1. 应用层协议
2. 概述

利用网络的应用程序有很多，如Web浏览器，电子邮件，能够让这些应用进行特定通信处理的正是这些应用协议，开发人员可以利用现有的应用协议，也可以自定义协议。

1. 远程登录
2. 概述

远程的呢过路是为了实现TSS（分时系统）的环境，将主机和终端的关系应用到计算机网络上的一个结果，TSS中通常有一个处理能力很强的主机，围绕着该主机的是多个终端，这些终端通过专线和主机相连。远程登录主要使用TELNET和SSH两种协议。

1. TELNET

TELNET利用TCP的一条连接，向主机发送文字命令并在主机上执行，本地用户好像直接和远程主机内部的Shell相连着一样，直接在本地操作。Shell是操作系统提供给用户的，便于使用该系统中各种功能的一种用户接口，它可以解释用户从键盘或鼠标输入的内容，并由操作系统执行。

TELNET分为两类基本服务，一个是仿真终端功能，一个是协商选项功能。TELNET过程如下：

1. 本地键入命令；
2. 发送命令给远程机的telnetd守护进程；
3. 向Shell发送文字命令；
4. 获取从Shell返回的结果；
5. 将结果返回给TELNET客户端；
6. 回显在屏幕上；

TELNET经常用于登录路由器或者高性能交换机等网络设备进行设置，客户端通常与目标主机的23号端口连接。

1. SSH

SSH是加密的远程登录系统，TELNET中登录时无需输入密码，有窃听危险，使用SSH可以进行加密通信。还有认证机制，端口转发功能，即将特定端口号收到的消息转发到特定的IP地址和端口号码中。

1. 文件传输

FTP是文件传输的协议，使用两条TCP连接，一条用来控制，一条用来数据传输。控制的TCP用于用户登录，设置参数等等，使用的是21端口，该连接会一直存在，除非用户要求断开；而用于数据传输的TCP连接在数据传输完成后会被关闭，且传输的方向与控制的方向是相反的，那么在通过NAT连接外部的FTP服务器时，无法直接建立传输数据使用的TCP连接，这是必须使用PASV命令来修改建立连接的方向才行，数据传输的TCP连接使用的是20端口，或者随机数端口。

1. 电子邮件
2. 概述

提供电子邮件服务的协议叫做SMTP，传输层使用了TCP协议。发送端和接收端通过邮件服务器进行收发邮件，发送端通过SMTP协议发送邮件，接收端通过POP3协议接受邮件。电子邮件机制由三部分组成，分别是邮件地址，数据格式以及发送协议。

1. 邮件地址

邮件地址的格式如下：

姓名@通信地址

[如974076924@qq.com](mailto:如974076924@qq.com)

974076924是姓名，而qq是接受邮件的主机名称，com则是域名。现在的电子邮件发送地址由DNS管理，DNS中注册有邮件地址以及作为发送地址时对应的邮件服务器的域名，这些映射信息被称为MX记录。很明显，发送给这个地址的邮件会被发送给qq服务器。

1. MIME

电子邮件所能够发送的数据类型已经被扩展到MIME了，可以发送各种数据，MIME由首部和正文组成，首部的“Content-Type”指定了数据格式。

1. SMTP

SMTP是发送电子邮件的协议，使用的是TCP的25号端口，在这个连接上进行控制和应答以及数据的发送，客户端以文本形式发出请求，服务端返回一个3位数字的应答。由于SMTP本身没有验证发送者的功能，因此无法避免垃圾邮件到达自己的邮件服务器。不过现在通过SMTP认证进行认证，能够防止冒充发送者。

1. POP

由于接收端电脑不可能一直处于开机状态，用户希望在一开机就能够接收到邮件，而SMTP没有这种机制。POP协议是一个专门用来接收电子邮件的协议，发送端的邮件根据SMTP协议会被转发给POP服务器，接收端再根据POP协议接受邮件。

1. WWW
2. 概述

万维网是将互联网中的信息以超文本的形式展现的系统，也叫作Web，可以显示WWW信息的客户端叫做Web浏览器。WWW中定义了三个重要的概念，访问信息的手段与位置（URI），信息的表现形式（HTML），信息转发（HTTP）。

1. URI

URI是统一资源标识符，用于标识资源，而URL是统一资源定位符，用于定位互联网中资源的具体位置，但是URI不局限与标识互联网资源，可以作为所有资源的标识符。

1. HTML

HTML是表示Web页的一种语言，可以展示各种数据。

1. HTTP

HTTP默认80端口，首先客户端向服务器的80端口建立一个TCP连接，然后在这个TCP连接上进行请求和应答以及数据报的发送。HTTP常用两个版本，一个是HTTP1.0，一个是HTTP1.1。在HTTP1.0中每个命令和应答都会触发一次TCP连接的建立和断开，而从HTTP1.1开始，允许在一个TCP连接中发送多个命令和应答，减少了TCP连接数量，提高了效率，这种方式称为保持连接。

1. 网络安全
2. 防火墙

防火墙的类型有很多，如专门过滤特定数据包的包过滤防火墙，数据到达应用后由应用处理并拒绝非法访问的应用网关，防火墙基本的设计思路是暴露给危险的主机和路由器的个数是有限的。比如我们只开放80端口和22端口，其他端口都不开放，或者只允许TCP连接从内网发起，外网不允许连接内网，这就通过监控TCP包首部的SYN和ACK标志位来实现，当SYN=1，ACK=0时属于互联网发来的包，应当丢弃。

1. PKI

PKI是公钥基础结构，通过可信赖的第三方检查通信对方是否真实而进行验证的机制。可信赖的第三方称为CA，用户可以利用CA颁发的数字证书来验证通信对方的真实性。该数字证书包含用户身份信息，用户公钥信息以及证书签发机构对该证书的数字签名信息。CA的数字签名可以确保用户身份和公钥信息的真实性，而公钥信息可以用于加密数据或验证对应私钥的签名。PKI通常用于HTTPS通信中。

1. 对称密码

加密指的是利用（某个值）密钥对明文的数据通过一定的算法变换为加密数据的过程。加密和解密使用相同的密钥叫做对称加密方式，如果使用不同的密钥，即公钥和密钥则是公钥加密方式，这种方式需要严格地管理私钥，会花费更多的时间。

对称加密方式包括AES，DES，而公钥加密方式包括RSA，DH等。

1. 安全协议
2. VPN与IPsec

在互联网上构造一个虚拟的私有网络VPN，构建VPN时使用的是IPsec，在IP首部的后面追加“封装安全有效载荷”和“认证首部”，从而对此后的数据进行加密，收包时根据首部对数据进行解密，恢复成原始数据。

1. TLS/SSL 和HTTPS

使用TLS/SSL对HTTP通信加密，即HTTPS通信，采用的是对称加密方式，而在发送其公钥时采用的是公钥加密方式。下面是HTTPS的详细步骤：

1. 客户端向Web服务器发送HTTPS请求；
2. Web服务器发送自己的公钥和电子证书，电子证书被认证中心的私钥加密；
3. 客户端确认电子证书，因为认证中心的公钥一般都存储在Web浏览器中，所以浏览器既可以通过认证中心的公钥来确认电子证书的正确性以及确认Web服务器的公钥；
4. 客户端生成对称加密方式的密钥，使用Web服务器的公钥对刚生成的对称加密的密钥进行加密后发送；
5. Web服务器收到后用自己的私钥解密，得到对称加密的密钥；
6. 至此，客户端和Web服务端都有了对称加密的密钥了，就可以进行通信了。