第21章

地址映射，差错报告和多播

21-1 地址映射

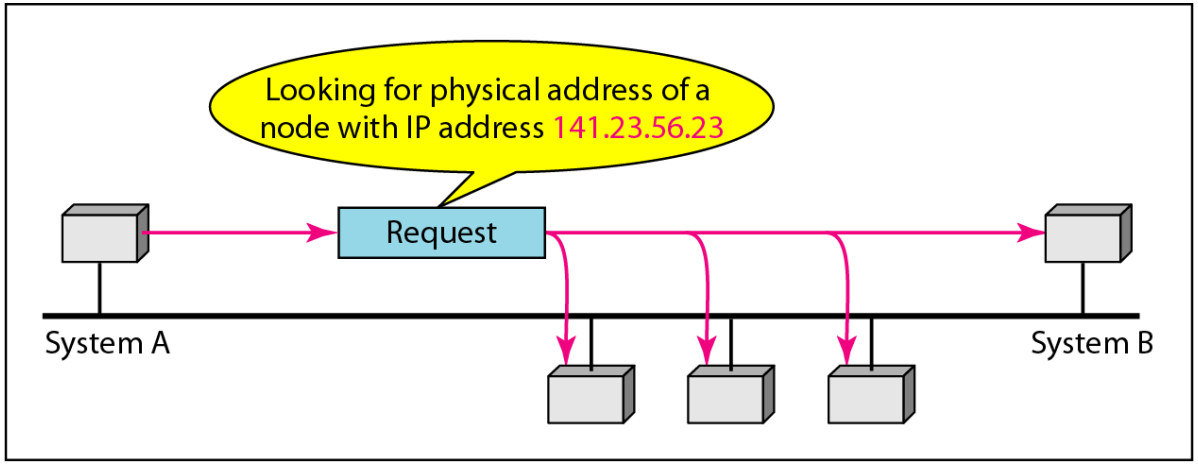
将分组传递到主机或路由器需要两级地址：逻辑地址 和 物理地址. 我们需要将一个逻辑地址映射成为它对应的物理地址，反过来也一样。这可以通过静态或动态映射完成。

讨论:

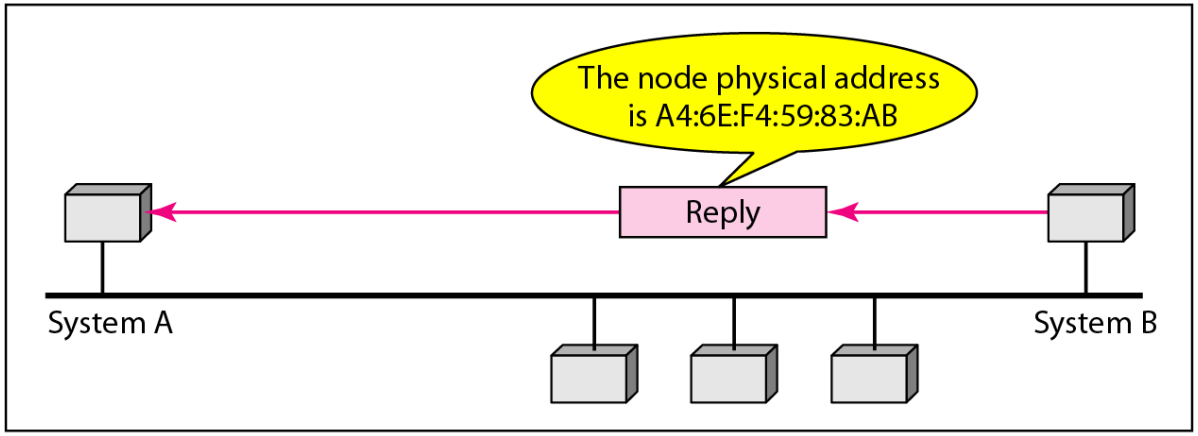
逻辑地址映射到物理地址，*ARP*（Address Resolution Protocol）

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

图 21.1 *ARP*（Address Resolution Protocol）*操作*（逻辑地址到物理地址



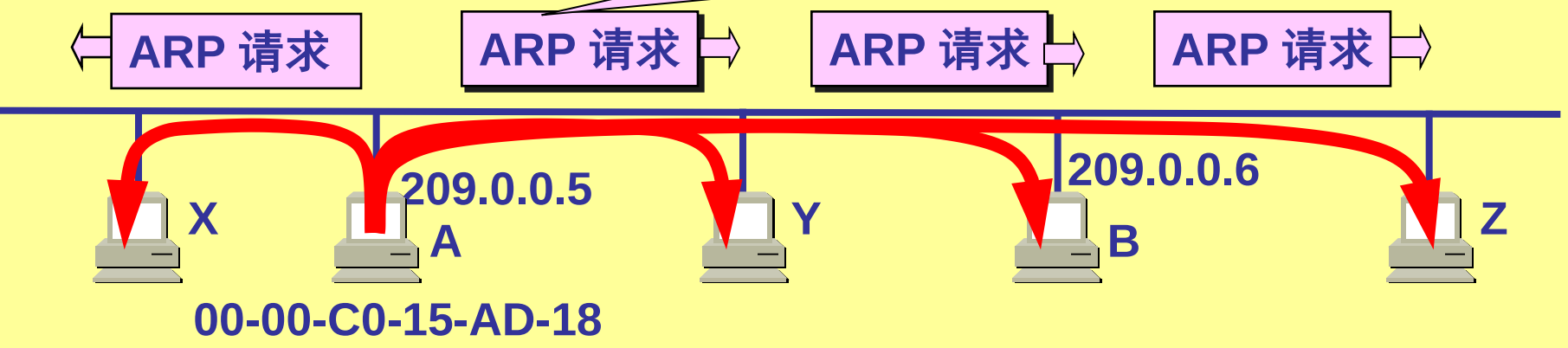
a. ARP request is broadcast



b. ARP reply is unicast

主机 A 广播发送
ARP 请求分组

我是 209.0.0.5，硬件地址是 00-00-C0-15-AD-18
我想知道主机 209.0.0.6 的硬件地址



主机 B 向 A 发送
ARP 响应分组

我是 209.0.0.6
硬件地址是 08-00-2B-00-EE-0A

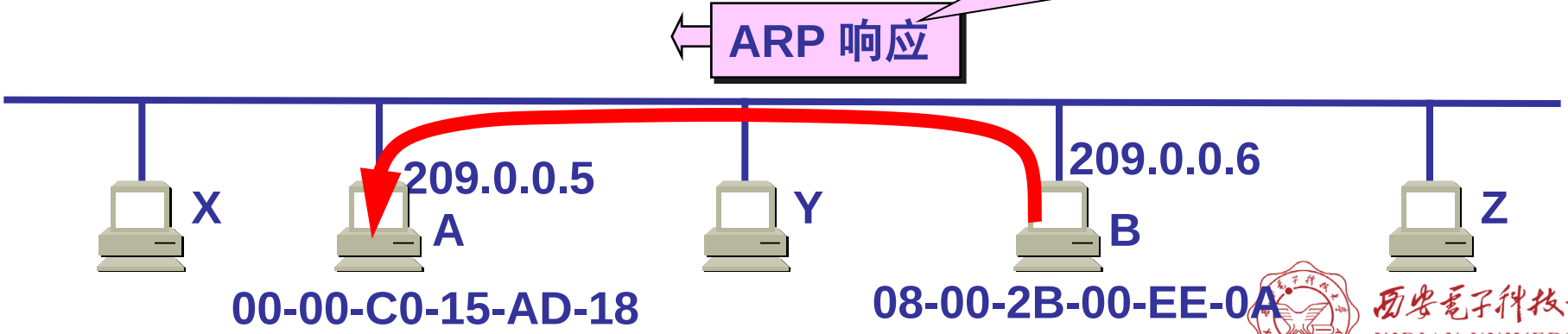


图 21.2 *ARP 分组*

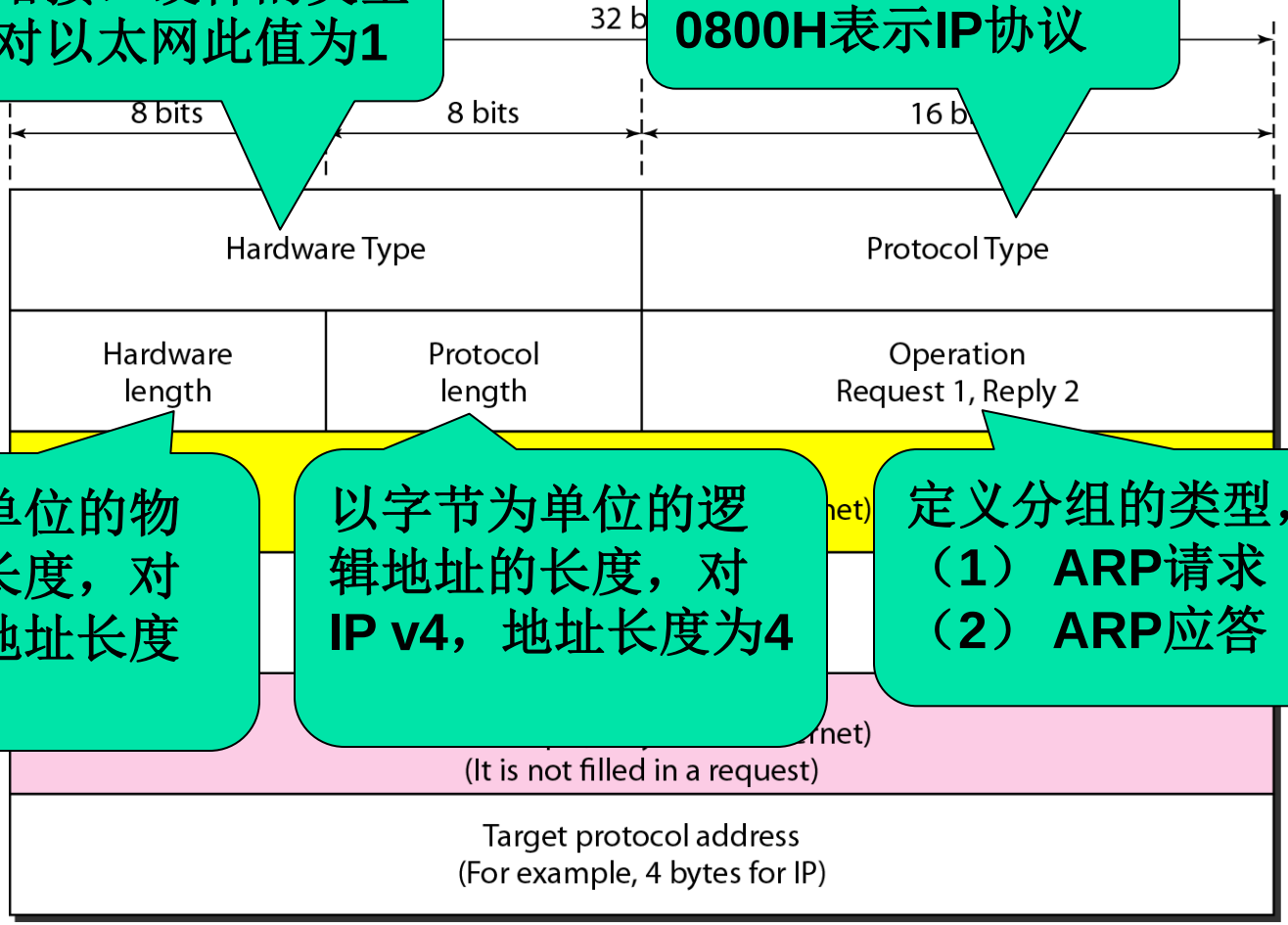


图 21.3 *ARP 分组的封装*

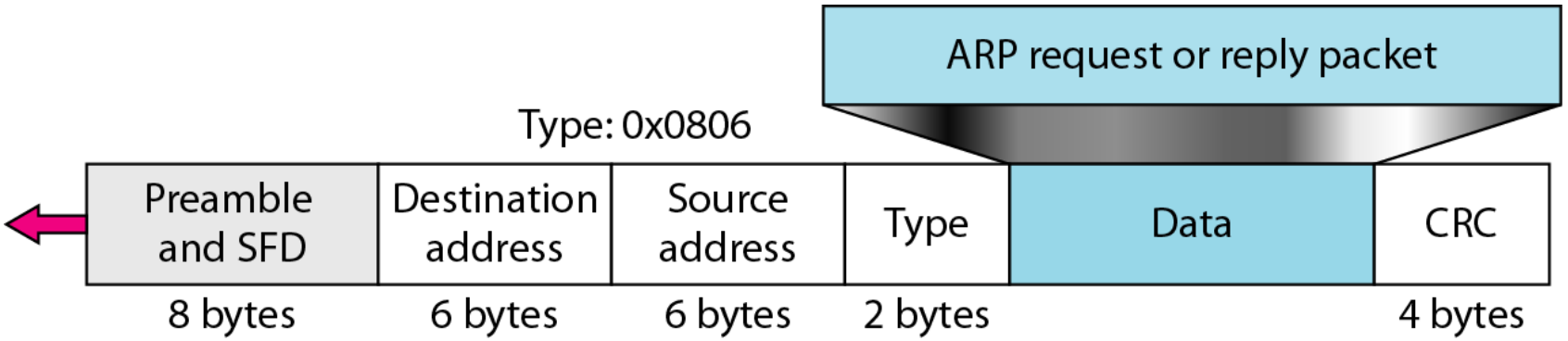
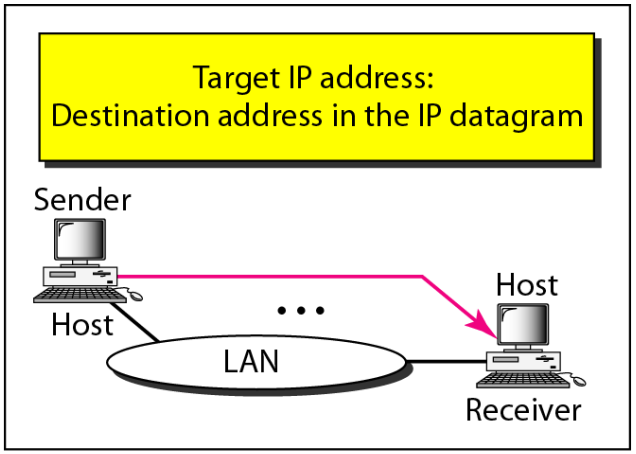
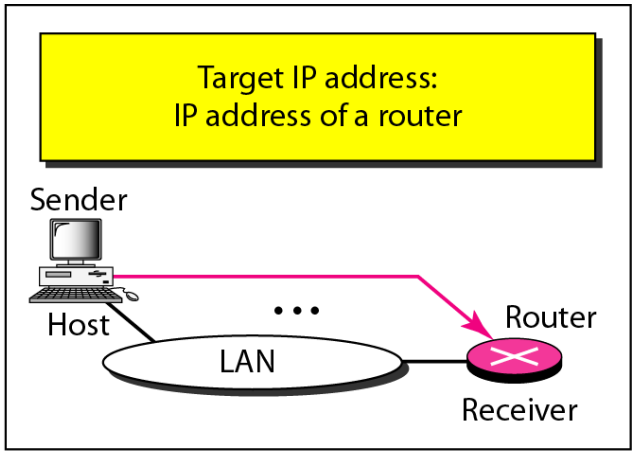


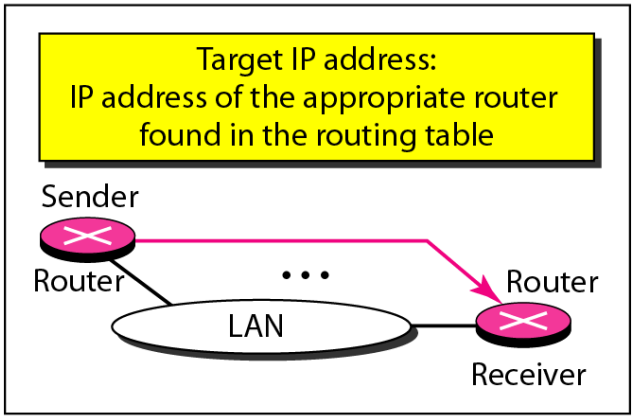
图 21.4 使用ARP的四种情况



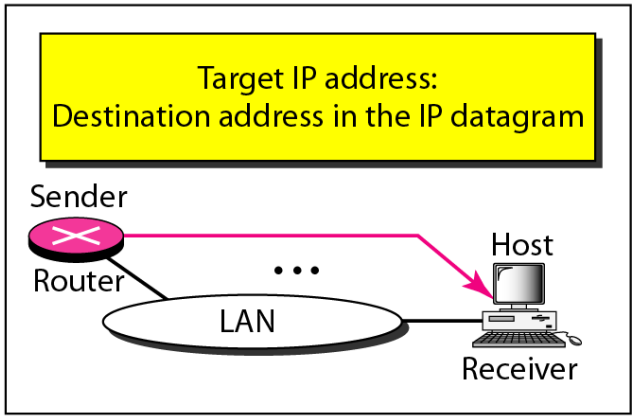
Case 1. A host has a packet to send to another host on the same network.



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.

注意

ARP 请求报文是广播发送;
ARP 回答报文是单播发送.

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（第一个主机并不知道该物理地址）。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，这就是我们为什么不以4字节界限表示这些地址

图 21.5 例21.1, ARP 请求与回答分组

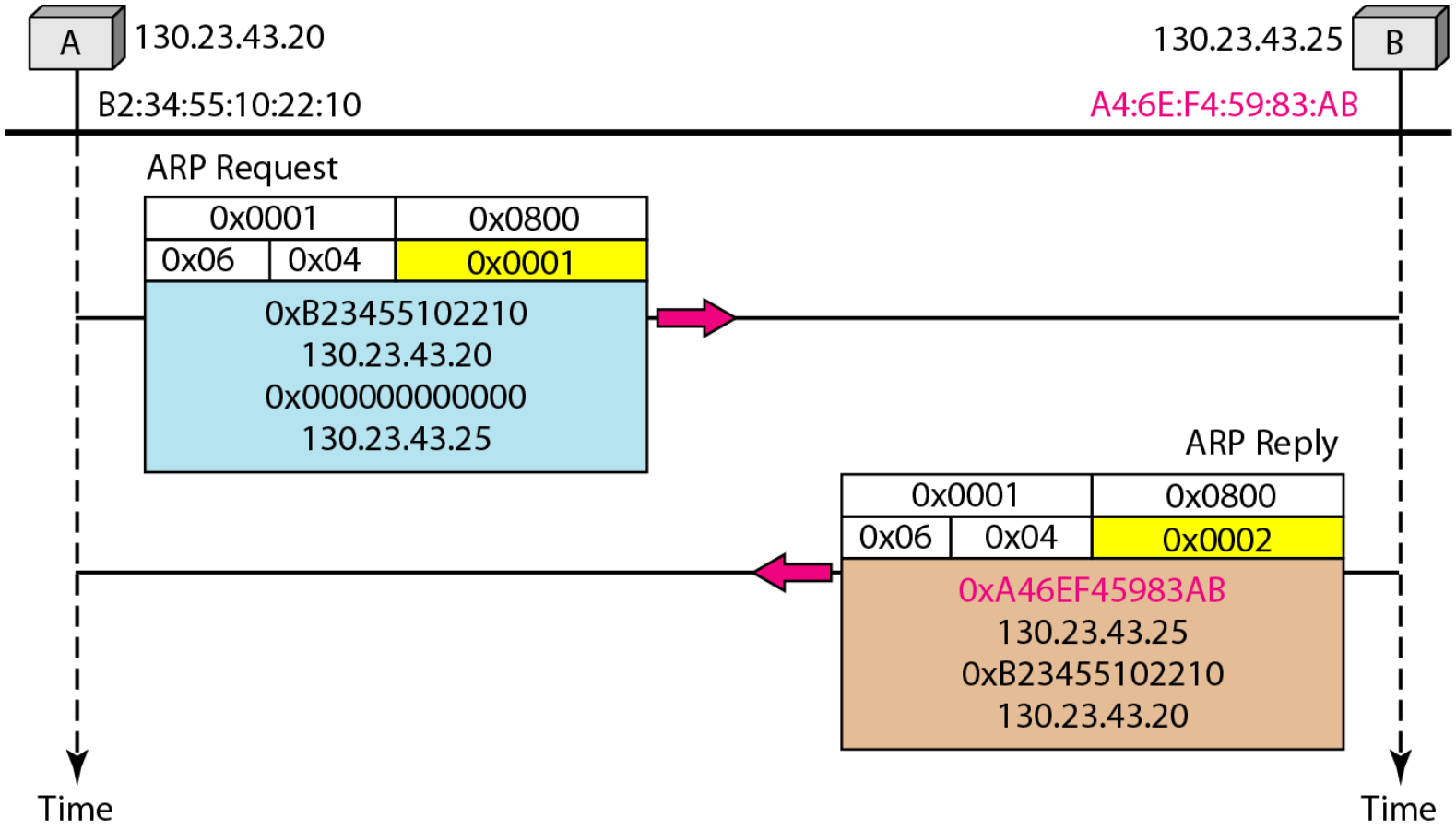


图 21.6 代理ARP

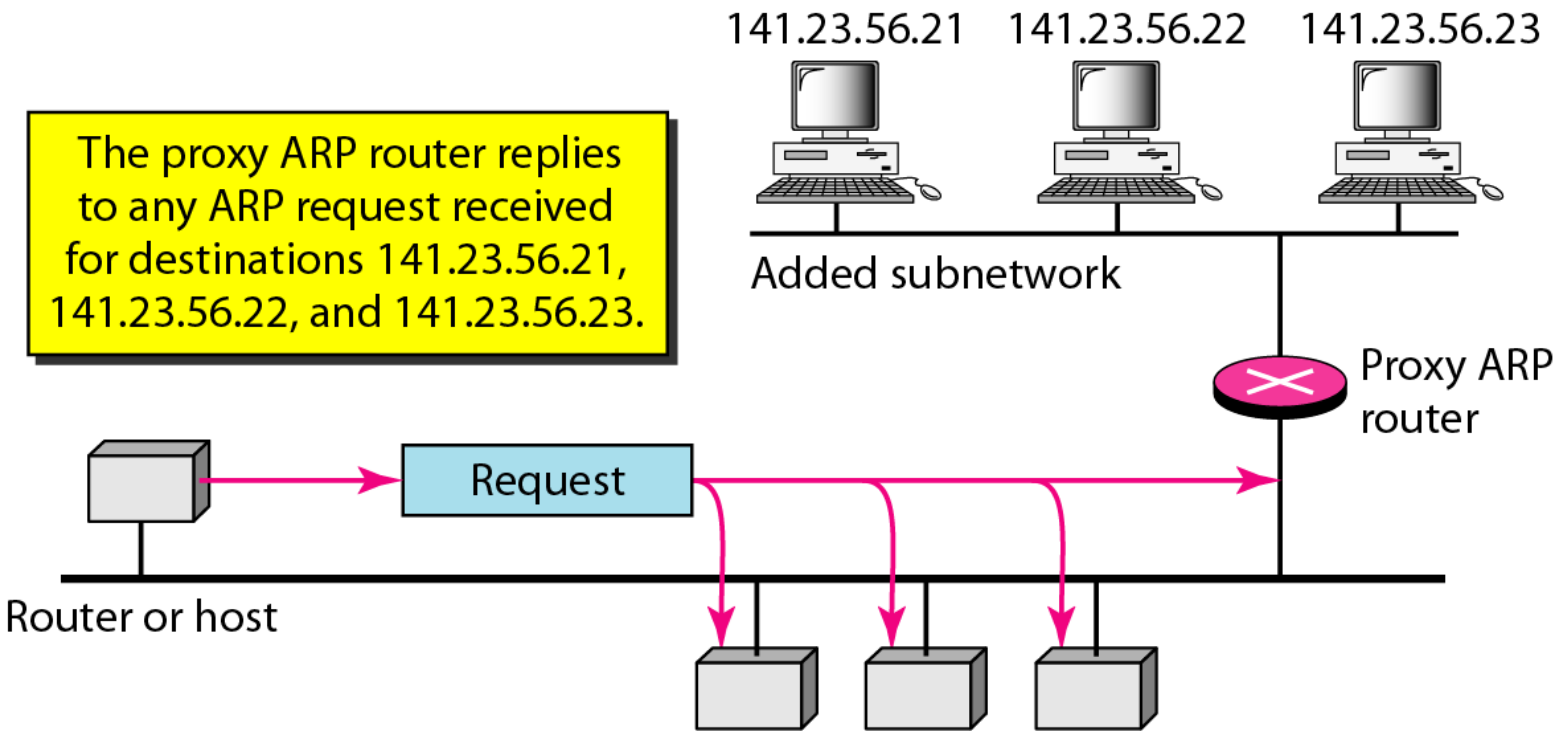


图 21.7 在同一网络上和不同网络上的BOOTP客户和服务器

1.BOOTP是一种C/S协议，提供物理地知到逻辑地址的转换

2. BOOTP报文被封装到UDP分组中，UDP再被封装到IP分组中。

3. BOOTP的优点是它在应用层上，因此客户机无IP地址，只能广播。广播报不能通过路由器。多数情况下在同一个局域网内。

4.BOOTP不能动态配置，只能静态配置。

注意

DHCP 提供可以是人工的或自动的静态或动态的地址配置。

- **Dynamic Host Configuration Protocol**
- **DHCP有第二个数据库，即一个可用的IP地址池。**
- **得到的IP地址有租用期(lease)**

21-2 ICMP

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。

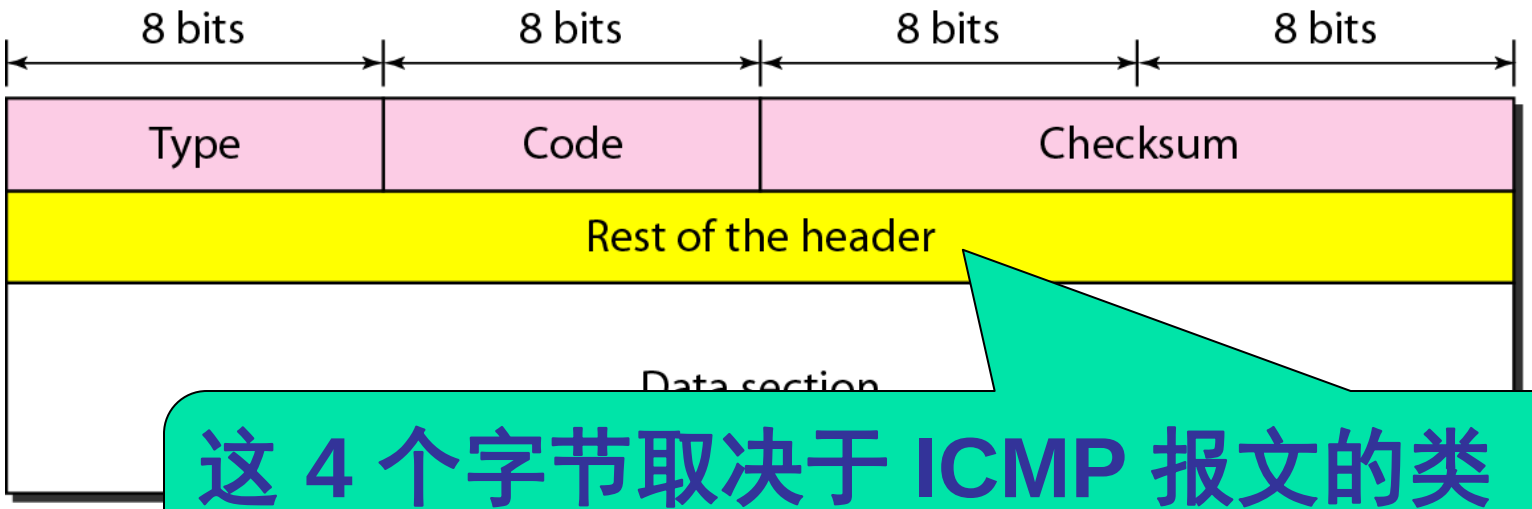
讨论:

报文类型
报文格式
差错报告和查询
调试工具

ICMP

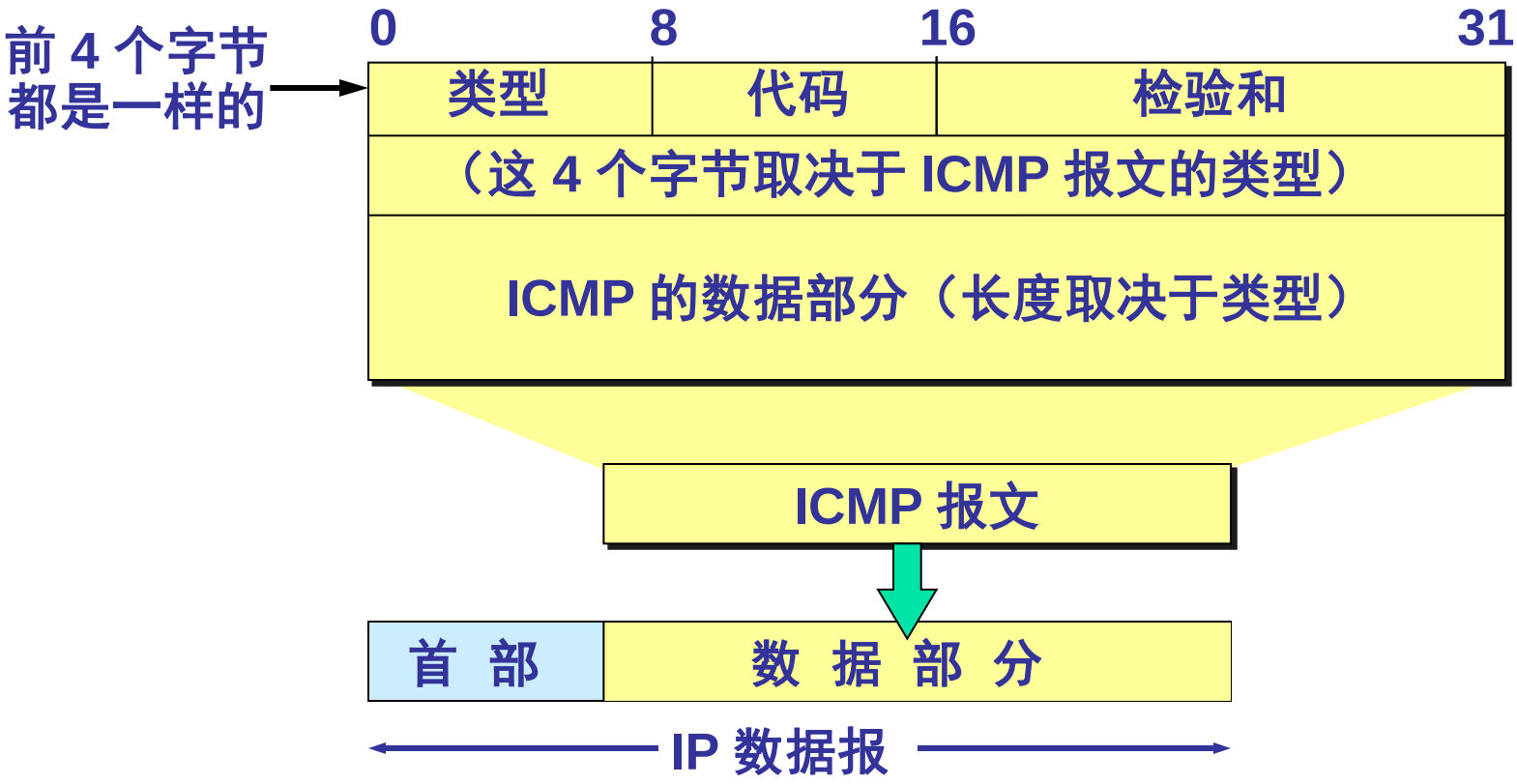
- 为了提高 IP 数据报交付成功的机会，在网际层使用了因特网控制报文协议 ICMP (Internet Control Message Protocol)。
- ICMP 允许主机或路由器报告差错情况和提供有关异常情况的报告。
- ICMP 不是高层协议，而是 IP 层的协议。
- ICMP 报文作为 IP 层数据报的数据，加上数据报的首部，组成 IP 数据报发送出去。
- ICMP不能纠错，只能报告错误

图 21.8 *ICMP 报文一般格式*



这 4 个字节取决于 ICMP 报文的类型

ICMP 报文的格式



注意

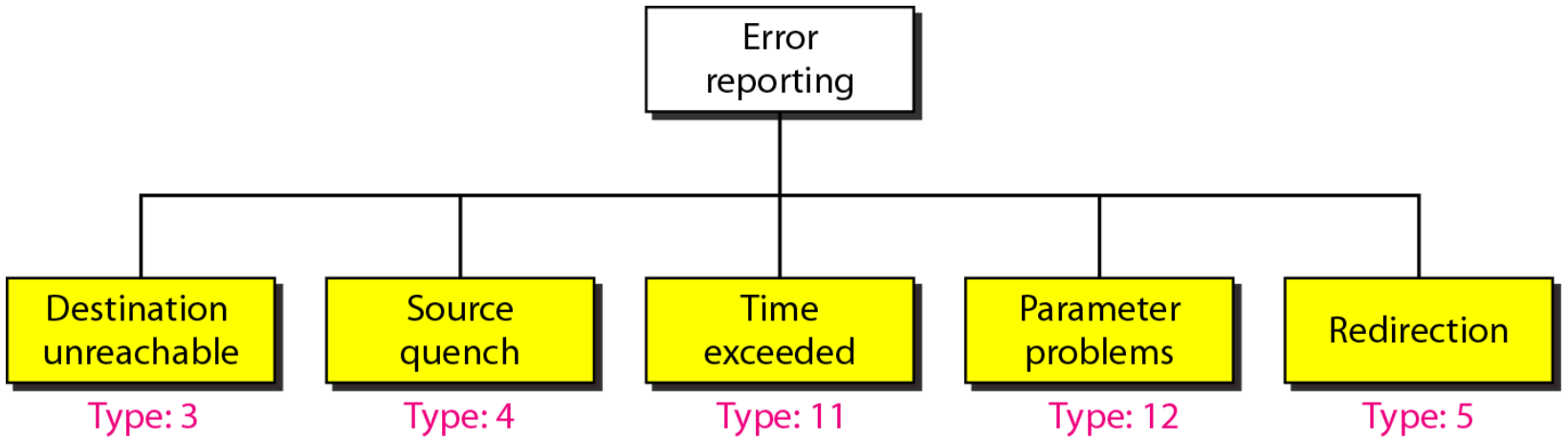
ICMP 总是向原始的源方报告差错报文。

注意

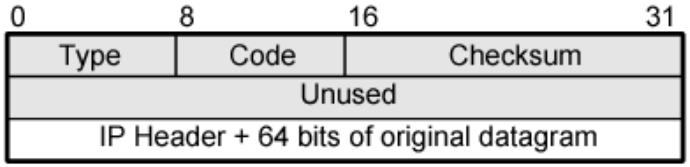
关于ICMP 差错报文有下列要点:

- 对于携带ICMP差错报文的数据报，不再产生ICMP差错报文。
- 对于分段的数据报文，如果不是第一个分段则不产生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。

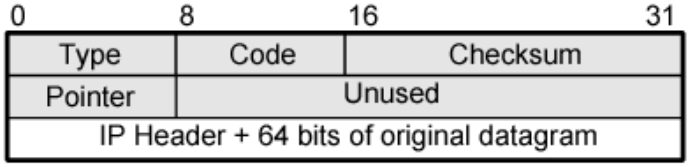
图 21.9 差错报告报文



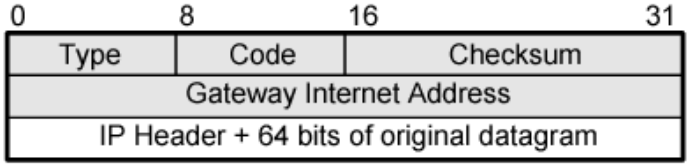
ICMP Message Formats



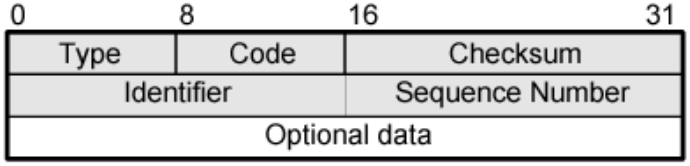
(a) Destination Unreachable; Time Exceeded; Source Quench



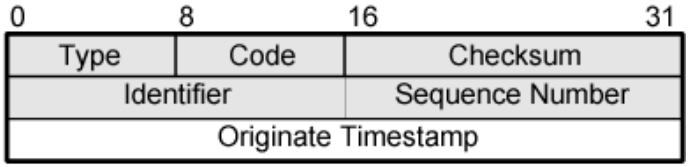
(b) Parameter Problem



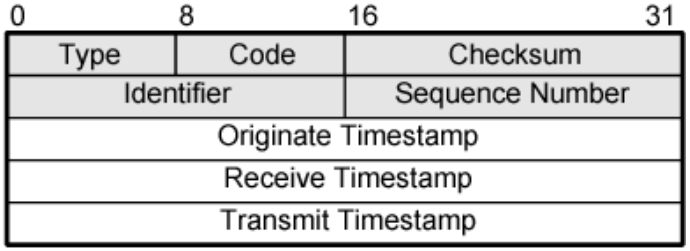
(c) Redirect



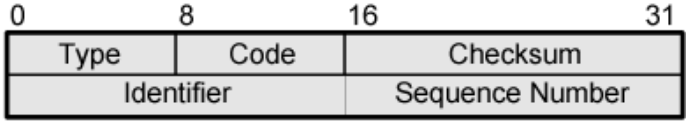
(d) Echo, Echo Reply



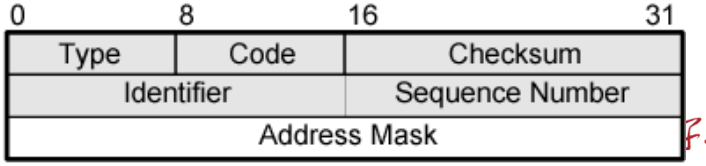
(e) Timestamp



(f) Timestamp Reply



(g) Address Mask Request



(h) Address Mask Reply

目的不可达

- 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
- 目的端的不可达报文或者有路由器产生，或者由目的主机创建

抑制源端

- 用来补充流量控制
- 当路由器或者目的主机中产生拥塞的时候，路由器或者目的主机丢弃数据报，发送source-quench message报文给发送方
- 类似于拥塞控制中的阻流分组。

时间超时

- 产生的原因有两种：
  - TTL减为0时，路由器丢弃数据报，
  - 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

参数问题

- IP分组的Header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Parameter-problem message

图 21.10 差错报文的数据字段的内容

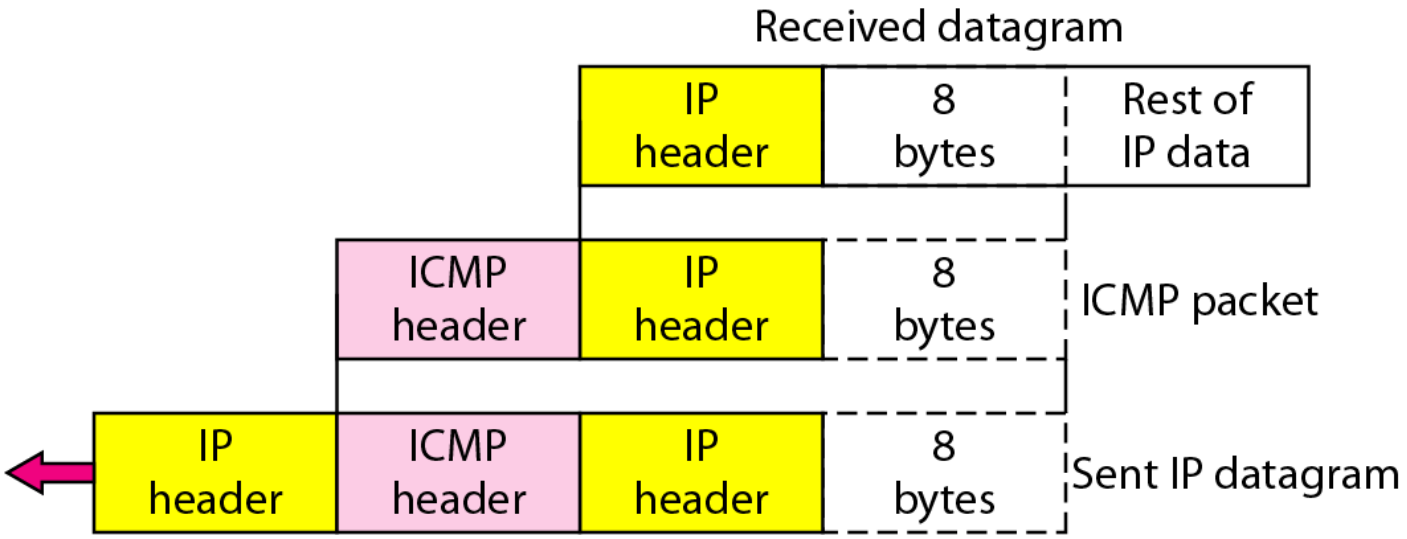
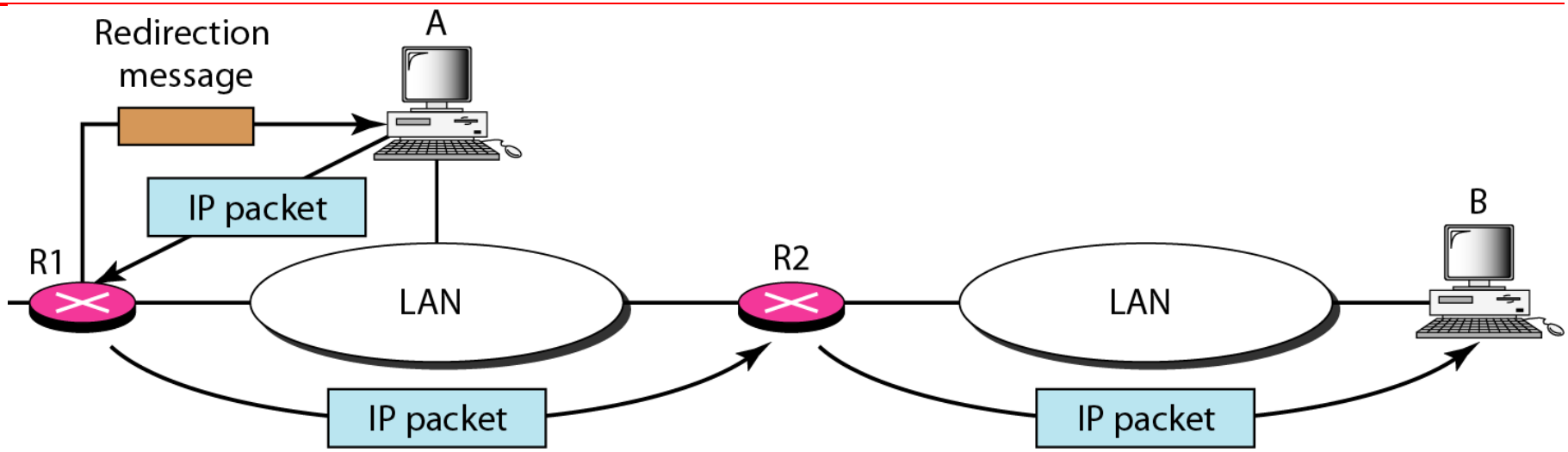
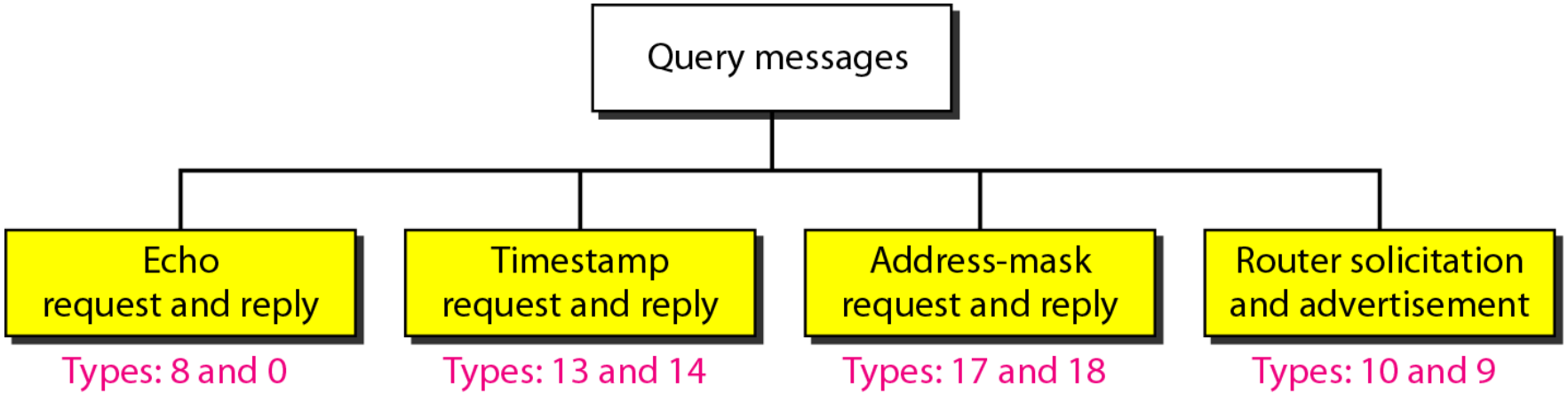


图 21.11 *重定向概念*



- 是路由更新过程中出现的问题
- 例子中：**A想向B发送数据报，R2有有效的路由，但A却选择了R1，R1收到后发现应该走R2，把分组发给R2，同时向A发送Redirection message.**

图 21.12 *查询报文*



- 回送请求报文：诊断网络
- 时间戳请求和回答：确定数据报的往返时间
- 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。

例21.3

我们用ping 程序测试服务器fhda.edu。
结果如下：

ping程序发送报文的序列号从0开始，每次探测给出这次的往返时间。封装了 ICMP报文的IP数据报的TTL（生存时间）字段已被为置为62，这就是说该分组的传输不能超过62跳。

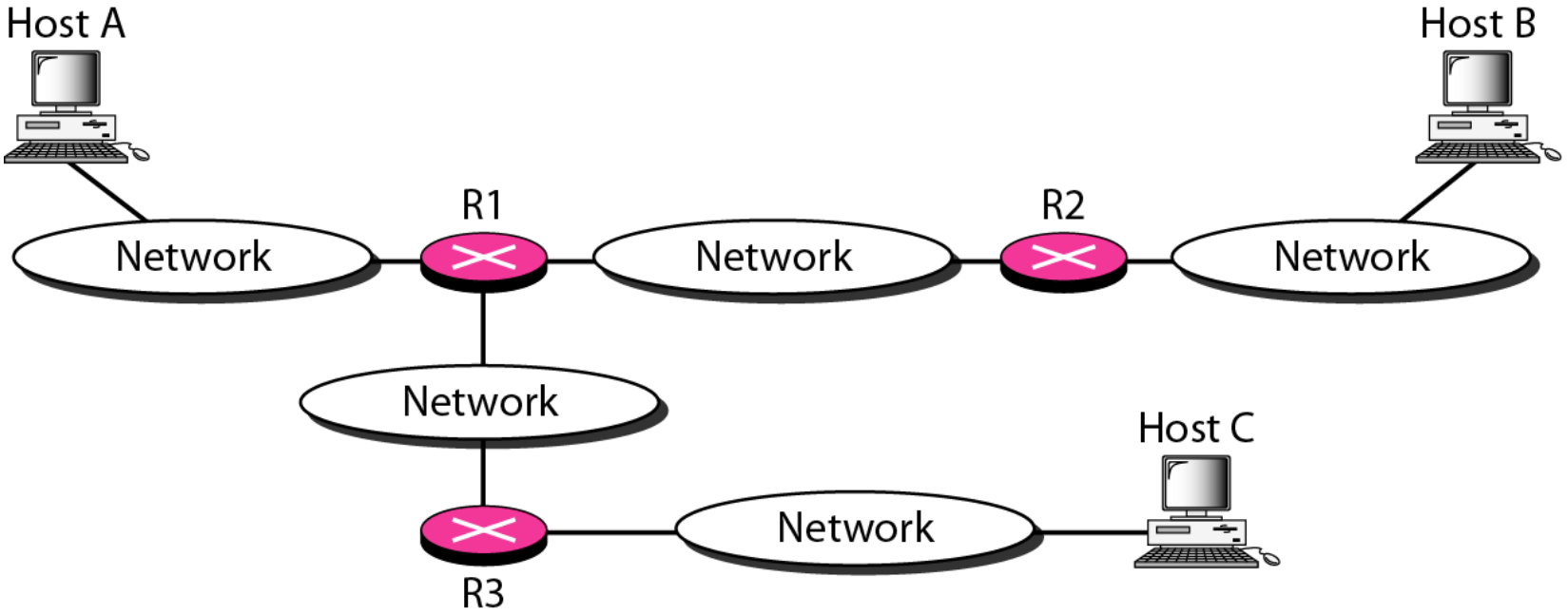
一开始ping程序定义数据部分为56个字节，IP数据报总长度为84字节。这是显然的，这是因为我们要增加ICMP头部8字节和IP头部20字节，所以其结果是84字节。但是注意:每次探测ping程序定义的字节个数为64，这是ICMP分组的总长度(56+8)。

例 21.3 (续)

```
$ ping fhda.edu
PING fhda.edu (153.18.8.1)   56 (84)  bytes of data.
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=0    ttl=62    time=1.91 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=1    ttl=62    time=2.04 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=2    ttl=62    time=1.90 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=3    ttl=62    time=1.97 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=4    ttl=62    time=1.93 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=5    ttl=62    time=2.00 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=6    ttl=62    time=1.94 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=7    ttl=62    time=1.94 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=8    ttl=62    time=1.97 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=9    ttl=62    time=1.89 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=10   ttl=62    time=1.98 ms

--- fhda.edu ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10103ms
      rtt min/avg/max = 1.899/1.955/2.041 ms
```

图 21.15 *traceroute 程序的操作*



例21.4

我们用traceroute程序求计算机voyager.deanza.edu到服务器fuda.edu的路由，下面表示其结果:

```
$ traceroute fhda.edu
traceroute to fhda.edu    (153.18.8.1), 30 hops max, 38 byte packets
 1  Dcore.fhda.edu        (153.18.31.254)    0.995 ms    0.899 ms    0.878 ms
 2  Dbackup.fhda.edu      (153.18.251.4)     1.039 ms    1.064 ms    1.083 ms
 3  tiptoe.fhda.edu       (153.18.8.1)       1.797 ms    1.642 ms    1.757 ms
```

命令后无序列的行表示了目的端是153.18.8.1， TTL值是30跳，该分组包含38个字节：IP头部20个字节、UDP头部8个字节和应用数据10个字节。traceroute程序使用应用数据存储分组的轨迹。

例 21.4 (continued)

第一行表示访问第一个路由器，该路由器名称是Dcore.fuda.edu，其IP地址为135.18.31.254。第一个往返时间是0.995ms，第二个往返时间是0.899ms，第三个往返时间是0.878ms。

第二行表示访问第二个路由器，该路由器名称是Dbackup.fhda.edu，其IP地址为153.18.251.40，也显示了三个往返时间。

第三行表示目的主机。我们知道这是目的主机，因为没有更多的行。目的主机是服务器fhda.edu，但它的名称是tiptoe.fuda.edu，其IP地址为153.18.8.1，也显示了三个往返时间。

例21.5

下页的例子我们追踪了一个较长的路由，到xerox.com的路由。此处在源端到目的端有17跳。注意：有些往返时间看起来非常异常，这可能是路由器太忙不能立即处理分组。

例 21.5 (续)

```
$ traceroute xerox.com
traceroute to xerox.com (13.1.64.93), 30 hops max, 38 byte packets
 1  Dcore.fhda.edu          (153.18.31.254)     0.622 ms   0.891 ms   0.875 ms
 2  Ddmz.fhda.edu           (153.18.251.40)     2.132 ms   2.266 ms   2.094 ms
 3  Cinic.fhda.edu          (153.18.253.126)    2.110 ms   2.145 ms   1.763 ms
 4  cenic.net               (137.164.32.140)    3.069 ms   2.875 ms   2.930 ms
 5  cenic.net               (137.164.22.31)     4.205 ms   4.870 ms   4.197 ms
      . . . .                 . . . .             . . .      . . . .    . . .
14  snfc21.pbi.net          (151.164.191.49)    7.656 ms   7.129 ms   6.866 ms
15  sbcglobal.net           (151.164.243.58)    7.844 ms   7.545 ms   7.353 ms
16  pacbell.net             (209.232.138.114)   9.857 ms   9.535 ms   9.603 ms
17  209.233.48.223          (209.233.48.223)    10.634 ms  10.771 ms  10.592 ms
18  alpha.Xerox.COM         (13.1.64.93)        11.172 ms  11.048 ms  10.922 ms
```

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(正如我们将会看到)，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*

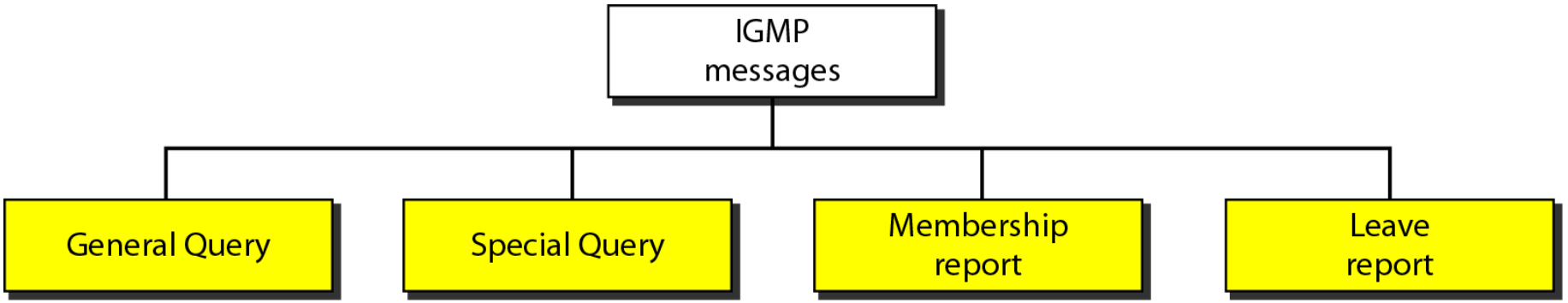


图 21.17 *IGMP报文格式*

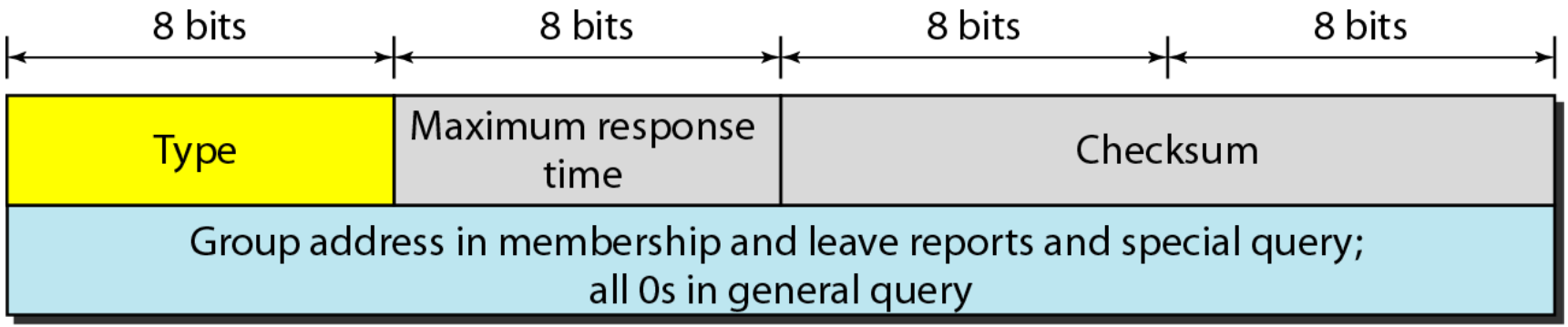
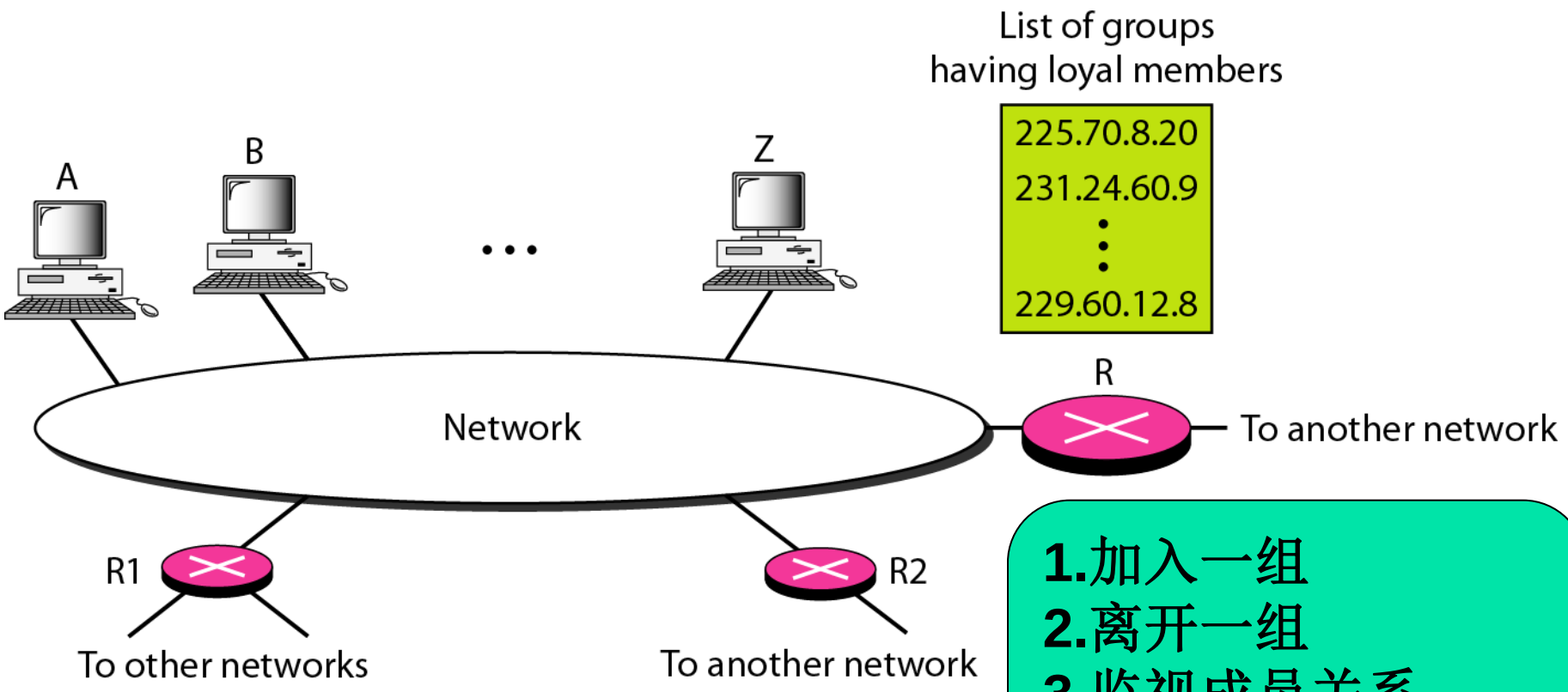


Table 21.1 *IGMP 类型字段*

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*



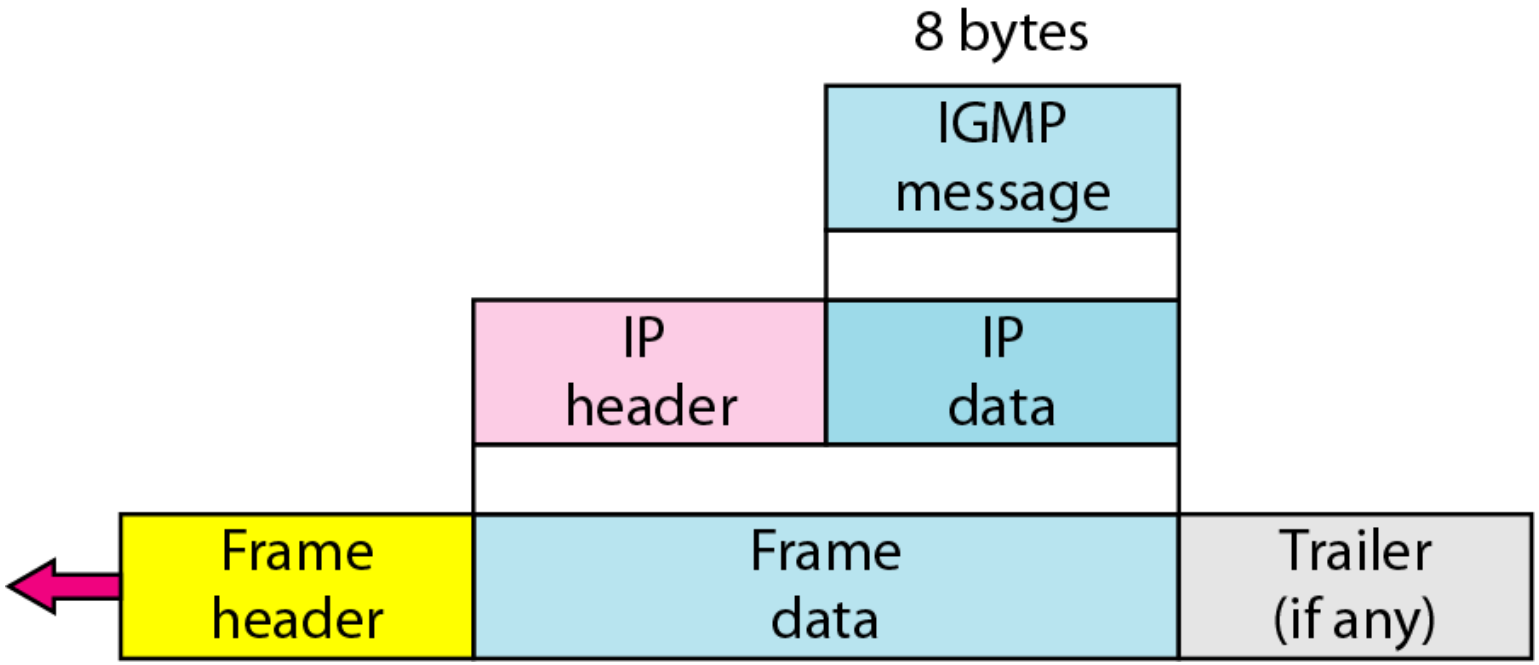
1.加入一组
2.离开一组
3.监视成员关系
4.延迟响应
5.查询路由器

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*



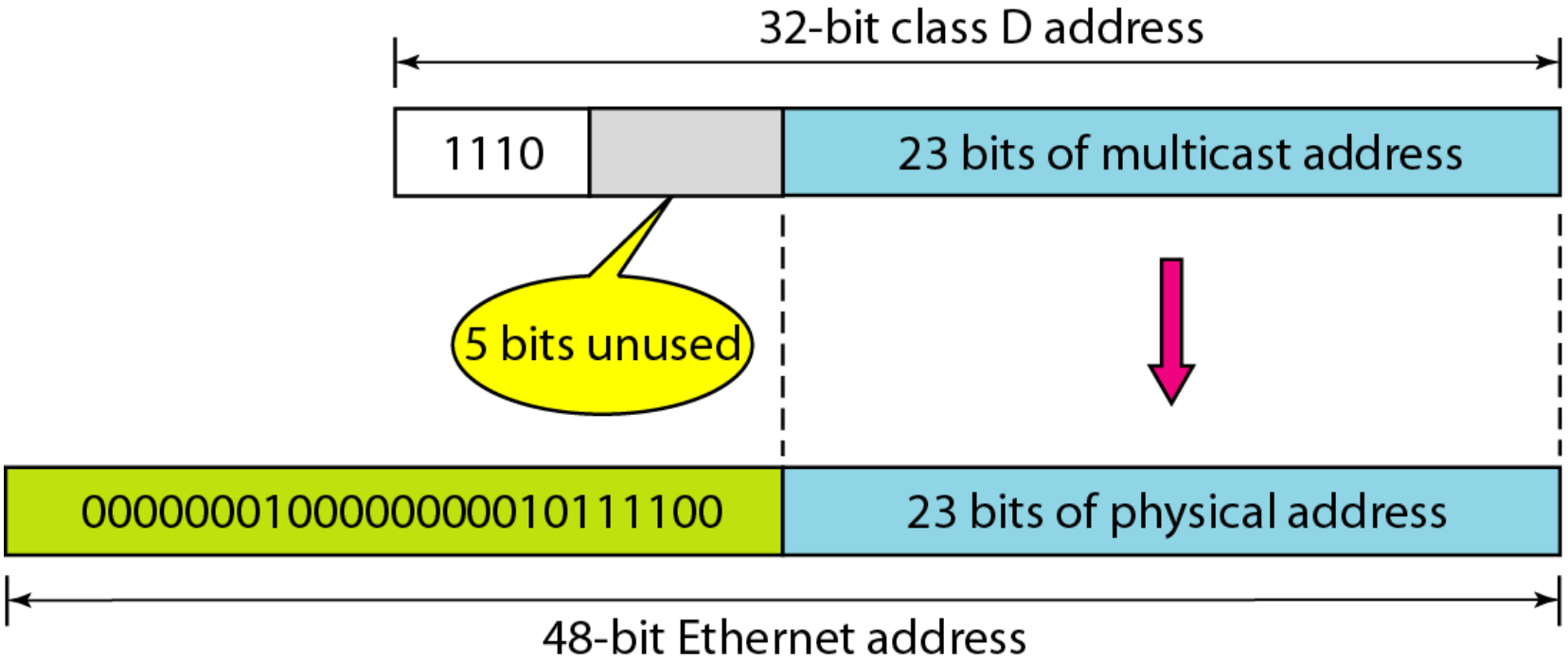
注意

携带IGMP分组的IP分组的TTL字段的值为1

Table 21.2 目的IP地址

Type	*IP Destination Address*
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

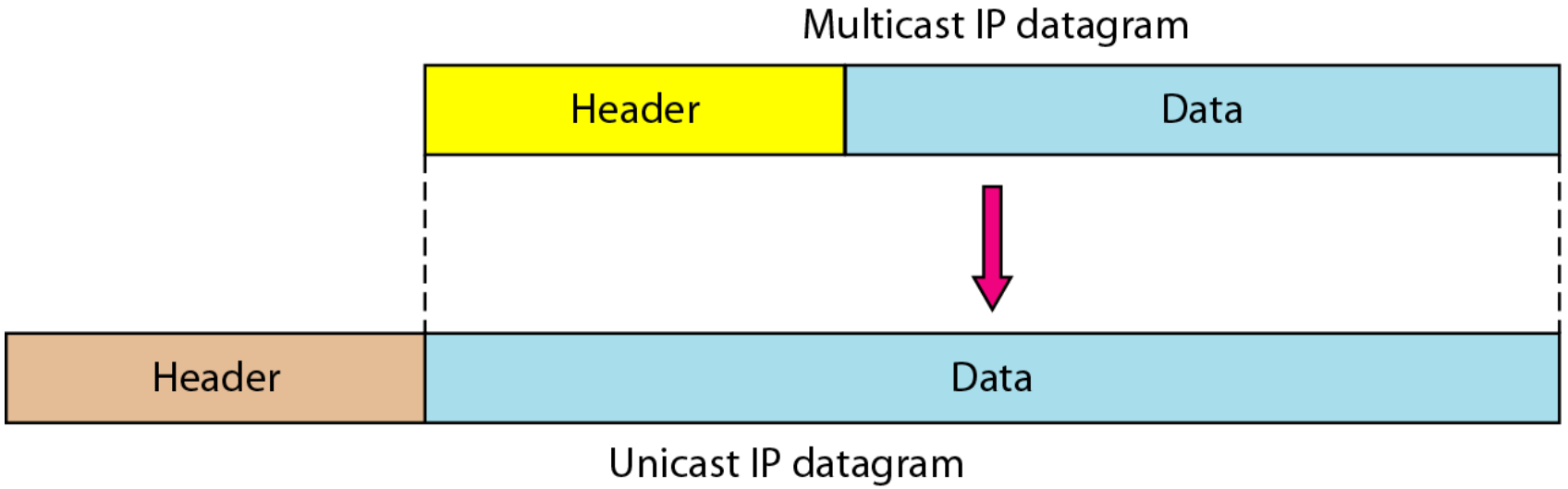


注意

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*



是指无物理多播地址支持的一种方法。

例21.9

我们使用带有三个选项的netstat命令（见下页）：-n，-r和-a。

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)。注意:这里仅给出与我们讨论有关的项目。“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)。

注意: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。

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

21-4 ICMPv6

我们在第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

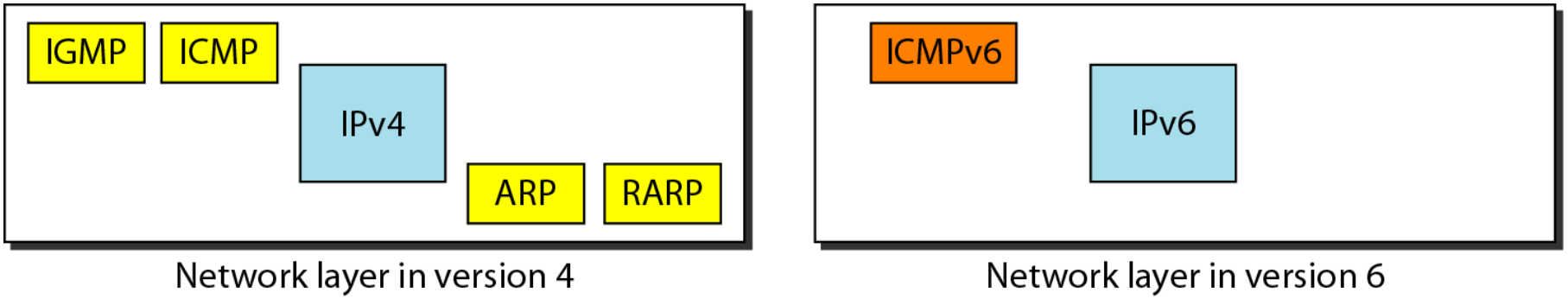


Table 21.3 *ICMPv4和ICMP峭的差错报告的比较*

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

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

作业：

- P425页
- 13,15