**滑动窗口协议（2008）：**也称为回退N步协议（Go-Back-N，GBN）中，允许发送方发送多个分组（当有多个分组可用时）而不需等待确认，但它受限于在流水线 中为未确认的分组数不能超过某个最大允许数N。滑动窗口协议是TCP使用的一种流量控制方法，此协议能够加速数据的传输。

只有在接收窗口向前滑动时（与此同时也发送了确认），发送窗口才有可能向前滑动。

收发两端的窗口按照以上规律不断地向前滑动，因此这种协议又称为滑动窗口协议。

扩展：

　　当发送窗口和接收窗口的大小都等于1时，就是停止等待协议。

　　当发送窗口大于1，接收窗口等于1时，就是回退N步协议。

　　当发送窗口和接收窗口的大小均大于1时，就是选择重发协议。

协议中规定，对于窗口内未经确认的分组需要重传。这种分组的数量最多可以等于发送窗口的大小，即滑动窗口的大小n减去1（因为发送窗口不可能大于（n-1），起码接收窗口要大于等于1）。

**慢启动算法：** 每个发送方位维护两个窗口：一个是接收方准许的窗口，第二个是拥塞窗口。最终允许发送的字节数以接受窗口和发送窗口的最小值为准。因此有效窗口是发送方认为没有问题的窗口和接收方认为没有问题的窗口中最小的那个。

事实上拥塞控制中还定义有第三个参数：阈值，初始值为64KB。

慢启动过程：

（1）当一个链接建立起来以后，发送方的拥塞窗口初始化为该链接上当前使用的最大数据段值。然后发送一个最大数据段，如果该数据段在定时器过期之前确认，那么拥塞窗口变成2。以后拥塞窗口按指数级别增长。

（2）当拥塞窗口增长到阈值的时候，指数增长停滞，从这个点开始，每次成功的传输，都会使拥塞窗口线程增长，（即每次只增长一个最大数据段）。

（3）当超时发生时，阈值被设置为当前拥塞窗口的一半 ，而拥塞窗口被充值为一个最大数据段，之后使用相同的慢启动算法来决定网络的处理能力。

**CSMA/CD （Carrier Sense Multiple Access / Collision Detection） 载波监听多点接入、冲突检测** （**2008**）

CSMA/CD应用在 OSI 的第二层数据链路层。它的工作原理是: 发送数据前 先侦听信道是否空闲 ,若空闲，则立即发送数据。若信道忙碌，则等待一段时间至信道中的信息传输结束后再发送数据；若在上一段信息发送结束后，同时有两个或两个以上的节点都提出发送请求，则判定为冲突。若侦听到冲突,则立即停止发送数据，等待一段随机时间,再重新尝试。其原理简单总结为：先听后发，边发边听，冲突停发，随机延迟后重发

**IEEE802.5令牌环网（2006）：**令牌环网由IBM公司由1969年推出，后被列为IEEE802.5标准协议，它在物理和逻辑上均基于环结构，传输速率可达到4到16Mbps.令牌环网使用双绞线或者同轴电缆作为传输介质，并将于各个站相连接的接口逐个链接起来组成一个闭合的环路，环上的每个环接口均有两种工作方式：发送方式和收转方式。该网络通过一个很小的自由令牌在环上单向循环来控制和管理传输介质的使用，以保证整个环路最多只有一个站处于发送方式，其他站处于收转方式。

**ICMP(2006)：**Internet Control Message Protocol,它是TCP/IP协议族的一个子协议，用于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，主机是否到达，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，但是对于用户的数据的传递起着重要的作用。

**路由协议（RIP）（2005）**：是一种分布式的基于距离向量的路由选择协议，是因特网标准协议，其最大优点是简单。但RIP只能允许一条路径包含15个路由器。因此只适用于小型互联网。

**虚拟局域网Vlan(2005)**:是指在交换局域网的基础上，采用网络管理软件构建的可跨越不同网段，不同网络的端到端的逻辑网络。一个VLAN组成一个逻辑子网，即一个逻辑广播域，它可以覆盖多个网络设备，允许处于不同的地理位置的网络用户加入一个逻辑子网中。

VLAN是建立在物理网络基础上的一种逻辑子网，因此建立VLAN需要相应的支持VLAN技术的网络设备。当网络中的不同VLAN间进行相互通信时，需要路由的支持，这时就需要增加路由设备-要实现路由功能，即可以采用路由器，也可以采用三层交换机来完成。

使用VLAN具有以下优点：1）控制广播风暴2）提高网络整体安全性3）网络管理简单，只管

**防火墙（2005）：**防火墙是一种网络安全的防范措施，其工作方式是将内联网络与因特网之前或与其他外联网之间互相间隔，通过访问控制的方式来保护内联网络。设置防火墙目的是为了在内联网和外联网之间设立唯一的通道，简化网络的安全管理。

**ARP协议（2004）**

**数字签名（2004）**

**OSPF（2004）**

**持续和非持续CSMA（2003）**

**多模光纤和单模光纤（2003）**

**自治系统（2008）**

**慢启动（2008）**

**滑动窗口协议（2008）**

**CSMA/CD**（**2008**）

**IEEE802.5令牌环网（2006）**

**ICMP(2006)**

**虚拟局域网Vlan(2005)**

**防火墙（2005）**

**子网掩码（2009）**

**拥塞（2009）**

**网络地址转化（2010）**

**ARP协议（2010）**

**MTU（2011）**

**生成树算法（2011）**

**路由协议RIP（2012）**

**VPN（2012）**

**VLAN（2013）**

**CIDR（2013）**

**慢开始（2014）**

**时延带宽积（2014）**

**1.ADSL (Asymmetric Digital Subscriber Line) 非对称数字用户线**  释义：非对称数字用户线路，亦可称作非对称数字用户环路。是一种新的数据传输方式。它因为上行和下行带宽不对称，因此称为非对称数字用户线环路。

**2.AH（Authentication Header） 鉴别首部** 释义：AH(Authentication Header)认证头协议用以保证数据包的完整性和真实性，防止黑客截断数据包或向网络中插入伪造的数据包。考虑到计算效率，AH没有采用数字签名而是采用了安全哈希算法来对数据包进行保护。AH没有对用户数据进行加密。当需要身份验证而不需要机密性的时候，使用AH协议时最好的选择。

**3.API （Application Programming Interface） 应用编程接口**  释义：API（Application Programming Interface,应用程序编程接口）是一些预先定义的函数，目的是提供应用程序与开发人员基于某软件或硬件的以访问一组例程的能力，而又无需访问源码，或理解内部工作机制的细节。

**4.ARP （Address Research Protocol） 地址解析协议** 释义：ARP(Address Resolution Protocol，地址解析协议)是获取物理地址的一个TCP/IP协议。某节点的IP地址的ARP请求被广播到网络上后，这个节点会收到确认 其物理地址的应答，这样的数据包才能被传送出去。RARP(逆向ARP)经常在无盘工作站上使用，以获得它的逻辑IP地址。

**5.AS （Autonomous System） 自治系统** 释义：一个自治系统就是处于一个管理机构控制之下的路由器和网络群组。它可以是一个路由器直接连接到一个LAN上，同时也连到Internet上；它可以是一个由企业骨干网互连的多个局域网。在一个自治系统中的所有路由器必须相互连接，运行相同的路由协议，同时分配同一个自治系统编号。

**6.BER （Basic Encoding Rule） 基本编码规则**

**释义：基本编码规则(标准规格用于基本ASN.1编码资料**

**7.BGP （Border Gateway Protocol） 边界网关协议**

**释义：**边界网关协议（BGP）是运行于 TCP 上的一种自治系统的路由协议。 BGP 是唯一一个用来处理像因特网大小的网络的协议，也是唯一能够妥善处理好不相关路由域间的多路连接的协议。 BGP 构建在 EGP 的经验之上。 BGP 系统的主要功能是和其他的 BGP 系统交换网络可达信息。网络可达信息包括列出的自治系统（AS）的信息。这些信息有效地构造了 AS 互联的拓朴图并由此清除了路由环路，同时在 AS 级别上可实施策略决策。

**28.IPsec（IP security） IP安全协议**  释义：保护 IP 数据包的内容。 通过数据包筛选及受信任通讯的实施来防御网络攻击。 这两个目标都是通过使用基于加密的保护服务、安全协议与动态密钥管理来实现的。这个基础为专用网络计算机、域、站点、远程站点、Extranet 和拨号用户之间的通信提供了既有力又灵活的保护。它甚至可以用来阻碍特定通讯类型的接收和发送。

**29.ISP (Internet Service Provider) 因特网服务提供者**

**释义：互联网服务提供商，即向广大用户综合提供互联网接入业务、信息业务、和增值业务的电信运营商。**

**30.KDC（Key Distribution Center） 密匙分配中心**

**释义：密码学中的密钥分发中心（ KDC ）是密钥体系的一部分，旨在减少密钥体制所固有的交换密钥时所面临的风险。 KDC应用在这样的系统中：系统内一些用户能够使用某些服务，而其他人不能使用那些服务。DC在kerberos中通常提供两种服务： 1.Authentication Service (AS)：认证服务 2.Ticket-Granting Service (TGS)：授予票据服务**

**31..LAN（Location Area Network） 局域网 释义：局域网（Local Area Network，LAN）是指在某一区域内由多台计算机互联成的计算机组。一般是方圆几千米以内。局域网可以实现文件管理、应用软件共享、打印机共享、工作组内的日程安排、电子邮件和传真通信服务等功能。局域网是封闭型的，可以由办公室内的两台计算机组成，也可以由一个公司内的上千台计算机组成。**

**32.MAC（Medium Access Control） 媒体接入控制**

释义：它定义它定义了数据包怎样在介质上进行传输。在共享同一个带宽的链路中，对连接介质的访问是“先来先服务”的。物理寻址在此处被定义，逻辑拓扑（信号通过物理拓扑的路径）也在此处被定义。线路控制、出错通知（不纠正）、帧的传递顺序和可选择的流量控制也在这一子层实现。怎样在介质上进行传输。在共享同一个带宽的链路中，对连接介质的访问是“先来先服务”的。物理寻址在此处被定义，逻辑拓扑（信号通过物理拓扑的路径）也在此处被定义。线路控制、出错通知（不纠正）、帧的传递顺序和可选择的流量控制也在这一子层实现。

**33.MD（Message Digest） 报文摘要** 释义：报文摘要是指单向哈希函数算法将任意长度的输入报文经计算得出固定位的输出称为报文摘要.所谓单向是指该算法是不可逆的找出具有同一报文摘要的两个不同报文是很困难的。

**34.MIB（Management Information Base） 管理信息库**

释义：所谓“管理信息”就是指在因特网的网管框架中被管对象的集合。被管对象必须维持可供管理程序读写的若干控制和状态信息。这些被管对象构成了一个虚拟的信息存储器，所以才称为管理信息库 MIB。

**35.MIME（Multipurpose Internet Mail Extensions）**

**通用因特网邮件扩充 释义：多用途互联网邮件扩展类型就是设定某种扩展名的文件用一种应用程序来打开的方式类型，当该扩展名文件被访问的时候，浏览器会自动使用指定应用程序来打开。多用于指定一些客户端自定义的文件名，以及一些媒体文件打开方式。**

**36.MPLS（MultiProtocol Label Switching ） 多协议标记交换**

**释义：多协议标签交换（MPLS）是一种用于快速数据包交换和路由的体系，它为网络数据流量提供了目标、路由、转发和交换等能力。更特殊的是，它具有管理各种不同形式通信流的机制。**

**37.MRU（Maximum Receive Unit） 最大接收单元 释义：略**

**38.NAP（Network Access Point） 网络接入点 释义：NAP是因特网的路由选择层次体系中的通信交换点。每个网络接入点都由一个共享交换系统或者局域网组成，用来交换业务量。通达因特网主干线的点。ISP互相连接的点。NAP可用作主要业务提供者的数据互换点。1999年初NAP和城域交换局（MAE）被统称为公共因特网交换点（IXP）**

**39.NCP（Network Control Protocol） 网络控制协议 释义：NCP指Network Control Protocol 网络控制协议（NCP）管理对 NetWare 服务器资源的访问。NCP 向 NetWare 文件共享协议（即NFSP：NetWare File Sharing Protocol）发送过程调用消息，处理 NetWare 文件和打印资源请求。 NCP 是用于 NetWare 服务器和客户机之间传输信息的主要协议。 NCP 主要负责处理登入请求以及其它文件系统和打印系统请求。NCP 是一种基于客户机/服务器的 LAN 协议。工作站建立 NCP 请求并通过 IPX 在网络上发送这些请求服务。服务器端负责接收、拆包（unpacked）并解读 NCP 请求。 NCP 服务包括：文件访问、文件锁定（file locking）、安全性、资源分配跟踪（tracking of resource allocation）、事件通知（event notification）、与其它服务器同步、连接和通信、打印服务，以及队列和网络管理。**

**40.NFS（Network File System） 网络文件系统**

**释义：NFS，是Network File System的简写。网络文件系统是FreeBSD支持的文件系统中的一种，也被称为NFS. NFS允许一个系统在网络上与他人共享目录和文件。通过使用NFS，用户和程序可以像访问本地文件一样访问远端系统上的文件。**

**41.NIC（Network Interface Card） 网络接口卡 网卡 释义：网卡是局域网中最基本的部件之一，它是连接计算机与网络的硬件设备。无论是双绞线连接、同轴电缆连接还是光纤连接，都必须借助于网卡才能实现数据的通信。它的主要技术参数为带宽、总线方式、电气接口方式等。它的基本功能为：从并行到串行的数据转换，包的装配和拆装，网络存取控制，数据缓存和网络信号。目前主要是8位和16位网卡。**

**42.OSPF （Open Shortest Path First） 开放最短路径优先 释义：OSPF(Open Shortest Path First开放式最短路径优先）是一个内部网关协议(Interior Gateway Protocol，简称IGP），用于在单一自治系统（autonomous system,AS）内决策路由。是对链路状态路由协议的一种实现，隶属内部网关协议（IGP），故运作于自治系统内部。**

**43.P2P（Peer-to-Peer） 对等方式 释义：对等网络又称工作组，网上各台计算机有相同的功能，无主从之分，一台计算机都是既可作为服务器，设定共享资源供网络中其他计算机所使用，又可以作为工作站，没有专用的服务器，也没有专用的工作站。对等网络是小型局域网常用的组网方式。**

**44.PDU（Protocol Data Unit） 协议数据单元 释义：在分层网络结构，例如在开放式系统互联(OSI)模型中，在传输系统的每一层都将建立协议数据单元(PDU)。PDU包含来自上层的信息，以及当前层的实体附加的信息。然后，这个PDU被传送到下一较低的层。物理层实际以一种编帧的位流形式传输这些PDU，但是由协议栈的较高层建造这些PDU。接收系统自下而上传送这些分组通过协议栈，并在协议栈的每一层分离出PDU中的相关信息。**

**45.PING （Packet Interface Groper） 分组网间探测 ICMP的一种应用 释义：于检测网络通与不通，也叫时延，其值越大，速度越慢。用于测试网络连接量的程序。Ping发送一个ICMP(Internet Control Messages Protocol）即因特网信报控制协议；回声请求消息给目的地并报告是否收到所**

**46.PK （public key） 公钥 公开密钥 释义：公钥是与私钥算法一起使用的密钥对的非秘密一半。公钥通常用于加密会话密钥、验证数字签名，或加密可以用相应的私钥解密的数据。公钥和私钥是通过一种算法得到的一个密钥对（即一个公钥和一个私钥）其中的一个向外界公开，称为公钥；另一个自己保留，称为私钥。通过这种算法得到的密钥对能保证在世界范围内是唯一的。使用这个密钥对的时候，如果用其中一个密钥加密一段数据，必须用另一个密钥解密。比如用公钥加密数据就必须用私钥解密，如果用私钥加密也必须用公钥解密，否则解密将不会成功。**

**47.RARP（Reverse Address Resolution Protocol） 逆地址解析协议 释义：反向地址转换协议（RARP：Reverse Address Resolution Protocol） 反向地址转换协议（RARP）允许局域网的物理机器从网关服务器的 ARP 表或者缓存上请求其 IP 地址。网络管理员在局域网网关路由器里创建一个表以映射物理地址（MAC）和与其对应的 IP 地址。当设置一台新的机器时，其 RARP 客户机程序需要向路由器上的 RARP 服务器请求相应的 IP 地址。假设在路由表中已经设置了一个记录，RARP 服务器将会返回 IP 地址给机器，此机器就会存储起来以便日后使用。 RARP 可以使用于以太网、光纤分布式数据接口及令牌环 LAN**

**48.RIP（Routing Information Protocol） 路由解析协议 释义：路由信息协议（RIP）是一种在网关与主机之间交换路由选择信息的标准。RIP 是一种内部网关协议。在国家性网络中如当前的因特网，拥有很多用于整个网络的路由选择协议。作为形成网络的每一个自治系统(AS)，都有属于自己的路由选择技术，不同的 AS 系统，路由选择技术也不同。**

**49.RPB (Reverse Path Broadcasting) 反向路径广播 释义：略**

**50..RTCP（Real-time Transfer Control Protocol） 实时传送控制协议 释义：配合RTP使用的协议 主要用于服务质量的监测与反馈，媒体之间的同步，以及多播组中成员的标志。**

**51.RTO（Retransmission Time-Out） 超时重传时间 释义：TCP超时重传机制(RTO：Retransmission Timeout) ，是TCP操作计时器的一种！ 为了防止数据报丢失,当TCP发送一个报文时,就启动重传计时器,有2种情况: 1.若在计时器超时之前收到了特定报文的确认,则撤消这个计时器; 2.特定数据报在计时器超时前没有收到确认,则重传该数据报,并把计时器复位 RTO的数值基于平滑的往返时间及其偏差,大多数使用下面的公式: 最初 -->初始值 在任意次测试后 -->RTO=SRTT+4\*DRTT**

**52.RTSP（Real-Time Streaming Protocol） 实施流式协议 释义：RTSP是为了给流式过程增加更多的功能而设计的协议。RTSP本身并不传送数据，而仅仅是媒体播放器能够控制多媒体流的传送。（有点像文件传送协议FTP有一个控制信道），因此RTSP又称为带外协议。**

**53.RTT（Round-Trip Time） 往返时间**

**释义：返延时(RTT)由三个部分决定：即链路的传播时间、末端系统的处理时间以及路由器的缓存中的排队和处理时间。其中，前面两个部分的值作为一个TCP连接相对固定，路由器的缓存中的排队和处理时间会随着整个网络拥塞程度的变化而变化。所以RTT的变化在一定程度上反映了网络拥塞程度的变化。**

**54.SA（Security Association） 安全关联 释义：SA是一种安全关联，SA 对两台计算机之间的策略协议进行编码，指定它们将使用哪些算法和什么样的密钥长度，以及实际的密钥本身。**

**55.SCTP (Stream Control Transmission Protocol) 流控制传输协议**

**释义：是IETF新定义的一个传输层transport layer协议（2000年）。是提供基于不可靠传输业务的协议之上的可靠的数据报传输协议。SCTP的设计用于通过IP网传输SCN窄带信令消息。流控制传输协议（Stream Control Transmission Protocol，SCTP）是一种可靠的传输协议，它在两个端点之间提供稳定、有序的数据传递服务（非常类似于 TCP），并且可以保护数据消息边界（例如 UDP）。然而，与 TCP 和 UDP 不同，SCTP 是通过多宿主（Multi-homing）和多流（Multi-streaming）功能提供这些收益的，这两种功能均可提高可用性**

**56.SIP（Session Initiation Protocol） 回话发起协议 释义：SIP(Session Initiation Protocol)是一个应用层的信令控制协议。用于创建、修改和释放一个或多个参与者的会话。这些会话可以是Internet多媒体会议[1]、IP电话或多媒体分发。会话的参与者可以通过组播（multicast）、网状单播（unicast）或两者的混合体进行通信。 使用 SIP，服务提供商可以随意选择标准组件。不论媒体内容和参与方数量，用户都可以查找和联系对方。SIP 对会话进行协商，以便所有参与方都能够就会话功能达成一致以及进行修改。它甚至可以添加、删除或转移用户。**

**57.SK （Secret Key） 秘钥 释义：略**

**58.SMI（Structure of Management Information） 管理信息结构 释义：管理信息结构SMI（structure of management information) 它是简单网络管理协议（SNMP）的一部分，指定了在 SNMP 的 MIB 中用于定义管理目标的规则。 SMI 是一种语言，是为了确保网络管理数据的语法和语义明确和无二义性而定义的语言。 它是定义被管理网络实体中特定数据的语言。 它定义了数据类型、对象模型，以及写入和修改管理信息的规则。**

**59.SMTP（Simple Mail Transfer Protocol） 简单邮件传送协议 释义：SMTP（Simple Mail Transfer Protocol）即简单邮件传输协议,它是一组用于由源地址到目的地址传送邮件的规则，由它来控制信件的中转方式。SMTP协议属于TCP/IP协议族，它帮助每台计算机在发送或中转信件时找到下一个目的地。通过SMTP协议所指定的服务器,就可以把E－mail寄到收信人的服务器上了，整个过程只要几分钟。SMTP服务器则是遵循SMTP协议的发送邮件服务器，用来发送或中转发出的电子邮件。**

**60.SNMP（Simple Network Management Protocol） 简单邮件传送协议 释义：简单网络管理协议（SNMP），由一组网络管理的标准组成，包含一个应用层协议（application layer protocol）、数据库模型（database schema）和一组资料物件。该协议能够支持网络管理系统，用以监测连接到网络上的设备是否有任何引起管理上关注的情况。该协议是互联网工程工作小组（IETF，Internet Engineering Task Force）定义的internet协议簇的一部分。**

**61.TCP（Transmission Control Protocol） 传输控制协议 释义：TCP是一种面向连接（连接导向）的、可靠的、基于字节流的传输层（Transport layer）通信协议，由IETF的RFC 793说明（specified）。TCP在IP报文的协议号是6。在简化的计算机网络OSI模型中，它完成第四层传输层所指定的功能，UDP是同一层内另一个重要的传输协议。**

**62.UA（User Agent） 用户代理 释义：略**

**63.UDP（User Datagram Protocol） 用户数据报协议 释义：UDP是OSI参考模型中一种无连接的传输层协议，它主要用于不要求分组顺序到达的传输中，分组传输顺序的检查与排序由应用层完成[1]，提供面向事务的简单不可靠信息传送服务。UDP 协议基本上是IP协议与上层协议的接口。UDP协议适用端口分别运行在同一台设备上的多个应用程序。**

**64.URL （Uniform Resources Locator） 统一资源定位符 释义：统一资源定位符（Uniform Resource Locator，缩写为URL）是对可以从互联网上得到的资源的位置和访问方法的一种简洁的表示，是互联网上标准资源的地址。互联网上的每个文件都有一个唯一的URL，它包含的信息指出文件的位置以及浏览器应该怎么处理它。**

**65.VLAN （Virtual LAN） 虚拟局域网**

**释义：VLAN（Virtual Local Area Network）的中文名为"虚拟局域网"。VLAN是一种将局域网设备从逻辑上划分成一个个网段，从而实现虚拟工作组的新兴数据交换技术。这一新兴技术主要应用于交换机和路由器中，但主流应用还是在交换机之中。但又不是所有交换机都具有此功能，只有VLAN协议的第二层以上交换机才具有此功能，这一点可以查看相应交换机的说明书即可得知。**

**66.VPN（Virtual Private Network） 虚拟专用网 释义：拟专用网络（Virtual Private Network，简称VPN）指的是在公用网络上建立专用网络的技术。其之所以称为虚拟网，主要是因为整个VPN网络的任意两个节点之间的连接并没有传统专网所需的端到端的物理链路，而是架构在公用网络服务商所提供的网络平台，如Internet、ATM（异步传输模式）、Frame Relay（帧中继）等之上的逻辑网络，用户数据在逻辑链路中传输。它涵盖了跨共享网络或公共网络的封装、加密和身份验证链接的专用网络的扩展。**

**67.WAN (Wide Area Network) 广域网 释义：广域网（WAN，Wide Area Network）也称远程网（long haul network ）。通常跨接很大的物理范围，所覆盖的范围从几十公里到几千公里，它能连接多个城市或国家，或横跨几个洲并能提供远距离通信，形成国际性的远程网络。**

**68.WLAN (Wireless Local Area Network) 虚拟专用网 释义：无线局域网络(Wireless Local Area Networks； WLAN)是相当便利的数据传输系统，它利用射频（Radio Frequency； RF）的技术，取代旧式碍手碍脚的双绞铜线（Coaxial）所构成的局域网络，使得无线局域网络能利用简单的存取架构让用户透过它，达到“信息随身化、便利走天下”的理想境界。**

**69.WWW （World Wide Web） 万维网 释义：WWW可以让Web客户端（常用浏览器）访问浏览Web服务器上的页面。 WWW提供丰富的文本和图形，音频，视频等多媒体信息，并将这些内容集合在一起，并提供导航功能，使得用户可以方便地在各个页面之间进行浏览。由于WWW内容丰富，浏览方便，目前已经成为互联网最重要的服务。**