

使用 ppp chap hostname 和 ppp authentication chap callin 命令的 PPP 认证

目录

[简介](#)

[先决条件](#)

[规则](#)

[要求](#)

[使用的组件](#)

[背景理论](#)

[配置](#)

[配置单向 CHAP 验证](#)

[配置与路由器名称不同的用户名](#)

[网络图](#)

[配置](#)

[配置说明](#)

[验证](#)

[故障排除](#)

[调试输出示例](#)

[相关信息](#)

简介

PPP 协商包括几个步骤，例如链路控制协议 (LCP) 协商、身份验证和网络控制协议 (NCP) 协商。如果双方不能就正确的参数达成协议，那么连接将被终止。一旦链路建立，双方将使用在 LCP 协商期间确定的身份验证协议进行相互验证。在开始 NCP 协商之前，必须成功通过身份验证。

PPP 支持两种身份验证协议：密码验证协议 (PAP) 和质询握手身份验证协议 (CHAP)。

先决条件

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

要求

本文档没有任何特定的前提条件。

使用的组件

本文档中的信息基于以下软件和硬件版本。

- Cisco IOS® 软件版本 11.2 或更高版本

背景理论

PAP 身份验证包含两次握手，在两次握手过程中，用户名和密码在链路上以明文发送。因此，PAP 身份验证无法防御回放和线路探测。

另一方面，CHAP 身份验证将定期使用三次握手验证远程节点的身份。在建立 PPP 链路后，主机发送将会发送一个“质询”消息到远程节点。远程节点使用通过单向哈希功能计算出来的值进行响应。主机使用自己计算出来的哈希值对响应进行检查。如果两个值匹配，则身份验证将被确认；否则，将终止连接。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意：要查找有关本文档中使用的命令的其他信息，请使用IOS命令查找工具

配置单向 CHAP 验证

当两个设备正常使用 CHAP 身份验证时，一方向另一方发送一个质询，另一方予以响应，并由质询程序进行验证。每一方都独立地验证另一方的身份。如果您希望通过呼叫路由器或设备操作不支持身份验证的非 Cisco 路由器，您必须使用 `ppp authentication chap callin` 命令。在使用带 `callin` 关键字的 `ppp authentication` 命令时，如果远程设备发起呼叫（例如远程设备“拨入”），接入服务器只需验证远程设备即可。在这种情况下，仅指定对传入（收到的）呼叫进行身份验证。

配置与路由器名称不同的用户名

当远程Cisco路由器连接到使用不同管理控制机制的Cisco或非Cisco的中央路由器，或网络服务提供商(ISP)或中央路由器轮循上时，必须配置不同于主机名的认证用户名。在此情况下，不提供路由器主机名，或者不同的时间使用不同的主机名（轮循）。并且，ISP 分配的用户名和口令可能不是远程路由器的主机名。在这种情况下，可以使用 `ppp chap hostname` 命令来指定要用于身份验证的备用用户名。

例如，请考虑多个远程设备拨入一个中心站点的情况。使用正常的 CHAP 身份验证，必须在中央路由器上配置每台远程设备的用户名（应为主机名）和共享秘密。在这种情况下，中央路由器的配置管理可能变得十分冗长和繁琐；然而，如果远程设备使用与它们的主机名称不同的用户名，则可以避免这种情况。可以为中心站点配置一个用户名和共享秘密，并将此用户名和共享秘密用于验证多个拨入客户端。

网络图

如果路由器1向路由器2发起呼叫，路由器2会向路由器1发起呼叫，但路由器1不会向路由器2发起呼叫。这是因为路由器1上配置了 `ppp authentication chap callin` 命令。这是单向身份验证的示例。

在此设置中，路由器 1 上配置了 `ppp chap hostname alias-r1` 命令。路由器 1 使用“alias-r1”而非“r1”作为用于 CHAP 身份验证的主机名。路由器 2 拨号器映射名称应与路由器 1 的 `ppp chap` 主机名匹配否则，将会建立两条 B 通道，每个方向一条通道。



配置

路由器 1

```

!
 isdn switch-type basic-5ess
!
hostname r1
!
username r2 password 0 cisco
! -- Hostname of other router and shared secret !
interface BRI0/0 ip address 20.1.1.1 255.255.255.0 no ip
directed-broadcast encapsulation ppp dialer map ip
20.1.1.2 name r2 broadcast 5772222
 dialer-group 1
 isdn switch-type basic-5ess
 ppp authentication chap callin
! -- Authentication on incoming calls only ppp chap
hostname alias-r1
! -- Alternate CHAP hostname ! access-list 101 permit
ip any any dialer-list 1 protocol ip list 101 !

```

路由器 2

```

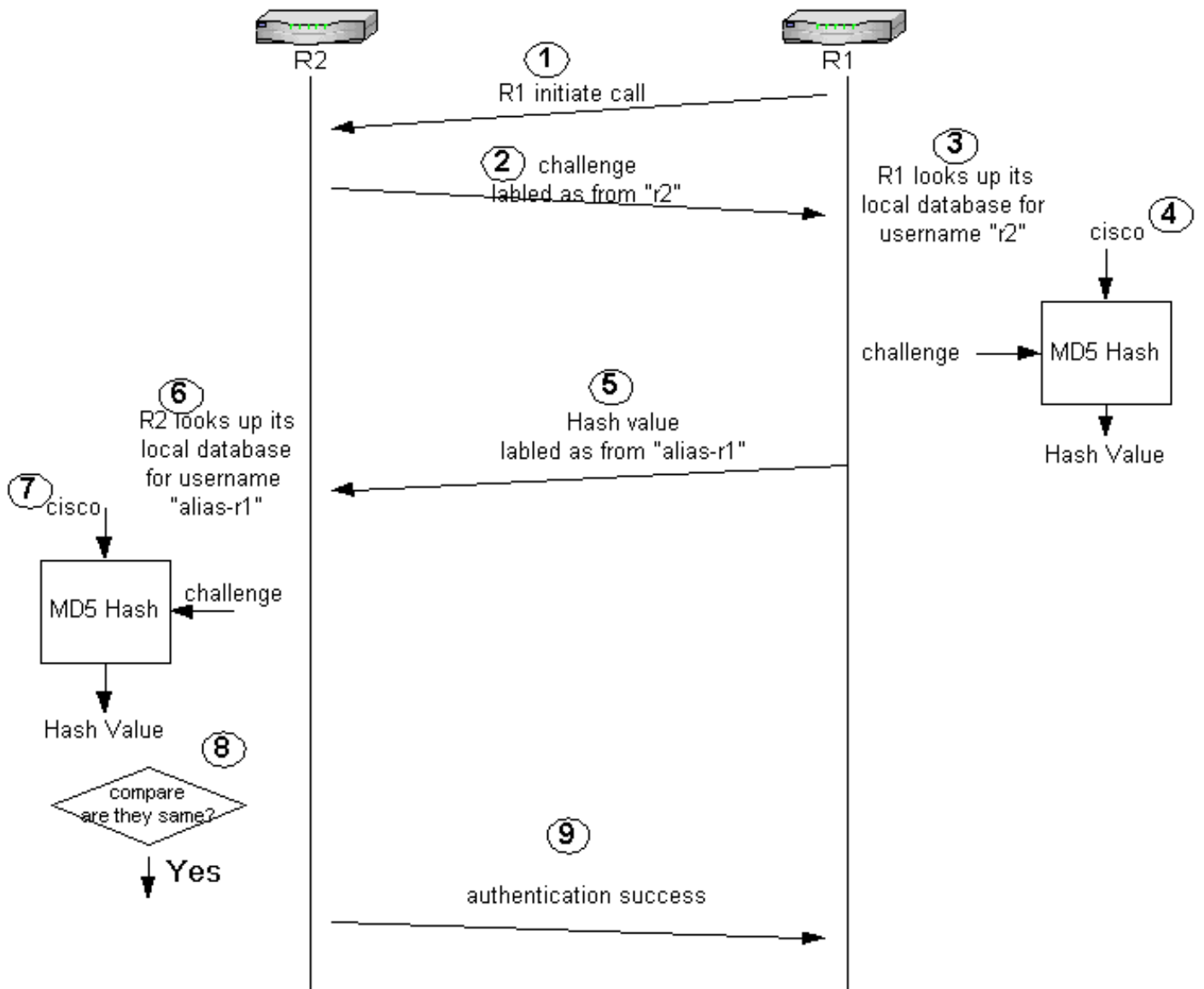
!
 isdn switch-type basic-5ess
!
hostname r2
!
username alias-r1 password 0 cisco
! -- Alternate CHAP hostname and shared secret. ! --
The username must match the one in the ppp chap hostname
! -- command on the remote router.

!
interface BRI0/0
 ip address 20.1.1.2 255.255.255.0
 no ip directed-broadcast
 encapsulation ppp
 dialer map ip 20.1.1.1 name
 alias-r1 broadcast 5771111
! -- Dialer map name matches alternate hostname
"alias-r1". dialer-group 1 isdn switch-type basic-5ess
 ppp authentication chap ! access-list 101 permit ip any
any dialer-list 1 protocol ip list 101 !

```

配置说明

相关解释请参阅位于此图下面的各个编号项：



1. 在本例中，路由器 1 发起呼叫。由于路由器 1 配置有 `ppp authentication chap callin` 命令，因此它不会质询作为呼叫方的路由器 2。
2. 当路由器 2 收到呼叫时，它将向路由器 1 发出质询以验证其身份。默认情况下，在这种身份验证中路由器的主机名是用来标识自己的。如果配置了 `ppp chap hostname name` 命令，路由器将使用此名称替代主机名作为自己的标识。在本例中，质询被标记为来自“r2”。
3. 路由器 1 收到路由器 2 的质询，并在其本地数据库中查找用户名“r2”。
4. 路由器 1 找到了“r2”口令，此口令为“cisco”。路由器 1 使用此口令和来自路由器 2 的质询作为 MD5 哈希函数的输入参数。此时即会生成哈希值。
5. 路由器 1 向路由器 2 发送哈希输出值。在此，由于 `ppp chap hostname` 命令配置为“alias-r1”，因此应答标记为来自“alias-r1”。
6. 路由器 2 收到回复，并为密码在本地数据库中查找“alias-r1” 用户名。
7. 路由器 2 发现“alias-r1”的口令是“cisco”。路由器 2 将之前发送到路由器 1 的口令和质询作为 MD5 哈希函数的输入参数。哈希函数生成一个哈希值。
8. 路由器 2 将其生成的哈希值与从路由器 1 处收到的哈希值进行比较。
9. 由于输入参数（质询和口令）相同，因此哈希值同样会成功通过验证。

验证

当前没有可用于此配置的验证过程。

故障排除

本部分提供的信息可用于对配置进行故障排除。

在尝试使用任何调试命令前，请参阅[关于调试命令的重要信息](#)

调试输出示例

以下是一个 debug ppp authentication 命令的输出示例：

路由器 1

```
r1#ping 20.1.1.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 20.1.1.2, timeout is 2 seconds:
```

```
*Mar 1 20:06:27.179: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to up
```

```
*Mar 1 20:06:27.183: %ISDN-6-CONNECT:
```

```
Interface BRI0/0:1 is now connected to 5772222
```

```
*Mar 1 20:06:27.187: BR0/0:1 PPP: Treating connection as a callout
```

```
*Mar 1 20:06:27.223: BR0/0:1 CHAP: I CHALLENGE id 57 len 23 from "r2"
```

```
! -- Received a CHAP challenge from other router (r2) *Mar 1 20:06:27.223: BR0/0:1 CHAP:
```

```
Using alternate hostname alias-r1
```

```
! -- Using alternate hostname configured with ! -- ppp chap hostname command *Mar 1
```

```
20:06:27.223: BR0/0:1 CHAP: O RESPONSE id 57 Len 29 from "alias-r1" ! -- Sending response from
```

```
"alias-r1" ! -- which is the alternate hostname for r1 *Mar 1 20:06:27.243: BR0/0:1 CHAP: I
```

```
SUCCESS id 57 Len 4 ! -- Received CHAP authentication is successful ! -- Note that r1 is not
```

```
challenging r2 .!!!! Success rate is 80 percent (4/5), round-trip min/avg/max = 36/38/40 ms r1#
```

```
*Mar 1 20:06:28.243: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0/0:1, changed state to
```

```
up r1# *Mar 1 20:06:33.187: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected to 5772222 r2
```

路由器 2

```
r2#
```

```
20:05:20: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to up
```

```
20:05:20: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected to 5771111
```

```
20:05:20: BR0/0:1 PPP: Treating connection as a callin
```

```
20:05:21: BR0/0:1 CHAP: O CHALLENGE id 57 Len 23 from "r2"
```

```
! -- r2 is sending out a challenge 20:05:21: BR0/0:1 CHAP: I RESPONSE id 57 Len 29 from
```

```
"alias-r1"
```

```
! -- Received a response from alias-r1, ! -- which is the alternate hostname on r1 20:05:21:
```

```
BR0/0:1 CHAP: O SUCCESS id 57 Len 4 ! -- Sending out CHAP authentication is successful 20:05:22:
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0/0:1, changed state to up 20:05:26: %ISDN-6-
```

```
CONNECT: Interface BRI0/0:1 is now connected to 5771111 alias-r1
```

相关信息

- [用于广域网的 PPP 命令](#)
- [了解 PPP 和 PPP 身份验证](#)
- [ISDN 调试信息](#)