

网络运维管理

第6讲 使用DHCP管理园区网IP地址

河南中医药大学信息技术学院
《网络运维管理》课程教学组

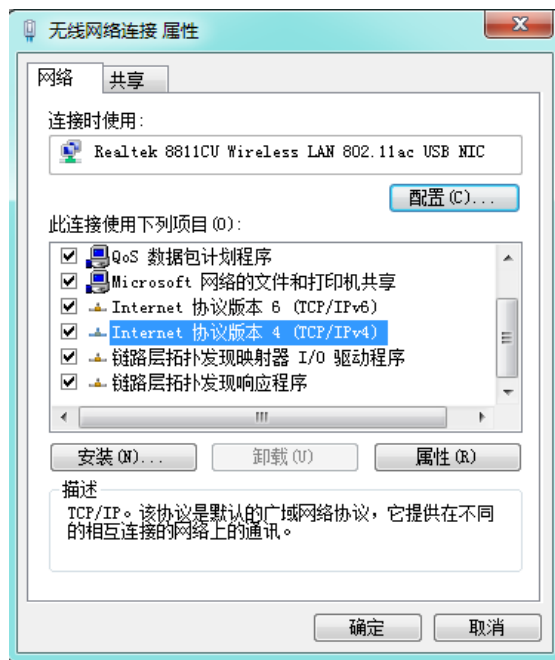
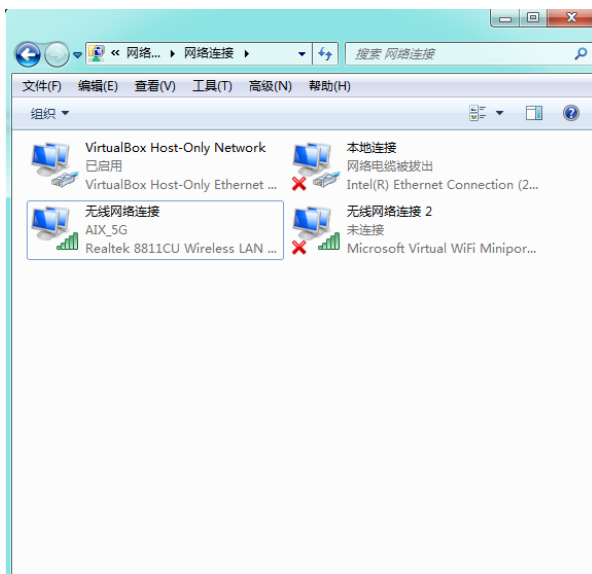
本章主要内容

- 什么是DHCP
- DHCP的工作原理
- 抓包分析DHCP的工作过程
- DHCP中继
- DHCP安全



一、什么是DHCP?

思考：手工方式给网络内的计算机分配静态IP地址，会带来什么问题？



1. 什么是DHCP?

□ 手工管理IP地址的不足

- 在TCP/IP体系互连网络中，IP地址就相当于计算机的门牌号，标识着计算机在网络中的位置，因此每台计算机都需要配置IP地址。
- 当网络中只有少数几台计算机时，只需要通过手动的方式为每台计算机配置IP地址。但如果网络中有成百上千台计算机，显然用手工方式为每一台计算机配置IP地址，会有很高的管理成本！

1. 什么是DHCP?

□ 认识DHCP

- DHCP (Dynamic Host Configuration Protocol, 动态主机配置协议) 是一个局域网的网络协议, 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。

1. 什么是DHCP?

□ DHCP一般用于以下场景中:

- 网络规模较大, 手工配置需要很大的工作量, 并难以对整个网络进行集中管理。
- 网络中主机数目大于该网络支持的IP地址数量, 无法给每个主机分配一个固定的IP地址。例如, Internet接入服务提供商, 限制同时接入网络的用户数目, 大量用户必须动态获得自己的IP地址。

1. 什么是DHCP?

□ 使用DHCP有以下好处:

- 减少配置和管理的工作量, 便于管理, 提高效率。
- 配置更加可靠。
- 节约IP资源, 租用!

1. 什么是DHCP?

□ DHCP也存在一些缺点

- 如果DHCP服务器设置有误或出现故障，尤其是当网络中只有一台DHCP服务器时，就会导致网络中所有DHCP客户端无法正常获取IP地址，影响网络通信。
- 通常在一个网络中配置两台以上的DHCP服务器，当其中一台DHCP服务器失效时，由另一台（或几台）DHCP服务器提供服务，不影响网络的正常运行。

1. 什么是DHCP?

□ DHCP服务不仅提供IP地址自动分配功能，还有以下功能：

- 通过IP地址与MAC地址绑定，实现IP地址的固定分配。
- 可以自动配置客户端的DNS服务器和默认网关。
- 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。



1. 什么是DHCP?

□ DHCP的作用域

- DHCP服务器能够进行分配的IP地址段，是需要网络管理员事先配置好的，即配置DHCP的作用域。
- DHCP作用域是本地逻辑子网中可以使用的IP地址的集合，例如，若在DHCP服务器上配置作用域为192.168.1.1 ~ 192.168.1.254，则DHCP服务器只能使用作用域中定义的IP地址来分配给DHCP客户端。

二、DHCP的工作原理

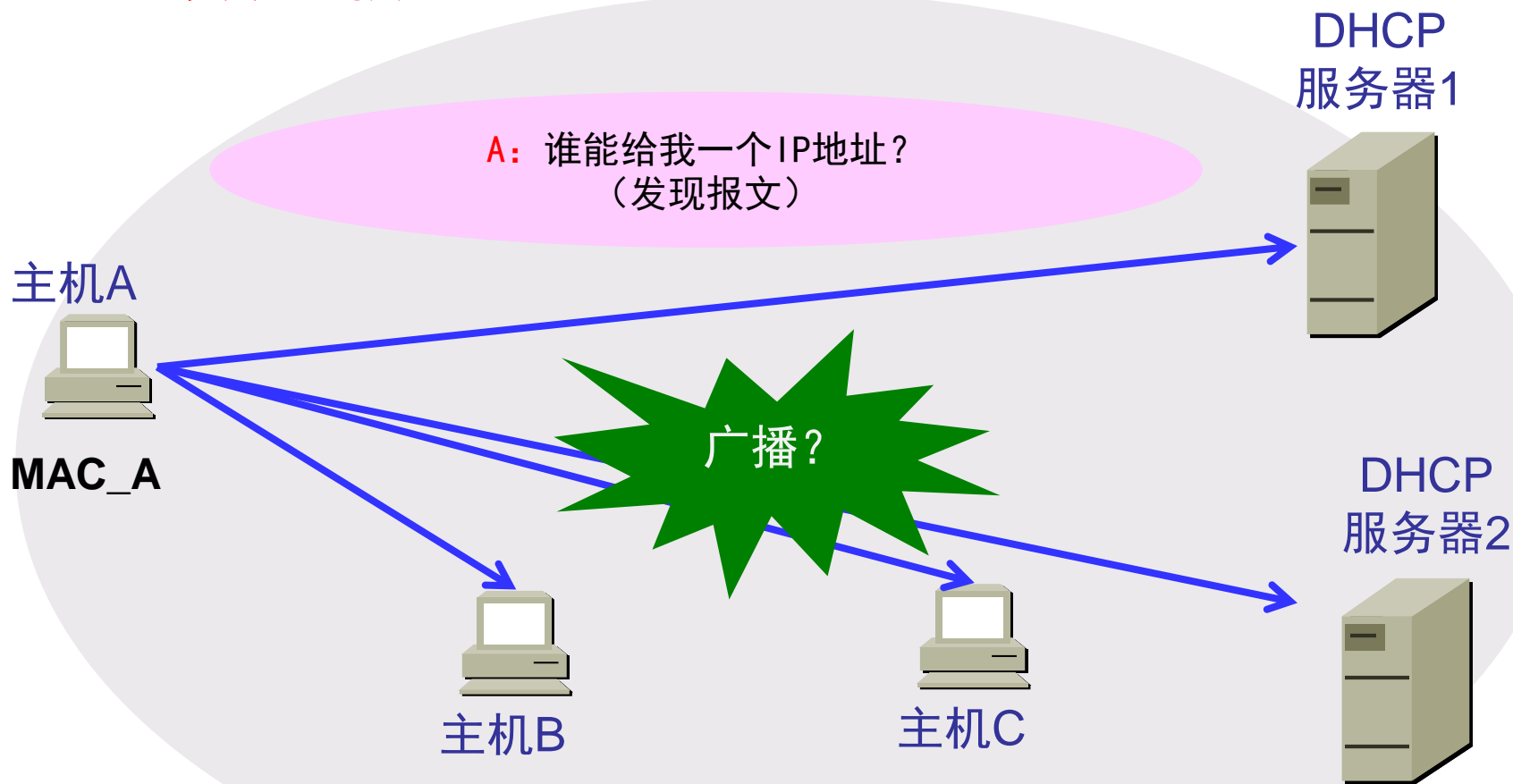
2.工作原理

□ DHCP客户端获取IP地址的基本过程

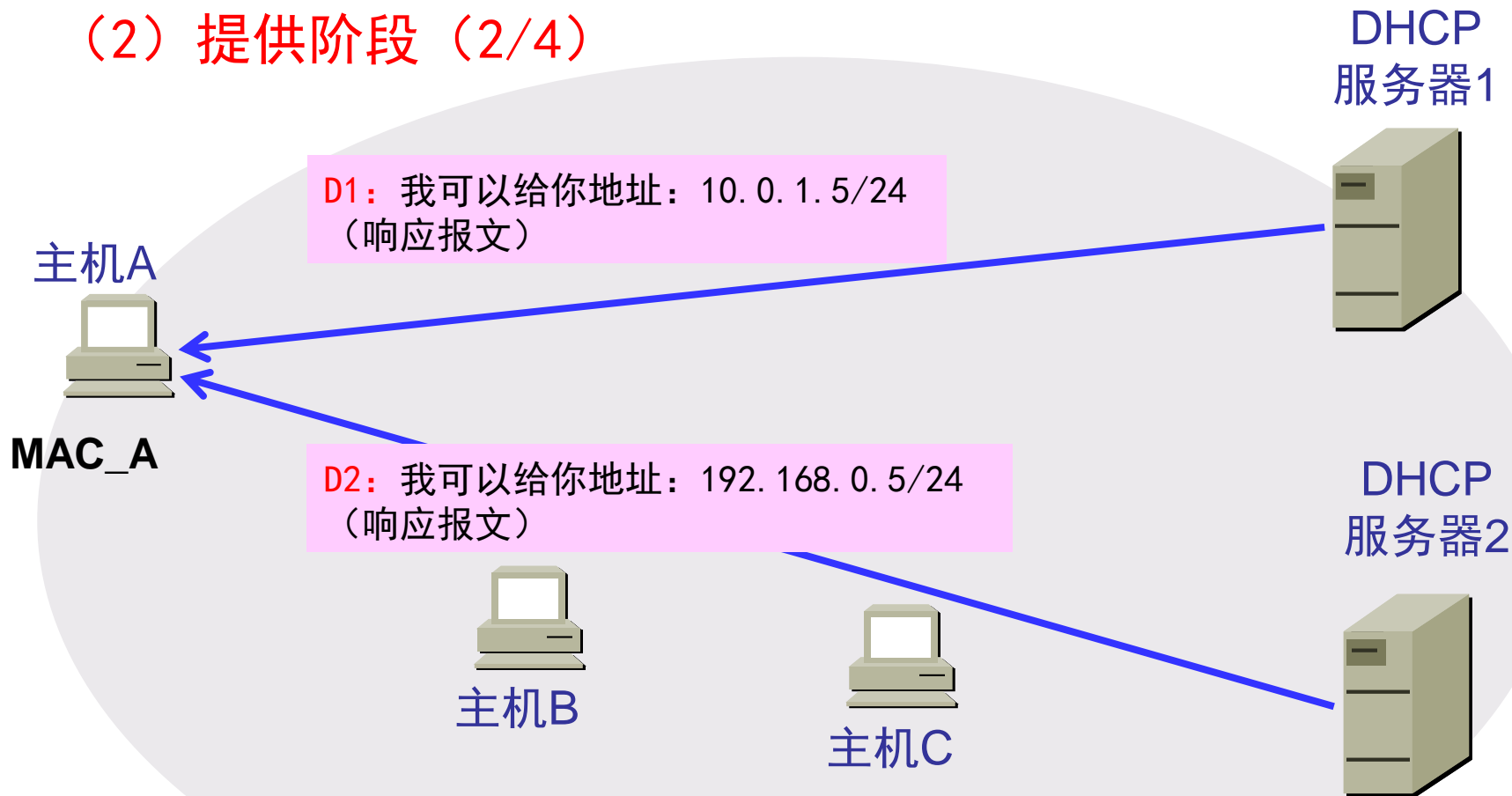
■ DHCP客户端从DHCP服务器获得IP地址信息的过程分为4个阶段：

- 发现（客户端→服务器）
- 提供（服务器→客户端）
- 请求（客户端→服务器）
- 确认（服务器→客户端）

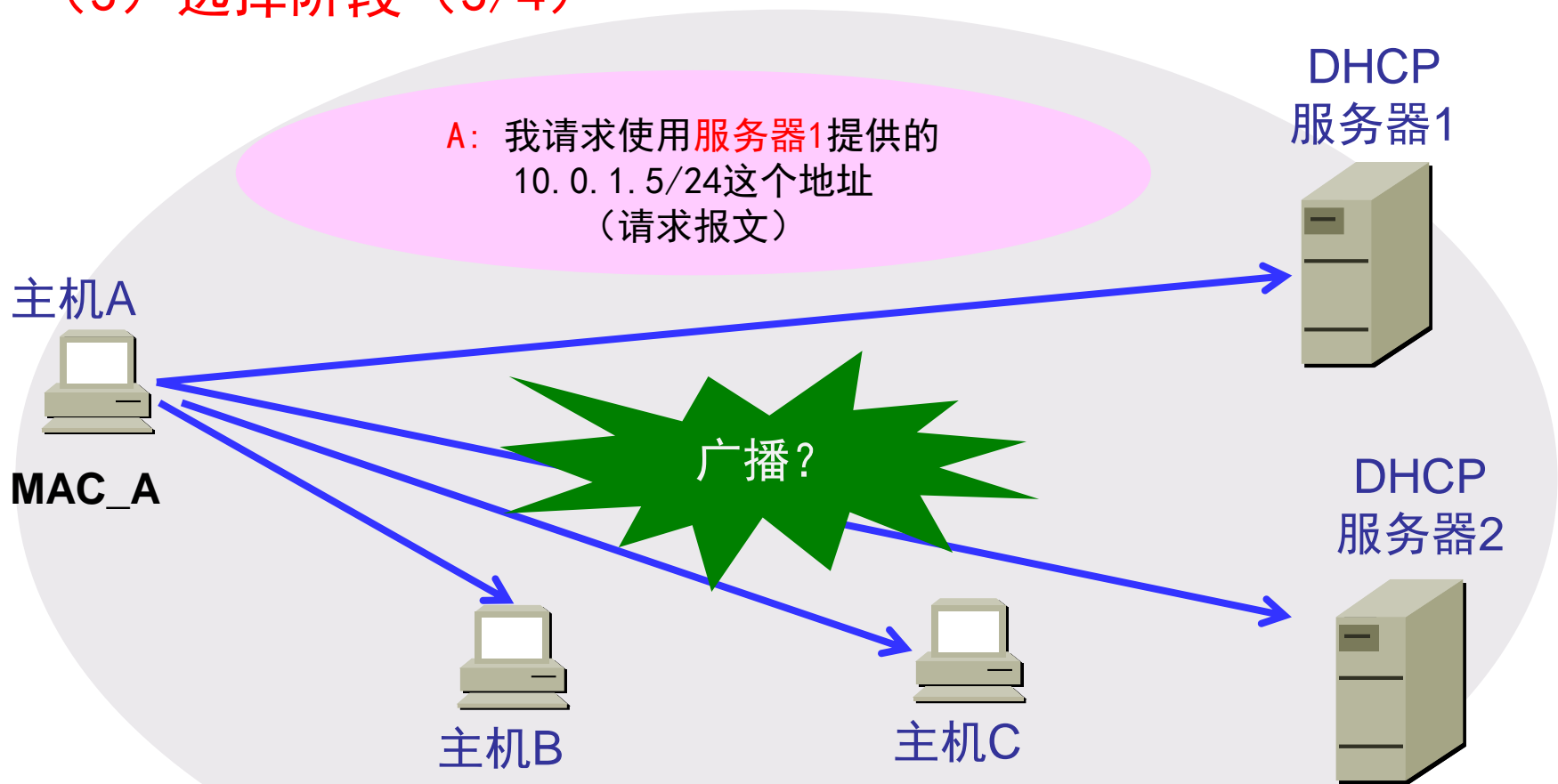
(1) 发现阶段 (1/4)



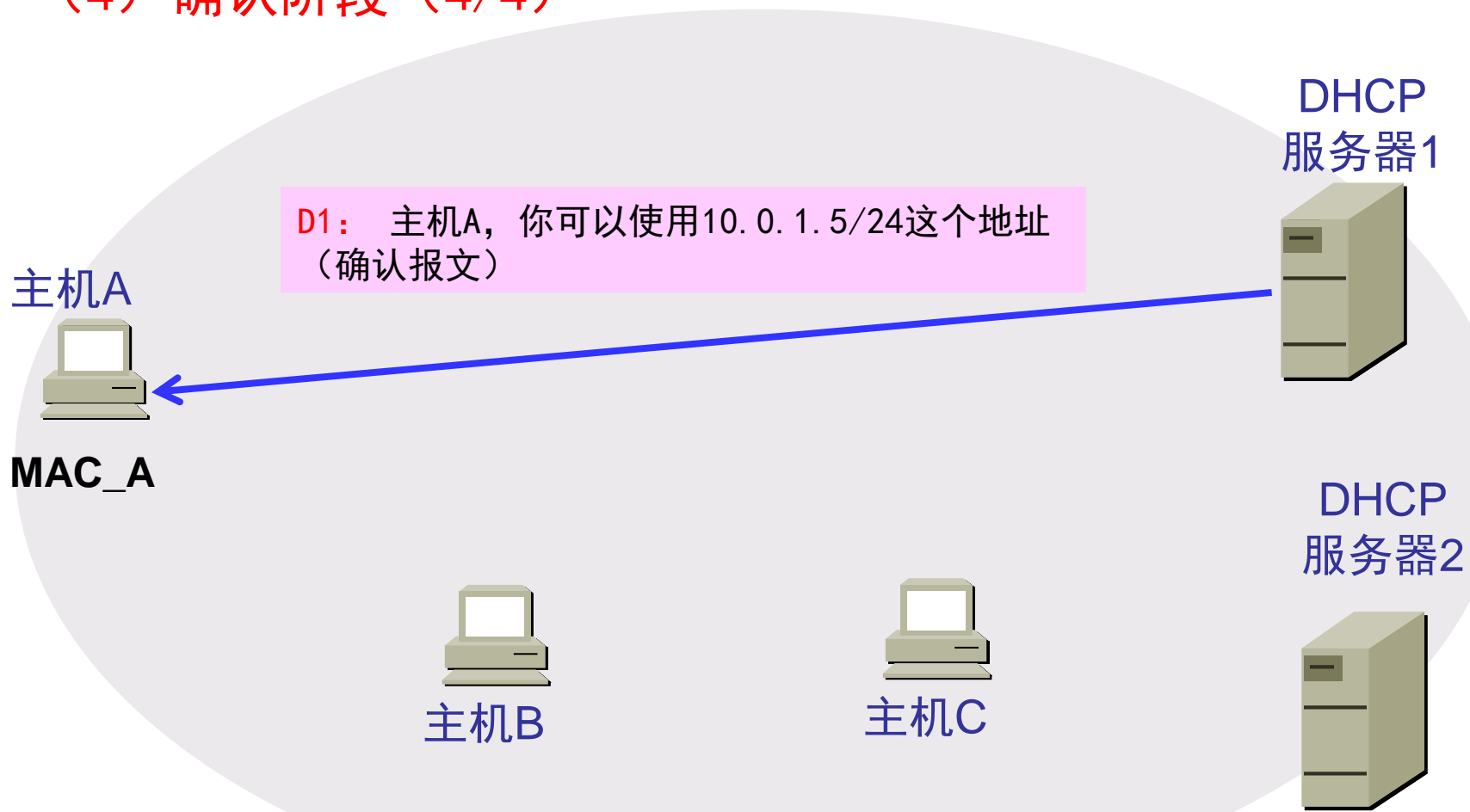
(2) 提供阶段 (2/4)



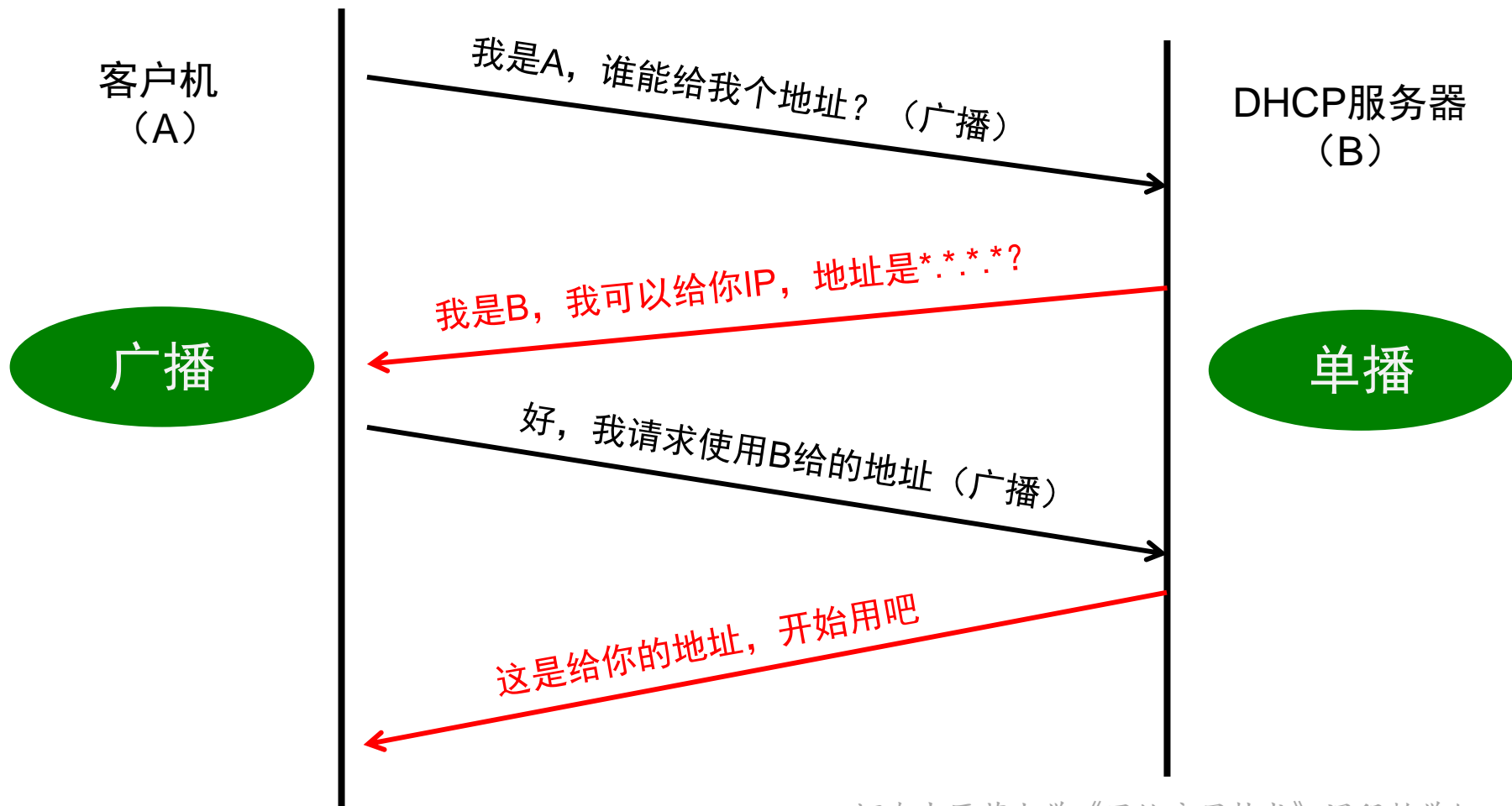
(3) 选择阶段 (3/4)



(4) 确认阶段 (4/4)



客户端获取IP地址的过程——总结



2.工作原理

□ DHCP服务的8种类型报文:

- DHCP服务在实现时, 会通过发送不同的报文, 实现客户端和服务
器之间的通信, 从而完成IP地址的获取等工作流程。
- DHCP共有8种类型的报文, 分别起着不同的作用。

2.工作原理

□ DHCP服务的8种类型报文:

■ DHCPDISCOVER (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, 如果客户端发现本机上没有任何IP地址等相关参数时, 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。



2.工作原理

□ DHCP服务的8种类型报文:

- DHCPOFFER（提供报文）：告知客户端本服务器可以为其提供IP地址
 - 当网络中的任何一个DHCP服务器收到客户端发出的DHCPDISCOVER广播后，**回应给客户端一个DHCPOFFER报文**，告诉客户端自己可以提供的IP地址等信息内容。

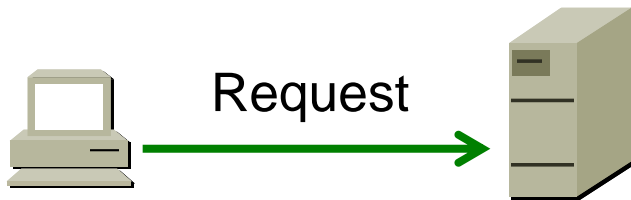


2.工作原理

□ DHCP服务的8种类型报文:

■ DHCPREQUEST (请求报文) : 明确服务器及希望获得分配的IP地址。

- ▶ 如果客户端收到网络上多台DHCP服务器的回应, 则会从中选择一个DHCP OFFER (通常是最先到达的那个), 并且会向网络上发送一个DHCPREQUEST广播数据包, 告诉所有DHCP服务器它将选用哪一台服务器提供的IP地址。



2.工作原理

□ DHCP服务的8种类型报文:

■ DHCPACK（确认报文）：通知用户可以使用分配的IP地址。

- 当DHCP服务器接收到客户端的DHCPREQUEST广播数据包后，会**向客户端发出DHCP ACK回应**，以确认IP租约的正式生效，也就结束了一个DHCP工作过程。同时，被选择的DHCP服务器将该IP地址保留，不再租用给其他客户使用。



2.工作原理

□ DHCP服务的8种类型报文：

- DHCPNAK（应答报文）：通知客户端无法分配合适的IP地址。
- DHCPRELEASE（请求报文）：请求释放相应的IP地址。
- DHCPDECLINE（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。
- DHCPINFORM（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。

2.工作原理

□ DHCP的租约

- DHCP 服务器分配给 DHCP 客户的 IP 地址是临时的，因此 DHCP 客户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。
- 租用期的数值应由 DHCP 服务器自己决定。DHCP 客户也可在自己发送的报文中（例如，发现报文）提出对租用期的要求。

2.工作原理

□ 更新租约 —— 自动更新

- 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。
- DHCP 客户端除了在开机的时候发出 DHCP request 请求之外，在租约期限一半的时候也会发出 DHCP request，如果此时得不到 DHCP 服务器的确认的话，客户端还可以继续使用该 IP；
- 当租约期过了87.5%时，如果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。若网络上没有其他DHCP服务器在运行，且租约到期，该客户端必须停止使用该IP地址，并重新发送一个DHCPDiscover数据包开始，再一次重复整个IP地址获取过程。

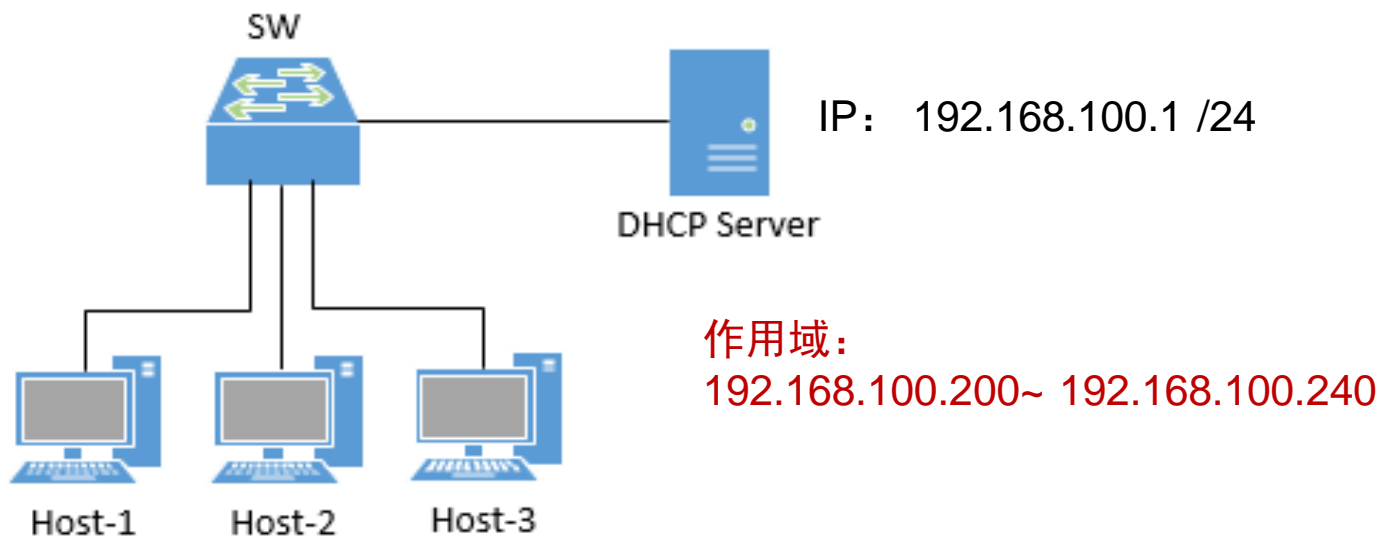
2.工作原理

□ 更新租约 —— 手动更新

- 如果需要立即更新DHCP配置消息，用户可以手动更新IP租约。例如，如果用户希望DHCP客户端立即从DHCP服务器获取新的配置参数（如DNS服务器地址等）。
- 可在Windows的命令行界面中，使用ipconfig命令，并带/renew开关参数。这条命令向DHCP服务器发送一条DHCPREQUEST消息请求更新配置选项和续订租约时间。

三、抓包分析DHCP的工作过程

■ 网络拓扑



-
- 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？
 - 例如：客户机发出的发现报文中，
 - 源MAC? / 目的MAC?
 - 源IP? / 目的IP ?

DHCP discover报文 - 地址信息



源MAC: 客户机MAC地址

目的MAC: 广播地址

No.	Time	Source	Destination	Protocol	Length	Info
5	6.895000	0.0.0.0	255.255.255.255	DHCP	410	DHCP Discover - Transaction
7	7.956000	192.168.100.1	192.168.100.203	DHCP	342	DHCP Offer - Transaction
8	8.907000	0.0.0.0	255.255.255.255	DHCP	410	DHCP Request - Transaction
9	8.923000	192.168.100.1	192.168.100.203	DHCP	342	DHCP ACK - Transaction

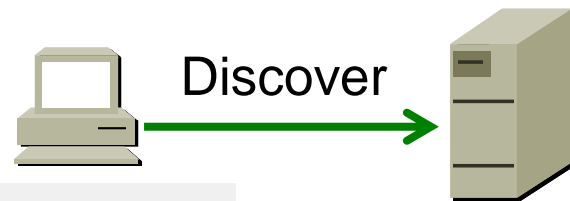
▶ Frame 5: 410 bytes on wire (3280 bits), 410 bytes captured (3280 bits) on interface 0
▶ Ethernet II, Src: HuaweiTe_b7:2b:95 (54:89:98:b7:2b:95), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
▶ User Datagram Protocol, Src Port: 68, Dst Port: 67
▶ Bootstrap Protocol (Discover)

源IP: 全0地址

目的IP: 全1广播地址
直接广播地址
有限广播地址

报文内容见下页

抓包分析：DHCP discover报文 - 报文内容



Bootstrap Protocol (Discover)

Message type: Boot Request (1)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0x0000512a

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_b7:2b:95 (54:89:98:b7:2b:95)

Client hardware address padding: 00000000000000000000

Server host name not given

Boot file name not given

Magic cookie: DHCP

此时客户端的IP地址是全0

抓包分析：DHCP discover报文 - 数据信息2



▷ Option: (53) DHCP Message Type (Discover)

✦ Option: (61) Client identifier

Length: 7

Hardware type: Ethernet (0x01)

Client MAC address: HuaweiTe_b7:2b:95 (54:89:98:b7:2b:95)

客户端的标识符 (即MAC地址)

✦ 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

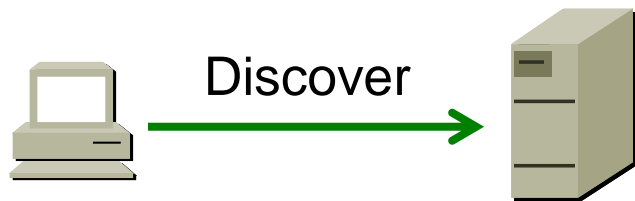
Parameter Request List Item: (184) Unassigned

申请参数列表

▷ Option: (255) End

Padding: 00...

- 客户机在首次发送Discover报文时，其地址如何配置？



□ 归纳一下

■ 在discover报文首部中

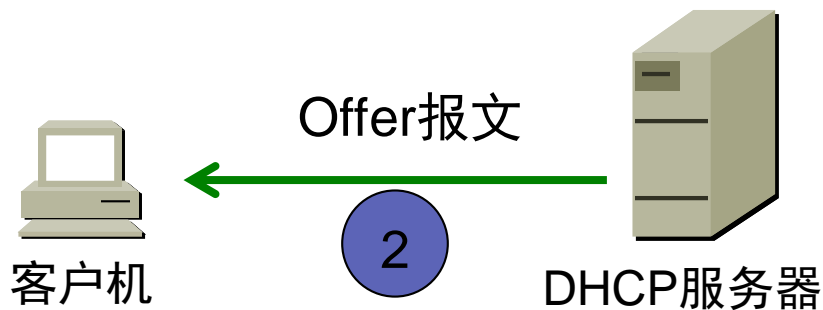
- 源IP地址：0.0.0.0，目的IP地址：255.255.255.255；
- 源MAC：DHCP客户机的MAC地址，目的MAC：全1的地址；

■ 在discover报文中

- 包含有DHCP客户机的MAC地址，以便DHCP服务器知道这是谁发的DHCPDISCOVER报文

问题2:

- 服务器的DHCP OFFER报文中，包含了什么信息？



抓包分析：DHCP offer报文 - 地址信息



源MAC：服务器MAC地址

目的MAC：客户端MAC地址

No.	Time	Source	Destination	Protocol	Length	Info
5	6.895000	0.0.0.0	255.255.255.255	DHCP	410	DHCP Discover - Transaction ID 0x4
7	7.956000	192.168.100.1	192.168.100.203	DHCP	342	<u>DHCP Offer</u> - Transaction ID 0x4
8	8.907000	0.0.0.0	255.255.255.255	DHCP	410	DHCP Request - Transaction ID 0x4
9	8.923000	192.168.100.1	192.168.100.203	DHCP	342	DHCP ACK - Transaction ID 0x4

▶ Frame 7: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
▶ Ethernet II, Src: PcsCompu_c1:97:81 (08:00:27:c1:97:81), Dst: HuaweiTe_b7:2b:95 (54:89:98:b7:2b:95)
▶ Internet Protocol Version 4, Src: <u>192.168.100.1</u> , Dst: <u>192.168.100.203</u>
▶ User Datagram Protocol, Src Port: 67, Dst Port: 68
▶ <u>Bootstrap Protocol (Offer)</u>

源IP：服务器IP地址

目的IP：准备分配给客户端的IP

报文内容见下页

抓包分析：DHCP offer报文 - 报文中的数据信息1



▣ Bootstrap Protocol (Offer)

Message type: Boot Reply (2)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0x0000512a

Seconds elapsed: 0

▢ Bootp flags: 0x0000 (Unicast)

Client IP address: 0.0.0.0

Your (client) IP address: 192.168.100.203

Next server IP address: 0.0.0.0

Relay agent IP address: 0.0.0.0

Client MAC address: HuaweiTe_b7:2b:95 (54:89:98:b7:2b:95)

Client hardware address padding: 0000000000000000000000

Server host name not given

Boot file name not given

Magic cookie: DHCP

准备分配给客户端的IP地址



抓包分析：DHCP offer报文 - 报文中的数据信息2

- ▀ Option: (53) DHCP Message Type (Offer)
Length: 1
DHCP: Offer (2)
- ▀ Option: (54) DHCP Server Identifier DHCP服务器标识符
Length: 4
DHCP Server Identifier: 192.168.100.1 DHCP服务器的IP
- ▀ Option: (51) IP Address Lease Time IP租约时间
Length: 4
IP Address Lease Time: (43200s) 12 hours IP租约时间是12小时
- ▀ Option: (1) Subnet Mask 子网掩码
Length: 4
Subnet Mask: 255.255.255.0
- ▀ Option: (3) Router
Length: 4
Router: 192.168.100.254 准备发给客户端的网关地址
- ▀ Option: (6) Domain Name Server 域名服务器
Length: 4
Domain Name Server: 8.8.8.8 域名服务器的IP地址
- ▀ Option: (255) End
Option End: 255
Padding: 00

□ 服务器的OFFER报文中，包含哪些信息？



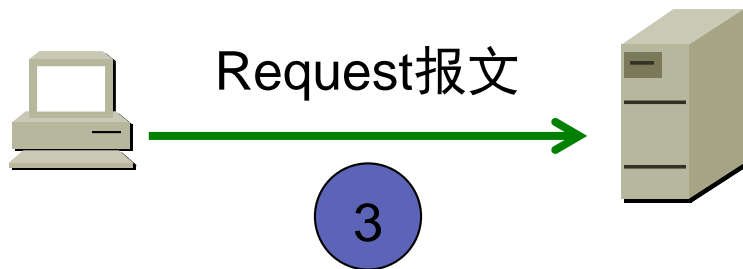
- DHCP客户机的MAC地址; —————→ 想给谁?

- 准备提供给客户机的IP地址;
- 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?

问题3:

- DHCP服务器如何知道客户机选择了自己所提供的地址参数?



抓包分析：DHCP Request报文 - 地址信息



源MAC：客户机MAC地址

目的MAC：广播地址

No.	Time	Source	Destination	Protocol	Length	Info
5	6.895000	0.0.0.0	255.255.255.255	DHCP	410	DHCP Discover - Transaction
7	7.956000	192.168.100.1	192.168.100.203	DHCP	342	DHCP Offer - Transaction
8	8.907000	0.0.0.0	255.255.255.255	DHCP	410	<u>DHCP Request</u> - Transaction
9	8.923000	192.168.100.1	192.168.100.203	DHCP	342	DHCP ACK - Transaction

▶ Frame 8: 410 bytes on wire (3280 bits), 410 bytes captured (3280 bits) on interface 0
▶ Ethernet II, Src: HuaweiTe_b7:2b:95 (54:89:98:b7:2b:95), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶ Internet Protocol Version 4, Src: <u>0.0.0.0</u> , Dst: <u>255.255.255.255</u>
▶ User Datagram Protocol, Src Port: 68, Dst Port: 67
▶ <u>Bootstrap Protocol (Request)</u>

源IP：0.0.0.0

目的IP：广播地址

见下页

抓包分析：DHCP Request报文 - 报文中的数据信息1



Bootstrap Protocol (Request)

Message type: Boot Request (1)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0x0000421f

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_b7:2b:95 (54:89:98:b7:2b:95)

Client hardware address padding: 00000000000000000000

Server host name not given

Boot file name not given

Magic cookie: DHCP

抓包分析：DHCP Request报文 - 报文中的数据信息2



```
Option: (53) DHCP Message Type (Request)
  Length: 1
  DHCP: Request (3)
```

```
Option: (54) DHCP Server Identifier
  Length: 4
  DHCP Server Identifier: 192.168.100.1
```

DHCP服务器的标识符（即其IP地址）
表明“我”申请使用该服务器分配的IP地址

```
Option: (50) Requested IP Address
  Length: 4
  Requested IP Address: 192.168.100.203
```

所申请的IP地址

```
Option: (61) Client identifier
  Length: 7
  Hardware type: Ethernet (0x01)
  Client MAC address: HuaweiTe_b7:2b:95 (54:89:98:b7:2b:95)
```

客户端标识符（即MAC地址）
表明“我”是谁

```
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（即子网掩码、默认网关等信息）

```
Option: (255) End
  Option End: 255
```

```
Padding: 0000000000000000000000000000000000000000000000000000000000000000...
```

❑ DHCP服务器如何知道客户机选择了自己所提供的地址参数?



- ❑ 如果有多个DHCP服务器向DHCP客户端回应DHCP OFFER报文，则DHCP客户端一般只接收第一个收到的OFFER报文，然后以广播方式发送DHCP REQUEST报文，该报文中包含客户端想选择的DHCP服务器标识符（即Option 54）和客户端申请的IP地址（即Option 50）。
- ❑ DHCP客户端广播发送DHCP REQUEST报文通知所有的DHCP服务器，它将选择某个DHCP服务器提供的IP地址，其他DHCP服务器可以重新将曾经分配给客户端的IP地址分配给其他客户端。
- ❑ 客户机在发送DHCP Request消息时，虽然客户机已经选择了IP地址，但是还没有最终确认并配置IP地址，因此，在DHCPREQUEST报文中仍然使用0.0.0.0的地址作为源IP地址；

问题4:

- 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客户机获得IP后，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DHCPRequest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DHCPACK确认信息。

□ DHCP客户机获得IP后，每次重新启动时，如何与DHCP服务器联系？

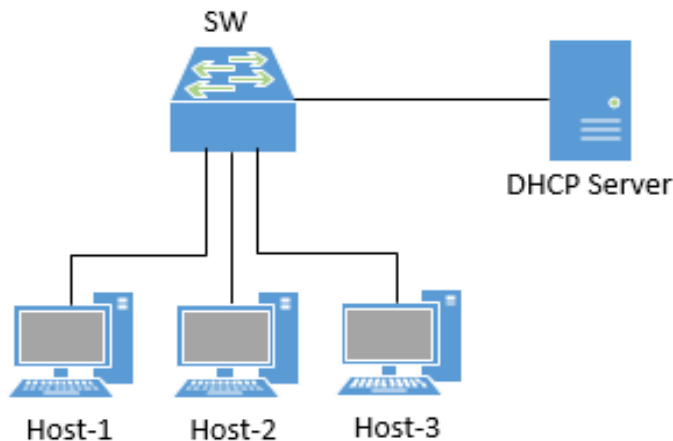
- 如果此IP地址已无法再分配给原来的DHCP客户机使用时（比如此IP地址已分配给其它DHCP客户机使用，或者因为客户机移到其他子网），则DHCP服务器给DHCP客户机回答一个DHCP `nack` 否认信息。
- 当原来的DHCP客户机收到此DHCP `nack` 否认信息后，它就必须重新发送DHCP `discover` 发现信息来请求新的IP地址。

四、DHCP中继 (DHCP Relay)

4. DHCP 中继代理

□ 为什么会用到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。



4. DHCP 中继代理

□ 为什么会用到DHCP中继?

- 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。

4. DHCP 中继代理

➤ IP地址规划:

Host-1: 192.168.0.1~192.168.0.100

Host-2: 192.168.1.1~192.168.1.100

Host-3: 192.168.2.1~192.168.2.100

Host-4: 192.168.3.1~192.168.3.100

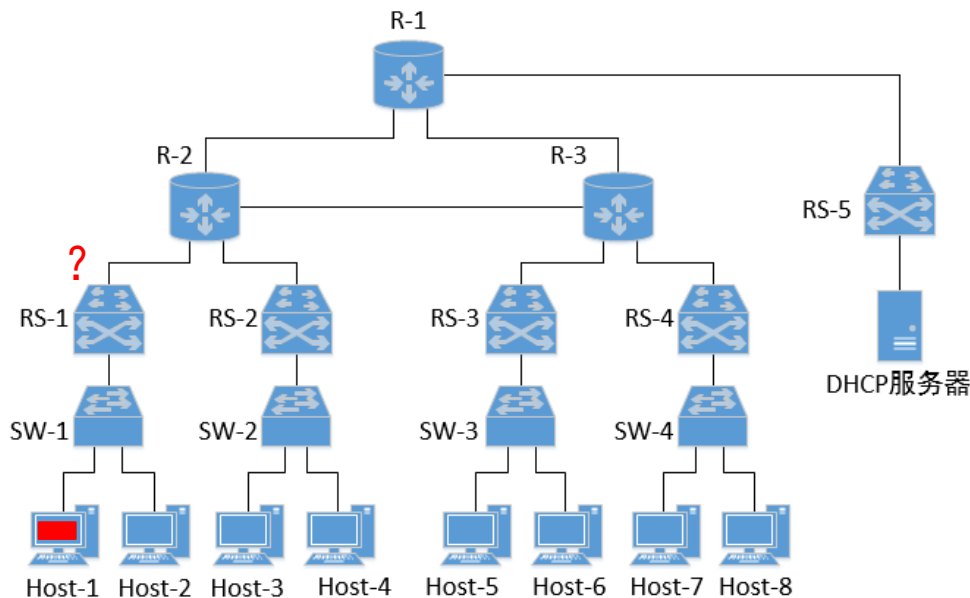
Host-5: 192.168.4.1~192.168.4.100

Host-6: 192.168.5.1~192.168.5.100

Host-7: 192.168.6.1~192.168.6.100

Host-8: 192.168.7.1~192.168.7.100

DHCP服务器: 192.168.100.1



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

4. DHCP 中继代理

□ 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，需要在每个子网络内（即每一个广播域内）配置一个DHCP中继（通常配置在路由交换机上）。
- DHCP中继上配置有DHCP服务器的IP地址信息，通过DHCP中继服务，与DHCP服务器不在同一子网的DHCP客户端可以通过DHCP中继与其他网段的DHCP服务器通信，使得DHCP客户端能够自动获取到IP地址。

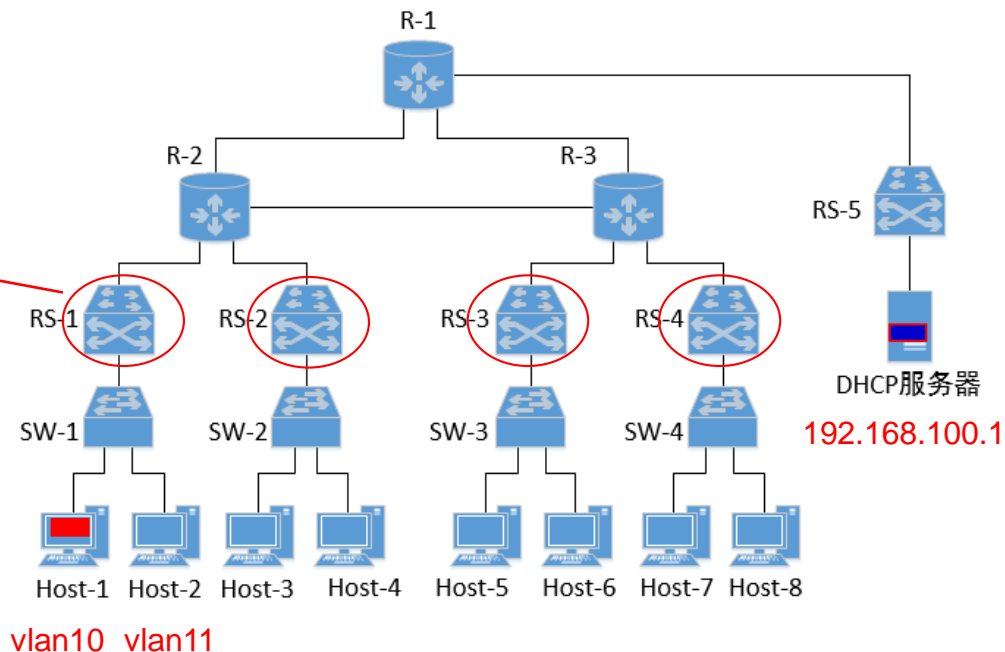
4. DHCP 中继代理

➤ DHCP中继的配置举例（华为s5700）：

```
[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

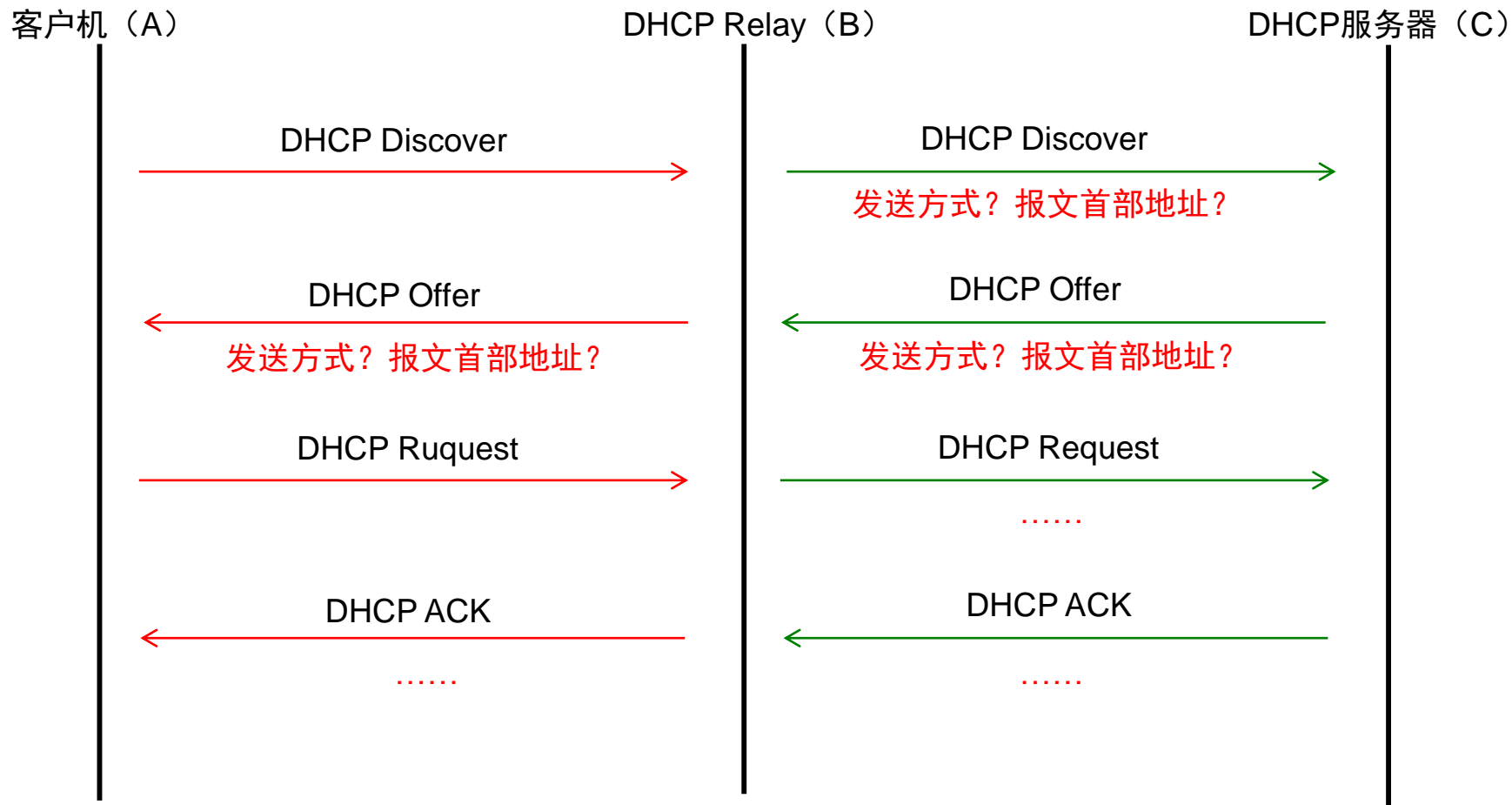
[RS-1] interface vlanif 11
[RS-1-Vlanif11] dhcp select relay
[RS-1-Vlanif11] dhcp relay server-ip 192.168.100.1
[RS-1-Vlanif11] quit
```

针对每个用户VLAN，在
网关处配置DHCP中继。

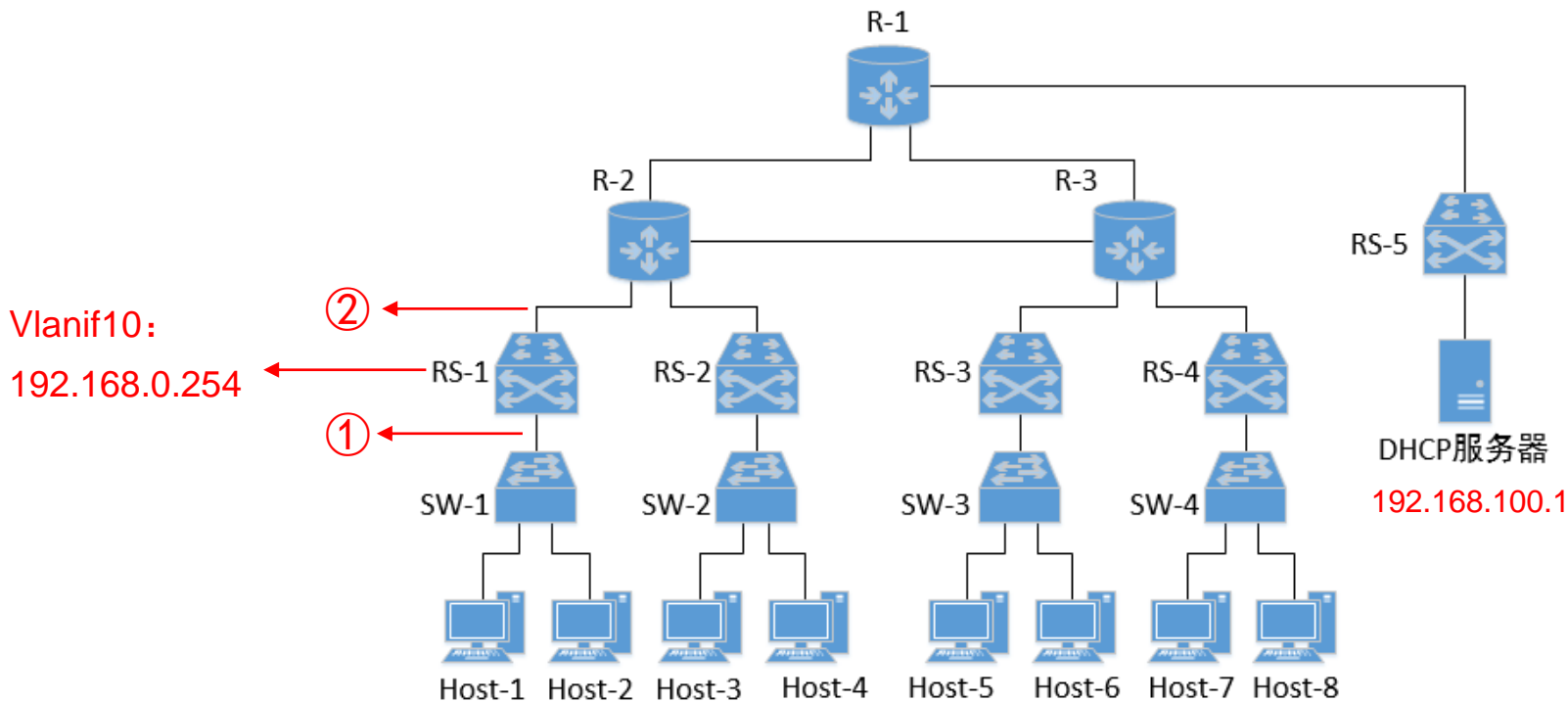


在RS-1~RS-4上配置DHCP中继

DHCP Relay的工作过程



抓包分析DHCP Relay的工作过程



vlan10

Host-1将要获取192.168.0.1~192.168.0.100中的IP地址

■ 抓包分析DHCP Relay的工作过程

Host-1 ↔ DHCP 中继 (RS-1)

①

No.	Time	Source	Destination	Protocol	Length	Info
3	3.525000	<u>0.0.0.0</u>	<u>255.255.255.255</u>	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. Host-1发出DHCPDISCOVER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）。

DHCP 中继 (RS-1) ↔ DHCP服务器

②

No.	Time	Source	Destination	Protocol	Length	Info
5	6.489000	<u>192.168.0.254</u>	<u>192.168.100.1</u>	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

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)

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 -

4. 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）

DHCP 中继 (RS-1) ↔ DHCP服务器

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 -

3. 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。

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)

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	<u>0.0.0.0</u>	<u>255.255.255.255</u>	DHCP	414	DHCP Request -
8	5.584000	192.168.100.1	192.168.0.1	DHCP	346	DHCP ACK -

5. Host-1发出request报文（包含所申请的地址信息），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）。

DHCP 中继 (RS-1) ↔ DHCP服务器

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	<u>192.168.0.254</u>	<u>192.168.100.1</u>	DHCP	410	DHCP Request -
10	8.502000	192.168.100.1	192.168.0.254	DHCP	342	DHCP ACK -

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

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)

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 -

8. 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)

DHCP 中继 (RS-1) ↔ DHCP服务器

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 -

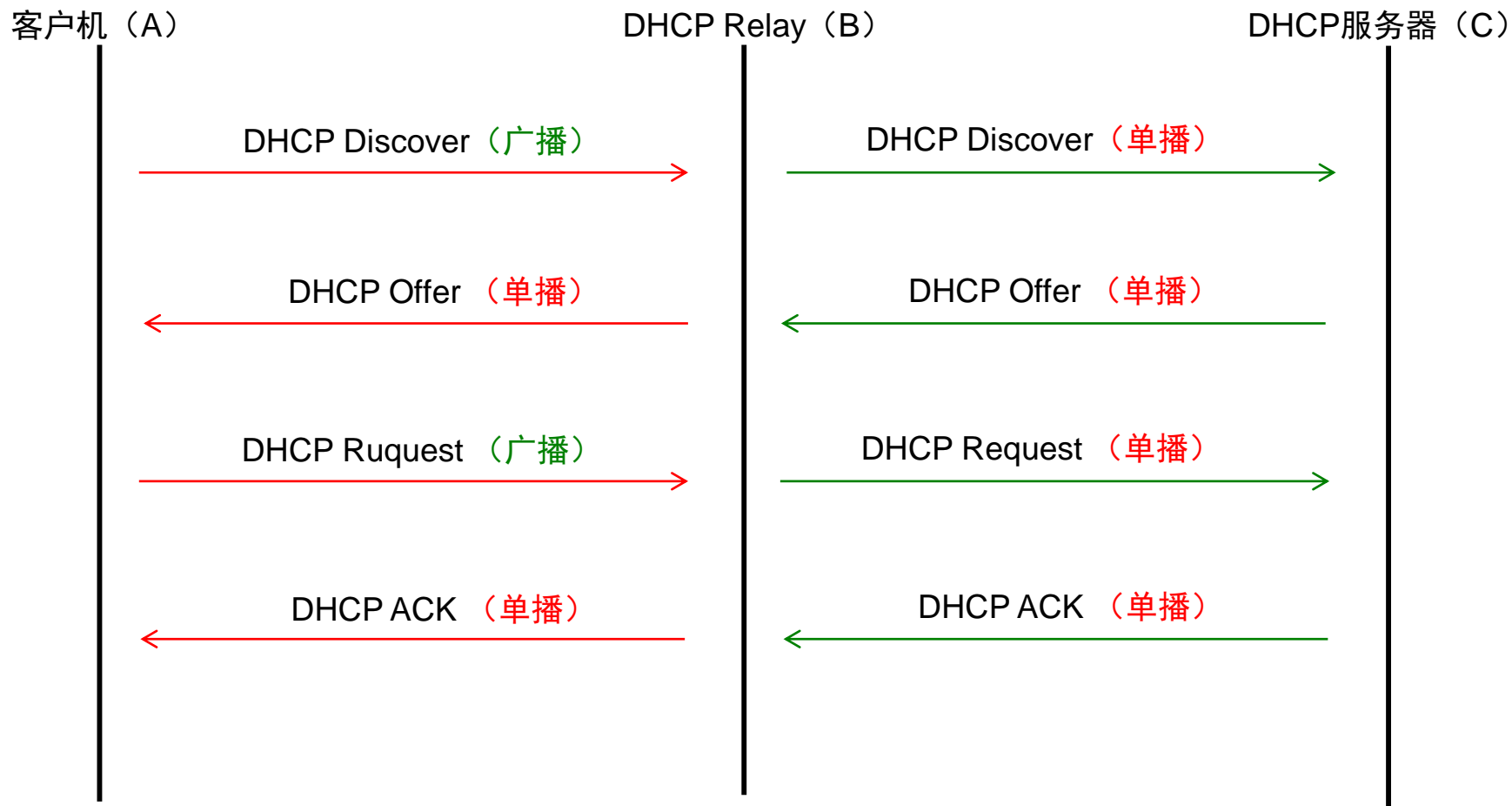
7. DHCP服务器从收到的request报文中获取了DHCP中继的IP地址和客户端的MAC地址, 然后向DHCP中继发回ACK报文 (单播报文), 报文首部的IP地址如图所示。

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



4. 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服务器自动获取IP地址的过程与直接从DHCP服务器自动获取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。

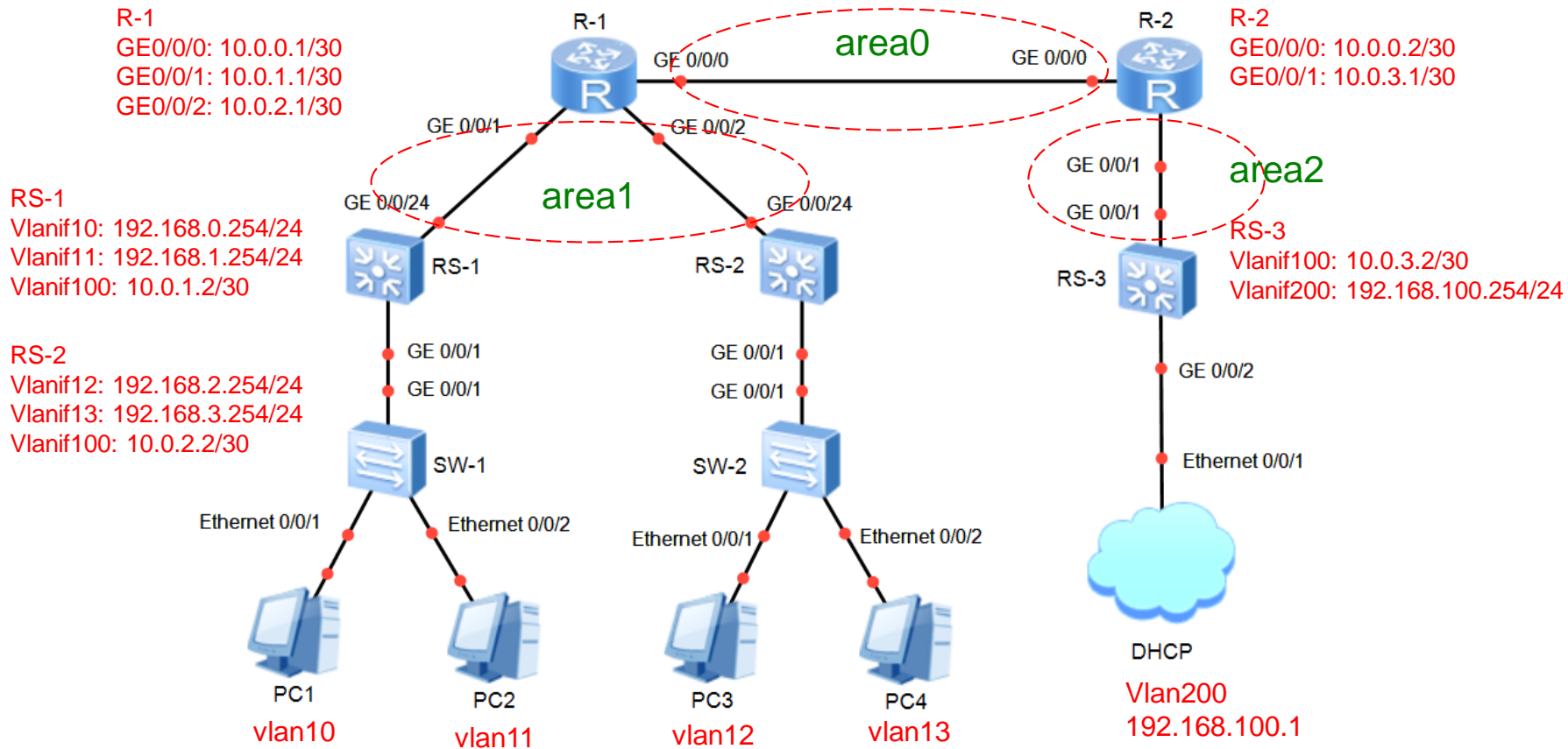
4. DHCP 中继代理

□ DHCP中继的工作特点

- DHCP客户端发出请求报文（以广播报文形式），DHCP中继收到该报文并适当处理后，以**单播**形式发送给指定的、位于其它网段上的DHCP服务器。
- 服务器根据请求报文中提供的信息，将返回的报文以**单播**的形式，发给DHCP中继，然后再通过DHCP中继将配置信息返回给客户端，完成对客户端的动态配置。

□ DHCP中继案例

DHCP中继案例



DHCP中继案例

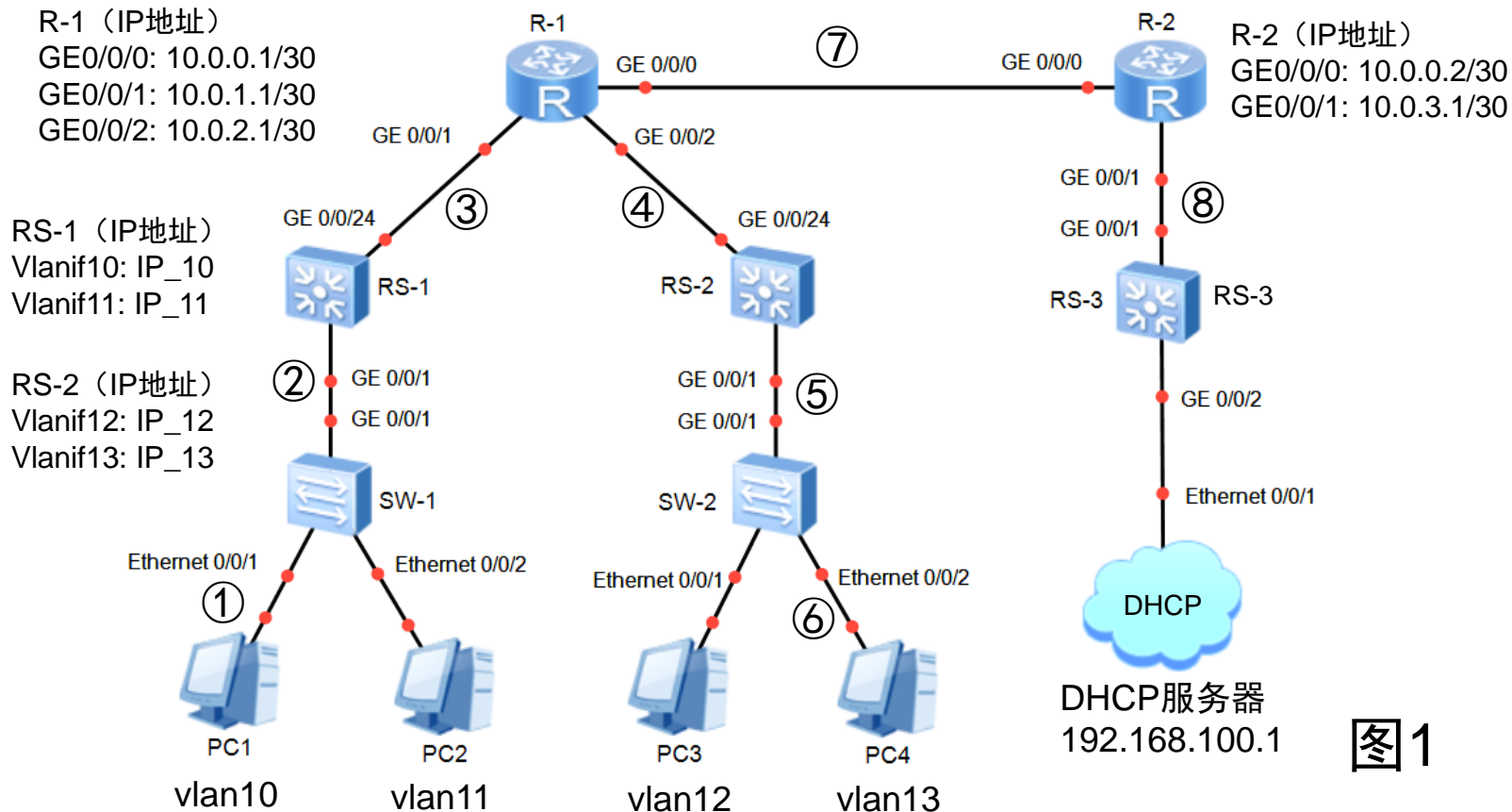


图 1

DHCP中继案例

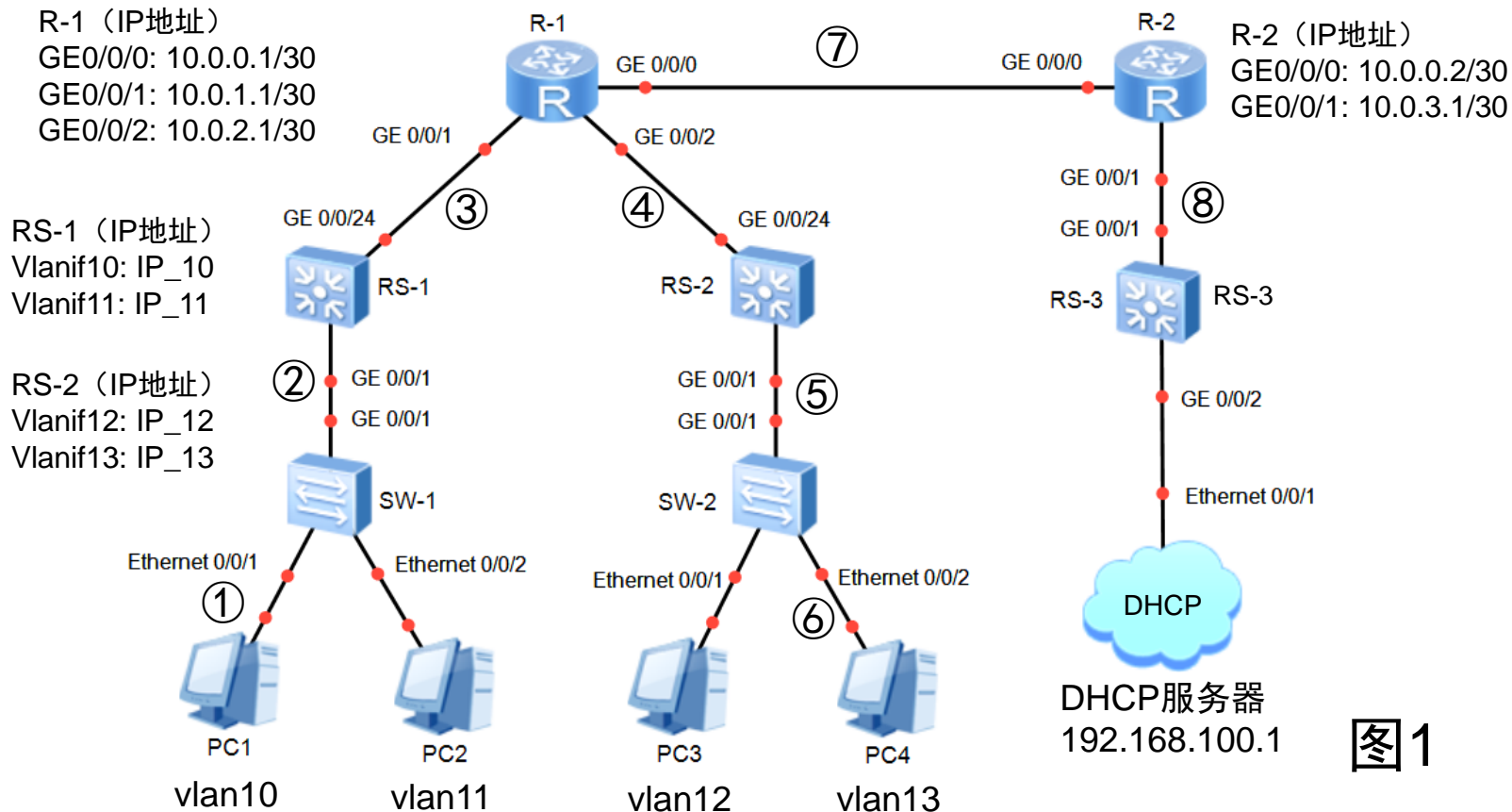
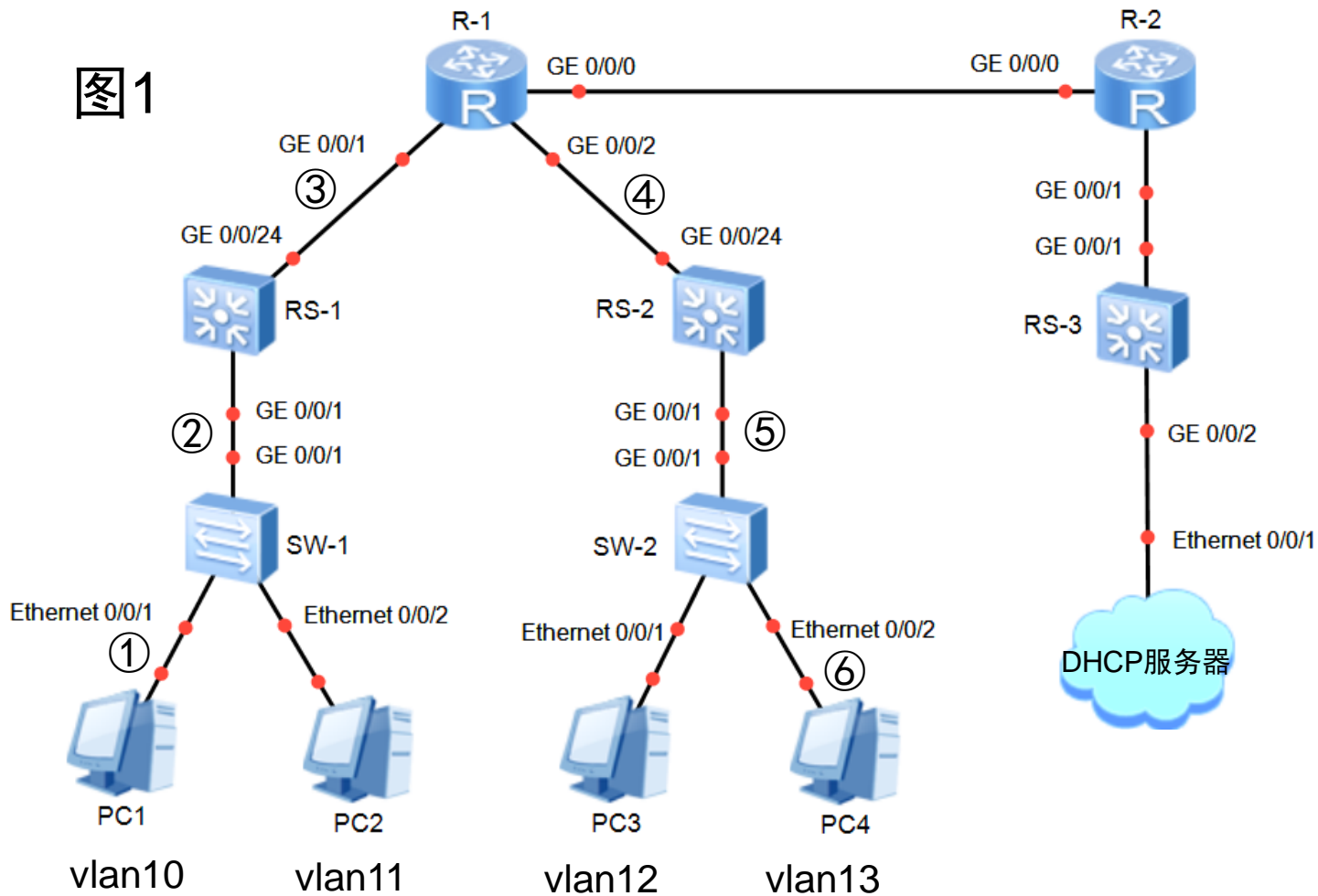


图 1

图1



60

40

90

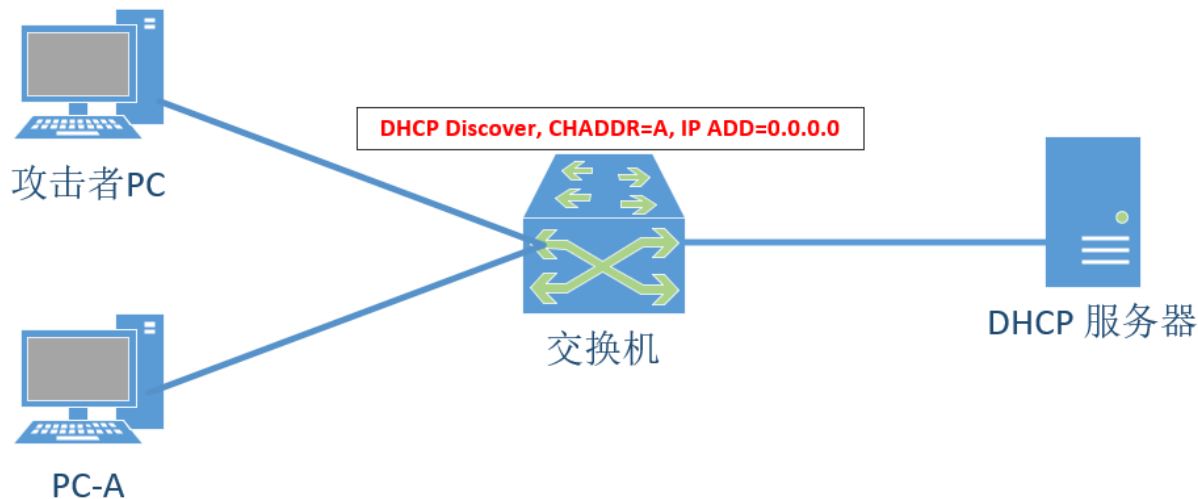
五、DHCP安全

5. DHCP 安全

- 网络攻击无处不在，针对DHCP的攻击也不例外。 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饿死攻击
 - 仿冒DHCP Server攻击
 - 仿冒DHCP 报文攻击
 - DHCP中间人攻击

DHCP饿死攻击

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

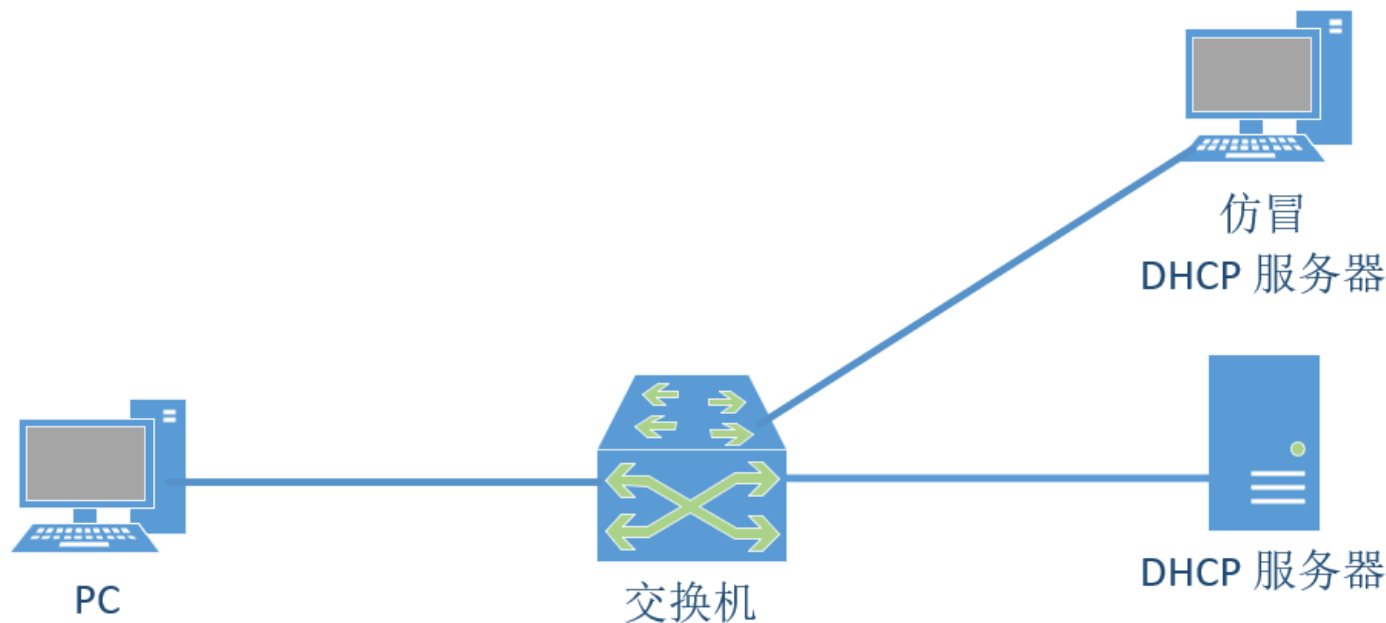


- 攻击原理：攻击者持续大量的向DHCP Server申请IP地址，直到耗尽DHCP Server地址池中的IP地址，导致DHCP Server不能给正常的用户进行分配。

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。

仿冒DHCP Server攻击



- 攻击原理：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。

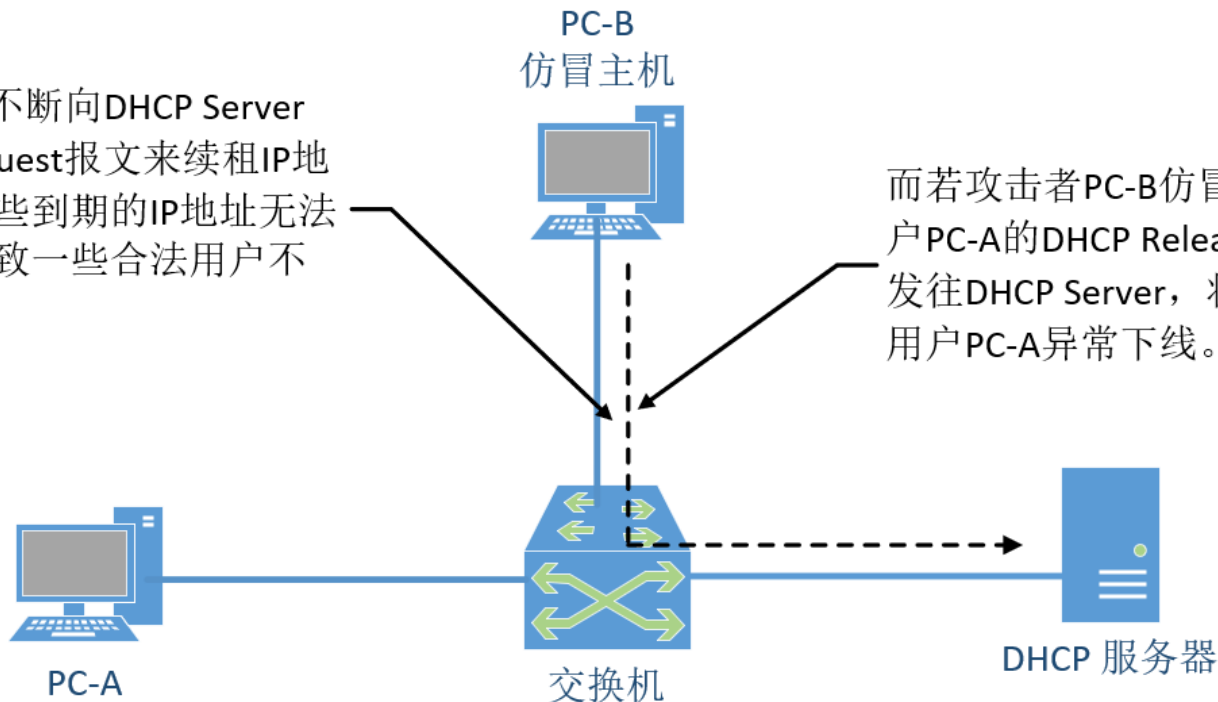
仿冒DHCP Server攻击

- ❑ 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。
- ❑ 协议原理：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。

仿冒DHCP 报文攻击

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。

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。

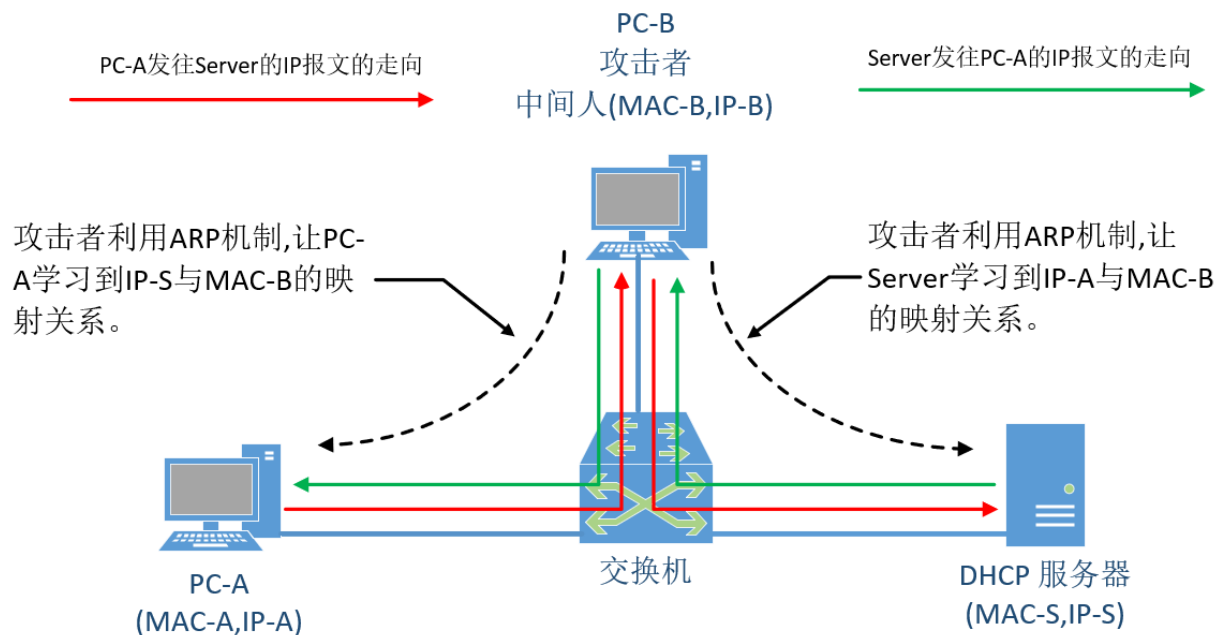


- 攻击原理：DHCP服务器在主机提出续租或释放请求时，一般都会满足主机。

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客户端和服务端。
- 产生危害：造成信息泄露等。

5. DHCP 安全

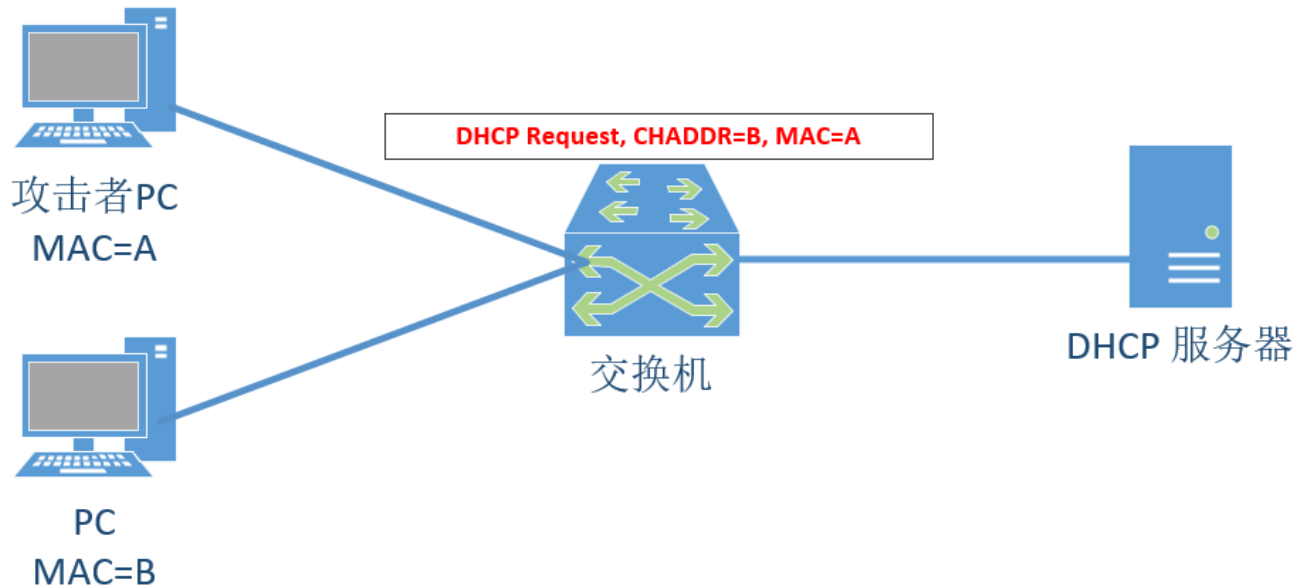
□ DHCP Snooping

- 为了增强网络安全，防止DHCP受到攻击，一种称为DHCP Snooping的技术应运而生。DHCP Snooping不是一种标准技术，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）
- 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。

5. DHCP 安全

□ DHCP Snooping防饿死攻击

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



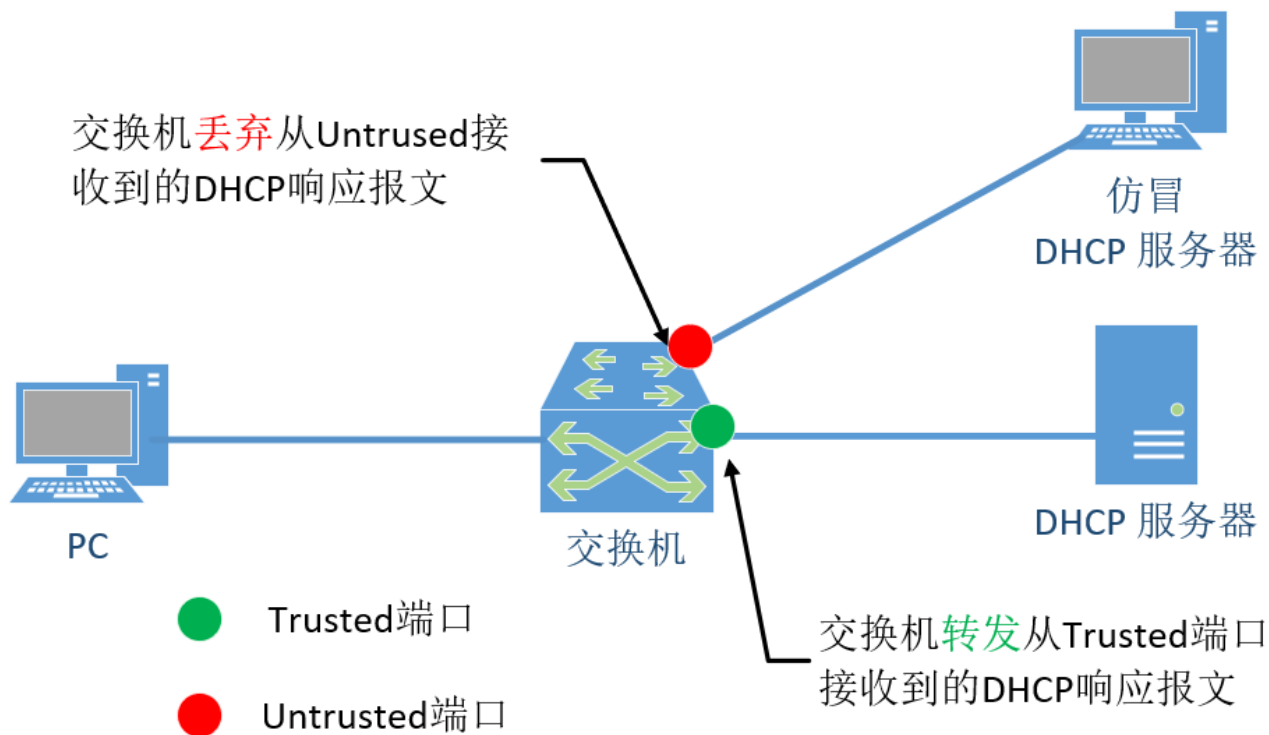
5. DHCP 安全

□ DHCP Snooping防饿死攻击

- 饿死攻击是攻击者通过不断修改CHADDR字段，然后让DHCP服务器误认为是来自不同PC的用户进行申请IP地址，开启DHCP Snooping功能之后，可以检查DHCP Request报文帧头的源MAC与DHCP数据区中的CHADDR字段是否一致，如果一致进行转发，不一致就不会进行转发。
- 简单说就是CHADDR字段有个MAC地址，然后在封装数据包的时候又IP层面的数据包，里面会含有自身的MAC地址，使能了DHCP Snooping之后也就允许其对于IP包进行检查，从而进行判定发送的数据包是否真实。如图中的CHADDR=B，MAC=A，不一致就会被丢弃。

5. DHCP 安全

□ DHCP Snooping防止仿冒DHCP Server攻击



5. DHCP 安全

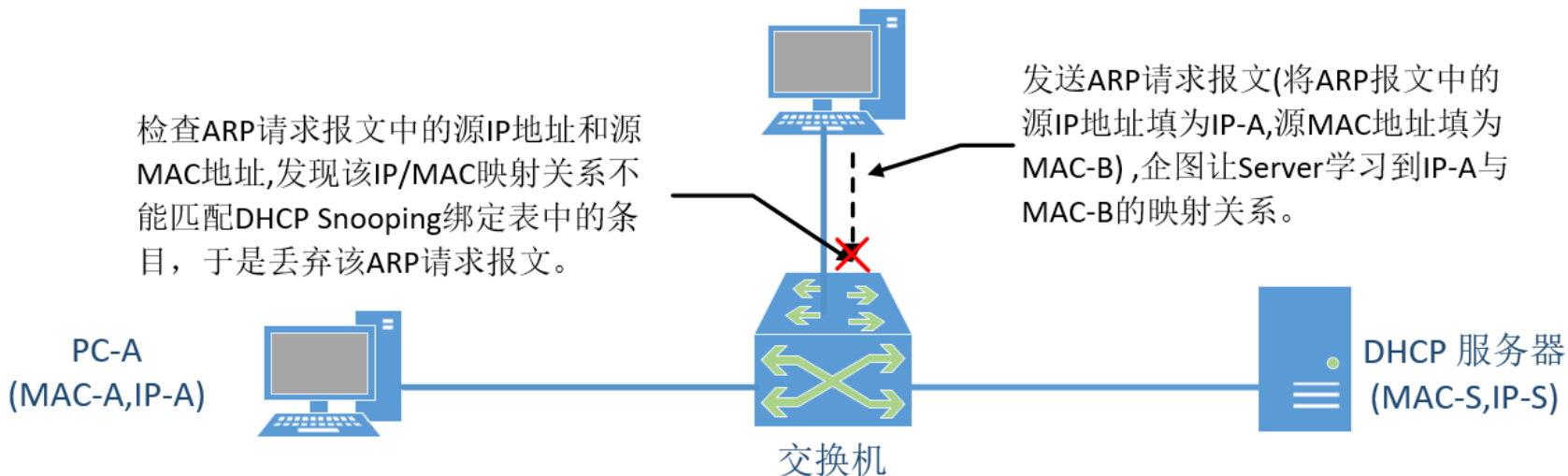
□ DHCP Snooping防止仿冒DHCP Server攻击

- 由于DHCP Server和DHCP Client之间没有认证机制，所以如果在网络上随意添加一台DHCP服务器，它就可以为客户端分配IP地址以及其他网络参数。如果该DHCP服务器为用户分配错误的IP地址和其他网络参数，将会对网络造成非常大的危害。
- 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。此后，从“非信任（Untrusted）”接口上收到的DHCP回应报文将被直接丢弃，这样可以有效防止DHCP Server仿冒者的攻击。

5. DHCP 安全

□ DHCP Snooping防止中间人攻击

PC-B，攻击者，中间人，(MAC-B,IP-B)



DHCP Snooping 绑定表

MAC	IP	lease Time	VLAN-ID	...
MAC-A	IP-A
MAC-B	IP-B
...

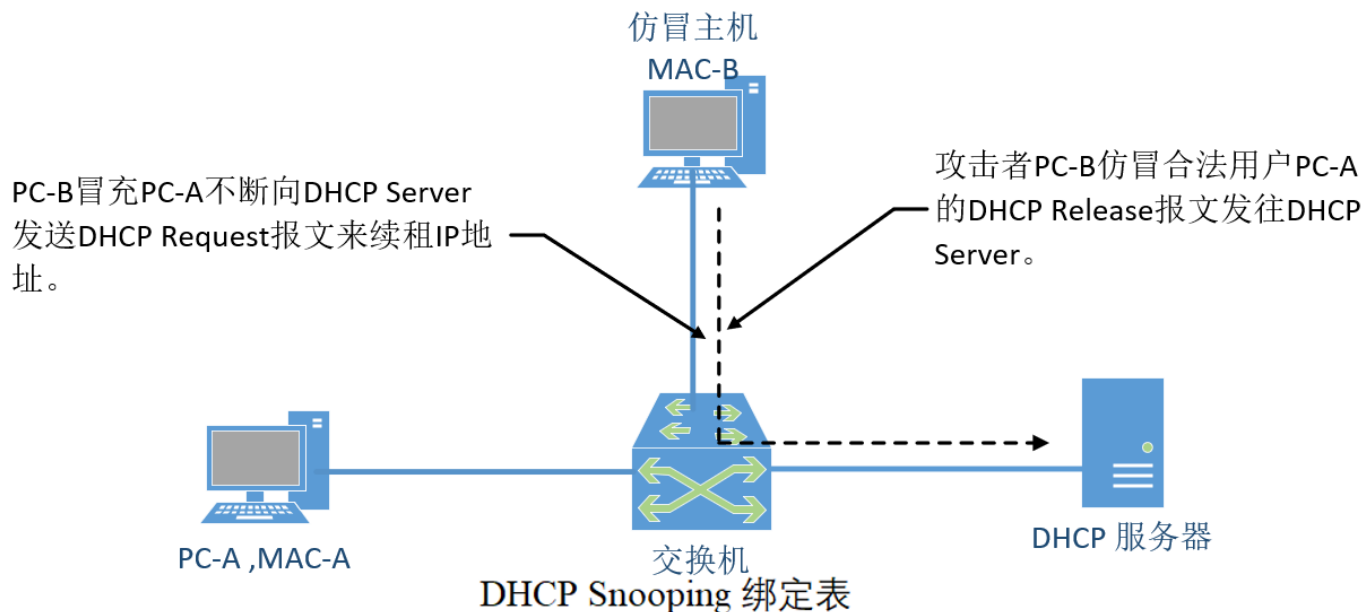
5. DHCP 安全

□ DHCP Snooping防止中间人攻击

- 从协议出发，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。
- 当交换机开启了DHCP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。（客户端对DHCP服务器进行请求时是使用MAC地址进行请求，如果请求成功，DHCP Server最终会发送Ack报文，此时绑定表中就会记录相应的IP与MAC对应关系，如果以后IP与MAC对应关系不一致，则会将报文丢弃）

5. DHCP 安全

□ DHCP Snooping防止仿冒DHCP报文攻击



MAC	IP	lease Time	VLAN-ID	...
MAC-A	IP-A
MAC-B	IP-B
...

5. DHCP 安全

□ DHCP Snooping防止仿冒DHCP报文攻击

- 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。

第6讲 使用DHCP管理IP地址

完