

目 录

第 1 章 L3 转发配置	1-1
1.1 三层接口	1-1
1.1.1 三层接口介绍.....	1-1
1.1.2 三层接口配置.....	1-1
1.2 IP 配置	1-2
1.2.1 IPv4、IPv6 介绍.....	1-2
1.2.2 IP 配置.....	1-4
1.2.3 IP 配置举例.....	1-10
1.2.4 IPv6 排错帮助.....	1-15
1.3 IP 转发	1-15
1.3.1 IP 转发介绍.....	1-15
1.3.2 IP 路由聚合配置.....	1-15
1.4 URPF	1-15
1.4.1 URPF 介绍.....	1-15
1.4.2 URPF 配置任务序列.....	1-16
1.4.3 URPF 典型案例.....	1-17
1.4.4 URPF 排错帮助.....	1-18
1.5 ARP	1-19
1.5.1 ARP 介绍.....	1-19
1.5.2 ARP 配置.....	1-19
1.5.3 ARP 转发排错帮助.....	1-20
第 2 章 防 ARP 扫描功能操作配置	2-1
2.1 防 ARP 扫描功能介绍.....	2-1
2.2 防 ARP 扫描配置任务序列.....	2-1
2.3 防 ARP 扫描典型案例.....	2-3
2.4 防 ARP 扫描排错帮助.....	2-4
第 3 章 ARP、ND 绑定配置	3-1
3.1 概述	3-1
3.1.1 ARP（地址解析协议）.....	3-1
3.1.2 ARP 绑定.....	3-1
3.1.3 如何进行 ARP/ND 绑定.....	3-1
3.2 ARP、ND 绑定配置	3-2

3.3 ARP、ND绑定举例.....	3-3
第 4 章 ARP GUARD配置	4-1
4.1 ARP GUARD 的介绍.....	4-1
4.2 ARP GUARD配置任务序列.....	4-1
第 5 章 Arp local proxy配置.....	5-1
5.1 Arp local proxy功能简介.....	5-1
5.2 Arp local proxy功能配置任务序列.....	5-2
5.3 Arp local proxy功能典型案例.....	5-2
5.4 Arp local proxy功能排错帮助.....	5-3
第 6 章 免费ARP发送功能操作配置.....	6-1
6.1 免费ARP发送功能简介	6-1
6.2 免费ARP发送功能配置任务序列	6-1
6.3 免费ARP发送功能典型案例	6-2
6.4 免费ARP发送功能排错帮助	6-2
第 7 章 ND Snooping配置	7-1
7.1 ND Snooping介绍.....	7-1
7.2 ND snooping基本配置.....	7-1
7.3 ND Snooping举例.....	7-3
7.4 ND Snooping排错帮助.....	7-5
第 8 章 Keepalive gateway配置.....	8-1
8.1 keepalive gateway介绍	8-1
8.2 keepalive gateway功能配置任务序列.....	8-1
8.3 keepalive gateway举例	8-2
8.4 keepalive gateway排错帮助	8-3

第1章 L3 转发配置

说明：

本章所指的交换机和路由器代表了一般意义下的路由器或运行了路由协议的无线控制产品。

交换机支持三层转发功能。三层转发是将三层协议报文（IP 报文）跨越 VLAN 进行转发，这种转发是用 IP 地址寻址的，当交换机的一个接口接收到 IP 报文后，会根据自己的路由表进行检索，然后根据结果决定对数据报文的操作，如果 IP 报文的目的地址是本交换机可达的另一个子网，那么就将此报文从交换机的相应接口发送出去。交换机可以使用硬件对 IP 报文进行转发，交换机的转发芯片中有主机路由表和缺省路由表。其中，主机路由表用来存储与交换机直接相连的主机路由，缺省路由表存储（经聚合算法计算后的）网段路由。

当单播流量转发需要的路由（主机路由或网段路由）在转发芯片中存在了，流量的转发就完全由硬件负责，因此大大提升了转发效率，可以达到线速转发。

1.1 三层接口

1.1.1 三层接口介绍

在交换机上可以创建三层接口。三层接口并不是实际的物理接口，它是一个虚拟的接口。三层接口是在 VLAN 的基础上创建的。三层接口可以包含一个或多个二层端口（它们同属于一个 VLAN），但也可以不包含任何二层端口。三层接口包含的二层端口中，需要至少有一个是 UP 状态，三层接口才是 UP 状态，否则为 DOWN 状态。交换机中所有的三层接口缺省使用一个相同的 MAC 地址，此地址是在三层接口创建时从交换机保留的 MAC 地址中选取的。三层接口是三层协议的基础，在三层接口上可以配置 IP 地址，交换机可以通过配置在三层接口上的 IP 地址，与其它设备进行 IP 协议的传输。交换机也可以在不同的三层接口之间转发 IP 协议报文。Loopback 接口也属于三层接口。

1.1.2 三层接口配置

三层接口配置任务序列：

1. 创建三层接口
2. 配置三层接口的带宽
3. 配置 VLAN 接口描述
4. 打开或关闭 VLAN 接口

1.创建三层接口

命令	解释
全局配置模式	
interface vlan <vlan-id> no interface vlan <vlan-id>	创建一个 VLAN 接口（VLAN 接口属于三层接口）；本命令的 no 操作为删除交换机创建的 VLAN 接口（三层接口）。
interface loopback <loopback-id> no interface loopback <loopback-id>	创建一个 Loopback 接口并进入 Loopback 接口配置模式；本命令的 no 操作为删除指定的 Loopback 接口。

2. 配置三层接口的带宽

命令	解释
VLAN 接口配置模式	
bandwidth <bandwidth> no bandwidth	配置 interface vlan 的带宽。本命令的 no 命令为恢复 interface vlan 的带宽值为默认值。

3. 配置 VLAN 接口描述

命令	解释
VLAN 接口配置模式	
description <text> no description	配置 VLAN 接口的描述信息；其 no 形式取消该 VLAN 接口的描述信息。

4. 打开或关闭 VLAN 接口

命令	解释
VLAN 接口配置模式	
shutdown no shutdown	打开或关闭 VLAN 接口。

1.2 IP配置

1.2.1 IPv4、IPv6 介绍

IPv4 是全球通用因特网协议的当前版本。事实证明，IPv4 简单、灵活、开放、稳固耐用、便于实施，且能够和多种上下层协议良好协同工作。尽管 IPv4 自 20 世纪 80 年代初确立以来就几乎未曾改动，但是 IPv4 始终支持因特网的升迁，一直发展到目前的全球规模。然而，随着因特网基础设施与因特网应用服务的发展不断地突飞猛进，IPv4 在因特网的目前规模与复杂性面前已暴露其不足之处。

IPv6 指的是互联网协议第六版，是由 IETF 设计的下一代互联网协议，用以取代现有的互联网协议第四版（IPv4）。IPv6 是专为弥补 IPv4 不足而开发出来的，以便让因特网能够进一步发展壮大。

IPv6 所解决的最重要问题就是增加 IP 地址的数量。IPv4 地址已近枯竭，而因特网用户的数量却在不断以几何级数增长。随着需要使用 IP 地址的因特网服务与应用设备（利用因特网的信息终端、家庭与小型办公室网络、IP 电话与无线服务等）不断大量涌现，IP 地址的供给更显紧张。人们早就开始着手解决 IPv4 地址紧缺的问题，采用各种技术延长现有 IPv4 基础架构的寿命，其中包括网络地址转换（Network Address Translation，简称 NAT）和无类别域间路由（Classless Inter-Domain Routing，简称 CIDR）等技术。

虽然 CIDR、NAT 和私有编址的组合暂时缓和了 IPv4 地址空间紧缺的问题，但是 NAT 技术破坏了 IP 设计初衷的端到端模型，使作为网络中间节点的路由设备必须保持每个连接的状态，大大增加了网络延迟，降低了网络性能。而且网络数据包地址的变换阻碍了端到端的网络安全检查，如 IPSec 认证报头(AH)就是一个例子。

因此，要综合解决 IPv4 存在的诸多问题，IETF 设计的下一代互联网协议 IPv6 已经成为目前唯一可行的解决方案。

首先 IPv6 协议 128 比特的编址方案能确保在时间和空间范围内为全球 IP 网络节点提供足够的全球唯一的 IP 地址。而且，除了增加地址空间以外，IPv6 还对 IPv4 的其它许多关键设计进行了改进。

层次化编址方案有助于路由聚合，有效减少了路由器的路由表项，提高了路由选择与数据包处理的效率与可扩展性。

IPv6 的包头设计相比 IPv4 更有效率，数据字段更少，去掉了包头校验和，从而加快了基本 IPv6 包头的处理速度。在 IPv6 包头中，分片字段作为可选扩展字段出现，路由器转发过程中不用再对数据包做分片处理，通过路径 MTU 发现机制协同数据包源点工作，提高了路由器处理效率。

支持地址自动配置与即插即用。IPv6 的地址自动配置功能使大量 IP 主机能够轻松发现网络路由器，并自动获得全球唯一的 IPv6 地址，这使利用 IPv6 因特网的设备具备了即插即用特性。自动地址配置功能还使对现有网络的重新编址变得更加简单便捷，使网络运营商能够更加方便地管理从一个提供商到另一个提供商的转换。

支持 IPSec。IPSec 在 IPv4 中为可选项，而在 IPv6 协议中则是必须实现的。IPv6 提供了安全扩展包头，能够提供诸如访问控制、机密性与数据完整性等端到端的安全服务，从而使加密、验证和虚拟专用网络 (VPN) 的实施变得更加容易。

增强对移动 IP (Mobile IP) 与移动计算设备的支持。在 IETF 标准中定义的移动 IP 协议使移动设备不必脱离其现有连接即可自由移动，这是一种日益重要的网络功能。与 IPv4 不同的是，IPv6 的移动性是使用内置自动配置获取转交地址 (Care-Of-Address)，因而无需外地代理 (Foreign Agent)。此外，这种联编过程使通信节点 (Correspondent Node) 能够与移动节点 (Mobile Node) 直接通信，从而避免了在 IPv4 中所要求的三角路由选择的额外系统开销。其结果是，在 IPv6 中，移动 IP 的处理效率大为提高。

避免网络地址转换 (NAT) 的使用。NAT 机制的引入是为了在不同的网络区段之间共享

和重新使用相同的地址空间。这种机制在暂时缓解了 IPv4 地址紧缺问题的同时，却为网络设备与应用程序增加了处理地址转换的负担。由于 IPv6 的地址空间大大增加，也就无需再进行地址转换，NAT 部署带来的问题与系统开销也随之解决。

支持广泛部署的路由选择协议。IPv6 保持并扩展了对现有内部网关协议（Interior Gateway Protocols, 简称 IGP）与外部网关协议（Exterior Gateway Protocols, 简称 EGP）的支持，例如，RIPng、OSPFv3、IS-ISv6 与 MBGP4+ 等 IPv6 路由协议。

组播地址数量增加，对组播的支持有所增强。IPv6 取消了广播功能，使用组播机制来处理 IPv4 的广播功能，不仅节省了网络带宽，而且提高了网络效率。

1.2.2 IP 配置

可以将三层接口配置为 IPv4 接口或者 IPv6 接口。

1.2.2.1 IPv4 地址配置

IPv4 配置任务序列：

1. 配置三层接口的 IPv4 地址

1. 配置三层接口的 IPv4 地址

命令	解释
VLAN 接口配置模式	
ip address <ip-address> <mask> [secondary] no ip address [<ip-address> <mask>]	配置 VLAN 接口的 IP 地址；本命令的 no 操作为删除 VLAN 接口 IP 地址。

1.2.2.2 IPv6 地址配置

IPv6 配置任务序列如下：

1. IPv6 基本配置
 - (1) 配置接口 IPv6 地址
 - (2) 配置 IPv6 静态路由
2. IPv6 邻居发现配置
 - (1) 配置 DAD 邻居请求消息数目
 - (2) 配置发送邻居请求消息间隔
 - (3) 使能与禁止路由器公告
 - (4) 配置路由器公告生存期
 - (5) 配置路由器公告最小间隔时间
 - (6) 配置路由器公告最大间隔时间
 - (7) 配置前缀公告参数

- (8) 设置静态邻居表项
- (9) 清除邻居表项
- (10) 设置发送路由公告的 hoplimit 值
- (11) 设置发送路由公告的 mtu 值
- (12) 设置发送路由公告的 reachable-time 值
- (13) 设置发送路由公告的 retrans-timer 值
- (14) 配置标识除地址信息之外的其他信息是否由 dhcpv6 获取
- (15) 配置标识地址信息是否由 dhcpv6 获取

3. IPv6 隧道配置

- (1) 创建/删除隧道
- (2) 配置隧道描述
- (3) 配置隧道源
- (4) 配置隧道目的
- (5) 配置隧道下一跳
- (6) 配置隧道模式
- (7) 配置隧道路由

1. IPv6 基本配置

(1) 配置接口 IPv6 地址

命令	解释
接口配置模式	
ipv6 address <ipv6-address/prefix-length> [eui-64] no ipv6 address <ipv6-address /prefix-length>	配置 IPv6 地址，包括可聚合全球单播地址，本地站点地址，本地链路地址。本命令的 no 操作为删除 IPv6 地址。

(2) 设置 IPv6 静态路由

命令	解释
全局配置模式	

<pre> ipv6 route <ipv6-prefix/prefix-length> {<nexthop-ipv6-address> <interface-type interface-number> {<nexthop-ipv6-address> <interface-type interface-number>}} [distance] no ipv6 route <ipv6-prefix/prefix-length> {<nexthop-ipv6-address> <interface-type interface-number> {<nexthop-ipv6-address> <interface-type interface-number>}} [distance]</pre>	配置 IPv6 静态路由。本命令的 no 操作 为删除 IPv6 静态路由。
--	---

2. IPv6 邻居发现配置

(1) 配置 DAD 邻居请求消息数目

命令	解释
接口配置模式	
<pre> ipv6 nd dad attempts <value> no ipv6 nd dad attempts</pre>	设置接口进行重复地址检测时，连续发出的邻居请求消息数目，本命令的 no 操作为恢复默认值（1）。

(2) 配置发送邻居请求消息间隔

命令	解释
接口配置模式	
<pre> ipv6 nd ns-interval <seconds> no ipv6 nd ns-interval</pre>	设置接口发送邻居请求消息的时间间隔。本命令的 no 操作为恢复默认值（1 秒）。

(3) 使能与禁止路由器公告

命令	解释
接口配置模式	
<pre> ipv6 nd suppress-ra no ipv6 nd suppress-ra</pre>	禁止 IPv6 路由器公告，本命令的 no 操作为开启 IPv6 路由器公告。

(4) 配置路由器公告生存期

命令	解释
接口配置模式	

ipv6 nd ra-lifetime <seconds>	配置路由器公告的生存期, 本命令的 no 操作为恢复默认值 (1800 秒)。
no ipv6 nd ra-lifetime	

(5) 配置路由器公告最小间隔时间

命令	解释
接口配置模式	
ipv6 nd min-ra-interval <seconds>	配置用于路由器公告的最小时间间隔, 本命令的 no 操作为恢复默认值 (200 秒)。
no ipv6 nd min-ra-interval	

(6) 配置路由器公告最大间隔时间

命令	解释
接口配置模式	
ipv6 nd max-ra-interval <seconds>	配置用于路由器公告的最大时间间隔, 本命令的 no 操作为恢复默认值 (600 秒)。
no ipv6 nd max-ra-interval	

(7) 配置前缀公告参数

命令	解释
接口配置模式	
ipv6 nd prefix <ipv6-address/prefix-length> <valid-lifetime> <preferred-lifetime> [off-link] [no-autoconfig]	配置路由器公告的地址前缀及其公告参数, 本命令的 no 操作为删除路由公告的地址前缀。
no ipv6 nd prefix <ipv6-address/prefix-length> <valid-lifetime> <preferred-lifetime> [off-link] [no-autoconfig]	

(8) 设置静态邻居表项

命令	解释
接口配置模式	
ipv6 neighbor <ipv6-address> <hardware-address> interface <interface-type interface-name>	设置静态邻居表项, 包括邻居 IPv6 地址, MAC 地址, 二层端口。
no ipv6 neighbor <ipv6-address>	删除邻居表项

(9) 清除邻居表项

命令	解释
特权配置模式	
clear ipv6 neighbors	清除所有静态邻居表项。

(10) 设置发送路由公告的 hoplimit 值

命令	解释
接口配置模式	
ipv6 nd ra-hoplimit <value>	设置发送路由公告的 hoplimit 值。

(11) 设置发送路由公告的 mtu 值

命令	解释
接口配置模式	
ipv6 nd ra-mtu <value>	设置发送路由公告的 mtu 值。

(12) 设置发送路由公告的 reachable-time 值

命令	解释
接口配置模式	
ipv6 nd reachable-time <seconds>	设置发送路由公告的 reachable-time 值。

(13) 设置发送路由公告的 retrans-timer 值

命令	解释
接口配置模式	
ipv6 nd retrans-timer <seconds>	设置发送路由公告的 retrans-timer 值。

(14) 配置标识除地址信息之外的其他信息是否由 dhcpv6 获取

命令	解释
接口配置模式	
ipv6 nd other-config-flag	标识除地址信息之外的其他信息是否由 DHCPv6 获取。

(15) 配置标识地址信息是否由 dhcpv6 获取

命令	解释
接口配置模式	
ipv6 nd managed-config-flag	标识地址信息是否由 DHCPv6 获取。

3. IPv6 隧道配置

(1) 创建/删除隧道

命令	解释
全局配置模式	
interface tunnel <tnl-id> no interface tunnel <tnl-id>	创建一条隧道。本命令的 no 操作为删除一条隧道。

(2) 配置隧道描述

命令	解释
隧道配置模式	
description <desc> no description	配置隧道描述, 本命令的 no 操作删除隧道描述。

(3) 配置隧道源

命令	解释
隧道配置模式	
tunnel source {<ipv4-address> <ipv6-address> <interface-name>} no tunnel source	配置隧道源端 IPv4/IPv6 地址, 或者允许隧道源取自接口的主 IPv4/IPv6 地址, 本命令的 no 操作为删除隧道源端的 IPv4/IPv6 地址或隧道源接口名。

(4) 配置隧道目的

命令	解释
隧道配置模式	
tunnel destination {<ipv4-address> <ipv6-address>} no tunnel destination	配置隧道目的端的 IPv4/IPv6 地址, 本命令的 no 操作为删除隧道目的端的 IPv4/IPv6 地址。

(5) 配置隧道下一跳

命令	解释
隧道配置模式	
tunnel nexthop <ipv4-address> no tunnel nexthop	配置隧道的下一跳 IPv4 地址, 本命令的 no 操作为删除隧道的下一跳 IPv4 地址。

(6) 配置隧道模式

命令	解释
----	----

隧道配置模式	
tunnel mode [[gre] ipv6ip [6to4 isatap]] no tunnel mode	配置隧道模式，本命令的 no 操作为清除隧道模式。

(7) 配置隧道路由

命令	解释
全局配置模式	
ipv6 route <ipv6-address/prefix-length> {<interface-type interface-number> tunnel <tnl-id>} no ipv6 route <ipv6-address/prefix-length> {<interface-type interface-number> tunnel <tnl-id>}	配置隧道路由，本命令的 no 操作为删除隧道路由。

1.2.3 IP配置举例

1.2.3.1 IPv4 典型案例

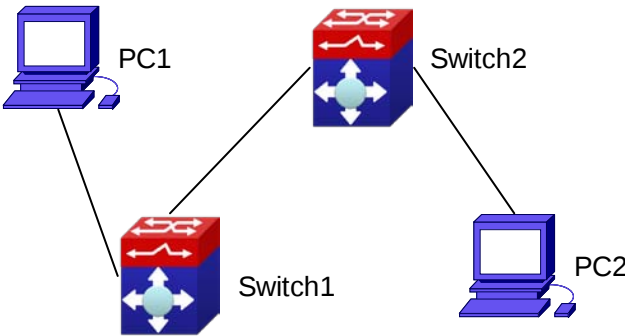


图 1-1 IPv4 典型案例

用户有如下配置需求：在 switch 1 和 switch 2 上配置不同网段的 IPv4 地址，配置静态路由，利用 ping 功能验证可达性。

配置说明：

- 1、在 Switch1 上配置两个 vlan，分别为 vlan1 和 vlan2

- 2、在 Switch1 的 vlan1 内配置 IPv4 地址 192.168.1.1 255.255.255.0，在 vlan2 内配置 IPv4 地址 192.168.2.1 255.255.255.0
- 3、在 Switch2 上配置两个 vlan，分别为 vlan2 和 vlan3
- 4、在 Switch2 的 vlan2 内配置 IPv4 地址 192.168.2.2 255.255.255.0，在 vlan3 内配置 IPv4 地址 192.168.3.1 255.255.255.0
- 5、PC1 的 IPv4 地址为 192.168.1.100 255.255.255.0，PC2 的 IPv4 地址是 192.168.3.100 255.255.255.0
- 6、在 Switch1 上配置静态路由 192.168.3.0/24，在 Switch2 上配置静态路由 192.168.1.0/24
- 7、PC 机之间互 ping

注：首先要确定 PC1 和 Switch1 可以 ping 通，PC2 和 Switch2 可以 ping 通

配置步骤如下：

```
Switch1(Config)#interface vlan 1
Switch1(Config-if-Vlan1)#ip address 192.168.1.1 255.255.255.0
Switch1(Config)#interface vlan 2
Switch1(Config-if-Vlan2)#ip address 192.168.2.1 255.255.255.0
Switch1(Config-if-Vlan2)#exit
Switch1(Config)#ip route 192.168.3.0 255.255.255.0 192.168.2.2
```

```
Switch2(Config)#interface vlan 2
Switch2(Config-if-Vlan2)#ip address 192.168.2.2 255.255.255.0
Switch2(Config)#interface vlan 3
Switch2(Config-if-Vlan3)#ip address 192.168.3.1 255.255.255.0
Switch2(Config-if-Vlan3)#exit
Switch2(Config)#ip route 192.168.1.0 255.255.255.0 192.168.2.1
```

1.2.3.2 IPv6 典型案例

案例 1:

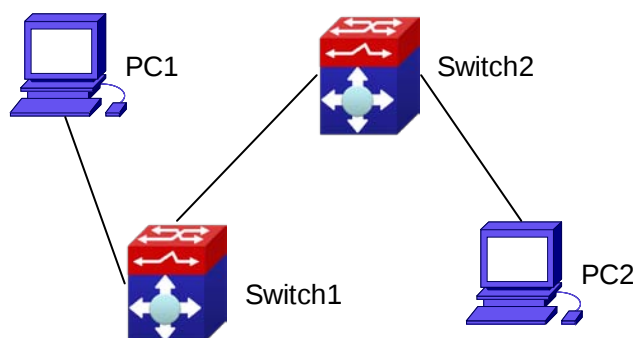


图 1-2 IPv6 典型案例

用户有如下配置需求：在 Switch 1 和 Switch 2 上配置不同网段的 IPv6 地址，配置静态路由，利用 ping6 功能验证可达性。

配置说明：

- 1、在 Switch1 上配置两个 vlan，分别为 vlan1 和 vlan2
- 2、在 Switch1 的 vlan1 内配置 IPv6 地址 2001::1/64,在 vlan2 内配置 IPv6 地址 2002::1/64
- 3、在 Switch2 上配置两个 vlan，分别为 vlan2 和 vlan3
- 4、在 Switch2 的 vlan2 内配置 IPv6 地址 2002::2/64，在 vlan3 内配置 IPv6 地址 2003::1/64
- 5、PC1 的 IPv6 地址为 2001::11/64,PC2 的 IPv6 地址是 2003::33/64
- 6、在 Switch1 上配置静态路由 2003::33/64,在 Switch2 上配置静态路由 2001::11/64
- 7、pc 机之间互相 ping6

注：首先要确定 PC1 和 Switch1 可以 ping 通，PC2 和 Switch2 可以 ping 通

配置步骤如下：

```
Switch1(Config)#interface vlan 1
Switch1(Config-if-Vlan1)#ipv6 address 2001::1/64
Switch1(Config)#interface vlan 2
Switch1(Config-if-Vlan2)#ipv6 address 2002::1/64
Switch1(Config-if-Vlan2)#exit
Switch1(Config)#ipv6 route 2003::33/64 2002::2
```

```
Switch2(Config)#interface vlan 2
Switch2(Config-if-Vlan2)#ipv6 address 2002::2/64
Switch2(Config)#interface vlan 3
Switch2(Config-if-Vlan3)#ipv6 address 2003::1/64
Switch2(Config-if-Vlan3)#exit
Switch2(Config)#ipv6 route 2001::33/64 2002::1
```

```
Switch1#ping6 2003::33
```

配置结果：

```
Switch1#show run
interface Vlan1
  ipv6 address 2001::1/64
!
interface Vlan2
  ipv6 address 2002::2/64
!
```

```
interface Loopback
  mtu 3924
!
ipv6 route 2003::/64 2002::2
!
no login
!
end
```

```
Switch2#show run
interface Vlan2
  ipv6 address 2002::2/64
!
interface Vlan3
  ipv6 address 2003::1/64
!
interface Loopback
  mtu 3924
!
ipv6 route 2001::/64 2002::1
!
no login
!
End
```

案例 2:

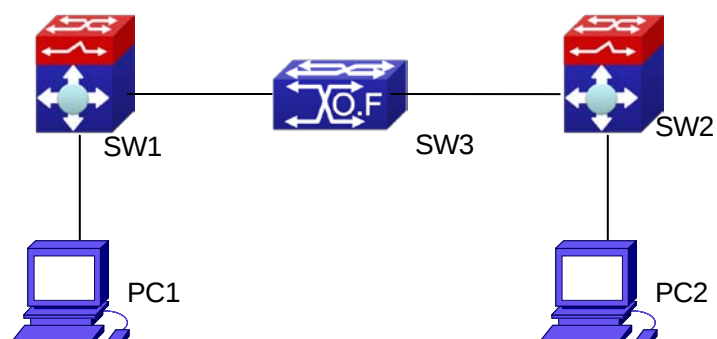


图 1-3 IPv6 隧道

该案例为 IPv6 隧道，用户有如下配置需求：SW1 和 SW2 为隧道的节点，支持双栈。SW3 只是运行 IPv4，PC1 和 PC2 进行通信

配置说明：

- 1、在 SW1 上配置两个 vlan，分别为 vlan1 和 vlan2。Vlan1 是 IPv6 域，vlan2 连接 IPv4 域
- 2、在 SW1 的 vlan1 中配置 IPv6 地址 2002:caca:ca01:2::1/64，并且打开 RA 功能，在 vlan2 配置 IPv4 地址 202.202.202.1
- 3、在 SW2 上配置两个 vlan，分别是 vlan3 和 vlan4，vlan4 是 IPv6 域，vlan3 是连接 IPv4 域
- 4、在 SW2 的 vlan4 中配置 IPv6 地址 2002:cbcb:cb01:2::1/64，并且打开 RA 功能，在 vlan3 上配置 IPv4 地址 203.203.203.1
- 5、在 SW1 上配置手工隧道，隧道的源 IPv4 地址为 202.202.202.1，配置默认 IPv6 路由指向该隧道
- 6、在 SW2 上配置手工隧道，隧道的源 IPv4 地址为 203.203.203.1，配置默认 IPv6 路由指向该隧道
- 7、在 SW3 上配置两个 vlan，分别为 vlan2 和 vlan3，在 vlan2 上配置 IPv4 地址 202.202.202.202 在 vlan3 上配置 IPv4 地址 203.203.203.203
- 8、PC1 和 PC2 通过 SW1 和 SW2 获得 2002 的前缀自动配置 IPv6 地址
- 9、在 PC1 上 ping PC2 的 IPv6 地址

配置步骤如下：

```
SW1(Config-if-Vlan1)#ipv6 address 2002:caca:ca01:2::1/64
```

```
SW1(Config-if-Vlan1)#no ipv6 nd suppress-ra
```

```
SW1(Config-if-Vlan1)#interface vlan 2
```

```
SW1(Config-if-Vlan2)#ipv4 address 202.202.202.1 255.255.255.0
```

```
SW1(Config-if-Vlan1)#exit
```

```
SW1(config)# interface tunnel 1
```

```
SW1(Config-if-Tunnel1)#tunnel source 202.202.202.1
```

```
SW1(Config-if-Tunnel1)#tunnel destination 203.203.203.1
```

```
SW1(Config-if-Tunnel1)#tunnel mode ipv6ip
```

```
SW1(config)#ipv6 route ::/0 tunnel1
```

```
SW2(Config-if-Vlan4)#ipv6 address 2002:cbcb:cb01:2::2/64
```

```
SW2(Config-if-Vlan4)#no ipv6 nd suppress-ra
```

```
SW2 (Config-if-Vlan3)#interface vlan 3
```

```
SW2 (Config-if-Vlan2)#ipv4 address 203.203.203.1 255.255.255.0
```

```
SW2 (Config-if-Vlan1)#exit
```

```
SW2(Config)#interface tunnel 1
```

```
SW2(Config-if-Tunnel1)#tunnel source 203.203.203.1
```

```
SW2(Config-if-Tunnel1)#tunnel destination 202.202.202.1
```

```
SW2(Config-if-Tunnel1)#tunnel mode ipv6ip
```

```
SW2(config)#ipv6 route ::/0 tunnel1
```

1.2.4 IPv6 排错帮助

☞ 配置路由器的生存期时不应该小于发送路由器公告的时间间隔。如果相连 PC 未获得 IPv6 地址时，应注意 RA 公告的开关（默认为关闭）。

1.3 IP 转发

1.3.1 IP 转发介绍

网关设备可以将 IP 协议报文从一个子网转发到另一个子网中，这种转发是通过路由寻径的。交换机的 IP 转发是由硬件协助完成的，可以达到端口的线速转发；同时还可以提供各种灵活的控制，对转发行为进行调整和监控。交换机可以支持禁止或允许优化的聚合算法以调整交换芯片中网段路由表项的生成，查看 IP 转发的统计信息，监视 IP 报文的收发状况，以及查看硬件转发芯片的状况。

1.3.2 IP 路由聚合配置

- IP 路由聚合配置任务序列：
1. 配置是否使用优化 IP 路由聚合算法

1.配置是否使用优化 IP 路由聚合算法

命令	解释
全局配置模式	
ip fib optimize no ip fib optimize	配置交换机使用优化 IP 路由聚合算法；本命令的 no 操作为交换机不使用优化 IP 路由聚合算法。

1.4 URPF

1.4.1 URPF 介绍

URPF（Unicast Reverse Path Forwarding，单播逆向路径转发）将组播中使用的RPF技术应用到单播中，用于防止基于源地址欺骗的网络攻击行为。

交换机接收报文，同时获取报文的源地址和入接口，然后把该源地址作为目的地址在路由表中查找路由，如果查到的路由出接口和接收该报文的入接口不匹配，交换机则认为该报

文的源地址是伪装的，并丢弃该报文。

源地址欺骗攻击为入侵者构造出一系列带有伪造源地址的报文，对于使用基于 IP 地址验证的应用来说，此攻击方法可以导致未被授权用户以他人身份获得访问系统的权限，甚至是以管理员权限来访问。即使响应报文不能达到攻击者，同样也会造成对被攻击对象的破坏。

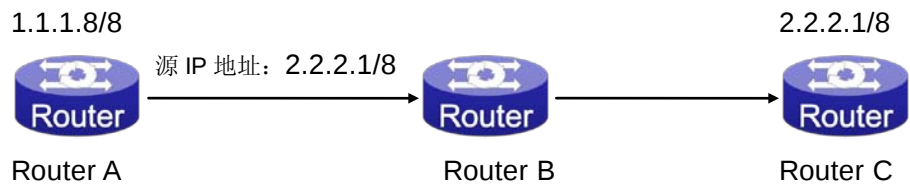


图 1-4 URPF 应用环境

如上图所示，在Router A上伪造源地址为2.2.2.1/8 的报文，向服务器Router B发起请求，Router B响应请求时将向真正的“2.2.2.1/8”发送报文。这种非法报文对Router B和Router C都造成了攻击。URPF 技术可以应用在上述环境中，阻止基于源地址欺骗的攻击。

1.4.1.1 IPv6 URPF运行机制

目前URPF的运行机制依赖于交换机芯片提供的ACL功能。

首先全局使能URPF功能监视路由表变化：将路由表FIB中的每条路由生成对应的URPF permit ACL规则。URPF严格模式下，ACL规则的形式为：入数据包源地址网段+入数据包入接口VID。入数据包源地址网段对应FIB表路由表项的目的网段地址，入数据包入接口VID对应FIB表路由表项的出接口VID。URPF松散模式下，ACL规则的形式为入数据包源地址网段，入数据包源地址网段对应FIB表路由表项的目的网段地址。

在端口上启动URPF后：将端口绑定URPF规则，并且生成默认的DENY ALL规则下发硬件。

通过以上操作，就可以确保，在数据到达此端口时，只有符合上述规则的数据才能进入端口，其它数据都会被丢掉。

目前对应URPF的ACL规则优先级较低，不会阻挡各种协议包数据，因此启动该功能不影响该交换机路由协议的正常运行。

1.4.2 URPF配置任务序列

- 1) 启动 URPF
- 2) 端口启动 URPF
- 3) 显示和调试 URPF 相关信息

1) 全局启动 URPF

命令	解释
----	----

全局配置模式	
urpf enable no urpf enable	全局启动和关闭 URPF。

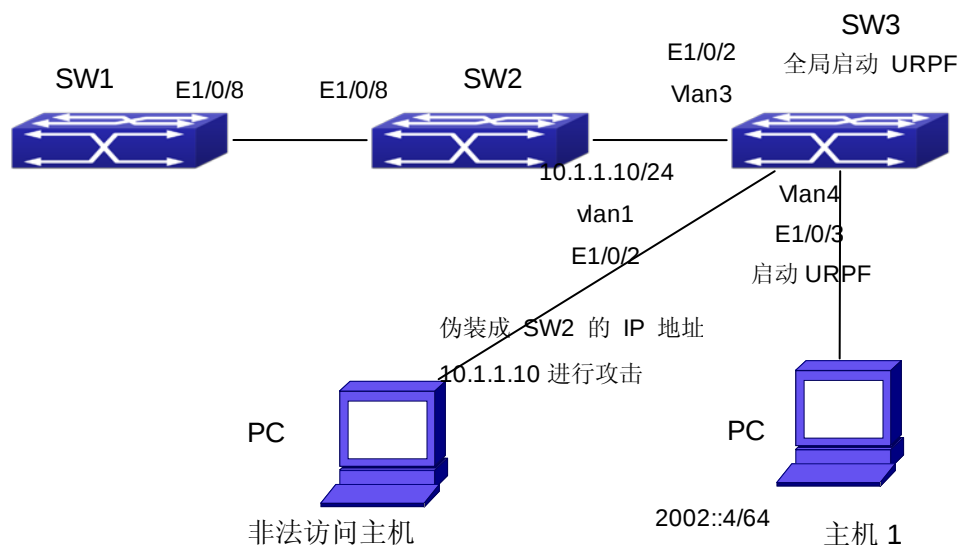
2) 端口启动 URPF

命令	解释
端口配置模式	
ip urpf enable {loose strict} {allow-default-route } no ip urpf enable	端口启动和关闭 URPF。

3) 显示和调试 URPF 相关信息

命令	解释
特权配置模式	
debug urpf {notice warn error} no debug urpf {notice warn error}	关闭/打开 URPF 调试功能, 在 URPF 规则安装失败时提示错误。
特权和配置模式	
show urpf	显示哪些端口启动了 URPF。
show urpf rule ipv4 num interface ethernet IFNAME	显示端口绑定的 IPv4 规则数目。
show urpf rule ipv6 num interface ethernet IFNAME	显示端口绑定的 ipv6 规则数目。
show urpf rule ipv4 interface ethernet IFNAME	显示端口绑定的 ipv4 规则明细。
show urpf rule ipv6 interface ethernet IFNAME	显示端口绑定的 ipv6 规则明细。

1.4.3 URPF 典型案例



如上图所示的网络拓扑中，一台 SW3 上启动 URPF 功能。当链接的网络中有人冒充别人的 IP 地址进行恶意攻击时，交换机通过硬件 FFP 功能直接丢弃所有的攻击报文。

设置 SW3 Ethernet1/0/3 启动 URPF 功能。

SW3 配置任务序列：

```
Switch#config
```

```
Switch(config)#urpf enable
```

```
Switch(config)#interface ethernet 1/0/3
```

```
Switch(Config-If-Ethernet1/0/3)#ip urpf enable strict
```

1.4.4 URPF排错帮助

URPF协议的正常运行非常依赖URPF对应规则的正确下发，如果在配置URPF后，发现功能与预期不符：

- ☞ 判断是否因为交换机配置了与 URPF 冲突的规则（URPF 的优先级要小于 ACL），如果发生互斥，则 ACL 的规则起作用。
- ☞ 判断 FIB 表中是否存在相关的路由，只有 FIB 表中存在该路由后，才会在该端口下发相应的 ACL 规则。
- ☞ 判断是否硬件的 ACL 表现已满，从而导致无法对新生成的路由下发 ACL 规则。
- ☞ 如果在正常配置下，URPF 运行的情况仍然和预期不匹配，请打开 URPF 的调试功能，并且利用 `show urpf` 和相关的显示规则数目以及明细规则的命令观察生成的 URPF 规则是否正常，并将结果发送给技术服务中心。

1.5 ARP

1.5.1 ARP介绍

ARP（Address Resolution Protocol）地址解析协议，主要用于 IP 地址到以太网 MAC 地址的解析。交换机除了支持动态 ARP 外，也支持静态配置。此外，在某些应用中，交换机还支持配置代理 ARP。如当交换机的接口收到某 ARP 请求，该请求的 IP 地址与接口地址在一个 IP 网段，但却不在同一物理网络中，此时该接口若启动了代理 ARP 的功能，接口会将自己的 MAC 地址作为 ARP 的回应，然后将收到的实际数据报文进行转发。启动代理 ARP 功能可以使因为物理网络分离但属于同一 IP 网段的机器忽视物理网络分离的事实，经过具有代理 ARP 接口的转发像处在一个物理网络中。

1.5.2 ARP配置

ARP 配置任务序列：

1. 配置静态 ARP
2. 配置代理 ARP
3. 清除动态 ARP
4. 选择 hash 算法
5. 清除 ARP 报文统计信息

1. 配置静态 ARP

命令	解释
VLAN 接口模式	
arp <ip_address> <mac_address> {interface [ethernet] <portName> } no arp <ip_address>	配置静态 ARP 表项；本命令的 no 操作为删除指定 IP 地址的 ARP 表项。

2. 配置代理 ARP

命令	解释
VLAN 接口模式	
ip proxy-arp no ip proxy-arp	打开以太网代理 ARP 的功能；本命令的 no 操作为关闭代理 ARP 的功能。

3.清除动态 ARP

命令	解释
特权用户模式	
clear arp-cache	清除交换机学习到的动态 ARP。

4. 选择 hash 算法

命令	解释
全局配置模式	
l3 hashselect [<crc16l crc16u crc32l crc32u lsb>]	设置 L3 表的 hash 算法，该命令的使用涉及到 ARP 表项在硬件中的存储，必须在厂商技术人员的指导下使用，该命令的详细信息请参考命令手册的相应部分。

5. 清除 ARP 报文统计信息

命令	解释
特权用户模式	
clear arp traffic	清除交换机 ARP 报文统计信息。

1.5.3 ARP 转发排错帮助

交换机无法 PING 通直接相连的网络设备，检查可能存在的情况和建议的解决方法：

- ☞ 首先检查交换机是否学习到相应的 ARP。
- ☞ 若 ARP 未能学习到，那么使用 ARP 的调试信息，观察 ARP 协议报文的收发情况。
- ☞ 用户比较容易遇到的现象是线缆有问题，导致 ARP 不能学习。

第2章 防ARP扫描功能操作配置

2.1 防ARP扫描功能介绍

ARP 扫描是一种常见的网络攻击方式。为了探测网段内的所有活动主机，攻击源将会产生大量的 ARP 报文在网段内广播，这些广播报文极大的消耗了网络的带宽资源；攻击源甚至有可能通过伪造的 ARP 报文而在网络内实施大流量攻击，使网络带宽消耗殆尽而瘫痪。而且 ARP 扫描通常是其他更加严重的攻击方式的前奏，如病毒自动感染，或者继而进行端口扫描、漏洞扫描以实施如信息窃取、畸形报文攻击，拒绝服务攻击等。

由于 ARP 扫描给网络的安全和稳定带来了极大的威胁，所以防 ARP 扫描功能将具有重大意义。交换机防 ARP 扫描的整体思路是若发现网段内存在具有 ARP 扫描特征的主机或端口，将切断攻击源头，保障网络的安全。

有两种方式来防 ARP 扫描：基于端口和基于 IP。基于端口的 ARP 扫描会计算一段时间内从某个端口接收到的 ARP 报文的数量，若超过了预先设定的阈值，则会 down 掉此端口。基于 IP 的 ARP 扫描则计算一段时间内从网段内某 IP 收到的 ARP 报文的数量，若超过了预先设置的阈值，则禁止来自此 IP 的任何流量，而不是 down 与此 IP 相连的端口。此两种防 ARP 扫描功能可以同时启用。端口或 IP 被禁掉后，可以通过自动恢复功能自动恢复其状态。

为了提高交换机的效率，可以配置受信任的端口和 IP，交换机不检测来自受信任的端口或 IP 的 ARP 报文，这样可以有效地减少交换机的负担。

2.2 防ARP扫描配置任务序列

- 1) 启动防 ARP 扫描功能
- 2) 配置基于端口和基于 IP 的防 ARP 扫描的阈值
- 3) 配置信任端口
- 4) 配置信任 IP
- 5) 配置自动恢复时间
- 6) 显示和调试防 ARP 扫描相关信息

1) 启动防 ARP 扫描功能

命令	解释
全局配置模式	
anti-arpscan enable no anti-arpscan enable	全局启动或关闭防 ARP 扫描功能。

2) 配置基于端口和基于 IP 的防 ARP 扫描的阈值

命令	解释
全局配置模式	
anti-arpscan port-based threshold <threshold-value> no anti-arpscan port-based threshold	设置基于端口的防 ARP 扫描阈值。
anti-arpscan ip-based threshold <threshold-value> no anti-arpscan ip-based threshold	设置基于 IP 的防 ARP 扫描阈值。

3) 配置信任端口

命令	解释
端口配置模式	
anti-arpscan trust <port supertrust-port> no anti-arpscan trust <port supertrust-port>	设置端口的信任属性。

4) 配置信任 IP

命令	解释
全局配置模式	
anti-arpscan trust ip <ip-address> [<netmask>] no anti-arpscan trust ip <ip-address> [<netmask>]	设置 IP 的信任属性。

5) 配置自动恢复时间

命令	解释
全局配置模式	
anti-arpscan recovery enable no anti-arpscan recovery enable	启动或关闭自动恢复功能。
anti-arpscan recovery time <seconds> no anti-arpscan recovery time	设置自动恢复时间。

6) 显示和调试防 ARP 扫描相关信息

命令	解释
全局配置模式	
anti-arpscan log enable no anti-arpscan log enable	打开或关闭防 ARP 扫描的日志功能。
anti-arpscan trap enable no anti-arpscan trap enable	打开或关闭防 ARP 扫描的 SNMP Trap 功能。
show anti-arpscan [trust <ip port supertrust-port> prohibited <ip port>]	显示防 ARP 扫描的运行和配置情况。
特权用户配置模式	

debug anti-arpscan <port ip> no debug anti-arpscan <port ip>	打开或关闭防 ARP 扫描的调试开关。
---	---------------------

2.3 防ARP扫描典型案例

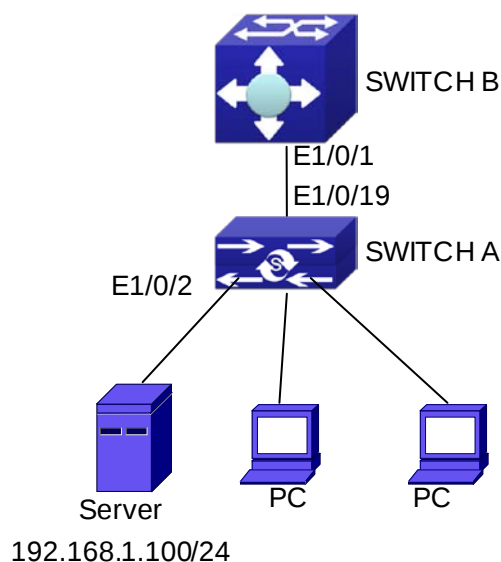


图 2-1 防 ARP 扫描典型配置案例

在上述网络拓扑图中，SWITCH B 的端口 e1/0/1 与 SWITCH A 的端口 e1/0/19 相连，SWITCH A 上的端口 e1/0/2 与文件服务器(IP 地址为 192.168.1.100/24)相连，其他端口都与普通 PC 相连。可通过下面的配置有效地防止 ARP 扫描，而又不影响系统的正常运行。

SWITCH A 配置任务序列：

```

SwitchA(config)#anti-arpscan enable
SwitchA(config)#anti-arpscan recovery time 3600
SwitchA(config)#anti-arpscan trust ip 192.168.1.100 255.255.255.0
SwitchA(config)#interface ethernet1/0/2
SwitchA (Config-If-Ethernet1/0/2)#anti-arpscan trust port
SwitchA (Config-If-Ethernet1/0/2)#exit
SwitchA(config)#interface ethernet1/0/19
SwitchA (Config-If-Ethernet1/0/19)#anti-arpscan trust supertrust-port
Switch A(Config-If-Ethernet1/0/19)#exit
  
```

SWITCH B 配置任务序列：

```

SwitchB(config)#anti-arpscan enable
SwitchB(config)#interface ethernet1/0/1
SwitchB(Config-If-Ethernet1/0/1)#anti-arpscan trust port
  
```

```
SwitchB(Config-If-Ethernet1/0/1)exit
```

2.4 防ARP扫描排错帮助

- ☞ 防ARP扫描默认是关闭的。打开防ARP扫描后，可以同时打开调试开关debug anti-arpscan来查看调试信息。

第3章 ARP、ND绑定配置

3.1 概述

3.1.1 ARP（地址解析协议）

简单地说，ARP（RFC-826）协议主要负责将局域网中的 IP 地址转换为对应的 48 位物理地址，即网卡的 MAC 地址，比如 IP 地址为 192.168.0.1 网卡 MAC 地址为 00-03-0F-FD-1D-2B。整个转换过程是一台主机先向目标主机发送包含 IP 地址信息的广播数据包，即 ARP 请求，然后目标主机向该主机发送一个含有 IP 地址和 MAC 地址数据包，通过 MAC 地址两个主机就可以实现数据传输了。

3.1.2 ARP绑定

按照 ARP 协议的设计，为了减少网络上过多的 ARP 数据通信，一台主机，即使收到的 ARP 应答并非自己请求得到的，它也会将其插入到自己的 ARP 缓存表中，这样，就造成了“ARP 绑定”的可能。如果黑客想探听同一网络中两台主机之间的通信（即使是通过交换机相连），他会分别给这两台主机发送一个 ARP 应答包，让两台主机都“误”认为对方的 MAC 地址是第三方即黑客所在的主机，这样，双方看似“直接”的通信连接，实际上都是通过黑客所在的主机间接进行的。黑客一方面得到了想要的通信内容，另一方面，只需要更改数据包中的一些信息，成功地做好转发工作即可。在这种嗅探方式中，黑客所在主机是不需要设置网卡的混杂模式的，因为通信双方的数据包在物理上都是发送给黑客所在的中转主机的。

3.1.3 如何进行ARP/ND绑定

由于现在网络上充斥着很多基于 ARP 协议的嗅探、监听及攻击行为，而且几乎所有的攻击行为都是基于 ARP 绑定来进行的，所以如何防止 ARP 绑定就显得十分重要。ARP 绑定首先是通过伪造合法 IP 进入正常的网络环境，向交换机发送大量的伪造的 ARP 申请报文，交换机在学习到这些报文后，可能会覆盖原来学习到的正确的 IP、MAC 地址的映射关系，将一些正确的 IP、MAC 地址映射关系修改成攻击报文设置的对应关系，导致交换机在转发报文时出错，从而影响整个网络的运行。或者交换机被恶意攻击者利用，利用错误的 ARP 表，截获交换机转发的报文或者对其它服务器、主机或者网络设备进行攻击。

在网络中防止基于 ARP 的攻击和绑定交换机的方法有两种：

一、关闭交换机的自动更新功能

关闭交换机的自动更新功能以后，当交换机收到 ARP 报文时，如果是新的 ARP 报文（交换机的 ARP 表中不存在该 IP 的表项），则正常学习，这样新的用户可以正常登录网络；如果该 ARP 报文对应的 IP 地址在交换机的 ARP 表中已经存在，则判断 ARP 报文中的 MAC

地址、收到 ARP 报文的端口和交换机 ARP 表中记录的是否相同，不相同则认为是欺骗报文予以丢弃，相同则正常接收，相应的 ARP 表项老化定时器被重置。通过该机制可以防止合法的 ARP 表项被欺骗报文篡改，从而可以避免交换机遭受 ARP 绑定和攻击。

二、关闭交换机的自动学习功能

关闭交换机的自动学习功能以后，交换机不再接收 ARP 报文，适合静态配置 ARP 表项的场合。一方面可以配置静态 ARP 表项，另一方面可以将当前学习到的动态 ARP 表项转换为静态表项（可以减轻一一配置 ARP 静态表项所带来的繁重工作量。关闭交换机的自动学习功能时，如果动态表项不转换为静态表项，会正常老化掉）。在 ARP 表项均为静态配置的情况下，可以有效地避免 ARP 绑定。

ND 是 IPV6 协议中的邻居发现协议，其工作原理同 ARP 类似，因此我们采取同 ARP 绑定相同的方法处理利用 ND 进行绑定和攻击的手段。

3.2 ARP、ND绑定配置

配置 ARP、ND 绑定配置序列如下：

1. 关闭 ARP、ND 自动更新功能
2. 关闭 ARP、ND 自动学习与更新功能
3. 将动态的 ARP、ND 转化为静态 ARP、ND 的功能

1. 关闭 ARP、ND 自动更新功能

命令	解释
全局配置模式和接口配置模式	
ip arp-security updateprotect no ip arp-security updateprotect ipv6 nd-security updateprotect no ipv6 nd-security updateprotect	关闭和启动 ARP、ND 的自动更新功能。

2. 关闭 ARP、ND 自动学习与更新功能

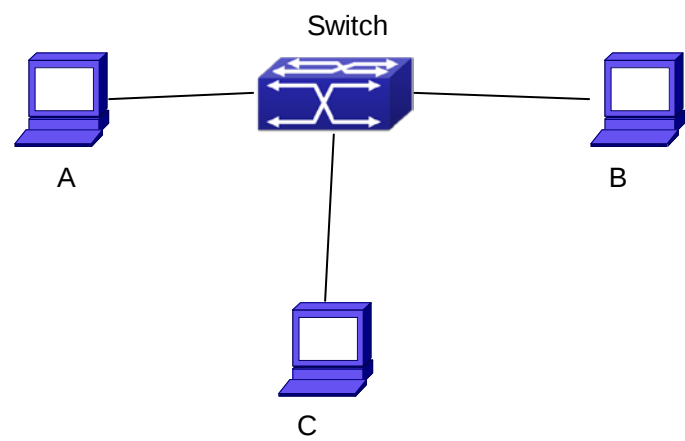
命令	解释
全局配置模式和接口配置模式	
ip arp-security learnprotect no ip arp-security learnprotect ipv6 nd-security learnprotect no ipv6 nd-security learnprotect	关闭和启动 ARP、ND 的自动学习与更新功能。

3. 将动态的 ARP、ND 转化为静态 ARP、ND 的功能

命令	解释
全局配置模式和接口配置模式	

<code>ip arp-security convert</code> <code>ipv6 nd-security convert</code>	将动态 ARP、ND 转化静态。
---	------------------

3.3 ARP、ND绑定举例



设备说明：

设备	配置	数量
switch	IP:192.168.2.4; IP:192.168.1.4; mac: 00-00-00-00-00-04	1
A	IP:192.168.2.1; mac: 00-00-00-00-00-01	1
B	IP:192.168.1.2; mac: 00-00-00-00-00-02	1
C	IP:192.168.2.3; mac: 00-00-00-00-00-03	若干

在上图中首先 B 与 C 正常通信。A 想要交换机将 B 发给 C 的报文转发给自己，所以需要交换机将从 B 来的报文发给 A。首先 A 先发送 ARP 应答包给交换机，格式如：192.168.2.3，00-00-00-00-00-01。就是将自己的 MAC 地址换上 C 的 IP，这样交换机在更新 ARP 表时就会将 B 发给 IP 地址：192.168.2.3 的数据报发到 00-00-00-00-00-01 的地址（A 地址）去了。

进一步将 A 也可以将收到的数据报中的源地址，目的地址更改下，让交换机将自己发的包给 C，这样 B 与 C 相互通信的数据在不知情的状况下就都可以被 A 接收。由于 ARP 表是定时更新的，所以 A 还有 1 个任务是持续不断的向交换机发送 ARP 应答包，刷新交换机的 ARP 表。

所以重要的是将 ARP 表保护起来，可以在环境稳定后配置禁止 ARP 学习的命令，然后将所有的动态 ARP 转换为静态的，这样已经学习到的 ARP 就不会被刷新，从而为用户提供保护。

```
Switch(config)#
Switch(Config)#interface vlan 1
Switch(Config-If-Vlan1)#arp 192.168.2.1 00-00-00-00-00-01 interface eth 1/0/2
```

```
Switch(Config-If-Vlan1)#interface vlan 2
Switch(Config-If-Vlan2)#arp 192.168.1.2 00-00-00-00-00-02 interface eth 1/0/2
Switch(Config-If-Vlan2)#interface vlan 3
Switch(Config-If-Vlan3)#arp 192.168.2.3 00-00-00-00-00-03 interface eth 1/0/2
Switch(Config-If-Vlan3)#exit
Switch(Config)#ip arp-security learnprotect
Switch(Config)#
Switch(config)#ip arp-security convert
```

如果环境经常变动，也可以开启禁止 ARP 更新的命令，这样一旦学习到的 ARP 属性，就不会被新的 ARP 应答包所更新，保护用户数据不会被“嗅探”。

```
Switch#config
Switch(config)#ip arp-security updateprotect
```

第4章 ARP GUARD配置

4.1 ARP GUARD 的介绍

ARP 协议的设计存在严重的安全漏洞，任何网络设备都可以发送 ARP 报文通告 IP 地址和 MAC 地址的映射关系。这就为 ARP 欺骗提供了可乘之机，攻击者发送 ARP REQUEST 报文或者 ARP REPLY 报文通告错误的 IP 地址和 MAC 地址映射关系，导致网络通讯故障。ARP 欺骗的危害主要表项为两种形式：1、PC4 发送 ARP 报文通告 PC2 的 IP 地址映射为自己的 MAC 地址，将导致本应该发送给 PC2 的 IP 报文全部发送到了 PC4，这样 PC4 就可以监听、截获 PC2 的报文；2、PC4 发送 ARP 报文通告 PC2 的 IP 地址映射为非法的 MAC 地址，将导致 PC2 无法接收到本应该发送给自己的报文。特别是如果攻击者假冒网关进行 ARP 欺骗，将导致整个网络瘫痪。

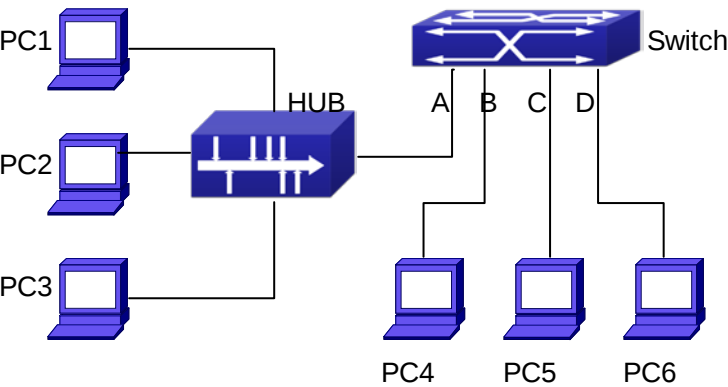


图 4-1 ARP GUARD 原理图

我们利用交换机的过滤表项保护重要网络设备的 ARP 表项不能被其它设备假冒。基本原理就是利用交换机的过滤表项，检测从端口输入的所有 ARP 报文，如果 ARP 报文的源 IP 地址是受到保护的 IP 地址，就直接丢弃报文，不再转发。

ARP GUARD 功能常用于保护网关不被攻击，如果要保护网络内的所有接入 PC 不受 ARP 欺骗攻击，需要在端口配置大量受保护的 ARP GUARD 地址，这将占用大量芯片 FFP 表项资源，可能会因此影响到其它应用功能，并不适合。此时推荐采用 FREE RESOURCE 相关接入方案，详情请参考相关文档。

4.2 ARP GUARD配置任务序列

1. 配置受到保护的 IP 地址

命令	解释
端口配置模式	

arp-guard ip <addr> no arp-guard ip <addr>	配置/删除 ARP GUARD 地址。
---	---------------------

第5章 Arp local proxy配置

说明：

本章所指的三层交换机代表了一般意义下的路由器或运行了路由协议的无线控制产品。

5.1 Arp local proxy功能简介

某种实际的应用环境中，为了防止 ARP 的欺骗，要求汇聚层的交换机实现 local arp proxy 功能，限制 ARP 报文在同一 vlan 内的转发，从而引导数据流量通过交换机进行 L3 转发。

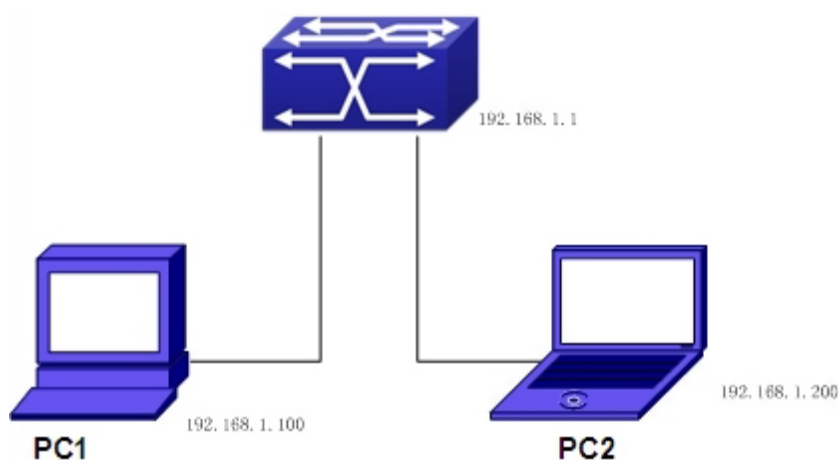


图 5-1 Arp local proxy 功能示意图

例如上图，PC1 要向 PC2 发送一个 IP 报文，整个的流程大致如下（省略了一些非 ARP 的细节）：

1. 由于 PC1 没有 PC2 的 ARP，因此 PC 发送 ARP REQUEST 并广播出去。
2. 交换机硬件收到 ARP 报文，依据新的 ARP 处理规则，芯片不会硬件转发该报文，只是把 ARP REQUEST 送 CPU。
3. 在启动 local arp proxy 的情况下，交换机向 PC1 发送 arp reply 报文（填充自己的 mac 地址）。
4. PC1 收到该 arp reply 之后，创建 ARP，发送 ip 报文，封装的以太网头的目的 MAC 为交换机的 MAC。
5. 当交换机收到该 ip 报文之后，交换机查询路由表（创建路由缓存），并下发硬件表项。
6. 当交换机有 PC2 的 ARP 的情况下，直接封装以太网头部并发送报文（目的 MAC 为 PC2）。
7. 如果交换机没有 PC2 的 ARP，那么会请求 PC2 的 ARP，然后发送 ip 报文。

该功能通常需要和其他的安全功能配合使用，例如在汇聚交换机上配置 local arp

proxy，而在下连的二层交换机上配置端口隔离功能，这样将会引导所有的 ip 流量通过汇聚交换机上进行三层转发，而由于端口隔离，ARP 报文不会在 vlan 内转发，其他 PC 也不会收到。

5.2 Arp local proxy功能配置任务序列

1. 启动/关闭 arp local proxy 功能

1. 启动/关闭 arp local proxy 功能

命令	解释
VLAN 接口配置模式	
ip local proxy-arp no ip local proxy-arp	启动或者关闭 arp local proxy 功能。

5.3 Arp local proxy功能典型案例

如下图所示，S1 为支持 arp local proxy 的中高端三层交换机，S2 为支持端口隔离的二层接入交换机。

为了安全的考虑，在 S2 上启动端口隔离功能，这样 S2 的所有下连端口彼此隔离，所有的 ARP 报文都能通过 S1 转发。如果再在 S1 上启动 arp local proxy，则在 S1 上的所有端口隔离 ARP，同时代理 ARP，从而引导 IP 流量经过 S1 进行 3 层转发，而不是原来的 2 层转发。

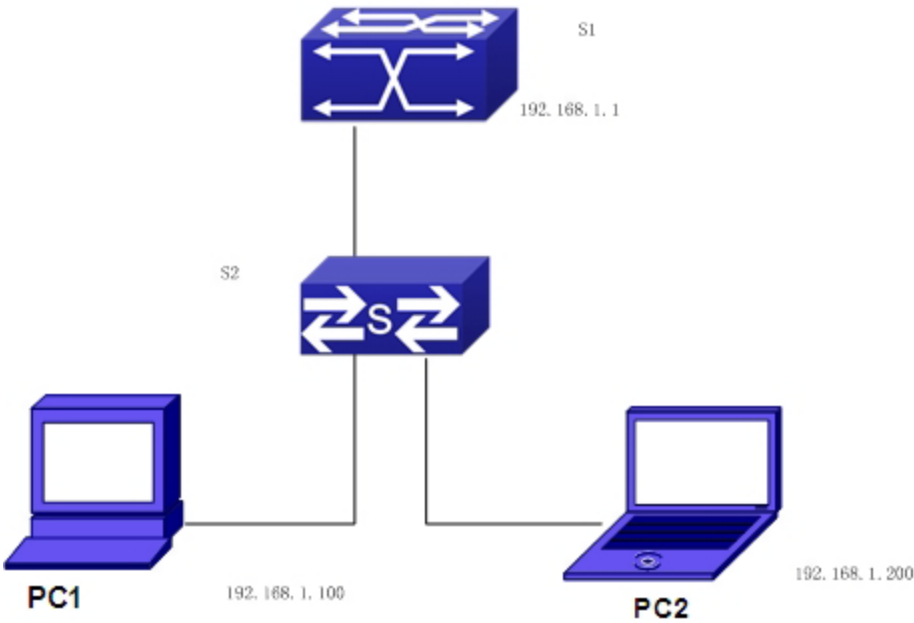


图 5-2 Arp local proxy 功能典型案例示意图

我们可以对 S1 进行如下配置：

```
Switch(config)#interface vlan 1
```

```
Switch(Config-if-Vlan1)#ip address 192.168.1.1 255.255.255.0
```

```
Switch(Config-if-Vlan1)#ip local proxy-arp
```

```
Switch(Config-if-Vlan1)#exit
```

5.4 Arp local proxy 功能排错帮助

arp local proxy 功能默认是关闭的，可以使用显示命令（show running-config）看目前的配置情况。在确认配置正确的情况下，打开 ARP 的 debug，可以看到是不是成功代理 ARP，并发送代理 ARP 报文。

在操作过程中，如果有操作错误，系统将会给出具体的错误提示信息。

第6章 免费ARP发送功能操作配置

6.1 免费ARP发送功能简介

主机发送以自己 IP 地址为目标 IP 地址的 ARP 请求，这种 ARP 请求称为免费 ARP（gratuitous ARP）。

交换机基于三层接口的免费 ARP 发送功能的整体思路是：在交换机的接口模式下配置该接口定时发送免费 ARP 报文；或者在交换机的全局配置模式下配置交换机系统中所有存在的接口定时发送免费 ARP 报文。

在本系统中主要实现免费 ARP 的如下两个作用：

- 1. 减少局域网内主机向交换机网关发送 ARP 请求的次数。局域网内主机会每隔一段时间向交换机网关发送 ARP 请求，请求网关的 MAC 地址。如果交换机每隔一段时间向局域网内广播免费 ARP，这样局域网内主机就不用发送 ARP 请求了，从而减少了局域网内主机向网关发送 ARP 请求的次数。
- 2. 可以防止针对网关的 ARP 欺骗。交换机定时向局域网内主机广播免费 ARP，这样局域网内主机的 ARP 缓存会定时更新，所以在局域网内主机受到针对网关的 ARP 欺骗后，主机会在收到交换机的免费 ARP 后，更新其 ARP 缓存而得到正确网关 MAC 地址，这样就防止了针对网关的 ARP 欺骗。

6.2 免费ARP发送功能配置任务序列

- 1. 启动免费 ARP 发送功能和配置免费 ARP 报文的发送时间间隔
- 2. 显示免费 ARP 发送功能的配置信息

1. 启动免费 ARP 发送功能和配置免费 ARP 报文的发送时间间隔

命令	解释
全局配置模式和接口配置模式	
ip gratuitous-arp <5-1200> no ip gratuitous-arp	使能免费 ARP 发送功能，并设置发送免费 ARP 报文的发送时间间隔。其中 no 操作取消使能免费 ARP 发送功能。

2. 显示免费 ARP 发送功能的配置信息

命令	解释
特权和配置模式	

```
show ip gratuitous-arp [interface vlan
<1-4094>]
```

显示免费 ARP 发送功能的配置信息。

6.3 免费 ARP 发送功能典型案例

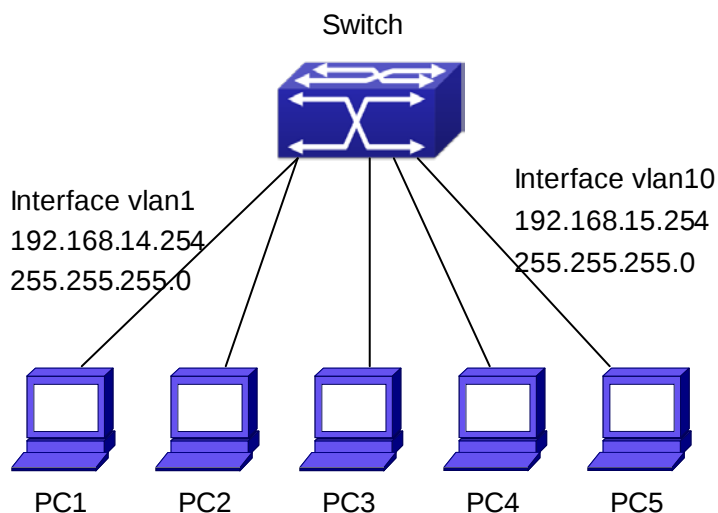


图 6-1 免费 ARP 发送功能配置案例

在上述网络拓扑图中，Switch 系统中的 interface vlan 10（IP 地址为 192.168.15.254，子网掩码为：255.255.255.0）下连接有 3 台 PC 主机（PC3、PC4 和 PC5），interface vlan 1（IP 地址为：192.168.14.254，子网掩码为：255.255.255.0）下连接有两台 PC 主机（PC1 和 PC2）。可通过如下方法配置免费 ARP 发送功能：

1. 一次设置两个接口的免费 ARP 发送功能

```
Switch(config)#ip gratuitous-arp 300
```

```
Switch(config)#exit
```

2. 一次设计一个接口的免费 ARP 发送功能

```
Switch(config)#interface vlan 10
```

```
Switch(Config-if-Vlan10)#ip gratuitous-arp 300
```

```
Switch(Config-if-Vlan10)#exit
```

```
Switch(config)#exit
```

6.4 免费 ARP 发送功能排错帮助

免费 ARP 发送功能默认是关闭的。打开免费 ARP 发送功能后，可以打开调试开关 debug arp send 来查看交换机发送的 arp 报文信息。

在全局配置模式下使能免费 ARP 发送功能后，必须在全局配置模式才能取消使能免费 ARP 发送功能；在接口配置模式下使能免费 ARP 发送功能后，必须在接口配置模式下才能取消使能免费 ARP 发送功能。

第7章 ND Snooping配置

说明：

本章所指的三层交换机和路由器代表了一般意义下的路由器或运行了路由协议的无线控制产品。

7.1 ND Snooping介绍

ND Snooping 模块开发的意图：利用 Control Packet Snooping(CPS)机制，即通过源 IPv6 地址和锚信息绑定的方式，对端口接入报文进行合法性检测，放行匹配绑定的报文，丢弃不匹配的报文，以达到对直连链路 IPv6 节点准入控制的目的。该模块的需求开发主要参考 IPv6 邻节点发现 (NDP) 协议和《Control Packet Snooping Based Binding draft-bi-savi-cps-00》草案，同时 ND Snooping 还采用了《First-Come First-Serve Source-Address Validation Implementation draft-ietf-savi-fcfs-01》草案的“先来先服务”即先建立绑定的节点为合法节点的安全原则来检查节点的合法性。

ND Snooping 主要应用于接入设备（如二层交换机，无线接入点等）中，接入设备根据端口收到的邻节点发现协议（NDP）报文，建立关于本地链路上节点的绑定信息表（本模块绑定是指 IPv6 地址与节点的 MAC 地址和所属端口 ID 的绑定），然后根据节点绑定信息表项，下发 FFP（Fast Filter Processor）硬件驱动规则，实现本地链路节点的准入控制。

7.2 ND snooping基本配置

ND Snooping 配置任务序列如下：

1. 开启或关闭 ND Snooping 的监控功能
 2. 配置 ND Snooping 的生存期
 - 1) 设置 SAC_BOUND 状态绑定的生存期。
 - 2) 设置 SAC_START 状态绑定的生存期。
 - 3) 设置 SAC_QUERY 状态绑定的生存期。
 3. ND Snooping 的绑定功能
 - 1) 配置 ND Snooping 地址动态绑定策略。
 - 2) 添加一个静态绑定
 - 3) 配置同一 MAC 地址与不同 IPv6 地址建立绑定的最大数目
 - 4) 设置端口的可绑定数目
 - 5) 清除所有 ND Snooping 动态绑定。
 4. 设置交换机的信任端口为 trust 口
-
1. 开启或关闭 ND Snooping 的监控功能

命令	解释
全局配置模式	
ipv6 nd snooping enable no ipv6 nd snooping enable	开启或关闭 ND Snooping 全局功能。
端口配置模式	
ipv6 nd snooping user-control no ipv6 nd snooping user-control	开启或关闭 ND Snooping 端口功能。

2. 配置 ND Snooping 的生存期

命令	解释
全局配置模式	
[no] ipv6 nd snooping max-sac-lifetime <max-sac-lifetime>	重新设置 SAC_BOUND 状态绑定生存期为<max-sac-lifetime>或 2 小时。
[no] ipv6 nd snooping max-dad-delay <max-dad-delay>	重新设置 SAC_START 状态绑定生存期为<max-dad-delay>或 1 秒。
[no] ipv6 nd snooping max-dad-prepare-delay <max-dad-prepare-delay>	重新设置 SAC_QUERY 状态绑定生存期为<max-dad-prepare-delay>或 0.5 秒。

3. ND Snooping 的绑定功能

命令	解释
全局配置模式	
ipv6 nd snooping policy {bind-eui64-address bind-non-eui64-address} no ipv6 nd snooping policy	配置 ND Snooping 地址动态绑定策略。
ipv6 nd snooping static-binding <ipv6-address> hardware-address <hardware-address> interface <interface-name> no ipv6 nd snooping static-binding <ipv6-address>	添加一个静态绑定。
ipv6 nd snooping mac-binding-limit <number> no ipv6 nd snooping mac-binding-limit	配置同一 MAC 地址与不同 IPv6 地址建立绑定的最大数目。
端口配置模式	解释

ipv6 nd snooping port-binding-limit <binding-number>	设置端口的可绑定数目,该绑定数目只限制端口上的动态绑定数目,不限制端口上的静态绑定数目。
no ipv6 nd snooping port-binding-limit	
特权配置模式	解释
clear ipv6 nd snooping binding [<interface-name>]	清除所有 ND Snooping 动态绑定。

4. 设置交换机的信任端口为 trust 口

命令	解释
全局配置模式	
ipv6 nd snooping trust no ipv6 nd snooping trust	设置交换机的信任端口为 trust 口。

7.3 ND Snooping 举例

典型案例：

ND Snooping 应用典型环境如下图所示：

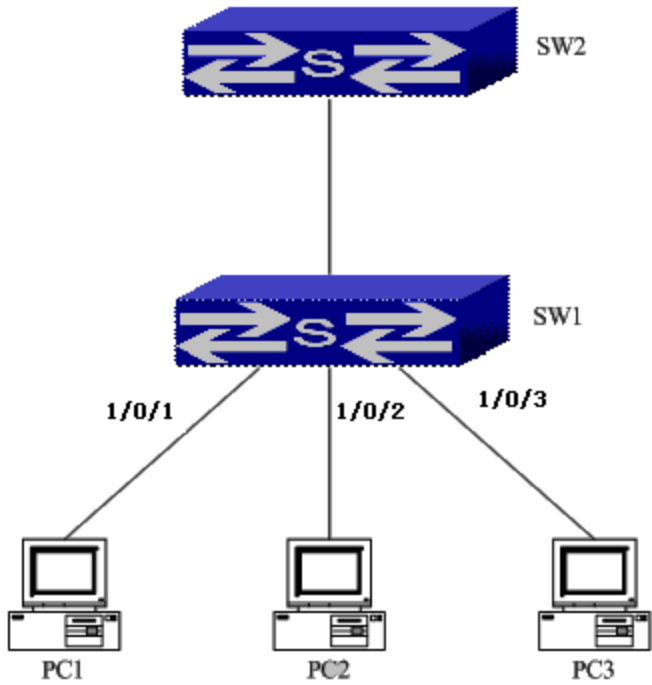


图 7-1 ND Snooping 典型配置

配置说明：

SW2 为三层交换机，下连 SW1 二层交换机，在 SW2 启用 IPv6 功能和 RA 功能；
SW1 为二层交换机，启用 IPv6 功能，并同时启用 ND Snooping 全局功能，并在下连

三台 PC 节点的端口启用 ND Snooping 控制功能。

PC1, PC2, PC3 为三台 PC 机, 每台 PC 机都已安装 IPv6 协议, 直连 SW1, 直连端口分别为 1/0/1, 1/0/2, 1/0/3。

ND Snooping 在二层交换机 SW1 启用后, PC1、PC2 和 PC3 正确收到 SW2 三层交换机发来的 RA 路由器公告报文, 根据 RA 报文中的链路前缀 2001::/64, 三台 PC 机自动生成 IPv6 地址, 分别为:

PC1 : FE80::2AA:FF:FE9A:4CA2 、 2001::2AA:FF:FE9A:4CA2 、 2001::23:4A:1122:C411;

PC2 : FE80::2BB:FF:FE9A:4CA2 、 2001::2BB:FF:FE9A:4CA2 、 2001::32:4B:2211:11C4;

PC3 : FE80::2CC:FF:FE9A:4CA2 、 2001::2CC:FF:FE9A:4CA2 、 2001::22:4A:1133:C422;

同时, 三台 PC 机向直连链路发送重复地址检测 DAD NS 报文, ND Snooping 模块根据收到的 DAD NS 报文, 建立相应的动态绑定表, 动态绑定表项如下表:

IPv6 地址	MAC 地址	端口号
FE80::2AA:FF:FE9A:4CA2	02-AA-00-9A-4C-A2	1/0/1
2001::2AA:FF:FE9A:4CA2	02-AA-00-9A-4C-A2	1/0/1
2001::23:4A:1122:C411	02-AA-00-9A-4C-A2	1/0/1
FE80:: BB:FF:FE9A:4CA2	02-BB-00-9A-4C-A2	1/0/2
2001::2BB:FF:FE9A:4CA2	02-BB-00-9A-4C-A2	1/0/2
2001::32:4B:2211:11C4	02-BB-00-9A-4C-A2	1/0/2
FE80:: CC:FF:FE9A:4CA2	02-CC-00-9A-4C-A2	1/0/3
2001::2CC:FF:FE9A:4CA2	02-CC-00-9A-4C-A2	1/0/3
2001::22:4A:1133:C422	02-CC-00-9A-4C-A2	1/0/3

在规定的时间内, 三台 PC 机没有收到回应的 DAD NA 报文, 则根据动态绑定表, 端口 1/0/1, 1/0/2, 1/0/3 下发绑定表项的 FFP 硬件驱动表项。对端口后续收到的数据报文进行源地址检测, 如果匹配绑定表项, 则放行 IPv6 报文, 否则直接拒绝 IPv6 报文。

配置步骤如下:

SW1:

```
SW1(config)# ipv6 nd snooping enable
```

```
SW1(config)# interface vlan 1
```

```
SW1(config-if-vlan1)# ipv6 address 2001::1/64
```

```
SW1(config)# interface ethernet 1/0/1; 1/0/2; 1/0/3
```

```
SW1(config-if-port-range)# ipv6 nd snooping user-control
```

SW2:

```
SW2(config)# interface vlan 1
```

```
SW2(config-if-vlan1)# ipv6 address 2001::2/64
```

```
SW2(config-if-vlan1)# no ipv6 nd suppress-ra
```

7.4 ND Snooping排错帮助

当在使用 ND Snooping 过程中遇到问题，请检查是否是如下原因：

- ☞ 是否启动了全局 `ipv6 nd snooping enable`，并且是否在端口上配置了 `ipv6 nd snooping user-control`。
- ☞ 通过 `debug ipv6 nd snooping` 观察交换机能否能正确接收和处理相关的报文。
- ☞ 交换机先和 PC 链接，等端口 UP 后，再开启 ND Snooping 功能，会建立不了绑定，因为此时 PC 不会再发 DAD NS 报文，要再将连接 PC 的端口 `shutdown/no shutdown`。

第8章 Keepalive gateway配置

说明：

本章所指的三层交换机和路由器代表了一般意义下的路由器或运行了路由协议的无线控制产品。

8.1 keepalive gateway介绍

市场需要使用以太网端口参与备份或者负载均衡，由于以太网端口是广播式信道，在网关 down 的情况下由于检测不到物理信号的变化，所以以太网端口无法 down 下来。该功能主要用在网关使用以太网端口上连上一级网关形成点到点的网络拓扑的情况下，希望可以检测到上一级网关的连通性。

例如：路由器连接光端机，路由器到光端机的线路始终是 up 的，而 modem 与远端设备之间的线路不通的时候环境下，需要使用有效手段检测对端设备是否可达。目前，使用 ARP 机制来检测网关的连通性，通过定时的给网关发送 ARP 请求来探测网关的连通性，如果 ARP 解析失败，表明网关已经 down，这时 down 掉三层接口；继续定时的发送 ARP 请求，如果 ARP 解析成功，则 up 接口。

该功能只对三层交换机支持，二层交换机不支持。

8.2 keepalive gateway功能配置任务序列

1. 开启或关闭 keepalive gateway 功能和配置发送 ARP 请求报文的间隔周期和判定探测失败的重试次数
2. 显示接口 keepalive gateway 运行情况和接口 ipv4 运行状态

1. 启动 keepalive gateway 功能和配置发送 ARP 请求报文的间隔周期和判定探测失败的重试次数

命令	解释
接口配置模式	
keepalive gateway <ip-address> [{<interval-seconds> msec <interval-millisecond >}] [retry-count]	使能 keepalive gateway 功能，配置探测的网关 IP 地址、发送 ARP 请求报文的间隔周期和判定探测失败的重试次数；no 命令为关闭该功能。
no keepalive gateway	

2. 显示接口 keepalive gateway 运行情况和接口 ipv4 运行状态

命令	解释
----	----

特权和配置模式	
show keepalive gateway [interface-name]	显示指定接口的 keepalive 运行情况。如果不指定则显示所有接口的 keepalive 运行情况。
show ip interface [interface-name]	显示指定接口的 IPv4 运行状态。如果不指定则显示所有接口的 IPv4 运行状态。

8.3 keepalive gateway 举例

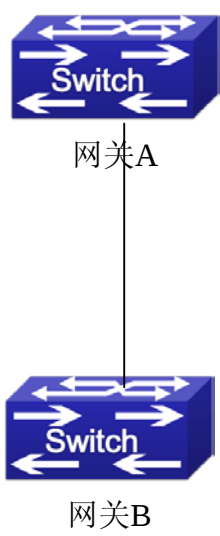


图 8-1 keepalive gateway 典型应用举例

在上述网络拓扑中，网关 A interface vlan10 接口地址为 1.1.1.1 255.255.255.0，网关 B interface vlan100 接口地址为 1.1.1.2 255.255.255.0，网关 B 支持 keepalive gate 功能，可通过如下方法配置网关 B 上的 keepalive gateway 功能：

- 1、采用默认的发送 arp 间隔和判定探测失败重复次数（缺省发送 arp 探测报文周期为 10s，缺省判定探测失败重复次数为 5 次）

```
Switch(config)#interface vlan 100
Switch(config-if-vlan100)#keepalive gateway 1.1.1.1
Switch(config-if-vlan100)#exit
```

- 2、手动配置发送 arp 间隔和判定探测失败重复次数

```
Switch(config)#interface vlan 100
Switch(config-if-vlan100)#keepalive gateway 1.1.1.1 3 3
Switch(config-if-vlan100)#exit
```

探测网关 A 是否可达，每隔 3 秒发送一次 ARP 探测，探测 3 次失败后认为网关 A 不可达。

8.4 keepalive gateway 排错帮助

当在使用 keepalive gateway 过程中遇到问题，请检查是否是如下原因：

- ☞ 确认设备为三层交换机，二层交换机不支持该功能。
- ☞ 该种探测方法仅适用于点对点的拓扑模式。
- ☞ 该方法是探测的 IPv4 可达性。因此探测结果，只能影响接口的 IPv4 工作状态。当探测失败时，只能禁止接口上不再运行 IPv4 业务；但 IPv6 等其它业务不受该探测的影响。
- ☞ 接口的物理状态仅受物理信号的控制，不受该探测功能的控制。
- ☞ 当判定网关不可达后，接口不能运行 IPv4 业务。因此所有同该接口相关的 IPv4 路由被删除，IPv4 路由协议不能在该接口上建立邻居。