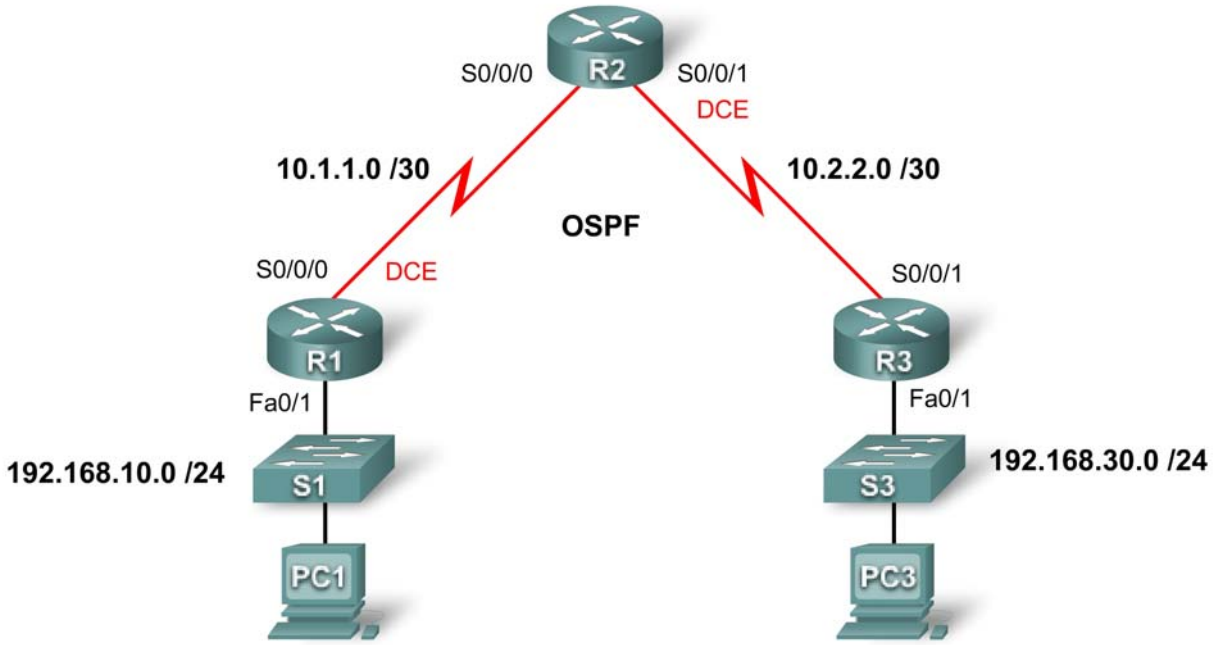
PT Activity 4.3.3: Configuring OSPF Authentication

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	**Fa0/1**	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
R3	**Fa0/1**	192.168.30.1	255.255.255.0
	S0/0/1	10.2.2.2	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 simple authentication
- Configure OSPF MD5 authentication
- Test connectivity

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Introduction

This activity covers both OSPF simple authentication and OSPF MD5 (message digest 5) authentication. You can enable authentication in OSPF to exchange routing update information in a secure manner. With simple authentication, the password is sent in clear-text over the network. Simple authentication is used when devices within an area cannot support the more secure MD5 authentication. With MD5 authentication, the password does not sent over the network. MD5 is considered the most secure OSPF authentication mode. When you configure authentication, you must configure an entire area with the same type of authentication. In this activity, you will configure simple authentication between R1 and R2, and MD5 authentication between R2 and R3.

Task 1: Configure OSPF Simple Authentication

Step 1. Configure R1 with OSPF simple authentication.

To enable simple authentication on R1, enter router configuration mode using the **router ospf 1** command at the global configuration prompt. Then issue the **area 0 authentication** command to enable authentication.

```
R1(config)#router ospf 1
R1(config-router)#area 0 authentication
00:02:30: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.1 on Serial0/0/0 from FULL to
DOWN, Neighbor Down: Dead timer expired
00:02:30: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.1 on Serial0/0/0 from FULL to
Down: Interface down or detached
```

The **area 0 authentication** command enables authentication for all the interfaces in area 0. Using only this command works for R1, because it does not have to support any other types of authentication.

Eventually, you will see a console message that adjacency with R2 is down. R1 loses all OSPF routes from its routing table until it is able to authenticate routes with R2. Even though you have not yet configured a password, R1 is requiring any neighbors to use authentication in OSPF routing messages and updates.

To configure R1 will a simple authentication password, enter interface configuration mode for the link that connects to R2. Then issue the **ip ospf authentication-key cisco123** command. This command sets the authentication password to **cisco123**.

```
R1(config-router)#interface S0/0/0
R1(config-if)#ip ospf authentication-key cisco123
```

Step 2. Configure R2 with OSPF simple authentication.

You configured authentication on R1 for the entire area. Because R2 will support both simple and MD5 authentication, the commands are entered at the interface level.

Enter the interface configuration mode for S0/0/0. Specify that you are using simple authentication with the **ip ospf authentication** command. Then issue the **ip ospf authentication-key cisco123** command to set the authentication password to **cisco123**.

```
R2(config)#interface S0/0/0
R2(config-if)#ip ospf authentication
R2(config-if)#ip ospf authentication-key cisco123
00:07:45: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on Serial0/0/0 from
EXCHANGE to FULL, Exchange Done
```

When you have completed these configuration tasks, you should eventually see a console message indicating that adjacency is reestablished between R1 and R2. The OSPF routes are reinstalled into the routing table.

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Step 3. Check results.

Your completion percentage should be 50%. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Configure OSPF MD5 Authentication

Step 1. Configure R3 with OSPF MD5 authentication.

To enable MD5 authentication on R3, enter router configuration mode using the **router ospf 1** command at the global configuration prompt. Then issue the **area 0 authentication message-digest** command to enable authentication.

```
R3(config)#router ospf 1
R3(config-router)#area 0 authentication message-digest
00:10:00: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.1 on Serial0/0/1 from FULL to
DOWN, Neighbor Down: Dead timer expired
00:10:00: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.1 on Serial0/0/1 from FULL to
Down: Interface down or detached
```

Eventually, you will see a console message that adjacency with R2 is down. R3 loses all OSPF routes from its routing table until it is able to authenticate routes with R2.

To configure R3 will the MD5 authentication password, enter interface configuration mode for the link that connects to R2. Then issue the **ip ospf message-digest-key 1 md5 cisco123** command. This command sets the OSPF authentication password to **cisco123**, protected with the MD5 algorithm.

```
R3(config-router)#interface S0/0/1
R3(config-if)#ip ospf message-digest-key 1 md5 cisco123
```

Step 2. Configure R2 with OSPF MD5 authentication.

On R2, enter interface configuration mode for the link that connects to R3. Issue the **ip ospf authentication message-digest** command to enable MD5 authentication. This command is necessary on R2 because this router is using two types of authentication.

Then issue the **ip ospf message-digest-key 1 md5 cisco123** command to set up the authentication password.

```
R2(config)#interface S0/0/1
R2(config-if)#ip ospf authentication message-digest
R2(config-if)#ip ospf message-digest-key 1 md5 cisco123
00:13:51: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on Serial0/0/1 from
EXCHANGE to FULL, Exchange Done
```

After entering this command, give the routers a moment to converge. You should see a console message on both R2 and R3 indicating that neighbor adjacency is reestablished. You can confirm that R2 has reinstalled the OSPF routes and that R2 has R3 as an OSPF neighbor.

```
R2#show ip route
<output omitted>

Gateway of last resort is not set

     10.0.0.0/30 is subnetted, 2 subnets
C       10.1.1.0 is directly connected, Serial0/0/0
C       10.2.2.0 is directly connected, Serial0/0/1
O    192.168.10.0/24 [110/65] via 10.1.1.1, 00:06:13, Serial0/0/0
O    192.168.30.0/24 [110/65] via 10.2.2.2, 00:00:07, Serial0/0/1
```

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

```
R2#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.10.1      1   FULL/-          00:00:32    10.1.1.1        Serial0/0/0
192.168.30.1      1   FULL/-          00:00:37    10.2.2.2        Serial0/0/1
```

Step 3. Check results.

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

Task 3: Test Connectivity

Authentication should now be configured correctly on all three routers, so PC1 should have no trouble pinging PC3. Click **Check Results**, and then **Connectivity Tests** to see if it is successful.

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.