# Autenticación de PPP utilizando los comandos ppp chap hostname y ppp authentication chap callin

## Contenido



## Introducción

La negociación PPP implica varios pasos tales como la negociación LCP (Link Control Protocol), autenticación y negociación NCP (Network Control Protocol). Si los dos lados no pueden estar de acuerdo con los parámetros correctos, se termina la conexión. Una vez establecido el link, los dos lados se autentican entre sí mediante el protocolo de autenticación definido durante la negociación de LCP. La autenticación debe ser realizada de forma exitosa antes de que se dé inicio a la negociación NCP.

PPP admite dos protocolos de autenticación: Protocolo de autenticación de contraseña (PAP) y Protocolo de confirmación de aceptación de la autenticación (CHAP).

## Prerequisites

### Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

## Requirements

No hay requisitos previos específicos para este documento.

## Componentes Utilizados

La información que contiene este documento se basa en las versiones de software y hardware indicadas a continuación.

- Versión 11.2 o más reciente del software IOS® de Cisco

## Teoría Precedente

La autenticación PAP implica un intercambio de señales bidireccional donde el nombre de usuario y la contraseña se envían a través del link en texto sin formato; por lo tanto, la autenticación PAP no proporciona ninguna protección contra la reproducción y el rastreo de línea.

Por otra parte, la autenticación CHAP verifica periódicamente la identidad del nodo remoto mediante un intercambio de señales tridireccional. Después de establecer el link PPP, el host envía un mensaje de "desafío" al nodo remoto. El nodo remoto responde con un valor calculado mediante una función hash unidireccional. El host verifica la respuesta con su propio cálculo del valor hash esperado. Si los valores coinciden, se reconoce la autenticación; de no ser así, la conexión finaliza.

# Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

**Nota:** Para encontrar información adicional sobre los comandos usados en este documento, utilice la herramienta de búsqueda de comandos de IOS

## Configuración de autenticación CHAP unidireccional

Cuando dos dispositivos utilizan normalmente la autenticación CHAP, cada lado envía un desafío al que el otro lado responde y es autenticado por el contendiente. Cada lado se autentica mutuamente independientemente. Si desea operar con routers que no son de Cisco que no soportan la autenticación por parte del router o dispositivo de llamada, debe utilizar el comando **ppp authentication chap callin**. Cuando se utiliza el comando **ppp authentication** con la palabra clave **callin**, el servidor de acceso sólo autenticará el dispositivo remoto si el dispositivo remoto inició la llamada (por ejemplo, si el dispositivo remoto "llamó"). En este caso, la autenticación sólo se especifica en las llamadas entrantes (recibidas).

## Configuración de un nombre de usuario diferente al nombre del router

Cuando un router remoto de Cisco se conecta a un router central de Cisco o a un router que no es de Cisco de un control administrativo diferente, a un proveedor de servicios de Internet (ISP) o a una rotación de routers centrales, es necesario configurar un nombre de usuario de autenticación que sea diferente del nombre de host. En esta situación, el nombre de host del

router no se proporciona o es diferente en diferentes momentos (rotatorio). Además, es posible que el nombre de usuario y la contraseña que asigna el ISP no sean el nombre de host del router remoto. En una situación así, se usa el comando ppp chap hostname para especificar un nombre de usuario alternativo que se utilizará para la autenticación.

Por ejemplo, considere una situación en la que varios dispositivos remotos están marcando en un sitio central. Mediante la autenticación CHAP normal, el nombre de usuario (que sería el nombre de host) de cada dispositivo remoto y un secreto compartido se deben configurar en el router central. En este escenario, la configuración del router central puede volverse larga y engorrosa de administrar; sin embargo, si los dispositivos remotos utilizan un nombre de usuario diferente a su nombre de host, esto puede evitarse. El sitio central se puede configurar con un único nombre de usuario y secreto compartido que se puede utilizar para autenticar varios clientes de marcado.

## Diagrama de la red

Si el Router 1 inicia una llamada al Router 2, el Router 2 desafiaría al Router 1, pero el Router 1 no desafiaría al Router 2. Esto ocurre porque el comando **ppp authentication chap callin** se configura en el Router 1. Éste es un ejemplo de una autenticación unidireccional.

En esta configuración, el comando **ppp chap hostname alias-r1** se configura en el Router 1. El router 1 utiliza "alias-r1" como nombre de host para la autenticación CHAP en lugar de "r1". El nombre del mapa de marcado del router 2 debe coincidir con el nombre de host ppp chap del router 1; de lo contrario, se establecen dos canales B, uno para cada dirección.


## Configuraciones

**Router 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 !
```

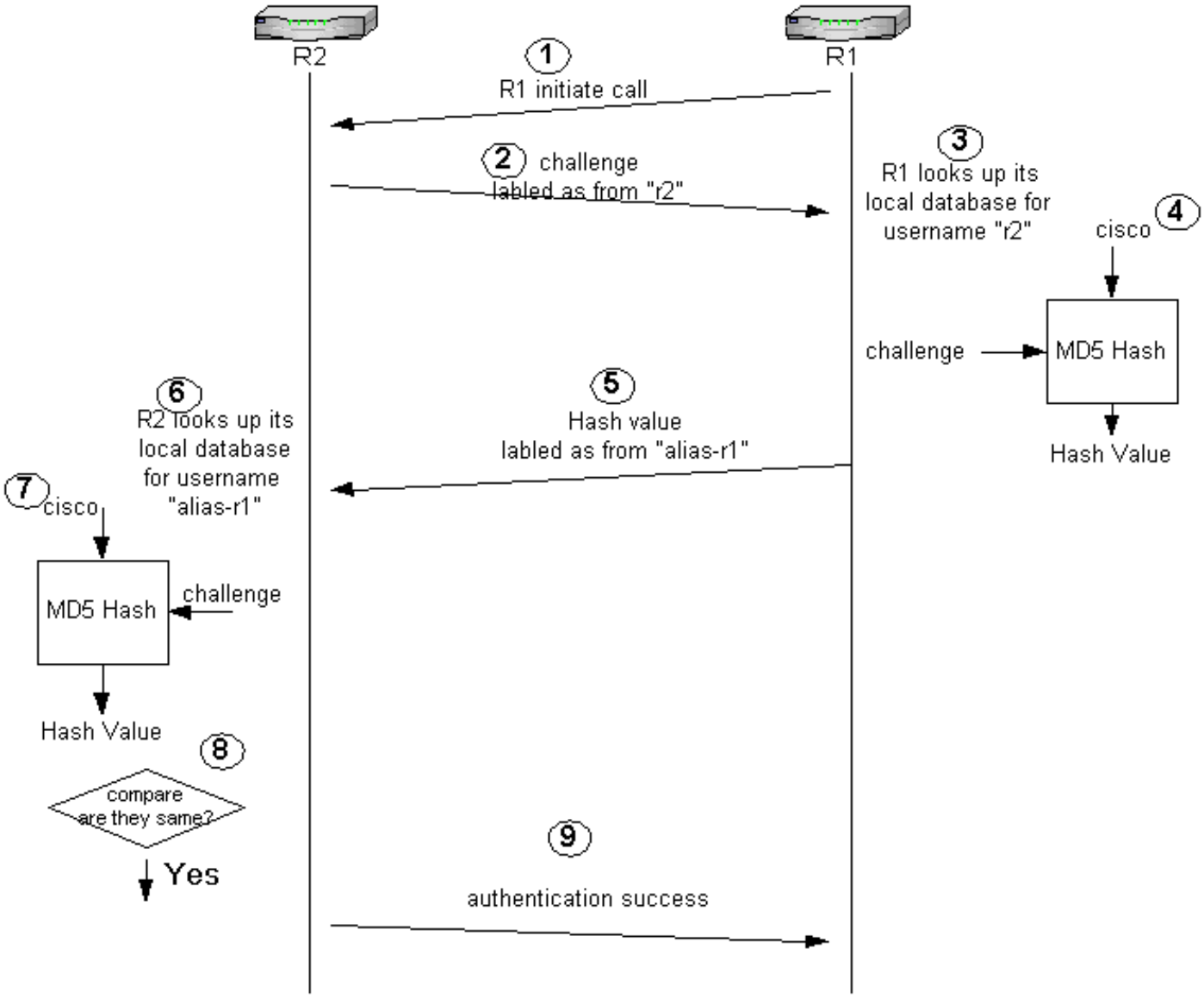
**Router 2**

```
!
 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 !
```

## Explicación sobre la configuración

Consulte los números que aparecen a continuación para obtener más información:




1. En este ejemplo, el Router 1 inicia la llamada. Dado que el Router 1 está configurado con el comando ppp authentication chap callin, no desafía a la parte llamadora, que es el Router 2.
2. Cuando el Router 2 recibe la llamada, desafía al Router 1 para la autenticación. De forma predeterminada para esta autenticación, el nombre de host del router se utiliza para identificarse. Si se configura el comando ppp chap hostname name, un router utiliza el nombre en lugar del nombre de la computadora principal para identificarse. En este ejemplo, el desafío se etiqueta como proviene de "r2".
3. El Router 1 recibe el desafío del Router 2 y busca en su base de datos local el nombre de usuario "r2".
4. El router 1 encuentra la contraseña "r2", que es "cisco". El Router 1 utiliza esta contraseña y el desafío del Router 2 como parámetros de entrada de la función hash MD5. Se genera el valor de troceo.
5. El Router 1 envía el valor de salida hash al Router 2. Aquí, dado que el comando **ppp chap hostname** se configura como "alias-r1", la respuesta se etiqueta como proveniente de "alias-r1".
6. El router 2 recibe la respuesta y busca el nombre de usuario "alias-r1" en su base de datos local para la contraseña.
7. El router 2 encuentra que la contraseña de "alias-r1" es "cisco". El Router 2 utiliza la contraseña y el desafío enviado anteriormente al Router 1 como parámetros de entrada para la función hash MD5. La función de troceo genera un valor de troceo.

8. El Router 2 compara el valor de troceo que generó y el que recibe del Router 1.
9. Dado que los parámetros de entrada (desafío y contraseña) son idénticos, el valor hash es el mismo, lo que produce una autenticación correcta.

# Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

# Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Antes de intentar la ejecución de alguno de los comandos de depuración, consulte la sección Información importante sobre comandos de depuración

## Ejemplo de resultado del comando debug

A continuación aparece una muestra de un resultado del comando debug ppp authentication:

### Router 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
```

### Router 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
```

# Información Relacionada

- Comandos PPP para redes de área extensa
- Introducción al PPP y de la autenticación de PPP
- Información de depuración de ISDN