



# Data Communications and Networking

Fourth Edition

Forouzan

## 第21章

地址映射、  
差错报告和多播

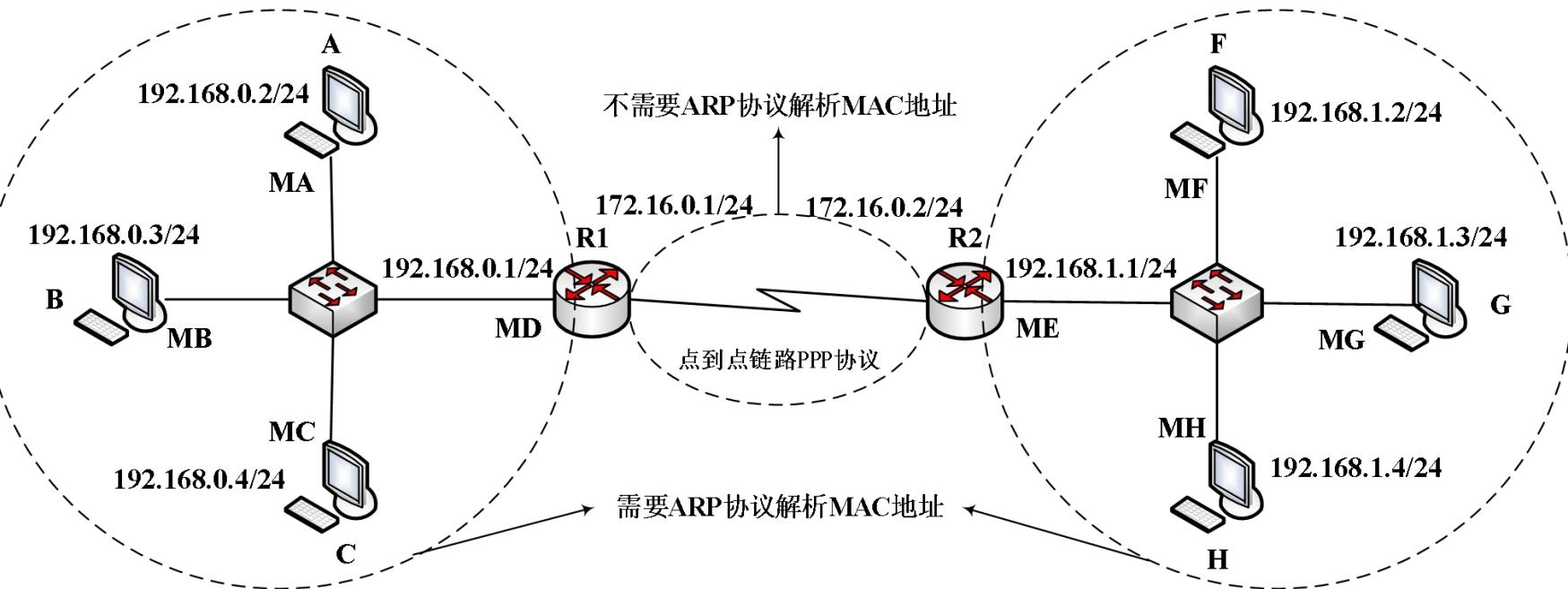
## 21-1 地址映射

将分组传递到主机或路由器需要两级地址：**逻辑地址** 和 **物理地址**，需要将一个逻辑地址映射成为它对应的物理地址，反过来也一样。这可以通过静态或动态映射完成。

### 讨论:

逻辑地址映射到物理地址， ARP (Address Resolution Protocol)  
物理地址映射到逻辑地址， RARP (Reversed Address Resolution Protocol)

# 以太网需要ARP协议



	192.168.0.3	192.168.0.2	MA	MB
--	-------------	-------------	----	----

↑  
目的IP地址  
↑  
源IP地址  
↑  
源MAC地址  
↑  
目的MAC地址

同一网段的帧

	192.168.1.4	192.168.0.2	MA	MD
--	-------------	-------------	----	----

↑  
目的IP地址  
↑  
源IP地址  
↑  
源MAC地址  
↑  
目的MAC地址

跨网段的帧

# 查看IP地址和MAC地址对应表

```
管理员: 命令提示符
版权所有 <c> 2009 Microsoft Corporation。保留所有权利。
C:\Users\Administrator>arp -a

接口: 168.168.214.20 --- 0xb
    Internet 地址          物理地址          类型
    168.168.214.32          18-60-24-98-27-16   动态
    168.168.214.99          18-60-24-ae-44-c0   动态
    168.168.214.254         78-2c-29-f5-d0-5b   动态
    168.168.214.255         ff-ff-ff-ff-ff-ff   静态
    224.0.0.22               01-00-5e-00-00-16   静态
    224.0.0.251              01-00-5e-00-00-fb   静态
    224.0.0.252              01-00-5e-00-00-fc   静态
    239.11.20.1              01-00-5e-0b-14-01   静态
    239.255.255.250         01-00-5e-7f-ff-fa   静态

接口: 192.168.56.1 --- 0xf
    Internet 地址          物理地址          类型
    192.168.56.255          ff-ff-ff-ff-ff-ff   静态
    224.0.0.22               01-00-5e-00-00-16   静态
    224.0.0.251              01-00-5e-00-00-fb   静态
    224.0.0.252              01-00-5e-00-00-fc   静态
    239.11.20.1              01-00-5e-0b-14-01   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

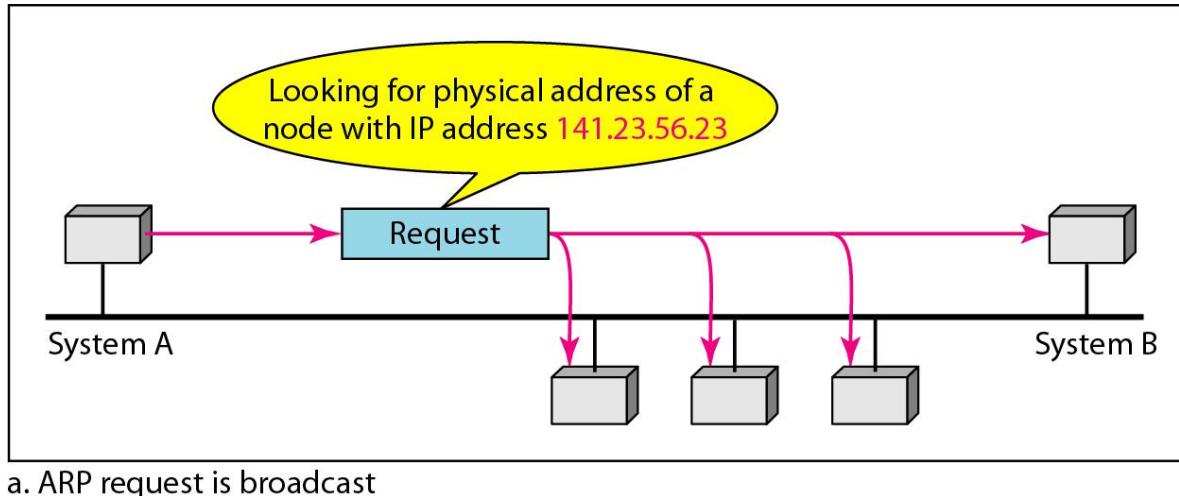
接口: 169.254.25.136 --- 0x12
    Internet 地址          物理地址          类型
    169.254.255.255         ff-ff-ff-ff-ff-ff   静态
    224.0.0.22               01-00-5e-00-00-16   静态
    224.0.0.251              01-00-5e-00-00-fb   静态
    224.0.0.252              01-00-5e-00-00-fc   静态
    239.11.20.1              01-00-5e-0b-14-01   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
```

# 地址映射

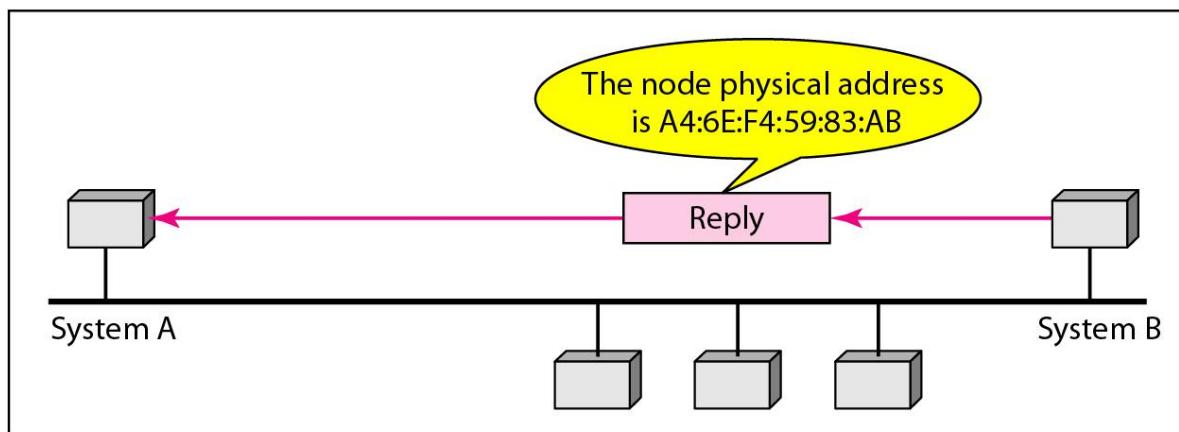
---

- 静态映射：创建一个将逻辑地址和物理地址对应的表，存储在网络的每个机器上。
- 动态映射：当机器知道逻辑地址和物理地址之一时，可以利用协议求出另一个地址。

## 图 21.1 ARP (Address Resolution Protocol)



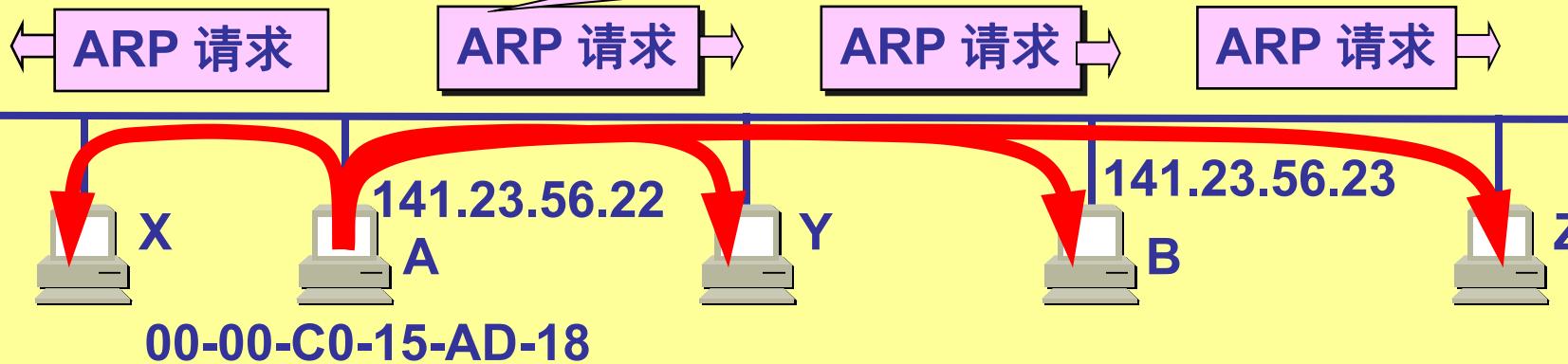
a. ARP request is broadcast



b. ARP reply is unicast

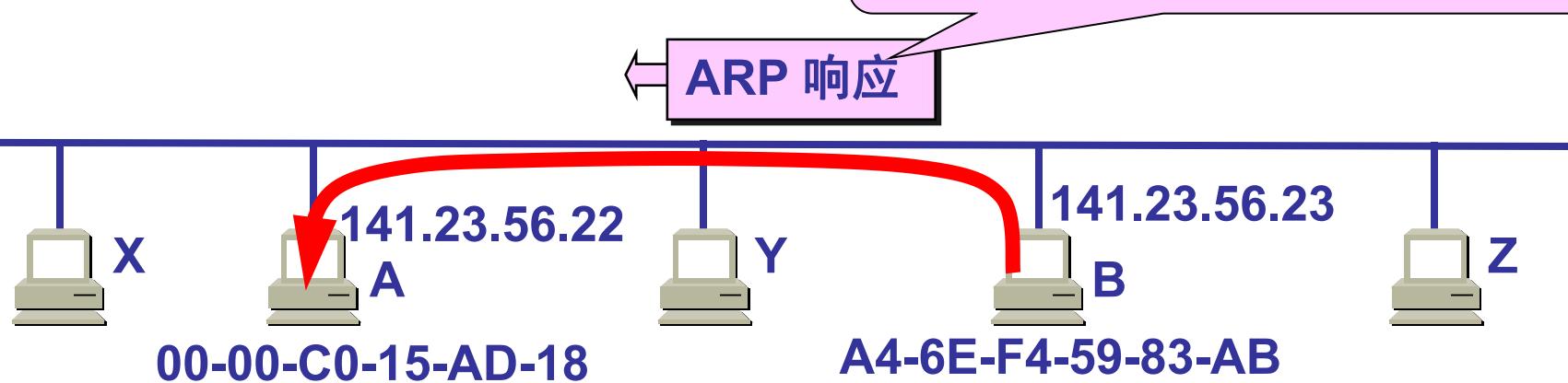
主机 A 广播发送  
ARP 请求分组

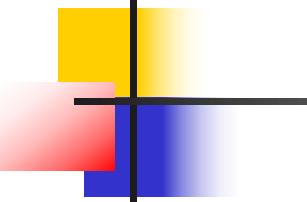
我是 141.23.56.22，硬件地址是 00-00-C0-15-AD-18  
我想知道主机 141.23.56.23 的硬件地址



主机 B 向 A 发送  
ARP 响应分组

我是 141.23.56.23  
硬件地址是 A4-6E-F4-59-83-AB





注意

---

**ARP 请求报文是广播发送，  
ARP 回答报文是单播发送。**

---

## 图 21.2 ARP 分组

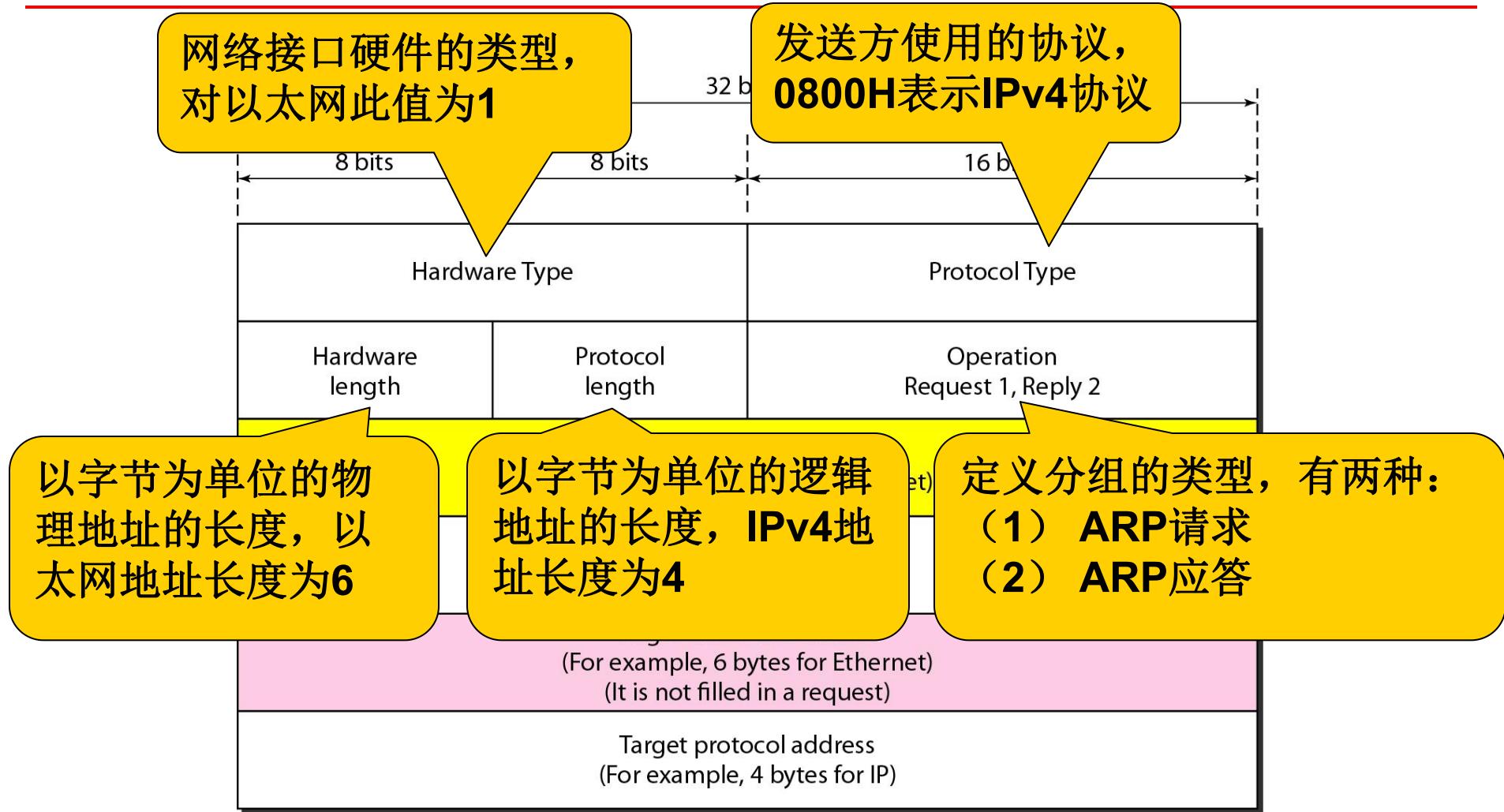
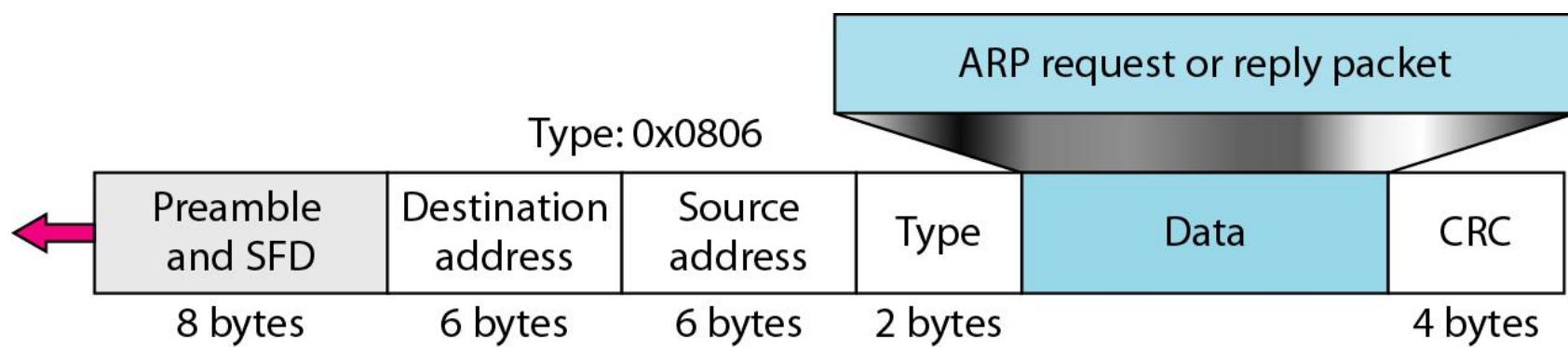


图 21.3 ARP 分组的封装



# ARP请求帧

Microsoft - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
107	35.518700	192.168.1.108	140.210.88.44	HTTP	Continuation or non-HTTP traffic
108	35.518952	192.168.1.108	140.210.88.44	HTTP	Continuation or non-HTTP traffic
109	37.465749	192.168.1.108	140.210.88.44	HTTP	Continuation or non-HTTP traffic
110	38.846968	06:d5:a6:6d:41:32	Broadcast	ARP	who has 192.168.1.1? Tell 192.168.1.104
111	41.920897	00:5c:86:06:c3:10	Broadcast	ARP	Who has 192.168.1.108? Tell 192.168.1.1
112	41.920930	5c:3a:45:c2:6c:c7	00:5c:86:06:c3:10	ARP	192.168.1.108 is at 5c:3a:45:c2:6c:c7
113	46.269920	192.168.1.108	117.33.163.3	TCP	[TCP Keep-Alive] 53022 > http [ACK] Seq=0 Ack=1
114	46.884407	192.168.1.108	117.33.163.3	TCP	[TCP Keep-Alive] 60559 > http [ACK] Seq=0 Ack=1
115	46.884407	192.168.1.108	117.33.163.3	TCP	[TCP Keep-Alive] 50286 > http [ACK] Seq=0 Ack=1
116	46.884591	192.168.1.108	117.33.163.3	TCP	[TCP Keep-Alive] 55544 > http [ACK] Seq=0 Ack=1
117	47.601470	192.168.1.108	117.33.163.3	TCP	[TCP Keep-Alive] 61420 > http [ACK] Seq=0 Ack=1
118	48.476019	117.18.232.200	192.168.1.108	TLSv1.2 Application Data	
119	48.476021	117.18.232.200	192.168.1.108	TLSv1.2 Encrypted Alert	
120	48.476021	117.18.232.200	192.168.1.108	TCP	https > 55290 [FIN, ACK] Seq=96 Ack=1 Win=135
121	48.476321	192.168.1.108	117.18.232.200	TCP	55290 > https [ACK] Seq=1 Ack=97 win=1024 Len=0

Frame 111: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)  
Ethernet II, Src: 00:5c:86:06:c3:10 (00:5c:86:06:c3:10), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
Destination: Broadcast (ff:ff:ff:ff:ff:ff)  
Source: 00:5c:86:06:c3:10 (00:5c:86:06:c3:10)  
Type: ARP (0x0806)  
Address Resolution Protocol (request)  
Hardware type: Ethernet (0x0001)  
Protocol type: IP (0x0800)  
Hardware size: 6  
Protocol size: 4  
Opcode: request (0x0001)  
[Is gratuitous: False]  
Sender MAC address: 00:5c:86:06:c3:10 (00:5c:86:06:c3:10)  
Sender IP address: 192.168.1.1 (192.168.1.1)  
Target MAC address: 00:00:00\_00:00:00 (00:00:00:00:00:00)  
Target IP address: 192.168.1.108 (192.168.1.108)

0000	ff ff ff ff ff ff	00 5c 86 06 c3 10	08 06 00 00 00 01	.....\.....
0010	08 00 06 04 00 01	00 5c 86 06 c3 10	c0 a8 01 01	.....\.....
0020	00 00 00 00 00 00	c0 a8 01 6c	.....\.....	1

# ARP应答帧

Microsoft - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
107	35.518700	192.168.1.108	140.210.88.44	HTTP	Continuation or non-HTTP traffic
108	35.518952	192.168.1.108	140.210.88.44	HTTP	Continuation or non-HTTP traffic
109	37.465749	192.168.1.108	140.210.88.44	HTTP	Continuation or non-HTTP traffic
110	38.846968	06:d5:5a:6d:41:32	Broadcast	ARP	Who has 192.168.1.1? Tell 192.168.1.104
111	41.920897	00:5c:86:06:c3:10	Broadcast	ARP	Who has 192.168.1.108? Tell 192.168.1.1
112	41.920930	5c:3a:45:c2:6c:c7	00:5c:86:06:c3:10	ARP	192.168.1.108 is at 5c:3a:45:c2:6c:c7
113	46.269920	192.168.1.108	117.33.163.3	TCP	[TCP Keep-Alive] 53022 > http [ACK] Seq=0 Ack=1
114	46.884407	192.168.1.108	117.33.163.3	TCP	[TCP Keep-Alive] 60559 > http [ACK] Seq=0 Ack=1
115	46.884407	192.168.1.108	117.33.163.3	TCP	[TCP Keep-Alive] 50286 > http [ACK] Seq=0 Ack=1
116	46.884591	192.168.1.108	117.33.163.3	TCP	[TCP Keep-Alive] 55544 > http [ACK] Seq=0 Ack=1
117	47.601470	192.168.1.108	117.33.163.3	TCP	[TCP Keep-Alive] 61420 > http [ACK] Seq=0 Ack=1
118	48.476019	117.18.232.200	192.168.1.108	TLSv1.2 Application Data	
119	48.476021	117.18.232.200	192.168.1.108	TLSv1.2 Encrypted Alert	
120	48.476021	117.18.232.200	192.168.1.108	TCP	https > 55290 [FIN, ACK] Seq=96 Ack=1 Win=135
121	48.476321	192.168.1.108	117.18.232.200	TCP	55290 > https [ACK] Seq=1 Ack=97 Win=1024 Len=0

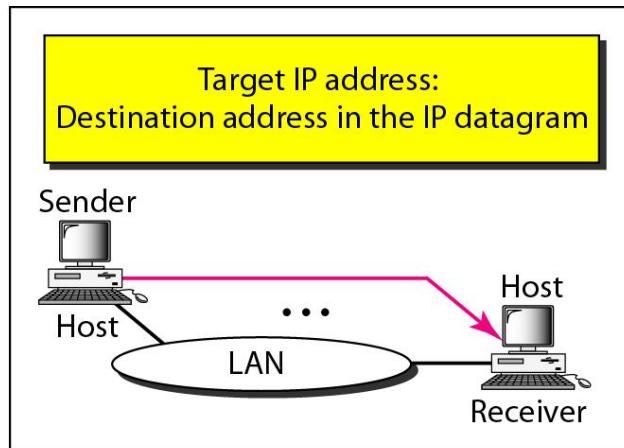
Frame 112: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)  
Ethernet II, Src: 5c:3a:45:c2:6c:c7 (5c:3a:45:c2:6c:c7), Dst: 00:5c:86:06:c3:10 (00:5c:86:06:c3:10)  
    Destination: 00:5c:86:06:c3:10 (00:5c:86:06:c3:10)  
    Source: 5c:3a:45:c2:6c:c7 (5c:3a:45:c2:6c:c7)  
    Type: ARP (0x0806)  
Address Resolution Protocol (reply)  
    Hardware type: Ethernet (0x0001)  
    Protocol type: IP (0x0800)  
    Hardware size: 6  
    Protocol size: 4  
    Opcode: reply (0x0002)  
    [Is gratuitous: False]  
    Sender MAC address: 5c:3a:45:c2:6c:c7 (5c:3a:45:c2:6c:c7)  
    Sender IP address: 192.168.1.108 (192.168.1.108)  
    Target MAC address: 00:5c:86:06:c3:10 (00:5c:86:06:c3:10)  
    Target IP address: 192.168.1.1 (192.168.1.1)

0000	00	5c	86	06	c3	10	5c	3a	45	c2	6c	c7	08	06	00	01	.\\....\\: E.1....;
0010	08	00	06	04	00	02	5c	3a	45	c2	6c	c7	c0	a8	01	6c	.\\....\\: E.1....;
0020	00	5c	86	06	c3	10	c0	a8	01	01	..	..	..	..	..	..	..

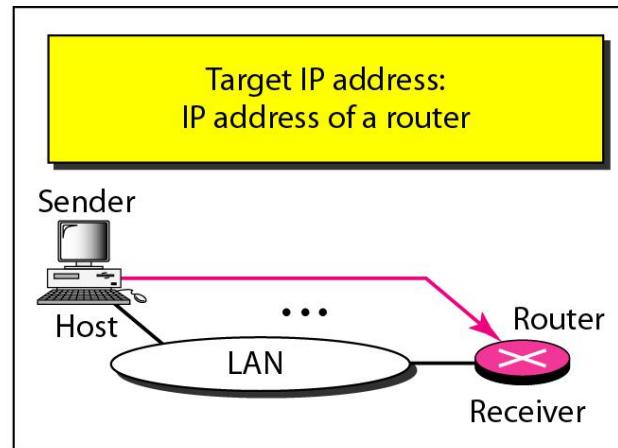
# ARP工作过程

- IP请求ARP协议产生一个ARP请求报文，填入发送方物理地址、IP地址以及目标的IP地址，目标的物理地址字段填0；
- 将这个报文发送给数据链路层封装成帧，使用发送方物理地址作为源地址进行广播；
- 每个主机和路由器均接收到此帧，除了目标机器，其它机器丢弃该帧；
- 目标机器使用单播方式以ARP回答报文进行应答，回答报文包括其物理地址；
- 发送方收到回答报文，知道目标机器的物理地址；
- 将发送给目标机器的IP数据报封装成帧，以单播方式发送。

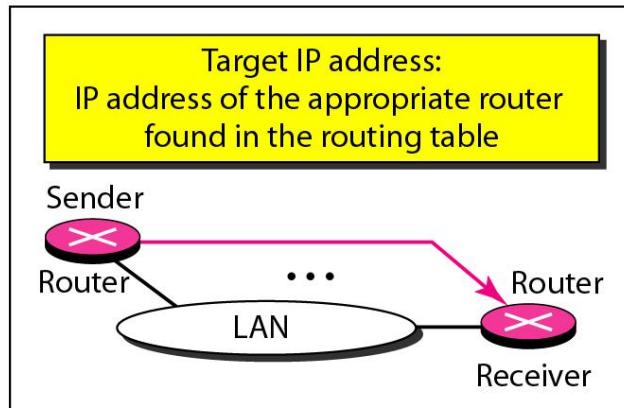
## 图 21.4 使用ARP的四种情况



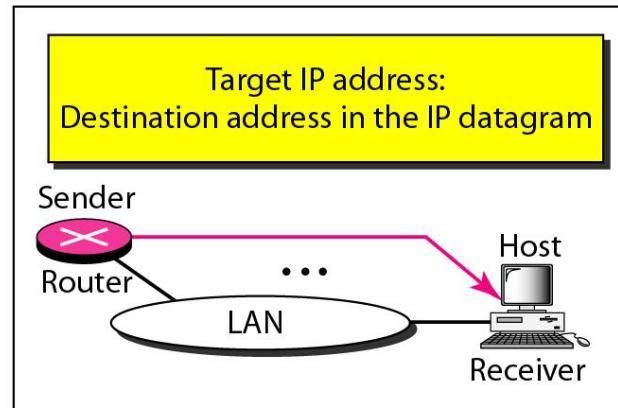
Case 1. A host has a packet to send to another host on the same network.



Case 2. A host wants to send a packet to another host on another network.  
It must first be delivered to a router.



Case 3. A router receives a packet to be sent to a host on another network. It must first be delivered to the appropriate router.



Case 4. A router receives a packet to be sent to a host on the same network.

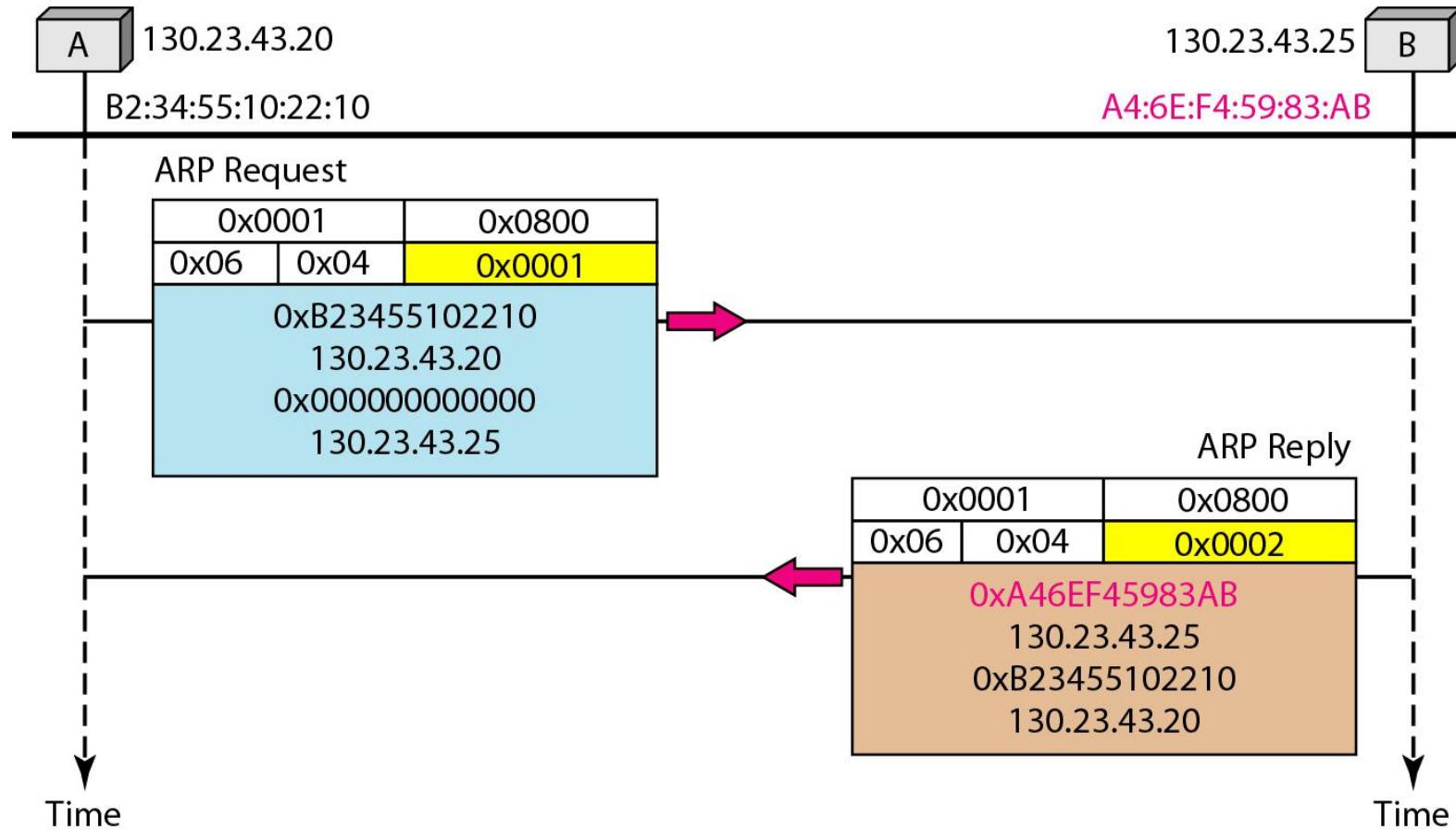
## 例 21.1

一个主机的IP地址为130.23.43.20，物理地址为B2:34:55:10:22:10，它有一个分组想要发送给另一个主机，其IP地址为130.23.43.25，物理地址为A4:6E:F4:59:83:AB（第一个主机不知道该物理地址）。两个主机在同一个网络上。试说明ARP请求与回答分组如何封装在以太网帧中。

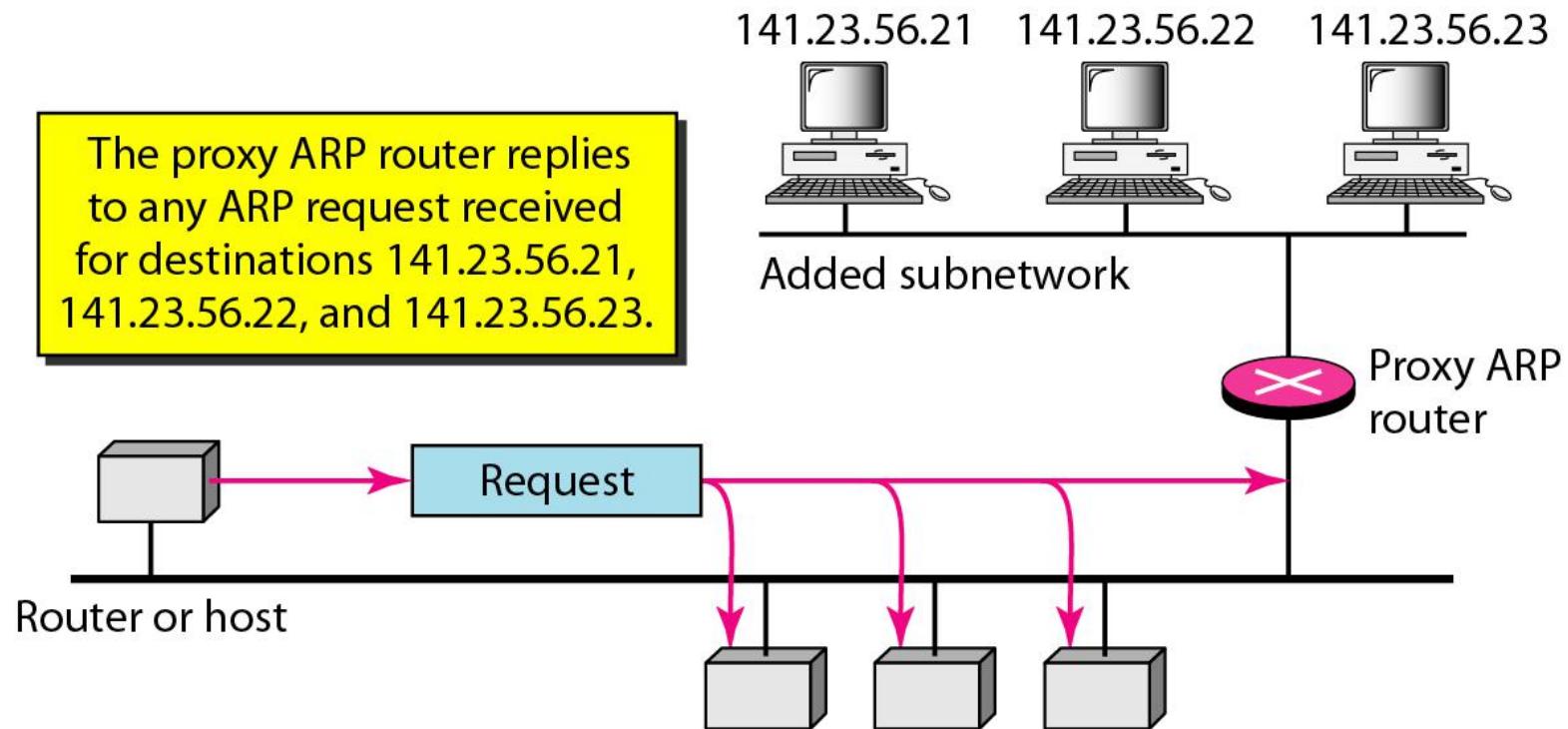
**解答：**

图 21.5 显示了ARP请求与回答分组。注意：此时 ARP数据字段是28个字节，而单个地址不适合用4字节表示界限，这就是不以4字节界限表示这些地址的原因。

图 21.5 例 21.1 ARP 请求与回答分组

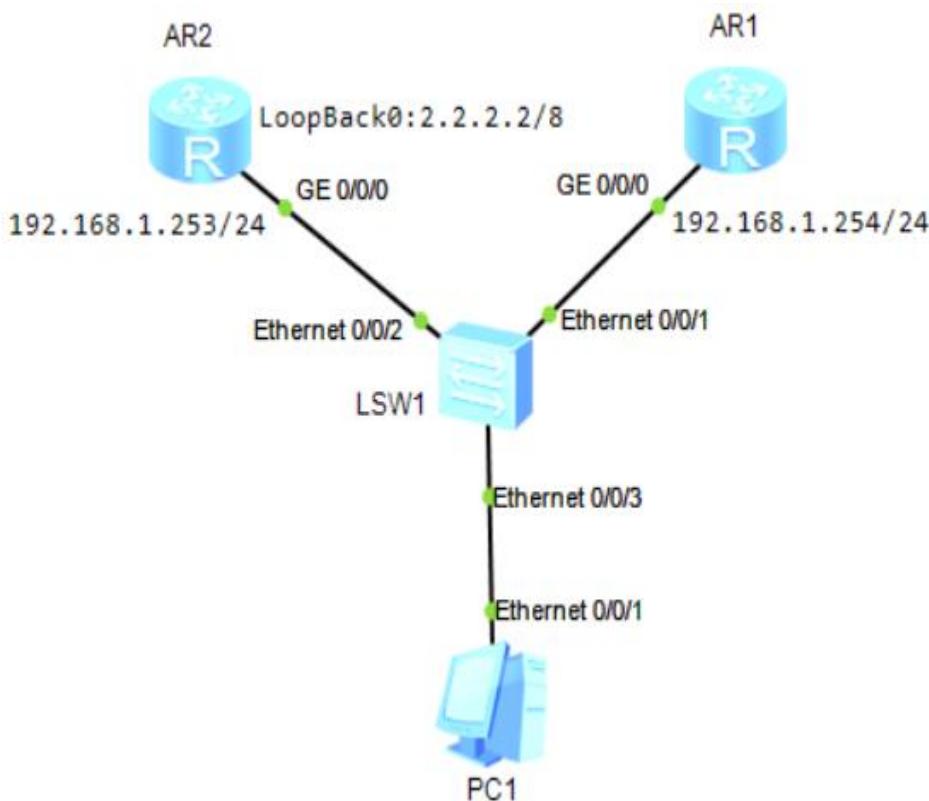


## 图 21.6 代理ARP



# ARP和ping命令

在执行ping命令时，第一个包常常会丢失，这是因为开始时ARP缓存中还没有映射信息，第一个包没有ARP解析，也就没有对应的目的MAC地址，因此无法发出去。后面的包在有了地址映射信息之后就可以发送了。



PC1

基础配置 命令行 组播 UDP发包工具 串口

Welcome to use PC Simulator!

PC>arp -a

Internet Address	Physical Address	Type
2.2.2.2	00-E0-FC-8A-5B-21	dynamic

PC>ping 2.2.2.2

Ping 2.2.2.2: 32 data bytes, Press Ctrl\_C to break Request timeout!

From 2.2.2.2: bytes=32 seq=2 ttl=255 time=125 ms

From 2.2.2.2: bytes=32 seq=3 ttl=255 time=63 ms

From 2.2.2.2: bytes=32 seq=4 ttl=255 time=62 ms

From 2.2.2.2: bytes=32 seq=5 ttl=255 time=47 ms

--- 2.2.2.2 ping statistics ---

5 packet(s) transmitted

4 packet(s) received

20.00% packet loss

round-trip min/avg/max = 0/74/125 ms

PC>arp -a

Internet Address	Physical Address	Type
192.168.1.253	00-E0-FC-8A-5B-21	dynamic
192.168.1.254	00-E0-FC-EB-53-B6	dynamic

# ARP欺骗

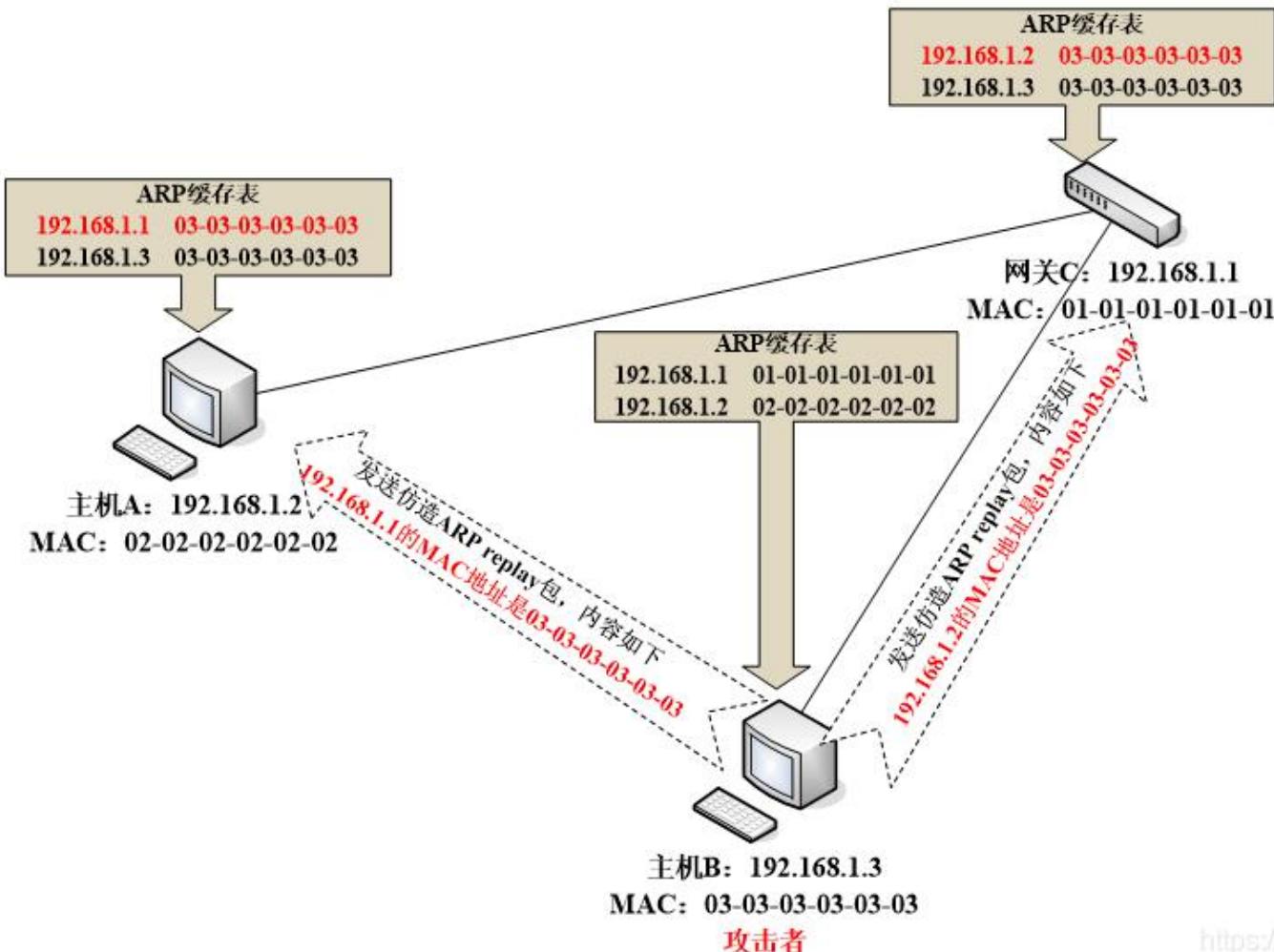
## ◆ 对路由器ARP表的欺骗

通知路由器一系列错误的内网MAC地址，并按照一定的频率不断进行，使真实的地址信息无法通过更新保存在路由器中，结果路由器的所有数据只能发送给错误的MAC地址，造成正常PC无法收到信息。

## ◆ 对内网PC的网关欺骗

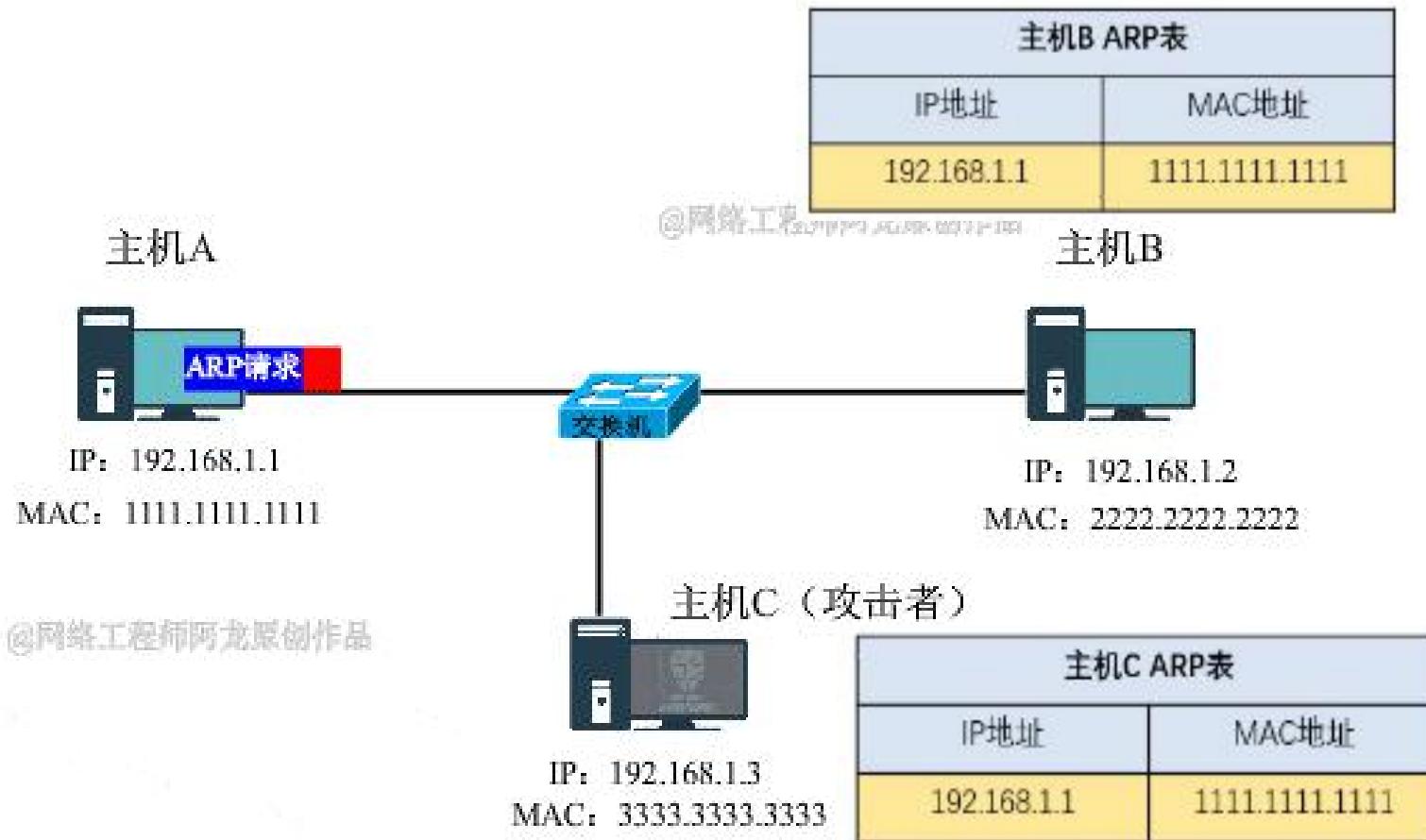
建立虚假网关，使被欺骗的PC向假网关发送数据，而不是通过正常的路由器途径上网。ARP欺骗可以导致目标计算机与网关通信失败，更会导致通信重定向，所有的数据都会通过攻击者的机器，因此存在极大的安全隐患。

# ARP欺骗

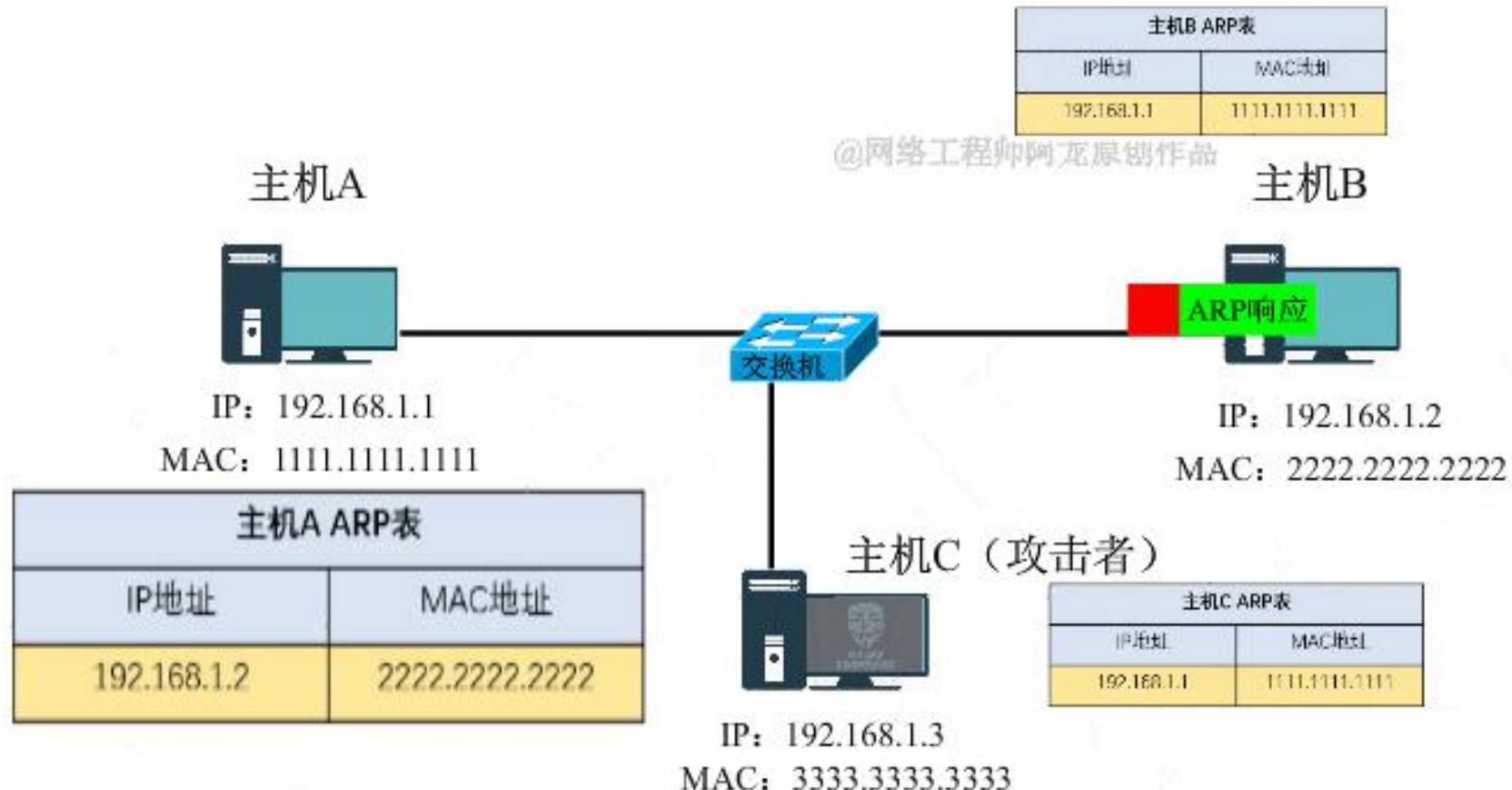


# ARP欺骗

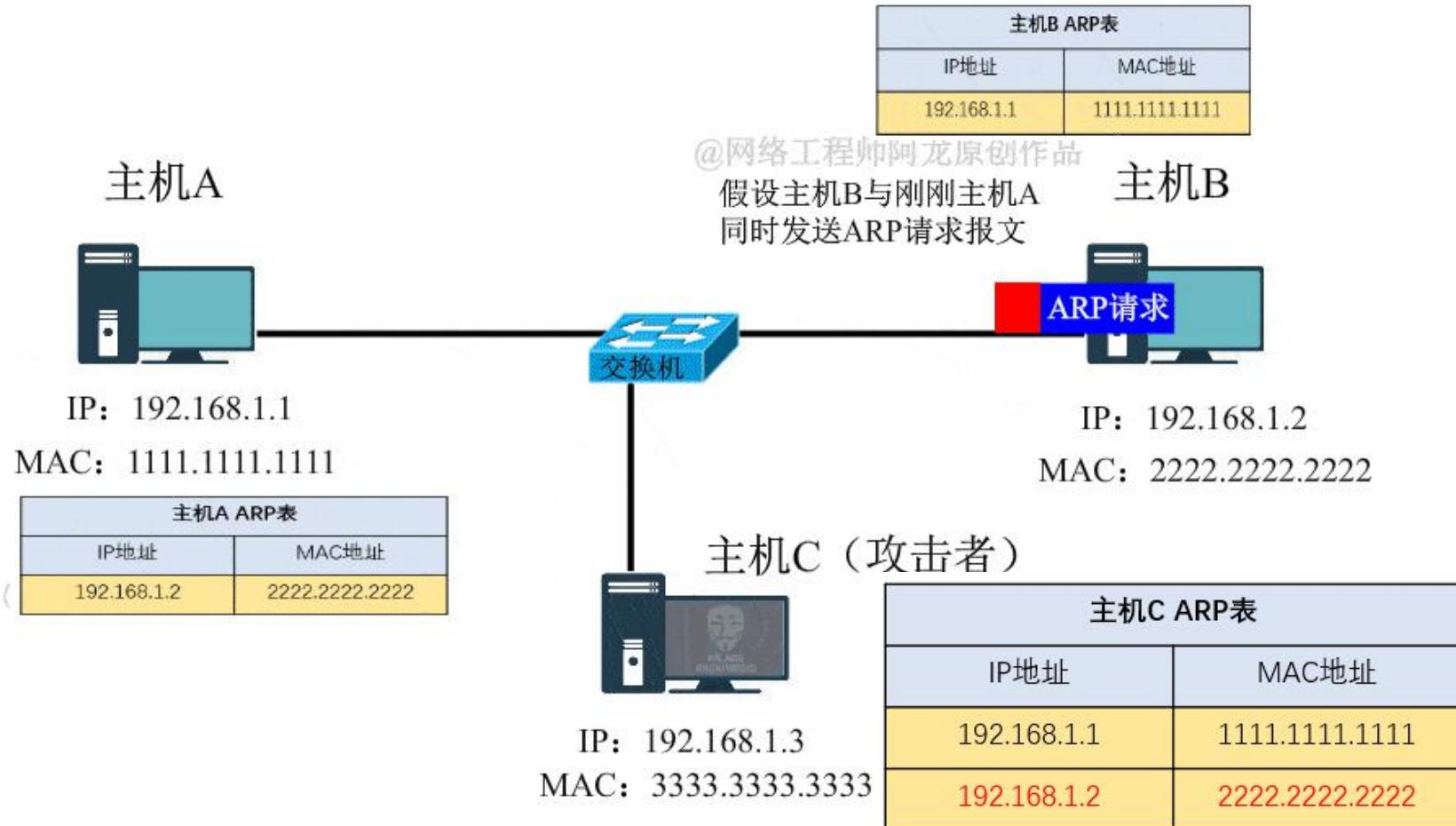
## 1、信息收集：局域网内正常用户的IP和MAC信息



# ARP欺骗

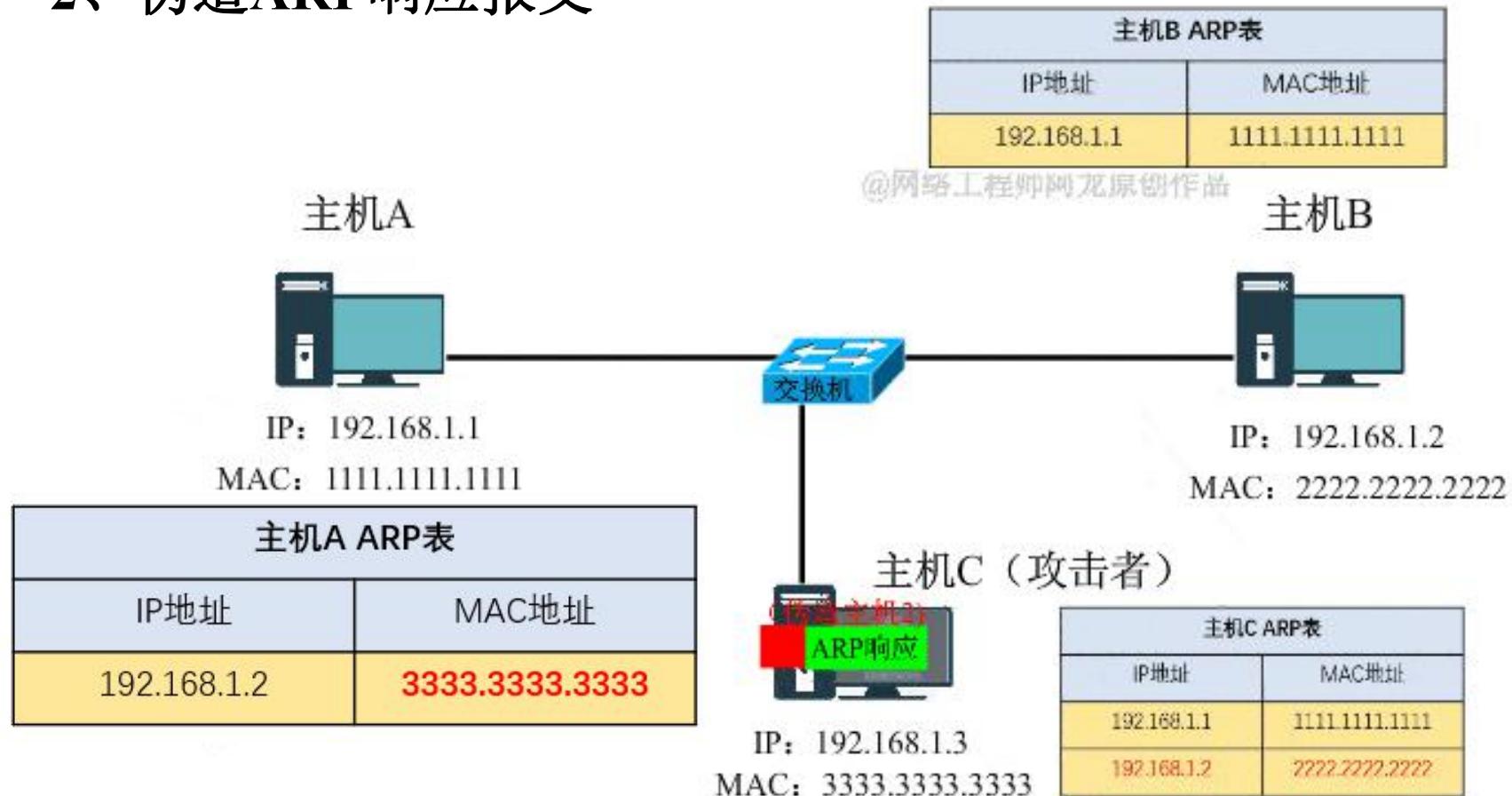


# ARP欺骗



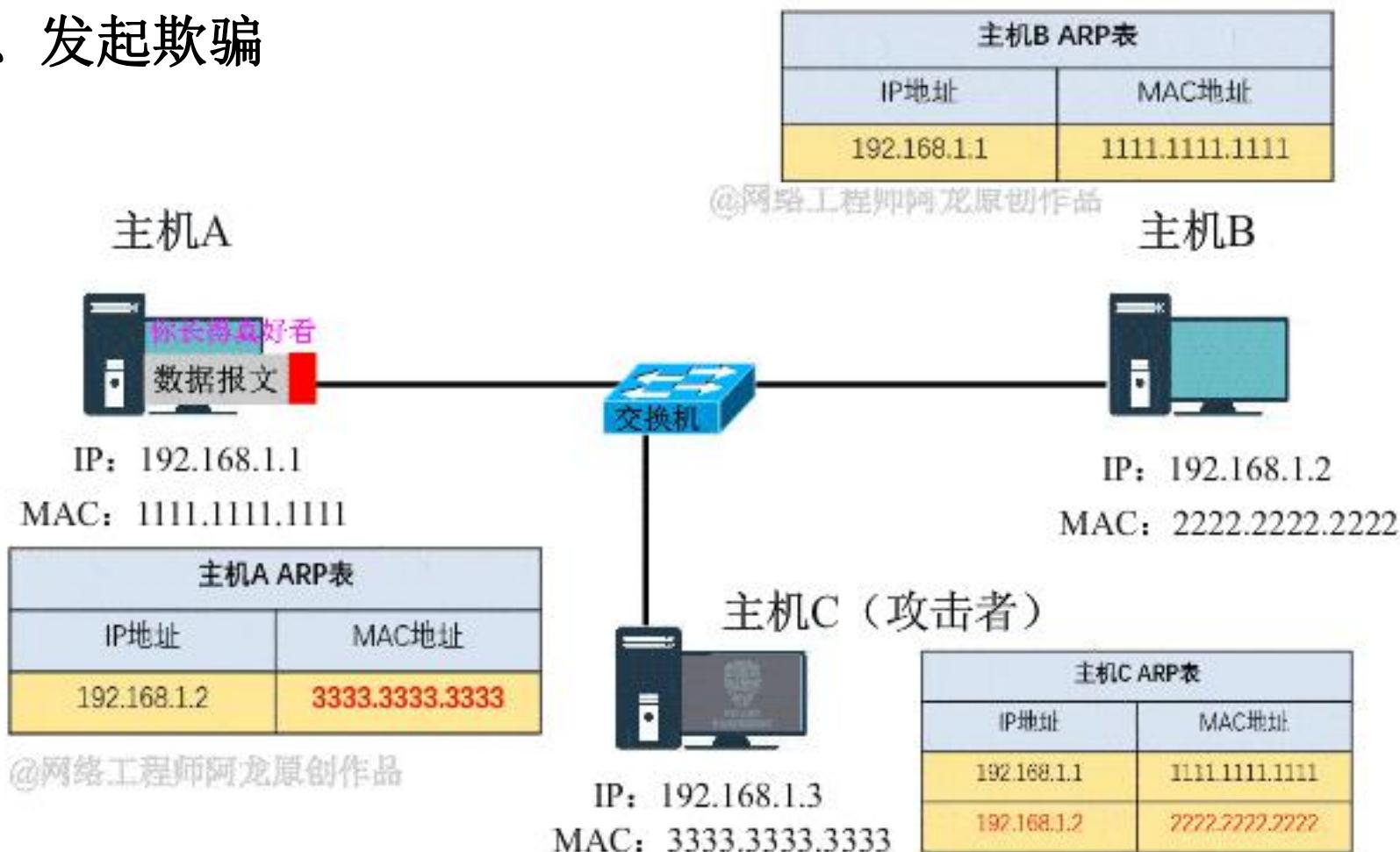
# ARP欺骗

## 2、伪造ARP响应报文



# ARP欺骗

## 3、发起欺骗



# 物理地址到逻辑地址的映射RARP

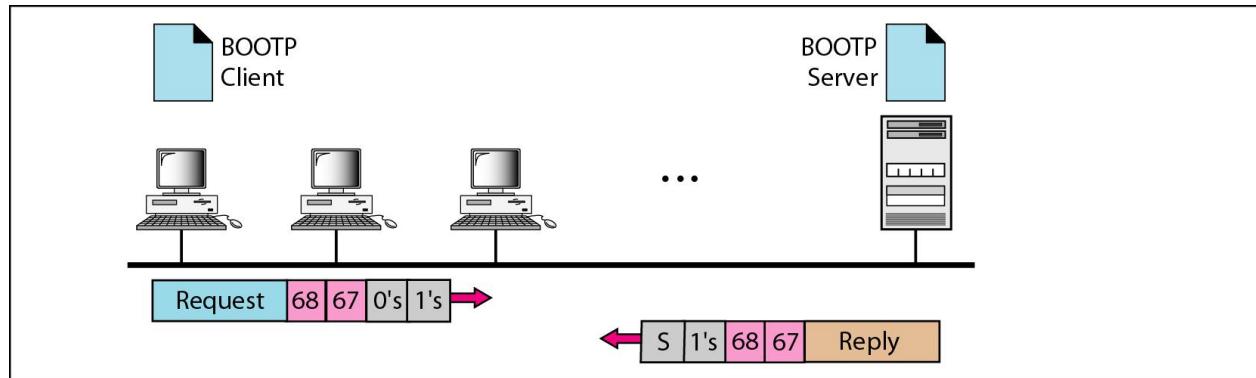
---

- 网络上的每台设备都会有一个硬件地址，通常是由设备厂商分配的MAC地址。PC从网卡上读取MAC地址，然后在网络上发送一个RARP请求的广播数据包，请求RARP服务器回复该PC的IP地址。RARP服务器收到了RARP请求数据包，为其分配IP地址，并将RARP回应发送给PC。PC收到RARP回应后，就使用得到的IP地址进行通信。
- 虽然RARP在概念上很简单，但是一个RARP服务器的设计与系统相关而且比较复杂。相反，提供一个ARP服务器很简单，通常是TCP/IP在内核中实现的一部分。由于内核知道IP地址和硬件地址，因此当它收到一个询问IP地址的ARP请求时，只需用相应的硬件地址来提供应答就可以了。
- 由于RARP的请求是在硬件层上的广播，不能通过路由转发，因此在每个网络都要设置一个RARP服务器。另外在同一网络中不同主机可能会同时进行RARP请求，增大了冲突的概率。

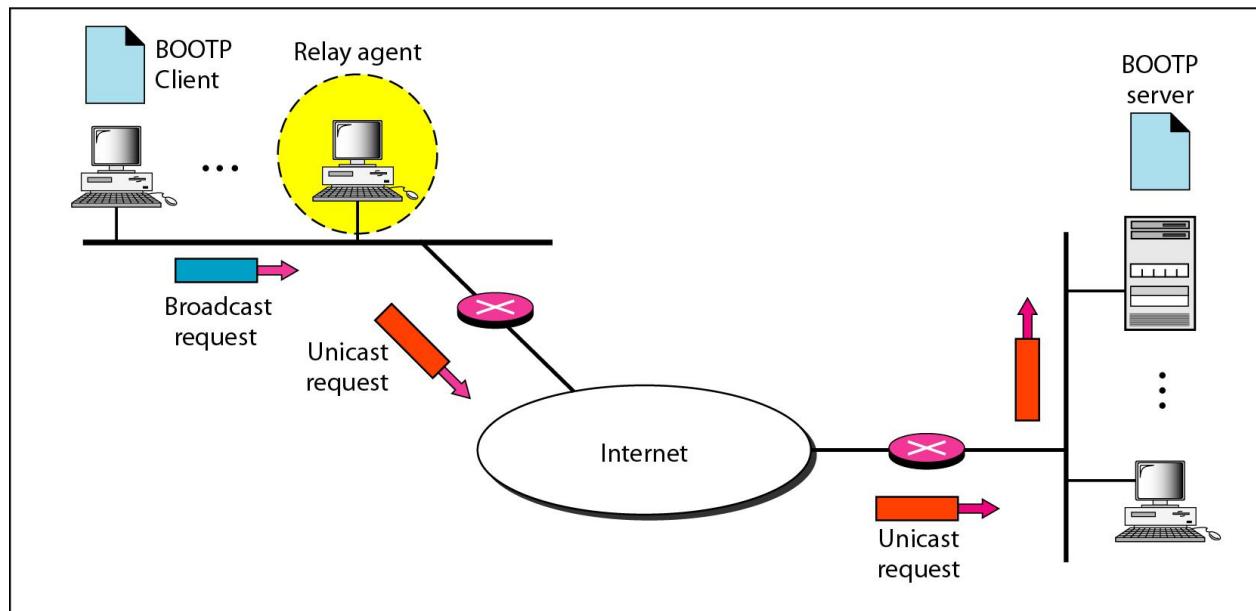
# 引导程序协议BOOTP（Bootstrap Protocol）

- BOOTP是一种引导协议，基于IP/UDP协议，也称自举协议，是DHCP协议的前身。
- BOOTP用于无盘工作站的局域网中，可以让无盘工作站从中心服务器获得IP地址。通过BOOTP协议可以为局域网中的无盘工作站分配动态IP地址，这样就不需要管理员去为每个用户去设置静态IP地址。
- DHCP协议是从BOOTP的基础上发展而来，它们都是主机配置协议，都可以大大减少管理员的工作量。BOOTP可看成是简单版的DHCP，是对主机的静态配置，而DHCP可以依据一些策略对主机进行动态配置。BOOTP用于无盘工作站的启动和配置，而DHCP更适用于客户端接入变化的网络，即客户端接入时间、接入地点不固定。

图 21.7 在同一网络上和不同网络上的 BOOTP客户和服务器



a. Client and server on the same network



b. Client and server on different networks

# 动态主机配置协议DHCP（Dynamic Host Configuration Protocol）

---

- DHCP服务器控制一段IP地址范围，客户机登录服务器时就可自动获得服务器分配的IP地址和子网掩码，是局域网的网络协议。
- DHCP 提供人工的或自动的、静态或动态的地址配置。静态地址配置与BOOTP相同，与BOOTP后向兼容，客户机可请求静态地址，DHCP服务器有一个数据库静态地绑定物理地址和IP地址。
- DHCP还有一个动态数据库，即一个可用的IP地址池。DHCP客户机向DHCP服务器发送请求时，服务器先查询静态数据库，如有则返回永久IP地址；如没有则从可用IP地址池中选择一个IP地址，指定给该用户并添加到动态数据库。
- 得到的IP地址有租用期（lease）。

# 动态主机配置协议DHCP

---

## ■ DHCP DISCOVER寻找服务器

当 DHCP客户端首次登录网络的时候，如果发现本机上没有任何IP配置，则会向网络发出一个 DHCP Discover广播，源地址为 0.0.0.0，目的地址则为 255.255.255.255。

## ■ DHCP OFFER分配IP地址

当DHCP服务器监听到客户端发出的 DHCP Discover 广播后，它会从那些还没有租出的地址范围内，选择最前面的空置IP，连同其它TCP/IP设定，发给客户端一个DHCP Offer，DHCP Offer会包含一个租约期限的信息。

# 动态主机配置协议DHCP

---

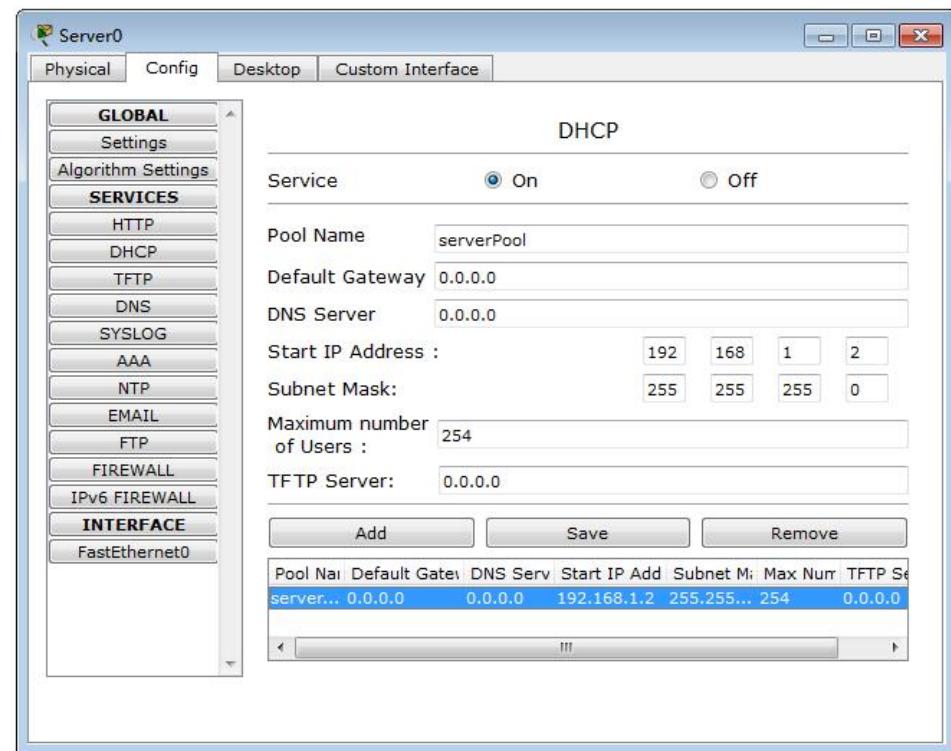
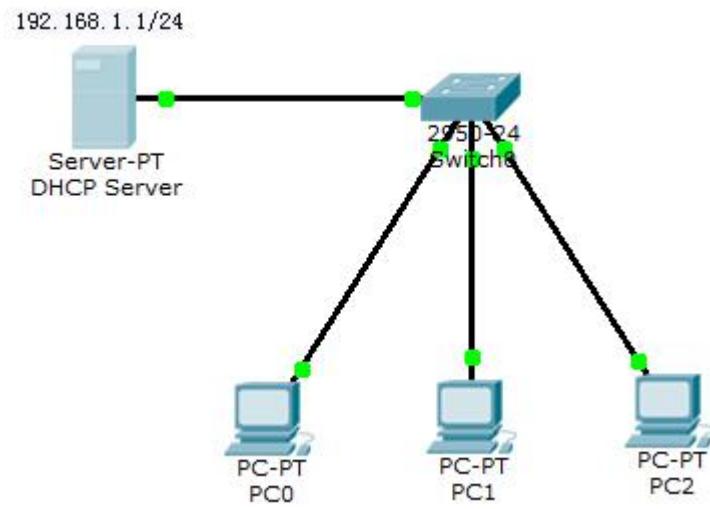
## ■ DHCP REQUEST 请求使用

如果客户端收到网络上多台DHCP协议服务器的响应，只会挑选其中一个DHCP Offer，并向网络发送一个DHCP Request广播，告诉所有DHCP服务器它将指定接受哪一台服务器提供的IP地址。同时，客户端还会向网络发送一个ARP，查询网络上面有没有其它机器使用该IP地址；如果发现该IP已经被占用，客户端则会送出一个DHCP Decline给DHCP服务器，拒绝接受其DHCP Offer，并重新发送DHCP Discover信息。

## ■ DHCP ACK IP地址分配确认

当DHCP服务器收到DHCP客户机回答的DHCP Request请求信息之后，它便向DHCP客户机发送一个包含它所提供的IP地址和其他设置的DHCP Ack确认信息，确认IP地址的正式生效。然后DHCP客户机便将其TCP/IP协议与网卡绑定。除DHCP客户机选中的服务器外，其它的DHCP服务器都将收回曾提供的IP地址。

# 动态主机配置协议DHCP



## 21-2 ICMP (Internet Control Message Protocol)

IP 协议没有差错报告或差错纠正机制。IP协议还缺少一种为主机和管理查询的机制。因特网控制报文协议 (**ICMP**) 就是为了弥补上述两个缺点而设计的，它是配合IP协议使用的。

### 讨论:

报文类型

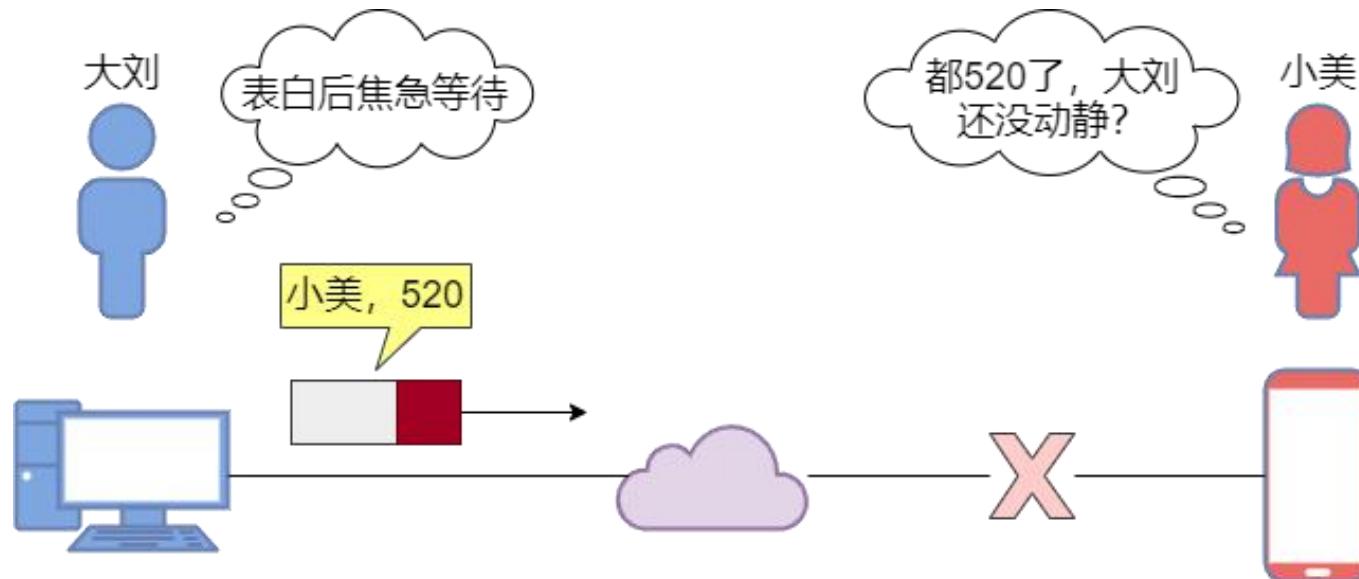
报文格式

差错报告和查询

调试工具

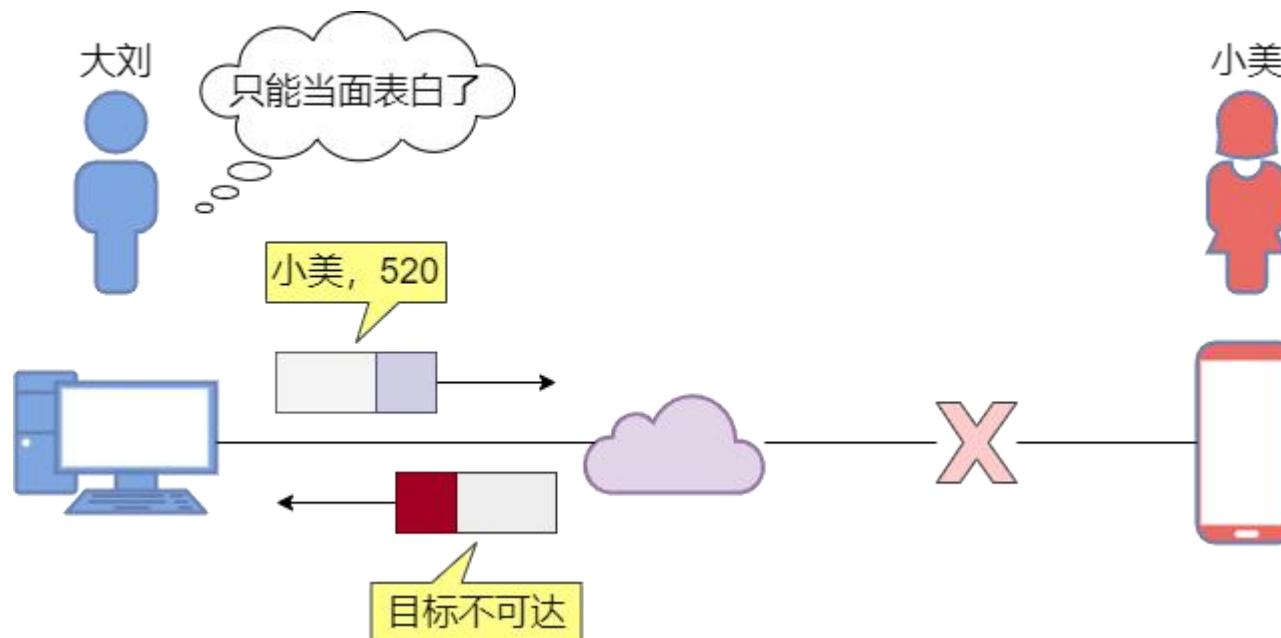
# 问题

IP 是尽最大努力传输的网络协议，提供的数据传输服务是不可靠的、无连接的，不能保证数据包能成功到达目的地。那么，如何确定数据包是否成功到达了目的地？



# 为什么需要ICMP？

这就需要一个网络层协议，提供错误检测功能和报告机制功能，于是出现了 **ICMP**。ICMP 的主要功能是，确认 IP 包是否成功送达目的地址，通知发送过程中 IP 包被丢弃的原因。有了这些功能，就可以检查网络是否正常、网络配置是否正确、设备是否异常等信息，方便进行网络问题诊断。

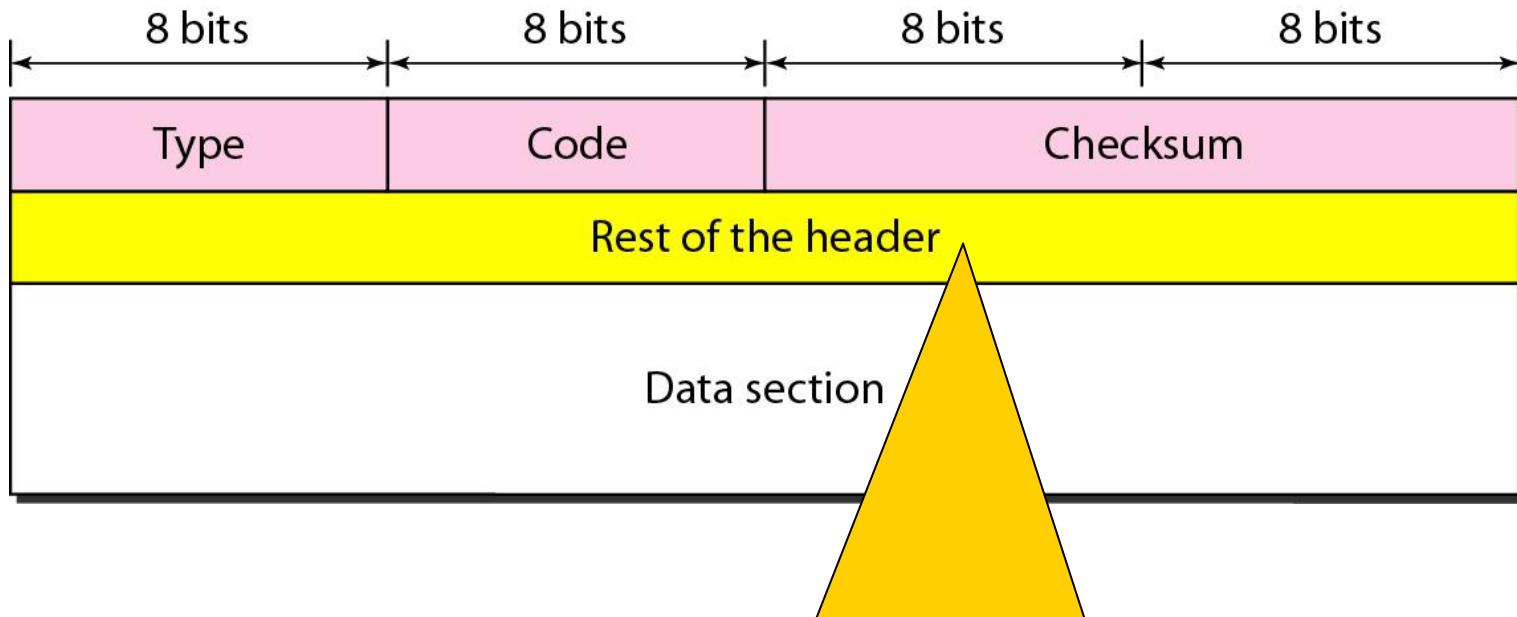


# ICMP的特点

---

- 为了提高 IP 数据报交付成功的机会，在网际层使用了因特网控制报文协议 ICMP。
- ICMP 允许主机或路由器报告差错情况和提供有关异常情况的报告。
- ICMP 不是高层协议，而是 IP 层的协议。ICMP 报文作为 IP 层数据报的数据，加上数据报的首部，组成 IP 数据报发送出去。
- ICMP不能纠错，只能报告错误。
- ICMP分为**差错报告报文**和**查询报文**。

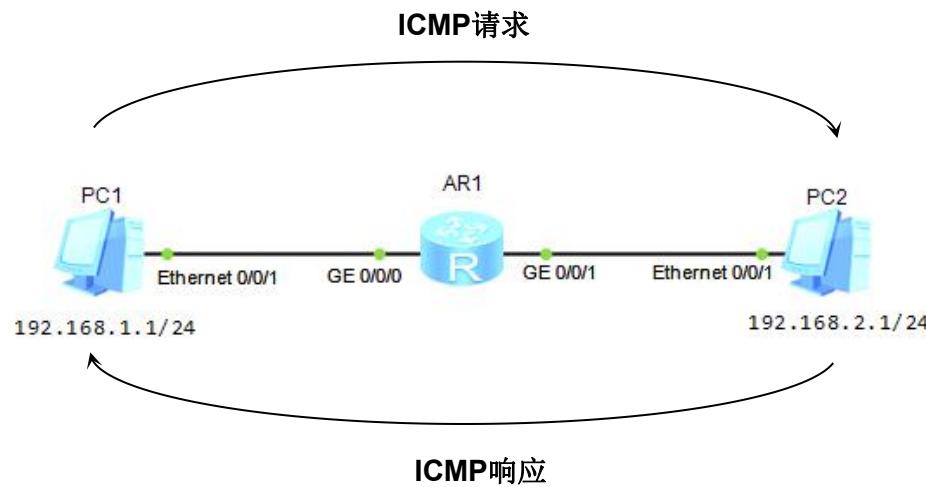
图 21.8 ICMP 报文一般格式



这 4 个字节取决于 ICMP 报文的类型

注意： ICMP 总是向原始的源方报告差错报文。

# ICMP 请求和响应报文



A screenshot of a software window titled 'PC1'. The window contains a terminal-like interface with the following text:

```
基础配置 命令行 组播 UDP发包工具 串口
Welcome to use PC Simulator!
PC>ping 192.168.2.1

Ping 192.168.2.1: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
From 192.168.2.1: bytes=32 seq=3 ttl=127 time=16 ms
From 192.168.2.1: bytes=32 seq=4 ttl=127 time=16 ms
From 192.168.2.1: bytes=32 seq=5 ttl=127 time=16 ms

--- 192.168.2.1 ping statistics ---
5 packet(s) transmitted
3 packet(s) received
40.00% packet loss
round-trip min/avg/max = 0/16/16 ms

PC>
```

# ICMP 请求报文

Capturing from Standard input - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	HuaweiTe_10:14:78	Broadcast	ARP	who has 192.168.2.1? Tell 192.168.2.254
2	0.000000	HuaweiTe_de:05:98	HuaweiTe_10:14:78	ARP	192.168.2.1 is at 54:89:98:de:05:98
3	1.966000	192.168.1.1	192.168.2.1	ICMP	Echo (ping) request (id=0xca30, seq(be/le)=2/512, ttl=127)
4	1.966000	192.168.2.1	192.168.1.1	ICMP	Echo (ping) reply (id=0xca30, seq(be/le)=2/512, ttl=128)
5	3.963000	192.168.1.1	192.168.2.1	ICMP	Echo (ping) request (id=0xcc30, seq(be/le)=3/768, ttl=127)
6	3.963000	192.168.2.1	192.168.1.1	ICMP	Echo (ping) reply (id=0xcc30, seq(be/le)=3/768, ttl=128)
7	4.977000	192.168.1.1	192.168.2.1	ICMP	Echo (ping) request (id=0xcd30, seq(be/le)=4/1024, ttl=127)
8	4.977000	192.168.2.1	192.168.1.1	ICMP	Echo (ping) reply (id=0xcd30, seq(be/le)=4/1024, ttl=128)
9	5.975000	192.168.1.1	192.168.2.1	ICMP	Echo (ping) request (id=0xce30, seq(be/le)=5/1280, ttl=127)
10	5.991000	192.168.2.1	192.168.1.1	ICMP	Echo (ping) reply (id=0xce30, seq(be/le)=5/1280, ttl=128)

Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)  
Ethernet II, Src: HuaweiTe\_10:14:78 (00:e0:fc:10:14:78), Dst: HuaweiTe\_de:05:98 (54:89:98:de:05:98)  
Internet Protocol, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.2.1 (192.168.2.1)  
Internet Control Message Protocol  
Type: 8 (Echo (ping) request)  
Code: 0  
Checksum: 0xbc4b [correct]  
Identifier: 0xca30  
Sequence number: 2 (0x0002)  
Sequence number (LE): 512 (0x0200)  
Data (32 bytes)

0000	54	89	98	de	05	98	00	e0	fc	10	14	78	08	00	45	00	T..... . . . x . . E.
0010	00	3c	30	c9	40	00	7f	01	46	a5	c0	a8	01	01	c0	a8	. <0. @ . . . F . . . . .
0020	02	01	08	00	bc	4b	ca	30	00	02	08	09	0a	0b	0c	0d	. . . . . K . 0 . . . . .
0030	0e	0f	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	. . . . . . . . . . . . . . .
0040	1e	1f	20	21	22	23	24	25	26	27							.. ! "# \$ % &

Standard input: <live capture in progress... Packets: 10 Displayed: 10 Marked: 0 Profile: Default

# ICMP 响应报文

Capturing from Standard input - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

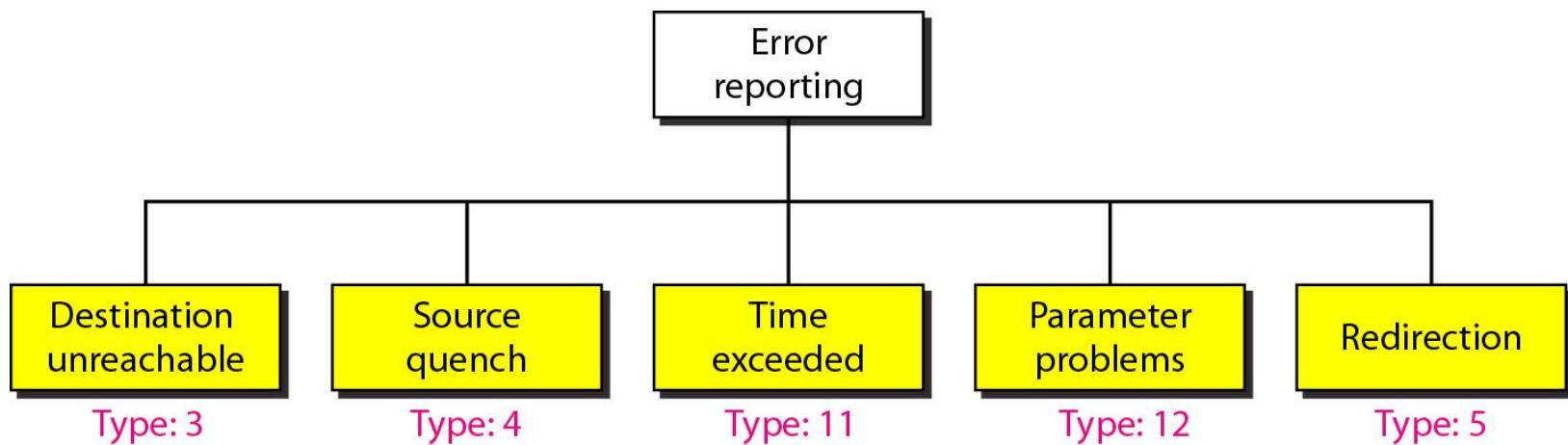
No.	Time	Source	Destination	Protocol	Info
1	0.000000	HuaweiTe_10:14:78	Broadcast	ARP	who has 192.168.2.1? Tell 192.168.2.254
2	0.000000	HuaweiTe_de:05:98	HuaweiTe_10:14:78	ARP	192.168.2.1 is at 54:89:98:de:05:98
3	1.966000	192.168.1.1	192.168.2.1	ICMP	Echo (ping) request (id=0xca30, seq(be/le)=2/512, ttl=127)
4	1.966000	192.168.2.1	192.168.1.1	ICMP	Echo (ping) reply (id=0xca30, seq(be/le)=2/512, ttl=128)
5	3.963000	192.168.1.1	192.168.2.1	ICMP	Echo (ping) request (id=0xcc30, seq(be/le)=3/768, ttl=127)
6	3.963000	192.168.2.1	192.168.1.1	ICMP	Echo (ping) reply (id=0xcc30, seq(be/le)=3/768, ttl=128)
7	4.977000	192.168.1.1	192.168.2.1	ICMP	Echo (ping) request (id=0xcd30, seq(be/le)=4/1024, ttl=127)
8	4.977000	192.168.2.1	192.168.1.1	ICMP	Echo (ping) reply (id=0xcd30, seq(be/le)=4/1024, ttl=128)
9	5.975000	192.168.1.1	192.168.2.1	ICMP	Echo (ping) request (id=0xce30, seq(be/le)=5/1280, ttl=127)
10	5.991000	192.168.2.1	192.168.1.1	ICMP	Echo (ping) reply (id=0xce30, seq(be/le)=5/1280, ttl=128)

Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)  
Ethernet II, Src: HuaweiTe\_de:05:98 (54:89:98:de:05:98), Dst: HuaweiTe\_10:14:78 (00:e0:fc:10:14:78)  
Internet Protocol, Src: 192.168.2.1 (192.168.2.1), Dst: 192.168.1.1 (192.168.1.1)  
Internet Control Message Protocol  
Type: 0 (Echo (ping) reply)  
Code: 0  
Checksum: 0xc44b [correct]  
Identifier: 0xca30  
Sequence number: 2 (0x0002)  
Sequence number (LE): 512 (0x0200)  
Data (32 bytes)

0000	00	e0	fc	10	14	78	54	89	98	de	05	98	08	00	45	00	.....XT. ....E.
0010	00	3c	30	c9	40	00	80	01	45	a5	c0	a8	02	01	c0	a8	.<0. @... E.....
0020	01	01	00	00	c4	4b	ca	30	00	02	08	09	0a	0b	0c	0d	.....K.0 .....
0030	0e	0f	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	....!#"\$. &'
0040	1e	1f	20	21	22	23	24	25	26	27							

Standard input: <live capture in progress> Packets: 10 Displayed: 10 Marked: 0 Profile: Default

图 21.9 差错报告报文



# ICMP报文类型和代码意义

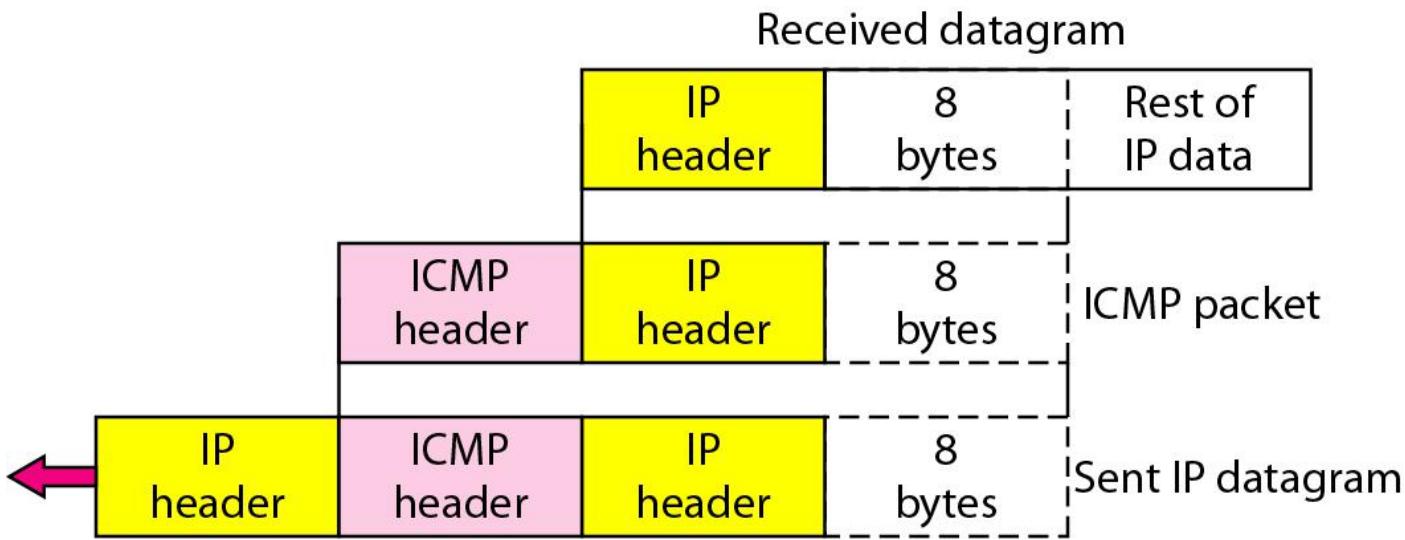
报文类型	类型值	代码	描述
请求报文	8	0	请求回显报文
响应报文	0	0	回显应答报文
差错报告报文	3 (终点不可达)	0	网络不可达
		1	主机不可达
		2	协议不可达
		3	端口不可达
		4	需要进行分片但设置了不分片
		13	由于路由器过滤，通信被禁止
	4	0	源端被关闭
	5 (改变路由)	0	对网络重定向
		1	对主机重定向
	11	0	传输期间生存时间TTL=0
12 (参数问题)		0	坏的IP首部
		1	缺少必要的选项

# ICMP 差错报文

---

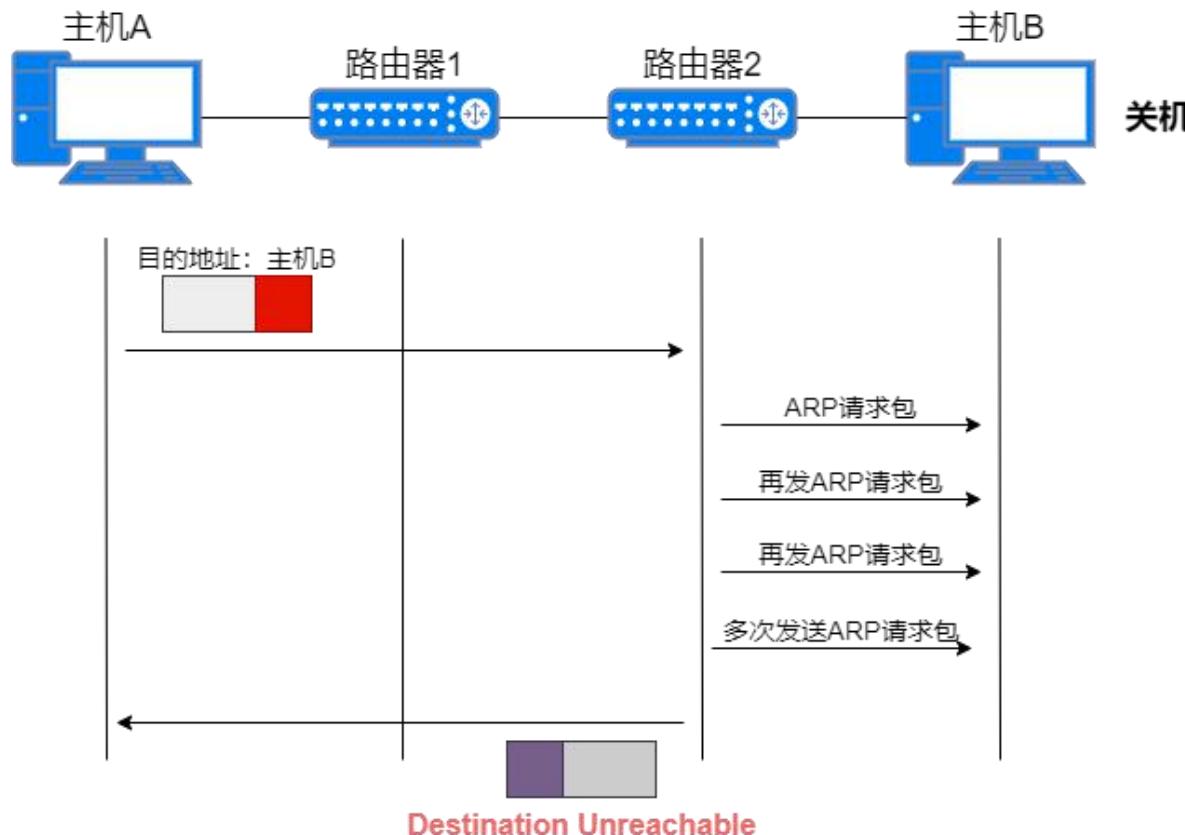
- ❑ 对于携带ICMP差错报文的数据报，不再生产ICMP差错报文。
- ❑ 对分段的数据报文，只对第一个分段产生ICMP差错报文。
- ❑ 对于多播地址的数据报文，不产生ICMP差错报文。
- ❑ 具有特殊地址的数据报文，如127.0.0.0或者0.0.0.0，不产生ICMP差错报文。

图 21.10 差错报文的数据字段的内容



# 目的端不可达 (Destination Unreachable)

- 当路由器不能找到路由或者主机不能传递数据时候，丢弃这个数据报，然后发回目的端不可达报文。
- 目的端不可达报文或者由路由器产生，或者由目的主机创建。

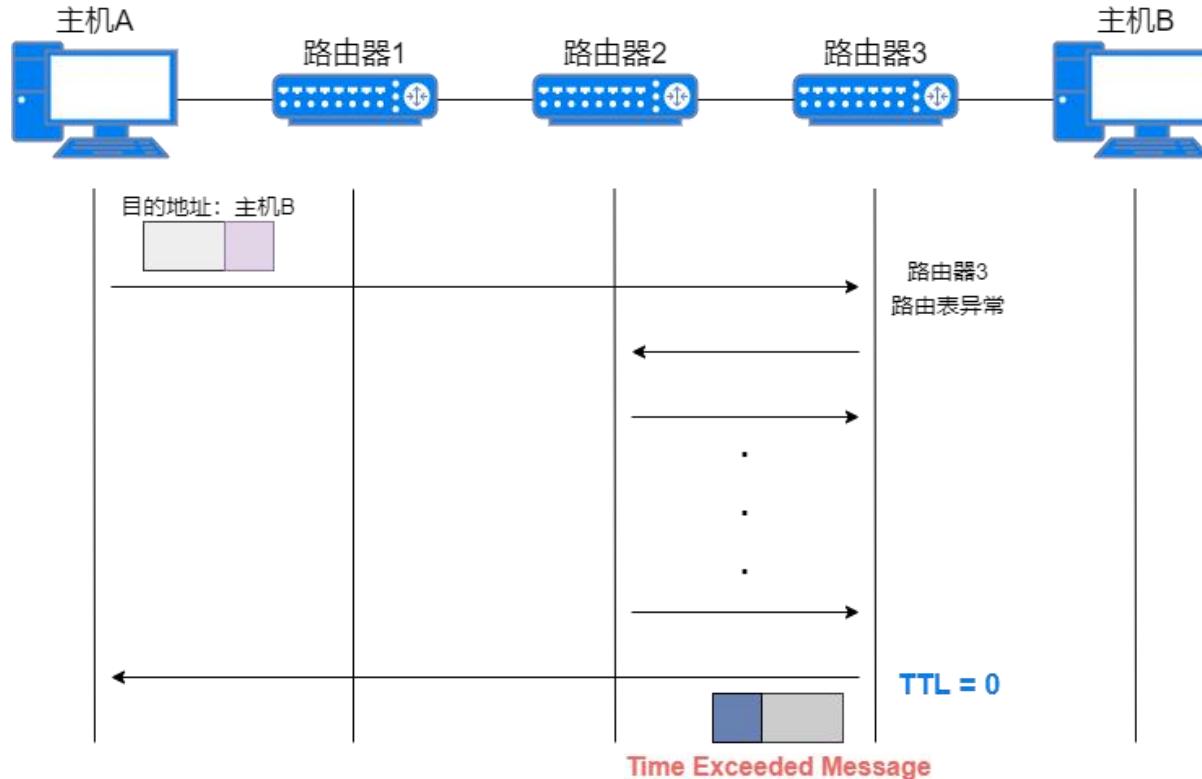


# 源端抑制（source quench）

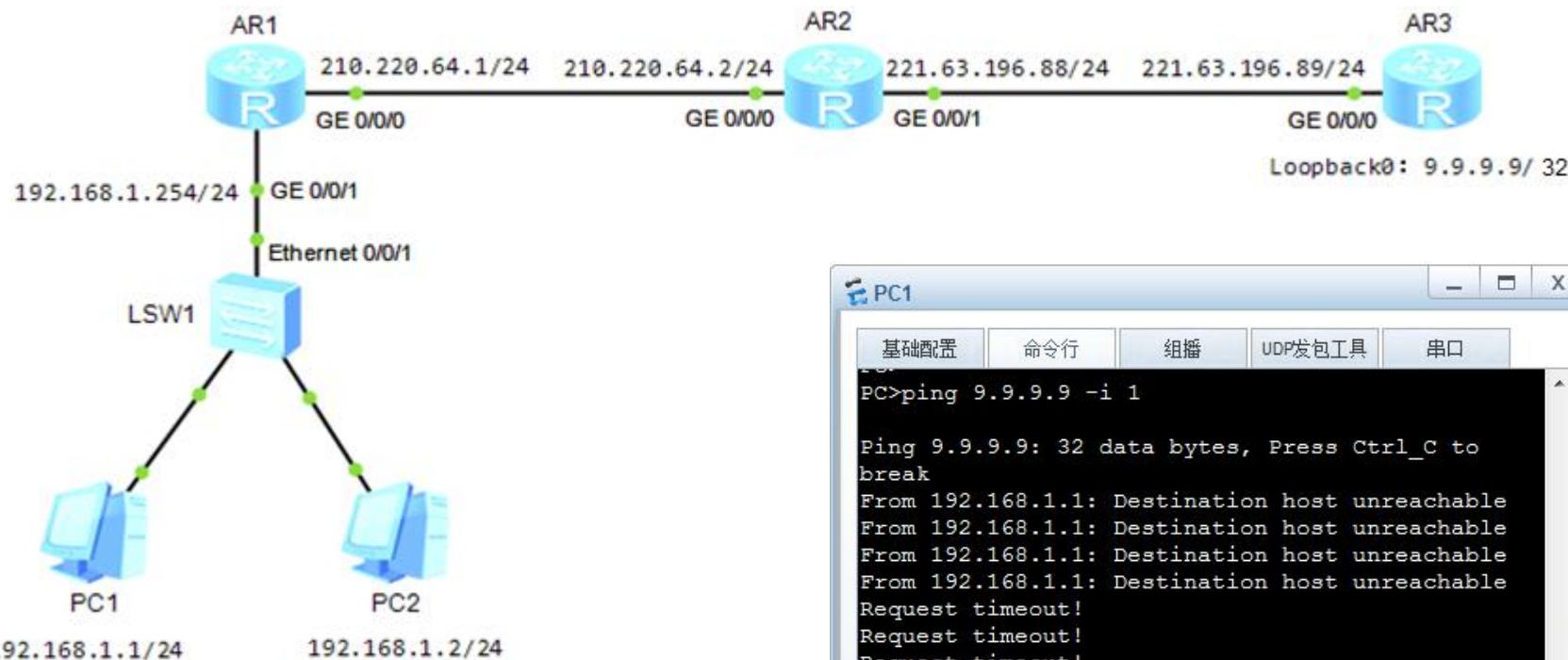
- 用来补充流量控制；
- 当路由器或者目的主机中产生拥塞时，路由器或者目的主机丢弃数据报，发送源端抑制报文给发送方。

# 时间超时（Time Exceeded）

- TTL减为0时，路由器丢弃数据报，并发送一个 Time Exceeded 消息给源设备，通知IP包已被丢弃。
- 报文的所有分片没有在有限的时间内到达（超时），由目的主机发送。



# 观察时间超时的ICMP协议

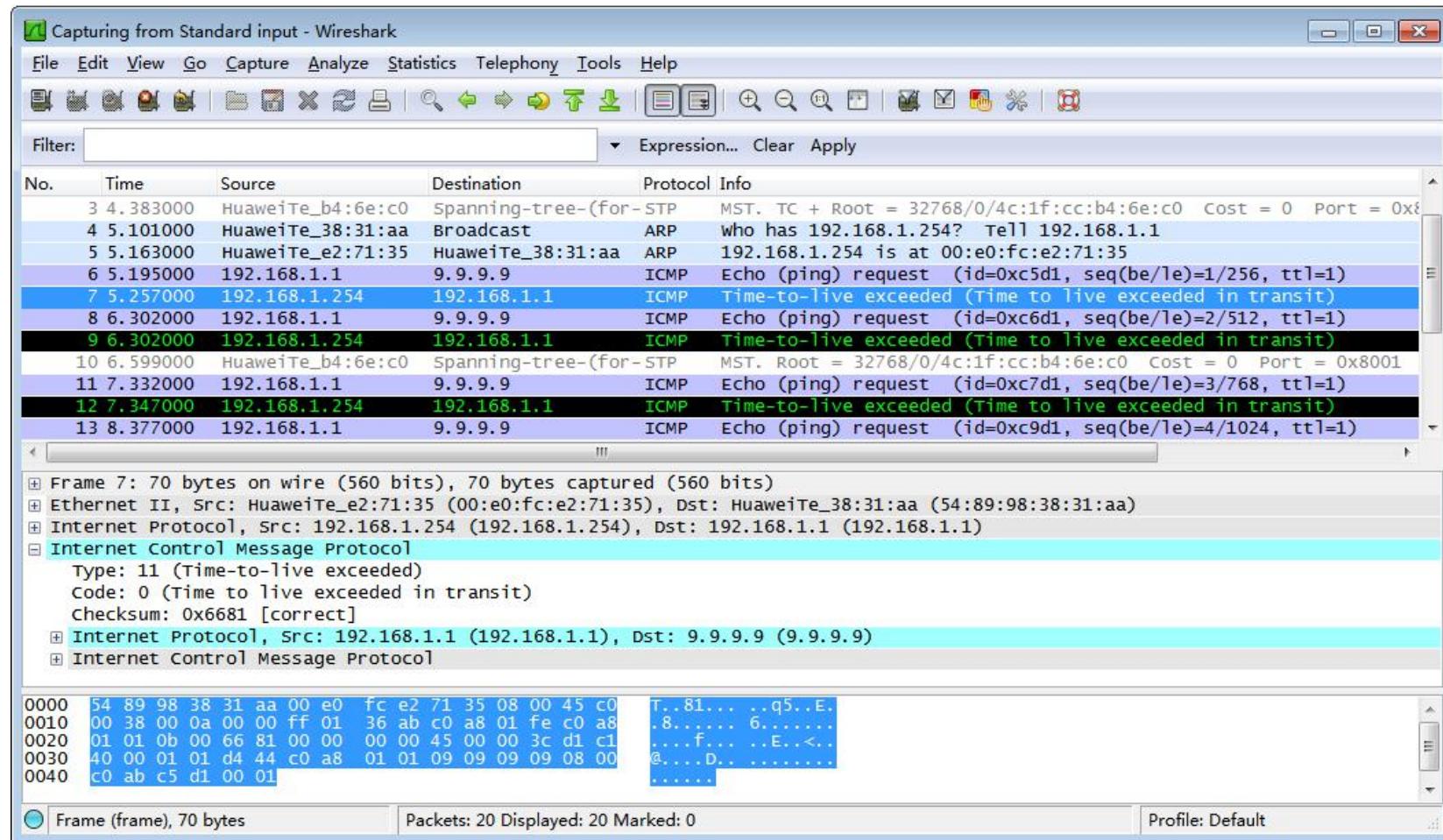


```
PC>ping 9.9.9.9 -i  
Ping 9.9.9.9: 32 data bytes, Press Ctrl_C to break  
From 192.168.1.1: Destination host unreachable  
Request timeout!  
Request timeout!  
Request timeout!  
Request timeout!  
Request timeout!  
Request timeout!  
--- 9.9.9.9 ping statistics ---  
5 packet(s) transmitted  
0 packet(s) received  
100.00% packet loss
```

在PC1上ping路由器AR3的环回接口9.9.9.9，使用参数-i指定不同的TTL值，观察ICMP报文的产生情况。

# 使用Wireshark观察时间超时的ICMP报文

在PC1上ping路由器AR3的环回接口9.9.9.9，使用参数-i指定TTL值为1，在AR1的GE0/0/1接口抓包，可以看到AR1的GE0/0/1接口（192.168.1.254）产生ICMP报文。



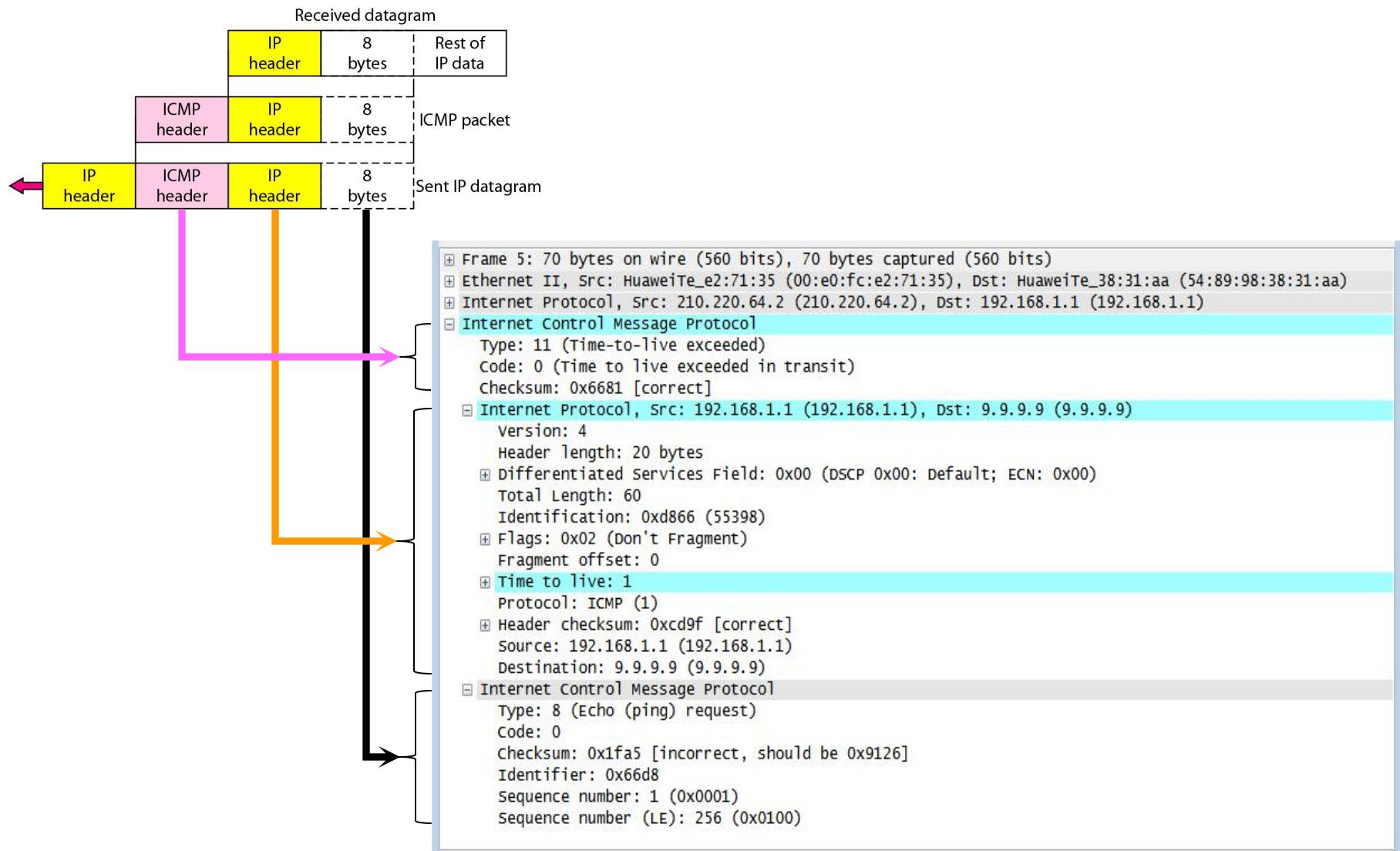
# 使用Wireshark观察时间超时的ICMP报文

在PC1上ping路由器AR3的环回接口9.9.9.9，使用参数-i指定TTL值为2，在AR2的GE0/0/0接口抓包，可以看到AR2的GE0/0/0接口（210.220.64.2）产生ICMP报文。

The screenshot shows the Wireshark interface with the following details:

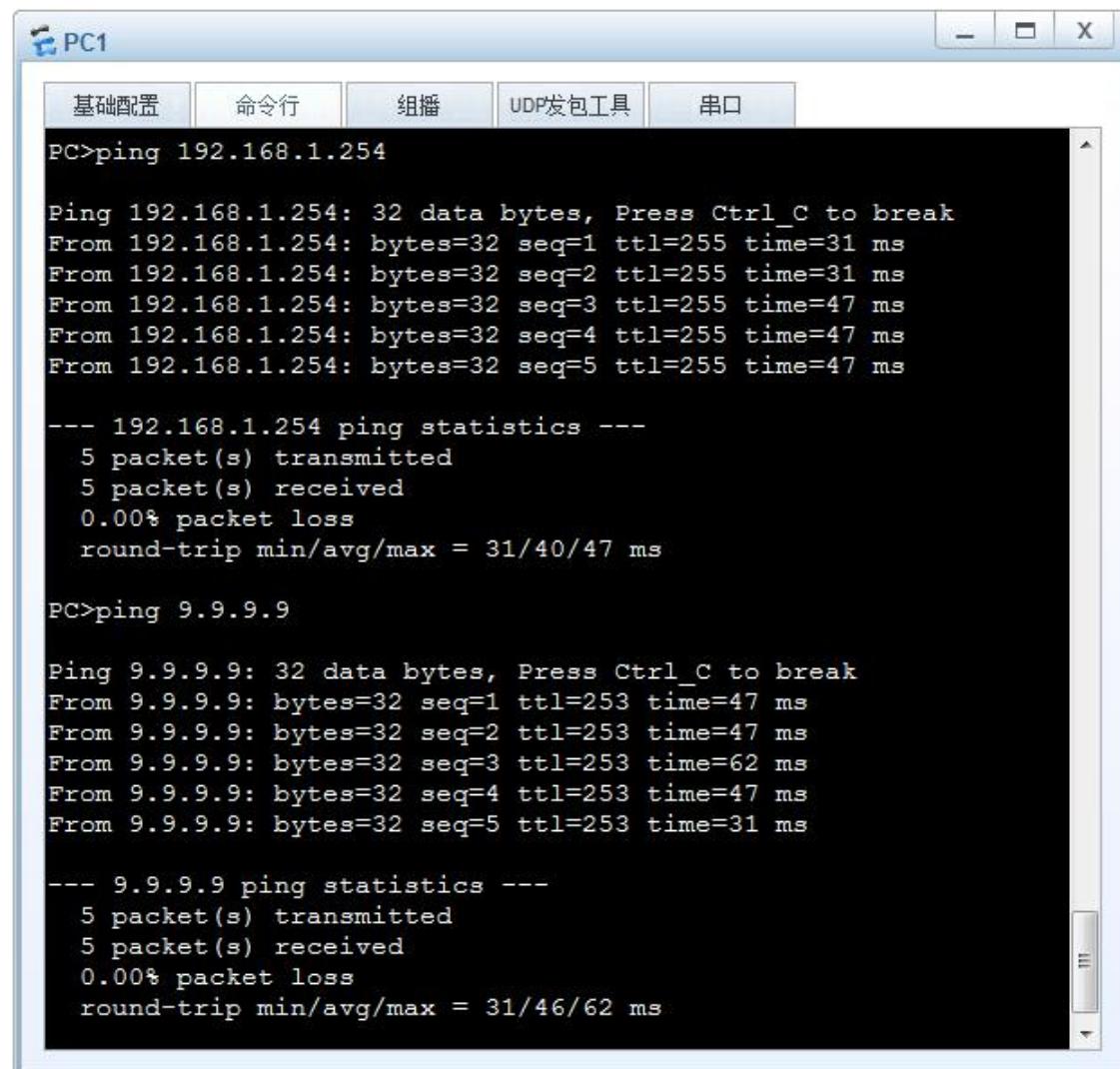
- File menu:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Help.
- Toolbar:** Standard icons for opening files, saving, zooming, and filtering.
- Filter bar:** Shows "Filter: Expression... Clear Apply".
- Table:** The main packet list table with columns: No., Time, Source, Destination, Protocol, Info. The table lists 14 packets, with rows 8 through 14 highlighted in blue, indicating they are ICMP Time-to-Live exceeded frames.
- Packet details pane:** Shows the details for the selected packet (Frame 9).
  - Frame 9: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
  - Ethernet II, Src: HuaweiTe\_e2:71:35 (00:e0:fc:e2:71:35), Dst: HuaweiTe\_38:31:aa (54:89:98:38:31:aa)
  - Internet Protocol, Src: 210.220.64.2 (210.220.64.2), Dst: 192.168.1.1 (192.168.1.1)
  - Internet Control Message Protocol
    - Type: 11 (Time-to-live exceeded)
    - Code: 0 (Time to live exceeded in transit)
    - Checksum: 0x6681 [correct]
  - Internet Protocol, Src: 192.168.1.1 (192.168.1.1), Dst: 9.9.9.9 (9.9.9.9)
  - Internet Control Message Protocol
- Hex dump pane:** Shows the raw hex and ASCII data for the selected frame.
- Status bar:** Frame (frame), 70 bytes | Packets: 68 Displayed: 68 Marked: 0 | Profile: Default

# 差错报告报文各字段的内容



# 观察TTL的变化

在PC1上ping自己的网关，可以看到TTL=255，当PC1 ping路由器AR3时，可以看出TTL=253，这是因为经过了两个路由器。



The screenshot shows a Windows command prompt window titled "PC1". The window has tabs at the top: 基础配置 (selected), 命令行, 组播, UDP发包工具, and 串口. The main area displays the output of a ping command.

```
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=31 ms
From 192.168.1.254: bytes=32 seq=2 ttl=255 time=31 ms
From 192.168.1.254: bytes=32 seq=3 ttl=255 time=47 ms
From 192.168.1.254: bytes=32 seq=4 ttl=255 time=47 ms
From 192.168.1.254: bytes=32 seq=5 ttl=255 time=47 ms

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

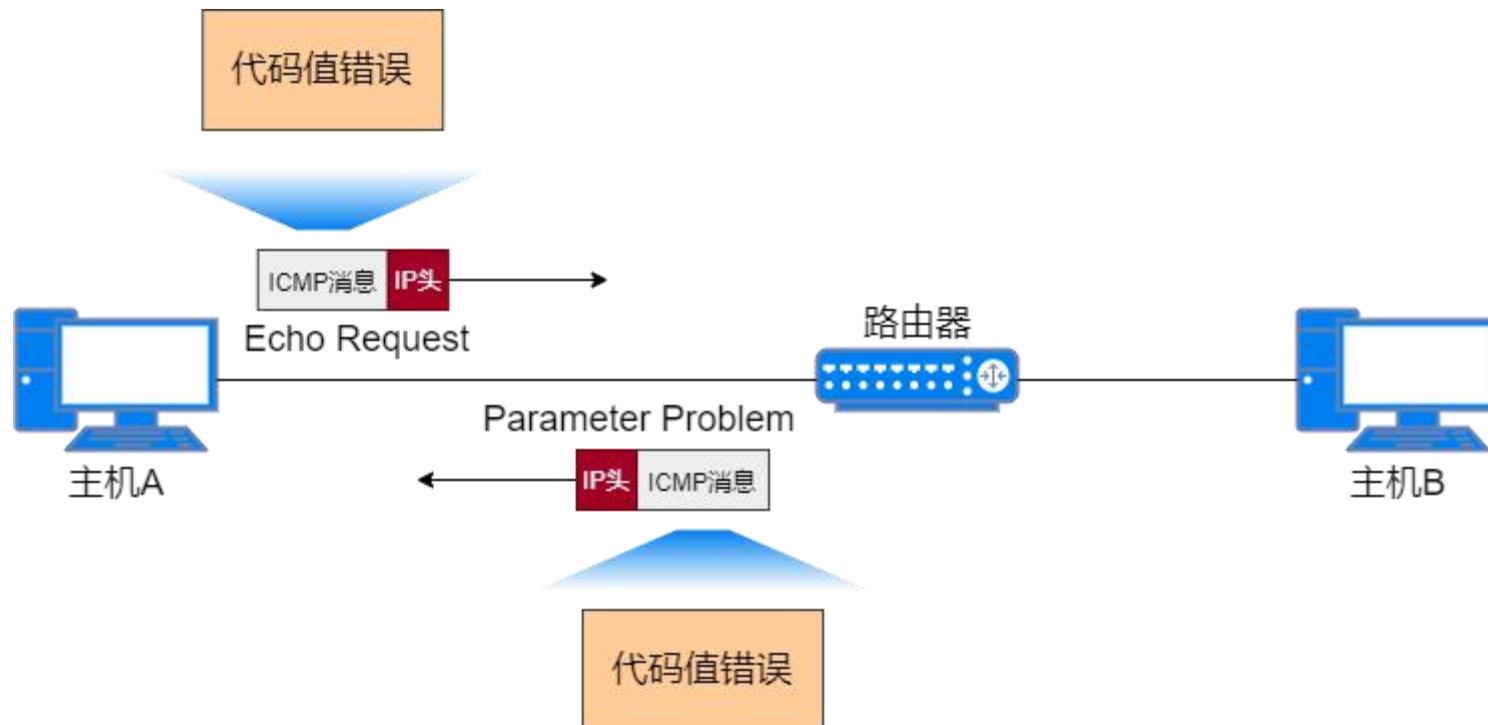
PC>ping 9.9.9.9

Ping 9.9.9.9: 32 data bytes, Press Ctrl_C to break
From 9.9.9.9: bytes=32 seq=1 ttl=253 time=47 ms
From 9.9.9.9: bytes=32 seq=2 ttl=253 time=47 ms
From 9.9.9.9: bytes=32 seq=3 ttl=253 time=62 ms
From 9.9.9.9: bytes=32 seq=4 ttl=253 time=47 ms
From 9.9.9.9: bytes=32 seq=5 ttl=253 time=31 ms

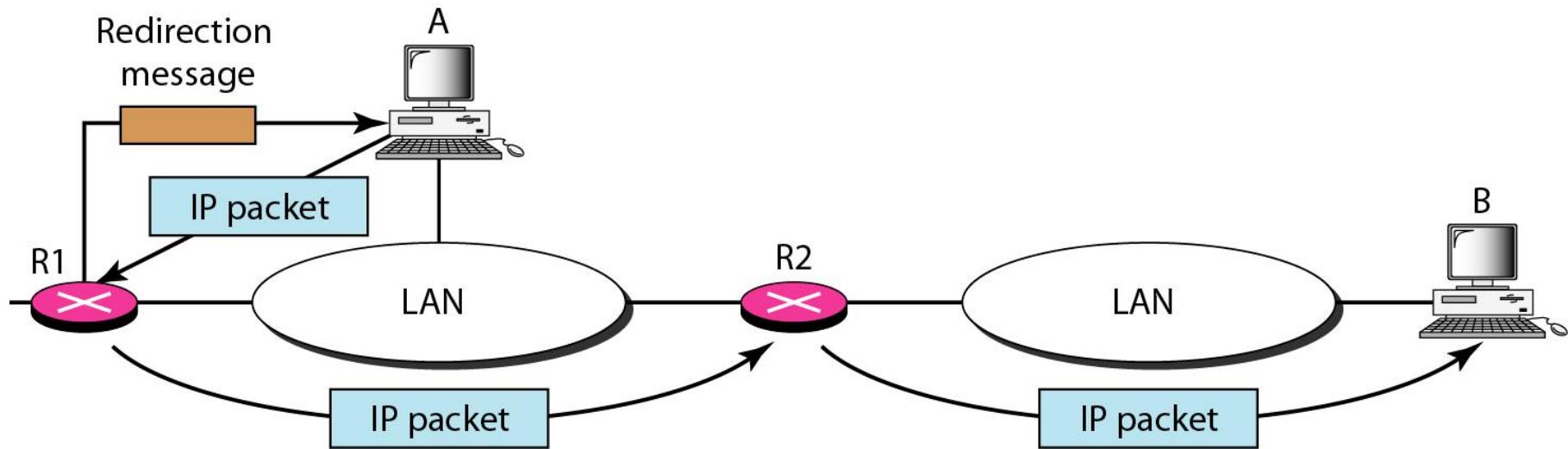
--- 9.9.9.9 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 31/46/62 ms
```

# 参数问题 (Parameter problems)

- IP分组的头部中产生错误或者二义性；
- 路由器或者主机丢弃这个分组，然后向源方发送 参数问题报文。

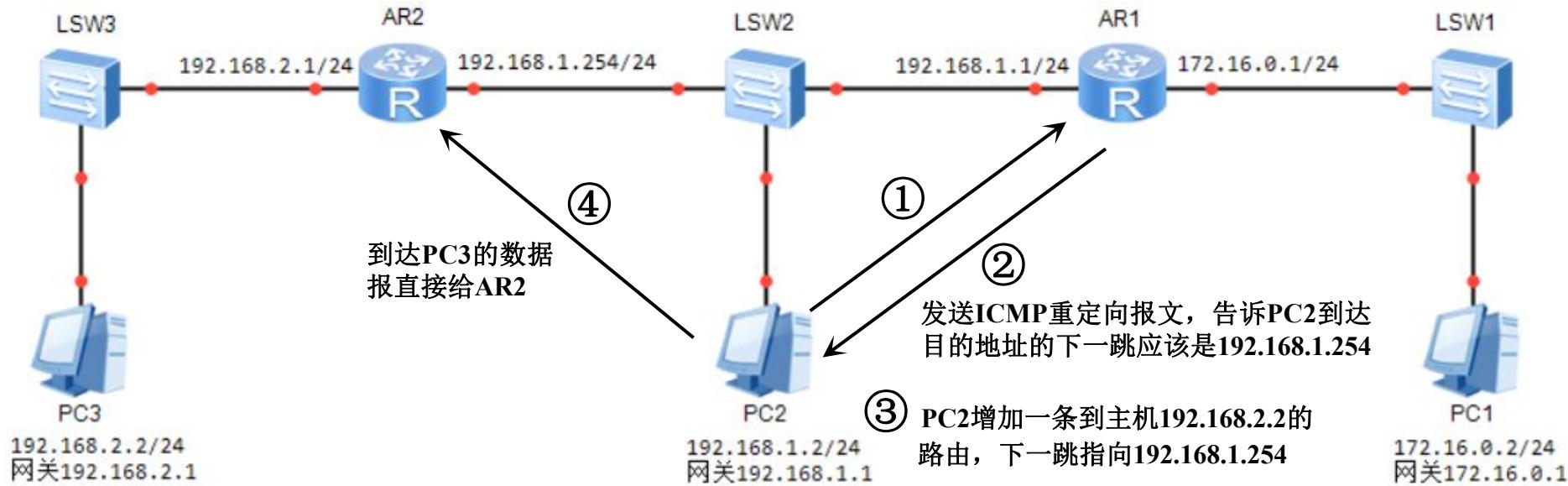


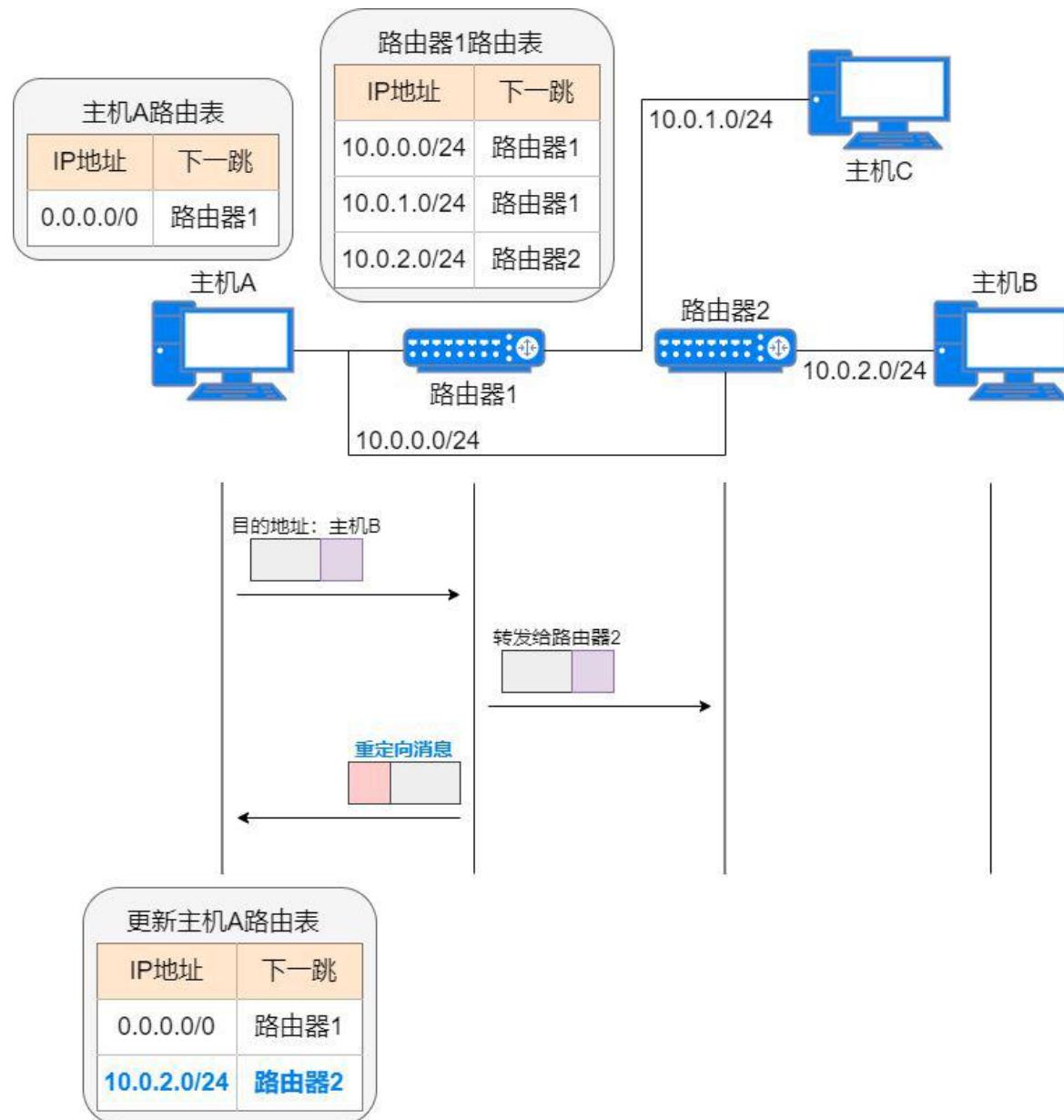
## 图 21.11 重定向 (Redirection)



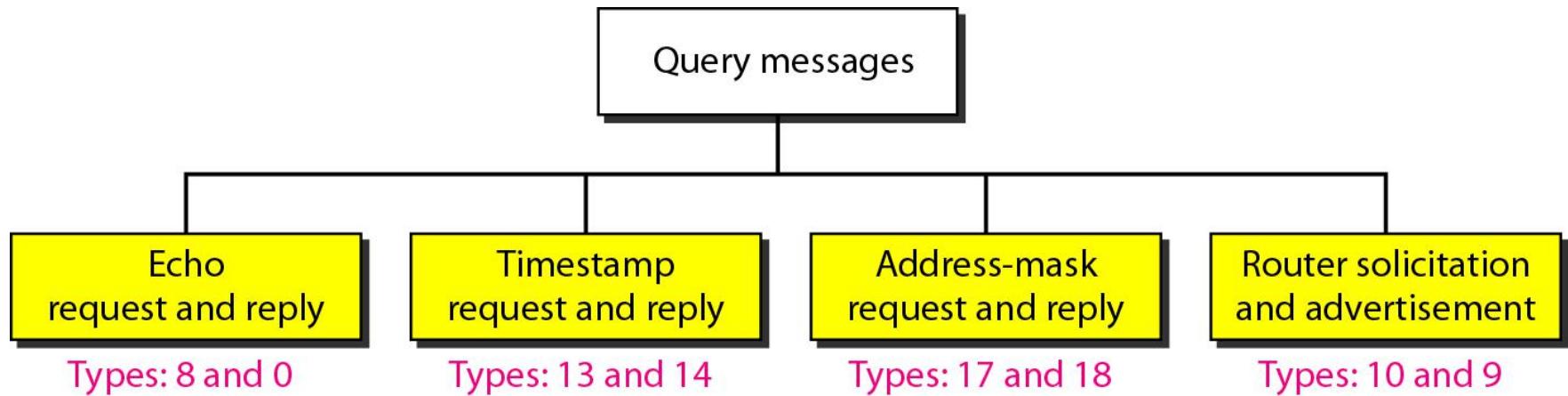
- 如果路由器发现一条更优的路径发送数据，那么它就会返回一个 Redirection 消息给主机，这个消息包含了最合适路由信息和源数据。
- A想向B发送数据报，R2是有效的路由，但A却选择了R1，R1收到后发现应该发往R2，于是把分组发给R2，同时向A发送重定向报文。

# 重定向





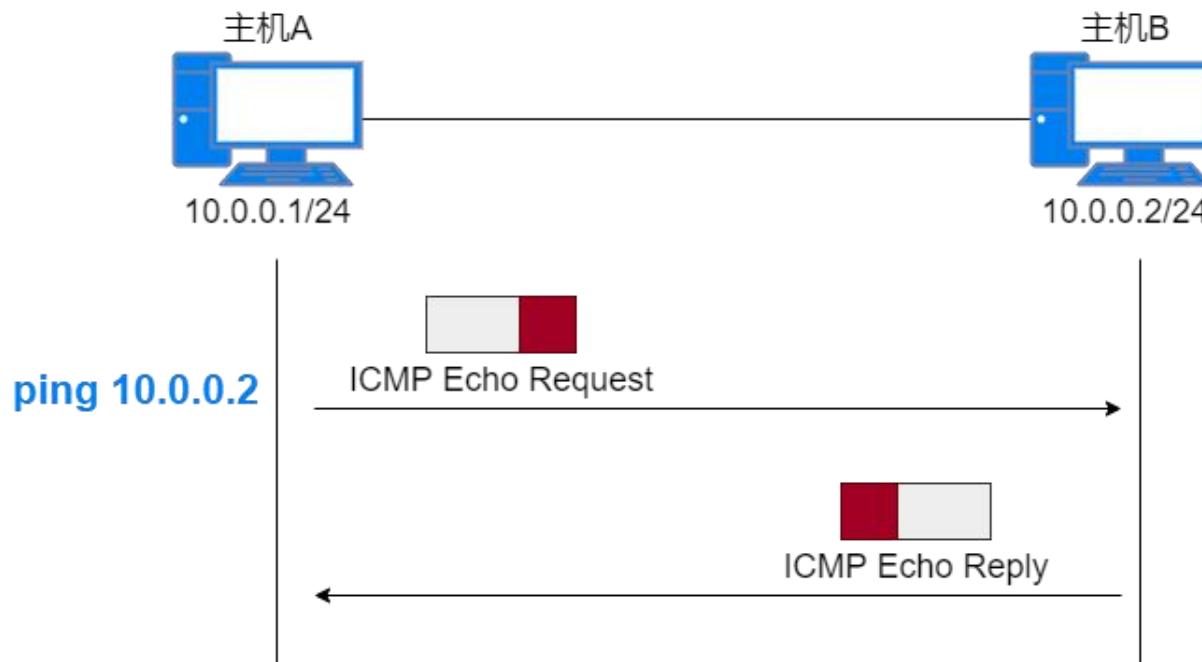
## 图 21.12 查询报文



- 回送请求和回答：诊断网络
- 时间戳请求和回答：确定数据报的往返时间，同步
- 地址掩码请求和回答：获取地址对应的掩码
- 路由器询问和通告：询问路由器是否可正常工作

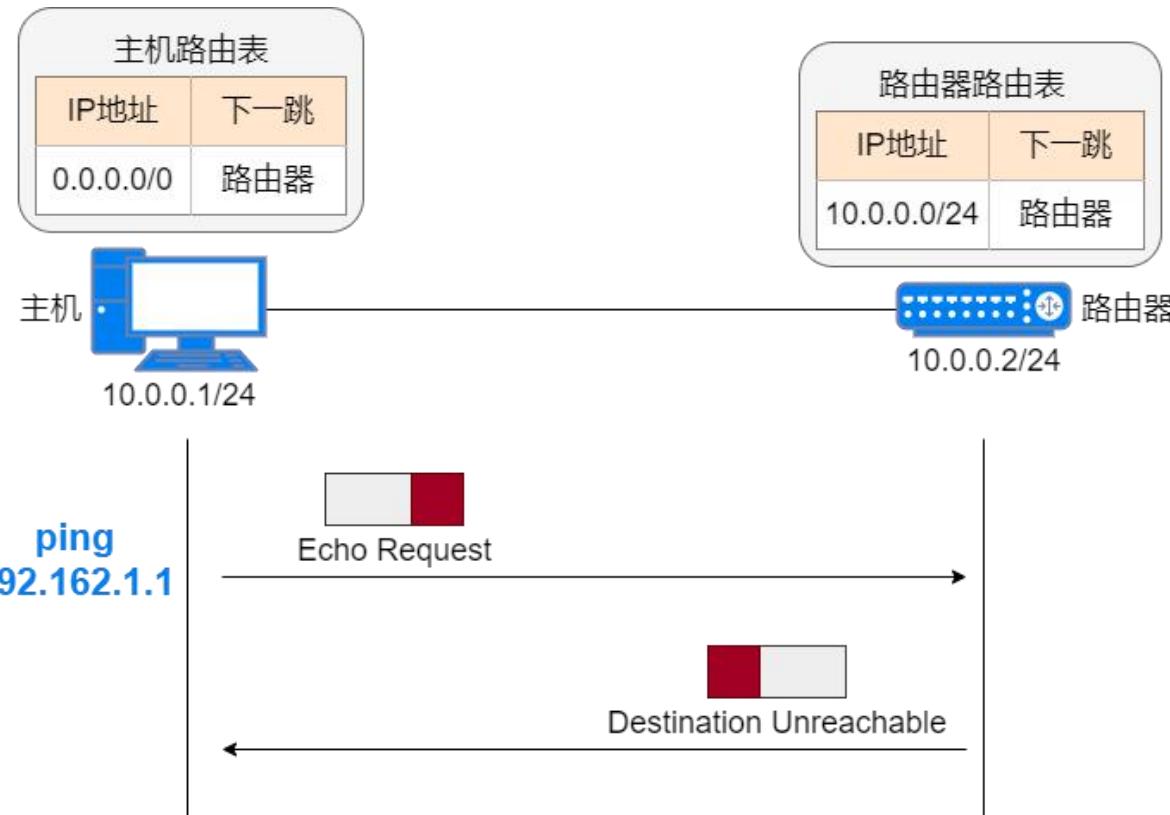
# Ping命令

ping 是 ICMP 最著名的一个应用，通过 ping 可以测试网络的可达性，即网络上的报文能否成功到达目的地。源设备向目的设备发送 Echo request 消息，目的地址是目的设备的 IP 地址。目的设备收到 Echo request 消息后，向源设备回应一个 Echo reply 消息，可知目的设备是可达的。也可以通过 ping 命令来判断目标主机是否启用。



# Ping不通的情况

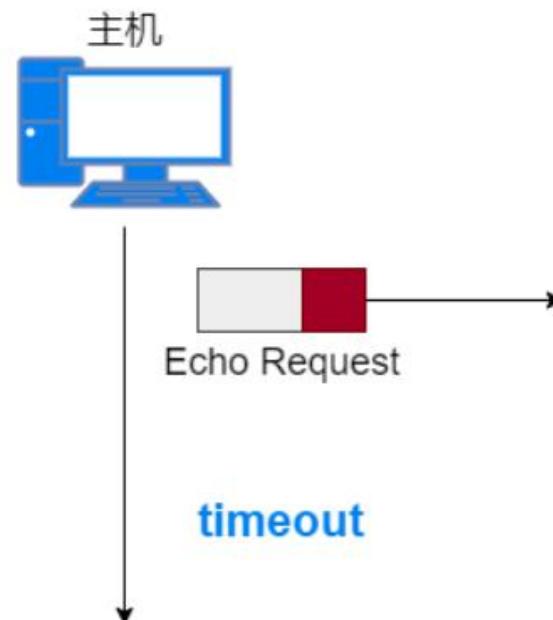
如果中间某个路由器没有到达目的网络的路由，便会向源设备回应一个 Destination Unreachable 消息，告知目的设备不可达。



# Ping不通的情况

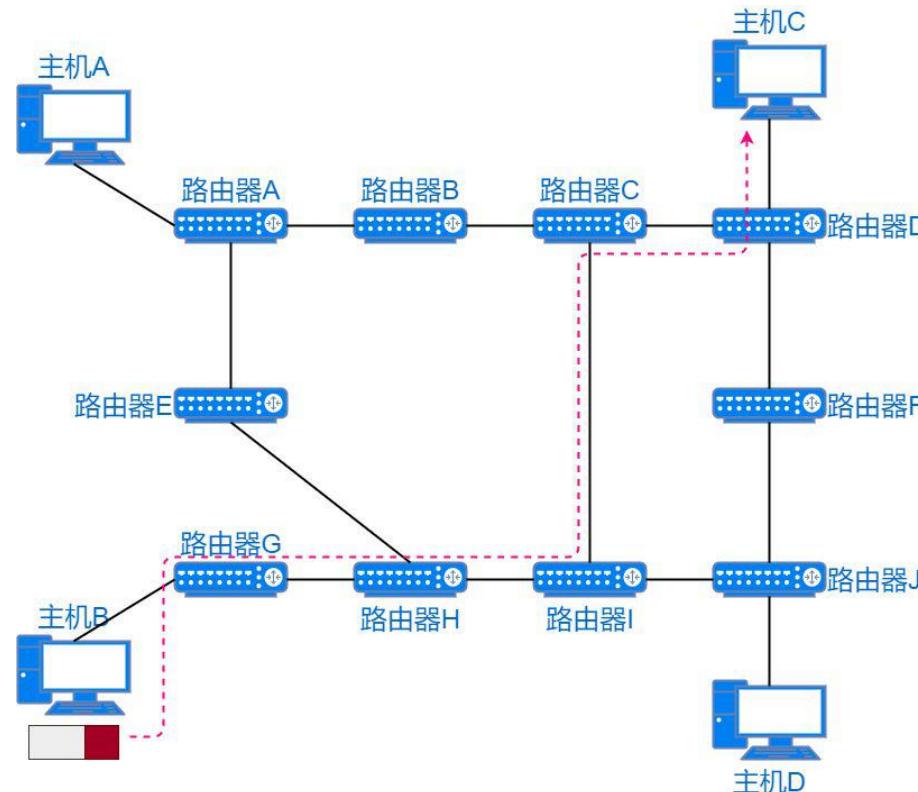
如果源主机在一定时间内无法收到回应报文，就认为目的设备不可达，并显示超时。

**注意：**ping 过程是双向的消息通信，只有双向都成功传输时，才能说明通信是正常的。另外主机也可能因为防火墙拦截，导致 ping 不通。



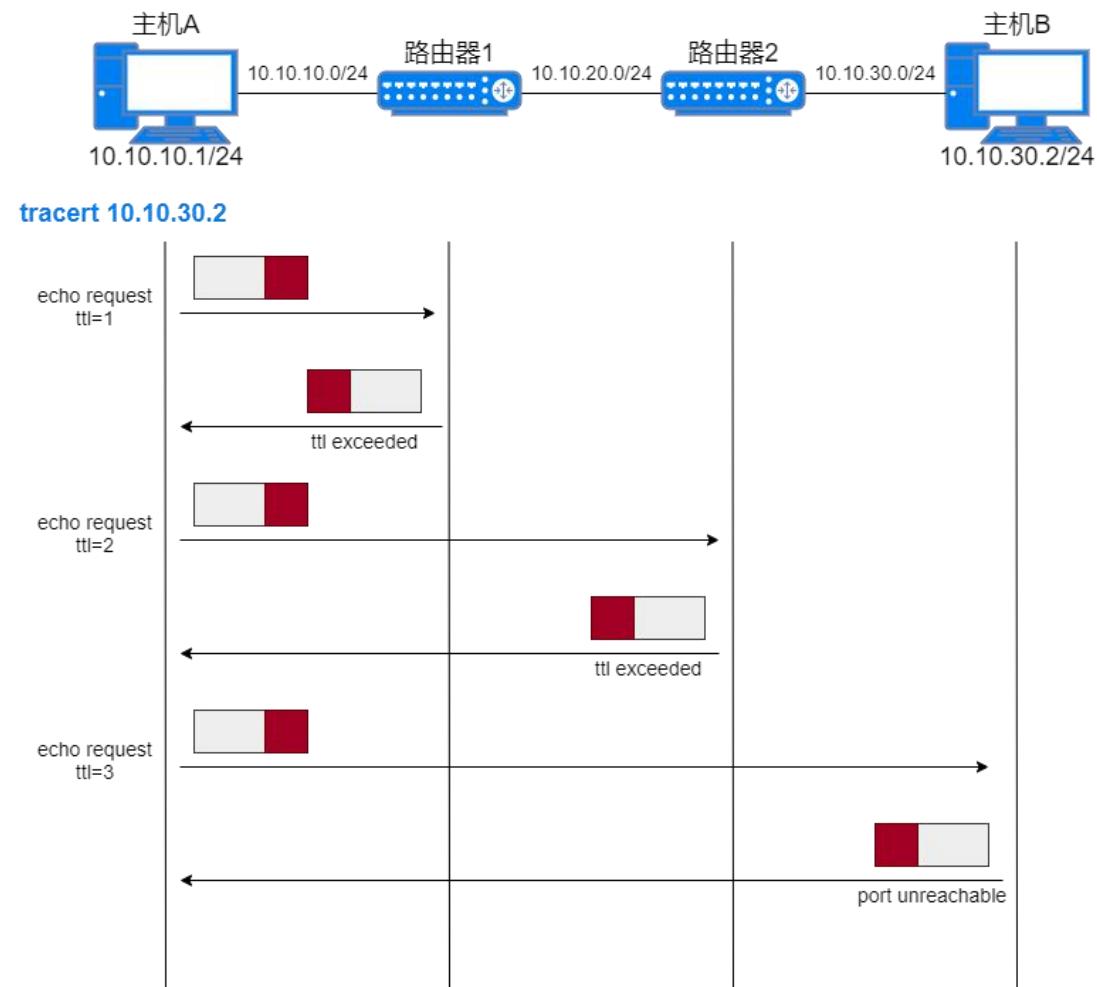
# Tracert命令

- ◆ ping 工具只能测试目的设备的连通性，但是看不到数据包的传输路径。在网络不通的情况下，无法知道网络问题发生在哪个位置。tracert 工具可以查看数据包的整条传输路径，包括途中经过的中间设备。
- ◆ 在 Windows 中命令是 tracert，在 Unix 、 MacOS 中命令是 traceroute。



# Tracert命令

- ◆ Tracert 是基于TTL字段和 ICMP 协议实现的。
- ◆ 源设备发送第一个数据报时 TTL 值为 1。第一个路由器收到数据报后 TTL 值减 1，丢弃数据报并返回**时间超时**ICMP报文。源设备收到响应报文后，取出源 IP 地址，即路径上的第一个路由器地址。然后发送一个 TTL 值为 2 的数据报。以此类推。
- ◆ 当主机B收到数据报后TTL减为0但不丢弃该报文。主机A在发送数据报时将目的端口设置为UDP不支持的端口，当主机B收到该数据报时找不到接收该数据报的应用，丢弃并发送**目的端不可达**ICMP报文。
- ◆ tracert 过程也是双向消息通信，只有双向都成功传输时，才能正确探测路径。主机安装了防火墙也可能造成路径探测失败。



命令提示符

```
C:\Users\GY>tracert www.xidian.edu.cn

通过最多 30 个跃点跟踪
到 www.xidian.edu.cn [202.117.112.74] 的路由:

 1   8 ms    8 ms    9 ms  192.168.1.1
 2   6 ms    11 ms   4 ms  10.206.255.254
 3   *        *       *      请求超时。
 4   3 ms    3 ms    3 ms  172.16.14.6
 5   *        4 ms    4 ms  172.16.14.9
 6   7 ms    11 ms   11 ms 172.16.11.21
 7   6 ms    6 ms    5 ms  172.16.11.6
 8   23 ms   4 ms    25 ms 10.255.62.5
 9   4 ms    3 ms    9 ms  202.117.112.74

跟踪完成。
```

命令提示符

```
C:\Users\GY>tracert www.bu.edu

通过最多 30 个跃点跟踪
到 d6c88qfbxnvam.cloudfront.net [52.222.214.67] 的路由:

 1   18 ms    27 ms    6 ms  192.168.1.1
 2   4 ms     7 ms    7 ms  10.206.255.254
 3   *        *       *      请求超时。
 4   *        *       *      请求超时。
 5   5 ms    11 ms   14 ms 113.200.174.1
 6   8 ms     7 ms    *     123.139.1.37
 7   *        *       10 ms  221.11.0.53
 8   30 ms   27 ms   27 ms  219.158.112.17
 9   67 ms   48 ms   34 ms  219.158.5.150
10   34 ms   36 ms   44 ms  219.158.3.182
11   157 ms   *      *     219.158.98.138
12   171 ms   185 ms  173 ms  219.158.40.26
13   *        *      *     请求超时。
14   *        *      *     请求超时。
15   *        *      *     请求超时。
16   184 ms   184 ms   *     15.230.131.160
17   *        *      *     请求超时。
18   162 ms   161 ms  162 ms  server-52-222-214-67.fra56.r.cloudfront.net [52.222.214.67]

跟踪完成。
```

## 21-3 IGMP

IP协议可用到两种类型的通信：单播和多播。  
因特网组管理协议(**Internet Group Management Protocol, IGMP**) 是其中一个必要的，但不是充分的协议，多播也包含其他的协议。在IP协议中，IGMP是一个辅助协议。

### 本节讨论：

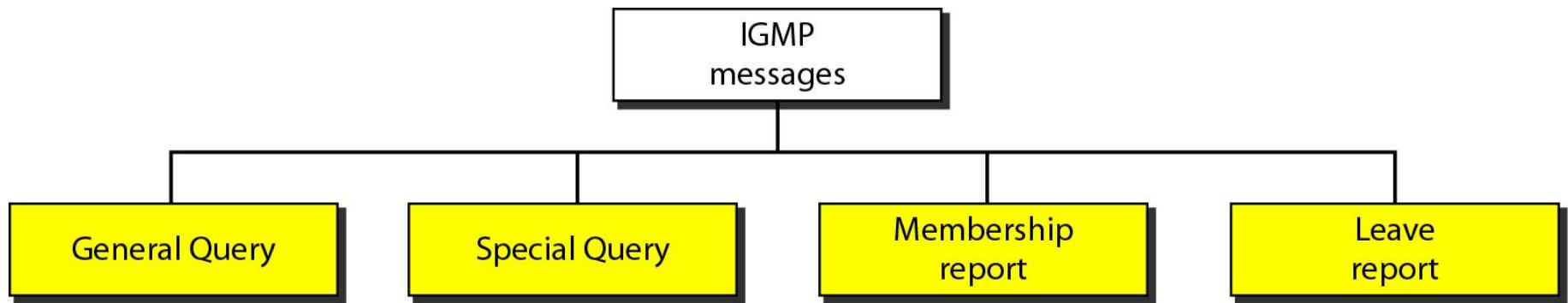
组管理

IGMP 报文and IGMP 操作

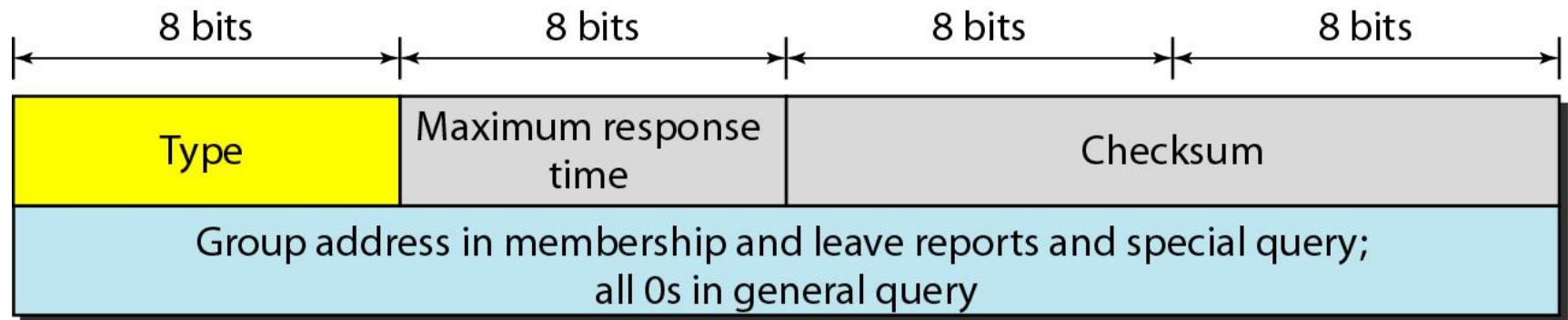
封装

Netstat 应用程序

图 21.16 IGMP报文类型



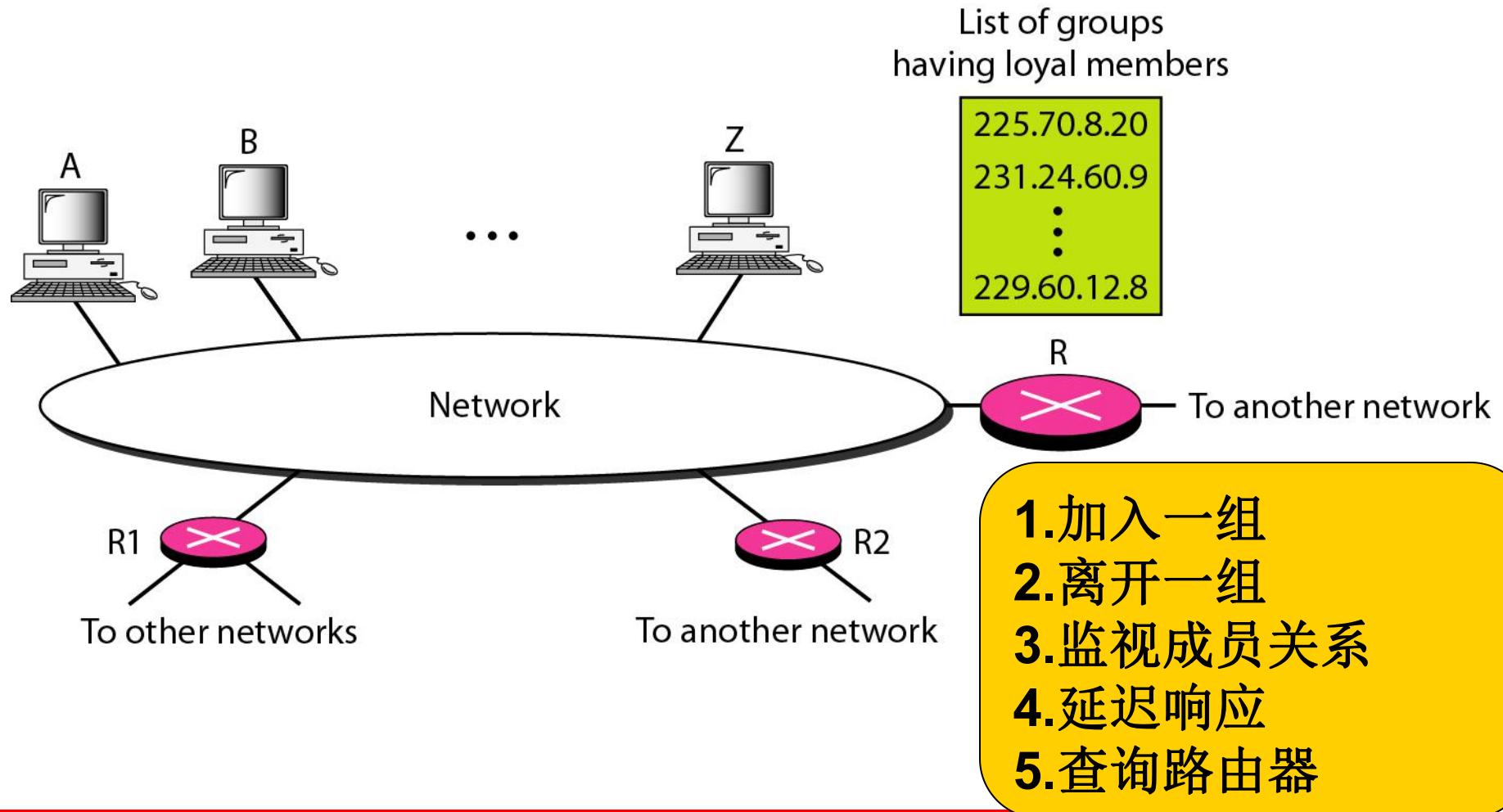
## 图 21.17 IGMP报文格式

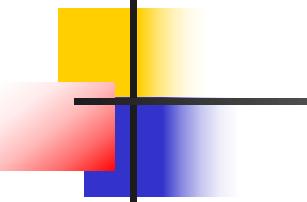


### Table 21.1 IGMP 类型字段

Type	Value
General or special query	0x11 or 00010001
Membership report	0x16 or 00010110
Leave report	0x17 or 00010111

图 21.18 IGMP 操作

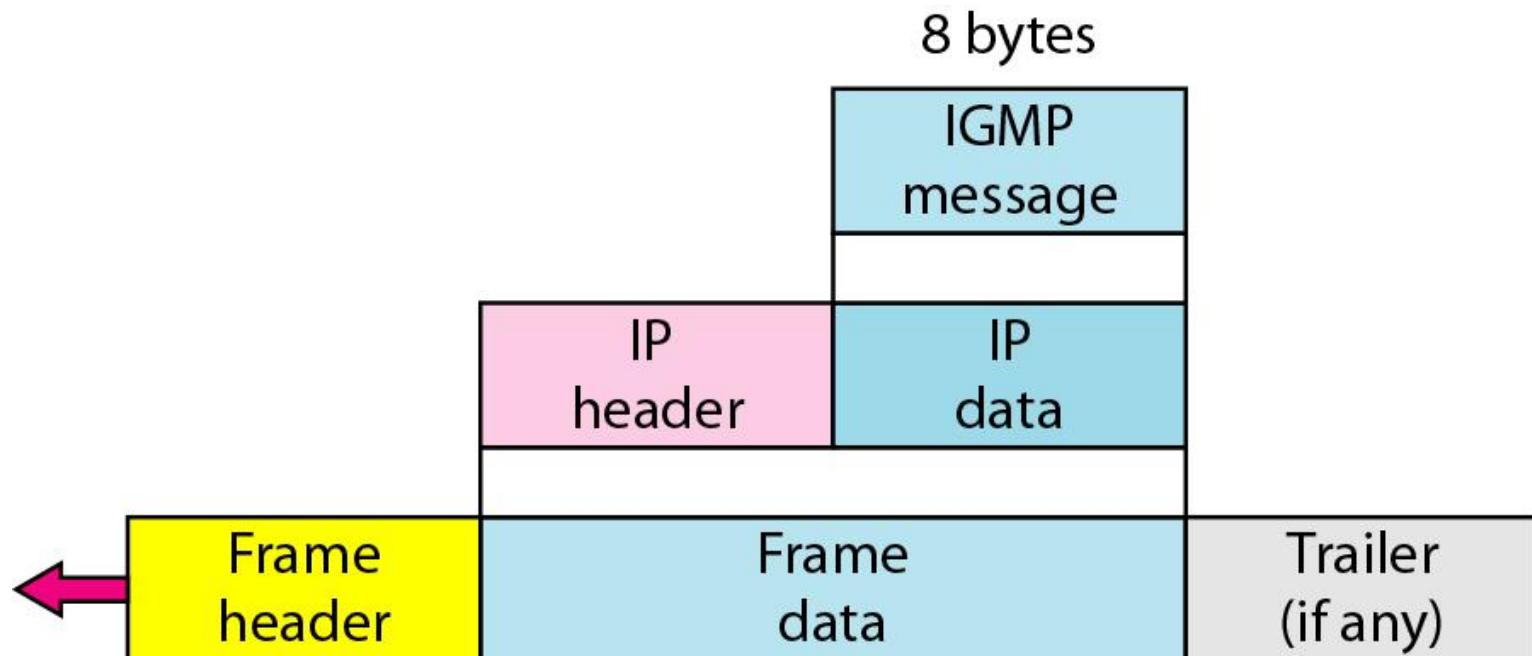


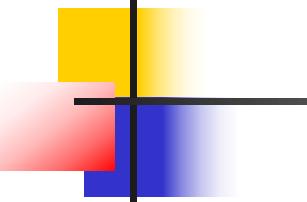


## 注意

- 在 **IGMP**中，成员关系报告一个接着一个地发送两次。
- 普通查询报文没有定义一个特殊的组。

图 21.20 IGMP分组的封装





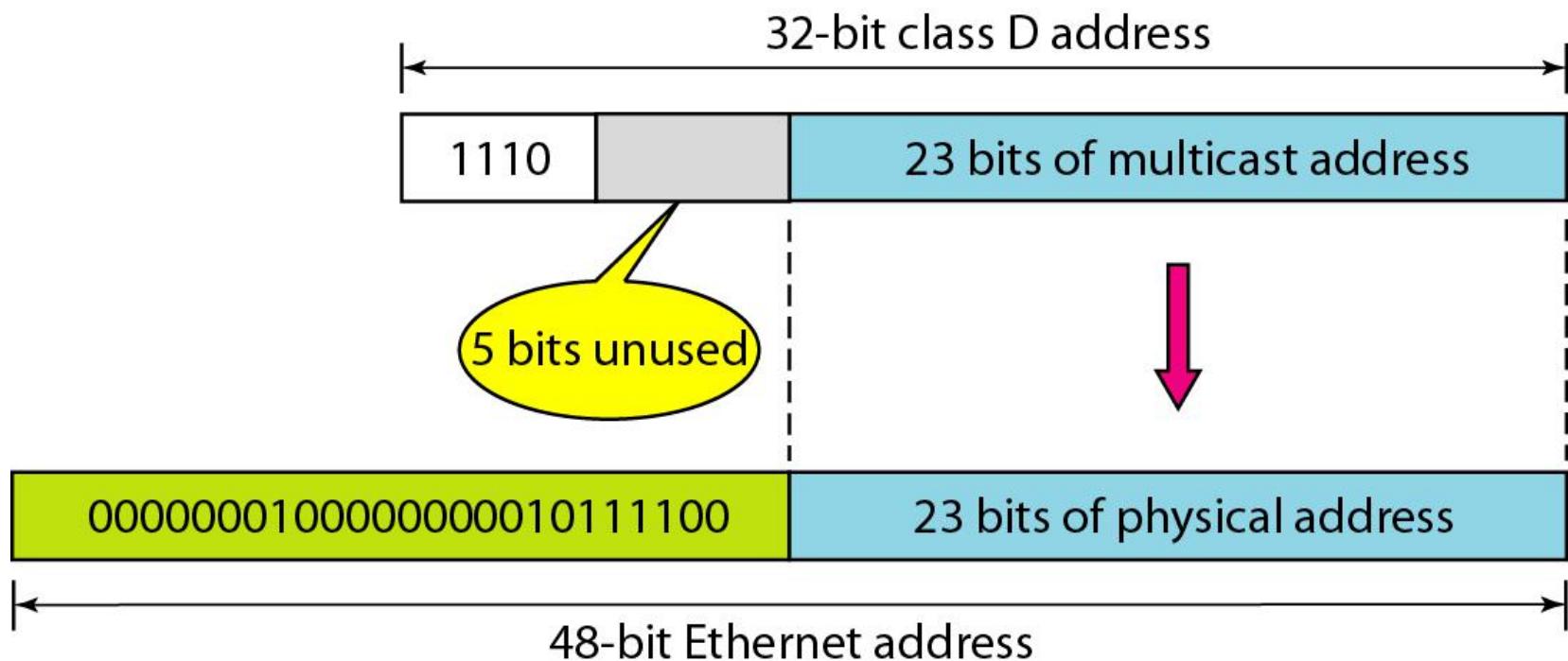
注意

**携带IGMP分组的IP分组的TTL字段值为1。**

## Table 21.2 目的IP地址

<i>Type</i>	<i>IP Destination Address</i>
Query	224.0.0.1 All systems on this subnet
Membership report	The multicast address of the group
Leave report	224.0.0.2 All routers on this subnet

图 21.21 将D类地址映射到以太网物理地址

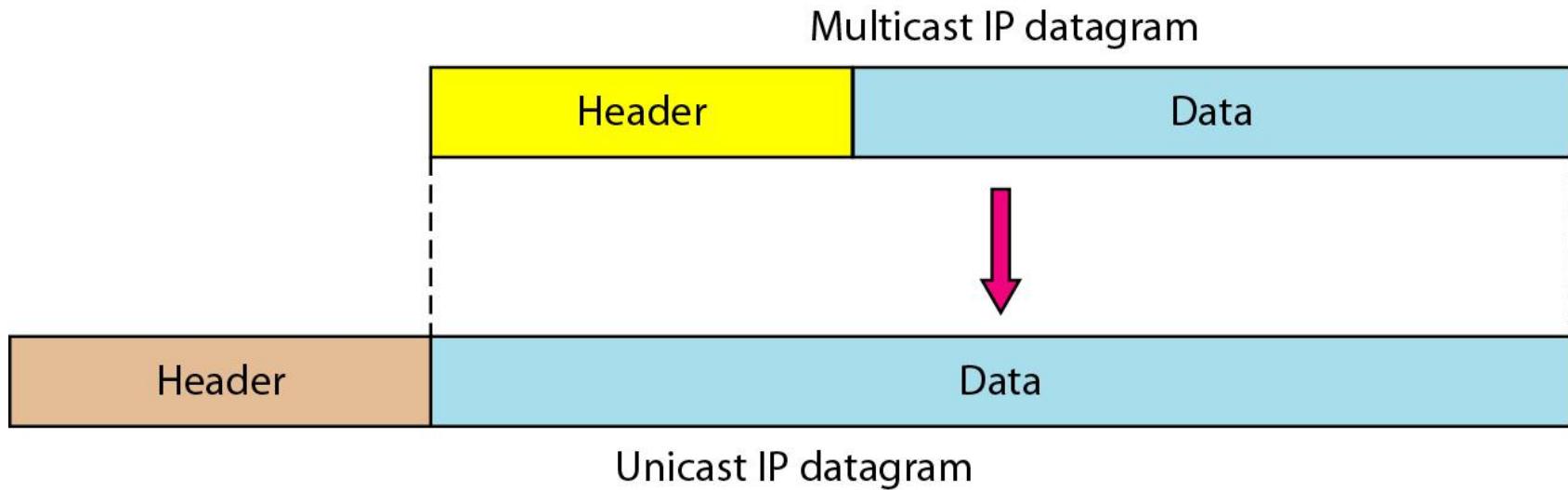


注意

以太网的多播物理地址范围：

**01: 00: 5E: 00: 00: 00 — 01: 00: 5E: 7F: FF: FF**

图 21.22 隧道技术



无物理多播地址支持

## 例 21.9

Netstat是在内核中访问网络连接状态及其相关信息的程序，它能提供TCP连接，TCP和UDP监听，进程内存管理的相关报告。Netstat用于显示与IP、TCP、UDP和ICMP协议相关的统计数据，一般用于检验本机各端口的网络连接情况。

- 选项-n是以数字形式显示IP地址；
- 选项-r显示路由表；
- 选项-a显示所有的地址(单播和多播地址)；
- “Destination”定义目的地址；
- “Gateway”定义路由器；
- “Iface”定义接口；
- “Mask” 定义掩码；
- “Flag” 定义标记。标记U表示该路由可使用，标志G表示该路由是一个网关(路由器)。

## 例 21.9 (续)

```
$ netstat -nra
```

Kernel IP routing table

Destination	Gateway	Mask	Flags	Iface
153.18.16.0	0.0.0.0	255.255.240.0	U	eth0
169.254.0.0	0.0.0.0	255.255.0.0	U	eth0
127.0.0.0	0.0.0.0	255.0.0.0	U	lo
224.0.0.0	0.0.0.0	224.0.0.0	U	eth0
0.0.0.0	153.18.31.254	0.0.0.0	UG	eth0

其中多播地址用彩色表示。具有从240.0.0.0到239.255.255.255多播地址的任何分组都被屏蔽，并传递给以太网接口。

## 21-4 ICMPv6

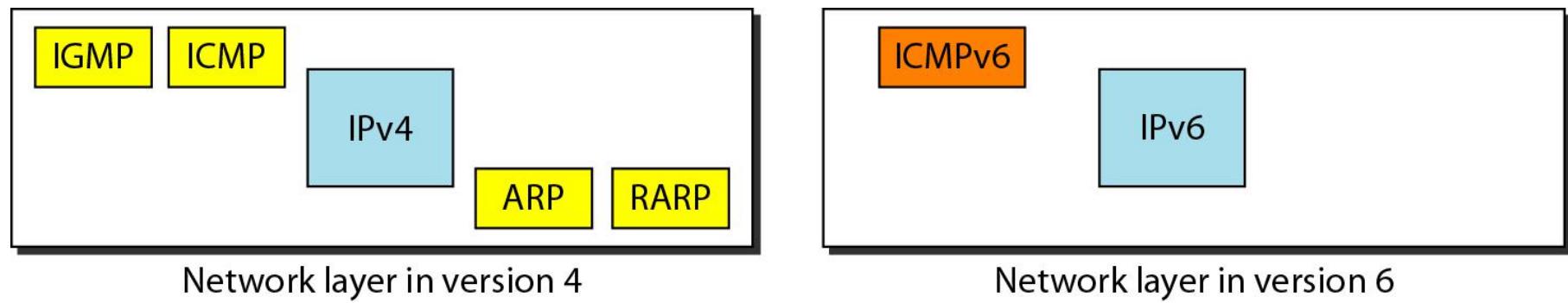
在第20章中讨论过IPv6。在TCP/IP协议族的版本6中被修改的另一个协议是ICMP(ICMPv6)。这个新版本与版本4的策略和目的一样。

讨论:

差错报告

查询

图 21.23 版本4和版本6的网络层比较



## Table 21.3 ICMPv4和ICMPv6的差错报告的比较

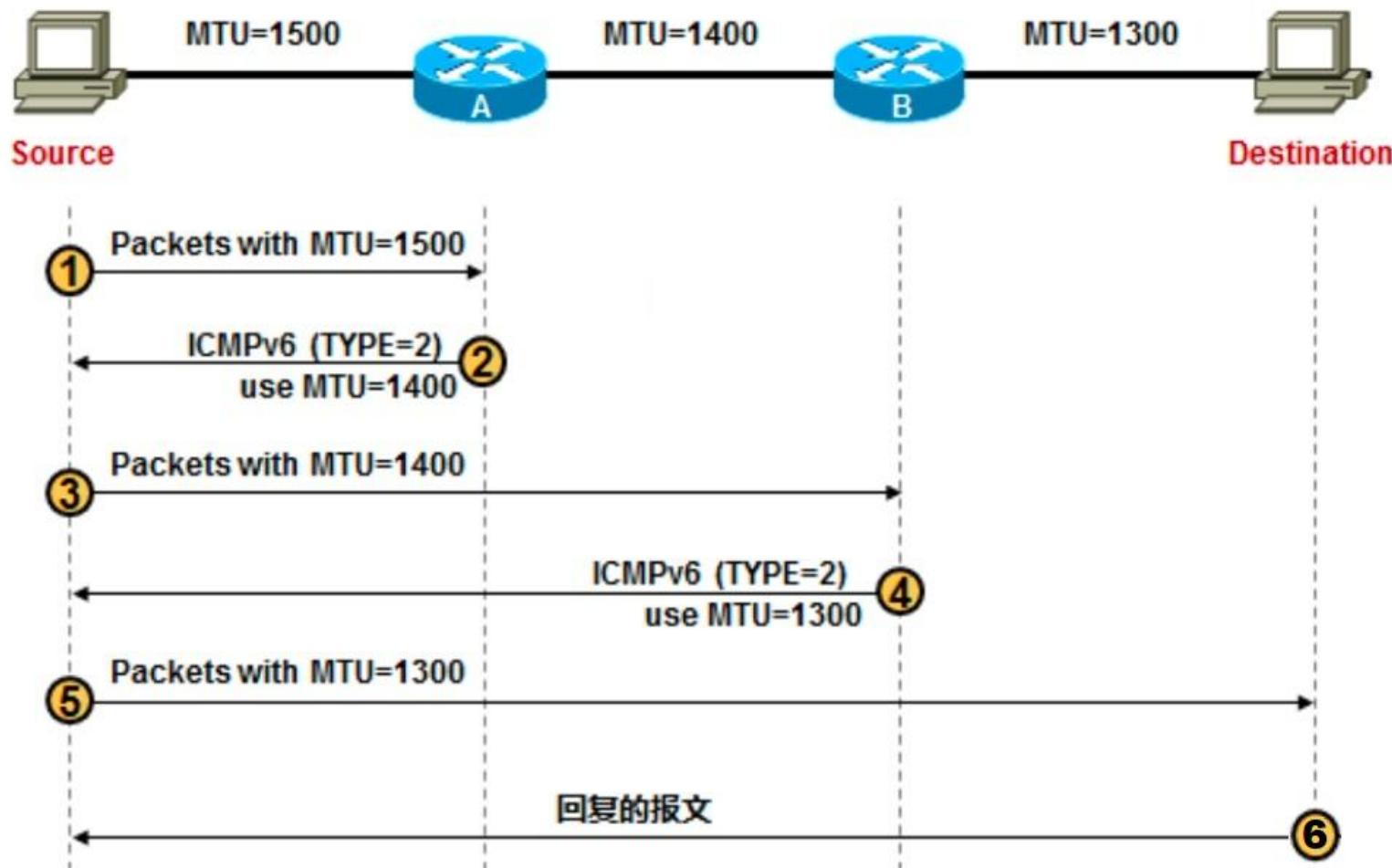
<i>Type of Message</i>	<i>Version 4</i>	<i>Version 6</i>
Destination unreachable	Yes	Yes
Source quench	Yes	No
Packet too big	No	Yes
Time exceeded	Yes	Yes
Parameter problem	Yes	Yes
Redirection	Yes	Yes

# ICMPv6分组太大差错报告

---

- ◆ 在IPv4中，如果分组不适合外发链路的MTU，则到目的地路径上的任何路由器都能将一个分组进行分段，而IPv6不支持这项功能。
- ◆ 虽然对于主机而言，在需要分段的地方由路由器来实施会非常方便，但这为路由器带来了很大的处理负担，因为路由器必须为分段过程保持状态并使用额外内存。
- ◆ IPv6具有路径MTU探测的功能，当到达目的路径上的路由器发现分组太大时，会发送分组太大差错报告给源主机，指明分组需要分段。主机在收到分组太大的ICMPv6消息后，它减小MTU值并再次发送，直到得到一个合适的MTU值。

# MTU探测



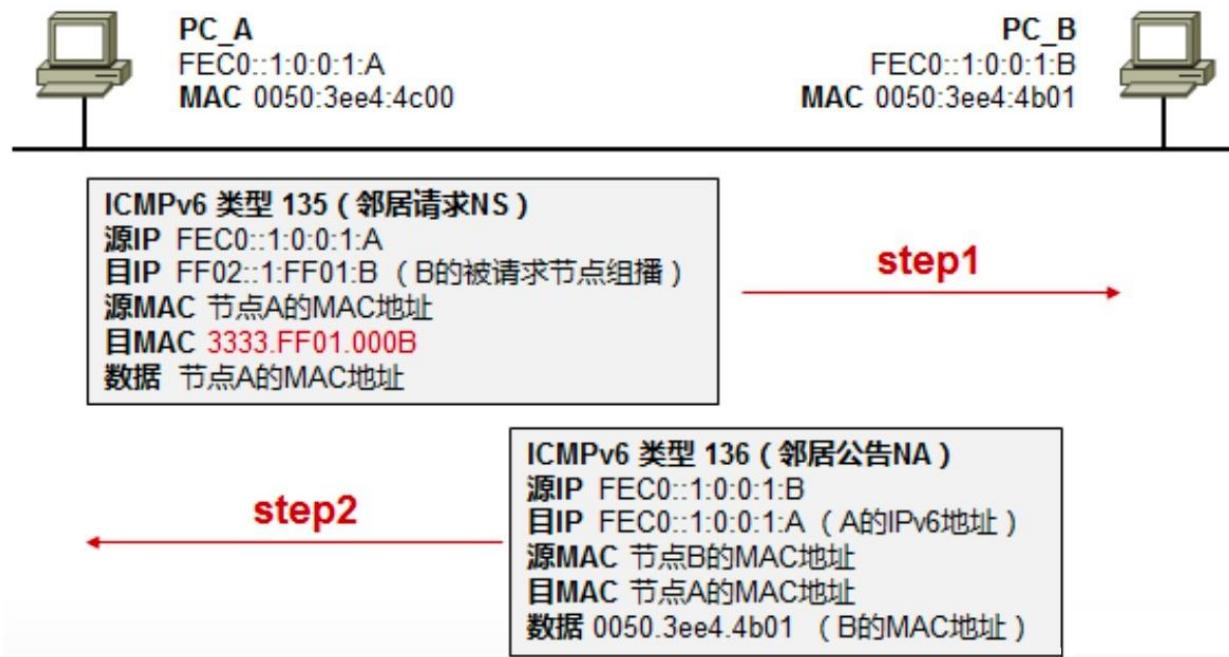
## Table 21.4 ICMPv4和IMCPv6中查询报文的比较

Type of Message	Version 4	Version 6
Echo request and reply	Yes	Yes
Timestamp request and reply	Yes	No
Address-mask request and reply	Yes	No
Router solicitation and advertisement	Yes	Yes
Neighbor solicitation and advertisement	ARP	Yes
Group membership	IGMP	Yes

# 邻居发现协议NDP (Neighbor Discovery Protocol)

- ◆ NDP是IPv6协议体系中一个重要的基础协议，替代了IPv4的ARP和ICMP路由器发现，它定义了使用ICMPv6报文实现地址解析，跟踪邻居状态，重复地址检测，路由器发现以及重定向等功能。
- ◆ ARP报文是直接封装在以太网帧中，普遍观点认为ARP为第2.5层协议。NDP基于ICMPv6实现，使用的所有报文均封装在ICMPv6报文中，地址解析过程中使用了邻居请求NS(Neighbor Solicitation)和邻居通告NA(Neighbor Advertisement)两种ICMPv6报文。
- ◆ 通常NDP被看作第3层的协议。在三层完成地址解析的好处如下：
  - ✓ 不同的二层介质可以采用相同的地址解析协议；
  - ✓ 可以使用三层的安全机制避免地址解析攻击；
  - ✓ 使用组播方式发送请求报文，减少了二层网络的性能压力。

# IPv6地址解析过程



- ◆ Host A在向Host B发送报文之前必须解析出Host B的链路层地址。Host A发送一个NS报文，源地址为Host A的IPv6地址，目的地址为Host B的被请求节点多播地址，需要解析的目标IP为Host B的IPv6地址，表示Host A想知道Host B的链路层地址。其中NS报文的Options字段中还携带了Host A的链路层地址。
- ◆ Host B接收到NS报文后回应NA报文，其中源地址为Host B的IPv6地址，目的地址为Host A的IPv6地址（使用NS报文中的Host A的链路层地址进行单播），Host B的链路层地址被放在Options字段中。

# 作业

---

- P425页
  - 13,15
-