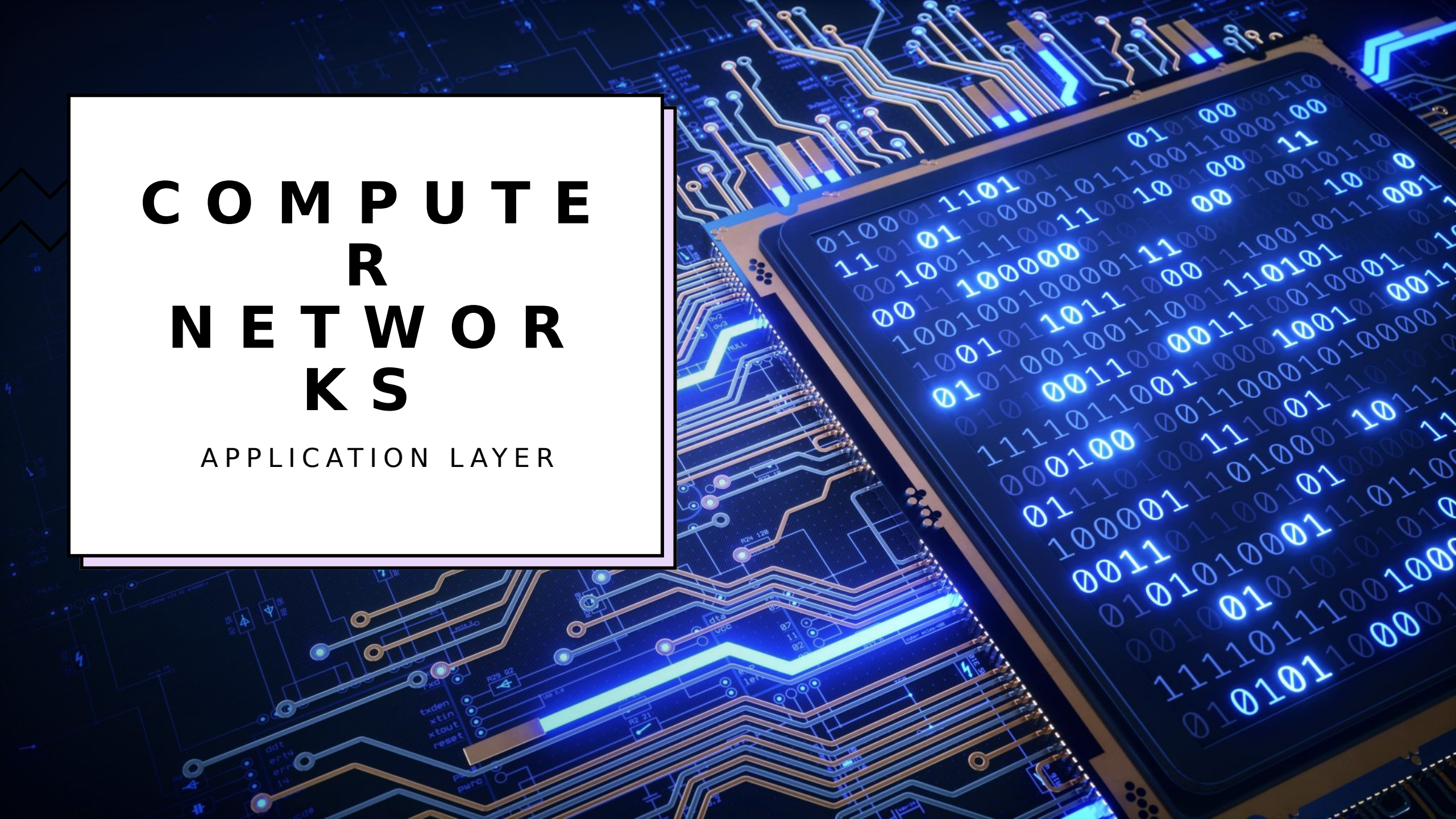


COMPUTER NETWORKS

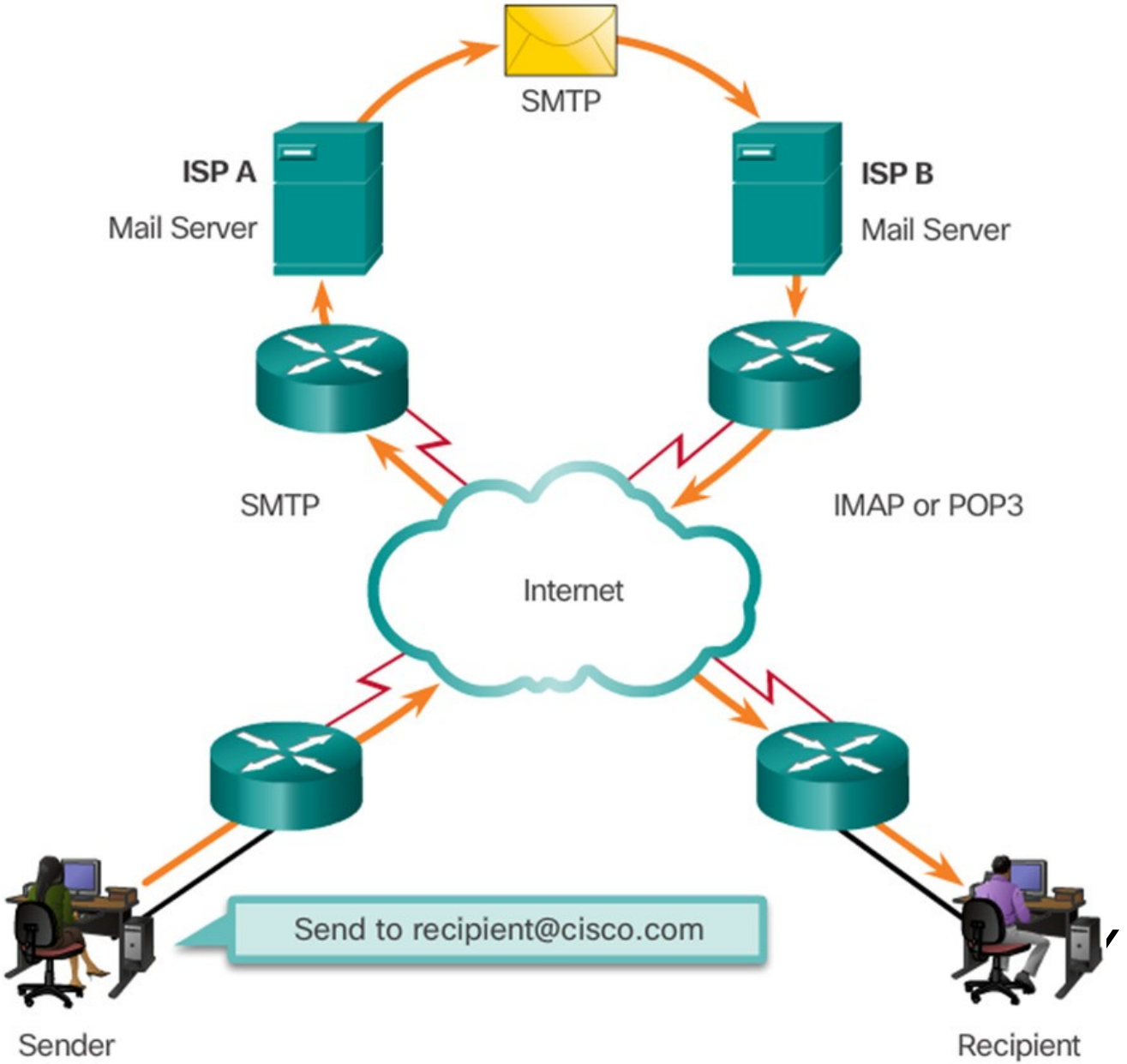
APPLICATION LAYER

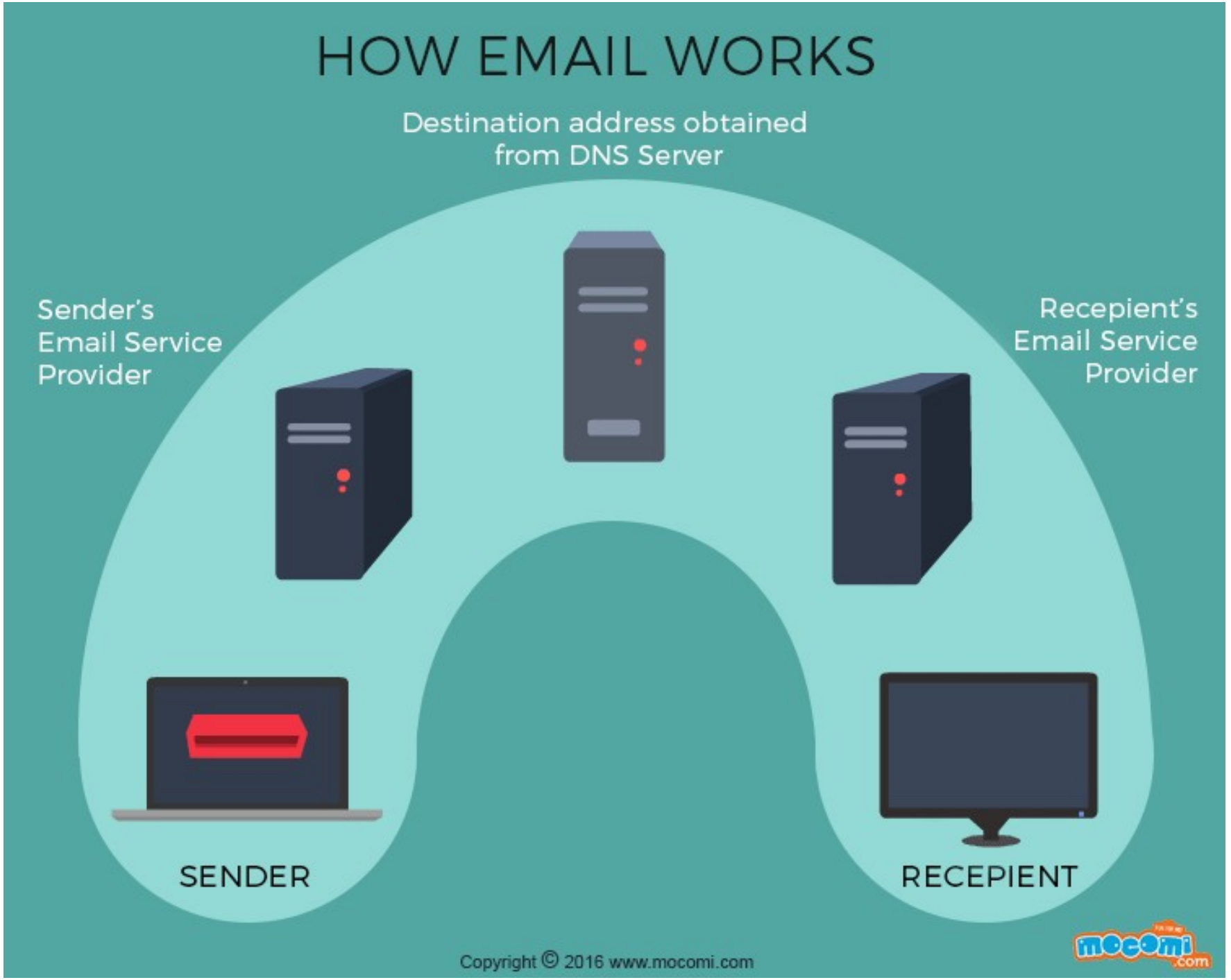
Topic of the day

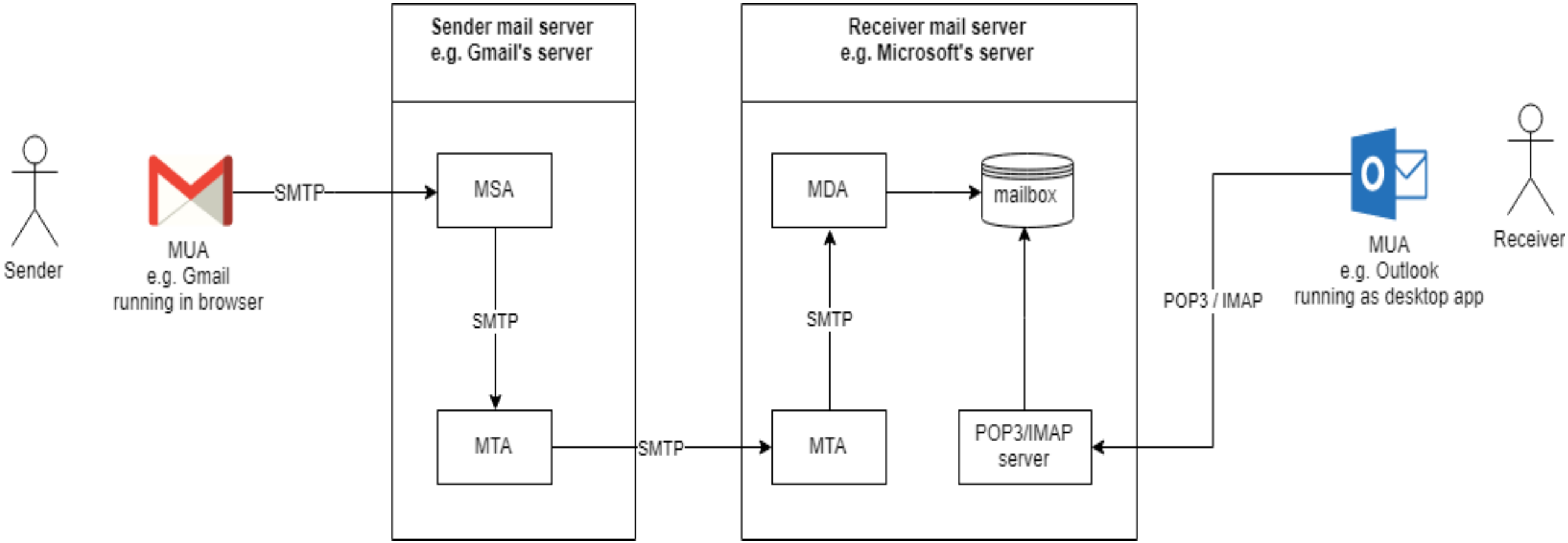
- Email Protocol
  - SMTP
  - POP3
  - IMAP
  - MIME
- IP Addressing Protocols
  - DNS

Email Protocol

- Email is a store-and-forward method of sending, storing, and retrieving electronic messages.
- Email messages are stored in databases on mail servers.
- Email clients communicate with mail servers to send and receive email.
- Mail servers communicate with other mail servers to transport messages from one domain to another.
- Email clients do not communicate directly when sending email.
- Email relies on three separate protocols for operation: SMTP (sending),POP (retrieving), IMAP (retrieving).




HOW EMAIL WORKS
Destination address obtained from DNS Server
Sender's Email Service Provider
Recepient's Email Service Provider
SENDER
RECEPIENT
Copyright © 2016 www.mocomi.com


Sender mail server
e.g. Gmail's server
Receiver mail server
e.g. Microsoft's server
Sender
MUA
e.g. Gmail
running in browser
SMTP
MSA
SMTP
MTA
SMTP
MDA
mailbox
SMTP
MTA
POP3/IMAP
server
POP3 / IMAP
MUA
e.g. Outlook
running as desktop app
Receiver

- **MUA (Mail User Agent) :**Client application that allows receiving and sending emails. It can be a desktop application such as Microsoft Outlook/Thunderbird/… or web-based such as Gmail/Hotmail/… (the latter is also called Webmail).
- **MSA (Mail Submission Agent):** A server program that receives mail from an MUA, checks for any errors, and transfers it (with SMTP) to the MTA hosted on the same server.
- **MTA (Mail Transfer Agent):** A server application that receives mail from the MSA, or from another MTA. It will find (through name servers and the DNS) the MX record from the recipient domain's DNS zone in order to know how to transfer the mail. It then transfers the mail (with SMTP) to another MTA (which is known as SMTP relaying) or, if the recipient's server has been reached, to the MDA.

  Examples of MTAs are Postfix, Exim, Sendmail, qmail, ...
- **MDA (Mail Delivery Agent):** A server program that receives mail from the server's MTA, and stores it into the mailbox. MDA is also known as LDA (Local Delivery Agent).

  An example is Dovecot, which is mainly a POP3 and IMAP server allowing an MUA to retrieve mail, but also includes an MDA which takes mail from an MTA and delivers it to the server's mailbox.
- **Mailbox: maildir/mbox:** The server's mail storage. Maildir is a way of storing email messages. It is usually preferable over mbox.

- **SMTP**

  Protocol used by MUAs to send emails to an MSA.

- **IMAP/POP3**

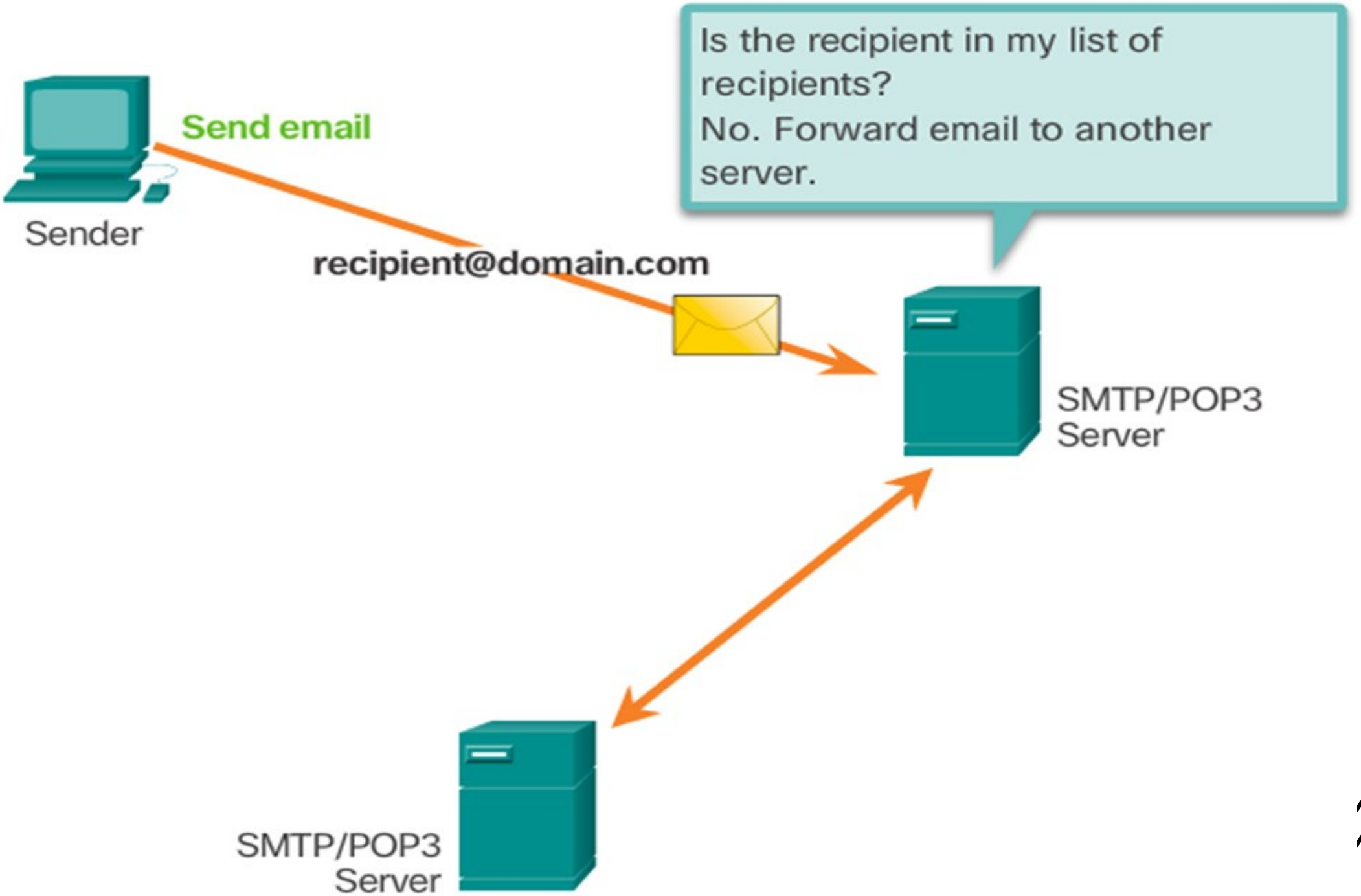
  Protocols used by MUAs to retrieve emails from a server mailbox. POP3 deletes the email messages from the server after they have been downloaded. IMAP is usually preferable as it maintains all email messages on the server, permitting management of a mailbox by multiple email clients.

- **MX (Mail Exchanger) record**

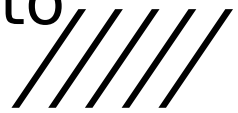
  A Mail Exchanger (MX) record in the DNS specifies which server is responsible for accepting email addresses on behalf of a domain. The host name from the MX record must map to one or more address record (A or AAAA) in the DNS, and must not point to any CNAME records.

SMTP Operation

- SMTP message formats require a message header and body.
- The body can contain any amount of text.
- The header must have a properly formatted recipient email address and a sender address.
- An SMTP client sends an email by connecting to a SMTP server **on port 25, 465(secure)**.
- The server receives the message and stores it message in a local mailbox or relays the message to another mail server.
- Users use email clients to retrieve messages stored on the server.
- IMAP and POP are two protocols commonly used by email clients to retrieve messages.


Is the recipient in my list of recipients?
No. Forward email to another server.
Send email
Sender
recipient@domain.com
SMTP/POP3 Server
SMTP/POP3 Server

- SMTP is application level protocol.
- SMTP is connection oriented protocol.
- SMTP is text based protocol.
- It handles exchange of messages between e-mail servers over TCP/IP network.
- Apart from transferring e-mail, SMPT also provides notification regarding incoming mail.
- When you send e-mail, your e-mail client sends it to your e-mail server which further contacts the recipient mail server using SMTP client.
- These SMTP commands specify the sender's and receiver's e-mail address, along with the message to be send.
- The exchange of commands between servers is carried out without intervention of any user.
- In case, message cannot be delivered, an error report is sent to the sender which makes SMTP a reliable protocol.



- **HELLO**

  This command initiates the SMTP conversation.

- **EHELLO**

  This is an alternative command to initiate the conversation. ESMTP indicates that the sender server wants to use extended SMTP protocol.

- **MAIL FROM**

  This indicates the sender’s address.

- **RCPT TO**

  It identifies the recipient of the mail. In order to deliver similar message to multiple users this command can be repeated multiple times.

- **SIZE**

  This command let the server know the size of attached message in bytes.

- **DATA**

  The DATA command signifies that a stream of data will follow. Here stream of data refers to the body of the message.

- **QUIT**

  This commands is used to terminate the SMTP connection.

- **VERFY**

  This command is used by the receiving server in order to verify whether the given username is valid or not.

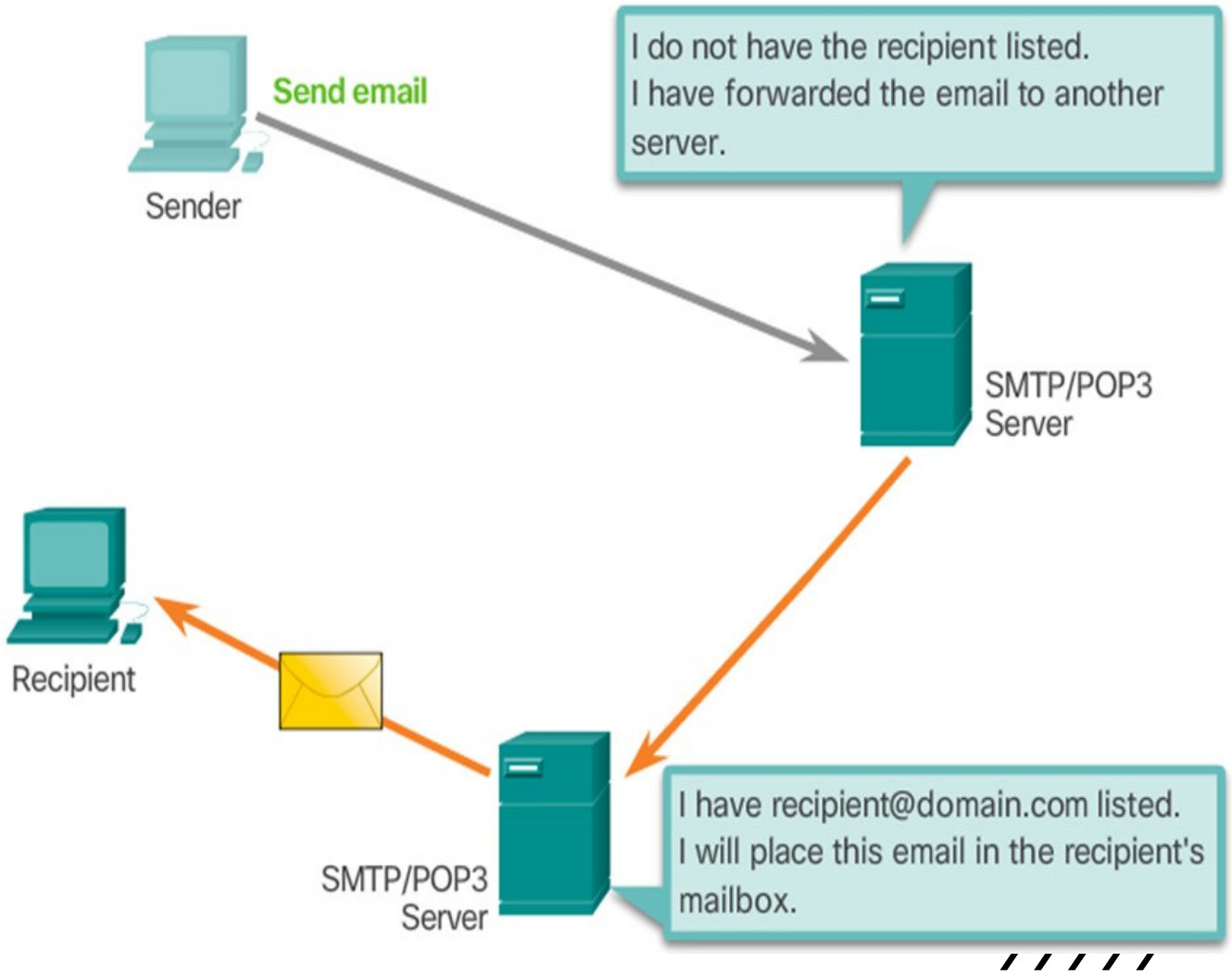
- **EXPN**

  It is same as VRFY, except it will list all the users name when it used with a distribution list.

Client does:	Server normally responds with:
Connects to the server	`220 Helo there`
`HELO` **`client-hostname`**	`250 Pleased to meet you`
`MAIL FROM:<`**`Sender address`**`>`	`250 OK`
`RCPT TO:<`**`Recipient address`**`>` (May be repeated)	`250 OK`
`DATA`	`354 Start mail input; end with <CRLF>.<CRLF>`
Sends the actual email message	(Nothing, it's waiting for the . that ends the message)
.	`250 OK, accepted for delivery`

POP Operation

- Messages are downloaded from the server to the client.
- The server listens on **port 110, 995(secure) TCP** for client requests.
- Email clients direct their POP requests to mail servers on port TCP 110.
- The POP client and server exchange commands and responses until the connection is closed or aborted.
- POP allows for email messages to be downloaded to the client's device (computer or phone) and removed from the server.
- There is no centralized location where email messages are kept.
- A downloaded message resides on the device that triggered the download.

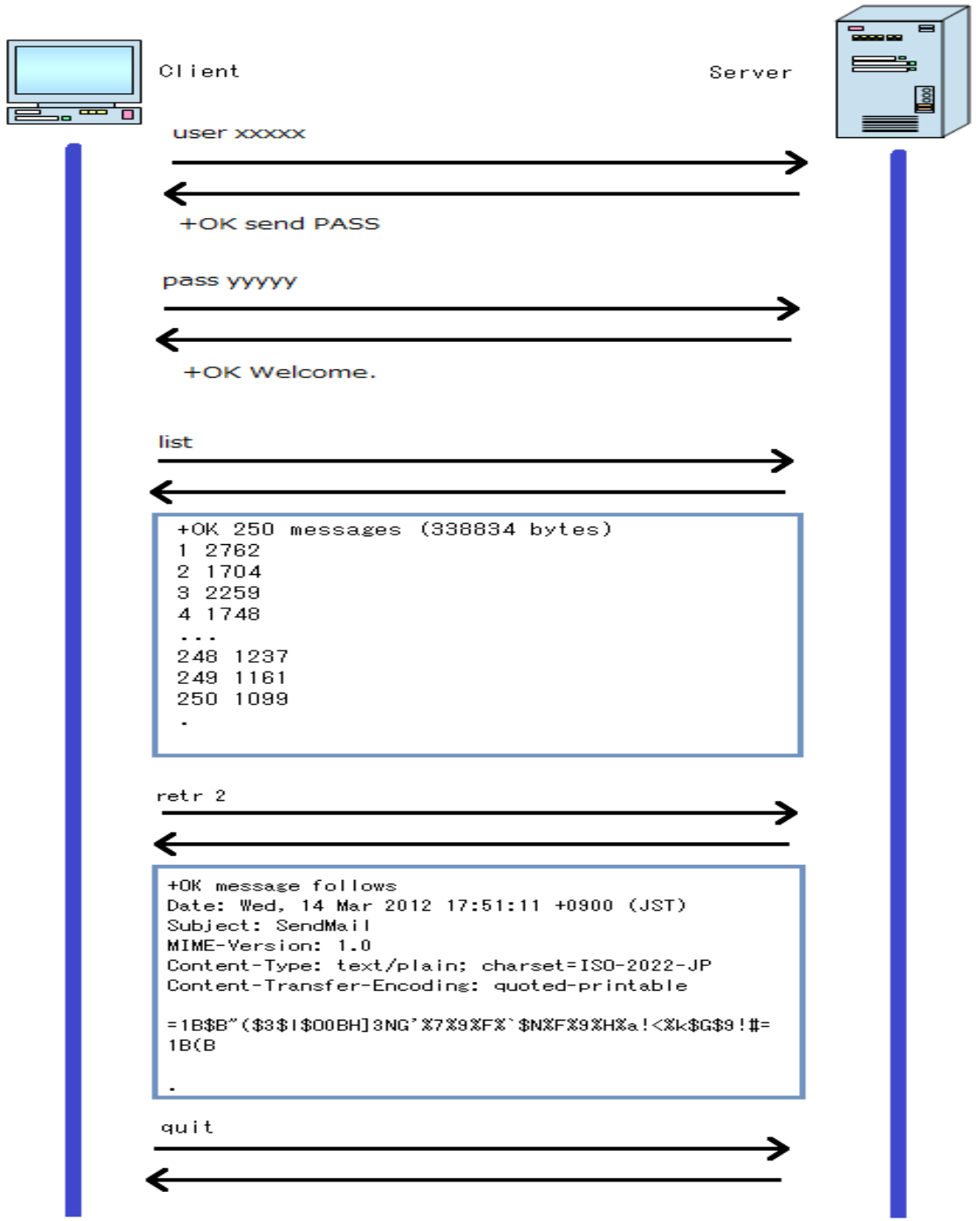


- POP is an application layer internet standard protocol.
- Since POP supports offline access to the messages, thus requires less internet usage time.
- POP does not allow search facility.
- In order to access the messaged, it is necessary to download them.
- It allows only one mailbox to be created on server.
- It is not suitable for accessing non mail data.
- POP commands are generally abbreviated into codes of three or four letters. Eg. STAT.

S.N.	Command Description
1	**LOGIN** This command opens the connection.
2	**STAT** It is used to display number of messages currently in the mailbox.
3	**LIST** It is used to get the summary of messages where each message summary is shown.
4	**RETR** This command helps to select a mailbox to access the messages.
5	**DELE** It is used to delete a message.
6	**RSET** It is used to reset the session to its initial state.
7	**QUIT** It is used to log off the session.

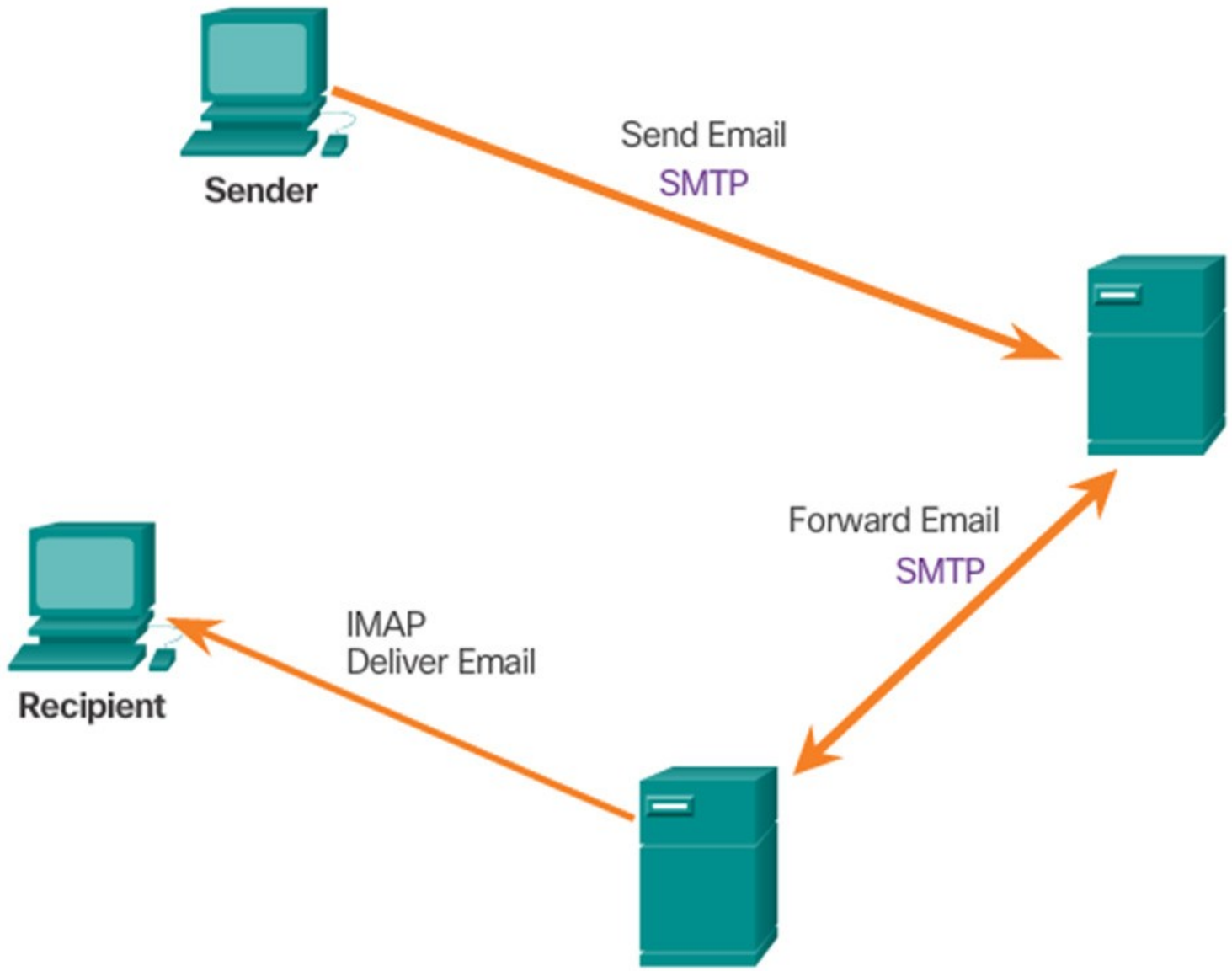
Here is the basic flow to receive mail:

- Open connection
- Authenticate
- List
- Retr
- Quit



IMAP Operation

- IMAP is another protocol used to retrieve email messages.
  - Allows for messages to be displayed to the user rather than downloaded
  - The original messages reside on the server until manually deleted by the user.
  - Users view copies of the messages in their email client software.
  - Users can create a folder hierarchy on the server to organize and store mail.
  - That file structure is displayed on the email client.
  - When a user decides to delete a message, the server synchronizes that action and deletes the message from the server.



- IMAP allows the client program to manipulate the e-mail message on the server without downloading them on the local computer.
- The e-mail is hold and maintained by the remote server.
- It enables us to take any action such as downloading, delete the mail without reading the mail.It enables us to create, manipulate and delete remote message folders called mail boxes.
- IMAP enables the users to search the e-mails.
- It allows concurrent access to multiple mailboxes on multiple mail servers.

Home TASK

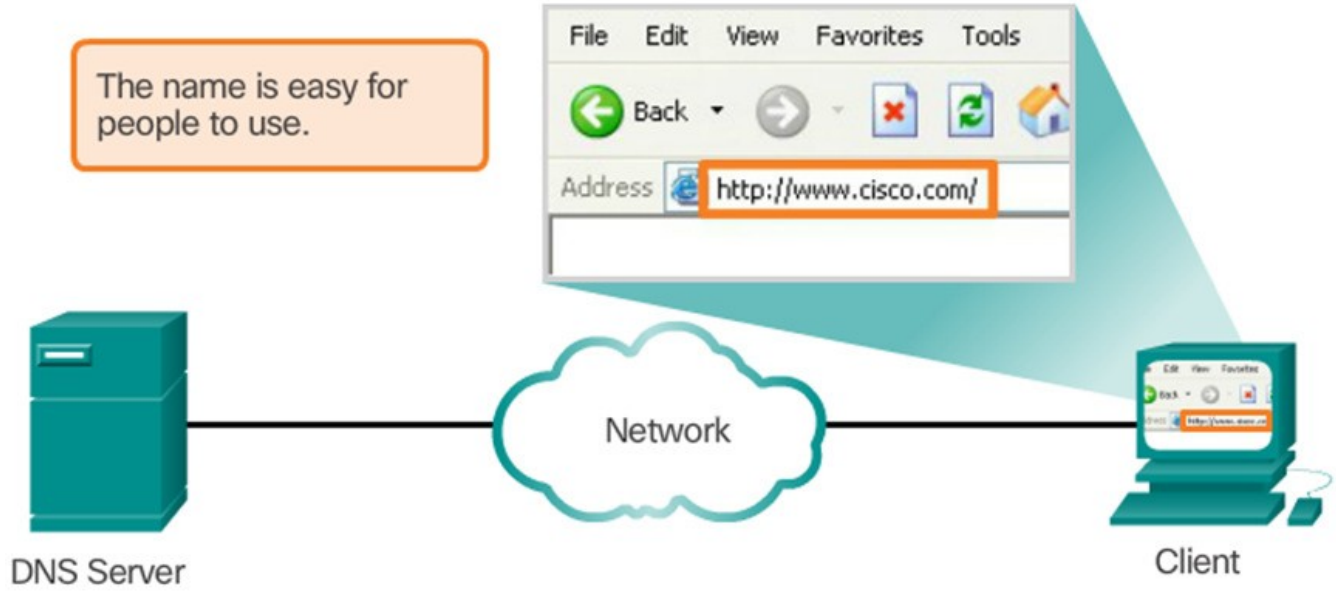
- Explore MIME
- Write a short report on its working.
- Identify the issues(security and performance) in it?

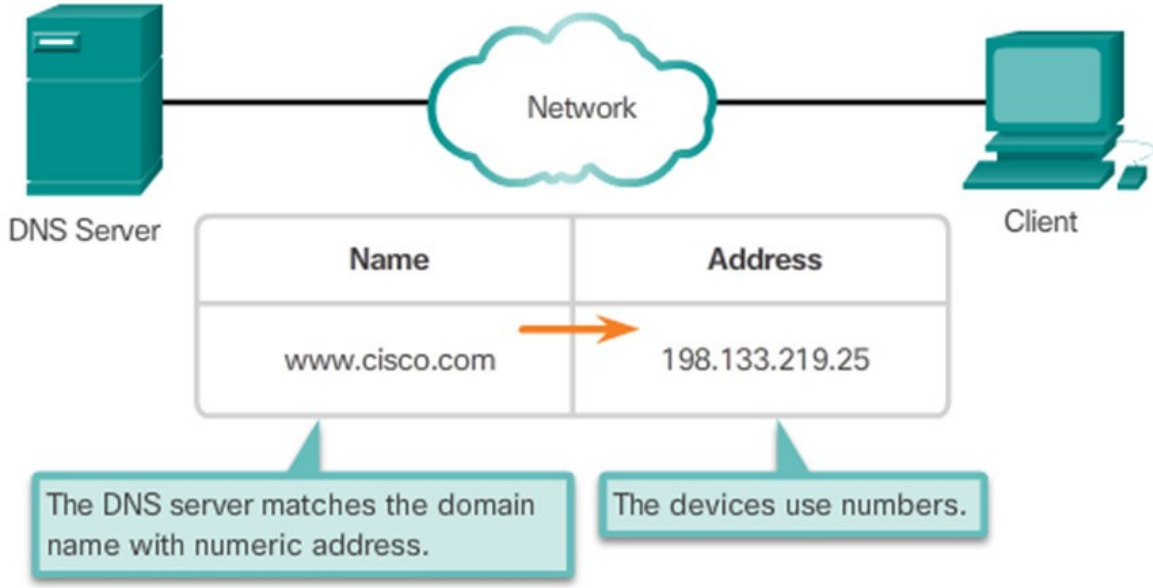
IP Addressing Protocols - DNS

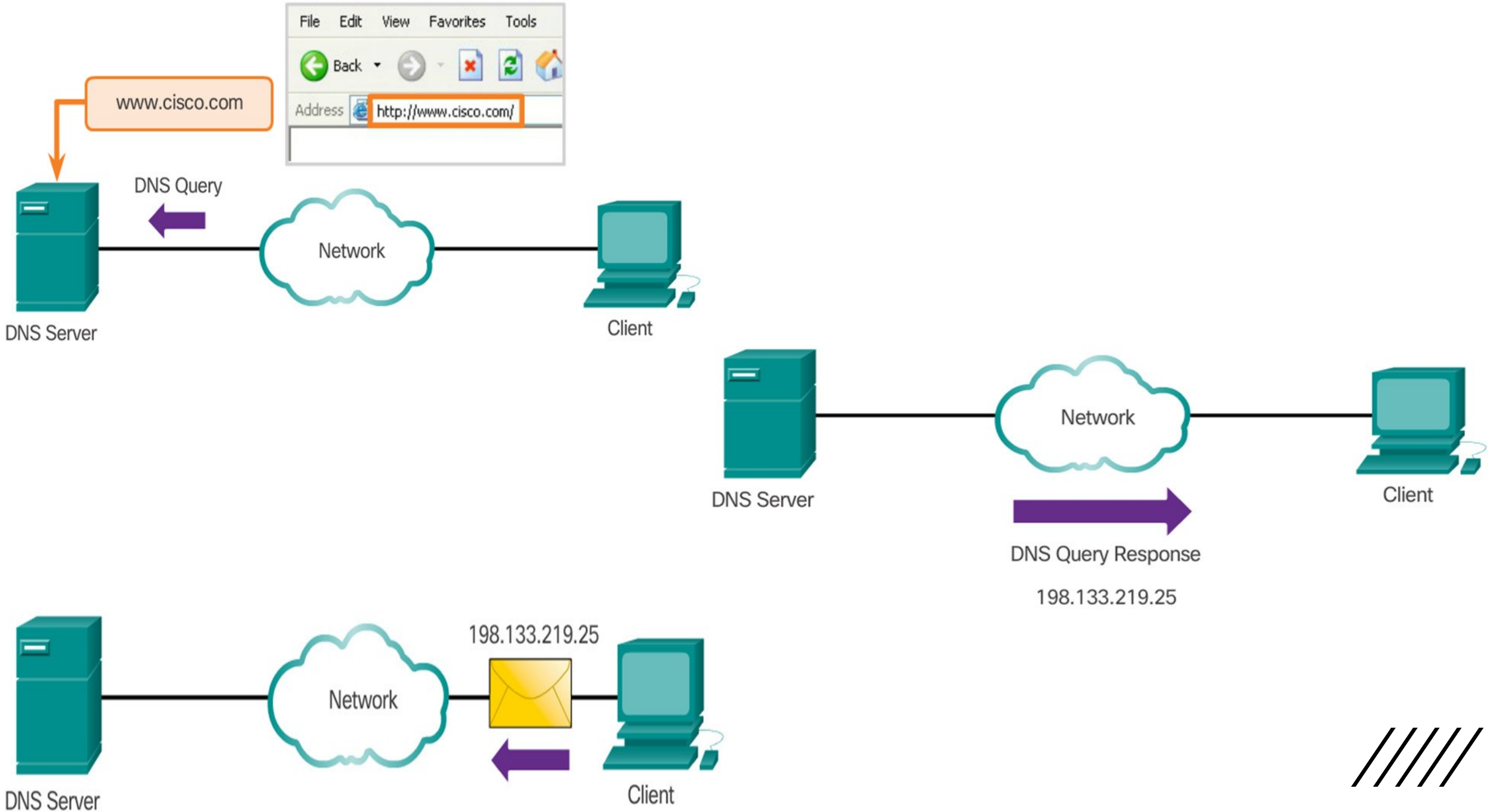
- Domain Name System
- While IP addresses are crucial for network communication, they are not easy to memorize.
- Domain names are created to make server addresses more user-friendly.
- Domain names such as http://www.cisco.com are user-friendly addresses associated with the IP address of a specific server.
- However, computers still need the actual numeric address before they can communicate.

Domain Name System

- The DNS protocol allows for the dynamic translation of a domain name into the correct IP address.
- The DNS protocol communications using a single format called a message.





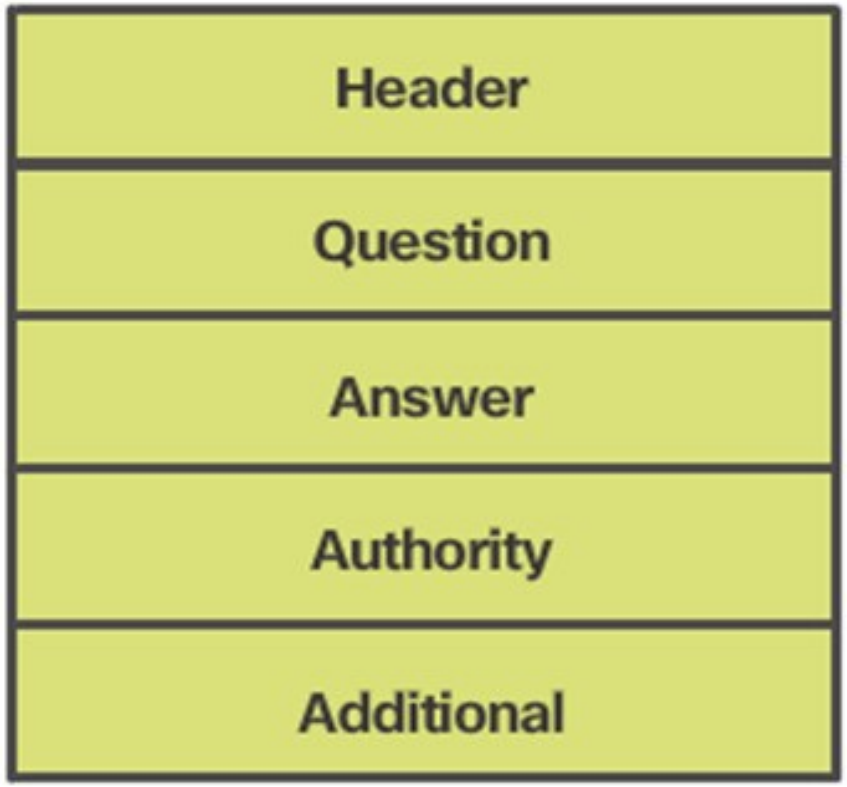

File Edit View Favorites Tools
Back
Address
http://www.cisco.com/
www.cisco.com
DNS Query
Network
DNS Server
Client
Network
DNS Server
Client
DNS Query Response
198.133.219.25
198.133.219.25
Network
DNS Server
Client

DNS Message Format

- DNS supports different types of records. Some of these record types are:
  - **A** - An end device IPv4 address
  - **NS** - An authoritative name server
  - **AAAA** - An end device IPv6 address (pronounced quad-A)
  - **MX** - A mail exchange record
- DNS servers will first look at its own records to resolve the name. If the server is unable to resolve the name using its locally stored records, it relays the query to other servers.
- The response is then forwarded to the requesting client.
- The DNS Client service on Windows PCs also stores previously resolved names in memory.
- **ipconfig /displaydns** displays all of the cached DNS entries on

DNS uses the same message format for:

- all types of client queries and server responses
- error messages
- the transfer of resource record information between servers



The question for the name server

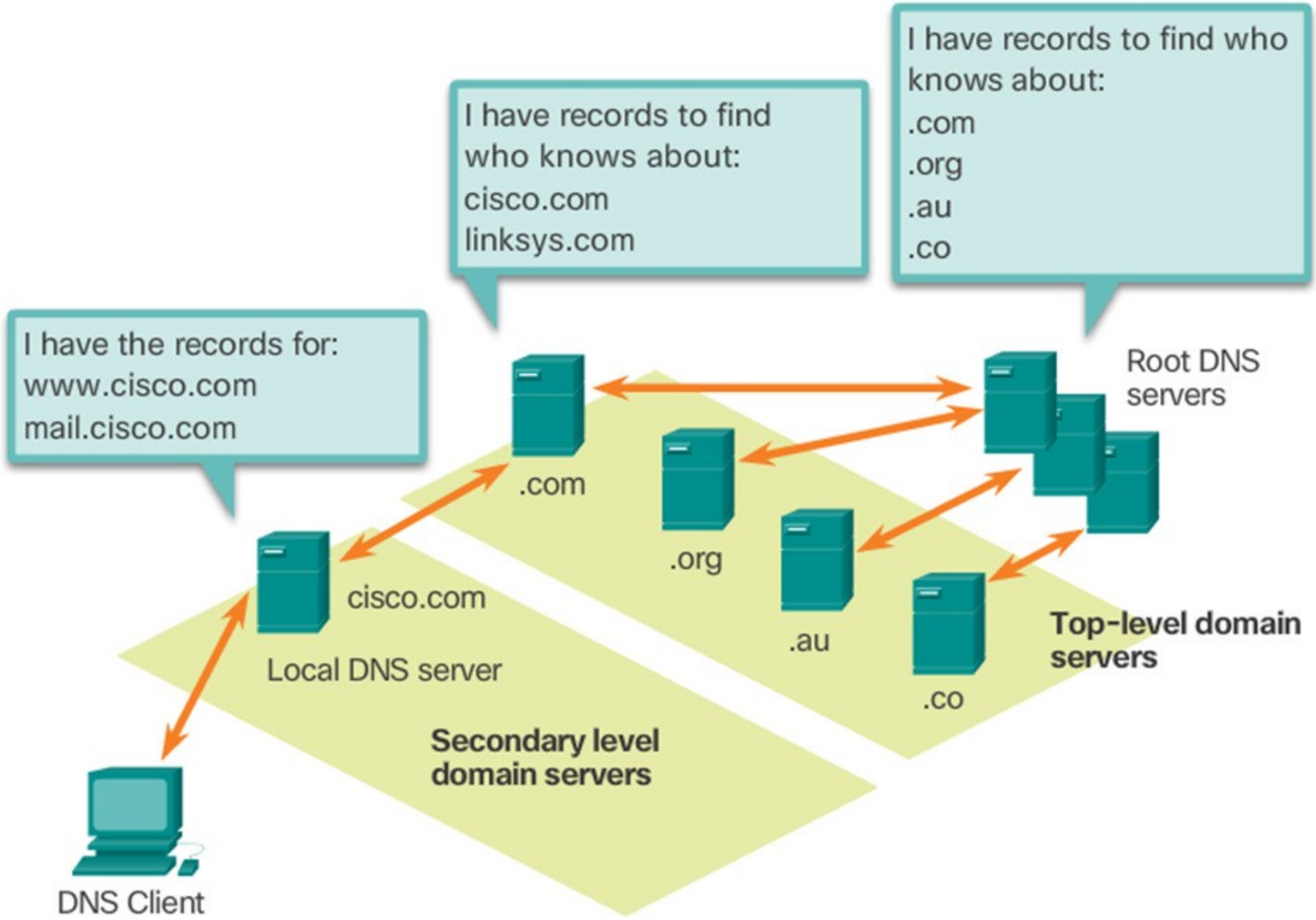
Resource Records answering the question

Resource Records pointing toward an authority

Resource Records holding additional information

DNS Hierarchy

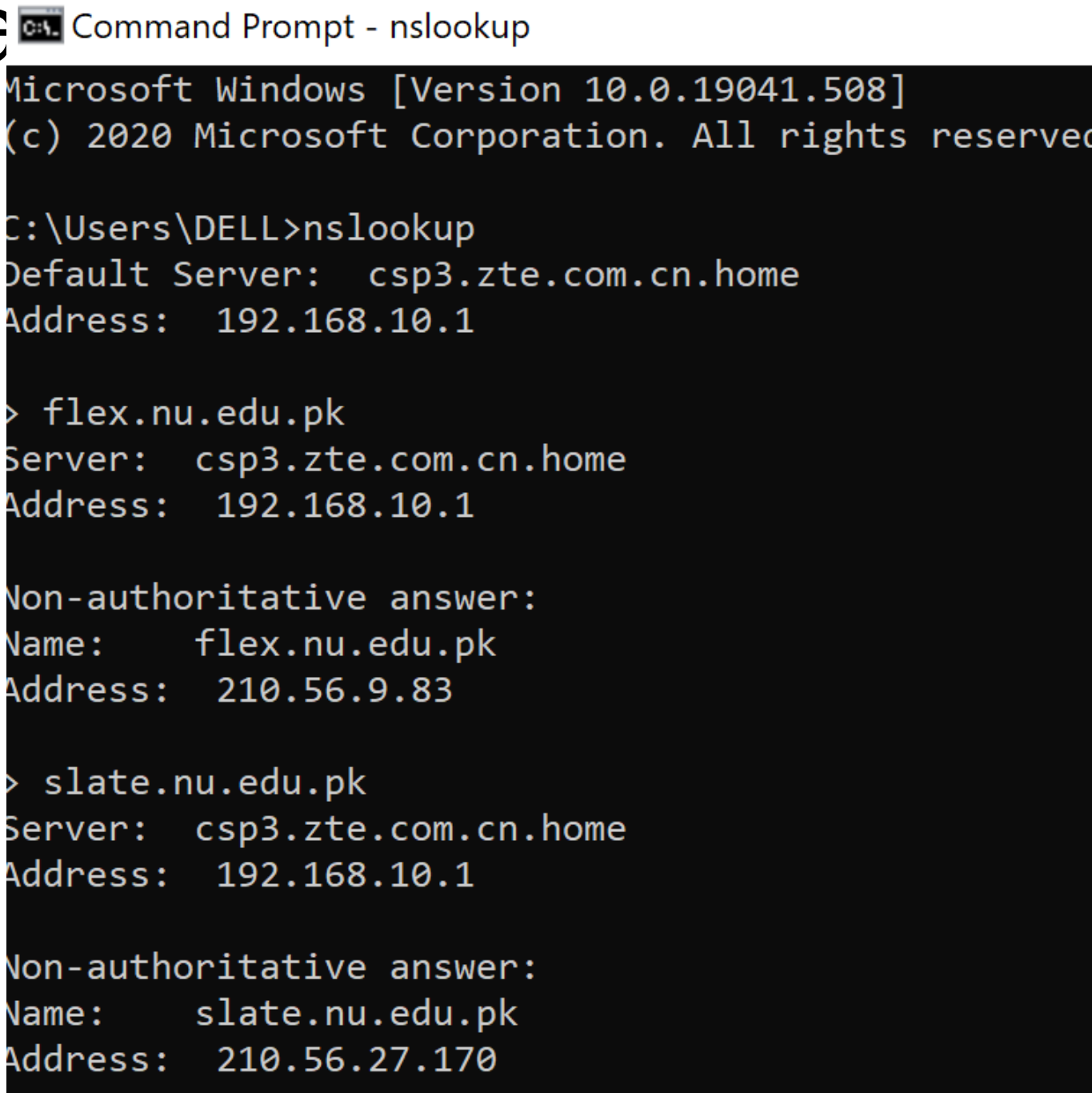
- The DNS protocol uses a hierarchical system, with the root at the top and branches below. The naming structure is broken down into small, manageable zones.
- Each DNS server is only responsible for managing name-to-IP mappings for that small portion of the DNS structure.
- Requests for zones not stored in a specific DNS server are forwarded to other servers for translation.
- Top-level domains represent either the type of domain or the country of origin.
- Examples of top-level domains are:
    - **.com** - a business or industry
    - **.org** - a non-profit organization
    - **.au** - Australia
    - **.co** - Colombia


I have records to find who knows about:
.com
.org
.au
.co
I have records to find who knows about:
cisco.com
linksys.com
I have the records for:
www.cisco.com
mail.cisco.com
Root DNS servers
.com
.org
.au
.co
cisco.com
Local DNS server
Top-level domain servers
Secondary level domain servers
DNS Client

Nslookup Comma

- Allows the user to manually place DNS queries.
- It can also be used to troubleshoot name resolution issues.
- Has many options available for extensive testing and verification of the DNS process.

- DDNS: Dynamic Domain Name System
- DNS Caching



DNS Security Issues

- Major attacks:
- DNS Hijacking
- Cache Poisoning/ DNS Spoofing
- DNS DOS attack

- DNS SEC

References

- https://www.siteground.com/tutorials/email/protocols-pop3-smtp-imap/#:~:text=By%20default%2C%20the%20IMAP%20protocol,to%20connect%20using%20IMAP%20securely

  .
- https://afreshcloud.com/sysadmin/mail-terminology-mta-mua-msa-mda-smtp-dkim-spf-dmarc
- https://www.ukessays.com/essays/computer-science/email-protocol-smtp-pop-mime-9752.php
- https://www.codeproject.com/Articles/404066/Understanding-the-Insides-of-the-POP3-Mail-Protoco
- https://www.tutorialspoint.com/internet_technologies/e_mail_protocols.htm