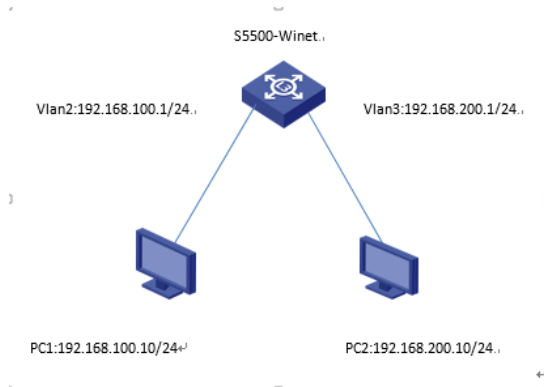


组网及说明

S5500系列交换机配置单向访问案例

1: 网络拓扑



实现PC1可以主动ping通和telnet到PC2上, 但是PC2不能ping通和telnet到PC1上

问题描述

2: 网络需求

实现S5500-winet交换机下面终端单向访问。

过程分析

3: 注意事项

交换机只能实现tcp的单向访问, 并不实现UDP的单向访问。并且单向访问只能是命令行下配置, 无法在web界面上配置。

解决方法

4: 配置步骤

1. 创建vlan100和vlan200, 并把接口g1/0/10添加加入到vlan100, g1/0/20添加到vlan200中去
<H3C>sys
[H3C]vlan 100
[H3C-vlan10]port GigabitEthernet 1/0/10
[H3C-vlan10]qu
[H3C]vlan 200
[H3C-vlan200]port GigabitEthernet 1/0/20
[H3C-vlan200]qu
2. 创建vlan虚接口
[H3C]interface Vlan-interface 100
[H3C-Vlan-interface100]ip address 192.168.100.1 24
[H3C-Vlan-interface100]qu
[H3C]interface Vlan-interface 200
[H3C-Vlan-interface200]ip address 192.168.200.1 24
[H3C-Vlan-interface200] qu
3. 创建ACL3000
[H3C]acl number 3000
[H3C-acl-adv-3000]rule 0 deny tcp syn 1 ack 1 source 192.168.100.0 0.0.0.255 destination 192.168.200.0 0.0.0.255
[H3C-acl-adv-3000]rule 5 deny icmp source 192.168.100.0 0.0.0.255 destination 192.168.200.0 0.0.0.255 icmp-type echo-reply
[H3C-acl-adv-3000]qu
4. 在g1/0/10上调用进方向的包过滤
[H3C]interface GigabitEthernet 1/0/10
[H3C-GigabitEthernet1/0/10]packet-filter 3000 inbound

[H3C-GigabitEthernet1/0/10]qu

5. 保存配置

[H3C]save