

教学班：周三

序号： 55

浙江大学

本科实验总结

课程名称： 无线网络应用

姓 名： 颜晗

学院（系）： 竺可桢学院

专 业： 计算机科学与技术

学 号： 3200105515

指导教师： 张昱，史笑兴，李惠忠，金心宇

2021 年 6 月 26 日

实验总结的实验项目清单

第一部分 基本实验总结

- 1、实验四：无线网络安全性配置应用之 DMZ 及过滤实验
- 2、实验五：无线 AP 的组网之 Bridge 桥接模式组网实验

第二部分 补选实验总结

- 1、补充选做实验 1：基于无线路由器的 VPN 共享上网实验

无线网络安全性配置应用之 DMZ 及过滤实验

一、实验原理与内容

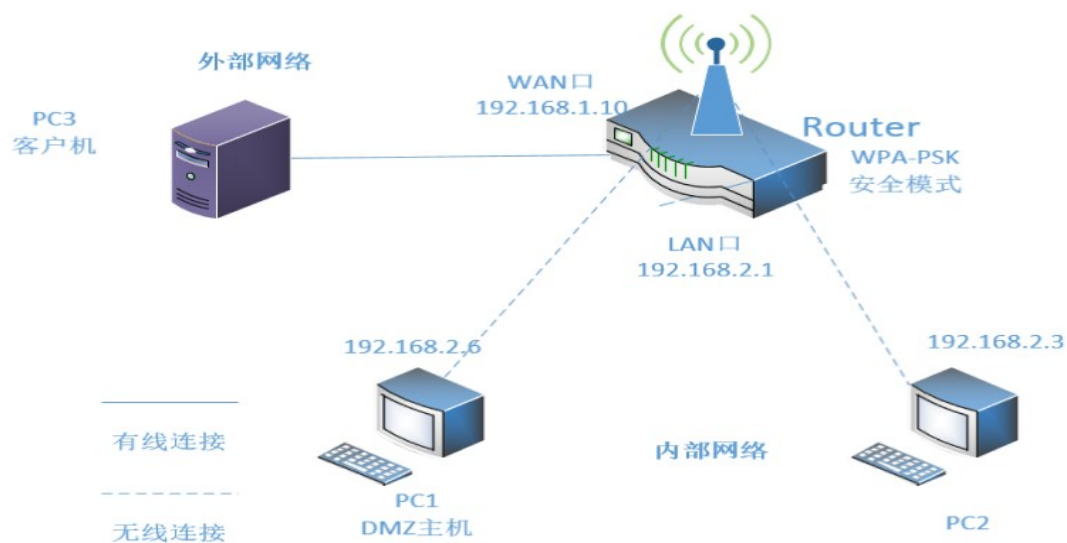
防火墙过滤功能的存在保护了内部计算机不受外部攻击的影响，但是也一定程度上限制了内部主机与外部主机的合法通信。而在某些特殊情况下，我们需要将某些主机“完全暴露”给广域网，借此实现双向无限制通信。

该需求可通过设置 DMZ 主机来实现。非军事区 DMZ 代表内外用户都可以访问的区域，外部主机可访问指定 DMZ 主机的所有端口，防火墙设置将对 DMZ 主机不起作用，其安全性高于外部网络，低于内部网络。但是向 DMZ 添加客户机会给本地网络增添不稳定因素，建议慎用。

另外，利用无线路由器的过滤设置，可以防止蹭网，使网络更加安全。

实验将 PC1 设置为 DMZ 主机，并设置好 Web 服务，使处于外部网络的 PC3 可以访问 PC1 的 Web 服务；将 PC2 通过路由器设置过滤，使 PC2 无法连接并访问外部网络，即无法 ping 通 PC3，而 PC1 与 PC3 仍可正常通信。

二、实验拓扑图



三、实验过程与结果

首先进行路由器的设置，利用有线连接接入 LAN 口，进入 Web 配置界面，设置好名称，密码，信道等。接下来就是较为重要的 LAN 口设置与上网设置。本实验中 LAN 口地址应设置 192.168.2.1，与往常的 192.168.1.1 区分开来，LAN 口设置后应重启路由器，与此同时要将计算机的 IP 地址设置为 192.168.2.*才可以再进入配置页面，如下图所示。

● 使用下面的 IP 地址(S):	
IP 地址(I):	192 . 168 . 2 . 6
子网掩码(U):	255 . 255 . 255 . 0
默认网关(W):	192 . 168 . 2 . 1

然后是上网设置，本实验中设置 WAN 口固定 IP 地址为 192.168.1.10，即将 1.*设置为外网，2.*设置为内网，具体设置如下图。

WAN口连接类型	固定IP地址
IP地址	192.168.1.10
子网掩码	255.255.255.0
网关	192.168.1.10
首选DNS服务器	10.10.0.21
备用DNS服务器	10.10.2.21 (可选)
<button>保存</button>	

然后进入应用管理中的已安装应用，可看见 DMZ 主机选项，打开功能，并添加 PC1 的 IP 地址将其设置为 DMZ 主机。

在所有设置完成后，我们会发现从 PC1、PC2 上 ping PC3 是可以 ping 通的，PC3 也可访问 PC1 上的 Web 服务，但是由于未将 PC2 设置未 DMZ 主机，PC3 是无法访问 PC2 上的 FTP 服务的，符合实验预期。

再从路由器配置界面的设备管理将 PC2 禁用，我们会发现 PC2 已无法 ping 通 PC3,而再将其启用，又可以 ping 通 PC3,可见路由器的过滤作用确实有一定作用，可以防止不明计算机随意接入网络。

```
管理员: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ping 192.168.1.5

正在 Ping 192.168.1.5 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

192.168.1.5 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),

C:\Users\Administrator>ping 192.168.1.5

正在 Ping 192.168.1.5 具有 32 字节的数据:
来自 192.168.1.5 的回复: 字节=32 时间=22ms TTL=63
来自 192.168.1.5 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.1.5 的回复: 字节=32 时间=8ms TTL=63
来自 192.168.1.5 的回复: 字节=32 时间=1ms TTL=63

192.168.1.5 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 = 1ms, 最长 = 22ms, 平均 = 8ms

C:\Users\Administrator>
```

四、心得体会

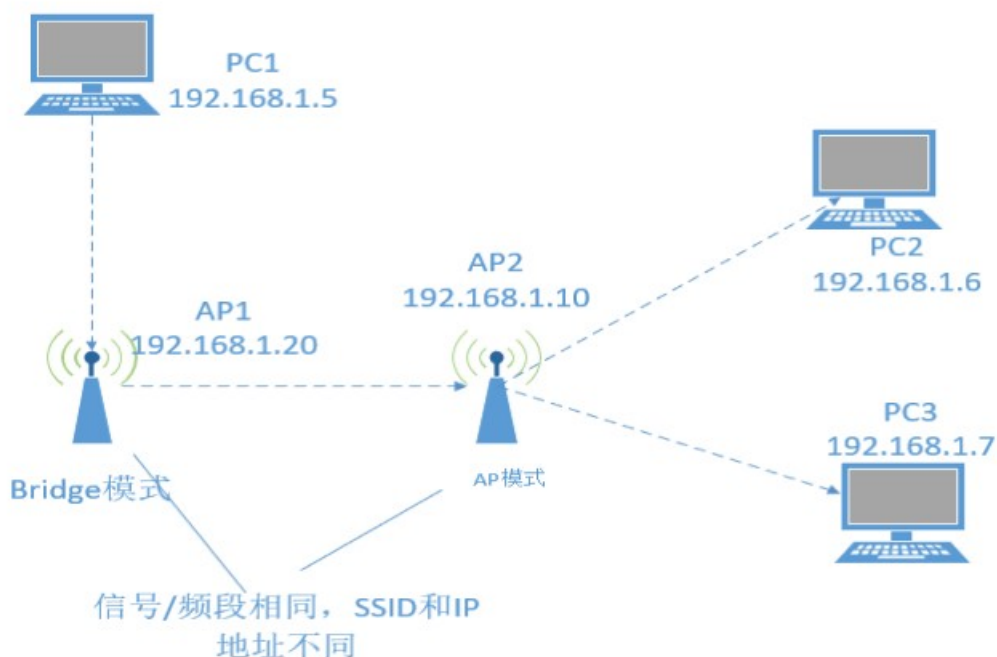
无线 AP 的组网之 Bridge 桥接模式组网实验

一、实验原理与内容

无线 AP 具有多种工作模式，除默认的 AP 模式外，还有一种 Bridge 模式，可以与另一台无线 AP 进行连接，设置为 Bridge 模式的 AP 可以与设置为 AP 模式的无线 AP 配合使用，组成点对多点网络。即可以将两个不同的 WLAN 连接起来，使不同网络的主机间可以相互通信。需要注意的是，两网络所处的网段应当相同，即 AP 和主机的 IP 地址应都为 192.168.*，且 AP 的信道和安全模式应该相同，而两个 AP 依旧管理两个网络，它们的 SSID 应不同。

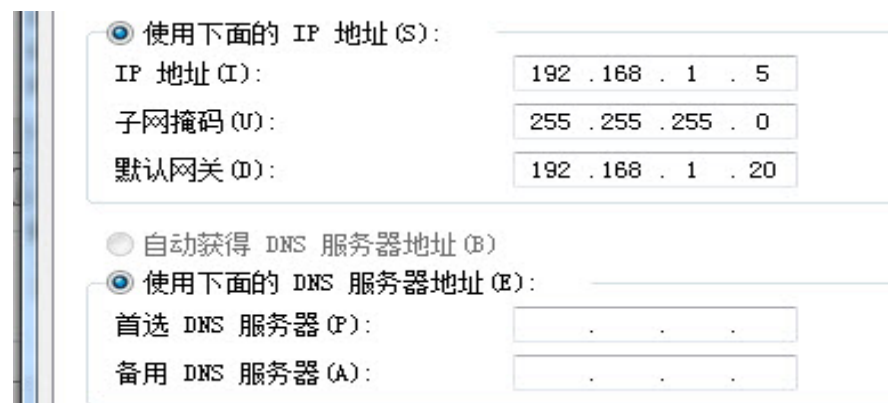
本实验将使 PC1 和 AP1 处于一个网络并将 AP1 设为 Bridge 模式，使 PC2、PC3 和 AP2 处于另一个网络并将 AP2 设置为 AP 模式，组成点对多点网络，实现 PC1、PC2、PC3 间互相 ping 通。

二、实验拓扑图



三、实验过程与结果

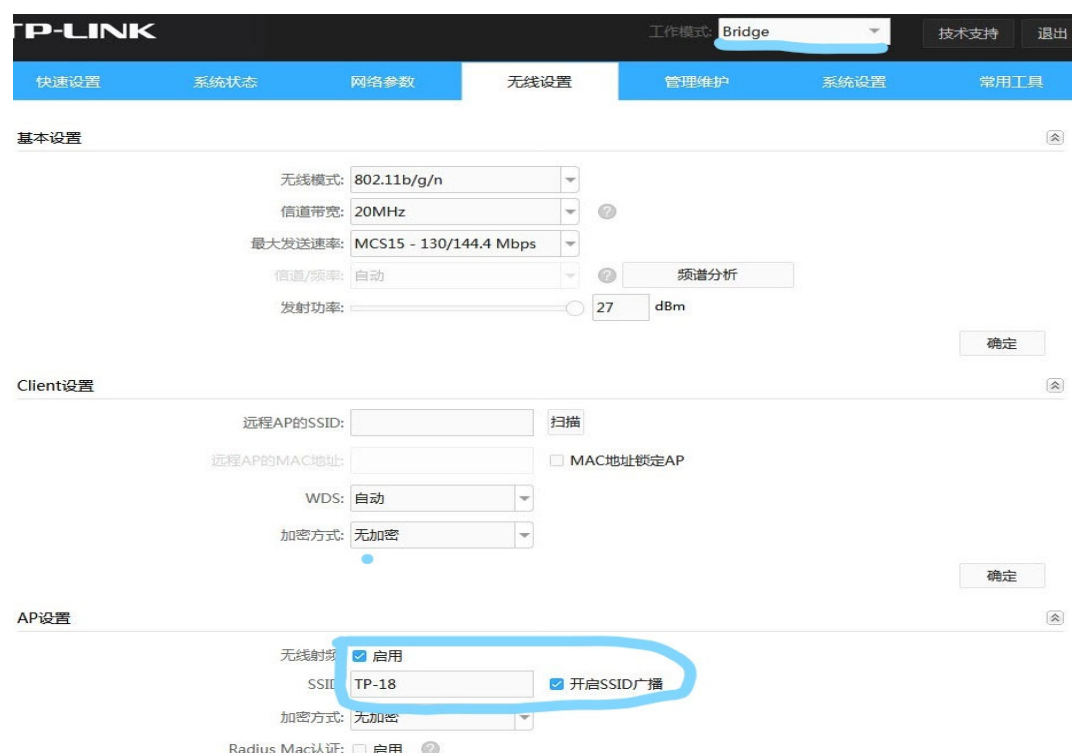
首先如图所示，根据拓扑图将各 PC 的 IP 地址设置好，默认网关可以为空或填写对应 AP 的 IP 地址，DNS 服务由于本次实验无需用到，也可以空着。



The image shows a network configuration window with the following fields and values:

- ☒ 使用下面的 IP 地址 (S):
 - IP 地址 (I): 192 . 168 . 1 . 5
 - 子网掩码 (M): 255 . 255 . 255 . 0
 - 默认网关 (D): 192 . 168 . 1 . 20
- ☐ 自动获得 DNS 服务器地址 (B)
- ☒ 使用下面的 DNS 服务器地址 (E):
 - 首选 DNS 服务器 (P): . . .
 - 备用 DNS 服务器 (A): . . .

然后分别连接 AP，进入 AP 的 Web 配置界面，在网络参数界面修改 AP 的 IP 地址（见拓扑图），修改后一定要重新登陆并保存配置。在 AP1 的配置界面右上角的工作模式中选择 Bridge 模式，保存配置。并在无线设置板块设置 SSID，启用无线射频，开启 SSID 广播。

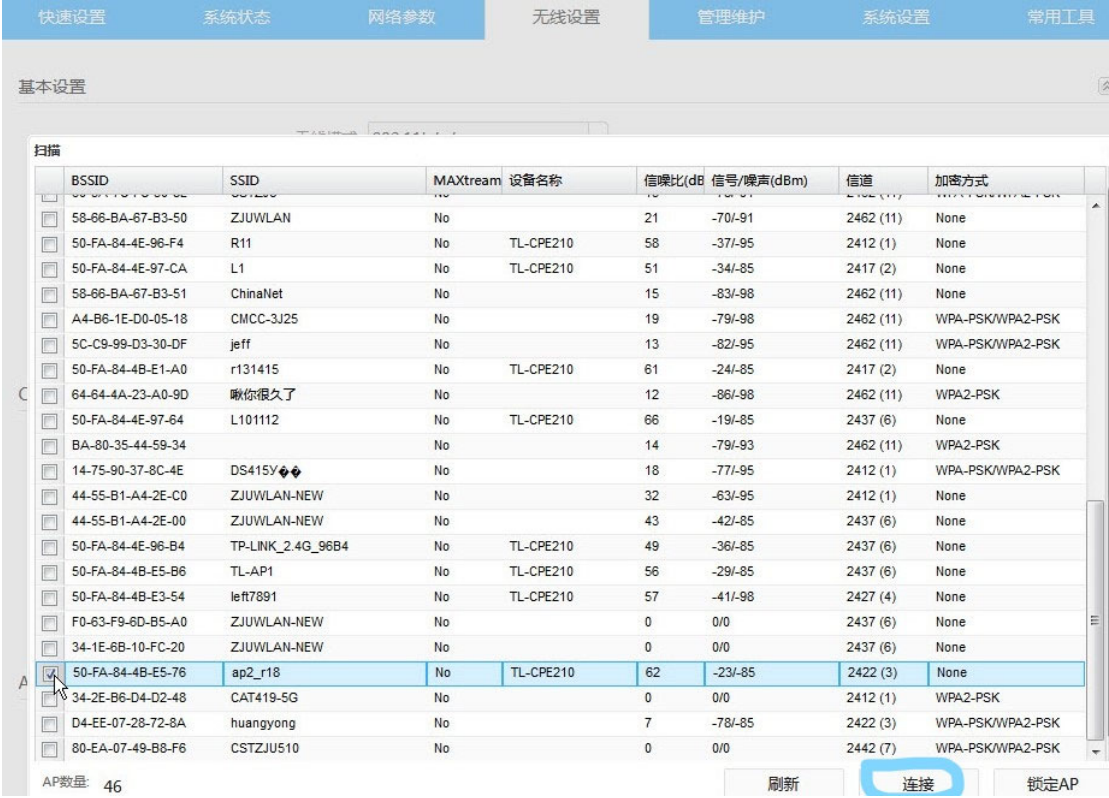


The image shows the TP-LINK AP configuration interface with the following settings:

- 工作模式: Bridge
- 快速设置 | 系统状态 | 网络参数 | 无线设置 | 管理维护 | 系统设置 | 常用工具
- 基本设置
 - 无线模式: 802.11b/g/n
 - 信道带宽: 20MHz
 - 最大发送速率: MCS15 - 130/144.4 Mbps
 - 信道/频率: 自动
 - 发射功率: 27 dBm
- Client设置
 - 远程AP的SSID: [扫描]
 - 远程AP的MAC地址: [] ☐ MAC地址锁定AP
 - WDS: 自动
 - 加密方式: 无加密
- AP设置
 - 无线射频: ☒ 启用
 - SSID: TP-18 ☒ 开启SSID广播
 - 加密方式: 无加密
 - Radius Mac认证: ☐ 启用

同样打开 AP2 的配置界面，确认其工作模式为 AP(Access Point) 模式，并设置不同的 SSID 和相同的信道。

设置好 AP2 后，点击 AP1 无线设置第二栏 Client 设置的“扫描”按钮，选中 AP2 并连接。



所有配置都确认并保存好后，就可以确认实验结果了，打开 cmd 窗口，从各个主机分别 ping 其余主机，发现都可以 ping 通，说明本次实验圆满成功，下面是 PC2 的结果截图。

```
C:\ 管理员: C:\Windows\system32\cmd.exe

来自 192.168.1.7 的回复: 字节=32 时间=6ms TTL=64
来自 192.168.1.7 的回复: 字节=32 时间=10ms TTL=64
来自 192.168.1.7 的回复: 字节=32 时间=1ms TTL=64
来自 192.168.1.7 的回复: 字节=32 时间=1ms TTL=64

192.168.1.7 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 = 1ms, 最长 = 10ms, 平均 = 4ms

C:\Users\Administrator>ping 192.168.1.5

正在 Ping 192.168.1.5 具有 32 字节的数据:
来自 192.168.1.5 的回复: 字节=32 时间=3ms TTL=64
来自 192.168.1.5 的回复: 字节=32 时间=3ms TTL=64
来自 192.168.1.5 的回复: 字节=32 时间=4ms TTL=64
来自 192.168.1.5 的回复: 字节=32 时间=21ms TTL=64

192.168.1.5 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 = 3ms, 最长 = 21ms, 平均 = 7ms

C:\Users\Administrator>
```

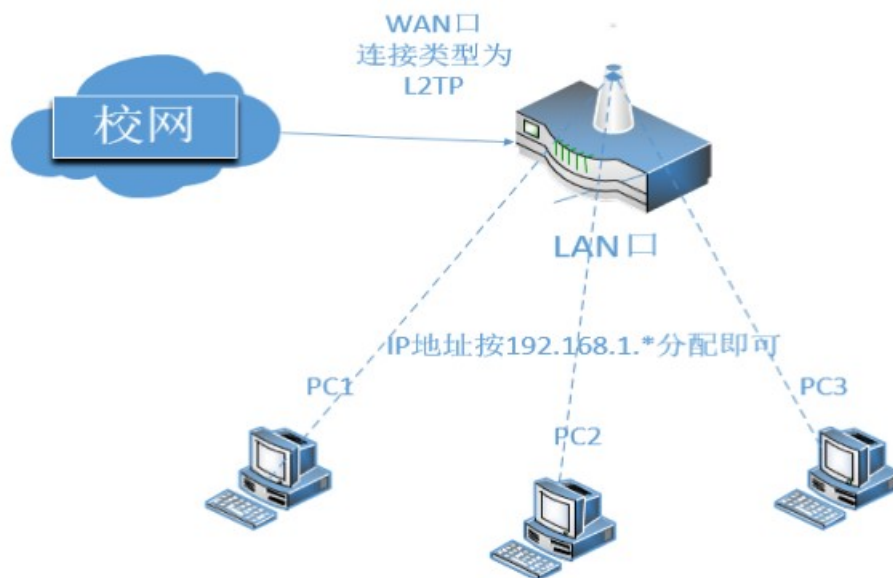
四、讨论心得

基于无线路由器的 VPN 共享上网实验

一、实验原理与内容

TL-WR847N 型无线路由器 WAN 口可支持 VPN 上网，而有时我们只有一个 VPN 账号，想要实现多台主机共同上网，就需要对路由器的设置进行一定修改。将 WAN 口连接类型修改为 L2TP，填写服务器地址和账号信息，就可以使多台 PC 利用一个 VPN 账号上网了。

二、实验拓扑图



三、实验过程与结果

首先设置好 PC1 的 IP 地址并与路由器连接，进入配置界面设置基本参数，如设置 SSID 并开启 SSID 广播等。然后进入 WAN 口设置，连接类型选择“L2TP”，输入校园网账号密码。服务器 IP/域名处填写“lms.zju.edu.cn”。再将路由器拿至教室后的交换机处连接好 WAN 口。再从 PC1 处进入配置界面在 WAN 口设置处连接等待连接成功。下图为正常连接后界面。

WAN口设置

WAN口连接类型: L2TP

上网帐号: 3200103936

上网口令:

连接 断线 已连接

☒ 动态 IP ☐ 静态 IP

服务器 IP /域名: lns.zju.edu.cn

IP 地址: 10.78.18.74

子网掩码: 255.255.255.0

网关: 10.78.18.254

DNS: 10.10.0.21 , 10.10.2.53

Internet IP: 2.205.61.93

Internet DNS: 10.10.0.21 , 10.10.2.21

数据包MTU(字节): 1460 (缺省值为1460, 如非必要, 请勿修改)

根据您的需要, 请选择对应的连接模式:

自动断线等待时间: 15 分 (0 表示不自动断线)

☒ 按需连接, 在有访问数据时自动进行连接

☐ 自动连接, 在开机和断线后自动连接

☐ 手动连接, 由用户手动连接

保存 帮助

但是实验过程中出现了一点小插曲, PC1 重新进入配置界面后, 始终无法连接成功, 如下图所示始终为空。

IP 地址: 0.0.0.0

子网掩码: 0.0.0.0

网关: 0.0.0.0

DNS: 0.0.0.0 , 0.0.0.0

Internet IP: 0.0.0.0

Internet DNS: 0.0.0.0 , 0.0.0.0

在各种尝试修改账号、参数之后没有任何改善, 我们只能去请教老师。老师解释说这是因为共享账号属于“违法操作”, 因此实验室的器材被查到后遭到封禁, 无法连接到服务器。而这种封禁基于 MAC 地址, 只要在 MAC 地址克隆功能处将路由器对广域网的 MAC 地址克隆为 PC 的 MAC 地址即可。

MAC地址克隆

本页设置路由器对广域网的MAC地址。

MAC 地址:

08-1F-71-21-21-0D

恢复出厂MAC

当前管理PC的MAC地址:

08-1F-71-21-21-0D

克隆MAC地址

注意: 只有局域网中的计算机才能使用本功能。

保存

帮助

在克隆 MAC 地址后，我们果然成功连接，并且可以访问校网与
外网。



四、讨论心得