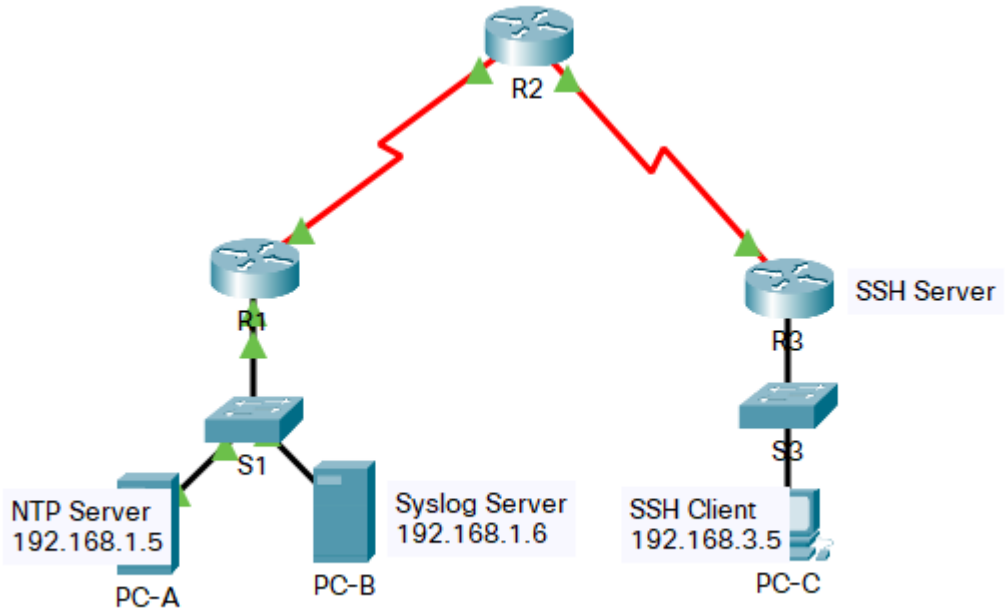
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»
ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ
Кафедра компьютерной инженерии и моделирования

Configure Cisco Routers for Syslog, NTP, and SSH Operations

Отчет по лабораторной работе № 12
по дисциплине «Компьютерные сети»
студента 2 курса группы ИВТ-б-о-202(1)
Шор Константина Александровича

Направления подготовки 09.03.01«Информатика и вычислительная техника»

Симферополь, 2022



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 FA0/6

Task 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.

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.3.1: bytes=32 time<1ms TTL=255
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>telnet 192.168.3.1
Trying 192.168.3.1 ...Open


User Access Verification

Password:
R3>exit

[Connection to 192.168.3.1 closed by foreign host]
C:\>
```

```
R2>ping 10.2.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/16/19 ms


R2>telnet 10.2.2.1
Trying 10.2.2.1 ...Open


User Access Verification

Password:
Password:
R3>exit

[Connection to 10.2.2.1 closed by foreign host]
R2>
```

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

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

```
R1>ena
Password:
R1#sh
R1#show ntp status
%NTP is not enabled.
R1#
R1(config)#ntp server 192.168.1.5
R1(config)#
```

```
R2(config)#ntp server 192.168.1.5
R2(config)#show ntp st
R2(config)#show ntp sta
R2(config)#end
R2#
*Mar 01, 00:15:38.1515: SYS-5-CONFIG_I: Configured from console by console
R2#show ntp st
R2#show ntp status
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1990)
clock offset is 0.00 msec, root delay is 0.00  msec
root dispersion is 0.00 msec, peer dispersion is 0.00 msec.
loopfilter state is 'FSET' (Drift set from file), drift is - 0.000001193 s/s system poll
interval is 4, never updated.
```

```
R3(config)#ntp server 192.168.1.5
R3(config)#end
R3#
*Mar 01, 00:18:23.1818: SYS-5-CONFIG_I: Configured from console by console
R3#sh
R3#show ntp ?
  associations  NTP associations
  status        NTP status
R3#show ntp st
R3#show ntp status
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1990)
clock offset is 0.00 msec, root delay is 0.00  msec
root dispersion is 0.00 msec, peer dispersion is 0.00 msec.
loopfilter state is 'FSET' (Drift set from file), drift is - 0.000001193 s/s system poll
interval is 4, never updated.
R3#
```

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.

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

```
R1(config)#ntp update-calendar
R1(config)#end
R1#
*Apr 08, 15:04:17.044: SYS-5-CONFIG_I: Configured from console by console
R1#sh
R1#show clo
R1#show clock
15:4:28.149 UTC Fri Apr 8 2022
```

```
R2(config)#ntp update-calendar
R2(config)#end
R2#
*Apr 08, 15:07:26.077: SYS-5-CONFIG_I: Configured from console by console
R2#sh clock
15:7:30.836 UTC Fri Apr 8 2022
```

```
R3(config)#ntp update-calendar
R3(config)#do sh clock
15:10:22.596 UTC Fri Apr 8 2022
R3(config)#
```

Task 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.

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

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

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

```
R1#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
          0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.


No Inactive Message Discriminator.


    Console logging: level debugging, 5 messages logged, xml disabled,
          filtering disabled
    Monitor logging: level debugging, 5 messages logged, xml disabled,
          filtering disabled
    Buffer logging:  disabled, xml disabled,
          filtering disabled

    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped
    Trap logging: level debugging, 5 message lines logged
        Logging to 192.168.1.6  (udp port 514,  audit disabled,
             authentication disabled, encryption disabled, link up),
             2 message lines logged,
             0 message lines rate-limited,
             0 message lines dropped-by-MD,
             xml disabled, sequence number disabled
             filtering disabled
R1#
```

```
R2#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
          0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.


No Inactive Message Discriminator.


    Console logging: level debugging, 6 messages logged, xml disabled,
          filtering disabled
    Monitor logging: level debugging, 6 messages logged, xml disabled,
          filtering disabled
    Buffer logging:  disabled, xml disabled,
          filtering disabled

    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped
    Trap logging: level debugging, 6 message lines logged
        Logging to 192.168.1.6  (udp port 514,  audit disabled,
              authentication disabled, encryption disabled, link up),
              2 message lines logged,
              0 message lines rate-limited,
              0 message lines dropped-by-MD,
              xml disabled, sequence number disabled
              filtering disabled
```

```
R3#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
          0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.


No Inactive Message Discriminator.


    Console logging: level debugging, 5 messages logged, xml disabled,
          filtering disabled
    Monitor logging: level debugging, 5 messages logged, xml disabled,
          filtering disabled
    Buffer logging:  disabled, xml disabled,
          filtering disabled

    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped
    Trap logging: level debugging, 5 message lines logged
        Logging to 192.168.1.6  (udp port 514,  audit disabled,
              authentication disabled, encryption disabled, link up),
              2 message lines logged,
              0 message lines rate-limited,
              0 message lines dropped-by-MD,
              xml disabled, sequence number disabled
              filtering disabled
```

Step 3. Examine logs of the Syslog server.

From the **Config** 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.

	Time	HostName	Message
1	03.01.1993 01:11:33.808 AM	10.1.1.2	%SYS-5-CONFIG_I: Configured from ...
2	03.01.1993 01:11:33.808 AM	10.1.1.2	: %SYS-6-LOGGINGHOST_ST...
3	03.01.1993 01:12:28.825 AM	10.2.2.1	%SYS-5-CONFIG_I: Configured from ...
4	03.01.1993 01:12:28.825 AM	10.2.2.1	: %SYS-6-LOGGINGHOST_ST...

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
```

Task 3: Configure R3 to support SSH connections.

Step 1. Configure a domain name.

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

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

Step 2. Configure users for login from the SSH client on R3.

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

Step 3. Configure the incoming VTY lines on R3.

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

```
LINE  The UNENCRYPTED (cleartext) user secret
R3(config)#username SSHadmin privilege 15 secret ciscosshpa55
R3(config)#username SSHadmin privilege 15 secret ciscosshpa55
R3(config)#line vty 0 4
R3(config-line)#login local
R3(config-line)#tra
R3(config-line)#transport input
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.

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

```
R3(config)#crypto key zeroize rsa
% 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 [Enter]
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.

```
R3(config)#crypto key ?
  generate  Generate new keys
  zeroize   Remove keys
R3(config)#crypto key ge
R3(config)#crypto key generate ?
  rsa  Generate RSA keys
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]
```

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.

```
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 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**.

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

```
% Unrecognized command
R3(config)#ip ssh time-out ?
  <1-120>  SSH time-out interval (secs)
R3(config)#ip ssh time-out 90
Enter configuration commands, one per line.  End
R3(config)#ip ssh aiu
R3(config)#ip ssh aou
R3(config)#ip ssh auth
R3(config)#ip ssh authentication-retries 2
R3(config)#ip ssh ver 2
R3(config)#ip ssh ver
R3(config)#ip ssh version 2
R3(config)#
```

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, since R3 has been configured to accept only SSH connections on the virtual terminal lines.

```
Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.3.1
Trying 192.168.3.1 ...Open

[Connection to 192.168.3.1 closed by foreign host]
C:\>
```

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**.

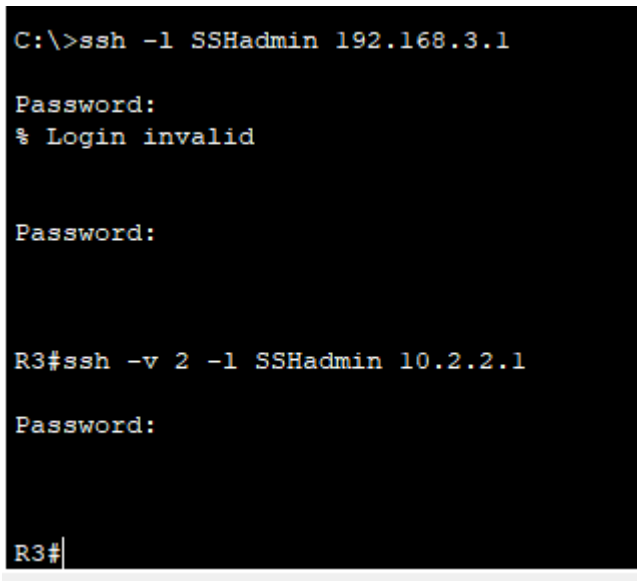
```
PC> ssh -l SSHadmin 192.168.3.1
```

```
Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.3.1
Trying 192.168.3.1 ...Open

[Connection to 192.168.3.1 closed by foreign host]
C:\>ssh -l SSHadmin 192.168.3.1

Password:



R3#
```

Step 10. Connect to R3 using SSH on R2.

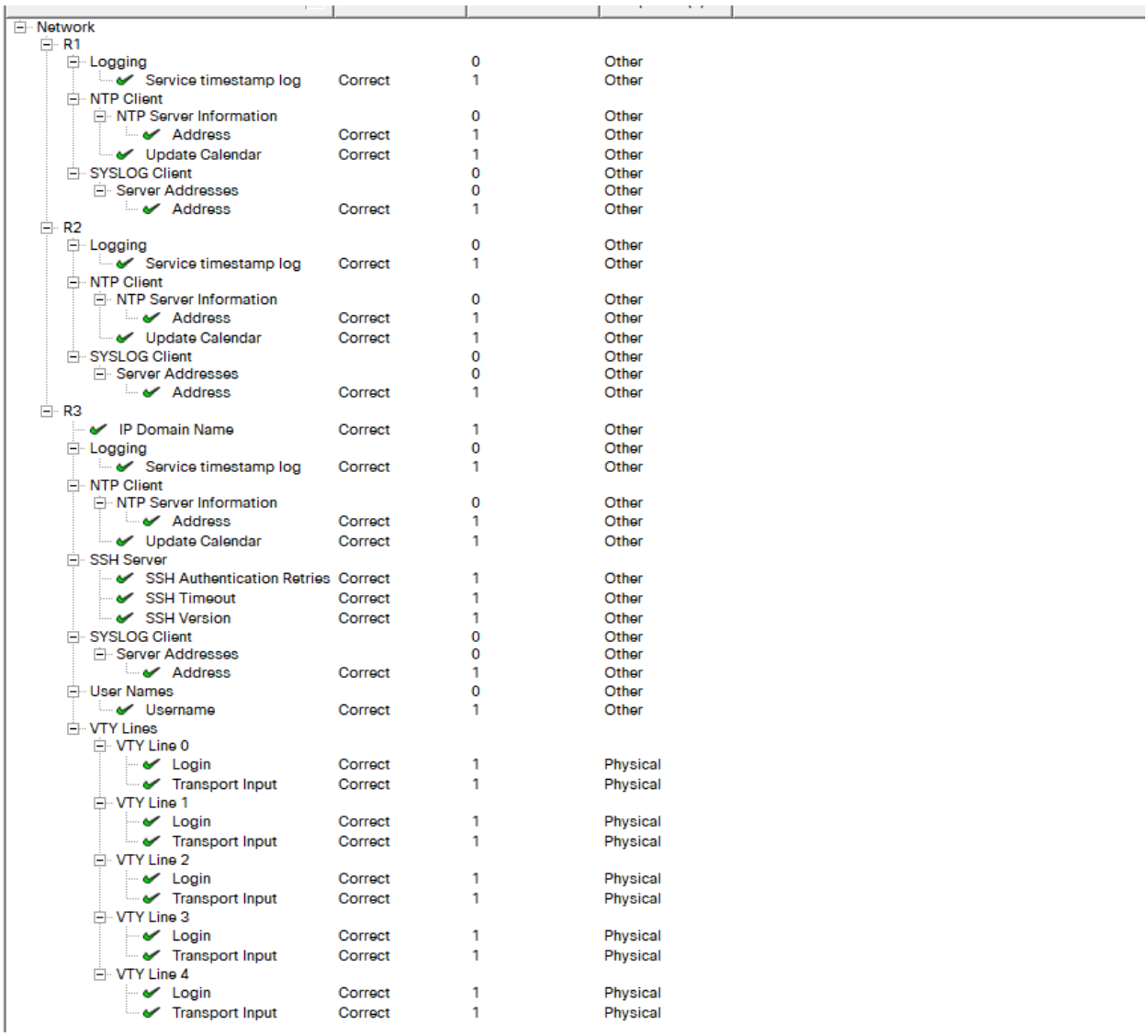
In order to troubleshoot and maintain the R3 router, the administrator at the ISP must use SSH to access the router CLI. From the CLI of R2, enter the command to connect to R3 via SSH version 2 using the SSHadmin user account. When prompted for the password, enter the password configured for the administrator: **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 see feedback and verification of which required components have been completed.



Network			
R1			
Logging		0	Other
Service timestamp log	Correct	1	Other
NTP Client			
NTP Server Information		0	Other
Address	Correct	1	Other
Update Calendar	Correct	1	Other
SYSLOG Client		0	Other
Server Addresses		0	Other
Address	Correct	1	Other
R2			
Logging		0	Other
Service timestamp log	Correct	1	Other
NTP Client			
NTP Server Information		0	Other
Address	Correct	1	Other
Update Calendar	Correct	1	Other
SYSLOG Client		0	Other
Server Addresses		0	Other
Address	Correct	1	Other
R3			
IP Domain Name	Correct	1	Other
Logging		0	Other
Service timestamp log	Correct	1	Other
NTP Client			
NTP Server Information		0	Other
Address	Correct	1	Other
Update Calendar	Correct	1	Other
SSH Server			
SSH Authentication Retries	Correct	1	Other
SSH Timeout	Correct	1	Other
SSH Version	Correct	1	Other
SYSLOG Client		0	Other
Server Addresses		0	Other
Address	Correct	1	Other
User Names		0	Other
Username	Correct	1	Other
VTY Lines			
VTY Line 0			
Login	Correct	1	Physical
Transport Input	Correct	1	Physical
VTY Line 1			
Login	Correct	1	Physical
Transport Input	Correct	1	Physical
VTY Line 2			
Login	Correct	1	Physical
Transport Input	Correct	1	Physical
VTY Line 3			
Login	Correct	1	Physical
Transport Input	Correct	1	Physical
VTY Line 4			
Login	Correct	1	Physical
Transport Input	Correct	1	Physical