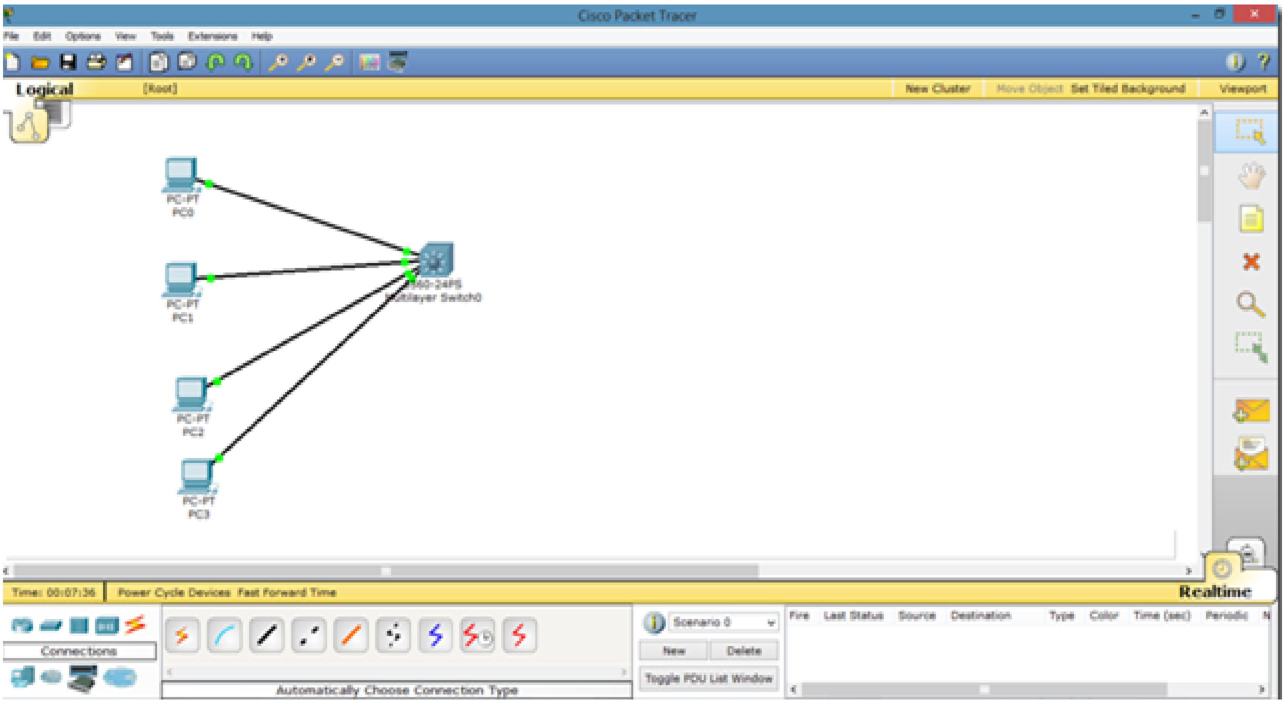
NATIONAL UNIVERSITY OF COMPUTER & EMERGING SCIENCE
Computer Networks Lab (CL307)
Lab Session 05

Application Layer Protocol

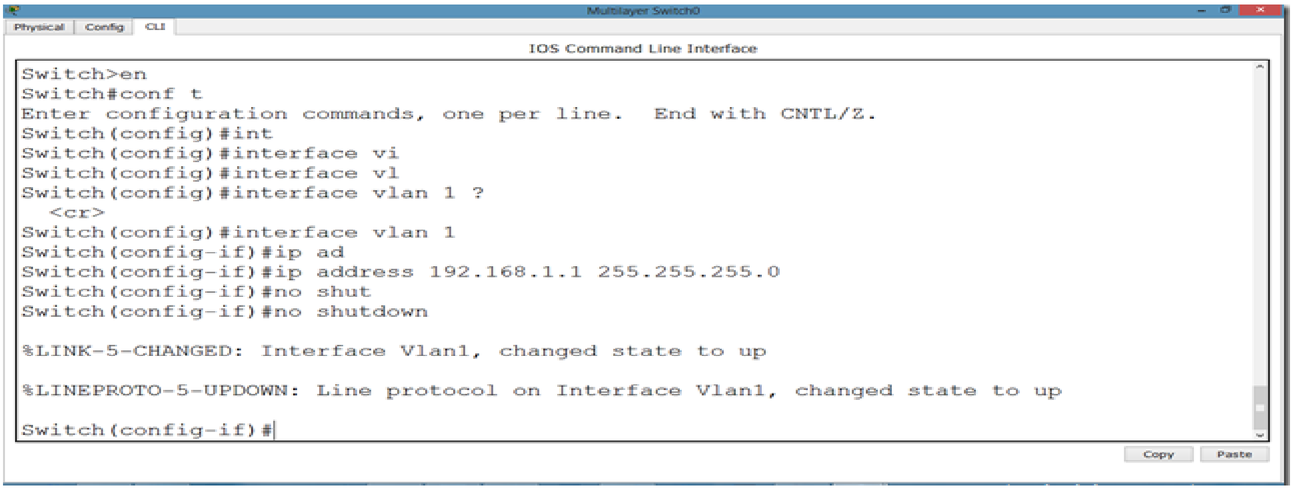
TELNET

A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers. To telnet means to establish a connection with the Telnet protocol, either with command line client or with a programmatic interface.

Let us apply Telnet on packet tracer.

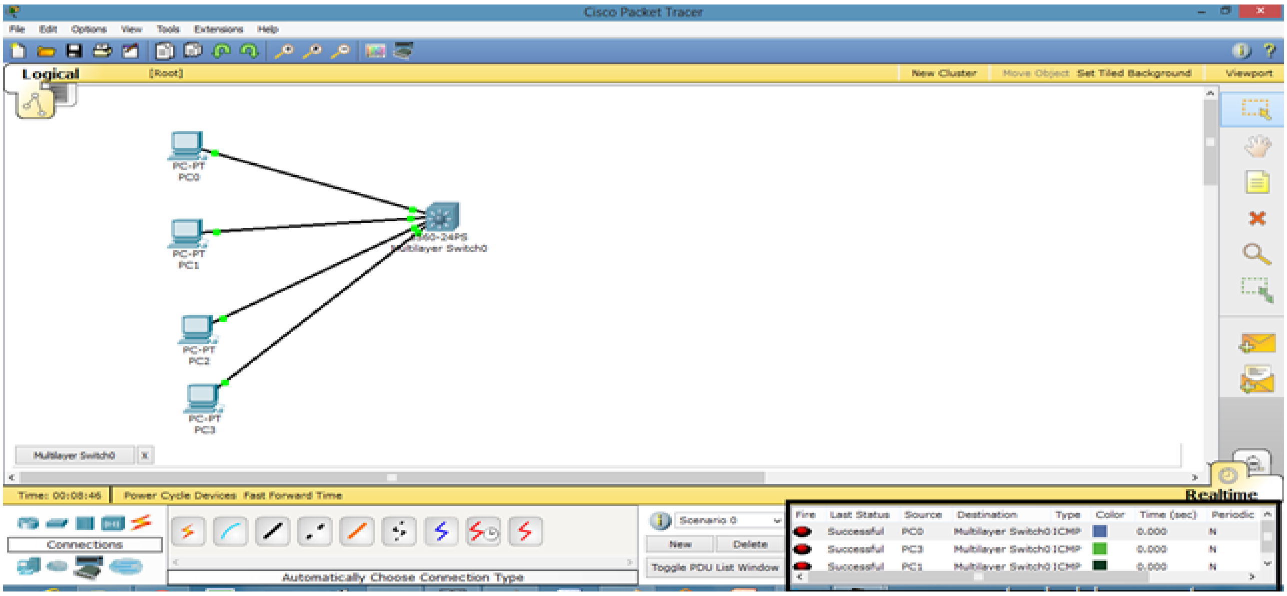


Take the topology as in the above diagram. Set IPs on the PCs. As, by default, all PCs are in vlan 1. We will create a virtual interface on switch with vlan 1 as follows.



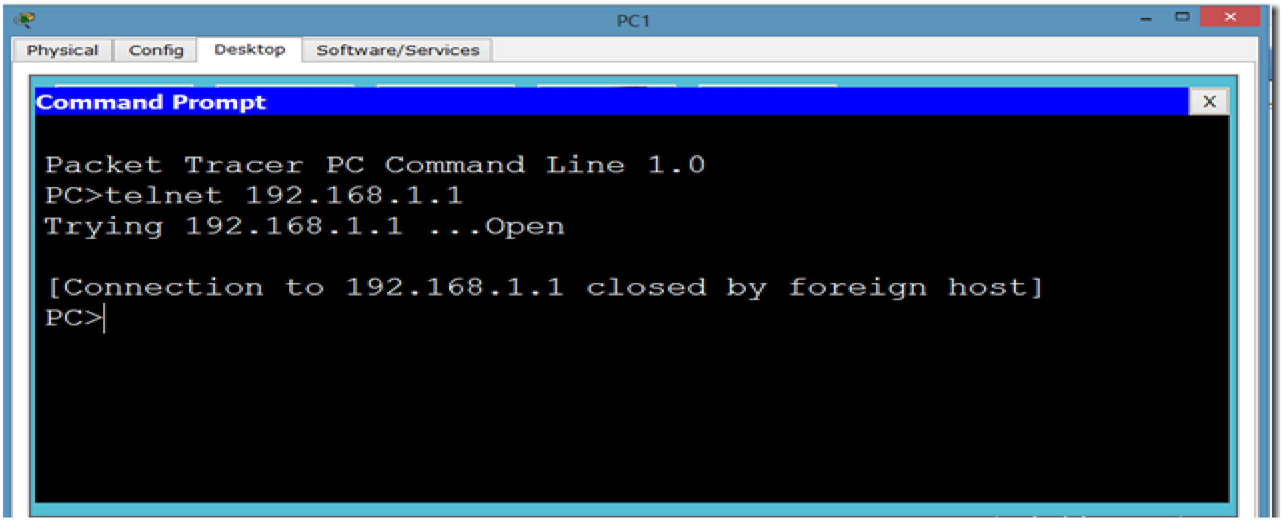
```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int
Switch(config)#interface vi
Switch(config)#interface vl
Switch(config)#interface vlan 1 ?
  <cr>
Switch(config)#interface vlan 1
Switch(config-if)#ip ad
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#no shutdown

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

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

Switch(config-if)#
```

Now, we can ping to switch by our hosts because hosts are in vlan 1 and switch also has a vlan 1 interface.



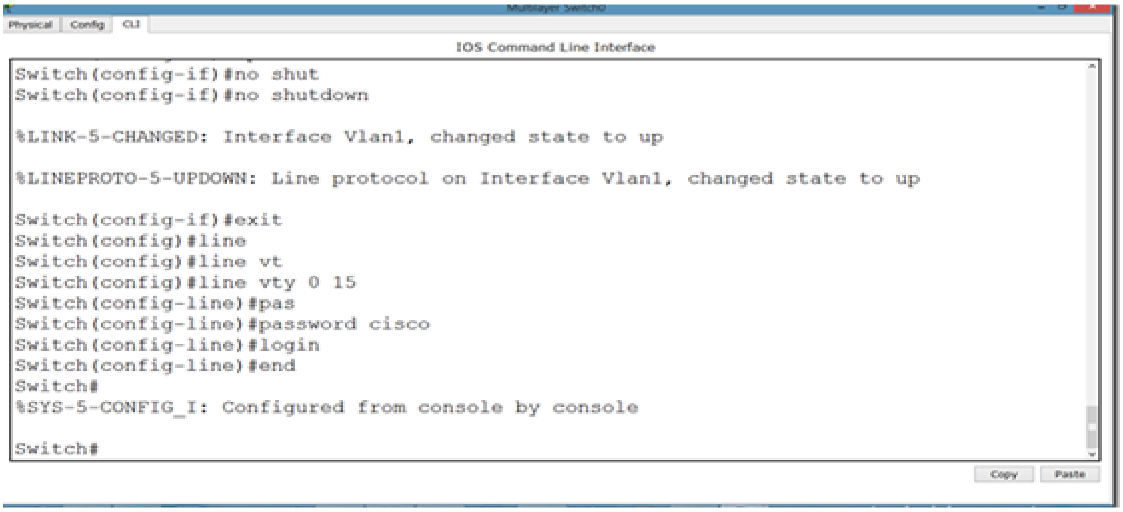
Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic
●	Successful	PC0	Multilayer Switch0	ICMP	🟦	0.000	N
●	Successful	PC3	Multilayer Switch0	ICMP	🟩	0.000	N
●	Successful	PC1	Multilayer Switch0	ICMP	■	0.000	N

Now, try to telnet the switch from our PC, it refuses because we have not applied authentication on the switch yet.



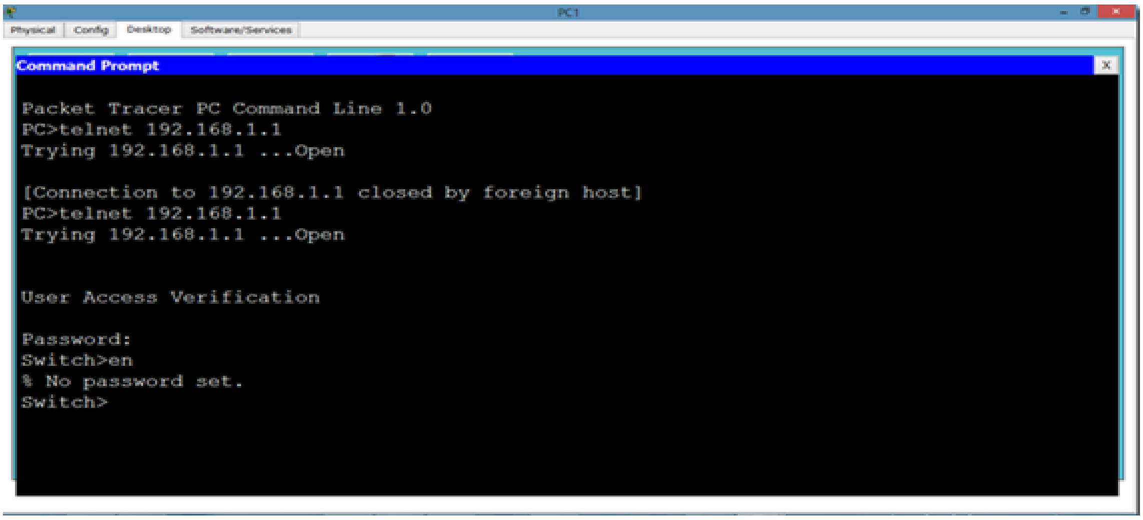
```
Packet Tracer PC Command Line 1.0
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

[Connection to 192.168.1.1 closed by foreign host]
PC>
```

So, let’s apply line authentication on the switch. The system supports 20 virtual tty (vty) lines for Telnet, Secure Shell Server (SSH) and FTP services. Each Telnet, SSH, or FTP session requires one vty line. You can add security to your system by configuring the software to validate login requests.



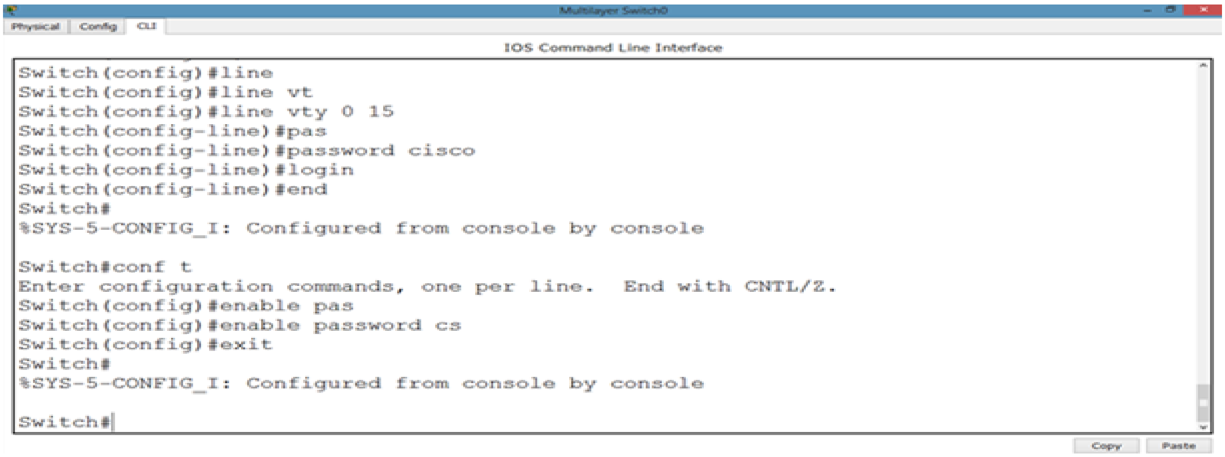
```
Switch(config-if)#no shut
Switch(config-if)#no shutdown

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

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

Switch(config-if)#exit
Switch(config)#line
Switch(config)#line vt
Switch(config)#line vty 0 15
Switch(config-line)#pas
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
```

Now, we can easily telnet. But it does not let us go in the switch enabled mode because we have not set the password on the switch yet.



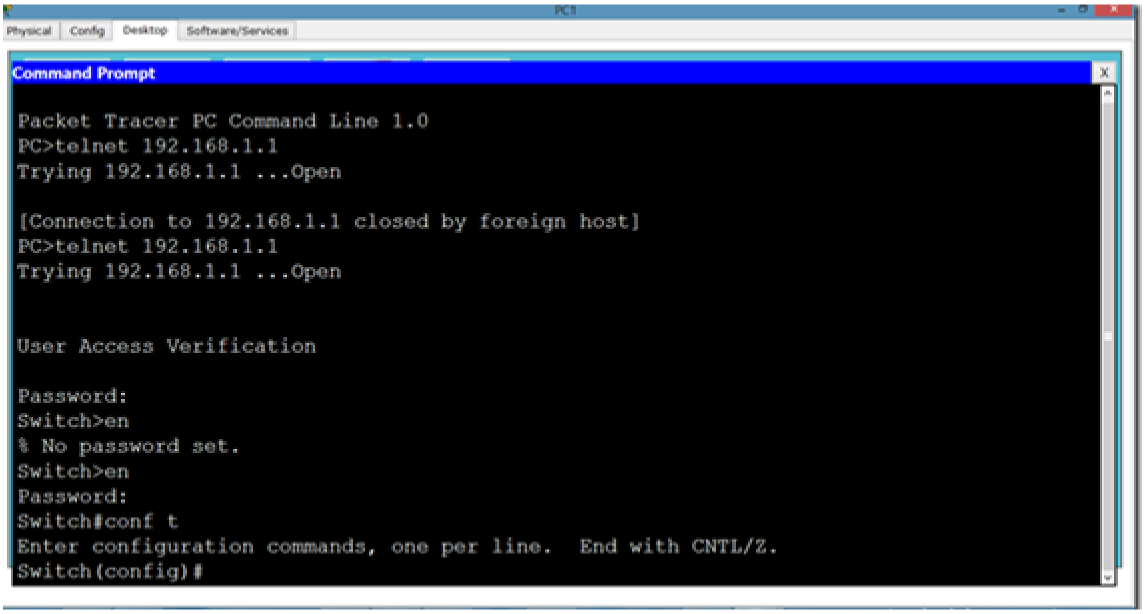
```
Packet Tracer PC Command Line 1.0
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

[Connection to 192.168.1.1 closed by foreign host]
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open


User Access Verification

Password:
Switch>en
% No password set.
Switch>
```

Let’s apply password on the switch enabled mode.



```
Switch(config)#line
Switch(config)#line vt
Switch(config)#line vty 0 15
Switch(config-line)#pas
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#enable pas
Switch(config)#enable password cs
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
```

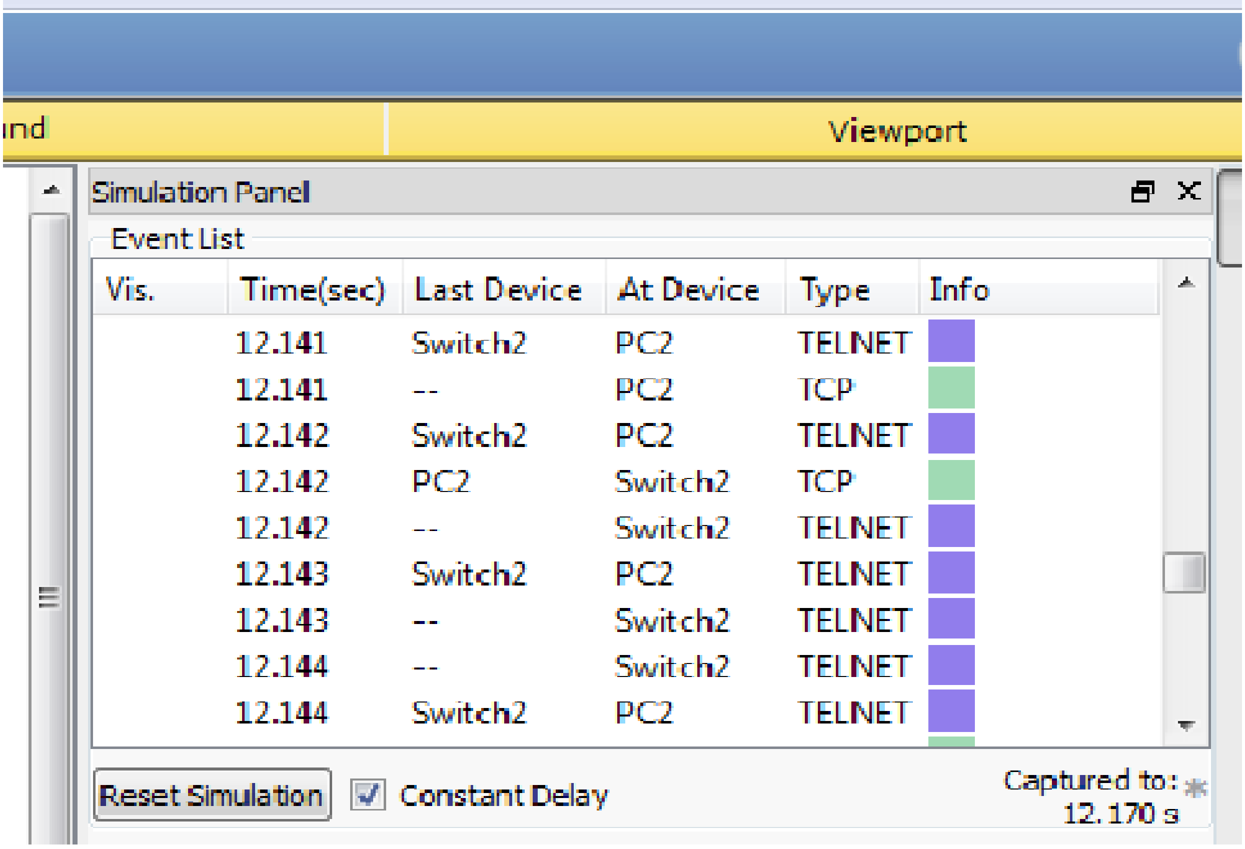
Now, we can go inside Switch configuration mode from our pc.



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

[Connection to 192.168.1.1 closed by foreign host]
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open


User Access Verification

Password:
Switch>en
% No password set.
Switch>en
Password:
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
```

SIMULATION

a) Now click on simulation icon in the right bottom of packet Tracer.
b) Now click on auto capture /play icon for packet capturing.
c) Click on the PC and go to Desktop →Command Prompt then Telnet 192.168.1.1



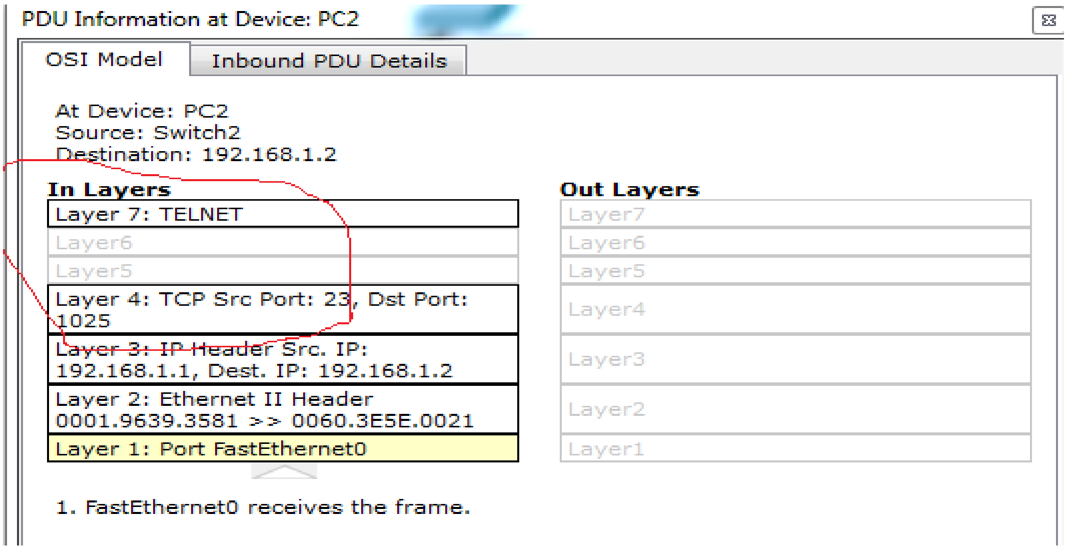
Vis.	Time(sec)	Last Device	At Device	Type	Info
	12.141	Switch2	PC2	TELNET	🟪
	12.141	--	PC2	TCP	🟩
	12.142	Switch2	PC2	TELNET	🟪
	12.142	PC2	Switch2	TCP	🟩
	12.142	--	Switch2	TELNET	🟪
	12.143	Switch2	PC2	TELNET	🟪
	12.143	--	Switch2	TELNET	🟪
	12.144	--	Switch2	TELNET	🟪
	12.144	Switch2	PC2	TELNET	🟪

Captured to: 12.170 s

Now click on the TELNET packet show its header.

a) Shows OSI layers involved in transmission.

The popped up window (below) will enable you to trace the content of the message through the OSI layer and what changes will occur at each layer (use next and previous buttons to trace each layer content).



PDU Information at Device: PC2

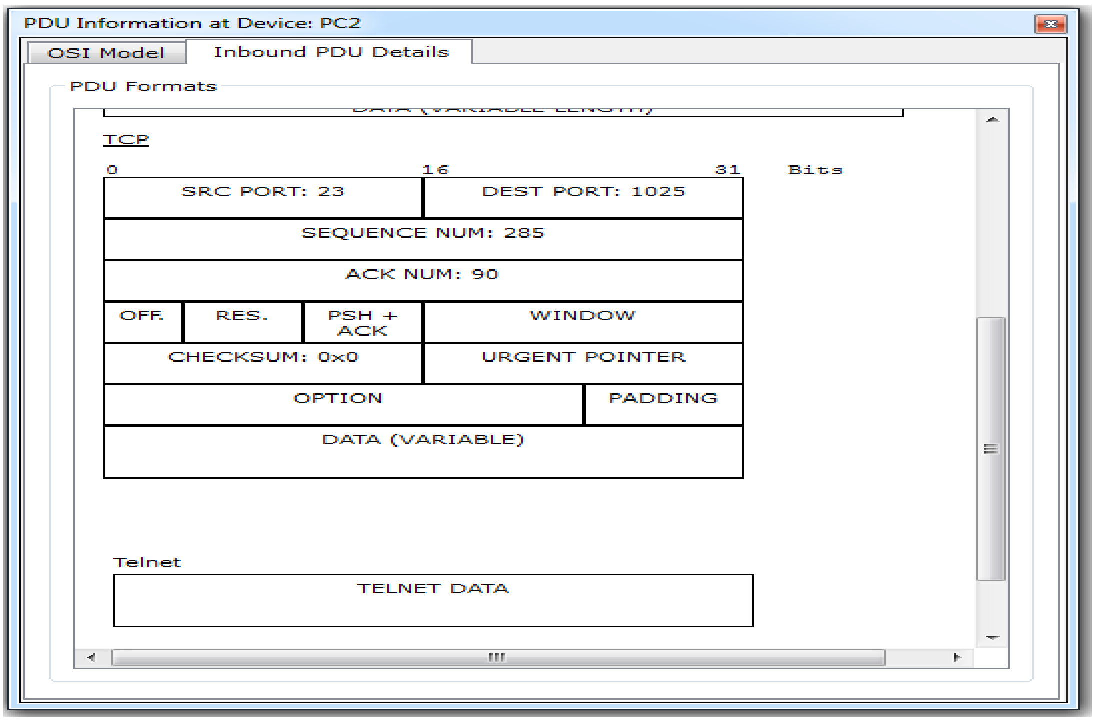
At Device: PC2
Source: Switch2
Destination: 192.168.1.2

In Layers	Out Layers
Layer 7: TELNET	Layer7
Layer6	Layer6
Layer5	Layer5
Layer 4: TCP Src Port: 23, Dst Port: 1025	Layer4
Layer 3: IP Header Src. IP: 192.168.1.1, Dest. IP: 192.168.1.2	Layer3
Layer 2: Ethernet II Header 0001.9639.3581 >> 0060.3E5E.0021	Layer2
Layer 1: Port FastEthernet0	Layer1

1. FastEthernet0 receives the frame.

b) Show Inbound PDU Details.

The inbound tab shows the content of the message (header format) during the receiving process.



PDU Information at Device: PC2

PDU Formats

DATA (VARIABLE LENGTH)

TCP

0 16 31 Bits

SRC PORT: 23			DEST PORT: 1025
SEQUENCE NUM: 285			
ACK NUM: 90			
OFF.	RES.	PSH + ACK	WINDOW
CHECKSUM: 0x0			URGENT POINTER
OPTION			PADDING
DATA (VARIABLE)			

Telnet

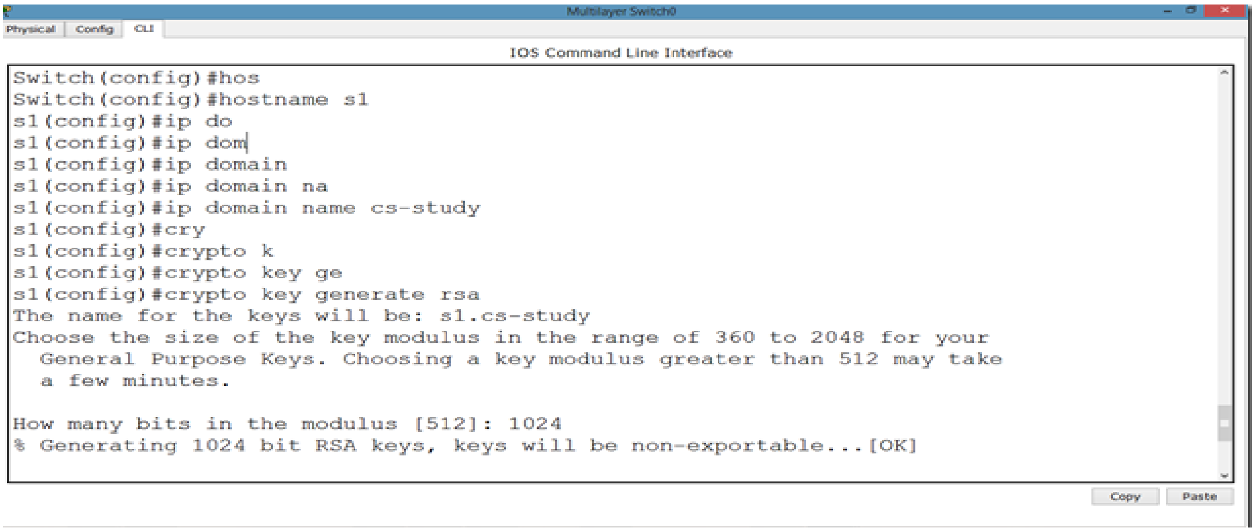
TELNET DATA

SSH

Secure Shell (SSH) is a cryptographic network protocol for secure data communication, remote shell services or command execution and other secure network services between two networked computers that connects, via a secure channel over an insecure network, a server and a client (running SSH server and SSH client programs, respectively). It was designed as a replacement for Telnet and other insecure remote shell protocols such as the Berkeley rsh and rexec protocols, which send information, notably passwords, in plaintext, rendering them susceptible to interception and disclosure using packet analysis. The encryption used by SSH is intended to provide confidentiality and integrity of data over an unsecured network, such as the Internet.

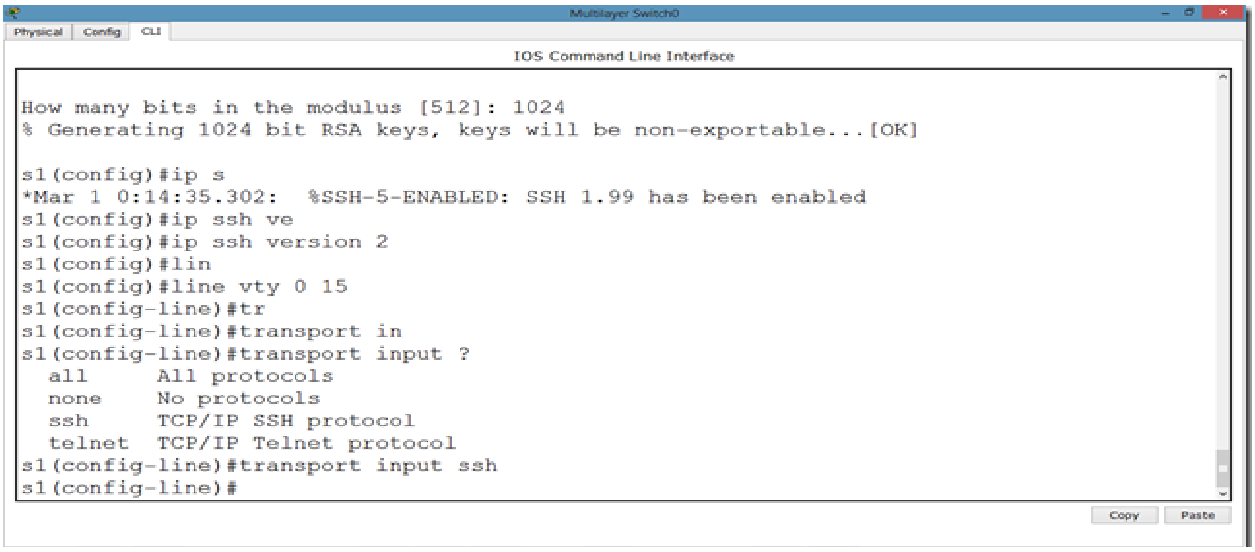
A network protocol that ensures a high-level encryption, allowing for the data transmitted over insecure networks, such as the Internet, to be kept intact and integrate. SSH and SSH Telnet, in particular, work for establishing a secure communication between two network-connected computers as an alternative to remote shells, such as TELNET, that send sensitive information in an insecure environment. In contrast to other remote access protocols, such as FTP, SSH Telnet ensures higher level of connection security between distant machines but at the same time represents a potential threat to the server stability. Thus, SSH access is considered a special privilege by hosting providers and is often assigned to users only per request.

So, now let us apply SSH on the switch.



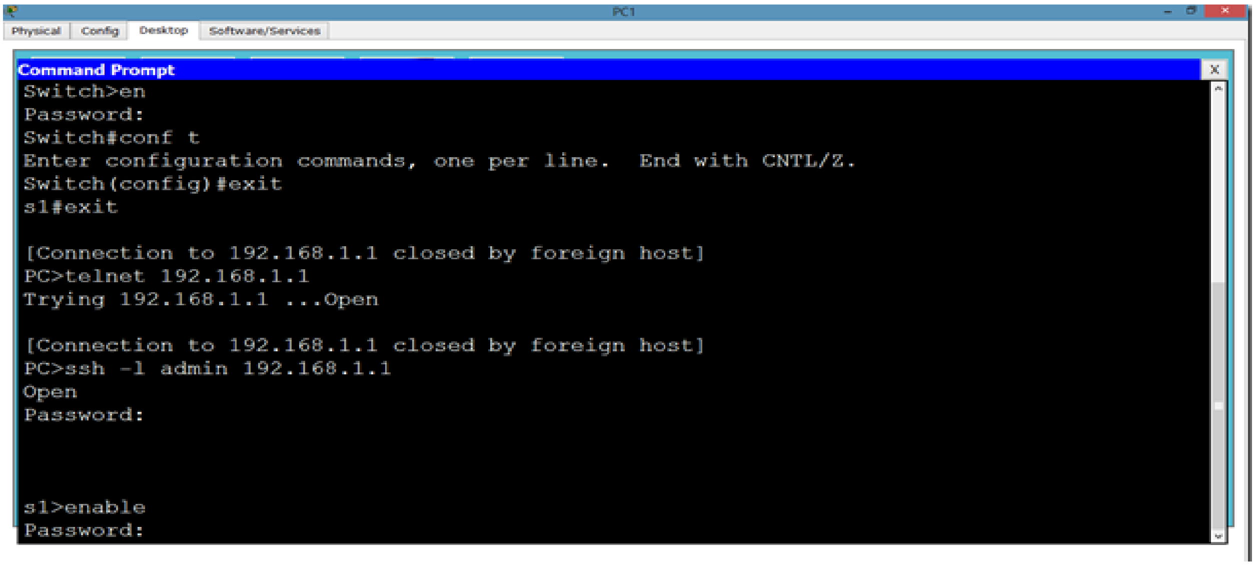
```
Switch(config)#hos
Switch(config)#hostname s1
s1(config)#ip do
s1(config)#ip dom
s1(config)#ip domain
s1(config)#ip domain na
s1(config)#ip domain name cs-study
s1(config)#cry
s1(config)#crypto k
s1(config)#crypto key ge
s1(config)#crypto key generate rsa
The name for the keys will be: s1.cs-study
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]
```

Commands continued.



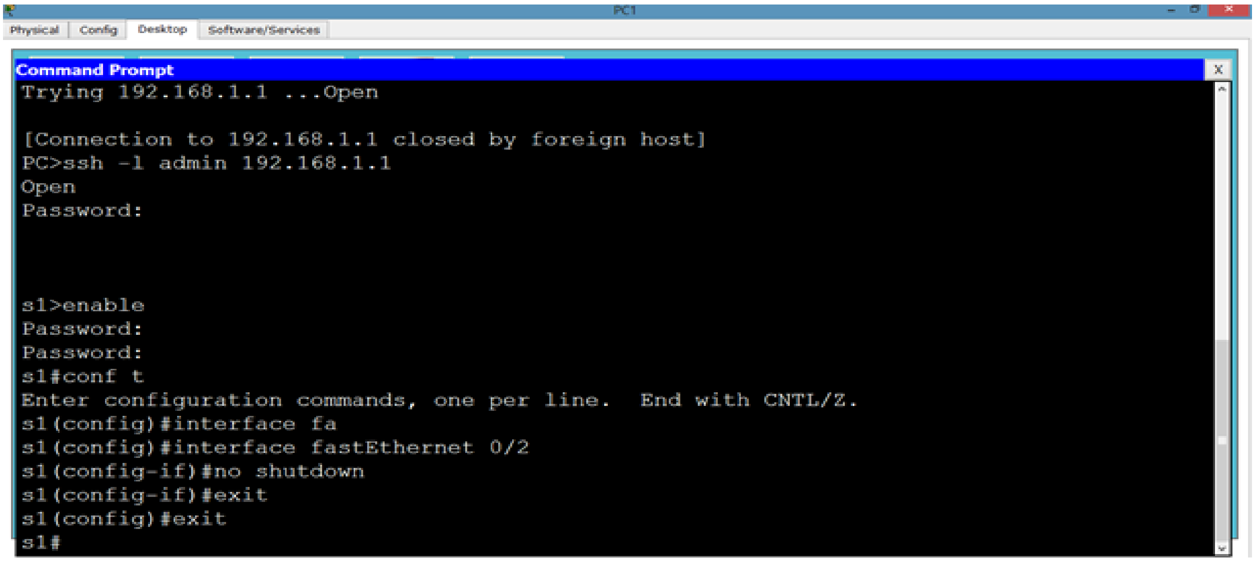
```

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

s1(config)#ip s
*Mar 1 0:14:35.302:  %SSH-5-ENABLED: SSH 1.99 has been enabled
s1(config)#ip ssh ve
s1(config)#ip ssh version 2
s1(config)#lin
s1(config)#line vty 0 15
s1(config-line)#tr
s1(config-line)#transport in
s1(config-line)#transport input ?
  all      All protocols
  none     No protocols
  ssh      TCP/IP SSH protocol
  telnet   TCP/IP Telnet protocol
s1(config-line)#transport input ssh
s1(config-line)#
```

Now, we try to telnet it but it is refused because ssh has over ruled telnet. So, we will use SSH protocol on it. By default username is admin.



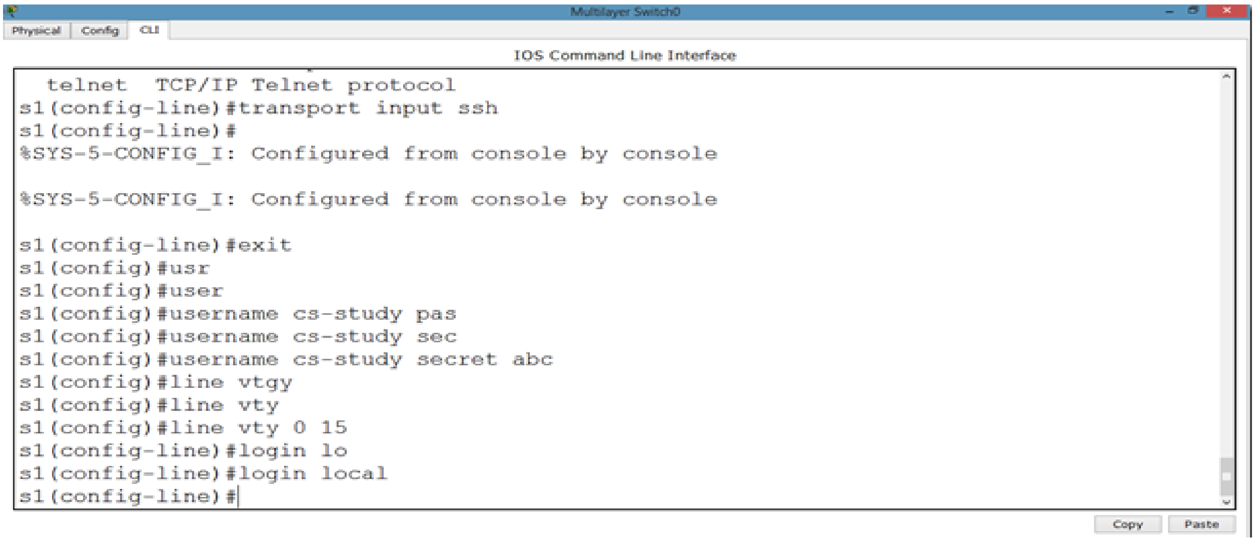
```
Switch>en
Password:
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#exit
s1#exit

[Connection to 192.168.1.1 closed by foreign host]
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

[Connection to 192.168.1.1 closed by foreign host]
PC>ssh -l admin 192.168.1.1
Open
Password:



s1>enable
Password:
```

And we can apply any sort of configuration on our switch from out pc.



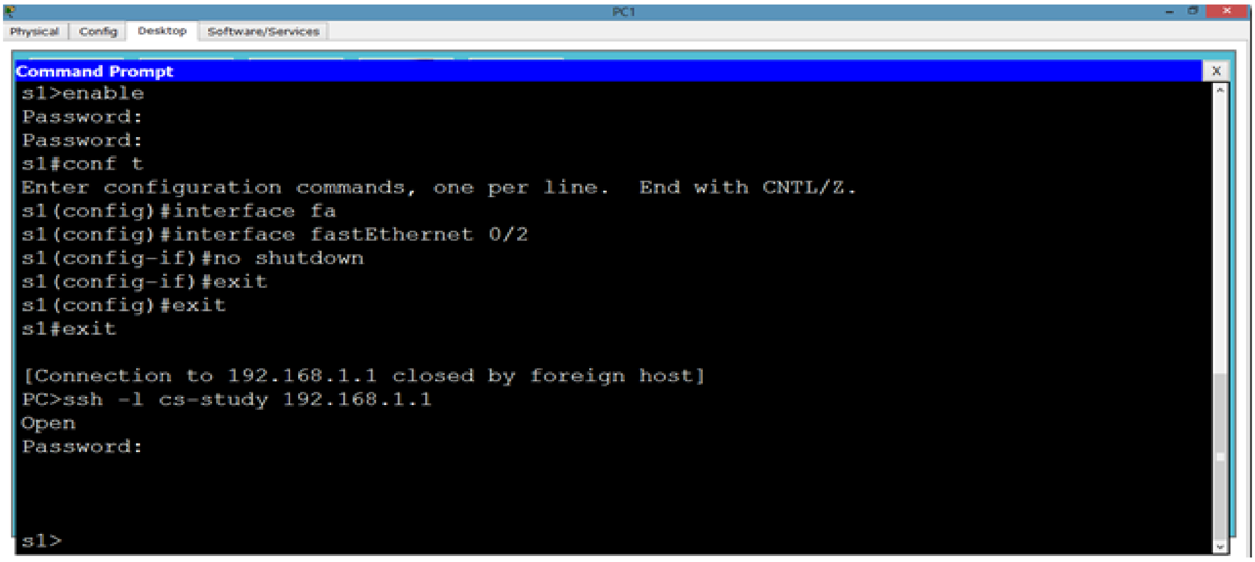
```
Trying 192.168.1.1 ...Open

[Connection to 192.168.1.1 closed by foreign host]
PC>ssh -l admin 192.168.1.1
Open
Password:



s1>enable
Password:
Password:
s1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
s1(config)#interface fa
s1(config)#interface fastEthernet 0/2
s1(config-if)#no shutdown
s1(config-if)#exit
s1(config)#exit
s1#
```

Now, if we want to change the username from admin to something else, we will do it as follows.



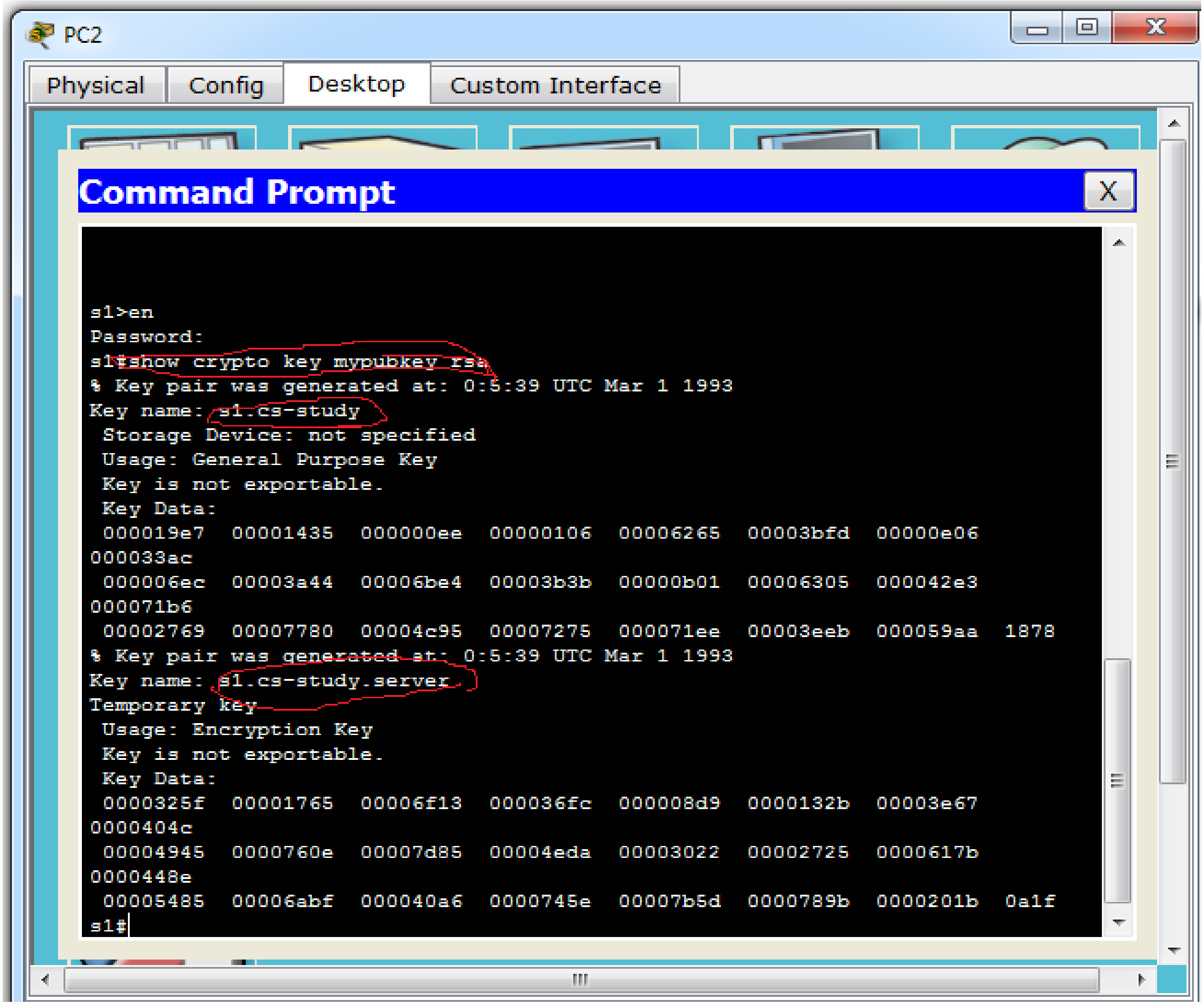
```
  telnet  TCP/IP Telnet protocol
s1(config-line)#transport input ssh
s1(config-line)#
%SYS-5-CONFIG_I: Configured from console by console

%SYS-5-CONFIG_I: Configured from console by console

s1(config-line)#exit
s1(config)#usr
s1(config)#user
s1(config)#username cs-study pas
s1(config)#username cs-study sec
s1(config)#username cs-study secret abc
s1(config)#line vtgy
s1(config)#line vty
s1(config)#line vty 0 15
s1(config-line)#login lo
s1(config-line)#login local
s1(config-line)#
```

And from our pc as follows.



```
s1>enable
Password:
Password:
s1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
s1(config)#interface fa
s1(config)#interface fastEthernet 0/2
s1(config-if)#no shutdown
s1(config-if)#exit
s1(config)#exit
s1#exit

[Connection to 192.168.1.1 closed by foreign host]
PC>ssh -l cs-study 192.168.1.1
Open
Password:



s1>
```

You can also see the generated keys in SSH as shown below.



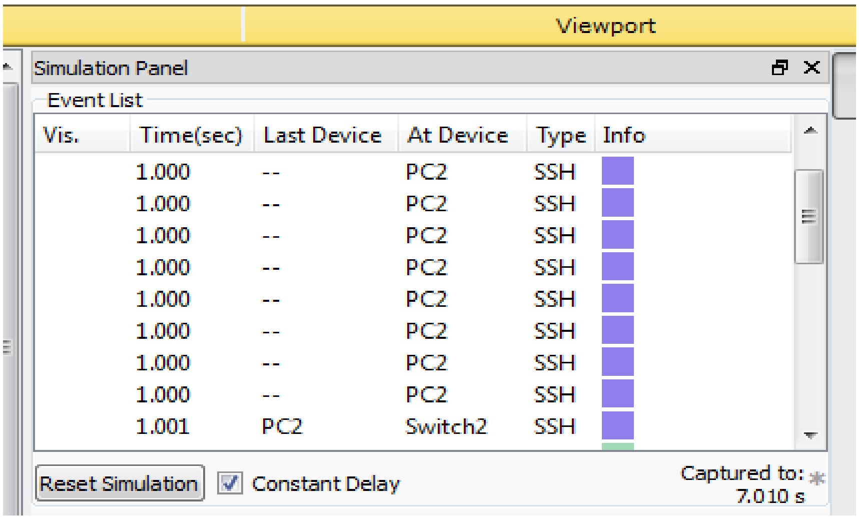
```
s1>en
Password:
s1#show crypto key mypubkey rsa
% Key pair was generated at: 0:5:39 UTC Mar 1 1993
Key name: s1.cs-study
 Storage Device: not specified
 Usage: General Purpose Key
 Key is not exportable.
 Key Data:
 000019e7  00001435  000000ee  00000106  00006265  00003bfd  00000e06
000033ac
 000006ec  00003a44  00006be4  00003b3b  00000b01  00006305  000042e3
000071b6
 00002769  00007780  00004c95  00007275  000071ee  00003eeb  000059aa  1878
% Key pair was generated at: 0:5:39 UTC Mar 1 1993
Key name: s1.cs-study.server
Temporary key
 Usage: Encryption Key
 Key is not exportable.
 Key Data:
 0000325f  00001765  00006f13  000036fc  000008d9  0000132b  00003e67
0000404c
 00004945  0000760e  00007d85  00004eda  00003022  00002725  0000617b
0000448e
 00005485  00006abf  000040a6  0000745e  00007b5d  0000789b  0000201b  0a1f
s1#
```

SIMULATION:

a) Now click on simulation icon in the right bottom of packet Tracer.

b) Now click on auto capture /play icon for packet capturing.

c) Click on the PC and go to Desktop →Command Prompt then ssh -l admin 192.168.1.1



Vis.	Time(sec)	Last Device	At Device	Type	Info
	1.000	--	PC2	SSH	🟪
	1.000	--	PC2	SSH	🟪
	1.000	--	PC2	SSH	🟪
	1.000	--	PC2	SSH	🟪
	1.000	--	PC2	SSH	🟪
	1.000	--	PC2	SSH	🟪
	1.000	--	PC2	SSH	🟪
	1.000	--	PC2	SSH	🟪
	1.001	PC2	Switch2	SSH	🟪

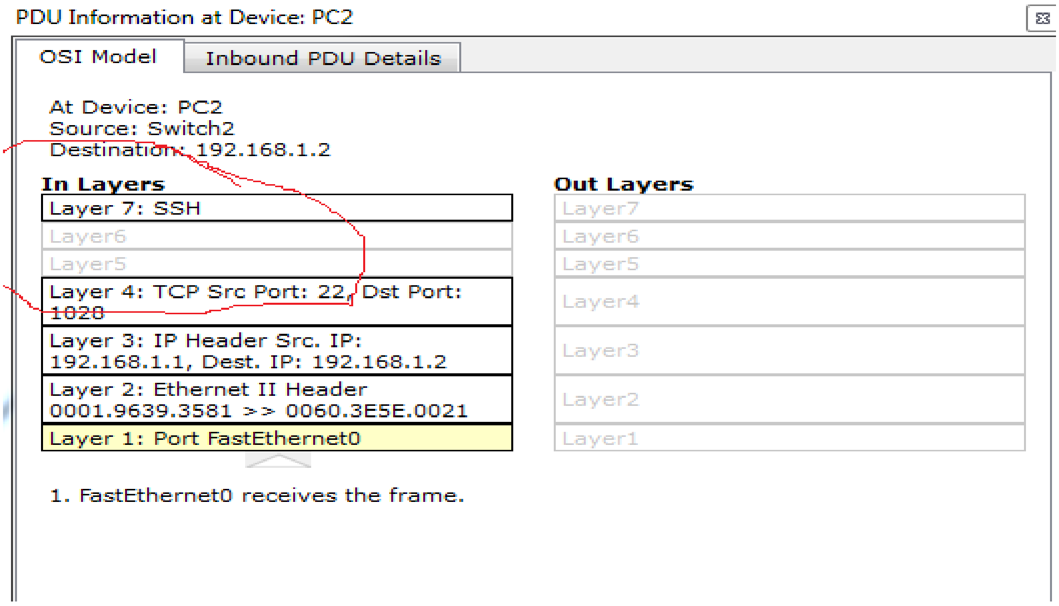
☑ Constant Delay

Captured to:
7.010 s

Now click on the SSH packet show its header.

b) Shows OSI layers involved in transmission.

The popped up window (below) will enable you to trace the content of the message through the OSI layer and what changes will occur at each layer (use next and previous buttons to trace each layer content).



PDU Information at Device: PC2

At Device: PC2
Source: Switch2
Destination: 192.168.1.2

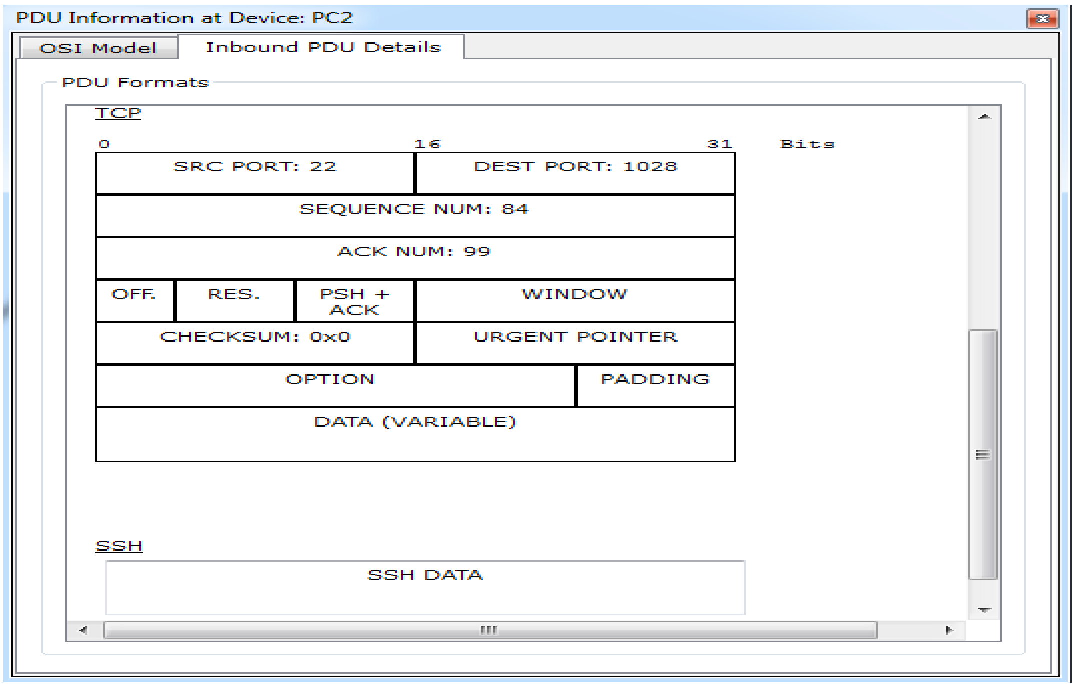
In Layers
Layer 7: SSH
Layer6
Layer5
Layer 4: TCP Src Port: 22, Dst Port: 1028
Layer 3: IP Header Src. IP: 192.168.1.1, Dest. IP: 192.168.1.2
Layer 2: Ethernet II Header 0001.9639.3581 >> 0060.3E5E.0021
Layer 1: Port FastEthernet0

Out Layers
Layer7
Layer6
Layer5
Layer4
Layer3
Layer2
Layer1

1. FastEthernet0 receives the frame.

b) Show Inbound PDU Details.

The inbound tab shows the content of the message (header format) during the receiving process.



TCP

0 16 31 Bits

SRC PORT: 22 | DEST PORT: 1028

SEQUENCE NUM: 84

ACK NUM: 99

OFF. | RES. | PSH + ACK | WINDOW

CHECKSUM: 0x0 | URGENT POINTER

OPTION | PADDING

DATA (VARIABLE)

SSH

SSH DATA