第18章

计算机网络及分布式系统

网络面试例题主要包括局域网、广域网、IP 管理等诸方面。

18.1 网络结构

面试例题 1：在 OSI 参考模型中，物理层的作用是（1）。对等实体在一次交互作用中传送的信息单位称为（2），它包括（3）两部分。上下层实体之间的接口称为服务访问点（SAP），网络层的服务访问点也称为（4），通常分为（5）两部分。[中国某著名综合软件公司 2005 年面试题]

（1）A. 建立和释放连接　　B. 透明的传输比特流
　　C. 在物理实体间传送数据祯　　D. 发送和接收用户数据
（2）A. 接口数据单元　　B. 服务数据单元
　　C. 协议数据单元　　D. 交互数据单元
（3）A. 控制信息和用户数据　　B. 接口信息和用户数据
　　C. 接口信息和控制信息　　D. 控制信息和校验信息
（4）A. 用户地址　　B. 网络地址
　　C. 端口地址　　D. 网卡地址
（5）A. 网络号和端口号　　B. 网络号和主机地址
　　C. 超网号和子网号　　D. 超网号和端口地址

解析：网络问题。

OSI 参考模型有 7 层，其分层原则如下：

- 根据不同层次的抽象分层。
- 每层应当有一个定义明确的功能。
- 每层功能的选择应该有助于制定网络协议的国际标准。
- 各层边界的选择应尽量节省跨过接口的通信量。
- 层数应足够多，以避免不同的功能混杂在同一层中，但也不能太多，否则体系结构会过于庞大。

根据以上标准，OSI 参考模型分为物理层、数据链路层、网络层、传输层、会话层、表示层、应用层。

物理层涉及在信道上传输的原始比特流。

数据链路层的主要任务是加强物理层传输原始比特流的功能，使之对应的网络层显现为一条无错线路。发送包把输入数据封装在数据帧，按顺序传送出去并处理接收方回送的确认帧。

网络层关系到子网的运行控制，其中一个关键问题是确认从源端到目的端如何选择路由。

传输层的基本功能是从会话层接收数据而且把其分成较小的单元传递给网络层。

会话层允许不同机器上的用户建立会话关系。

表示层用来完成某些特定的功能。

应用层包含着大量人们普遍需要的协议。

答案：B，C，A，B，B。

面试例题 2：TCP 和 UDP 有什么区别？[中国著名金融软件公司 S 2005 年面试题]

解析：举例说明两者间的区别。

TCP 连接就像打电话，两者之间必须有一条不间断的通路，数据不到达对方，对方就一直在等待，除非对方直接挂电话。先说的话先到，后说的话后到，有顺序。

UDP 就像寄一封信，发信者只管发，不管到。但是你的信封上必须写明对方的地址。发信者和收信者之间没有通路，靠邮电局联系。信发到时可能已经过了很久，也可能根本没有发到。先发的信未必先到，后发的也未必后到。

答案：TCP 是传输控制协议，提供的是面向连接、可靠的字节流服务。当客户和服务器彼此交换数据前，必须先在双方之间建立一个 TCP 连接，之后才能传输数据。TCP 提供超时重发、丢弃重复数据、检验数据、流量控制等功能，保证数据能从一端传到另一端。

UDP 是用户数据报协议，是一个简单的面向数据报的运输层协议。UDP 不提供可靠性，它只是把应用程序传给 IP 层的数据报发送出去，但是并不保证它们能到达目的地。由于 UDP 在传

输数据报前不用在客户和服务器之间建立一个连接，且没有超时重发等机制，故而传输速度很快。

18.2　网络协议问题

面试例题 1：If we divide the network 40.15.0.0 into two subnets, and the first one is 40.15.0.0/17, then the second subnet will be ____.（如果把一个网络 40.15.0.0 分为两个子网，第一个子网是 40.15.0.0/17，那么第二个子网将会是_____。）[中国台湾某著名杀毒软件公司 2005 年 10 月面试题]

A．40.15.1.0/17　　B．40.15.2.0/16

C．40.15.100.0/17　　D．40.15.128.0/17

解析：让主网分成两个网段，子网掩码分别是 0xff 0xff 0x80 0x00 和 0xff 0xff 0x00 0x00。

答案：D

面试例题 2：If a worm scans the hosts in Class A IP address space on a home PC, it is quite probably that the host will received a lot of ____.（如果一个蠕虫病毒攻击了一个家用 PC 的 A 类地址主机的话，这个地址最有可能接收很多_____。）[中国台湾某著名杀毒软件公司 2005 年 10 月面试题]

A．HTTP response packet（HTTP 回应包）

B．DNS response packet（DNS 回应包）

C．ICMP destination unreachable packet（ICMP 目的无法抵达包）

D．ARP response（ARP 回应）

解析：大量发出 IP 请求，肯定很多不可达，返回不可达错误。

答案：C

面试例题 3：Before an IP datagram arrived at the destination, it ____.（在一个 IP 数据包到达目的地址之前，它_____。）[中国台湾某著名杀毒软件公司 2005 年 10 月面试题]

A．may be fragmented but never reassembled（可能成为碎片，而且不会重组）

B．may be fragmented or reassembled（可能成为碎片，或者重组）

C．can't be fragmented or reassembled（不能成为碎片，或者重组）

D．can't be fragmented but may be reassembled（不能成为碎片，但是可能会重组）

解析：网络问题，包未达到终点不可能重组，但可以分散成碎片。

答案：A

面试例题 4: In TCP/IP protocol stack, which of following is taken as an indication of congestion?（在 TCP/IP 协议栈里，如果出现阻塞情况，下面哪种情况最有可能发生？）[中国台湾某著名杀毒软件公司 2005 年 10 月面试题]

A. Link failure（连接错误）　　B. Free buffer（释放缓存）

C. Packet loss（丢包）　　D. Packet error（包错误）

解析: 网络阻塞问题。拥塞导致丢包。

答案: C

面试例题 5: If the TCP based server program crashed before the client data arrived on the connection that established earlier, the TCP/IP stack may return a ____.（如果 TCP 服务器在客户端发出数据报之前已经崩溃了，TCP/IP 栈可能返回一个_____。）[中国台湾某著名杀毒软件公司 2005 年 10 月面试题]

A. RST　　B. FIN　　C. SYN　　D. ACK

解析: SYN 包是 TCP 连接的第一个包，是非常小的一种数据包。SYN 攻击包括大量此类的包。由于这些包看上去来自实际不存在的站点，因此无法有效地进行处理。SYN 攻击就是利用 TCP 连接的 3 次握手机制，但发起攻击端只来一两次握手，而被攻击端一直在试图完成 TCP 连接，因此造成资源不足。

答案: C

面试例题 6: 如何编写 Socket 套接字? [中国著名通信企业 H 公司 2008 年面试题]

解析: Socket 相当于进行网络通信两端的插座，只要对方的 Socket 和自己的 Socket 有通信联接，双方就可以发送和接收数据了。其定义类似于文件句柄的定义。如果你要编写的是一个服务程序，那么先调用 socket()创建一个套接字，调用 bind()绑定 IP 地址和端口，然后启动一个死循环，循环中调用 accept()接受连接。对于每个接受的连接，可以启动多线程方式进行处理，在线程中调用 send()、recv()发送和接收数据。

如果你要编写的是一个客户端程序，那么就简单多了。先调用 socket()创建一个套接字，然后调用 connect()连接服务器，之后就是调用 send()、recv()发送和接收数据了。

答案:　服务器端程序编写:

（1）调用 ServerSocket(int port)创建一个服务器端套接字，并绑定到指定端口上。

（2）调用 accept()，监听连接请求，则接收连接，返回通信套接字。

（3）调用 Socket 类的 getOutStream()和 getInputStream 获取输出流和输入流，开始网络

数据的发送和接收。

（4）关闭通信套接字.Socket.close()。

客户端程序编写:

（1）调用 Socket()创建一个流套接字，并连接到服务器端。

（2）调用 Socket 类的 getOutputStream()和 fetInputStream 获取输出流和输入流，开始网络数据的发送和接收。

（3）关闭通信套接字.Socket.close()。

18.3　网络安全问题

面试例题 1: 入侵检测与防火墙有何不同，各有什么优缺点？[中国著名通信企业 H 公司 2008 年面试题]

答案:

防火墙的优点: 它能增强机构内部网络的安全性，用于加强网络间的访问控制，防止外部用户非法使用内部网的资源，保护内部网络的设备不被破坏，防止内部网络的敏感数据被窃取。防火墙系统决定了哪些内部服务可以被外界访问; 外界的哪些人可以访问内部的哪些服务，以及哪些外部服务可以被内部人员访问。

防火墙的缺点: 对于发生在内网的攻击无能为力; 对于部分攻击，可以绕过防火墙，防火墙发现不了; 防火墙的策略是静态的，不能实施动态防御; 等等。

入侵检测的优势: 入侵监测系统扫描当前网络的活动，监视和记录网络的流量，根据定义好的规则来过滤从主机网卡到网线上的流量，提供实时报警。大多数的入侵监测系统可以提供关于网络流量非常详尽的分析。它们可以监视任何定义好的流量。很多系统对 FTP、HTTP 和 Telnet 流量都有默认的设置，还有其他的流量，如 NetBus、本地和远程登录失败，等等。也可以自己定制策略。如果定义了策略和规则，便可以获得 FTP、SMTP、Telnet 和任何其他的流量。这种规则有助于追查该连接和确定网络上发生过什么，以及现在正在发生什么。这些程序在需要确定网络中策略实施的一致性情况时是非常有效的工具。

入侵检测的缺点: 目前入侵检测技术的方法主要停留在异常检测统计方法和误用检测方法上，这两种方法都还存在这样或那样的问题。网络入侵技术在不断地发展，入侵的行为表现出不确定性、多样性等特点。网络应用的发展又带来新的安全问题。如高速网络技术出现流量大的特点，那么基于网络的入侵检测系统如何适应这种情况？基于主机审计数据怎样做

到既减少数据量，又能有效地检测到入侵？入侵检测研究领域急需其他学科知识提供新的入侵检测解决方法。入侵检测只是仅仅试图发现计算机网络中的安全问题，要解决网络安全的问题还需要其他的网络安全技术。另外，入侵检测系统本身还存在安全问题。入侵检测系统也可能会受到攻击。

终上所述，其实防火墙和入侵检测各有优劣。打个比方，防火墙就相当于一栋大楼外的门卫系统，而入侵检测就相当于大楼内的监控系统，两者缺一不可。应该将入侵检测系统与防火墙联动起来，当入侵检测系统发现到有入侵行为时，应及时报告防火墙，以阻断入侵。

面试例题 2：25 端口是做什么用的，有什么漏洞么？[中美合资通信企业 HS 公司 2008 年面试题]

答案： 25 端口为 SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）服务器所开放，主要用于发送邮件，如今绝大多数邮件服务器都使用该协议。比如在使用电子邮件客户端程序的时候，在创建账户时会要求输入 SMTP 服务器地址，该服务器地址默认情况下使用的就是 25 端口。

端口漏洞：利用 25 端口，黑客可以寻找 SMTP 服务器，用来转发垃圾邮件。25 端口被很多木马程序开放，比如 Ajan、Antigen、Email Password Sender、ProMail、Trojan、Tapiras、Terminator、WinPC、WinSpy，等等。拿 WinSpy 来说，通过开放 25 端口，可以监视计算机正在运行的所有窗口和模块。

扩展知识（端口概念）

在网络技术中，端口（Port）大致有两种意思：一是物理意义上的端口，比如，ADSL MODEM、集线器、交换机、路由器用于连接其他网络设备的接口，如 RJ-45 端口、SC 端口，等等；二是逻辑意义上的端口，一般是指 TCP/IP 协议中的端口，端口号的范围为 0～65 535，比如用于浏览网页服务的 80 端口，用于 FTP 服务的 21 端口，等等。我们这里将要介绍的就是逻辑意义上的端口。

逻辑意义上的端口有多种分类标准，下面将介绍两种常见的分类。

1）按端口号分布划分

①知名端口（Well-Known Ports）

知名端口即众所周知的端口号，范围为 0～1023，这些端口号一般固定分配给一些服务。比如 21 端口分配给 FTP 服务，25 端口分配给 SMTP（简单邮件传输协议）服务，80 端口分配给 HTTP 服务，135 端口分配给 RPC（远程过程调用）服务，等等。

②动态端口（Dynamic Ports）

动态端口的范围为 1024～65535，这些端口号一般不固定分配给某个服务，也就是说许多服务都可以使用这些端口。只要运行的程序向系统提出访问网络的申请，那么系统就可以从这些端口号中分配一个供该程序使用。比如 1024 端口就是分配给第一个向系统发出申请的程序。在关闭程序进程后，就会释放所占用的端口号。

不过，动态端口也常常被病毒木马程序所利用，如冰河默认连接端口是 7626，WAY 2.4 是 8011，Netspy 3.0 是 7306，YAI 病毒是 1024，等等。

2）按协议类型划分

按协议类型划分，可以分为 TCP、UDP、IP 和 ICMP（Internet 控制消息协议）等端口。下面主要介绍 TCP 和 UDP 端口。

①TCP 端口

TCP 端口，即传输控制协议端口，需要在客户端和服务器之间建立连接，这样可以提供可靠的数据传输。常见的包括 FTP 服务的 21 端口，Telnet 服务的 23 端口，SMTP 服务的 25 端口，以及 HTTP 服务的 80 端口，等等。

②UDP 端口

UDP 端口，即用户数据包协议端口，无须在客户端和服务器之间建立连接，安全性得不到保障。常见的有 DNS 服务的 53 端口，SNMP（简单网络管理协议）服务的 161 端口，QQ 使用的 8000 和 4000 端口，等等。

对于常见网络端口如端口 0 、1、7 、21、22、23、53、67、68、69、79、80、99 等，读者要有一定理解。请查阅相关网络书籍，这里不再赘述。

18.4　网络其他问题

面试例题 1： 在子网 210.27.48.21/30 中有多少个可用地址，分别是什么？[中美合资某著名通信企业面试题]

答案：210.27.48.21/30 代表的子网的网络号是 30 位，即网络号是 210.27.48.21 & 255.255.255.251=210.27.48.20，此子网的地址空间是 2 位，即可以有 4 个地址：210.27.48.20、210.27.48.21、210.27.48.22 和 210.27.48.23。第一个地址的主机号（host number/id）是 0，而主机号 0 代表的是 multicast（多播）地址。最后一个地址的最后两位是 11，主机号每一位都为 1 代表的是广播（broadcast）地址。所以只有中间两个地址可以给 host 使用。

面试例题 2： 网络中常见的 ping 命令是什么协议？[中美合资通信企业 HS 公司面试题]

解析：ICMP 是“Internet Control Message Protocol”（Internet 控制消息协议）的缩写。它是 TCP/IP 协议族的一个子协议，用于在 IP 主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。

在网络中经常会使用到 ICMP 协议，只不过觉察不到而已。比如经常使用的用于检查网络通不通的 ping 命令，这个“ping”的过程实际上就是 ICMP 协议工作的过程。还有其他的网络命令，如跟踪路由的 Tracert 命令也是基于 ICMP 协议的。

ICMP 协议对于网络安全具有极其重要的意义。ICMP 协议本身的特点决定了它非常容易被用于攻击网络上的路由器和主机。例如，在 1999 年 8 月某公司“悬赏”50 万元测试防火墙的过程中，其防火墙遭受到的 ICMP 攻击达 334 050 次之多，占整个攻击总数的 90%以上。可见，ICMP 的重要性绝不可以忽视。

比如，可以利用操作系统规定的 ICMP 数据包最大尺寸不超过 64KB 这一规定，向主机发起“Ping of Death”（死亡之 Ping）攻击。“Ping of Death”攻击的原理是：如果 ICMP 数据包的尺寸超过 64KB 上限时，主机就会出现内存分配错误，导致 TCP/IP 堆栈崩溃，致使主机死机。

此外，向目标主机长时间、连续、大量地发送 ICMP 数据包，也会最终使系统瘫痪。大量的 ICMP 数据包会形成“ICMP 风暴”，使得目标主机耗费大量的 CPU 资源处理，疲于奔命。

答案：

ping.exe 的原理是，向指定的 IP 地址发送一定长度的数据包，按照约定，若指定 IP 地址存在的话，会返回同样大小的数据包，当然，若在特定的时间内没有返回，就是“超时”，就认为指定的 IP 地址不存在。由于 ping 使用的是 ICMP 协议，有些防火墙软件会屏蔽 ICMP 协议，所以有时候 ping 的结果只能作为参考，ping 不通并不一定说明对方 IP 不存在。

ping 命令是一个非常有用的网络命令，大家常用它来测试网络连通情况。但同时它也是一把“双刃剑”，别人使用 ping 命令能探测到你计算机上的很多敏感信息，造成不安全。为了安全，防止 ping 的方法也有很多，比如防火墙，又比如创建一个禁止所有计算机 ping 本机 IP 地址的安全策略。

由于 ping 使用的是 ICMP 协议，有些防火墙软件会屏蔽掉 ICMP 协议。IPSec 安全策略是如何“防 ping”的？其原理是通过新建一个 IPSec 策略过滤本机所有的 ICMP 数据包。这样确实可以有效地“防 ping”，但同时也会留下后遗症。因为 ping 命令和 ICMP 协议有着密切的关系。在 ICMP 协议的应用中包含有 11 种报文格式，其中 ping 命令就是利用 ICMP 协议中的“Echo Request”报文进行工作的。但 IPSec 安全策略防 ping 时采用格杀勿论的方法，

把所有的 ICMP 报文全部过滤了，特别是很多有用的其他格式的报文也同时被过滤了。因此在某些有特殊应用的局域网环境中，容易出现数据包丢失的现象，影响用户正常办公。因此建议使用防火墙。

扩展知识（常见网络协议）

1. 动态主机配置协议

动态主机配置协议从原有的 BOOTP 协议发展而来，原来的目的是为无盘工作站分配 IP 地址的协议，当前更多地用于对多个客户计算机集中分配 IP 地址，以及 IP 地址相关的信息的协议，这样就能将 IP 地址和 TCP/IP 的设置统一管理起来，而避免不必要的地址冲突的问题。它提供了 3 种 IP 地址分配机制：自动分配——给客户机分配永久的地址；动态分配——给客户机分配有一定租用期限的地址；手工分配——由网络管理员给客户机分配地址，并通过 DHCP 传达给客户机。

2. 边界网关协议

边界网关协议是不同自治系统路由器之间进行通信的外部网关协议，是 EGP 的替代品。BGP 系统之间交换网络可达到信息。这些信息包括数据到达这些网络所必须经过的自治系统 AS 中的所有路径，通过这些信息构造自治系统连接图，然后根据连接图删除选路环，制定选路策略。

3. VoIP 协议

VoIP（Voice over Internet Protocol）是一种以 IP 电话为主，并推出相应的增值业务的技术。VoIP 最大的优势是能广泛地采用 Internet 和全球 IP 互连的环境，提供比传统业务更多、更好的服务。VoIP 可以在 IP 网络上便宜地传送语音、传真、视频和数据等业务，如统一消息、虚拟电话、虚拟语音/传真邮箱、查号业务、Internet 呼叫中心、Internet 呼叫管理、电视会议、电子商务、传真存储转发和各种信息的存储转发等。

使用 VoIP 的主要优点是把 VoIP 集成到集中器或 RAS 中，企业将进入一个充满机遇的新世界。如果该企业是服务提供商或传输服务提供商，则能够向用户提供附加业务。如果是远程用户，则访问过程将明显简化。

4. P2P 协议

P2P 是以太网上的点对点协议，是将以太网和 PPP 协议结合后的协议，目前广泛应用在 ADSL 接入方式中。通过 PPPoE 技术和宽带调制解调器（比如 ADSL MODEM），我们就可以实现高速宽带网的个人身份验证访问，为每个用户创建虚拟拨号连接，这样就可以高速连接到 Internet。

5. ARP 协议

ARP（Address Resolution Protocol，地址解析协议）主要负责将局域网中的 32 位 IP 地址转换为对应的 48 位物理地址，即网卡的 MAC 地址，比如 IP 地址为 192.168.0.1 的网卡 MAC 地址为 00-03-0F-FD-1D-2B。整个转换过程是一台主机先向目标主机发送包含 IP 地址信息的广播数据包，即 ARP 请求，然后目标主机向该主机发送一个含有 IP 地址和 MAC 地址的数据包。通过 MAC 地址，两个主机就可以实现数据传输了。

6. IPX/SPX 协议

IPX/SPX 协议即 IPX 与 SPX 协议的组合。它是 Novell 公司为了适应网络的发展而开发的通信协议，具有很强的适应性，安装方便，同时还具有路由功能，可以实现多网段间的通信。其中，IPX 负责数据包的传送；SPX 负责数据包传输的完整性。在微软的 Windows NT 操作系统中，一般使用 NWLink IPX/SPX 兼容协议和 NWLink NetBIOS 两种 IPX/SPX 的兼容协议，该兼容协议继承了 IPX/SPX 协议的优点，更适应 Windows 的网络环境。IPX/SPX 协议一般可以应用于大型网络（比如 Novell）和局域网游戏环境中（比如反恐精英、星际争霸）。不过，如果不是在 Novell 网络环境中，一般不使用 IPX/SPX 协议，而是使用 IPX/SPX 兼容协议，尤其是在 Windows 9x/2000 组成的对等网中。

7. SNMP 协议

简单网络管理协议（SNMP）首先是由 Internet 工程任务组织（Internet Engineering Task Force，IETF）的研究小组为了解决 Internet 上的路由器管理问题而提出的。

SNMP 被设计成与协议无关，所以它可以在 IP、IPX、AppleTalk、OSI 及其他用到的传输协议上被使用。它们提供了一种从网络上的设备中收集网络管理信息的方法。SNMP 也为设备向网络管理工作站报告问题和错误提供了一种方法。

8. TCP

TCP（Transmission Control Protocol，传输控制协议）主要用于在主机间建立一个虚拟连接，以实现高可靠性的数据包交换。IP 协议可以进行 IP 数据包的分割和组装，但是通过 IP 协议并不能清楚地了解到数据包是否顺利地发送给目标计算机。而使用 TCP 协议就不同了。在该协议传输模式中，在将数据包成功发送给目标计算机后，TCP 会要求发送一个确认；如果在某个时限内没有收到确认，那么 TCP 将重新发送数据包。另外，在传输的过程中，如果接收到无序、丢失及被破坏的数据包，TCP 还可以负责恢复。

9. IP 协议

IP（互联网协议）主要负责 IP 寻址、路由选择和 IP 数据包的分割和组装。通常

所说的 IP 地址可以理解为符合 IP 协议的地址。目前，常用的 IP 协议是 IP 协议的第四版本，即 IPv4，是互联网中最基础的协议，于 1981 年在 RFC 791 中定义。

IPv4 使用了 32 位地址，通常使用圆点分隔的 4 个十进制数字表示，比如 192.168.0.1。目前，IPv4 最多支持 4 294 967 296（2 的 32 次方）个地址连接到 Internet。随着互联网的迅猛发展，IP 地址的需求越来越大，在未来几年有被用完的危机。

10. Layer 2 Tunneling Protocol

Layer 2 Tunneling Protocol 即第二层隧道协议。该协议是一种工业标准的 Internet 隧道协议，功能大致和 PPTP 协议类似，比如同样可以对网络数据流进行加密。不过也有不同之处，比如 PPTP 要求网络为 IP 网络，L2TP 要求面向数据包的点对点连接；PPTP 使用单一隧道，L2TP 使用多隧道；L2TP 提供包头压缩、隧道验证，而 PPTP 不支持。

在 VPN 连接中要设置 L2TP 连接，方法同 PPTP VPN 设置，同样是在 VPN 连接属性窗口的“网络”选项卡中，将 VPN 类型设置为“L2TP IPSec VPN”即可。

11. NetBIOS Extend User Interface

NetBIOS Extend User Interface 即 NetBIOS 用户扩展接口协议。是 IBM 于 1985 年提出的，主要用于 20～200 台计算机的小型局域网中，比如早期的 DOS、LAN Manager、Windows 3.x，等等。NetBEUI 协议可以看做是 NetBIOS 协议的延伸和改良版本，具有体积小、效率高、速度快等特点。NetBEUI 可以看做是一种传输协议，而 NetBIOS 仅仅是通过一组命令来让系统使用网络而已。

面试例题 3： 说一下 TCP 的 3 次握手 4 次挥手全过程是什么样的？

[中美合资某通信企业 HS 公司面试题]

答案：在 TCP/IP 协议中，TCP 协议提供可靠的连接服务，采用 3 次握手建立一个连接。

第 1 次握手：建立连接时，客户端发送 SYN 包（syn=j）到服务器，并进入 SYN_SEND 状态，等待服务器确认。

第 2 次握手：服务器收到 SYN 包，必须确认客户的 SYN（ack=j+1），同时自己也发送一个 SYN 包（syn=k），即 SYN+ACK 包，此时服务器进入 SYN_RECV 状态。

第 3 次握手：客户端收到服务器的 SYN＋ACK 包，向服务器发送确认包 ACK(ack=k+1)，此包发送完毕，客户端和服务器进入 ESTABLISHED 状态，完成 3 次握手。

完成 3 次握手，客户端与服务器开始传送数据。在上述过程中，还有一些重要的概念。

未连接队列：在 3 次握手协议中，服务器维护一个未连接队列，该队列为每个客户端的

SYN 包（syn=j）开设一个条目，该条目表明服务器已收到 SYN 包，并向客户发出确认，正在等待客户的确认包。这些条目所标识的连接在服务器处于 Syn_RECV 状态，当服务器收到客户的确认包时，删除该条目，服务器进入 ESTABLISHED 状态。

Backlog 参数：表示未连接队列的最大容纳数目。

SYN-ACK 重传次数：服务器发送完 SYN-ACK 包，如果未收到客户确认包，服务器进行首次重传，等待一段时间仍未收到客户确认包，进行第二次重传，如果重传次数超过系统规定的最大重传次数，系统将该连接信息从半连接队列中删除。注意，每次重传等待的时间不一定相同。

半连接存活时间：是指半连接队列的条目存活的最长时间，即服务从收到 SYN 包到确认这个报文无效的最长时间，该时间值是所有重传请求包的最长等待时间总和。有时我们也称半连接存活时间为 Timeout 时间、SYN_RECV 存活时间。