Network Notes

Oct.2019

XU Kangyan

1. **Client-Server Architecture**
   Server: Always-on host / Permanent IP Address
   Client: No directly communicate / may dynamic IP Address
2. **Peer to Peer (P2P)**
   No always-on server / arbitrary end systems directly communicate
3. **CDN:** Content Delivery Network (all over world only store replica)
4. **ISP:** Internet Service Provider
5. **Hub:** fastest, identify no address
   Switch: only identify MAC address
   Router: identify MAC and IP address
6. In **switched network**, the switch "reassemble" the frame and check the "header" of the frame to read the "destination" MAC address. Then, consult with "forward database" that maps MAC address to physical port and forward bits to the port.
7. **Internet** is worldwide, publicly accessible network of inter-connected computer networks that transmit data by *packet switching*, using the standard "Internet Protocol"(IP). It is a "network of networks".
8. IP(unreliable) / TCP(reliable) / UDP(unreliable)
9. The two most important network performance measures are **Delay**(sec) and **Throughput**(bps).
10. **End to End delay:** Tp, Tt, Tprocess(random), Queue Delay(random)
11. **Bandwidth:** The maximum amount of data that can travel through a channel (bps or Hz).
    Throughput: how much data actually does travel through the channel *successfully*.
12. **RTT:** Round Trip Time
13. loss and delay reason: packets queue in buffer / packets arrival rate exceeds output rate / packets queue wait for turn
14. **Rb:** *Data Rate*, the rate of which the bits are transmitted.
15. **Bandwidth delay product:** the maximum number of bits can be inserted in the link in a given interval of time (Tp or RTT).
16. **OSI(Open System Interconnection) Model: Application** / presentation / session / **Transport**(TCP segment or UDP datagram) / **Network**(IP packet) / **Datalink**(frame) / **Physical**
17. **IP address:** net id & host id (assigned by local administer) 32bits
    MAC Address: 48bits
    Port number: 16bits identify application

18. FOUR QUESTIONS

Q: How does a host/router *get the MAC address* of another host /router on the same LAN?

A: **ARP (Address Resolution Protocol)**

Q: How does a host *get the IP address* of another host across the Internet?

A: **DNS (Domain Name System)**

Q: How does a host *get its own IP address*?

A: **DHCP (Dynamic Host Configuration Protocol)**

Q: How do we distinguish between two or more applications running on the same host?

A: Port Numbers / Sockets

19. DHCP: C Discovery / S Offer / C Request / S Acknowledge

DHCP server: not necessary on each network / might more than one

Transaction ID

Both client & server side are well-known port number (S-67 C-68).

Return Your IP / Router IP / DNS Server IP / subnet mask ...

20. DNS

Local Name Server: The default name server that will receive the DNS query from the host.

Root Name Server

Authoritative Name Server: Where the host register its name/IP address.

Recursive / Iterative

21. A **socket** is an abstract representation of a communication endpoint.

A socket allows the application to "plug in" to the network and communicate with other applications.

A socket is uniquely identified by the IP address, port number and the underlying transport layer protocol.

Parent socket / child socket

Socket types: reliable(TCP) / unreliable(UDP)

22. Multiplexing

Statistical TDM (used in internet): Time slots allocated dynamically based on demand, time slots needn't of same duration, every time slots need to be processed by a header.

Synchronous TDM (used in telephone): many slots wasted.

23. HTTP: persistent(w or w/o pipelining) / non-persistent(parallel or serial)

24. single parity check

25. FCS: Frame Check Sequence

26. Bit stuffing: used to avoid confusion with data containing 01111110.

27. Protocols define format, order of messages and received among network entities, and actions taken on message transmission, receipt.
28. Error Control: Stop-and-wait ARQ / **Sliding Window ARQ** (**Go-Back-n / selective reject**)

ARQ: Automatic Repeat Request

Stop-and-wait: send one frame at a time

Sliding window: send several frames at a time

SWS: sender window size (max number of frames the sender can send before he has to stop)

RWS: receiver window size (max number of frames the receiver is willing to receive)

Go-Back-n: SWS <= $2^m - 1$ / RWS = 1

Selective Reject: SWS <= 2^{m-1} / RWS = SWS

29. Link Utilization: percentage of time the link is actually used for "useful" transmission of information (%).
30. Multiple Access Protocol:

Random Access Protocols: ALOHA CSMA/CD CSMA/CA(Wi-Fi) (collision allowed)

Controlled Access Protocols: Reservation Polling Token-passing

Channelization Protocols: FDMA(frequency) TDMA(time) CDMA(code)

31. ALOHA: random access send and hope you are the only one (uti 18%). Time collision may occur: 2Tf

Slotted ALOHA: Must transmit at the beginning of time slot (uti 36%). Time collision may occur: Tf

32. CSMA/CD: Carrier Sense Multiple Access with Collision Detection (*Ethernet*)

A node should not finish transmitting its frame (Tf) before a possible collision can be detected (2TP for detecting).

For the protocol to work: Tf >= 2Tp

An Ethernet Frame: cannot be too short (protocol will not work) / cannot be too long (unfair)

33. Learning Switch (How does a switch configure itself)

Switch is a *plug & play* device.

Modes of operation: *Filtering* (drop) / *Forwarding* / *Flooding* (as hub)

Learning based on source MAC address

L2 switch is a *transparent device* as far as the end hosts are concerned. Node not communicate with switch (unlike router).

L2 switch *doesn't isolate broadcast domains*.

34. Wireless LANs (Wi-Fi: Wireless Fidelity)

CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance

AP: Access Point

35. BSS: Basic Service Set (using one AP, choosing one frequency)

36. CSMA/CD not work given *wireless Link Characteristics* & *Hidden Terminal Problem*.

37. In 802.11 there divide 11 frequencies, each 10 MHz wide, occupying ≈ 85MHz. There is overlapping channel, channel 1, 6, 11 not.

38. Channel Association

SSID: Service Set Identifier

MAC address

Passive Scanning: AP broadcast a **Beacon** at his frequency. Your NIC scan all channels, choosing stronger one.

Active Scanning: Your NIC broadcast a **Probe**. If no reply or weak, NIC change the channel.

Hot Spot: Someone willing to share this Wi-Fi.

39.MAC Protocol:

CSMA/CA: Collision Avoidance (Required) Based on random access.

RTS/CTS: *Request to send / Clear to send* (Option) To combat the Hidden Terminal Problem.

40. IFS: Inter-Frame Spacing

DIFS: *Distributed IFS* (50 μsec)

SIFS: *Short IFS* (10 μsec)

41. Wi-Fi cannot detect collision. Once transmitting, *NO STOP*. ACK to tell collision not occurred.

42. CSMA/CA:

Station ready to send starts sensing the medium.

If the medium is free for the duration of an IFS, the station can start sending.

If the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a *random* back-off time (collision avoidance, multiple of slot-time, **Contention Window**).

If another station occupies the medium during the back-off time of the station, the back-off timer stops (count / freeze / resume counting).

43. RTS / CTS:

Allow sender to "reserve" channel rather than random access of data frames: avoid collisions of long data frames.

Sender first transmits small **RTS** frames (may still collide but short) with reservation parameter (amount of time the data frame needs the medium) after waiting for DIFS.

AP broadcasts **CTS** in response to RTS after SIFS (*CTS heard by all nodes*).

Sender transmits data, acknowledgement via ACK, other stations defer transmissions.

44. Exposed Terminal Problem

45. Ethernet Router not understand 802.11 frame. AP translates to 802.3 frame.

46. 802.11 frame addressing: Address 1 – MAC address of wireless host or AP to receive this frame. / Address 2 – MAC address of wireless host or AP transmitting this frame. / Address 3 – MAC address of router interface to which AP is attached. / Address 4 used only in ad hoc mode.

47. Drop: network congest / TTL expires / Header check

48. MTU: Maximum Transmission Unit, the **maximum size** of the **data field** (**payload**) in the **frame**. If Packet size > MTU, needs **Fragmentation**.

49. Fragmentation can be done by the source host and/or any router across the internet.

Reassemble of fragments can be done *ONLY* at destination host.

Fragments can be fragmented again.

50. Total length (16-bits): (header (20-60 bytes) + **payload)** (**in bytes**)

51. Packet Header Fields related to Fragmentation:

Identification (**16-bits**): All fragments of a packet has **the same ID number** which is the same as that of the original packet.

Flags (3-bits): D=1 Do not Fragment / M=1 More Fragment **M=0 Last**

Fragmentation Offset (**13-bits**): Relative position of the fragment to the whole **packet** measured in units of 8 Bytes.

(8 is because $2^{16}/2^{13} = 8$) can avoid lost.

52. The payload of each fragment (in bytes) must be **a multiple of 8** *except for the last fragment*.

53. Classful IP Addressing

A: First 0, net id 7bits (1~126,0,127), host id 24bits.

B: First 10, net id 14bits, host id 16bits. 128~191.

C: First 110, net id 21bits, host id 8bits. 192~223.

D: 1110 224~239. E: 1111 240~255.

54. IP Packet Format