**Logo

Description automatically generated**

*Independent University Bangladesh (IUB)* **Course ID: CSE316L  
Semester:  Summer 2021  
Section: 04  
  
  
Submitted To:  
Instructor:** **Dr. Mst. Najnin  
  
Submitted By:  
Name: Md. Ashikur Rahman  
ID: 1831110  
  
Lab Report 3**

**Working Date:  13th August 2021  
                                      Submission Date: 15th August 2021**

**EXPERIMENT** **03:** Initial Router Configurations

**Objective:**

1. Enable Remote login for the router with TELNET/SSH
2. Remote login to a router from workstation

**Tools and Materials:**

**In a real-life Scenario:**

Workstation with terminal Program (such as putty), Cisco router, rollover cable, cross-over RJ45 cable

# For Lab Purpose:

Cisco Packet Tracer Software

**Instructions:**

**Connect Router1 and Router2 using cable and access router CLI from the Workstation terminal emulator software:**

We need to configure loopback addresses of two routers and then use telnet and SSH (secure shell) to remote log in in Router, from one router to another router.

This experiment shows how to connect it using the Cisco simulator software Packet Tracer.

Shape

Description automatically generated

Click OK to accept the default settings and the router CLI will appear. Just hit ENTER in your keyboard and you will get to the user mode (Router>).

The default settings in that small screen represent what you would set in a third-party software to connect to the router. Windows can use open source terminal emulator software Putty. In the Putty you would set a connection use the same settings of that small screen

**Configure Router using initial setup:**

Continue with configuration dialog? [yes/no]: **no**

A good Network Administrator will never use initial configuration mode. It is far too time consuming and is unlikely to produce the configuration you need.

Router> **enable**

Enters router enable mode

# Loopback address set up: Instruction

* 1. **Set the ip addresses of physical interfaces connecting the two routers as follows:**

**R1: 192.168.1.1/24 R2: 192.168.1.2/24**

* 1. **Create a loopback interface on each router: R1: 1.1.1.1/32**

**R2: 2.2.2.2/32**

* 1. **From each Router, attempt to ping both the local loopback interface and the loopback interface of remote router**

First we need to set up ip address in the interfaces, both Routers are connected with f0/0 interface.

R1:

Router>enable Router#config t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname R1

R1(config)#interface fa 0/0

R1(config-if)#ip address 192.168.1.1 255.255.255.0 R1(config-if)#no shut down

Router(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

R2:

Router>enable Router#config t

Enter configuration commands, one per line. End with CNTL/Z. Router(config)#hostname R2

R2(config)#interface f0/0

R2(config-if)#ip address 192.168.1.2 255.255.255.0 R2(config-if)#no shutdown

R2(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

# Ping R1 from R2:

R2(config-if)#do ping 192.168.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 0/16/64 ms

R2(config-if)#

# Loopback ip address set up:

R1:

R1(config)#interface loopback 0

R1(config-if)#

%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R1(config-if)#ip address 1.1.1.1 255.255.255.255 R1(config-if)#

R2:

R2>enable R2#config t

Enter configuration commands, one per line. End with CNTL/Z. R2(config)#int lo

% Incomplete command. R2(config)#interface loopback 0

R2(config-if)#

%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R2(config-if)#ip address 2.2.2.2 255.255.255.255 R2(config-if)#end

R2#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR P - periodic downloaded static route

Gateway of last resort is not set

# /32 is submitted, 1 subnets

**C 2.2.2.2 is directly connected, Loopback0**

**C 192.168.1.0/24 is directly connected, FastEthernet0/0 [no information regarding 1.1.1.1]**

R2#

R2#ping 2.2.2.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/10 ms

# Remote login with Telnet and SSH:

CSE316# **configure terminal**

Privileged EXEC command to enter global configuration mode. You are in global configuration mode when the prompt changes to Router(config)#.

CSE316(config)# **line vty** *0 15*

Giving range of vty(virtual terminal line) from 0 to 15 (means all 16 lines) CSE316(config- line)# **login** *local*

Use local usename and password. Alternatively authenticate using aaa method list can be used

CSE316(config-line)# **transport input** *all*

Both Telnet and SSH can be used to remotely log into the router

**Ctrl+C /** CSE316(config-line)# **end** Return back to router enable mode Alternate Way:

CSE316(config)#line con 0

CSE316(config-line)#line vty 0 4

CSE316(config-line)#line aux 0 CSE316(config-line)#login

% Login disabled on line 0, until 'password' is set CSE316(config-line)#line vty 0 4 CSE316(config-line)#password cisco CSE316(config-line)#login

CSE316(config-line)#end CSE316#

%SYS-5-CONFIG\_I: Configured from console by console CSE316#write

Building configuration... [OK]

From another Router, say R2, R2#telnet 1.1.1.1

Trying 1.1.1.1 …open User access verification Password: [type cisco] CSE316>

[remote log in complete with telnet] CSE316>enable

CSE316#config t

Enter configuration commands, one per line. End with CNTL/Z. CSE316(config)#username cisco password cisco CSE316(config)#do sh run

Building configuration... CSE316(config)#line vty 0 4 CSE316(config-line)#no password cisco CSE316(config-line)#login local CSE316(config-line)#

[use local database. Configure username and password. From other router, access CSE316 router, here R2]

From R2:

R2#telnet 1.1.1.1

Trying 1.1.1.1 … open User access verification Username: cisco Password: [type cisco]

CSE316>exit

[connection to 1.1.1.1 closed by foreign host]

**SSH Connectivity:**

For SSH, we should configure domain-name. Then we need to generate key. Without domain name problem.

Domain name in remote router, here CSE316, where to access remotely

/

CSE316(config)# **no ip domain-lookup**

Disables DNS lookup function

CSE316(config)# **ip domain-name** *CSE316.cisco.com* Specifies the DNS domain name CSE316(config)# **username** *student* **secret** *cse*

Create user and assign password. The Clear Text Password is MD5 Encrypted

CSE316(config)# **crypto key generate rsa**

To generate Rivest,Shamir, and Adelman (RSA) key pairs, use the crypto key generate rsa command in global configuration mode

Practice:

CSE316(config)#crypto key generate rsa

The name for the keys will be: CSE316.CSE316.cisco.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]

CSE316(config)#

CSE316(config)#ip ssh ?

\*Jun 22 18:24:9.884: %SSH-5-ENABLED: SSH 1.99 has been enabled authentication-retries Specify number of authentication retries

time-out Specify SSH time-out interval

version Specify protocol version to be supported CSE316(config)#ip ssh version 2

CSE316(config)#line vty 0 4 [configure 5 virtual terminal lines] CSE316(config-line)#transport input ?

all All protocols none No protocols

ssh TCP/IP SSH protocol telnet TCP/IP Telnet protocol

CSE316(config-line)#transport input all CSE316(config-line)#

From R2: [Access CSE316 from R2]

R2#telnet 1.1.1.1 Trying 1.1.1.1 … Open

User Access Verification Username: cisco Password:

CSE316>exit R2# ssh 1.1.1.1

%no user specified, not available R2# ssh –l cisco 1.1.1.1 Password:

CSE316>exit

**New Approach:**

Graphical user interface, text, application, chat or text message

Description automatically generated

IP set up in Switch: no direct ip in switch, we use vlan 1 for setting IP address. Switch>;enable

Switch#config t

Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#int vlan 1

Switch(config-if)#ip address 192.168.1.2 255.255.255.0 Switch(config-if)#no shutdown

Switch(config-if)#

%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up IP address in Router:

Router>enable Router#config t

Enter configuration commands, one per line. End with CNTL/Z. Router(config)#int fa 0/0

Router(config-if)#ip address 192.168.1.1 255.255.255.0 Router(config-if)#no shutdown

Router(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

User creation in Router and Switch: Router(config-if)#exit

Router(config)#username akram password 1234 Router(config)#

Switch(config)#username akram password 1234 Switch(config)#

telnet set up: Switch(config)#line vty 0 15

Switch(config-line)#login local Switch(config-line)#transport input? input

Switch(config-line)#transport input

% Incomplete command. Switch(config-line)#transport input ? all All protocols

none No protocols

ssh TCP/IP SSH protocol telnet TCP/IP Telnet protocol

Switch(config-line)#transport input

% Incomplete command.

Switch(config-line)#transport input telnet telnet configure in Router: Router(config)#line vty 0 15 Router(config-line)#login local Router(config-line)#transport input telnet Router(config-line)#

From PC Telnet:

At first IP Configuration in PC.

IP: 192.168.1.11/24

Graphical user interface, text, application

Description automatically generated

From Command Prompt

PC>telnet 192.168.1.2

Trying 192.168.1.2 ...Open

User Access Verification Switch>exit

PC>telnet 192.168.1.1

Trying 192.168.1.1 ...Open User Access Verification

Username: cisco Password:

Router> Username: akram Password:

Switch>

SSH Connectivity:

Four Steps:

* + - * 1. Configure the hostname for the devices
        2. Must configure the DNS domain name
        3. Must generate the key for encrypt the message
        4. Must enable vty lines

**Step 1 Hostname for Switch and Router**:

Switch>enable Switch#config t

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hostname sw1 sw1(config)#

Router>enable Router#config t

Enter configuration commands, one per line. End with CNTL/Z. Router(config)#hostname R1

R1(config)#

# Step 2 IP address set up:

R1(config)#int fa0/0

R1(config-if)#ip address 192.168.1.1 255.255.255.0 R1(config-if)#no shutdown

R1(config-if)#

sw1(config)#int vlan 1

sw1(config-if)#ip address 192.168.1.2 255.255.255.0 sw1(config-if)#no shutdown

sw1(config-if)#

**step 3 User Creation for login:**

sw1(config-if)#exit

sw1(config)#username cisco password CCNA

sw1(config)#

[We should remember passwords are case sensitive)

R1(config-if)#exit

R1(config)#username cisco password CCNA R1(config)#

**Step 4: DNS domain name set up** R1(config)#ip domain-name cisco.com R1(config)#

sw1(config)#ip domain-name cisco.com sw1(config)#

Step 5: Generate the key for encryption sw1(config)#crypto key generate rsa

The name for the keys will be: sw1.cisco.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]

# [key length for encryption and decryption, default value 1024]

sw1(config)#

R1(config)#ip domain-name cisco.com R1(config)#crypto key generate rsa

The name for the keys will be: R1.cisco.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: configure the vty line

R1(config)#line vty 0 15

\*Mar 1 0:24:29.903: %SSH-5-ENABLED: SSH 1.99 has been enabled R1(config-line)#login local

R1(config-line)#transport input ssh R1(config-line)#exec-timeout 5

[after 5 minutes no activity, line disconnection. Time input by default in minute ] R1(config-line)#

sw1(config)#line vty 0 15

\*Mar 1 0:22:5.514: %SSH-5-ENABLED: SSH 1.99 has been enabled sw1(config-line)#login local

sw1(config-line)#transport input ssh sw1(config-line)#exec-timeout 5 sw1(config-line)#

**Step 7: Enable SSH version 2** sw1(config-line)#exit sw1(config)#ip ssh version 2 sw1(config)#

R1(config-line)#exit R1(config)#ip ssh version 2 R1(config)#

Step 8: Already in PC (Workstation), IP address set up completed

Packet Tracer PC Command Line 1.0 PC>telnet 192.168.1.2

Trying 192.168.1.2 ...Open

[Connection to 192.168.1.2 closed by foreign host]

PC>

Now, telnet doesn’t work. Write this command

PC>ssh -l cisco 192.168.1.2 [username akram] Open

Password: [password 1234] sw1>

nw for R1:

sw1>exit

[Connection to 192.168.1.2 closed by foreign host] PC>ssh -l cisco 192.168.1.1 [username akram] Open

Password: [ password 1234] R1>

R1>exit