# 项目3

# PAP 与 CHAP 认证技术

教学目标

- 1. 理解 PPP 协议的概念和特点。
- 2. 理解 PPP 协议的会话过程。
- 3. 理解 PPP 协议的两种认证方式。
- 4. 掌握 PPP 协议的配置。

项目内容

某公司设有行政部、设计部、财务部和营销部等多个部门,公司的局域网包括多台交换 机、路由器和计算机。路由器之间通过串口相连并使用 PPP 协议,为了提高串口之间的安 全性,路由器之间使用 PAP 与 CHAP 认证技术。本项目主要介绍如何在路由器上配置 PAP 和 CHAP 功能,以提高网络接入的安全性。

相关知识

为了实现串口 PPP 协议之间的安全传输,需要使用 PAP 与 CHAP 认证技术。因此,需要先了解 PPP 协议的概念、特点、组成和会话过程,PAP 的认证和配置命令,以及 CHAP 的认证和配置命令等知识。

# 3.1 PPP 协议的概念

任何第三层的协议要通过拨号或专用链路穿越广域网时,都必须封装一种数据链路层的协议。TCP/IP 协议是 Internet 中使用十分广泛的协议,在广域网的数据链路层主要有两种用于 封装 TCP/IP 的协议: SLIP 协议和 PPP 协议。

SLIP 协议(Serial Line IP, 串行线 IP 协议)出现在 20 世纪 80 年代中期,它是一种在串行线路上封装 IP 包的简单形式。SLIP 协议只支持 IP 网络层协议,不支持 IPX 网络层协议,不提供纠错机制,无协商过程,尤其是不能协商通信双方 IP 地址等网络层属性。由于 SLIP 协议具有诸多缺陷,所以逐步被 PPP 协议所替代。

PPP 协议(Point-to-Point Protocol, 点到点协议)是一种在点到点链路上传输、封装网络 层数据包的数据链路层协议。PPP 协议处于 OSI 参考模型的数据链路层,主要用于支持全双 工的同步和异步链路,进行点到点的数据传输。

# 3.2 PPP 协议的特点

PPP 协议是目前使用十分广泛的广域网协议,具有以下特点。

- PPP 协议是面向字符的,既支持同步链路又支持异步链路。
- PPP 协议通过链路控制协议(LCP)能够有效控制数据链路的建立。
- PPP 协议支持密码认证协议 (PAP) 和询问握手认证协议 (CHAP), 可以保证网络的安 全性。
- PPP 协议支持各种网络控制协议 (NCP),可以同时支持多种网络层协议。
- PPP 协议可以对网络层地址进行协商,支持 IP 地址的远程分配,能够满足拨号线路的 需求。
- PPP 协议无重传协议,网络开销较小。

# 3.3 PPP 协议的组成

PPP 协议并非单一的协议,而是由一系列协议构成的协议簇。如图 3-1 所示,链路控制协议(Link Control Protocol, LCP)主要用于管理 PPP 数据链路,包括进行链路层参数的协商,建立、拆除和监控数据链路。网络控制协议(Network Control Protocol, NCP)主要用于协商所承载的网络层协议的类型及其属性,协商在该数据链路上所传输的数据包格式和类型,配置网络层协议等。认证协议主要是指 PAP 和 CHAP 协议,主要用于认证 PPP 协议对端设备的身份合法性,在一定程度上保证了链路的安全性。



图 3-1 PPP 协议的组成

汉所有

# 3.4 PPP 协议的会话过程

PPP 协议的会话主要分为以下 3 个过程。

#### 1. 链路建立阶段

运行 PPP 协议的设备通过发送 LCP 报文来检测链路的可用情况,如果链路可用,则会成功建立链路,否则链路建立失败。

#### 2. 可选的认证阶段

链路成功建立后,根据 PPP 数据帧中的认证选项决定是否进行认证。如果需要认证,则 开始进行 PAP 或 CHAP 认证,认证成功后进入网络层协商阶段。

#### 3. 网络层协商阶段

运行 PPP 协议的设备双方通过发送 NCP 报文来选择并配置网络层协议,双方协商使用网

络层协议,同时选择并配置网络层地址。如果协商通过,则 PPP 链路建立成功。 PPP 协议的会话过程如图 3-2 所示。



图 3-2 PPP 协议的会话过程

(1)当物理层不可用时, PPP 链路处于 Dead 阶段,链路必须从这个阶段开始和结束。当 通信双方的两端检测到物理线路激活(通常会检测到链路上有载波信号)时,就会从当前阶段 跃迁至下一个阶段。

(2)当物理层可用时,进入 Establish 阶段。PPP 链路在 Establish 阶段进行 LCP 协商,协 商的内容包括是否采用链路捆绑、使用何种认证方式、最大传输单元等。协商成功后 LCP 进 入 Opened 状态,表示底层链路已经建立。

(3)如果配置了认证,则进入 Authenticate 阶段,开始 CHAP 或 PAP 认证。这个阶段仅支 持链路控制协议、认证协议和质量检查数据报文,其他的数据报文都被丢弃。

(4) 如果认证失败,则进入 Terminate 阶段,拆除链路,LCP 状态转为 Down;如果认证 成功,则进入 Network 阶段,由 NCP 协商网络层协议参数,此时 LCP 状态仍为 Opened,而 NCP 状态从 Initial 转为 Request。

(5) NCP 协商支持 IPCP 协商, IPCP 协商主要包括双方的 IP 地址。通过 NCP 协商选择 和配置一个网络层协议。只有相应的网络层协议协商成功后,该网络协议才可以通过这条 PPP 链路发送报文。

(6) PPP 链路将一直保持通信,直至有明确的 LCP 或 NCP 的帧来关闭这条链路,或者发 生某些外部事件。

(7) PPP 协议能在任何时候终止链路。在载波丢失、认证失败、链路质量检测失败和管理员人为关闭链路等情况下均会导致链路终止。

# 3.5 PAP 认证

PAP 认证为两次握手认证,认证的过程仅在链路初始建立阶段进行。PAP 认证过程如图 3-3 所示,被认证方以明文形式发送用户名和密码到主认证方。主认证方认证用户名和密码,如果此用户名合法且密码正确,则会给对端发送 ACK 消息,通知对端认证通过,允许进入下一阶段协商;如果用户名或密码不正确,则发送 NAK 消息,通知对端认证失败。

PAP 认证失败后并不会直接将链路关闭。只有当认证失败次数达到一定值时,链路才会被 关闭,这样可以防止因误传、链路干扰等造成不必要的 LCP 重新协商过程。

PAP 认证可以在一方进行,即由一方认证另一方的身份,也可以进行双向认证。双向认证 可以理解为两个独立的单向认证过程,即要求通信双方都要通过对方的认证程序,否则无法建 立二者之间的链路。在 PAP 认证过程中,用户名和密码在网络中以明文的方式传输,如果在 传输过程中被监听,监听者可以获知用户名和密码,并利用其通过认证,从而可能对网络安全 造成威胁。因此, PAP 认证适用于对网络安全要求相对较低的环境。



图 3-3 PAP 认证过程

# 3.6 CHAP 认证

CHAP 认证为三次握手认证, CHAP 协议在链路建立开始时就完成了, 在链路建立完成后的任何时间都可以重复发送进行再认证。CHAP 认证过程如图 3-4 所示。



图 3-4 CHAP 认证过程

CHAP 单向认证是指一端作为主认证方,另一端作为被认证方。双向认证是单向认证的简 单叠加,即两端都既作为主认证方又作为被认证方。

# 3.7 PAP 与 CHAP 的区别

PAP 通过两次握手的方式完成认证,而 CHAP 通过三次握手认证远端节点。PAP 认证由 被认证方首先发起认证请求,而 CHAP 认证由主认证方首先发起认证请求。PAP 认证的密码 以明文的方式在链路上发送,并且当 PPP 链路建立后,被认证方会不停地在链路上反复发送 用户名和密码,直到身份认证过程结束,所以不能防止攻击。CHAP 认证只在网络上传输用户 名,并不传输密码,因此它的安全性比 PAP 认证高。

PAP 和 CHAP 都支持双向身份认证,也就是说,参与认证的一方可以同时是认证方和被认证方。由于 CHAP 认证的安全性优于 PAP 认证,所以 CHAP 认证的应用更加广泛。

# 3.8 PAP 的配置命令

40

#### 1. PAP 主认证方的配置命令

```
[H3C] int s1/0
[H3C-Serial1/0] link-protocol ppp
[H3C-Serial1/0 ]ppp authentication-mode pap
```

/\*进入路由器的串口模式 /\*接口封装 PPP 协议

项目 3 PAP 与 CHAP 认证技术

/*配置端口为 PAP 认证,若配置了这条命令,那么这台设备就为主认证方					
[H3C-Serial1/0] quit					
[H3C] local-user 用户名 class network	/*创建被认证方的用户名和密码				
[H3C-luser-network-test] password simple 密码					
[H3C-luser-network-test] service-type ppp	/* <b>用户类型为</b> PPP <b>用户</b>				

#### 2. PAP 被认证方的配置命令

[H3C] int s1/0 /\*进入路由器的串口模式 [H3C-Serial1/0] ppp pap local-user 用户名 password simple 密码 /\*被认证方将用户名和密码发送给主认证方

操作示例:如图 3-5 所示, RTA 和 RTB 之间使用 PPP 协议,为了提高串口之间的安全性,使用了 PAP 单向认证, RTA 为主认证方, RTB 为被认证方,认证的用户名为 sxvtc,密码为 654321。



在 RTA 上配置 PAP 认证的主认证方。

```
<H3C> system-view
[H3C] sysname RTA
[RTA] int s1/0
[RTA-Serial1/0] ip address 10.1.1.1 30
[RTA-Serial1/0] link-protocol ppp
[RTA-Serial1/0] ppp authentication-mode pap /*主认证方开启 PAP 认证
[RTA-Serial1/0] quit
[RTA] local-user sxvtc class network /*创建用户 sxvtc,密码为 654321
[RTA-luser-network-sxvtc] password simple 654321
[RTA-luser-network-sxvtc] service-type ppp
[RTA-luser-network-sxvtc] quit
```

在 RTB 上配置 PAP 认证的被认证方。

```
<H3C> system-view
[H3C] sysname RTB
[RTB] int s1/0
[RTB-Serial1/0] ip address 10.1.1.2 30
[RTB-Serial1/0] link-protocol ppp
[RTB-Serial1/0] ppp pap local-user sxvtc password simple 654321
/*被认证方发送账号密码给主认证方进行认证
```

[RTB-Serial1/0] quit

# 3.9 CHAP 的配置命令

1. CHAP 主认证方的配置命令

[H3C] local-user 对端用户名 class network

/\*创建对端用户名和密码



```
[H3C-luser-network-user] password simple 密码/*双方密码应一致[H3C-luser-network-user] service-type ppp/*用户类型为 PPP 用户[H3C-luser-network-user] quit/*进入路由器的串口模式[H3C] int s1/0/*进入路由器的串口模式[H3C-Serial1/0] ppp authentication-mode chap/*配置端口为 CHAP 认证,若配置了这条命令,那么这台设备就是主认证方[H3C-Serial1/0] ppp chap user 本端用户名/*发送本端用户名[H3C-Serial1/0] quit/*
```

#### 2. CHAP 被认证方的配置命令

```
[H3C] local-user 对端用户名 class network/*创建对端用户名和密码[H3C-luser-network-user] password simple 密码/*双方密码应一致[H3C-luser-network-user] service-type ppp/*用户类型为 PPP 用户[H3C-luser-network-user] quit/*用之型为 PPP 用户[H3C] int s1/0/*进入路由器的串口模式[H3C-Serial1/0] ppp chap user 本端用户名/*发送本端用户名
```

操作示例:如图 3-6 所示, RTA 和 RTB 之间使用 PPP 协议,为了提高串口之间的安全性,使用了 CHAP 双向认证, RTA 和 RTB 既是主认证方又是被认证方,密码为 123123。



在 RTA 上的配置如下所示。

```
<H3C> system-view
[H3C] sysname RTA
[RTA] int s1/0
[RTA-Serial1/0] ip address 20.1.1.1 30
[RTA-Serial1/0] ppp authentication-mode chap /*开启 CHAP 认证,作为主认证方
[RTA-Serial1/0] ppp chap user rta /*发送本地用户名 RTA 给对端
[RTA-Serial1/0] quit
[RTA] local-user rtb class network /*创建对端用户 RTB 和密码 123123
[RTA-luser-network-rtb] password simple 123123
[RTA-luser-network-rtb] service-type ppp /*用户类型为 PPP 用户
[RTA-luser-network-rtb] quit
```

```
在 RTB 上的配置如下所示。
```

```
<H3C> system-view
[H3C] sysname RTB
[RTB] int s1/0
[RTB-Serial1/0] ip address 20.1.1.2 30
[RTB-Serial1/0] ppp authentication-mode chap
[RTB-Serial1/0] ppp chap user rtb
[RTB-Serial1/0] quit
[RTB] local-user rta class network
/*创建对端用户名 RTA 和密码 123123
```

```
[RTB-luser-network-rta] password simple 123123
[RTB-luser-network-rta] service-type ppp /*用户类型为 PPP 用户
[RTB-luser-network-rta] quit
```

# 3.10 工作任务示例

如图 3-7 所示,某公司的局域网由 3 台路由器、1 台三层交换机和 1 台二层交换机组成, SW3 与 R1 和 R2 之间运行 OSPF 路由协议,R2 和 R3 之间运行 RIPv2 路由协议。为了提高串 口之间的安全性,R1 和 R2 之间使用 PAP 单向认证,R1 为主认证方,R2 为被认证方,认证 的用户名为 test1,密码为 123456。R2 和 R3 之间使用 CHAP 双向认证,用户名为对方的路由 器名称,密码为 123456。若你是公司的网络管理员,请进行合理的设置使全网互通。



图 3-7 网络拓扑结构

该公司局域网的 IP 地址规划如表 3-1 所示。

表 3-1 IP 地址规划

设备名称	IP 地 址	子网掩码	网关
SW3的GE_0/24	10.1.1.1	255.255.255.0	
SW3 的 SVI 10	192.168.10.1	255.255.255.0	
SW3 的 SVI 20	192.168.20.1	255.255.255.0	
R1的GE_0/0	10.1.1.2	255.255.255.0	CL RA
R1的S_1/0	20.1.1.1	255.255.255.0	
R2的S_1/0	20.1.1.2	255.255.255.0	
R2的S_2/0	30.1.1.1	255.255.255.0	
R3 的 S_2/0	30.1.1.2	255.255.255.0	
R3的G0/0.30	192.168.30.1	255.255.255.0	
R3的G0/0.40	192.168.40.1	255.255.255.0	
PC1	192.168.10.10	255.255.255.0	192.168.10.1
PC2	192.168.20.20	255.255.255.0	192.168.20.1
PC3	192.168.30.30	255.255.255.0	192.168.30.1
PC4	192.168.40.40	255.255.255.0	192.168.40.1

## 具体实施步骤

步骤 1: 为 SW3、R1、R2 和 R3 的端口配置 IP 地址。 在 SW3 上划分 VLAN,并配置基本的 IP 地址。

```
/*由用户视图进入系统视图
<H3C>system-view
[H3C]sysname SW3
                                           /*将设备命名为 SW3
                                           /*创建 VLAN 10
[SW3]vlan 10
                                           /*将 G1/0/1 端口加入 VLAN 10 中
[SW3-vlan10]port GigabitEthernet 1/0/1
[SW3-vlan10]vlan 20
[SW3-vlan20]port GigabitEthernet 1/0/2
                                           /*配置 VLAN 10 的网关为 192.168.10.1
[SW3-vlan20]int vlan 10
[SW3-Vlan-interface10]ip address 192.168.10.1 24
                                           /*配置 VLAN 20 的网关为 192.168.20.1
[SW3-Vlan-interface10]int vlan 20
[SW3-Vlan-interface20]ip address 192.168.20.1 24
[SW3-Vlan-interface20]quit
[SW3]int GigabitEthernet 1/0/24
                                           /*进入 G1/0/24 端口
                                                 /*交换机端口开启路由模式
[SW3-GigabitEthernet1/0/24]port link-mode route
[SW3-GigabitEthernet1/0/24]ip address 10.1.1.1 24
[SW3-GigabitEthernet1/0/24]quit
                                           /*杳看 SW3 的 IP 地址
[SW3]dis ip int b
*down: administratively down
(s): spoofing (1): loopback
Interface
                                               IP Address
                                                              Description
                        Physical
                                   Protocol
GE1/0/24
                                               10.1.1.1
                       up
                                   up
                                                               _ _
MGE0/0/0
                       down
                                   down
Vlan10
                                               192.168.10.1
                                   up
                       up
Vlan20
                                               192.168.20.1
                       up
                                   up
```

在 R1 上配置基本的 IP 地址。

```
<H3C>system-view
                                             /*将设备命名为 R1
[H3C]sysname R1
[R1]int q0/0
[R1-GigabitEthernet0/0]ip address 10.1.1.2 24
[R1-GigabitEthernet0/0]int s1/0
[R1-Serial1/0]ip address 20.1.1.1 24
                                             /*查看 R1 的 IP 地址
[R1-Serial1/0]dis ip int b
*down: administratively down
(s): spoofing (l): loopback
Interface
                      Physical Protocol IP Address
                                                        Description
GE0/0
                      up
                               up
                                         10.1.1.2
GE0/1
                      down
                                down
GE0/2
                                down
                      down
                                down
GE5/0
                      down
GE5/1
                      down
                                down
GE6/0
                      down
                                down
GE6/1
                      down
                                down
Ser1/0
                                         20.1.1.1
                       up
                                up
```

项目 3 PAP 与 CHAP 认证技术

Ser2/0	down	down	 
Ser3/0	down	down	 
Ser4/0	down	down	 

在 R2 上配置基本的 IP 地址。

<h3c>system-view</h3c>				
[H3C]sysname R2			/*将设备命令	<b>3为</b> R2
[R2]int s1/0				
[R2-Serial1/0]ip addr	ess 20.1.	1.2 24		
[R2-Serial1/0]int s2/	0			
<pre>[R2-Serial2/0]ip addr [R2-Serial2/0]dis ip</pre>	ess 30.1. int b	1.1 24	/* <b>查看</b> R2 的	] IP <b>地址</b>
*down: administrative	ly down			
(s): spoofing (l): lo	oopback			
Interface	Physical	Protocol	IP Address	Description
GE0/0	down	down		
GE0/1	down	down		
GE0/2	down	down		
GE5/0	down	down		
GE5/1	down	down		
GE6/0	down	down		
GE6/1	down	down		
Ser1/0	up	up	20.1.1.2	
Ser2/0	up	up	30.1.1.1	
Ser3/0	down	down		
Ser4/0	down	down		

在R3上配置基本的IP地址。

```
<H3C>system-view
                                                       /*将设备命名为 R3
[H3C]sysname R3
[R3]int s2/0
[R3-Serial2/0]ip address 30.1.1.2 24
[R3-Serial2/0]quit
[R3]int GigabitEthernet 0/0.30
[R3-GigabitEthernet0/0.30]vlan-type dot1q vid 30
/*子接口封装为 dot1q 协议并分配给 VLAN 30
[R3-GigabitEthernet0/0.30]ip address 192.168.30.1 24
                                                       /*配置子接口的 IP 地址
[R3-GigabitEthernet0/0.30]int g0/0.40
[R3-GigabitEthernet0/0.40] vlan-type dot1g vid 40
/*子接口封装为 dot1q 协议并分配给 VLAN 40
[R3-GigabitEthernet0/0.40]ip address 192.168.40.1 24
                                                       /*配置子接口的 IP 地址
[R3-GigabitEthernet0/0.40]guit
[R3]dis ip int b
                                                       /*查看 R3 的 IP 地址
*down: administratively down
(s): spoofing (l): loopback
Interface
                      Physical Protocol IP Address
                                                       Description
GE0/0
                      up
                               up
                                                        ___
GE0/0.30
                      up
                               up
                                        192.168.30.1
                                                       --
GE0/0.40
                                        192.168.40.1
                      up
                               up
```

#### H3C 高级路由与交换技术

GE0/1	down	down		
GE0/2	down	down		
GE5/0	down	down		
GE5/1	down	down		
GE6/0	down	down		
GE6/1	down	down		
Ser1/0	down	down		
Ser2/0	up	up	30.1.1.2	
Ser3/0	down	down		
Ser4/0	down	down		
[83]				

在 SW2 上划分 VLAN,将端口加入相应的 VLAN 中。

步骤 2: 为 SW3、R1、R2 和 R3 配置动态路由协议。 为 SW3 配置 OSPF 动态路由协议。

```
[SW3]ospf
[SW3-ospf-1]area 0
[SW3-ospf-1-area-0.0.0.0]network 10.1.1.0 0.0.0.255
[SW3-ospf-1-area-0.0.0.0]network 192.168.10.0 0.0.0.255
[SW3-ospf-1-area-0.0.0.0]network 192.168.20.0 0.0.0.255
[SW3-ospf-1-area-0.0.0.0]quit
```

为R1 配置 OSPF 动态路由协议。

```
[R1]ospf
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0]network 20.1.1.0 0.0.0.255
[R1-ospf-1-area-0.0.0]network 10.1.1.0 0.0.0.255
[R1-ospf-1-area-0.0.0]quit
[R1-ospf-1]
```

为 R2 的 S0/0 配置 OSPF 动态路由协议,为 S0/1 配置 RIPv2 动态路由协议。

```
[R2]ospf
[R2-ospf-1]area 0
[R2-ospf-1-area-0.0.0.0]network 20.1.1.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]quit
[R2-ospf-1]quit
[R2]rip
[R2-rip-1]version 2
```

```
[R2-rip-1]undo summary
[R2-rip-1]network 30.1.1.0
[R2-rip-1]quit
```

为R3 配置 RIPv2 动态路由协议。

```
[R3]rip
[R3-rip-1]version 2
[R3-rip-1]undo summary
[R3-rip-1]network 30.1.1.0
[R3-rip-1]network 192.168.30.0
[R3-rip-1]network 192.168.40.0
[R3-rip-1]quit
/*在 R1 上查看路由表,发现没有学到 RIP 的路由,只学习了 2 条 OSPF 的路由,因为没有配置路由引入
```

[R1]dis ip routing-table

Destinations : 19 Routes : 19

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
10.1.1.0/24	Direct	0	0	10.1.1.2	GE0/0
10.1.1.0/32	Direct	0	0	10.1.1.2	GE0/0
10.1.1.2/32	Direct	0	0	127.0.0.1	InLoop0
10.1.1.255/32	Direct	0	0	10.1.1.2	GE0/0
20.1.1.0/24	Direct	0	0	20.1.1.1	Ser1/0
20.1.1.0/32	Direct	0	0	20.1.1.1	Ser1/0
20.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
20.1.1.2/32	Direct	0	0	20.1.1.2	Ser1/0
20.1.1.255/32	Direct	0	0	20.1.1.1	Ser1/0
127.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.10.0/24	O_INTRA	10	2	10.1.1.1	GE0/0
192.168.20.0/24	O_INTRA	10	2	10.1.1.1	GE0/0
224.0.0/4	Direct	0	0	0.0.0	NULLO
224.0.0/24	Direct	0	0	0.0.0.0	NULLO
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

步骤 3: 在 R2 上配置路由引入。

```
[R2]ospf 1
[R2-ospf-1]import-route rip /*在 OSPF 路由中引入 RIP 路由
[R2-ospf-1]quit
[R2]rip
[R2-rip-1]import-route ospf cost 2 /*在 RIP 路由中引入 OSPF 路由
[R2-rip-1]quit
/*再次查看 R1 的路由表,发现没有 30.1.1.0 这个网段,请思考这是为什么
[R1]dis ip routing-table
```

Destinations : 21 Routes : 21

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
10.1.1.0/24	Direct	0	0	10.1.1.2	GE0/0
10.1.1.0/32	Direct	0	0	10.1.1.2	GE0/0
10.1.1.2/32	Direct	0	0	127.0.0.1	InLoop0
10.1.1.255/32	Direct	0	0	10.1.1.2	GE0/0
20.1.1.0/24	Direct	0	0	20.1.1.1	Ser1/0
20.1.1.0/32	Direct	0	0	20.1.1.1	Ser1/0
20.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
20.1.1.2/32	Direct	0	0	20.1.1.2	Ser1/0
20.1.1.255/32	Direct	0	0	20.1.1.1	Ser1/0
127.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.10.0/24	O_INTRA	10	2	10.1.1.1	GE0/0
192.168.20.0/24	O_INTRA	10	2	10.1.1.1	GE0/0
192.168.30.0/24	O_ASE2	150	1	20.1.1.2	Ser1/0
192.168.40.0/24	O_ASE2	150	1	20.1.1.2	Ser1/0
224.0.0/4	Direct	0	0	0.0.0.0	NULLO
224.0.0/24	Direct	0	0	0.0.0.0	NULLO
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
/*因为对 R2 来说只是将 F	RIPv2 中的	路由	E分发到 OSPE	中,而30.1.1.0	这个网段对 R2 来说是直连

网段, R2 重发布的时候没有发布直连网段, 所以 R1 是学习不到 30.1.1.0 这个网段的

步骤 4: 在 R2 上重分发直连网段。

```
[R2]ospf
[R2-ospf-1]import-route direct
[R2-ospf-1]quit
/*再次查看 R1 的路由表,已经有 30.1.1.0 这个网段,学习了全网路由
[R1]dis ip routing-table
Destinations : 23
                   Routes : 23
Destination/Mask
                 Proto Pre Cost
                                      NextHop
                                                    Interface
0.0.0.0/32
                  Direct 0 0
                                      127.0.0.1
                                                    InLoop0
10.1.1.0/24
                 Direct 0 0
                                      10.1.1.2
                                                    GE0/0
10.1.1.0/32
                 Direct 0 0
                                      10.1.1.2
                                                    GE0/0
10.1.1.2/32
                  Direct 0 0
                                      127.0.0.1
                                                    InLoop0
                                      10.1.1.2
10.1.1.255/32
                 Direct 0 0
                                                   GE0/0
20.1.1.0/24
                  Direct 0
                             0
                                      20.1.1.1
                                                    Ser1/0
20.1.1.0/32
                  Direct 0
                                      20.1.1.1
                                                    Ser1/0
                             0
20.1.1.1/32
                 Direct 0 0
                                      127.0.0.1
                                                   InLoop0
20.1.1.2/32
                  Direct 0 0
                                      20.1.1.2
                                                    Ser1/0
20.1.1.255/32
                  Direct 0 0
                                      20.1.1.1
                                                    Ser1/0
30.1.1.0/24
                                      20.1.1.2
                  O ASE2 150 1
                                                    Ser1/0
30.1.1.2/32
                  O ASE2 150 1
                                      20.1.1.2
                                                    Ser1/0
```

127.0.0.1

InLoop0

Direct 0 0

127.0.0.0/8

127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.10.0/24	O_INTRA	10	2	10.1.1.1	GE0/0
192.168.20.0/24	O_INTRA	10	2	10.1.1.1	GE0/0
192.168.30.0/24	O_ASE2	150	1	20.1.1.2	Ser1/0
192.168.40.0/24	O_ASE2	150	1	20.1.1.2	Ser1/0
224.0.0/4	Direct	0	0	0.0.0	NULLO
224.0.0/24	Direct	0	0	0.0.0	NULLO
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

步骤 5:为 PC1、PC2、PC3、PC4 配置 IP 地址和网关,测试 PC1 与 PC2、PC3、PC4 之 间的连通性。测试 HCL 主机连通性的方法如下: Ping –S(大写) 源地址 目的地址。

1. PC1 可以和 PC2 互通

PC1与PC2的通信情况如图 3-8 所示。



图 3-8 PC1 与 PC2 的通信情况

#### 2. PC1 可以和 PC3 互通

PC1与PC3的通信情况如图 3-9 所示。



图 3-9 PC1 与 PC3 的通信情况

## 3. PC1 可以和 PC4 互通

PC1 与 PC4 的通信情况如图 3-10 所示。



图 3-10 PC1 与 PC4 的通信情况

所不

PC1 与 PC2、PC3、PC4 已经可以相互通信,全网互通,但是 R1 和 R2 之间、R2 和 R3 之间还未开启 PAP 与 CHAP 认证。

步骤 6: 在 R1 的 S1/0 和 R2 的 S1/0 之间配置 PAP 认证,其中 R1 是主认证方, R2 是被 认证方。

```
[R1] int s1/0[R1-Serial1/0]link-protocol ppp/*接口封装 PPP 协议[R1-Serial1/0]ppp authentication-mode pap/*开启 PAP 认证[R1-Serial1/0]quit[R1]local-user test1 class network[R1-luser-network-test1]password simple 123456[R1-luser-network-test1]service-type ppp[R1-luser-network-test1]quit
```

[R2]int s1/0	/*进入 R2 的 S1/0 端口
[R2-Serial1/0]shutdown	/* <b>关闭</b> R2 <b>的</b> S1/0 <b>端口</b>
[R2-Serial1/0]undo shutdown	/* <b>开启</b> R2 <b>的</b> S1/0 <b>端口</b>
[R2-Serial1/0]dis ip int b	

/\*关闭和开启的 S1/0 端口, PAP 认证生效, 查看 S1/0 的状态,发现 S1/0 已经 down,因为 R1 开 启了 PAP 认证

```
*down: administratively down
```

(s):	spoofing	(1): 1	oopback			
Inter	face		Physical	Protocol	IP Address	Description
GE0/0	)		down	down		
GE0/1	-		down	down		
GE0/2	2		down	down		
GE5/0	)		down	down		
GE5/1	-		down	down		
GE6/0	)		down	down		
GE6/1	-		down	down		
Ser1/	′0		up	down	20.1.1.2	
Ser2/	0		up	up	30.1.1.1	
Ser3/	0		down	down		
Ser4/	0		down	down		

[R2-Serial1/0]ppp pap local-user test1 password simple 123456 /\*R2 将用户名和密码发给主认证方 R1

[R2-Serial1/0]

%Oct 12 02.39.35.428 2016 R2 IFNET/5/LINK\_UPDOWN: Line protocol state on the interface Serial1/0 changed to up.

#### /\*路由器弹出提示 S1/0 端口的状态变为 up

%Oct 12 02.39.36.442 2016 R2 OSPF/5/OSPF\_NBR\_CHG: OSPF 1 Neighbor 20.1.1.1(Serial1/0) changed from LOADING to FULL.

/\*路由器弹出提示 OSPF 的状态变为 FULL

[R2-Serial1/0]dis ip int b /\*查看 R2 路由表发现 S1/0 端口的状态变为 up

*down: administratively down					
(s): spoofing (l): lo	oopback				
Interface	Physical	Protocol	IP Address	Description	
GE0/0	down	down			
GE0/1	down	down			
GE0/2	down	down			
GE5/0	down	down			
GE5/1	down	down			
GE6/0	down	down			
GE6/1	down	down			
Ser1/0	up	up	20.1.1.2		
Ser2/0	up	up	30.1.1.1		
Ser3/0	down	down			
Ser4/0	down	down			

#### 步骤 7:在 R2 上开启 CHAP 双向认证。

[R2]local-user R3 class network	/* <b>创建用户</b>
[R2-luser-network-R3]password simple 123456 [R2-luser-network-R3]service-type ppp	/* <b>用户类型为</b> PPP
[R2-luser-network-R3]quit	
[R2]int s2/0	
[R2-Serial2/0]ppp authentication-mode chap	/*开启 CHAP 认证
[R2-Serial2/0]ppp chap user R2	/* <b>发送认证用户名</b> R2
[R2-Serial2/0]quit	

#### 步骤 8: 在 R3 上开启 CHAP 双向认证。

```
[R3]local-user R2 class network
                                                 /*创建用户 R2, 密码为 123456
[R3-luser-network-R2]password simple 123456
[R3-luser-network-R2]service-type ppp
                                                 /*用户类型为 PPP
[R3-luser-network-R2]quit
[R3]int s2/0
                                                /*开启 CHAP 认证
[R3-Serial2/0]ppp authentication-mode chap
                                                 /*发送认证用户名 R3
[R3-Serial2/0]ppp chap user R3
[R3-Serial2/0]quit
[R3]dis ip int b
*down: administratively down
(s): spoofing (l): loopback
Interface
                      Physical Protocol IP Address
                                                        Description
GE0/0
                      up
                               up
                                         _ _
GE0/0.30
                                         192.168.30.1
                      up
                               up
                                                        192.168.40.1
GE0/0.40
                      up
                               up
                                                        1.2
GE0/1
                               down
                      down
GE0/2
                               down
                      down
GE5/0
                               down
                      down
GE5/1
                               down
                      down
GE6/0
                      down
                               down
GE6/1
                      down
                               down
Ser1/0
                      down
                                down
Ser2/0
                                         30.1.1.2
                               up
                      up
```

#### H3C 高级路由与交换技术

Ser3/0 Ser4/0	down down	d d	own own				
步骤 9: 再次查看 R1	的路由表知	发现伯	乃能学到全网	网路由,全网	贯通。		
[R1]dis ip routing-t	table		/*查看	FR1 的路由表()	乃能学到≦	全网路由	
Destinations : 23	Route	es :	23				
Destination/Mask	Proto	Pre	Cost	NextHop		Interface	
0.0.0/32	Direct	0	0	127.0.0.1		InLoop0	
10.1.1.0/24	Direct	0	0	10.1.1.2		GE0/0	
10.1.1.0/32	Direct	0	0	10.1.1.2		GE0/0	
10.1.1.2/32	Direct	0	0	127.0.0.1		InLoop0	
10.1.1.255/32	Direct	0	0	10.1.1.2		GE0/0	
20.1.1.0/24	Direct	0	0	20.1.1.1		Ser1/0	
20.1.1.0/32	Direct	0	0	20.1.1.1		Ser1/0	
20.1.1.1/32	Direct	0	0	127.0.0.1		InLoop0	
20.1.1.2/32	Direct	0	0	20.1.1.2		Ser1/0	
20.1.1.255/32	Direct	0	0	20.1.1.1		Ser1/0	
30.1.1.0/24	O_ASE2	150	1	20.1.1.2		Ser1/0	
30.1.1.2/32	O_ASE2	150	1	20.1.1.2		Ser1/0	
127.0.0.0/8	Direct	0	0	127.0.0.1		InLoop0	
127.0.0.0/32	Direct	0	0	127.0.0.1		InLoop0	
127.0.0.1/32	Direct	0	0	127.0.0.1		InLoop0	
127.255.255.255/32	Direct	0	0	127.0.0.1		InLoop0	
192.168.10.0/24	O_INTRA	10	2	10.1.1.1		GE0/0	
192.168.20.0/24	O_INTRA	10	2	10.1.1.1		GE0/0	
192.168.30.0/24	O_ASE2	150	1	20.1.1.2		Ser1/0	
192.168.40.0/24	O_ASE2	150	1	20.1.1.2		Ser1/0	
224.0.0/4	Direct	0	0	0.0.0.0		NULLO	
224.0.0/24	Direct	0	0	0.0.0.0		NULLO	
255.255.255.255/32	Direct	0	0	127.0.0.1		InLoop0	

# 3.11 项目小结

PAP 认证过程非常简单,采用二次握手机制,使用明文格式发送用户名和密码。发起方为被认证方,可以做无限次尝试(暴力破解)。只在链路建立的阶段进行 PAP 认证,一旦链路建立成功将不再进行认证检测。目前,PAP 认证在 PPPOE 拨号环境中用得比较多。CHAP 认证 过程比较复杂,采用三次握手机制,使用密文格式发送 CHAP 认证信息。由认证方发起 CHAP 认证 认证,有效避免暴力破解,在链路建立成功后具有再次认证检测机制。目前,CHAP 认证在企 业网的远程接入环境中用得比较多。

# 习题

一、选择题

- 1. 下列对 PPP 协议的特点的描述正确的是 ( )。
  - A. PPP 协议既支持同步链路又支持异步链路
  - B. PPP 协议支持身份认证
  - C. PPP 协议可以对网络地址进行协商
  - D. 以上几项都正确
- 2. 下列对 PAP 认证的描述正确的是 ( )。
  - A. PAP 认证采用二次握手机制
  - B. PAP 的用户名是明文,但密码是密文
  - C. PAP的用户名是密文,但密码是明文
  - D. PAP 的用户名和密码都是密文
- 3. 在配置完 PAP 认证后,发现协议层处于 Down 状态,可能是因为 ()。
  - A. 主认证方没有创建认证用户
  - B. 被认证方发送了错误的账号密码
  - C. 广域网端口封装协议没有配置为 PPP
  - D. 以上几项都正确
- 4. 下列对 CHAP 认证的描述正确的是 ( )。
  - A. CHAP 认证采用二次握手机制
  - B. CHAP 认证采用三次握手机制
  - C. CHAP的用户名是明文,但密码是密文
  - D. CHAP的用户名是密文,但密码是明文
- 二、简答题
- 1. 简述 CHAP 双向认证的工作原理。
- 2. 与 PAP 认证相比, CHAP 认证的不同之处和优点表现在哪些方面?
- 3. 简述 CHAP 单向认证和双向认证在配置上的不同之处。