

PPP与PPPoE

广域网协议 (**WAN**协议)

- 帧中继
- ISDN
- HDLC
- PPP
- PPPoE
- DSL
- ATM
-

补充：广域网协议（WAN协议）

- **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**”。

补充：广域网协议（**WAN**协议）

- **2) HDLC封装**
- Router(config-if)#encapsulation hdlc
- 启用HDLC封装
- HDLC是同步串口的缺省封装格式

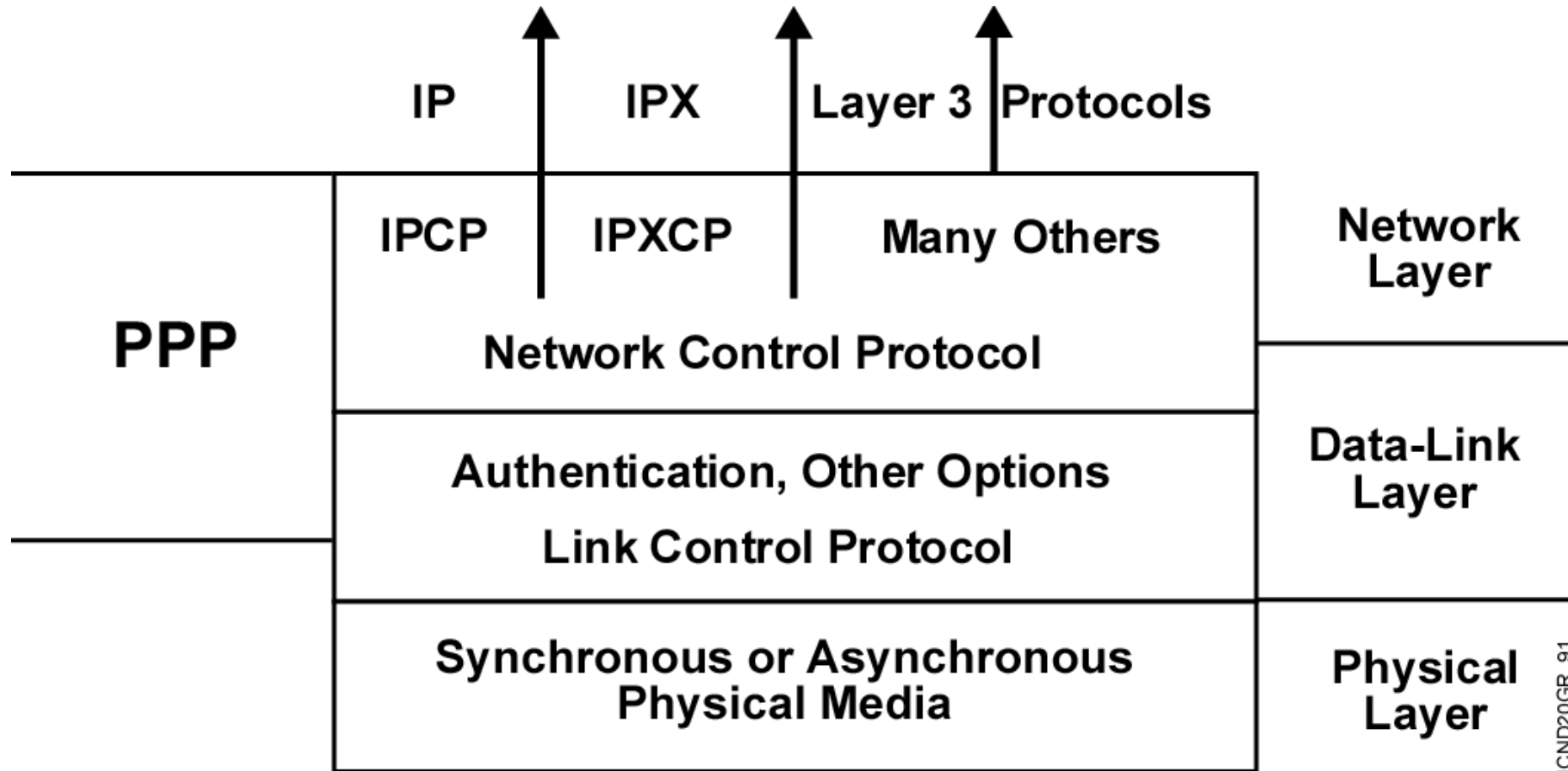
补充：广域网协议（WAN协议）

- **3)** 最常用的两个点对点广域网封装协议是HDLC、PPP
- **PPP**：用于在链路建立过程当中检查链路质量；另外，还支持PAP和CHAP密码验证
- **HDLC**：是思科串行线路的缺省协议，只允许点对点的连接
- 如果连接的是非CISCO设备，就需要使用其他的数据封装类型。如FR，PPP

PPP

- 1) PPP协议的基本概念
- PPP全称: Point-to-Point Protocol, 点到点协议。
- HDLC、PPP、帧中继(Frame-Relay)均为数据链路层协议。
- PPP的前身是SLIP、CSLIP。
- 2) PPP基本工作流程
 - (1) 链路关闭阶段---Link Dead
 - (2) 链路建立阶段---Link Establishment
 - (3) 认证阶段---Authentication
 - (4) 网络层协议阶段---Network Layer Protocol
 - (5) 链路终结阶段---Link Termination

- 3) PPP的层次原理
- PPP: 为网络层服务的数据链路层协议



4) PPP概述

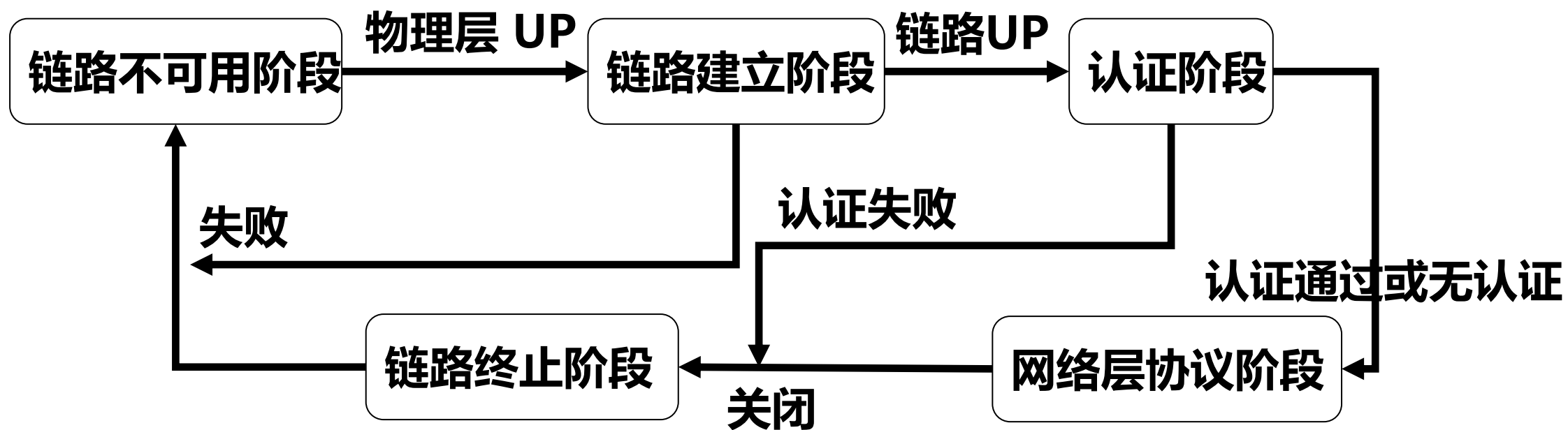
- **PPP（Point to Point Protocol）** 协议是在点对点链路上运行的数据链路层协议。
- 用户使用拨号电话线接入Internet时，一般都是使用 **PPP** 协议。



- 在80年代末，人们在串行线路协议（**SLIP**）基础上开发 **PPP** 协议来解决远程互联网连接的问题。

- 5) PPP协议优点
 - 支持同步或异步串行链路传输
 - 支持多种网络层协议
 - 支持网络层动态**IP**地址协商
 - 支持错误检测
 - 支持认证
 - 支持进行数据压缩
 - 支持多链路捆绑

- 6) PPP链路的建立

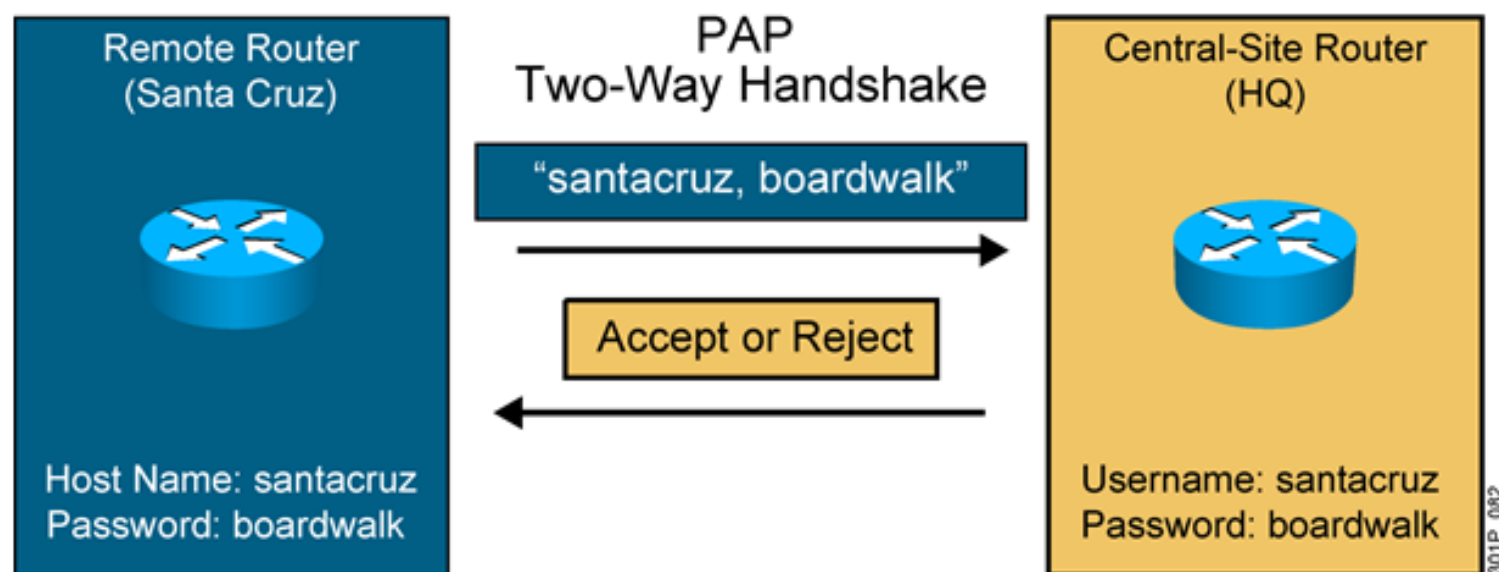


- 7) PPP会话建立过程
 - (1) 链路建立和配置协调(LCP)
 - (2) 链路验证阶段（可选）
两种PPP验证协议：PAP和CHAP
 - (3) 网络层协议连接(NCP)
 - (4) 链路终止阶段
- PPP 通过 LCP 建立和控制连接
 - 用来建立、配置、维护、终止一条点对点链路
- PPP 通过 NCP 携带多个协议的数据包
 - 用来建立、配置不同的网络层协议，包括IPCP、IPXCP等协议；

- 8) PPP认证
- 在PPP会话中，认证是可选的。
- 如果需要验证，须通信双方的路由器要交换彼此的验证信息。
- PPP协议支持两种认证协议：
 - PAP（Password Authentication Protocol，密码认证协议）
 - CHAP（Challenge Handshake Authentication Protocol，询问握手认证协议）
 - 在一般情况下，CHAP是首选协议。

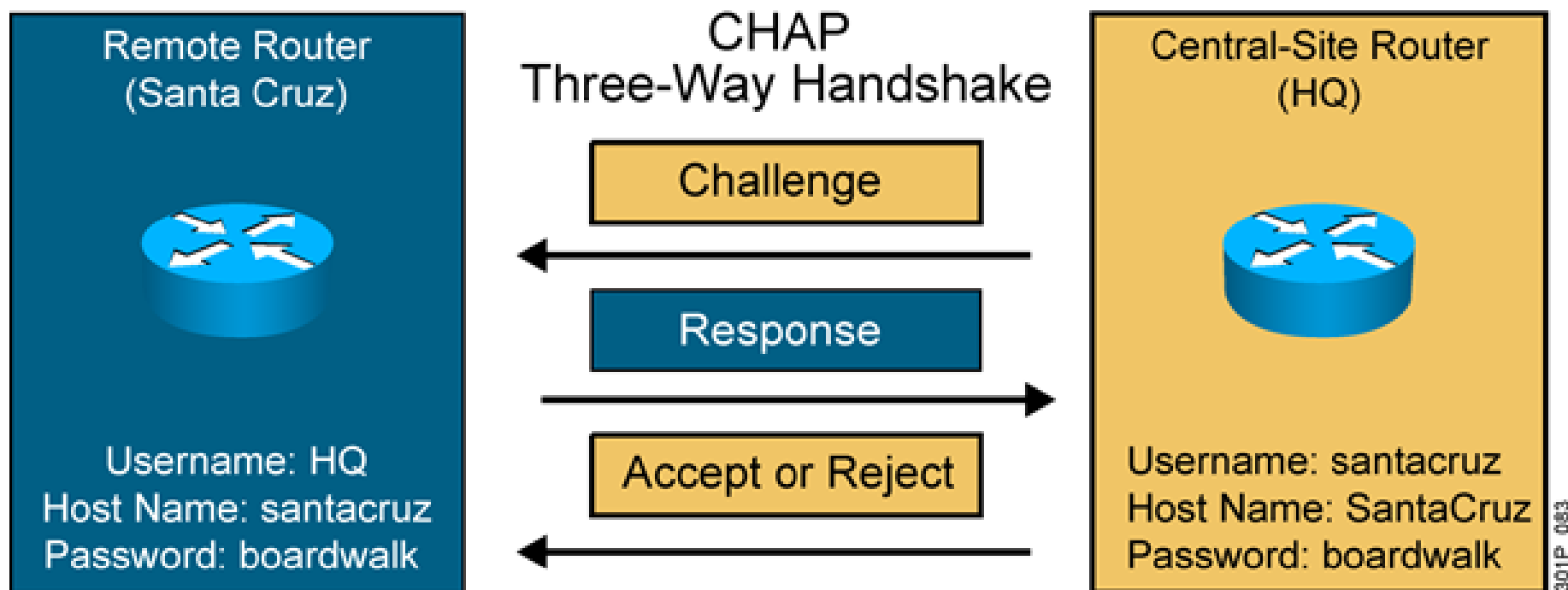
(1) PAP认证

- 简单认证（两次握手），密码明文传输
- 客户端（被认证方）直接发送包含用户名/口令的认证请求,服务器（认证方）端处理并回应



(2) CHAP认证

- 三次握手认证协议，密码加密传输
- 认证方先发起请求，安全性比PAP高



- 9) PPP封装

- (1) 在串口下封装PPP协议，并配置IP地址

```
[R1]int s0/0/0
[R1-Serial0/0/0]link-protocol ?
    atm    ATM protocol
    fr      Select FR as line protocol
    hdlc    Enable HDLC protocol
    ppp     Point-to-Point protocol
    tdm     TDM (Time Division Multiplexer) protocol

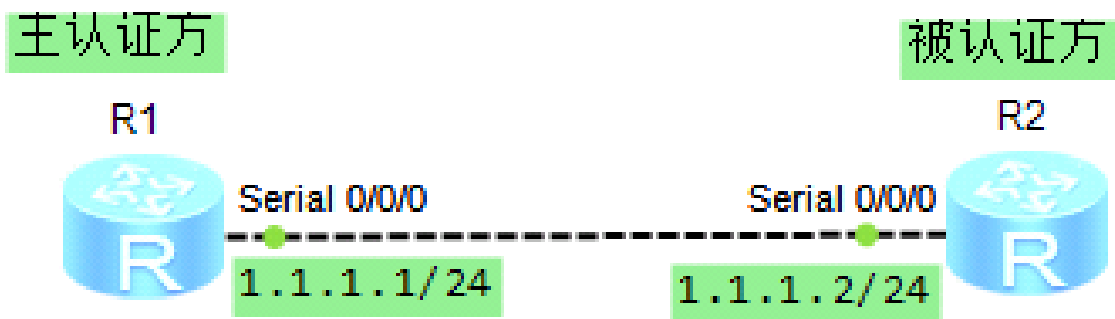
[R1-Serial0/0/0]link-protocol ppp
[R1-Serial0/0/0]ip address 12.1.1.1 30
```

- (2) 在串口下封装PPP协议，对端通过协商获取IP地址

```
[R1]int s0/0/0
[R1-Serial0/0/0]link-protocol ppp
[R1-Serial0/0/0]ip address 12.1.1.1 30
[R1-Serial0/0/0]remote address 12.1.1.2
```

```
[R2]int s0/0/0
[R2-Serial0/0/0]link-protocol ppp
[R2-Serial0/0/0]ip address ppp-negotiate
```

- 10) PPP认证配置
- (1) PAP单向认证配置



- 主认证方R1:
 - `aaa #将对端用户名和密码加入本地用户列表并设置服务类型`
 - `local-user rtb password cipher hello`
 - `local-user rtb service-type ppp`
 - `int s0/0/0`
 - `ip add 1.1.1.1 24 #指定物理接口的IP地址和掩码`
 - `ppp authentication-mode pap #在接口视图下设置本地验证对端的方式为PAP`
 - `q`

- 被认证方R2:
- int s0/0/0
- ip add 1.1.1.2 24 #指定物理接口的IP地址和掩码
- ppp pap local-user rtb password cipher hello #配置PAP验证时被验证方发送的PAP用户名和密码

- 测试结果:

```
[R1]ping 1.1.1.2
  PING 1.1.1.2: 56 data bytes, press CTRL_C to break
    Reply from 1.1.1.2: bytes=56 Sequence=1 ttl=255 time=40 ms
    Reply from 1.1.1.2: bytes=56 Sequence=2 ttl=255 time=50 ms
    Reply from 1.1.1.2: bytes=56 Sequence=3 ttl=255 time=20 ms
    Reply from 1.1.1.2: bytes=56 Sequence=4 ttl=255 time=30 ms
    Reply from 1.1.1.2: bytes=56 Sequence=5 ttl=255 time=50 ms
```

- (2) PAP双向认证配置
- **R1既是主认证方，又是被认证方：**
- **aaa #将对端用户名和密码加入本地用户列表并设置服务类型**
- **local-user R2 password cipher hello**
- **local-user R2 service-type ppp**
- **int s0/0/0**
- **ip add 1.1.1.1 24 #指定物理接口的IP地址和掩码**
- **ppp authentication-mode pap #在接口视图下设置本地验证对端的方式为PAP**
- **ppp pap local-user R1 password cipher hello #本地同时作为被验证方**
- **R2既是主认证方，又是被认证方：**
- **aaa #将对端用户名和密码加入本地用户列表并设置服务类型**
- **local-user R1 password cipher hello**
- **local-user R1 service-type ppp**
- **int s0/0/0**
- **ip add 1.1.1.1 24 #指定物理接口的IP地址和掩码**
- **ppp authentication-mode pap #在接口视图下设置本地验证对端的方式为PAP**
- **ppp pap local-user R2 password cipher hello #本地同时作为被验证方**

- (3) CHAP双向认证配置
- **R1既是主认证方，又是被认证方：**
- **aaa #在R1上将R2的用户名和口令添加到本地用户列表**
- **local-user rtb password cipherhello**
- **local-user rtb service-type ppp**
- **int s0/0/0**
- **ip add 1.1.1.1 24**
- **ppp authentication-mode chap #指定R1为主验证方，验证方式为CHAP验证**
- **ppp chap user rta #配置R1自己的用户名为rta**
- **ppp chap password cipher hello**
- **R2既是主认证方，有是被认证方：**
- **aaa #在R6上将R5的用户名和口令添加到本地用户列表**
- **local-user rta password cipherhello**
- **local-user rta service-type ppp**
- **int s0/0/0**
- **ip add 1.1.1.2 24**
- **ppp chap user rtb #配置R6自己的用户名为rtb**
- **ppp chap password cipher hello**

- (4) CHAP单向认证配置
- **R1是主认证方:**
- **aaa #在R1上将R2的用户名与密码添加到本地用户列表**
- **local-user rtb password cipher hello**
- **local-user rtb service-type ppp**
- **q**
- **int s0/0/0**
- **ip add 1.1.1.1 24**
- **ppp authentication-mode chap #指定R1为主验证方, 验证方式为CHAP验证**
- **R2是被认证方:**
- int s0/0/0
- ppp chap user rtb #在R2上配置R2自己的用户名和密码
- ppp chap password cipher hello
- ip add 1.1.1.2 24

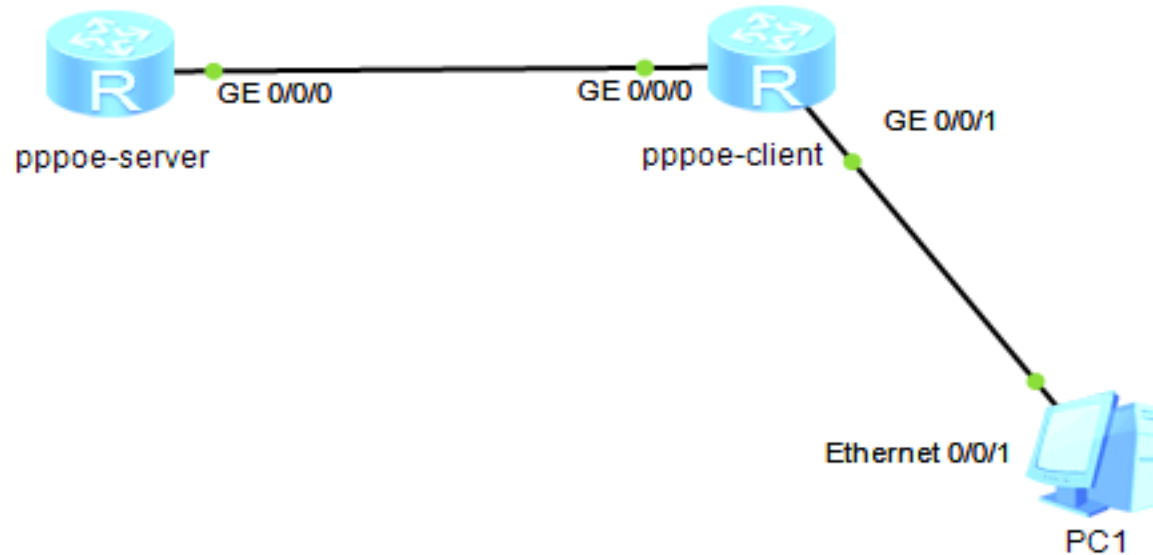
• PPPoE

• 1) PPPoE概述

- pppoe是ppp over Ethernet的技术，将PPP报文封装进以太网中进行传输，因为ISP既需要一台设备连接多个客户终端（以太网和交换机最合适），又需要对用户进行控制，如计费、认证等（PPP协议最适合），所以因为需求所以产生技术，这就是pppoe产生的价值所在，市场决定需求，需求决定技术。
- pppoe是一种C/S构架，分为服务端和客户端。典型应用就是xDSL技术，代表有ADSL技术，就是拨号上网技术，使用modem进行的拨号上网技术。pppoe分为2个阶段，discovery发现阶段和session会话阶段。其中在：
 - 一、discovery阶段，是进行pppoe的发现和响应阶段。
 - 二、session阶段，是进行ppp链路建立的阶段

2) PPPoE配置

- pppoe分为服务器端的配置和客户端的配置，下面分别来配置pppoe服务器和pppoe客户端，这里使用路由器作为pppoe客户端代替用户进行拨号连接。拓扑如下：



- 这张拓扑的网络环境是：PC1通过nat进行连接到internet上网，pppoe-client路由器代替用户进行pppoe拨号及nat功能使用户能够进行ADSL拨号上网，ppoe-server路由器模拟ISP端的pppoe服务器与pppoe-client建立pppoe连接，实现pc1能够访问internet的需求。

(1) **pppoe**服务器端的配置

配置思路:

1、**Virtual-Template**虚拟模板接口的配置:

为了让同为L2层协议的以太网承载**ppp**，那么就需要配置**vt**虚拟模板（**Virtual-Template**），**VT**模板就是为了让一条链路上可以封装多种同层协议的虚拟接口。因为现在的以太网物理接口已经默认封装了以太网协议，无法再封装其他的**wan**协议了，所以才需要**vt**来模拟一个(**WAN**)**ppp**接口，然后封装其他协议如**ppp**，最后在把**vt**绑定到物理接口，实现**ppp**和以太网协议的嵌套。

所以需要在**VT**虚拟接口中，来配置**ppp**协议，所以要在**vt**接口中配置**ppp**的认证、加密方式、**ipcp**协商等

2、配置**ppp**的其他选项，如为**pppoe**客户端分配的**ip**地址、**dns**、网关以及用于**ppp**认证的用户名和密码

3、配置好以上两步后，最后就需要把**vt**虚拟接口和连接**pppoe**客户端的物理以太网接口绑定，完成**pppoe**协议的封装。

(1) pppoe服务器端的配置

配置命令:

1、配置vt及ppp的各种参数

```
[server]interface Virtual-Template 10
  ppp authentication-mode chap
  remote address pool pppoe
  “pppoe” 中的ip地址
  ip address 12.1.1.1 255.255.255.0
  #
```

2、配置ppp的其他选项

```
ip pool pppoe
  地址池 “pppoe”
  gateway-list 12.1.1.1
  network 12.1.1.0 mask 255.255.255.0
  dns-list 218.30.19.40 61.134.1.4
  #
```

首先创建vt接口编号随意，这里是10
定义ppp采用chap方式认证
为远程pppoe客户端分配ip池

设置本端vt接口的ip地址为12.1.1.1

首先配置用于给客户端分配ip地址的地

给客户端分配的网关

给客户端分配的ip地址的范围

给客户端分配的dns地址

(1) pppoe服务器端的配置

配置命令：

aaa	进入 aaa 本地用户数据库
local-user pppoe password cipher pppoe 和密码	定义用于 ppp 认证的用户名 “ pppoe ”
local-user pppoe service-type ppp 认证的	定义用户 “ pppoe ” 的用途是做 ppp
3、将物理接口与VT虚拟接口进行绑定，实现pppoe协议的封装	
#	
interface GigabitEthernet0/0/0	
pppoe-server bind Virtual-Template 10	将 GE0/0/0 接口与 VT10 接口进行绑定
#	

到这里**pppoe-server**的配置就完成了，如果需要使用**raids**服务器进行认证的话，就需要配置**pppoe**服务器连接**radis**服务器进行验证即可，配置后面补充。

(2) pppoe客户端的配置

配置思路:

1、**DCC**（拨号控制中心）虚拟拨号接口（**dialer**）的配置，就是专门用来控制拨号的接口，在这个接口下配置封装协议、**ppp**认证、**ip**地址自动获得、**dialer**接口拨号使用的用户名、**pppoe**连接建立的等待时间、**dialer**所属的组、指定**dialer**接口的编号（这个编号是用来和物理接口绑定时候用到的编号）、**nat**地址转换等等的配置，都是在是该拨号接口下完成的。

2、用于控制**pppoe**客户端按需拨号的拨号规则，如定义哪些流量允许进行**pppoe**拨号连接。这一步只有当**pppoe**客户端是按需拨号时候才需要配置，如果是永久链接的**pppoe**，无需配置拨号规则**dialer-rule**。

3、配置好以上两步后，最后就需要把**DCC**的**dialer**虚拟接口和连接**pppoe**服务端的物理以太网接口绑定，完成**pppoe**协议。，并且修改物理接口的**MTU=1492Byte**（因为正常的以太网帧=**1500Byte**，但是**pppoe**的头部+**ppp**的头部=**6+2=8byte**，所以该物理接口以太网帧的**MTU**就应改为**1500-8=1492Byte**大小，防止该帧加上以太网头部后超过**1500Byte**）

4、添加默认路由指向**dialer**接口，以及其他的配置，如为**pc**主机分配的**dhcp**地址池、使用**nat**让**pc**主机上网等的配置。

(2) pppoe客户端的配置

配置命令：

```
[client]interface Dialer 1
link-protocol ppp
ppp chap user pppoe
ppp chap password simple pppoe
ip address ppp-negotiate
dialer user pppoe
认证用户一至
dialer bundle 1
绑定)
dialer timer idle 300
有流量就断开)
dialer-group 1
interface GigabitEthernet0/0/0
pppoe-client bind bundle 1
```

创建DCC的dialer 1 接口

封装ppp协议

配置ppp的chap认证

设置pppoe客户端自动获取ip地址

指定dialer接口拨号所使用的用户，与ppp

指定dialer 1 接口的编号（用于和物理接口

设置按需pppoe拨号的空闲时间（300s没