深入的探讨点对点（ ）协议 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/250/2021_2022__E6_B7_B1_E5_85_A5_E7_9A_84_E6_c101_250987.htm 因为第2层隧道协议在很大程度上依靠PPP协议的各种特性，因此有必要对PPP协议进行深入的探讨。PPP协议主要是设计用来通过拨号或专线方式建立点对点连接发送数据。PPP协议将IP，IPX 和NETBEUI包封装在PP桢内通过点对点的链路发送。 PPP协议主要应用于连接拨号用户和NAS. PPP拨号会话过程可以分成4个不同的阶段。分别如下： 阶段1：创建PPP链路 PPP使用链路控制协议（LCP）创建，维护或终止一次物理连接。 在LCP阶段的初期，将对基本的通讯方式进行选择。应当注意在链路创建阶段，只是对验证协议进行选择，用户验证将在第2阶段实现。同样，在LCP阶段还将确定链路对等双方是否要对使用数据压缩或加密进行协商。实际对数据压缩/加密算法和其它细节的选择将在第4阶段实现。 阶段2：用户验证 在第2阶段，客户会PC将用户的身份明发给远端的接入服务器。该阶段使用一种安全验证方式避免第三方窃取数据或冒充远程客户接管与客户端的连接。大多数的PPP方案只提供了有限的验证方式，包括口令验证协议（PAP），挑战握手验证协议（CHAP）和微软挑战握手验证协议（MSCHAP）。 1.口令验证协议（PAP） PAP是一种简单的明文验证方式。NAS要求用户提供用户名和口令，PAP以明文方式返回用户信息。很明显，这种验证方式的安全性较差，第三方可以很容易的获取被传送的用户名和口令，并利用这些信息与NAS建立连接获取NAS提供的所有资源。所以，一旦用户

密码被第三方窃取，PAP无法提供避免受到第三方攻击的保障措施。 2.挑战-握手验证协议（CHAP） CHAP是一种加密的验证方式，能够避免建立连接时传送用户的真实密码。NAS向远程用户发送一个挑战口令（challenge），其中包括会话ID 和一个任意生成的挑战字串（arbitrary challengestring）。远程客户必须使用MD5单向哈希算法（one-wayhashingalgorithm）返回用户名和加密的挑战口令，会话ID以及用户口令，其中用户名以非哈希方式发送。CHAP对PAP进行了改进，不再直接通过链路发送明文口令，而是使用挑战口令以哈希算法对口令进行加密。因为服务器端存有客户的明文口令，所以服务器可以重复客户端进行的操作，并将结果与用户返回的口令进行对照。CHAP为每一次验证任意生成一个挑战字串来防止受到再现攻击（replay attack）。在整个连接过程中，CHAP将不定时的向客户端重复发送挑战口令，从而避免第3方冒充远程客户（remoteclient impersonation）进行攻击。 3.微软挑战-握手验证协议（MS-CHAP） 与CHAP相类似，MS-CHAP也是一种加密验证机制。同CHAP一样，使用MS-CHAP时，NAS会向远程客户发送一个含有会话ID和任意生成的挑战字串的挑战口令。远程客户必须返回用户名以及经过MD4哈希算法加密的挑战字串，会话ID和用户口令的MD4哈希值。采用这种方式服务器端将只存储经过哈希算法加密的用户口令而不是明文口令，这样就能够提供进一步的安全保障。此外，MS-CHAP同样支持附加的错误编码，包括口令过期编码以及允许用户自己修改口令的加密的客户-服务器（client-server）附加信息。使用MS-CHAP，客户端和NAS双方各自生成一个用于随后数据

加密的起始密钥。MS-CHAP使用基于MPPE的数据加密，这一点非常重要，可以解释为什么启用基于MPPE的数据加密时必须进行MS-CHAP验证。 在第2阶段PPP链路配置阶段，NAS收集验证数据然后对照自己的数据库或中央验证数据库服务器（位于NT主域控制器或远程验证用户拨入服务器）验证数据的有效性。 阶段3：PPP回叫控制（callbackcontrol） 微软设计的PPP包括一个可选的回叫控制阶段。该阶段在完成验证之后使用回叫控制协议（CBCP）如果配置使用回叫，那么在验证之后远程客户和NAS 之间的连接将会被断开。然后由NAS使用特定的电话号码回叫远程客户。这样可以进一步保证拨号网络的安全性。NAS只支持对位于特定电话号码处的远程客户进行回叫。 阶段4：调用网络层协议 在以上各阶段完成之后，PPP将调用在链路创建阶段（阶段1）选定的各种网络控制协议（NCP）。例如，在该阶段IP控制协议（IPCP）可以向拨入用户分配动态地址。在微软的PPP方案中，考虑到数据压缩和数据加密实现过程相同，所以共同使用压缩控制协议协商数据压缩（使用MPPC）和数据加密（使用 MPPE）。 数据传输阶段 一旦完成上述4阶段的协商，PPP就开始在连接对等双方之间转发数据。每个被传送的数据报都被封装在PPP包头内，该包头将会在到达接收方之后被去除。如果在阶段1选择使用数据压缩并且在阶段4完成了协商，数据将会在被传送之间进行压缩。类似的，如果如果已经选择使用数据加密并完成了协商，数据（或被压缩数据）将会在传送之前进行加密。 点对点隧道协议（PPTP） PPTP是一个第2层的协议，将PPP数据桢封装在IP数据报内通过IP网络，如Internet传送。PPTP还可用于专用局域网络之间的连

接。 RFC草案“ 点对点隧道协议 ”对PPTP协议进行了说明和介绍。该草案由PPTP论坛的成员公司，包括微软，Ascend，3Com，和ECI等公司在 1996年6月提交至IETF.可在如下站点http://www.ietf.org http://www.ietf.org参看草案的在线拷贝。PPTP使用一个TCP连接对隧道进行维护，使用通用路由封装（GRE）技术把数据封装成PPP数据桢通过隧道传送。可以对封装PPP桢中的负载数据进行加密或压缩。图7所示为如何在数据传递之前组装一个PPTP数据包。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com