Cómo funciona y se configura la autenticación PPP CHAP

Contenido

Introducción

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.

prerrequisitos

Requisitos

Quienes lean este documento deben tener conocimiento de los siguientes temas:

- Cómo habilitar PPP en la interfaz con el comando **encapsulation ppp**.
- La salida del comando **debug ppp negotiation** . Refiérase a Cómo Comprender la Salida de debug ppp negotiation para obtener más información.
- Capacidad para resolver problemas cuando la fase Link Control Protocol (LCP) no está en el 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 el comando **debug ppp negotiation** no indica que el LCP está abierto, debe resolver este problema antes de continuar.

Nota: Éste documento no se refiere a S-CHAP (Versión 1 o Versión 2). Para obtener más información sobre MS-CHAP, refiérase a los documentos Soporte de MS-CHAP y MSCHAP versión 2.

Componentes Utilizados

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

Convenciones

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

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.

Cuadro 1 Routers del dos del del â conectado 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 comando **ppp authentication chap**.
3. Configure los nombres de usuario y las contraseñas. Para hacer así pues, publique el **comando username username password password**, donde está el nombre de host el *nombre de usuario 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:** En forma predeterminada, el router usa su nombre de host para identificarse a sí mismo en el par. Sin embargo, este nombre de usuario de CHAP se puede cambiar mediante el comando **ppp chap hostname**. Refiérase a 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 comando **ppp authentication chap callin** en el router de llamada.

La tabla 1 muestra cuándo configurar la opción callin.

del del â del cuadro 1 cuándo configurar la opción CALLIN

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

Para obtener más información sobre cómo implementar la autenticación unidireccional, refiérase a Autenticación PPP con los Comandos ppp chap hostname y ppp authentication chap callin.

Comandos y opciones de configuración de CHAP

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

Comandos chap y opciones del del del â del cuadro 2

Comando	Descripción
ppp authentication {chap	*ms-chap*	*ms-chap-v2*	*eap* |pap} [callin]	Este comando habilita la autenticación local del peer PPP remoto con el protocolo especificado.

ppp chap hostname username	Este comando define un nombre de host CHAP específico de la interfaz. Refiérase a Autenticación PPP con los Comandos ppp chap hostname y ppp authentication chap callin para obtener más información.
ppp chap password password	Este comando define una contraseña CHAP específica de la interfaz.
ppp direction callin / *reclamo* / *dedicado*	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).
ppp chap refuse [callin]	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 callin 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.
ppp chap wait	Este comando especifica que el llamante debe autenticar primero (valor predeterminado habilitado). Este comando especifica que el router no autenticará un peer que solicite la autenticación CHAP hasta después de que el peer se haya autenticado para el router.
ppp max-bad-auth valor	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.
ppp chap splitnames	Este comando oculto permite diferentes nombres de host para un desafío CHAP y una respuesta (el valor predeterminado es inhabilitado).
ppp	Este comando oculto ignora los desafíos CHAP

chap ignoreus	con el nombre local (el valor predeterminado es habilitado).

Ejemplo de transacción

Los diagramas de esta sección muestran la serie de eventos que ocurren durante una autenticación CHAP entre dos routers. Éstos no representan los mensajes reales vistos en la salida del comando **debug ppp negotiation**. Para obtener más información, refiérase a Cómo Comprender la Salida de debug ppp negotiation .

Llamada

El cuadro 2 del del â la llamada viene adentro

La figura 2 muestra estos pasos:

1. La llamada entra en 3640-1. La interfaz entrante se configura con el comando **ppp authentication chap**.
2. LCP negocia CHAP y MD5. Para obtener más información sobre cómo determinar esto, refiérase a Cómo Comprender la Salida de debug ppp negotiation.
3. En esta llamada, se requiere un desafío CHAP de 3640-1 al router de llamada.

Desafío

Se construye el cuadro 3 del del â un paquete Challenge de la GRIETA

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

Proceso recibo del del del â y MD5 del cuadro 4 del paquete Challenge 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 claves MD5.El resultado es un desafío CHAP con hash MD5 unidireccional que se devuelve en la respuesta CHAP.

Respuesta (continuado)

Se construye el cuadro 5 del del â el paquete de respuesta de la GRIETA enviado al authenticator.

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.

El cuadro 6 del del â el desafiador 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

El cuadro 7 Mensaje de éxito del del del â se envía al router de llamada

La figura 7 ilustra el mensaje de éxito enviado al router de llamada. 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.el del del inâ de la recepción del del del â es simplemente un mensaje de texto que proporciona una explicación que puede ser comprensible para 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.el del del failureâ de la autenticación del del del â o el otro mensaje de texto, eso proporciona una explicación que puede ser comprensible para el usuario.
3. El paquete exitoso o fallido es luego enviado al router que realiza la llamada.**Nota:** Este

ejemplo describe 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

Refiérase a Troubleshooting de la Autenticación PPP para obtener información sobre cómo resolver problemas.

Información Relacionada

- Introducción al resultado de debug ppp negotiation
- Troubleshooting de la Autenticación PPP
- Autenticación de PPP utilizando los comandos ppp chap hostname y ppp authentication chap callin
- Páginas de soporte de la tecnología de acceso
- Soporte Técnico - Cisco Systems