

# NATIONAL UNIVERSITY OF COMPUTER & EMERGING SCIENCE

## Computer Networks Lab (CL307)

### Lab Session 05

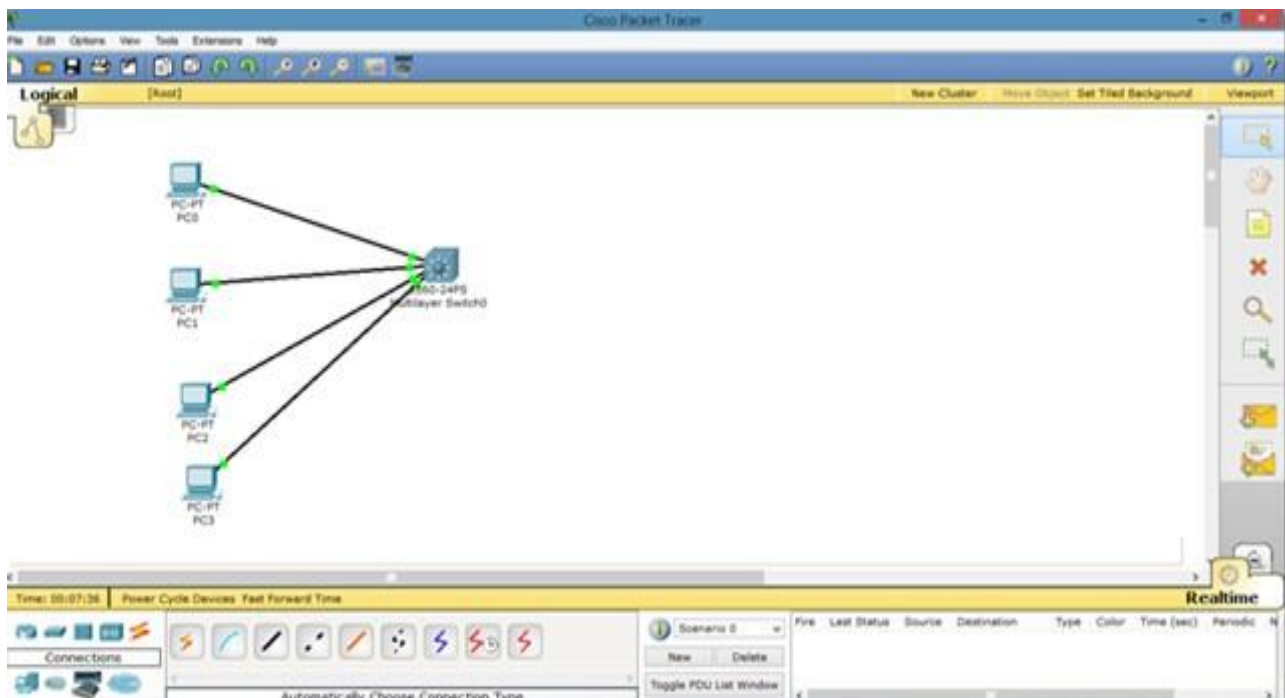
Awais Ahmed || Faizan Yousuf || Munim Ali Khan  
[awais.ahmed@nu.edu.pk](mailto:awais.ahmed@nu.edu.pk) || [faizan.yousuf@nu.edu.pk](mailto:faizan.yousuf@nu.edu.pk) || [munim.ali@nu.edu.pk](mailto:munim.ali@nu.edu.pk)

## 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.

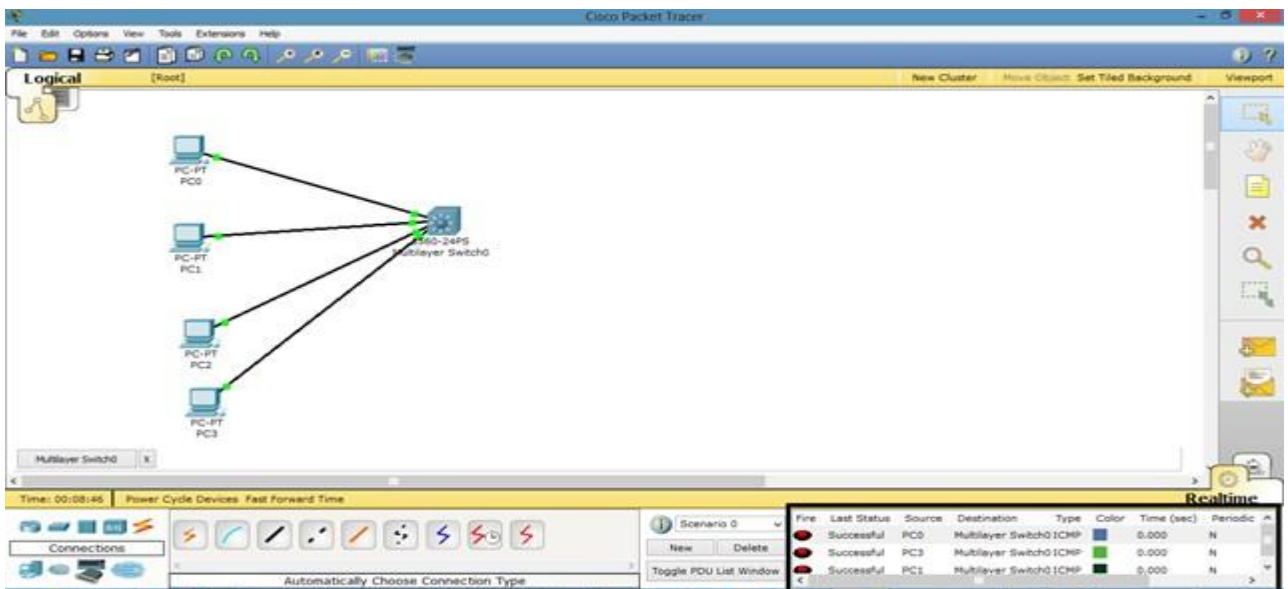
```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int
Switch(config)#interface vi
Switch(config)#interface vl
Switch(config)#interface vlan 1 ?
<cr>
Switch(config)#interface vlan 1
Switch(config-if)#ip ad
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
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.

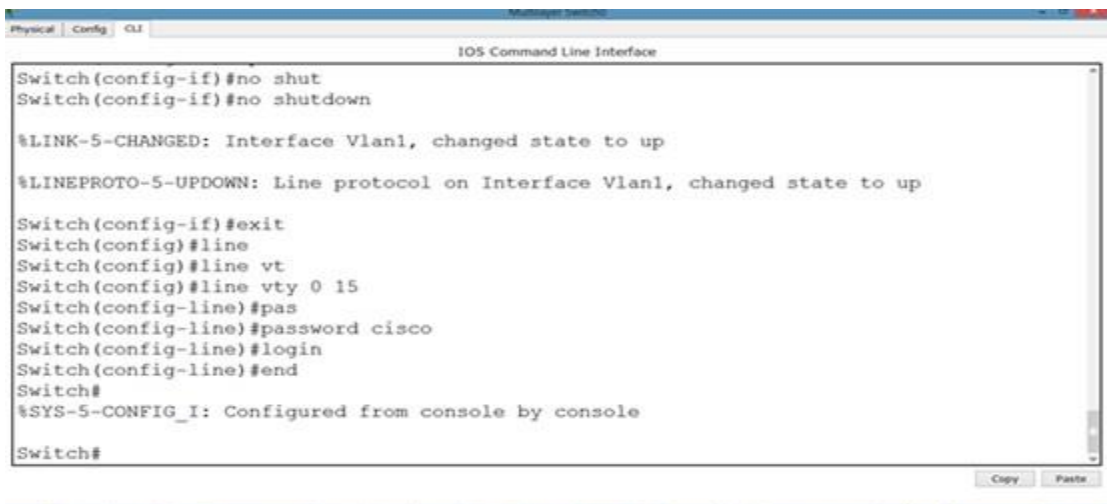


Now, try to telnet the switch from our PC, it refuses because we have not applied authentication on the switch yet.

```
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

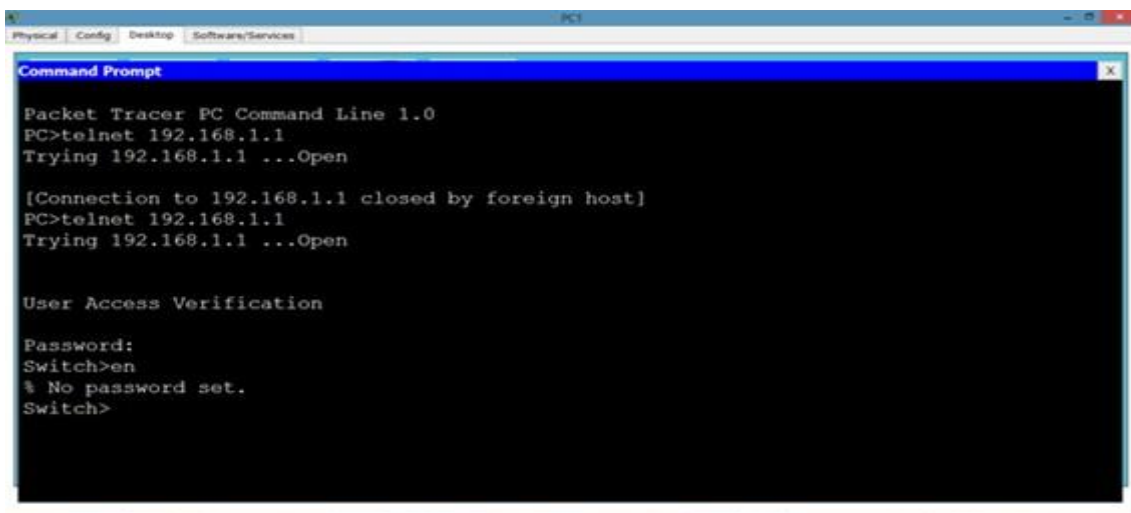
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%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.



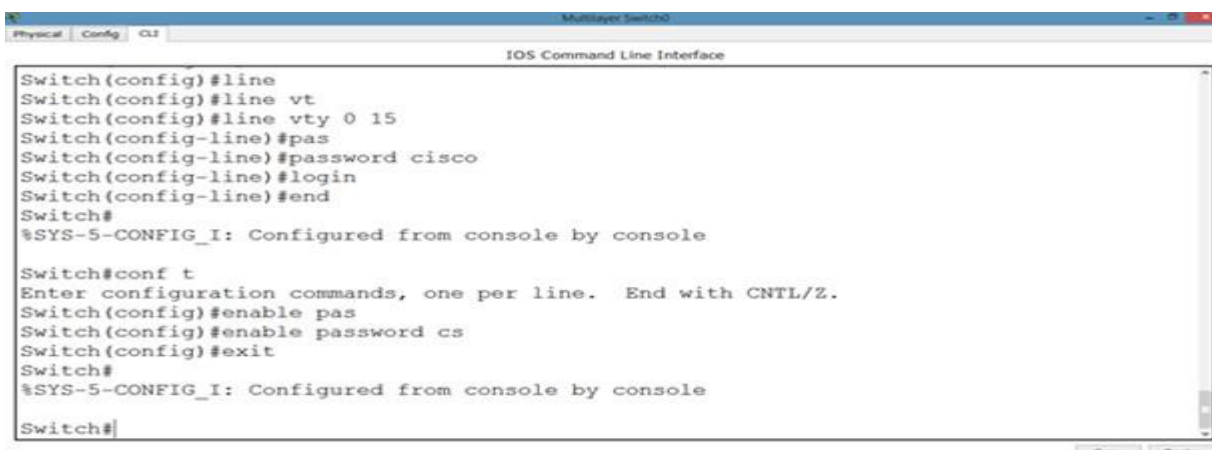
```
Packet Tracer PC Command Line 1.0
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

[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.

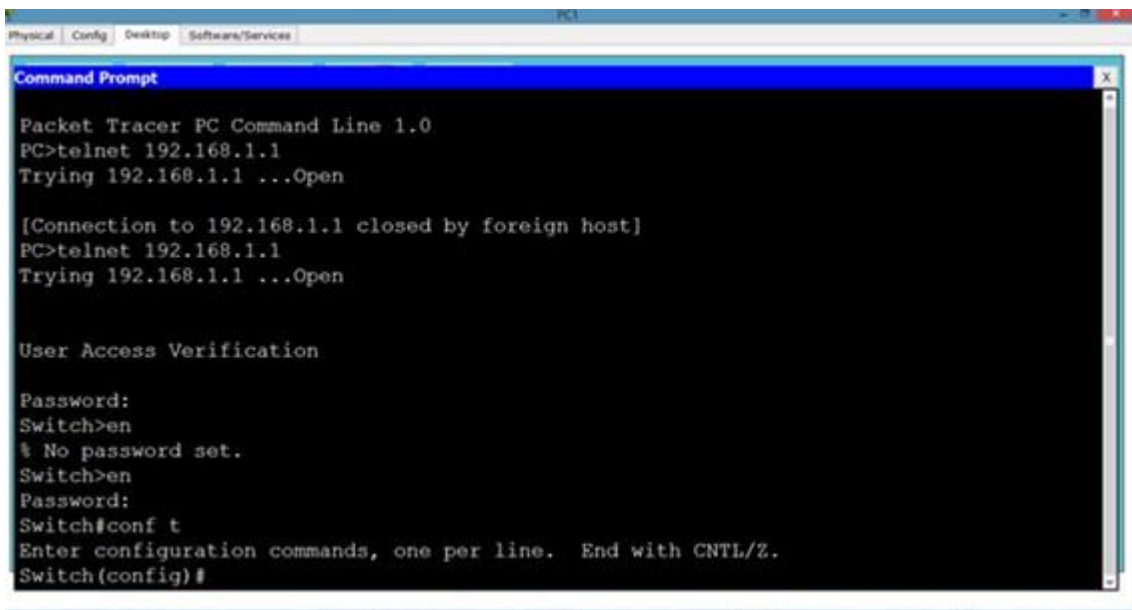


```
Switch(config)#line
Switch(config)#line vt
Switch(config)#line vty 0 15
Switch(config-line)#pas
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

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

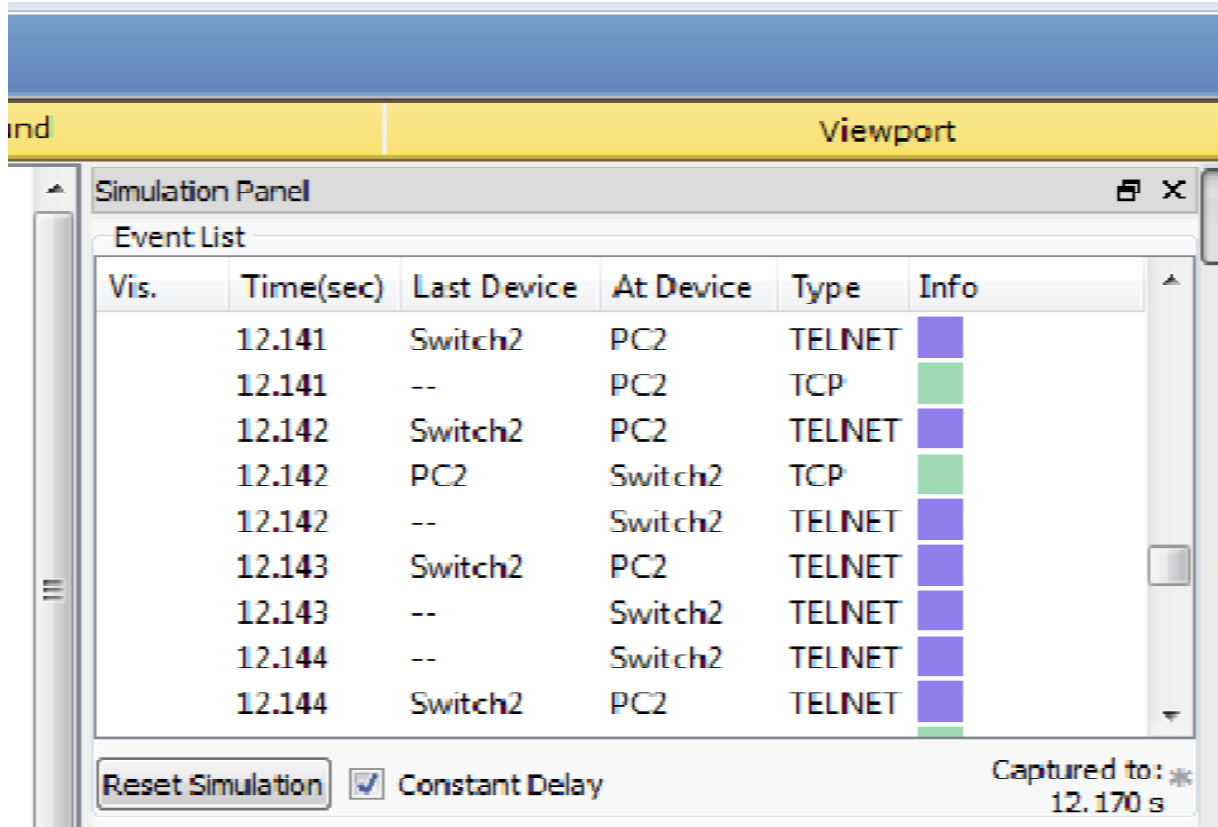
Switch#
```

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



### SIMULATION

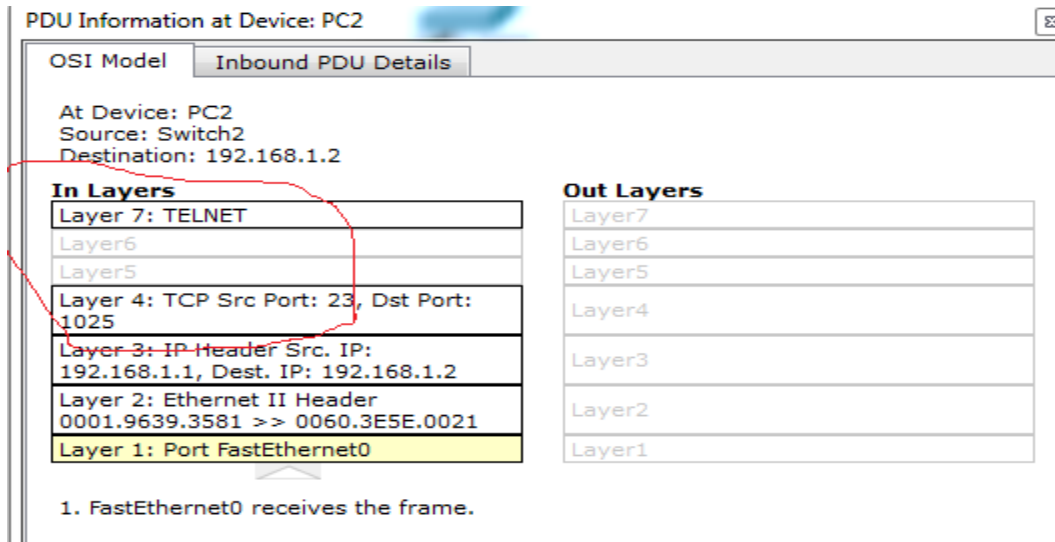
- a) Now click on simulation icon in the right bottom of packet Tracer.
- b) Now click on auto capture /play icon for packet capturing.
- c) Click on the PC and go to Desktop →Command Prompt then Telnet 192.168.1.1



**Now click on the TELNET packet show its header.**

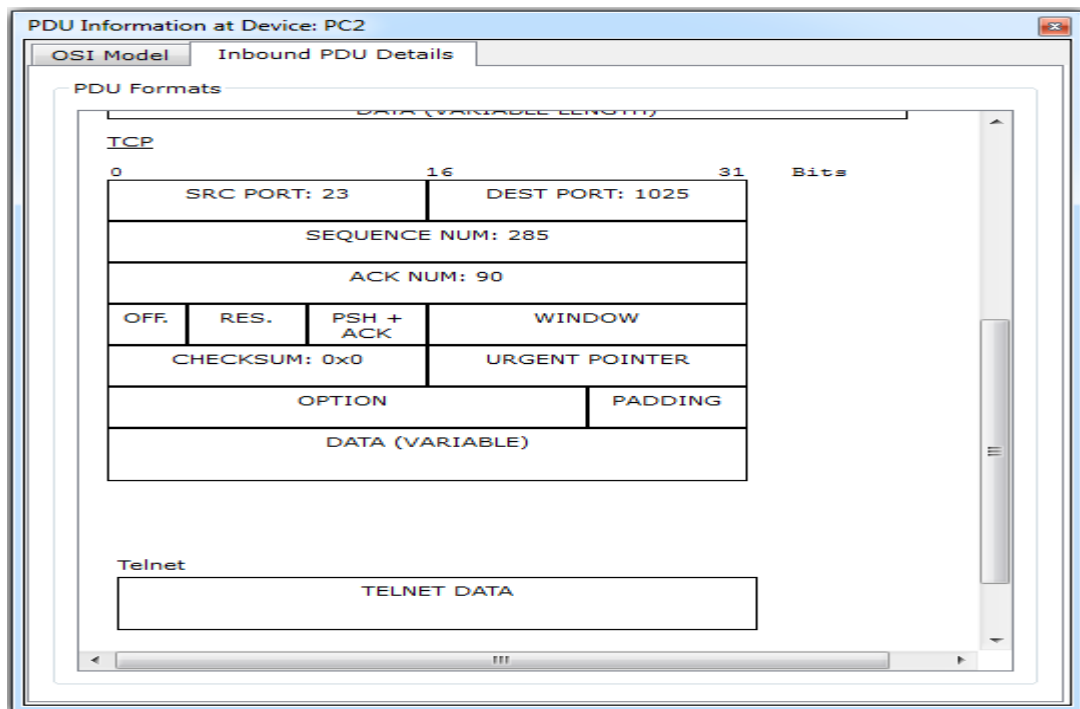
a) **Shows OSI layers involved in transmission.**

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.

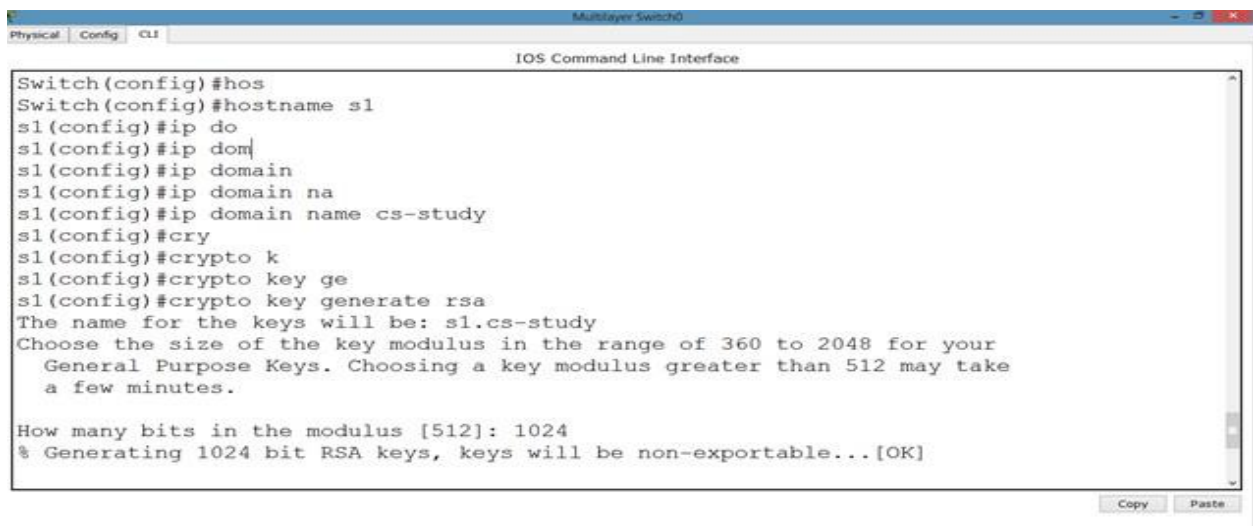


# SSH

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.

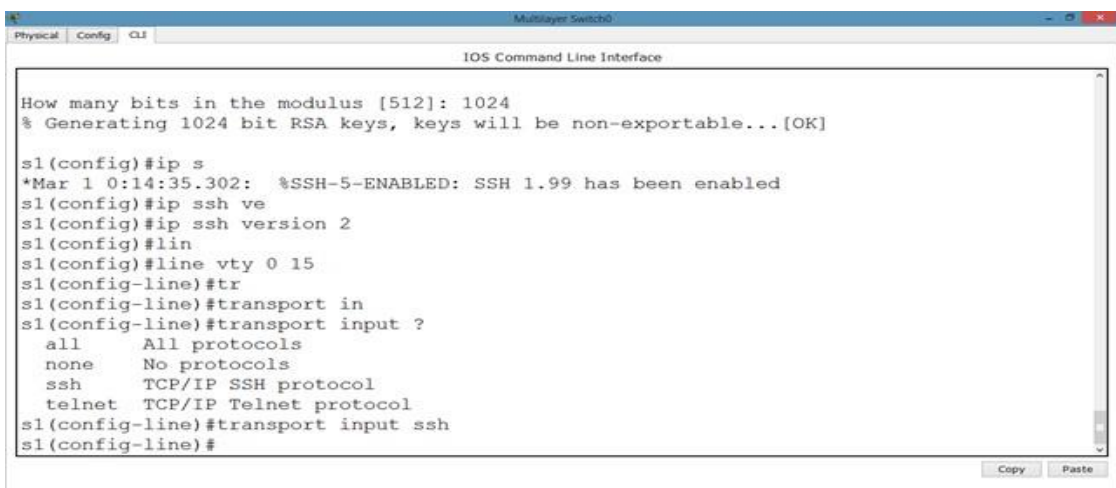
A network protocol that ensures a high-level encryption, allowing for the data transmitted over insecure networks, such as the Internet, to be kept intact and integrate. SSH and SSH Telnet, in particular, work for establishing a secure communication between two network-connected computers as an alternative 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.



```
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.

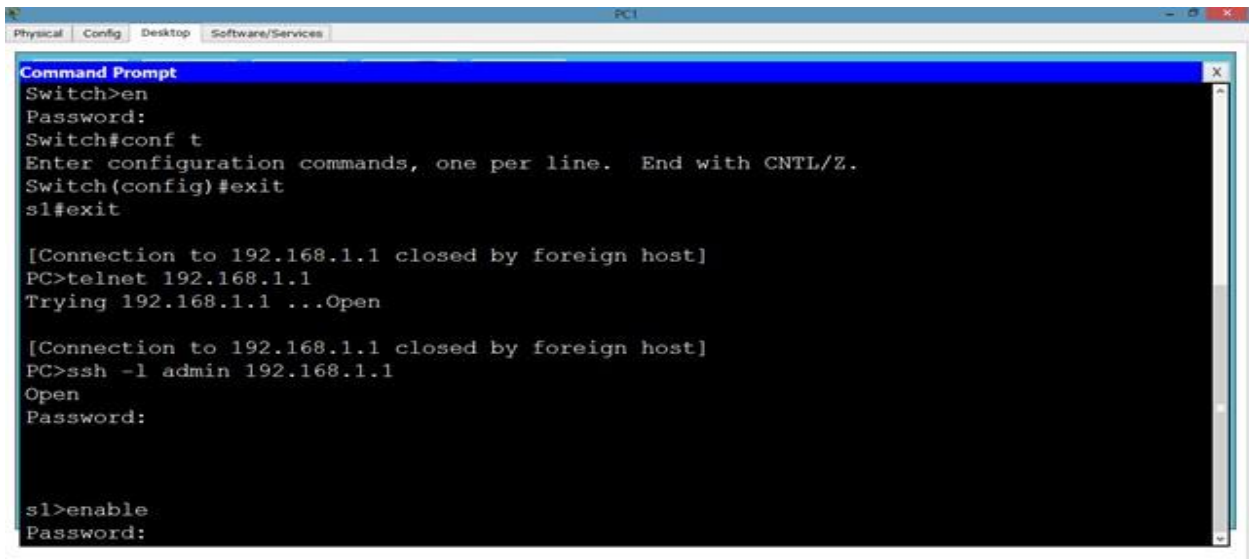
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```



```
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.



```
PC1
Physical Config Desktop Software/Services
Command Prompt
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.

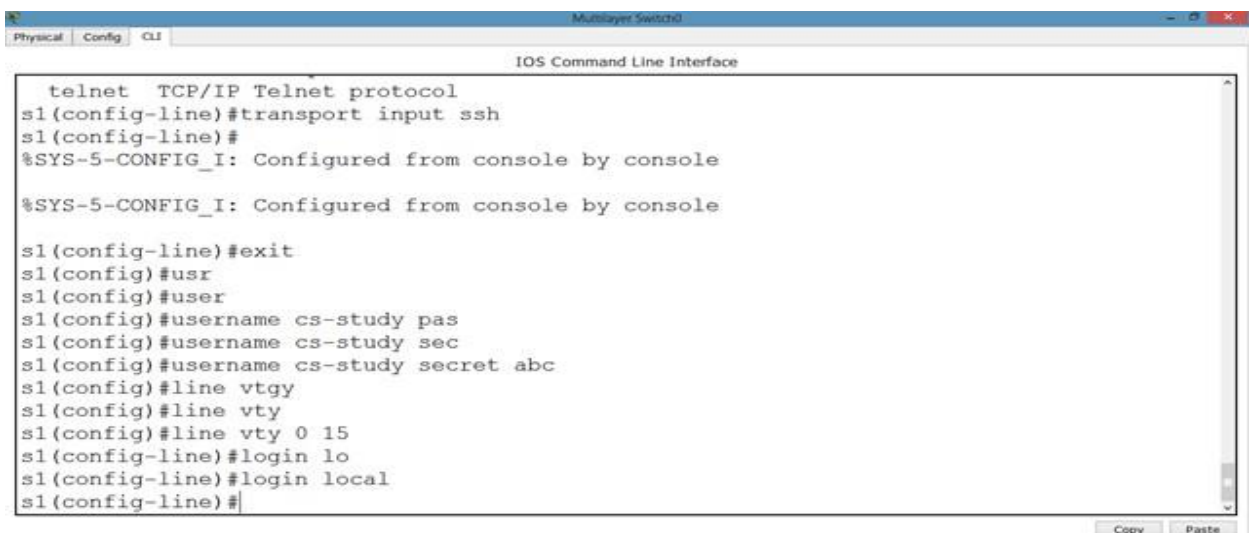


```
PC1
Physical Config Desktop Software/Services
Command Prompt
Trying 192.168.1.1 ...Open

[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.



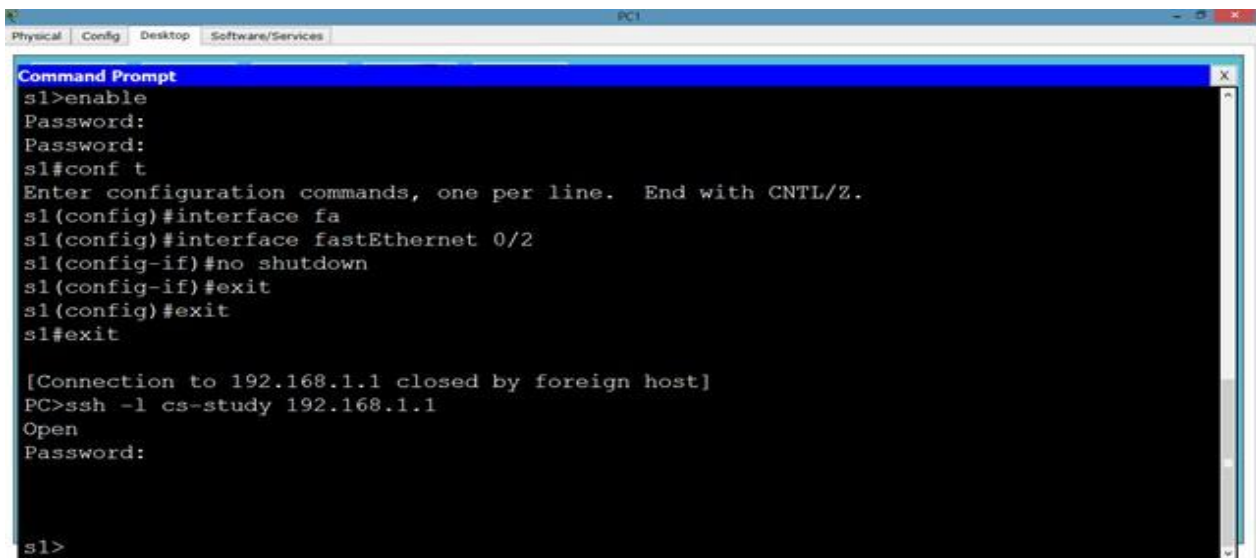
```
Multilayer Switch1
Physical Config CLI
IOS Command Line Interface

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 vty
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.

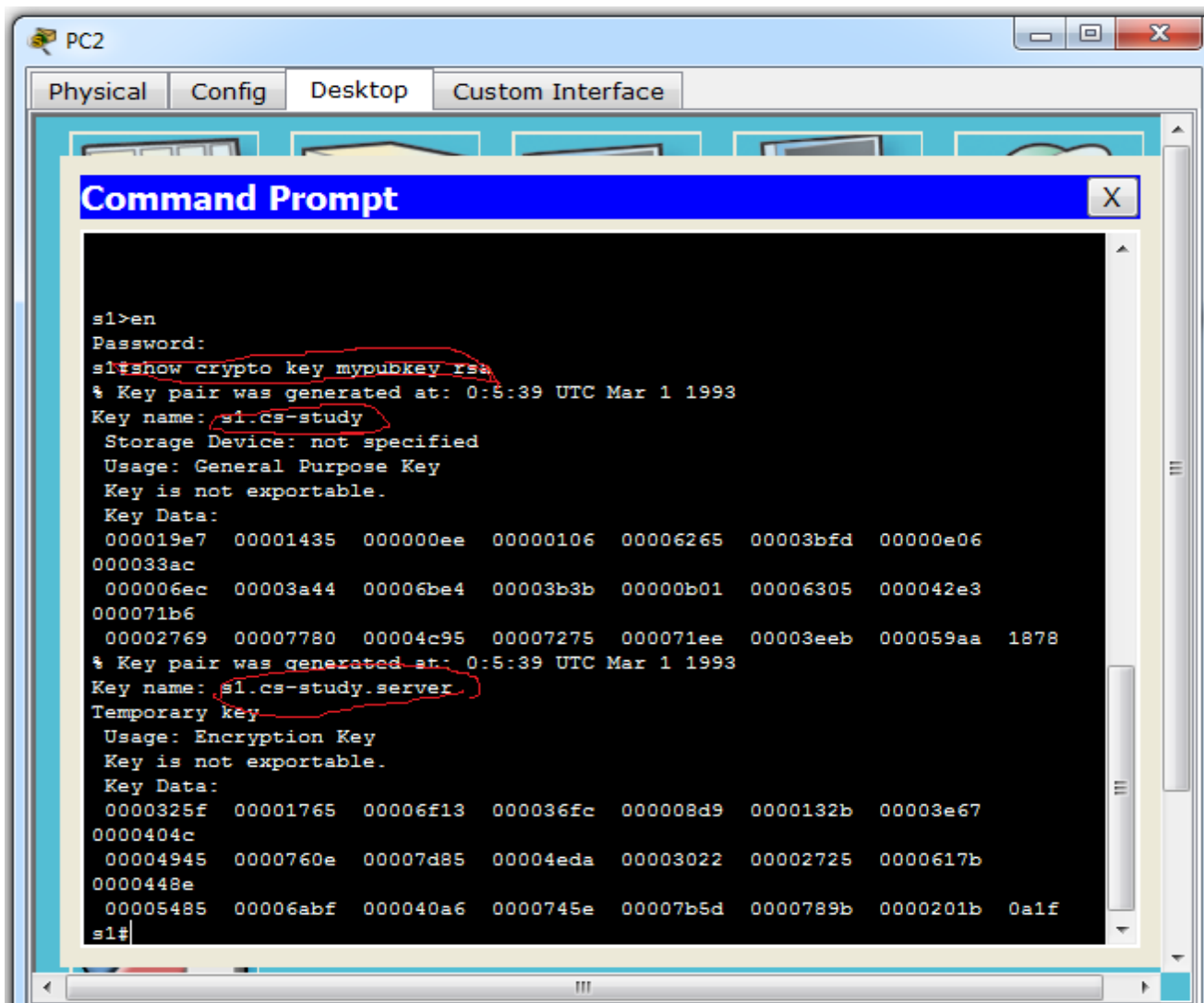


```
PC1
Physical Config Desktop Software/Services
Command Prompt
s1>enable
Password:
Password:
s1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
s1(config)#interface fa
s1(config)#interface fastEthernet 0/2
s1(config-if)#no shutdown
s1(config-if)#exit
s1(config)#exit
s1#exit

[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.



```
PC2
Physical Config Desktop Custom Interface
Command Prompt
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#
```

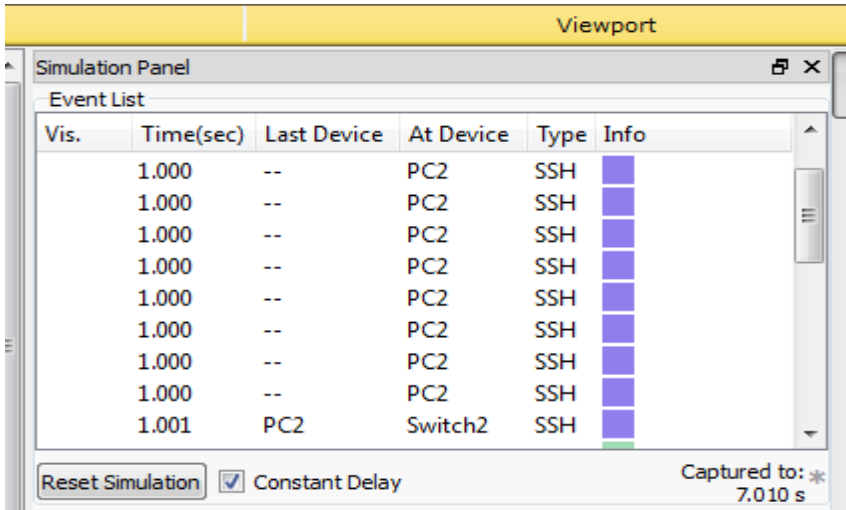


**SIMULATION:**

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

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

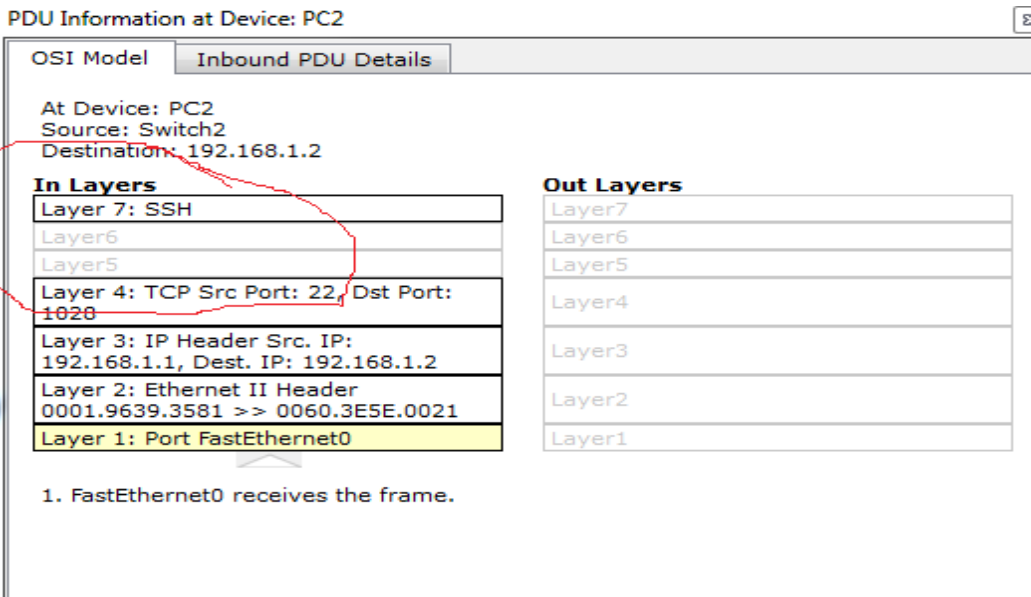
c) Click on the PC and go to Desktop → Command Prompt then ssh -l admin 192.168.1.1



**Now click on the SSH packet show its header.**

b) Shows OSI layers involved in transmission.

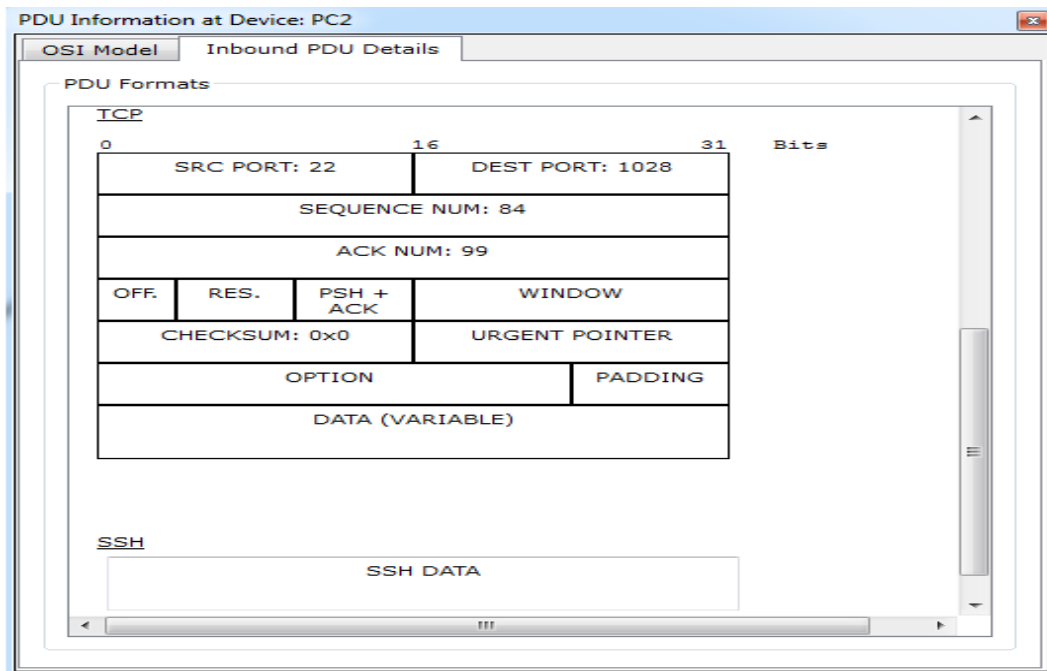
The popped up window (below) will enable you to trace the content of the message through the OSI layer and what changes will occur at each layer (use next and previous buttons to trace each layer content).



**b) Show Inbound PDU Details.**

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

process.



## Domain Name System

The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for the purpose of locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet.

An often-used analogy to explain the Domain Name System is that it serves as the phone book for the Internet by translating human-friendly computer hostnames into IP addresses. For example, the domain name `www.example.com` translates to the addresses `93.184.216.119` (IPv4) and `2606:2800:220:6d:26bf:1447:1097:aa7` (IPv6). Unlike a phone book, the DNS can be quickly updated, allowing a service's location on the network to change without affecting the end users, who continue to use the same host name. Users take advantage of this when they use meaningful Uniform Resource Locators (URLs), and e-mail addresses without having to know how the computer actually locates the services.

The Domain Name System distributes the responsibility of assigning domain names and mapping those names to IP addresses by designating authoritative name servers for each domain. Authoritative name servers are assigned to be responsible for their supported domains, and may delegate authority over sub domains to other name servers. This mechanism provides distributed and fault tolerant service and was designed to avoid the need for a single central database. Some common DNS record types are:

### A record:

The A record is one of the most commonly used record types in any DNS system. An A record is actually an address record, which means it maps a fully qualified domain name (FQDN) to an IP address. For example, an A record is used to point a domain name, such as "google.com", to the IP address of Google's hosting server, "74.125.224.147". This allows the end user to type in a human-readable domain, while the computer can continue working with numbers. The name in the A record is the host for your domain, and the domain name is automatically attached to your name.

### CNAME record:

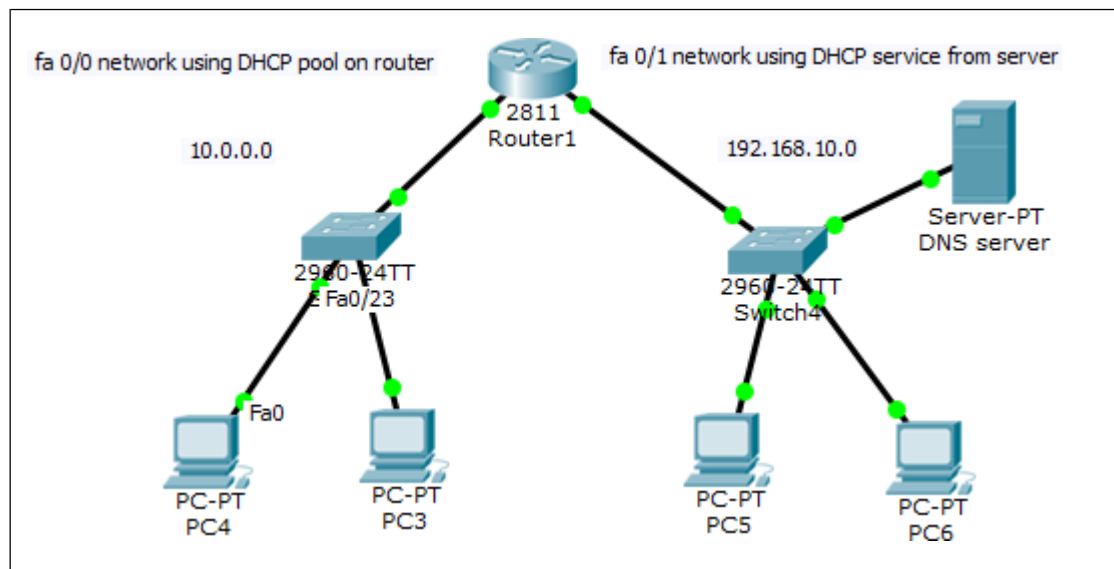
Canonical name records, or CNAME records, are often called alias records because they map an alias to the canonical name. When a name server finds a CNAME record, it replaces the name with the canonical name and looks up the new name. This allows pointing multiple systems to one IP without assigning an A record to each host name. It means that if you decide to change your IP address, you will only have to change one A record.

### NS record:

An NS record identifies which DNS server is authoritative for a particular zone. The "NS" stands for "name server". NS records that do not exist on the apex of a domain are primarily used for splitting up the management of records on sub-domains.

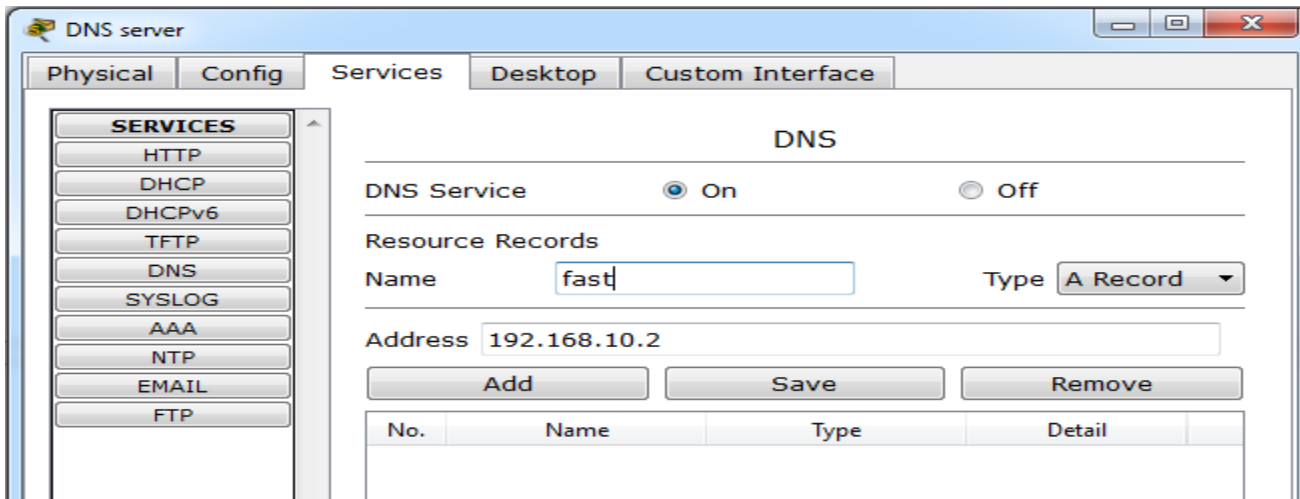
### SOA record:

The SOA or Start of Authority record for a domain stores information about the name of the server that supplies the data for the zone, the administrator of the zone and the current version of the data. It also provides information about the number of seconds a secondary name server should wait before checking for updates or before retrying a failed zone transfer.

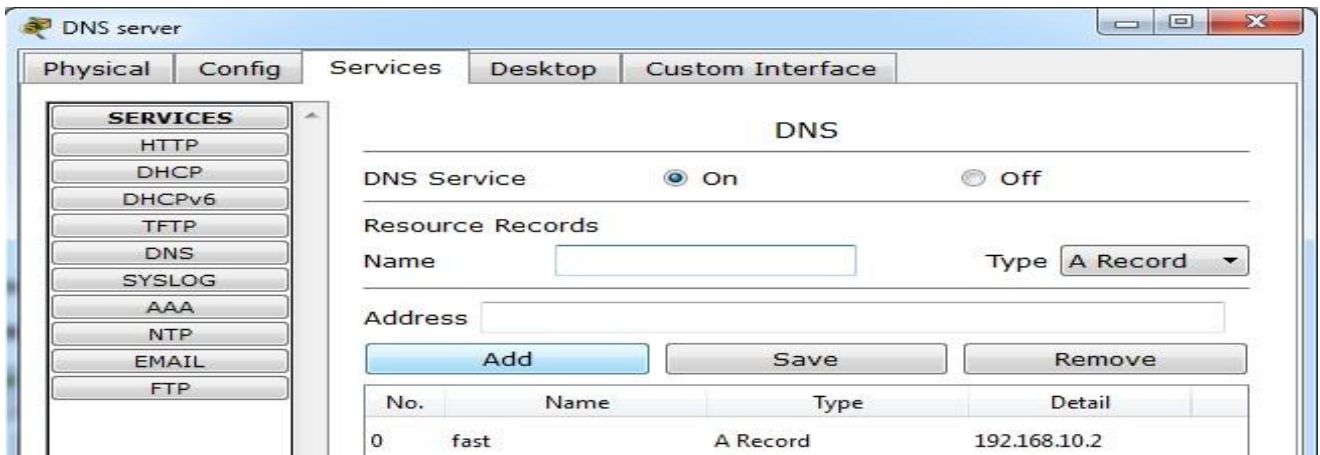


Now using the DNS service on Server0.Go to server

→services →DNS First we add A record.



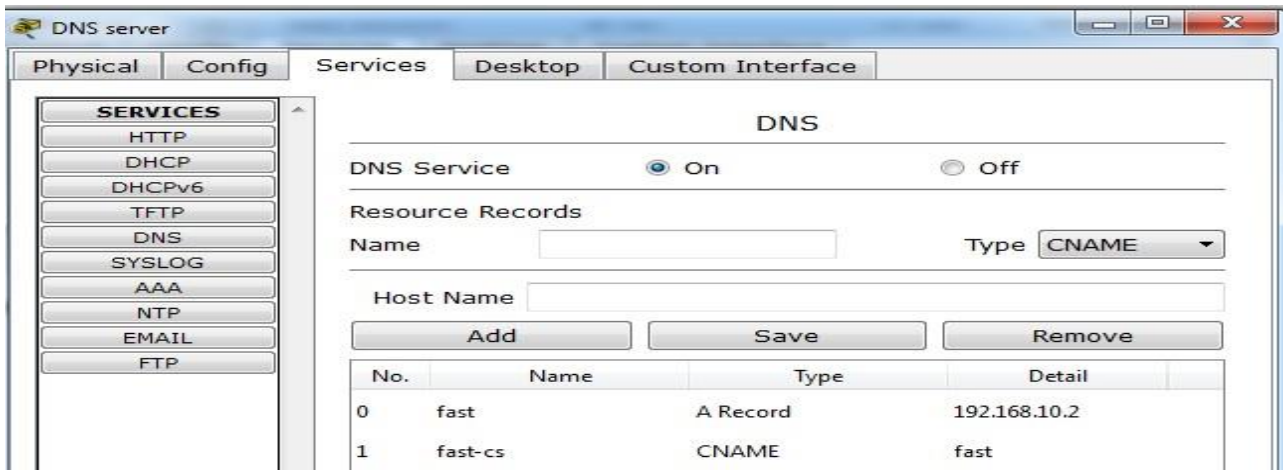
Now click on Add.



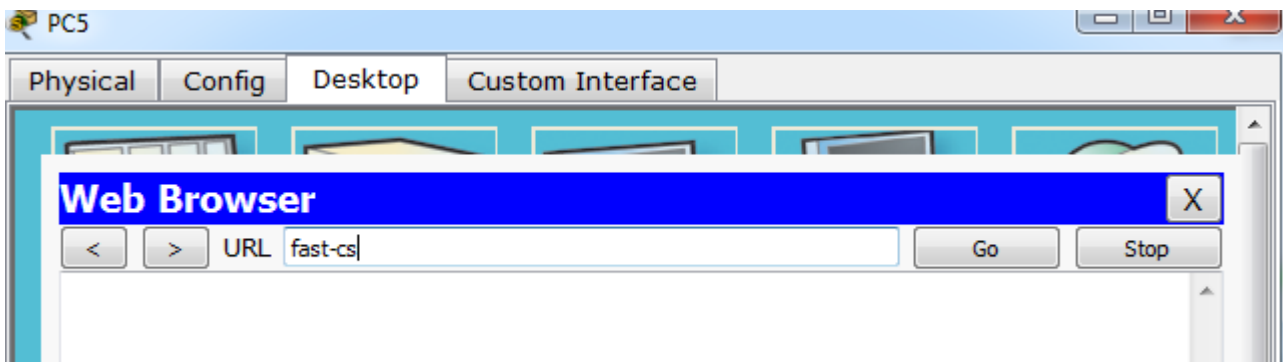
Now add Cname record.



Now click on Add.



Now go to pc5 → Desktop → web browser → type fast-cs and see how DNS works.



Start simulation.

The screenshot shows the 'Simulation Panel' with an 'Event List' table. The table contains the following data:

Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.006	Switch4	DNS server	DNS	
	0.007	DNS server	Switch4	DNS	
	0.008	--	PC5	TCP	
	0.008	Switch4	PC5	DNS	
	0.008	--	PC5	TCP	
	0.009	PC5	Switch4	TCP	
	0.010	Switch4	DNS server	TCP	
	0.011	DNS server	Switch4	TCP	
	0.012	Switch4	PC5	TCP	



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).

The screenshot shows a network analysis tool window titled "PDU Information at Device: DNS server". It has three tabs: "OSI Model", "Inbound PDU Details", and "Outbound PDU Details". The "OSI Model" tab is active. The window displays the following information:

At Device: DNS server  
Source: PC5  
Destination: 192.168.10.2

In Layers	Out Layers
Layer 7: DNS	Layer 7: DNS
Layer 6	Layer 6
Layer 5	Layer 5
Layer 4: UDP Src Port: 1025, Dst Port: 53	Layer 4: UDP Src Port: 53, Dst Port: 1025
Layer 3: IP Header Src. IP: 192.168.10.7, Dest. IP: 192.168.10.2	Layer 3: IP Header Src. IP: 192.168.10.2, Dest. IP: 192.168.10.7
Layer 2: Ethernet II Header 0030.F217.9616 >> 0001.C786.AC87	Layer 2: Ethernet II Header 0001.C786.AC87 >> 0030.F217.9616
Layer 1: Port FastEthernet0	Layer 1: Port(s): FastEthernet0

A red circle highlights the "Out Layers" section, specifically the Layer 4, 3, and 2 rows. A double-headed arrow is positioned between the "In Layers" and "Out Layers" columns.