

网络技术与信息安全

第8讲 使用DHCP管理IP地址

河南中医药大学信息技术学院

网络技术课程教学组

本章教学目标

- 理解通过DHCP获取IP地址的基本过程
- 掌握获取IP地址过程中，四报文的首部地址信息
- 掌握DHCP中继的配置和应用
- 了解DHCP的安全性问题及解决方案



一、为什么要使用DHCP?

为什么要使用DHCP?

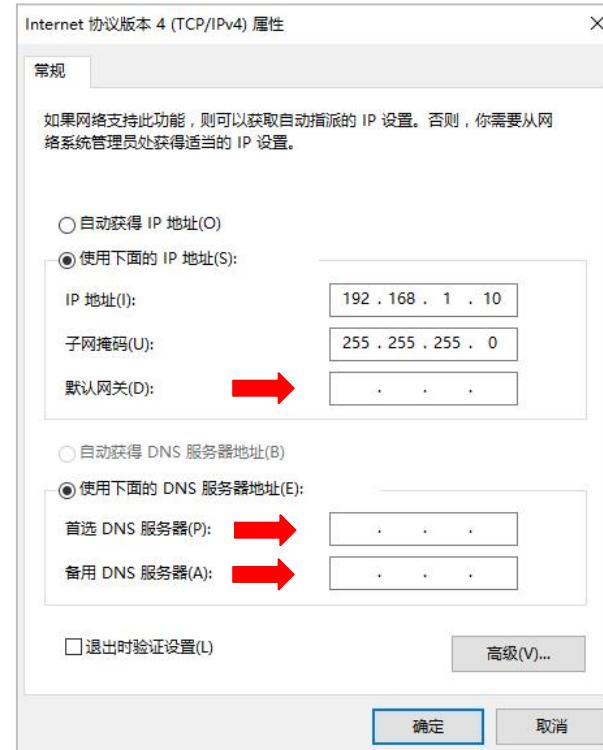
□ DHCP的作用

- DHCP (Dynamic Host Configuration Protocol, 动态主机配置协议) 是一个**局域网**的协议，使用UDP协议工作。
- 通过DHCP服务，DHCP服务器可以为网络中安装了DHCP客户端程序的计算机自动分配IP地址和其他相关配置 (DNS, 网关等)，而不需要管理员对每个主机进行逐一配置，极大的降低了管理成本。
- **DHCP应用于**网络规模较大，手工配置IP地址需要很大工作量的场合，从而加强对整个网络的IP地址进行集中管理。

为什么要使用DHCP?

□ DHCP服务不仅提供IP地址自动分配功能，还有以下功能：

- 可以自动配置客户端的DNS服务器和默认网关。
- 通过IP地址与MAC地址绑定，实现IP地址的固定分配。
- 利用IP地址排除功能，使静态分配给其他主机的IP地址不再分配给另外的DHCP客户端。



二、通过DHCP获取IP地址基本过程

通过DHCP获取IP地址基本过程

□ 先认识一下DHCP服务的8种类型报文：

■ DHCP服务共有8种报文，其中4种用于实现IP地址的正常获取过程；另外4种，用于应对特殊情况。

- 实现IP获取：Discover、Offer、Request、ACK
- 对应特殊情况：NAK、Release、Decline、INForm

通过DHCP获取IP地址基本过程

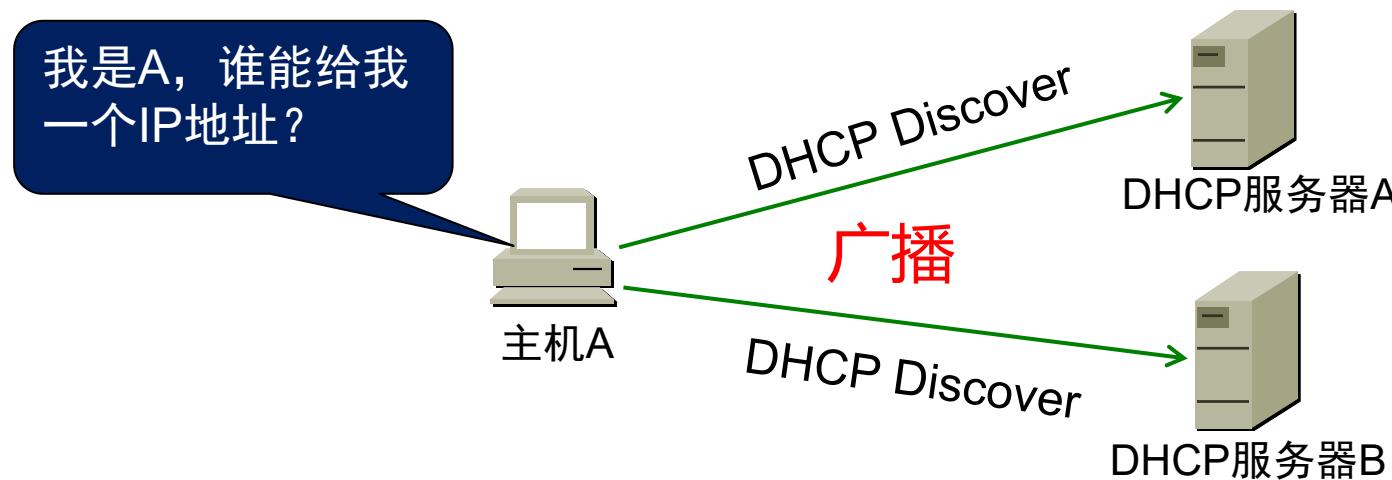
□ DHCP客户端从DHCP服务器获得IP地址信息的过程分为4个阶段：

- 发现阶段：使用DHCP Discover报文 (客户端→服务器)
- 提供阶段：使用DHCP Offer报文 (客户端←服务器)
- 请求阶段：使用DHCP Request报文 (客户端→服务器)
- 确认阶段：使用DHCP ACK报文 (客户端←服务器)
- 具体过程如下页

通过DHCP获取IP地址基本过程

阶段1：DHCP Discover (发现报文)：发现网络中的DHCP服务器

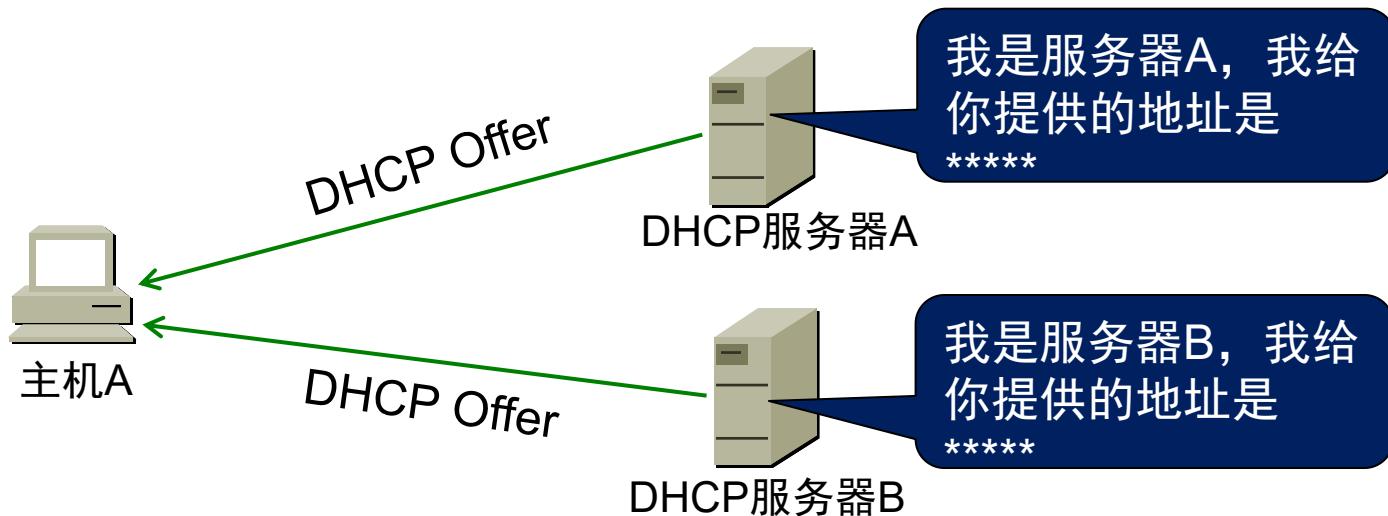
- 当DHCP客户端第一次启动时，如果客户端发现自己没有配置IP地址，就会向它所处的网络内广播一个DHCP Discover报文，请求获取IP配置信息。



通过DHCP获取IP地址基本过程

阶段2：DHCP Offer（提供报文）：为客户端提供IP地址

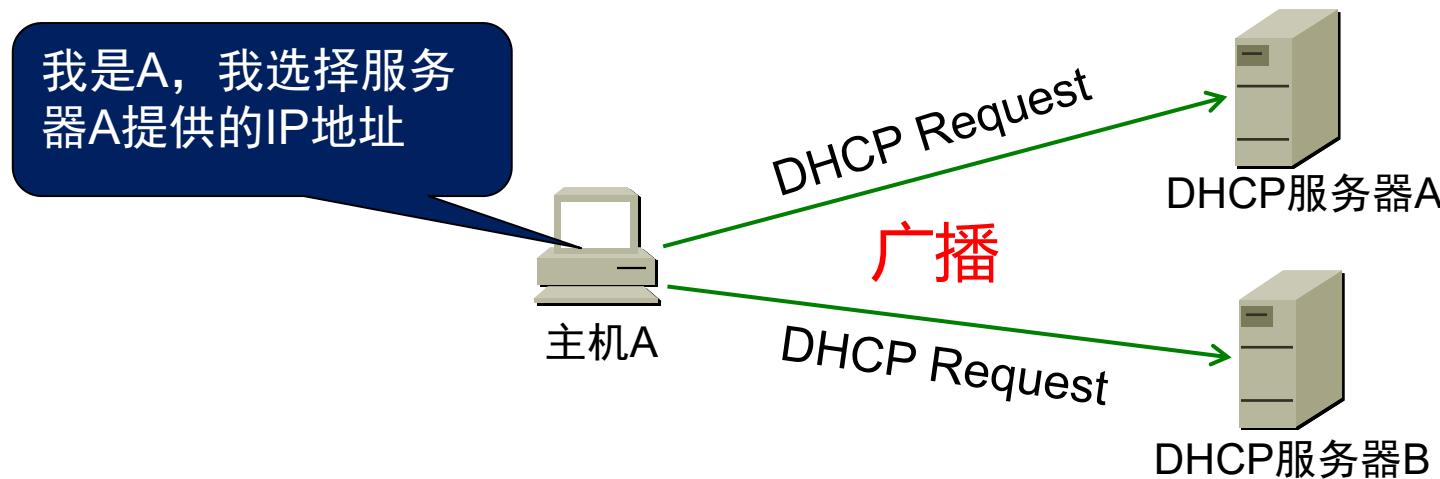
- 网络中的任一DHCP服务器收到DHCP Discover广播报文后，都回应给客户端一个DHCP Offer报文，告诉客户端自己可以提供的IP地址等信息内容，并且将该IP地址暂时锁定，不再分配给其他客户端。



通过DHCP获取IP地址基本过程

阶段3：DHCP Request（请求报文）：明确选择哪个服务器提供的地址

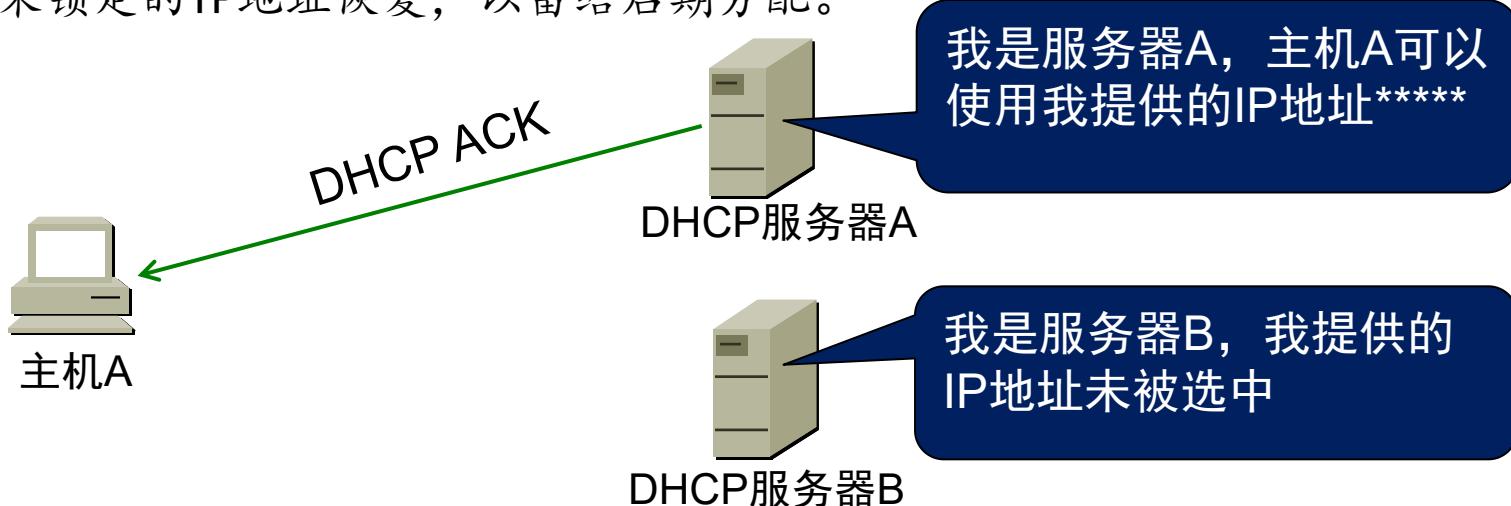
- 若客户端收到多台DHCP服务器的回应，会从中选择最先到达的那个DHCP Offer报文，然后向网络上发送一个DHCP Request广播报文，告诉所有DHCP服务器它将选用哪一台服务器提供的IP地址。



通过DHCP获取IP地址基本过程

阶段4：DHCP ACK（确认报文）：通知客户端可以使用分配的IP地址

- DHCP服务器A接收到DHCP Request广播报文后，发现自己被选中，会向客户端发出DHCP ACK回应，以确认IP租约的正式生效，结束IP获取过程。同时，将已分配的IP地址保留，不再租用给其他客户使用。
- DHCP服务器B接收到DHCP Request广播报文后，发现自己未被选中，将原来锁定的IP地址恢复，以留给后期分配。



通过DHCP获取IP地址基本过程

□ DHCP服务的8种类型报文：

■ 其他4种报文

- DHCP NAK（应答报文）：通知客户端无法分配合适的IP地址。
- DHCP Release（请求报文）：请求释放相应的IP地址。
- DHCP Decline（请求报文）：告知服务器分配的IP地址不可用，希望获取新的IP地址。
- DHCP INForm（请求报文）：DHCP客户端需要从DHCP服务器获取更为详细的配置信息时，则向DHCP服务器发送DHCP INForm请求报文。

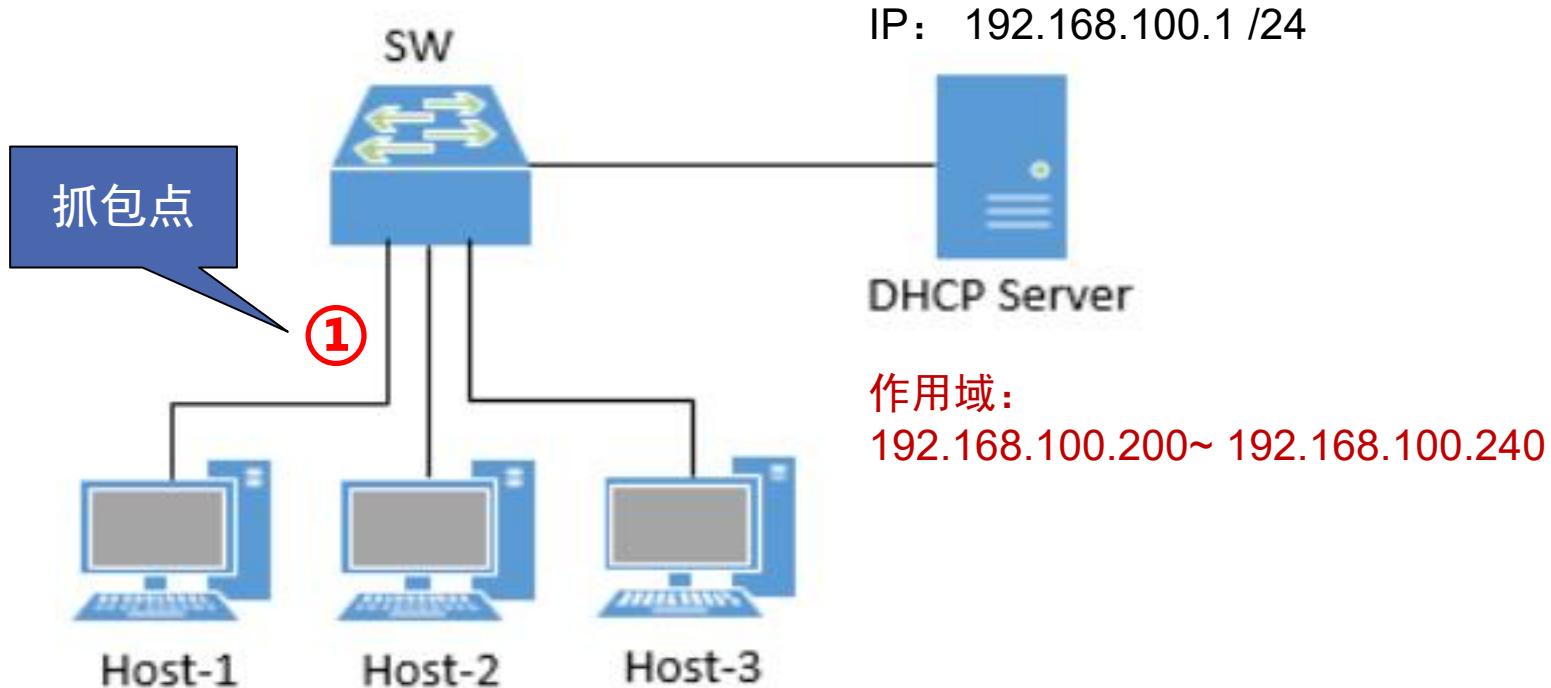
通过DHCP获取IP地址基本过程

□ DHCP的租约

- DHCP服务器分配的IP地址是临时的，DHCP客户机只能在一段有限的时间内使用这个分配到的IP地址。DHCP协议称这段时间为**租用期**。
- 为了使用IP地址的连续性，客户机在租约到期之前，会自动续订。在租约期到一半的时候会再次发出DHCP Request，重新续租；如果此时得不到DHCP服务器的确认，客户端还暂时可以继续使用该IP；
- 当租约期过了87.5%时，若客户端仍然无法与当初的DHCP服务器联系上，它将与其它DHCP服务器通信，并请求更新它的配置信息。
- 若租约到期且网络上没有其他DHCP服务器在运行，客户端必须停止使用该IP地址，并从发送DHCP Discover报文开始，再一次重复整个IP地址获取过程。

三、 抓包分析DHCP的工作过程

◆ 网络拓扑描述



-
- 思考几个问题

➤ 问题1：

□ 客户机在首次发送Discover报文时，其报文首部的地址如何配置？

■ 客户机发出的发现报文中，

- 源MAC? / 目的MAC?
- 源IP? / 目的IP ?

■ 提醒：

- 此时，客户机自身没有IP地址，也不知道DHCP服务器的IP地址

抓包分析：DHCP discover报文 - 首部信息



源MAC: 客户机MAC地址

目的MAC: 广播地址

No.	Source	Destination	Protocol	Info
82	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Tr
83	192.168.100.1	192.168.100.202	DHCP	DHCP Offer - Tr
85	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Tr
86	192.168.100.1	192.168.100.202	DHCP	DHCP ACK - Tr

- > Frame 82: 410 bytes on wire (3280 bits), 410 bytes captured (3280 bits)
- > Ethernet II, Src: 54:89:98:f3:0a:28, Dst: ff:ff:ff:ff:ff:ff
- > Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
- > User Datagram Protocol, Src Port: 68, Dst Port: 67
- > Dynamic Host Configuration Protocol (Discover)

源IP: 全0地址

目的IP: 全1广播地址

源端口: 68 (客户端)
目的端口: 67 (服务器端)

报文内容见下页

抓包分析：DHCP discover报文 - 内容信息 (1)



Dynamic Host Configuration Protocol (Discover)

Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x0000503f
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: HuaweiTe_f3:0a:28 (54:89:98:f3:0a:28)
Client hardware address padding: 00000000000000000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (Discover)
Option: (61) Client identifier
Option: (55) Parameter Request List
Option: (255) End
Padding: 00...

Discover报文的内容信息

抓包分析：DHCP discover报文 - 内容信息（2）



▼ Dynamic Host Configuration Protocol (Discover)

Message type: Boot Request (1)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

此时客户端的IP地址是全0

Transaction ID: 0x0000503f

Seconds elapsed: 0

➤ Bootp flags: 0x0000 (Unicast)

Client IP address: 0.0.0.0

Your (client) IP address: 0.0.0.0

Next server IP address: 0.0.0.0

Relay agent IP address: 0.0.0.0

Client MAC address: HuaweiTe f3

Client hardware address padding: 00000000000000000000

Client hardware address padding: 00000000000000000000

上半部分
內容信息

抓包分析：DHCP discover报文 - 内容信息 (3)



- > Option: (53) DHCP Message Type (Discover)
- `v Option: (61) Client identifier
 Length: 7
 Hardware type: Ethernet (0x01)
 Client MAC address: HuaweiTe_f3:0a:28 (54:89:98:f3:0a:28)
- `v Option: (55) Parameter Request List
 Length: 9
 - Parameter Request List Item: (1) Subnet Mask
 - Parameter Request List Item: (3) Router
 - Parameter Request List Item: (6) Domain Name Server
 - Parameter Request List Item: (15) Domain Name
 - Parameter Request List Item: (28) Broadcast Address
 - Parameter Request List Item: (33) Static Route
 - Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
 - Parameter Request List Item: (121) Classless Static Route
 - Parameter Request List Item: (184) Unassigned
- > Option: (255) End

客户端的标识符（即MAC地址）

下半部分
内容信息

客户端申请
参数列表

➤ 问题1：（抓包分析，结论）



□ 客户机在首次发送Discover报文时，其报文头部的地址如何配置？

- 客户机发出发现报文：由于客户机采用动态获得IP地址的方式（即DHCP方式），因此客户机在启动时会自动找DHCP服务器，即以广播形式发出DHCP的发现报文（DHCP Discover）报文；
- 运输层的封装：Discover报文在运输层进行封装时，使用UDP协议，使用UDP68端口作为源端口，使用UDP67端口作为目的端口。（注：DHCP客户使用的UDP端口是68，而DHCP服务器使用的UDP端口是67）
- 网络层的封装：Discover报文在网络层进行封装时，由于客户机还没有IP地址，它会使用0.0.0.0作为源地址，使用255.255.255.255作为目标IP地址来广播。



➤ 问题1：（抓包分析，结论）

□ 客户机在首次发送Discover报文时，其报文首部的地址如何配置？

- 数据链路层的封装：发现报文在数据链路层进行封装时，使用DHCP客户机的MAC地址作为源地址，使用ff:ff:ff:ff:ff:ff作为目的MAC地址，进行广播。
- 在discover报文数据字段中
 - 包含有DHCP客户机的标识信息（即MAC地址），以便DHCP服务器知道这是谁发的DHCP Discover报文

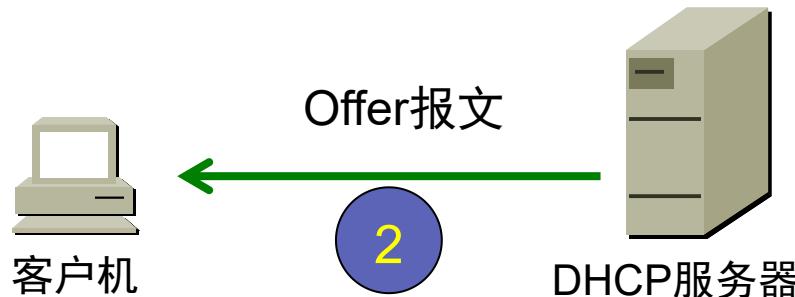
➤ 问题2：

□ 服务器发出的DHCP Offer报文中，包含了什么信息？

■ DHCP Offer报文的头部中，各种地址信息是什么？

- 源MAC? / 目的MAC?
- 源IP? / 目的IP ?

■ 服务器响应客户端的信息内容有什么？



抓包分析：DHCP offer报文 - 首部信息



No.	Source	Destination	Protocol	Info
82	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID: 1
83	192.168.100.1	192.168.100.202	DHCP	DHCP Offer - Transaction ID: 1
85	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID: 1
86	192.168.100.1	192.168.100.202	DHCP	DHCP ACK - Transaction ID: 1

Below the table, several details about the selected frame (Frame 83) are listed:

- > Frame 83: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
- > Ethernet II, Src: 08:00:27:c1:97:81, Dst: 54:89:98:f3:0a:28
- > Internet Protocol Version 4, Src: 192.168.100.1, Dst: 192.168.100.202
- > User Datagram Protocol, Src Port: 67, Dst Port: 68
- > Dynamic Host Configuration Protocol (Offer)

源MAC: 服务器MAC

目的MAC: 客户端MAC

报文内容见下页

源IP: 服务器IP

目的IP: 准备分配给客户端的IP

源端口: 67 (服务器端)
目的端口: 68 (客户端)

抓包分析：DHCP offer报文 - 内容信息1



Dynamic Host Configuration Protocol (Offer)

Message type: Boot Reply (2)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0x0000503f

准备分配给客户端的IP地址

Seconds elapsed: 0

Bootp flags: 0x0000 (Unicast)

Client IP address: 0.0.0.0

Your (client) IP address: 192.168.100.202

表明offer报文所响应的客户端的MAC地址

Next server IP address: 0.0.0.0

Relay agent IP address: 0.0.0.0

Client MAC address: HuaweiTe_f3:0a:28 (54:89:98:f3:0a:28)

Client hardware address padding: 00000000000000000000000000000000

抓包分析：DHCP offer报文 - 内容信息2



- > Option: (53) DHCP Message Type (Offer)
- v Option: (54) DHCP Server Identifier (192.168.100.1)
 Length: 4
 DHCP Server Identifier: 192.168.100.1 → DHCP服务器标识
- v Option: (51) IP Address Lease Time
 Length: 4
 IP Address Lease Time: (43200s) 12 hours → IP租约时间12小时
- v Option: (1) Subnet Mask (255.255.255.0)
 Length: 4
 Subnet Mask: 255.255.255.0 → 准备配置给客户端的子网掩码
- v Option: (3) Router
 Length: 4
 Router: 192.168.100.254 → 准备配置给客户端的默认网关地址
- v Option: (6) Domain Name Server
 Length: 4
 Domain Name Server: 8.8.8.8 → 准备配置给客户端的域名服务器IP地址

➤ 问题2：（抓包分析，结论）



□ 服务器发出的DHCP Offer报文中，包含哪些信息？

- 当DHCP服务器接收到客户机发来的Discover报文时，它就在自己的IP地址池（即作用域）中查找是否有合法的IP地址提供给客户机。如果有，DHCP服务器就将此IP地址做上标记，暂时不再分配给其他客户机。
- DHCP服务器收到Discover报文后，会**返回**DHCP Offer报文。
 - Offer报文的内容（总结）
 - Offer报文头部的地址信息（总结）

➤ 问题2：（抓包分析，结论）



□ 服务器发出的DHCP Offer报文中，包含哪些信息？

■ DHCP Offer报文中包含的信息

➤ Offer报文所响应的客户端的MAC地址；

→ 想给谁？

➤ 准备提供给客户端的IP地址；

➤ 准备提供给客户端的子网掩码；默认网关、DNS等；

➤ IP地址的租约时间；

→ 给什么？

➤ DHCP服务器的标识符（即IP地址）

→ 谁给的？

以上信息主要是提供给客户机的配置信息

➤ 问题2：（抓包分析，结论）



□ 服务器发出的DHCP Offer报文中，包含哪些信息？

■ DHCP Offer报文首部中的地址信息

- 运输层首部：源端口（67）、目的端口（68）；
- 网络层首部：源IP（服务器的IP）、目的IP（准备分配给客户机的IP）
- 数据链路层首部：源MAC（服务器MAC）、目的MAC（客户机的MAC）

以上信息用于报文传输

➤ 引申思考：

服务器发出的Offer报文，是广播？还是单播？

(注意，该结论同样适用于ACK报文)

➤ 两个抓包案例 —— Offer报文到底是单播，还是广播？

此处可看出，offer报文是单播！

No.	Source	Destination	Protocol	Info
82	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Tra
83	192.168.100.1	192.168.100.202	DHCP	DHCP Offer - Tra
85	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Tra

No.	Time	Source	Destination	Protocol	Leng	Info
91	14.054362	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover -
92	14.057984	172.16.1.201	255.255.255.255	DHCP	342	DHCP Offer -
93	14.058100	0.0.0.0	255.255.255.255	DHCP	350	DHCP Request

此处可看出，offer报文是广播！



Offer



➤ 引申思考：

□ 服务器发出的Offer报文，是广播？还是单播？

■ 看看RFC2131是怎么规定的

A client that **cannot** (不能) receive **unicast** (单播) **IP datagrams** (IP数据报) until its protocol software has been **configured with** (配置) an IP address, SHOULD set the **BROADCAST bit** (广播位) in the ‘**flags**’ field (flags字段) to 1 in any **DHCPDISCOVER** or **DHCPREQUEST** messages that client sends.

The **BROADCAST bit** will provide a **hint** (提示) to the **DHCP** server and **BOOTP relay agent** (DHCP中继代理) to broadcast any messages to the client on the client’s **subnet** (子网) .

A client that can receive unicast IP datagrams before its protocol software has been configured, SHOULD clear the **BROADCAST bit** to 0.

➤ 引申思考：



□ 服务器发出的Offer报文，是广播？还是单播？

■ 看看RFC2131是怎么规定的

A client that cannot receive unicast IP datagrams until its protocol software has been configured with an IP address , SHOULD set the BROADCAST bit in the 'flags' field to 1 in any DHCPDISCOVER or DHCPREQUEST messages that client sends. The BROADCAST bit will provide a hint to the DHCP server and BOOTP relay agent to broadcast any messages to the client on the client's subnet. A client that can receive unicast IP datagrams before its protocol software has been configured, SHOULD clear the BROADCAST bit to 0.

在客户端无法接收单播IP数据报文直到其协议软件配置了IP地址的情况下，应将DHCPDISCOVER或DHCPREQUEST消息中的'flags'字段的广播位设置为1。这将提示DHCP服务器和BOOTP中继代理在客户端子网上广播任何消息。如果客户端能够在协议软件配置之前接收单播IP数据报文，则应将广播位清零为0。



Offer



➤ 引申思考：

□ 服务器发出的Offer报文，是广播？还是单播？

- 关键是看DHCP客户机在完成IP地址配置前，是否能接收单播报文！

- 有些IP协议栈在完成IP地址的配置前，是可以接收Destination IP = Any 的IP报文。而有些IP协议栈在完成IP地址的配置前，是不会接收任何单播IP报文的，只会接收广播IP报文，即Destination IP = 255.255.255.255。
- 这里有一个关键因素“广播位”！
 - 当一个客户端请求IP地址时，DHCP服务器或BOOTP中继代理会检查所收到报文中的广播位字段。如果这个位被设置，服务器或代理就会将消息广播到整个子网，而不是直接发送到特定的IP地址。这确保了即使客户端尚未获得IP地址，也能接收到必要的配置信息。

➤ 引申思考：



□ 服务器发出的Offer报文，是广播？还是单播？

■ “广播位”的应用 —— 服务器如何判断DHCP客户机能否接收单播报文？

- RFC2131规定：如果协议栈在初始化过程中，不能接收单播IP报文，则在DHCP Discover / Request报文的Flags字段里明确告知服务器，通过设置“BROADCAST flag = 1”，服务器就使用广播来和客户端通信。此时Offer和ACK报文就是广播报文。
- 如果协议栈在初始化过程中，可以接收单播IP报文，则在DHCP Discover / Request报文的Flags字段里明确告知服务器，通过设置“BROADCAST flag = 0”，服务器就使用单播来和客户端通信。此时Offer和ACK报文就是单播报文。
- 注意：Discover报文和Request报文，都是从DHCP客户端发出的报文。



Figure 1: Format of a DHCP message

➤ DHCP报文的结构

➤ 本例中，服务器发出的Offer报文是单播！

此处可看出，offer报文是单播！

No.	Source	Destination	Info
82	0.0.0.0	255.255.255.255	DHCP Discover - Tra
83	192.168.100.1	192.168.100.202	DHCP Offer - Tra
85	0.0.0.0	255.255.255.255	DHCP Request - Tra

> Frame 82: 410 bytes on wire (3280 bits), 410 bytes captured (3280)
> Ethernet II, Src: 54:89:98:f3:0a:28, Dst: ff:ff:ff:ff:ff:ff
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
▼ Dynamic Host Configuration Protocol (Discover)

Message type: Boot Request (1)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0x0000503f

Seconds elapsed: 0

> Bootp flags: 0x0000 (Unicast) (Unicast, 单播)

Client IP address: 0.0.0.0

Your (client) IP address: 0.0.0.0

注意，此处是Discover报文的内容！

若客户端发出的DHCP Discover或DHCP Request报文中，“Bootp flags: 0x0000 (Unicast)”，说明客户机请求DHCP服务器使用单播来发送回应报文。

➤ 另一例中，服务器发出的Offer报文，是广播。

可看出，此处offer报文是广播！

No.	Time	Source	Destination	Description		
91	14.054362	0.0.0.0	255.255.255.255	342	DHCP Discover	- Transaction ID 0x4
92	14.057984	172.16.1.201	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x4
93	14.058100	0.0.0.0	255.255.255.255	DHCP	340	DHCP Request - Transaction ID 0x4

Frame 91: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
> Ethernet II, Src: WistronI_af:28:e1 (f8:0f:41:af:28:e1), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
▼ Bootstrap Protocol (Discover)
 Message type: Boot Request (1)
 Hardware type: Ethernet (0x01)
 Hardware address length: 6
 Hops: 0
 Transaction ID: 0x4fc4a2c0
 Seconds elapsed: 0
 Bootp flags: 0x8000, Broadcast flag (Broadcast)
 Client IP address: 0.0.0.0
 Your (client) IP address: 0.0.0.0

注意，这是Discover报文的内容！

若客户端发出的DHCP Discover或DHCP Request报文中，“Bootp flags: 0x8000 (Broadcast)”，说明客户机请求DHCP服务器使用广播来发送回应报文。
(Broadcast, 广播)

另一例中，DHCP Discover报文部分信息

➤ 问题3：

□ DHCP服务器如何知道客户机选择/或未选择自己所提供的地址参数？

- Request报文中包含了哪些信息？



DHCP Request 首部地址信息与Discover相同



No.	Source	Destination	Protocol	Info
82	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Tran
83	192.168.100.1	192.168.100.202	DHCP	DHCP Offer - Tran
85	0.0.0.0	255.255.255.255	DHCP	<u>DHCP Request</u> - Tran
86	192.168.100.1	192.168.100.202	DHCP	DHCP ACK - Tran

- > Frame 85: 410 bytes on wire (3280 bits), 410 bytes captured (3280 b
- > Ethernet II, Src: 54:89:98:f3:0a:28, Dst: ff:ff:ff:ff:ff:ff
- > Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
- > User Datagram Protocol, Src Port: 68, Dst Port: 67
- < Dynamic Host Configuration Protocol (Request)

源IP: 0.0.0.0

目的IP:
255.255.255.255

源端口: 68 (客户端)
目的端口: 67 (服务器端)

报文内容见下页

抓包分析：DHCP Request报文 - 内容信息 (1)



Dynamic Host Configuration Protocol (Request) —————> 指明是Request报文

Message type: Boot Request (1)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

此时客户端的IP地址还是全0

Transaction ID: 0x0000503f

Seconds elapsed: 0

> Bootp flags: 0x0000 (Unicast)

Client IP address: 0.0.0.0

Your (client) IP address: 0.0.0.0

Next server IP address: 0.0.0.0

Relay agent IP address: 0.0.0.0

Client MAC address: 54:89:98:f3:0a:28

Client hardware address padding: 000000000000000000000000

Server host name not given

抓包分析：DHCP Request报文 - 内容信息 (2)



> Option: (53) DHCP Message Type (Request)

 ` Option: (54) DHCP Server Identifier (192.168.100.1)

 Length: 4

 DHCP Server Identifier: 192.168.100.1

DHCP服务器的标识(IP地址)
，表明客户机请求使用该服务器分配的IP地址

 ` Option: (50) Requested IP Address (192.168.100.202)

 Length: 4

 Requested IP Address: 192.168.100.202

客户机申请的IP地址

 ` Option: (61) Client identifier

 Length: 7

 Hardware type: Ethernet (0x01)

 Client MAC address: 54:89:98:f3:0a:28

客户端标识(即MAC地址)
表明“谁”在提出请求

 ` Option: (55) Parameter Request List

 Length: 4

 Parameter Request List Item: (1) Subnet Mask

 Parameter Request List Item: (3) Router

 Parameter Request List Item: (6) Domain Name Server

 Parameter Request List Item: (15) Domain Name

客户端所申请的网络参数
列表，包括子网掩码、默
认网关、DNS等信息。

> Option: (255) End

➤ 问题3：（抓包分析，结论）



□ DHCP服务器如何知道客户机选择了自己所提供的地址参数？

- DHCP客户机发出Discover报文后，有可能收到多个DHCP服务器回应的DHCP Offer报文，DHCP客户机一般只选择接受第一个收到的Offer报文。
- DHCP客户机收到Offer报文后，会根据该Offer报文中的服务器地址信息，发出DHCP Request报文。该报文中包含为该客户机提供IP配置的服务器的IP地址，表明客户机选中了哪台服务器。并且，DHCP Request是广播报文（目的IP是255.255.255.255），以便能通知到本网内所有的DHCP服务器。
- 注意，虽然此时客户机已经收到某个服务器提供的IP地址，但是因为还没有最终确认并配置该IP地址，所以，在DHCP Request报文中仍然使用0.0.0.0作为源IP地址。

➤ 问题4：

□ 客户机什么时候开始使用DHCP服务器提供的IP地址？



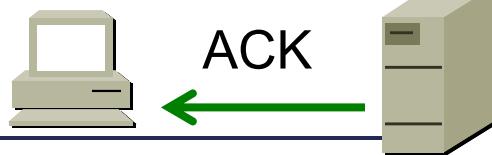
➤ 问题4：



□ 客户机什么时候开始使用DHCP服务器提供的IP地址？

- DHCP服务器接收到客户机发来的DHCP Request报文后，会查看报文中的服务器标识字段，以确定自己是否被选中。
 - 若未被选中，则取消前期的IP地址提供。
 - 若被选中，会返回DHCP ACK报文，作为最后的确认。
- DHCP ACK报文分析见下页

DHCP ACK报文首部地址信息与Offer报文相同



No.	Source	Destination	Protocol	Info
82	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID: 1
83	192.168.100.1	192.168.100.202	DHCP	DHCP Offer - Transaction ID: 1
85	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID: 1
86	192.168.100.1	192.168.100.202	DHCP	DHCP ACK - Transaction ID: 1

> Frame 86: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
> Ethernet II, Src: 08:00:27:c1:97:81, Dst: 54:89:98:f3:0a:28
> Internet Protocol Version 4, Src: 192.168.100.1, Dst: 192.168.100.202
> User Datagram Protocol, Src Port: 67, Dst Port: 68
▼ Dynamic Host Configuration Protocol (ACK)

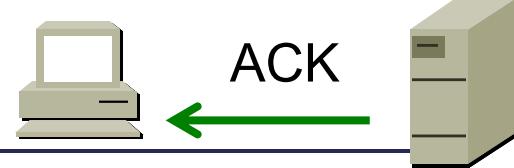
源MAC: 服务器MAC
目的MAC: 客户端MAC

报文内容见下页

源IP: 服务器IP
目的IP: 准备分配给客户端的IP

源端口: 67 (服务器端)
目的端口: 68 (客户端)

抓包分析：DHCP ACK报文 - 内容信息



Dynamic Host Configuration Protocol (ACK) DHCP消息类型

Message type: Boot Reply (2)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x0000503f
Seconds elapsed: 0
> Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 192.168.100.202
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: 54:89:98:f3:0a:28
Client hardware address padding: 000000000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
> Option: (53) DHCP Message Type (ACK)
> Option: (54) DHCP Server Identifier (192.168.100.1)
> Option: (51) IP Address Lease Time
> Option: (1) Subnet Mask (255.255.255.0)
> Option: (3) Router
> Option: (255) End

ACK报文的内容与Offer报文相似

准备分配给客户端的IP地址

表明ACK报文所响应的客户端的MAC地址

DHCP服务器标识

服务器提供给客户端的其他配置信息

➤ 问题4：（抓包分析，结论）



□ 客户机什么时候开始使用DHCP服务器提供的IP地址？

- 客户机收到DHCP ACK报文后，是否就可以直接配置自己的IP地址了？
- DHCP客户机收到DHCPACK报文后的动作
 - Client对所分配的网络参数进行最终检测和记录。例如地址复用（冲突）检测，如果所分配的地址已经被网络中其他主机占用，则Client会发送DECLINE报文（告诉服务器该地址不能用），随后在一定时间后重启DHCP交互过程。

➤ 问题5：

- DHCP客户机获得IP后，以后DHCP客户机每次重新启动时，如何与DHCP服务器联系？
 - DHCP客户机总是试图重新租用它接收过的最后一个IP地址，这给网络带来一定的稳定性。
 - 以后DHCP客户机每次重新登录网络时，就不需要再发送DHCP discover发现信息了，而是直接发送包含前一次所分配的IP地址的DHCP Request请求信息。
 - 当DHCP服务器收到这一信息后，它会尝试让DHCP客户机继续使用原来的IP地址，并回答一个DHCP ACK确认信息。

➤ 问题5：

□ DHCP客户机获得IP后，以后DHCP客户机每次重新启动时，如何与DHCP服务器联系？

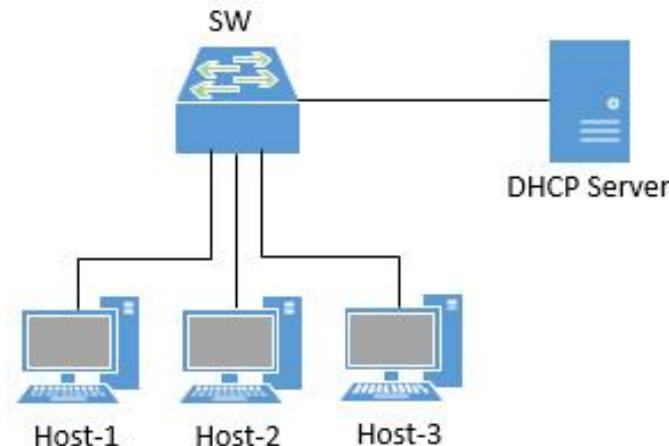
- 如果此IP地址已无法再分配给原来的DHCP客户机使用时（比如此IP地址已分配给其它DHCP客户机使用，或者因为客户机移到其他子网），则DHCP服务器给DHCP客户机回答一个DHCP nack否认信息。
- 当原来的DHCP客户机收到此DHCP nack否认信息后，它就必须重新发送DHCP discover发现信息来请求新的IP地址。

四、DHCP中继 (DHCP Relay)

DHCP中继

□ 为什么用到DHCP中继？

- 由于DHCP客户端在获取IP地址时，是通过广播方式发送报文的，因此DHCP协议是一个局域网（一个广播域）协议。
- 但是，通常一个园区网内部有多个局域网（即多个广播域），网络管理者并不愿意在每一个网络内都部署一台DHCP服务器，因为这样会使DHCP服务器的数量太多，采用DHCP中继（DHCP Relay）可以解决这一问题。



DHCP 中继

➤ IP地址规划：

Host-1: 192.168.0.1~192.168.0.100 /24

Host-2: 192.168.1.1~192.168.1.100 /24

Host-3: 192.168.2.1~192.168.2.100 /24

Host-4: 192.168.3.1~192.168.3.100 /24

Host-5: 192.168.4.1~192.168.4.100 /24

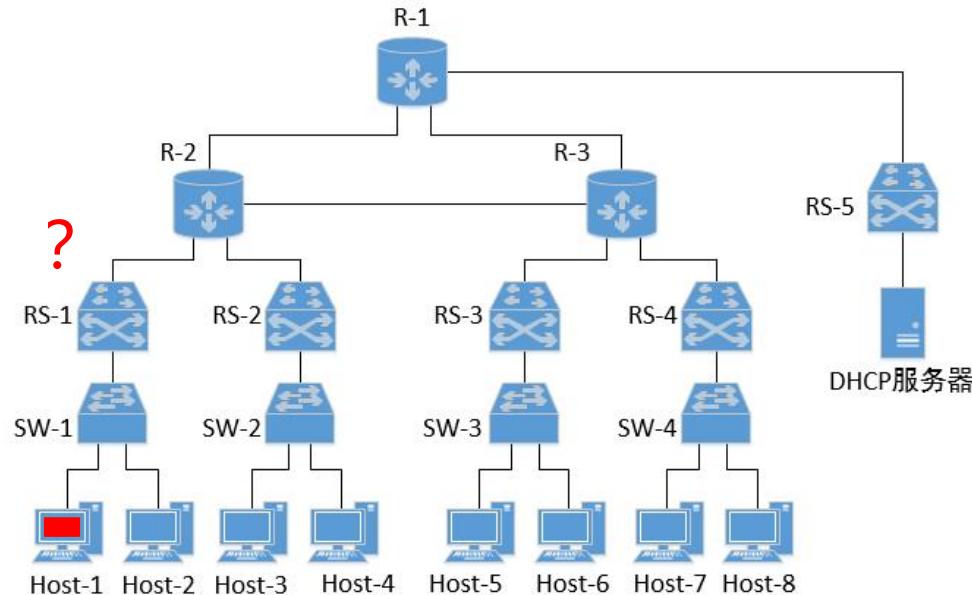
Host-6: 192.168.5.1~192.168.5.100 /24

Host-7: 192.168.6.1~192.168.6.100 /24

Host-8: 192.168.7.1~192.168.7.100 /24

DHCP服务器: 192.168.100.1 /24

注: PC分属于不同的VLAN



问题: Host-1发出的DHCP Discover
(发现报文) 能被谁收到?

DHCP 中继

□ 如何应用DHCP中继

- 为了使全网都能获得同一台DHCP服务器提供的服务，需要在每个子网络的默认网关处（想想为什么？），配置DHCP中继。
- 某个子网（或VLAN）中的主机通过DHCP中继获取IP地址的过程如下：
 1. DHCP客户机发出的DHCP报文（例如Discover）会首先到达本网络中的DHCP中继；
 2. DHCP中继上配置有DHCP服务器的IP地址信息，因此，DHCP中继会将收到的DHCP客户机发来的DHCP报文，转发给DHCP服务器；
 3. DHCP服务器发回的报文，会先到达DHCP中继，然后再由DHCP中继转发给DHCP客户机。
 4. 最终，DHCP客户机获取到IP地址。

➤ DHCP 中继配置举例（华为s5700）

➤ 分别给VLAN10、VLAN11的子网络配置DHCP中继：

[RS-1] dhcp enable

[RS-1] interface vlanif 10

[RS-1-Vlanif10] dhcp select relay

[RS-1-Vlanif10] dhcp relay server-ip 192.168.100.1

[RS-1-Vlanif10] quit

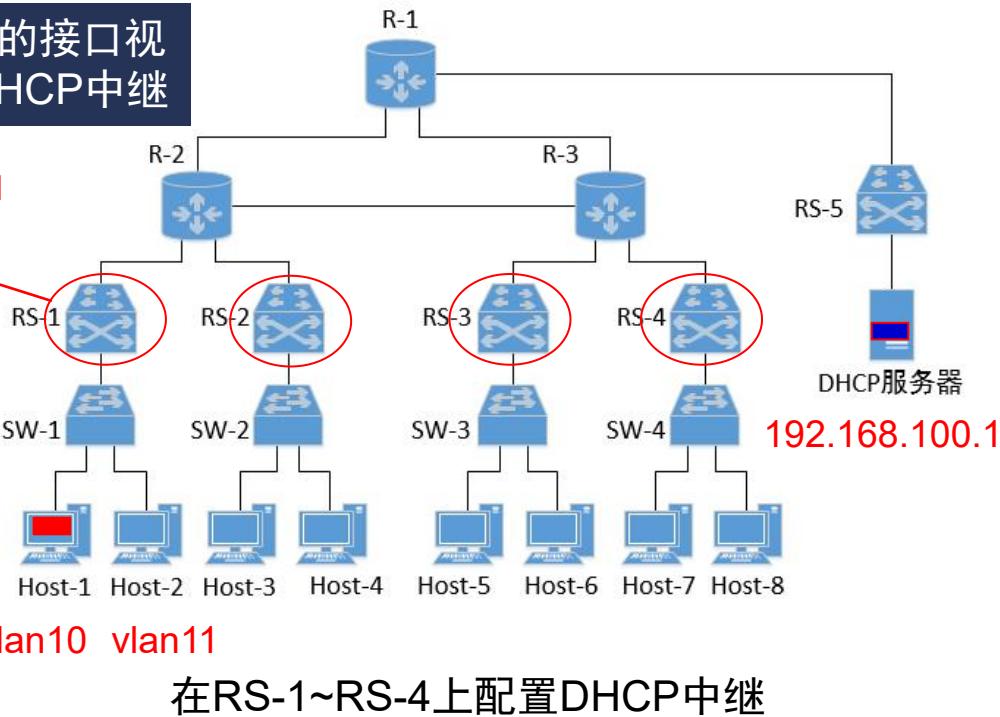
[RS-1] interface vlanif 11

[RS-1-Vlanif11] dhcp select relay

[RS-1-Vlanif11] dhcp relay server-ip 192.168.100.1

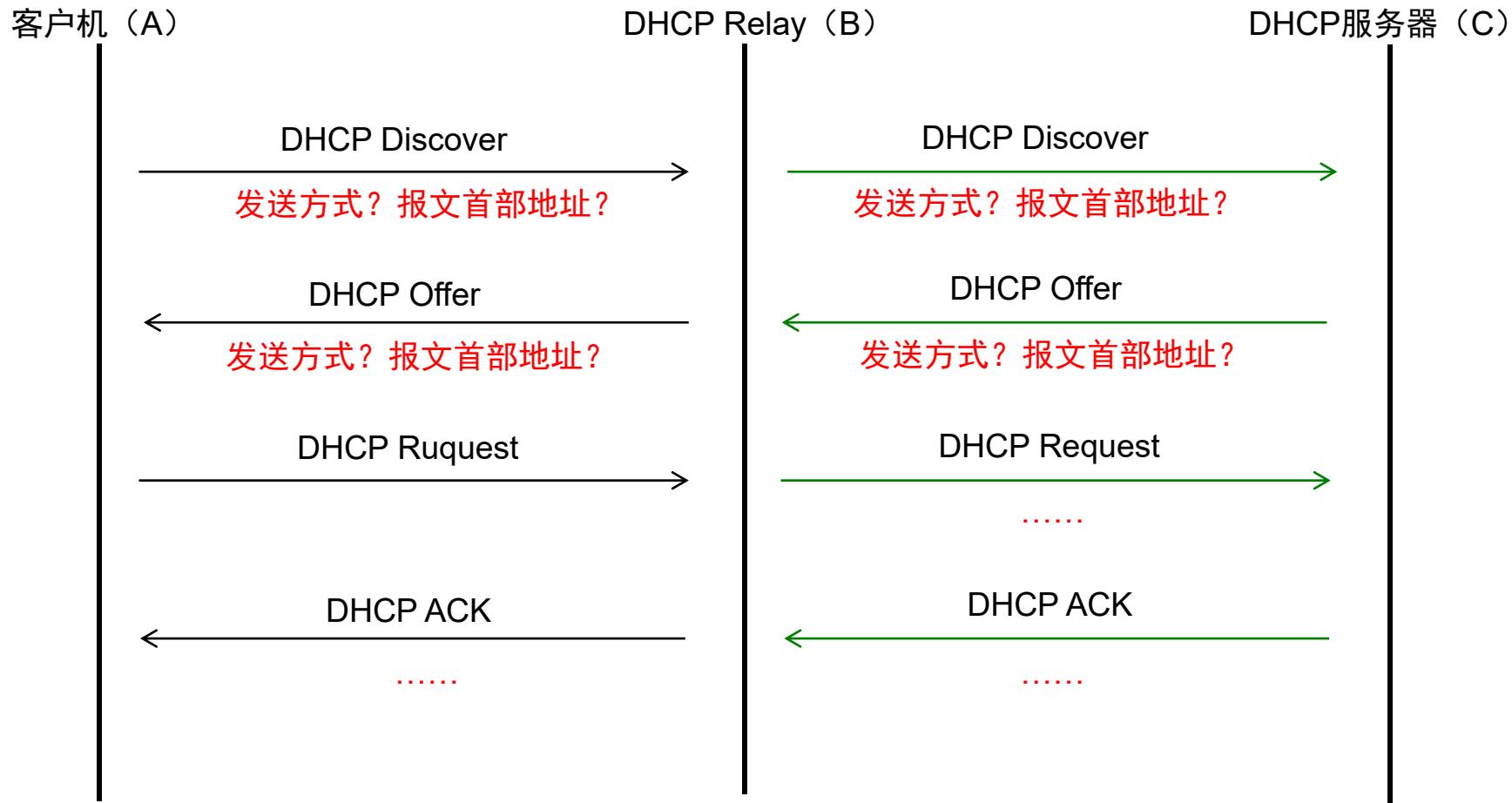
[RS-1-Vlanif11] quit

在VLAN10的接口视图中配置DHCP中继

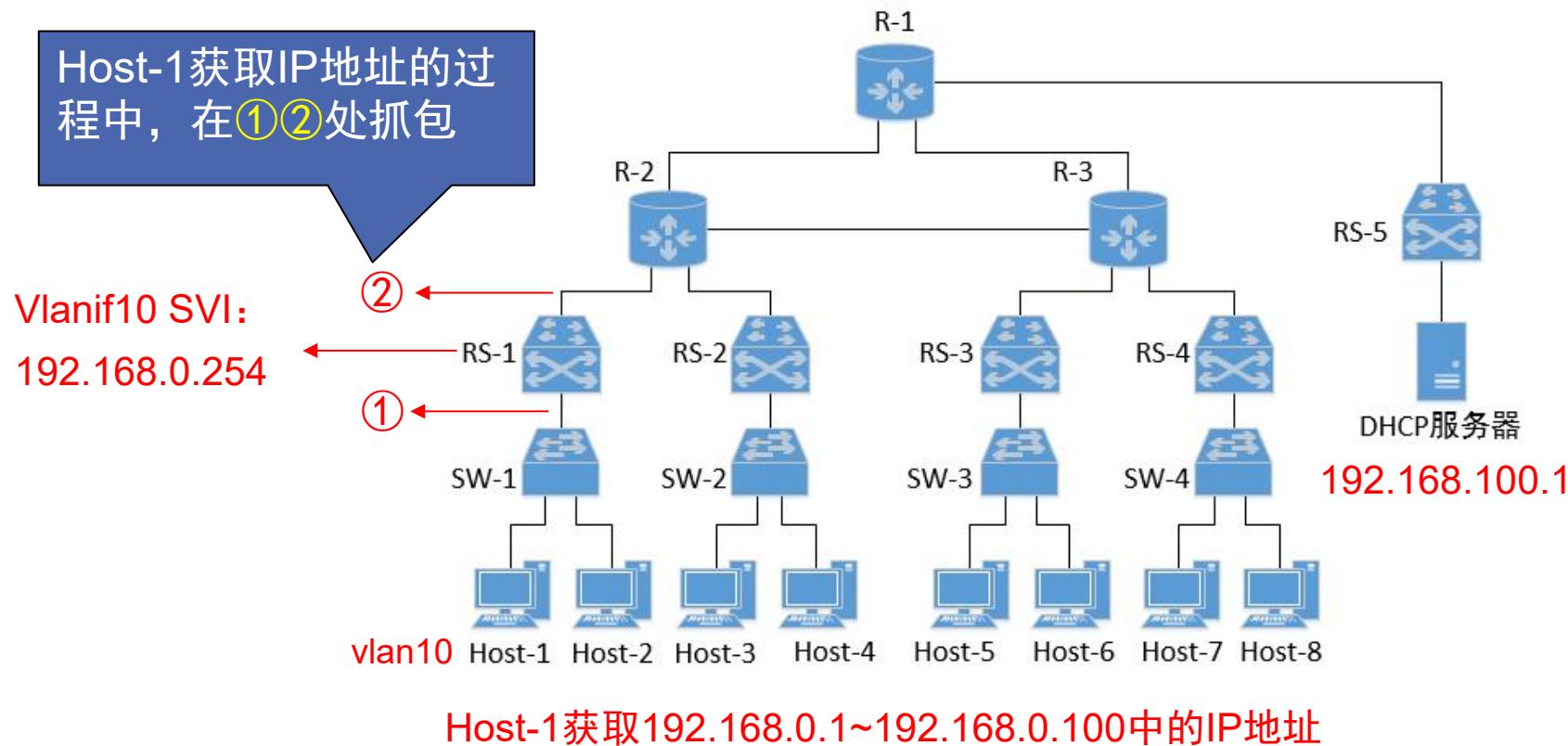


针对每个用户VLAN，在网关处配置DHCP中继。

深入思考：DHCP Relay转发报文时，首部地址如何变化？



■ 抓包分析DHCP Relay的工作过程



■ 抓包分析DHCP Relay的工作过程

Host-1 ↔ DHCP 中继 (RS-1)

1. Host-1发出DHCP DISCOVER广播报文，该报文可到达位于三层交换机RS-1的DHCP中继（即vlanif10）。

①

No.	Time	Source	Destination	Protocol	Length	Info
3	3.525000	0.0.0.0	255.255.255.255	DHCP	414	DHCP Discover -
4	3.619000	192.168.100.1	192.168.0.1	DHCP	346	DHCP Offer -
7	5.522000	0.0.0.0	255.255.255.255	DHCP	414	DHCP Request -
8	5.584000	192.168.100.1	192.168.0.1	DHCP	346	DHCP ACK -

2. Vlanif10发现这是一个DISCOVER报文，根据管理员配置的DHCP服务器地址，将该报文重新封装后发给DHCP服务器（单播报文），首部地址如图所示。报文中包含客户端MAC和中继的IP

②

No.	Time	Source	Destination	Protocol	Length	Info
5	6.489000	192.168.0.254	192.168.100.1	DHCP	410	DHCP Discover -
6	6.552000	192.168.100.1	192.168.0.254	DHCP	342	DHCP Offer -
9	8.455000	192.168.0.254	192.168.100.1	DHCP	410	DHCP Request -
10	8.502000	192.168.100.1	192.168.0.254	DHCP	342	DHCP ACK -

Vlanif10: 192.168.0.254

DHCP服务器: 192.168.100.1

Host-1获取IP: 192.168.0.1

■ 抓包分析DHCP Relay的工作过程

Host-1 ←→ DHCP 中继 (RS-1)

- DHCP中继收到服务器发回的offer报文后，根据报文中的客户端MAC和所分配的IP地址，对offer报文重新封装后，发给客户端（单播）

①

No.	Time	Source	Destination	Protocol	Length	Info
3	3.525000	0.0.0.0	255.255.255.255	DHCP	414	DHCP Discover -
4	3.619000	192.168.100.1	192.168.0.1	DHCP	346	DHCP Offer -
7	5.522000	0.0.0.0	255.255.255.255	DHCP	414	DHCP Request -
8	5.584000	192.168.100.1	192.168.0.1	DHCP	346	DHCP ACK -

- DHCP服务器从收到的discover报文中获取了DHCP中继的IP地址和客户端的MAC地址，然后向DHCP中继发回offer报文（单播报文），报文首部的IP地址如图所示。

②

No.	Time	Source	Destination	Protocol	Length	Info
5	6.489000	192.168.0.254	192.168.100.1	DHCP	410	DHCP Discover -
6	6.552000	192.168.100.1	192.168.0.254	DHCP	342	DHCP Offer -
9	8.455000	192.168.0.254	192.168.100.1	DHCP	410	DHCP Request -
10	8.502000	192.168.100.1	192.168.0.254	DHCP	342	DHCP ACK -

Vlanif10: 192.168.0.254

DHCP服务器: 192.168.100.1

Host-1获取IP: 192.168.0.1

■ 抓包分析DHCP Relay的工作过程

Host-1 ↔ DHCP 中继 (RS-1)

5. Host-1发出request报文（包含所申请的地址信息等），广播报文，该报文可到达位于三层交换机RS-1的DHCP中继（即vlanif10）。

No.	Time	Source	Destination	Protocol	Length	Info
3	3.525000	0.0.0.0	255.255.255.255	DHCP	414	DHCP Discover -
4	3.619000	192.168.100.1	192.168.0.1	DHCP	346	DHCP Offer -
7	5.522000	0.0.0.0	255.255.255.255	DHCP	414	DHCP Request -
8	5.584000	192.168.100.1	192.168.0.1	DHCP	346	DHCP ACK -

①

DHCP 中继 (RS-1) ↔ DHCP服务器

6. Vlanif10发现这是一个request报文，根据管理员配置的DHCP服务器地址，将该报文重新封装后发给DHCP服务器（单播报文），首部地址如图所示。报文中包含客户端MAC和中继的IP

No.	Time	Source	Destination	Protocol	Length	Info
5	6.489000	192.168.0.254	192.168.100.1	DHCP	410	DHCP Discover -
6	6.552000	192.168.100.1	192.168.0.254	DHCP	342	DHCP Offer -
9	8.455000	192.168.0.254	192.168.100.1	DHCP	410	DHCP Request -
10	8.502000	192.168.100.1	192.168.0.254	DHCP	342	DHCP ACK -

②

Vlanif10: 192.168.0.254

DHCP服务器: 192.168.100.1

Host-1获取IP: 192.168.0.1

■ 抓包分析DHCP Relay的工作过程

Host-1 ↔ DHCP 中继 (RS-1)

- DHCP中继收到服务器发回的ACK报文后，根据报文中的客户端MAC和所分配的IP地址，对ACK报文重新封装后，发给客户端（单播）

①

No.	Time	Source	Destination	Protocol	Length	Info
3	3.525000	0.0.0.0	255.255.255.255	DHCP	414	DHCP Discover -
4	3.619000	192.168.100.1	192.168.0.1	DHCP	346	DHCP Offer -
7	5.522000	0.0.0.0	255.255.255.255	DHCP	414	DHCP Request -
8	5.584000	192.168.100.1	192.168.0.1	DHCP	346	DHCP ACK -

- DHCP服务器从收到的request报文中获取了DHCP中继的IP地址和客户端的MAC地址，然后向DHCP中继发回ACK报文（单播报文），报文头部的IP地址如图所示。

②

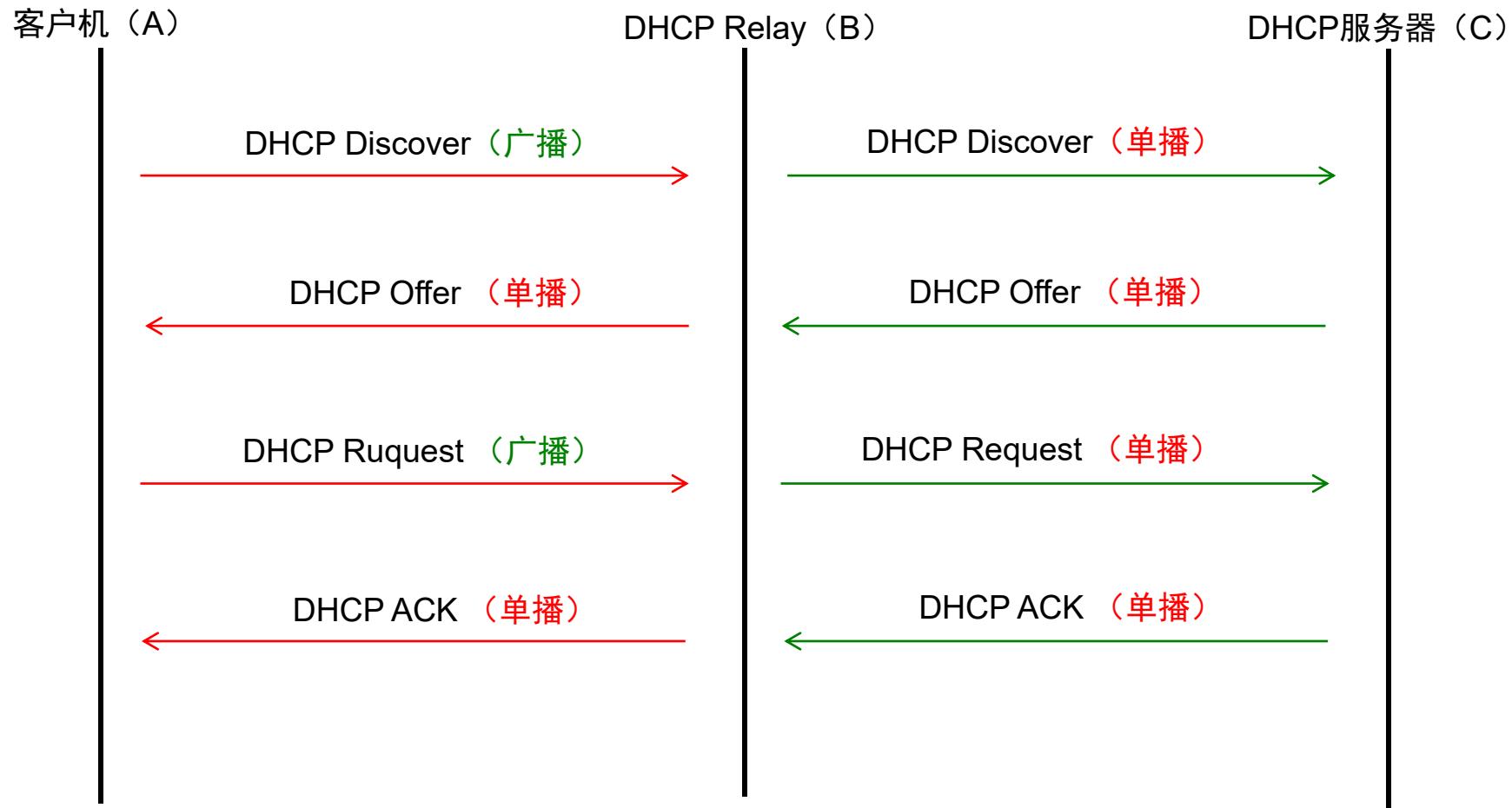
No.	Time	Source	Destination	Protocol	Length	Info
5	6.489000	192.168.0.254	192.168.100.1	DHCP	410	DHCP Discover -
6	6.552000	192.168.100.1	192.168.0.254	DHCP	342	DHCP Offer -
9	8.455000	192.168.0.254	192.168.100.1	DHCP	410	DHCP Request -
10	8.502000	192.168.100.1	192.168.0.254	DHCP	342	DHCP ACK -

Vlanif10: 192.168.0.254

DHCP服务器: 192.168.100.1

Host-1获取IP: 192.168.0.1

DHCP Relay的工作过程（假设DHCP客户端能接收单播报文）

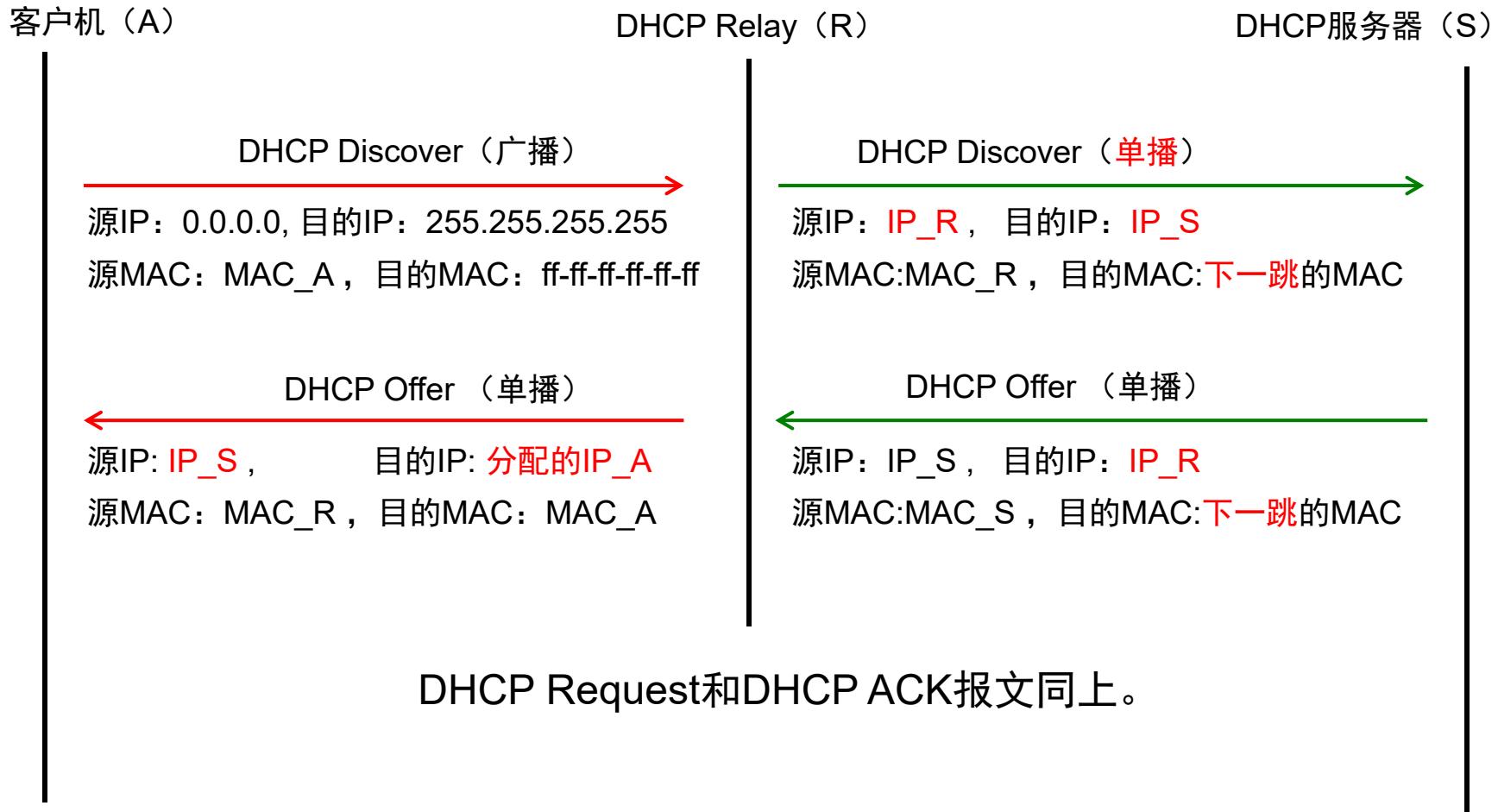


DHCP 中继代理

□ DHCP中继的工作特点

- DHCP客户端通过DHCP中继代理从DHCP服务器获取IP地址的过程与直接从DHCP服务器获取IP地址的过程相类似，都需要经历发现、提供、选择和确认四个阶段。
- 中继代理只是充当一个中介代理角色，负责转发DHCP客户端与DHCP服务器之间交互的请求和应答报文。
- **但是**，DHCP中继在转发DHCP报文时，需要重新封装报文，因此报文首部的地址会发生变化。总结如下页

➤ DHCP Relay工作过程中报文首部地址变化 (假设客户端能接收单播报文)



五、DHCP安全（自主学习）

5.1 DHCP中存在的安全问题

DHCP中存在的安全问题

- 目前DHCP协议（RFC2131）在应用的过程中遇到很多安全方面的问题，网络中存在一些针对DHCP的攻击。DHCP在设计上未充分考虑到安全因素，从而留下了许多安全漏洞，使得DHCP很容易受到攻击。实际网络中，针对DHCP的攻击行为主要有以下四种：
 - DHCP Server拒绝服务攻击（又称饿死攻击）
 - 仿冒DHCP Server攻击
 - 仿冒DHCP 报文攻击
 - DHCP中间人攻击

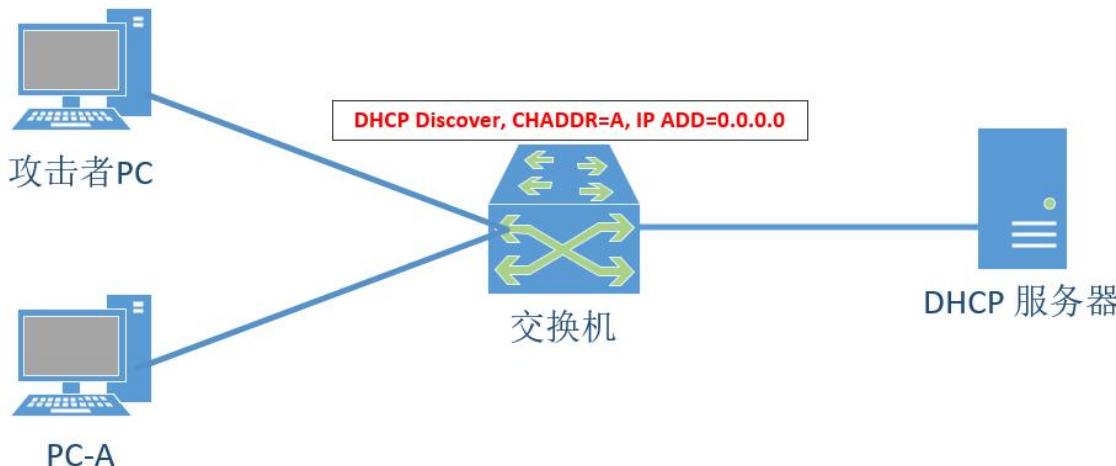
DHCP中存在的安全问题

□ DHCP饿死攻击

- 攻击原理：攻击者持续大量的向DHCP Server申请IP地址，直到耗尽DHCP Server地址池中的IP地址，导致DHCP Server不能给正常的用户进行分配。

攻击者通过不断修改DHCP报文中的
CHADDR字段值,持续大量地向DHCP
Server申请IP地址

chaddr 字段：客户端硬件地址 (Client Hardware Address)



DHCP中存在的安全问题

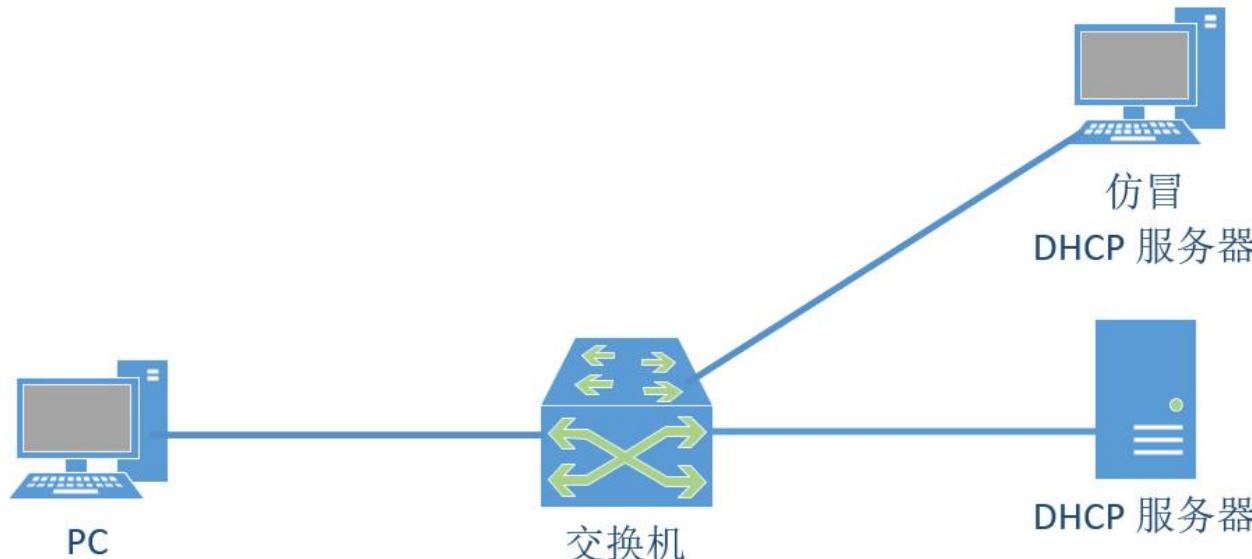
□ DHCP饿死攻击

- **漏洞分析：** DHCP Server在向申请者提供IP地址时，无法区分正常的申请者与恶意的申请者。
- **协议原理：** DHCP Server通常仅根据DHCP Request报文中的CHADDR (Client Hardware Address) 字段来确认客户端的MAC地址。如果攻击者通过不断的修改CHADDR字段向DHCP Server申请地址，就会导致DHCP Server中的IP地址耗尽，从而无法为其它正常用户提供DHCP服务。
- **产生危害：** 用户无法正常获取到IP地址，IP地址被浪费掉。

DHCP中存在的安全问题

□ 仿冒DHCP Server攻击

- 攻击描述：攻击者仿冒DHCP Server向客户端分配错误的IP地址以及错误的网关等信息，导致用户无法正常的访问网络。



DHCP中存在的安全问题

□ 仿冒DHCP Server攻击

- **漏洞分析：** DHCP客户端收到DHCP Server的DHCP消息之后，无法区分这些DHCP消息是来自仿冒的DHCP Server还是合法的DHCP Server。
- **攻击原理：** DHCP Discover报文是广播报文，无论是合法的DHCP Server，还是非法的DHCP Server都可以接收到DHCP Client发送的DHCP Discover报文。因为DHCP客户端会接收第一个发送DHCP Offer报文的数据，然后使用第一个接收到的DHCP Server发送的IP地址，然而在现实中，DHCP Server往往都是使用代理进行分配的，所以攻击者只要把设备放在同DHCP客户端同一个的网段中，往往都会比真正的DHCP服务器回复速度快。
- **产生危害：** 用户获取到错误的地址网关等，数据包可能经由恶意的设备，造成信息泄露等。用户可能无法正常使用网络。

DHCP中存在的安全问题

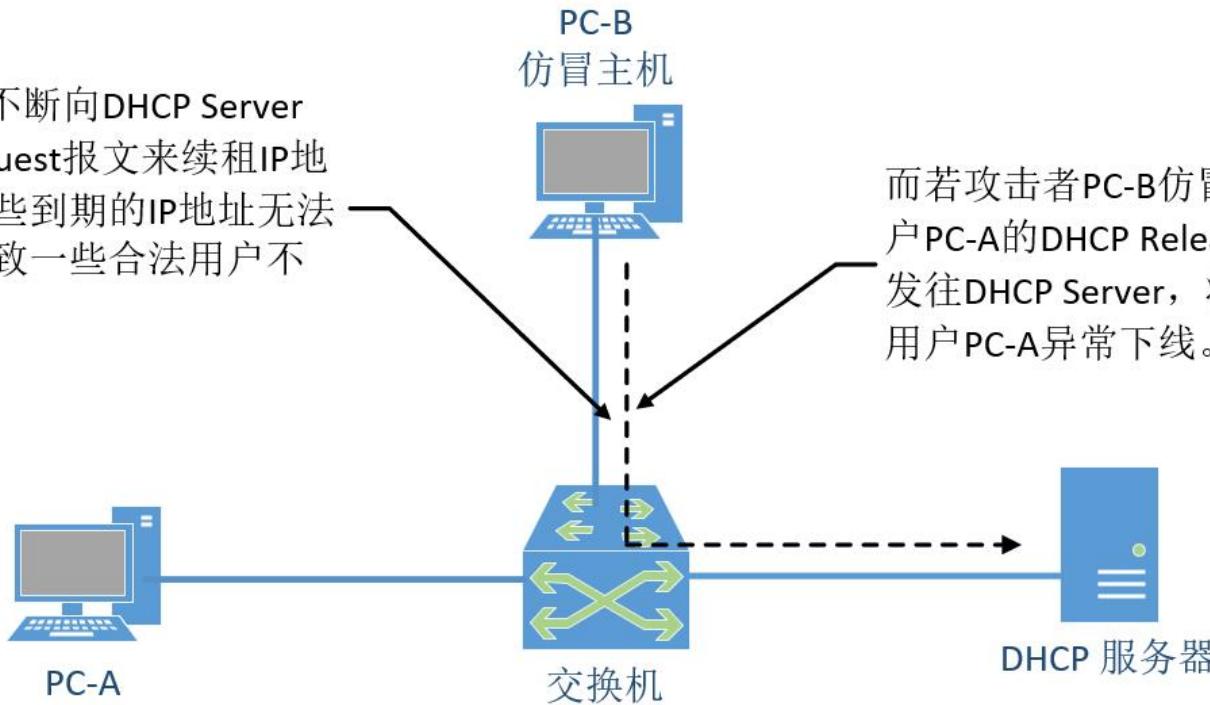
□ 仿冒DHCP 报文攻击

- 攻击原理：DHCP服务器在主机提出续租或释放请求时，一般都会满足主机。

PC-B冒充PC-A不断向DHCP Server发送DHCP Request报文来续租IP地址，会导致这些到期的IP地址无法正常回收，以致一些合法用户不能获得IP地址。

PC-B
仿冒主机

而若攻击者PC-B仿冒合法用户PC-A的DHCP Release报文发往DHCP Server，将会导致用户PC-A异常下线。



DHCP中存在的安全问题

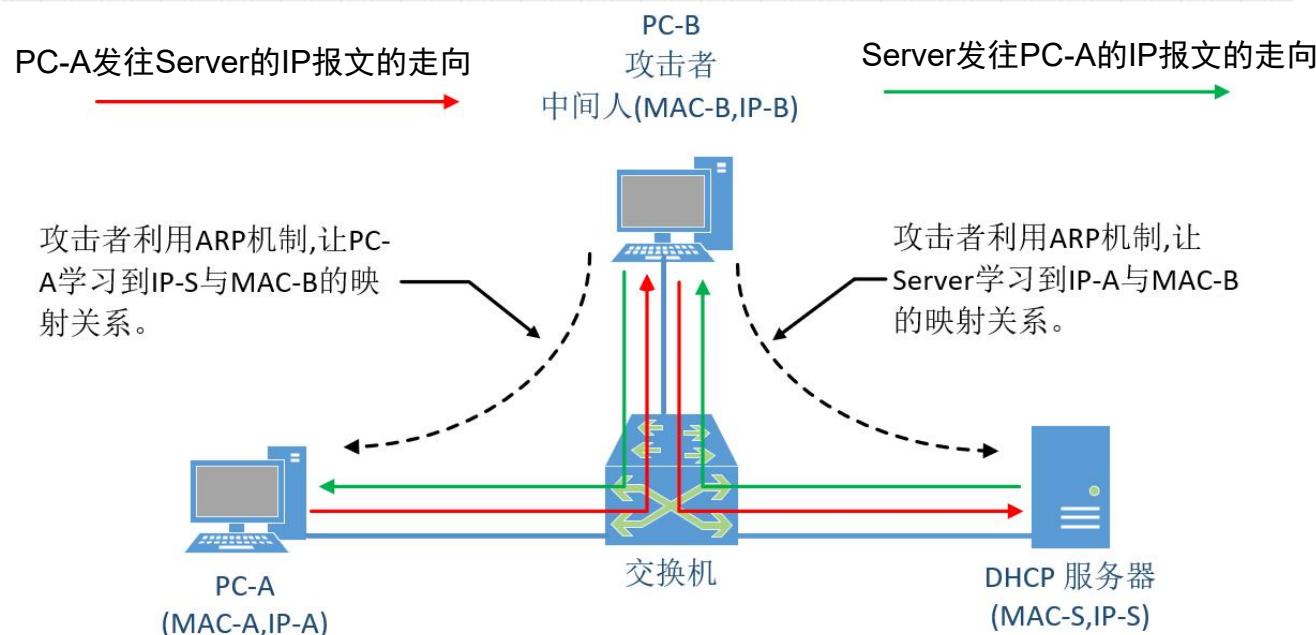
□ 仿冒DHCP 报文攻击

- 漏洞分析：DHCP Server收到主机发来的DHCP消息之后，无法区分这些DHCP消息是来自仿冒的主机还是合法主机。
- 产生危害：主机无法获取IP或者不正常下线。

DHCP中存在的安全问题

□ DHCP中间人攻击

- 攻击原理：攻击者利用ARP机制，让PC-A学习到IP-S与MAC-B的映射关系（就是让PC-A认为DHCP Server是PC-B），又让Server学习到IP-A与MAC-B的映射关系。这样一来PC-A与Server之间交互的IP报文都会经过攻击者中转。



DHCP中存在的安全问题

□ DHCP中间人攻击

- 漏洞分析：从本质上讲，中间人攻击是一种Spoofing IP/MAC攻击，中间人利用了虚假的IP地址与MAC地址之间的映射关系来同时欺骗DHCP客户端和服务器。
- 产生危害：造成信息泄露等。

5. 2 DHCP Snooping的应用

DHCP Snooping的应用

□ 什么是DHCP Snooping?

- DHCP Snooping是DHCP的一种安全特性，用于保证DHCP客户端从合法的DHCP服务器获取IP地址，并记录DHCP客户端IP地址与MAC地址等参数的对应关系，防止网络上针对DHCP攻击。
- DHCP Snooping部署在交换机上，其作用类似于在DHCP客户端与DHCP服务器端之间构筑了一道虚拟的防火墙，以抵御网络中针对DHCP的各种攻击。
- DHCP Snooping分为DHCPv4 Snooping和DHCPv6 Snooping，两者实现原理相似，本讲以DHCPv4 Snooping为例进行描述
- DHCP Snooping尚未有统一的标准规范，不同的网络设备制造商在DHCP Snooping的实现上也不尽相同。（不同厂商的DHCP Snooping设置会有差别）。本讲以华为设备为例。

DHCP Snooping的应用

□ DHCP Snooping实现DHCP安全的两种方式

■ DHCP Snooping主要通过以下两种方式加强DHCP的安全性：

- **DHCP Snooping信任功能：** 防范非法DHCP Server，保证客户端从合法的服务器获取IP地址。
- **DHCP Snooping绑定表：** 防范非法DHCP Client，使得交换机接收DHCP客户端发来的DHCP报文时，会进行匹配检查，能够有效防范非法用户的攻击。

DHCP Snooping的应用

□ DHCP Snooping信任功能（防范非法DHCP Server）

- 网络中如果存在私自架设的DHCP Server仿冒者，则可能导致DHCP客户端获取错误的IP地址和网络配置参数，无法正常通信。
- DHCP Snooping信任功能可以控制DHCP服务器应答报文的来源，以防止网络中可能存在的DHCP Server仿冒者为DHCP客户端分配IP地址及其他配置信息。
 - 简单的说，就是通过配置Snooping功能，使得交换机（接口）只转发合法的DHCP服务器的DHCP OFFER/ACK/NAK报文，丢弃非法的DHCP服务器的DHCP OFFER/ACK/NAK报文，从而达到阻断非法DHCP服务器的目的。

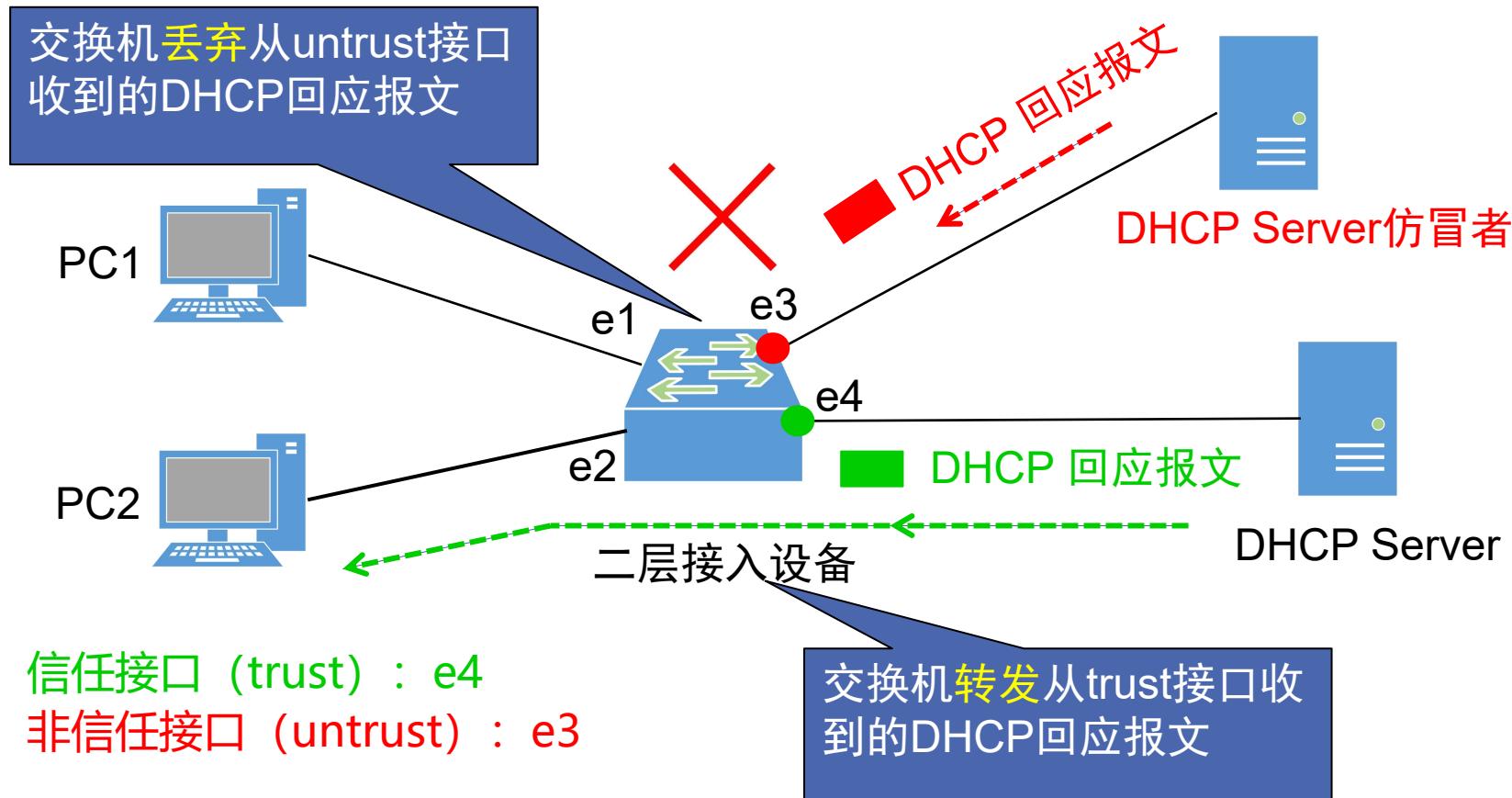
DHCP Snooping的应用

□ DHCP Snooping信任功能（防范非法DHCP Server）

■ DHCP Snooping信任功能的实现方式

- 为了防止仿冒的DHCP Server攻击，可以设置交换机的“信任/非信任”的工作模式。将与合法DHCP服务器直接或间接连接的接口设置为**信任接口**，其他接口设置为**非信任接口**。
- **信任接口：**正常接收DHCP服务器响应的DHCP ACK、DHCP NAK和DHCP Offer报文。另外，设备只会将DHCP客户端的DHCP请求报文通过信任接口发送给合法的DHCP服务器。（**让信任接口对应合法DHCP服务器**）
- **非信任接口：**在接收到DHCP服务器响应的DHCP ACK、DHCP NAK和DHCP Offer报文后，丢弃该报文。（**让非信任接口对应非法DHCP服务器**）
- **结果：**通过DHCP Snooping信任功能，从而保证DHCP客户端只能从合法的DHCP服务器获取IP地址，DHCP Server仿冒者无法为DHCP客户端分配IP地址

◆ 举例：DHCP Snooping信任功能防止仿冒Server



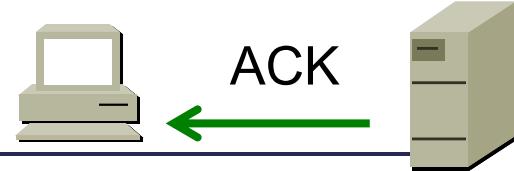
DHCP Snooping的应用

□ DHCP Snooping绑定表： (防范非法DHCP Client)

■ 绑定表的形成

- DHCP客户端（PC）通过广播形式发送DHCP请求报文，使能了DHCP Snooping功能的二层接入设备将其通过信任接口转发给DHCP服务器。最后DHCP服务器将含有IP地址信息的DHCP ACK报文通过单播的方式发送给客户端（PC）。
- 在这个过程中，二层接入设备收到DHCP ACK报文后，会从该报文中（回忆一下）提取关键信息（包括PC的MAC地址、获取到的IP地址、地址租期），并获取与PC连接的使能了DHCP Snooping功能的接口信息（包括接口编号及该接口所属的VLAN），根据这些信息生成DHCP Snooping绑定表。
- 举例

回忆一下：DHCP ACK报文的内容信息



Dynamic Host Configuration Protocol (ACK)

Message type: Boot Reply (2)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x0000503f
Seconds elapsed: 0
> Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 192.168.100.202 → 准备分配给客户端的IP地址
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: 54:89:98:f3:0a:28 → 表明ACK报文所响应的客户端的MAC地址
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
> Option: (53) DHCP Message Type (ACK)
> Option: (54) DHCP Server Identifier (192.168.100.1) → DHCP服务器标识
> Option: (51) IP Address Lease Time
> Option: (1) Subnet Mask (255.255.255.0)
> Option: (3) Router
> Option: (255) End

ACK报文的内容与Offer报文相似

DHCP消息类型

DHCP服务器标识

服务器提供给客户端的其他配置信息

◆ 举例：DHCP Snooping绑定表的生成

➤ 信任接口：e4

DHCP Snooping绑定表			
IP地址	MAC地址	VLAN	接口
192.168.1.1	MAC1	2	e1
192.168.2.1	MAC2	3	e2

PC1 (VLAN2)

MAC1
获取IP：
192.168.1.1

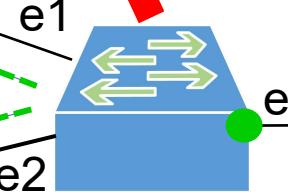


PC2 (VLAN3)

MAC2
获取IP：
192.168.2.1



二层接入设备



以PC1为例，交换机从DHCP ACK报文中提取IP和MAC，再获取与PC1连接的接口信息e1，生成一条绑定表项。

DHCP ACK报文



DHCP Server

DHCP Snooping的应用

□ DHCP Snooping绑定表： (防范非法DHCP Client)

■ 绑定表的应用

- 使能了DHCP Snooping的设备生成DHCP Snooping绑定表后，设备可根据绑定表项，对DHCP报文进行匹配检查，只有匹配成功的报文设备才将其转发，否则将丢弃。这将能有效的防止非法用户通过发送伪造DHCP报文冒充合法用户进行续租或释放IP地址。
- 举例

DHCP Snooping的应用

□ DHCP Snooping绑定表应用

■ 例1：防止DHCP Server服务拒绝攻击导致部分用户无法上线

- DHCP Server通常仅根据DHCP Request报文中的CHADDR (Client Hardware Address) 字段来确认客户端的MAC地址。若攻击者通过不断修改DHCP请求报文中的CHADDR (客户端MAC地址) 字段值，让DHCP服务器误认为是来自不同PC的用户申请IP地址，造成大量地址被非法占用。
- 解决：开启DHCP Snooping绑定表功能之后，可使能设备检测DHCP Request报文帧头MAC与DHCP数据区中CHADDR字段是否一致功能，此后设备（交换机）将检查收到的DHCP Request报文中的帧头MAC地址是否与CHADDR值相等，相等则转发，否则丢弃。

DHCP Snooping的应用

□ DHCP Snooping绑定表应用

■ 例1：防止DHCP Server服务拒绝攻击导致部分用户无法上线

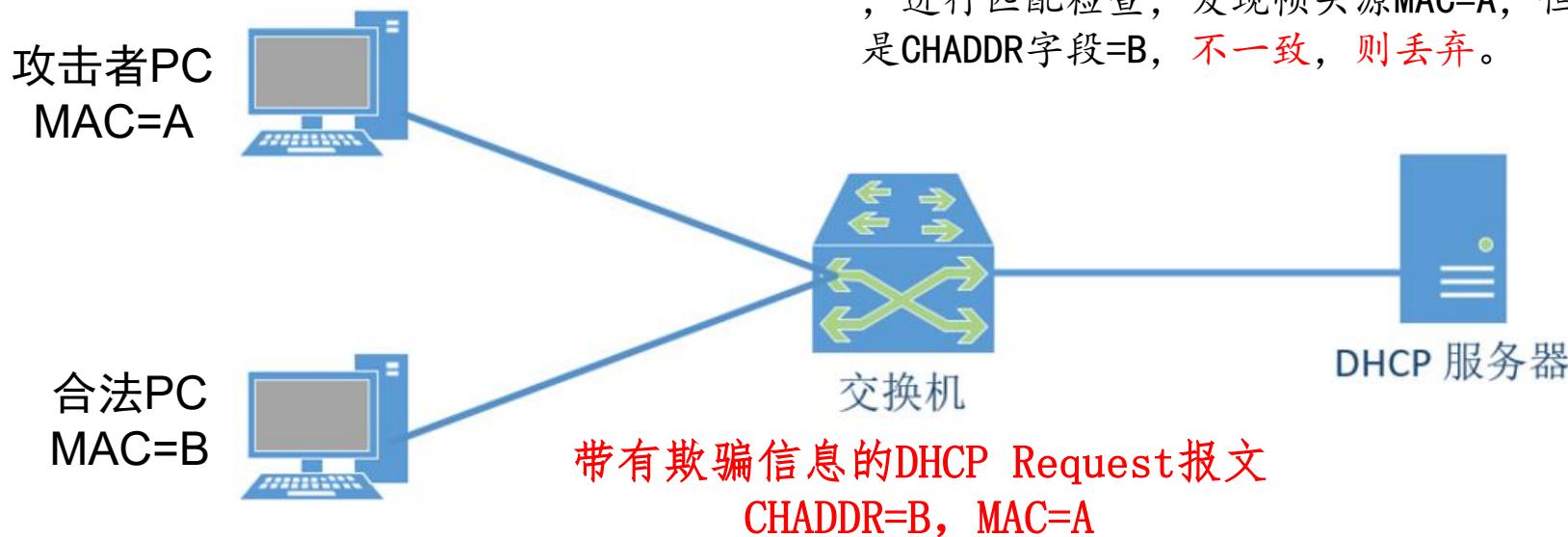
➤ 相关命令

- 执行命令`system-view`，进入系统视图。
- 执行命令`dhcp snooping check dhcp-request enable vlan {vlan-id}`，开启对从指定VLAN内上送的DHCP请求报文进行绑定表匹配检查的功能。缺省情况下，未开启此功能。
- 执行命令`dhcp snooping check dhcp-chaddr enable vlan {vlan-id}`，开启检测DHCP Request报文帧头源MAC地址与CHADDR字段是否相同的功能。缺省情况下，未开启此功能。

➤ 举例见下页

◆ 例1：防止DHCP Server服务拒绝攻击

攻击者通过不断修改DHCP请求报文中的CHADDR字段值，持续大量地向DHCP服务器申请IP地址



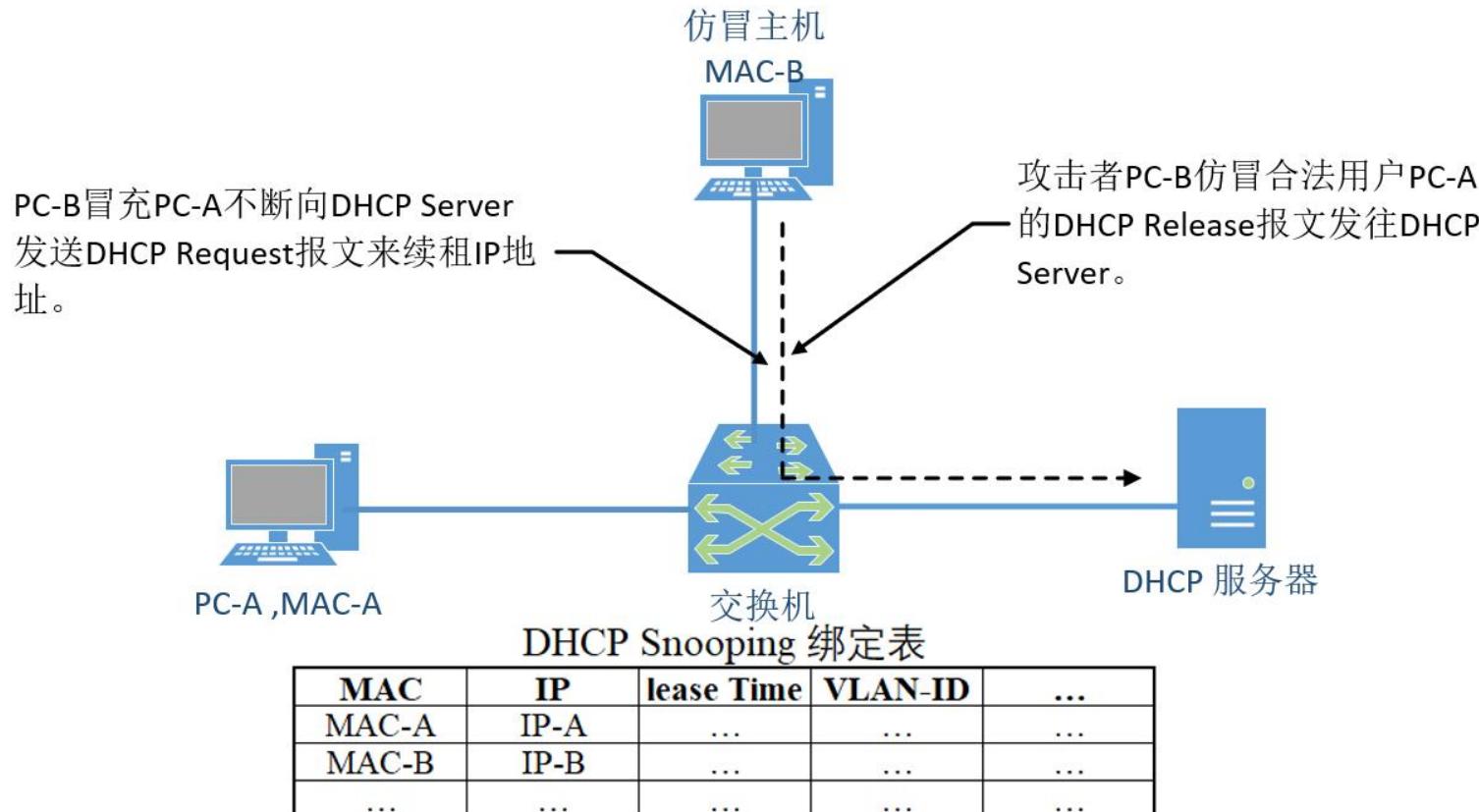
DHCP Snooping的应用

□ DHCP Snooping绑定表应用

■ 例2：防止仿冒DHCP报文攻击导致合法用户无法获得IP地址或异常下线

- 攻击原理：已获取到IP地址的合法用户通过向服务器发送DHCP Request或DHCP Release报文用以续租或释放IP地址。如果攻击者冒充合法用户不断向DHCP Server发送DHCP Request报文来续租IP地址，会导致这些到期的IP地址无法正常回收，以致一些合法用户不能获得IP地址；而若攻击者仿冒合法用户的DHCP Release报文发往DHCP Server，将会导致用户异常下线。
- 解决方法：为了有效的防止仿冒DHCP报文攻击，可利用DHCP Snooping绑定表的功能。设备通过将DHCP Request续租报文和DHCP Release报文与绑定表进行匹配操作能够有效的判别报文是否合法（主要是检查报文中的VLAN、IP、MAC、接口信息是否匹配动态绑定表），若匹配成功则转发该报文，匹配不成功则丢弃。

◆ 例2：防止仿冒DHCP报文攻击



DHCP Snooping的应用

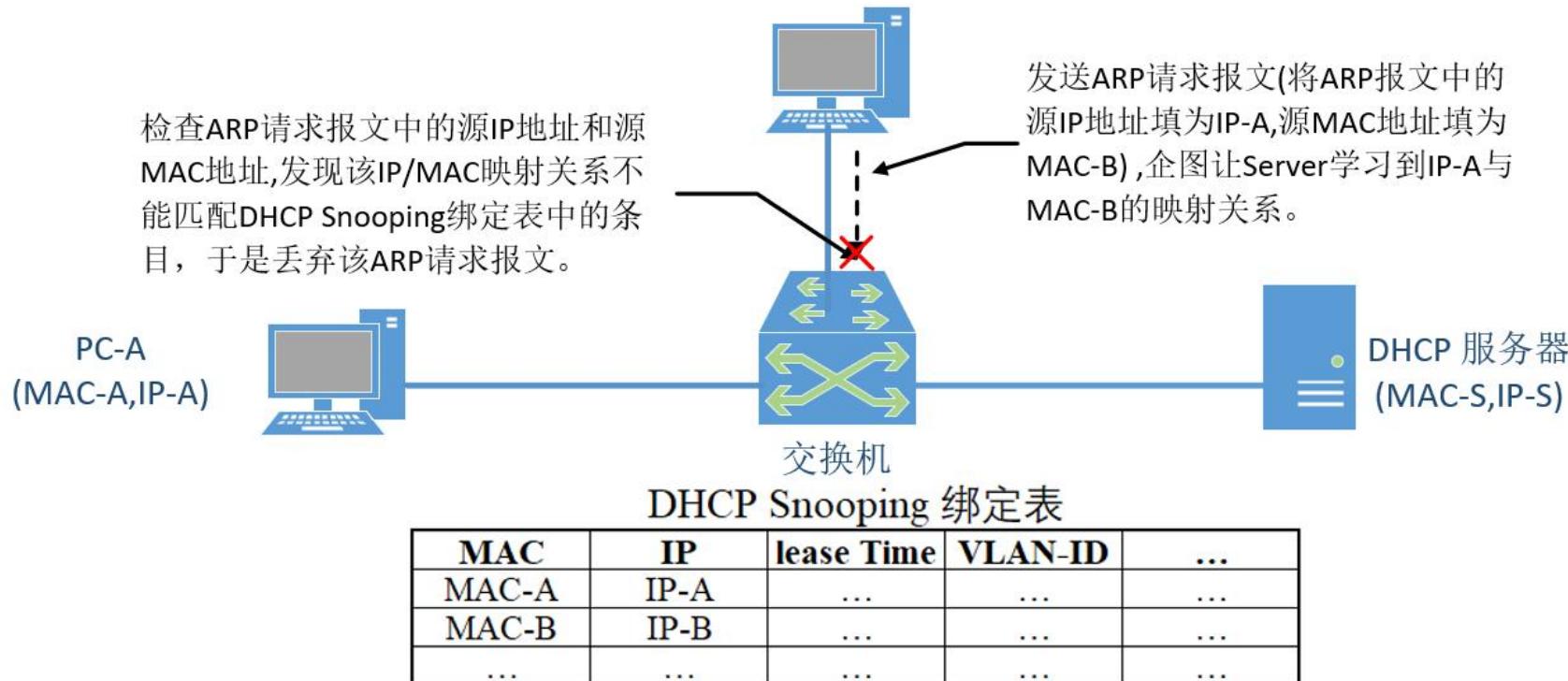
□ DHCP Snooping绑定表应用

■ 例3：防止中间人攻击

- 攻击原理：DHCP的数据包中本身含有IP地址和MAC地址的对应关系，中间人攻击主要就是让IP与MAC不对应，然后让别人发包时往错误的方向进行发送。
- 解决方法：当交换机开启了DHCP Snooping绑定表的功能，这张表中就有从DHCP报文中解析出来的IP与MAC对应信息。通过对收到的报文（ARP报文）进行匹配检查，如果报文中IP与MAC对应关系与绑定表不一致，则会将报文丢弃。
- 举例见下页

◆ 例3：防止中间人攻击

PC-B , 攻击者 , 中间人 , (MAC-B,IP-B)



第8讲 使用DHCP管理IP地址

完