Lab Assignment
& Solution

Cybersecurity Professional Program

Network Security

Network Attacks & Mitigation

NS-03-LS2
Layer 3 Mitigation

Note: Solutions for the instructor are shown inside the green box.

Lab Objective

The objective is to gain an understanding of risk mitigation in the network layer of the OSI model.

Lab Mission

Learn about best practices to configure mitigation settings for DHCP, NTP, and OSPF spoofing.

Lab Duration

20–30 minutes

Requirements

- Basic knowledge of Cisco IOS commands and navigation
- Basic knowledge of NTP authentication
- Basic knowledge of DHCP snooping
- Basic knowledge of OSPF authentication

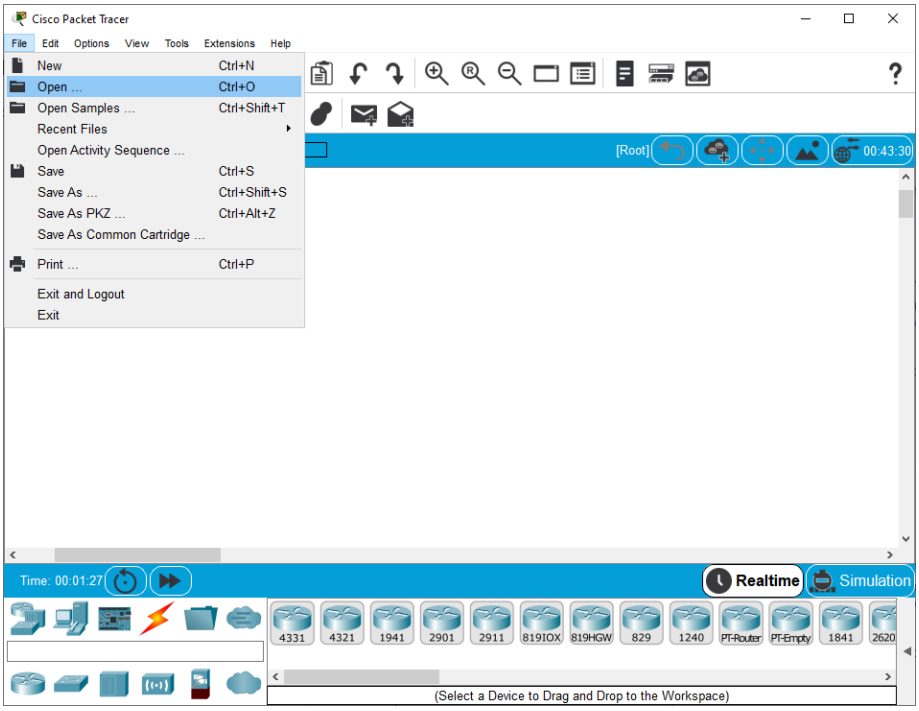
Resources

- Environment & Tools
  - Cisco Packet Tracer 7.2.2 or later
- Extra Lab Files
  - ***NS-03-L2.pkt***

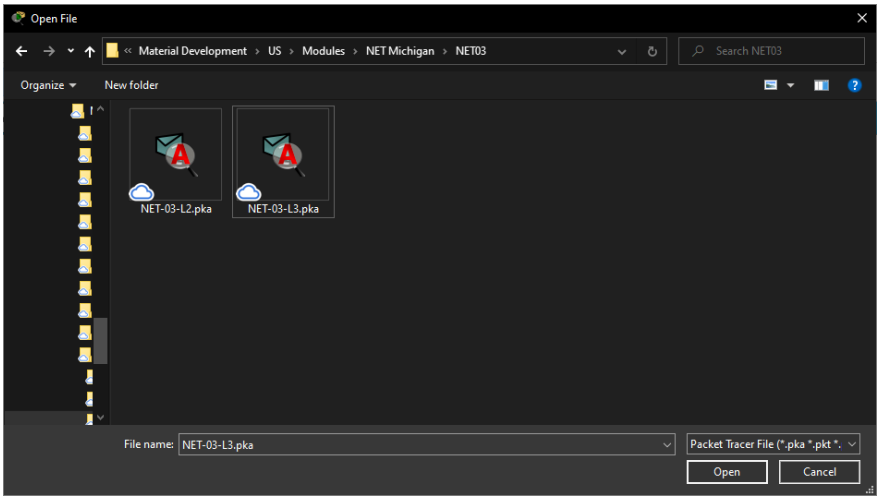
Instructions for PKT Lab Files

Lab material includes the lab document and a PKT lab file.

Open the PKT file through the Cisco Packet Tracer menu by clicking **File** and then ***Open…***.



Navigate to the file's location and open it.



Note: Double-clicking the PKT file in your file explorer may not work (depending on the Packet Tracer version).

Lab Task 1: Configuring NTP Authentication

This task involves synchronizing router clocks with the NTP server, enabling NTP authentication on the server, and configuring routers for authentication via the server.

Tip
Check the time with the ***show clock*** command

1 Configure all routers to receive clock information from the NTP server.

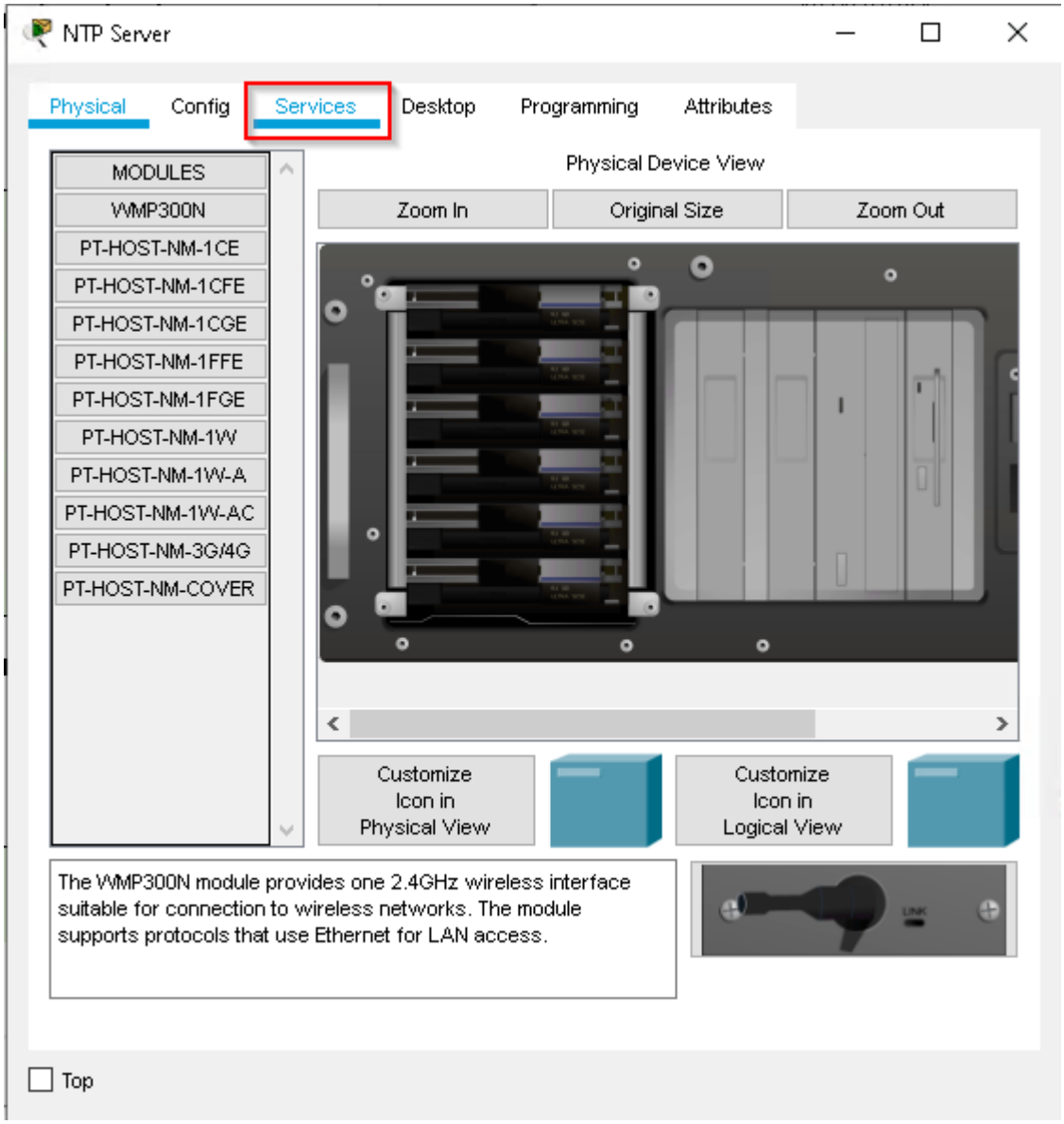
```
R1:

R1>enable
R1#configure terminal
R1(config)#ntp server 192.168.0.2

R2:

R2>enable
R2#configure terminal
R2(config)#ntp server 192.168.0.2


R3:

R3>enable
R3#configure terminal
R3(config)#ntp server 192.168.0.2
```

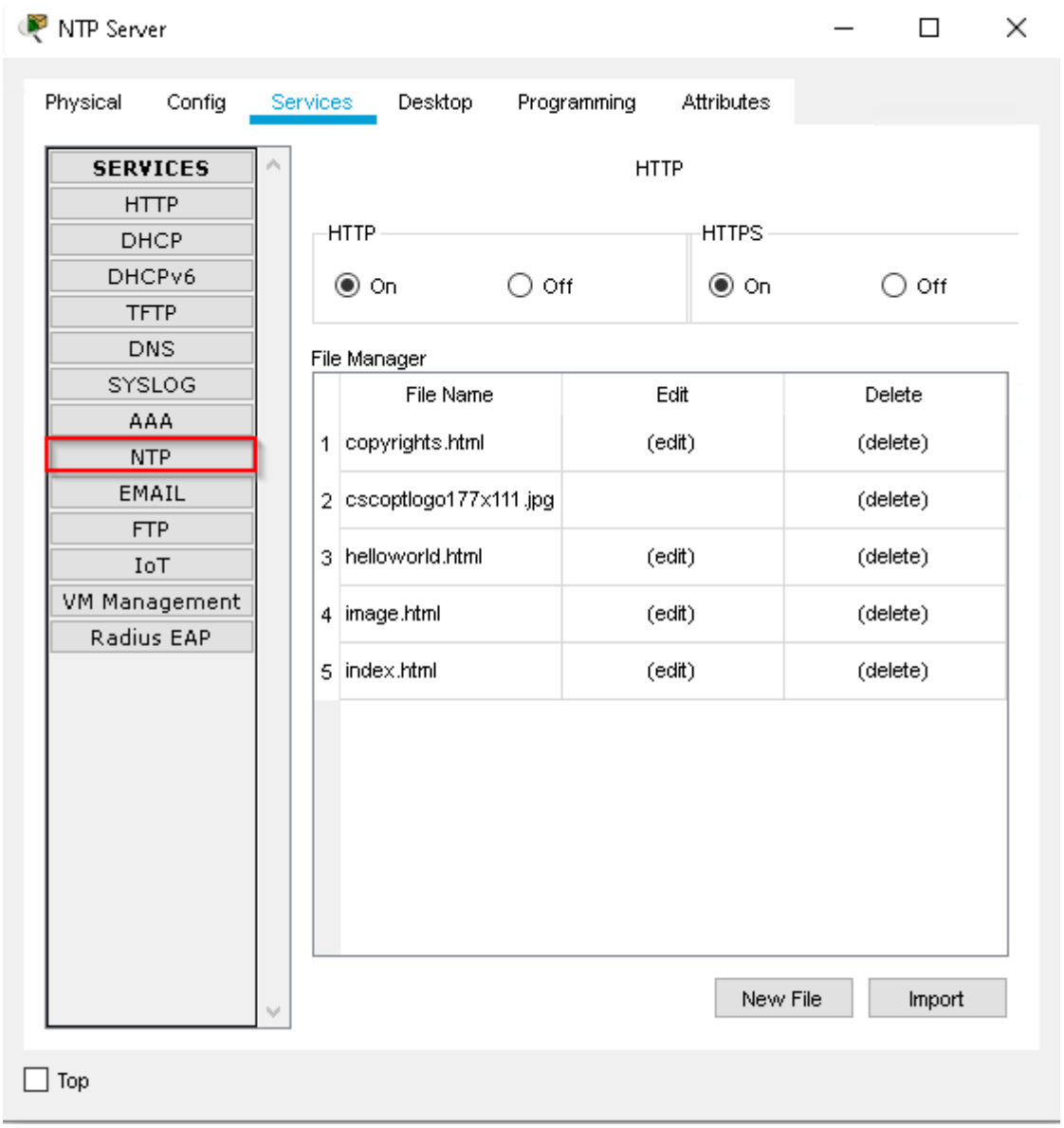
2 Enable the authentication key on the NTP server using the following settings:

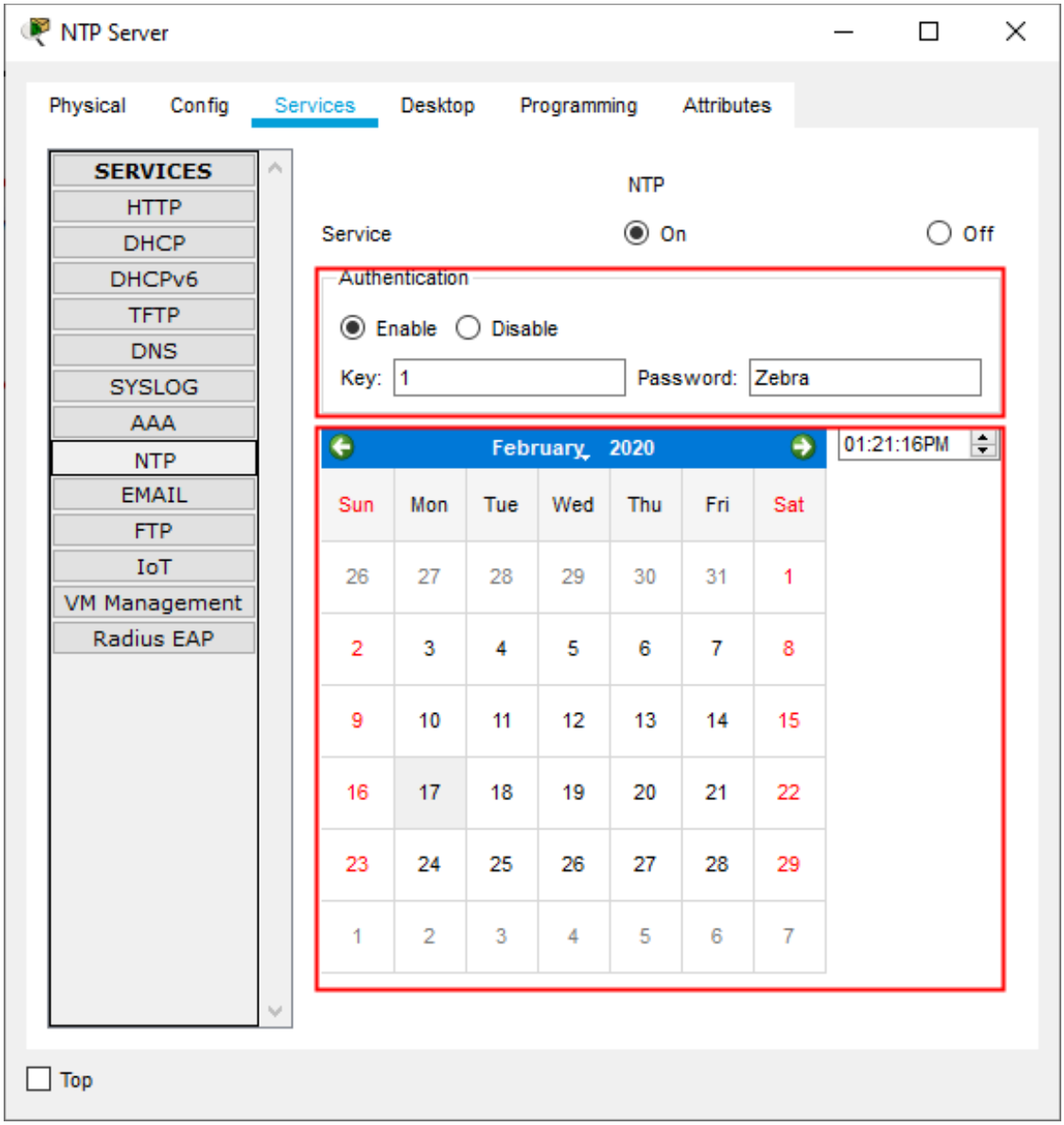
- Key-id: 1
- Password: Zebra
- Set the clock to the current date and time.

Go to the NTP server and click ***Services***. Navigate to NTP and enter the required information.

Note: Make sure the correct time and date are set on the server.




NTP Server
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
HTTP
HTTP
On
Off
HTTPS
On
Off
File Manager
File Name
Edit
Delete
1 copyrights.html (edit) (delete)
2 cscoptlogo177x111.jpg (delete)
3 helloworld.html (edit) (delete)
4 image.html (edit) (delete)
5 index.html (edit) (delete)
New File
Import
Top


NTP Server
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
NTP
Service
On
Off
Authentication
Enable
Disable
Key:
1
Password:
Zebra
February
2020
01:21:16PM
Sun
Mon
Tue
Wed
Thu
Fri
Sat
26 27 28 29 30 31 1
2 3 4 5 6 7 8
9 10 11 12 13 14 15
16 17 18 19 20 21 22
23 24 25 26 27 28 29
1 2 3 4 5 6 7
Top

3 On all routers, configure NTP authentication as follows:

- Enable NTP authentication.
- Configure the appropriate key-id and password.
- Configure the trusted key and server address.

These settings will force the routers and server to validate the key and password before synchronizing.

```
R1:

R1(config)#ntp authenticate
R1(config)#ntp authentication-key 1 md5 Zebra
R1(config)#ntp trusted-key 1
R1(config)#ntp server 192.168.0.2 key 1
R1(config)#exit

R2:

R2(config)#ntp authenticate
R2(config)#ntp authentication-key 1 md5 Zebra
R2(config)#ntp trusted-key 1
R2(config)#ntp server 192.168.0.2 key 1
R2(config)#exit

R3:

R3(config)#ntp authenticate
R3(config)#ntp authentication-key 1 md5 Zebra
R3(config)#ntp trusted-key 1
R3(config)#ntp server 192.168.0.2 key 1
R3(config)#exit
```

4 Use the ***show clock*** and ***show NTP status*** commands on all routers to verify the clock and NTP settings.

Important: If the clock was not changed, enter the command ***show clock***, click ***Fast-forward*** at the bottom left corner *several times,* and check again.

```
R1:

R1#show clock
```

```
R1>enable
R1#show clock
4:48:21.853 UTC Fri May 29 2020
R1#show ntp status
Clock is synchronized, stratum 2, reference is 192.168.0.2
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz,
precision is 2**24
reference time is E2538597.000000D3 (4:48:23.211 UTC Fri May
29 2020)
clock offset is 0.00 msec, root delay is 5.00  msec
root dispersion is 10.53 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift
is - 0.000001193 s/s system poll interval is 4, last update
was 7 sec ago.
R1#
```

```
R2:

R2#show clock
```

```
R2>enable
R2#show clock
4:51:22.899 UTC Fri May 29 2020
R2#show ntp status
Clock is synchronized, stratum 2, reference is 192.168.0.2
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz,
precision is 2**24
reference time is E2538615.000002CA (4:50:29.714 UTC Fri May
29 2020)
clock offset is 0.00 msec, root delay is 0.00  msec
root dispersion is 10.50 msec, peer dispersion is 0.48 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift
is - 0.000001193 s/s system poll interval is 6, last update
was 59 sec ago.
R2#
```

```
R3:

R3#show clock
```

```
R3>enable
R3#show clock
4:52:9.345 UTC Fri May 29 2020
R3#show ntp status
Clock is synchronized, stratum 2, reference is 192.168.0.2
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz,
precision is 2**24
reference time is E2538680.000000C7 (4:52:16.199 UTC Fri May
29 2020)
clock offset is 0.00 msec, root delay is 5.00  msec
root dispersion is 10.17 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift
is - 0.000001193 s/s system poll interval is 4, last update
was 2 sec ago.
R3#
```

Lab Task 2: Enabling DHCP Snooping

This task involves enabling DHCP snooping on the switches in the network. The settings in this part help prevent DHCP spoofing and starvation.

Note: A DHCP server with all the necessary pools is already preconfigured. Do not change or alter them. It is recommended to verify that the IP assignment on all PCs was performed via the DHCP server.

1 In S1, enable DHCP snooping globally.

```
S1>enable
S1#configure terminal
S1(config)#ip dhcp snooping
```

2 In S1, enable DHCP snooping on VLAN 1.

```
S1(config)#ip dhcp snooping vlan 1
```

3 In S1, configure the uplink interface pointing in the direction of the DHCP server as ***trusted***.

```
S1(config)#interface gigabitethernet 0/1
S1(config-if)#ip dhcp snooping trust
S1(config-if)#exit
```

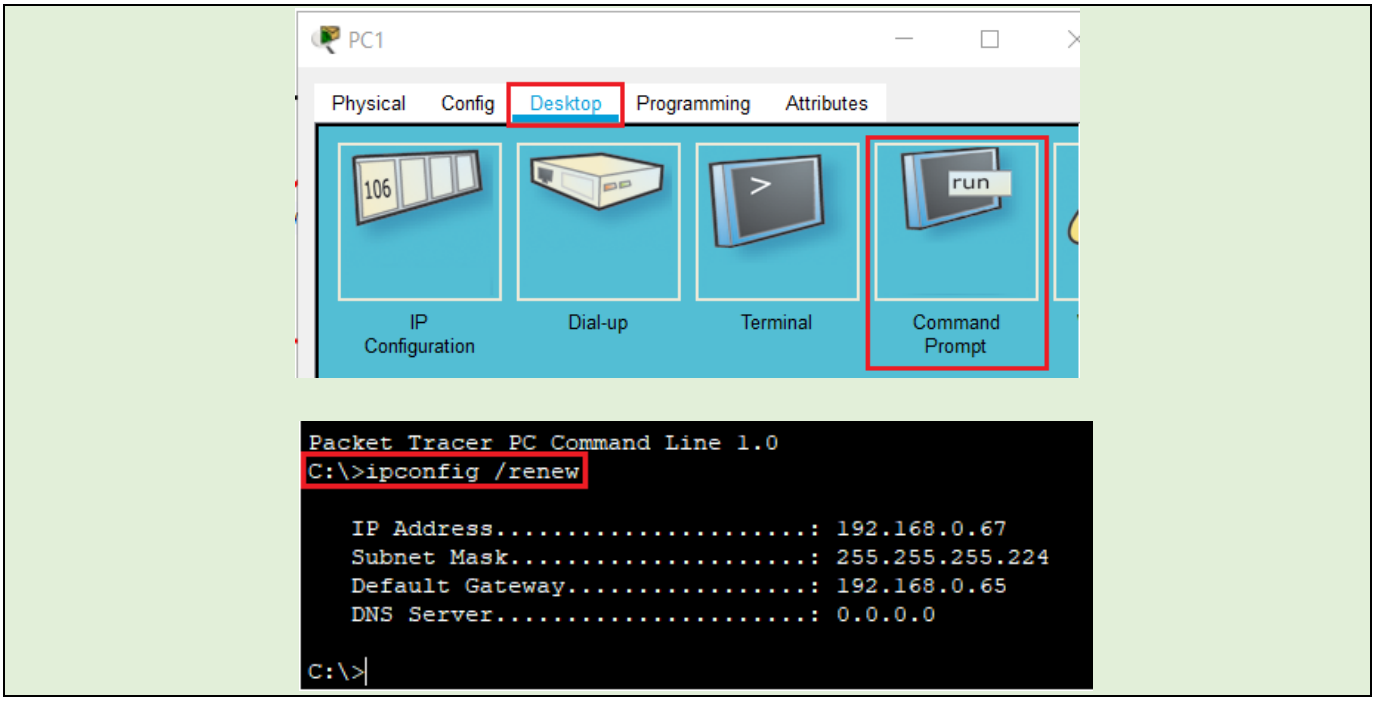
4 On all other ports that are connected to end devices and potentially not trusted, limit the number of DHCP requests per second to 3 (which mitigates DHCP starvation).

```
S1(config)#interface range fastethernet 0/1-24
S1(config-if-range)#ip dhcp snooping limit rate 3
S1(config-if-range)#exit
```

5 Repeat steps 1–4 on S2.

```
S2>enable
S2#configure terminal
S2(config)#ip dhcp snooping
S2(config)#ip dhcp snooping vlan 1
S2(config)#interface gigabitethernet 0/1
S2(config-if)#ip dhcp snooping trust
S2(config-if)#exit
S2(config)#interface range fastethernet 0/1-24, gigabitethernet 0/2
S2(config-if-range)#ip dhcp snooping limit rate 3
S2(config-if-range)#exit
```

6 In the command prompt (**Desktop** tab) of PCs 1–6, run ***ipconfig /renew*** to re-initiate the DHCP process between the client and server. By doing so, the feature will then build the DHCP snooping binding table.



7 Verify the DHCP snooping feature setting by displaying the IP DHCP snooping binding table on S1 and S2. Verify your configurations for the ones presented in the images.

S1:

```
S1>show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:04:9A:CB:A2:0B   192.168.0.67     86400       dhcp-snooping  1     FastEthernet0/1
00:01:97:D3:35:90   192.168.0.66     86400       dhcp-snooping  1     FastEthernet0/2
00:E0:F9:BC:63:B2   192.168.0.68     86400       dhcp-snooping  1     FastEthernet0/3
Total number of bindings: 3
S1>
```

S2:

```
S2#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:0C:CF:1A:56:CD   192.168.0.130    86400       dhcp-snooping  1     FastEthernet0/1
00:0C:CF:72:DC:ED   192.168.0.132    86400       dhcp-snooping  1     FastEthernet0/2
00:03:E4:9A:81:E4   192.168.0.131    86400       dhcp-snooping  1     FastEthernet0/3
Total number of bindings: 3
S2#
```

Lab Task 3: Configuring OSPF Authentication

This task involves the configuration of authentication for OSPF updates among adjacent machines.

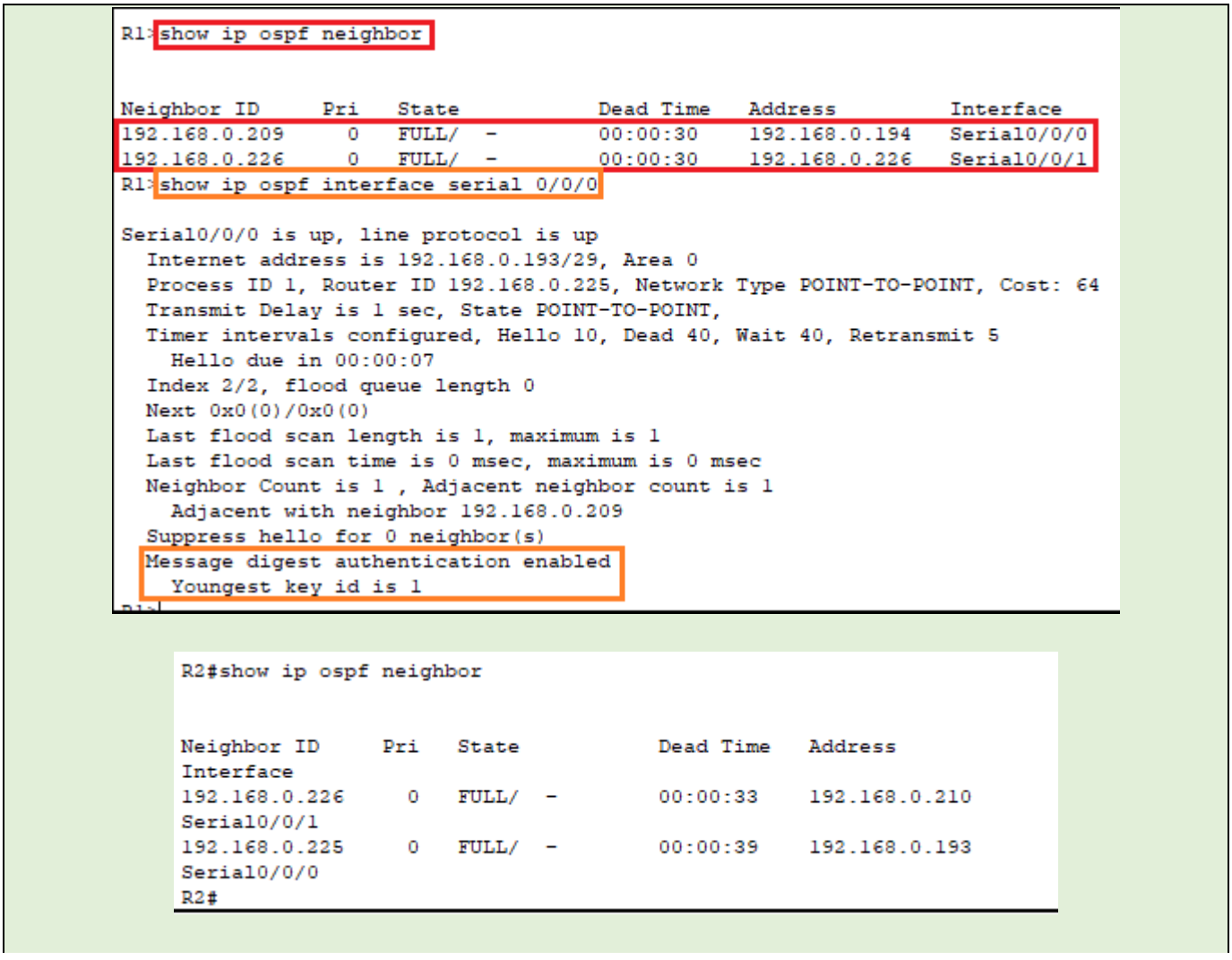
Note: Basic OSPF settings are already present on the router and should not be changed.

1 Configure OSPF MD5 authentication on the serial router interfaces of all three routers, using ***Panda*** as the pre-shared key.

```
R1:

R1>enable
R1#configure terminal
R1(config)#interface serial 0/0/0
R1(config-if)#ip ospf message-digest-key 1 md5 Panda
R1(config-if)#ip ospf authentication message
R1(config-if)#exit
R1(config)#interface serial 0/0/1
R1(config-if)#ip ospf message-digest-key 1 md5 Panda
R1(config-if)#ip ospf authentication message
R1(config-if)#exit

R2:

R2>enable
R2#configure terminal
R2(config)#interface serial 0/0/0
R2(config-if)#ip ospf message-digest-key 1 md5 Panda
R2(config-if)#ip ospf authentication message
R2(config-if)#exit
R2(config)#interface serial 0/0/1
R2(config-if)#ip ospf message-digest-key 1 md5 Panda
R2(config-if)#ip ospf authentication message
R2(config-if)#exit

R3:

R3>enable
R3#configure terminal
R3(config)#interface serial 0/0/0
R3(config-if)#ip ospf message-digest-key 1 md5 Panda
R3(config-if)#ip ospf authentication message
R3(config-if)#exit
R3(config)#interface serial 0/0/1
R3(config-if)#ip ospf message-digest-key 1 md5 Panda
R3(config-if)#ip ospf authentication message
R3(config-if)#exit
```

2 Display the OSPF neighbors table on each router to verify that the authentication process was successful. To verify that ID authentication is enabled, you can also use the ***show ip ospf interface <interface-id>*** command.

```
R1(config)#exit
R1#show ip ospf neighbor

R2(config)#exit
R2#show ip ospf neighbor

R3(config)#exit
R3#show ip ospf neighbor
```



```
R3#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address
Interface
192.168.0.209     0   FULL/  -        00:00:33    192.168.0.209
Serial0/0/1
192.168.0.225     0   FULL/  -        00:00:35    192.168.0.225
Serial0/0/0
R3#
```