Cisco Catalyst第3層固定組態交換器上的第2層安全功能組態範例

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[相關產品](#)
[慣例](#)
[背景資訊](#)
[設定](#)
[網路圖表](#)
[連線埠安全性](#)
[DHCP窺探](#)
[動態ARP檢測](#)
[IP來源防護](#)
[驗證](#)
[疑難排解](#)
[相關資訊](#)

簡介

本檔案為部分第2層安全功能(例如連線埠安全、DHCP窺探、動態位址解析通訊協定(ARP)檢查和IP來源防護)提供組態範例，這些功能可在Cisco Catalyst第3層固定組態交換器上實作。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據版本12.2(25)SEC2的Cisco Catalyst 3750系列交換器。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

相關產品

此組態也可以用於以下硬體：

- Cisco Catalyst 3550 系列交換器
- Cisco Catalyst 3560 系列交換器
- Cisco Catalyst 3560-E系列交換器
- Cisco Catalyst 3750-E系列交換器

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

與路由器類似，第2層和第3層交換機都有各自的網路安全要求。與路由器一樣，交換機也容易受到許多第3層攻擊。但是，一般而言，交換機和OSI參考模型的第2層會受到不同方式的網路攻擊。其中包括：

- **內容可定址儲存器(CAM)表溢位**內容可定址儲存器(CAM)表的大小有限。如果在其它條目過期之前在CAM表中輸入了足夠的條目，則CAM表將被填滿，直到不能接受任何新條目。通常，網路入侵者會用大量無效的源媒體訪問控制(MAC)地址泛洪交換機，直到CAM表填滿。發生這種情況時，交換機將用傳入流量泛洪所有埠，因為它在CAM表中找不到特定MAC地址的埠號。從本質上講，交換機就像一個集線器。如果入侵者不保持源地址泛洪，交換機最終會從CAM表中超時較舊的MAC地址條目，並開始再次像交換機一樣運行。CAM表溢位僅泛洪本地VLAN內的流量，因此入侵者只能看到其連線的本地VLAN內的流量。通過在交換機上配置埠安全，可以緩解CAM表溢位攻擊。此選項適用於指定特定交換器連線埠上的MAC位址，或是指定交換器連線埠可以得知的MAC位址數量。在連線埠上偵測到無效的MAC位址時，交換器可能會封鎖有問題的MAC位址，或關閉連線埠。對於生產環境來說，交換機埠上的MAC地址規格太難管理了。可管理對交換器連線埠上MAC位址數量的限制。更具管理可擴充性的解決方案是在交換機上實施動態埠安全。為了實施動態埠安全，請指定要學習的最大MAC地址數。
- **媒體存取控制(MAC)位址欺騙**介質訪問控制(MAC)欺騙攻擊涉及使用另一台主機的已知MAC地址，試圖使目標交換機將發往遠端主機的幀轉發給網路攻擊者。當使用另一台主機的源乙太網地址傳送單個幀時，網路攻擊者會覆蓋CAM表條目，以便交換機將發往該主機的資料包轉發給網路攻擊者。在主機傳送流量之前，不會接收任何流量。當主機發出流量時，CAM表條目會再次重寫，以便它移回原始埠。使用埠安全功能來緩解MAC欺騙攻擊。埠安全提供指定連線到特定埠的系統的MAC地址的功能。此功能也允許您指定在發生埠安全違規時採取的操作。
- **位址解析通訊協定(ARP)欺騙**ARP用於將IP編址對映到同一子網的主機所在的區域網段中的MAC地址。通常，主機發出廣播ARP請求以查詢具有特定IP地址的另一台主機的MAC地址，ARP響應來自其地址與請求匹配的主機。請求的主機然後快取此ARP響應。在ARP協定中，為主機提供了另一個資源來執行未經請求的ARP應答。未經請求的ARP應答稱為無償ARP(GARP)。攻擊者可以惡意利用GARP偽造LAN網段上IP地址的身份。這通常用於在「中間人」攻擊中欺騙兩台主機或進出預設網關的所有流量。手工建立ARP應答時，網路攻擊者可使自己的系統看起來像是傳送者尋求的目的主機。ARP回覆使傳送方將網路攻擊者系統的MAC地址儲存在ARP快取中。此MAC地址也由交換機儲存在其CAM表中。通過這種方式，網路攻擊者將其系統的MAC地址插入到交換機CAM表和傳送方的ARP快取中。這使得網路攻擊者能夠攔截發往他或她正在欺騙的主機的幀。介面配置選單中的抑制計時器可以通過設定條目在ARP快取中停留的時間長度來緩解ARP欺騙攻擊。然而，壓抑計時器本身是不夠的。需要修改所有終端系統上的ARP快取過期時間以及靜態ARP條目。另一個可用於緩解各種基於ARP的網路漏洞的解決方案是將DHCP監聽與動態ARP檢查結合使用。這些Catalyst功能可驗證網路中的ARP資料

包，並允許擷取、記錄和丟棄具有無效MAC地址到IP地址繫結的ARP資料包。DHCP監聽過濾受信任的DHCP消息以提供安全性。然後，這些消息用於構建和維護DHCP監聽繫結表。DHCP監聽將來自任何面向使用者的埠（不是DHCP伺服器埠）的DHCP消息視為不可信。從DHCP監聽的角度來看，這些不信任面向使用者的埠不得傳送DHCP伺服器型別響應，如DHCPOFFER、DHCPPACK或DHCPNAK。DHCP監聽繫結表包含與交換機的本地不可信介面對應的MAC地址、IP地址、租用時間、繫結型別、VLAN編號和介面資訊。DHCP監聽繫結表不包含與受信任介面互連的主機的資訊。不可信介面是配置為從網路或防火牆外部接收消息的介面。可信介面是配置為僅接收來自網路內部的消息的介面。DHCP監聽繫結表可以包含動態和靜態MAC地址到IP地址的繫結。動態ARP檢測根據儲存在DHCP監聽資料庫中的有效MAC地址與IP地址繫結確定ARP資料包的有效性。此外，動態ARP檢測可以根據使用者可配置的訪問控制清單(ACL)來驗證ARP資料包。 這樣可檢查使用靜態配置的IP地址的主機的ARP資料包。動態ARP檢測允許使用每個埠和VLAN訪問控制清單(PACL)將特定IP地址的ARP資料包限製為特定MAC地址。

- **動態主機設定通訊協定(DHCP)匱乏**DHCP耗竭攻擊通過廣播帶有偽裝MAC地址的DHCP請求來起作用。如果傳送了足夠的請求，網路攻擊者可能會在一段時間內耗儘可用於DHCP伺服器的地址空間。然後，網路攻擊者可以在其系統上設定非法DHCP伺服器，並響應來自網路客戶端的新DHCP請求。通過在網路上放置非法DHCP伺服器，網路攻擊者可以向客戶端提供地址和其他網路資訊。由於DHCP響應通常包含預設網關和DNS伺服器資訊，因此網路攻擊者可以將自己的系統用作預設網關和DNS伺服器。這會導致中間人攻擊。但是，引入非法DHCP伺服器不需要耗盡所有DHCP地址。Catalyst系列交換機中的其他功能（例如DHCP監聽）可用於幫助防止DHCP耗竭攻擊。DHCP監聽是一項安全功能，用於過濾不受信任的DHCP消息，並構建和維護DHCP監聽繫結表。繫結表包含的資訊包括MAC地址、IP地址、租用時間、繫結型別、VLAN號以及與交換機的本地不可信介面對應的介面資訊。不可信消息是指從網路或防火牆外部收到的消息。不可信交換機介面配置為從網路或防火牆外部接收此類消息。其他Catalyst交換機功能（如IP源保護）可以針對DHCP耗竭和IP欺騙等攻擊提供額外的防禦。與DHCP監聽類似，IP源防護會在不受信任的第2層埠上啟用。所有IP流量最初都會被阻止，但DHCP監聽進程捕獲的DHCP資料包除外。一旦客戶端從DHCP伺服器收到有效的IP地址，就會將PACL應用到埠。這會將客戶端IP流量限製為繫結中配置的源IP地址。任何源地址不同於繫結中地址的IP流量都會被過濾。

設定

本節提供用於設定連線埠安全性、DHCP窺探、動態ARP檢查和IP來源防護安全功能的資訊。

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

Catalyst 3750交換器的設定包含以下各項：

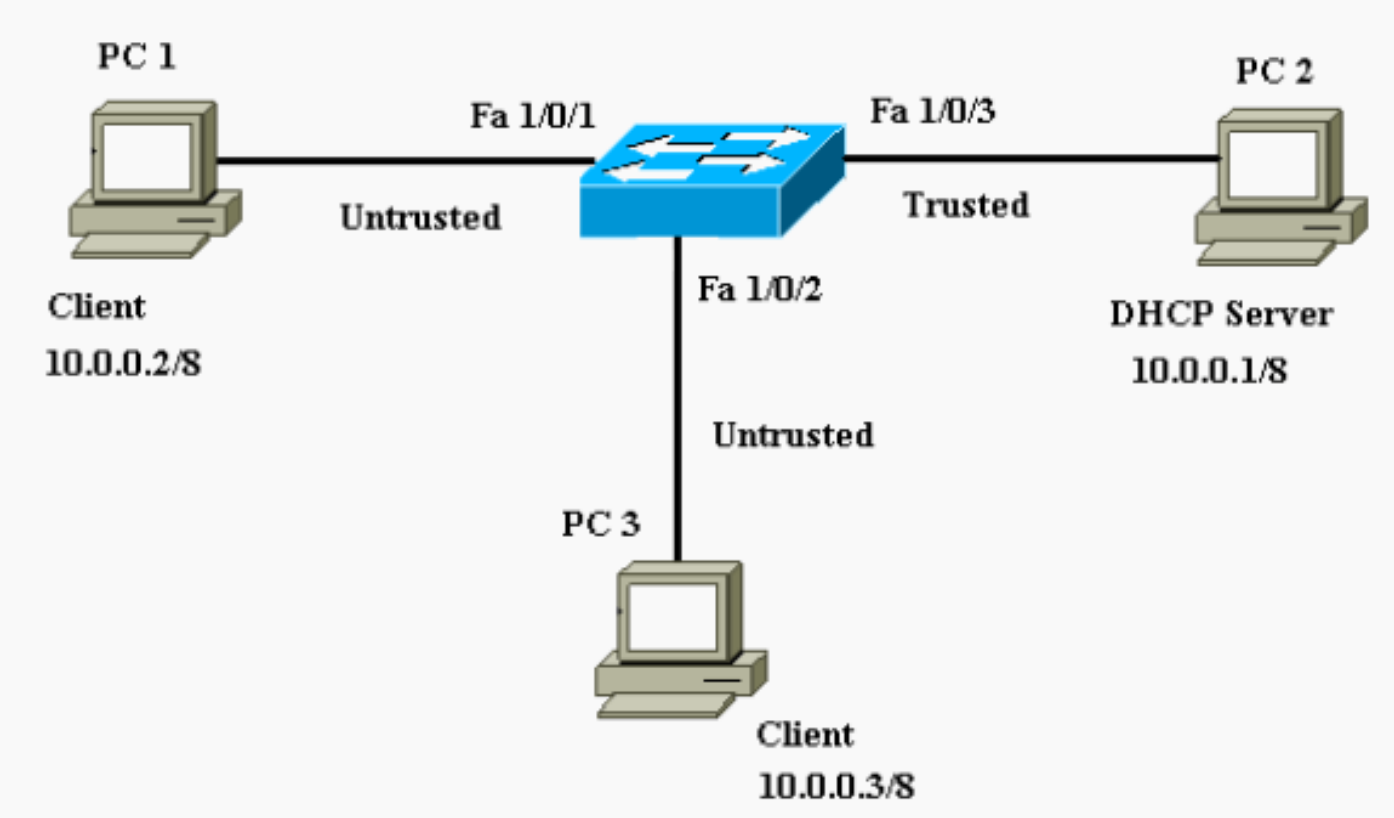
- 連線埠安全性
- DHCP窺探
- 動態ARP檢測
- IP來源防護

網路圖表

本檔案會使用以下網路設定：

- PC 1和PC 3是連線到交換機的客戶端。

- PC 2是連線到交換機的DHCP伺服器。
- 交換器的所有連線埠位於同一個VLAN(VLAN 1)中。
- DHCP伺服器配置為根據客戶端的MAC地址為客戶端分配IP地址。



連線埠安全性

您可以使用連線埠安全功能來限制和識別允許存取連線埠的工作站的MAC位址。這樣會限制對介面的輸入。將安全MAC地址分配給安全埠時，該埠不會轉發源地址位於已定義地址組之外的資料包。如果您將安全MAC地址的數量限製為一個，並分配一個安全MAC地址，則連線到該埠的工作站將獲得該埠的完整頻寬。如果將連線埠設定為安全連線埠，且已達到安全MAC位址的數量上限，則當嘗試存取連線埠的站台的MAC位址與任何已識別的安全MAC位址不同時，會發生資安違規。此外，如果在某個安全連線埠上設定或學習安全MAC位址的站台嘗試存取另一個安全連線埠，則會標籤違規。預設情況下，當超出安全MAC位址的最大數目時，連線埠會關閉。

注意：Catalyst 3750交換器加入堆疊時，新交換器會收到已設定的安全位址。新堆疊成員會從其他堆疊成員下載所有動態安全位址。

有關如何配置埠安全的准則，請參閱配置准則。

這裡顯示的是FastEthernet 1/0/2介面上配置的埠安全功能。預設情況下，該介面的安全MAC地址的最大數量為1。您可以發出**show port-security interface**命令以驗證介面的連線埠安全狀態。

連線埠安全性

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

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


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

註：不應將交換機不同埠上的相同MAC地址配置為安全和靜態MAC地址。

IP電話通過為語音VLAN配置的switchport連線到交換機時，會傳送未標籤的CDP資料包和已標籤的語音CDP資料包。因此，IP電話的MAC地址在PVID和VVID上獲知。如果沒有配置適當數量的安全地址，您可能會收到類似以下消息的錯誤消息：

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

為了解決此問題，您必須將連線埠上允許的最大安全位址數（對於IP電話）設定為二，加上存取VLAN上允許的最大安全位址數。

如需詳細資訊，請參閱設定連線埠安全性。

DHCP窺探

DHCP監聽的作用類似於不可信主機和DHCP伺服器之間的防火牆。您可以使用DHCP監聽區分連線到終端使用者的不可信介面和連線到DHCP伺服器或另一台交換機的可信介面。當交換機在不可信介面上收到資料包，並且該介面屬於已啟用DHCP監聽的VLAN時，交換機將比較源MAC地址和DHCP客戶端硬體地址。如果位址相符（預設值），交換器就會轉送封包。如果地址不匹配，交換機將丟棄資料包。發生以下情況之一時，交換器會捨棄DHCP封包：

- 從DHCP伺服器（例如DHCPOFFER、DHCPACK、DHCPNAK或DHCPLEASEQUERY資料包）收到的資料包來自網路或防火牆外部。
- 在不可信介面上收到資料包，源MAC地址與DHCP客戶端硬體地址不匹配。
- 交換機收到DHCP監聽繫結資料庫中具有MAC地址的DHCPRELEASE或DHCPDECLINE廣播消息，但繫結資料庫中的介面資訊與接收消息的介面不匹配。
- DHCP中繼代理轉發包括非0.0.0.0的中繼代理IP地址的DHCP資料包，或者中繼代理將包括選項82資訊的資料包轉發到不可信埠。

有關如何配置DHCP監聽的指南，請參閱DHCP監聽配置指南。

注意：要使DHCP監聽正常工作，所有DHCP伺服器必須通過受信任介面連線到交換機。

注意：在搭載Catalyst 3750交換器的交換器堆疊中，DHCP窺探在堆疊主機上管理。新交換器加入堆疊時，會收到來自堆疊主機的DHCP窺探組態。當成員離開堆疊時，與交換機關聯的所有DHCP監聽繫結都將過期。

註：為了確保資料庫中的租用時間準確，思科建議您啟用和配置NTP。如果配置了NTP，則僅當交換機系統時鐘與NTP同步時，交換機才將繫結更改寫入繫結檔案。

DHCP監聽功能可以緩解非法DHCP伺服器。發出**ip dhcp snooping**命令，以在交換器上全域啟用DHCP。如果配置了DHCP監聽，則VLAN中的所有埠對於DHCP應答均不受信任。在這裡，只有連線到DHCP伺服器的FastEthernet介面1/0/3被配置為受信任。

DHCP窺探
Cat3750#**conf t** Enter configuration commands, one per line. End with CNTL/Z. Cat3750(config)#**ip dhcp snooping** *!--- Enables DHCP snooping on the switch.*

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

有關詳細資訊，請參閱配置DHCP功能。

動態ARP檢測

動態ARP檢查是一項安全功能，用於驗證網路中的ARP資料包。它會攔截、記錄並丟棄具有無效IP到MAC地址繫結的ARP資料包。此功能可保護網路免受某些中間人攻擊。

動態ARP檢查可確保僅中繼有效的ARP請求和響應。交換機執行以下活動：

- 攔截不可信埠上的所有ARP請求和響應
- 在更新本地ARP快取或將資料包轉發到適當的目標之前，驗證每個截獲的資料包都具有有效的IP到MAC地址繫結
- 丟棄無效ARP資料包

動態ARP檢測根據儲存在可信資料庫（DHCP監聽繫結資料庫）中的有效IP到MAC地址繫結確定ARP資料包的有效性。如果在VLAN和交換機上啟用了DHCP監聽，則此資料庫由DHCP監聽構建。如果在受信任的介面上收到ARP資料包，交換機將轉發該資料包，而不進行任何檢查。在不受信任的介面上，交換機只有在資料包有效時才轉發資料包。

在非DHCP環境中，動態ARP檢測可以根據使用者為具有靜態配置IP地址的主機配置的ARP ACL驗證ARP資料包。您可以發出**arp access-list**全域組態指令來定義ARP ACL。ARP ACL優先於

DHCP監聽繫結資料庫中的條目。只有當您發出**ip arp inspection filter vlan**全域性配置命令來配置ACL時，交換機才會使用ACL。交換機首先將ARP資料包與使用者配置的ARP ACL進行比較。如果ARP ACL拒絕ARP資料包，則交換機也會拒絕該資料包，即使由DHCP監聽填充的資料庫中存在有效的繫結。

有關如何配置動態ARP檢測的指南，請參閱動態ARP檢測配置指南。

發出**ip arp inspection vlan**全域性配置命令，以便基於每個VLAN啟用動態ARP檢測。在這裡，只有連線到DHCP伺服器的FastEthernet介面1/0/3使用**ip arp inspection trust**命令配置為受信任。必須啟用DHCP監聽才能允許具有動態分配IP地址的ARP資料包。有關DHCP監聽配置資訊，請參閱本文檔的DHCP監聽部分。

動態ARP檢測

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

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

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

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

有關詳細資訊，請參閱配置動態ARP檢測。

IP來源防護

IP源保護是一項安全功能，可根據DHCP監聽繫結資料庫和手動配置的IP源繫結過濾流量，以限制非路由第2層介面上的IP流量。您可以使用IP源防護來防止主機嘗試使用其鄰居的IP地址時引起的流量攻擊。IP源保護可防止IP/MAC欺騙。

在不可信介面上啟用DHCP監聽時，可以啟用IP源保護。在介面上啟用IP源保護後，交換機將阻止在該介面上接收的所有IP流量，但DHCP監聽允許的DHCP資料包除外。埠ACL應用於介面。埠ACL僅允許IP源繫結表中具有源IP地址的IP流量，並拒絕所有其他流量。

IP源繫結表具有通過DHCP監聽獲取或手動配置的繫結（靜態IP源繫結）。 此表中的條目具有IP地址、其關聯的MAC地址及其關聯的VLAN編號。僅當啟用IP源保護時，交換機才使用IP源繫結表。

您可以使用源IP地址過濾或源IP和MAC地址過濾來配置IP源防護。通過此選項啟用IP源保護後，將

根據源IP地址過濾IP流量。當源IP地址與DHCP監聽繫結資料庫中的條目或IP源繫結表中的繫結匹配時，交換機將轉發IP流量。通過此選項啟用IP源保護時，將根據源IP和MAC地址過濾IP流量。僅當源IP和MAC地址與IP源繫結表中的條目匹配時，交換機才會轉發流量。

注意：僅第2層埠（包括接入埠和中繼埠）支援IP源保護。

有關如何配置IP源防護的指南，請參閱IP源防護配置指南。

這裡使用**ip verify source**指令在FastEthernet 1/0/1介面上設定具有來源IP篩選的IP來源防護。在VLAN上啟用具有來源IP過濾的IP來源防護時，必須在介面所屬的存取VLAN上啟用DHCP窺探。發出**show ip verify source**命令，以驗證交換器上的IP來源防護組態。

IP來源防護

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

如需詳細資訊，請參閱瞭解IP來源防護。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- 使用專用VLAN和VLAN訪問控制清單保護網路
- LAN 產品支援
- LAN 交換技術支援
- 技術支援與文件 - Cisco Systems