目录

简介

本文档为可在 Cisco Catalyst 第 3 层固定配置交换机上实施的某些第 2 层安全功能，如端口安全、DHCP 监听、动态地址解析协议 (ARP) 检测和 IP 源防护，提供示例配置。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于 12.2(25)SEC2 版本的 Cisco Catalyst 3750 系列交换机。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

相关产品

此配置也可用于以下硬件：

- Cisco Catalyst 3550 系列交换机
- Cisco Catalyst 3560 系列交换机
- Cisco Catalyst 3560-E 系列交换机
- Cisco Catalyst 3750-E 系列交换机

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

与路由器类似，第 2 层和第 3 层交换机也有各自的网络安全需求。与路由器一样，交换机同样容易遭受许多第 3 层攻击。但总体说来，交换机和 OSI 参考模型第 2 层受到的网络攻击的表现形式并不相同。这些新发展包括：

- **内容可寻址内存 (CAM) 表溢出**内容可寻址内存 (CAM) 表的大小有限。如果在其他条目过期之前，在 CAM 表中输入足够的条目，CAM 表将会填满，以致无法接受新条目。通常，网络入侵者会向交换机发送大量无效源媒体访问控制 (MAC) 地址，直到 CAM 表被填满。如果出现这种情况，由于无法在 CAM 表中找到特定 MAC 地址的端口号，交换机的所有端口都会充斥着传入流量。交换机实际上是在起类似于集线器的作用。如果入侵者无法维持无效源 MAC 地址泛洪，交换机最终会使 CAM 表中较旧的 MAC 地址条目超时，并重新开始正常运行。由于 CAM 表溢出仅泛洪本地 VLAN 中的流量，因此入侵者只能查看其连接的本地 VLAN 中的流量。在交换机上配置端口安全可以防范 CAM 表溢出攻击。特定交换机端口上的 MAC 地址规范或可由交换机端口识别的 MAC 地址数量规范可采用此选项。如果在端口上检测到无效 MAC 地址，交换机会阻止恶意 MAC 地址或关闭端口。在生产环境中，交换机端口上的 MAC 地址规范是一种非常难以管理的解决方案。相对而言，限制交换机端口上的 MAC 地址数量更易于管理。一种在管理上更具可扩展性的解决方案，是在交换机上实施动态端口安全。要实施动态端口安全，请指定可识别的 MAC 地址的最大数量。
- **媒体访问控制 (MAC) 地址伪装**媒体访问控制 (MAC) 伪装攻击是指试图使用另一主机的已知 MAC 地址，欺骗目标交换机将发送给远程主机的帧转发给网络攻击者。使用另一主机的源以太网地址传送单个帧时，网络攻击者会覆盖 CAM 表条目，导致交换机将发送给该主机的数据包转发给网络攻击者。在该主机发送流量之前，它不会收到任何流量。主机送出流量时，会再次重写 CAM 表条目，使之返回到原始端口。请使用端口安全功能防范 MAC 伪装攻击。使用端口安全功能可指定连接到特定端口的系统的 MAC 地址。使用此功能还可指定发生端口安全违规时应采取的操作。
- **地址解析协议 (ARP) 伪装**ARP 用于在相同子网的主机所在的局域网段中将 IP 编址映射为 MAC 地址。通常，主机会送出一个广播 ARP 请求，查找特定 IP 地址的另一主机的 MAC 地址，而地址与请求相匹配的主机则会进行 ARP 响应。然后，发出请求的主机会缓存此 ARP 响应。同时，ARP 协议会提供另一配置，以便主机执行未经请求的 ARP 回复。未经请求的 ARP 回复称为无故 ARP (GARP)。GARP 可能会被攻击者恶意利用，用于伪装成 LAN 段上的 IP 地址。在“中间人”攻击中，攻击者通常利用此 GARP 在两台主机，或某个默认网关的所有来回流量之间伪装身份。伪造 ARP 回复后，网络攻击者就可以将自己的系统伪装成发送方寻找的目标主机。此类 ARP 回复会导致发送方将网络攻击者系统的 MAC 地址存储在 ARP 缓存中。交换机也会将此 MAC 地址存储在它的 CAM 表中。这样一来，网络攻击者就将自己系统的 MAC 地址插入到了交换机 CAM 表和发送方的 ARP 缓存中。因此，网络攻击者可以拦截那些发送到被其以伪装手段欺骗的主机的帧。在接口配置菜单的 Hold-down Timer 中设置某个条目在 ARP 缓存中保存的时间长度，可以防范 ARP 伪装攻击。然而，Hold-down Timer 本身还不足以防范这种攻击。您还需要修改所有终端系统的 ARP 缓存有效期以及静态 ARP 条目。防范各种基于 ARP 的网络攻击的另一种解决方案，是结合使用 DHCP 监听与动态 ARP 检测。这些 Catalyst 功能用于验证网络中的 ARP 数据包，并允许拦截、记录和丢弃 MAC 地址与 IP 地址绑定无效的 ARP 数据包。DHCP 监听会过滤受信任 DHCP 消息，以确保安全。然后，再使用这些消息建立和维护 DHCP 监听绑定表。DHCP 监听将源自任何面向用户的端口（并非 DHCP 服务器端口）的 DHCP 消息视为不受信任消息。从 DHCP 监听的角度看，这些不受信任、面向用户的端口不得发送 DHCP 服务器类型的响应，如 DHCPOFFER、DHCPACK 或 DHCPNAK。DHCP 监听绑定表中包含 MAC 地址、IP 地址、租用时间、绑定类型、VLAN 编号，以及与交换机的本地不受信任接口对应的接口信息。DHCP 监听绑定表并不包含与受信任接口互联的主

机的相关信息。不受信任接口是指已配置为接收网络或防火墙外部消息的接口。受信任接口是指已配置为仅接收网络内部消息的接口。DHCP 监听绑定表可能包含动态和静态 MAC 地址与 IP 地址的绑定。动态 ARP 检测可根据存储在 DHCP 监听数据库中的有效 MAC 地址与 IP 地址绑定确定 ARP 数据包的有效性。另外，动态 ARP 检测还能根据可由用户配置的访问控制列表 (ACL) 验证 ARP 数据包。这样一来，使用静态配置 IP 地址的主机就可以检测 ARP 数据包。动态 ARP 检测允许使用每端口和 VLAN 访问控制列表 (PACL)，使得特定 IP 地址的 ARP 数据包只能发往特定 MAC 地址。

- **动态主机配置协议 (DHCP) 耗竭**DHCP 耗竭攻击通过广播包含伪装 MAC 地址的 DHCP 请求来实施。如果发送足够多的请求，网络攻击者能够将可供 DHCP 服务器使用的地址空间耗尽一段时间。然后，网络攻击者就可以在自己的系统上设置一个非法 DHCP 服务器，用于响应网络客户端提出的新 DHCP 请求。通过在网络上放置非法 DHCP 服务器，网络攻击者可以为客户端提供地址和其他网络信息。由于 DHCP 响应通常包括默认网关和 DNS 服务器信息，因此，网络攻击者可以将自己的系统伪装成默认网关和 DNS 服务器。这会导致中间人攻击。但是，引入非法 DHCP 服务器不一定需要耗尽所有 DHCP 地址。Catalyst 系列交换机的其他功能，如 DHCP 监听，可用于帮助防御 DHCP 耗竭攻击。DHCP 监听是一项安全功能，它过滤不受信任的 DHCP 消息，并建立和维护 DHCP 监听绑定表。绑定表中包含的信息包括 MAC 地址、IP 地址、租用时间、绑定类型、VLAN 编号，以及与交换机的本地不受信任接口对应的接口信息。不受信任消息是指从网络或防火墙外部收到的消息。不受信任交换机接口是指已配置为接收网络或防火墙外部消息的接口。其他 Catalyst 交换机功能，如 IP 源防护，可以为防范 DHCP 耗竭和 IP 伪装等攻击提供额外的保护。与 DHCP 监听类似，可在不受信任的第 2 层端口上启用 IP 源防护。一开始会阻止所有 IP 流量，由 DHCP 监听进程捕获的 DHCP 数据包除外。客户端从 DHCP 服务器收到有效 IP 地址后，将对端口应用 PACL。这限制了发送到那些在绑定中配置的源 IP 地址的客户端 IP 流量。源地址不同于绑定中地址的任何其他 IP 流量都将被过滤。

配置

在此部分中，您将了解端口安全、DHCP 监听、动态 ARP 检测和 IP 源防护等安全功能的配置信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

Catalyst 3750 交换机的配置包括以下安全功能：

- 端口安全性
- DHCP 监听
- 动态 ARP 检查
- IP 源防护

网络图

本文档使用以下网络设置：

- PC 1 和 PC 3 是连接到交换机的客户端。
- PC 2 是连接到交换机的 DHCP 服务器。
- 交换机的所有端口均处在同一 VLAN (VLAN 1) 中。
- DHCP 服务器配置为根据客户端的 MAC 地址向其分配 IP 地址。

端口安全性

您可以使用端口安全功能限制和标识允许访问端口的站点的 MAC 地址。这将限制对接口的输入。如果为安全端口分配了安全 MAC 地址，那么当数据包的源地址不是已定义地址组中的地址时，端口不会转发这些数据包。如果您将安全 MAC 地址的数量限制为一个，并且只分配单个安全 MAC 地址，则可以确保连接到该端口的工作站获得端口的全部带宽。如果端口已配置为安全端口且安全 MAC 地址的数量已达最大值，同时试图访问该端口的站点的 MAC 地址不同于任何已标识的安全 MAC 地址，则会发生安全违规。此外，如果站点在某个安全端口进行安全 MAC 地址的配置或识别，但却试图访问另一安全端口，则也会发生违规。默认情况下，当安全 MAC 地址的数量超出允许的最大值时，端口就会关闭。

注意： 当 Catalyst 3750 交换机加入堆叠时，新交换机会收到已配置的安全地址。所有动态安全地址均由新堆叠成员从其他堆叠成员那里下载。

有关配置端口安全的指南，请参阅配置指南。

此处显示端口安全功能在 FastEthernet 1/0/2 接口上配置。默认情况下，该接口的安全 MAC 地址的最大数量为一。您可以发出 **show port-security interface** 命令来验证接口的端口安全状态。

端口安全性

```
Cat3750#show port-security interface fastEthernet 1/0/2Port
Security              : DisabledPort Status                :
Secure-downViolation Mode             : ShutdownAging Time
: 0 minsAging Type                  : AbsoluteSecureStatic
Address Aging : DisabledMaximum MAC Addresses      : 1Total
MAC Addresses        : 0Configured MAC Addresses    : 0Sticky
MAC Addresses       : 0Last Source Address:Vlan    :
0000.0000.0000:0Security Violation Count    : 0!--- Default
port security configuration on the switch.Cat3750#conf tEnter
configuration commands, one per line.  End with
CNTL/Z.Cat3750(config)#interface fastEthernet
1/0/2Cat3750(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 state00:22:51: %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 down00:22:53: %LINK-3-
UPDOWN: Interface FastEthernet1/0/2, changed state to down!--
- Interface shuts down when a security violation is
detected.Cat3750#show interfaces fastEthernet
1/0/2FastEthernet1/0/2 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 1/0/2Port Security              : EnabledPort
Status                 : Secure-shutdownViolation Mode
: ShutdownAging Time                 : 0 minsAging Type
: AbsoluteSecureStatic Address Aging : DisabledMaximum MAC
Addresses       : 1Total MAC Addresses         : 1Configured
MAC Addresses    : 1Sticky MAC Addresses        : 0Last Source
Address:Vlan    : 0011.8565.4B75:1Security Violation Count    :
1
```

注意： 交换机不同端口的安全和静态 MAC 地址不得配置为相同的 MAC 地址。

IP 电话通过为语音 VLAN 配置的交换机端口连接到交换机时，会发送无标记 CDP 数据包和带标记语音 CDP 数据包。因此，在 PVID 和 VVID 上都可以识别 IP 电话的 MAC 地址。如果没有配置适当数量的安全地址，您可能会收到与以下消息类似的错误消息：

```
Cat3750#show port-security interface fastEthernet 1/0/2Port Security              : DisabledPort Status
: Secure-downViolation Mode             : ShutdownAging Time                : 0 minsAging Type
: AbsoluteSecureStatic Address Aging : DisabledMaximum MAC Addresses      : 1Total MAC Addresses        :
0Configured MAC Addresses    : 0Sticky MAC Addresses       : 0Last Source Address:Vlan    :
0000.0000.0000:0Security Violation Count    : 0!--- Default port security configuration on the
switch.Cat3750#conf tEnter configuration commands, one per line.  End with
CNTL/Z.Cat3750(config)#interface fastEthernet 1/0/2Cat3750(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 state00:22:51: %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 down00:22:53: %LINK-3-UPDOWN: Interface FastEthernet1/0/2, changed state to down!--- Interface
shuts down when a security violation is detected.Cat3750#show interfaces fastEthernet
1/0/2FastEthernet1/0/2 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 1/0/2Port Security              : EnabledPort Status                : Secure-
shutdownViolation Mode             : ShutdownAging Time                : 0 minsAging Type
: AbsoluteSecureStatic Address Aging : DisabledMaximum MAC Addresses      : 1Total MAC Addresses        :
1Configured MAC Addresses    : 1Sticky MAC Addresses       : 0Last Source Address:Vlan    :
0011.8565.4B75:1Security Violation Count    : 1
```

要解决此问题，您必须将端口上允许的安全地址的最大数量设置为 2（适用于 IP 电话），同时还需设置接入 VLAN 上允许的安全地址的最大数量。

有关详细信息，请参阅配置端口安全。

DHCP 监听

DHCP 监听的作用类似于不受信任主机与 DHCP 服务器之间的一个防火墙。您可以使用 DHCP 监听来区分连接到最终用户的不受信任接口与连接到 DHCP 服务器或其他交换机的受信任接口。当不受信任接口上的交换机收到数据包，且该接口属于已启用 DHCP 监听的 VLAN 时，交换机会比较源 MAC 地址和 DHCP 客户端硬件地址。如果地址匹配（默认），交换机会转发数据包。如果地址不

匹配，交换机会丢弃数据包。如果发生下述情况之一，交换机会丢弃 DHCP 数据包：

- 从网络或防火墙外部收到来自 DHCP 服务器的数据包，如 DHCPOFFER、DHCPACK、DHCPNAK 或 DHCPLEASEQUERY 数据包。
- 在不受信任接口上收到数据包，且源 MAC 地址与 DHCP 客户端硬件地址不匹配。
- 交换机收到具有 DHCP 监听绑定数据库中 MAC 地址的 DHCPRELEASE 或 DHCPDECLINE 广播消息，但绑定数据库中的接口信息与接收消息的接口不匹配。
- DHCP 中继代理转发了其中包括中继代理 IP 地址（并非 0.0.0.0）的 DHCP 数据包，或者中继代理将其中包括 option-82 信息的数据包转发到了不受信任端口。

有关如何配置 DHCP 监听的指南，请参阅 DHCP 监听配置指南。

注意： 要使 DHCP 监听正常运行，所有 DHCP 服务器必须通过受信任接口连接到交换机。

注意： 在包含 Catalyst 3750 交换机的交换机堆叠中，DHCP 监听由堆叠主交换机管理。当新交换机加入堆叠时，该交换机会从堆叠主交换机那里收到 DHCP 监听配置。某个成员离开堆叠时，与此交换机关联的所有 DHCP 监听绑定都将会过期。

注意： 为确保数据库中租用时间的准确性，Cisco 建议您启用并配置 NTP。如果已配置 NTP，则只有当交换机系统时钟与 NTP 同步时，交换机才会将绑定更改写入到绑定文件中。

使用 DHCP 监听功能可以防范非法 DHCP 服务器。发出 **ip dhcp snooping** 命令可在交换机上全局启用 DHCP。配置 DHCP 监听后，对 DHCP 回复而言，VLAN 中的所有端口均为不受信任端口。在这里，仅连接到 DHCP 服务器的 FastEthernet 接口 1/0/3 配置为受信任接口。

DHCP 监听

```
Cat3750#conf tEnter 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
1/0/3Cat3750(config-if)#ip dhcp snooping trust!--- Configures
the interface connected to the DHCP server as
trusted.Cat3750#show ip dhcp snoopingSwitch DHCP snooping is
enabledDHCP snooping is configured on following
VLANs:1Insertion of option 82 is disabledOption 82 on
untrusted port is not allowedVerification of hwaddr field is
enabledInterface                    Trusted     Rate limit
(pps)------------------------     -------     ---------------
-FastEthernet1/0/3            yes         unlimited!---
Displays the DHCP snooping configuration for the
switch.Cat3750#show ip dhcp snooping bindingMacAddress
IpAddress        Lease(sec)  Type           VLAN  Interface--
---------------  ----------  ----------  ----------
----  --------------------00:11:85:A5:7B:F5     10.0.0.2
86391       dhcp-snooping  1
FastEtheret1/0/100:11:85:8D:9A:F9     10.0.0.3        86313
dhcp-snooping  1    FastEtheret1/0/2Total 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.
```

有关详细信息，请参阅配置 DHCP 功能。

动态 ARP 检查

动态 ARP 检测是一项安全功能，用于验证网络中的 ARP 数据包。它拦截、记录并丢弃具有 IP 到 MAC 地址的无效绑定的 ARP 数据包。使用此功能可以防止网络受到某些中间人攻击。

动态 ARP 检测可确保仅转发有效 ARP 请求和响应。交换机可执行以下活动：

- 拦截不受信任端口上的所有 ARP 请求和响应
- 验证此类被拦截的数据包的 IP 到 MAC 地址绑定是否均有效，然后更新本地 ARP 缓存，或将数据包转发给相应的目标
- 丢弃无效的 ARP 数据包

动态 ARP 检测可根据受信任数据库（DHCP 监听绑定数据库）中存储的 IP 到 MAC 地址的有效绑定来确定 ARP 数据包的有效性。如果已在 VLAN 和交换机上启用 DHCP 监听，则此数据库可通过 DHCP 监听来构建。如果在受信任接口上收到 ARP 数据包，交换机将在不做任何检查的情况下转发数据包。在不受信任接口上，交换机仅转发有效数据包。

在非 DHCP 环境中，可以根据用户配置的 ARP ACL，通过动态 ARP 检测对使用静态配置 IP 地址的主机的 ARP 数据包进行验证。要定义 ARP ACL，可以发出 **arp access-list** 全局配置命令。ARP ACL 优先于 DHCP 监听绑定数据库中的条目。只有当您发出 **ip arp inspection filter vlan** 全局配置命令来配置 ACL 时，交换机才会使用 ACL。交换机会先将 ARP 数据包与用户配置的 ARP ACL 进行比较。如果 ARP ACL 拒绝 ARP 数据包，则交换机也会拒绝该数据包，即使 DHCP 监听功能填充的数据库中存在有效的绑定，也是如此。

有关如何配置动态 ARP 检测的指南，请参阅动态 ARP 检测配置指南。

可以发出 **ip arp inspection vlan** 全局配置命令在每个 VLAN 上启用动态 ARP 检测。在这里，使用 **ip arp inspection trust** 命令只能将连接到 DHCP 服务器的 FastEthernet 接口 1/0/3 配置为受信任接口。必须启用 DHCP 监听以允许具有动态分配 IP 地址的 ARP 数据包。有关 DHCP 监听配置的信息，请参阅本文档的 DHCP 监听部分。

动态 ARP 检查

```
Cat3750#conf tEnter 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
1/0/3Cat3750(config-if)#ip arp inspection trust!---
Configures the interface connected to the DHCP server as
trusted.Cat3750#show ip arp inspection vlan 1Source Mac
Validation      : DisabledDestination Mac Validation :
DisabledIP 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#
```

有关详细信息，请参阅配置动态 ARP 检测。

IP 源防护

IP 源防护是一项安全功能，可根据 DHCP 监听绑定数据库和手动配置的 IP 源绑定过滤流量，以限制第 2 层非路由接口上的 IP 流量。您可以使用 IP 源防护阻止因主机试图使用其邻居的 IP 地址而导致的流量攻击。IP 源防护可防止 IP/MAC 伪装。

在不受信任接口上启用 DHCP 监听时，您可以启用 IP 源防护。在接口上启用 IP 源防护后，除 DHCP 监听允许的 DHCP 数据包外，交换机会阻止该接口收到的所有 IP 流量。这时会对该接口应用端口 ACL。端口 ACL 仅允许源 IP 地址位于 IP 源绑定表中的 IP 流量，而拒绝所有其他流量。

IP 源绑定表中包含由 DHCP 监听识别的绑定或手动配置的绑定（静态 IP 源绑定）。此表中的条目具有 IP 地址、关联的 MAC 地址和关联的 VLAN 编号。只有在启用 IP 源防护时，交换机才会使用 IP 源绑定表。

您可以使用源 IP 地址过滤或源 IP 及 MAC 地址过滤来配置 IP 源防护。使用此选项启用 IP 源防护时，将基于源 IP 地址过滤 IP 流量。当源 IP 地址与 DHCP 监听绑定数据库中的条目或 IP 源绑定表中的绑定匹配时，交换机将转发 IP 流量。使用此选项启用 IP 源防护时，将基于源 IP 与 MAC 地址过滤 IP 流量。只有当源 IP 和 MAC 地址与 IP 源绑定表中的条目匹配时，交换机才会转发流量。

注意： 仅第 2 层端口（包括接入和中继端口）支持 IP 源防护。

有关如何配置 IP 源防护的指南，请参阅 IP 源防护配置指南。

在这里，可使用 **ip verify source** 命令在 FastEthernet 1/0/1 接口上配置带源 IP 过滤功能的 IP 源防护。在 VLAN 上启用带源 IP 过滤功能的 IP 源防护时，必须在接口所属的接入 VLAN 上启用 DHCP 监听。发出 **show ip verify source** 命令可验证交换机上的 IP 源防护配置。

IP 源防护

```
Cat3750#conf tEnter 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 1/0/1Cat3750(config-if)#ip verify source!---
Enables IP source guard with source IP filtering.Cat3750#show
ip verify sourceInterface  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#
```

有关详细信息，请参阅了解 IP 源防护。

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 使用专用 VLAN 和 VLAN 访问控制列表保护网络安全
- LAN 产品支持
- LAN 交换技术支持
- 技术支持和文档 - Cisco Systems