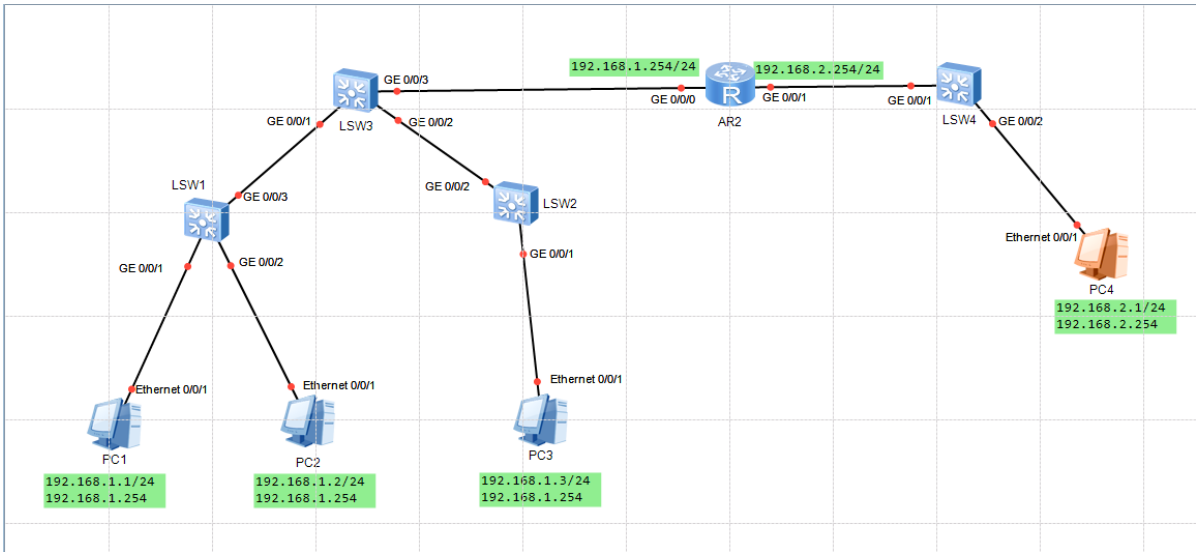


ARP欺骗攻击与防御策略

环境拓扑



实验步骤

配置AR2

```
1 <Huawei>sys
2 [Huawei]sys AR2
3 [AR2]undo info en
4 [AR2]int g0/0/0
5 [AR2-GigabitEthernet0/0/0]ip add 192.168.1.254 255.255.255.0
6 [AR2-GigabitEthernet0/0/0]q
7 [AR2]int g0/0/1
8 [AR2-GigabitEthernet0/0/1]ip add 192.168.2.254 255.255.255.0
9 [AR2-GigabitEthernet0/0/1]q
10 [AR2]
```

ping各PC之间的情况

```
PC>ping 192.168.2.1

Ping 192.168.2.1: 32 data bytes, Press Ctrl_C to break
From 192.168.2.1: bytes=32 seq=1 ttl=127 time=110 ms
From 192.168.2.1: bytes=32 seq=2 ttl=127 time=62 ms
From 192.168.2.1: bytes=32 seq=3 ttl=127 time=93 ms
From 192.168.2.1: bytes=32 seq=4 ttl=127 time=94 ms
From 192.168.2.1: bytes=32 seq=5 ttl=127 time=110 ms

--- 192.168.2.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 62/93/110 ms
```

```

PC>ping 192.168.1.2

Ping 192.168.1.2: 32 data bytes, Press Ctrl_C to break
From 192.168.1.2: bytes=32 seq=1 ttl=128 time=47 ms
From 192.168.1.2: bytes=32 seq=2 ttl=128 time=31 ms
From 192.168.1.2: bytes=32 seq=3 ttl=128 time=47 ms
From 192.168.1.2: bytes=32 seq=4 ttl=128 time=31 ms
From 192.168.1.2: bytes=32 seq=5 ttl=128 time=47 ms

--- 192.168.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 31/40/47 ms

PC>ping 192.168.1.3

Ping 192.168.1.3: 32 data bytes, Press Ctrl_C to break
From 192.168.1.3: bytes=32 seq=1 ttl=128 time=78 ms
From 192.168.1.3: bytes=32 seq=2 ttl=128 time=78 ms
From 192.168.1.3: bytes=32 seq=3 ttl=128 time=94 ms
From 192.168.1.3: bytes=32 seq=4 ttl=128 time=62 ms
From 192.168.1.3: bytes=32 seq=5 ttl=128 time=78 ms

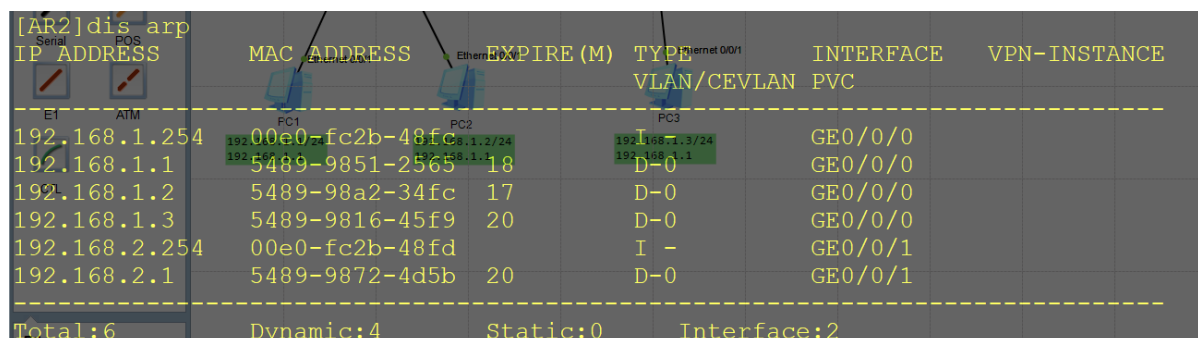
--- 192.168.1.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 62/78/94 ms

PC>ping 192.168.1.254

Ping 192.168.1.254: 32 data bytes, Press Ctrl_C to break
From 192.168.1.254: bytes=32 seq=1 ttl=255 time=125 ms
From 192.168.1.254: bytes=32 seq=2 ttl=255 time=62 ms
From 192.168.1.254: bytes=32 seq=3 ttl=255 time=63 ms
From 192.168.1.254: bytes=32 seq=4 ttl=255 time=46 ms
From 192.168.1.254: bytes=32 seq=5 ttl=255 time=63 ms

```

查看路由器的mac和IP地址绑定情况(arp表)



[AR2]dis arp

IP ADDRESS	MAC ADDRESS	EXPIRE (M)	TYPE	INTERFACE	VPN-INSTANCE
			VLAN/CEVLAN	PVC	
192.168.1.254	00e0-fc2b-48fc	18	D-0	GE0/0/0	
192.168.1.1	5489-9851-2565	17	D-0	GE0/0/0	
192.168.1.2	5489-98a2-34fc	20	D-0	GE0/0/0	
192.168.1.3	5489-9816-45f9	20	D-0	GE0/0/0	
192.168.2.254	00e0-fc2b-48fd		I -	GE0/0/1	
192.168.2.1	5489-9872-4d5b	20	D-0	GE0/0/1	
Total:6	Dynamic:4	Static:0	Interface:2		

修改pc3 IP地址为pc1 IP地址，并查看arp信息，清除arp

1修改ip

PC3

基础配置 命令行 组播 UDP发包工具 串口

主机名:

MAC 地址:

IPv4 配置

☒ 静态 ☐ DHCP ☐ 自动获取 DNS 服务器地址

IP 地址: DNS1:

子网掩码: DNS2:

网关:

IPv6 配置

☒ 静态 ☐ DHCPv6

IPv6 地址:

前缀长度:

IPv6 网关:

应用

2清除arp信息

arp -d

```
PC>arp -d

PC>arp -a

Internet Address      Physical Address      Type
```

使用PC3 ping PC4 查看AR1的arp表项

1.使用PC3 ping PC4

```
PC>ping 192.168.2.1

Ping 192.168.2.1: 32 data bytes, Press Ctrl_C to break
Request timeout!
From 192.168.2.1: bytes=32 seq=2 ttl=127 time=78 ms
From 192.168.2.1: bytes=32 seq=3 ttl=127 time=78 ms
From 192.168.2.1: bytes=32 seq=4 ttl=127 time=78 ms
From 192.168.2.1: bytes=32 seq=5 ttl=127 time=79 ms

--- 192.168.2.1 ping statistics ---
 5 packet(s) transmitted
 4 packet(s) received
20.00% packet loss
round-trip min/avg/max = 0/78/79 ms
```

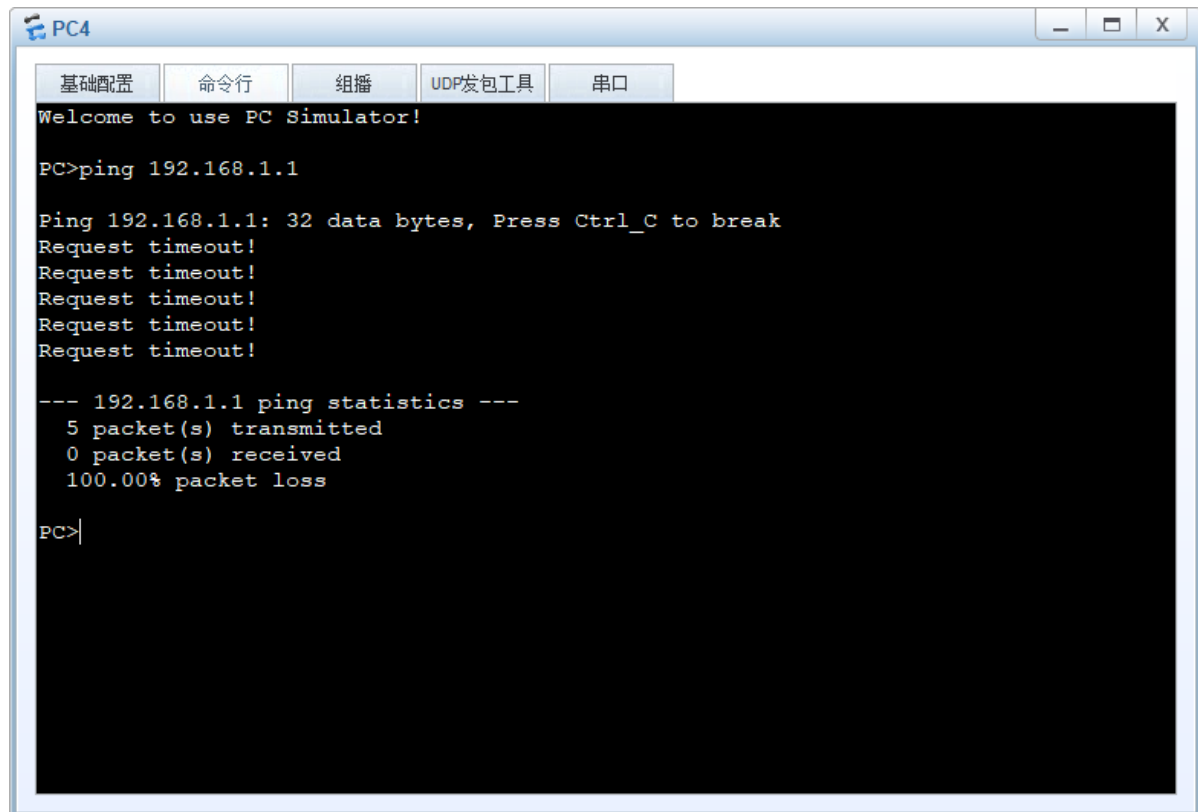
2.AR1的arp表项

[AR2]dis arp

IP ADDRESS	MAC ADDRESS	EXPIRE (M)	TYPE	INTERFACE	VPN-INSTANCE
192.168.1.254	00e0-fc2b-48fc		I -	GE0/0/0	
192.168.1.1	5489-9816-45f9	19	D-0	GE0/0/0	
192.168.1.2	5489-98a2-34fc	7	D-0	GE0/0/0	
192.168.1.3	5489-9816-45f9	10	D-0	GE0/0/0	
192.168.2.254	00e0-fc2b-48fd		I -	GE0/0/1	
192.168.2.1	5489-9872-4d5b	19	D-0	GE0/0/1	

Total:6 Dynamic:4 Static:0 Interface:2

PC3 IP地址重新修改为192.168.1.3,然后让PC4 ping 192.168.1.1



防御策略

在AR2绑定网关与MAC地址映射关系

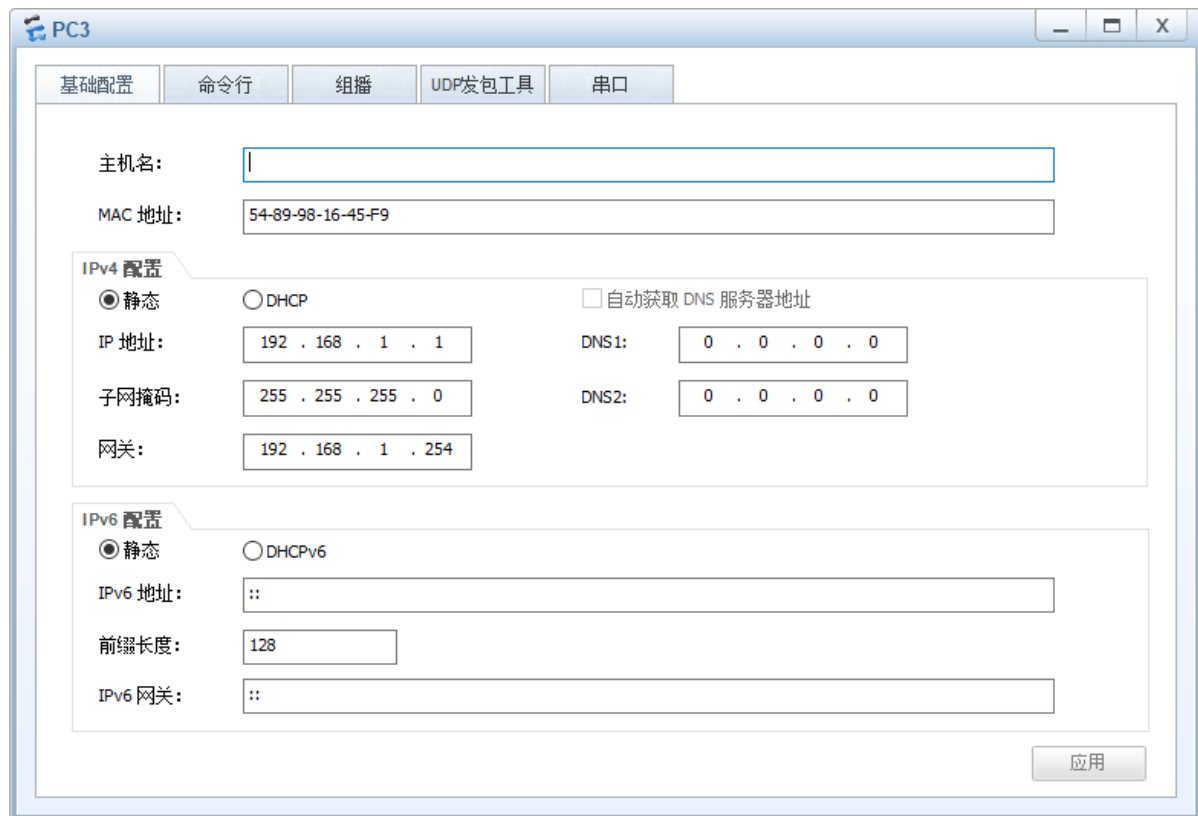
```
1 <AR2>sys
2 [AR2]user-bind static ip-address 192.168.1.1 MAC-address 5489-9851-2565
3 Info: 1 static user-bind item(s) added.
```

在交换机SW3开启动态arp监测

```
1 <Huawei>sys
2 Enter system view, return user view with Ctrl+Z.
3 [Huawei]int g0/0/3
4 [Huawei-GigabitEthernet0/0/3]arp anti-attack check user-bind enable
```

验证

将pc3的IP地址改为pc1后 无法ping通



The image shows the 'PC3' configuration window in a network simulator. The '基础配置' (Basic Configuration) tab is active. The '主机名' (Hostname) field is empty. The 'MAC 地址' (MAC Address) field is set to '54-89-98-16-45-F9'. The 'IPv4 配置' (IPv4 Configuration) section has the '静态' (Static) radio button selected. The 'IP 地址' (IP Address) is '192.168.1.1', '子网掩码' (Subnet Mask) is '255.255.255.0', and '网关' (Gateway) is '192.168.1.254'. The 'DNS1' and 'DNS2' fields are both '0.0.0.0'. The 'IPv6 配置' (IPv6 Configuration) section has the '静态' (Static) radio button selected. The 'IPv6 地址' (IPv6 Address) is '::', '前缀长度' (Prefix Length) is '128', and 'IPv6 网关' (IPv6 Gateway) is '::'. An '应用' (Apply) button is at the bottom right.

PC3

基础配置 命令行 组播 UDP发包工具 串口

主机名:

MAC 地址:

IPv4 配置

☒ 静态 ☐ DHCP ☐ 自动获取 DNS 服务器地址

IP 地址: DNS1:

子网掩码: DNS2:

网关:

IPv6 配置

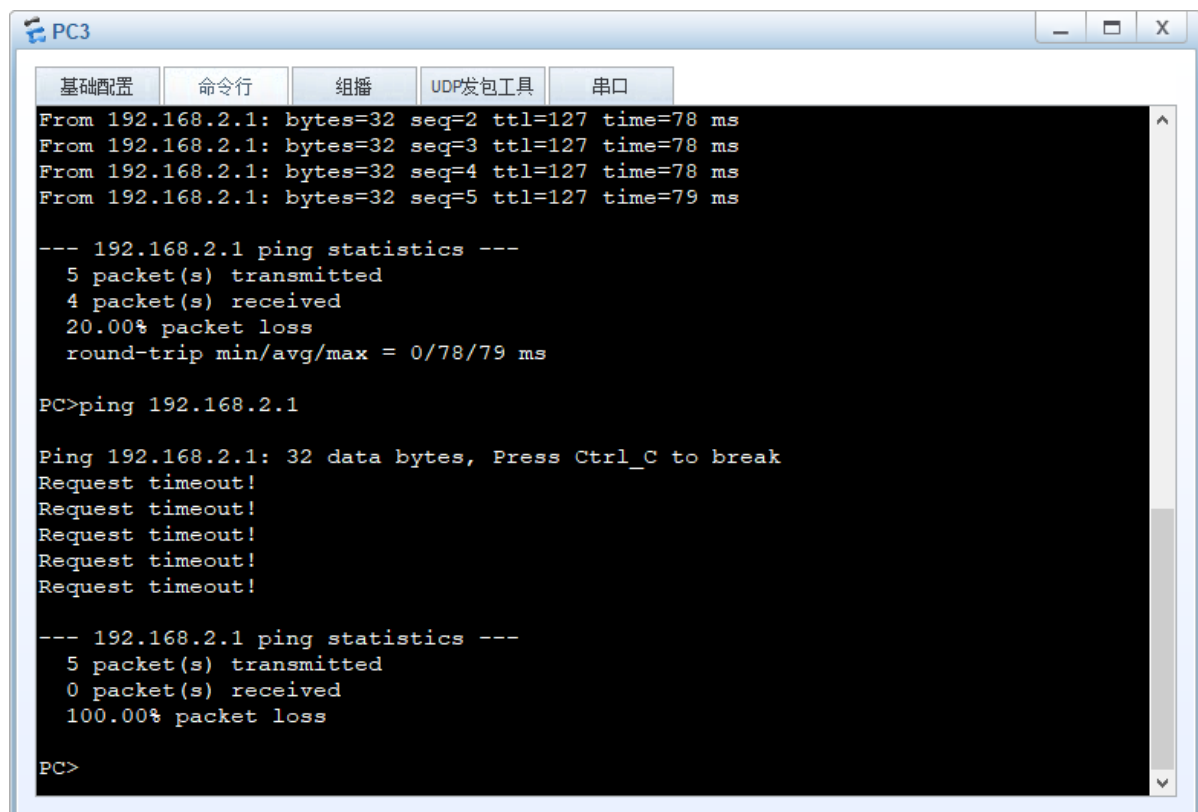
☒ 静态 ☐ DHCPv6

IPv6 地址:

前缀长度:

IPv6 网关:

应用



The image shows the 'PC3' command line window in a network simulator. The '基础配置' (Basic Configuration) tab is active. The window displays the output of a ping command from 192.168.2.1 to 192.168.2.1. The output shows 5 packets transmitted, 4 packets received, and a 20.00% packet loss. The round-trip times are 0/78/79 ms. The command 'PC>ping 192.168.2.1' is entered, and the output shows 'Ping 192.168.2.1: 32 data bytes, Press Ctrl_C to break' followed by four 'Request timeout!' messages. The command line prompt 'PC>' is visible at the bottom.

PC3

基础配置 命令行 组播 UDP发包工具 串口

```
From 192.168.2.1: bytes=32 seq=2 ttl=127 time=78 ms
From 192.168.2.1: bytes=32 seq=3 ttl=127 time=78 ms
From 192.168.2.1: bytes=32 seq=4 ttl=127 time=78 ms
From 192.168.2.1: bytes=32 seq=5 ttl=127 time=79 ms

--- 192.168.2.1 ping statistics ---
 5 packet(s) transmitted
 4 packet(s) received
20.00% packet loss
round-trip min/avg/max = 0/78/79 ms

PC>ping 192.168.2.1

Ping 192.168.2.1: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
Request timeout!
Request timeout!
Request timeout!

--- 192.168.2.1 ping statistics ---
 5 packet(s) transmitted
 0 packet(s) received
100.00% packet loss

PC>
```

查看AR2的arp表

[AR2]dis arp

IP ADDRESS	MAC ADDRESS	EXPIRE (M)	TYPE	INTERFACE	VPN-INSTANCE
Serial	POS	Ethernet 0/0/1	Ethernet 0/0/1	VLAN/CEVLAN PVC	
192.168.1.254	00e0-fc2b-48fc		I	GE0/0/0	
192.168.1.1	5489-9851-2565	16	D-0	GE0/0/0	
192.168.1.2	5489-98a2-34fc	3	D-0	GE0/0/0	
192.168.1.3	5489-9816-45f9	7	D-0	GE0/0/0	
192.168.2.254	00e0-fc2b-48fd		I -	GE0/0/1	
192.168.2.1	5489-9872-4d5b	17	D-0	GE0/0/1	
Total:6	Dynamic:4	Static:0	Interface:2		

任务总结

- 1.交换机可以只绑定IP与MA C 地址关系，即执行如下操作
- user-bind static ip-address 192.168.1.1 MAC-address 5489-9851-2565
- 2.为防范ARP攻击，假如管理员没有开启动态ARP监测(DAI)功能,在客户机上可以自己手动绑定网关IP与MAC地址关系以避免遭受攻击
- 3.ARP欺骗劫持不属于病毒木马，不能通过安装防病毒软件达到防御效果