

Entendendo e configurando a autenticação de PPP CHAP

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar CHAP](#)

[Autenticação uni e bidirecional](#)

[Comandos e opções de configuração de CHAP](#)

[Exemplo transacional](#)

[Chamada](#)

[Desafio](#)

[Resposta](#)

[Verificar CHAP](#)

[Resultado](#)

[Resolver problemas de CHAP](#)

[Informações Relacionadas](#)

Introdução

O Challenge Handshake Authentication Protocol (CHAP) (definida na RFC 1994) verifica a identidade do peer por meio de handshake de três vias. Estas são as etapas gerais executadas no CHAP:

1. Após a conclusão da fase do LCP (Link Control Protocol) e a negociação do CHAP entre os dispositivos, o autenticador envia uma mensagem de desafio ao peer.
2. O peer responde com um valor calculado através de uma função de hash unidirecional (Message Digest 5 (MD5)).
3. O autenticador verifica a resposta, comparando-a com seu próprio cálculo do valor esperado de mistura. Se os valores forem correspondentes, a autenticação terá êxito. Caso contrário, a conexão será encerrada.

Este método de autenticação depende de um “segredo” conhecido apenas pelo autenticador e pelo peer. O segredo não é enviado pelo enlace. Embora a autenticação seja apenas unidirecional, você pode negociar o CHAP em ambas as direções, com a ajuda do mesmo segredo definido para a autenticação mútua.

[Para obter mais informações sobre as vantagens e desvantagens do CHAP, consulte o RFC 1994.](#)

Pré-requisitos

Requisitos

Os leitores deste documento devem estar cientes destes tópicos:

- Como habilitar o PPP na interface através do comando **encapsulation ppp**.
- A saída do comando **debug ppp negotiation**. Consulte [Como Entender a Saída do Comando debug ppp negotiation](#) para obter mais informações.
- Capacidade de resolver problemas quando a fase do Link Control Protocol (LCP) não estiver no estado aberto. Isto ocorre porque a fase de autenticação do PPP não é iniciada até que a fase do LCP seja concluída e até que ele esteja no estado aberto. Se o comando **debug ppp negotiation** não indicar que o LCP está aberto, será necessário resolver esse problema antes de continuar.

Nota: Esse documento não aborda o MS-CHAP (versão 1 ou versão 2). Para obter mais informações sobre o MS-CHAP, consulte os documentos [Suporte ao MS-CHAP](#) e [MSCHAP Versão 2](#).

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Convenções

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

Configurar CHAP

O procedimento para configurar o CHAP é relativamente simples. Por exemplo, suponha que você possui dois roteadores, à esquerda e à direita, conectados ao longo de uma rede, como mostrado na [figura 1](#).

Figura 1 Roteadores do dois do do â conectado através de uma rede

Para configurar a autenticação de CHAP, realize as seguintes etapas:

1. Na interface, emita o comando **encapsulation ppp**.
2. Habilite o uso da autenticação de CHAP em ambos os roteadores usando o comando **ppp authentication chap**.
3. Configure os nomes de usuários e as senhas. Para fazer assim, emita o **comando username username password password**, onde o *username* é o hostname do par. Assegure que:As senhas sejam idênticas em ambas as extremidades.O nome de roteador e a senha sejam exatamente as mesmas, já que há diferenciação entre maiúsculas e minúsculas.**Nota:** Por padrão, o roteador utiliza seu nome de host para se identificar para o peer. Entretanto, o nome de usuário do CHAP poderá ser alterado através do comando **ppp chap hostname**. Consulte [Autenticação PPP Usando os Comandos ppp chap hostname e ppp authentication chap callin](#) para obter mais informações.

Autenticação uni e bidirecional

O CHAP é definido como um método de autenticação unidirecional. Entretanto, você poderá usar o CHAP em ambas as direções para criar uma autenticação bidirecional. Por isso, com o CHAP bidirecional, um cumprimento em tridirecional é iniciado por cada lado.

Na implementação Cisco CHAP, como padrão, o número chamado deve autenticar quem origina a chamada (a menos que a autenticação esteja completamente desativada). Desse modo, uma autenticação unidirecional iniciada pelo número chamado é a mínima autenticação possível. Porém, quem origina a chamada também pode verificar a identidade do número chamado, e isso resulta em uma autenticação bidirecional.

A autenticação unidirecional é geralmente exigida quando você se conecta a dispositivos que não sejam da Cisco.

Para obter a autenticação unidirecional, configure o comando `ppp authentication chap callin` no roteador que origina a chamada.

A [Tabela 1](#) mostra quando configurar a opção `callin`.

do do â da tabela 1 quando configurar a opção de callin

Tipo de autenticação	Cliente (chamando)	NAS (chamado)
Sentido único (unidirecional)	<code>ppp authentication chap callin</code>	abertura de autenticação ppp
Dois sentidos (bidirecional)	abertura de autenticação ppp	abertura de autenticação ppp

Para obter mais informações sobre como implementar a autenticação unidirecional, consulte [Autenticação PPP Usando os Comandos `ppp chap hostname` e `ppp authentication chap callin`](#).

Comandos e opções de configuração de CHAP

A [Tabela 2](#) lista os comandos e as opções de CHAP:

Comandos chap e opções do do do â da tabela 2

Comando	Descrição
<code>ppp authentication {chap / ms-chap / ms-chap-v2 / eap / pap} [callin]</code>	Esse comando habilita a autenticação local do peer PPP remoto com o protocolo especificado.

<p>ppp chap hostname username</p>	<p>Esse comando define um nome de host de CHAP específico para a interface. Consulte Autenticação PPP Usando os Comandos ppp chap hostname e ppp authentication chap callin para obter mais informações.</p>
<p>ppp chap password password</p>	<p>Esse comando define uma senha de CHAP específica para a interface.</p>
<p>ppp direction callin / callout / dedicated</p>	<p>Esse comando força uma direção de chamada. Use esse comando quando um roteador confundir se a chamada está sendo recebida ou realizada (por exemplo, quando estiver conectado diretamente ou quando estiver conectado através de linhas alugadas e quando a Unidade de Serviço de Canal ou Unidade de Serviço de Dados (CSU/DSU, Channel Service Unit/Data Service Unit) ou o Adaptador de Terminal (TA, Terminal Adapter) ISDN estiverem configurados para discar).</p>
<p>ppp chap refuse [callin]</p>	<p>Esse comando desabilita a autenticação remota por um peer (padrão habilitado). Com esse comando, a autenticação de CHAP é desabilitada para todas as chamadas, o que significa que todas as tentativas do peer para forçar a autenticação pelo usuário com a ajuda do CHAP serão recusadas. A opção callin especifica que o roteador recusará responder aos desafios de autenticação de CHAP recebidos do peer, mas ainda exigirá que o peer responda aos desafios de CHAP enviados pelo roteador.</p>
<p>ppp chap wait</p>	<p>Esse comando especifica que quem origina a chamada deve autenticar primeiro (padrão habilitado). Esse comando especifica que o roteador não autenticará um peer que solicite a autenticação de CHAP até que o peer tenha se autenticado para o roteador.</p>
<p>ppp max-bad-auth value</p>	<p>Esse comando especifica o número permitido de novas tentativas de autenticação (o valor padrão é 0). Esse comando configura uma interface ponto-a-ponto de modo que ela não seja redefinida imediatamente após uma falha de autenticação, mas que, em vez disso, permita um número especificado de novas tentativas de autenticação.</p>
<p>ppp chap</p>	<p>Esse comando oculto permite nomes de host diferentes para um desafio e uma resposta de</p>

splitnames	CHAP (o valor padrão é disabled).
ppp chap ignores	Esse comando oculto ignora os desafios de CHAP com o nome local (o valor padrão é enabled).

Exemplo transacional

Os diagramas nesta seção mostram a série de eventos que ocorre durante uma autenticação de CHAP entre dois roteadores. Eles não representam as mensagens reais vistas na saída do comando **debug ppp negotiation**. Para obter mais informações, consulte [Como Entender a Saída do Comando debug ppp negotiation](#).

Chamada

A figura 2 do do â o atendimento entra

A [Figura 2](#) mostra estas etapas:

1. A chamada é recebida em 3640-1. A interface de entrada é configurada com o comando **ppp authentication chap**.
2. O LCP negocia CHAP e MD5. Para obter mais informações sobre como determiná-la, consulte [Como Entender a Saída do Comando debug ppp negotiation](#).
3. Um desafio da CHAP de 3640-1 para o roteador de chamada é necessário nessa chamada.

Desafio

A figura 3 do do â um pacote de intercâmbio da RACHADURA é construída

A [Figura 3](#) ilustra estas etapas na autenticação de CHAP entre os dois roteadores:

1. Um pacote de desafio de CHAP é criado com as seguintes características: 01 = identificador do tipo de pacote de desafio ID = o número seqüencial que identifica o desafio. random = um número razoavelmente aleatório gerado pelo roteador. 3640-1 = o nome de autenticação do desafiante.
2. A identificação e os valores aleatórios são mantidos no roteador chamado.
3. O pacote de desafio é enviado para o roteador de chamada. Uma lista dos desafios mais importantes é mantida.

Resposta

Processamento recibo do do do â e MD5 da figura 4 do pacote de intercâmbio do par

A [Figura 4](#) ilustra como o pacote de desafio é recebido do peer e como é processado (MD5). O roteador processa o pacote de desafio de CHAP de entrada desta maneira:

1. O valor ID é colocado no gerador de hash MD5.
2. O valor random é colocado no gerador de hash MD5.
3. O nome 3640-1 é usado para procurar a senha. O roteador procura uma entrada que corresponda ao nome de usuário no desafio. Neste exemplo, ele procura: `username 3640-1`

password pcl

4. A senha é alimentada no gerador de hash MD5. O resultado é o desafio de CHAP com hash MD5 unidirecional que é enviado novamente na resposta de CHAP.

Resposta (continua)

A figura do do â 5 o pacote de resposta da RACHADURA enviado ao autenticador é construída. A [Figura 5](#) ilustra como o pacote de resposta de CHAP enviado ao autenticador é criado. O diagrama mostra estas etapas:

1. O pacote de resposta é montado a partir destes componentes: 02 = identificador de tipo de pacote de resposta CHAP. ID = copiada do pacote de desafio. hash = a saída do gerador de hash MD5 (as informações misturadas do pacote de desafio). 766-1 = o nome de autenticação deste dispositivo. Isto é necessário para que o peer procure a entrada de nome de usuário e senha necessária para verificar a identidade (confira uma explicação mais detalhada na seção [Verificar CHAP](#)).
2. O pacote de resposta é então enviado ao desafiante.

Verificar CHAP

Esta seção fornece dicas para verificar sua configuração.

Figure que do do â 6 o desafiador processa o pacote de resposta

A [Figura 6](#) mostra como o desafiante processa o pacote de resposta. Estas são as etapas envolvidas quando o pacote de resposta de CHAP é processado (no autenticador):

1. O ID é utilizado para localizar o pacote de desafio original.
2. O ID é alimentado no gerador de mistura MD5.
3. O valor aleatório do desafio original é alimentado no gerador de hash do MD5.
4. O nome 766-1 é utilizado para procurar a senha de uma das seguintes fontes: Banco de dados de nome de usuário e senha local. Servidor RADIUS ou TACACS+.
5. A senha é alimentada no gerador de hash MD5.
6. O valor de hash recebido no pacote de resposta é comparado ao valor de hash MD5 calculado. A autenticação do CHAP será bem-sucedida se o valor calculado e o valor de hash recebido forem iguais.

Resultado

A figura mensagem de sucesso do do do â 7 é enviada ao roteador de chamada

A [Figura 7](#) ilustra a mensagem de sucesso enviada ao roteador de chamada. Ela envolve estas etapas:

1. Se a autenticação for bem sucedida, um pacote de sucesso de CHAP será criado a partir destes componentes: 03 = tipo de mensagem de êxito de CHAP. ID = copiada do pacote de resposta. o do do inâ da boa vinda do do do â é simplesmente um mensagem de texto que forneça uma explicação legível por usuário.
2. Se a autenticação falhar, um pacote de falha de CHAP será criado a partir destes componentes: 04 = Tipo de mensagem de falha de CHAP. ID = copiada do pacote de

resposta.o do do failureâ da autenticação do do do â ou o outro mensagem de texto, isso fornecem uma explicação legível por usuário.

3. O pacote com êxito ou com falha é, em seguida, enviado ao roteador de chamada.**Nota:** Este exemplo demonstra uma autenticação unidirecional. Em uma autenticação bidirecional, todo esse processo é repetido. Entretanto, o roteador de chamada começa o desafio inicial.

[Resolver problemas de CHAP](#)

Consulte [Troubleshooting da Autenticação de PPP](#) para obter mais informações sobre como resolver problemas.

[Informações Relacionadas](#)

- [Entendendo a saída de negociação de debug ppp](#)
- [Troubleshooting da Autenticação de PPP](#)
- [Autenticação PPP Usando os Comandos `ppp chap hostname` e `ppp authentication chap callin`](#)
- [Páginas de suporte de tecnologia de acesso](#)
- [Suporte Técnico - Cisco Systems](#)