第 7 章 HDLC 和 PPP

路由器经常用于构建广域网，广域网链路的封装和以太网上的封装有着非常大的差别。常见的广域网封装有 HDLC、PPP、Frame-relay 等，本章介绍 HDLC 和 PPP。相对而言，PPP 比起 HDLC 有较多的功能。

7.1 HDLC 和 PPP 简介

7.1.1 HDLC 介绍

HDLC 是点到点串行线路上（同步电路）的帧封装格式，其帧格式和以太网帧格式有很大的差别,HDLC 帧没有源 MAC 地址和目的 MAC 地址。Cisco 公司对 HDLC 进行了专有化,Cisco 的 HDLC 封装和标准的 HDLC 不兼容。如果链路的两端都是 Cisco 设备，使用 HDLC 封装没有问题，但如果 Cisco 设备与非 Cisco 设备进行连接，应使用 PPP 协议。HDLC 不能提供验证，缺少了对链路的安全保护。默认时，Cisco 路由器的串口是采用 Cisco HDLC 封装的。如果串口的封装不是 HDLC，要把封装改为 HDLC 使用命令“encapsulation hdlc”。

7.1.2 PPP 介绍

1. PPP 概述

和 HDLC 一样，PPP 也是串行线路上（同步电路或者异步电路）的一种帧封装格式，但是 PPP 可以提供对多种网络层协议的支持。PPP 支持认证、多链路捆绑、回拨、压缩等功能。PPP 经过 4 个过程在一个点到点的链路上建立通信连接：

- 链路的建立和配置协调：通信的发起方发送 LCP 帧来配置和检测数据链路
- 链路质量检测：在链路已经建立、协调之后进行，这一阶段是可选的
- 网络层协议配置协调：通信的发起方发送 NCP 帧以选择并配置网络层协议
- 关闭链路：通信链路将一直保持到 LCP 或 NCP 帧关闭链路或发生一些外部事件

2. PPP 认证：PAP 和 CHAP

（1）PAP——密码验证协议

PAP（Password Authentication Protocol）利用 2 次握手的简单方法进行认证。在 PPP 链路建立完毕后，源节点不停地在链路上反复发送用户名和密码，直到验证通过。PAP 的验证中，密码在链路上是以明文传输的，而且由于是源节点控制验证重试频率和次数，因此 PAP 不能防范再生攻击和重复的尝试攻击。

（2）CHAP——询问握手验证协议

CHAP(Challenge Handshake Authentication Protocol)利用 3 次握手周期地验证源端节点的身份。CHAP 验证过程在链路建立之后进行，而且在以后的任何时候都可以再次进行。这使得链路更为安全；CHAP 不允许连接发起方在没有收到询问消息的情况下进行验证尝试。CHAP 每次使用不同的询问消息，每个消息都是不可预测的唯一的值，CHAP 不直接传送密码，只传送一个不可预测的询问消息，以及该询问消息与密码经过 MD5 加密运算后的加密值。所以 CHAP 可以防止再生攻击，CHAP 的安全性比 PAP 要高。

7.2 实验 1:HDLC 和 PPP 封装

1. 实验目的

通过本实验，读者可以掌握如下技能：

（1） 串行链路上的封装概念

（2） HDLC 封装

（3） PPP 封装

2. 实验拓扑

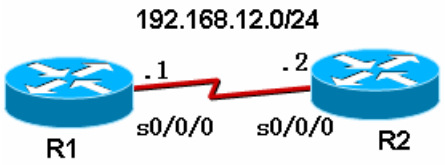

图 7-1 实验 1--实验 3 拓扑图

3. 实验步骤

（1） 步骤 1：在 R1 和 R2 路由器上配置 IP 地址、保证直连链路的连通性

```
R1(config)#int s0/0/0
R1(config-if)#ip address 192.168.12.1 255.255.255.0
R1(config-if)#no shutdown

R2(config)#int s0/0/0
R2(config-if)#clock rate 128000
R2(config-if)#ip address 192.168.12.2 255.255.255.0
R2(config-if)#no shutdown

R1#show interfaces s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 192.168.12.1/24
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set          //该接口的默认封装为 HDLC 封装
（此处省略）
```

（2） 步骤 2：改变串行链路两端的接口封装为 PPP 封装

```
R1(config)#int s0/0/0
R1(config-if)#encapsulation ppp

R2(config)#int s0/0/0
R2(config-if)#encapsulation ppp

R1#show int s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 192.168.12.1/24
```

MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, LCP Open　//该接口的封装为 PPP 封装
Open: IPCP, CDPCP, loopback not set　//网络层支持 IP 和 CDP 协议
（此处省略）

4. 实验调试

（1） 测试 R1 和 R2 之间串行链路的连通性

```
R1#ping 192.168.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/13/16 ms
```

如果链路的两端封装相同，则 ping 测试应该正常

（2） 链路两端封装不同协议

```
R1(config)#int s0/0/0
R1(config-if)#encapsulation ppp

R2(config)#int s0/0/0
R2(config-if)#encapsulation hdlc

R1#show int s0/0/0
Serial0/0/0 is up, line protocol is down
```

（此处省略）
//两端封装不匹配，导致链路故障

【提示】显示串行接口时，常见以下几种状态：

```
Serial0/0/0 is up, line protocol is up
```

//链路正常

```
Serial0/0/0 is administratively down, line protocol is down
```

//没有打开该接口，执行“no shutdown”可以打开接口

```
Serial0/0/0 is up, line protocol is down
```

//物理层正常，数据链路层有问题，通常是没有配置时钟、两端封装不匹配、PPP 认证错误

```
Serial0/0/0 is down, line protocol is down
```

//物理层故障，通常是连线问题

7.3 实验 2:PAP 认证

1. 实验目的

通过本实验，读者可以掌握如下技能：

（1） PAP 认证的配置方法

2. 实验拓扑

如图 7-1。

3. 实验步骤

在实验 1 基础上继续本实验。首先配置路由器 R1（远程路由器，被认证方）在路由器

R2（中心路由器，认证方）取得验证：

(1) 两端路由器上的串口采用 PPP 封装，用“encapsulation”命令：

R1(config)#int s0/0/0

R1(config-if)#encapsulation ppp

(2) 在远程路由器 R1 上，配置在中心路由器上登录的用户名和密码，使用“ppp pap sent-username 用户名 password 密码”命令：

R1(config-if)#ppp pap sent-username R1 password 123456

(3) 在中心路由器上的串口采用 PPP 封装，用“encapsulation”命令：

R2(config)#int s0/0/0

R2(config-if)#encapsulation ppp

(4) 在中心路由器上，配置 PAP 验证，使用“ppp authentication pap”命令：

R2(config-if)#ppp authentication pap

(5) 中心路由器上为远程路由器设置用户名和密码，使用“username 用户名 password 密码”命令：

R2(config)#username R1 password 123456

以上的步骤只是配置了 R1（远程路由器）在 R2（中心路由器）取得验证，即单向验证。然而在实际应用中通常是采用双向验证，即：R2 要验证 R1，而 R1 也要验证 R2。我们要采用类似的步骤进行配置 R1 对 R2 进行验证，这时 R1 为中心路由器，R2 为远程路由器了：

(6) 在中心路由器 R1 上，配置 PAP 验证，使用“ppp authentication pap”命令：

R1(config-if)#ppp authentication pap

(7) 在中心路由器 R1 上为远程路由器 R2 设置用户名和密码，使用“username 用户名 password 密码”命令：

R1(config)#username R2 password 654321

(8) 在远程路由器 R2 上，配置以什么用户和密码在远程路由器上登录，使用“ppp pap sent-username 用户名 password 密码”命令：

R2(config-if)#ppp pap sent-username R2 password 654321

【提示】在 ISDN 拨号上网时，却通常只是电信对用户进行验证（要根据用户名来收费），用户不能对电信进行验证，即验证是单向的。

4. 实验调试

使用“debug ppp authentication”命令可以查看 ppp 认证过程。

```
R1#debug ppp authentication
PPP authentication debugging is on
//以上打开 ppp 认证调试
R1(config)#int s0/0/0
R1(config-if)#shutdown
R1(config-if)#no shutdown
//由于 PAP 认证是在链路建立后进行一次，把接口关闭重新打开以便观察认证过程
*Feb 22 12:18:20.355: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state to up
*Feb 22 12:18:20.355: Se0/0/0 PPP: Using default call direction
*Feb 22 12:18:20.355: Se0/0/0 PPP: Treating connection as a dedicated line
*Feb 22 12:18:20.355: Se0/0/0 PPP: Session handle[C0000006] Session id[15]
*Feb 22 12:18:20.355: Se0/0/0 PPP: Authorization required
*Feb 22 12:18:20.359: Se0/0/0 PAP: Using hostname from interface PAP
```

*Feb 22 12:18:20.359: Se0/0/0 PAP: Using password from interface PAP
*Feb 22 12:18:20.359: Se0/0/0 PAP: O AUTH-REQ id 13 len 14 from "R1"
*Feb 22 12:18:20.363: Se0/0/0 PAP: I AUTH-REQ id 2 len 14 from "R2"
*Feb 22 12:18:20.363: Se0/0/0 PAP: Authenticating peer R2
*Feb 22 12:18:20.363: Se0/0/0 PPP: Sent PAP LOGIN Request
*Feb 22 12:18:20.363: Se0/0/0 PPP: Received LOGIN Response PASS
*Feb 22 12:18:20.363: Se0/0/0 PPP: Sent LCP AUTHOR Request
*Feb 22 12:18:20.363: Se0/0/0 PPP: Sent IPCP AUTHOR Request
*Feb 22 12:18:20.363: Se0/0/0 LCP: Received AAA AUTHOR Response PASS
*Feb 22 12:18:20.363: Se0/0/0 IPCP: Received AAA AUTHOR Response PASS
*Feb 22 12:18:20.363: Se0/0/0 PAP: O AUTH-ACK id 2 len 5
*Feb 22 12:18:20.363: Se0/0/0 PAP: I AUTH-ACK id 13 len 5
*Feb 22 12:18:20.363: Se0/0/0 PPP: Sent CDPCP AUTHOR Request
*Feb 22 12:18:20.363: Se0/0/0 CDPCP: Received AAA AUTHOR Response PASS
*Feb 22 12:18:20.367: Se0/0/0 PPP: Sent IPCP AUTHOR Request
*Feb 22 12:18:21.363: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
//以上是认证成功的例子

*Feb 22 12:22:07.391: Se0/0/0 PPP: Authorization required
*Feb 22 12:22:09.411: Se0/0/0 PAP: Using hostname from interface PAP
*Feb 22 12:22:09.411: Se0/0/0 PAP: Using password from interface PAP
*Feb 22 12:22:09.411: Se0/0/0 PAP: O AUTH-REQ id 15 len 14 from "R1"
*Feb 22 12:22:09.411: Se0/0/0 PAP: I AUTH-REQ id 4 len 14 from "R2"
*Feb 22 12:22:09.411: Se0/0/0 PAP: Authenticating peer R2
*Feb 22 12:22:09.411: Se0/0/0 PPP: Sent PAP LOGIN Request
*Feb 22 12:22:09.415: Se0/0/0 PPP: Received LOGIN Response FAIL
*Feb 22 12:22:09.415: Se0/0/0 PAP: O AUTH-NAK id 4 len 26 msg is **"Authentication failed"**
//以上是认证失败的例子，例如密码错误等

7.4 实验 3:CHAP 认证

1. 实验目的

通过本实验，读者可以掌握如下技能：

(1) CHAP 认证的配置方法

2. 实验拓扑

如图 7-1。

3. 实验步骤

在实验 1 基础上继续本实验。

(1) 使用“**username 用户名 password 密码**” 命令为对方配置用户名和密码，需要注意的是两方的密码要相同：

R1(config)**#username R2 password hello**

R2(config)**#username R1 password hello**

(2) 路由器的两端串口采用 PPP 封装，并采用配置 CHAP 验证：

```
R1(config)#int s0/0/0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication chap

R2(config)#int s0/0/0
R2(config-if)#encapsulation ppp
R2(config-if)#ppp authentication chap
```

上面是 CHAP 验证的最简单配置，也是实际应用中最常用的配置方式。配置时要求用户名为对方路由器名，而双方密码必须一致。原因是：由于 CHAP 默认使用本地路由器的名字做为建立 PPP 连接时的识别符。路由器在收到对方发送过来的询问消息后，将本地路由器的名字作为身份标识发送给对方；而在收到对方发过来的身份标识之后，默认使用本地验证方法，即在配置文件中寻找，看看有没有用户身份标识和密码；如果有，计算加密值，结果正确则验证通过；否则验证失败，连接无法建立。

【提示】在配置验证时也可以选择同时使用 PAP 和 CHAP，如：

```
R2(config-if)#ppp authentication chap pap 或
R2(config-if)#ppp authentication pap chap
```

如果同时使用两种验证方式，那么在链路协商阶段将先用第一种验证方式进行验证。如果对方建议使用第二种验证方式或者只是简单拒绝使用第一种方式，那么将采用第二种方式。

7.5 本章小结

本章介绍了串行链路上常用的两种封装方法:HDLC 和 PPP,前者只在 Cisco 设备间使用，后者可以用于不同厂商的设备间。PPP 和 HDLC 相比有较多的功能：支持多网络层协议、支持认证、支持多链路捆绑、支持回拨和压缩等。PPP 的认证有两种方式：PAP 和 CHAP，CHAP 比起 PAP 具有较好的安全性能。表 7-1 是本章出现的命令。

表 7-1 本章命令汇总

命令	作用
encapsulation hdlc	把接口的封装改为 hdlc
encapsulation ppp	把接口的封装改为 ppp
ppp pap sent-username R1 password 123456	pap 认证时，向对方发送用户名 R1 和密码 123456
ppp authentication pap	PPP 的认证方式为 pap
username R1 password 123456	为对方创建用户 R1，密码为 123456
debug ppp authentication	打开 ppp 的认证调试过程
ppp authentication chap	PPP 的认证方式为 chap