**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

### 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 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 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.

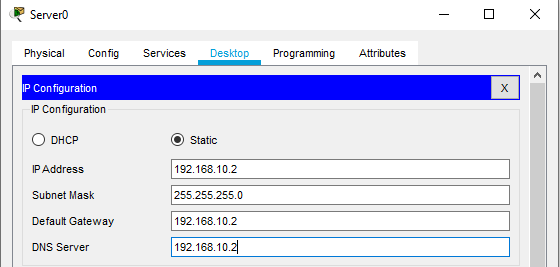
#### NS record:

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.

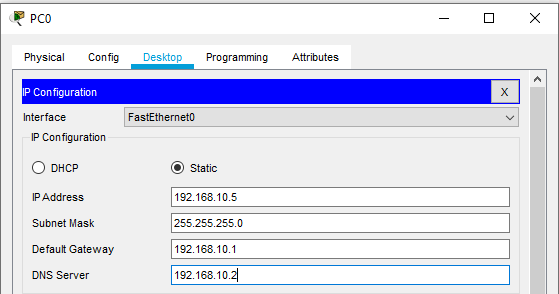
#### SOA record:

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.

Assigning IP to DNS server & PCs.



*Fig-1: DNS server*

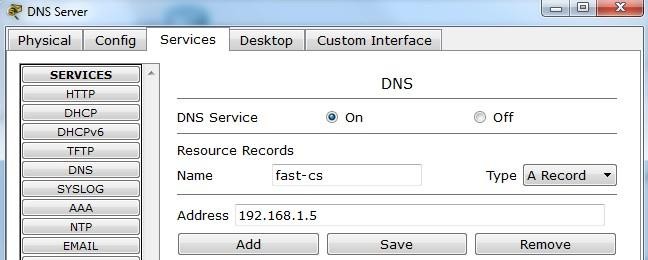


*Fig-1: Provide IP to system through static IP*

1. **DNS Configuration & Simulation:**

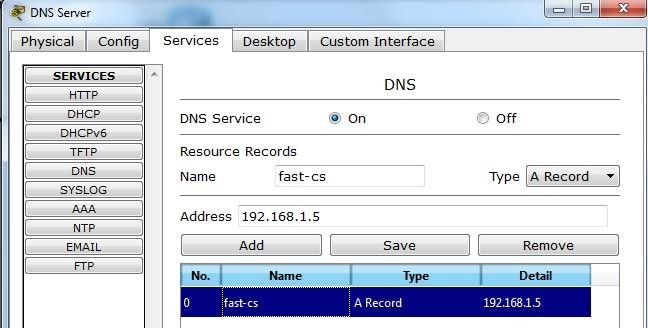
Now using the DNS service on DNS Server. Go to server services DNS.

First, we add A record. We assign the web server IP against our Domain name



*Fig-3: DNS server configuration adding a record*

Now click on Add.



*Fig-3: Record is added in DNS server*

Now add Cname record.

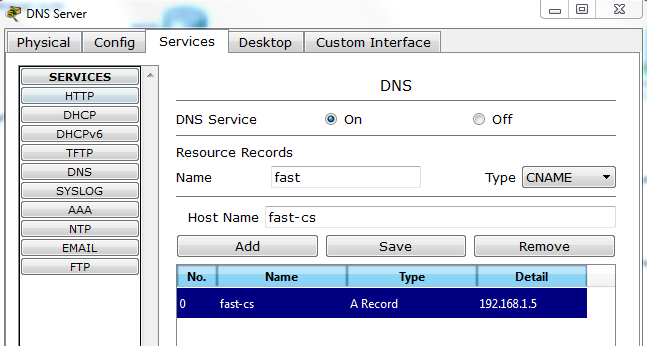


Fig-4: Adding CNAME record in DNS server

Now click on Add

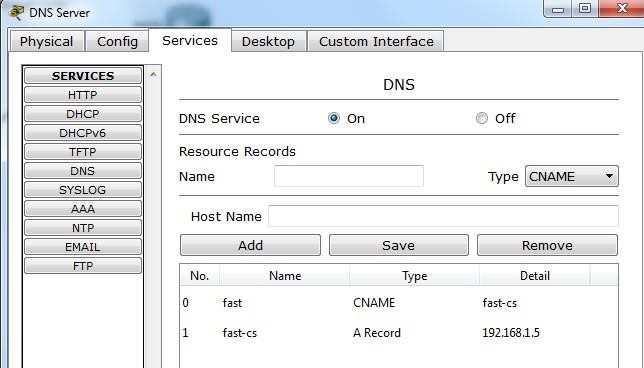


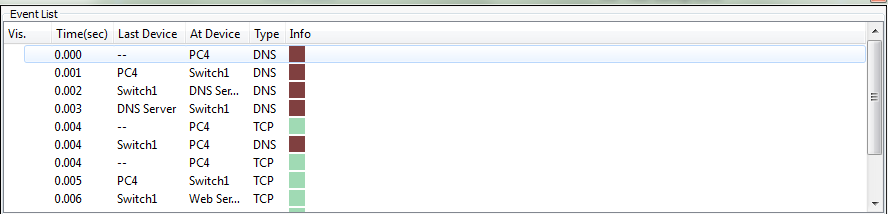
Fig-5: CNAME record is added in DNS server

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



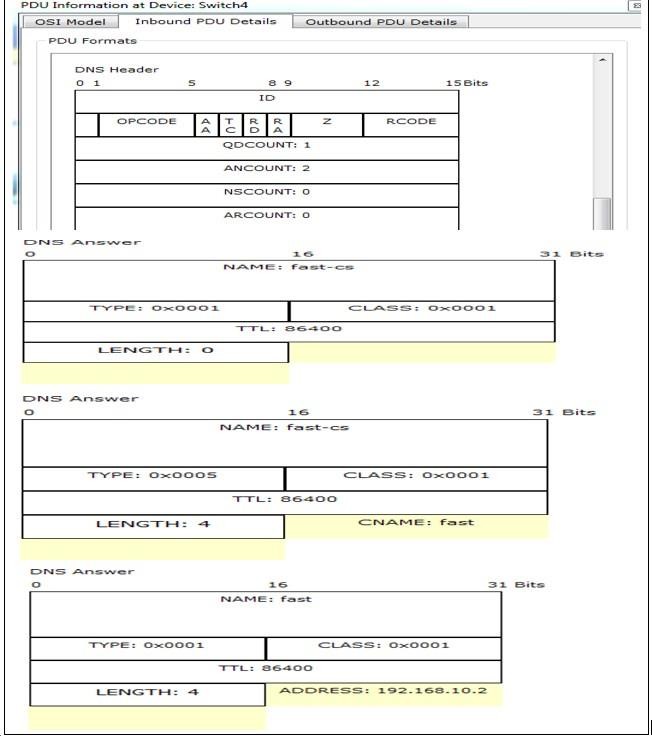
*Fig-6: Opening website*

Start simulation.



*Fig-7: Packets exchange in DNS simulation*

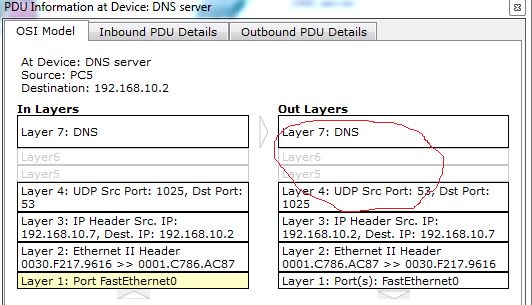
Click on DNS packet. See how DNS server resolved the name.



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

#### Shows OSI layers involved in transmission.

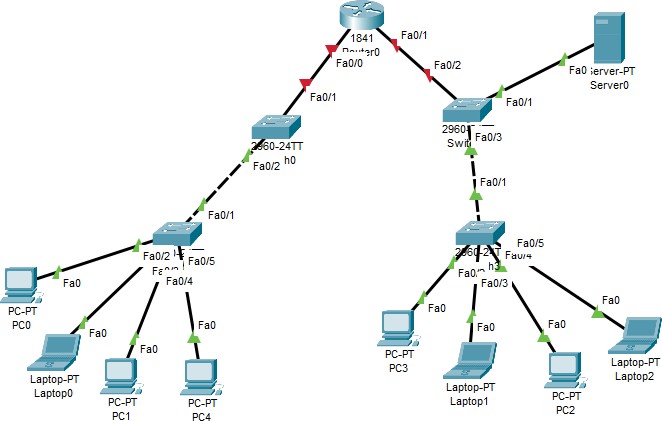
The popped up window (below) will enable you to trace the content of the message through the OSI layer and whatchanges will occur at each layer (use next and previous buttons to trace each layer content).



*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:**

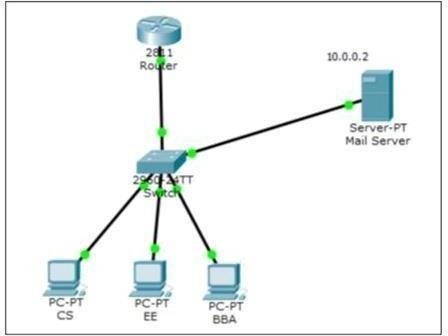
Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (email) transmission. First defined by RFC 821 in 1982, it was last updated in 2008 with Extended SMTP additions by RFC 5321,which is the protocol in widespread use today. Although electronic mail servers and other mail 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.

# 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 |

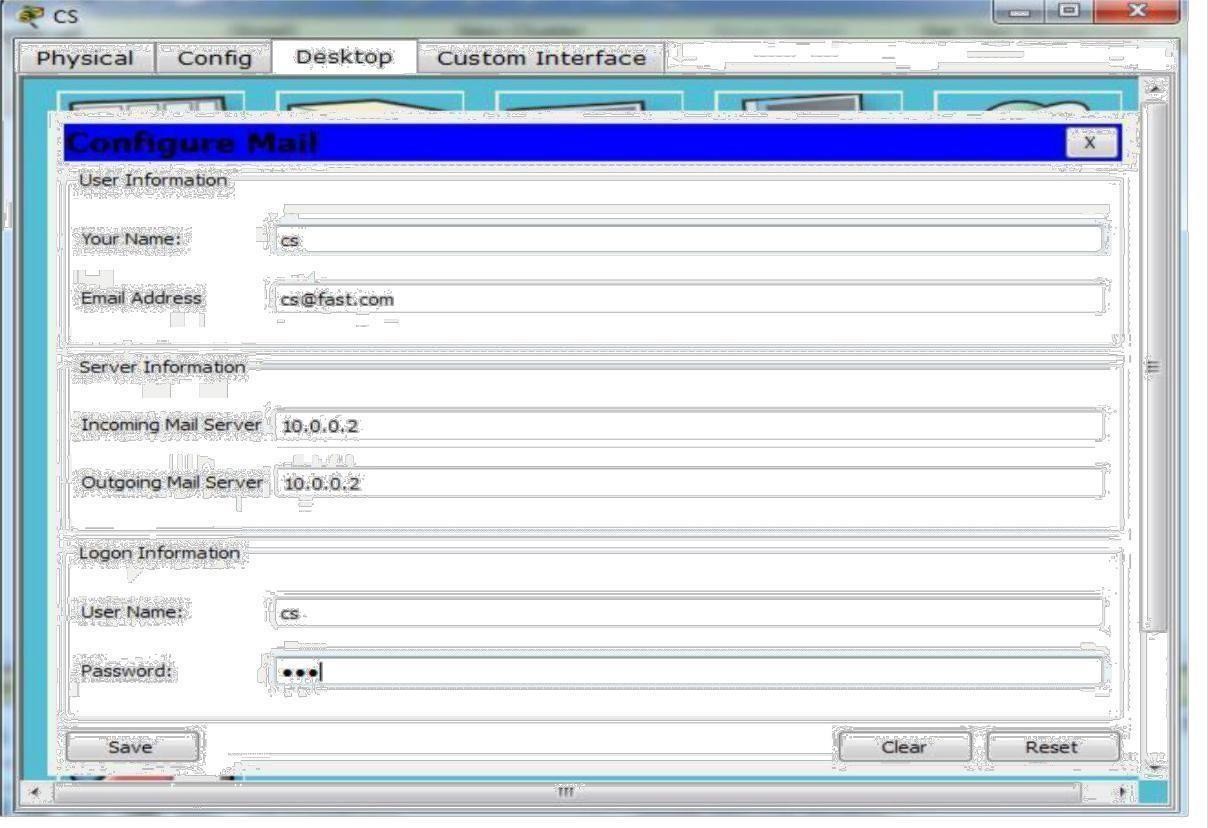
*Table-1: User name & their passwords*

Now configure user email account. Goto PC  Desktop  Email

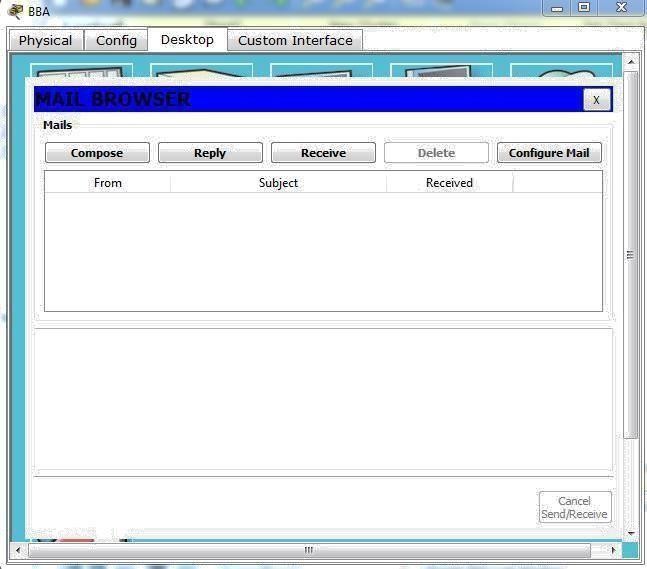
Fill the following fields as shown in figure 3.

Click “Save” to save the configurations and do the same for EE and BBA.

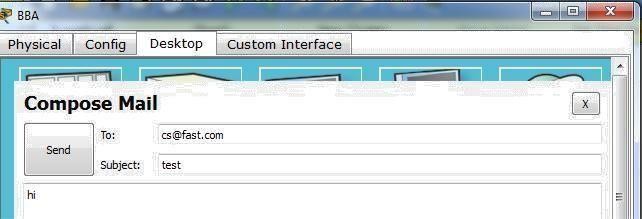




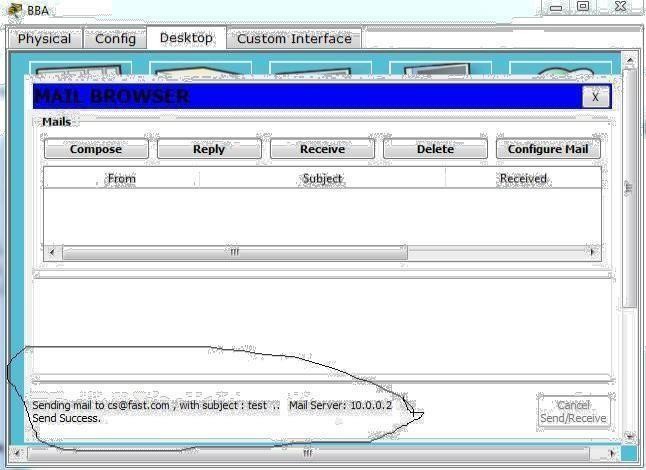
*Fig-3: User Email configuration*



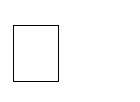
*Fig-4: Mail browser view of user PC after mail configuration*

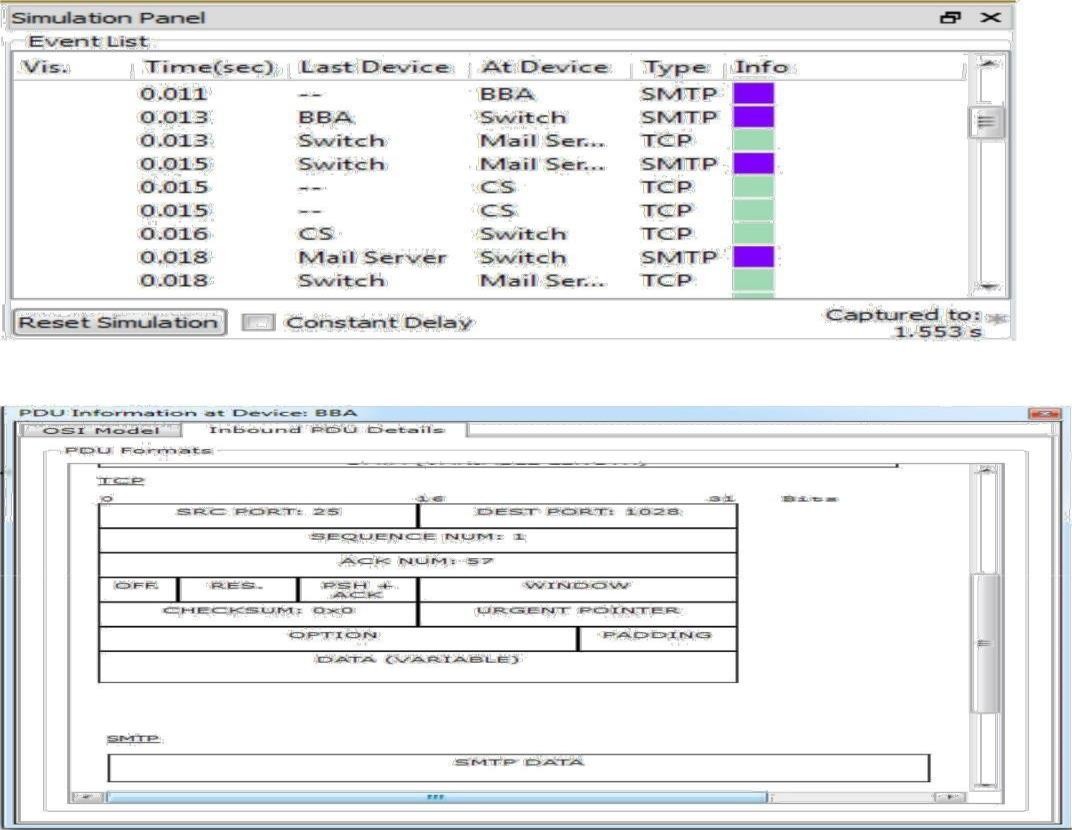
Now compose email [**cs@fast.com**](mailto:cs@fast.com)

Click on “Send” to send Email.

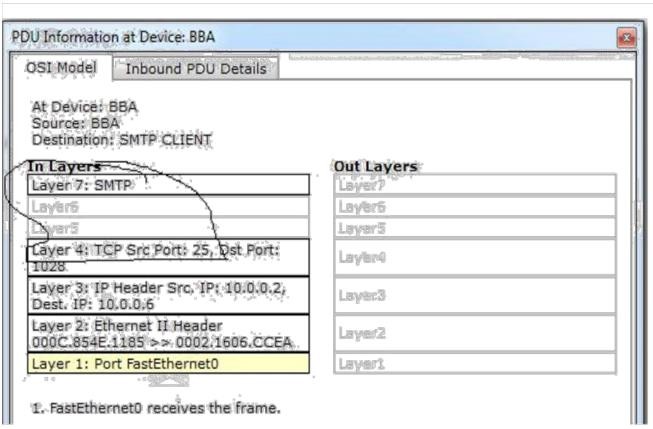


#### Simulation:

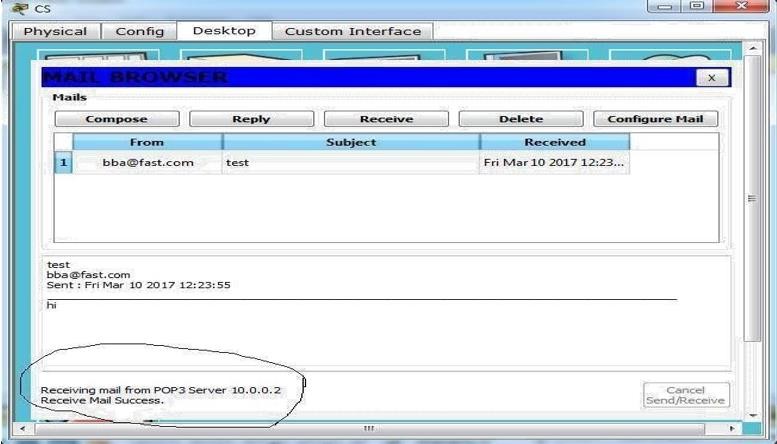
To note POP 3 header format information, go to simulation mode edit filters & check SMTP & POP 3 boxes. After that click on capture/forward button. Now see how mail server works



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



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



**Introduction:**

**FTP**

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.

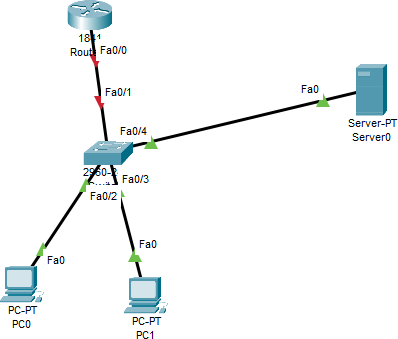
## Implementation:

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.

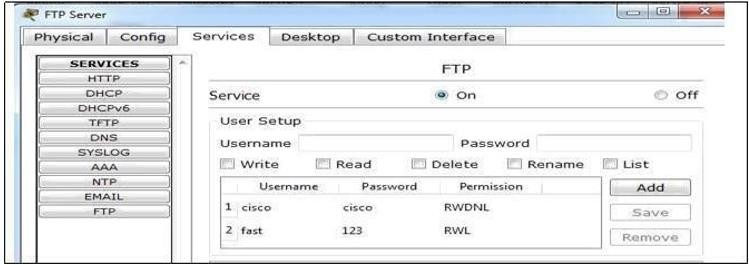
#### Part 1: Configure FTP services on server

1. Click Server > Config tab > FTP.
2. Click On to enable FTP service.
3. 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 |

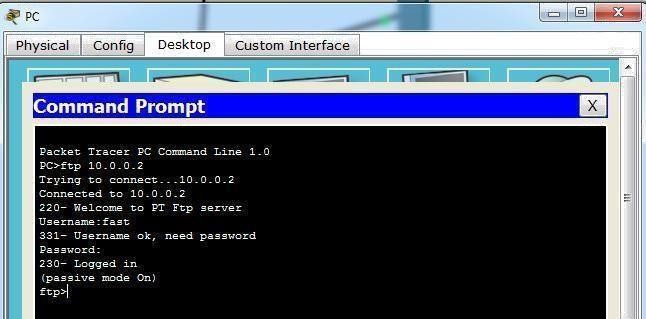


*Fig-10: Topology*



*Fig-11: Enabling STP services on server*

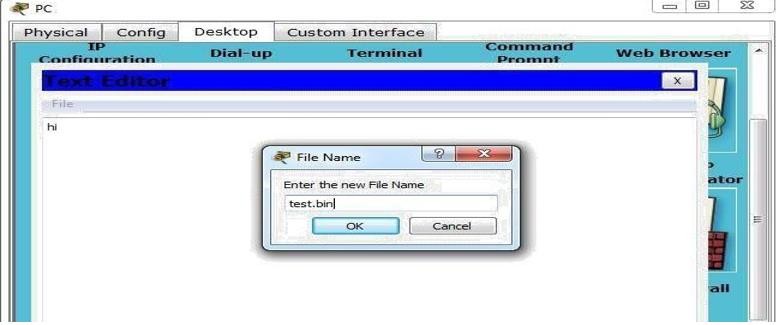
Now go to PC Desktop command prompt. Connect with the FTP server using username & password assignto FTP server.



*Fig-12: PC established connection with FTP server*

**Part 2: Upload the file to FTP server**

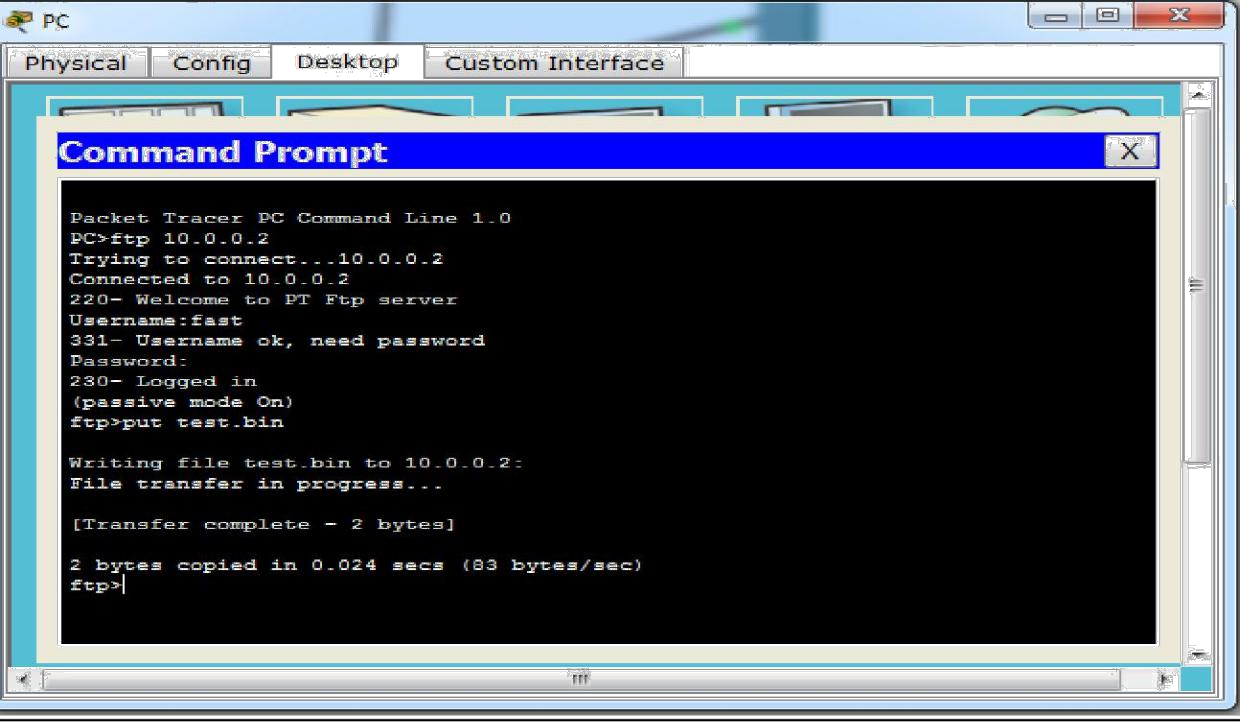
Go to PC Desktop text editor create file named test.bin



*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***

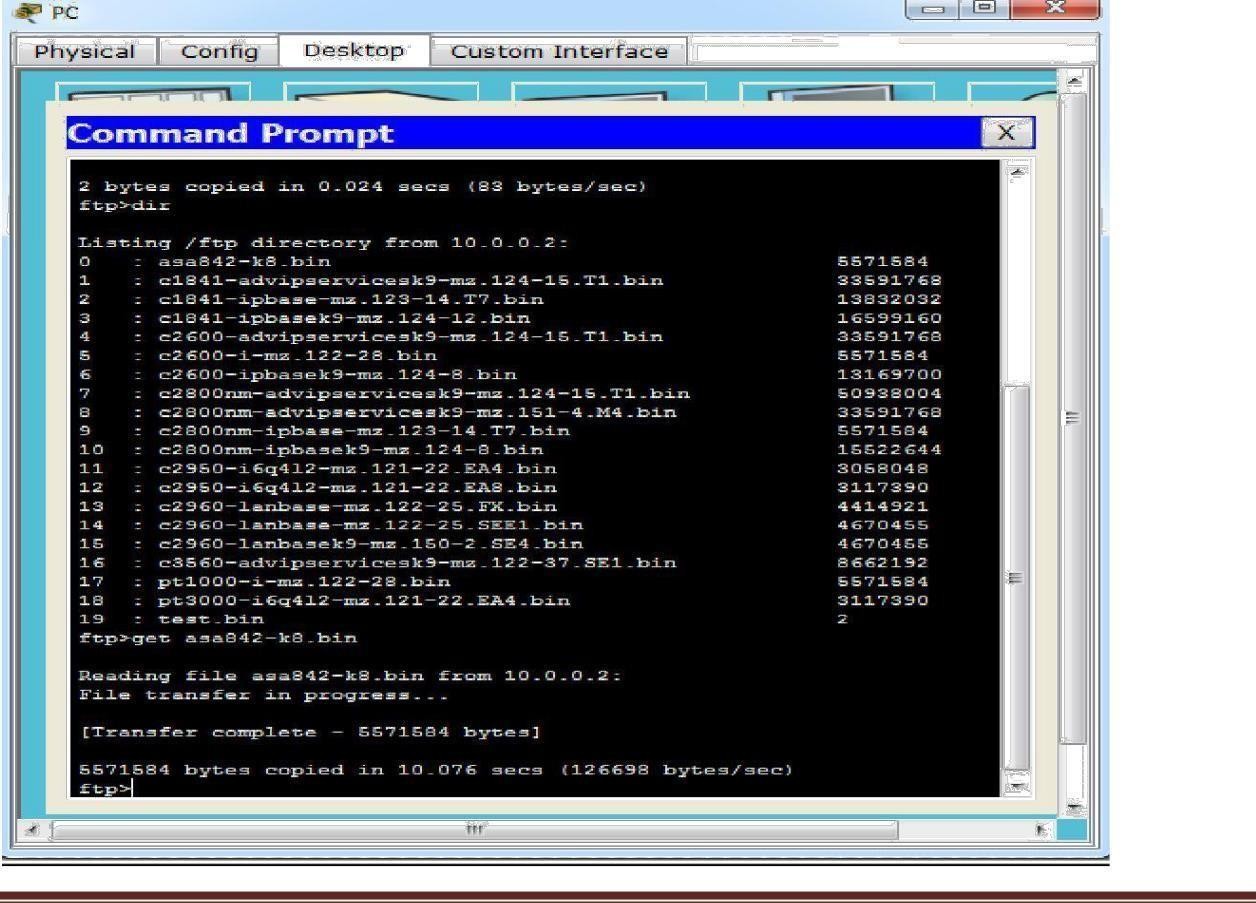


*Fig-14: transfer of file from PC to FTP server*

### 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

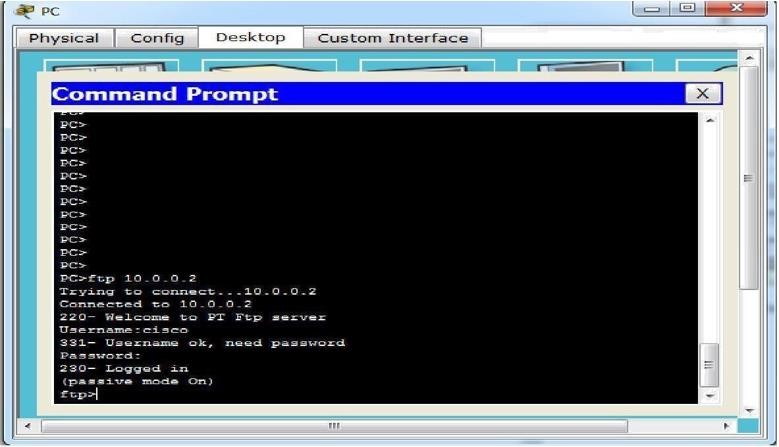
***dir*** command to see the files in FTP server.



*Fig-15: List of current Files in FTP server*

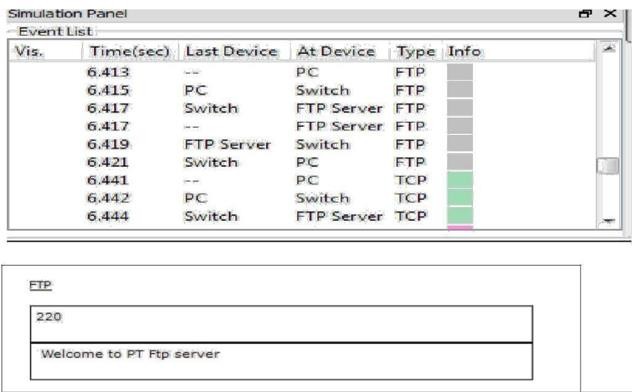
#### Simulation

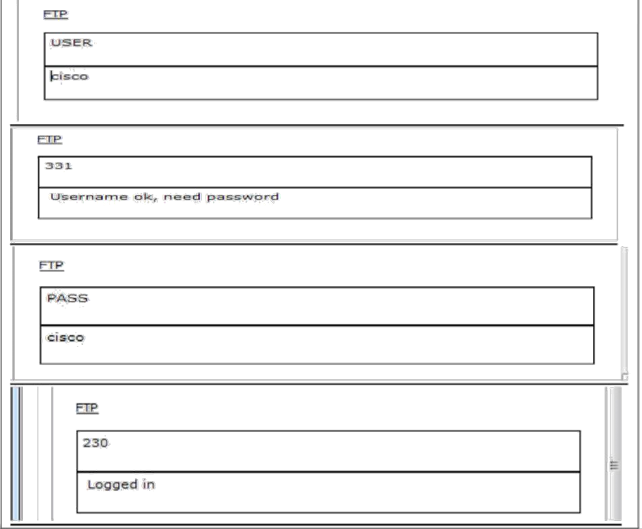
Select the simulation mode. Go to PC desktop command prompt again make connection with FTP serverusing its IP address.



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.

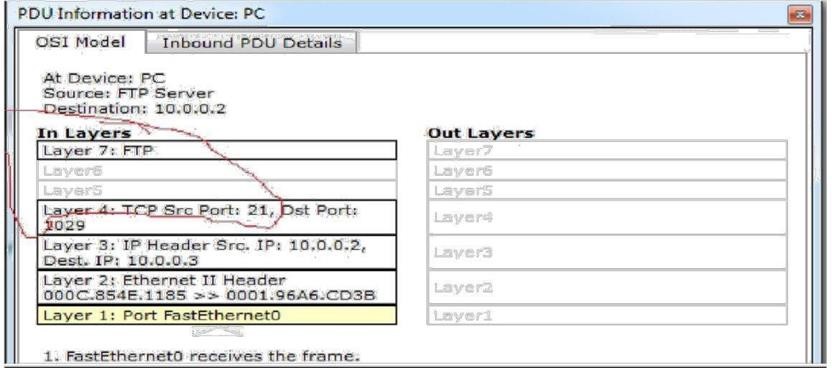
How FTP server resolves the login request.





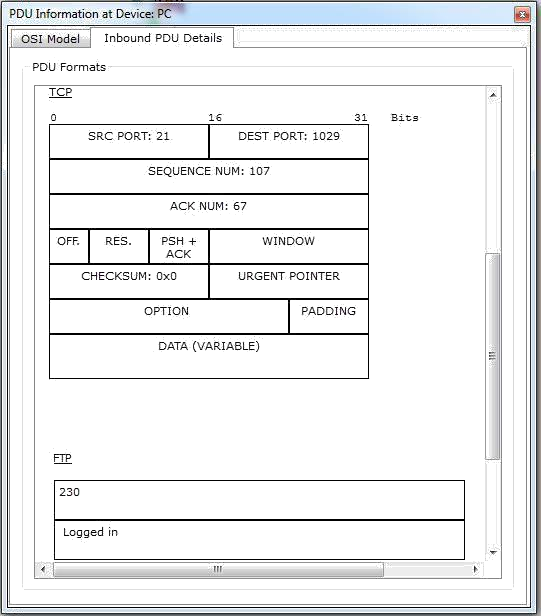
*Fig-17: Packets capture in simulation mode*

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



*Fig-18: PDU information at PC*

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



*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.

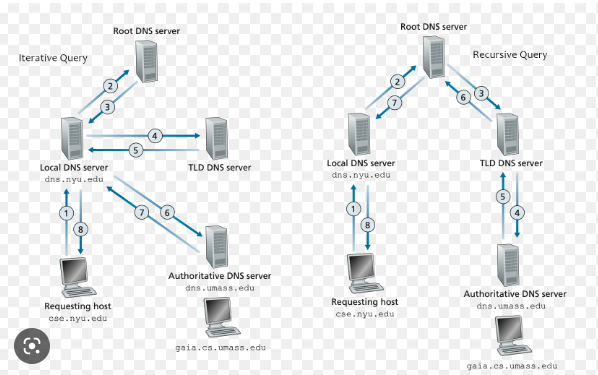
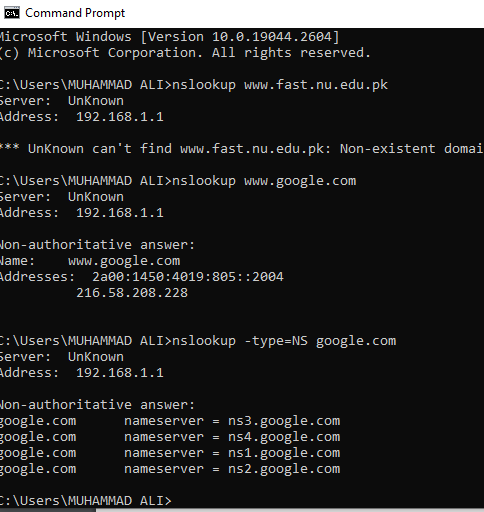
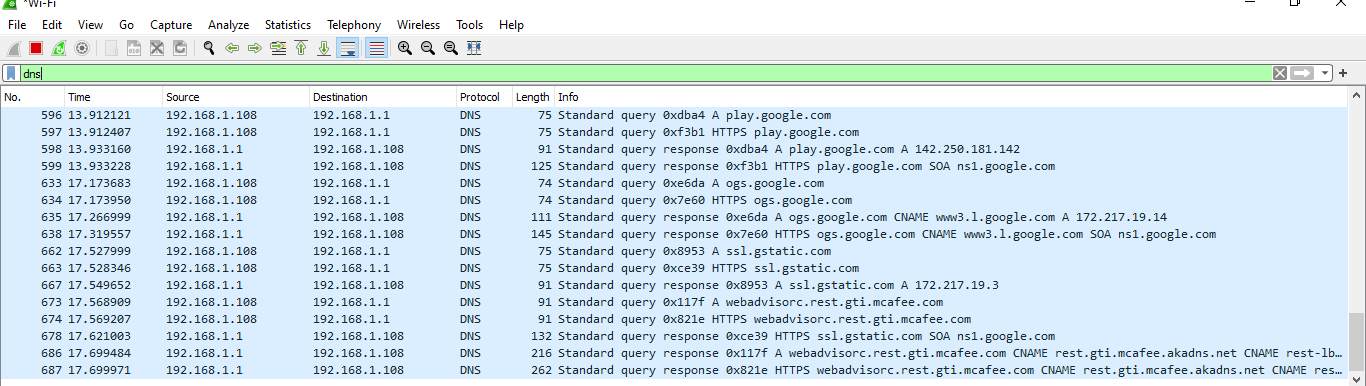


Figure DNS





Wireshark DNS lab:



**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:

1. Configure SMTP (create account with your last name) send mail from PC-A to PC-B.
2. 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