

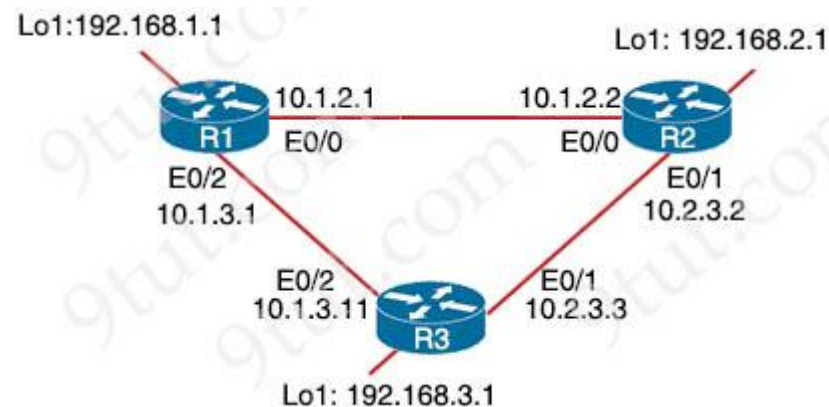
IP Services Sim

Guidelines

This is a lab item in which tasks will be performed on virtual devices.

- + Refer to the **Tasks** tab to view the tasks for this lab item.
- + Refer to the **Topology** tab to access the device console(s) and perform the tasks.
- + Console access is available for all required devices by clicking the device icon or using the tab(s) above the console window.
- + All necessary preconfigurations have been applied.
- + Do not change the enable password or hostname for any device.
- + **Save your configurations** to NVRAM before moving to the next item.
- + Click **Next** at the bottom of the screen to submit this lab and move to the next question.
- + When **Next** is clicked, the lab closes and cannot be reopened.

Topology



Tasks

Connectivity between three routers has been established, and IP services must be configured in the order presented to complete the implementation. Tasks assigned include configuration of NAT, NTP, DHCP, and SSH services.

1. All traffic sent from R3 to the R1 Loopback address must be configured for NAT on R2. All source addresses must be translated from R3 to the IP address of Ethernet0/0 on R2, while using only a standard access list named NAT. To verify, a ping must be successful to the R1 Loopback address sourced from R3. **Do not use NVI NAT configuration.**
2. Configure R1 as an NTP server and R2 as a client, not as a peer, using the IP address of the R1 Ethernet0/2 interface. Set the clock on the NTP server for midnight on January 1, 2019.
3. Configure R1 as a DHCP server for the network 10.1.3.0/24 in a pool named NETPOOL. Using a single command, exclude addresses 1-10 from the range. Interface Ethernet0/2 on R3 must be issued the IP address of 10.1.3.11 via DHCP.
4. Configure SSH connectivity from R1 to R3, while excluding access via other remote connection protocols. Access for user **netadmin** and password **N3t4ccess** must be set on

router R3 using RSA and 1024 bits. Verify connectivity using an SSH session from router R1 using a destination address of 10.1.3.11. **Do NOT modify console access or line numbers to accomplish this task.**

Solution

Please open Lab with Packet Tracer v8.1.1.0022 or newer. In Packet Tracer, there is one command that is slightly different. It is the command “crypto key generate rsa modulus 1024”. In Packet Tracer you have to type the command “crypto key generate rsa general-keys modulus 1024” instead. Packet Tracer does not support the “ntp source ...” command.

Note: Please check the ACL name username, password, clock... carefully in your exam as they may be different!

Task 1. All traffic sent from R3 to the R1 Loopback address must be configured for NAT on R2. All source addresses must be translated from R3 to the IP address of Ethernet0/0 on R2, while using only a standard access list named NAT. To verify, a ping must be successful to the R1 Loopback address sourced from R3. Do not use NVI NAT configuration.

```
R2(config)# ip access-list standard NAT //Note: The name of the ACL
may be different so please check carefully!
R2(config-std-nacl)#permit 10.2.3.3
R2(config-std-nacl)#permit 192.168.3.1
R2(config-std-nacl)#permit 10.1.3.11
R2(config-std-nacl)#exit
R2(config)# interface e0/1
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#interface e0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#ip nat inside source list NAT interface e0/0 overload
```

Verification

```
R3#ping 192.168.1.1
.!!!! (ping should work)
```

Task 2. Configure R1 as an NTP server and R2 as a client, not as a peer, using the IP address of the R1 Ethernet0/2 interface. Set the clock on the NTP server for midnight on January 1, 2019.

Configure R1 as an NTP server:

```
R1(config)#ntp master 1
R1(config)#ntp source E0/2
R1(config)#exit
```

When R1 sends an NTP packet, the source IP address is normally set to the address of the interface through which the NTP packet is sent so R2 will see E0/0 interface (IP 10.1.2.1) of R1 as the NTP source. Therefore we should use the "ntp source E0/2" command to change the NTP source to E0/2 interface as requested.

Midnight means 00:00:00. Note: The date may be different so please check carefully!

```
R1#clock set 00:00:00 January 1 2019
```

Configure R2 as the NTP client (not NTP peer):

```
R2#config t
R2(config)#ntp server 10.1.3.1
```

Verification

Check the clock on R2 to see if it is the same as R1:

```
R2#show clock
0:0:01.60 UTC Tue Jan 1 2019
```

Task 3. Configure R1 as a DHCP server for the network 10.1.3.0/24 in a pool named NETPOOL. Using a single command, exclude addresses 1-10 from the range. Interface Ethernet0/2 on R3 must be issued the IP address of 10.1.3.11 via DHCP.

```
R1(config)#ip dhcp pool NETPOOL
R1(dhcp-config)#network 10.1.3.0 255.255.255.0
R1(dhcp-config)#exit
R1(config)#ip dhcp excluded-address 10.1.3.1 10.1.3.10
```

Configure interface E0/2 of R3 to receive IP address issued from R1 (DHCP Server):

```
R3(config)#interface e0/2
R3(config-if)#ip address dhcp
```

Verification

Check to see if E0/2 interface has been assigned the IP address of 10.1.3.11 or not:

```
R3(config-if)#exit
```

```
R3(config)#exit
R3#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
...					
Ethernet0/2	10.1.3.11	YES	DHCP	up	up

Task 4. Configure SSH connectivity from R1 to R3, while excluding access via other remote connection protocols. Access for user **netadmin** and password **N3t4ccess** must be set on router R3 using RSA and 1024 bits. Verify connectivity using an SSH session from router R1 using a destination address of 10.1.3.11. **Do NOT modify console access or line numbers to accomplish this task.**

```
R3(config)#line vty 0 4 //we should use the "show run" command to
confirm if the "line vty 0 4" or "line vty 0 15"
R3(config-line)#transport input ssh
R3(config-line)#login local
R3(config-line)#exit
R3(config)#username netadmin password N3t4ccess //Note: Please check
the username and password given carefully. It may not be "netadmin"
and "N3t4ccess" as shown here
R3(config)#crypto key generate rsa modulus 1024
```

Note: The command "ip domain-name xyz.com" has been configured so we don't need to type this command again. This command must be used before the "crypto key generate rsa" command or an error will be shown.

Verification

```
R1# ssh -l netadmin 10.1.3.11
Password: {please type N3t4ccess here}
```

Save the configuration

As the guidelines clearly stated that we have to save the configuration to NVRAM so please save all your configurations on R1, R2 and R3:

```
R1#, R2#, R3#copy running-config startup-config
```

Note: Just for your information, this lab requires "Do not use NVI NAT configuration" so what is NVI NAT?

Cisco IOS Release 12.3(14)T introduced a feature called NAT Virtual Interface (NVI), which allows you to do a NAT configuration without the need to specify an interface as being an inside or an outside interface. Specifically, instead of issuing the "ip nat inside" or "ip nat

outside" command in interface configuration mode, you can issue the "ip nat enable" command. Not only does this feature make configuration easier , but it also allows traffic to flow between two interfaces that would both be considered inside interfaces, from a classic NAT perspective.

Reference: <https://www.oreilly.com/library/view/ccnp-routing-and/9780133149883/ch12lev3sec6.html>