

北京科技大学实验报告

学院：计通学院

专业：信息安全

班级：信安 211

姓名：李晓坤

学号：U202141863

实验日期：2023 年 11 月 30 日

实验名称：

实验一：交换机的基本操作

实验目的：

- (1) 了解交换机配置的方法
- (2) 掌握 CLI 配置环境
- (3) 掌握交换机的基本配置

另外，受限于报告篇幅，对报告中部分图片进行裁剪，不影响结果展示。

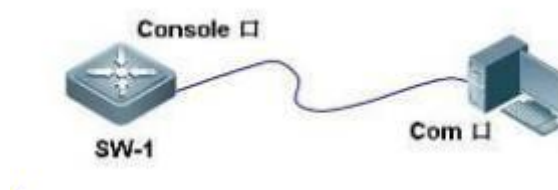
实验仪器：

交换机 1 台、主机 1 台

实验原理：

交换机工作在数据链路层的网络连接设备，基本功能是在多个计算机或网段之间交换数据。交换机内部的 CPU 会在每个端口成功连接时，通过将 MAC 地址和端口对应，形成一张 MAC 表。交换机在数据链路层进行数据转发时，根据数据包的 MAC 地址决定数据转发的端口，而不是简单的向所有的端口进行转发，因此，交换机可用于划分数据链路层广播，即冲突域；但它不能划分网络层广播，即广播域。具体来说，当交换机接收到一个数据帧时，它首先会记录数据帧的源端口和源 MAC 地址的映射，然后将数据帧的目的 MAC 地址与系统内部的动态查找表进行比较，并根据比较结果将数据包发送给相应的目的端口。若数据包的目的 MAC 层地址不在查找表中，则将包广播到每个端口。

基于 Cisco 互连网操作系统对交换机进行配置，以 CLI 的形式对交换机进行配置和管理。基本网络拓扑结构如下：



实验内容与步骤:

(一) 基本操作部分

(1) 查看设备选型并登录

通过实验室的计算机登陆实验平台，看到本小组的设备，其中有路由器、二层交换机、三层交换机。这里我选择 12T-S2928-1，即第十二组的第一台二层交换机。



(2) 熟悉交换机的配置模式，登陆进入所选择的交换机，然后开始配置

- a、通过 enable 进入特权模式
- b、通过 configure terminal 进入全局配置模式
- c、通过 interface Gigabitethernet 0/5 进入交换机 f0/5 的接口模式
- d、通过 exit 返回上一级操作模式
- e、通过 end 直接退回到特权模式

本环节主要测试了上述指令，熟悉了交换机的配置模式，部分中间截图如下：



(3) 命令行快捷指令

a、通过？ 查看当前模式下所有可执行的命令

```
Telnet 222.28.78.100

Ruijie>
Ruijie>?
Exec commands:
<1-99>      Session number to resume
disable     Turn off privileged commands
disconnect  Disconnect an existing network connection
enable      Turn on privileged commands
exit        Exit from the EXEC
help        Description of the interactive help system
lock        Lock the terminal
ping        Send echo messages
show        Show running system information
telnet      Open a telnet connection
traceroute  Trace route to destination
Ruijie>
```

b、通过 d? 查看当前模式下所有 d 开头的命令

```
Telnet 222.28.78.100

Ruijie>d?
disable disconnect
Ruijie>d
```

c、通过命令简写 conf ter 进入全局配置模式

```
Telnet 222.28.78.100

Ruijie>co?
% Unrecognized command.

Ruijie>?
Exec commands:
<1-99>      Session number to resume
disable     Turn off privileged commands
disconnect  Disconnect an existing network connection
enable      Turn on privileged commands
exit        Exit from the EXEC
help        Description of the interactive help system
lock        Lock the terminal
ping        Send echo messages
show        Show running system information
telnet      Open a telnet connection
traceroute  Trace route to destination
Ruijie>d?
disable disconnect
Ruijie>enable
Ruijie#
Ruijie#
Ruijie#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#
Ruijie(config)#
Ruijie(config)#
```

d、通过 conf+TAB 补全成 configure

```
Telnet 222.28.78.100

Ruijie>?
Exec commands:
<1-99>      Session number to resume
disable     Turn off privileged commands
disconnect  Disconnect an existing network connection
enable      Turn on privileged commands
exit        Exit from the EXEC
help        Description of the interactive help system
lock        Lock the terminal
ping        Send echo messages
show        Show running system information
telnet      Open a telnet connection
traceroute  Trace route to destination
Ruijie>d?
disable disconnect
Ruijie>enable
Ruijie#
Ruijie#
Ruijie#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#
Ruijie(config)#
Ruijie(config)#exit
Ruijie#*Nov 30 17:23:47: %SYS-5-CONFIG_I: Configured from console by console

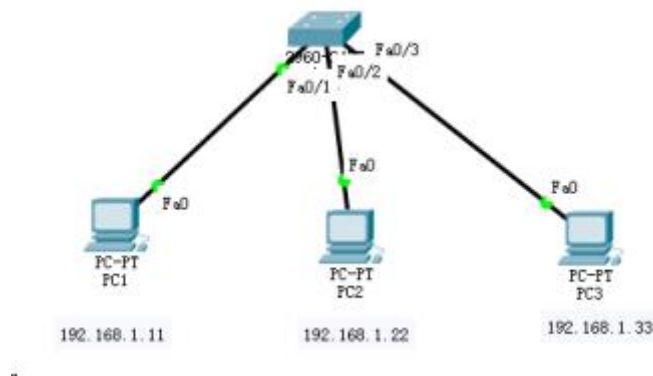
Ruijie#
Ruijie#conf
Ruijie#configure t
Ruijie#configure terminal
```

e、通过 `hostname+name` 将设备名称修改为 `name`（需要注意该操作在特权模式下进行），我这里修改为了 `SW_12_1`，表示第十二组的第一个二层交换机。

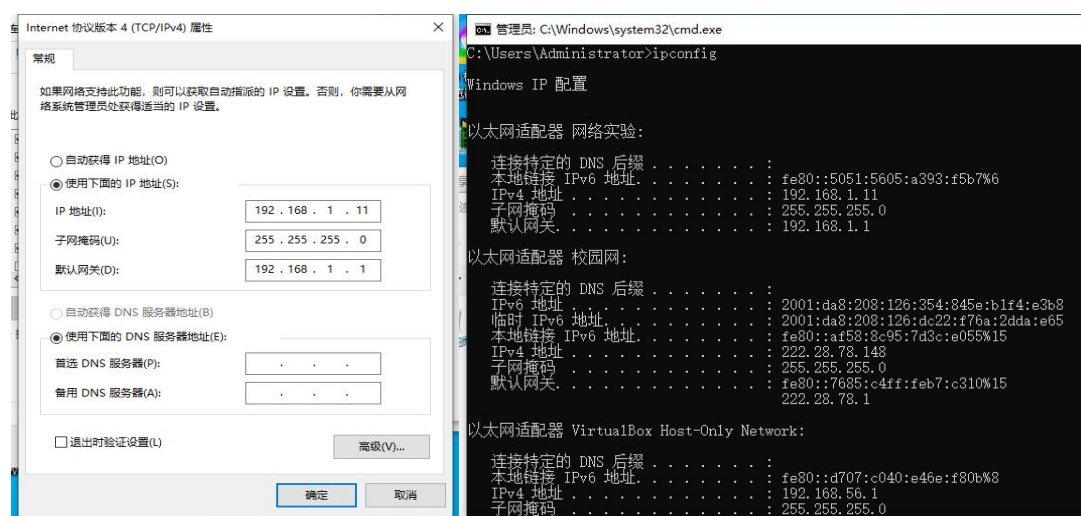
f、通过 show version 查看交换机版本信息

g、通过 `show mac-address-table` 查看当前交换机的 MAC 地址表，通过 `show running-config` 查看当前生效的配置

（二）组建局域网，查看 MAC 表的生成过程



(1) 配置“网络时延”网卡地址，采用静态地址，在网络-属性下进行设置，设置完毕后通过 cmd 命令 ipconfig 查看。

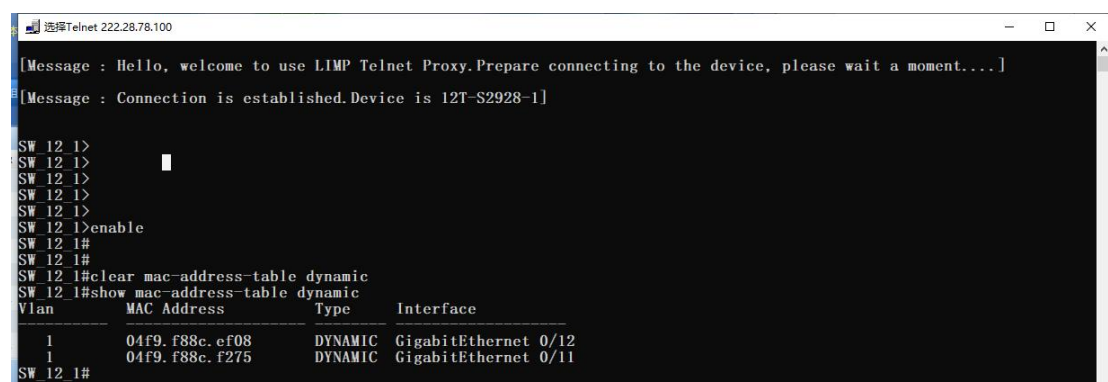


(2) 将两台 PC 与一台交换机相连

- 通过 clear mac-address-table 命令清除 MAC 表内容
- 通过 show mac-address-table 命令查看 MAC 表为空

(3) PC1 ping PC2

(4) 再次过 show mac-address-table 命令查看 MAC 表内容如下：

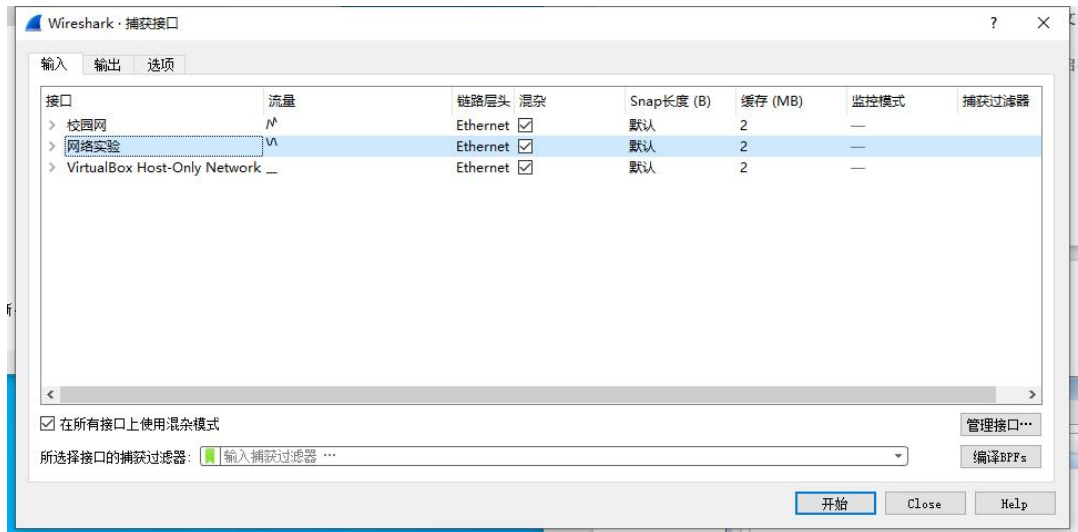


PC1 发出的报文，首先到达交换机，交换机从数据帧的源地址学习，完成 F0/1-MAC1 的

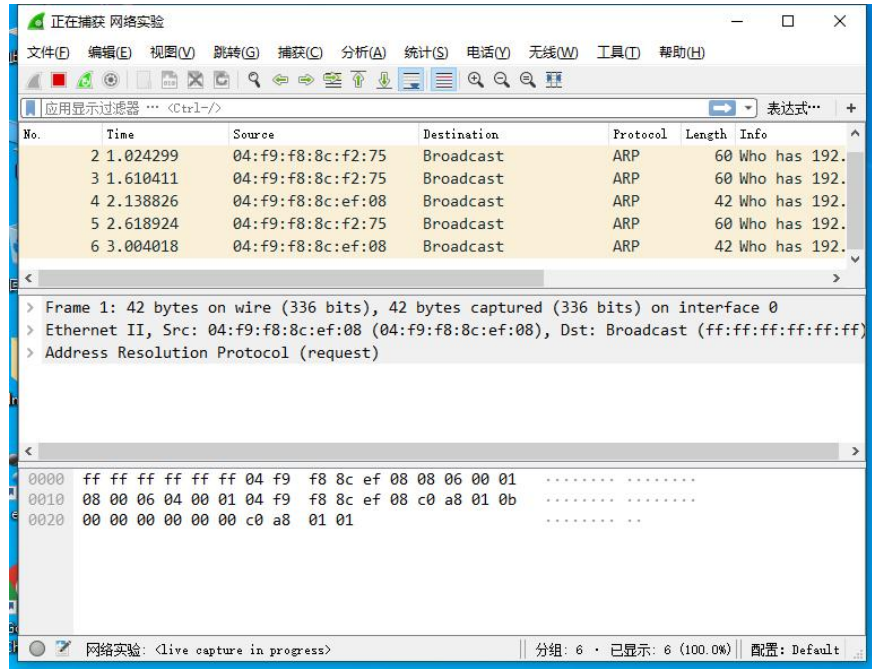
映射，PC2 回复的报文，到达交换机后，交换机完成 F0/2-MAC2 的映射。在报告后续的总结中会对其进行分析。

(5) Wireshark 抓包分析

在 wireshark 软件下，修改捕获网卡，选择“网络实验”，然后准备进行两次抓包。



a、第一次抓包时，直接启动抓包，在抓包期间执行 PC1 ping PC2 的操作，停止抓包得到如下的 ICMP 报文。



b、在命令行中执行 ARP -d 命令，开始抓包，在抓包期间执行 PC1 ping PC2 的操作，停止抓包得到如下的 ICMP 报文。

```
管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 10.0.19045.2604]
(c) Microsoft Corporation。保留所有权利。

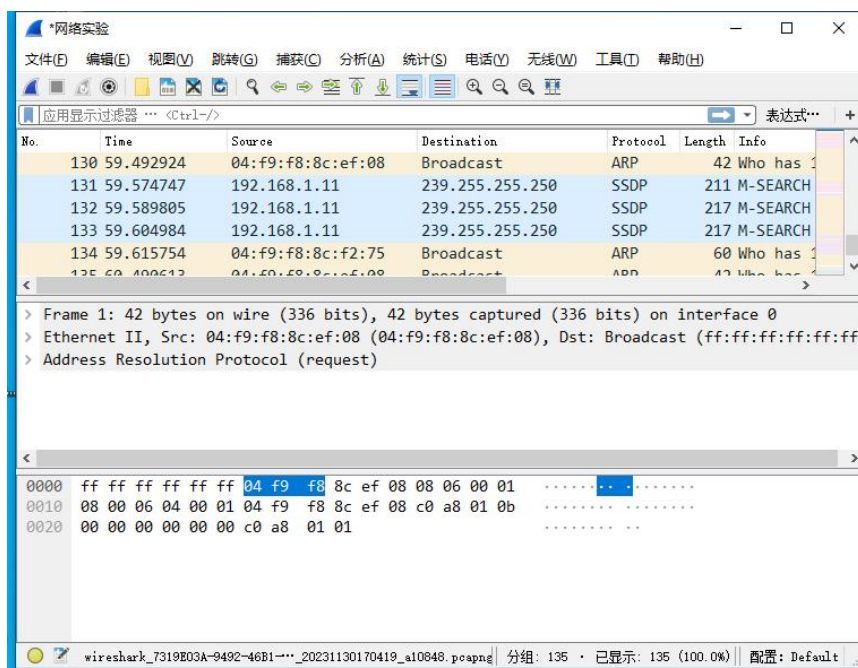
C:\Users\Administrator>ping 192.168.1.22

正在 Ping 192.168.1.22 具有 32 字节的数据:
来自 192.168.1.22 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.22 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.22 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.22 的回复: 字节=32 时间<1ms TTL=128

192.168.1.22 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\Administrator>arp -d

C:\Users\Administrator>
```



实验数据：

由于本次实验主要熟悉交换机的配置过程、常用命令以及 MAC 表的形成过程，因此本次实验中得到的实验数据主要是 wireshark 数据包。受限于报告篇幅，不能够全部展示数据包内容，因此只展示部分截图。在后续的实验数据处理环节，会对数据包进行简要分析。

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1701335066.271453000 seconds

[Time delta from previous captured frame: 0.000104000 seconds]

[Time delta from previous displayed frame: 0.000104000 seconds]

[Time since reference or first frame: 6.421635000 seconds]

Frame Number: 12

Frame Length: 74 bytes (592 bits)

Capture Length: 74 bytes (592 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:icmp:data]

[Coloring Rule Name: ICMP]

[Coloring Rule String: icmp | | icmpv6]

Ethernet II, Src: 04:f9:f8:8c:ef:08 (04:f9:f8:8c:ef:08), Dst: 04:f9:f8:8c:f2:75 (04:f9:f8:8c:f2:75)

Destination: 04:f9:f8:8c:f2:75 (04:f9:f8:8c:f2:75)

Source: 04:f9:f8:8c:ef:08 (04:f9:f8:8c:ef:08)

Address: 04:f9:f8:8c:ef:08 (04:f9:f8:8c:ef:08)

.... 0. = LG bit: Globally unique address (factory default)

.... 0 = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.1.11, Dst: 192.168.1.22

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 60

Identification: 0x3a0d (14861)

Flags: 0x0000

Fragment offset: 0

Time to live: 128

Protocol: ICMP (1)

Header checksum: 0x7d42 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.1.11

Destination: 192.168.1.22

Internet Control Message Protocol

Type: 0 (Echo (ping) reply)

Code: 0

Checksum: 0x554e [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence number (BE): 13 (0x000d)

Sequence number (LE): 3328 (0x0d00)

[Request frame: 11]

[Response time: 0.104 ms]

Data (32 bytes)

这个 Wireshark 捕获的数据包是一个 ICMP 的回显应答。

(1) Ethernet II 帧头:

源 MAC 地址: 04:f9:f8:8c:ef:08

目标 MAC 地址: 04:f9:f8:8c:f2:75

以太网类型: IPv4 (0x0800)

(2) IPv4 头部:

源 IP 地址: 192.168.1.11

目标 IP 地址: 192.168.1.22

协议类型: ICMP (1)

(3) ICMP 协议:

类型: 0 (回显应答)

代码: 0

校验和: 0x554e

标识符: 1 (0x0001)

序列号: 13 (0x000d)

数据: 32 字节

(4) 时间信息:

抵达时间: Nov 30, 2023 17:04:26.271453000 中国标准时间

捕获到达时间: 1701335066.271453000 秒

帧长度: 74 字节

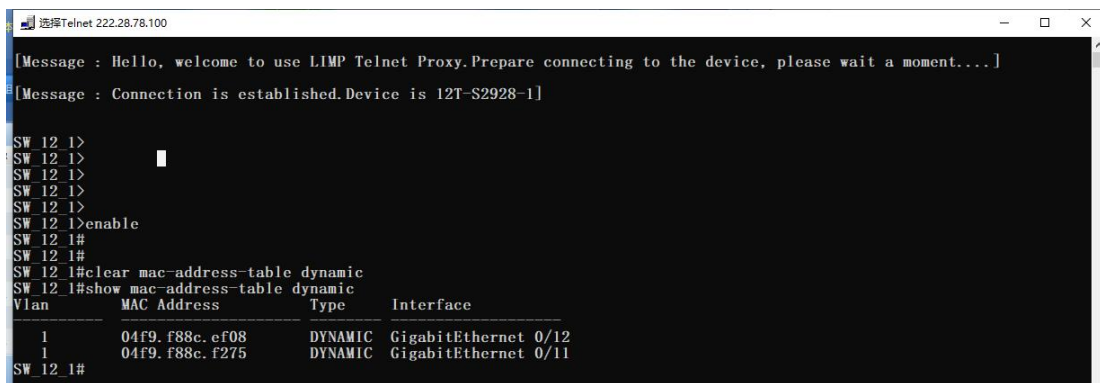
捕获长度: 74 字节

捕获接口: \Device\NPF_{7319E03A-9492-46B1-AFA7-B0A0EAAFB72B}

实验结果与分析:

在这个环节, 对实验指导书中的总结与分析进行回答。

(1) 给出交换机 MAC 地址表的截图, 交换机 MAC 地址表是如何建立的?



当交换机接收到一个帧时，它会查看帧中的源 MAC 地址，并记录该地址与接收到该帧的端口的对应关系。如果这个源 MAC 地址已经存在于 MAC 地址表中，交换机会更新该条目的时间戳。如果该源 MAC 地址不在表中，交换机会添加一个新的表项。

当交换机接收到一个帧时，它会查看目标 MAC 地址，并在 MAC 地址表中查找对应的条目。如果找到了，交换机就知道了要将帧发送到哪个端口。如果在表中找不到目标 MAC 地址的对应条目，交换机会将帧广播到所有端口（除了接收到该帧的端口之外），以确保目标设备能够收到。

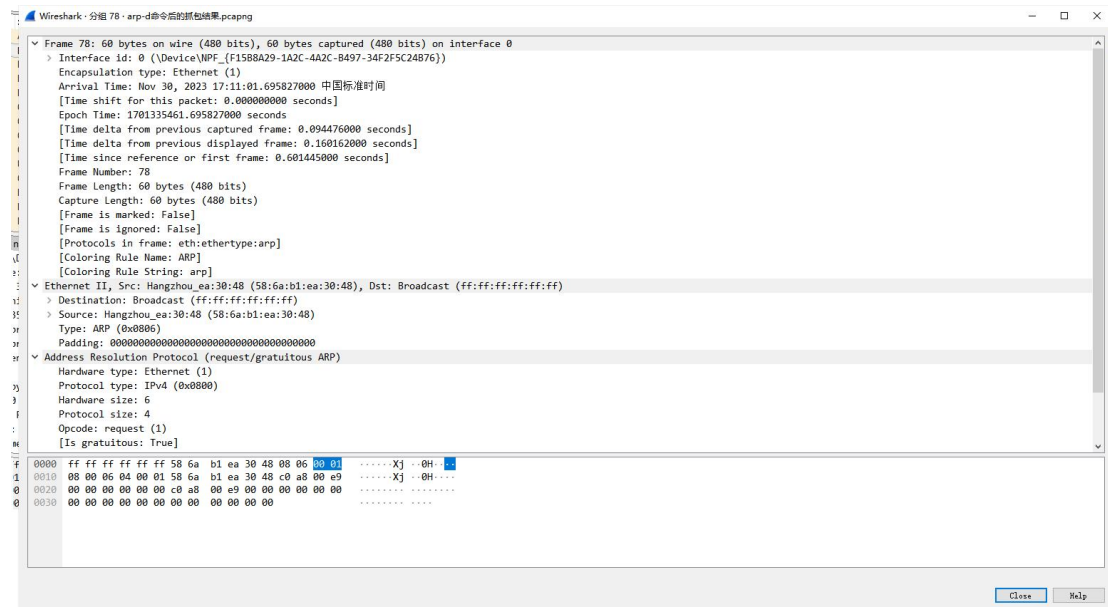
（2）使用 wireshark 软件抓包，抓取一组 ICMP 请求和应答的报文，完成下表。

使用之前的操作中抓取到的报文进行该问题的解答，具体分析过程在数据处理环节已经进行。

请求 报文 序号	源 MAC	目的 MAC	源 IP	目的 IP	Type	Code
11	04:f9:f8:8c:f2:75	04:f9:f8:8c:ef:08	192.168.1.22	192.168.1.11	IPv4 (0x0800)	Echo (ping) request (Type: 8, Code: 0)
回答 报文 序号	源 MAC	目的 MAC	源 IP	目的 IP	Type	Code
12	04:f9:f8:8c:ef:08	04:f9:f8:8c:f2:75	192.168.1.11	192.168.1.22	IPv4 (0x0800)	Echo (ping) reply (Type: 0, Code: 0)

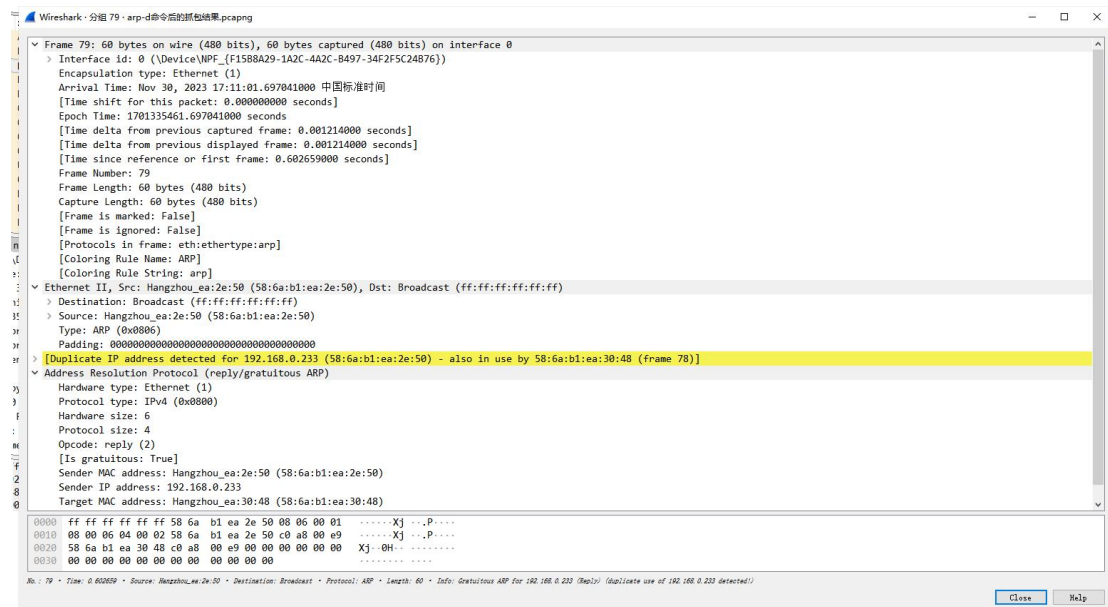
(3) 对通过 arp -d 命令后的 ping 命令住区的 ARP 数据包进行分析。

a、展开第一条 ARP 请求报文，截图显示链路层和 ARP 协议详细信息



目的 MAC 是 ff:ff:ff:ff:ff:ff，说明 arp 请求是广播帧；源 MAC 地址是 Hangzhou_ea:30:48 (58:6a:b1:ea:30:48)，说明是设备 Hangzhou_ea:30:48 (58:6a:b1:ea:30:48) 发出的 ARP 请求。ARP 请求帧询问 IP 地址为 192.168.0.233 对应的 MAC 地址。

b、展开第二条 ARP 应答报文，截图显示链路层和 ARP 协议详细信息



源 MAC 地址是 Hangzhou_ea:2e:50 (58:6a:b1:ea:2e:50)，说明是设备 Hangzhou_ea:2e:50 (58:6a:b1:ea:2e:50) 发出的 arp 应答。目的地址是 ff:ff:ff:ff:ff:ff 说明 arp 应答是广播 帧，arp 请求的 IP 地址为 192.168.0.233 所对应的 MAC 地址为 Hangzhou_ea:30:48 (58:6a:b1:ea:30:48)。

北京科技大学实验报告

学院：计通学院	专业：信息安全	班级：信安 211
姓名：李晓坤	学号：U202141863	实验日期：2023 年 11 月 30 日

实验名称：

实验二：广播风暴与生成树

实验目的：

- (1) 了解广播风暴产生的原因
- (2) 掌握交换机生成树的配置方法
- (3) 理解根交换机和根端口选举规则

实验仪器：

交换机 1 台
主机 2 台

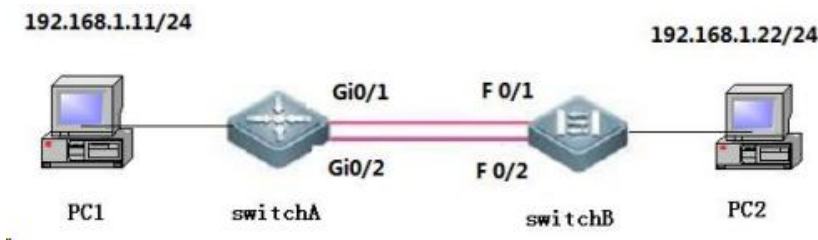
实验原理：

为了提高网络的可靠性和健壮性，通常设置冗余链路，即备份链路。当主链路出现故障时，备份链路自动启动，避免网络发生单点故障。但这也带来一个问题，就是在二层网络中产生了环路，数据帧会在网络中循环，占用带宽资源，从而形成广播风暴，最终导致链路中断。

生成树协议在网络中提供冗余链路并解决交换网络中的环路问题。常使用 SPA 生成树算法，在网络中生成没有环路的树形网络。该算法将交换网络冗余的备份链路逻辑上断开，当主链路出现故障时，自动切换到备份链路上，保证数据正常转发。

生成树协议常见的版本有 STP、RSTP、MSTP。其中，STP 收敛时间长，RSTP 在 STP 上增加了替换端口和备份端口，分别作为根端口和指定端口的冗余端口，从而实现快速收敛。

本实验用到的网络拓扑结构如下：



实验内容与步骤:

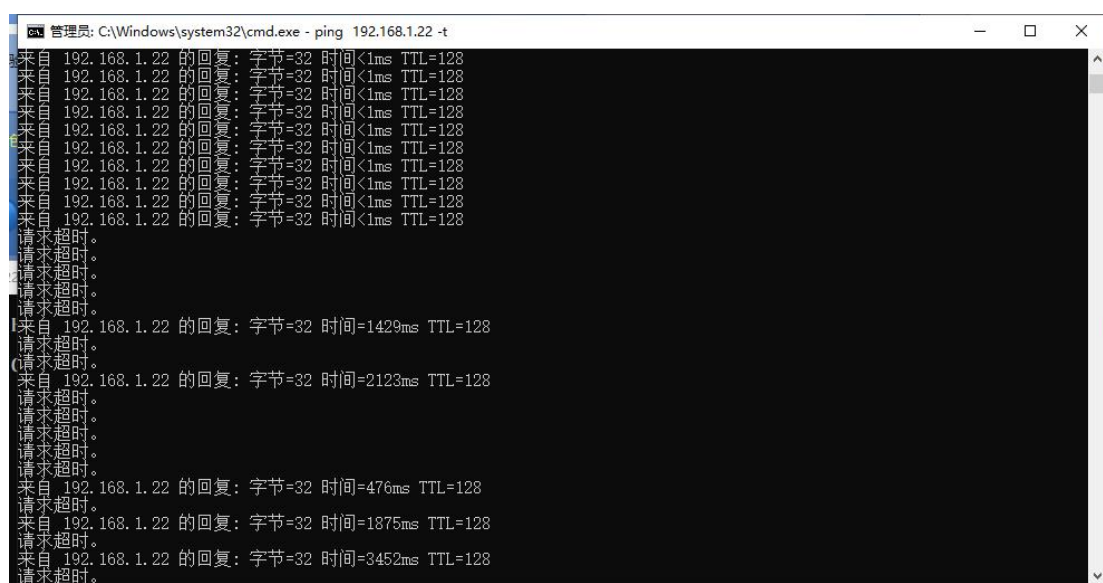
(1) 配置两台交换机的主机名、管理 IP 地址和 Trunk

该环节主要通过特权模式下的 `hostname`、`interface` 等命令进行设置。主要是将两台交换机分别重命名为 L2-SW、L3-SW；ip 地址设置为 192.168.1.2、192.168.1.1；子网掩码设置为 255.255.255.0；端口模式设置为 Trunk。

(2) 接线，交换机之间将 G0/1- F0/1 相连，二层交换机将 G0/5 与 PC1 机相连，三层交换机将 F0/5 与 PC2 机相连；G0/2- F0/2 稍后再连接。具体的连接方式与前文的网络拓扑结构相同。

(3) 不启用生成树协议，PC1 ping PC2，能够连通。

(4) 此时，启用备份链路，一段时间后观察到请求超时，产生广播风暴现象。



```
管理员: C:\Windows\system32\cmd.exe - ping 192.168.1.22 -t
来自 192.168.1.22 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.22 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.22 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.22 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.22 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.22 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.22 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.22 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.22 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.22 的回复: 字节=32 时间<1ms TTL=128
请求超时。
请求超时。
请求超时。
请求超时。
请求超时。
来自 192.168.1.22 的回复: 字节=32 时间=1429ms TTL=128
请求超时。
请求超时。
来自 192.168.1.22 的回复: 字节=32 时间=2123ms TTL=128
请求超时。
请求超时。
请求超时。
请求超时。
请求超时。
来自 192.168.1.22 的回复: 字节=32 时间=476ms TTL=128
请求超时。
来自 192.168.1.22 的回复: 字节=32 时间=1875ms TTL=128
请求超时。
来自 192.168.1.22 的回复: 字节=32 时间=3452ms TTL=128
请求超时。
```

(5) 接下来通过 `spanning-tree` 和 `spanning-tree mode rstp` 命令启用生成树协议并修改生成树协议类型为 RSTP。



```
Telnet 222.28.78.100
L2-SW(config)#spanning-tree mode rstp
L2-SW(config)#*Nov 30 18:59:38: %SPANTREE-5-ROOTCHANGE: Root Changed: New Root Port is GigabitEthernet 0/1. New Root Mac Address is 5869.6c6e.1b23.
*Nov 30 18:59:38: %SPANTREE-5-TOPOTRAP: Topology Change Trap.
*Nov 30 18:59:40: %SPANTREE-6-RCVDTCPDU: Received tc bpu on port GigabitEthernet 0/2 on MST0
*Nov 30 18:59:42: %SPANTREE-6-RCVDTCPDU: Received tc bpu on port GigabitEthernet 0/2 on MST0
```

(6) 一段时间后观察到链路由中断变为连通。

链路开销值低，累加值 COST 最低得路径是根路径。L3-SW 上 Fa0/1 和 Fa0/2 都与根桥相连，路径开销也相同，端口号 Fa0/1 比 Fa0/2 小，Fa0/1 被选为根端口。所有根端口都为指定端口，参与数据的转发，Fa0/2 端口为非指定端口，将被阻塞，无法转发数据。

(8) 指定三层交换机为根网桥，指定二层交换机的 Gi0/2 端口为根端口。

这一操作主要通过命令 `spanning-tree priority xxxx` 进行设置优先级，设置完毕后通过命令 `show spanning-tree` 进行查看。

```
Telnet 222.28.78.100
[Message : Hello, welcome to use LIMP Telnet Proxy.Prepare connecting to the device, please wait a moment....]
[Message : Connection is established.Device is 12T-S2928-1]
L2-SW(config)#
L2-SW(config)#
L2-SW(config)#Show spanning-tree interface Gi 0/2
PortAdminPortFast : Disabled
PortOperPortFast : Disabled
PortAdminAutoEdge : Enabled
PortOperAutoEdge : Disabled
PortAdminLinkType : auto
PortOperLinkType : point-to-point
PortBPDUGuard : Disabled
PortBPDUFilter : Disabled
PortGuardmode : None
PortState : forwarding
PortPriority : 128
PortDesignatedRoot : 4096.5869.6c6e.1b23
PortDesignatedCost : 0
PortDesignatedBridge : 4096.5869.6c6e.1b23
PortDesignatedPortPriority : 96
PortDesignatedPort : 2
PortForwardTransitions : 3
PortAdminPathCost : 200000
PortOperPathCost : 200000
Inconsistent states : normal
PortRole : rootPort
L2-SW(config)#
```

```
Telnet 222.28.78.100
L3-SW(config-if-FastEthernet 0/2)#spanning-tree port-priority 96
L3-SW(config-if-FastEthernet 0/2)#show sp
L3-SW(config-if-FastEthernet 0/2)#show spanning-tree int
L3-SW(config-if-FastEthernet 0/2)#show spanning-tree interface *Nov 30 18:15:55: %NFPP_ARP
=192.168.1.44,MAC=N/A,port=Fa0/2,VLAN=1> was detected. (2023-11-30 18:5:28)
% Incomplete command.
L3-SW(config-if-FastEthernet 0/2)#show spanning-tree interface F 0/2
PortAdminPortFast : Disabled
PortOperPortFast : Disabled
PortAdminAutoEdge : Enabled
PortOperAutoEdge : Disabled
PortAdminLinkType : auto
PortOperLinkType : point-to-point
PortBPDUGuard : Disabled
PortBPDUFilter : Disabled
PortGuardmode : None
PortState : forwarding
PortPriority : 96
PortDesignatedRoot : 4096.5869.6c6e.1b23
PortDesignatedCost : 0
PortDesignatedBridge : 4096.5869.6c6e.1b23
PortDesignatedPortPriority : 96
PortDesignatedPort : 2
PortForwardTransitions : 2
PortAdminPathCost : 200000
PortOperPathCost : 200000
Inconsistent states : normal
PortRole : designatedPort
L3-SW(config-if-FastEthernet 0/2)#
```

(9) 验证配置，在三层交换机 L3-SW 上长时间的 ping 二层交换机 L2-SW，其间断开 L2-SW 上的根端口 Gi0/2，这时观察替换端口能够在多长时间内成为转发端口。

该操作主要通过例如 `ping 192.168.1.2 ntimes 1000` 进行。

[illegible][illegible]

从中可以看到替换端口变成转发端口的过程中，丢失了 7 个 ping 包，中断时间小于 60ms。

当网络主链路发生故障时，网络拓扑结构会发生变化，处于阻塞状态的端口，通过 **BPD** 报文侦听了解到这一变化，端口状态立刻从阻塞转变到学习状态，完成 **MAC** 地址表的建立后，端口转变为转发状态。一个端口从禁用到转发大约需要 **50** 秒，用于生成树协议了解整个网络的拓扑结构。

实验数据：

该实验为验证性实验，已将中间过程以图片的形式进行记录，具体见前述的报告内容。

实验数据处理：

由于实验数据均为图片，无需处理，在实验过程中已将其进行分析。

实验结果与分析：

该环节解释实验指导书中的思考问题部分。

（1）广播风暴产生的原因是什么？它有什么危害？

广播风暴是网络中发生广播消息传播过度，导致网络中的设备被不必要的广播消息淹没的现象。产生广播风暴的主要原因包括：

- a、网络环路：当网络中存在环路时，广播消息可能在网络中无限循环，导致广播风暴。
- b、网络设备故障：某个网络设备故障可能导致它不正确地转发广播消息，使得广播消息在网络中无限传播。
- c、网络设计不当：不良的网络设计或配置错误可能导致广播消息无法正确处理，从而引发广播风暴。

广播风暴可能导致以下危害：

- a、网络拥塞：大量不必要的广播消息会占用网络带宽，导致网络拥塞，影响正常的数据传输。
- b、性能下降：广播风暴会导致网络设备过度负荷，使其性能下降，影响正常的网络通信。
- c、服务不可用：在极端情况下，广播风暴可能导致网络服务不可用，使网络中的设备无法正常通信。
- d、网络不稳定：广播风暴可能导致网络不稳定，影响用户正常的网络体验。

（2）根交换机也称为根桥，它的选举规则是什么？

- a、Bridge ID 比较：每个交换机都有一个唯一的 Bridge ID，由优先级和 MAC 地址组成。生成树协议中，Bridge ID 越小，优先级越高。交换机会比较所有相邻交换机的 Bridge ID，选择具有最小 Bridge ID 的交换机作为根交换机。
- b、优先级比较：如果有多个交换机具有相同的最小 Bridge ID，那么将比较它们的优先级。交换机的优先级是一个 16 位的值，默认值为 32768。优先级越低，优先级越高。
- c、MAC 地址比较：如果两个交换机具有相同的 Bridge ID 和优先级，那么将比较它们的 MAC 地址。MAC 地址越小，优先级越高。

（3）非根交换机，怎样选举根端口？

- a、根路径成本比较：非根交换机的每个端口都会计算到根交换机的路径成本。路径成本是从该端口到根交换机的总带宽代价。端口选择具有最低路径成本的路径作为根端口。
- b、根路径成本相同的情况下，比较桥优先级：如果存在多个端口具有相同的最低路径成本，那么将比较相邻交换机的桥优先级。桥优先级越低的交换机将优先选择为根端口。
- c、桥优先级相同的情况下，比较本地端口优先级：如果相邻交换机的桥优先级相同，那么将比较本地端口的优先级。本地端口优先级越低的端口将被选择为根端口。
- d、端口号比较：如果以上都相同，将比较端口号。端口号越小的端口将被选择为根端口。