第 3 章

数据链路层协议

数据链路层位于 OSI/RM 参考模型中自底而上的第二层，介于物理层和网络层之间。数据链路层利用物理层提供的服务，且在此基础上向网络层提供服务。数据链路层的基本服务是把源主机网络层的数据，以帧为单位，透明、无差错地传输给目标主机的网络层。数据链路层通常涉及以下基本问题：

- 如何将数据组成数据帧(Frame)；
- 如何控制帧在物理信道上的传输，包括如何处理传输差错，如何进行流量控制；
- 如何管理数据链路的建立、维持和释放。

本章分为两部分。第一部分包括 3.1 节，涉及数据链路层协议的基础知识。第二部分包括 3.2 节、3.3 节和 3.4 节，内容涉及 PPP、以太网和 IEEE 802.11 协议的原理、协议分析和仿真。

3.1 数据链路层协议概述

数据链路层的任务是将网络层交付的数据报通过一段链路从一个站点传输到相邻站点。数据链路层协议交换的数据单元称为帧(Frame)，每个数据链路层的帧通常封装了网络层的一个数据报，该封装过程称为成帧。数据链路层协议定义了在链路两端的站点之间交互的帧格式，以及当发送和接收帧时，站点所采取的操作。在发送帧前，数据链路层首先要进行成帧操作，接下来接收帧，其可以选择的操作包括差错检测、可靠传输、流量控制和随机接入等。著名的数据链路层协议包括点到点协议(Point to Point Protocol，PPP)、以太网和 IEEE 802.11 协议。

数据链路层的基本服务是将网络层分组通过通信链路从一个站点移动到相邻站点，设计数据链路层协议通常涉及以下基本问题。

1. 成帧(Framing)

数据链路层的帧在链路上传输之前，需将每个网络层数据报用数据链路层的帧封装起来。如何确定帧的边界位置即帧定界非常重要。帧定界通常采用识别特殊的帧序列来进行。帧通常由若干首部字段和一个数据字段组成，其中网络层数据报就承载在其数据字段中。事实上，除了首部字段外，部分帧协议还可能包括帧尾部字段，而这种首部字段和尾部字段可以统称为首部字段。帧的特定结构由所使用的数据链路层协议进行规定。

2. 差错检测(Error Detection)

帧在传输过程中，由于信道上存在信号衰减和电磁噪声等因素，其中的某个比特位 1

在接收方可能被判断为0,反之亦然。大部分的数据链路层协议能够提供一种机制来检测是否存在差错,例如发送方系统在帧中设置差错检测比特,接收方系统采用同样的方法进行差错检测,若产生的差错检测比特不同,就通知对方重新发送该帧,直至得到正确帧为止。数据链路层的差错检测通常用硬件实现。与差错检测不同,差错纠正(Error Detection)通过引入更多的冗余比特,不仅能够检测出帧中存在的差错,而且能够准确地判断帧中差错出现的位置,进而纠正差错。

3. 可靠交付(Reliable Delivery)

当数据链路层提供可靠交付服务时,将保证无差错地经过链路传输每个帧。对于比特差错率极低的光纤、铜缆和双绞线构成的数据链路层,通常认为引入数据链路层的可靠交付服务会带来不必要的开销,会严重影响网络的数据传输速率,偶尔出现的差错可以由位于网络边缘的传输层来处理。但对于差错率较高的无线链路,一般都会在链路层采用可靠交付措施,因为将差错交由高层协议来处理,将导致整个网络系统的低效。

4. 媒体访问(Medium Access)

媒体访问控制(Medium Access Control,MAC)协议规定了站点在链路上传输帧的规则。当链路两端仅有一个站点时,MAC协议比较简单,因为不会出现帧碰撞,所以收发双方无需协调发送帧的顺序。但对于多个站点共享一条通信信道时,就必然会遇到多路访问(Multiple Access)问题,即多个站点经过同一共享信道通信,进而出现碰撞和复用/分用解问题,此时需要使用MAC协议协调多个站点之间的帧传输。

5. 流量控制(Flow Control)

链路上的站点具有缓存帧的能力,但其缓存能力通常是有限的。如果发送站点发送分组过快,就可能造成接收站点缓存区溢出,从而造成帧丢失,数据链路层协议需要提供某种流量控制策略,以解决该问题。但数据链路层的流量控制服务会引入不必要的开销,并且会严重影响网络的数据传输速率,同时增加网络核心设备的成本,因此流量控制服务通常由位于网络边缘的高层协议进行处理。

3.2 PPP协议分析

3.2.1 PPP协议概述

PPP(Point to Point Protocol,点到点协议)是为点对点链路上传输多种协议的数据包提供的一种标准方法,其最初的设计目的是为两个对等站点之间的IP传输提供一种封装协议。除了IP协议以外,PPP协议还可以封装其他协议,包括Novell的IPX(Internetwork Packet Exchange,网间分组交换)协议等。早在1994年7月,IETF就对PPP协议进行了标准化(RFC 1661),至今,PPP协议仍然在广泛应用。

PPP协议规定了以下内容:

- 帧格式;
- 用于建立、配置和测试PPP链路的LCP(Link Control Protocol,链路控制协议);
- 用于建立、配置网络层协议的NCP(Network Control Protocol,网络控制协议),

对于 IP 网络，使用 IPCP(IP Control Protocol，IP 控制协议)协议；

- 若需要认证时，可选用 PAP(Password Authentication Protocol，口令认证协议)和 CHAP(Challenge Handshake Authentication Protocol，基于挑战的握手认证协议)。

1. PPP 协议流程

在建立、保持和终止 PPP 链路的过程中，PPP 链路需要经过 5 个阶段，除认证阶段外，其他 4 个阶段都是必要阶段。PPP 协议链路转换过程如图 3.1 所示。

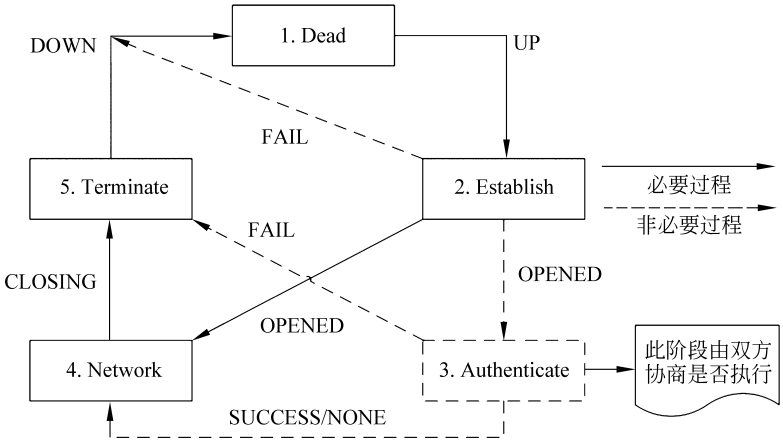

图 3.1　PPP 协议链路转换过程

(1) 链路不可用阶段(Dead)

链路状态的起始点和终止点，当一个外部事件(例如检测到载波信号)指出物理层已经准备就绪时，就进入“链路建立阶段”。

(2) 链路建立阶段(Establish)

通信双方使用 LCP 协议进行参数协商、配置链路。若协商成功，进入“认证阶段”，否则回到“链路不可用阶段”。

(3) 认证阶段(Authenticate)

认证阶段不是必要过程，若发起方希望根据某一特定的认证协议进行认证，则发起方必须在“链路建立阶段”，声明要求使用的认证协议，常用的认证协议有 PAP 和 CHAP。认证应尽可能在链路建立后立即进行，在认证完成之前，禁止从“认证阶段”进入到“网络层协议阶段”。若认证失败，则进入“链路终止阶段”。

(4) 网络层协议阶段(Network)

在传输数据之前，需要使用 NCP 协议协商双方通信时的参数，通常会进行 IP 地址的协商。若协商成功，双方开始通信，否则进入“链路终止阶段”。

(5) 链路终止阶段(Terminate)

PPP 协议可以在任何时刻终止链路，PPP 链路终止后，物理层链路仍然可用。通信方收到对方发出的链路终止请求时，应给予确认。若载波信号丢失或停止时，应回到“链路不可用阶段”。

2. PPP 帧格式

PPP 帧格式如图 3.2 所示。

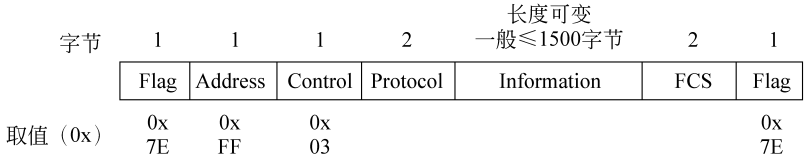

图 3.2 PPP 协议帧格式

Flag 字段为帧定界标志，用于标识 PPP 帧的开始与结束，长度为 1 字节，取值固定为 0x7E。若两个 Flag 字段紧靠在一起，表示该 PPP 帧未包含任何数据，此外，连续传送 PPP 帧时，会省略标识结束用的 Flag 字段，此时每一帧之间只用一个 Flag 字段加以区分，连续多帧省略结束 Flag 标志的示例如图 3.3 所示。

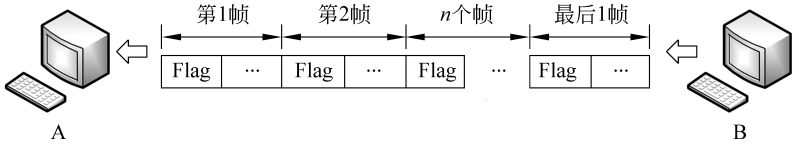

图 3.3 PPP 协议省略结束 Flag 标志示例

Address 字段为地址字段，用于标识接收方的地址，长度为 1 字节，因点到点链路的接收方是唯一的，故此字段取值固定为 0xFF，表示只有对方才能接受到数据。

Control 字段为控制字段，长度为 1 字节，取值固定为 0x03，表示无序号信息（Unnumbered Information）。

Protocol 字段为协议字段，用于标识 PPP 帧封装的协议数据类型，长度为 2 字节。此字段使 PPP 得以封装不同的协议。其部分取值和含义见表 3.1。

Information 字段为信息字段，该字段长度不固定，最大长度等于 MRU（Maximum Receive Unit）值，默认为 1500 字节。此字段存放承载的协议数据，包括 LCP、NCP 等。

FCS（Frame Checksum）字段为帧校验和字段，用于检测 PPP 帧的完整性，长度为 2 字节。

表 3.1 Protocol 字段取值及含义

字 段 值	协 议
0x0021	IP（Internet Protocol）
0x0029	Appletalk
0x8021	IPCP（Internet Protocol Control Protocol）
0xC021	LCP（Link Control Protocol）
0xC023	PAP（Password Authentication Protocol）
0xC025	LQR（Link Quality Report）
0xC223	CHAP（Challenge Handshake Authentication Protocol）

3. LCP

LCP(Link Control Protocol,链路控制协议)用于建立、配置、维护和终止 PPP 链路。当使用 PPP 协议通信的双方需要建立链路时,发起方发送 LCP 报文给对方,该报文中承载了建立链路需要协商的各种参数,若双方协商成功,则链路成功建立,否则,由发起方决定是否需要再次协商。

LCP 协议负责 PPP 的链路管理,其与具体的上层(网络层)协议无关,无论 PPP 封装的是 IP、IPX 协议,还是其他协议,都使用相同的 LCP 协议进行链路管理。

当 PPP 帧中 Protocol 字段为 0xC021 时,表示 Information 字段的数据为 LCP 报文。LCP 报文的格式如图 3.4 所示。

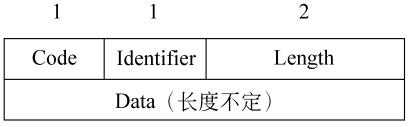

图 3.4　LCP 报文格式

(1) LCP 报文的种类

LCP 报文从功能上进行划分,可分为三大类型:链路配置报文、链路终止报文和链路维护报文,每种类型具有不同的报文格式,LCP 报文的功能与报文的对应关系如表 3.2 所示。

① 链路配置报文

链路配置报文用于链路建立和配置,4 种常用的链路配置报文说明如下。

- **Configure-Request(配置请求)**

当需要建立逻辑链路时,发起方发送 Configure-Request(配置请求)报文,用于协商参数;若接收方对收到的每个配置选项值都可以接受时,则回送 Configure-Ack(配置确认)报文;若收到的配置选项可以识别,但部分配置选项参数不能接受,则回送 Configure-Nak(配置否认)报文,并标示出需要重新协商的配置选项;若配置选项不可识别或不可接受,则回送 Configure-Reject(配置拒绝)报文。

Configure-Request 的 Code 字段值为 0x01,Data 字段值为 1 到多个选项(Options)列表,选项列表中的参数可同时进行协商。选项字段格式如图 3.5 所示。

表 3.2　LCP 功能与报文的对应关系

类　型	功　能	报文类型	报文代码
链路配置	建立和配置链路	Configure-Request	1
		Configure-Ack	2
		Configure-Nak	3
		Configure-Reject	4
链路终止	终止链路	Terminate-Request	5
		Terminate-Ack	6

续表

类　型	功　能	报文类型	报文代码
链路维护	管理和调试链路	Code-Reject	7
		Protocol-Reject	8
		Echo-Request	9
		Echo-Reply	10
		Discard-Request	11

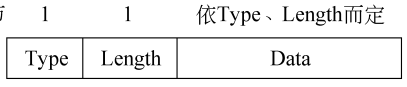

图 3.5　选项字段格式

Type 为类型字段，用于区分不同的协商参数，Type 字段对应参数及功能如表 3.3 所示。

Length 为长度字段，Length 字段指出该配置选项（包括 Type、Length 和 Data 字段）的长度。

Data 为数据字段，Data 字段为零或者多个八位字节，其中包含配置选项的特定详细信息。若 Data 字段的数据长度超过 Length 字段所指出的长度，则接收方应丢弃整个配置报文。

表 3.3　Type 字段对应参数及功能

Type 值	对应参数	功　能
0x00	Reserved	保留
0x01	Maximum Receive Unit	最大接收单元
0x02	Asynchronous Control Character Map	异步控制字符映射
0x03	Authentication Protocol	认证协议
0x04	Quality Protocol	质量协议
0x05	Magic Number	幻数
0x07	Protocol Field Compression	协议域压缩
0x08	Address and Control Field Compression	地址及控制域压缩

LCP 常用的 7 种选项如下：

最大接收单元（Maximum Receive Unit，MRU）　用于通告对方可以接收的最大报文长度，一般默认值是 1500 字节。此选项 Type 字段取值 0x01，Length 字段为 0x04，Data 字段占 2 字节，指出最大报文长度。

异步控制字符映射（Asynchronous Control Character Map，ACCM）　字段用于协商在异步链路中透明传输控制字符的方法。

认证协议(Authentication Protocol,AP)　用于向对方通告所使用的认证协议。此选项 Type 字段为 0x03,Length 字段的值大于或等于 0x04,Data 字段分为两个部分,前半部分是 2 字节的认证协议字段,指出认证阶段想要使用的认证协议,若取值为 0xC023,则使用 PAP 认证协议,若取值为 0xC223,则使用 CHAP 认证协议;后半部分是具体配置协议跟随的附加数据。

质量协议(Quality Protocol,QP)　用于向对方通告所使用的链路质量监控协议。此选项 Type 字段取值为 0x04,Length 字段的值大于或等于 0x04,Data 字段分为两个部分,前半部分是 2 字节的质量协议字段,指出链路想要使用的质量监测协议,一般取值为 0xC025,代表 LQR(Link Quality Report,链路质量报告);后半部分是具体质量协议的附加数据。

幻数(Magic Number,MN)　字段用于监测网络中是否有自环现象。若通信的一方发现自己最近发出的报文中包含的幻数总是与最近收到的幻数相同,即可判定出现了回路。此选项 Type 字段取值为 0x05,Length 字段取值为 0x06,Data 字段为 4 字节的幻数值。

协议域压缩(Protocol Field Compression,PFC)　字段用于通知对方可以接收"Protocol"字段经过压缩的帧。此选项 Type 字段取值为 0x07,Length 字段取值为 0x02,无 Data 字段。

地址及控制域压缩(Address and Control Field Compression,ACFC)　字段用于通知对方可以接收"Address"和"Control"字段经过压缩的 PPP 帧。此选项 Type 字段取值为 0x08,Length 字段取值为 0x02,无 Data 字段。

图 3.6 给出了一个 LCP Configure-Request 报文的示例。在此 PPP 帧中,Protocol 域取值为 0xC021,标识其后的 Data 字段部分封装的是 LCP 报文。LCP 报文代码字段取值为 0x01,标识为 0x01,长度 24,标识该 LCP 报文为 Configure-Request 报文,总长度是 24 字节。其后是各部分协商的内容,包括 MRU 为 1500 字节,使用 PAP 认证协议作为认证协议,质量协议使用 LQR。

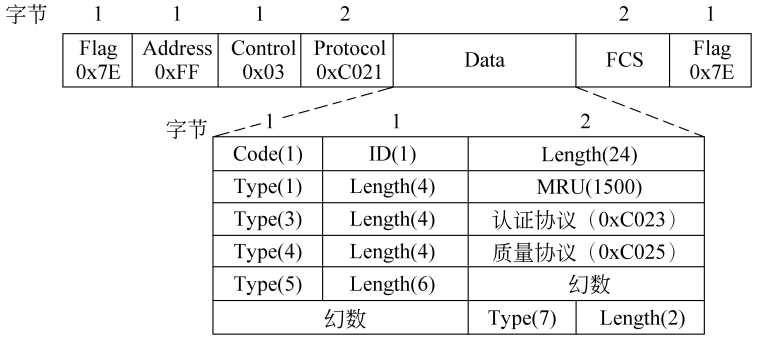

图 3.6　LCP Configure-Request 报文示例

- **Configure-Ack(配置确认)**

若接收的 Configure-Request 报文中的每一个配置选项值都可接受,则回送

Configure-Ack(配置确认)报文,回送的 Configure-Ack 报文中的 Identifier 字段必须与最后接收的 Configure-Request 报文相匹配。此外,Configure-Ack 报文中的配置选项必须与最后接收的 Configure-Request 报文完全匹配。

Configure-Ack 报文中的 Code 字段值为 0x02,Data 部分包含零到多个确认配置选项列表。配置选项的格式与 Configure-Request 报文相同。

- **Configure-Nak(配置否认)**

若收到的每个配置选项都可以识别,但是配置选项值不能接受,则接收方必须回送 Configure-Nak。配置选项部分仅用不能接受的配置选项进行填充,回送的 Configure-Nak 报文中的 Identifier 字段必须与最后接收的 Configure-Request 报文相匹配。

Configure-Nak 报文的 Code 字段值为 0x03,Data 部分包含零到多个没有确认的配置选项列表,配置选项的格式与 Configure-Request 报文相同。

- **Configure-Reject(配置拒绝确认)**

若收到的部分配置选项是不可识别或不能接受,则回送 Configure-Reject 报文。配置选项部分仅用不能接受的配置选项进行填充,回送的 Configure-Reject 报文中的 Identifier 字段必须与最后接收的 Configure-Request 报文相匹配。

Configure-Reject 报文中的 Code 字段值为 0x04,Data 部分包含零到多个没有确认的配置选项列表,配置选项的格式与 Configure-Request 报文相同。

② 链路终止报文

链路终止报文用于链路的释放,包括两种报文,分别是 Terminate-Request(终止请求)报文和 Terminate-Ack(终止应答)报文。链路终止报文的格式和 LCP 报文格式一致(如图 3.4 所示),也由 Code、Identifier、Length 和 Data 字段组成。其中 Code 字段取值为 0x05 和 0x06,Length 字段指出该配置选项的总长度。数据字段可为空,也可以是发送方自定义的数值,例如链路终止原因的描述等。

③ 链路维护报文

链路维护报文用于链路的管理和调试。LCP 规定了 5 种链路维护报文,其中 Code-Reject(代码拒绝)和 Protocol-Reject(协议拒绝)报文用于报告 Code 及 Protocol 字段的错误,Echo-Request(回复请求)和 Echo-Reply(回复应答)报文用于链路质量和性能测试,Discard-Request(丢弃请求)报文用于辅助调试从发送方到接收方的链路状态,对方在接收到这种报文后,应直接丢弃。

- **Code-Reject(代码拒绝)**

Code-Reject(代码拒绝)报文表示无法识别报文的 Code 字段,Code 字段值为 0x07。若收到该类错误,应立即终止链路,该报文的格式如图 3.7 所示,其中"被拒绝的报文"字段包含了无法识别的 LCP 报文。

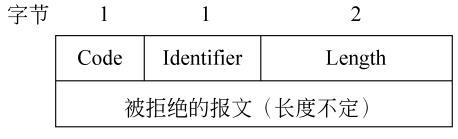

图 3.7 Code-Reject 报文格式

- **Protocol-Reject(协议拒绝)**

Protocol-Reject(协议拒绝)报文表示无法识别报文的 Protocol 字段,Code 字段值为 0x08。若收到该类错误,应停止发送该类型的协议报文,该报文的格式如图 3.8 所示,其

中“被拒绝的协议”字段指明了无法识别的协议，“被拒绝的信息”字段包含了被拒绝的 PPP 帧的数据区。

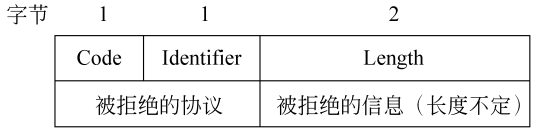

图 3.8　Protocol -Reject 报文格式

- **Echo-Request（回复请求）和 Echo-Reply（回复应答）**

Echo-Request（回复请求）和 Echo-Reply（回复应答）报文用于链路质量和性能测试，Code 字段值为 0x09 和 0x0A，其格式如图 3.9 所示。

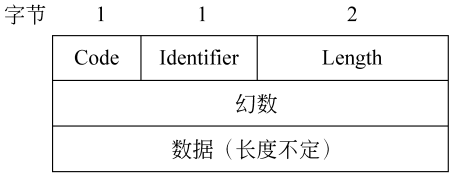

图 3.9　Echo-Request 和 Echo-Reply 报文格式

- **Discard-Request（丢弃请求）**

Discard-Request（丢弃请求）报文用于辅助错误调试，无实质用途。其 Code 字段值为 0x0B。该报文收到即会丢弃，其格式与 Echo-Request 和 Echo-Reply 报文格式相同（如图 3.9 所示）。

（2）LCP 报文工作流程

LCP 报文的工作流程可以分为 3 种：包括链路建立和配置流程、链路终止流程和链路维护流程。

① 链路建立和配置流程

当需要建立链路时，发起方发送 Configure-Request 报文，用于协商参数；若接收方对收到的配置选项和其值均可接受，则回送 Configure-Ack 报文，经过双方一到多次的交互，PPP 链路成功建立；若收到的配置选项可识别，但部分参数不能接受，则回送 Configure-Nak 报文，并标示出需要重新协商的参数，其后发起方会再次进行协商；若有参数不可识别或不能接受，则回送 Configure-Reject 报文，由发起方决定是否再次协商。PPP 链路建立和配置流程如图 3.10 所示，在实际的 PPP 链路建立过程中，不一定能观察到 Configure-Nak 和 Configure-Reject 报文。

② 链路终止流程

若通信的一方要终止链路时，需向对方发送 Terminate-Request 报文，并且在收到 Terminate-Ack 报文响应前，应该不断发送；接收方在接收到 Terminate-Request 报文时，必须响应 Terminate-Ack 报文。PPP 链路终止流程如图 3.11 所示，若载波信号丢失或停止，通信双方间不存在链路终止流程，则直接回到“链路不可用阶段”。

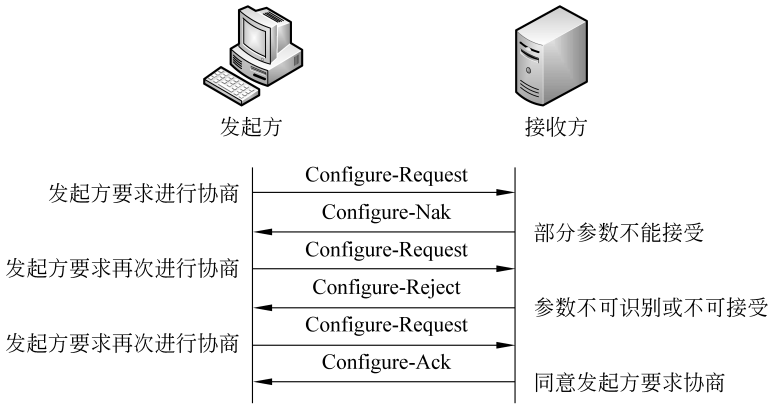

图 3.10　PPP 链路建立和配置流程

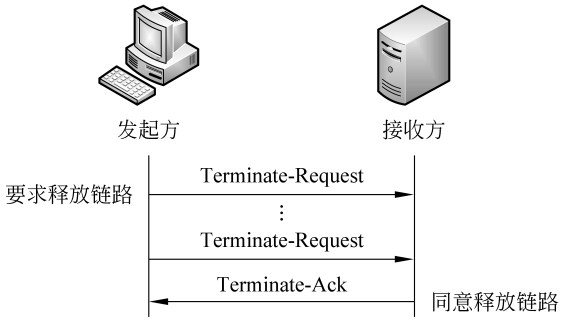

图 3.11　PPP 链路终止流程

③ 链路维护流程

在链路维护期间，LCP 协议使用消息来提供反馈和测试链路。PPP 链路维护流程示例如图 3.12 所示。

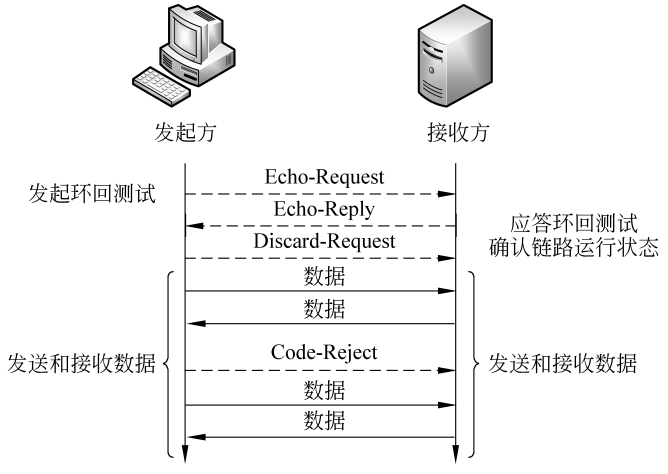

图 3.12　PPP 链路维护流程示例

其中 Echo-Request、Echo-Reply 和 Discard-Request 报文可用于测试链路。例如，发起方若想对链路进行环回测试时，其发送 Echo-Request 报文，接收方收到 Echo-Request 报文后，回应 Echo-Reply 报文，通过该过程除完成握手以外，还可通过对幻数字段的检测，判定网络是否发生自环现象，若链路发生了自环，则应采取相应措施对链路复位。如果 PPP 发送的 Echo-Request 报文产生丢失，则在连续丢失最大允许丢失的个数之后，也会将链路复位，以免过多的无效数据传输。

Code-Reject 和 Protocol-Reject 报文用于数据通信期间，也就是用于发送和接收数据的过程中，如果无法识别报文的 Code 字段或无法识别报文的 Protocol 字段，可使用这两种报文来提供反馈。例如，如果从对方那里收到无法解释的报文，则回应 Code-Reject 报文。

4. NCP

通过 LCP 将各种链路参数协商成功后，通信双方就建立了逻辑链路，若发起方希望进行认证，则进入认证阶段，确认对方的合法性。认证成功后，还需要进一步协商上层（网络层）的一些参数，此时需要使用 NCP（Network Control Protocol，网络控制协议）进行参数协商。

不同的网络层协议会使用不同的 NCP 协议，例如：IP 协议使用 IPCP（Internet Protocol Control Protocol，IP 控制协议）进行协商，Appletalk 协议使用 Appletalk NCP 进行协商，Novell 的 IPX 协议使用 IPE（Internet Packet Exchange，互联网包交换协议）进行协商。因目前较为广泛应用的协议是 TCP/IP，故本书只介绍 IPCP。

若 PPP 帧中 Protocol 字段取值为 0x8021 时，表示 PPP 帧正在使用 IPCP 协议协商相关通信参数，IPCP 协议完成协商 IP 地址等工作后，该 PPP 链路上就可以传送 IP 数据报；若 IP 数据报传送完毕，若要关闭 IP 协议，则仍需通过 IPCP 协议协商终止，此时 PPP 的链路仍然存在，若要释放链路，则需借助 LCP 协议。

（1）IPCP 格式

IPCP（Internet Protocol Control Protocol，IP 控制协议）报文格式和 LCP 报文的格式非常相似，其格式如图 3.13 所示。

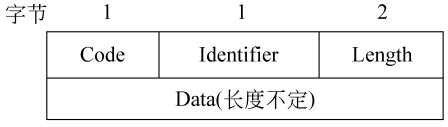

图 3.13　IPCP 报文格式

Code 为代码字段（也称类型字段），长度为 1 字节，用于标识 IPCP 报文的类型。IPCP 与 LCP 的配置协商流程类似，其报文类型有 7 种：Configure-Request、Configure-Ack、Configure-Nak、Configure-Reject、Terminate-Request、Terminate-Ack 和 Code-Reject，常见的代码如表 3.4 所示。注意，虽然 IPCP 和 LCP 非常相似，甚至连 Code 字段值都类似，但 IPCP 仅负责 TCP/IP 网络层相关传输参数的设置。

Identifier 为标识字段，长度为 1 字节，为报文的唯一标识，Identifier 字段用于匹配请

求和回复。

Length 为长度字段，长度为 2 字节，Length 字段指出该报文的长度，包括 Code、Identifier、Length 和 Data 的长度。

Data 为数据字段，长度可以是零或多个八位字节，由 Length 字段声明。Data 字段的格式由 Code 字段决定。

表 3.4 IPCP 代码与报文类型对应关系

Code(代码)	IPCP 报文类型
0x01	Configure-Request
0x02	Configure-Ack
0x03	Configure-Nak
0x04	Configure-Reject
0x05	Terminate-Request
0x06	Terminate-Ack
0x07	Code-Reject

(2) IPCP 配置选项

IPCP 协议中，通信双方可协商的配置选项有 3 种：多个 IP 地址(IP-Addresses)、IP 压缩协议(IP Compression Protocol)和 IP 地址(IP Address)。

- 多个 IP 地址(IP-Addresses)　由于多个 IP 地址很难全部协商成功，故本选项很少使用。
- IP 压缩协议(IP Compression Protocol)　本选项用于协商使用的压缩协议。IPCP 协议中仅规定了“Van Jacobson”一种压缩协议，编号为 0x002D，Type 字段取值为 0x02。该选项默认值为不进行压缩。
- IP 地址(IP Address)　若发起方请求对方分配一个 IP 地址，接收方收到后会返回一个合法的 IP 地址。此时，报文 Type 字段设置为 0x03，Length 字段设置为 0x6，其后 4 字节全为 0x00，指明由对方提供 IP 地址。

图 3.14 给出一个 IPCP 协议 Configure-Request 报文示例。在该 PPP 帧中，Protocol 字段取值为 0x8021，表示数据部分为 IPCP 报文；Code 字段为 0x01，Identifier 字段为 0x05；Length 字段额外为 0x10，指示该报文为 Configure-Request 报文，总长度为 16 字节；其后是各部分的协商参数，指定 Van Jacobson 为压缩协议，由对方提供 IP 地址。

5. PAP

PPP 中，常用的认证协议有 PAP(Password Authentication Protocol，口令认证协议)和 CHAP(Challenge Handshake Authentication Protocol，基于挑战的握手认证协议)。PAP 的整个认证流程非常简单，这是 PAP 最大的优点，但 PAP 认证只能在链路建立阶段进行，身份和口令以明文进行传输，安全性低；CHAP 协议可以在链路建立和数据通信阶段多次使用，同时安全性较高。目前 PPP 协议的认证阶段多使用 CHAP 认证协议。

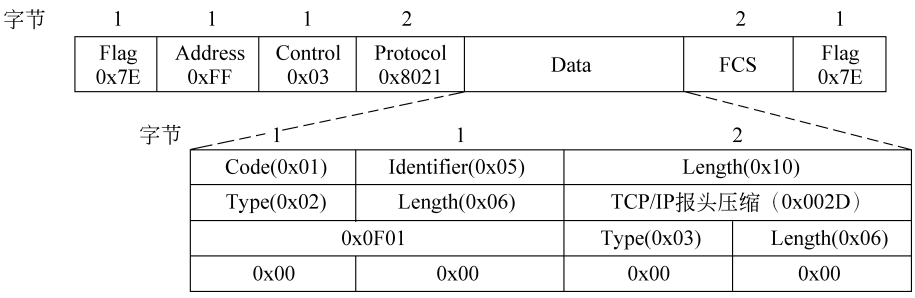

图 3.14　IPCP 协议 Configure-Request 报文示例

(1) PAP 认证流程

PAP 的认证流程如图 3.15 所示。认证方向被认证方一直发送 Authenticate-Request (认证请求)报文直到收到回复为止,其中包含了身份(通常是账号)和口令信息;若认证通过,认证方回复 Authenticate-Ack(认证确认)报文,否则认证失败,返回 Authenticate-Nak(认证否认)报文。

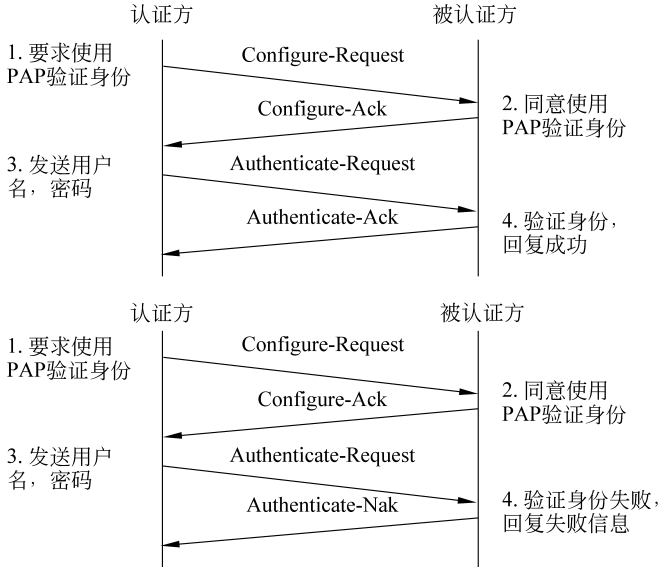

图 3.15　PAP 认证流程

(2) PAP 报文格式

当 PPP 帧中 Protocol 字段取值为 0xC023 时,表示 Information 字段承载的是 PAP 报文。图 3.16 给出了 PAP 的报文格式。

若 Code 取值为 0x01,表示报文是 Authenticate-Request 报文,该报文带有身份和口令的长度和内容;若 Code 取值为 0x02 或 0x03,表示报文是 Authenticate-Ack 报文或 Authenticate-Nak 报文,该报文带有 Message Length 和 Message 字段,指示认证描述信息的长度和内容,如认证失败时,可返回失败原因。

字节	1	1	2
	Code(0x01)	Identifier	Length
	Peer-ID Length	Peer-ID(长度不定)	
	Password Length	Password(长度不定)	

	Code(0x01或0x02)	Identifier	Length
	Message Length	Message(长度不定)	

图 3.16　PAP 报文格式

6. CHAP

CHAP(Challenge Handshake Authentication Protocol,询问握手认证协议)通过三次握手周期性地校验对方身份,可以在初始链路建立之后重复进行。通过递增改变的标识和可变的询问值,防止来自端点的重放攻击,限制暴露于单个攻击的时间。目前 PPP 协议的认证阶段多使用 CHAP 认证协议。

(1) CHAP 认证流程

CHAP 认证流程由 Challenge、Response 和 Success/Failure 报文组成,并配合事先协商好的算法,确认被认证方的身份。CHAP 协议通常使用 MD5(Message Digest Algorithm 5)作为其默认算法,因此 CHAP 又称为 MD5 CHAP。CHAP 认证流程如图 3.17 所示。

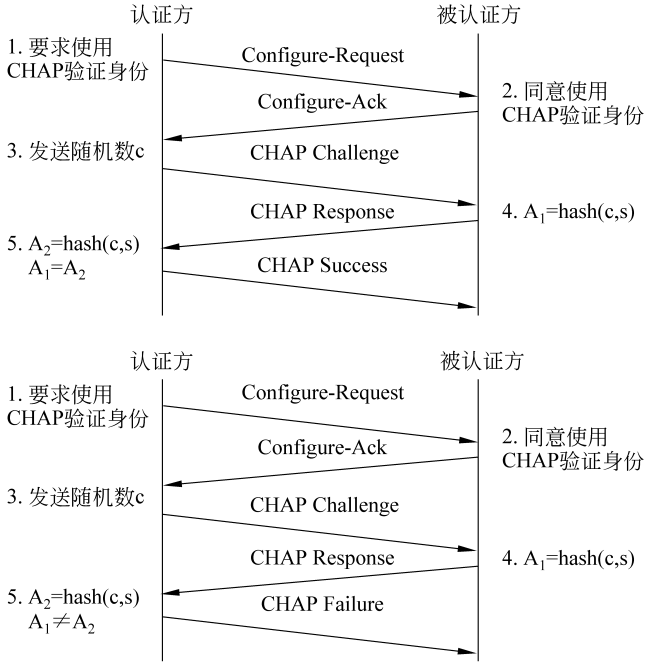

图 3.17　CHAP 认证流程

其中，认证方给被认证方发送一个 Challenge 报文，其中包含了随机数 c；作为响应，被认证方将双方共享的秘密值 s 和 c 一起作为输入，计算散列值 A_1，散列函数通常使用 MD5 算法，并通过 Response 报文返回；认证方在本地将 s 和 c 作为输入，用同一散列函数计算散列值 A_2，计算出来的结果进行比较，若两者相同，认证通过，返回 Success 报文；若不同，则认证失败，返回 Failure 报文。

(2) CHAP 报文格式

若 PPP 帧中 Protocol 字段取值为 0xC223 时，表示 Information 字段承载的是 CHAP 报文。图 3.18 给出了 CHAP 报文格式。

字节

1	1	2
Code(0x01或0x02)	Identifier	Length
Value-Size	Value(长度不定)	
Name(长度不定)		

Code(0x03或0x04)	Identifier	Length
Message(长度不定)		

图 3.18　CHAP 报文格式

若 Code 取值为 0x01 或 0x02，则分别表示 Challenge 报文和 Response 报文；Value-Size 字段表示 Value 字段的长度，其值是随机数，每次认证的 Value 字段值都不同，认证方和被认证方配合事先协商好的算法来计算散列值；Name 字段包含了发送方的身份描述信息。

若 Code 取值为 0x03 或 0x04，则分别表示 Success 报文和 Failure 报文。Message 字段由零到多字节组成，内含相关的描述信息。

3.2.2　PPP 协议分析

本节以 GNS3 为工作平台，以实验形式展开 PPP 协议的分析工作。

1. 总体思路

通过 GNS3 模拟两台 Cisco 路由器，并在路由器之间配置一条 PPP 链路。首先，利用 Wireshark 工具在 PPP 链路进行捕获，利用捕获结果分析 PPP 链路建立和网络层协商过程；其次，分析 PPP 数据传输过程；最后，在 PPP 链路配置采用 CHAP 协议进行认证，分析 CHAP 认证过程。

2. 网络环境搭建

(1) 网络拓扑配置

在 GNS3 中新建工程，配置网络拓扑如图 3.19 所示，其中，R1 和 R2 都是 Cisco 2600 系列路由器(本示例选用 Cisco 2691，选用的 IOS 映像为 c2691-jk9o3s-mz.123-22.bin)，R1 和 R2 的 WICs 插槽 wic 0 配置为 WIC-2T 模块接口卡(为路由器提供两个 serial 端口，如图 3.20 所示)，并在路由器 R1 的 serial 0/0 端口与路由器 R2 的 serial 0/0 端口之间建立链路。

图 3.19　PPP 协议分析网络拓扑

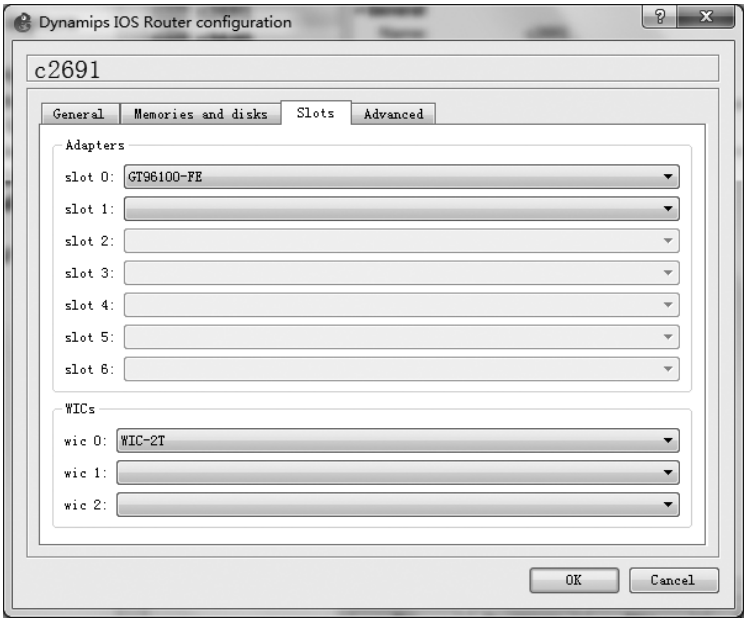

图 3.20　WICs 插槽配置示例

(2) 路由器基础配置

在 GNS3 中启动所有设备,路由器 R1 作为 DCE 设备,路由器 R2 作为 DTE 设备,分别对路由器 R1 和 R2 的 serial 0/0 端口配置 IP 地址,停用路由器 R1 和 R2 的 serial 0/0 端口。路由器 R1 配置如下所示。

```
1:  R1>enable
2:  R1#configure terminal
3:  R1(config)#interface serial 0/0
4:  R1(config-if)#ip address 192.168.1.1 255.255.255.0
5:  R1(config-if)#clock rate 128000
6:  R1(config-if)#encapsulation ppp
7:  R1(config-if)#shutdown
```

第 1 行输入 enable 命令,进入全局模式。

第 2 行输入 configure terminal 命令,进入特权模式。

第 3 行输入 interface serial 0/0 命令,进入接口配置模式对 serial 0/0 进行配置。

第 4 行输入 ip address 192.168.1.1 255.255.255.0 命令,对 serial 0/0 配置 ip 地址为

192.168.1.1，子网掩码为 255.255.255.0。

第 5 行输入 clock rate 128000 命令，serial 0/0 作为 DCE 设备，向 DTE 端提供时钟，时钟速率为 128000。

第 6 行输入 encapsulation ppp 命令，serial 0/0 封装 ppp 协议。

第 7 行输入 shutdown 命令，停用 serial 0/0 端口。

路由器 R2 配置如下所示。

```
1:  R2>enable
2:  R2#configure terminal
3:  R2(config)#interface serial 0/0
4:  R2(config-if)#ip address 192.168.1.2 255.255.255.0
5:  R2(config-if)#encapsulation ppp
6:  R2(config-if)#shutdown
```

第 4 行输入 ip address 192.168.1.2 255.255.255.0 命令，对 serial 0/0 配置 ip 地址为 192.168.1.2，子网掩码为 255.255.255.0。

成功进行上述配置后，因路由器 R1 和 R2 的 serial 0/0 均处于停用状态，路由器 R1 和 R2 之间的 ppp 链路并未建立。

3. 链路建立和网络层协商

(1) 数据捕获

① 启动 Wireshark 进行捕获

在 GNS3 中 PPP 链路的上右击，弹出如图 3.21 所示菜单。

图 3.21　捕获 PPP 链路示例

单击“Start capture”菜单项，弹出捕获端口选择窗口，如图 3.22 所示，选择路由器 R1 的 serial 0/0 按照 PPP 协议进行捕获；在包捕获窗口中选择 OK 按钮，启动 Wireshark 并开始捕获，如图 3.23 所示。

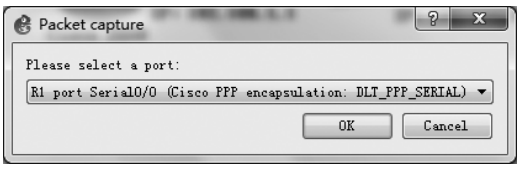

图 3.22　捕获端口选择示例

② 启用路由器 R1 和 R2 端口

路由器 R1 和 R2 上启用 serial 0/0 端口，路由器 R1 具体配置如下(路由器 R2 配置同路由器 R1)：

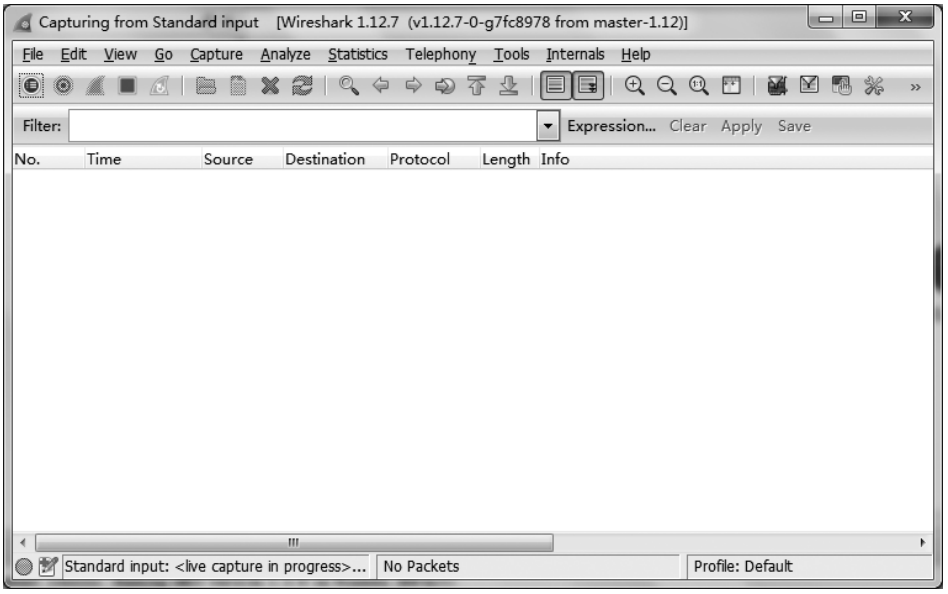

图 3.23 Wireshark 捕获窗口

```
1:  R1>enable
2:  R1#configure terminal
3:  R1(config)#interface serial 0/0
4:  R1(config-if)#no shutdown
```

路由器 R1 配置说明如下：

第 4 行的 no shutdown 命令，用于启用 serial 0/0 端口。

(2) 数据格式分析

成功启用路由器 R1 和 R2 的 serial 0/0 端口后，路由器 R1 和 R2 通过链路建立和配置流程建立 PPP 链路，并通过 IPCP 协商双方 IP 地址，借助 Wireshark 可以协助分析其过程。图 3.24 是链路建立和 IPCP 协商示例。

图 3.24 中，第 1～4 包是通信双方使用 LCP 协议的链路建立和配置过程；第 5、7、10 和 11 包是通信双方使用 IPCP 协商 IP 地址的过程；第 6、8、9 和 12 包是通信双方使用 CDPCP(Cisco Discovery Protocol Control Protocol，思科发现协议控制协议)协商 CDP(Cisco Discovery Protocol，思科发现协议)参数的过程；第 13、14 和 19 包是双方路由器采用 CDP 协议交换相邻路由器信息的过程；第 15～18 包是通信双方使用 LCP 协议进行链路质量和性能测试的过程。因 CDPCP 和 CDP 协议是 Cisco 的私有协议，本节不讨论 CDPCP 和 CDP 相关内容。

通过分析第 1～4 包，可勾勒出 LCP 协议的链路建立和配置的基本流程。PPP 链路的建立是双向的，示例中第 1 包和第 3 包组成 DCE 请求 DTE 建立连接过程；第 2 包和第 4 包组成 DTE 请求 DCE 建立连接过程，因其过程类似，仅分析第 1 包和第 3 包。第 1～4 包原始内容如表 3.5 所示。

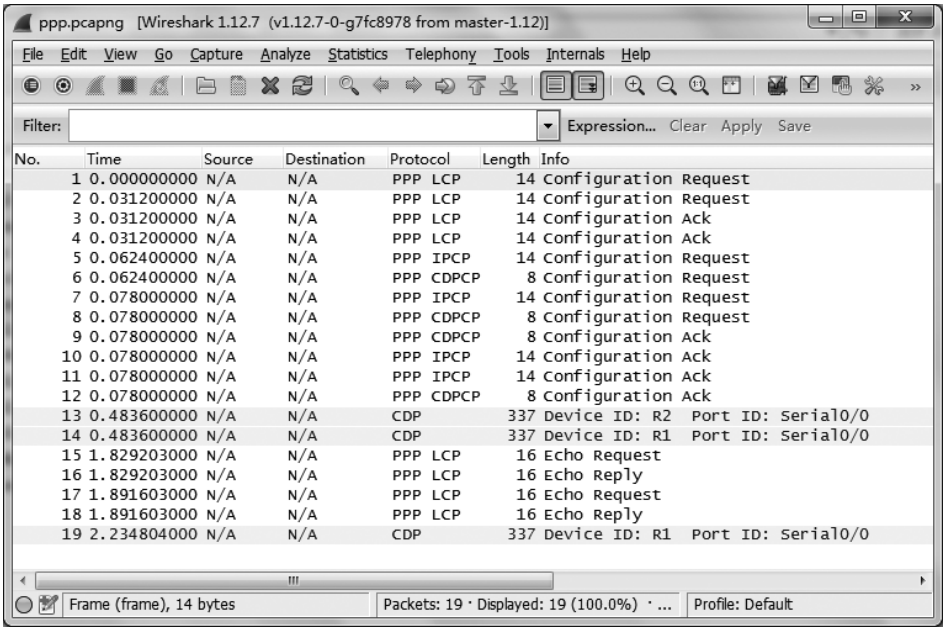

图 3.24　链路建立和 IPCP 协商示例

表 3.5　链路建立和配置流程报文原始内容示例

包序号	对 应 参 数		
1	0000	ff 03 c0 21 01 0b 00 0a 05 06 01 0e 22 7b	...!.....\"{
2	0000	ff 03 c0 21 01 01 00 0a 05 06 02 11 78 52	...!.....xR
3	0000	ff 03 c0 21 02 0b 00 0a 05 06 01 0e 22 7b	...!.....\"{
4	0000	ff 03 c0 21 02 01 00 0a 05 06 02 11 78 52	...!.....xR

第 1 包的第 1 字节的值为 0xFF，为 Address 字段，应为 PPP 协议，是点到点的协议，接收方必定只有一个，故此字段固定值为 0xFF，表示所有站点，只有联网的对方才能收到数据；第 2 字节的值为 0x03，为 Control 字段，该字段固定值为 0x03，表示无序号信息；第 3、4 字节的值为 0xC021，为 Protocol 字段，表示 LCP 协议。后续的 Information 信息应该按照 LCP 协议进行解析；第 5 字节的值为 0x01，为 LCP 报文的 Code 字段，0x01 表示 Configure-Request 报文；第 6 字节的值为 0x0B，为 LCP 报文的 Identifier 字段，0x0B 用于标识报文，作为识别之用，当接收方响应 Configure-Request 报文时，其响应报文也必须填入相同值，主要是使 LCP 的请求报文和响应报文能够匹配；第 7、8 字节的值为 0x000A，为 LCP 报文的 Length 字段，0x000A 表示 LCP 报文长度为 10 字节，减去 Code、Identifier 和 Length 字段 4 字节，表示其后的 Data 字段只有 6 字节；第 9～14 字节的值为 0x05 06 01 0E 22 7B，为 LCP 报文的 Data 字段，此处表示 Configure-Request 报文的选项，0x05 表示类型为幻数(Magic Number)，0x06 表示选项长度为 6，0x01 0E 22 7B 为 4 字节的幻数(Magic Number)值。

第 3 包的第 5 字节的值为 0x02，为 LCP 报文的 Code 字段，0x02 表示 Configure-Ack 报文；第 6 字节的值为 0x0B，为 LCP 报文的 Identifier 字段，0x0B 表示对 Identifier 字段为 0x0B 的 Configure-Request 报文进行确认；第 7、8 字节的值为 0x000A，为 LCP 报文的 Length 字段，0x000A 表示 LCP 报文长度为 10 字节，减去 Code、Identifier 和 Length 字段 4 字节，其后的 Data 字段只有 6 字节；第 9～14 字节的值为 0x05 06 01 0E 22 7B，为 LCP 报文的 Data 字段，此处表示 Configure-Ack 报文的选项，0x05 表示类型为幻数(Magic Number)，0x06 表示选项长度为 6，0x01 0E 22 7B 为 4 字节的幻数(Magic Number)值。

因通信双方未配置认证协议，双方直接进入“网络层协议阶段”，使用 IPCP 协商 IP 地址，通过对第 5、7、10 和 11 包的分析，有助于了解 PPP 链路通过 IPCP 协商相关通信参数的过程(参见本章“3.2.1 PPP 协议概述”的 NCP 部分)，其协商过程也是双向的，示例中第 5 包和第 10 包组成一个 IPCP 协商过程；第 7 包和第 11 包也组成一个 IPCP 协商过程，其过程类似，均为 IP 地址的协商，本例仅分析第 5 包和第 10 包。第 5、7、10 和 11 包原始内容如表 3.6 所示。

表 3.6　IPCP 协商报文原始内容示例

包序号	对 应 参 数		
5	0000	ff 03 80 21 01 01 00 0a 03 06 c0 a8 01 01	...!.....
7	0000	ff 03 80 21 01 01 00 0a 03 06 c0 a8 01 02	...!.....
10	0000	ff 03 80 21 02 01 00 0a 03 06 c0 a8 01 01	...!.....
11	0000	ff 03 80 21 02 01 00 0a 03 06 c0 a8 01 02	...!.....

第 5 包的第 3、4 字节的值为 0x8021，为 Protocol 字段，表示 IPCP 协议。后续的 Information 信息应该按照 IPCP 报文进行解析；第 5 字节的值为 0x01，为 IPCP 报文的 Code 字段，0x01 表示 Configure-Request；第 6 字节的值为 0x01，为 IPCP 报文的 Identifier 字段，0x01 用于标识报文，作为识别之用，当接收方响应 Configure-Request 报文时，其响应报文也必须填入相同值；第 7、8 字节的值为 0x000A，为 IPCP 报文的 Length 字段，0x000A 表示 IPCP 报文长度为 10 字节，减去 Code、Identifier 和 Length 字段 4 字节，表示其后的 Data 字段只有 6 字节；第 9～14 字节的值为 0x03 06 C0 A8 01 01，为 IPCP 报文的 Data 字段，此处表示 Configure-Request 报文的选项。0x03 表示类型为 IP 地址(IP Address)，0x06 表示选项长度为 6，0xC0 A8 01 01 为 4 字节 IP 地址值(192.168.1.1)。

第 10 包的第 5 字节的值为 0x02，为 IPCP 报文的 Code 字段，0x02 表示 Configure-Ack；第 6 字节的值为 0x01，为 IPCP 报文的 Identifier 字段，表示对 Identifier 字段为 0x01 的 Configure-Request 报文进行确认；第 7、8 字节的值为 0x000A，为 IPCP 报文的 Length 字段，0x000A 表示 IPCP 报文长度为 10 字节，减去 Code、Identifier 和 Length 字段 4 字节，表示其后的 Data 字段只有 6 字节；第 9～14 字节的值为 0x03 06 C0 A8 01 01，为 IPCP 报文的 Data 字段，此处表示 Configure-Ack 报文的选项。0x03 表示类型为 IP 地址(IP Address)，0x06 表示选项长度为 6，0xC0 A8 01 01 为 4 字节 IP 地址值(192.168.1.1)。