Computer Networks Lab 05

Course: Computer Networks (CL3001) **Semester:** Spring 2024
Instructor: Waseem Rauf **T.A:** N/A

Note:

- Maintain discipline during the lab.
- Listen and follow the instructions as they are given.
- Just raise hand if you have any problem.
- Completing all tasks of each lab is compulsory.
- Get your lab checked at the end of the session.

Lab 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. 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 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.

c) NS Record:

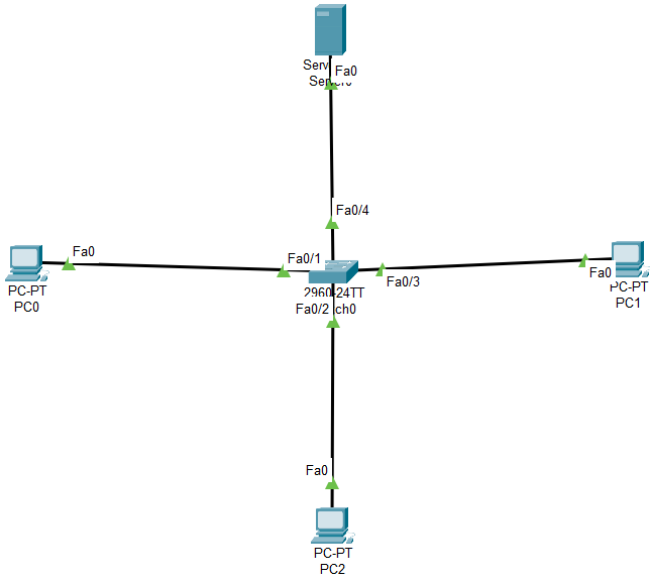
An NS record identifies which DNS server is authoritative for a particular zone. The "NS" stands for "name server". NS records that do not exist on the apex of a domain are primarily used for splitting up the management of records on sub-domains.

d) SOA Record:

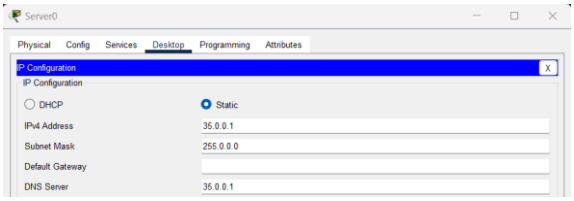
The SOA or Start of Authority record for a domain stores information about the name of the server that supplies the data for the zone, the administrator of the zone and the current version of the data. It also provides information about the number of seconds a secondary name server should wait before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

Implementation:

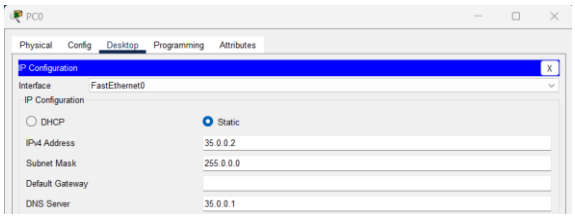
Consider the following topology:

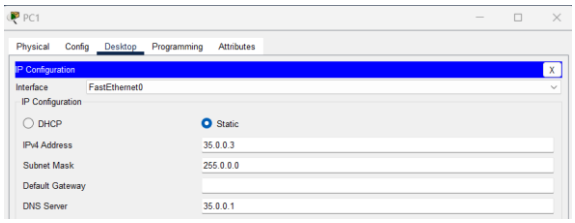


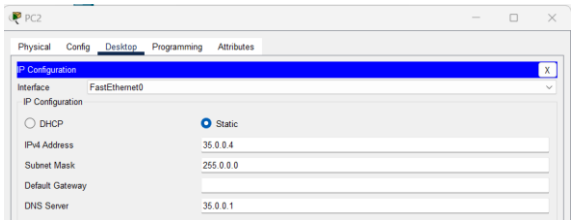
Assigning IP to DNS server:



Assigning IP to PCs:

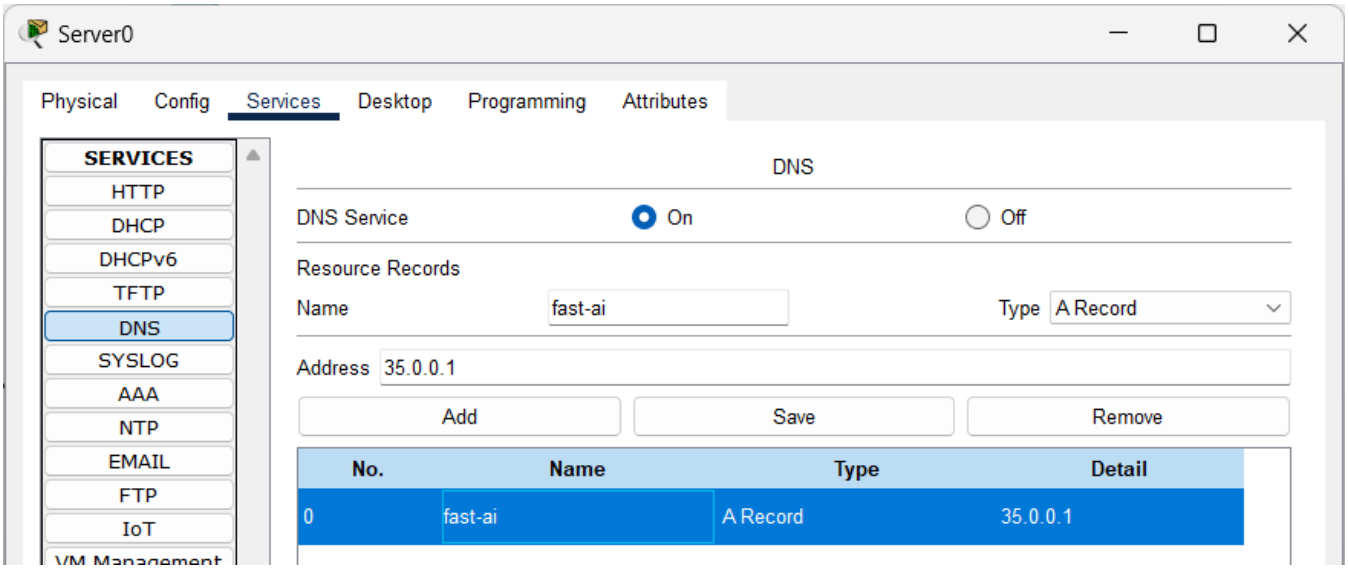




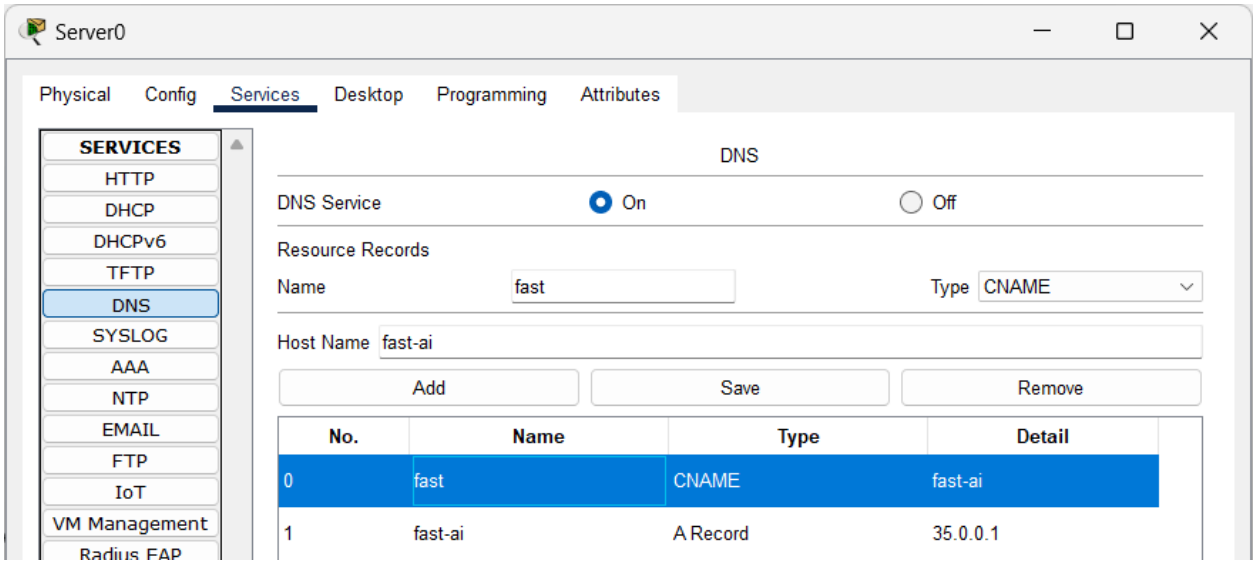


2. DNS Configuration & Simulation

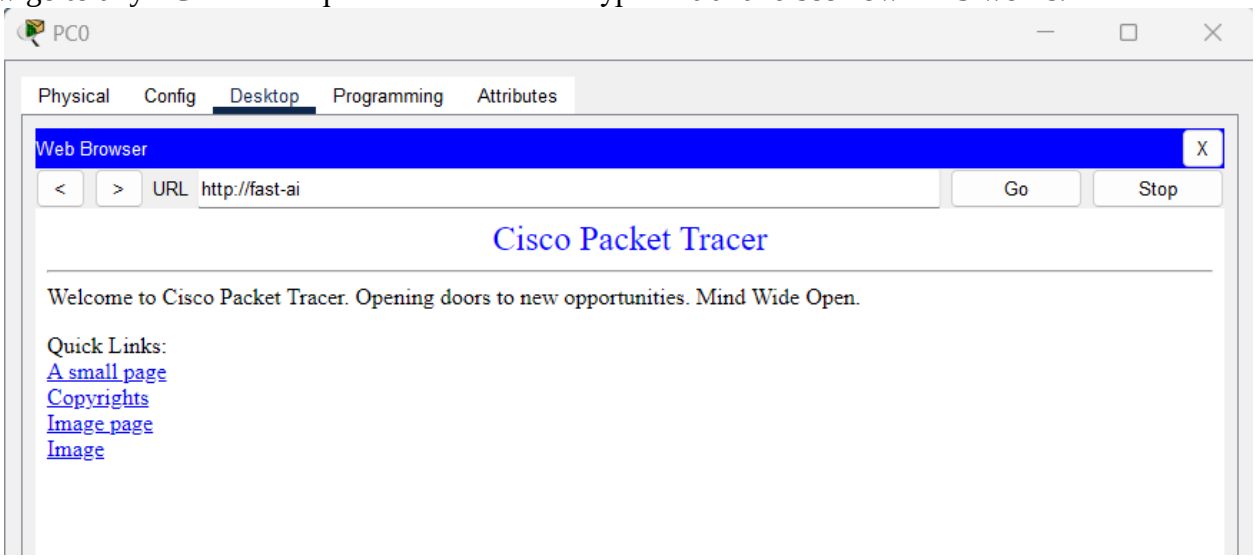
Now using the DNS service on DNS Server. Go to server services DNS.
First, we add A record. We assign the web server IP against our Domain name. Now click on Add.



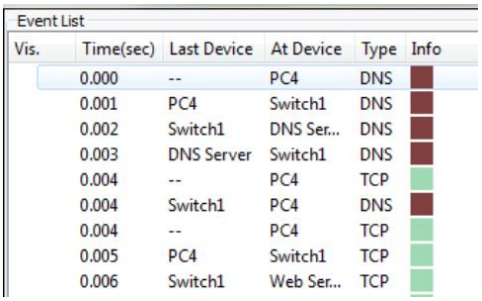
Now add CNAME record.



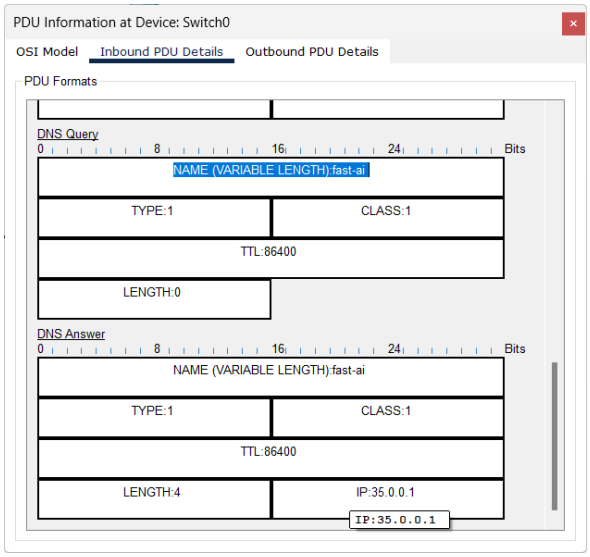
Now go to any PC →Desktop →web browser → type fast-ai and see how DNS works.



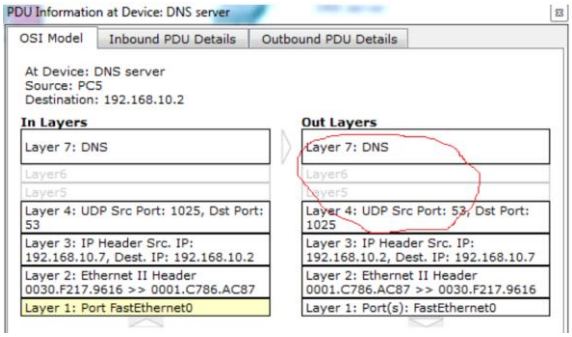
Start simulation.



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

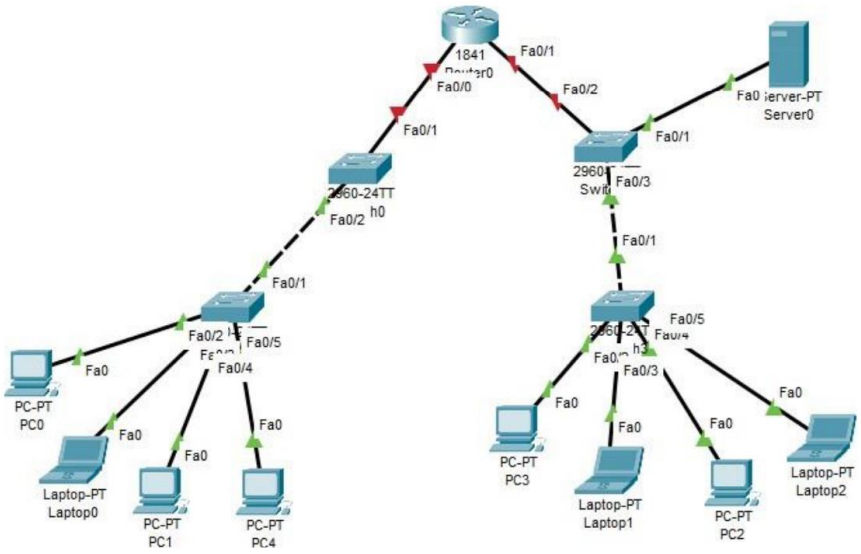


Shows OSI layers involved in transmission.



Lab Exercises

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



SMTP

1. Introduction to SMTP

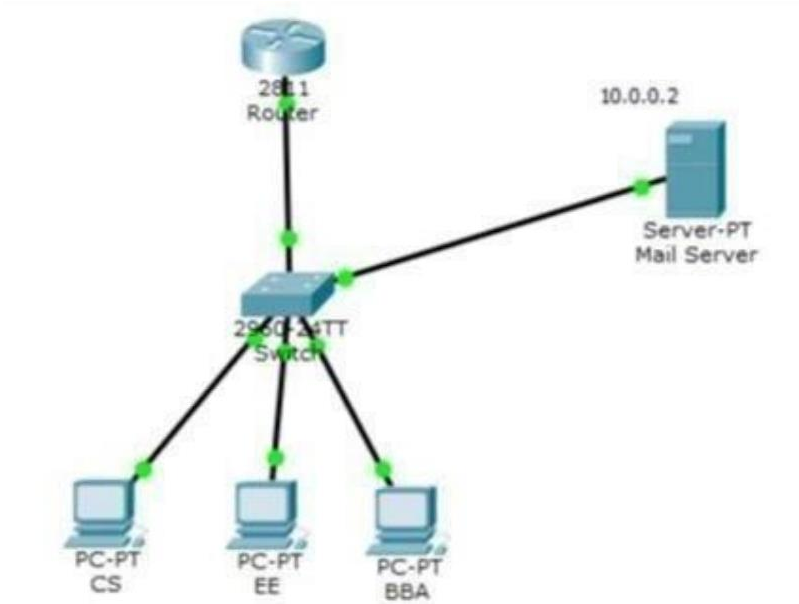
Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (email) transmission. First defined by RFC 821in1982, it was last updated in 2008with Extended SMTP additions by RFC 5321, which is the protocol in widespread use today. Although electronic mail servers and other mail transfer agents use SMTP to send and receive mail messages, user-level client mail applications typically use SMTP only for sending messages to a mail server for relaying. For retrieving messages, client applications usually use either IMAP or POP3.

SMTP communication between mail servers uses port 25. Mail clients on the other hand, often submit the outgoing 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:

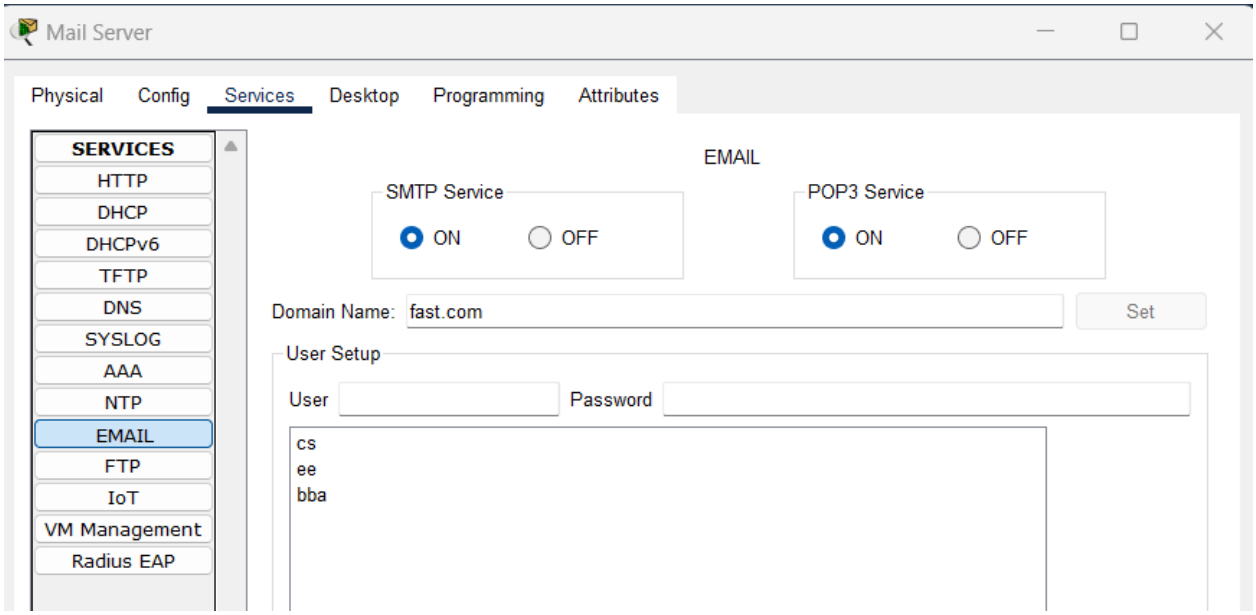
Topology:



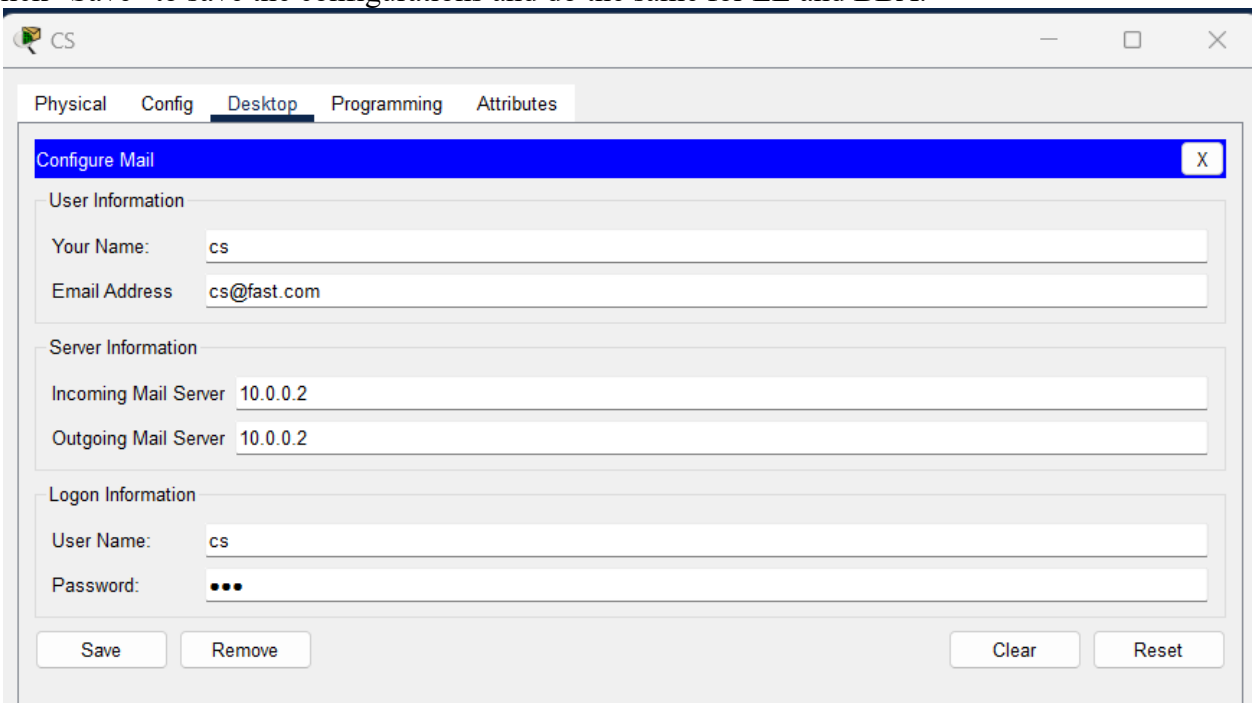
Configure and Verify Email Services:

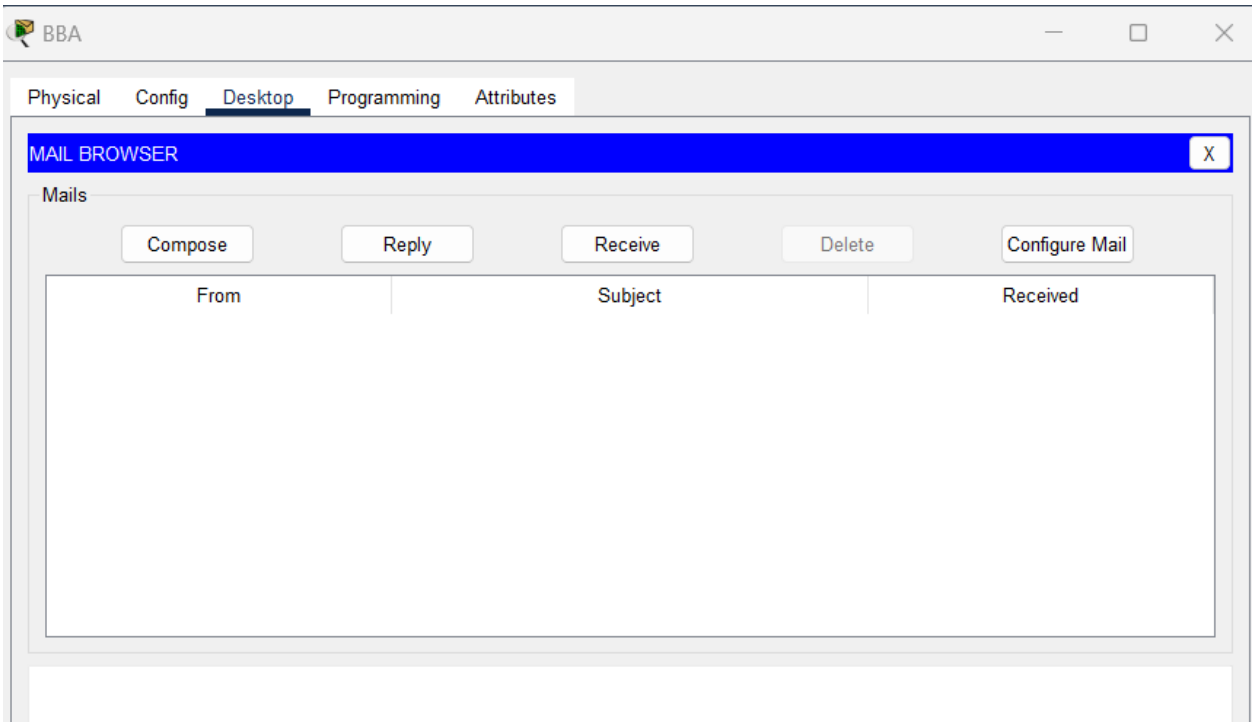
- Click on Mail server.
- Go to services & then email services.
- Enable SMTP & POP3 Service.
- Set Domain name e.g. fast.com.
- Add following users.

Usernames	Passwords
cs	123
ee	456
bba	789

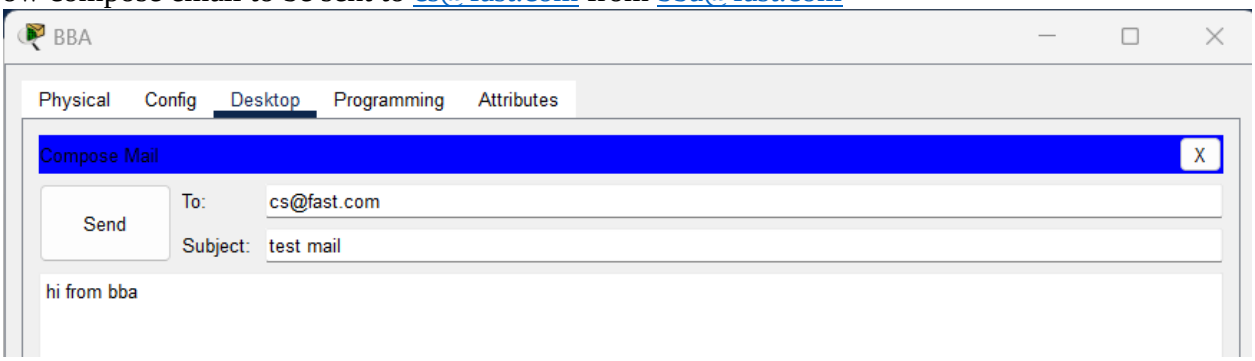


Now configure user email account.
Go to PC → Desktop → Email.
Fill the following fields as shown below.
Click “Save” to save the configurations and do the same for EE and BBA.

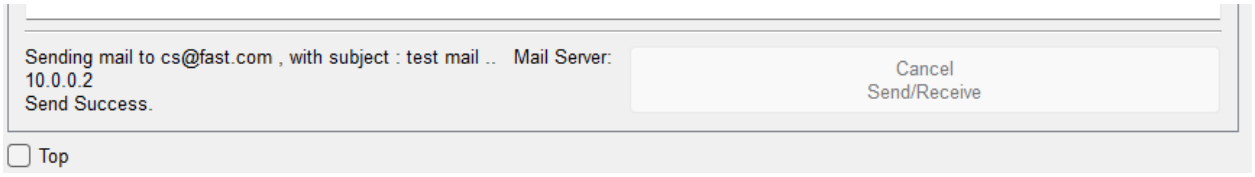




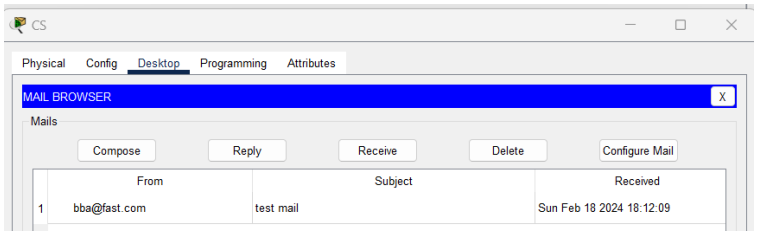
Now compose email to be sent to cs@fast.com from bba@fast.com



Click on “Send” to send Email.



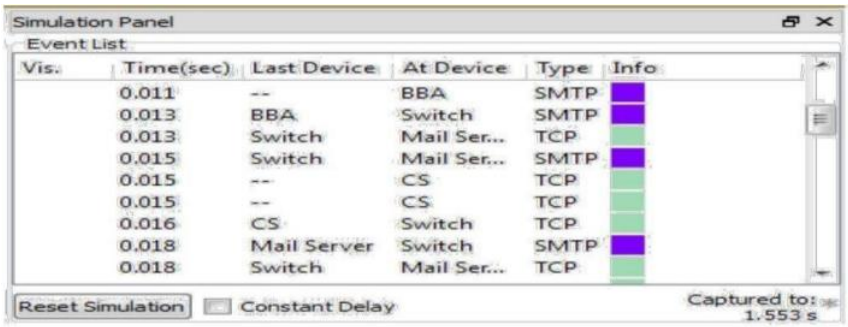
Now open email again on cs and click receive to see the email received from bba.

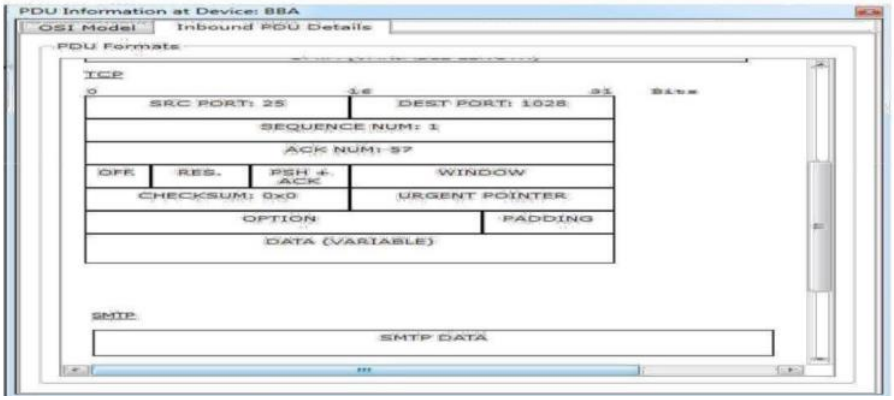


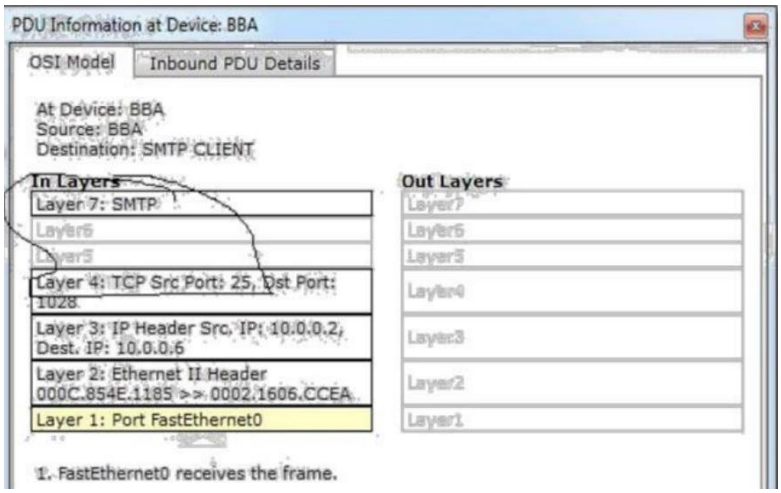
Simulation:

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.







FTP

1. Introduction to 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 asits 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.

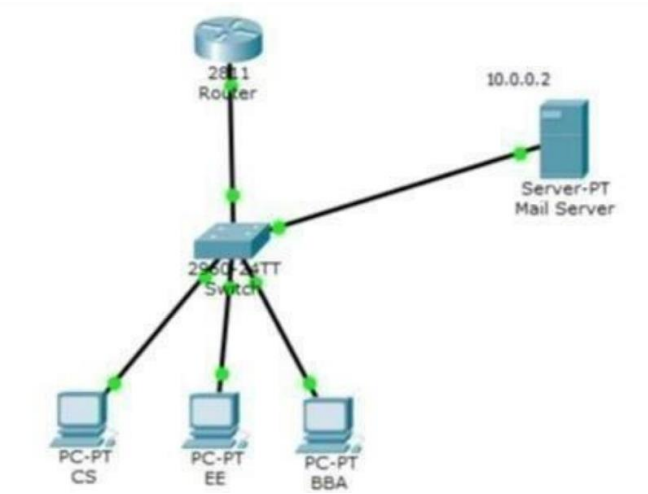
Both modes were updated in September 1998 to support IPv6. Further changes were introduced to the passive mode at that time, updating it to extended passive mode.

Implementation:

In this activity, you will configure FTP server in Cisco Packet Tracer. After configuration you will transfer files between client & server. This activity is divided into 3 parts.

First Construct the topology & repeat all essential steps which we are done in pervious section.

Topology:



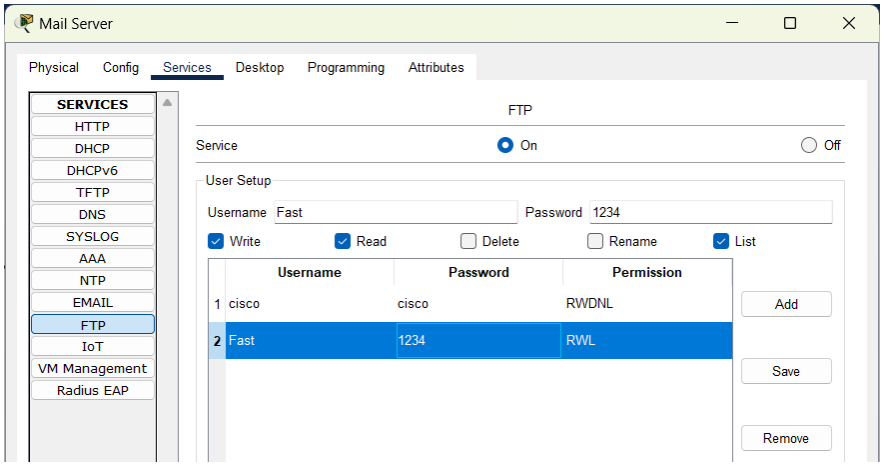
Part I: Configure FTP services on server

a) Click server > Config tab > FTP.

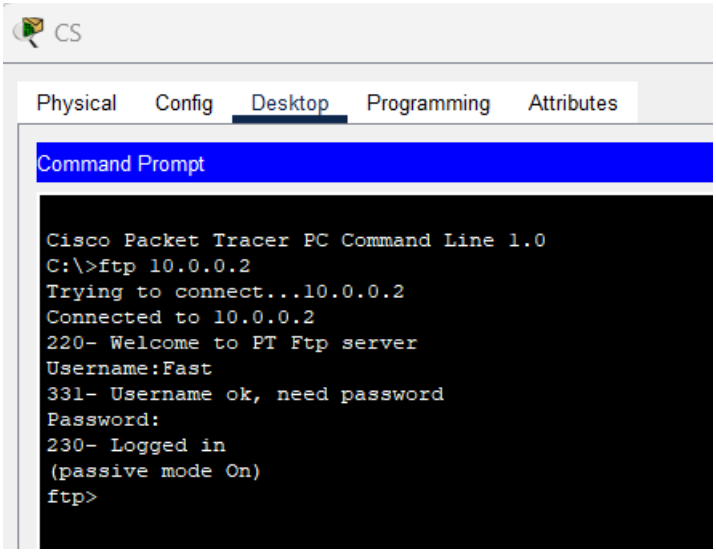
b) Click On to enable FTP service.

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

Username	Password	Permissions
Fast	1234	Limited to Read, write & list.

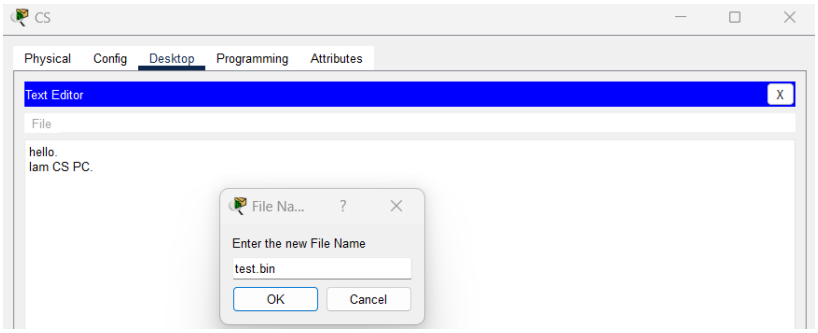


Now go to any PC Desktop command prompt. Connect with the FTP server using username & password assigned to FTP server.



Part II: Upload file(s) to the FTP server

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



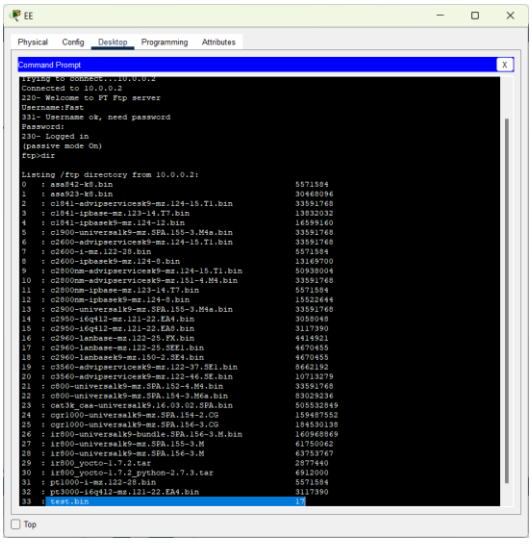
After creating the file go to PC Desktop command prompt and write the following command to transfer file from PC to FTP server.

put test.bin

```
ftp>put test.bin

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

[Transfer complete - 17 bytes]

17 bytes copied in 0.037 secs (459 bytes/sec)
ftp>
```

Part III: Upload file(s) to the FTP server

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

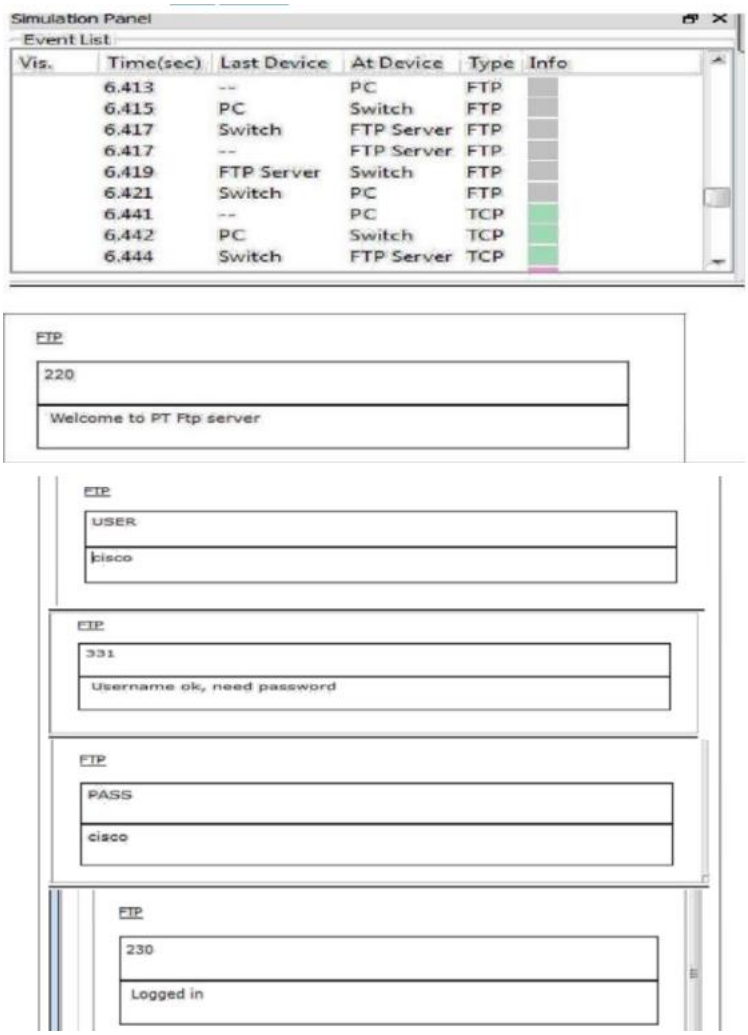


Simulation:

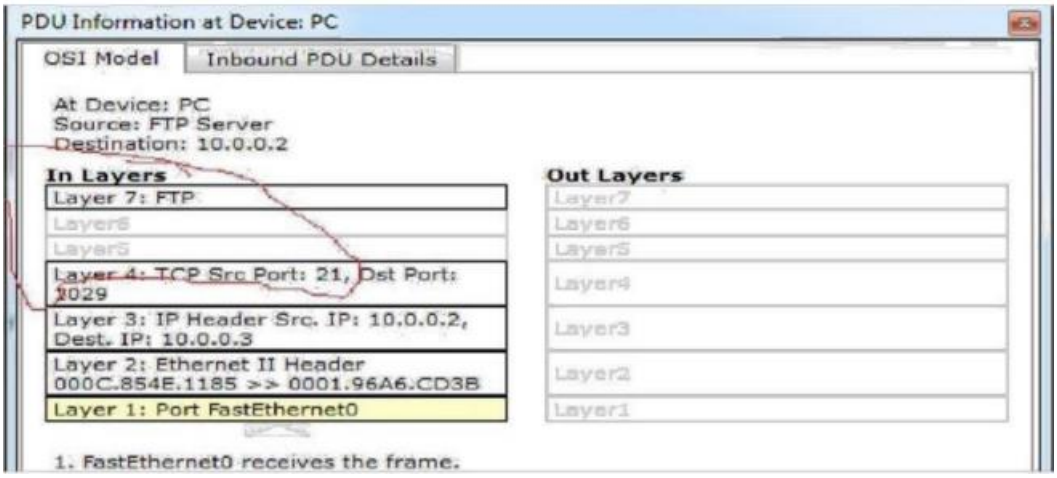
Select the simulation mode. Go to PC desktop command prompt again make connection with FTP server using its IP address.

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

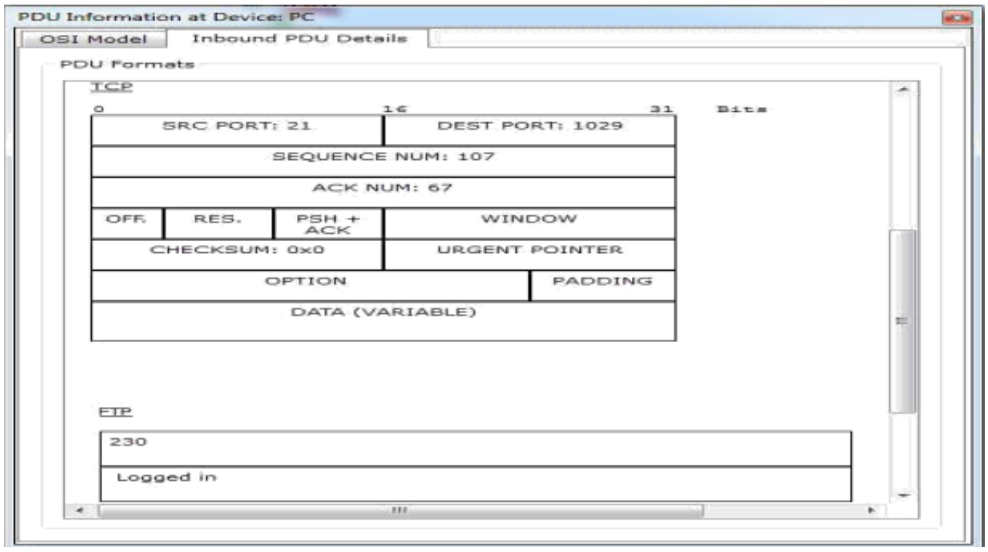
How FTP server resolves the login request.



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



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



Lab Exercises

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

a) Configure SMTP (create account with your last name along with last 3 digits roll number) 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.