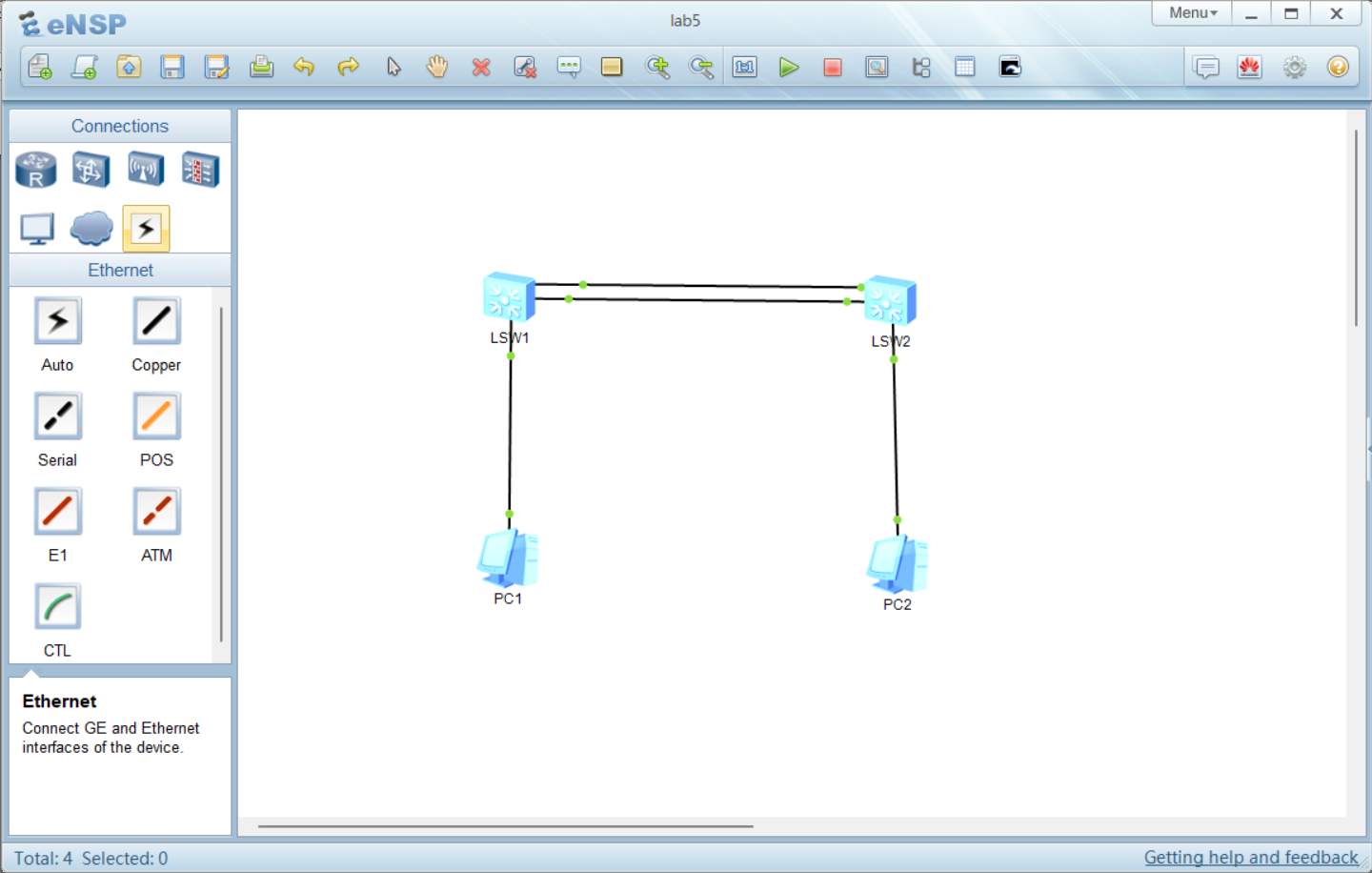
**实验报告**

**实验名称：实验3.3.1：广播风暴与MAC地址表震荡分析**

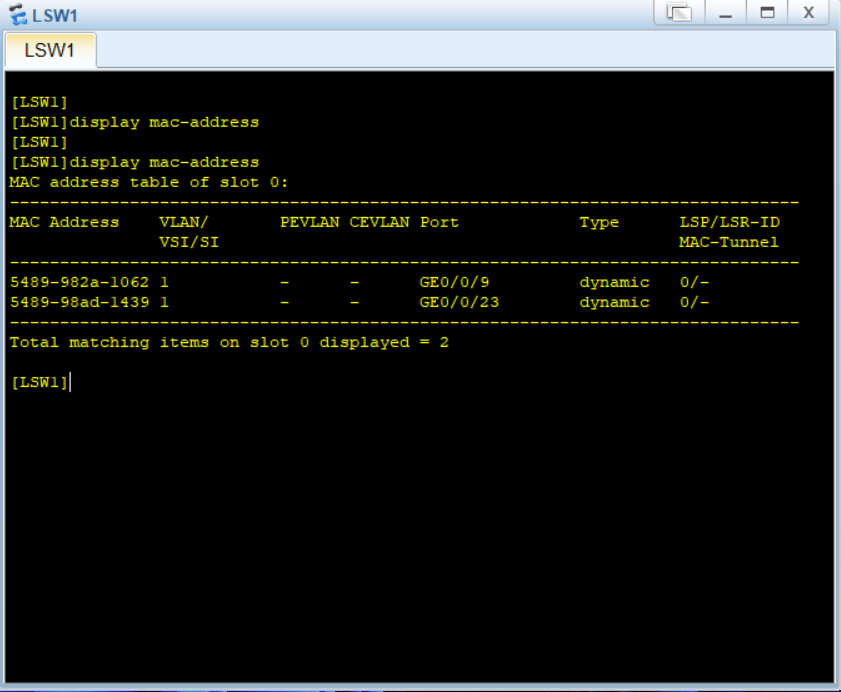
学院： 计算机学院 班级： 07112005 学号： 1120202695 姓名： 穆新宇

**步骤4：开启和查看交换机STP状态**

1. 请将创建的网络拓扑的截图粘贴到实验报告中。



1. 请将交换机LSW1的MAC地址表内容的截图粘贴到实验报告中。

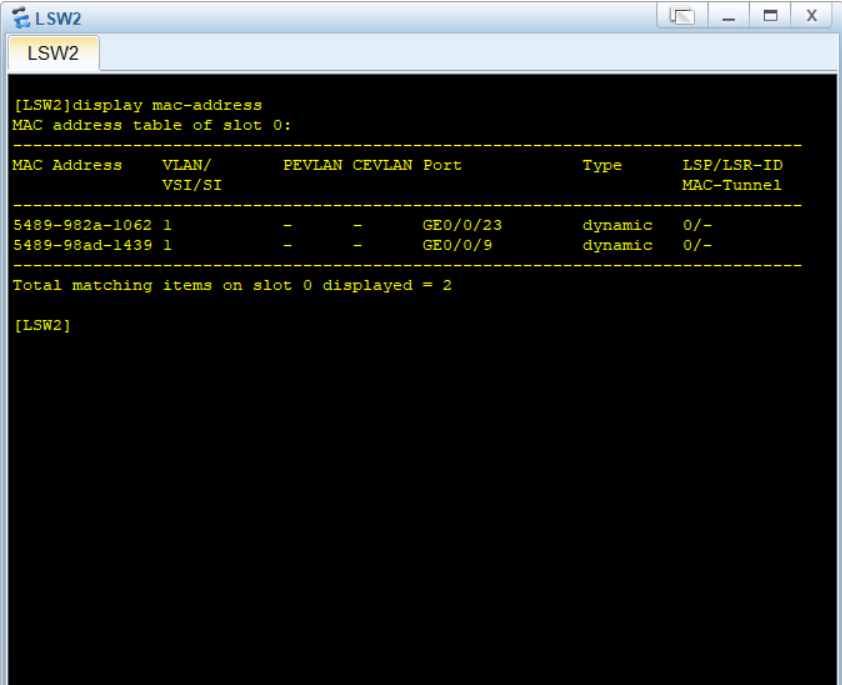


1. 请将交换机LSW1及其端口的STP状态和生成树状态信息填入表3-29。

表3-29 开启交换机LSW1的STP后各端口的STP角色和状态

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 交换机BID | 32768.4c1f-cc60-5c87 | | 网桥角色 | | ▪根网桥 🞎指定网桥 | |
| 端口 | 端口角色 | 端口状态 | | 端口ID | | 路径代价 | |
| GE 0/0/9 | Designated Port | FORWADING | | 128.9 | | Config=auto / Active=20000 | |
| GE 0/0/23 | Designated Port | FORWADING | | 128.23 | | Config=auto / Active=20000 | |
| GE 0/0/24 | Designated Port | FORWADING | | 128.24 | | Config=auto / Active=20000 | |

1. 请将交换机LSW2的MAC地址表内容的截图粘贴到实验报告中。



1. 请将交换机LSW2及其端口的STP状态和生成树状态信息填入表3-30。

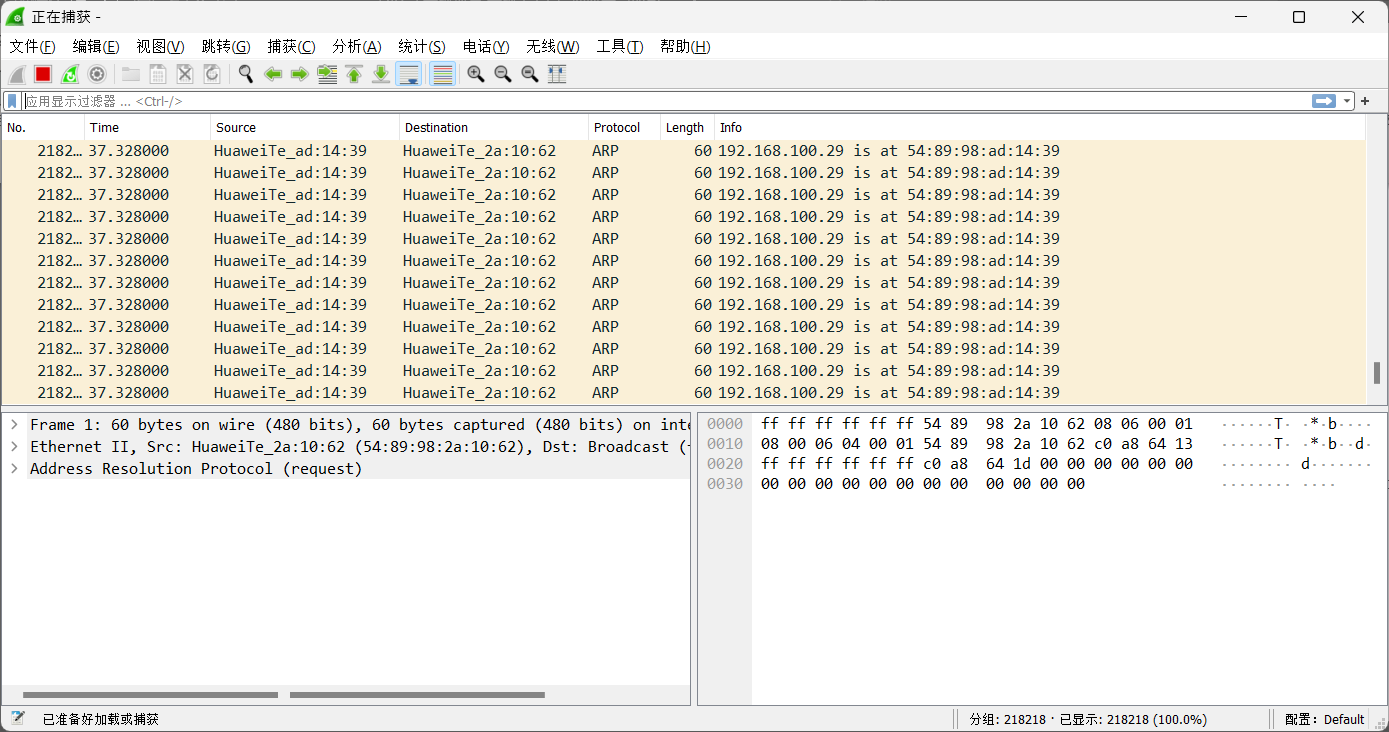
表3-30 开启交换机LSW2的STP后各端口的STP角色和状态

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 交换机BID | 32768.4c1f-ccb4-14e5 | | 网桥角色 | | ▪根网桥 🞎指定网桥 | |
| 端口 | 端口角色 | 端口状态 | | 端口ID | | 路径代价 | |
| GE 0/0/9 | Designated Port | FORWARDING | | 128.9 | | Config=auto / Active=20000 | |
| GE 0/0/23 | Root Port | FORWARDING | | 128.23 | | Config=auto / Active=20000 | |
| GE 0/0/24 | Designated Port | DISCARDING | | 128.24 | | Config=auto / Active=20000 | |

**步骤6：广播风暴分析**

1. Wireshark是否抓取到了广播风暴？广播风暴的现象是什么？请将Wireshark中广播风暴通信的截图粘贴到实验报告中，并标记出这些广播风暴通信。

Wireshark抓取到了广播风暴. 现象是交换机不停转发数据帧.



1. 查看交换机LSW1和LSW2命令窗口中输出的日志信息。2台交换机的CPU的利用率分别为多少？

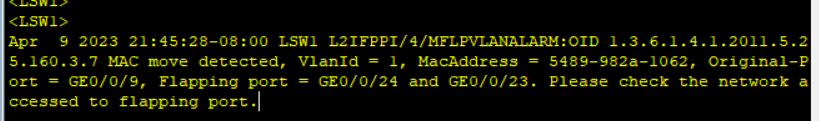
ENSP(10%) + OS(90%) = 100%

**步骤7：交换机MAC地址表震荡分析**

1. 在交换机LSW1控制台窗口中输出的日志信息中，哪个或哪些MAC地址对应的交换机端口有变化？有何变化？请将该命令结果的截图粘贴实验报告中，并标记出MAC地址对应的端口的变化情况。

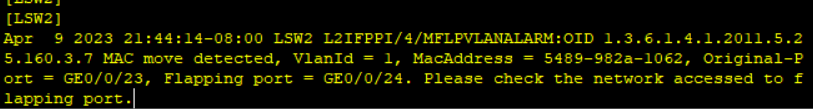
5489-982a-1062对应的交换机端口有变化, 初始端口: 0/0/9, Flapping Port: 0/0/23

和0/0/24



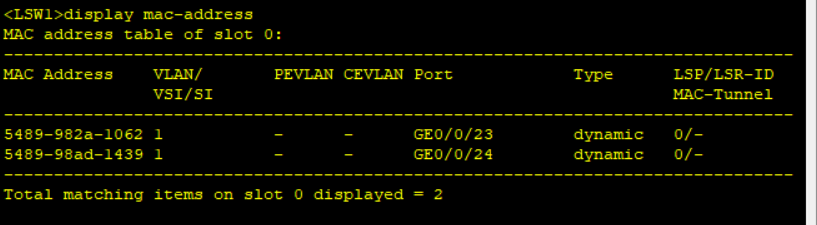
1. 在交换机LSW2控制台窗口中输出的日志信息中，哪个或哪些MAC地址对应的交换机端口有变化？有何变化？请将该命令结果的截图粘贴实验报告中，并标记出MAC地址对应的端口的变化情况

5489-982a-1062对应的交换机端口有变化, 初始端口: 0/0/23, Flapping Port: 0/0/24

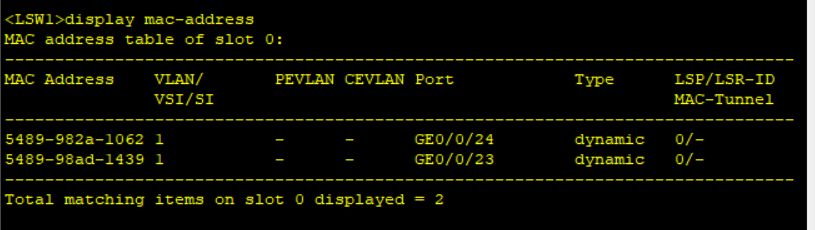


1. 请将禁用端口STP后交换机LSW1在时刻1和时刻2的MAC地址表内容的截图粘贴到实验报告中。

时刻1:



时刻2:



1. 在不同时刻，交换机LSW1的端口GE 0/0/9、GE 0/0/23和GE 0/0/24学习到MAC地址分别是什么？将结果填入表3-31中。

表3-31 禁用端口STP后LSW1端口学习到的MAC地址

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 端口 | 时刻1 | | 时刻2 | |
| 时间  (年-月-日 时:分:秒) | 学习到的  MAC地址 | 时间  (年-月-日 时:分:秒) | 学习到的  MAC地址 |
| GE 0/0/9 | 2023-4-9 21:50:05 | - | 2023-4-9 21:50:10 | - |
| GE 0/0/23 | 2023-4-9 21:50:10 | 5489-982a-1062 | 2023-4-9 21:50:10 | 5489-98ad-1439 |
| GE 0/0/24 | 2023-4-9 21:50:10 | 5489-98ad-1439 | 2023-4-9 21:50:10 | 5489-982a-1062 |

1. 如何停止或消除当前的广播风暴？

停止所有设备

1. 为减少或阻止此类因配置错误所导致的环路，有什么技术解决方案？
   1. Spanning Tree Protocol（STP）：STP是一种网络协议，可以检测和防止网络中的环路，从而避免广播风暴。STP将网络中的交换机组织成一个树形拓扑结构，从而防止环路的发生。如果发现环路，STP将自动禁用其中一个端口，以防止广播风暴的发生。
   2. Rapid Spanning Tree Protocol（RSTP）：RSTP是一种改进版的STP，可以更快地检测和恢复网络中的故障。与STP不同，RSTP支持快速端口转发和端口翻转，这可以大大减少广播风暴的影响。
   3. PortFast：PortFast是Cisco推出的一种技术，可以将交换机端口快速转换为正常操作模式，从而避免因端口转换时间过长而引起的广播风暴。PortFast可以将端口快速转换为正常操作模式，并立即激活端口。
   4. BPDU Guard：BPDU Guard是一种技术，可以防止非授权交换机进入网络，从而避免由于交换机配置错误而引起的广播风暴。BPDU Guard可以检测到非授权的交换机，并将其端口关闭，以防止广播风暴的发生。