

实验十二、路由器广域网 PPP 封装 PAP 验证配置

一、实验目的

1. 掌握 PAP 验证配置
2. 理解验证过程

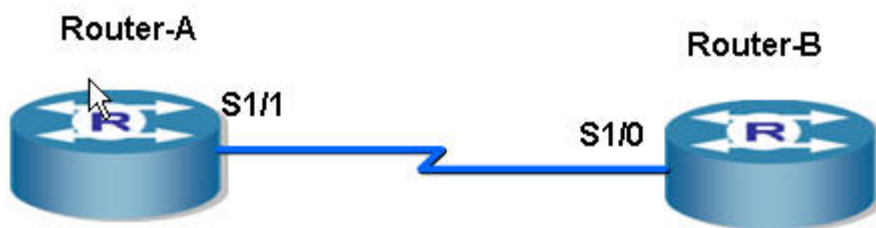
二、应用环境

基于安全的考虑，需要路由器双方经过验证后才能建立连接

三、实验设备

- | | |
|-------------|----|
| 1. DCR-1751 | 两台 |
| 2. CR-V35MT | 一条 |
| 3. CR-V35FC | 一条 |

四、实验拓扑



五、实验要求

Router-A		Router-B	
接口	IP 地址	接口	IP 地址
S1/1 DCE	192.168.1.1	S1/0 DTE	192.168.1.2
帐号	密码	帐号	密码
RouterA	digitalchinaA	RouterB	digitalchinaB

六、实验步骤

第一步 Router-A 的配置

Router>enable

Router #config

Router _config#hostname Router-A

Router-A_config#username RouterB password digitalchinaB ! 设置帐号密码

! 进入特权模式

! 进入全局配置模式

! 修改机器名

```
Router-A_config#interface s1/1          ! 进入接口模式
Router-A_config_s1/0#ip address 192.168.1.1 255.255.255.0    ! 配置 IP 地址
Router-A_config_s1/1#encapsulation PPP          ! 封装 PPP 协议
Router-A_config_s1/0#ppp authentication pap      ! 设置验证方式
Router-A_config_s1/0#ppp pap sent-username RouterA digitalchinaA
                                           ! 设置发送给对方验证的帐号密码
Router-A_config_s1/0#physical-layer speed 64000          ! 配置 DCE 时钟频率
Router-A_config_s1/0#no shutdown
Router-A_config_s1/0#^Z                      ! 按 ctrl + z 进入特权模式
```

第二步：查看配置

```
Router-A#show interface s1/1          ! 查看接口状态
Serial1/0 is up, line protocol is down    ! 对端没有配置，所以协议是 DOWN
Mode=Sync DCE Speed=64000                ! 查看 DCE
DTR=UP,DSR=UP,RTS=UP,CTS=DOWN,DCD=UP
Interface address is 192.168.1.1/24        ! 查看 IP 地址
MTU 1500 bytes, BW 64 kbit, DLY 2000 usec
Encapsulation prototol PPP, link check interval is 10 sec    ! 查看封装协议
Octets   Received0, Octets Sent 0
Frames Received 0, Frames Sent 0, Link-check Frames Received0
Link-check Frames Sent 89,   LoopBack times 0
Frames Discarded 0, Unknown Protocols Frames Received 0, Sent failuile 0
Link-check Timeout 0, Queue Error 0, Link Error 0,
60 second input rate 0 bits/sec, 0 packets/sec!
60 second output rate 0 bits/sec, 0 packets/sec!
 0 packets input, 0 bytes, 8 unused_rx, 0 no buffer
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 8 packets output, 192 bytes, 0 unused_tx, 0 underruns
error:
 0 clock, 0 grace
PowerQUICC SCC specific errors:
 0 recv allocb mblk fail      0 recv no buffer
 0 transmitter queue full    0 transmitter hwqueue_full
```

第三步：Router-B 的配置

```
Router>enable          ! 进入特权模式
Router #config          ! 进入全局配置模式
Router _config#hostname Router-B    ! 修改机器名
Router-B_config#username RouterA password digitalchinaA !设置帐号密码
Router-B_config#interface s1/0      ! 进入接口模式
Router-B_config_s1/0#ip address 192.168.1.2 255.255.255.0    ! 配置 IP 地址
Router-B_config_s1/1#encapsulation PPP    ! 封装 PPP 协议
Router-A_config_s1/0#ppp authentication pap    ! 设置验证方式
Router-A_config_s1/0#ppp pap sent-username RouterB digitalchinaB
```

! 设置发送给对方验证的帐号密码

Router-B_config_s1/0#no shutdown

Router-B_config_s1/0#^Z

! 按 ctrl + z 进入特权模式

第四步：查看配置

Router-A#show interface s1/0

! 查看接口状态

Serial1/0 is **up**, line protocol is **up**

! 接口和协议都是 **up**

Mode=Sync **DTE**

! 查看 **DTE**

DTR=UP,DSR=UP,RTS=UP,CTS=DOWN,DCD=UP

Interface address is **192.168.1.2/24**

! 查看 **IP 地址**

MTU 1500 bytes, BW 64 kbit, DLY 2000 usec

Encapsulation prototol **PPP**, link check interval is 10 sec ! 查看封装协议

Octets Received0, Octets Sent 0

Frames Received 0, Frames Sent 0, Link-check Frames Received0

Link-check Frames Sent 89, LoopBack times 0

Frames Discarded 0, Unknown Protocols Frames Received 0, Sent failuile 0

Link-check Timeout 0, Queue Error 0, Link Error 0,

60 second input rate 0 bits/sec, 0 packets/sec!

60 second output rate 0 bits/sec, 0 packets/sec!

0 packets input, 0 bytes, 8 unused_rx, 0 no buffer

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

8 packets output, 192 bytes, 0 unused_tx, 0 underruns

error:

0 clock, 0 grace

PowerQUICC SCC specific errors:

0 recv allocb mblk fail 0 recv no buffer

0 transmitter queue full 0 transmitter hwqueue_full

第五步：测试连通性

Router-A#ping 192.168.1.2

PING 192.168.1.2 (192.168.1.2): 56 data bytes

!!!!

--- 192.168.1.2 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss

round-trip min/avg/max = 20/22/30 ms

七、注意事项和排错

1. 帐号密码一定要交叉对应，发送的帐号密码要和对方帐号数据库中的帐号密码对应
2. 不要忘记配置 DCE 的时钟频率

八、配置序列

Router-A 的序列

Building configuration...

Current configuration:

```
!  
!version 1.3.2E  
service timestamps log date  
service timestamps debug date  
no service password-encryption  
!  
hostname Router-A  
!  
!  
!  
!  
username routerb password 0 digitalb  
!  
!  
!  
interface FastEthernet0/0  
  ip address 192.168.2.1 255.255.255.0  
  no ip directed-broadcast  
!  
interface Ethernet2/0  
  no ip address  
  no ip directed-broadcast  
  duplex half  
!  
interface Serial1/0  
  no ip address  
  no ip directed-broadcast  
  physical-layer speed 64000  
!  
interface Serial1/1  
  ip address 192.168.1.1 255.255.255.0  
  no ip directed-broadcast  
  encapsulation ppp  
  ppp pap sent-username routera digitala  
  physical-layer speed 64000  
!  
interface Async0/0  
  no ip address  
  no ip directed-broadcast  
!  
!
```



九、共同思考

1. 在什么环境下需要配置验证方式？
2. PAP 验证是否非常安全？

十、课后练习

本实验是双向验证，尝试做单向验证的配置

十一、相关命令详解

ppp authentication

使用接口配置命令 `ppp authentication` 指定接口上使用 CHAP 或 PAP 协议的次序，使用 `no ppp authentication` 取消认证。

ppp authentication {chap|ms-chap|pap} [[list-name|default][callin]

no ppp authentication

参数

参数	参数说明
chap	在串行接口上激活CHAP
pap	在串行接口上激活PAP
ms-chap	在串行接口上激活MS-CHAP
list-name	（可选的）与AAA/TACACS+一起使用，指定执行认证时使用的TACACS+方法列表名。如果没有指定列表名，系统将使用缺省列表。使用命令 <code>aaa authentication ppp</code> 创建列表。
default	（可选的）与AAA/TACACS+一起使用。使用命令 <code>aaa authentication ppp</code> 创建缺省缺省列表。
callin	（可选的）指定仅对收到的呼叫（calls）进行认证。

进行 PPP 认证时，chap、ms-chap 和 pap 三者必选其一，或者三者任意组合。

缺省

不进行 PPP 认证。

命令模式

接口配置态

使用说明

一旦你激活了 **CHAP**、**MS-CHAP** 和 **PAP** 认证中的一个、两个或者全部激活，本地路由器在允许远端设备传送数据之前，要求对其身份进行验证。

- (1) **PAP** 认证要求远端设备发送一个名字/口令对，来检验在本地用户数据库或者远程 **TACACS/TACACS+** 数据库中是否有一个匹配项。
- (2) **CHAP** 认证发送一个 **challenge** 给远端设备，远端设备必须使用公有密钥对 **challenge** 进行加密并把加密结果和自身名字以 **response** 报文的形式返回给本地路由器。本地路由器使用远端设备名字在本地用户数据库或者远程 **TACACS/TACACS+** 数据库中查找到相应的密钥，用它对最初 **challenge** 进行加密，并验证该加密结果是否与远端设备返回的结果相同。

你可能以任何次序激活 **PAP**、**MS-CHAP** 和 **CHAP**。如果两种方法都被激活了，那么使用第一个方法在链路协商阶段提出请求。如果远端建议使用第二种方法或者简单地拒绝了第一种方法，将使用第二种方法。一些远端设备仅仅支持 **CHAP** 或仅仅支持 **PAP**。至于指定这两种认证方法的次序，则要根据你对远端设备正确进行协商的能力的估计，以及你对数据线路安全方面的考虑。**PAP** 的用户名和口令是作为明文传送的，有可能被截获和重新使用；而 **CHAP** 则消除了目前所知的大部分安全漏洞。

激活或者取消 **PPP** 认证都不会影响本地路由器是否要向远端设备验证自己。

示例

下面例子在接口 **s1/0** 上激活了 **CHAP** 认证并使用认证列表 **access1**

```
interface s1/0
encapsulation ppp
ppp authentication chap access1
```