4.3.2 Challenge Handshake Authentication Protocol Bi-directional

Lab_A
Server

Lab_B
Client

Objectives:

- Learn how to configure point to point links on routers using CHAP (Challenge Handshake Authentication Protocol)
- Learn how to set PPP encapsulation on a router
- Debug the authentication process using CHAP

Background:

This lab will teach students how to configure the PPP authentication protocol, CHAP. CHAP is the authentication options requiring that the calling side of the link, the peer, enter authentication information to help ensure that the user has the network administrator's permission to make the call. In this lab, however, two-way authentication will be used. Therefore, each router requires the peer router to authenticate.

When configuring PPP authentication, you can select Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). In general, CHAP is the preferred protocol. CHAP is used to periodically verify the identity of the remote node, using a **three-way** handshake. This is done upon initial link establishment and can be repeated any time after the link has been established. CHAP offers features such as periodic verification to improve security; this makes CHAP more effective than PAP because CHAP requires a challenge before authentication can take place. Also, CHAP passwords are a shared secret and are not sent over the line in clear text like PAP.

Definition:

Challenge Handshake Authentication Protocol (CHAP)—Is a security feature supported on links using PPP encapsulation that prevents unauthorized access. CHAP does not itself prevent unauthorized access; it merely identifies the remote end. The router or access server then determines whether that user is allowed access.

Tools/Preparation:

- Standard router setup
  - Lab_A
  - Lab_B

Step 1:

Power on the routers and ensure connectivity by pinging between routers

Step 2:

On Lab_A

Define username and password to expect from the remote router.

Lab_A(config)# username *username* **password** *password*

(username is the peer router's name and the password is a shared password between Lab_A and Lab_B)

What username and password were entered?

_____

Step 3:

Enter interface configuration mode for the desired WAN interface. Configure the interface on for PPP encapsulation

Lab_A (config-if)# encapsulation ppp

Step 4:

See which ppp authentication options are available.

Lab_A (config-if)# ppp authentication ?

Record the output below.

_____

Step 5:

Now configure for CHAP authentication

Lab_A (config-if)# ppp authentication chap

Step 6:

Repeat steps 2-4 on Lab_B

Step 7:

From Lab_A, ping Lab_B**.** Was the ping successful?

_____

If the ping is unsuccessful, make sure the passwords are correct on both routers. Then proceed to Step 7, enable debugging, and use the information to determine where the problem is. Do not proceed to Step 8 until you have connectivity between the routers.

Step 8:

Enable debugging on both routers with the command.

Lab_A# debug ppp authentication

Step 9:

Break the serial link between the two routers by pulling a v.35 cable from S0 or S1 on either router. Wait for the interface to go into a down state before proceeding to Step 10.

Step 10:

Plug the v.35 cable in to reestablish the connection and view the debug output of CHAP authentication.

Does the output indicate success or failure? _____

Record the debug output below.

_____

_____

_____

_____

_____

Step 11:

Now delete the username or password on both routers.

Lab_A(config)# no username ***name*** password***password***

Now configure an incorrect username or password on both routers.

Lab_A(config)# username ***wrong_name*** password ***wrong_password***

Step 12:

Un-plug one of the serial port V.35 cables between the routers and wait for the interface to shutdown. Then plug it back in and view the authentication process displayed in the debug output.

Does the output indicate success or failure? _____
How would this output help solve authentication problems?

_____

Record the debug output below.

_____
_____
_____
_____
_____
_____
_____

Notes:

_____
_____
_____
_____
_____
_____