

# Autenticação PPP Utilizando os Comandos ppp chap hostname e ppp authentication chap callin

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Convenções](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Material de Suporte](#)

[Configurar](#)

[Configurando a autenticação CHAP unidirecional](#)

[Configurando um nome de usuário diferente do nome do roteador](#)

[Diagrama de Rede](#)

[Configurações](#)

[Explicação de configuração](#)

[Verificar](#)

[Troubleshooting](#)

[Exemplo de debug](#)

[Informações Relacionadas](#)

## [Introdução](#)

A negociação de PPP envolve diversas etapas, como a negociação do Link Control Protocol (LCP), a autenticação e a negociação do Network Control Protocol (NCP). Se os dois lados não puderem concordar quanto aos parâmetros corretos, a conexão será encerrada. Assim que o enlace estiver estabelecido, os dois lados se autenticarão usando o protocolo de autenticação decidido durante a negociação de LCP. A autenticação deve ser bem-sucedida antes de a negociação NCP ser iniciada.

O PPP suporta dois Protocolos de Autenticação: Protocolo de autenticação de senha (PAP) e Protocolo de autenticação de handshake de desafio (CHAP).

## [Pré-requisitos](#)

### [Convenções](#)

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

### [Requisitos](#)

Não existem requisitos específicos para este documento.

## Componentes Utilizados

As informações neste documento são baseadas nas versões de software e hardware abaixo.

- Cisco IOS® Software Release 11.2 ou posterior

## Material de Suporte

A autenticação PAP envolve um handshake bidirecional no qual o nome de usuário e a senha são enviados pelo link em texto sem formatação; assim, a autenticação PAP não fornece nenhuma proteção contra analisadores de linha e playback.

A autenticação CHAP, por outro lado, confirma periodicamente a identidade do nó remoto usando um handshake tridirecional. Depois que o link PPP é estabelecido, o host envia uma mensagem de "desafio" ao nó remoto. O nó remoto responde com um valor calculado usando uma função de hash unidirecional. O host verifica a resposta, comparando-a com seu próprio cálculo do valor de hash esperado. Se os valores forem correspondentes, a autenticação será reconhecida; caso contrário, a conexão será encerrada.

## Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

**Note:** Para localizar informações adicionais sobre os comandos utilizados neste documento, utilize a [ferramenta IOS Command Lookup](#).

### Configurando a autenticação CHAP unidirecional

Quando dois dispositivos usam normalmente a autenticação CHAP, cada lado envia um desafio ao qual o outro lado responde e é, assim, autenticado pelo desafiante. Cada lado autentica o outro de maneira independente. Se você desejar trabalhar com roteadores não fabricados pela Cisco que não suportem a autenticação pelo roteador ou dispositivo de chamada, deverá usar o comando **ppp authentication chap callin**. Quando se usa o comando **ppp authentication** com a palavra-chave **callin**, o servidor de acesso autentica o dispositivo remoto somente se este houver iniciado a chamada (se o dispositivo remoto "tiver feito a chamada"). Neste caso, a autenticação é especificada somente em chamadas de entrada (recebidas).

### Configurando um nome de usuário diferente do nome do roteador

Quando um Cisco Router remoto conecta-se a um roteador central fabricado ou não pela Cisco de um provedor de Internet (ISP, Internet Service Provider), um rodízio de roteadores centrais ou um controle administrativo diferente, é necessário configurar um nome de usuário de autenticação que seja diferente do nome de host. Nesta situação, o nome de host do roteador não é fornecido ou é diferente em momentos diferentes (rotativo). Além disso, o nome de usuário e a senha que são atribuídos pelo ISP não podem ser o nome de host do roteador remoto. Em tal situação, é usado o comando **ppp chap hostname** para especificar um nome de usuário alternativo que será utilizado para autenticação.

Por exemplo, considere uma situação na qual vários dispositivos remotos estejam discando para um local central. Usando a autenticação CHAP normal, o nome de usuário (que seria o nome de host) de cada dispositivo remoto e um segredo compartilhado devem ser configurados no roteador central. Neste cenário, a configuração do roteador central pode ser longa e complicada; contudo, se os dispositivos remotos usarem um nome de usuário diferente do nome de host, isso pode ser evitado. O local central pode ser configurado com um único nome de usuário e um segredo compartilhado que podem ser usados para autenticar vários clientes de discagem.

## Diagrama de Rede

Se o Roteador 1 iniciar uma chamada para o Roteador 2, este desafiará o Roteador 1, que, por sua vez, não desafiará o Roteador 2. Isso ocorre porque o comando **ppp authentication chap callin** é configurado no Roteador 1. Este é um exemplo de uma autenticação unidirecional.

Nessa instalação, o comando **ppp chap hostname alias-r1** é configurado no Roteador 1. Este usa "alias-r1" como seu nome de host para a autenticação CHAP em vez de "r1". O nome do mapa de discador do Roteador 2 deve corresponder ao **ppp chap hostname** do Roteador 1; caso contrário, dois canais B são estabelecidos, um para cada direção.



## Configurações

Roteador 1
<pre>! 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 !</pre>
Roteador 2
<pre>! isdn switch-type basic-5ess ! hostname r2 !</pre>

```

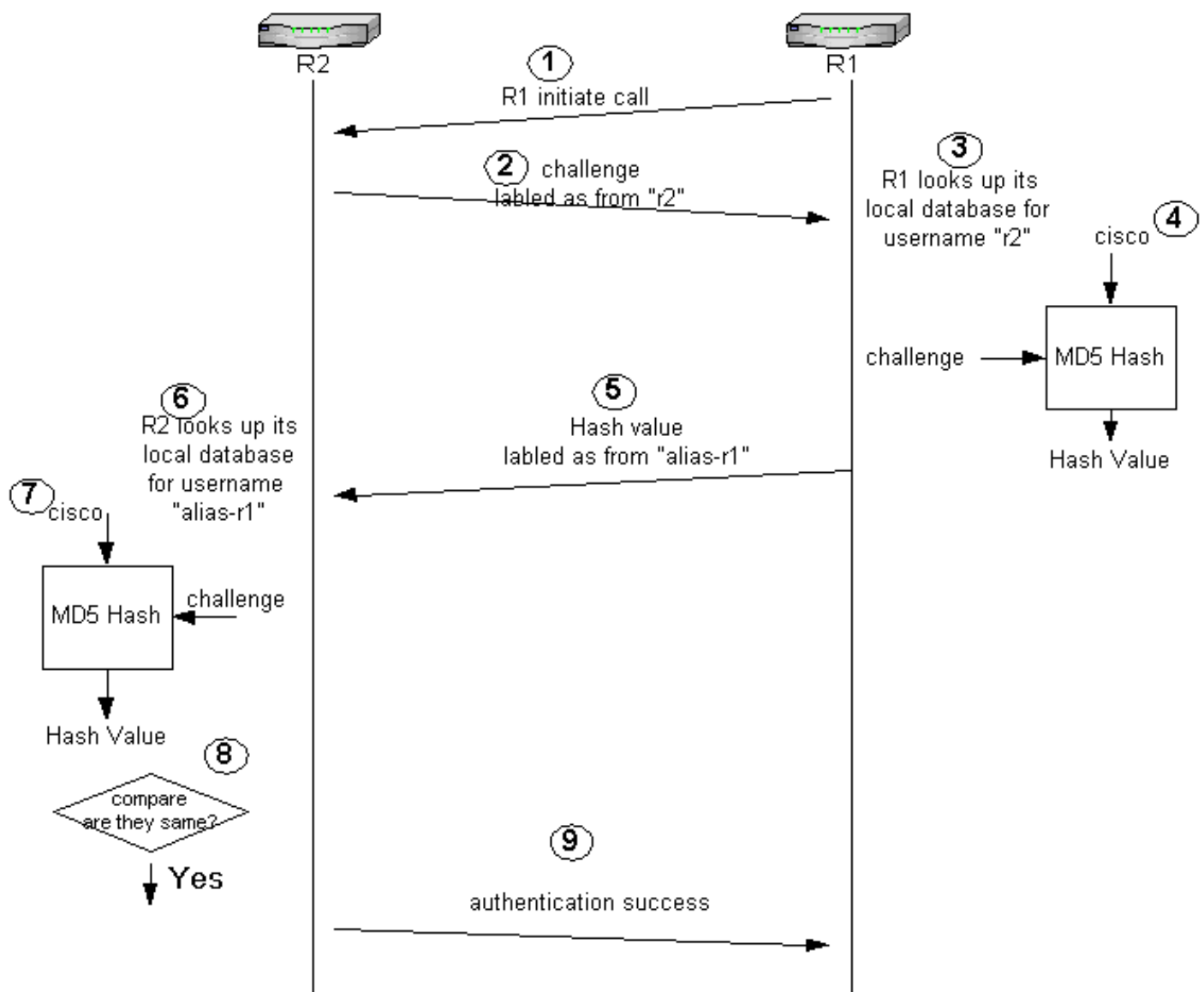
username alias-r1 password 0 cisco
! -- Alternate CHAP hostname and shared secret. ! --
The username must match the one in the ppp chap hostname
! -- command on the remote router.

!
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 !

```

## Explicação de configuração

Consulte os números abaixo deste gráfico para obter explicações:



1. Neste exemplo, o roteador 1 inicia a chamada. Como o Roteador 1 é configurado com o comando `ppp authentication chap callin`, ele não desafia a parte chamadora, que é o Roteador 2.

2. Quando o Roteador 2 recebe uma chamada, ele desafia o Roteador 1 para autenticação. Como padrão para essa autenticação, o nome de host do roteador é usado para identificá-lo. Se o comando `ppp chap hostname name` estiver configurado, um roteador utiliza o nome em lugar do nome do host para se identificar. Neste exemplo, o desafio é rotulado como se estivesse vindo de "r2".
3. O Roteador 1 recebe o desafio do Roteador 2 e examina seu banco de dados local para detectar o nome de usuário "r2".
4. O Roteador 1 descobre a senha de "r2", que é "cisco". O Roteador 1 usa essa senha e o desafio do Roteador 2 como parâmetros de entrada da função de hash MD5. O valor de hash é gerado.
5. O Roteador 1 envia o valor de saída de hash para o Roteador 2. Aqui, como o comando `ppp chap hostname` está configurado como "alias-r1", a resposta é rotulada como originada em "alias-r1".
6. O roteador 2 recebe a resposta e procura pelo nome de usuário "alias-r1" na base de dados local para obter a senha.
7. O Roteador 2 descobre que a senha de "alias-r1" é "cisco". O Roteador 2 usa a senha e o desafio enviados anteriormente para o Roteador 1 como parâmetros de entrada para a função de hash MD5. A função de hash gera um valor de hash.
8. O Roteador 2 compara o valor de hash que ele gerou com aquele recebido do Roteador 1.
9. Visto que os parâmetros de entrada (desafio e senha) são idênticos, o valor de hash é o mesmo, o que resulta em uma autenticação bem-sucedida.

## Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

## Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Antes de tentar qualquer um dos comandos de depuração, consulte [Informações Importantes sobre Comandos de Depuração](#)

## Exemplo de debug

A seguir temos um exemplo de saída do comando `debug ppp authentication`:

### Roteador 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
```

## Roteador 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
```

## Informações Relacionadas

- [Comandos PPP para Redes de Longa Distância](#)
- [Compreendendo o PPP e a autenticação de PPP](#)
- [Informações sobre depuração de ISDN](#)