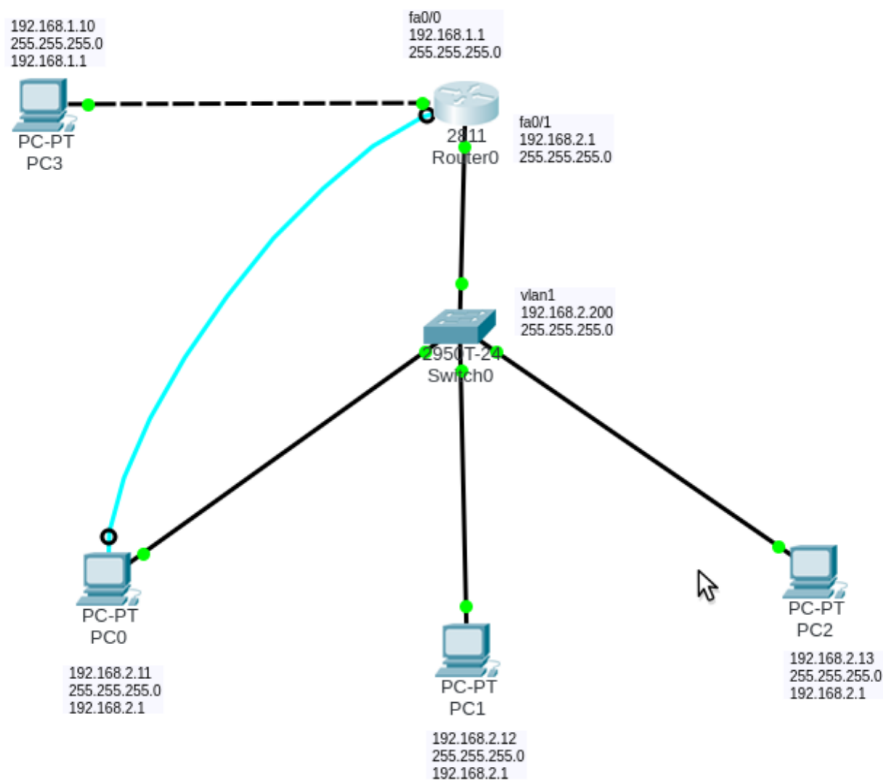**Name:** Sudip Basu
Department : CST
Roll: 16
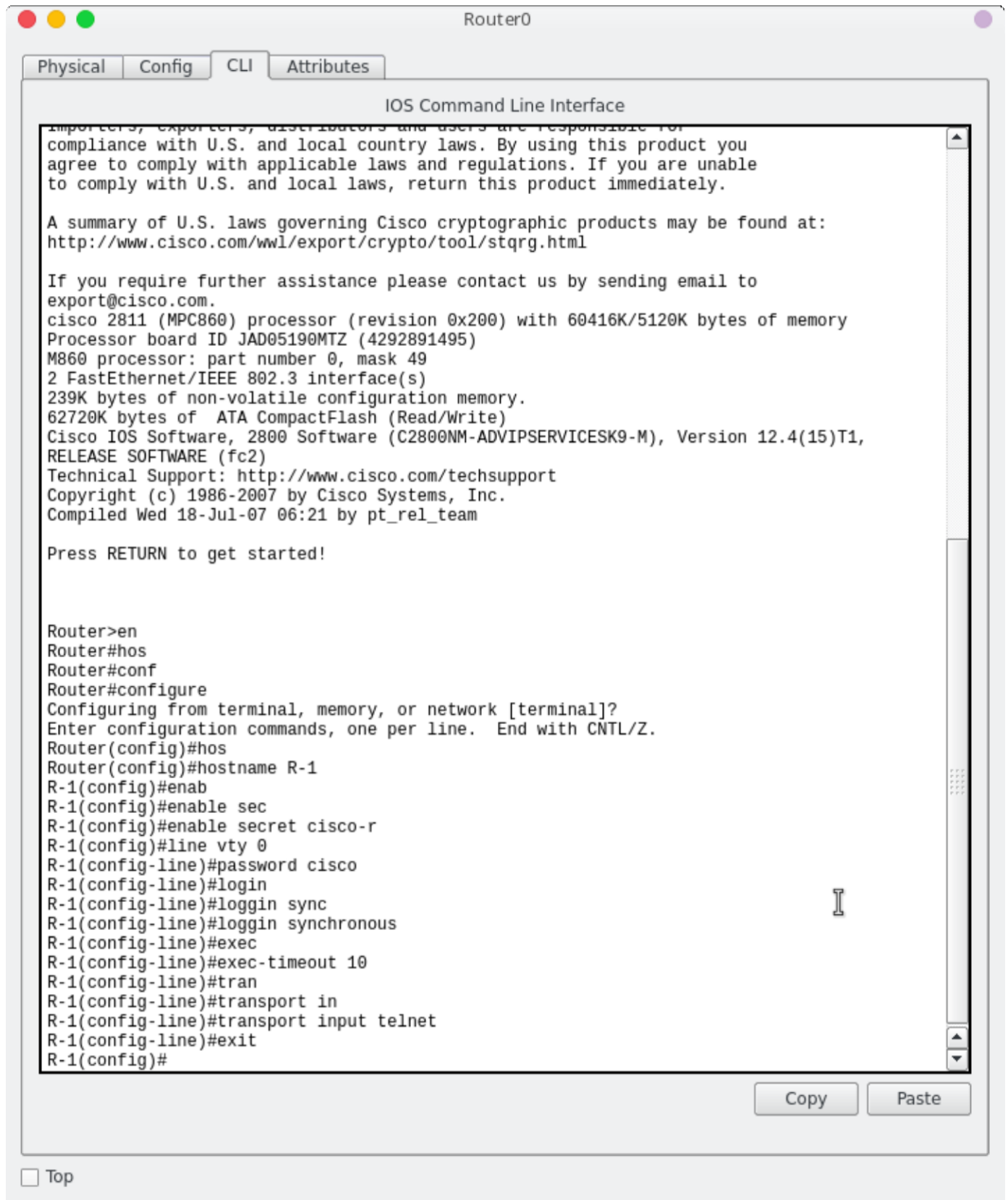**Semester:** 4th

COMPUTER NETWORK
ASSIGNMENT

Configure Telnet and SSH on Cisco Packet Tracer

To enable telnet or SSH on Cisco router, simply do it with "line vty" command. lets Configure:

- **First create topology Network. and set a static IP for PC client, router and switch. See the picture below.**

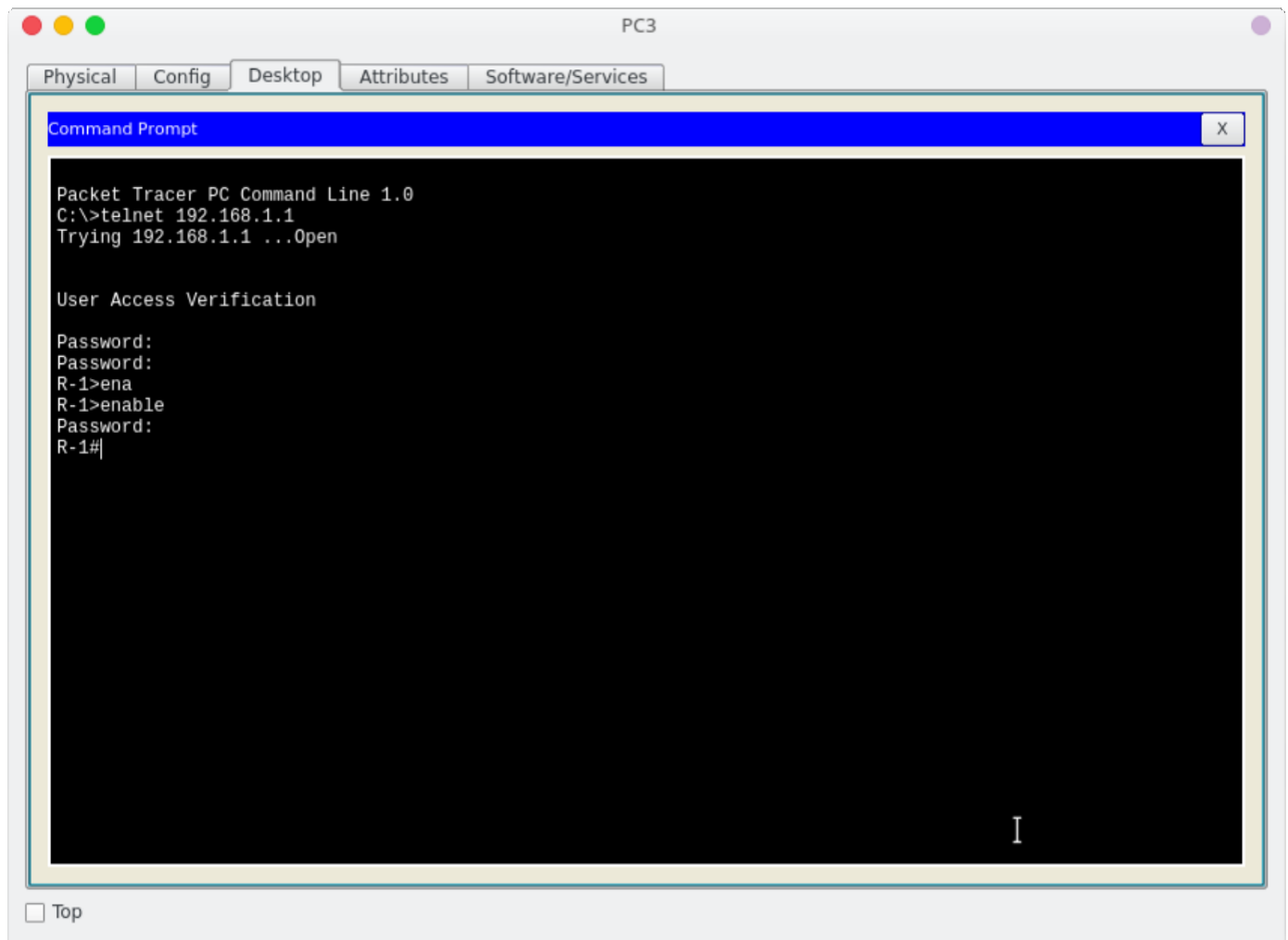- **Go to Router0 console and configure Hostname, Secret password and telnet with "line vty" command.**

Router0 — IOS Command Line Interface

```
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
239K bytes of non-volatile configuration memory.
62720K bytes of  ATA CompactFlash (Read/Write)
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(15)T1,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 06:21 by pt_rel_team

Press RETURN to get started!



Router>en
Router#hos
Router#conf
Router#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hos
Router(config)#hostname R-1
R-1(config)#enab
R-1(config)#enable sec
R-1(config)#enable secret cisco-r
R-1(config)#line vty 0
R-1(config-line)#password cisco
R-1(config-line)#login
R-1(config-line)#loggin sync
R-1(config-line)#loggin synchronous
R-1(config-line)#exec
R-1(config-line)#exec-timeout 10
R-1(config-line)#tran
R-1(config-line)#transport in
R-1(config-line)#transport input telnet
R-1(config-line)#exit
R-1(config)#
```

- "Enable secret 'your password'" command for your router password user privileges.
- The "line vty" command enable the telnet and the "0" is just let a single line or session to the router. If you need more session simultaneously, you must type "line vty 0 10", its mean 11 client can access telnet.
- The "logging synchronous" command stops any message output from splitting your typing.

- The "exec-timeout" command just sets the time-out limit on the line from the default to "10″ minutes.

- **Testing Telnet Connectivity.**

   Let's test telnet from the admin or client PC. Type telnet 192.168.1.1 and press enter, then enter the telnet username & password. Next type enable command and press enter, then type the router password.

```
Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open


User Access Verification

Password:
Password:
R-1>ena
R-1>enable
Password:
R-1#
```

- Now you are remotely connected to router R1 and you can execute all router commands through telnet command line interface.
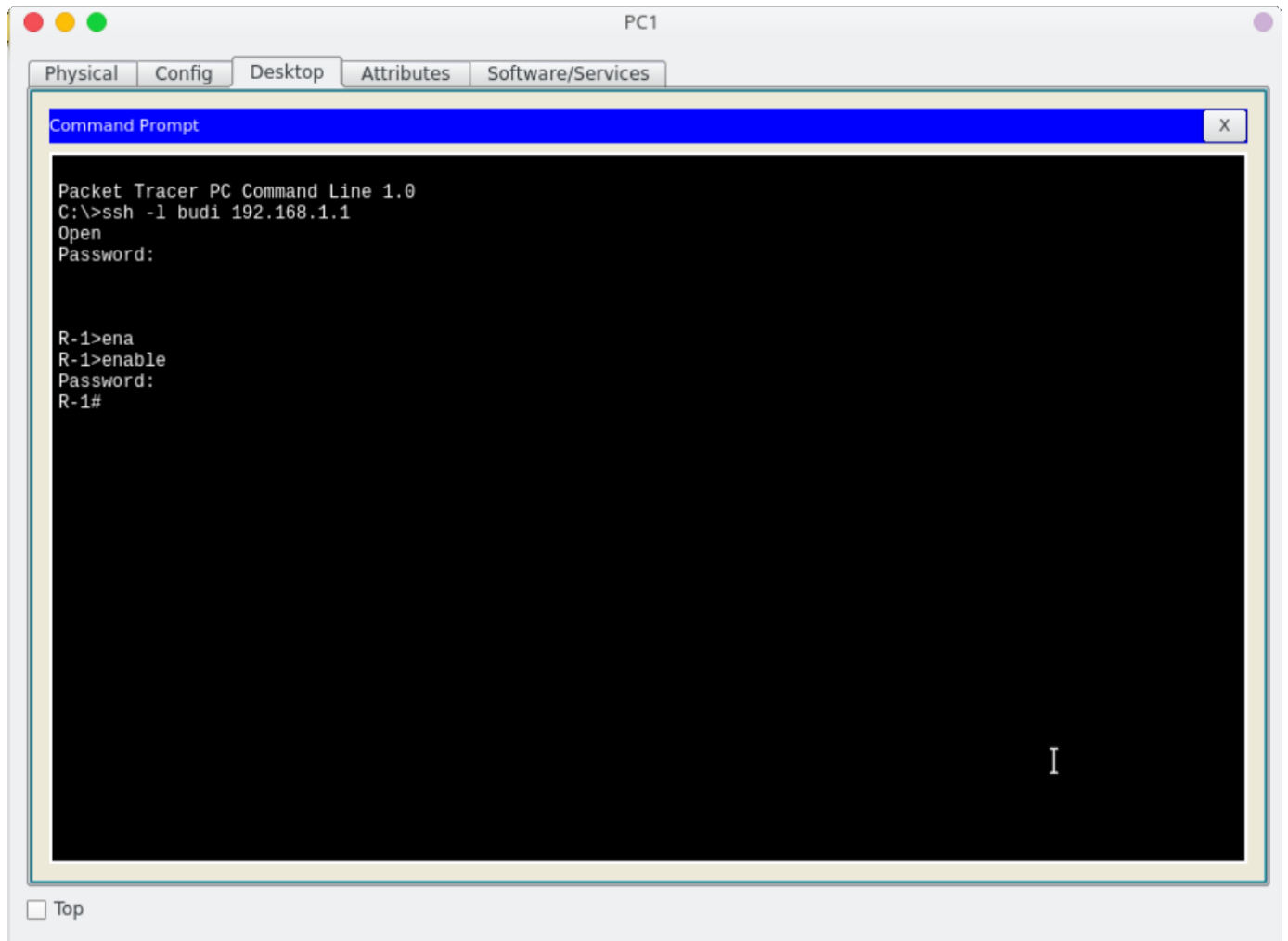
- **SSH Configuration.**

```
                                    Router0

 Physical    Config    CLI    Attributes

                          IOS Command Line Interface

  R-1>en
  Password:
  R-1#conf t
  Enter configuration commands, one per line.  End with CNTL/Z.
  R-1(config)#ip domain name budiluhur.ac.id
  R-1(config)#username budi password luhur
  R-1(config)#cypto
  R-1(config)#cypto key gene
  R-1(config)#cyr
  R-1(config)#cr
  R-1(config)#crypto key gene
  R-1(config)#crypto key generate rsa
  The name for the keys will be: R-1.budiluhur.ac.id
  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]

  R-1(config)#ip ssh versi
  *Mar 1 0:24:25.504:  %SSH-5-ENABLED: SSH 1.99 has been enabled
  R-1(config)#ip ssh version 2
  R-1(config)#line vty 1 3
  R-1(config-line)#transpo
  R-1(config-line)#transport in
  R-1(config-line)#transport input ssh
  R-1(config-line)#login local
  R-1(config-line)#login syn
  R-1(config-line)#login sync
  R-1(config-line)#loggin
  R-1(config-line)#logging syn
  R-1(config-line)#logging synchronous
  R-1(config-line)#exit
  R-1(config)#service
  R-1(config)#service pas
  R-1(config)#service password-encryption
  R-1(config)#

                                               Copy        Paste

 □ Top
```

- "line vte 1 3" <~ this command will set only line 1 to 3 Virtual Teminal Lines can access SSH.
- "username budi password luhur" <~ this your username and password for SSH access.
- "crypto key generate rsa" command, when ask you "How many bits in the modulus [512]:" just type "1024" and press enter. The system will generate 1024 bits keys to secure session lines. You can choose modulus in the range of 360 to 2048.

- service password-encryption <~ encrypt your SSH password.

- **Testing SSH Connectivity**

  From a client PC, open the command line and type "ssh -l budi 192.168.1.1" then press enter.

PC1

| Physical | Config | Desktop | Attributes | Software/Services |

Command Prompt   X

```
Packet Tracer PC Command Line 1.0
C:\>ssh -l budi 192.168.1.1
Open
Password:


R-1>ena
R-1>enable
Password:
R-1#
```

☐ Top

Now we have connected successfully and the connection is secured with Secure Shell.