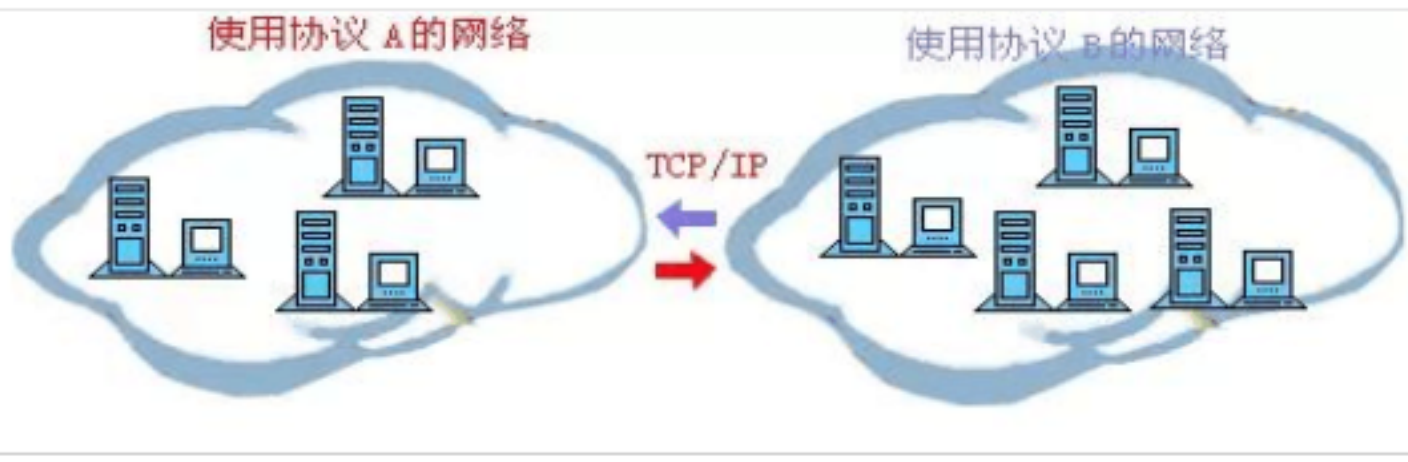
计算机网络基础知识总结

计算机网络学习的核心内容就是网络协议的学习。 网络协议是为计算机网络中进行数据交换而建立的规则、 标准或者说是约定的集合。 因为不同用户的数据终端可能采取的字符集是不同的， 两者需要进行通信， 必须要在一定的标准上进行。一个很形象地比喻就是我们的语言， 我们大天朝地广人多， 地方性语言也非常丰富，而且方言之间差距巨大。 A地区的方言可能 B地区的人根本无法接受，所以我们要为全国人名进行沟通建立一个语言标准，这就是我们的普通话的作用。同样，放眼全球，我们与外国友人沟通的标准语言是英语，所以我们才要苦逼的学习英语。

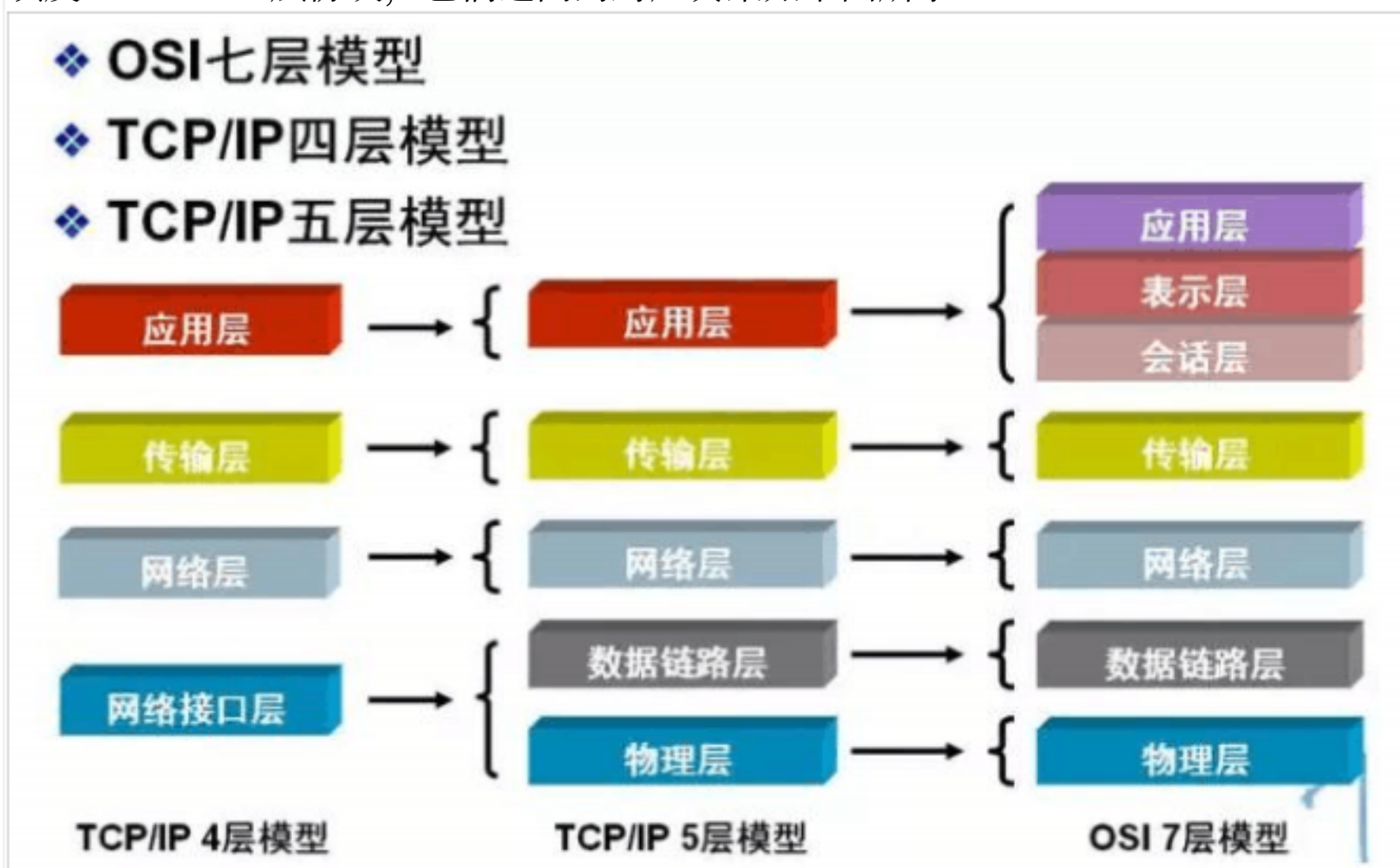
计算机网络协议同我们的语言一样，多种多样。而 ARPA公司与 1977 年到 1979 年推出了一种名为 ARPANET的网络协议受到了广泛的热捧，其中最主要的原因就是它推出了人尽皆知的 TCP/IP 标准网络协议。目前 TCP/IP 协议已经成为 Internet 中的“ 通用语言 ”，下图为不同计算机群之间利用 TCP/IP 进行通信的示意图。



1. 网络层次划分

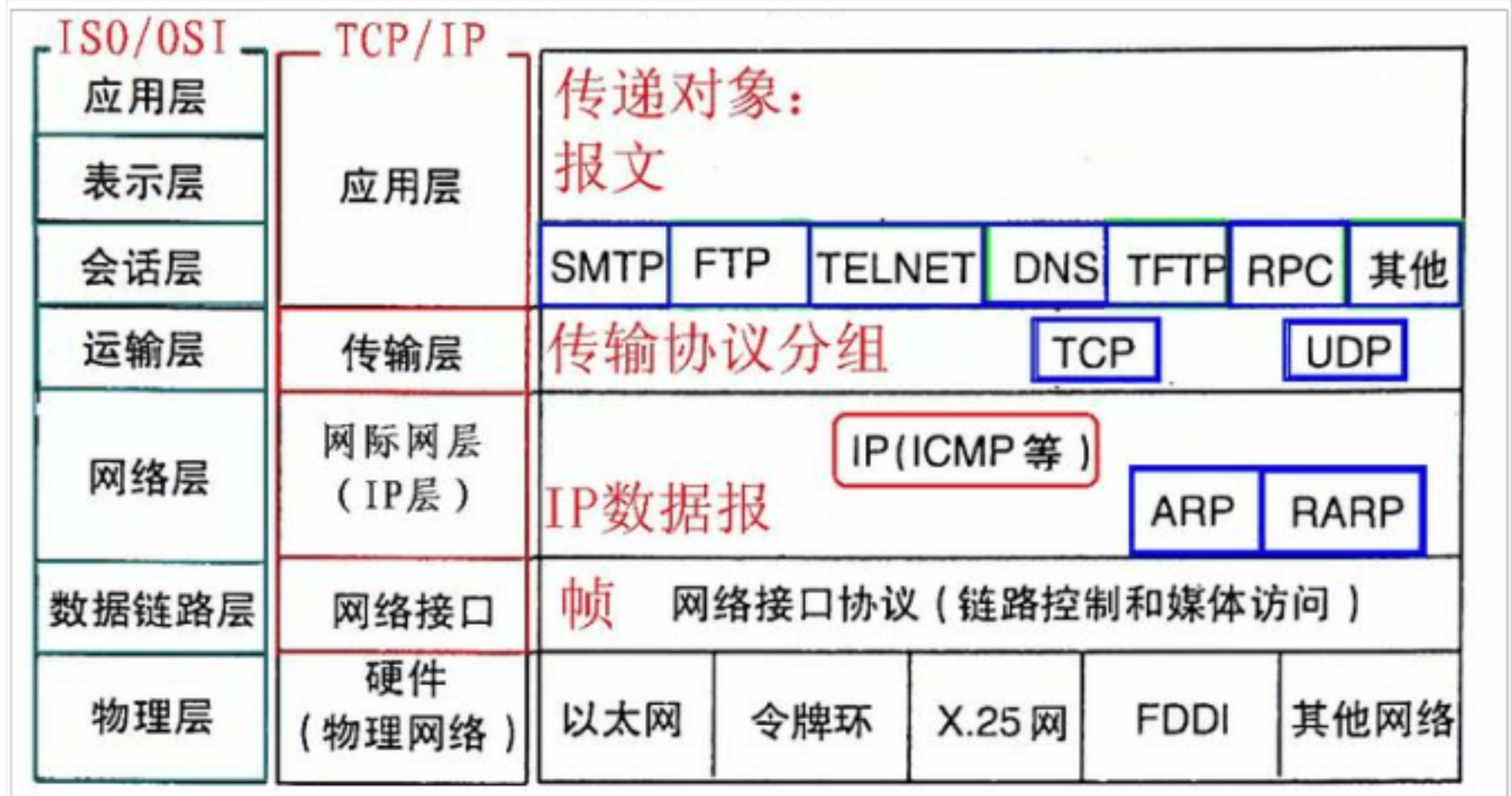
为了使不同计算机厂家生产的计算机能够相互通信，以便在更大的范围内建立计算机网络，国际标准化组织（ISO）在 1978 年提出了“开放系统互联参考模型”，即著名的 OSI/RM模型（OpenSystem Interconnection/Reference Model）。它将计算机网络体系结构的通信协议划分为七层，自下而上依次为：物理层（Physics Layer）、数据链路层（Data Link Layer）、网络层（Network Layer）、传输层（Transport Layer）、会话层（Session Layer）、表示层（Presentation Layer）、应用层（Application Layer）。其中第四层完成数据传送服务，上面三层面向用户。

除了标准的 OSI 七层模型以外，常见的网络层次划分还有 TCP/IP 四层协议以及 TCP/IP 五层协议，它们之间的对应关系如下图所示：



2. OSI 七层网络模型

TCP/IP 协议毫无疑问是互联网的基础协议，没有它就根本不可能上网，任何和互联网有关的操作都离不开 TCP/IP 协议。不管是 OSI 七层模型还是 TCP/IP 的四层、五层模型，每一层中都要自己的专属协议，完成自己相应的工作以及与上下层级之间进行沟通。由于 OSI 七层模型为网络的标准层次划分，所以我们以 OSI 七层模型为例从下向上进行一一介绍。



1）物理层（ Physical Layer ）

激活、维持、关闭通信端点之间的机械特性、电气特性、功能特性以及过程特性。 该层为上层协议提供了一个传输数据的可靠的物理媒体。简单的说，物理层确保原始的数据可在各种物理媒体上传输。 物理层记住两个重要的设备名称，中继器（ Repeater，也叫放大器）和集线器。

2）数据链路层（ Data Link Layer ）

数据链路层在物理层提供的服务的基础上向网络层提供服务， 其最基本的服务是将源自网络层来的数据可靠地传输到相邻节点的目标机网络层。 为达到这一目的，数据链路必须具备一系列相应的功能， 主要有：如何将数据组合成数据块，在数据链路层中称这种数据块为帧（ frame），帧是数据链路层的传送单位；如何控制帧在物理信道上的传输， 包括如何处理传输差错， 如何调节发送速率以使与接收方相匹配； 以及在两个网络实体之间提供数据链路通路的建立、 维持和释放的管理。数据链路层在不可靠的物理介质上提供可靠的传输。 该层的作用包括：物理地址寻址、数据的成帧、流量控制、数据的检错、重发等。

有关数据链路层的重要知识点：

1> 数据链路层为网络层提供可靠的数据传输；

2> 基本数据单位为帧；

3> 主要的协议：以太网协议；

4> 两个重要设备名称：网桥和交换机。

3）网络层（ Network Layer ）

网络层的目的是实现两个端系统之间的数据透明传送，具体功能包括寻址和路由选择、连接的建立、保持和终止等。它提供的服务使传输层不需要了解网络中的数据传输和交换技术。如果您想用尽量少的词来记住网络层，那就是“路径选择、路由及逻辑寻址”。

网络层中涉及众多的协议，其中包括最重要的协议，也是 TCP/IP 的核心协议——IP 协议。IP 协议非常简单，仅仅提供不可靠、无连接的传送服务。IP 协议的主要功能有：无连接数据报传输、数据报路由选择和差错控制。与 IP 协议配套使用实现其功能的还有地址解析协议 ARP、逆地址解析协议 RARP、因特网报文协议 ICMP、因特网组管理协议 IGMP。具体的协议我们会在接下来的部分进行总结，有关网络层的重点为：

1> 网络层负责对子网间的数据包进行路由选择。此外，网络层还可以实现拥塞控制、网际互连等功能；

2> 基本数据单位为 IP 数据报；

3> 包含的主要协议：

IP 协议（Internet Protocol，因特网互联协议）；

ICMP协议（Internet Control MessageProtocol，因特网控制报文协议）；

ARP协议（Address Resolution Protocol，地址解析协议）；

RARP协议（Reverse Address Resolution Protocol，逆地址解析协议）。

4> 重要的设备：路由器。

4）传输层（Transport Layer）

第一个端到端，即主机到主机的层次。传输层负责将上层数据分段并提供端到端的、可靠的或不可靠的传输。此外，传输层还要处理端到端的差错控制和流量控制问题。

传输层的任务是根据通信子网的特性，最佳的利用网络资源，为两个端系统的会话层之间，提供建立、维护和取消传输连接的功能，负责端到端的可靠数据传输。在这一层，信息传送的协议数据单元称为段或报文。

网络层只是根据网络地址将源结点发出的数据包传送到目的结点，而传输层则负责将数据可靠地传送到相应的端口。

有关网络层的重点：

1> 传输层负责将上层数据分段并提供端到端的、可靠的或不可靠的传输以及端到端的差错控制和流量控制问题；

2> 包含的主要协议：TCP协议（Transmission Control Protocol，传输控制协议）、UDP协议（User Datagram Protocol，用户数据报协议）；

3> 重要设备：网关。

5）会话层

会话层管理主机之间的会话进程，即负责建立、管理、终止进程之间的会话。会话层还利用在数据中插入校验点来实现数据的同步。

6）表示层

表示层对上层数据或信息进行变换以保证一个主机应用层信息可以被另一个主机的应用程序理解。表示层的数据转换包括数据的加密、压缩、格式转换等。

7）应用层

为操作系统或网络应用程序提供访问网络服务的接口。

会话层、表示层和应用层重点：

1> 数据传输基本单位为报文；

2> 包含的主要协议：FTP（文件传送协议）、Telnet（远程登录协议）、DNS(域名解析协议）、SMTP(邮件传送协议），POP3协议（邮局协议），HTTP协议（Hyper Text Transfer Protocol）。

3. IP 地址

1）网络地址

IP 地址由网络号（包括子网号）和主机号组成，网络地址的主机号为全 0，网络地址代表着整个网络。

2）广播地址

广播地址通常称为直接广播地址，是为了区分受限广播地址。

广播地址与网络地址的主机号正好相反，广播地址中，主机号为全 1。当向某个网络的广播地址发送消息时，该网络内的所有主机都能收到该广播消息。

3）组播地址

D类地址就是组播地址。

先回忆下 A，B，C，D类地址吧：

A类地址以 00开头，第一个字节作为网络号，地址范围为：0.0.0.0~127.255.255.255 ；

B类地址以 10开头，前两个字节作为网络号，地址范围是：128.0.0.0~191.255.255.255;

C类地址以 110开头，前三个字节作为网络号，地址范围是：192.0.0.0~223.255.255.255 。

D类地址以 1110开头，地址范围是 224.0.0.0~239.255.255.255 ，D类地址作为组播地址（一对多的通信）；

E类地址以 1111开头，地址范围是 240.0.0.0~255.255.255.255 ，E类地址为保留地址，供以后使用。

注：只有 A,B,C 有网络号和主机号之分， D类地址和 E类地址没有划分网络号和主机号。

4）255.255.255.255

该 IP 地址指的是受限的广播地址。受限广播地址与一般广播地址（直接广播地址）的区别在于， 受限广播地址只能用于本地网络， 路由器不会转发以受限广播地址为目的地址的分组；一般广播地址既可在本地广播，也可跨网段广播。例如：主机 192.168.1.1/30 上的直接广播数据包后，另外一个网段 192.168.1.5/30 也能收到该数据报；若发送受限广播数据报，则不能收到。

注：一般的广播地址（直接广播地址）能够通过某些路由器（当然不是所有的路由器），而受限的广播地址不能通过路由器。

5）0.0.0.0

常用于寻找自己的 IP 地址，例如在我们的 RARP, BOOTP和 DHCP协议中， 若某个未知 IP 地址的无盘机想要知道自己的 IP 地址，它就以 255.255.255.255 为目的地址， 向本地范围 （具体而言是被各个路由器屏蔽的范围内） 的服务器发送 IP 请求分组。

6）回环地址

127.0.0.0/8 被用作回环地址，回环地址表示本机的地址，常用于对本机的测试，用的最多的是 127.0.0.1 。

7）A、B、C类私有地址

私有地址 (private address)　也叫专用地址，它们不会在全球使用，只具有本地意义。

A类私有地址： 10.0.0.0/8 ，范围是： 10.0.0.0~10.255.255.255

B类私有地址： 172.16.0.0/12 ，范围是： 172.16.0.0~172.31.255.255

C类私有地址： 192.168.0.0/16 ，范围是： 192.168.0.0~192.168.255.255

4. 子网掩码及网络划分

随着互连网应用的不断扩大，原先的 IPv4 的弊端也逐渐暴露出来，即网络号占位太多， 而主机号位太少， 所以其能提供的主机地址也越来越稀缺， 目前除了使用 NAT在企业内部利用保留地址自行分配以外，通常都对一个高类别的 IP 地址进行再划分，以形成多个子网，提供给不同规模的用户群使用。

这里主要是为了在网络分段情况下有效地利用 IP 地址，通过对主机号的高位部分取作为子网号， 从通常的网络位界限中扩展或压缩子网掩码， 用来创建某类地址的更多子网。 但创建更多的子网时， 在每个子网上的可用主机地址数目会比原先减少。

什么是子网掩码？

子网掩码是标志两个 IP 地址是否同属于一个子网的， 也是 32位二进制地址，其每一个为 1 代表该位是网络位，为 0 代表主机位。它和 IP 地址一样也是使用点式十进制来表示的。如果两个 IP 地址在子网掩码的按位与的计算下所得结果相同，即表明它们共属于同一子网中。

在计算子网掩码时，我们要注意 IP 地址中的保留地址，即“ 0 ”地址和广播地址，它们是指主机地址或网络地址全为“ 0 ”或“ 1 ”时的 IP 地址，它们代表着本网络地址和广播地址，一般是不能被计算在内的。

子网掩码的计算：

对于无须再划分成子网的 IP 地址来说，其子网掩码非常简单，即按照其定义即可写出： 如某 B类 IP 地址为 10.12.3.0 ，无须再分割子网， 则该 IP 地址的子网掩码 255.255.0.0 。如果它是一个 C类地址，则其子网掩码为 255.255.255.0 。其它类推，不再详述。下面我们关键要介绍的是一个 IP 地址，还需要将其高位主机位再作为划分出的子网网络号，剩下的是每个子网的主机号，这时该如何进行每个子网的掩码计算。

下面总结一下有关子网掩码和网络划分常见的面试考题：

1）利用子网数来计算

在求子网掩码之前必须先搞清楚要划分的子网数目，　以及每个子网内的所需主机数目。

(1)　将子网数目转化为二进制来表示　；

如欲将 B 类 IP 地址 168.195.0.0　划分成 27 个子网： 27=11011；

(2)　取得该二进制的位数，为　N；

该二进制为五位数，　N = 5

(3)　取得该 IP 地址的类子网掩码，将其主机地址部分的的前　　N 位置 1 即得出该 IP 地址划分子网的子网掩码。

将 B 类地址的子网掩码　255.255.0.0　的主机地址前　5 位置 1，得到 255.255.248.0

2）利用主机数来计算

如欲将 B 类 IP 地址 168.195.0.0　划分成若干子网，每个子网内有主机　700 台：

(1)　将主机数目转化为二进制来表示；

700=1010111100;

(2)　如果主机数小于或等于　254（注意去掉保留的两个　IP 地址），则取得该主机的二进制位数，为　N，这里肯定 N<8。如果大于 254，则 N>8，这就是说主机地址将占据不止　8 位；

该二进制为十位数，　N=10;

(3)　使用 255.255.255.255　来将该类 IP 地址的主机地址位数全部置　1，然后从后向前的将　N 位全部置为 0，即为子网掩码值。

将该 B 类地址的子网掩码　255.255.0.0　的主机地址全部置　1，得到 255.255.255.255 ，然后再从后向前将后　10 位置 0, 即为：

11111111.11111111.11111100.00000000，即 255.255.252.0 。这就是该欲划分成主机为 700 台的 B 类 IP 地址 168.195.0.0　的子网掩码。

3）还有一种题型，要你根据每个网络的主机数量进行子网地址的规划和计算子网掩码。这也可按上述原则进行计算。

比如一个子网有　10 台主机，那么对于这个子网需要的　IP 地址是：

10＋1＋1＋1＝13

注意：加的第一个 1 是指这个网络连接时所需的网关地址，接着的两个 1 分别是指网络地址和广播地址。

因为 13 小于 16（16 等于 2 的 4 次方），所以主机位为 4 位。而 256－16＝240，所以该子网掩码为 255.255.255.240 。

如果一个子网有 14 台主机，不少人常犯的错误是： 依然分配具有 16 个地址空间的子网， 而忘记了给网关分配地址。 这样就错误了， 因为 14＋1＋1＋1＝17，17 大于 16，所以我们只能分配具有 32 个地址（32 等于 2 的 5 次方）空间的子网。这时子网掩码为： 255.255.255.224 。

5. ARP/RARP协议

地址解析协议，即 ARP（Address Resolution Protocol），是根据 IP 地址获取物理地址的一个 TCP/IP 协议。主机发送信息时将包含目标 IP 地址的 ARP 请求广播到网络上的所有主机， 并接收返回消息， 以此确定目标的物理地址； 收到返回消息后将该 IP 地址和物理地址存入本机 ARP缓存中并保留一定时间，下次请求时直接查询 ARP缓存以节约资源。地址解析协议是建立在网络中各个主机互相信任的基础上的， 网络上的主机可以自主发送 ARP应答消息， 其他主机收到应答报文时不会检测该报文的真实性就会将其记入本机 ARP缓存；由此攻击者就可以向某一主机发送伪 ARP应答报文，使其发送的信息无法到达预期的主机或到达错误的主机，这就构成了一个 ARP欺骗。ARP命令可用于查询本机 ARP缓存中 IP 地址和 MAC地址的对应关系、添加或删除静态对应关系等。

ARP工作流程举例：

主机 A 的 IP 地址为 192.168.1.1 ， MAC地址为 0A-11-22-33-44-01 ；

主机 B 的 IP 地址为 192.168.1.2 ， MAC地址为 0A-11-22-33-44-02 ；

当主机 A 要与主机 B 通信时，地址解析协议可以将主机 B 的 IP 地址（192.168.1.2 ）解析成主机 B 的 MAC地址，以下为工作流程：

（1）根据主机 A 上的路由表内容， IP 确定用于访问主机 B 的转发 IP 地址是 192.168.1.2 。然后 A 主机在自己的本地 ARP缓存中检查主机 B 的匹配 MAC地址。

（2）如果主机 A 在 ARP缓存中没有找到映射，它将询问 192.168.1.2 的硬件地址，从而将 ARP请求帧广播到本地网络上的所有主机。源主机 A 的 IP 地址和 MAC地址都包括在 ARP请求中。本地网络上的每台主机都接收到 ARP请求并且检查是否与自己的 IP 地址匹配。如果主机发现请求的 IP 地址与自己的 IP 地址不匹配，它将丢弃 ARP请求。

（3）主机 B 确定 ARP请求中的 IP 地址与自己的 IP 地址匹配，则将主机 A 的 IP 地址和 MAC地址映射添加到本地 ARP缓存中。

（4）主机 B 将包含其 MAC 地址的 ARP 回复消息直接发送回主机 A。

（5）当主机 A 收到从主机 B 发来的 ARP 回复消息时，会用主机 B 的 IP 和 MAC 地址映射更新 ARP 缓存。本机缓存是有生存期的，生存期结束后，将再次重复上面的过程。主机 B 的 MAC 地址一旦确定，主机 A 就能向主机 B 发送 IP 通信了。

逆地址解析协议，即 RARP，功能和 ARP 协议相对，其将局域网中某个主机的物理地址转换为 IP 地址，比如局域网中有一台主机只知道物理地址而不知道 IP 地址，那么可以通过 RARP 协议发出征求自身 IP 地址的广播请求，然后由 RARP 服务器负责回答。

RARP 协议工作流程：

（1）给主机发送一个本地的 RARP 广播，在此广播包中，声明自己的 MAC 地址并且请求任何收到此请求的 RARP 服务器分配一个 IP 地址；

（2）本地网段上的 RARP 服务器收到此请求后，检查其 RARP 列表，查找该 MAC 地址对应的 IP 地址；

（3）如果存在，RARP 服务器就给源主机发送一个响应数据包并将此 IP 地址提供给对方主机使用；

（4）如果不存在，RARP 服务器对此不做任何的响应；

（5）源主机收到从 RARP 服务器的响应信息，就利用得到的 IP 地址进行通讯；如果一直没有收到 RARP 服务器的响应信息，表示初始化失败。

6. 路由选择协议

常见的路由选择协议有：RIP 协议、OSPF 协议。

RIP 协议：底层是贝尔曼福特算法，它选择路由的度量标准（metric）是跳数，最大跳数是 15 跳，如果大于 15 跳，它就会丢弃数据包。

OSPF 协议：Open Shortest Path First 开放式最短路径优先，底层是迪杰斯特拉算法，是链路状态路由选择协议，它选择路由的度量标准是带宽，延迟。

7. TCP/IP 协议

TCP/IP 协议是 Internet 最基本的协议、Internet 国际互联网络的基础，由网络层的 IP 协议和传输层的 TCP 协议组成。通俗而言：TCP 负责发现传输的问题，一有问题就发出信号，要求重新传输，直到所有数据安全正确地传输到目的地。而 IP 是给因特网的每一台联网设备规定一个地址。

IP 层接收由更低层（网络接口层例如以太网设备驱动程序）发来的数据包，并把该数据包发送到更高层---TCP 或 UDP 层；相反，IP 层也把从 TCP 或 UDP 层接收来的数据包传送到更低层。IP 数据包是不可靠的，因为 IP 并没有做任何事

情来确认数据包是否按顺序发送的或者有没有被破坏，　　IP 数据包中含有发送它的主机的地址（源地址）和接收它的主机的地址（目的地址）。

TCP是面向连接的通信协议，通过三次握手建立连接，通讯完成时要拆除连接，由于 TCP是面向连接的所以只能用于端到端的通讯。　　TCP提供的是一种可靠的数据流服务，采用“ 带重传的肯定确认 ”技术来实现传输的可靠性。　　TCP还采用一种称为“ 滑动窗口 ”的方式进行流量控制，所谓窗口实际表示接收能力，用以限制发送方的发送速度。

TCP报文首部格式：

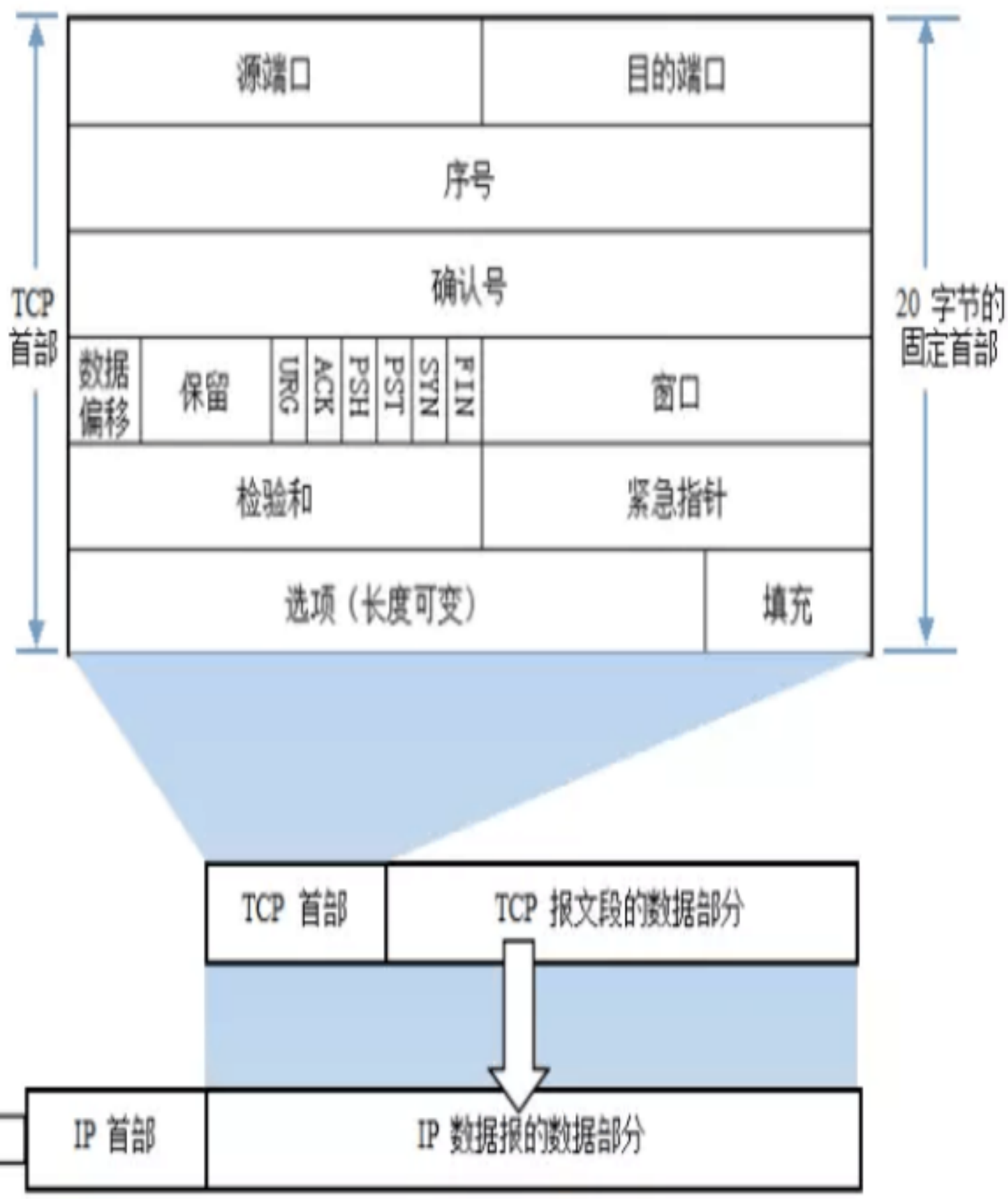
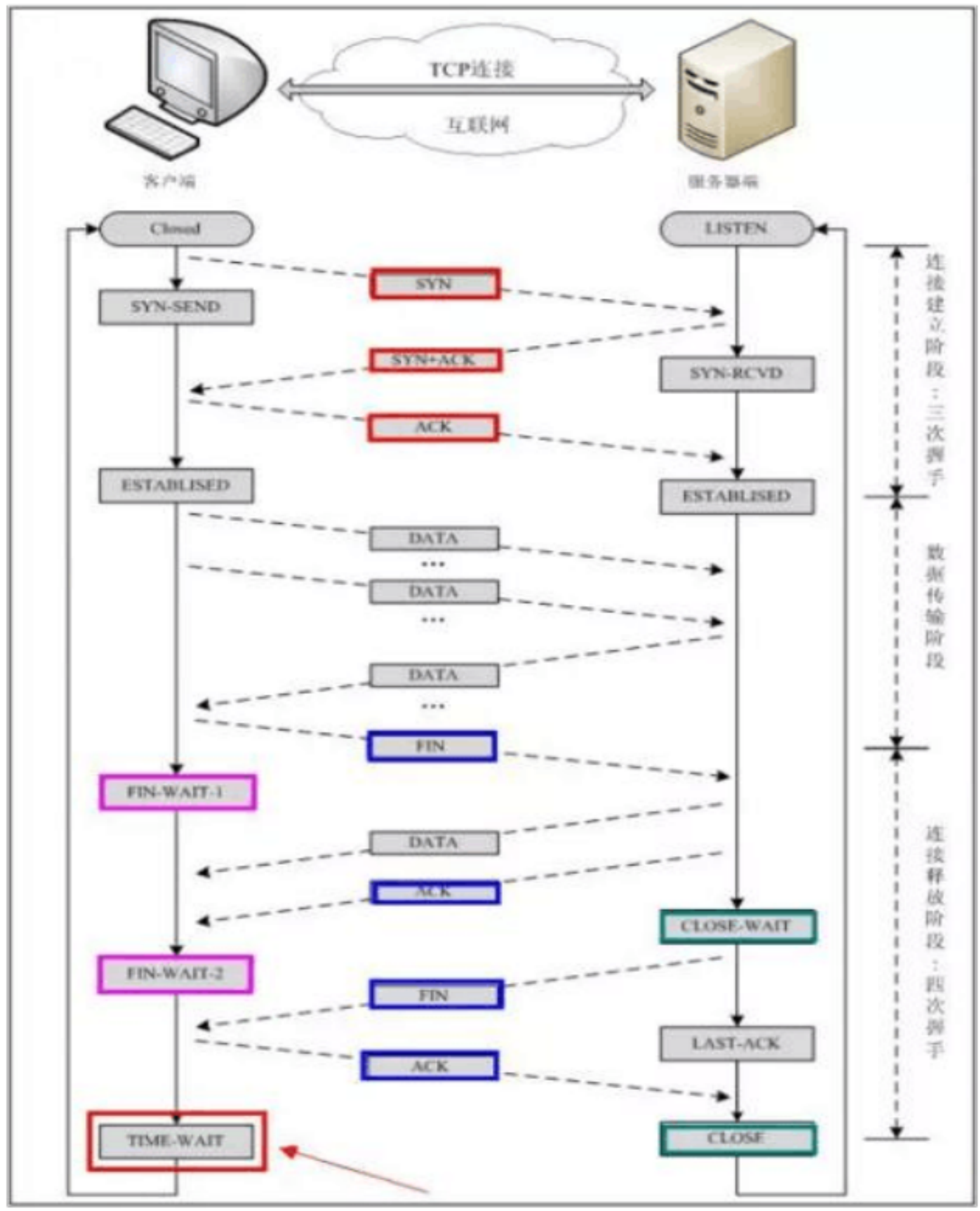


图 TCP 报文段的首部格式

TCP协议的三次握手和四次挥手：



注：seq:"sequance" 序列号；ack:"acknowledge" 确认号；SYN"synchronize" 请求同步标志； ；ACK"acknowledge" 确认标志 "；FIN："Finally" 结束标志。

TCP连接建立过程： 首先 Client 端发送连接请求报文， Server 段接受连接后回复 ACK报文，并为这次连接分配资源。 Client 端接收到 ACK报文后也向 Server 段发生 ACK报文，并分配资源，这样 TCP连接就建立了。

TCP连接断开过程： 假设 Client 端发起中断连接请求，也就是发送 FIN 报文。 Server 端接到 FIN 报文后，意思是说 "我 Client 端没有数据要发给你了 "，但是如果你还有数据没有发送完成，则不必急着关闭 Socket，可以继续发送数

据。所以你先发送 ACK，"告诉 Client 端，你的请求我收到了，但是我还没准备好，请继续你等我的消息 "。这个时候 Client 端就进入 FIN_WAIT状态，继续等待 Server 端的 FIN 报文。当 Server 端确定数据已发送完成，则向 Client 端发送 FIN 报文，"告诉 Client 端，好了，我这边数据发完了，准备好关闭连接了 "。Client 端收到 FIN 报文后，"就知道可以关闭连接了，但是他还是不相信网络，怕 Server 端不知道要关闭，所以发送 ACK后进入 TIME_WAIT状态，如果 Server 端没有收到 ACK则可以重传。“， Server 端收到 ACK后，"就知道可以断开连接了"。Client 端等待了 2MSL后依然没有收到回复， 则证明 Server 端已正常关闭，那好，我 Client 端也可以关闭连接了。 Ok，TCP连接就这样关闭了！

为什么要三次挥手？

在只有两次“ 握手 ”的情形下，假设 Client 想跟 Server 建立连接，但是却因为中途连接请求的数据报丢失了，故 Client 端不得不重新发送一遍；这个时候 Server 端仅收到一个连接请求，因此可以正常的建立连接。但是，有时候 Client 端重新发送请求不是因为数据报丢失了，而是有可能数据传输过程因为网络并发量很大在某结点被阻塞了， 这种情形下 Server 端将先后收到 2 次请求，并持续等待两个 Client 请求向他发送数据 ... 问题就在这里， Cient 端实际上只有一次请求， 而 Server 端却有 2 个响应，极端的情况可能由于 Client 端多次重新发送请求数据而导致 Server 端最后建立了 N多个响应在等待，因而造成极大的资源浪费！所以，“ 三次握手 ”很有必要！

为什么要四次挥手？

试想一下，假如现在你是客户端你想断开跟 Server 的所有连接该怎么做？第一步，你自己先停止向 Server 端发送数据， 并等待 Server 的回复。 但事情还没有完，虽然你自身不往 Server 发送数据了，但是因为你们之前已经建立好平等的连接了，所以此时他也有主动权向你发送数据；故 Server 端还得终止主动向你发送数据， 并等待你的确认。 其实，说白了就是保证双方的一个合约的完整执行！

使用 TCP的协议： FTP（文件传输协议）、 Telnet （远程登录协议）、 SMTP（简单邮件传输协议）、 POP3(和 SMTP相对，用于接收邮件）、 HTTP协议等。

8. UDP 协议

UDP用户数据报协议，是面向无连接的通讯协议， UDP数据包括目的端口号和源端口号信息，由于通讯不需要连接，所以可以实现广播发送。 UDP通讯时不需要接收方确认，属于不可靠的传输，可能会出现丢包现象，实际应用中要求程序员编程验证。

UDP与 TCP位于同一层，但它不管数据包的顺序、错误或重发。因此， UDP不被应用于那些使用虚电路的面向连接的服务， UDP主要用于那些面向查询 --- 应答的服务，例如 NFS。相对于 FTP或 Telnet ，这些服务需要交换的信息量较小。

每个 UDP报文分 UDP报头和 UDP数据区两部分。报头由四个 16 位长（ 2 字节）字段组成，分别说明该报文的源端口、 目的端口、 报文长度以及校验值。 UDP报头由 4 个域组成，其中每个域各占用 2 个字节，具体如下：

（1）源端口号；

（2）目标端口号；

（3）数据报长度；

（4）校验值。

使用 UDP协议包括：TFTP(简单文件传输协议） 、SNMP(简单网络管理协议） 、DNS(域名解析协议）、 NFS、 BOOTP。

TCP 与 UDP 的区别： TCP是面向连接的，可靠的字节流服务； UDP是面向无连接的，不可靠的数据报服务。

9. DNS 协议

DNS是域名系统 (DomainNameSystem)的缩写， 该系统用于命名组织到域层次结构中的计算机和网络服务， 可以简单地理解为将 URL转换为 IP 地址。域名是由圆点分开一串单词或缩写组成的，每一个域名都对应一个惟一的 IP 地址，在 Internet 上域名与 IP 地址之间是一一对应的， DNS就是进行域名解析的服务器。DNS命名用于 Internet 等 TCP/IP 网络中， 通过用户友好的名称查找计算机和服务。

10. NAT 协议

NAT网络地址转换 (Network Address Translation) 属接入广域网 (WAN)技术，是一种将私有（保留）地址转化为合法 IP 地址的转换技术，它被广泛应用于各种类型 Internet 接入方式和各种类型的网络中。原因很简单， NAT不仅完美地解决了 IP 地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。

11. DHCP 协议

DHCP动态主机设置协议（ Dynamic Host Configuration Protocol ）是一个局域网的网络协议， 使用 UDP协议工作， 主要有两个用途： 给内部网络或网络服务供应商自动分配 IP 地址，给用户或者内部网络管理员作为对所有计算机作中央管理的手段。

12. HTTP 协议

超文本传输协议（HTTP，HyperText Transfer Protocol）是互联网上应用最为广泛的一种网络协议。所有的 WWW 文件都必须遵守这个标准。

HTTP 协议包括哪些请求？

GET：请求读取由 URL所标志的信息。

POST：给服务器添加信息（如注释）。

PUT：在给定的 URL下存储一个文档。

DELETE：删除给定的 URL所标志的资源。

HTTP 中， POST 与 GET 的区别

1）Get 是从服务器上获取数据， Post 是向服务器传送数据。

2）Get 是把参数数据队列加到提交表单的 Action 属性所指向的 URL中，值和表单内各个字段一一对应，在 URL中可以看到。

3）Get 传送的数据量小，不能大于 2KB；Post 传送的数据量较大，一般被默认为不受限制。

4）根据 HTTP规范， GET用于信息获取，而且应该是安全的和幂等的。

I. 所谓 安全的 意味着该操作用于获取信息而非修改信息。换句话说，GET请求一般不应产生副作用。就是说，它仅仅是获取资源信息，就像数据库查询一样，不会修改，增加数据，不会影响资源的状态。

II. 幂等 的意味着对同一 URL的多个请求应该返回同样的结果。

13. 一个举例

在浏览器中输入 www.baidu.com 后执行的全部过程

现在假设如果我们在客户端 （客户端）浏览器中输入 http://www.baidu.com，而 baidu.com 为要访问的服务器 （服务器），下面详细分析客户端为了访问服务器而执行的一系列关于协议的操作：

1）客户端浏览器通过 DNS解析到 www.baidu.com的 IP 地址 220.181.27.48 ，通过这个 IP 地址找到客户端到服务器的路径。 客户端浏览器发起一个 HTTP会话到 220.161.27.48 ，然后通过 TCP进行封装数据包，输入到网络层。

2）在客户端的传输层，把 HTTP会话请求分成报文段，添加源和目的端口，如服务器使用 80 端口监听客户端的请求，客户端由系统随机选择一个端口如

5000，与服务器进行交换，服务器把相应的请求返回给客户端的 5000 端口。然后使用 IP 层的 IP 地址查找目的端。

3）客户端的网络层不用关系应用层或者传输层的东西，主要做的是通过查找路由表确定如何到达服务器，期间可能经过多个路由器，这些都是由路由器来完成的工作，不作过多的描述，无非就是通过查找路由表决定通过那个路径到达服务器。

4）客户端的链路层，包通过链路层发送到路由器，通过邻居协议查找给定 IP 地址的 MAC 地址，然后发送 ARP 请求查找目的地址，如果得到回应后就可以使用 ARP 的请求应答交换的 IP 数据包现在就可以传输了，然后发送 IP 数据包到达服务器的地址。