

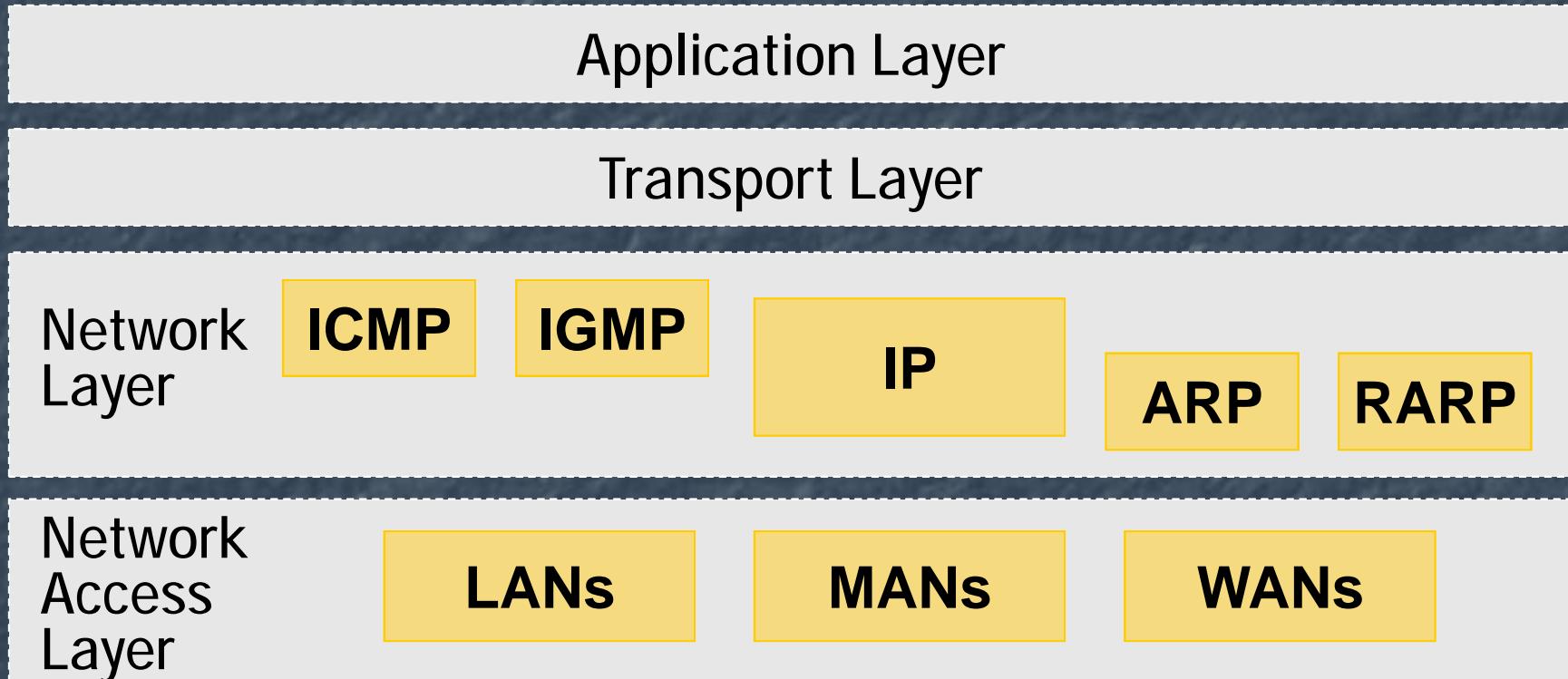
Chapter 4 Internet Protocol (IP, 网际协议)

■ IP分组的交付与路由选择

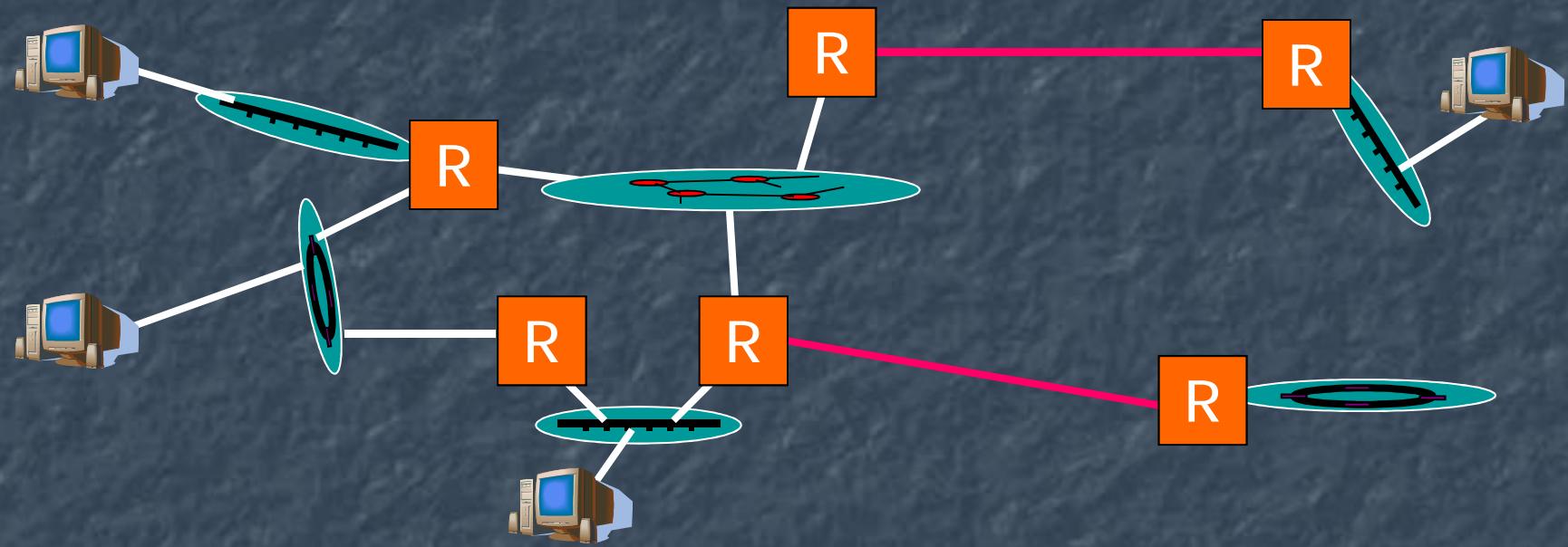
■ IP数据包格式

Internet Protocol (IP)

n RFC 791: INTERNET PROTOCOL (1981)



Architecture of the Internet



- 信息: IP 分组
- 节点: Router
- 信道: physical network

How about
only IP Adress?

Delivery and Routing



- Delivery (交付, 递交)
 - 对分组的物理转发
- Routing (路由选择, 选路)
 - 为分组寻找路径

Route: 路由、路径

Routing : 路由、路由选择、选路

第一部分

Delivery and Routing of IP Packets

(IP分组的交付与路由选择)

- n Connection
- n Delivery
- n Routing methods
- n Static vs. dynamic routing
- n Routing table and routing module
- n Classless addressing: CIDR

4.1 Connection-oriented vs. Connectionless Services

- Service (服务)
 - Network application: 业务
 - This chapter: 通信协议

网络层分组交换	面向连接		无连接
	建立连接 à 交付分组 à 终止连接		交付分组
	仅在建立连接时选路		每个分组独立选路
	相同		可以不同

The Features of IP Communication

n Features

n Connectionless 无连接的

- 特点：
每个数据报包含完整的地址信息；独立路由、不同的路径
- 优点：
多种（异构）网络都能满足的通信方式 → 通用性
允许多种路由选择策略（如：带宽、延时等）

n Unreliable 不可靠的

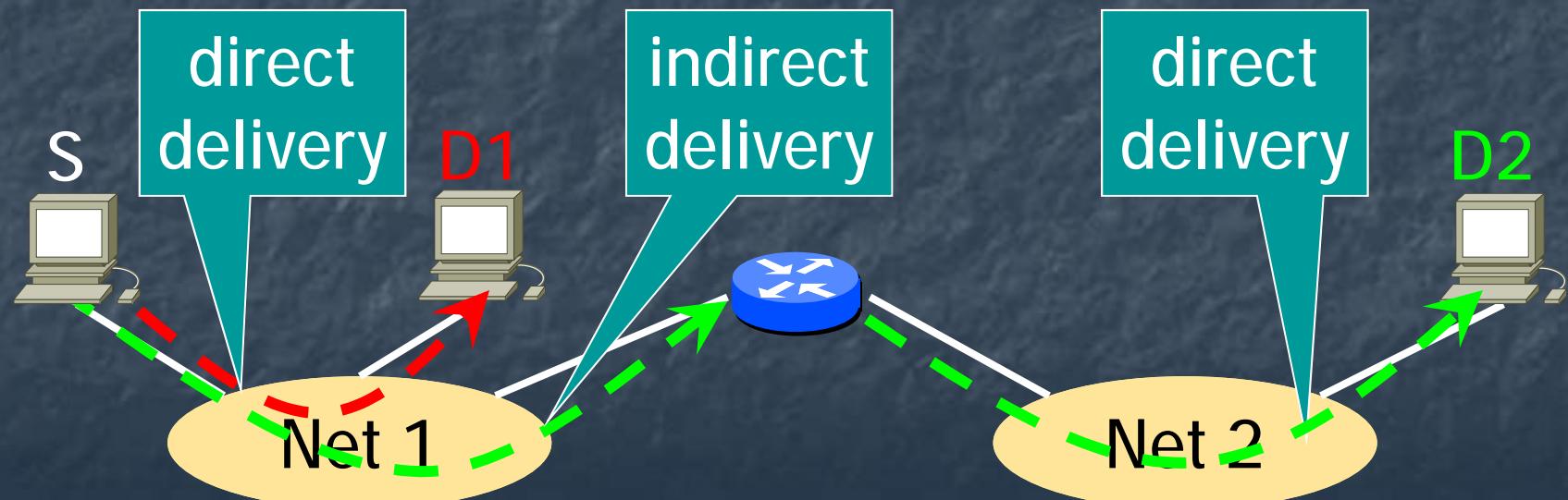
- 数据报可能丢失、顺序错乱
- 可靠性问题交由高层协议解决

n Best - effort delivery 尽最大努力交付

- IP协议不会随意丢弃数据报。只有当数据报出现差错、路由器资源耗尽、网络故障时才会丢弃数据报。

4.2 Direct vs. Indirect Delivery

- n Direct delivery (直接交付)
 - n 分组目的与分组的发送接口在同一IP网络中
- n Indirect delivery (间接交付)
 - n 分组目的与分组的发送接口在不同IP网络中



Delivery

- 交付方式的判断

- 分组目的IP与其发送接口是否在同一IP网络中？

目的IP & 发送口掩码 $\overset{?}{=}$ 发送口IP & 发送口掩码

- 相等：直接交付

- 不等：间接交付

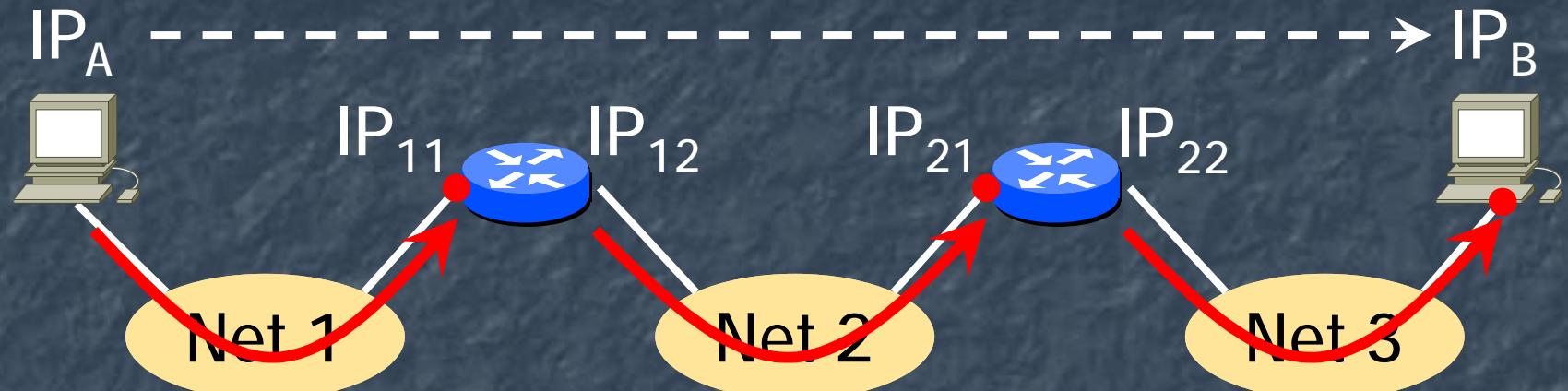
- 交付操作——地址映射：IP地址 \rightarrow 物理地址

- 直接交付：目的IP地址 \rightarrow 物理地址

- 间接交付：下一跳IP地址 \rightarrow 下一跳物理地址

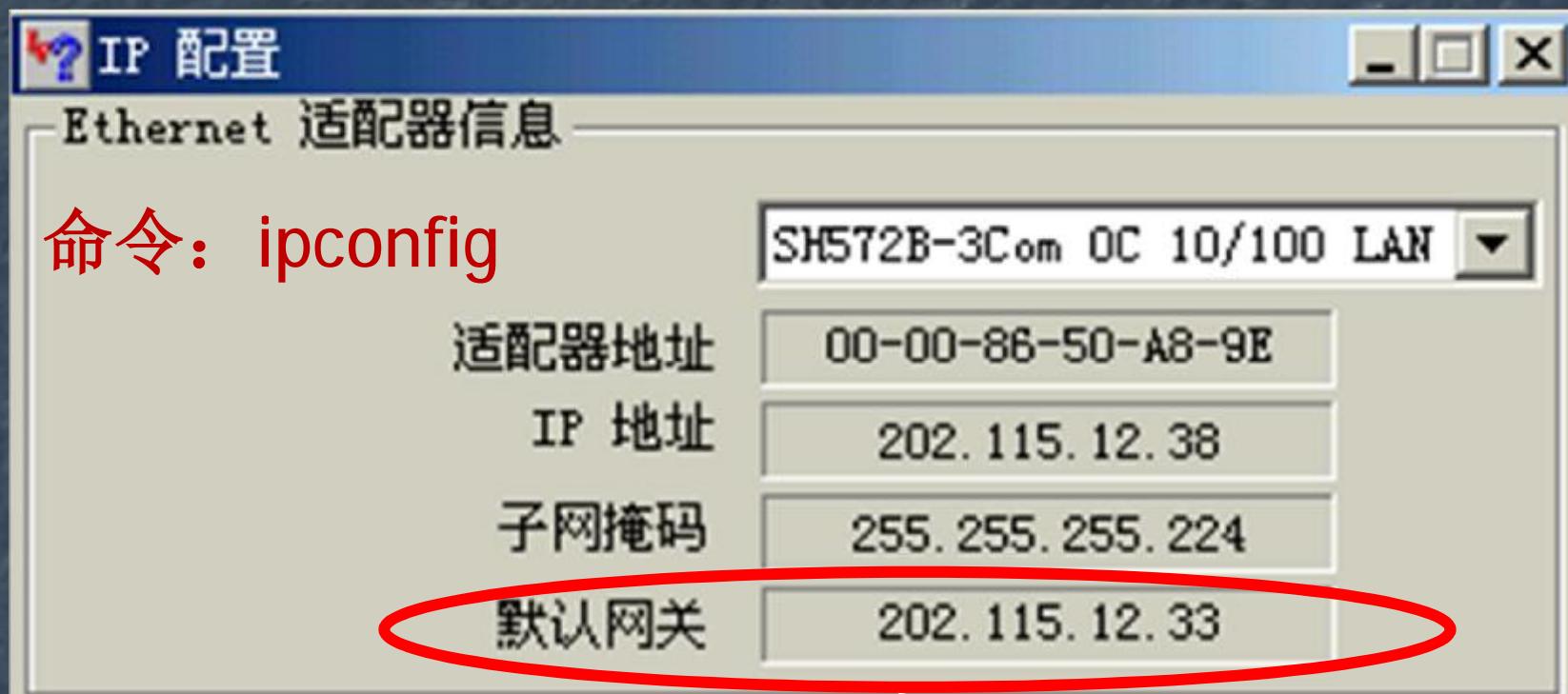
ARP

Next Hop (下一跳)



- Src IP = IP_A, Dst IP = IP_B 主机A的默认网关
- 1st delivery: indirect, Next-hop IP = IP₁₁
- 2nd delivery: indirect, Next-hop IP = IP₂₁
- 3th delivery: direct, Dst IP = IP_B

Indirect Delivery Configuration of the Host



Windows使用TCP/IP与网外通信时使用的间接交付地址，一般设置为可与外网进行通信的路由器。

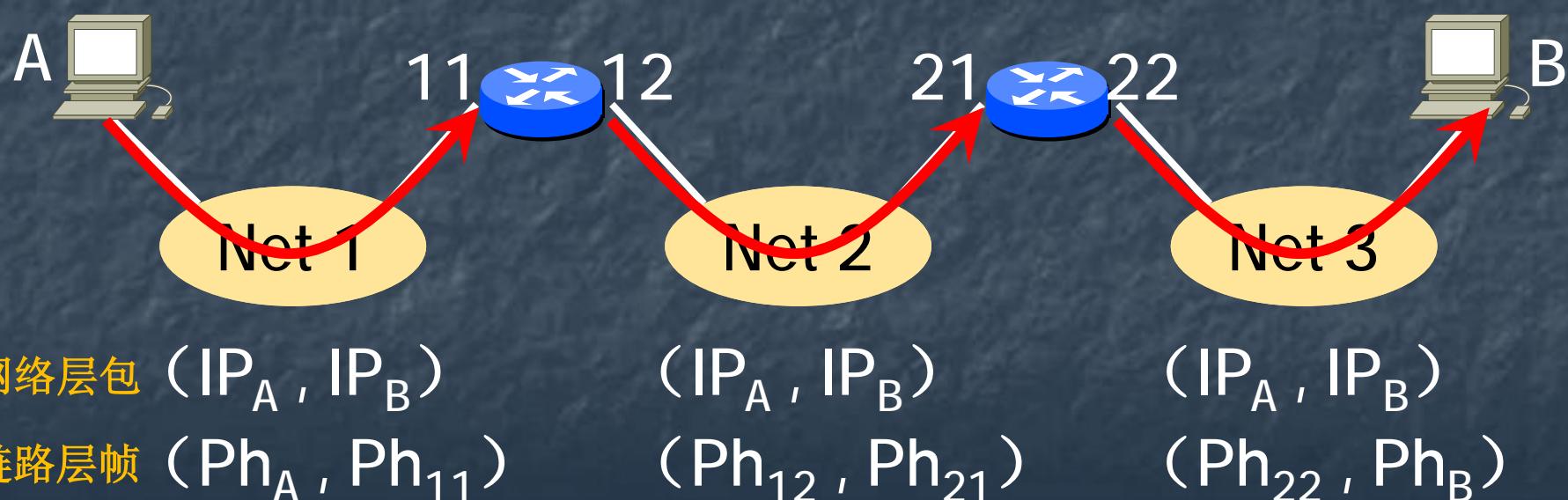
Discussion

■ 一次交付过程

■ 0或多个间接交付+1个直接交付（最后的交付）

■ 分组：（源IP地址， 目的IP地址） **保持不变**

■ 帧：（源物理地址， 目的物理地址） **逐跳改变**



思考

- n 下图所示的以太网中，哪几对主机间能进行IP通信？哪几对不能进行IP通信？为什么？

200.1.1.1/24



- n Solution

200.1.1.2/24



200.1.2.1/24



200.1.2.2/24



n IP网内：直接交付 à 目的IP地址

n IP网间：间接交付 à 下一跳IP地址（路由器）

n 能通信： A→B → B , C→B → D

n 不能通信： IP网间 (因没有路由器)

4.3 Routing Methods

路由选择的方法

- n 两种策略: based on when and how the routes are discovered
 - n Proactive routing (先应式路由、主动路由)
 - n 特点: 预先获得目的地路由, 周期性地维护路由表。
 - n Table- driven routing (表驱动路由选择)
 - n Route table (路由表)
 - n Reactive routing (反应式路由选择、按需路由)
 - n 特点: 收到IP分组后才为其选路。路由表按需建立起来的, 当发现新的路由时才更新。
 - n On- demand routing

Table-Driven Routing

- n Idea

- n 使用尽可能少的信息实现选路

- n Information for routing

- n 可能的目的 à 目的网络，而非目的主机

- 节约路由表的存储空间，提高查表效率

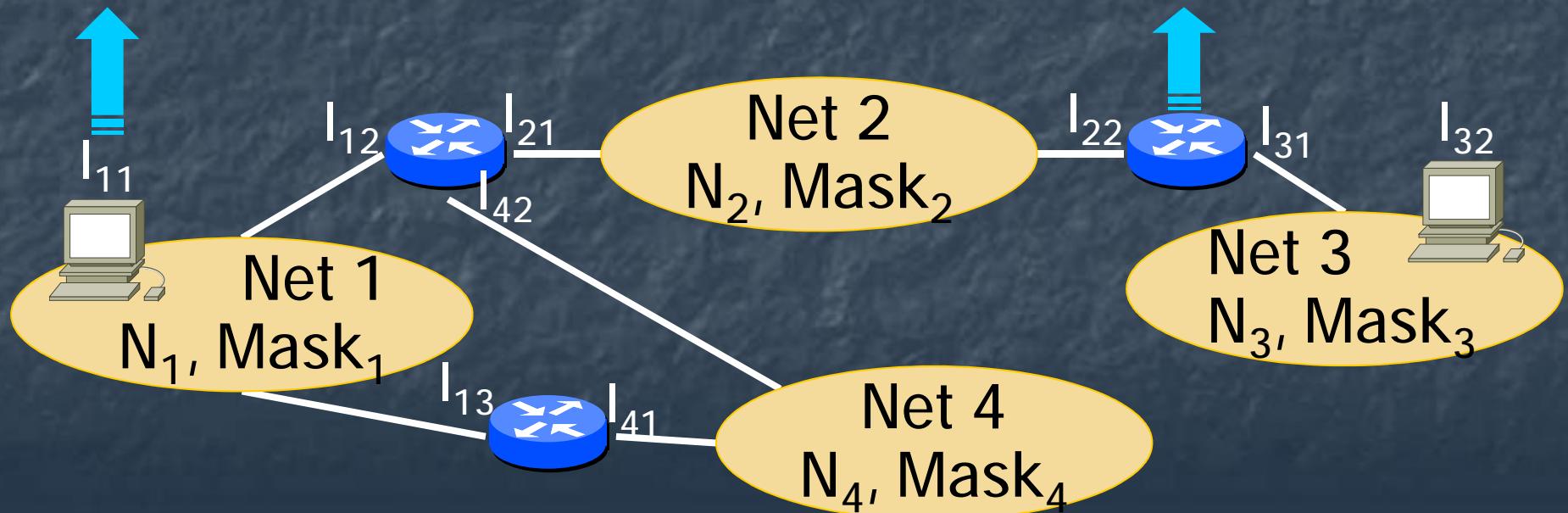
- n 如何到达目的 ?à Next-hop routing，而非完整路径

- 简化路由表，每个路由器独立选路

Example

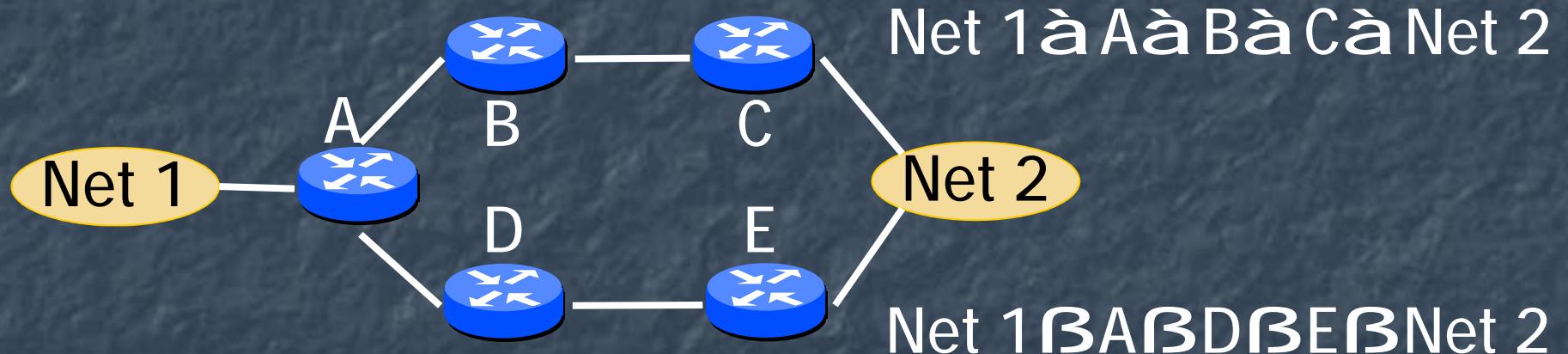
Dst. Network		Next-hop Address	发送接口
IP	Mask		
N_1	$Mask_1$	—	I_{11}
N_2	$Mask_2$	I_{12}	I_{11}
N_3	$Mask_3$	I_{12}	I_{11}
N_4	$Mask_4$	I_{13}	I_{11}

Dst. Network		Next-hop Address	发送接口
IP	Mask		
N_1	$Mask_1$	I_{21}	I_{22}
N_2	$Mask_2$	—	I_{22}
N_3	$Mask_3$	—	I_{31}
N_4	$Mask_4$	I_{21}	I_{22}



Discussion

- 路由表的大小只与网络的个数有关，与每个网络的大小（包含的主机数多少）无关
- 路由器独立选路，从Net 1到Net 2的路径可能与从Net 2到Net 1的路径不是同一条



只有最后一个路由器才知道目的主机是否存在。

Host-specific routing

特定主机路由

- 思想

- 为某台主机单独指定
路由

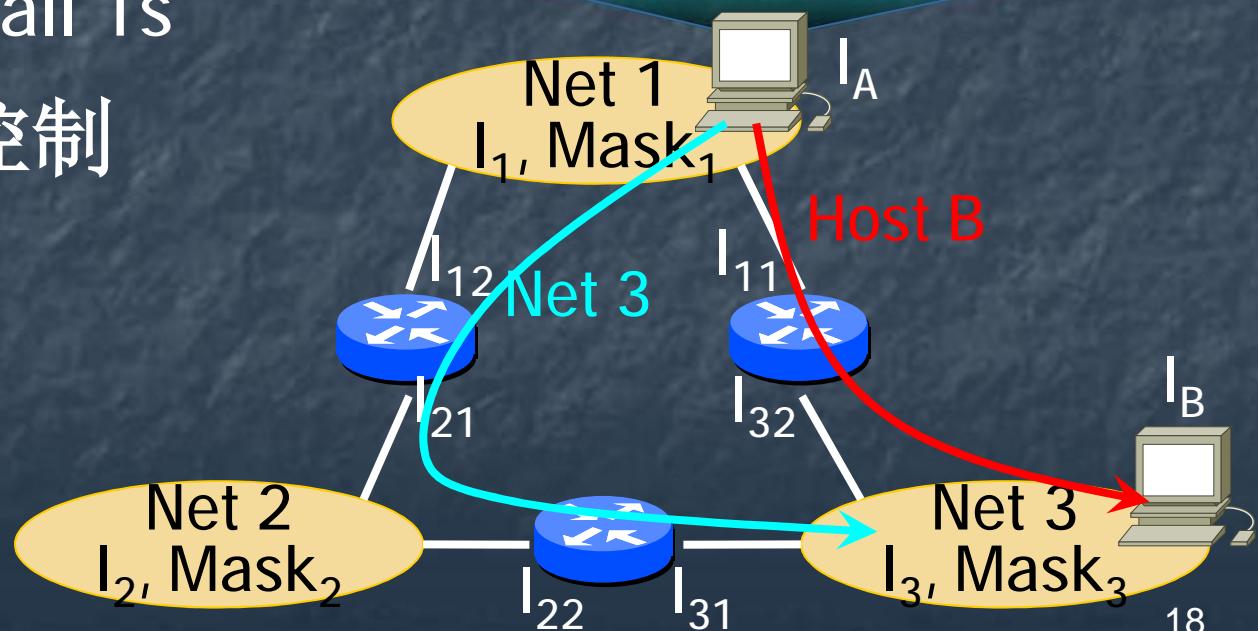
- 特点

- Host mask : all 1s

- 作用：更多控制

- 投递路径
- 安全

Dst. Network		Next-hop Address
IP	Mask	
I_1	$Mask_1$	—
I_B	/32	I_{11}
I_3	$Mask_3$	I_{12}



Default routing 默认路由

- n Idea

- n Use a default route if no entry for destination network in the routing table



区别于IP
Address

- n Feature

- n Destination network address = 0.0.0.0
 - n Destination network mask = 0.0.0.0

- n Function

- n Make the routing table smaller
 - n A lot of routing information is hidden

Example

n Host



Dst. Network		Next-hop Address
IP地址	Mask	
I_1	Mask_1	—
I_2	Mask_2	I_{12}
0.0.0.0	0.0.0.0	I_{13}

Default Router

n Router



Dst. Network		Next-hop Address
IP	Mask	
I_1	Mask_1	—
I_2	Mask_2	—
0.0.0.0	0.0.0.0	I_{13}

Example: a Host's Routing Table

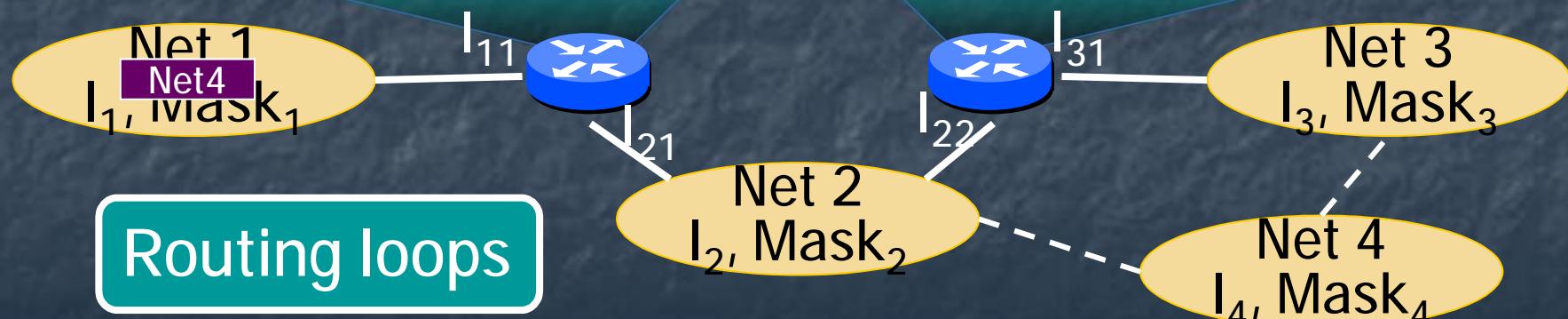
```
C:\>route print
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x2 ...00 02 2d 0b f2 bc ..... ORiNOCO Wireless LAN PC Card (5 volt)
=====
=====
Active Routes:
Network Destination      Netmask         Gateway       Interface Metric
          0.0.0.0        0.0.0.0   202.115.12.17  202.115.12.18    30
        127.0.0.0    255.0.0.0       127.0.0.1   127.0.0.1       1
  202.115.12.16  255.255.255.248  202.115.12.18  202.115.12.18    30
  202.115.12.18  255.255.255.255       127.0.0.1   127.0.0.1    30
  202.115.12.255 255.255.255.255       202.115.12.18  202.115.12.18    30
        224.0.0.0    240.0.0.0   202.115.12.18  202.115.12.18    30
  255.255.255.255 255.255.255.255       202.115.12.18  202.115.12.18       1
Default Gateway: 202.115.12.17
=====
Persistent Routes:
  None
```

思考

n 主机和路由器的默认路由设置

Dst. Network		Next-hop Address
IP	Mask	
I_1	$Mask_1$	—
I_2	$Mask_2$	—
0.0.0.0	/0	I_{22}

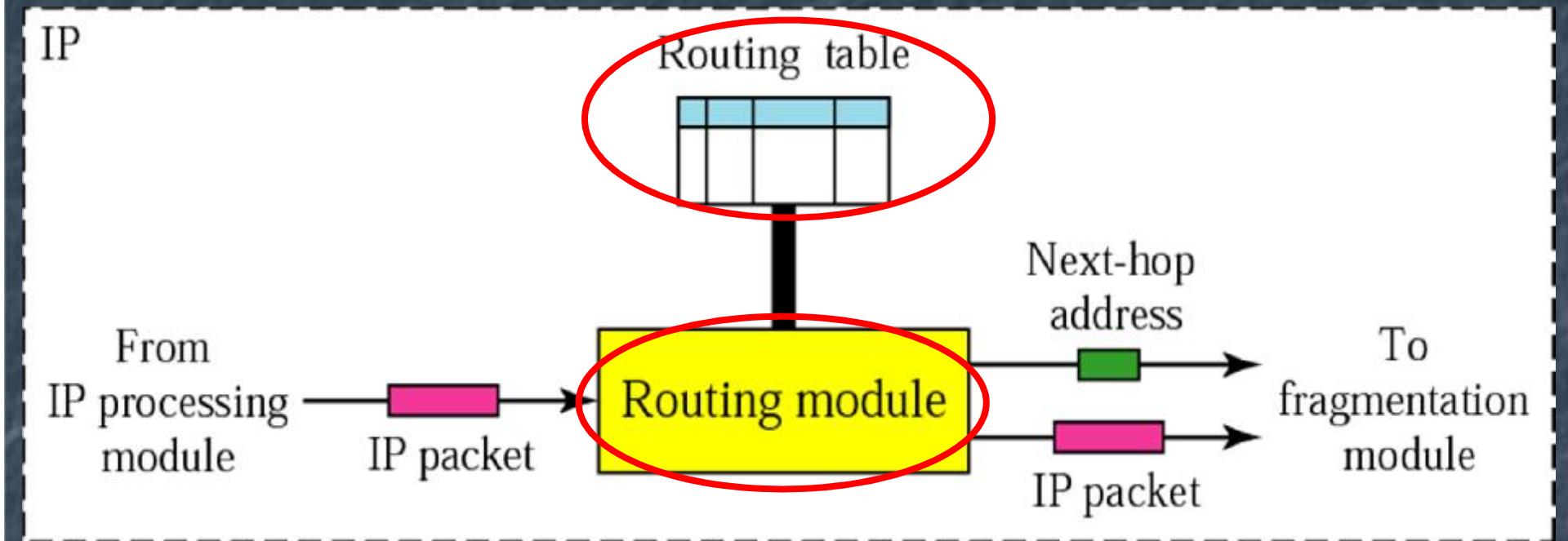
Dst. Network		Next-hop Address
IP	Mask	
I_2	$Mask_2$	—
I_3	$Mask_3$	—
0.0.0.0	/0	I_{21}



4.4 Static vs. Dynamic Routing

- n Static routing (静态路由选择)
 - n 管理员手工设置和更新
 - n 优点: 路由开销低, 安全性好, 可试验性
 - n 缺点: 维护困难, 灵活性差
- n Dynamic routing (动态路由选择)
 - n 由动态路由协议发现和更新路由
 - n 优点: 高灵活性和适应性, 低维护开销
 - n 缺点: 路由开销高

4.5 Routing Table and Routing Module



Policy:

$d\text{IP} \& \text{Mask}(i) = \text{Net}(i)$ the first one



直连路由

间接路由

最长匹配 (longest match)

Routing Table

n Forwarding table (转发表)

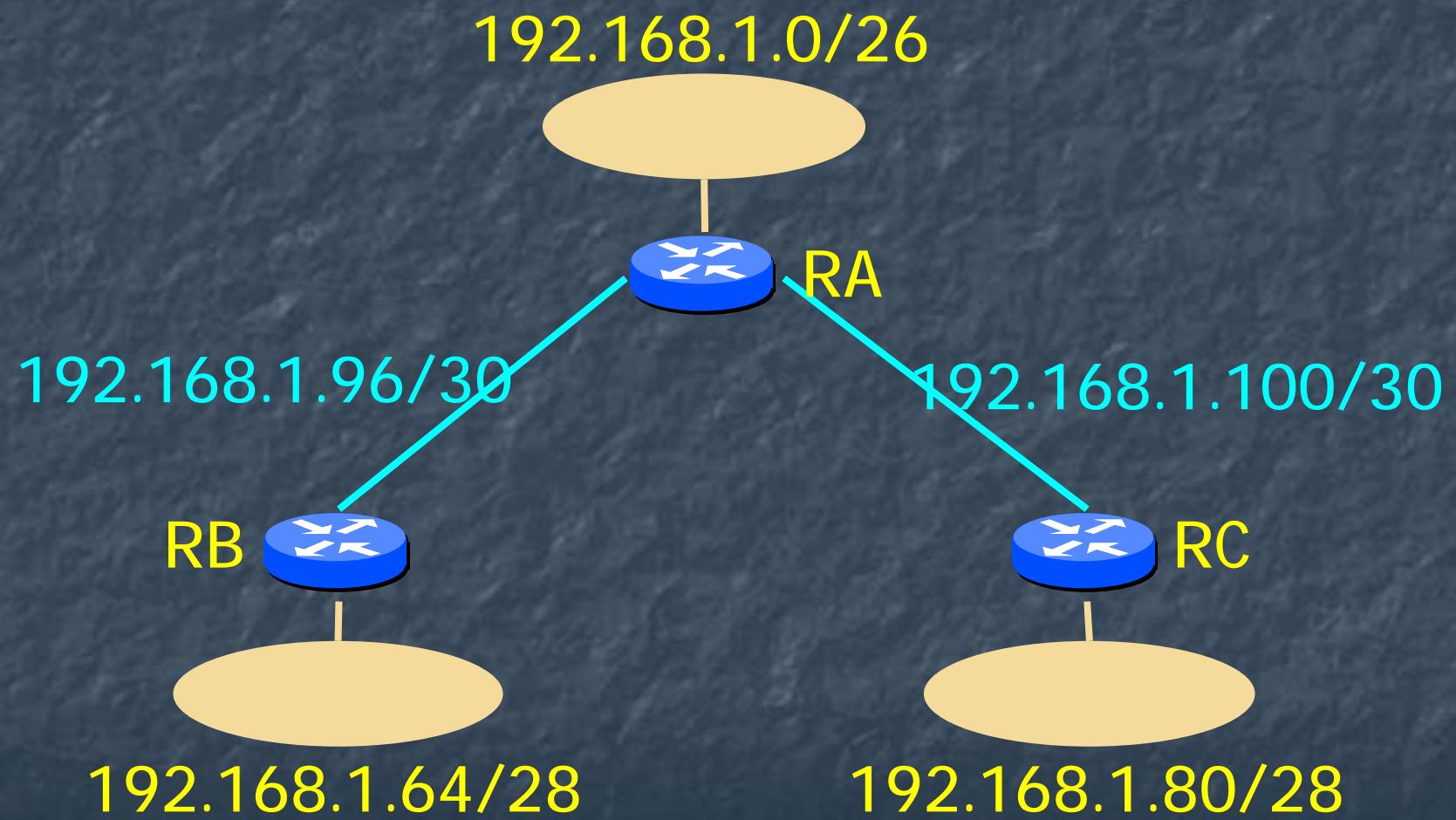
Mask	Destination address	Next-hop address	Flags	Reference count	Use	Interface
255.0.0.0	124.0.0.0	145.6.7.2	UG	4	20	m2
.....
.....

n Next-hop address

n Direct delivery: destination address

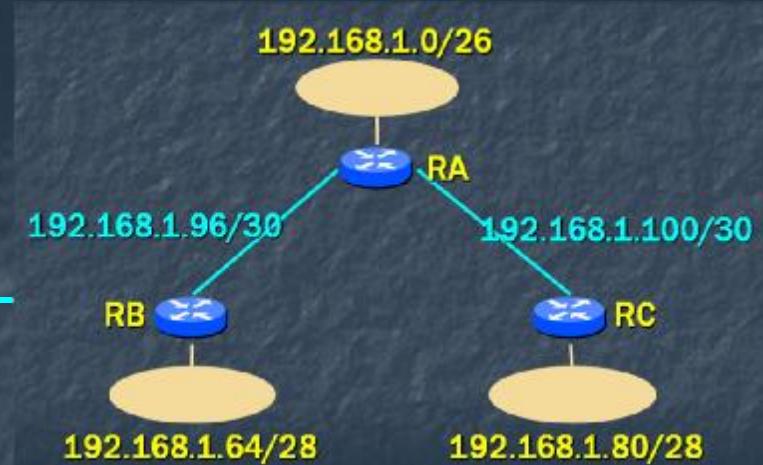
n Indirect delivery: next-hop address

Example 1



Routing Table of

RA# show ip route



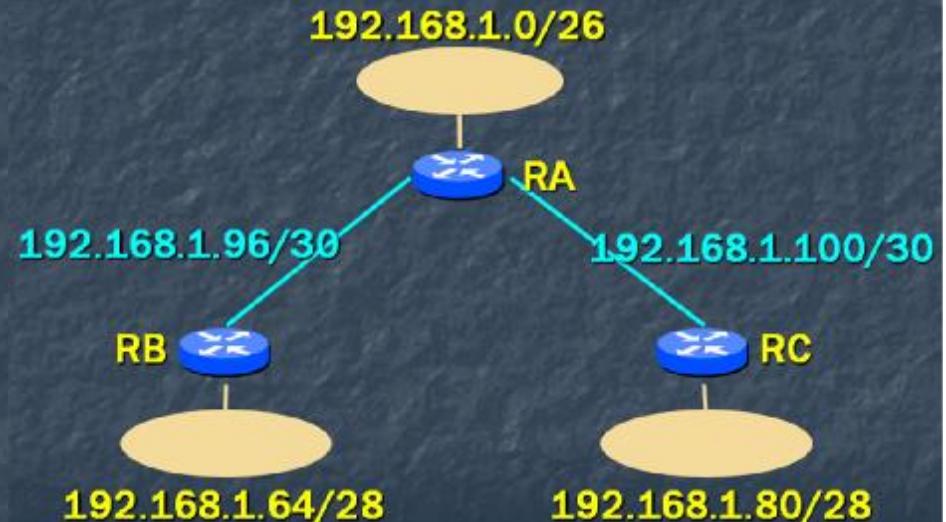
192.168.1.0/24 is variably subnetted, 6 subnets, 3 masks

- C 192.168.1.96/30 is directly connected, serial1
- C 192.168.1.100/30 is directly connected, serial0
- R 192.168.1.64/28 [120/1] via 192.168.1.97, serial1
- R 192.168.1.80/28 [120/1] via 192.168.1.102, serial0
- C 192.168.1.0/26 is directly connected, ethernet0

显示的顺序

Questions

- n 在RA的路由表中查找到达以下目的的路径
 - n 192.168.1.2
 - n 192.168.1.65
 - n 192.168.1.105



目的: 192.168.1.2

RA# show ip route

.....

192.168.1.0/24 is variably subnetted, 6 subnets, 3 masks

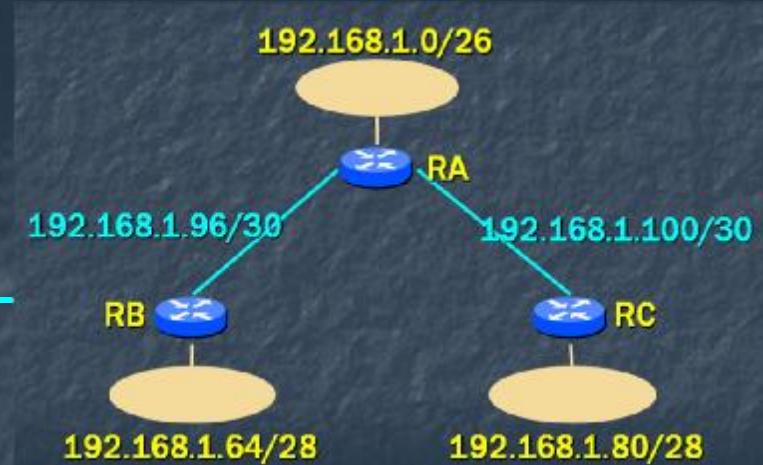
→C 192.168.1.96/30 is directly connected, serial1

→C 192.168.1.100/30 is directly connected, serial0

R 192.168.1.64/28 [120/1] via 192.168.1.97, serial1

R 192.168.1.80/28 [120/1] via 192.168.1.102, serial0

→C 192.168.1.0/26 is directly connected, ethernet0



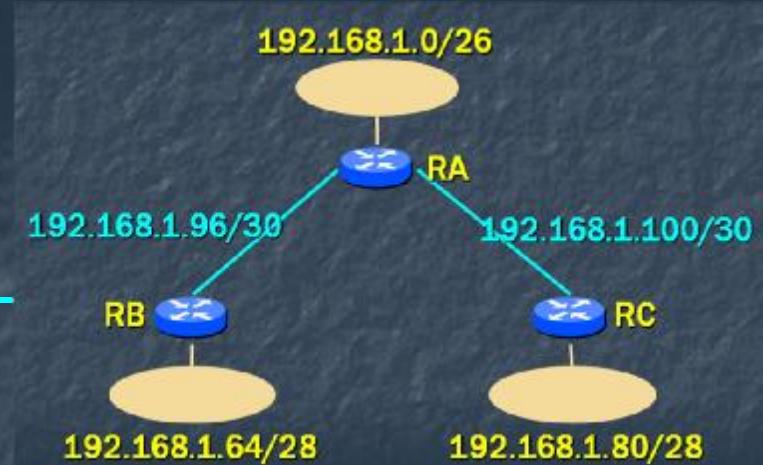
目的: 192.168.1.65

RA# show ip route

.....

192.168.1.0/24 is variably subnetted, 6 subnets, 3 masks

- C 192.168.1.96/30 is directly connected, serial1
- C 192.168.1.100/30 is directly connected, serial0
- R 192.168.1.64/28 [120/1] via 192.168.1.97, serial1
- R 192.168.1.80/28 [120/1] via 192.168.1.102, serial0
- C 192.168.1.0/26 is directly connected, ethernet0



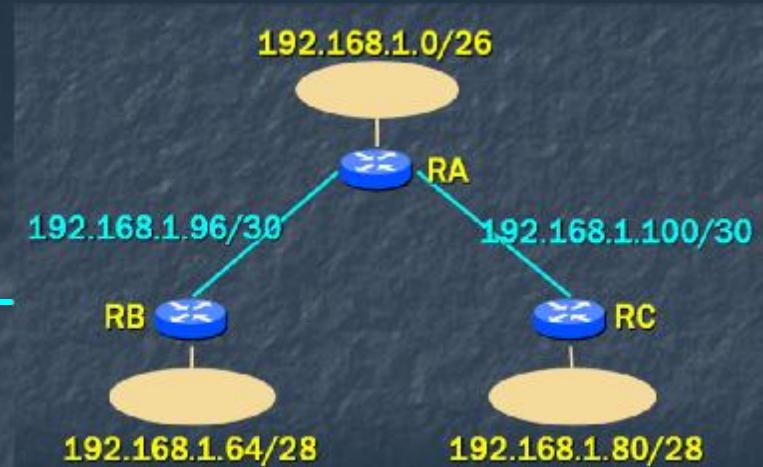
目的: 192.168.1.105

RA# show ip route

.....

192.168.1.0/24 is variably subnetted, 6 subnets, 3 masks

- C 192.168.1.96/30 is directly connected, serial1
- C 192.168.1.100/30 is directly connected, serial0
- R 192.168.1.64/28 [120/1] via 192.168.1.97, serial1
- R 192.168.1.80/28 [120/1] via 192.168.1.102, serial0
- C 192.168.1.0/26 is directly connected, ethernet0



没有匹配项，又没有默认路由，路由选择失败，发送ICMP差错报文

Example 2

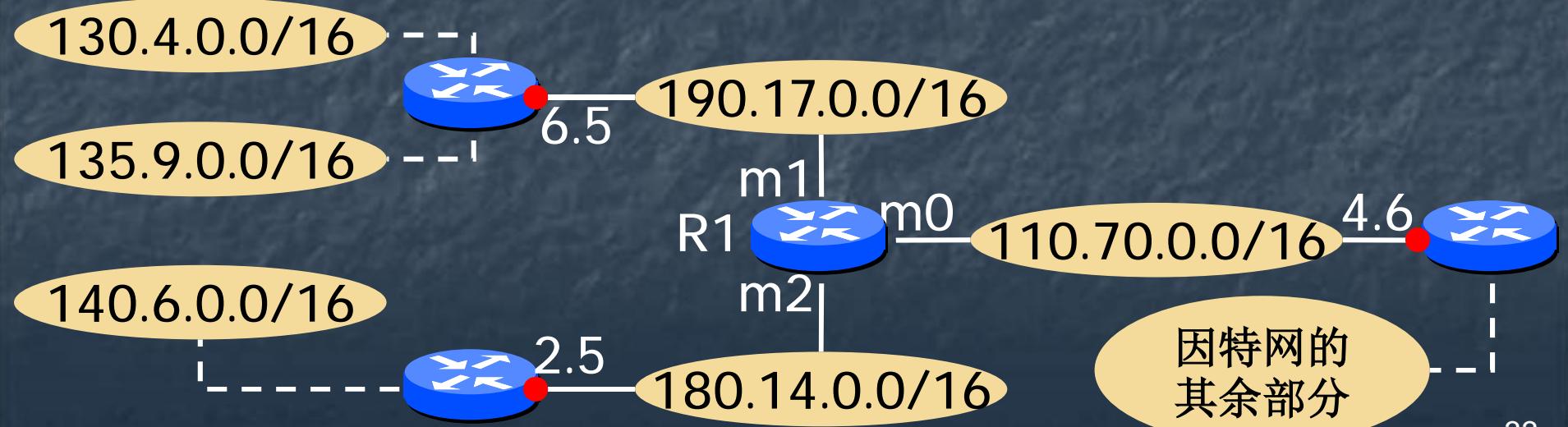
n 路由器R1的路由表如下：

Mask	Destination	Next Hop	Interface
255.255.0.0	110.70.0.0	--	m0
255.255.0.0	180.14.0.0	--	m2
255.255.0.0	190.17.0.0	--	m1
255.255.0.0	130.4.0.0	190.17.6.5	m1
255.255.0.0	135.9.0.0	190.17.6.5	m1
255.255.0.0	140.6.0.0	180.14.2.5	m2
0.0.0.0	0.0.0.0	110.70.4.6	m0

根据以上路由表画出网络拓扑图。

Solution

Mask	Destination	Next Hop	Interface
255.255.0.0	110.70.0.0	--	m0
255.255.0.0	180.14.0.0	--	m2
255.255.0.0	190.17.0.0	--	m1
255.255.0.0	130.4.0.0	190.17.6.5	m1
255.255.0.0	135.9.0.0	190.17.6.5	m1
255.255.0.0	140.6.0.0	180.14.2.5	m2
0.0.0.0	0.0.0.0	110.70.4.6	m0



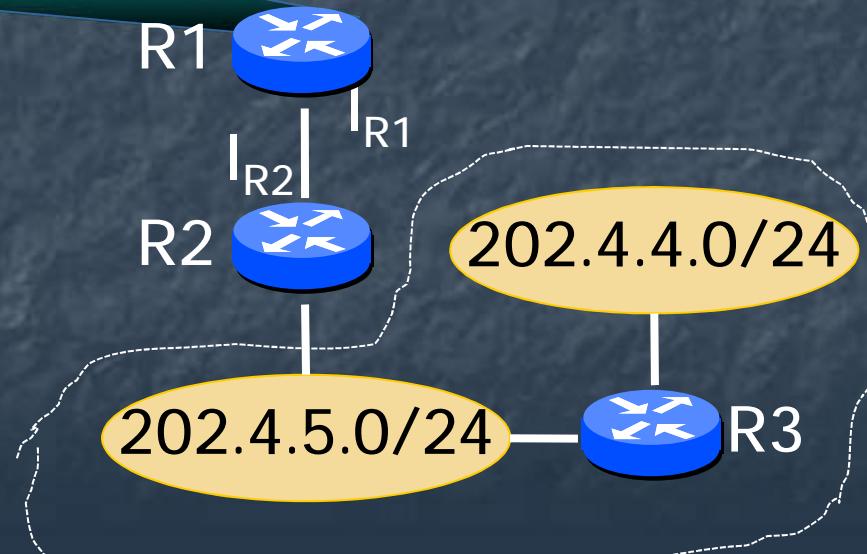
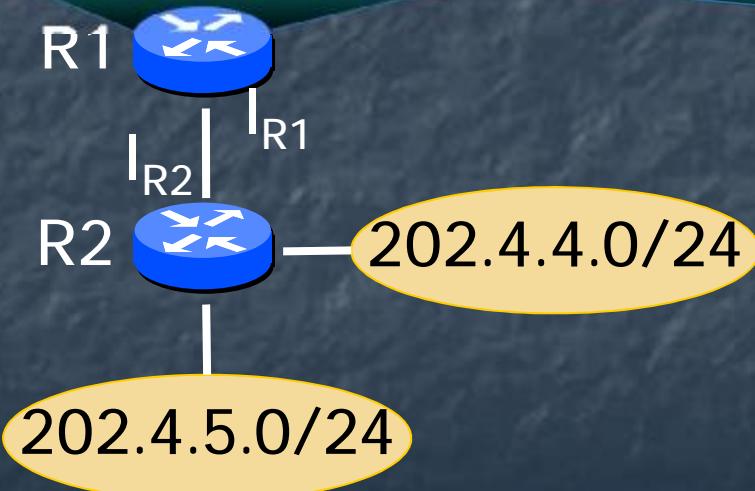
4.6 CIDR

- n Classless Inter-Domain Routing
 - n 无类别域间路由
 - n A routing technology, not a routing protocol
 - n RFC 1518, RFC 1519
 - n Function: reduce the size of the routing table
 - n Hierarchical and geographical routing
 - n 分层路由选择 和 区域路由选择
 - n Route aggregation (路由聚合)

Route Aggregation

Network/Mask	Next-hop
202.4.4.0	/24
I _{R2}	
202.4.5.0	/24
I _{R2}	

4: 0000010	0	4&254=4
5: 0000010	1	5&254=4
254: 1111111	0	
202.4.4.0 /23		I _{R2} I _{R1}



聚合应用

- 合理的IP地址规划

- 有效减少关键路由器选路表项，充分发挥路由器的转发性能

- 隐藏网络结构

- 自主管理网络边界使用路由器（即R2）与外界相连，在不改变原有IP地址范围的条件下，网络内部任意划分子网、改变拓扑结构等，都不会影响外部的路由器（即R1）选路表项。



第一部分小结：内容

- n 交付、路由选择
- n 面向连接、无连接协议
- n IP协议
 - n 不可靠、无连接、数据报交付协议
- n 直接交付、间接交付：地址映射
- n 路由表：作用、内容、查找规则
- n 路由类型
 - n 网络拓扑：直连路由、非直连路由
 - n 目的范围：主机路由、网络路由、默认路由
 - n 获得方式：静态路由、动态路由

第一部分小结: 应用

- n 根据网络拓扑或分组的源、目的IP地址
 - n 判断直接交付和间接交付
- n 根据路由表
 - n 查找到达给定目的的路径
- n 路由聚合

第二部分 IP数据包格式

nDatagram

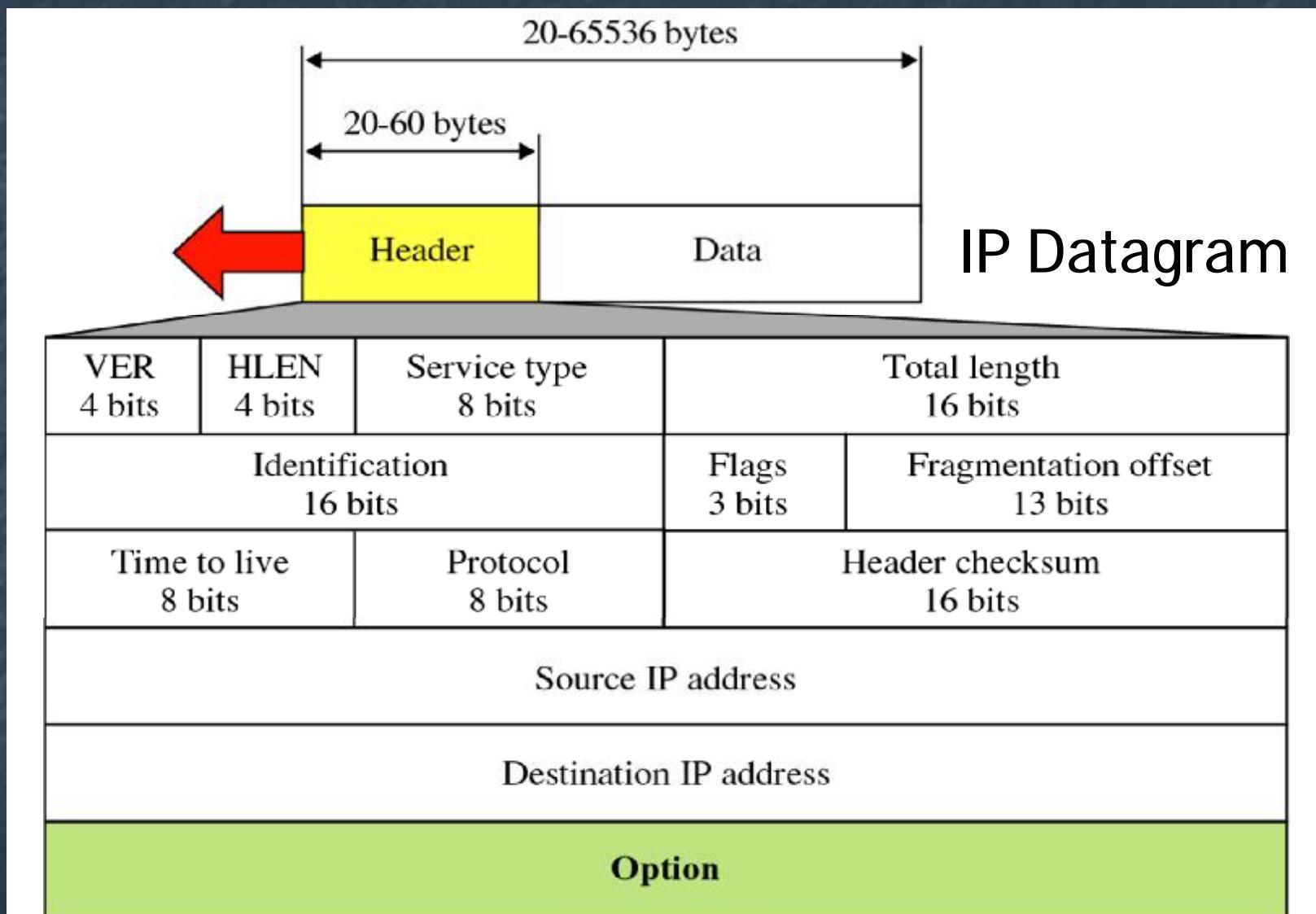
nFragmentation

nOptions

nChecksum

nIP package

4.1 Datagram



版本字段

VER 4 bits	HLEN 4 bits	Service type 8 bits	Total length 16 bits						
Identification 16 bits		Flags 3 bits	Fragmentation offset 13 bits						
Time to live 8 bits	Protocol 8 bits	Header checksum 16 bits							
Source IP address									
Destination IP address									

- VER: 4 bits, 指 IP 协议的版本
- 目前的 IP 协议版本号为 4 (即 IPv4)

首部长度字段

VER 4 bits	HLEN 4 bits	Service type 8 bits	Total length 16 bits						
Identification 16 bits		Flags 3 bits	Fragmentation offset 13 bits						
Time to live 8 bits	Protocol 8 bits	Header checksum 16 bits							
Source IP address									
Destination IP address									

n HLEN: 4 bits

 n 以4字节（即32bits）为单位

 n 取值: 5 ~ 15 (即首部长度为 20 ~ 60 bytes)

服务类型字段

VER 4 bits	HLEN 4 bits	Service type 8 bits	Total length 16 bits
Identification 16 bits		Flags 3 bits	Fragmentation offset 13 bits
Time to live 8 bits	Protocol 8 bits	Header checksum 16 bits	
Source IP address			
Destination IP address			

- Service type: 8 bits
 - 该分组所期望的服务质量

Type of Service Field



总长度字段

VER 4 bits	HLEN 4 bits	Service type 8 bits	Total length 16 bits						
Identification 16 bits		Flags 3 bits	Fragmentation offset 13 bits						
Time to live 8 bits	Protocol 8 bits	Header checksum 16 bits							
Source IP address									
Destination IP address									

- Total length (总长度字段) : 16 bits
 - 以字节为单位
 - 首部长度 (即 $4 \times HLEN$) + 数据长度

思考: IP分组的最大长度是多少?

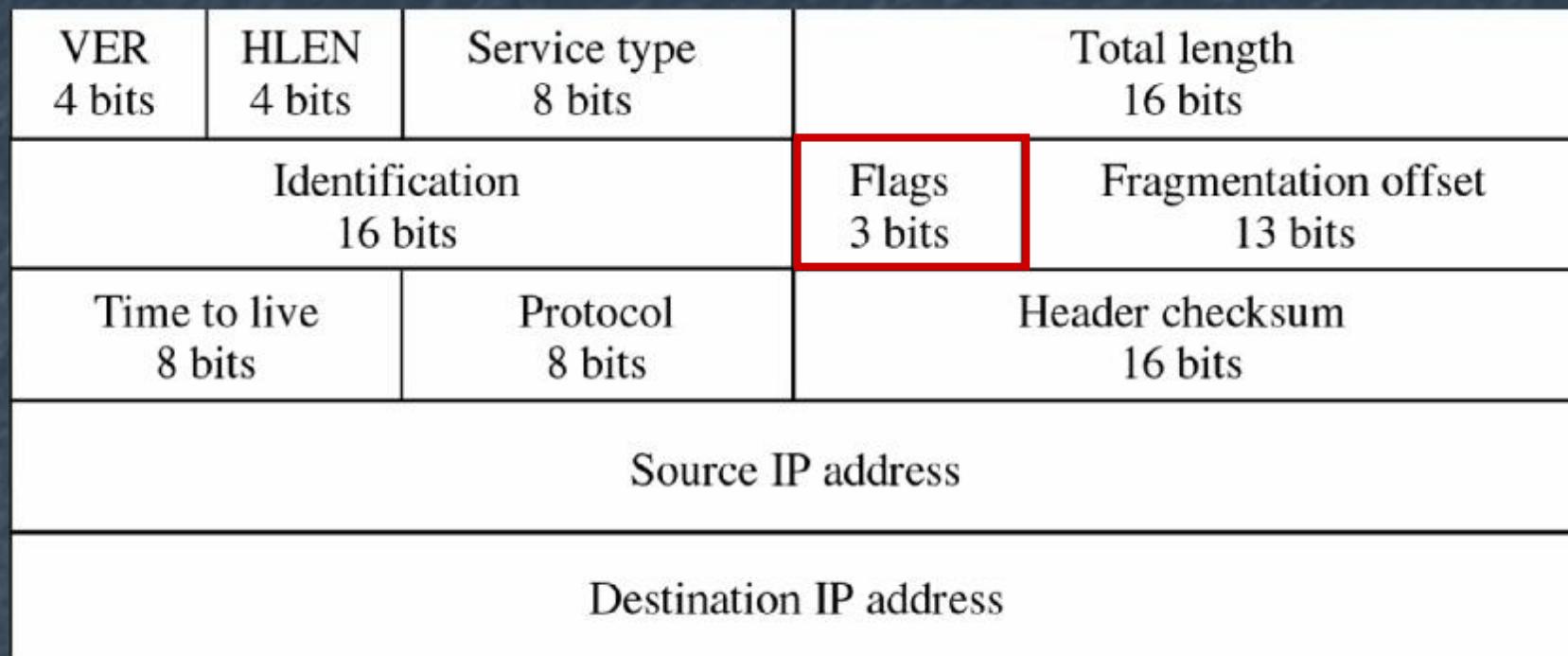
65535

标识字段

VER 4 bits	HLEN 4 bits	Service type 8 bits	Total length 16 bits									
Identification 16 bits			Flags 3 bits	Fragmentation offset 13 bits								
Time to live 8 bits	Protocol 8 bits		Header checksum 16 bits									
Source IP address												
Destination IP address												

- Identification (标识字段) : 16 bits
 - 源站每发送一个分组，标识值+1
 - (源IP地址, 标识) à 全网唯一分组标识

标志字段



n Flags (标志字段) : 3 bits

Flags



D: Do not fragment
M: More fragments

标志字段

Flags



D: Do not fragment
M: More fragments

- 1: 不分片
- 0: 在需要时可以分片

- 1: 不是最后的分片, 后面还有更多的分片
- 0: 后面没有分片
若片偏移字段值:
 - 大于0: 表示是最后的分片
 - 为0: 唯一的分片, 即没有分片

片偏移字段

VER 4 bits	HLEN 4 bits	Service type 8 bits	Total length 16 bits
Identification 16 bits		Flags 3 bits	Fragmentation offset 13 bits
Time to live 8 bits	Protocol 8 bits	Header checksum 16 bits	
Source IP address			
Destination IP address			

- Fragmentation offset (片偏移字段) : 13 bits
 - 以8 bytes为单位

思考：IP数据报为什么需要被分片？

生存时间字段

VER 4 bits	HLEN 4 bits	Service type 8 bits	Total length 16 bits						
Identification 16 bits		Flags 3 bits	Fragmentation offset 13 bits						
Time to live 8 bits	Protocol 8 bits	Header checksum 16 bits							
Source IP address									
Destination IP address									

n TTL（生存时间）：8 bits

Time to Live Field

- TTL（生存时间）：8 bits
 - 分组的寿命：防止路由成环或网络故障时无限时存在
 - 取值：分组传输时间+路由器转发处理时间 → 困难
 - 实际：源和目的之间的路由器个数（跳数）
 - 路由器转发时将 TTL值减1，TTL值为零时丢弃该分组

```
C:\>ping 202.112.14.151
```

```
Pinging 202.112.14.151 with 32 bytes of data:
```

```
Reply from 202.112.14.151: bytes=32 time=2ms TTL=252
```



```
Ping statistics for 202.112.14.151:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

Time to Live Field

■ TTL（生存时间）：8 bits

不同操作系统默认的TTL值（单位：秒）：

- Unix : 255
- Linux : 64
- Windows 9x/Me : 32
- Windows 200x /NT/XP : 128
- Windows7: 64

思考：

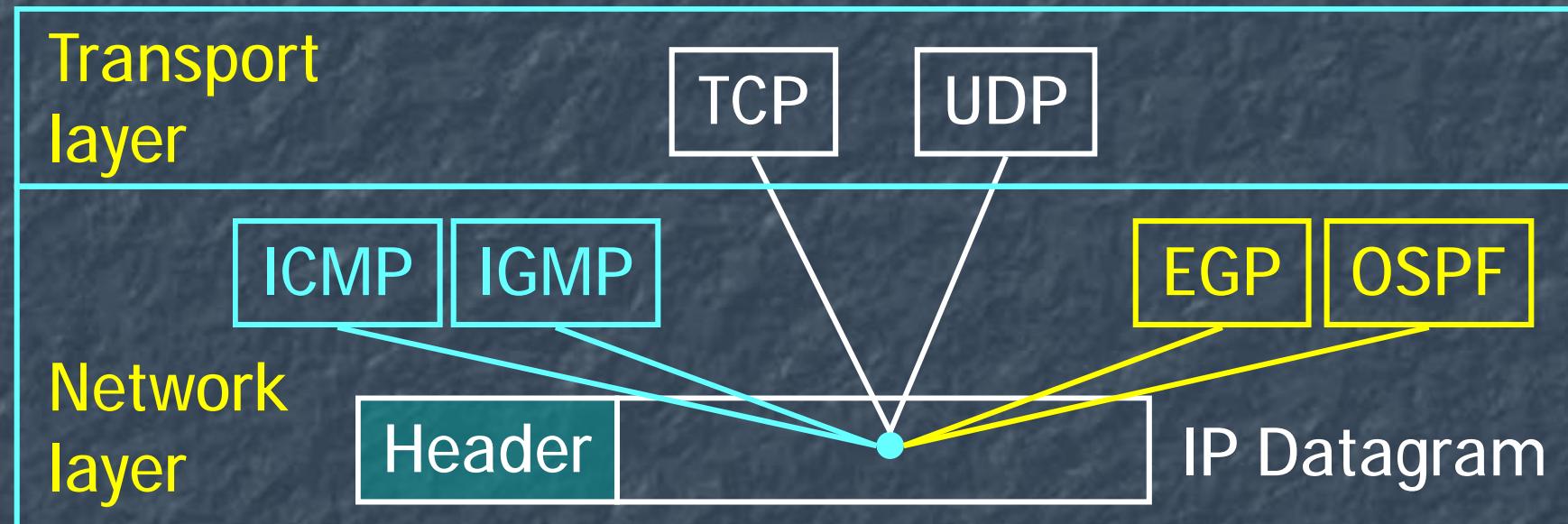
1. 若某路由器收到一个TTL为 1 的IP数据报，且目的IP非直连，则该路由器应将它_____。
A) 转发 B) 丢弃
2. 若某目的主机收到一个TTL为 0 的IP数据报，则该主机应将它_____。
A) 接受 B) 丢弃

协议字段

VER 4 bits	HLEN 4 bits	Service type 8 bits	Total length 16 bits					
Identification 16 bits		Flags 3 bits		Fragmentation offset 13 bits				
Time to live 8 bits	Protocol 8 bits		Header checksum 16 bits					
Source IP address								
Destination IP address								

- 协议: 8 bits
- 使用IP服务的高层协议

Protocol Field

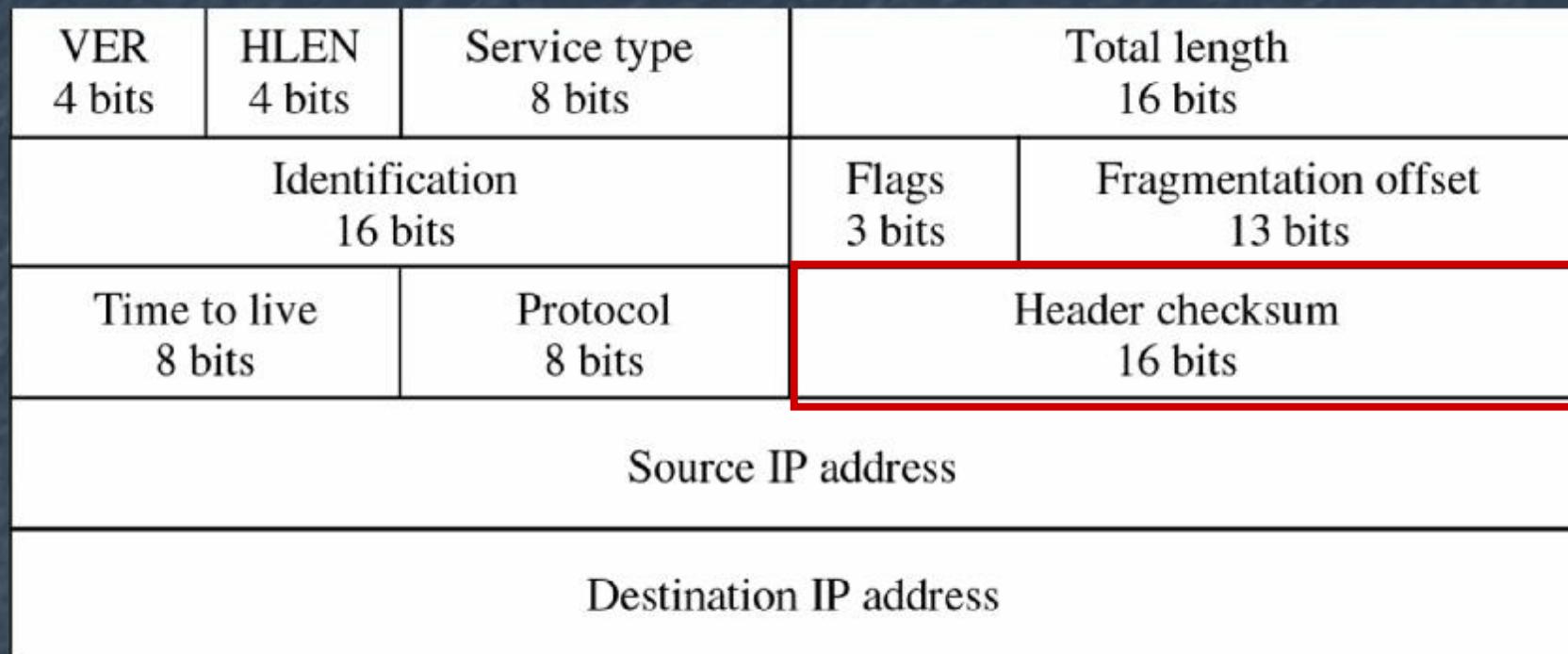


校验和字段

VER 4 bits	HLEN 4 bits	Service type 8 bits	Total length 16 bits	
Identification 16 bits		Flags 3 bits	Fragmentation offset 13 bits	
Time to live 8 bits	Protocol 8 bits	Header checksum 16 bits		
Source IP address				
Destination IP address				

- n 校验和: 16 bits
- n 差错检测

校验和字段



- 只校验首部，数据部分由高层协议校验
 - 无须重复校验数据部分
 - 缩短了路由器转发分组时的处理时间

校验和字段

VER 4 bits	HLEN 4 bits	Service type 8 bits	Total length 16 bits	
Identification 16 bits		Flags 3 bits	Fragmentation offset 13 bits	
Time to live 8 bits	Protocol 8 bits	Header checksum 16 bits		
Source IP address				
Destination IP address				

『 源IP地址， 32字节，在传递过程中始终保持不变』

校验和字段

VER 4 bits	HLEN 4 bits	Service type 8 bits	Total length 16 bits			
Identification 16 bits		Flags 3 bits	Fragmentation offset 13 bits			
Time to live 8 bits	Protocol 8 bits	Header checksum 16 bits				
Source IP address						
Destination IP address						

n 目的IP地址，32字节，在传递过程中始终保持不变

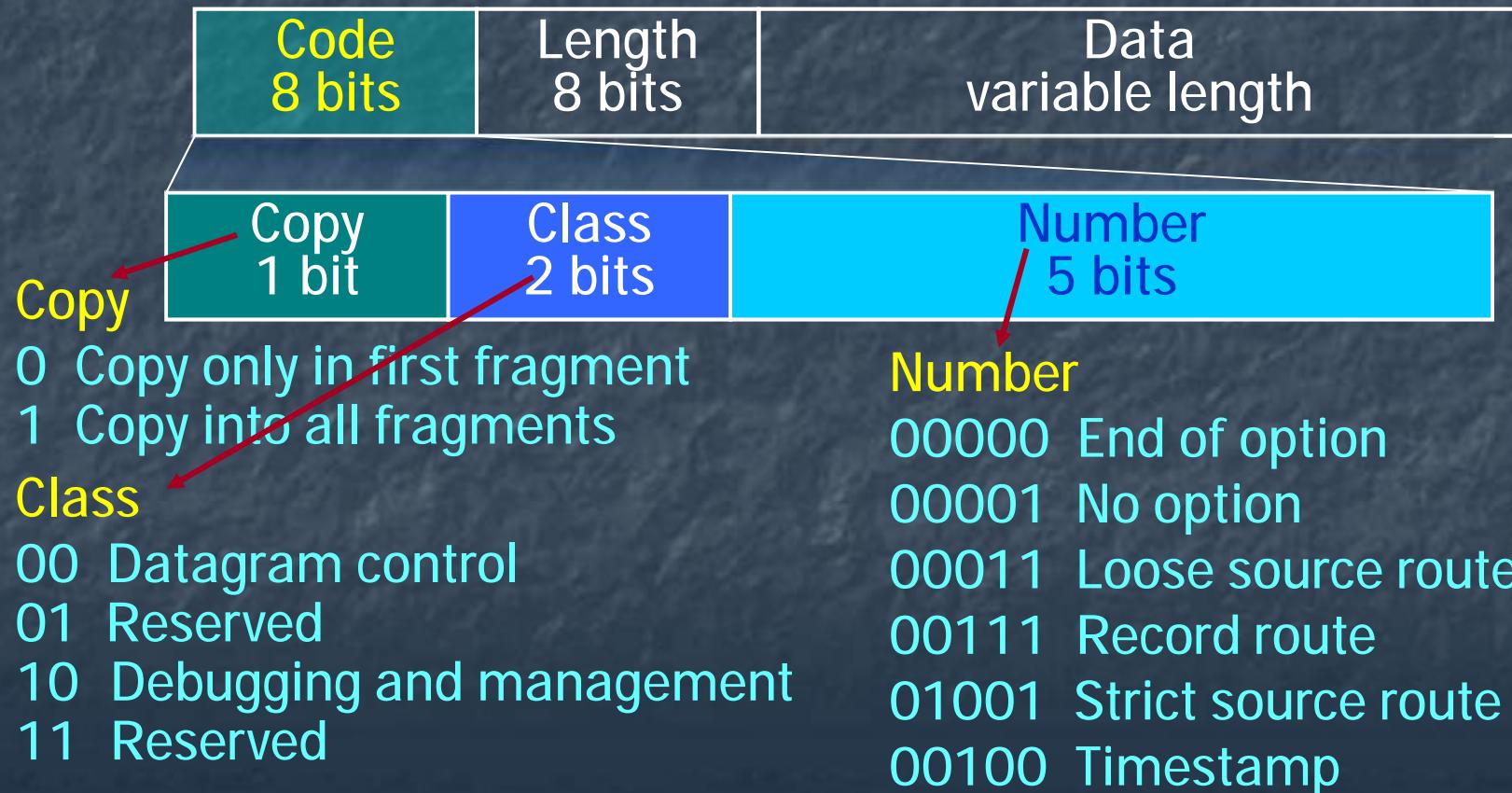
可选项字段

VER 4 bits	HLEN 4 bits	Service type 8 bits	Total length 16 bits						
Identification 16 bits		Flags 3 bits	Fragmentation offset 13 bits						
Time to live 8 bits	Protocol 8 bits	Header checksum 16 bits							
Source IP address									
Destination IP address									
Option									

- Option (选项): 0 ~ 40 bytes

Option Field

- 选项: 0 ~ 40 bytes
 - 网络测试或调试
 - 不是IP分组的必需部分，但其处理是IP软件的必需部分



IP数据报的封装

■ Example: Ethernet fram



Ethernet frame header

IP header

IP data

IP Datagram Example

```
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP:     000. .... = routine
IP:     ...0 .... = normal delay
IP:     .... 0... = normal throughput
IP:     .... .0.. = normal reliability
IP:     .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP:     .... ...0 = CE bit - no congestion
IP: Total length      = 60 bytes
IP: Identification    = 22984
IP: Flags            = 4X
IP:     .1... .... = don't fragment
IP:     ..0. .... = last fragment
IP: Fragment offset  = 0 bytes
IP: Time to live     = 63 seconds/hops
IP: Protocol         = 6 (TCP)
IP: Header checksum  = 34C9 (correct)
IP: Source address   = [202.115.12.6]
IP: Destination address = [202.115.12.62]
IP: No options
IP:

000000000: 00 90 27 1a 67 e7 00 90 27 a7 98 41 08 00 45 00 .? .q?? A.. E.
000000010: 00 3c 59 c8 40 00 3f 06 34 c9 ca 73 0c 06 ca 73 .<Y漢.?.4墒s.單
000000020: 0c 3e 94 69 05 99 55 85 24 5c 00 00 00 00 a0 02 .>擅.櫻?\....?
000000030: 16 d0 f2 65 00 00 02 04 05 b4 04 02 08 0a 00 2e 序e....?....
000000040: 7d 94 00 00 00 00 01 03 03 00 }?..... 2
```

思考题

n 1. 目的主机收到一个IP分组，其前 8 位为
 01000010_2 ，目的主机丢弃了该分组。为什么？

首部长度: 0010, 即 2 , $2 \times 4 = 8$ (Byte) , 错误!

n 2. 某IP分组中，HLEN的值是二进制的 1000。请问
该分组携带了多少个字节的选项？

首部长度: 1000, 即 8 , $8 \times 4 = 32$, $32 - 20 = 12$ (Byte)

n 3. 某IP分组中，HLEN的值是 5_{16} ，总长度字段的值
是 0028_{16} 。请问该分组携带了多少字节的数据？

首部长度: 5, $5 \times 4 = 20$ (Byte) , 总长度: $2 \times 16 + 8 = 40$ (Byte)

数据部分长度: $40 - 20 = 20$ (Byte)

IP分组处理

- n 合法性检查
 - n 版本
 - n 长度
 - n TTL
 - n Protocol
 - n Checksum
 - n IP地址
- n 分片与重组
- n 选项处理（自学）

4.2 Fragmentation 分片

- 适应在不同 MTU (最大传输单元) 的物理网中传输

Datagram

IP datagram

Frame Header

MTU

Trailer

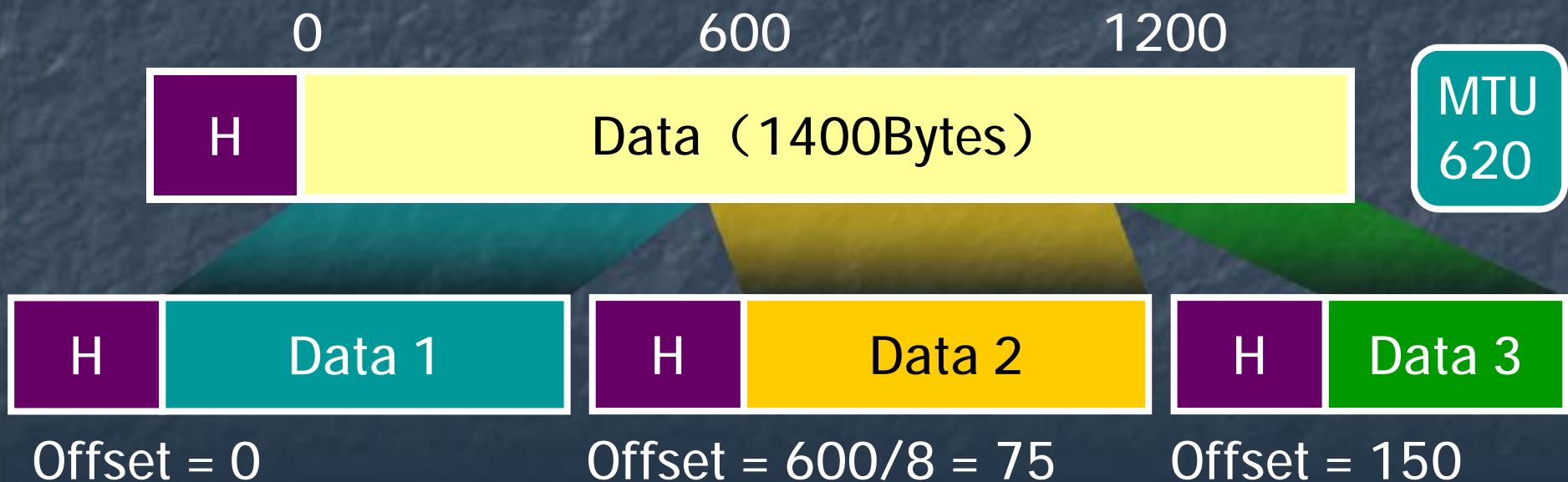
数据帧中封装的最大数据长度

Physical Network	MTU
Token ring (16 Mbps)	17914
Token ring (4 Mbps)	4464
FDDI	4352
Ethernet	1500
X.25	576
PPP	296

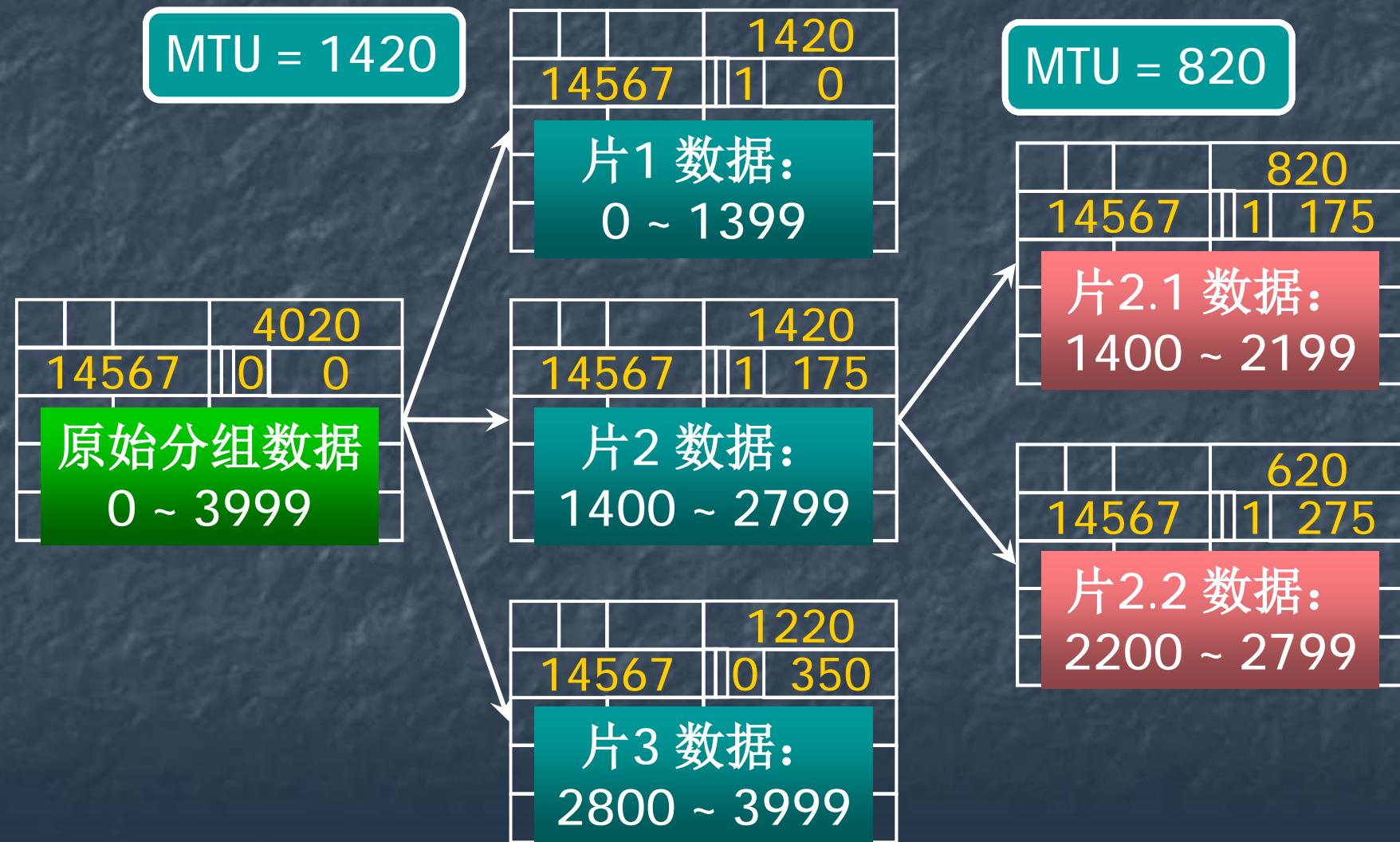
Fragmentation Operation

分片操作

- 只有源主机和路由器才能分片
- 只有在确实需要时才分片
- 一个数据报可以被分片多次
- 每个分片都要包含IP首部：无连接通信

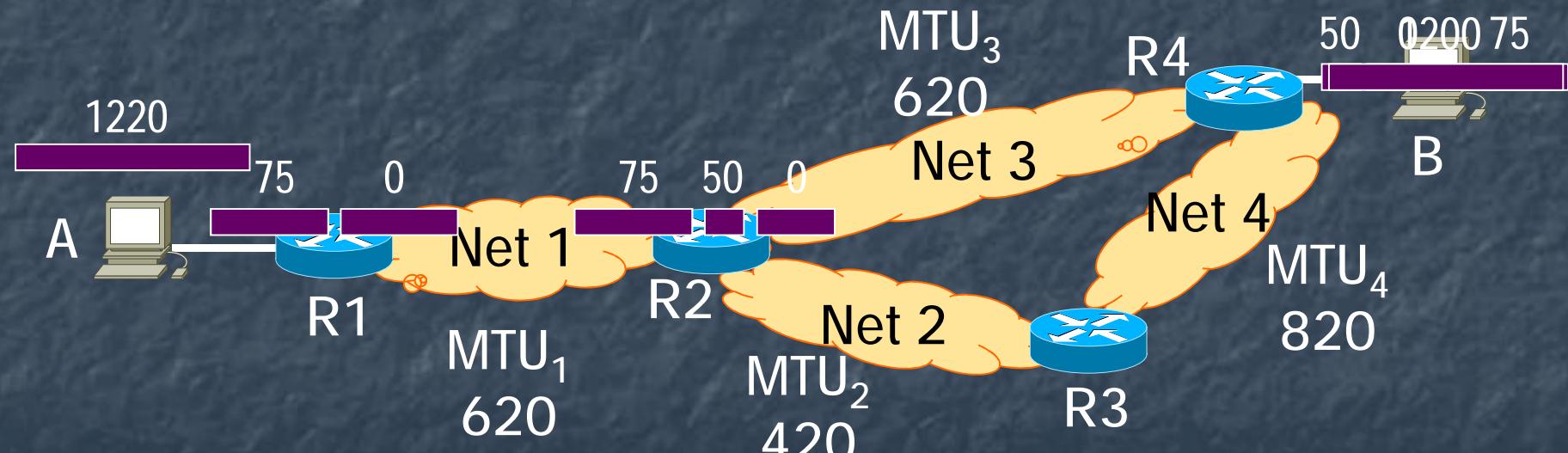


Fragmentation Example



Reassembly (重组操作)

- 仅由目的主机执行：在将数据递交到上层时
 - 只有在收到所有的分片后才能执行重组
 - Connectionless → 各分片的传输路径可不同
 - 重组超时，或分片丢失，则不将重组IP分组



§ 目的主机能区分和重组不同的源IP报文（源IP地址，标识）

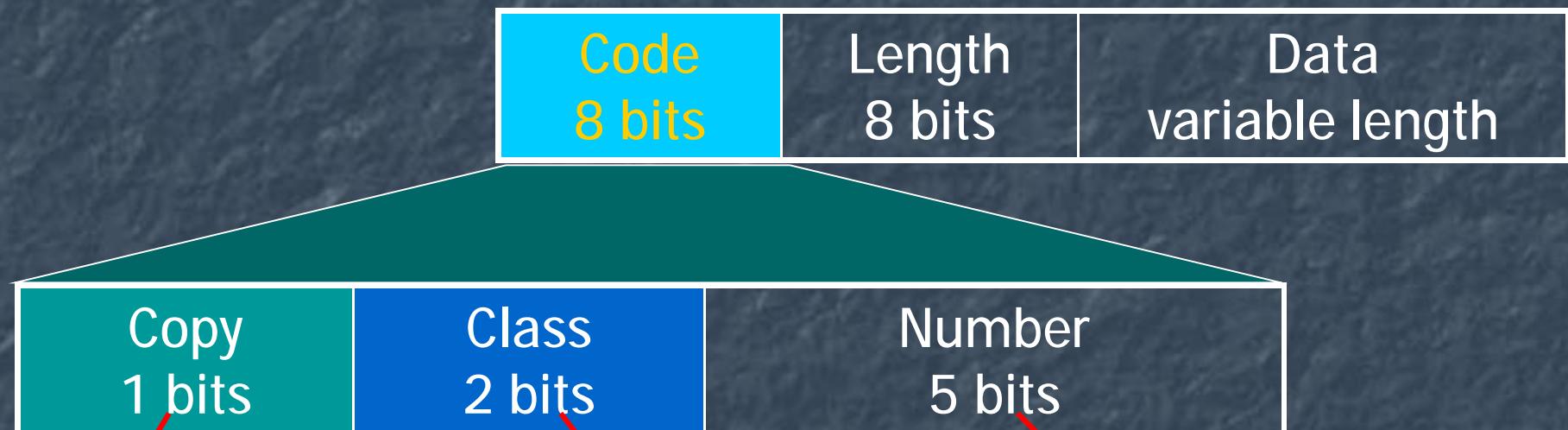
4.3 Options (选项)

VER 4 bits	HLEN 4 bits	Service type 8 bits	Total length 16 bits						
Identification 16 bits		Flags 3 bits	Fragmentation offset 13 bits						
Time to live 8 bits	Protocol 8 bits	Header checksum 16 bits							
Source IP address									
Destination IP address									
Option									

- Option: 0~40 bits
 - 用于数据报的控制、排错或测试

4.3 Options (选项)

n 格式



Copy

0: 选项仅复制到第一个分片中

1: 选项被复制到所有分片

Class

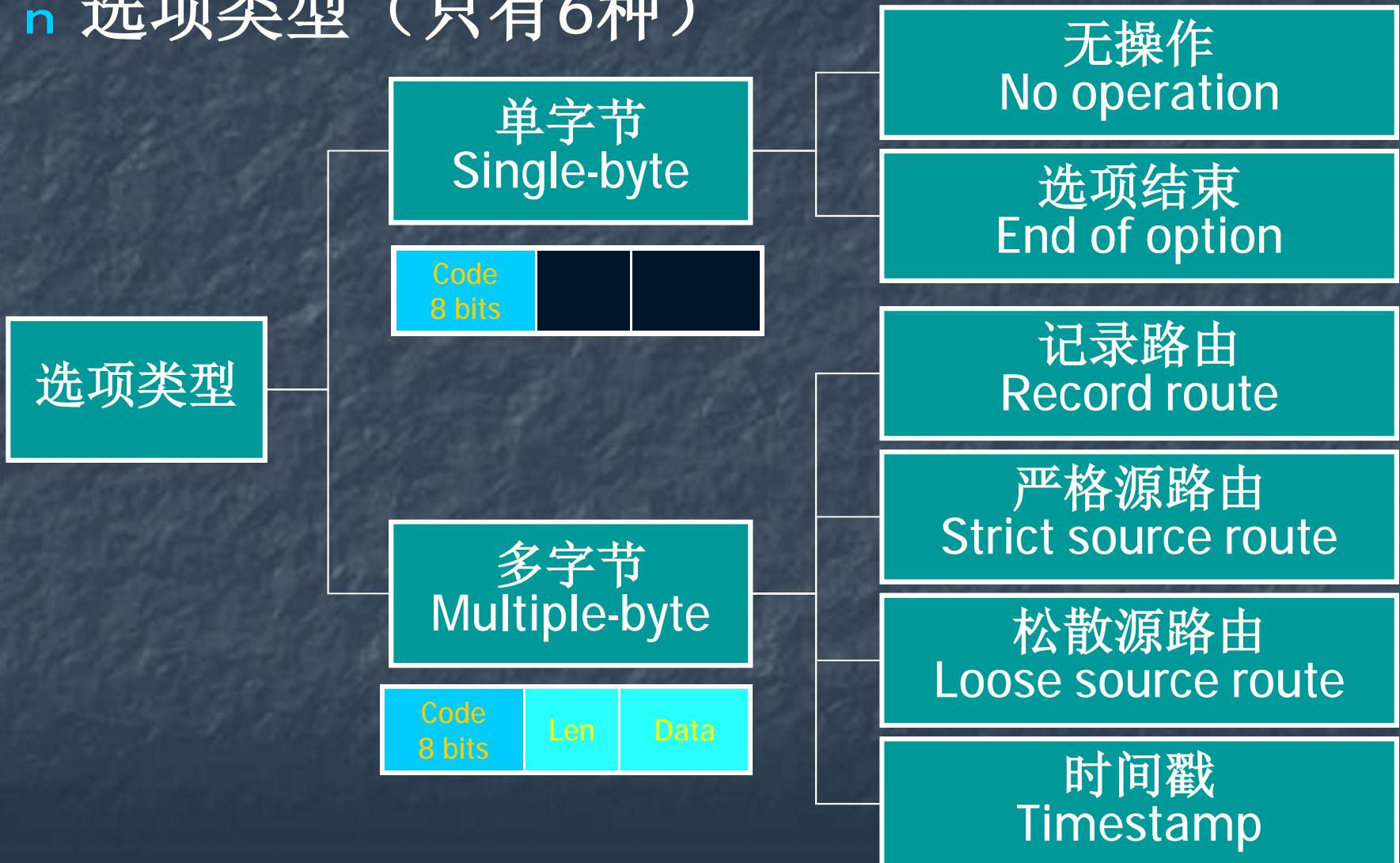
00: 数据报控制
10: 调试和管理

Number

选项类型编码
如 01001 : 严格路由

4.3 Options (选项)

n 选项类型（只有6种）



Fragmentation with Options

- 哪些选项会复制到所有分片中？哪些只在第一个分片中出现？
- 哪些选项用于数据报控制？哪些选项用于调试管理？

No operation	0	00	00001	No copy	Control
End of option	0	00	00000	No copy	Control
Record route	0	00	00111	No copy	Control
Strict source route	1	00	01001	Copy	Control
Loose source route	1	00	00011	Copy	Control
Timestamp	0	10	00100	No copy	Debug

源路由选项

选项编码：

00000 选项结束

00001 无操作

00011 松散源路由

00111 记录路由

01001 严格源路由

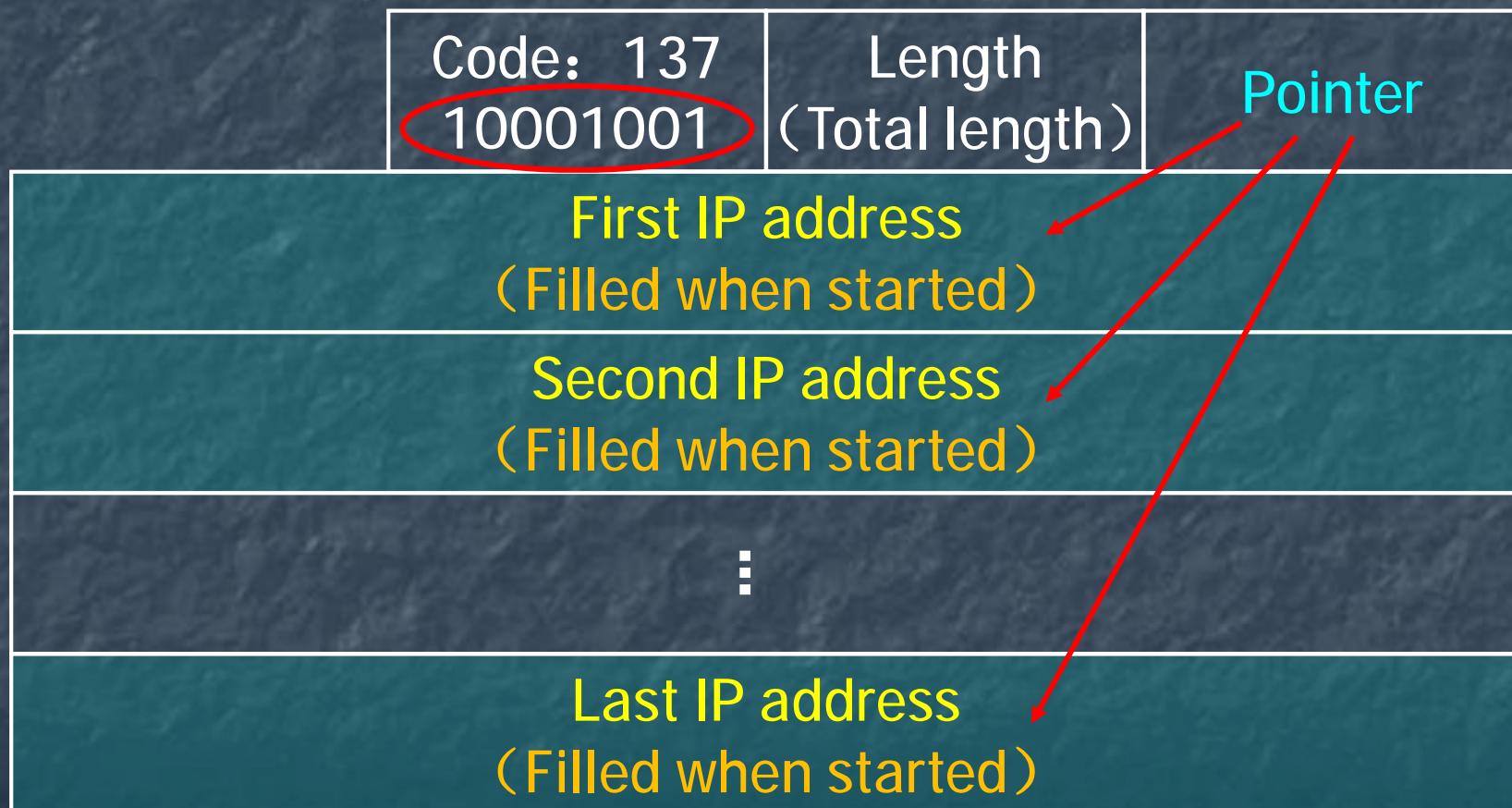
00100 时间戳

- 要求IP数据报在传输过程中，必须经过源主机指定的路由器，且顺序不能颠倒。
- 可以经过没有指定的其它路由器

- 要求IP数据报在传输过程中，必须经过源主机指定的路由器，且顺序不能颠倒。
- 不能经过没有指定的其它路由器

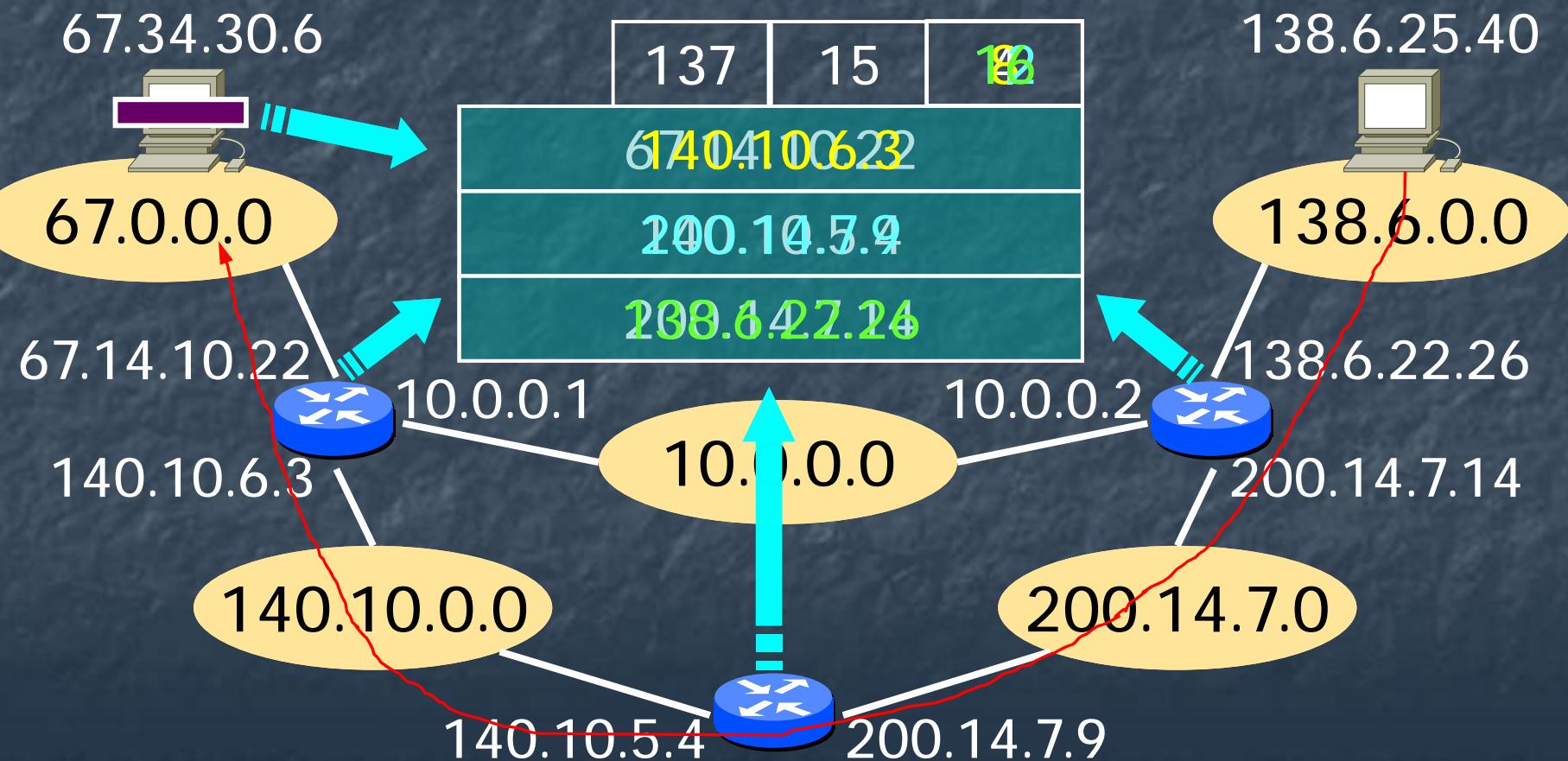
严格源路由选项

n 格式



严格源路由示例

- 严格按给定的IP地址逐跳转发，中间不允许经过其它IP地址



严格源路由选项

严格源路由时，当路由器收到一个IP数据报，判断：

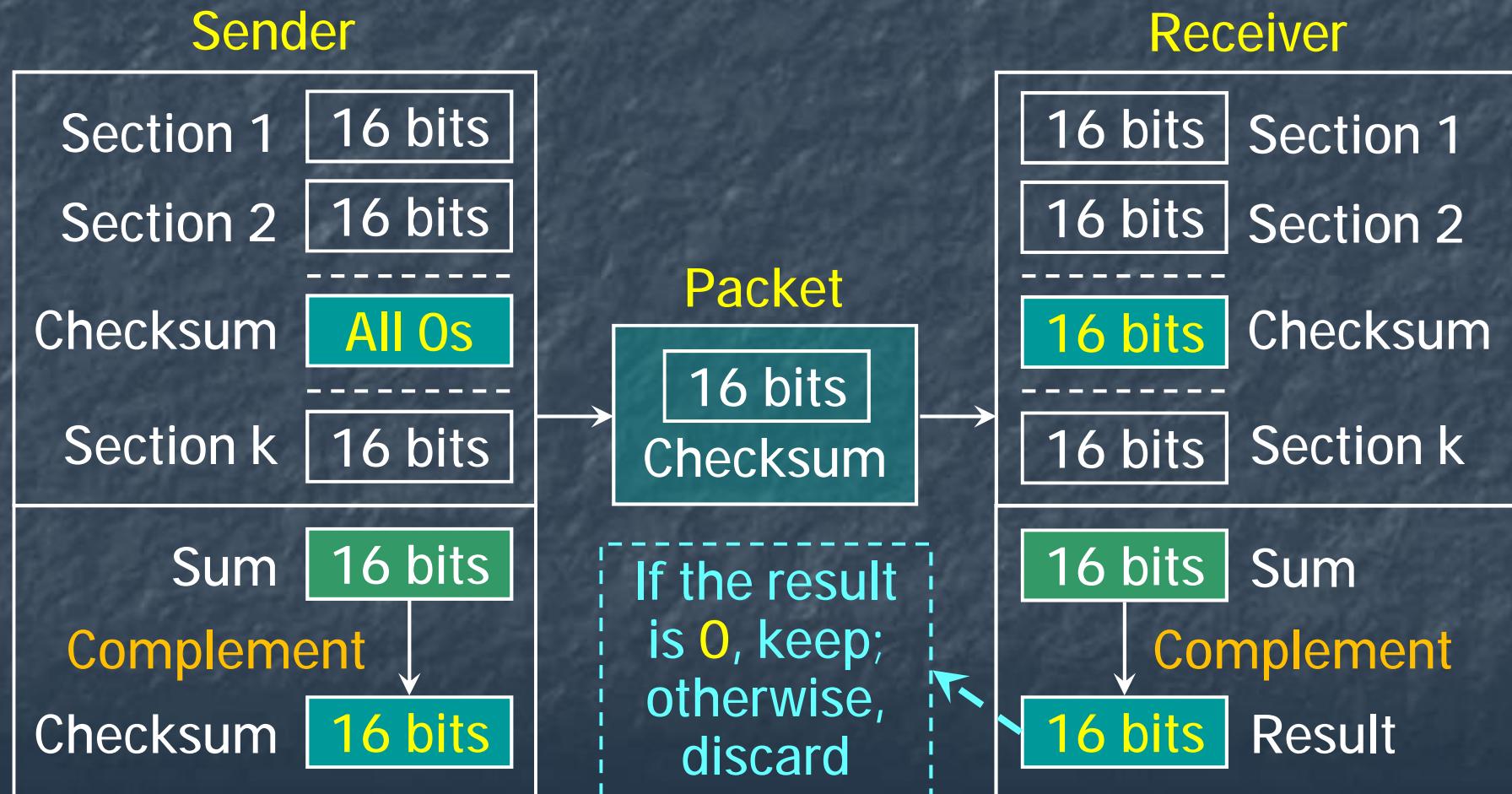
- 若指针值大于长度值，则丢弃并向源发出差错报文 **思考...**
- 若指针值不大于长度值，则取出指针所指的IP地址，判断：
 - 若IP地址与入口IP地址相等，则受理（应由它接受）。两个操作：
 - 1) 将转发出口的IP地址填入IP数据报，替换原IP地址
 - 2) 将指针值加4
 - 若不相等，则丢弃并向源发出差错报文 **思考...**

目标主机也需要配合处理，判断：

- 若指针值大于长度值，则接受该IP数据报
- 若指针值小于或等于长度值，则丢弃并向源发出差错报文

4.4 Checksum 校验和

n RFC 1071 (RFC 1141, 1624, 1936) , 附录C



Example

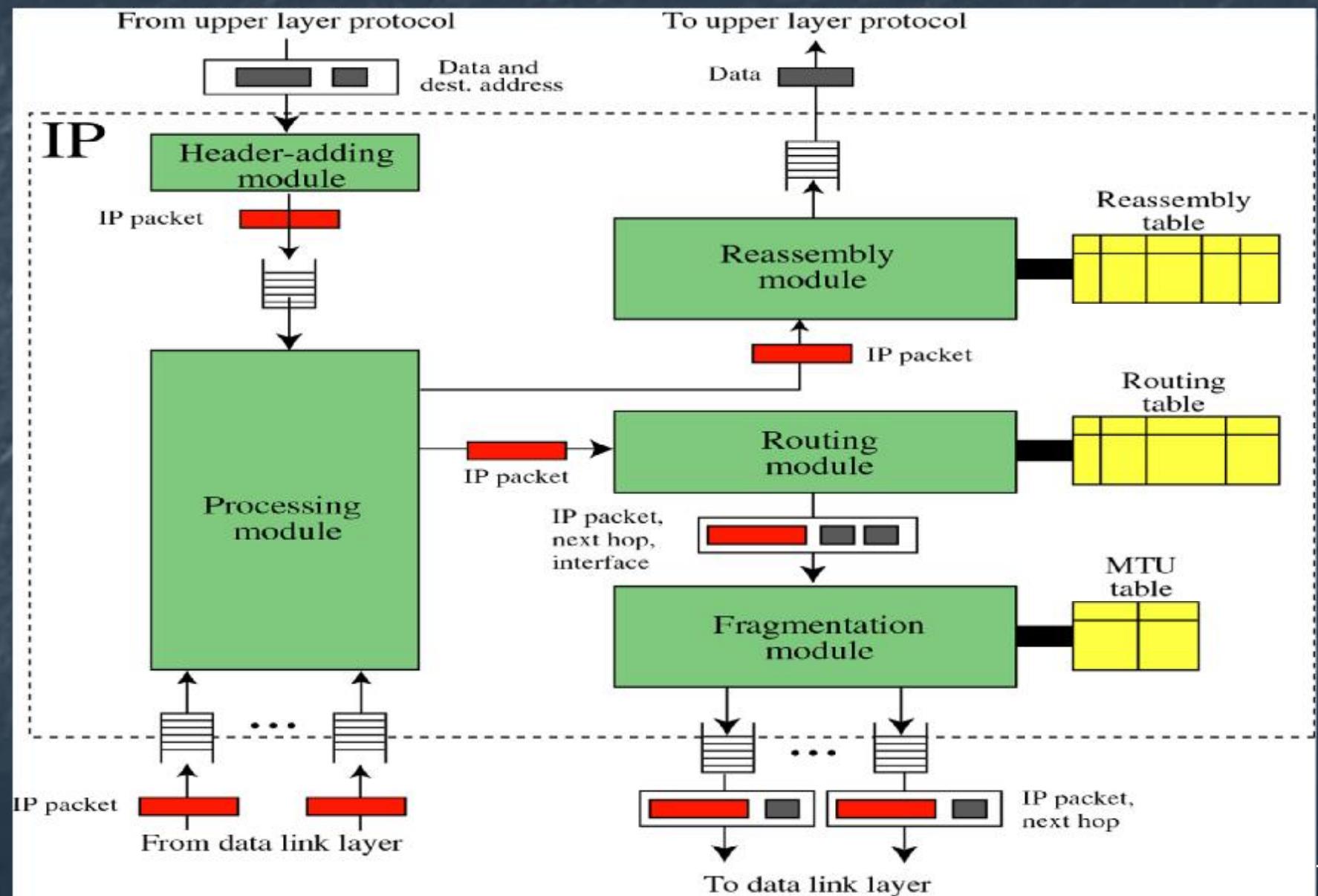
4	5	0	30	
	1	0	0	0
10	17	0		
100.12.14.5				
102.36.7.9				

Checksum: 0x D190

11010001 10010000

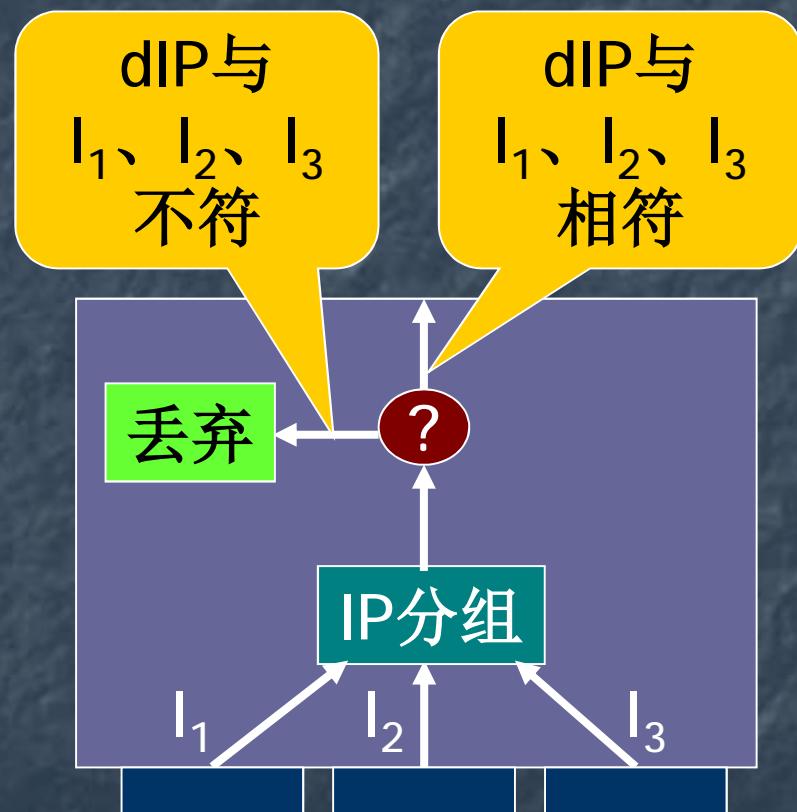
$$\begin{array}{r} \text{取} \\ \text{反} \\ \hline + & 00000111 & 00001001 \\ \hline 1 & 00101110 & 01101110 \end{array}$$

4.5 IP Package



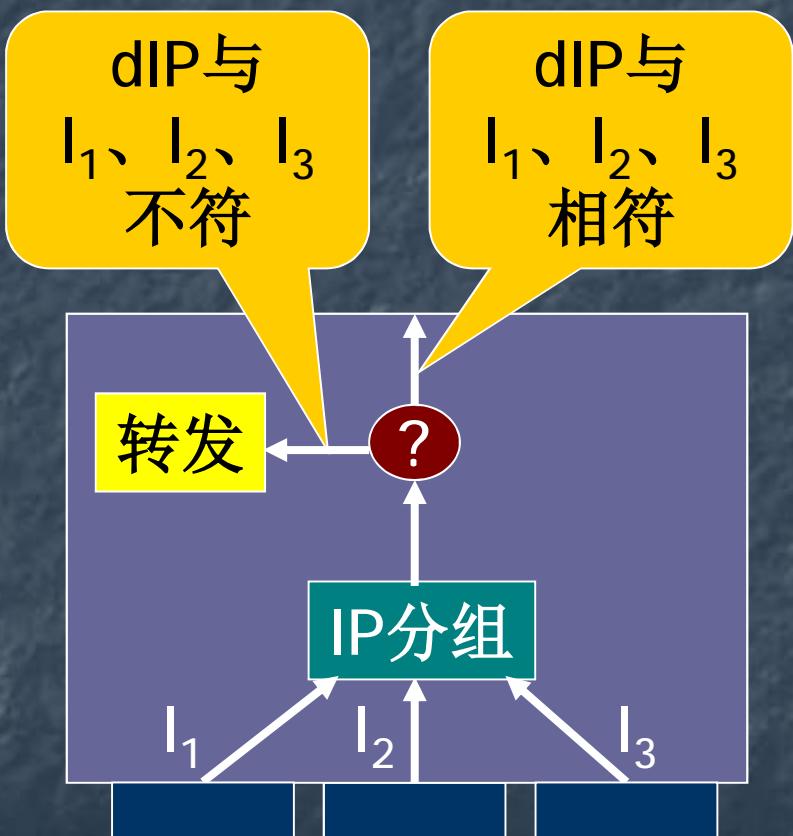
To receive IP Packets

n Host



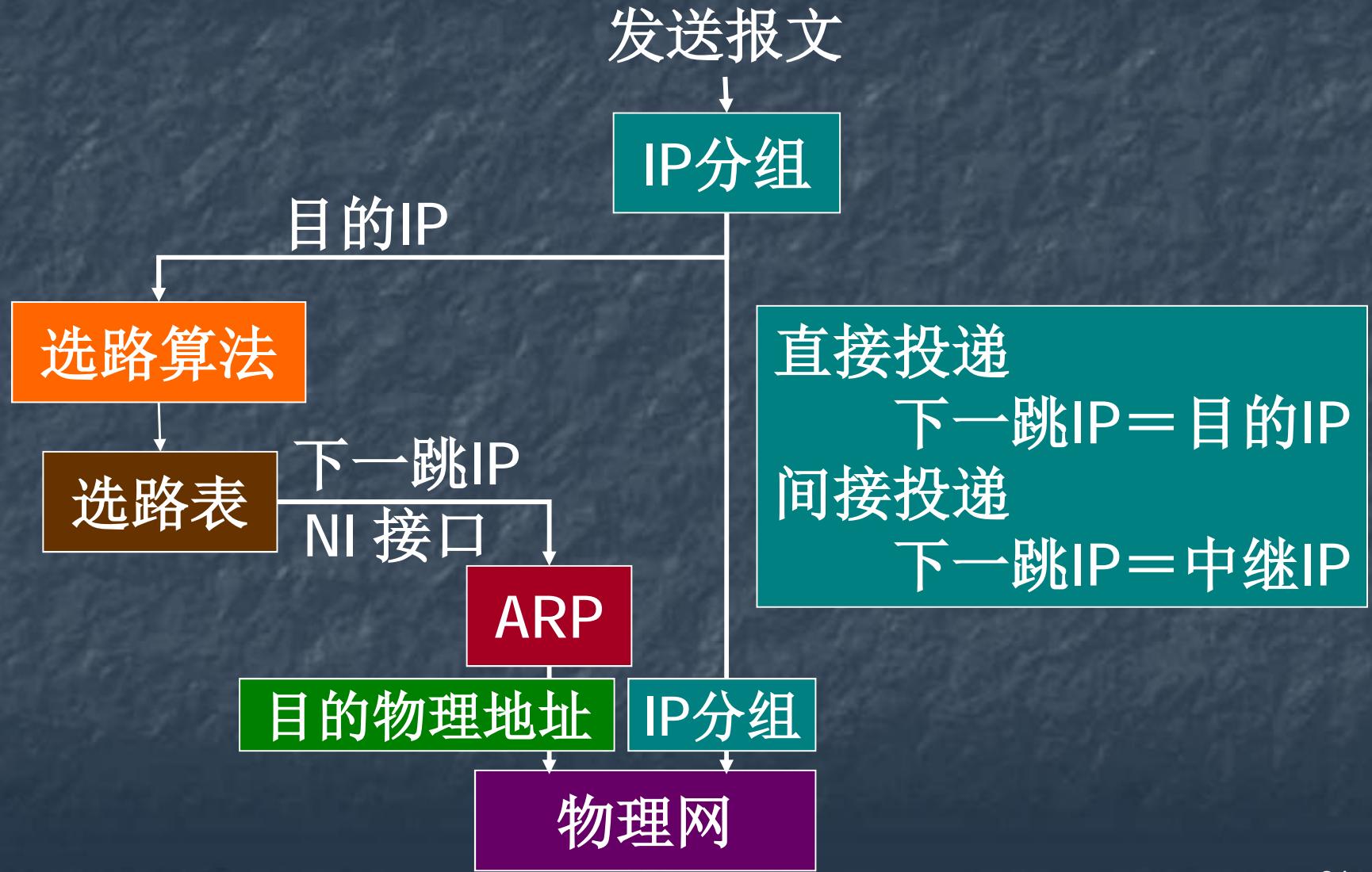
接收数据包

n Router



接收数据包

To Send IP Packets



第二部分小结

- IP分组格式

- 数据报：首部 + 数据
 - 首部：各字段的含义、作用、取值
(长度、TTL、协议、片标志、片偏移、校验和)
 - 封装：直接封装在数据帧中

- IP分组处理

- TTL、校验和计算、分片和重组、选项处理

谢谢！