# Experimental eight-packet filtering firewall and its settings

【Purpose】

(1) Understand the basic functions of gateways and routers ;

(2) Establish the concept of network security ;

(3) Understand the relevant knowledge of the firewall and the simple setting process of the packet filtering firewall;

【Experimental task】

(1) Configuration of standard access control lists;

(2) Extend the configuration of the access control list.

【experiment equipment】

3-6 people in each group, 6 microcomputers with dual network cards in each group, WindowsXP starts normally;

Each group has 2 Layer 2 switches, 1 Layer 3 switch, and 2 routers;

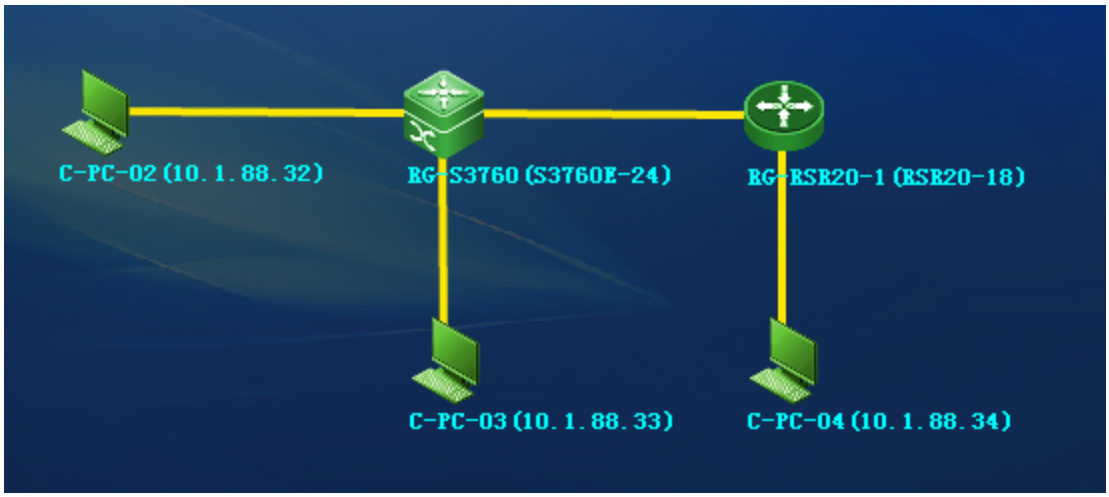
The LIMP laboratory comprehensive management platform started normally.

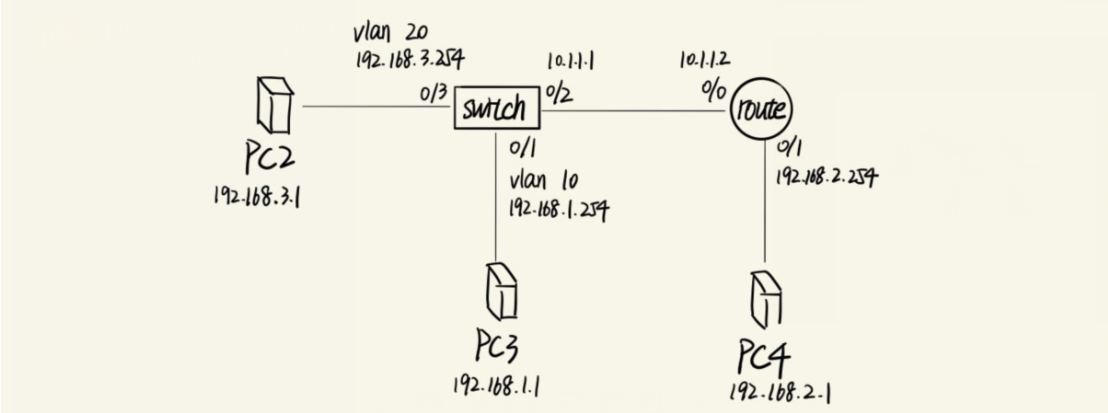
## 【Experimental content】

Item 3 group exercise

According to the experimental topology diagram 7.1, it is required to divide VLAN10 and VLAN20 on SwitchA, and through the access list to control everyone, PC2 can be normal, and only VLAN10 cannot be accessed.

Experimental topology:






## S 3760 :

Configure VLAN10:

SwitchA(config)# vlan 10 //Create vlan10

SwitchA(config-vlan)# exit

SwitchA(config)# int f0/1 //Enter interface f0/1

SwitchA(config-if)# switchport access vlan 10 //Add f0/1 to vlan10

SwitchA(config-if)# exit

SwitchA(config)# interface vlan 10

SwitchA(config-if)# ip address 192.168.1.254 255.255.255.0 //Configure IP address for vlan10

SwitchA(config-if)# no shutdown //Activate this interface

SwitchA(config-if)# exit

```
SwitchA>enable
SwitchA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#vlan 10
SwitchA(config-vlan)#exit
SwitchA(config)#int f0/1
SwitchA(config-FastEthernet 0/1)#switch access vlan 10
SwitchA(config-FastEthernet 0/1)#exit
SwitchA(config)#interface vlan 10
SwitchA(config-VLAN 10)#*Aug 23 08:57:27: %LINEPROTO-5-UPDOWN: Line protocol on
Interface VLAN 10, changed state to up.
ip address 192.168.1.254 255.255.255.0
SwitchA(config-VLAN 10)#no shutdown
SwitchA(config-VLAN 10)#exit
```

Configure VLAN20 :

```
SwitchA(config)#vlan 20
SwitchA(config-vlan)#exit
SwitchA(config)#int f0/3
SwitchA(config-FastEthernet 0/3)#switchport access vlan 20
SwitchA(config-FastEthernet 0/3)#exit
SwitchA(config)#interface vlan 20
SwitchA(config-VLAN 20)#ip address 192.168.3.254 255.255.255.0
SwitchA(config-VLAN 20)#no shutdown
SwitchA(config-VLAN 20)#exit
```

VLAN configuration:

```
SwitchA(config)#show vlan
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
---
   1 VLAN0001                          STATIC    Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gi0/25, Gi0/26
  10 VLAN0010                          STATIC    Fa0/1
  20 VLAN0020                          STATIC    Fa0/3
```

Port f 0/2 configuration:

SwitchA(config)# ip routing //Enable the routing function of the switch

SwitchA(config)# interface fastethernet 0/2

SwitchA(config-if)# no switchport //Transform the Layer 2 interface into a Layer 3 interface

SwitchA(config-if)# ip address 10.1.1.1 255.255.255.0 //Set an IP address for f0/2

SwitchA(config-if)# no shutdown

```
SwitchA(config-router)#ip routing
SwitchA(config)#ip routing
SwitchA(config)#interface fastethernet 0/2
SwitchA(config-FastEthernet 0/2)#no switchport
SwitchA(config-FastEthernet 0/2)#ip address 10.1.1.1 255.255.255.0
SwitchA(config-FastEthernet 0/2)#no shutdown
SwitchA(config-FastEthernet 0/2)#exit
```

Dynamic routing configuration:

```
SwitchA(config)#router rip
SwitchA(config-router)#network 192.168.1.0
SwitchA(config-router)#network 192
                           ^
% Invalid input detected at '^' marker.

SwitchA(config-router)#network 192.168.3.0
SwitchA(config-router)#network 10.1.1.0
```

Routing table configuration result:

```
SwitchA(config-router)#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    10.1.1.0/24 is directly connected, FastEthernet 0/2
C    10.1.1.1/32 is local host.
C    192.168.1.0/24 is directly connected, VLAN 10
C    192.168.1.254/32 is local host.
R    192.168.2.0/24 [120/1] via 10.1.1.2, 00:01:08, FastEthernet 0/2
C    192.168.3.0/24 is directly connected, VLAN 20
C    192.168.3.254/32 is local host.
```

**Set the extended control access list for fa0/1 of the S3760:**

**(After research and discussion, we use extended access control list)**

**Switch A(cinfig)#access-list 101 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255**

```
SwitchA(config)#interface fa 0/1
SwitchA(config-FastEthernet 0/1)#ip access-group 102 out
SwitchA(config-FastEthernet 0/1)#exit
SwitchA(config)#exit
SwitchA#*Aug 23 10:52:31: %SYS-5-CONFIG_I: Configured from console by console
show access-list

ip access-list extended 102
 10 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

## Router 1 configuration process:

**Router1 configures port 0 address as 10.1.1.2/24 configures port 1 address as 192.168.2.254:**

```
Ruijie>en
Ruijie#con
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#hostname Router1
Router1(config)#interface fa 0/0
Router1(config-if-FastEthernet 0/0)#ip address 10.1.1.2 255.255.255.0
Router1(config-if-FastEthernet 0/0)#no shutdown
Router1(config-if-FastEthernet 0/0)#exit
Router1(config)#interface fa 0/1
Router1(config-if-FastEthernet 0/1)#ip address 192.168.2.254 255.255.255.0
Router1(config-if-FastEthernet 0/1)#no shutdown
Router1(config-if-FastEthernet 0/1)#exit
```

**Enable dynamic routing protocols:**

```
Router1(config)#router rip
Router1(config-router)#network 192.168.2.0
Router1(config-router)#network 10.1.1.0
Router1(config-router)#end
```

**Show routing table:**

```
show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    10.1.1.0/24 is directly connected, FastEthernet 0/0
C    10.1.1.2/32 is local host.
C    192.168.2.0/24 is directly connected, FastEthernet 0/1
C    192.168.2.254/32 is local host.
```

## Experimental result test:

**Before the access is prohibited, PC3 to PC4 can be pinged directly**

```
C:\Documents and Settings\Administrator>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time<1ms TTL=62
Reply from 192.168.2.1: bytes=32 time<1ms TTL=62
Reply from 192.168.2.1: bytes=32 time<1ms TTL=62
Reply from 192.168.2.1: bytes=32 time<1ms TTL=62

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

**Prohibit network 192.168.1.0 from accessing 192.168.2.0, PC3 to PC4 cannot be pinged directly**

```
C:\Documents and Settings\Administrator>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

**PC2 to PC4 can be pinged directly**

```
C:\Documents and Settings\Administrator>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time<1ms TTL=62
Reply from 192.168.2.1: bytes=32 time<1ms TTL=62
Reply from 192.168.2.1: bytes=32 time<1ms TTL=62
Reply from 192.168.2.1: bytes=32 time<1ms TTL=62

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

## 【Summary and harvest】

The content of this experiment is the packet filtering firewall and its settings. Although we encountered many problems in the experiment, we successfully completed the experiment under our discussion and the guidance of the teacher. At the same time, from the teacher's explanation before the experiment and our experience in the experiment, we understand the basic functions of gateways and routers , establish the concept of network security in our minds , and understand the relevant knowledge of firewalls and the simple settings of packet filtering firewalls. process. This has benefited us a lot.