

第五章 网络层（8）

袁华: hyuan@scut.edu.cn

华南理工大学计算机科学与工程学院
广东省计算机网络重点实验室

本节主要内容

- 理解CIDR的基本思想（P342）
- NAT/PAT的基本原理
- ICMP协议及其应用（5.6.4）
- 主要的地址解析协议
 - ARP
 - RARP
- IP地址的分配方式(RARP\Bootp\DHCP)

IP 地址问题_{P373}

- IP 正变成过渡流行的牺牲品： 它的地址快要耗尽了
- 原则上，有40多亿个IP地址存在，但是，由于分类，造成了数百万个地址浪费了
- 对于大多数组织来说：
 - A类地址网络，有16 M 个地址，太大了
 - C类地址网络，有256个地址，又太小了
 - B类地址网络，有65,536个地址，够用！（很多组织都申请B类地址）
- 但是，现实中，超过一半的B类网络拥有的主机数不超过 50 台主机
- 还有另一个问题：路由表膨胀 P374

无类别域间路由--CIDR P342

□ **Classless InterDomain Routing**

□ 缓解了地址枯竭的趋势；控制甚至缩减了路由表的开销

□ **CIDR的基本思想描述在 RFC 1519 中**

■ 分配IP地址的时候不再以类别来分，而是按照可变长的地址块来分配

□ 如：某用户需要 2000 个地址

IP 地址分配实例 P343

- 一块地址从194.24.0.0开始，可用地址数为8192 (2^{13})，即194.24.0.0/19
- 剑桥申请2048个地址：194.24.0.0~194.24.7.255
- 牛津申请4096个地址：194.24.16.0~194.24.31.255
- 爱丁堡申请1024个地址：194.24.8.0~194.24.11.255

University	First address	Last address	How many	Written as
Cambridge	194.24.0.0	194.24.7.	2048	194.24.0.0/21
Edinburgh	194.24.8.0	194.24.11.255	1024	194.24.8.0/22
(Available)	194.24.12.0	194.24.15.255	1024	194.24.12/22
Oxford	194.24.16.0	194.24.31.255	4096	194.24.16.0/20

为什么牛津不从194.24.8.0开始？ P343

□ P343: 4096个地址必须位于4096字节的边

- a block of 4096 addresses must lie on a 4096-byte boundary

□ 假如从194.24.8.0开始:

- 00001000.00000000
- 主机位应该能从 全零 变化到 全1
- 不连续, 或者无法表示: 194.24.8.0/20?

CIDR路由

- 路由表必须扩展，增加一个 **32-bit** 的子网掩码
- 每个路由表有一个三元组 (IP address, **subnet mask**, outgoing line)
- 当一个分组到来到的时候
 - 分组中的目标IP地址 (**Destination IP**) 被检查
 - 目标IP和子网掩码进行与操作，获得目标网络地址，以查找路由表。
 - 如果路由表中有多个表项匹配 (这些表项有不同的子网掩码)，**使用子网掩码最长的那个表项** (为什么？)

最长地址前缀选择子网掩码长的匹配项P344

□ 目标IP

- 192.24.12.4: 11000000. 00011000. 00001100. 00000100

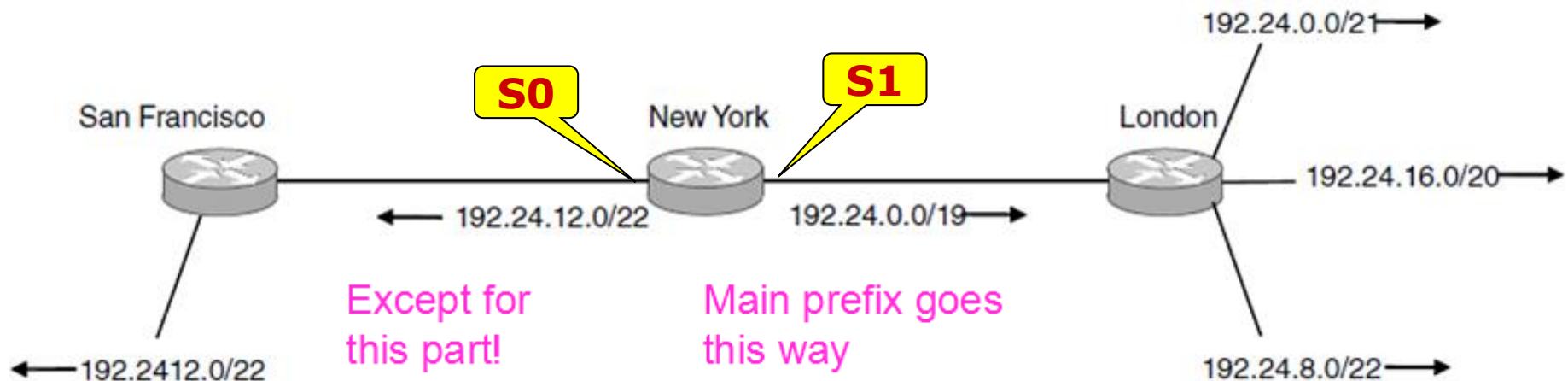
□ 路由表中有两个表项匹配

- 192.24.12.0/24

□ 11000000. 00011000. 00001100. 00000000

- 192.24.0.0/19

□ 11000000. 00011000. 000011 00. 00000000



上例中New York路由器的路由表

□ 最长前缀匹配

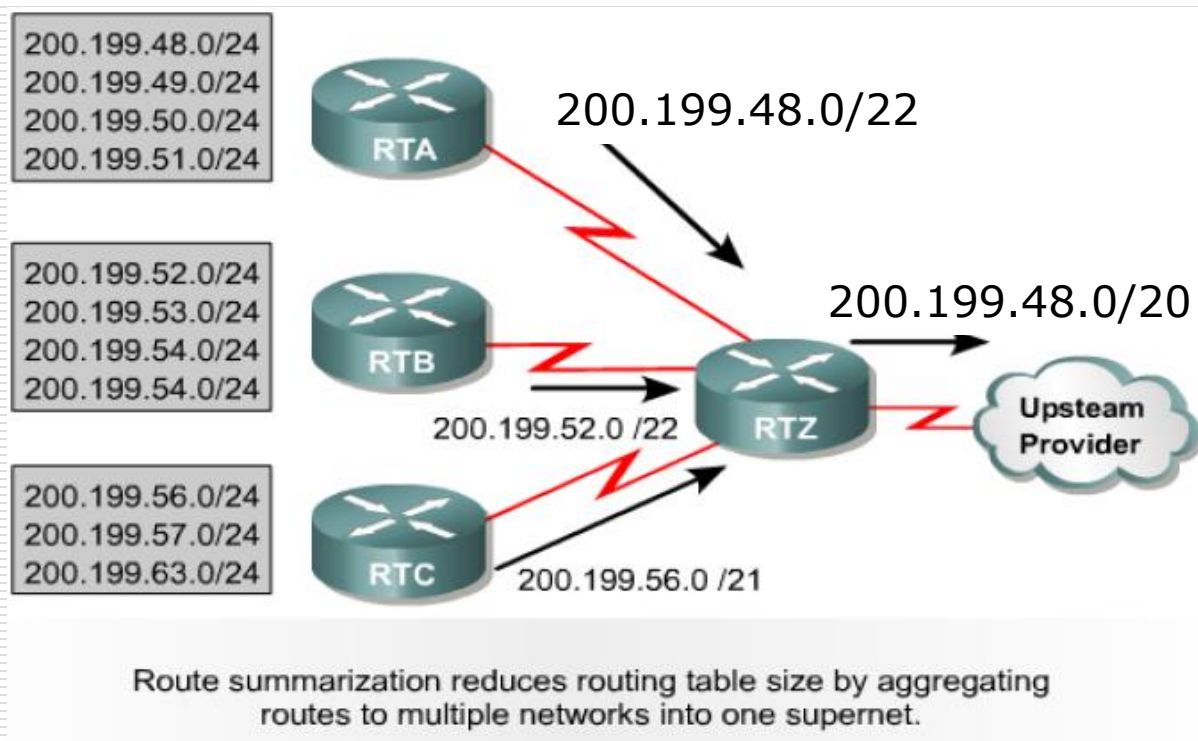
目的网络	转出接口
192.24.12.0/24	S0
192.24.0.0/19	S1

如何计算可用的IP地址？

- 一个IP地址是194.24.6.112，它的子网掩码是255.255.248.0；等同于194.24.6.112/21
- 相应的子网络号是：194.24.00000000.0
- 相应的主机位 $32-21=11$ ，所以主机IP有2048个
从00000 000.000000000=0.0
到00000 111.11111111=7.255

路由聚合

- 缩减路由表规模
- 隔离路由翻动



怎样聚合呢？ 计算不变的位数！

- 200.199.48.0/24
- 200.199.49.0/24
- 200.199.50.0/24
- 200.199.51.0/24
- 上述四个网络可以聚合成一个网络：
200.199.48.0/22

□ 00110000

第三个8位组

□ 00110001

□ 00110010

□ 00110011

- 不变的位数：
 $8+8+6=22$ ，正是网络
位数，或掩码位

本节主要内容

- 理解CIDR的基本思想（P342）
- NAT/PAT的基本原理
- ICMP协议及其应用（5.6.4）
- 主要的地址解析协议
 - ARP
 - RARP
- IP地址的分配方式(RARP\Bootp\DHCP)

NAT 概述 P377

□ NAT: net address translate NAT

- 私有IP地址和公有IP地址之间的转换。

□ PAT: port address translate (超载)

- 将多个私有IP地址影射到同一个公有IP地址的不同端口

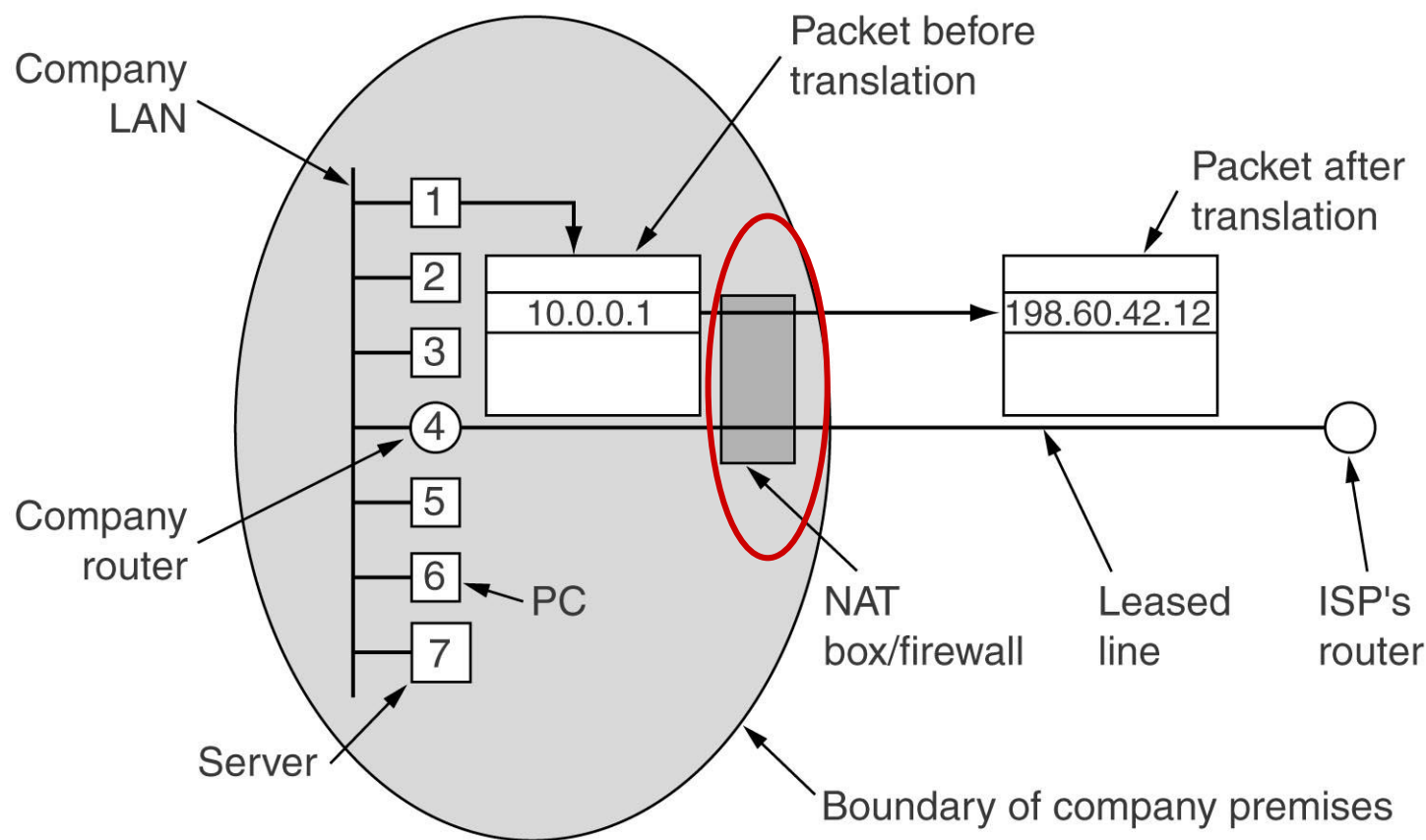
□ Private IP address: 不可路由的地址、也可用于广域网链路上

Class	RFC 1918 Internal Address Range	CIDR Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

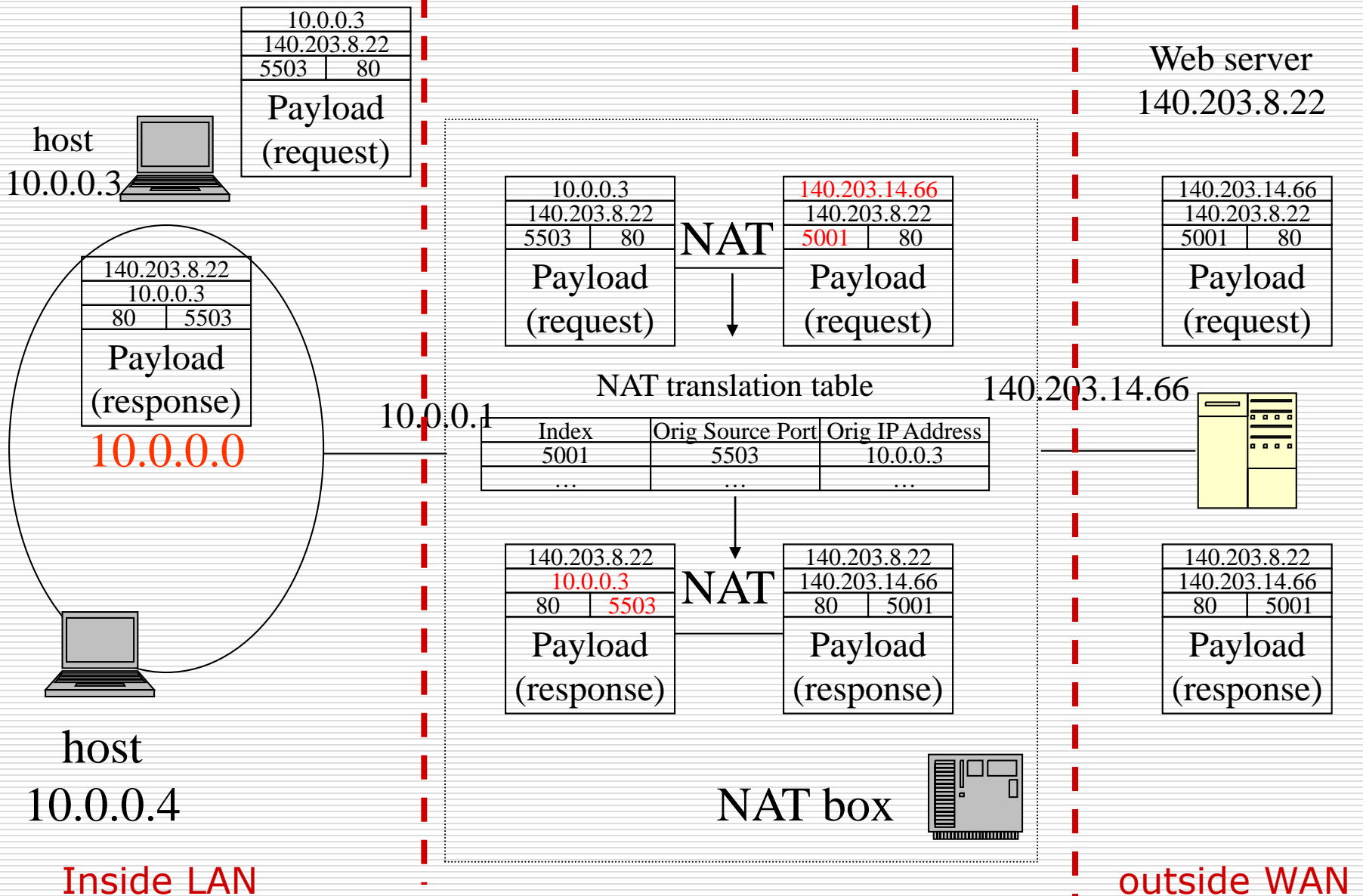
NAT—Network Address Translation P377

- ❑ 一个IP地址耗尽的快速修补方案
- ❑ RFC 3022 描述了NAT
- ❑ 内部网络使用私人地址，当内网需要和外网通信的时候，私人地址转换成合法的global 的地址
- ❑ 由NAT转换器（盒子）完成这种转换；NAT转换器能够转换并且维护一个地址转换表，以便回来的分组找到它的去处
- ❑ 当回来的分组到达NAT转换器的时候，它查找地址转换表（以源端口作索引），获得目标机的私人地址，并转换地之后发往目标机

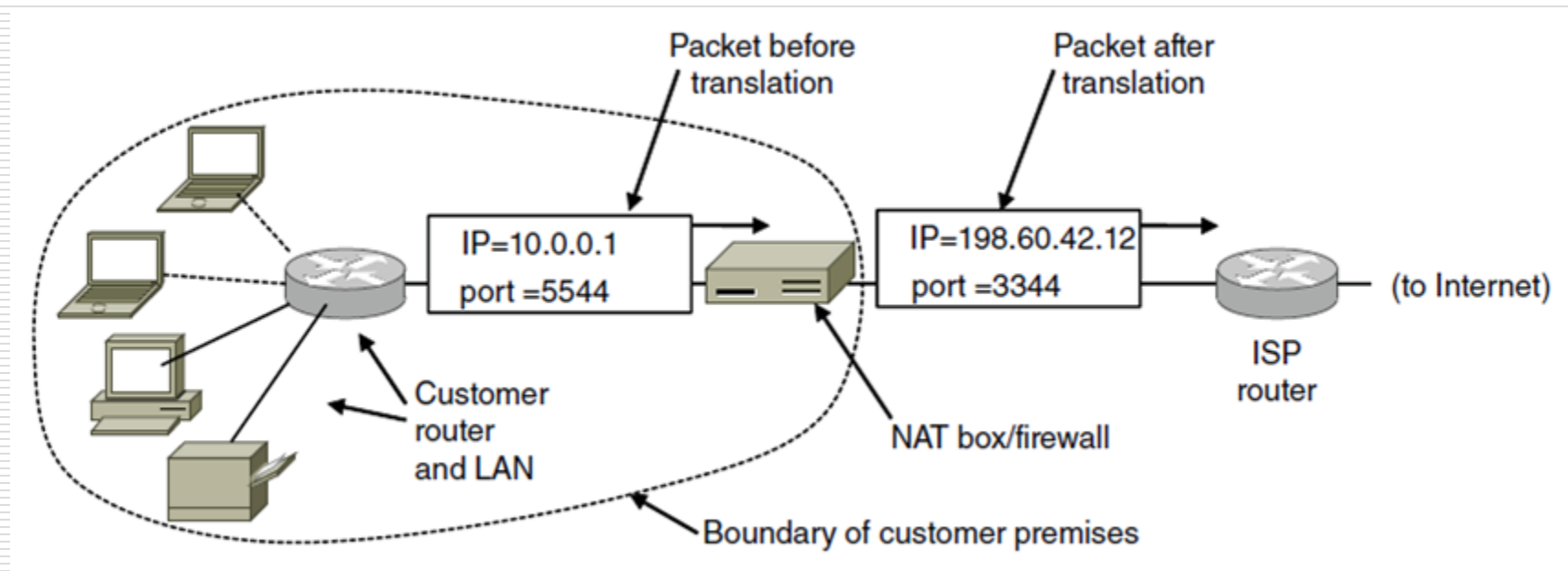
NAT转换器 (NAT Box) 的位置和功能



NAT 工作原理



常见的例子：家用路由器P348



NAT 带来的问题_{P349}

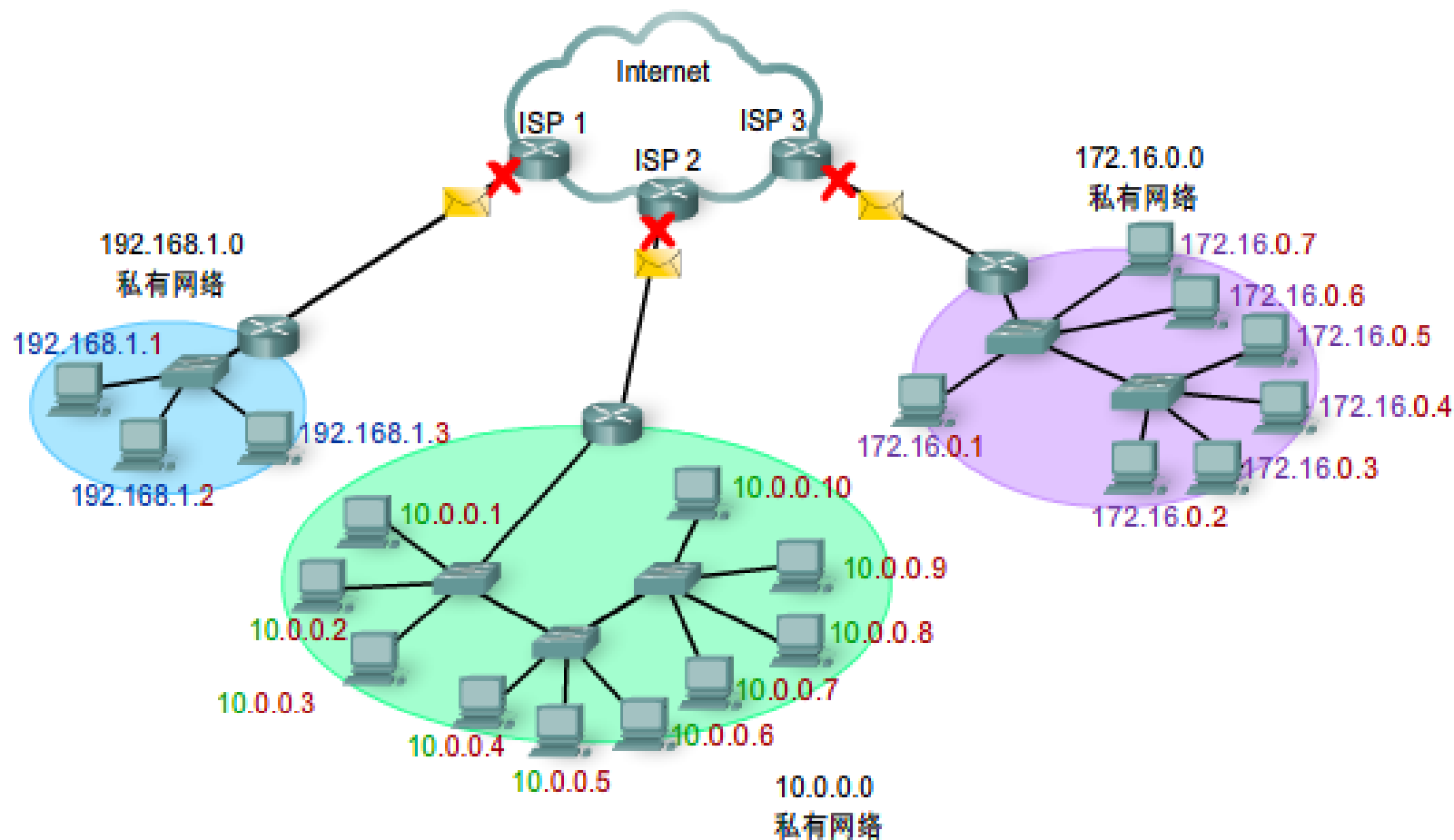
- ❑ NAT违背了IP的结构模型 —每个IP地址唯一地标识了一台机器
- ❑ NAT将互联网改变成了“面向连接”的网络，
NAT转换器维护着连接的状态，一旦它崩溃，
连接也没有了
- ❑ NAT违背了最基本的协议分层原则

NAT 带来的问题 (续) P 349

- ❑ 如果传输层不是采用TCP或UDP，而是采用了其它的协议，NAT将不再工作
- ❑ 有些应用会在payload中插入IP地址，然后接收方会提取出该IP地址并使用，但是NAT转换器对此一无所知，导致该类应用不再有效
- ❑ NAT让一个IP地址可以承载61,440 (65536-4096) 个私人地址 (超载, PAT)

注意

无 NAT 服务的网络中使用的私有地址



NAT/PAT小结

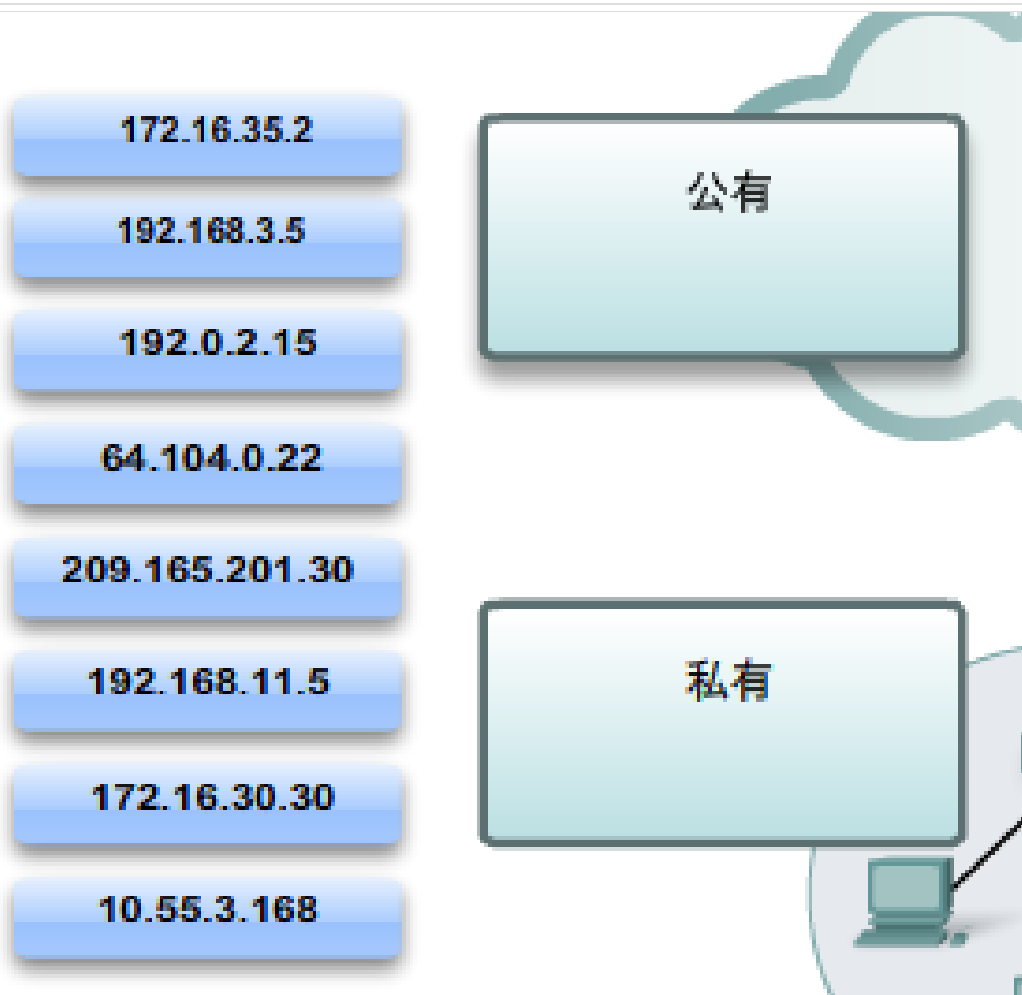
□ 优点

- 节省了公有IP地址;
- 提供了内部网访问外网的灵活性;
- 有一定的保密性。

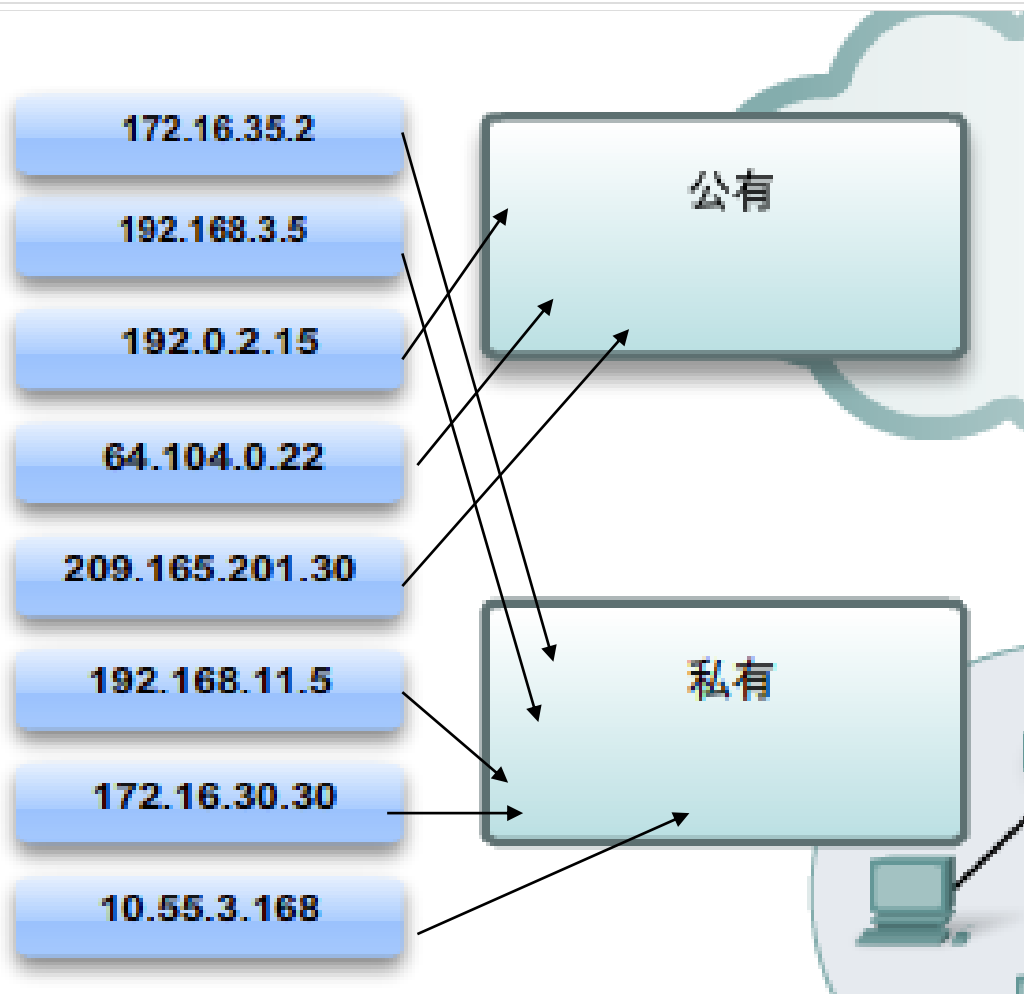
□ 缺点

- 影响了部分协议和应用的通信;
- 增加了网络延时;
- NAT转换设备的性能可能成为网络的瓶颈;
- 影响了路由追踪工具的使用。

课堂练习



参考答案



互联网网络层协议

□ 除了IP协议，还有其它的一些辅助协议

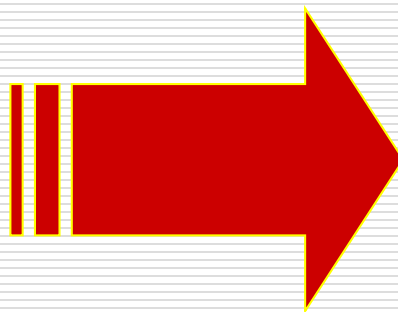
■ ICMP

■ ARP

■ RARP

■ BOOTP

■ DHCP



动态获取**IP**地址的三种方法

ICMP - Internet Control Message Protocol P357

□ 用来报告意外的事件或测试互联网

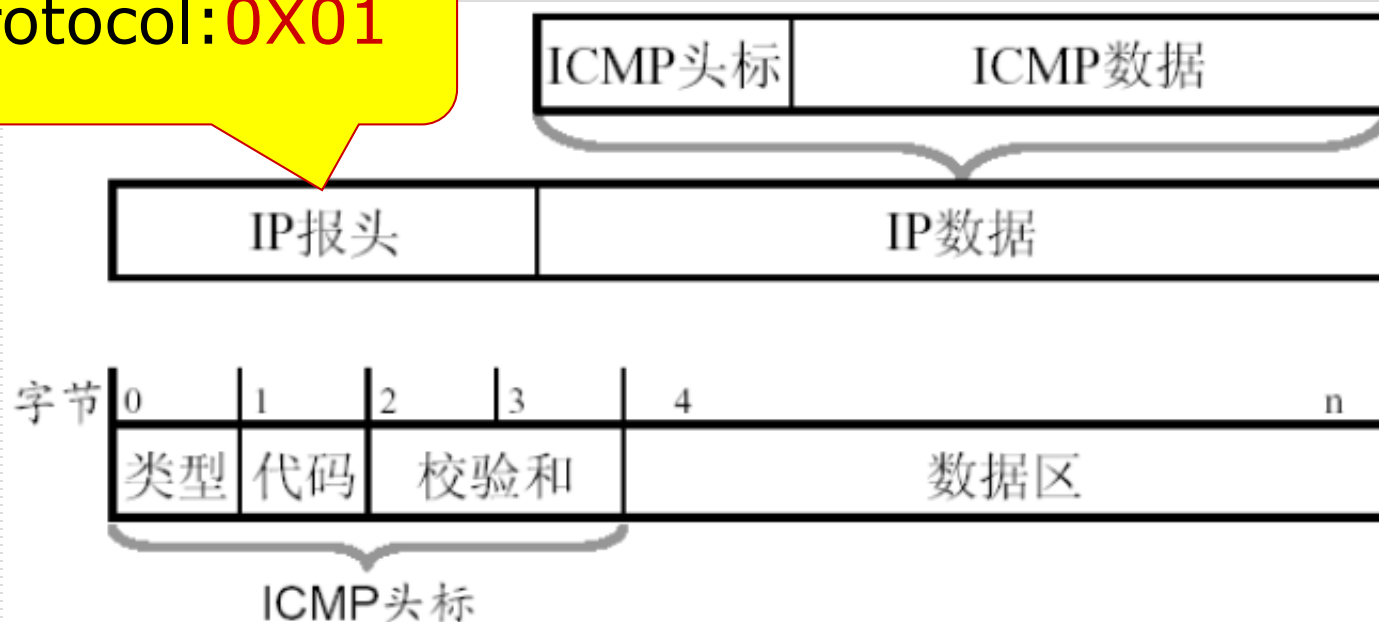
□ More ICMP Types:

<http://www.iana.org/assignments/icmp-parameters>

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo	Ask a machine if it is alive
Echo reply	Yes, I am alive
Timestamp request	Same as Echo request, but with timestamp
Timestamp reply	Same as Echo reply, but with timestamp

ICMP 消息格式

Protocol: 0X01



2个真实的ICMP消息

- [-] Internet Protocol Version 4, Src: 220.231.141.193 (220.231.141.193)
 - Version: 4
 - Header length: 20 bytes
 - + Differentiated Services Field: 0x00 (DSCP 0) [Priority]
 - Total Length: 12
 - Identification: 0
 - + Flags: 0x00
 - Fragment offset: 0
 - Time to live: 47
 - Protocol: ICMP (1)
 - + Header checksum: 0xe342 [correct]
 - Source: 220.231.141.193 (220.231.141.193)
 - Destination: 192.168.1.101 (192.168.1.101)
- [-] Internet Control Message Protocol
 - Type: 3 (Destination unreachable) [Destination unreachable]
 - Code: 10 (Host unreachable)
 - Checksum: 0xe342 [correct]
- [-] Internet Protocol Version 4, Src: 113.67.24.203 (113.67.24.203)
 - Version: 4
 - Header length: 20 bytes
 - + Differentiated Services Field: 0x00 (DSCP 0) [Priority]
 - Total Length: 56
 - Identification: 0xab8a (43914)
 - + Flags: 0x00
 - Fragment offset: 0
 - Time to live: 119
 - Protocol: ICMP (1)
 - + Header checksum: 0x4c1f [correct]
 - Source: 113.67.24.203 (113.67.24.203)
 - Destination: 192.168.1.101 (192.168.1.101)
- [-] Internet Control Message Protocol
 - Type: 3 (Destination unreachable) [Destination unreachable]
 - Code: 3 (Port unreachable)
 - Checksum: 0x7795 [correct]
- [-] Internet Protocol Version 4, Src: 192.168.1.101 (192.168.1.101)

应用 1: ping 的工作原理

- 使用ping命令（即调用ping过程）时，将向目的站点发送一个ICMP回声请求报文（包括一些任选的数据），
- 如目的站点接收到该报文，必须向源站点发回一个ICMP回声应答报文，源站点收到应答报文（且其中的任选数据与所发送的相同），则认为目的站点是可达的，否则为不可达。

ICMP 工具 —— ping

- ❑ 测试TCP/IP是否正常工作: ping 127.0.0.1
 - ❑ 网络设备是否正确: ping 本机IP地址
 - ❑ 检查对外连接的路由器: ping 默认网关IP
 - ❑ 检查与某台设备的畅通情况: ping IP
 - ❑ 检查DNS设置: 如ping www.scut.edu.cn
 - ❑ 执行DNS反向查询, ping -a IP地址
 - ❑ C:\Documents and Settings\dcampus>ping -a 202.112.17.33
- Pinging orange.gznet.edu.cn [202.112.17.33] with 32 bytes of data:

实例1 (ok)

```
C>ping 172.16.1.20
```

Pinging 172.16.1.20 with 32 bytes of data: (正常)

Reply from 172.16.1.20: bytes=32 time<10ms TTL=127

Reply from 172.16.1.20: bytes=32 time<10ms TTL=127

Reply from 172.16.1.20: bytes=32 time<10ms TTL=127

Reply from 172.16.1.20: bytes=32 time<10ms TTL=127

Ping statistics for 172.16.1.20:

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

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

实例2 (have problem)

C>ping 172.16.1.20

Pinging 172.16.1.21 with 32 bytes of data: (有问题)

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 172.16.1.21:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

应用 2: **tracert**命令

- ❑ tracert过程是通过ICMP数据报**超时报文**来得到一张**途经**的路由器列表
- ❑ 源主机向目的主机发一个IP报文，**并置TTL为1**，到达第一个路由器时，TTL减1，为0，则该路由器回发一个ICMP数据报**超时报文**，源主机取出路由器的IP地址即为途经的第一个路由端口地址
- ❑ 接着源主机再向目的主机发第二个IP报文，并**置TTL为2**，然后再发第三个、第四个IP数据报，.....直至到达目的主机
- ❑ 但互联网的运行环境状态是动态的，每次路径的选择有可能不一致，所以，只有在相对较稳定（相对变化缓慢）的网络中，tracert才有意义

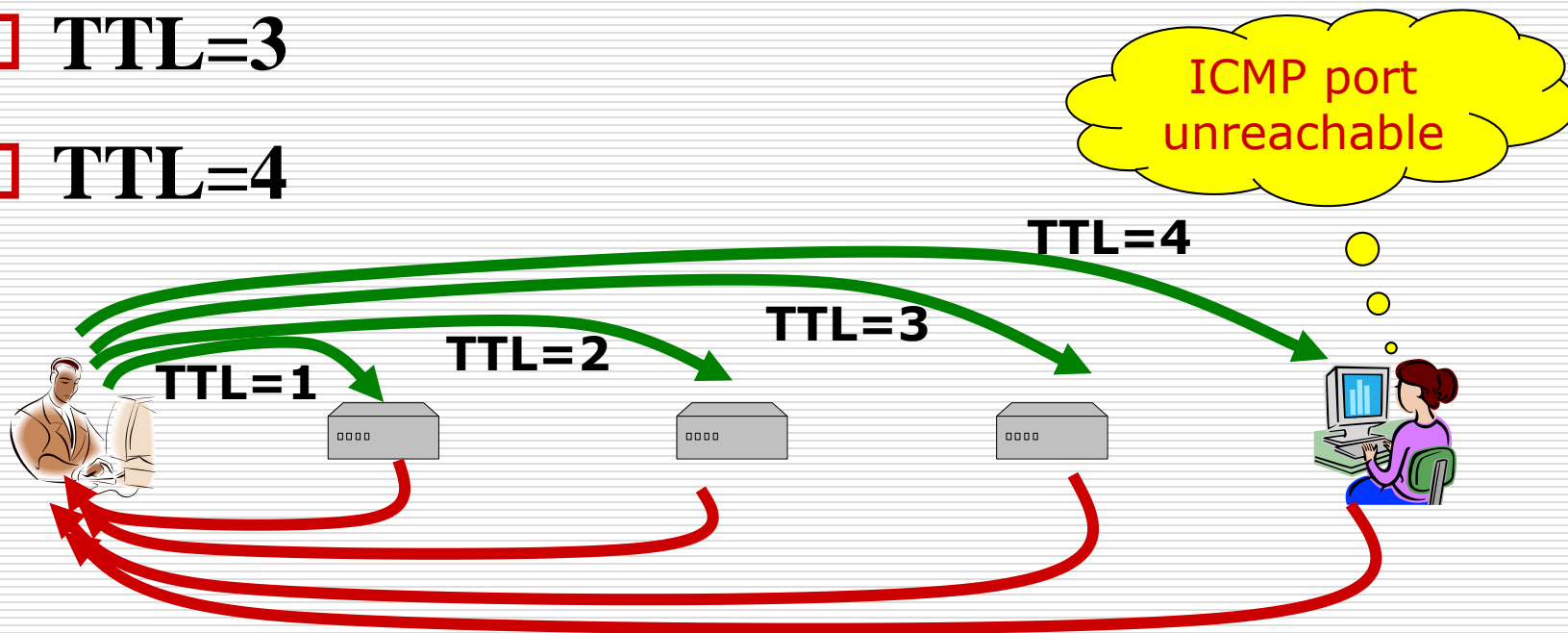
Traceroute原理图示P358

□ TTL=1

□ TTL=2

□ TTL=3

□ TTL=4



一个Tracert实例

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\dcampus>tracert www.sina.com.cn

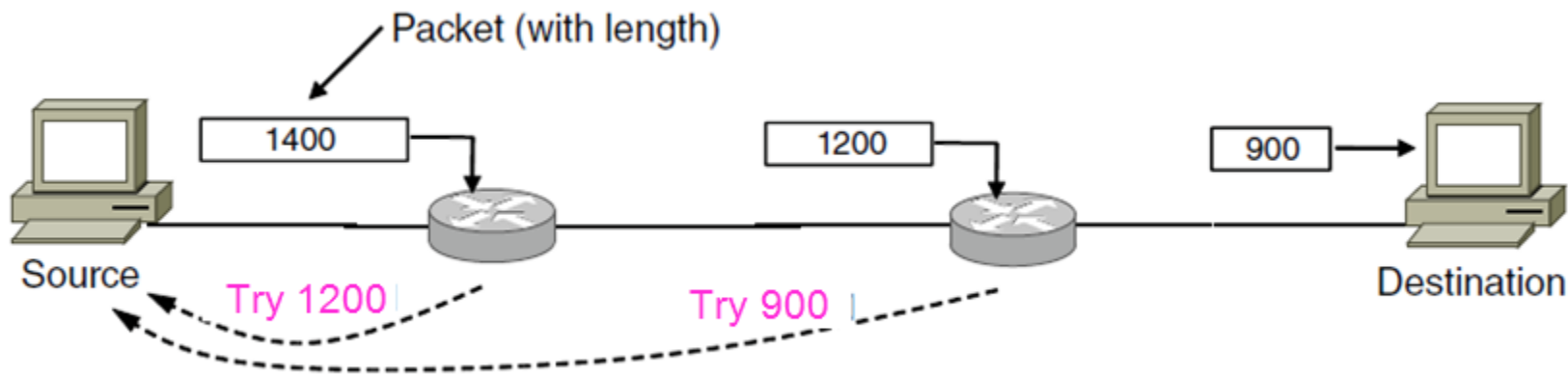
Tracing route to jupiter.sina.com.cn [202.205.3.130]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms    scut-bgw5.scut.edu.cn [202.112.18.254]
  2    <1 ms    <1 ms    <1 ms    scn-rgw8.gznet.edu.cn [202.112.19.93]
  3    *        *        *        Request timed out.
  4    <1 ms    <1 ms    <1 ms    202.127.216.22
  5    *        37 ms    34 ms    202.127.216.21
  6    34 ms    33 ms    34 ms    cd1.cernet.net [202.112.53.74]
  7    34 ms    34 ms    33 ms    wdc1.cernet.net [202.112.38.82]
  8    34 ms    34 ms    34 ms    202.205.13.249
  9    34 ms    34 ms    34 ms    202.205.13.210
 10    34 ms    34 ms    34 ms    202.205.3.130



Trace complete.
```

应用3: PMTU P334

- ❑ 发数据包，分段标记DF=1，尝试1400，1200，900，直到到达目的机
- ❑ 结果：MTU=900



type=3的code

Codes 	Description 	Reference
0	Net Unreachable	[RFC792]
1	Host Unreachable	[RFC792]
2	Protocol Unreachable	[RFC792]
3	Port Unreachable	[RFC792]
4	Fragmentation Needed and Don't Fragment was Set	[RFC792]
5	Source Route Failed	[RFC792]
6	Destination Network Unknown	[RFC1122]
7	Destination Host Unknown	[RFC1122]
8	Source Host Isolated	[RFC1122]
9	Communication with Destination Network is Administratively Prohibited	[RFC1122]
10	Communication with Destination Host is Administratively Prohibited	[RFC1122]

注意

- 一般来说，ICMP消息仅送给源机
- ICMP数据传输方式和其他数据传输方式一样，也可能遇到同样的错误，规定：**ICMP消息不生成自己的差错报告**

ICMP Message Types	
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect/ Change Request
8	Echo Request
9	Router Advertisement
10	Router Selection
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply

地址解析协议 P359

□ ARP（地址解析协议）：

Address Resolution Protocol

IP 地址 → MAC 地址

□ RARP（逆向地址解析协议）：

Reverse Address Resolution Protocol

MAC 地址 → IP 地址

ARP — Address Resolution Protocol P382

- ❑ ARP 的任务是找到一个给定IP地址所对应的MAC地址
- ❑ ARP is defined in RFC 826.

问题：为什么需要地址解析？

ARP的工作原理

request

我是128.1.2.7, 谁知道IP地址为
128.1.2.15的主机对应的MAC地址?

主机A
128.1.2.7
0:a0:24:ec:c1:b4

Ethernet

听见/不回答

听见/不回答

听见/不回答

听见/回答

128.1.2.15
8:0:20:e:28:ef
主机E

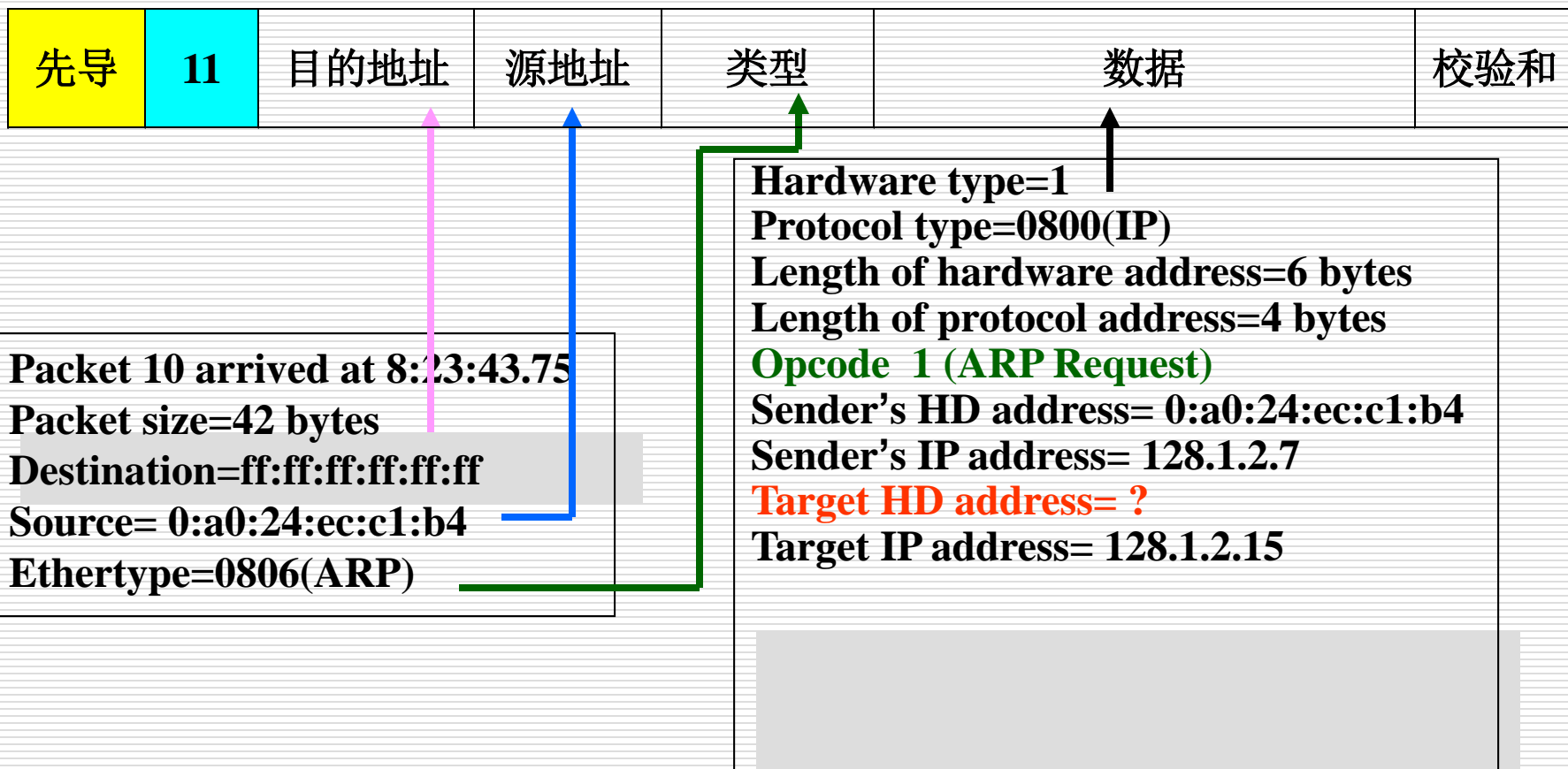
主机A的ARP表

IP	MAC
128.1.2.7	0:a0:24:ec:c1:b4
128.1.2.11	0:20:c5:e2:c6:a2
128.1.2.15	8:0:20:e:28:ef

主机128.1.2.7, 我是128.1.2.15,
我的MAC地址是8:0:20:e:28:ef !

reply

ARP请求 (Request)



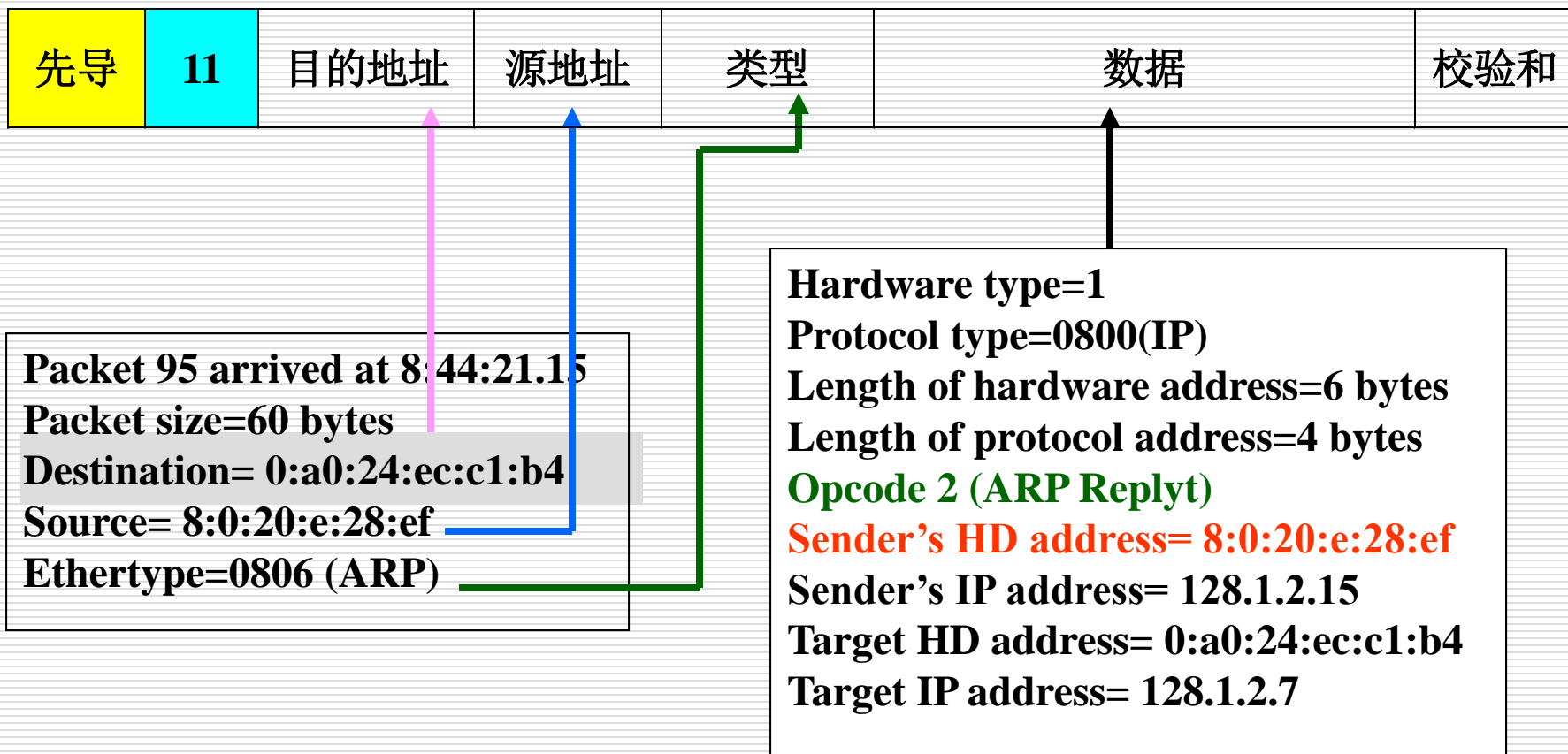
Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
100	14.031477	Cisco_67:8c:00	Broadcast	ARP	60	who has 202.38.254.191? Tell 202.38.254.254
101	14.376052	Cisco_67:8c:00	Broadcast	ARP	60	who has 202.38.254.243? Tell 202.38.254.254
102	14.434828	Cisco_67:8c:00	Broadcast	ARP	60	who has 202.38.254.177? Tell 202.38.254.254
103	14.436926	Cisco_67:8c:00	Broadcast	ARP	60	who has 202.38.254.206? Tell 202.38.254.254
104	14.531717	Cisco_67:8c:00	Broadcast	ARP	60	who has 202.38.254.242? Tell 202.38.254.254
105	16.457350	Cisco_67:8c:00	Broadcast	ARP	60	who has 202.38.254.197? Tell 202.38.254.254
109	16.884609	Cisco_67:8c:00	Broadcast	ARP	60	who has 202.38.254.248? Tell 202.38.254.254

- Frame 104: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
- Ethernet II, Src: Cisco_67:8c:00 (00:12:44:67:8c:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 - Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 - Source: Cisco_67:8c:00 (00:12:44:67:8c:00)
 - Type: ARP (0x0806)
 - Trailer: 00
- Address Resolution Protocol (request)
 - Hardware type: Ethernet (1)
 - Protocol type: IP (0x0800)
 - Hardware size: 6
 - Protocol size: 4
 - opcode: request (1)
 - [Is gratuitous: False]
 - Sender MAC address: Cisco_67:8c:00 (00:12:44:67:8c:00)
 - Sender IP address: 202.38.254.254 (202.38.254.254)
 - Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
 - Target IP address: 202.38.254.242 (202.38.254.242)

0000	ff ff ff ff ff ff 00 12 44 67 8c 00 08 06 00 01 Dg.....
0010	08 00 06 04 00 01 00 12 44 67 8c 00 ca 26 fe fe Dg...&..
0020	00 00 00 00 00 00 ca 26 fe f2 00 00 00 00 00 00&
0030	00 00 00 00 00 00 00 00 00 00 00 00

ARP回答 (Reply)





Filter: arp Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1888	26.303091	Cisco_67:8c:00	Broadcast	ARP	60	who has 202.38.254.217? Tell 202.38.254.254
1893	26.544726	Cisco_67:8c:00	Broadcast	ARP	60	who has 202.38.254.180? Tell 202.38.254.254
1900	27.663903	Cisco_67:8c:00	Broadcast	ARP	60	who has 202.38.254.208? Tell 202.38.254.254
1901	28.269122	LgElectr_22:7e:d5	Broadcast	ARP	42	who has 202.38.254.254? Tell 202.38.254.155
1902	28.269723	Cisco_67:8c:00	LgElectr_22:7e:d5	ARP	60	202.38.254.254 is at 00:12:44:67:8c:00
1903	28.290843	LgElectr_22:7e:d5	Broadcast	ARP	42	who has 202.38.254.254? Tell 202.38.254.155
1904	28.291417	Cisco_67:8c:00	LgElectr_22:7e:d5	ARP	60	202.38.254.254 is at 00:12:44:67:8c:00
1905	28.331818	LgElectr_22:7e:d5	Broadcast	ARP	42	who has 202.38.254.254? Tell 202.38.254.155

Frame 1902: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

Ethernet II, Src: Cisco_67:8c:00 (00:12:44:67:8c:00), Dst: LqElectr_22:7e:d5 (00:e0:91:22:7e:d5)

Destination: LqElectr_22:7e:d5 (00:e0:91:22:7e:d5)

Source: Cisco_67:8c:00 (00:12:44:67:8c:00)

Type: ARP (0x0806)

[illegible]

Address Resolution Protocol (reply)

Hardware type: Ethernet (1)

Protocol type: IP (0x0800)

Hardware size: 6

Protocol size: 4

```
opcode: reply (2)
```

```
[Is gratuitous: False]
```

Sender MAC address: Cisco_67:8c:00 (00:12:44:67:8c:00)

Sender IP address: 202.38.254.254 (202.38.254.254)

Target MAC address: LgElectr_22:7e:d5 (00:e0:91:22:7e:d5)

Target IP address: 202.38.254.155 (202.38.254.155)

```
0000  00 e0 91 22 7e d5 00 12  44 67 8c 00 08 06 00 01  ..."~... Dq.....
```

```
0010 08 00 06 04 00 02 00 12 44 67 8c 00 ca 26 fe fe ..... Dg...&..
```

```
0020  00 e0 91 22 7e d5 ca 26 fe 9b 00 00 00 00 00 00  ..."~..& .....
```

```
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  . . . . .
```

怎样工作得更好? P360

□ 为了让ARP的工作更加高效，下面是几种优化措施：

- 缓存 ARP 结果
- 在ARP请求中包括源机的 IP-to-MAC 地址的映射
- 每台机器在启动的时候，广播它的IP-MAC地址对



免费ARP (Gratuitous ARP P360)

□ 免费ARP

- 当一台主机启动时，发送要给一个免费ARP，
(如果意外收到一个应答，即是IP地址发生了冲突)
- 当一个接口 (interface) 的配置发生了改变，会发送一个免费ARP

□ 例子：一台主机 (172.16.1.1, 0002 4A87 0D92) 发送的免费ARP

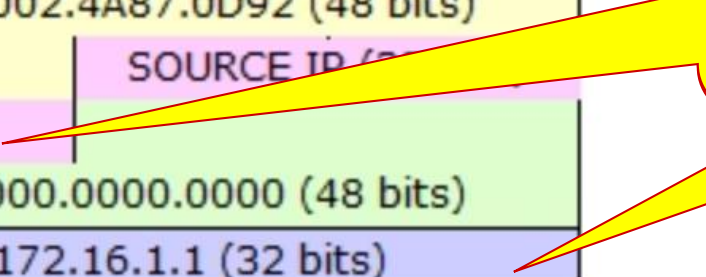
An Example

□ A host (172.16.1.1, 0002 4A87 0D92)

Ethernet II

0	4	8	14	19 Bytes
PREAMBLE: 101010...1011		DEST MAC: FFFF.FFFF.FFFF		SRC MAC: 0002.4A87.0D92
TYPE: 0x806		DATA (VARIABLE LENGTH)		FCS: 0x0

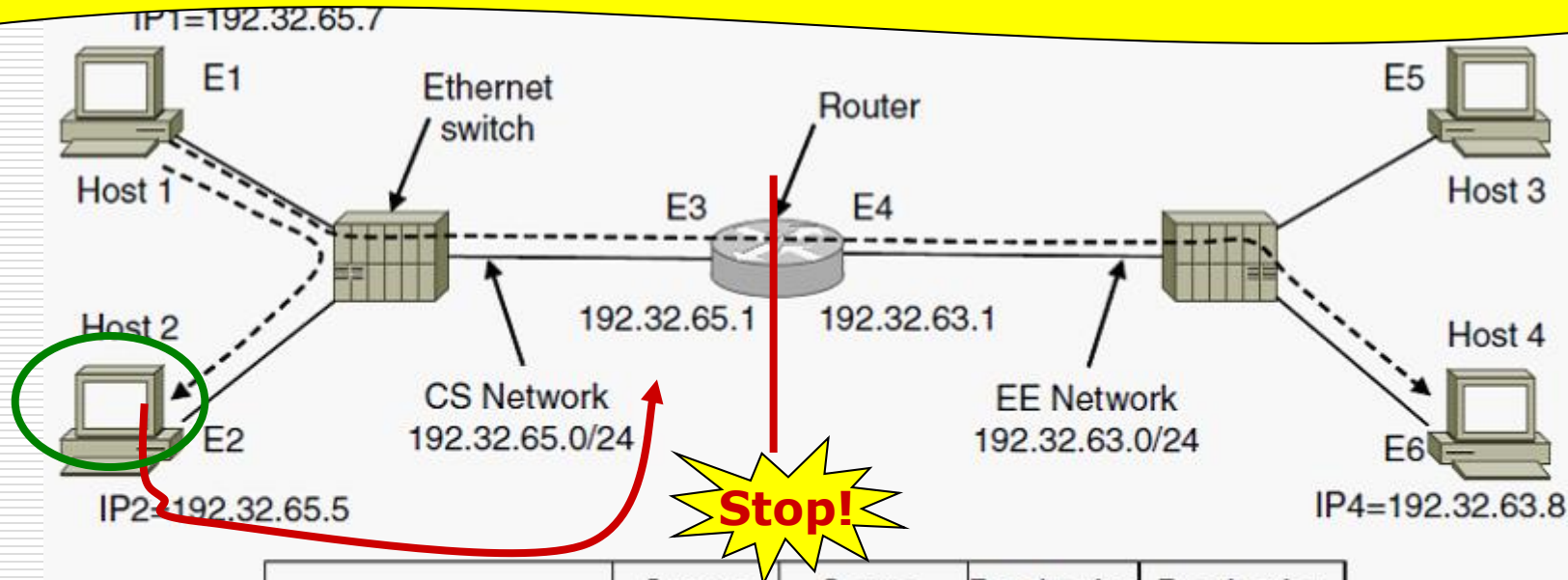
ARP

0	8	16	31	Bits
HARDWARE TYPE: 0x1		PROTOCOL TYPE:		
HLEN: 0x6	PLEN: 0x4	OPCODE: 0x1		
SOURCE MAC: 0002.4A87.0D92 (48 bits)				
172.16.1.1		SOURCE IP (32 bits)		
TARGET MAC: 0000.0000.0000 (48 bits)				
TARGET IP: 172.16.1.1 (32 bits)				

**Source IP
==
target IP**

如果远程主机不在同子网呢？ P360

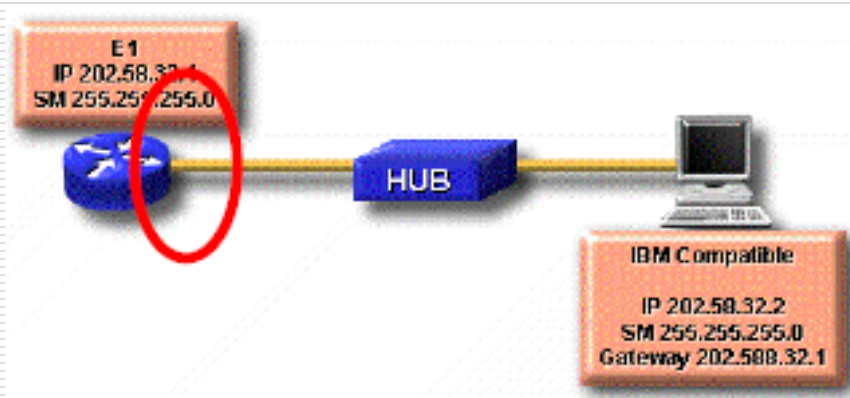
Host1 want to send packet to host4, but don't know its's MAC!



Frame	Source IP	Source Eth.	Destination IP	Destination Eth.
Host 1 to 2, on CS net	IP1	E1	IP2	E2
Host 1 to 4, on CS net	IP1	E1	IP4	E3
Host 1 to 4, on EE net	IP1	E4	IP4	E6

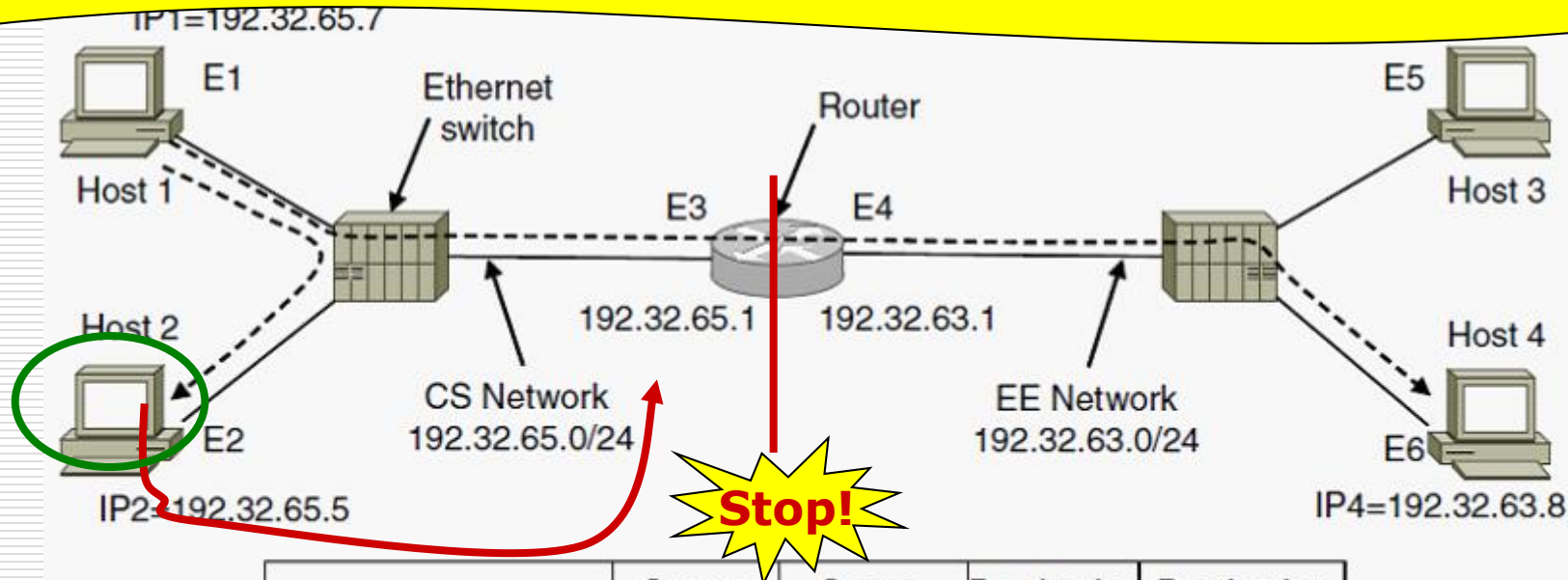
缺省网关（代理 **ARP**） P360

- 当源设备需要的目的地址与自己不在同一个网络时，如果源不知道目的MAC地址，它必须使用路由器的服务使它的数据达到目的，当路由器在这种方式下使用时，称为缺省网关。
- 缺省网关是与源设备所处的网段相连的路由器接口上的IP地址



如果远程主机不在同子网呢？

ARP Request: Target IP is 192.32.65.1(default gateway)



Frame	Source IP	Source Eth.	Destination IP	Destination Eth.
Host 1 to 2, on CS net	IP1	E1	IP2	E2
Host 1 to 4, on CS net	IP1	E1	IP4	E3
Host 1 to 4, on EE net	IP1	E4	IP4	E6

ARP table

- IP地址到MAC地址的映射表，储存在存储器（RAM）中，自动维护。（掉电消失）
- 为了减少ARP请求的次数，每个设备拥有自己的ARP表，包括路由器。
- 自动维护ARP表
 - 通过广播ARP请求中的源设备信息添加更新表；
 - 利用自己的ARP请求之应答信息来添加、更新表；
 - 删除超过一定时限的信息

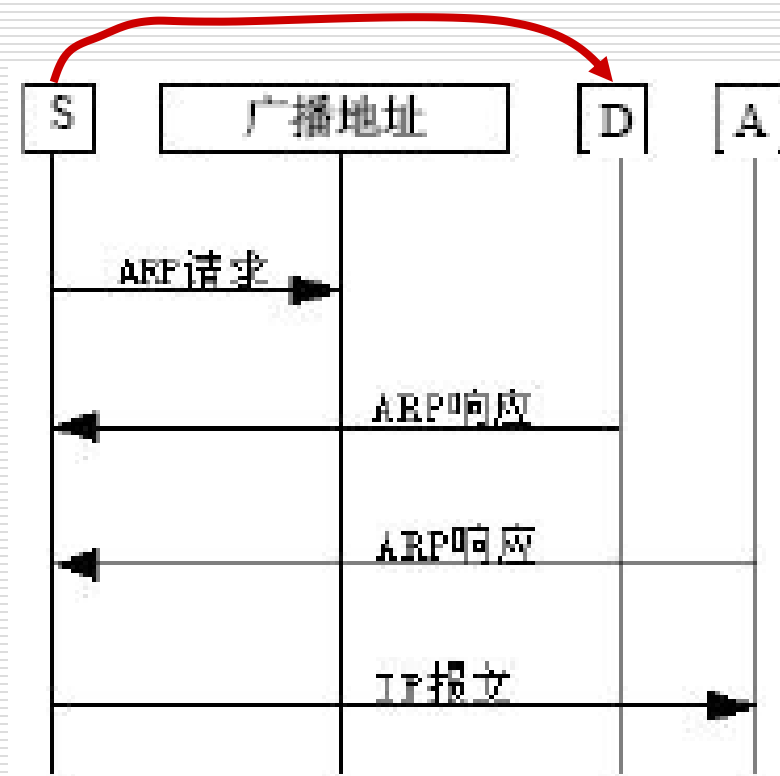
ARP工具程序

- Windows的ARP.exe, linux的arpwatch。
- 查看arp表内容: `arp -a`
- 删除arp表中指定的纪录:
 - `Arp -d [IP 地址]`
- 添加记录
 - `Arp -s [IP地址] [MAC地址]`

什么是ARP 欺骗?

□ ARP spoofing /cheating

S want to communicate with D



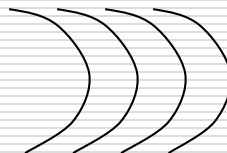
怎样避免被ARP欺骗？

- 静态ARP
- 不马上写ARP缓存
- 设置ARP服务器
- 硬件屏蔽，如路由器采用静态ARP且作全权代理
- 。 。 。 。 。 。

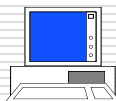
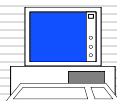
RARP协议的工作原理

request

我的MAC地址是0:a0:24:ec:c1:b4,
谁知道我的IP地址?



主机A
(无盘)



主机E
(服务器)

Ethernet

听见/不回答

听见/不回答

听见/不回答

听见/回答

主机A获得自己的IP地址,
开始自己的开机过程。

主机0:a0:24:ec:c1:b4, 你的
IP地址是128.1.2.7!

reply

IP地址的动态分配方式P361

□ 静态分配

□ 动态分配

■ 给定一个MAC地址，如何得到对应的IP地址？

□ RARP (Reverse Address Resolution Protocol) 在 RFC 903 描述，用来获取本机MAC地址对应的IP地址

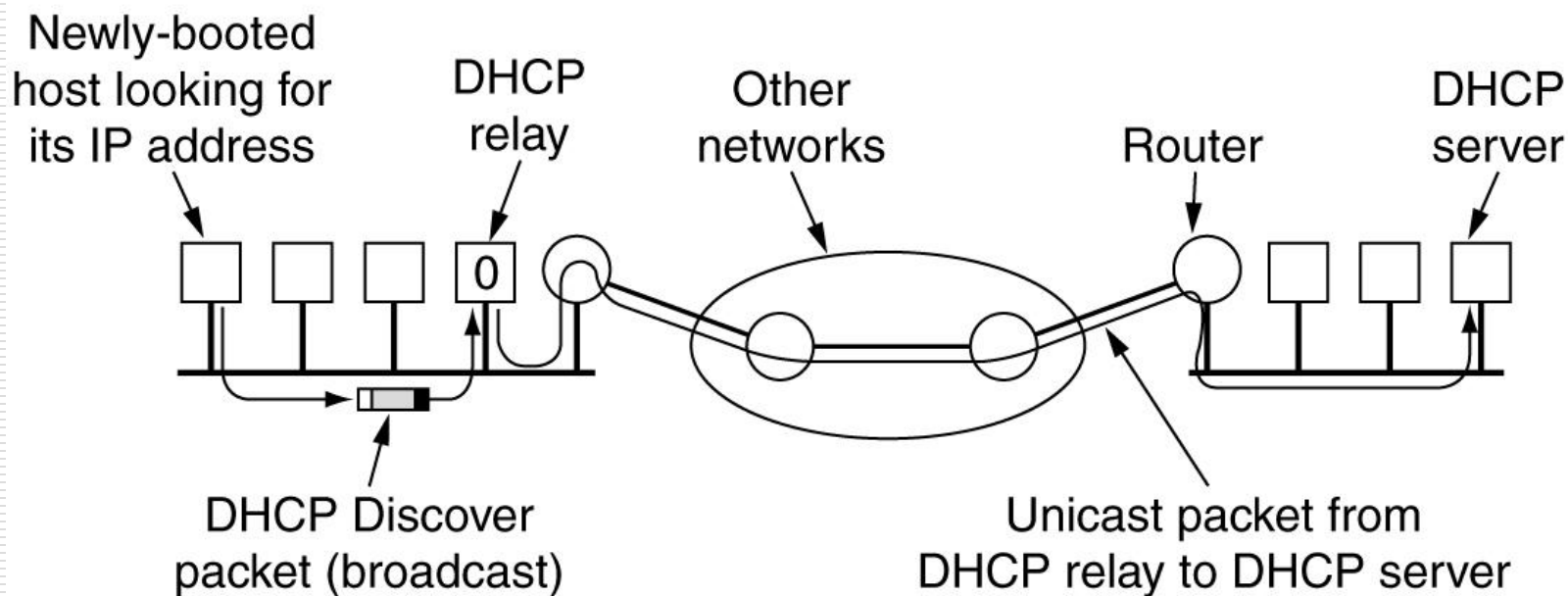
□ BOOTP 在RFC 951、 1048 和1084中描述，（缺点：需要手工配置）

□ DHCP (Dynamic Host Configuration Protocol)在 RFCs 2131 和 2132中描述

DHCP: 动态主机配置协议^{P361}

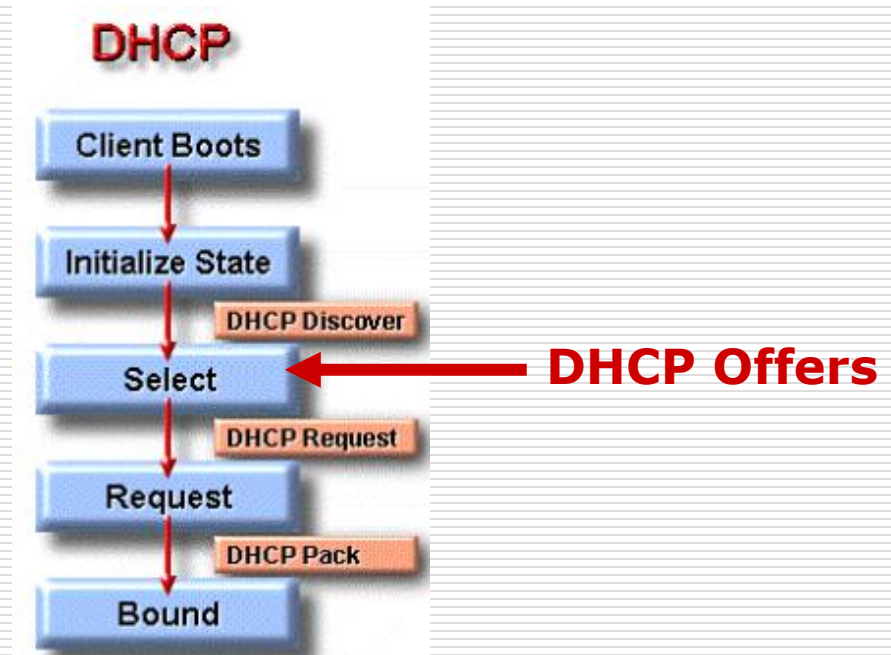
□ **D**ynamic **H**ost **C**onfigure **P**rotocol

□ 可以灵活分配IP地址，节约IP地址的使用



DHCP

- ❑ 使一台主机迅速并动态地获取一个IP地址
- ❑ 通过DHCP获取的 IP是租来的，可能会过期
- ❑ DHCP过程
 - 初始化状态
 - 选择状态
 - 请求状态
 - 绑定状态



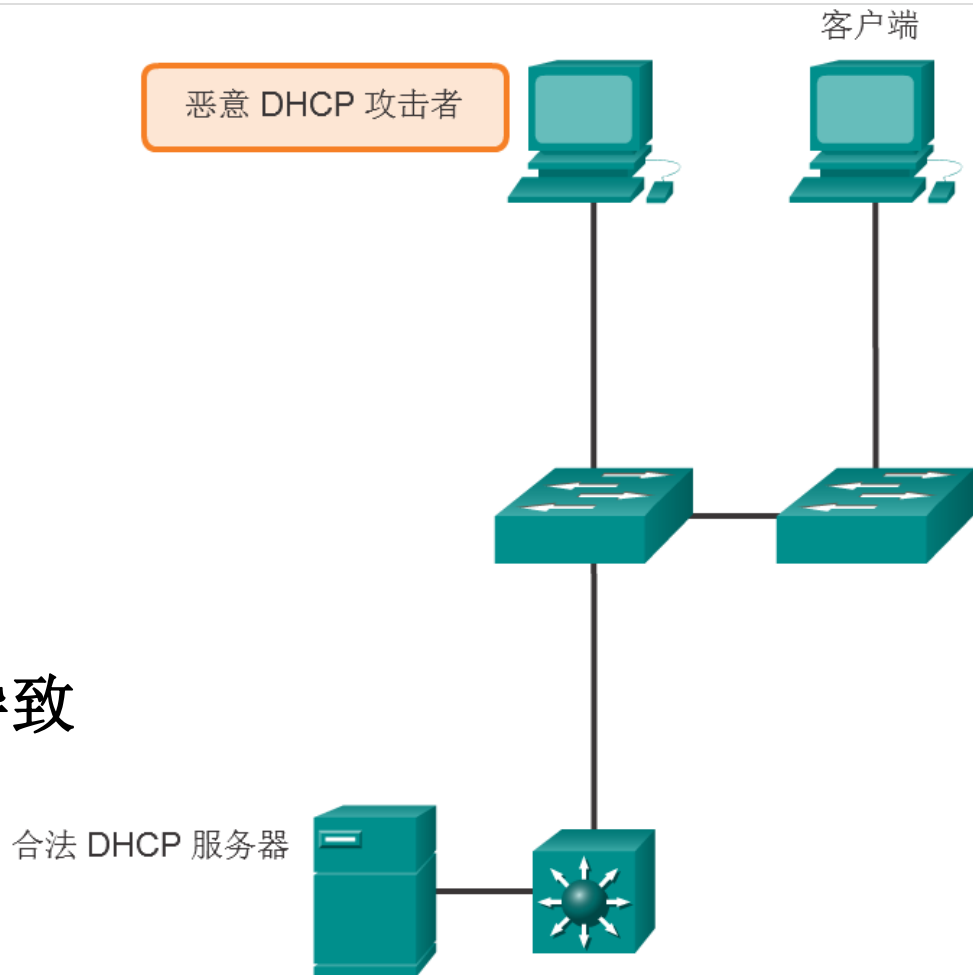
DHCP欺骗和耗竭攻击

□ DHCP欺骗:

- 伪装DHCP server

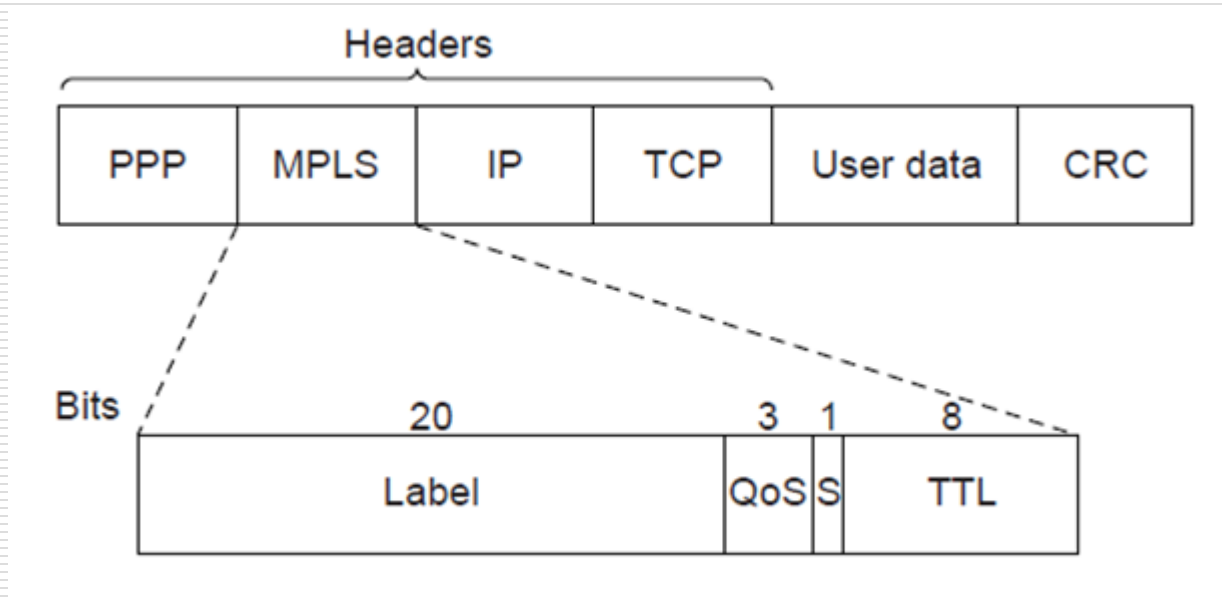
□ DHCP耗竭

- 因分配完IP地址而导致
正常客户无法获得地址

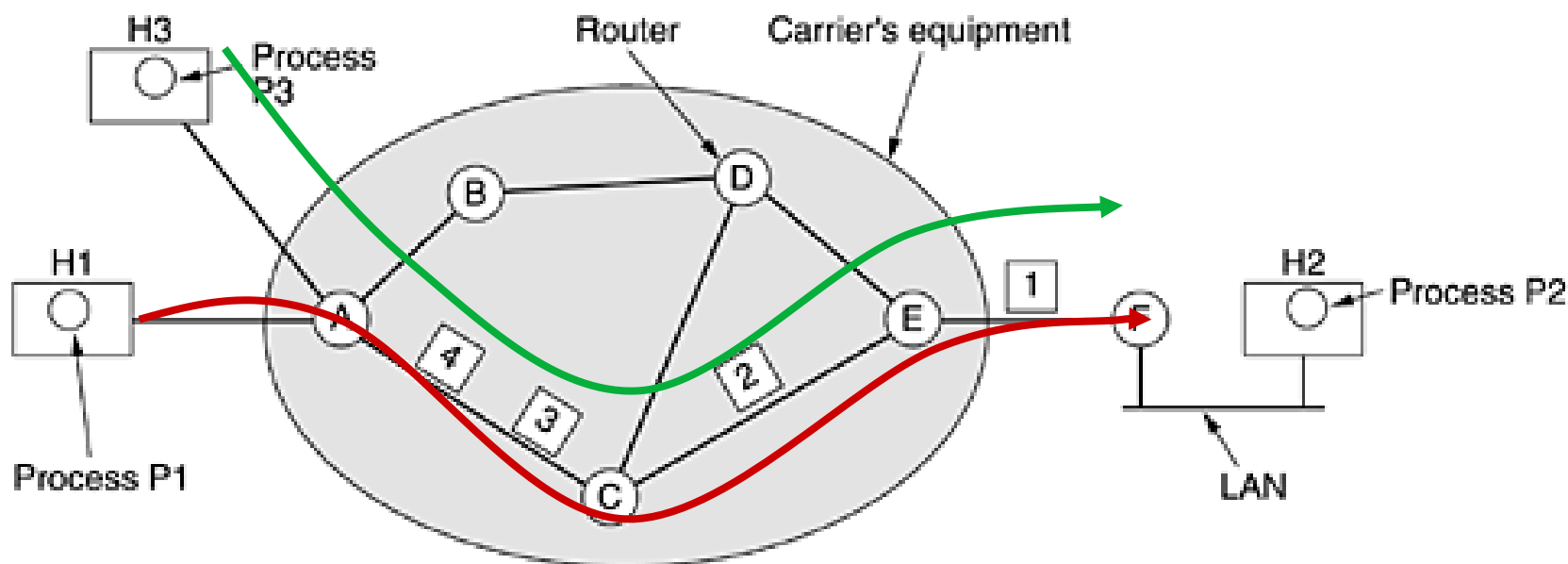


标签交换和MPLS P362

- ❑ MPLS: 多协议标签交换
- ❑ 在IP头之前增加一个MPLS头部（4字节）
- ❑ 2.5层协议



面向连接的服务-虚电路子网P277~278



A's table

H1	1	C	1
H3	1	C	2
In		Out	

C's table

A	1	E	1
A	2	E	2

E's table

C	1	F	1
C	2	F	2

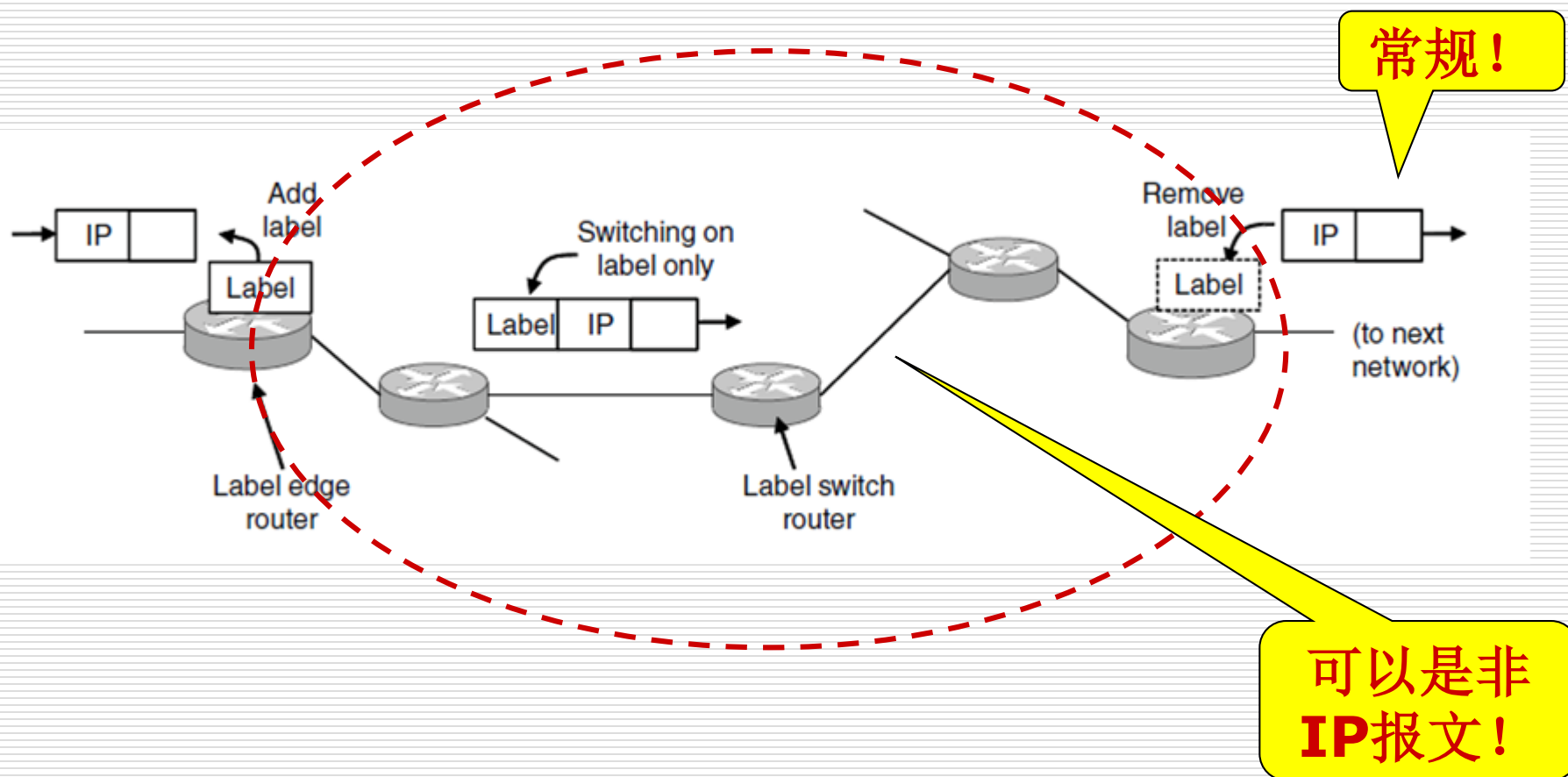
Lable Switch

MPLS跟普通的标签交换有什么区别？

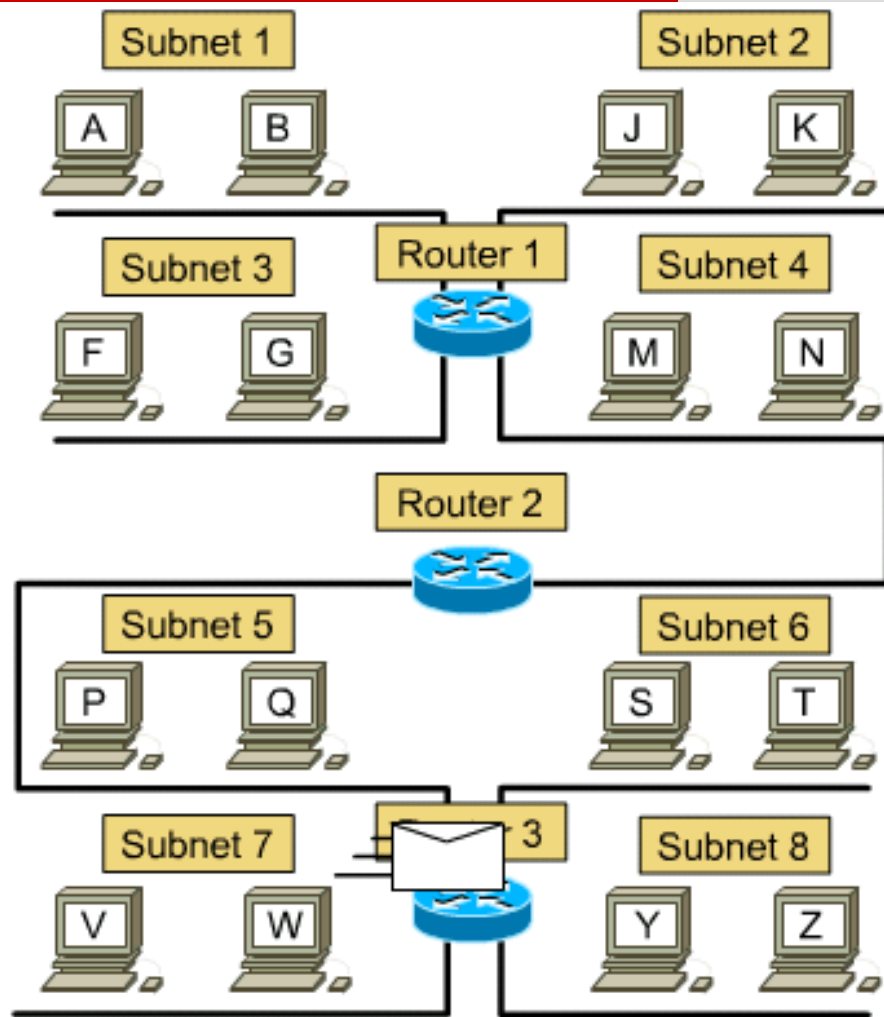
- ☐ 是否在走回头路？
- ☐ 肯定不是
- ☐ 区别
 - 聚合水平：FEC（转发等价类）
 - 多标签
 - 是否需要连接建立
 - ☐ 标签转发表由MPLS路由器建立

MPLS的工作情形

□ 标签边缘路由器



一个分组如何从源机到达目的机?



本节小结

- **CIDR的基本思想**
- **NAT/PAT的工作原理**
- **ICMP 及其应用**
- **地址解析协议**
 - **ARP**
 - **RARP**
- **IP地址的分配方式 (RARP\Boot\pDHCP)**

Thank you!



Important terms

- **Routing protocol: 路由协议**
- **Interior gateway protocol (IGP): 内部网关协议**
 - **Distance vector protocol (DV): 距离适量路由选择协议**
 - **Routing information protocol (RIP): 路由信息协议**
 - **Link state protocol (LS): 状态路由选择协议**
 - **Open Shortest Path First (OSPF): 开放最短路径优先**

Important terms (cont'd)

- ❑ **Border Gateway Protocol (BGP)：** 边界网关协议
- ❑ **Hierarchical routing：** 分层路由
- ❑ **Broadcast routing：** 广播路由
 - **reverse path forwarding (RPF)：** 逆向路径转发
- ❑ **Multicast routing：** 组播路由
- ❑ **Anycast routing：** 任播路由
- ❑ **Mobile routing：** 移动路由

Important terms (cont'd)

- Congestion control: 拥塞控制
- Quality of service (QoS): 服务质量
- traffic Shaping: 流量整形
 - leaky Bucket: 漏桶
 - token bucket: 令牌桶
- Router: 路由器
 - Routing table: 路由表

Important terms (cont'd)

- **Internet Protocol (IP) : 互联网协议**
 - **IP packet format: IP分组格式**
 - **IP address : IP地址**
- **Reserved IPv4 address: 保留的IP地址**
- **Subnetting: 子网规划**
- **Subnet mask: 子网掩码**
 - **Variable Length Subnet Mask (VLSM) : 可变长的子网掩码**
- **Dynamic Host Configure Protocol (DHCP) : 动态主机配置协议**

Important terms (cont'd)

- ❑ **Classless InterDomain Routing (CIDR)：** 无类域间路由
- ❑ **Network Address Translation (NAT)：** 网络地址翻译
 - **Port Address Translate (PAT)：** 端口地址翻译（超载，overload）
- ❑ **Internet Control Message Protocol (ICMP)：** 互联网控制协议
- ❑ **Address Resolution Protocol (ARP)：** 地址解析协议