運行Cisco IOS軟體的Catalyst 6500/6000系列和Catalyst 4500/4000系列交換機的最佳實踐

目錄

簡介

本文提供在Supervisor Engine上執行Cisco IOS®軟體的Catalyst 6500/6000和4500/4000系列交換器的最佳實踐。

Catalyst 6500/6000和Catalyst 4500/4000系列交換器支援在Supervisor Engine上執行的以下兩個作業系統之一：

- Catalyst OS(CatOS)
- Cisco IOS軟體

使用CatOS時，您可以選擇在路由器子卡或模組(例如：

- Catalyst 6500/6000中的多層次交換功能卡(MSFC)
- Catalyst 4500/4000中的4232第3層(L3)模組

在此模式下，有兩個配置命令列：

- 用於交換的CatOS命令列
- 用於路由的Cisco IOS軟體命令列

CatOS是系統軟體，在Supervisor Engine上執行。在路由模組上運行的Cisco IOS軟體是一個需要CatOS系統軟體的選項。

若是Cisco IOS軟體，則只有一個用於組態的命令列。在此模式下，CatOS的功能已整合到Cisco IOS軟體中。該整合將為交換和路由配置生成單個命令列。在此模式中，Cisco IOS軟體是系統軟體，並取代CatOS。

CatOS和Cisco IOS軟體作業系統均部署在關鍵網路中。以下交換機系列支援CatOS以及路由器子卡和模組的Cisco IOS軟體選項：

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

以下交換機系列支援Cisco IOS系統軟體：

- Catalyst 6500/6000
- Catalyst 4500/4000

請參閱執行CatOS設定和管理的Catalyst 4500/4000、5500/5000和6500/6000系列交換器的最佳實踐檔案，瞭解CatOS的相關資訊，因為本檔案涵蓋Cisco IOS系統軟體。

Cisco IOS系統軟體為使用者提供了以下優勢：

- 單一使用者介面
- 統一的網路管理平台
- 增強的QoS功能
- 分散式交換支援

本文檔提供模組化配置指導。因此，您可以單獨閱讀每個部分，並採用分階段的方法進行更改。本檔案假設對Cisco IOS軟體使用者介面有基本的瞭解和熟悉。本文檔不涵蓋整個園區網路設計。

開始之前

背景

本文檔提供的解決方案代表了思科工程師多年來在複雜網路和許多最大客戶領域工作的現場經驗。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：

- 從統計學上看，這些解決辦法在實地有最廣泛的接觸，因而風險最低
- 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

參考資料

Cisco.com上有許多Catalyst 6500/6000和Catalyst 4500/4000產品線的參考網站。本節列出的參考進一步深入瞭解了本文檔討論的主題。

請參閱LAN交換技術支援，以取得更多有關本檔案所涵蓋的任何主題資訊。支援頁面提供產品檔案、疑難排解和組態檔案。

本文檔提供公共線上材料的參考以便您進一步閱讀。但是，其他好的基礎和教育參考資料還有：

- Cisco ISP基本知識
- 適用於Cisco Catalyst 6500系列交換器的Cisco Catalyst和Cisco IOS作業系統的比較
- Cisco LAN交換（CCIE專業發展系列）
- 構建思科多層交換網路
- 效能和故障管理
- 安全：企業網路的安全藍圖
- 思科現場手冊：Catalyst交換器組態

基本配置

本節討論使用大多數Catalyst網路時部署的功能。

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。當您處理每個部分時，對協定的基本理解很有幫助。

Supervisor Engine流量

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，必須對keepalive消息、配置引數和管理更改進行受控交換。無論這些通訊協定是Cisco專有技術(例如思科探索通訊協定(CDP))，還是基於標準的通訊協定(例如ieee 802.1D（跨距樹狀目錄通訊協定[STP]），在Catalyst系列上實作這些通訊協定時，都有某些共同的元素。

在基本幀轉發中，使用者資料幀源自終端系統。資料幀的源地址(SA)和目的地地址(DA)不會在整個第2層(L2)交換域中更改。每台交換機Supervisor Engine上的內容可定址儲存器(CAM)查詢表由SA學習過程填充。這些表指示哪個出口埠轉發收到的每個幀。如果目的地未知，或者幀的目的地是廣播或組播地址，則地址學習過程不完整。當該過程不完整時，幀會被轉發（泛洪）到該VLAN中的所有埠。交換機還必須識別哪些幀將通過系統交換，哪些幀將定向到交換機CPU本身。交換機CPU也稱為網路管理處理器(NMP)。

CAM表中的特殊條目用於建立Catalyst控制平面。這些特殊條目稱為系統條目。控制平面在內部交

換機埠上接收流量並將其定向到NMP。因此，使用具有已知目的地MAC位址的通訊協定時，可以將控制平面流量與資料流量分離。

思科具有保留的乙太網MAC地址和協定地址範圍，如本節中的表所示。為了方便起見，本文檔詳細介紹每個保留地址，但此表提供了概要：

功能	SNAP[1] HDLC2協議型別	目的地多點傳送MAC
PAgP[3]	0x0104	01-00-0c-cc-cc-cc
PVST+、RPVST+[4]	0x010b	01-00-0c-cc-cc-cd
VLAN網橋	0x010c	01-00-0c-cd-cd-ce
UDLD[5]	0x0111	01-00-0c-cc-cc-cc
CDP	0x2000	01-00-0c-cc-cc-cc
DTP[6]	0x2004	01-00-0c-cc-cc-cc
STP UplinkFast	0x200a	01-00-0c-cd-cd-cd
IEEE生成樹802.1D	不適用 — DSAP[7] 42 SSAP[8] 42	01-80-c2-00-00-00
ISL[9]	不適用	01-00-0c-00-00-00
VTP[10]	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

[1] SNAP =子網訪問協定。

[2] HDLC =高級資料鏈路控制。

[3] PAgP =埠聚合協定。

[4] PVST+ =每個VLAN生成樹+,RPVST+ =快速PVST+。

[5] UDLD =單向連結偵測。

[6] DTP =動態Trunk協定。

[7] DSAP =目標服務接入點。

[8] SSAP =源服務接入點。

[9] ISL =交換器間連結。

[10] VTP = VLAN中繼協定。

大多數思科控制協定使用IEEE 802.3 SNAP封裝，其中包括邏輯鏈路控制(LLC)0xAAAA03和組織唯一識別符號(OUI)0x00000C。您可以在LAN分析器追蹤中看到此情況。

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台Catalyst交換機通過非Cisco交換機透明通訊。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行為不一致。通常，避免通過多供應商環境進行點對多點連線。這些協定在第3層路由器上終止，並且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。

現在，討論轉向SA。交換器通訊協定使用從可用位址庫中取得的MAC位址。機箱上的EPROM提供可用地址庫。發出**show module**命令，以顯示每個模組可用於流量來源(例如STP橋接器通訊協定資料單元(BPDU)或ISL訊框)的地址範圍。以下是命令輸出範例：

```
>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
!--- These are the MACs for sourcing traffic.
```

VLAN 1

VLAN 1在Catalyst網路中具有特殊意義。

建立中繼時，Catalyst Supervisor Engine一律使用預設VLAN(VLAN 1)來標籤許多控制和管理通訊協定。此類協定包括CDP、VTP和PAgP。預設情況下，包括內部sc0介面的所有交換機埠都配置為VLAN 1的成員。預設情況下，所有中繼都承載VLAN 1。

為了幫助澄清Catalyst網路中一些常用的術語，以下定義是必要的：

- sc0駐留在CatOS和低端交換機的管理VLAN中。您可以變更此VLAN。當您同時使用CatOS和Cisco IOS交換機時，請記住這一點。
- 本徵VLAN是埠不中繼時返回的VLAN。此外，本徵VLAN是IEEE 802.1Q中繼上的未標籤VLAN。

調整網路和改變VLAN 1中埠的行為有幾個很好的理由：

- 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），您需要修回VLAN。如需詳細資訊，請參閱交換器管理介面和本地VLAN一節。
- 您需要將VLAN 1上的控制平面資料與使用者資料分開，以簡化故障排除並最大化可用CPU週期。設計不使用STP的多層園區網路時，應避免VLAN 1中的第2層環路。為了避免第2層回圈，請手動清除主干連線埠中的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已經從中繼中清除，並且不是本徵VLAN，也會出現這種情況。如果清除使用者資料的VLAN 1，該操作對仍使用

VLAN 1傳送的控制平面流量沒有影響。
- 在ISL主幹上，DTP資料包在VLAN1上傳送。即使VLAN 1已從主幹中清除，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。即使本徵VLAN已從主幹中清除，情況也是如此。
- 在PVST+中，除非已從中繼中清除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會針對所有其他VLAN傳送和標籤。如需更多詳細資訊，請參閱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，以便所有VLAN避免其邊界埠的MST網橋置於根不一致狀態。如需詳細資訊，請參閱瞭解多生成樹通訊協定(802.1s)。

標準功能

本文此節重點介紹任何環境通用的基本交換功能。在客戶網路中的所有Cisco IOS軟體Catalyst交換裝置上配置這些功能。

VLAN Trunk通訊協定

目的

VTP域（也稱為VLAN管理域）由一台或多台交換機通過共用同一VTP域名的中繼互連。VTP旨在允許使用者在一台或多台交換機上集中更改VLAN配置。VTP會自動將更改傳送到（網路）VTP域中的所有其它交換機。您可以將交換機配置為僅位於一個VTP域中。建立VLAN之前，請確定要在網路中使用的VTP模式。

操作概述

VTP是第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，以保持VLAN配置的一致性。VTP可最大限度地減少可能導致許多問題的配置錯誤和配置不一致。這些問題包括VLAN名稱重複、VLAN型別規範不正確以及存在安全違規。

預設情況下，交換機處於VTP伺服器模式且處於無管理域狀態。當交換機通過中繼鏈路收到域的通告或配置管理域時，這些預設設定會發生更改。

VTP協定使用公認的乙太網目標組播MAC(01-00-0c-cc-cc-cc)和SNAP HDLC協定型別0x2003在交換機之間通訊。與其他固有協定類似，VTP也使用IEEE 802.3 SNAP封裝，其中包括LLC 0xAAAA03和OUI 0x00000C。您可以在LAN分析器追蹤中看到此情況。VTP在非中繼埠上不起作用。因此，在DTP啟動中繼之前，無法傳送消息。換句話說，VTP是ISL或802.1Q的負載。

消息型別包括：

- 每300秒的摘要通告（秒）
- 發生更改時的子集通告和請求通告
- 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，該表在整個域中傳播。

刪除VLAN時，曾經是VLAN成員的埠進入非活態。同樣，如果處於客戶端模式的交換機在啟動時無法從VTP伺服器或其他VTP客戶端接收VTP VLAN表，則除預設VLAN 1外，VLAN中的所有埠都會被停用。

您可以將大多數Catalyst交換機配置為在以下任一VTP模式下運行：

- 伺服器 — 在VTP伺服器模式下，您可以：建立VLAN修改VLAN刪除VLAN為整個VTP域指定其他配置引數，例如VTP版本和VTP修剪VTP伺服器向同一VTP域中的其它交換機通告其VLAN配置。VTP伺服器還會根據通過中繼鏈路接收的通告，將其VLAN配置與其他交換機同步。VTP伺服器是預設模式。
- 客戶端 — VTP客戶端的行為方式與VTP伺服器相同。但是您不能在VTP客戶端上建立、更改或刪除VLAN。此外，使用者端在重新啟動後不會記得VLAN，因為沒有VLAN資訊寫入NVRAM。
- 透明 — VTP透明交換機不參與VTP。VTP透明交換機不會通告其VLAN配置，也不會根據收到的通告同步其VLAN配置。但是，在VTP版本2中，透明交換機確實會轉發交換機從其中繼介面接收的VTP通告。

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

[1] Cisco IOS軟體無法使用關閉模式來停VTP。

下表是初始配置的摘要：

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修剪	已禁用

在VTP透明模式下，VTP更新會被忽略。公認VTP組播MAC地址從系統CAM中刪除，該系統通常用於提取控制幀，並將它們定向到Supervisor Engine。因為協定使用組播地址，所以處於透明模式的交換機或其他供應商交換機只是將幀泛洪到域中的其他Cisco交換機。

VTP第2版(VTPv2)包括本清單所述的功能靈活性。但是，VTPv2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 — 交換機現在傳播它們無法解析的值。
- 版本相關的透明模式 — 透明模式不再檢查域名。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，則可以使用單個交換機的配置來啟用所有交換機。

如需詳細資訊，請參閱瞭解VLAN中繼線通訊協定(VTP)。

Cisco IOS軟體中的VTP操作

CatOS中的組態變更會在變更後立即寫入NVRAM。相反，除非您發出**copy run start**命令，否則Cisco IOS軟體不會將配置更改儲存到NVRAM。VTP客戶端和伺服器系統要求來自其他VTP伺服器的VTP更新立即儲存到NVRAM中，無需使用者干預。預設的CatOS操作滿足VTP更新要求，但Cisco IOS軟體更新模式需要替代更新操作。

對於此變更，Catalyst 6500的Cisco IOS軟體中引入了VLAN資料庫，作為立即儲存VTP客戶端和伺服器的VTP更新的方法。在某些軟體版本中，此VLAN資料庫是NVRAM中獨立檔案的形式，稱為vlan.dat檔。檢查您的軟體版本，以確定是否需要VLAN資料庫的備份。如果您發出**show vtp status**命令，則可以檢視VTP客戶端或VTP伺服器的vlan.dat檔案中儲存的VTP/VLAN資訊。

在這些系統上發出**copy run start**命令時，整個VTP/VLAN配置不會儲存到NVRAM中的啟動配置檔案中。這並不適用於以VTP transparent模式運行的系統。當您發出**copy run start**命令時，VTP透明系統會將整個VTP/VLAN配置儲存到NVRAM中的啟動配置檔案中。

在低於Cisco IOS軟體版本12.1(11b)E的Cisco IOS軟體版本中，只能通過VLAN資料庫模式配置VTP和VLAN。VLAN資料庫模式與全域性配置模式是不同的模式。此配置要求的原因在於，當您在VTP模式伺服器或VTP模式客戶端中配置裝置時，VTP鄰居可以通過VTP通告動態更新VLAN資料庫。您不希望這些更新自動傳播到配置。因此，VLAN資料庫和VTP資訊不會儲存在主配置中，而是儲存在NVRAM中名為vlan.dat的檔案中。

此範例顯示如何在VLAN資料庫模式下建立乙太網路VLAN:

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

在Cisco IOS軟體版本12.1(11b)E和更新版本中，可以透過VLAN資料庫模式或全域組態模式設定VTP和VLAN。在VTP模式伺服器或透明VTP模式中，VLAN的配置仍會更新NVRAM中的vlan.dat檔案。但是，這些命令不會儲存在配置中。因此，這些命令不會顯示在運行配置中。

如需詳細資訊，請參閱設定VLAN檔案的*全域組態模式中的VLAN組態*一節。

此範例顯示如何在全域組態模式下建立乙太網路VLAN，以及如何驗證組態：

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

註：VLAN配置儲存在vlan.dat檔案中，該檔案儲存在非易失性記憶體中。若要對組態執行完整備份，請將vlan.dat檔與組態一起包含在備份中。接下來，如果整個交換器或Supervisor Engine模組都需要更換，則網路管理員必須上傳以下兩個檔案才能還原完整的組態：

- vlan.dat檔案
- 配置檔案

VTP和擴展VLAN

擴展系統ID功能用於啟用擴展範圍VLAN標識。啟用擴展系統ID後，它將禁用用於VLAN生成樹的MAC地址池，並保留一個用於識別交換機的MAC地址。Catalyst IOS軟體版本12.1(11b)EX和12.1(13)E為Catalyst 6000/6500引入了延伸系統ID支援，以符合IEEE 802.1Q標準支援4096 VLAN。此功能在適用於Catalyst 4000/4500交換器的Cisco IOS軟體版本12.1(12c)EW中匯入。這些VLAN被組織成多個範圍，每個範圍可以不同的使用。使用VTP時，其中一些VLAN會傳播到網路中的其他交換機。擴展範圍VLAN不會傳播，因此您必須在每個網路裝置上手動配置擴展範圍VLAN。此擴展系統ID功能等同於Catalyst OS中的MAC地址縮減功能。

下表描述了VLAN範圍：

VLAN	範圍	使用	是否通過VTP傳播？
0、4095	保留	僅供系統使用。看不到或使用這些VLAN。	—
1	正常	思科預設值。您可以使用此VLAN，但不能將其刪除。	是
2–1001	正常	對於乙太網VLAN。您可以建立、使用和刪除這些VLAN。	是
1002–1005	正常	Cisco預設的FDDI和權杖環。不能刪除VLAN 1002-1005。	是
1006–4094	保留	僅適用於乙太網路VLAN。	否

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

預設情況下，具有1024個MAC地址的Catalyst交換機不會啟用擴展系統ID。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。這使交換機能夠支援1024個VLAN，每個VLAN使用唯一的網橋識別符號。

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、	1024

OSR-7609-AC、OSR-7609-DC	
WS-C6513、WS-C6509-NEB-A、WS-C6504-E、WS-C6503-E、WS-C6503、CISCO7603、CISCO7606、CISCO7609、CISCO7613	64[1]

[1]具有64個MAC地址的機箱預設啟用擴展系統ID，並且不能禁用該功能。

如需詳細資訊，請參閱設定STP和IEEE 802.1s MST的*瞭解橋接器ID*一節。

對於具有1024個MAC地址的Catalyst系列交換機，要啟用擴展系統ID，則允許在PVST+下運行的4096個VLAN或16個MISTP例項具有唯一識別符號，而無需增加交換機上所需的MAC地址數量。擴展系統ID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。

下圖顯示了未啟用擴展系統ID時的網橋識別符號。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。

擴展系統ID修改網橋協定資料單元(BPDU)的生成樹協定(STP)網橋識別符號部分。 原始2位元組優先順序欄位被分割為2個欄位；4位橋接器優先順序欄位和12位系統ID擴展，允許VLAN編號為0-4095。

在Catalyst交換機上啟用擴展系統ID以利用擴展範圍VLAN時，需要在同一STP域內的所有交換機上啟用它。這是保持所有交換機上STP根計算一致所必需的。啟用擴展系統ID後，根網橋優先順序將變為4096與VLAN ID的倍數。沒有擴展系統ID的交換機可能會無意中宣告根，因為它們在選擇其網橋ID時具有更細的粒度。

雖然建議在同一個STP域內保持一致的擴展系統ID配置，但向STP域引入具有64個MAC地址的新機箱時，在所有網路裝置上強制實施擴展系統ID是不切實際的。但是，必須瞭解當兩個系統配置了相同的生成樹優先順序時，沒有擴展系統ID的系統具有更好的生成樹優先順序。發出以下命令以啟用擴展系統ID配置：

spanning-tree extend system-id

內部VLAN從VLAN 1006開始按升序分配。為了避免使用者VLAN和內部VLAN之間的衝突，建議儘可能靠近使用者VLAN 4094。在交換器上發出**show vlan internal usage**指令，以顯示內部指派的VLAN。

```
Switch#show vlan internal usage

VLAN Usage
---- --------------------
1006 online diag vlan0
1007 online diag vlan1
1008 online diag vlan2
1009 online diag vlan3
```

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

在本徵IOS中，**可以配置vlan內部分配**策略降序，以便按降序分配內部VLAN。CatOS軟體的CLI等效版本不受正式支援。

vlan內部分配策略降序

思科組態建議

當Catalyst 6500/6000處於VTP伺服器模式時，即使沒有VTP域名，也可以建立VLAN。在運行Cisco IOS系統軟體的Catalyst 6500/6000交換機上配置VLAN之前，請先配置VTP域名。此順序中的組態會與執行CatOS的其他Catalyst交換器保持一致性。

對於是否使用VTP客戶端/伺服器模式或VTP透明模式，沒有特建議。有些客戶喜歡VTP客戶端/伺服器模式的易管理性，儘管本節指出了一些注意事項。建議在每個域中配備兩台伺服器模式交換機以實現冗餘，通常為兩台分佈層交換機。將域中的其餘交換機設定為客戶端模式。在使用VTPv2實施客戶端/伺服器模式時，請記住在同一個VTP域中始終接受更高的修訂版號。如果配置為VTP客戶端或伺服器模式的交換機被引入到VTP域中，並且其修訂版號高於現有的VTP伺服器，則這將覆蓋VTP域中的VLAN資料庫。如果無意更改了配置，並且刪除了VLAN，則此覆蓋可能會導致網路出現重大故障。為了確保客戶端或伺服器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。許多企業更喜歡謹慎的方法，並使用VTP `transparent`模式，原因如下：

- 此做法有助於進行良好的更改控制，因為必須考慮在交換機或中繼埠上修改VLAN的要求。
- VTP透明模式限制了管理員出錯的風險，例如意外刪除VLAN。此類錯誤可能會影響整個域。
- 可以將VLAN從中繼向下修剪到在VLAN中沒有埠的交換機。這會使幀泛洪更加節省頻寬。手動修剪還具有降低的生成樹直徑。如需詳細資訊，請參閱動態Trunk通訊協定一節。每台交換機的VLAN配置也鼓勵這種做法。
- 具有更高的VTP修訂版號的新交換機可以覆蓋整個域VLAN配置，因此不存在引入網路的風險。
- Cisco Works2000的Campus Manager 3.2支援Cisco IOS軟體VTP透明模式。之前要求在VTP域中至少有一台伺服器的限制已被刪除。

VTP命令	意見
vtp域	CDP會檢查該名稱，以便幫助防止網域之間的纜線連線錯誤。域名區分大小寫。

名	
vtp mode {server |客戶端 |透明}	VTP在三種模式之一下運行。
vlan *vlan_number*	這將使用提供的ID建立VLAN。
switchport trunk allowed *vlan_range*	這是一個介面命令，它使中繼可以在需要時傳輸VLAN。預設為所有VLAN。
switchport trunk pruning *vlan_range*	這是一個介面命令，它通過手動修剪來限制STP直徑，例如從分佈層到接入層的中繼上（VLAN不存在）。預設情況下，所有VLAN都適合修剪。

其他選項

在強烈建議使用客戶端/伺服器模式的權杖環環境中，VTPv2是一項要求。

本文檔的思科配置建議部分介紹了修剪VLAN以減少不必要的幀泛洪的好處。**vtp pruning**命令可自動修剪VLAN，從而阻止不需要幀的無效泛洪。

注意：與手動VLAN修剪不同，自動修剪不會限制生成樹直徑。

IEEE已經制定了基於標準的體系結構，以便實現與VTP相似的結果。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。但是，GVRP不在本檔案的範圍之內。

注意：Cisco IOS軟體沒有VTP關閉模式功能，它僅支援具有修剪功能的VTPv1和VTPv2。

快速乙太網路自動交涉

目的

自動協商是IEEE 802.3u快速乙太網(FE)標準的選用功能。自動協商使裝置能夠通過鏈路自動交換有關速度和雙工功能的資訊。自動交涉在第1層(L1)執行。 此功能針對分配給臨時使用者或裝置連線到網路的區域的埠。示例包括接入層交換機和集線器。

操作概述

自動協商使用針對10BASE-T裝置的修改版本的鏈路完整性測試來協商速度並交換其他自動協商引數。最初的10BASE-T鏈路完整性測試稱為正常鏈路脈衝(NLP)。 針對10/100 Mbps自動交涉的連結完整性測試的修改版本稱為快速連結脈衝(FLP)。 作為鏈路完整性測試的一部分，10BASE-T裝置預期每16(+/-8)毫秒(ms)有一個突發脈衝。用於10/100-Mbps自動協商的FLP每16(+/-8)毫秒傳送一次突發脈衝，每62.5(+/-7)微秒傳送一次額外脈衝。突發序列中的脈衝生成代碼字，用於鏈路夥伴之間的相容性交換。

在10BASE-T中，每當站台啟動時都會傳送鏈路脈衝。這是每16毫秒傳送的單個脈衝。當鏈路空閒時，10BASE-T裝置還每16毫秒傳送一次鏈路脈衝。這些鏈路脈衝也稱為心跳或NLP。

100BASE-T裝置發出FLP。此脈衝作為突發而不是一個脈衝傳送。突發在2毫秒內完成，並且每16毫秒再次重複。初始化時，裝置向鏈路夥伴傳送16位FLP消息以進行速度、雙工和流量控制的協商。此16位消息被重複傳送，直到合作夥伴確認該消息。

注意：根據IEEE 802.3u規範，您不能手動將一個鏈路夥伴配置為100 Mbps全雙工，仍可與另一個鏈路夥伴自動協商為全雙工。嘗試將一個連結夥伴設定為100 Mbps全雙工，而將另一個連結夥伴設定為自動交涉，會導致雙工不相符。雙工不相符的結果，因為一個連結夥伴會進行自動交涉，但看不到另一個連結夥伴的任何自動交涉引數。第一個連結夥伴接著預設為半雙工。

所有Catalyst 6500乙太網路交換模組支援10/100 Mbps和半雙工或全雙工。發出**show interface capabilities**命令，以在其他Catalyst交換器上驗證此功能。

導致10/100 Mbps乙太網路連結上的效能問題的原因中，其中一個最常見的是發生在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時。當您重設連結上的一個或兩個連線埠時，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，有時會發生這種情況。當您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。在以下情況下，可以避免發出與效能相關的支援呼叫：

- 建立一個策略，該策略要求為所有非臨時裝置所需的行為配置埠
- 通過適當的更改控制措施實施該策略

效能問題的典型症狀會增加交換機上的幀校驗序列(FCS)、循環冗餘校驗(CRC)、對齊或殘餘計數器。

在半雙工模式下，有一對接收線和一對傳輸線。兩條電線不能同時使用。當接收端存在資料包時，裝置無法傳輸。

在全雙工模式下，有一對相同的接收和傳輸線。但是，由於載波偵聽和衝突檢測功能已被禁用，因此可以同時使用這兩種功能。裝置可以同時傳送和接收。

因此，半雙工到全雙工連線可以運作，但半雙工端發生大量衝突，造成效能下降。之所以會發生衝突，是因為設定為全雙工的裝置可以在收到資料的同時進行傳輸。

此清單中的檔案詳細討論自動交涉。以下檔案說明自動交涉的運作方式，並討論各種組態選項：

- 設定和疑難排解乙太網路 10/100/1000Mb 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，可能手動將其中一個連結夥伴設定為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。出現此情況是因為一個連結夥伴自動交涉，看不到另一個連結夥伴的任何自動交涉引數，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。但是如果您發出**show interface** ***mod/port*** capabilities命令，就可以確認這點。

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）免受與物理層/信令相關的故障的影響。

遠端故障是連結中的錯誤，一個站台可偵測到，而另一個站台無法偵測。斷開的傳輸線就是一個例子。在此示例中，傳送站仍接收有效資料，並通過鏈路完整性監控器檢測鏈路是否正常。但是，傳送站無法檢測到另一個站沒有收到傳輸。檢測到此類遠端故障的100BASE-FX站可以修改其傳輸的IDLE流，以便傳送特殊位元模式來通知鄰居遠端故障。特殊位模式稱為FEFI-IDLE模式。FEFI-IDLE模式隨後會觸發遠端埠關閉(errDisable)。 有關故障保護的更多資訊，請參閱本文檔的單向鏈路檢測部分。

以下模組/硬體支援FEFI:

- Catalyst 6500/6000和4500/4000:所有100BASE-FX模組和GE模組

思科基礎架構連線埠建議

是否在10/100-Mbps連結上設定自動交涉，或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，如果網路介面卡(NIC)或廠商交換器不能完全相符，則可能會出現問題。此外，用於10/100-Mbps自動協商的IEEE 802.3u規範中未描述的特定於供應商的高級功能可能會導致硬體不相容和其他問題。這些型別的高級功能包括自動極性變換和佈線完整性。本檔案將提供範例：

- 現場警報：連線到CAT4K/6K的英特爾Pro/1000T NIC的效能問題

在某些情況下，您需要設定主機、連線埠速度和雙工。一般來說，請完成以下基本故障排除步驟：

- 請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。
- 檢視發行說明以瞭解常見警告。
- 驗證所運行的NIC驅動程式或作業系統的版本。通常需要最新的驅動程式或修補程式。

通常，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。自動協商還可與其它裝置配合使用，例如：

- 使用非臨時裝置，如伺服器和固定工作站
- 從交換機到交換機
- 從交換機到路由器

但是，由於本節提及的一些原因，可能會出現談判問題。如需這些情況下的基本疑難排解步驟，請參閱設定和疑難排解乙太網路10/100/1000Mb半/全雙工自動交涉。

禁用以下項的自動協商：

- 支援交換機和路由器等網路基礎設施裝置的埠
- 其他非臨時終端系統，如伺服器和印表機

請始終對這些埠的速度和雙工設定進行硬編碼。

手動為速度和雙工配置以下10/100 Mbps鏈路配置（通常為100 Mbps全雙工）：

- 交換機到交換機
- 交換機到伺服器
- 交換機到路由器

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

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

發出以下介面命令以設定速度和雙工：

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

思科接入埠建議

終端使用者、移動工作者和臨時主機需要自動協商，以便最大程度地減少對這些主機的管理。您也可以使用Catalyst交換器進行自動交涉。通常需要最新的NIC驅動程式。

核發以下全域命令，以便啟用連線埠的速度自動交涉：

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

註：如果在10/100 Mbps乙太網路連線埠上將連線埠速度設定為自動，則速度和雙工都會自動交涉。無法變更自動交涉連線埠的雙工模式。

當NIC或廠商交換器不完全符合IEEE規範802.3u時，可能會出現問題。此外，用於10/100-Mbps自動協商的IEEE 802.3u規範中未描述的特定於供應商的高級功能可能會導致硬體不相容和其他問題。這些高級功能包括自動極性變換和佈線完整性。

其他選項

當交換機之間的自動協商被禁用時，第1層故障指示也會因某些問題而丟失。使用第2層協定增強故障檢測，如主動式UDLD。

即使啟用了自動協商，自動協商也檢測不到這些情況：

- 連線埠會停滯不前，而且不會接收或傳輸
- 線的一邊向上，但另一邊向下
- 光纜佈線錯誤

自動協商不會檢測到這些問題，因為它們不在物理層。這些問題可能導致STP環路或流量黑洞。

如果兩端都設定了UDLD，UDLD可以偵測到所有這些情況，並錯誤停用連結上的兩個連線埠。透過這種方式，UDLD可以防止STP回圈和流量黑洞。

Gigabit乙太網路自動交涉

目的

Gigabit乙太網路(GE)的自動交涉程式比10/100-Mbps乙太網路(IEEE 802.3z)使用的程式更廣泛。使用GE埠時，使用自動協商進行交換：

- 流量控制引數
- 遠端故障資訊
- 雙工資訊**注意**：Catalyst系列GE埠僅支援全雙工模式。

IEEE 802.3z已被IEEE 802.3:2000規範取代。有關詳細資訊，請參閱本地和都會網路+草案(LAN/MAN 802s)標準訂用。

操作概述

與使用10/100-Mbps FE的自動交涉不同，GE自動交涉不涉及連線埠速度交涉。此外，您無法發出**set port speed**命令來停用自動交涉。GE埠協商預設啟用，GE鏈路兩端的埠必須具有相同的設定。如果鏈路兩端的埠設定不一致，則鏈路不會啟動，這意味著交換的引數不同。

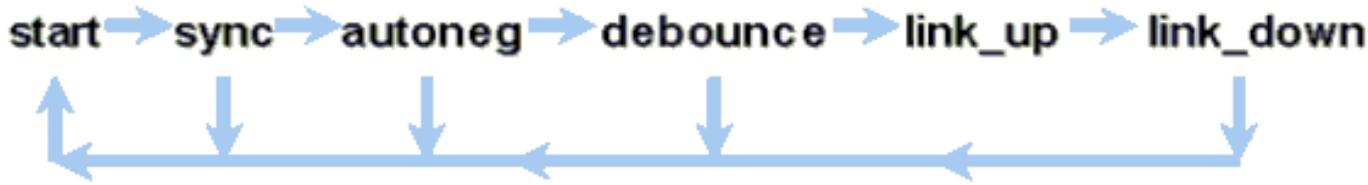
例如，假設有兩個裝置：A和B。每台裝置皆可啟用或停用自動交涉。下表包含可能的設定及其各自的連結狀態：

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中都是有效的。

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，將斷言同步失敗情況，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，則自動階段將不再可行。

GE銅纜規範(1000BASE-T)支援通過下一頁交換自動協商。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：但**是**,GE光纖規範僅對雙工、流量控制和遠端故障檢測的協商作了規定。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。**sync-restart-delay**命令僅在自動協商設定為啟用時才生效。

思科基礎架構連線埠建議

在GE環境中，自動協商的配置比10/100 Mbps環境中重要得多。僅在以下情況下禁用自動協商：

- 在連線到無法支援交涉的裝置的交換器連線埠上
- 當互操作性問題導致連線問題時

在所有交換機到交換機鏈路上，通常在所有GE裝置上啟用Gigabit協商。Gigabit介面的預設值為自動交涉。但是，發出以下命令以確保啟用自動交涉：

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

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，請關閉這兩個功能。如果不關閉這些功能，交換機埠報告未連線，GSR報告錯誤。以下是介面命令序列範例：

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

思科接入埠建議

由於FLP可能因供應商而異，因此您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伺服器上遇到一些千兆位協商問題。讓所有裝置使用千兆位自動協商，除非NIC供應商明確另有說明。

其他選項

流量控制是802.3x規範的可選部分。如果使用流量控制，則必須對其進行協商。裝置可以或不能傳送和/或響應暫停幀（眾所周知的MAC 01-80-C2-00-00-00 0F）。 且裝置可能不同意遠端鄰居的流量控制請求。具有輸入緩衝區並開始填滿的連線埠會向連結夥伴傳送暫停訊框。連結夥伴會停止傳輸，並在連結夥伴輸出緩衝區中保留任何其他訊框。此函式不能解決任何穩態超訂用問題。但是，該函式有效地使輸入緩衝區在突發事件中比夥伴輸出緩衝區大一些部分。

PAUSE功能旨在防止裝置（交換機、路由器或終端站）由於短期瞬態流量過載導致的緩衝區溢位情況而不必要的丟棄接收的幀。流量過載下的裝置在傳送暫停幀時防止內部緩衝區溢位。暫停訊框包含引數，指出全雙工夥伴在傳送更多資料訊框前等待的時間長度。收到暫停訊框的合作夥伴會在指定的期間停止傳送資料。當此計時器到期時，站台開始再次傳送資料幀，從站台關閉的位置。

發出暫停的站點可以發出包含零時間引數的另一個暫停幀。此操作將取消暫停期的剩餘時間。因此，新接收的暫停訊框會覆寫目前進行中的任何暫停作業。此外，發出暫停訊框的站台可以延長暫停時間。站會在第一個暫停期間到期前發出包含非零時間引數的另一個暫停訊框。

此暫停操作不是基於速率的流量控制。該操作是一種簡單的啟動和停止機制，允許流量下的裝置（傳送暫停幀的裝置）有機會減少緩衝區擁塞。

此功能的最佳用途是在存取連線埠和終端主機之間的連結上，其中主機輸出緩衝區可能和虛擬記憶體一樣大。使用交換機到交換機的好處有限。

發出以下介面命令，以在交換器連線埠上控制這點：

```
flowcontrol {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和WS-X4306）不會傳送暫停幀，即使它們協商這樣做，因為它們是無阻塞的。

動態Trunk協定

目的

為了在裝置之間擴展VLAN，中繼會臨時識別和標籤（本地鏈路）原始乙太網幀。此操作使幀能夠在單個鏈路上多路複用。該操作還可以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。

操作概述

DTP是第二代動態ISL(DISL)。DISL僅支援ISL。DTP同時支援ISL和802.1Q。這種支援可確保中繼任一端的交換機就中繼幀的不同引數達成一致。這些引數包括：

- 已配置的封裝型別
- 本徵VLAN
- 硬體功能

DTP支援還有助於防止非中繼埠泛洪已標籤的幀，這是潛在的嚴重安全風險。DTP可防止此類泛洪，因為它可確保埠及其鄰居處於一致的狀態。

中繼模式

DTP是在交換機埠與其鄰居之間協商配置引數的第2層協定。DTP使用另一個眾所周知的組播MAC地址01-00-0c-cc-cc-cc和SNAP協定型別0x2004。下表介紹了每種可能的DTP協商模式的功能：

模式	功能	傳輸的DTP幀？	最終狀態（本地埠）
動(相當於CatOS中動模式)	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，定期	
(相當於CatOS中機模式)	將埠置於永久模式，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，定期	無條件
Negotiate	使埠進入模式，但不允許埠生成DTP幀。您必須手動將相鄰埠配置為中繼埠，才能建立中繼鏈路。這對於不支援DTP的裝置很有用。	否	無條件
desirable(CatOS comparable命令是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，定期	只有在遠端模式為on、auto或desirable時，它才會處於trunk狀

			態。
	將埠置於永久，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。	否，在穩定狀態，但從on更改後傳輸通知以加快遠端端檢測。	

注意：可以設定或協商ISL和802.1Q封裝型別。

在預設配置中，DTP在鏈路上承擔以下特徵：

- 點對點連線和Cisco裝置支援僅是點對點的802.1Q中繼埠。
- 在整個DTP協商過程中，埠不參與STP。只有在埠型別變為以下三種型別之一時，才會將埠新增到STP:存取ISL802.1Q在連線埠加入STP之前，PAgP是下一個要執行的程式。PAgP用於EtherChannel自動協商。
- VLAN 1始終存在於中繼埠上。如果埠在ISL模式下是中繼埠，則DTP資料包在VLAN 1上傳送。如果埠在ISL模式下不是中繼埠，則DTP資料包在本徵VLAN上傳送（對於802.1Q中繼埠或非中繼埠）。
- DTP資料包傳輸VTP域名，以及中繼配置和管理狀態。VTP域名必須匹配才能使協商中繼啟動。這些資料包在協商過程中每秒傳送一次，在協商後每隔30秒傳送一次。如果處於或desirable模式的埠在5分鐘（分鐘）內未檢測到DTP資料包，則該埠將被設定為非中繼。

注意：您必須瞭解，模式trunk、nonegotiate**和**access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。

封裝型別

ISL操作概述

ISL是Cisco專有的中繼協定（VLAN標籤方案）。ISL已使用多年。相比之下，802.1Q更新很多，但802.1Q是IEEE標準。

ISL以兩級標籤方案完全封裝原始幀。因此，ISL實際上是一種隧道協定，而且作為額外的優勢，它承載非乙太網幀。ISL為標準乙太網幀新增了一個26位元組的報頭和4位元組的FCS。配置為中繼的埠需要和處理較大的乙太網幀。ISL支援1024個VLAN。

幀格式 — ISL標籤為著色

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

Encapsulated Frame	FCS
Variable length	32 bits

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

雖然IEEE 802.1Q標準只適用於乙太網，但該標準規定的範圍遠遠超出封裝型別。802.1Q包括通用屬性註冊協定(GARP)、生成樹增強功能和802.1p QoS標籤。有關詳細資訊，請參閱IEEE Standards Online

802.1Q幀格式保留了原始乙太網SA和DA。但是，交換機現在必須預期會收到小巨型幀，即使在主機可以使用標籤來表示QoS信令的802.1p使用者優先順序的接入埠上也是如此。標籤是4個位元組。802.1Q乙太網v2幀為1522位元組，是IEEE 802.3ac工作組的成果。此外，802.1Q支援4096 VLAN的編號空間。

除了本徵VLAN中的資料幀之外，傳輸和接收的所有資料幀都帶有802.1Q標籤。在這種情況下，有一個基於輸入交換器連線埠組態的隱含標籤。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，這些幀也可以通過標籤接收。

請參閱以下文件以瞭解更多資訊：

- VLAN互通性
- 使用Cisco CatOS系統軟體的802.1q封裝在Catalyst 4500/4000、5500/5000和6500/6000系列交換器之間建立中繼

802.1Q/802.1p幀格式

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

思科組態建議

思科的一個主要設計原則是在可能實現一致性的情況下努力保持網路的一致性。所有較新的Catalyst產品都支援802.1Q，某些產品僅支援802.1Q，例如Catalyst 4500/4000和Catalyst 6500系列中的早期模組。因此，所有新的實施都必須遵循此IEEE 802.1Q標準，而舊的網路需要從ISL逐步遷移。

發出以下介面命令以在特定埠上啟用802.1Q中繼：

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

IEEE標準允許廠商互通性。隨著新的支援主機802.1p的NIC和裝置的推出，供應商互操作性在所有的思科環境中都是有利的。儘管ISL和802.1Q實施都很可靠，但IEEE標準最終擁有更大的現場曝光度以及更大的第三方支援，包括對網路分析器的支援。此外，一個次要的考慮因素是，802.1Q標準的封裝開銷也比ISL低。

為完整起見，本徵VLAN上的隱式標籤會帶來安全隱患。幀可以從一個VLAN(VLAN X)傳輸到另一個VLAN(VLAN Y)，而無需路由器。如果來源連線埠(VLAN X)與同一交換器上802.1Q主幹的本徵VLAN位於同一VLAN中，則無需路由器便可進行傳輸。因應措施是對中繼的本徵VLAN使用虛擬VLAN。

發出以下介面命令，為特定埠上的802.1Q中繼建立本地（預設）VLAN:

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

由於所有較新的硬體都支援802.1Q，因此所有新的實施都遵循IEEE 802.1Q標準，並逐步從ISL遷

移早期網路。直到最近，許多Catalyst 4500/4000模組都不支援ISL。因此，802.1Q是乙太網中繼的唯一選項。請參閱**show interface capabilities** 命令的輸出，或適用於CatOS的**show port capabilities**命令。由於中繼支援需要適當的硬體，因此不支援802.1Q的模組永遠無法支援802.1Q。軟體升級不支援802.1Q。Catalyst 6500/6000和Catalyst 4500/4000交換機的大多數新硬體都支援ISL和802.1Q。

如果交換機管理介面和本徵VLAN一節討論的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。控制協定的示例包括CDP和VTP。

此外，如VLAN 1一節所述，建立中繼時，CDP、VTP和PAgP資料包始終在VLAN 1上傳送。使用dot1q(802.1Q)封裝時，如果交換器原生VLAN發生變更，這些控制幀將使用VLAN 1進行標籤。如果連線到路由器的dot1q中繼和交換機上的本徵VLAN發生更改，則VLAN 1中的子介面對於接收標籤的CDP幀和在路由器上提供CDP鄰居可見性是必要的。

注意：本地VLAN的隱式標籤導致dot1q存在潛在的安全問題。在沒有路由器的情況下，幀可以從一個VLAN傳輸到另一個VLAN。有關詳細資訊，請參閱入侵檢測FAQ 。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。為了達到此目的，大多數Cisco客戶只需將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。

思科建議在兩端使用`dynamic desirable`的顯式中繼模式配置。此模式為預設模式。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，即埠處於`up`狀態並處於中繼狀態。此模式與`on`模式不同，後者可使連線埠在鄰居設定錯誤的情況下顯示為開啟。此外，`desirable` mode trunk在鏈路的一端無法成為trunk或丟棄trunk狀態時提供穩性。

如果使用DTP在交換機之間協商封裝型別，並且如果兩端都支援ISL，則預設選擇ISL作為獲勝者，您必須發出此介面命令以指定dot1q[1]:

```
switchport trunk encapsulation dot1q
```

[1]包括WS-X6548-GE-TX和WS-X6148-GE-TX的某些模組不支援ISL中繼。這些模組不接受**switchport trunk encapsulation *dot1q*** 指令。

註：發出switchport mode access命令可禁用埠上的中繼。此停用有助於在開啟主機連線埠時消除浪費的交涉時間。

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

其他選項

另一種常見客戶配置在分佈層使用`dynamic desirable`模式，在接入層使用最簡單的預設配置(`dynamic auto` mode)。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。您可以使用`nonegotiate`模式將埠設定為與這些裝置無條件地中繼。此模式有助於在整個園區實現通用設定的標準化。

連線到Cisco IOS路由器時，思科建議`nonegotiate`。在整個橋接過程中，從配置了**switchport mode trunk**的連線埠接收的某些DTP訊框可以返回主干連線埠。收到DTP幀後，交換機埠會嘗試進行不必要的重新協商。為了重新交涉，交換器連線埠將TRUNK，然後開啟如果啟用`nonegotiate`，交換機將不傳送DTP幀。

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

生成樹通訊協定

目的

生成樹在冗餘交換網路和網橋網路中維護無環路的第2層環境。如果沒有STP，幀將無限循環和/或倍增。此事件會導致網路崩潰，因為高流量會中斷廣播域中的所有裝置。

在某些方面，STP是早期的協定，最初是為基於軟體的網橋規範(IEEE 802.1D)開發的。 但是，要在具有以下功能的大型交換網路中成功實施STP，可能會很複雜：

- 許多VLAN
- 域中的許多交換機
- 多供應商支援
- 較新的IEEE增強功能

Cisco IOS System Software已進行了新的STP開發。包括802.1w快速STP和802.1s多生成樹協定的新IEEE標準提供快速收斂、負載共用和控制平面擴展。此外，STP增強功能（如RootGuard、BPDU過濾、Portfast BPDU防護和環路防護）可提供針對第2層轉發環路的額外保護。

PVST+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是從所有交換機傳送的，其中包含每台交換機的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中從根攜帶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。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並將其與根資訊一起傳送。

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。

請參閱以下文件以瞭解更多資訊：

- 配置STP和IEEE 802.1s MST
- 瞭解快速跨距樹狀目錄通訊協定 (802.1w)

基	名	功能

本計時器預設值	稱	
2秒	你好	控制BPDU的離開。
15秒	轉發延遲(Fwd delay)	控制埠處於listening狀態和learning狀態的時間長度，並影響拓撲更改過程。
20秒	maxage	控制交換機在查詢備用路徑之前保持當前拓撲的時間長度。在最大老化時間（最大老化時間）過後，BPDU會視為已過時，並且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，則交換機聲稱自己是指定埠上的根埠。

思科建議您不要更改計時器，因為這會對穩定性產生負面影響。部署的大多數網路均未調整。可通過命令列訪問的簡單STP計時器（如hello-interval、maxage等）本身由一組複雜的其他假定和內部計時器組成。因此，很難調整計時器和考慮所有影響。此外，您可以破壞UDLD保護。有關詳細資訊，請參閱單向鏈路檢測部分。

STP計時器注意事項：

預設STP計時器值基於這樣的計算：考慮七台交換機的網路直徑（從根到網路邊緣的七個交換機跳），以及BPDU從根網橋傳輸到網路中相隔七跳的邊緣交換機所需的時間。此假設可計算大多數網路可接受的計時器值。但是，您可以將這些計時器更改為更最佳化的值，以便在網路拓撲更改過程中加快收斂時間。

您可以使用特定VLAN的網路直徑配置根網橋，並相應地計算計時器值。思科建議，如果您必須做出更改，則只在VLAN的根網橋上配置直徑和可選的hello時間引數。

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

此宏使指定VLAN的交換機成為根橋，根據指定的直徑和hello時間計算新的計時器值，並將配置BPDU中的此資訊傳播到拓撲中的所有其它交換機。

新埠狀態和埠角色一節描述了802.1D STP，並將802.1D STP與快速STP(RSTP)進行比較和比較。如需RSTP的詳細資訊，請參閱瞭解快速跨距樹狀目錄通訊協定(802.1w)。

新埠狀態和埠角色

802.1D有四種不同的埠狀態：

- 偵聽
- 學習
- 封鎖
- 轉發

有關詳細資訊，請參閱埠狀態部分中的表。連線埠的狀態是混合的（無論是封鎖流量還是轉送流量），連線埠在作用中拓撲所扮演的角色（根連線埠、指定連線埠等）亦然。 例如，從操作角度來看，處於阻塞狀態的埠和處於偵聽狀態的埠之間沒有區別。它們都丟棄幀，而且不會獲知MAC地址。真正的區別在於生成樹分配給埠的角色。可以安全地假設偵聽埠是指定埠或根埠，並且正在進入轉發狀態。遺憾的是，一旦埠處於轉發狀態，就無法從埠狀態推斷埠是根埠還是指定埠。這證明了此基於狀態的術語的失敗。RSTP解決了此故障，因為RSTP將埠角色和狀態分離。

埠狀態

STP 802.1D中的埠狀態

埠狀態	手段	到下一個狀態的預設計時
	管理性關閉。	
	接收BPDU並停止使用者資料。	監控BPDU的接收。如果檢測到直接/本地鏈路故障，則等待20秒以等待maxage過期或立即更改。
	傳送或接收BPDU，以檢查是否需要返回阻塞狀態。	等待15秒Fwddelay。
	構建拓撲/CAM表。	等待15秒Fwddelay。
	傳送/接收資料。	

基本拓撲更改總數為：

- 20 + 2(15)= 50秒（如果等待maxage過期）
- 直接鏈路故障30秒

RSTP中只剩下三種埠狀態，對應於三種可能的運行狀態。802.1D禁用、阻塞和偵聽狀態已合併為唯一的802.1w丟棄狀態。

STP(802.1D)埠狀態	RSTP(802.1w)埠狀態	埠是否包含在活動拓撲中？	埠是否學習MAC地址？
已禁用	丟棄	否	否
封鎖	丟棄	否	否
偵聽	丟棄	是	否
學習	學習	是	是
轉發	轉發	是	是

埠角色

角色現在是分配給給定埠的變數。根埠和指定埠角色仍然保留，但阻塞埠角色現在拆分為備份和替代埠角色。跨距樹狀目錄演演算法(STA)根據BPDU判斷連線埠的作用。請記住有關BPDU的以下內

容以保持簡單：總有一種方法可以比較任意兩個BPDU並確定其中一個比另一個更有用。此決定的基礎是儲存在BPDU中的值，有時是接收BPDU的埠。本節的其餘部分說明了埠角色非常實用的方法。

根埠角色

在網橋上接收最佳BPDU的埠是根埠。這是在路徑開銷方面離根網橋最近的埠。STA會在整個橋接網路（每個VLAN）中選擇一個根網橋。 根網橋傳送的BPDU比任何其他網橋可以傳送的BPDU更有用。根網橋是網路中唯一沒有根埠的網橋。所有其他網橋在至少一個埠上接收BPDU。

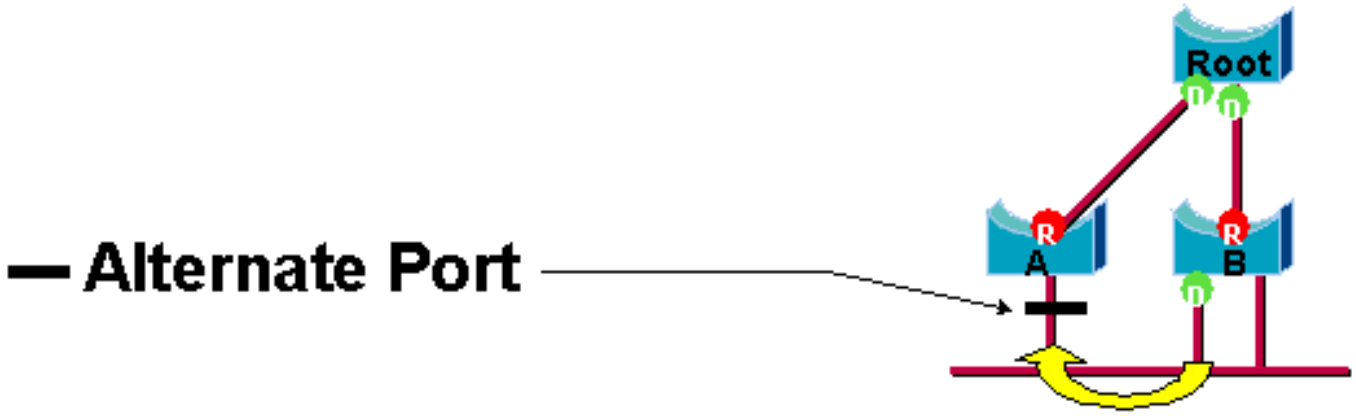
指定埠角色

如果連線埠可以傳送連線埠所連線網段上的最佳BPDU，則指定連線埠。802.1D網橋將不同的網段（例如乙太網網段）連結在一起，以便建立橋接域。在給定的網段上，只能有一個通向根網橋的路徑。如果有兩條路徑，則網路中有一個橋接回圈。連線到指定網段的所有網橋都會偵聽其他網段的BPDU，並同意將最佳BPDU作為指定網段的指定網橋傳送到的網橋。該網橋上的相應埠是指定的。

備用和備用埠角色

這兩個埠角色對應於802.1D的阻塞狀態。阻塞埠的定義是一個非指定埠或根埠埠。阻塞埠收到的BPDU比它在其網段上發出的BPDU更有用。請記住，連線埠絕對需要接收BPDU才能保持封鎖狀態。RSTP為此引入了這兩個角色。

備用埠是從另一個網橋接收更有用的BPDU而被阻塞的埠。此圖說明：



備用埠是埠，通過從埠所在的同一網橋接收更有用的BPDU而被阻止。此圖說明：

此區別已在802.1D內部做出。這基本上就是Cisco UplinkFast的運作方式。其基本原理是備用埠提供到根網橋的備用路徑。因此，如果根埠發生故障，此埠可以替換根埠。當然，備份埠提供到同一網段的冗餘連線，並且無法保證到根網橋的備用連線。因此，備份埠被排除在上行鏈路組之外。

因此，RSTP會使用與802.1D完全相同的標準來計算生成樹的最終拓撲。使用不同網橋和埠優先順序的方式沒有變化。名稱阻止用於思科實施中的丟棄狀態。CatOS版本7.1和更新版本仍顯示偵聽和學習狀態，這甚至提供了比IEEE標準要求的更多有關埠的資訊。但是，新的功能是，現在協定為埠確定的角色與其當前狀態之間存在差異。例如，現在對埠進行指定和同時阻塞是完全有效的。雖然這通常發生很短時間，但這僅僅意味著該埠處於面向指定轉發的過渡狀態。

STP與VLAN的互動

將VLAN與生成樹關聯有三種不同的方法：

- 適用於所有VLAN的單個生成樹或通用生成樹協定(CST)，例如IEEE 802.1D
- 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(MST)，例如IEEE 802.1s

從配置角度來看，這三種與與VLAN互動有關的生成樹模式可以配置為以下三種模式之一：

- **pvst** — 每個VLAN生成樹。這實際上實施了PVST+，但在Cisco IOS軟體中僅記錄為PVST。
- **rapid-pvst** - 802.1D標準的演化加快了收斂時間，並融合了UplinkFast和BackboneFast基於標準的(802.1w)屬性。
- **mst** — 這是每組VLAN或MST生成樹的802.1s標準。這也將802.1w快速元件納入標準中。

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或PVST+有一個生成樹允許負載均衡，但隨著VLAN數量的增加，需要更多的BPDU CPU處理。

新的802.1s標準(MST)允許定義最多16個活動STP例項/拓撲並將所有VLAN對映到這些例項。在典型的園區環境中，只需要定義兩個例項。此技術允許STP擴展到數千個VLAN，同時支援負載均衡。

適用於Catalyst 6500的Cisco IOS軟體版本12.1(11b)EX和12.1(13)E中引入了快速PVST和預標準MST支援。Catalyst 4500搭載Cisco IOS軟體版本12.1(12c)EW和更新版本支援預先標準MST。適用於Catalyst 4500平台的Cisco IOS軟體版本12.1(19)EW新增了快速PVST支援。適用於Catalyst 6500的Cisco IOS軟體版本12.2(18)SXF和適用於Catalyst 4500系列交換器的Cisco IOS軟體版本12.2(25)SG支援標準相容的MST。

如需詳細資訊，請參閱瞭解快速跨距樹狀目錄通訊協定(802.1w)和瞭解多重跨距樹狀目錄通訊協定(802.1s)。

生成樹邏輯連線埠

Catalyst 4500和6500版本說明針對每台交換機的生成樹中的邏輯埠數量提供指導。所有邏輯埠的總和等於交換機上的中繼數乘以中繼上的活動VLAN數，再加上交換機上的非中繼介面數。如果最大邏輯介面數超過限制，Cisco IOS軟體將生成系統日誌消息。建議不要超出建議指導。

下表比較了各種STP模式和管理引擎型別支援的邏輯埠數：

主管	PVST+	RPVST+	MST
Catalyst 6500監督器1	每個交換模塊共計6,0001,200	每個交換模組共6,000個1,200個	每個交換模組共25,000個3,002個
Catalyst 6500監督器2	每個交換模塊共計13,000個1,8002個	每個交換模組共10,000個1,8002個	每個交換模組共50,000個6,0002個
Catalyst 6500監督器720	每個交換模組共13,000個共1,8002個	每個交換模組共10,000個1,8002個	每個交換模組50,003共6,0002個
Catalyst 4500監督器II plus	共計1 500人	共計1 500人	共計25,000
Catalyst 4500監督器II plus-10GE	共計1 500人	共計1 500人	共計25,000
Catalyst 4500監督器IV	共3,000個	共3,000個	總共50,000人
Catalyst 4500監督器V	共3,000個	共3,000個	總共50,000人
Catalyst 4500監	共3,000個	共3,000個	共計80,000

督器V 10GE			

[1] Cisco IOS軟體版本12.1(13)E之前的PVST+支援的最大邏輯連線埠總數為4,500。

[2] 10 Mbps、10/100 Mbps和100 Mbps交換模組最多支援每個模組1,200個邏輯介面。

[3] Cisco IOS軟體版本12.2(17b)SXA之前的MST支援的最大邏輯連線埠總數為30,000。

建議

如果沒有硬體、軟體、裝置數量和VLAN數量等詳細資訊，很難提供生成樹模式建議。通常，如果邏輯埠數未超過推薦的准則，則建議在新網路部署中使用快速PVST模式。快速PVST模式提供快速的網路融合，無需額外配置（如主幹快速和上行鏈路快速）。發出以下命令以在快速PVST模式下設定生成樹：

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

其他選項

在具有舊硬體和舊軟體的混合網路中，建議使用PVST+模式。發出此命令，在PVST+模式下設定生成樹：

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

對於具有大量VLAN的VLAN everywhere網路設計，建議使用MST模式。對於此網路，邏輯埠的總和可以超過PVST和快速PVST的指導標準。發出以下命令以在MST模式下設定生成樹：

```
spanning-tree mode mst
```

BPDU格式

為了支援IEEE 802.1Q標準，思科擴展了現有的PVST協定，以便提供PVST+協定。PVST+增加了對IEEE 802.1Q單生成樹區域鏈路的支援。PVST+相容IEEE 802.1Q單生成樹和現有的Cisco PVST協定。此外，PVST+新增了檢查機制，以確保交換機之間的埠中繼和VLAN ID配置不不一致。PVST+與PVST的即插即用相容，無需新的命令列介面(CLI)命令或配置。

以下是PVST+協定運行理論的一些亮點：

- PVST+可與802.1Q單生成樹互操作。PVST+通過802.1Q中繼與通用STP上符合802.1Q標準的交換機互操作。預設情況下，通用生成樹位於VLAN 1（本徵VLAN）上。在802.1Q鏈路上傳送或接收一個公共的生成樹BPDU，其使用IEEE標準網橋組MAC地址（01-80-c2-00-00-00，協定型別0x010c）。通用生成樹可以植根於PVST或單生成樹區域。
- PVST+通過802.1Q VLAN區域將PVST BPDU作為組播資料隧道。對於中繼上的每個VLAN，會傳輸或接收具有Cisco共用STP(SSTP)MAC地址(01-00-0c-cc-cd)的BPDU。對於等於埠VLAN識別符號(PVID)的VLAN，BPDU未標籤。對於所有其他VLAN，會標籤BPDU。

- PVST+通過ISL中繼向後相容PVST上的現有Cisco交換機。ISL封裝的BPDU通過ISL中繼傳輸或接收，這與以前的Cisco PVST相同。
- PVST+會檢查埠和VLAN是否不一致。PVST+會阻塞那些接收不一致BPDU的埠，以防止出現轉發環路。PVST+還通過系統日誌消息通知使用者任何不一致。

注意：在ISL網路中，所有BPDU都使用IEEE MAC地址傳送。

思科配置建議

所有Catalyst交換機預設啟用STP。即使您選擇的設計不包括第2層環路且未啟用STP以主動維護阻塞埠，也出於以下原因保持啟用該功能：

- 如果存在環路，STP可防止因組播和廣播資料而導致問題惡化。錯誤修補、纜線損壞或其他原因通常會引發回圈。
- STP可防止EtherChannel故障。
- 大多數網路都配置了STP，因此可獲得最大的現場風險。更多的曝光通常等同於更穩定的代碼。
- STP可防止雙連線NIC的不當行為（或在伺服器上啟用橋接）。
- 許多協定與代碼中的STP密切相關。示例包括：PAgP網際網路群組訊息通訊協定(IGMP)窺探中繼如果不使用STP運行，可能會獲得不想要的結果。
- 在所報告的網路中斷期間，思科工程師通常建議，如果不使用STP（如果可以想象的話）是故障的核心。

若要在所有VLAN上啟用生成樹，請發出以下全域性命令：

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

請勿更改計時器，否則會影響穩定性。部署的大多數網路均未調整。可通過命令列訪問的簡單STP計時器（如hello-interval和maxage）包含一組複雜的其他假定和內部計時器。因此，如果您嘗試調整計時器，並考慮所有影響，可能會遇到困難。此外，您可以破壞UDLD保護。

理想情況下，將使用者流量限制在管理VLAN之外。Catalyst 6500/6000 Cisco IOS交換器不適用此規則。但是，對於可以擁有單獨管理介面並且需要與Cisco IOS交換機整合的小端Cisco IOS交換機和CatOS交換機，您仍需要遵守此建議。尤其是對於較舊的Catalyst交換機處理器，將管理VLAN與使用者資料分隔開來，以避免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，以致處理器可能錯過一個或多個BPDU。但是，具有更強大的CPU和節流控制的較新交換機可以緩解這種顧慮。如需詳細資訊，請參閱本檔案的交換器管理介面和本地VLAN一節。

請勿過度設計冗餘。這會導致阻塞埠過多，並對長期穩定性產生不利影響。將STP總直徑保持在七跳以下。儘可能採用此設計嘗試設計思科多層模型。模型具有以下特性：

- 更小的交換域
- STP三角形
- 確定性阻塞埠

影響和瞭解根功能和阻塞埠所在的位置。在拓撲圖中記錄此資訊。瞭解您的生成樹拓撲，這對於故障排除至關重要。阻塞埠是STP故障排除開始的地方。從阻塞狀態變為轉發狀態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，因為這些層被視為網路的最穩定部分。檢查最佳第3層和熱待命路由器協定(HSRP)與第2層資料轉發路徑的重疊。

此命令是配置網橋優先順序的宏。根將優先順序設定為大大低於預設值(32,768)，而輔助將優先順序設定為合理低於預設值：

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

注意：此宏將根優先順序設定為以下任一項：

- 預設值為8192
- 當前根優先順序減去1（如果知道另一個根網橋）
- 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，這是一種雙向練習。該操作限制不需要特定VLAN的網路部分的STP和NMP處理開銷的直徑。VTP自動修剪不會從中繼中刪除STP。您還可以從中繼中移除預設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

思科有另一個STP協定，稱為**VLAN網橋**，它使用公認的目標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，而不干擾這些VLAN上運行的IEEE生成樹例項，則此協定最有用。如果非橋接流量的VLAN介面被第2層流量阻塞，則重疊的第3層流量也會在不經意間被剪除，這是不需要的副作用。如果非橋接流量的VLAN介面與IP VLAN屬於同一STP，則很容易發生第2層阻塞。VLAN網橋是橋接協定的STP的一個單獨例項。該協定提供了獨立的拓撲，可以對其進行操作而不會影響IP流量。

如果需要在思科路由器（如MSFC）上的VLAN之間進行橋接，請運行VLAN網橋協定。

STP PortFast功能

您可以使用PortFast繞過存取連線埠上的正常跨距樹狀目錄作業。PortFast可加速終端站與鏈路初始化後終端站需要連線的服務之間的連線。Microsoft DHCP實施需要在鏈路狀態啟動後立即看到處於模式的接入埠，以便請求和接收IP地址。某些通訊協定(例如網際網路封包交換(IPX)/序列封包交換(SPX))在連結狀態啟動模式的存取連線埠，以避免產生最近的伺服器(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。

PortFast操作概述

PortFast會跳過STP的正常、和狀態。在連結顯示為開啟後，此功能會將連線埠直接從移至模式。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。此過程可能佔用(2 x ForwardDelay)時間，預設情況下為30秒。

Portfast式可防止每次連線埠狀態從學習到轉送發生變化時產生STP拓撲變通知(TCN)。TCN是正常的。但是，一波TCN到達根網橋可能會不必要地延長收斂時間。一波TCN通常發生在人們開啟個人電腦的早晨。

思科接入埠配置建議

將所有已啟用主機埠的STP PortFast設定為on。此外，對於交換機 — 交換機鏈路和未使用的埠，將STP PortFast明確設定為off。

在介面組態模式下發出**switchport host** macro命令，以便為存取連線埠實作建議組態。此配置還顯著幫助自動協商和連線效能：

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

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

註：PortFast並不意味著埠上完全沒有運行生成樹。BPDU仍會被傳送、接收和處理。生成樹對於功能全面的LAN至關重要。如果沒有環路檢測和阻塞，環路可能會無意中迅速導致整個LAN癱瘓。

此外，請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。如果您讓這些協定進行協商，埠啟用的後續延遲可能會導致不良情況。來自工作站的初始資料包（如DHCP和IPX請求）不會被轉發。

更好的選擇是在全域性配置模式下使用以下命令預設配置PortFast:

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

接下來，在任何只有一個集線器或交換器位於一個VLAN中的存取連線埠上，使用**interface**指令在每個介面上停用PortFast功能：

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

其他選項

PortFast BPDU防護提供了一種防止環路的方法。BPDU防護會在非中繼埠上接收BPDU時將埠轉換為errDisable狀態。

在正常情況下，切勿在為PortFast配置的接入埠上接收任何BPDU資料包。傳入BPDU表示配置無效。最佳操作是關閉存取連線埠。

Cisco IOS系統軟體提供有用的全域性命令，可在為UplinkFast啟用的任何埠上自動啟用BPDU-ROOT-GUARD。*始終*使用此命令。此命令針對每台交換機運行，而不是針對每個埠。

發出此全域性命令以啟用BPDU-ROOT-GUARD:

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

如果連線埠關閉，簡單網路管理通訊協定(SNMP)陷阱或系統日誌訊息會通知網路管理員。您還可以為errDisabled連線埠設定自動時間。如需詳細資訊，請參閱本檔案的單向連結偵測一節。

如需進一步的詳細資訊，請參閱跨距樹狀目錄PortFast BPDU防護增強功能。

註：Cisco IOS軟體版本12.1(11b)E中引入了中繼埠的PortFast。中繼埠的PortFast旨在增加第3層網路的收斂時間。使用此功能時，請確保根據介面禁用BPDU防護和BPDU過濾器。

UplinkFast

目的

UplinkFast在網路接入層發生直接鏈路故障後提供快速STP收斂。UplinkFast無需修改STP即可運行。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。請參閱瞭解和設定Cisco UplinkFast功能。

操作概述

在接入層使用思科多層設計模型時，如果轉發上行鏈路丟失，阻塞上行鏈路會立即移動到狀態。此功能不會等待`listening`和`learning`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，無需經歷典型的30秒收斂延遲。

因為UplinkFast有效地繞過正常的STP拓撲更改處理過程(和)，所以需要替代的拓撲更正機制。機制需要使用本地終端站可通過備用路徑到達的資訊更新域中的交換機。因此，運行UplinkFast的接入層交換機也會為其CAM表中的每個MAC地址生成幀，以生成一個眾所周知的組播MAC地址（01-00-0c-cd-cd-cd HDLC協定0x200a）。 此過程將使用新拓撲更新域中所有交換機的CAM表。

思科建議

如果執行802.1D跨距樹狀目錄，思科建議您為具有受阻連線埠的存取交換器啟用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UplinkFast（通常是Cisco多層設計中的分佈層交換機和核心層交換機）。一般情況下，請勿在有兩條以上出網路的交換器上啟用UplinkFast。如果交換機處於複雜的訪問環境中，並且您有多個鏈路阻塞和一個鏈路轉發，請避免在交換機上使用此功能，或者諮詢高級服務工程師。

發出此全域性命令以啟用UplinkFast:

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

Cisco IOS軟體中的此命令不會自動將所有橋接器優先順序值調整為高值。相反，該命令只更改那些具有網橋優先順序的VLAN，而這些優先順序尚未手動更改為其他值。此外，與CatOS不同，當還原已啟用UplinkFast的交換器時，此指令的no形式(**no spanning-tree uplinkfast**)會將所有變更的值回覆為預設值。因此，當您使用此命令時，*必須*在前後檢查網橋優先順序的當前狀態，以確保達到預期的結果。

注意：啟用協定**過濾**功能時，UplinkFast命令需要all protocols關鍵字。因為CAM在啟用協定過濾時記錄協定型別以及MAC和VLAN資訊，所以必須為每個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RSTP配置UplinkFast，因為該機制是原生包括在RSTP中並自動啟用的。

BackboneFast

目的

BackboneFast可從間接鏈路故障中快速收斂。BackboneFast可將收斂時間從預設的50秒縮短到（通常為）30秒，從而向STP新增功能。同樣地，此功能僅適用於運行802.1D的情況。運行快速PVST或MST（包括快速元件）時，請勿配置該功能。

操作概述

當交換器上的根連線埠或封鎖連線埠收到來自指定橋接器的次級BPDU時，會啟動BackboneFast。當下游交換機失去與根的連線並開始傳送BPDU以選擇新的根時，埠通常會收到下級BPDU。下級BPDU將交換機標識為根網橋和指定網橋。

在正常的生成樹規則下，接收交換機在配置的最大時間忽略下級BPDU。預設情況下，最大值為20秒。但是，使用BackboneFast時，交換機將下級BPDU視為拓撲可能變化的訊號。交換機使用根鏈路查詢(RLQ)BPDU來確定它是否有到根網橋的備用路徑。此RLQ協定新增允許交換機檢查根是否仍然可用。RLQ將阻塞埠移到，並通知傳送下級BPDU的隔離交換機根仍然在那裡。

以下是協定操作的一些要點：

- 交換器僅將RLQ封包從根連線埠發出（這表示封包將前往根目錄）。
- 接收RLQ的交換機可以回覆是根交換機，或者該交換機知道它失去了與根的連線。如果交換機不知道這些事實，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，交換機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，請丟棄該回覆。

該操作可以將STP收斂時間縮短最多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。

思科建議

只有在整個生成樹域可以支援此功能的情況下，才能在運行STP的所有交換機上啟用BackboneFast。您可以在不中斷生產網路的情況下新增該功能。

發出以下全域性命令以啟用BackboneFast:

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

注意：必須在域中的所有交換機上配置此全域性級別命令。該命令為STP新增了所有交換機都需要瞭解的功能。

其他選項

Catalyst 2900XL和3500XL交換器不支援BackboneFast。一般情況下，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，則需要啟用BackboneFast。在具有XL交換機的環境中，在嚴格的拓撲下，實施BackboneFast時，可以啟用以下功能：XL交換機是線路中的最後一個交換機，並且只在兩個位置連線到核心。如果XL交換機的架構採用菊花鏈方式，請不要實施此功能。

您無需使用RSTP或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。環路防護可保護第2層網路，防止由於網路介面故障、CPU繁忙或任何阻止BPDU正常轉發的因素而出現的環路。當冗餘拓撲中的阻塞埠錯誤地轉換到轉發狀態時，會建立STP環路。發生這種情況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如此。其思想是，在點對點鏈路上，如果不傳送下級BPDU或關閉鏈路，指定的網橋就無法消失。STP環路防護功能在適用於Catalyst 6500的Catalyst Cisco IOS軟體版本12.1(13)E和適用於Catalyst 4500交換器的Cisco IOS軟體版本12.1(9)EA1中匯入。

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），直到它再次開始接收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。通過這種方式，恢復是自動的。

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。環路防護可防止使用中的STP版本速度的STP環路。不依賴STP本身（802.1D或802.1w）或調整STP計時器時。出於這些原因，思科建議在依賴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-SP-2-LOOPGUARD_BLOCK: Loop guard blocking port GigabitEthernet2/1 on VLAN0010
```

在處於環路不一致STP狀態的埠上收到BPDU後，該埠會轉換到另一個STP狀態。根據收到的BPDU，這意味著恢復是自動的，無需干預。復原後，系統會記錄以下訊息：

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

與其他STP功能的互動

根防護

根防護會強制始終指定埠。環路防護僅在埠是根埠或備用埠時有效，這意味著它們的功能是互斥的。因此，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。如果環路防護使根埠進入阻塞狀態，則UplinkFast會將新的根埠置於轉發狀態。此外，UplinkFast不會選擇環路*不一致的端*口作為根埠。

BackboneFast

環路防護與BackboneFast相容。BackboneFast是通過接收來自指定網橋的下級BPDU來觸發的。由於從該鏈路接收BPDU，因此環路防護不會啟動。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的連線埠不是根/備用連線埠，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，以便形成通道。在EtherChannel上設定回圈防護時，請注意以下警告：

- 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。
- 如果一組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，並且新的通道埠可能獲得具有指定角色的轉發狀態。
- 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，單個物理埠也可能達到指定角色的轉發狀態。

在最後兩種情況下，在UDLD檢測到故障之前，可能會出現環路。但環路防護無法檢測到它。

環路防護和UDLD功能比較

環路防護和UDLD功能部分重疊，部分重疊部分是為了防止單向鏈路導致的STP故障。這兩種功能在解決問題的方法和功能上均有所不同。具體而言，UDLD無法檢測某些特定的單向故障，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建立以來一直為單向鏈路的情況下不起作用。如果連結自連結以來一直為單向的連結，則連線埠永遠不會收到BPDU且會成為指定連線埠。這可能是正常行為，因此環路防護不會覆蓋此特定情況。UDLD確實針對這種情況提供保護。

啟用UDLD和環路防護可提供最高級別的保護。有關環路防護和UDLD之間功能比較的詳細資訊，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的環路防護與單向鏈路檢測部分
- 本檔案的UDLD一節

思科建議

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。您可以在所有埠上全域性啟用環路防護。實際上，所有點對點鏈路都啟用了此功能。點對點連結會透過連結的雙工狀態來檢測。如果雙工為全雙工，則鏈路視為點對點。

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

其他選項

對於不支援全域性環路防護配置的交換機，建議在所有單個埠（包括埠通道埠）上啟用該功能。儘管在指定埠上啟用環路防護沒有任何好處，但不要認為啟用是一個問題。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。

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

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。如果構建無環拓撲並希望避免網路隔離問題，可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。

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

或

```
Switch(config)#interface type slot#/port#
Switch(config-if)#no spanning-tree guard loop
!--- This is the interface 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。根防護在非常早期的Cisco IOS軟體版本12.1E及更高版本中可用。

操作概述

根防護是STP內建機制。根防護沒有自己的計時器，僅依賴接收BPDU。對連線埠套用根防護時，會拒絕此連線埠成為根連線埠的可能性。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。此系統日誌消息說明：

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

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。此系統日誌消息顯示轉換：

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

恢復是自動進行的。無需人為干預。

由於根防護強制埠被指定，而環路防護僅在埠是根埠或備用埠時才有效，因此這些功能是互斥的。因此，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。

思科建議

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。要配置根防護，請在介面配置模式下使用以下命令：

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

乙太通道

目的

EtherChannel包含幀分配演算法，可高效地將幀多路複用到元件10/100 Mbps或Gigabit鏈路上。幀分配演算法允許將多個通道反向複用到單個邏輯鏈路中。雖然每個平台在實施時與下一個平台不同，但您必須瞭解以下常見屬性：

- 必須存在一種演算法，用於在多個通道上統計多路複用幀。在Catalyst交換器中，這是與硬體相關的。以下是範例：Catalyst 5500/5000 — 模組上存在或缺少乙太網路套件組合晶片(EBC)Catalyst 6500/6000s — 可進一步讀取幀並按IP地址多路複用的演算法
- 通過建立邏輯通道，可以運行單個STP例項或利用單個路由對等，這取決於它是第2層還是第3層EtherChannel。
- 有一個管理協定用於檢查鏈路兩端的引數一致性，並幫助管理鏈路故障或新增後的捆綁恢復。此通訊協定可以是PAgP或連結彙總控制通訊協定(LACP)。

操作概述

EtherChannel包含幀分配演算法，可高效地將幀多路複用到元件10/100 Mbps、Gigabit或10 Gigabit鏈路中。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，該演算法不會導致作為任何給定會話一部分的幀的錯誤排序或幀重複。

下表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 3750系列	執行Cisco IOS軟體負載均衡演演算法的Catalyst 3750，此演演算法使用MAC位址或IP位址、訊息來源或訊息目的地，或兩者都使用。
Catalyst 4500系列	執行Cisco IOS軟體負載均衡演演算法的Catalyst 4500，使用MAC位址、IP位址或第4層(L4)連線埠號碼，以及訊息來源或訊息目的地，或兩者都使用。
C	有兩種雜湊演算法可以使用，取決於Supervisor

atalyst 6500/6000系列	Engine硬體。雜湊是一個在硬體中實現的十七次多項式。在任何情況下，雜湊都會獲取MAC、IP地址或IP TCP/UDP埠號，並應用演算法以生成3位值。對於SA和DA，此過程分別進行。然後與結果一起使用XOR操作以生成另一個3位值。該值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，最多可以是八個連線埠。

下表說明各種Catalyst 6500/6000 Supervisor Engine型號所支援的發佈方法。該表還顯示了預設行為：

硬體	說明	分佈方法
WS-F6020A（第2層引擎）WS-F6K-PFC（第3層引擎）	更高版本的Supervisor引擎I和Supervisor引擎IA管理引擎IA/策略功能卡1(PFC1)	第2層MAC:SA;DA;SA和DA第3層IP:SA;DA;SA和DA（預設）
WS-F6K-PFC 2	Supervisor引擎II/PFC2	第2層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和D埠
WS-F6K-PFC3A WS-F6K-PFC3B WS-F6K-PFC3BXL	Supervisor Engine 720/PFC3A Supervisor Engine 720/Supervisor Engine 32/PFC3B Supervisor Engine 720/PFC3BXL	第2層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和D埠

注意：在第4層分發中，第一個分段的資料包使用第4層分發。所有後續資料包都使用第3層分佈。

註：請參閱以下文檔，以瞭解更多有關其他平台上的EtherChannel支援，以及如何配置和排除EtherChannel故障的詳細資訊：

- 瞭解 Catalyst 交換器上的 EtherChannel 負載平衡和備援
- 配置第3層和第2層EtherChannel（Catalyst 6500系列Cisco IOS軟體配置指南，12.2SX）
- 配置第3層和第2層EtherChannel（Catalyst 6500系列Cisco IOS軟體配置指南，12.1E）
- 設定EtherChannel(Catalyst 4500系列交換器Cisco IOS軟體組態設定指南12.2(31)SG)
- 設定EtherChannel(Catalyst 3750交換器軟體組態設定指南12.2(25)SEE版)
- 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。

思科建議

Catalyst 3750、Catalyst 4500和Catalyst 6500/6000系列交換器預設會對來源IP位址和目的地IP位址進行雜湊處理，藉此執行負載平衡。建議這樣做，並假設IP是主要的協定。發出以下命令以設定負載平衡：

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

其他選項

根據流量流，如果大多數流量位於同一源IP地址和目標IP地址之間，則可以使用第4層分佈來改進負載均衡。您必須瞭解，當配置第4層分佈時，雜湊僅包括第4層源埠和目的埠。它不會將第3層IP地址合併到雜湊演算法中。發出以下命令以設定負載平衡：

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

注意：Catalyst 3750系列交換機上無法配置第4層分佈。

發出**show etherchannel load-balance**命令以檢查幀分配策略。

根據硬體平台的不同，您可以使用CLI命令確定EtherChannel中的哪個介面轉發特定流量，並根據幀分配策略進行轉發。

若是Catalyst 6500交換器，請發出**remote login switch**指令，以遠端登入交換器處理器(SP)主控台。然後，發出**test etherchannel load-balance interface** ***port-channel number*** {ip | **l4port | mac}** **[*source_ip_add* |** *source_mac_add* **|** *source_l4_port***] [***dest_ip_add* **|** *dest_mac_add* **|** *dest_l4_port*]**命令。

若是Catalyst 3750交換器，發出**test etherchannel load-balance interface** ***port-channel number*** {ip **| mac} [*source_ip_add* |** *source_mac_add***] [***dest_ip_add* **|** *dest_mac_add*]**命令。

對於Catalyst 4500，等效命令不可用。

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。完成這些准則和限制以避免捆綁問題。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。對於執行Cisco IOS軟體的Catalyst 6500交換器，可以使用**no mls qos channel-consistency** port-channel interface指令停用EtherChannel套件組合上的QoS連線埠屬性檢查。**show interface capability** ***mod/port*** 命令顯示QoS埠功能並確定埠是否相容。

請參閱不同平台的以下准則，以避免組態問題：

- 配置第3層和第2層EtherChannel（Catalyst 6500系列Cisco IOS軟體配置指南，12.2SX）
- 配置第3層和第2層EtherChannel（Catalyst 6500系列Cisco IOS軟體配置指南，12.1E）
- 設定EtherChannel(Catalyst 4500系列交換器Cisco IOS軟體組態設定指南12.2(31)SG)
- 設定EtherChannel(Catalyst 3750交換器軟體組態設定指南12.2(25)SEE版)

支援的最大EtherChannel數量也取決於硬體平台和軟體版本。執行Cisco IOS軟體版本

12.2(18)SXE和更新版本的Catalyst 6500交換器最多支援128連線埠通道介面。低於Cisco IOS軟體版本12.2(18)SXE的軟體版本最多支援64連線埠通道介面。無論軟體版本如何，可配置的組編號可以是1到256。Catalyst 4500系列交換器最多支援64個EtherChannel。若是Catalyst 3750交換器，建議不要在交換器堆疊上設定超過48個EtherChannel。

生成樹連線埠成本計算

您必須瞭解EtherChannel的跨距樹狀目錄連線埠成本計算。您可以使用short或long方法計算EtherChannel的跨距樹狀目錄連線埠成本。預設情況下，埠成本在短模式下計算。

下表說明第2層EtherChannel的跨距樹狀目錄連線埠成本（基於頻寬）：

頻寬	舊STP值	新的長STP值
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1 Gbps	4	20,000
N X 1 Gbps	3	6660
10 Gbps	2	2,000
100 Gbps	不適用	200
1 Tbps	不適用	20
10 Tbps	不適用	2

註：在 CatOS中，在連線埠通道成員連結失敗後，EtherChannel的跨距樹狀目錄連線埠成本會保持不變。在Cisco IOS軟體中，EtherChannel的連線埠成本會立即更新，以反映新的可用頻寬。如果要避免不必要的生成樹拓撲更改，可以使用**spanning-tree cost** 命令靜態配置生成樹埠開銷。

連線埠彙總通訊協定(PAgP)

目的

PAgP是在鏈路兩端檢查引數一致性的管理協定。PAgP還幫助通道適應鏈路故障或新增。以下是PAgP的特徵：

- 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EtherChannel參與中不包括動態VLAN。
- 如果套件組合已存在，且修改了連線埠的組態，則會修改套件組合中的所有連線埠以與該組態相符。例如VLAN更改或中繼模式改。
- 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。用於CDP資料包的同一組播組MAC地址用於傳送PAgP資料包。MAC地址為01-00-0c-cc-cc-cc。但是，協定值為0x0104。以下是協定操作的摘要：

- 只要物理埠處於開啟狀態，PAgP資料包就會在檢測期間每秒傳輸一次，而在穩定狀態下則每30秒傳輸一次。
- 如果接收到資料包但沒有收到PAgP資料包，則假定埠連線到不支援PAgP的裝置。
- 偵聽PAgP資料包以證明物理埠與另一個支援PAgP的裝置具有雙向連線。

- 在一組實體連線埠上收到兩個此類封包後，嘗試形成聚合連線埠。
- 如果PAgP資料包停止一段時間，則PAgP狀態會被斷開。

正常處理

這些概念有助於演示協定的行為：

- Agport — 由同一聚合中的所有物理埠組成的邏輯埠，可由其自己的SNMP ifIndex標識。Agport不包含非運行埠。
- 通道 — 滿足形成條件的聚合。通道可以包含非運行埠，並且是agport的超集。包括STP和VTP但不包括CDP和DTP的協定通過agport運行在PAgP之上。在PAgP將agport連線到一個或多個物理埠之前，這些協定都無法傳送或接收資料包。
- 組功能 — 每個物理埠和agport都具有一個稱為group-capability的配置引數。物理埠可以與具有相同group-capability的任何其他物理埠聚合，並且只能與此類物理埠聚合。
- 聚合過程 — 當物理埠達到UpData或UpPAgP狀態時，該埠會連線到相應的agport。當連線埠從其中任一種狀態轉為另一狀態時，連線埠會從agport分離。

下表提供了有關狀態的更多詳細資訊：

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達成一致。該分組被定義為連線兩端都允許的agport中的最大埠組。

當實體連線埠達到UpPAgP狀態時，會將連線埠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group-capability相符，且處於BiDir狀態或UpPAgP狀態。任何此類BiDir埠都會同時移動到UpPAgP狀態。如果沒有具有與新就緒物理埠相容的構成物理埠引數的agport，則將該埠分配給具有適當引數的無關聯物理埠的agport。

物理埠上已知的最後一個鄰居可能發生PAgP超時。超時埠將從agport中刪除。同時，將刪除同一agport上所有具有已逾時的計時器的物理埠。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

如果存在通道中的連結失敗，agport就會更新，且流量會在保留但不會丟失的連結上雜湊。此類故障的示例包括：

- 埠已拔出
- 已移除Gigabit介面轉換器(GBIC)
- 光纖已損壞

注意：關閉或移除模組後，通道中的連結發生失敗時，行為可能會有所不同。根據定義，通道需要兩個實體連線埠。如果系統在兩個埠通道中丟失了一個埠，則邏輯agport將關閉，並且原始物理埠將相對於生成樹重新初始化。流量可能會被丟棄，直到STP允許埠再次對資料可用。

規劃網路維護時，這兩種故障模式的差異非常重要。可能會出現STP拓撲更改，在執行模組線上刪除或插入時需要考慮這些更改。您必須使用網路管理系統(NMS)管理通道中的每個實體連結，因為agport可以不受故障干擾。

完成以下建議之一，以緩解Catalyst 6500/6000上不需要的拓撲更改：

- 如果每個模組使用一個埠以形成通道，請使用三個或更多模組（總共三個）。
- 如果通道跨兩個模組，則在每個模組上使用兩個埠（共4個）。
- 如果兩個卡之間需要雙埠通道，則僅使用Supervisor Engine埠。

組態選項

您可以在不同的模式下配置EtherChannel，如下表總結：

模式	可設定選項
	PAgP未運行。埠通道，無論相鄰埠的配置方式如何。如果相鄰埠模式為 `on`，則會形成通道。
	聚合由PAgP控制。埠被置於被動協商狀態。在至少收到一個PAgP資料包指示傳送方在`desirable`模式下運行之前，不會在介面上傳送PAgP資料包。
`Desirable`	聚合由PAgP控制。埠被置於活動協商狀態，在該狀態下，埠通過PAgP資料包的傳輸發起與其他埠的協商。在`desirable`或`auto`模式下與另一個埠組形成通道。
`Non-silent` Catalyst 5500/5000光纖FE和GE埠上這是預設設定。	`auto`或`desirable`模式關鍵字。如果介面上未收到資料包，則該介面從未連線到agport，並且不能用於資料。之所以為特定Catalyst 5500/5000硬體提供此雙向檢查，是因為某些連結失敗會導致通道中斷。啟用非時，從不允許恢復的鄰居埠重新開啟並且不必要地斷開通道。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。
這是所有Catalyst 6500/6000和4500/4000埠以及5500/5000銅纜埠的預設值。	`auto`或`desirable`模式關鍵字。如果介面上未收到資料包，在15秒超時時間後，該介面將單獨連線到agport。因此，該介面可用於資料傳輸。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設定影響埠對導致單向流量的情況做出反應。當連線埠因為實體介面發生故障或光纖或纜線中斷而無法傳輸時，鄰近連線埠仍然可以保持使用狀態。合作夥伴繼續傳輸資料。但是，由於無法接收返回流量，資料將會丟失。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)時使該連線埠進入非營運狀態。 此操作會導致夥伴埠變為非操作狀態，並有效地導致鏈路兩端的埠關閉。

使用傳輸資料(BPDU)的裝置且無法檢測單向條件時，請使用non-silent模式，以允許埠保持非運行狀態，直到收到資料並且鏈路驗證為雙向。PAgP檢測單向鏈路的時間大約為3.5 * 30秒= 105秒。30秒是兩個連續PAgP消息之間的時間。使用UDLD，它是單向連結的更快速偵測器。

使用不傳輸任何資料的裝置時，請使用silent模式。無論接收的資料是否存在，使用silent模式都會強制埠連線並運行。此外，對於那些可以檢測存在單向條件的埠，預設情況下會使用silent模式。這些連線埠的範例是使用第1層FEFI和UDLD的較新平台。

若要關閉介面上的通道化，請發出命令no channel-group *number*.

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

驗證

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PAgP通道模式方案。其中某些組合可能會導致STP將通道化端的埠置於errDisable狀態，這意味著這些組合會關閉通道化端的埠。EtherChannel組態錯誤防護功能預設會啟用。

切換通道模式	交換器B通道模式	切換通道狀態	交換機B的通道狀態
於	於	通道（非PAgP）	通道（非PAgP）
於	未配置	Not Channel（錯誤停用）	非通道
於	自動	Not Channel（錯誤停用）	非通道
於	Desirable	Not Channel（錯誤停用）	非通道
未配置	於	非通道	Not Channel（錯誤停用）
未配置	未配置	非通道	非通道
未配置	自動	非通道	非通道
未配置	Desirable	非通道	非通道
自動	於	非通道	Not Channel（錯誤停用）
自動	未配置	非通道	非通道
自動	自動	非通道	非通道

自動	Desirable	PAgP通道	PAgP通道
Desirable	於	非通道	非通道
Desirable	未配置	非通道	非通道
Desirable	自動	PAgP通道	PAgP通道
Desirable	Desirable	PAgP通道	PAgP通道

適用於L2通道的思科組態建議

在所有EtherChannel鏈路上啟用PAgP並使用desirable-desirable設定。如需詳細資訊，請參閱以下輸出：

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

透過以下方式驗證設定：

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

防止EtherChannel配置錯誤

您可能會錯誤配置EtherChannel並建立生成樹環路。這種組態錯誤可能會使交換器流程不堪重負。Cisco IOS系統軟體包括**spanning-tree etherchannel guard misconfig**功能以便防止此問題。

在作為系統軟體執行Cisco IOS軟體的所有Catalyst交換器上發出此組態命令：

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

其他選項

當對不支援PAgP但支援LACP的兩台裝置進行通道化時，建議啟用兩端均處於活動狀態的LACP。有關詳細資訊，請參閱本文檔的鏈路聚合控制協定(LACP)部分。

當通道連線到不支援PAgP或LACP的裝置時，必須將通道硬編碼為on。此要求適用於以下範例裝置：

- 伺服器
- 本地導向器
- 內容交換機
- 路由器
- 具有早期軟體的交換器
- Catalyst 2900XL/3500XL交換器
- Catalyst 8540s

發出以下命令：

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

連結彙總控制通訊協定(LACP)

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Cisco專有的協定，您只能在Cisco交換機和許可供應商發佈的交換機上運行。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。

以下平台和版本支援LACP:

- 採用Cisco IOS軟體版本12.1(11b)EX和更新版本的Catalyst 6500/6000系列
- 採用Cisco IOS軟體版本12.1(13)EW和更新版本的Catalyst 4500系列
- 採用Cisco IOS軟體版本12.1(14)EA1和更新版本的Catalyst 3750系列

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，並在形成套件組合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和中繼型別

LACP與PAgP的顯著區別是：

- LACP通訊協定只能在全雙工連線埠上執行，且不支援半雙工連線埠。
- LACP協定支援熱備用埠。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（例如，如果遠端系統具有更嚴格的硬體限制），則無法主動包含在通道中的所有埠將進入熱備用狀態，並且僅當其中一個已使用的埠出現故障時才使用。

注意：對於Catalyst 4500系列交換機，可以為其分配相同管理金鑰的最大埠數為8。對於執行Cisco IOS軟體的Catalyst 6500和3750交換器，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控制每個要捆綁的物理埠（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。在每個可聚合鏈路上定期傳送傳輸。
- 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，並決定採取何種操作。
- 在通道中設定相容的連線埠，最多為硬體允許的最大值（八個連線埠）。
- 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，如果狀態資訊發生變化，該協定將事件驅動的LACPDU傳輸給夥伴。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：

- 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(預設優先順序為32768)，也可以由管理員選擇。系統優先順序主要用於與系統的MAC地址結合使用以形成系統識別符號。
- 一種標識與給定系統所理解的與每個埠和每個聚合器相關聯的功能集的方法。系統中的每個埠必須自動分配優先順序（預設優先順序為128）或由管理員分配。優先順序與埠號結合使用以形成埠識別符號。
- 一種標識鏈路聚合組及其關聯聚合器的方法。埠與另一個埠聚合的能力是由一個嚴格大於零的簡單的16位整數引數（稱為金鑰）總結的。每個金鑰根據不同的因素確定，例如：埠物理特性，包括資料速率、雙工和點對點或共用介質網路管理員建立的配置限制每個連線埠有兩個相關的金鑰：管理金鑰操作金鑰管理金鑰允許管理操作金鑰值，因此，使用者可以選擇此金鑰。系統使用操作金鑰來形成聚合。使用者無法直接選擇或更改此金鑰。給定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。

因此，如果給定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從最高優先順序系統中的最高優先順序埠開始聚合埠。此行為是可能的，因為每個系統都知道以下優先順序：

- 其自己的優先順序，由使用者或軟體分配
- 其合作夥伴優先順序，通過LACP資料包發現

失敗時的行為

LACP的故障行為與PAgP的故障行為相同。如果現有通道中的鏈路發生故障（例如，如果埠被拔出、GBIC被移除，或者光纖被破壞），則agport會被更新，並在1秒內將流量雜湊到其餘鏈路上。任何在故障發生後不需要重新雜湊的流量（即繼續在同一鏈路上傳送的流量）都不會受到任何損失。恢復出現故障的鏈路會觸發對agport的另一次更新，流量將再次雜湊。

組態選項

您可以在不同的模式下配置LACP EtherChannel，如下表所示：

模式	可設定選項
於	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。
關閉（或）未配置	無論鄰居是如何配置的，埠都不會進行通道化。
被動（預設）	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（處於活動狀態）發起協商（通過傳送LACP資料包），交換機會接收該協商並回覆，最終與對等體形成聚合通道。
Active	這類似於PAgP中的**desirable**模式。交換器啟動交涉以形成聚合連結。如果另一端以LACP主動或被動模

（作用中）	式運行，則會形成鏈路聚合。

在建立LACP EtherChannel後，LACP會使用30秒間隔計時器(Slow_Periodic_Time)。使用較長超時（Slow_Periodic_Time的3倍）時，收到的LACPDU資訊失效之前的秒數是90。建議使用UDLD作為更快速的單向鏈路檢測器。您無法調整LACP計時器，此時您無法將交換機配置為使用快速協定資料單元(PDU)傳輸（每秒）以便在通道形成後保持通道。

驗證

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EtherChannel防護將通道端上的連線埠進入錯誤停用狀態。EtherChannel組態錯誤防護功能預設會啟用。

切換通道模式	交換器B通道模式	切換通道狀態	交換機B的通道狀態
於	於	通道（非LACP）	通道（非LACP）
於	Off	Not Channel（錯誤停用）	非通道
於	被動	Not Channel（錯誤停用）	非通道
於	Active（作用中）	Not Channel（錯誤停用）	非通道
Off	Off	非通道	非通道
Off	被動	非通道	非通道
Off	Active（作用中）	非通道	非通道
被動	被動	非通道	非通道
被動	Active（作用中）	LACP通道	LACP通道
Active（作用中）	Active（作用中）	LACP通道	LACP通道

思科建議

思科建議您對思科交換機之間的通道連線啟用PAgP。當對不支援PAgP但支援LACP的兩台裝置進行通道化時，建議啟用兩端均處於活動狀態的LACP。

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使用PAgP通道通訊協定。為了將埠配置為使用LACP，必須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。此限制不適用於執行Cisco IOS軟體的交換器。運行Cisco IOS軟體的交換機可以在同一模組上支援PAgP和LACP。發出以下命令，以將

LACP通道模式設定為活動狀態，並分配管理金鑰編號：

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

show etherchannel summary命令會顯示每個通道組的一行摘要，其中包括以下資訊：

- 組編號
- 埠通道號
- 連線埠的狀態
- 作為通道一部分的連線埠

show etherchannel port-channel命令會顯示所有通道組的詳細連線埠通道資訊。輸出包括以下資訊：

- 通道的狀態
- 使用的協定
- 自埠捆綁後的時間

若要顯示特定通道組的詳細資訊，並分別顯示每個連線埠的詳細資訊，請使用**show etherchannel** ***channel_number***命令。命令輸出包括合作夥伴詳細資訊和埠通道詳細資訊。如需詳細資訊，請參閱在Catalyst 6500/6000和Catalyst 4500/4000之間設定LACP(802.3ad)。

其他選項

對於不支援PAgP或LACP的通道裝置，必須將通道硬編碼為on。此要求適用於以下裝置：

- 伺服器
- 本地導向器
- 內容交換機
- 路由器
- 使用舊版軟體的交換器
- Catalyst 2900XL/3500XL交換器
- Catalyst 8540s

發出以下命令：

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

單向連結偵測

目的

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。還有其他檢測傳輸介質雙向狀態的方法，例如FEFI。但是，有些情況下，第1層檢測機制是不夠的。這些情況可能導致：

- STP的不可預測操作
- 資料包的泛洪錯誤或過多
- 交通黑洞

UDLD功能可解決光纖和銅纜乙太網介面上的以下故障情況：

- 監控物理佈線配置 — 以errDisabled關閉任何有線錯誤埠。
- 防止單向鏈路 — 當檢測到由於介質或埠/介面故障而發生的單向鏈路時，受影響的埠將以errDisabled關閉。生成相應的系統日誌消息。
- 此外，UDLD主動模式會檢查先前認為的雙向鏈路在鏈路因擁塞而變得不可用時不會失去連線。UDLD主動模式通過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正常模式UDLD無法處理的故障情況下對流量進行黑洞。

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。

跨距樹狀目錄具有穩態的單向BPDU流，並且可能會出現本節列出的故障。埠可能突然無法傳輸BPDU，從而導致鄰居的STP狀態從blocking更改為forwarding。但是，由於連線埠仍能接收，因此循環仍然存在。

操作概述

UDLD是工作在LLC層之上的第2層協定（目標MAC 01-00-0c-cc-cc-cc，SNAP HDLC協定型別0x0111）。 當您結合運行UDLD和FEFI以及自動協商第1層機制時，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。這些功能包括:

- 鄰居資訊的檢測與快取
- 關閉任何連線不當的埠
- 檢測非點對點鏈路上的邏輯介面/埠故障或故障**注意：**當鏈路不是點對點時，它們會通過媒體轉換器或集線器。

UDLD使用這兩種基本機制。

1. UDLD會瞭解鄰居，並在本地快取中保持資訊最新。
2. UDLD會在偵測到新鄰居時或每當鄰居要求重新同步快取時，傳送一系列UDLD探測/回應(hello)訊息。

UDLD會持續在所有連線埠上傳送探測/回應訊息。在埠上接收相應的UDLD消息時，觸發檢測階段和驗證過程。如果滿足所有有效條件，則啟用埠。如果埠是雙向的，並且正確佈線，則滿足這些條件。如果不滿足條件，則埠為errDisabled，它會觸發此系統日誌消息：

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

有關按設施分類的系統消息的完整清單（包括UDLD事件），請參閱UDLD消息（Cisco IOS系統消息，第2卷，共2卷）。

在建立鏈路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/回應消息。

下表提供有關埠狀態的資訊：

埠狀態	意見
未確定	檢測正在進行/相鄰UDLD已禁用。
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。

鄰居快取維護

UDLD會在每個作用中介面上定期傳送hello探測/回應封包，以維護UDLD鄰居快取的完整性。在收到hello消息時，消息被快取並儲存在記憶體中一個最大時段，該時段定義為保持時間。當保持時間到期時，相應的快取記憶體條目老化。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。

每當啟用UDLD的介面被禁用或裝置被重置時，配置更改影響的所有現有快取條目都會被清除。此清除維護UDLD快取的完整性。UDLD傳輸至少一則訊息，以通知各自的鄰居需要刷新對應的快取專案。

回聲檢測機制

回波機制是檢測演算法的基礎。每當UDLD裝置得知新鄰居或收到不同步鄰居的重新同步要求時，裝置都會在連線其側啟動或重新啟動偵測視窗，並傳送一連串回應訊息來回覆。由於所有鄰居的這種行為必須相同，因此回應要求回顯傳送方接收回顯。如果檢測視窗結束時未收到任何有效應答消息，則鏈路被視為單向鏈路。此時，可能會觸發鏈路重建或埠關閉過程。裝置檢查的其他罕見異常情況包括：

- 環回傳輸(Tx)光纖到同一埠的Rx聯結器
- 共用介質互聯（例如集線器或類似裝置）情況下的連線錯誤

收斂時間

為了防止STP環路，Cisco IOS軟體版本12.1和更新版本將UDLD預設訊息間隔從60秒縮短至15秒。更改此間隔是為了在802.1D生成樹中以前被阻塞的埠能夠轉換到轉發狀態之前關閉單向鏈路。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，會將配置的消息間隔傳送到鄰居，該對等體的超時間隔計算為：

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

因此，在丟失三個連續的hello（或探測）之後，對等關係超時。因為消息間隔在每一端上是不同的，所以此超時值在每一端上也是不同的，並且有一端可更快速地識別故障。

UDLD檢測先前穩定的鏈路的單向故障大約需要時間：

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

這大約為41秒，預設消息間隔為15秒。此時間量遠小於STP重新收斂通常所需的50秒。如果NMP CPU有一些空閒週期，並且使用者仔細監控其使用級別（一種很好的做法），將消息間隔（偶數）減少到至少7秒是可以接受的。此外，此消息間隔縮短有助於以顯著因素加快檢測速度。

註：Cisco IOS軟體版本12.2(25)SEC中的最小值為1秒。

因此，UDLD預設依賴於預設跨距樹狀目錄計時器。如果STP經過調整後收斂速度比UDLD更快，請考慮替代機制，例如STP環路防護功能。在這種情況下，當您實施RSTP(802.1w)時，也考慮另一種機制，因為RSTP的收斂特性以ms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，以提供最大的保護。環路防護可防止使用中的STP版本速度的STP環路。此外，UDLD會負責檢測單個EtherChannel連結上的單向連線，或在BPDU不沿中斷方向流動的情況下進行檢測。

注意：UDLD獨立於STP。UDLD不會捕獲每個STP故障情況，例如那些由CPU導致的故障，該CPU在大於(2 * Fwddelay + maxage)的時間段內不傳送BPDU。 因此，Cisco建議您在依賴STP的拓撲中將UDLD與環路防護結合實施。

注意：請注意2900XL/3500XL交換器中的早期版本UDLD使用不可設定的60秒預設訊息間隔。它們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：

- UDLD PDU的丟失是對稱的，兩端都會超時。在這種情況下，兩個連線埠都不會錯誤停用。
- 連結的一端連線埠停滯（Tx和Rx）。
- 連結的一端保持開啟狀態，而連結的另一端已關閉。
- 已停用自動交涉或其他第1層故障偵測機制。
- 希望降低對第1層FEFI機制的依賴。
- 您需要針對點對點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攻擊型探測器可以視為心跳，其存在可保證鏈路的正常運行。

實施UDLD主動型的最常見情況是在禁用或無法使用自動協商或其他第1層故障檢測機制時，對捆綁的成員執行連線檢查。它對於EtherChannel連線特別有用，因為PAgP和LACP（即使已啟用）在穩定狀態下不使用非常低的hello計時器。在這種情況下，UDLD主動性還有額外的優勢，可防止可能的生成樹環路。

必須瞭解，UDLD正常模式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是用來偵測引起STP回圈的第2層問題，而這些問題通常是單向的（因為在穩定狀態下，BPDU僅沿一個方向流動）。 因此，將UDLD正常模式與自動協商和環路防護結合使用（對於依賴STP的網路）幾乎總是足夠的。啟用UDLD主動模式後，在通告或檢測階段中，連線埠的所有鄰居都已老化後，UDLD主動模式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。如果連線經過一連串快速訊息（八個重試失敗）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。這被認為速度不夠快，無法防止潛在的STP環路（假定使用預設STP引數）。

UDLD連結的自動復原

錯誤停用復原功能預設會全域停用。全域性啟用後，如果連線埠進入錯誤停用狀態，就會在選定的時間間隔後自動重新啟用。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。如果您使用針對UDLD的錯誤停用逾時復原機制將連線埠的錯誤停用逾時設定為停用，就可以手動禁止連線埠重新啟用，視軟體版本而定：

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

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期間的詳細資訊，請參閱**錯誤停用復原**（Catalyst 6500系列Cisco IOS命令參考，12.1 E）。

當存取交換器分散於園區環境，且手動存取每台交換器以重新啟用兩個上行鏈路需要花費大量時間時，錯誤停用復原對於存取層的UDLD尤其重要。

思科不建議在網路核心層進行錯誤停用復原，因為核心層通常有多個輸入點，而核心層中的自動復原可能會導致問題復發。因此，如果UDLD停用連線埠，必須手動重新啟用核心上的連線埠。

路由連結上的UDLD

在本討論中，路由鏈路是以下兩種連線型別之一：

- 兩個路由器節點之間的點對點（配置有30位子網掩碼）
- 具有多個埠但僅支援路由連線的VLAN，例如分割的第2層核心拓撲中

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。本節介紹與本討論相關的特性，這些特性與目前常用的兩種路由協定(開放最短路徑優先(OSPF)協定和增強型IGRP(EIGRP))不同。

注意：任何點對點路由網路上的第1層或第2層故障都會導致第3層連線幾乎立即斷開。由於該VLAN中唯一的交換機埠在第1/第2層出現故障時轉換為未連線狀態，因此介面自動狀態功能可在大約兩秒內同步第2層和第3層埠狀態，並將第3層VLAN介面置於開啟/關閉狀態（線路協定關閉）。

如果假定預設計時器值，OSPF每10秒傳送一次hello消息，並且死間隔為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。即使第1層/第2層故障不是純點對點連線故障，並且第3層協定必須處理的故障情況不完整，情況也是如此。由於UDLD的檢測時間非常類似於OSPF dead計時器到期的檢測時間（約40秒），因此在OSPF第3層點對點鏈路上配置UDLD正常模式的優點有限。

在許多情況下，EIGRP收斂速度比OSPF更快。但必須注意的是，對於鄰居交換路由資訊而言，不需要進行雙向通訊。在非常特定的半固定的故障情形中，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為止。UDLD正常模式可以緩解這些情況，因為它會檢測單向連結失敗並因為錯誤而停用連線埠。

對於使用任何路由協定的第3層路由連線，UDLD正常模式仍可針對初始鏈路啟用時出現的問題（例如佈線錯誤或硬體故障）提供保護。此外，UDLD主動模式在第3層路由連線上提供以下優勢：

- 防止不必要的流量黑洞（某些情況下需要最小計時器）
- 將擺動連結進入錯誤停用狀態
- 防止第3層EtherChannel配置導致的環路

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。由於UDLD是僅交換機之間需要的基礎架構協定，因此，銅纜埠上預設禁用UDLD（通常用於主機訪問）。請注意，您必須先在介面級別全域性啟用UDLD，鄰居才能達到雙向狀態。預設消息間隔為15秒。但是，在某些情況下，預設消息間隔可以顯示為7秒。如需詳細資訊，請參閱Cisco錯誤ID CSCea70679 (僅限註冊客戶)。預設消息間隔可在7到90秒之間配置，並且禁用UDLD主動模式。Cisco IOS軟體版本12.2(25)SEC進一步將此最小計時器減少為一秒。

思科組態建議

在絕大多數情況下，思科建議您在思科交換機之間的所有點對點FE/GE鏈路上啟用UDLD正常模式，並在使用預設802.1D生成樹計時器時，將UDLD消息間隔設定為15秒。此外，如果網路依靠STP實現冗餘和收斂（這意味著拓撲中存在一個或多個處於STP阻塞狀態的埠），請結合適當的功能和協定使用UDLD。這些功能包括FEFI、自動協商、環路防護等。通常，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第1層的故障檢測。

發出以下兩個命令選項之一以啟用UDLD:

註：語法在不同平台/版本之間已更改。

-

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

或

-

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

您必須手動啟用由於單向連結症狀而關閉的連線埠。使用以下方法之一：

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

errdisable recovery cause udld和**errdisable recovery interval** interval全域性配置命令可用於自動從UDLD錯誤停用狀態中復原。

如果對交換器的實體存取有困難，思科建議只在網路的存取層使用錯誤停用復原機制，復原計時器應不少於20分鐘。最佳情況是在連線埠重新連線並造成網路不穩定之前，為網路穩定和疑難排解留出時間。

思科建議您不要在網路的核心層使用*恢復機制*，因為這樣會導致每次重新開啟故障鏈路時與收斂事件相關的不穩定性。核心網路的冗餘設計為故障鏈路提供備用路徑，並留出時間調查UDLD故障原因。

使用不帶STP環路防護的UDLD

對於具有無環路STP拓撲的第3層點對點或第2層鏈路（無埠阻塞），Cisco建議您在思科交換機之間的點對點FE/GE鏈路上啟用主動UDLD。在這種情況下，消息間隔設定為7秒，802.1D STP使用預設計時器。

EtherChannel上的UDLD

無論是否部署了STP環路防護，都建議對任何EtherChannel配置使用UDLD主動模式，同時使用desirable channel模式。在EtherChannel配置中，如果通道鏈路分離，則傳送跨距樹狀目錄BPDU和PAgP控制流量的通道鏈路出現故障可能會導致通道夥伴之間立即出現環路。UDLD主動模

式關閉故障埠。然後，PAgP（自動/期望通道模式）可以協商新的控制鏈路並有效地從通道中消除故障鏈路。

採用802.1w生成樹的UDLD

為了在使用較新的生成樹版本時防止環路，請使用UDLD正常模式和STP環路防護與RSTP（如802.1w）配合使用。UDLD可以在連結階段提供針對單向連結的保護，而STP回圈防護可以在UDLD將連結設定為雙向之*後，連結變成單向時，防止*STP回圈。由於不能將UDLD配置為小於預設802.1w計時器，因此STP環路防護對於完全防止冗餘拓撲中的環路是必需的。

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。

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(例如拔掉一股光纖以檢視所需的`errdisable`狀態)，則需要首先關閉第1層自動協商。否則，實體連線埠會關閉，這會重設UDLD訊息通訊。遠端在UDLD正常模式下移至`undetermined`狀態，並僅在使用UDLD主動模式的情況下移至錯誤停用狀態。

另一種測試方法模擬UDLD的鄰居PDU丟失。此方法使用MAC層過濾器來封鎖UDLD/CDP硬體位址，同時允許其他位址通過。當連線埠設定為交換連線埠分析器(SPAN)目的地（模擬不回應的UDLD鄰居）時，某些交換器不會傳送UDLD訊框。

若要監控UDLD，請使用以下命令：

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

此外，在Cisco IOS軟體版本12.2(18)SXD或更新版本交換器的啟用模式下，您可以發出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快取進行比較以便驗證是否存在協定特定的異常時，通常非常有用。每當CDP也受到影響時，通常意味著所有BPDU/PDU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。

您可以使用Cisco UDLD SNMP MIB變數監控UDLD狀態和配置一致性。

多層交換

概觀

在Cisco IOS系統軟體中，Catalyst 6500/6000系列支援多層交換(MLS)，且僅在內部支援。這表示路由器必須安裝在交換機中。較新版本的Catalyst 6500/6000 Supervisor Engine支援MLS CEF，其中路由表下載到每個卡。這要求額外的硬體，包括存在分散式轉發卡(DFC)。CatOS軟體不支援DFC，即使您選擇在路由器卡上使用Cisco IOS軟體。只有Cisco IOS系統軟體支援DFC。

用於在Catalyst交換機上啟用NetFlow統計資訊的MLS快取是Supervisor Engine I卡和舊版Catalyst交換機用於啟用第3層交換的基於流的快取。預設情況下，在具有MSFC或MSFC2的Supervisor Engine 1（或Supervisor Engine 1A）上啟用MLS。預設MLS功能無需其他MLS配置。您可以在以下三種模式之一中配置MLS快取：

- 目的地
- source-destination
- source-destination port

流量掩碼用於確定交換機的MLS模式。這些資料隨後用於在Supervisor Engine IA調配的Catalyst交換機中啟用第3層流。Supervisor Engine II刀鋒不使用MLS快取來交換封包，因為此卡是硬體CEF啟用，是一項可擴充性高得多的技術。MLS快取保留在Supervisor引擎II卡中，以便僅啟用NetFlow統計匯出。因此，如有必要，可以啟用Supervisor引擎II進行完全流量傳輸，不會對交換機產生負面影響。

組態

MLS老化時間適用於所有MLS快取條目。老化時間值直接應用於目標模式老化。將MLS老化時間值除以二，可匯出源到目標模式的老化時間。將MLS老化時間值除以八，以查詢全流老化時間。預設MLS老化時間值為256秒。

可以以8秒為增量配置正常老化時間，範圍為32到4092秒。任何不是八秒倍數的老化時間值都將調整為最接近的8秒倍數。例如，值65調整為64，值127調整為128。

其他事件可能導致清除MLS條目。此類事件包括：

- 路由更改
- 鏈路狀態的更改例如，PFC鏈路已關閉。

為了將MLS快取大小保持在32,000個條目以下，請在發出**mls aging**命令後啟用這些引數：

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

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

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

組態

刪除的典型快取條目是進出域名伺服器(DNS)或TFTP伺服器的流的條目，該條目在建立後可能再也無法使用。這些條目的檢測和老化為MLS快取中的其他資料流量節省了空間。

如果需要啟用MLS快速老化時間，請將初始值設定為128秒。如果MLS快取的大小繼續增長到32,000個條目以上，請降低設定直到快取大小保持在32,000個條目以下。如果快取繼續增長到32,000個條目，請縮短正常的MLS老化時間。

Cisco建議的MLS配置

將MLS保留為預設值（僅目標），除非需要NetFlow匯出。如果需要NetFlow，請僅在Supervisor引擎II系統上啟用MLS完全流。

發出以下命令以啟用MLS流目標：

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

巨量訊框

最大傳輸單位

最大傳輸單元(MTU)是介面可以傳送或接收的最大資料包或封包大小（以位元組為單位），而不會將封包分段。

根據IEEE 802.3標準，最大乙太網幀大小為：

- **一般訊框**的1518位元組（1500位元組加上18位元組的乙太網路標頭和CRC標尾）
- 802.1Q封裝幀的1522位元組（1518加4位元組標籤）

Baby Giants:Baby Giants功能允許交換器通過/轉送略大於IEEE乙太網路MTU的封包，而不是宣佈訊框過大並捨棄這些封包。

巨量:幀大小的定義取決於供應商，因為幀大小不是IEEE標準的一部分。巨型幀是指大於標準乙太網幀大小（即1518位元組，包括第2層報頭和幀校驗序列[FCS]）的幀。

在單個埠上啟用巨型幀支援後，預設MTU大小為9216位元組。

預期大於1518位元組的資料包的時機

若要在交換網路中傳輸流量，請確保傳輸的流量MTU不超過交換器平台支援的流量。某些訊框的MTU大小可能會被截斷的原因有很多：

- **供應商特定的**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。之所以發生這種變化，是因為研究證明，增加乙太網幀的大小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送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802.1Q
- **多重協定標籤交換(MPLS)** — 在介面上啟用MPLS後，MPLS可能會增加封包的訊框大小，這取決於MPLS標籤封包的標籤堆疊中的標籤數量。標籤的總大小為4位元組。標籤堆疊的總大小為：
  ```
  n * 4 bytes
  ```
  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，通常一次只能有一個標籤對硬體可見。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)/第2層通道通訊協定第3版（第2TPv3）** - UTI/第2層TPv3封裝要透過IP網路轉送的第2層資料。UTI/第2層TPv3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）、第2層TPv3報頭（12位元組）和一個新的第2層報頭。第2層TPv3負載包含完整的第2層幀，其中包括第2層報頭。

目的

基於硬體的高速（1-Gbps和10-Gbps）交換使巨型幀成為解決吞吐量不佳問題的非常具體的解決方案。雖然對於巨型幀大小沒有官方標準，但該欄位通常採用的值是9216位元組(9 KB)。

網路效率注意事項

如果將其負載大小除以開銷值和負載大小之和，則可以計算資料包轉發的網路效率。

即使巨型幀帶來的網路效率提高幅度不大，從94.9%（1500位元組）變為99.1%（9216位元組），網路裝置和終端主機的處理開銷（CPU利用率）也會成比例地隨資料包大小而降低。這就是高效能LAN和WAN網路技術傾向於選擇較大最大幀大小的原因。

只有在執行長時間的資料傳輸時，效能才會得到改善。示例應用程式套件括：

- 伺服器背對背通訊（例如，網路檔案系統[NFS]事務）
- 伺服器集群
- 高速資料備份
- 高速超級電腦互聯
- 圖形應用程式資料傳輸

網路效能注意事項

TCP在WAN(Internet)上的效能已得到廣泛的研究。此方程式說明了TCP吞吐量如何根據以下條件達到上限：

- 最大區段大小(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。這表示在持續RTT和封包遺失的情況下，如果將封包大小增加一倍，則可使TCP輸送量增加一倍。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。

操作概述

IEEE 802.3標準規範將最大乙太網幀大小定義為**1518**。長度為1519和1522位元組的802.1Q封裝訊框在稍後階段透過IEEE Std 802.3ac-1998附錄，被新增到802.3規範中。在文獻中，它們有時被稱為**小巨人**。

通常，當資料包超出特定乙太網**連線的**指定乙太網最大長度時，將其歸類為巨型幀。巨型資料包也稱為巨**型幀**。

有關巨型幀的主要混淆點在於配置：不同的介面支援不同的最大資料包大小，有時以稍有不同的方式處理大型資料包。

Catalyst 6500 系列

下表嘗試彙總Catalyst 6500平台上不同卡目前支援的MTU大小：

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、WS-X6348-RJ45V、WS-X6348-RJ-21和WX-X6348-RJ21V	8092位元組（受PHY晶片限制）
WS-X6148-RJ-45(V)、WS-X6148-RJ-21(V)、WS-X6148-45AF和WS-X6148-21AF	9100位元組(100 Mbps)/9216位元組(10 Mbps)
X6516-GE-TX	8092位元組（以100 Mbps的速度執行）9216位元組（以10或1000 Mbps的速度執行）
WS-X6148(V)-GE-TX、WS-X6148-GE-45AF、WS-X6548(V)-GE-TX和WS-X6548-GE-45AF	1500 位元組
OSM ATM(OC12c)	9180 位元組
OSM CHOC3、CHOC12、CHOC48和CT3	9216位元組（OCx和DS3）7673位元組(T1/E1)
FlexWAN	7673位元組(CT3 T1/DS0)9216位元組(OC3c POS)7673位元組(T1)
WS-X6148-GE-TX和WS-X6548-GE-TX	不支援

如需詳細資訊，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。

Catalyst 6500/6000 Cisco IOS軟體中的第2層和第3層巨型支援

在配置為第2層和第3層物理介面的所有GE埠上，都存在具有PFC/MSFC1、PFC/MSFC2和PFC2/MSFC2的第2層和第3層巨型支援。無論這些埠是中繼埠還是通道埠，都存在支援。Cisco IOS軟體版本12.1.1E和更新版本提供此功能。

- 所有啟用巨型的物理埠的MTU大小繫結在一起。其中一個的改變會改變一切。啟用後，它們總是保持相同的巨型訊框MTU大小。
- 在配置期間，將同一VLAN中的所有埠啟用為巨量啟用，或者不啟用任何巨量啟用。

- 交換虛擬介面(SVI)（VLAN介面）MTU大小與實體連線埠MTU分開設定。物理埠MTU的更改不會更改SVI MTU大小。此外，SVI MTU的變化不會影響物理埠MTU。
- FE介面上的第2層和第3層巨型幀支援開始於Cisco IOS軟體版本12.1(8a)EX01。**mtu 1500**命令在FE上禁用巨型幀，而**mtu 9216**命令在FE上啟用巨型幀。請參閱Cisco錯誤ID CSCdv90450 (僅限註冊客戶)。
- 只有以下裝置支援VLAN介面上的第3層巨型幀：PFC/MSFC2(Cisco IOS軟體版本12.1(7a)E及更新版本)PFC2/MSFC2(Cisco IOS軟體版本12.1(8a)E4及更新版本)
- 不建議對VLAN介面(SVI)使用搭載PFC/MSFC1的巨型訊框，因為MSFC1可能不能按需要處理分段。
- 相同VLAN中的封包不支援分段（第2層巨型）。
- 需要在VLAN/子網中進行分段的資料包（第3層巨型幀）將傳送到軟體進行分段。

瞭解Catalyst 6500/6000 Cisco IOS軟體中的巨型訊框支援

巨型幀是指大於預設乙太網幀大小的幀。為了啟用巨型幀支援，您可以在埠或VLAN介面上配置大於預設MTU大小，並使用Cisco IOS軟體版本12.1(13)E及更高版本配置全域性LAN埠MTU大小。

Cisco IOS軟體中的橋接和路由流量大小檢查

線路卡	**輸入**	**輸出**
10、10/100、100Mbps埠	MTU大小檢查完成。巨型幀支援將入口流量大小與配置了非預設MTU大小的入口10、10/100和100 Mbps乙太網和10 GE LAN埠的全域性LAN埠MTU大小進行比較。連線埠會捨棄過大的流量。	MTU大小檢查未完成。使用非預設MTU大小配置的埠傳輸包含任何大小大於64位元組的資料包的幀。如果配置了非預設MTU大小，則10、10/100和100 Mbps乙太網LAN埠不會檢查輸出幀是否過大。
GE埠	MTU大小檢查未完成。使用非預設MTU大小配置的埠接受包含任何大小大於64位元組的資料包的幀，並且不會檢查超大輸入幀。	MTU大小檢查完成。巨型訊框支援將輸出流量大小與輸出GE時的全域輸出LAN連線埠MTU大小以及已設定非預設MTU大小的10-GE LAN連線埠進行比較。連線埠會捨棄過大的流量。
10-GE埠	MTU大小檢查完成。連線埠會捨棄過大的流量。	MTU大小檢查完成。連線埠會捨棄過大的流量。
S	MTU大小檢查未完成。	MTU大小檢查完成。在

VI	SVI不會檢查入口端的幀大小。	SVI的出口端檢查MTU大小。
	PFC	
所有路由流量	對於必須路由的流量，PFC上的巨型幀支援將流量大小與配置的MTU大小進行比較，並為使用足以容納流量的MTU大小配置的介面之間的巨型流量提供第3層交換。未配置足夠大MTU大小的介面之間： • 如果未設定「不分段(DF)」位元，則PFC會將流量傳送到MSFC，以便在軟體中分段和路由。 • 如果已設定DF位元，則PFC捨棄流量。	

思科建議

如果實施得當，巨型幀可能會使乙太網連線的TCP吞吐量提高六倍，同時減少分段開銷（以及降低終端裝置的CPU開銷）。

必須確保中間沒有無法處理指定MTU大小的裝置。如果此裝置將資料包分段並轉發，則會使整個進程無效。這會導致此裝置上用於分段和重組資料包的開銷。

在這種情況下，IP路徑MTU探索可協助傳送者找到適於沿每條路徑傳輸流量的最小通用封包長度。或者，您可以配置巨型幀感知主機裝置，其MTU大小是網路中支援的所有裝置的最小大小。

必須仔細檢查每台裝置，以確保其可以支援MTU大小。請參閱本節中的MTU大小支援表。

可以在以下型別的介面上啟用巨型幀支援：

- 連線埠通道介面
- SVI
- 物理介面（第2層/第3層）

您可以在埠通道或參與埠通道的物理介面上啟用巨型幀。確保所有物理介面的MTU都相同非常重要。否則，可能導致介面掛起。您需要更改埠通道介面的MTU，因為它會更改所有成員埠的MTU。

注意：如果由於成員埠是阻塞埠而不能將成員埠的MTU更改為新值，則埠通道將掛起。

在SVI上配置巨型幀支援之前，請始終確保VLAN中的所有物理介面都配置為巨型幀。在SVI的輸入端未檢查封包的MTU。但是，在SVI的出口端會檢查該配置。如果封包MTU大於輸出SVI MTU，軟體會將封包分段（如果沒有設定DF位元），這會導致效能下降。只有第3層交換會發生軟體分段。將封包轉送到第3層連線埠或MTU較小的SVI時，會發生軟體分段。

SVI的MTU需要始終小於VLAN中所有交換機埠中的最小MTU。

Catalyst 4500 系列

Catalyst 4500線卡的非阻塞埠主要支援巨型幀。這些無阻塞GE埠與Supervisor Engine交換矩陣直接連線，並支援巨型幀：

- 管理引擎WS-X4515、WS-X4516 - Supervisor引擎IV或V上的兩個上行鏈路GBIC埠WS-X4516-10GE — 兩個10-GE上行鏈路和四個1-GE小型可插拔(SFP)上行鏈路WS-X4013+ — 兩個1-GE上行鏈路WS-X4013+10GE — 兩個10-GE上行鏈路和四個1-GE SFP上行鏈路WS-X4013+TS - 20個1-GE埠
- 線路卡WS-X4306-GB — 六埠1000BASE-X(GBIC)GE模組WS-X4506-GB-T — 六埠

10/100/1000-Mbps和六埠SFPWS-X4302-GB — 雙埠1000BASE-X(GBIC)GE模組18埠伺服器交換GE模組(WS-X4418-GB)的前兩個GBIC埠和WS-X4232-GB-RJ模組的GBIC埠
- 固定組態交換器WS-C4948 — 所有48個1-GE埠WS-C4948-10GE — 所有48個1-GE埠和兩個10-GE埠

可以使用這些無阻塞GE埠來支援9 KB巨型幀或硬體廣播抑制（僅限Supervisor Engine IV）。 所有其他線卡都支援小巨型框架。您可以使用小型巨型路由器橋接MPLS或使用Q中傳遞的Q，最大負載為1552位元組。

注意：幀大小隨ISL/802.1Q標籤而增加。

小型巨型和巨型幀對於具有Supervisor Engine IV和V的其他Cisco IOS功能是透明的。

Cisco IOS軟體安全功能

基本安全功能

曾幾何時，園區設計往往忽視安全性。但是，安全性現在是每個企業網路的重要組成部分。通常，客戶端已經建立了安全策略來幫助定義思科提供的哪些工具和技術適用。

基本密碼保護

大多數Cisco IOS軟體裝置都配置了兩種級別的密碼。第一級用於裝置的Telnet訪問，也稱為vty訪問。授予vty訪問許可權後，您需要獲得啟用模式或特權exec模式的訪問許可權。

保護交換機的啟用模式

啟用密碼允許使用者獲得對裝置的完全訪問許可權。僅向受信任的人提供啟用密碼。

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

請確保密碼符合以下規則：

- 密碼必須包含一個到25個大寫和小寫字母數字字元。
- 密碼不能以數字作為第一個字元。
- 可以使用前導空格，但它們會被忽略。可以識別中間空格和尾空格。
- 密碼檢查區分大小寫。例如，密碼Secret不同於密碼密碼。

注意：enable secret命令使用單向加密消息摘要5(MD5)雜湊函式。如果您發出**show running-config**命令，就可以看到此加密密碼。使用**enable password**命令是設定啟用密碼的另一種方式。但是，與**enable password**命令一起使用的加密演算法很弱，可以很容易地將其反向以獲得密碼。因此，請勿使用**enable password**命令。使用**enable secret**命令可獲得更好的安全性。有關詳細資訊，請參閱Cisco IOS密碼加密事實。

對交換機的Telnet/VTY安全訪問

預設情況下，Cisco IOS軟體支援五個活動Telnet會話。這些會話稱為vty 0到4。您可以啟用這些線路進行訪問。但是，要啟用登入，您還需要設定這些行的密碼。

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

login命令將這些線路配置為Telnet訪問。**password**命令可配置密碼。請確保密碼符合以下規則：

- 第一個字元不能是數字。
- 該字串可以包含任何字母數字字元，最多可以包含80個字元。字元包括空格。
- 不能以number-space-character格式指定密碼。數字後面的空格會導致問題。例如，Hello 21是合法密碼，而21 hello不是合法密碼。
- 密碼檢查區分大小寫。例如，密碼Secret不同於密碼密碼。

注意：透過此vty線路組態，交換器會將密碼以明文形式儲存。如果有人發出**show running-config**命令，則會顯示此密碼。為了避免這種情況，請使用**service password-encryption**命令。該命令對口令進行鬆散加密。此命令僅加密vty線路口令和使用**enable password**命令配置的使能口令。使用**enable secret**命令配置的使能口令使用更強大的加密。建議使用**enable secret**命令進行配置。

注意：為了更靈活地管理安全性，請確保所有Cisco IOS軟體裝置均實施身份驗證、授權和記帳(AAA)安全模型。AAA可以使用本地、RADIUS和TACACS+資料庫。如需詳細資訊，請參閱TACACS+驗證設定一節。

AAA安全服務

AAA操作概述

訪問控制控制有權訪問交換機的人員以及這些使用者可以使用的服務。AAA網路安全服務提供了在交換機上設定訪問控制的主要框架。

以下部分詳細介紹AAA的各個方面：

- 身份驗證 — 此過程驗證終端使用者或裝置的宣告身份。首先，指定可用於驗證使用者身份的各種方法。這些方法定義要執行的身份驗證型別（例如TACACS+或RADIUS）。 還定義了嘗試這些身份驗證方法的順序。然後將這些方法應用於適當的介面，從而啟用身份驗證。
- 授權 — 此進程向使用者、使用者組、系統或進程授予訪問許可權。AAA進程能夠基於每個任務執行一次性授權或授權。該過程定義使用者有權執行的屬性（在AAA伺服器上）。每當使用者嘗試啟動服務時，交換機都會查詢AAA伺服器並請求授權使用者的許可權。如果AAA伺服器批准，則授權使用者。如果AAA伺服器未批准，則使用者無權執行該服務。您可以使用此過程指定某些使用者只能執行某些命令。
- 記帳 — 此過程允許您跟蹤使用者訪問的服務以及使用者使用的網路資源數量。啟用記帳後，交換機以記帳記錄的形式向AAA伺服器報告使用者活動。報告的使用者活動示例包括會話時間以及開始和停止時間。然後，可以出於管理或記帳目的對此活動進行分析。

雖然AAA是主要的和推薦的訪問控制方法，但Cisco IOS軟體提供了附加功能，以實現不在AAA範圍內的簡單訪問控制。這些附加功能包括：

- 本地使用者名稱身份驗證
- 線路密碼驗證
- 啟用密碼身份驗證

但這些功能無法提供與AAA相同的訪問控制級別。

為了更好地瞭解AAA，請參閱以下檔案：

- 驗證、授權及記帳(AAA)
- 設定存取伺服器上的基礎 AAA
- TACACS+ 和 RADIUS 比較

這些文檔不一定提到交換機。但是檔案所述的AAA概念適用於交換機。

TACACS+

目的

預設情況下，非特權模式和特權模式口令是全域性口令。這些密碼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。在網路裝置上實施這些密碼非常耗時而且非集中化。此外，您也可能難以通過使用容易產生組態錯誤的存取控制清單(ACL)來實作存取限制。為了解決這些問題，請在中央伺服器上配置使用者名稱、密碼和訪問策略時採取集中方法。此伺服器可以是思科安全存取控制伺服器(ACS)或任何第三方伺服器。裝置配置為使用這些集中資料庫來執行AAA功能。在這種情況下，裝置是Cisco IOS軟體交換機。裝置和中央伺服器之間使用的協定可以是：

- TACACS+
- RADIUS
- Kerberos

TACACS+是思科網路中的常見部署，是本節的重點。TACACS+提供以下功能：

- 身份驗證 — 標識和驗證使用者的過程。可以使用多種方法來驗證使用者的身份。但最常用的方法包括使用者名稱和密碼的組合。
- Authorization — 當使用者嘗試執行命令時，交換機可以與TACACS+伺服器進行檢查，以確定是否授予使用者使用該特定命令的許可權。
- 記帳 — 此過程記錄使用者在裝置上執行的操作或已執行的操作。

請參閱TACACS+和RADIUS比較，以比較TACACS+和RADIUS。

操作概述

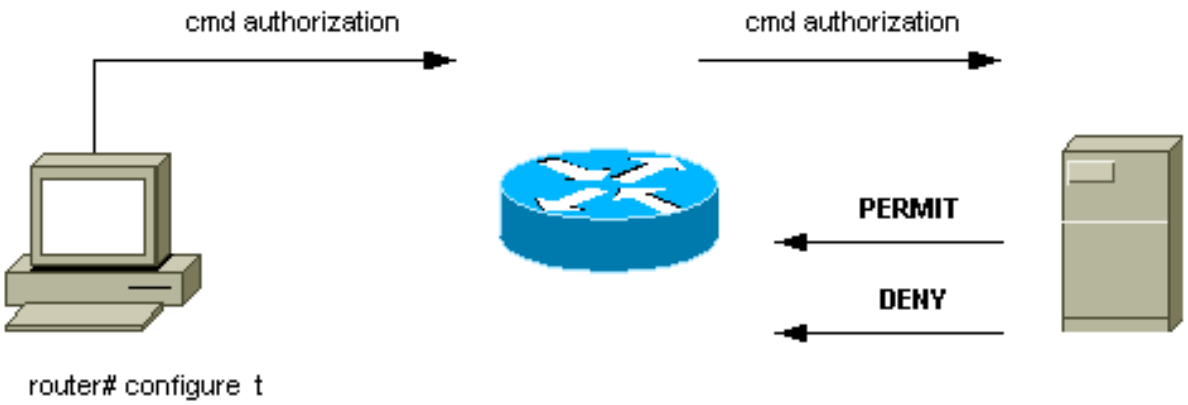
TACACS+通訊協定將使用者名稱和密碼轉送到中央伺服器。此資訊通過網路使用MD5單向雜湊進行加密。如需詳細資訊，請參閱RFC 1321 。TACACS+使用TCP連線埠49作為傳輸通訊協定，相對於UDP具有以下優點：

注意：RADIUS使用UDP。

- 面向連線的傳輸
- 單獨確認已收到請求（TCP確認[ACK]），無論後端身份驗證機制的載入方式如何
- 即時指示伺服器崩潰（重置[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。此步驟可更有效控制交換器上執行的指令，並提供與驗證機制的解耦。通過使用命令記帳，您可以稽核特定使用者連線到特定網路裝置時發出的命令。

此圖顯示所涉及的授權程式：



使用者在簡單的ASCII登入嘗試中使用TACACS+對網路裝置進行驗證時，通常會進行以下程式：

- 建立連線後，交換器會聯絡TACACS+服務精靈以取得使用者名稱提示。然後交換器會顯示使用者的提示。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。交換器會為使用者顯示密碼提示，使用者輸入密碼，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。拒絕使用者進一步訪問或提示使用者重試登入順序。結果取決於TACACS+後台程式。ERROR — 身份驗證過程中某一時刻出錯。錯誤可能出現在守護程式上，也可能出現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。TACACS+後台程式返回ACCEPT或REJECT授權響應。如果返回ACCEPT響應，則該響應包含屬性形式的資料，用於為該使用者引導EXEC或NETWORK會話。這決定了使用者可以訪問哪些命令。

基本AAA配置步驟

瞭解基本流程後，AAA的配置相對簡單。要在使用AAA的思科路由器或接入伺服器上配置安全性，請執行以下步驟：

1. 要啟用AAA，請發出**aaa new-model**全域性配置命令。
   ```
   Switch(config)#aaa new-model
   ```

   提示：在配置AAA命令之前儲存配置。只有在您完成了所有AAA配置並確信配置工作正常後，才能再次儲存配置。然後，如有必要，您可以重新載入交換器，以從無法預見的封鎖中復原（在儲存組態之前）。
2. 如果您決定使用單獨的安全伺服器，請配置安全協定引數，例如RADIUS、TACACS+或Kerberos。
3. 使用**aaa authentication**命令定義身份驗證的方法清單。
4. 使用**login authentication**命令可將方法清單應用於特定介面或線路。
5. 發出可選的**aaa authorization**命令以配置授權。
6. 發出可選的**aaa accounting**命令以配置記帳。
7. 配置AAA外部伺服器以處理來自交換機的身份驗證和授權請求。**附註：** 有關詳細資訊，請參閱AAA伺服器文檔。

TACACS+驗證組態

執行以下步驟以配置TACACS+身份驗證：

1. 在全域性配置模式下發出**aaa new-model**命令，以在交換機上啟用AAA。
2. 定義TACACS+伺服器和關聯的金鑰。此金鑰用於加密TACACS+伺服器和交換器之間的流量。在**tacacs-server host 1.1.1.1 key mysecretkey**命令中，TACACS+伺服器的IP地址為1.1.1.1，加密金鑰為mysecretkey。若要確認交換器是否可連線至TACACS+伺服器，請自交換器發起網際網路控制訊息通訊協定(ICMP)Ping。
3. 定義方法清單。方法清單定義嘗試各種服務的身份驗證機制序列。各種服務可以是，例如：啟用登入（用於vty/Telnet訪問）**註：有關**vty/Telnet訪問的資訊，請參閱本文檔的基本安全功能部分。主控台此範例僅考慮**login**。必須將方法清單應用到介面/線路：

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

在此配置中，**aaa authentication login**命令使用虛構清單名稱METHOD-LIST-LOGIN，並在使用方法行之前使用方法tacacs+。使用者是使用TACACS+伺服器作為第一種方法進行驗證。如果TACACS+伺服器沒有響應或傳送錯誤消息，則線路上配置的密碼將用作第二種方法。但是，如果TACACS+伺服器拒絕使用者並使用REJECT消息進行響應，則AAA會認為事務成功，不會使用第二種方法。**注意：**在將清單(METHOD-LIST-LOGIN)應用於vty線路之前，配置不完整。線上路配置模式下發出**login authentication METHOD-LIST-LOGIN**命令，如示例所示。**注意：**此示例為TACACS+伺服器不可用時建立後門。安全管理員可以或可能不能接受後門的實施。確保實施此類後門的決定符合站點的安全策略。

RADIUS驗證設定

RADIUS組態幾乎與TACACS+組態相同。只需在組態中將RADIUS一詞替換為TACACS。以下是COM連線埠存取的RADIUS組態範例：

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

登入橫幅

建立相應的裝置橫幅，明確說明未經授權訪問時執行的操作。不要向未經授權的使用者通告站點名稱或網路資訊。在裝置受損且罪犯被抓住的情況下，標語提供追索權。發出以下命令可建立登入橫幅：

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

實體安全

請確保必須進行適當的授權才能以物理方式訪問裝置。將裝置保持在受控（鎖定）的空間中。為確保網路保持正常運行並且不受惡意篡改或環境因素的影響，請確保所有裝置都具有：

- 適當的不間斷電源(UPS)，儘可能配備冗餘電源
- 溫度控制（空調）

請記住，如果具有惡意意圖的人違反物理訪問，則更有可能通過密碼恢復或其他方式中斷。

管理配置

網路圖

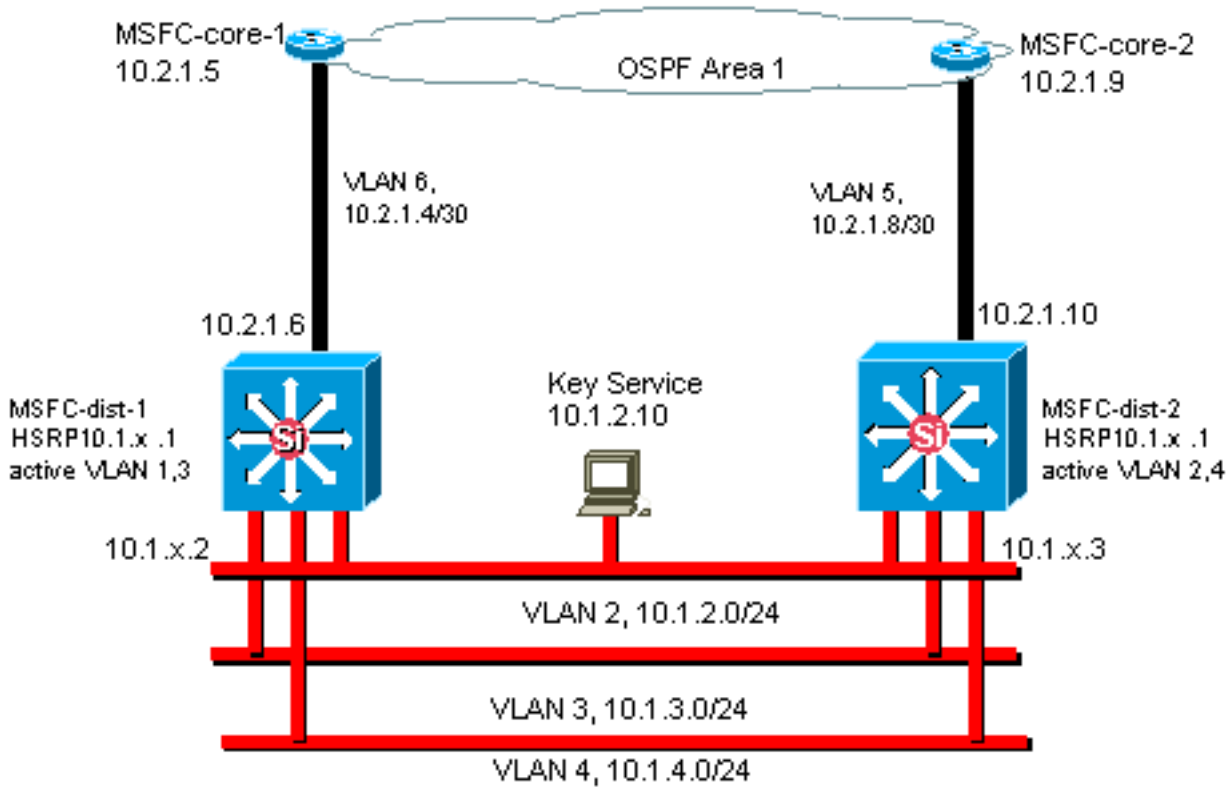
目的

清晰的網路圖是網路操作的基本部分。在故障排除過程中，這些圖變得至關重要，並且是在故障期間向供應商和合作夥伴上報資訊的最重要工具。不要低估網路圖提供的準備、就緒性和可訪問性。

建議

需要以下三種型別的圖：

- **總體圖** — 即使對於最大的網路，顯示端到端物理或邏輯連線的圖也非常重要。通常，已實施分層設計的企業會分別記錄每一層。當您計畫和解決問題時，重要的是要很好地瞭解域如何連線在一起。
- **物理圖** — 此圖顯示所有交換機和路由器硬體及佈線。請確保圖表標籤了以下每個方面：中繼連結速度通道組連接埠號碼插槽機箱型別軟體VTP域根網橋備用根網橋優先順序MAC 地址每個VLAN的阻塞埠為更清楚起見，請將Catalyst 6500/6000 MSFC路由器等內部裝置描繪為通過中繼連線的單臂路由器。
- **邏輯圖** — 此圖僅顯示第3層功能，這意味著它會將路由器顯示為對象，將VLAN顯示為乙太網段。請確保圖標籤了以下方面：IP地址子網輔助定址HSRP主用和備用接入核心分佈層路由資訊



交換機管理介面和本徵VLAN

目的

本節介紹使用預設VLAN 1的意義和潛在問題。本節還說明在6500/6000系列交換器上將管理流量執行到相同VLAN中交換器的潛在問題。

Supervisor Engine和Catalyst 6500/6000系列的MSFC上的處理器使用VLAN 1作為許多控制和管理協定。示例包括：

- 交換器控制通訊協定：STP BPDUVTPDTPCDP
- 管理協定：SNMPTelnet安全殼層通訊協定(SSH)系統日誌

以這種方式使用VLAN時，它稱為本地VLAN。預設交換機配置將VLAN 1設定為Catalyst中繼埠上的預設本地VLAN。您可以將VLAN 1保留為本徵VLAN。但請記住，在網路中運行Cisco IOS系統軟體的任何交換機預設將配置為第2層交換機埠的所有介面都設定為訪問VLAN 1中的埠。最有可能的是，網路中某個位置的交換機使用VLAN 1作為使用者流量的VLAN。

使用VLAN 1的主要顧慮是，一般來說，Supervisor引擎NMP無需被終端站生成的許多廣播和多播流量中斷。組播應用尤其傾向於在伺服器和客戶端之間傳送大量資料。Supervisor Engine不需要看到此資料。如果Supervisor Engine在監聽不必要流量時完全佔用了Supervisor Engine的資源或緩衝區，則Supervisor Engine可能無法看到可能導致跨距樹狀目錄回圈或EtherChannel失敗的管理封包（在最糟糕的情況下）。

show interfaces ***interface_type slot****/port* counters命令和**show ip traffic**命令可以為您提供以下一些指示：

- 廣播流量與單播流量的比例

- IP流量與非IP流量的比例（管理VLAN中通常看不到此比例）

VLAN 1標籤和處理大部分控制平面流量。預設情況下，VLAN 1在所有中繼上啟用。對於大型園區網路，您需要小心VLAN 1 STP域的直徑。網路某一部分的不穩定會影響VLAN 1，並會影響所有其他VLAN的控制平面穩定性和STP穩定性。您可以限制使用者資料的VLAN 1傳輸和介面上的STP操作。請勿在TRUNK介面上設定VLAN。

此組態不會像使用網路分析器一樣，停止VLAN 1中交換器之間傳輸控制封包。但是，不會轉發任何資料，並且STP不會在此鏈路上運行。因此，您可以使用此技術將VLAN 1拆分為較小的故障域。

註：無法將VLAN 1從中繼清除到Catalyst 2900XL/3500XL。

即使您謹慎地將使用者VLAN限制到相對較小的交換機域和相對較小的故障/第3層邊界，一些客戶仍然會傾向於以不同方式處理管理VLAN。這些客戶嘗試使用單個管理子網覆蓋整個網路。中央NMS應用必須與應用管理的裝置相鄰的第2層沒有技術原因，這也不是一個合格的安全引數。將管理VLAN的直徑限製為與使用者VLAN相同的路由域結構。將帶外管理和/或SSH支援視為提高網路管理安全性的方法。

其他選項

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生成樹。通過這種方式，設計要求將每個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。

您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？這個問題沒有簡單的答案。考慮以下兩個選項，以便與您的思科工程師一起進行設計稽核：

- **選項1** — 將兩個或三個唯一的VLAN從分佈層向下中繼到每個接入層交換機。此配置允許使用資料VLAN、語音VLAN和管理VLAN，並且仍具有STP處於非活動狀態的優點。若要從TRUNK清除VLAN 1，需要額外的配置步驟。在此解決方案中，還有一些設計要點需要考慮，以避免在故障恢復期間臨時阻塞路由流量。將STP PortFast用於中繼（將來）或通過STP轉發進行VLAN自動狀態同步。
- **選項2** — 可以接受單個資料和管理的VLAN。如果您希望將sc0介面與使用者資料分隔開來，那麼較新的交換機硬體會使這個場景較以前的問題更少。較新的硬體提供：更強大的CPU和控制平面速率限制控制多層設計提倡的廣播域相對較小的設計為了做出最終決定，請檢查VLAN的廣播流量配置檔案，並與您的思科工程師討論交換機硬體的功能。如果管理VLAN包含該接入層交換機上的所有使用者，請根據Cisco IOS軟體安全功能部分使用IP輸入過濾器從使用者處保護交換機。

Cisco管理介面和本徵VLAN建議

管理介面

Cisco IOS系統軟體為您提供在VLAN中將介面配置為第3層介面或第2層交換機埠的選項。在Cisco IOS軟體中使用**switchport**命令時，預設情況下，所有交換器連線埠都是VLAN 1中的存取連線埠。因此，除非另有設定，否則使用者資料預設情況下也可能存在於VLAN 1上。

將管理VLAN設為VLAN 1以外的VLAN。將所有使用者資料放在管理VLAN之外。而是將loopback0介面配置為每台交換機的管理介面。

註：如果使用OSPF協定，此地址也將成為OSPF路由器ID。

確保環回介面具有32位子網掩碼，並將環回介面配置為交換機上的純第3層介面。範例如下：

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

本徵VLAN

將本徵VLAN配置為路由器上從未啟用的一個明顯的虛擬VLAN。Cisco過去曾推薦VLAN 999，但這個選擇完全是任意的。

發出以下介面命令，將VLAN建立為特定埠上802.1Q中繼的本機（預設）：

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

有關其他中繼配置建議，請參閱本文檔的動態中繼協定部分。

帶外管理

目的

如果圍繞生產網路構建獨立的管理基礎架構，則可以提高網路管理的可用性。此設定允許遠端訪問裝置，而不管驅動流量或發生控制平面事件。這兩種方法是典型的：

- 使用專用LAN進行帶外管理
- 使用終端伺服器的帶外管理

操作概述

您可以為網路中的每台路由器和交換機提供管理VLAN上的帶外乙太網管理介面。您可以在管理VLAN中的每個裝置上配置一個乙太網埠，並將其從生產網路外部連線到單獨的交換管理網路。

註：Catalyst 4500/4000交換機在Supervisor Engine上有一個特殊的me1介面，該介面僅用於帶外管理，而不用作交換機埠。

此外，如果使用RJ-45串列電纜配置Cisco 2600或3600路由器，以訪問佈局中每台路由器和交換機的控制檯埠，則可以實現終端伺服器連線。使用終端伺服器還可以避免配置備份方案，例如每台裝置的輔助埠上的數據機。您可以在終端伺服器的輔助埠上配置單個數據機。此配置在網路連線發生故障時向其他裝置提供撥號服務。如需詳細資訊，請參閱將資料機連線到Catalyst交換器上的主控台連線埠。

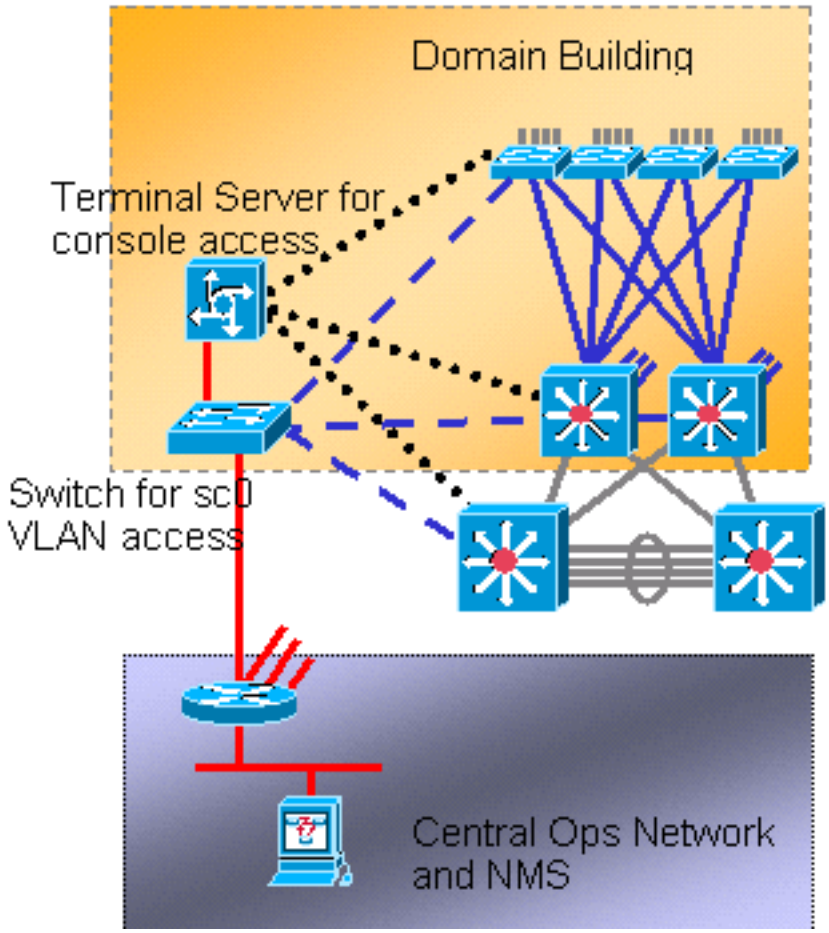
建議

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。這種安排實現了高可用性的網路管理。好處包括：

- 該配置將管理流量與使用者資料分離。
- 為了安全，管理IP地址位於單獨的子網、VLAN和交換機中。

- 可在網路故障期間為管理資料傳送提供更高保證。
- 管理VLAN中沒有活動的生成樹。這裡的冗餘不是關鍵。

此圖顯示帶外管理：



系統記錄

目的

系統日誌消息特定於思科，與標準化的SNMP相比，它可以提供更快速且準確的資訊。例如，Cisco Resource Manager Essentials(RME)和Network Analysis Toolkit(NATKit)等管理平台可有力地利用系統日誌資訊來收集清單和配置更改。

思科系統日誌配置建議

系統日誌記錄是一種常見且可接受的操作實踐。UNIX系統日誌可以捕獲和分析路由器上的資訊/事件，例如：

- 介面狀態
- 安全警報
- 環境條件
- CPU進程掛起
- 其他活動

Cisco IOS軟體可以對UNIX系統日誌伺服器執行UNIX日誌記錄。Cisco UNIX系統日誌格式與4.3 Berkeley Standard Distribution(BSD)UNIX相容。使用以下Cisco IOS軟體日誌設定：

- no logging console — 預設情況下，所有系統消息都會傳送到系統控制檯。控制檯日誌記錄是Cisco IOS軟體中的高優先順序任務。此函式主要用於在系統出現故障之前向系統操作員提供錯誤消息。在所有裝置配置中禁用控制檯日誌記錄，以避免在裝置等待來自終端的響應時，路由器/交換機可能掛起的情況。但控制檯消息在故障隔離期間非常有用。在這些情況下，啟用控制檯日誌記錄。發出logging console level命令可獲取所需的消息日誌記錄級別。日誌記錄級別為0到7。
- no logging monitor — 此命令禁用除系統控制檯之外的終端線路的日誌記錄。可能需要監視日誌記錄(使用logging monitor debugging或其他命令選項)。 在這種情況下，請在活動所必需的特定日誌記錄級別啟用監控日誌記錄。有關日誌記錄級別的詳細資訊，請參閱此清單中的no logging console項。
- logging buffered 16384 — 需要將logging buffered命令新增到內部日誌緩衝區的日誌系統消息中。日誌記錄緩衝區是循環的。一旦日誌記錄緩衝區被填滿，較舊的條目將被較新的條目覆蓋。日誌記錄緩衝區的大小可由使用者配置，並以位元組為單位。系統緩衝區的大小因平台而異。16384是一個很好的預設值，在大多數情況下提供充足的日誌記錄。
- logging trap notifications — 此命令提供到指定syslog伺服器的通知級別(5)消息。所有裝置（控制檯、監視器、緩衝區和陷阱）的預設日誌記錄級別是調試（第7級）。 如果將陷阱日誌記錄級別設為7，則會生成許多與網路運行狀況無關或不相關的消息。將陷阱的預設日誌記錄級別設定為5。
- logging facility local7 — 此命令為UNIX系統日誌設定預設日誌記錄工具/級別。為相同的設施/級別配置接收這些消息的系統日誌伺服器。
- logging host — 此命令設定UNIX日誌記錄伺服器的IP地址。
- logging source-interface loopback 0 — 此命令為系統日誌消息設定預設IP SA。對日誌記錄SA進行硬編碼，以便更容易識別傳送消息的主機。
- service timestamps debug datetime localtime show-timezone msec — 預設情況下，日誌消息沒有時間戳。您可以使用此命令啟用日誌消息的時間戳並配置系統調試消息的時間戳。時間戳提供記錄事件的相對計時並增強即時調試。當客戶將調試輸出傳送給您的技術支援人員尋求幫助時，此資訊尤其有用。要啟用系統調試消息的時間戳，請在全域性配置模式下使用命令。該命令僅在啟用調試時有效。

注意：此外，在所有基礎設施Gigabit介面上啟用鏈路狀態和捆綁狀態日誌記錄。

Cisco IOS軟體提供單一機制來設定所有目的地為syslog伺服器的系統訊息的設施和記錄層級。將日誌記錄陷阱級別設定為通知（級別5）。 如果將陷阱消息級別設定為通知，則可以最小化轉發到系統日誌伺服器的資訊消息數量。此設定可以顯著減少網路上的系統日誌通訊量，並減輕對系統日誌伺服器資源的影響。

向執行Cisco IOS軟體的每個路由器和交換器新增以下命令，以便啟用系統日誌訊息：

- 全域性系統日誌配置命令：

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

- 介面系統日誌配置命令：

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

SNMP

目的

您可以使用SNMP檢索儲存在網路裝置MIB中的統計資訊、計數器和表。HP OpenView等NMS可以使用這些資訊來：

- 生成即時警報
- 測量可用性
- 生成能力計畫資訊
- 幫助執行配置和故障排除檢查

SNMP管理介面操作

SNMP是一種應用層協定，為SNMP管理器和代理之間的通訊提供消息格式。SNMP提供標準化框架和通用語言，用於監控和管理網路中的裝置。

SNMP框架由以下三個部分組成：

- SNMP管理器
- SNMP代理
- MIB

SNMP管理器是使用SNMP控制和監控網路主機活動的系統。最常見的管理系統稱為NMS。您可以將術語NMS應用於用於網路管理的專用裝置或此類裝置上使用的應用程式。各種網路管理應用程式可用於SNMP。這些應用範圍從簡單的CLI應用到功能豐富的GUI（如CiscoWorks產品系列）。

SNMP代理是受管裝置中的軟體元件，用於維護裝置的資料並根據需要將這些資料包告給管理系統。代理和MIB駐留在路由裝置（路由器、接入伺服器或交換機）上。 要在Cisco路由裝置上啟用SNMP代理，必須定義管理器和代理之間的關係。

MIB是用於網路管理資訊的虛擬資訊儲存區域。MIB由託管對象的集合組成。在MIB中，存在在MIB模組中定義的相關對象的集合。MIB模組以SNMP MIB模組語言編寫，如STD 58、RFC 2578、RFC 2579 和RFC 2580 定義。

註：單個MIB模組也稱為MIB。例如，介面組MIB(IF-MIB)是系統上MIB中的MIB模組。

SNMP代理包含MIB變數，SNMP管理器可通過get或set操作請求或更改這些變數的值。管理器可以從代理獲取值或向代理儲存值。代理從MIB收集資料，MIB是有關裝置引數和網路資料的資訊儲存庫。代理還可以響應管理器獲取或設定資料的請求。

管理器可以傳送代理請求以獲取和設定MIB值。代理可以響應這些請求。獨立於此互動，代理可以向管理器傳送未經請求的通知（陷阱或通知），以便向管理器通知網路條件。藉助某些安全機制，NMS可以通過`get`和`get next`請求檢索MIB中的資訊，還可以發出**set**命令以更改引數。此外，您還可以設定網路裝置以生成陷阱消息到NMS以即時警報。IP UDP埠161和162用於陷阱。

SNMP通知操作概述

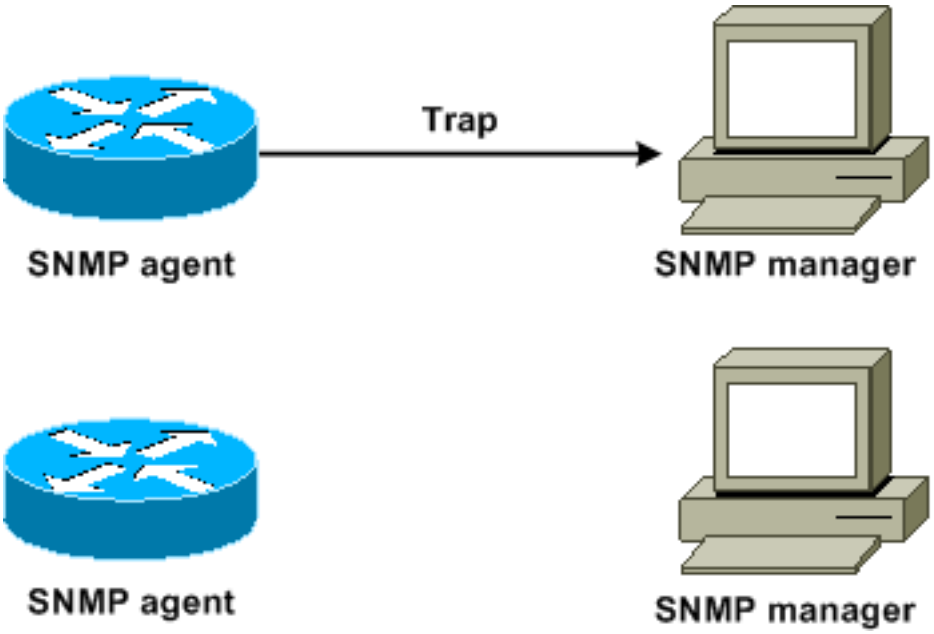
SNMP的主要功能是能夠從SNMP代理生成通知。這些通知不要求從SNMP管理器傳送請求。未經請求的（非同步）通知可以作為陷阱或通知請求生成。陷阱是向SNMP管理器發出網路條件警報的消息。通知請求（通知）是陷阱，包括來自SNMP管理器的確認接收的請求。通知可以指示以下重要事件：

- 使用者身份驗證不正確
- 重新啟動
- 連線的關閉
- 與鄰居路由器的連線中斷
- 其他活動

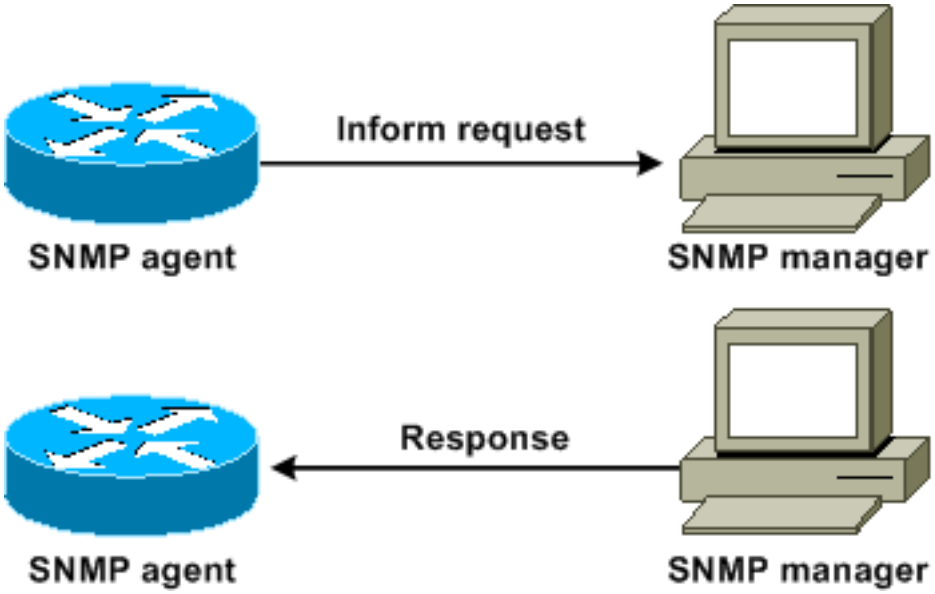
陷阱不如通知可靠，因為接收方在收到陷阱時不會傳送任何確認。傳送方無法確定陷阱是否收到。接收通知請求的SNMP管理器使用SNMP響應協定資料單元(PDU)確認消息。 如果管理器未收到通知請求，則管理器不會傳送響應。如果傳送方從未收到響應，則傳送方可以再次傳送通知請求。通知更有可能到達預定目的地。

但陷阱通常是首選的，因為通知會消耗路由器和網路中的更多資源。陷阱一旦傳送即被丟棄。但通知請求必須儲存在記憶體中，直到收到響應或請求超時。此外，陷阱僅傳送一次，而通知可以重試多次。重試會增加流量，並導致網路開銷增加。因此，陷阱和通知請求在可靠性和資源之間提供了一個權衡。如果您需要SNMP管理器接收每個通知，請使用通知請求。但是，如果您對網路上的流量或路由器的內存有顧慮，並且您不需要接收每個通知，請使用陷阱。

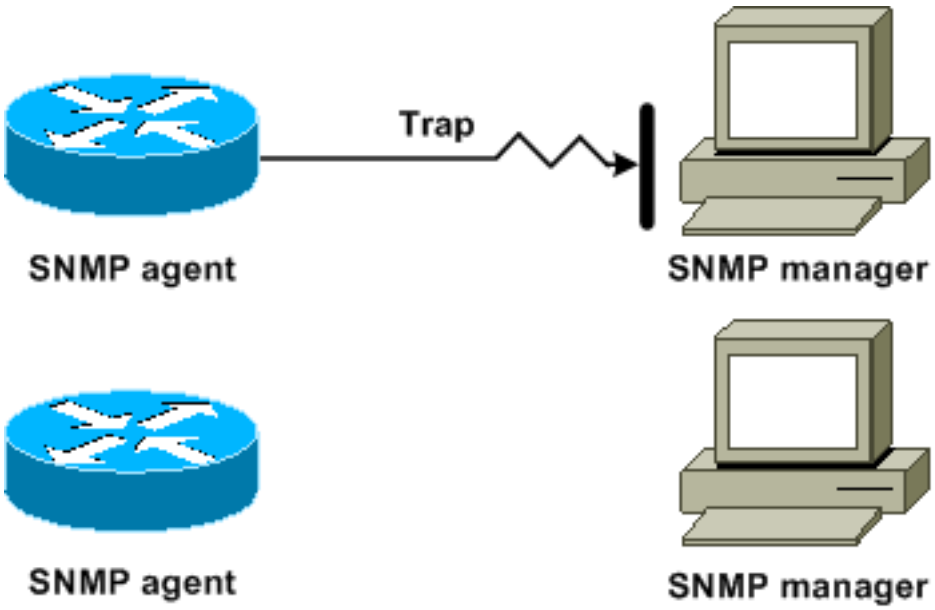
這些圖說明了陷阱和通知請求之間的區別：



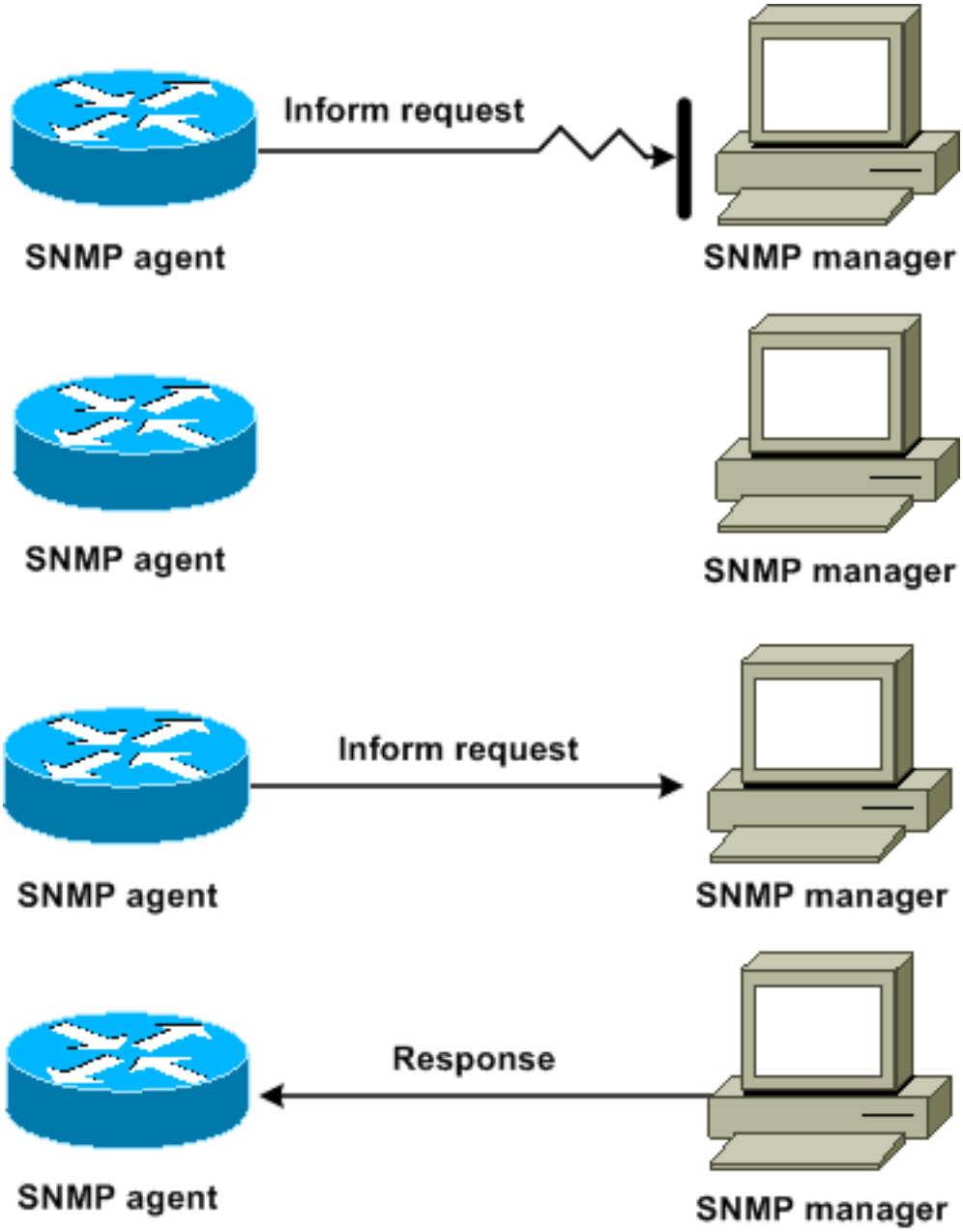
此圖說明代理路由器如何成功將陷阱傳送到SNMP管理器。雖然管理器收到陷阱，但是它不會向代理傳送任何確認。代理無法知道陷阱到達目的地。



此圖說明代理路由器如何成功向管理器傳送通知請求。當管理器接收到通知請求時，管理器向代理傳送響應。這樣，代理就知道通知請求到達了目的地。請注意，在此示例中，流量是此示例的兩倍。但代理知道經理收到了通知。



在此圖中，代理向管理器傳送陷阱，但該陷阱無法到達管理器。代理無法知道陷阱沒有到達目的地，因此不會再次傳送陷阱。經理永遠不會收到陷阱。



在此圖中，代理向管理器傳送通知請求，但通知請求沒有到達管理器。由於管理器未收到通知請求，因此沒有響應。一段時間後，代理將重新傳送通知請求。第二次，管理器接收通知請求並用響應回覆。在此範例中，存在更多流量。但通知到達SNMP管理器。

Cisco MIB和RFC參考

RFC文檔通常定義MIB模組。RFC文檔將提交給國際標準機構Internet工程任務組(IETF)。個人或團體編寫RFC供網際網路協會(ISOC)和整個Internet社群審議。請參閱Internet協會 (Internet Society)首頁，瞭解標準流程和IETF的活動。請參閱IETF 首頁，以閱讀思科檔案參考的所有RFC、Internet草稿(I-D)和STD的全文。

Cisco的SNMP實施使用：

- RFC 1213 描述的MIB II變數的定義
- RFC 1215 描述的SNMP陷阱的定義

Cisco為每個系統提供自己的專用MIB擴展。除非檔案另有說明，否則思科企業MIB符合相關RFC所述的准則。您可以在Cisco MIB首頁上找到MIB模組定義檔案以及每個Cisco平台支援的MIB清單。

SNMP版本

Cisco IOS軟體支援以下版本的SNMP:

- SNMPv1 - RFC 1157 定義的完整Internet標準。RFC 1157 ，取代作為RFC 1067 和RFC 1098發佈的較早版本 。安全性以社群字串為基礎。
- SNMPv2c - SNMPv2c是SNMPv2的基於社群字串的管理框架。SNMPv2c（c表示社群）是一個實驗性的Internet協定，RFC 1901 、RFC 1905 和RFC 1906 定義。SNMPv2c是SNMPv2p(SNMPv2 Classic)協定操作和資料型別的更新。SNMPv2c使用SNMPv1的基於社群的安全模型。
- SNMPv3 - SNMPv3是RFC 2273 、RFC 2274 和RFC 2275 定義的基於標準的可互操作協定。SNMPv3通過網路結合身份驗證和資料包加密，提供對裝置的安全訪問。SNMPv3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。Authentication — 確定消息來自有效源。加密 — 對資料包的內容進行擾動，防止未經授權的源進行發現。

SNMPv1和SNMPv2c都使用基於社群的安全形式。IP地址ACL和密碼定義了能夠訪問代理MIB的管理器社群。

SNMPv2c支援包括批次檢索機制和向管理站報告的更詳細的錯誤消息。批次檢索機制支援對表和大量資訊的檢索，這最大程度地減少了所需的往返次數。SNMPv2c改進的錯誤處理支援包括區分不同錯誤條件的擴展錯誤代碼。通過SNMPv1中的單個錯誤代碼報告這些情況。現在，錯誤返回代碼報告錯誤型別。

SNMPv3同時提供安全模型和安全級別。安全模型是為使用者和使用者所在的組設定的身份驗證策略。安全級別是安全模型中允許的安全級別。安全模型和安全級別的組合決定了處理SNMP資料包時使用的安全機制。

常規SNMP配置

在所有客戶交換器上發出以下命令，以便啟用SNMP管理：

- SNMP ACL的命令：

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

- 全域SNMP命令：

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

SNMP陷阱建議

SNMP是網路管理的基礎，並在所有網路中啟用和使用。

SNMP代理可以與多個管理器通訊。因此，您可以將軟體配置為支援與使用SNMPv1的一個管理站和使用SNMPv2的另一個管理站的通訊。大多數客戶和NMS仍然使用SNMPv1和SNMPv2c，因為NMS平台中的SNMPv3網路裝置支援有些滯後。

為所有正在使用的功能啟用SNMP陷阱。如果需要，可以禁用其他功能。啟用陷阱後，可以發出**test**

snmp命令，並在NMS上為錯誤設定適當的處理。此類處理的示例包括尋呼機警報或彈出消息。

預設情況下禁用所有陷阱。在核心交換機上啟用所有陷阱，如以下示例所示：

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

此外，為關鍵埠（例如到路由器和交換機的基礎設施鏈路以及關鍵伺服器埠）啟用埠陷阱。其他連線埠（例如主機連線埠）不需要啟用。發出以下命令可設定連線埠並啟用連結開啟/關閉通知：

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

接下來，指定接收陷阱的裝置並相應地執行陷阱。現在，您可以將每個陷阱目標配置為SNMPv1、SNMPv2或SNMPv3收件人。對於SNMPv3裝置，可以傳送可靠通知而不是UDP陷阱。以下是組態：

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

SNMP輪詢建議

請確保這些MIB是在園區網路中輪詢或監控的重要MIB:

注意：此建議來自思科網路管理諮詢組。

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

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

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

網路時間協定

目的

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。NTP允許在建立系統日誌時和其他特定時間事件發生時關聯事件。

操作概述

RFC 958首 先記錄NTP。但是NTP是通過RFC 1119 （NTP版本2）發展起來的。RFC 1305 現在定義了NTP，這是其第三個版本。

NTP將電腦客戶端或伺服器的時間與另一伺服器或參考時間源（如無線電、衛星接收器或數據機）同步。NTP提供的客戶端準確性通常在LAN上的一毫秒內，在WAN上最多為幾十毫秒（相對於同步的主伺服器）。例如，您可以使用NTP通過全球定位服務(GPS)接收器協調協調世界時(UTC)。

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。

NTP通過UDP運行，而UDP又通過IP運行。所有NTP通訊都使用UTC，與格林尼治平均時間相同。

目前，NTP第3版(NTPv3)和NTP第4版(NTPv4)實施可用。正在開發的最新軟體版本是NTPv4，但官方的Internet標準仍是NTPv3。此外，某些作業系統供應商會自定義該協定的實施。

NTP保障措施

NTP實現還試圖避免與時間可能不準確的電腦同步。NTP通過兩種方式實現這一點：

- NTP不會與自身未同步的電腦同步。
- NTP始終比較多台電腦報告的時間，並且不會與時間明顯不同於其他電腦的電腦同步，即使該電腦具有較低層。

關聯

運行NTP的電腦之間的通訊（稱為關聯）通常是靜態配置的。每台電腦都獲得了需要與之建立關聯的所有電腦的IP地址。通過在具有關聯的每對電腦之間交換NTP消息，可以實現準確計時。但是在LAN環境中，可以將NTP配置為使用IP廣播消息。使用此替代方法，可以將電腦配置為傳送或接收廣播消息，但計時準確度會略有降低，因為資訊流是單向的。

如果網路與Internet隔離，Cisco NTP實施允許您配置電腦，以便當電腦實際確定使用其它方法的時間時，電腦就像與使用NTP同步一樣。其他電腦使用NTP與該電腦同步。

NTP關聯可以是：

- 對等關聯這表示此系統可以同步到另一個系統或允許另一個系統與其同步。
- 伺服器關聯這表示只有此系統與另一個系統同步。另一個系統無法與此系統同步。

如果要與其他系統建立NTP關聯，請在全域性配置模式下使用以下命令之一：

指令	目的
ntp peer *ip-address* [normal-sync] [version *number*] [key *key-id*] [source *interface*] [prefer]	與其他系統形成對等關聯
ntp server *ip-address* [version *number*] [key *key-id*] [source *interface] [prefer]*	與另一個系統建立伺服器關聯

注意：僅需要配置關聯的一端。另一個系統自動建立關聯。

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，它們通過無線電、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個公共輔助伺服器與主伺服器同步。這些伺服器向Internet上總數超過100,000台客戶端和伺服器提供同步。Public NTP Servers 頁維護當前清單並經常更新。

此外，還有大量專用主要和輔助伺服器，它們通常不向公眾開放。請參閱網路時間協定專案（德拉瓦大學），瞭解公共NTP伺服器的清單以及有關如何使用這些伺服器的資訊。無法保證這些公共Internet NTP伺服器可用並生成正確的時間。因此，您必須考慮其他選項。例如，使用直接連線到許多路由器的各種獨立GPS裝置。

另一個選項是使用設定為第1層主機的各種路由器。但不建議使用此類路由器。

層

NTP使用層來描述機器離開權威時間源的NTP跳數。第1層時間伺服器有一個直接連線的無線電時鐘或原子時鐘。第2層時間伺服器從第1層時間伺服器接收其時間，以此類推。運行NTP的電腦會自動選擇具有最低層數的電腦作為時間源，該電腦配置為通過NTP進行通訊。該策略有效地建立了NTP發言人的自組織樹。

NTP會避免與時間可能不準確的裝置同步。有關詳細資訊，請參閱網路時間協定的*NTP保護*部分。

伺服器對等關係

- 伺服器響應客戶端請求，但不嘗試合併來自客戶端時間源的任何日期資訊。
- 對等體響應客戶請求，並嘗試將客戶請求用作更好的時間源的潛在候選者，並幫助穩定其時脈頻率。
- 要成為真正的對等體，連線的兩端必須建立對等體關係，而不是一個使用者充當對等體，另一個使用者充當伺服器的情況。讓對等體交換金鑰，以便只有受信任的主機才能作為對等體與他人通訊。
- 在向伺服器的客戶機請求中，伺服器回答客戶機並忘記客戶機提出的問題。
- 在向對等體的客戶端請求中，伺服器會應答客戶端。伺服器儲存有關客戶端的狀態資訊，以便跟蹤客戶端在計時時的表現以及客戶端運行的層級伺服器。

NTP伺服器可以處理數千個客戶端而沒有問題。但是，當NTP伺服器處理多個客戶端（最多幾百個）時，記憶體會對伺服器保留狀態資訊的能力產生影響。當NTP伺服器處理超過建議數量時，會佔用更多的CPU資源和頻寬。

與NTP伺服器的通訊模式

以下是與伺服器通訊的兩種不同模式：

- 廣播模式
- 客戶端/伺服器模式

在廣播模式下，客戶端偵聽。在客戶端/伺服器模式下，客戶端輪詢伺服器。如果由於速度原因沒有涉及WAN鏈路，則可以使用NTP廣播。要通過WAN鏈路，請使用客戶端/伺服器模式（通過輪詢）。 廣播模式是為LAN設計的，在這種模式下，許多客戶端可能需要輪詢伺服器。如果沒有廣播模式，此類輪詢可能會在網路上生成大量資料包。NTP組播在NTPv3中尚不可用，但在NTPv4中可用。

預設情況下，Cisco IOS軟體會與NTPv3的使用進行通訊。但軟體向後相容NTP的早期版本。

輪詢

NTP協定允許客戶端隨時查詢伺服器。

在思科機箱中首次配置NTP時，NTP會以NTP_MINPOLL（2^4=16秒）間隔快速連續傳送八個查詢。NTP_MAXPOLL為2^14秒（16,384秒或4小時33分鐘4秒）。 此時間段是NTP再次輪詢響應之前的最長時間段。目前，思科沒有方法允許使用者手動強制POLL時間。

NTP輪詢計數器從2^6(64)秒或1分鐘4秒開始。當兩個伺服器彼此同步時，此時間以2的冪遞增到2^10。根據伺服器或對等配置，可以預期以64、128、256、512或1024秒之間的時間間隔傳送同步消息。輪詢之間的時間間隔較長，因為鎖相環路使當前時鐘變得更加穩定。鎖相環切割本地時鐘晶體，長達1024秒（17分鐘）。

當冪為2時，時間在64秒和1024秒之間（等於每64、128、256、512或1024秒一次）。 時間取決於傳送和接收資料包的鎖相環路。如果時間中有大量抖動，則輪詢發生頻率更高。如果參考時鐘準確且網路連線一致，則每次輪詢之間的輪詢時間會收斂到1024秒。

NTP輪詢間隔會隨著客戶端與伺服器之間的連線更改而更改。如果連線更佳，輪詢間隔會更長。在這種情況下，更好的連線意味著NTP客戶端已收到八個響應（針對最後八個請求）。輪詢間隔隨後加倍。單個未響應導致輪詢間隔縮短一半。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秒到1024秒所需的時間略多於2小時。

廣播

NTP廣播從不轉發。如果您發出**ntp broadcast**命令，則路由器開始在配置它的介面上發起NTP廣播。

通常，發出**ntp broadcast**命令可將NTP廣播傳送到LAN，以便為客戶端站和伺服器提供服務。

時間同步

客戶端與伺服器的同步包括幾個資料包交換。每個交換都是請求/回覆對。當客戶端傳送請求時，客戶端將其本地時間儲存在傳送的資料包中。當伺服器收到資料包時，會將自己對當前時間的估計儲存在資料包中，然後返回該資料包。當接收到回覆時，接收者再次記錄其自身的接收時間，以便估計該分組的傳送時間。

可以使用這些時間差異來估計資料包從伺服器傳輸到請求者所需的時間。在對當前時間進行估計時，該往返時間被考慮在內。往返時間越短，當前時間的估計就越準確。

在多次進行協商資料包交換之前，不會接受該時間。將一些基本值放入多級濾波器，以估計樣本品質。通常，NTP客戶端與伺服器同步大約需要5分鐘。有趣的是，對於根據定義完全沒有延遲的本地參考時鐘也是如此。

此外，網路連線品質也影響最終的準確性。具有變化延遲的緩慢且不可預測的網路會對時間同步產生不良影響。

NTP同步需要小於128 ms的時間差。Internet上的典型準確度範圍從5毫秒到100毫秒不等，可能會因網路延遲而異。

NTP流量級別

NTP使用的頻寬是最小的。對等體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。 通過仔細規劃，您可以在通過WAN鏈路的路由器網路中維護此功能。使NTP客戶端與本地NTP伺服器對等，而不是一直通過WAN連線到中央站點核心路由器（即第2層伺服器）。

收斂的NTP客戶端平均每台伺服器使用約0.6位/秒(bps)。

Cisco NTP建議

- 思科建議您使用多個時間伺服器和不同的網路路徑，以便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。
- 根據RFC，NTP實際上設計為允許您輪詢多個不同的時間伺服器並使用複雜的統計分析來得出有效時間，即使您並不確定您輪詢的所有伺服器都具有權威性。NTP估計所有時鐘的錯誤。因此，所有NTP伺服器都會返回時間以及當前錯誤的估計值。當使用多個時間伺服器時，NTP還希望這些伺服器在一段時間內達成一致。
- Cisco實施的NTP不支援第1層服務。您不能連線到無線電時鐘或原子時鐘。Cisco建議從IP Internet上可用的公共NTP伺服器派生網路的時間服務。
- 使所有客戶端交換機能夠定期向NTP伺服器傳送每日時間請求。每個客戶端最多可配置10個伺服器/對等地址，以便實現快速同步。
- 為了降低協定開銷，輔助伺服器通過NTP將時間分配給其餘的本地網路主機。為了提高可靠性，您可以為選定的主機配備不太準確但成本較低的時鐘，以便在主伺服器和/或輔助伺服器或其之間的通訊路徑出現故障時進行備份。
- **ntp update-calendar** - NTP通常只更改系統時鐘。此命令允許NTP更新日曆上的日期/時間資訊

。僅當同步了NTP時間時，更新才會完成。否則，日曆會保留自己的時間，不會受到NTP時間或系統時鐘的影響。請一律在高端路由器上使用。

- **clock calendar-valid** — 此命令宣告日曆資訊有效且已同步。在NTP主機上使用此選項。如果未進行此配置，則具有日曆的高端路由器仍認為其時間不具有權威性，即使它具有NTP主線路。
- 任何超過15的層號都被視為不同步。這就是在時鐘不同步的路由器上，**show ntp status**命令的輸出中看到第16層的原因。如果主機與公共NTP伺服器同步，請確保NTP主機行上的層數比您輪詢的公共伺服器上最高層數高一或二。
- 許多客戶在其Cisco IOS軟體平台上以伺服器模式配置了NTP，並從來自網際網路或無線電時鐘的多個可靠源同步。在內部，當操作大量交換機時，伺服器模式的更簡單替代方案是在交換域中的管理VLAN上啟用廣播模式的NTP。此機制允許Catalyst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。您可以通過兩種方式解決安全問題：控制伺服器更新，思科建議這樣做通過身份驗證

NTP全域性配置命令

```
!--- For the client: clock timezone EST  -5  ????
ntp source loopback 0 ?????
ntp server ip_address key 1
ntp peer ip_address
!--- This is for a peer association. ntp authenticate
ntp authentication-key 1 md5 xxxx
ntp trusted-key 1

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

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

NTP狀態命令

```
show ntp status

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

這是當路由器充當NTP主路由器時Cisco路由器的參考時鐘地址。如果路由器尚未與任何NTP伺服器同步，則路由器會使用此地址作為參考ID。有關配置和命令的詳細資訊，請參閱執行基本系統管理的*配置NTP*部分。

思科探索通訊協定

目的

CDP在所有思科路由器、網橋、接入伺服器和交換機上在第2層（資料鏈路層）上運行。CDP允許網路管理應用發現與已知裝置相鄰的Cisco裝置。特別是，網路管理應用程式可以發現運行較低層透明協定的鄰居。通過CDP，網路管理應用程式可以瞭解相鄰裝置的裝置型別和SNMP代理地址。此功能使應用程式能夠向相鄰裝置傳送SNMP查詢。

與CDP功能關聯的**show**命令可讓網路工程師確定以下資訊：

- 其它相鄰啟用CDP的裝置的模組/埠號
- 相鄰裝置的以下地址：MAC 地址IP 位址埠通道地址
- 相鄰裝置軟體版本
- 有關相鄰裝置的以下資訊：速度雙工VTP域本地VLAN設定

操作概述部分重點介紹了CDP版本2(CDPv2)相對於CDP版本1(CDPv1)的一些增強功能。

操作概述

CDP在支援SNAP的所有LAN和WAN介質上運行。

每個配置CDP的裝置定期向組播地址傳送消息。每個裝置至少通告一個地址，裝置可以在該地址接收SNMP消息。廣告還包含生存時間或儲存時間資訊。此資訊指示接收裝置在丟棄之前保留CDP資訊的時間長度。

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。在令牌環上，使用功能地址c000.0800.0000。每分鐘定期傳送CDP幀。

CDP消息包含一條或多條消息，允許目的裝置收集和儲存有關每個相鄰裝置的資訊。

下表提供了CDPv1支援的引數：

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	傳送更新的介面的第3層地址
3	埠ID	傳送CDP更新的埠
4	功能	按以下方式描述裝置的功能功能： • 路由器：0x01 • SR[1] bridge:0x04 • 交換器:0x08（提供第2層和/或第3層交換） • 主機：0x10 • IGMP條件篩選：0x20 • 網橋或交換機不會在非路由器埠上轉發IGMP報告資料包。
5	版本	包含軟體版本的字串 **注意：show version命令**輸出會顯示相同的資訊。
6	平台	硬體平台，例如WS-C5000、WS-C6009和Cisco RSP[2]

[1] SR = source-route。

[2] RSP =路由交換處理器。

在CDPv2中，引入了額外的型別、長度、值(TLV)。CDPv2支援任何TLV。但是此表提供的引數在交換環境中特別有用，並且Catalyst軟體也使用此引數。

當交換機運行CDPv1時，交換機將丟棄CDPv2幀。當交換機運行CDPv2並在介面上收到CDPv1幀時，除了CDPv2幀外，交換機開始從該介面傳送CDPv1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，如果埠不是中繼，則埠所在的VLAN幀將保持未標籤狀態。這通常稱為本徵VLAN。
11	全/半雙工	此TLV包含傳送埠的雙工設定。
14	裝置VLAN-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	連線裝置預期消耗的最大功率(mW)。
17	MTU	用來傳輸CDP幀的介面的MTU。
18	擴展信任	表示連線埠處於擴充信任模式。
19	不可信埠的COS	用於標籤在連線的交換裝置的不可信埠上接收的所有資料包的服務類別(CoS)值。
20	系統名稱	裝置的完全限定域名（0，如果未知）。
25	請求的電源	由可供電裝置傳送以便協商合適的功率電平。
26	可用功率	由交換機傳輸。允許可供電裝置協商並選擇適當的功率設定。

CDPv2/乙太網供電

某些交換器（例如Catalyst 6500/6000和4500/4000）能夠透過非遮蔽雙絞線(UTP)纜線為可供電裝置供電。通過CDP（引數16、25、26）接收到的資訊有助於最佳化交換機電源管理。

CDPv2/Cisco IP電話互動

Cisco IP電話為外部連線的10/100 Mbps乙太網裝置提供連線。此連線是通過在IP電話內整合內部三埠第2層交換機實現的。內部交換機埠稱為：

- P0（內部IP電話裝置）
- P1（外部10/100 Mbps連線埠）
- P2（連線到交換機的外部10/100 Mbps埠）

如果設定dot1q存取中繼連線埠，便可以在交換器連線埠上的獨立VLAN上傳輸語音流量。此附加VLAN稱為輔助(CatOS)或語音（Cisco IOS軟體）VLAN。因此，來自IP電話的dot1q標籤流量可在輔助/語音VLAN上傳送，而未標籤流量可通過電話的外部10/100-Mbps埠經由接入VLAN傳送。

Catalyst交換器可以透過CDP將語音VLAN ID通知IP電話(引數–14:裝置VLAN-ID(TLV)。 因此，IP電話使用適當的VLAN ID和802.1p優先順序標籤所有與VoIP相關的資料包。此CDP TLV還用於標識IP電話是否通過裝置ID引數連線。

開發QoS策略時可以利用此概念。您可以將Catalyst交換器設定為以三種方式與IP電話互動：

- 信任裝置Cisco IP電話僅當通過CDP檢測到IP電話時，才有條件地信任CoS。每當通過CDP Parameter-14檢測到IP電話時，埠信任狀態都設定為Trust COS。如果未檢測到IP電話，則埠為Untrusted。
- 擴展信任交換機可以通過CDP（引數–18）通知IP電話信任其外部10/100-Mbps裝置埠收到的所有幀。
- 重寫不可信埠的COS交換機可以通過CDP（引數–19）通知IP電話重寫在其外部10/100-Mbps裝置埠上收到的802.1p CoS值。**注意：**預設情況下，IP電話外部10/100-Mbps埠上接收的所有流量都是不受信任的。

附註： 以下是如何將非Cisco IP電話連線到交換器的組態範例。

附註： 例如，

```
Switch(config)#interface gigabitEthernet 2/1
Switch(config-if)#switchport mode trunk

!--- For example use VLAN 30 for voice VLAN, and VLAN 10 for access VLAN. Switch(config-
if)#switchport trunk native vlan 10
Switch(config-if)#switchport trunk allow vlan 10,30
Switch(config-if)#switchport voice vlan 30
Switch(config-if)#spanning-tree portfast trunk

!--- And besides that enable LLDP as Non Cisco IP Phone do not use CDP. Switch(config)#lldp run
```

思科組態建議

當您排查第2層連線問題時，CDP提供的資訊會非常有用。在支援其操作的所有裝置上啟用CDP。發出以下命令：

- 要在交換機上全域性啟用CDP:
  ```
  Switch(config)#cdp run
  ```
- 若要針對每個連線埠啟用CDP:
  ```
  Switch(config)#interface type slot#/port#
  Switch(config-if)#cdp enable
  ```

配置核對表

全域命令

登入、啟用並進入全域組態模式，以開始交換器組態程式。

```
Switch>enable
Switch#
Switch#configure terminal
Switch(Config)#
```

通用全域性命令（企業範圍）

此全域命令部分列出應用於客戶企業網路中所有交換機的全域命令。

此配置包含新增到初始配置中的建議全域性命令。在將文本複製並貼上到CLI之前，必須更改輸出中的值。核發以下命令，以便應用全域組態：

```
vtp domain domain_name
vtp mode transparent
spanning-tree portfast bpduguard
spanning-tree etherchannel guard misconfig
cdp run
no service pad
service password-encryption
enable secret password
clock timezone EST -5
clock summer-time EDT recurring 1 Sun Apr 3:00 last Sun Oct 3:00
clock calendar-valid
ip subnet-zero
ip host tftpserver your_tftp_server
ip domain-name domain_name
ip name-server name_server_ip_address
ip name-server name_server_ip_address
ip classless
no ip domain-lookup
no ip http server
no logging console
no logging monitor
logging buffered 16384
logging trap notifications
logging facility local7
logging syslog_server_ip_address
logging syslog_server_ip_address
logging source-interface loopback0
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
access-list 98 permit host_ip_address_of_primary_snmp_server
access-list 98 permit host_ip_address_of_secondary_snmp_server
snmp-server community public ro 98
snmp-server community laneng rw 98
snmp-server enable traps entity
snmp-server host host_address traps public
snmp-server host host_address traps public
banner motd ^CCCCC

This is a proprietary system, NOT for public or personal use.  All work products,
communications, files, data or information directly or indirectly created, input
or accessed on this system are and shall become the sole property of the company.
This system is actively monitored and accessed by the company.  By logging onto
this system, the user consents to such monitoring and access.

USE OF THIS SYSTEM WITHOUT OR IN EXCESS OF THE PROPER AUTHORIZATION MAY SUBJECT
```

```
THE USER TO DISCIPLINE AND/OR CIVIL AND CRIMINAL PENALTIES

^C
line console 0
exec-timeout 0 0
password cisco
login
transport input none
line vty 0 4
exec-timeout 0 0
password cisco
login
length 25
clock calendar-valid
ntp server ntp_server_ip_address
ntp server ntp_server_ip_address
ntp update-calendar
```

特定於每個交換機機箱的全域性命令

本節中的全域性命令特定於網路中安裝的每個交換機機箱。

機箱特定配置變數

若要設定日期和時間，請發出以下命令：

```
Switch#clock set hh:mm:ss day month year
```

要設定裝置主機名，請發出以下命令：

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Cat6500
```

若要設定用於管理的回送介面，請發出以下命令：

```
CbrCat6500(config)#interface loopback 0
Cat6500(config-if)#description Cat6000 - Loopback address and Router ID
Cat6500(config-if)#ip address ip_address subnet_mask
Cat6500(config-if)#exit
```

若要顯示Supervisor Engine Cisco IOS軟體版本，請發出以下命令：

```
Cbrcat6500#show version | include IOS
IOS (tm) MSFC Software (C6MSFC-DSV-M), Version 12.1(13)E9, EARLY DEPLOYMENT RELE
ASE SOFTWARE (fc1)
cat6500#
```

要顯示MSFC引導檔案修訂版，請發出以下命令：

```
Cat6500#dir bootflash:
```

```
Directory of bootflash:/
 1 -rw- 1879040 Aug 19 2003 19:03:29 c6msfc-boot-mz.121-19.E1a

15990784 bytes total (14111616 bytes free
```

要指定SNMP伺服器聯絡資訊和位置，請發出以下命令：

```
Cat6500(config)#snmp-server contact contact_information
Cat6500(config)#snmp-server location location_of_device
```

若要將啟動組態從現有Supervisor Engine複製到新的Supervisor Engine，可能會遺失一些組態，例如現有Supervisor介面上的組態。思科建議將組態複製到文字檔中，並將其貼上到主控台中，以便檢視是否有任何組態問題。

介面命令

思科功能連線埠型別

Cisco IOS軟體中的交換機埠稱為介面。Cisco IOS軟體中有兩種介面模式：

- 第3層路由介面
- 第2層交換機介面

介面功能是指連線埠的設定方式。埠配置可以是：

- 路由介面
- 交換式虛擬介面(SVI)
- 接入埠
- 中繼
- 乙太通道
- 以下各項的組合

介面型別是指連線埠型別。連線埠型別可以是：

- FE
- GE
- 連線埠通道

以下清單簡要說明不同的Cisco IOS軟體介面功能：

- 路由物理介面（預設） — 預設情況下，交換機上的每個介面都是路由的第3層介面，類似於任何思科路由器。路由介面必須位於唯一的IP子網上。
- Access switch port interface — 此功能用於將介面置於同一個VLAN中。必須將連線埠從路由介面轉換為交換介面。
- SVI - SVI可以與包含用於InterVLAN路由的接入交換機埠的VLAN關聯。當需要不同VLAN上接入交換機埠之間的路由或網橋時，請將SVI配置為與VLAN關聯。
- Trunk switch port interface — 此功能用於將多個VLAN傳輸到另一台裝置。必須將連線埠從路由介面轉換為主幹交換器連線埠。
- EtherChannel - EtherChannel用於將單個埠捆綁到單個邏輯埠中，以實現冗餘和負載平衡。

思科功能埠型別建議

使用本節中的資訊可幫助確定要應用於介面的引數。

注意：在可能的情況下會合併某些特定於介面的命令。

自動交涉

在下列任一情況下，請勿使用自動交涉：

- 適用於支援交換機和路由器等網路基礎設施裝置的埠
- 對於其他非臨時終端系統（如伺服器和印表機）

手動配置速度和雙工這些10/100 Mbps鏈路配置。這些配置通常為100 Mbps全雙工：

- 100 MB鏈路交換機到交換機
- 100 MB鏈路交換機到伺服器
- 100 MB鏈路交換機到路由器

您可以透過以下方式設定這些設定：

```
Cat6500(config-if)#interface [type] mod#/port#
Cat6500(config-if)#speed 100
Cat6500(config-if)#duplex full
```

思科建議終端使用者使用10/100 Mbps鏈路配置。移動工作者和臨時主機需要自動協商，如以下示例所示：

```
Cat6500(config-if)#interface [type] mod#/port#
Cat6500(config-if)#speed auto
```

Gigabit介面的預設值為。但發出以下命令以確保啟用自動交涉。思科建議啟用Gigabit交涉：

```
Cat6500(config-if)#interface gigabitethernet mod#/port#
Cat6500(config-if)#no speed
```

生成樹根

考慮網路設計，確定最適合作為每個VLAN根的交換機。通常，選擇位於網路中間的強大交換機。將根網橋置於網路中心，並將根網橋直接連線到伺服器和路由器。此設定通常會減少從客戶端到伺服器和路由器的平均距離。請參閱擴充樹通訊協定問題和相關設計考量以瞭解更多資訊。

若要強制交換器成為指定VLAN的根，請發出以下命令：

```
Cat6500(config)#spanning-tree vlan vlan_id root primary
```

生成樹PortFast

PortFast會繞過存取連線埠上的正常跨距樹狀目錄作業，以便加快終端站連線到交換器時發生的初始連線延遲。有關PortFast的詳細資訊，請參閱使用PortFast和其他命令修復工作站啟動連線延遲。

對於連線到單個主機的所有已啟用接入埠，請將STP PortFast設定為on。範例如下：

```
Cat6500(config-if)#interface [type] mod#/port#
Cat6500(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION
%Portfast has been configured on FastEthernet3/1 but will only have effect
when the interface is in a non-trunking mode.
```

UDLD

僅在光纖連線的基礎架構埠或銅纜乙太網電纜上啟用UDLD，以便監控電纜的物理配置。核發以下命令，以便啟用UDLD:

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#udld enable
```

VLAN配置資訊

使用以下命令配置VLAN:

```
Cat6500(config)#vlan vlan_number
Cat6500(config-vlan)#name vlan_name
Cat6500(config-vlan)#exit
Cat6500(config)#spanning-tree vlan vlan_id
Cat6500(config)#default spanning-tree vlan vlan_id
```

對每個VLAN重複命令，然後退出。發出以下命令：

```
Cat6500(config)#exit
```

發出以下命令以驗證所有VLAN:

```
Cat6500#show vlan
```

路由SVI

為InterVLAN路由配置SVI。發出以下命令：

```
Cat6500(config)#interface vlan vlan_id
Cat6500(config-if)#ip address svi_ip_address subnet_mask
Cat6500(config-if)#description interface_description
Cat6500(config-if)#no shutdown
```

對包含路由SVI的每個介面函式重複這些命令，然後退出。發出以下命令：

```
Cat6500(config-if)#^Z
```

路由的單個物理介面

發出以下命令，以設定預設路由第3層介面：

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#ip address ip_address subnet_mask
Cat6500(config-if)#description interface_description
```

對包含路由物理介面的每個介面函式重複這些命令，然後退出。發出以下命令：

```
Cat6500(config-if)#^Z
```

路由EtherChannel(L3)

若要在第3層介面上設定EtherChannel，請發出本節中的命令。

請透過以下方式設定邏輯連線埠通道介面：

```
Cat6500(config)#interface port-channel port_channel_interface_#
Cat6500(config-if)#description port_channel_description
Cat6500(config-if)#ip address port_channel_ip_address subnet_mask
Cat6500(config-if)#no shutdown
```

對構成該特定通道的連線埠執行本節中的步驟。將剩餘資訊套用連線埠通道，如以下範例所示：

```
Cat6500(config)#interface range [type] mod/port_range
Cat6500(config-if)#channel-group 1-64 mode [active | auto | desirable | on | passive]
Cat6500(config-if)#no shutdown
Cat6500(config-if)#^Z
```

註：設定EtherChannel後，應用於連線埠通道介面的設定會影響EtherChannel。應用於LAN連線埠的組態僅影響應用組態的LAN連線埠。

含中繼的EtherChannel(L2)

請透過以下方式設定用於中繼的第2層EtherChannel:

```
Cat6500(config)#interface port-channel port_channel_interface_#
Cat6500(config-if)#switchport
Cat6500(config-if)#switchport encapsulation encapsulation_type
Cat6500(config-if)#switchport trunk native vlan vlan_id
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

僅對構成該特定通道的連線埠執行本節中的步驟。

```
Cat6500(config)#interface range [type] mod/port_range
Cat6500(config-if)#channel-group 1-64 mode [active | auto | desirable | on | passive]
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

註：設定EtherChannel後，應用於連線埠通道介面的設定會影響EtherChannel。應用於LAN連線埠的組態僅影響應用組態的LAN連線埠。

檢驗是否建立了所有EtherChannel和trunk。範例如下：

```
Cat6500#show etherchannel summary
Cat6500#show interface trunk
```

存取連線埠

如果介面功能是設定為單一介面的存取連線埠，請發出以下命令：

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#switchport mode access
Cat6500(config-if)#switchport access vlan vlan_id
Cat6500(config-if)#exit
```

對需要配置為第2層交換機埠的每個介面重複這些命令。

如果要將交換器連線埠連線到終端站，請發出以下命令：

```
Cat6500(config-if)#spanning-tree portfast
```

中繼埠（單個物理介面）

如果介面功能是設定為單一介面的主干連線埠，請發出以下命令：

```
Cat6500(config)#interface [type] mod#/port#
Cat6500(config-if)#switchport
Cat6500(config-if)#switchport trunk encapsulation dot1q
Cat6500(config-if)#switchport trunk native vlan vlan_id
Cat6500(config-if)#no shutdown
Cat6500(config-if)#exit
```

對需要配置為中繼埠的每個介面功能重複這些命令。

密碼資訊

發出以下命令獲取密碼資訊：

```
Cat6500(config)#service password-encryption
Cat6500(config)#enable secret password

CbrCat6500(config)#line con 0
```

```
Cat6500(config-line)#password password

CbrCat6500(config-line)#line vty 0 4
Cat6500(config-line)#password password
Cat6500(config-line)#^Z
```

儲存組態

發出以下命令以儲存組態：

```
Cat6500#copy running-config startup-config
```

Cisco IOS軟體版本12.1(13)E中的新軟體功能

有關IP電話支援的詳細資訊，請參閱配置Cisco IP電話支援。

請參閱網路型應用程式辨認和分散式網路型應用程式辨識，以取得更多有關適用於LAN連線埠的網路型應用程式辨識(NBAR)的資訊。

附註：

- MSFC2上的軟體支援LAN埠的NBAR。
- PFC2為配置NBAR的LAN埠上的輸入ACL提供硬體支援。
- 啟用PFC QoS後，通過配置NBAR的LAN埠的流量會通過入口和出口隊列以及丟棄閾值。
- 啟用PFC QoS時，MSFC2將輸出服務類別(CoS)設定為輸出IP優先順序。
- 流量通過輸入隊列後，所有流量都會在您配置NBAR的LAN埠的MSFC2上用軟體處理。
- 使用Cisco IOS軟體版本12.1(6)E及更高版本的FlexWAN介面上提供分散式NBAR。

NetFlow資料輸出(NDE)增強功能包括：

- Destination-source-interface和full-interface流掩碼
- PFC2的NDE版本5
- 取樣NetFlow
- 用於在NDE記錄中填充這些附加欄位的選項：下一跳路由器的IP地址輸入介面SNMP ifIndex輸出介面SNMP ifIndex源自治系統編號

有關這些增強功能的詳細資訊，請參閱配置NDE。

其他功能增強包括：

- 設定UDLD
- 配置VTP
- 使用WCCP配置Web快取服務

這些命令是新命令：

- **備用延遲最小重新載入**
- **連結反跳動**
- **vlan內部分配策略{升序 |降序}**
- **system jumbomtu**
- **clear catalyst6000流量計**

以下命令是增強型命令：

- **show vlan internal usage** — 此命令經過增強，包括WAN介面使用的VLAN。
- **show vlan id** — 此命令經過增強，可支援輸入範圍的VLAN。
- **show l2protocol-tunnel** — 此命令經過增強以支援VLAN ID的條目。

Cisco IOS軟體版本12.1(13)E支援以下軟體功能，這些功能先前在Cisco IOS軟體版本12.1 EX版本中支援：

- 配置第2層EtherChannel，包括不同配備DFC的交換模組上的介面請參閱Cisco錯誤ID CSCdt27074 (僅限註冊客戶)的12.1(13)E版中已解決的一般警告。
- 路由處理器備援Plus(RPR+)備援請參閱設定RPR或RPR+ Supervisor Engine備援。**註：在**Cisco IOS軟體版本12.1(13)E和更新版本中，RPR和RPR+備援功能取代了增強型高系統可用性(EHSA)備援。
- 4,096個第2層VLAN請參閱設定VLAN。**註：**Cisco IOS軟體版本12.1(13)E和更高版本支援配置4,096個第3層VLAN介面。使用Supervisor Engine II或Supervisor Engine I，在MSFC2上配置總共不超過2,000個第3層VLAN介面和第3層埠。在MSFC上配置總共不超過1,000個第3層VLAN介面和第3層埠。
- IEEE 802.1Q通道請參閱設定IEEE 802.1Q通道和第2層通訊協定通道。
- IEEE 802.1Q協定隧道請參閱設定IEEE 802.1Q通道和第2層通訊協定通道。
- IEEE 802.1s多生成樹(MST)請參閱配置STP和IEEE 802.1s MST。
- IEEE 802.1w快速STP(RSTP)請參閱配置STP和IEEE 802.1s MST。
- IEEE 802.3ad LACP請參閱設定第3層和第2層EtherChannel。
- PortFast BPDU過濾請參閱配置STP功能。
- 自動建立第3層VLAN介面以支援VLAN ACL(VACL)請參閱配置網路安全。
- VACL捕獲埠可以是任何VLAN中的任何第2層乙太網埠請參閱配置網路安全。
- 可在單個物理第3層埠上配置的MTU大小請參閱介面組態概觀。
- 將SPAN目的地連線埠設定為主幹，以便所有SPAN流量都進行標籤請參閱設定本地和遠端SPAN。

相關資訊

- **工具與資源 — Cisco Systems**
- **交換器產品支援**
- **LAN 交換技術支援**
- **技術支援與文件 - Cisco Systems**