一、 静态路由

静态路由和动态路由的区别：

静态路由：手动配置并固定的路由，当网络拓扑图发生变化的时候，需要手动更新路由表，但是没有路由器间的路由协议开销。适用于小型，简单的网络环境或网络拓扑不常变化的情况。

动态路由：是使用路由协议自动更新路由表的方式。路由器通过和其他路由器交换路由信息来自动适应网络拓扑的变化，但是路由协议有开销，可能影响网络性能。适合复杂和大规模的网络。

为什么使用静态路由：

因为实验建立的网络简单小型，拓扑图不常变化，所以使用静态路由，而且能够避免使用动态路由，而造成由路由协议产生的额外开销。

动态路由协议有什么：

域内有路由协议：RIP(基于跳数的路由协议，最大跳数 15，适用于较小规模的网络),
OSPF(基于链路状态的协议，使用 Dijkstra 适用于中大型网络)

域间有路由协议：BGP(用于不同自治系统——AS 之间的路由选择，是互联网核心的路由协议)

LSW2:

配置 VLAN 1 和关联对象 VLANIF 1:

三个端口（G0/0/1、G0/0/2、G0/0/3）全部划入 VLAN 1——实现三层交换机的路由枢纽功能：

1.让所有端口属于同一个广播域，确保 AR2,AR3,PC3 能直接通过 MAC 地址通信（无需路由），实现二层互通。

2.将端口划入 VLAN1，使得对应 VLANIF 接口（192.168.5.195）生效，启用三层路由功能，该三层路由接口（VLANIF 1）作为网 2 的网关，来处理跨网段流量。

当您看到交换机配置了 VLANIF IP 时，就意味着：
该交换机已启用三层路由功能
它既能做二层交换（基于 MAC），也能做三层路由（基于 IP）
用单台 LSW2 同时完成：
网 2 的接入交换（二层）
网 1/网 2/网 3 间的路由（三层）
流量中转枢纽（连接 AR2/AR3）

配置网关的本质:

vlan 1 # 创建 vlan 1
int vlanif 1
ip address 192.168.5.195 24 # 配置网关，实际上是在配置 VLAN 接口（VLANIF）的 IP，此作为该 VLAN 内主机的默认网关

为什么需要三层路由功能:

LSW2 需要承担网间路由的关键角色，具有跨网段通信（网 1 通过网 2 从而与网 3 通信），路由决策（根据路由表的目标 IP 选择下一跳），代替路由器（在真实网络中，

用三层交换机比"路由器+二层交换机"方案更高效）的功能。

静态路由路由表配置：

在路由器 AR2,AR3 和交换机 LSW2 上配置静态路由，

ip route static <目的网段> <子网掩码> <下一跳的目标地址>

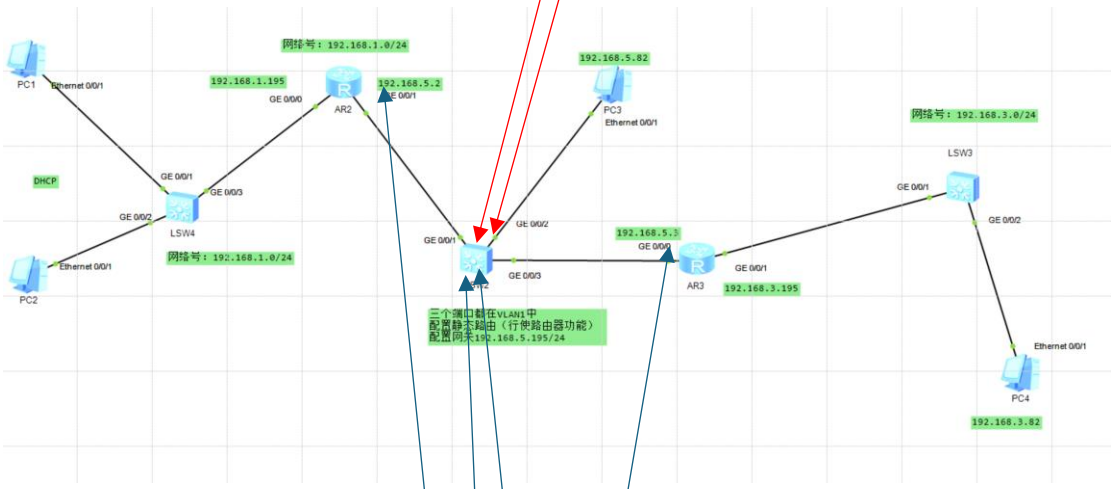
AR2 上：

想去 192.168.5.0/24 的下一跳是 192.168.5.195

ip route-static 192.168.5.0 24 192.168.5.195

想去 192.168.3.0/24 的下一跳是 192.168.5.195

ip route-static 192.168.3.0 24 192.168.5.195



AR3 上：

ip route-static 192.168.1.0 24 192.168.5.195

ip route-static 192.168.5.0 24 192.168.5.195

LSW2:

想去 192.168.1.0/24 的下一跳是 192.168.5.2

ip route-static 192.168.1.0 24 192.168.5.2

想去 192.168.3.0/24 的下一跳是 192.168.5.3

ip route-static 192.168.3.0 24 192.168.5.3

RIP 配置原理：

RIP 只需配置直连网络号（如网 1 和网 2、网 2 和网 3）是因为：

1.RIP 会通过周期性广播将路由表传递给邻居路由器

2.网 1 的路由信息会通过 AR2→LSW2→AR3 传递到网 3

3.最终所有路由器都能学习到完整路由表

RIP 工作原理：

周期性（30 秒）广播整个路由表给邻居

使用跳数（Hop Count）作为度量值

最大跳数限制为 15（16 表示不可达）
通过毒性反转和水平分割防止路由环路

主机之间为什么能 Ping 通：

属于同一网段的设备可以直接通过二层（MAC 地址）通信，无需经过网关，直连路由。

属于不同网段的 PC:

例如：PC1（网 1）ping PC3（网 2）流程:

PC1 检查目标 IP（192.168.5.82）不在同一网段
将数据包发送给默认网关（192.168.1.195）
AR2 查询路由表，通过静态路由转发到 LSW2（192.168.5.195）
LSW2 通过直连路由将数据包送达 PC3

二、 DHCP（路由器上配置）

DHCP 开启：

PC1/2 相应位置打钩

DHCP 实现设备：

路由器 AR2 作为 DHCP 服务器实现（通过 **dhcp enable** 命令）

DHCP 配置步骤：

设置路由器端口 IP（如 GE0/0/0 的 192.168.1.195）
启用 DHCP 服务（dhcp enable）
创建地址池（ip pool ggls_pl）
指定分配网段（network 192.168.1.0 mask 24）
设置网关（gateway-list 192.168.1.195）
在接口启用全局分配（dhcp select global）

DHCP 原理：

Discover：客户端广播寻找服务器
Offer：服务器回应可用 IP 地址
Request：客户端确认请求分配
Ack：服务器最终确认分配

IP 地址分配机制：

地址池采用"先到先得"的分配原则
可设置地址租期（默认 24 小时）
客户端续租时会直接向原服务器发送 Request

PC4 改用 DHCP：

AR3 配置:

```
dhcp enable
ip pool pool3
network 192.168.3.0 mask 24
```

gateway-list 192.168.3.195

三、 限速以及 ARP

限速命令解析:（配置 LSW4 的 g0/0/1）

qos lr inbound cir 500000 # 入方向限速

qos lr outbound cir 500000 # 出方向限速

- lr：line-rate（线性速率限制）
- cir：承诺信息速率 Committed Information Rate
- 500000（单位 kbps）：500Mbps，因千兆端口速率为 1000Mbps

GE 端口是千兆端口——1000Mbps，限速 50%，500Mbps

500000 单位则为 kbps

查看命令：display this

ARP 的作用，为什么要使用 ARP：

实现 IP 地址到 MAC 地址的解析，实现数据链路层的通信。

解析过程：当主机需要发送数据到另一个 IP 地址时，首先会检查自己的 ARP 缓存表，如果没有找到对应的 MAC 地址，会广播一个 ARP 请求，询问目标 IP 的 MAC 地址。

缓存：一旦获得目标 MAC 地址，会将其缓存起来，以便后续通信使用。

ARP 攻击有什么，原理是什么：

1.ARP 泛洪攻击：

原理：攻击者发送大量伪造的 ARP 请求或应答，导致 CPU 负荷过重而无法处理其他业务；或发送大量目标 IP 地址无法解析的 IP 报文，触发大量 ARP Miss 消息来消耗网络资源（触发 ARP Miss 消息的 IP 报文会被上送到设备进行处理，设备会根据 ARP Miss 消息生成和下发大量临时 ARP 表项并向目的网络发送大量 ARP 请求报文）

影响：网络性能下降，网络瘫痪

2.ARP 欺骗攻击：

原理：攻击者伪造合法的 ARP 应答，欺骗目标设备将流量重定向到攻击者的设备上。

伪造网关：攻击者把自己伪装成网关，截获用户所有流量。

伪造主机：攻击者把自己伪造成特定主机，监听或篡改该主机与其他主机的通信。

ARP 泛洪攻击的解决办法以及原理：

1. 在 AR2/3 上配置 ARP 报文限速：

如果设备对收到的大量 ARP 报文全部进行处理，可能导致 CPU 负荷过重而无法处理其他业务。因此，在处理之前，设备需要对 ARP 报文进行限速，以保护 CPU 资源

int g0/0/0

arp anti-attack rate-limit enable

arp anti-attack rate-limit <rate> <burst>

rate：限制的 ARP 报文速率（通常以 pps 为单位）——每秒最多允许 80 个 ARP 报文

burst：允许的突发 ARP 报文数量——在短时间内允许超出 <rate>的 ARP 报文数量，**1** 表示允许在短时间内有一个突发 ARP 报文。这通常用于应对短暂的 ARP 请求高峰，而不是一直保持高负载。

2. 在 AR2/3 上配置 ARP Miss 限速：

   配置 ARP Miss 消息的限速，防止因未知 IP 导致设备会根据 ARP Miss 消息生成和下发大量临时 ARP 表项并向目的网络发送大量 ARP 请求报文，从而使得资源耗尽。

   arp-miss anti-attack rate-limit enable

ARP 欺骗攻击的解决办法以及原理：

1. ARP 报文合法性检查

   判断 ARP 报文的格式跟 ARP 协议的规定是否一致

   设备会对收到的 ARP 报文进行以太网数据帧首部中的源 MAC 地址和 ARP 报文数据区中的源 MAC 地址的一致性检查，如果两者不一致，则直接丢弃该 ARP 报文，否则允许该 ARP 报文通过

   # ARP 报文合法性检查

   arp anti-attack packet-check sender-mac

2. ARP 表项固化

   fixed-all 方式：只有当 ARP 报文对应的 MAC 地址、接口、VLAN 信息和 ARP 表项中的信息完全匹配时，设备才可以更新 ARP 表项的其他内容。适用于用户 MAC 固定且接入位置不变（如服务器）。

   fixed-mac 方式：仅校验 MAC 地址是否匹配，不检查接口/VLAN（允许用户在不同端口/VLAN 间漫游，但 MAC 必须正确）。适用于移动终端（如 Wi-Fi 用户）。

   send-ack 方式：当收到 ARP 更新请求时，先向原 MAC 地址发送单播 ARP 确认，若未收到响应则拒绝更新（防中间人攻击）。此方式适用于用户的 MAC 地址和接入位置均频繁变动的场景。

   # ARP 表项固化

   arp anti-attack entry-check fixed-all enable

查看配置：display arp anti-attack configuration all