

课程入门

□ 命令行命令

- ping命令
- tracert命令
- ipconfig命令
- netstat命令
- arp命令
- net命令

Ping命令

- ❑ 在Windows环境下，ping命令语法如下：

```
ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]  
      [-r count] [-s count] [[-j host-list] | [-k host-list]]  
      [-w timeout] target_name
```

- ❑ 最常用形式：“ping IP地址” 或 “ping 域名”
 - ❑ 注意参数t、l、s用法
-

Ping命令

实例

- C:\> ping www.sohu.com
- C:\> ping 118.228.148.143
- C:\> ping www.sysu.edu.cn -t
- C:\> ping -r 6 -l 200 172.18.187.254
- C:\> ping -s 4 -l 200 172.18.187.254

养成良好的实验习惯：尝试上述命令，记下显示的结果，并进一步分析结果

tracert命令

- ❑ Tracert（跟踪路由）是路由跟踪实用程序，用于获得IP数据报访问目标时从本地计算机到目的主机的路径信息。
 - ❑ 在Windows环境下，Tracert命令语法如下：
tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name
 - ❑ 最常用形式：“tracert IP地址”或“tracert 域名”
-

tracert命令

实例

□ C:\>**tracert www.sina.com**

□ C:\>**tracert 172.16.0.88 -d**

参数d指定不将地址解析为计算机名。这样可加速显示tracert的结果

ipconfig命令

- ❑ ipconfig命令可以显示所有当前的 TCP/IP 网络配置值（如IP地址、网关、子网掩码）、刷新动态主机配置协议 (DHCP) 和域名系统 (DNS) 设置。
 - ❑ 在Windows环境下，语法格式为：
ipconfig [/? | /all | /renew [adapter] | /release [adapter] | /flushdns | /displaydns | /registerdns | /showclassid adapter | /setclassid adapter [classid]]
 - ❑ 最常用形式：“ipconfig” 或 “ipconfig/all”
-

ipconfig命令

实例

□ ipconfig

显示所有适配器的基本TCP/IP配置

□ ipconfig /all

显示所有适配器的完整 TCP/IP 配置

netstat命令

- ❑ netstat命令可以显示当前活动的TCP连接、计算机侦听的端口、以太网统计信息、IP路由表、IPv4统计信息（对于IP、ICMP、TCP和UDP协议）以及IPv6统计信息
 - ❑ 在Windows环境下，netstat的语法格式为：
**netstat [-a] [-b] [-e] [-n] [-o] [-p proto] [-r]
[-s] [-v] [interval]**
 - ❑ 最常用参数：**-an、-e -s**
-

netstat命令

实例

❑ netstat -an

显示所有活动的 TCP 连接以及计算机侦听的 TCP 和 UDP 端口

❑ netstat -e -s

显示以太网统计信息，如发送和接收的字节数、数据包数

arp命令

❑ ARP 把基于 TCP/IP 的软件使用的 IP 地址解析成 LAN 硬件使用的媒体访问控制地址。

❑ 其语法格式为：

arp [-a [InetAddr] [-N IfaceAddr]] [-g [InetAddr] [-N IfaceAddr]] [-d InetAddr [IfaceAddr]] [-s InetAddr EtherAddr [IfaceAddr]]

❑ 最常用参数：-a、-d

arp命令

实例

❑ **arp -a**

显示所有接口的ARP 缓存表。

❑ **arp -a -N 192.168.1.100**

显示IP 地址为 192.168.1.100 的接口ARP 缓存表。

❑ **arp -s 10.0.0.80 00-AA-00-4F-2A-9C**

将 IP 地址 10.0.0.80与物理地址 00-AA-00-4F-2A-9C绑定(静态ARP缓存项)。

❑ 注意：在IPv6协议下，已经取消了arp协议，代之以NDP（邻居发现）协议。

net命令

- ❑ **net**命令是功能强大的以命令行工具，它包含了管理网络环境、服务、用户、登陆等**Windows** 中大部分重要的管理功能。使用**net**可以管理本地或者远程计算机的网络环境，以及各种服务程序的运行和配置，或者进行用户管理和登陆管理等。**net**命令所执行的功能都可以在相对应的图形界面完成。
 - ❑ **Windows**中，**net**命令的语法是：
 - ❑ **net [accounts | computer | config | continue | file | group | help | helpmsg | localgroup | pause | session | share | start | statistics | stop | time | use | user | view]**
-

net命令

□ net命令实例

□ 建立本地机用户myuser、口令159357:

net user myuser 159357 /add

□ 删除本地机用户myuser

net user myuser /delete

□ 建立本地目录c:\myshare为共享目录，其共享名myshare、共享权限为只读，访问用户为myuser:

net share myshare=c:\myshare /GRANT:myuser,READ

在Windows7，用户myuser必须是存在并设置有密码的。权限可以是READ、CHANGE或FULL。

端口

- 在网络技术中，端口(**Port**)包括逻辑端口和物理端口两种类型。
 - **物理端口**指的是物理存在的端口，如交换机、路由器上用于连接其他网络设备的接口，如**RJ-45**端口、**SC**端口等等。
 - **逻辑端口**是指逻辑意义上用于区分服务的端口，如**TCP/IP**协议中的服务端口，端口号的范围从**0**到**65535**，比如用于浏览网页服务的**80**端口，用于**FTP**服务的**21**端口等。由于物理端口和逻辑端口数量较多，为了对端口进行区分，将每个端口进行了编号，这就是端口号。
 - **TCP/IP**协议中的**端口**指的是什么呢？
 - 如果把**IP**地址比作一间房子，端口就是出入这间房子的门。真正的房子只有几个门，但是一个**IP**地址的端口可以有**65536**个之多
 - 端口是通过端口号来标记的，端口号只有整数，范围是从**0**到**65535**。
-

端口

- 端口有什么用呢？
 - 一台拥有**IP**地址的主机可以提供许多服务，比如**Web**服务、**FTP**服务、**SMTP**服务等，这些服务完全可以通过**1个IP**地址来实现。那么，主机是怎样区分不同的网络服务呢？显然不能只靠**IP**地址，因为**IP**地址与网络服务的关系是一对多的关系。实际上是通过“**IP**地址+端口号”来区分不同的服务的。
-

端口

二号门诊楼

相当于一个IP地址

相当于端口号

9层 皮肤科 睡眠监测中心
临床营养科
预防保健科
神经内科检查室
脑卒中筛查门诊
院士工作站 特色门诊

8层 遗传诊断中心
挂号收费

7层 眼科 耳鼻喉科
神经内科 神经外科

6层 超声科 功能科
挂号收费

5层 妇科 生殖妇科

4层 内科门诊 挂号收费

3层 外科门诊 采血中心
挂号收费 生殖妇科手术室

2层 产科 儿科康复 新生儿随访
采血中心 挂号收费

M层 药学部 门诊药房
中药房

1层 预约挂号处
服务台 建档处

IP地址

□在IPv4系统中，IP地址是一个32位的二进制地址

如：11001010 01110010 11001110 11001010

□为便于记忆，将其划为4组，每组8位，由小数点分开，用四个字节来表示。

如：11001010.01110010.11001110.11001010

□用点分开的每个字节的数值范围是0-255，称为“点分十进制表示法”

如：202.114.206.202

IP地址

- 网络地址（主机号全为“0”）
主机号全为0的IP地址表示某网络号的网络本身
 - 广播地址（主机号全为“1”）
主机号各位全为1的IP地址表示本网广播或称为本地广播
 - 回环地址
A类地址第一段十进制数值为127是保留地址，用于环路反馈等测试。如127.0.0.1代表本机地址
 - 全“0”地址
整个IP地址全为0代表一个未知的网络如：0.0.0.0。在路由器的配置中，用于默认路由的配置
-

IPv4地址分类

- **IPV4地址分类:**
 - **A类: 1–126** (127是回环和诊断测试保留的)
 - **B类: 128–191**
 - **C类: 192–223**
 - **D类: 224–239** (保留, 主要用于**IP组播**)
 - **E类: 240–254** (保留, 研究测试用)
-

IP地址

☐ IPv4 A类地址



☐ B类地址



☐ C类地址



☐ D类地址



IPv4私有IP地址

- ❑ 10.0.0.0~10.255.255.255 1个A类地址
 - ❑ 172.16.0.0~172.31.255.255 16个连续的B类地址
 - ❑ 192.168.0.0~192.168.255.255 256个连续的C类地址
 - ❑ 这些私有地址常被用于局域网内部地址
-

网络掩码

- 作用：标识一个IP地址的网络号范围
- 结构：掩码长度32bit，由一串1和紧随的一串0组成。1对应于IP地址中的网络号（子网号），0对应于IP地址中的主机号

A类地址掩码

1	1	1	1	1	1	1	1	0	0	0
---	---	---	---	---	---	---	---	---	---	---

B类地址掩码

11111111(255)	11111111(255)	0	0
---------------	---------------	---	---

C类地址掩码

11111111(255)	11111111(255)	11111111(255)	0
---------------	---------------	---------------	---

IP地址

□ 192.168.1.0

不表示一个具体IP地址，而是表示一网段的网络地址

□ 192.168.1.255

表示一个广播地址

□ 192.168.1.1/24

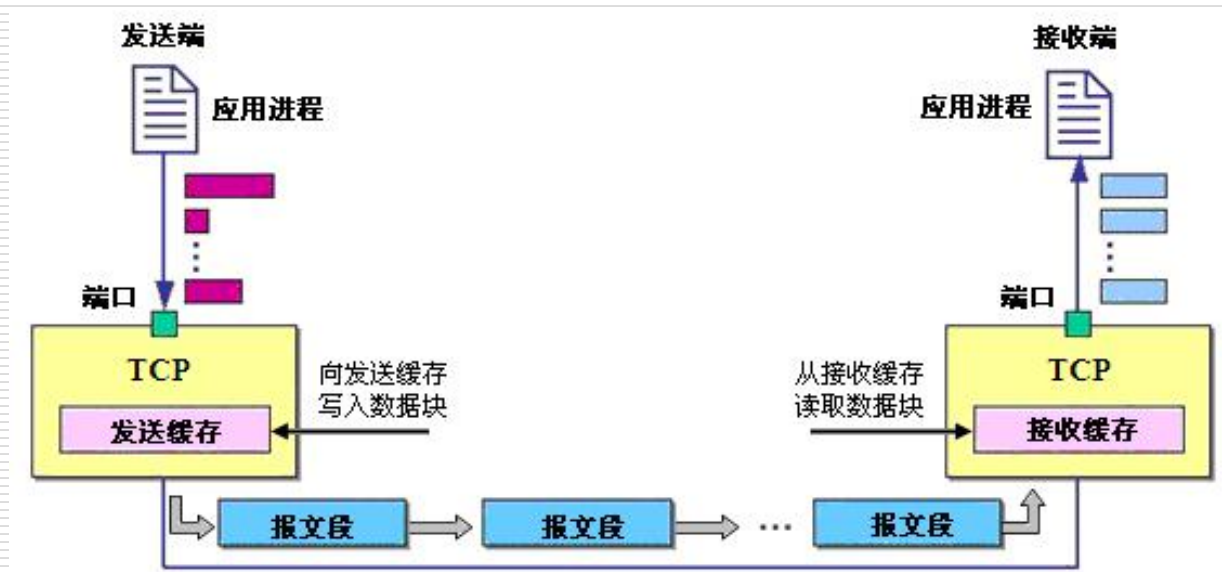
斜杠后的数字表示掩码的高24位为1，其余为0

TCP/UDP/ICMP协议

- ❑ **TCP、UDP、ICMP**协议是**TCP/IP**协议族中的协议
 - ❑ **TCP、UDP**工作于传输层，**ICMP**工作于网络层
 - ❑ **TCP**为两台主机上的应用程序提供高可靠的端到端的数据通信，包括把应用程序交给它的数据分成数据块交给网络层、确认接收到的分组等
 - ❑ **UDP**则为应用层提供不可靠的数据通信，它只是把数据包的分组从一台主机发送到另一台主机，不保证数据能到达另一端。
 - ❑ 所有的**TCP、UDP、ICMP**数据都以**IP**数据包格式传输。
-

TCP协议

□ TCP报文的传输过程



特点：传输双方先建立连接，再传输数据，是可靠传输协议

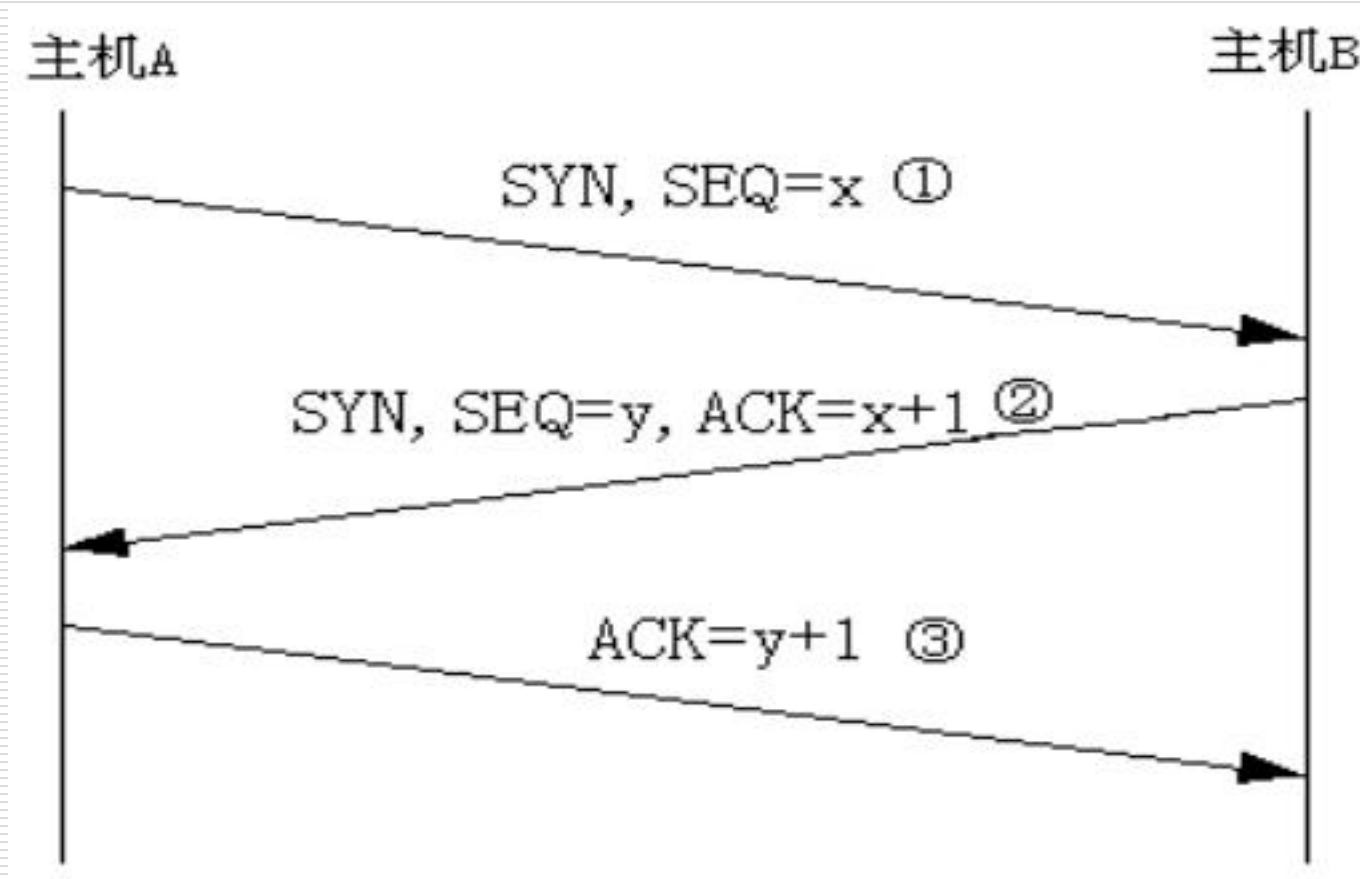
TCP三次握手

第一次握手：客户端TCP首先给服务器端TCP发送一个特殊的TCP数据段。该数据段不包含应用层数据，并将头部中的SYN位设置为1，所以该数据段被称为SYN数据段。另外，客户选择一个初始序列号SEQ，设 $SEQ=x$ ，并将这个编号放到初始的TCP SYN数据段的序列号字段中。该数据段被封装到一个IP数据报中，并发送给服务器。

第二次握手：一旦装有TCP SYN数据段的IP数据报到达了服务器主机，服务器将从该数据报中提取出TCP SYN数据段，给该连接分配TCP缓冲区和变量，并给客户TCP发送一个允许连接的数据段。这个允许连接的数据段也不包含任何应用层数据。但是，它的头部中装载着3个重要信息。首先，SYN被设置为1；其次，TCP数据段头部的确认字段被设置为 $x+1$ ；最后，服务器选择自己的初始顺序号， $SEQ=y$ ，并将该值放到TCP数据段头部的序列号字段中。

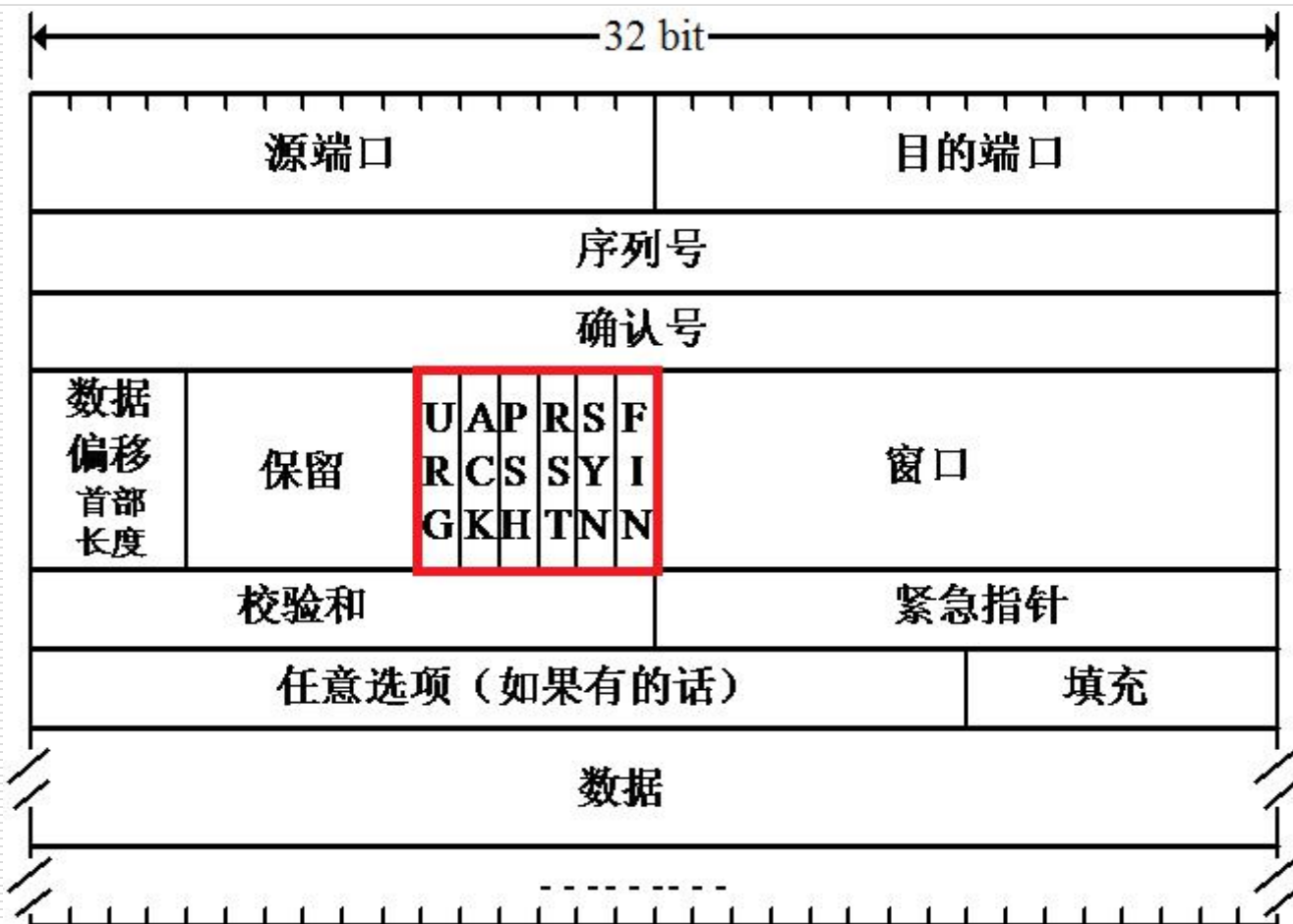
第三次握手：在接收到允许连接数据段之后，客户也会给连接分配缓冲区和变量。客户端主机还会给服务器发送另一个数据段，对服务器的允许连接数据段给出确认。

TCP三次握手

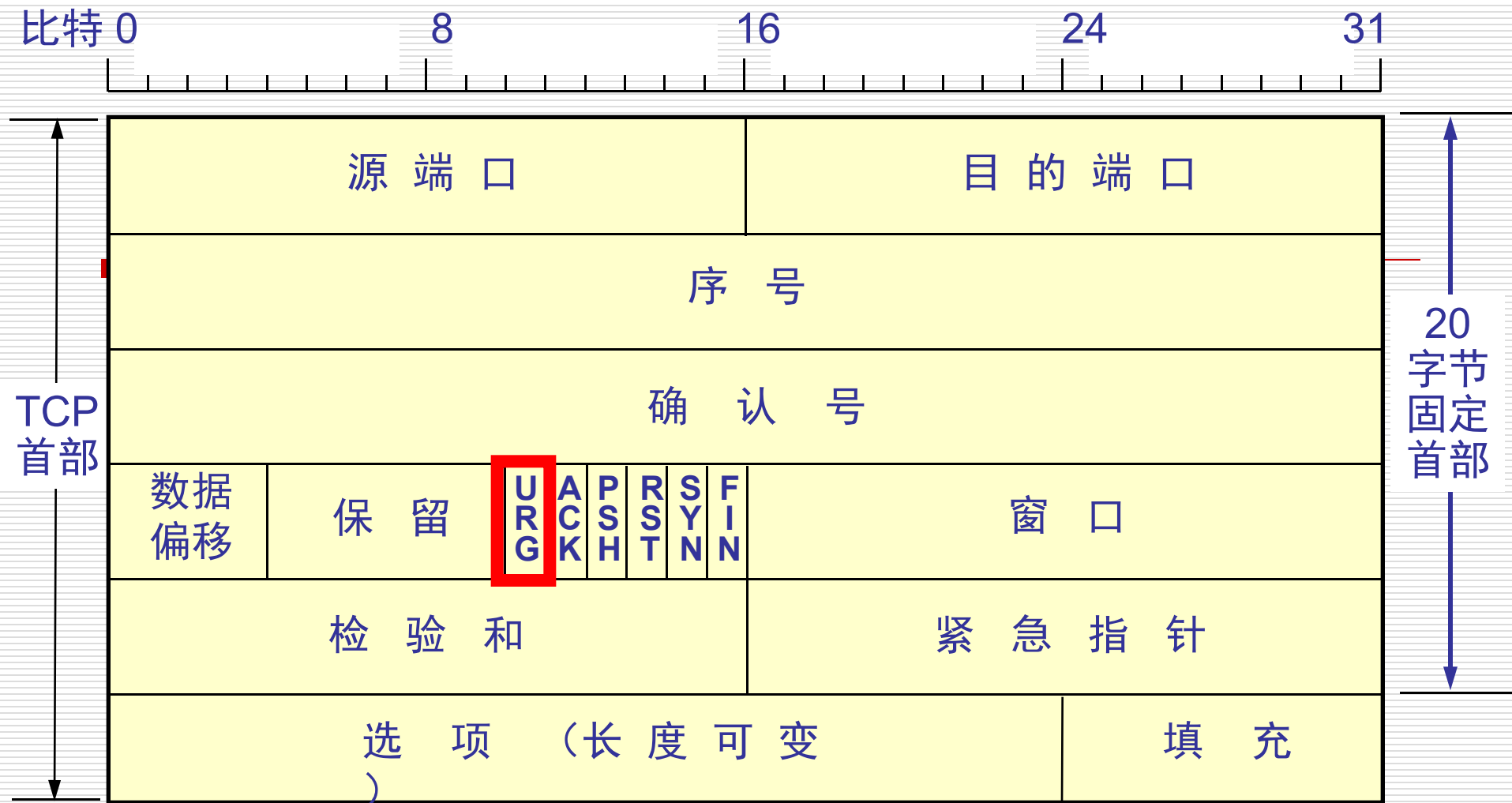


TCP协议中连接建立的过程

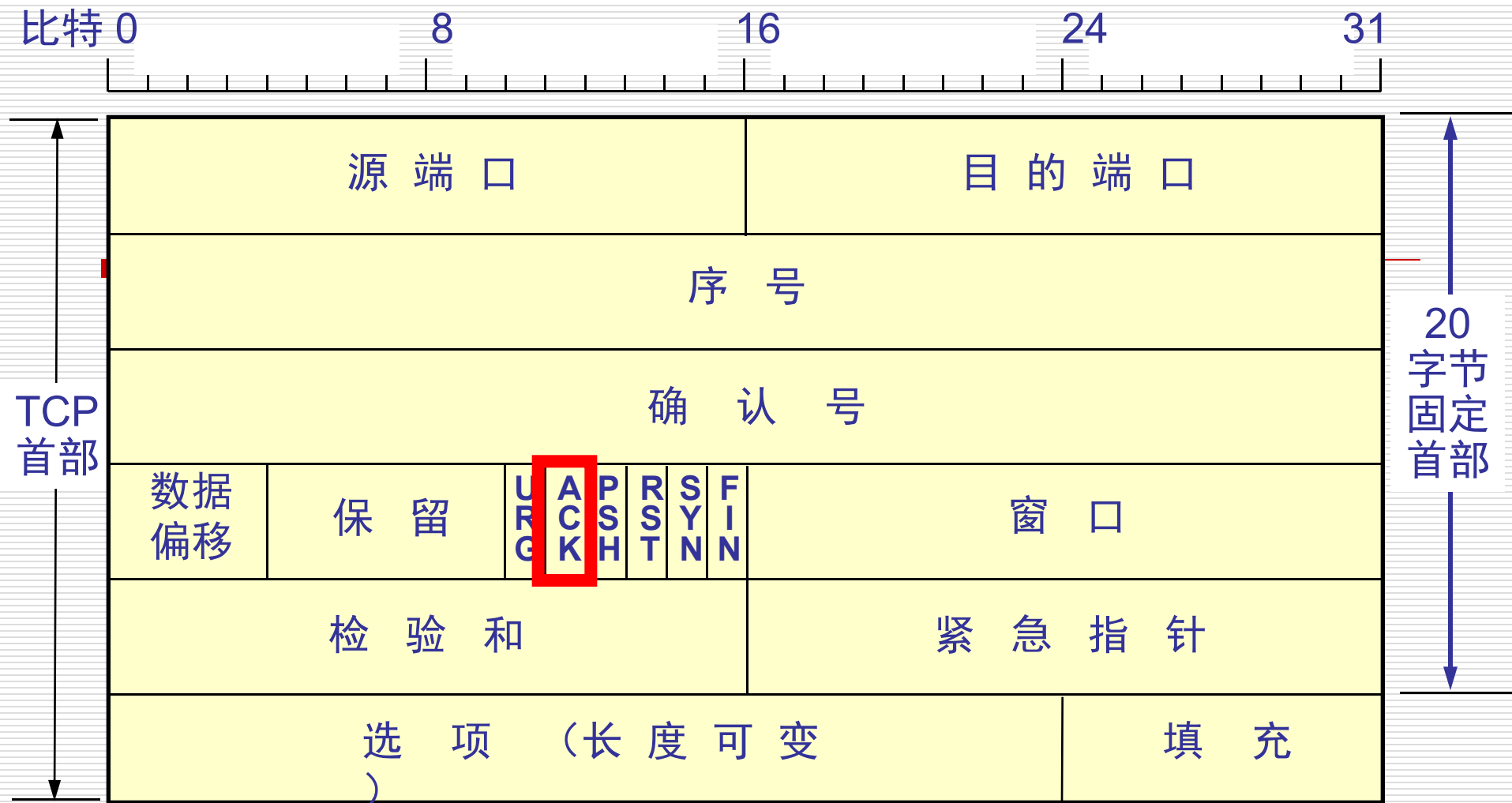
TCP三次握手



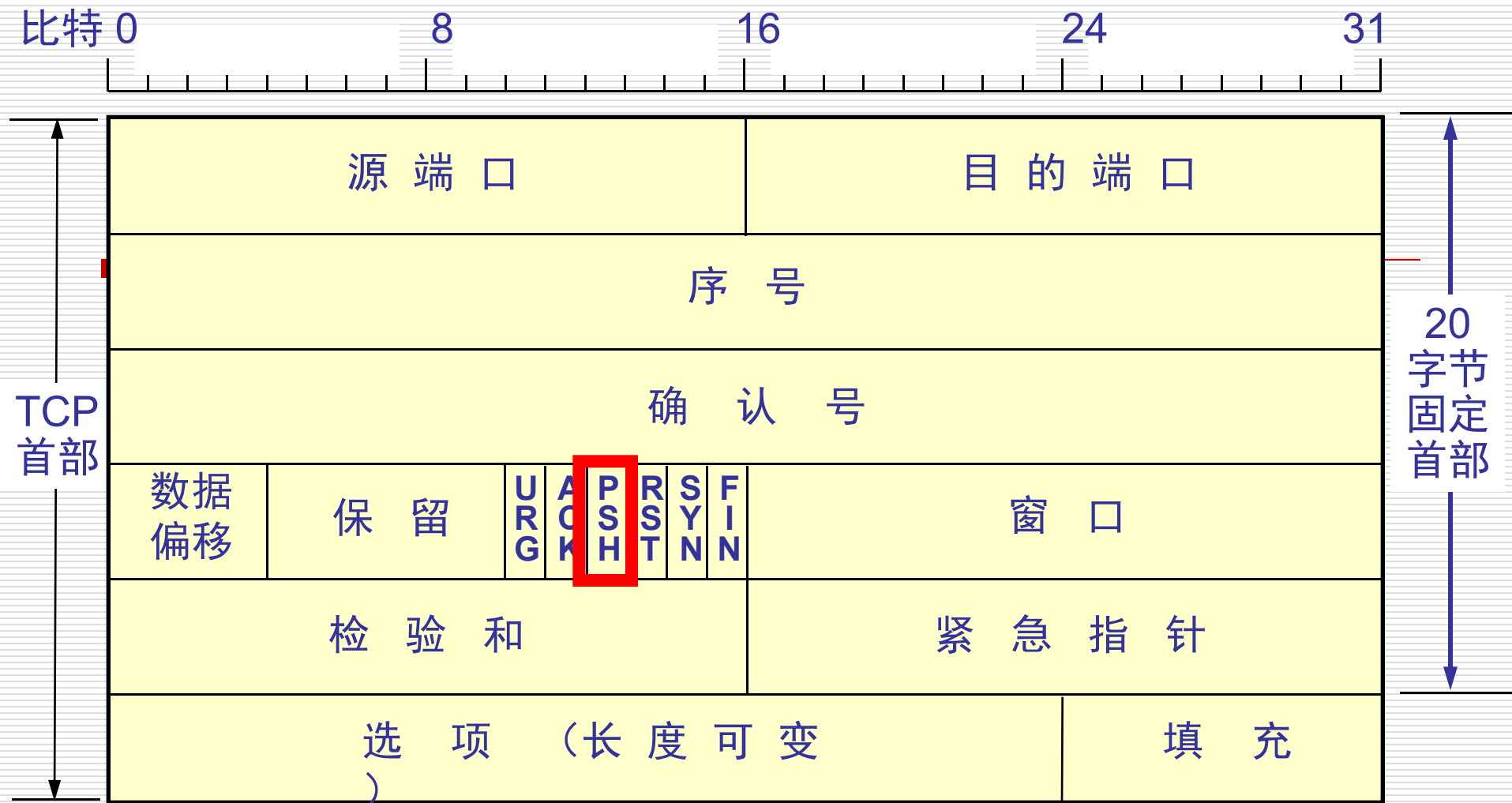
TCP数据报文



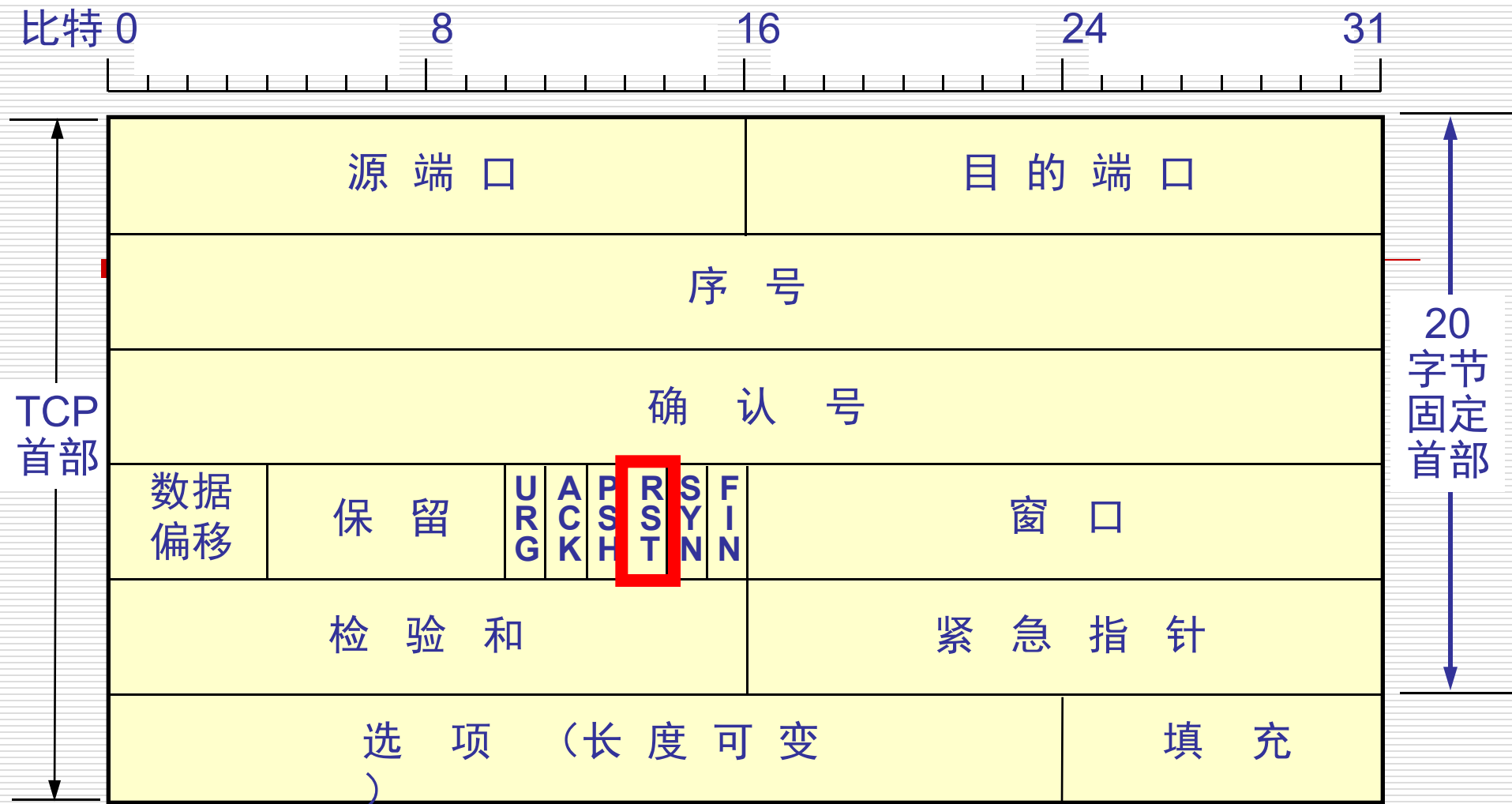
紧急比特 **URG** —— 当 $URG = 1$ 时，表明紧急指针字段有效。它告诉系统此报文段中有紧急数据，应尽快传送(相当于高优先级的数据)。



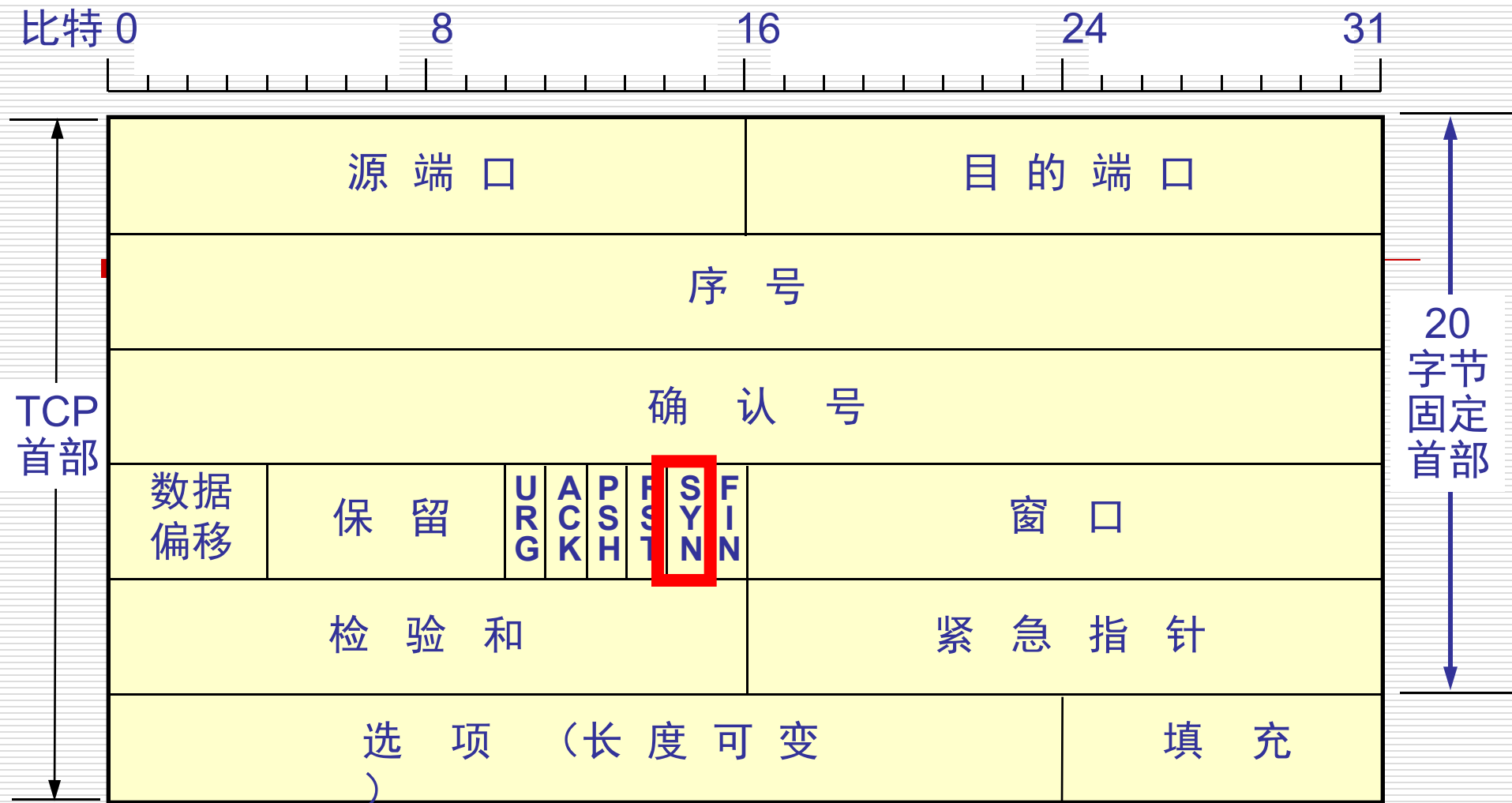
确认比特 **ACK** —— 只有当 $ACK = 1$ 时确认号字段才有效。当 $ACK = 0$ 时，确认号无效。



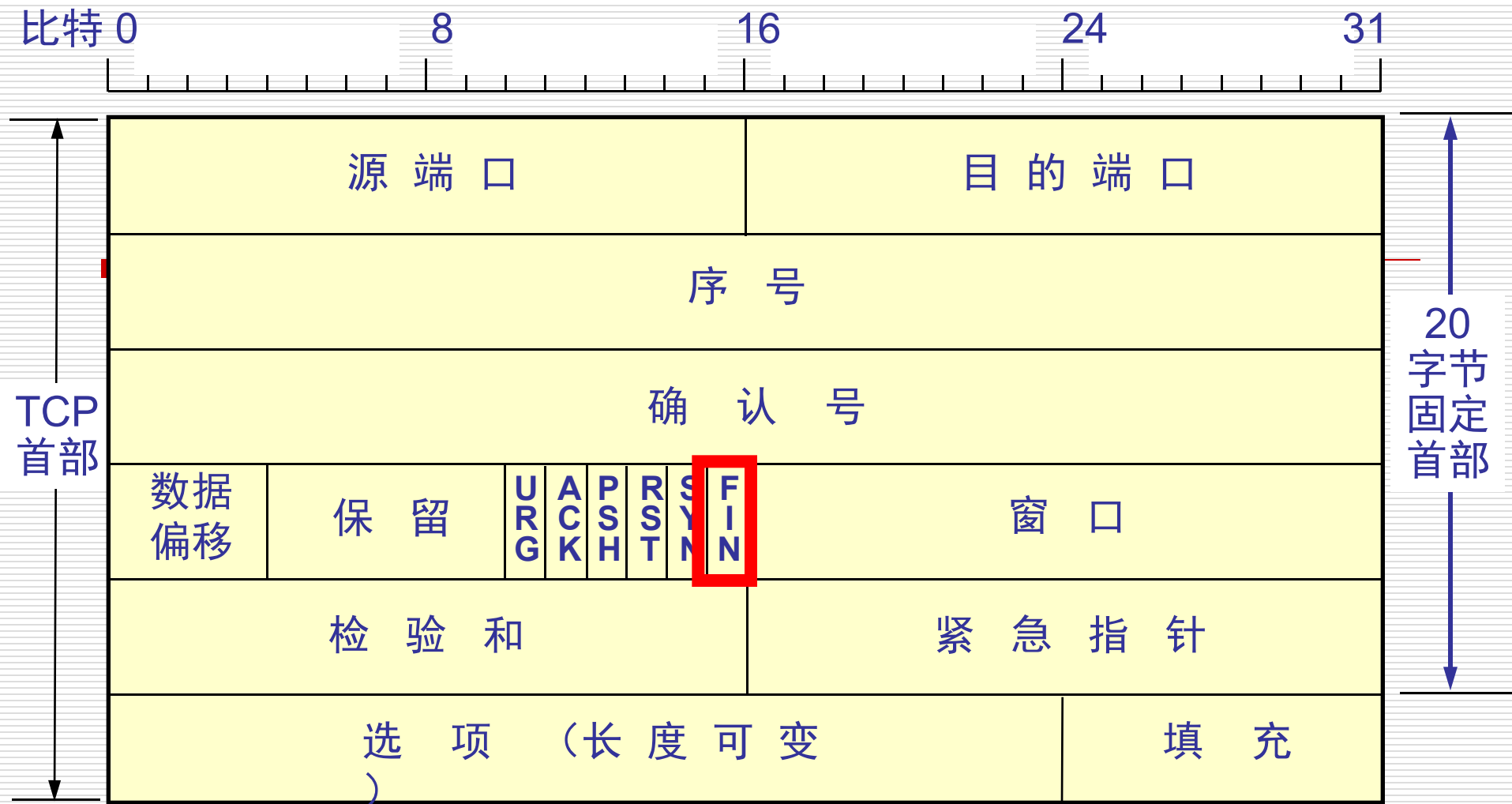
推送比特 **PSH** (PuSH) —— 接收 TCP 收到推送比特置 1 的报文段，就尽快地交付给接收应用进程，而不再等到整个缓存都填满了后再向上交付。



复位比特 **RST** (ReSeT) —— 当 $RST = 1$ 时，表明 TCP 连接中出现严重差错（如由于主机崩溃或其他原因），必须释放连接，通知一下对方。



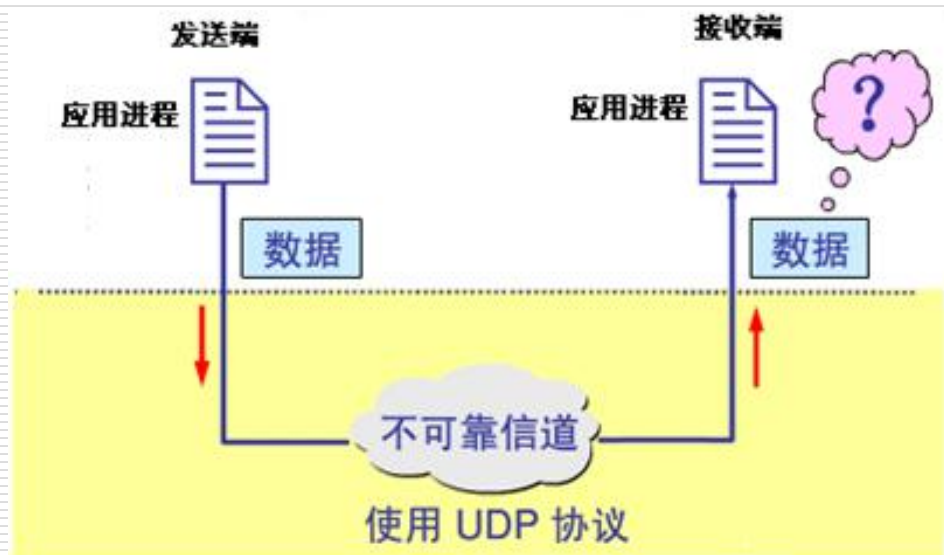
同步比特 **SYN**—— 同步比特 SYN 置为 1，就表示这是一个连接请求或连接接受报文。



终止比特 **FIN** (FINal) —— 用来释放一个连接。当 $FIN = 1$ 时，表明此报文段的发送端的数据已发送完毕，并要求释放运输连接。

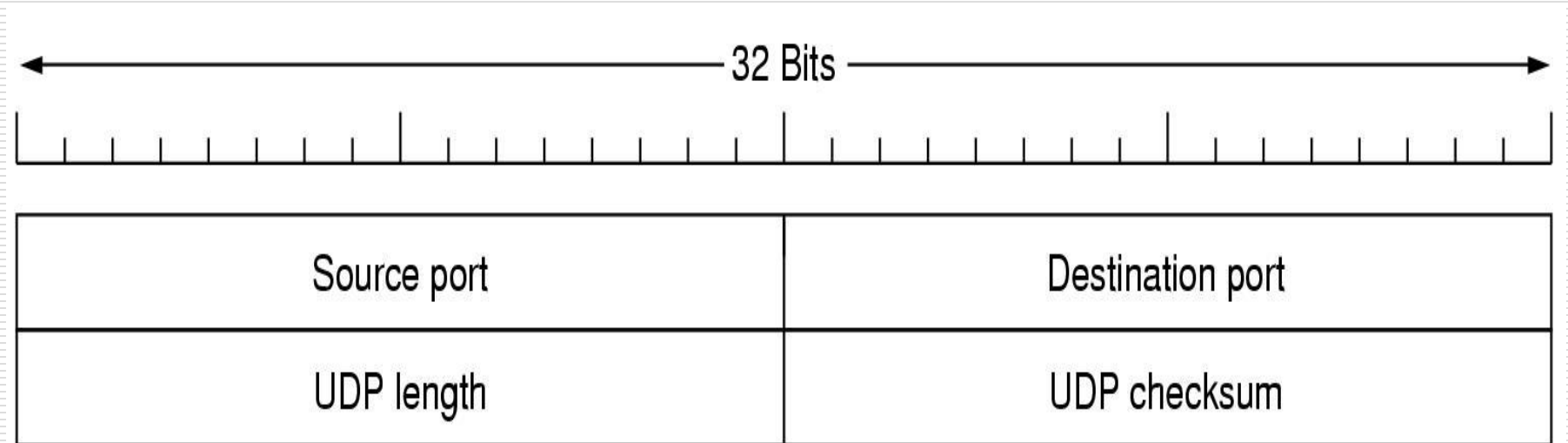
UDP协议

□ UDP协议



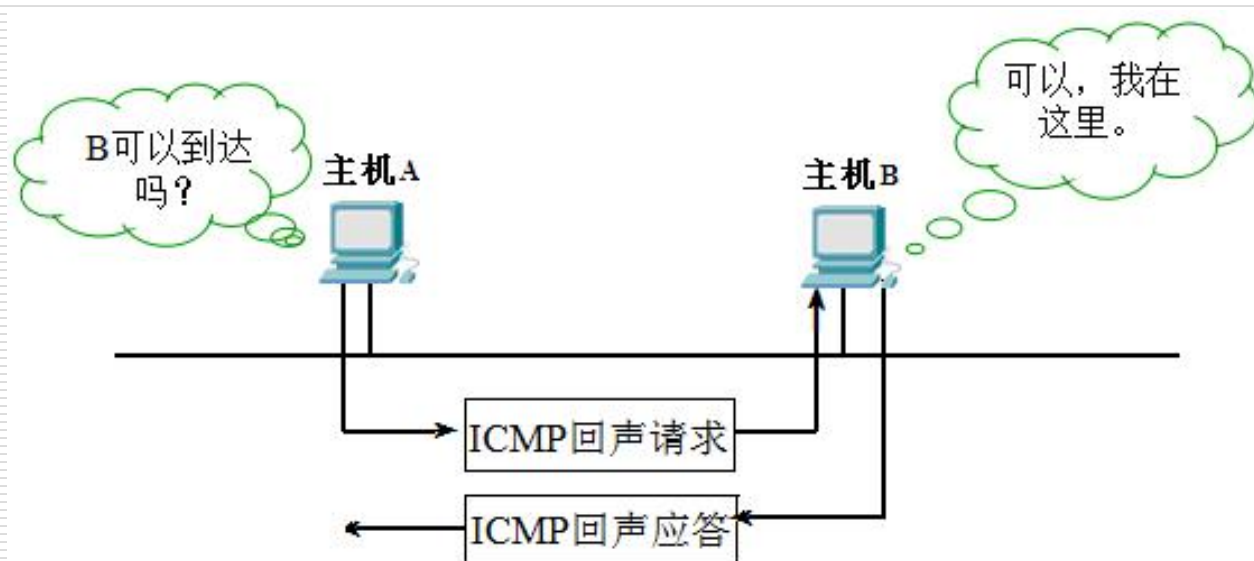
特点：传输双方未建立连接，即传输数据，是不可靠传输协议

UDP报文头结构



ICMP协议

□ ICMP协议



ICMP的目的主要是用于在TCP/IP网络中发送出错和控制消息。ICMP的错误报告只能通知出错数据包的源主机，而无法通知从源主机到出错路由器途中的所有路由器(环路时)。ICMP数据包是封装在IP数据包中的。

ICMP协议报文格式



常见的ICMP报文类型

名 称	类型
ICMP Destination Unreachable (目标不可达)	3
ICMP Source Quench (源抑制)	4
ICMP Redirection (重定向)	5
ICMP Timestamp Request/Reply (时间戳请求/应答)	13/14
ICMP Address Mask Request/Reply (地址掩码请求/应答)	17/18
ICMP Echo Request/Reply (响应请求/应答)	8/0

协议分析软件Wireshark

- ❑ **Wireshark** 是常用网络包分析工具。网络包分析工具的主要作用是尝试捕获网络包，并显示包的尽可能详细的情况
- ❑ 通过仔细分析**Wireshark**截取的数据包能够帮助使用者对于网络行为有更清楚的了解
- ❑ **Wireshark**没有数据包生成器，因而只能查看数据包而不能修改
- ❑ **Wireshark** 的官方网站
<http://www.wireshark.org/download.html>

Wireshark简介

- ❑ **Wireshark**是一个免费的开源网络数据包分析工具，可以在**Linux**、**Solaris**、**Windows**等多种平台运行。
 - ❑ 下载<http://www.wireshark.org/download.html>
 - ❑ 它允许用户从一个活动的网络中捕捉数据包并进行分析，详细探究数据包的协议字段信息和会话过程。
 - ❑ 帮助网络管理员解决网络问题，帮助网络安全工程师检测安全隐患，开发人员可以用它来测试协议执行情况、学习网络协议。
 - ❑ 具有很好的可扩展性，用户能自由地增加插件以实现额外功能。
-

Wireshark更名的故事

- ❑ 2006年6月8号, **Ethereal**软件的创始人**Gerald Coombs** (杰拉尔·德库姆斯) 宣布离开**NIS**公司 (**Ethereal**所属公司), 正式加入**CaceTech**。
 - ❑ 由于**Coombs**最终没能与**NIS**公司达成协议, **Coombs**想保留**Ethereal**商标权, 因此将**Ethereal**后续版本更名为**Wireshark**, 属于**CaceTech**公司。
 - ❑ **Ethereal**原网站(<http://ethereal.com/>)依旧提供下载服务。
 - ❑ 在安装**Wireshark**时, 要同时安装**Winpcap**, 它是提供**Windows** 系统所需要的封包捕获驱动程序
-



Gerald Combs

Director of Open Source Projects at Riverbed Technology

美国 加利福尼亚 萨克拉门托 | 计算机网络

目前就职	Riverbed Technology, Wireshark Development Team
曾经就职	CACE Technologies, Network Integration Services, Unicom Communications
教育背景	University of Missouri-Kansas City
推荐信	9 位会员推荐了Gerald
网站链接	公司网站 Wireshark 个人网站

Wireshark的特点

- ❑ 支持多种通讯接口（如**Ethernet**、**Token-ring**、**X.25**等）及数据包协议类型（如**ARP**、**TCP**、**UDP**等），可以组合**TCP**上的封包且显示出以**ASCII**或是**EBCDIC**型态的数据（**TCP Stream**），所捕获的封包可以被储存。
 - ❑ 支持**Capture Filter**（捕获前过滤）和**Display Filter**（捕获后过滤）功能帮助用户筛选想要的数据包。
-

Display filter

- ❑ 在捕获数据包结束后设定。用来设定显示数据包的条件，属于**捕获后过滤**
 - ❑ 好处:可以让你选择要看的数据包
 - ❑ **Example:**
 - 同Capture filter
 - `tcp.port == 80`
 - `tcp port 80` （此过滤规则是上一条的不同写法）
-

协议分析软件Wireshark

主工具栏选项





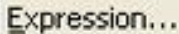


图标	工具栏项	对应菜单项	描述
	接口	Capture/Interfaces...	打开接口列表对话框
	选项...	Capture/Options	打开捕捉选项对话框
	Start	Capture/Start	使用最后一次的捕捉设置立即开始捕捉
	STOP	Capture/Stop	停止当前的捕捉
	Restart	Capture/Rstart	停止当前捕捉，并立即重新开始
	Open...	File/Open	启动打开文件对话框，用于载入文件
	Save As...	File/Save As...	保存当前文件为任意其他的文件
	Close	File/Close	关闭当前文件。若未保存将会提示是否保存
	Reload	View/Reload	重新载入当前文件
	Print	File/Print	打印捕捉文件的全部或部分
	Go To First Packet	Go/First Packet	跳转到第一包
	Go To Last Packet	Go/Last Packet	跳转到最后一个包
	Colorize	View/Coloreze	切换是否以彩色方式显示包列表
	Auto Scroll in Live	View/Auto Scrool in Live Capture	开启/关闭实时捕捉时自动滚动包列表

	Zoom in	View/Zoom In	增大字体
	zoom out	View/Zoom Out	缩小字体
	Normal Size	View/Normal Size	设置缩放大小为 100%
	<u>Resize</u> Columns	View/ <u>Resize</u> Columns	重置列宽，使内容适合列宽(使包列表内的文字可以完全显示)
	Capture Filters...	Capture/Capture Filters...	打开对话框，用于创建、编辑过滤器
	Display Filters...	Analyze/ Filters...	打开对话框，用于创建、编辑过滤器
	Coloring Rules...	View/Coloring Rules...	定义以色彩方式显示数据包的规则
	Preferences...	Edit/Preferences	打开首选项对话框
	Help	Help/Contents	打开帮助对话框

"Filter"工具栏

Filter:

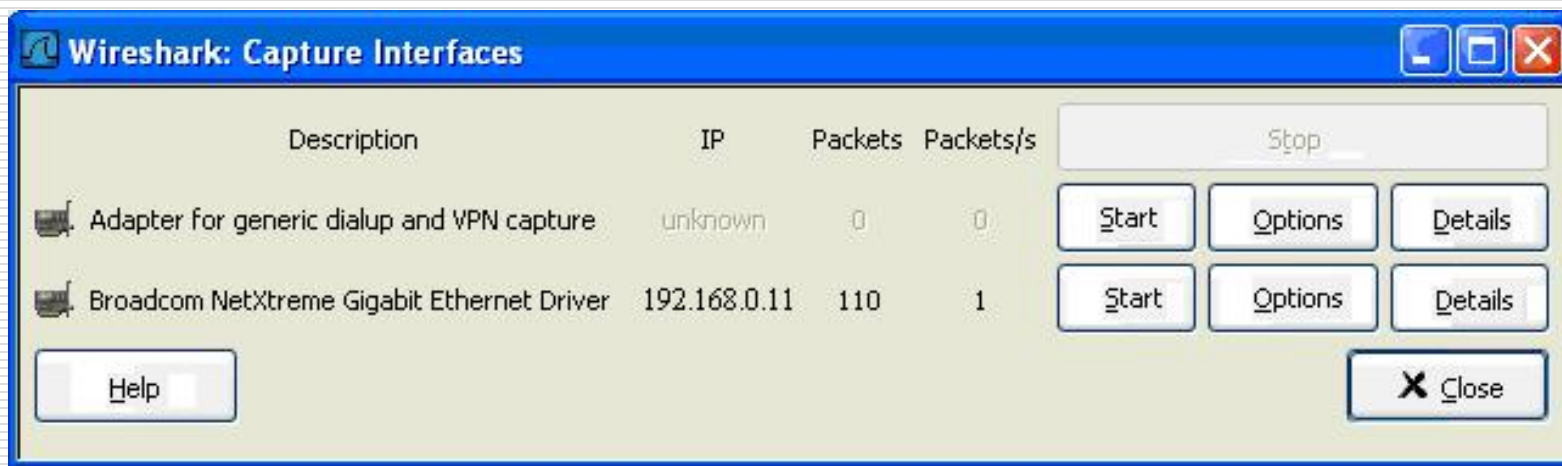
▼ Expression... Clear Apply Save

	过滤	打开构建过滤器对话框
	过滤输入框	在此区域输入或修改显示的过滤字符，在输入过程中会进行语法检查。如果输入的格式不正确，或者未输入完成，则背景显示为红色。直到输入合法的表达式，背景会变为绿色。可以点击下拉列表选择先前键入的过滤字符。即使重新启动程序，列表也会一直保留。输入完后点击右边的 Apply 按钮或者回车，以使过滤生效
	表达式...	为表达式的按钮打开一个对话框用以从协议字段列表中编辑过滤器
	清除	重置当前过滤器，清除输入框
	应用	应用当前输入框的表达式为过滤器进行过滤

协议分析软件Wireshark

Wireshark使用方法

- ①使用下图按钮，打开捕捉接口对话框，浏览可用的本地网络接口，选择需要进行捕捉的接口启动捕捉



协议分析软件Wireshark

- ②使用捕捉选项按钮，启动捕捉选项配置对话框；
有时需要配置高级选项，例如需要捕获一个文件，或者限制捕获的时间或大小，可以单击主菜单Capture的options
 - ③如果前次捕捉时的设置和现在的要求一样，可以点击图中开始捕捉按钮或者是菜单项立即开始本次捕捉
 - ④启动捕捉后，即开始捕捉接口信息。当不再需要捕捉时，可使用捕捉信息对话框上的"stop"按钮停止
-

协议分析软件Wireshark

Wireshark的过滤规则

- ❑ Wireshark的一个重要功能，就是Filter。由于其所捕捉的数据较复杂，要迅速、准确的获取我们需要的信息，就要使用过滤工具
 - ❑ 可以有两次过滤：第一次是捕捉过滤，用来筛选需要的捕捉结果；第二次是显示过滤，只将需要查看的结果显示
 - ❑ Filter位于主工具栏上，可按规则输入过滤条件
-

协议分析软件Wireshark

- 常用的过滤规则例
 - tcp
 - tcp or udp
 - tcp || udp （此过滤规则是上一条的不同写法）
 - tcp and ip.addr=192.168.1.34
 - tcp.port == 80
 - tcp port 80 （此过滤规则是上一条的不同写法）
-

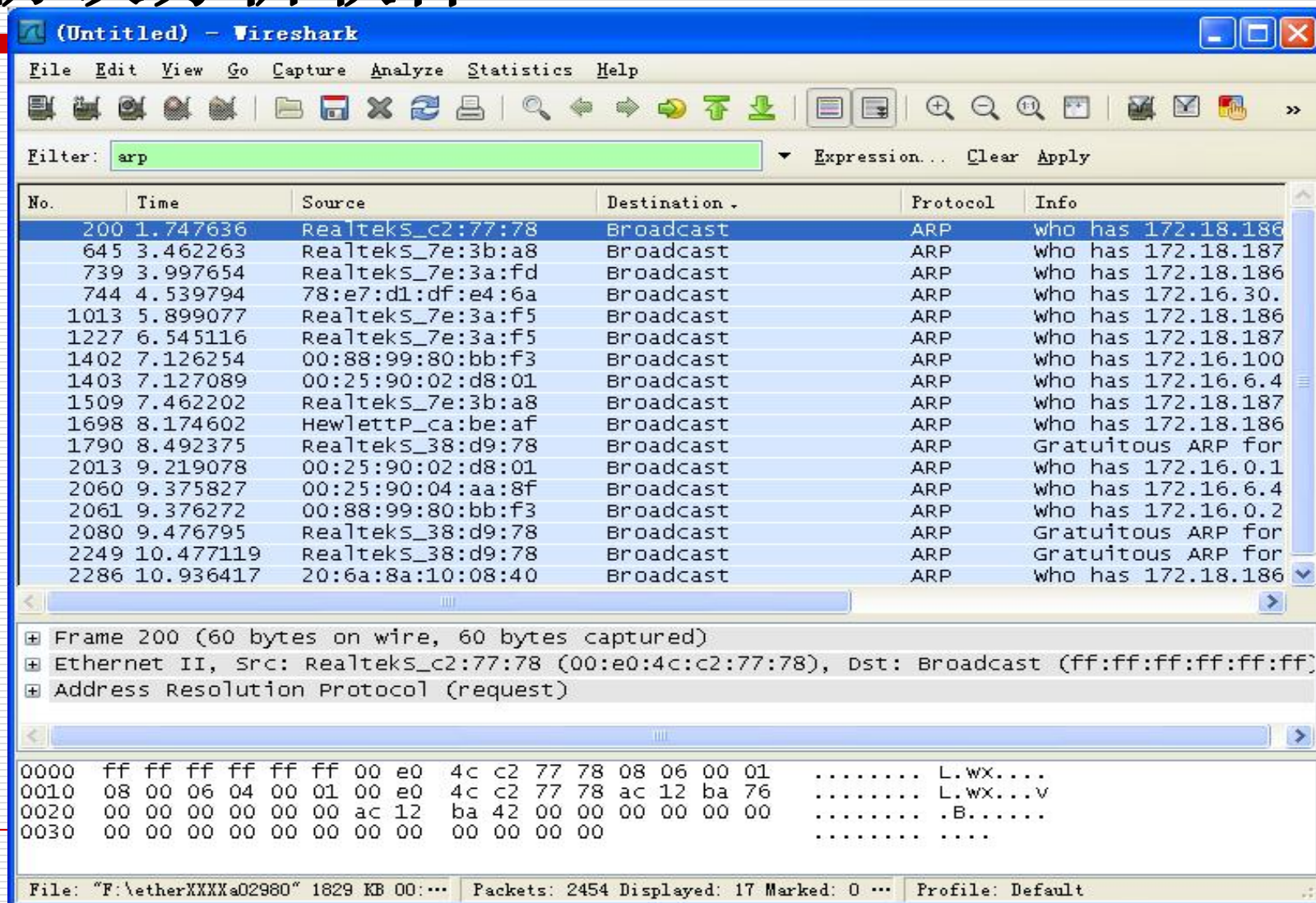
协议分析软件Wireshark

数据包捕获实例

□ Wireshark的界面窗口主要分为三部分

- 最上面为数据包列表，用来显示截获的每个数据包的总结性信息
 - 中间为协议树，用来显示选定的数据包所属的协议信息
 - 最下面是以十六进制形式表示的数据包的内容，用来显示数据包在物理层上传输时的最终形式
-

协议分析软件Wireshark



(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
200	1.747636	RealtekS_c2:77:78	Broadcast	ARP	who has 172.18.186
645	3.462263	RealtekS_7e:3b:a8	Broadcast	ARP	who has 172.18.187
739	3.997654	RealtekS_7e:3a:fd	Broadcast	ARP	who has 172.18.186
744	4.539794	78:e7:d1:df:e4:6a	Broadcast	ARP	who has 172.16.30.
1013	5.899077	RealtekS_7e:3a:f5	Broadcast	ARP	who has 172.18.186
1227	6.545116	RealtekS_7e:3a:f5	Broadcast	ARP	who has 172.18.187
1402	7.126254	00:88:99:80:bb:f3	Broadcast	ARP	who has 172.16.100
1403	7.127089	00:25:90:02:d8:01	Broadcast	ARP	who has 172.16.6.4
1509	7.462202	RealtekS_7e:3b:a8	Broadcast	ARP	who has 172.18.187
1698	8.174602	HewlettP_ca:be:af	Broadcast	ARP	who has 172.18.186
1790	8.492375	RealtekS_38:d9:78	Broadcast	ARP	Gratuitous ARP for
2013	9.219078	00:25:90:02:d8:01	Broadcast	ARP	who has 172.16.0.1
2060	9.375827	00:25:90:04:aa:8f	Broadcast	ARP	who has 172.16.6.4
2061	9.376272	00:88:99:80:bb:f3	Broadcast	ARP	who has 172.16.0.2
2080	9.476795	RealtekS_38:d9:78	Broadcast	ARP	Gratuitous ARP for
2249	10.477119	RealtekS_38:d9:78	Broadcast	ARP	Gratuitous ARP for
2286	10.936417	20:6a:8a:10:08:40	Broadcast	ARP	who has 172.18.186

Frame 200 (60 bytes on wire, 60 bytes captured)

Ethernet II, Src: RealtekS_c2:77:78 (00:e0:4c:c2:77:78), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Address Resolution Protocol (request)

Offset	Hex	ASCII
0000	ff ff ff ff ff ff 00 e0 4c c2 77 78 08 06 00 01 L.wx....
0010	08 00 06 04 00 01 00 e0 4c c2 77 78 ac 12 ba 76 L.wx...v
0020	00 00 00 00 00 00 00 ac 12 ba 42 00 00 00 00 00B.....
0030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File: "F:\etherXXXXa02980" 1829 KB 00:... Packets: 2454 Displayed: 17 Marked: 0 ... Profile: Default

协议分析软件Wireshark

- ❑ Wireshark窗口的数据包列表的每一行都对应着网络上的单独一个数据包。默认情况下，每行会显示数据包的时间、源地址和目标地址，所使用的协议及关于数据包的一些信息。通过单击此列表中的某一行，可以获悉更详细的信息
 - ❑ 中间的树状信息包含着上部列表中选择某数据包的详细信息。“+”图标揭示了包含在数据包内的每一层信息不同的细节内容。这部分的信息分布与查看的协议有关，一般包含物理层、数据链路层、网络层、传输层等各层信息
 - ❑ 底部的窗格以十六进制及ASCII形式显示出数据包的内容，其内容对应于中部窗格的某一行
-

协议分析软件Wireshark

- Wireshark是一款功能强大而操作相对简便的抓包软件。在进行网络实验时，往往采用抓包分析的方法来验证一些实验，故应熟练掌握此工具软件
-

实验报告

- ❑ 每次实验由老师给出有具体要求的模板，学生按要求完成实验；
 - ❑ 实验报告必须独立完成，如有抄袭行为，抄袭各方均以“0”分计；
 - ❑ 实验作业要按时完成。逾期未交者，不接受补交。不能在期末一次补交多个作业。
-

实验报告

- 对实验过程进行监控
 - 注意实验前后的对比、分析
 - 实验截图
 - 当前活动窗口（同时按下Alt+PrScrn键）
 - 整个屏幕（按下PrScrn键）
 - 窗口中的任意部分（使用Windows附件中的截图工具）
 - 截图加工（使用Windows附件中的图画工具）
 - 撰写实验报告
-

实验截图例



阅读文献

- 陈霜霜，计算机网络安全的研究与探讨.科技信息，**2011（35），136-137**
 - 王世伟，论信息安全、网络安全、网络空间安全.中国图书馆学报，**2015/2，72-84**
-