计算机网络

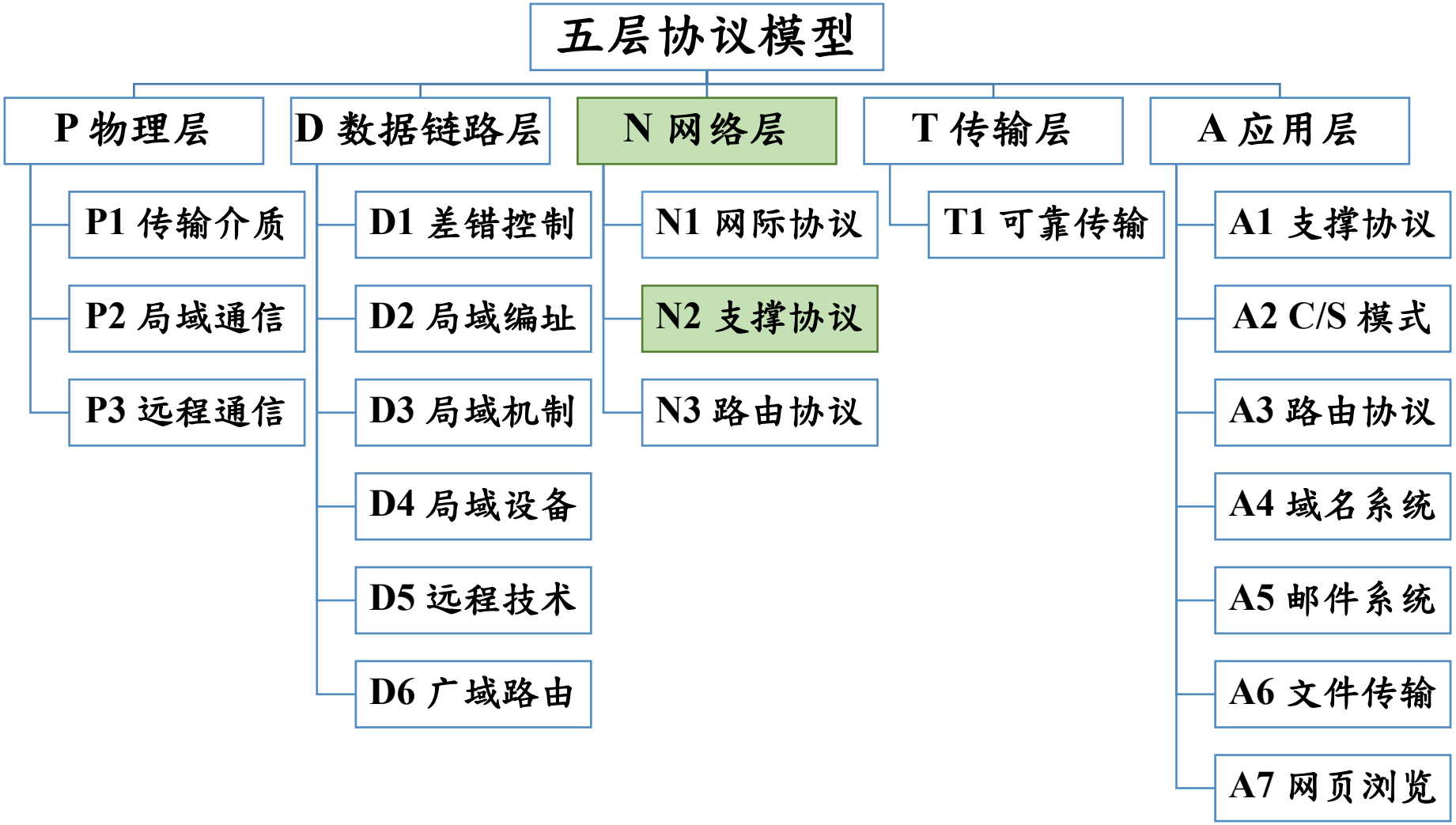
T11

IP 支撑协议和 IPv6

厦门大学信息学院软件工程系

黄炜 副教授

主要内容


五层协议模型
P 物理层
D 数据链路层
N 网络层
T 传输层
A 应用层
P1 传输介质
P2 局域通信
P3 远程通信
D1 差错控制
D2 局域编址
D3 局域机制
D4 局域设备
D5 远程技术
D6 广域路由
N1 网际协议
N2 支撑协议
N3 路由协议
T1 可靠传输
A1 支撑协议
A2 C/S 模式
A3 路由协议
A4 域名系统
A5 邮件系统
A6 文件传输
A7 网页浏览

主要内容

- ICMP协议
  - ICMP的报文种类、主要功能
  - IP与ICMP的关系
  - ping 命令测试可达性的原理
  - tracert 命令追踪路由的原理
  - 使用ICMP发现MTU
- ARP协议
  - 地址解析，地址解析的方法

主要内容

- 支撑协议与技术
  - DHCP、私有地址和NAT技术
- IPv6
  - IPv4地址的瓶颈
  - 地址格式

对应课本章节

- **PART IV Internetworking**
  - **Chapter 23 Support Protocols And Technologies**
  - **Chapter 24 The Future IP (IPv6)**

1. 差错报告机制

Internet控制报文协议（ ICMP ）

- Internet控制报文协议（ ICMP ）
  - Internet Control Message Protocol
  - 目的：提高 IP 数据报交付成功的机会。
  - 协议层：网络层
- 机制
  - 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 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。

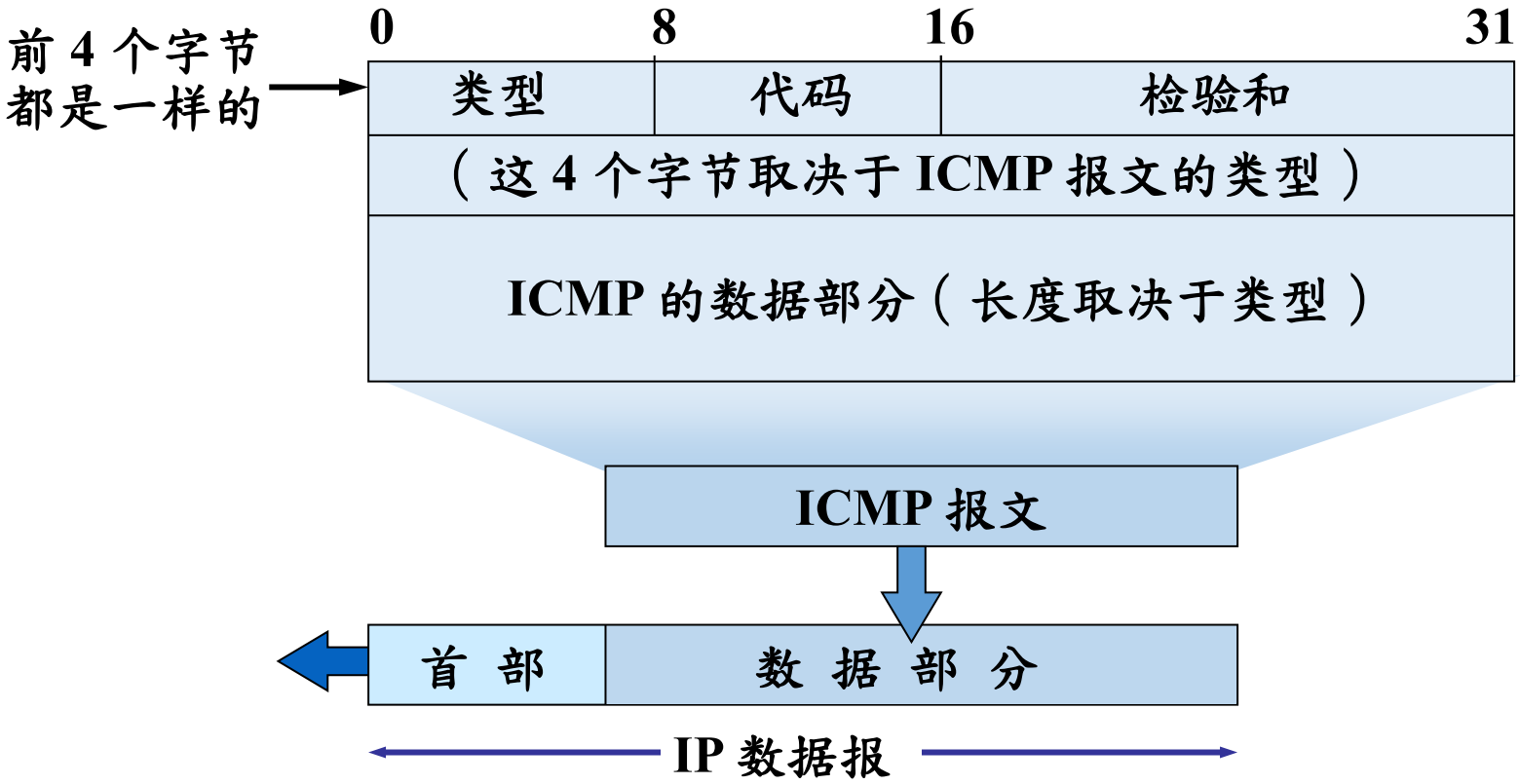
ICMP 错误报文与信息报文

- **ICMP 报文的种类**
  - 差错报告报文 和 询问报文。

报文种类	类型值	说明
差错报告报文 Error Messages	3	目的不可达
	4	源站抑制（ Source Quench ）
	11	超时（ Time Exceeded ）
	12	参数问题（ Parameter Problem ）
	5	重定向（ Redirect ）
询问报文 Informational Messages	8 / 0	回应请求/应答（ Echo Request/Reply ）
	13 / 14	时间戳请求/应答（ Timestamp Request/Reply ）
	17 / 18	地址掩码请求/应答（ Address Mask Request/Reply ）
	10 / 9	路由器请求/通告（ Router Solicitation / Advertisement ）

ICMP 报文格式

- ICMP 报文格式



ICMP 询问报文：目的请求

```
Ethernet Type 2
  Destination:          00:50:56:FC:52:95  VMware:FC:52:95  [0-5]
  Source:               00:0C:29:17:29:CA  VMware:17:29:CA  [6-11]
  Protocol Type:        0x0800  IP  [12-13]
IP Version 4 Header - Internet Protocol Datagram
  Version:              4  [14 Mask 0xF0]
  Header Length:        5  (20 bytes)  [14 Mask 0x0F]
...

  Fragment Offset:      0  (0 bytes)  [20-21 Mask 0x1FFF]
  Time To Live:         128  [22]
  Protocol:             1  ICMP - Internet Control Message Protocol  [23]
  Header Checksum:      0x0000  Checksum invalid. Should be:  0x1128  [24-25]
  Source IP Address:    192.168.7.4  [26-29]
  Dest. IP Address:     123.125.114.144  [30-33]
ICMP - Internet Control Messages Protocol
  ICMP Type:            8  Echo Request  [34]
  ICMP Code:            0  [35]
  ICMP Checksum:        0x4D5A  [36-37]
  Identifier:           0x0001  [38-39]
  Sequence Number:      1  [40-41]
  ICMP Data Area:       abcdefghijklmnopqrstuvwabcdefghi  [42-73]
```

ICMP 询问报文：目的应答

```
Ethernet Type 2
  Destination:          00:0C:29:17:29:CA  VMware:17:29:CA  [0-5]
  Source:               00:50:56:FC:52:95  VMware:FC:52:95  [6-11]
  Protocol Type:        0x0800  IP  [12-13]
IP Version 4 Header - Internet Protocol Datagram
  Version:              4  [14 Mask 0xF0]
  Header Length:        5  (20 bytes)  [14 Mask 0x0F]
...

  Fragment Offset:      0  (0 bytes)  [20-21 Mask 0x1FFF]
  Time To Live:         128  [22]
  Protocol:             1  ICMP - Internet Control Message Protocol  [23]
  Header Checksum:      0xB747  [24-25]
  Source IP Address:    123.125.114.144  [26-29]
  Dest. IP Address:     192.168.7.4  [30-33]
ICMP - Internet Control Messages Protocol
  ICMP Type:            0  Echo Reply  [34]
  ICMP Code:            0  [35]
  ICMP Checksum:        0x555A  [36-37]
  Identifier:           0x0001  [38-39]
  Sequence Number:      1  [40-41]
  ICMP Data Area:       abcdefghijklmnopqrstuvwabcdefghi  [42-73]
```

ICMP 差错报告报文：超时

```
Ethernet Type 2
  Destination:          00:0C:29:17:29:CA  VMware:17:29:CA  [0-5]
  Source:               00:50:56:FC:52:95  VMware:FC:52:95  [6-11]
  Protocol Type:        0x0800  IP  [12-13]
IP Version 4 Header - Internet Protocol Datagram
  Version:              4  [14 Mask 0xF0]
  Header Length:        5  (20 bytes)  [14 Mask 0x0F]
...

  Fragment Offset:      0  (0 bytes)  [20-21 Mask 0x1FFF]
  Time To Live:         128  [22]
  Protocol:             1  ICMP - Internet Control Message Protocol  [23]
  Header Checksum:      0x8288  [24-25]
  Source IP Address:    192.168.7.2  [26-29]
  Dest. IP Address:     192.168.7.4  [30-33]
ICMP - Internet Control Messages Protocol
  ICMP Type:            11  Time Exceeded  [34]
  ICMP Code:            0  Time to Live count exceeded  [35]
  ICMP Checksum:        0xF4FF  [36-37]
  Unused (must be zero):0x00000000  [38-41]
```

ICMP 差错报告报文：超时

```
Header of packet that caused error follows.
IP Version 4 Header - Internet Protocol Datagram
  Version:              4  [42 Mask 0xF0]
  Header Length:        5  (20 bytes)  [42 Mask 0x0F]
...

  Fragment Offset:      0  (0 bytes)  [48-49 Mask 0x1FFF]
  Time To Live:         1  [50]
  Protocol:             1  ICMP - Internet Control Message Protocol  [51]
  Header Checksum:      0x1C3F  [52-53]
  Source IP Address:    192.168.7.4  [54-57]
  Dest. IP Address:     210.34.0.12  [58-61]
ICMP - Internet Control Messages Protocol
  ICMP Type:            8  Echo Request  [62]
  ICMP Code:            0  [63]
  ICMP Checksum:        0xF7F7  [64-65]
  Identifier:           0x0001  [66-67]
  Sequence Number:      7  [68-69]
  ICMP Data
Area:       ..................................................  [70-133]
```

ICMP 差错报告报文

- 不应发送 ICMP 差错报告报文的几种情况
  - 对 ICMP 差错报告报文不再发送 ICMP 差错报告报文。
  - 对第一个分片的数据报片的所有后续数据报片都不发送 ICMP 差错报告报文。
  - 对具有多播地址的数据报都不发送 ICMP 差错报告报文。
  - 对具有特殊地址（如127.0.0.0 或 0.0.0.0）的数据报不发送 ICMP 差错报告报文。

ping 使用ICMP消息测试可达性

- PING（Packet Internet Groper），因特网包探索器
- 报文类型：ICMP回送请求和回送回复消息。
  - 把包含ICMP回送请求消息的IP数据报发送到指定的目的地。
  - 每当一个回送请求到达，ICMP软件必须发送一个回送应答。
- ping 是应用层直接使用网络层 ICMP 的例子
  - 它没有通过传输层的 TCP 或UDP。

tracert 使用ICMP追踪路由器

- 每个路由器处理生存周期（TIME TO LIVE）计数器。
  - traceroute 程序发送一系列数据报，等待每一个响应
  - 如果计数器达到零，则路由器丢弃数据报，并将ICMP超时错误发送回源。
  - traceroute 不断增加 TTL 值，直到该值足够大到数据报到达其最终目标。
  - 发送ICMP回送请求消息；目标主机将生成ICMP回送应答。
  - 将数据报发送给不存在的应用程序；目标主机将生成ICMP目的地无法到达的消息。

相关命令行程序（Windows为例）

- Ping
  - 因特网分组测程序（Packet Internet Groper）
- Tracert
  - 跟踪路由（Trace Router）
- Route
  - 路由（Route）
- 高级用法，请进入控制台，输入：XXXX /?

检查网络是否连通

```
C:\Windows\system32>ping www.xmu.edu.cn

正在 Ping www.xmu.edu.cn [210.34.0.12] 具有 32 字节的数据:
来自 210.34.0.12 的回复: 字节=32 时间=1ms TTL=128
来自 210.34.0.12 的回复: 字节=32 时间=1ms TTL=128
来自 210.34.0.12 的回复: 字节=32 时间=1ms TTL=128
来自 210.34.0.12 的回复: 字节=32 时间=1ms TTL=128

210.34.0.12 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms，最长 = 1ms，平均 = 1ms
```

操作网络路由表

```
C:\Windows\system32>route print -4
===========================================================
IPv4 路由表
===========================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0      192.168.7.2    192.168.7.132     10
        127.0.0.0        255.0.0.0         在链路上         127.0.0.1    306
        127.0.0.1  255.255.255.255         在链路上         127.0.0.1    306
  127.255.255.255  255.255.255.255         在链路上         127.0.0.1    306
      192.168.7.0    255.255.255.0         在链路上    192.168.7.132    266
    192.168.7.132  255.255.255.255         在链路上    192.168.7.132    266
    192.168.7.255  255.255.255.255         在链路上    192.168.7.132    266
        224.0.0.0        240.0.0.0         在链路上         127.0.0.1    306
        224.0.0.0        240.0.0.0         在链路上    192.168.7.132    266
  255.255.255.255  255.255.255.255         在链路上         127.0.0.1    306
  255.255.255.255  255.255.255.255         在链路上    192.168.7.132    266
===========================================================================
永久路由:
  无
```

搜索目标的跃点数

```
C:\Windows\system32>tracert www.xmu.edu.cn

通过最多 30 个跃点跟踪
到 www.xmu.edu.cn [210.34.0.12] 的路由:

  1    <1 毫秒    1 ms    12 ms  192.168.7.2
  2     *         *        *     请求超时。
  3     *         *        *     请求超时。
  4     *         *        *     请求超时。
  5     1 ms      1 ms     1 ms  210.34.0.12

跟踪完成。
```

使用ICMP发现路径MTU

- 路径MTU发现
  - RFC1191使用分段标志中的“不能分段”来要求中间路由器在发现包太长时返回一个ICMP出错报文。
  - 尽管大多数的系统不支持路径MTU发现功能，但可以很容易地修改traceroute程序，用它来确定路径MTU。
  - 发送的第一个分组的长度正好与出口MTU相等，每次收到“不能分片”差错时就减小分组的长度。如果路由器发送的ICMP差错报文是新格式，包含出口的MTU，那么就用该MTU值来发送，否则就用下一个最小的MTU值来发送。

2. 地址解析协议

地址解析（Address Resolution）

- 将IP地址解析为MAC地址的叫做地址解析
  - IP是虚拟的，但数据链路层需要物理地址，最终要换的
- 地址解析协议（Address Resolution Protocol，ARP）
- 概念地址边界
  - IP地址、物理地址

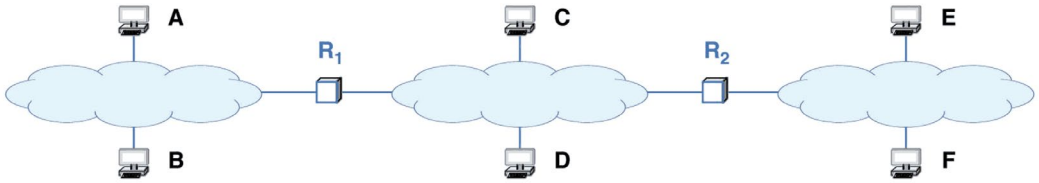


Figure 23.1 An example internet of three networks and computers connected to each.

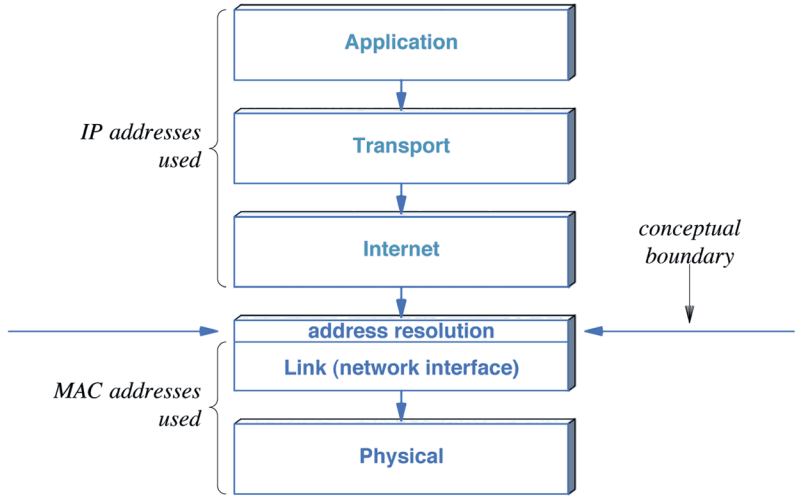
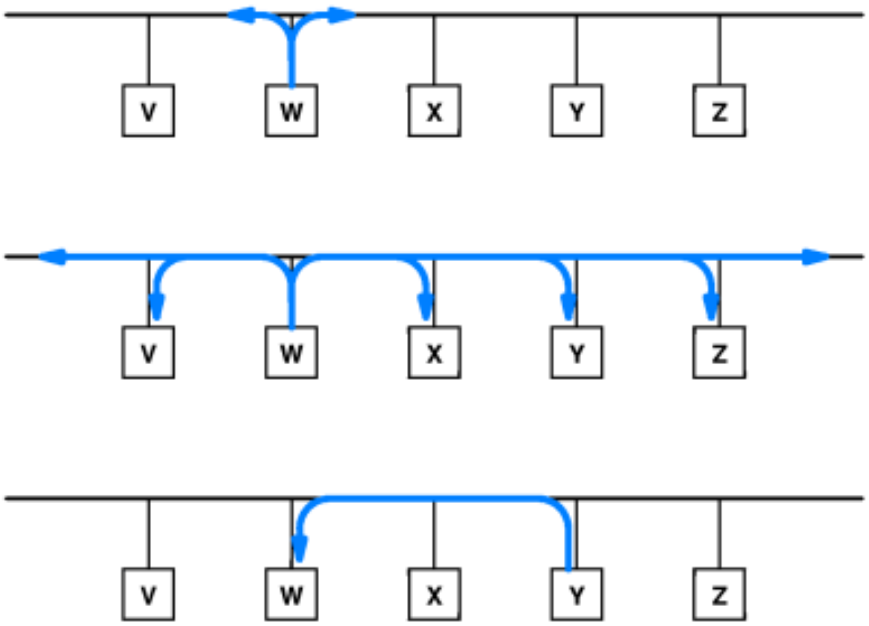


Figure 23.5 Illustration of the boundary between the use of IP addresses and MAC addresses.

地址解析技术

- 不管网络层使用的是什么协议，在实际网络的链路上传送数据帧时，最终还是必须使用硬件地址。
- ARP标准定义了请求与响应



地址解析技术分类

- 查表（Table lookup）
  - 存储在内存表。
- 相近形式计算
  - 配置使得硬件地址可通过简单的布尔和算术运算得出对应的协议地址。
- 消息交换
  - 一台计算机发出某个地址联编的请求消息后，另一台计算机返回一个包含所需信息的应答消息。

使用 ARP 的四种典型情况

- 主机发送数据报到本网络上的另一台主机。
  - 找到目的主机的硬件地址。
- 主机发送数据报到另一个网络上的一台主机。
  - 找到本网络上一个路由器的硬件地址。由该路由器转发。
- 路由器转发数据报到本网络上的一台主机。
  - 找到目的主机的硬件地址。
- 路由器转发数据报到另一个网络上的一台主机。
  - 找到本网络上另一个路由器的硬件地址。由该路由器转发。

ARP 消息格式

- **ARP帧格式**

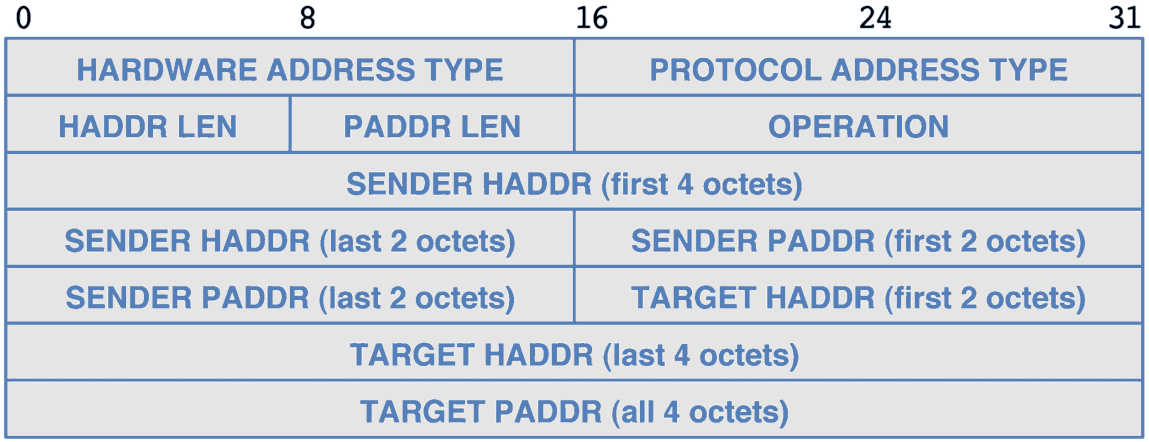


Figure 23.3 The format for an ARP message when binding an IPv4 address to an Ethernet address.

- **ARP 封装**
  - **帧类型: 0x0806**

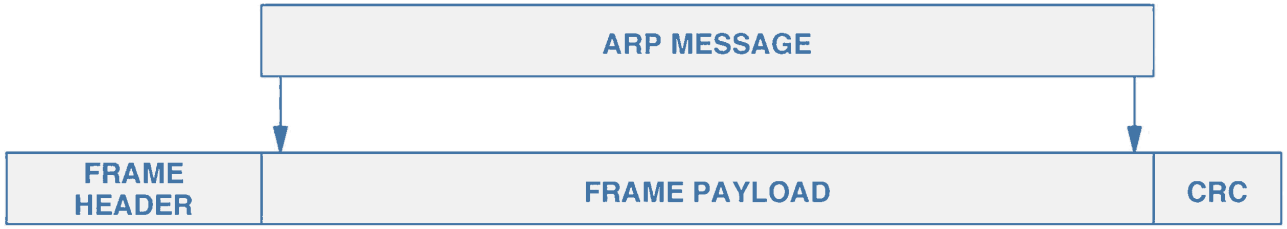


Figure 23.4 Illustration of ARP encapsulation in an Ethernet frame.

ARP路由表

```
C:\Windows\system32>arp -a

接口: 192.168.33.3 --- 0xd
  Internet 地址          物理地址                类型
  192.168.33.6           f8-b1-56-b5-39-bc     动态
  192.168.33.14          9c-21-6a-f6-82-6d     动态
  224.0.0.22             01-00-5e-00-00-16     静态

接口: 192.168.1.1 --- 0x12
  Internet 地址          物理地址                类型
  224.0.0.22             01-00-5e-00-00-16     静态

接口: 169.254.0.1 --- 0x13
  Internet 地址          物理地址                类型
  224.0.0.22             01-00-5e-00-00-16     静态
```

ARP 消息格式

```
Packet Info
  Packet Number:          1
  Flags:                  0x00000000
  Status:                 0x00000000
  Packet Length:          64
  Timestamp:              14:17:23.430079000 04/11/2014
Ethernet Type 2
  Destination:            FF:FF:FF:FF:FF:FF  Ethernet Broadcast  [0-5]
  Source:                 00:0C:29:17:29:CA  VMware:17:29:CA  [6-11]
  Protocol Type:          0x0806  IP ARP  [12-13]
ARP - Address Resolution Protocol
  Hardware:               1  Ethernet (10Mb)  [14-15]
  Protocol:               0x0800  IP  [16-17]
  Hardware Addr Length: 6  [18]
  Protocol Addr Length: 4  [19]
  Operation:              1  ARP Request  [20-21]
  Sender Hardware Addr: 00:0C:29:17:29:CA  VMware:17:29:CA  [22-27]
  Sender Internet Addr: 192.168.7.4  [28-31]
  Target Hardware Addr: 00:00:00:00:00:00  Xerox:00:00:00  (ignored)  [32-37]
  Target Internet Addr: 192.168.7.2  [38-41]
Extra bytes
  Number of bytes:
  ................  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  [42-57]
  ..                00 00  [58-59]
```

ARP 消息格式

```
Packet Info
  Packet Number:          2
  Flags:                  0x00000000
  Status:                 0x00000000
  Packet Length:          64
  Timestamp:              14:17:23.516605000 04/11/2014
Ethernet Type 2
  Destination:            00:0C:29:17:29:CA  VMware:17:29:CA  [0-5]
  Source:                 00:50:56:FC:52:95  VMware:FC:52:95  [6-11]
  Protocol Type:          0x0806  IP ARP  [12-13]
ARP - Address Resolution Protocol
  Hardware:               1  Ethernet (10Mb)  [14-15]
  Protocol:               0x0800  IP  [16-17]
  Hardware Addr Length: 6  [18]
  Protocol Addr Length: 4  [19]
  Operation:              2  ARP Response  [20-21]
  Sender Hardware Addr: 00:50:56:FC:52:95  VMware:FC:52:95  [22-27]
  Sender Internet Addr: 192.168.7.2  [28-31]
  Target Hardware Addr: 00:0C:29:17:29:CA  VMware:17:29:CA  [32-37]
  Target Internet Addr: 192.168.7.4  [38-41]
Extra bytes
  Number of bytes:
  ................  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  [42-57]
  ..                00 00  [58-59]
```

应当注意的问题

- ARP 解决同一局域网上的IP和硬件地址的映射问题。
  - 如果目标主机和源主机不在同一个局域网，则通过 ARP 找到位于本局域网上的某个路由器的硬件地址，把分组发送给这个路由器转发给下一个网络。直到同一局域网。
  - 从IP地址到硬件地址的解析是对用户是透明的。
  - 只要主机或路由器要和本网络上的另一个已知 IP 地址的主机或路由器进行通信，ARP 协议就会自动地将该 IP 地址解析为链路层所需要的硬件地址。

ARP欺骗

- ARP欺骗的核心思想
  - 向目标主机发送伪造的ARP应答，并使目标主机接收应答中伪造的IP地址与MAC地址之间的映射对，以此更新目标主机ARP缓存。
- ARP欺骗的防范
  - S代表源主机，被欺骗的目标主机；D代表目的主机，S本来向它发送数据；A代表攻击者，进行ARP欺骗。

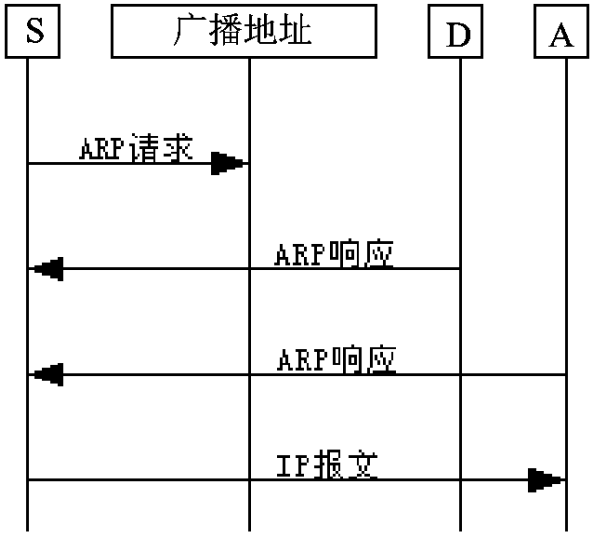


图1 实施ARP欺骗的过程

ARP高速缓存（ARP Cache）

- 局域网各主机和路由器的IP 地址到硬件地址的映射表。
  - 当主机 A 欲向本局域网上的某个主机 B 发送 IP 数据报时，就先在其 ARP 高速缓存中查看有无主机 B 的 IP 地址。如有，就可查出其对应的硬件地址，再将此硬件地址写入 MAC 帧，然后通过局域网将该 MAC 帧发往此硬件地址。
  - 为了减少网络上的通信量，主机 A 在发送其 ARP 请求分组时，就将其 IP 地址到硬件地址的映射写入 ARP 请求分组。
  - 当主机 B 收到 A 的 ARP 请求分组时，就将主机 A 的这一地址映射写入主机 B 自己的 ARP 高速缓存中。

3. 动态主机配置协议

IP地址哪里来

- 向ISP购买一个（或段）IP的使用权
- 大量设备如何使用有限的地址上网
  - DHCP服务：“时分多路复用”，轮流使用IP地址
  - NAT、NAPT服务：“频分多路复用”，共用一个IP地址

动态主机配置协议（DHCP）

- 早期：反向地址解析协议（RARP）
- 作用：从服务器获得IP地址。
- 已知条件
  - 本地机器：没有IP（本机IP：0.0.0.0；MAC已知）
  - 目的机器：有IP但不知道（目的IP、MAC，全1广播）
- DHCP获得的IP地址有租期，可附加其他配置
- DHCP提供一个好心的服务（防君子不防小人）

监听结果

- 用Omnipeek软件解析DHCP包
  - 拔出网线，开软件，勾选DHCP，插入网线，再解析

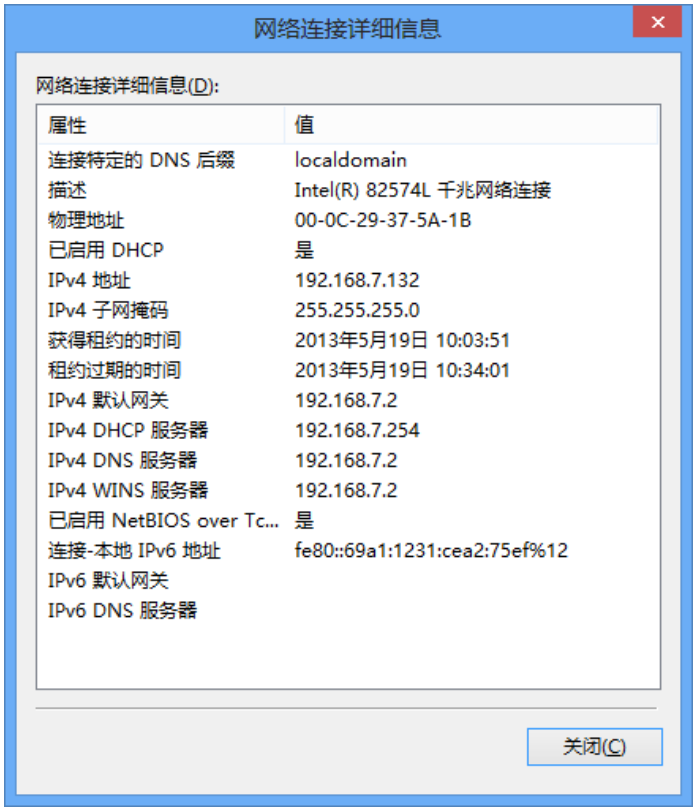
ID	Src. Logical	Src. Physical	Src. Port	Dest. Log.	Dest. Phy.	Dest. Prt.	Summary	Expert
1	0.0.0.0	00:0C:29:37:5A:1B	UDP 68	255.255.255.255	FF:FF:FF:FF:FF:FF	UDP 67	C DISCOVER 192.168.7.132 WIN-KG9CLM76UIA	
2	192.168.7.254	00:50:56:E2:AF:04	UDP 67	192.168.7.132	00:0C:29:37:5A:1B	UDP 68	R OFFER 192.168.7.132	
3	0.0.0.0	00:0C:29:37:5A:1B	UDP 68	255.255.255.255	FF:FF:FF:FF:FF:FF	UDP 67	C REQUEST 192.168.7.132 WIN-KG9CLM76UIA	
4	192.168.7.254	00:50:56:E2:AF:04	UDP 67	192.168.7.132	00:0C:29:37:5A:1B	UDP 68	R ACK	DHCP Low Lease Time (30 minutes, threshold=30 minutes)

监听结果节选

```
Packet #1
Ethernet Type 2
  Destination:          FF:FF:FF:FF:FF:FF  Ethernet Broadcast  [0-5]
  Source:               00:0C:29:37:5A:1B  VMware:37:5A:1B  [6-11]
  Protocol Type:        0x0800  IP  [12-13]
IP Version 4 Header - Internet Protocol Datagram
  Version:              4  [14 Mask 0xF0]
  Protocol:             17  UDP  [23]
  Source IP Address:    0.0.0.0  [26-29]
  Dest. IP Address:     255.255.255.255  IP Broadcast  [30-33]
UDP - User Datagram Protocol
  Source Port:          68  bootpc  [34-35]
  Destination Port:     67  bootps  [36-37]
BootP - Bootstrap Protocol
  IP Address Known By Client:   0.0.0.0  IP Address Not Known By Client  [54-57]
  Client IP Addr Given By Srvr: 0.0.0.0  [58-61]
  Server IP Address:            0.0.0.0  [62-65]
  Gateway IP Address:           0.0.0.0  [66-69]
  Client Hardware Addr:         00:0C:29:37:5A:1B  VMware:37:5A:1B  [70-75]
DHCP - Dynamic Host Configuration Protocol
Requested IP Address
  Address:              192.168.7.132  [296-299]
Host Name Address
  String:               WIN-KG9CLM76UIA  [302-316]
```

DHCP的配置

- Windows提供DHCP Client服务



4. 网络地址转换

网络地址转换（NAT）

- NAT应用场景
  - 多台主机上网，但是只有一个公网IP地址
- NAT动机：IP地址紧张，端口号并不紧张

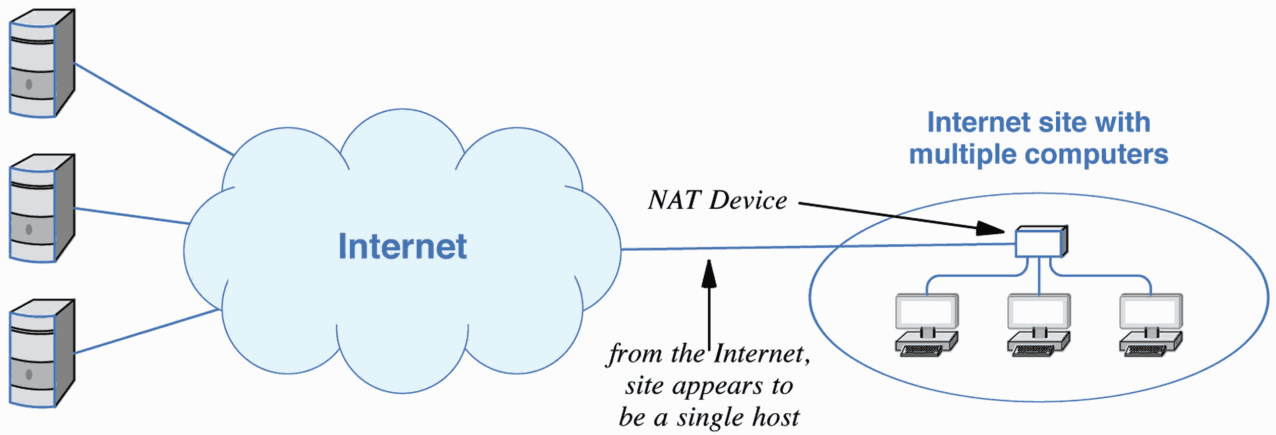


Figure 23.9 The conceptual architecture used with NAT.

私有地址

- 目的：虚拟的寻址机制
  - NAT的目的是提供一种错觉。
- NAT使用的私有地址块

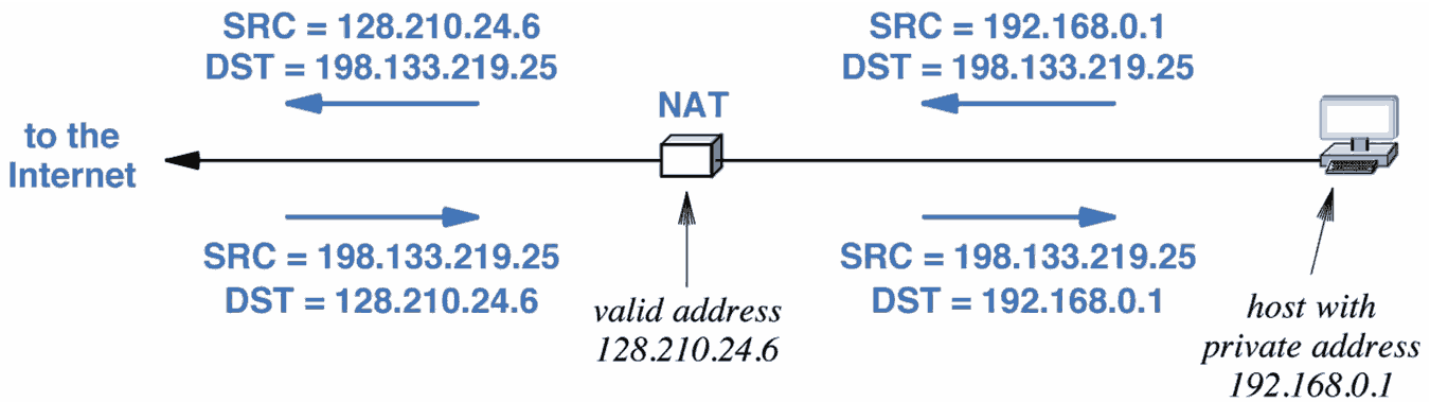
网络号	类	个数	说明
10.0.0.0/8	A	1	
169.254.0.0/16	B	1	一般开启DHCP客户端又无法获取到IP时使用
172.16.0.0/12	B	16	
192.168.0.0/16	C	256	

- 防止IP冲突，私有地址不被路由

NAT的地址转换

- NAT的最基本形式将数据报中的IP源地址由站点替换为Internet，并且将IP目的地址由Internet替换为站点

Direction	Field	Old Value	New Value
out	IP Source	192.168.0.1	128.210.24.6
	IP Destination	198.133.219.25	-- no change --
in	IP Source	198.133.219.25	-- no change --
	IP Destination	128.210.24.6	192.168.0.1



传输层的NAT（NAPT）

- 传输层的特别之处：端口号
- 端口号也参与转换
  - 因为终究是主机上的应用在上网
- NAT有时候也用于负载均衡

Dir.	Fields	Old Value	New Value
out	IP SRC:TCP SRC	192.168.0.1 :30000	128.10.24.6 :40001
out	IP SRC:TCP SRC	192.168.0.2 :30000	128.10.24.6 :40002
in	IP DEST:TCP DEST	128.10.19.20 :40001	192.168.0.1 :30000
in	IP DEST:TCP DEST	128.10.19.20 :40002	192.168.0.2 :30000

FTP Login (VMWare)

```
  Timestamp:            21:00:57.444125300 04/11/2014
Ethernet Type 2
  Destination:          00:50:56:FC:52:95  VMware:FC:52:95  [0-5]
  Source:               00:0C:29:17:29:CA  VMware:17:29:CA  [6-11]
  Protocol Type:        0x0800  IP  [12-13]
IP Version 4 Header - Internet Protocol Datagram
...
  Fragment Offset:      0  (0 bytes)  [20-21 Mask 0x1FFF]
  Time To Live:         128  [22]
  Protocol:             6  TCP - Transmission Control Protocol  [23]
  Header Checksum:      0x0000  Checksum invalid. Should be:  0xB059  [24-25]
  Source IP Address:    192.168.7.4  [26-29]
  Dest. IP Address:     59.77.7.25  [30-33]
TCP - Transport Control Protocol
  Source Port:          4425  netrockey6  [34-35]
  Destination Port:     21  ftp  [36-37]
  Sequence Number:      1304971726  [38-41]
  Ack Number:           1171416600  [42-45]
  TCP Offset:           5  (20 bytes)  [46 Mask 0xF0]
...
FTP Control - File Transfer Protocol
  Line  1:              USER student<CR><LF>  [54-65]
```

FTP Login (NAT)

```
  Timestamp:            21:00:57.764403200 04/11/2014
Ethernet Type 2
  Destination:          3C:E5:A6:D0:**:**  HangzhouH3:D0:**:**  [0-5]
  Source:               F8:B1:56:B5:**:**  [6-11]
  Protocol Type:        0x0800  IP  [12-13]
IP Version 4 Header - Internet Protocol Datagram
...
  Fragment Offset:      0  (0 bytes)  [20-21 Mask 0x1FFF]
  Time To Live:         128  [22]
  Protocol:             6  TCP - Transmission Control Protocol  [23]
  Header Checksum:      0x0000  Checksum invalid. Should be:  0x0B26  [24-25]
  Source IP Address:    59.77.5.***  [26-29]
  Dest. IP Address:     59.77.7.25  [30-33]
TCP - Transport Control Protocol
  Source Port:          10405  [34-35]
  Destination Port:     21  ftp  [36-37]
  Sequence Number:      2633766987  [38-41]
  Ack Number:           300260607  [42-45]
  TCP Offset:           5  (20 bytes)  [46 Mask 0xF0]
...
FTP Control - File Transfer Protocol
  Line  1:              USER student<CR><LF>  [54-65]
```

FTP Response (NAT)

```
  Timestamp:            21:00:57.764979200 04/11/2014
Ethernet Type 2
  Destination:          F8:B1:56:B5:**:**  [0-5]
  Source:               3C:E5:A6:D0:**:**  HangzhouH3:D0:**:**  [6-11]
  Protocol Type:        0x0800  IP  [12-13]
IP Version 4 Header - Internet Protocol Datagram
...
  Fragment Offset:      0  (0 bytes)  [20-21 Mask 0x1FFF]
  Time To Live:         63  [22]
  Protocol:             6  TCP - Transmission Control Protocol  [23]
  Header Checksum:      0xB59D  [24-25]
  Source IP Address:    59.77.7.25  [26-29]
  Dest. IP Address:     59.77.5.***  [30-33]
TCP - Transport Control Protocol
  Source Port:          21  ftp  [34-35]
  Destination Port:     10405  [36-37]
  Sequence Number:      300260607  [38-41]
  Ack Number:           2633767001  [42-45]
  TCP Offset:           5  (20 bytes)  [46 Mask 0xF0]
...
FTP Control - File Transfer Protocol
  Line  1:              331 User name okay, need password.<CR><LF>  [54-87]
```

FTP Response (VMWare)

```
  Timestamp:            21:00:57.444794300 04/11/2014
Ethernet Type 2
  Destination:          00:0C:29:17:29:CA  VMware:17:29:CA  [0-5]
  Source:               00:50:56:FC:52:95  VMware:FC:52:95  [6-11]
  Protocol Type:        0x0800  IP  [12-13]
IP Version 4 Header - Internet Protocol Datagram
...
  Fragment Offset:      0  (0 bytes)  [20-21 Mask 0x1FFF]
  Time To Live:         128  [22]
  Protocol:             6  TCP - Transmission Control Protocol  [23]
  Header Checksum:      0xF389  [24-25]
  Source IP Address:    59.77.7.25  [26-29]
  Dest. IP Address:     192.168.7.4  [30-33]
TCP - Transport Control Protocol
  Source Port:          21  ftp  [34-35]
  Destination Port:     4425  netrockey6  [36-37]
  Sequence Number:      1171416600  [38-41]
  Ack Number:           1304971740  [42-45]
  TCP Offset:           5  (20 bytes)  [46 Mask 0xF0]
...
FTP Control - File Transfer Protocol
  Line  1:              331 User name okay, need password.<CR><LF>  [54-87]
```

5. 未来的IP：IPv6

IPv6的产生

- 2011年2月3日IPv4的42亿地址分配用尽。
- IP的瓶颈

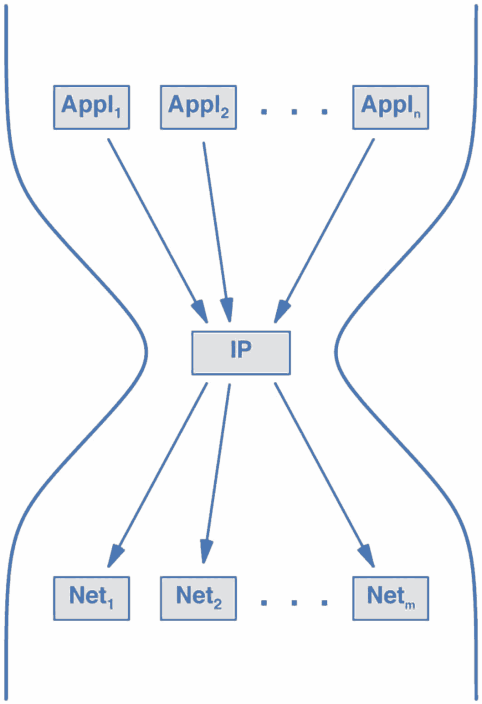


Figure 24.1 The hourglass model of Internet communication with IP at the center.

IPv6的特点

- 地址空间：128位
- 头部格式：新的头部
- 扩展头部：不同信息编码到不同头部中
  - 经济性、可扩展性
- 支持实时业务：允许底层网络建立高质量通路
- 可扩充的协议：允许在数据报添加额外的信息

IPv6数据报格式

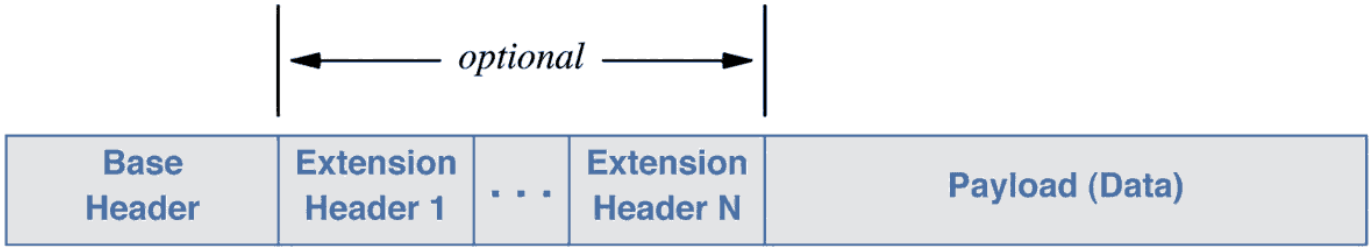


Figure 24.2 The general form of an IPv6 datagram.

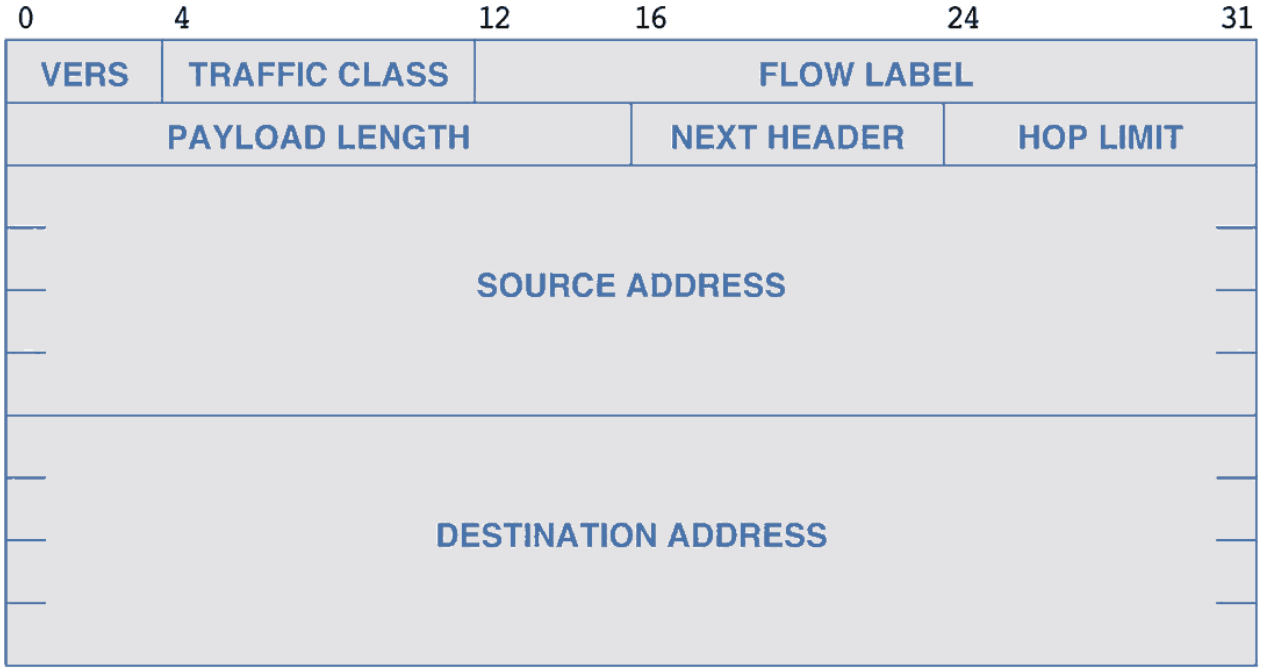


Figure 24.3 The format of the base header in an IPv6 datagram.

IPv6地址

- 冒分十六进制数表示法（兼容CIDR表示法）
  - 按16位一组，以冒号分隔每个组
    - 2001:0db8:85a3:0000:0000:8a2e:0370:7334
  - 前导0压缩：0db8写成db8
  - 零压缩：两个冒号代替连续出现两个以上的零，最多1次
    - 2001:db8:85a3::8a2e:370:7334
  - IPv4扩展到IPv6
    - ::ffff:0:0/96前缀

计算机网络

T11

谢谢

厦门大学信息学院软件工程系

黄炜 副教授