一、实验目的：

1. 将路由协议、交换机配置、VLAN规划等零散知识点整合到真实网络环境中，强化对网络协议原理的理解；
2. 通过复杂网络场景设计（如多网段互通、访问控制策略等），提升解决实际问题的能力
3. 以企业需求为导向，模拟公司网络架构（如分公司与总部的网络隔离、公网IP管理等），增强实际工作场景的适应性

二、实验场景：

某中小型企业A有三个部门，在企业的两栋办公楼中皆有分支：技术部(vlan 10)、商务部(vlan 20)和财务部(vlan 30)。每栋楼的主机与二层交换网络相连，且不同部门之间需要通过三层交换机互通，基于路由转发满足互访。企业有一台内部web服务器和文件FTP服务器，Web服务器承载着内部网站，方便员工了解公司的实时信息，两台服务器均连接三层交换机(vlan 40)。企业有一条专线通过企业路由器接到运营商提供的公共网络（接口地址：202.103.24.68/24），并从运营商获取到一个公有网络地址（202.103.24.50/24），满足企业员工访问互联网。局域网路由器启用静态路由。

三、实验要求：

a. 搭建拓扑网络，并为所有网络设备命名；

b.为三层交换机、公司路由器设置特权密码（以学号作为密码），启用远程访问登陆功能（以学号作为登录密码）；

c.配置各网元接口IP地址；

d.每栋楼的每个部门至少需要一台主机做代表；

e.二层交换机与三层交换机之间采用链路聚合（两个成员接口）；

f.在拓扑图上标注各网元的IP、中文名称，vlan名称等注释。

g.企业内部网络为10.0.XX.0/24（XX是学号后两位）其中技术部分配不多于60个主机地址，商务部分配不多于28个主机地址，财务部分配不多于12个主机地址。

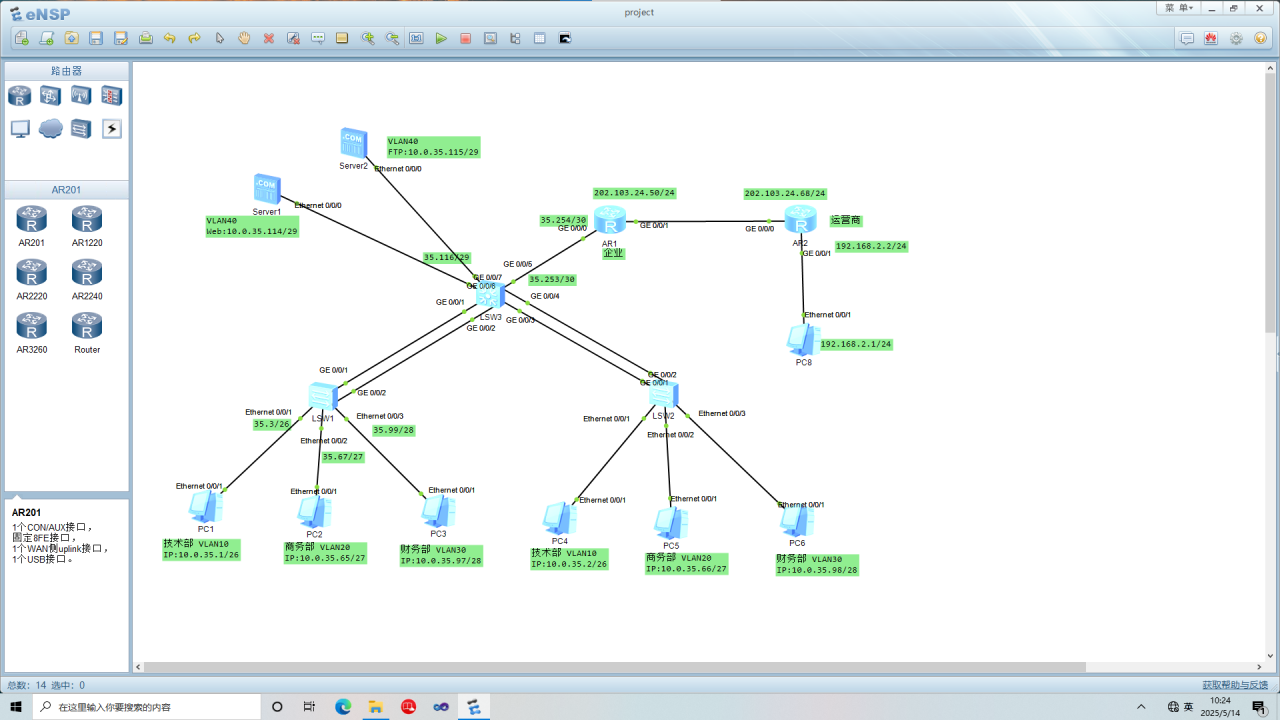
h.三层交换机与路由器之间、两台企业服务器均属于公司内部网络。要求基于VLSM技术，科学划分IP地址。

i.[VLAN]创建vlan 10、vlan 20、vlan 30、vlan 40使连接技术部门的接口归属vlan 10，连接商务部门的接口归属vlan 20，连接财务部的接口归属vlan 30，两服务器的连接口归属vlan 40

j.[路由配置]配置静态路由，使得全网互通（企业内部及外部）。在公司出口路由器上配置路由，下一跳指向运营商公网路由器地址202.103.24.68/24；

四、实验步骤

1. 实验拓扑图



1. 子网划分
2. 技术部（VLAN 10）

网段：10.0.35.0/26

可用地址：10.0.35.1/26 - 10.0.35.62/26

网关：10.0.35.3/26

1. 商务部（VLAN 20）

网段：10.0.35.64/27

可用地址：10.0.35.65/27 - 10.0.35.94/27

网关：10.0.35.67/27

1. 财务部（VLAN 30）

网段：10.0.35.96/28

可用地址：10.0.35.97/28 - 10.0.35.110/28

网关：10.0.35.99/28

1. 服务器（VLAN 40）

网段：10.0.35.112/29

可用地址：10.0.35.113/29 - 10.0.35.118/29

网关：10.0.35.116/29

1. 互联网（VLAN 50）

网段：10.0.35.252/30

可用地址：10.0.35.253/30 - 10.0.35.254/30

网关：企业路由器接口（10.0.35.254/30）

三层交换机接口（10.0.35.253/30）

1. 配置数据

<SW1>dis cu

#

sysname SW1

#

vlan batch 10 20 30 40

#

cluster enable

ntdp enable

ndp enable

#

drop illegal-mac alarm

#

diffserv domain default

#

drop-profile default

#

aaa

authentication-scheme default

authorization-scheme default

accounting-scheme default

domain default

domain default\_admin

local-user admin password simple admin

local-user admin service-type http

#

interface Vlanif1

#

interface Vlanif10

#

interface MEth0/0/1

#

interface Eth-Trunk1

port link-type trunk

port trunk allow-pass vlan 2 to 4094

#

interface Ethernet0/0/1

port link-type access

port default vlan 10

#

interface Ethernet0/0/2

port link-type access

port default vlan 20

#

interface Ethernet0/0/3

port link-type access

port default vlan 30

#

interface Ethernet0/0/4

#

interface Ethernet0/0/5

#

interface Ethernet0/0/6

#

interface Ethernet0/0/7

#

interface Ethernet0/0/8

#

interface Ethernet0/0/9

#

interface Ethernet0/0/10

#

interface Ethernet0/0/11

#

interface Ethernet0/0/12

#

interface Ethernet0/0/13

#

interface Ethernet0/0/14

#

interface Ethernet0/0/15

#

interface Ethernet0/0/16

#

interface Ethernet0/0/17

#

interface Ethernet0/0/18

#

interface Ethernet0/0/19

#

interface Ethernet0/0/20

#

interface Ethernet0/0/21

#

interface Ethernet0/0/22

#

interface GigabitEthernet0/0/1

eth-trunk 1

#

interface GigabitEthernet0/0/2

eth-trunk 1

#

interface NULL0

#

ip route-static 10.0.35.112 255.255.255.248 10.0.35.116

#

user-interface con 0

user-interface vty 0 4

#

Return

<SW2>dis cu

#

sysname SW2

#

vlan batch 10 20 30 40

#

cluster enable

ntdp enable

ndp enable

#

drop illegal-mac alarm

#

diffserv domain default

#

drop-profile default

#

aaa

authentication-scheme default

authorization-scheme default

accounting-scheme default

domain default

domain default\_admin

local-user admin password simple admin

local-user admin service-type http

#

interface Vlanif1

#

interface MEth0/0/1

#

interface Eth-Trunk2

port link-type trunk

port trunk allow-pass vlan 2 to 4094

#

interface Ethernet0/0/1

port link-type access

port default vlan 10

#

interface Ethernet0/0/2

port link-type access

port default vlan 20

#

interface Ethernet0/0/3

port link-type access

port default vlan 30

#

interface Ethernet0/0/4

#

interface Ethernet0/0/5

#

interface Ethernet0/0/6

#

interface Ethernet0/0/7

#

interface Ethernet0/0/8

#

interface Ethernet0/0/9

#

interface Ethernet0/0/10

#

interface Ethernet0/0/11

#

interface Ethernet0/0/12

#

interface Ethernet0/0/13

#

interface Ethernet0/0/14

#

interface Ethernet0/0/15

#

interface Ethernet0/0/16

#

interface Ethernet0/0/17

#

interface Ethernet0/0/18

#

interface Ethernet0/0/19

#

interface Ethernet0/0/20

#

interface Ethernet0/0/21

#

interface Ethernet0/0/22

#

interface GigabitEthernet0/0/1

eth-trunk 2

#

interface GigabitEthernet0/0/2

eth-trunk 2

#

interface NULL0

#

user-interface con 0

user-interface vty 0 4

#

port-group trunk

#

Return

<SW3>dis cu

#

sysname SW3

#

vlan batch 10 20 30 40 50

#

cluster enable

ntdp enable

ndp enable

#

undo nap slave enable

#

drop illegal-mac alarm

#

diffserv domain default

#

drop-profile default

#

aaa

authentication-scheme default

authorization-scheme default

accounting-scheme default

domain default

domain default\_admin

local-user admin password simple admin

local-user admin service-type http

#

interface Vlanif1

#

interface Vlanif10

ip address 10.0.35.3 255.255.255.192

#

interface Vlanif20

ip address 10.0.35.67 255.255.255.224

#

interface Vlanif30

ip address 10.0.35.99 255.255.255.240

#

interface Vlanif40

ip address 10.0.35.116 255.255.255.248

#

interface Vlanif50

ip address 10.0.35.253 255.255.255.252

#

interface MEth0/0/1

#

interface Eth-Trunk1

port link-type trunk

port trunk allow-pass vlan 2 to 4094

#

interface Eth-Trunk2

port link-type trunk

port trunk allow-pass vlan 2 to 4094

#

interface GigabitEthernet0/0/1

eth-trunk 1

#

interface GigabitEthernet0/0/2

eth-trunk 1

#

interface GigabitEthernet0/0/3

eth-trunk 2

#

interface GigabitEthernet0/0/4

eth-trunk 2

#

interface GigabitEthernet0/0/5

port link-type access

port default vlan 50

#

interface GigabitEthernet0/0/6

port link-type access

port default vlan 40

#

interface GigabitEthernet0/0/7

port link-type access

port default vlan 40

#

interface GigabitEthernet0/0/8

#

interface GigabitEthernet0/0/9

#

interface GigabitEthernet0/0/10

#

interface GigabitEthernet0/0/11

#

interface GigabitEthernet0/0/12

#

interface GigabitEthernet0/0/13

#

interface GigabitEthernet0/0/14

#

interface GigabitEthernet0/0/15

#

interface GigabitEthernet0/0/16

#.

interface GigabitEthernet0/0/17

#

interface GigabitEthernet0/0/18

#

interface GigabitEthernet0/0/19

#

interface GigabitEthernet0/0/20

#

interface GigabitEthernet0/0/21

#

interface GigabitEthernet0/0/22

#

interface GigabitEthernet0/0/23

#

interface GigabitEthernet0/0/24

#

interface NULL0

#

ip route-static 0.0.0.0 0.0.0.0 10.0.35.254

ip route-static 202.103.24.0 255.255.255.0 10.0.35.254

#

user-interface con 0

user-interface vty 0 4

user privilege level 15

set authentication password simple 20221023135

#

port-group default

#

Return

<AR1>dis cu

[V200R003C00]

#

sysname AR1

#

snmp-agent local-engineid 800007DB03000000000000

snmp-agent

#

clock timezone China-Standard-Time minus 08:00:00

#

portal local-server load flash:/portalpage.zip

#

drop illegal-mac alarm

#

wlan ac-global carrier id other ac id 0

#

set cpu-usage threshold 80 restore 75

#

aaa

authentication-scheme default

authorization-scheme default

accounting-scheme default

domain default

domain default\_admin

local-user admin password cipher %$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$

local-user admin service-type http

#

firewall zone Local

priority 15

#

interface GigabitEthernet0/0/0

ip address 10.0.35.254 255.255.255.252

#

interface GigabitEthernet0/0/1

ip address 202.103.24.50 255.255.255.0

#

interface GigabitEthernet0/0/2

#

interface NULL0

#

ip route-static 0.0.0.0 0.0.0.0 202.103.24.68

ip route-static 10.0.35.0 255.255.255.192 10.0.35.253

ip route-static 10.0.35.64 255.255.255.224 10.0.35.253

ip route-static 10.0.35.96 255.255.255.240 10.0.35.253

ip route-static 10.0.35.112 255.255.255.248 10.0.35.253

#

user-interface con 0

authentication-mode password

user-interface vty 0 4

authentication-mode password

user privilege level 15

set authentication password cipher %$%$QjY>PDIyAZ]OHBTJ;0/5,"`[X\hBU>-$e)`huhI8

op[#"`^,%$%$

user-interface vty 16 20

#

wlan ac

#

Return

<AR2>dis cu

[V200R003C00]

#

sysname AR2

#

snmp-agent local-engineid 800007DB03000000000000

snmp-agent

#

clock timezone China-Standard-Time minus 08:00:00

#

portal local-server load flash:/portalpage.zip

#

drop illegal-mac alarm

#

wlan ac-global carrier id other ac id 0

#

set cpu-usage threshold 80 restore 75

#

aaa

authentication-scheme default

authorization-scheme default

accounting-scheme default

domain default

domain default\_admin

local-user admin password cipher %$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$

local-user admin service-type http

#

firewall zone Local

priority 15

#

interface GigabitEthernet0/0/0

ip address 202.103.24.68 255.255.255.0

#

interface GigabitEthernet0/0/1

ip address 192.168.2.2 255.255.255.0

#

interface GigabitEthernet0/0/2

#

interface NULL0

#

ip route-static 10.0.35.0 255.255.255.192 202.103.24.50

ip route-static 10.0.35.64 255.255.255.224 202.103.24.50

ip route-static 10.0.35.96 255.255.255.240 202.103.24.50

ip route-static 10.0.35.112 255.255.255.248 202.103.24.50

ip route-static 10.0.35.252 255.255.255.252 202.103.24.50

#

user-interface con 0

authentication-mode password

user-interface vty 0 4

user-interface vty 16 20

#

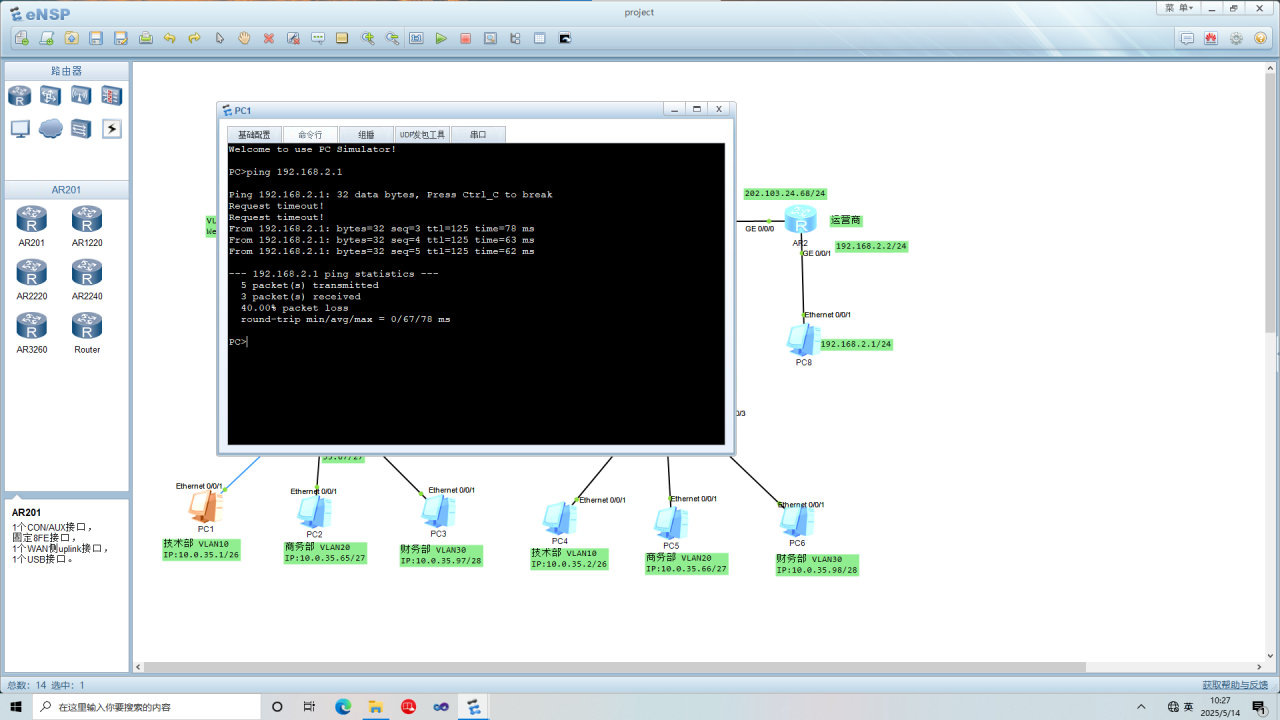
wlan ac

#

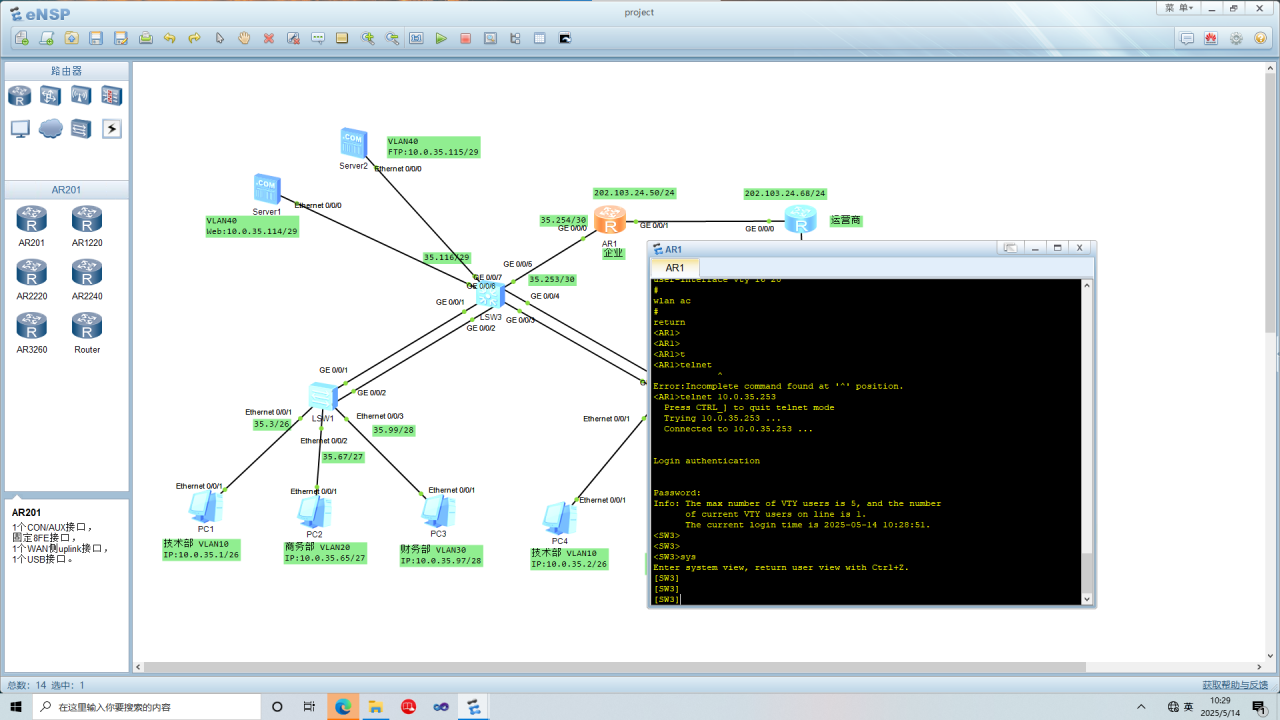
return

1. 实验测试

Ping测试：



远程登陆测试：



1. 实验总结

本实验围绕某中小型企业网络搭建展开，基于华为eNSP平台完成宽带接入技术的综合实验配置。通过本次实验，我深入理解了企业级网络架构的规划与配置流程。子网划分部分让我掌握了VLSM技术的核心，根据部门需求精准分配IP地址，例如服务器采用/29掩码而不使用/28掩码，避免了IP地址的浪费。VLAN的创建与接口绑定实现了网络的隔离，有效控制广播域，提升网络安全性。在静态路由配置中，通过手动指定路由条目，明确了数据的流向，尤其在不允许使用默认路由时，需要逐条配置路由，确保互通。这部分让我对路由表的作用有了更加直观的认识。此外，三层交换机通过VLAN接口实现跨网段通信，解决了物理接口无法直接配置IP的限制，体现了三层交换机的核心优势。在静态路由的配置过程中，因为忽略了外网IP的不确定性，导致静态路由配置出现了一些小问题。在老师的提醒下，我迅速修改了静态路由的目的网段，确保公司员工可以访问任意外网地址。本次实验将理论转化为实践，强化了综合问题分析与解决能力，同时深化了对企业网络架构设计的理解，为后续复杂网络场景的实践奠定了基础。