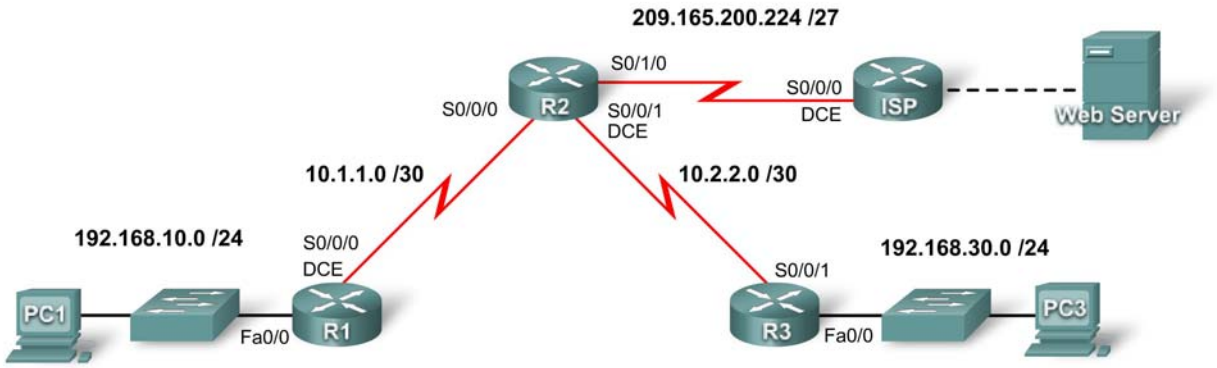
PT Activity 2.4.6: Configuring PAP and CHAP Authentication

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	Fa0/0	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.252
R3	Fa0/0	192.168.30.1	255.255.255.0
	S0/0/0	10.2.2.2	255.255.255.252
ISP	S0/0/0	209.165.200.226	255.255.255.252
	Fa0/0	209.165.200.1	255.255.255.252
Web Server	NIC	209.165.200.2	255.255.255.252
PC1	NIC	192.168.10.10	255.255.255.0
PC3	NIC	192.168.30.10	255.255.255.0

Learning Objectives

- Configure OSPF routing
- Configure PAP authentication between R1 and R2
- Configure CHAP authentication between R3 and R2

Introduction

PPP encapsulation allows for two different types of authentication: PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). PAP uses a clear-text password, while CHAP invokes a one-way hash that provides more security than PAP. In this activity, you will configure both PAP and CHAP as well as review OSPF routing configuration.

Task 1: Configure OSPF Routing

Step 1: Enable OSPF on R1.

With a *process-ID* of **1**, use the **router ospf 1** command to enable OSPF routing.

Step 2: Configure network statements on R1.

In router configuration mode, add all the networks connected to R1 using the **network** command. The OSPF *area-id* parameter is **0** for all the **network** statements in this topology.

```
R1(config-router)#network 192.168.10.0 0.0.0.255 area 0
R1(config-router)#network 10.1.1.0 0.0.0.3 area 0
```

Step 3: Configure network statements on R2 and R3.

Repeat steps 1 and 2 for routers R2 and R3. Use the addressing table to determine the correct statements. On R2, do *not* advertise the 209.165.202.224/30 network. You will configure a default route in the next step.

Step 4: Establish and redistribute the OSPF default route.

- On R2, create a static default route to ISP with the command **ip route 0.0.0.0 0.0.0.0 s0/1/0**.
- At the router prompt, issue the **default-information originate** command to include the static route in OSPF updates sent from R2.

Step 5: Verify end-to-end connectivity.

At this point in your configuration, all devices should be able to ping all locations.

Click **Check Results**, and then click **Connectivity Tests**. The Status should be “Correct” for both tests**.** The routing tables for R1, R2, and R3 should be complete. R1 and R3 should have a default route as shown in the routing table for R1 below:

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
<output omitted>

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

     10.0.0.0/30 is subnetted, 2 subnets
C       10.1.1.0 is directly connected, Serial0/0/0
O       10.2.2.0 [110/128] via 10.1.1.2, 00:03:59, Serial0/0/0
C    192.168.10.0/24 is directly connected, FastEthernet0/0
O    192.168.30.0/24 [110/129] via 10.1.1.2, 00:02:19, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 10.1.1.2, 00:02:19, Serial0/0/0
```


Step 6: Check results.

Your completion percentage should be 40%. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Configure PAP Authentication

Step 1: Configure R1 to use PAP authentication with R2.

- On R1 in global configuration mode, type the command **username R2 password cisco123**. This command enables the remote router R2 to connect to R1 when using the password **cisco123**.
- Change the encapsulation type on the s0/0/0 interface of R1 to PPP using the **encapsulation ppp** command.
- While in the serial interface, configure PAP authentication with the **ppp authentication pap** command.
- Configure the username and password that will be sent to R2 with the **ppp pap sent-username R1 password cisco123** command. Although Packet Tracer does not grade the **ppp pap sent-username R1 password cisco123** command, the command is required to successfully configure PAP authentication.
- Return to the privileged exec mode and use the **show ip interface brief** command to observe that the link between R1 and R2 has gone down.

```
R1(config)#username R2 password cisco123
R1(config)#interface s0/0/0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication pap
R1(config-if)#ppp pap sent-username R1 password cisco123
R1(config-if)#end
%SYS-5-CONFIG_I: Configured from console by console
R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.10.1    YES manual up                    up
FastEthernet0/1        unassigned      YES manual administratively down down
Serial0/0/0            10.1.1.1        YES manual up                    down
Serial0/0/1            unassigned      YES manual administratively down down
Vlan1                  unassigned      YES manual administratively down down
```

Step 2: Configure R2 to use PAP authentication with R1.

Repeat Step 1 for R2, using the serial link to R1.

Remember, the name used in the command **username** *name* **password** *password* is always the name of the remote router, but in the **ppp pap sent-username** *name* **password** *password* command, the name is that of the originating router.

Note: Although Packet Tracer will bring the link up, on real equipment it is necessary to **shutdown** and then **no shutdown** the interface to force PAP to reauthenticate. You could also simply reload the routers.

Step 3: Test connectivity between the PC1 and the web server.

Use the **show ip interface brief** command to observe that the link between R1 and R2 is now up. Access to the web server from R1 should now be restored. Test this by sending a ping from PC1 to the web server.

```
R2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES manual administratively down down
FastEthernet0/1        unassigned      YES manual administratively down down
```



```
Serial0/0/0            10.1.1.2        YES manual up                    up
Serial0/0/1            10.2.2.1        YES manual up                    up
Serial0/1/0            209.165.200.225 YES manual up                    up
Serial0/1/1            unassigned      YES manual administratively down down
Vlan1                  unassigned      YES manual administratively down down
```

Step 4: Check results.

Your completion percentage should be 70%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Configure CHAP Authentication

Step 1: Configure R3 to use CHAP authentication with R2.

- In global configuration mode for R3, type **username R2 password cisco123**.
- On the s0/0/1 interface, issue the **encapsulation ppp** and **ppp authentication chap** commands, enabling PPP encapsulation and CHAP authentication.
- Use the **show ip interface brief** command to observe that the link between R2 and R3 has gone down.

```
R3(config)#username R2 password cisco123
R3(config)#interface s0/0/1
R3(config-if)#encapsulation ppp
R3(config-if)#ppp authentication chap
```

Step 2: Configure R2 to use CHAP authentication with R3.

Repeat Step 1 for R2, but change the username to R3**,** because R3 is the remote router.

Step 3: Test connectivity between PC3 and the web server.

Using the **show ip interface brief** command, you should see that the link between R2 and R3 is now up, and PC3 can ping the web server.

Step 4: Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

