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).

prerrequisitos

Convenciones

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

Requisitos

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.

- Software Release 11.2 o Posterior de Cisco IOS®

Teoría Precedente

La autenticación PAP implica una entrada en contacto bidireccional en donde el nombre de usuario y contraseña se envía a través del link en el texto claro; por lo tanto, la autenticación PAP no proporciona ninguna protección contra reproducción y sabueso de línea.

La autenticación CHAP, por otra parte, verifica periódicamente la identidad del nodo remoto usando una entrada en contacto de tres vías. Después de que se establezca el link PPP, el host envía un mensaje de "impugnación" al nodo remoto. El nodo remoto responde con un valor calculado usando una función de parcialización unidireccional. El host marca la respuesta contra su propio cálculo del valor de troceo esperado. Si los valores hacen juego, 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.

Note: Para obtener información adicional sobre los comandos que se utilizan en este documento, use la herramienta IOS Command Lookup

Configuración de autenticación CHAP unidireccional

Cuando dos dispositivos utilizan normalmente la autenticación CHAP, cada lado envía un desafío al cual el otro lado responda y sea autenticado por el desafiador. Cada uno echa a un lado autentica uno otro independientemente. Si usted quiere actuar con los routeres no perteneciente a Cisco que no soportan la autenticación por el router de llamada o el dispositivo, usted debe utilizar el **comando ppp authentication chap callin**. Al usar el **comando ppp authentication** con la **palabra clave para llamada**, el servidor de acceso autenticará solamente el dispositivo remoto si el dispositivo remoto inició la llamada (por ejemplo, si el dispositivo remoto “llamado en”). En este caso, la autenticación se especifica en las llamadas (recibidas) entrantes solamente.

Configuración de un nombre de usuario diferente al nombre del router

Cuando un router Cisco remoto conecta con Cisco o un router central del no Cisco de un diverso control administrativo, de un Proveedor de servicios de Internet (ISP), o de un rotatorio de los routeres 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 ni

es diferente en los momentos diferentes (rotatorios). También, el nombre de usuario y contraseña que es afectado un aparato por el ISP puede no ser 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 donde los dispositivos remotos múltiples están marcando en un sitio central. Usando 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 conseguir muy larga e incómoda manejar; sin embargo, si los dispositivos remotos utilizan un nombre de usuario que es diferente de su nombre de host esto puede ser evitado. El sitio central se puede configurar con un solos nombre de usuario y secreto compartido que se puedan utilizar para autenticar a los clientes de marcación de entrada múltiples.

Diagrama de la red

Si el router1 inicia una llamada al router2, el router2 el router de impugnación 1, pero el router1 no el router de impugnación 2. Esto ocurre porque configuran al **comando ppp authentication chap callin** en el router1. Éste es un ejemplo de una autenticación unidireccional.

En esta configuración, configuran al **comando ppp chap hostname alias-r1** en las aplicaciones del router1 del router 1. el "alias-r1" como su nombre de host para la autenticación CHAP en vez del "r1." que el nombre de mapa de marcado del router2 debe hacer juego el nombre de host del PPP chap del router 1's; 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 !
```

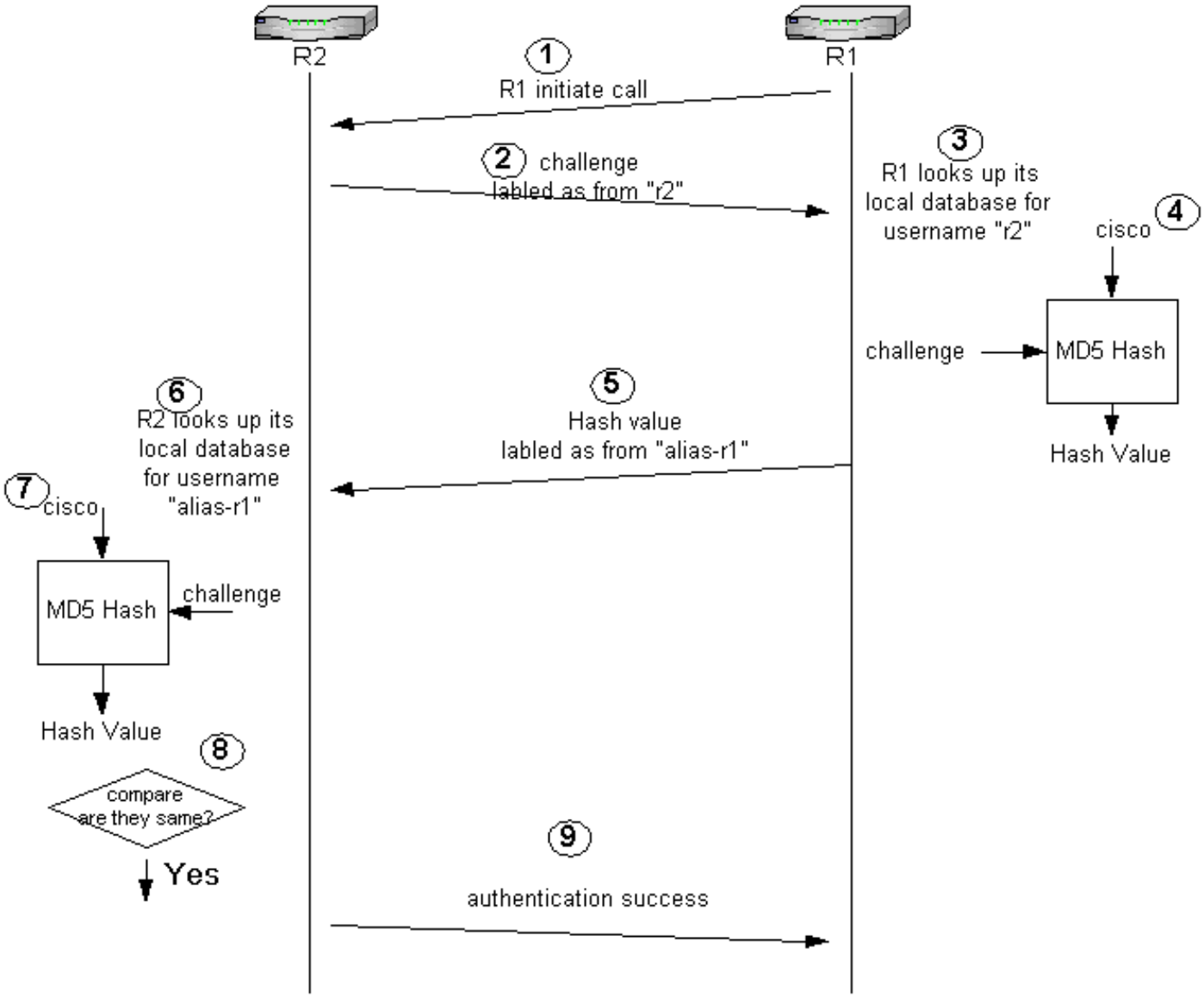
Router 2

```
!
 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

Refiera por favor a los números debajo de este gráfico para obtener explicaciones:



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 router2 recibe la llamada, desafía el router1 para la autenticación. Por abandono 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, se etiqueta el desafío mientras que está viniendo a partir de la "r2."
3. El router1 recibe el desafío del router 2's y mira en su base de datos local para el nombre de usuario el "r2."
4. El router1 encuentra la contraseña del "r2", que es “Cisco.” El router1 utiliza esta contraseña y el desafío del router2 como parámetros de entrada de la función de troceo MD5. Se genera el valor de troceo.
5. El router1 envía el valor de resultado del troceo al router2. Aquí, puesto que configuran al **comando ppp chap hostname** mientras que el "alias-r1," la contestación se etiqueta como viniendo a partir de la "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 router2 encuentra que la contraseña para el "alias-r1" es “Cisco.” El router2 utiliza la contraseña y el desafío enviados anterior al router1 como parámetros de entrada para la función de troceo 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. Puesto que los parámetros de entrada (desafío y contraseña) son idénticos, el valor de troceo es lo mismo dando por resultado una autenticación satisfactoria.

Verificación

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

Troubleshooting

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

Antes de intentar los comandos debug uces de los, vea por favor la información importante en los comandos Debug

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 la conexión de red en un área ancha
- Introducción al PPP y de la autenticación de PPP
- Información de depuración de ISDN