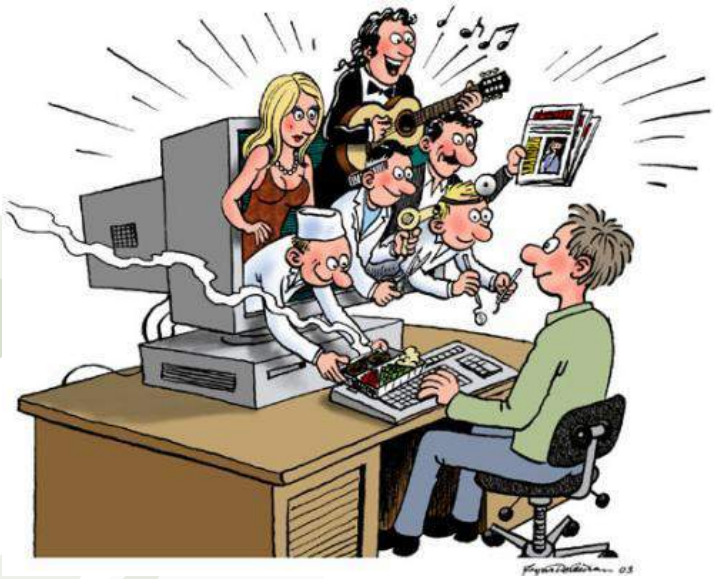
Basic of Internet and Web Technology

Shyamalendu Kandar,
Assistant Professor, IT.
IIEST, Shibpur

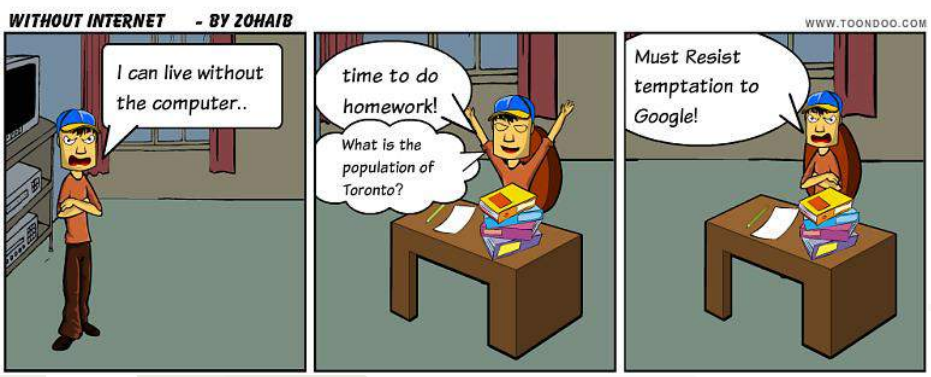


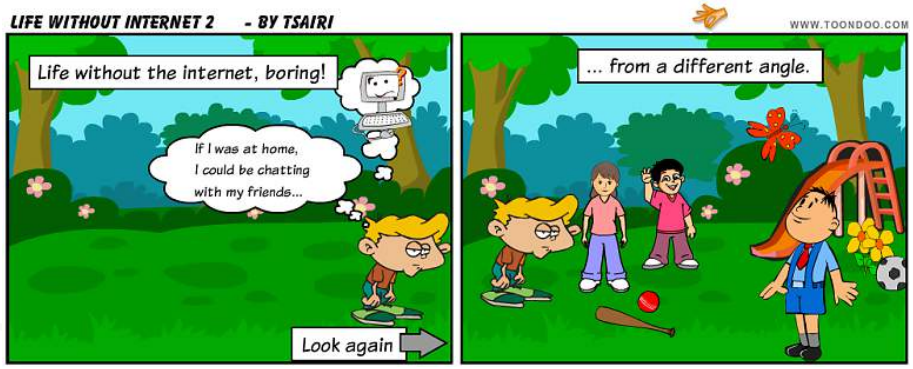
Few things which are obsolete !

Imagine….

A world without internet……

- ✓Communication
- ✓Business—Banking, Stock market
- ✓Access to information & resources cut
- ✓Screaming of teenagers ---no facebook, whatsapp





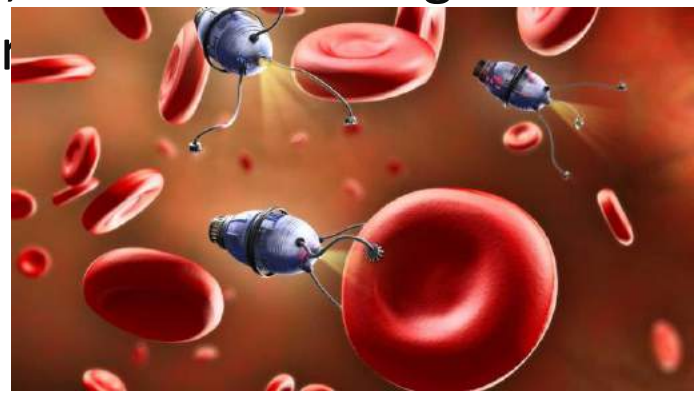
Driving forces of today's world

- Commoditization: cost of goods, cost of distribution, and pricing
- digital revolution
- social mediaization throughout society
- globalization
- the turbulent world (Obviously bad) : disputes among different different nations
- Acceleration : towards good

The future world..

Nanobots will plug our brains straight into the cloud

(virtual reality, solution for forget about memory problems, evidence pr



People reincarnation through AI : will be possible to create a convincing virtual version of somebody who's passed on.

IoT technology will change product designs

Space tourism: a week in orbit

Self-driving cars will make driving safer

Power from a plant: generating electricity from plant's photosynthesis

Ocean Thermal Energy can take us to 100% renewable-energy

Drone as flying car

24 X 7 health care and monitoring

Internet ……Definition

- The Internet, sometimes called simply "the Net," is a worldwide system of computer networks - a network of networks in which users at any one computer can, if they have permission, get information from any other computer (and sometimes talk directly to users at other computers).

-------**Definition from WhatIs.com**

The **Internet** is the global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link devices worldwide. It is a *network of networks* that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies. The Internet carries an extensive range of information resources and services, such as the inter-linked hypertext documents and applications of the World Wide Web (WWW), electronic mail, telephony, and file sharing.

……**From wikipedia**

Web Technology-----Definition

- **Web technology** refers to the means by which computers communicate with each other using markup languages and multimedia packages. It gives us a way to interact with hosted information, like websites.

Internet Vs Web Technology

- global network connecting millions of computers.
- decentralized.
- Each Internet computer is independent.
- variety of ways to access the Internet.
- more than 3,700,000,000 Internet Users in the world.

- system of Internet servers that support specially formatted documents.
- Documents are formatted in a markup language that supports links to other documents.
- can jump from one document to another simply by clicking on hot spots (hyperlinks).
- Applications called Web browsers that make it easy to access the World Wide Web.
- more than 1,275,000,000 Websites.

World wide web

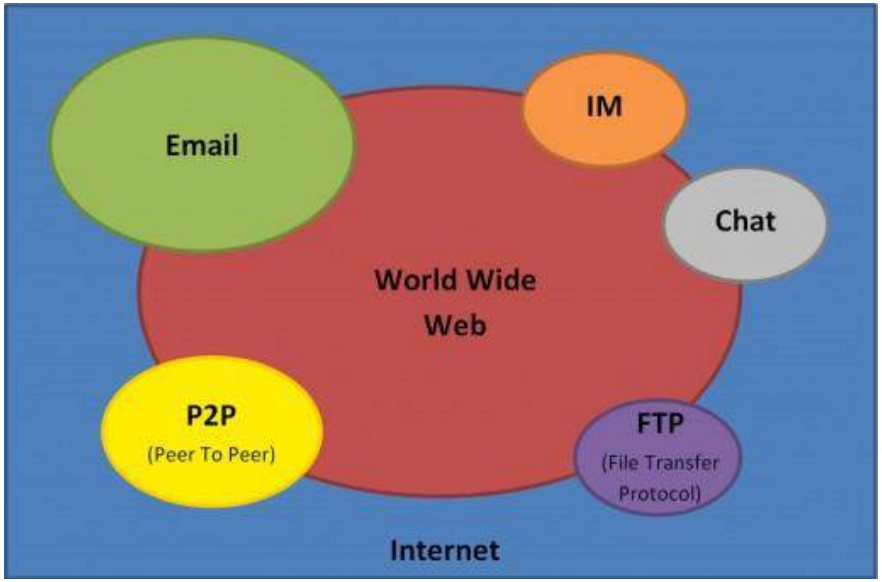
- an information system on the Internet which allows documents to be connected to other documents by hypertext links, enabling the user to search for information by moving from one document to another.

Internet VS www

World Wide Web (WWW) is one

set of software services running on the Internet.

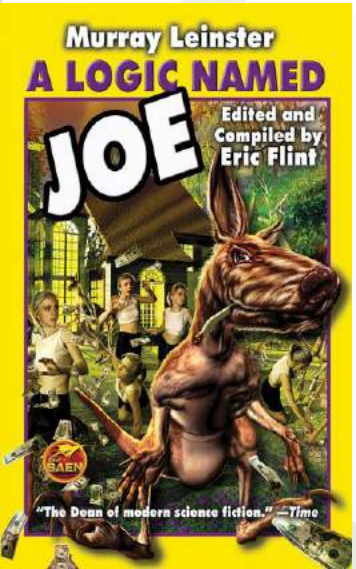
The **Internet** itself is a global, interconnected network of computing devices. This network supports a wide variety of interactions and communications between its devices. The World Wide Web **is a subset of these interactions and supports websites and URI**s.



	Internet	WWW
Estimated year of Origin	1969 . But commercial interests began only in 1988	1993
Name of the first version	ARPANET	NSFnet
Comprises	Network of Computers, copper wires, fibre-optic cables & wireless networks	Files, folders & documents stored in various computers
Governed by	Internet Protocol	Hyper Text Transfer Protocol
Dependency	This is the base, independent of the World Wide Web	depends on Internet to work
Nature	Hardware	Software

History of Internet

- 1946 American fiction story writer Murray Leinster
- Story was “A Logic Named Joe”
- concept of computer terminal called ‘logic’ were in every home.
- envisioned logics in every home, linked through a distributed system of servers (called "tanks"), to provide communications, entertainment, data access, and even commerce. One of his characters says that *logics are civilization*.



History of Internet

- After the Second World War Soviet Union also acquired the nuclear power.
- United States of America were frightened of nuclear attack from Soviet Union.
- U.S military wanted a strong communication infrastructure so that the scientist, politicians, diplomats can communicate with each other at the war time hiding in the underground bunkers!

- In October 1962, United States of America department of Defense (USA Defense) started a project of information processing to difference branches of it under the Defense's Advance Research Projects Agency (DARPA).
- J.C.R. Licklider appointed as the head of the project.
- three stations were set up. A)System Development Corporation (S.D.C.) in Santa Monica B) Project Genie at the University of California, Berkeley and C) Massachusetts Institute of Technology (MIT).
- The three terminals were governed by three different sets of user commands. If any one of any of the terminals wants to communicate with anyother situated in different terminals he has to get up from the main terminal(S.D.C or California or MIT) and login into the other terminal to enter into the node.

- In an interview Licklider told

“I said, it's obvious what to do (But I don't want to do it): If you have these three terminals, there ought to be one terminal that goes anywhere you want to go where you have interactive computing. That idea is the ARPAnet."

- 1961 :Paul Baran introduced the concept of Packet Switching. It was store & forward switching.
- This technology gives a better bandwidth utilization than message switching.
- first used in the Advance Research Projects Agency (ARPA).
- In 1969 Robert Taylor first established an ARPAnet link between University of California and the Stanford Research Institute.
- gave birth to a new term in Computer Sc called internet (small ‘i’) which is nothing but network of computer networks.

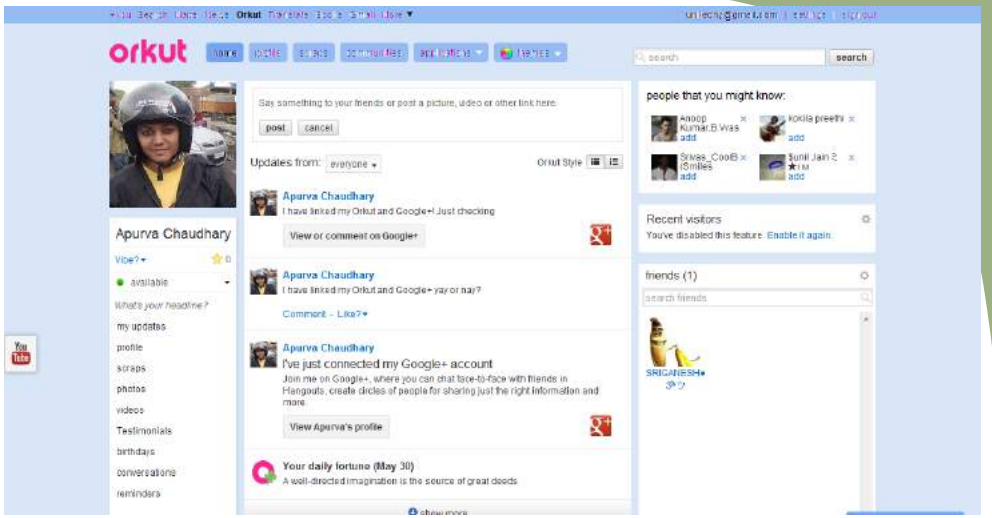
- Number of such network increases.
- need of addressing scheme to recognize each such physically separated computer networks.
- As addressing scheme was introduced, scientists realized the need of a new device to transfer the data packets correctly to the physically separated computer networks. This device is called router.
- researchers of different countries started developing new networks such as CSNET, NEARnet, SERCnet, JAnet etc.
- early 1980, 10 such different networks were formed and stated to communicating among them. This is known as Internet (Capital ‘I’).

Internet timeline….

1965	Two computers at MIT Lincoln Lab communicate with one another
1968	Interface Message Processor (IMP) specifications
1969	The first message is "LO, [LOGIN] sent by Charles Kline
1972	Ray Tomlinson introduces network email.
1973	University College of London (England) and Royal Radar Establishment (Norway) connect to ARPANET. The term Internet is born.
1974	first Internet Service Provider (ISP) is born with the introduction of a commercial version of ARPANET, known as Telenet.
1976	Vinton Cerf and Bob Kahn developed Protocol for Packet Network Interconnection," which details the design of TCP. Queen Elizabeth II hits the “send button” on her first email.
1982	Transmission Control Protocol (TCP) and Internet Protocol (IP), as the protocol suite, commonly known as TCP/IP, emerge as the protocol for ARPANET.

1983	Domain Name System (DNS) establishes the familiar .edu, .gov, .com, .mil, .org, .net, and .int system for naming websites
1985	Symbolics.com, the website for Symbolics Computer Corp. in Massachusetts, becomes the first registered domain.
1987	hosts on the Internet exceeds 20,000. Cisco ships its first router.
1990	Tim Berners-Lee, a scientist at CERN develops HyperText Markup Language (HTML).
1993	Marc Andreesen develops the Mosaic Web browser at the University of Illinois,
1994	Netscape Communications is born. Microsoft creates a Web browser for Windows 95. yahoo! is created by Jerry Yang and David Filo
1997	Microsoft come with new browser. Browser was begins. First mobile internet by Nokia
1998	Google search engine is born IPV6 introduced, first 3G
2000	The dot-com bubble bursts. Web sites such as Yahoo! and eBay are hit by a large-scale denial of service attack,
2003	Android, skype
2004	Orkut launches. Entry to social networking. Facebook launches
2005	Youtube launches


MR
Google!
BETA
Search the web using Google!
Google Search
I'm feeling lucky
Special Searches
Stanford Search
Linux Search
Help!
About Google!
Company Info
Google! Logos
Get Google! updates monthly:
your e-mail
Subscribe
Archive
Copyright ©1998 Google Inc.
Google in 1998


orkut
search
Say something to your friends or post a picture, video or other link here.
post
cancel
Updates from: everyone
Orkut Style
Apurva Chaudhary
I have linked my Orkut and Google+! Just checking
View or comment on Google+
Apurva Chaudhary
I have linked my Orkut and Google+ yay or nay?
Comment - Like?
Apurva Chaudhary
I've just connected my Google+ account
Join me on Google+, where you can chat face-to-face with friends in Hangouts, create circles of people for sharing just the right information and more.
View Apurva's profile
Your daily fortune (May 30)
A well-directed imagination is the source of great deeds
people that you might know:
Recent visitors
friends (1)
SRIGANESH


Yahoo - A Guide to WWW
[What's New? | What's Cool? | What's Popular? | Stats | A Random Link]
Top
Up
Search
Mail
Add
Help
Art(466)
Business(6426)
Computers(2609)
Economy(743)
Education(1487)
Entertainment(6199)
Environment and Nature(193)
Events(53)
Government(1031)
Health(367)
Humanities(163)
Law(163)
News(185)
Politics(148)
Reference(474)
Regional Information(2606)
Science(2634)
Social Science(93)
Society and Culture(648)
23836 entries in Yahoo [Yahoo | Up | Search | Mail | Add | Help]
Copyright © 1994 David Filo and Jerry Yang

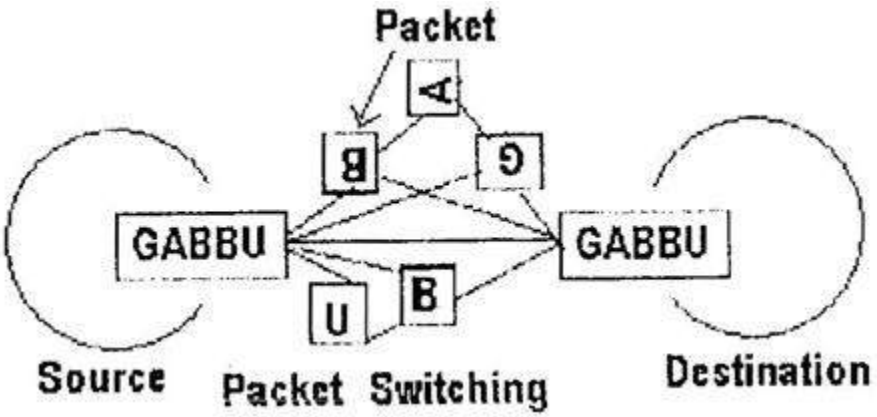

[thefacebook]
home search global social net invite faq logout
Profile (This is you)
Scranton
quick search
Picture
Information
Account Info:
Basic Info:
Extended Info:
Connection
This is you.
Access
is currently logged in from a non-residential location.

First youtube video “Me at the zoo”

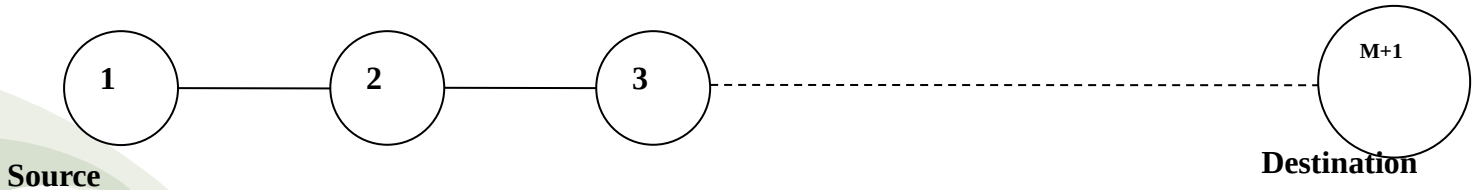
2006	Twitter launched
2007	Flipkart
2008	Apple app store with 500 apps
2009	Whatsapp, first 4G

Why Packet Switching?

- whole message is broken up into a number of smaller but optimal pieces.
- called packets.
- Each packet is attached with a header which includes destination address, packet number (Sequence Number).
- As the size of each packet is much smaller than the size of the whole message, much less time is required to transmit each packet from one node to another.
- Pipelining effect is included a great benefit to packet switching.



Lets’ compare Message and Packet Switching…



- **For Message Switching:**

- between M+1 numbers of nodes there are M links
- transmitting a message of size S between two consecutive node time required is S/C [C is the link speed].
- Transmit from source to destination time required is **M.S/C.**
- As the size of the header is much less than the size of the message so it is ignored at the time of calculation.

- **For Packet Switching**

Let the total message is divided into N number of equal sized packets. Let each packet is attached with a headed of size h. So size of each packet is (S/N + h).

transmitting the first packet from source to destination time is[M(S/N + h)]/C

- For the next each (S/N + h)/C time, one packet will be received at the destination.[Pipeline Effect for last (N-1) packets]
- Total time to transmit the message of size S from source to destination is

[M(S/N + h)]/C + (N-1)(S/N + h)/C

[First Packet] [Rest N-1 packets]

Total amount of data transfer during message switching is M [Header size is negligible]

Total amount of data transfer during packet switching is M + N.h [Header of size h for N packets]

(Time required for Packet Switching)

(Time required for Message Switching)

➔ $$\frac{[M(S/N + h)]/C + (N-1)(S/N + h)/C}{MS/C}$$

➔ $$\frac{M(S/N + h) + (N-1)(S/N + h)}{MS}$$

➔ $$\frac{[M+(N-1)]\ [S/N +h]}{MS}$$

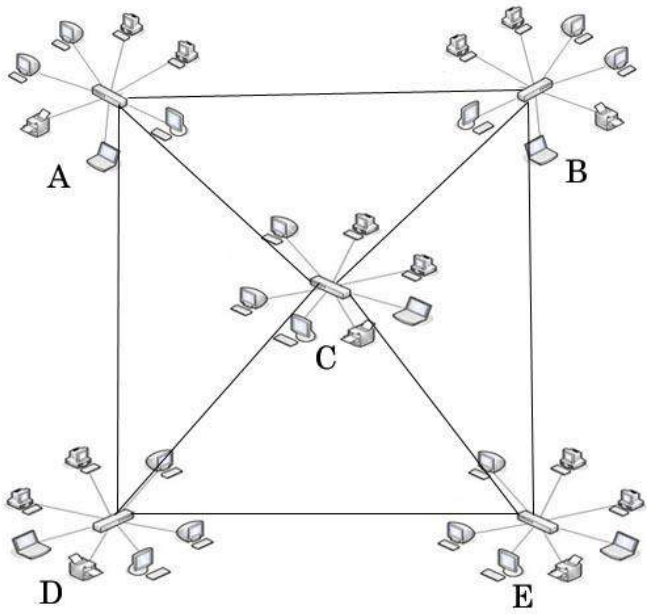
➔ $$\frac{[M+(N-1)]}{M} \times \frac{[S/N +h]}{S}$$

➔ $[1+ (N-1)/M] \times [1/N + h/S]$

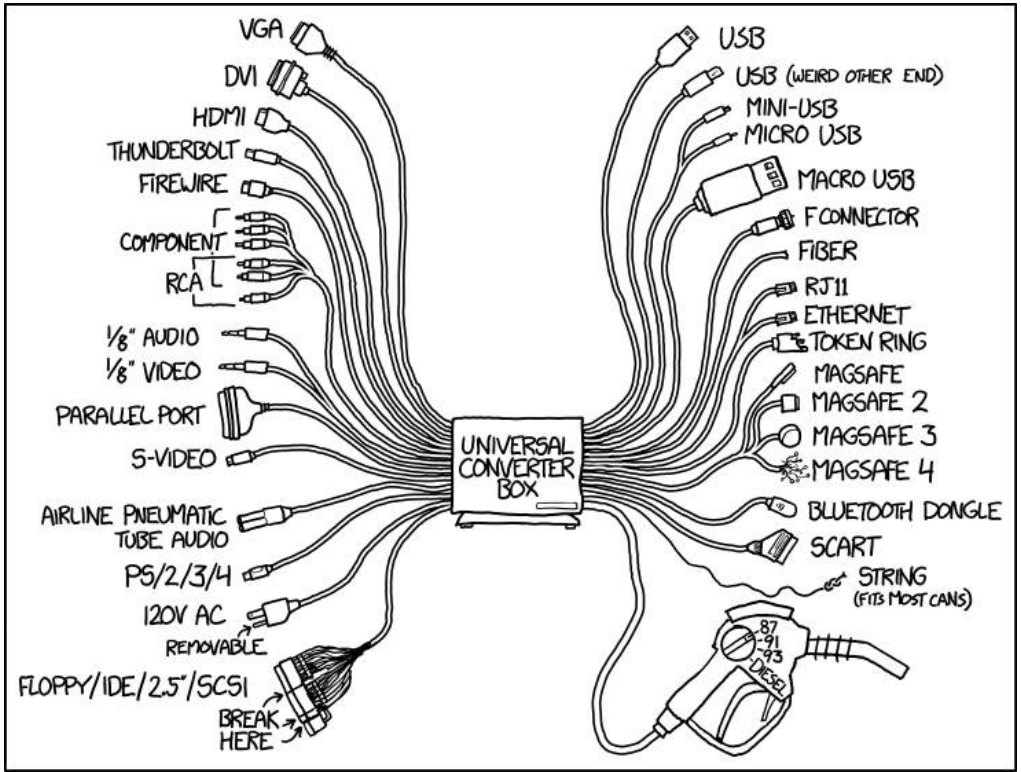
1/N is a fraction, h/S is also a fraction [S >> h] their addition will also result to a fraction [If N is large].

$[1+ (N-1)/M] \times [1/N + h/S]$ is less than 1 [If N is large].

Globally accepted Protocol for Internet



- If any node of network A wants to communicate with any node in network B, then protocol A will be converted to protocol B in network B and protocol B will be converted to protocol A in network A.



- N number of networks N(N-1) different protocol converters are needed.
- If a new network is included with the existing, then each of the N networks N new protocol converters are required.
- very difficult to enlarge an existing network.
- need of a globally accepted protocol
- protocol for those different networks may be different but when one network will communicate with another; that communication will be performed by that globally accepted protocol.

Why TCP/IP ?

- When anyone are set up with direct access to the Internet, that computer is provided with a copy of the TCP/IP program.
- The higher layer is called TCP
- TCP manages the partition of a message or file into smaller packets.
- Transmission, receiving and reassembling managed by TCP
- Internet Protocol (IP), handles the address part, attached with each packet header
- so that it gets to the right destination
- Each gateway computer checks address to see where to forward the message.

- very robust protocol →automatically recover from any communication link failures.
- If transmission lines are damaged or if a computer fails to respond, it re-routes data packets utilizing any available network path.
- TCP/IP is accepted as an industry standard protocol
- HTTP, FTP, Telnet (Telnet) ,SMTP. and other protocols are often packaged together with TCP/IP as a "suite."
- works on almost all network operating systems
- allows connectivity between two dissimilar systems

Web communication protocol

HyperText Transfer Protocol (HTTP): classic "client-server" protocol

Telnet: Oldest communication protocol. used to log on to the remote server

File Transfer Protocol (FTP): used to transfer files such as documents, images, music

Hypertext Transfer Protocol Secure (HTTPS): Similar to HTTP, but combines with a security protocol called SSL/TLS to provide secure client-server communications over unsecure networks

IP Security (IPSec): encrypt packets of data and send them between two computers that share the same cryptographic keys

HTTP Vs Telnet

- HTTP allows to request specific files from remote computers, but not to actually be logged on as a user of that computer.
- HTTP works on port 80

- TELNET is the protocol that is used to login to a remote computer and work on it remotely like secure shell (SSH)

- It works on port 23.

HTTPS

- Hypertext Transfer Protocol Secure
- uses an encrypted HTTP connection by transport-layer security.
- allow authorization and secured transactions. (Credit card, Online banking)
- uses a port 443 by default to transfer the information.
- HTTPS is quite slower compared to HTTP.
- data being transmitted cannot be changed by another party, as will be verified by **Message Authentication Code** (MAC).

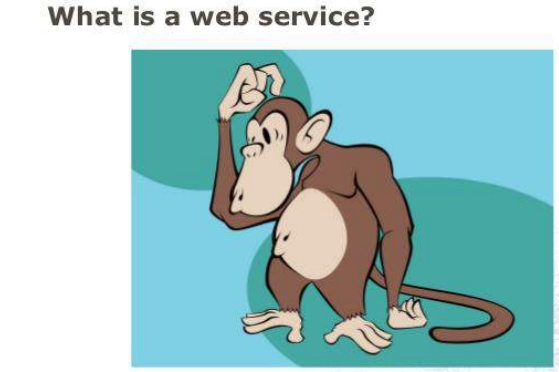
HTTP

- URL begins with "http://"
- uses port 80 for communication
- Unsecured
- Operates at Application Layer
- No encryption
- No certificates required

HTTPS

- URL begins with "https://"
- It uses port 443 for communication
- Secured
- Operates at Transport Layer
- Encryption is present
- Certificates required

Web Services



- collection of open protocols and standards used for exchanging data between applications or systems.
- basic web services platform is XML + HTTP.
- any piece of software that makes itself available over the internet and uses a standardized XML messaging system.
- XML : to encode all communications to a web service.

Security

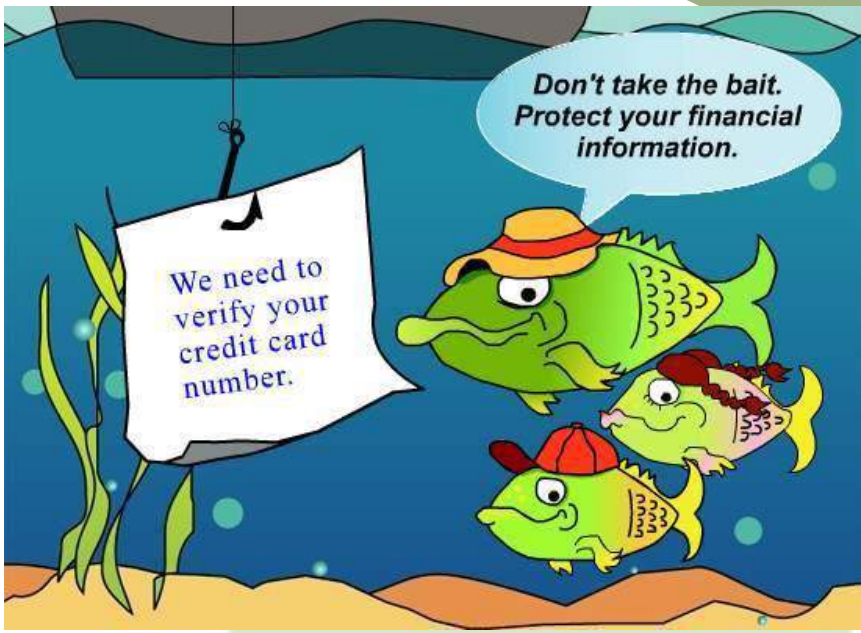
- Confidentiality
- Authentication
- Network Security

Components

SOAP (Simple Object Access Protocol)
UDDI (Universal Description, Discovery and Integration)
WSDL (Web Services Description Language)

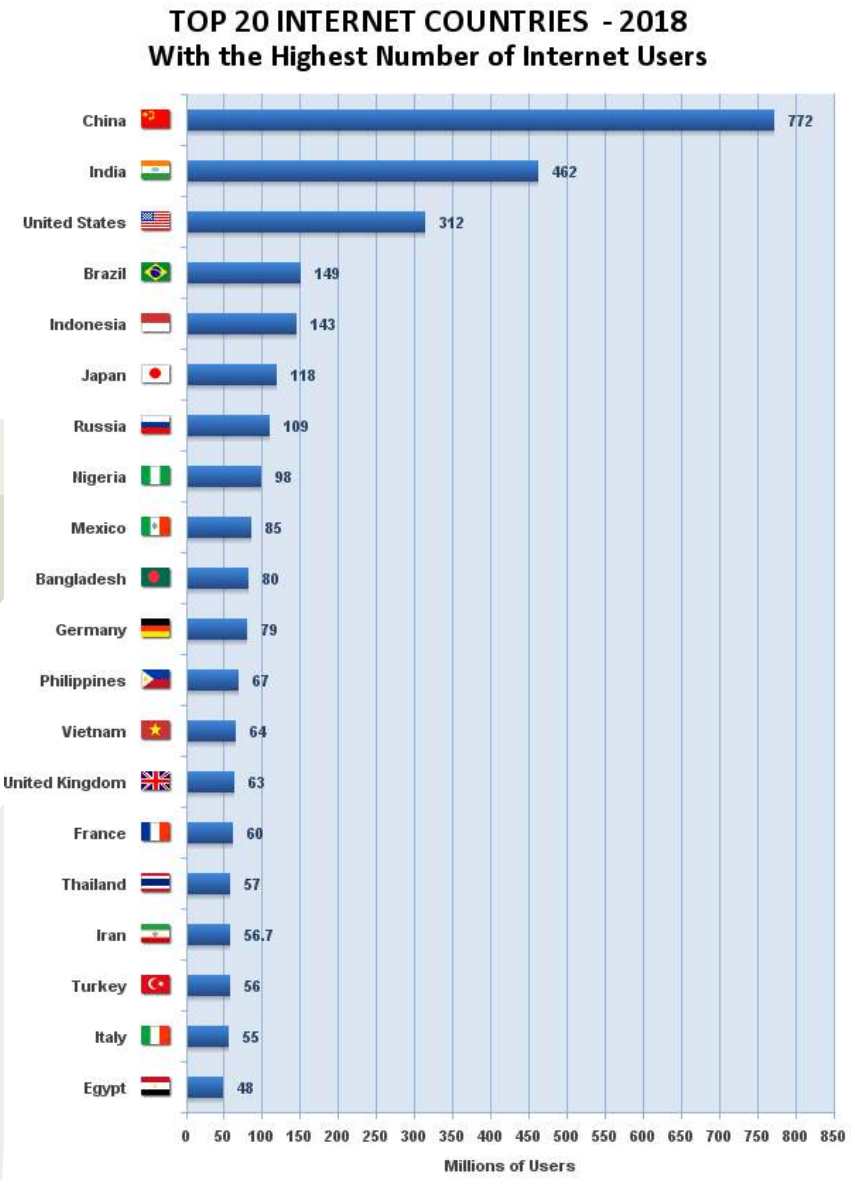
Internet threat

- **Spam** - Spam emails are not a direct threat. However, many can contain malware.
- **Adware-** displays unwanted ads when a user is surfing the internet.
- **Trojan-** often present themselves as harmless computer programmes so that hackers can penetrate your computer without being detected.
- **Virus:** replicate functional copies of themselves and spread by user act, Floppy, CD, USB
- **Worms:** are standalone software and do not require a host program or human help to propagate.
- **Phishing**

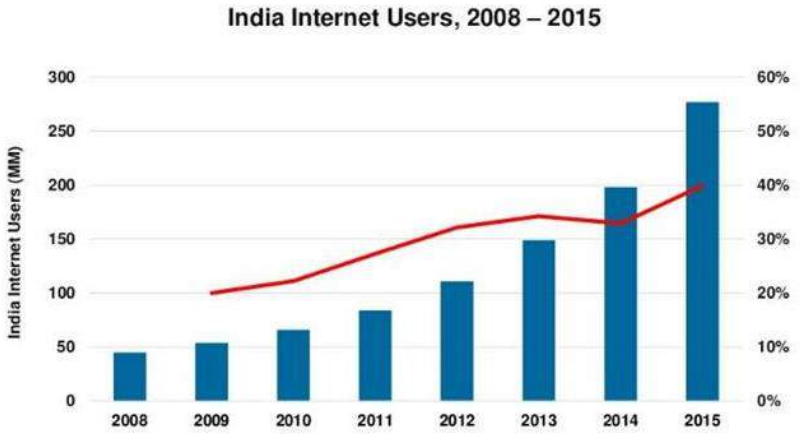


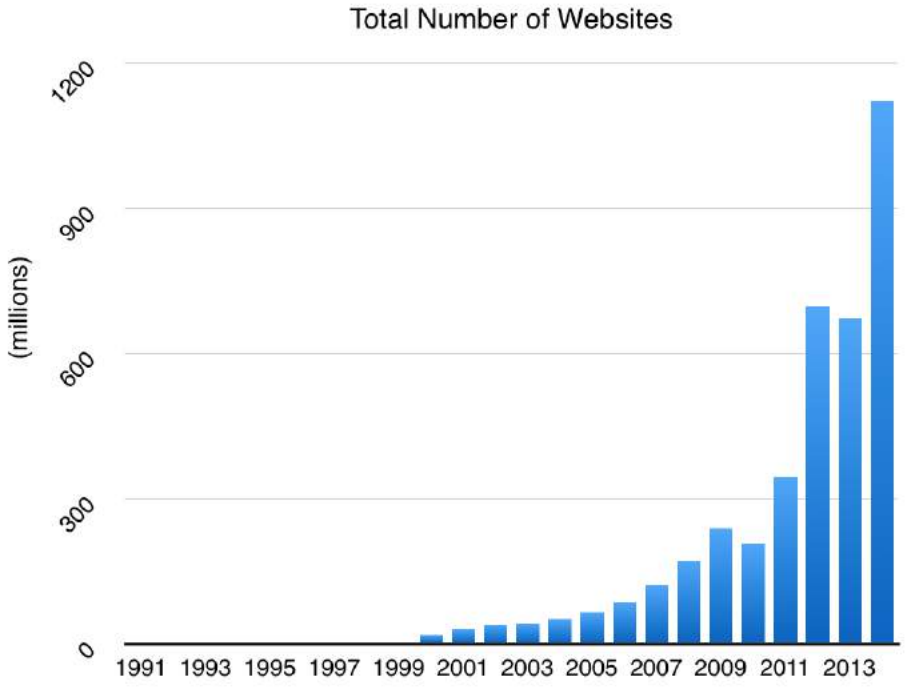
- **Spyware:** usually attached to pop-ups of downloadable files. Once installed can monitor keystrokes, read and delete files, reformat hard drive, and access applications.
- **Keyloggers:** record a user's keyboard actions
- **Pharming:** complex version of phishing that exploits the DNS system. Mimicking a web page. Steal user login and financial detail

Some statistics



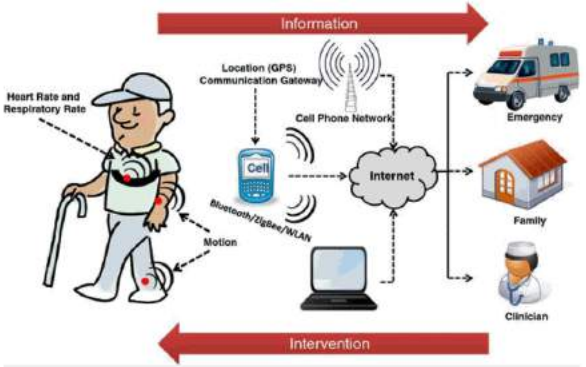
Source: Internet World Stats - www.internetworldstats.com/top20.htm
2,937,139,302 Internet users in the Top 20 countries in December 31, 2018





The future of Internet

- **connection will be permanent and automatic**
- **Augmented and virtual reality**
- **Machines might take over your job**
- **Privacy will become commoditized –** May happen that only rich can afford their privacy secured.
- **The 'Internet of Things' will fully mature:** will extend to vehicles, wallets, health monitors, and perhaps even our paper currency.
- **Earth won't be the only planet with Internet access**
- **Radically Improved Health Industry**
- **Grid and cloud in full swing, no worry about spaces.**



IoT in Remote Health Monitoring

Some interesting facts

- The first-ever email sent has the same sender and receiver. (Ray Tomlinson, 1971)
- The double slash “//” on the web URLs is the inventor’s greatest regret.
- first-ever spam email was intended to sell computers. (1978, Gary Thuerk)
- 70,000 search queries Google serves per second
- China has treatment camps for internet addicts.
- Common people are not allowed to use Internet in North Korea.
- NASA has an internet speed of 91 gigabits per second.
- The country with the highest internet speed is Taiwan (85.02) and slowest in Yemen (0.38)
- Before the internet, “LOL” was supposed to mean “lots of love.”
- ” Gangnam Style ” by PSY is still the most viewed videos of all time with more than 2,840,000,000 views.
- 400 Hours of video contents are uploaded on YouTube Every Minute
- Australia have recorded the highest internet speed of 44.2 Terabits per second. (2020)

Thank You

Web Search Engine

What is?

- a software system that is designed to search for information on the World Wide Web.
- The results are generally presented in a line of results often referred to as search engine results pages (SERPs).
- The information may be a mix of web pages, images, and other types of files.
- Some search engines also mine data available in databases or open directories.
- Also maintain real-time information by running an algorithm on a web crawler.

History

Archie:

- Created in 1990 by Alan Emtage, a student at McGill University in Montreal.
- "archives," it shortened to Archie.
- Used regular expression matcher for retrieving file names matching a user query.
- searched FTP sites to create index of downloadable files
- Due to limited space, only the listings were available

Veronica:

Developed by University of Nevada System Computing Services group .

Worked on plain text files.

Jughead (1993)

- Also searched file names and titles in Gopher index systems, but only searched a single server at a time

History

Primitive Web Search (1993)

- **JumpStation:** Info about a page's title and header using simple linear search

Yahoo search (1994):

- Created by David Filo and Jerry Yang, beginning as a collection of favorable web pages that incuded a man-made description with each URL
- Increasing size influenced them to become a searchable directory
- Informational sites added for free, but they expanded to included commercial sites.

Google (1998):

Began in 1995 as a research project by Larry Page and Sergey Brin, Ph.D. students at Stanford University.

understanding the link structure of www as a huge graph.

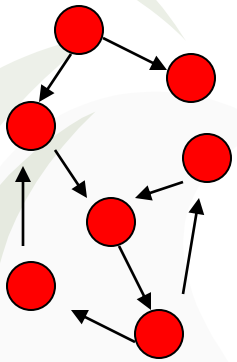
Brin and Page developed the Page Rank algorithm. ----given web page into a measure of importance.

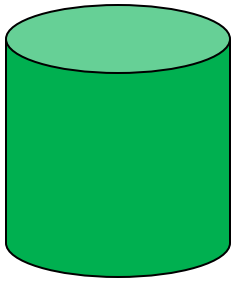
How a search engine work?

Three terms

Crawling, Indexing and Ranking

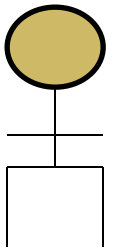
1. web crawler gathers a snapshot of the Web





2. Gathered pages are indexed for easy retrieval

3. search query submitted by user



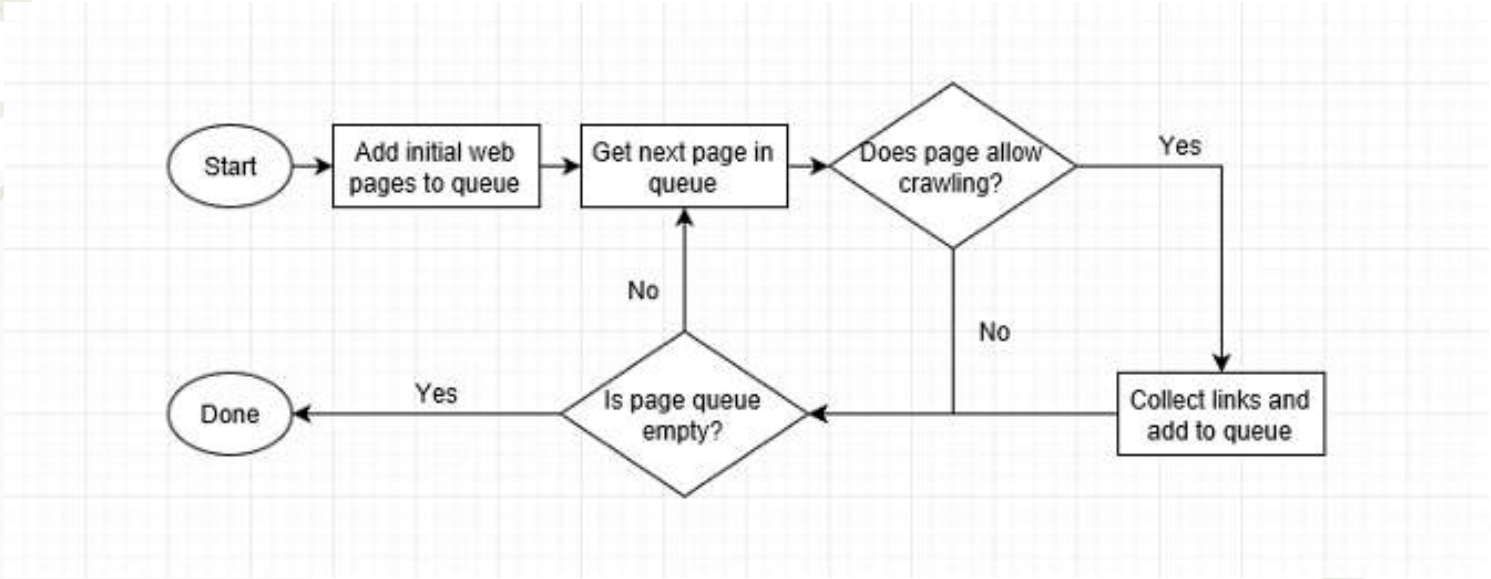
4. Search engine ranks pages that match the query and returns an ordered list

Web Crawler (Web Spider)

How web is crawled?

An automated bot (called a “spider”) visits page after page as quickly as possible, using page links to find where to go next.

In the beginning Google’s spiders could read several hundred pages per second. Nowadays, it’s in the thousands.



- Web crawlers also revisit past pages once in a while to see if any changes happened.
- Some sites are crawled more frequently, and some are crawled to greater depths, but sometimes a crawler may give up if a site’s page hierarchy is too complex.

Internet bot

- Web robot or www robot. Abbreviated to bot.
- A software application that runs automated tasks (scripts) over the Internet.
- used to perform simple and repetitive tasks that would be time-consuming, mundane or impossible for a human to perform.

GOOD

used to gather information, automatic interaction with instant messaging, Dynamic interaction with websites

BAD

Gather passwords
Log keystrokes
Obtain financial information
Relay spam
Capture and analyze packets
Launch DoS attacks
Open back doors on the infected computer
Exploit back doors opened by viruses and worms

Features of a crawler

Must provide:

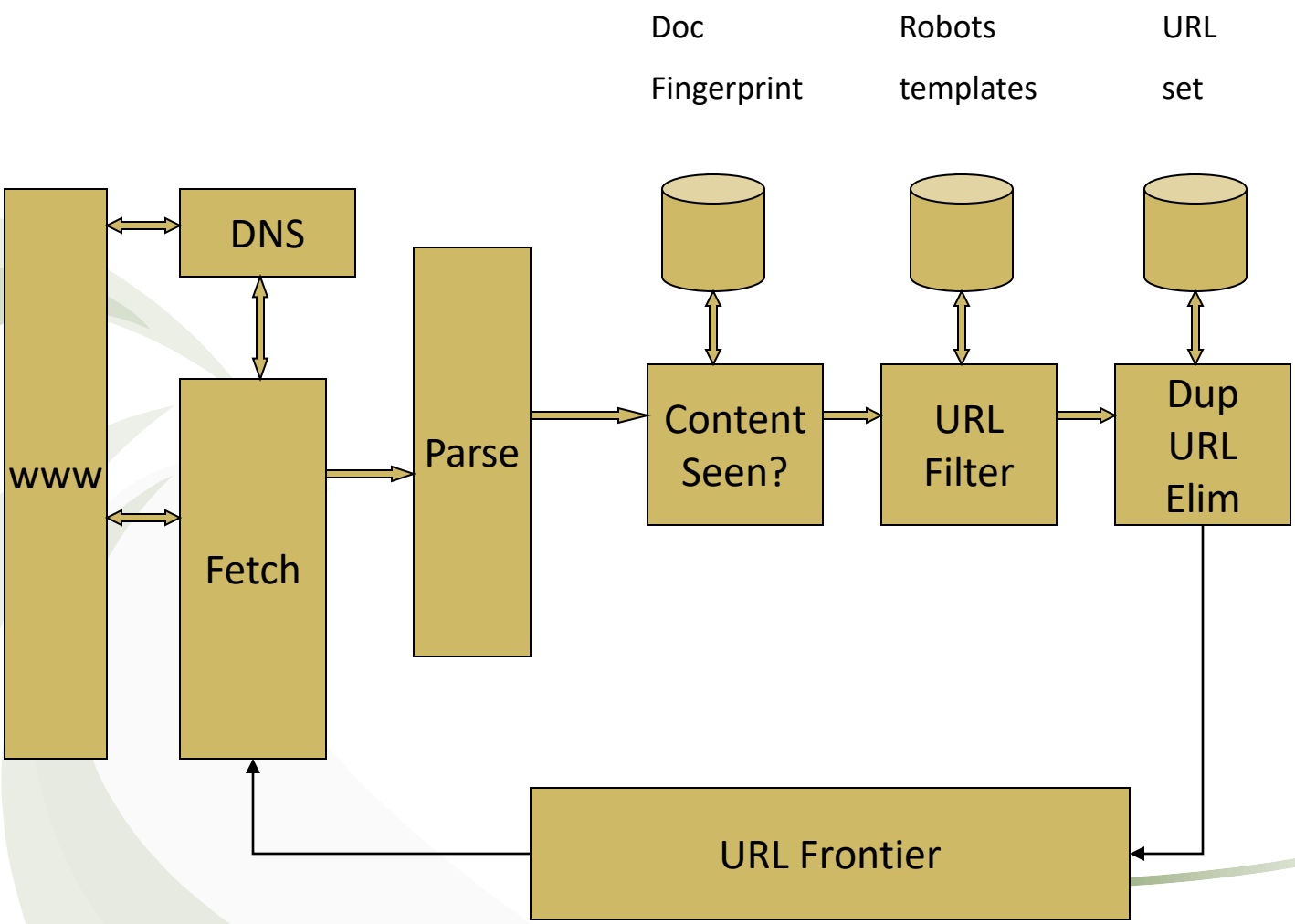
- **Robustness:** spider traps
  - Infinitely deep directory structures

Politeness: which pages can be crawled, and which cannot

Should Provide

- Distributed
- Scalable
- Performance and efficiency
- Quality
- Freshness
- Extensible

Web Crawler architecture



- **URL Frontier**: containing URLs yet to be fetches in the current crawl. At first, a seed set is stored in URL Frontier, and a crawler begins by taking a URL from the seed set.
- Fetch: generally use the http protocol to fetch the URL.
- Parse: the page is parsed. Texts (images, videos, and etc.) and Links are extracted.

Regular expression and Web crawler

- \b: stands for the beginning or end of a Word.
  - E.g.: \bhi\b find hi accurately
- \w: matches letters, or numbers, or underscore.
- .: matches everything except the newline
- *: content before * can be repeated any number of times
  - \bhi\b.*\bLucy\b
- +: content before + can be repeated one or more times
- []: match characters in it
  - E.g: \b[aeiou]+[a-zA-Z]*\b
- {n}: repeat n times
- {n,}: repeat n or more times
- {n,m}: repeat n to m times

- Target: Detect the email address
- Specifications:
  - A@B
  - A: combinations English characters a to z, or digits, or . or _ or % or + or –
  - B: cse.cuhk.edu.hk or cuhk.edu.hk (English characters)
- Answer:
  - \b[a-z0-9._%+-]+@[a-z.]+\.[a-z]{2}\b

Indexing

Index: A database where information after being collected parsed and processed is stored to allow for quick retrieval.

Cache based engines store the index along with corpus. (Collection of documents)

When something is added to the corpus, the index is updated.

Search engine use

- Inverted index
- Document matrix

Inverted index: Mostly used Words are mapped to their location in a document.

“Sparse matrix” because it doesn’t list all of the words in each document.

Fully inverted index:

Words are not only mapped to their location in the document but also the location of each occurrence of the word is also mapped.

Document matrix: stores the occurrences of words in documents in a two-dimensional sparse matrix.

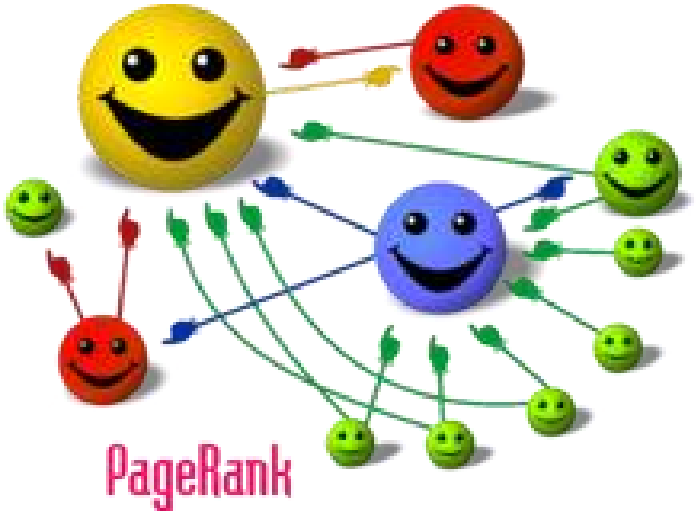
Ranking

- The primary challenge of a search engine is to return results that match a user's needs.
- A word will potentially map to millions of documents
- How to order them?

Ans: Page ranking

PageRank was named after Larry Page, one of the founders of Google. PageRank is a way of measuring the importance of website pages.

Cartoon illustrating the basic principle of PageRank. The size of each face is proportional to the total size of the other faces which are pointing to it.



Source: wikipedia

Page rank—A simplified algo..

Assume a small universe of four web pages: **A**, **B**, **C** and **D**.

only links in the system were from pages **B**, **C**, and **D** to **A**, each link would transfer 0.25 PageRank to **A** upon the next iteration, for a total of 0.75.

PR(A)=PR(B)+PR(C)+PR(D)

Suppose instead that page **B** had a link to pages **C** and **A**, page **C** had a link to page **A**, and page **D** had links to all three pages.

$$PR(A) = \frac{PR(B)}{2} + \frac{PR(C)}{1} + \frac{PR(D)}{3}$$

- PageRank conferred by an outbound link is equal to the document's own PageRank score divided by the number of outbound links **L( )**.

$$PR(A) = \frac{PR(B)}{L(B)} + \frac{PR(C)}{L(C)} + \frac{PR(D)}{L(D)}.$$

- In General pagerank value for any page u is

$$PR(u) = \sum_{v \in B_u} \frac{PR(v)}{L(v)},$$

World Wide Web

Brief history of www

"***The World Wide Web is the universe of network-accessible information, an embodiment of human knowledge***." -----Tim Berners Lee

- After 1980 when the Internet became the largest network, many people realized the increasing need to be able to find and organize files and information.
- Tim Berners Lee a researcher working in European Organization for Nuclear Research (CERN), Switzerland developed a model named ENQUIRE, a personal database for people & software model.
- Aim was to improve CERN's research document handling and sharing mechanism.
- Used PASCAL programming language.
- used a new thing called hypertext by which each new page of information in ENQUIRE had to be linked to an existing page.
- In 1989 Lee proposed "a large hypertext database with typed links"
- Lee developed necessary software application for hypertext server program and made it free to download.

Brief history of www

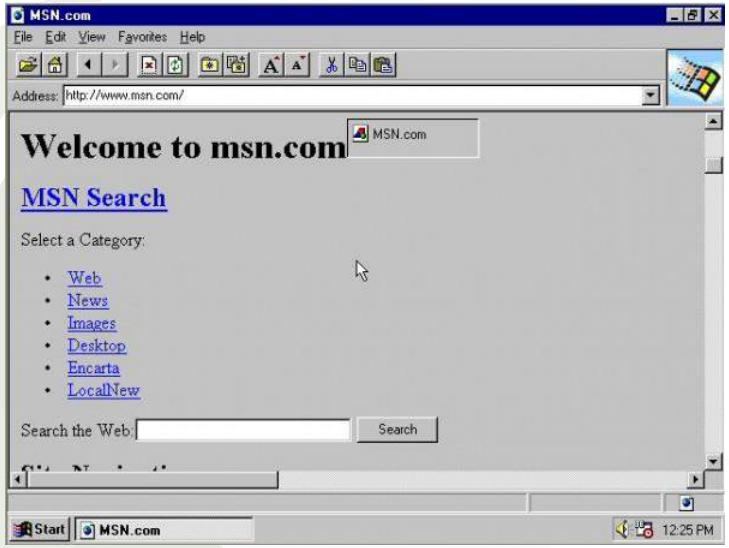
- new feature of bidirectionality allows ideas, notes, etc. to link to each other without the author being aware of this.
- Tried to implement this on newly installed NeXT computes.
- idea was to connect hypertext & Internet.
- System of hypertext documents were named as World Wide Web (WWW)
- Lee realized that people from around the world needed to share data, files with no common machines and no common presentation software.
- By 1990 he built all the necessary things like hypertext transfer protocol(http), Hypertext Markup language(HTML), a web server (http://info.cern.ch) and the first web page to run his project.

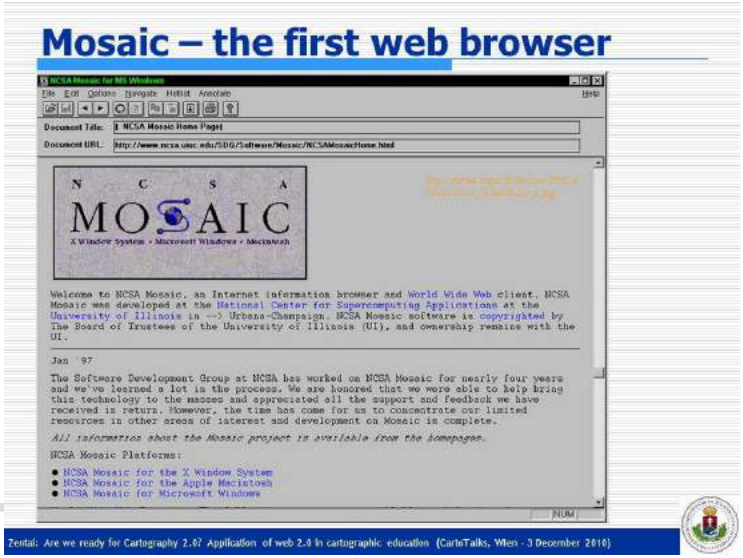
According to Tim Berners Lee ---

"The dream behind the Web is of a common information space in which we communicate by sharing information. Its universality is essential: the fact that a hypertext link can point to anything, be it personal, local or global, be it draft or highly polished."

Brief history of www

- In 1993 Marc Andreessen of University of Illinois wrote a program called Mosaic.
- It can read a document created in hypertext format.
- It contains an interpreter thus output as hypertext document was displayed on user screen.
- This was the first web browser.
- Business version of Mosaic is Netscape Navigator.
- Then Microsoft came into the scenario with Internet explorer.





w3C

- **World Wide Web Consortium** (**W3C**) is the main international standards organization for the World Wide Web (abbreviated WWW or W3). (1994)
- Founded and currently led by Tim Berners-Lee.
- Consortium is made up of member organizations which maintain full-time staff for the purpose of working together in the development of standards for the World Wide Web.
- As of 1 April 2017, the World Wide Web Consortium (W3C) has 461 members.
- Mission is developing protocols and guidelines that ensure the long-term growth of the Web.
- It includes web for all (people) and web for everything(device).

How does a web server work?

- In case of web client is web browser and server is web server.
- **web server** is a computer program (running on server computer) that processes requests via HTTP, This is why a Web Server is also called an HTTP Server.
- Actual communication (request for web page and actual web page) between client and server is performed using TCP/IP.
- Web server is a program running on server computer. Additionally it contains the website with number of web pages.
- Web pages are computer files written in specially designed language called HTML.
- Web server constantly and passively waits for request from web page from a browser program at client.
- It locates the corresponding page upon receiving the request.
- Every website has a server process to listen TCP connection request.
- Upon TCP connection established client send one request and server sends one response.
- This is governed by HTTP.

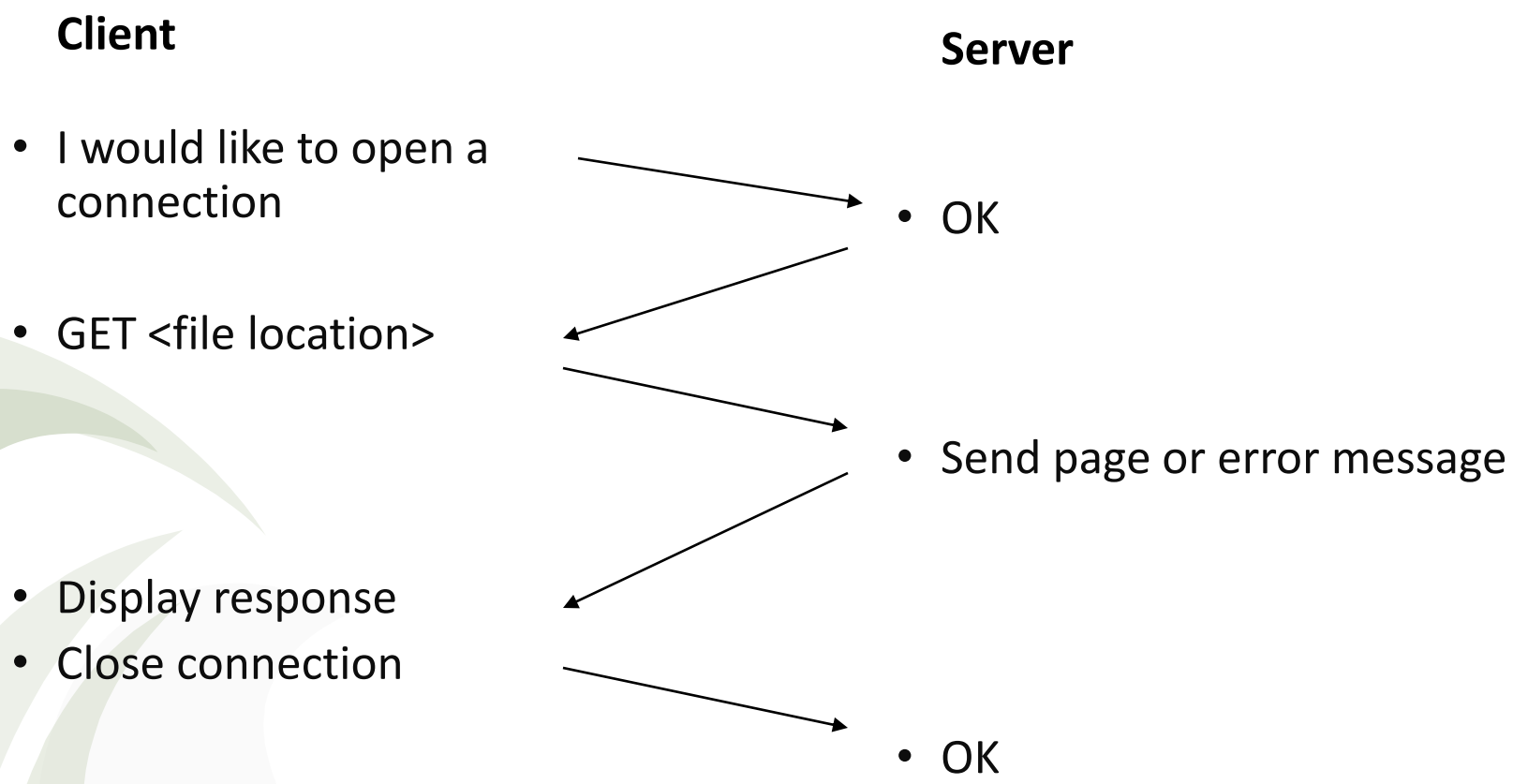
- Client requests for a particular web page (Not a file like FTP).
- Web page is stored in HTML format in web server.
- OS of server locates the file and sends it to client using TCP/IP. (Stored to primary memory of client)
- Browser on client interprets the HTML file from the memory of client computer and displays it.

HTTP

- hypertext transfer protocol
- Invented by T.B.Lee.
- is the set of rules governing the format and content of the conversation between a Web client and server
- Protocol for transfer of various data formats between server and client

  ----Plaintext, Hypertext, Images, Video and Sound

An HTTP conversation

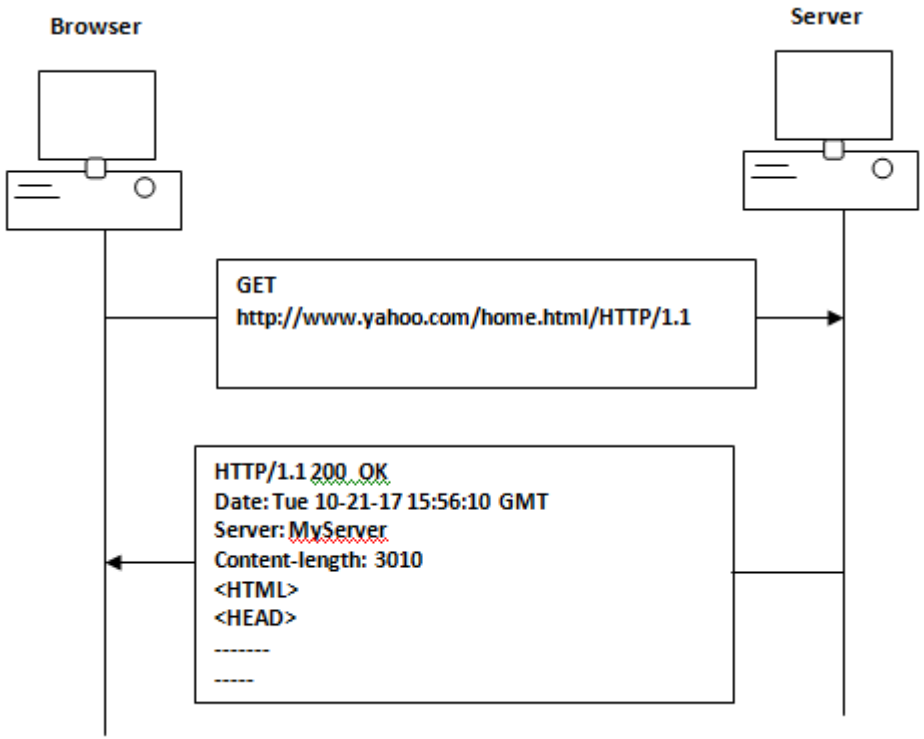


HTTP commands

HTTP Command	Description
GET	Browser command. Request for obtaining a web page.
HEAD	Request to read the header of a web page. (Last modified date)
PUT	Sends a file to store it there
POST	Similar to PUT, but used for updating a web page
DELETE	Deleting a particular web page
LINK	Establish a hyperlink between two pages
UNLINK	Remove existing hyperlink between two pages

HTTP status code

General Format	Status code	Description
1xx Informational responses	100 continue	
	101 Switching protocol	The requester has asked the server to switch protocols and the server has agreed to do so
2xx Success	200 OK	Standard response for successful HTTP requests.
	202 Accepted	The request has been accepted for processing, but the processing has not been completed.
	204 No Content	The server successfully processed the request and is not returning any content.
3xx Redirection	301 Moved Permanently	This and all future requests should be directed to the given URI
	307 Temporary Redirect	the request should be repeated with another URI; however, future requests should still use the original URI.
4xx Client errors	400 Bad Request	The server cannot or will not process the request due to an apparent client error (malformed request syntax, size too large, invalid request message framing, or deceptive request routing)
	403 Forbidden	The request was valid, but the server is refusing action.
	404 Not Found	The requested resource could not be found but may be available in the future. Subsequent requests by the client are permissible.
5xx Server error	500 Internal Server Error	when an unexpected condition was encountered and no more specific message is suitable
	502 Bad Gateway	
	503 Service Unavailable	The server is currently unavailable (because it is overloaded or down for maintenance)
	505 HTTP Version Not Supported	The server does not support the HTTP protocol version used in the request


Browser
Server
GET
http://www.yahoo.com/home.html/HTTP/1.1
HTTP/1.1 200 OK
Date: Tue 10-21-17 15:56:10 GMT
Server: MyServer
Content-length: 3010
<HTML>
<HEAD>

HTTP is a stateless protocol

- **stateless protocol** is a communications protocol in which no information is retained by either sender or receiver.
- Sender transmits a packet to the receiver and does not expect an acknowledgment of receipt.
- HTTP is called a stateless protocol because in this each command is executed independently, without any knowledge of the commands that came before it.
- unable to retain a memory of the identity of each client that connects to a Web site and therefore treats each request for a Web page as a unique and independent connection, with no relationship whatsoever to the connections that preceded it.

Why?

A popular web server that takes millions of hits per day.

- Each one of those hits consists of a quick connect/disconnect.
- If each person using the web site maintained an open connection the whole time that they were there, it could potentially overwhelm the server. Also, there would often be conversations left open when the user has stopped looking at your web page !

HTTP versions

- First version developed by Tim Berners-Lee. Had only one method, GET, which would request a page from a server. The response from the server was always an HTML page. (1989)
- HTTP V 0.9 proposed by Dave Raggett in 1995, which is modified to HTTP V 1.0 in 1996. It includes extended operations (Methods), tied with a security protocol which became more efficient by adding additional methods and header fields.
- HTTP 1.1 : provides faster delivery of Web pages than the original HTTP and reduces Web traffic. (1997)
- **Pipelined:** Instead of opening and closing a connection for each application request, HTTP 1.1 provides a *persistent connection* that allows multiple requests to be batched or ***pipelined*** to an output buffer.
- **Reduced 'GET':** requests for a sequence of "get a file" requests is reduced, fewer packets need to flow across the Internet. Since requests are pipelined, TCP segments are more efficient. Less Internet traffic and faster performance for the user.
- **Compressed file: B**rowser supporting HTTP 1.1 can decompress HTML files, a server will compress them for transport across the Internet, providing a substantial aggregate savings in the amount of data that has to be transmitted.

HTTP versions

- HTTP 2.0: Standardized by **Internet Engineering Steering Group** (IESG) in Feb 2015.

Major features:

- Data compression of HTTP headers
- HTTP/2 Server Push
- Pipelining of requests

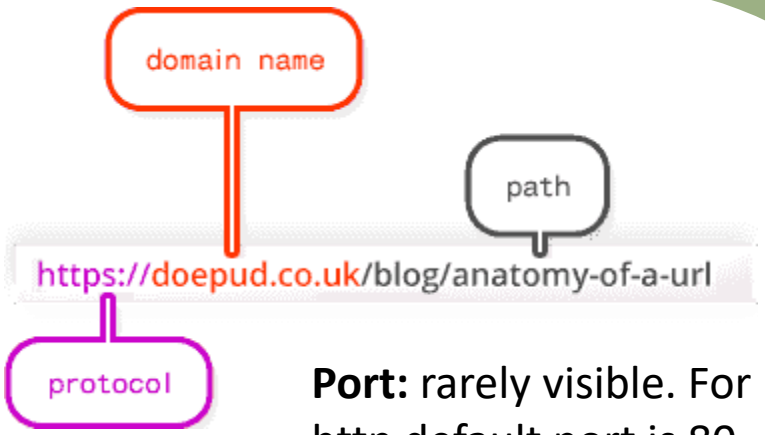
HTTPS: S for secure.

all communications between browser and the website are encrypted.

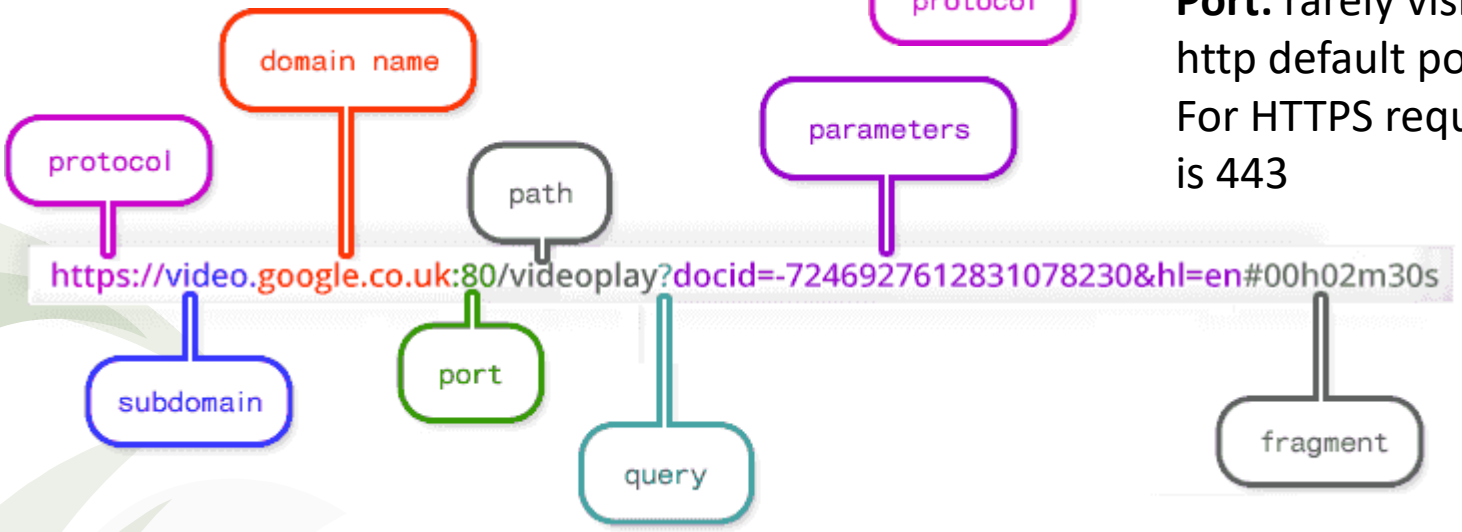
were primarily used for payment transactions on the World Wide Web, e-mail and for sensitive transactions in corporate information systems.

URI

Subdomain: www.**mail**.yahoo.com



Port: rarely visible. For http default port is 80. For HTTPS request port is 443



Domain name: unique reference that identifies a web site on the internet, for example www.**yahoo**.com. A domain name always includes the top-level domain (TLD)

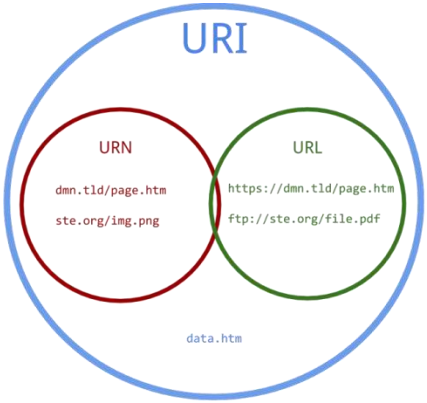
Path: typically refers to a file or directory on the web server

Query: commonly found in the URL of dynamic pages (ones which are generated from database or user-generated content) and is represented by a question mark followed by one or more parameters.

URI, URL and URN

URI: Uniform Resource Identifier (**URI**) is a string of characters used to identify a resource. Identifies a resource either by location, or a name, or both.

There are two types of URIs, Uniform Resource Identifiers (URLs) and Uniform Resource Names (URNs).



URL:

- begins by stating which protocol
- defines the network location of a specific resource.
- Unlike a URN, the URL defines how the resource can be obtained.

URN: Uniform Resource Name identifies a resource by name in a given namespace (Like Surname of human). A namespace refers a group of names or identifiers. [Surname with name]. Persistent. Will not work is web page shifted to new location. (URL changed)

How does a web browser work?

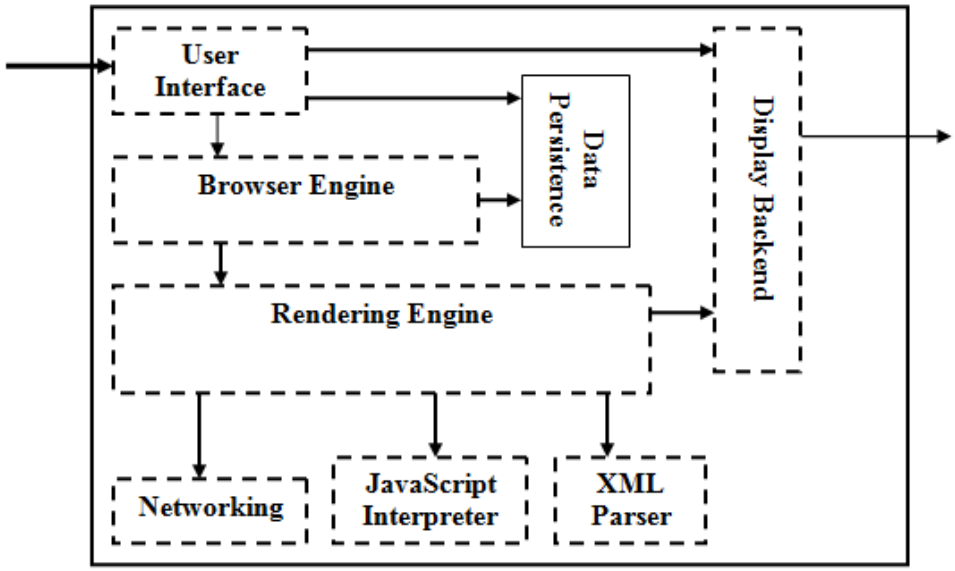
- User types the URL of the page he wants on his web browser.
- URL contains protocol (let http), TLD (let .com), domain name (let yahoo) and the file name (let home.html).
- Browser requests DNS for IP address of the corresponding domain (Here www.yahoo.com)
- DNS replies with the IP address.
- Browser makes a TCP connection with the computer of that IP address.
- Client makes an explicit request for the page (file) to the server using HTTP request. **(Have GET and HOST like GET /home.html HOST:yahoo.com)**
- Request is handed over to HTTP software running on client machine.
- HTTP software at client hands over this to TCP/IP software running at client machine.
- TCP/IP breaks it into packets adds header and sends those to server. (Routing mechanism)
- TCP/IP at web server reassembles the packets removes header and reforms HTTP request.

- TCP/IP at server side hands over the request to HTTP on server.
- It interprets the request and finds that browser has asked for home.html.
- Request the OS for the file.
- OS locates the file and hands over it to HTTP software on server.
- HTTP adds some header and forms HTTP response .
- HTTP now hands over it to TCP/IP at server.
- It breaks it into number of packets and adds header and sends those over the TCP connection to the client.
- TCP/IP acknowledges HTTP when all the packets are transmitted correctly.
- TCP/IP at clients removes header and reassemble the packets and hands over to HTTP at client.
- HTTP submits it to web browser for interpretation.

Internal architecture of web browser

- Web Browser is a software that allows us to view websites.
- **Web browser** is an application software for retrieving, presenting, and traversing information resources on the World Wide Web.
- The internal architecture of a web browser varies from browser to browser of different companies. But in general a Web browser consists of 8 parts.

Internal architecture of web browser



User Interface: user interact with the application software.

Browser Engine: provides a high-level interface for querying and manipulating the Rendering Engine

Rendering Engine: performs parsing and layout for HTML documents, optionally styled with CSS

Network Subsystem: handles the network related issues.

Java Script Interpreter: Handles code written in JavaScript.

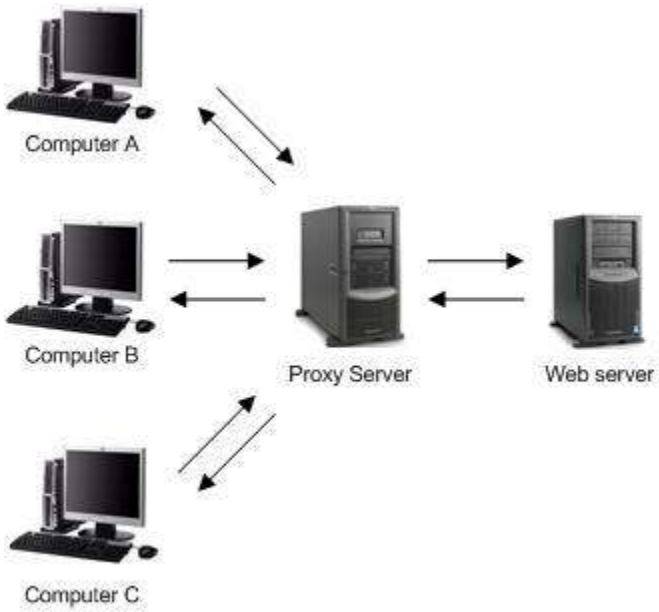
XML parser: Handles code written in XML.

Display Backend: handles font types, sizes, color issues etc.

Data Persistence: stores various data associated with the browsing session on disk, including bookmarks, cookies etc.

Proxy server

- also known as a "proxy" or "application-level gateway“
- a computer that acts as a gateway between a local network (e.g., all the computers at one company or in one building) and a larger-scale network such as the Internet.
- Provides increased performance and security. In some cases, they monitor employees' use of outside resources.
- proxy server works by intercepting connections between sender and receiver.
- All incoming data enters through one port and is forwarded to the rest of the network via another port.
- By blocking direct access between two networks, proxy servers make it much more difficult for hackers to get internal addresses and details of a private network.



Purpose of Proxy

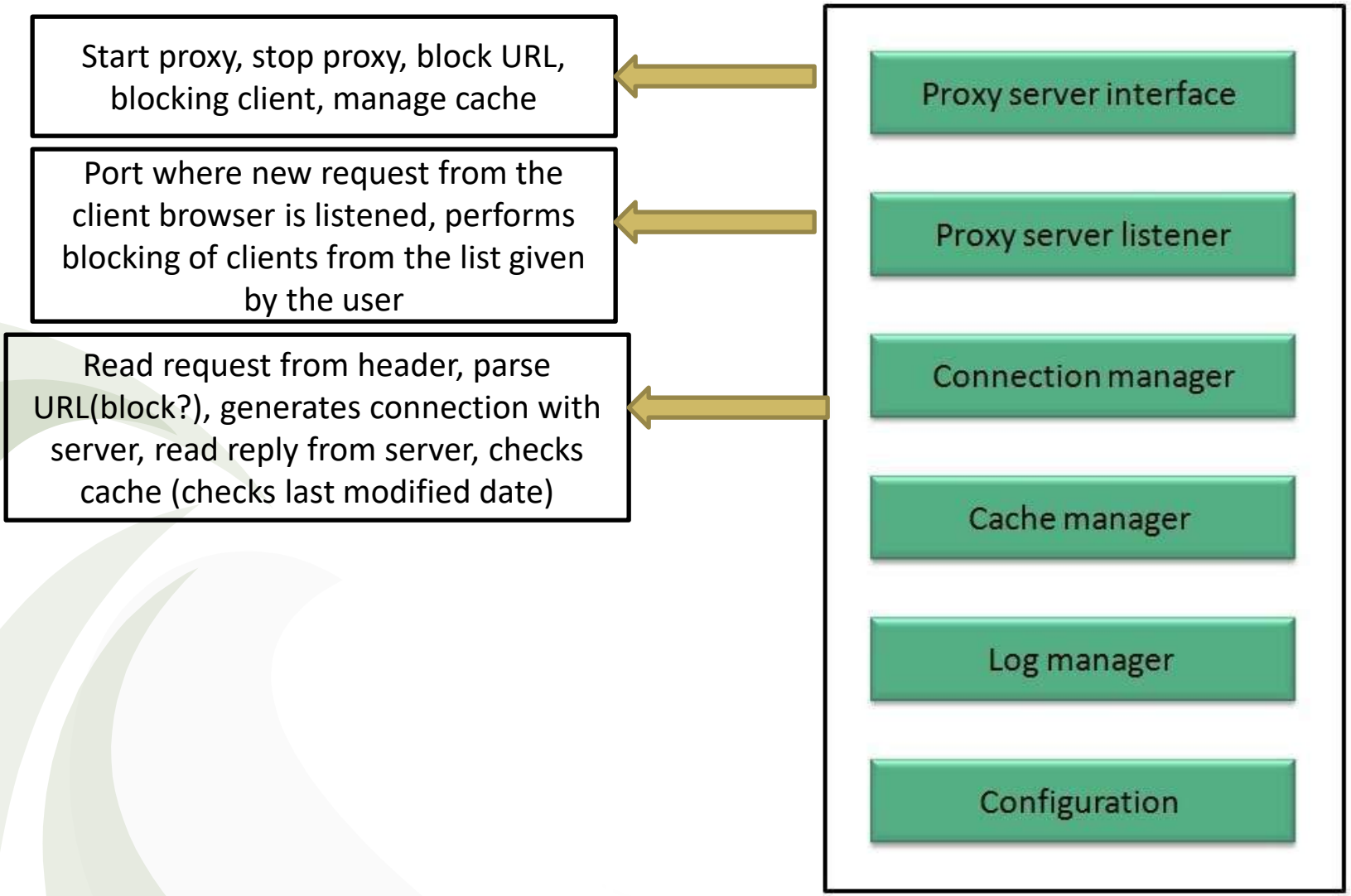
- Monitoring and Filtering
- Improving performance (Retrieving information from cache)
- Accessing services anonymously
- Security

Content Filtering
Filttering encrypted data
Bypass filters
Logging and eavasdropping

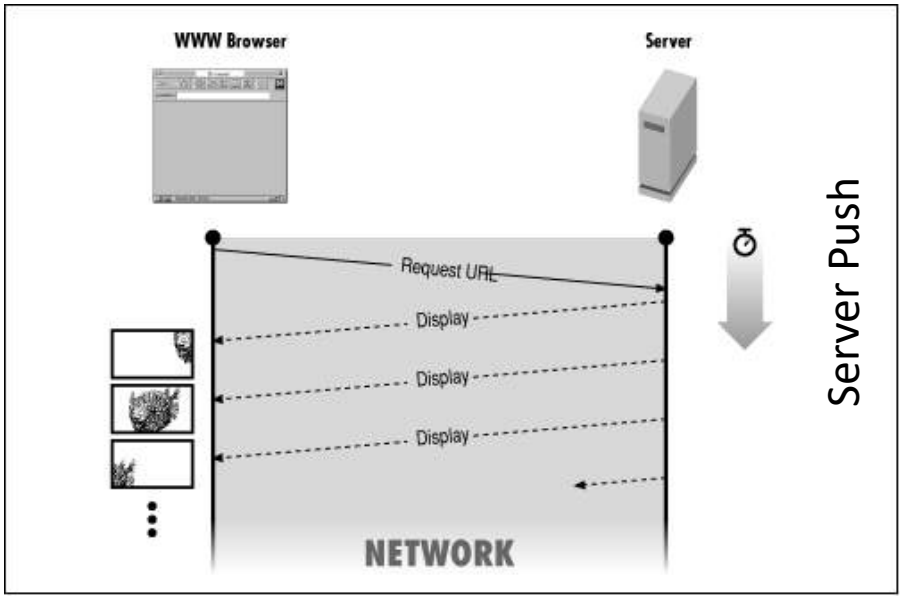
Hides the identity of the user hence it protects from spam and the hacker attacks.

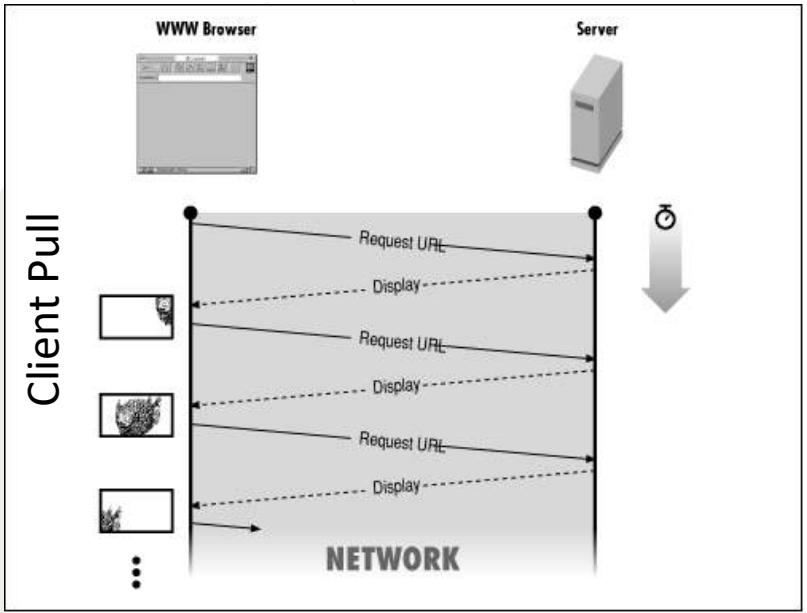
Destination server receives the request from the proxy server and thus does not receive information about the end user.

Proxy architecture



Client pull and server push

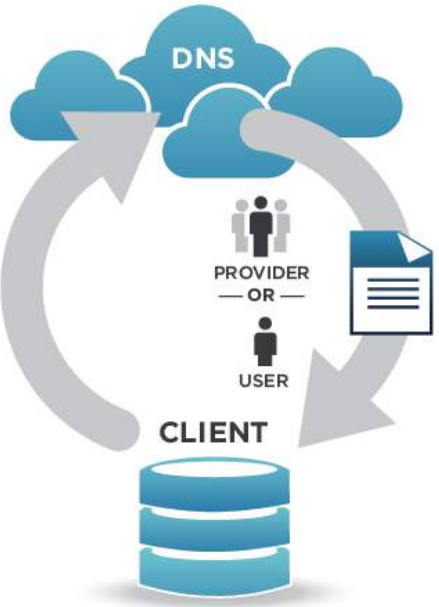




Server push

- The server sends a chunk of data.
- The browser displays the data, but leaves the connection open.
- The server sends more data whenever it wants and the browser displays it, always leaving the connection open.
- HTTP connection is held open for an indefinite period of time (until the server sends a terminator, or until the client interrupts the connection).

DNS, Email,FTP



Naming a computer

- Human feel ease to a **name** rather than a number.
- Every node in a network has an **IP address**…**name is used for easy to remember**.
- Domain refers to a group of computers that are called by a **single common name**. [Like Title of a family]
- Domain name may be a name, but ultimate communication is performed by IP address.
- Two computers in a same network **can not have same name** to uniquely identify.
- valid for globally.

Let a person have only his/her ADDHAAR number but no name…..
How to remember????

Let a person have only his/her ADDHAAR number but no name….. How to remember????

- Provide name for each person… [May be duplicated…but for family it is unique]
- Maintain a table…
- While uniquely identifying search the table….

That is DNS

Domain name

- organization name.A

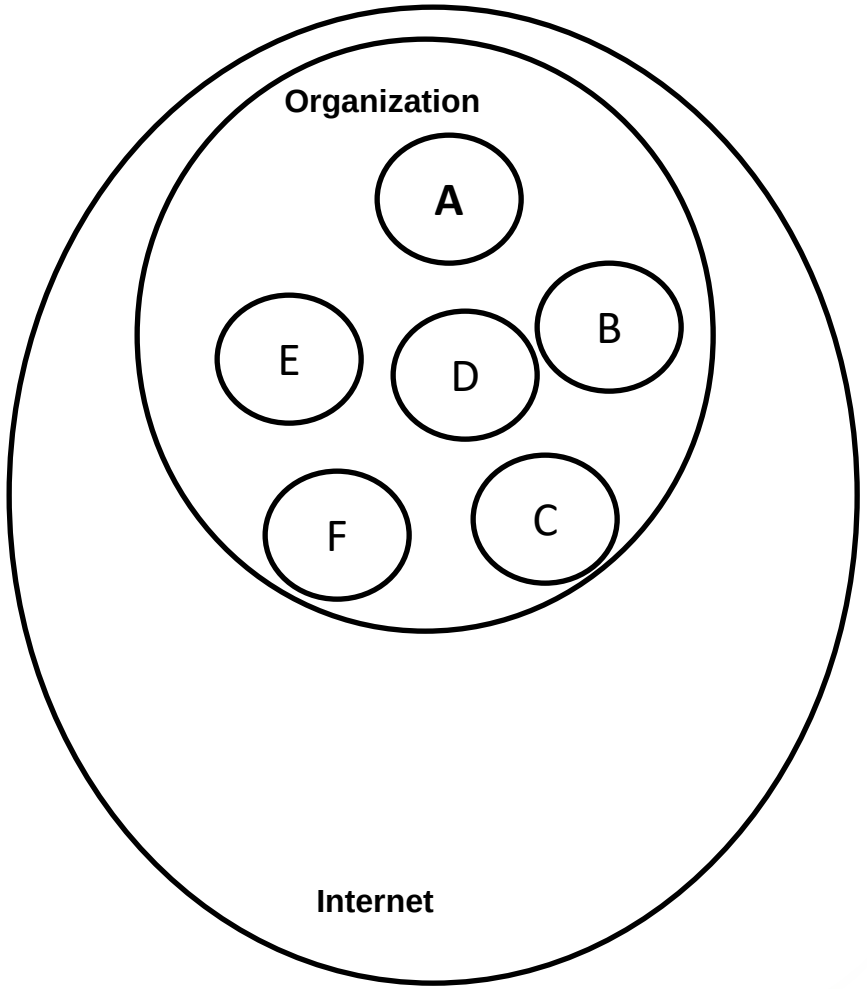
(A,B,C…are unique as they exists in a same network. Can be managed)

Radhika.IBM

- If there exists same organization in internet (Vast thus can not be managed)

(what about for IBM university? if it want to give name IBM?)

- Another suffix needed. –According to the type of work
- Commercial, Educational, Government, military etc.



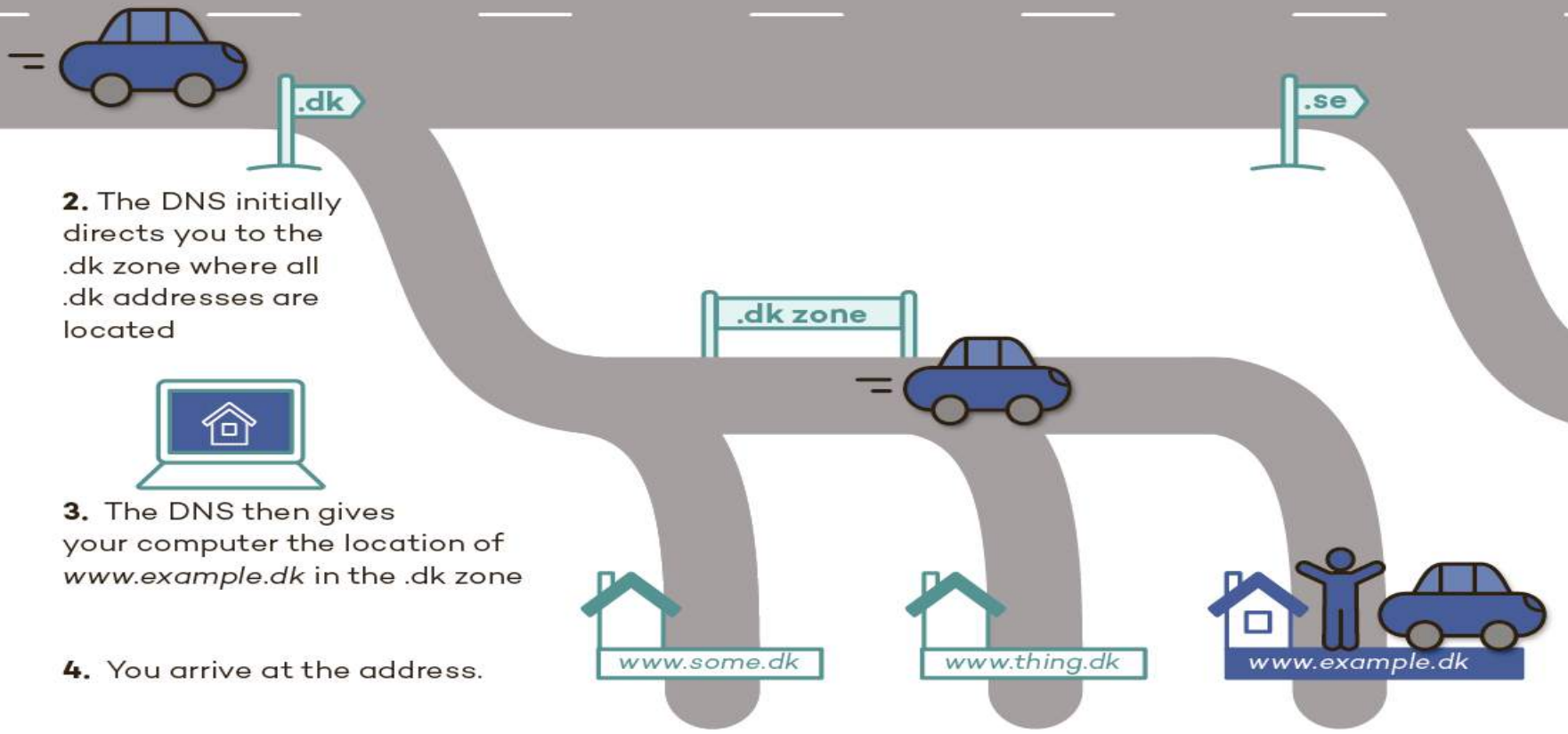
General domain names

Domain Name	Description
com	Commercial organization
edu	Educational institution
gov	Government organization
int	International organization
mil	Military group
net	Network support group
org	non profit organization

WHAT IS **DNS?**

When you type a www address into your browser, the DNS directs you to the correct location on the internet. This is perhaps best compared with the GPS navigator you use to find your way when you're travelling by car.

1. You type in the www address you would like to visit, for instance www.example.dk



2. The DNS initially directs you to the .dk zone where all .dk addresses are located

3. The DNS then gives your computer the location of *www.example.dk* in the .dk zone

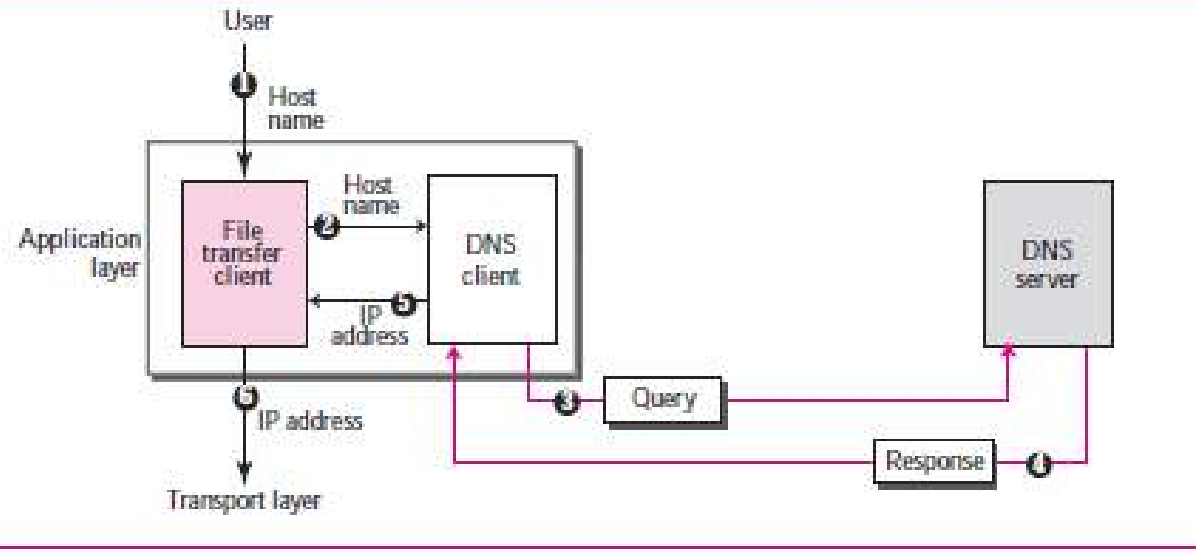
4. You arrive at the address.

DNS

- Domain name system
- phone book for the Internet. If you know a person's name but don't know their telephone number
- Technique to **translate** domain name or host name to corresponding IP address.
- earlier this were recorded in a file **host.txt**
- **Network information center** (NIC) maintained this file.
- Every night host attached to internet would receive a copy of the updated file
- By mid 80 the size of the file become **extremely large**.
- maintaining host.txt on a single server faced problems like traffic volumes, failure effects delay, maintenance.
- Domain name system came into picture.
- **A distributed database**
- Hierarchical domain based naming architecture

DNS Client and Server

- DNS Client helps to resolve **DNS requests** using an external DNS server
- DNS servers store and manage information about **domains** and respond to **resolution requests** for clients
- DNS database is a **distributed** name database stored on many DNS servers.
- Server uses a hierarchical tree structure for its name space and a hierarchical tree for name authorities and registration.
- Since **distributed** there is **no single server** that has information about every domain in the system.

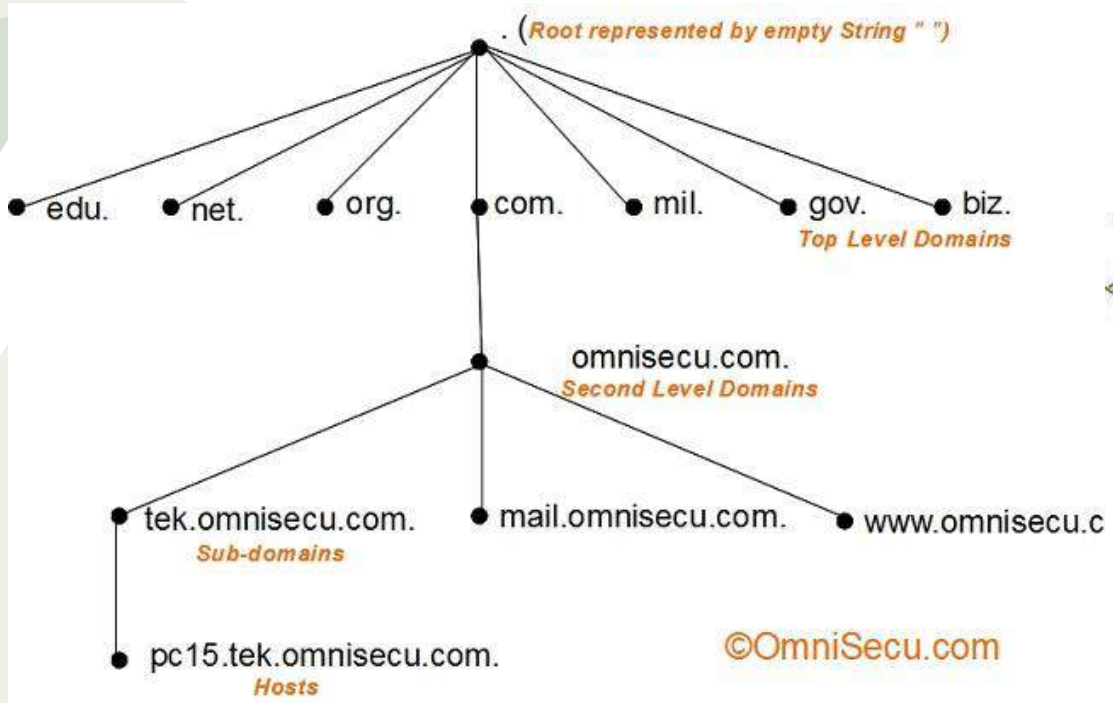


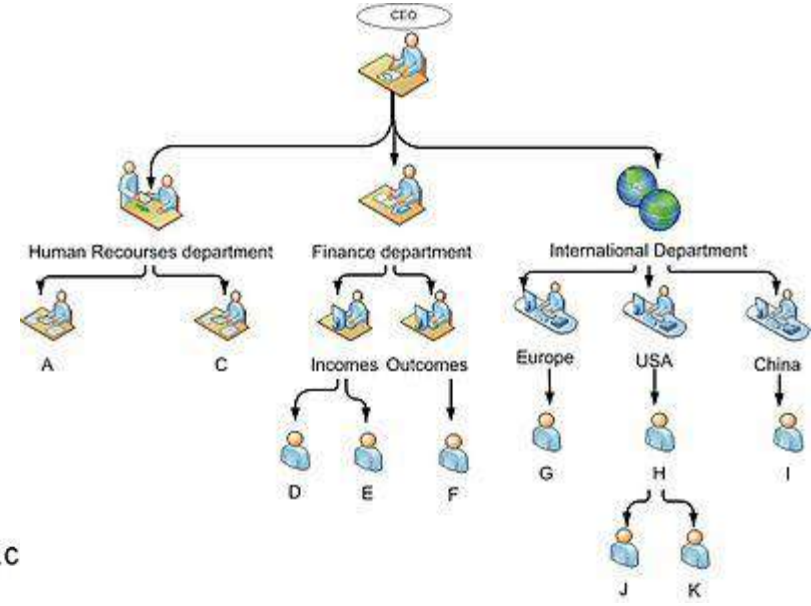
Each computer, after **being booted**, knows the address of **one DNS client**. The DNS client sends a message to a **DNS server with a query** that gives the file transfer server name using the known IP address of the DNS server.

- Further reading ---DNS query message format

DNS name space

- Internet is theoretically divided into hundreds of top-level domains.
- each domain can further be subdivided into sub-domains.
- subdivisions of the domain namespace and private TCP/IP network DNS domains supports new growth on the Internet and the ability to continually expand name and administrative groupings.
- Subdivisions are generally based on departmental or geographic divisions.





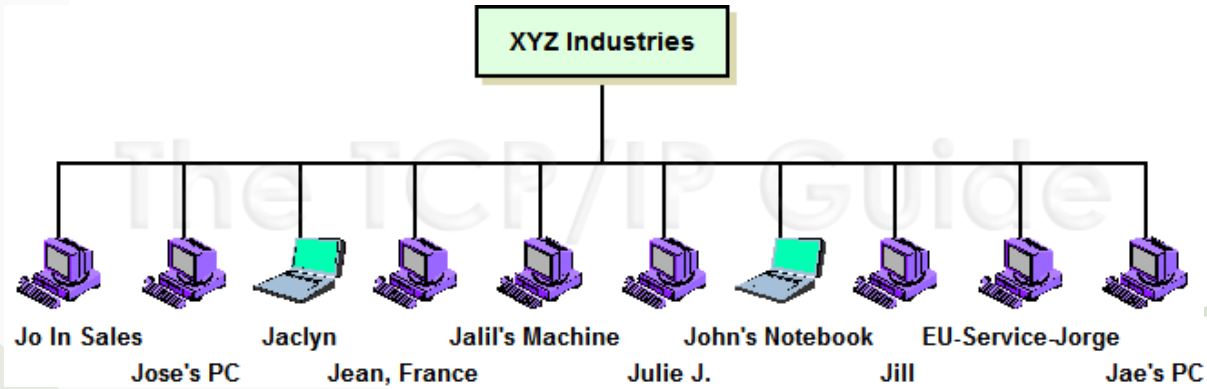
Name Space

- Must be carefully selected from a name space with complete control over the binding between the names and IP addresses.
- The names must be unique because the addresses are unique.
- A **name space that maps each address to a unique name can be organized in two ways:** flat or hierarchical.

Flat name space:

- A name is assigned to an address.
- A name in this space is a sequence of characters without structure.
- The names may or may not have a common section; if they do, it has no meaning.
- The main disadvantage ---- it cannot be used in a large system such as the Internet because it must be centrally controlled to avoid ambiguity and duplication.

Example: Within IIEST LAN ,HOD IT, DIRECTOR, REGISTRAR, DEAN etc.



Hierarchical Name Space

- **Each name is made of several parts. The first part can** define the **nature of the organization**, the second part can define **the name of an organization**, the third part can define departments in the organization, and so on.
- The authority to assign and control the name spaces can be decentralized.
- A central authority can assign the part of the name that defines the nature of the organization and the name of the organization.
- Responsibility of the rest of the name can be given to the organization itself.

http://www.narayanagroup.com/ //Educational

http://www.narayanahealth.org/ //Healthcare

http://hit.gov.in/ Howrah Improvement trust

http://hithaldia.in haldia institute of technology

Domain Name Space:

- To have a hierarchical name space, a **domain name space was designed.**
- The names are defined in an inverted-tree structure with the root at the top.

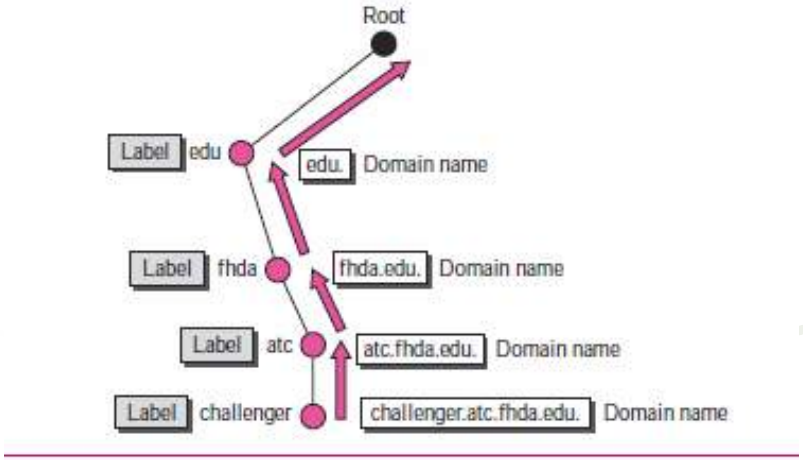
a) Label:

- Each node in the tree has a **label.**
- **String with a maximum of 63 characters.**
- Root label is a null string (empty string).

DNS requires that children of a node (nodes that branch from the same node) have different labels, which guarantees the uniqueness of the domain names.

b) Domain name:

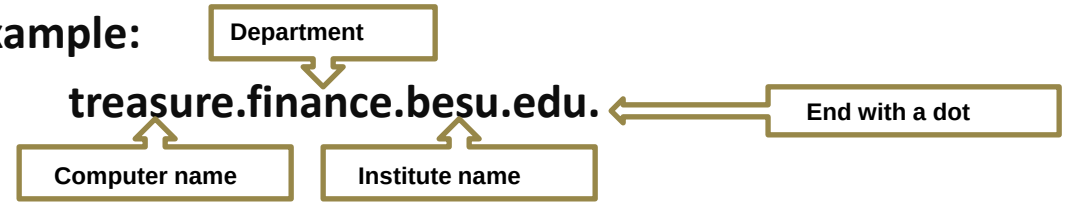
- Each node in the tree has a domain name. A full **domain name is a sequence of labels** separated by dots (.).
- Domain names are read from the node up to the root.
- Last label is the label of the root (null) [last character is a dot because the null string is nothing]



Fully Qualified Domain Name (FQDN):

- referred to as an *absolute domain name*
- **An FQDN is a domain name that contains** the full name of a host. It contains all labels, from the most specific to the most general, that uniquely define the name of the host.

Example:



Partially Qualified Domain Name (PQDN):

- used to specify a portion of a domain name, normally the host portion of it
- starts from a node, **but it does not reach the root**.
- used when the name to be resolved belongs to the same site as the client.

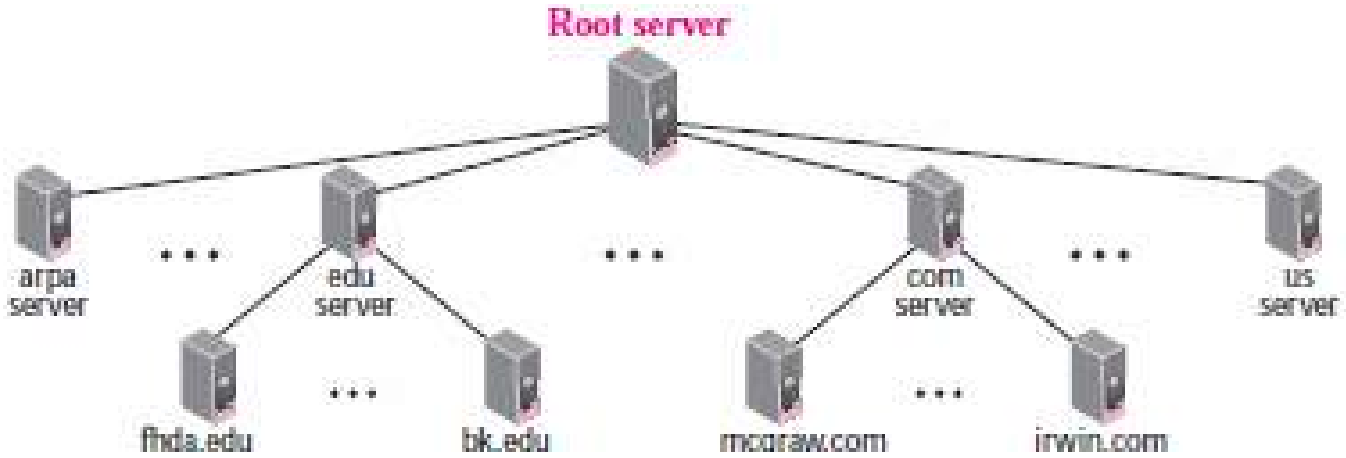
Distribution of name space

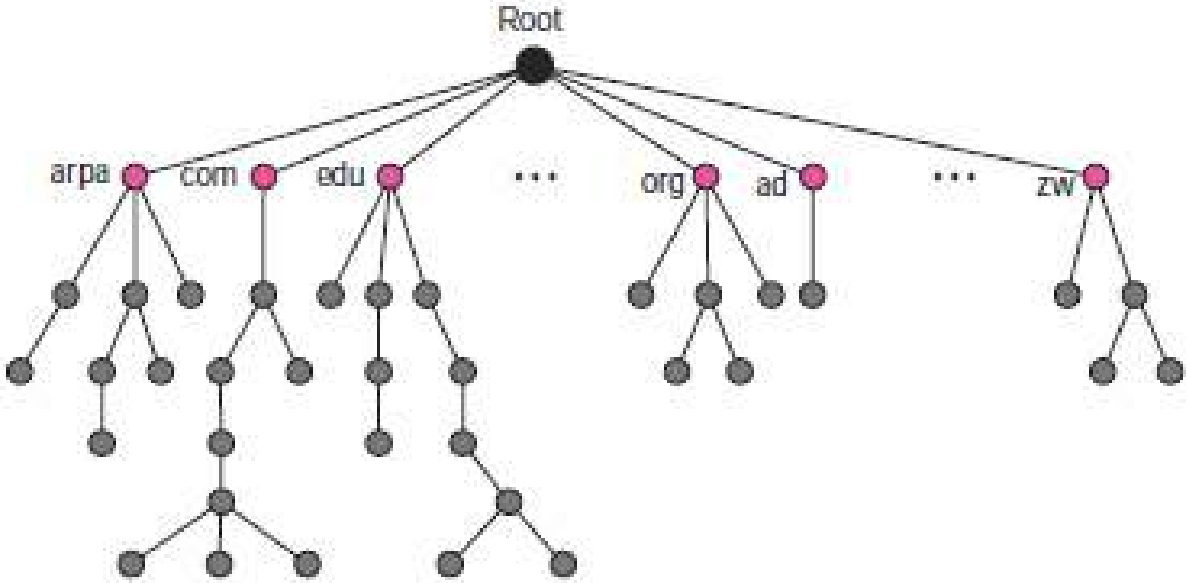
- The information contained in the domain name space must be stored.
- However, it is very inefficient **not reliable to have just one computer** store such a huge amount of information.
- Responding to requests from all over the world places a heavy load on the system.
- **Not reliable** ---any failure makes the data inaccessible.

Hierarchy of Name Servers:

Solution is to distribute the information among many computers called **DNS servers.**

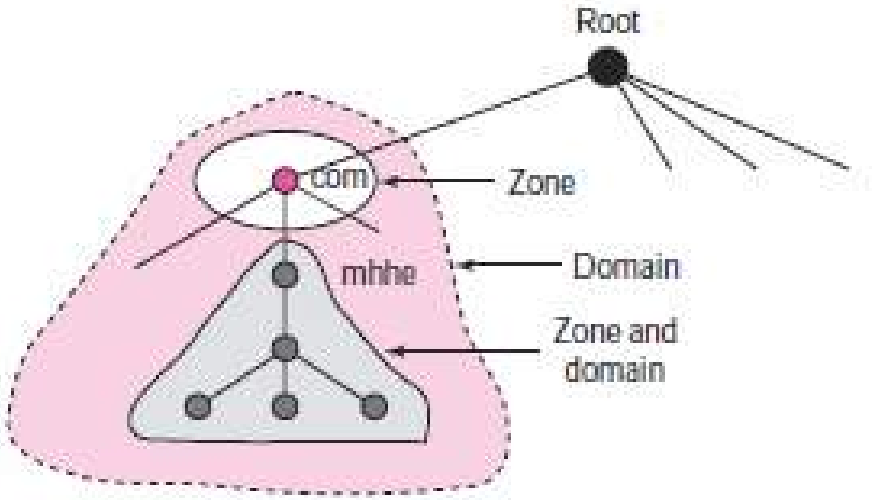
- One way to do this is to **divide the whole space into many domains** based on the first level.
- Let the root stand alone and **create as many domains** (subtrees) as there are first-level nodes.
- DNS allows domains to be divided further into smaller domains(subdomains).
- Each server can be responsible (authoritative) for either a large or small domain.
- In other words, we have a hierarchy of servers in the same way that we have a hierarchy of names


Root server
arpa server
edu server
com server
us server
fhda.edu
bk.edu
mcgraw.com
irwin.com


Root
arpa
com
edu
org
ad
zw

Zone: Complete domain name hierarchy cannot be stored on a single server, it is divided among many servers. **What a server is responsible for or has authority over is called a zone.**

- If a server accepts responsibility for a domain and does not divide the domain into smaller domains, the “domain” and the “zone” refer to the same thing.
- server makes a database called a zone file and keeps all the information for every node under that domain.
- If domain has subdomain and delegates part of its authority to other servers, “domain” and “zone” refer to different things.



Root server:

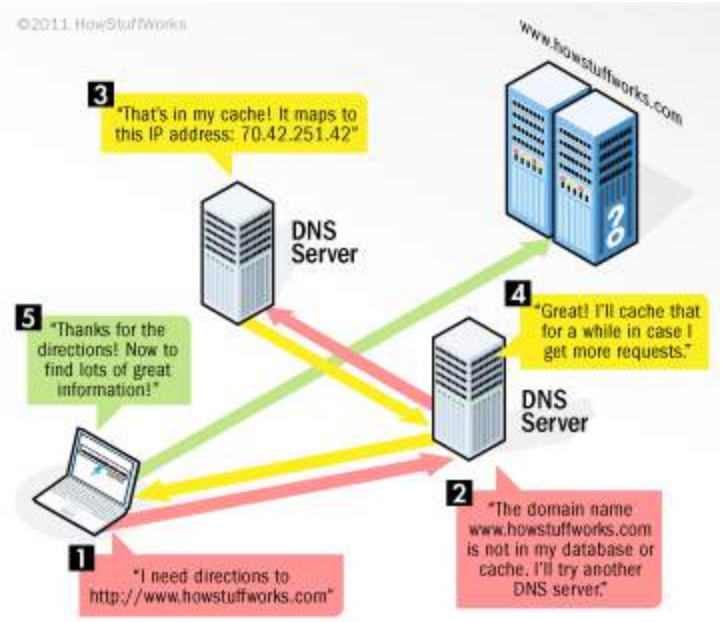
- Server whose zone consists of the whole tree.
- Usually does not store any information about domains but delegates its authority to other servers, keeping references to those servers.

Primary and Secondary Servers:

- DNS defines two types of servers: primary and secondary.
- **Primary server** stores a file about the zone for which it is an authority.
- Responsible for creating, maintaining, and updating the zone file. zone file on a local disk.
- **Secondary server transfers the complete information about a** zone from another server (primary or secondary) and stores the file on its local disk.
- Neither creates nor updates the zone files. If updating is required, it **must be done by the primary server**, and updated version is sent to the secondary.

DNS server

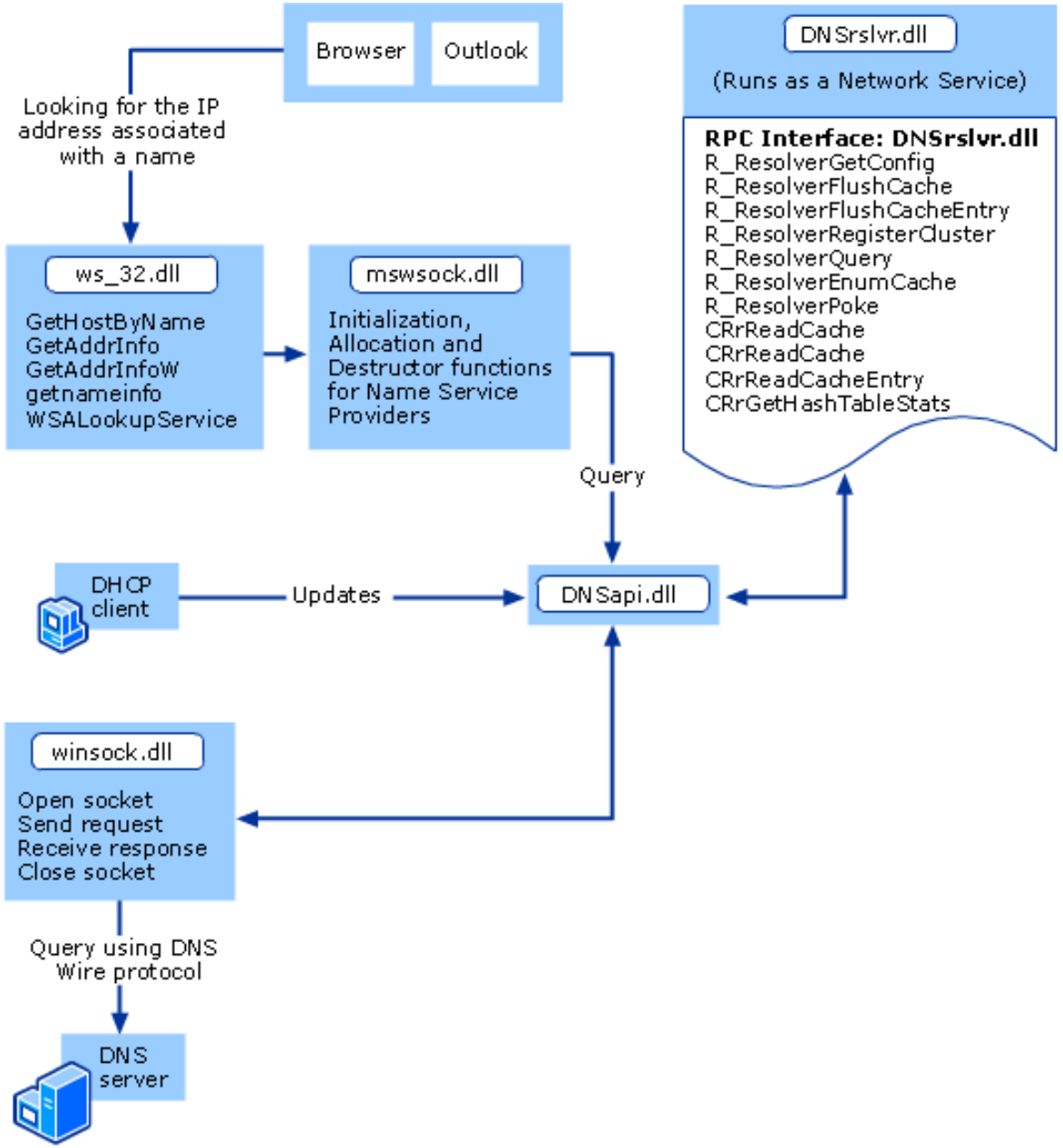
- computer server that contains a database of public IP addresses and their associated hostnames,
- serves to resolve, or translate, common names to IP addresses as requested.



How DNS server work?

Step 1: Request information

- process begins from a user ask his computer to resolve a hostname, such as visiting *http://dyn.com*.
- computer looks is its local DNS cache, which stores information that the computer has recently retrieved.
- If the computer doesn't already know the answer, it needs to perform a **DNS query** to find out.


Browser
Outlook
Looking for the IP address associated with a name
ws_32.dll
GetHostByName
GetAddrInfo
GetAddrInfoW
getnameinfo
WSALookupService
mswsock.dll
Initialization, Allocation and Destructor functions for Name Service Providers
DNSrslvr.dll
(Runs as a Network Service)
RPC Interface: DNSrslvr.dll
R_ResolverGetConfig
R_ResolverFlushCache
R_ResolverFlushCacheEntry
R_ResolverRegisterCluster
R_ResolverQuery
R_ResolverEnumCache
R_ResolverPoke
CRrReadCache
CRrReadCache
CRrReadCacheEntry
CRrGetHashTableStats
Query
DHCP client
Updates
DNSapi.dll
winsock.dll
Open socket
Send request
Receive response
Close socket
Query using DNS Wire protocol
DNS server

DNS Server

Step 2.1: Ask the recursive DNS servers

- If the information is not stored locally, computer queries (contacts) its ISP's **recursive DNS servers**.
- These specialized computers perform the legwork of a DNS query on your behalf.
- Recursive servers have their own caches, so the process usually ends here and the information is returned to the user.

Step 2.2: Ask the root nameservers

- If the recursive servers don't have the answer, they query the **root nameservers**.
- A **nameserver** is a computer that answers questions about domain names, such as IP addresses.
- The thirteen root nameservers act as a kind of telephone switchboard for DNS.
- They don't know the answer, but they can direct our query to someone that knows where to find it.

DNS Server

Step 2.3: Ask the TLD nameservers

- The root nameservers look at the first part of the request, reading from right to left — *www.google*. ***com*** — and direct it query to the **Top-Level Domain (TLD) nameservers** for *.com*. Each TLD, such as *.com*, *.org*, and *.us*, have their own set of nameservers, **which act like a receptionist** for each TLD.

Step 2.4: Ask the authoritative DNS servers

- TLD nameservers review the next part of the request — *www.google****.com*** — and direct our query to the nameservers responsible for this *specific* domain. These **authoritative nameservers** are responsible for knowing all the information about a specific domain, which are stored in **DNS records**. There are many types of records, which each contain a different kind of information.

DNS Server

3. Retrieve the record

- The recursive server retrieves the A record for *google.com* from the **authoritative nameservers and stores the record in its local cache**.
- Further request for same name will not need to go through the lookup process again.
- All records have a **time-to-live** value, which is like an expiration date. After a while, the recursive server will need to ask for a new copy of the record to make sure the information doesn't become out-of-date.

4 & 5. Receive the answer

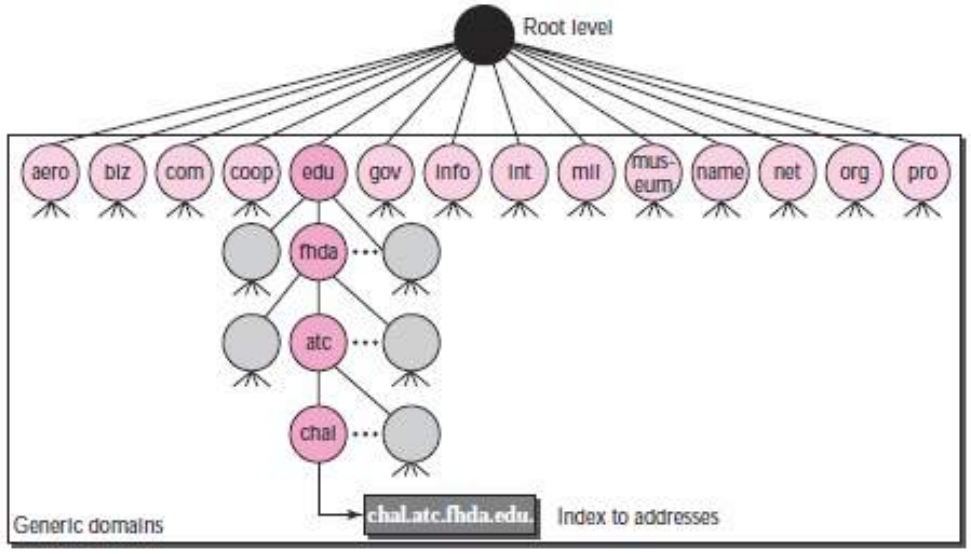
- Armed with the answer, recursive server **returns the a record back** to the requesting computer. It stores the record in its cache.
- reads the IP address from the record, then passes this information to browser. The browser then opens a connection to the webserver and receives the website.

DNS in the Internet

- DNS is a protocol that can be used in different platforms.
- In the Internet, the domain name space (tree) is divided into three different sections: generic domains, country domains, and the inverse domain.

Generic Domains:

- Define registered hosts according to their **generic behavior**.
- Each node in the tree defines a domain, which is an index to the domain name space database.



Label	*Description*
aero	Airlines and aerospace companies
biz	Businesses or firms (similar to "com")
com	Commercial organizations
coop	Cooperative business organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International organizations
mil	Military groups
museum	Museums and other non-profit organizations
name	Personal names (individuals)
net	Network support centers
org	Nonprofit organizations
pro	Professional individual organizations

Country Domain:

Uses **two-characte**r country abbreviations.

Some country like US has state abbreviation under country domain.

can be found https://www.domainit.com/domains/country-domains.mhtml.

Country Code Domain Extensions
.au (Australia)
.br (Brazil)
.ca (Canada)
.cn (China)
.de (Germany)
.fr (France)
.in (India)
.nl (Netherlands)
.jp (Japan)
.ru (Russia)
.us (United States)
.uk (United Kingdom)
etc...

Generic Domain Extensions	
Sponsored	Unsponsored
.aero	.com
.asia	.net
.cat	.org
.coop	.biz
.edu	.info
.gov	.name
.int	.pro
.jobs	
.mil	
.mobi	
.museum	
.tel	
.travel	

Inverse Domain

- Used to map an **address to a name**.

Situation…….

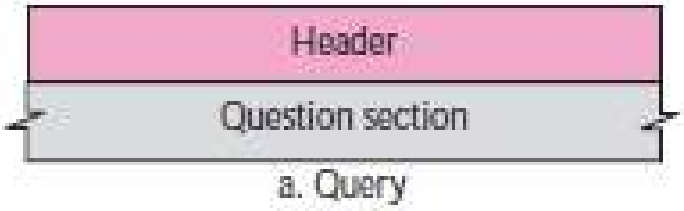
- A server has received a request from a client to do a task.
- It has a file that contains a list of authorized clients, **only the IP address** of the client (extracted from the received IP packet).
- Server asks its resolver to send a query to the DNS server to map an address to a name to determine if the client is on the authorized list.

Indian domain name

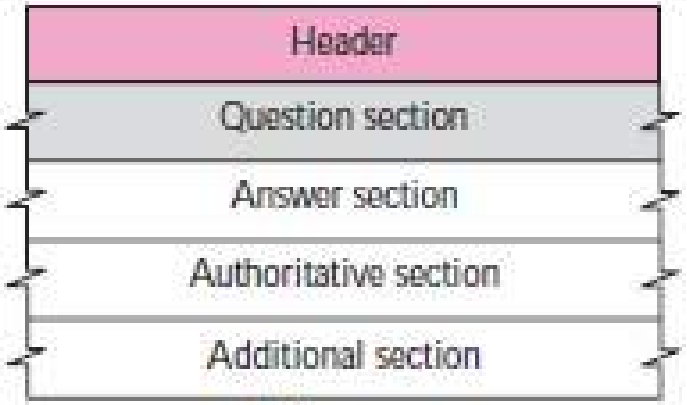
- **.co.in** : commercial website in India.
- **.net.in** : network website in India.
- **.org.in** :non-profit organization website in India.
- **.gen.in** : general website in India.
- **.firm.in** : used for firm in India
- **.ac.in** : academic institutes in India
- **.edu.in** : educational institutes / colleges / schools

DNS Messages

- DNS has two types of messages: query and response.
- Both types have the same format.
- The query message consists of a header and question records; the response message consists of a header, question records, answer records, authoritative records, and additional records.



a. Query



b. Response

Identification	Flags
Number of question records	Number of answer records (All 0s in query message)
Number of authoritative records (All 0s in query message)	Number of additional records (All 0s in query message)

Header section:

Identification:

- 16-bit field used by the **client** to match the **response with the query**.
- Client uses a **different identification number** each time it sends a query.
- Server **duplicates this number** in the corresponding response.

Flag

- 16-bit field consisting of the subfields
- **QR (query/response):** 1-bit subfield defines the type of message. 0: query message. 1: Response message.
- **OpCode:** 4-bit subfield defines the type of query or response. [0: standard, 1: inverse, 2: server status request]
- **AA (authoritative answer):** 1-bit subfield. set (value of 1) means that the name server is an authoritative server. It is used only in a response message.
- **TC (truncated):** This is a 1-bit subfield. **set (value of 1) means** that the response was more than 512 bytes and truncated to 512. It is used when DNS uses the services of UDP
- **RD (recursion desired):** 1-bit subfield. set means the **client desires a recursive answer**. It is set in the query message and repeated in the response message.

- **RA (recursion available):** 1-bit subfield. set in the response**,** it means that a **recursive response is available**. It is set only in the response message.
- **Reserved:** 3-bit subfield set to 000**.**
- **rCode:** 4-bit field that shows the status of the error in the response**.** only an authoritative server can make such a judgment

Value	*Meaning*	*Value*	*Meaning*
0	No error	4	Query type not supported
1	Format error	5	Administratively prohibited
2	Problem at name server	6–15	Reserved
3	Domain reference problem		

- **Number of question records:** 16-bit field containing the number of queries in the question section of the message.
- **Number of answer records:** 16-bit field containing the number of answer records in the answer section of the response message. Its value is zero in the query message.
- **Number of authoritative records:** 16-bit field containing the number of authoritative records in the authoritative section of a response message. Its value is zero in the query message.
- **Number of additional records:** 16-bit field containing the number of additional records in the additional section of a response message. Its value is zero in the query message.

- A resolver sends a query message to a local server to find the IP address for the host "*chal.fhda.edu.". We discuss the query and response messages separately. Figure shows the query* message sent by the resolver.

0x1333		0x0100	
1		0	
0		0	
4	'c'	'h'	'a'
'l'	4	'f'	'h'
'd'	'a'	3	'e'
'd'	'u'	0	Continued on next line
1	1		

0x0100 → 0000000100000000

QR	OpCode	AA	TC	RD	RA	Reserved	rCode
0	0000	0	0	1	0	000	0000

0x1333	0x8180
1	1
0	0

Response message header

QR	OpCode	AA	TC	RD	RA	Reserved	rCode
1	0000	0	0	1	1	000	0000

Security of DNS

- DNS can be attacked in several ways
- Attacker may read the **response of a DNS server** to find the nature or names of sites the **user mostly accesses**. This type of information can be used to find the user's profile.
- Attacker may intercept the response of a DNS server and **change it** or create a totally new bogus response to direct the user to the site or domain the attacker wishes the user to access. Can be protected using message origin authentication and message integrity
- Attacker may flood the DNS server to overwhelm it or eventually crash it. **DoS.**

DNSCrypt

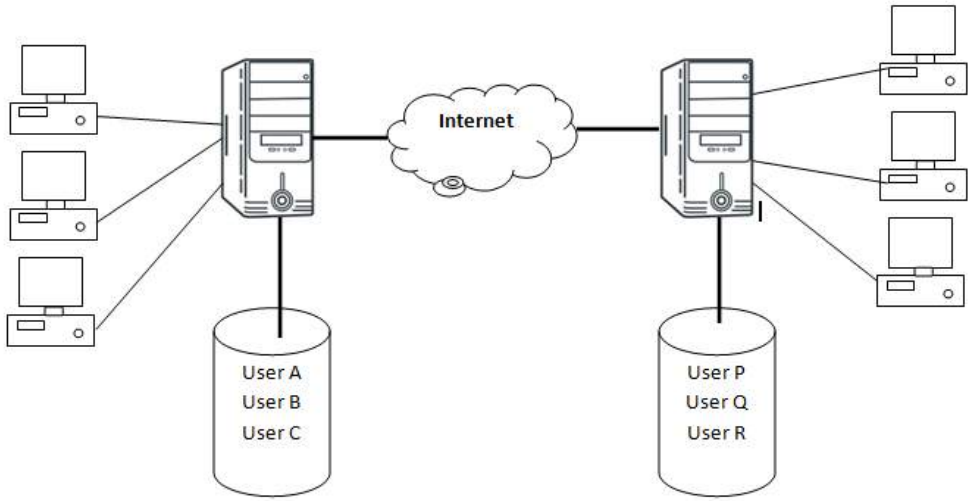
turns regular DNS traffic into encrypted DNS traffic that is secure from eavesdropping and man-in-the-middle attacks.

doesn't require any changes to domain names or how they work.

simply provides a method for securely encrypting communication between client and DNS servers

Email

- communication is asynchronous.
- may keep a mail box in each node.
- but communication is not possible if another node is not open.
- to solve this problem—put another computer with responsibility of storing and forwarding email messages.-----**email server**.
- mailbox facility (some dedicated disk space) provided for each client using its email facility.
- The server is kept on constantly
- A copy of the email is always stored on the mail server disk space—spooling



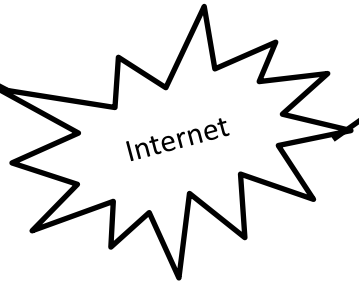
Email anatomy

- Each electronic mailbox on the server has a unique email address.
- Two parts

user name	@	Domain name

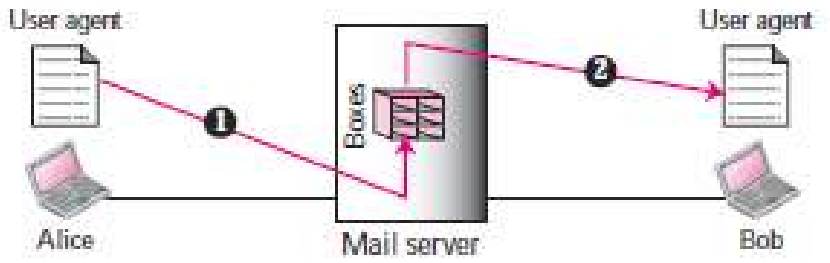
yahoo.com		
atul	rk	sg1
jitesh	shivam	mani

gmail.com		
bimal	aka	sg1
sujan	suman	ritu



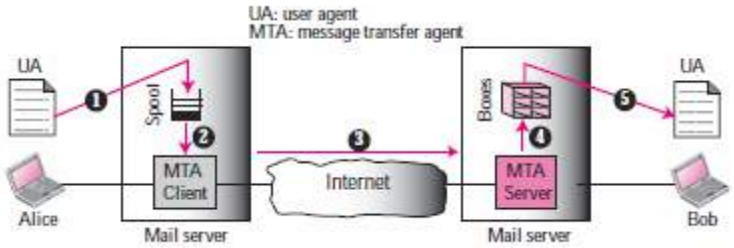
Architecture of Email

Case I: Sender and receiver of the e-mail are users on the same mail server:



- Directly connected to a shared mail server.
- The administrator creates one mailbox (*part of a local hard drive, a special file with permission restrictions.*) for each user where the received messages are stored.
- When Alice needs to send a message to Bob,→runs a *user agent (UA) program to prepare the message and store it in* Bob's mailbox.
- The message has the sender and recipient mailbox addresses (names of files).
- Bob can retrieve and read the contents of his mailbox at his convenience using a user agent.

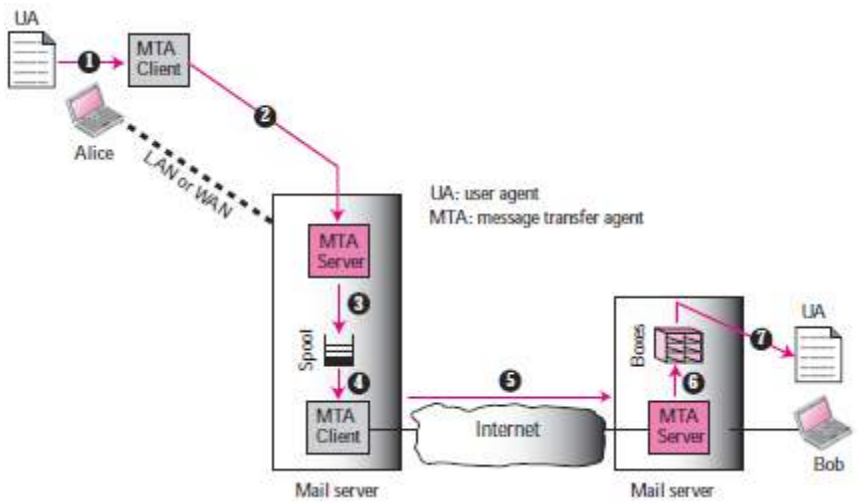
Case II: sender and the receiver are on two different mail servers



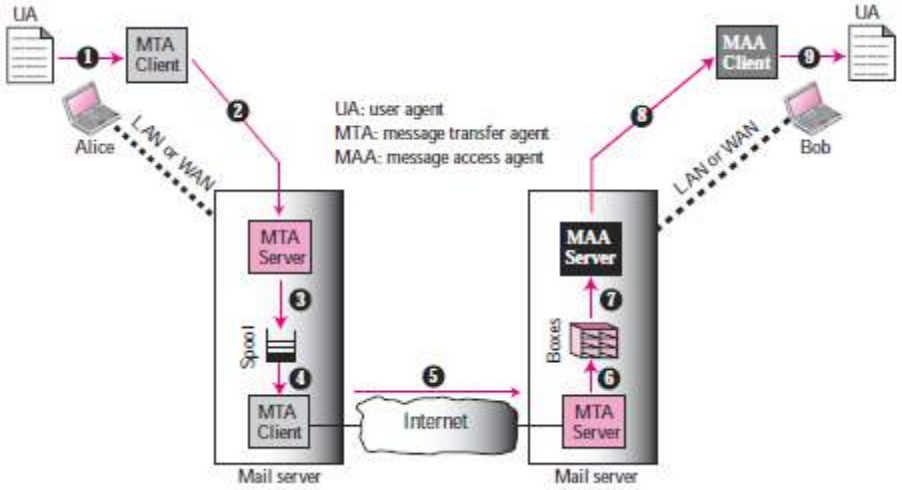
- Message needs to be sent over the Internet. Need user agents (UAs) and message transfer agents (MTAs)
- Alice use a user agent program → send message to the mail server at her own site. →Mail server maintains a queue (spool) to store messages waiting to be sent.
- Two message transfer agents are needed: one client and one server. Server needs to run all of the time.
- The client, can be triggered by the system when there is a message in the queue to be sent.

Case III: Bob is directly connected to mail server but Alice is separated from mail server

- Alice is either connected to the mail server via a point-to-point WAN—such as a dial-up modem, a DSL, or a cable modem—or she is connected to a LAN in an organization that uses one mail server for handling e-mails; all users need to send their messages to this mail server.
- Alice prepares her message using UA. → sends it through LAN or WAN.
- Can be done through a pair of message transfer agents (client and server).
- Whenever Alice has a message to send, she calls the user agent which, in turn, calls the MTA client.
- MTA client establishes a connection with the MTA server on the system, which is running all the time.
- The system at Alice's site queues all messages received. It then uses an MTA client to send the messages to the system at Bob's site; the system receives the message and stores it in Bob's mailbox.


UA
MTA Client
Alice
LAN or WAN
UA: user agent
MTA: message transfer agent
MTA Server
Spool
MTA Client
Mail server
Internet
Boxes
MTA Server
Mail server
UA
Bob

Case IV: Both Alice and Bob are separated from mail server



- Message has arrived at Bob's mail server, Bob needs to retrieve it.
- Need another set of client-server agents, which is called **message access agents (MAAs).** Bob uses an MAA client to retrieve his messages**.**
- **MAA client** sends a request to the MAA server, which is running all the time, and requests the transfer of the messages.

SMTP

- Heart of email system.
- **port 25 is the default transmission channel for internet email.** (**Port 587 is reserved for email message submission**)
- Consists of two aspects, user agent (UA) and mail transfer agent (MTA).
- User agent is the user interface client email software. It provides user facility for reading an email retrieving it from server, composing an email etc.
- MTA is the interface between email system and local email server.
- SMTP performs two transfers

a) sender computer to sender's SMTP server

b) Sender SMTP server to receiver's SMTP server

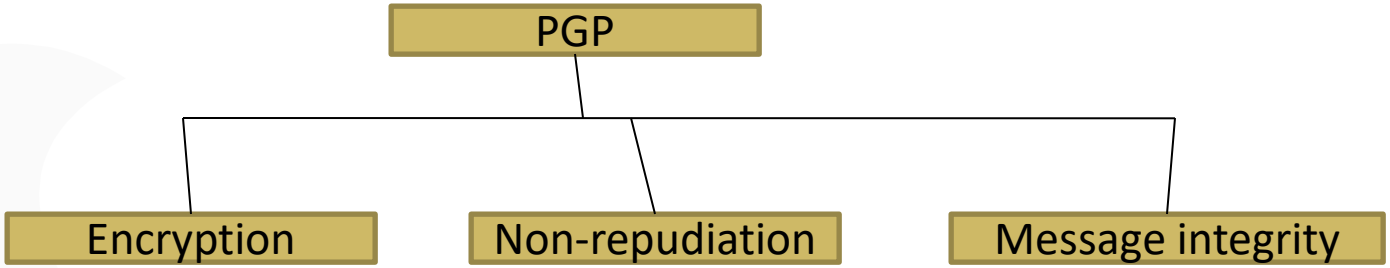
The rest is performed by POP and IMAP (Internet Message Access Protocol).

SMTP is asynchronous (different from other protocol) thus delayed delivery.

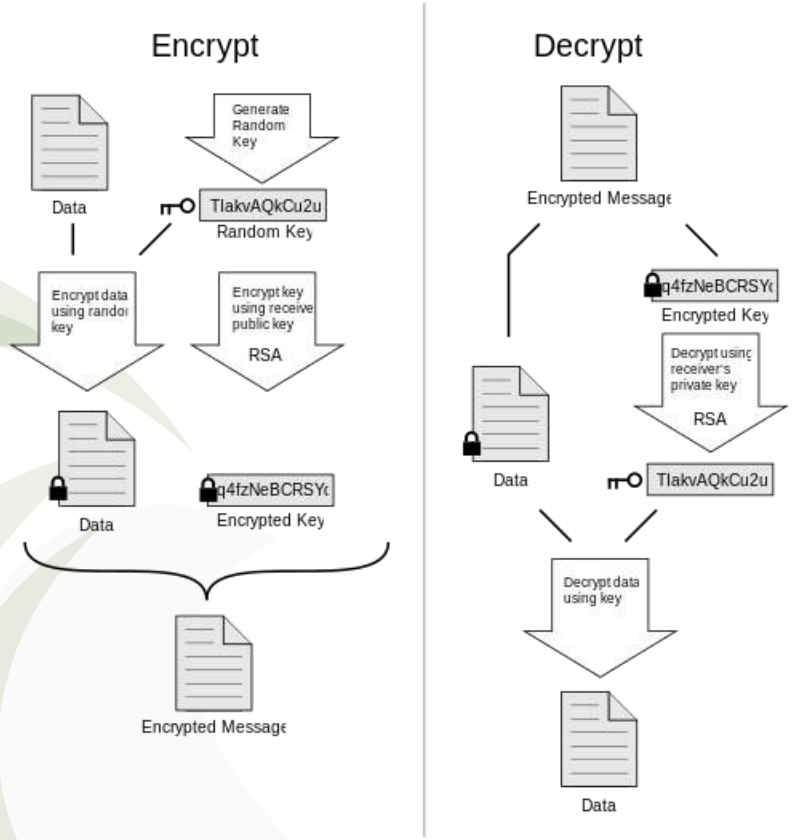
Further reading: Types of responses returned by server.

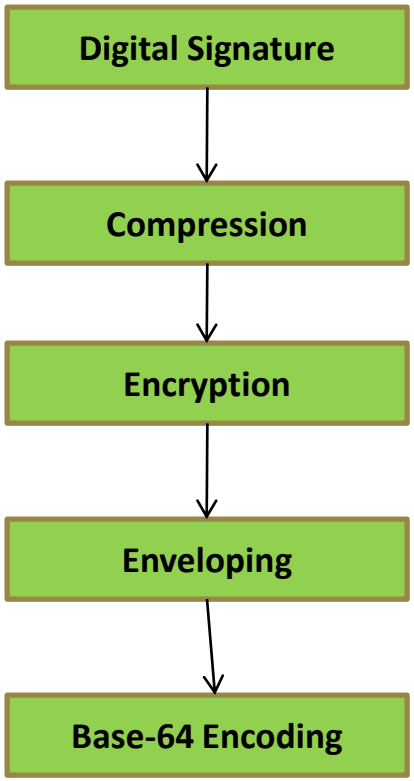
email privacy

- email message potentially travel a number of intermediate routers and networks.
- require privacy.
- Pretty good Privacy (PGP).
- Modified version of Privacy Enhanced Mail (PEM).
- Phil Zimmerman introduced PGP protocol.
- Supports basic requirement of cryptography.
- Viacrypt is an advanced version for organization (low cost)



How PGP work?


Encrypt
Data
Generate Random Key
TlakvAQkCu2u
Random Key
Encrypt data using rando key
Encrypt key using receive public key
RSA
Data
q4fzNeBCRSYc
Encrypted Key
Encrypted Message
Decrypt
Encrypted Message
q4fzNeBCRSYc
Encrypted Key
Decrypt using receiver's private key
RSA
Data
TlakvAQkCu2u
Decrypt data using key
Data


Digital Signature
Compression
Encryption
Enveloping
Base-64 Encoding

Function	Algorithms Used	Description
Digital signature	DSS/SHA or RSA/SHA	A hash code of a message is created using SHA-1. This message digest is encrypted using DSS or RSA with the sender's private key and included with the message.
Message encryption	CAST or IDEA or Three-key Triple DES with Diffie-Hellman or RSA	A message is encrypted using CAST-128 or IDEA or 3DES with a one-time session key generated by the sender. The session key is encrypted using Diffie-Hellman or RSA with the recipient's public key and included with the message.
Compression	ZIP	A message may be compressed, for storage or transmission, using ZIP.
Email compatibility	Radix 64 conversion	To provide transparency for email applications, an encrypted message may be converted to an ASCII string using radix 64 conversion.
Segmentation	—	To accommodate maximum message size limitations, PGP performs segmentation and reassembly.

- Use the concept of RSA cryptosystem in encryption.
- PGP allows four security options while sending an email.

a) Signature only

b) Signature and base 64 encoding

c) Signature encryption , enveloping and encoding.

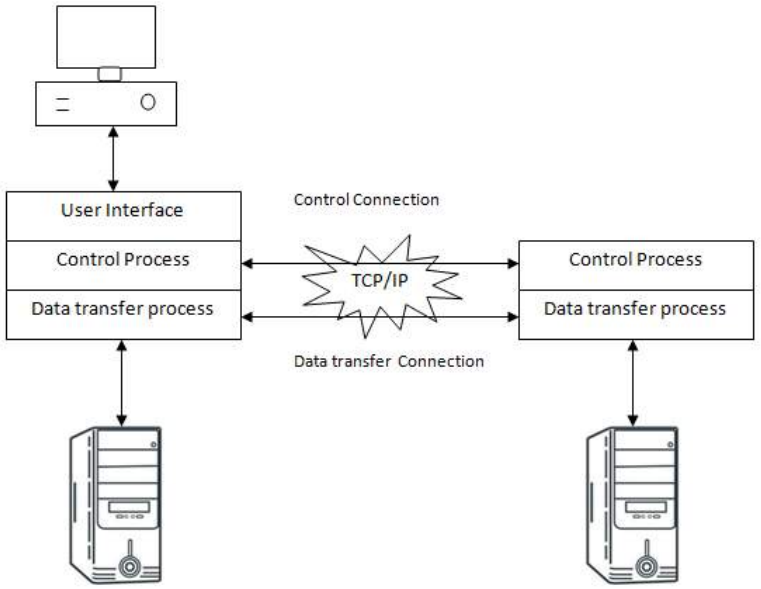
FTP

- FTP (**F**ile **T**ransfer **P**rotocol) utility program is commonly used for transferring files to and from other computers.
- Why FTP? SMTP is already there…
- client need necessary authorization to download a file from server.
- Client and server may be different in terms of h/w and OS.
- FTP contacts remote computer using TCP/IP.
- Once the connection is established storing to a remote computer or downloading from a remote computer is possible.
- FTP uses two connections between client and server for inter-communication.
- one used for actual files's data transfer, other used for control information (Command & responses).
- Here FTP differs from other protocols and makes FTP more efficient.

FTP connection

Control Connection:

- Server passively waits for a client –passive open
- (server waits endlessly for accepting TCP connection from its client/s)
- Client sends an open request (TCP request) to the server. ---Active open



➢client node opens FTP client software. **(Prompts the user for the domain name/IP address of the server)**

➢FTP at client issues a TCP connection with IP address of server to the underlying TCP software.

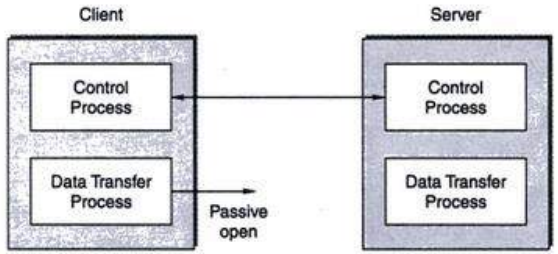
➢TCP on client establishes TCP connection between client and server using three way handshake.(Other protocols are IP and ARP)

➢After establishing successful connection client can download or upload file.

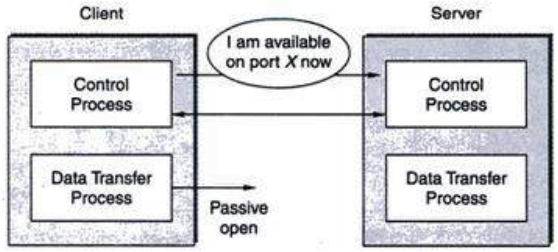
FTP connection

Data transfer connection:

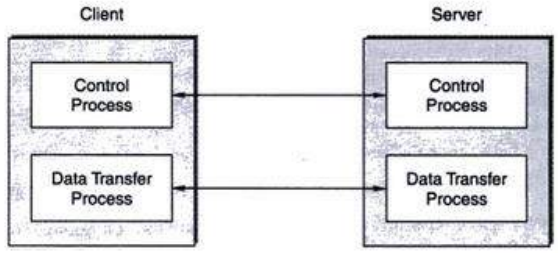
- client opens a passive open command for data transfer connection on a particular port number.
- Client sends the port number to server by already established control connection.
- Invokes a open request
- server opens a data transfer connection on port 20 (Standard FTP port).



Step 1 Passive open of the data transfer process by the client



Step 2 Client sends the port number of the data transfer process to the server



Step 3 Active open by the server to compete the data transfer connection with the client

Client server communication using FTP

- Control connection
- Data transfer connection
- Type of the file to be transferred
- The structure of the data (Byte oriented –transferred as a continuous stream or Record oriented-file is divided into records then sent one by one).
- Transmission mode

Stream mode: default mode. FTP to TCP in continuous stream of data then packet.

For byte oriented no end of character is needed.

for record oriented each record has end of character and file itself has eof.

Block mode: Data delivered from FTP to TCP in terms of block.

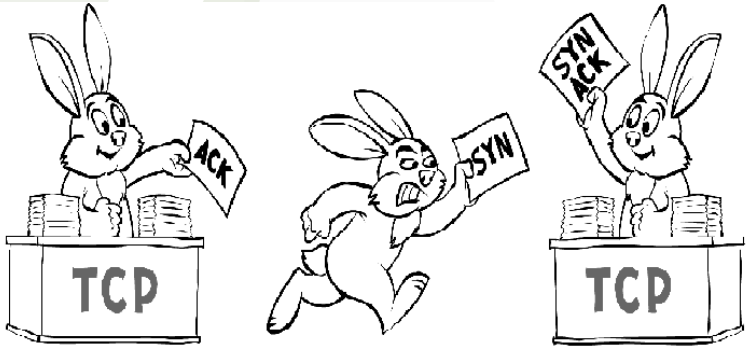
Each block has 3 byte header. First byte is called block descriptor another two byte for block size.

Compressed mode: Normally RLE is used.

FTP Commands

TCP/IP Basic

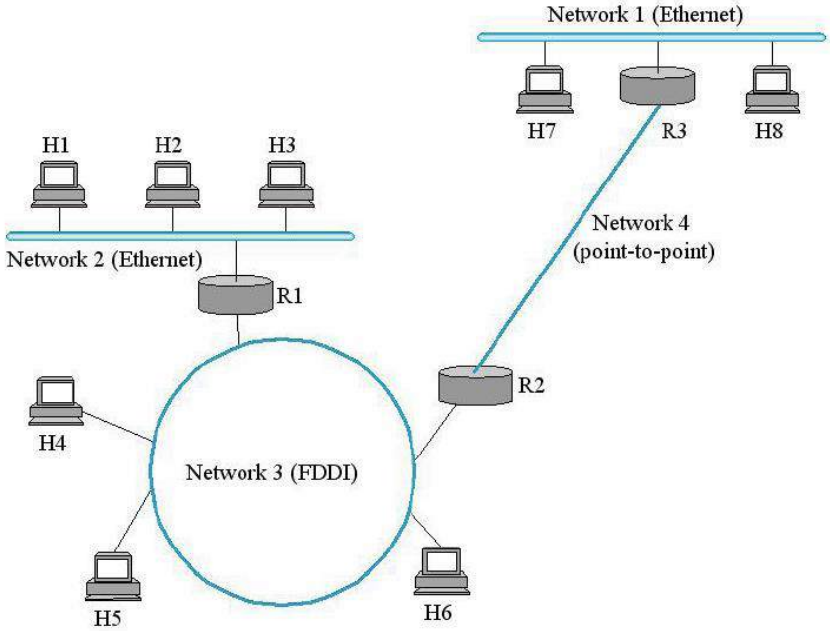
Shyamalendu Kandar



internet vs Internet

internet (small ‘i’):

- ✓ Connecting many computer network together.
- ✓ use of gateways that provide a common method of routing information packets between the networks.
- ✓ is a logical network, which is built out of a collection of physical networks.



Internet:

- ✓ global internetwork to which a large percentage of networks are now connected.
- ✓ is one of internets, and is the largest one.
- ✓ In some of the first printed mentions of the Internet, like many other US government projects of the period, it was referred to in all caps as INTERNET.

----Some guides specify -----capitalized as a noun but not capitalized as an adjective, e.g., "internet resources"

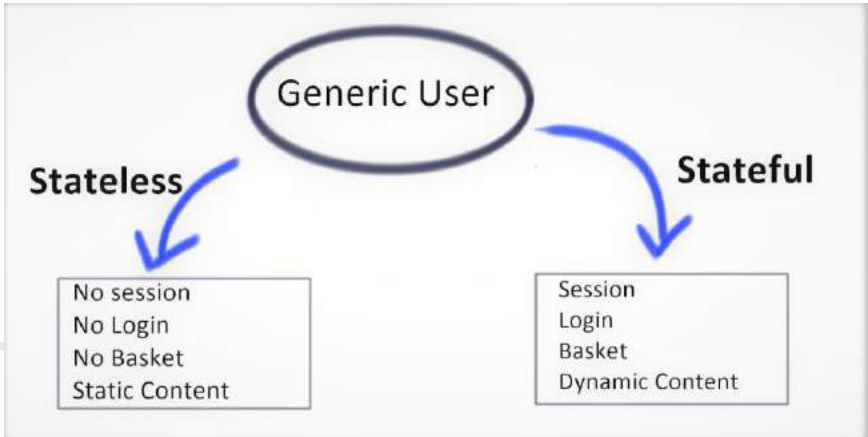
TCP/IP basic

- designed in 1970s by 2 DARPA scientists—Vint Cerf and Bob Kahn

- basic communication protocol of the Internet.
- higher layer, Transmission Control Protocol.
- manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message.
- The lower layer, Internet Protocol.
- It handles the address part of each packet so that it gets to the right destination.
- Each gateway computer checks this address to see where to forward the message.

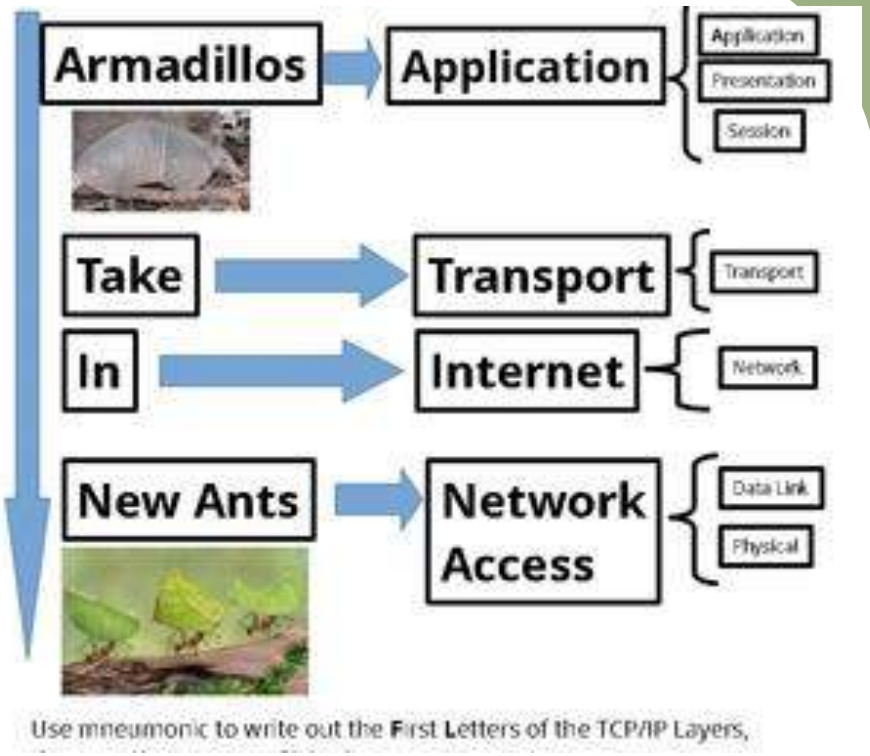
Cerf (left) and Kahn being awarded the *Presidential Medal Of Freedom* by Former President Bush in 2005

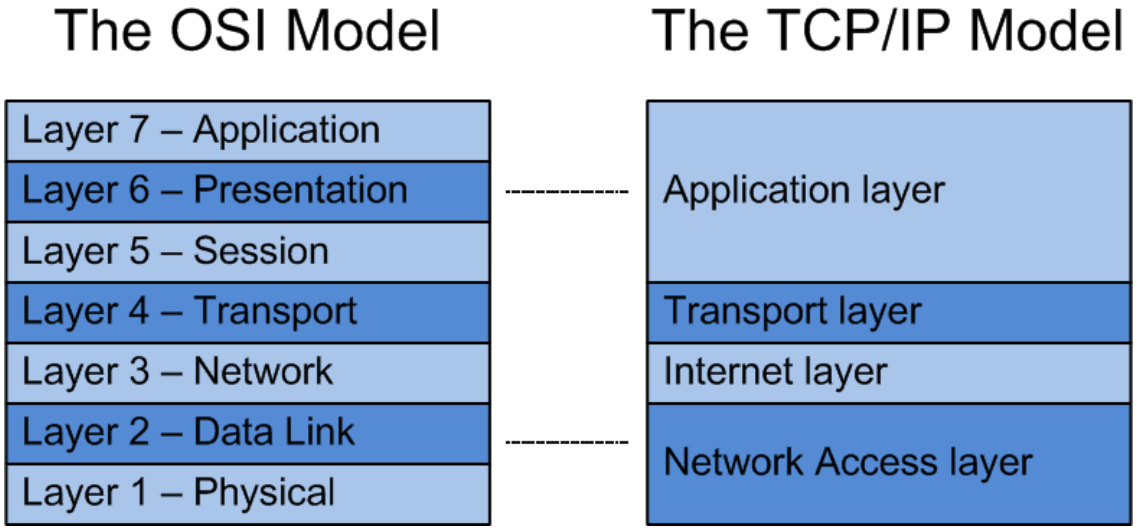
- uses the client/server model of communication.--- A computer user (a client) requests and is provided a service (such as sending a Web page) by another computer (a server) in the network.
- communication is primarily point-to-point, meaning each communication is from one point (or host computer) in the network to another point or host computer.
- Stateful protocol-- both systems maintain information about the session itself during its life.
- Connection orriented– need to establish an end-to-end connection before any data is sent.
- sometimes called a "reliable" network service, because it guarantees that data will arrive in the proper sequence.



Layers in TCP/IP

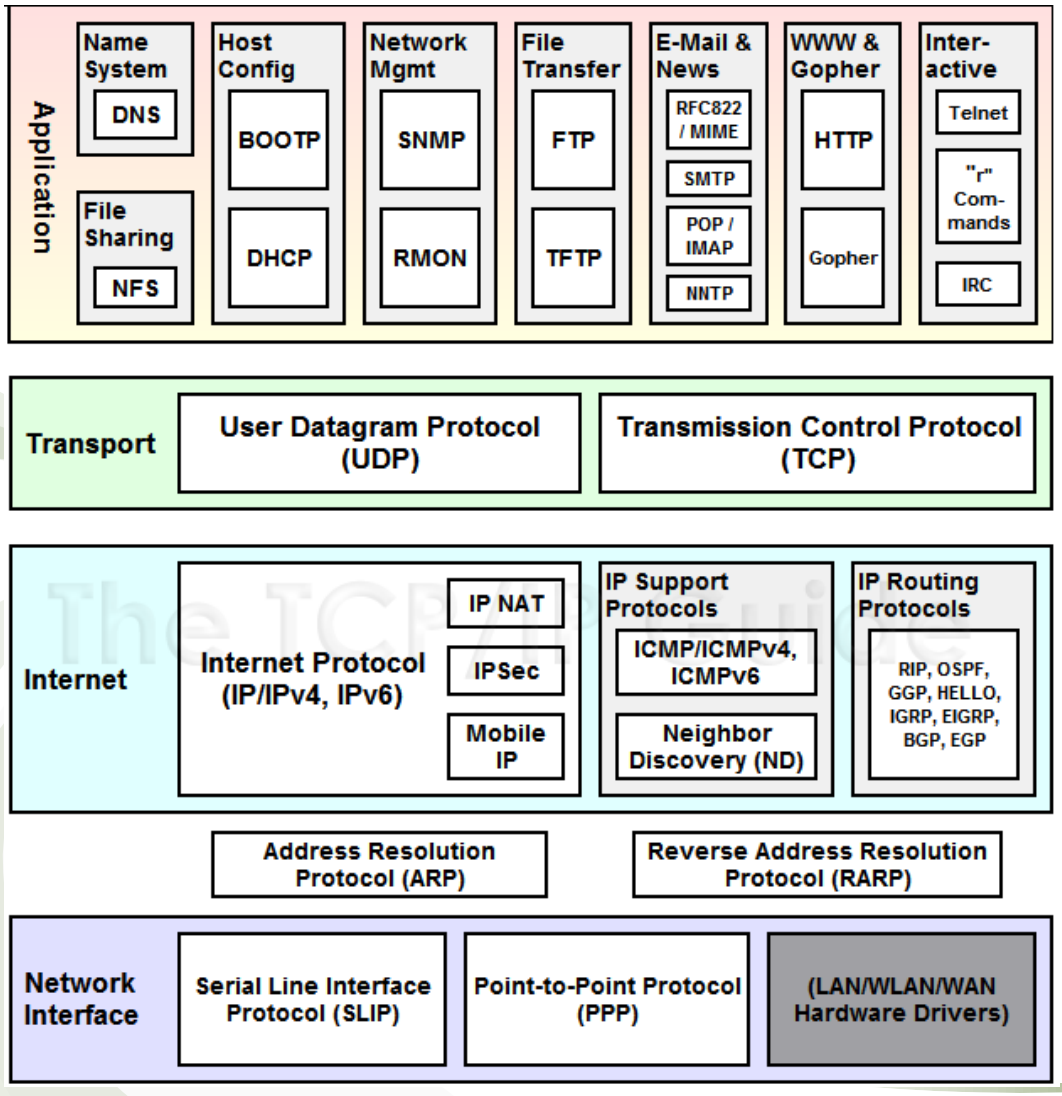
- TCP/IP developed before OSI
- Instead TCP/IP consists of 4 layers.
- Data link and Physical merged



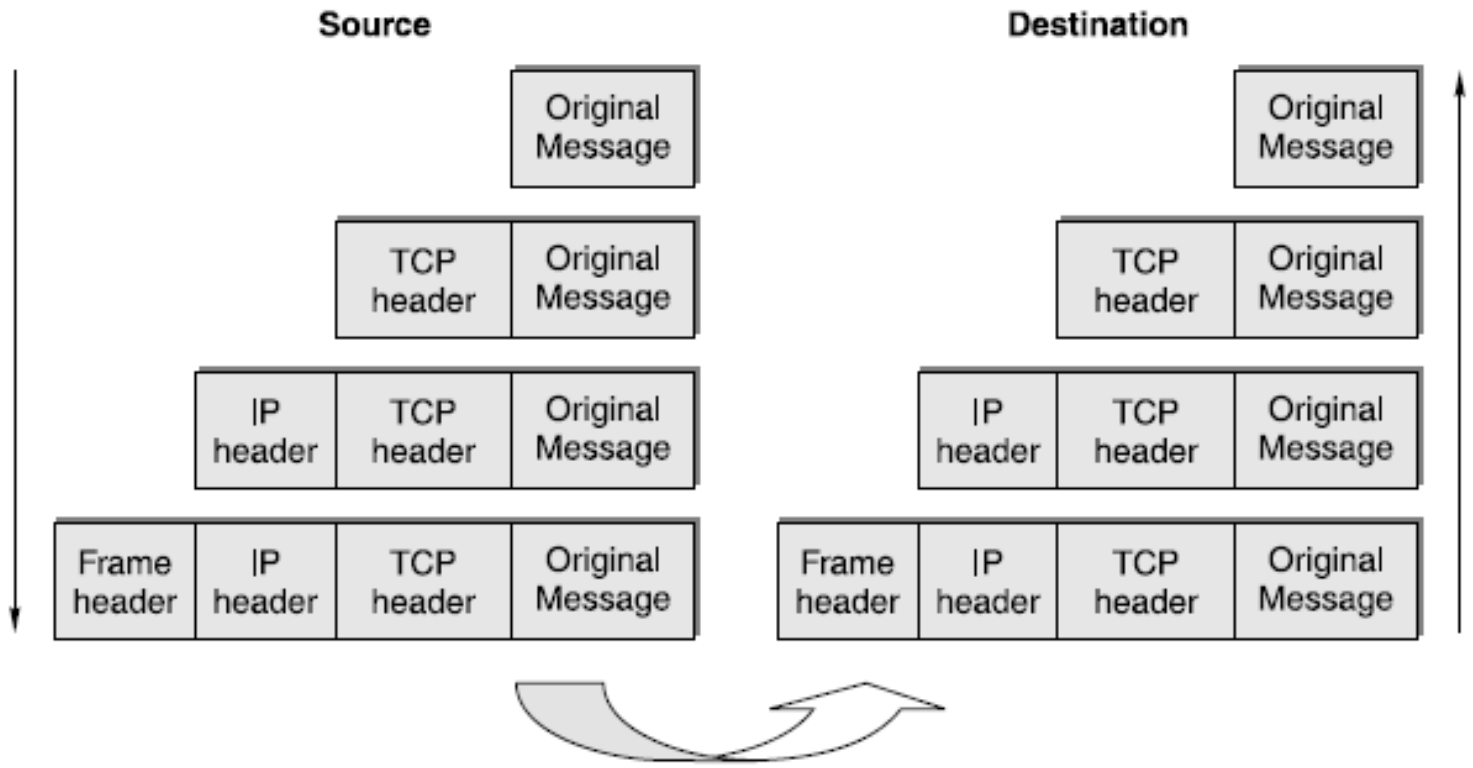


- **Network access--**Deals with hardware level, voltage etc.
- covers media access and control(MAC) strategies i.e who can send data and when. Deals with frame format.
- **Internet layer:** Concerned with the format of datagram. Forwarding datagram from source to destination via one or more routers.
- **Transport layer:** ensures reliable communication between sender and receiver, error free communication, in-sequence communication
- **Application:** Runs various applications.

Protocol in different layers



General TCP/IP Packet format

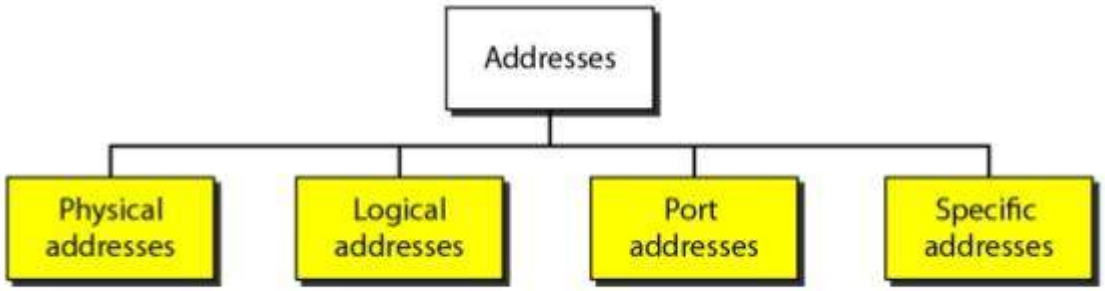


Addressing

- like the postal address on envelope

4 types of computer address:

Address Type	Purpose
Physical	Used in network access layer
Logical	Used in network layer
Port	Used in transport layer
Specific	Used by application layer



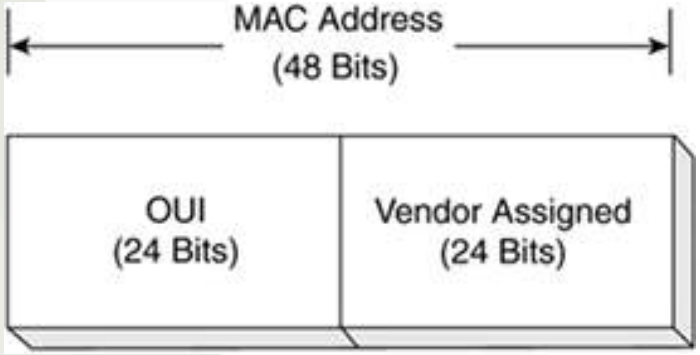
Physical address:

- hardware-level address
- MAC address (burned into the ROM of the NIC card)
- used by the Ethernet interface
- Every device must have a unique physical address.
- used to communicate on the network
- hardware manufacturer obtains a block of physical address numbers from the IEEE

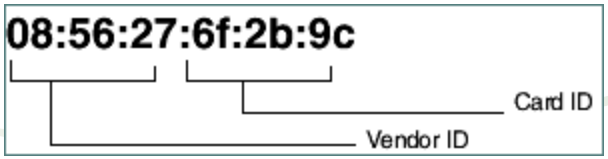
(When a manufacturer has exhausted all MAC addresses available under their first three bits, then they apply to the IEEE for another manufacturer address.)

- Size vary across technology.
- Eathernet use 48 bit.

mm:mm:mm:cc:cc:cc



OUI: Organizationally unique identifier



How to get physical address

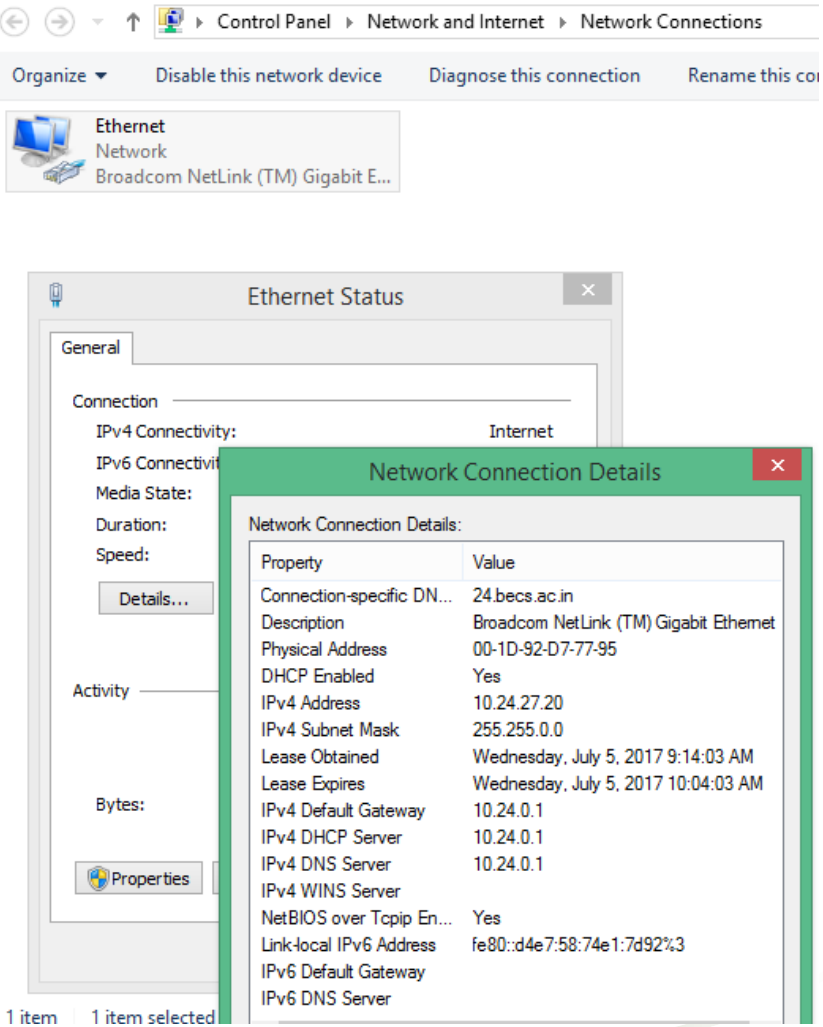
Windows 7, 8, 8.1, and 10

Start button→ Control Panel.

→View network status and tasks →Change adapter settings→select Status →Details

Or

Start → run→ cmd→ ipconfig/all



Physical address:

Is MAC address unique?

“Devices are Uniquely Identified by Their MAC Addresses”

------incorrect.

Vendor may put same MAC for two devices by mistake or intentionally.

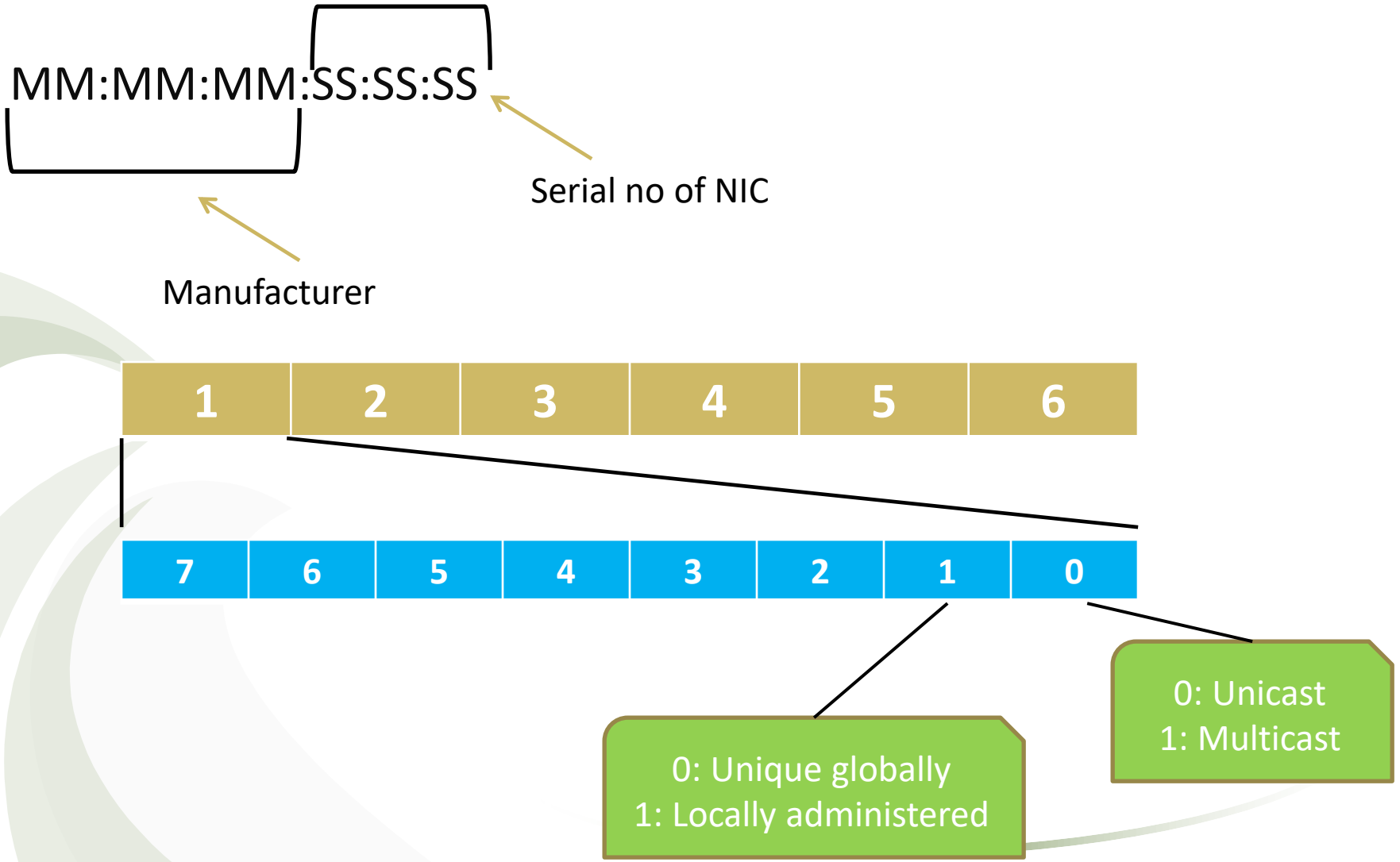
By MAC Spoofing it can be changed. There are tools which can make an operating system believe that the NIC has the MAC address of a user's choosing.

If manufacturer assigns same MAC to two devices and ships those in different parts of the world.

Very little chance network cards with the same MAC Address will end up on the same network.

Reason: Physical address has authority within LAN or WAN.

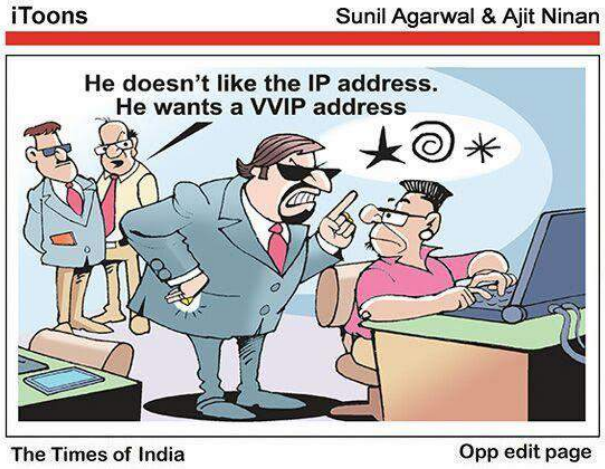
Format of MAC



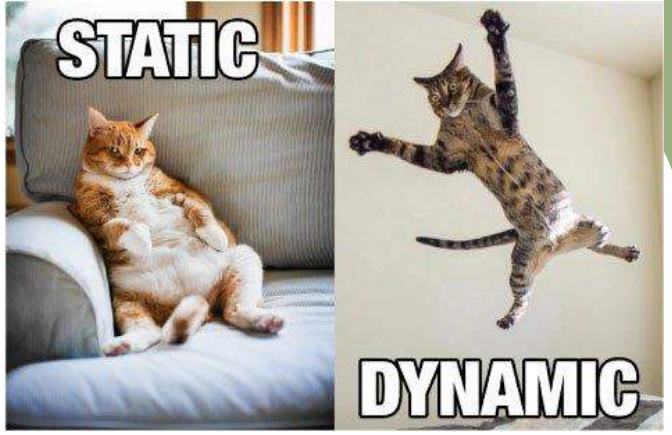
Logical Address

- **first** deployed in 1983 in the ARPANET.
- universal address , known as IP address
- independent of the underlying network infrastructure.
- 32 bit address (**four decimal numbers separated by period '.' characters for IPV4)**
- a network-layer address that is interpreted by a protocol handler.
- assigned to it for the purpose of routing between networks.

When a packet sent from a sender for a receiver,
it goes through one or more routers.
IP never change. But source and destination physical
Address keep changing at each step..



Logical Address



Private IP: For local network, Not recognized for Internet, Assigned by LAN administrator

Public IP : for Internet, assigned by service provider

(For home network every device has private IP, where as router has public IP)

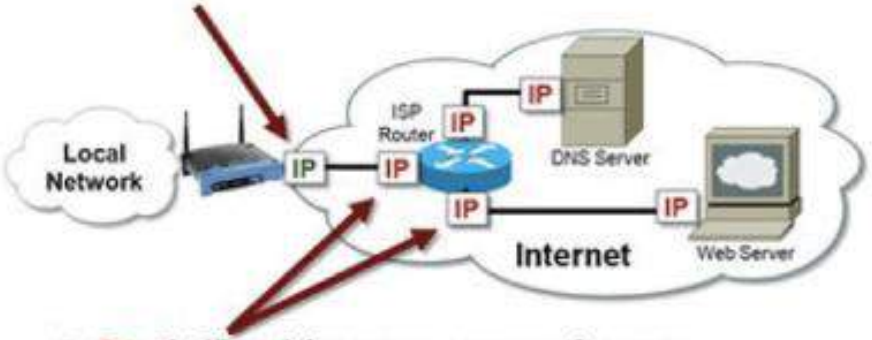
Static IP: Fixed, created manually. Needs for devices having constant access.

Dynamic IP: Changes. assigned, as needed, by Dynamic Host Configuration Protocol (DHCP) servers.

	Private address range	
Class	start address	finish address
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

	Public address range	
Class	start address	finish address
A	0.0.0.0	126.255.255.255
B	128.0.0.0	191.255.255.255
C	192.0.0.0	223.255.255.255
D	224.0.0.0	239.255.255.255
E	240.0.0.0	254.255.255.255

- *Dynamic* IP addresses periodically change
  - Typically assigned to ISP customers



- *Static* IP addresses never change

STATIC IP

Advantages

Better DNS support: much easier to set up and manage with DNS servers

Server hosting: web server, email server, or any other kind of server, having a static IP address makes it easier for customers to find you via DNS.

Convenient remote access: easier to work remotely using a Virtual Private Network (VPN) or other remote access programs.

More reliable communication: easier to use Voice over Internet Protocol (VoIP) for teleconferencing or other voice and video communications.

More reliable geo-location services: easier to get services can match the IP address with its physical location. Weather forecast

Disadvantages

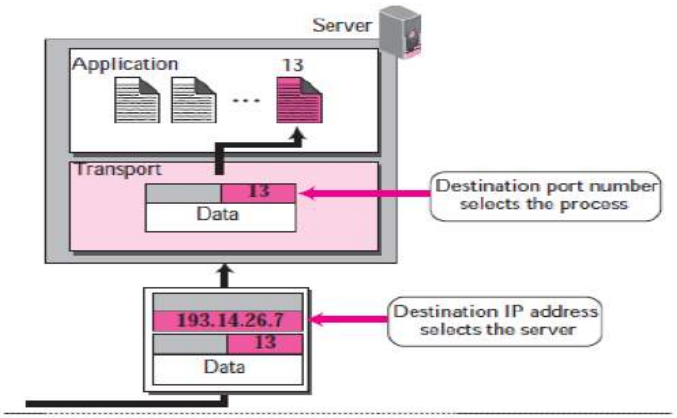
more hackable: hackers know exactly where your server is on the Internet. That makes it easier for them to attack it.

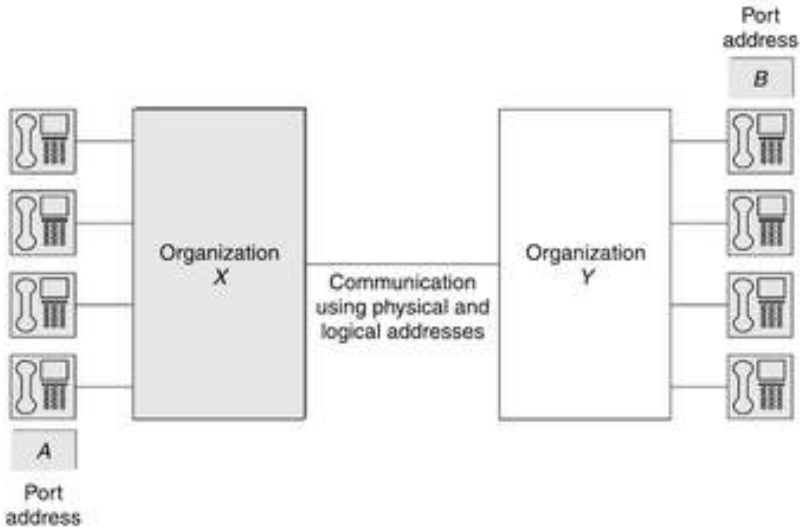
Higher cost: ISPs generally charge more for static IP addresses.

Real-world security concerns: Anyone with the right network tools can find where you and your computers are located.

Port address

- ensures packets reach to right application. is an endpoint of communication
- logical address of each application or process that uses a network or the Internet to communicate.
- Router job is to send the packet to the receiver. Port address uniquely identifies an network application on the receiving computer.
- Each application run with a port no.(logically) on the computer.
- Each application/program is allocated a 16-bit integer port number. This number is assigned automatically by the OS, manually by the user or is set as a default for some popular applications.
- logical construct that identifies a specific process or a type of network service.
- Transmission Control Protocol and the User Datagram Protocol, a **port** number is 16-bit unsigned numbers that is put in the header appended to a message unit.





Port address

- Port numbers work in collaboration with networking protocols. ----incoming message/packet, IP address is used to identify the destination computer/node, whereas the port number further specifies the destination application/program in that computer.
- Similarly, all outgoing network packets contain application port numbers in the packet header to enable the receiver to distinguish the specific application.
- mainly used in TCP and UDP based networks, with an available range of 65,535 for assigning port numbers.

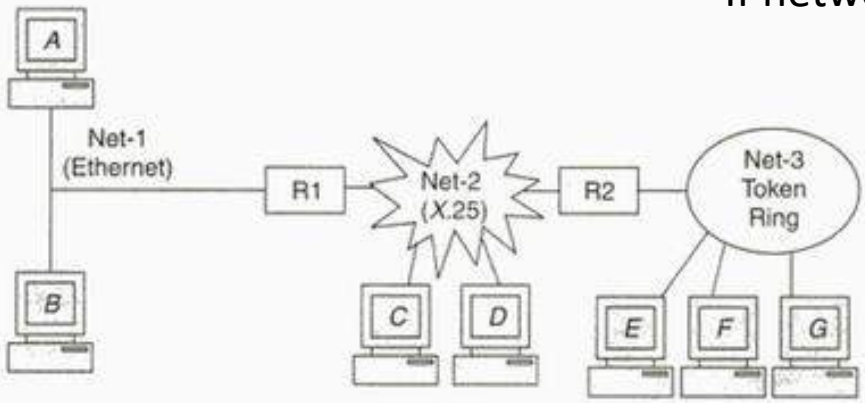
Specific Address

- Application specific
- user-friendly addresses designed for that specific application.
- email address, web address
- Conversion required (from human to machine and vice versa)

"My business card is large to accommodate my website URL, email, Twitter address, Facebook address, fax number, voice mail, private line number, cell number, and Tumblr address."

A real scenario...

- Three networks.
- Governed by eathernet, X.25, Token ring protocol
- Connected by router R1 and R2.
- If network1 wants to send message to network3 ?



Preamble (8 bytes)	Destination Address (6 bytes)	Source Address (6 bytes)	Frame Type (2 bytes)	Data (46–1500 bytes)	CRC (4 bytes)

(a) Ethernet frame format

General Format Identifier (4 bytes)	Logical Channel Identifier (12 bytes)	Receive Number (4 bytes)	Send Number (4 bytes)	Data (Variable length)

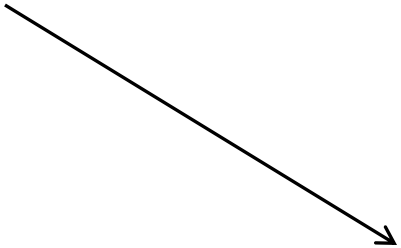
(b) X.25 datagram format

Preamble (8 bytes)	Access Control Field (8 bytes)	Frame Control (48 bytes)	Destination Address (48 bytes)	Source Address (48 bytes)	Data (Variable length)	Other data (56 bytes)

(c) Token Ring frame format

End user and other people dealing with their own network.

Single large n/w of computers

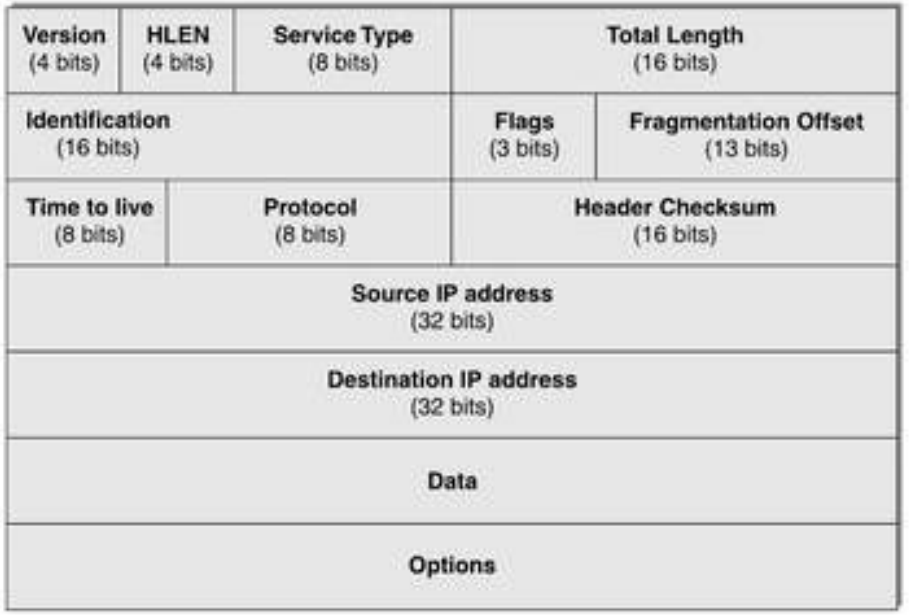


Free to choose the H/W and n/w technology that suit their requirements

How to identify a computer in the n/w?

- MAC is there why IP is required?
- IP is there why MAC is required?

IP datagram



Version: Current version. Now 4 In future 6

Header Length:

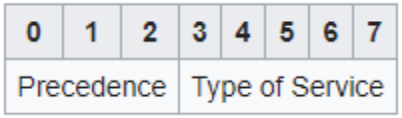
- size of the header
- length of the header is variable (between 20 and 60 bytes).
- default length is 20 bytes, and the value of this field is 5 (5 x 4 = 20).
- When the option field is at its maximum size, the value of this field is 15 (15 x 4 = 60).

Service type:

- allow different types of IP datagrams (**for example, datagrams particularly requiring low delay, high throughput, or reliability**) to be distinguished from each other.

[it might be useful to distinguish real-time datagrams such as those used by an IP telephony application)

- is a policy issue determined by the router's administrator.
- first 3 bits are called precedence bits. The next 4 bits are called type of service (TOS) bits and the last bit is not used.
- is now used by **Differentiated Services** and is called the **Diff Serv Code Point (DSCP)**.



Precedence:

- used for **QOS** (Quality of Service) Purposes.
- defines the priority of the datagram in issues such as congestion
- some data has higher importance than other.
- Higher priority data should be processed first because it could contain packets which are important to run network communication such as routing protocols data.

- Precedence value, higher has more priority
- **000** (0) - Routine
- **001** (1) - Priority
- **010** (2) - Immediate
- **011** (3) - Flash
- **100** (4) - Flash Override
- **101** (5) - Critical
- **110** (6) - Internetwork Control
- **111** (7) - Network Control

- If a router is congested and needs to discard some datagrams, those datagrams with lowest precedence are discarded first

Type of service:

Bits 0-2: Precedence.
Bit 3: Delay (0 = Normal Delay, 1 = Low Delay)
Bit 4: Throughput (0 = Normal Throughput, 1 = High Throughput)
Bit 5: Reliability (0 = Normal Reliability, 1 = High Reliability)
Bits 6: Reserved
Bit 7 : Not used

0	1	2	3	4	5	6	7
PRECEDENCE			D	T	R	0	0

IP Datagram

Total length:

- denotes total length of the IP datagram.
- theoretical maximum size of the IP datagram is 65,535 bytes.
- However, datagrams are rarely larger than 1,500 bytes.

if that packet goes into an interface that has a less than 1500 byte MTU?

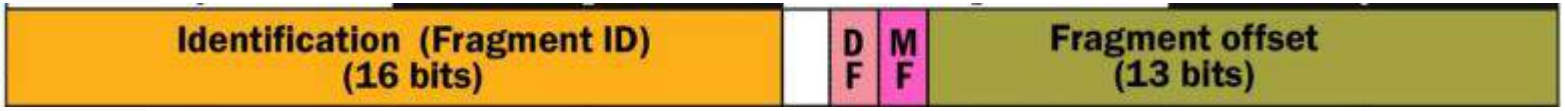
Identification:

- incremented by 1 each time a datagram is sent.
- Used in a situation when datagram is fragmented
- assigned to manage fragmentation and reassembly.
- Uniquely identifies the datagram.
- All fragments of a datagram contain the same identification value.
- allows the destination host to determine which fragment belongs to which datagram.

[Datagram passes through different n/w s. May need to be fragmented to sub-datagram to match the physical frame size of the underlying n/w]

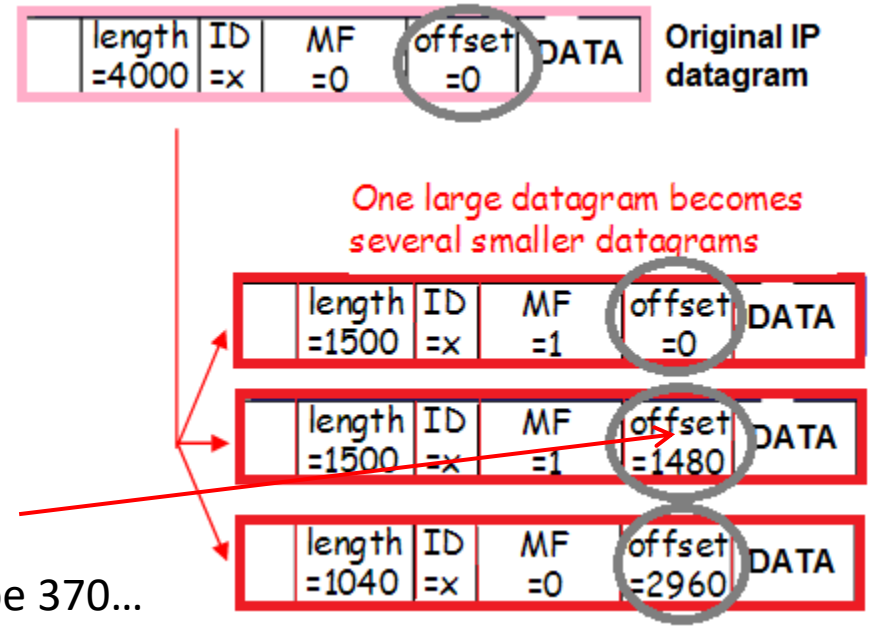
Flag:

- has three bits: one unused bit (always 0), one “don’t fragment”(DF) bit, and one “more fragment”(MF) bit.
- DF bit is 1, it forces the router not to fragment the packet.
- DF bit is 1---packet length > *maximum transmission unit* (*MTU*) -- the router will have to discard the packet and send an error message to the source host.
- If there are more, the MF bit is set to 1; otherwise it is set to 0.
- whether the datagram is the last fragment, or there are more fragments.



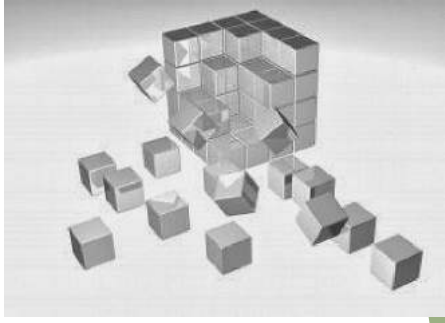
Fragmentation offset:

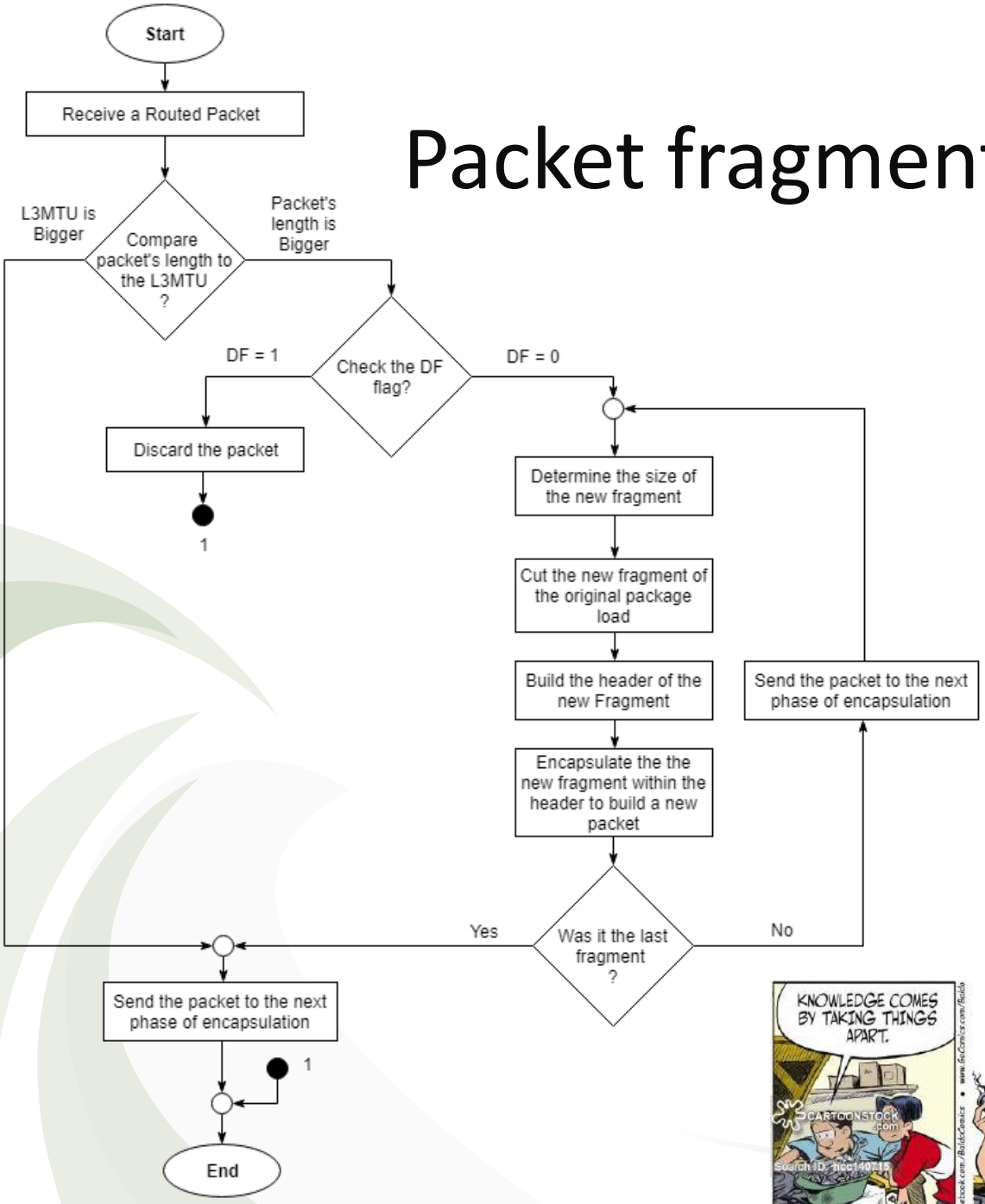
- datagram is fragmented,
- it is necessary to reassemble the fragments in the correct order.
- The fragment offset numbers the fragments in such a way that they can be reassembled correctly.
- fragment offset field is measured in units of eight-byte blocks.
- allows a maximum offset of $(2^{13} - 1) \times 8 = 65{,}528$ bytes, which would exceed the maximum IP packet length of 65,535 bytes with the header length included (65,528 + 20 = 65,548 bytes). [Seems odd? If header is 60?]



Actually this will be 1480/8=185, next will be 370…

Packet fragmentation





Fragmentation

- To fragment a long internet packet, a router creates a new IP packet
- copies the contents of the IP header fields from the long packet into the new IP header.
- The data of the long packet is divided into two portions on a 8 byte (64 bit) boundary so that the first packet is less than the MTU of the out-going interface.
- max size of each fragment is the MTU minus the IP header size (20 bytes minimum; 60 bytes maximum).
- The MF in the first packet is set to one (to indicate that more fragments of this packet follow).
- The MF may already be set in this packet if it has already been fragmented by another system. This packet is forwarded.
- Second packet header field is identical to that of the original packet. MF is 0 is it is the last one..

For example, for an MTU of 1,500 bytes and a header size of 20 bytes, the fragment offsets would be multiples of (1500–20)/8 = 185. These multiples are 0, 185, 370, 555, 740, ..

Answer…

- a packet of 4,520 bytes, including the 20 bytes of the IP header (without options) is fragmented to two packets on a link with an MTU of 2,500 bytes. What will be the Flag and fragmentation offset?

Fragment	Total bytes	Header bytes	Data bytes	"More fragments" flag	Fragment offset (8-byte blocks)
1	2500	20	2480	1	0
2	2040	20	2020	0	310

Let this fragmented datagram again encountered with a link with an MTU of 1,500 bytes. What will be the Flag and fragmentation offset?

Fragment	Total bytes	Header bytes	Data bytes	"More fragments" flag	Fragment offset (8-byte blocks)
1	1500	20	1480	1	0
2	1020	20	1000	1	185
3	1500	20	1480	1	310
4	560	20	540	0	495

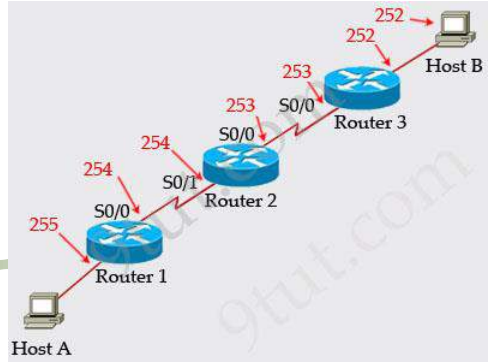
IP Datagrams

Time to live:

- A datagram has a limited lifetime in its travel through an internet.
- originally designed to hold a timestamp, which was decremented by each visited router.

- datagram discarded when the value became zero.
- now all the machines must have synchronized clocks .
- Today, this field is used mostly to control the maximum number of hops (routers) visited
- When a source host sends the datagram, it stores a number in this field.
- value is approximately 2 times the maximum number of routes between any two hosts.
- Each router that processes the datagram decrements this number by 1.
- after being decremented, is zero, the router discards the datagram.
- may travel between two or more routers for a long time without ever getting delivered to the destination host. This field limits the lifetime of a datagram.

[Avoids congestion]



IP Datagram

Protocol:

- 8-bit field defines the higher-level protocol that uses the services of the IPv4 layer.
- IPv4 datagram can encapsulate data from several higher-level protocols such as TCP, UDP, ICMP, and IGMP.
- This field specifies the final destination protocol to which the IPv4 datagram is delivered.
- value of this field helps the receiving network layer know to which protocol the data belong
- When a router receives a packet destined for itself, it examines this Protocol field to learn how to interpret data which are encapsulated in the IP packet.
- Maintains by Internet Assigned Numbers Authority (IANA).

Value (Hexadecimal)	Value (Decimal)	Protocol / Extension Header
00	0	Hop-By-Hop Options Extension Header (note that this value was "Reserved" in IPv4)
01	1	ICMPv4
02	2	IGMPv4
04	4	IP in IP Encapsulation
06	6	TCP
08	8	EGP
11	17	UDP
29	41	IPv6
2B	43	Routing Extension Header
2C	44	Fragmentation Extension Header
2E	46	Resource Reservation Protocol (RSVP)
32	50	Encrypted Security Payload (ESP) Extension Header
33	51	Authentication Header (AH) Extension Header
3A	58	ICMPv6
3B	59	No Next Header
3C	60	Destination Options Extension Header

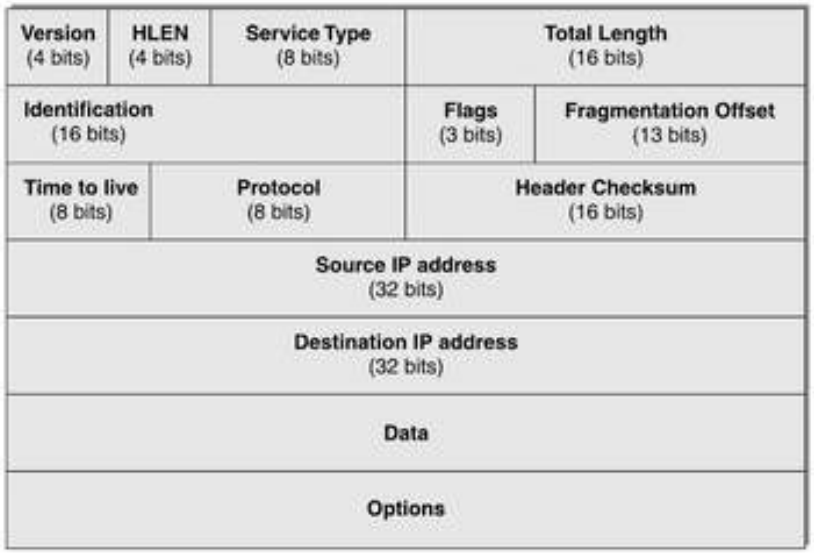
Checksum:

- to protect the header of IPv4 data packets against data corruption.
- has to be calculated on each hop(router) and if it does not matches then packet has to be discarded.
- First, the value of the checksum field is set to 0.
- Then the entire header is divided into 16-bit sections and added together.
- The result (sum) is complemented and inserted into the checksum field.
- The checksum in the IPv4 packet covers only the header, not the data.

Checksum calculation

I. 16 bit block formation:

- version(4), Header length(20) ToS(0) [all default] is a one block of 16 bit fields ---- hex turns to 4500.
- Total length and Identification are two 16 bit field
- Flags(001) and fragment offset(2560) make another 16 bit field---2140 in hex.
- In the same way all the fields are arranged to make blocks of 16 bits each. Hence complete IP packet header can be represented as(hex):
- **4500 0514 42A2 2140 8001 50B2**(Header Checksum) C0A8 0003 C0A8 0001



II. Calculating Checksum

- First calculate the sum of each 16 bit value within the header, skipping only the checksum field itself. [Taking it zero]

- 4500+0514+42A2+2140+8001+0000+C0A8+0003+C0A8+0001 = 2AF4B

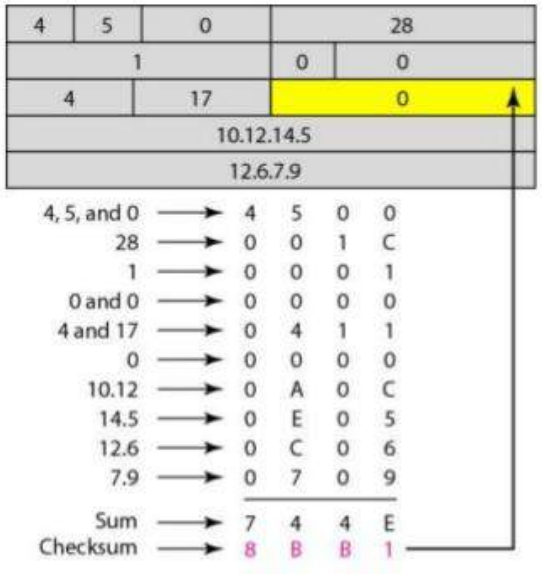
- Calculating further, adding carrys: 2+AF4B = AF4D

- Converted it to binary AF4D = 1010111101001101

- Compute one's complement. = 0101000010110010

- represented in hex 50B2

Example of checksum calculation in IPv4

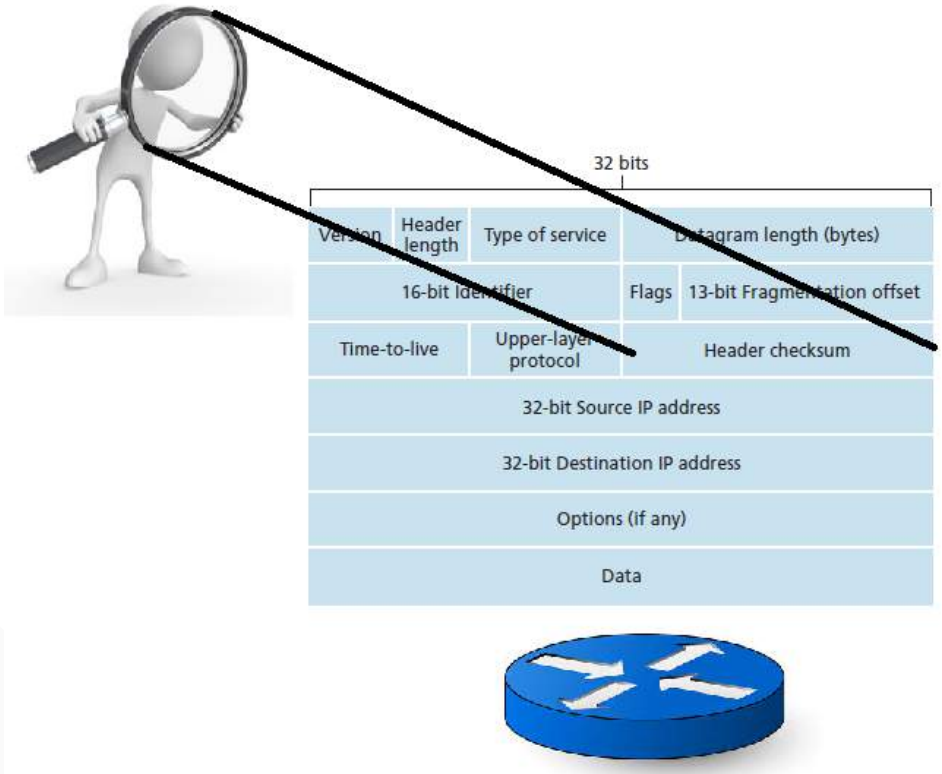


- **The packet**
- 4500 0514 42A2 2140 8001 **50B2**(Header Checksum) C0A8 0003 C0A8 0001

----------**Checksum in IP covers only the header, not the data.**

III. Checksum calculation at receiver

- Add all the 16 bit fields including the checksum:
- 4500+0514+42A2+2140+8001+50B2+C0A8+0003+CoA8+0001 = 2FFFD
- Calculating further, adding carry: 2+FFFD = FFFF which is
- all ones hence the header checksum is correct.



IP Datagrams

Source and destination address: Required*

Options:

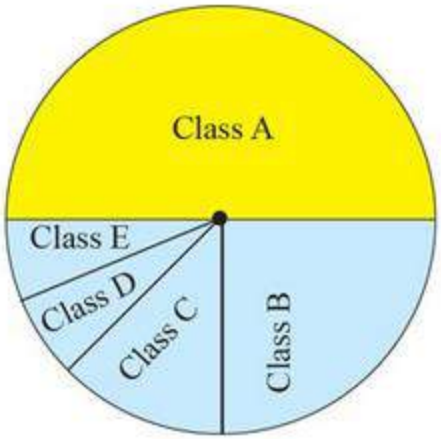
- made of two parts: a fixed part and a variable part.
- The fixed part is 20 bytes long and the variable part comprises the options that can be a maximum of 40 bytes.
- Options, as the name implies, are not required for a datagram.
- They can be used for network testing and debugging.
- contains routing details, timing, management

this may be changed in transit by a network address translation device.

IP Address—Classful and Classless

- Started with the concept of classful
- From mid 90 new architecture proposed---classless

Classful: 5 classes



Class A: 2^{31} = 2,147,483,648 addresses, 50%

Class B: 2^{30} = 1,073,741,824 addresses, 25%

Class C: 2^{29} = 536,870,912 addresses, 12.5%

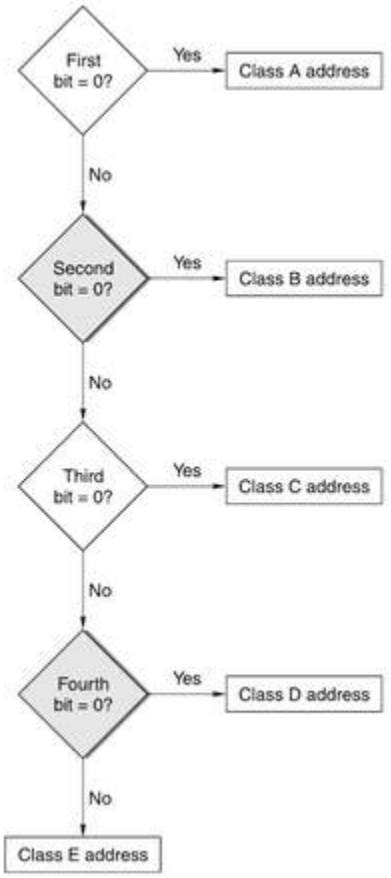
Class D: 2^{28} = 268,435,456 addresses, 6.25%

Class E: 2^{28} = 268,435,456 addresses, 6.25%

IP address

Class	Address Range
Class A	1.0.0.1 to 126.255.255.254
Class B	128.1.0.1 to 191.255.255.254
Class C	192.0.1.1 to 223.255.254.254
Class D	224.0.0.0 to 239.255.255.255
Class E	240.0.0.0 to 254.255.255.254

Class	*Number of Addresses*	*Percentage of address space*
A	20 Lakh	50%
B	10 Lakh	25%
C	5 Lakh	12.5%
D	2.5 Lakh	6.25%
E	2.5 Lakh	6.25%



Who issue?

Who issues IP address?

- Internet assigned number authority (ISNA) issues the prefix or network portion and give it to Internet service provider. Organization approaches to ISP.

- Wholesaler →retailer → customer !!!

Fragmentation

- Each protocol has a specific frame format.---Maximum data field.
- MTU differs from one physical network protocol to another.
- Fragmentation is required

- A fragmented datagram may need to be fragmented again.
- When a datagram is fragmented, required parts of the header must be copied by all fragments.
- The host or router that fragments a datagram must change the values of three fields:

  flags, fragmentation offset, and total length.

The rest of the fields must be copied. Only the value of the checksum must be recalculated regardless of fragmentation.

Fields related to fragmentation

Identification:

If a datagram is fragmented a counter is initialized to a positive number.

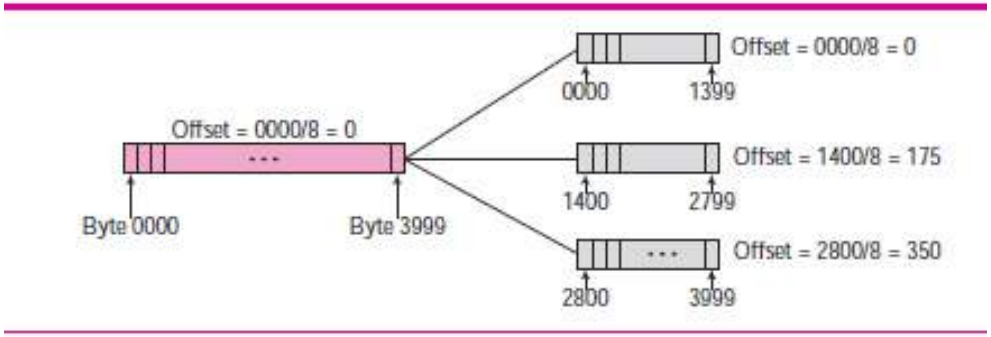
- When IP sends the datagram it copies the current value of the counter in the identification field.
- Increase counter by one---For next datagram.
- When datagram is fragmented the value of identification is copied to all fragments.
- Helps the destination to reassemble.

Only data in a datagram is fragmented

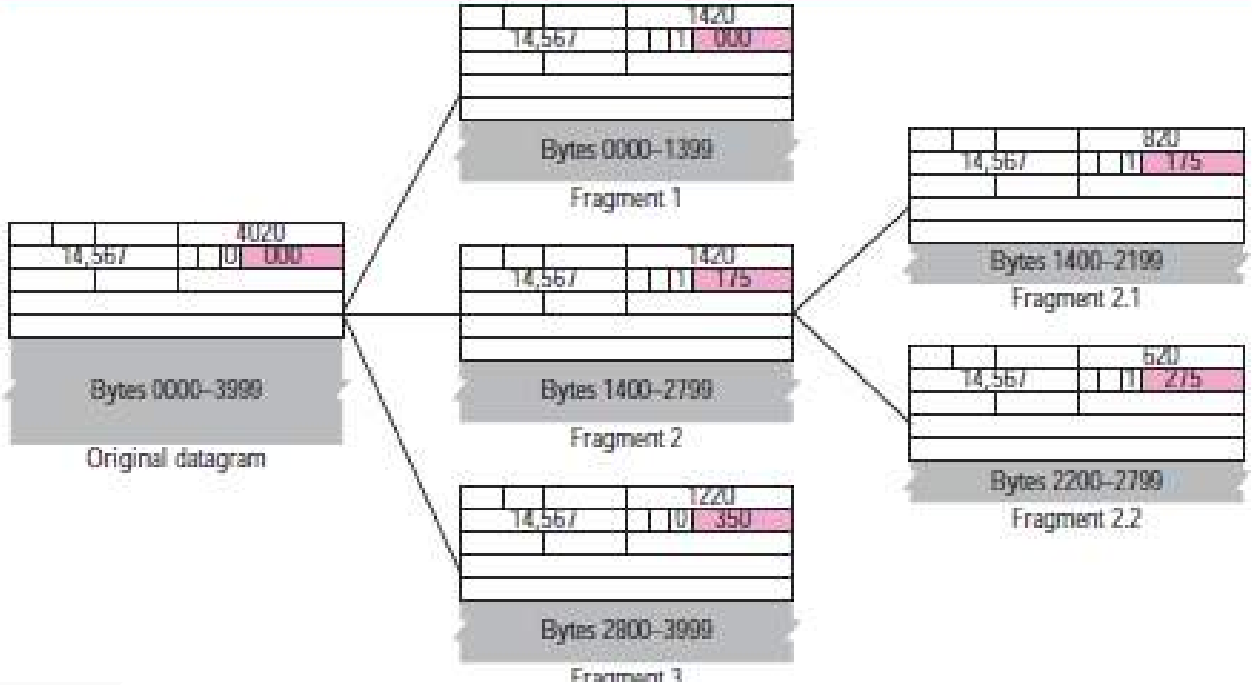
- **Flag: Second bit 1: Do not fragment**
  Third bit 1: More fragment

- If it cannot pass the datagram through any available physical network, it discards the datagram and sends an ICMP error message to the source host
- last bit is 1, it means the datagram is not the last fragment; there are more fragments after this one.
- If its value is 0, it means this is the last or only fragment

- **Fragmentation offset:** shows the relative position of this fragment with respect to the whole datagram.
- It is the offset of the data in the original datagram measured in units of 8 bytes.



- Data size of 4000 bytes fragmented into three fragments.
- bytes in the original datagram are numbered 0 to 3999. The first fragment carries bytes 0 to 1399. The offset for this datagram is 0/8=0
- The second fragment carries bytes 1400 to 2799;→offset value 1400/8= 175.
- Third fragment carries bytes 2800 to 3999. → offset value 2800/8= 350.
- length of the offset field 13 bits →cannot represent a sequence of bytes greater than 8191.
- forces hosts or routers that fragment datagrams to choose the size of each fragment so that the first byte number is divisible by 8.


4020
14,567
0
000
Bytes 0000–3999
Original datagram
1420
14,567
1
000
Bytes 0000–1399
Fragment 1
1420
14,567
1
175
Bytes 1400–2799
Fragment 2
1220
14,567
0
350
Bytes 2800–3999
820
14,567
1
175
Bytes 1400–2199
Fragment 2.1
620
14,567
1
275
Bytes 2200–2799
Fragment 2.2

Questions

Q. A packet has arrived with an *M bit value of 1 and a fragmentation offset value of zero. Is this the* first fragment, the last fragment, or a middle fragment?

Because the *M bit is 1, it is either the first fragment or a middle one. Because the offset value is 0,* it is the first fragment.

Q. A packet has arrived in which the offset value is 100. What is the number of the first byte? Do we know the number of the last byte?

Multiply the offset value by 8. This means that the first byte number is 801.(800 is already been sent.) We cannot determine the number of the last byte unless we know the length of the data.

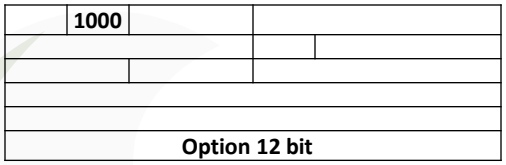
Q. A packet has arrived in which the offset value is 100, the value of HLEN is 5 and the value of the total length field is 1000. What is the number of the first byte and the last byte?

Question

- An IP packet has arrived with the first 8 bits as shown: 01000010. The receiver discards the packet. Why?

Error in this packet. The 4 left-most bits (0100) show the version, which is correct. The next 4 bits (0010) show the wrong header length (2 × 4= 8). The minimum number of bytes in the header must be 20. The packet has been corrupted in transmission.

Q. In an IP packet, the value of HLEN is 1000 in binary. How many bytes of options are being carried by this packet?



Total number of bytes in the header is 8 × 4 or 32 bytes.
The first 20 bytes are the base header, the next 12 bytes are the options.

Q. In an IP packet, the value of HLEN is 5_{16} and the value of the total length field is 0028_{16}. How many bytes of data are being carried by this packet?

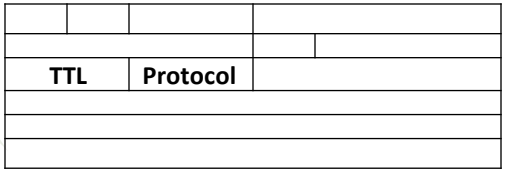
Length of data = total length-header length

Question

- An IP packet has arrived with the first few hexadecimal digits as shown below:

4500002800010000102 . . .

How many hops can this packet travel before being dropped? The data belong to what upper layer protocol?



Value	*Protocol*	*Value*	*Protocol*
1	ICMP	17	UDP
2	IGMP	89	OSPF
6	TCP		

Discard 16 hexadecimal digit
4500002800010000**01**02 . . .

Only one hop.

02 means IGMP (Internet Group Management **Protocol**)

GATE

- In an IPv4 datagram, the M bit is 0, the value of HLEN is 10 (decimal), the value of total length is 400 and the fragment offset value is 300. The position of the datagram, the sequence numbers of the first and the last bytes of the payload, respectively are
  (A) Last fragment, 2400 and 2789
  (B) First fragment, 2400 and 2759
  (C) Last fragment, 2400 and 2759
  (D) Middle fragment, 300 and 689

M = 0 indicates that this packet is the last packet among all fragments of original packet.
So the answer is either A or C.
It is given that HLEN field is 10. Header length is number of 32 bit words. So header length = 10 * 4 = 40
Also, given that total length = 400.
Total length indicates total length of the packet including header.
So, packet length excluding header = 400 – 40 = 360
Last byte address = 2400 + 360 – 1 = 2759 (Because numbering starts from 0)
(C)

GATE

- An IP router with a Maximum Transmission Unit (MTU) of 1500 bytes has received an IP packet of size 4404 bytes with an IP header of length 20 bytes. The values of the relevant fields in the header of the third IP fragment generated by the router for this packet are

(A)MF bit: 0, Datagram Length: 1444; Offset: 370

(B) MF bit: 1, Datagram Length: 1424; Offset: 185

(C) MF bit: 1, Datagram Length: 1500; Offset: 37

(D) MF bit: 0, Datagram Length: 1424; Offset: 2960

Number of packet fragments = [(total size of packet)/(MTU)]
= [4404/1500]
= [2.936]
= 3

So Datagram with data 4404 byte fragmented into 3 fragments.

The first frame carries bytes 0 to 1479 (because MTU is 1500 bytes and HLEN is 20 byte so the total bytes in fragments is maximum 1500-20=1480). the offset for this datagram is 0/8 = 0.

The second fragment carries byte 1480 to 2959. The offset for this datagram is 1480/8 = 185.finally the third fragment carries byte 2960 to 4404.the offset is 370.and for all fragments except last one the M bit is 1.so in the third bit M is 0..

- An IP datagram of size 1000 bytes arrives at a router. The router has to forward this packet on a link whose MTU (maximum transmission unit) is 100 bytes. Assume that the size of the IP header is 20 bytes. The number of fragments that the IP datagram will be divided into for transmission is :

  (A) 10
  (B) 50
  (C) 12
  (D) 13

  Explanation: MTU = 100 bytes
  Size of IP header = 20 bytes
  So, size of data that can be transmitted in one fragment = 100 – 20 = 80 bytes
  Size of data to be transmitted = Size of datagram – size of header = 1000 – 20 = 980 bytes

  Now, we have a datagram of size 1000 bytes.
  So, we need ceil(980/80) = 13 fragments.

  Thus, there will be 13 fragments of the datagram.

- Consider an IP packet with a length of 4,500 bytes that includes a 20-byte IPv4 header ans 40-byte TCP header. The packet is forwarded to an IPv4 router that supports a Maximum Transmission Unit (MTU) of 600 bytes. Assume that the length of the IP header in all the outgoing fragments of this packet is 20 bytes. Assume that the fragmentation offset value stored in the first fragment is 0.

The fragmentation offset value stored in the third fragment is _____ .

Explanation: MTU = 600 bytes and IP Header = 20 bytes
So, Payload will be 600 – 20 = 580 bytes
580 is not multiple of 8, but we know fragment size should be multiple of 8. So fragment size = **576 bytes**
K^{th} fragmentation offset value = Fragment Size * (K^{th} fragment – 1) / Scaling Factor
Offset value of 3^{rd} fragment = 576 * (3 – 1) / 8 = **144**

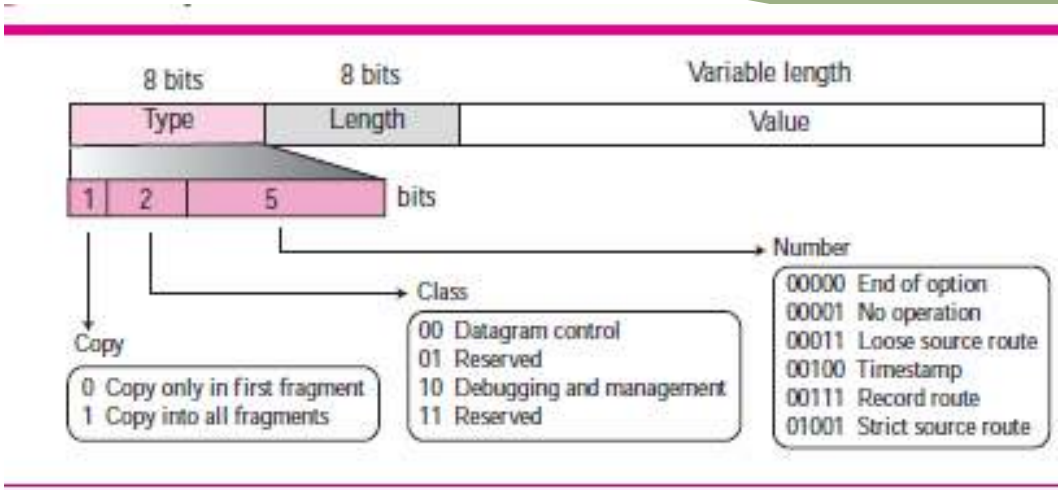
Option

- Header has two parts: fixed part and variable part.
- Fixed part is 20 bytes long.
- The variable part comprises the options, which can be a maximum of 40 bytes.

  (15*4=60-20=40)
- The name implies, OPTION not required for a datagram.
- Used for network testing and debugging.
- Although options are not a required part of the IP header, option processing is required of the IP software.
- This means that all implementations must be able to handle options if they are present in the header.

Format of OPTION

Type: 8 bits long and contains three subfields: copy, class, and number.



Copy:

- 1-bit subfield controls the presence of the option in fragmentation.
- value is 0, ---option must be copied only to the first fragment.
- value is 1--- option must be copied to all fragments

Class:

2-bit subfield defines the general purpose of the option.

00→ used for datagram control.

10 → used for debugging and management.

01 and 11 → Reserved

Number

5-bit subfield defines the **type of option**.

currently only 6 types are in use.

Format of Option

Length

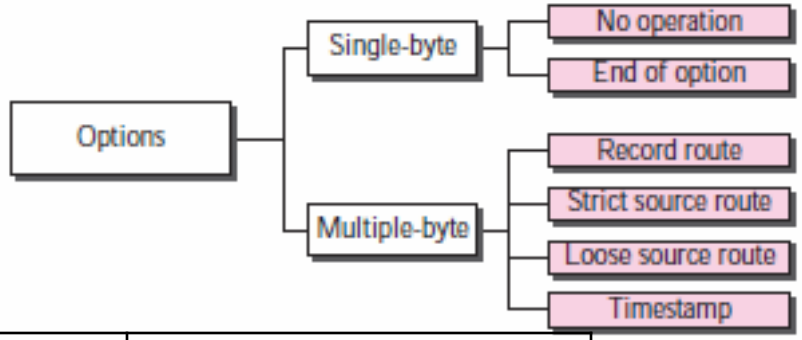
- Defines the total length of the option including the type field and the length field itself.
- This field is not present in all of the option types.

Value

- Contains the data that specific options require.
- This field is also not present in all option types.

Option type (5 bit number field)

- options are currently being used.
- Two of these are 1-byte options, and they do not require the length or the data fields.
- Four of them are multiple-byte options; they require the length and the data fields.

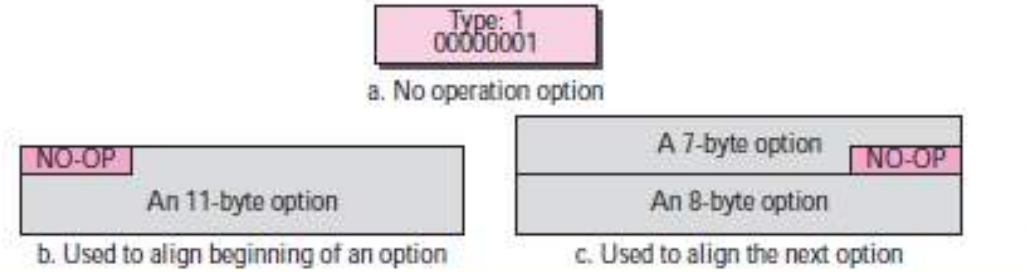


Value	Type
00001	No option
00000	End of option
00111	Record route
01001	Strict source to route
00011	Loose source route
00100	Time stamp

No-Operation Option:

➢1-byte option used as a filler between options.

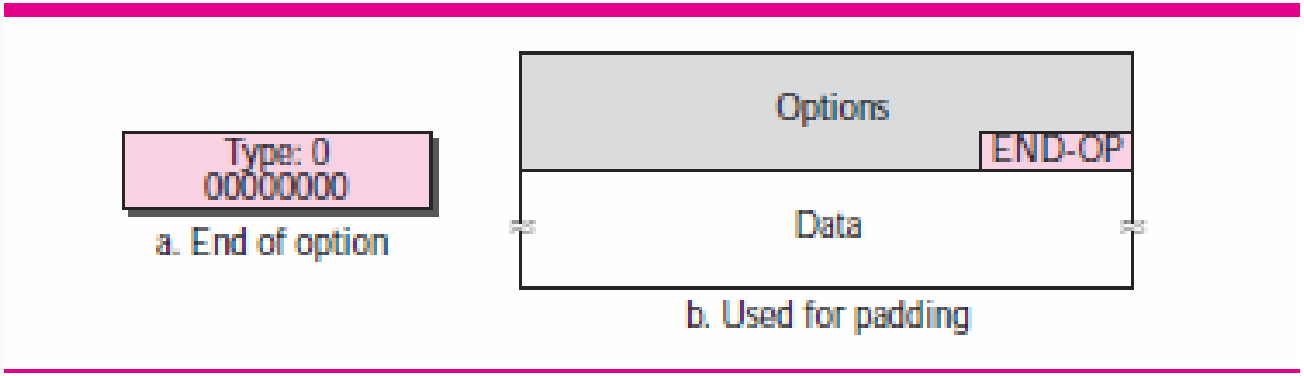
➢used as "internal padding" to align certain options on a 16 or 32-bit boundary when required.



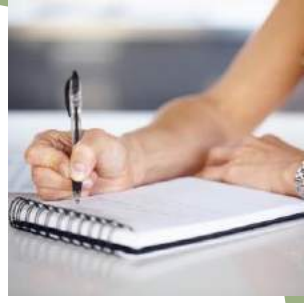
Option type (5 bit number field)

End of option:

- used for padding at the end of the option field.
- It, however, can only be used as the last option.
- Only one end-of-option option can be used.
- After this option, the receiver looks for the payload data
- if more than 1 byte is needed to align the option field, some no-operation options must be used, followed by an end-of-option option

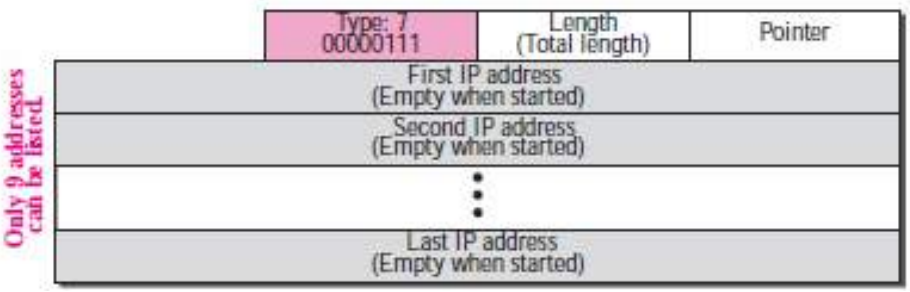


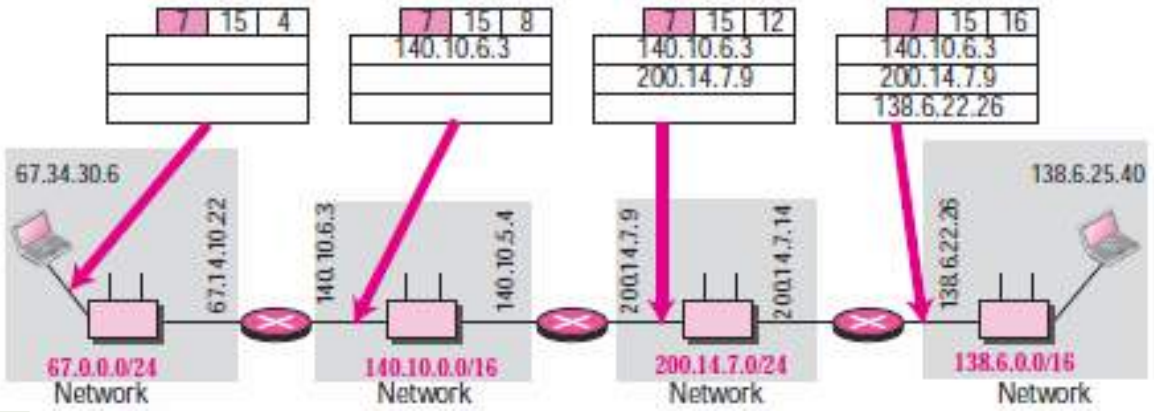
Option type (5 bit number field)



Record-Route Option*: record the routers that handle the datagram*

- Used to record the Internet routers that handle the datagram.
- Can list up to nine router IP addresses. [In header 15 * 4 =60 . Option is max 40 byte. IP 9 * 4=36 + 3 (Type, length and pointer)].
- Source creates placeholder fields in the option to be filled by the visited routers.
- **pointer field (1 byte)→**offset integer field containing the byte number of the first empty entry. In other words, it points to the first available entry.
- Datagram from source, all of the fields are empty. Pointer field has a value of 4, pointing to the first empty field.
- passing a router that processes the datagram finds the value of the pointer with the value of the length. If pointer value >value of the length, the option is full and no changes are made.
- If not router adds the IP address of its interface from which the datagram is leaving.
- Increase the pointer value by 4.




7 15 4
7 15 8
140.10.6.3
7 15 12
140.10.6.3
200.14.7.9
7 15 16
140.10.6.3
200.14.7.9
138.6.22.26
67.34.30.6
67.14.10.22
140.10.6.3
140.10.5.4
200.14.7.9
200.14.7.14
138.6.22.26
138.6.25.40
67.0.0.0/24
Network
140.10.0.0/16
Network
200.14.7.0/24
Network
138.6.0.0/16
Network

Option type (5 bit number field)

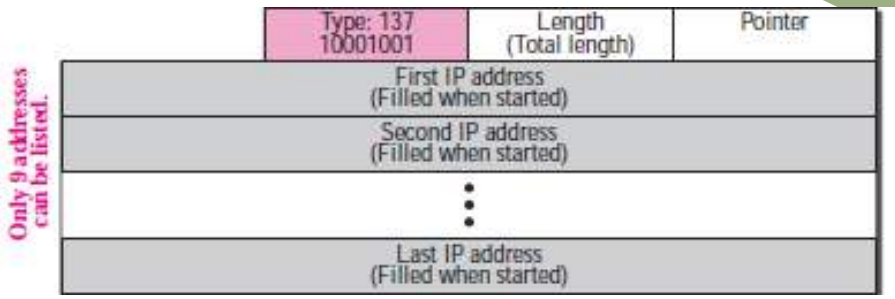
Strict-Source-Route Option:

- Used by the source to predetermine a route for the datagram as it travels through the Internet.
- **Advantages:**

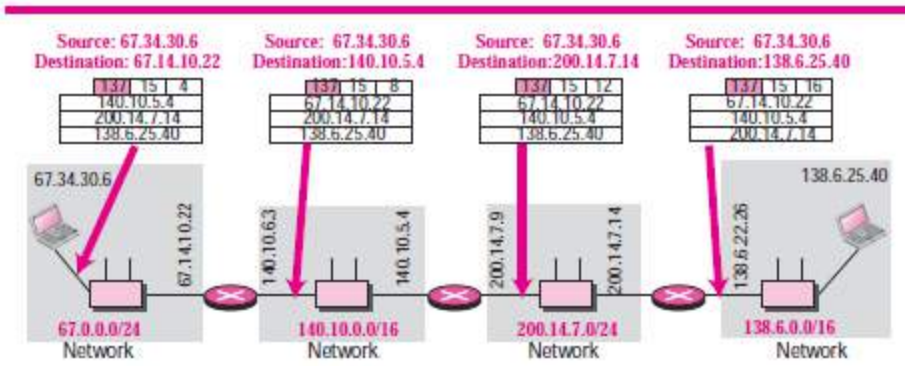
➢ For specific type of service →minimum delay or maximum throughput.

➢ May choose a route that is safer or more reliable. for the sender's purpose. [For example, a sender can choose a route so that its datagram does not travel through a competitor's network.]

- all of the routers defined in the option must be visited by the datagram.
- A router must not be visited if its IP address is not listed. If the it visits a router not listed→ the datagram is discarded and an error message is issued.
- If the datagram arrives at the destination and some of the entries were not visited, it will also be discarded and an error message issued. ----Problem
- General users, however, are not usually aware of the physical topology of the Internet. Thus strict source routing is not the choice of most users.
- Similar to record route, but the entry are done by sender



- router that processes the datagram compares value of the pointer with the value of the length.
- If the value of the pointer > value of the length, the datagram has visited all of the predefined routers. →cannot travel anymore →discarded and an error message is created
- If not router compares the destination IP address with its incoming IP address: If they are equal, → process the datagram→ swaps the IP address pointed by the pointer with the destination address→increments the pointer by 4 → forwards the datagram. If they are not equal, it discards the datagram and issues an error message.



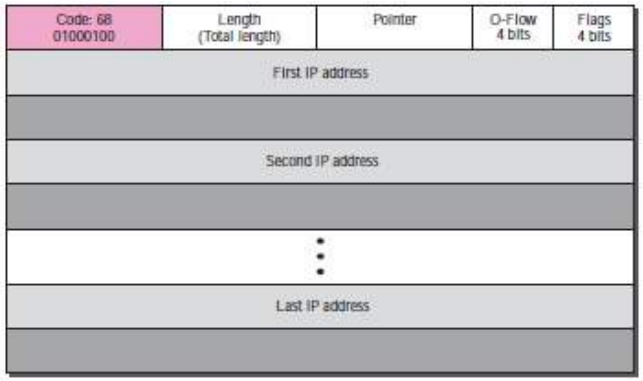
Option type (5 bit number field)

Loose-Source-Route Option:

- Similar to the strict source route, but more relaxed.
- Each router in the list must be visited, but the datagram can visit other routers as well.

Time stamp:

- Used to record the time of datagram processing by a router.
- Time is expressed in milliseconds from midnight, universal time.
- All routers may use Universal Time (**Network time protocol**), their local clocks may not be synchronized.
- Time stamp help users and managers track the behavior of the routers in the Internet.
- Timestamp option is not a choice for most users. [Not aware of physical topology]



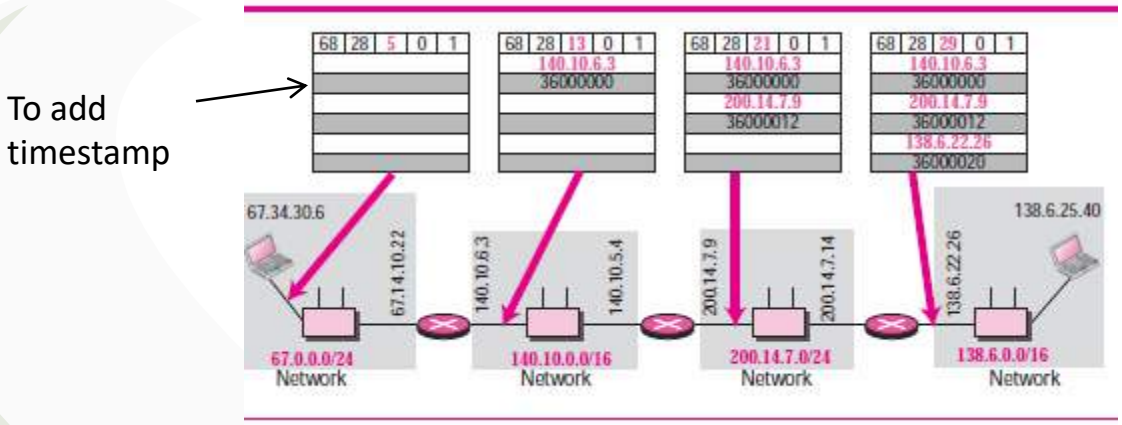
Option type (5 bit number field)

- Overflow field records the number of routers that could not add their timestamp. (because no more fields were available.)
- The flags field specifies the visited router responsibilities.

  0 → each router adds only the timestamp in the provided field.

  1 → each router add its outgoing IP address and the timestamp.

  3 → IP addresses are given, and each router check the given IP address with its own incoming IP address. If match, the router overwrites the IP address with its outgoing IP address and adds the timestamp.



Question

- For a datagram HLEN field is 1001 in binary. Type bit is 111. How many IP address it can record?

  9*4=36-20=16 (Option field)

  16-3=13 byte is left to record IP. Max 3.

- For a datagram HLEN is 1011 in binary. Option type is 137. Pointer value after released by a router is 20. Whether it will be accepted by the next router?

  11*4=44-20=24
  24-3=21 left to record IP
  Entry of 5 IP addresses. Pointer is initialized by 4 when released by source.
  Maximum possible value is 4+20=24.
  20 means will be accept.

Question

- Value of HLEN is 1110. Option type value is 137. Pointer value 36 or 40 , which is possible?

  56-20=36-3=33
  33/4=8
  Pointer value max = 4+32=36.

- Value of HLEN is 1110. Option type value is 68.
  How may entries will be there if Flag value of option is a) 0 b) 1 c) 3

  56-20=36-4 (one extra byte for overflow+flag)=32 byte

  a) 0 only timestamp so 8
  b) 1 IP+ timestamp so 4
  c) 3 same as b

Checksum

- Error detection method used by most TCP/IP protocols
- Protects against the corruption that may occur during the transmission of a packet.
- Redundant information added to the packet.
- Calculated at the sender and the value is sent with the packet.
- Receiver recalculates on the whole packet including the checksum. If satisfactory the packet is accepted; otherwise, rejected.

a. Checksum calculation at sender

b. Checksum calculation at receiver

Checksum in IP covers only the header, not the data.

Checksum calculation at sender and receiver

Sender:

- The packet is divided into *k sections, each of n bits. [Generally n=16]*
- All sections are added together using one's complement arithmetic.
- The final result is complemented to make the checksum.

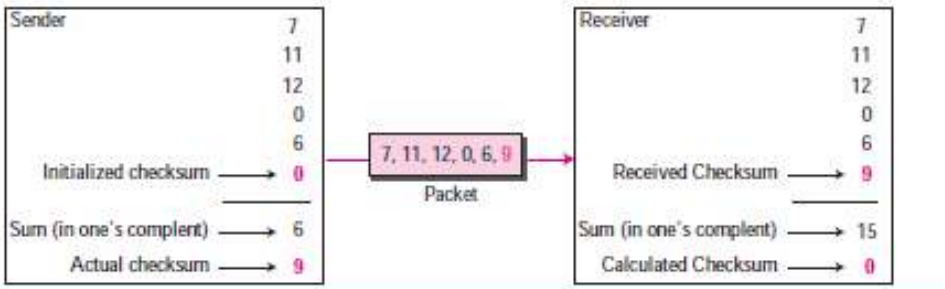
Receiver:

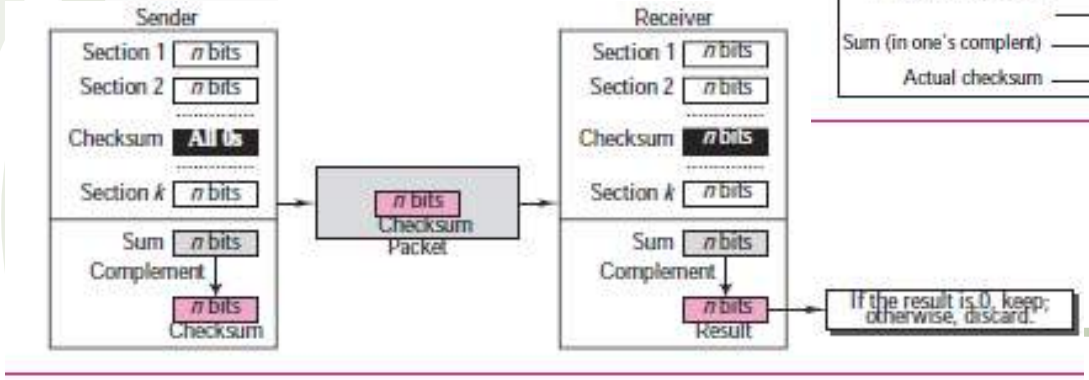
- packet is divided into k sections and all sections are added.
- The result is complemented.
- Final result is 0 ? Yes → Accepted; Else → Rejected.

$7+11+12+0+6=36=(100100)_2$

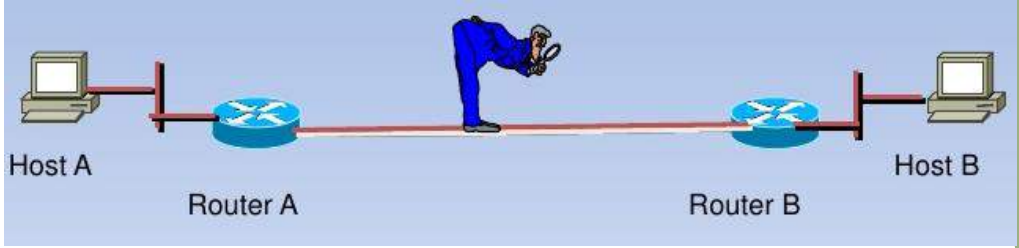
$(10)_2 + (0100)_2 = (0110)_2 = (6)_2$

15-6=9 (actual checksum)





Security



- Earlier no security was provided for the IPv4 protocol. Internet runs on trust.
- Security issues particularly applicable to the IP protocol: **packet sniffing**, **packet modification**, and **IP spoofing**.

Packet Sniffing:

A passive attack. (Does not change the content of the packet)

An intruder may intercept an IP packet and make a copy of it.

- Very difficult to detect because the sender and the receiver may never know that the packet has been copied.
- Sniffing cannot be stopped. Solution → *Encryption*
- Sniffer cannot find its contents.

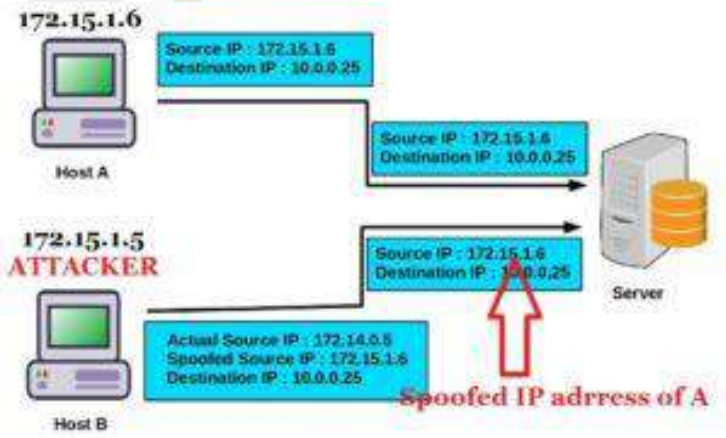
Packet Modification:

- Attacker intercepts the packet, changes its contents, and sends the new packet to the receiver.
- Receiver believes that the packet is coming from the original sender.
- Can be detected using a *data integrity mechanism.*

Security

IP Spoofing:

- technique used to gain unauthorized access to machines.
- an attacker illicitly impersonates another machine by manipulating IP packets.
- involves modifying the packet header with a forged (spoofed) source IP address, a checksum, and the order value.
- starts by identifying the host and finding the IP address trusted by the host so that user can send data packets and the host will see them as originating from a trusted IP address
- This type of attack can be prevented using an *origin authentication mechanism.*
- perform activities that are malicious and illegal. Like--Service denial and man in the middle attacks.



Properties of IP.

Unreliable: Does not provide any datagram will definitely reach to the destination. Best-effort delivery mechanism.

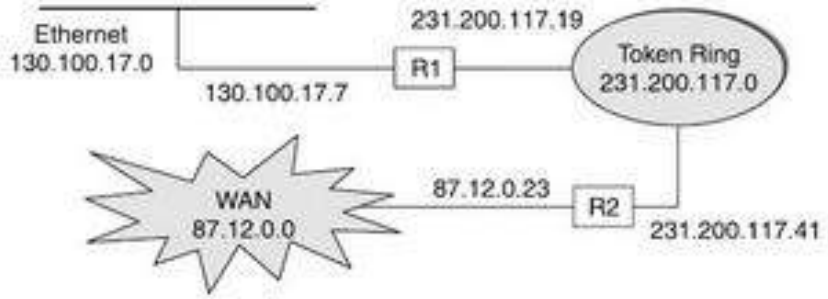
IP lets the reliability become the responsibility of the transport layer.

Connectionless: Each datagram send by IP is considered to be an independent.

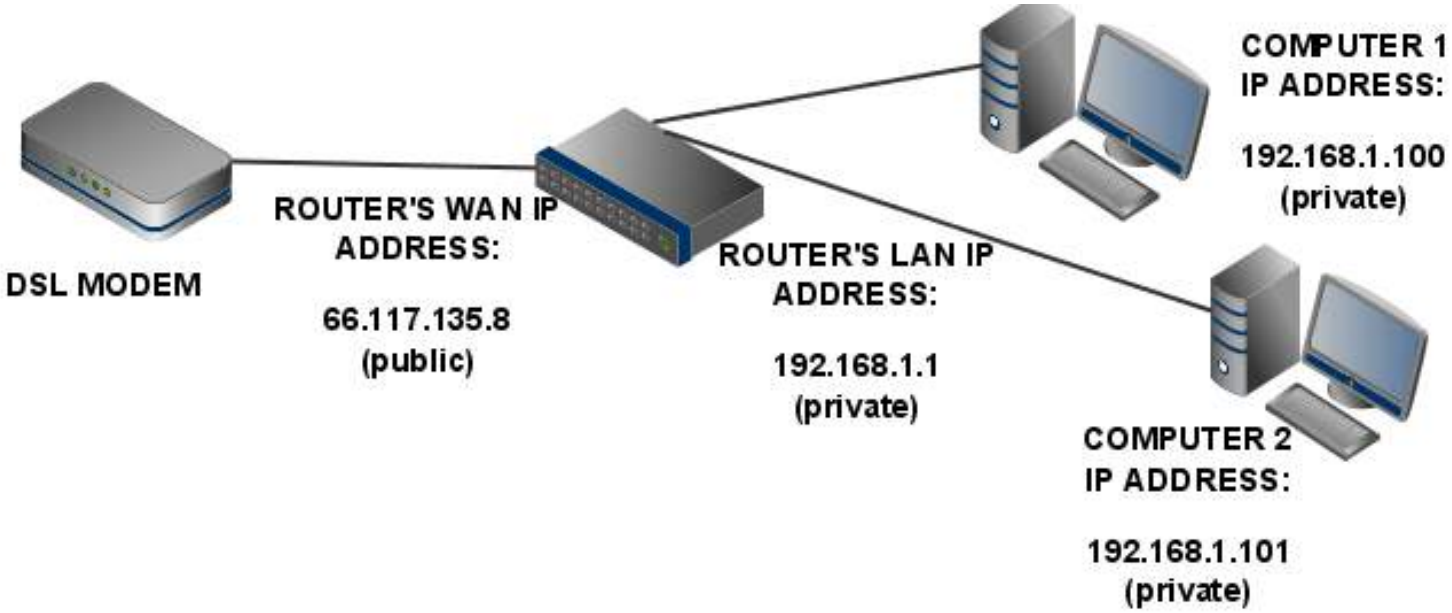
all packets in **IP** network are routed independently, they may not necessarily go through the same route, while in a virtual circuit network which is connection oriented, all packets go through the same route.

Router and IP address

- If a router connects networks it will have an IP addresses.



A router has two or more IP addresses

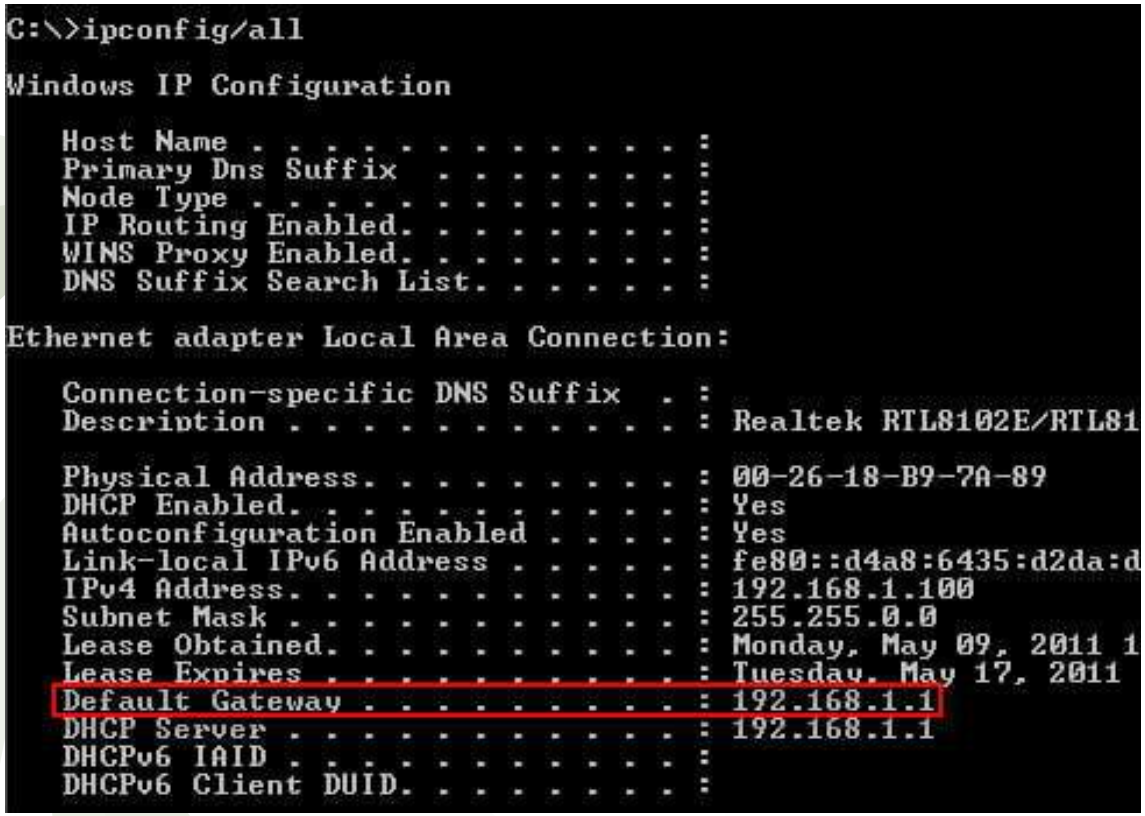


- Public IPs are used by routers and by computers connected directly to DSL modems without a router.
- Private IP addresses are special IP addresses that are known only to a router and its home network. is used to assign computers within your private space without letting them directly expose to the Internet.
- A Web server will not deliver Internet data to a private IP address. It will deliver the data to the router (which has a public IP address) and then the router will deliver the data to the computer that has the private IP address.

How to get the two IP addresses?

- Private IP

Type ipconfig.



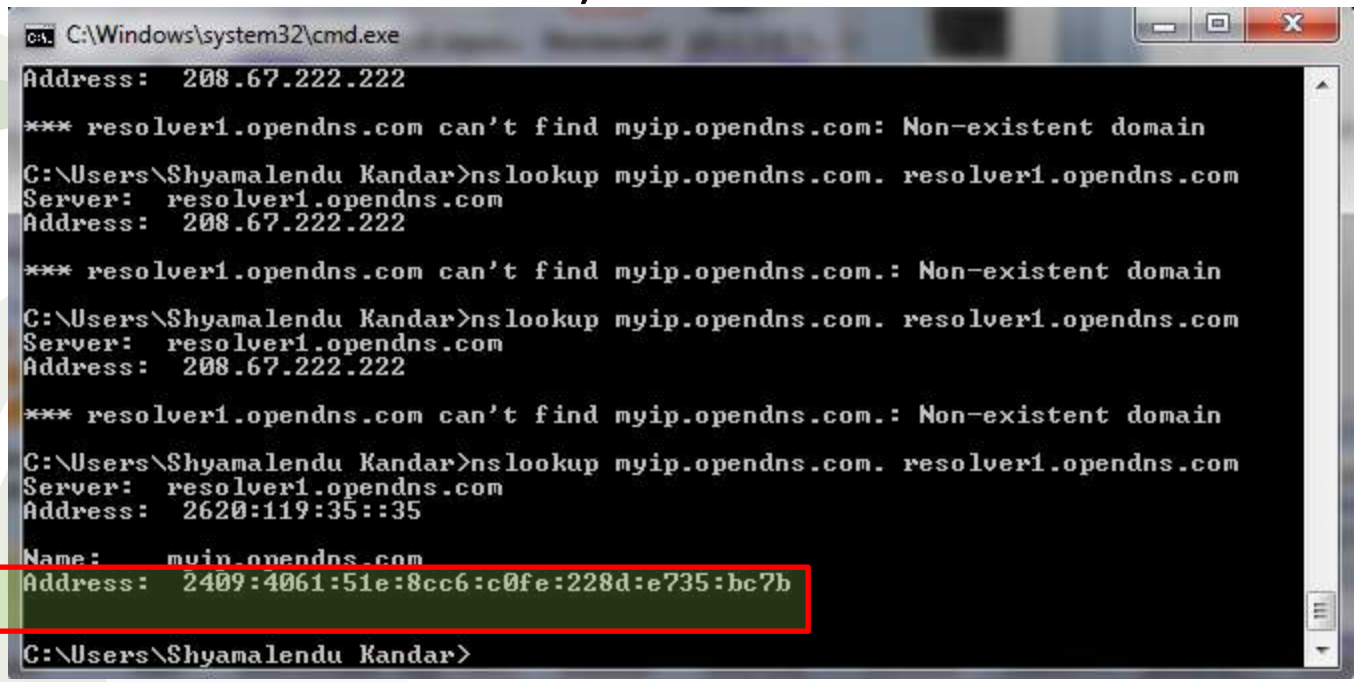
- Private IP

type ip4.me in the URL bar of the browser.

Or type in cmd prompt

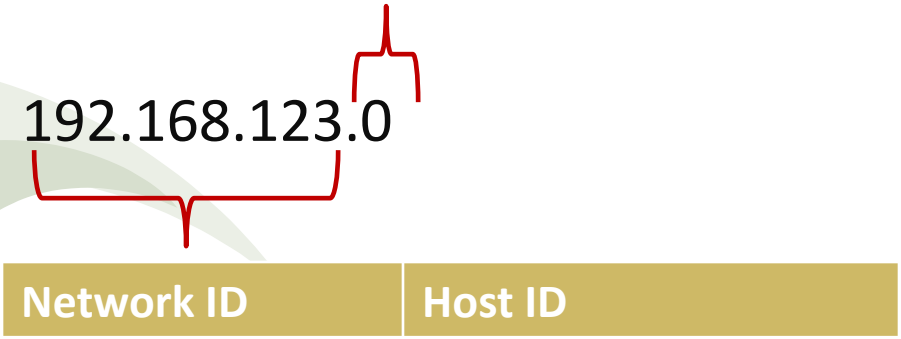
nslookup myip.opendns.com resolver1.opendns.com

(some ISP bans to enter)



Who decides IP?

- Internet assigned number authority (IANA) allocates IP prefix to ISP.
- ISP allocates host number and suffixes.



Subnet mask determines the network part and host part by the presence of consecutive ‘1’ s.

Subnetting

- breaking a large network into smaller networks by adding ones to the subnet mask.
- Host's formula: how many hosts will be allowed on a network that has a certain subnet mask.
- $2^h - 2$. h : number of zeros in the subnet mask converted to binary. (The first and last addresses are reserved. First: to identify the network and the last to be used as the broadcast address)
- Example: IP address space 192.168.0.0. Number of node is 100.
- Use 255.255.255.0 as subnet mask. ($2^8 – 2 = 254$) 254>100
- We would have 192.168.0.1 through 192.168.0.254 for your hosts. (2 addresses are reserved)
- Next year node become 300. Make subnet mask 255.255.254.0.($2^9 – 2$)
- Adding ones to the subnet mask means you get fewer hosts per network subnet but more network subnets. If you remove ones from the subnet mask, you get more hosts per network but fewer networks.

Subnetting

- Subnet formula : 2^S where S denotes number of ‘1’ added to the subnet mask.
- As we add subnet bits, the number of subnets increases by a factor of two, and the number of hosts per subnet decreases by a factor of two.

Classless Inter-Domain Routing (CIDR) representation: appends the number of subnet mask bits to the network address.

we append a forward slash (/) and the number of ‘1’ bits in the subnet mask.

192.168.0.1/23 means

IP : 192.168.0.1 Subnet mask: 255.255.254.0

Subnetting

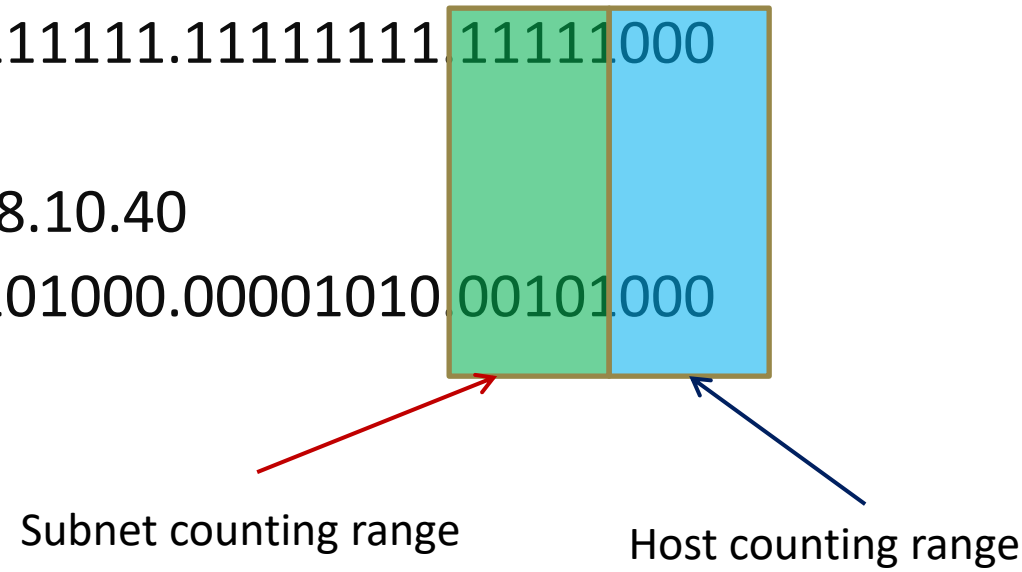
- IP address 192.168.10.44
- Subnet Mask 255.255.255.248

Binary 11111111.11111111.11111111.11111000

Bitwise AND

Subnet Address 192.168.10.40

Binary 11000000. 10101000.00001010.00101000



First address 192.168.10.41

Last Address 192.168.10.46

Broadcast 192.168.10.47

Next subnet 11000000. 10101000.00001010.00110000

192.168.10.48 Total no of Subnet 32

Number of nodes per subnet 6 (8-2)

Benefits of subnetting

- Improve network performance and speed.

  A single broadcast packet sends out information that reaches every device connected to that network because each device has an entry point into the network.
- Reduce network congestion.
- Boost network security.
- Control network growth.
- Ease administration.

Communication in Same network

Direct and indirect delivery

Source and destination are in same network.—Direct.

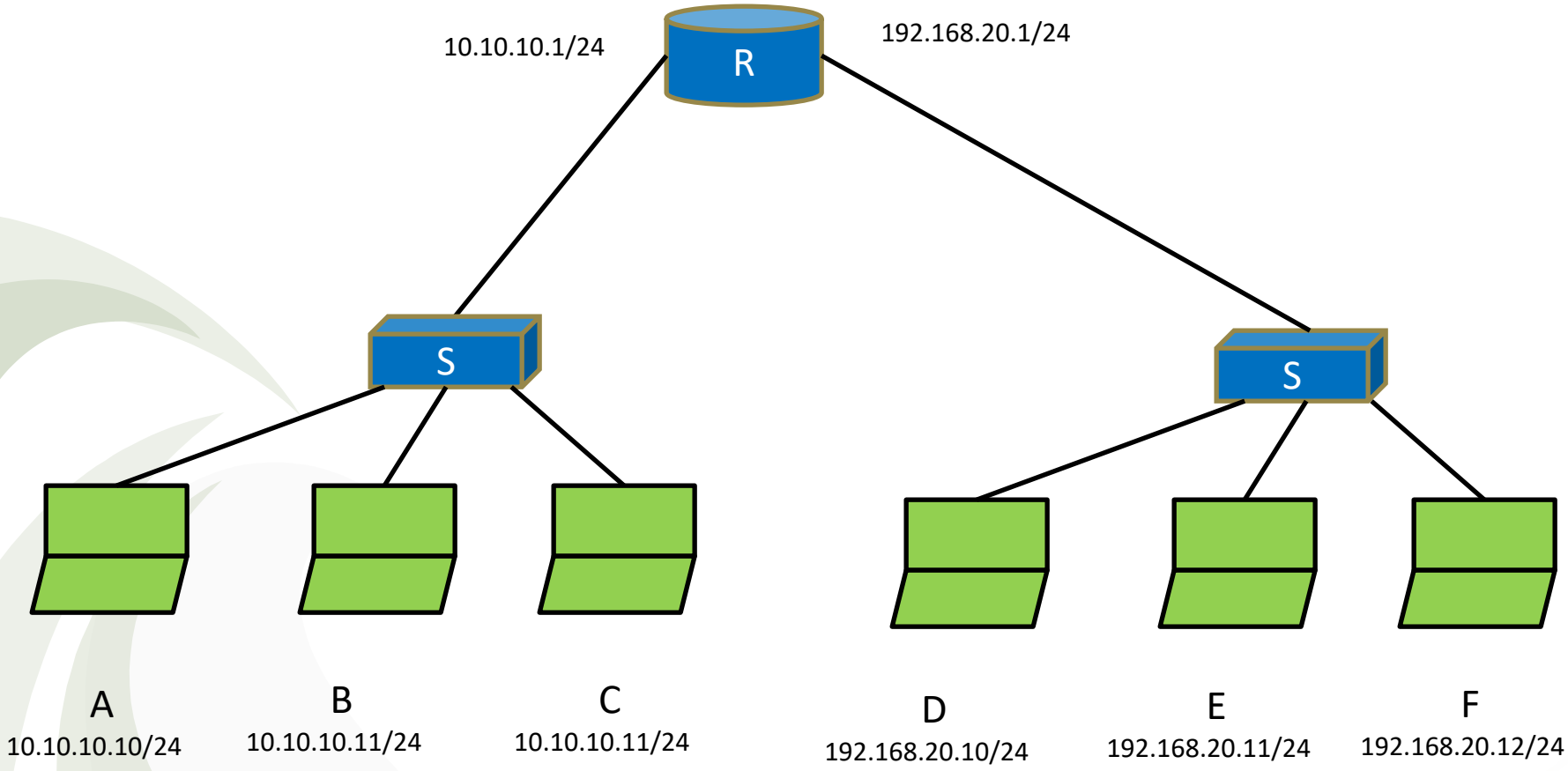
How to know?

AND operation is performed between source IP address , source subnet mask and destination IP address, source subnet mask. If the two results matches then both nodes resides in same n/w.

If does not matches –Indirect

Forward the packet to the router.

Communication in Same network

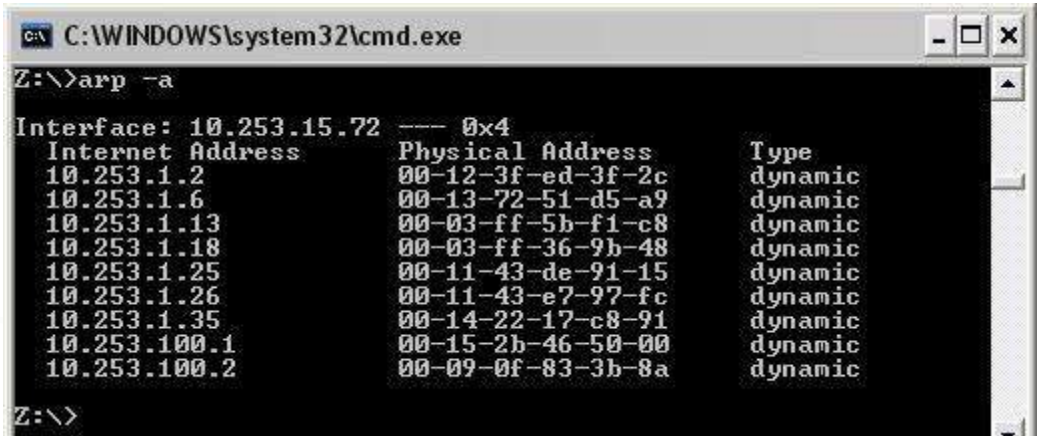


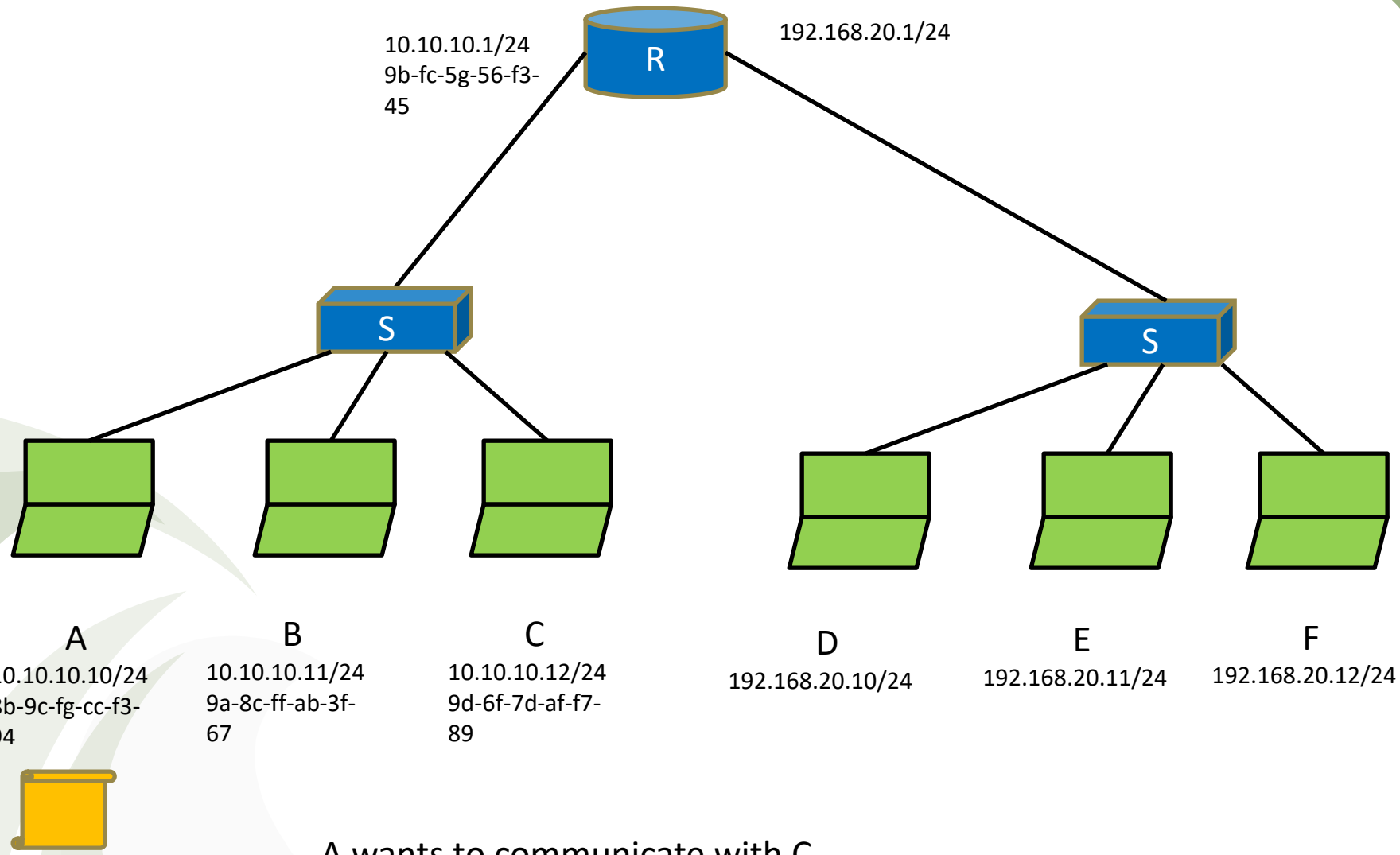
Communication in Same network

- Let node A wants to communicate with C
- Bitwise AND with IP of A with A's subnet mask and IP of C and A's subnet mask. The two results are same. Thus A and C are in same network.
- If A does not know the MAC address of C it broadcast a ARP request packet with the MAC address of A in the same network. It reaches to all nodes including Router interface to the n/w
- All except C will reject but C will accept with a ARP reply packet (unicast) with its MAC address.

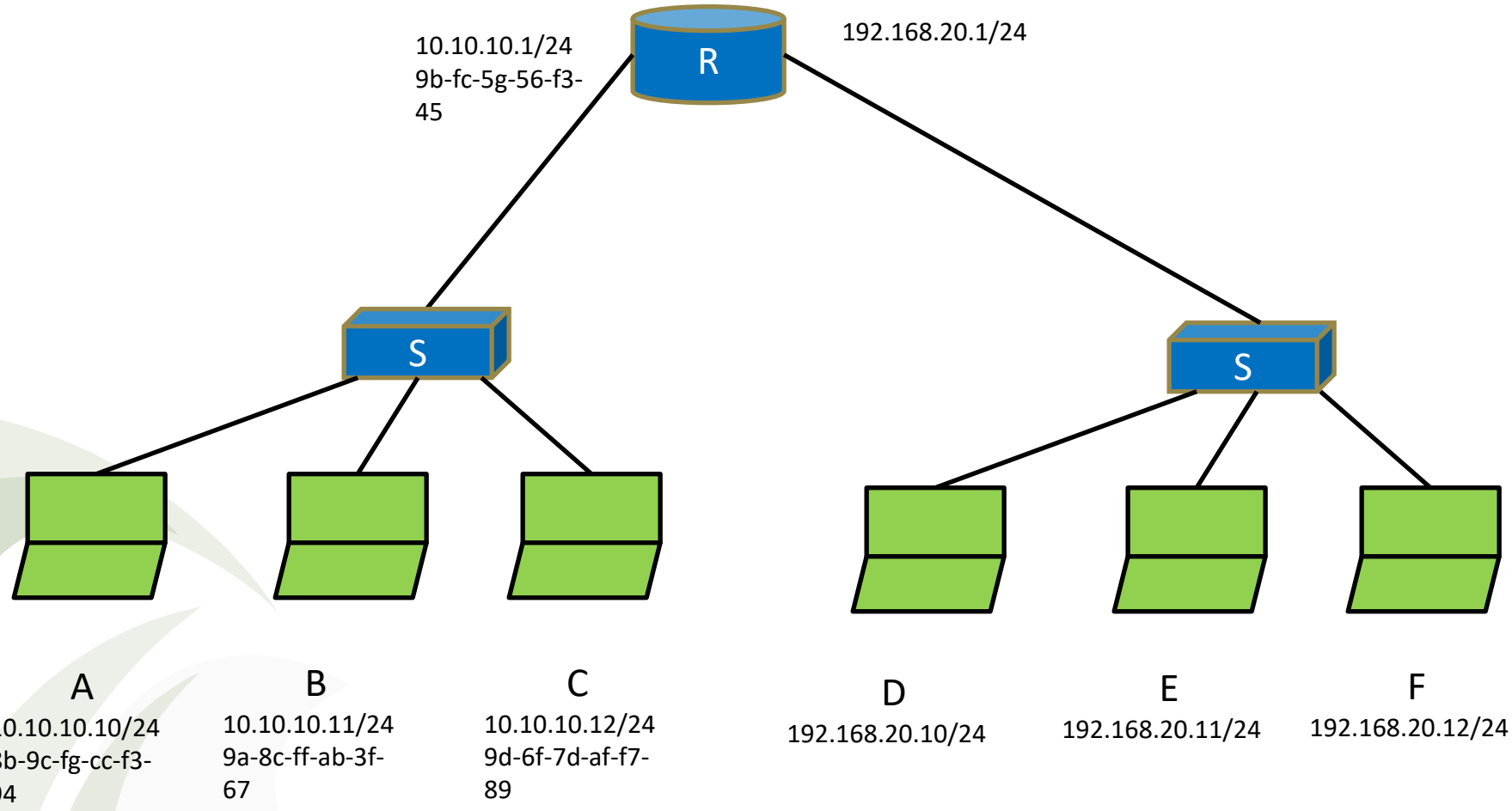
[**ARP cache** is a table maintained by ARP which contains IP address with its associated MAC address and type. If MAC address is learned dynamically then the type will be dynamic and if MAC address is added manually then type will be static.]

Let two nodes are in same network. You know the IP of the node. From arp -a you are not getting the MAC in ARP table. Just ping that address. If successfully ping then again type arp –a. The MAC for the new address is added.



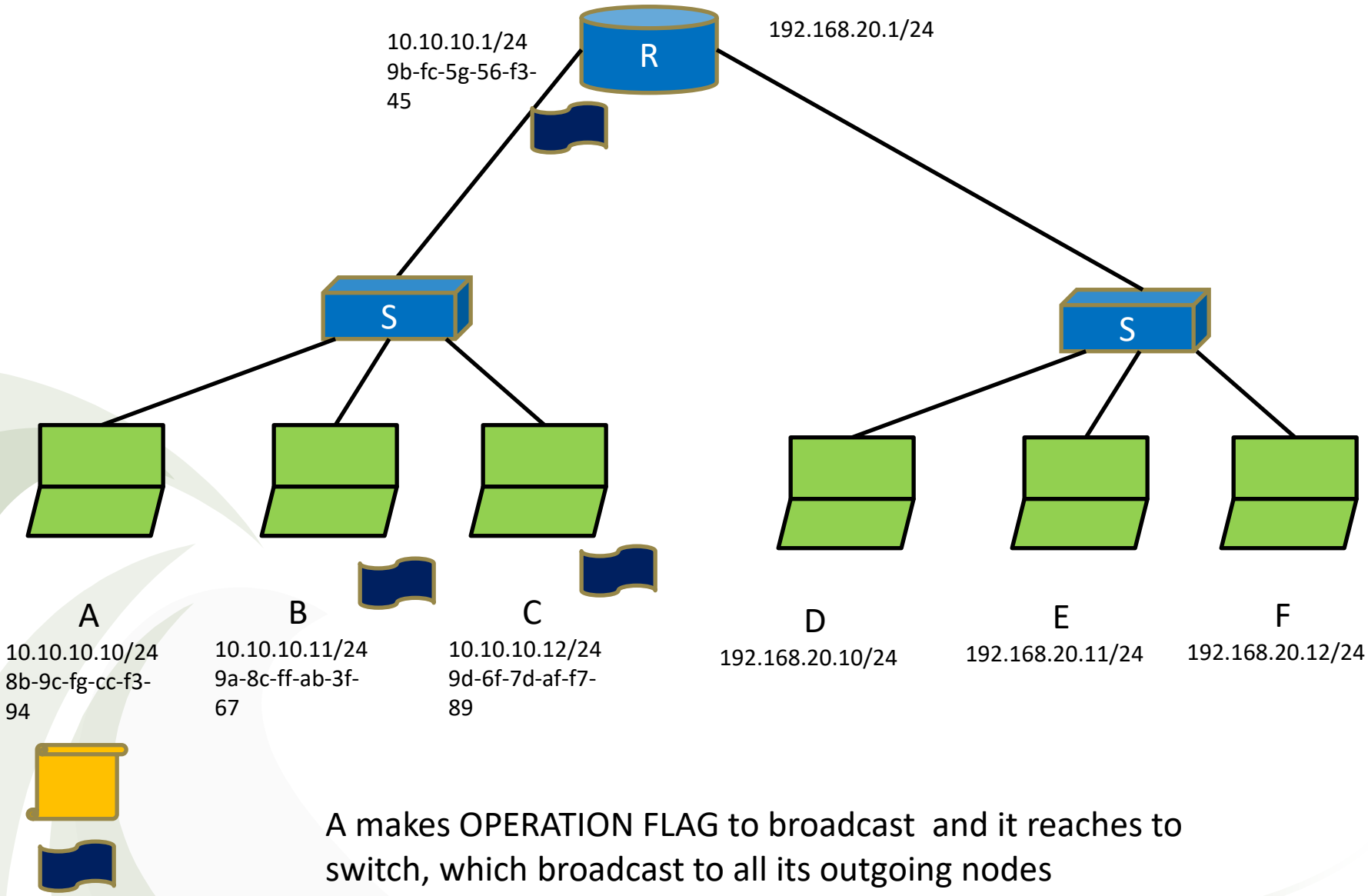


A wants to communicate with C

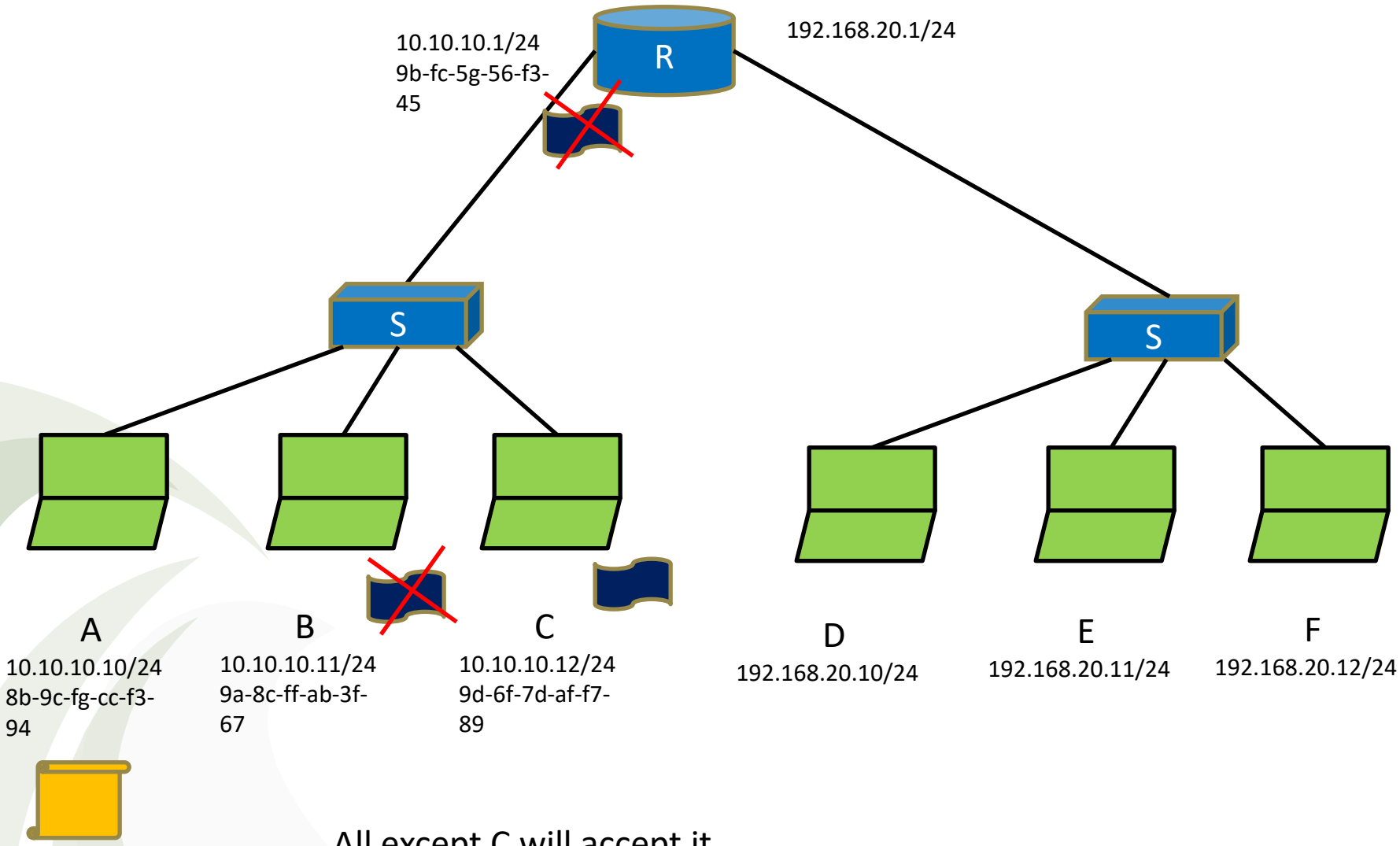


A does not know the MAC address of C

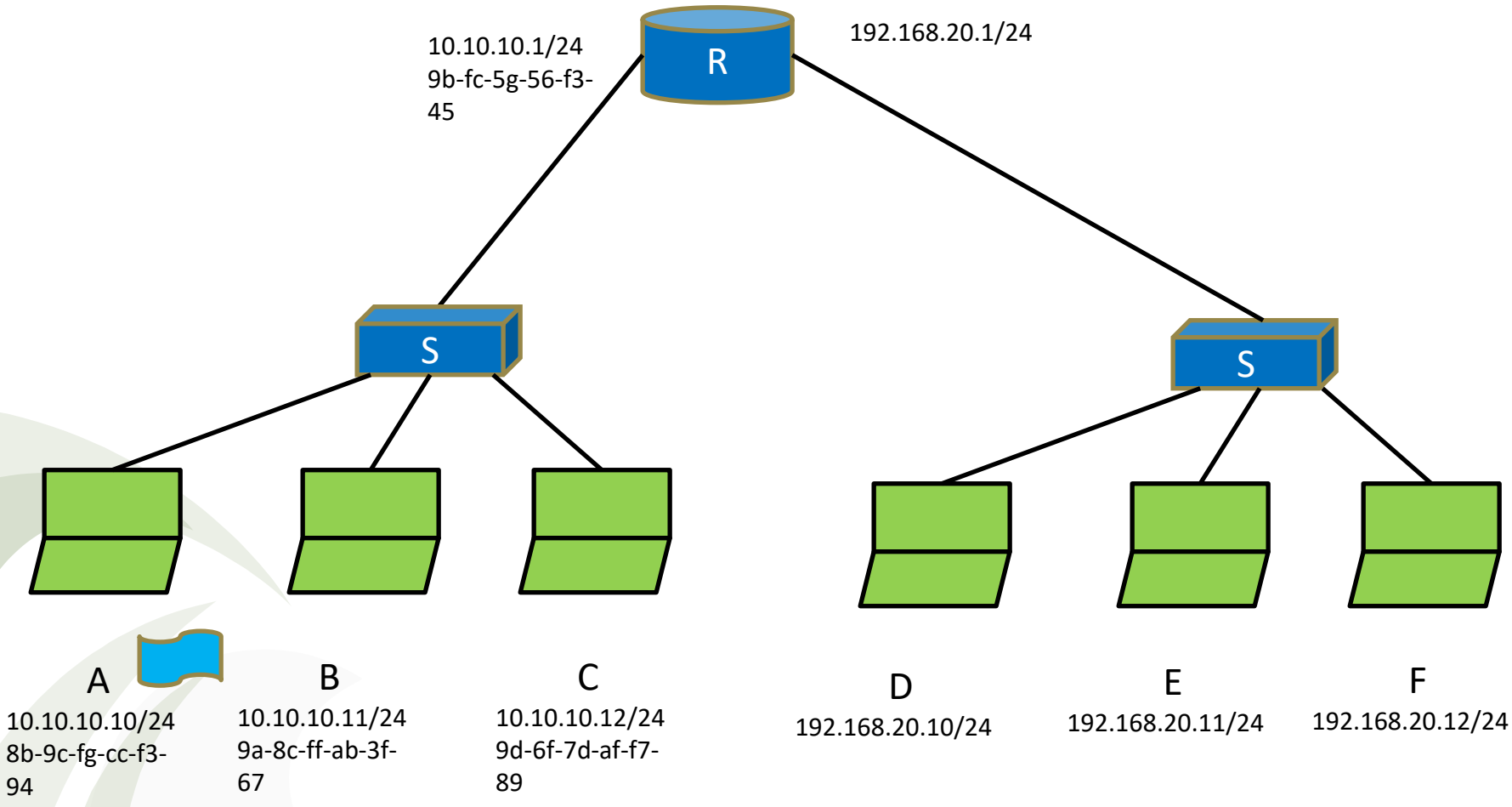
A generates an ARP request with the IP address of C.



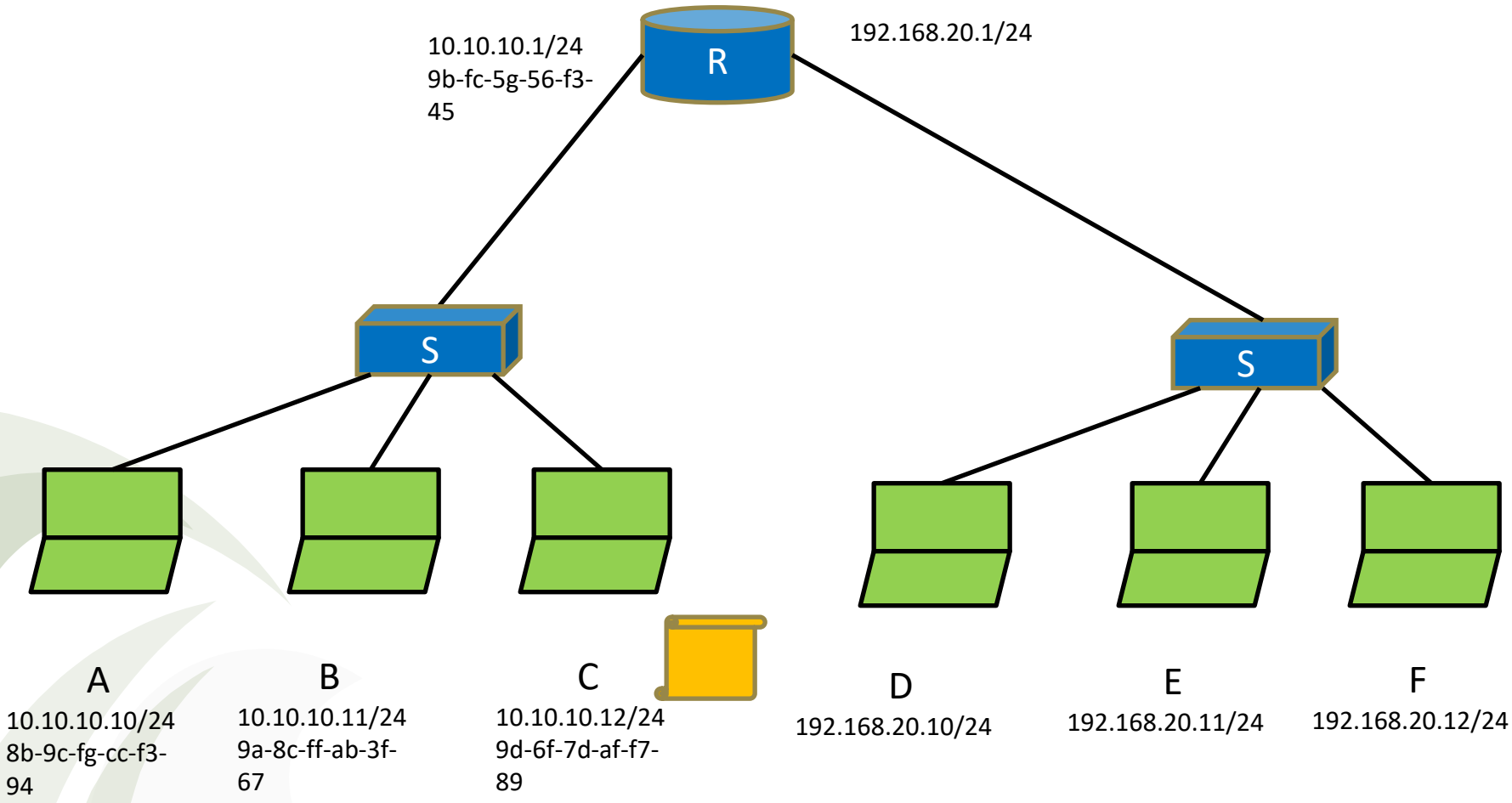
A makes OPERATION FLAG to broadcast and it reaches to switch, which broadcast to all its outgoing nodes



All except C will accept it



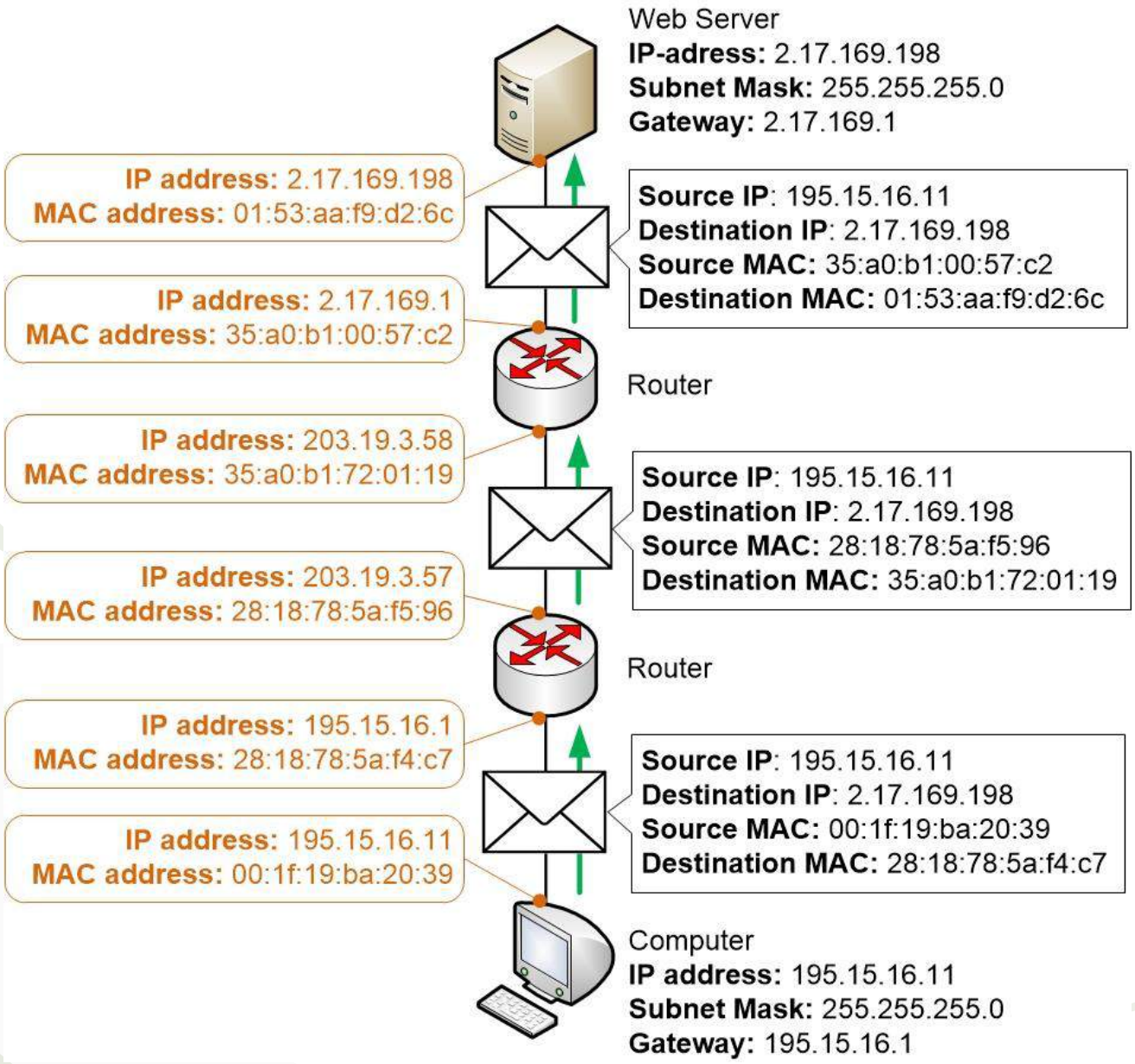
C will unicast an ARP reply to A via switch. In the traversal process S also updates its ARP cache. A also updates its ARP cache and from further communication A does not need to generate ARP request.



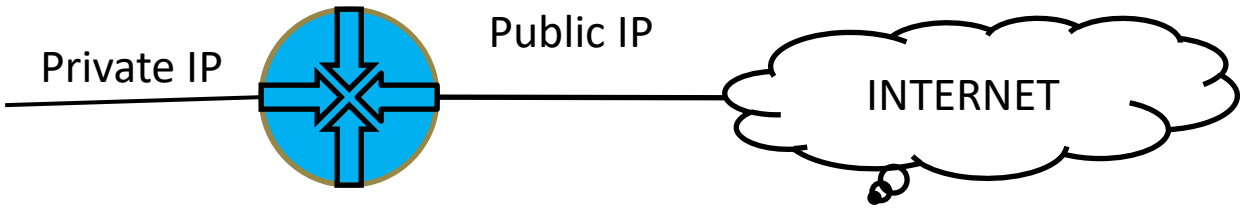
Now A can directly send the message to C

Communication in different network

- **AND operation** is performed between source IP address , source subnet mask and destination IP address, source subnet mask. If the two results does not matches then both nodes resides in same n/w.


Web Server
IP-adress: 2.17.169.198
Subnet Mask: 255.255.255.0
Gateway: 2.17.169.1
IP address: 2.17.169.198
MAC address: 01:53:aa:f9:d2:6c
Source IP: 195.15.16.11
Destination IP: 2.17.169.198
Source MAC: 35:a0:b1:00:57:c2
Destination MAC: 01:53:aa:f9:d2:6c
IP address: 2.17.169.1
MAC address: 35:a0:b1:00:57:c2
Router
IP address: 203.19.3.58
MAC address: 35:a0:b1:72:01:19
Source IP: 195.15.16.11
Destination IP: 2.17.169.198
Source MAC: 28:18:78:5a:f5:96
Destination MAC: 35:a0:b1:72:01:19
IP address: 203.19.3.57
MAC address: 28:18:78:5a:f5:96
Router
IP address: 195.15.16.1
MAC address: 28:18:78:5a:f4:c7
Source IP: 195.15.16.11
Destination IP: 2.17.169.198
Source MAC: 00:1f:19:ba:20:39
Destination MAC: 28:18:78:5a:f4:c7
IP address: 195.15.16.11
MAC address: 00:1f:19:ba:20:39
Computer
IP address: 195.15.16.11
Subnet Mask: 255.255.255.0
Gateway: 195.15.16.1

NAT



Network address Translation. Operates mainly in router and firewall

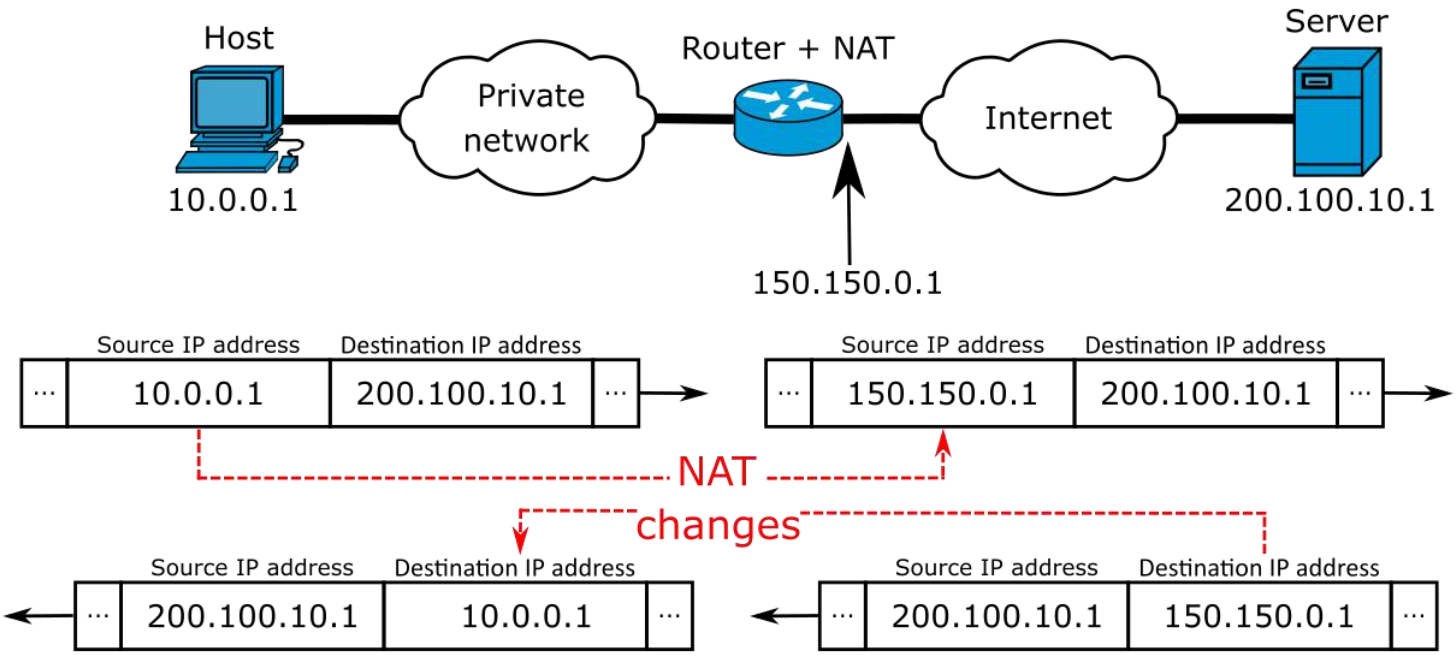
Technique to is to allow multiple devices to access the Internet through a single public address.

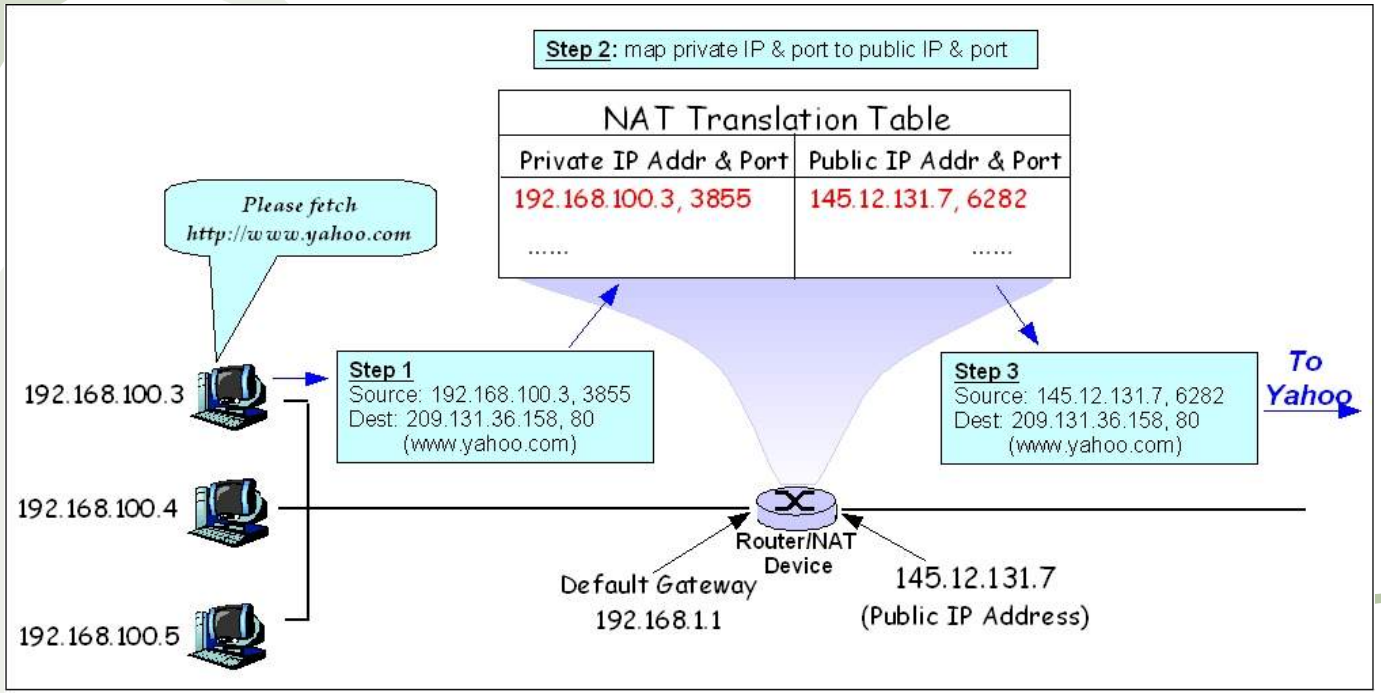
Use: to limit the number of public IP addresses an organization or company must use, for both economy and security purposes.

Packet from private IP address and port number (source) is translated to public IP and port is also masked.

corresponding entries of IP address and port number in the NAT table.

NAT works at the border router, whose one interface is in private network and another one is in private network.





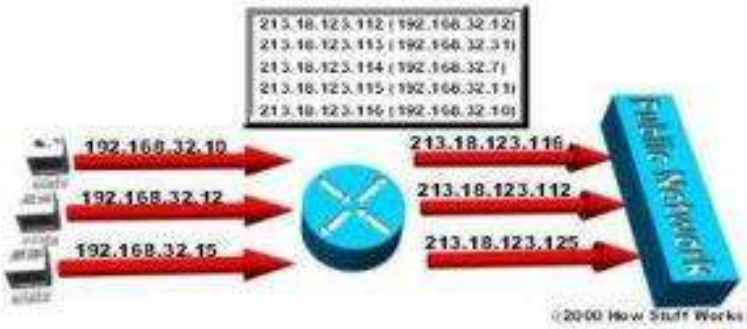
Source: wikipedia

NAT

- Why port number is translated?

Types:

Static NAT: Used in web hosting. private IP are mapped to public IP in 1:1 basic



Dynamic NAT: Maps a private IP address to a public IP address from a group of public IP addresses.

PORT NAT: A form of dynamic NAT that maps multiple public IP addresses to a single public IP address by using different ports. This is known also as PAT (Port Address Translation), single address NAT or port-level multiplexed NAT.

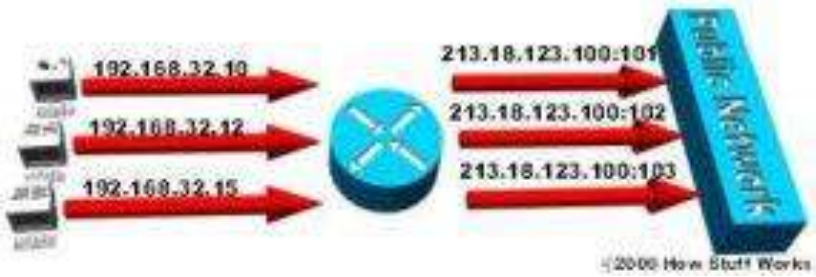


Image source: https://computer.howstuffworks.com/nat.htm

NAT and Proxy

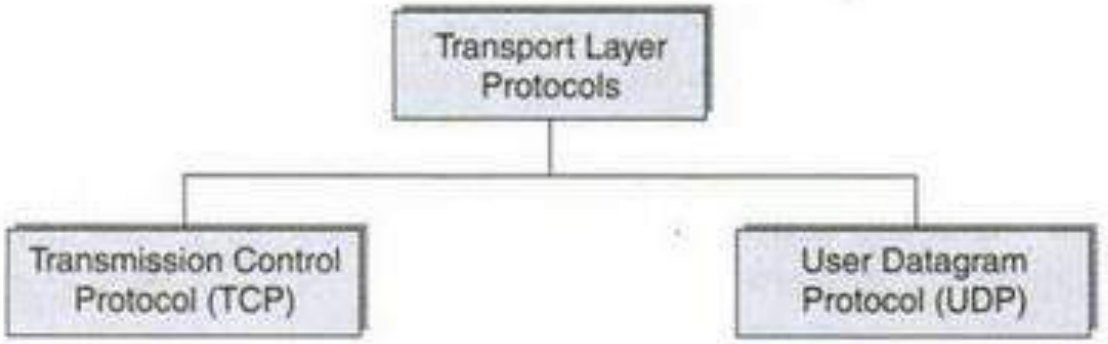
- Proxy function at layer 7 where as NAT in layer 3 or 4.
- Proxy used for security purpose whereas NAT is used for network administration.

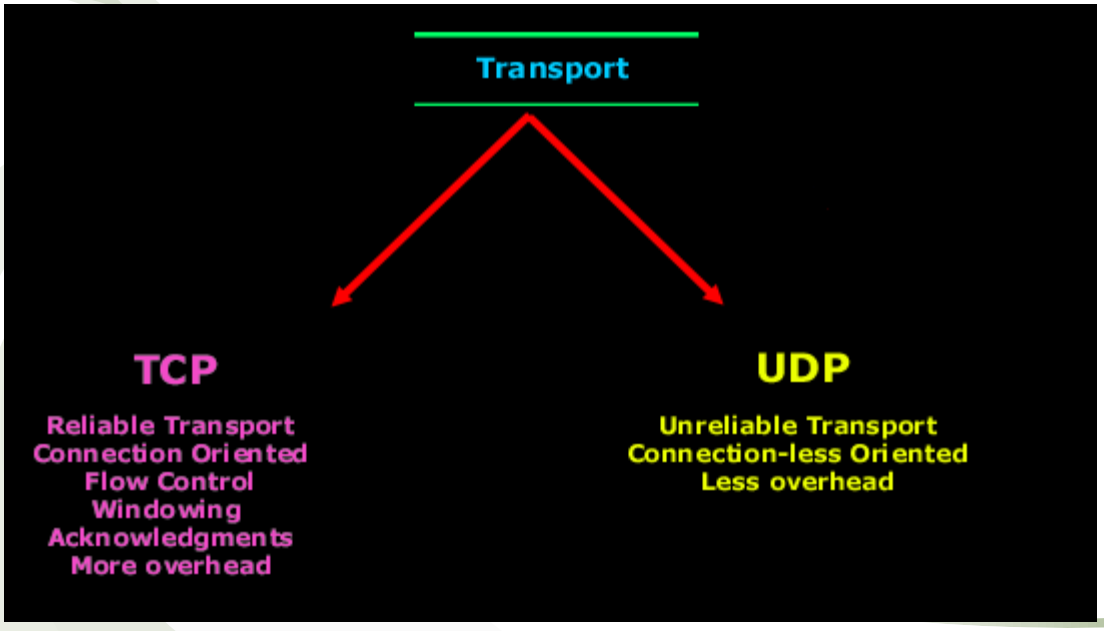
More on IP

- IP is unreliable: does not guarantee the delivery of a datagram to its destination.
- Best effort delivery mechanism.
- **IP** does not support flow control, retransmission, acknowledgement and error recovery. (Surprised? Actually IP lets it over upper layer protocol TCP)
- IP does not have any tracking mechanism to check whether a datagram is sent to next hop or not.
- IP is connectionless thus stateless. all packets in **IP** network are routed independently, they may not necessarily go through the same route, (except virtual circuit network)
- The minimum size of an IP datagram is 576 bytes and the maximum size is 65535 bytes.

From Internet layer to Transport layer

- Mainly concerned with the transportation of packets from source to the destination. (end to end delivery)
- Ensures correct delivery.
- In TCP/IP the transport layer has two protocols. TCP and UDP


Transport Layer Protocols
Transmission Control Protocol (TCP)
User Datagram Protocol (UDP)


Transport
TCP
Reliable Transport
Connection Oriented
Flow Control
Windowing
Acknowledgments
More overhead
UDP
Unreliable Transport
Connection-less Oriented
Less overhead

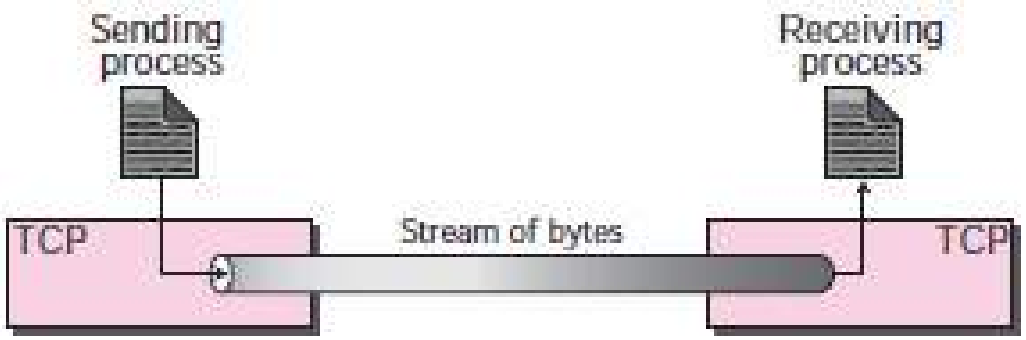
Transmission Control Protocol(TCP)

- Process to process communication.
- Done through port number.
- provides reliable, ordered, and error-checked delivery of a stream of octets (bytes) between applications running on hosts communicating via an IP network.

Port	*Protocol*	*Description*
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
20 and 21	FTP	File Transfer Protocol (Data and Control)
23	TELNET	Terminal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name Server
67	BOOTP	Bootstrap Protocol
79	Finger	Finger
80	HTTP	Hypertext Transfer Protocol

TCP

- allows the sending process to deliver data as a stream of bytes and allows the receiving process to obtain data as a stream of bytes.
- Creates an environment in which the two processes seem to be connected by an imaginary “tube” that carries their bytes across the Internet
- The sending process produces (writes to) the stream of bytes and the receiving process consumes (reads from) them.



Sending and Receiving Buffers

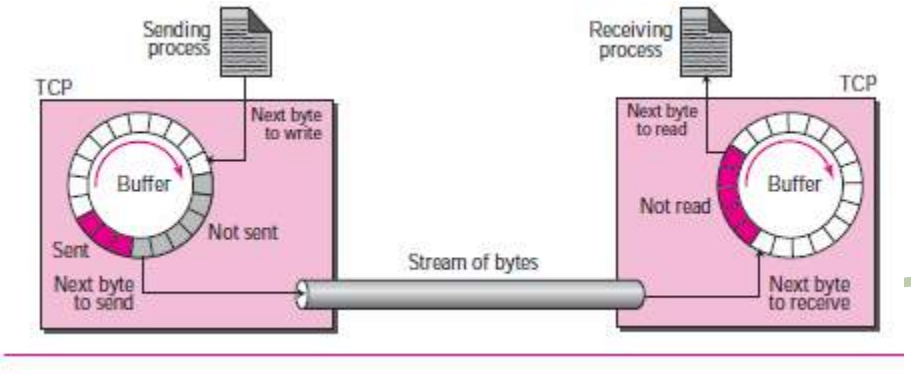
- Sending and the receiving processes may not necessarily write or read data at the same rate.
- TCP needs buffers for storage.
- Two buffers, the sending buffer and the receiving buffer, one for each direction.
- Buffers are circular array of 1-byte locations.
- Has three types of chambers.
- Sending buffer has three types of chambers

a)empty chambers –that can be filled by the sending process (producer),

b) Chamber with byte been sent but not yet acknowledged. (TCP sender keeps these bytes in the buffer until it receives an acknowledgment)

c) Chamber contains bytes to be sent by the sending TCP.

- After getting acknowledgement those become empty.



Sending and Receiving Buffers

Two types of chambers in receiving buffer.

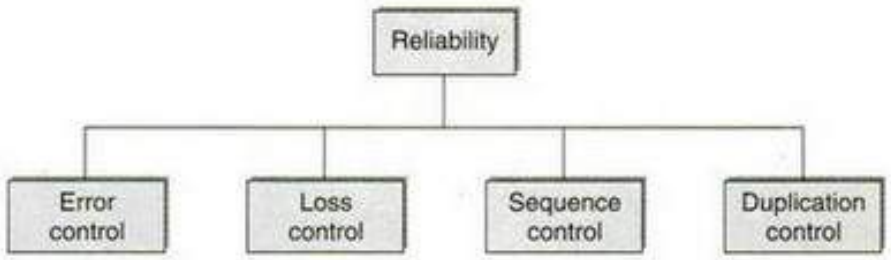
a) empty chambers to be filled by bytes received from the network.

b) received bytes that can be read by the receiving process.

(When a byte is read by the receiving process, the chamber is recycled)

Features of TCP

- Reliability
- Point to point communication
- Connection oriented approach



Reliability

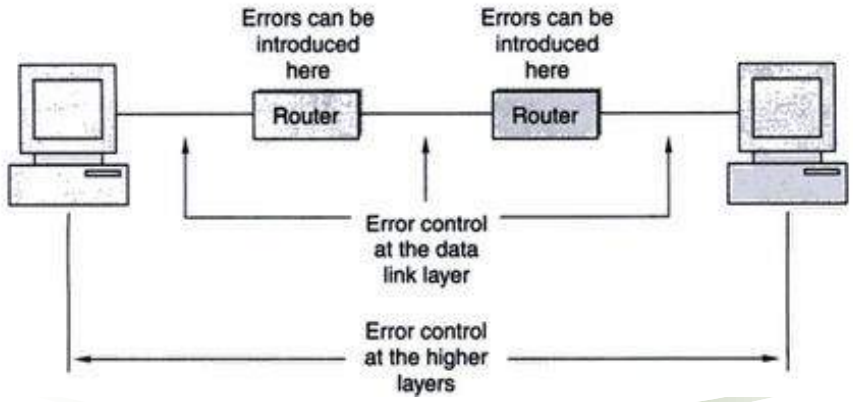
Reliability:

- Ensures end to end delivery
- No data loss or change in the order of the data.

Error control: Has own checksum.

[Q. CRC is already there why extra?

A. Data link layer ensures error free delivery between two networks. If error is introduced in router? Beyond the reach of data link layer.]



Connection oriented service

If process at node A wants to communicate with another process at node B

a. The two TCPs establish a virtual connection between them.

b. Data are exchanged in both directions.

c. The connection is terminated.

Loss control: provides segment number while breaking original message into segments. If one of them is loss (**IP is connection less and does not guarantee delivery**) destination will find the mismatch.

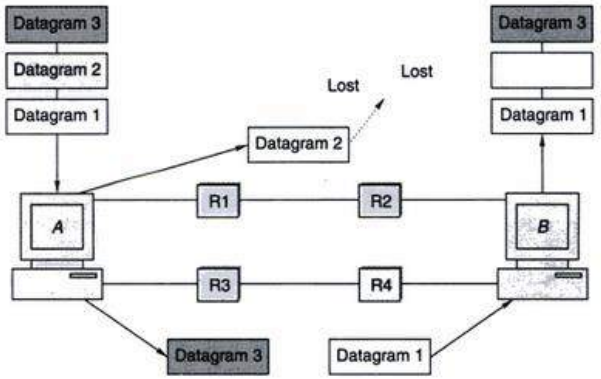
Sequence control: Different segment takes different route in routing.

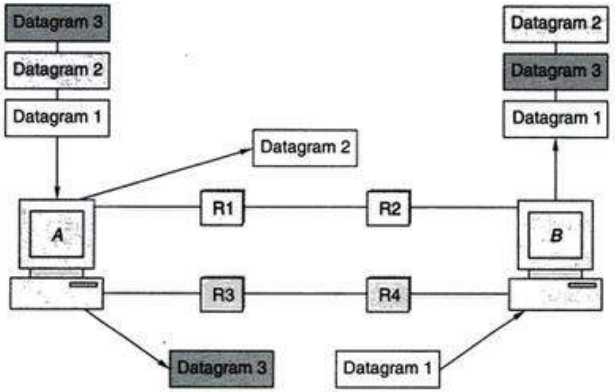
They are arranged properly at destination

Duplication control: opposite to loss control

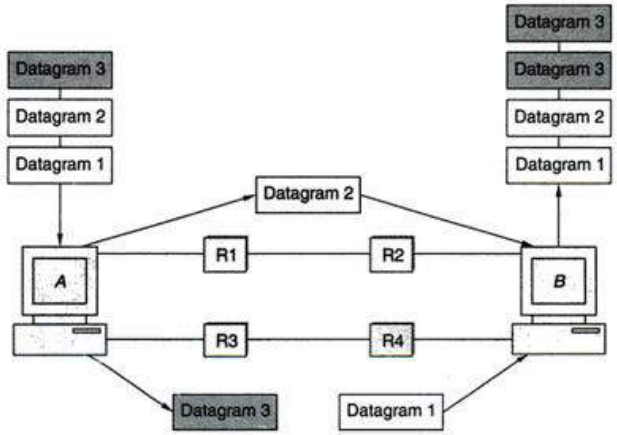
Same datagram may reach to destination twice or more through different paths.

destination must have the mechanism to detect the duplication





Sequence control



Duplication control

Point to point communication: port to port communication

Connection oriented:

- Connection provided by TCP is called virtual connection
- connection must be established between two ends of a transmission before either can transmit data.
- Regarding virtual connection sender and receiver are aware but intermediate router do not have any clue.

Relationship between TCP and IP

Communication using TCP/IP

TCP features

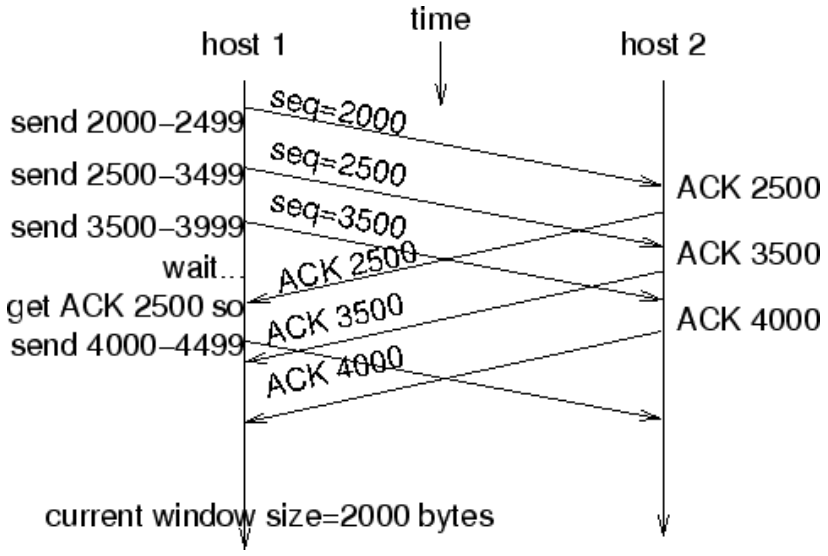
I. Numbering System:

- In TCP there is no field for segment number in header.
- There are two fields called the *sequence number and the acknowledgment number.*
- *These* fields refer to a byte number and not a segment number.

a) Byte Number:

- TCP numbers all data bytes (octets) that are transmitted in a connection.
- Numbering is independent in each direction.
- TCP
- TCP receives bytes from a process and stores them in the sending buffer and numbers them.
- TCP chooses an arbitrary number between 0 and $2^{32} - 1$ for the number of the first byte.

Example: Let the number is 1,057 and the total data to be sent is 6,000 bytes, the bytes are numbered from 1,057 to 7,056.



TCP features

b) Sequence number:

- After the bytes are numbered, TCP assigns a sequence number to each segment that is being sent.
- The sequence number for each segment is the number of the first byte of data carried in that segment.

c) Acknowledgment Number:

- Communication in TCP is full duplex; when a connection is established, both parties can send and receive data at the same time.
- sequence number in each direction shows the number of the first byte carried by the segment.
- Each party uses an acknowledgment number to confirm the bytes it has received.
- Acknowledgment number defines the number of the next byte that the party expects to receive.
- Acknowledgment number is cumulative, ---party takes the number of the last byte that it has received, safe and sound, adds 1 to it, and announces this sum as the acknowledgment number.

TCP features

II. Flow Control:

- TCP controls how much data can be accepted from the sending process; the receiving TCP controls how much data can to be sent by the sending TCP.
- Done to prevent the receiver from being overwhelmed with data.
- Numbering system allows TCP to use a byte oriented flow control.

III. Error Control:

- TCP implements an error control mechanism.
- Includes mechanisms for detecting corrupted segments, lost segments, out-of-order segments, and duplicated segments.
- Error control also includes a mechanism for correcting errors after they are detected.
- Error detection and correction in TCP is achieved using checksum, acknowledgment, and time-out.

TCP features

III.a. TCP uses a 16-bit **checksum** that is mandatory in every segment.

III.b.

- TCP uses acknowledgments to confirm the receipt of data segments.
- Control segments that carry no data but consume a sequence number are also acknowledged.
- ACK segments are never acknowledged.

III.c.

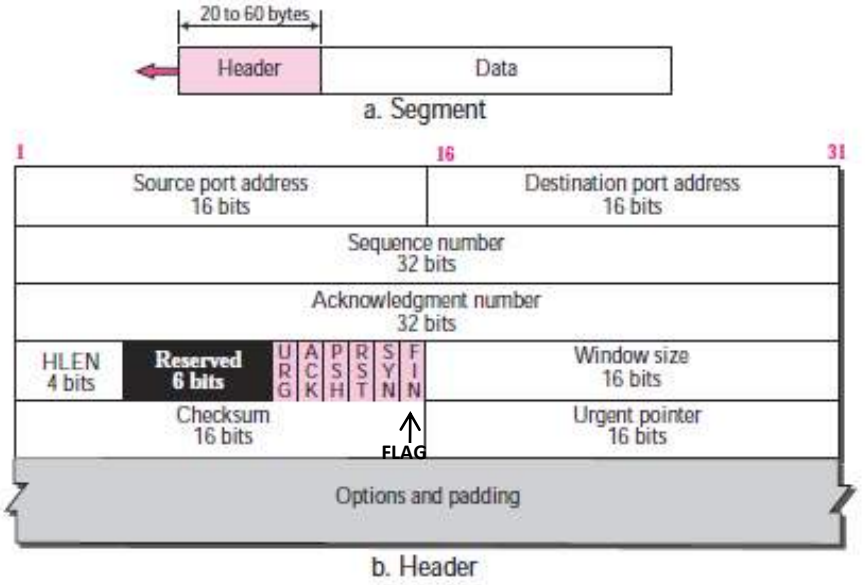
- Retransmission of segments.
- When a segment is corrupted, lost, or delayed, it is retransmitted.
- A segment is retransmitted when a retransmission timer expires.

TCP segment format

- Has header of size 20 to 60 byte followed by actual data.
- TCP segment without option –20 byte else 60 byte

Source port number: port number of the source computer corresponding to the application that is sending this TCP segment

Destination port number: corresponding to the application that is expected to receive this TCP segment



Port	*Protocol*	*Description*
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day

Port	*Protocol*	*Description*
19	Chargen	Returns a string of characters
20 and 21	FTP	File Transfer Protocol (Data and Control)
23	TELNET	Terminal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name Server
67	BOOTP	Bootstrap Protocol
79	Finger	Finger
80	HTTP	Hypertext Transfer Protocol

TCP segment format

Sequence number:

- TCP is connection oriented.
- Each byte to be transmitted from source to destination is numbered in an increasing sequence.
- sequence number tells the destination which byte in this sequence is the first byte in the segment.
- During connection establishment (discussed later) each party uses a random number generator to create an **initial sequence number (ISN), which is** usually different in each direction.
- If ISN is 'n' and first TCP segment is carrying 2000 byte, then sequence number will be n+2. [n and n+1 are used in connection establishment]. Next it will be (n+2+2000).

Acknowledgement number:

If destination host receives a byte number X correctly [last byte of a sequence], it sends X+1 as acknowledgement back to source.

- Acknowledgment and data can be piggybacked together.

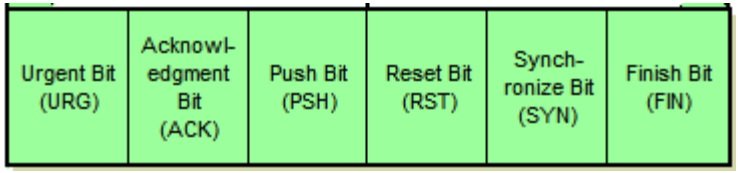
Header length:

- 4 bit field specifies the number of 4 byte words in the TCP header.
- Field can be between 5 to 15 (5 X4 =20 to 15 x 4=60 header length)

Reserved: Currently unused

TCP segment format

Flag: 6 bit field defines 6 different control flags
each occupying one bit.



Subfield name	Description
URG	Urgent bit: 1: Priority transfer
ACK	Acknowledgement: 1 means carrying an acknowledgement. Value of the Acknowledgement number field is valid carrying next sequence number expected from destination of this segment
PSH	Push bit: data in this segment be immediately pushed to the application on the receiving device
RST	Reset bit: sender encounters a problem and want to reset the connection.
SYN	source wants to establish a connection with the destination
FIN	Finish bit: 1 --sender wants to terminate the TCP connection

TCP segment format

Window size: determines the size of the sliding window that the other party must maintain.

Checksum: for facilitating error detection and correction.

Urgent pointer: Used in situation where some data in a TCP segment is more important or urgent that other data in the same TCP connection.

TCP connection--A three way handshaking

- Requires three phases: **connection establishment**, **data transfer**, and **connection termination.**

Connection Establishment:

- TCP transmits data in full-duplex mode.
- TCP in two machines able to send segments to each other simultaneously.
- This implies that each party must initialize communication and get approval from the other party before any data are transferred.
- Connection establishment in TCP is called **Three way handshaking**

TCP connection

- Application program of client, wants to make a connection with another application program of server, using TCP.
- Process starts with the server. Server program tells its TCP that it is ready to accept a connection. This request is called a *passive open.*
- Client program issues a request for an *active open.*
- *A client that wishes to connect* to an open server tells its TCP to connect to a particular server.

Steps**: I. Synchronization:**

i) client sends the first segment, a SYN segment, in which only the SYN flag is set.

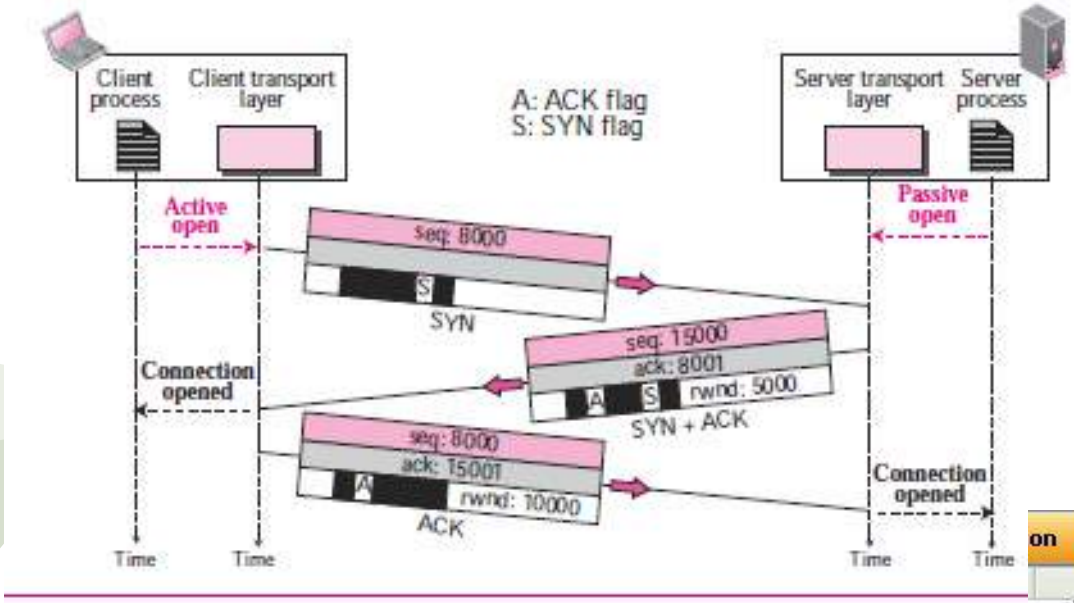
ii) Used for synchronization of sequence numbers.

iii) The client chooses a random number [initial sequence number(ISN)] as the first sequence number and sends this number to the server.

iv) This segment does not contain an acknowledgment number. Does not define the window size [window size definition makes sense only when a segment includes an acknowledgment]

v) SYN segment is a control segment and carries no data. However, it consumes one sequence number. When the data transfer starts, the ISN is incremented by 1

Three way handshaking



Three way handshaking

II. Server synchronization and acknowledgement:

- Server sends the second segment, a SYN + ACK segment with two flag bits set: SYN and ACK.
- Serves dual purposes. First, it is a SYN segment for communication with INS number sent from the server to the client.
- Second acknowledgement of the receipt of the SYN segment from the client by setting the ACK flag and displaying the next sequence number it expects to receive from the client.
- Needs to define the receive window size, *rwnd (to be used by the client)*

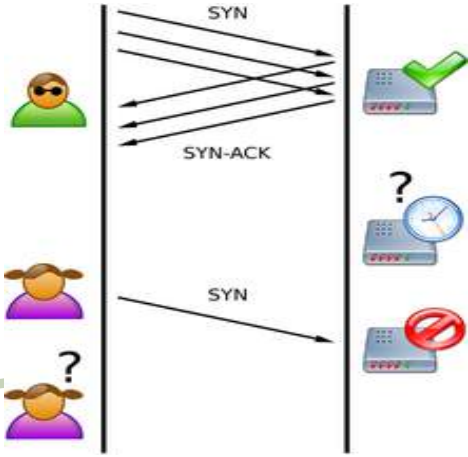
TCP connection

III.

- Client sends the third segment. Just an ACK segment.
- Acknowledges the receipt of the second segment with the ACK flag and acknowledgment number field.
- Sequence number in this segment is the same as the one in the SYN segment; the ACK segment does not consume any sequence numbers.
- The client must also define the server window size.

SYN flooding attack

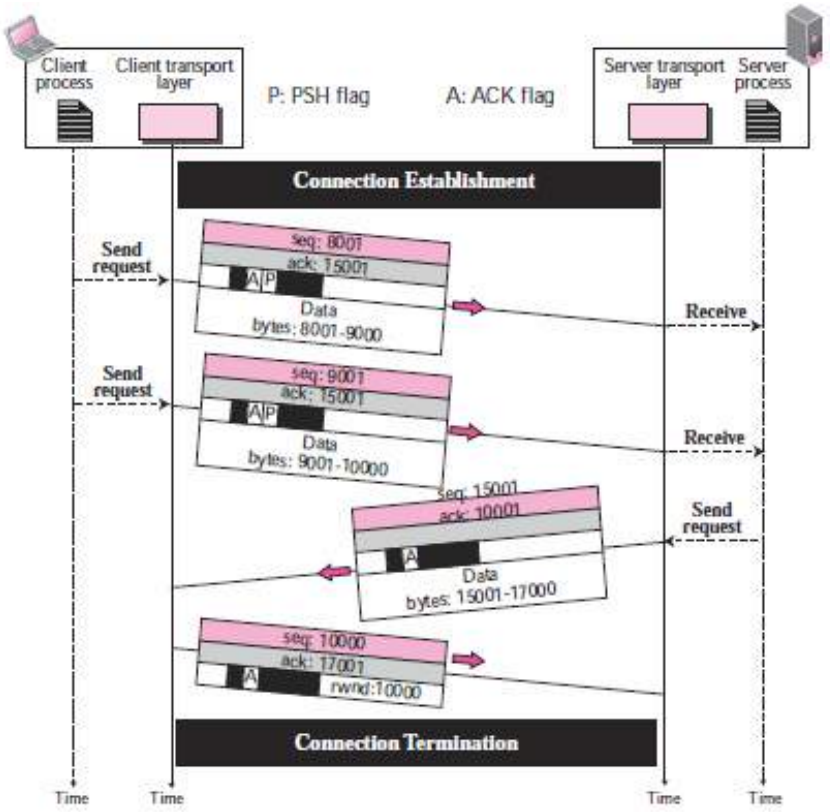
- serious security problem in TCP connection.
- Several malicious attackers send a large number of SYN segments to a server pretending that each of them is coming from a different client (by faking the source IP addresses in the datagrams)
- The server, assuming that the clients are issuing an active open, allocates the necessary resources.
- The TCP server then sends the SYN + ACK segments to the fake clients, which are lost.
- When the server waits for the third leg of the handshaking process, however, resources are allocated without being used.
- If, during this short period of time, the number of SYN segments is large, the server eventually runs out of resources and may be unable to accept connection requests from valid clients
- Distributed Denial of Service (DDoS) attack



TCP connection

Data Transfer:

- After connection is established, bidirectional **data transfer can take place.**
- **Client** and server can send data and acknowledgments in both directions.
- These are numbered as discussed earlier.



- Last segment carries only an acknowledgment because there is no more data to be sent.
- The data segments sent by the client have the PSH (push) flag set so that the server TCP tries to deliver data to the server process as soon as they are received.

TCP connection

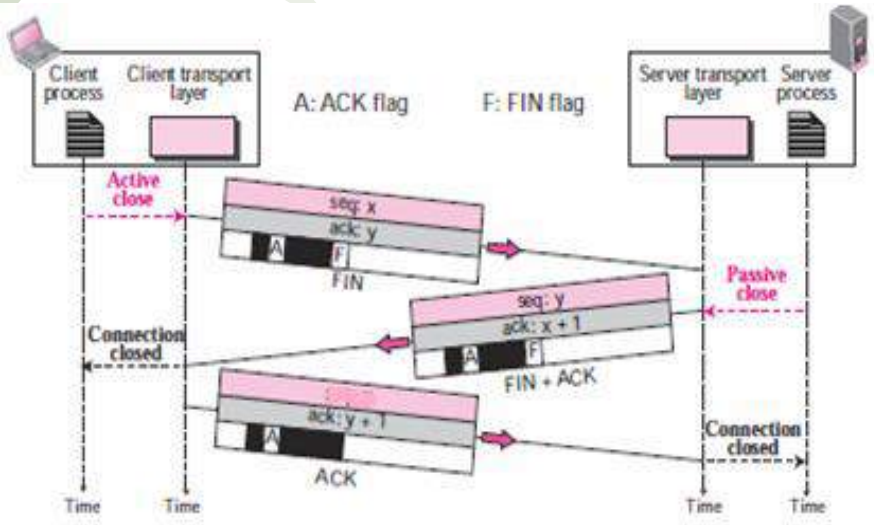
- In data transfer two types of bit play role a) PSH bit b) URG bit.
- Buffering of data in receiving TCP --delivered them to the application program when it is ready or when it is convenient for the receiving TCP.
- Situation when delayed transmission and delayed delivery of data may not be acceptable by the application program.
- Application program at sender can request a *push operation. Indicates sending TCP* ***must not wait for the window to be*** **filled**. It must create a segment and send it immediately.
- This is done by setting **PSH** bit.
- There are occasions in which an application program needs to send *urgent bytes,* ***some bytes that need to be treated in a special way*** *by the application at* the other end. →Send a segment with the **URG** bit set.

TCP connection

Connection Termination:

- Usually initiated by the client.
- Most implementations today allow two options for connection termination: three-way handshaking and four-way handshaking with a half-close option.

Three way handshaking:



i)

- TCP at client receives a close command from the client process.
- Send FIN segment in which the FIN flag is set.
- it consumes only one sequence number and contains last chunk of data if exist.

ii)

- Server receives the FIN segment
- informs its process of the situation
- and sends the second segment, a FIN+ACK segment.
- it consumes only one sequence number and contains last chunk of data if exist.

TCP connection

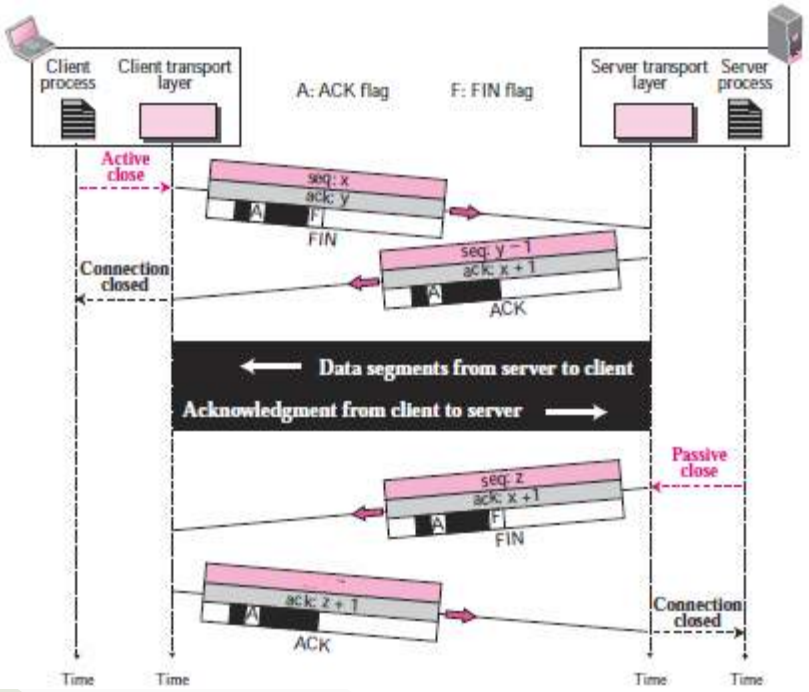
iii)

- Client TCP sends the last segment, an ACK segment.
- Confirm the receipt of the FIN segment from the TCP server. Contains the acknowledgment number, which is one plus the sequence number received in the FIN segment from the server.
- This segment cannot carry data and consumes no sequence numbers.

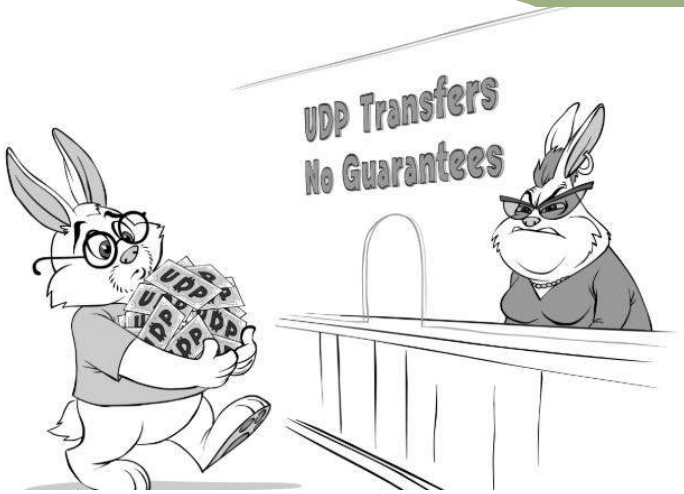
Half close operation

- Here one end can stop sending data while still receiving data.
- Server or the client both can issue a half-close request.
- occur when the server needs all the data before processing can begin.

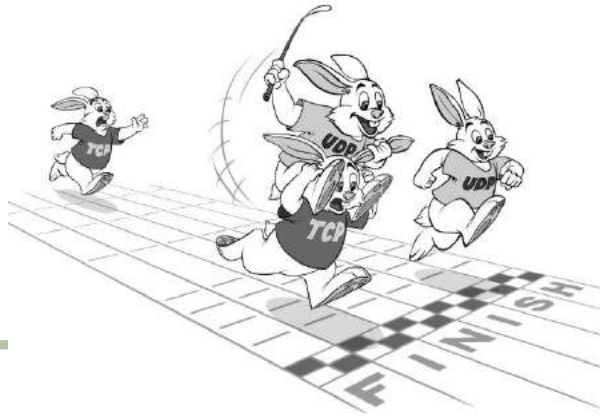
[Example: Sorting at server. Server needs to receive all the data before sorting starts. Client, after sending all data, can close the connection in the client-to-server direction. However, the server-to-client direction must remain open to return the sorted data. The server, after receiving the data, still needs time for sorting; its outbound direction must remain open.]



UDP



- User datagram protocol.
- far simpler but less reliable than TCP
- connectionless protocol.
- No error checking involved
- Does not provide any acknowledgement
- Do not have any sequence or reordering mechanism
- is a **connectionless, unreliable transport protocol**
- provides process-to-process communication
- Left on application program that uses UDP to accept full responsibility to handle issues as reliability, data loss, duplication, delay, loss of connection.
- UDP is a better choice for voice or video communication as lost of few bit does not effect so much on QoS.
- For data transmission TCP is the best.
- UDP is faster than TCP



UDP datagram

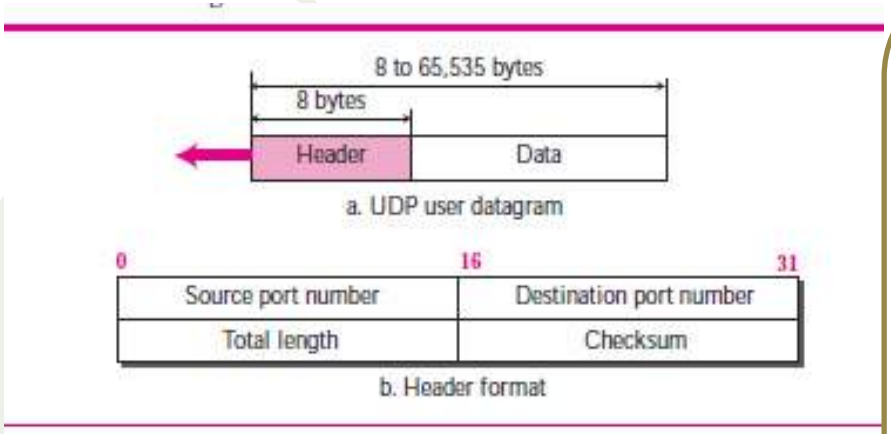
Source port number: Port number used by the process running on the source host. It is 16 bits long.

Destination port number: Port number used by the process running on the destination host. It is also 16 bits long.

Total packet length: total length of UDP datagram (header + data)

UDP datagram length = IP datagram length – IP header length

The length field in a UDP user datagram is actually not necessary. A UDP is encapsulated in an IP datagram. IP datagram has the field total length. Has also length of the header. So **UDP length= IP length– IP header's length**



Checksum: For error detection.

Till why?

However, the designers of the UDP protocol felt that it was more efficient for the destination UDP to calculate the length of the data from the information provided in the UDP user datagram rather than ask the IP software to supply this information.

We should remember that when the IP software delivers the UDP user datagram to the UDP layer, it has already dropped the IP header.

Question

UDP header in hexadecimal format

CB84000D001C001C

a. What is the source port number?

b. What is the destination port number?

c. What is the total length of the user datagram?

d. What is the length of the data?

e. Is the packet directed from a client to a server or vice versa? (Hint: Destination port number 13.)

f. What is the client process?

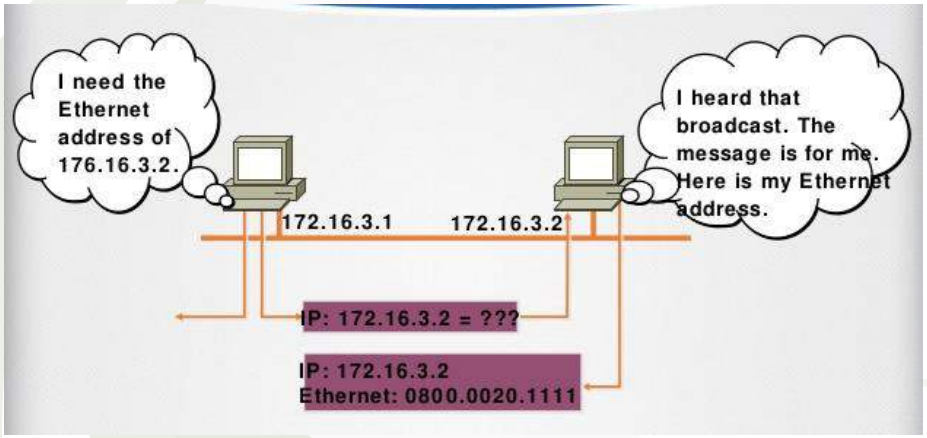
TCP VS UDP

	TCP	UDP
Connection	connection-oriented	connection-less
Function	As a message makes its way across the internet from one computer to another. This is connection based.	one program can send a load of packets to another and that would be the end of the relationship.
Usage	suited for applications that require high reliability, and transmission time is relatively less critical.	suitable for applications that need fast, efficient transmission, such as games. useful for servers that answer small queries from huge numbers of clients.
Use by other protocols	HTTP, HTTPs, FTP, SMTP, Telnet	DNS, DHCP, TFTP, SNMP, RIP, VOIP.
Ordering of data packets	rearranges data packets in the order specified.	no inherent order as all packets are independent of each other. If ordering is required, it has to be managed by the application layer.
Speed of transfer	slower than UDP	faster because error recovery is not attempted.
Reliability	absolute guarantee that the data transferred remains intact and arrives in the same order in which it was sent.	There is no guarantee that the messages or packets sent would reach at all.

	TCP	UDP
Header Size	20 bytes	8 bytes.
Common Header Fields	Source port, Destination port, Check Sum	Source port, Destination port, Check Sum
Weight	heavy-weight. requires three packets to set up a socket connection, before any user data can be sent. handles reliability and congestion control.	lightweight. no ordering of messages, no tracking connections, etc. small transport layer designed on top of IP.
Data Flow Control	does Flow Control. requires three packets to set up a socket connection, before any user data can be sent. TCP handles reliability and congestion control.	UDP does not have an option for flow control
Error Checking	does error checking and error recovery. Erroneous packets are retransmitted from the source to the destination.	UDP does error checking but simply discards erroneous packets. Error recovery is not attempted.
Acknowledgement	Acknowledgement segments	No Acknowledgment
Handshake	SYN, SYN-ACK, ACK	No handshake (connectionless protocol)

ARP

- *Logical address is usually implemented* in software.
- Every protocol that deals with interconnecting networks requires logical addresses.
- The logical addresses in the TCP/IP protocol suite are called **IP addresses.**
- Packets pass through physical networks to reach these hosts and routers.
- Hosts and routers are recognized by their physical addresses----the **local address.**
- Delivery of a packet to a host or a router requires two levels of addressing: logical and physical.
- Must be able to map a logical address to its corresponding physical address and vice versa.
- Done using either static or dynamic mapping



ARP

Static mapping:

- Creating a table that associates a logical address with a physical address.
- Table is stored in each machine on the network.
- Machine knowing the IP address of another machine but not its physical address can look it up in the table.

Have some limitations

- A machine could change its NIC, resulting in a new physical address.
- Some LANs, like LocalTalk, the physical address changes every time the computer is turned on. (by MAC spoofing)
- A mobile computer can move from one physical network to another, resulting in a change in its physical address.
- Static table must be updated periodically.

ARP

Dynamic Mapping:

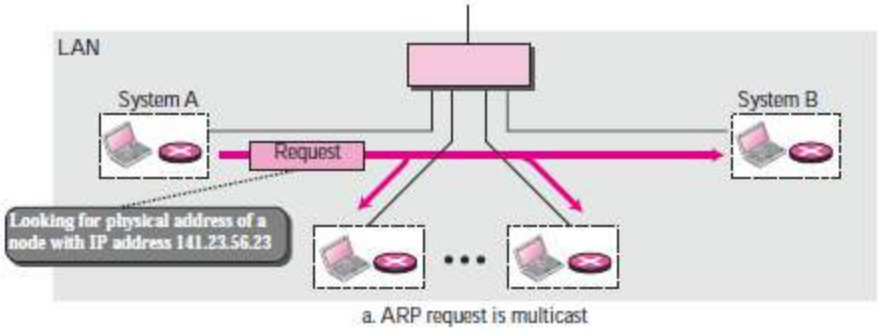
- Each time a machine knows the logical address of another machine.
- Use two protocols to find the physical address. Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP).
- ARP maps a logical address to a physical address; RARP maps a physical address to a logical address.

ARP

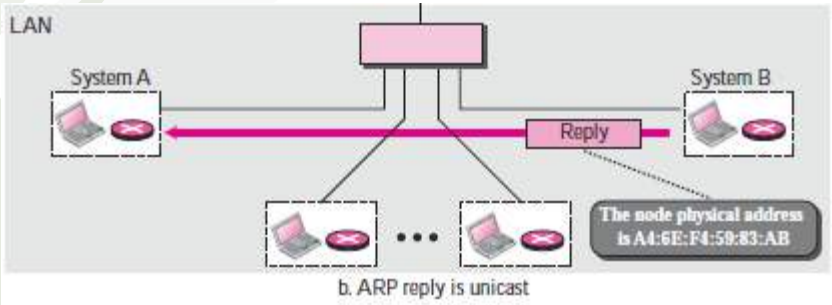
The Protocol:

- Anytime a host, or a router, needs to find the physical address of another host or router on its network.
- Sends an ARP query packet.
- The packet includes the physical and IP addresses of the sender and the IP address of the receiver.
- Sender does not know the physical address of the receiver, the query is broadcast over the network.
- Every host or router on the network receives and processes the ARP query packet, but only the intended recipient recognizes its IP address and sends back an ARP response packet.
- It contains the recipient's IP and physical addresses.
- The packet is unicasted directly to the inquirer using the physical address received in the query packet.

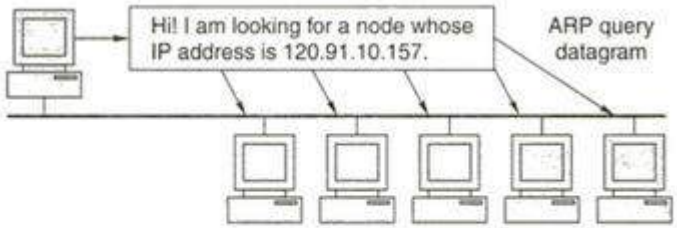
ARP



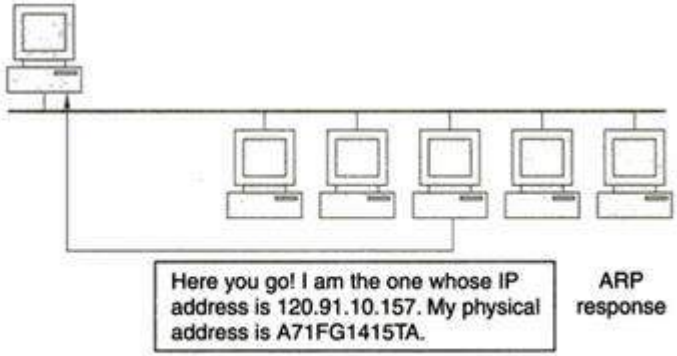
a. ARP request is multicast



b. ARP reply is unicast



(a) A router or a host sends an ARP query datagram (Request)



(b) Only the concerned host replies back and also sends its physical address

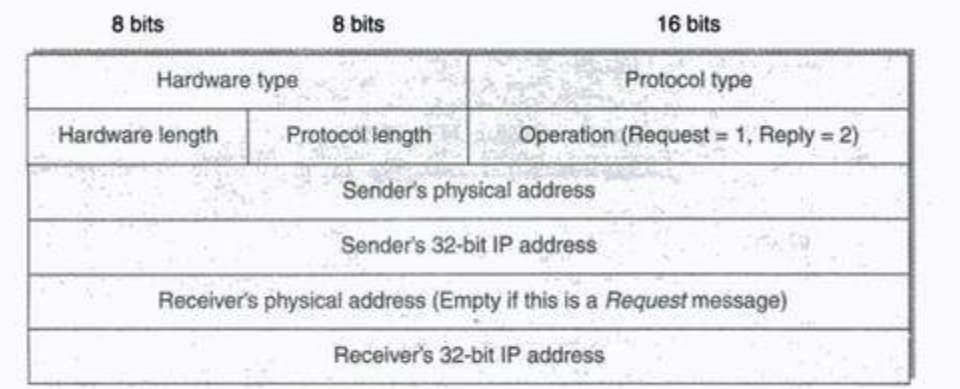
ARP Packet format

Hardware type:

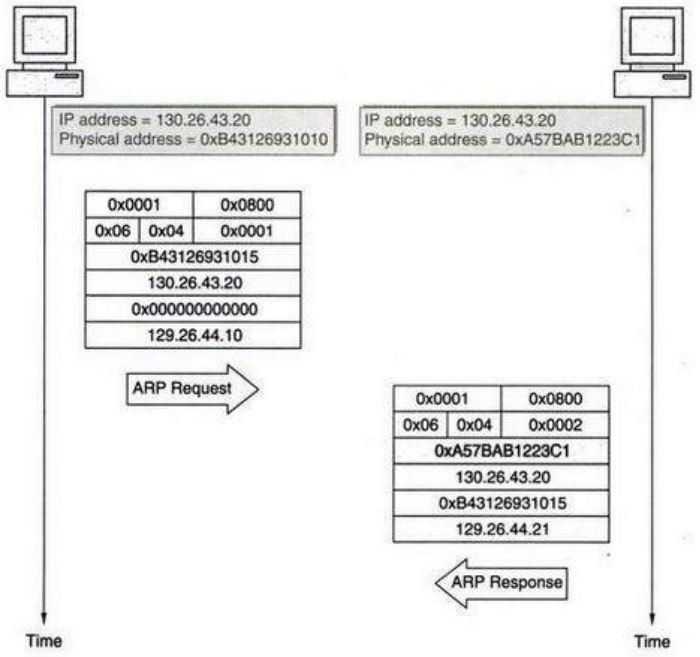
HRD Value	Hardware Type
1	Ethernet (10 Mb)
6	IEEE 802 Networks
7	ARCNET
15	Frame Relay
16	Asynchronous Transfer Mode (ATM)
17	HDLC
18	Fibre Channel
19	Asynchronous Transfer Mode (ATM)
20	Serial Line

Protocol Type: For IPv4 addresses, this value is 2048 (0800 hex), which corresponds to the EtherType code for the Internet Protocol.

Hardware Address Length: Specifies how long hardware addresses are in this message. For Ethernet or other networks using IEEE 802 MAC addresses, the value is 6.



ARP packet format



Sample ARP exchange

ARP Packet format

Protocol Length: For IP(v4) addresses this value is of course 4.

Operation: Specifies nature of ARP message being sent.
1 and 2 for regular ARP.

Opcode	ARP Message Type
1	ARP Request
2	ARP Reply
3	RARP Request
4	RARP Reply
5	DRARP Request
6	DRARP Reply
7	DRARP Error
8	InARP Request
9	InARP Reply

Sender physical Address:

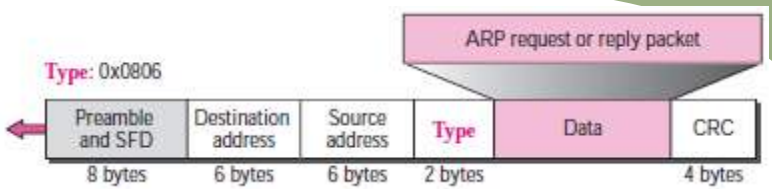
Sender IP Address:

Target physical Address : Empty in request message

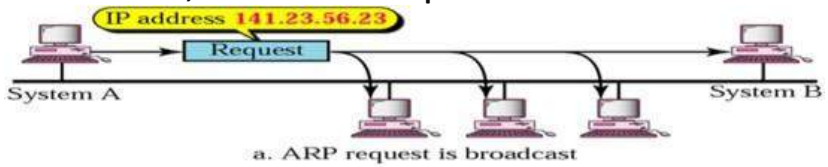
Target IP Address:

ARP

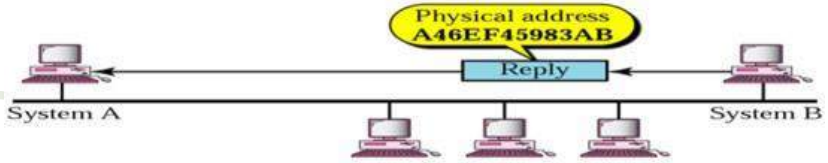
Searching operation:



1. The sender knows the IP address of the target.
2. IP asks ARP to create an ARP request message, filling in the sender physical address, the sender IP address, and the target IP address. The target physical address field is filled with 0s.
3. The message is passed to **the data link layer** where it is encapsulated in a frame using the physical address of the sender as the source address and the physical broadcast address as the destination address.
4. Every host or router receives the frame. Because the frame contains a broadcast destination address, all stations remove the message and pass it to ARP. All machines except the one targeted drop the packet. The target machine recognizes the IP address.
5. The target machine replies with an ARP reply message that contains its physical address. The message is unicast.
6. The sender receives the reply message. It now knows the physical address of the target machine.
7. The IP datagram, which carries data for the target machine, is now encapsulated in a frame and is unicast to the destination.



a. ARP request is broadcast



b. ARP reply is unicast

ARP

Four different cases:

four different cases in which the services of ARP can be used

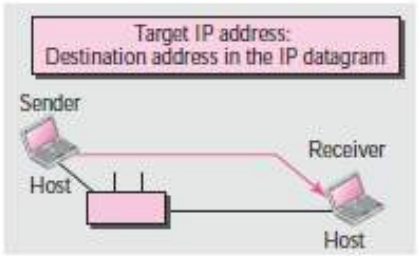
Case 1: The sender is a host and wants to send a packet to another host on the same network. In this case, the logical address that must be mapped to a physical address is the destination IP address in the datagram header.

Case 2: The sender is a host and wants to send a packet to another host on another network. In this case, the host looks at its routing table and finds the IP address of the next hop (router) for this destination. If it does not have a routing table, it looks for the IP address of the default router. The IP address of the router becomes the logical address that must be mapped to a physical address.

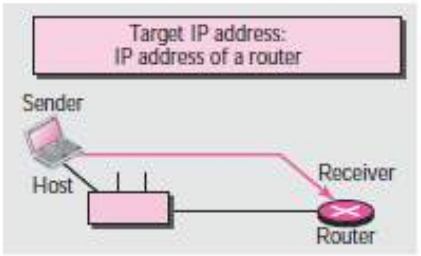
Case 3: The sender is a router that has received a datagram destined for a host on another network. It checks its routing table and finds the IP address of the next router. The IP address of the next router becomes the logical address that must be mapped to a physical address.

Case 4: The sender is a router that has received a datagram destined for a host in the same network. The destination IP address of the datagram becomes the logical address that must be mapped to a physical address.

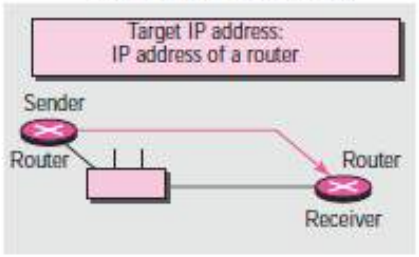
Case 1: A host has a packet to send to a host on the same network.



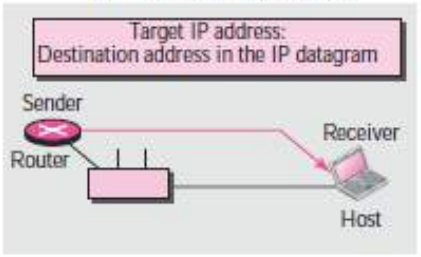
Case 2: A host has a packet to send to a host on another network.



Case 3: A router has a packet to send to a host on another network.

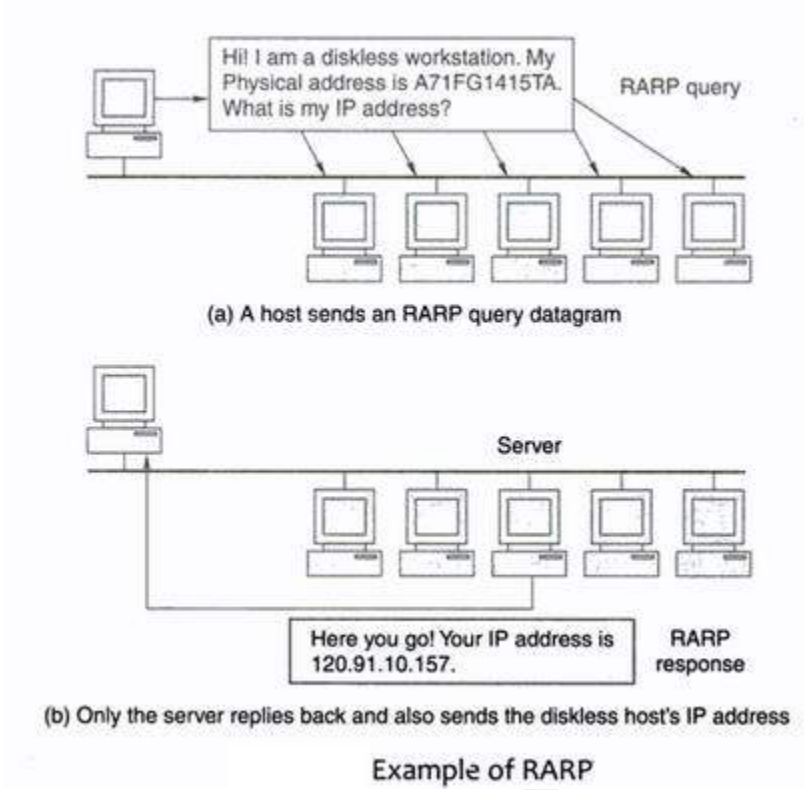


Case 4: A router has a packet to send to a host on the same network.



RARP

- Finds IP address from physical address.
- Used when a new host is connected. Or a hard disk less workstation
- RARP query datagram send to all nodes including server.
- Server recognizes the kind of datagram



Example of RARP

ICMP

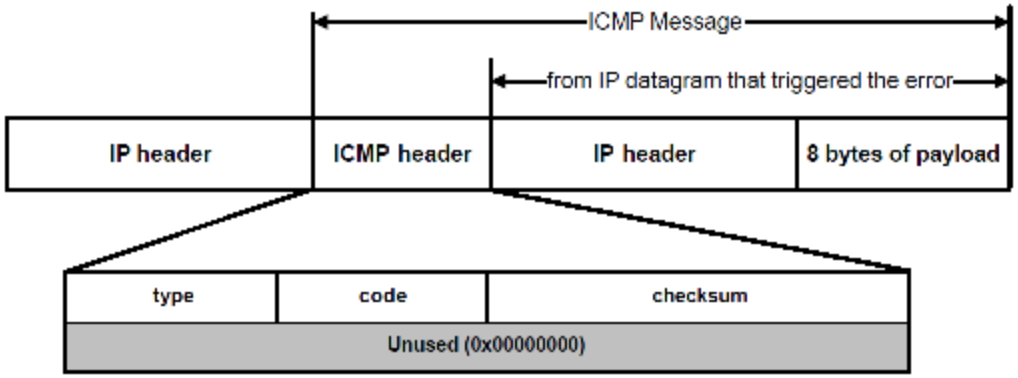
- Internet control message protocol.
- IP does not guarantee datagram delivery correctly while TCP does.
- IP does not have error detection/retransmission/ acknowledgement mechanism. (TCP has)
- The issues of connection management between source to destination, correct delivery are handled by ICMP.
- Let a router receiving datagrams too fast to handle, or may be one host is down, without knowing another host try to send datagram to the host repetedly.
- If this occur to a number of nodes the server may crash.
- ICMP serves as an error reporting mechanism.
- Does not play any role in correction of the problems.
- can be used to show when a particular End System (ES) is not responding, when an IP network is **not reachable**, when a node **is overloaded**, when an **error occurs in the IP header information**, etc. to verify correct operations of End Systems (ES) and to check that routers are correctly routing packets to the specified destination address.

ICMP datagram

- ICMP message:

Type 8bit	Code (error) 8bit	Checksum 16bit

Error Code	Error message
3	Destination unreachable
4	Source quench
5	Redirect
11	Time exceed



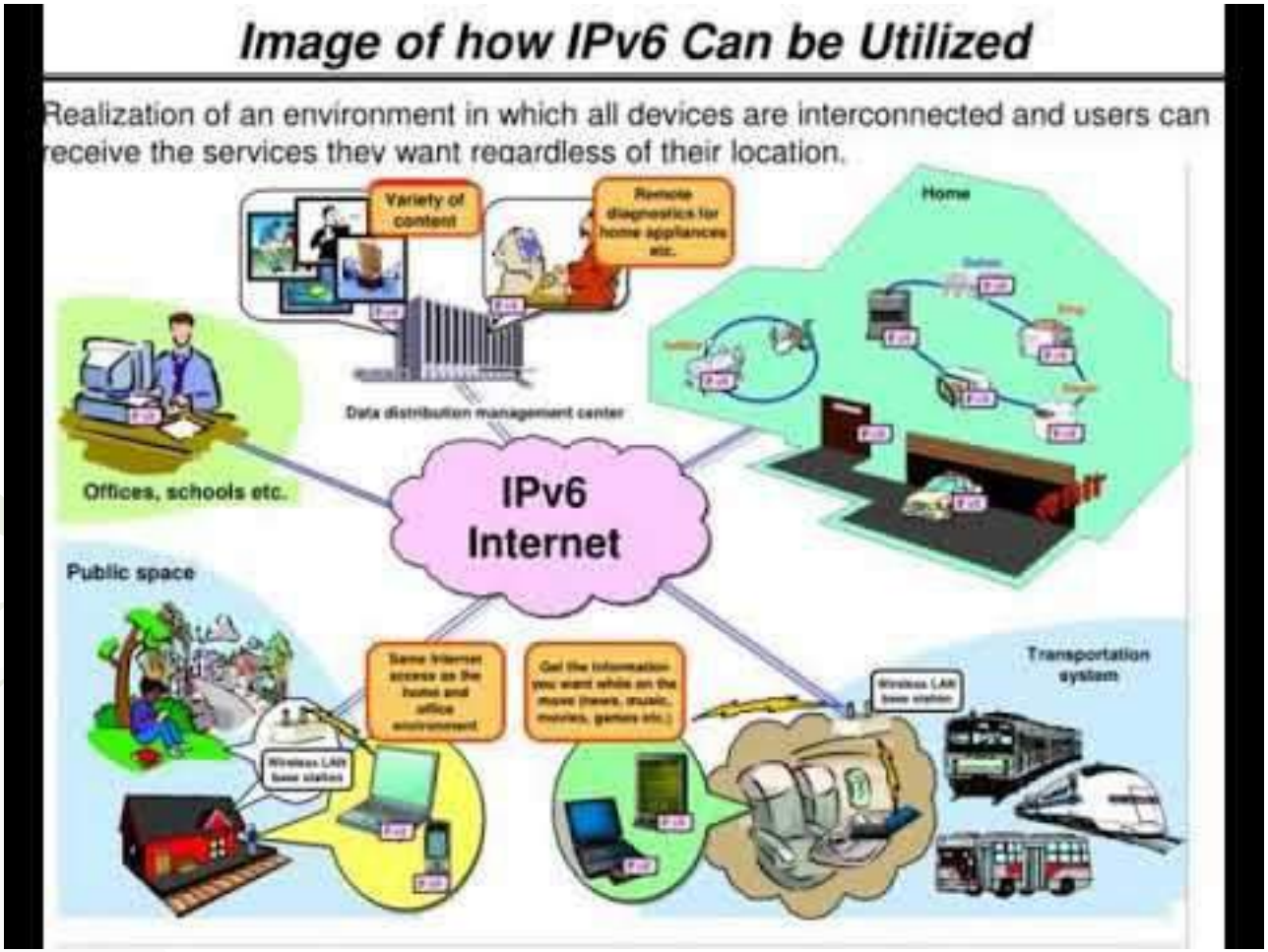
ping

- helps to verify IP-level connectivity.
- use **ping** to send an ICMP echo request to a target host name or IP address.
- Use **ping** whenever you need to verify that a host computer can connect to the TCP/IP network and network resources.

SMTP

- Simple mail transfer protocol
- defined in 1982
- specified for outgoing mail uses
- uses TCP port 25

Shortage of IPV4 address…



For IPv4, this pool is **32**-bits (232) in size and contains **4,294,967,296** IPv4 addresses.

Shortage of IPV4 address…

Class	1st Octet Decimal Range	1st Octet High Order Bits	Network/Host ID (N=Network, H=Host)	Default Subnet Mask	Number of Networks	Hosts per Network (Usable Addresses)
A	1 – 126*	0	N.H.H.H	255.0.0.0	126 ($2^7 - 2$)	16,777,214 ($2^{24} - 2$)
B	128 – 191	10	N.N.H.H	255.255.0.0	16,382 ($2^{14} - 2$)	65,534 ($2^{16} - 2$)
C	192 – 223	110	N.N.N.H	255.255.255.0	2,097,150 ($2^{21} - 2$)	254 ($2^8 - 2$)
D	224 – 239	1110	Reserved for Multicasting			
E	240 – 254	1111	Experimental; used for research			

Note: Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and is reserved for loopback and diagnostic functions.

What happened to IPv5?

- It was designated to an experimental protocol called "**internet streaming protocol**" but unfortunately it was never fully deployed.
- was developed as a means of streaming video and voice data, and it was experimental.
- never transitioned to public use in part because of its 32-bit limitations.
- IPV6 came to play its role

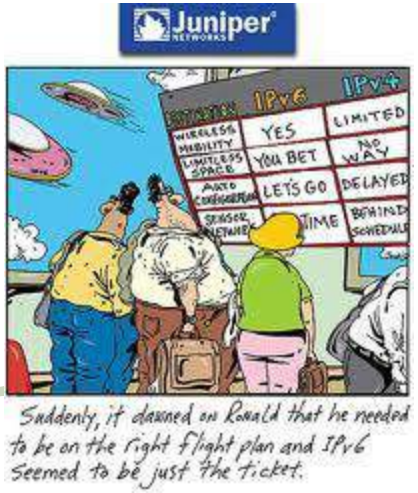
An example of an IPv6 address is 2001:0db8:0000:0000:1234:0ace:6006:001e

IPV6

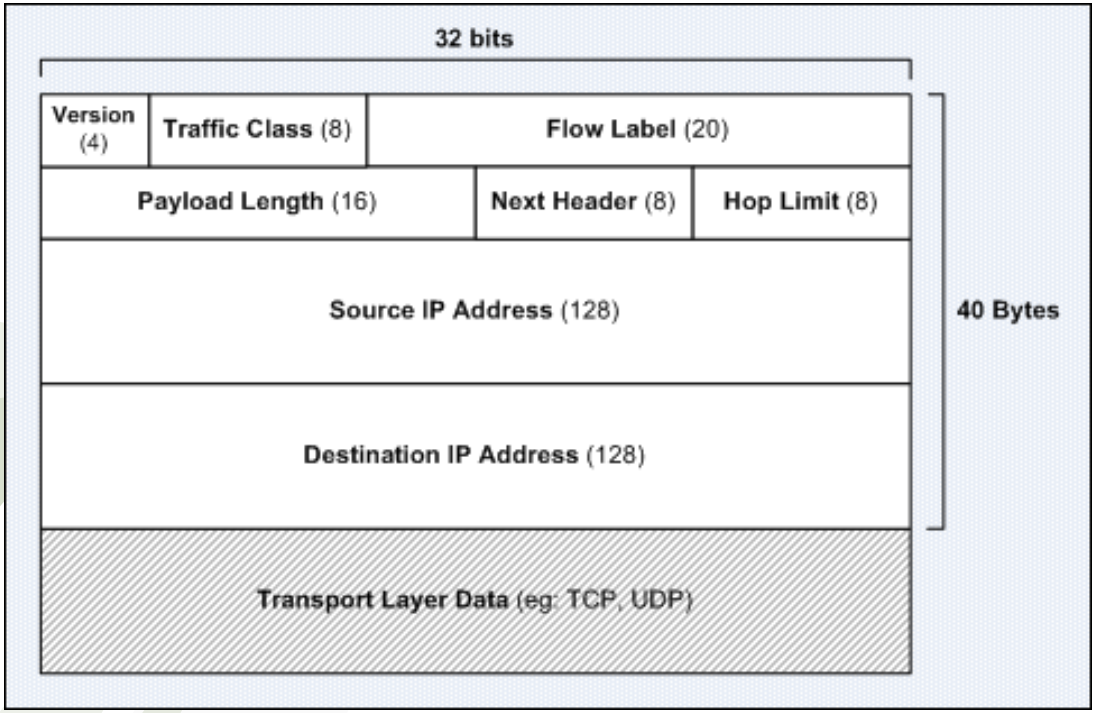
- 32 bit address will be insufficient in coming years to cope up with large number of devices.
- IP addresses are exhausting too fast
- IPV4 is unable to deal real time audio video collaborating technology.
- IP version 6 is also known as IP next generation (IPng).
- Has 128 bit IP address.
- has been under development now since the mid-1990s.
- **IPv6 address** is represented as eight groups of four hexadecimal digits, each group representing 16 bits (two octets, a group sometimes also called a hextet).

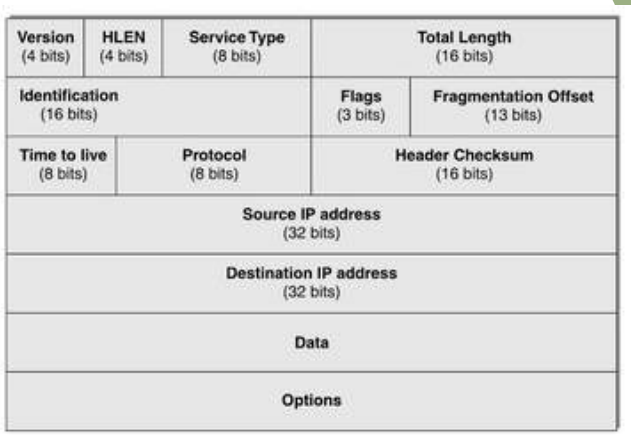
The groups are separated by colons (:).

An **example** : 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

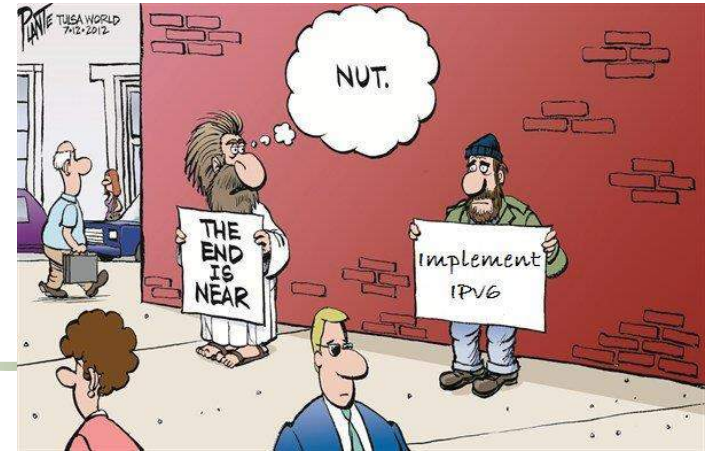


IPV6 Header format





IPV4



IPV6

- **Version:**
  - size 4 bits.
  - shows the version of IP and is set to 6.
- **Traffic Class:**
  - size 8 bits.
  - similar to the IPv4 Type of Service (ToS) field.
  - field indicates the IPv6 packet's class or priority.
- **Flow Label:**
  - size is 20 bits.
  - provide additional support for real-time datagram delivery and quality of service features.
  - The purpose is to indicate that this packet belongs to a specific sequence of packets between a source and destination and can be used to prioritized delivery of packets for services like voice.
- **Payload Length:**

size is 16 bits.

shows the length of the IPv6 payload, including the extension headers and the upper layer protocol data

IPV6

- **Next Header:**
  - size is 8 bits.
  - shows either the type of the first extension (if any extension header is available) or the protocol in the upper layer such as TCP, UDP, or ICMPv6.
- **Hop Limit:**
  - size is 8 bits
  - shows the maximum number of routers the IPv6 packet can travel.
  - similar to IPv4 Time to Live (TTL) field.
  - typically used by distance vector routing protocols, like Routing Information Protocol (RIP) to prevent layer 3 loops (routing loops).
- **Source Address:**
  - size is 128 bits.
  - field shows the IPv6 address of the source of the packet.
- **Destination Address:**
  - size is 128 bits.
  - shows the IPv6 address of the destination of the packet.

Thank You