

技术概要

网络保护：交换机访问控制功能

简介

本文主要介绍HP ProCurve Networking交换机的访问控制安全功能。同时，还提供一些使用模式，以便您了解这些功能的实施过程。欲了解产品配置的最新信息和高级功能，请查阅产品手册：www.procurve.com/customer-care/support/manuals/index.htm

DHCP侦听

目前的网络问题是，用户可能意外或故意将未经授权的动态主机配置协议(DHCP)服务器配置到网络上。因而，通过为这些服务器分配IP地址方案之外的地址或主DHCP服务器已发布的重复地址，对客户端造成拒绝服务攻击。在大型网络中查找恶意DHCP服务器并非易事。

许多ProCurve交换机都通过其DHCP侦听，解决此类问题。此功能通过配置“可信”和“不可信”交换机端口发挥作用。可信端口允许DHCP服务器流量通过，而不可信端口则会对这些数据包予以阻止。当DHCP客户端插入不可信端口时，DHCP侦听数据库将跟踪客户端IP地址和MAC地址映射。该工具对解决DHCP问题十分实用。

```
ProCurve Switch# showDHCP-snooping binding
```

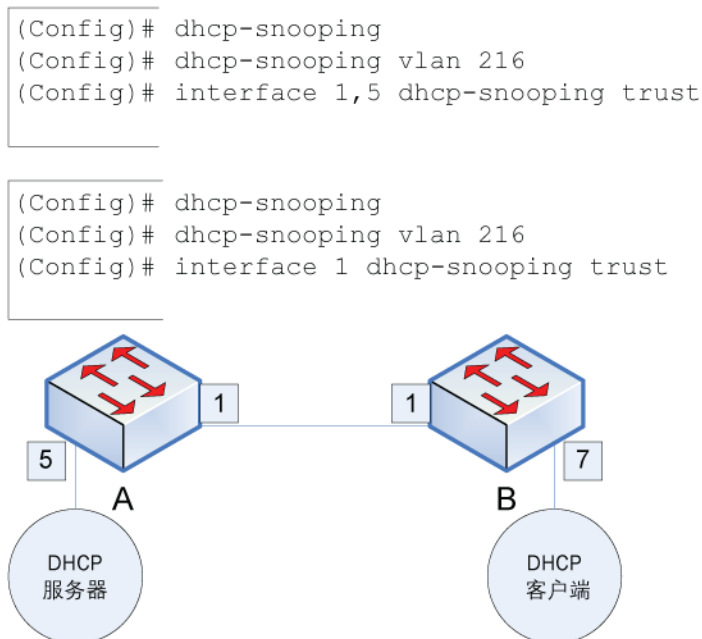
DHCP允许客户端从DHCP服务器获取IP地址。默认情况下，启用DHCP选项82并允许交换机跟踪客户端所连接设备和端口的详细信息。此选项可使DHCP服务能够根据客户端位置分配IP地址。DHCP服务器必须支持DHCP选项82才可使用此功能。

目录	
简介	1
DHCP侦听	1
动态ARP保护	2
动态IP锁定	4
通过IP锁定实现病毒遏制	4
网络身份验证和授权	4
通过IEEE 802.1X的用户身份验证	5
通过web身份验证的用户身份验证	6
通过MAC身份验证的用户身份验证	6

受恶意DHCP服务器威胁的所有交换机和虚拟局域网(VLAN)都应启用DHCP侦听功能。注意：已启用DHCP侦听功能的所有互联交换机端口都应设为“可信”。否则，这些交换机之间的DHCP流量将会丢失。ProCurve建议在网络边缘配置DHCP侦听功能，因为这里最可能连接恶意DHCP服务器。DHCP侦听的租赁表大小为8000个条目。

在图1的示例中，恶意DHCP服务器无法发送DHCP Offer数据包，除非连接可信端口。

图1. DHCP侦听示例



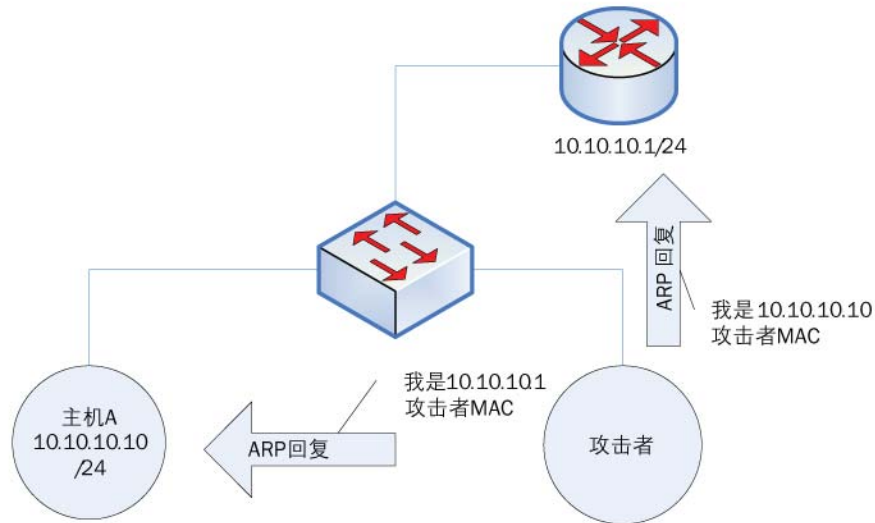
动态ARP保护

以下部分重点介绍有关地址解析协议(ARP)的一些问题。恶意用户通过使用伪MAC-to-IP地址映射填充主机ARP高速缓存，对设备造成拒绝服务攻击。这就叫做ARP缓存投毒，它可以在网络设备的IP地址或端节点上进行。另一个问题是恶意用户可利用ARP变成中间人并拦截数据包。

直接发送ARP回复包到特定端口或整个网络,都可能引起以上这两种攻击。图2是通过ARP回复包进行中间人攻击的示例。

该图中，攻击者可以通过转发HostA的所有数据包到默认网关10.10.10.1/24，拦截数据包。

图2. 通过ARP回复包进行中间人攻击



ProCurve交换机可以通过动态ARP保护，防御这些攻击。该功能通过DHCP侦听数据库将MAC地址动态映射到IP地址发挥作用。使用动态ARP保护时无需配置DHCP侦听，但必须将其在VLAN上启用。

动态ARP保护通过使用可信端口和不可信端口发挥作用。可信端口已禁用保护。该选项可用于连接配置了ARP保护的其他交换机端口。“信赖”这些互联交换机链路非常重要，因为每个交换机都利用自己的数据库进行DHCP侦听和ARP保护。一台交换机不会了解另一台交换机的已知映射，而且还可能阻止其ARP数据包。

边缘端口应该是不可信的。如果客户端没有通过DHCP接收到IP地址，静态MAC则必须配置到交换机上的IP映射。当一台交换机端口不可信时，主机必须有映射可以发送ARP请求或ARP回复包。

另外还应注意，如果选择在一个VLAN上使用ARP保护，交换机可能会由于排除的VLAN而出现系统漏洞。

```
(Config)# arp-protect
(Config)# arp-protect vlan <vlan>
(eth-1)# arp-protect trust <port>
(Config)#IPsource-binding <vlan> <ip address> <mac address> <port>
```

动态IP锁定

动态IP锁定是一个全新的功能，它可以提供基于IP地址级别端口的安全性，防御IP侦听攻击。恶意用户一般通过侦听其IP地址，避开安全控制和避免被跟踪。该功能的覆盖范围包括，从通过源IP地址进行身份验证的应用程序到根据源IP地址批准流量的访问列表(ACL)。

任何要实施IP锁定的VLAN上都必须启用DHCP侦听。可通过DHCP侦听数据库动态获取IP-to-MAC地址映射，或按如下步骤进行静态设置。

```
(Config)#IPsource-lockdown
(Config)#IPsource-lockdown <port-list>
```

静态设置捆绑功能时，可使用以下命令：

```
(config)#IPsource-binding <vlan> <ip> <mac> <port>
```

通过IP锁定实现病毒遏制

病毒遏制(VT)技术功能强大，可以检测和响应实际的病毒和蠕虫攻击。惠普实验室开发的VT技术，通过HP ProCurve Switch 3500yl、5300xl、5400zl、6200yl和8212zl系列交换机的连接速度过滤功能进行实施。此技术通过监测所有IP连接请求发挥作用，并设置了新计算机的连接速度限制。感染了病毒（如众所周知的“Sasser”）的计算机试图感染网络上的更多计算机，因此触发了VT技术做出响应。

恶意用户可能通过使用类似网络“蠕虫”的行为触发VT引擎。启用IP锁定功能可避免恶意用户侦听系带主机IP地址，强制网络在触发病毒遏制之后拦截该IP地址。除部署IP锁定外，VT还可为“白名单”特定的设备提供接口。欲了解有关VT的更多信息，请访问ProCurve网站：www.hp.com/rnd/pdfs/virus_throttling_tech_brief.pdf

网络身份验证和授权

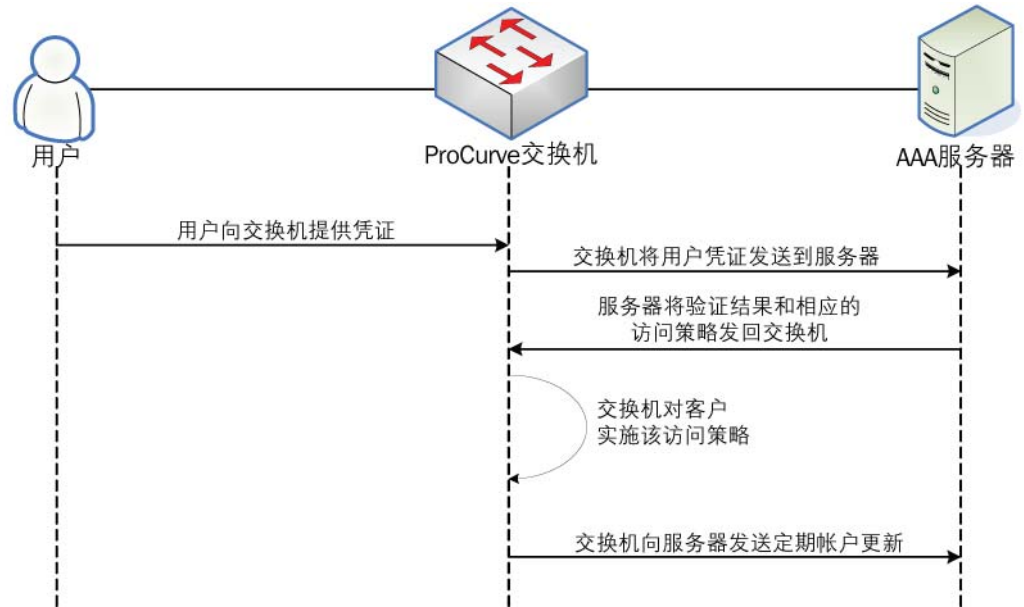
依靠物理访问限制用户访问网络的时代早已过去。网络连接已延伸到了会议室和休息场所，并包括电话和打印机等设备。过去，用户对在这些地点连接计算机访问其所有网络资源十分关注。现在，限制用户访问特定资源变得更有意义。

用户身份验证是限制用户访问网络的一个方法。用户身份验证方法是需要用户向交换机提供一些用户证书，然后交换机根据用户数据库进行验证。身份验证流程还允许验证服务器充当授权机构，并为用户提供访问策略。然后，将这些访问策略应用于用户连接的端口。ProCurve交换机为用户提供的策略如下：

- **VLAN** — 确定用户要连接的网络
- **入口速率限制** — 限制用户发送到网络的流量速率
- **服务质量(QoS)** — 设置用户流量优先级
- **ACL** — 限制用户流量

除进行身份验证和授权外，ProCurve交换机还可将统计更新发送到包含用户统计数据的统计服务器上。该服务器将汇总ProCurve的身份验证、授权和统计(AAA)服务。RADIUS服务器通常被用作AAA服务器。图3显示了该AAA流程的步骤顺序。

图3. 网络AAA流程



用户策略的配置和监测还可以通过HP ProCurve Identity Driven Manager (IDM)得到加强。IDM是HP ProCurve Manager (PCM) Plus软件的一个安全插件。它可以为网络或安全管理员提供图形界面，以便其在网络上应用和实施网络访问策略。这些访问策略可以根据时间安排、位置或用户相关联的组进行实施。此外，IDM还可以简化ProCurve适应性边缘网络访问控制的部署。

ProCurve交换机有三种用户身份验证方法：

- IEEE 802.1X
- Web身份验证
- MAC身份验证

下面，分别介绍每种验证方法。

通过IEEE 802.1X的用户身份验证

IEEE 802.1X为客户端提供了一种网络身份验证方法。下面是在ProCurve交换机上配置IEEE 802.1X的基本配置命令：

```
(config)# aaa port-access authenticator <ports>
(config)# aaa port-access authenticator active
(config)# radius-server host <ip address> key <radius secret>
```

为确保IEEE 802.1X正常运行，每个客户端都必须安装IEEE 802.1X客户端软件（申请者）。该软件将用户证书发送到交换机，然后交换机便可通过网络对用户进行身份验证。IEEE 802.1X的优势在于，可同时对没有安装申请者的客户端进行Web身份验证和MAC身份验证。

通过Web身份验证的用户身份验证

此流程与IEEE 802.1X非常相似，交换机会首先阻止所有未经授权的用户访问网络。当IEEE 802.1X需要客户端的专用软件时，Web身份验证可在客户端通过标准浏览器首次发出Web（HTTP或HTTPS）请求时提供捕获门户。继而，交换机会拦截该初始Web请求，并为用户显示登录页面。用户证书提交给交换机后，交换机将执行与IEEE 802.1X相同的用户身份验证，并获得用户属性（如果证书有效）。以下是启用ProCurve交换机上Web身份验证功能所需的基本配置命令：

```
(config)# aaa port-access web-based <ports>
(config)# radius-server host <ip address> key <radius secret>
```

Web身份验证需要用户在获取网络访问权限之前，打开Web浏览器。

通过MAC身份验证的用户身份验证

如前所述，IEEE 802.1X的部署需要在所有授权客户端安装一个软件。Web身份验证需要所有客户端都有一个用户与捕获门户的互动，以提供用户证书。但网络上的设备既没有交互用户可进行身份验证，也无法安装专用的IEEE 802.1X软件。这样的设备包括一些IP语音(VoIP)电话、打印机和传统服务器。

为使这些设备能够访问网络和根据用户证书提供访问策略配置，ProCurve提供了MAC身份验证。MAC身份验证将客户端的MAC地址作为设备的用户证书，然后将其发送至验证服务器。

```
(config)# aaa port-access mac-based <ports>
(config)# aaa port-access mac-based <ports> addr-format <fmt>
(config)# radius-server host <ip address> key <radius secret>
```

MAC身份验证可以同时与IEEE 802.1X配合使用。例如，可能有一个VoIP电话采用MAC身份验证，连接电话的台式机可同时采用IEEE 802.1X身份验证。MAC身份验证存在两个问题。第一，恶意用户可以侦听端口所连接设备的MAC地址。第二，大量的MAC地址维护工作过于繁琐。



惠普网络“网”者之选

更多信息

欲了解有关HP ProCurve Networking的更多信息，请访问：www.hp.com.cn/network

© Hewlett-Packard Development Company, L.P. 2009年版权所有。本文信息如有更改，恕不另行通知。惠普产品与服务的全部保修内容在此类产品和服务附带的保修单中明确说明。本文信息不得视为额外的保修承诺。惠普对于本文所包含的技术或编辑错误、遗漏概不负责。

4AA0-5708CHP, 2009年3月