Nepal Institute of
Engineering

Application layer protocols

- Remote login to hosts: Telnet
- File transfer: File Transfer Protocol (FTP)
- Electronic mail transport: Simple Mail Transfer Protocol (SMTP)
- Networking support: Domain Name System (DNS)
- Remote host management: Simple Network Management Protocol (SNMP)

Web: HTTP

- Hyper Text Transfer Protocol(HTTP)- Heart of web
- Implemented in two Programs
  - Server program
  - Client program
- Server and Client programs exchanges using HTTP msg.
- Defines how web client (web browser) requests pages
  - Browser sends HTTP request to server
  - Server respond with HTTP respond
- HTTP is “Stateless”: HTTP server maintains no information about past client requests, it just sends HTTP respond
- Uses TCP as underlying transport protocol (Port no. 80)

HTTP Methods

- HTTP defines methods to indicate the desired action to be performed on the identified resource.
- GET
    - Retrieve resource specified in the URL(Uniform Resource Locator) from the server[eg. Of URL- http://www.abc.com:80/images/pic.jpg]
        - simple page request
        - run a CGI (***C**ommon* ***G**ateway* ***I**nterface*) program with arguments in URL

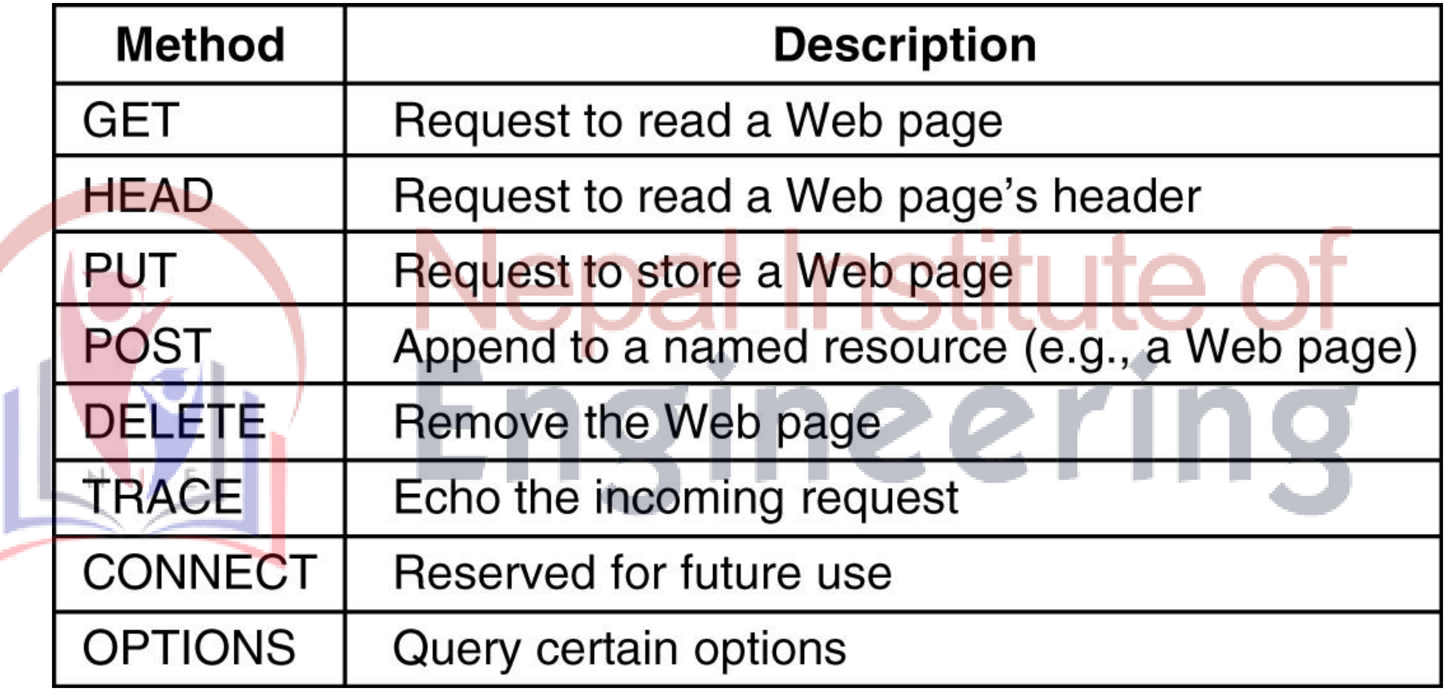
HTTP Methods

- POST
  - preferred method for forms processing
  - run a CGI program
  - parameterized data in SYSIN (SYStem INput)
  - more secure and private than GET
- HEAD
  - requests URLs status header only
  - used for conditional URL handling for performance enhancement schemes
    - retrieve URL only if not in local cache or date is more recent than cached copy
- PUT
  - Used to transfer a file from the client to the server

GET vs POST Method

GET Method	POST Method
Can be bookmarked	Cannot be bookmarked
Can be cached	Cannot be cached
Parameters remain in browser history	Parameters are not saved in browser history
When sending data, the GET method adds the data to the URL and the length of URL is limited(maximum URL length is 2048 characters)	No restriction
Only ASCII characters are allowed	No restriction. Binary data is also allowed
GET is less secure compared to POST Because data sent is part of the URL	POST is little safer than GET because the parameters are not stored in browser history or in web server logs

HTTP Methods



Method	Description
GET	Request to read a Web page
HEAD	Request to read a Web page’s header
PUT	Request to store a Web page
POST	Append to a named resource (e.g., a Web page)
DELETE	Remove the Web page
TRACE	Echo the incoming request
CONNECT	Reserved for future use
OPTIONS	Query certain options

The built-in HTTP request methods.

HTTPS (HTTP Secure)

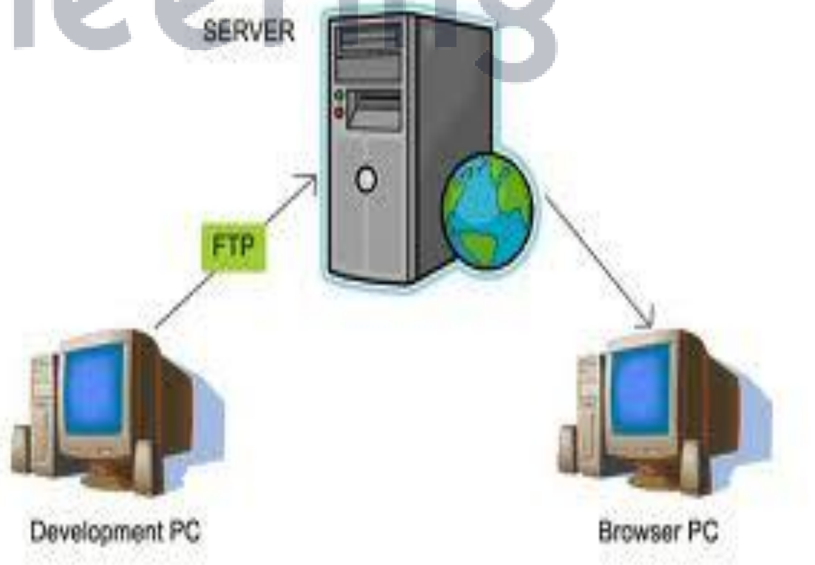
- Use of Secure Socket Layer (SSL) or Transport Layer Security (TLS) as a sub-layer under regular HTTP application layering.
- Encrypts and decrypts user page requests as well as the pages that are returned by the Web server.
- Use of HTTPS protects against eavesdropping and man-in-the-middle attacks. [*eavesdropping: Secretly viewing message*]
- Developed by Netscape.
- HTTPS and SSL support the use of X.509 digital certificates from the server so that, if necessary, a user can authenticate the sender.
- Uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.

HTTP and HTTPS

- HTTPS URLs begin with "https://" and use port 443 by default, whereas HTTP URLs begin with "http://" and use port 80 by default.
- HTTP is insecure and is subject to man-in-the-middle and eavesdropping attacks, which can let attackers gain access to website accounts and sensitive information.
- HTTPS is designed to withstand such attacks and is considered secure against such attacks

FTP (File Transfer Protocol)

- FTP is reliable, connection-oriented service that uses TCP to transfer files between systems that support FTP.
- Protocol for exchanging files from one host to another host typically form your computer to a web server
- The transfer is asynchronous, meaning not at the same time, and therefore faster than other protocols
- Downloading –
  - copying files to your computer
- Uploading –
  - transmit a file from you computer to another computer on internet

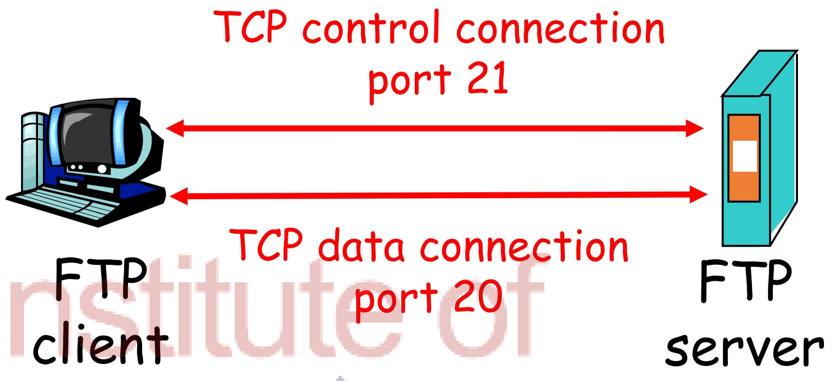


FTP (File Transfer Protocol)

- FTP establishes two connections between the client and server.
  - data transfer and
  - control information.
- The control connection uses simple rules of communication. Only one line of command or a line of response is transferred at a time.
- But the data connection uses more complex rules due to variety of data types being transferred.
- FTP uses port 21 for control connection and port 20 for the data connection.

FTP (File Transfer Protocol)

- Control connection is maintained during the entire FTP session
- The data connection is first opened, file is transferred and connection is closed. This is done for transferring each file.



Electronic Mail (eMail)

Three major components:

- User agents
- Mail servers
- Simple Mail Transfer Protocol: SMTP

User Agent

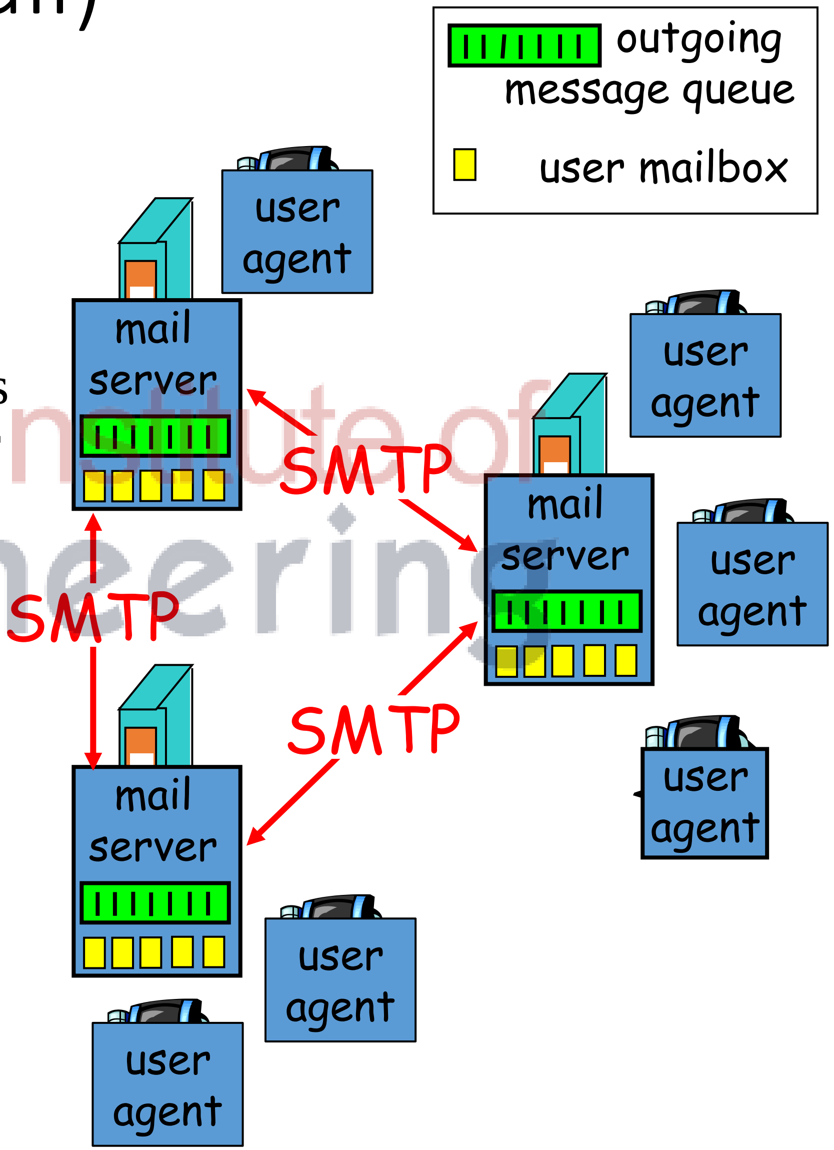
- composing, editing, reading mail messages
- Eg. Eudora, Outlook, Netscape Messenger

Mail Servers

- mailbox contains incoming messages for user
- message queue of outgoing (to be sent) mail messages

SMTP protocol between mail servers to send email messages

- "client": sending mail server
- "server": receiving mail server



SMTP [Simple Mail Transfer Protocol]

- Is principle application-layer protocol for Internet e-mail.
- It uses the reliable transfer service of TCP, uses port 25
- direct transfer: sending server to receiving server
- three phases of transfer
  1) handshaking (greeting)
  2) transfer of messages
  3) closure
- messages must be in 7-bit ASCII
- 7-bit ASCII restriction is a bit of pain- requires binary multimedia data to be encoded to ASCII before being sent over SMTP

Scenario: Alice sends message to Bob

1) Alice uses UA to compose message to: `bob@someschool.edu`

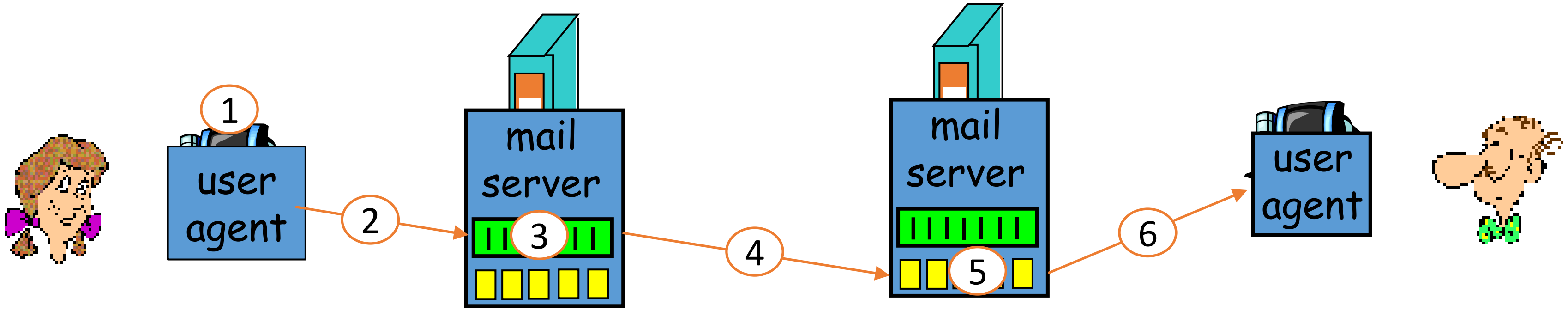
2) Alice's UA sends message to her mail server; message placed in message queue

3) Client side of SMTP opens TCP connection with Bob's mail server

4) SMTP client sends Alice's message over the TCP connection

5) Bob's mail server places the message in Bob's mailbox

6) Bob invokes his user agent to read message



MIME
(Multipurpose Internet Mail Extension)

- Internet standard that extends the format of email to support:
  - Text in character sets other than ASCII
  - Non-text attachments: audio, video, images, application programs etc.

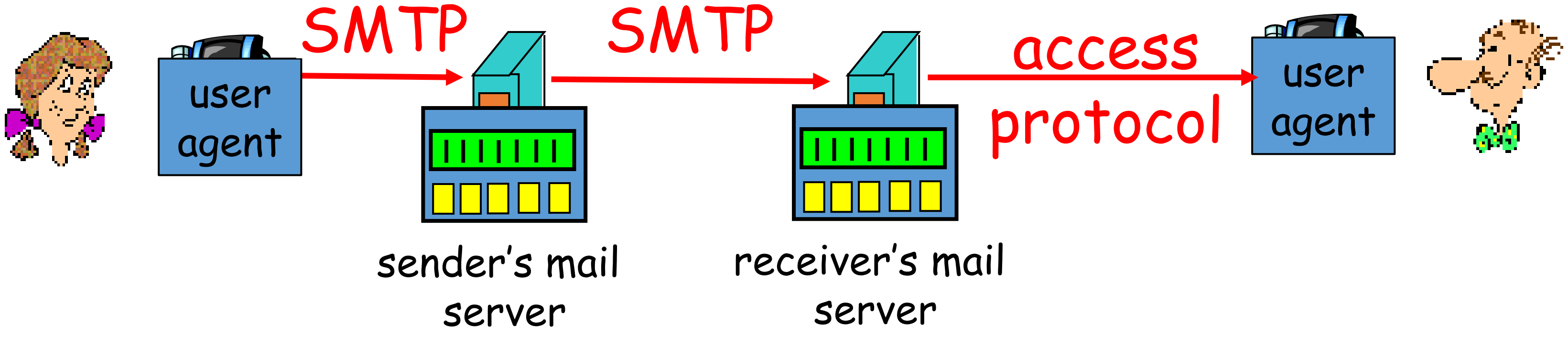
Mail Access Protocol (Pull Protocol)

- SMTP was a Mail Transfer Protocol or push Protocol and
- used to push the mail message up to the receiver’s mail server

- **Mail Access Protocol**: retrieval from server
  - **HTTP** is also used to Compose and retrieve Emails.
  - Also called Web based email.
  - Eg. Hotmail, Yahoo Mail Etc.

Mail Access Protocol (Pull Protocol)

- **POP: Post Office Protocol (POP3)**
  - authorization (agent <-->server) and download (deleted from server)
  - TCP Port no. 110
- **IMAP: Internet Mail Access Protocol**
  - more features (more complex).
  - TCP Port no. 143
  - Remote manipulation of stored messages on server

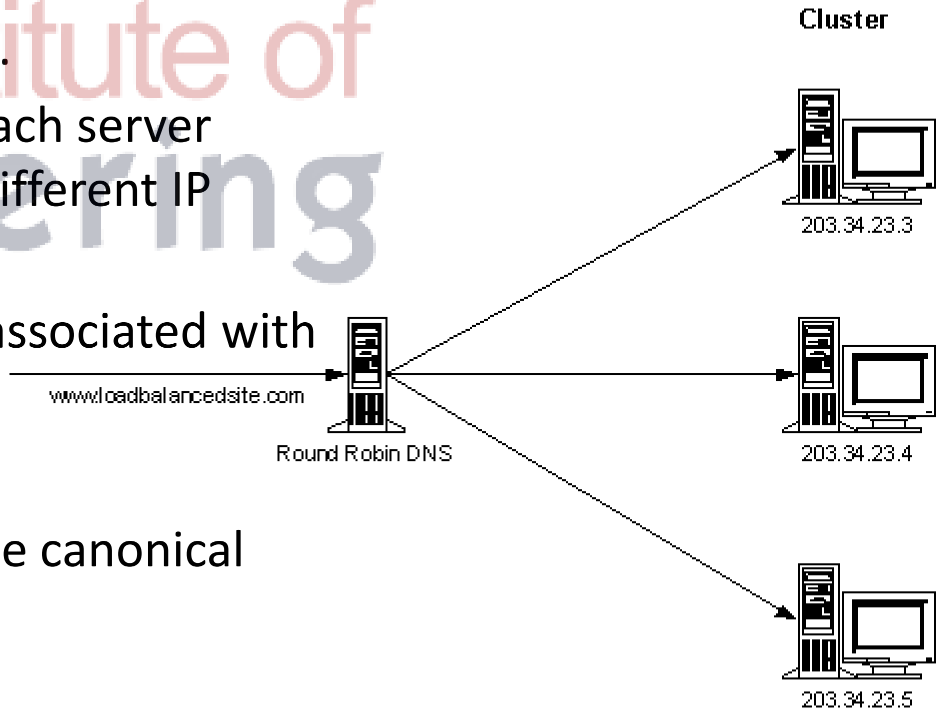


DNS: Domain Name System

- Internet hosts:
  - IP address (32 bit) - used for addressing datagram
  - “name”, e.g., www.yahoo.com - used by humans
- DNS: provides translation between host name and IP address
- distributed database implemented in hierarchy of many name servers
- Distributed for scalability & reliability
- Uses UDP Port no. 53

DNS Services

- Hostname to IP address translation
- Mail server aliasing
  - Permits Company’s mail server and web server to have identical (aliased) hostnames.
  - E.g. wlink.com: for mail server and for web server also.
  - Busy sites are replicated over multiple servers. With each server running on a different end system and each having a different IP address.
  - For replicated web servers, a set of IP address is thus associated with one canonical hostname.
  - Load distribution
    - Replicated Web servers: set of IP addresses for one canonical name



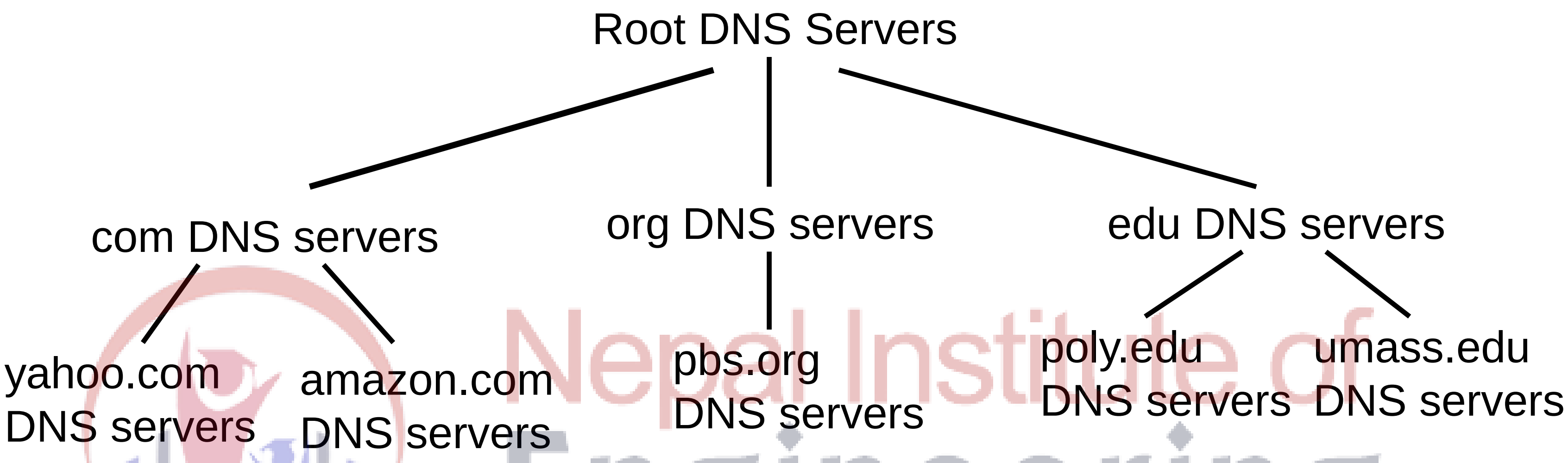
A distributed, Hierarchical database

- 3 classes of DNS servers:
  - Root DNS server
  - Top-level domain (TLD) DNS servers.
  - Authoritative DNS servers.

TLD and Authoritative Servers

- Top-level domain (TLD) servers: responsible for com, org, net, edu, etc, and all top-level country domains uk, fr, ca, jp.
  - Network solutions maintains servers for com TLD
  - Educational institutions use for edu TLD
- Authoritative DNS servers: organization's DNS servers, providing authoritative hostname to IP mappings for organization's servers (e.g., Web and mail).
  - Can be maintained by organization or service provider

Distributed, Hierarchical Database



Client wants IP for www.amazon.com; 1st approx:

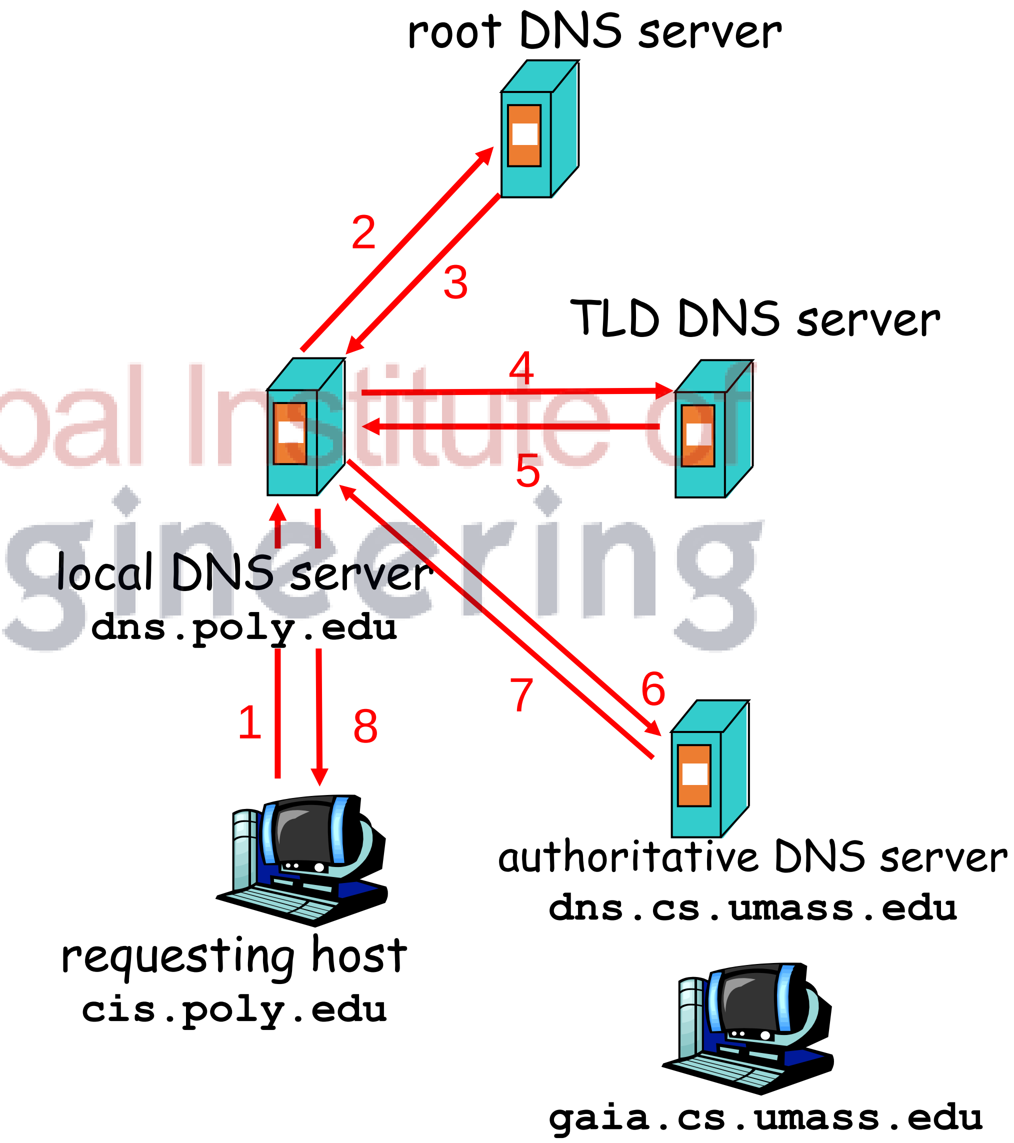
- Client queries a root server to find "com" DNS server
- Client queries com DNS server to get amazon.com DNS server
- Client queries amazon.com DNS server to get IP address for www.amazon.com

Local Name Server

- Does not strictly belong to hierarchy
- Each ISP (residential ISP, company, university) has one.
  - Also called “default name server”
- When a host makes a DNS query, query is sent to its local DNS server
  - Acts as a proxy, forwards query into hierarchy.

Example

Host at cis.poly.edu wants IP address for gaia.cs.umass.edu



DNS records-(Query type)

DNS: distributed database storing Resource Records (RR)

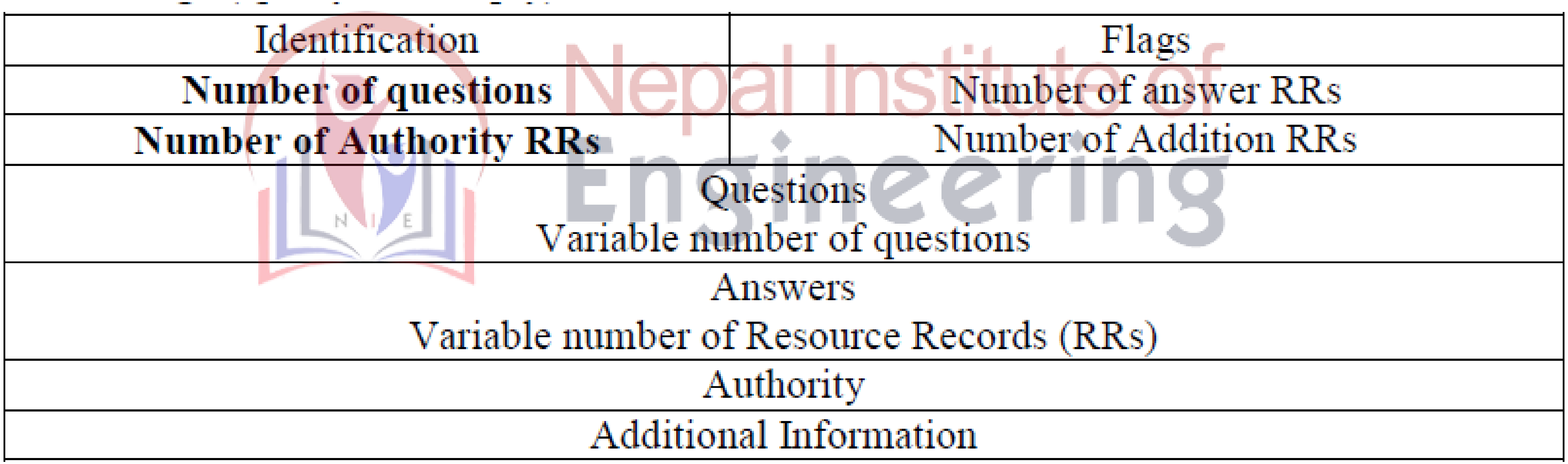
RR format: `(name, value, type, ttl)`

There are 5 types of DNS records:

- **A**
- **CNAME**
- **NS**
- **MX and**
- **PTR**

- **i)** Type =A
  - Address (A) records direct a hostname to a numerical IP address.
  - For e.g., if you want www.urdomain.com to point to IP (which is for e.g. 192.168.0.1) you would enter a record that looks like (www.urdomain.com, 192.168.0.1, A)
- **ii)** Type= CNAME
  - Canonical name (CNAME) allows a machine to be known by one or more host names.
  - There must be always an A record first, and this is known as canonical name or official name.For e.g.: (www.urdomain.com,192.168.0.1,A)
  - Using CNAME, you can point other hostnames to the canonical (A record) address.For example:
    - (fitp.urdomain.com, urdomain.com, CNAME)
    - (mail.urdomain.com, urdomain.com, CNAME)
    - (ssh.urdomain.com, urdomain.com, CNAME)
- **iii)** Type=NS
  - Name server (NS) records specify the authoritative name servers for the domain.
  - For e.g.: urdomain.com, dns.urdomain.com, NS)
- **iv)** Type = MX
  - Mail exchangers (MX) records serve the purpose of using mail server through its web server i.e., canonical name.
  - For e.g.: (urdomain.com, mail.urdomain.com, MX)
- **v)** Type=PTR
  - Pointer (PTR) records are used for reverse lookups.
  - For e.g.: to make 192.168.0.1 resolve the www.urdomain.com the record would look like (1.0.168.192.in addr.arpa, www.urdomain.com, PTR)

DNS message Format



Identification	Flags
Number of questions	Number of answer RRs
Number of Authority RRs	Number of Addition RRs
Questions Variable number of questions	
Answers Variable number of Resource Records (RRs)	
Authority	
Additional Information	

DNS messages

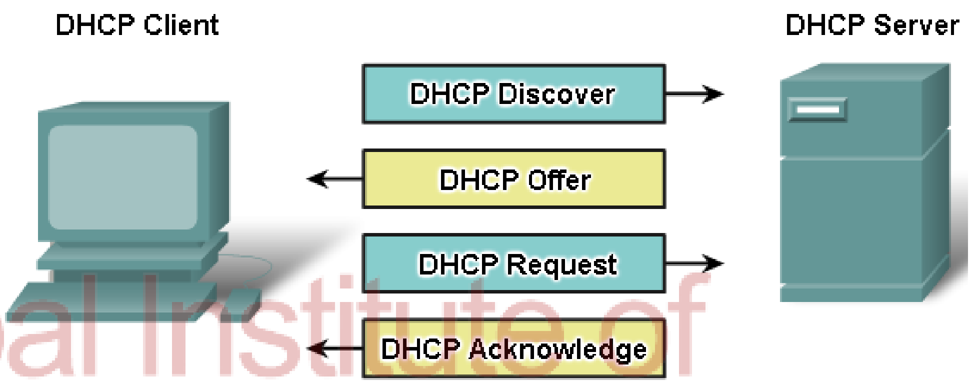
- The first 12 bytes is the header section which has a number of fields.
- The first field is a 16-bit number that identifies the query. This identifier is copied into the reply message to a query allowing the client to match received replies with sent queries.
- There are a number of flags in the flag field.
  - A 1 bit query/reply flag indicates whether the message is a query (0) or a reply (1).
  - A 1-bit authoritative flag is set in a reply message when a DNS server is an authoritative server for a queried name.
  - A 1-bit recursion-desired flag is set when a client (host or DNS server) desires that the DNS server perform recursion when it doesn’t have the record.
  - A 1-bit recursion available field is set in a reply if the DNSserver supports recursion.

DNS messages

- The question section contains information about the query that is being made.
- This section includes
  - a) A name field that contains the name that is being queried.
  - b) A type field that indicates the type of question being asked about the names for e.g. a host address associated with a name (Type A) or the mail server for the name (Type MX)
- In a reply form a DNS server the answer section contains the resource records for the name that was originally queried. Recall that in each resource record there is the Type (for e.g.: A, NS, CNAME, or MX), the value and the TTL. A reply can return multiple RRs in the answer.
- Since a hostname can have multiple IP addresses (for e.g. for replicated web servers, as discussed earlier in the section). The authority section contains records of other authoritative servers.
- The additional section contains other helpful records. For e.g.: the answer field in a reply to an MX query contains a resource record providing the canonical hostname of a mail server. The additional section contains a Type A record providing the IP address for the canonical hostname of the mail server.

Dynamic Host Configuration Protocol (DHCP)

- When a DHCP-configured device boots up or connects to the network, the client broadcasts a DHCP DISCOVER packet to identify any available DHCP servers on the network



A DHCP server replies with a DHCP OFFER, which is a lease offer message with an assigned IP address, subnet mask, DNS server ... etc

- The client might choose from multiple DHCP OFFERs it receives and broadcast a DHCP REQUEST
- If the DHCP OFFER is still available the DHCP server will reply with DHCP ACKNOWLEDGE
- If the DHCP OFFER is not available the server with reply with DHCP NAK the process will start all over again

Proxy Server (Web Caching)

- Dedicated server that stores caching information in between the client and the web server in a shared location so that all clients can use the same shared data.

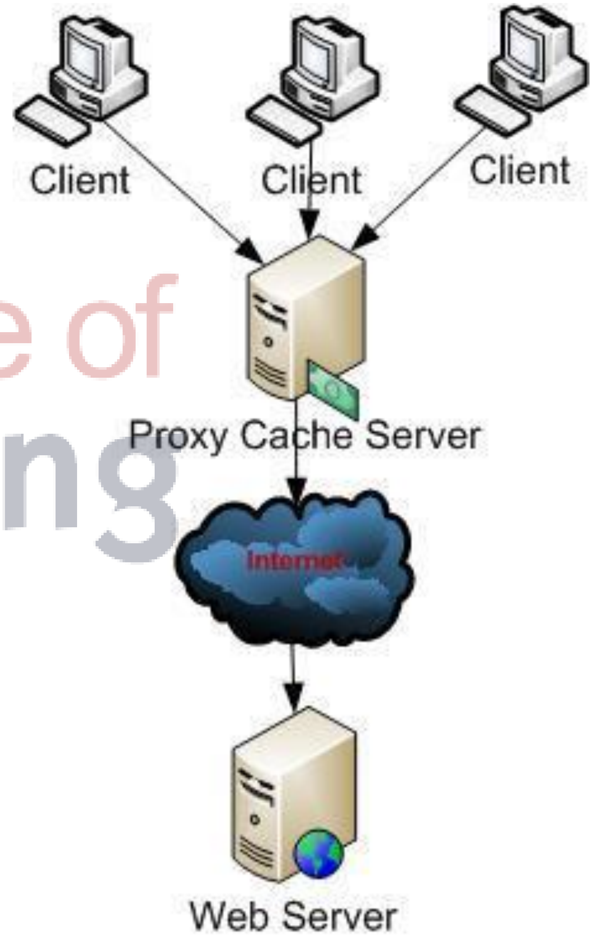
Main Uses of proxy server:

-Caching:

  - When a user accesses a web page, that page is temporarily stored in the proxy cache.
  - Then, when a subsequent user requests the same web page, they access the copy in the proxy cache, rather than having the web page sent again from the originating server.
  - It improves performance and frees up Internet bandwidth for other tasks.

-Filtering: Allows to block specific sites

- Maintain Privacy: Can hide actual IP address of Client from the outside world



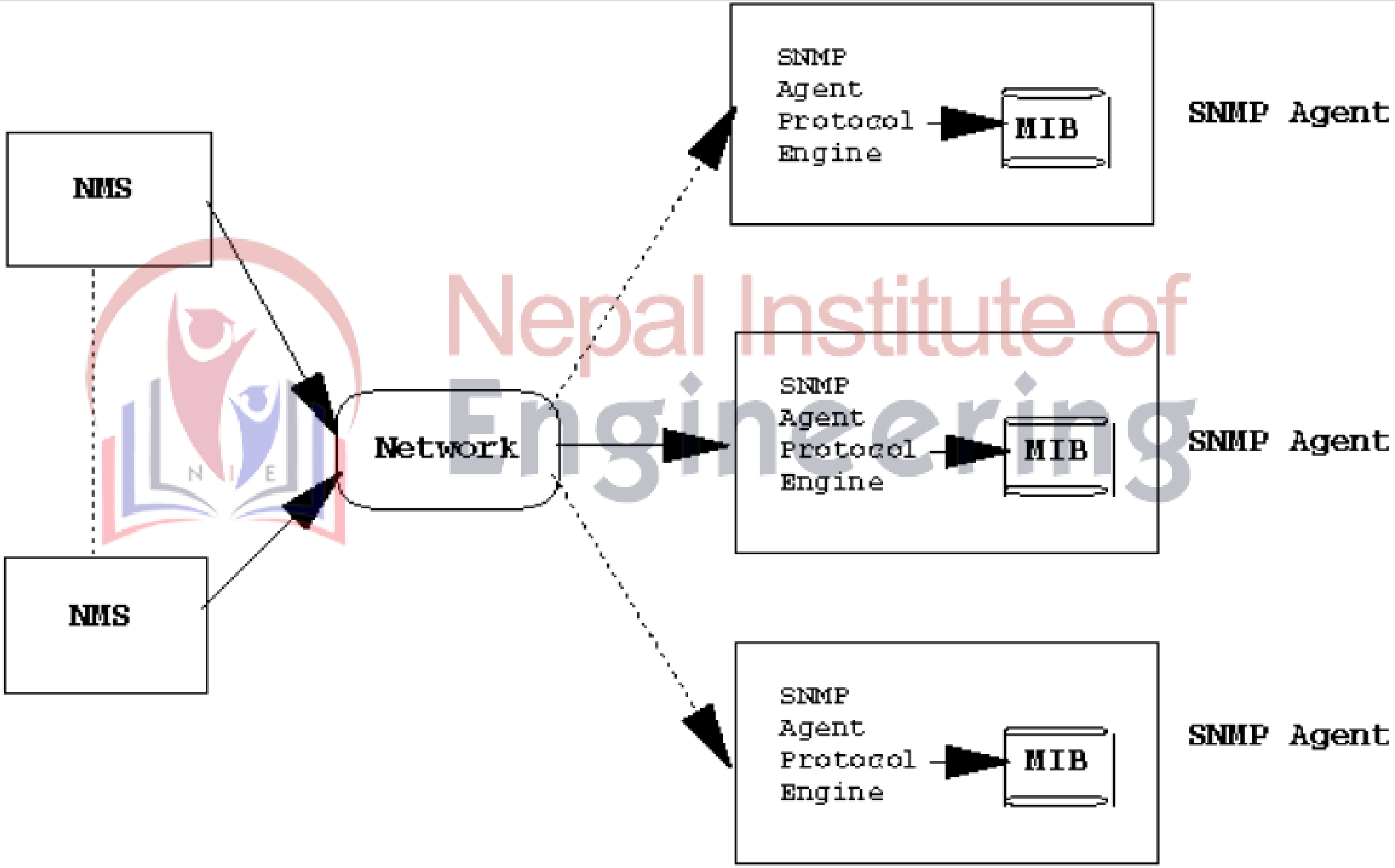
TELNET

- *TELNET* – It provides bi-directional text-oriented services for remote login to the hosts over the network. **TELNET (Terminal Network):**
- TELNET is client-server application that allows a user to log onto remote machine and lets the user to access any application program on a remote computer.
- TELNET uses the NVT (Network Virtual Terminal) system to encode characters on the local system.
- On the server (remote) machine, NVT decodes the characters to a form acceptable to the remote machine.
- TELNET is a protocol that provides a general, bi-directional, eight-bit byte oriented communications facility.
- Many application protocols are built upon the TELNET protocol
- Telnet services are used on PORT 23.

Simple Network Management Protocol, SNMP

- ***Simple Network Management Protocol, SNMP*** – It is for managing, monitoring the network and for organizing information about the networked devices.
- **Simple Network Management Protocol (SNMP)** is an "Internet-standard protocol for managing devices on IP networks.
- Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more.
- It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.
- *The Simple Network Management Protocol (SNMP) is a framework for managing devices in an Internet using the TCPIIP protocol suite. It provides a set of fundamental operations for monitoring and maintaining an Internet.*
- **An SNMP-managed network consists of three key components:**
  - Managed device
  - Agent — software which runs on managed devices
  - Network management system (NMS)— software which runs on the manager

Architecture


NMS
NMS
Network
SNMP Agent Protocol Engine
MIB
SNMP Agent
SNMP Agent Protocol Engine
MIB
SNMP Agent
SNMP Agent Protocol Engine
MIB
SNMP Agent

SNMP

- **To do management tasks, SNMP uses two other protocols:**

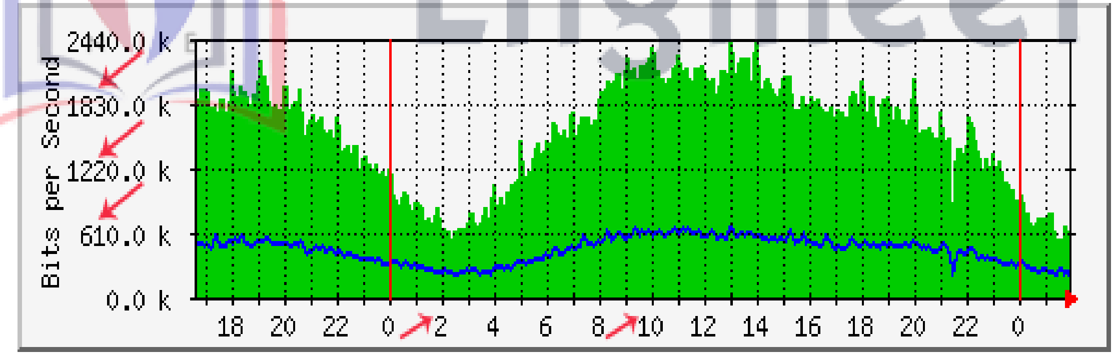
1. Structure of Management Information (SMI)
2. Management Information Base (MIB).

- **A typical agent usually:**
  - Implements full SNMP protocol.
  - Stores and retrieves management data as defined by the Management Information Base
  - Can asynchronously signal an event to the manager
  - Can be a proxy (The proxy agent then translates the protocol interactions it receives from the management station) for some non-SNMP manageable network node.

- **A typical manager usually**:
  - Implemented as a Network Management Station (the NMS)
  - Implements full SNMP Protocol
  - Able to Query agents
  - Get responses from agents

Multi Router Traffic Grapher (MRTG)

- The **Multi Router Traffic Grapher** (MRTG) is free software for monitoring and measuring the traffic load on network links.
- It allows the user to see traffic load on a network over time in graphical form.
- It was originally developed by Tobias Oetiker and Dave Rand to monitor router traffic, but has developed into a tool that can create graphs and statistics for almost anything.
- MRTG is written in Perl and can run on Windows, Linux, Unix, Mac OS and NetWare.



How it works

- **SNMP**

✓ MRTG uses the **Simple Network Management Protocol** (SNMP) to send requests with two object identifiers (OIDs) to a device.

✓ The device, which must be SNMP-enabled, will have a management information base (MIB) to look up the OIDs specified.

✓ After collecting the information it will send back the raw data encapsulated in an SNMP protocol.

✓ MRTG records this data in a log on the client along with previously recorded data for the device.

✓ The software then creates an HTML document from the logs, containing a list of graphs detailing traffic for the selected devices in the server.

- **Script output**

✓ Alternatively, MRTG can be configured to run a script or command, and parse its output for counter values.

✓ The MRTG website contains a large library of external scripts to enable monitoring of SQL database statistics, firewall rules, CPU fan RPMs, or virtually any integer-value data.

Paessler Router Traffic Graphic (PRTG)

- **PRTG** Network Monitor (Paessler Router Traffic Grapher until version 7) is an agentless network monitoring software from Paessler AG.
- It can monitor and classify system conditions like bandwidth usage or uptime and collect statistics from miscellaneous hosts as switches, routers, servers and other devices and applications.
- Specification:-
- PRTG Network Monitor has an auto-discovery mode that scans predefined areas of an enterprise network and creates a device list from this data.
- In the next step, further information on the detected devices can be retrieved using various communication protocols.
- Typical protocols are Ping, SNMP, WMI, NetFlow, jFlow, sFlow, but also communication via DICOM or the RESTful API is possible.
- The tool is only available for Windows systems. In addition, Paessler AG offers the cloud-based monitoring solution "PRTG hosted by Paessler"

- **1.1 Sensors**
- The software is based on sensors that are configured for a specific purpose. For example, there are HTTP, SMTP/POP3 (e-mail) application sensors and hardware-specific sensors for switches, routers and servers. PRTG Network Monitor has over 200 different predefined sensors that retrieve statistics from the monitored instances, e.g. response times, processor, memory, database information, temperature or system status.
- 1.2 **Web interface and desktop client**
- The software can be operated completely via a AJAX-based web interface. The web interface is suitable for both real-time troubleshooting and data exchange with non-technical staff via maps (dashboards) and user-defined reports. An additional administration interface in the form of a desktop application for Windows and macOS is available.
- **1.3 Notification and reports**
- In addition to the usual communication channels such as Email and SMS, notification is also provided via push notification on smartphones using an app for iOS or Android. PRTG also offers customizable reports.
- **1.4 Pricing**
- PRTG Network Monitor's licensing is based on sensors. Most devices require between five and ten sensors to be fully monitored. A version with 100 integrated sensors is available free of charge.

Packet Analyzer

- A packet analyzer (also known as a **packet sniffer)** is a computer program or piece of computer hardware (such as a packet capture appliance) that can intercept and log traffic that passes over a digital network or part of a network.
- Packet capture is the process of intercepting and logging traffic.
- A packet analyzer used for intercepting traffic on wireless networks is known as a wireless analyzer or WiFi analyzer.
- A packet analyzer can also be referred to as a network analyzer or protocol analyzer though these terms also have other meanings.
- ***Packet sniffers can:***
- Analyze network problems
- Detect network misuse by internal and external users
- Monitor WAN bandwidth utilization
- Gather and report network statistics

Wireshark

- Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format.
- Wireshark includes filters, color coding, and other features that let you dig deep into network traffic and inspect individual packets.
- Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.
- **Features:-**
- Wireshark is a data capturing program that "understands" the structure (encapsulation) of different networking protocols.
- Data can be captured "from the wire" from a live network connection or read from a file of already captured packets.
- Live data can be read from different types of networks, including Ethernet, IEEE 802.11, PPP, and loopback.
- Data display can be refined using a display filter.
- Wireless connections can also be filtered as long as they traverse the monitored Ethernet.
- Various settings, timers, and filters can be set to provide the facility of filtering the output of the captured traffic