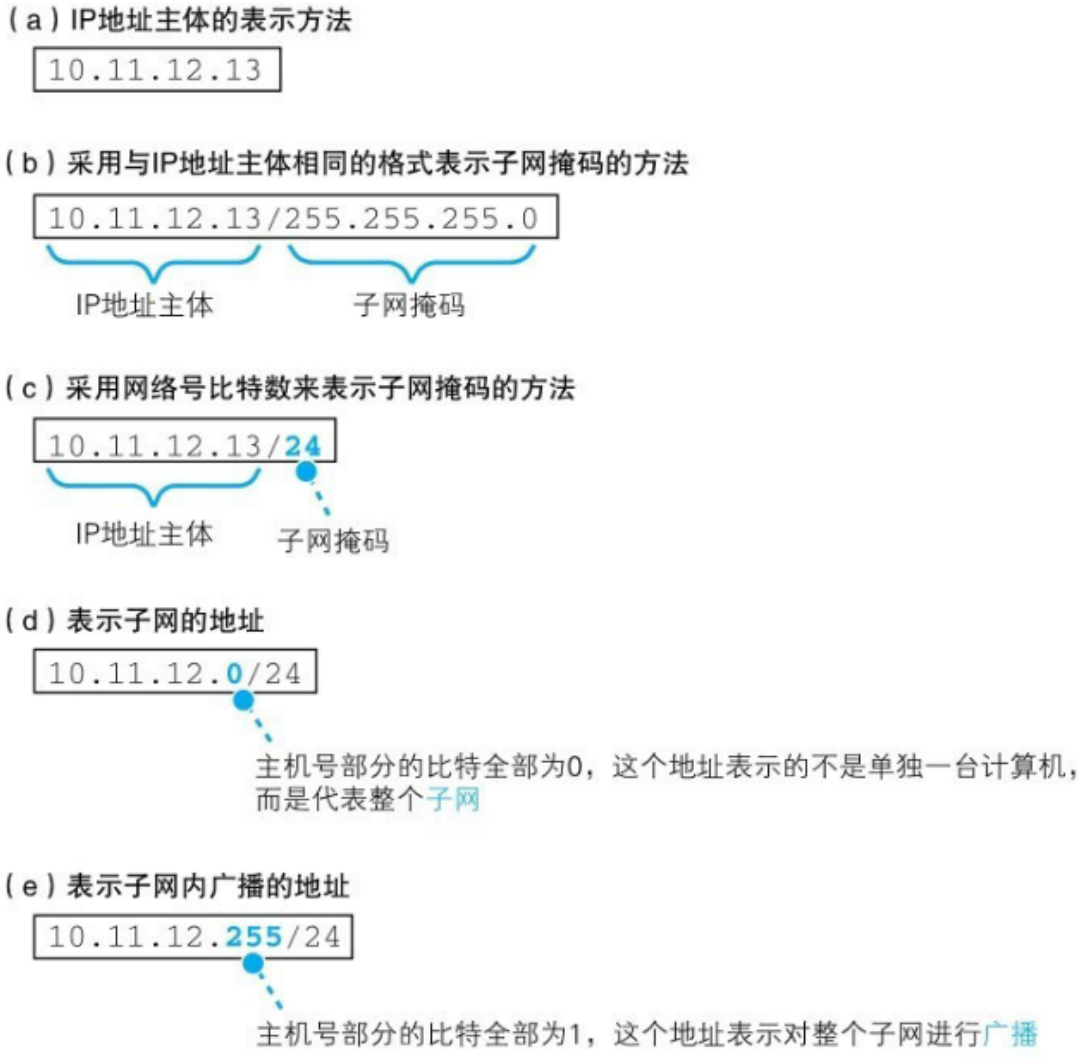
1 向DNS服务器查询Web服务器的IP地址

TCP/IP结构：多台计算机通过集线器连接起来形成子网，子网通过路由器连接起来形成网络。

IP地址类比 xx路xx号：网络号类比xx路，主机号类比xx号，整体称为IP地址。

简单的传输过程：子网内消息经过集线器转发到最近的路由器上，路由器经过路由器子网内的集线器转发到下一个路由器，以上步骤不断重复，直到抵达目的地。

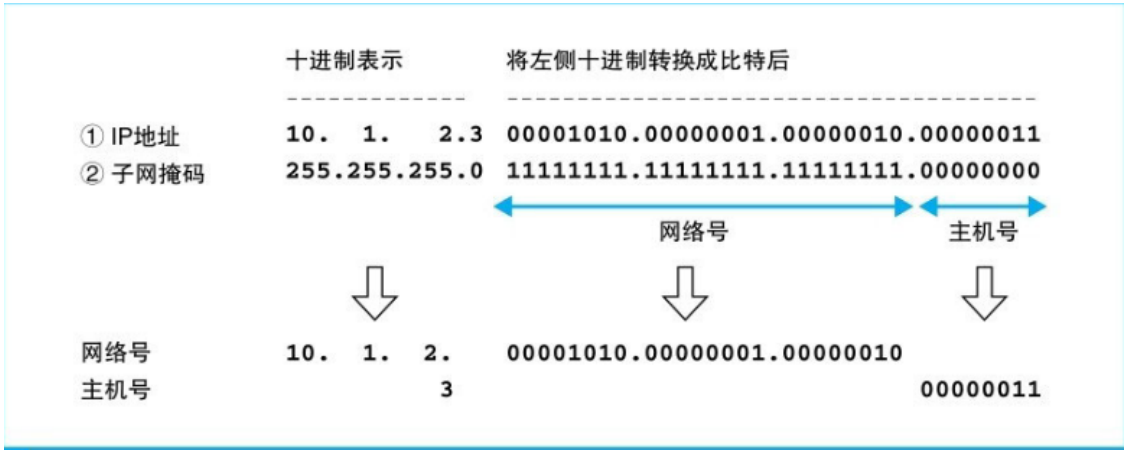
IP地址由4组8比特（1字节，八位二进制）数字组成。通过附加信息（子网掩码）可以判断哪部分是网络号，主机号。



子网掩码中1的部分即为网络号，0的部分为主机号。

1. a为IP地址主体

2. b为IP地址与子网掩码，如图



3. c为将子网掩码中1的个数写作一个数字

Socket库查询IP地址的过程：

1. 生成发送给DNS服务器的查询信息
2. 向DNS服务器发送UDP信息（操作系统协议栈）
3. DNS服务器回传一个UDP信息
4. 从响应信息中取出IP地址，存放到应用程序指定的内存地址中
5. 返回应用程序。

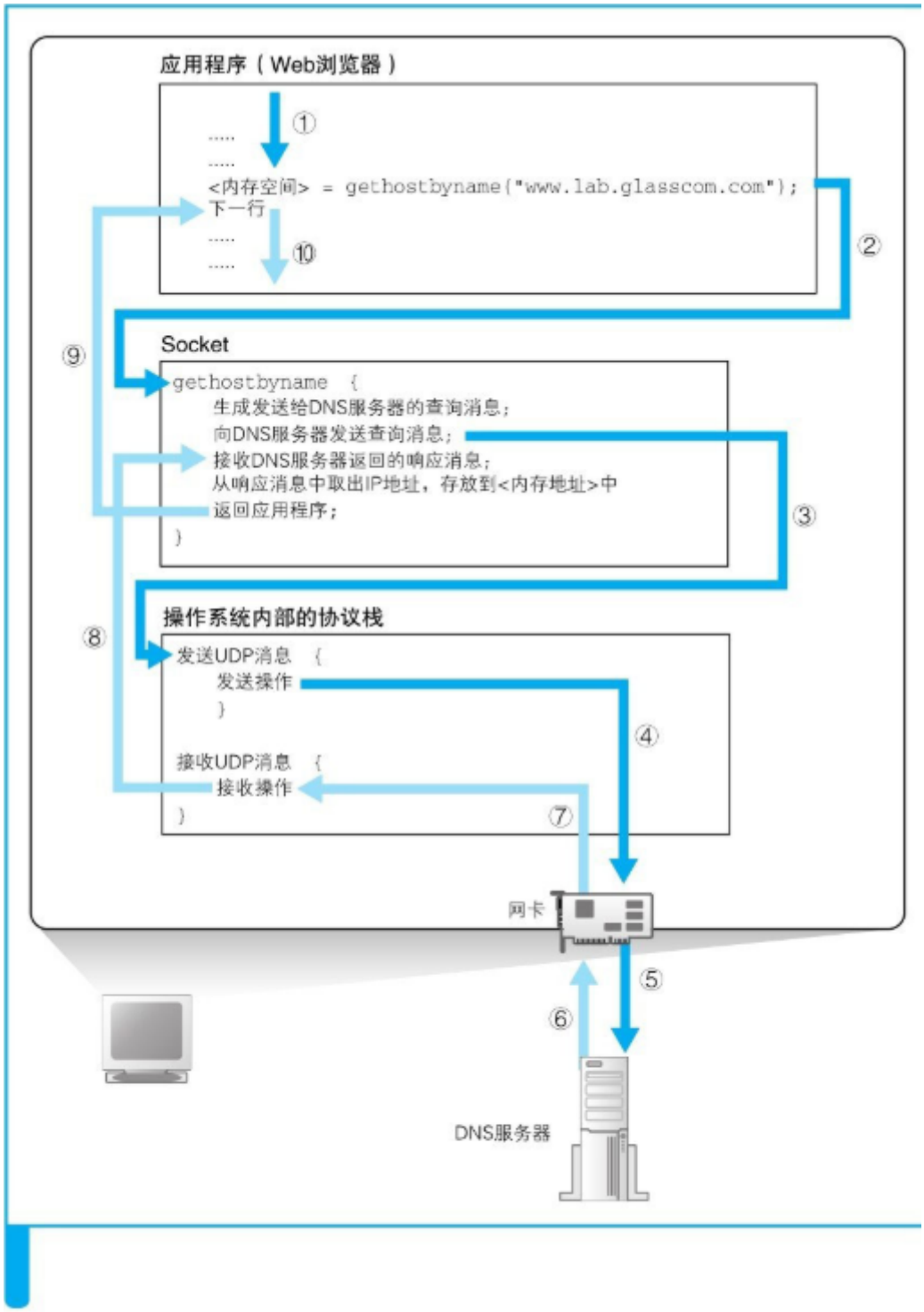


图1.12 调用解析器时计算机内部的工作流程

向DNS服务器发信息也需要知晓DNS服务器的IP地址，由TCP/IP的一个设置项目事先设置好了，不需要再查询了，例windows中：

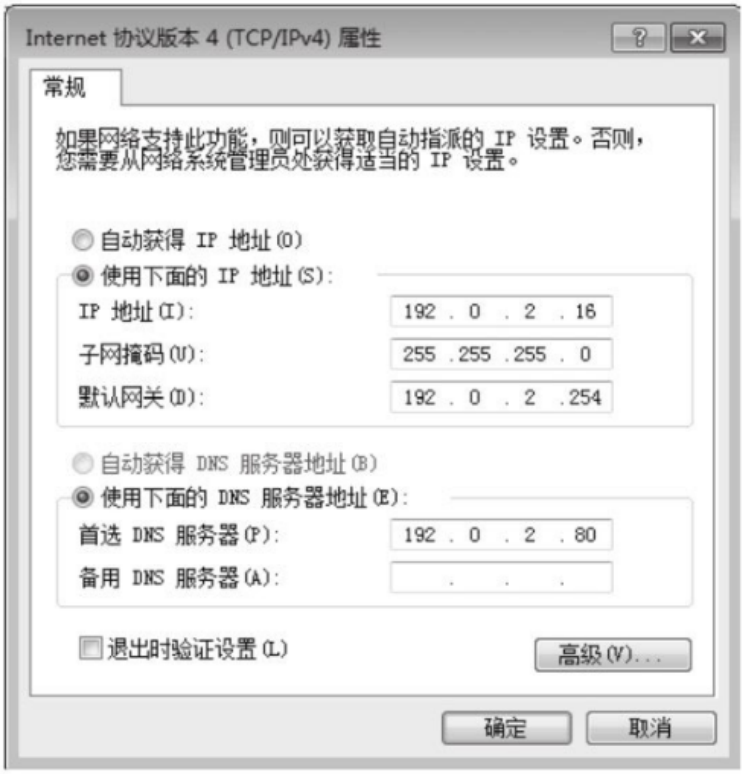


图1.13 DNS服务器地址的设置

2 DNS服务器保存的信息

来自客户端的信息中包含三种信息：

1. 域名
2. Class，识别网络的信息，现在只有互联网，故值永远为IN
3. 记录类型，表示域名对应何种类型的记录，IP地址or邮件服务器等。

DNS服务器保存有这三种信息对应的IPor邮件服务器等

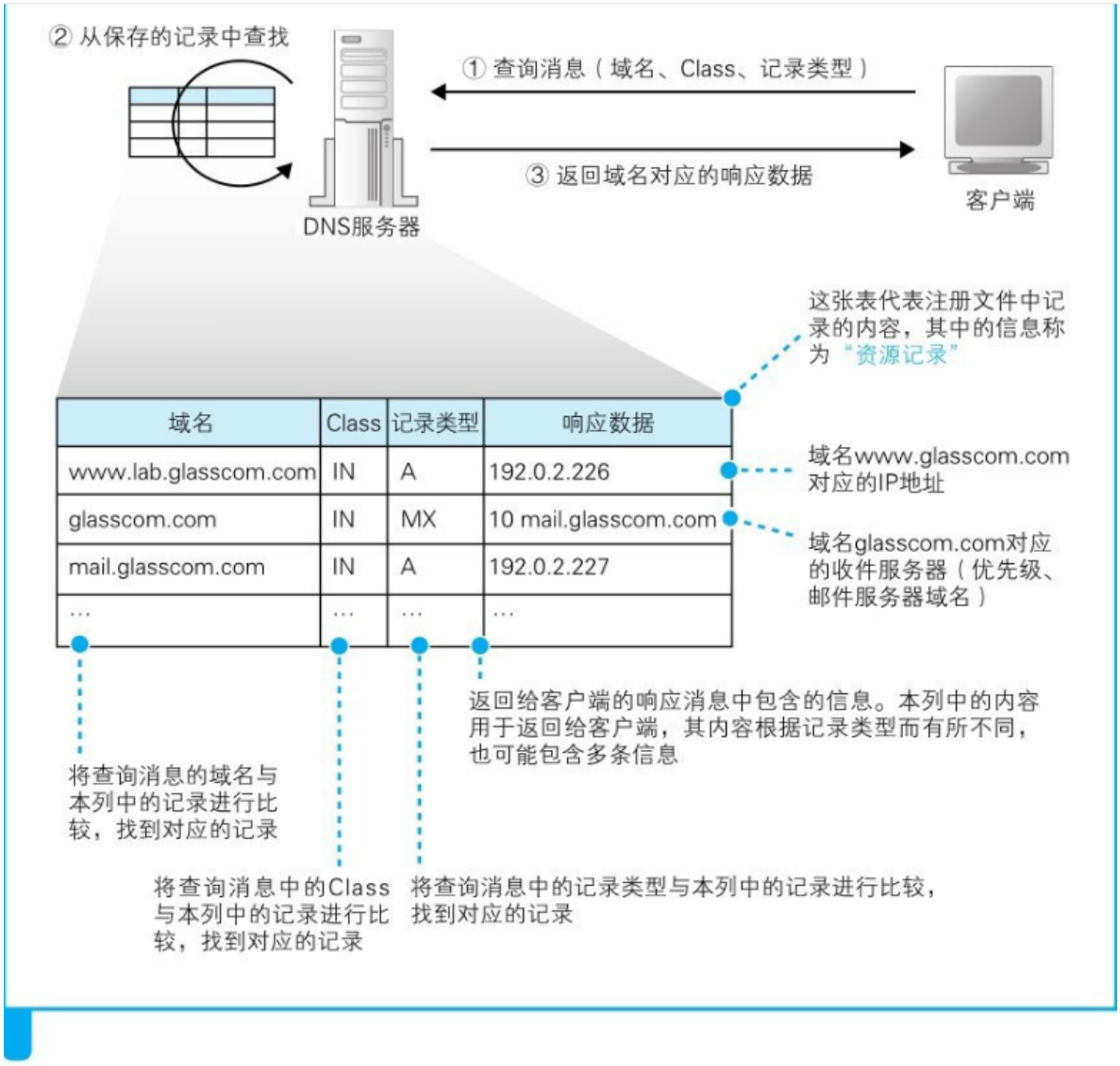


图1.14 DNS服务器的基本工作

域名层次结构，域名中越靠右的位置表示其层级越高。

于是更细一点的客户端向DNS服务器请求IP地址是这样的：

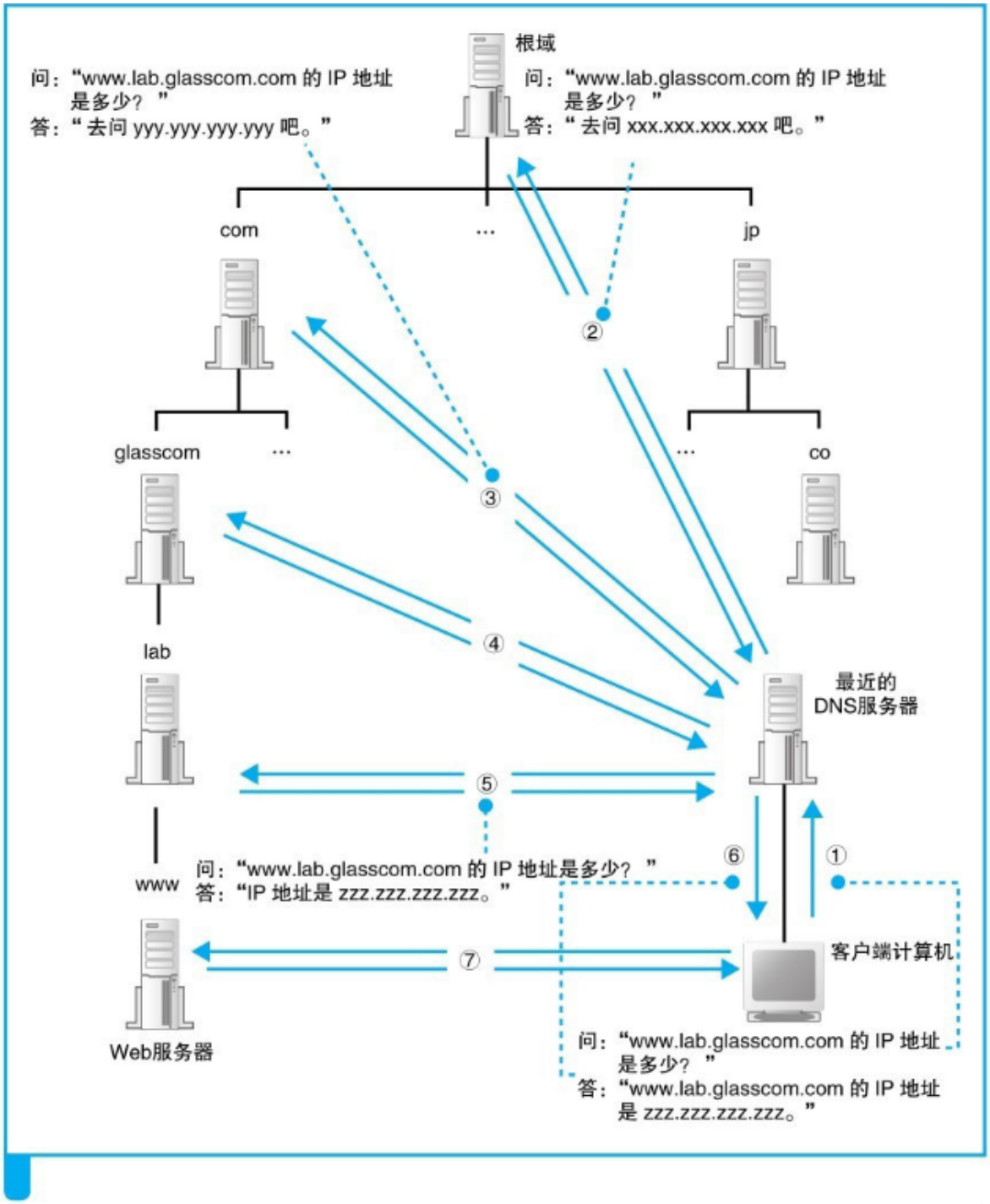


图1.16 DNS服务器之间的查询操作

真实网络中，一台DNS服务器可以同时管理好多个域，上下级的或同级的都有可能。

DNS服务器具有缓存功能（有时效），缓存域名与相关信息以及"不存在"的响应结果。

委托协议栈发消息：

（1）创建套接字（创建套接字阶段）

（2）将管道连接到服务器端的套接字上（连接阶段）

（3）收发数据（通信阶段），客户端向指定IP的指定端口发送HTTP请求消息，服务器响应消息。

（4）断开管道并删除套接字（断开阶段），通讯结束客户端或服务器先行断开，另一端也随之断开。

3 套接字

套接字中记录了是否收到响应，发送数据后经过了多长时间（判断超时即认定数据丢失）。

协议栈根据套接字中记录的控制信息来工作。

netstat是用于显示套接字内容的命令，-ano选项表示下面的意思。
a 不仅显示正在通信的套接字，还显示包括尚未开始通信等状态的所有套接字
n 显示IP地址和端口号
o 显示使用该套接字的程序PID

下图的每一行信息代表一个套接字。

如下图表示pid为5168的进程使用IP地址为127.0.0.1的49672端口与地址为。。。。的进行通信。

```
TCP    127.0.0.1:49672        127.0.0.1:49673        ESTABLISHED     5168
```

如下图，IP地址全0说明通信未开始，IP地址不确定。

```
TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1056
```

创建套接字时，首先分配一个套接字所需的内存空间，然后向其中写入初始状态。

接下来将这个套接字的描述符告知应用程序，描述符相当于区分协议栈中不同套接字的“门牌号”，然后应用程序向协议栈进行收发数据委托时提供该描述符即可，协议栈就知晓到底该和谁通信了。

TCP头部格式

表2.1 TCP头部格式

字段名称		长度（比特）	含　义
TCP头部（20字节～）	发送方端口号	16	发送网络包的程序的端口号
	接收方端口号	16	网络包的接收方程序的端口号
	序号（发送数据的顺序编号）	32	发送方告知接收方该网络包发送的数据相当于所有发送数据的第几个字节
	ACK 号（接收数据的顺序编号）	32	接收方告知发送方接收方已经收到了所有数据的第几个字节。其中，ACK 是 acknowledge 的缩写
	数据偏移量	4	表示数据部分的起始位置，也可以认为表示头部的长度
	保留	6	该字段为保留，现在未使用
	控制位	6	该字段中的每个比特分别表示以下通信控制含义。 URG：表示紧急指针字段有效 ACK：表示接收数据序号字段有效，一般表示数据已被接收方收到 PSH：表示通过 flush 操作发送的数据 RST：强制断开连接，用于异常中断的情况 SYN：发送方和接收方相互确认序号，表示连接操作 FIN：表示断开连接
	窗口	16	接收方告知发送方窗口大小（即无需等待确认可一起发送的数据量）
	校验和	16	用来检查是否出现错误
	紧急指针	16	表示应紧急处理的数据位置
	可选字段	可变长度	除了上面的固定头部字段之外，还可以添加可选字段，但除了连接操作之外，很少使用可选字段

4 收发数据

将应用程序要发送的数据存放在内部的发送缓冲区中，并等待该程序的下一段数据。

设置两个标记，一个是网络包可以容纳的最大数据长度（MTU网络包最大长度与MSS去掉头部之后可以容纳的TCP数据的最大长度），另一个是时间。

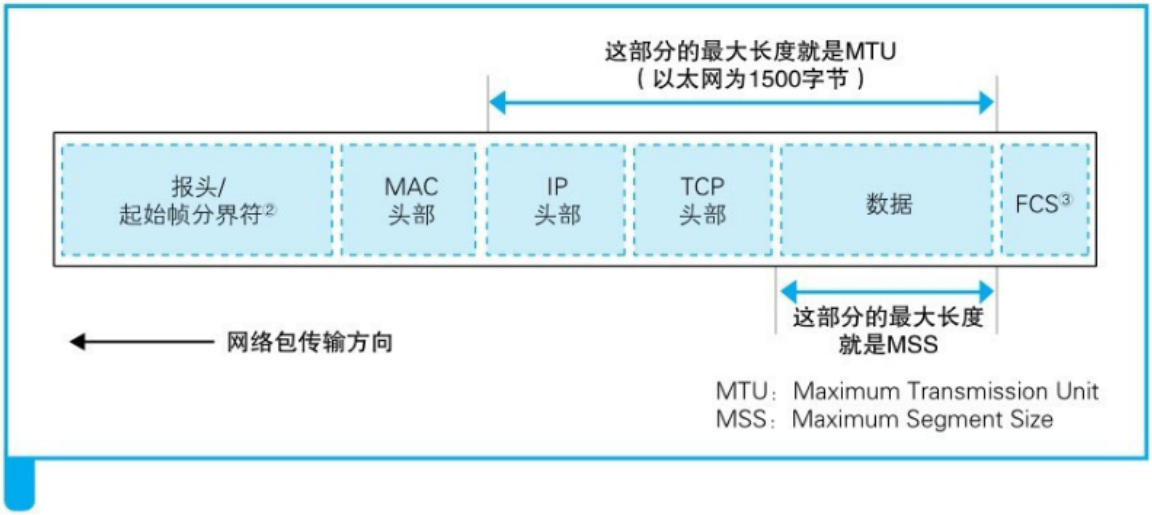

这部分的最大长度就是MTU
（以太网为1500字节）
报头/
起始帧分界符②
MAC
头部
IP
头部
TCP
头部
数据
FCS③
这部分的最大长度
就是MSS
网络包传输方向
MTU：Maximum Transmission Unit
MSS：Maximum Segment Size

图2.5 MTU与MSS