

第 3 章

数据链路层

数据链路层是 OSI 参考模型中的第二层，介于物理层和网络层之间。数据链路层在物理层提供的服务的基础上向网络层提供服务，其最基本的服务是将源端网络层传来的数据可靠地传输到相邻节点的目标端网络层。

数据链路简称链路，故数据链路连接简称链路连接。它可分为两路存在形式，当链路非复用传送数据单元时，称为物理链路。当链路复用传送数据单元时，称为逻辑链路。

本章学习要点：

- 数据链路层设计要点
- PPP 协议的特性
- PPP 协议的帧格式
- PPP 协议的链路过程
- 使用广播信道的数据链路层
- 以太网技术

3.1 数据链路层设计要点

在第 1 章中，读者已经了解 OSI 参考模型中数据链路的一些相关知识。下面通过数据链路层的模型、数据链路层的功能以及数据链路的服务等内容，系统地学习数据链路层。

3.1.1 数据链路层的模型

数据链路层的基本服务是把源主机的网络层数据以帧为单位透明、无差错地传输给目的地主机的网络层。

数据链路层完成这一服务是通过物理连接来实现的，但具体的数据通路则要经过层间接口形成，即由网络层将数据传向数据链路层，再由数据链路层传向物理层，并由物理层发送到目的地主机。

目的地主机接收后，以相反的顺序传送到目的地主机的网络层。用户也可以将这一过程看作是两个数据链路层实体使用数据链路协议进行通信，如图 3-1 所示。

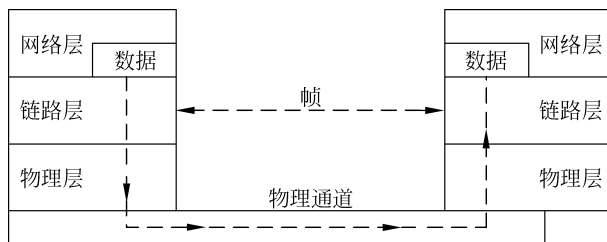


图 3-1 数据链路层模型

数据链路层为物理层加强传输原始比特流的功能，并为物理层提供

了逻辑上无差错的数据链路。同时使网络层表现为一条无差错的链路。数据链路层的基本功能是为网络层提供透明且可靠的数据传送服务。

透明性是指该层上传输的数据的内容、格式及编码没有限制，也没有必要解释信息结构的意义；可靠的传输使用户免去对丢失信息、干扰信息及顺序不正确等的担心。

注意

在计算机网络中，“链路”和“数据链路”并不是同一概念。所谓链路，是指一条没有任何中间节点的点到点的物理线路。两台计算机进行数据通信的通路正是一条一条的链路加上中间节点串接而成的。但要想在链路上传输数据，除了物理线路以外，还必须配有控制数据传输的规程。链路连同实现这些规程的软、硬件一起就构成了数据链路，在数据链路上才能进行数据通信。另外，当采用多路复用技术时，一条链路上可以有多个数据链路。所以有时为了更明确一些，也将链路称为物理链路，而将数据链路叫作逻辑链路。

3.1.2 数据链路层的功能

在计算机网络的传输介质中，由于存在各种各样的干扰以及信号的衰减，物理层链路的输入并不可靠。而数据链路层的基本功能是向网络层提供服务，将物理层提供的不可靠的物理链路通过本层的协议变为逻辑上可靠的数据链路，所以数据链路层必须具备以下主要功能。

1. 链路管理

在面向连接服务中，两台计算机进行通信时，发送方必须确知接收方是处在准备接收数据的状态。为此，通信双方必须交换一些必要的信息，建立一条数据链路，并且为保证数据传输的可靠性，做一些必要的准备（如帧序号的初始化）。

同时，在传输数据时要维持数据链路（如当在数据通信过程中，出现差错时，需要重新初始化，重新建立连接）；通信完毕时要释放数据链路，以期待建立下一次的连接。数据链路的建立、维持和释放就叫作链路管理。

2. 帧同步

在数据链路层，数据以帧为单位传送。物理层的比特流按照数据链路层协议的规定

被封装在数据帧中传送。为此，接收方应该能够从物理层上传送过来的无结构的比特流中准确地区分出一帧的开始和结束，将这一功能称为帧同步。

3. 帧的封装与拆装

在传输数据过程中，当发送方发现发送报文过长时，需要将过长的报文分成若干份分别进行传送，每一份配上一些数据链路层的控制信息换为一帧。数据传输时，以帧为单位的优点是当出现差错时可以只重新发送出差错的帧，而不需要将全部数据都重新发送。

源主机在发送数据时，要将从网络层传下来的分组附上目的地址等数据链路层控制信息构成帧，这个过程称为帧的封装。而到达目的主机时，将接收的数据信息传送网络层之前，要将发送方附上的数据链路控制信息去掉，将分组信息传送至网络层，这个过程称为帧的拆装。

4. 流量控制

在数据信息发送过程中，通信双方的数据处理速度不同，为解决这一问题双方分别建立了缓冲区。但当接收端缓存能力不足时，仍然会造成数据的丢失。

为了避免数据的丢失，源主机发送数据的速率必须使目的地主机能够来得及接收和处理。当目的地主机来不及接收时，就必须及时地控制发送端发送数据的速率。

另外，在传输过程中，由于出现差错和数据丢失等原因，目的地主机收到帧的顺序可能与源主机发送的顺序不同，在数据链路层实体将收到的信息上传网络层之前，还需要调整接收到的帧的顺序。

5. 差错控制

在源主机向目的地主机发送数据时，要求极低的误码率。因此，必须采用差错控制技术。差错控制技术要使目的地主机能够发现传送错误，并能纠正传输错误。

误码率是指发生错误的码元数与接收到的总码元数据的比率。因此，需要提供检测和纠正错误的功能，对于一些不可靠的系统，能够在数据链路层上及时发现和纠正错误，将提高系统的传输效率。

在数据链路层中广泛采用编码技术来实现差错的控制。编码技术有两大类：一类称为前向纠错方式，即当目的地主机收到有差错的数据帧时，目的地主机能够自动根据冗余码将差错纠正过来，但这种方法开销较大，不适合于计算机通信；另一类是检错重发方式，即目的地主机可以根据冗余码检测出收到的帧中是否有差错，但并不知道错在哪里，而是让发送端重复发送这一帧直到正确接收为止，但重传的次数也是有限制的。当重传多次仍然失败，则作为不可恢复的故障向上层报告，这种方法是通信过程中最常用的。

6. 区分数据信息及控制信息

由于数据和控制信息不仅在同一信道中传送，而且在许多情况下数据和控制信息还处于同一帧中，所以要采取相应措施使用目的地主机能将它们区别开来。

7. 寻址

计算机网络结构错综复杂，在多点连接的情况下，要保证每一帧能传送到正确的目的节点。接收方也应当知道发送方是哪一个节点。

3.1.3 数据链路层的服务

数据链路层服务是将源主机中来自网络层的数据传输到目的主机的网络层。通过网络层与数据链路层之间的接口，以服务原语的形式完成服务的调用与被调用，网络层调用数据链路层的服务，数据链路层为网络层提供服务，它们之间使用了标准的请求、指示、响应和确认服务原语。

数据链路层提供的服务，实际上在不同的系统中可能是不一样的。对于传输质量较高的网络，由于其传输系统的误码率很低，几乎可以省去复杂的差错控制，将检错和纠错的工作交给高层去处理；对于一些要求通信快捷、允许少量出错的实时通信系统，也可以不进行差错控制；但对于不可靠的通信系统（如无线网络），能够在数据链路层上及早发现和纠正错误，将会大大提高传输效率。

数据链路层为网络层提供的服务主要有以下 3 种。

1. 无确认的无连接服务

在这种服务中源主机和目的地主机在通信之前不建立连接，结束之后也不释放；通信双方不需要对数据帧进行确认，即对于因线路中的噪声引起的数据帧的出错或丢失情况不进行恢复。这种服务适用于局域网，因为局域网误码率低，偶尔出现的错误可以由高层解决。

2. 有确认的无连接服务

在这种服务中源主机和目的地主机在通信之前不建立连接。但源主机每发送一帧都要得到单独的确认，并具有超时重发的功能。

3. 有确认面向连接的服务

这是最复杂的服务，源主机和目的主机在进行数据传输前必须建立连接，保证数据可靠传输。这种服务分为建立连接、数据传输、断开连接 3 个阶段。

3.2 点对点协议

PPP（Point to Point Protocol，点对点协议）协议是为在两个对等实体间传输数据包，建立简单连接而设计的，主要用于广域网的连接，但在局域网的拨号连接中同样可以采用。

3.2.1 PPP 协议的特性

在 20 世纪 80 年代末，SLIP（Serial Line Internet Protocol，串行线互联网协议）因传

输性能问题阻碍了互联网的发展，于是人们开发了 PPP 协议来解决远程互联网连接的问题。

而且 PPP 协议还满足了动态分配 IP 地址的需要，并能够对上层的多种协议提供支持。无论是同步电路，还是异步电路，PPP 协议都能够建立路由器之间或者主机到网络之间的连接。

PPP 协议是目前应用得最广的一种广域网协议，它主要具有以下几方面特性。

- 能够控制数据链路的建立，方便了广域网的应用。
- 能够对 IP 地址进行分配和管理，有效地控制了所进行的网络通信。
- 允许同时采用多种网络层协议，丰富了协议的应用。
- 能够配置并测试数据链路，并能进行错误检测。保证了通信的可靠。
- 能够对网络层的地址和数据压缩进行可选择的协商。

PPP 协议主要由以下三部分组成。

- **HDLC** PPP 协议采用 HDLC (High Level Data Link Control, 高级数据链路控制) 技术作为在点对点的链路上封装数据报的基本方法。
- **LCP** PPP 协议使用 LCP (Link Control Protocol, 链路控制协议) 来建立、配置和测试数据链路。
- **NCP** PPP 协议使用 NCP (Network Control Protocol, 网络控制协议) 来建立和配置不同的网络层协议。PPP 协议允许同时采用多种网络层协议。目前，PPP 协议除了支持 IP 协议外，还支持 IPX 协议和 DECnet 协议。

3.2.2 PPP 协议的帧格式

PPP 是为在同等单元之间传输数据包这样简单的链路而设计的，这种链路提供全双工操作，并按照顺序传递数据包，为基于各种主机、网桥和路由器的简单连接提供一种共通的解决方案。

因为 PPP 是链路层协议，所以人们将它的单位称为帧，如图 3-2 所示。每一个 PPP 数据帧均是以一个标志字节起始和结束的，该字节为 0x7E (这样很容易区分出每个 PPP 帧)。

1B	1B	1B	2B	缺省 1500B	2B	1B
标志	地址	控制	协议	数据	校验	标志
7E	FF	03				7E

图 3-2 PPP 链路层协议数据帧格式

在数据帧格式中，各标志的含义如下。

- **标志 (Flag) 域** 指示一个帧的开始或结束，该域值包含二进制数 01111110。
- **地址 (Address) 域** 该域值包含二进制数 11111111，是标准的广播地址。PPP 协议不指定单个工作站的地址。
- **控制 (Control) 域** 长度为 1 个字节，该域值包含二进制数 00000011，表示用

户数据采用无序帧方式传输。它提供的无连接链路服务类似于 LLC (Logical Link Control, 逻辑链路控制) 类型提供的方法。

□ **协议 (Protocol) 域** 长度为 2 个字节, 用于标识封装在帧的数据域中的协议类型。通过确定帧序列的结尾, 为 FCS 域留出 2 个字节, 便可确定数据域的结尾。该域最大长度的默认值是 1500 字节。

□ **校验 (FCS) 域** 通常为 2 个字节。PPP 帧中包含这些额外的字节来进行差错控制。

在带宽需要付费时, 封装和帧可以减少到 2 或 4 个字节。为了支持高速的执行, 默认的封装只使用简单的字段, 多路分解只需要对其中的一个字段进行检验。默认的头和信息字段落在 32 位边界上, 尾字节可以被填补到任意的边界上。

为了在一个很宽广的环境内能够方便地使用, PPP 提供了 LCP 子协议。LCP 用于就封装格式选项自动地达成一致, 处理数据包大小的变化, 探测 looped-back 链路和其他普通的配置错误, 以及终止链路。

3.2.3 PPP 协议的链路过程

为了通过点对点链路建立通信, PPP 链路的每一端, 必须首先发送 LCP 包以便设定和测试数据链路。在链路建立之后, 点对点连接才可以被认证。

然后, PPP 必须发送 NCP 包以便选择和设定一个或更多的网络层协议。一旦每个被选择的网络层协议都被设定好了, 来自每个网络层协议的数据报就能在链路上发送了。链路将保持通信设定不变, 直到外部的 LCP 和 NCP 关闭链路, 如图 3-3 所示。

对整个过程来说, PPP 链路的连接需要经过以下 5 个阶段。

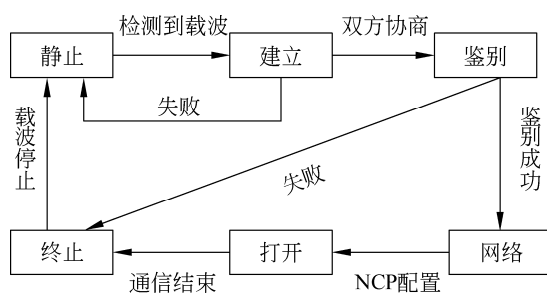


图 3-3 PPP 协议链路过程

1. PPP 链路建立准备阶段

为了在点到点连接中建立通信, PPP 连接的每一端都必须首先发送 LCP 数据包来配置和测试数据连接。

在此阶段, LCP 协议自动处在初始或正在开始状态。当进入到建立连接阶段后会引发生件, 并通知 LCP 协议。

注意

在这个阶段应用注意事项是典型的, 一个连接将在调制解调器连接断开后自动返回到此阶段。在使用电话线的连接情况下, 这个阶段将相当的短, 短到很少有足够的时间能用仪器检测到它的存在。

2. 链路建立阶段

LCP 通过交换配置数据包建立连接。一旦一个配置成功信息包 (Configure-Ack

Packet) 被发送且被接收, 就完成了交换, 进入了 LCP 开启状态。

当 LCP 协议自动进入已打开状态, 并且发送和接收过配置确认数据包时, 建立连接的交换过程才完成。

3. 认证阶段

认证阶段应该紧接在建立连接阶段后。因为, 可能有连接质量的问题并行出现, 应用时绝对不允许连接质量问题影响数据包的交换, 使认证有不确定的延迟。

认证阶段后的网络层协议阶段必须等到认证结束后才能开始。如果认证失败, 将转而进入终止连接阶段。仅仅是连接控制协议、认证协议、连接质量监测的数据包才被允许在此阶段中出现。所有其他在此阶段中接收到的数据包都将被丢弃。

注意

在这个阶段的应用注意事项有两个方面: 一是, 应用时不能简单地因为超时或缺少回应就认为认证失败。应该允许重传, 仅当试图认证的次数超过一定的限制时才进入终止连接阶段; 二是, 如果对方拒绝认证, 己方有权进入终止连接阶段。

4. 网络层协议阶段

一旦 PPP 协议完成了上述阶段, 每一个网络层协议(例如 IP 协议、IPX 协议、AppleTalk 协议) 必须单独由相应的 NCP 配置。每一个网络控制协议可以随时打开或关闭。

在此阶段, 连接上流通的包括 LCP 数据包、NCP 数据包和网络层协议数据包。

注意

在此阶段应用同样需注意两个方面: 一是, 可能一开始需要花费大量的连接时间来分析连接质量, 所以当等待对方进行网络控制协议配置时应该避免使用固定的超时限制; 二是, 当一个网络控制协议自动达到已打开的状态时, PPP 连接后就可以传送相应的网络层协议数据包。当接收到的任何所支持的网络层协议数据包时, 只要相应的网络控制协议状态中的自动状态未打开, 都将作丢弃处理。只要 LCP 协议状态中的自动状态处于打开状态, 任何接收到的不支持的协议数据包都将返回协议拒绝包(后面将提到)。所支持的协议数据包都将丢弃。

5. 链路终止阶段

PPP 连接可以随时终止, 原因可能是载波丢失、认证失败、连接质量失败、超时计数器溢出, 或者是网络管理员关闭连接。

LCP 通过交换连接终止包来终止连接。当连接正在被终止的时候, PPP 协议会通知网络层以便它采取相应的动作。

在交换过终止请求包后, 将通知物理层断开以便使连接真正终止, 尤其是在认证失败的时候。然后 PPP 协议应该进入连接死亡阶段, 结束此次 PPP 通信。

3.3 使用广播信道的数据链路层

广播信道(Broadcasting Information Channel, BCH) 是通过广播的方式传输信息的信息通道。广播的方式是指通过向所有站点发送分组的方式, 传输信息。现实中, 无线

广播电台、局域网大多采用这种方式传播分组信息。

3.3.1 局域网的数据链路层

由于局域网不需要路由选择，因此它并不需要网络层，而只需要底部的两层：物理层和数据链路层。

按 IEEE 802 标准，又将数据链路层分为两个子层：MAC（Media Access Control，介质访问控制）子层和 LLC（Logical Link Control，逻辑链路控制）子层，如图 3-4 所示。

物理层用来建立物理连接是必需的。数据链路层把数据转换成帧来传输，并实现帧的顺序控制、差错控制及流量控制等功能，使不可靠的链路变成可靠的链路也是必要的。

由于在 IEEE 802 成立之前，采用了不同的传输介质和拓扑结构的局域网的存在，这些局域网采用不同的介质访问控制方式，各有特点和适用场合。IEEE 802 无法用统一的方法取代它们，只能允许其存在。因而需要为每种介质访问方式制定一个标准，从而形成了 MAC 协议。为使各种介质访问控制方式能与上层接口并保证传输可靠，所以在其上又制定了一个单独 LLC 子层。

通过上述了解，相信读者已经对 LAN/RM（局域网参考模型）有了一个初步的认识。下面再来了解一下各层功能。

1. 物理层

物理层提供在物理实体间发送和接收比特的能力，一对物理实体能确认出两个介质访问控制（MAC）子层实体间同等层比特单元的交换。

物理层也要实现电气、机械、功能和规程四大特性的匹配。物理层提供的发送和接收信号的能力包括对宽带的频带分配和对基带的信号调制。

2. LLC 子层

LLC 子层向高层提供一个或多个逻辑接口（具有帧发和帧收功能）。发送时把要发送的数据加上地址和 CRC 检验字段构成帧。介质访问时把帧拆开，执行地址识别和 CRC 校验功能，并具有帧顺序控制和流量控制等功能。

LLC 子层还包括某些网络层功能，如数据报、虚拟控制和多路复用等。

3. MAC 子层

MAC 子层支持数据链路功能，并为 LLC 子层提供服务。它将上层交下来的数据封装成帧进行发送（接收时进行相反过程，将帧拆卸）、实现和维护 MAC 协议、比特差错检验和寻址等。

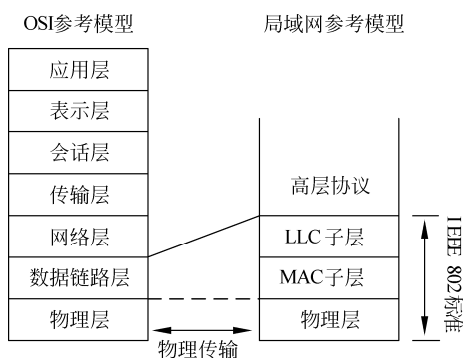


图 3-4 数据链路层分为两个子层

3.3.2 CSMA/CD 协议

CSMA/CD（Carrier Sense Multi-Access/Collision Detection，载波监听多路访问/冲突检测）是一种设备通过采用竞争的方法来获取对总线使用权的技术，它只适用于逻辑上属于总线型拓扑结构的网络，包含载波监听多路访问（CSMA）和冲突检测（CD）两方面的内容。

在网络中，一台计算机在发送数据前，首先侦听线路查看线路上是否有信息发送，用来测试线路上有无其他计算机正在发送信息。如果侦测到其他计算机正在发送信息，即信道已被占用，则该计算机在等待一段时间后再次争取发送权；如果侦听得知线路是空闲的，没有其他计算机发送信息，那么就立刻抢占信道并发送信息，如图 3-5 所示。其中，计算机侦听信道是否被占用，称之为“载波侦听”。

在计算机侦听信道是否被占用时，CSMA 技术为其提供了两种解决办法。

- 持续的载波侦听多路访问。即继续侦听线路，一直等到发现信道空闲为止。在发现信道空闲时立即抢占并发送信息。
- 非持续的载波侦听多路访问。即随机等待一定时间后，再次发送侦听信号，这样重复循环，直到发现信道空闲为止，并发送信息。

当信道处于空闲时的某一时刻，如果线路上有两台或两台以上的计算机同时发送数据时，结果导致它们同时发送数据，产生了冲突。

另一种情况，某台计算机侦听到信道是空闲的，但这种空闲可能是较远站点已经发送了信包，但由于在传输介质上信号的传播存在延时，该信包还未到此站点的缘故，如果此站点又发送信息，则也将产生冲突。

如果发生冲突，计算机停止发送数据帧，导致冲突发生的计算机，随机发送一个信号以保证网络上其他的计算机都知道已经发生冲突，使其等待一段随机时间后，重新尝试发送数据。

经过上面的介绍，可以了解到任何一个节点在发送数据前都要通过 CSMA/CD 去争取总线的使用权，其发送过程可以简单理解为“先听后说，边听边说；一旦冲突，立即停说；等待时机，然后再说”3 个部分。

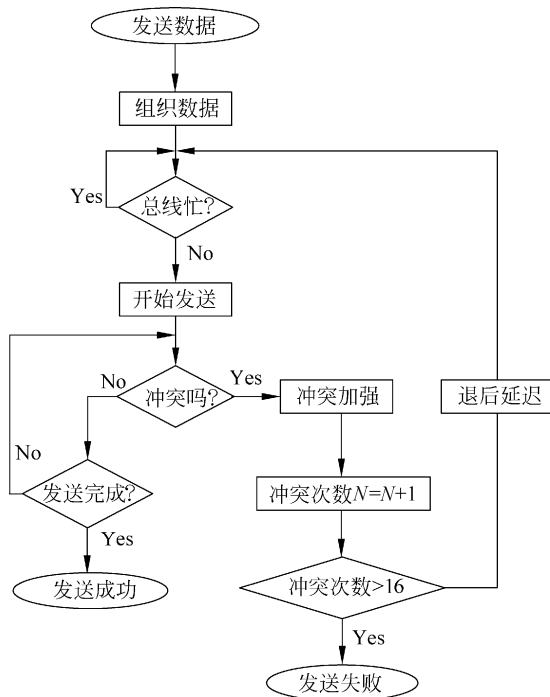


图 3-5 CSMA/CD 工作流程

3.4 以太网技术

随着计算机技术及网络技术的不断发展，以太网的技术也发生不小的变化，如从传统的以太网(10Mb/s)到快速以太网(100Mb/s)，从快速以太网到千兆以太网(1000Mb/s)，从千兆以太网到万兆以太网(10Gb/s)等。

3.4.1 传统以太网

传统以太网也被称为标准以太网或共享式以太网，是最早期的以太网，它使用载波监听多路访问/冲突检测(CSMA/CD)访问控制方法。

传统以太网的核心思想是在共享的公共传输媒体上以半双工传输模式工作，其吞吐量只有10Mb/s。传统以太网在同一时刻只能发送数据或者接收数据，但不能同时发送和接收数据，其传输介质通常采用双绞线。

1. 10Base-5

10Base-5是最早的以太网IEEE 802.3标准，它使用直径为10mm、电阻为50Ω的粗同轴电缆进行连接，它允许每段有100个站点。因此在一个网段上所有站点经过一根同轴电缆进行连接，其最大长度为500m。在设计时需要遵循5-4-3标准，在该标准中各数字代表的意义如下。

- 5表示网络中任意两个端到端的节点之间最多只能有5个电缆段。
- 4表示网络中任意两个端到端的节点之间最多只能有4个中继器。
- 3表示网络中任意两个端到端的节点之间最多只能有3个共享网段。

在使用10Base-5标准以太网时，站点必须使用收发器连接到电缆上，或者使用介质连接单元(MAU)。

2. 10Base-2

10Base-2是一个细缆以太网标准，被人们戏称为“廉价网”，它采用的传输介质是基带细同轴电缆，电阻为50Ω，数据传输速率为10Mb/s，拓扑结构为总线型，电缆段上工作站间的距离为0.5m的整数倍，每个电缆段内最多只能使用30台终端，每个电缆段不能超过185m。它也遵循5-4-3标准，电缆长度最大为925m。

10Base-2细缆可以通过BNC-T型连接器、网卡BNC连接插头直接与网卡连接。为了防止同轴电缆端头的信号反射，在同轴电缆的两个端头需要连接两个阻抗为50Ω的终端匹配器。

3. 10Base-T

1991年IEEE 802.3工作组发布了以太网10Base-T标准。它与使用同轴电缆作为传输介质的以太网不同，在10Base-T网络中采用了总线和星型相结合或单独使用星型的拓扑结构，即所有的站点均连接到一个中心集线器上，其中每个电缆段长度不能超过100m。它也遵循5-4-3标准，整个网络最大跨距为500m。

10Base-T 以太网的优点之一是故障检测较为容易，其只需使用双绞线，从根本上改变了传统局域网不易布线和维护的困难，而且不降低数据的传输速率，在使用时应注意以下规则。

- 集线器与集线器间的最大距离为 100m。
- 任何一条线路都不能形成环路。
- 双绞线与网络接口及集线器之间均采用 RJ-45 标准接口。
- 传输介质均采用非屏蔽双绞线。
- 一条链路最多可以串联 4 个集线器。

4. 10Base-F

10Base-F 是光缆以太网标准，它基于光缆互联中继器，即通过光缆链路以达到扩展传输距离的目的。它遵循 5-4-3 标准，但由于受到 CSMA/CD 的限制，其整个网络的最大跨距为 4000m。

10Base-F 使用两条光缆，其中一条光缆用于接收，另一条光缆用于发送，并定义了 FOIRL、10Base-FP、10Base-FB 和 10Base-FL 规范。

3.4.2 快速以太网

1993 年，Grand Junction 公司推出了世界上第一台快速以太网集线器 Fast Ethernet Hub10/100 和网络接口卡 FastNIC100，至此快速以太网技术才得以正式应用。随后 Intel、Synoptics、3Com、Bay Networks 等公司也相继推出了自己的快速以太网设备。1995，IEEE 802 工作组也通过了 IEEE 802.3u 标准，将以太网的带宽扩大为 100Mb/s。这样快速以太网的时代才正式到来。

从技术上讲，IEEE 802.3u 并不是一种新的标准，它是对现存 IEEE 802.3 标准的升级，其基本思想是：保留所有旧的分组格式、接口以及程序规则，只是将定时从 100ns 减少到 10ns，并且所有的快速以太网系统均使用集线器。快速以太网除了继续支持在共享介质上的半双工通信外，在 1997 年 IEEE 通过 IEEE 802.3x 标准后，其还支持在两个通道上进行的双工通信。双工通信则进一步改善了以太网的传输性能。另外，在快速以太网中所使用的网络设备与 10Mb/s 所用的网络设备相比也不贵，致使 100Base-T 快速以太网得到非常快速的发展。

100Base-T 快速以太网定义了 100Base-TX、100Base-FX 和 100Base-T4 这 3 种物理层规范。

1. 100Base-TX

100Base-TX 采用两对 5 类 UTP 双绞线（非屏蔽双绞线）或两对 1 类 STP 双绞线（屏蔽双绞线）作为传输介质。其中一对用于发送数据信息，另一对用于接收数据信息。其最大网段长度为 100m。对于 5 类 UTP 来说使用 RJ-45 连接器；对于 1 类 STP 来说使用 DB9 连接器。另外，它支持全双工的数据传输，符合 EIA586 的 5 类布线标准和 IBM 的 STP1 类布线标准。

100Base-TX 采用了一种运行在 125MHz 下的被称为 4B/5B 的编码方案,该编码方案将每 4b 的数据编制成 5b 的数据,挑选时每组数据中不允许出现多于 3 个 0,然后在将 4B/5B 码进一步编成 NRZI 码进行传输。

2. 100Base-FX

100Base-FX 可以采用单模光纤(62.5 μm)或多模光纤(125 μm)作为传输介质。在全双工传输模式下,单模光纤传输距离可达 40km,多模光纤传输距离可达 2km。它适用于高速主干网、有电磁干扰环境、要求通信保密性能良好和传输距离远等应用场合。

100Base-FX 与 FDDI 网使用相同的物理层规范,在传输中使用 4B/5B 编码方式,信号频率为 125MHz,另外它可以使用 FDDI/MIC 连接器、ST 连接器和 SC 连接器。

3. 100Base-T4

100Base-T4 采用 4 对 3 类、4 类、5 类 UTP 双绞线作为传输介质。其中,这 4 对线中的 3 对用于数据传输,1 对用于冲突检测。它使用 RJ-45 连接器,最大网段长度为 100m,与前面两种不同的是,它采用 8B/6T 编码方法。

快速以太网与原来在 100Mb/s 带宽下工作的 FDDI 网相比具有许多优点,最主要体现为快速以太网技术可以有效地保障用户在布线基础实施上的投资,它支持 3、4、5 类双绞线以及光纤的连接,能有效地利用现有的设施。

快速以太网的不足其实也是以太网技术的不足,即快速以太网仍是基于载波监听多路访问和冲突检测(CSMA/CD)技术,当网络负载较重时,会造成工作效率的下降,当然这可以使用交换技术来弥补。

3.4.3 千兆以太网

随着以太网技术的深入应用和发展,企业及各种组织对网络传输速度的要求却越来越高,高速研究组(Higher Speed Study Group)研究了将快速以太网速度增至 1000Mb/s 的可行性和实现方法。

1996 年,IEEE 标准委员会批准了千兆位以太网方案授权申请(Gigabit Ethernet Project Authorization Request)。随后 IEEE 802.3 工作组成立了 802.3z 工作委员会。IEEE 802.3z 委员会的目的是建立千兆以太网标准,它包括在 1000Mb/s 通信速率下进行全双工和半双工通信、使用 IEEE 802.3 以太网的帧格式、使用 CSMA/CD 访问控制方法来处理冲突问题、在一个冲突域中支持一个中继器(Repeater)、编址方式和 10Base-T、100Base-T 兼容。它表明千兆以太网要与以前的以太网完全兼容。

为了确保与以太网技术的向后兼容性,千兆以太网遵循了以太网对数据链路层以上部分的规定。在数据链路层以下,千兆以太网融合了 IEEE 802.3 以太网和 ANSI X3T11 光纤通道两种不同的网络技术,实现了速度上的飞跃。图 3-6 所示为三者之间的关系。

1997 年,在成立的 IEEE 802.3ab 工作组中,集中解决了使用 5 类线构造千兆以太网的标准问题,而 IEEE 802.3z 工作组则集中制定使用光纤和对称屏蔽铜缆的千兆以太网标准。

千兆以太网在处理新应用和新数据类型方面具有灵活性,它是 10Mb/s 和 100Mb/s 以太网标准 IEEE 802.3 的延伸,提供 1000Mb/s 的数据带宽。目前,千兆以太网主要有

1000Base-CX、1000Base-T、1000Base-LX 和 1000Base-SX 这 4 种技术。

1. 1000Base-CX

1000Base-CX 是使用铜缆作为网络介质的两种千兆以太网技术之一，另外一种就是将在后面介绍的 1000Base-T。它使用一种特殊规格的高质量平衡双绞线对的屏蔽铜缆，其最大传输距离为 25m，使用 9 芯 D 型连接器连接电缆，系统采用 8B/10B 编码和解码方式。

1000Base-CX 适用于交换机之间的短距离连接，尤其适合千兆主干交换机和主服务器之间的短距离连接。以上连接往往可以在机房配线架上以跨线方式实现，不需要再使用长距离的铜缆或光缆。

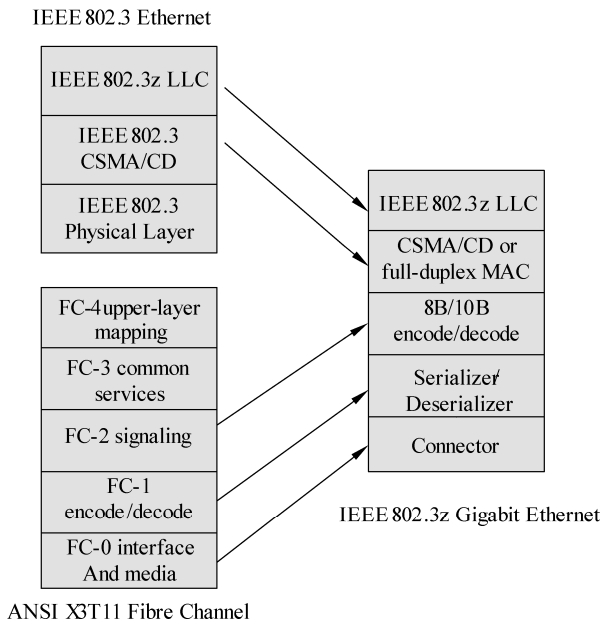


图 3-6 千兆以太网体系结构

2. 1000Base-T

1000Base-T 是一种使用 5 类 UTP 作为传输介质的千兆以太网技术，其最长传输距离与 100Base-TX 一样可以达到 100m。用户可以采用这种技术在原有的快速以太网系统中实现从 100Mb/s 到 1000Mb/s 的平滑升级。但它不支持 8B/10B 编码解码方案，需要采用专门的更先进的编码/译码机制。

3. 1000Base-LX

1000Base-LX 是一种用长波激光作为信号源的网络介质技术，在收发器上配置波长为 1270~1355nm（一般为 1300nm）的激光传输器，即可以驱动多模光纤，也可以驱动单模光纤。

1000Base-LX 使用的光纤规格为 62.5 μ m 多模光纤、50 μ m 多模光纤、9 μ m 单模光纤。其中，在使用多模光纤、全双工模式下，最大传输距离可达 550m；使用单模光纤、全双工模式下的最长距离为 5km。系统采用 8B/10B 编码方案，连接光纤所使用的 SC 型光纤连接器与快速以太网 100Base-FX 所使用的连接器型号相同。

4. 1000Base-SX

1000Base-SX 是一种使用短波激光作为信号源的网络介质技术，收发器上所配置的波长为 770~860nm（一般为 800nm）的激光传输器不支持单模光纤，只能驱动多模光纤。它包括 62.5 μ m 多模光纤和 50 μ m 多模光纤两种。使用 62.5 μ m 多模光纤、全双工模式下的最长传输距离为 275m；使用 50 μ m 多模光纤、全双工模式下最长传输距离为 550m。系统采用 8B/10B 编码方案，它使用的光纤连接器与 1000Base-LX 一样也是 SC 型连接器。

千兆以太网还利用 IEEE 802.1Q VLAN 支持、第四层过滤技术、千兆位的第三层交

换技术。千兆以太网原先是作为一种交换技术设计的，采用光纤作为上行链路，用于楼宇之间的连接。之后，在服务器的连接和骨干网中，千兆以太网获得广泛应用，由于 IEEE 802.3ab 标准（采用 5 类及以上非屏蔽双绞线的千兆以太网标准）的出台，千兆以太网可适用于任何大、中、小型企事业单位。

目前，千兆以太网已经发展成为主流网络技术。大到成千上万人的大型企业，小到几十人的中小型企业，在建设企业级局域网时都会把千兆以太网技术作为首选的高速网络技术。千兆以太网技术甚至正在取代 ATM 技术，成为城域网建设的主力军。

3.4.4 万兆以太网

随着千兆以太网标准化以及在生产实践中的广泛应用，以太网技术逐渐延伸到城域网的汇聚层。千兆以太网通常用作将小区用户汇聚到城域网节点，或者将汇聚层设备连接到骨干层。虽然以太网多链路聚合技术已完成标准化且多厂商互通指日可待，可以将多个千兆链路捆绑使用。但是考虑光纤资源以及波长资源、链路捆绑等因素，它一般只用在点内或者短距离应用环境。

为了解决由带宽及传输距离而导致以太网技术不适用于在城域网骨干/汇聚层的问题，1999 年 IEEE 标准委员会成立了 IEEE 802.3ae 工作组进行研究。在 2002 年 6 月由 IEEE 正式发布了 IEEE 802.3ae 10Gb/s 以太网标准，自此以太网的发展势头又进一步增强。这标志着万兆以太网标准的统一，使用户在选择时不必再担心厂商之间的产品不能互相兼容的问题，也规范了各厂商间的竞争。目前包括华为、3Com、Cisco、Avaya、Enterasys、Foundry 和 Riverstone 公司在内的多家厂商已经推出多款万兆以太网交换机产品，成就了今天以太网技术的全新局面。

网络拓扑结构的设计和操作也随着智能化万兆以太网多层交换机的推出发生了转变。比如第三层路由和第四层至第七层智能，包括服务质量（QoS）、服务级别（CoS）、高速缓存、服务器负载均衡、安全性和基于策略的网络功能。万兆以太网的主要特点包括以下几个方面。

- 保留 802.3 以太网帧格式。
- 保留 802.3 以太网的帧长和最小帧长。
- 只使用全双工工作模式，彻底改变了传统以太网的半双工广播工作模式。
- 使用光纤作为传输媒体，已不再适用铜缆。
- 使用点对点链路，支持星型结构的 LAN。
- 数据传输率非常高，不直接和端用户相连。
- 制定了新的光物理媒体相关（PMD）子层。
- 与 SONET OC-192 帧结构的融合，可以与 OC-192 电路和 SONET/SDH 设备仪器运行。

3.5 课堂练习：ADSL 连接 Internet

ADSL 就是一种经济廉价的宽带连接方式，它的信息传输利用的是应用最广泛的电话线或有线电视线。多用于家庭和小型办公网络，具有带宽较大、连接简单、投资较小

等优点。在本练习中,将通过 Windows 8 系统,来详细介绍创建 ADSL 连接及 ADSL 连接 Internet 网络的操作方法。

操作步骤:

- 1 右击【开始】图标,执行【控制面板】命令,选择【网络和 Internet】选项,如图 3-7 所示。



图 3-7 【控制面板】对话框

- 2 在展开的列表中选择【网络和共享中心】选项,如图 3-8 所示。



图 3-8 选择具体选项

- 3 在【网络和共享中心】对话框中,选择【更改网络设置】列表中的【设置新的连接或网络】选项,如图 3-9 所示。



图 3-9 更改网络设置

- 4 在弹出的【设置连接或网络】对话框中,选择【连接到 Internet】选项,并单击【下一

步】按钮,如图 3-10 所示。



图 3-10 选择连接类型

- 5 在弹出的对话框中,选择【宽带(PPPoE)】选项,如图 3-11 所示。



图 3-11 选择宽带类型

- 6 在弹出的对话框中输入用户名、密码、连接名称,并启用【允许其他人使用此连接】复选项,单击【连接】按钮即可,如图 3-12 所示。



图 3-12 设置连接参数

3.6 课堂练习：清理系统垃圾

Windows 优化大师是一款功能强大的系统辅助软件，它不仅提供了全面有效且简便的系统检测、系统优化和系统清理功能，而且还提供了系统维护功能以及多个附加的工具软件。通过 Windows 优化大师不仅能够有效地帮助用户清理系统垃圾、修复系统故障和安全漏洞，而且还可以检测计算机的硬件信息、维护系统的正常运转。

操作步骤：

- 1 系统优化。安装并运行 Windows 优化大师，选择【系统优化】分类列表中的【磁盘缓存优化】选项，并单击【优化】按钮，如图 3-13 所示。



图 3-13 磁盘缓存优化

- 2 选择【系统优化】分类列表中的【开机速度优化】选项，在列表框中启用相应的复选框，并单击【优化】按钮，如图 3-14 所示。

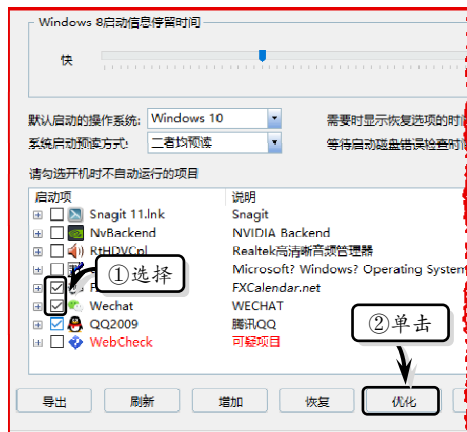


图 3-14 开机速度优化

- 3 系统清理。选择【系统清理】分类列表中的【注册信息清理】选项，在【请选择要扫描的项目】列表框中选择扫描项，单击【扫描】按钮，如图 3-15 所示。

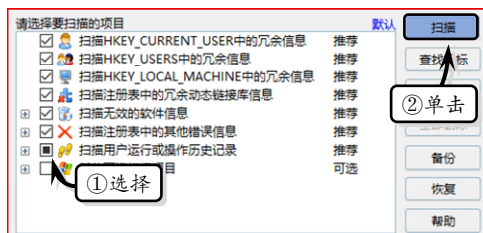


图 3-15 扫描注册表信息

- 4 扫描结束后，单击【全部删除】按钮，在弹出的提示对话框中单击【否】按钮，然后在弹出的提示对话框中单击【确定】按钮，如图 3-16 所示。

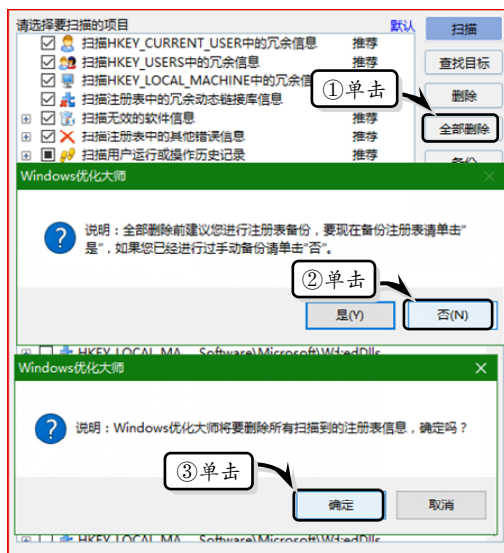


图 3-16 删除扫描项

- 5 选择【系统清理】分类列表中的【磁盘文件管理】选项，选择需要扫描的磁盘，单击【扫描】按钮，如图 3-17 所示。

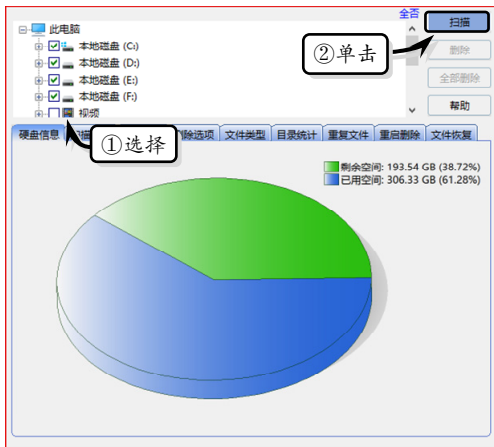


图 3-17 选择扫描磁盘

- 6 扫描结束之后，在【扫描结果】选项卡中，将显示扫描结果，单击【全部删除】按钮，删除扫描项，如图 3-18 所示。
- 7 选择【系统清理】分类列表中的【历史痕迹清理】选项，在【请选择要扫描的项目】列表框中选择扫描项，单击【扫描】按钮，如图 3-19 所示。
- 8 扫描结束之后，将在下方列表框中显示扫描结果，单击【全部删除】按钮，删除扫描项，如图 3-20 所示。

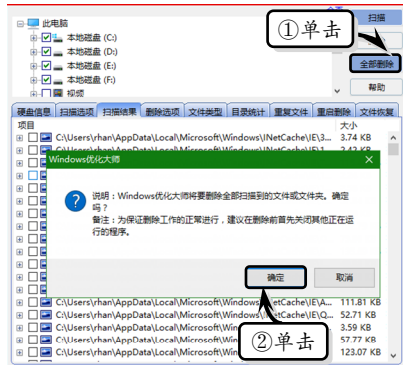


图 3-18 删除扫描项

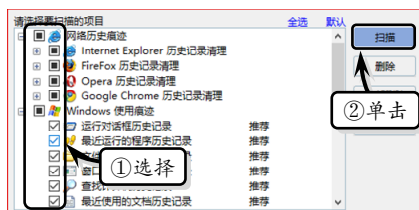


图 3-19 选择扫描项



图 3-20 删除历史痕迹

3.7 思考与练习

一、填空题

- 在数据链路层，数据的传送单位是_____。
- 在计算机通信中，采用_____方式进行差错控制。
- 所谓_____就是不管所传数据是什么样的比特组合，都应当能够在链路上传送。
- 物理层要解决_____同步的问题；数据链路层要解决_____同步的问题。
- 所谓_____就是从收到的比特流中

正确无误地判断出一个帧从哪个比特开始以及到哪个比特结束。

- Internet 中使用最广泛的数据链路层协议是_____和_____协议。
- 数据链路层最重要的作用就是通过一些_____协议，在不太可靠的物理链路上实现_____数据传输。

二、选择题

- 无论是 SLIP 还是 PPP 协议，都是_____。
A. 物理层 B. 数据链路层

- C. 网络层 D. 传输层
2. HDLC 是_____。
- A. 面向字符型的同步协议
B. 面向比特型的同步协议
C. 异步协议
D. 面向字计数的同步协议
3. _____是数据链路层的通信设备之一。
- A. 路由器 B. 中继器
C. 网桥 D. 网关

三、问答题

1. 在停止等待协议中，应答帧为什么不需要序号？
2. HDLC 帧字段的意义是什么？
3. 什么是零比特填充法？
4. 数据链路（逻辑链路）与链路（物理链路）有何区别？
5. 正常响应方式的特点是什么？

四、上机练习

1. 查看主机 TCP/IP 连接状态

Netstat 是在内核中访问网络及相关信息的程序，它能提供 TCP 连接、TCP 和 UDP 监听、进程内存管理的相关报告。在 Windows 10 系统中，如果用户需要查看主机当前的 TCP/IP 连接状态，可以右击桌面上的【此电脑】图标，执行【属性】命令，在打开的对话框中查看计算机的名称，如图 3-21 所示。

然后，单击【开始】按钮，执行【运行】命令，输入“cmd”并单击【确定】按钮。在弹出的 MS-DOS 窗口中，输入“netstat ran”命令，即可查看 TCP/IP 网络连接状态，如图 3-22 所示。

2. 查看跟踪路由节点

Tracert 是路由跟踪实用程序，用于确定 IP 数据报访问目标所采取的路径。如果用户需要查看从用户自己到目标逐级到底经过了哪些路径。右击【开始】按钮，执行【运行】命令，输入“cmd”

并单击【确定】按钮。在弹出的 MS-DOS 窗口中，输入“tracert www.ncie.gov.cn”命令，然后等待片刻，就会看到用户经过的一个个路由节点，如图 3-23 所示。



图 3-21 查看计算机名称

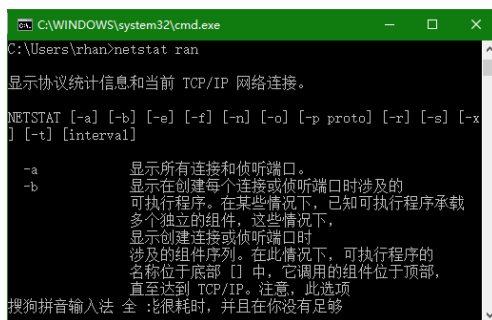


图 3-22 查看 TCP/IP 的网络连接状态



图 3-23 查看跟踪路由节点