



## 2.3.2.6 CONFIGURACIÓN DE LA AUTENTICACIÓN CHAP Y PAP

YANET ISLAS YAÑEZ

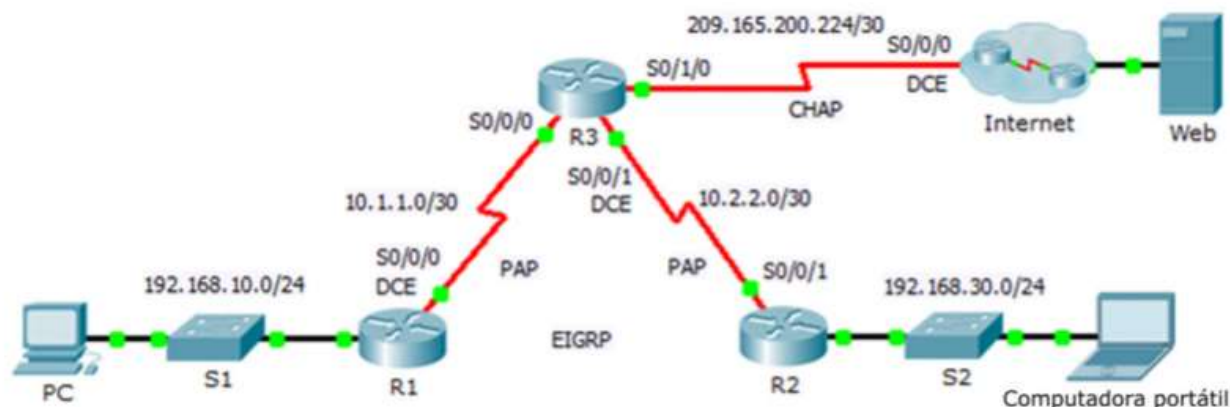
ITI 91

Aplicación de  
Telecomunicaciones

MTI. Oscar Lira Uribe

## Packet Tracer: Configuración de la autenticación CHAP y PAP

### Topología



### Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0	192.168.10.1	255.255.255.0	N/D
	S0/0/0	10.1.1.1	255.255.255.252	N/D
R2	G0/0	192.168.30.1	255.255.255.0	N/D
	S0/0/1	10.2.2.2	255.255.255.252	N/D
R3	S0/0/0	10.1.1.2	255.255.255.252	N/D
	S0/0/1	10.2.2.1	255.255.255.252	N/D
	S0/1/0	209.165.200.225	255.255.255.252	N/D
ISP	S0/0/0	209.165.200.226	255.255.255.252	N/D
	G0/0	209.165.200.1	255.255.255.252	N/D
Web	NIC	209.165.200.2	255.255.255.252	209.165.200.1
PC	NIC	192.168.10.10	255.255.255.0	192.168.10.1
Computador a portátil	NIC	192.168.30.10	255.255.255.0	192.168.30.1

### Objetivos

**Parte 1: Revisar las configuraciones de routing**

**Parte 2: Configurar PPP como método de encapsulamiento**

**Parte 3: Configurar la autenticación de PPP**

### Aspectos básicos

En esta actividad, practicará cómo configurar el encapsulamiento de PPP en enlaces seriales. También configurará la autenticación PAP de PPP y CHAP de PPP.

## Parte 1: Revisar las configuraciones del routing

### Paso 1: Ver las configuraciones en ejecución en todos los routers.

Mientras analiza las configuraciones del router, observe el uso del enrutamiento estático y de las rutas dinámicas en la topología.

```
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
description Link to R1
ip address 10.1.1.2 255.255.255.252
!
interface Serial0/0/1
description Link to R2
ip address 10.2.2.1 255.255.255.252
clock rate 4000000
!
interface Serial0/1/0
description Link to ISP
ip address 209.165.200.225 255.255.255.252
!
interface Serial0/1/1
no ip address
clock rate 2000000
!
interface Vlan1
no ip address
shutdown
```

```
interface GigabitEthernet0/0
ip address 192.168.30.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
no ip address
clock rate 4000000
!
interface Serial0/0/1
ip address 10.2.2.2 255.255.255.252
!
interface Vlan1
no ip address
shutdown
!
router eigrp 1
passive-interface GigabitEthernet0/0
network 10.2.2.0 0.0.0.3
network 192.168.30.0
```

```
interface GigabitEthernet0/0
ip address 192.168.10.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
ip address 10.1.1.1 255.255.255.252
clock rate 4000000
!
interface Serial0/0/1
no ip address
clock rate 2000000
!
interface Vlan1
no ip address
shutdown
!
router eigrp 1
passive-interface GigabitEthernet0/0
network 192.168.10.0
network 10.1.1.0 0.0.0.3
```

## Parte 2: Configurar PPP como el método de encapsulación

### Paso 1: Configurar el R1 para que utilice la encapsulación PPP con el R3.

Ingrese los siguientes comandos en R1:

```
R1(config)# interface s0/0/0
R1(config-if)# encapsulation ppp
```

```
R1>en
R1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#in s0/0/0
R1(config-if)#encapsulation ppp
R1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.1.1.2 (Serial0/0/0) is down: interface down
```

## Paso 2: Configurar el R2 para que utilice la encapsulación PPP con el R3.

Ingrese los comandos apropiados en R2:

```
R2>en
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int s0/0/1
R2(config-if)#encapsulation
% Incomplete command.
R2(config-if)#encapsulation ppp
R2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.2.2.1 (Serial0/0/1) is down: interface down
```

## Paso 3: Configurar el R3 para que utilice la encapsulación PPP con el R1, el R2 y el ISP.

Ingrese los comandos apropiados en R3:

```
R3>
R3>en
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#int s0/0/0
R3(config-if)#encapsulation ppp
R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.1.1.1 (Serial0/0/0) is up: new adjacency

R3(config-if)#int s0/0/1
R3(config-if)#encapsulation ppp
R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.2.2.2 (Serial0/0/1) is up: new adjacency

R3(config-if)#int s0/1/0
R3(config-if)#encapsulation ppp
R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to down

R3(config-if)#
```

## Paso 4: Configurar el ISP para que utilice la encapsulación PPP con el R3.

- Haga clic en la nube de Internet, luego ISP. Introduzca los siguientes comandos:

```
Router(config)# interface s0/0/0
Router(config-if)# encapsulation ppp
```

- Salga de la nube de Internet haciendo clic en Back en la esquina superior izquierda o presionando la flecha de Alt+left.

```
Router(config-if)#encapsulation ppp
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up
```



## Parte 3: Configurar la autenticación PPP

### Paso 1: Configurar la autenticación PAP de PPP entre el R1 y el R3.

Nota: En lugar de utilizar la contraseña **de la palabra** clave como se muestra en el programa, utilizará la contraseña secreta **de la palabra** clave para proporcionar una mejor encriptación de la contraseña.

- a. Ingrese los siguientes comandos en R1:

```
R1(config)# username R3 secret class
R1(config)# interface s0/0/0
R1(config-if)# ppp authentication pap
R1(config-if)# ppp pap sent-username R1 password cisco
```

- b. Introduzca los siguientes comandos en R3:

```
R3(config)# username R1 secret cisco
R3(config)# interface s0/0/0
R3(config-if)# ppp authentication pap
R3(config-if)# ppp pap sent-username R3 password class
```

```
R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int s0/0/0
R1(config-if)#exit
R1(config)#username R3 secret class
R1(config)#int s0/0/0
R1(config-if)#ppp authentication pap
R1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to down

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.1.1.2 (Serial0/0/0) is
down: interface down

R1(config-if)#ppp pap sent
% Incomplete command.
R1(config-if)#ppp pap sent-username R1 password cisco
R1(config-if)#
```

```
R3>en
R3#confi
Configuring from terminal, memory, or network [terminal]? t
Enter configuration commands, one per line. End with CNTL/
Z.
R3(config)#username R1 secret cisco
R3(config)#int s0/0/0
R3(config-if)#ppp authentication pap
R3(config-if)#ppp pap sent-username R3 password class
R3(config-if)#
R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up
```

## Paso 2: Configurar la autenticación PAP de PPP entre el R2 y el R3.

Repita el Paso 1 para configurar la autenticación entre **R2** y **R3** que cambia los nombres de usuario según sea necesario. Observe que cada contraseña enviada en cada puerto serial coincide con la contraseña que se esperaba por el router opuesto.

```
R2(config)#username R3 secret class
R2(config)#int s0/0/1
R2(config-if)#ppp authentication pap
R2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to down

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.2.2.1 (Serial0/0/1) is
down: interface down

R2(config-if)#ppp sent-username R2 password cisco
R2(config-if)#
% Invalid input detected at '^' marker.

R2(config-if)#ppp pap sent-username R2 password cisco
R2(config-if)#

R3(config)#username R2 secret cisco
R3(config)#int s0/0/1
R3(config-if)#ppp authentication pap
R3(config-if)#ppp pap sent-username R3 password class
R3(config-if)#
```

## Paso 3: Configurar la autenticación CHAP de PPP entre el R3 y el ISP.


- Introduzca los siguientes comandos en el **ISP**. El nombre de host se envía como nombre de usuario:
- Introduzca los siguientes comandos en **R3**. Las contraseñas deben coincidir para la autenticación CHAP:

```
Router(config)# hostname ISP
ISP(config)# username R3 secret cisco
ISP(config)# interface s0/0/0
ISP(config-if)# ppp authentication chap

R3(config)# username ISP secret cisco
R3(config)# interface serial0/1/0
R3(config-if)# ppp authentication chap

Router(config)#username R3 secret cisco
Router(config)#int s0/0/0
Router(config-if)#ppp authentication chap
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to down

R3(config-if)#exit
R3(config)#username ISP secret cisco
R3(config)#int s0/1/0
R3(config-if)#ppp authentication chap
R3(config-if)#
```

 PT Activity: 03:32:38

**Paso 4: Configurar ISP para que use el encapsulamiento PPP con R3.**

- Haga clic en la nube de Internet, luego ISP. Introduzca los siguientes comandos:

```
Router(config)# interface s0/0/0
Router(config-if)# encapsulation ppp
```
- quit la nube de Internet haciendo clic en Back en la esquina superior izquierda o presionando la flecha de Alt+left.

**Paso 5: Probar la conectividad al servidor web.**

La PC y computadoras portátiles deben poder hacer ping al servidor Web en 209.165.200.2. Esto puede demorar cierto tiempo mientras que las interfaces comienzan a trabajar nuevamente y EIGRP vuelve a converger.

**Parte 3: Configurar la autenticación de PPP**

**Paso 1: Configurar la autenticación PAP de PPP entre R1 y R3.**

Nota: En lugar de utilizar la contraseña de la palabra clave como se muestra en el programa, utilizará la contraseña secreta de la palabra clave para proporcionar una mejor encriptación de la contraseña.

Time Elapsed: 03:32:38Completion: 90/90

☐ Top

Check Results

Reset Activity

<

1/1

>

## CONCLUSION

El protocolo de autenticación (CHAP) se usa para verificar periódicamente la identidad del usuario, utilizando un protocolo de enlace de tres vías. Esto se realiza en el establecimiento inicial del enlace y se puede repetir periódicamente. El principio distintivo de CHAP se basa en la protección que se brinda al evitar la transmisión de cualquier contraseña a través del enlace, en lugar de confiar en un proceso de desafío y respuesta que solo puede tener éxito si tanto el autenticado como los dispositivos autorizados están reconociendo un valor conocido como secreto es decir la contraseña y así evitar posibles “intrusos”