單向通訊例項而開發。雖然有其他方法可以檢測傳輸介質的雙向狀態，例如FEFI，但也有某些情況下，L1檢測機制是不夠的。這些情況可能會導致以下任何情況：

- STP的不可預測操作
- 資料包的泛洪錯誤或過多
- 交通黑洞

UDLD功能旨在解決光纖和銅纜乙太網介面上的以下故障情況：

- 監控實體佈線組態，並作為錯誤停用關閉所有連線錯誤埠。
- 針對單向鏈路提供保護。當檢測到單向鏈路時，由於介質或埠/介面故障，受影響的埠將作為errdisable關閉，並生成相應的系統日誌消息。
- 此外，UDLD主動模式會檢查以前被視為雙向的鏈路在擁塞期間不會丟失連線並且變得不可用。UDLD會跨鏈路執行持續連線測試。UDLD主動模式的主要目的是避免在某些故障情況下對流量進行黑洞。

跨距樹狀目錄及其穩態單向BPDU流，是這些故障的嚴重受害者。很容易看到埠如何突然無法傳輸BPDU，從而導致鄰居的STP狀態從變為。此變更會建立回圈，因為連線埠仍能接收。

### 操作概述

UDLD是工作在LLC層之上的L2協定（目標MAC 01-00-0c-cc-cc-cc，SNAP HDLC協定型別

0x0111）。 結合運行UDLD和FEFI以及自動協商L1機制時，可以驗證鏈路的物理(L1)和邏輯(L2)完整性。

UDLD提供FEFI和自動協商無法執行的功能和保護功能，即檢測和快取鄰居資訊、關閉任何連線不當的埠以及檢測非點對點鏈路（穿越媒體轉換器或集線器的鏈路）上的邏輯介面/埠故障或故障。

UDLD採用兩種基本機制；它會瞭解鄰居，並在本地快取中保持資訊最新，並在檢測到新鄰居或鄰居請求快取重新同步時傳送一系列UDLD探測/回應(hello)消息。

UDLD會在啟用UDLD的所有連線埠上持續傳送探測訊息。每當在連線埠上收到特定的「觸發」UDLD訊息，就會開始檢測階段和驗證程式。如果在此過程結束時滿足所有有效條件，則不會更改埠狀態。為了滿足這些條件，埠必須雙向且正確佈線。否則，連線埠會處於`errdisable`，且系統日誌訊息顯示。系統日誌消息類似於以下消息：

- `UDLD-3-DISABLE:[dec]/[dec]`
- `UDLD-4-ONEWAYPATH:[dec]/[dec] [chars][dec]/[dec]`

請參閱訊息和恢復程式（Catalyst系列交換器，7.6），以取得按設施分類的系統訊息的完整清單，其中包括UDLD事件。

建立連結並將其分類為雙向後，UDLD會繼續以預設的15秒間隔通告探測/回應訊息。下表顯示**show udld port**命令輸出中報告的有效UDLD連結狀態：

| **埠狀態** | **意見** |
|---|---|
| 未確定 | 正在進行檢測，或者相鄰UDLD實體已禁用或其傳輸已被阻止。 |
| 不適用 | UDLD已禁用。 |
| 關機 | 偵測到單向連結且連線埠已停用。 |
| 雙向 | 檢測到雙向鏈路。 |

- **Neighbor Cache Maintenance** - UDLD定期在每個活動介面上傳送hello探測/回應資料包，以維護UDLD鄰居快取的完整性。每當收到hello消息時，都會將其快取並儲存在記憶體中一個定義為保持時間的最大時間段。當保持時間到期時，相應的快取記憶體條目將老化。如果在保持時間段內接收到新的hello消息，則新消息替換舊條目，並且相應的生存時間計時器被重置。
- 為了保持UDLD快取的完整性，每當啟用UDLD的介面被禁用或裝置被重置時，受配置改變影響的介面的所有現有快取條目都被清除，並且UDLD傳送至少一個消息以通知各自的鄰居刷新相應的快取條目。
- **回聲檢測機**制 — 回聲機制是檢測演算法的基礎。每當UDLD裝置得知新鄰居或收到來自失去同步的鄰居的重新同步要求時，都會在連線其一側開始/重新啟動偵測視窗，並傳送一連串回應訊息來回覆。由於所有鄰居的此行為必須相同，因此回應要求回應要求回送傳送者。如果檢測視窗結束並且未收到有效的回覆消息，則認為該鏈路是單向的，並且可能會觸發鏈路重建或埠關閉過程。

## 收斂時間

為了防止STP回圈，CatOS 5.4(3)將UDLD預設訊息間隔從60秒縮短為15秒，以便在受阻連線埠能夠轉換為轉送狀態之前關閉單向連結。

**注意：**消息間隔值確定鄰居在鏈路連線或檢測階段後傳送UDLD探測的速率。消息間隔不需要在鏈路兩端匹配，但需要儘可能採用一致的配置。建立UDLD鄰居時，將傳送配置的消息間隔，並計算

該對等體的超時間隔為(3 * message_interval)。 因此，在丟失三個連續的hello（或探測）後，對等關係超時。由於每一端的消息間隔不同，因此該超時值在每一端也是不同的。

UDLD偵測單向失敗所需的大約時間約為（2.5 * message_interval + 4秒），或使用預設訊息間隔15秒約需41秒。這遠遠低於STP重新收斂通常所需的50秒。如果NMP CPU有一些空閒週期，並且仔細監控其使用級別，您可以將消息間隔（偶數）減少到至少7秒。此消息間隔有助於以顯著因素加快檢測速度。

因此，UDLD預設依賴於預設跨距樹狀目錄計時器。如果調整STP收斂速度比UDLD更快，請考慮替代機制，例如CatOS 6.2環路防護功能。實施RSTP(IEEE 802.1w)時還要考慮另一種機制，因為RSTP的收斂特性以毫秒為單位，具體取決於拓撲。對於這些例項，請將環路防護與UDLD結合使用，後者可提供最多的保護。環路防護可防止STP環路的速度與正在使用的STP版本的速度相同，並且UDLD會檢測單個EtherChannel鏈路上的單向連線，或者BPDU不會沿斷開的方向流動的情況。

**註**：UDLD不會捕獲每個STP故障情況，例如由於CPU傳送的BPDU的時間不大於(2 * FwdDelay + Maxage)而導致的故障。 因此，Cisco建議您在依賴STP的拓撲中將UDLD與環路防護（在CatOS 6.2中引入）結合使用。

**注意**：請注意UDLD的早期版本使用不可配置的60秒預設消息間隔。這些版本容易受到生成樹環路情況的影響。

## UDLD主動模式

建立積極UDLD是為了專門解決那些需要持續測試雙向連線的（少數）情況。因此，主動模式功能可在以下情況下針對危險的單向鏈路狀況提供增強保護：

- 當UDLD PDU的丟失是對稱的，並且兩端超時時，兩個埠都不會被錯誤禁用。
- 連結的一端連線埠停滯（傳輸[Tx]和Rx）。
- 連結的一端保持開啟狀態，而連結的另一端已關閉。
- 已禁用自動協商或其他L1故障檢測機制。
- 希望降低對L1 FEFI機制的依賴。
- 必須針對點對點FE/GE鏈路上的單向鏈路故障提供最大保護。具體來說，如果兩個鄰居之間不允許出現故障，則UDLD主動探測可以視為「心跳」，其存在可保證鏈路的正常運行。

實施積極UDLD的最常見情況是，當自動協商或其他L1故障檢測機制被禁用或不可用時，對套件組合的成員執行連線檢查。EtherChannel連線尤其如此，因為PAgP/LACP（即使已啟用）在穩定狀態下也不會使用非常低的hello計時器。在這種情況下，主動式UDLD還有額外的優勢，可防止可能的跨距樹狀目錄回圈。

導致UDLD探測資料包對稱丟失的情況更難以描述。您必須瞭解，正常的UDLD會檢查單向連結情況，即使連結達到雙向狀態之後也是如此。UDLD的用意是檢測導致STP環路的L2問題，而那些問題通常是單向的，因為BPDU在穩態時僅沿一個方向流動。因此，將普通UDLD與自動協商和環路防護（對於依賴STP的網路）結合使用幾乎總是足夠的。但是，UDLD主動模式在擁塞受到兩個方向的影響相同的情況下是有益的，這會導致兩個方向的UDLD探測器丟失。例如，如果鏈路兩端的CPU利用率提高，則可能會發生UDLD探測的丟失。雙向連線丟失的其他示例包括下列裝置之一的故障：

- 高密度分波多工(DWDM)轉頻器
- 媒體轉換器
- 集線器
- 另一個L1裝置**注意**：自動協商無法檢測到故障。

在這些故障情況下，主動的UDLD錯誤會禁用埠。在非點對點連結上啟用UDLD主動式模式時，請謹

慎考慮後果。與媒體轉換器、集線器或類似裝置的鏈路不是點對點鏈路。中間裝置可以防止UDLD資料包的轉發，並強制不必要地關閉鏈路。

連線埠的所有鄰居都已老化後，UDLD主動模式（如果已啟用）會重新啟動連結序列，嘗試與任何可能不同步的鄰居重新同步。這項工作在廣告或檢測階段進行。如果連線經過一連串快速訊息（八次重試失敗）後仍認為連結「未決定」，則連線埠會進入錯誤停用狀態。

**注意**：某些交換機不支援積極UDLD。目前，Catalyst 2900XL和Catalyst 3500XL的硬編碼消息間隔為60秒。我們認為此間隔不夠快，無法防止潛在的STP環路（使用預設STP引數）。

## 路由連結上的UDLD

在本討論中，路由鏈路是兩種連線型別之一：

- 兩個路由器節點之間的點對點此鏈路配置有30位子網掩碼。
- 具有多個埠但僅支援路由連線的VLAN例如，拆分L2核心拓撲。

每個內部網關路由協定(IGRP)在處理鄰居關係和路由收斂方面都有其獨有的特徵。當您對比當前使用的兩種較流行的路由協定(開放最短路徑優先(OSPF)協定和增強型IGRP(EIGRP))時，本節討論的特性是相關的。

首先，請注意，任何點對點路由網路上的L1或L2故障都會導致L3連線幾乎立即斷開。由於該VLAN中的唯一交換機埠在L1/L2故障時轉換為非連線狀態，因此MSFC自動狀態功能可在大約兩秒內同步L2和L3埠狀態。此同步會將L3 VLAN介面置於開啟/關閉狀態（關閉線路通訊協定）。

採用預設計時器值。OSPF每10秒傳送一次hello消息，死間隔為40秒(4 * hello)。 對於OSPF點對點網路和廣播網路，這些計時器是一致的。因為OSPF需要雙向通訊才能形成鄰接關係，所以最壞情況下的故障切換時間為40秒。即使L1/L2故障不是純點對點連線，也會發生此故障切換，這就留有了L3協定必須處理的半操作場景。由於UDLD的檢測時間與OSPF dead計時器的過期時間（約40秒）非常相似，因此在OSPF L3點對點鏈路上配置UDLD正常模式的優勢有限。

在許多情況下，EIGRP收斂速度比OSPF更快。但是，您必須注意，鄰居之間無需雙向通訊即可交換路由資訊。在非常特定的半運行故障情況下，EIGRP容易受到流量黑孔的影響，該黑孔會持續到某個其他事件使通過該鄰居的路由變為「活動」狀態。UDLD正常模式可以緩解本節註明的情形。UDLD正常模式檢測單向鏈路故障並錯誤禁用埠。

對於使用任何路由協定的L3路由連線，UDLD正常模式仍提供保護，防止在初始鏈路啟用時出現問題。這些問題包括佈線錯誤或硬體故障。此外，UDLD主動模式在L3路由連線上提供以下優勢：

- 防止不必要的流量黑洞**注意：在**某些情況下需要最小計時器。
- 將抖動鏈路置於`errdisable`狀態
- 防止由第3層EtherChannel配置引起的環路

## UDLD的預設行為

預設情況下，UDLD全域性禁用並在光纖埠上啟用就緒狀態。因為UDLD是僅交換機之間必需的基礎架構協定，所以在銅纜埠上預設禁用UDLD。銅纜埠通常用於主機訪問。

**注意**：必須在介面級別全域性啟用UDLD，鄰居才能達到雙向狀態。在CatOS 5.4(3)及更新版本中，預設訊息間隔為15秒，可在7到90秒之間設定。

錯誤停用復原功能預設會全域停用。全域性啟用後，如果連線埠進入`errdisable`狀態，則會在選定的

時間間隔後自動重新啟用連線埠。預設時間為300秒，這是全域計時器，會為交換器中的所有連線埠進行維護。如果將連線埠的錯誤停用逾時設定為，可以手動防止連線埠重新啟用。發出set port errdisable-timeout *mod*/*port* disable 命令。

**注意：**此命令的使用取決於您的軟體版本。

當您在沒有帶外網路管理功能的情況下實作UDLD主動模式時，特別是在存取層或在發生錯誤停用情況時可能與網路隔離的任何裝置上，請考慮使用錯誤停用逾時功能。

有關如何為處於錯誤停用狀態的連線埠設定逾時時間的詳細資訊，請參閱設定乙太網路、快速乙太網路、GB乙太網路和10-GB乙太網路交換。

## 建議

如果正確使用普通模式UDLD並結合適當的功能和協定，在絕大多數情況下，正常模式UDLD就足夠了。這些功能/協定包括：

- FEFI
- 自動交涉
- 環路防護

部署UDLD時，請考慮是否需要持續測試雙向連線（主動模式）。通常情況下，如果啟用了自動協商，則不需要主動模式，因為自動協商會補償L1的故障檢測。

Cisco建議在將UDLD訊息間隔設定為15秒預設值的Cisco交換器之間的所有點對點FE/GE連結上啟用UDLD正常模式。此組態假設使用預設的802.1d跨距樹狀目錄計時器。此外，在依賴STP實現冗餘和融合的網路中，將UDLD與環路防護結合使用。此建議適用於拓撲中有一個或多個埠處於STP阻塞狀態的網路。

核發以下命令，以便啟用UDLD:

```
set udld enable
!--- After global enablement, all FE and GE fiber !--- ports have UDLD enabled by default. set udld enable port range
!--- This is for additional specific ports and copper media, if needed.
```

您必須手動啟用由於單向連結症狀而錯誤停用的連線埠。發出**set port enable**命令。

如需詳細資訊，請參閱瞭解和設定單向連結偵測通訊協定(UDLD)功能。

## 其他選項

要獲得針對由單向鏈路導致的症狀的最大保護，請配置主動模式UDLD:

```
set udld aggressive-mode enable port_range
```

此外，在受支援的情況下，您可以將UDLD消息間隔值調整為每端7到90秒，以加快收斂速度：

```
set udld interval time
```

發生錯誤停用情況時，請考慮在可能從網路隔離的任何裝置上使用錯誤停用逾時功能。對於接入層以及當您實施不帶帶外網路管理功能的UDLD主動模式時，通常會出現這種情況。

如果連線埠處於errdisable狀態，則連線埠預設會保持關閉狀態。您可以發出以下命令，該命令會在超時間隔後重新啟用埠：

**注意：**預設情況下，超時間隔為300秒。

```
>set errdisable-timeout enable ?
bpdu-guard
!--- This is BPDU port-guard. channel-misconfig !--- This is a channel misconfiguration. duplex-
mismatch udld other !--- These are other reasons. all !--- Apply errdisable timeout to all
reasons.
```

如果夥伴裝置不支援UDLD（例如終端主機或路由器），則不要運行協定。發出以下命令：

```
set udld disable port_range
```

## 測試和監控UDLD

如果實驗室中沒有真正的故障/單向元件（例如GBIC故障），UDLD就不容易測試。此協定旨在檢測比實驗室中通常使用的方案更不常見的故障方案。例如，如果執行簡單的測試並拔下光纖的一股電纜以檢視所需的errdisable狀態，則需要關閉L1自動交涉。否則，實體連線埠會關閉，這會重設UDLD訊息通訊。遠端在UDLD正常情況下移動到未確定狀態。如果使用UDLD主動模式，遠端會移至errdisable狀態。

還有一種額外的測試方法來模擬UDLD的鄰居PDU丟失。使用MAC層過濾器可封鎖UDLD/CDP硬體位址，但允許其他位址通過。

若要監控UDLD，請發出以下命令：

```
>show udld

UDLD              : enabled
Message Interval  : 15 seconds
```

```
>show udld port 3/1

UDLD              : enabled
Message Interval  : 15 seconds
Port      Admin Status  Aggressive Mode  Link State
--------  ------------  ---------------  ----------------
3/1       enabled       disabled         bidirectional
```

您還可以在enable模式下發出hidden show udld neighbor命令，以檢查UDLD快取內容（方式與CDP相同）。將UDLD快取與CDP快取進行比較以驗證是否存在協定特定的異常通常很有用。每當CDP也受到影響時，所有PDU/BPDU通常都會受到影響。因此，還要檢查STP。例如，檢查最近的根標識更改或根/指定埠位置更改。

```
>show udld neighbor 3/1

Port  Device Name            Device ID    Port-ID OperState
----- --------------------  ------------ ------- ----------
3/1   TSC07117119M(Switch)   000c86a50433 3/1     bidirectional
```

此外，您還可以使用Cisco UDLD SNMP MIB變數監控UDLD狀態和配置一致性。

## 巨量訊框

所有乙太網埠（包括GE和10 GE）的預設最大傳輸單元(MTU)幀大小為1518位元組。巨型幀功能使介面能夠交換大於標準乙太網幀大小的幀。此功能可用於最佳化伺服器到伺服器的效能，並支援多協定標籤交換(MPLS)、802.1Q隧道和L2隧道協定版本3(L2TPv3)等應用程式，這些應用程式會增加原始幀的大小。

### 操作概述

IEEE 802.3標準規範將常規幀的最大乙太網幀大小定義為1518位元組，將802.1Q封裝幀定義為1522位元組。802.1Q封裝的幀有時稱為「小巨人」。 通常，當資料包超過特定乙太網連線的指定乙太網最大長度時，資料包會被分類為巨型幀。巨型資料包也稱為巨型幀。

某些幀的MTU大小可能超過1518位元組的原因有很多，以下是一些示例：

- 供應商特定要求 — 應用程式和某些NIC可以指定超出標準1500位元組的MTU大小。指定此類MTU大小的趨勢是由於已進行的研究，這些研究證明了乙太網幀大小的增加可以提高平均吞吐量。
- 中繼 — 為了在交換機或其他網路裝置之間傳輸VLAN ID資訊，已採用中繼來擴展標準乙太網幀。如今，兩種最常見的中繼形式是Cisco專有ISL封裝和IEEE 802.1Q。
- MPLS — 在介面上啟用MPLS後，可能會增加資料包的幀大小。此增強取決於標籤堆疊中標籤數量為MPLS標籤的資料包。標籤的總大小為4位元組。標籤堆疊的總大小為*n* x 4位元組。如果形成標籤堆疊，則幀可能會超過MTU。
- 802.1Q通道 — 802.1Q通道資料包包含兩個802.1Q標籤，通常硬體每次只能看到其中一個標籤。因此，內部標籤會將4個位元組新增到MTU值（負載大小）。
- 通用傳輸介面(UTI)/L2TPv3 - UTI/L2TPv3封裝要通過IP網路轉發的L2資料。封裝可以將原始幀大小最多增加50位元組。新幀包括一個新的IP報頭（20位元組）、一個L2TPv3報頭（12位元組）和一個新的L2報頭。L2TPv3負載包含完整的L2幀，其中包括L2報頭。

不同的Catalyst交換機支援各種幀大小的能力取決於許多因素，包括硬體和軟體。某些模組可以支援比其它模組更大的幀大小，即使在同一平台中也是如此。

- Catalyst 5500/5000交換器在CatOS 6.1版本中支援巨型訊框。在連線埠上啟用巨型訊框功能時，MTU大小會增至9216位元組。在基於10/100 Mbps非遮蔽雙絞線(UTP)的線卡上，支援的最大幀大小僅為8092位元組。此限制是ASIC限制。啟用巨型幀大小功能時通常沒有限制。您可以將此功能用於中繼/非中繼和通道/非通道。
- 由於ASIC限制，Catalyst 4000交換機（Supervisor Engine 1 [WS-X4012]和Supervisor Engine 2 [WS-X4013]）不支援巨型幀。但是，例外情況是802.1Q中繼。
- Catalyst 6500系列平台可支援CatOS 6.1(1)及更新版本中的巨型幀大小。但是，此支援取決於您使用的線卡的型別。啟用巨型幀大小功能時通常沒有限制。您可以將此功能用於中繼/非中繼和通道/非通道。在單個埠上啟用巨型幀支援後，預設MTU大小為9216位元組。無法使用CatOS設定預設MTU。但是，Cisco IOS軟體版本12.1(13)E引入了system jumbomtu 命令以覆寫預設的MTU。

如需詳細資訊，請參閱Catalyst交換器上的巨型訊框支援組態範例。

下表說明Catalyst 6500/6000系列交換器的不同線卡支援的MTU大小：

**注意**：MTU大小或封包大小僅指乙太網路負載。

| **線路卡** | **MTU大小** |
|---|---|
| 預設 | 9216 位元組 |
| WS-X6248-RJ-45、WS-X6248A-RJ-45 WS-X6248-TEL、WS-X6248A-TEL WS-X6348-RJ-45(V)、WS-X6348-RJ-21(V) | 8092位元組（受PHY晶片限制） |
| WS-X6148-RJ-45(V)、WS-X6148-RJ-21(V)WS-X6148-45AF、WS-X6148-21AF | 9100位元組(@ 100 Mbps)9216位元組(@ 10 Mbps) |
| WS-X6148A-RJ-45、WS-X6148A-45AF、WS-X6148-FE-SFP | 9216 位元組 |
| WS-X6324-100FX-MM，-SM，WS-X6024-10FL-MT | 9216 位元組 |
| WS-X6548-RJ-45、WS-X6548-RJ-21、WS-X6524-100FX-MM WS-X6148X2-RJ-45、WS-X6148X2-45AF WS-X6196-RJ-21、WS-X619 -21AF WS-X6408-GBIC、WS-X6316-GE-TX、WS-X6416-GBIC WS-X6516-GBIC、WS-X6516A-GBIC、WS-X6816-GBIC管理引擎1、2、32和720上行鏈路 | 9216 位元組 |
| X6516-GE-TX | 8092位元組(@ 100 Mbps)9216位元組（@ 10或1000 Mbps） |
| WS-X6148-GE-TX、WS-X6148V-GE-TX、WS-X6148-GE-45AF、WS-X6548-GE-TX、WS-X6548V-GE-TX、WS-X6548-GE-45AF | 1500位元組（不支援巨型訊框） |
| WS-X6148A-GE-TX、WS-X6148A-GE-45AF、WS-X6502-10GE、WS-X67xx系列 | 9216 位元組 |
| OSM ATM(OC12c) | 9180 位元組 |
| OSM CHOC3、CHOC12、CHOC48、CT3 | 9216位元組（OCx和DS3）7673位元組(T1/E1) |
| Flex WAN | 7673位元組(CT3 T1/DS0)9216位元組(OC3c POS)7673位元組(T1) |

| | |
|---|---|
| CSM(WS-X6066-SLB-APC) | 9216位元組(自CSM 3.1(5)和3.2(1)起) |
| OSM POS OC3c、OC12c、OC48c;OSM DPT OC48c，OSM GE WAN | 9216 位元組 |

## 第3層巨型訊框支援

Catalyst 6500/6000交換器搭載Supervisor Engine上執行的CatOS和在MSFC上執行的Cisco IOS軟體，也使用PFC/MSFC2、PFC2/MSFC2或更新版本硬體，在Cisco IOS®軟體版本12.1(2)E和更新版本中提供L3巨型訊框支援。如果入口和出口VLAN都配置為巨型幀，則所有資料包都由PFC以線速進行硬體交換。如果輸入VLAN是為巨型幀配置的，而輸出VLAN未配置，則有兩種情況：

- 終端主機傳送的巨型訊框，其中已設定「不分段(DF)」位元（用於路徑MTU探索） — 捨棄封包，並將無法連線的網際網路控制訊息通訊協定(ICMP)傳送給終端主機，其中具有所需的訊息代碼片段和DF。
- 終端主機傳送的未設定DF位元的巨型幀 — 將資料包傳送到MSFC2/MSFC3，以便在軟體中進行分段和交換。

下表總結了各種平台的L3巨量支援：

| **L3交換機或模組** | **最大L3 MTU大小** |
|---|---|
| Catalyst 2948G-L3/4908G-L3系列 | 不支援巨型幀。 |
| Catalyst 5000 RSM[1]/RSFC[2] | 不支援巨型幀。 |
| Catalyst 6500 MSFC1 | 不支援巨型幀。 |
| Catalyst 6500 MSFC2及更高版本 | Cisco IOS軟體版本12.1(2)E:9216 位元組 |

[1] RSM =路由交換模組

[2] RSFC =路由交換功能卡

## 網路效能注意事項

TCP在WAN(Internet)上的效能已得到廣泛的研究。此等式說明TCP吞吐量如何具有基於以下各項的上限：

- 最大片段大小(MSS)，即MTU長度減去TCP/IP標頭的長度
- 來回時間(RTT)
- 封包遺失

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

根據此公式，可達到的最大TCP吞吐量與MSS成正比。在持續RTT和資料包丟失的情況下，如果資料包大小翻倍，則TCP吞吐量可以翻倍。同樣，如果使用巨型幀而不是1518位元組幀，則大小增加六倍可能會使乙太網連線的TCP吞吐量提高六倍。

其次，伺服器群不斷增長的效能需求需要更高效的方法來確保網路檔案系統(NFS)UDP資料包具有較高的資料速率。NFS是在基於UNIX的伺服器之間傳輸檔案的最廣泛部署資料儲存機制，它具有8400位元組的資料包。假定乙太網的擴展9 KB MTU，單個巨型幀足夠大，可承載8 KB的應用程式資料包（例如NFS）加上資料包報頭開銷。此功能偶爾允許在主機上實現更高效的直接記憶體訪問(DMA)傳輸，因為軟體不再需要將NFS塊分段為單獨的UDP資料包。

### 建議

當需要巨型幀支援時，請將巨型幀的使用限制到所有交換機模組(L2)和介面(L3)都支援巨型幀的網路區域。此組態會防止路徑中的任何位置進行分段。由於需要分段，因此配置大於路徑中支援的訊框長度的巨型訊框將消除使用該功能獲得的任何增益。如此巨型幀部分中的表所示，不同的平台和線卡可能會因支援的最大資料包大小而異。

為主機裝置所在的整個L2 VLAN配置巨型幀感知主機裝置，其MTU大小是網路硬體支援的最小公分母。若要對具有巨型訊框支援的模組啟用巨型訊框支援，請發出以下命令：

```
set port jumbo mod/port enable
```

此外，如果您希望跨第3層邊界支援巨型幀，請在所有適用的VLAN介面上配置最大可用MTU值9216位元組。在VLAN介面下發出**mtu**命令：

```
interface vlan vlan# mtu 9216
```

此配置可確保模組支援的L2巨型幀MTU始終小於或等於為流量經過的L3介面配置的值。這可防止流量從VLAN通過L3介面路由時進行分段。

## 管理配置

本節將討論Catalyst網路控制、布建及疑難排解的注意事項。

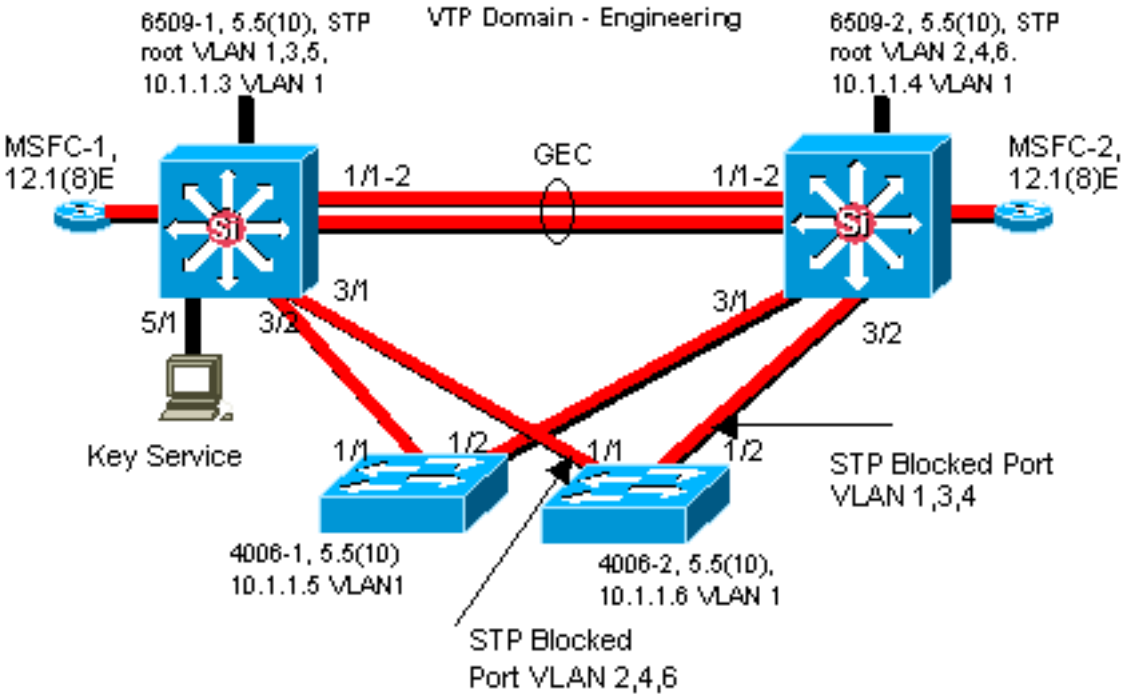
### 網路圖

清晰的網路圖是網路操作的基本部分。在故障排除過程中，它們變得至關重要，在故障期間上報給供應商和合作夥伴時，它們是資訊通訊的最重要工具。它們的準備、就緒性和可訪問性不容低估。

### 建議

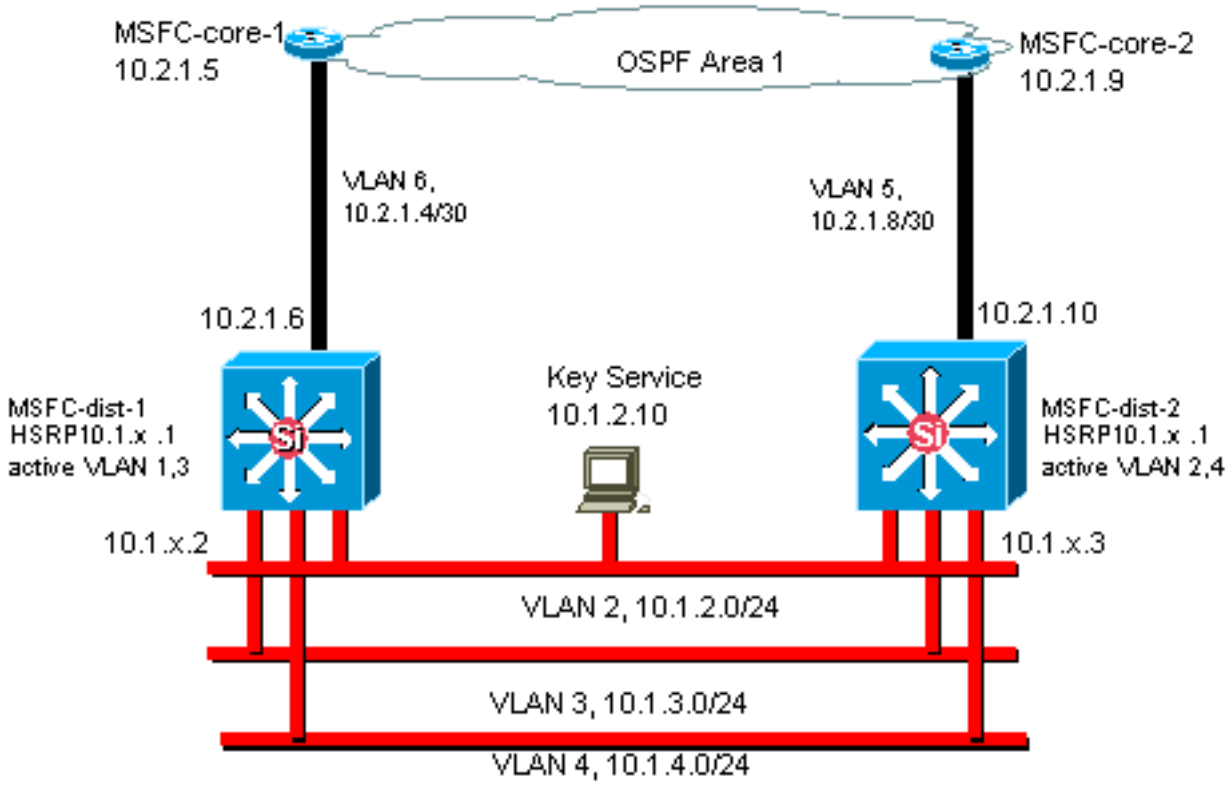
思科建議您建立以下三個圖表：

- **總體圖** — 即使對於最大的網路，顯示端到端物理和邏輯連線的圖也非常重要。實施分層設計的企業通常會分別記錄每個層。然而，在規劃和解決問題的過程中，往往需要很好地瞭解各個領域是如何連線在一起的。
- **物理圖** — 顯示所有交換機和路由器硬體及佈線。必須標籤每個VLAN的中繼、鏈路、速度、通道組、埠號、插槽、機箱型別、軟體、VTP域、根網橋、備份根網橋優先順序、MAC地址和阻塞埠。將內部裝置（例如Catalyst 6500/6000 MSFC）描述為通過中繼連線的單臂路由器通常




更為清晰。

- **Logical Diagram** — 僅顯示L3功能（路由器作為對象，VLAN作為乙太網段）。必須標籤IP地址、子網、輔助定址、HSRP主用和備用、接入核心分佈層和路由資訊。




## 帶內管理

根據配置，交換機帶內（內部）管理介面（稱為sc0）可能必須處理以下資料：

- 交換機管理協定，例如SNMP、Telnet、安全殼協定(SSH)和系統日誌
- 廣播和組播等使用者資料
- 交換機控制協定，例如STP BPDU、VTP、DTP、CDP等

思科多層設計中的常見做法是配置跨交換域並包含所有sc0介面的管理VLAN。這有助於將管理流量與使用者流量分開，並提高交換機管理介面的安全性。本節介紹使用預設VLAN 1和將管理流量與使

用者流量運行到同一VLAN中的交換機的重要性和潛在問題。

## 操作概述

對於將VLAN 1用於使用者資料的問題，主要考慮是Supervisor引擎NMP通常不需要被終端站生成的許多組播和廣播流量中斷。較舊的Catalyst 5500/5000硬體（尤其是監督器引擎I和管理器引擎II）只有有限的資源來處理此流量，但該原則適用於所有Supervisor引擎。如果Supervisor引擎CPU、緩衝區或到背板的帶內通道被完全佔用，偵聽不必要的流量，則可能會丟失控制幀。在最壞的情況下，這可能導致生成樹環路或EtherChannel故障。

如果在Catalyst上發出show interface和**show ip stats**命令，它們可以提供有關廣播流量與單播流量的比例以及IP流量與非IP流量的比例的一些指示（管理VLAN中通常看不到此部分）。

對舊版Catalyst 5500/5000硬體的進一步運行狀況檢查是檢查**show inband** 的輸出 / *biga(*隱藏命令)表示資源錯誤(RsccrcErrors)，類似於路由器中的緩衝區丟棄。如果這些資源錯誤持續增加，記憶體將不可用於接收系統資料包，可能是因為管理VLAN中存在大量廣播流量。單一資源錯誤可能意味著Supervisor Engine無法處理封包（例如BPDU），這很快就會成為一個問題，因為跨距樹狀目錄等通訊協定不會重新傳送遺失的BPDU。

## 建議

如本檔案的Cat控制一節重點說明的，VLAN 1是標籤和處理大多數控制平面流量的特殊VLAN。預設情況下，VLAN 1在所有中繼上啟用。對於大型園區網路，需要注意VLAN 1 STP域的**直徑**;網路某一部分的不穩定性可能會影響VLAN 1，從而影響控制平面穩定性，因此會影響所有其他VLAN的STP穩定性。在CatOS 5.4及更高版本中，可以使用以下命令限制VLAN 1傳輸使用者資料和運行STP:

```
clear trunk mod/port vlan 1
```

這不會停止控制資料包從VLAN 1中的交換機傳送到交換機，如網路分析器所示。但是，不會轉發任何資料，也不會通過此鏈路運行STP。因此，此技術可用於將VLAN 1劃分為更小的故障域。

**附註：** 目前無法清除3500和2900XL上的VLAN 1中繼。

即使注意園區設計將使用者VLAN限制到相對較小的交換機域和相對較小的故障/L3邊界，一些客戶仍會傾向於以不同方式處理管理VLAN，並嘗試使用單個管理子網覆蓋整個網路。中央NMS應用與其管理的裝置之間必須是L2鄰接，這是沒有技術原因的，也不是合格的安全引數。思科建議您將管理VLAN的直徑限制在與使用者VLAN相同的路由域結構中，並考慮將帶外管理和/或CatOS 6.x SSH支援作為提高網路管理安全性的一種方式。

## 其他選項

但是，在某些拓撲中，存在這些思科建議的設計注意事項。例如，理想的通用思科多層設計可以避免使用活動的生成樹。這需要您將每個IP子網/VLAN限製為單個接入層交換機或交換機集群。在這些設計中，不能向下配置到接入層的中繼。

對於是否建立獨立的管理VLAN並啟用中繼以便在第2層接入層和第3層分佈層之間傳輸它的問題，沒有簡單的答案。以下兩個選項供您的思科工程師進行設計稽核：

- **選項1:**將兩個或三個唯一的VLAN從分佈層向下中繼到每台接入層交換機。例如，這允許使用資料VLAN、語音VLAN和管理VLAN，並且仍然具有STP處於非活動狀態的優點。（請注意，如果從中繼中清除VLAN 1，則會執行額外的配置步驟。）在此解決方案中，為了避免在故障恢復期間臨時阻塞路由流量，還需要考慮以下設計要點：中繼的STP PortFast（CatOS 7.x及更高版本）或具有STP轉發的VLAN自動狀態同步（CatOS 5.5[9]以上）。
- **選項2:**資料和管理的單個VLAN是可以接受的。使用較新的交換機硬體（例如更強大的CPU和控制平面速率限制控制），再加上多層設計所倡導的具有相對較小的廣播域的設計，許多客戶的實際情況是，保持sc0介面與使用者資料分離不像以前那樣是一個問題。最好通過檢查該VLAN的廣播流量量變曲線，並與您的思科工程師討論交換機硬體的功能來作出最終決定。如果管理VLAN確實包含該接入層交換機上的所有使用者，則強烈建議使用IP輸入過濾器從使用者那裡保護交換機，如本文安全配置一節所述。

## 帶外管理

將前一節的論點進一步擴大，通過在生產網路周圍構建單獨的管理基礎設施，可以使網路管理更加可用，以便無論發生什麼流量驅動事件或控制平面事件，都能始終遠端訪問裝置。這兩種方法是典型的：

- 使用專用LAN的帶外管理
- 使用終端伺服器的帶外管理

### 操作概述

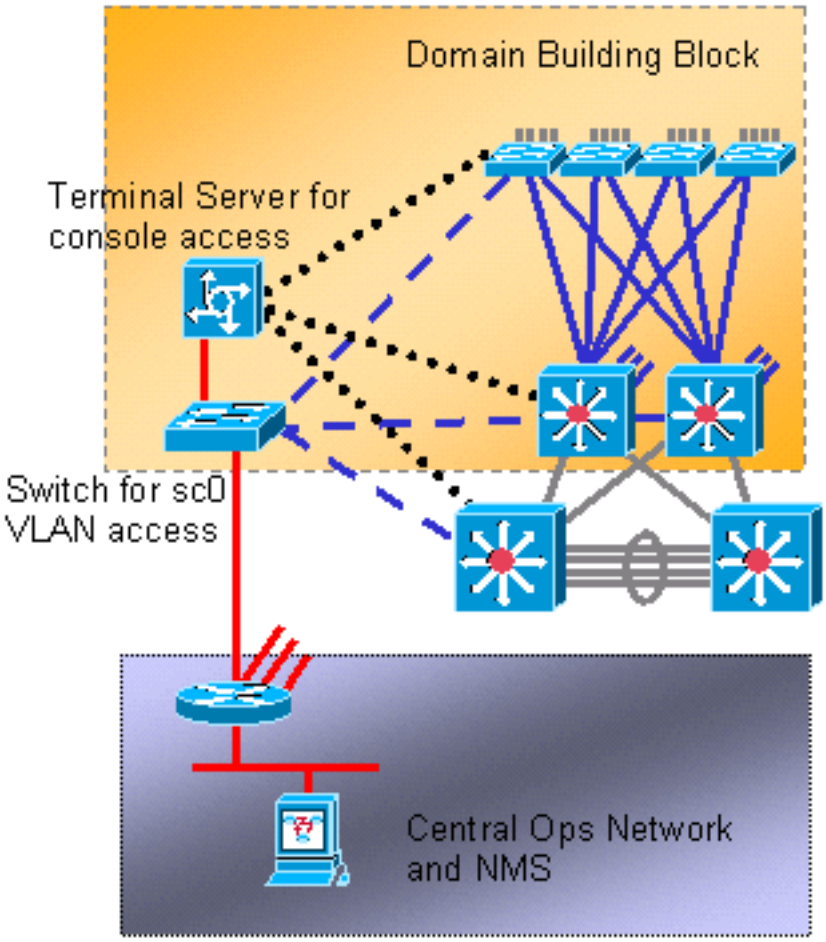
網路中的每台路由器和交換機都可以在管理VLAN上提供帶外乙太網管理介面。每個裝置上的一個乙太網埠配置在管理VLAN中，並在生產網路外部通過sc0介面連線到單獨的交換管理網路。請注意，Catalyst 4500/4000交換器在Supervisor Engine上有一個特殊的me1介面，該介面僅用於頻外管理，而不是用作交換器連線埠。

此外，終端伺服器連線可通過配置Cisco 2600或3600（使用RJ-45到串列電纜）來訪問佈局中每台路由器和交換機的控制檯埠。終端伺服器還避免配置備份方案，例如每台裝置的輔助埠上的數據機。可在終端伺服器的輔助埠上配置單個數據機，以便在網路連線失敗期間向其他裝置提供撥號服務。

### 建議

通過這種配置，除了多條帶內路徑外，還可以提供到每台交換機和路由器的兩條帶外路徑，從而實現高可用網路管理。帶外負責：

- 帶外將管理流量與使用者資料分離。
- 帶外將管理IP地址放在單獨的子網、VLAN和交換機中，以實現更高的安全性。
- 在網路出現故障時，帶外可為管理資料傳送提供更高的保證。
- 帶外管理VLAN中沒有活動的生成樹。冗餘不是關鍵。




## 系統測試

### 開機診斷

在系統啟動期間，會執行許多進程，以確保提供可靠的運行平台，使有故障的硬體不會中斷網路。Catalyst啟動診斷分為加電自檢(POST)和線上診斷。

### 操作概述

根據平台和硬體配置，啟動時以及卡熱插拔到機箱時執行不同的診斷。更高級別的診斷會導致檢測到更多的問題，但引導週期更長。可以選擇以下三個級別的POST診斷（所有測試都檢查DRAM、RAM和快取存在和大小並初始化它們）：

| 操作概述 | | | |
|---|---|---|---|
| 旁路 | 不適用 | 3 | 在使用CatOS 5.5或更低版本的4500/4000系列上不可用。 |
| 最小 | 僅對第一個MB DRAM執行模式寫入測試。 | 30 | 5500/5000和6500/6000系列上的預設值；在4500/4000系列上不可用。 |
| 完成 | 所有記憶體的模式寫入測試。 | 60 | 4500/4000系列的預設設定。 |

### 線上診斷

這些測試會檢查交換器內的封包路徑。必須注意的是，聯機診斷因此是系統範圍的測試，而不僅僅是埠測試。在Catalyst 5500/5000和6500/6000交換器上，首先從待命Supervisor Engine執行測試，然後從主Supervisor Engine再次執行測試。診斷的長度取決於系統配置（插槽、模組、埠數）。測試分為三類：

- 環回測試 — 將來自Supervisor Engine NMP的資料包傳送到每個埠，然後返回到NMP並檢查錯誤。
- 繫結測試 — 建立最多八個埠的通道，並對agport執行環回測試，以驗證到特定鏈路的雜湊(有關詳細資訊，請參閱本文檔的EtherChannel部分)。
- 增強型位址識別邏輯(EARL)測試 — 測試中央Supervisor Engine和內嵌乙太網路模組L3重寫引擎。在從NMP通過每個模組上的交換硬體傳送示例資料包（針對每種協定封裝型別）並返回到NMP之前，會建立硬體轉發條目和路由埠。適用於Catalyst 6500/6000 PFC模組及更新版本。

完成線上診斷大約需要兩分鐘。最低診斷不會對除Supervisor Engine以外的模組執行套件組合或重寫測試，且可能要花費大約90秒。

在儲存器測試期間，當在模式讀回中發現與所寫入的模式相比的差異時，埠狀態變為。如果發出**show test**命令，然後是要檢查的模組號，就可以看到這些測試的結果：

```
>show test 9

Diagnostic mode: complete (mode at next reset: complete)
!--- Configuration setting. Module 9 : 4-port Multilayer Switch Line Card Status for Module 9 :
PASS Port Status : Ports 1 2 3 4 ----------------- . . . . Line Card Diag Status for Module 9 (.
= Pass, F = Fail, N = N/A) Loopback Status [Reported by Module 1] : Ports 1 2 3 4 ----------
--- . . F . !--- Faulty. Channel Status : Ports 1 2 3 4 ----------------- . . . .
```

## 建議

思科建議將所有交換機設定為使用完整的診斷程式，以便進行最大程度故障檢測，並防止在正常操作期間發生停機。

**注意**：此更改在下次引導裝置時才會生效。發出以下命令以設定完整的診斷程式：

```
set test diaglevel complete
```

## 其他選項

在某些情況下，較之等待運行完全診斷，快速啟動時間更為可取。系統啟動時還涉及其他因素和時間，但總體而言，POST和線上診斷大約又增加了三分之一的時間。在搭載Catalyst 6509的完全填充的單個Supervisor Engine九插槽機箱進行測試時，完全診斷的總啟動時間大約為380秒，最少診斷時間大約為300秒，而繞過診斷時僅為250秒。發出以下命令以配置旁路：

```
set test diaglevel bypass
```

**註**：Catalyst 4500/4000接受配置為最小診斷，儘管這仍會導致進行完整測試。將來在此平台上可能支援最小模式。

## 運行時診斷

系統運行後，交換機Supervisor Engine將對其他模組執行各種監控。如果模組無法通過管理消息（通過帶外管理匯流排運行的串列控制協定[SCP]）訪問，Supervisor引擎會嘗試重新啟動卡或採取其他適當的操作。

### 操作概述

Supervisor Engine自動進行各種監控；這不需要任何配置。若是Catalyst 5500/5000和6500/6000，交換器的這些元件會受到監控：

- 通過監視程式的NMP
- 增強型EARL晶片錯誤
- 從Supervisor引擎到背板的帶內通道
- 透過帶外通道的keepalive模組(Catalyst 6500/6000)
- 備用Supervisor Engine會監控作用中Supervisor Engine的狀態(Catalyst 6500/6000)

## 系統和硬體錯誤檢測

### 操作概述

在CatOS 6.2及更新版本中，已新增更多功能來監控關鍵系統和硬體層元件。支援以下三個硬體元件：

- 帶內
- 埠計數器
- 記憶體

啟用該功能並檢測到錯誤情況時，交換機將生成系統日誌消息。該消息通知管理員，在明顯的效能降低之前，問題存在。在CatOS版本6.4(16)、7.6(12)、8.4(2)和更新版本中，所有三個元件的預設模式都從停用更改為啟用。

### 帶內

如果檢測到帶內錯誤，系統日誌消息會通知您在發生明顯的效能降低之前出現問題。此錯誤顯示帶內故障發生的型別。例如：

- 帶內阻塞
- 資源錯誤
- 啟動期間帶內失敗

在檢測到帶內ping故障時，此功能還會報告附加的系統日誌消息，其中包含交換機帶內連線、CPU和背板負載上的當前Tx和Rx速率的快照。此消息使您能夠正確確定帶內是停滯不前（無Tx/Rx）還是過載（過量Tx/Rx）。 此附加資訊有助於確定帶內ping失敗的原因。

### 埠計數器

啟用此功能後，它會建立並啟動一個進程以調試埠計數器。埠計數器定期監視選擇內部埠錯誤計數器。線卡的架構，尤其是模組上的ASIC，決定了功能查詢的計數器。然後，思科技術支援或開發工程部門可以使用此資訊排除故障。此功能不會輪詢與連結夥伴連線直接相關的錯誤計數器，例如FCS、CRC、校準和runts。若要加入此功能，請參閱本文檔的EtherChannel/鏈路錯誤處理部分。

輪詢每30分鐘執行一次，並在所選錯誤計數器的後台運行。如果在同一埠上的兩次後續輪詢之間計

數增加，系統日誌消息將報告事件，並提供模組/埠和錯誤計數器詳細資訊。

Catalyst 4500/4000平台不支援連線埠計數器選項。

### 記憶體

啟用此功能將執行後台監控和檢測DRAM損壞情況。此類記憶體損壞情況包括：

- 分配
- 釋放
- 超出範圍
- 對齊錯誤

### 建議

啟用所有錯誤檢測功能，包括支援的帶內、埠計數器和記憶體。啟用這些功能可為Catalyst交換機平台實現改進的主動系統和硬體警告診斷。發出以下命令，以啟用所有三個錯誤檢測功能：

```
set errordetection inband enable
!--- This is the default in CatOS 6.4(16), 7.6(12), 8.4(2), and later. set errordetection
portcounters enable
!--- This is the default in CatOS 6.4(16), 7.6(12), 8.4(2), and later. set errordetection memory
enable
!--- This is the default in CatOS 6.4(16), 7.6(12), 8.4(2), and later.
```

發出以下命令，以確認是否已啟用錯誤檢測：

```
>show errordetection

Inband error detection:                  enabled
Memory error detection:                  enabled
Packet buffer error detection:           errdisable
Port counter error detection:            enabled
Port link-errors detection:              disabled
Port link-errors action:                 port-failover
Port link-errors interval:               30 seconds
```

## EtherChannel/連結錯誤處理

### 操作概述

在CatOS 8.4及更新版本中，已匯入一項新功能，以提供從EtherChannel中一個連線埠到同一EtherChannel中另一個連線埠的流量自動容錯移轉。當通道中的某個連線埠超出指定間隔內的可設定錯誤臨界值時，會發生連線埠容錯移轉。只有在EtherChannel中還剩一個運行埠時，才會發生埠故障切換。如果故障埠是EtherChannel中的最後一個埠，則該埠不會進入`port-failover`狀態。無論接收的錯誤型別如何，此埠都會繼續傳遞流量。單個非通道化的埠不會進入`port-failover`狀態。在指定的間隔內超過錯誤閾值時，這些連線埠會進入`errdisable`狀態。

此功能僅在啟用**set errordetection portcounters**時有效。要監控的連結錯誤取決於三個計數器：

- InErrors
- RxCRC(CRCAlignErrors)

- TxCRC

在交換器上發出show counters命令，以顯示錯誤計數器數量。範例如下：

```
>show counters 4/48

.......

32 bit counters

0  rxCRCAlignErrors           =          0
.......

6  ifInErrors                 =          0
.......

12 txCRC                      =          0
```

下表列出可能的組態引數和各自的預設組態：

| 引數 | 預設 |
|---|---|
| 全域性 | 已禁用 |
| 適用於RxCRC的連線埠監控器 | 已禁用 |
| InErrors的埠監視器 | 已禁用 |
| 適用於TxCRC的連線埠監控器 | 已禁用 |
| 動作 | 埠故障切換 |
| 間隔 | 30秒 |
| 取樣計數 | 3個連續 |
| 低閾值 | 1000 |
| 高閾值 | 1001 |

如果啟用該功能，並且埠的錯誤計數在指定的取樣計數週期內達到可配置閾值的高值，則可配置的操作是錯誤禁用或埠故障切換。錯誤停用操作會將連線埠置於狀態。如果配置埠故障切換操作，則考慮埠通道狀態。只有當連線埠位於通道中，而該連線埠不是通道中最後一個可使用的連線埠時，連線埠才會因為錯誤而停用。此外，如果設定的操作是連線埠容錯移轉，且連線埠是單一連線埠或未通道化，則連線埠錯誤計數達到臨界值的高值時，會將其置於errdisable狀態。

間隔是用於讀取埠錯誤計數器的計時器常數。link-errors interval的預設值為30秒。允許的範圍是介於30和1800秒之間。

連線埠可能會因為意外的一次性事件而意外錯誤停用。為了將此風險降至最低，僅當這種情況持續存在時，才會對埠執行操作。預設取樣值為3，允許的範圍為1到255。

閾值是要基於鏈路錯誤間隔檢查的絕對數。預設鏈路錯誤低閾值為1000，允許的範圍為1到65,535。預設鏈路錯誤高閾值為1001。當連續取樣次數達到低閾值時，將傳送系統日誌。如果連續取樣時間達到高閾值，將傳送系統日誌並觸發錯誤禁用或埠故障轉移操作。

**注意**：對通道中的所有埠使用相同的埠錯誤檢測配置。如需詳細資訊，請參閱Catalyst 6500系列軟體組態設定指南的這些章節：

- 檢查狀態和連線的*配置EtherChannel/鏈路錯誤處理*部分
- 設定乙太網路、快速乙太網路、GB乙太網路和10-GB乙太網路交換的*設定連線埠錯誤偵測*一節

### 建議

因為該功能使用SCP消息來記錄和比較資料，所以大量活動埠可能佔用大量的CPU。如果將閾值間隔設定為非常小的值，則此情況會更加佔用大量CPU。對於指定為關鍵鏈路並承載敏感應用流量的埠，可酌情啟用此功能。發出以下命令可全域性啟用鏈路錯誤檢測：

```
set errordetection link-errors enable
```

另外，請從預設閾值、間隔和取樣引數開始。並使用預設操作，埠故障切換。

核發以下命令，以將全域連結錯誤引數套用到個別連線埠：

```
set port errordetection mod/port inerrors enable

set port errordetection mod/port rxcrc enable

set port errordetection mod/port txcrc enable
```

您可以發出以下命令以驗證link-errors配置：

```
show errordetection

show port errordetection {mod | mod/port}
```

## Catalyst 6500/6000封包緩衝區診斷

在CatOS版本6.4(7)、7.6(5)和8.2(1)中引入了Catalyst 6500/6000封包緩衝區診斷程式。資料包緩衝區診斷（預設情況下啟用）檢測由瞬時靜態RAM(SRAM)故障引起的資料包緩衝區故障。在以下這些48埠10/100-Mbps線路模組上進行檢測：

- X6248-RJ45
- X6248-RJ21
- X6348-RJ45
- X6348-RJ21
- X6148-RJ45
- X6148-RJ21

當發生故障情況時，48個10/100 Mbps埠中有12個繼續保持連線，並可能遇到隨機連線問題。從這種情況下恢復的唯一方法是重新通電線路模組。

### 操作概述

資料包緩衝區診斷程式檢查儲存在資料包緩衝區的特定部分中的資料，以確定資料是否因瞬時SRAM故障而損壞。如果進程讀取的內容與寫入的內容不同，則會執行兩個可能的可配置恢複選項：

1. 預設操作是錯誤禁用受緩衝區故障影響的線卡埠。

2. 第二個選項是重新通電線路卡。

新增了兩個syslog消息。這些訊息提供由於封包緩衝區錯誤而導致連線埠錯誤停用或模組電源循環的警告：

```
%SYS-3-PKTBUFFERFAIL_ERRDIS:Packet buffer failure detected.
Err-disabling port 5/1.
%SYS-3-PKTBUFFERFAIL_PWRCYCLE: Packet buffer failure detected.
Power cycling module 5.
```

在低於8.3和8.4的CatOS版本中，線卡重新通電時間介於30秒和40秒之間。CatOS版本8.3和8.4引入了快速啟動功能。該功能在初始啟動過程中自動將韌體下載到安裝的線卡，以最小化啟動時間。快速引導功能將重新通電時間減少到大約10秒。

## 建議

思科建議使用預設選項*errdisable*。在生產期間，此操作對網路服務的影響最小。如果可能，將受錯誤停用連線埠影響的連線移動到其他可用交換器連線埠，以便還原服務。在維護時段安排線卡的手動電源週期。發出reset module *mod* 命令，以完全從損毀的封包緩衝區狀況中復原。

**注意：**如果在重置模組後錯誤仍然存在，請嘗試重新安放模組。

發出此命令，以啟用*errdisable*選項：

```
set errordetection packet-buffer errdisable
!--- This is the default.
```

## 其他選項

因為要完全恢復遇到SRAM故障的所有埠，線卡需要重新通電，所以另一個恢復操作是配置重新通電選項。如果可以接受網路服務中斷（可能持續30到40秒），此選項非常有用。此時間長度是線路模組在不使用快速引導功能的情況下完全重啟電源並恢復服務所需的時間。使用電源重啟選項，快速引導功能可將網路服務中斷時間縮短到10秒。發出以下命令以啟用電源重啟選項：

```
set errordetection packet-buffer power-cycle
```

## 封包緩衝區診斷

此測試僅適用於Catalyst 5500/5000交換器。本測試旨在查詢使用乙太網模組的Catalyst 5500/5000交換機上的故障硬體，該乙太網模組具有在使用者埠和交換機背板之間提供10/100 Mbps連線的特定硬體。由於它們無法對中繼幀執行CRC檢查，因此，如果埠資料包緩衝區在運行時發生故障，資料包可能會被損壞並導致CRC錯誤。遺憾的是，這可能會導致壞幀進一步傳播到Catalyst 5500/5000 ISL網路，在最壞的情況下可能導致控制平面中斷和廣播風暴。

較新版本的Catalyst 5500/5000模組和其他平台已更新內建的硬體錯誤檢查，且不需要封包緩衝區測試，因此沒有可設定它的選項。

需要資料包緩衝區診斷程式的線路模組是WS-X5010、WS-X5011、WS-X5013、WS-X5020、WS-X5111、WS-X5113、WS-X5114、WS-X5201、WS-X5203、WS-X5213 X5509、WS-U5531、WS-U5533和WS-U5535。

## 操作概述

此診斷程式會檢查儲存在資料包緩衝區的特定部分中的資料是否因硬體故障而意外損壞。如果進程回讀與寫入不同的內容，則會在failed模式下關閉埠，因為該埠可能會損壞資料。不需要錯誤閾值。在重置模組（或更換）之前，無法再次啟用故障埠。

封包緩衝區測試有兩種模式：計畫和按需。測試開始時，將生成系統日誌消息以指示測試的預期長度（向上舍入到最接近的分鐘）以及測試已經開始的事實。確切的測試長度因埠型別、緩衝區大小和測試運行型別而異。

為了能在幾分鐘內完成，按需測試非常積極。由於這些測試會主動干擾資料包記憶體，因此埠在測試之前必須管理性關閉。發出以下命令以關閉連線埠：

```
> (enable) test packetbuffer 4/1
Warning: only disabled ports may be tested on demand - 4/1 will be skipped.
> (enable) set port disable 4/1
> (enable) test packetbuffer 4/1
Packet buffer test started. Estimated test time: 1 minute.
%SYS-5-PKTTESTSTART:Packet buffer test started
%SYS-5-PKTTESTDONE:Packet buffer test done. Use 'show test' to see test results
```

計畫測試比按需測試積極性要低得多，並且是在後台執行的。這些測試在多個模組之間並行執行，但每次在每個模組的一個埠上執行。該測試在恢複使用者資料包緩衝區資料之前保留、寫入和讀取小部分資料包緩衝區記憶體，因此不會生成錯誤。但是，由於該測試寫入緩衝區記憶體，因此它會阻塞傳入資料包幾毫秒，並在繁忙鏈路上造成一些損失。預設情況下，每個緩衝區寫入測試之間有8秒的暫停以最小化任何資料包丟失，但這表示需要資料包緩衝區測試的系統可能需要超過24小時才能完成測試。預設情況下，從CatOS 5.4或更高版本開始，此預設測試將啟用為每週日03:30運行，並且可以通過以下命令確認測試狀態：

```
>show test packetbuffer status

!--- When test is running, the command returns !--- this information: Current packet buffer test
details Test Type : scheduled Test Started : 03:30:08 Jul 20 2001 Test Status : 26% of ports
tested Ports under test : 10/5,11/2 Estimated time left : 11 minutes !--- When test is not
running, !--- the command returns this information: Last packet buffer test details Test Type :
scheduled Test Started : 03:30:08 Jul 20 2001 Test Finished : 06:48:57 Jul 21 2001
```

## 建議

思科建議您對Catalyst 5500/5000系統使用排程封包緩衝區測試功能，因為發現模組上的問題的益處超過低封包遺失的風險。

然後，必須在整個網路中安排標準化的每週時間，使客戶能夠根據需要更改故障埠或RMA模組的鏈路。由於此測試可能導致某些資料包丟失（具體取決於網路負載），因此必須將其安排在比較安靜的網路時間，例如預設時間是星期日上午3:30。發出以下命令以設定測試時間：

```
set test packetbuffer Sunday 3:30
!--- This is the default.
```

一旦啟用（例如CatOS首次升級到5.4及更高版本時），就有可能暴露先前隱藏的記憶體/硬體問題，並自動關閉埠。您可以看到以下訊息：

```
%SYS-3-PKTBUFBAD:Port 1/1 failed packet buffer test
```

## 其他選項

如果每週每個埠承擔低水準資料包丟失的風險是不可接受的，則建議在計畫中斷期間使用按需功能。發出此命令，以便逐個範圍手動啟動此功能（雖然連線埠必須首先在管理上停用）：

```
test packetbuffer port range
```

## 系統記錄

系統日誌消息特定於思科，是主動故障管理的關鍵部分。與通過標準化SNMP相比，使用系統日誌報告的網路和協定條件範圍更廣。Cisco Resource Manager Essentials(RME)和Network Analysis Toolkit(NATkit)等管理平台可有效地利用系統日誌資訊，因為它們執行以下任務：

- 按嚴重性、消息、裝置等顯示分析
- 啟用對傳入消息進行過濾以進行分析
- 觸發警報，例如尋呼機或按需收集庫存和配置更改

## 建議

一個重要的焦點是要在本地生成並保留在交換機緩衝區中的日誌記錄資訊的級別，而不是傳送到系統日誌伺服器的日誌記錄資訊級別(使用set logging server severity *value*命令)。 有些組織會集中記錄較高級別的資訊，而有些組織則轉到交換機本身檢視更詳細的事件日誌，或者僅在故障排除期間啟用更高級別的系統日誌捕獲。

CatOS平台上的調試與Cisco IOS軟體不同，但使用set logging session enable，可以基於每個會話啟用詳細的系統日誌記錄，而無需更改預設日誌記錄。

思科通常建議您將spantree和系統系統日誌設施提升到第6級，因為這些是需要跟蹤的關鍵穩定性功能。此外，對於組播環境，建議將mcast設施的日誌記錄級別設定為4，以便在刪除路由器埠時生成syslog消息。很遺憾，在CatOS 5.5(5)之前，這會導致記錄IGMP加入和離開的系統日誌消息，這種消息太嘈雜而無法監控。最後，如果使用IP輸入清單，建議最低記錄級別為4以捕獲未經授權的登入嘗試。發出以下命令以設定以下選項：

```
set logging buffer 500
!--- This is the default. set logging server syslog server IP address set logging server enable
!--- This is the default. set logging timestamp enable
set logging level spantree 6 default
!--- Increase default STP syslog level. set logging level sys 6 default
!--- Increase default system syslog level. set logging server severity 4
!--- This is the default; !--- it limits messages exported to syslog server. set logging console
disable
```

關閉控制檯消息以防止交換機在消息量較大時掛起的風險，因為交換機需要等待來自速度慢或不存在的終端的響應。在CatOS下，控制檯日誌記錄是高優先順序，主要用於捕獲故障排除時或交換機崩潰場景中的最終消息。

下表提供了Catalyst 6500/6000的各個日誌記錄工具、預設級別和建議的更改。每個平台具有略有不同的工具，具體取決於支援的功能。

| 設施 | 預設級別 | 建議的操作 |
|---|---|---|
| acl | 5 | 別管了。 |
| cdp | 4 | 別管了。 |
| cops | 3 | 別管了。 |
| dtp | 8 | 別管了。 |
| 厄爾 | 2 | 別管了。 |
| ethc[1] | 5 | 別管了。 |
| 檔案系統 | 2 | 別管了。 |
| gvrp | 2 | 別管了。 |
| ip | 2 | **如果使用IP輸入清單，請更改為4。** |
| 核心 | 2 | 別管了。 |
| 1天 | 3 | 別管了。 |
| mcast | 2 | **如果使用多點傳送，請變更為4（CatOS 5.5[5]及更新版本）。** |
| 管理 | 5 | 別管了。 |
| mls | 5 | 別管了。 |
| pagp | 5 | 別管了。 |
| 配置檔案 | 2 | 別管了。 |
| 修剪 | 2 | 別管了。 |
| 專用VLAN | 3 | 別管了。 |
| qos | 3 | 別管了。 |
| radius | 2 | 別管了。 |
| rsvp | 3 | 別管了。 |
| 安全性 | 2 | 別管了。 |
| snmp | 2 | 別管了。 |
| spantree | 2 | **更改為6。** |
| sys | 5 | **更改為6。** |
| tac | 2 | 別管了。 |
| tcp | 2 | 別管了。 |
| telnet | 2 | 別管了。 |
| TFTP | 2 | 別管了。 |
| UDLD | 4 | 別管了。 |
| VMPS | 2 | 別管了。 |
| VTP | 2 | 別管了。 |

[1]在CatOS 7.x及更新版本中，ethc設施代碼會取代pagp設施代碼，以便反映LACP支援。

**註：目前，Catalyst交換機記錄所執行的每個set或clear命令的配置更改syslog 6級消息，這與Cisco IOS軟體不同，Cisco IOS軟體僅在退出配置模式後觸發該消息。**如果您需要RME在此觸發器後即時備份配置，則這些消息也需要傳送到RME系統日誌伺服器。對於大多數客戶來說，定期備份Catalyst交換機配置就足夠了，無需更改預設伺服器日誌記錄嚴重性。

如果調整NMS警報，請參閱系統消息指南。

## 簡單網路管理協定

SNMP用於檢索網路裝置管理資訊庫(MIB)中儲存的統計資訊、計數器和表。 NMS（如HP Openview）可以使用收集的資訊生成即時警報、測量可用性、生成容量規劃資訊，以及幫助執行配置和故障排除檢查。

### 操作概述

藉助一些安全機制，網路管理站能夠使用SNMP協定get和get next請求檢索MIB中的資訊，並使用**set**命令更改引數。此外，網路裝置可配置為生成用於NMS的陷阱消息以進行即時警報。SNMP輪詢使用IP UDP埠161,SNMP陷阱使用埠162。

Cisco支援以下版本的SNMP:

- SNMPv1:RFC 1157網際網路標準，使用明文社群字串安全。IP地址訪問控制清單和密碼定義了能夠訪問代理MIB的管理器社群。
- SNMPv2C:SNMPv2（在RFC 1902至1907中定義的網際網路標準草案）和SNMPv2C（基於SNMPv2的社群管理框架，是RFC 1901中定義的實驗草案）的組合。好處包括批次檢索機制，該機制支援對表和大量資訊的檢索，最大限度地減少了所需的往返次數，並改進了錯誤處理。
- SNMPv3:RFC 2570建議草案通過結合身份驗證和加密網路上的資料包，提供對裝置的安全訪問。SNMPv3中提供的安全功能包括：消息完整性：確保資料包在傳輸過程中未被篡改驗證:確定消息來自有效的源加密：對資料包的內容進行擾動，以防止未經授權的源輕易檢視該資料包

下表列出了安全模型的組合：

| 型號級別 | 驗證 | 加密 | 結果 |
|---|---|---|---|
| v1 | noAuthNoPriv，社群字串 | 否 | 使用社群字串匹配進行身份驗證。 |
| v2c | noAuthNoPriv，社群字串 | 否 | 使用社群字串匹配進行身份驗證。 |
| v3 | noAuthNoPriv，使用者名稱 | 否 | 使用使用者名稱匹配進行身份驗證。 |
| v3 | authNoPriv、MD5或SHA | Np | 提供基於HMAC-MD5或HMAC-SHA演算法的身份驗證。 |
| v3 | authPriv、MD5或SHA | DES | 提供基於HMAC-MD5或HMAC-SHA演算法的身份驗證。除了基於CBC-DES(DES-56)標準的身份驗證外，還提供DES 56位加密。 |

**注意：**請記住有關SNMPv3對象的以下資訊：

- 每個使用者都屬於一個組。
- 組為一組使用者定義訪問策略。
- 訪問策略定義可以訪問SNMP對象進行讀取、寫入和建立的對象。
- 組決定其使用者可以接收的通知的清單。
- 組還為其使用者定義安全模型和安全級別。

## SNMP陷阱建議

SNMP是所有網路管理的基礎，並在所有網路上啟用和使用。必須將交換機上的SNMP代理設定為使用管理站支援的SNMP版本。由於代理可以與多個管理器通訊，因此可以配置軟體以支援與一個使用SNMPv1協定的管理站以及另一個使用SNMPv2協定的管理站的通訊。

目前，大多數NMS站點在此配置下使用SNMPv2C:

```
set snmp community read-only string
!--- Allow viewing of variables only. set snmp community read-write string
!--- Allow setting of variables. set snmp community read-write-all string
!--- Include setting of SNMP strings.
```

思科建議為所有使用中的功能啟用SNMP陷阱（如果需要，可以禁用未使用的功能）。 啟用陷阱後，即可使用test snmp命令進行測試，並在NMS上針對錯誤（例如尋呼機警報或彈出視窗）設定相應的處理方式。

預設情況下會禁用所有陷阱，需要單獨或通過使用**all**引數將其新增到配置中，如下所示：

```
set snmp trap enable all
set snmp trap server address read-only community string
```

CatOS 5.5中的可用陷阱包括：

| 陷阱 | 說明 |
|---|---|
| 身份驗證 | 驗證 |
| 網橋 | 網橋 |
| 機箱 | 機箱 |
| 設定 | 組態 |
| 實體 | 實體 |
| ippermit | IP允許 |
| 模組 | 模組 |
| 中繼器 | 中繼器 |
| stpx | 生成樹擴展 |
| 系統日誌 | 系統日誌通知 |
| vmps | VLAN成員原則伺服器 |
| vtp | VLAN Trunk通訊協定 |

**注意：**syslog陷阱會將交換機生成的所有系統日誌消息也作為SNMP陷阱傳送到NMS。如果Cisco Works 2000 RME等分析器已經在執行系統日誌警報，則兩次接收此資訊不一定有用。

與Cisco IOS軟體不同，埠級別SNMP陷阱預設處於禁用狀態，因為交換機可以有數百個活動介面。因此，思科建議關鍵埠（例如到路由器、交換機和主伺服器的基礎設施鏈路）啟用埠級別SNMP陷阱。不需要其他埠（如使用者主機埠），這有助於簡化網路管理。

```
set port trap port range enable
!--- Enable on key ports only.
```

## SNMP輪詢建議

建議進行一次網路管理審查，以詳細討論具體需要。但是，下面列出了一些管理大型網路的思科基本理念：

- 做一些簡單的事情，並且做得很好。
- 減少由於資料輪詢、收集、工具和手動分析過多導致的員工過載。
- 只需使用幾個工具即可實現網路管理，例如HP Openview（作為NMS）、Cisco RME（作為配置）、系統日誌、清單和軟體管理器、Microsoft Excel（作為NMS資料分析器）以及CGI（作為發佈到Web的方式）。
- 將報告發佈到Web可以讓使用者（如高級管理層和分析師）幫助自己獲取資訊，而不會給操作人員帶來許多特別請求。
- 找出哪些裝置在網路上運行良好，然後放過它。集中精力處理不能正常工作的問題。

NMS實施的第一個階段必須是為網路硬體確立基準。從路由器上的簡單CPU、記憶體和緩衝區利用率，以及交換機上的NMP CPU、記憶體和背板利用率，可以推斷出裝置和協定的健康狀況。只有在硬體基線之後，L2和L3流量負載、峰值和平均基線才會完全有意義。基線通常是在數個月內建立，以便根據公司的商業週期瞭解每日、每週和每季度的趨勢。

許多網路都因輪詢過大而存在NMS效能和容量問題。因此，建議在基線建立後，在裝置自身上設定警報和事件RMON閾值，以向NMS發出異常更改警報，從而刪除輪詢。這樣，網路就能夠告訴操作員什麼事情是不正常的，而不是不斷輪詢來檢查是否一切正常。閾值可以根據各種規則進行設定，例如最大值加上百分比或者與平均值的標準偏差，這些規則不屬於本文檔的範圍。

NMS實施的第二階段是使用SNMP更詳細地輪詢特定網路區域。這包括有疑問的領域、變革前領域，或表現良好的領域。使用NMS系統作為探照燈，詳細掃描網路並照亮熱點（不要嘗試照亮整個網路）。

Cisco Network Management Consulting團隊建議應在園區網路中分析或監控這些關鍵故障MIB。請參閱思科網路監控和事件關聯准則以瞭解詳細資訊（例如要輪詢的效能MIB）。

| 對象名稱 | 對象描述 | OID | 輪詢間隔 | 閾值 |
|---|---|---|---|---|
| MIB-II | | | | |
| sysUpTime | 系統正常運行時間（1/100秒） | 1.3.6.1.2.1.1.3 | 5分鐘 | < 30000 |

| 對象名稱 | 對象描述 | OID | 輪詢間隔 | 閾值 |
|---|---|---|---|---|
| CISCO-PROCESS-MIB | | | | |

| | | | | |
|---|---|---|---|---|
| cpmCPUTotal5min | 過去5分鐘內的總CPU忙碌百分比 | 1.3.6.1.4.1.9.9.109.1.1.1.1.5 | 10分鐘 | 基線 |

| 對象名稱 | 對象描述 | OID | 輪詢間隔 | 閾值 |
|---|---|---|---|---|
| CISCO-STACK-MIB | | | | |
| sysEnableChassisTraps | 指示是否必須生成此MIB中的chassisAlarmOn和chassisAlarmOff陷阱。 | 1.3.6.1.4.1.9.5.1.1.24 | 24小時 | 1 |
| sysEnableModuleTraps | 指示是否必須生成此MIB中的moduleUp和moduleDown陷阱。 | 1.3.6.1.4.1.9.5.1.1.25 | 24小時 | 1 |
| sysEnableBridgeTraps | 指示是否必須生成BRIDGE-MIB(RFC 1493)中的newRoot和topologyChange陷阱。 | 1.3.6.1.4.1.9.5.1.1.26 | 24小時 | 1 |
| sysEnableRepeaterTraps | 指示是否必須生成REPEATER-MIB(RFC1516)中的陷阱。 | 1.3.6.1.4.1.9.5.1.1.29 | 24小時 | 1 |
| sysEnableIpPermitTraps | 指示是否必須生成此MIB中的IP允許陷阱。 | 1.3.6.1.4.1.9.5.1.1.31 | 24小時 | 1 |
| sysEnableVmpsTraps | 指示是否必須生成CISCO-VLAN-MEMBERSHIP-MIB中定義的vmVmpsChange陷阱。 | 1.3.6.1.4.1.9.5.1.1.33 | 24小時 | 1 |
| sysEnableConfigTraps | 指示是否必須生成此MIB中的sysConfigChange陷阱。 | 1.3.6.1.4.1.9.5.1.1.35 | 24小時 | 1 |
| sysEnableStpxTrap | 指示是否必須在CISCO-STP-EXTENSIONS-MIB中生成stpxInconsistencyUpdate陷阱。 | 1.3.6.1.4.1.9.5.1.1.40 | 24小時 | 1 |
| chassisPs1status | 電源1的狀態。 | 1.3.6.1.4.1.9.5.1.2.4 | 10分鐘 | 2 |
| chassisPs1TestResult | 有關電源1狀態的詳細資訊。 | 1.3.6.1.4.1.9.5.1.2.5 | 根據需要。 | |
| 機箱Ps2狀態 | 電源2的狀態。 | 1.3.6.1.4.1.9.5.1.2.7 | 10分鐘 | 2 |
| 機箱 | 有關電源2狀態的詳細資訊 | 1.3.6.1. | 根 | |

| | | | | |
|---|---|---|---|---|
| Ps2測試結果 | | 4.1.9.5.1.2.8 | 據需要。 | |
| 機箱風扇狀態 | 機箱風扇的狀態。 | 1.3.6.1.4.1.9.5.1.2.9 | 10分鐘 | 2 |
| chassisFanTestResult | 有關機箱風扇狀態的詳細資訊。 | 1.3.6.1.4.1.9.5.1.2.10 | 根據需要。 | |
| 機箱次要警報 | 機箱次要警報狀態。 | 1.3.6.1.4.1.9.5.1.2.11 | 10分鐘 | 1 |
| 機箱重大警報 | 機箱主要警報狀態 | 1.3.6.1.4.1.9.5.1.2.12 | 10分鐘 | 1 |
| chassisTempAlarm | 機箱溫度警報狀態。 | 1.3.6.1.4.1.9.5.1.2.13 | 10分鐘 | 1 |
| 模組狀態 | 模組的運行狀態。 | 1.3.6.1.4.1.9.5.1.3.1.1.10 | 30分鐘 | 2 |
| moduleTestResult | 有關模組條件的詳細資訊。 | 1.3.6.1.4.1.9.5.7.3.1.1.11 | 根據需要。 | |
| moduleStandbyStatus | 冗餘模組的狀態。 | 1.3.6.1.4.1.9.5.7.3.1.1.21 | 30分鐘 | =1或=4 |

| **對象名稱** | **對象描述** | **OID** | **輪詢間隔** | **閾值** |
|---|---|---|---|---|
| CISCO-MEMORY-POOL-MIB | | | | |
| dot1dStpTimeSinceTopologyChange | 自實體上次檢測到拓撲更改以來的時間（1/100秒）。 | 1.3.6.1.2.1.17.2.3 | 5分鐘 | <30000 |
| dot1dStpTopChanges | 自上次重置或初始化管理實體後，此網橋檢測到的拓撲更改總數。 | 1.3.6.1.2.1.17.2.4 | 根據需要 | |

| | | | | |
|---|---|---|---|---|
| | | | 。 | |
| dot1dStpPort State [1] | 應用生成樹協定定義的埠的當前狀態。返回值可以是以下值之一：`disabled(1)blocking(2) listening(3)learning(4) forwarding(5)`或`broken(6)`。 | 1.3.6.1.2.1.17.2.15.1.3 | 根據需要。 | |

| 對象名稱 | 對象描述 | OID | 輪詢間隔 | 閾值 |
|---|---|---|---|---|
| CISCO-MEMORY-POOL-MIB | | | | |
| ciscoMemoryPoolUsed | 指示受管裝置上應用程式當前正在使用的記憶體池中的位元組數。 | 1.3.6.1.4.1.9.9.48.1.1.1.5 | 30分鐘 | 基線 |
| ciscoMemoryPoolFree | 指示受管裝置上當前未使用的記憶體池位元組數。<br>**註**：ciscoMemoryPoolUsed和ciscoMemoryPoolFree的總和是池中的記憶體總量。 | 1.3.6.1.4.1.9.9.48.1.1.1.6 | 30分鐘 | 基線 |
| ciscoMemoryPoolLargestFree | 表示受管裝置上當前未使用的記憶體池中的最大連續位元組數。 | 1.3.6.1.4.1.9.9.48.1.1.1.7 | 30分鐘 | 基線 |

有關Cisco MIB支援的詳細資訊，請參閱Cisco網路管理工具包 — MIB。

**注意**：某些標準MIB假定特定SNMP實體僅包含MIB的一個例項。因此，標準MIB沒有任何允許使用者直接訪問MIB的特定例項的索引。在這些情況下，會提供社群字串索引以存取標準MIB的每個例項。語法是[community string]@[instance number]，其中例項通常是VLAN編號。

## 其他選項

SNMPv3的安全方面意味著其使用有望在時間上超過SNMPv2。思科建議客戶將準備此新協定作為其NMS策略的一部分。優點是從SNMP裝置可以安全地收集資料，而不必擔心資料被篡改或損壞。可以對更改交換機配置的SNMP **set**命令資料包等機密資訊進行加密，以防止其內容在網路中暴露。此外，不同的使用者組可以具有不同的許可權。

**註**：SNMPv3的配置與SNMPv2命令列明顯不同，Supervisor Engine上的CPU負載預計會增加。

## 遠端監控

RMON允許網路裝置本身對MIB資料進行預處理，以便為網路管理器對該資訊的通用使用或應用做準備，例如執行歷史基線確定和閾值分析。

RMON處理的結果儲存在RMON MIB中，供NMS後續收集(如RFC 1757 中所定義)。

## 操作概述

Catalyst交換機在每個埠的硬體中支援mini-RMON，該埠包括四個基本RMON-1組：統計資訊（組1）、歷史記錄（組2）、警報（組3）和事件（組9）。

RMON-1功能最強大的部分是由**警報和事**件組提**供的閾值**機制。如前所述，RMON閾值的配置允許交換機在發生異常情況時傳送SNMP陷阱。確定關鍵埠後，可使用SNMP輪詢計數器或RMON歷史記錄組，並建立基線，記錄這些埠的正常流量活動。接下來，可以設定RMON上升閾值和下降閾值，並配置警報，以便當存在與基線定義的差異時。

閾值配置最好使用RMON管理包來執行，因為在警報和事件表中成功建立引數行非常繁瑣。商業RMON NMS包（例如Cisco Works 2000的Cisco Traffic Director）包含可簡化RMON閾值設定的GUI。

出於基線考慮，etherStats組提供一系列有用的第2層流量統計資訊。此表中的對象可用於獲取有關單播、組播和廣播流量以及各種第2層錯誤的統計資訊。交換機上的RMON代理還可以配置為將這些取樣值儲存在歷史記錄組中。這種機制能夠在不降低取樣率的情況下減少輪詢量。RMON歷史記錄可以提供準確的基線，而不會產生大量的輪詢開銷。但是，收集的歷史記錄越多，使用的交換機資源就越多。

雖然交換器僅提供RMON-1的四個基本群組，但不要忘記RMON-1和RMON-2的其餘部分。所有群組都在RFC 2021中定義，包括UserHistory（群組18）和ProbeConfig（群組19）。使用SPAN連線埠或VLAN ACL重新導向功能(此功能可將流量複製到外部RMON交換器探測或內部網路分析模組(NAM))，可從交換器擷取L3和更高資訊。

NAM支援所有RMON組，甚至可以檢查應**用層資料**，包括啟用MLS時從Catalyst匯出的Netflow資料。運行MLS意味著路由器不會交換流中的所有資料包，因此只有Netflow資料匯出計數器而不是介面計數器可以提供可靠的VLAN記帳。

您可以使用SPAN連線埠和交換器探測器擷取特定連線埠、主幹或VLAN的封包流，並上傳封包以使用RMON管理封包進行解碼。SPAN連線埠透過CISCO-STACK-MIB中的SPAN群組由SNMP控制，因此此程式易於自動化。Traffic Director使用這些功能及其漫遊代理功能。

跨整個VLAN有一些警告。即使使用1Gbps探測，來自一個VLAN或甚至一個1Gbps全雙工埠的整個資料包流也可能超過SPAN埠的頻寬。如果SPAN連線埠繼續以全頻寬執行，可能會遺失資料。如需詳細資訊，請參閱設定Catalyst交換連線埠分析器(SPAN)功能。

## 建議

Cisco建議部署RMON閾值和警報，以便以比單獨使用SNMP輪詢更智慧的方式幫助網路管理。這減少了網路管理流量開銷，並且允許網路在基線發生變化時智慧地發出警報。RMON需要由外部代理（如流量導向器）驅動；沒有CLI支援。核發以下命令，以便啟用RMON:

```
set snmp rmon enable
set snmp extendedrmon netflow enable mod
!--- For use with NAM module only.
```

請務必記住，交換機的主要功能是轉發幀，而不是充當大型多埠RMON探頭。因此，當您在多個埠上為多個條件設定歷史記錄和閾值時，請記住資源正在被消耗。如果要擴展RMON，請考慮使用NAM模組。另請記住重要連線埠規則：僅輪詢和設定規劃階段中確定為重要的埠的閾值。

## 記憶體要求

在所有與統計資訊、歷史記錄、警報和事件有關的交換機平台上，RMON記憶體使用率是固定的。RMON使用桶來儲存RMON代理（本例中為交換機）上的歷史記錄和統計資訊。 桶大小在RMON探測（交換機探測）或RMON應用（流量導向器）上定義，然後傳送到交換機以進行設定。通常，記憶體限制只是考慮舊版DRAM小於32MB的Supervisor引擎。請參閱以下准則：

- 為了支援mini-RMON（這是四組RMON），向NMP映像新增了大約450K的代碼空間：統計資訊、歷史記錄、警報和事件)。 RMON的動態記憶體要求會有所不同，因為它取決於運行時配置。以下說明每個迷你RMON組的運行時RMON記憶體使用資訊：Ethernet Statistics group — 每個交換乙太網/FE介面佔用800位元組。歷史記錄組 — 對於乙太網介面，每個配置的歷史記錄控制條目具有50個儲存桶，大約佔用3.6KB的記憶體空間，每個額外儲存桶佔用56個位元組。Alarms and Events組 — 每個已配置的警報及其相應的事件條目佔用2.6KB。
- 如果系統總NVRAM大小為256K或更高，則儲存RMON相關配置需要大約20K NVRAM空間；如果總NVRAM大小為128K，則需要10K NVRAM空間。

## 網路時間協定

NTP(RFC 1305 )在一組分散式時間伺服器和客戶端之間同步計時，並允許在建立系統日誌或其他特定時間事件發生時關聯事件。

NTP提供客戶端時間精度，通常在LAN上為毫秒內，在WAN上為幾十毫秒，相對於同步到協調世界時(UTC)的主伺服器。 典型的NTP配置使用多個冗餘伺服器和不同的網路路徑，以實現高準確性和可靠性。某些配置包括加密身份驗證以防止意外或惡意協定攻擊。

### 操作概述

NTP最初記錄在RFC 958 中，但已通過RFC 1119（NTP版本2）演變，現在已是RFC 1305 中定義的第三個版本。它通過UDP埠123運行。所有NTP通訊都使用UTC，該時間與格林尼治標準時間相同。

### 訪問公共時間伺服器

NTP子網目前包括50多個公共主伺服器，通過無線電、衛星或數據機直接與UTC同步。通常，客戶端數量相對較少的客戶端工作站和伺服器不會與主伺服器同步。大約有100台公共輔助伺服器與主伺服器同步，從而提供與Internet上超過100,000台客戶端和伺服器的同步。當前清單在「公共NTP伺服器清單」頁面上維護，該頁面定期更新。有許多專用主伺服器和輔助伺服器通常也不對公眾可用。有關公共NTP伺服器清單以及如何使用它們的資訊，請訪問德拉瓦大學時間同步伺服器 網站。

由於無法保證這些公共Internet NTP伺服器將可用，或者無法保證它們生成正確的時間，因此強烈建議考慮其他選項。這可能包括使用直接連線到許多路由器的各種獨立全球定位服務(GPS)裝置。

另一個可能的選項是使用配置為Stratum 1主機的各種路由器，但不建議這樣做。

### 層

每個NTP伺服器都採用一個層，該層表示伺服器距離外部時間源的距離。第1層伺服器可以訪問某種外部時間源，例如無線電時鐘。第2層伺服器從一組指定的第1層伺服器獲取時間詳細資訊，而第3層伺服器從第2層伺服器獲取時間詳細資訊，以此類推。

### 伺服器對等關係

- 伺服器是對客戶端請求作出響應的伺服器，但不嘗試合併來自客戶端時間源的任何日期資訊。
- 對等體是對客戶端請求作出響應的，但試圖將客戶端請求用作更佳時間源的潛在候選者，並幫助穩定其時脈頻率。
- 為了成為真正的對等體，連線的兩端必須建立對等體關係，而不是將一個使用者作為對等體，而將另一個使用者作為伺服器。還建議對等體交換金鑰，以便只有受信任的主機作為對等體相互通訊。
- 在向伺服器發出客戶端請求時，伺服器回答客戶端，並忘記客戶端曾經提過問題；在向對等體的客戶端請求中，伺服器會應答客戶端，並保留有關客戶端的狀態資訊，以跟蹤客戶端在計時時的運行情況以及所運行的層級伺服器。**注意**：CatOS只能充當NTP客戶端。

NTP伺服器可以處理數千個客戶端，這是沒有問題的。但是，處理數百個對等體會影響記憶體，並且狀態維護會佔用機箱上更多的CPU資源以及頻寬。

## 輪詢

NTP協定允許客戶端隨時查詢伺服器。實際上，當NTP在思科裝置中首次配置時，它會以NTP_MINPOLL（24 = 16秒）間隔快速連續傳送八個查詢。NTP_MAXPOLL是214秒（即16,384秒或4小時33分鐘4秒），這是NTP再次輪詢響應之前花費的最長時間。目前，思科沒有手動強制使用者設定POLL時間的方法。

NTP輪詢計數器從$2^6$(64)秒開始，以兩的冪遞增到$2^{10}$。也就是說，可以預期每個已配置的伺服器或對等體以64、128、256、512或1024秒的間隔傳送同步消息。根據傳送和接收資料包的鎖相環路，時間在64秒和1024秒之間變化，其功率為2。如果時間中有很多抖動，則輪詢頻率更高。如果參考時鐘準確且網路連線一致，您會看到每次輪詢之間的輪詢時間收斂到1024秒。

在現實世界中，這意味著NTP輪詢間隔會隨著客戶端和伺服器之間的連線變化而變化。連線越好，輪詢間隔越長，意味著NTP客戶端收到對其最後八個請求的八個響應（輪詢間隔隨後加倍）。單個未響應導致輪詢間隔減半。輪詢間隔從64秒開始，最大值為1024秒。在最佳情況下，輪詢間隔從64秒變為1024秒大約需要2個多小時。

## 廣播

NTP廣播從不轉發。**ntp broadcast**命令使路由器在配置它的介面上發起NTP廣播。ntp broadcastclient 命令使路由器或交換機在配置它的介面上偵聽NTP廣播。

## NTP流量級別

NTP使用的頻寬是最小的，因為對等體之間交換的輪詢消息之間的間隔通常會回溯到每17分鐘（1024秒）不超過一條消息。 在仔細規劃後，這可以通過WAN鏈路在路由器網路中維護。NTP客戶端必須與本地NTP伺服器對等，而不是一直通過WAN連線到將成為第2層伺服器的中心站點核心路由器。

融合的NTP客戶端大約每台伺服器使用0.6位/秒。

## 建議

目前，許多客戶在其CatOS平台上以客戶端模式配置了NTP，並從來自網際網路或無線電時鐘的多個可靠源同步。但是，當運行大量交換機時，伺服器模式的一種更簡單的替代方案是在交換域中的管理VLAN上啟用廣播客戶端模式下的NTP。此機制允許Catalyst的整個域從單個廣播消息接收時鐘。但是，由於資訊流是單向的，計時準確度會略有降低。

使用環回地址作為更新源也有助於保持一致性。可以通過以下兩種方式解決安全顧慮：

- 篩選伺服器更新
- 驗證

事件之間的時間關聯在兩種情況下是非常有價值的：故障排除和安全審計。必須小心保護時間源和資料，建議進行加密，以免有意或無意地清除金鑰事件。

思科建議使用以下設定：

**Catalyst組態**

```
set ntp broadcastclient enable
set ntp authentication enable
set ntp key key
!--- This is a Message Digest 5 (MD5) hash. set ntp
timezone
```

**備用Catalyst配置**

```
!--- This more traditional configuration creates !---
more configuration work and NTP peerings. set ntp client
enable
set ntp server IP address of time server set timezone
zone name set summertime date change details
```

**路由器配置**

```
!--- This is a sample router configuration to distribute
!--- NTP broadcast information to the Catalyst broadcast
clients. ntp source loopback0
ntp server IP address of time server ntp update-calendar
clock timezone zone name clock summer-time date change
details ntp authentication key key ntp access-group
access-list
!--- To filter updates to allow only trusted sources of
NTP information. Interface to campus/management VLAN
containing switch sc0 ntp broadcast
```

## 思科探索通訊協定

CDP通過資料鏈路層在相鄰裝置之間交換資訊，對於確定邏輯或IP層之外的網路拓撲和物理配置非常有用。支援的裝置主要是交換機、路由器和IP電話。本節重點介紹CDP版本2相對於版本1的一些增強功能。

### 操作概述

CDP使用型別代碼為2000的SNAP封裝。在乙太網、ATM和FDDI上，使用目標組播地址**01-00-0c-cc-cc-cc，HDLC協定型別**0x2000。在令牌環上，使用功能地址c000.0800.0000。預設情況下，每

分鐘定期傳送CDP幀。

CDP消息包含一條或多條子消息，允許目的裝置收集和儲存關於每個相鄰裝置的資訊。

CDP第1版支援以下引數：

| 引數 | 類型 | 說明 |
|---|---|---|
| 1 | 裝置ID | 裝置的主機名或ASCII格式的硬體序列號。 |
| 2 | 地址 | 已傳送更新的介面的L3地址。 |
| 3 | Port-ID | 傳送CDP更新的埠。 |
| 4 | 功能 | 描述裝置的功能功能：路由器：0x01 TB網橋：0x02 SR網橋：0x04交換機：0x08（提供L2和/或L3交換）主機：0x10 IGMP條件過濾：0x20網橋或交換機不會在非路由器埠上轉發IGMP報告資料包。中繼器：0x40 |
| 5 | 版本 | 包含軟體版本的字串(與**show version**中的內容相同)。 |
| 6 | 平台 | 硬體平台，例如WS-C5000、WS-C6009或Cisco RSP。 |

在CDP第2版中，引入了其他協定欄位。CDP版本2支援任何欄位，但所列出的欄位在交換環境中特別有用，並且用於CatOS。

**附註：** 當交換機運行CDPv1時，它會丟棄v2幀。當運行CDPv2的交換機在介面上收到CDPv1幀時，它開始傳送該介面的CDPv1幀以及CDPv2幀。

| 引數 | 類型 | 說明 |
|---|---|---|
| 9 | VTP域 | VTP域（如果在裝置上配置）。 |
| 10 | 本徵VLAN | 在dot1q中，這是未標籤的VLAN。 |
| 11 | 全/半雙工 | 此欄位包含傳送埠的雙工設定。 |

## 建議

CDP預設啟用，對於獲得相鄰裝置的可視性和故障排除至關重要。網路管理應用程式也使用它來構建L2拓撲圖。發出以下命令以設定CDP:

```
set cdp enable
!--- This is the default. set cdp version v2
!--- This is the default.
```

在需要高度安全性的網路部分（例如面向網際網路的DMZ），必須按如下方式關閉CDP:

```
set cdp disable port range
```

show cdp neighbors 命令會顯示本地CDP表。標有星號(*)的專案表示VLAN不匹配；標有#的條目表示雙工不匹配。這對故障排除很有幫助。

```
>show cdp neighbors

* - indicates vlan mismatch.
# - indicates duplex mismatch.
Port  Device-ID          Port-ID Platform
----- ----------------- ------- ------------
 3/1  TBA04060103(swi-2) 3/1     WS-C6506
 3/8  TBA03300081(swi-3) 1/1     WS-C6506
15/1  rtr-1-msfc         VLAN 1  cisco    Cat6k-MSFC
16/1  MSFC1b             Vlan2   cisco    Cat6k-MSFC
```

### 其他選項

某些交換機（如Catalyst 6500/6000）能夠通過UTP電纜為IP電話供電。通過CDP接收的資訊有助於交換機的電源管理。

由於IP電話可以連線PC，且兩台裝置都連線到Catalyst上的同一埠，因此交換機能夠將VoIP電話置於獨立的VLAN（輔助）。這使交換機能夠輕鬆為VoIP流量應用不同的服務品質(QoS)。

此外，如果修改了輔助VLAN（例如，為了強制電話使用特定VLAN或特定標籤方法），此資訊將通過CDP傳送到電話。

| 引數 | 類型 | 說明 |
|---|---|---|
| 14 | 裝置ID | 允許通過單獨的VLAN-id（輔助VLAN）將VoIP流量與其他流量區分開來。 |
| 16 | 功耗 | VoIP電話耗電量（毫瓦）。 |

**注意**：Catalyst 2900和3500XL交換機當前不支援CDPv2。

## 安全配置

理想情況下，客戶已制定安全策略，以幫助定義思科提供的哪些工具和技術合格。

**注意**：Cisco IOS軟體安全性與CatOS相反，在許多文檔(例如Cisco ISP基本版)中都有涉及。

### 基本安全功能

#### 密碼

配置使用者級密碼（登入）。 在CatOS 5.x及更高版本中，密碼區分大小寫，長度為0到30個字元，包括空格。設定啟用密碼：

```
set password password set enablepass password
```

使用時，所有密碼都必須符合登入和啟用密碼的最小長度標準（例如，最少六個字元、字母和數字的組合、大寫字母和小寫字母）。這些密碼使用MD5雜湊演算法加密。

為了在管理密碼安全和裝置訪問方面實現更大的靈活性，思科建議使用TACACS+伺服器。如需詳細資訊，請參閱本檔案的TACACS+一節。

## 安全殼層

利用SSH加密為到交換機的Telnet會話和其他遠端連線提供安全性。僅對交換機的遠端登入支援SSH加密。您無法加密從交換機發起的Telnet會話。CatOS 6.1支援SSH版本1,CatOS 8.3新增了版本2支援。SSH版本1支援資料加密標準(DES)和三重DES(3-DES)加密方法，而SSH版本2支援3-DES和高級加密標準(AES)加密方法。您可以將SSH加密與RADIUS和TACACS+身份驗證配合使用。SSH(k9)映像支援此功能。如需詳細資訊，請參閱如何在執行CatOS的Catalyst交換器上設定SSH。

```
set crypto key rsa 1024
```

若要停用版本1回退並接受版本2連線，請發出以下命令：

```
set ssh mode v2
```

## IP允許篩選條件

以下是用於保護通過Telnet和其它協定訪問管理sc0介面的過濾器。當用於管理的VLAN中還包含使用者時，這一點尤為重要。發出以下命令以啟用IP地址和埠過濾：

```
set ip permit enable
set ip permit IP address mask Telnet|ssh|snmp|all
```

但是，如果使用此命令限制Telnet訪問，則只能通過幾個受信任的終端站才能訪問CatOS裝置。此設定可能會妨礙故障排除過程。請記住，偽裝IP地址並欺騙過濾訪問是可能的，因此這只是第一層保護。

## 連線埠安全性

考慮使用連線埠安全性，以便僅允許一個或多個已知MAC位址在特定連線埠上傳遞資料（例如，為了停止將靜態終端站交換為新站台，而不進行變更控制）。 使用靜態MAC地址可以做到這一點。

```
set port security mod/port enable MAC address
```

這也可以通過動態學習受限制的MAC地址來實現。

```
set port security port range enable
```

可以配置以下選項：

- set port security *mod/port* age *time value* — 指定在獲取新地址之前保護埠上地址的持續時間。有效時間（分鐘）為10 - 1440。預設設定為無過期。
- set port *securitymod/port* maximum *value* — 指定要在埠上保護的最大MAC地址數的關鍵字。有效值為1（預設值）— 1025。
- set port security *mod/port* violation shutdown — 在發生違規時關閉埠（預設），並傳送系統日誌消息（預設）並丟棄流量。
- set port security *mod/port* shutdown *time value* — 埠保持禁用狀態的持續時間。有效值為10 - 1440分鐘。預設為永久關閉

在CatOS 6.x及更高版本中，思科引入了802.1x驗證，允許客戶端在啟用埠資料之前向中央伺服器進行驗證。此功能在Windows XP等平台上的支援尚處於早期階段，但許多企業都將其視為戰略方向。有關如何配置運行Cisco IOS軟體的交換機的埠安全的資訊，請參閱配置埠安全。

### 登入橫幅

建立相應的裝置橫幅，明確說明針對未經授權訪問所採取的操作。請勿通告可能向未授權使用者提供資訊的站點名稱或網路資料。這些橫幅提供了追索權，以防裝置受損且犯罪者被抓獲：

```
# set banner motd ^C
*** Unauthorized Access Prohibited ***
***  All transactions are logged   ***
------------- Notice Board -------------
----Contact Joe Cisco at 1 800 go cisco for access problems----
^C
```

### 實體安全

未經適當授權，不得實際接觸裝置，因此裝置必須位於受控（鎖定）空間內。為確保網路保持運行不受環境因素惡意篡改的影響，所有裝置都必須具有適當的UPS（儘可能配備冗餘電源）和溫度控制（空調）。 請記住，如果具有惡意目的的人員侵入物理訪問，則更有可能通過密碼恢復或其他方法造成中斷。

## 終端存取控制器存取控制系統

預設情況下，非特權模式和特權模式口令是全域性的，適用於從控制檯埠或通過網路上的Telnet會話訪問交換機或路由器的每個使用者。在網路裝置上實施它們非常耗時，而且非集中化。使用容易出現配置錯誤的訪問清單實施訪問限制也很困難。

有三種安全系統可用於幫助控制和管制對網路裝置的訪問。它們使用客戶端/伺服器架構將所有安全資訊放置在一個中央資料庫中。這三個安全系統是：

- TACACS+

- RADIUS
- Kerberos

TACACS+是思科網路中的常見部署，是本章的重點。它提供以下功能：

- 身份驗證 — 使用者的識別和驗證過程。可以使用多種方法驗證使用者，但最常見的方法包括使用者名稱和密碼的組合。
- Authorization — 使用者通過身份驗證後，可授予各種命令的授權。
- 記帳 — 記錄使用者在裝置上執行或已經執行的操作。

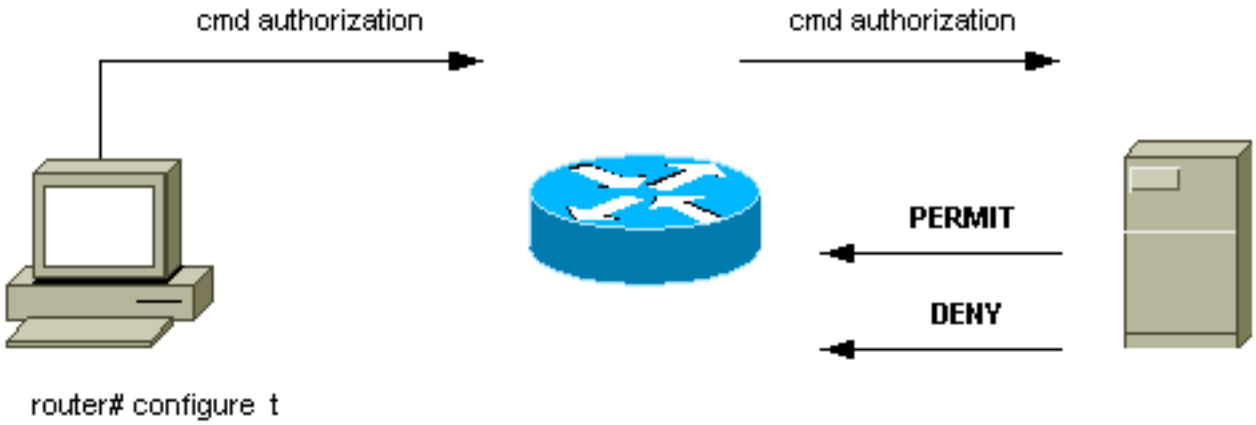
如需詳細資訊，請參閱在Cisco Catalyst交換器上設定TACACS+、RADIUS和Kerberos。

## 操作概述

TACACS+通訊協定將使用者名稱和密碼轉送到中央伺服器，並使用**MD5單向散**列(RFC 1321 )透過網路加密。 它使用TCP埠49作為其傳輸協定；相較於UDP（由RADIUS使用），具有以下優點：

- 面向連線的傳輸
- 無論後端身份驗證機制當前載入方式如何，都可單獨確認已收到請求(TCP ACK)
- 即時指示伺服器崩潰（RST資料包）

在作業階段進行期間，如果需要額外的授權檢查，交換器會對TACACS+進行檢查，確定使用者是否有獲得使用特定指令的許可權。這麼做可更有效控制從驗證機制中解除耦合時，可在交換器上執行的指令。使用命令記帳，可以稽核特定使用者在連線到特定網路裝置時發出的命令。




當使用者嘗試透過TACACS+驗證網路裝置進行簡單的ASCII登入時，通常會發生以下程式：

- 建立連線後，交換機會聯絡TACACS+後台程式以獲取使用者名稱提示，然後將其顯示給使用者。使用者輸入使用者名稱，交換器會連線TACACS+後台程式以取得密碼提示。交換器向使用者顯示密碼提示，使用者接著輸入密碼，此密碼也會傳送到TACACS+服務精靈。
- 網路裝置最終從TACACS+後台程式收到以下其中一個響應：ACCEPT — 使用者通過身份驗證，服務可以開始。如果網路裝置配置為需要授權，則此時開始授權。REJECT — 使用者無法進行身份驗證。使用者可能會遭到拒絕進一步存取，或根據TACACS+守候程式提示重試登入順序。ERROR — 身份驗證過程中某個時間出錯。這可以是在守護程式上，也可以是在守護程式和交換機之間的網路連線中。如果收到ERROR響應，網路裝置通常嘗試使用替代方法來驗證使用者。CONTINUE — 提示使用者輸入其他身份驗證資訊。
- 使用者必須先成功完成TACACS+驗證，才能繼續進行TACACS+授權。
- 如果需要TACACS+授權，則會再次聯絡TACACS+後台程式，並返回ACCEPT或REJECT授權響應。如果返回ACCEPT響應，則響應包含屬性形式的資料，用於指導該使用者的EXEC或NETWORK會話，並確定使用者可以訪問的命令。

### 建議

思科建議使用TACACS+，因為可以使用CiscoSecure ACS for NT、Unix或其他第三方軟體輕鬆實作。TACACS+功能包括詳細記帳，提供有關命令使用情況和系統使用情況的統計資訊、MD5加密演算法以及對驗證和授權進程的管理控制。

在此範例中，登入和啟用模式使用TACACS+伺服器進行驗證，如果伺服器無法使用，則可能會回退到本機驗證。這是大多數網路中要離開的重要後門。發出以下命令以設定TACACS+:

```
set tacacs server server IP primary set tacacs server server IP
!--- Redundant servers are possible. set tacacs attempts 3
!--- This is the default. set tacacs key key
!--- MD5 encryption key. set tacacs timeout 15
!--- Longer server timeout (5 is default). set authentication login tacacs enable
set authentication enable tacacs enable
set authentication login local enable
set authentication enable local enable
!--- The last two commands are the default; they allow fallback !--- to local if no TACACS+
server available.
```

### 其他選項

使用TACACS+授權可以控制每個使用者或使用者組可以在交換機上執行的命令，但很難提出建議，因為所有客戶在此方面都有各自的要求。如需詳細資訊，請參閱使用驗證、授權和計費控制對交換器的存取。

最後，記帳命令提供每個使用者鍵入和配置的內容的審計追蹤。以下是使用命令末尾接收審計資訊的常見做法的示例：

```
set accounting connect enable start-stop tacacs+
set accounting exec enable start-stop tacacs+
set accounting system enable start-stop tacacs+
set accounting commands enable all start-stop tacacs+
set accounting update periodic 1
```

此組態具有以下功能：

- **connect**命令啟用交換機上出站連線事件（例如Telnet）的記帳。
- **exec**指令會啟用交換器上登入作業階段（例如作業人員）的計量。
- **system**命令啟用交換機上系統事件（例如重新載入或重置）的記帳。
- **命令**可對**show**和組態命令在交換器上輸入的內容進行計量。
- 每分鐘*定期更新*到伺服器一次，對於記錄使用者是否仍然登入很有幫助。

## 配置核對表

本節提供建議配置的摘要，但不包括安全詳細資訊。

標籤所有埠非常有用。核發此命令，以便標籤連線埠：

**set port description** *descriptive name*

將此鍵與列出的命令表結合使用：

| **主要:** |
| --- |
| **粗體文本** — 建議的更改 |
| 普通文本 — 預設，建議設定 |

**全域性配置命令**

| **指令** | **意見** |
| --- | --- |
| **set vtp domain *name* *passwordx*** | 防止新交換機進行未經授權的VTP更新。 |
| **set vtp mode transparent** | 選擇本文檔中升級的VTP模式。有關詳細資訊，請參閱本文檔的VLAN中繼協定部分。 |
| set spantree enable all | 確保在所有VLAN上啟用STP。 |
| **set spantree root *vlan*** | 建議為每個VLAN設定根（和輔助根）網橋。 |
| **set spantree backbonefast enable** | 支援從間接故障中快速STP收斂（僅當域中的所有交換機都支援該功能時）。 |
| **set spantree uplinkfast enable** | 支援從直接故障中快速STP收斂（僅適用於接入層交換機）。 |
| **set spantree portfast bpdu-guard enable** | 如果存在未經授權的生成樹擴展，則使埠自動關閉。 |
| **set udld enable** | 啟用單向鏈路檢測（也需要埠級別配置）。 |
| **set test diaglevel complete** | 在啟動時啟用完全診斷（Catalyst 4500/4000上的預設設定）。 |
| set test packetbuffer sun 3:30 | 啟用連線埠緩衝區錯誤檢查（僅適用於Catalyst 5500/5000）。 |
| set logging buffer 500 | 維護最大內部系統日誌緩衝區。 |
| **set logging server *IP address*** | 為外部系統消息記錄配置目標syslog伺服器。 |
| **set logging server enable** | 允許外部日誌伺服器。 |
| set logging timestamp enable | 啟用日誌中消息的時間戳。 |
| **set logging level spantree 6 default** | 提高預設STP系統日誌級別。 |
| **set logging level sys 6 default** | 提高預設的系統系統日誌級別。 |
| set logging server severity 4 | 僅允許匯出高嚴重性系統日誌。 |
| **set logging console disable** | 除非進行故障排除，否則禁用控制檯。 |

| | |
|---|---|
| set snmp community read-only *string* | 配置密碼以允許遠端資料收集。 |
| set snmp community read-write *string* | 配置口令以允許遠端配置。 |
| set snmp community read-write-all *string* | 將密碼配置為允許包括密碼在內的遠端配置。 |
| set snmp trap enable all | 為NMS伺服器啟用故障和事件警報的SNMP陷阱。 |
| set snmp trap *server address string* | 配置NMS陷阱接收器的地址。 |
| set snmp rmon enable | 為本地統計資訊收集啟用RMON。有關詳細資訊，請參閱本文檔的遠端監控部分。 |
| set ntp broadcastclient enable | 從上游路由器啟用準確的系統時鐘接收。 |
| set ntp timezone *zone name* | 設定裝置的本地時區。 |
| set ntp summertime *date change details* | 如果適用於時區，請配置夏時制。 |
| set ntp authentication enable | 為安全目的配置加密的時間資訊。 |
| set ntp key *key* | 配置加密金鑰。 |
| set cdp enable | 確保已啟用鄰居發現（預設情況下也在埠上啟用）。 |
| set tacacs server *IP address* primary | 配置AAA伺服器的地址。 |
| set tacacs server *IP address* | 如有可能，提供冗餘AAA伺服器。 |
| set tacacs attempts 3 | 允許AAA使用者帳戶嘗試3次密碼。 |
| set tacacs key *key* | 設定AAA MD5加密金鑰。 |
| set tacacs timeout 15 | 允許更長的伺服器超時（預設值為5秒）。 |
| set authentication login tacacs enable | 使用AAA驗證登入。 |
| set authentication enable tacacs enable | 在啟用模式下使用AAA進行身份驗證。 |
| set authentication login local enable | 預設；如果沒有AAA伺服器可用，則允許回退到本地。 |
| set authentication enable local enable | 預設；如果沒有AAA伺服器可用，則允許回退到本地。 |

**主機埠配置命令**

| 指令 | 意見 |
|---|---|
| set port host *port range* | 刪除不必要的埠處理。此宏設定spantree PortFast enable、 |

| | |
|---|---|
| | channel off、trunk off。 |
| set udld disable *port range* | 刪除不必要的埠處理（預設情況下在銅纜埠上禁用）。 |
| set port speed *port range* auto | 對最新的主機NIC驅動程式使用自動協商。 |
| set port trap *port range* disable | 一般使用者不需要SNMP設陷；僅跟蹤關鍵埠。 |

**伺服器配置命令**

| 指令 | 意見 |
|---|---|
| **set port host *port range*** | 刪除不必要的埠處理。此宏設定spantree PortFast enable、channel off、trunk off。 |
| set udld disable *port range* | 刪除不必要的埠處理（預設情況下在銅纜埠上禁用）。 |
| **set port speed *port range 10 \| 100*** | 通常配置靜態/伺服器埠；否則，請使用自動交涉。 |
| **set port duplex *port range full \|半*** | 通常是靜態/伺服器埠；否則，請使用自動交涉。 |
| **set port trap *port range* enable** | 關鍵服務埠必須將陷阱傳送到NMS。 |

**未使用的埠配置命令**

| 指令 | 意見 |
|---|---|
| set spantree portfast *port range* disable | 為STP啟用必要的埠處理和保護。 |
| **set port disable *port range*** | 禁用未使用的埠。 |
| **set vlan *unused dummy vlan port range*** | 如果啟用連線埠，則會將未經授權的流量導向未使用的VLAN。 |
| **set trunk *port range* off** | 禁用埠的中繼功能，直到管理為止。 |
| **set port channel *port range* mode off** | 禁用埠通道化，直到管理為止。 |

**基礎架構埠（交換機、交換機、路由器）**

| 指令 | 意見 |
|---|---|
| set udld enable *port range* | 啟用單向連結偵測（並非銅纜連線埠上的預設值）。 |
| **set udld aggressive-mode enable *port range*** | 啟用主動模式（適用於支援主動模式的裝置）。 |
| set port | 允許鏈路引數的預設GE自動協商。 |

| | |
|---|---|
| negotiation *port* rangeenable | |
| **set port trap** ***port range*** **enable** | 允許這些關鍵埠使用SNMP陷阱。 |
| **set trunk** ***port range*** **off** | 不使用中繼時禁用功能。 |
| **set trunk** ***mod/port*** ***desirable*** ***ISL \| dot1q \|協商*** | 如果使用trunk，則首選dot1q。 |
| **clear trunk** ***mod/port*** ***vlan range*** | 通過從不需要的中繼修剪VLAN來限制STP直徑。 |
| **set port channel** ***port range*** **mode off** | 不使用通道時禁用功能。 |
| **set port channel** ***port range*** **mode desirable** | 如果使用通道，則啟用PAgP。 |
| set port channel all distribution ip both | 如果使用通道，則允許L3來源/目的地負載平衡（Catalyst 6500/6000上的預設值）。 |
| **set trunk** ***mod/port*** **nonegotiate** ***ISL \| dot1q*** | 如果中繼到路由器、Catalyst 2900XL、3500或其他供應商，請禁用DTP。 |
| **set port negotiation** ***mod/port*** **disable** | 某些舊的GE裝置可能不支援協商。 |

## 相關資訊

- Catalyst 4500/4000系列交換器上的常見CatOS錯誤訊息
- Catalyst 5000/5500系列交換器上的常見CatOS錯誤訊息
- Catalyst 6500/6000系列交換器上的常見CatOS錯誤訊息
- 交換器產品支援
- LAN 交換技術支援
- 技術支援與文件 - Cisco Systems