Lecture 1.

Internet network of networks/interconnected ISPs

Hosts = end systems

Network edge: hosts: clients and servers where servers often in data centers.

Network core: mesh of interconnected routers; network of networks.

How to connect to edge router: residential access nets; institutional access; mobile access.

DSL (digital subscriber line) data to internet, voice to telephone net.

HFC: hybrid fiber coax: asymmetric up to 30mbps downstream and 2 mbps upstream.

Fiber attaches homes to ISPs while DSL to access center.

Ethernet in companies/universities (10,100, 1024, 10240 mbps transmission rates) switch

Wireless end systems (lans/buildings 11, 54 mbps wide area/cellular 1-10mbps/3g 4g) router.

Host sends packets: **transmission** delay = Length(bits) / R [transmission rate = bandwidth] (bit/s).

Media: Communication links: guided fiber, copper, unguided radio, satellite.

|  |  |  |
| --- | --- | --- |
| Twisted pair | Coaxial cable | Fiber optic cable |
| Two insulated copper wires | Two concentric copper  Bidirectional  Broadband | Glass fiber carrying light  High-speed operation  Low error rate |

Packet- switching: host breaks mess. Into chunks and forwards them from one router to the next across links on path from source to destination at full link capacity. Each packet may have different route. In header info where to go.

Store-and-forward – l/r seconds to transmit, entire packet must arrive at router before it can be transmitted on next link. **End-end** delay = 2l/R.

Queueing: arrival rate exceeds transmission rate.

Packets can be lost/dropped if mem/buf fills up.

Routing determines source-destination route taken by packets.

Forwarding: move packets from router’s input to appropriate router output.

Circuit switching: dedicated point-to-point connection (no sharing).

Why layering? Explicit structure allows not to confused in complex system.

Application: FTP, SMTP, HTTP

Transport: TCP, UDP

Network: IP routing protocols

Link: IEEE, PPP

Physical: bits

Virus – self-replicating infection by receiving/executing object.

Worm- self-replicating infection by passively receiving object that gets itself executed.

Spyware malware can record keystroke’s, web sites visited, upload info to collection site.

Infected host can be enrolled in botnet, used for spam (DDoS) attacks.

Denial of service (DoS) – overwhelming resource with bogus traffic.

Sniffing – broadcast media,

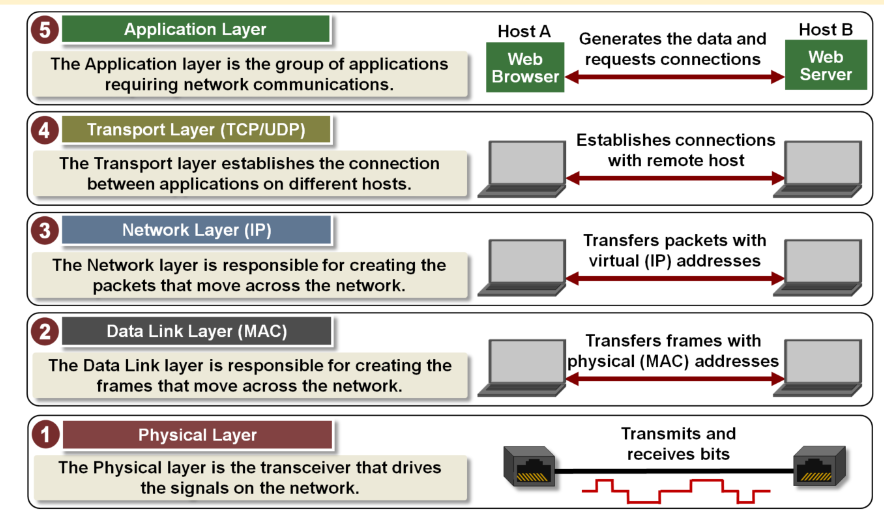
Ip spoofing – send packet with false source address.

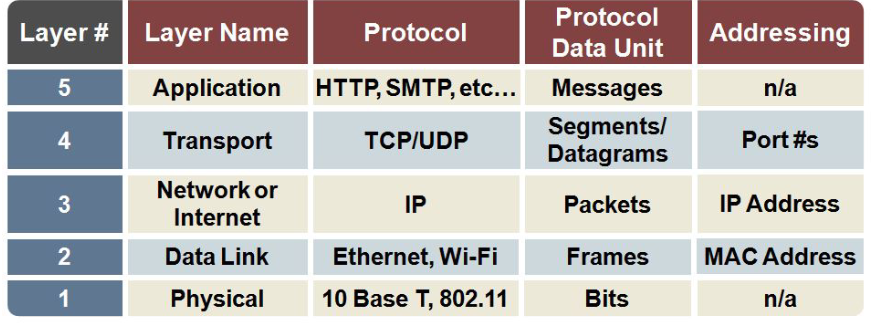
Lecture 2

Proprietary systems – uses technologies kept private by a particular commercial vendor.

Interoperability – ability of software and hardware from diff commercial vendors to communicate.

Open system – common model of network architecture and protocols used in its implementation.





Server always on host; permanent IP address; data center for scaling.

Client: communicate with server; may be intermittently connected; may have dynamic IP; do not com. directly.

App-layer defines: types of message exchanged: request/response

Message syntax: what filed/ how they delineated

Massage semantics: meaning of info

Rules: when and how send/respond

Open protocols: HTTP, SMTP

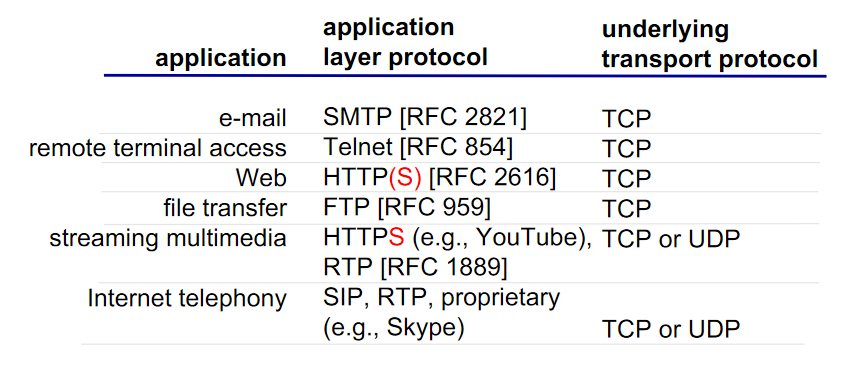
Proprietary protocols: Skype

Services app needs: data integrity; timing; throughput; security.

Network protocol set of rules communicate network applications including how exchanged data, transmit and receive.

Various protocols are available: speed; reliability; persistency; statelessness.

UDP: data transfer; provides reliability, flow control, congestion control, timing, throughput guarantee, security and connection setup.



Stateless (HTTP) maintains no info about past client requests.

Non-persistent 1. Open connection 2. Server accepts connection 2. Request message 3. Response message 4. Close connection 5. Client receives response. 6. Steps from 1-5 repeated. 2RTT

Persistent – 1 RTT

RTT – time for a small packet to travel form server client to server and back.

HTTP response time 1 RTT init, 1 RTT for HTTP request, file transmission => 2RTT + transmission

HTTP1.0 (get, post, head) HTTP 1.1 support persistent (Get, post, head put, delete) HTTP/2 used by default.

Post web page input to server in entity body.

Get URL input in URL field of request line.

HTTP statuses 200 ok, 301 moved permanently, 400 bad request, 404 not found, 505 http version not sup.

Cookies: response mess, request mess, cookie file on user host, back-end database.

Web caches: satisfy request without involving original server it acts as both client and server installed by ISP

Lab1

Curl: DNS-> con establish-> client get -> server response -> connection termination.

-h ‘connection: keep-alive’

Lecture 3.

1970’s ARPANET maintained by SRI-NIC pulled from a single machine.

1983 Paul **DNS (**RFC 1034 and 1035**). IP** address (32 bit) used for addressing datagrams.

Domain Name system: distributed database hierarchy of many name servers. Distributed, loosely coherent, scalable, reliable, dynamic database. Three components: ‘name space’, servers, resolvers.

Application-layer protocol: hosts, name servers communicate to resolve names.

Maintained locally, retrievable globally. Lookup from any device. Cache-able to improve performance.

Database can be updated dynamically -> add/delete/modified. Only master updates master database.

Goal: hostname to IP address translation, host aliasing, mail server aliasing, load distribution.

Decentralized: single point of failure, traffic volume, maintenance, security.

Root name servers contacted by local name servers there 13 root name servers worldwide.

DNS label presentation format. Each string between two ‘.’

DNS zone a set of names that are under the same authority.

Delegation transfer of authority for a domain. Example.org is delegation of org.

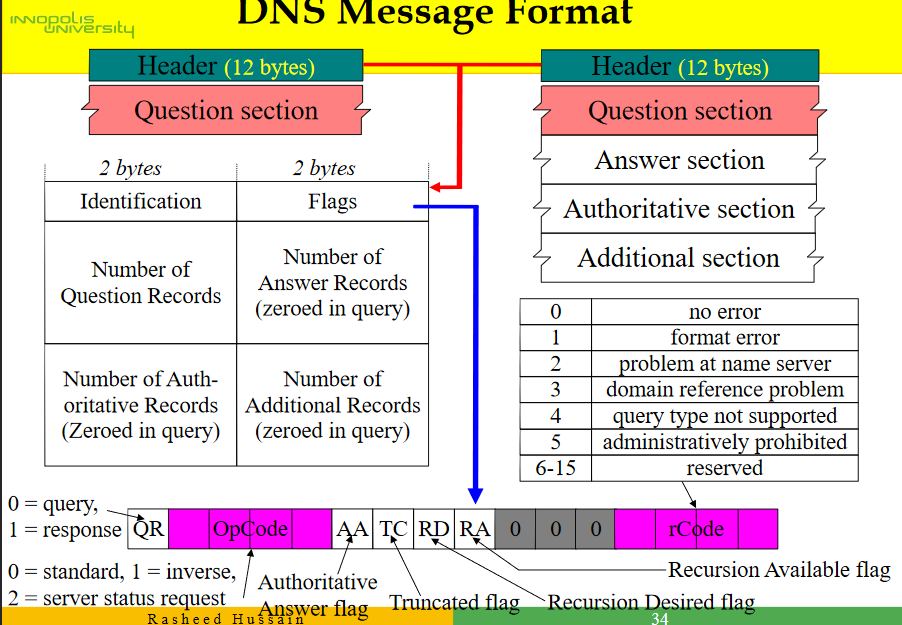
RR: a single Resource Record

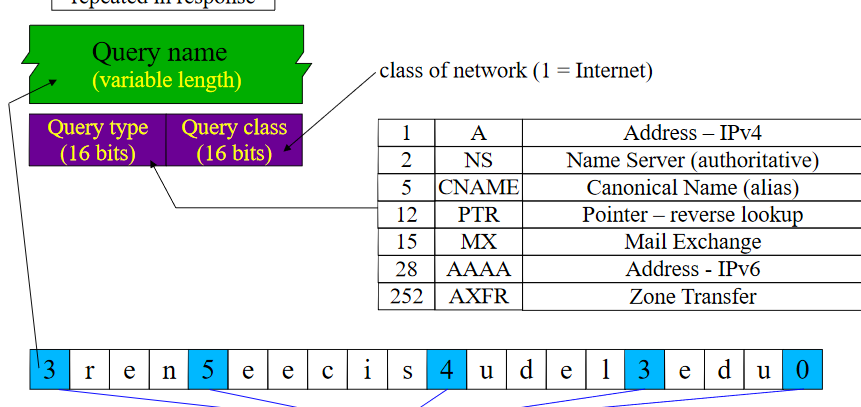
RRSet: all RRs of same type at a name.

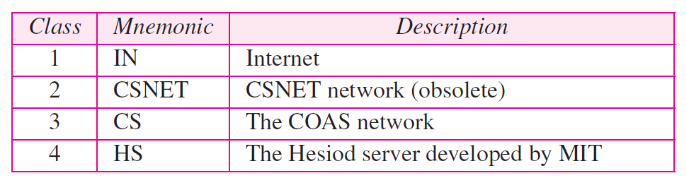
TTL time to live The time an RRSet can be cached/reused by a non-authoritative server.

Resolver: stub simple, only asks questions recursive takes simple query and makes all steps to get the full answer.

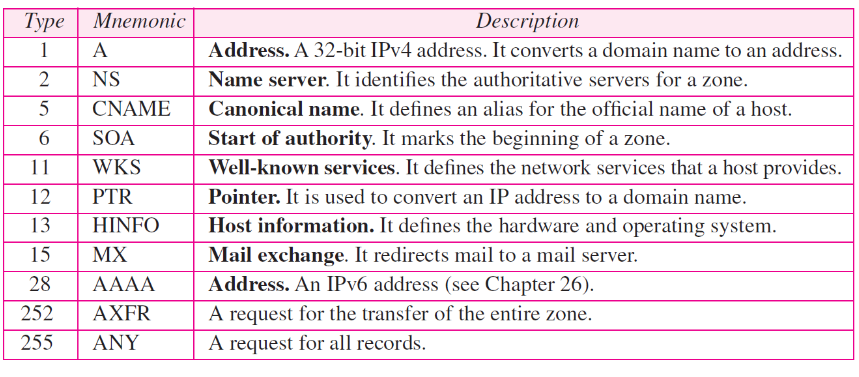
Server: Authoritative the servers that contain the zone file for a zone one Primary and one or more secondary. Caching a recursive resolver that stores prior results and reuses them.







Nslookup DNS to IP and reverse.



DNS maps names into data using Resource Records.

DNS query have name and type. RR is response to query(name, value, type and TTL).

One machine can have many aliases as well as one alias multiple machines.