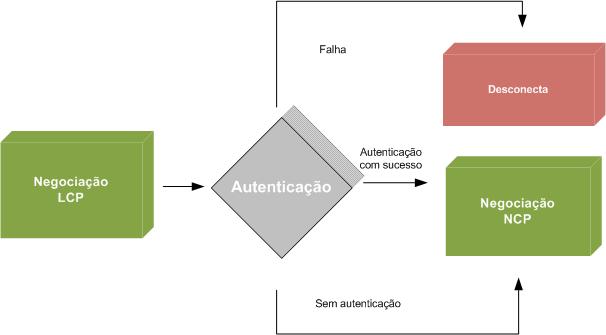
<http://www.rotadefault.com.br/autenticacao-ppp-utilizando-chap-em-roteadores-cisco/>

[**Autenticação PPP utilizando CHAP em Roteadores Cisco**](http://www.rotadefault.com.br/autenticacao-ppp-utilizando-chap-em-roteadores-cisco/)

Publicado por [diego](http://www.rotadefault.com.br/author/diego/)

A utilização do Protocolo PPP permite dois métodos de autenticação utilizando os protocolos PAP e/ou CHAP .

O processo de autenticação do PPP ocorre após o estabelecimento da negociação física, na negociação LCP da camada de enlace. Após a validação (ou não) das credenciais, o processo é finalizado ou direcionado para a Negociação NCP; responsável pela comunicação dos endereços da Camada 3.

[](http://www.rotadefault.com.br/wp-content/uploads/2011/07/Autentica%C3%A7%C3%A3o-PPP.jpg)

**Challenge-Handshake Authentication Protocol**

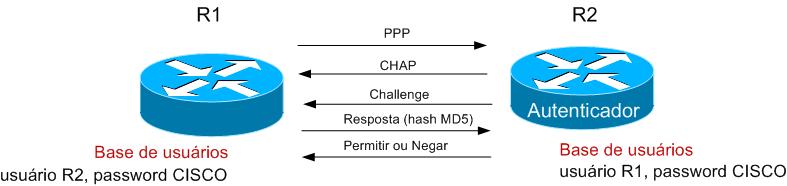
A autenticação no Protocolo PPP utilizando o CHAP permite a criptografia das credenciais no cruzamento do enlace.

Na  fase de autenticação o Roteador/Servidor Autenticador  envia mensagem de desafio (challenge) ao outro dispositivo. A reposta a esse desafio é com um valor calculado utilizando uma função hash de uma via (algoritmo MD5). O autenticador verifica se o valor de hash recebido é o esperado pelo desafio e valida a autenticação.

No protocolo CHAP a senha nunca será enviada em cima da primeira mensagem, mas utilizada para criar uma string hash de desafio em um só sentido (o servidor sabe a senha do cliente e compara o resultado das respostas).

O processo de autenticação do CHAP é detalhado na RFC 1994.

No cenário abaixo o Roteador R2 solicitará ao R1 a autenticação utilizando o protocolo CHAP.

[](http://www.rotadefault.com.br/wp-content/uploads/2011/07/PPP-CHAP.jpg)

No processo CHAP é verificada a validação dos nomes dos dispositivos no desafio (informando qual  o dispositivo que está transmitindo o frame), após isso é encaminhado  a senha para validação.

Apesar de um pouco diferente dos métodos de validação atuais, os logs do debug abaixo para autenticação PPP com CHAP é bem explicita quando refere-se a solicitação de autenticação por parte de R2 para R1. Nesse caso cadastramos o usuário como R3 e a senha como CISCO no Dispositivo R1 , para testes e visualização do “erro” no debug…

**R1#debug ppp authentication**

PPP authentication debugging is on

00:19:25.571: Se0/0 PPP: Authorization required

00:19:25.627: Se0/0 PPP: No authorization without authentication

00:19:25.635: Se0/0 CHAP: I CHALLENGE id 49 len 23 from “R2″

00:19:25.639: Se0/0 CHAP: Unable to authenticate for peer

! R1 não conhece R2 e por isso não responde as solicitações de desafio (CHALLENGE)

No processo CHAP é verificada a validação dos nomes dos dispositivos no desafio (informando qual o dispositivo que está transmitindo o frame), após o processo, é encaminhado a senha para validação.

**Configuração**

**R2:**

**username R1 password 0 CISCO**

! Configurando o usuário R1 com a senha CISCO

!

**interface Serial0/0**

**ip address 192.168.0.2 255.255.255.252**

**encapsulation ppp**

!Configurando o encapsulamento PPP na interface Serial0/0

**ppp authentication chap**

! Habilitando a autenticação CHAP

!

**R1:**

**username R2 password 0 CISCO**

! Configurando o usuário R2 com a senha CISCO

!

**interface Serial0/0**

**ip address 192.168.0.1 255.255.255.252**

**encapsulation ppp**

!Configurando o encapsulamento PPP na interface Serial0/0

**Comandos Show e Debug**

Verificação do Link antes da autenticação no R2

R2#show interface s0/0

Serial0/0 is up, line protocol is down

Hardware is GT96K Serial

Internet address is 192.168.0.1/30

MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation PPP, LCP Listen, loopback not set

!Debug da autenticação PPP ativado em R2 após a configuração completa em R1 e R2

**R2#debug ppp authentication**

00:19:17.679: Se0/0 PPP: Authorization required

00:19:17.743: Se0/0 CHAP: O CHALLENGE id 74 len 23 from “R2″

00:19:17.750: Se0/0 CHAP: I RESPONSE id 74 len 23 from “R1″

00:19:17.775: Se0/0 PPP: Sent CHAP LOGIN Request

00:19:17.779: Se0/0 PPP: Received LOGIN Response PASS

00:19:17.783: Se0/0 PPP: Sent LCP AUTHOR Request

00:19:17.787: Se0/0 LCP: Received AAA AUTHOR Response PASS

00:19:17.787: Se0/0 CHAP: O SUCCESS id 74 len

00:19:20.559: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up

Após a autenticação

**R2#show interface serial0/0**

Serial0/0 is up, line protocol is up

Hardware is GT96K Serial

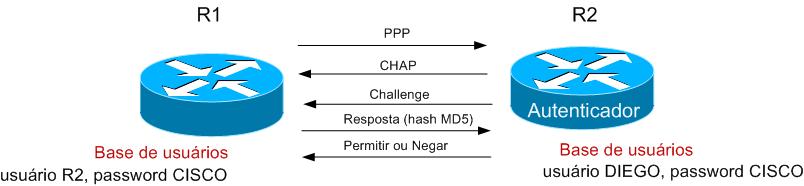
Internet address is 192.168.0.2/30

MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation PPP, LCP Open

**Mais…**

No script abaixo demonstraremos um segundo cenário forçando o Switch R1 autenticar com um hostname diferente somente para o processo CHAP, em nosso exemplo o hostname será DIEGO :  
[](http://www.rotadefault.com.br/wp-content/uploads/2011/07/PPP-CHAP-alternate-username1.jpg)

**R2:**

**username DIEGO password 0 CISCO**

! Configurando o usuário DIEGO com a senha CISCO

!

**interface Serial0/0**

**ip address 192.168.0.2 255.255.255.252**

**encapsulation ppp**

!Configurando o encapsulamento PPP na interface Serial0/0

**ppp authentication chap**

! Habilitando a autenticação CHAP

!

**R1:**

**username R2 password 0 CISCO**

! Configurando o usuário R2 com a senha CISCO

!

**interface Serial0/0**

**ip address 192.168.0.1 255.255.255.252**

**encapsulation ppp**

!Configurando o encapsulamento PPP na interface Serial0/0

**ppp chap hostname DIEGO**

!Configurando o hostname DIEGO para reposta ao Challenge do R2

**R2#debug ppp authentication**

00:39:55.875: Se0/0 PPP: Authorization required

00:39:56.023: Se0/0 CHAP: O CHALLENGE id 75 len 23 from “R2″

00:39:56.071: Se0/0 CHAP: I RESPONSE id 75 len 26 from “DIEGO”

00:39:56.071: Se0/0 PPP: Sent CHAP LOGIN Request

00:39:56.075: Se0/0 PPP: Received LOGIN Response PASS

00:39:56.079: Se0/0 PPP: Sent LCP AUTHOR Request

00:39:56.079: Se0/0 LCP: Received AAA AUTHOR Response PASS

00:39:56.083: Se0/0 CHAP: O SUCCESS id 75 len 4

00:39:57.083: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0 changed state to up