

Configuración y Comprensión de la Autenticación CHAP PPP

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Configurar CHAP](#)

[Autenticación unidireccional y bidireccional](#)

[Comandos y opciones de configuración de CHAP](#)

[Ejemplo de transacción](#)

[Llamada](#)

[Desafío](#)

[Respuesta](#)

[Respuesta \(continuado\)](#)

[Verificar CHAP](#)

[Resultado](#)

[Resolver Problemas de CHAP](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo el Protocolo de autenticación por desafío mutuo (CHAP, Challenge Handshake Authentication Protocol) verifica la identidad de un peer mediante un protocolo de enlace de tres vías.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cómo habilitar PPP en la interfaz a través del `encapsulation ppp` comando.
- `debug ppp negotiation` resultado del comando. Consulte [Comprensión de la Salida de debug ppp negotiation](#) para obtener más información.
- Cómo resolver problemas cuando la fase del Protocolo de control de enlaces (LCP) no está en estado abierto. Esto se debe a que la fase de autenticación PPP no comienza hasta que la fase LCP está completa y en estado abierto. Si `debug ppp negotiation` no indica que el LCP esté abierto, debe resolver este problema antes de continuar.

Nota: Este documento no se refiere a MS-CHAP (Versión 1 o Versión 2).

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Convenciones

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

Antecedentes

EL protocolo Challenge Handshake Authentication Protocol (CHAP) (definido en [RFC 1994](#)) [verifica la identidad del peer mediante una entrada en contacto de tres vías](#). Éstos son los pasos generales que se realizan en CHAP:

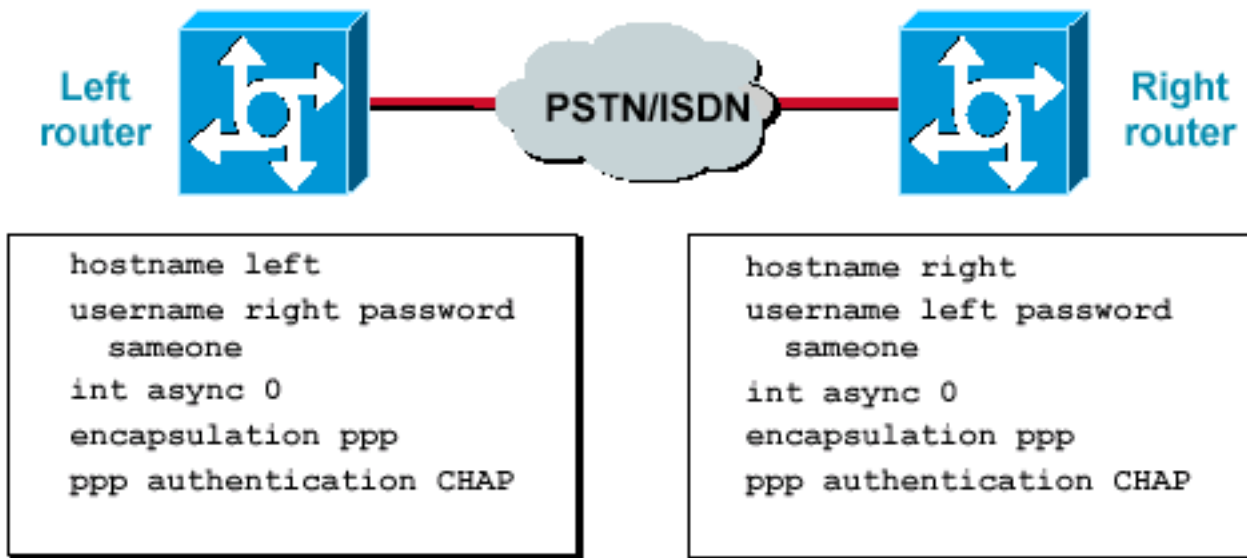
1. Una vez completada la fase LCP (Link Control Protocol), y negociado CHAP entre ambos dispositivos, el autenticador envía un mensaje de desafío al peer.
2. El peer responde con un valor calculado mediante una función de hash de una vía (publicación de mensaje 5 (MD5)).
3. El autenticador verifica la respuesta contra su propio cálculo del valor de troceo esperado. Si los valores coinciden, la autenticación es exitosa. De no ser así, la conexión finaliza.

Este método de autenticación depende de un "secreto" conocido solamente para el autenticador y el peer. El secreto no se envía por el link. Aunque la autenticación sea solamente unidireccional, puede negociar CHAP en ambas direcciones, con la ayuda del mismo secreto establecido para la autenticación recíproca.

Para obtener más información sobre las ventajas y desventajas de CHAP, consulte RFC 1994.

Configurar CHAP

El procedimiento para configurar CHAP es bastante directo. Por ejemplo, asuma que tiene dos routers, izquierdo y derecho, conectados a través de una red, tal y como se muestra en la figura 1.



routers conectados a través de una red

Dos

Figura 1: Dos routers conectados a través de una red

Para configurar la autenticación CHAP, complete estos pasos:

1. En la interfaz, emita el comando `encapsulation ppp`.
2. Habilite el uso de la autenticación CHAP en ambos routers con el `ppp authentication chap` comando.
3. Configure los nombres de usuario y las contraseñas. Para ello, ejecute el comando `username username password password`, donde `nombreusuario` es el nombre de host del par. Asegúrese de lo siguiente: Las contraseñas son idénticas en ambos extremos. El nombre de router y la contraseña son exactamente iguales, porque distinguen entre mayúsculas y minúsculas.

Nota: De forma predeterminada, el router utiliza su nombre de host para identificarse ante el par. Sin embargo, este nombre de usuario CHAP se puede cambiar a través del `ppp chap hostname` comando. Consulte [Autenticación PPP con los Comandos `ppp chap hostname` y `ppp authentication chap callin`](#) para obtener más información.

Autenticación unidireccional y bidireccional

CHAP se define como un método de autenticación unidireccional. Sin embargo, puede utilizar CHAP en ambas direcciones para crear una autenticación bidireccional. Por consiguiente, con un CHAP de dos vías, se inicia en cada lado una entrada en contacto de tres vías.

En la implementación de CHAP de Cisco, de manera predeterminada, la parte llamada debe autenticar a la parte llamadora (a menos que se desactive totalmente la autenticación). Por lo tanto, una autenticación unidireccional iniciada por la parte llamada es la autenticación mínima posible. Sin embargo, la parte llamadora también puede verificar la identidad de la parte llamada, y esto da lugar a una autenticación bidireccional.

La autenticación unidireccional se requiere a menudo cuando se conecta con dispositivos que no son Cisco.

Para la autenticación unidireccional, configure el `ppp authentication chap callin` en el router de llamada.

La tabla 1 muestra cuándo configurar la opción `callin`.

Tabla 1: Cuándo configurar la opción de llamada

Tipo de autenticación	Cliente (llamadas)	NAS (llamado)
Un sentido (unidireccional)	<code>ppp authentication chap callin</code>	<code>ppp authentication chap</code>
Bidireccional	<code>ppp authentication chap</code>	<code>ppp authentication chap</code>

Consulte [Autenticación PPP con los Comandos `ppp chap hostname` y `ppp authentication chap callin`](#) para obtener más información.

Comandos y opciones de configuración de CHAP

La tabla 2 enumera los comandos y las opciones de CHAP:

Tabla 2: Comandos y opciones de CHAP

Comando	Descripción
<code>ppp authentication {chap ms-chap ms-chap-v2 eap pap} [callin]</code>	Este comando habilita la autenticación local del peer PPP remoto con el protocolo especificado.
<code>ppp chap hostname username</code>	Este comando define un nombre de host CHAP específico de la interfaz. Consulte Autenticación PPP con los Comandos <code>ppp chap hostname</code> y <code>ppp authentication chap callin</code> para obtener más información.
<code>ppp chap password</code>	Este comando define una contraseña CHAP específica de la interfaz.
<code>ppp directioncallin rótulo dedicados</code>	Este comando fuerza una dirección de llamada. Utilice este comando cuando un router confunda si la llamada es entrante o saliente (por ejemplo, cuando esté conectado back-to-back o conectado mediante líneas arrendadas y la unidad de servicio de canal o la unidad de servicio de datos (CSU/DSU) o el adaptador de terminal ISDN (TA) estén configurados para marcar).
<code>ppp chap refuse [callin]</code>	Este comando inhabilita la autenticación remota de un peer (valor predeterminado habilitado). Con este comando, la autenticación CHAP se inhabilita para todas las llamadas, lo que significa que todas las tentativas del par para forzar al usuario a autenticar con la ayuda de CHAP se rechazan. La opción <code>callin</code> especifica que el router rechaza contestar a los desafíos de autenticación CHAP recibidos del peer, pero todavía requiere que el peer responda a cualquier desafío CHAP que envíe el router.
<code>ppp chap wait</code>	Este comando especifica que el llamante debe autenticar primero (valor predeterminado habilitado). Este comando especifica que el router no autentica a un par que solicita la autenticación CHAP hasta después de que el par se haya autenticado en el router.
<code>ppp max-bad-auth valor</code>	Este comando especifica el número permitido de reintentos de autenticación (el valor predeterminado es 0). Este comando configura una interfaz punto a punto para que no se restablezca inmediatamente después de una falla de autenticación, sino para que permita un número especificado de reintentos de autenticación.
<code>ppp chap</code>	Este comando oculto permite diferentes nombres de host para un desafío CHAP y

splitnames una respuesta (el valor predeterminado es inhabilitado).
ppp chap Este comando oculto ignora los desafíos CHAP con el nombre local (el valor predeterminado es habilitado).
ignoreus

Ejemplo de transacción

Los diagramas de esta sección muestran la serie de eventos que ocurren durante una autenticación CHAP entre dos routers. Estos no representan los mensajes reales que se ven en el debug ppp negotiation resultado del comando. Para obtener más información, consulte [Comprensión de la Salida de debug ppp negotiation](#).

Llamada



llamada entra

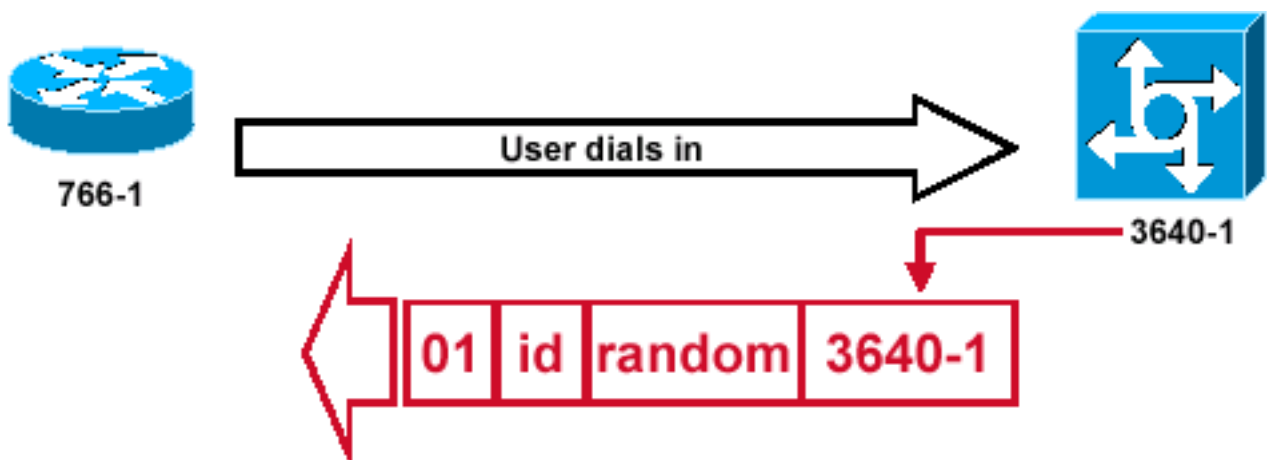
La

Figura 2: Se recibe la llamada

La [Figura 2](#) muestra estos pasos:

1. La llamada entra en 3640-1. La interfaz entrante se configura con el `ppp authentication chap` comando.
2. LCP negocia CHAP y MD5. Para obtener más información sobre cómo determinar esto, consulte [Comprensión de la Salida de debug ppp negotiation](#).
3. En esta llamada, se requiere un desafío CHAP de 3640-1 al router de llamada.

Desafío



paquete de desafío CHAP está construido

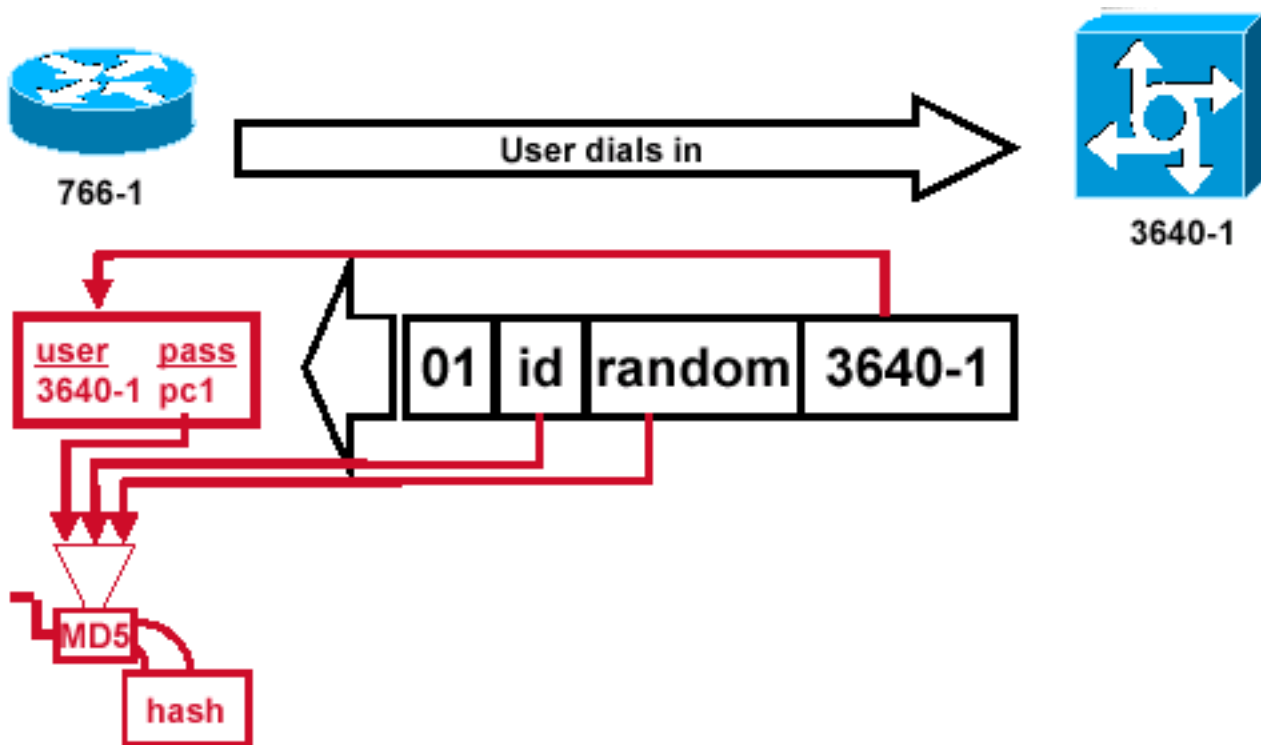
El

Figura 3: Se crea un paquete de desafío CHAP

La figura 3 ilustra estos pasos en la autenticación CHAP entre los dos routers:

1. Se genera un paquete de desafío CHAP con estas características: 01 = identificador de tipo de paquete de impugnación. ID = número secuencial que identifica el desafío. random = un número razonablemente aleatorio generado por el router. 3640-1 = nombre de autenticación del desafiante.
2. La ID y los valores aleatorios se guardan en el router llamado.
3. Se envía el paquete de impugnación al router que llama. Se mantiene una lista de desafíos extraordinarios.

Respuesta



Recepción y Procesamiento MD5 del Paquete de Desafío del Peer

Recepci

Figura 4: Recepción y procesamiento MD5 del paquete de desafío del par

La figura 4 ilustra cómo se recibe el paquete de desafío del peer, y cómo se procesa (MD5). El router procesa el paquete de desafío CHAP entrante de esta manera:

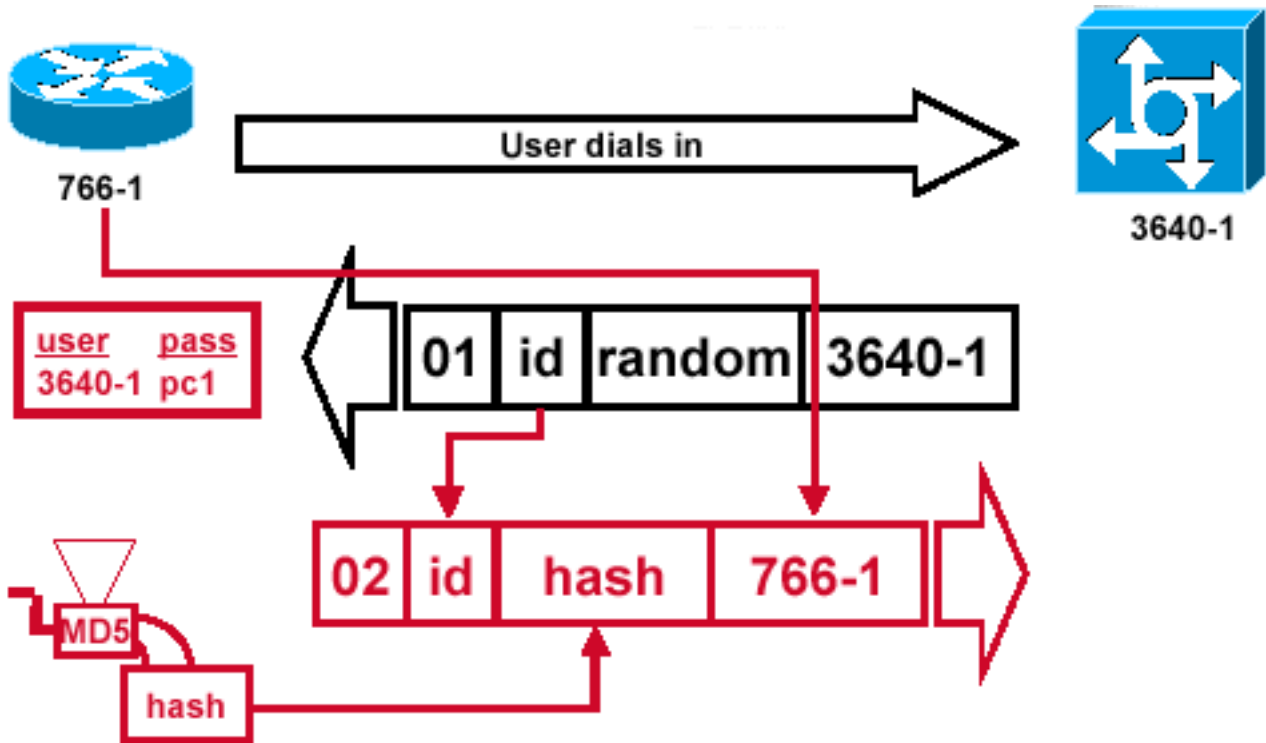
1. El valor de ID se introduce en el generador hash de MD5.
2. El valor aleatorio se introduce en el generador hash de MD5.
3. El nombre 3640-1 se utiliza para buscar la contraseña. El router busca una entrada que coincida con el nombre de usuario del desafío. En este ejemplo, busca:

```
username 3640-1 password pc1
```

4. La contraseña se introduce en el generador de hash MD5.

El resultado es un desafío CHAP con hash MD5 unidireccional que se devuelve en la respuesta CHAP.

Respuesta (continuado)



genera el paquete de respuesta CHAP enviado al autenticador

Se

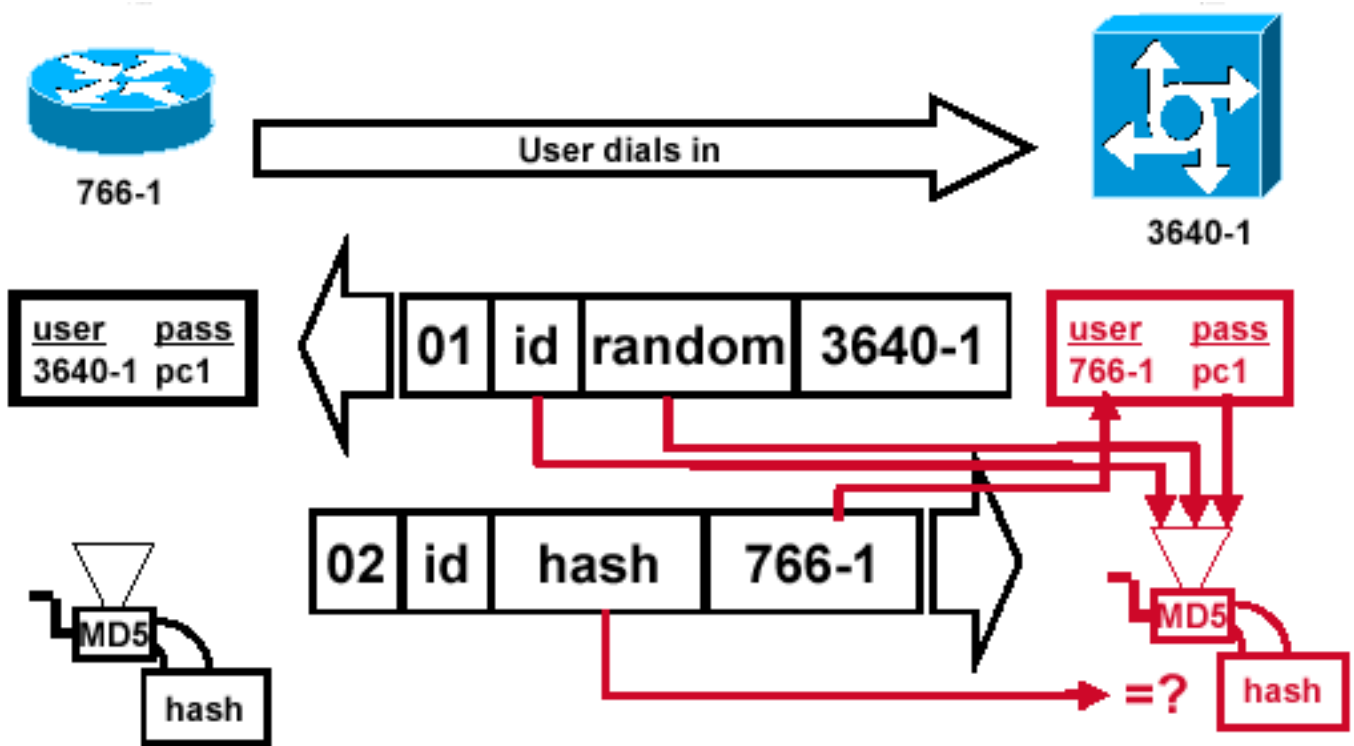
Figura 5: Se genera el paquete de respuesta CHAP enviado al autenticador

La figura 5 ilustra cómo se genera el paquete de respuesta CHAP enviado al autenticador. Este diagrama muestra estos pasos:

1. El paquete de respuesta se ensambla a partir de estos componentes: 02 = identificador de tipo de paquete de respuesta CHAP. ID = copiado del paquete challenge (de desafío). hash = la salida del generador de claves MD5 (la información cifrada del paquete de desafío). 766-1 = nombre de autenticación del dispositivo. Esto es necesario para que el peer busque la entrada de nombre de usuario y contraseña necesaria para verificar la identidad (esto se explica más detalladamente en la sección [Verificar CHAP](#)).
2. El paquete de respuesta es enviado luego al trasbordador.

Verificar CHAP

Esta sección proporciona sugerencias sobre cómo verificar la configuración.



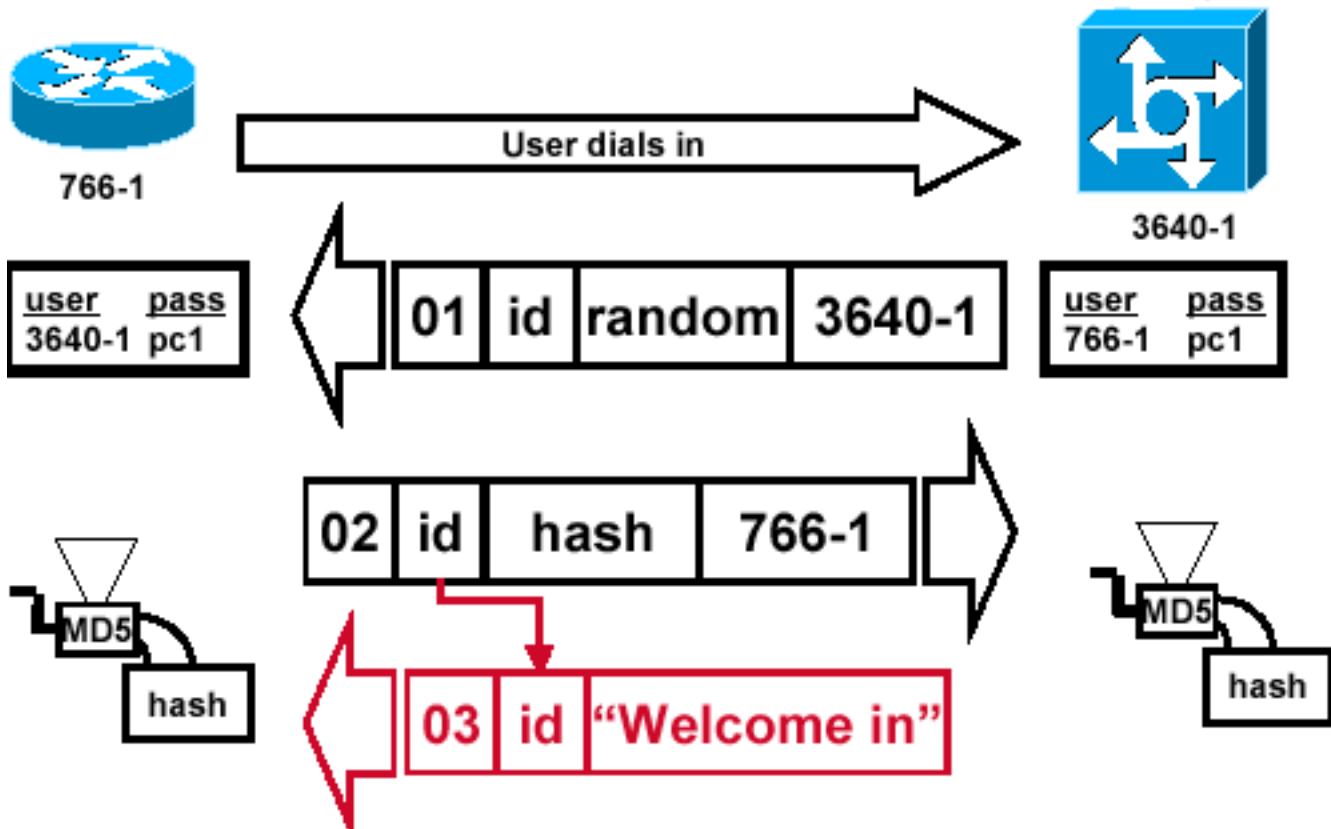
Challenger procesa el paquete de respuesta

Figura 6: El Challenger Procesa el Paquete de Respuesta

La figura 6 muestra cómo procesa el desafiador el paquete de respuesta. Éstos son los pasos implicados cuando se procesa el paquete de respuesta CHAP (en el autenticador):

1. La identificación (ID) se utiliza para encontrar el paquete de desafío original.
2. Se ingresa la ID en el generador de troceo MD5.
3. El valor aleatorio de impugnación original es alimentado dentro del generador de troceo MD5.
4. El nombre 766-1 se utiliza para buscar la contraseña a partir de uno de estos orígenes: Base de datos de nombre de usuario y de contraseñas locales. Servidor RADIUS o TACACS.
5. La contraseña se introduce en el generador de claves MD5.
6. El valor hash recibido en el paquete de respuesta se compara entonces con el valor hash MD5 calculado. La autenticación CHAP es exitosa si los valores hash calculados y recibidos son iguales.

Resultado



nsaje de Éxito Enviado al Router de Llamada

Me

Figura 7: El mensaje de éxito se envía al router de llamada

La figura 7 ilustra el mensaje de éxito enviado al router de llamada. Esto implica estos pasos:

1. Si la autenticación es correcta, se genera un paquete de éxito CHAP a partir de estos componentes: 03 = tipo de mensaje de éxito de CHAP. ID = copiado desde el paquete de respuesta. "Bienvenido" es simplemente un mensaje de texto que proporciona una explicación legible por el usuario.
2. Si la autenticación falla, se genera un paquete de falla CHAP a partir de estos componentes: 04 = Tipo de mensaje de falla CHAP. ID = copiado desde el paquete de respuesta. "Error de autenticación" u otro mensaje de texto que proporcione una explicación legible por el usuario.
3. El paquete exitoso o fallido es luego enviado al router que realiza la llamada.

Nota: Este ejemplo representa una autenticación unidireccional. En una autenticación bidireccional, todo este proceso se repite. Sin embargo, el router de llamada inicia el desafío inicial.

Resolver Problemas de CHAP

Consulte [Troubleshooting de la Autenticación PPP \(CHAP o PAP\)](#) para obtener información sobre cómo resolver cualquier problema.

Información Relacionada

- [Comprender el resultado de debug ppp negotiation](#)

- [Autenticación PPP con los comandos ppp chap hostname y ppp authentication chap callin](#)
- [Asistencia técnica y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).