郑州工商学院

《路由交换技术》项目报告

|  |  |
| --- | --- |
| 院系名称 |  |
| 姓　　名 |  |
| 学　　号 |  |
| 专　　业 |  |

目录

[一、项目概述 1](#_Toc154931857)

[1.1河南省实验中学网络升级项目 1](#_Toc154931858)

[1.2项目要求 2](#_Toc154931859)

[二、所用技术介绍 3](#_Toc154931860)

[2.1 VLAN 3](#_Toc154931861)

[2.2 链路聚合 3](#_Toc154931862)

[2.3 MSTP、VRRP多备份组 4](#_Toc154931863)

[2.3.1MSTP 4](#_Toc154931864)

[2.3.2VRRP 4](#_Toc154931865)

[2.4 OSPF协议 5](#_Toc154931866)

[2.5 NAT地址转换 5](#_Toc154931867)

[2.6 访问控制列表 6](#_Toc154931868)

[三、项目配置 7](#_Toc154931869)

[3.1 配置IP地址 7](#_Toc154931870)

[3.2 配置VLAN、链路聚合 8](#_Toc154931871)

[3.3 配置MSTP+VRRP多备份组 10](#_Toc154931872)

[3.4 配置OSPF协议 12](#_Toc154931873)

[3.5 配置NAT地址转换 14](#_Toc154931874)

[3.6 配置访问控制列表 14](#_Toc154931875)

[四、测试结果 15](#_Toc154931876)

[4.1 链路聚合测试结果 15](#_Toc154931877)

[4.2 MSTP多生成树测试结果 16](#_Toc154931878)

[4.3 VRRP多备份组测试结果 18](#_Toc154931879)

[4.4 OSPF协议测试结果 19](#_Toc154931880)

[4.5 NAT地址转换测试结果 23](#_Toc154931881)

[4.6 访问控制列表测试结果 25](#_Toc154931882)

[五、总结与收获 28](#_Toc154931883)

# 一、项目概述

## 1.1河南省实验中学网络升级项目

当谈及信息技术的迅猛发展，河南省实验中学一直秉持着为学生提供优质教育资源的宗旨。如今，随着时代的步伐，学校意识到网络基础设施的关键性。为了提升校园网络的可靠性、安全性和灵活性，将决定进行一次全面的网络升级项目。眼下的网络结构存在一些瓶颈和不足，比如部分楼栋间的网络互联存在障碍，对外网的访问管理缺乏细致的控制，并且在面对单点故障时缺乏有效的解决方案。为了解决这些问题，学校制定了一个全面的网络升级方案，目标是打造一个高效、安全、稳定的校园网络环境。

这项网络升级计划囊括了多方面的改进。首先，将致力于优化楼栋间的网络连接，采用更为先进的技术和设备来确保各个区域之间的畅通无阻。其次，针对外部网络访问的管理，将采取更为精细化的控制措施，以确保安全性和合规性。这涉及到强化网络安全防护措施。同时，也将注重在网络架构上建立冗余和备份系统，以防止单点故障对整个网络系统造成的影响。

除此之外，还将加强网络设备的更新和维护，确保设备运行在最佳状态下，并且针对未来的技术发展做好相应的准备和规划。这项升级计划不仅关乎网络基础设施的提升，更意味着为学生和教职员工创造一个更好的学习和工作环境。

通过这次网络升级项目，河南省实验中学将在教育领域迈出坚实的一步。这不仅是对网络技术的升级，更是对学校教育质量的提升和未来发展的投资。这样一个高效、安全、稳定的校园网络环境将为学生提供更广阔的学习资源和更安全的在线学习环境，也将为教师提供更便捷、高效的教学工具和资源，进而推动学校整体教育水平的提升。这次升级不仅是技术上的改进，更是对学校教育使命的践行和对未来发展的筹备，必将为学校带来更广阔的发展空间和更丰富的教育资源。

## 1.2项目要求

在网络升级计划中，河南省实验中学致力于在多个方面进行改进，以构建一个高效、安全、稳定的校园网络环境。其中，针对栋楼间网络互通，规划了IP地址和VLAN，旨在确保教学楼、行政楼、实验楼和宿舍楼之间实现良好的网络互联互通。这一步骤不仅是为了方便各个楼栋之间的数据交换和资源共享，更是为了支持学校各项教学、管理和研究活动的顺利展开。通过有效的IP地址规划和VLAN配置，学校将实现不同功能楼宇之间的高效沟通，为学校内部各项活动提供良好的网络支持。

外网访问管理也是这次网络升级计划中的重点之一。将采用OSPF协议，允许教学楼、行政楼和实验楼访问外网环境，同时通过访问控制列表（ACL）限制宿舍楼访问外网。这一举措不仅考虑到了网络安全性，更是为了合理利用网络资源。通过ACL的设置，学校能够精准控制宿舍楼的外网访问权限，保障网络安全，并确保网络带宽的合理分配和利用。

在面对网络故障时，也着重考虑了解决方案。为此，学校设立了冗余链路，并通过链路聚合实现配置MSTP+VRRP多备份组。这一措施旨在应对单点故障，确保网络在遇到故障时能够实现快速切换，从而提高网络的可靠性和稳定性。通过这样的配置，学校将极大地降低网络故障带来的影响，保障网络的连续性和稳定性。

网络安全是这次升级计划的重中之重。学校将在出口路由器上实现NAT地址转换，使内部主机使用内部全局地址访问外网环境。这一举措将增强网络整体的安全性和隐私保护。通过NAT地址转换，学校能够隐藏内部网络的真实结构，有效防止外部恶意攻击和信息泄露，提高网络的整体安全性。

过规划IP地址和VLAN、外网访问管理、冗余链路设置以及NAT地址转换等措施，学校将构建一个更为高效、安全、稳定的校园网络环境，为学生和教职员工提供更好的学习和工作体验，推动学校整体教育水平的提升。

# 二、所用技术介绍

## 2.1 VLAN

河南省实验中学作为一个拥有教学楼、实验楼、宿舍楼和行政楼等多个功能区域的综合性学校，网络结构的优化与管理至关重要。VLAN（Virtual Local Area Network，虚拟局域网）技术可以以实现网络的分割和管理，满足不同区域的安全性、性能和管理需求。VLAN技术被用于将不同功能的楼栋划分为逻辑上独立的网络单元。教学楼、实验楼、宿舍楼和行政楼的网络需要相互隔离，以确保安全性和网络资源的有效分配。

学校网络管理员可以实施更精细的访问控制策略。例如，限制宿舍楼访问外部网络，确保教学和行政楼能够访问外网资源，同时防止不必要的外部访问，提高网络安全性。VLAN的使用可以减少广播风暴的发生，优化网络性能。不同VLAN之间的通信需要经过路由器，限制了广播域的范围，有助于减少不必要的广播流量，提高网络效率。

根据学校的组织结构和功能区域划分，确定每个楼栋或功能区域对应的VLAN编号和IP地址范围。例如，教学楼可以是VLAN 10，行政楼是VLAN 20，实验楼是VLAN 30，宿舍楼是VLAN 40。

同时设置ACL（访问控制列表）限制宿舍楼的访问，确保其不能直接访问外部网络，以保障网络安全。同时，允许教学楼、行政楼和实验楼访问外网资源，满足教学与管理需求。VLAN技术在河南省实验中学的应用需要综合考虑安全性、性能和管理需求。通过合理的VLAN划分和精细化的管理策略，可以构建一个安全、高效、灵活的网络环境，为师生提供更好的教学和学习体验。

## 2.2 链路聚合

链路聚合技术（Link Aggregation）是一种网络技术，旨在增加网络带宽、提高可靠性和容错能力。它通过将多个物理网络连接（通常是以太网连接）捆绑为单个逻辑连接，从而形成一个高容量、高可靠性的链路

在河南省实验中学中链路聚合以增加带宽和负载均衡，通过将多个物理链路捆绑在一起，链路聚合可以合并它们的带宽，从而提高整体带宽。这不仅提升了网络性能，还实现了负载均衡，使流量在多条链路间均匀分布，避免某条链路过载。

提高可靠性和容错能力。链路聚合技术还可以提高网络的可靠性。当一个物理链路发生故障时，仍然可以保持连接，不会导致整个网络的中断，这种容错能力对于校园网络尤为重要。

冗余备份与故障恢复。链路聚合允许多个链路同时工作，即使一个链路出现故障，其他链路仍可继续工作，确保网络连通性。这对于实验中学这样对网络可用性要求高的场景至关重要。

## 2.3 MSTP、VRRP多备份组

### 2.3.1MSTP

MSTP（Multiple Spanning Tree Protocol，多路生成树协议）和VRRP（Virtual Router Redundancy Protocol，虚拟路由器冗余协议）是网络协议和容错机制时常用的技术，可以提高网络的高可用性和容错能力。

MSTP是STP的一种扩展，允许在网络中创建多个生成树实例，每个实例对应于不同的VLAN，一个实例可以加入多个。这意味着可以针对不同的VLAN使用不同的生成树路径，提高了网络的性能和容错能力。每个区域可以有自己的生成树，减少了因链路故障而导致整个网络拓扑变更的可能性。这有助于减少网络收敛时间，提高网络稳定性。

MSTP可以在不同的VLAN上独立运行生成树实例，使得网络资源得到更优化的利用，同时避免了单个生成树对整个网络性能的影响。

### 2.3.2VRRP

VRRP允许多台路由器共享一个虚拟IP地址，其中一台路由器被选为主路由器（Master），负责处理流量，其他路由器为备份（Backup）。如果主路由器出现故障，备份路由器可以迅速接管主路由器的职责，实现快速的故障转移。

VRRP提供了路由器的冗余备份，确保网络在路由器发生故障时仍能保持连

通，提高了网络的可用性。虽然VRRP通常用于提供冗余，但也可用于负载均衡。通过合理配置VRRP权重，可以让主备路由器分担不同比例的流量，从而实现负载均衡。

## 2.4 OSPF协议

链路状态路由选择协议又被称为最短路径优先协议，是一种内部网关协议，它基SPF（shortest path first ）算法。他比距离矢量协议复杂的多。路由器的链路状态的信息称为链路状态，包括：接口的IP地址和子网掩码，网络类型，（如以太网链路或串行点对点链路），该链路的开销，该链路上的所有的相邻路由器。

OSPF是基于链路状态的路由协议，它维护了一个路由器之间连接状态的数据库。每个路由器收集并发送链路状态信息，以构建整个网络的拓扑图，并计算最短路径。同时OSPF能够动态适应网络拓扑的变化，当网络发生变化时（如链路故障或新增路由器），它可以快速地调整路由路径，选择新的最佳路径。

OSPF在河南省实验中学能够发挥它的作用，因为它能够管理复杂的网络拓扑并提供灵活的路由策略。作为内部网关协议，OSPF用于路由数据包在内部网络中的传输，确定最佳路径并保证数据传输的可靠性和效率。

## 2.5 NAT地址转换

NAT（Network Address Translation，网络地址转换）是一种网络技术，用于将私有网络的IP地址转换为公共网络的IP地址，以实现内部网络和外部网络的通信。静态转换是指内部本地地址一对一转换成内部全局地址，相当内部本地的每一台PC都绑定了一个全局地址。一般用于在内网中对外提供服务的服务器。

在本次项目中采用了静态nat。

使用NAT可以隐藏内网的IP，以隐藏学校内网IP，防止网络攻击。使得内部网络可以访问互联网，同时防止从外部直接访问内部网络。

共享公共IP地址： 在企业内部网络中，多个设备可以通过NAT共享同一个公共IP地址访问互联网，节省了公共IP地址的使用。

内部访问外部网络： NAT允许内部网络中的设备访问互联网资源，但不允许外

部网络直接访问内部网络，增强了网络安全性。

隐藏内部结构： 通过地址转换，企业可以隐藏内部网络拓扑结构和真实IP地址，提高了安全性，并且减少了外部攻击的风险。

## 2.6 访问控制列表

ACL时，是网络设备上的一种重要机制，允许网络管理员基于一系列设定的规则，精确地控制网络中数据包的流动。这些规则可应用于路由器、防火墙或交换机等设备，以实现对数据流向的管理。

ACL由一系列规则组成，每条规则定义了特定的条件。这些条件可能基于源IP地址、目标IP地址、端口号、协议类型等。

最常见的用途是过滤数据流，允许或者拒绝特定类型的流量。这种策略可基于规则，控制数据包进出网络的方式，从而增强网络安全性。

# 三、项目配置

## 3.1 配置IP地址

PC机

PC4:

IP: 192.168.30.30

Subnet Mask: 255.255.255.0

Gateway: 192.168.30.254

PC3:

IP: 192.168.20.20

Subnet Mask: 255.255.255.0

Gateway: 192.168.20.254

PC2:

IP: 192.168.10.11

Subnet Mask: 255.255.255.0

Gateway: 192.168.10.253

PC6:

IP: 192.168.40.41

Subnet Mask: 255.255.255.0

Gateway: 192.168.40.253

R2 (No relevant network information in settings attribute)

PC5:

IP: 192.168.40.40

Subnet Mask: 255.255.255.0

Gateway: 192.168.40.253

Server1:

IP: 200.1.1.100

Subnet Mask: 255.255.255.0

Gateway: 200.1.1.254

PC1:

IP: 192.168.10.10

Subnet Mask: 255.255.255.0

Gateway: 192.168.10.254

## 3.2 配置VLAN、链路聚合

LSW3:

Vlan vatch 10 20 30 40

Interface E0/0/1

Port link-type trunk

Port trunk allow-pass vlan all

Interface E0/0/2

Port link-type trunk

Port trunk allow-pass vlan all

Interface E0/0/3

Port link-type access

Port default vlan 10

Interface E0/0/4

Port link-type access

Port default vlan 10

Interface E0/0/5

Port link-type aceess

Port default vlan 20

LSW4:

Vlan batch 10 20 30 40

Interface E0/0/1

Port link-type trunk

Port trunk allow-pass vlan all

Interface E0/0/2

Port link-type trunk

Port trunk allow-pass vlan all

Interface E0/0/3

Port link-type access

Port default vlan 30

Interface E0/0/4

Port link-type access

Port default vlan 40

Interface E0/0/5

Port link-type access

Port default vlan 40

LSW1:

Vlan batch 10 20 30 40

interface Eth-trunk 1

port link-type trunk

port trunk allow-pass vlan all

interface G0/0/23

Eth-trunk 1

Interface G0/0/24

Eth-trunk 1

Interface G0/0/3

Port link-type trunk

Port allow-pass vlan all

Interface G0/0/2

Port link-type trunk

Port allow-pass vlan all

LSW2

Vlan batch 10 20 30 40

Interface Eth-trunk 1

port link-type trunk

port trunk allow-pass vlan all

interface G0/0/23

Eth-trunk 1

Interface G0/0/24

Eth-trunk 1

Interface G0/0/2

Port link-type trunk

Port trunk allow-pass vlan all

Interface G0/0/3

Port link-type trunk

Port trunk allow-pass vlan all

## 3.3 配置MSTP+VRRP多备份组

LSW1:

Interface vlanif 10

Ip address 192.168.10.100

Vrrp vrid 10 virtual-ip 192.168.10.254

Vrrp vrid 10 priority 150

Vrrp vrid 11 virtual-ip 192.168.10.253

Interface vlanif 20

Ip address 192.168.20.100

Vrrp vrid 20 virtual-ip 192.168.20.254

Vrrp vrid 20 priority 150

Vrrp vrid 21 virtual-ip 192.168.20.253

Interface vlanif 30

Ip address 192.168.30.100

Vrrp vrid 30 virtual-ip 192.168.30.254

Vrrp vrid 30 priority 150

Vrrp vrid 31 virtual-ip 192.168.30.253

Interface vlanif 40

Ip address 192.168.40.100

Vrrp vrid 40 virtual-ip 192.168.40.254

Vrrp vrid 40 priority 150

Vrrp vrid 41 virtual-ip 192.168.40.253

Stp mode mstp

Stp region-configuration

Region-name chenyong

Instance 1 vlan 10 30

Instance 2 vlan 20 40

Active region -configuraion

Stp instan 1 root primary

LSW2:

Interface vlanif 10

Ip address 192.168.10.200

Vrrp vrid 10 192.168.10.254

Vrrp vrid 11 192.168.10.253

Vrrp vrid 11 priority 150

Interface vlanif 20

Ip address 192.168.20.200

Vrrp vrid 20 192.168.20.254

Vrrp vrid 21 192.168.20.253

Vrrp vrid 31 priority 150

Interface vlanif 30

Ip address 192.168.30.200

Vrrp vrid 30 192.168.30.254

Vrrp vrid 31 192.168.30.253

Vrrp vrid 31 priority 150

Interface vlanif 40

Ip address 192.168.40.200

Vrrp vrid 40 192.168.40.254

Vrrp vrid 41 192.168.40.253

Vrrp vrid 41 priority

Stp mode mstp

Stp region-configuration

Region-name chenyong

Instance 1 vlan 10 30

Instance 2 vlan 20 40

Active region-configuration

Stp instance 2 root primary

LSW3:

Stp mode mstp

Stp region-configuration

Region-name chenyong

Instance 1 vlan 10 30

Instance 2 vlan 20 40

Active region-configuration

LSW4:

Stp mode mstp

Stp region-configuration

Region-name chenyong

Instance 1 vlan 10 30

Instance 2 vlan 20 40

Active region-configuration

## 3.4 配置OSPF协议

R2：

Interface G0/0/0

Ip address 192.168.12.1 30

Q

Interface E0/0/0

Ip address 200.100.10.1 30

Q

Interface G0/0/1

Ip address 192.168.11.1 30

Q

Ospf 1

Area 0

Network 200.100.10.0 0.0.0.3

Network 192.168.11.0 0.0.0.3

Network 192.168.12.0 0.0.0.3

Q

LSW1:

Vlan batch 50

interface G0/0/1

port link-type access

port default vlan 50

q

interface vlanif 50

ip address 192.168.12.2 30

q

ospf 1

area 0

network 192.168.12.0 0.0.0.3

network 192.168.10.0 0.0.0.255

network 192.168.20.0 0.0.0.255

network 192.168.30.0 0.0.0.255

network 192.168.40.0 0.0.0.255

LSW2:

Vlan batch 50

Interface G0/0/1

Port link-type access

Port default vlan 50

Q

Interface vlanif 50

Ip address 192.168.11.2 30

Q

Ospf 1

Area 0

network 192.168.11.0 0.0.0.3

network 192.168.10.0 0.0.0.255

network 192.168.20.0 0.0.0.255

network 192.168.30.0 0.0.0.255

network 192.168.40.0 0.0.0.255

AR2:

Interface G0/0/0

Ip address 200.100.10.2 30

Q

Interface G0/0/1

Ip address 200.1.1.254 24

Q

Ospf 1

Area 0

Network 200.100.10.0 0.0.0.3

Network 200.1.1.0 0.0.0.255

## 3.5 配置NAT地址转换

AR2:

Interface G0/0/1

nat static global 202.199.184.10 inside 192.168.10.10

nat static global 202.199.184.11 inside 192.168.10.11

nat static global 202.199.184.12 inside 192.168.20.20

nat static global 202.199.184.13 inside 192.168.30.30

nat static global 202.199.184.14 inside 192.168.40.40

nat static global 202.199.184.15 inside 192.168.40.41

## 3.6 配置访问控制列表

Acl 2000

Rule deny source 202.199.184.15 0

Rule deny source 202.199.184.14 0

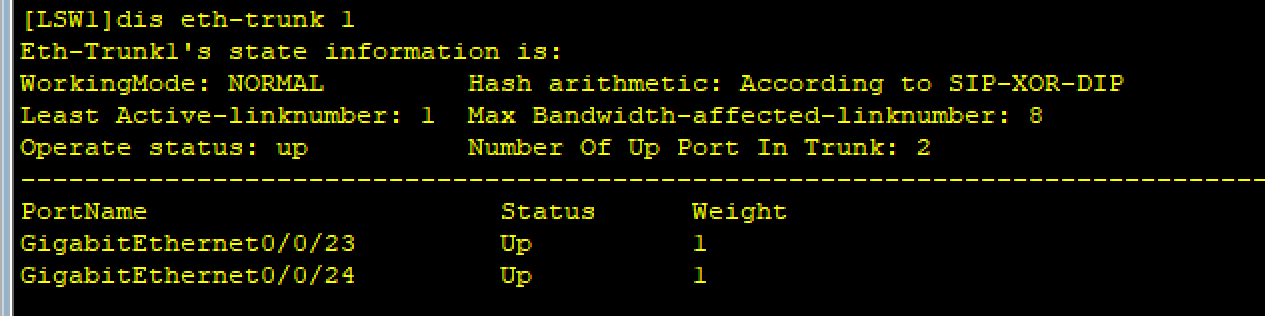
Interface G0/0/0

traffic-filter inbound acl 2000

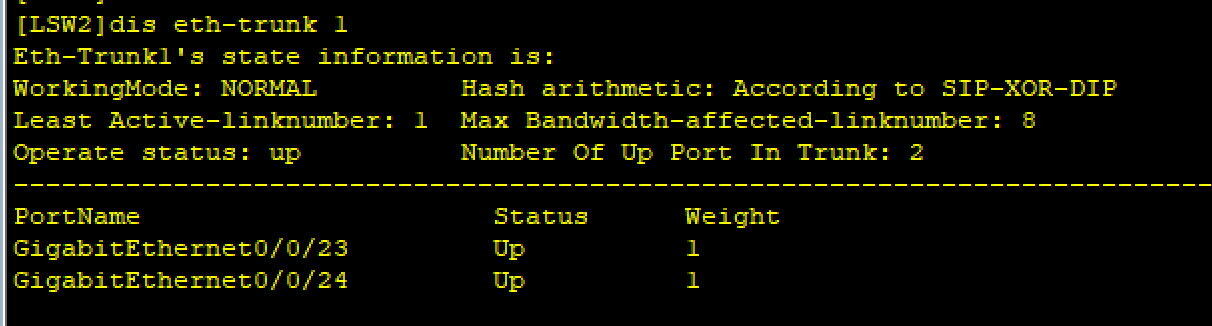
# 四、测试结果

## 4.1 链路聚合测试结果

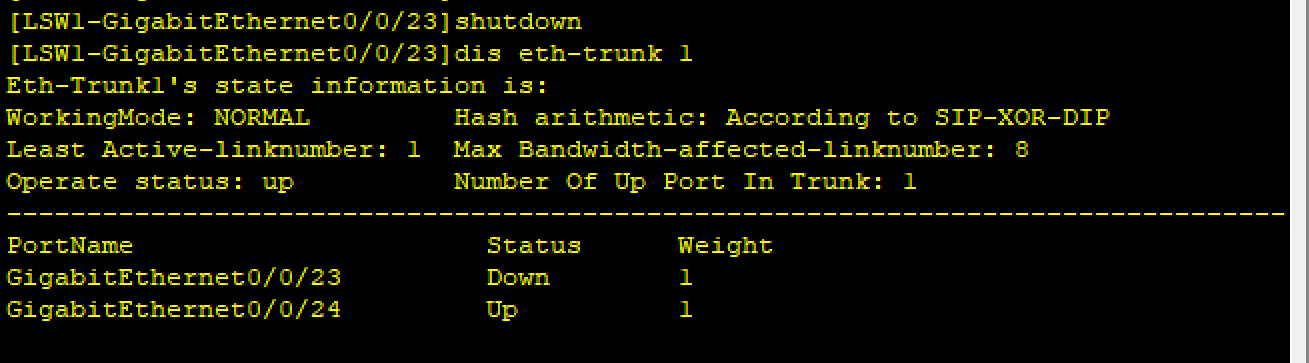
在LSW1上执行：dis eth-trunk 1



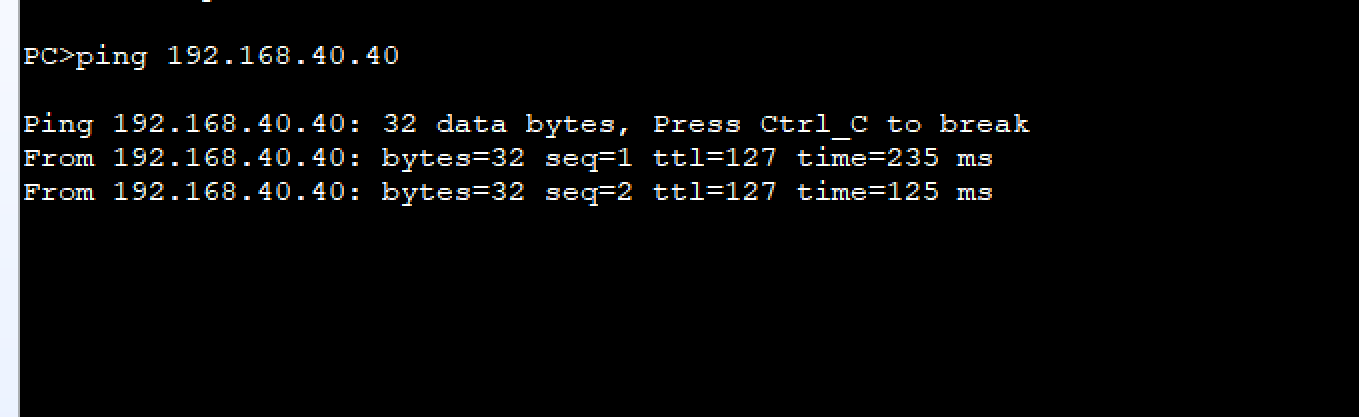
在LSW2上执行：dis eth-trunk 1



将G0/0/23 down掉，在执行：dis eth-trunk 1

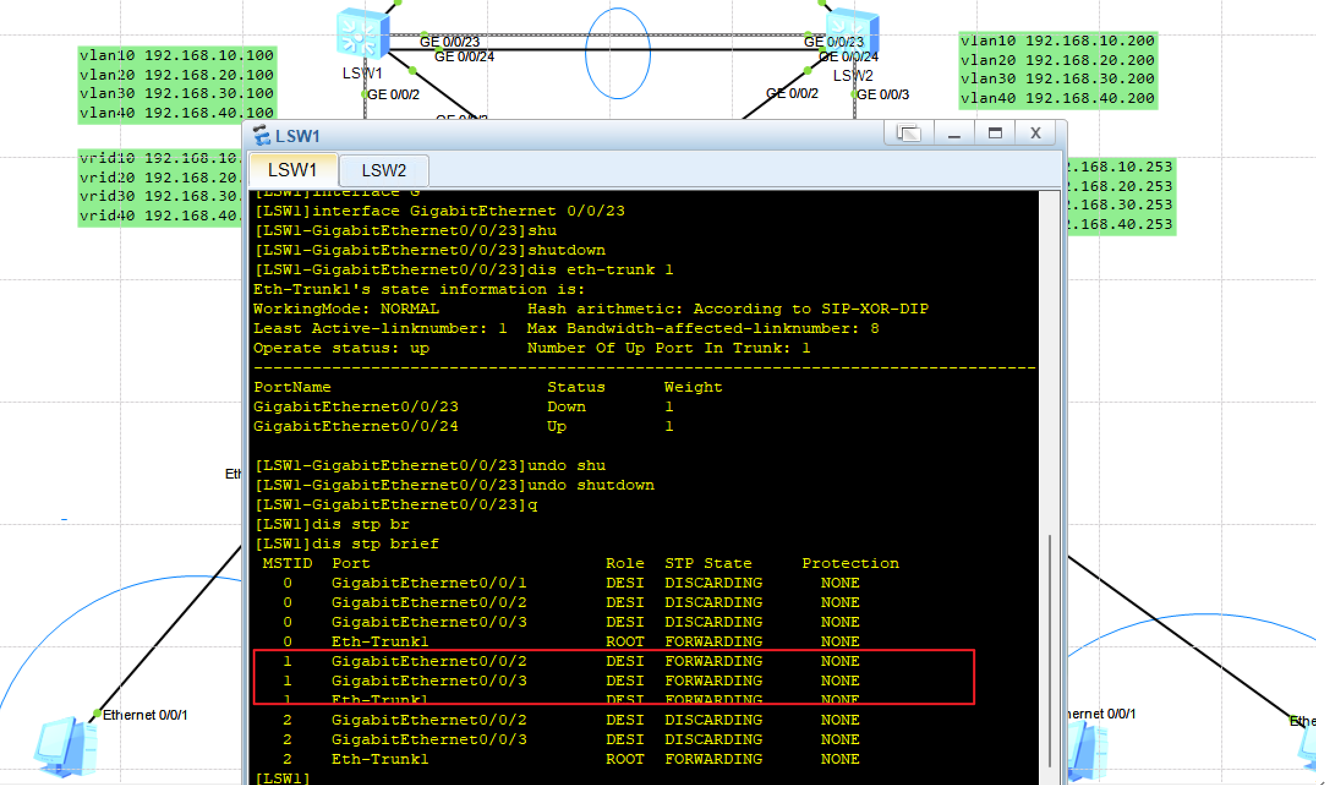


依然可以ping通



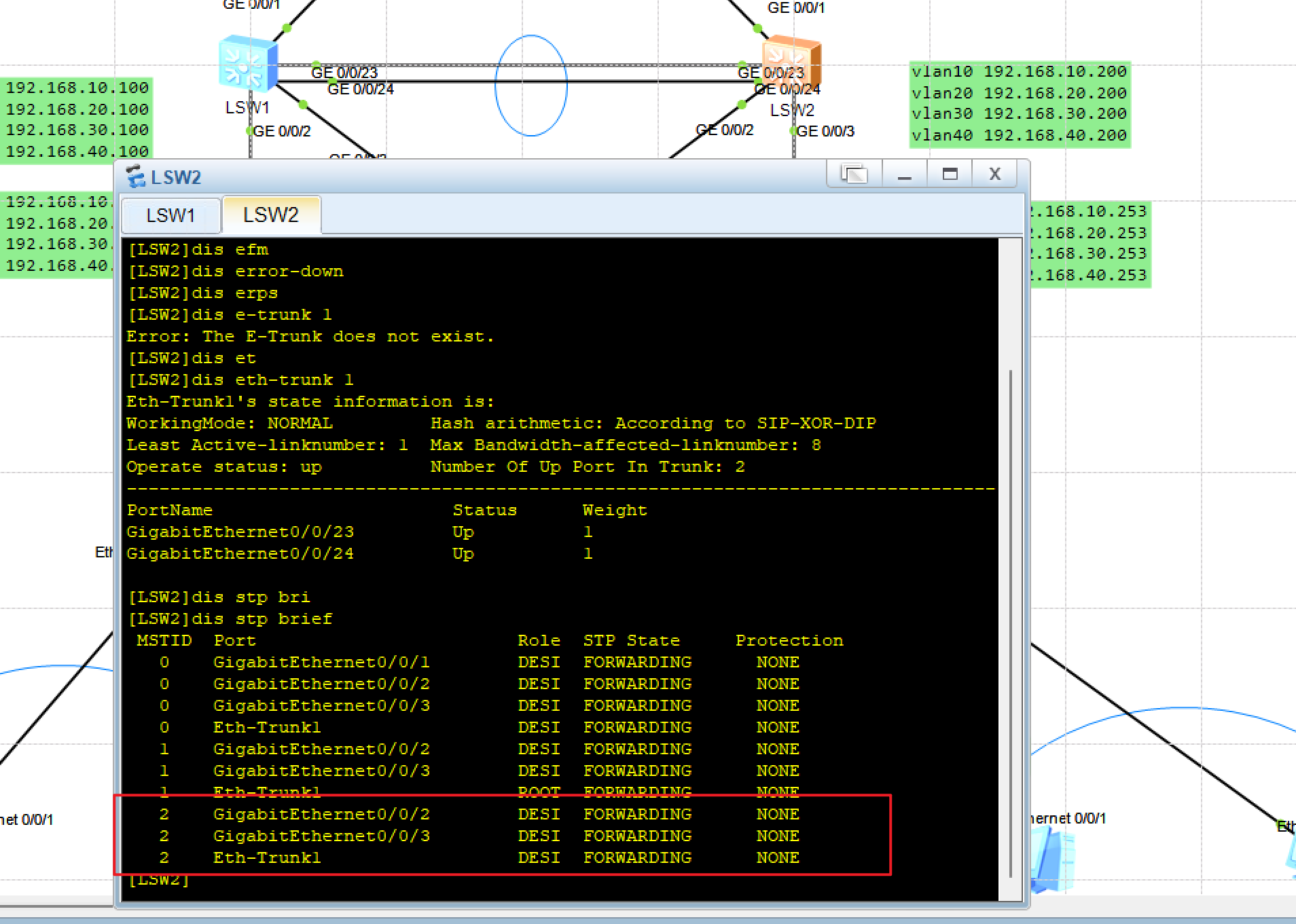
## 4.2 MSTP多生成树测试结果

在LSW1中执行：dis stp brief



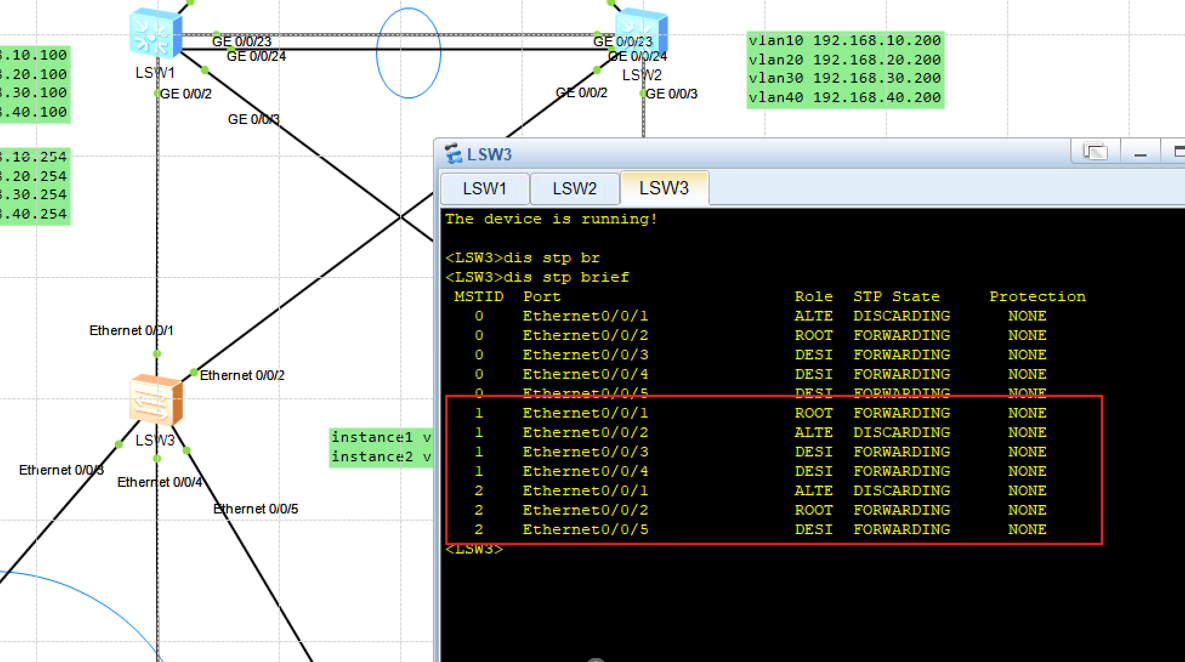
可以很明显发现，在MSTID为1中LSW1作为根桥，它的各个端口都为指定端口。

同理在LSW2中：

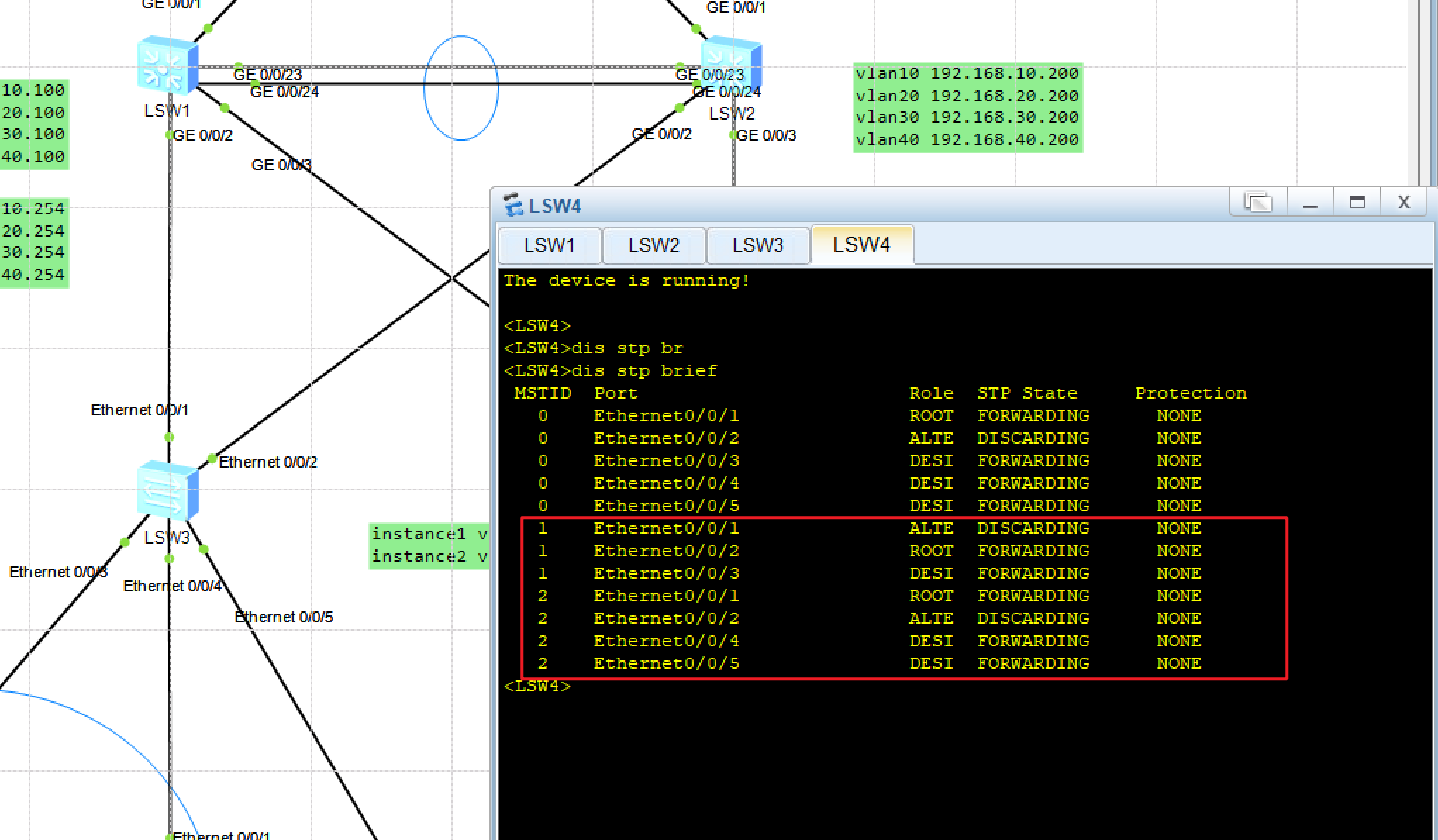


LSW2的所有端口都为指定端口。

在LSW3中：

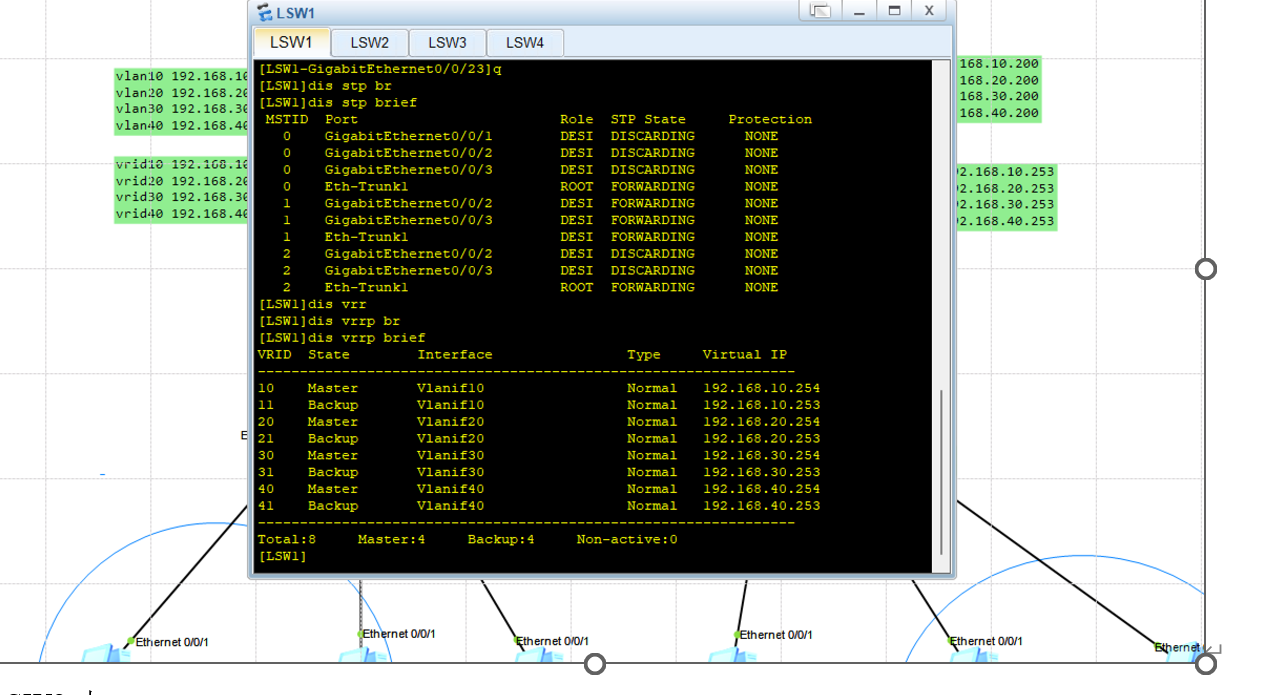


在LSW4中：

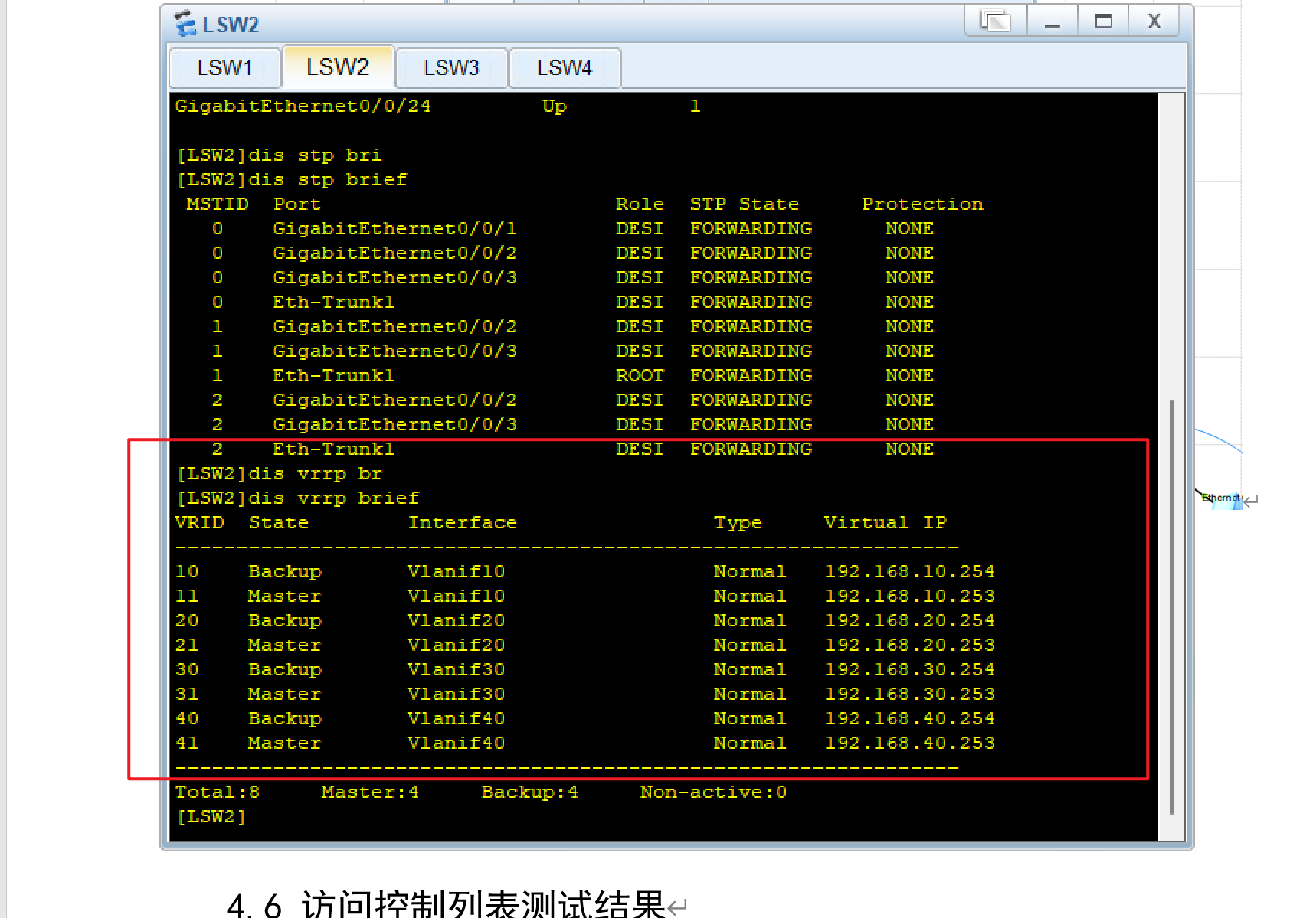


## 4.3 VRRP多备份组测试结果

LSW1中：



LSW2中：



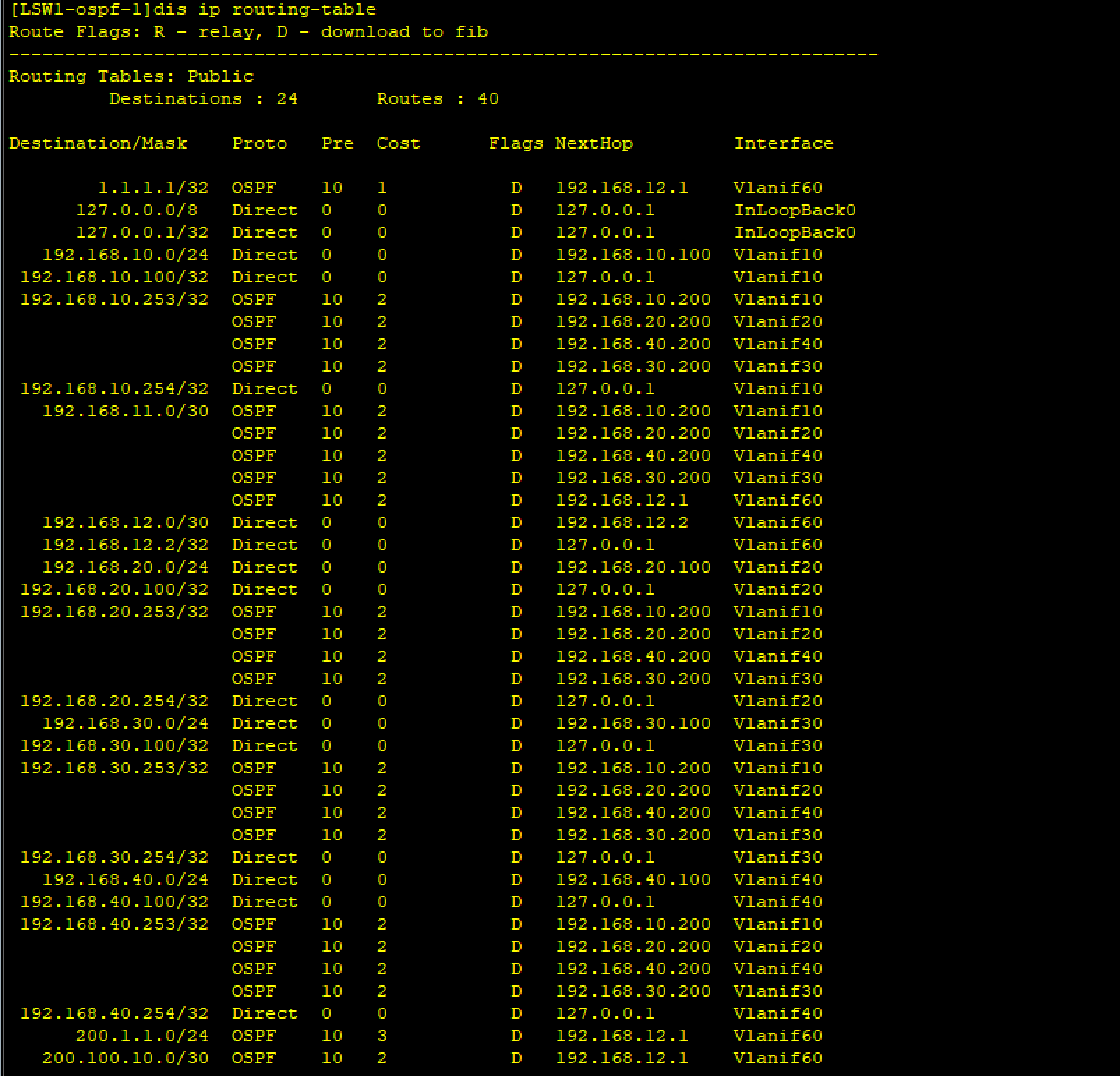
254在LSW1中作为master，253作为备份

253在LSW2中作为master，254作为备份

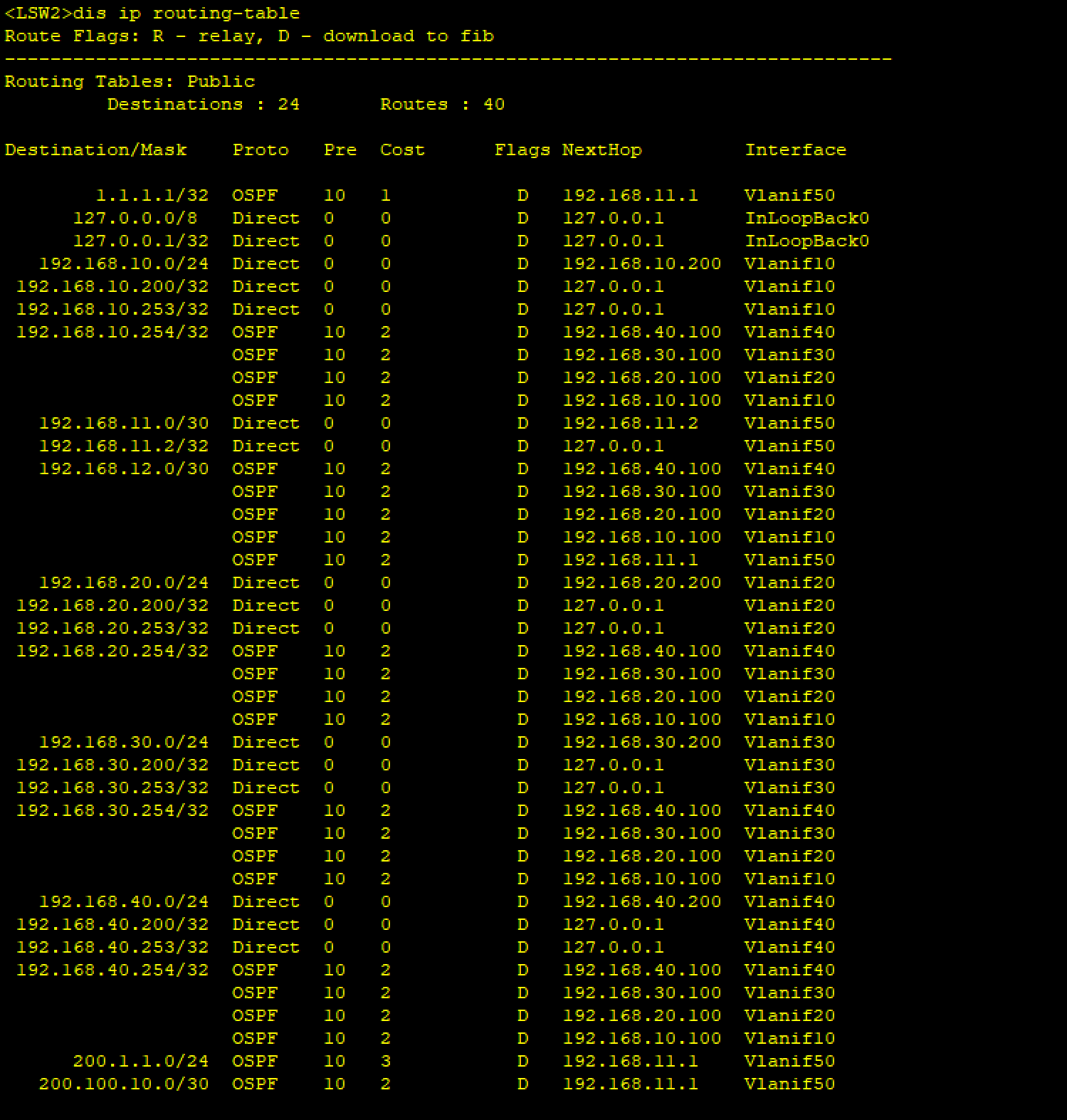
这样可以实现多备份组，充分利用资源。

## 4.4 OSPF协议测试结果

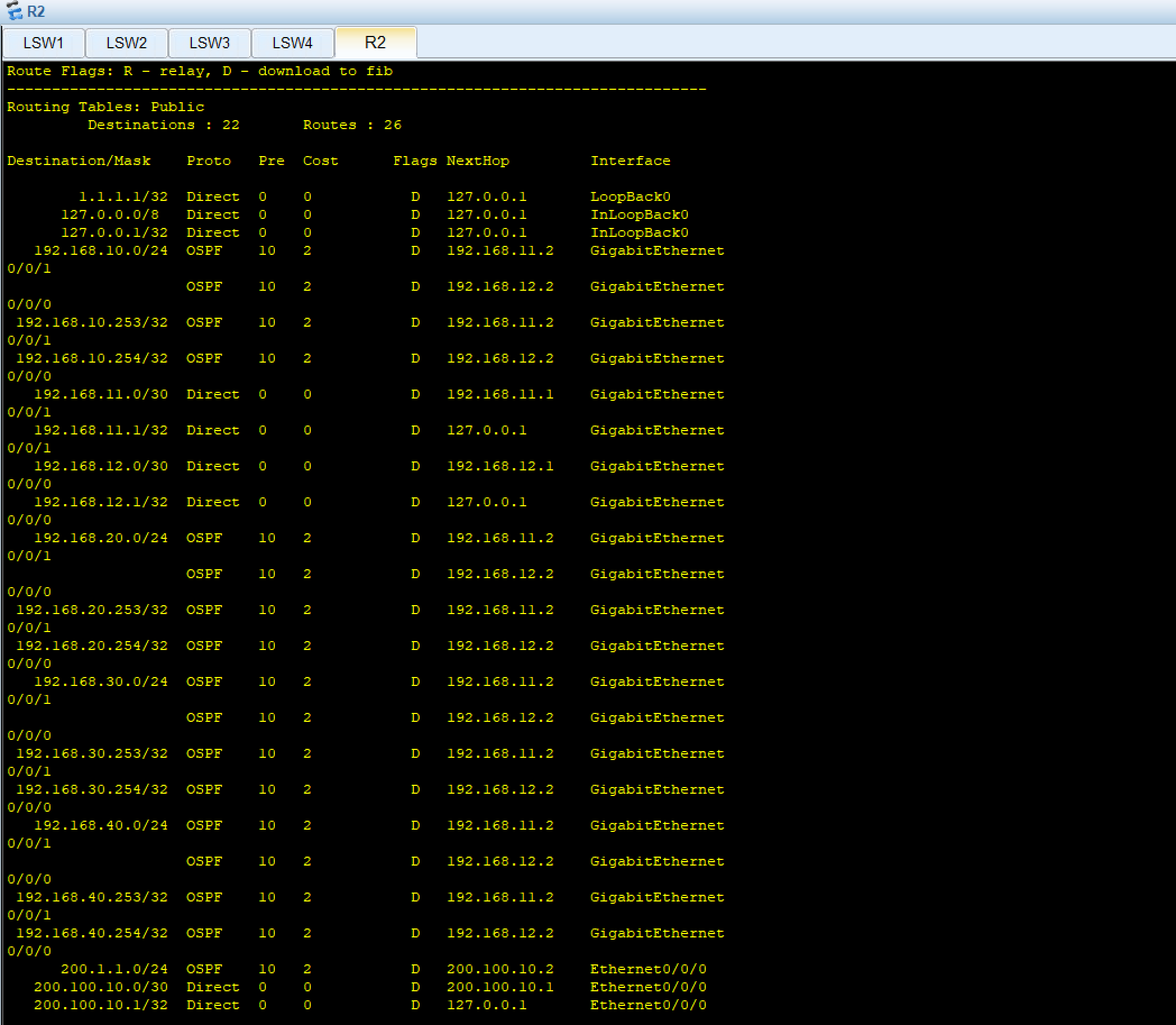
LSW1：



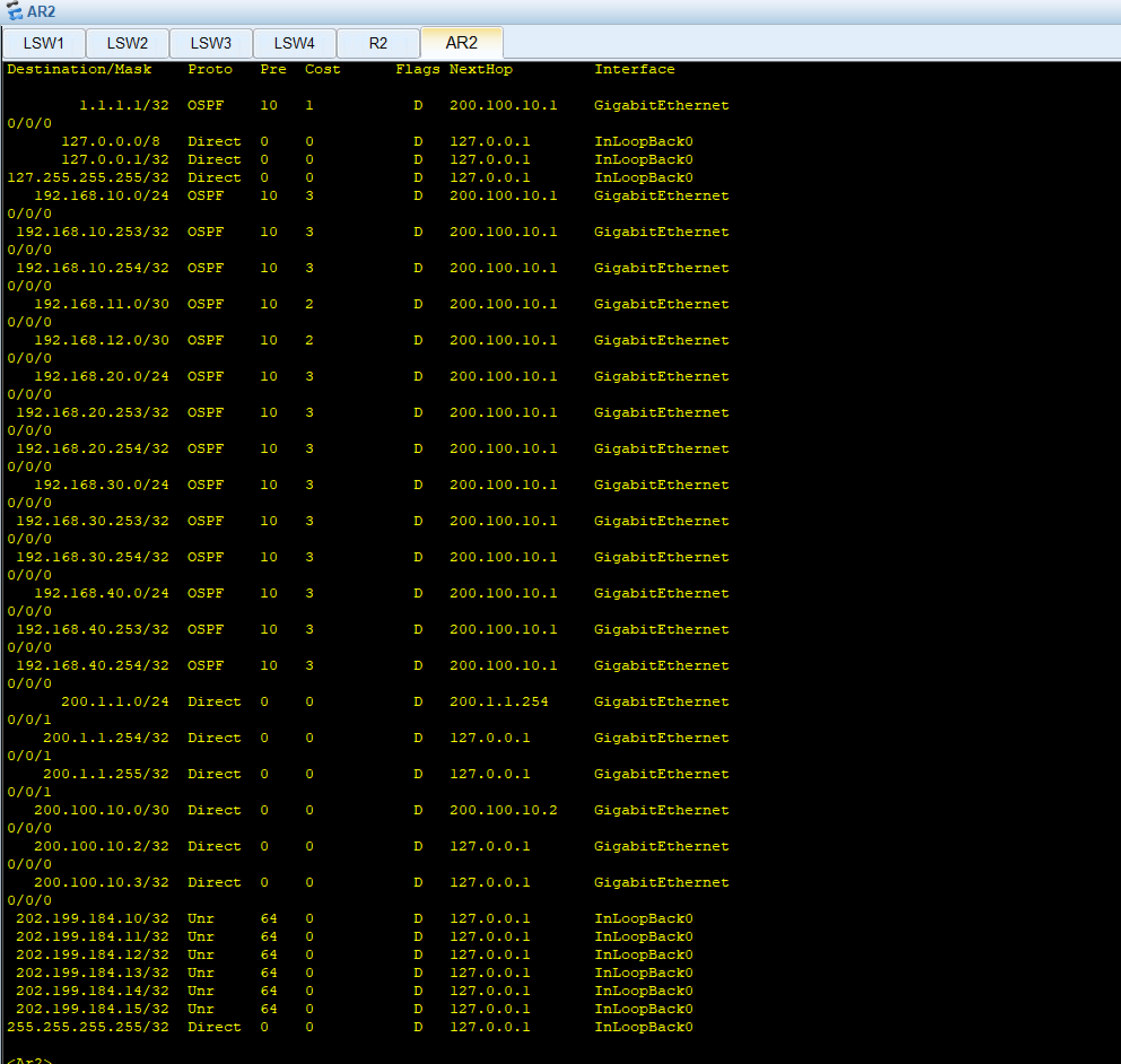
LSW2：



R2：

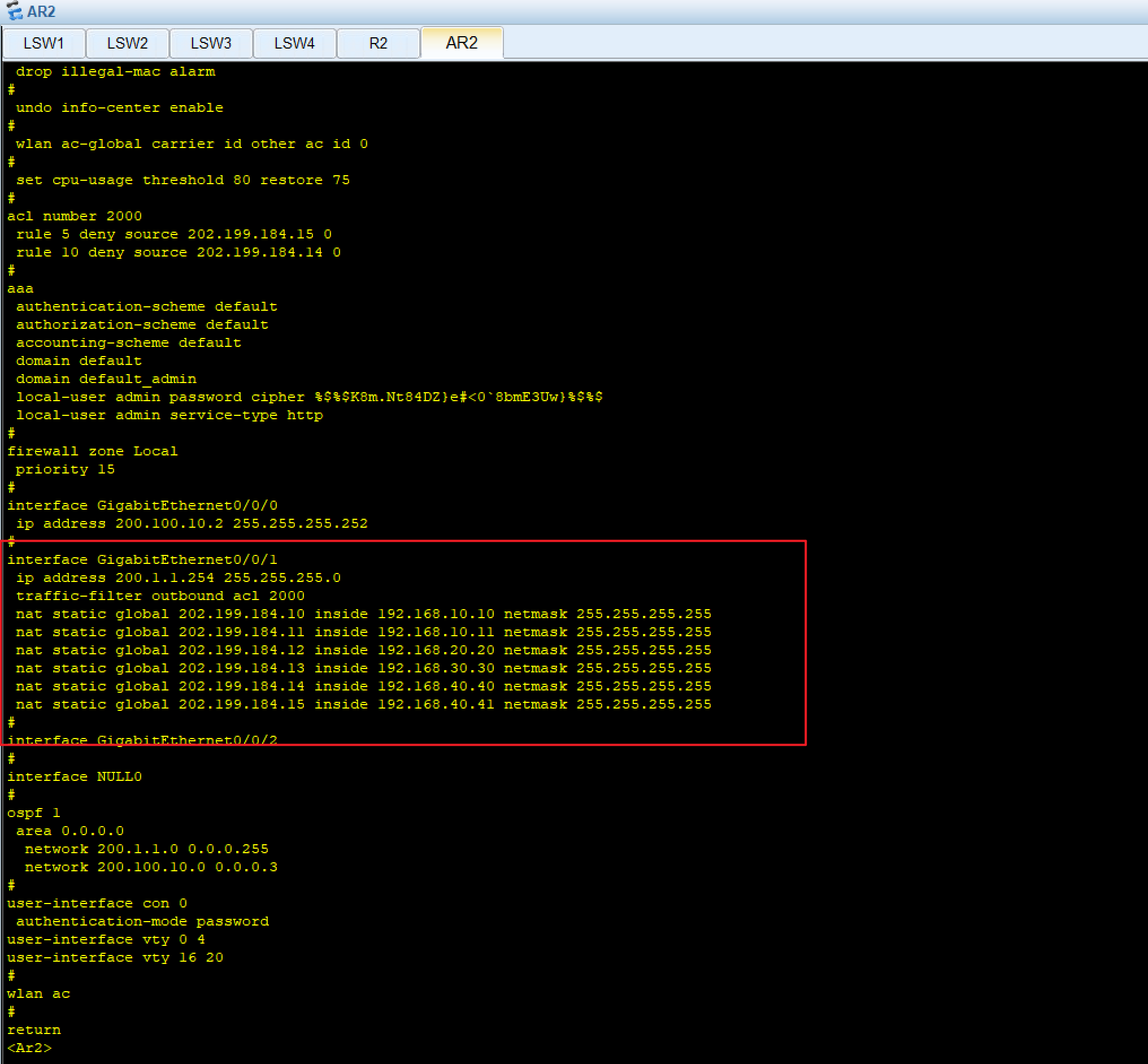


AR2：

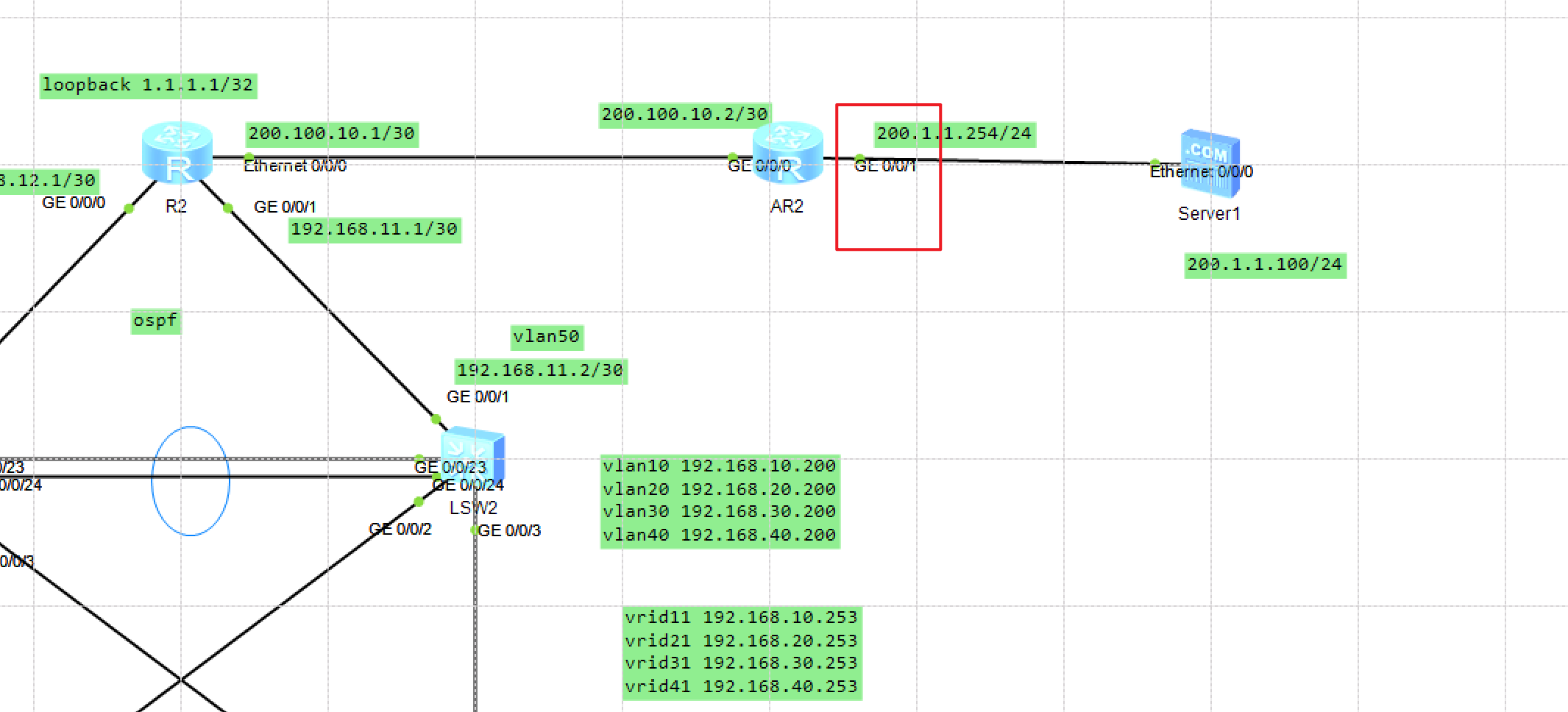


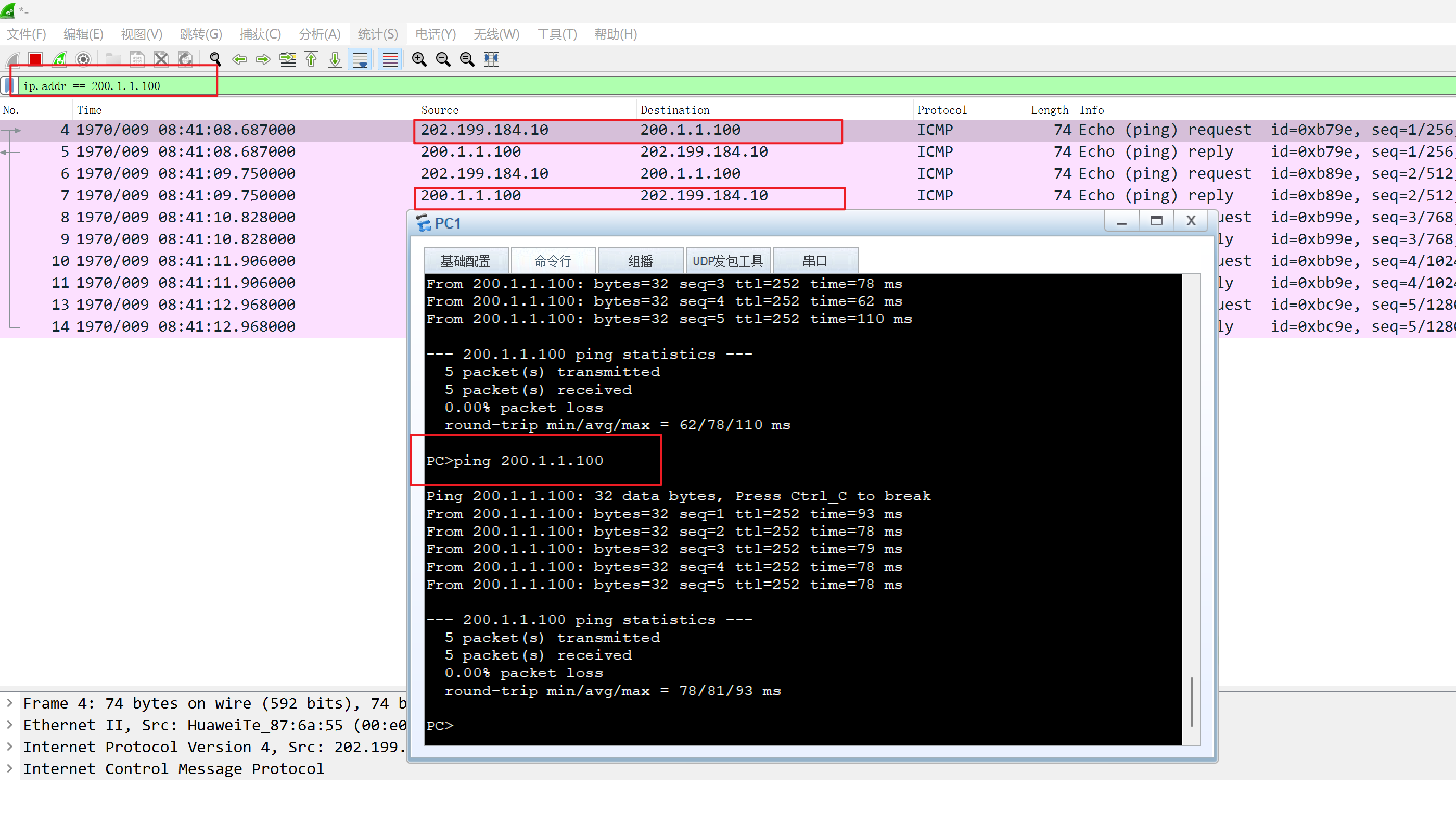
## 4.5 NAT地址转换测试结果

AR2：



当使用PC1（192.168.10.10）去ping服务器，在AR的0/0/1接口进行抓包：

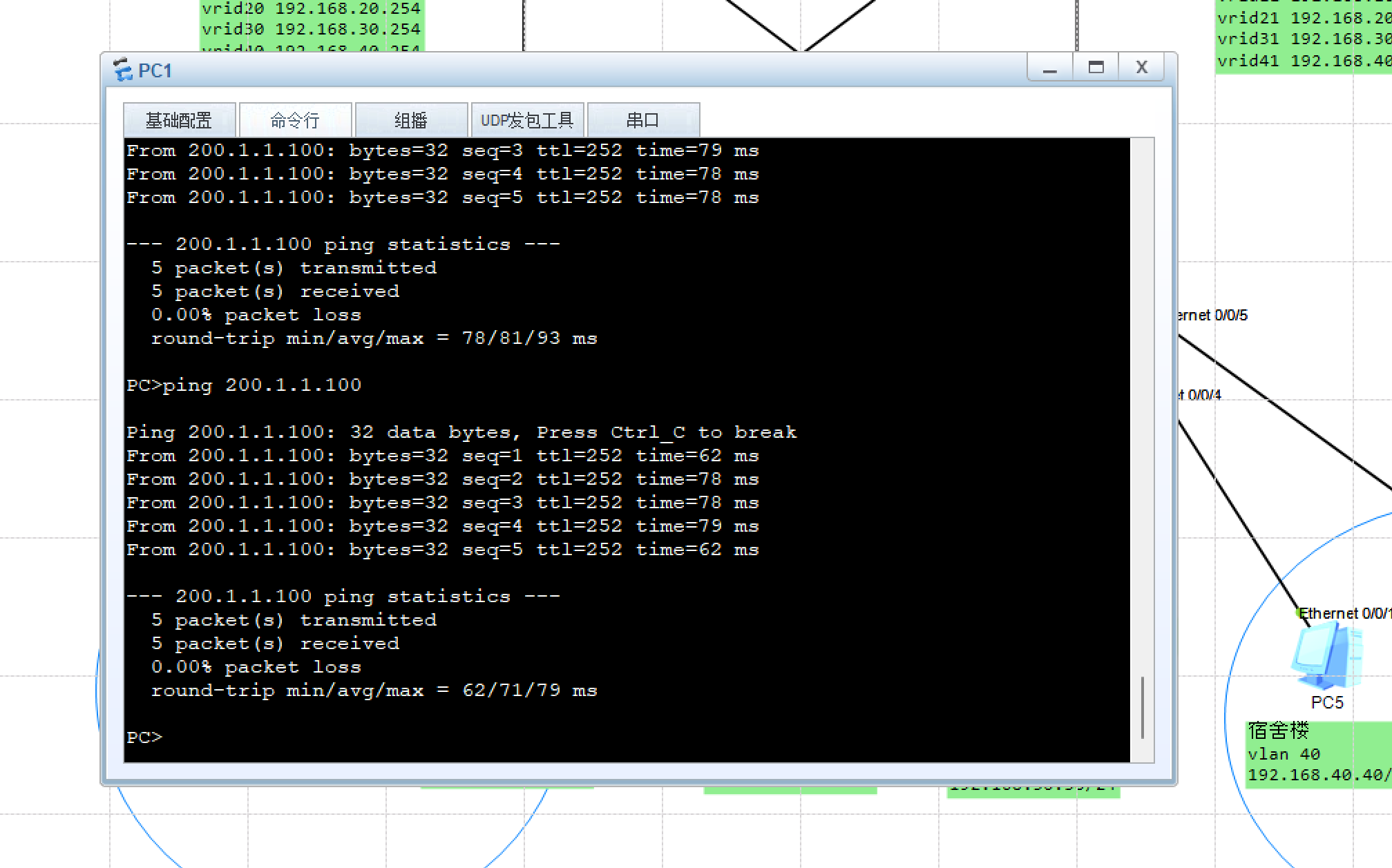




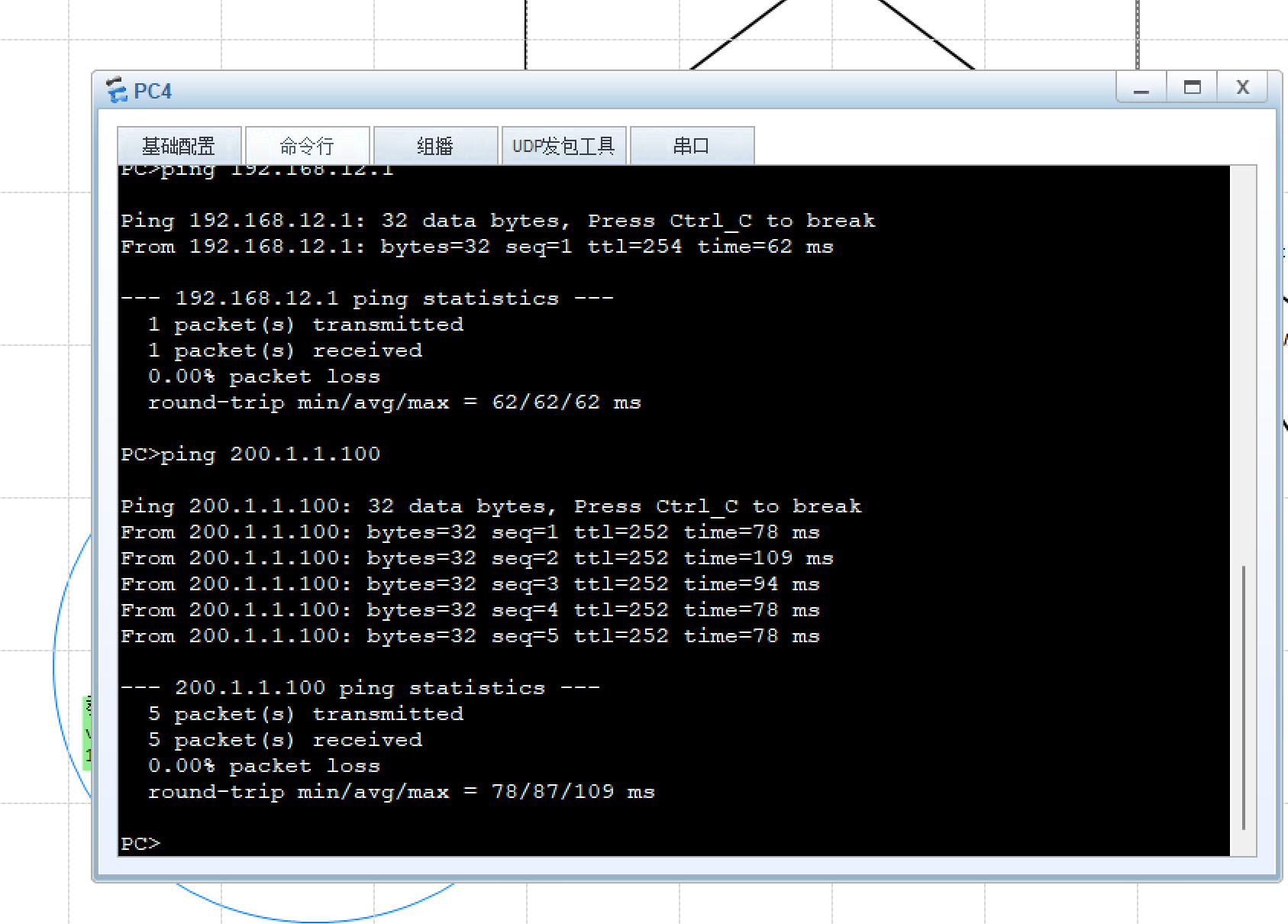
可以明显看出从1口出来的IP为202.199.184.10。已经转换成功。

## 4.6 访问控制列表测试结果

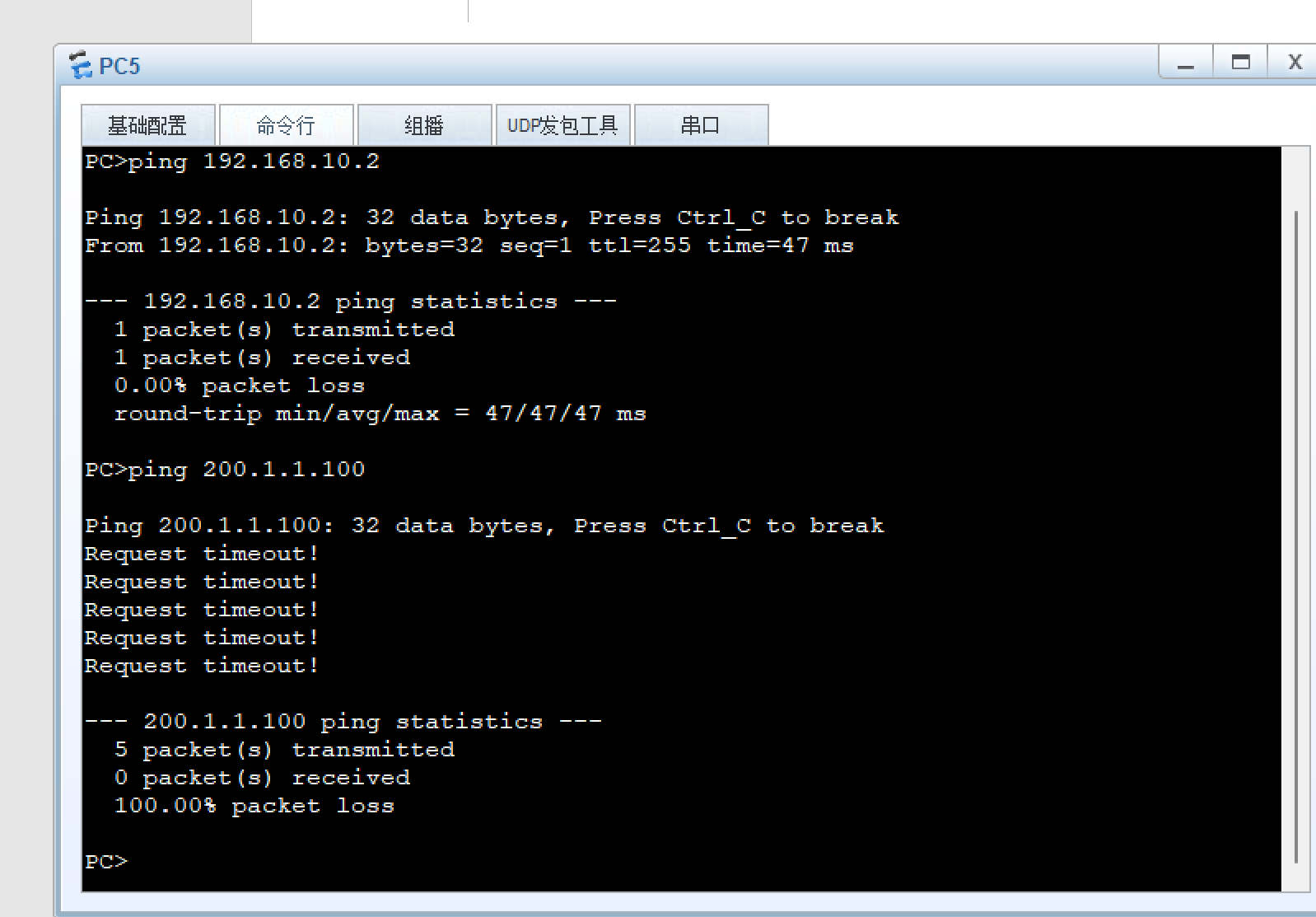
当使用PC1去访问服务器：



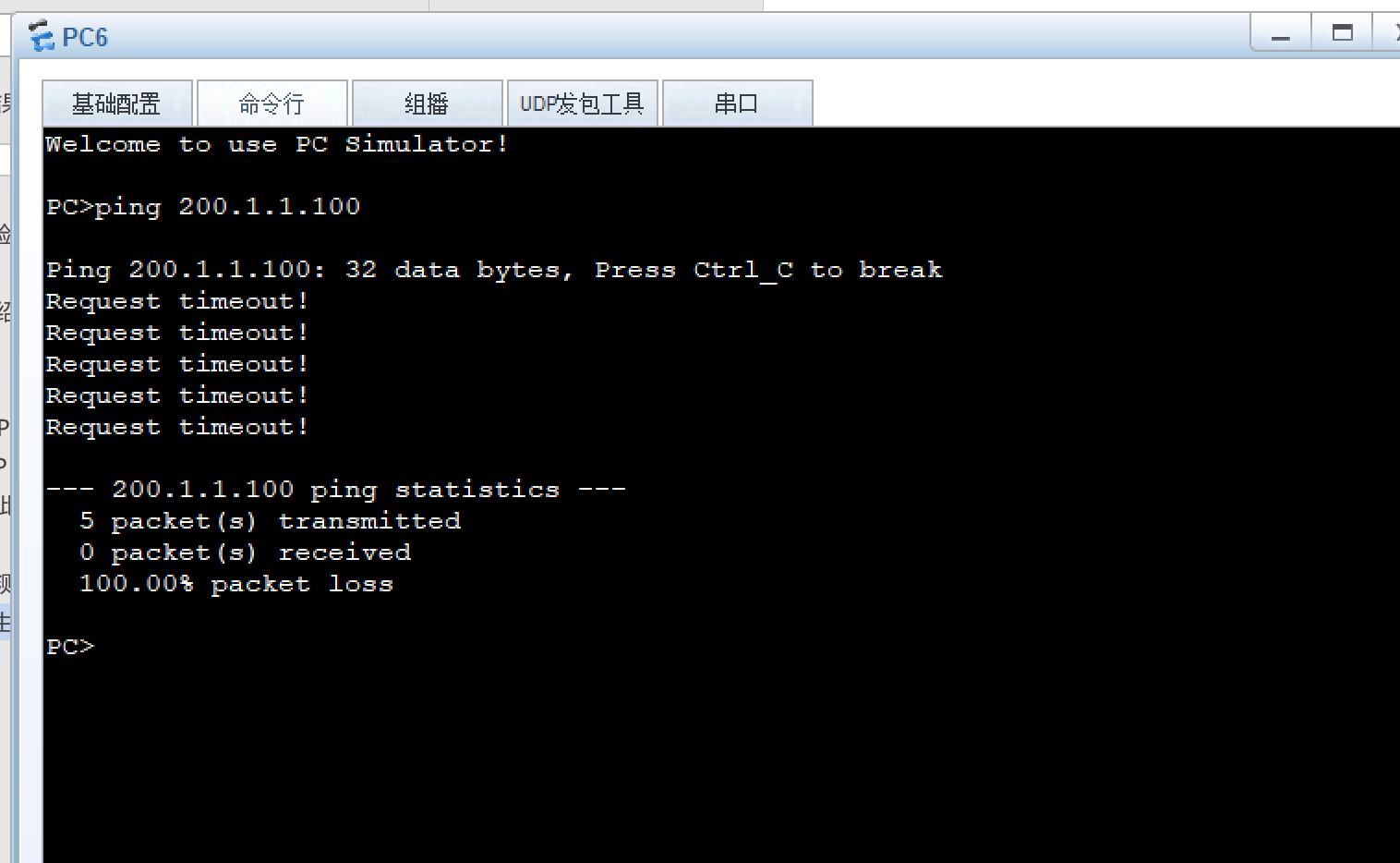
使用PC4去访问服务器：



使用PC5去访问服务器：



使用PC6访问服务器：



# 五、总结与收获

网络工程专业是我的第一志愿，从选择志愿的那一刻起，我就决定未来要从事和网络相关的工作，在本学期跟着这门课由浅至深的了解到了网络，同样也在本学期阅读了大量文章和文献。下面我就来总结一下本科三年级路由交换专业相关知识及收获。

路由交换我认为是我从入学以来学到的对于网络工程专业来说一门真正意义上的专业课。在局域网中通过划分Vlan将一个物理网络划分为多个逻辑上的网络，在路由器间通过数据线相连，但是一根数据线可能会导致线段网断，并且网络带宽也受到限制，因此可以通过配置链路聚合Eth-trunk，将两条甚至更多的物理上的数据线在逻辑上合并为一条，这样不仅可以增加网络带宽，也能提高网络的稳定性，提高容错率。

在早期小型的局域网中如学校、医院、企业，为了保证网络的可靠性和稳定性，也会使用STP生成树协议，使用STP不仅可以提高网络的稳定性，还能避免环路问题，避免广播风暴、MAC震荡等网络威胁。在STP网络中，交换机之间相互发送BPDU报文来动态选择根桥和备份桥，STP中包括根端口、指定端口、替代端口，端口状态还有五种：Blocking、Listening、Forwarding、Disabled，STP如果发生拓扑变化，将会重新发送BPDU，重新选择根桥等桥，这样的话就会引发新的问题，就是收敛速度，STP的状态太多了，每一种状态都有自己的时间。当发生变化时，则会等待非常多的时间，效率太低了，如果对于大型网络的话会严重影响工作效率。因此在未来又发明了RSTP，快速生成树协议。

RSTP收敛速度相对于STP得到了非常大的提升，虽然作为STP的升级版本，但是也兼容了STP协议。RSTP的端口角色分为：根端口、指定端口、备份端口、禁用端口，而端口状态相对于STP明显减少，三种状态分别为：Discarding、Learning、Forwarding。但是RSTP和STP都有一个致命的问题，他们都共享一颗树，如果时小型网络还好，但是对于大型网络，这显然不合理。因此，后来又发明了MSTP。

MSTP允许在网络中构建多个生成树实例，每个实例可以独立地进行计算和收敛。这样可以在保持网络稳定性的同时，提高网络的冗余性和可靠性。此外，MSTP还支持VLAN（虚拟局域网），使得不同VLAN的流量可以沿着不同的路径传输，提高了网络的灵活性和效率。

通过VRRP虚拟路由冗余协议加MSTP在网络中不仅可以增加网络的稳定性、负载均衡，在出现故障时也能及时转移路由器到备份路由器，在两个技术加在一起简直yyds。

前面都是学的交换机，后面后开始学路由器了，在网络中进行转发流量时经过的路由器，路由器可以将流量快速转发到另外一个网络中。当时在转发的时候会查看路由表，路由表又分为静态路由表和动态路由表，静态路由表需要用手一个一个打命令，在实际的网络中不会广泛运用，因为如果面对随时变化的网络来说不具有应对能力，需要管理员手动配置操作。动态路由表可以解决此问题，到那时动态路由表又分为RIP和OSPF，两个都是内部网关协议，RIP是基于路由向量，而OSPF是基于状态链路路由。RIP不适用于大型网络，而OSPF可以，OSPF可以将一个大的网络划分为几个小的区域。当在一个局域网中，流量要转发到外网时，还需要经过NAT和ACL控制。

使用NAT和ACL最大的好处就是在一定的程度上保证了网络安全，使用NAT将内网的IP映射到外网IP，在访问外网时不采用内网IP极大的保证了内网安全，而ACL就更不必说了，通过设置进出流量规则，从而限制内网机器访问外网或者限制外网访问内网。从传统上的网络安全来考虑，这些配置是远远不能够的，还需要加上防火墙、堡垒机、蜜罐、IPS、IDS，如果局域网有web应用还需要配置WAF。在未来我也会继续不忘初心、努力学习。

**《路由交换技术》考核A方案结课成绩表**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **学生姓名** | |  | **班级** |  | | **任课教师** | |  |
| **题目** | |  | | | | | | |
| **评分标准** | | | | | **总分** | | **得分** | |
| 结课报告评分指标 | 1.完成IP地址配置及链路聚合，并完成VLAN配置通信。 | | | | 15分 | |  | |
| 2.实现MSTP+VRRP多备份组。 | | | | 20分 | |  | |
| 3.完成OSPF协议配置。 | | | | 12分 | |  | |
| 4.完成NAT地址转换，并按要求完成访问控制列表配置。 | | | | 8分 | |  | |
| 5.项目报告撰写规范，总结与收获真实，有自己的体会和感悟。 | | | | 5分 | |  | |
| 实操 | 能在规定时间内完成实操演示，并操作熟练，结果正确。 | | | | 20分 | |  | |
| 答辩 | 能准确回答出老师提出的问题，且表述正确、流利。 | | | | 20分 | |  | |
|  | **合计** | | | |  | | | |
|  | 任课教师签字： 年 月 日 | | | | | | | |

注：1.评分标准栏应根据课程的不同进行适当的调整，包括评分标准选项的数量、内容、分值等；

2.评分标准要与考试审批中的评分标准保持一致；

3.该表由学生打印并填写抬头内容，装订在学生考试课材料的最后一页。