NATIONAL UNIVERSITY OF COMPUTER & EMERGINGSCIENCE
Computer Network Lab (CL3001) Lab

Session 05

Objective:

- Introduction to DNS & configuration of DNS in Cisco Packet Tracer
- Introduction to SMTP & FTP in Cisco Packet Tracer

DNS in Cisco Packet Tracer

1. Introduction to DNS:

The Domain Name System (DNS) is a hierarchical and distributed naming system for computers, services, and other resources in the Internet or other Internet Protocol (IP) networks. It associates various information with domain names assigned to each of the associated entities. Most prominently, it translates readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols.[1] The Domain Name System has been an essential component of the functionality of the Internet since 1985.

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) 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.

b) 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 anA 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.

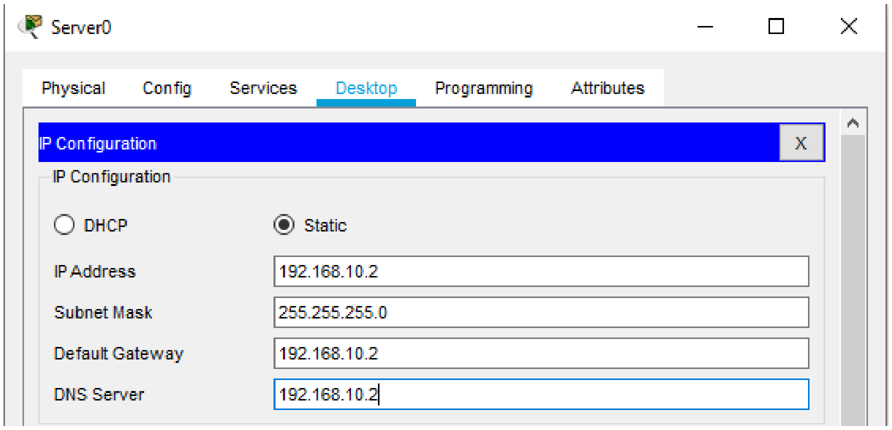
c) NS record:

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.

d) 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.

Assigning IP to DNS server & PCs.

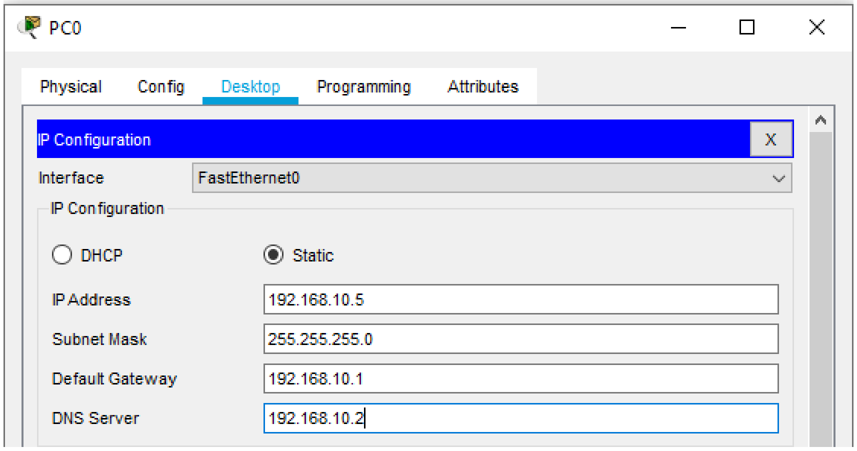


IP Configuration

○ DHCP ● Static

IP Address	192.168.10.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.2
DNS Server	192.168.10.2

Fig-1: DNS server



Interface: FastEthernet0

IP Configuration

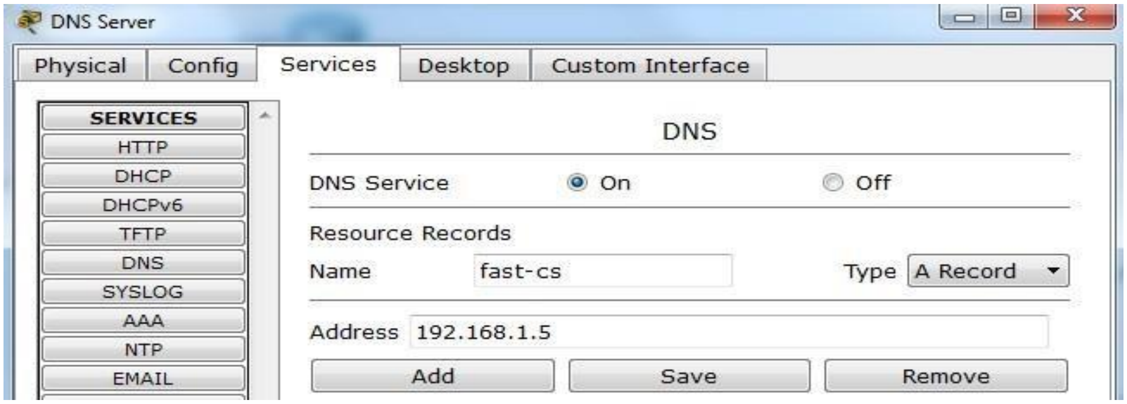
○ DHCP ● Static

IP Address	192.168.10.5
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
DNS Server	192.168.10.2

Fig-1: Provide IP to system through static IP

2. DNS Configuration & Simulation:

Now using the DNS service on DNS Server. Go to server services DNS.
First, we add A record. We assign the web server IP against our Domain name



DNS Service ● On ○ Off

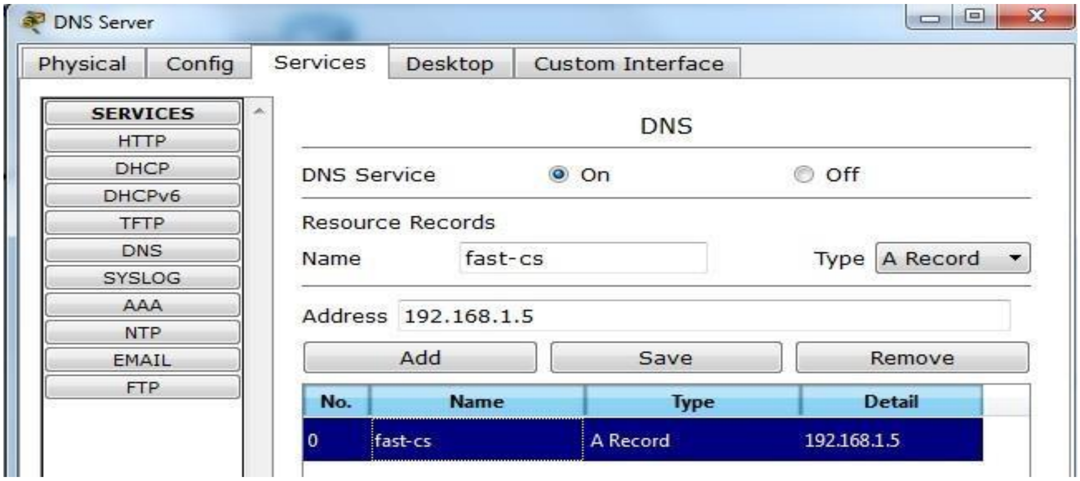
Resource Records

Name: fast-cs Type: A Record

Address: 192.168.1.5

Fig-3: DNS server configuration adding a record

Now click on Add.



DNS Service ● On ○ Off

Resource Records

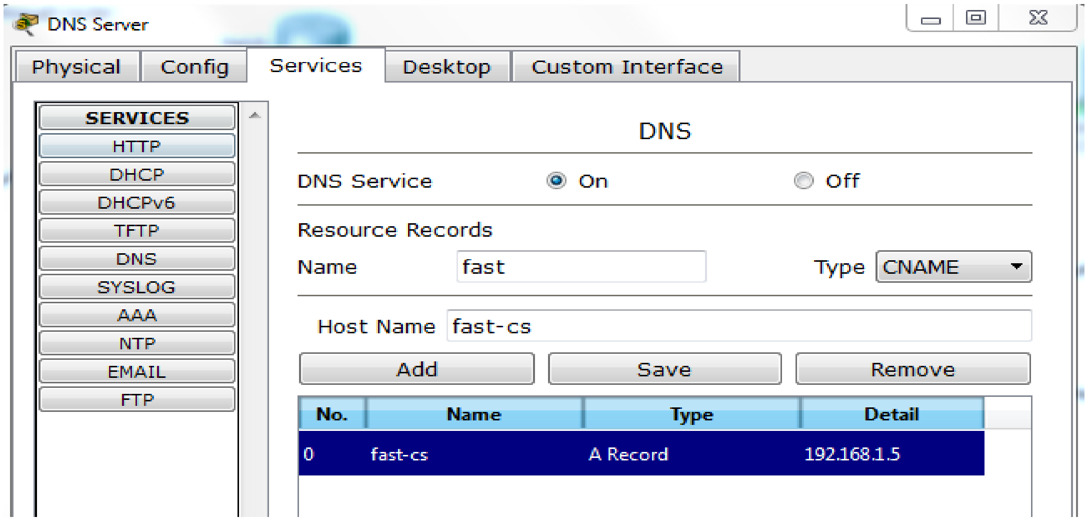
Name: fast-cs Type: A Record

Address: 192.168.1.5

No.	Name	Type	Detail
0	fast-cs	A Record	192.168.1.5

Fig-3: Record is added in DNS server

Now add Cname record.



DNS

DNS Service ● On ○ Off

Resource Records

Name: fast

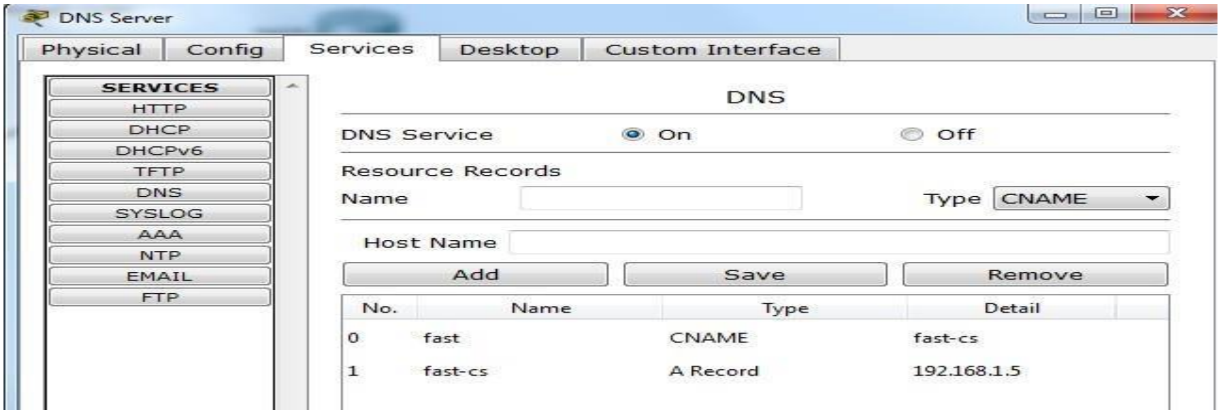
Type: CNAME

Host Name: fast-cs

No.	Name	Type	Detail
0	fast-cs	A Record	192.168.1.5

Fig-4: Adding CNAME record in DNS server

Now click on Add



DNS

DNS Service ● On ○ Off

Resource Records

Name

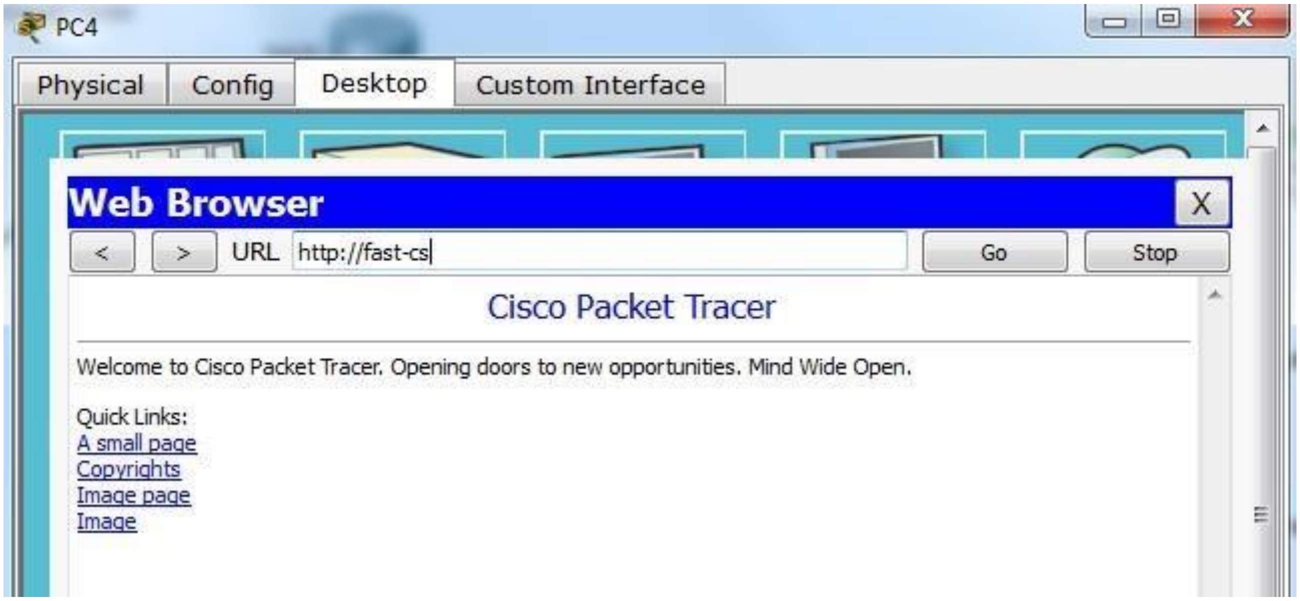
Type: CNAME

Host Name

No.	Name	Type	Detail
0	fast	CNAME	fast-cs
1	fast-cs	A Record	192.168.1.5

Fig-5: CNAME record is added in DNS server

Now go to PC4 →Desktop →web browser → type fast-cs and see how DNS works.



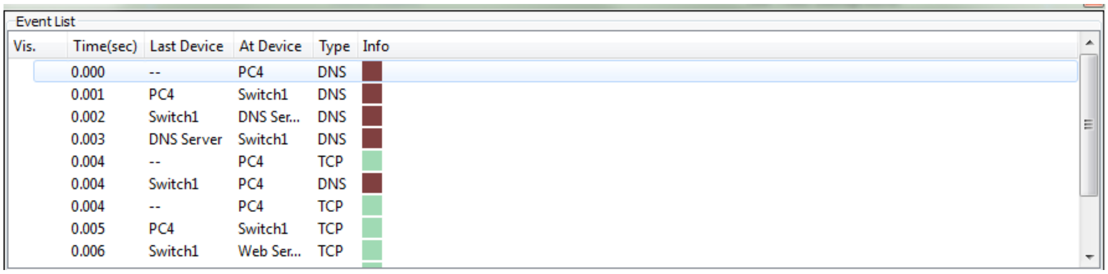
Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

Fig-6: Opening website

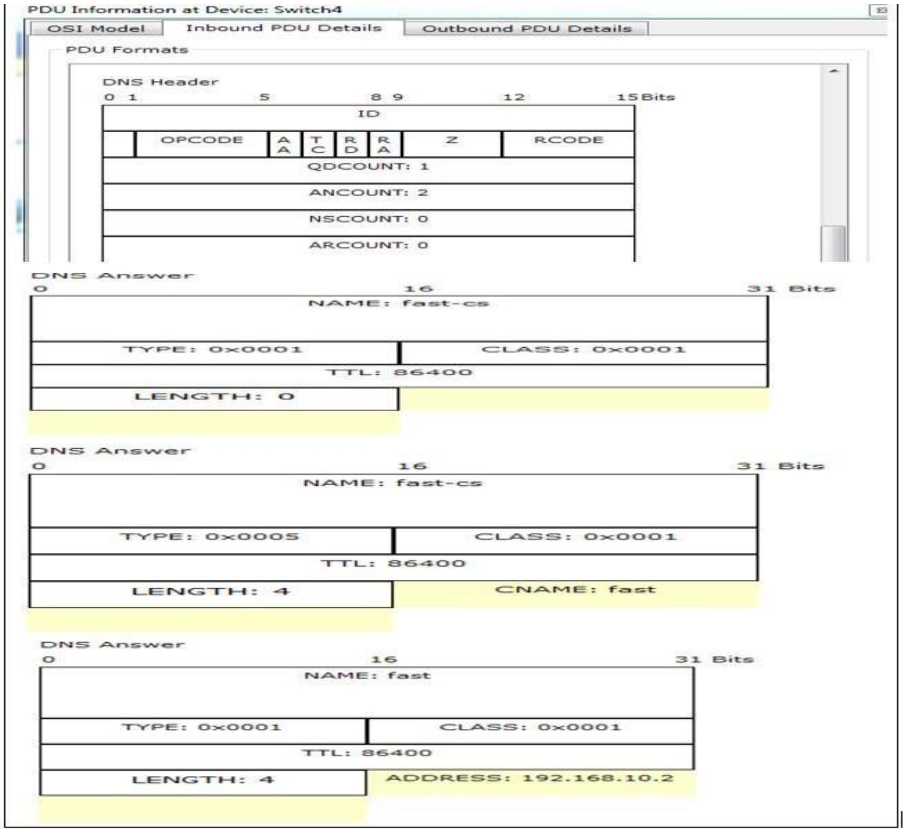
Start simulation.


Event List

Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.000	--	PC4	DNS	🟥
	0.001	PC4	Switch1	DNS	🟥
	0.002	Switch1	DNS Ser...	DNS	🟥
	0.003	DNS Server	Switch1	DNS	🟥
	0.004	--	PC4	TCP	🟩
	0.004	Switch1	PC4	DNS	🟥
	0.004	--	PC4	TCP	🟩
	0.005	PC4	Switch1	TCP	🟩
	0.006	Switch1	Web Ser...	TCP	🟩

Fig-7: Packets exchange in DNS simulation

Click on DNS packet. See how DNS server resolved the name.



PDU Information at Device: Switch4

OSI Model | Inbound PDU Details | Outbound PDU Details

PDU Formats

DNS Header

0 1 5 8 9 12 15 Bits

ID

OPCODE | AA | TC | RD | RA | Z | RCODE

QDCOUNT: 1

ANCOUNT: 2

NSCOUNT: 0

ARCOUNT: 0

DNS Answer

0 16 31 Bits

NAME: fast-cs

TYPE: 0x0001 | CLASS: 0x0001

TTL: 86400

LENGTH: 0

DNS Answer

0 16 31 Bits

NAME: fast-cs

TYPE: 0x0005 | CLASS: 0x0001

TTL: 86400

LENGTH: 4 | CNAME: fast

DNS Answer

0 16 31 Bits

NAME: fast

TYPE: 0x0001 | CLASS: 0x0001

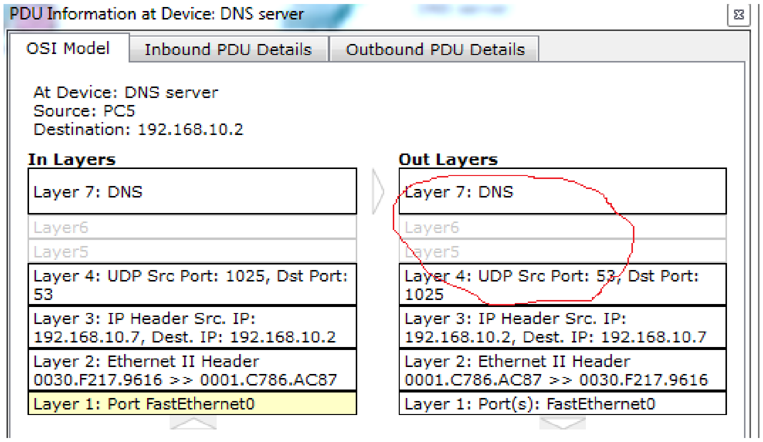
TTL: 86400

LENGTH: 4 | ADDRESS: 192.168.10.2

Fig-8: DNS header request & reply to resolve domain name

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 whatchanges will occur at each layer (use next and previous buttons to trace each layer content).



PDU Information at Device: DNS server

OSI Model | Inbound PDU Details | Outbound PDU Details

At Device: DNS server
Source: PC5
Destination: 192.168.10.2

In Layers	Out Layers
Layer 7: DNS	Layer 7: DNS
Layer6	Layer6
Layer5	Layer5
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

Fig-9: Showing OSI layer involvement in DNS

LAB EXERCISE:

1. Implement the given topology.
2. Add some web servers in your network.
3. Implement DNS & add records of your web servers.

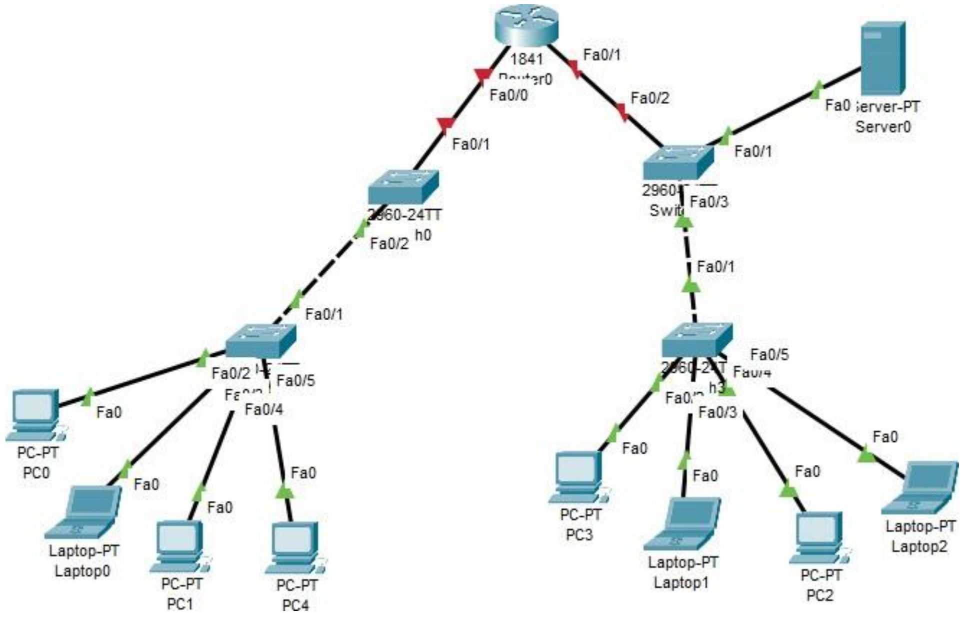


Fig-10: Network topology for task

SMTP

1. Introduction:

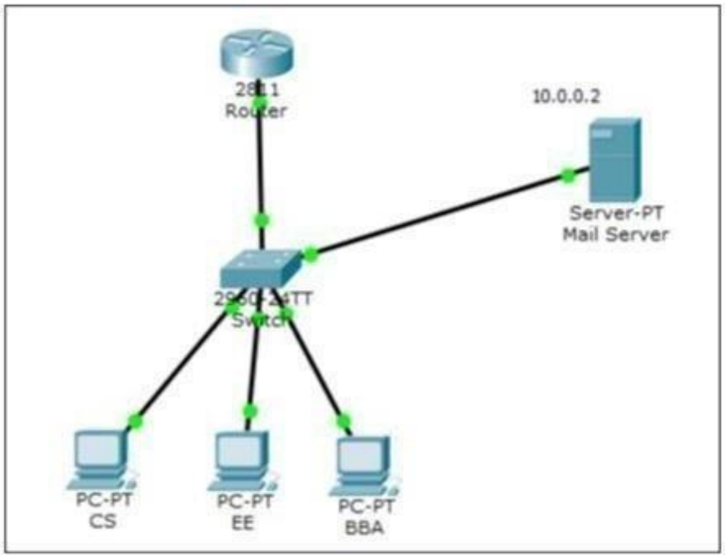
Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (email) transmission. First defined by RFC 821 in 1982, it was last updated in 2008 with Extended SMTP additions by RFC 5321,which is the protocol in widespread use today. Although electronic mail servers and other mail transfer agents use SMTP to send and receive mail messages, user-level client mail applications typically use SMTPonly for sending messages to a mail server for relaying. For retrieving messages, client applications usuallyuse either IMAP or POP3.

SMTP communication between mail servers uses port 25. Mail clients on the other hand, often submit theoutgoing emails to a mail server on port 587. Despite being deprecated, mail providers sometimes still permit the use of nonstandard port 465 for this purpose. SMTP runs over TCP.

2. Implementation:

Topology:

Construct thetopology shown in figure 1. Turn on router interface& assign IP's to PC using DHCP throughrouter as done in pervious lab. Assign static IP to email server.



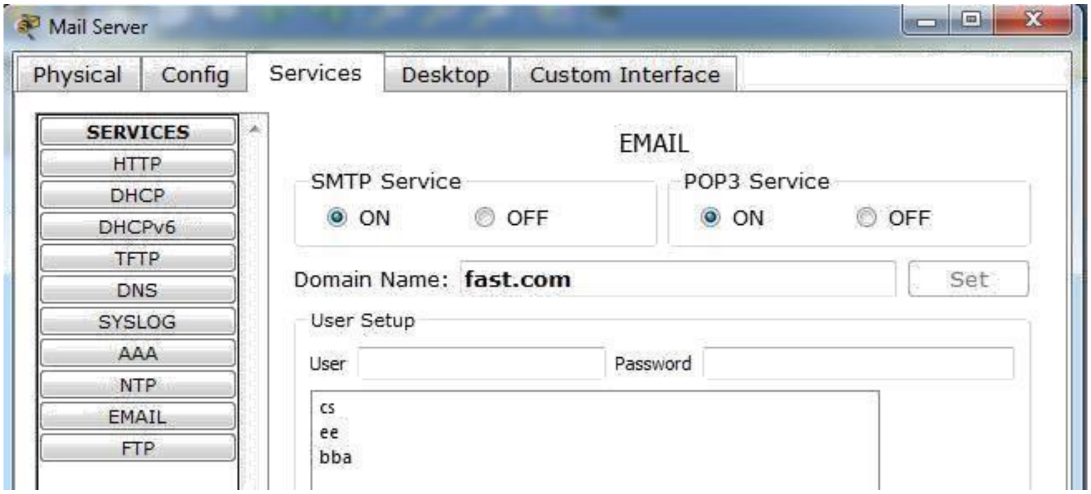
Configure and Verify Email Services

- Click on Mail server
- Go to services & then email services
- Enable SMTP & POP3 Service
- Set Domain name fast.com
- Add following users

Username	Password
CS	123
BBA	456
EE	789

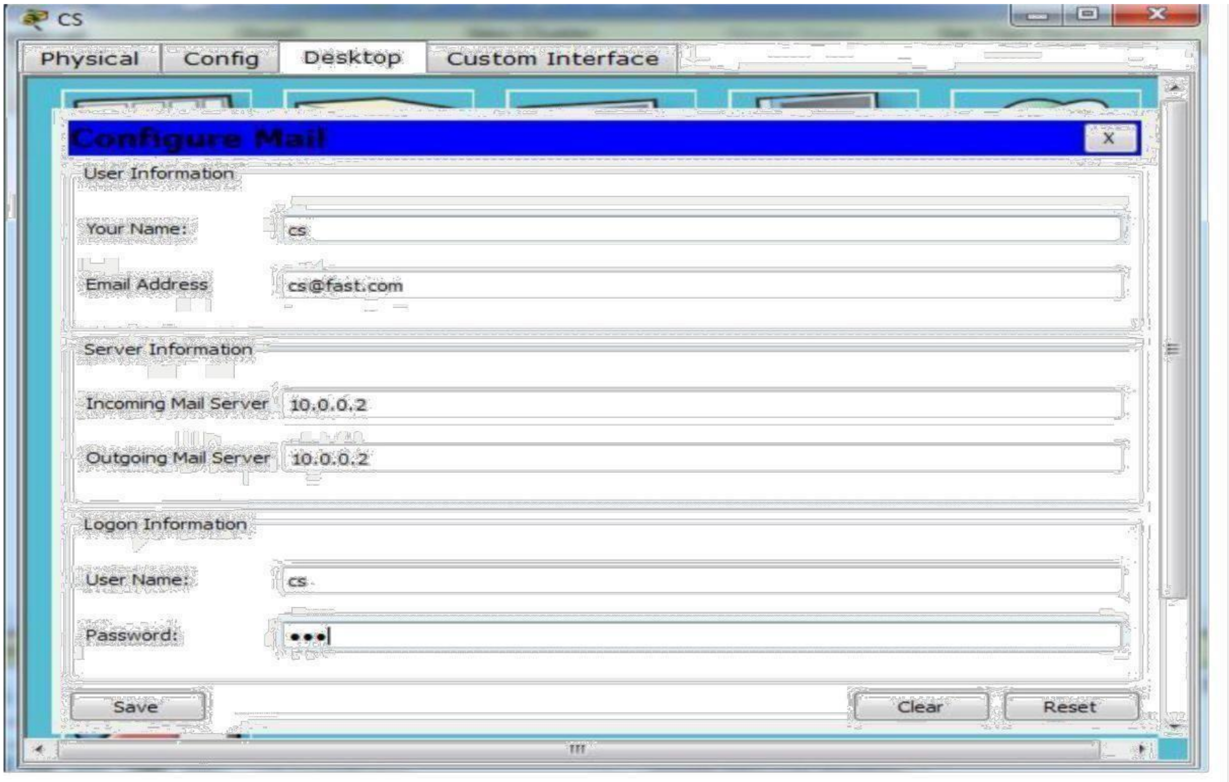
Table-1: User name & their passwords

Now configure user email account.
Goto PC → Desktop → Email
Fill the following fields as shown in figure 3.
Click "Save" to save the configurations and do the same for EE and BBA.



SMTP Service ● ON ○ OFF
POP3 Service ● ON ○ OFF
Domain Name: fast.com
User
Password

cs
ee
bba



Configure Mail

User Information

Your Name: cs

Email Address cs@fast.com

Server Information

Incoming Mail Server 10.0.0.2

Outgoing Mail Server 10.0.0.2

Logon Information

User Name: cs

Password: •••

Fig-3: User Email configuration

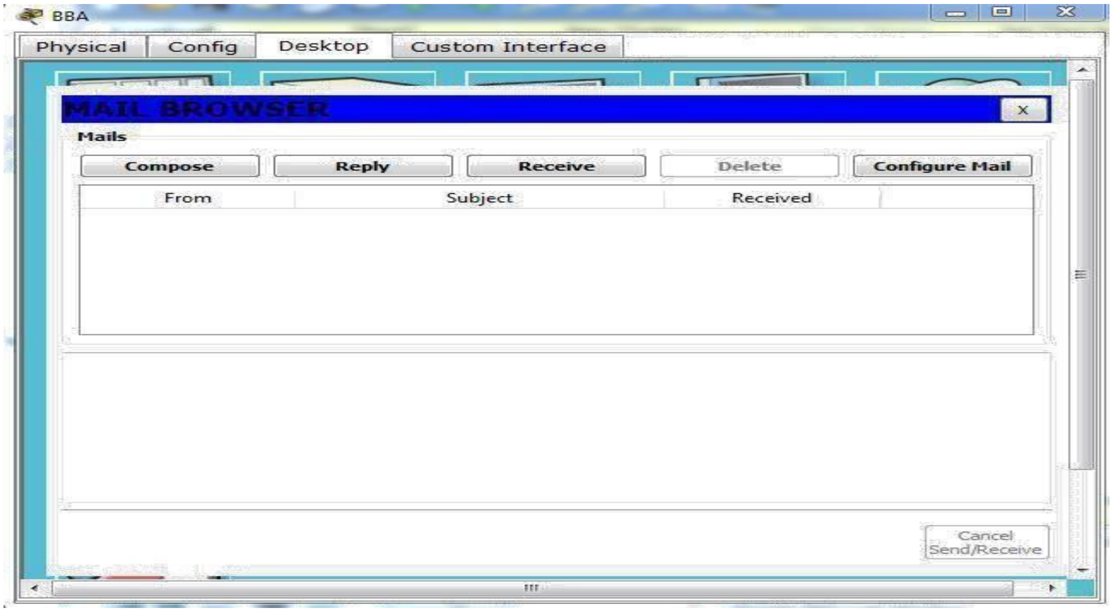
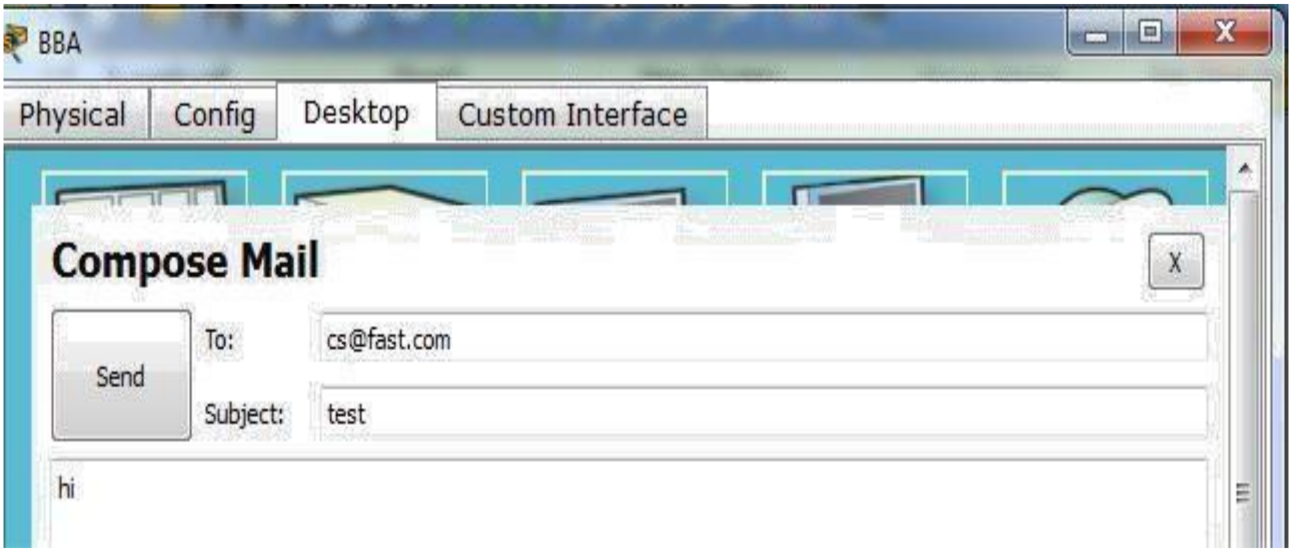


Fig-4: Mail browser view of user PC after mail configuration

Now compose email cs@fast.com

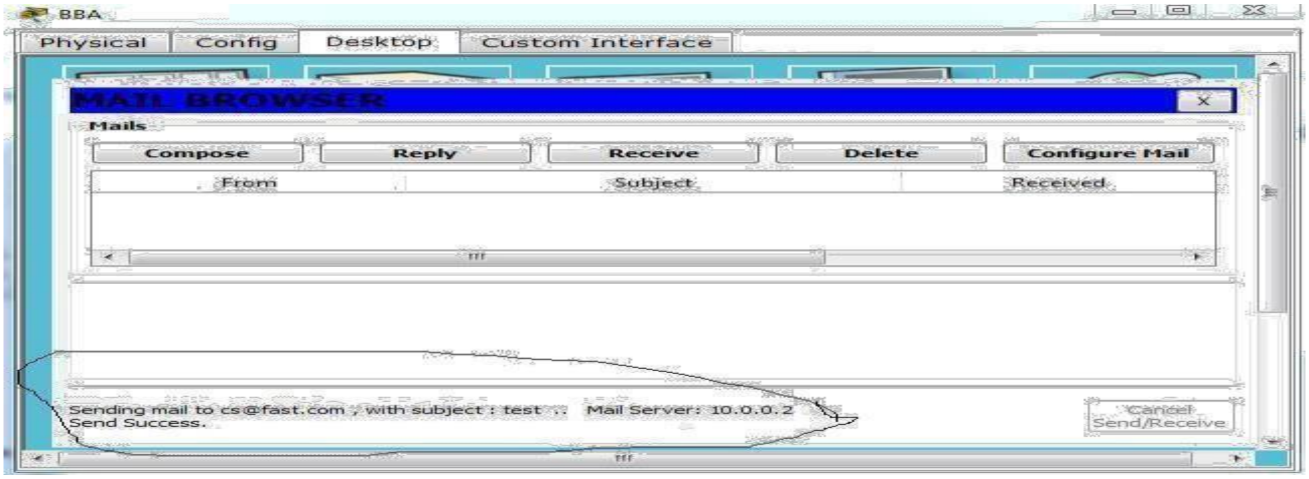


To: cs@fast.com

Subject: test

hi

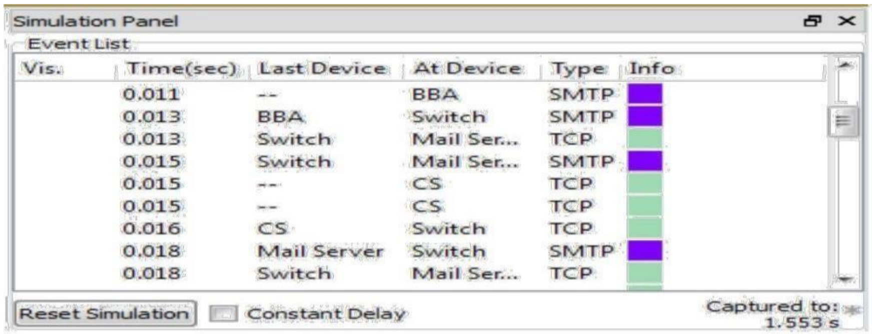
Click on “Send” to send Email.



```
Sending mail to cs@fast.com , with subject : test ..   Mail Server: 10.0.0.2
Send Success.
```

Simulation:

To note POP 3 header format information, go to simulation mode □ edit filters & check SMTP & POP 3 boxes. After that click on capture/forward button. Now see how mail server works

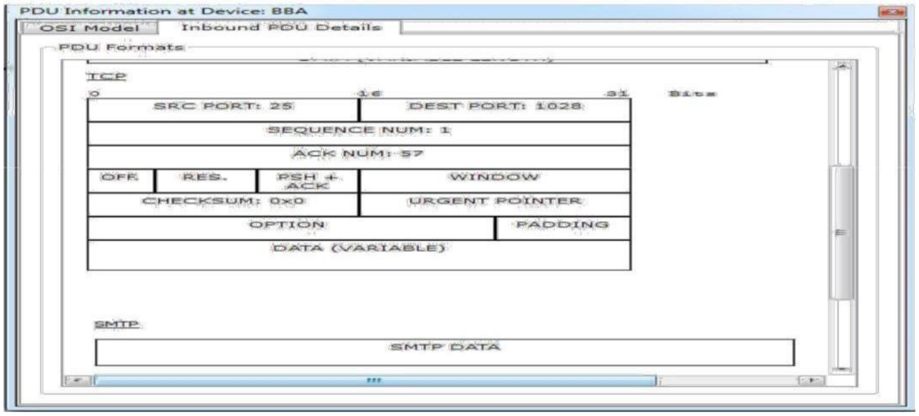


Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.011	--	BBA	SMTP	🟪
	0.013	BBA	Switch	SMTP	🟪
	0.013	Switch	Mail Ser...	TCP	🟩
	0.015	Switch	Mail Ser...	SMTP	🟪
	0.015	--	CS	TCP	🟩
	0.015	--	CS	TCP	🟩
	0.016	CS	Switch	TCP	🟩
	0.018	Mail Server	Switch	SMTP	🟪
	0.018	Switch	Mail Ser...	TCP	🟩

Captured to: 1.553 s



PDU Information at Device: BBA

TCP

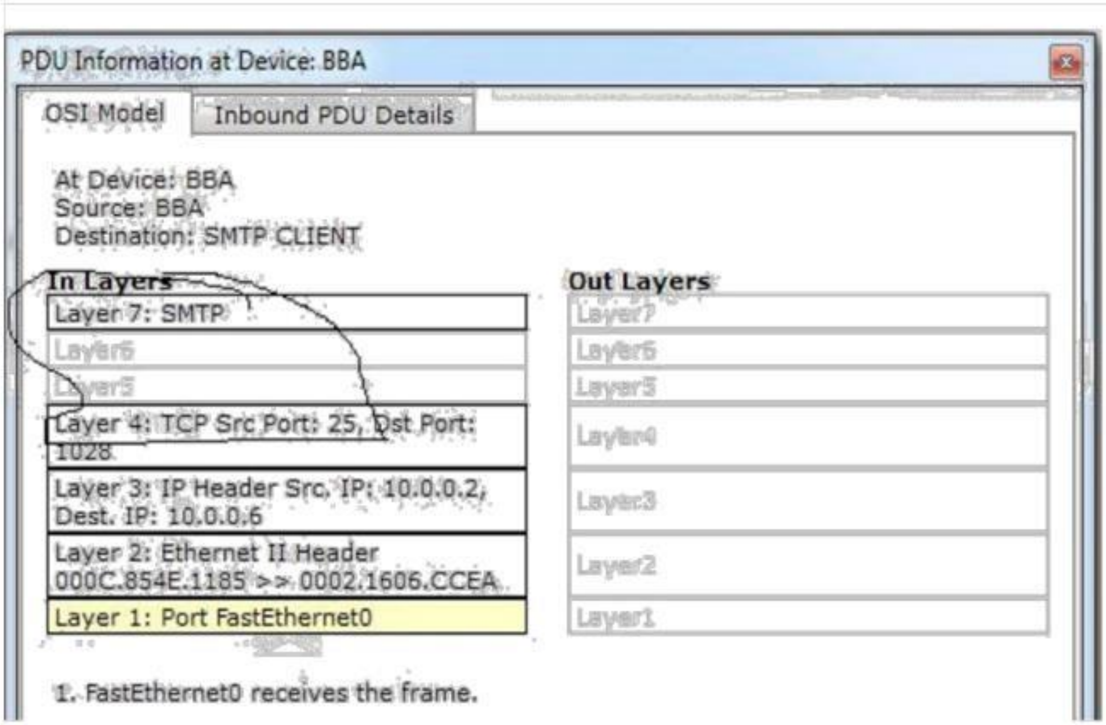
0 16 31 Bits

SRC PORT: 25		DEST PORT: 1028	
SEQUENCE NUM: 1			
ACK NUM: 57			
OFF.	RES.	PSH + ACK	WINDOW
CHECKSUM: 0x0		URGENT POINTER	
OPTION			PADDING
DATA (VARIABLE)			

SMTP

SMTP DATA

Fig-7: Packets capture in simulation mode & their PDU detail

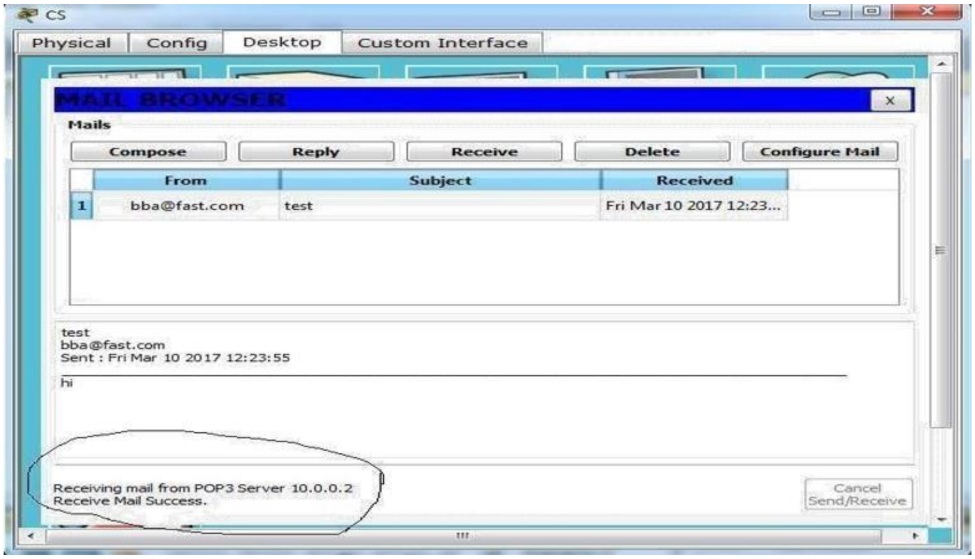


At Device: BBA
Source: BBA
Destination: SMTP CLIENT

In Layers	Out Layers
Layer 7: SMTP	Layer7
Layer6	Layer6
Layer5	Layer5
Layer 4: TCP Src Port: 25, Dst Port: 1028	Layer4
Layer 3: IP Header Src. IP: 10.0.0.2, Dest. IP: 10.0.0.6	Layer3
Layer 2: Ethernet II Header 000C.854E.1185 >> 0002.1606.CCEA	Layer2
Layer 1: Port FastEthernet0	Layer1

1. FastEthernet0 receives the frame.

Fig-8: OSI layer information about protocols at each layer in sending mail packet.



	From	Subject	Received
1	bba@fast.com	test	Fri Mar 10 2017 12:23...

test
bba@fast.com
Sent : Fri Mar 10 2017 12:23:55

hi

Receiving mail from POP3 Server 10.0.0.2
Receive Mail Success.

FTP

Introduction:

The File Transfer Protocol (FTP) is a standard network protocol used to transfer computer files between a client and server on a computer network. FTP is built on client-server model architecture and uses separate control and data connections between the client and the server. FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS) or replaced with SSH File Transfer Protocol (SFTP). FTP uses TCP as its under layer transport protocol for data reliability transfer. It uses port 21.

FTP may run in active or passive mode, which determines how the data connection is established.

- In active mode, the client starts listening for incoming data connections from the server on port M. It sends the FTP command PORT M to inform the server on which port it is listening. The server then initiates a data channel to the client from its port 20, the FTP server data port.
- In situations where the client is behind a firewall and unable to accept incoming TCP connections, passive mode may be used. In this mode, the client uses the control connection to send a PASV command to the server and then receives a server IP address and server port number from the server, which the client then uses to open a data connection from an arbitrary client port to the server IP address and server port number received.

Both modes were updated in September 1998 to support IPv6. Further changes were introduced to the passive mode at that time, updating it to extended passive mode.

Implementation:

In this activity, you will configure FTP server in Cisco Packet Tracer. After configuration you will transferfile between client & server. This activity is divided into 3 parts. First Construct the figure 10 topology & repeat all essential steps which we are done in pervious section.

Part 1: Configure FTP services on server

a) Click Server > Config tab > FTP.

b) Click On to enable FTP service.

c) In User Setup, create the following user accounts. Click the + button to add the account:

Username	Password	Permissions
Fast	123	limited to Read, write and List

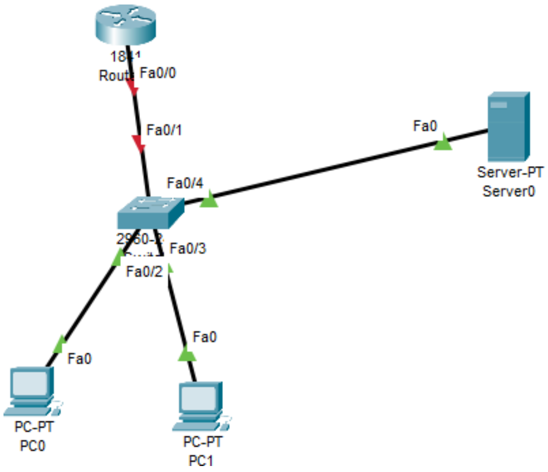
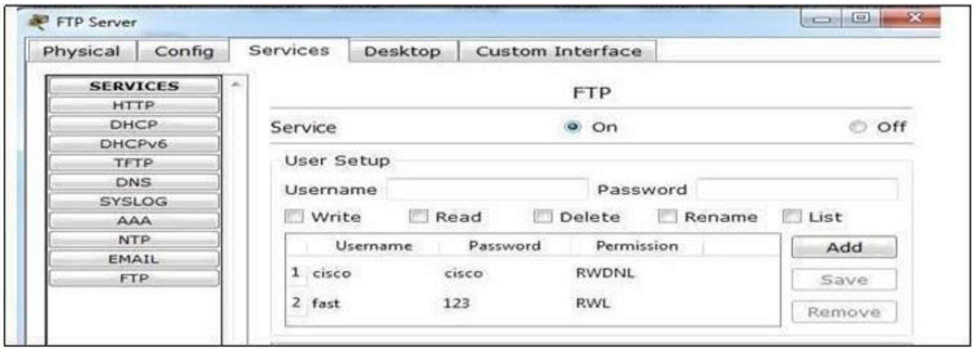


Fig-10: Topology



FTP

Service ● On ○ Off

User Setup

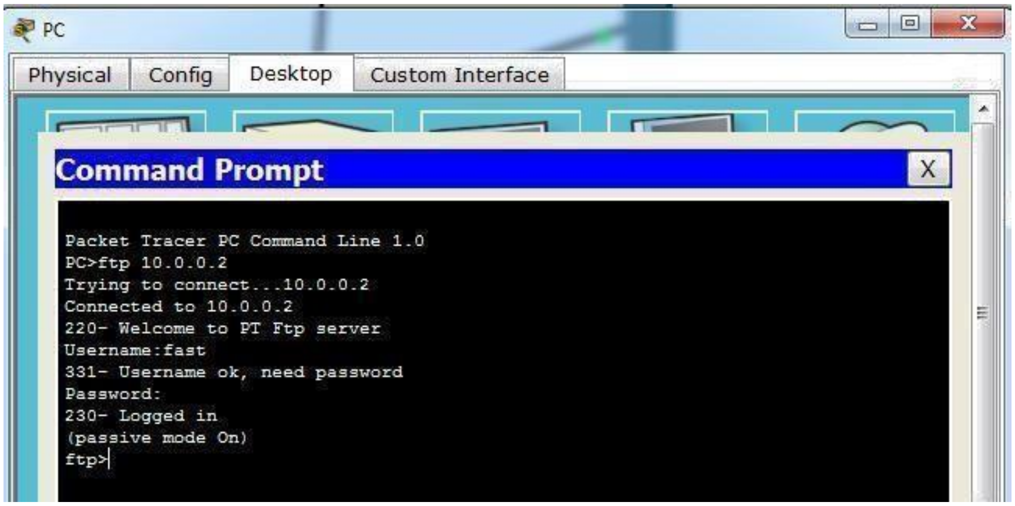
Username Password

□ Write □ Read □ Delete □ Rename □ List

	Username	Password	Permission
1	cisco	cisco	RWDNL
2	fast	123	RWL

Fig-11: Enabling STP services on server

Now go to PC Desktop command prompt. Connect with the FTP server using username & password assignto FTP server.



```
Packet Tracer PC Command Line 1.0
PC>ftp 10.0.0.2
Trying to connect...10.0.0.2
Connected to 10.0.0.2
220- Welcome to PT Ftp server
Username:fast
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

Fig-12: PC established connection with FTP server

Part 2: Upload the file to FTP server

Go to PC Desktop text editor create file named test.bin

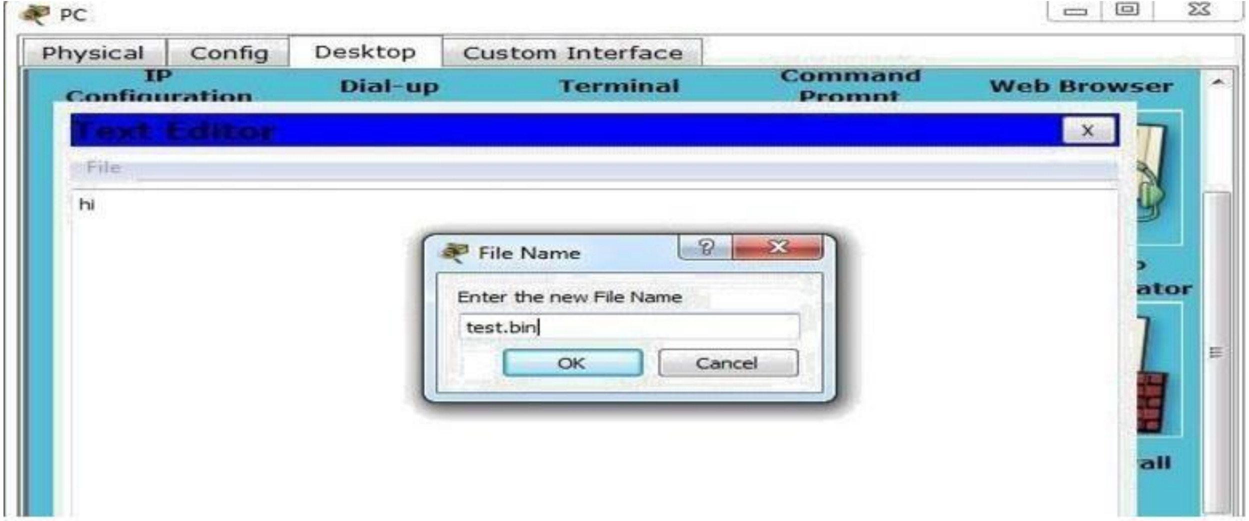
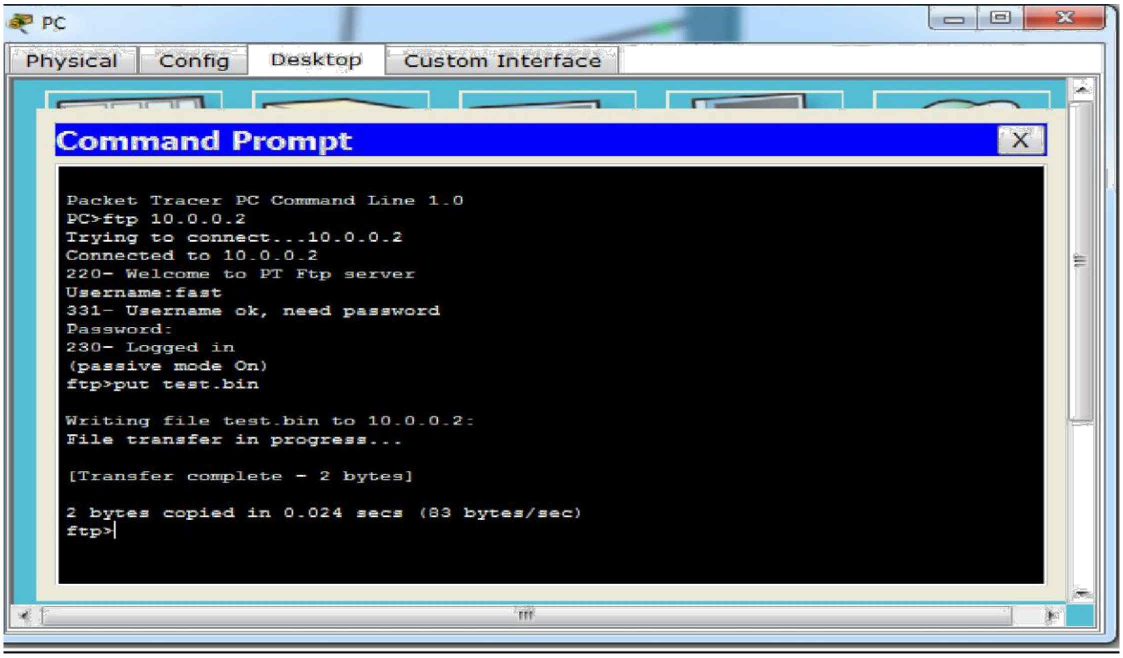


Fig-13: Creating text file in PC

After creating the file go to PC Desktop command prompt and write the following command to transfer filefrom PC to FTP server.

PUT test.bin

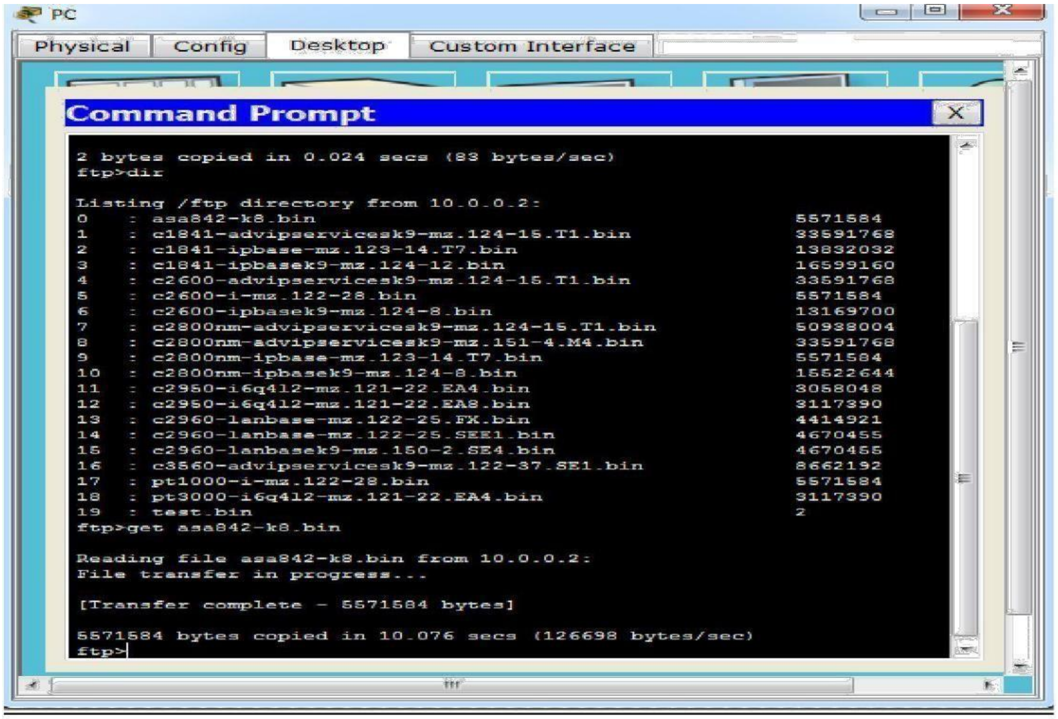


```
Packet Tracer PC Command Line 1.0
PC>ftp 10.0.0.2
Trying to connect...10.0.0.2
Connected to 10.0.0.2
220- Welcome to PT Ftp server
Username:fast
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>put test.bin

Writing file test.bin to 10.0.0.2:
File transfer in progress...

[Transfer complete - 2 bytes]

2 bytes copied in 0.024 secs (83 bytes/sec)
ftp>
```

Fig-14: transfer of file from PC to FTP server

Part 3: Download the file from FTP server

Now go to other PC desktop command prompt. Established connection with FTP server and then write the ***dir*** command to see the files in FTP server.

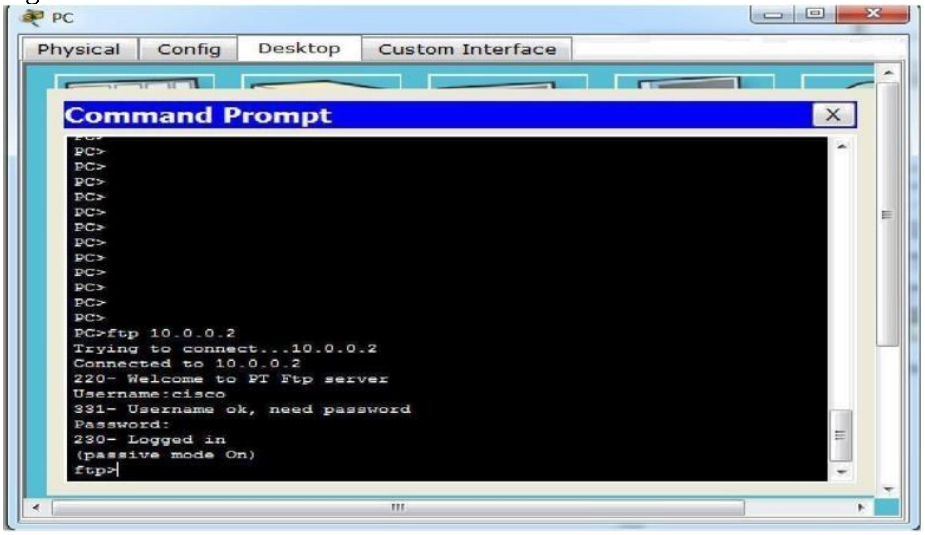


```
2 bytes copied in 0.024 secs (83 bytes/sec)
ftp>dir

Listing /ftp directory from 10.0.0.2:
0    : asa842-k8.bin                                        5571584
1    : c1841-advipservicesk9-mz.124-15.T1.bin               33591768
2    : c1841-ipbase-mz.123-14.T7.bin                        13832032
3    : c1841-ipbasek9-mz.124-12.bin                         16599160
4    : c2600-advipservicesk9-mz.124-15.T1.bin               33591768
5    : c2600-i-mz.122-28.bin                                5571584
6    : c2600-ipbasek9-mz.124-8.bin                          13169700
7    : c2800nm-advipservicesk9-mz.124-15.T1.bin             50938004
8    : c2800nm-advipservicesk9-mz.151-4.M4.bin              33591768
9    : c2800nm-ipbase-mz.123-14.T7.bin                      5571584
10   : c2800nm-ipbasek9-mz.124-8.bin                        15522644
11   : c2950-i6q4l2-mz.121-22.EA4.bin                       3058048
12   : c2950-i6q4l2-mz.121-22.EA8.bin                       3117390
13   : c2960-lanbase-mz.122-25.FX.bin                       4414921
14   : c2960-lanbase-mz.122-25.SEE1.bin                     4670455
15   : c2960-lanbasek9-mz.150-2.SE4.bin                     4670455
16   : c3560-advipservicesk9-mz.122-37.SE1.bin              8662192
17   : pt1000-i-mz.122-28.bin                               5571584
18   : pt3000-i6q4l2-mz.121-22.EA4.bin                      3117390
19   : test.bin                                             2
ftp>get asa842-k8.bin

Reading file asa842-k8.bin from 10.0.0.2:
File transfer in progress...

[Transfer complete - 5571584 bytes]

5571584 bytes copied in 10.076 secs (126698 bytes/sec)
ftp>
```

Fig-15: List of current Files in FTP server

Simulation

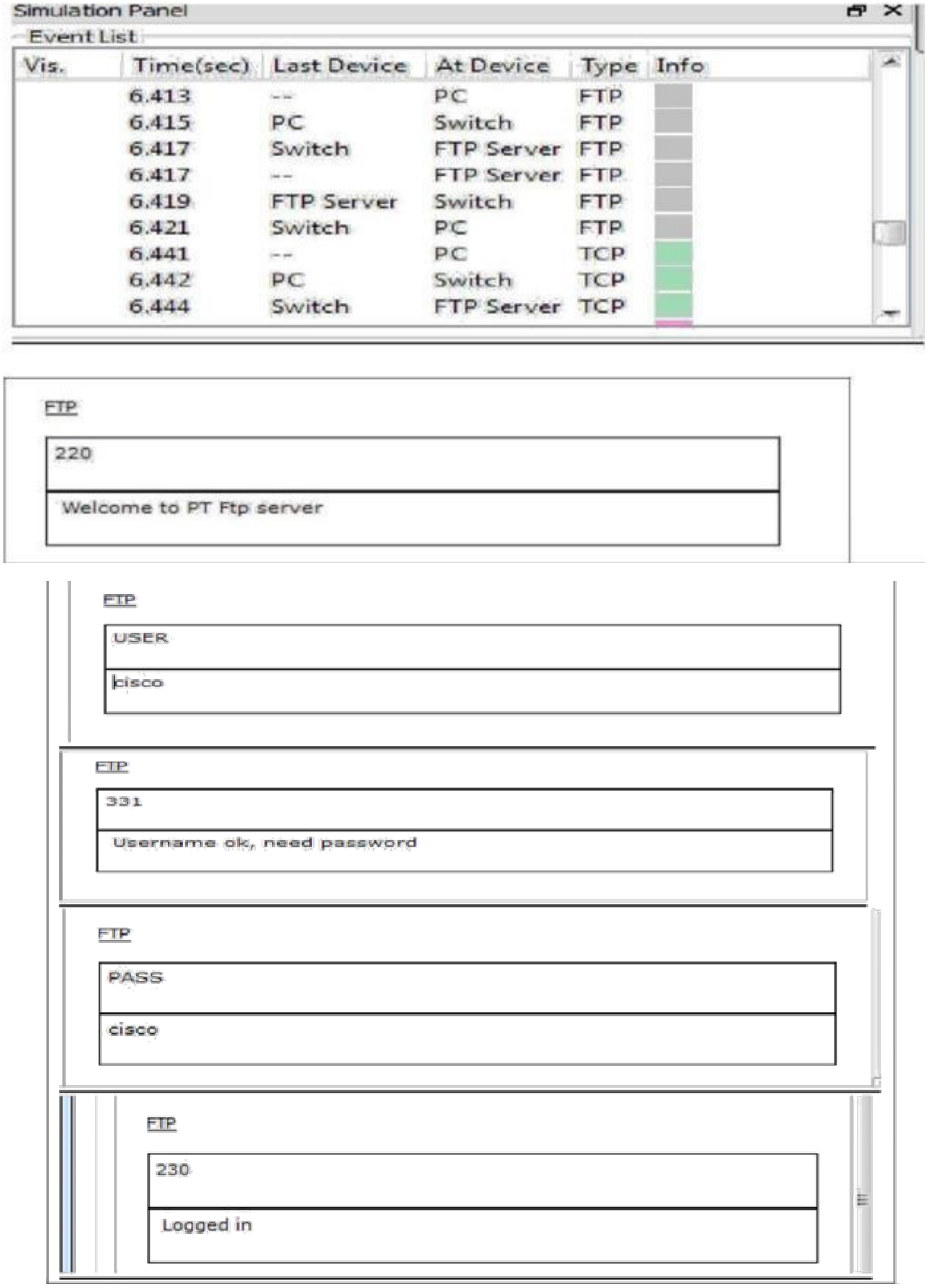
Select the simulation mode. Go to PC desktop command prompt again make connection with FTP serverusing its IP address.



```
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>ftp 10.0.0.2
Trying to connect...10.0.0.2
Connected to 10.0.0.2
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

Now to note the FTP header format information go to simulation mode edit filters and click on FTP check boxthen click on capture/forward button.

How FTP server resolves the login request.



Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type	Info
	6.413	--	PC	FTP	▨
	6.415	PC	Switch	FTP	▨
	6.417	Switch	FTP Server	FTP	▨
	6.417	--	FTP Server	FTP	▨
	6.419	FTP Server	Switch	FTP	▨
	6.421	Switch	PC	FTP	▨
	6.441	--	PC	TCP	🟩
	6.442	PC	Switch	TCP	🟩
	6.444	Switch	FTP Server	TCP	🟩

FTP

220
Welcome to PT Ftp server

FTP

USER
cisco

FTP

331
Username ok, need password

FTP

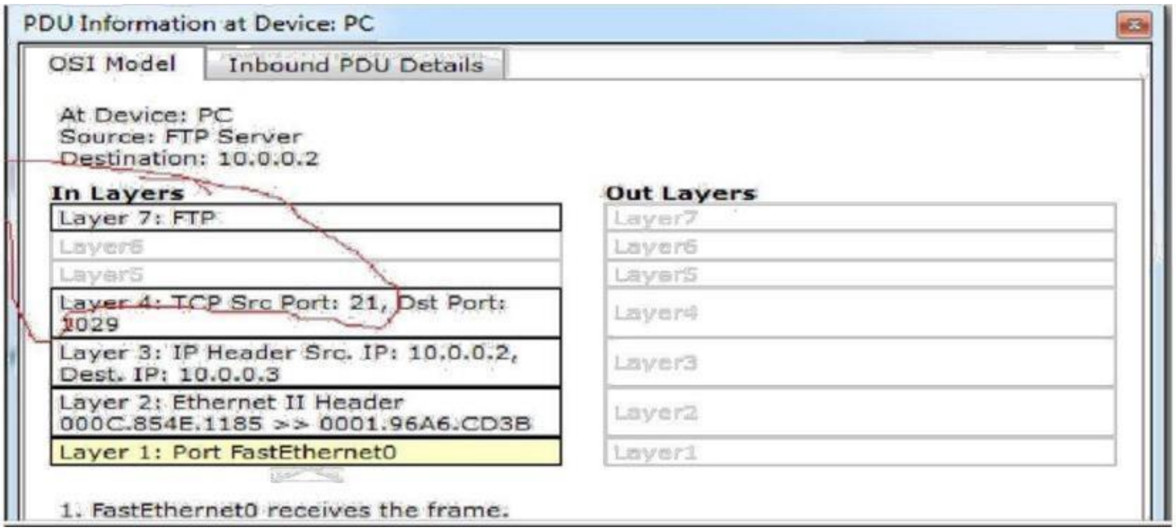
PASS
cisco

FTP

230
Logged in

Fig-17: Packets capture in simulation mode

Now click on the FTP packet, you can note that the destination port is 21.



At Device: PC
Source: FTP Server
Destination: 10.0.0.2

In Layers

- Layer 7: FTP
- Layer6
- Layer5
- Layer 4: TCP Src Port: 21, Dst Port: 1029
- Layer 3: IP Header Src. IP: 10.0.0.2, Dest. IP: 10.0.0.3
- Layer 2: Ethernet II Header 000C.854E.1185 >> 0001.96A6.CD3B
- Layer 1: Port FastEthernet0

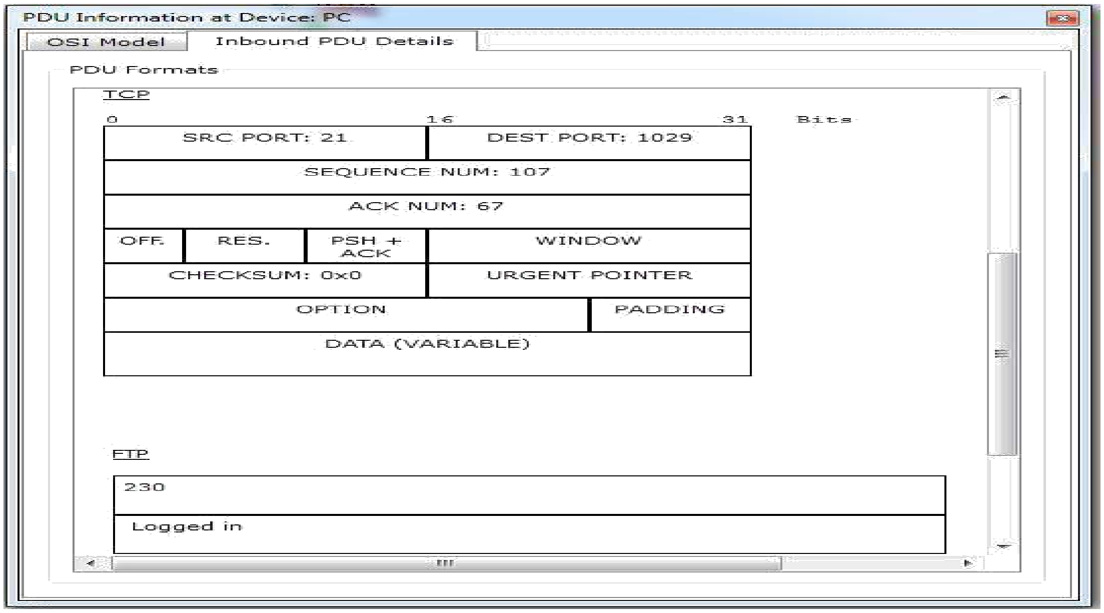
Out Layers

- Layer7
- Layer6
- Layer5
- Layer4
- Layer3
- Layer2
- Layer1

1. FastEthernet0 receives the frame.

Fig-18: PDU information at PC

Now scroll the Outbound PDU Details, you can see the FTP PDU



TCP

SRC PORT: 21		DEST PORT: 1029	
SEQUENCE NUM: 107			
ACK NUM: 67			
OFF.	RES.	PSH + ACK	WINDOW
CHECKSUM: 0x0		URGENT POINTER	
OPTION			PADDING
DATA (VARIABLE)			

FTP

230
Logged in

Fig-19: PDU details

1. nslookup In this lab, we’ll make extensive use of the nslookup tool, which is available in most Linux/Unix and Microsoft platforms today. To run nslookup in Linux/Unix, you just type the nslookup command on the command line. To run it in Windows, open the Command Prompt and run nslookup on the command line. In it is most basic operation, nslookup tool allows the host running the tool to query any specified DNS server for a DNS record. The queried DNS server can be a root DNS server, a top-level-domain DNS server, an authoritative DNS server, or an intermediate DNS server (see the textbook for definitions of these terms). To accomplish this task, nslookup sends a DNS query to the specified DNS server, receives a DNS reply from that same DNS server, and displays the result.

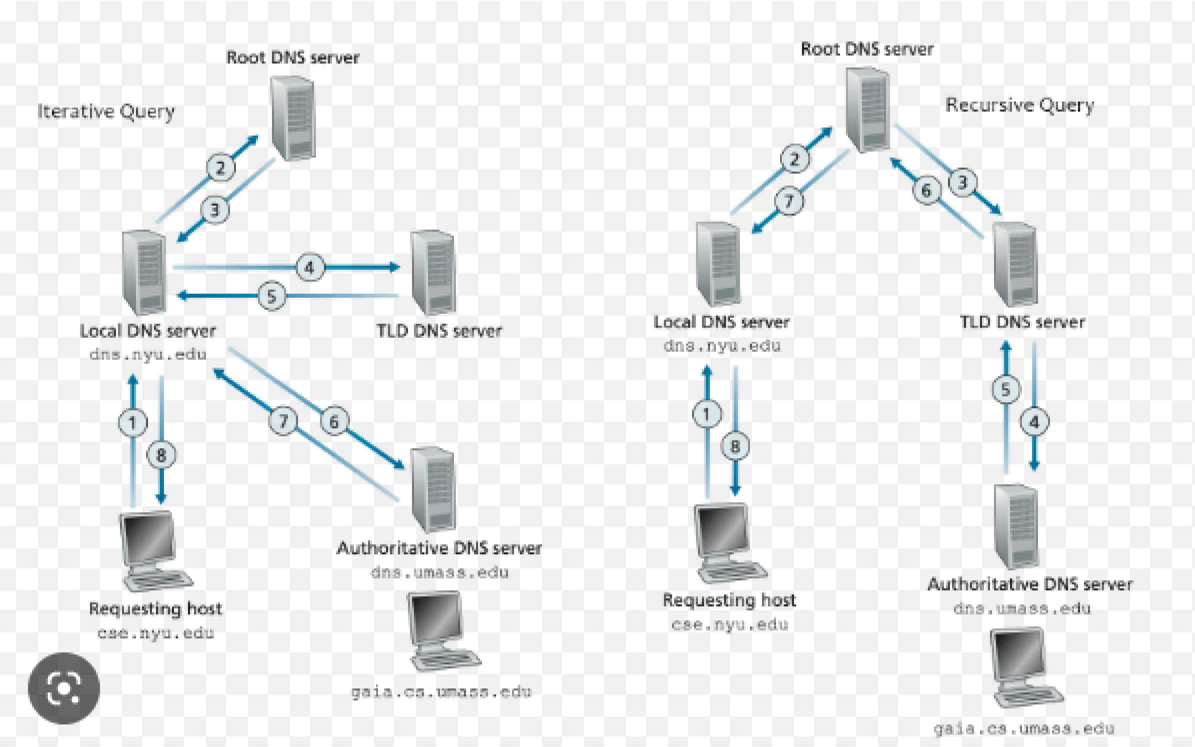
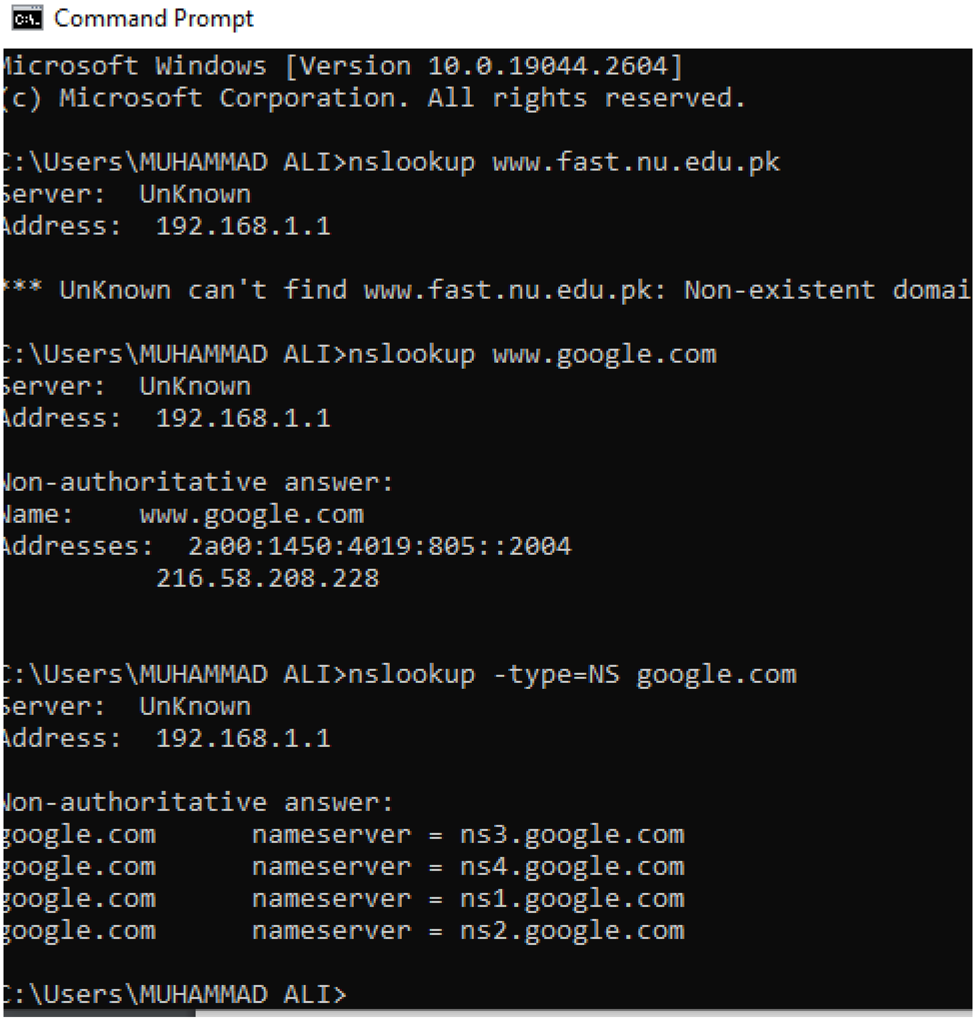
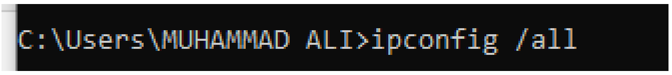


Figure 1 DNS

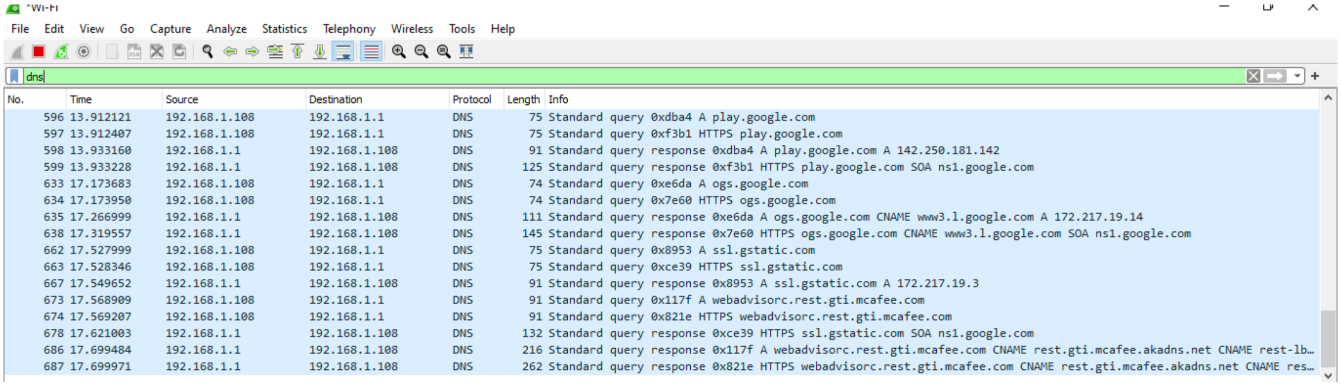


```
Microsoft Windows [Version 10.0.19044.2604]
(c) Microsoft Corporation. All rights reserved.

C:\Users\MUHAMMAD ALI>nslookup www.fast.nu.edu.pk
Server:  UnKnown
Address:  192.168.1.1

*** UnKnown can't find www.fast.nu.edu.pk: Non-existent domai

C:\Users\MUHAMMAD ALI>nslookup www.google.com
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
Name:    www.google.com
Addresses:  2a00:1450:4019:805::2004
          216.58.208.228


C:\Users\MUHAMMAD ALI>nslookup -type=NS google.com
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
google.com      nameserver = ns3.google.com
google.com      nameserver = ns4.google.com
google.com      nameserver = ns1.google.com
google.com      nameserver = ns2.google.com

C:\Users\MUHAMMAD ALI>
```



```
C:\Users\MUHAMMAD ALI>ipconfig /all
```

Wireshark DNS lab:



No.	Time	Source	Destination	Protocol	Length	Info
596	13.912121	192.168.1.108	192.168.1.1	DNS	75	Standard query 0xdba4 A play.google.com
597	13.912407	192.168.1.108	192.168.1.1	DNS	75	Standard query 0xf3b1 HTTPS play.google.com
598	13.933160	192.168.1.1	192.168.1.108	DNS	91	Standard query response 0xdba4 A play.google.com A 142.250.181.142
599	13.933228	192.168.1.1	192.168.1.108	DNS	125	Standard query response 0xf3b1 HTTPS play.google.com SOA ns1.google.com
633	17.173683	192.168.1.108	192.168.1.1	DNS	74	Standard query 0xe6da A ogs.google.com
634	17.173950	192.168.1.108	192.168.1.1	DNS	74	Standard query 0x7e60 HTTPS ogs.google.com
635	17.266999	192.168.1.1	192.168.1.108	DNS	111	Standard query response 0xe6da A ogs.google.com CNAME www3.l.google.com A 172.217.19.14
638	17.319557	192.168.1.1	192.168.1.108	DNS	145	Standard query response 0x7e60 HTTPS ogs.google.com CNAME www3.l.google.com SOA ns1.google.com
662	17.527999	192.168.1.108	192.168.1.1	DNS	75	Standard query 0x8953 A ssl.gstatic.com
663	17.528346	192.168.1.108	192.168.1.1	DNS	75	Standard query 0xce39 HTTPS ssl.gstatic.com
667	17.549652	192.168.1.1	192.168.1.108	DNS	91	Standard query response 0x8953 A ssl.gstatic.com A 172.217.19.3
673	17.568909	192.168.1.108	192.168.1.1	DNS	91	Standard query 0x117f A webadvisorc.rest.gti.mcafee.com
674	17.569207	192.168.1.108	192.168.1.1	DNS	91	Standard query 0x821e HTTPS webadvisorc.rest.gti.mcafee.com
678	17.621003	192.168.1.1	192.168.1.108	DNS	132	Standard query response 0xce39 HTTPS ssl.gstatic.com SOA ns1.google.com
686	17.699484	192.168.1.1	192.168.1.108	DNS	216	Standard query response 0x117f A webadvisorc.rest.gti.mcafee.com CNAME rest.gti.mcafee.akadns.net CNAME rest-lb…
687	17.699971	192.168.1.1	192.168.1.108	DNS	262	Standard query response 0x821e HTTPS webadvisorc.rest.gti.mcafee.com CNAME rest.gti.mcafee.akadns.net CNAME res…

Lab Exercise:

Let’s suppose your organization need to create it’s on small server (for provide some services) basednetwork. With bellow mentioned topology and instructions:

a) Configure SMTP (create account with your last name) send mail from PC-A to PC-B.
b) Configure FTP server create account with your first name, password with your roll number and filename with your last name (.bin extension) show all connection results.

1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?
2. Run nslookup to determine the authoritative DNS servers for a university in Europe.
3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

4. Locate the DNS query and response messages. Are then sent over UDP or TCP?
5. What is the destination port for the DNS query message? What is the source port of DNS response message?
6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?
7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

11. What is the destination port for the DNS query message? What is the source port of DNS response message?
12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?
15. Provide a screenshot.

Now repeat the previous experiment, but instead issue the command: nslookup –type=NS mit.edu Answer the following questions5 :
16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?
19. Provide a screenshot. Now repeat the previous experiment, but instead issue the command: nslookup www.aiit.or.kr bitsy.mit.edu Answer the following questions6:
20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?
21. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?
23. Provide a screenshot. 5 If you are unable to run Wireshark and capture a trace file, use t