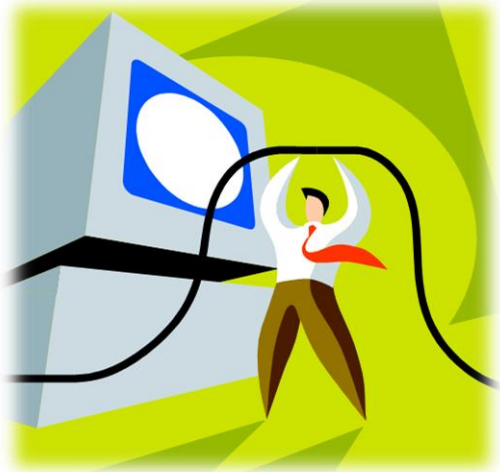
第1章　计算机网络的定义、发展、分类与拓朴

➢学习目标

- 理解网络的定义；
- 掌握网络的分类与拓扑结构（重点）；
- 理解计算机网络体系结构的概念（重点）；
- 掌握OSI/RM模型的分层结构（重点难点）；
- 理解报文的封装与解封装过程（重点）；
- 掌握TCP/IP协议族的各层典型协议（重点）；
- 掌握IP地址分类（重点）；
- 掌握子网划分的编址方法（重点难点）。



五、OSI参考模型

网络协议就是为了使计算机网络中的不同设备能进行数据通信而预先制定的一套通信双方相互了解和共同遵守的格式和约定，是一系列规则和约定的规范性描述，定义了网络设备之间如何进行信息交换。网络协议是计算机网络的基础，只有遵从相应协议的网络设备之间才能够通信。

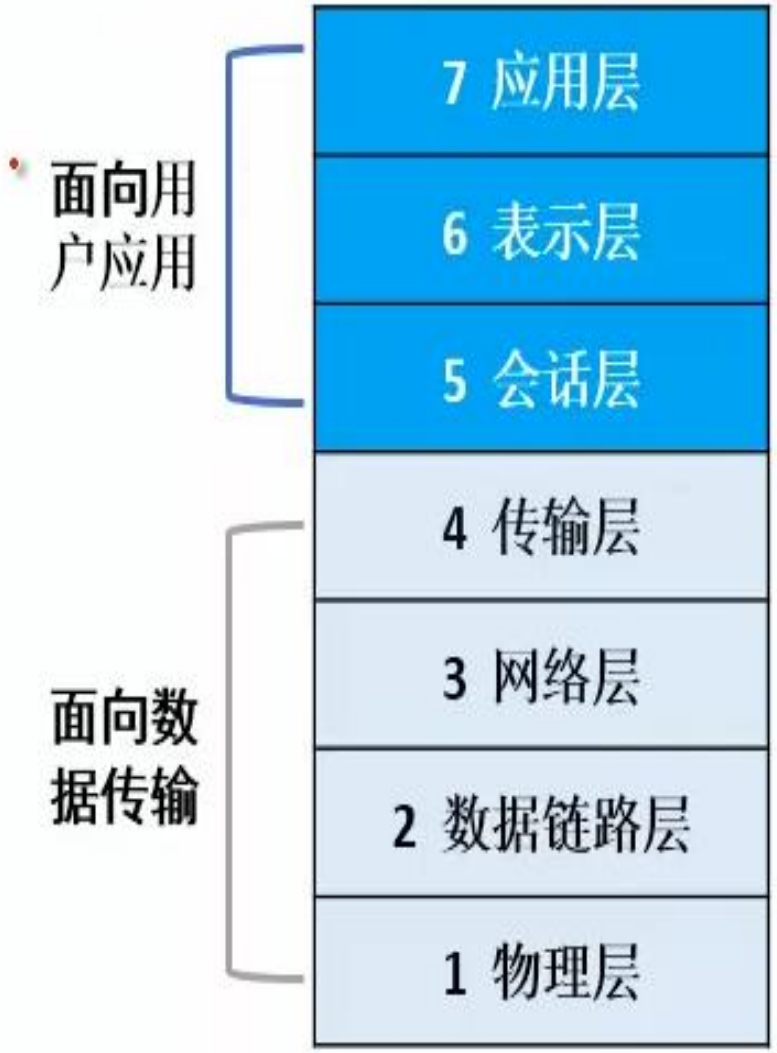
分层法最核心的思路是上一层的功能建立在下一层的功能基础上，并且在每一层内均要遵守一定的规则。

层次和协议的集合组成网络的体系结构。体系结构应当具有足够的信息，以允许软件设计人员为每层编写实现该层协议的有关程序，即通信软件。

为了解决网络之间的兼容性问题，帮助各个厂商生产出可兼容的网络设备，国际标准化组织（International Organization for Standardization，ISO）于1984年提出开放系统互联（Open System Interconnection，OSI）参考模型。OSI参考模型很快成为了计算机网络通信的基础模型。

如图所示，OSI参考模型采用分层结构技术将整个网络的通信功能分为7层，由低层至高层依次是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。每一层都有各自特定的功能，并且上一层会利用下一层所提供的功能和服务。

图OSI参考模型



- ✓ OSI模型每层都定义了自己的功能集
- ✓ 层与层之间相互独立又相互依靠
- ✓ 上层依赖于下层，下层为上层提供服务

1．应用层

应用层是OSI参考模型中的最高层，直接面向用户以满足不同的需求，是利用网络资源唯一向应用程序直接提供服务的层次。应用层主要由用户终端的应用软件构成，如常见的Telnet、FTP、SNMP等协议都属于应用层的协议。

2．表示层

表示层主要解决用户信息的语法表示问题，它向上为应用层提供服务。表示层的功能是对信息进行格式和编码的转换，例如将ASCII码转换成EBCDIC码等，确保一个系统的应用层发送的数据能被另一个系统的应用层识别。此外，对传送的信息进行加密与解密也是表示层的任务。

3．会话层

会话层的任务就是提供一种有效的方法来组织及协调两个表示层进程之间的会话，并管理它们之间的数据交换。会话层的主要功能是依据应用进程之间的原则，按照正确的顺序发/收数据，进行各种形态的对话。这些对话既包括核实对方是否有权参加会话，也包括通过协商选择一致的通信方式，如选全双工通信还是选半双工通信。

4．传输层

传输层位于OSI参考模型的第四层，可以为主机应用程序提供端到端的数据传输服务。设备通过端口号来区分每一个应用程序进程，因此，可以说传输层的任务是负责为两个主机进程间的通信提供通用的数据传输服务。传输层的基本功能包括分段与数据重组、按端口号寻址、连接管理、差错控制和流量控制等。

5．网络层

网络层是OSI参考模型的第三层，介于传输层与数据链路层之间。数据链路层提供两个相邻节点间数据帧的传输功能，网络层在此基础上进一步管理网络中的数据通信，选择合适的路径并转发数据包，使数据包从源端经过若干中间节点传输到目的端，从而向传输层提供最基本的端到端的数据传输服务。

网络层的主要功能包括编址、路由选择、拥塞管理、异种网络互联等。

6．数据链路层

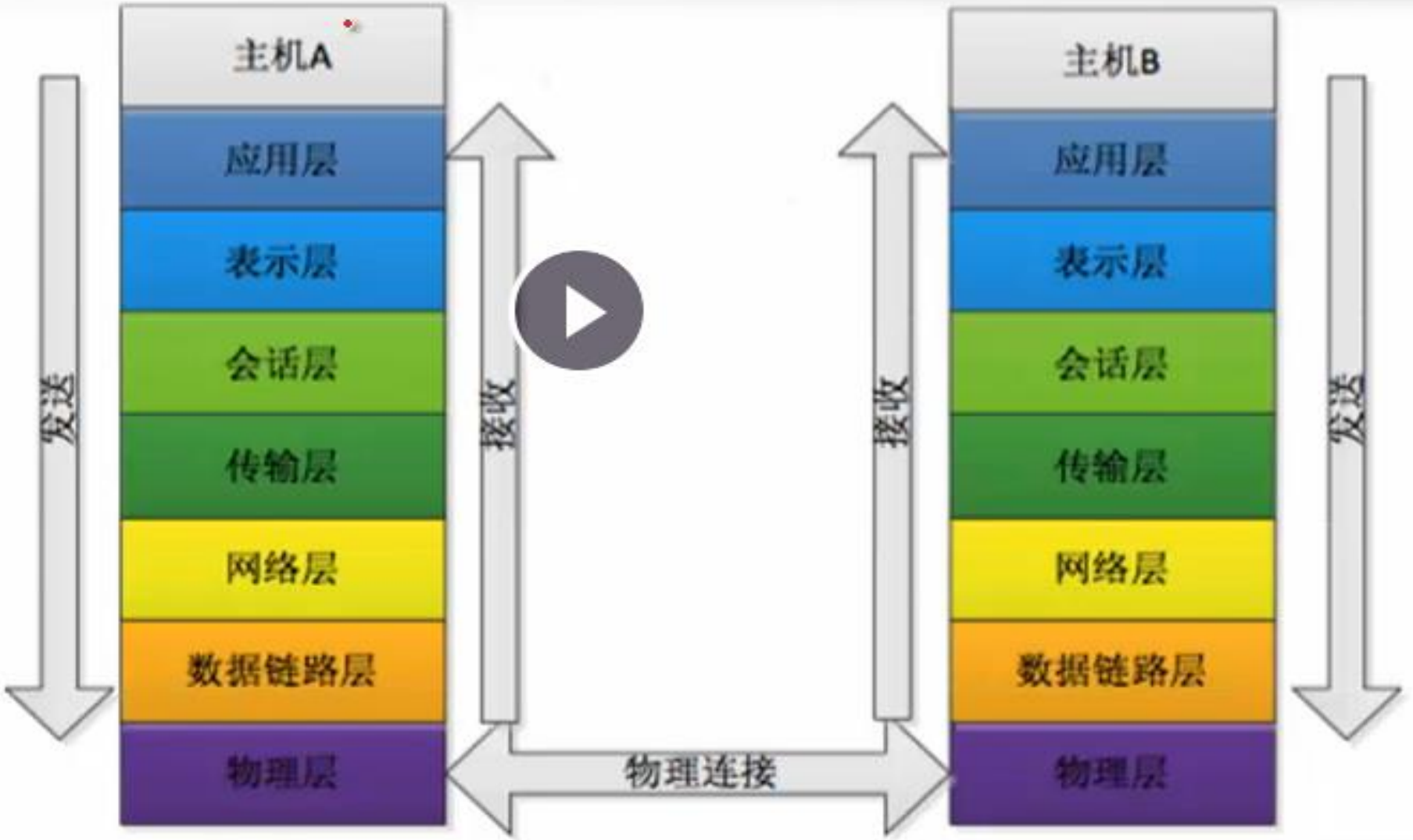
数据链路层是OSI参考模型的第二层，介于物理层和网络层之间，主要负责物理层面上互联节点之间的数据传输。数据链路层利用物理层的服务，在通信实体间传输以帧为单位的数据单元，并采用差错控制和流量控制方法建立可靠的数据传输链路。数据链路层是对物理层传输原始比特流功能的加强，将物理层提供的可能出错的物理连接改造成逻辑上无差错的数据链路，使之对网络层表现为无差错的线路。

7．物理层

物理层是OSI参考模型的第一层，也是最低层，功能是提供比特流传输。在这一层中规定的既不是物理媒介，也不是物理设备，而是物理设备和物理介质相连接的方法及规定。

物理层协议定义了通信传输介质的机械特性、电气特性、功能特性和规格特性。机械特性说明端口所使用接线器的形状和尺寸、引线的数目和排列等，例如，对各种规格的电源插头的尺寸都有严格的规定。电气特性说明在端口电缆的每根线上出现的电压、电流的范围。功能特性说明某根线上出现的某一电平表示何种意义。规格特性说明各种不同功能的可能事件的出现顺序。

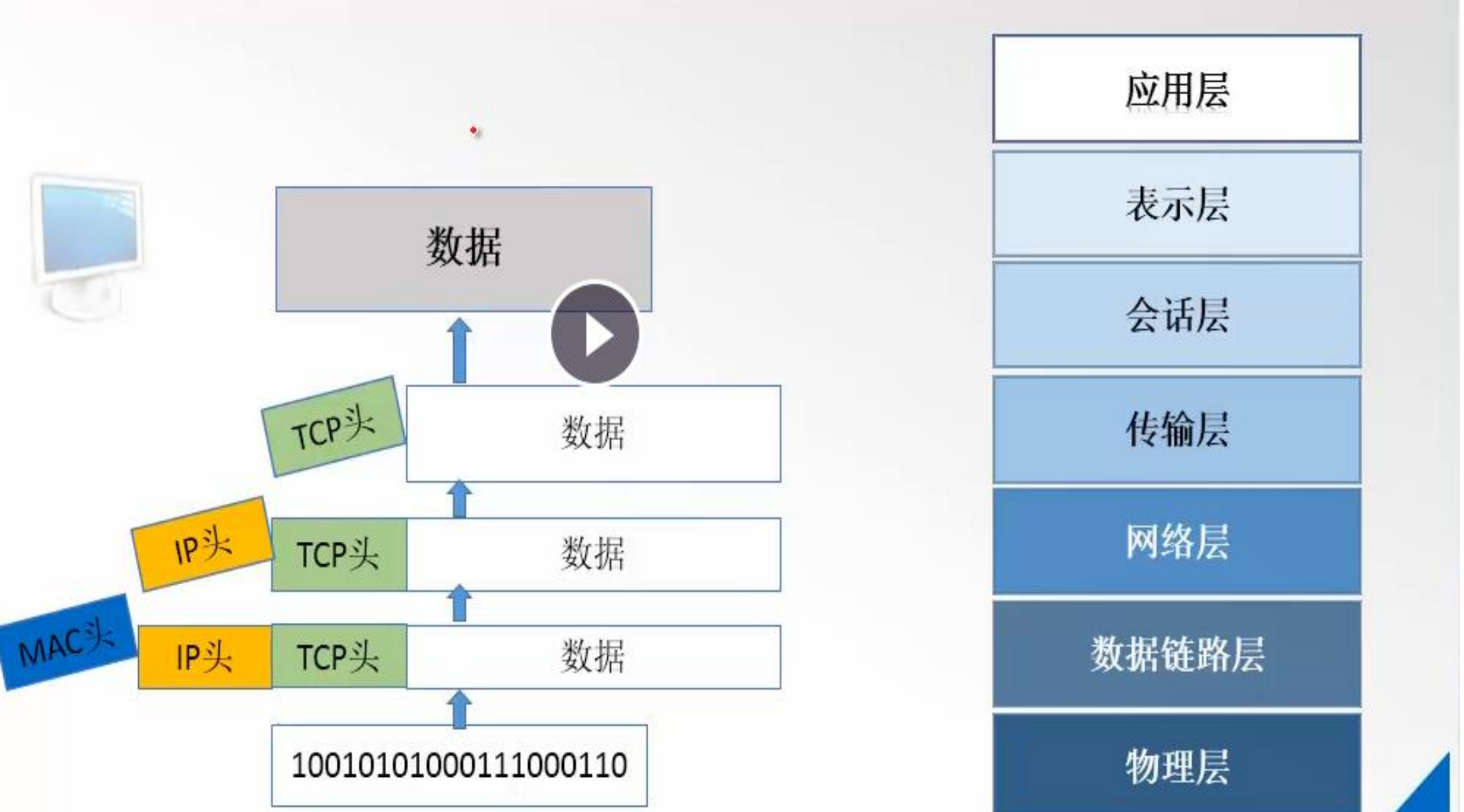

为应用程序提供网络服务
应用层
数据格式化、加密、解密
表示层
建立、维护、管理会话连接
会话层
建立、维护、管理主机端到端连接
传输层
段
IP寻址和路由选择
网络层
数据包
控制网络层与物理层之间通信
数据链路层
帧
比特流传输
物理层
比特流


主机A
应用层
表示层
会话层
传输层
网络层
数据链路层
物理层
发送
接收
物理连接
主机B
应用层
表示层
会话层
传输层
网络层
数据链路层
物理层
接收
发送

数据传输过程


数据
TCP头
数据
IP头
TCP头
数据
MAC头
IP头
TCP头
数据
应用层
表示层
会话层
传输层
网络层
数据链路层
物理层

数据封装过程


数据
TCP头
数据
IP头
TCP头
数据
MAC头
IP头
TCP头
数据
10010101000111000110
应用层
表示层
会话层
传输层
网络层
数据链路层
物理层

数据解封过程

六、TCP/IP协议族

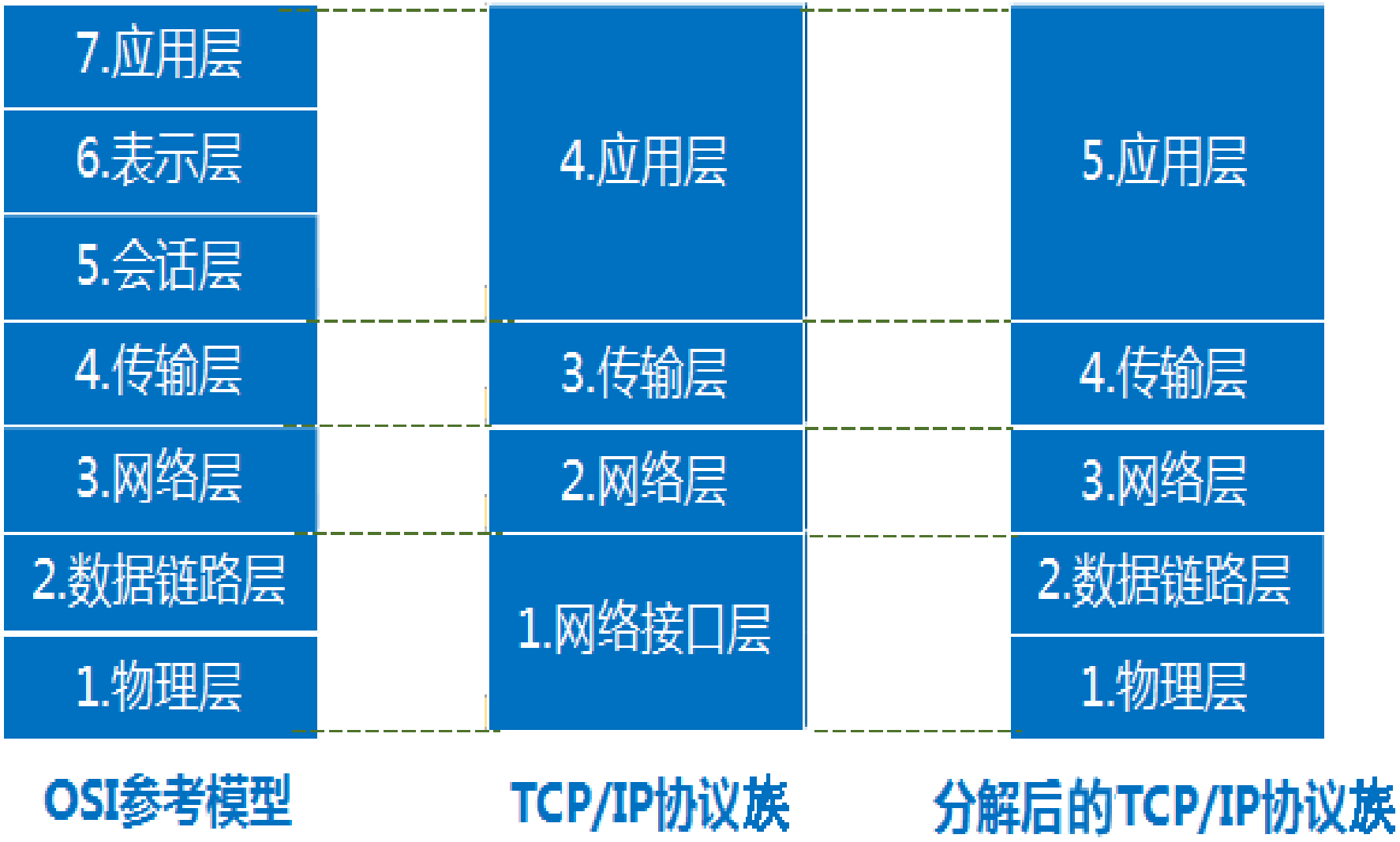
1 TCP/IP协议族概述

TCP/IP协议族起源于1969年美国国防部高级研究项目管理局（Advanced Research Projects Agency，APRA）有关分组交换广域网（Packet-Switched Wide-Area Network）的科研项目，因此起初的网络称为ARPA网。1973年，TCP（传输控制协议）正式投入使用；1981年，IP（网际协议）投入使用。TCP/IP协议族得到了众多厂商的支持，不久就有了很多分散的网络。

所有这些单个的TCP/IP网络互联起来组成了Internet。基于TCP/IP协议族的Internet已逐步发展成为当今世界上规模最大、拥有用户和资源最多的超大型计算机网络，TCP/IP协议族也因此成为事实上的工业标准，而且IP网络也正逐步成为当代乃至未来计算机网络的主流。

与OSI参考模型一样，TCP/IP协议族也分为不同的层次，每一层具有不同的通信功能。但是，TCP/IP协议族简化了层次设计，将原来的7层模型合并为4层体系结构，自顶向下依次是应用层、传输层、网络层、网络接口层，结构比较简单，分层少。

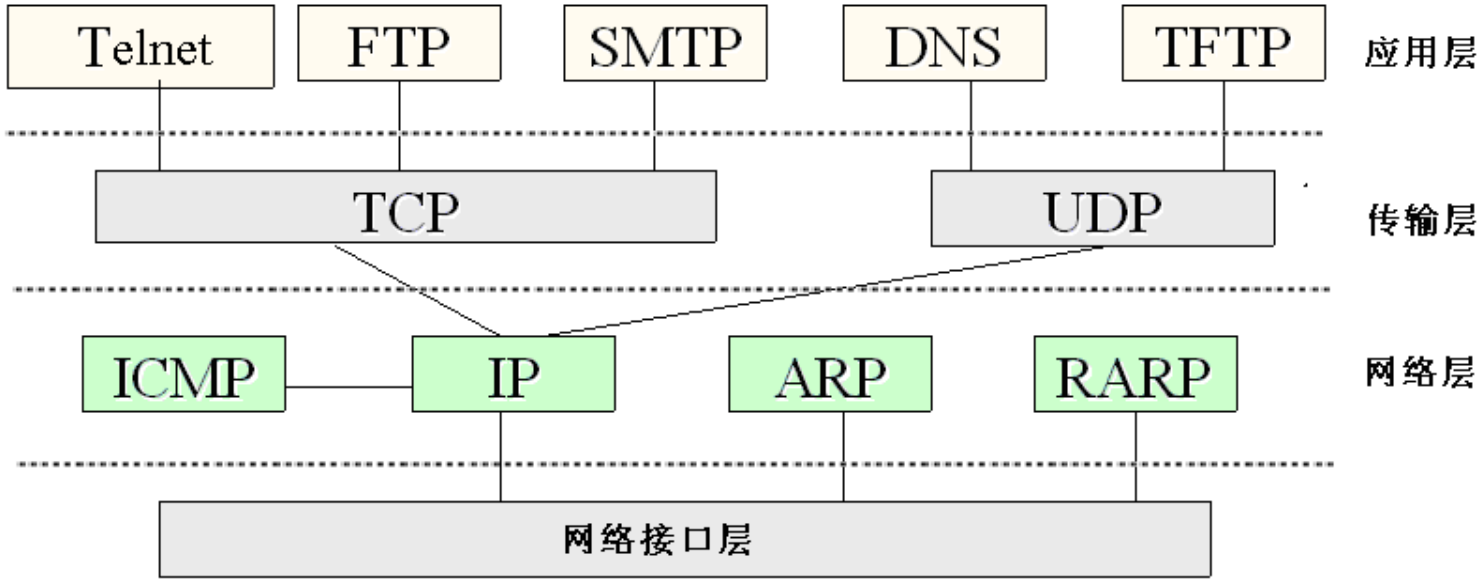
从图可以看出，TCP/IP协议族协议的层次与OSI参考模型的层次有清晰的对应关系，应用层包含了OSI参考模型的应用层、表示层和会话层的所有协议，网络接口层包含了OSI参考模型的数据链路层和物理层的所有协议。为了结合实际应用理解计算机网络通信的整个过程，分析时常将TCP/IP协议族网络接口层分解成数据链路层和物理层。TCP/IP协议族是在Internet网络的不断发展中建立的，基于实践，有很高的可信任度。相比较而言，OSI参考模型是基于理论的，主要作为一种向导。



图TCP/IP协议族与OSI参考模型比较

TCP/IP协议族负责确保网络设备之间能够通信。TCP/IP协议族是数据通信协议的集合，包含许多协议，TCP/IP这个名字来源于其中最主要的两个协议TCP和IP。

TCP/IP协议族各层次支持的协议如图2-4所示。

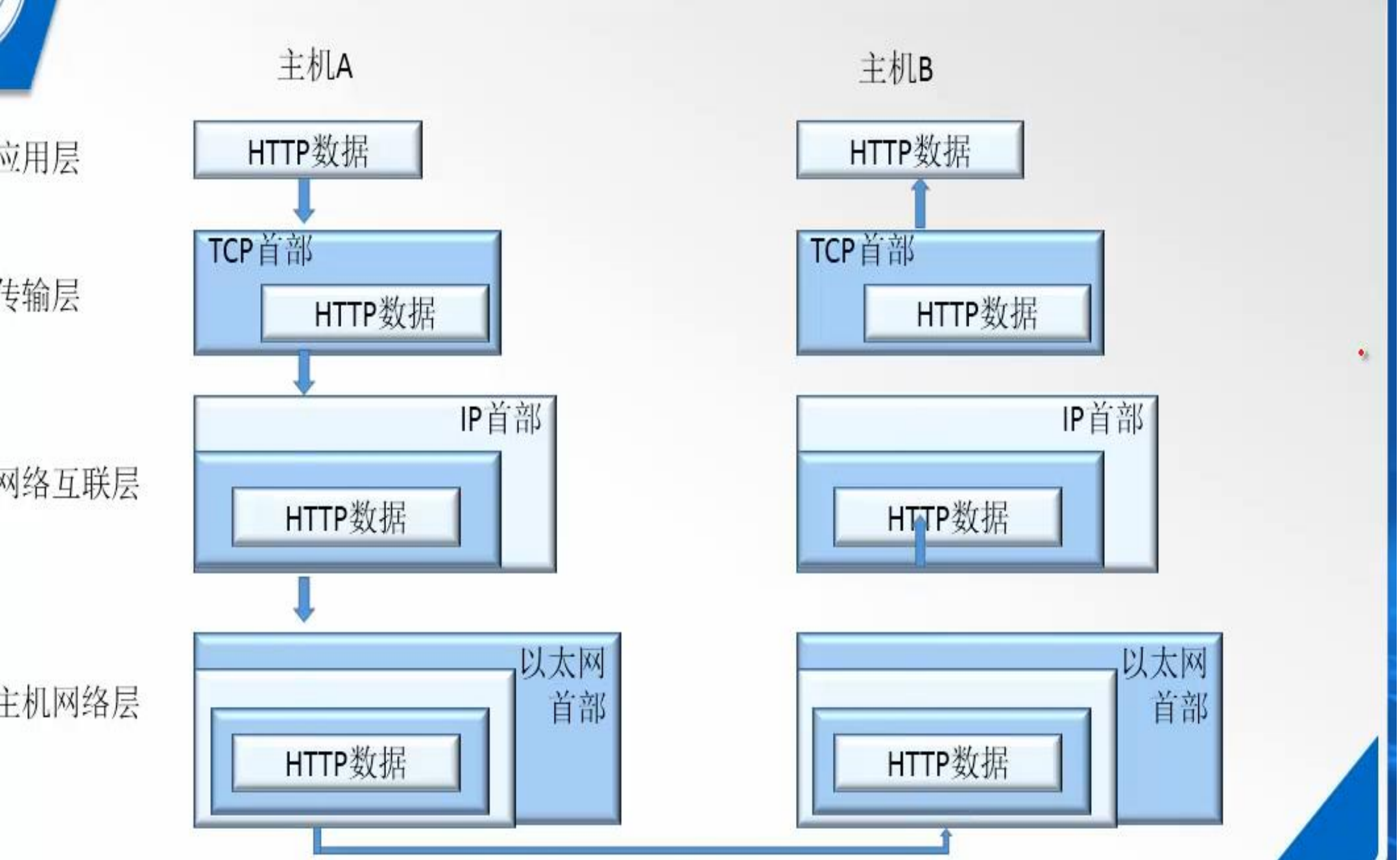


图TCP/IP协议族各层次支持的协议

2. TCP/IP各层功能

层次名称	功 能	协 议
应用层 （Application Layer ）	负责实现一切与应用程序相关的功能	FTP（文件传输协议） HTTP（超文本传输协议） DNS（域名服务器协议） SMTP（简单邮件传输协议） NFS（网络文件系统协议）
传输层 （Transport Layer ）	负责提供可靠的传输服务	TCP（控制传输协议） UDP（用户数据报协议）
网际层 （Inter-network Layer ）	负责网络间的寻址、数据传输，	IP（网际协议） ICMP（网际控制消息协议） ARP（地址解析协议） RARP（反向地址解析协议）
网络接口 （Host-to-Net Layer ）	负责实际数据的传输	HDLC（高级链路控制协议） PPP（点对点协议） SLIP（串行线路接口协议）

3. TCP/IP的数据传输过程



报文的封装与解封装

TCP/IP协议族的每个层次接收上层传递过来的数据后，都要将本层次的控制信息加入数据单元的头部，一些层次还要将校验和等信息附加到数据单元的尾部，这个过程叫作封装。

在发送方，封装的操作是逐层进行的，应用层的应用程序将要发送的数据传送给传输层，传输层将数据分为大小一定的数据段后加上本层的报文头发送给网络层。传输层报文头中包含接收它所携带的数据的上层协议或应用程序的端口号，例如，Telnet 的端口号是23。传输层协议利用端口号来调用和区别应用层的各种应用程序。

网络层对来自传输层的数据段进行一定的处理，例如，利用协议号区分传输层协议、寻找下一跳地址、解析数据链路层物理地址等，加上本层的IP报文头后转换为数据包，然后发送给数据链路层。

数据链路层依据不同的协议为数据加上本层的帧头后发送给物理层。

物理层以比特流的形式将报文发送出去。

TCP/IP协议族的数据封装如图2-5所示。

协议数据单元（Protocol Data Unit，PDU）是指对等层次之间传递的数据单位。

每层封装后的PDU有不同叫法，应用层的PDU统称为data（数据），传输层的PDU称为segment（数据段），网络层的PDU称为packet（数据包），数据链路层的PDU称为frame（数据帧），物理层的PDU称为bits（比特流）。

当数据到达接收端时，每一层读取相应的控制信息后根据控制信息中的内容向上层传递数据单元，在向上层传递之前会去掉本层的控制头部信息和尾部信息（如果有），此过程叫作解封装。这个过程逐层执行，直至将对端应用进程产生的数据发送给本端相应的应用进程。

七、传输层协议

传输层协议有TCP（传输控制协议）和UDP（用户数据报协议）两种，虽然TCP和UDP都使用相同的网络层协议IP，但是TCP和UDP却分别为应用层提供完全不同的服务。

TCP为应用程序提供可靠的面向连接的通信服务，适用于要求得到响应的应用程序。目前，许多流行的应用程序都使用TCP。

UDP提供了无连接通信，且不对传输数据包提供可靠的保证，适于一次传输少量数据的情况，可靠性由应用层来负责。

1.TCP

TCP 提供面向连接的、可靠的字节流服务。面向连接意味着使用TCP作为传输层协议的两个应用之间在相互交换数据之前必须建立一个TCP 连接，TCP 通过确认、校验、重组等机制为上层应用提供可靠的传输服务。但是TCP 连接的建立及确认、校验等功能会产生额外的开销。

1）TCP的报文格式

下图所示为TCP的报文格式。


0
8
16
24
31
16位源端口
16位目的端口
32位序列号
32位确认号
头长度
保留(6位)
U
A
P
R
S
F
16位窗口大小
16位TCP校验和
16位紧急指针
选 项
数 据
20B

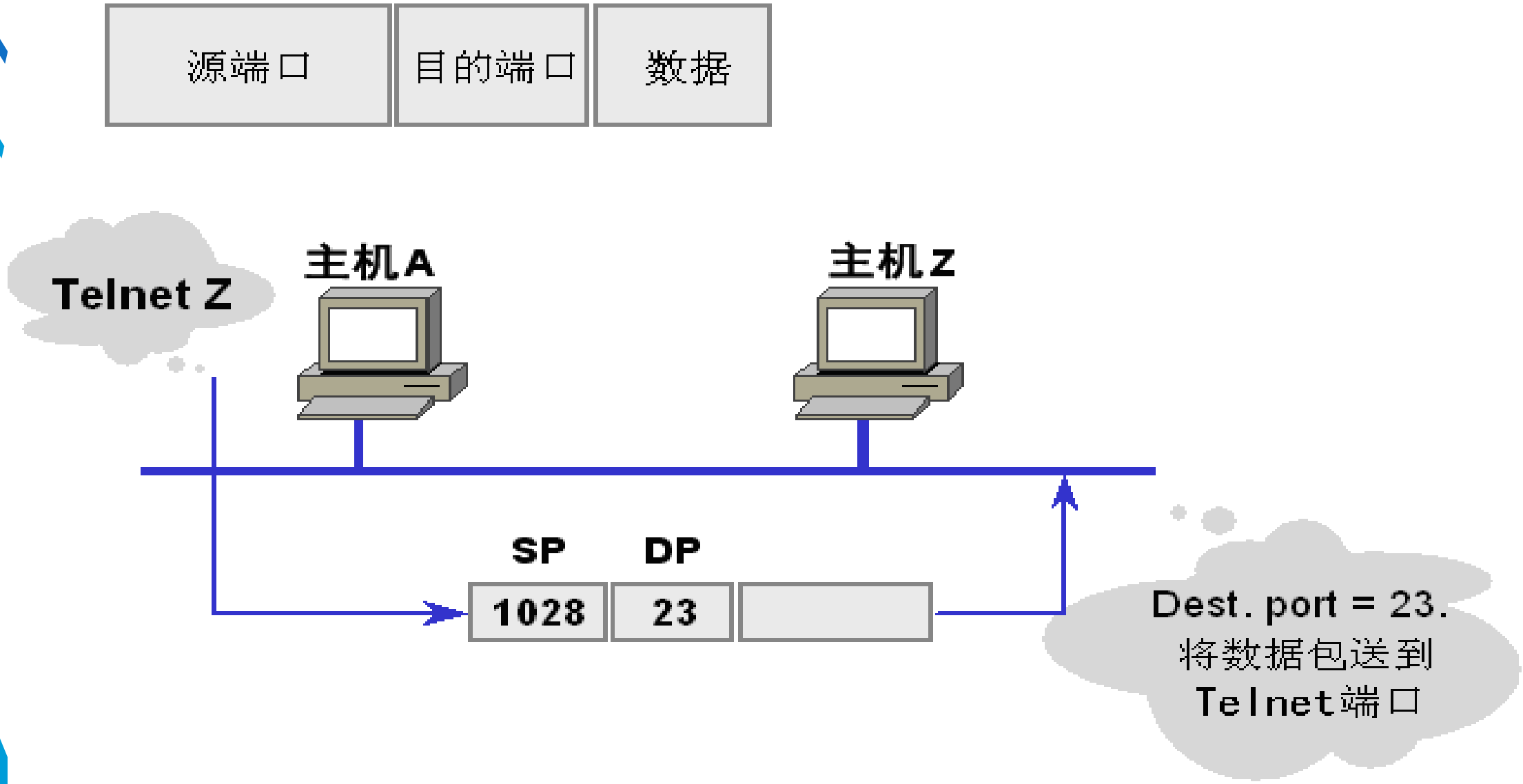
TCP的报文格式

（1）每个TCP报文头部都包含源端口号（Source Port）和目的端口号（Destination Port），用于标识和区分源端设备和目的端设备的应用进程。在TCP/IP协议族中，源端口号和目的端口号分别与源IP地址和目的IP地址组成套接字，唯一地确定一条TCP连接。

TCP/IP协议族的协议所提供的服务使用的端口号一般是1～1023，这些端口号由Internet号码分配机构（Internet Assigned Numbers Authority，IANA）分配管理，其中，低于255的端口号保留，用于公共应用；255～1023的端口号分配给各个公司，用于特殊应用。高于1023的端口号称为临时端口号，IANA未对其做规定。

常用的TCP端口号有HTTP 80、FTP 20/21、Telnet 23、SMTP 25及DNS 53等；常用的UDP端口号有DNS 53、BootP 67（Server）/ 68（Client）、TFTP 69及SNMP 161等。

如图2-7所示，主机A对主机Z进行Telnet远程连接，其中目的端口号为端口号23，源端口号为1028。对于源端口号，只需保证其在本机上是唯一的即可，一般从1023以上找出空闲端口号进行分配。因为源端口号存在的时间很短暂，所以源端口号又称作临时端口号。


源端口
目的端口
数据
Telnet Z
主机A
主机Z
SP
DP
1028
23
Dest. port = 23.
将数据包送到
Telnet端口

TCP的端口号示例

（2）序列号（Sequence Number）字段用来标识TCP源端设备向目的端设备发送的字节流，它表示这个字节流中的第一个数据字节。如果将字节流看作两个应用程序间的单向流动，则TCP会用序列号对每个字节进行计数。序列号是一个32bit的数。

确认号（Acknowledgement Number，32bit）包含发送确认的一端所期望接收到的下一个字节的序号。因此，确认号应该是上次已成功收到的数据字节序列号加1。

TCP的序列号和确认号应用示例如图2-8所示。

- 序列号的作用：一方面用于标识数据顺序，以便接收者在将其递交给应用程序前按正确的顺序进行装配；另一方面用于消除网络中的重复报文包，这种现象在网络拥塞时会出现。
- 确认号的作用：接收者告诉发送者哪个数据段已经成功接收，并告诉发送者希望接收的下一个字节。

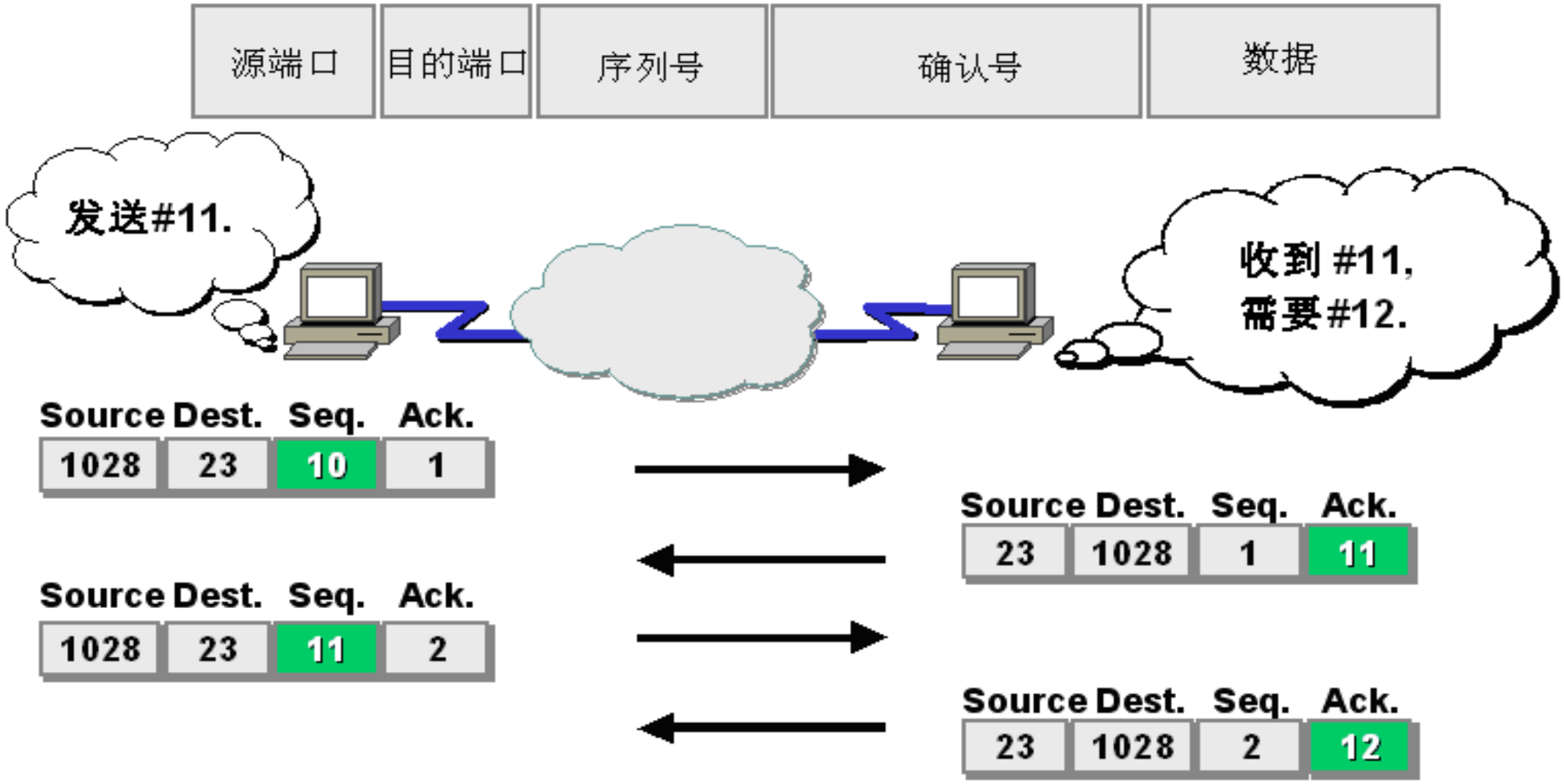


图2-8 TCP的序列号和确认号应用示例

（3）TCP的流量控制功能由连接的每一端通过声明的窗口大小（Windows Size）来实现。窗口大小用字节数来表示，例如Windows Size=1024，表示一次可以发送1024B的数据。窗口大小起始于确认号指明的值，是一个16bit字段，可以调节。

TCP的窗口控制示例如图2-9所示。假定发送方设备每一次发送4096B数据，也就是窗口大小为4096，接收方设备成功接收数据包，用序列号4097确认。接收方设备由于性能的原因还未全部送至上层协议处理时，也将发送确认报文对收到的数据进行确认，同时调整窗口大小。发送方设备收到确认后，将以窗口大小2048发送数据。如果发送方接收到携带窗口号为0的确认，将停止这一方向的数据传输，直到收到窗口号大于0的确认报文再进行发送。

滑动窗口机制为端到端设备间的数据传输提供了可靠的流量控制机制。然而，它只能在源端设备和目的端设备上起作用，当网络中间设备（如路由器等）发生拥塞时，滑动窗口机制将不起作用。此时可以利用ICMP源抑制机制进行拥塞管理。

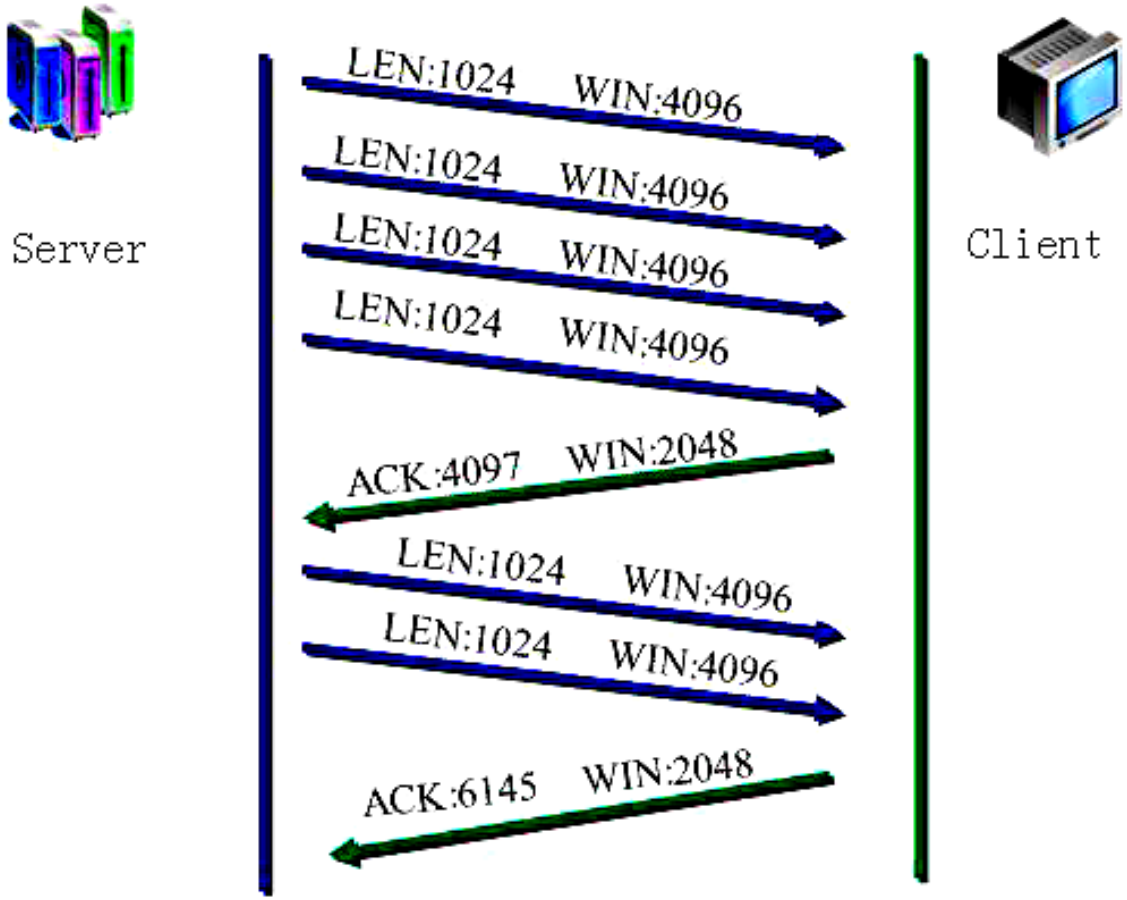


图2-9 TCP的窗口控制示例

2）TCP三次握手——建立连接

TCP是面向连接的传输层协议，所谓面向连接，就是在真正的数据传输开始前要完成连接建立的过程，否则不会进入真正的数据传输阶段。

TCP的连接建立过程通常称为三次握手，如图2-10所示。

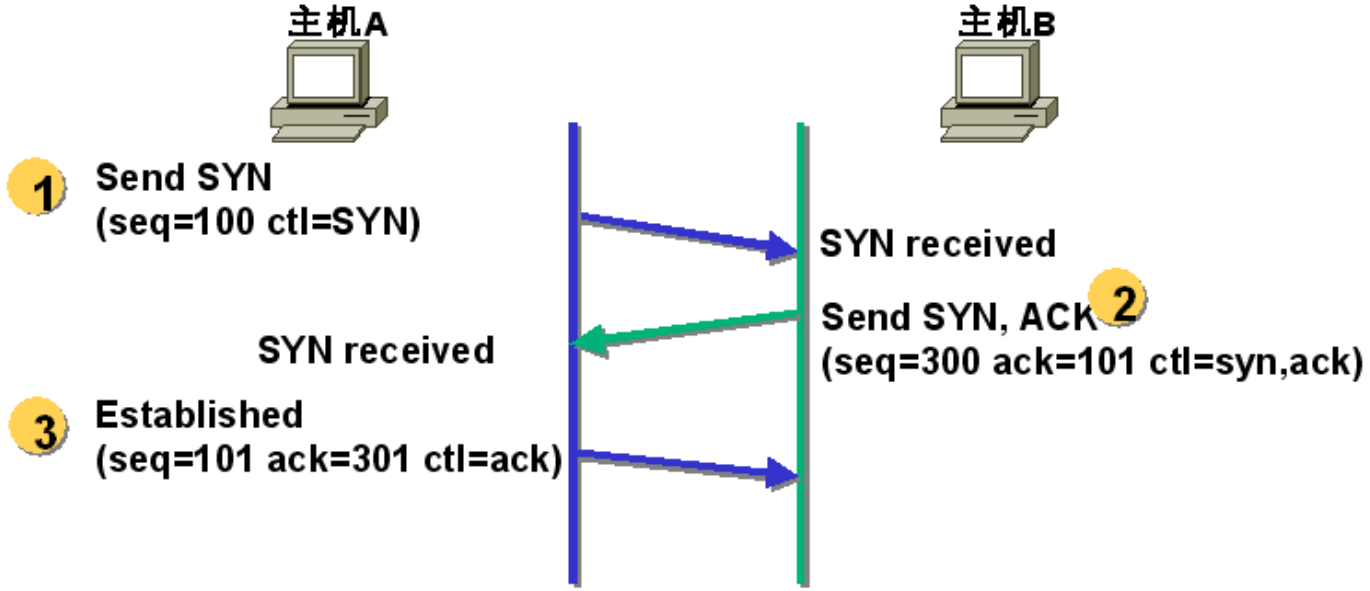


图2-10 TCP三次握手

（1）主机A发送一个初始序列号为100的报文段1。

（2） 主机B发回包含自身初始序列号300的报文段2，并用确认号101对主机A的报文段1进行确认。

（3）主机A接收主机B发回的报文段2，发送报文段3，用确认号301对报文段2进行确认。

这样便在主机和服务器之间成功建立了一条TCP连接。

3）TCP四次握手——终止连接

TCP连接采用全双工方式传输数据，因此每个方向必须单独进行关闭。当一方完成它的数据发送任务后，就发送一个FIN指令来终止这个方向的连接。一端收到一个FIN指令后，它必须通知应用层另一端已经终止了那个方向的数据传送。可见TCP终止连接的过程需要四次信息交互，称为四次握手，如图2-11所示。

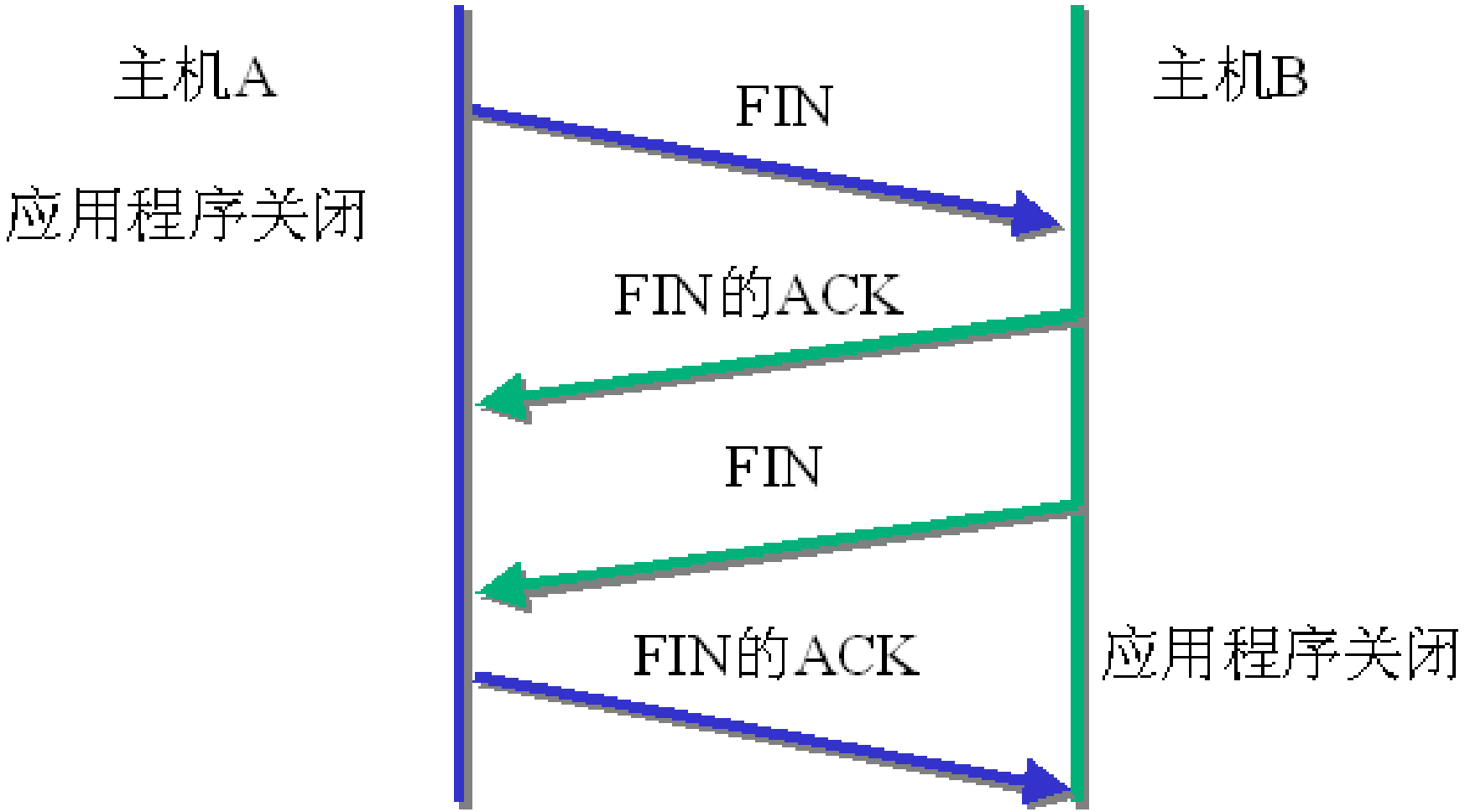
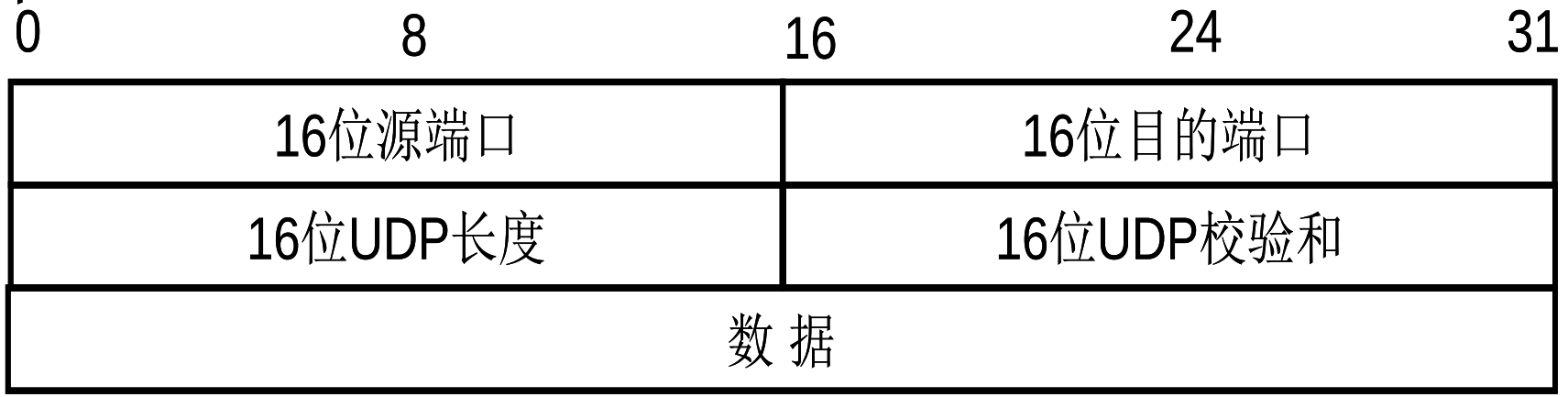


图2-11 TCP四次握手

2 UDP

相对于TCP报文，UDP报文只有少量的字段，包括源端口号、目的端口号、长度、校验和等，如图2-12所示，各个字段功能和TCP报文的相应字段一样。



UDP的报文格式

2.6 IP

IP是TCP/IP协议族中最为核心的协议，处于网络层。IP作为低开销协议，只提供通过互联网系统从源主机向目的主机传送数据包所必需的功能。IP不关心数据报文的内容，提供无连接的、不可靠的服务。

网络层收到传输层的TCP数据段后，会再为其加上网络层IP 头部信息。普通的IP 头部长度固定为20B，不包含IP选项字段。IP数据报文格式如图2-13所示。

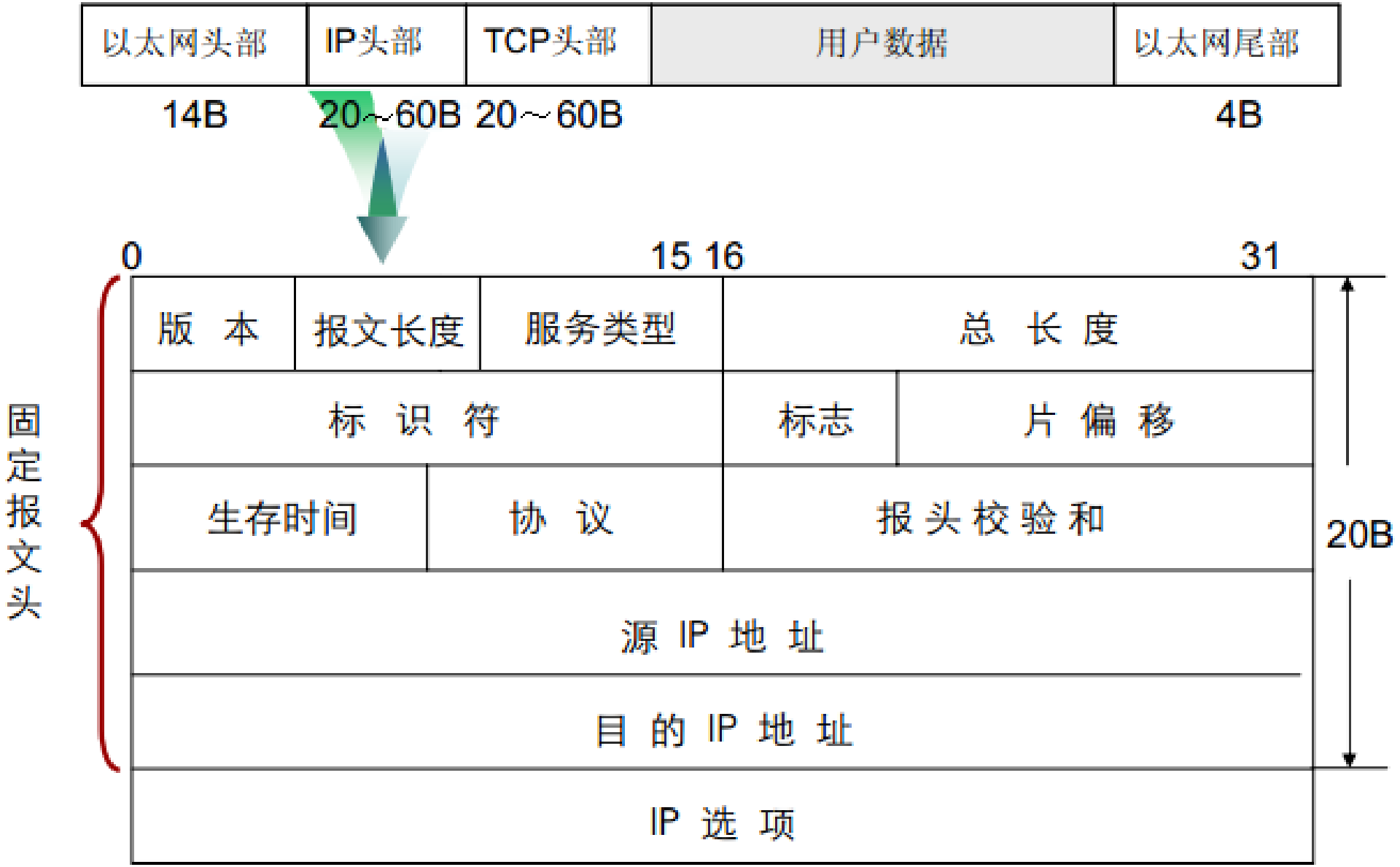


图2-13 IP数据报文格式

（1）版本（Version）：标明IP的版本号。目前的协议版本号为4，下一代IP的版本号为6。

（2）报文长度：指的是以32bit组（即4B）为单位的IP数据包头部长度，包括IP选项。由于它是一个4bit字段，每单位代表4B，因此首部最长为60B。普通IP数据包（没有任何选择项）字段的值是5，即长度为20B。

（3）服务类型（TOS）：包括一个3bit的优先权子字段、4bit的TOS子字段和1bit未用位（必须置0）的子字段。4bit的TOS分别代表最小时延、最大吞吐量、最高可靠性和最小费用。4bit中只能置其中的1bit为1。

（4）总长度：指整个IP数据包的长度，以字节为单位。利用报文长度字段和总长度字段，就可以知道IP数据包中数据内容的起始位置和长度。由于该字段长16bit，所以IP数据包最长可达65535B。

（5）标志：唯一地标识主机发送的每一份数据包。通常每发送一份报文，它的值就会加1。数据链路层一般要限制每次发送数据帧的最大长度。IP把最大传输单元MTU与数据包长度进行比较，如果需要则进行分片，分片可以发生在源端主机上，也可以发生在中间路由器上。把一份IP数据包分片以后，只有到达目的地后才进行重新组装。重新组装由目的端的IP层来完成，其目的是使分片和重新组装过程对传输层（TCP和UDP）透明，即使只是丢失了一片数据，也要重传整个数据包。

（6）片偏移：指的是该片偏离原始数据包开始处的位置。当数据包被分片后，每个片的总长度值要改为该片的长度值。

（7）生存时间（Time To Live，TTL）：该字段设置了数据包可以经过的最多路由器数，它指定了数据包的生存时间。TTL的初始值由源端主机设置（通常为32或64），一旦经过一个处理它的路由器，它的值就减去1，当该字段的值为0时，数据包就被丢弃，并发送ICMP报文通知源主机。

（8）协议：用于识别向IP传送数据的协议。由于TCP、UDP、ICMP和IGMP及一些其他协议都要利用IP传送数据，因此IP必须在生成的IP首部中加入某种标志，以表明其承载的数据针对哪一类协议。其中，1表示为ICMP，2表示为IGMP，6表示为TCP，17表示为UDP。

（9）报头检验和：根据IP首部计算的检验和码。它不对首部后面的数据进行计算，因为ICMP、IGMP、UDP和TCP在它们各自的首部中均含有同时覆盖首部和数据的校验和码。

（10）IP选项：是数据包中的一个可变长的可选信息。在选项很少被使用，并非所有的主机和路由器都支持这些选项。IP选项字段一直都是以32bit作为界限，在必要的时候会插入值为0的填充字节，保证IP首部长度始终是32bit的整数倍。

（11）源IP地址和目的IP地址：每一份IP数据包都包含32bit的源IP地址和目的IP地址。