广域网协议配置

目 录

第 1 章 PPP 配置 1
1.1 概述 1
1.2 PPP 配置任务列表 2
1.2.1 启用 PPP 封装 2
1.2.2 启用 CHAP 或 PAP 认证 2
1.2.3 配置 IP 地址池 4
1.2.4 停用或重新启用对端主机路由 5
1.2.5 配置多链路 PPP（multilink PPP） 5
1.3 PPP 配置举例 6
1.3.1 CHAP 配置举例 6
1.3.2 Multilink PPP 配置举例 7
第 2 章 HDLC 配置 9
2.1 概述 9
2.2 HDLC 配置任务 9
2.2.1 启用 HDLC 封装 9

第1章 PPP 配置

本章讲述如何配置点对点协议（PPP）。本章也描述了可应用于异步串行、同步串行和ISDN 接口上针对的点对点连接的地址池。

本章中 PPP 命令的完整描述，参见“PPP 命令参考”一章。

1.1 概述

PPP 协议提供了点对点链路上的多协议数据报的传输。路由器主要实现如下功能：

- 遵从 RFC1661，支持链路控制协议(LCP)，用于建立、配置和测试数据链接。
- 遵从 RFC1662，支持 IP 等上层协议在 PPP 上的封装，实现网络控制协议(NCP)中的 IPCP。
- 遵从 RFC1334，支持几种通用的认证协议，包括 PAP、CHAP、MC-CHAP 和 TACACS+。
- 遵从 RFC1144，支持 TCP/IP 报头压缩，提高有效数据吞吐量。
- 提供广泛的选项控制，适应于尽可能多的情况，支持与各种网络设备及主机通过 PPP 协议实现互联。
- 支持同步、异步 PPP 协议。
- 支持 PPP multilink 选项，实现多链路捆绑。
- 在路由器作为拨号服务器使用时支持 RADIUS 协议，可对用户身份进行认证(authentication)，授权(authorization)及统计(accouting)。用户信息存放在一台主机上,主机与路由器之间通过 RADIUS 协议交互信息。

PPP 协议中 RFC 1661 中进行了描述，该协议提供了在点对点连接上封装网络层协议信息的方法。PPP 协议可以在下列几种类型的物理接口上配置：

- 同步串行口

同样通过在物理接口启用PPP封装，PPP也应用于使用该物理接口的对应的拨号接口中。

当前路由器软件中，PPP 实现支持协商选项 2：异步控制字符映像；选项 3：使用 CHAP 或 PAP 的认证；选项 5：magic number 配置选项；选项 7：协议域压缩；选项 8：地址和控制域压缩。在 LCP 协商过程中，软件固定发送 5、7 和 8 号协商选项。如果是异步还发送协商选项 2。如果配置了认证，将发送协商选项 3。

在所有串行接口上，都支持 LCP 协商选项 5(magic number)。PPP 始终协商 magic number，用来检测线路上的回环（Loopback）。

本公司路由器软件在 PPP 协议中的支持 CHAP 认证协议和 PAP 认证协议。关于认证的详细信息，参见“安全配置指南”。

1.2 PPP配置任务列表

在串行接口(包括 ISDN)上,配置 PPP 需在接口配置模式下执行下列任务。

- 启用 PPP 封装

在下列段落中，你还可以执行如下任务。这些任务是可选的，它用于提供多种用法并增强 PPP 的功能。

- 启用 CHAP 或 PAP 认证
- 配置 IP 地址池
- 停用或重新启用对端主机路由
- 配置多链路 PPP（multilink PPP）

1.2.1 启用 PPP 封装

为了封装 IP 报文和其他网络层协议数据包，可以在串行线路上封装 PPP 协议。启用 PPP 封装，可以在接口配置模式下使用下列的命令：

命令	目的
encapsulation ppp	启用PPP封装。

1.2.2 启用 CHAP 或 PAP 认证

PPP 协议如果启用了 CHAP 认证协议或 PAP 认证协议，通常用来通知中心节点存在哪些远端路由器与之连接。

CHAP 和 PAP 最初在 RFC 1334 中说明，后 CHAP 在 RFC1994 中更新。这两个协议在同步和异步的串行接口上均支持。使用 CHAP 或 PAP 认证时，每个路由器或访问服务器要使用一个名字标识自己。这种身份验证过程避免了一台路由器与已经建立连接的路由器建立另一个呼叫，同时也防止了未授权的访问。

CHAP 或 PAP 对所有使用 PPP 封装的串行接口都适用。认证特性降低了路由器或访问服务器上的安全的危险。

注意：

使用 CHAP 或 PAP 前，必须运行 PPP 封装。

当某个接口上启用 CHAP 同时远端设备试图与它连接时，本地路由器或访问服务器会向远端设备发送一个 CHAP 数据包。CHAP 请求或“challenges” 数据包会等待远端设备的响应。“challenges”数据包中包括 ID，随机数和本地路由器的主机名。

期待的响应包括两部分：

- 由 ID，密码和随机数字生成的加密字串。
- 远端设备的主机名或用户名。

当本地路由器或访问服务器接收该响应时，通过执行响应中指示的相同的加密操作和查找要求的主机名称或用户名，以核实密码。远端设备和本地路由器的安全密码必须一致。

在传输响应过程中，密码从不以明文传输，以防止其他设备窃取它，同时获取系统的非法访问。没有正确的响应的情况下，远端设备不可能连接到本地路由器。

CHAP 报文交互只在链路建立后发生。 本地路由器或访问服务器在呼叫后期不再请求密码。（但本地设备在呼叫期间能响应来自其他设备的请求。）

当启用 PAP 时，试图连接到本地路由器或访问服务器的远端路由器必须发送一个认证请求。如果在接受到的认证请求中包括指定的用户名和密码，路由器软件将发送一个认证确认。

启用 CHAP 或 PAP 后，本地路由器或访问服务器需要远端设备的认证。如果远端设备不支持所启用的协议，那么将不与远端设备进行通信。

使用 CHAP 或 PAP 协议，必须执行下列的任务：

(1) 启用 PPP 封装。

(2) 在该接口上启用 CHAP 或 PAP。

(3) 对于 CHAP 认证，需要配置主机名。对于 PAP 认证，要配置用户名和密码。

启用 PPP 封装，在接口配置模式下使用下面的命令：

命令	目的
encapsulation ppp	在接口上启用PPP。

为了启用 CHAP 或 PAP 认证，可以在接口配置模式下使用下列的命令：

命令	目的
ppp authentication {**chap** | **ms-chap**| **pap**} [**word** | **default**] [**callin**]	定义支持的认证方法和使用的顺序。

在全局配置模式下的下列的命令，可以指定用于 CHAP 或 PAP 中主叫用户身份识别的密码。

命令	目的
username *name* **password** *secret*	配置身份识别。

密码不能包含空格。

1.2.3 配置 IP 地址池

点对点接口必须能通过 IP 控制协议（IPCP）地址协商过程向远端节点提供其 IP 地址。IP 地址可以通过不同的来源获得。地址可以通过命令行方式输入 EXEC 级的命令配置，或者由 TACACS＋提供，或者来自于本地 IP 地址池。

1. 对端地址分配

对端 IP 地址可以通过几种方法定位到一个接口：

IPCP 协商	如果对端在IPCP地址协商过程中提出了一个IP地址，并且没有分配其他对端地址，其提交的地址将被确认，仅在当前会话中使用。
缺省IP地址	缺省的IP地址可以通过命令peer default ip address定义。
TACACS+分配的IP地址或IP地址池	在IPCP地址协商的授权阶段，TACACS+可能返回一个IP地址，该地址可供拨号接口已经被认证的用户使用。
本地地址池	本地地址池包含了连续IP地址（最多1024个地址）的集合。空闲的地址按照从低地址到高地址递增的顺序轮流选取使用，以降低地址重新使用的机会，并能允许对端使用上次连接使用的地址重新连接。如果地址可用，就分配它；否则分配空闲的其他地址。

2. 优先原则

下面的对端 IP 地址优先原则 支持确定使用的 IP 地址。优先权从最可能列到最不可能：

(1) 本地 IP 地址池中的地址(通常不分配，除非没有其他地址存在)。

(2) 来自 peer default ip address 命令或 protocol translate 命令的配置地址。

(3) AAA/TACACS+ 提供的地址或 AAA/TACACS+命名的池中的地址。

(4) 对端由 IPCP 协商提供的地址。(除非没有其他地址，否则不被接受)。

3. 影响的接口

地址池允许在所有 可运行 PPP 此协议的异步串行、同步串行、ISDN BRI 和 ISDN PRI 接口中存在。

4. 配置各接口上的 IP 地址分配

- 在指定的接口上定义 IP 地址池。
- 为所有拨入用户在指定的接口上分配一个 IP 地址。

使用下列命令，定义应用于某接口的 IP 地址池：

命令	目的

ip local pool *poolname* {*begin-ip-address* [*ip-address-number*]}	创建一个或多个本地IP地址池。
interface *type number*	指定接口并进入接口配置模式。
peer default ip address pool *pool-name*	指定该接口使用的地址池。

使用下列命令，在指定的接口上分配一个 IP 地址：

命令	目的
ip local pool *poolname*{*begin-ip-address* } [*ip-address-number*]}	创建一个或多个本地IP地址池。
interface *type number*	指定接口并进入接口配置模式。
peer default ip address *ip-address*	指定分配的地址。

1.2.4 停用或重新启用对端主机路由

本公司路由器在缺省情况下自动创建对端主机路由；也就是说，当 PPP IPCP 协商完成后，它自动在点到点接口上建立一条到对端地址的路由。

在接口配置模式下使用下列命令，可以停用该缺省行为或在其停用后重新启用。

命令	目的
no peer neighbor-route	停止生成主机路由。
peer neighbor-route	重新生成主机路由。

1.2.5 配置多链路 PPP（multilink PPP）

多链路 PPP 协议的特色是在多个广域网链路上提供载荷平衡的功能。本公司路由器软件实现的多链路 PPP 协议支持 RFC 1717 中指定的报文分片和排序。

多链路 PPP 允许报文被分片，同时分片同时在多个点到点链路上发送到同一个远端地址。多重链路的启动是根据 dialer 上所定义的负载极限所确定。该负载可能由输入通信量、输出通信量或是两者共同组成。Multilink PPP 按需进行带宽分配同时减少在广域网传输上的等待时间。

多链路 PPP 可以工作在单个或多个接口上，可用的接口类型有：

- 串行接口（同步）

1. 在专线上配置 Multilink PPP

在多个专线接口上配置 Mutlilink PPP，你必须创建一个 multilink group 接口，其缺省配置成 Multilink PPP。然后独立配置每个专线接口并将其加入到相同的 multilink group 中。

建立 multilink group 接口的配置如下：

命令	目的

interface multilink group-*number*	定义multilink group接口。
ip address *ip-address mask*	指定适当的IP地址。
ppp lcp enddisc-type [**null|local|ip|ieee8021|ppp|psnd**]	(可选)指定enddisc类型。
ppp authentication [**pap|chap|ms-chap**]	(可选)启用PPP认证。
ppp multilink	启用 Multilink PPP。

配置隶属于 multilink group 中专线接口如下：

命令	目的
interface type *number*	定义一接口。
no ip address	不配置IP地址。
encapsulation ppp	启用PPP封装。
multilink-group *group-number*	添加该接口到multilink group 中。

注：

配置 multilink-group 的接口，其 PPP 配置将自动与相应的 multilink group 接口同步。

1.3 PPP配置举例

1.3.1 CHAP 配置举例

下面为两台设备在接口 serial1/0 上启用 CHAP 认证协议的示例。

环境说明：

两台路由器通过各自的 serial1/0 背靠背建立 PPP 连接。

配置路由器 router1

```
!
hostname router1
!
interface s1/0
encapsulation ppp
ppp authentication chap
ppp chap hostname user1
!
username user2 password 0 secret12
!
```

配置路由器 router2

```
!
```

```
hostname router2
!
interface s1/0
encapsulation ppp
ppp authentication chap
ppp chap hostname user2
!
username user1 password 0 secret12
!
```

1.3.2 Multilink PPP 配置举例

下列例子用于配置 Multilink PPP。第一个例子应用于一个 BRI 接口上 ，第二个用于配置隶属于 multilink group 接口的专线接口。第三个使用 virtual-template 配置 multilink。

1. 专线接口上配置 Multilink PPP

```
!
interface multilink 1
  ip address 192.168.20.100 255.0.0.0
  encapsulation ppp
  ppp lcp enddisc-type local
  ppp authentication chap
  ppp chap hostname router
  ppp multilink
!
interface s1/0
  no ip address
  encapsulation ppp
  ppp lcp enddisc-type local
  ppp authentication chap
  ppp chap hostname router
  ppp multilink
  multilink-gourp 1
!
interface s1/1
  no ip address
  encapsulation ppp
  ppp lcp enddisc-type local
  ppp authentication chap
  ppp chap hostname router
  ppp multilink
  multilink-gourp 1
!
interface s1/2
  no ip address
```

```
  encapsulation ppp
  ppp lcp enddisc-type local
  ppp authentication chap
  ppp chap hostname router
  ppp multilink
  multilink-gourp 1
!
```

2. 使用 virtual-template 配置 multilink

```
!
multilink virtual-template 1
!
interface virtual-template 1
 ip address 192.168.20.100
 ppp lcp enddisc-type ppp
 ppp multilink
!
interface s1/0
 physical-layer mode async
 no ip address
 no ip directed-broadcast
 ppp lcp enddisc-type ppp
 ppp authentication pap
 ppp multilink
 ppp pap sent-username router mypassword
 physical-layer speed 57600
!
interface s1/1
 physical-layer mode async
 no ip address
 no ip directed-broadcast
 ppp lcp enddisc-type ppp
 ppp authentication pap
 ppp multilink
 ppp pap sent-username router mypassword
 physical-layer speed 57600
!
```

第2章 HDLC 配置

2.1 概述

高级数据链路控制协议（HDLC）是从 IBM 的 SNA 中的同步数据链路控制协议（SDLC）演变而来的。在开发了 SDLC 后，IBM 把它提交给 ANSI 和 ISO，分别成为美国标准和国际标准。ANSI 修改了该协议，变成了高级数据通信控制协议 ADCCP；ISO 修改了该协议，变成了 HDLC。后来 CCITT 采纳并修改了 HDLC，成为链路访问规程（LAP）以及后来的 X.25 接口标准中的一部分。HDLC 是面向比特的协议，使用比特填充来保证数据的透明性。

HDLC 是一种数据打包协议，它定义了一种在同步线路上对 IP 包的链路封装，在点到点串行线路上运行 TCP/IP。

HDLC 一般用于 DDN 线路，该协议具有简单高效的特点。

HDLC 协议提供了在点对点连接上封装网络层协议信息的方法。该协议可以在下列几种类型的物理接口上配置：

- ISDN
- 同步串行口

2.2 HDLC配置任务

在串行接口(包括 ISDN)上,配置 HDLC 需在接口配置模式下执行下列任务。

2.2.1 启用 HDLC 封装

为了封装 IP 数据包，可以在串行线路上封装 HDLC 协议。

命令	目的
encapsulation hdlc	启用HDLC封装。