计算机网络

12.

IP Support Protocols, and UDP

厦門大學

止於至善

UNIVERSITAS AMOIENSIS

厦门大学软件学院

黄炜 助理教授

IP支撑协议

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

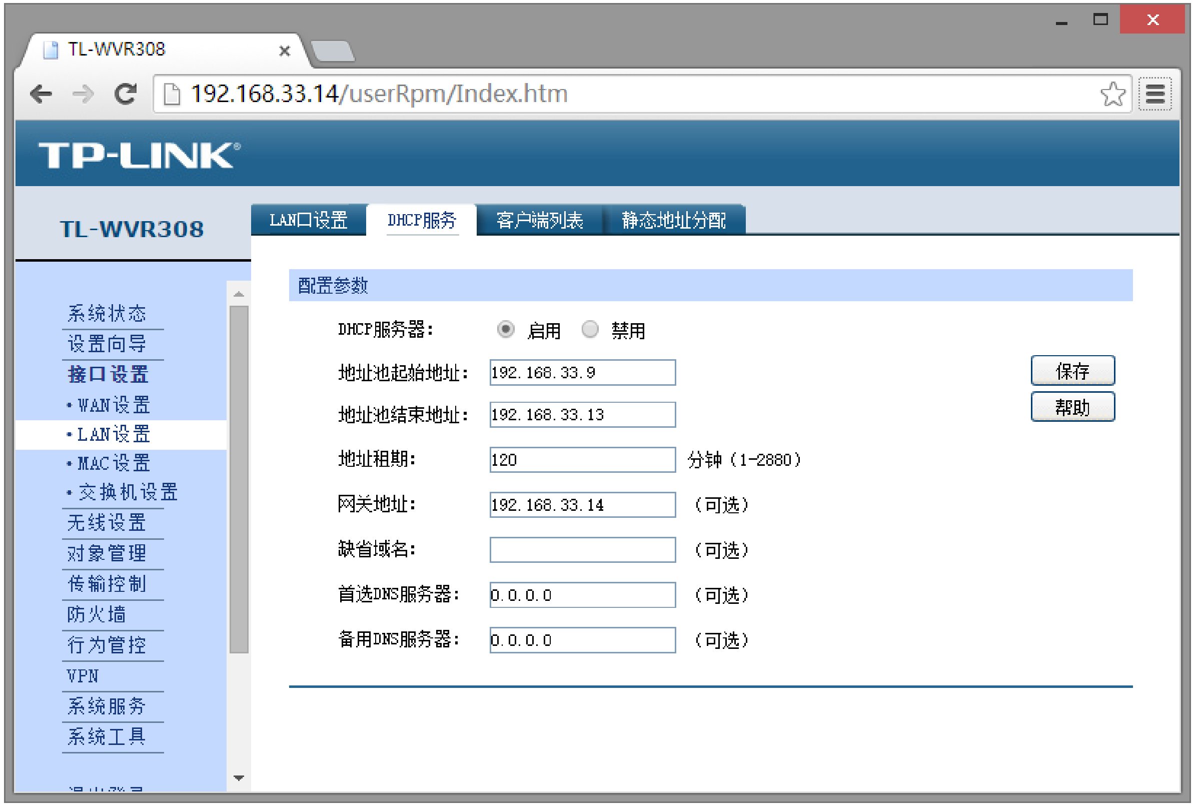
ID	Src. Logical	Src. Physical	Src. Port	Dest. Log.	Dest. Phy.	Dest. Prt.	Summary	Expert
1	0.0.0.0	00:0C:29:37:5A:1B	UDP 68	255.255.255.255	FF:FF:FF:FF:FF:FF	UDP 67	C DISCOVER 192.168.7.132 WIN-KG9CLM76UIA	
2	192.168.7.254	00:50:56:E2:AF:04	UDP 67	192.168.7.132	00:0C:29:37:5A:1B	UDP 68	R OFFER 192.168.7.132	
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]
```

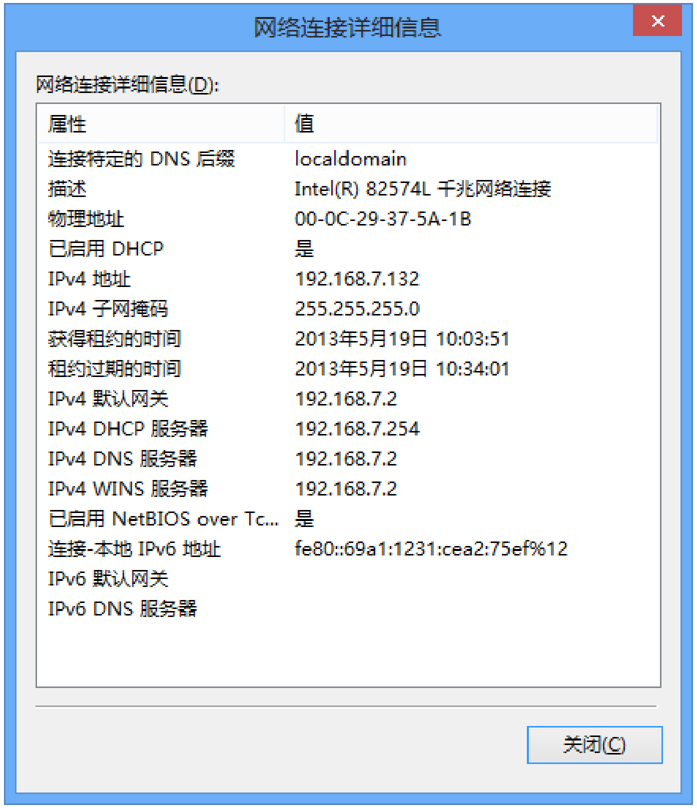
DHCP的配置

- **Windows提供DHCP Client服务**



配置参数

DHCP服务器：	● 启用 ○ 禁用	
地址池起始地址：	192.168.33.9	
地址池结束地址：	192.168.33.13	
地址租期：	120	分钟（1-2880）
网关地址：	192.168.33.14	（可选）
缺省域名：		（可选）
首选DNS服务器：	0.0.0.0	（可选）
备用DNS服务器：	0.0.0.0	（可选）

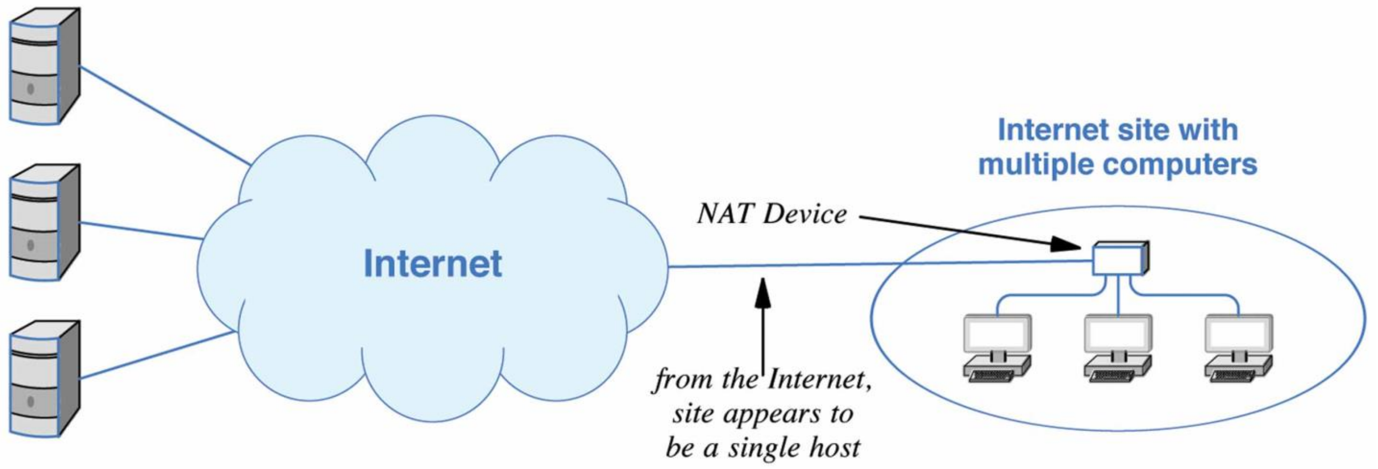


网络连接详细信息(D):

属性	值
连接特定的 DNS 后缀	localdomain
描述	Intel(R) 82574L 千兆网络连接
物理地址	00-0C-29-37-5A-1B
已启用 DHCP	是
IPv4 地址	192.168.7.132
IPv4 子网掩码	255.255.255.0
获得租约的时间	2013年5月19日 10:03:51
租约过期的时间	2013年5月19日 10:34:01
IPv4 默认网关	192.168.7.2
IPv4 DHCP 服务器	192.168.7.254
IPv4 DNS 服务器	192.168.7.2
IPv4 WINS 服务器	192.168.7.2
已启用 NetBIOS over Tc...	是
连接-本地 IPv6 地址	fe80::69a1:1231:cea2:75ef%12
IPv6 默认网关	
IPv6 DNS 服务器	

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



Internet site with multiple computers
NAT Device
Internet
from the Internet, site appears to be a single host

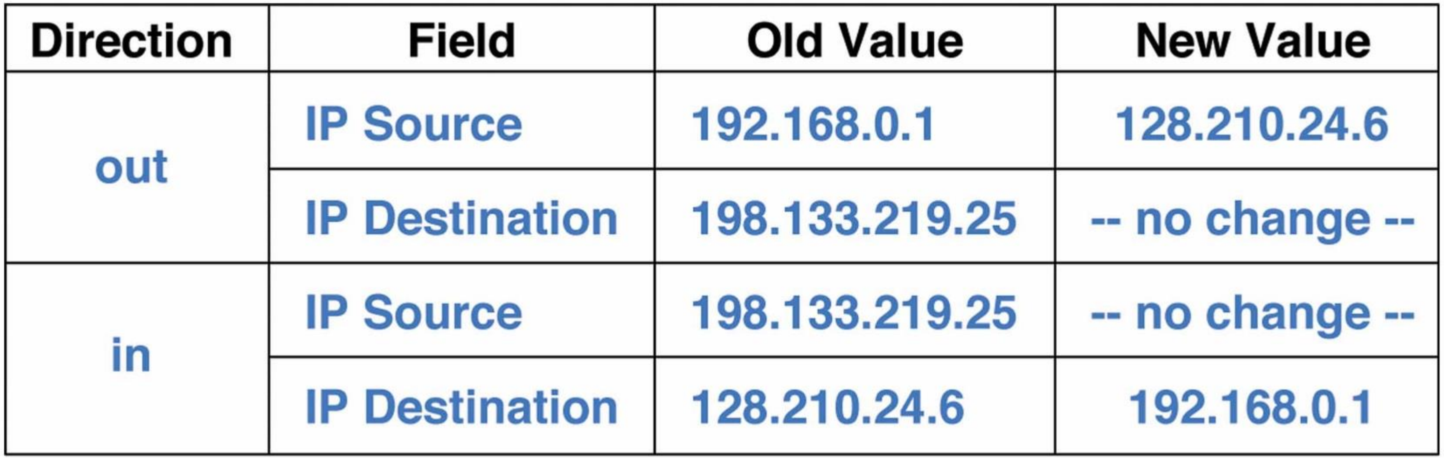
Figure 23.9 The conceptual architecture used with NAT.

私有地址

- 目的：虚拟的寻址机制
  - The goal of NAT is to provide an illusion (错觉).
- Blocks of private addresses (私有地址) used by NAT
  - 10.0.0.0/8：Class A private address block
  - 169.254.0.0/16：Class B private address block
    - 一般开启DHCP客户端又无法获取到IP时使用
  - 172.16.0.0/12：16 contiguous Class B blocks
  - 192.168.0.0/16：256 contiguous Class C blocks
- 防止IP冲突，私有地址不被路由

NAT的地址转换

- **The most basic form of NAT replaces the IP source address in datagrams passing from the site to the Internet, and replaces the IP destination address in datagrams passing from the Internet to the site**



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

NAT的地址转换

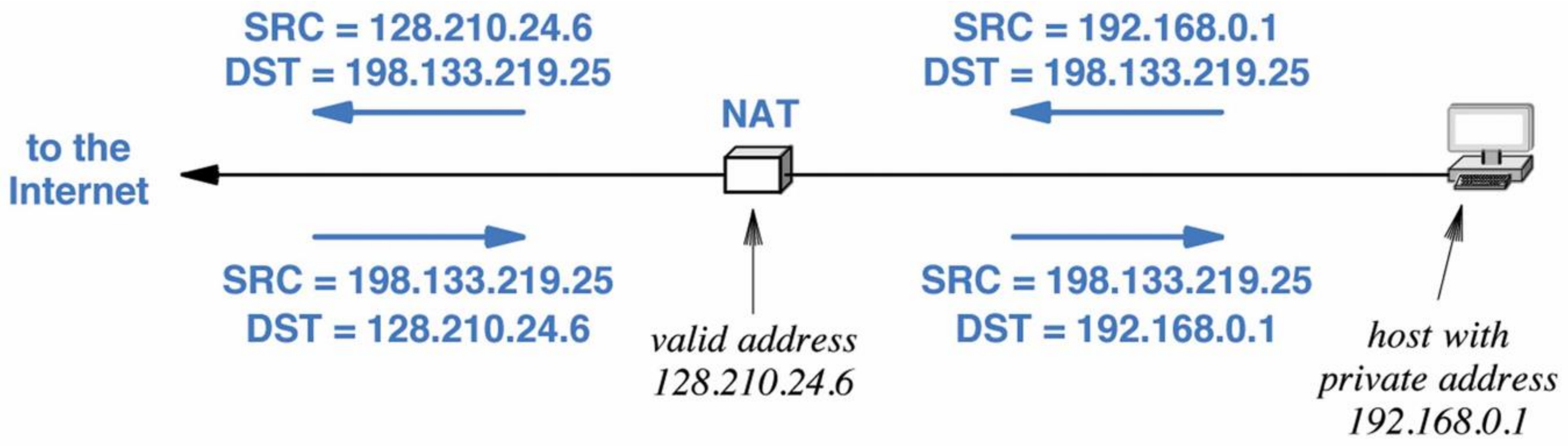
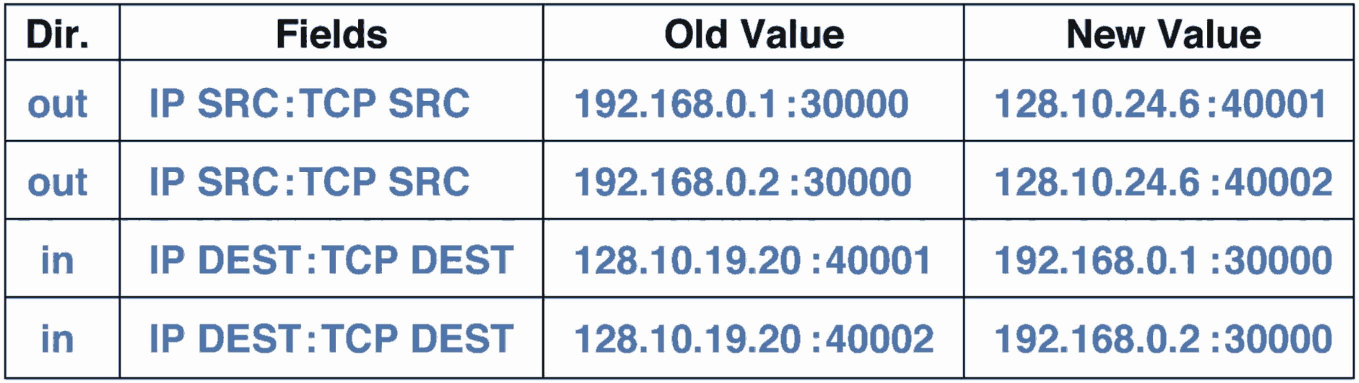


Figure 23.11 Illustration of basic NAT translation that changes the source address of an outgoing datagram and the destination address of an incoming datagram.

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]
```

Ch 19 Binding Protocol Addresses (ARP)

(地址解析协议)

19.3 Address Resolution 地址解析

- 地址解析协议（Address Resolution Protocol）
  - IP是虚拟的，但数据链路层需要物理地址，最终要换的
  - Translation from a computer’s protocol address to an equivalent hardware address.
  - Address resolution is local to a network.
  - A computer never resolves the address of a computer on a remote network.

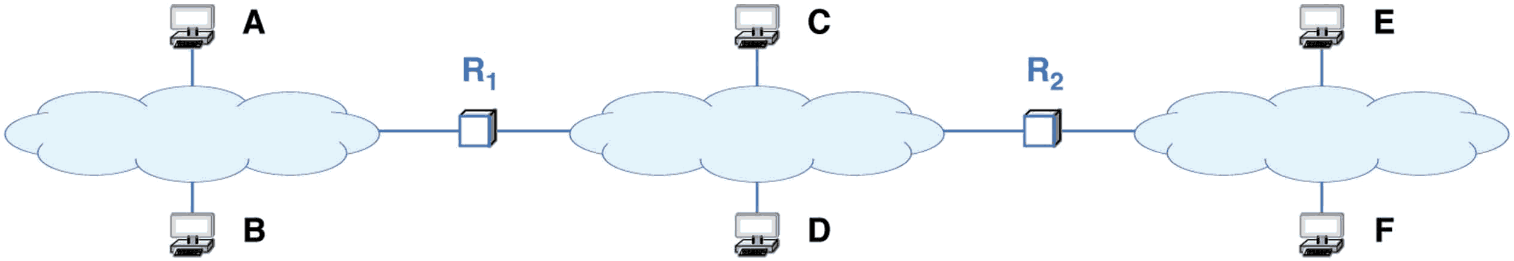


Figure 23.1 An example internet of three networks and computers connected to each.

地址解析（AR）

- 将IP地址解析为MAC地址的叫做地址解析
- 解析地址仅限同一个物理网络内
  - 不同网络内没用
- 概念地址边界
  - ARP以上的用IP地址
  - ARP以下的用物理地址
- ARP提供一种好心的服务
  - ARP欺骗

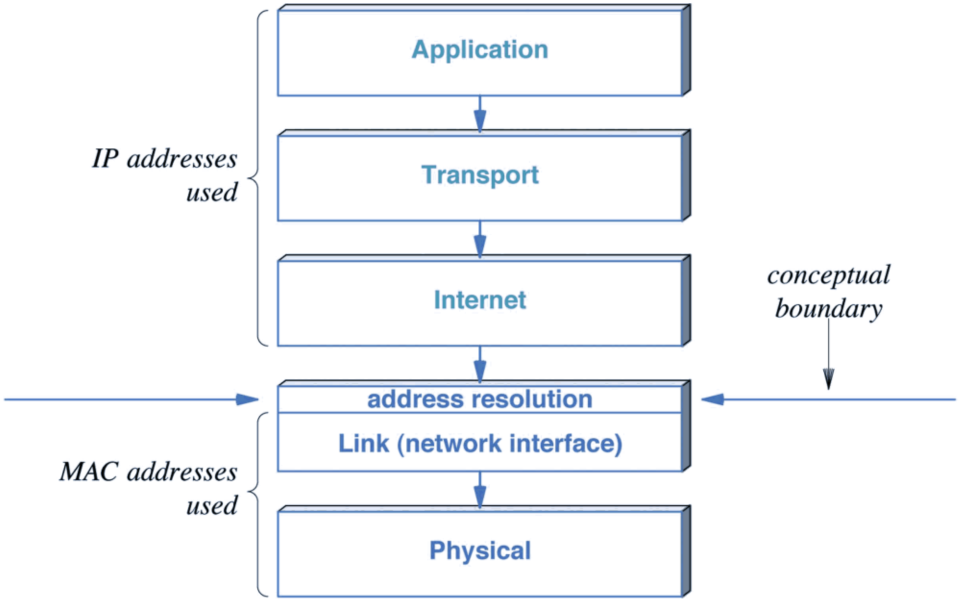
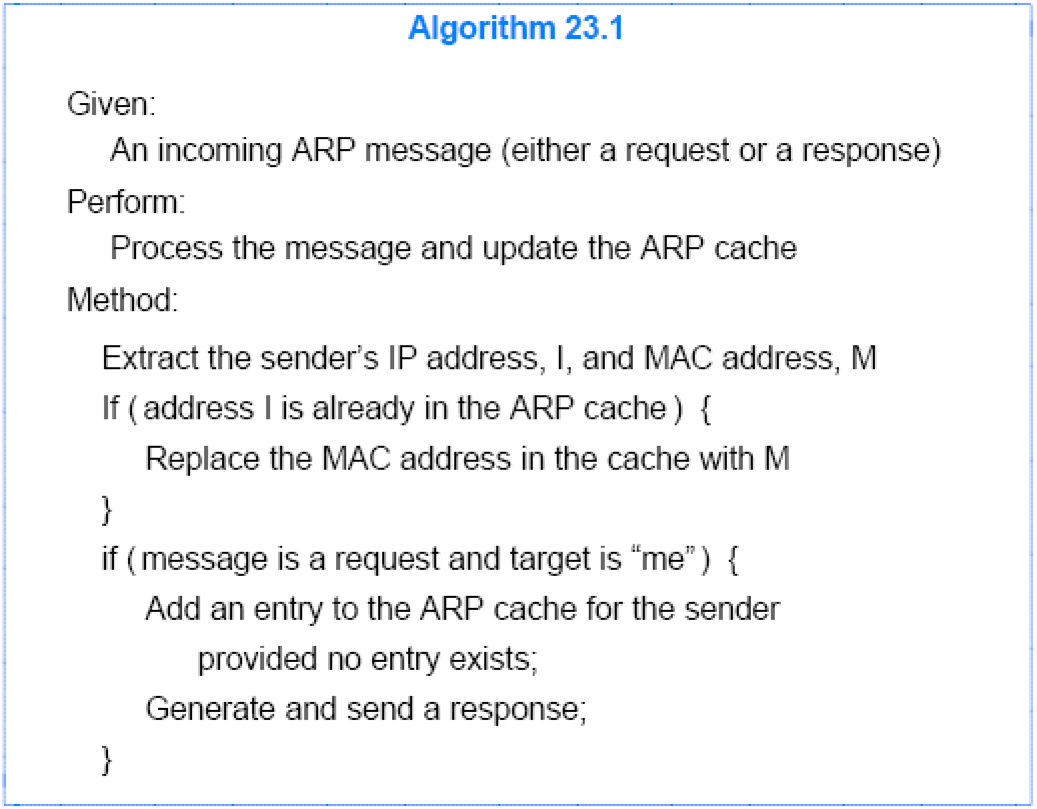


Figure 23.5 Illustration of the boundary between the use of IP addresses and MAC addresses.

19.4 Address Resolution Techniques

- 地址解析算法可分为三大基本类：
  - 查表（Table lookup）。存储在内存表。
  - 相近形式计算（Close-form computation）。配置使得硬件地址可通过简单的布尔和算术运算得出它的协议地址。
  - 消息交换（Message exchange）。计算机通过网络交换消息来解析一个地址。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。

19.4 Address Resolution Techniques



Algorithm 23.1

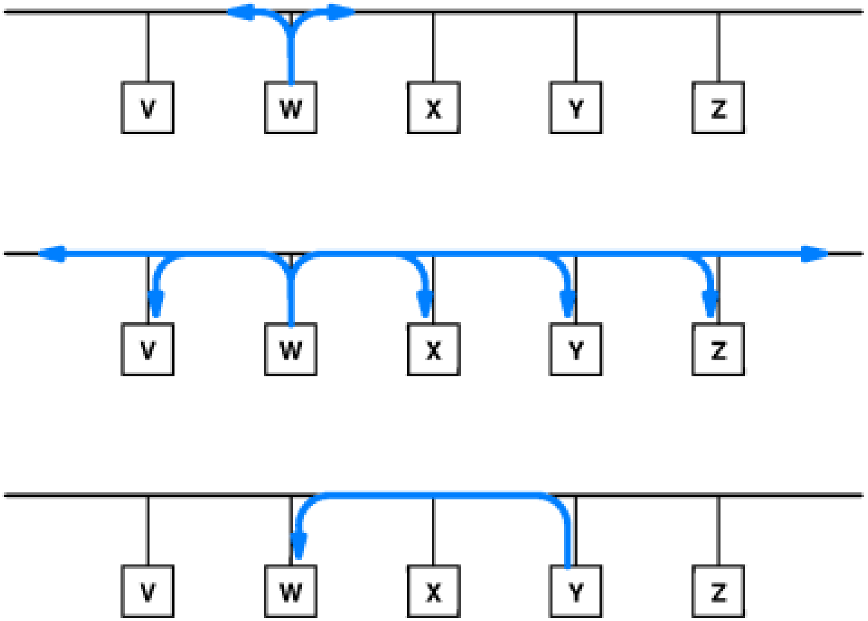
```
Given:
    An incoming ARP message (either a request or a response)
Perform:
    Process the message and update the ARP cache
Method:

   Extract the sender's IP address, I, and MAC address, M
   If ( address I is already in the ARP cache ) {
       Replace the MAC address in the cache with M
   }
   if ( message is a request and target is "me" ) {
       Add an entry to the ARP cache for the sender
            provided no entry exists;
       Generate and send a response;
   }
```

Algorithm 23.1 The steps ARP takes when processing an incoming message.

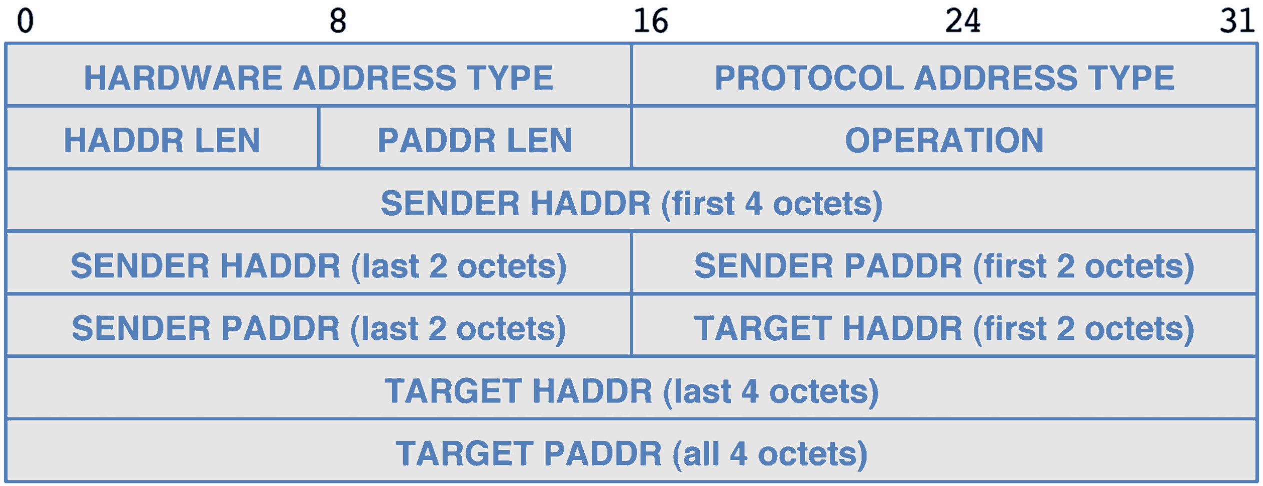
19.8 Address Resolution Protocol

- TCP/IP protocol suite includes an ARP
- The ARP standard defines a request and a response.
- Caching ARP Responses（缓存ARP相应）



19.10 ARP Message Format

- **Frame Format**



0 8 16 24 31

HARDWARE ADDRESS TYPE		PROTOCOL ADDRESS TYPE	
HADDR LEN	PADDR LEN	OPERATION	
SENDER HADDR (first 4 octets)			
SENDER HADDR (last 2 octets)		SENDER PADDR (first 2 octets)	
SENDER PADDR (last 2 octets)		TARGET HADDR (first 2 octets)	
TARGET HADDR (last 4 octets)			
TARGET PADDR (all 4 octets)			

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

- **ARP Encapsulation**
  - **Frame Type: 0x0806**

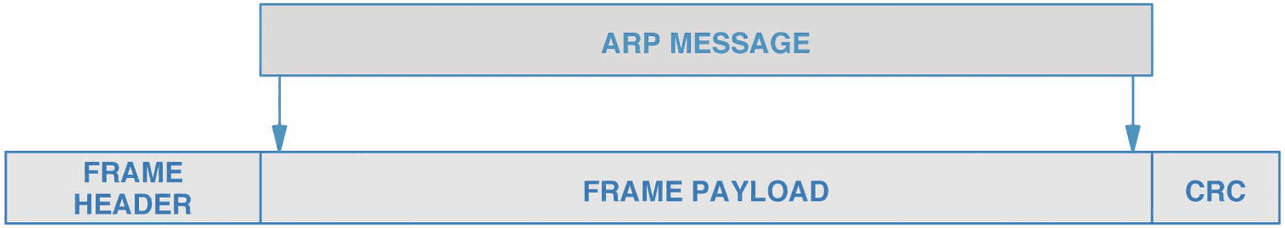


Figure 23.4 Illustration of ARP encapsulation in an Ethernet frame.

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
```

19.10 ARP Message Format

```
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]
```

19.10 ARP Message Format

```
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]
```

19.14 Processing An Incoming ARP Message

- To replace the previously stored binding.
- To examine the `OPERATION` field.
  - If the message is a request? a response?
- Address resolution software hides the details of physical addressing, allowing software in higher layers to use protocol addressing.

Ch 24 TCP:

Reliable Transport Service

TCP：可靠传输服务

两类应用：如果出错

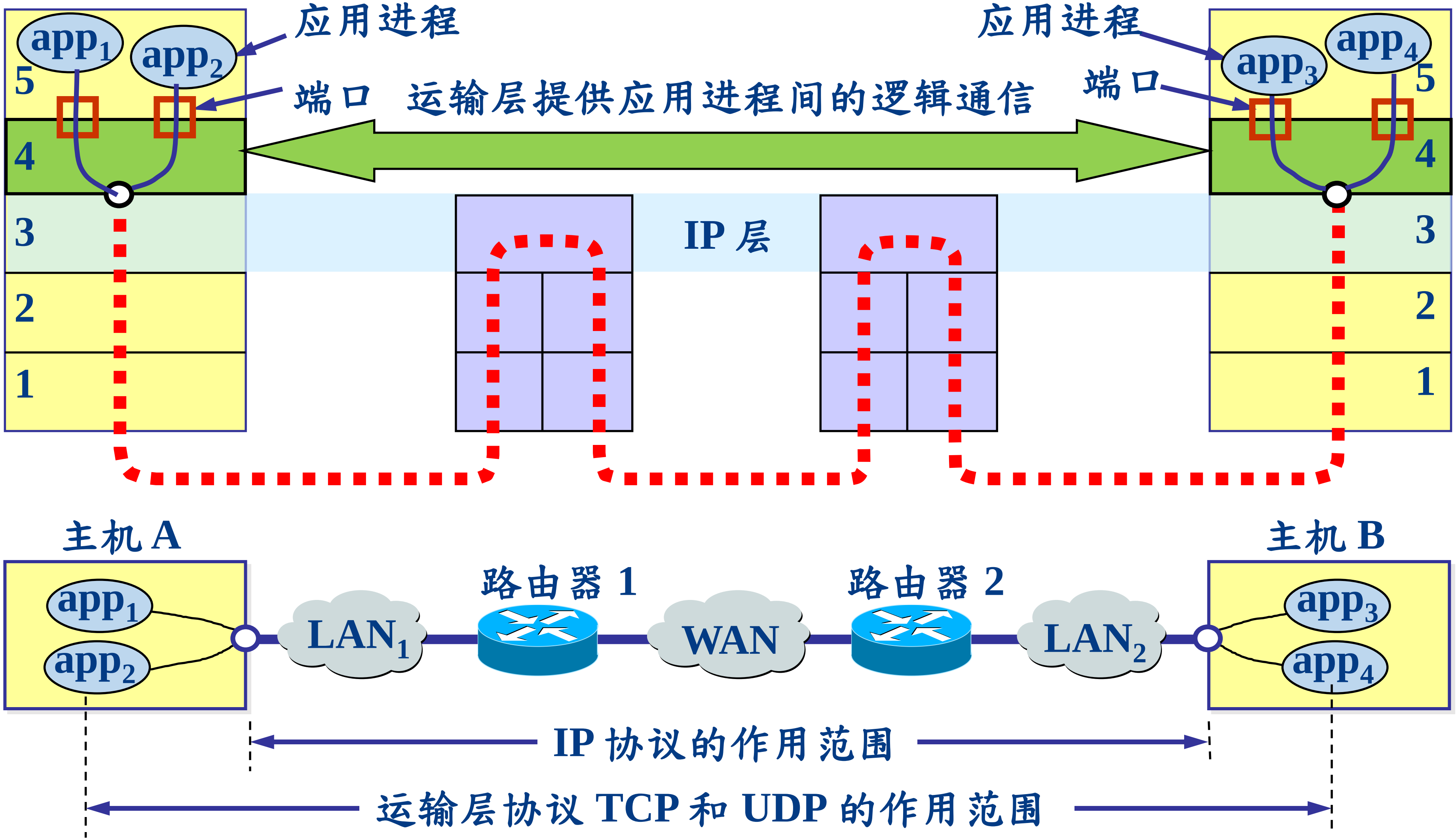
WWW服务器

球赛直播

传输层的必要性

- 网络通信本质上是两个进程的通信，不是主机间通信
- IP地址唯一标识主机；端口号唯一标识进程
- 传输层提供了进程间的复用和解复用
  - 传输层隐藏了硬件拓扑、路由细节等，使应用程序直接调用其接口，建立一条虚拟的端到端的通信信道

网络进程通信



应用进程
应用进程
端口
运输层提供应用进程间的逻辑通信
端口
app1
app2
app3
app4
5
4
3
2
1
5
4
3
2
1
IP 层
主机 A
主机 B
路由器 1
路由器 2
app1
app2
LAN1
WAN
LAN2
app3
app4
IP 协议的作用范围
运输层协议 TCP 和 UDP 的作用范围

运输层的两个主要协议

协议	UDP [RFC 768]	TCP [RFC 793]
全称	User Datagram Protocol，用户数据报协议	Transmission Control Protocol，传输控制协议
数据单位	UDP 数据报 (Datagram)	TCP 报文段 (segment)
作用	端到端	端到端、字节流
连接	无连接	面向连接
收到确认	接收方不给出确认	收到确认
多方	一对一、一对多、多对多	一对一
长度	任意	每报文不超过64KB
优点	高效	安全
比喻	发电报（短信）	打电话

协议端口号(Protocol Port Number)

- 端口（Port）
  - 软件端口，有别于交换机上的硬件端口
  - 端口号范围：0～65535，16bits
  - 作用：用于标识本机的不同进程
  - 分类：
    - 服务器用：熟知端口号：0～1023；登记端口号：1024～49151
    - 客户端用：49152（0xC000）～65535
    - 参考：www.iana.org

TCP与UDP端口（部分）

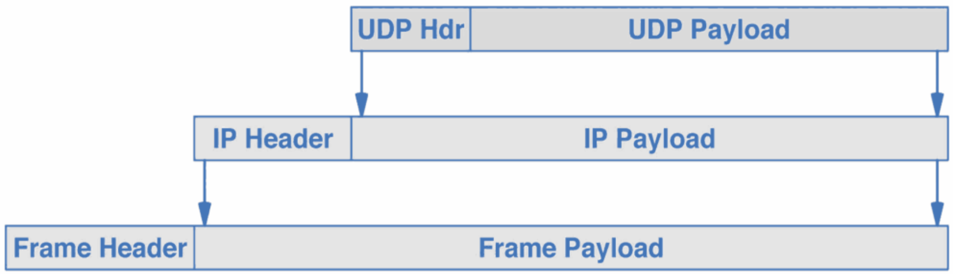
端口	描述	状态
0/TCP,UDP	保留端口；不使用（若发送过程不准备接受回复消息，则可以作为源端口）	官方
1/TCP,UDP	TCPMUX（传输控制协议端口服务多路开关选择器）	官方
5/TCP,UDP	RJE（远程作业登录）	官方
7/TCP,UDP	ECHO（回显）协议	官方
9/TCP,UDP	DISCARD（丢弃）协议	官方
11/TCP,UDP	SYSTAT协议	官方
13/TCP,UDP	DAYTIME协议	官方
15/TCP,UDP	NETSTAT协议	官方
17/TCP,UDP	QOTD（Quote of the Day，每日引用）协议	官方
18/TCP,UDP	消息发送协议	官方
19/TCP,UDP	CHARGEN（字符发生器）协议	官方
20/TCP,UDP	文件传输协议 - 默认数据端口	官方
21/TCP,UDP	文件传输协议 - 控制端口	官方
22/TCP,UDP	SSH (Secure Shell) - 远程登录协议，用于安全登录文件传输（SCP，SFTP）及端口重新定向	官方
23/TCP,UDP	Telnet 终端仿真协议 - 未加密文本通信	官方
25/TCP,UDP	SMTP（简单邮件传输协议）- 用于邮件服务器间的电子邮件传递	官方
更多请上网查询		

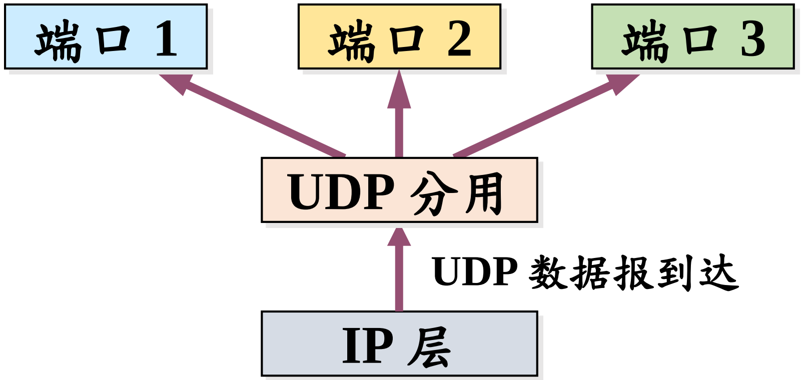
用户数据报协议

（UDP）

UDP概述

- 无连接：发送前不需要建立连接，发送后无可释放。
- 尽力交付：不保证可靠交付，同时也不使用拥塞控制。
- 面向报文的
  – 对应用层交下来的报文不合并、不拆分
  – 应用程序必须选择合适大小的报文，避免拆分





UDP分组结构

- 报文格式
  - 源端口：16 bits
  - 目的端口：16 bits
  - 数据报文长度（单位：字节）：最小为8，即只有头部
  - 校验和：不校正，错误即丢
    - 组成：伪首部（12B）、UDP首部（8B）、数据
    - 伪报文头

0 16 31

UDP SOURCE PORT	UDP DESTINATION PORT
UDP MESSAGE LENGTH	UDP CHECKSUM
PAYLOAD (MESSAGE DATA)	
. . .	

0 16 31

IP SOURCE ADDRESS		
IP DESTINATION ADDRESS		
ZERO	PROTO	UDP LENGTH

使用UDP的场合

- UDP offers best-effort delivery semantics as IP
  - A UDP message can be lost, duplicated, delayed, delivered out-of-order or bits can be corrupted in transit.
- 场合
  - 图像缺几个像素
  - 音频缺几个帧（MP3 44.1kHz，每帧26ms）
  - 音视频缺几个画面
  - 远程桌面连接丢失几个包
  - 丢包损失不大，应用层可以控制丢包

应用

- **Transaction-oriented**
  - **Simple query-response protocols**
    - **Domain name system or network time protocol.**
- **Provides datagrams**
  - **Modeling other protocols**
    - **IP tunneling, remote procedure call, the network file system.**
- **Simple**
  - **Bootstrapping or other purposes without full protocol stack**
    - **DHCP and trivial file transfer protocol**

应用（续）

- Stateless
  - Very large numbers of clients
    - Streaming media applications for example IPTV
- Lack of retransmission delays
  - Real-time applications
    - Voice over IP, online games, and many protocols built on top of the real time streaming protocol.
- Good at unidirectional communication
  - Broadcast information in many kinds of service discovery and shared information
    - Broadcast time or routing information protocol

TCP与UDP编程实验

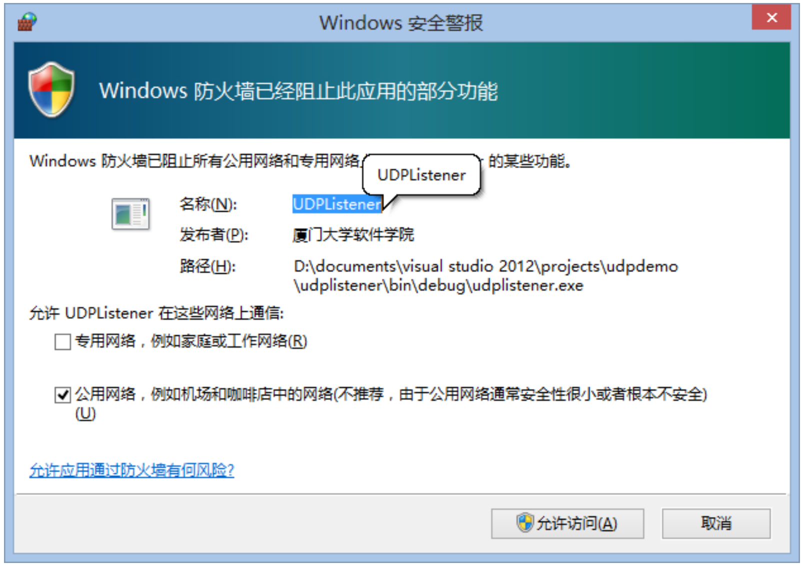
向广播地址11000端口发送UDP消息

```
using System;
using System.Net;
using System.Net.Sockets;
using System.Text;
class Program {
    static void Main(string[] args)  {
        Socket s = new Socket(AddressFamily.InterNetwork,
SocketType.Dgram, ProtocolType.Udp);
        IPAddress broadcast = IPAddress.Parse("192.168.1.255");
        byte[] sendbuf = Encoding.ASCII.GetBytes("HELLO
NETWORK");
        IPEndPoint ep = new IPEndPoint(broadcast, 11000);
        s.SendTo(sendbuf, ep);
        Console.WriteLine("Message sent to the broadcast
address");
        }
}
Output: Message sent to the broadcast address
```

侦听广播地址11000端口的消息

```
using System.Net;
using System.Net.Sockets;
using System.Text;

public class UDPListener {
    private const int listenPort = 11000;
    private static void StartListener()  {
            ……
    }
    public static int Main()  {
        StartListener();
        return 0;
    }
}
```



Windows 安全警报

Windows 防火墙已经阻止此应用的部分功能

Windows 防火墙已阻止所有公用网络和专用网络 UDPListener 的某些功能。

名称(N): UDPListener

发布者(P): 厦门大学软件学院

路径(H): D:\documents\visual studio 2012\projects\udpdemo
\udplistener\bin\debug\udplistener.exe

允许 UDPListener 在这些网络上通信:

☐ 专用网络，例如家庭或工作网络(R)

☑ 公用网络，例如机场和咖啡店中的网络(不推荐，由于公用网络通常安全性很小或者根本不安全)(U)

允许应用通过防火墙有何风险?

侦听广播地址11000端口的消息（续）

```
 private static void StartListener()    {
        bool done = false;
        UdpClient listener = new UdpClient(listenPort);
        IPEndPoint groupEP = new IPEndPoint(IPAddress.Any,
listenPort);
        try {
            while (!done) {
                Console.WriteLine("Waiting for broadcast");
                byte[] bytes = listener.Receive(ref groupEP);
                Console.WriteLine("Received broadcast from
{0} :\n {1}\n", groupEP.ToString(),
Encoding.ASCII.GetString(bytes, 0, bytes.Length));
            }
         }
        catch (Exception e)
{ Console.WriteLine(e.ToString()); }
        finally { listener.Close(); }
    }
```

侦听广播地址11000端口的消息（续）

```
Output on success:

Waiting for broadcast

Received broadcast from 192.168.1.1:52600 :

 HELLO NETWORK



Waiting for broadcast
```

计算机网络

12.

THANK YOU.

厦门大学软件学院

黄炜 助理教授