**重庆城南职业学校**

**网**

**络**

**规**

**划**

**与**

**设**

**计**

目录

[一、 项目介绍 1](#_Toc100492479)

[二、 需求分析 1](#_Toc100492480)

[三、 规划设计 2](#_Toc100492481)

[1 网络拓扑规划 2](#_Toc100492482)

[2 技术方案规划 2](#_Toc100492483)

[3 IP地址规划 3](#_Toc100492484)

[四、 配置实施 4](#_Toc100492485)

[4.1. 数据中心区域 4](#_Toc100492486)

[4.1.1防火墙FW2 4](#_Toc100492487)

[4.1.2核心Core3 5](#_Toc100492488)

[4.2. 核心区域 6](#_Toc100492489)

[4.2.1路由器R1 6](#_Toc100492490)

[4.2.2防火墙FW1 6](#_Toc100492491)

[4.2.3核心交换机1 7](#_Toc100492492)

[4.2.4核心交换机2 11](#_Toc100492493)

[4.2.5无线AC： 13](#_Toc100492494)

[4.3. A区 14](#_Toc100492495)

[4.3.1汇聚交换机 14](#_Toc100492496)

[4.3.2接入交换机 15](#_Toc100492497)

[4.3.3无线POE交换机 16](#_Toc100492498)

[4.4. B区 16](#_Toc100492499)

[4.4.1汇聚交换机 16](#_Toc100492500)

[4.4.2接入交换机 16](#_Toc100492501)

[4.4.3无线POE交换机 17](#_Toc100492502)

[五、 验证测试 18](#_Toc100492503)

[5.1访问数据中心服务器测试 18](#_Toc100492504)

[5.2无线网络测试 19](#_Toc100492505)

[5.3访问互联网测试 20](#_Toc100492506)

# 项目介绍

重庆城南职业学校，该学校办校多年，校内网络设施已十分老旧，再加上招生数量的增加导致校内办公楼需要另外增加部署，学校需要对其网络进行升级。为了给学生们一个良好的学习环境，其网络规划与设计显得十分重要，而一个安全的网络的关键在于拥有一个良好的网络组建规划 ，为使校园网络应用得更加安全和顺畅 ，现需要对学校的整体网络进行重新设计规划建设。

# 需求分析

目前城南职业学院整体分为A区和B区。以A区、B区为网络汇聚节点，办公楼、教学楼、宿舍楼、财务处为接入节点。网络规划设计需要采用三层架构，核心、汇聚等重要节点需要安全、冗余，避免单点故障发生。校园网整体网络需要连接到互联网，为保障校园网网络安全，需要对校园网内部网络进行安全防护。由于现今移动终端办公设备很多，学校部分区域还需要进行无线网络覆盖。

学校内部有WEB、DNS、教学管理等应用系统服务器，这些服务器需要规划设计部署到专业的网络数据中心区域，并对其进行安全防护。

分析网络建设整体需求具体如下：

1. 网络整体建设按照功能需求与物理区域采用分层设计，分为核心层、汇聚层、接入层与网络数据中心。
2. 核心层采用双机冗余结构，使用VRRP热备路由协议进行双机实时热备，再使用MSTP生产树协议与汇聚层进行双链路连接，实现网络骨干区域的安全冗余。
3. 所有服务器等应用系统全部部署到网络数据中心区域，并需要对其做网络安全防护。
4. 在校园网与互联网边界使用防火墙进行安全隔离，为保障学校校园网网络安全，设置只允许校园网访问互联网，禁止互联网访问校园网。
5. 在教学楼等区域进行无线网络覆盖，网络建设采用企业WLAN方式，所有无线AP由AC控制器统一管理，使用同一个SSID无线信号，实现无线网络自动漫游。
6. 校园网内部所有区域要求能够相互访问。

# 规划设计

## 网络拓扑规划

根据学校校园网网络建设需求，整体区域分为数据中心、A区、B区与核心区域，具体网络拓扑·规划如下：

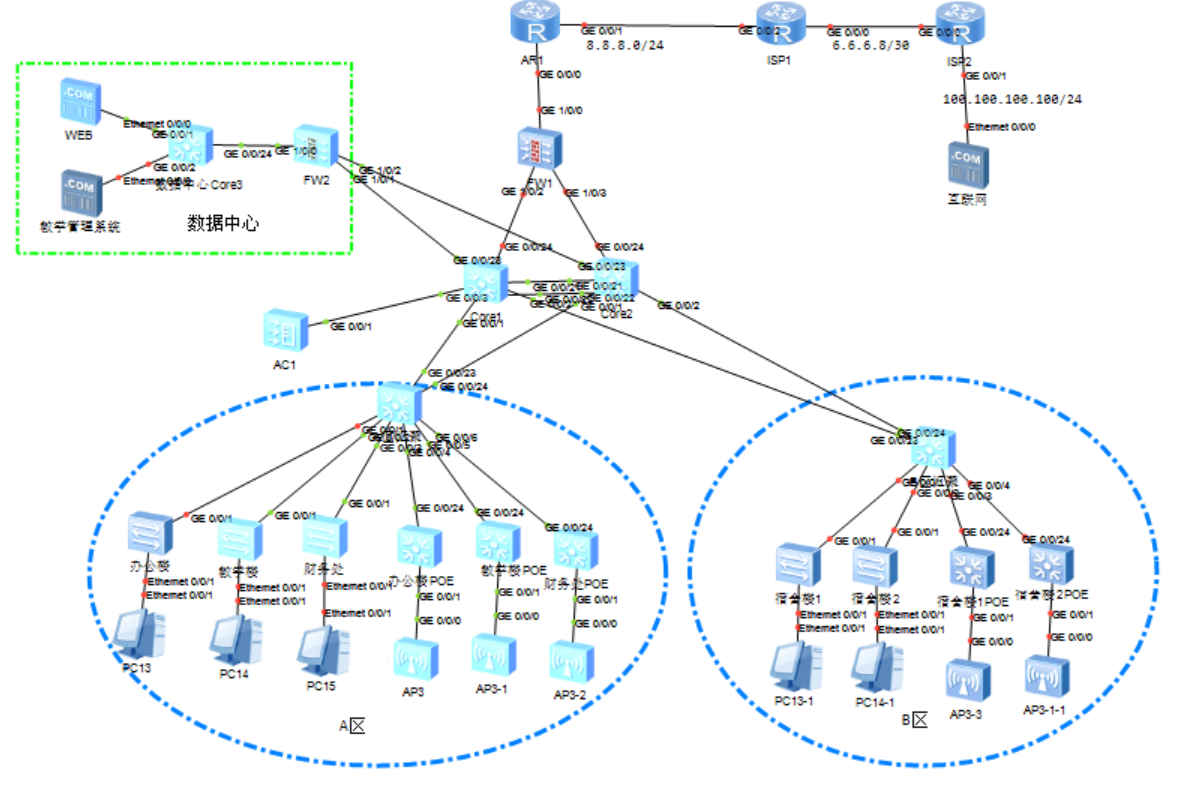


图3-1 网络规划拓扑图

## 技术方案规划

1. 核心层有主备核心，设计在主备核心之间使用VRRP技术，接入层设备分别连接到主备核心，运行MSTP生产树协议防止产生网络环路形成广播风暴。
2. 核心层与数据中心、外网防火墙、路由器之间使用OSPF动态路由协议。总校区与分校区通过隧道连接后也使用OSPF动态路由进行通信。
3. 使用防火墙划将总校区划分成Trust与untrust区域，校园网为Trust区域，外网为Untrust区域，为保障校园网网络信息安全，校园网可以访问外网，外网不能访问校园网。
4. 办公楼、教学楼、财务、宿舍、无线等每个区域使用一个独立的IP网段，每个网段对应一个独立的VLAN。

## IP地址规划

根据学校规模，规划在学校使用172.16.0.0/16的IP网段，再划分成/24位的子网，每个子网使用最后一个172.\*.\*.254的IP地址作为本网段的通信网关。IP地址具体规划如下：

**1）业务IP地址规划：**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **IP** | **子网掩码** | **VLAN** | **网关** | **备注** |
| 1 | 办公楼 | 172.16.1.0 | 255.255.255.0 | 1 | 172.16.1.254 |  |
| 2 | 教学楼 | 172.16.2.0 | 255.255.255.0 | 2 | 172.16.2.254 |  |
| 3 | 财务处 | 172.16.3.0 | 255.255.255.0 | 3 | 172.16.3.254 |  |
| 4 | 宿舍楼1 | 172.16.4.0 | 255.255.255.0 | 4 | 172.16.4.254 |  |
| 5 | 宿舍楼2 | 172.16.5.0 | 255.255.255.0 | 5 | 172.16.5.254 |  |
| 6 | 无线 | 172.16.6.0 | 255.255.255.0 | 6 | 172.16.6.254 |  |
| 7 | AP管理 | 172.16.7.0 | 255.255.255.0 | 7 | 172.16.7.254 |  |
| 8 | 数据中心 | 172.16.100.0 | 255.255.255.0 | 100 | 172.16.100.254 |  |

**表3-1 校园网业务IP规划**

**2）接口IP地址规划：**

路由器、防火墙、核心交换机、数据中心之间运行OSPF动态路由，这些网络设备需要配置用于OSPF通信的接口IP地址，接口IP地址具体规划如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **名称** | **接口** | **IP** | **名称** | **接口** | **IP** |
| Core3 | GE0/0/24(VLAN200） | 172.16.200.1/30 | FW2 | GE1/0/0 | 172.16.200.2/30 |
| AR1 | GE0/0/0 | 172.16.200.5/30 | FW1 | GE1/0/0 | 172.16.200.6/30 |
| FW1 | GE1/0/1 | 172.16.200.9/30 | Core1 | GE0/0/24(VLAN200） | 172.16.200.10/30 |
| FW1 | GE1/0/2 | 172.16.200.13/30 | Core2 | GE0/0/24(VLAN200） | 172.16.200.14/30 |
| Core1 | GE0/0/23(VLAN201） | 172.16.200.17/30 | FW2 | GE1/0/1 | 172.16.200.18/30 |
| Core2 | GE0/0/23(VLAN201） | 172.16.200.21/30 | FW2 | GE1/0/2 | 172.16.200.22/30 |

# 配置实施

网络模拟测试使用华为ENSP模拟器对网络进行模拟仿真配置，各个网络设备具体配置如下：

## 数据中心区域

### 4.1.1防火墙FW2

interface GigabitEthernet1/0/0

undo shutdown

ip address 172.16.200.2 255.255.255.252

service-manage all permit

quit

interface GigabitEthernet1/0/1

undo shutdown

ip address 172.16.200.18 255.255.255.252

service-manage all permit

quit

interface GigabitEthernet1/0/2

undo shutdown

ip address 172.16.200.22 255.255.255.252

service-manage all permit

quit

firewall zone trust

add interface GigabitEthernet1/0/0

quit

firewall zone untrust

add interface GigabitEthernet1/0/1

add interface GigabitEthernet1/0/2

quit

ip route-static 0.0.0.0 0.0.0.0 172.16.200.5

ospf 1

area 0.0.0.0

network 172.16.200.0 0.0.0.3

network 172.16.200.16 0.0.0.3

network 172.16.200.20 0.0.0.3

quit

quit

security-policy

rule name 1

source-zone trust

destination-zone untrust

action permit

rule name 2

source-zone untrust

destination-zone trust

source-address 172.16.0.0 mask 255.255.0.0

action permit

rule name 3

source-zone local

action permit

rule name 4

destination-zone local

action permit

quit

quit

### 4.1.2核心Core3

sysname Core3

vlan 200

vlan 100

interface Vlanif200

ip address 172.16.200.1 255.255.255.252

quit

interface Vlanif100

ip address 172.16.100.254 255.255.255.0

quit

interface GigabitEthernet0/0/24

port link-type access

port default vlan 200

quit

port-group 1

group-member GigabitEthernet 0/0/1 to GigabitEthernet 0/0/22

port link-type access

port default vlan 100

quit

ospf 1

area 0.0.0.0

network 172.16.200.0 0.0.0.3

network 172.16.100.0 0.0.0.255

quit

quit

ip route-static 0.0.0.0 0.0.0.0 172.16.200.5

## 核心区域

### 4.2.1路由器R1

sysname AR1

interface GigabitEthernet0/0/1

ip address 8.8.8.2 255.255.255.0

quit

interface GigabitEthernet0/0/0

ip address 172.16.200.5 255.255.255.252

quit

ip route-static 0.0.0.0 0 8.8.8.1

ospf 1

area 0.0.0.0

network 172.16.200.4 0.0.0.3

quit

quit

acl number 3001

rule 1 permit ip

quit

interface GigabitEthernet0/0/1

nat outbound 3001

quit

### 4.2.2防火墙FW1

interface GigabitEthernet1/0/0

undo shutdown

ip address 172.16.200.6 255.255.255.252

service-manage all permit

quit

interface GigabitEthernet1/0/2

undo shutdown

ip address 172.16.200.9 255.255.255.252

service-manage all permit

quit

interface GigabitEthernet1/0/3

undo shutdown

ip address 172.16.200.13 255.255.255.252

service-manage all permit

quit

firewall zone trust

add interface GigabitEthernet1/0/2

add interface GigabitEthernet1/0/3

quit

firewall zone untrust

add interface GigabitEthernet1/0/0

quit

ip route-static 0.0.0.0 0.0.0.0 172.16.200.5

ospf 1

area 0.0.0.0

network 172.16.200.4 0.0.0.3

network 172.16.200.8 0.0.0.3

network 172.16.200.12 0.0.0.3

quit

quit

security-policy

rule name 1

source-zone trust

destination-zone untrust

action permit

rule name 2

source-zone untrust

destination-zone trust

action deny

rule name 3

source-zone local

action permit

rule name 4

destination-zone local

action permit

quit

quit

### 4.2.3核心交换机1

sysname Core1

vlan 200

vlan 201

vlan batch 2 to 7

interface Vlanif200

ip address 172.16.200.10 255.255.255.252

quit

interface Vlanif201

ip address 172.16.200.17 255.255.255.252

quit

interface GigabitEthernet0/0/23

port link-type access

port default vlan 201

quit

interface GigabitEthernet0/0/24

port link-type access

port default vlan 200

quit

interface Vlanif1

ip address 172.16.1.252 255.255.255.0

vrrp vrid 1 virtual-ip 172.16.1.254

vrrp vrid 1 priority 180

quit

interface Vlanif2

ip address 172.16.2.252 255.255.255.0

vrrp vrid 2 virtual-ip 172.16.2.254

vrrp vrid 2 priority 180

quit

interface Vlanif3

ip address 172.16.3.252 255.255.255.0

vrrp vrid 3 virtual-ip 172.16.3.254

vrrp vrid 3 priority 180

quit

interface Vlanif4

ip address 172.16.4.252 255.255.255.0

vrrp vrid 4 virtual-ip 172.16.4.254

vrrp vrid 4 priority 180

quit

interface Vlanif5

ip address 172.16.5.252 255.255.255.0

vrrp vrid 5 virtual-ip 172.16.5.254

vrrp vrid 5 priority 180

quit

interface Vlanif6

ip address 172.16.6.252 255.255.255.0

vrrp vrid 6 virtual-ip 172.16.6.254

vrrp vrid 6 priority 180

quit

interface Vlanif7

ip address 172.16.7.252 255.255.255.0

vrrp vrid 7 virtual-ip 172.16.7.254

vrrp vrid 7 priority 180

quit

ospf 1

area 0.0.0.0

network 172.16.200.10 0.0.0.3

network 172.16.200.16 0.0.0.3

network 172.16.1.0 0.0.0.255

network 172.16.2.0 0.0.0.255

network 172.16.3.0 0.0.0.255

network 172.16.4.0 0.0.0.255

network 172.16.5.0 0.0.0.255

network 172.16.6.0 0.0.0.255

network 172.16.7.0 0.0.0.255

quit

quit

ip route-static 0.0.0.0 0.0.0.0 172.16.200.5

dhcp enable

ip pool vlan1

gateway-list 172.16.1.254

network 172.16.1.0 mask 255.255.255.0

dns-list 114.114.114.114 8.8.8.8

excluded-ip-address 172.16.1.250 172.16.1.253

quit

ip pool vlan2

gateway-list 172.16.2.254

network 172.16.2.0 mask 255.255.255.0

dns-list 114.114.114.114 8.8.8.8

excluded-ip-address 172.16.2.250 172.16.2.253

quit

ip pool vlan3

gateway-list 172.16.3.254

network 172.16.3.0 mask 255.255.255.0

dns-list 114.114.114.114 8.8.8.8

excluded-ip-address 172.16.3.250 172.16.3.253

quit

ip pool vlan4

gateway-list 172.16.4.254

network 172.16.4.0 mask 255.255.255.0

dns-list 114.114.114.114 8.8.8.8

excluded-ip-address 172.16.4.250 172.16.4.253

quit

ip pool vlan5

gateway-list 172.16.5.254

network 172.16.5.0 mask 255.255.255.0

dns-list 114.114.114.114 8.8.8.8

excluded-ip-address 172.16.5.250 172.16.5.253

quit

ip pool vlan6

gateway-list 172.16.6.254

network 172.16.6.0 mask 255.255.255.0

dns-list 114.114.114.114 8.8.8.8

excluded-ip-address 172.16.6.250 172.16.6.253

quit

ip pool vlan7

gateway-list 172.16.7.254

network 172.16.7.0 mask 255.255.255.0

dns-list 114.114.114.114 8.8.8.8

excluded-ip-address 172.16.7.250 172.16.7.253

quit

interface Vlanif1

dhcp select global

quit

interface Vlanif2

dhcp select global

quit

interface Vlanif3

dhcp select global

quit

interface Vlanif4

dhcp select global

quit

interface Vlanif5

dhcp select global

quit

interface Vlanif6

dhcp select global

quit

interface Vlanif7

dhcp select global

quit

interface Eth-Trunk1

port link-type trunk

port trunk allow-pass vlan 1 to 7

quit

interface GigabitEthernet0/0/21

eth-trunk 1

quit

interface GigabitEthernet0/0/22

eth-trunk 1

quit

stp root primary

port-group 1

group-member GigabitEthernet 0/0/1 to GigabitEthernet 0/0/10

port link-type trunk

port trunk allow-pass vlan 2 to 7

quit

### 4.2.4核心交换机2

sysname Core2

vlan 200

vlan 201

vlan batch 2 to 7

interface Vlanif200

ip address 172.16.200.18 255.255.255.252

quit

interface Vlanif201

ip address 172.16.200.21 255.255.255.252

quit

interface GigabitEthernet0/0/23

port link-type access

port default vlan 201

quit

interface GigabitEthernet0/0/24

port link-type access

port default vlan 200

quit

interface Vlanif1

ip address 172.16.1.253 255.255.255.0

vrrp vrid 1 virtual-ip 172.16.1.254

vrrp vrid 1 priority 80

quit

interface Vlanif2

ip address 172.16.2.253 255.255.255.0

vrrp vrid 2 virtual-ip 172.16.2.254

vrrp vrid 2 priority 80

quit

interface Vlanif3

ip address 172.16.3.253 255.255.255.0

vrrp vrid 3 virtual-ip 172.16.3.254

vrrp vrid 3 priority 80

quit

interface Vlanif4

ip address 172.16.4.253 255.255.255.0

vrrp vrid 4 virtual-ip 172.16.4.254

vrrp vrid 4 priority 80

quit

interface Vlanif5

ip address 172.16.5.253 255.255.255.0

vrrp vrid 5 virtual-ip 172.16.5.254

vrrp vrid 5 priority 80

quit

interface Vlanif6

ip address 172.16.6.253 255.255.255.0

vrrp vrid 6 virtual-ip 172.16.6.254

vrrp vrid 6 priority 80

quit

interface Vlanif7

ip address 172.16.7.253 255.255.255.0

vrrp vrid 7 virtual-ip 172.16.7.254

vrrp vrid 7 priority 80

quit

interface Vlanif100

ip address 172.16.100.253 255.255.255.0

vrrp vrid 100 virtual-ip 172.16.100.254

vrrp vrid 100 priority 80

quit

ospf 1

area 0.0.0.0

network 172.16.200.12 0.0.0.3

network 172.16.200.20 0.0.0.3

network 172.16.1.0 0.0.0.255

network 172.16.2.0 0.0.0.255

network 172.16.3.0 0.0.0.255

network 172.16.4.0 0.0.0.255

network 172.16.5.0 0.0.0.255

network 172.16.6.0 0.0.0.255

network 172.16.7.0 0.0.0.255

quit

quit

ip route-static 0.0.0.0 0.0.0.0 172.16.200.5

dhcp enable

ip pool vlan6

gateway-list 172.16.6.254

network 172.16.6.0 mask 255.255.255.0

dns-list 114.114.114.114 8.8.8.8

excluded-ip-address 172.16.6.250 172.16.6.253

quit

ip pool vlan7

gateway-list 172.16.7.254

network 172.16.7.0 mask 255.255.255.0

dns-list 114.114.114.114 8.8.8.8

excluded-ip-address 172.16.7.250 172.16.7.253

quit

interface Vlanif6

dhcp select global

quit

interface Vlanif7

dhcp select global

quit

interface Eth-Trunk1

port link-type trunk

port trunk allow-pass vlan 1 to 7

quit

interface GigabitEthernet0/0/21

eth-trunk 1

quit

interface GigabitEthernet0/0/22

eth-trunk 1

quit

stp root second

port-group 1

group-member GigabitEthernet 0/0/1 to GigabitEthernet 0/0/10

port link-type trunk

port trunk allow-pass vlan 2 to 7

quit

### 4.2.5无线AC：

vlan 6

vlan 7

quit

stp enable

interface GigabitEthernet0/0/23

port link-type trunk

port trunk allow-pass vlan all

quit

interface GigabitEthernet0/0/24

port link-type trunk

port trunk allow-pass vlan all

quit

interface Vlanif7

ip address 172.16.7.250 255.255.255.0

quit

ip route-static 0.0.0.0 0.0.0.0 172.16.7.254

capwap source interface Vlanif 7

wlan

regulatory-domain-profile name default

country-code CN

quit

ap auth-mode no-auth

security-profile name 001

security wpa-wpa2 psk pass-phrase abcd1234 aes

quit

ssid-profile name 001

ssid chennanxuexiao

quit

vap-profile name 001

forward-mode direct-forward

quit

vap-profile name 001

forward-mode direct-forward

service-vlan vlan-id 6

security-profile 001

ssid-profile 001

quit

ap-group name default

vap-profile 001 wlan 1 radio all

quit

quit

## A区

### 4.3.1汇聚交换机

vlan batch 2 to 7

port-group 1

group-member GigabitEthernet 0/0/1 to GigabitEthernet 0/0/24

port link-type trunk

port trunk allow-pass vlan 2 to 7

quit

### 4.3.2接入交换机

1. **办公楼**

vlan batch 2 to 7

interface GigabitEthernet0/0/1

port link-type trunk

port trunk allow-pass vlan all

quit

interface GigabitEthernet0/0/2

port link-type trunk

port trunk allow-pass vlan all

quit

port-group 1

group-member Ethernet 0/0/1 to Ethernet 0/0/20

port link-type access

port default vlan 1

quit

1. **教学楼**

vlan batch 2 to 7

interface GigabitEthernet0/0/1

port link-type trunk

port trunk allow-pass vlan all

quit

interface GigabitEthernet0/0/2

port link-type trunk

port trunk allow-pass vlan all

quit

port-group 1

group-member Ethernet 0/0/1 to Ethernet 0/0/20

port link-type access

port default vlan 2

quit

1. **财务处**

vlan batch 2 to 7

interface GigabitEthernet0/0/1

port link-type trunk

port trunk allow-pass vlan all

quit

interface GigabitEthernet0/0/2

port link-type trunk

port trunk allow-pass vlan all

quit

port-group 1

group-member Ethernet 0/0/1 to Ethernet 0/0/20

port link-type access

port default vlan 3

quit

### 4.3.3无线POE交换机

vlan batch 6 to 7

interface GigabitEthernet0/0/23

port link-type trunk

port trunk allow-pass vlan all

quit

interface GigabitEthernet0/0/24

port link-type trunk

port trunk allow-pass vlan all

quit

port-group 1

group-member GigabitEthernet 0/0/1 to GigabitEthernet 0/0/20

port link-type trunk

port trunk allow-pass vlan all

port trunk pvid vlan 7

quit

## B区

### 4.4.1汇聚交换机

vlan batch 2 to 7

port-group 1

group-member GigabitEthernet 0/0/1 to GigabitEthernet 0/0/24

port link-type trunk

port trunk allow-pass vlan 2 to 7

quit

### 4.4.2接入交换机

1. **宿舍楼1**

vlan batch 2 to 7

interface GigabitEthernet0/0/1

port link-type trunk

port trunk allow-pass vlan all

quit

interface GigabitEthernet0/0/2

port link-type trunk

port trunk allow-pass vlan all

quit

port-group 1

group-member Ethernet 0/0/1 to Ethernet 0/0/20

port link-type access

port default vlan 4

quit

1. **宿舍楼2**

vlan batch 2 to 7

interface GigabitEthernet0/0/1

port link-type trunk

port trunk allow-pass vlan all

quit

interface GigabitEthernet0/0/2

port link-type trunk

port trunk allow-pass vlan all

quit

port-group 1

group-member Ethernet 0/0/1 to Ethernet 0/0/20

port link-type access

port default vlan 5

quit

### 4.4.3无线POE交换机

vlan batch 6 to 7

interface GigabitEthernet0/0/23

port link-type trunk

port trunk allow-pass vlan all

quit

interface GigabitEthernet0/0/24

port link-type trunk

port trunk allow-pass vlan all

quit

port-group 1

group-member GigabitEthernet 0/0/1 to GigabitEthernet 0/0/20

port link-type trunk

port trunk allow-pass vlan all

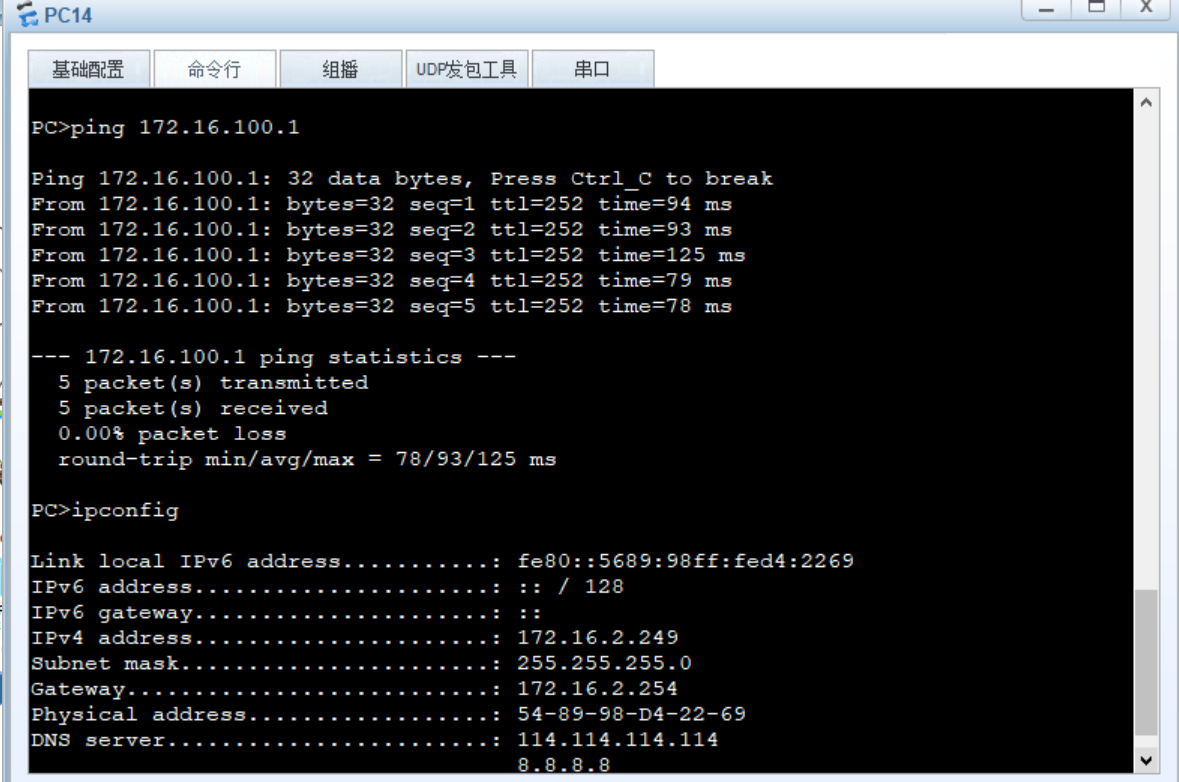
port trunk pvid vlan 7

quit

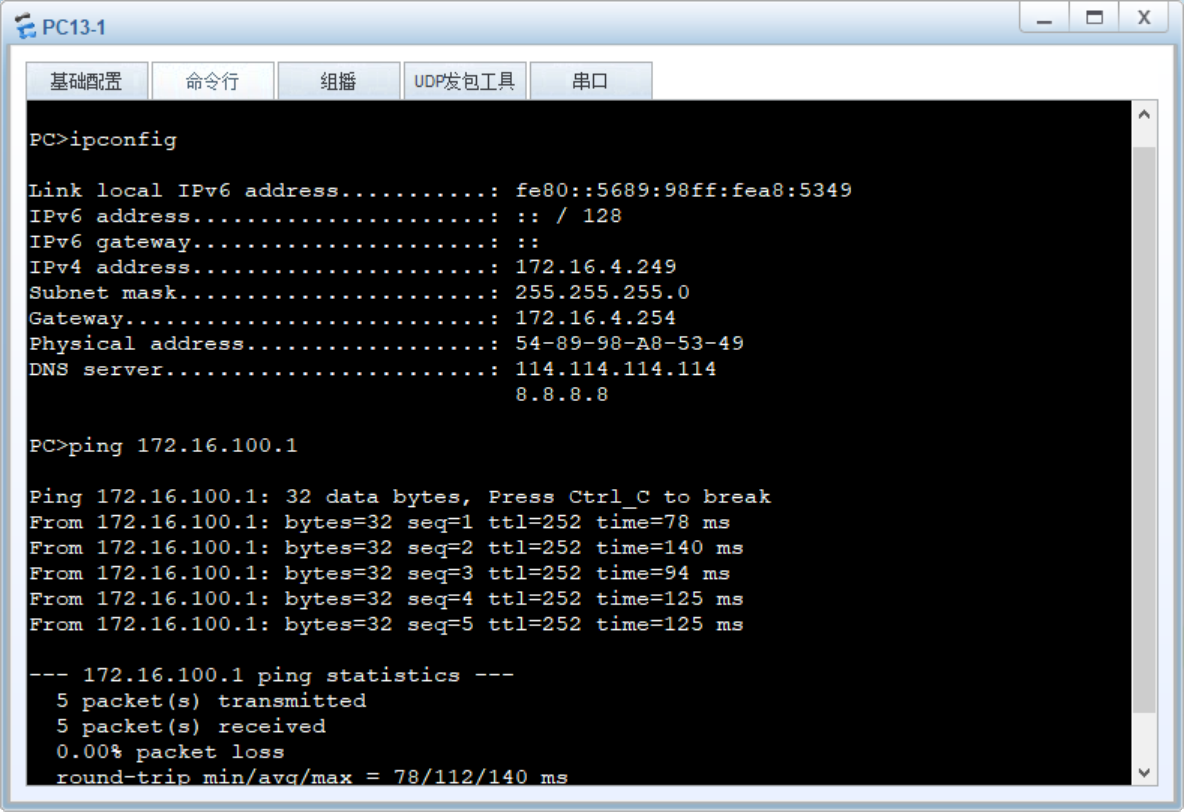
# 验证测试

## 5.1访问数据中心服务器测试

**1）A区访问数据中心服务器**



**1）B区访问数据中心服务器**

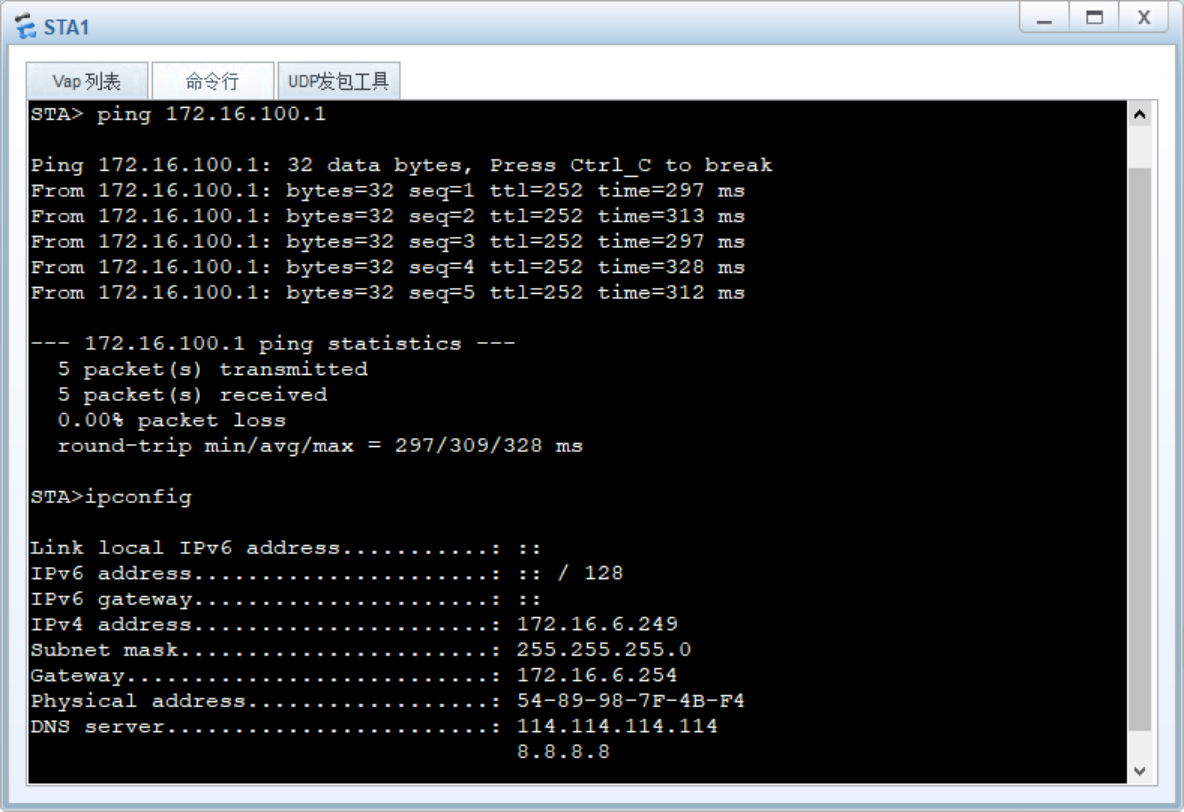


## 5.2无线网络测试

**1）无线网络连接**

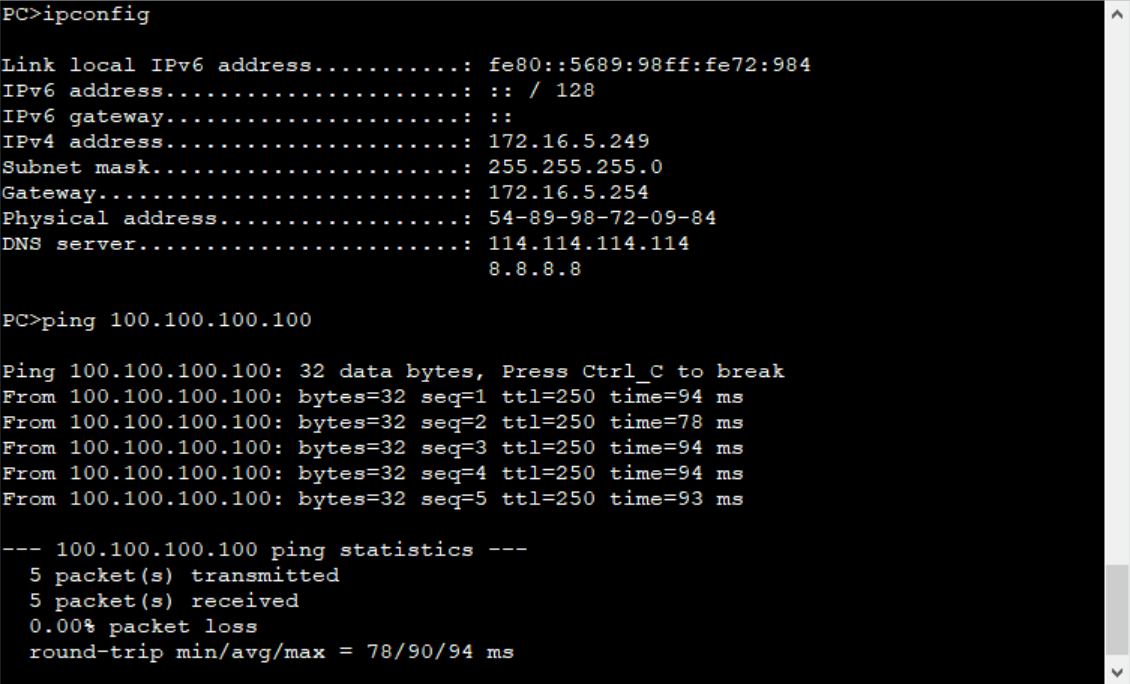


**2）无线网络访问数据中心服务器**



## 5.3访问互联网测试

**1）有线网络访问互联网**



**2）无线网络访问互联网**

