1. 名词解释

Part-A:

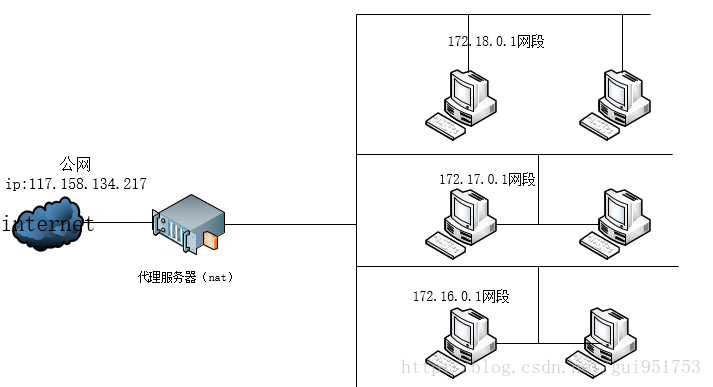
1. NAT:

NAT（Network Address Translation，网络地址转换）

当在专用网内部的一些主机本来已经分配到了本地IP地址（即仅在本专用网内使用的专用地址），但现在又想和因特网上的主机通信（并不需要加密）时，可使用NAT方法。

这种方法需要在专用网连接到因特网的路由器上安装NAT软件。装有NAT软件的路由器叫做NAT路由器，它至少有一个有效的外部全球IP地址。这样，所有使用本地地址的主机在和外界通信时，都要在NAT路由器上将其本地地址转换成全球IP地址，才能和因特网连接。

另外，这种通过使用少量的公有IP 地址代表较多的私有IP 地址的方式，将有助于减缓可用的IP地址空间的枯竭



一个A类或其他类的公网IP被分配给学校或组织，通过NAT进行网络网址转换，转换为许多个172开头的B类私有网络地址；

192开头的一般是C类私有网络地址；

69开头的是一个保留地址，是本地连接受限时系统自动分配的ip没有什么实际的意义，出现这种情况可能是服务器还没搭建好。果然，等我们重新搭建好了代理服务器之后，我们的网址又变回了现在的172.18开头的网址。

ipconfig得到的是private IP，百度等搜索出的是public ip；

1. Proxy:

**代理**（英语：**Proxy**），也称**网络代理**，是一种特殊的网络服务，允许一个网络终端（一般为客户端）通过这个服务与另一个网络终端（一般为服务器）进行非直接的连接。一些网关、路由器等网络设备具备网络代理功能。一般认为代理服务有利于保障网络终端的隐私或安全，防止攻击。

提供代理服务的电脑系统或其它类型的网络终端称为**代理服务器**（英文：**Proxy Server**）。代理[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8/100571" \t "https://baike.baidu.com/item/%E4%BB%A3%E7%90%86%E6%9C%8D%E5%8A%A1%E5%99%A8/_blank)（Proxy Server）是一种重要的服务器安全功能，它的工作主要在[开放系统互联](https://baike.baidu.com/item/%E5%BC%80%E6%94%BE%E7%B3%BB%E7%BB%9F%E4%BA%92%E8%81%94/9719696" \t "https://baike.baidu.com/item/%E4%BB%A3%E7%90%86%E6%9C%8D%E5%8A%A1%E5%99%A8/_blank)(OSI)模型的会话层，从而起到[防火墙](https://baike.baidu.com/item/%E9%98%B2%E7%81%AB%E5%A2%99/52767" \t "https://baike.baidu.com/item/%E4%BB%A3%E7%90%86%E6%9C%8D%E5%8A%A1%E5%99%A8/_blank)的作用。代理服务器大多被用来连接[INTERNET](https://baike.baidu.com/item/INTERNET" \t "https://baike.baidu.com/item/%E4%BB%A3%E7%90%86%E6%9C%8D%E5%8A%A1%E5%99%A8/_blank)（国际互联网）和Local Area Network（[局域网](https://baike.baidu.com/item/%E5%B1%80%E5%9F%9F%E7%BD%91/98626" \t "https://baike.baidu.com/item/%E4%BB%A3%E7%90%86%E6%9C%8D%E5%8A%A1%E5%99%A8/_blank)）。允许一个网络终端（一般为客户端）通过这个服务与另一个网络终端（一般为服务器）进行非直接的连接

1. HTTP Proxy:

代理http。

目前HTTP功能支持“直接连接”和“通过HTTP代理”两种形式的连接。例如QQ：简单地说，如果用户所在局域网并未设置任何代理服务器，则选择“直接连接”就可以实现QQ连通；而如果用户所在局域网设置了代理服务器，则必须选择“通过HTTP代理”，并填写所在局域网的代理服务器地址、端口等详细资料，方有可能实现QQ连通。 　代理客户机的http访问，主要代理浏览器访问网页，它的端口一般为80、8080、3128等。www对于每一个上网的人都再熟悉不过了，www连接请求就是采用的http协议，所以我们在浏览网页，下载数据（也可采用ftp协议）时就是用http代理。它通常绑定在代理服务器的80、3128、8080等端口上。

1. IPv6:

IPv6是英文“Internet Protocol Version 6”（互联网协议第6版）的缩写，是互联网工程任务组（IETF）设计的用于替代[IPv4](https://baike.baidu.com/item/IPv4/422599" \t "https://baike.baidu.com/item/IPv6/_blank)的下一代IP协议，其地址数量号称可以为全世界的每一粒沙子编上一个地址

IPv6是128位，是IPv4的4倍，用16进制表示；

一、冒分十六进制表示法  
　　格式为X:X:X:X:X:X:X:X，其中每个X表示地址中的16b，以十六进制表示，例如：  
　　ABCD:EF01:2345:6789:ABCD:EF01:2345:6789  
　　这种表示法中，每个X的前导0是可以省略的，例如：  
　　2001:0DB8:0000:0023:0008:0800:200C:417A→ 2001:DB8:0:23:8:800:200C:417A

二、0位压缩表示法  
　　在某些情况下，一个IPv6地址中间可能包含很长的一段0，可以把连续的一段0压缩为“::”。但为保证地址解析的唯一性，地址中”::”只能出现一次，例如：  
　　FF01:0:0:0:0:0:0:1101 → FF01::1101  
　　0:0:0:0:0:0:0:1 → ::1  
　　0:0:0:0:0:0:0:0 → ::

三、内嵌IPv4地址表示法  
　　为了实现IPv4-IPv6互通，IPv4地址会嵌入IPv6地址中，此时地址常表示为：X:X:X:X:X:X:d.d.d.d，前96b采用冒分十六进制表示，而最后32b地址则使用IPv4的点分十进制表示，例如::192.168.0.1与::FFFF:192.168.0.1就是两个典型的例子，注意在前96b中，压缩0位的方法依旧适用

1. SOCKS/SOCKS4/SOCKS4A/SOCKS5

SOCKS：[防火墙](https://baike.baidu.com/item/%E9%98%B2%E7%81%AB%E5%A2%99" \t "https://baike.baidu.com/item/socks/_blank)安全会话转换协议 （Socks: Protocol for sessions traversal across firewall securely） SOCKS 协议提供一个框架，为在 TCP 和 UDP 域中的客户机/服务器应用程序能更方便安全地使用[网络防火墙](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E9%98%B2%E7%81%AB%E5%A2%99/7112674" \t "https://baike.baidu.com/item/socks/_blank)所提供的服务。

SOCKS代理与其他类型的代理不同，它只是简单地传递数据包，而并不关心是何种应用协议，既可以是HTTP请求，所以SOCKS代理服务器比其他类型的代理服务器速度要快得多。

SOCKS代理又分为SOCKS4和SOCKS5

二者不同的是SOCKS4代理只支持TCP协议（即传输控制协议），而SOCKS5代理则既支持TCP协议又支持UDP协议（即用户数据包协议），还支持各种身份验证机制、服务器端域名解析等。

SOCK4能做到的SOCKS5都可得到，但SOCKS5能够做到的SOCK4则不一定能做到，比如我们常用的聊天工具QQ在使用代理时就要求用SOCKS5代理，因为它需要使用UDP协议来传输数据。通常对外开放的socks代理都是socks4代理，因此,UDP应用通常都不能被支持。

Socks4代理无法将要查询的域名传递到“退出节点”（exit node）进行解析，应用程序根本不经过Tor的代理就直接用了本地的Dns解析域名。  
Socks4a代理在Socks4的基础上做了一些改动，可以完全将要查询的域名传递到“退出节点”（exit node）进行解析，不会发生Dns解析泄漏。

1. UPNP

**通用即插即用**（英语：Universal Plug and Play，简称**UPnP**）是由“通用即插即用论坛”（UPnP™ Forum）推广的一套网络协议。该协议的目标是使**家庭网络**（数据共享、通信和娱乐）和**公司网络**中的**各种设备**能够**相互无缝连接**，并简化相关网络的实现。UPnP通过定义和发布基于开放、因特网通讯网协议标准的UPnP设备控制协议来实现这一目标。

1. DHT

DHT(Distributed Hash Table，分布式[哈希表](https://baike.baidu.com/item/%E5%93%88%E5%B8%8C%E8%A1%A8" \t "https://baike.baidu.com/item/DHT/_blank))类似Tracker的根据种子特征码返回种子信息的网络，是一种分布式存储方法。在不需要服务器的情况下，每个客户端负责一个小范围的路由，并负责存储一小部分数据，从而实现整个DHT网络的寻址和存储。

新版BitComet允许同时连接DHT网络和Tracker，也就是说在完全不连上Tracker服务器的情况下，也可以很好的下载，因为它可以在DHT网络中寻找下载同一文件的其他用户。

1. Port and service

端口与服务

有些服务是对外开放的，这个时候它就要用到端口。。。。比如你的IE，当你要使用IE的时候，默认情况，下它需要通过[80端口](https://www.baidu.com/s?wd=80%E7%AB%AF%E5%8F%A3&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao" \t "https://zhidao.baidu.com/question/_blank)和外界通讯，关闭了[80端口](https://www.baidu.com/s?wd=80%E7%AB%AF%E5%8F%A3&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao" \t "https://zhidao.baidu.com/question/_blank)，就无法连接出去了（除非你换了端口）。。。。。。

每个服务都有一个特定的端口。

端口有什么用呢？我们知道，一台拥有IP地址的主机可以提供许多服务，比如Web服务、FTP服务、SMTP服务等，这些服务完全可以通过1个IP地址来实现。那么，主机是怎样区分不同的网络服务呢？显然不能只靠IP地址，因为IP 地址与网络服务的关系是一对多的关系。实际上是通过“IP地址+端口号”来区分不同的服务的。

1. WIFI/IEEE 802.11

无线局域网最通用的标准是IEEE定义的802.11系列标准。

WIFI(WirelessFidelity，无线保真)技术是一个基于IEEE802．11系列标准的无线网路通信技术的品牌，可以改善基于IEEE802.11标准的无线网路产品之间的互通性。其目前可使用的标准有两个，分别是IEEE802.11a和IEEE802.11b。

简单来说WIFI就是一种无线联网的技术，以前通过网络连接电脑，而现在则是通过无线电波来连网。与蓝牙技术一样，wifi同属于在办公室和家庭中使用的短距离无线技术。该技术使用的使2.4GHz附近的频段，该频段目前尚属没用许可的无线频段。

1. ISM 段频

**ISM频段**（**I**ndustrial**S**cientific**M**edical Band），中文意思分别是**工业的**(Industrial)、**科学的**(Scientific)和**医学的**(Medical)，因此顾名思义ISM频段就是各国挪出某一段频段主要开放给[工业](https://baike.baidu.com/item/%E5%B7%A5%E4%B8%9A" \t "https://baike.baidu.com/item/ISM%E9%A2%91%E6%AE%B5/_blank)，[科学](https://baike.baidu.com/item/%E7%A7%91%E5%AD%A6" \t "https://baike.baidu.com/item/ISM%E9%A2%91%E6%AE%B5/_blank)和[医学](https://baike.baidu.com/item/%E5%8C%BB%E5%AD%A6" \t "https://baike.baidu.com/item/ISM%E9%A2%91%E6%AE%B5/_blank)机构使用。应用这些频段无需许可证或费用，只需要遵守一定的发射功率（一般低于1W），并且不要对其它频段造成干扰即可。ISM频段在各国的规定并不统一。如在[美国](https://baike.baidu.com/item/%E7%BE%8E%E5%9B%BD" \t "https://baike.baidu.com/item/ISM%E9%A2%91%E6%AE%B5/_blank)有三个频段902-928 MHz、2400-2484.5 MHz及5725-5850 MHz，而在[欧洲](https://baike.baidu.com/item/%E6%AC%A7%E6%B4%B2" \t "https://baike.baidu.com/item/ISM%E9%A2%91%E6%AE%B5/_blank)900MHz的频段则有部分用于[GSM](https://baike.baidu.com/item/GSM" \t "https://baike.baidu.com/item/ISM%E9%A2%91%E6%AE%B5/_blank)通信。而2.4G[Hz](https://baike.baidu.com/item/Hz" \t "https://baike.baidu.com/item/ISM%E9%A2%91%E6%AE%B5/_blank)为各国共同的ISM频段。因此[无线局域网](https://baike.baidu.com/item/%E6%97%A0%E7%BA%BF%E5%B1%80%E5%9F%9F%E7%BD%91" \t "https://baike.baidu.com/item/ISM%E9%A2%91%E6%AE%B5/_blank)（IEEE 802.11b/IEEE 802.11g），[蓝牙](https://baike.baidu.com/item/%E8%93%9D%E7%89%99" \t "https://baike.baidu.com/item/ISM%E9%A2%91%E6%AE%B5/_blank)，[ZigBee](https://baike.baidu.com/item/ZigBee" \t "https://baike.baidu.com/item/ISM%E9%A2%91%E6%AE%B5/_blank)等无线网络，均可工作在2.4GHz频段上。

1. 蓝牙

蓝牙（ Bluetooth）：是一种无线技术标准，可实现固定设备、移动设备和楼宇个人域网之间的短距离数据交换（使用2.4—2.485GHz的ISM波段的UHF无线电波）。蓝牙技术最初由电信巨头爱立信公司于1994年创制，当时是作为RS232数据线的替代方案。蓝牙可连接多个设备，克服了数据同步的难题。

1. 条形码

条形码(barcode)是将宽度不等的多个黑条和空白，按照一定的编码规则排列，用以表达一组信息的图形标识符。常见的条形码是由反射率相差很大的黑条（简称条）和白条（简称空）排成的平行线图案。条形码可以标出物品的生产国、制造厂家、商品名称、生产日期、图书分类号、邮件起止地点、类别、日期等许多信息，因而在商品流通、图书管理、邮政管理、银行系统等许多领域都得到广泛的应用。

1. 二维码

二维条码/二维码（2-dimensional bar code）是用某种特定的几何图形按一定规律在平面（二维方向上）分布的黑白相间的图形记录数据符号信息的；在代码编制上巧妙地利用构成计算机内部逻辑基础的“0”、“1”比特流的概念，使用若干个与二进制相对应的几何形体来表示文字数值信息，通过图象输入设备或光电扫描设备自动识读以实现信息自动处理：它具有条码技术的一些共性：每种码制有其特定的字符集；每个字符占有一定的宽度；具有一定的校验功能等。同时还具有对不同行的信息自动识别功能、及处理图形旋转变化点

1. IETF

国际互联网工程任务组（The Internet Engineering Task Force，简称 IETF）是一个公开性质的大型民间国际团体，汇集了与互联网架构和互联网顺利运作相关的网络设计者、运营者、[投资人](https://baike.baidu.com/item/%E6%8A%95%E8%B5%84%E4%BA%BA" \t "https://baike.baidu.com/item/%E4%BA%92%E8%81%94%E7%BD%91%E5%B7%A5%E7%A8%8B%E4%BB%BB%E5%8A%A1%E7%BB%84/_blank)和研究人员，并欢迎所有对此行业感兴趣的人士参与。

IETF的主要任务是负责互联网相关技术标准的研发和制定

1. RFC

Request For Comments（RFC），是一系列以编号排定的文件。文件收集了有关互联网相关信息，以及UNIX和互联网社区的[软件](https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6/12053" \t "https://baike.baidu.com/item/RFC/_blank)文件。基本的因特网通讯协定都有在RFC文件内详细说明。RFC文件还在标准内额外加入了许多的论题，例如对于因特网新开发的协定及发展中所有的记录。因此几乎所有的因特网标准都收录在RFC文件之中。

作为标准的RFC又分为几种，第一种是提议性的，就是说建议采用这个作为一个方案摆出来，Draft是已经有一部分在用了，希望被采用为正式的标准，还有一种就是完全被认可的标准，这种是大家都在用，而且是不应该改变的。

1. ITU-T

ITU-T的中文名称是[国际电信联盟](https://baike.baidu.com/item/%E5%9B%BD%E9%99%85%E7%94%B5%E4%BF%A1%E8%81%94%E7%9B%9F" \t "https://baike.baidu.com/item/_blank)电信标准分局(ITU-T for ITU Telecommunication Standardization Sector), 它是国际电信联盟管理下的专门制定电信标准的分支机构。

由ITU-T制定的国际标准通常被称为建议（Recommendations）。由于ITU-T是ITU的一部分，而ITU是联合国下属的组织，所以由该组织提出的国际标准比起其它的组织提出的类似的技术规范更正式一些。

1. VoIP

voice over internet protocol

这种将语音转化为IP数据包，部分或全部基于IP网络传输的技术就是VoIP （Voice over IP，IP承载语音）技术。

目录

声明：词条人人可编辑，创建、修改和认证均免费

详情

一分钟了解voip

6434 50"

voip

科普中国

本词条由“科普中国”科学百科词条编写与应用工作项目审核

贡献者鄢志丹详情

基于IP的语音传输（英语：Voice over Internet Protocol，缩写为VoIP）是一种语音通话技术，经由网际协议（IP）来达成语音通话与多媒体会议，也就是经由互联网来进行通信。其他非正式的名称有IP电话（IP telephony）、互联网电话（Internet telephony）、宽带电话（broadband telephony）以及宽带电话服务（broadband phone service）。

VoIP可用于包括VoIP电话、智能手机、个人计算机在内的诸多互联网接入设备，通过蜂窝网络、Wi-Fi进行通话及发送短信。

中文名

网络电话

外文名

Voice over Internet Protocol

简称

VoIP

作用

将模拟信号（Voice）数字化

原理

很多朋友都喜欢使用网络聊天工具来进行语音聊天，这种语音并不是通过电信运营商的传统电话网络进行传输，而是通过互联网进行传输。这种将语音转化为IP数据包，部分或全部基于IP网络传输的技术就是VoIP （Voice over IP，IP承载语音）技术。

VoIP的基本原理是通过语音的压缩算法对语音数据编码进行压缩处理，然后把这些语音数据按 TCP/IP 标准进行打包，经过 IP 网络把数据包送至接收地，再把这些语音数据包串起来，经过解压处理后，恢复成原来的语音信号，从而达到由互联网传送语音的目的。

1. VOD

Voice on demand

视频点播

1. SIP

SIP（Session Initiation Protocol，会话初始协议）是由IETF（Internet Engineering Task Force，因特网工程任务组）制定的多媒体通信协议。它是一个基于文本的应用层控制协议，用于创建、修改和释放一个或多个参与者的会话。广泛应用于CS（Circuit Switched，电路交换）、[NGN](https://baike.baidu.com/item/NGN/718175" \t "https://baike.baidu.com/item/SIP/_blank)（Next Generation Network，下一代网络）以及[IMS](https://baike.baidu.com/item/IMS/12003646" \t "https://baike.baidu.com/item/SIP/_blank)（IP Multimedia Subsystem，IP多媒体子系统）的网络中，可以支持并应用于语音、视频、数据等多媒体业务，同时也可以应用于Presence（呈现）、Instant Message（即时消息）等特色业务。可以说，有IP网络的地方就有SIP协议的存在。 [1-2]

SIP是类似于[HTTP](https://baike.baidu.com/item/HTTP/243074" \t "https://baike.baidu.com/item/SIP/_blank)。SIP可以减少应用特别是高级应用的开发时间。由于基于IP协议的SIP利用了IP网络，固定网运营商也会逐渐认识到SIP技术对于他们的深远意义。

1. H323
2. SS7

SS7是一种数字信令系统，适用于无线和有线的公共交换[电话网](https://baike.baidu.com/item/%E7%94%B5%E8%AF%9D%E7%BD%91/1493895" \t "https://baike.baidu.com/item/SS7/_blank)。这个标准定义了通过交换数字信令来建立呼叫、寻找路由和控制网络元素的过程和协议。它的功能十分全面，主要特征如下：

1、基本的呼叫建立、管理和终止过程。

2、个人通信服务（PCS）、无线漫游和移动用户认证等无线业务。

3、市话号码移植业务。

4、[免费电话](https://baike.baidu.com/item/%E5%85%8D%E8%B4%B9%E7%94%B5%E8%AF%9D/81505" \t "https://baike.baidu.com/item/SS7/_blank)（800）和长途线路服务（900）.

5、各种[增值服务](https://baike.baidu.com/item/%E5%A2%9E%E5%80%BC%E6%9C%8D%E5%8A%A1/9604525" \t "https://baike.baidu.com/item/SS7/_blank)，例如[呼叫转移](https://baike.baidu.com/item/%E5%91%BC%E5%8F%AB%E8%BD%AC%E7%A7%BB/3735384" \t "https://baike.baidu.com/item/SS7/_blank)、来电显示和[三方通话](https://baike.baidu.com/item/%E4%B8%89%E6%96%B9%E9%80%9A%E8%AF%9D/3735081" \t "https://baike.baidu.com/item/SS7/_blank)等。

6、提供有效、安全的全球通信。

SS7 的目的是提供了一个电话网络信令的国际标准。

1. RTP/RTCP/RTSP

RTP: Real-time Transport Protocol,实时传输协议，一般用于多媒体数据的传输。

RTCP: RTP Control Protocol，实时传输控制协议，同RTP一起用于数据传输的监视，控制功能。

RTSP: Real Time Streaming Protocol,实时流协议，用于多媒体数据流的控制，如播放，暂停等。

RTP/RTCP相对于底层传输层，和RTSP，SIP等上层协议一起可以实现视频会议，视频直播等应用。

1. 2G/2.5G/3G/4G/5G
2. SSL

SSL(Secure Sockets Layer [安全套接层](https://baike.baidu.com/item/%E5%AE%89%E5%85%A8%E5%A5%97%E6%8E%A5%E5%B1%82" \t "https://baike.baidu.com/item/ssl/_blank)),及其继任者[传输层安全](https://baike.baidu.com/item/%E4%BC%A0%E8%BE%93%E5%B1%82%E5%AE%89%E5%85%A8" \t "https://baike.baidu.com/item/ssl/_blank)（Transport Layer Security，TLS）是为[网络通信](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E9%80%9A%E4%BF%A1/9636548" \t "https://baike.baidu.com/item/ssl/_blank)提供安全及[数据完整性](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%AE%8C%E6%95%B4%E6%80%A7/110071" \t "https://baike.baidu.com/item/ssl/_blank)的一种安全协议。TLS与SSL在[传输层](https://baike.baidu.com/item/%E4%BC%A0%E8%BE%93%E5%B1%82/4329536" \t "https://baike.baidu.com/item/ssl/_blank)对网络连接进行加密。

SSL协议位于[TCP/IP协议](https://baike.baidu.com/item/TCP/IP%E5%8D%8F%E8%AE%AE" \t "https://baike.baidu.com/item/ssl/_blank)与各种[应用层](https://baike.baidu.com/item/%E5%BA%94%E7%94%A8%E5%B1%82" \t "https://baike.baidu.com/item/ssl/_blank)协议之间，为[数据通讯](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E9%80%9A%E8%AE%AF" \t "https://baike.baidu.com/item/ssl/_blank)提供安全支持。

SL协议可分为两层： SSL记录协议（SSL Record Protocol）：它建立在可靠的[传输协议](https://baike.baidu.com/item/%E4%BC%A0%E8%BE%93%E5%8D%8F%E8%AE%AE" \t "https://baike.baidu.com/item/ssl/_blank)（如TCP）之上，为高层协议提供[数据封装](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%B0%81%E8%A3%85" \t "https://baike.baidu.com/item/ssl/_blank)、压缩、加密等基本功能的支持。 SSL[握手协议](https://baike.baidu.com/item/%E6%8F%A1%E6%89%8B%E5%8D%8F%E8%AE%AE" \t "https://baike.baidu.com/item/ssl/_blank)（SSL Handshake Protocol）：它建立在SSL记录协议之上，用于在实际的数据传输开始前，通讯双方进行[身份认证](https://baike.baidu.com/item/%E8%BA%AB%E4%BB%BD%E8%AE%A4%E8%AF%81" \t "https://baike.baidu.com/item/ssl/_blank)、协商[加密算法](https://baike.baidu.com/item/%E5%8A%A0%E5%AF%86%E7%AE%97%E6%B3%95" \t "https://baike.baidu.com/item/ssl/_blank)、交换加密[密钥](https://baike.baidu.com/item/%E5%AF%86%E9%92%A5" \t "https://baike.baidu.com/item/ssl/_blank)等。

1. SSH

SSH 为 [Secure Shell](https://baike.baidu.com/item/Secure Shell" \t "https://baike.baidu.com/item/ssh/_blank) 的缩写，由 IETF 的网络小组（Network Working Group）所制定；SSH 为建立在应用层基础上的安全协议。SSH 是目前较可靠，专为[远程登录](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B%E7%99%BB%E5%BD%95/1071998" \t "https://baike.baidu.com/item/ssh/_blank)会话和其他网络服务提供安全性的协议。利用 SSH 协议可以有效防止远程管理过程中的信息泄露问题。SSH最初是UNIX系统上的一个程序，后来又迅速扩展到其他操作平台。SSH在正确使用时可弥补网络中的漏洞。SSH客户端适用于多种平台。几乎所有UNIX平台—包括[HP-UX](https://baike.baidu.com/item/HP-UX" \t "https://baike.baidu.com/item/ssh/_blank)、[Linux](https://baike.baidu.com/item/Linux" \t "https://baike.baidu.com/item/ssh/_blank)、[AIX](https://baike.baidu.com/item/AIX" \t "https://baike.baidu.com/item/ssh/_blank)、[Solaris](https://baike.baidu.com/item/Solaris/3517" \t "https://baike.baidu.com/item/ssh/_blank)、[Digital](https://baike.baidu.com/item/Digital" \t "https://baike.baidu.com/item/ssh/_blank) [UNIX](https://baike.baidu.com/item/UNIX" \t "https://baike.baidu.com/item/ssh/_blank)、[Irix](https://baike.baidu.com/item/Irix" \t "https://baike.baidu.com/item/ssh/_blank)，以及其他平台，都可运行SSH。

从客户端来看，SSH提供两种级别的安全验证。

**第一种级别（基于口令的安全验证）**

只要你知道自己帐号和口令，就可以登录到远程主机。所有传输的数据都会被加密，但是不能保证你正在连接的服务器就是你想连接的[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "https://baike.baidu.com/item/ssh/_blank)。可能会有别的服务器在冒充真正的服务器，也就是受到“中间人”这种方式的攻击。

**第二种级别（基于密匙的安全验证）**

需要依靠[密匙](https://baike.baidu.com/item/%E5%AF%86%E5%8C%99" \t "https://baike.baidu.com/item/ssh/_blank)，也就是你必须为自己创建一对密匙，并把公用密匙放在需要访问的服务器上。如果你要连接到SSH服务器上，客户端软件就会向服务器发出请求，请求用你的密匙进行安全验证。服务器收到请求之后，先在该服务器上你的主目录下寻找你的公用密匙，然后把它和你发送过来的公用密匙进行比较。如果两个密匙一致，服务器就用公用密匙加密“质询”（challenge）并把它发送给客户端软件。客户端软件收到“质询”之后就可以用你的私人密匙解密再把它发送给服务器。

用这种方式，你必须知道自己密匙的[口令](https://baike.baidu.com/item/%E5%8F%A3%E4%BB%A4" \t "https://baike.baidu.com/item/ssh/_blank)。但是，与第一种级别相比，第二种级别不需要在网络上传送口令。

第二种级别不仅加密所有传送的数据，而且“中间人”这种攻击方式也是不可能的（因为他没有你的私人密匙）。但是整个登录的过程可能需要10秒 [2]  。

SSH 主要由三部分组成：

**传输层协议 [SSH-TRANS]**

提供了服务器认证，保密性及完整性。此外它有时还提供压缩功能。 SSH-TRANS 通常运行在[TCP/IP](https://baike.baidu.com/item/TCP/IP" \t "https://baike.baidu.com/item/ssh/_blank)连接上，也可能用于其它可靠数据流上。 SSH-TRANS 提供了强力的加密技术、密码主机认证及完整性保护。该协议中的认证基于主机，并且该协议不执行[用户认证](https://baike.baidu.com/item/%E7%94%A8%E6%88%B7%E8%AE%A4%E8%AF%81" \t "https://baike.baidu.com/item/ssh/_blank)。更高层的用户认证协议可以设计为在此协议之上。

**用户认证协议 [SSH-USERAUTH]**

用于向服务器提供客户端用户鉴别功能。它运行在[传输层](https://baike.baidu.com/item/%E4%BC%A0%E8%BE%93%E5%B1%82" \t "https://baike.baidu.com/item/ssh/_blank)协议 SSH-TRANS 上面。当SSH-USERAUTH 开始后，它从低层协议那里接收会话[标识符](https://baike.baidu.com/item/%E6%A0%87%E8%AF%86%E7%AC%A6" \t "https://baike.baidu.com/item/ssh/_blank)（从第一次[密钥](https://baike.baidu.com/item/%E5%AF%86%E9%92%A5" \t "https://baike.baidu.com/item/ssh/_blank)交换中的交换哈希H ）。会话标识符唯一标识此会话并且适用于标记以证明私钥的所有权。 SSH-USERAUTH 也需要知道低层协议是否提供保密性保护。

**连接协议 [SSH-CONNECT]**

将多个加密隧道分成逻辑通道。它运行在用户认证协议上。它提供了交互式登录话路、远程命令执行、转发 TCP/IP 连接和转发 X11 连接。

1. VNC

VNC (Virtual Network Console)是[虚拟网络](https://baike.baidu.com/item/%E8%99%9A%E6%8B%9F%E7%BD%91%E7%BB%9C" \t "https://baike.baidu.com/item/_blank)控制台的缩写。

VNC基本上是由两部分组成：一部分是客户端的应用程序(vncviewer)；另外一部分是服务器端的应用程序([vncserver](https://baike.baidu.com/item/vncserver" \t "https://baike.baidu.com/item/_blank))。VNC的基本运行原理和一些Windows下的[远程控制软件](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B%E6%8E%A7%E5%88%B6%E8%BD%AF%E4%BB%B6" \t "https://baike.baidu.com/item/_blank)很相像。VNC的服务器端应用程序在UNIX和Linux操作系统中适应性很强，[图形用户界面](https://baike.baidu.com/item/%E5%9B%BE%E5%BD%A2%E7%94%A8%E6%88%B7%E7%95%8C%E9%9D%A2" \t "https://baike.baidu.com/item/_blank)十分友好，看上去和Windows下的[软件界面](https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6%E7%95%8C%E9%9D%A2" \t "https://baike.baidu.com/item/_blank)也很类似。在任何安装了客户端的应用程序(vncviewer)的Linux平台的计算机都能十分方便地和安装了服务器端的应用程序(vncserver)的计算机相互连接。另外，服务器端 (vncserver)还内建了Java Web接口，这样用户通过服务器端对其他计算机的操作就能通过[Netscape](https://baike.baidu.com/item/Netscape" \t "https://baike.baidu.com/item/_blank)显示出来了，这样的操作过程和显示方式比较直观方便。

1. RDP

远程桌面协议（RDP, Remote Desktop Protocol）是一个多通道的协议，让客户端连上提供微软终端机服务的电脑（服务器端或称“远程电脑”）。大部分的Windows都有客户端所需软件。其他操作系统也有这些客户端软件，例如Linux、FreeBSD、Mac OS X。服务端电脑方面，则听取送到TCP3389端口的数据。

1. Shadowsocks

托管在Github的知名代理项目Shadowsocks

1. MQ

消息队列（MQ）是一种应用程序对应用程序的通信方法。应用程序通过写和检索出入列队的针对应用程序的数据（消息）来通信，而无需专用连接来链接它们。消息传递指的是程序之间通过在消息中发送数据进行通信，而不是通过直接调用彼此来通信，直接调用通常是用于诸如远程过程调用的技术。排队指的是应用程序通过队列来通信。队列的使用除去了接收和发送应用程序同时执行的要求。

1. DLNA

DLNA的全称是digital living network alliance(数字生活网络联盟)， 其宗旨是Enjoy your music, photos and videos, anywhere anytime， DLNA(Digital Living Network Alliance) 由索尼、英特尔、微软等发起成立、旨在解决个人电脑，消费电器，移动设备在内的无线网络和有线网络的互联互通，使得数字媒体和内容服务的无限制的共享和增长成为可能，目前成员公司已达280多家。

1. Docker

Docker 是一个开源的应用容器引擎，让开发者可以打包他们的应用以及依赖包到一个可移植的镜像中，然后发布到任何流行的 Linux或Windows 机器上，也可以实现虚拟化。容器是完全使用沙箱机制，相互之间不会有任何接口。

补充：

1.RADIUS协议

由Livingston公司提出的

起先的目的是为拨号用户进行认证和计费

后经过多次改进成为了通用的认证计费协议

RADIUS服务器使用UDP协议进行通信。

采用UDP的基本考虑是因为NAS和RADIUS服务器大多在同一个局域网中，使用UDP更加方便快捷。

RADIUS服务器的1645(1812)端口负责认证，1646(1813)端口负责计费工作。

1. WEP

三分钟内破解WEP保护的无线网

WEP 是1999年9月通过的 IEEE 802.11 标准的一部分。WEP 的设计是要提供和传统有线的局域网路相当的机密性。

无线局域网中的WEP加密机制并不能够为无线用户提供足够的安全保护，密码分析已经找出 WEP 好几个弱点。

对 WEP 安全问题的解法是换到 WPA 或 WPA2，不论哪个都比 WEP 安全。

1. WAP

WPA 和 WPA2是WEP的升级协议，实现了 IEEE 802.11i 标准的大部分，是在 802.11i 完备之前替代 WEP 的过渡方案。

WPA 的设计可以用在所有的无线网卡上，但未必能用在第一代的无线点上。

WPA2 实作了完整的标准，但不能用在某些古老的网卡上。

4.

WPA2 实现了 802.11i 的强制性元素，特别是 Michael 算法由彻底安全的 CCMP 认证码所取代。

而 RC4 也被 AES 取代。