实验二 端口镜像

【实验目的】

1、掌握在交换机上配置端口镜像的方法；

2、通过网络协议分析仪验证端口镜像是否配置正确；

3、掌握网络协议分析仪的基本使用方法。

【实验学时】

4 学时

【实验环境】

在如图 2- 19 所示的实验拓扑图中，在交换机上配置端口镜像，在主机 C 上安装锐捷协议分析教学系统，通过其中的网络协议分析仪，对主机 A 和主机 B 之间的数据进行捕获。

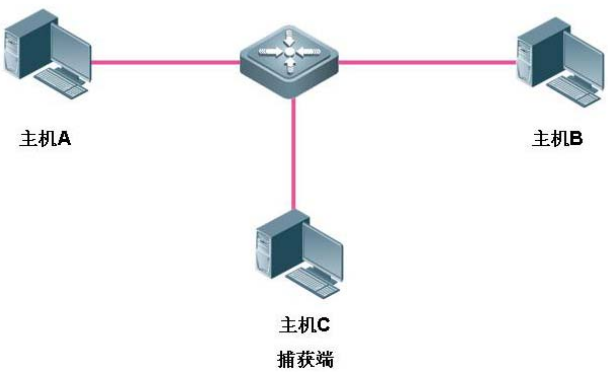

图 2- 19 实验拓扑图

【实验内容】

1、学会在交换机上配置端口镜像的方法；

2、学会使用网络协议分析仪捕获网络中特定主机流量的方法；

3、学习网络协议分析仪的各个组成部分及其功能；

4、学会分析数据帧的 MAC 首部和 LLC 首部的内容；

5、理解 MAC 地址的作用；

6、理解 MAC 首部中的长度/类型字段的功能；

7、学会观察并分析数据帧中的各个字段内容。

【实验流程】

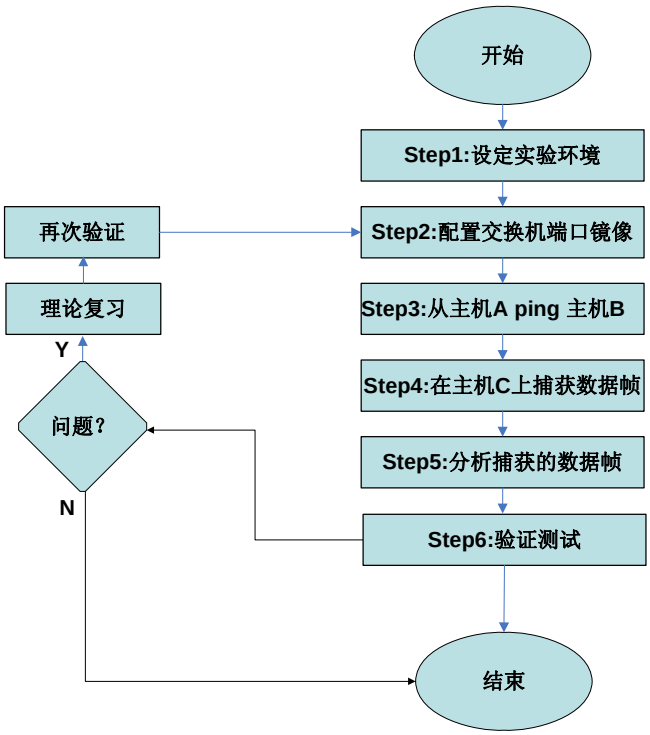

图 2- 20 实验流程图

【实验原理】

根据交换机的转发原理，交换机在收到一个数据帧后，根据该数据帧的目的 MAC 地址，通过查找 MAC 地址表可以将数据帧转发给目的主机。这时，如果该 MAC 地址已经存在于 MAC 地址表中，则交换机上连接的其余主机是没有机会收到该帧的。如图 2- 21 所示，主机 A 和主机 B 之间的数据流，主机 C 是无法接收到的，即使安装了网络协议分析仪，也不能捕获主机 A 和主机 B 之间的数据。

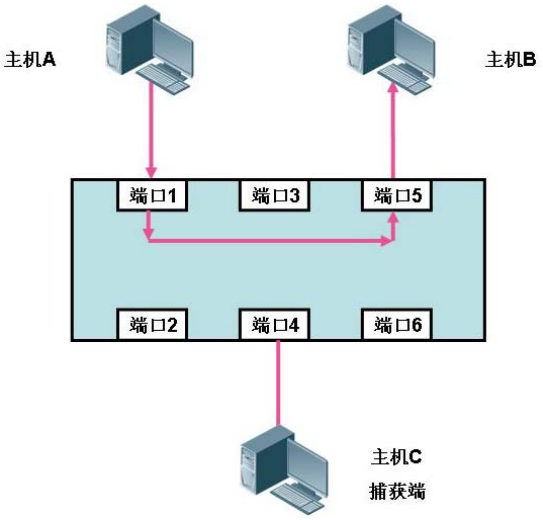

图 2- 21 没有端口镜像的时候

但有时，出于一定的目的，例如想要监控特定主机的流量、部署 IDS 或者进行网络故障排查，就需要使用交换机的端口镜像功能，以便能够捕获到转发给不同目的主机的流量，对某些可疑端口进行监控，同时又不影响被监控端口的数据交换。如图 2- 22 所示，可以将连接主机 A 和主机 B 的端口镜像到连接主机 C 的端口上，这样，主机 A 和主机 B 之间的数据就可以被主机 C 捕获到了。

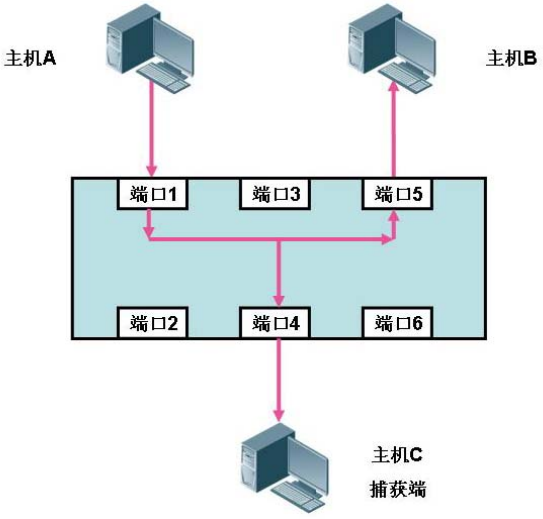

图 2- 22 有端口镜像的时候

简单的说，端口镜像就是把交换机一个或多个端口（源端口）的流量——包括发送和接收的流量——完全拷贝一份，发送给另外一个端口（目的端口），以便目的端口的主机可以

收到源端口的所有进出数据帧。这期间，目的端口不能收发自己的数据帧，完全作为源端口的镜像存在。

端口镜像的数据流主要分为三类：

(1)、输入数据流（RX）：指被源端口接收进来，其数据副本发送至监控端口的数据流；

(2)、输出数据流（TX）：指从源端口发送出去，其数据副本发送至监控端口的数据流；

(3)、双向数据流（Both）：即为以上两种的综合。

在交换机上配置端口镜像需要在全局模式下，包括 2 个步骤：配置源端口和配置目的端口，命令格式为：

Switch(config)# monitor session session_number source/destination interface type interface-id [rx/tx/both]

其中：

monitor session：配置端口镜像的命令关键字；

session-number：端口镜像的会话号，依据不同的设备型号支持的会话数不同，锐捷网络的 RG-S3750-24 型交换机支持 1 个会话；

source/destination：指明后续的端口号是端口镜像的源端口还是目的端口；

interface type interface-id：指定接口号，即镜像的源端口或者目的端口。如果指定的是源端口，交换机会把这个端口的流量拷贝一份，可以输入多个端口，多个用“,”隔开，连续的用“-”连接；如果指定的是目的端口，在源端口被拷贝的流量会从这个端口发出去，注意，目的端口号不能被包含在源端口的范围内；

rx/tx/both：可选项，在配置端口镜像的源端口时使用，是指拷贝源端口双向的（both）、仅输入（rx）还是仅输出（tx）的流量，默认是 both。

在配置端口镜像任务时应遵循以下原则：

(1)、对数据进行监控分析的设备应搭接在监控端口上；

(2)、聚合链路端口只能作为端口镜像任务的源端口；

(3)、在设置端口为源端口时，如果没有指定数据流的监控方向，默认为双向；

(4)、当端口镜像任务含有多个源端口时，这些端口可以来自不同的 VLAN；

(5)、取消某一个端口镜像任务的命令是：no monitor session session-number；

(6)、取消所有端口镜像任务的命令是：no monitor session all。

在配置镜像端口过程中，还应考虑到数据流量过大时，设备的处理速度及端口数据缓存的大小，要尽量减少被监控数据包的丢失。

【实验步骤】

步骤一：在交换机上配置端口镜像

主机 A 连接交换机的 FastEthernet 0/1 端口，主机 B 连接交换机的 FastEthernet 0/10 端口，主机 C 连接交换机的 FastEthernet 0/15 端口，在交换机上配置：

```
Switch#configure terminal
Switch(config)#monitor session 1 source interface fastEthernet 0/1 both
！配置源端口为 F0/1 端口，监控双向数据流
Switch(config)#monitor session 1 destination interface fastEthernet 0/15
！配置目的端口为 F0/15 端口
Switch(config)#exit
```

步骤二：从主机 A ping 主机 B

1、为主机 A 配置 IP 地址 192.168.1.10/24，并在主机 A 上运行 ipconfig /all 命令，得到主机 A 的 MAC 地址；

```
Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Realtek RTL8168C(P)/8111C(P) PCI-E G
igabit Ethernet NIC
        Physical Address. . . . . . . . . : 00-21-85-04-8B-DB
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.1.10
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . : 192.168.1.3
```

图 2- 23 主机 A 的 MAC 地址

2、为主机 B 配置 IP 地址 192.168.1.20/24，并在主机 B 上运行 ipconfig /all 命令，得到主机 B 的 MAC 地址；

```
Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Intel(R) PRO/1000 PL Network Connect
ion
        Physical Address. . . . . . . . . : 00-15-58-2F-7E-7E
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.1.20
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . : 192.168.1.3
```

图 2- 24 主机 B 的 MAC 地址

3、为主机 C 配置 IP 地址 192.168.1.30/24，并在主机 C 上运行 ipconfig /all 命令，得到主机 C 的 MAC 地址；

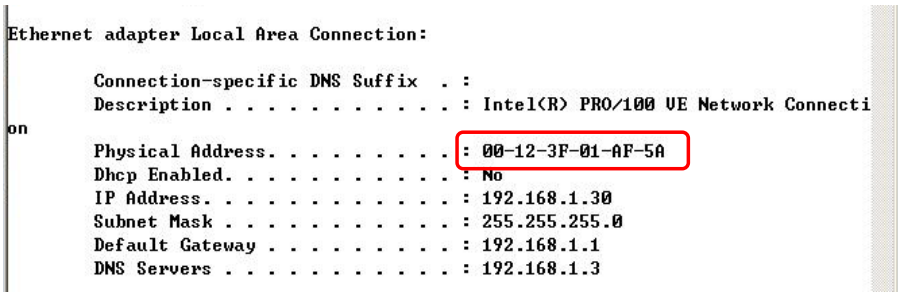

图 2- 25 主机 C 的 MAC 地址

4、从主机 A ping 主机 B，可以看到主机 A 的 Windows 系统会发出 4 个 ping 包，并收到主机 B 的 4 个响应数据包；

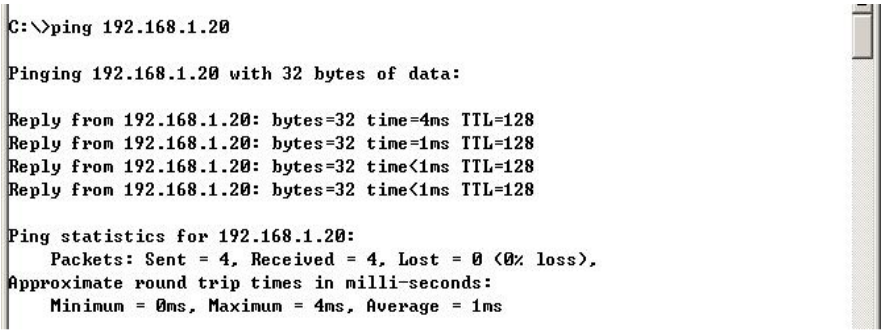

图 2- 26 主机 A ping 主机 B

步骤三：在主机 C 上运行网络协议分析仪捕获数据包

1、在主机 A ping 主机 B 的同时，在主机 C 上运行网络协议分析仪，点击工具栏上的“开始”按钮，捕获数据包，并在 ping 命令运行结束后，点击工具栏上的“结束”按钮，停止捕获；

2、可以在网络协议分析仪的“会话树”中，看到 8 个 ICMP 数据包，说明已经捕获到全部的 ping 数据包；

3、将捕获到的数据包“导出”保存。

步骤四：对捕获的数据包进行分析

图 2- 27 显示了捕获的结果，8 个单播的 ICMP 协议数据包：

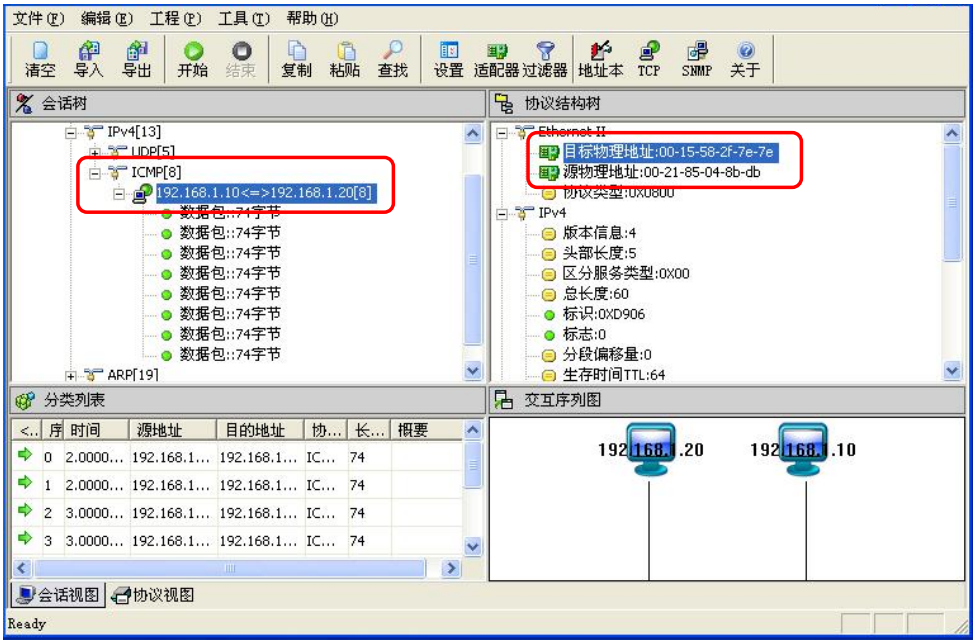

图 2- 27 端口镜像捕获结果

从中可以看出，IP 地址为 192.168.1.30/24，MAC 地址为 00-12-3f-01-af-5a 的主机 C，捕获到了主机 A （IP 地址为 192.168.1.10/24，MAC 地址为 00-21-85-04-8b-db）和主机 B（IP 地址为 192.168.1.20/24，MAC 地址为 00-15-58-2f-7e-7e）之间的单播数据包，说明端口镜像正在生效。

步骤五：验证测试

使用命令将交换机中的端口镜像配置清除：

Switch(config)#no monitor session 1

此时，从主机 A ping 主机 B，在主机 C 上用网络协议分析仪进行捕获，会发现无法捕获到主机 A、B 之间的单播数据包。

【参考配置】

Switch#show run

Building configuration...

Current configuration : 1267 bytes

!

```
hostname Switch
!
!
vlan 1
!
no service password-encryption
!
!
interface FastEthernet 0/1
!
interface FastEthernet 0/2
!
interface FastEthernet 0/3
!
interface FastEthernet 0/4
!
interface FastEthernet 0/5
!
interface FastEthernet 0/6
!
interface FastEthernet 0/7
!
interface FastEthernet 0/8
!
interface FastEthernet 0/9
!
interface FastEthernet 0/10
!
interface FastEthernet 0/11
!
interface FastEthernet 0/12
!
interface FastEthernet 0/13
!
interface FastEthernet 0/14
```

```
!
interface FastEthernet 0/15
!
interface FastEthernet 0/16
!
interface FastEthernet 0/17
!
interface FastEthernet 0/18
!
interface FastEthernet 0/19
!
interface FastEthernet 0/20
!
interface FastEthernet 0/21
!
interface FastEthernet 0/22
!
interface FastEthernet 0/23
!
interface FastEthernet 0/24
!
interface GigabitEthernet 0/25
!
interface GigabitEthernet 0/26
!
interface GigabitEthernet 0/27
!
interface GigabitEthernet 0/28
!
monitor session 1 destination interface FastEthernet 0/15
monitor session 1 source interface FastEthernet 0/1 both
!
!
line con 0
line vty 0 4
```

```
 login
!
end
```

【思考问题】

1、如果只想捕获主机 A 发出的数据包，应该在交换机上如何配置端口镜像？

2、这时如果从主机 C ping 主机 A，是否能 ping 通？