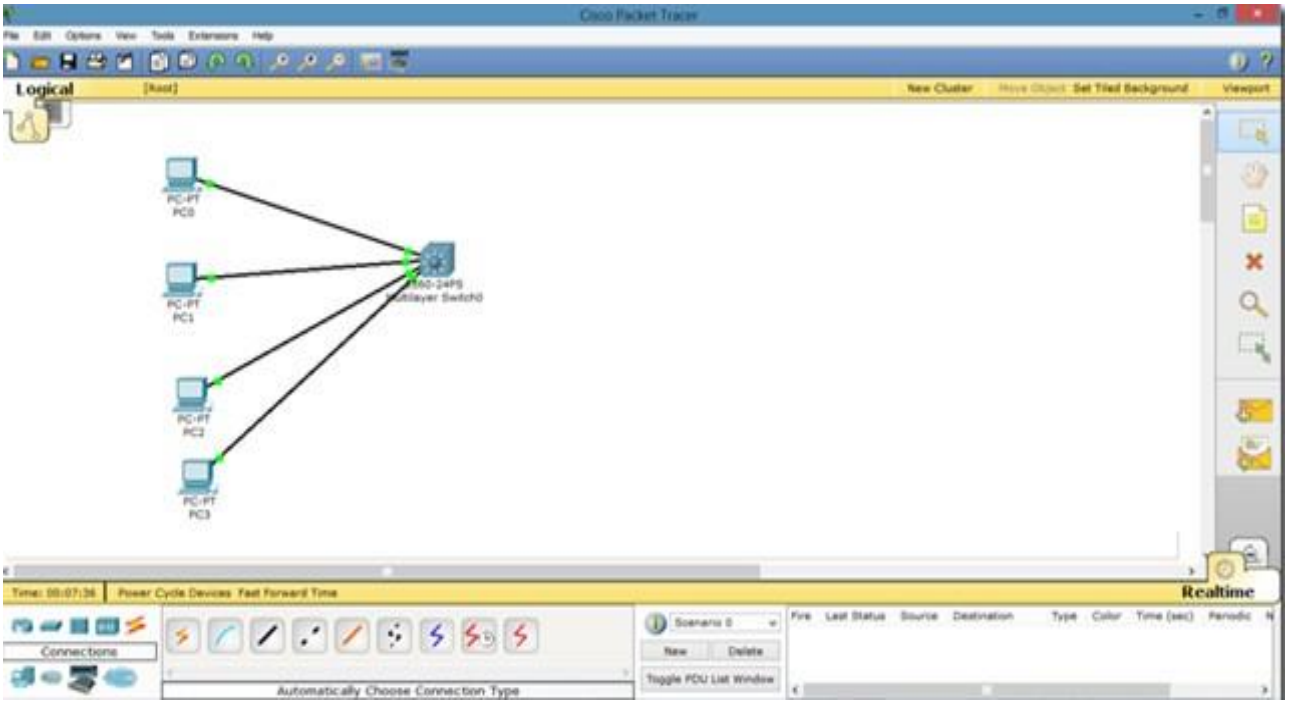
NATIONAL UNIVERSITY OF COMPUTER & EMERGING SCIENCE
Computer Networks Lab (CL307)
Lab Session 03
Application Layer Protocol

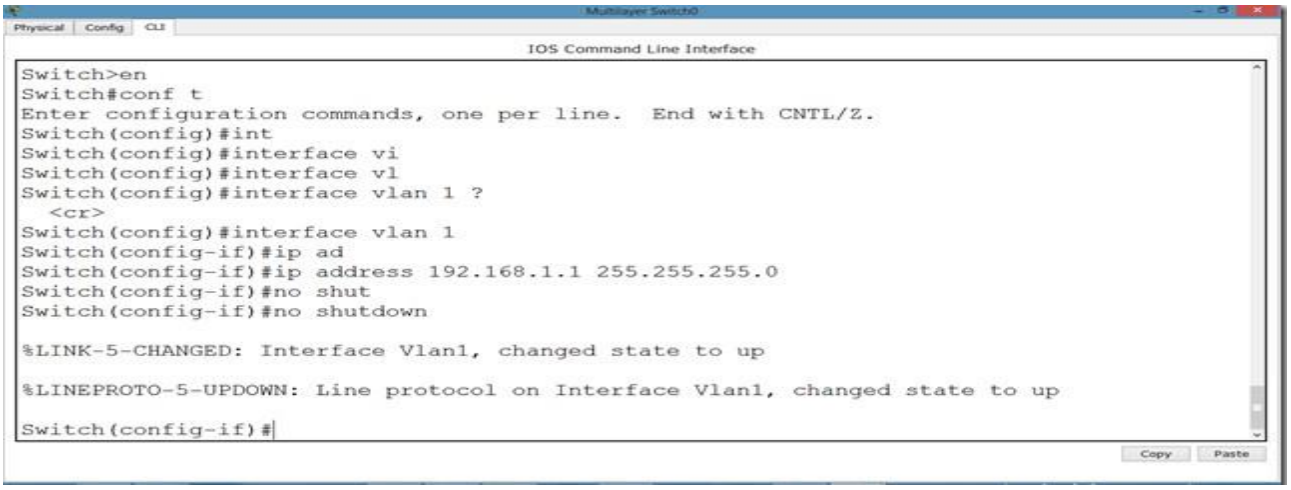
TELNET

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.

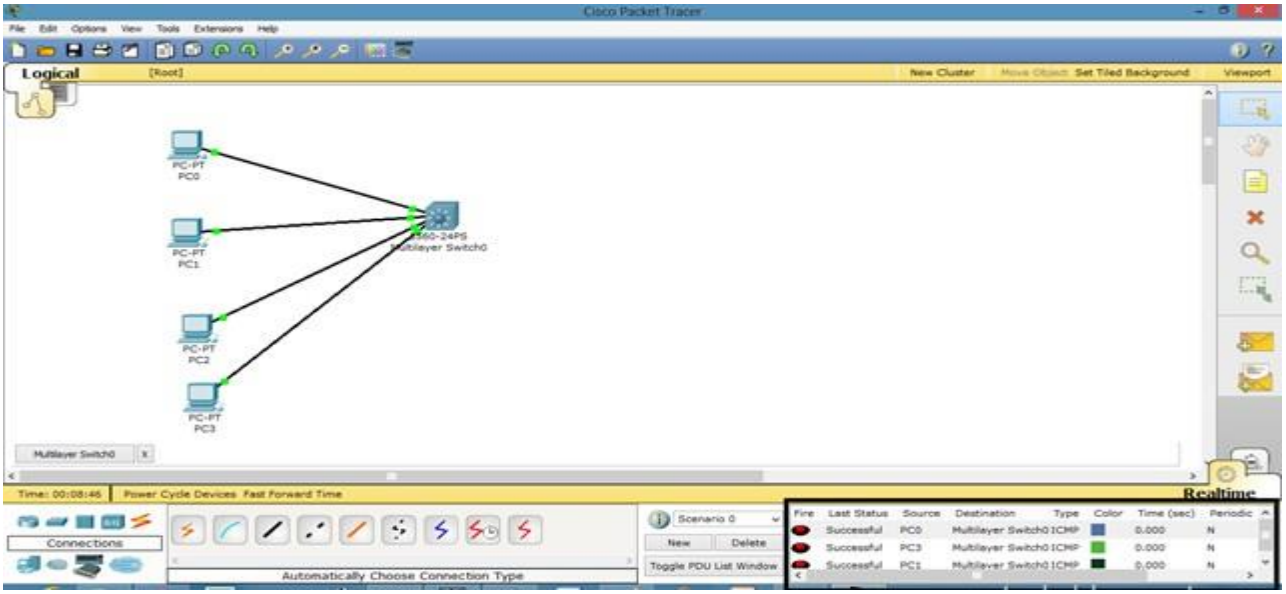
Let us apply Telnet on packet tracer.



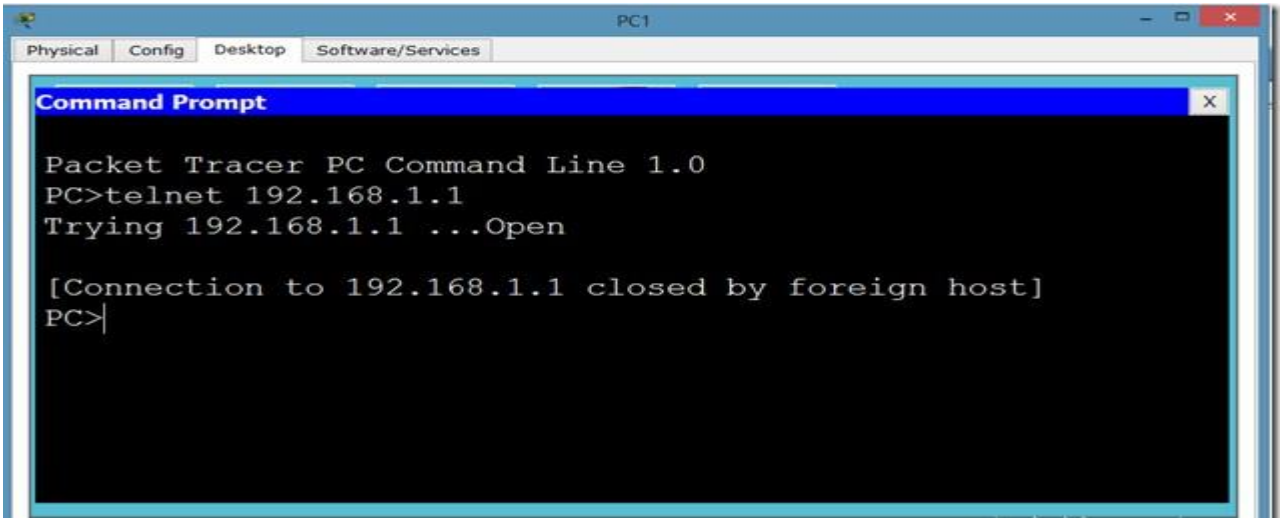
Take the topology as in the above diagram. Set IPs on the PCs. As, by default, all PCs are in vlan 1. We will create a virtual interface on switch with vlan 1 as follows.



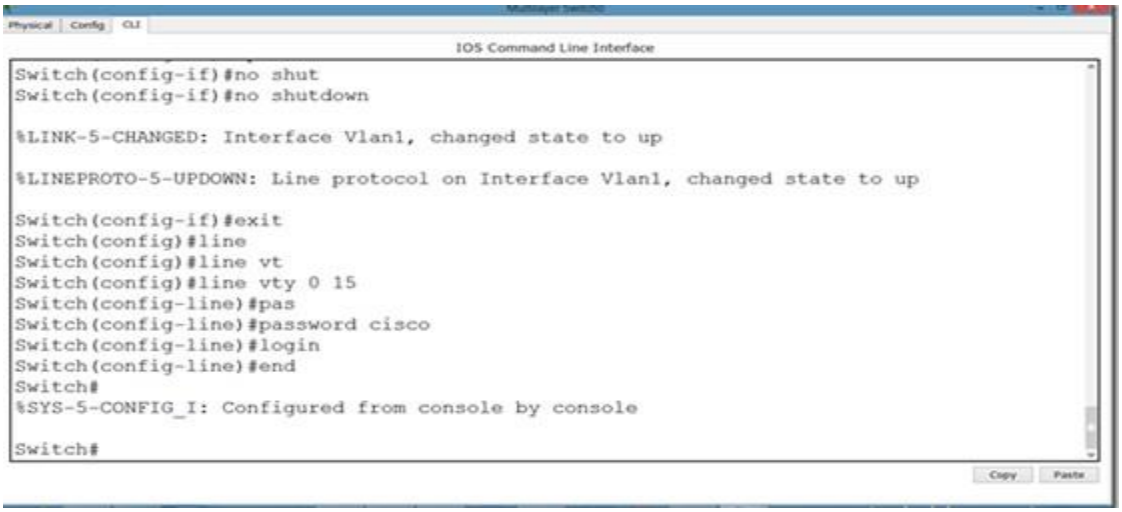
Now, we can ping to switch by our hosts because hosts are in vlan 1 and switch also has a vlan 1 interface.



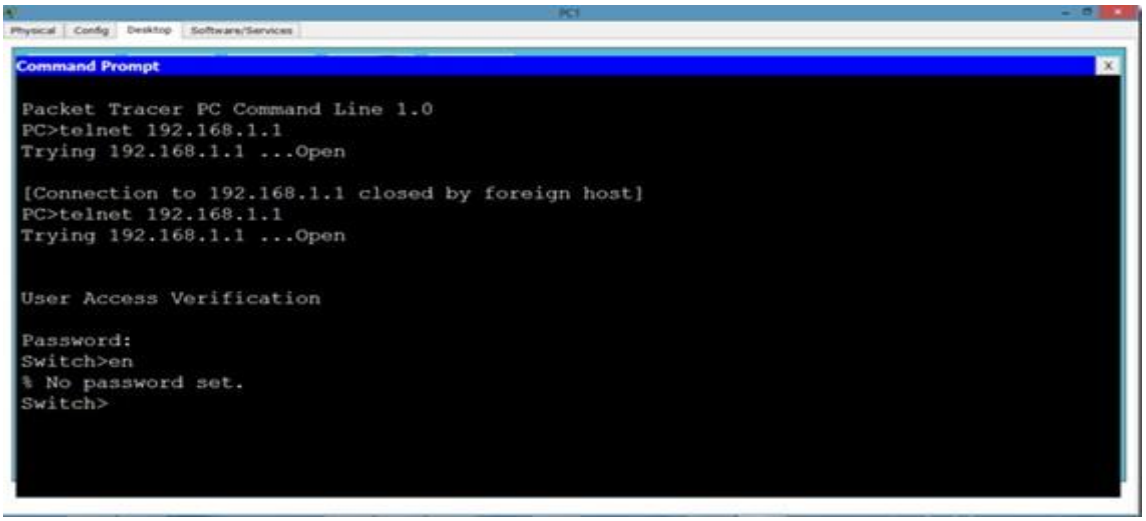
Now, try to telnet the switch from our PC, it refuses because we have not applied authentication on the switch yet.



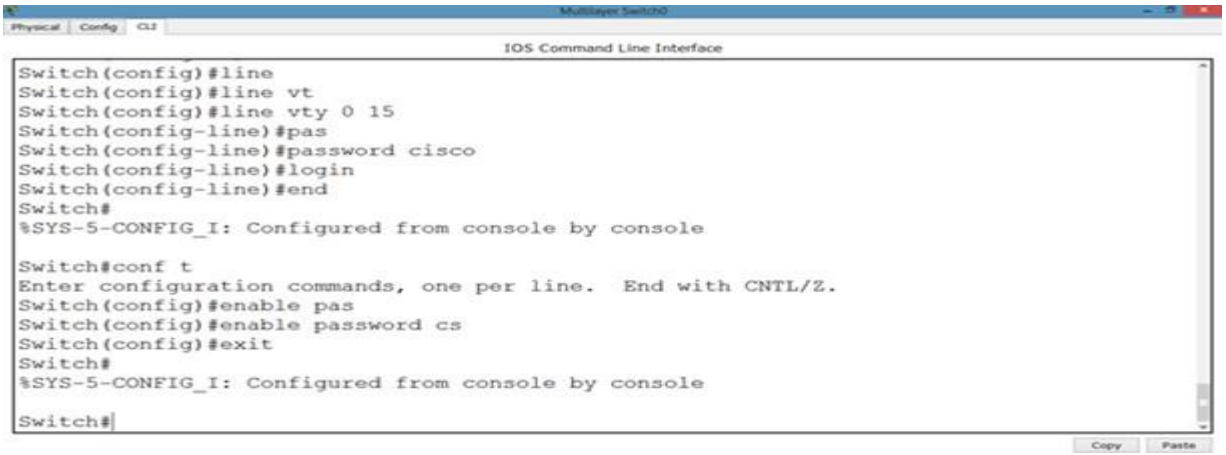
So, let's apply line authentication on the switch. The system supports 20 virtual tty (vty) lines for Telnet, Secure Shell Server (SSH) and FTP services. Each Telnet, SSH, or FTP session requires one vty line. You can add security to your system by configuring the software to validate login requests.



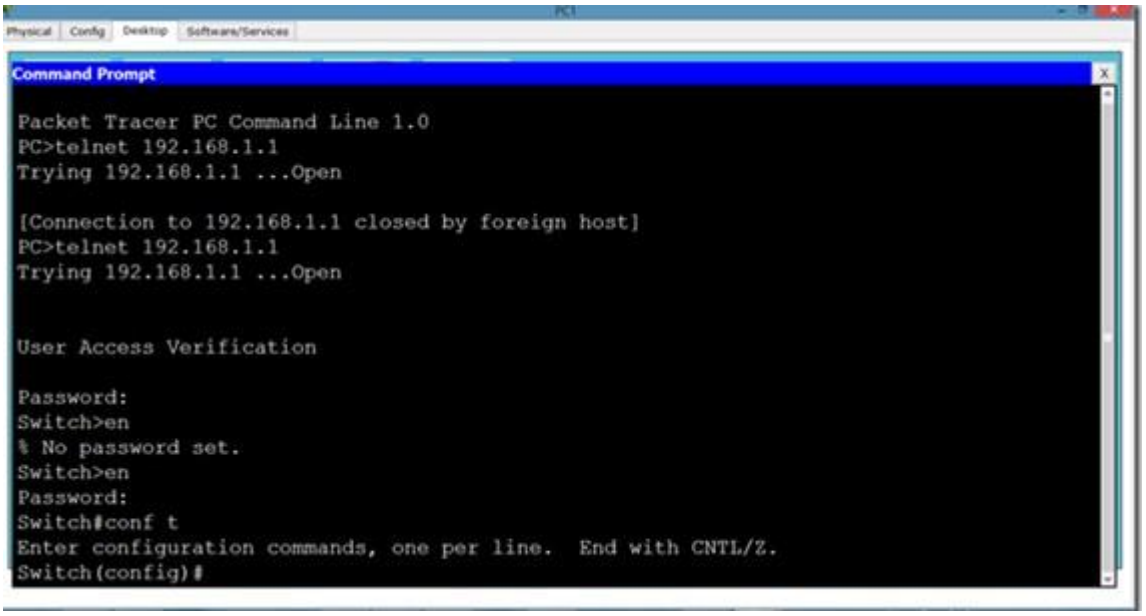
Now, we can easily telnet. But it does not let us go in the switch enabled mode because we have not set the password on the switch yet.



Let's apply password on the switch enabled mode.

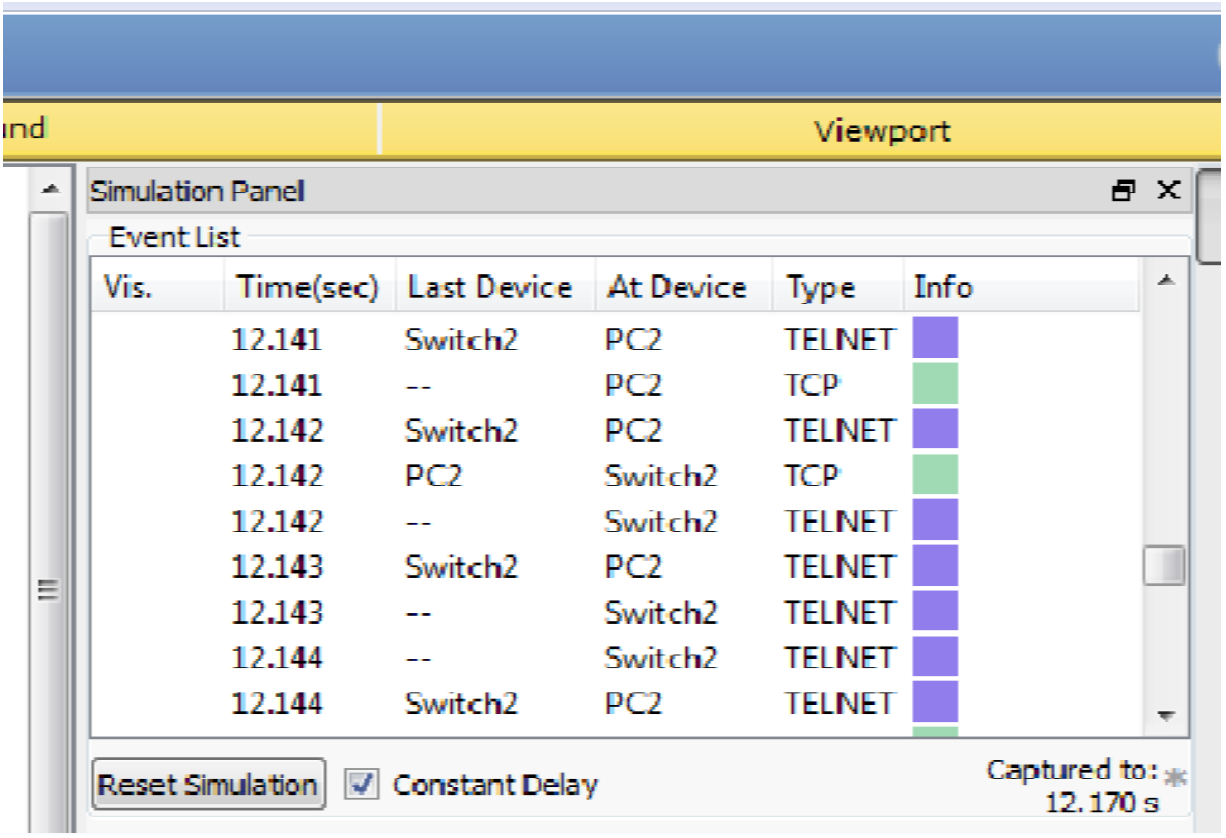


Now, we can go inside Switch configuration mode from our pc.



SIMULATION

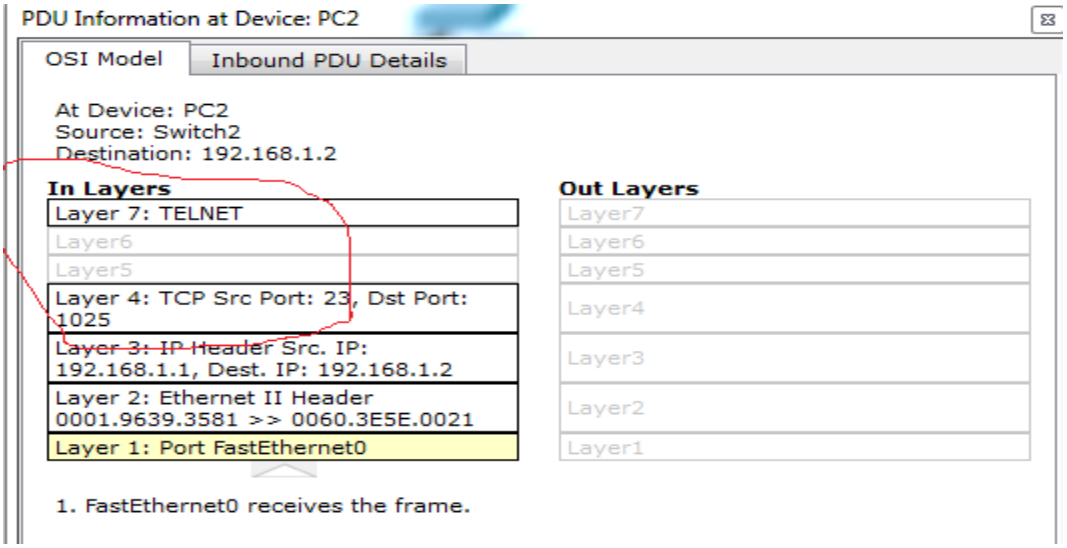
a) **Now click on simulation icon in the right bottom of packet Tracer.**
b) **Now click on auto capture /play icon for packet capturing.**
c) **Click on the PC and go to Desktop →Command Prompt then Telnet 192.168.1.1**



Now click on the TELNET packet show its header.

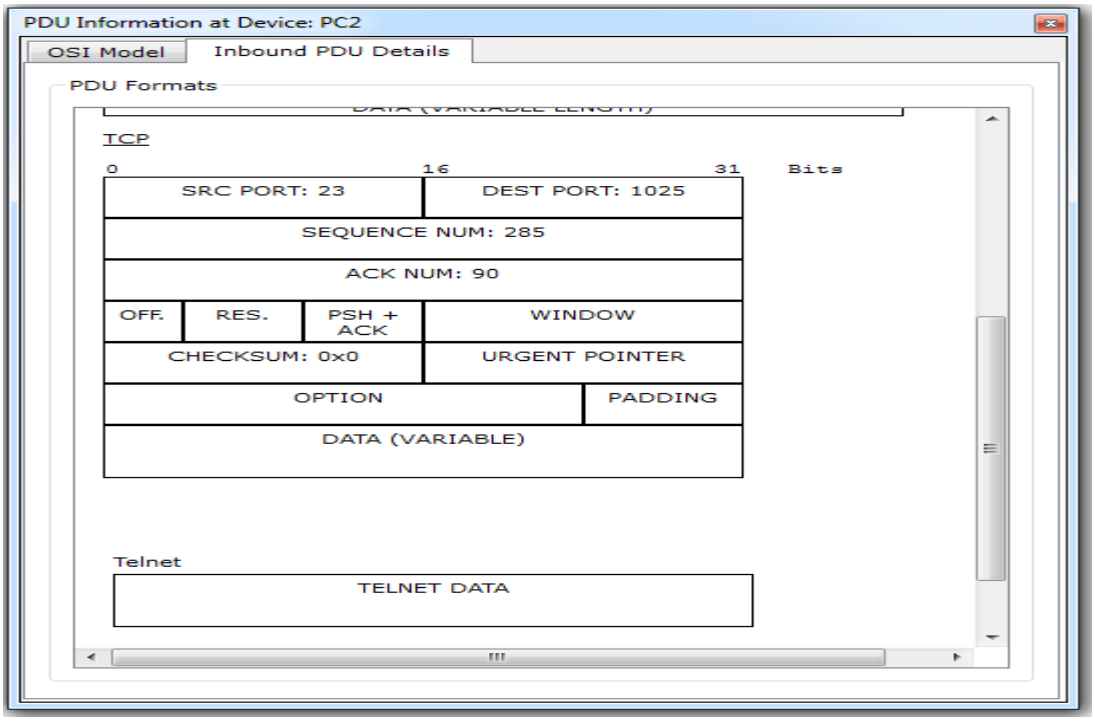
a) Shows OSI layers involved in transmission.

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).



b) Show Inbound PDU Details.

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

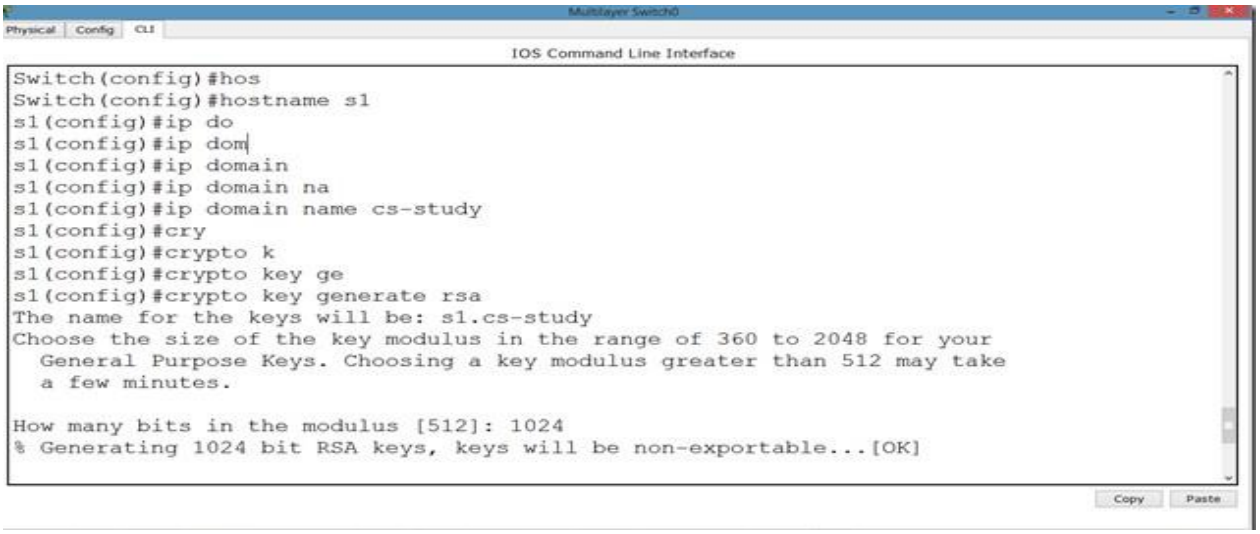


SSH

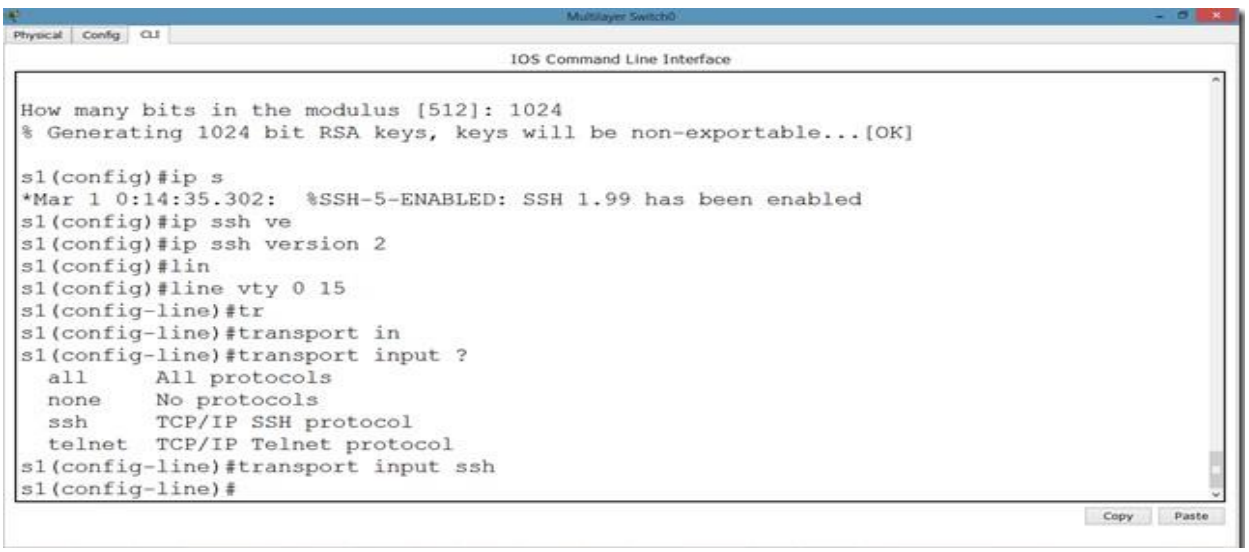
Secure Shell (SSH) is a cryptographic network protocol for secure data communication, remote shell services or command execution and other secure network services between two networked computers that connects, via a secure channel over an insecure network, a server and a client (running SSH server and 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.

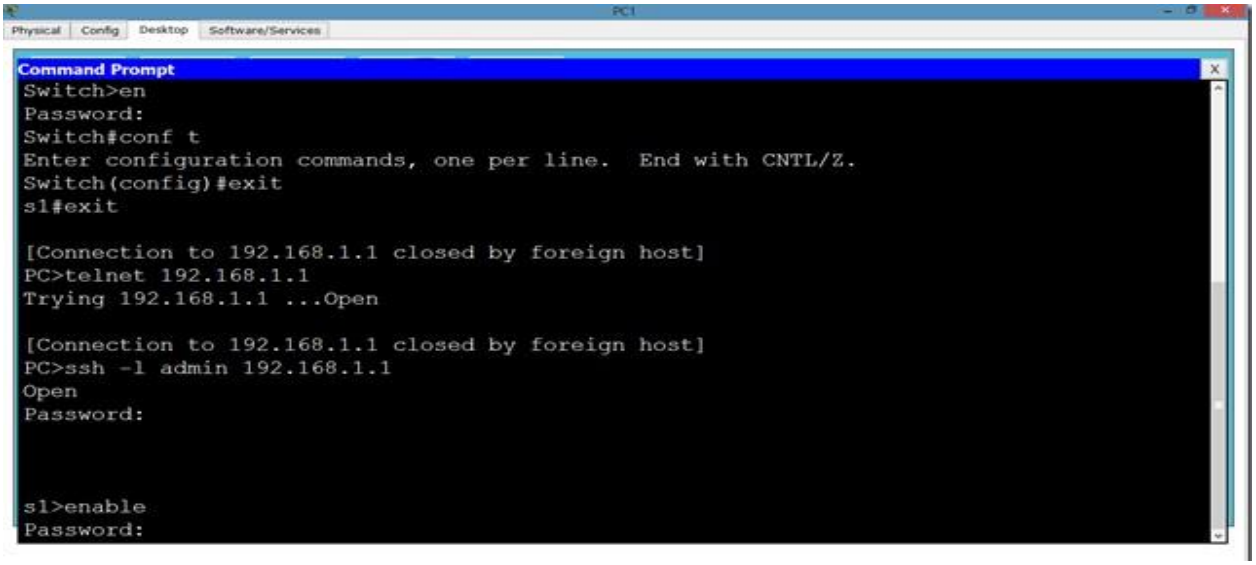
So, now let us apply SSH on the switch.



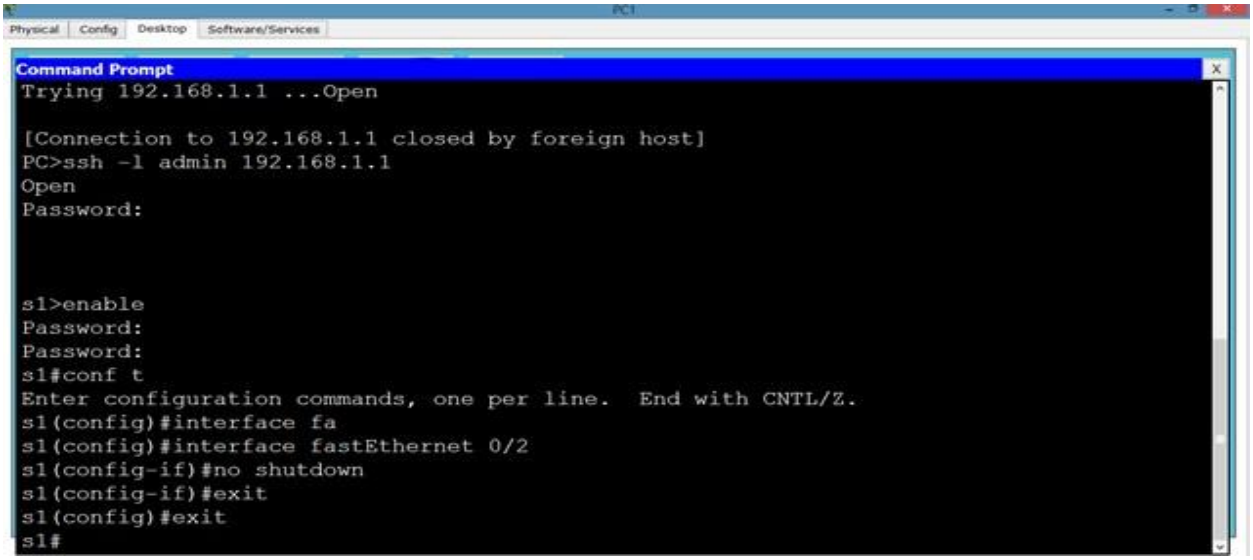
Commands continued.



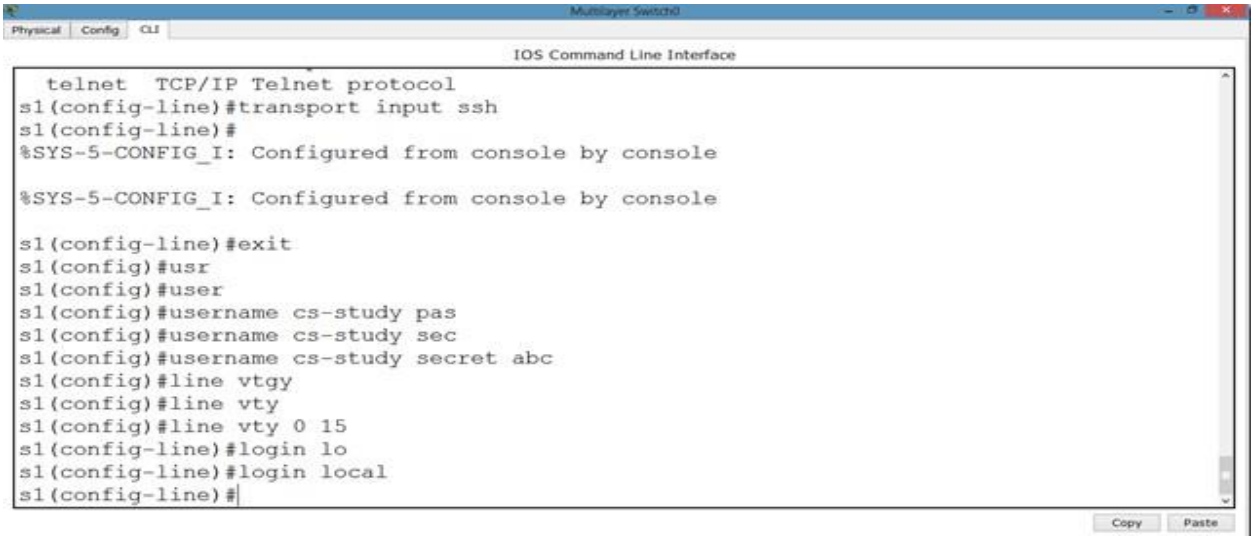
Now, we try to telnet it but it is refused because ssh has over ruled telnet. So, we will use SSH protocol on it. By default username is admin.



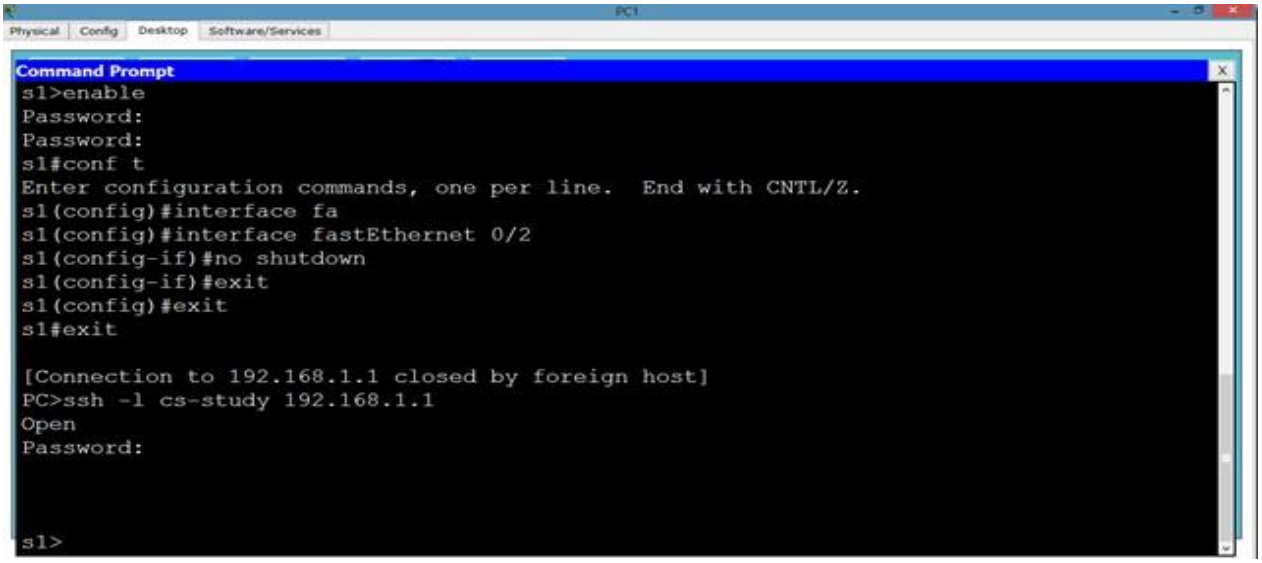
And we can apply any sort of configuration on our switch from out pc.



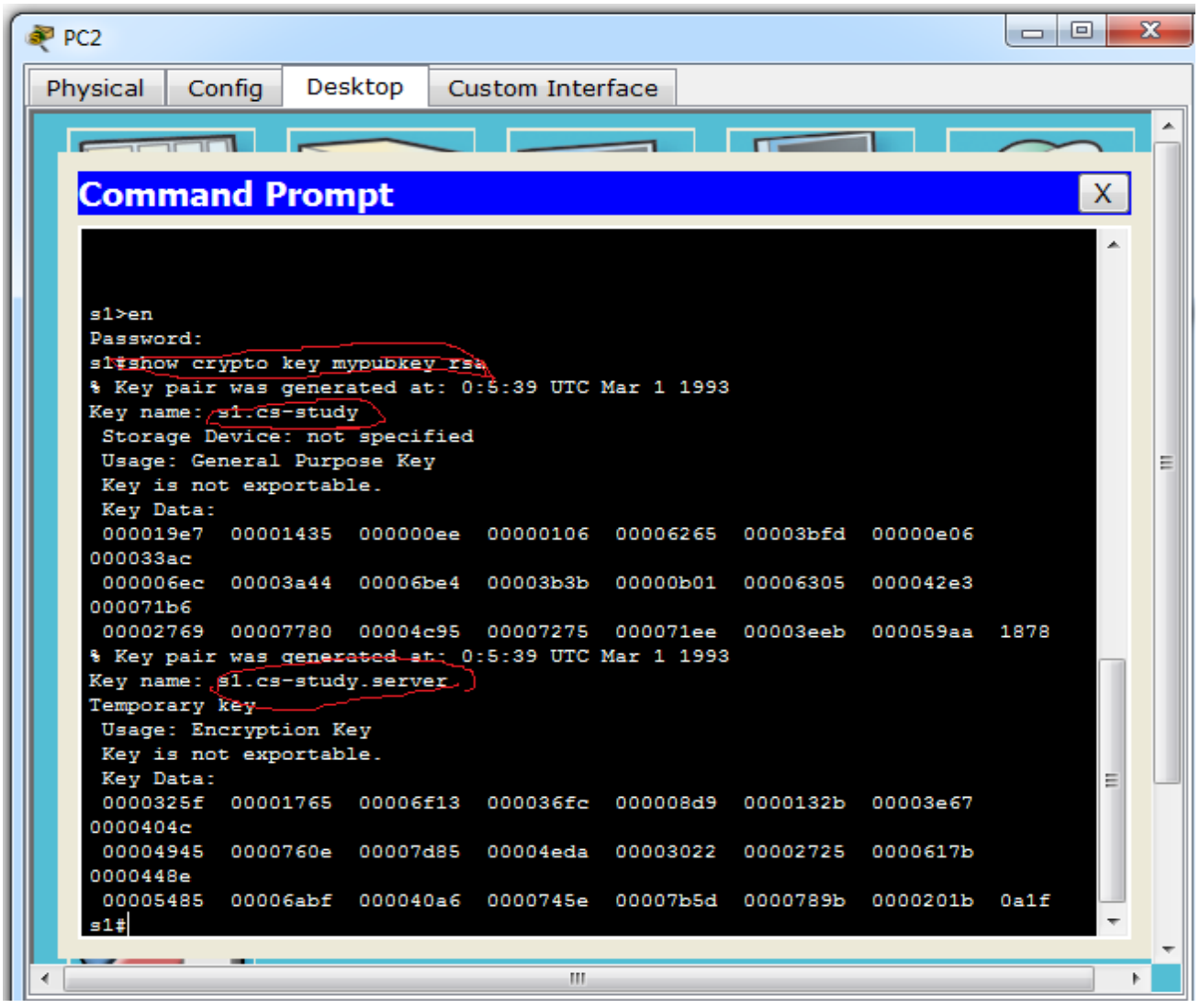
Now, if we want to change the username from admin to something else, we will do it as follows.



And from our pc as follows.



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

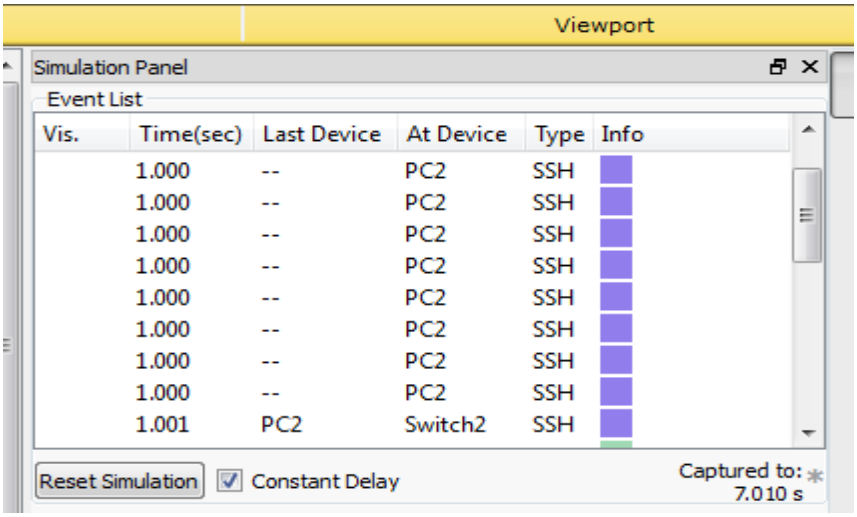


SIMULATION:

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

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

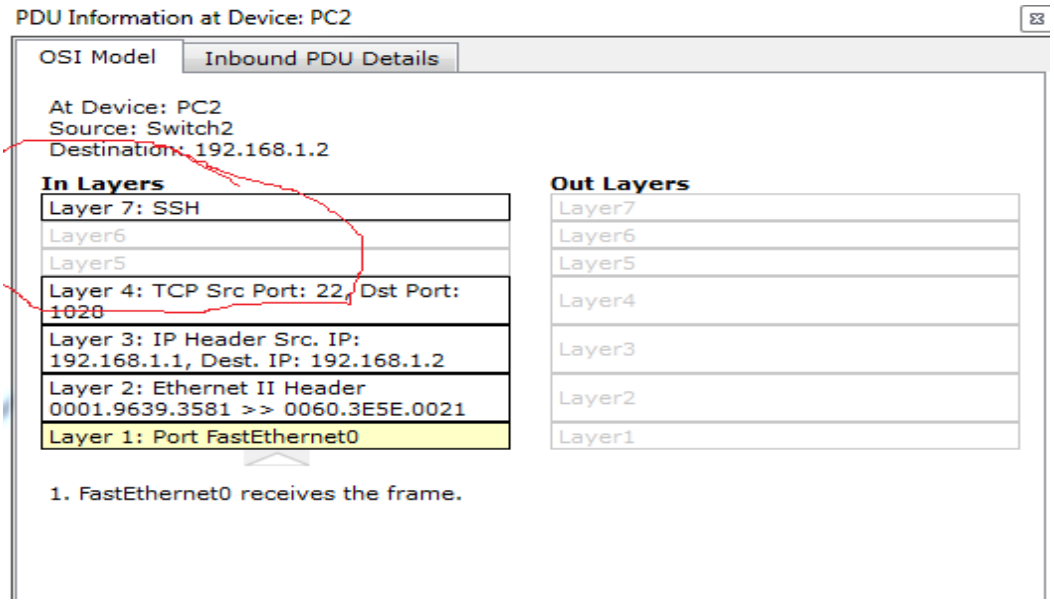
c) Click on the PC and go to Desktop →Command Prompt then ssh -l admin 192.168.1.1



Now click on the SSH packet show its header.

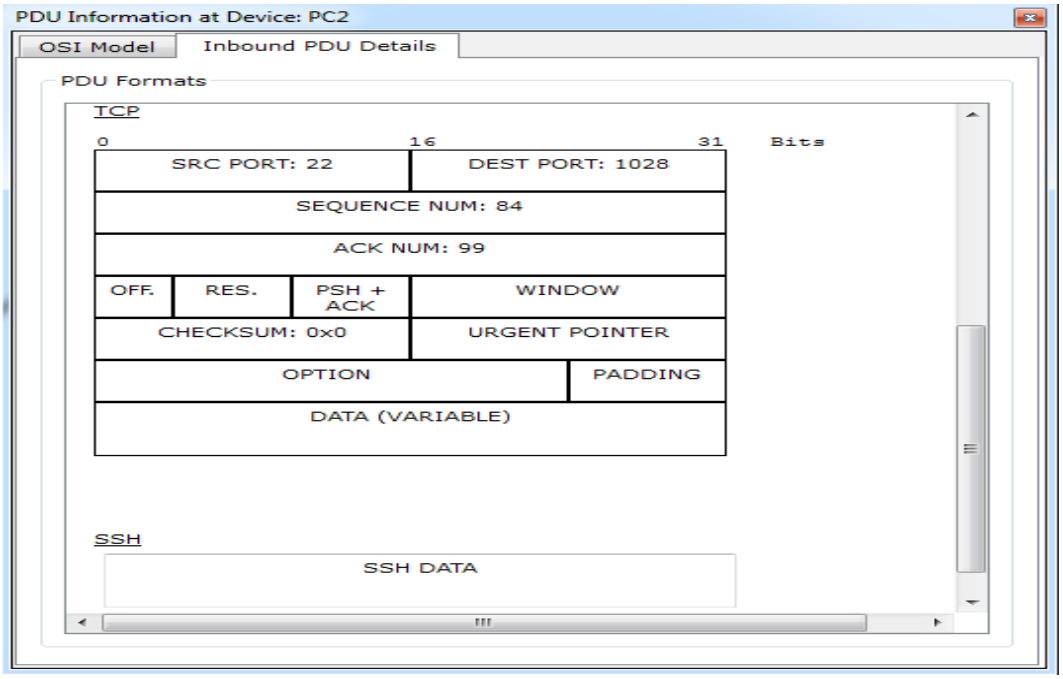
b) Shows OSI layers involved in transmission.

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).



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
OSI Model
Inbound PDU Details
PDU Formats
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