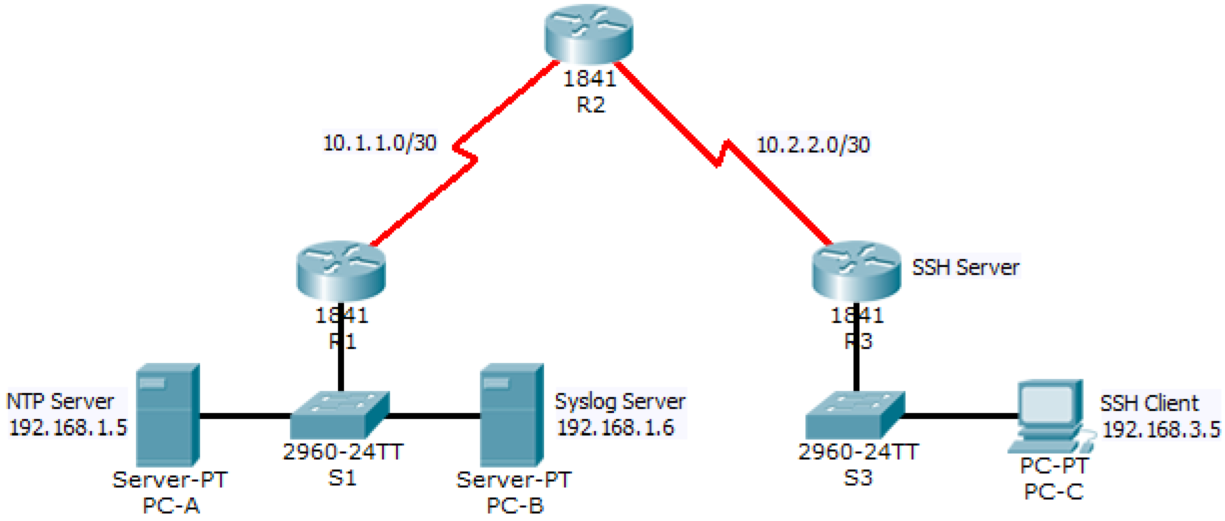
Packet Tracer - Configure Cisco Routers for Syslog, NTP, and SSH Operations (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	Fa0/1	192.168.1.1	255.255.255.0	N/A	S1 Fa0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	Fa0/1	192.168.3.1	255.255.255.0	N/A	S3 Fa0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.5	255.255.255.0	192.168.1.1	S1 Fa0/6
PC-B	NIC	192.168.1.6	255.255.255.0	192.168.1.1	S2 Fa0/18
PC-C	NIC	192.168.3.5	255.255.255.0	192.168.3.1	S3 Fa0/18

Objectives

- Configure routers as NTP clients.
- Configure routers to update the hardware clock using NTP.
- Configure routers to log messages to the syslog server.
- Configure routers to timestamp log messages.
- Configure local users.

- Configure VTY lines to accept SSH connections only.
- Configure RSA key pair on SSH server.
- Verify SSH connectivity from PC client and router client.

Background / Scenario

The network topology shows three routers. You will configure NTP and Syslog on all routers. You will configure SSH on R3.

Network Time Protocol (NTP) allows routers on the network to synchronize their time settings with an NTP server. A group of NTP clients that obtain time and date information from a single source have more consistent time settings and Syslog messages generated can be analyzed more easily. This can help when troubleshooting issues with network problems and attacks. When NTP is implemented in the network, it can be set up to synchronize to a private master clock, or to a publicly available NTP server on the Internet.

The NTP Server is the master NTP server in this lab. You will configure the routers to allow the software clock to be synchronized by NTP to the time server. Also, you will configure the routers to periodically update the hardware clock with the time learned from NTP. Otherwise, the hardware clock will tend to gradually lose or gain time (drift) and the software clock and hardware clock may become out of synchronization with each other.

The Syslog Server will provide message logging in this lab. You will configure the routers to identify the remote host (Syslog server) that will receive logging messages.

You will need to configure timestamp service for logging on the routers. Displaying the correct time and date in Syslog messages is vital when using Syslog to monitor a network. If the correct time and date of a message is not known, it can be difficult to determine what network event caused the message.

R2 is an ISP connected to two remote networks: R1 and R3. The local administrator at R3 can perform most router configurations and troubleshooting; however, because R3 is a managed router, the ISP needs access to R3 for occasional troubleshooting or updates. To provide this access in a secure manner, the administrators have agreed to use Secure Shell (SSH).

You use the CLI to configure the router to be managed securely using SSH instead of Telnet. SSH is a network protocol that establishes a secure terminal emulation connection to a router or other networking device. SSH encrypts all information that passes over the network link and provides authentication of the remote computer. SSH is rapidly replacing Telnet as the remote login tool of choice for network professionals.

The servers have been pre-configured for NTP and Syslog services respectively. NTP will not require authentication. The routers have been pre-configured with the following:

- Enable password: **ciscoenpa55**
- Password for vty lines: **ciscovtypa55**
- Static routing

Part 1: Configure Routers as NTP Clients

Step 1: Test Connectivity.

- Ping from **PC-C** to **R3**.
- Ping from **R2** to **R3**.
- Telnet from **PC-C** to **R3**. Exit the Telnet session.
- Telnet from **R2** to **R3**. Exit the Telnet session.

Step 2: Configure R1, R2, and R3 as NTP clients.

```
R1(config)# ntp server 192.168.1.5
R2(config)# ntp server 192.168.1.5
R3(config)# ntp server 192.168.1.5
```

Verify client configuration using the command **show ntp status**.

Step 3: Configure routers to update hardware clock.

Configure **R1**, **R2**, **and R3** to periodically update the hardware clock with the time learned from NTP.

```
R1(config)# ntp update-calendar
R2(config)# ntp update-calendar
R3(config)# ntp update-calendar
```

Verify that the hardware clock was updated using the command **show clock**.

Step 4: Configure routers to timestamp log messages.

Configure timestamp service for logging on the routers.

```
R1(config)# service timestamps log datetime msec
R2(config)# service timestamps log datetime msec
R3(config)# service timestamps log datetime msec
```

Part 2: Configure Routers to Log Messages to the Syslog Server

Step 1: Configure the routers to identify the remote host (Syslog Server) that will receive logging messages.

```
R1(config)# logging host 192.168.1.6
R2(config)# logging host 192.168.1.6
R3(config)# logging host 192.168.1.6
```

The router console will display a message that logging has started.

Step 2: Verify logging configuration using the command show logging.

Step 3: Examine logs of the Syslog Server.

From the **Services** tab of the **Syslog Server**’s dialogue box, select the **Syslog** services button. Observe the logging messages received from the routers.

Note: Log messages can be generated on the server by executing commands on the router. For example, entering and exiting global configuration mode will generate an informational configuration message.

Part 3: Configure R3 to Support SSH Connections

Step 1: Configure a domain name.

Configure a domain name of **ccnasecurity.com** on **R3**.

```
R3(config)# ip domain-name ccnasecurity.com
```

Step 2: Configure users for login to the SSH server on R3.

Create a user ID of **SSHadmin** with the highest possible privilege level and a secret password of **ciscosshpa55**.

```
R3(config)# username SSHadmin privilege 15 secret ciscosshpa55
```

Step 3: Configure the incoming VTY lines on R3.

Use the local user accounts for mandatory login and validation. Accept only SSH connections.

```
R3 (config)# line vty 0 4
R3 (config-line)# login local
R3(config-line)# transport input ssh
```

Step 4: Erase existing key pairs on R3.

Any existing RSA key pairs should be erased on the router.

```
R3(config)# crypto key zeroize rsa
```

Note: If no keys exist, you might receive this message: `% No Signature RSA Keys found in configuration`.

Step 5: Generate the RSA encryption key pair for R3.

The router uses the RSA key pair for authentication and encryption of transmitted SSH data. Configure the RSA keys with a modulus of **1024**. The default is 512, and the range is from 360 to 2048.

```
R3(config)# crypto key generate rsa
The name for the keys will be: R3.ccnasecurity.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

Note: The command to generate RSA encryption key pairs for **R3** in Packet Tracer differs from those used in the lab.

Step 6: Verify the SSH configuration.

Use the **show ip ssh** command to see the current settings. Verify that the authentication timeout and retries are at their default values of 120 and 3.

Step 7: Configure SSH timeouts and authentication parameters.

The default SSH timeouts and authentication parameters can be altered to be more restrictive. Set the timeout to **90** seconds, the number of authentication retries to **2**, and the version to **2**.

```
R3(config)# ip ssh time-out 90
R3(config)# ip ssh authentication-retries 2
R3(config)# ip ssh version 2
```

Issue the **show ip ssh** command again to confirm that the values have been changed.

Step 8: Attempt to connect to R3 via Telnet from PC-C.

Open the Desktop of **PC-C**. Select the Command Prompt icon. From **PC-C**, enter the command to connect to **R3** via Telnet.

```
PC> telnet 192.168.3.1
```

This connection should fail because **R3** has been configured to accept only SSH connections on the virtual terminal lines.

Step 9: Connect to R3 using SSH on PC-C.

Open the Desktop of **PC-C**. Select the Command Prompt icon. From **PC-C**, enter the command to connect to R3 via SSH. When prompted for the password, enter the password configured for the administrator **ciscosshpa55**.

```
PC> ssh –l SSHadmin 192.168.3.1
```

Step 10: Connect to R3 using SSH on R2.

In order to troubleshoot and maintain **R3**, the administrator at the ISP must use SSH to access the router CLI. From the CLI of **R2**, enter the command to connect to **R3** via SSH version **2** using the **SSHadmin** user account. When prompted for the password, enter the password configured for the administrator: **ciscosshpa55**.

```
R2# ssh –v 2 –l SSHadmin 10.2.2.1
```

Step 11: Check results.

Your completion percentage should be 100%. Click **Check Results** to view the feedback and verification of which required components have been completed.

!!!Scripts for R1 and R2!!!!

```
conf t
service timestamps log datetime msec
logging 192.168.1.6
ntp server 192.168.1.5
ntp update-calendar
end
```

!!!Scripts for R3!!!!

```
conf t
service timestamps log datetime msec
logging 192.168.1.6
ntp server 192.168.1.5
ntp update-calendar
ip domain-name ccnasecurity.com
username SSHadmin privilege 15 secret ciscosshpa55
 line vty 0 4
 login local
 transport input ssh
crypto key zeroize rsa
crypto key generate rsa
1024
ip ssh time-out 90
ip ssh authentication-retries 2
ip ssh version 2
end
```