第 3 章　网络分层与功能

根据考试大纲，本章要求考生掌握以下知识点：

（1）应用层：应用层功能、应用层实现模型。

（2）传输层：传输层功能、传输层的实现模型、流量控制策略。

（3）网络层：网络层功能、数据报与虚电路。

（4）数据链路层：数据链路层功能、数据链路层差错控制方法、基本链路控制规程、数据链路层协议。

（5）物理层：物理层功能、物理层协议。

3.1　应用层

应用层是 OSI/RM 体系中最高的一个功能层，是开放系统互联环境与本地系统的操作系统和应用系统直接接口的一个层次。在功能上，应用层为本地系统的应用进程（Application Process，AP）访问 OSI/RM 环境提供手段，也是唯一直接给应用进程提供各种应用服务的层次。根据分层原则，应用层向应用进程提供的服务是 OSI/RM 的所有层直接或间接提供服务的总和。

1．应用层功能与协议

常用的网络服务包括文件服务、电子邮件服务、打印服务、集成通信服务、目录服务、域名解析服务、网络管理、安全和路由互连服务等，如果要完成类似这样的网络服务，必须通过应用层的协议来完成。常用的应用层协议有 HTTP、FTP、Telnet、SNMP、SMTP、NNTP、DNS。

2．应用层实现模型

简单地说，应用层是由应用进程和其使用的应用实体（Application Entity，AE）组成，应用进程把信息处理功能和通信功能组合在一起，通过一个全局的名字可以调用这个功能。

例如，远程数据库访问可组成一个应用进程，这个应用进程与远处的数据库服务进程交互作用（发出检索命令、接收响应、处理结果），完成数据库检索。

应用进程的通信功能是由应用实体实现的。为了实现不同性质的通信，一个应用进程可能使用一个或多个应用实体。

一个应用实体还可以再划分为一个用户元素（User Element，UE）和若干的应用服务元素（Application Service Element，ASE）。

ASE 是具有简单通信能力的功能模块，对等的 ASE 之间有专用的服务定义和协议规范。应用实体首先要与对等的应用实体建立应用联系（Application Association，AA），然后才能通信。建立应用联系的过程主要是交换应用上下文（Application Context，AC）。AC 是可以用名字（对象标识符）引用一组 ASE 及其调用规则。在建立联系期间通过协商确定共同认可的应用上下文，并在应用活动期间遵守商定的通信规则。

3.2　传输层

传输层能提供可靠或不可靠的服务。既然有可靠的服务可用，为什么应用程序开发人员还要使用不可靠的服务呢？这个选择取决于应用程序本身的特性。对于传输层的上一层和下一层，定义什么是可靠、什么是不可靠是有意义的。

3.2.1　可靠性传输

传输层中的可靠性是指传输协议对在网络中传送的数据具有提供某种保证的能力。通过提供保证，数据传送变得可靠。

传输层中的不可靠性是指传输协议对在网络中传送的数据缺乏提供保证的能力。

由于网络是不可靠的。在 OSI/RM 的第 5～第 7 层中会发生许多的事件，这些事件都需要传输层来处理。传输层必须对报文丢失提供一种检测方法，以便可以重新传输丢失的数据。有时网络层会通过不同的链路路由多个报文，这导致报文以错误的顺序到达目的地。传输层必须能把这些报文按正确的顺序进行重新汇编，以便将数据传送给应用程序。由于大多数应用程序都是以结构化的格式交换数据，因此在接收数据时必须按正确的顺序重新汇编。

传输层必须能协调所有的情况。之所以不需要使用可靠的传输层，是因为对可靠或不可靠服务的选择取决于应用程序要交换的信息的类型。例如，用户要把一个重要的财务数据表保存到网络服务器，该网络服务器显然需要可靠性保证，以防止在文件传输时有一两个报文丢失。那么，传输层仅仅重新传输数据就可以了，因为传输层就是这样提供可靠性的。但是要是通过 IP 网络传送电话呢？如果传输层把交谈中可能丢失的所有数据都重新传输，这样有意义吗？每当含有声音的报文丢失，传输层只能在用户接收到声音数据后将丢失的报文重新传输。这将在电话的接收端引起严重混淆的接收效果。如果传输层等待一段时间并将要传输的数据存放在一个缓冲器中直到丢失的报文被重新传输完呢？这样做当然可以，不过由于附加的重新传输和重新汇编延迟，通话质量将严重下降。因此，在 IP 网络中使用不可靠协议传输声音数据会更好。

3.2.2　网络质量

根据通信子网提供的服务质量不同，网络服务可分为 A、B 和 C 类网络服务。

（1）A 型网络服务。A 类网络是一个完整的、理想的、可靠的服务，所需传输层协议非常简单。在该类网络服务下，网络中传输的分组不会丢失和失序，因此传输层不需要提供故障恢复和重新排序服务。多数局域网可提供 A 型网络服务，但广域网则很难达。

（2）B 型网络服务。具有较好的数据服务（误码率低）和较差的连接服务（故障多）。对该型网络，传输层协议必须提供故障恢复功能。大多数 X.25 网为 B 型网络。

（3）C 类网络服务。网络传输不可靠，可能会丢失分组或出现重复分组；网络故障率也高。例如简单的无线网络，容易丢失数据，网络故障率也高。

3.2.3 协议与控制

传输层定义了 5 类协议，都是面向连接的。

（1）0 类协议：最简单的协议，是面向 A 型网络服务的。该类协议没有差错恢复和复用功能。

（2）1 类协议：提供基本的传输连接，是面向 B 型网络服务的。它在 0 类协议的基础上增加了基本差错恢复功能。

（3）2 类协议：面向 A 型网络服务。该类协议具有流量控制、复用功能而没有网络连接和故障恢复功能。

（4）3 类协议：面向 B 型网络服务，既具有差错恢复功能，又有复用功能。

（5）4 类协议：是面向 C 型网络服务，具有差错检测、差错恢复、复用等功能。该类协议是最复杂、最全面的协议。

传输控制协议是实现端到端计算机之间的通信、实现网络系统资源共享所必不可少和非常重要的协议。传输控制协议所实现的功能不仅是保证相同计算机系统之间、相同计算机网络系统之间信息的可靠传输，还可实现不同计算机系统之间、不同计算机网络系统之间信息的可靠传输。

3.3 网络层

网络层是通信子网的最高层，用于控制和管理通信子网的操作。它体现了网络应用环境中资源子网访问通信子网的方式。网络层的数据传输单位为数据分组（包）。网络层的主要任务：在数据链路服务的基础上，实现整个通信子网内的连接，向传输层提供端到端的数据传输通路，为报文分组以最佳路径通过通信子网到达目的主机提供服务。如果两实体跨越多个网络，网络层还可提供正确的路由选择和数据传输服务等。

网络层的主要功能如下：

（1）建立、维持和拆除网络连接：在网络层，要为传输层实体之间通信提供网络连接的建立、维持和拆除。

（2）路由选择：根据一定的原则和算法，在多节点的通信子网中，选择一条从源节

点到目的节点的合适逻辑通路的控制过程。

（3）流量控制：网络层的流量控制是对进入整个通信子网内的数据流量及其分布进行控制和管理，以避免发生网络阻塞和死锁，提高网络传输效率和吞吐量。

（4）网络传输控制：网络层要对在通信子网中传输的数据进行控制，包括组包、拆包、包的按序重装，包信息的传输同步，差错控制和速率控制等。

3.4　数据链路层

数据链路层最基本的服务是将源计算机网络层来的数据可靠的传输到相邻节点的目标计算机的网络层。为达到这一目的，数据链路层必须具备一系列相应的功能，主要有：如何将数据组合成数据块（在数据链路层中将这种数据块称为帧，帧是数据链路层的传送单位）；如何控制帧在物理信道上的传输，包括如何处理传输差错，如何调节发送速率以使之与接收方相匹配；在两个网路实体之间提供数据链路通路的建立、维持和释放管理。

为了实现上述的目标，数据链路层主要需要完成的功能有组帧、差错控制、流量控制、链路管理、MAC 寻址、区分数据与控制信息、透明传输。

3.4.1　组帧方法

数据链路层为了能实现数据有效的差错控制，就采用了一种“帧”的数据块进行传输。而要采帧格式传输，就必须有相应的帧同步技术，这就是数据链路层的“组帧”（也称为“帧同步”、“成帧”）功能。

采用帧的好处是，在发现有数据传送错误时，只需将有差错的帧再次传送，而不需要将全部数据的位流进行重传，这样传送效率上将大大提高。但同时也带来了两方面的问题：

（1）如何识别帧的开始与结束。

（2）在夹杂着重传的数据帧中，接收方在接收到重传的数据帧时是识别成新的数据帧，还是识别成已传帧的重传帧呢？这就要靠数据链路层的各种“帧同步”技术来识别了。“帧同步”技术既可使接收方能从以上并不是完全有序的位流中准确地区分出每一帧的开始和结束，同时还可识别重传帧。

下面主要讨论 4 种最常用的组帧方法。

1．字符计数法

字符计数法是一种面向字节的同步规程，是利用帧头部中的一个字段来指定该帧中的字符数，以一个特殊字符表征一帧的起始，并以一个专门字段来标明帧内的字符数。这种方法遇到的问题是计数值有可能由于传输差错而导致字符数信息出错或丢失，目前很少使用这类计数法。

2．字符填充帧定界法

字符填充帧定界法只适用于面向字符的链路层协议，如 20 世纪 60 年代末由 IBM 公司开发的二进制同步通信（BInary SYNchronous Communication，BISYNC）协议。字符填充组帧法采取的措施是每个帧以 ASCII 字符序列 DLE STX 开头、DLE ETX 结束（DLE、STX 和 ETX 分别为 ASCII 字符集里的控制字符，其中 DLE 为 Data Link Escape，STX 为 Start of TeXt，ETX 为 End of TeXt）。用这种方法，接收端通过扫描输入线路上的 DLE STX 和 DLE ETX 就能确定帧的起始和结束。

字符填充组帧法带来的一个问题是，当用户数据中含有 DLE STX 或 DLE ETX 字符序列时，将严重干扰帧的定界。解决的办法是：让发送方在发送数据的每个 DLE 字符前面再插入一个 DLE 字符，而接收方在接收数据时删除插入的 DLE 字符，这种方法叫做字符填充（Character Stuffing）技术。这样，接收方在扫描物理线路的字符序列时，如果发现只是单个 DLE 出现，就可以断定一定是帧的起始或结束标识符 DLE STX 或 DLE ETX，而不是数据 DLE，因为后者总是成对出现的。图 3-1 给出了用户数据在进行字符填充前、填充后以及去掉填充字符后的情况。

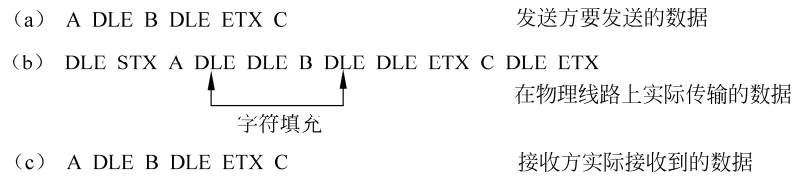

图 3-1 带字符填充组帧法

3．位填充帧定界法

位填充帧定界法是位填充组帧法。位填充组帧法克服了字符填充组帧法的缺点，因为它不依赖特定的字符集，允许发送的数据为任意的位组合。该方法可以用于面向位的链路层协议，如 IBM 的同步数据链路控制（Synchronous Data Link Control，SDLC）和 ISO 的高级数据链路控制（High Data Link Control，HDLC）协议。

位填充组帧法是在每一帧的头和尾各引入一个特殊的位组合作为帧的起始和结束标识符，如 01111110（十六进制 7E）。当接收方扫描到 01111110 时就知道是一帧的开头，接收方开始扫描并接收位串直到扫描到下一个 01111110 标识符为止。

位填充组帧法也带来一个同样的问题，即当发送的数据中含有 01111110 位组合时，也将严重干扰正常的组帧。为保证标识符的唯一性但又兼顾帧内数据的透明性，可以采用“0 位插入法”来解决。也就是说，在发送端发送用户数据，当发现有连续的 5 个“1”出现时便在其后添加一个“0”，然后继续发送后续的用户数据。在接收端接收用户数据除标识符以外的所有字段，当发现有连续 5 个“1”出现后，若其后一个位为“0”，则自动删除它以恢复原来的位流。图 3-2 给出了一个位填充的例子。

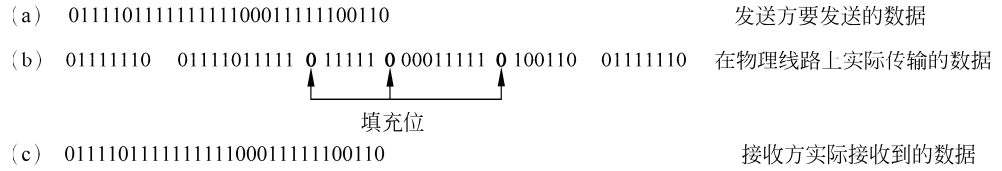

图 3-2　带位填充组帧法

4．物理层违例法

物理层违例法在物理层采用特定的位编码方法时采用。例如，曼彻斯特编码方法，是将数据位“1”编码成“高-低”电平对，将数据位“0”编码成“低-高”电平对。

希赛教育专家提示：数据位“0”编码成“高-低”电平对，将数据位“1”编码成“低-高”电平对，这种说法在考试中也是正确的。

不管哪种说法，“高-高”电平对和“低-低”电平对在数据位中是违法的。这样，在每个数据位中都有电平跳变，而作为帧界定符就不会有电平跳变，就借用这些违法编码序列来界定帧的起始与终止。

局域网 IEEE 802.3 和 802.5 标准中就采用了这种方法。违法编码法不需要任何填充技术，便能实现数据的透明性，但它只适于采用冗余编码的特殊编码环境。

3.4.2　差错控制

在数据通信过程可能会因物理链路性能和网络通信环境等因素，难免会出现一些传送错误，但为了确保数据通信的准确，又必须使得这些错误发生的机率尽可能低。这一功能也是在数据链路层实现的，就是它的“差错控制”功能。

在数字或数据通信系统中，通常利用抗干扰编码进行差错控制。一般分为以下 4 类：

（1）前向纠错（Forward Error Correction，FEC）。FEC 方式是在信息码序列中，以特定结构加入足够的冗余位——称为“监督元”（或“校验元”）。接收端解码器可以按照双方约定的这种特定的监督规则，自动识别出少量差错，并能予以纠正。FEC 最适于高速数据、且需要实时传输的情况。

（2）反馈检测（Auto Repeat reQuest，ARQ）。在非实时数据传输中，常用 ARQ 差错控制方式。解码器对接收码组逐一按编码规则检测其错误。如果无误，向发送端反馈“确认”ACK（ACKnowledge）信息；如果有错，则反馈回 ANK（ANKnowledge）信息，以表示请求发送端重复发送刚刚发送过的这一信息。ARQ 方式的优点在于编码冗余位较少，可以有较强的检错能力，同时编解码简单。由于检错与信道特征关系不大，在非实时通信中具有普遍应用价值。

（3）混合纠错（Header Error Correction，HEC）。HEC 方式是上述两种方式的有机结合，即在纠错能力内，实行自动纠错；而当超出纠错能力的错误位数时，可以通过检测而发现错码，不论错码多少都可以利用 ARQ 方式进行纠错。

（4）信息反馈（Information Repeat reQuest，IRQ）。IRQ 方式是一种全回执式最简单差错控制方式。在该检错方式中，接收端将收到的信码原样转发回发送端，并与原发送信码相比较，若发现错误，则发送端再进行重发。只适于低速非实时数据通信，是一种较原始的做法。

3.4.3 其他功能

本小节介绍数据链路层的流量控制、链路管理、MAC 寻址、区分数据域控制信息、透明传输等功能。

1．流量控制

在双方的数据通信中，如何控制数据通信的流量同样非常重要。它既可以确保数据通信的有序进行，还可避免通信过程中不会出现因为接收方来不及接收而造成的数据丢失。这就是数据链路层的“流量控制”功能。数据的发送与接收必须遵循一定的传送速率规则，可以使得接收方能及时地接收发送方发送的数据。并且当接收方来不及接收时，就必须及时控制发送方数据的发送速率，使两方面的速率基本匹配。

2．链路管理

数据链路层的“链路管理”功能包括数据链路的建立、链路的维持和释放三个主要方面。当网络中的两个结点要进行通信时，数据的发送方必须确知接收方是否已处在准备接收的状态。为此通信双方必须先要交换一些必要的信息，以建立一条基本的数据链路。在传输数据时要维持数据链路，而在通信完毕时要释放数据链路。

3．MAC 寻址

这是数据链路层中的 MAC 子层主要功能。这里所说的“寻址”与“IP 地址寻址”是完全不一样的，因为此处所寻找的地址是计算机网卡的 MAC 地址，也称为物理地址、硬件地址，而不是 IP 地址（逻辑地址）。在以太网中，采用 MAC 地址进行寻址，MAC 地址被烧入每个以太网网卡中。这在多点连接的情况下非常必需，因为在这种多点连接的网络通信中，必须保证每一帧都能准确地送到正确的地址，接收方也应当知道发送方是哪一个站。

4．区分数据与控制信息

由于数据和控制信息都是在同一信道中传输，在许多情况下，数据和控制信息处于同一帧中，因此一定要有相应的措施使接收方能够将它们区分开来，以便向上传送仅是真正需要的数据信息。

5．透明传输

透明传输是指可以让无论是哪种位组合的数据，都可以在数据链路上进行有效传输。这就需要在所传数据中的位组合恰巧与某一个控制信息完全一样时，能采取相应的技术措施，使接收方不会将这样的数据误认为是某种控制信息。只有这样，才能保证数据链路层的传输是透明的。

在链路层主要功能中，重要的还是组帧、差错控制、流量控制、链路管理、MAC 寻址，而区分数据与控制信息和透明传输是在前 5 项功能中附带实现的，并无需另外的技术。

3.4.4　数据链路层协议

数据链路层协议有 HDLC、PPP、SDLC 等，本节主要介绍 HDLC 和 PPP 协议。

1．HDLC 协议

HDLC 源于 IBM 开发的 SDLC，SDLC 是由 IBM 开发的第一个面向位的同步数据链路层协议。随后，ANSI 和 ISO 均采纳并发展了 SDLC，并且分别提出了自己的标准，ANSI 提出了高级数据链路控制规程（Advanced Data Communication Control Procedure，ADCCP），而 ISO 提出了 HDLC。

作为面向位的同步数据控制协议的典型，HDLC 只支持同步传输。但是 HDLC 既可工作在点到点线路方式下，也可工作在点到多点线路方式下；同时 HDLC 既适用于半双工线路，也适用于全双工线路。HDLC 协议的子集被广泛用于 X.25 网络、帧中继网络以及局域网的逻辑链路控制（Logic Link Control，LLC）子层作为链路层协议以支持相邻节点之间可靠的数据传输。

1）HDLC 帧格式

HDLC 协议的帧格式如图 3-3 所示。

1	1	1	>=0	2	1 字节
01111110	Address	Control	Infor	FCS	01111110

图 3-3　HDLC 协议的帧格式

每个字段的含义如下：

（1）标志字段 F（Flag）。该字段为 01111110 的位模式，用以标识帧的开始与结束，也可以作为帧与帧之间的填充。在连续发送多个帧时，同一个标识既可用于表示前一帧的结束，又可用于表示下一帧的开始。通常在不进行帧传送的时刻，信道仍处于激活状态，在这种状态下发送方不断地发送标识字段，而接收方则检测每一个收到的标识字段，一旦发现某个标识字段后面不再是一个标识字段，便可认为新的帧传输已经开始。采用“0 位插入法”可以实现用户数据的透明传输。

（2）地址字段 A（Address）。该字段的内容取决于所采用的操作方式。每个节点都被分配一个唯一的地址。控制帧中的地址字段携带的是对方节点的地址，而响应帧中的地址字段所携带的地址是本节点的地址。某一地址也可分配给不止一个节点，这种地址称为组地址。利用一个组地址传输的帧能被组内所有的节点接收。还可以用全“1”地址来表示包含所有节点的地址，全“1”地址称为广播地址，含有广播地址的帧传送给链路

上所有的节点。另外，还规定全“0”的地址不分配给任何节点，仅作为测试用。

地址字段长度通常是 8 位，可表示 256 个地址。当地址字段的首位为“1”时，表示地址字段只用 8 位；若首位为“0”时，表示本字节后面 1 个字节是扩充地址字段。这就意味着 HDLC 地址字段可以标识超过 256 个以上的站点地址。

（3）控制字段 C（Control）。控制字段占用 1 个字节长度。控制字段用于构成各种命令及响应，以便对链路进行监视与控制。该字段是 HDLC 帧格式的关键字段。控制字段中的第 1 位或第 2 位表示帧的类型，即信息帧 I 帧、监控帧 S 帧和无编号帧 U 帧。3 种类型的帧控制字段的第 5 位是 P/F（Poll/Final，轮询/终止）位。

（4）信息字段 I（Information）。信息字段可以是任意的二进制位串，长度未作限定，其上限由 FCS 字段或通信节点的缓冲容量来决定。目前，国际上用得较多的是 1000～2000 位，而下限可以是 0 ，即无信息字段。另外，监控帧中不可有信息字段。

（5）帧校验序列。在 HDLC 协议的所有帧中都包含一个 16 位的帧校验序列（Frame Check Sequence，FCS），用于差错检测。HDLC 协议的校验序列是对整个帧的内容进行 CRC 循环冗余校验，但标志字段和 0 位插入部分不包括在帧校验范围内。HDLC 协议帧校验序列的生成多项式一般采用多项式 $x^{16}+x^{12}+x^5+1$。

2）HDLC 帧类型

HDLC 的控制字段有 8 位。如果第 1 位为“0”时，表示该帧为信息帧；第 1、2 位为“10”时，表示该帧为监控帧；第 1、2 位为“11”时，表示该帧为无编号帧。

（1）信息帧（Information Frame）用于传送有效信息或数据，通常简称为 I 帧，其控制字段的帧格式如图 3-4 所示。

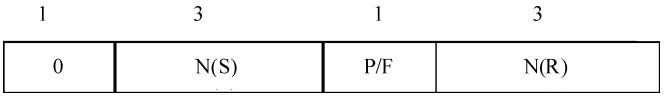

图 3-4　信息帧控制字段格式

I 帧控制字段的第 1 位为 0。HDLC 协议采用滑动窗口机制，允许发送方不必等待确认而连续发送多个信息帧。控制字段中的 N(S)用于存放发送帧的序列，N(R)用于存放接收方下一个预期要接收的帧的序号。N(S)与 N(R)均为 3 位，可取值 0～7。

（2）监控帧（Supervisor Frame）用于差错控制和流量控制，通常称为 S 帧。监控帧以控制字段第 1、2 位为 10 来标志。监控帧控制字段格式如图 3-5 所示。

图 3-5　监控帧控制字段格式

监控帧控制字段的第 3、4 位为监控帧类型编码，共有 4 种不同的编码，如表 3-1 所示。

表 3-1　监控帧的功能及 N(R)字段含义

帧类型	Type 字段	功能描述	N(R)字段的含义
RR	00	接收就绪，请求发送下一帧	期望接收的下一个 I 帧的序号
REJ	01	请求重新发送序号为 N(R)的所有帧	重发帧的开始序号
RNR	10	请求暂停发送数据帧	N(R)之前各帧已正确接收
SREJ	11	请求重发指定帧	重发帧的顺序号

接收方可以用接收就绪（Receive Ready，RR）监控帧应答发送方，希望发送方发送序号为 N(R)的信息帧。RR 帧就相当于专门应答帧（因为一般情况下，应答信息都是通过反向数据帧的捎带来完成的）。

接收方可以用拒绝（REJect，REJ）监控帧来要求发送方重传编号为 N(R)之后所有的信息帧（包括 N(R)帧），同时暗示 N(R)以前的信息帧被正确接收。

接收方返回接收未就绪（Receive Not Ready，RNR）监控帧，表示编号小于 N(R)的信息帧已被收到，但目前正忙，尚未准备好接收编号为 N(R)的信息帧，这可用来对链路进行流量控制。

接收方返回选择拒绝（Select REJect，SREJ）监控帧来要求发送方只发送编号为 N(R)的信息帧，并暗示其他编号的信息帧已经全部正确接收到。

RR 监控帧和 RNR 监控帧有两个主要功能：首先这两种监控帧用来表示接收方已经准备好或未准备好信息；其次确认编号小于 N(R)的所有信息帧都正确接收到。

REJ 监控帧和 SREJ 监控帧用于向发送方指出发生了差错，REJ 监控帧用于 GO-BACK-N 策略用以请求重发 N(R)起始的所有帧；SREJ 帧用于选择重传协议，用于指定重发某个特定的帧。

（3）无编号帧 U（Unnumbered Frame）用控制字段第 1、2 位为 11 来标识，如图 3-6 所示。

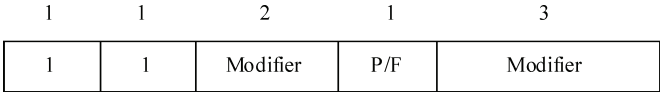

图 3-6　无编号帧控制字段格式

无编号帧因为其控制字段中不包含编号 N(S)和 N(R)而得名，简称 U 帧。U 帧用于提供对链路的建立、拆除以及多种控制工程。无编号帧 U 用 5 个修正（Modifier）位来进行定义，最多可以表示 32 种控制帧。

2．PPP 协议

PPP 是 RFC1171/1172 制定的，是在点对点线路上对包括 IP 在内的 LAN 协议进行中

继的 Internet 标准协议。PPP 被设计成支持多种上层协议，并设计成具有不依存于网络层协议的数据链路。在用 PPP 对各个网络层协议进行中继时，每个网络层协议必须有某个对应于 PPP 的规格，这些规格有一些已经存在。PPP 是由两种协议构成的：一种是为了确保不依存于协议的数据链路而采用的 LCP（Link Control Protocol，链路控制协议）；另一种为了实现在 PPP 环境中利用网络层协议控制功能的 NCP（Network Control Protocol，网络控制协议）。NCP 的具体名称在对应的网络层协议中有所不同。更准确地说，PPP 所规定协议只是 LCP，至于将 NCP 及网络层协议如何放入 PPP 帧中，要由开发各种网络层协议的厂家完成。PPP 帧具有传输 LCP、NCP 及网络层协议的功能。对利用 LCP 的物理层规格没有特殊限制。可以利用 RS-232-C、RS-422/423、V.35 等通用的物理连接器。传输速率的应用领域也没有特别规定，可以利用物理层规格所容许的传输速率。

1）PPP 协议的应用

PPP 协议是目前广域网上应用最广泛的协议之一，它的优点在于简单、具备用户验证能力、可以解决 IP 分配等。

家庭拨号上网就是通过 PPP 在用户端和运营商的接入服务器之间建立通信链路。目前，宽带接入已经成为取代拨号上网的新方式，在宽带接入技术日新月异的今天，PPP 也衍生出新的应用。典型的应用是在 ADSL 接入方式当中，PPP 与其他的协议共同派生出了符合宽带接入要求的新的协议，如 PPPoE（PPP over Ethernet，以太网上的 PPP），PPPoA（PPP over ATM，ATM 网上的 PPP）。

利用以太网资源，在以太网上运行 PPP 来进行用户认证接入的方式称为 PPPoE。PPPoE 既保护了用户方的以太网资源，又完成了 ADSL 的接入要求，是目前 ADSL 接入方式中应用最广泛的技术标准。

同样，在 ATM 网络上运行 PPP 协议来管理用户认证的方式称为 PPPoA。它与 PPPoE 的原理、作用都相同；不同的是，PPPoA 是在 ATM 网络上，而 PPPoE 是在以太网网络上运行，所以要分别适应 ATM 标准和以太网标准。

2）PPPoE 协议简介

随着宽带网络技术的不断发展，以 xDSL、Cable Modem 和以太网为主的几种主流宽带接入技术的应用已如火如荼地展开。同时，又给各大网络运营商们带来了种种新的问题，无论使用哪种接入技术，对于他们而言，可盼和可求的是如何有效地管理用户，如何从网络的投资中收取回报，因此对于各种宽带接入技术的收费问题就变得更加敏感。在传统的以太网模型中，是不存在所谓的用户计费的概念，要么用户能获取 IP 地址上网，要么用户就无法上网。IETF（Internet Engineering Task Force，互联网工程任务组）的工程师们在秉承窄带拨号上网的运营思路，制定出了在以太网上传送 PPP 数据包的协议，这个协议出台后，各网络设备制造商也相继推出自己品牌的宽带接入服务器（Broadband Access Server，BAS），它不仅能支持 PPPoE 协议会话的终结，而且还能支持其他许多协

议。例如，华为公司的 MA5200 和北电的 Shasta5000。

PPPoE 协议提供了在广播式的网络（如以太网）中多台主机连接到远端的访问集中器（称目前能完成上述功能的设备为宽带接入服务器）上的一种标准。在这种网络模型中，不难看出所有用户的主机都需要能独立地初始化自己的 PPP 协议栈，而且通过 PPP 协议本身所具有的一些特点，能实现在广播式网络上对用户进行计费和管理。为了能在广播式的网络上建立、维持各主机与访问集中器之间点对点的关系，那么就需要每个主机与访问集中器之间能建立唯一的点到点的会话。

PPPoE 协议共包括两个阶段，即 PPPoE 的发现阶段（PPPoE Discovery Stage）和 PPPoE 的会话阶段（PPPoE Session Stage）。对于 PPPoE 的会话阶段，可以看成和 PPP 的会话过程是一样的，而两者的主要区别在于只是在 PPP 的数据报文前封装了 PPPoE 的报文头。无论是哪一个阶段的数据报文最终会被封装成以太网的帧进行传送。

PPPoE 的数据报文是被封装在以太网帧的数据域内的。可以把 PPPoE 报文分成两大块，一大块是 PPPoE 的数据报头；另一块则是 PPPoE 的净载荷（数据域），对于 PPPoE 报文数据域中的内容会随着会话过程的进行而不断改变。图 3-7 所示为 PPPoE 的报文的格式。

版本	类型	代码	会话 ID
长度域		数据域	

图 3-7　PPPoE 数据报文格式

- PPPoE 数据报文最开始的 4 位为版本域，协议中给出了明确的规定，这个域的内容填充 0x01。紧接在版本域后的 4 位是类型域，协议中同样规定，这个域的内容填充为 0x01。代码域占用 1 字节，对于 PPPoE 的不同阶段这个域内的内容也是不一样的。会话 ID 占用 2 字节，当访问集中器还未分配唯一的会话 ID 给用户主机的话，则该域内的内容必须填充为 0x0000，一旦主机获取了会话 ID 后，那么在后续的所有报文中该域必须填充那个唯一的会话 ID 值。

长度域为 2 字节，用来指示 PPPoE 数据报文中净载荷的长度。数据域有时也称为净载荷域，在 PPPoE 的不同阶段该域内的数据内容会有很大的不同。在 PPPoE 的发现阶段时，该域内会填充一些 Tag（标记）；而在 PPPoE 的会话阶段，该域则携带的是 PPP 的报文。

3.5　物理层

物理层协议要解决的是主机、工作站等数据终端设备与通信线路上通信设备之间的接口问题。多数物理层是由 DTE 和 DCE 组成。DTE 的基本功能是处理数据以及发送和

接收数据。由于大多数的数据处理设备的数据传输能力的限制，如果将相隔很远的两个数据处理设备直接相连，必须在数据处理设备和传输介质之间，加上一个中间设备，否则不能进行通信。这个中间设备就是 DCE。DCE 的作用就是在 DTE 和传输线路之间提供信号变换和编码的功能，并且负责建立、保持和释放数据链路的连接。图 3-8 所示为 DTE/DCE 接口框图。

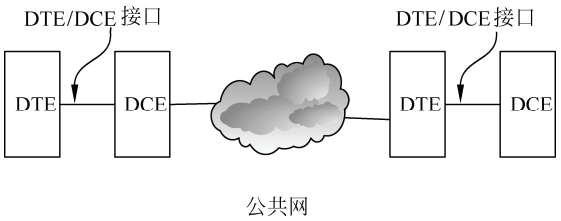

图 3-8　DTE/DCE 接口框图

DTE 与 DCE 之间的接口一般都有多条并行线，其中包括多种信号线和控制线。DCE 在通信过程中作为 DTE 和信道的连接点，DCE 将 DTE 传过来的数据，按位顺序逐个发往传输线路，或反过来从传输线路接收串行的位流，然后再交给 DTE。期间需要高度协调地工作，为了减轻数据处理设备用户的负担，必须对 DTE 和 DCE 的接口进行标准化，这种接口标准也就是物理层协议。

3.5.1　物理层特性

在 DTE 和 DCE 之间实现建立、维护和拆除物理链路连接的有关技术细节，ICCTT（International Consultative Committee on Telecommunications and Telegraphy，国际电报电话咨询委员会）和 ISO 用 4 个技术特性来描述，并给了适应不同情况的各种标准和规范。这 4 个技术特性是机械特性、电气特性、功能特性和规程特性。

1．机械特性

机械特性规定了物理连接时对插头和插座的几何尺寸、插针或插孔芯数及排列方式、锁定装置形式等。图 3-9 列出了各类已被 ISO 标准化了的 DCE 连接器的几何尺寸及插孔芯数和排列方式。

一般来说，DTE 的连接器常用插针形式，其几何尺寸与 DCE 连接器相配合，插针芯数和排列方式与 DCE 连接器成镜像对称。

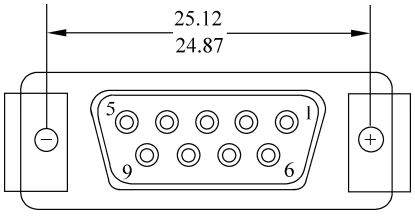

图 3-9　常用连接机械特性

2．电气特性

电气特性规定了在物理连接上导线的电气连接及有关的电路特性，一般包括接收器和发送器电路特性的说明、表示信号状态的电压/电流电平的识别、最大传输速率的说明、

以及与互连电缆相关的规则等。

物理层的电气特性还规定了 DTE-DCE 接口线的信号电平、发送器的输出阻抗、接收器的输入阻抗等电器参数。

DTE 与 DCE 接口的各根导线（也称电路）的电气连接方式有非平衡方式、采用差动接收器的非平衡方式和平衡方式三种。

（1）非平衡方式。该方式采用分立元件技术设计的非平衡接口，每个电路使用一根导线，收发两个方向共用一根信号地线，信号速率<20kb/s，传输距离<15m。由于使用共用信号地线，所以会产生比较大的串扰。CCITTV.28 建议采用这种电气连接方式，EIA RS-232C 标准基本与之兼容。

（2）采用差动接收器的非平衡方式。该方式采用集成电路技术的非平衡接口，与前一种方式相比，发送器仍使用非平衡式，但接收器使用差动接收器。每个电路使用一根导线，但每个方向都使用独立的信号地线，使串扰信号较小。这种方式的信号传输速率可达 300kb/s，传输距离为 10（传输速率为 300kb/s 时）～1000m（传输速率≤3kb/s 时）。CCITT V.10/X.26 建议采用这种电气连接方式，EAI RS-423 标准与之兼容。

（3）平衡方式。该方式采用集成电路技术设计的平衡接口，使用平衡式发送器和差动式接收器，每个电路采用两根导线，构成各自完全独立的信号回路，使得串扰信号减至最小。这种方式的信号速率≤10Mb/s，传输距离为 10（10Mb/s 时）～1000m（≤100kb/s 时）。CCITT V.11/X.27 建议采用这种电气连接方式，EAI RS-423 标准与之兼容。

3．功能特性

功能特性规定了接口信号的来源、作用以及其他信号之间的关系。

4．规程特性

规程特性规定了使用交换电路进行数据交换的控制步骤，这些控制步骤的应用使得位流传输得以完成。

3.5.2　物理层标准

物理层最常用的标准有 EIA-232-E 接口标准和 RS-449 接口标准。

1．EIA-232-E

EIA-232-E 最早是 1962 年制定的标准 RS-232。这里 RS 表示 EIA 一种“推荐标准”，232 是个编号。在 1969 年修订为 RS-232-C，C 是标准 RS-232 以后的第三个修订版本。1987 年 1 月，修订为 EIA-232-D。1991 年又修订为 EIA-232-E。由于标准修改得并不多，因此，现在很多厂商仍用旧的名称，有时简称为 EIA-232。

EIA-232-E 的传送距离最大约为 15m，最高速率为 20kb/s，并且 EIA-232-E 接口是为点对点（即只用一对收、发设备）通信而设计的。所以，EIA-232-E 只适合于本地通信使用。

通常，EIA-232-E 接口以 9 个接脚 （DB-9）或是 25 个接脚（DB-25）的型态出现，

一般个人计算机（Personal Computer，PC）上会有两组 EIA-232-E 接口，分别称为 COM1 和 COM2。

2．RS-449

RS-449 是 1977 年由 EIA 发表的标准，规定了 DTE 和 DCE 之间的机械特性和电气特性。RS-449 是想取代 RS-232-C 而开发的标准，但是几乎所有的数据通信设备厂家仍然采用原来的标准，所以 RS-232-C 仍然是最受欢迎的接口而被广泛采用。

RS-449 的连接器使用 ISO 规格的 37 引脚及 9 引脚的连接器，2 次通道（返回字通道）电路以外的所有相互连接的电路都使用 37 引脚的连接器，而 2 次通道电路则采用 9 引脚连接器。

3.6 覆盖网与对等网

早在 20 世纪 70 年代中期，源于局域网的文件共享 P2P（Peer to Peer）技术就开始流行起来了。首先计划是美国加利福尼亚大学伯克利分校的 SETI@home 研究计划。1999 年，SETI@home 开始使用 P2P 计算方法来分析星际间无线电信号，寻找宇宙中可能存在的其他外星文明证据。P2P 技术串联所有参与研究计划者闲置的电脑来执行庞大复杂的运算，然后把结果传到 SETI@home 总部。也正是 SETI@home 计划推动了 P2P 热潮的到来。2000 年用于共享 MP3 音乐的 Napster 软件与美国唱片界的一场官司更将 P2P 技术带入人们的视线。之后，各种基于对等网的应用风起云涌。

P2P 提出了一种对等网络模型，在这种网络中各个节点是对等的，具有相同的责任和义务，彼此互为客户端/服务器，协同完成任务。对等点之间通过直接互连共享信息资源、处理器资源、存储资源甚至高速缓存资源等，无须依赖集中式服务器资源就可以完成。与传统的 C/S（Client/Server，客户机/服务器）模式形成鲜明对比。P2P 技术主要指由硬件形成网络连接后的信息控制技术，表现形式在应用层上基于 P2P 网络协议的各种客户端软件。

如图 3-10 所示，它和传统的 C/S 不同，传统的 C/S 模式有一台指定的主机提供 Web、FTP、数据库等服务，它的架构是一种典型的中央集中式架构。P2P 没有特定的主机，是一种非集中架构，在网络中没有服务器或是客户机的概念，对于网络中的每一个实体，都会被认为是一个对等点，它们拥有相同的地位，任何一个实体都可以请求服务（客户机的特性）和提供服务（服务器的特性）。

1．P2P 网络的分类

P2P 网络有多种分类方法，从网络结构到应用类型多种多样，这是主要从网络集中化程度、网络结构和网络应用类型三个方面对 P2P 网络进行分类研究。这里主要讨论从网络集中化程度进行分类：

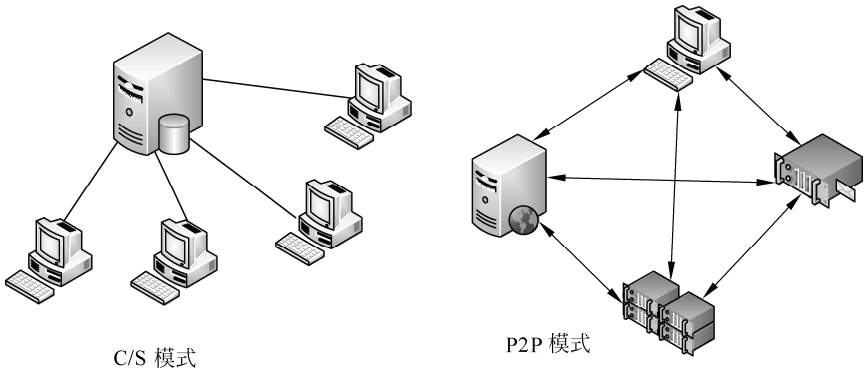

图 3-10　C/S 模式与 P2P 模式

（1）集中式 P2P 网络。集中式 P2P 模式中有一个中心服务器来负责记录共享信息以及回答对这些信息的查询；每一个对等实体对它将要共享的信息以及进行的通信负责，根据需要下载它所需要的其他对等实体上的信息。

（2）分布式 P2P 网络。在分布式对等网中，对等机通过与相邻对等机之间的连接遍布整个网络体系。每个对等机在功能上都是相似的，并没有专门的服务器，而对等机必须依靠它们所在的分布网络来查找文件和定位其他对等机。

（3）半分布型 P2P 网络。集中式 P2P 形式有利于网络资源的快速检索，以及只要服务器能力足够强大就可以无限扩展，但是其中心化的模式容易遭到直接的攻击；分布式 P2P 形式解决了抗攻击问题，但是又缺乏快速搜索和可扩展性。半分布式的 P2P 结合了集中式和分布式 P2P 形式的优点，在设计思想和处理能力上都得到近一步优化。它在分布式模式基础上，将用户节点按能力进行分类，使某些节点担任特殊的任务。

- 用户节点：普通的节点就是用户节点，它不具有任何特殊的功能。
- 超级节点：这些节点能够提供集中式 P2P 网络中一部分服务器的功能，这些节点相互间能够通信，它们可以是专门的超级服务节点，同时也可以具有普通用户的功能。超级节点通常都是动态推举和产生的，一般具有较好的物理性能，能够提供资源搜索和索引的能力，为其临近的若干普通节点提供服务。

2．P2P 资源定位方式

P2P 网络中进行资源定位是首先要解决问题。与 P2P 从网络集中化程度进行分类方式对应一般采用三种方式。

（1）集中方式索引。每一个节点将自身能够提供共享的内容注册到一个或几个集中式的目录服务器中。查找资源时首先通过服务器定位，然后两个节点之间再直接通信，如早期的 Napster 等。这类网络实现简单，但往往需要大的目录服务器的支持，并且系统的健壮性不好。

（2）广播方式。没有任何索引信息，内容提交与内容查找都通过相邻接节点直接广

播传递，如 Gnutella 等。一般情况下，采取这种方式的 P2P 网络对参与节点的带宽要求比较高。

（3）动态哈希表的方式。上述两种定位方式可以依据不同的 P2P 应用环境进行选择，但是人们普遍看好 DHT（Distributed Hash Table，分散式杂凑表）方式。基于 DHT 的 P2P 网络在一定程度上可以直接实现内容的定位。一个矛盾的问题是：如果一个节点提供共享的内容表示越复杂，则哈希函数越不好选择；相应地，网络的拓扑结构就越复杂。如果内容表示简单，则又达不到真正实现依据内容定位的能力。目前大多数 DHT 方式的 P2P 网络对节点所提供共享内容的表示都很简单，一般仅仅为文件名。

3．常用 P2P 软件

常用的 P2P 软件有以下几种：

（1）Napster：世界上第一个大型的 P2P 应用网络，主要用于查找 MP3，它有一个服务器用于存储 MP3 文件的链接位置并提供检索，而真正的 MP3 文件则存放在千千万万的 PC 上，搜索到的文件通过 P2P 方式直接在 PC 间传播共享。这种方式的缺点就是需要一台服务器，在 MP3 文件版权之争火热的年代，Napster 很快就成为众矢之的，被众多唱片公司诉讼侵犯版权而被迫关闭。当然服务器一关 Napster 也就不复存在。

（2）Gnutella 和 Gnutella2：Gnutella2 是对 Gnutella 的改进和扩展。Gnutella 是开源的、第一个真正非中心的无结构 P2P 网络，文件查询采用洪泛方式。Gnutella 吸取了 Napster 的失败教训，将 P2P 的理念更推进一步：它不存在中枢目录服务器，所有资料都放在 PC 上。用户只要安装了该软件，就将 PC 立即变成一台能够提供完整目录和文件服务的服务器，并会自动搜寻其他同类服务器，从而联成一台由无数 PC 组成的超级服务器网络。传统网络的服务器和客户机在它的面前被重新定义。

（3）eDonkey。自私的人们在利用 P2P 软件的时候大多只愿“获取”，而不愿“共享”，P2P 的发展遇到了意识的发展瓶颈。不过，一头“驴”很快改变了游戏规则，这就是电驴 eDonkey，它引入了强制共享机制。eDeonkey 将网络节点分成服务器层和客户层，并且将文件分块以提高下载速度。eMule 是 eDonkey 的后继，但是更出色，采用了 DHT 来构建底层网络拓扑，是目前非常流行的 P2P 文件共享软件。

（4）BitTorrent：借助分散式服务器提供共享文件索引的混合式 P2P 网络，文件分片下载。该方式下载速度高，没有查找功能，种子具有时效性。它将中心目录服务器的稳定性同优化的分布式文件管理结合起来。

4．P2P 技术主要涉及的领域和发展方向

P2P 技术主要涉及的领域和发展方向主要有以下几种：

（1）提供文件和其他内容共享的 P2P 网络，如 eMule、BitTorrent 等。

（2）基于 P2P 方式的协同处理与服务共享平台，如 JXTA、Magi、Groove、.NETMy Service 等。

（3）即时通信交流，如腾讯 QQ 等。

（4）语音与流媒体：由于 P2P 技术的使用，大量的用户同时访问流媒体服务器，也不会造成服务器因负载过重而瘫痪，如迅雷点播、PPlive 等。

（5）网格计算，挖掘 P2P 分布计算能力。使用 P2P 技术以集中那些联接在网络上的电脑的空闲的 CPU 时间片断、内存空间、硬盘空间来替代“超级计算机”。

3.7　例题分析

为了帮助考生进一步掌握网络体系结构方面的知识，了解考试的题型和难度，本节分析 9 道典型的试题。

例题 1

实现位流透明传输的层是（1），不属于该层的协议是（2）。

（1）A．物理层　　B．数据链路层　　C．网络层　　D．传输层

（2）A．V.35　　B．RS232C　　C．RJ-45　　D．HDLC

例题 1 分析

这是一道层归属判断题，考查了物理层的归属判断。实现位流透明传输显然是“物理层”的工作职责。V.35 定义了路由器与基带 Modem 间的连线标准；RS232C 定义的是 PC 中的串口标准；RJ-45 定义的双绞线以太网卡的连接口规范；HDLC 则是数据链路层协议。

例题 1 答案

（1）A　（2）D

例题 2

物理层定义了通信设备的（3）、电气、功能、（4）的特性。

（3）A．外观　　B．机械　　C．模具　　D．物理

（4）A．规程　　B．协议　　C．通信　　D．规则

例题 2 分析

这是一道基本原理题，考查了物理层的基本特点。物理层通过一系列协议定义了通信设备的机械的、电气的、功能的、规程的特征。

- 机械：主要是连接设备的外观，连接品的规格、尺寸、数量。
- 电气：主要是设备的电压值、范围值、变化值等。
- 功能：主要是定义每个连接点所完成的功能要求。
- 规程：主要是定义通信时所采用的过程。

例题 2 答案

（3）B　（4）A

例题 3

传输层的功能是（5），该层的服务访问点是（6）。

（5）A．实现端到端的数据分组传送　　B．完成异构网络的互连
　　C．建立一个无差错的物理信道　　D．提供透明的位流传输
（6）A．IP 地址　　B．端口　　C．逻辑地址　　D．物理地址

例题 3 分析

这是一道基本原理题，考查传输层的基本特点。传输层主要负责实现发送端和接收端的端到端的数据分组传送，负责保证实现数据包无差错、按顺序、无丢失和无冗余的传输。其服务访问点为端口。

例题 3 答案

（5）A　（6）B

例题 4

在下列 4 个协议中，（7）和其他三个不属于一类，它属于（8）层。
（7）A．CONS　　B．CLNP　　C．PLP　　D．CMIP
（8）A．数据链路层　B．网络层　　C．传输层　　D．应用层

例题 4 分析

这是一道层归属判断题，考查了 OSI 典型协议。在本题中所列出的 4 个协议是 OSI/RM 定义的协议，由于实际的 Internet 中主要使用的是 TCP/IP 协议，因此，可能大多数人都对其不熟悉。

- CONS：面向连接的网络层服务协议。
- CLNP：无连接的网络层服务协议。
- PLP：X.25 网络中的分组协议，它工作于网络层。
- CMIP：公共管理信息协议，是一种网络管理协议，工作在应用层。

例题 4 答案

（7）D　（8）D

例题 5

HDLC 协议采用的帧同步方法为（9）。
（9）A．字节计数法　　B．使用字符填充的首尾定界法
　　C．使用比特填充的首尾定界法　　D．传送帧同步信号

例题 5 分析

本题考查数据链路层协议 HDLC 的基本概念。

HDLC 源于 IBM 开发的 SDLC，SDLC 是由 IBM 开发的第一个面向位的同步数据链路层协议。随后，ANSI 和 ISO 均采纳并发展了 SDLC，并且分别提出了自己的标准，ANSI 提出了高级数据链路控制规程（Advanced Data Communication Control Procedure，ADCCP），而 ISO 提出了 HDLC。

作为面向位的同步数据控制协议的典型，HDLC 只支持同步传输。但是 HDLC 既可工作在点到点线路方式下，也可工作在点到多点线路方式下；同时 HDLC 既适用于半双

工线路，也适用于全双工线路。HDLC 协议的子集被广泛用于 X.25 网络、帧中继网络以及局域网的逻辑链路控制（Logic Link Control，LLC）子层作为链路层协议以支持相邻节点之间可靠的数据传输。

例题 5 答案

（9）C

例题 6

在下面 4 个协议中，属于 ISO OSI/RM 标准第二层的是（10）。

（10）A．LAPB　　B．MHS　　C．X.21　　D．X.25 PLP

例题 6 分析

本题考查数据链路层相关的协议。

链路访问过程平衡（LAPB）是数据链路层协议，负责管理在 X.25 中 DTE 设备与 DCE 设备之间的通信和数据帧的组织过程。LAPB 是源于 HDLC 的一种面向位的协议，它实际上是 ABM （平衡的异步方式类别）方式下的 HDLC。LAPB 能够确保传输帧的无差错和正确排序。

MHS 是表示消息处理服务的缩写词。

X.21 是对公用数据网中的同步式终端（DTE）与线路终端（DCE）间接口的规定。

X.25 PLP 描述网络层（第三层）中分组交换网络的数据传输协议。PLP 负责虚电路上 DTE 设备之间的分组交换。

例题 6 答案

（10）A

例题 7

在 PPP 链路建立以后，接着要进行认证过程。首先由认证服务器发送一个质询报文，终端计算该报文的 Hash 值并把结果返回服务器，然后服务器把收到的 Hash 值与自己计算的 Hash 值进行比较以确定认证是否通过。在下面的协议中，采用这种认证方式的是（11）。

（11）A．CHAP　　B．ARP　　C．PAP　　D．PPTP

例题 7 分析

本题考查 PPP 协议的验证方式。

PAP（Password Authentication Protocol，口令验证协议）是一种简单的明文验证方式。NAS（Network Access Server，网络接入服务器）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。

CHAP（Challenge-Handshake Authentication Protocol，挑战-握手验证协议）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 Challenge String）。远程客户必须使用 MD5 单向哈希算法（One-way Hashing Algorithm）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（Remote Client Impersonation）进行攻击。

例题 7 答案

（11）A

例题 8

P2P 业务和 C/S（或 B/S）结构的业务主要差别是__（12）__。

（12）A．P2P 业务模型中每个节点的功能都是等价的，节点既是客户机也是服务器

B．P2P 业务模型中的超级节点既是客户机也是服务器，普通节点只作为客户机使用

C．P2P 业务模型与 CS 或 BS 业务模型的主要区别是服务器的能力有差别

D．P2P 业务模型与 CS 和 BS 业务模型的主要区别是客户机的能力有差别

例题 8 分析

本题主要考查对 P2P 技术的理解。

端对端技术（peer-to-peer，P2P）又称对等互联网络技术，是一种网络新技术，依赖网络中参与者的计算能力和带宽，而不是把依赖都聚集在较少的几台服务器上。请注意与 point-to-point 之间的区别，peer-to-peer 一般译为端对端或群对群，指对等网中的节点；point-to-point 一般译为点对点，对应于普通网络节点。P2P 网络通常用于通过 Ad Hoc 连接来连接节点。这类网络可以用于多种用途，各种文件共享软件已经得到了广泛的使用。P2P 技术也被使用在类似 VoIP 等实时媒体业务的数据通信中。

纯点对点网络没有客户端或服务器的概念，只有平等的同级节点，同时对网络上的其他节点充当客户端和服务器。这种网络设计模型不同于客户端-服务器模型，在客户端-服务器模型中通信通常来往于一个中央服务器。

例题 8 答案

（12）A

例题 9

有人说，P2P 应用消耗大量的网络带宽，甚至占网络流量的 90%。对此的合理解释是__（13）__。

（13）A．实现相同的功能，P2P 方式比非 P2P 方式需要传输更多数据，占用更多的

网络带宽

B．实现相同的功能，P2P 方式比非 P2P 方式响应速度更快，需要占用更多的网络带宽

C．P2P 方式总是就近获取所需要的内容，单个 P2P 应用并不比非 P2P 方式占用更多的带宽，只是用户太多，全部用户一起占用的带宽大

D．P2P 方式需要从服务器获取所需要的内容，单个 P2P 应用比非 P2P 方式需要占用更多的带宽

例题 9 分析

本题考查 P2P 的基本知识。

P2P 网络没有集中式的服务器，每台计算机既是客户机，获取信息和服务，又是服务器，为别人提供信息和服务。P2P 网络中用户总是就近获取所需要的内容，信息的传输采用标准的方式进行，因此单个 P2P 用户或应用并不比非 P2P 方式占用更多的带宽，只是用户太多，且大多数情况下，P2P 应用都是视频类的，如电影、电视节目等，数据量大，需要较大的带宽，全部用户加在一起占用的带宽非常大。

例题 9 答案

（13）C