Friday, February 24, 2017

Introduction to Computer Networking

The Internet and IP

A day in the life of an application

- Connectivity
  - two computers can exchange data
- Network applications
  - Read and write data over network
- Bidirectional reliable byte stream connection
  - Dominant model
  - one sides reads what the other writes
  - Operates in both directions
  - Reliable (unless connection breaks)
  - Either side can close, refuse connection
- World Wide Web
  - HTTP - HyperText Transfer Protocol
  - command (get - request the page)
  - Respond (200 OK - request accepted and rest of the response are data, 400 - bad request)
  - HTTP - document centric way to communicate
- BitTorrent
  - Breaks files to pieces
  - Swarms - collections of collaborating clients
  - torrent file
    - using WWW and download it
    - information about file and tracker

  - Tracker
    - node that keeps track of what clients are members of swarm
- Skype
  - Proprietary system - no official documentation
  - Case 1
  - Case 2
    - Complication: NAT (Network Address Translation)
      - behind NAT you can open connection out to the Internet, other nodes can't easily open connection to you
      - personal computers are behind NAT (security), servers not
    - Rendezvous server
    - Reversed connection
  - Case 3
    - Both behind NAT communicate through relay

The 4-layer Internet Model

- Layering - applications can reuse the same building blocks
- Link Layer
  - Carry the data over one link at a time
  - Ethernet, WiFi
- Network Layer
  - Deliver packets end-to-end across the Internet
  - Network layer packets = datagrams
  - no concerns about how link layer sends the datagram
  - must use Internet Protocol (IP)
    - best effort attempt to deliver packets but no guarantees

    - IP packets can get lost, deliver out of order, corrupted
- Transport Layer
  - TCP
    - Transmission Control Protocol
    - TCP/IP - application uses both of them together
    - Right order, dropped datagrams retransmitted, correct
    - Email, web client
  - UDP
    - User Datagram Protocol
    - Bundles application data and hands it to the Network Layer
    - no delivery guarantees
    - Video
- Application Layer
- Each layer communicate with its peer layer
- IP is the “thin waist”
  - We have to use IP but otherwise we have many choices
- The 7 layer OSI Model
  - 1980 International Standart Organization =ISO
  - = & layer Open System Interconnection
  - Replaced by 4 layer model
  - numbering system (application layer = layer 7)

The IP Service Model

- Router - forwarding table
- IP
  - no guarantees and detection

    - Duplicated, lost, lateness, out of order
  - Simple, minimum service
  - doesn't maintain state = connectionless
- Why simple
  - Network simple -> fast, less maintenance
  - End-to-end principle
    - Where posible, implement features in the end host
    - Reliable communications and controlling congestion - end points (not network)
      - Different from telephone system (radical)
  - Reliability not ideal for some applications
  - works over any link layer - IP makes very few assumptions about link layer below
- Details
  - Tries to prevent packets looping forever - TTL
  - Fragment packets if they are too long
  - Header checksum to reduce chances of delivering datagram to wrong destination
  - Allows for new version of IP (IPv4, IPv6)
  - Allows for new options to be header
    - new features X no simple
- fields in the header
  - Protocol ID
    - what is inside of data field
    - Demultiplex arriving packets, sending them to the correct code to proccess
    - Internet Assigned Numbers Authority (IANA)
      - defines over 140 values of Protocol ID representing transport protocols
  - Version
    - version of IP

- Total packet length
  - Up to 64 kB
  - Header + data
- Packet ID, Flags, Fragment Offset
  - help routers to fragment IP packets
- Type of Service
  - for router, how important packet is
- Header Length
  - how big header is
  - Some headers have extra optional fields
- Checksum
  - Calculated over the whole header
  - when corrupted we are not likely to deliver it to the wrong destination

A Day in the Life of a Packet

- Application: steam of data -> transport: segment of data -> network: packets of data
- 3 way handshake
  - SYN - Client sends synchronize message to server
  - SYN-ACK - Server responds with synchronize message that also acknowledges the clients synchronize
  - ACK - Client responds by acknowledging the server's synchronize
- For network layer packets sent to different application on the same computer looks the same
  - we need IP address and TCP port address
  - IP packets to pc's IP address, packets have TCP segments with destination port 80
- forwarding table

  - Best = most specific match
  - Default route = least specific route
    - Useful in edge network
      - Everything that is not in network send to Internet = default route
- Wireshark
  - Tell Wireshark to listen on specific port and IP
  - Open web browser and request web page
  - Wireshark displays info
    - TCP port 80 - the HyperText Transport Protocol port on the server
      - We can see that in Info column
    - it is SYN packet
    - Then 3 way handshake -> GET request -> 200 OK
  - this is how it looks like in network layer
- Traceroute
  - shows you the hops that packets to a destination take
  - Wireless router
  - he is at home and he has cable modem and his ISP is Astound
  - Then routers in San Fransisco -> San Jose -> New York -> Boston
  - 3 stars - there is a router that won't tell trace route about itself
    - stars are trace route's way to showed it waited for a reply but the replied timed out

http://www.t1shopper.com/tools/traceroute/

The Principle of Packet Switching

- Packet

  - a self contained unit of data that carries information necessary for it to reach its destination

- packet switching
  - idea
    - Break data up into discrete, self contained chunks of data
    - Each chunk (called packet) carries sufficient information that a network can deliver it
  - Indenpendently for each arriving packet, pick its outgoing links. If link is free, sent it. Else hold the packet for later
- Self (source) routing
  - Each packet contains explicit route, specifying the IDs of each packet switch along the way
  - Internet supports this
    - but it is generally turned off because of security issues
- Consequences of packets switching
  - Simple packets forwarding
    - Switch can make individual decisions
    - Switch doesn't need keep state
  - Efficient sharing of links
    - Data structure is bursty
      - Packet switching allows flows to use all available link capacity
      - Packet switching allows flows to share link capacity
    - statistical multiplexing
      - user receives a statistical share of the resource based on how much others are using it
- Flow
  - A collection of datagrams belonging to the same end-to-end communication

- Switch doesn't need state for each flow (each packet is self-contained)

Layering Principle

- used outside networking too
- Hierarchical and communicate sequentially
  - Each layer has an interface only to the layer directly above or below
- reason for layering
  - Modularity - break down the system into smaller, more manageable modules
  - Well defined service - each layer provides service to the layer above
  - Reuse
  - separation of concerns - each layer focuses on its own job
  - Continuous improvement

Encapsulation Principle

- principle by which you organize information in packets so that you can maintain layers
- Each protocol layer has some header. Followed by some footers
- we can see encapsulation in Wireshark
- Encapsulation allows you to layer recursively
- VPN
  - Virtual Private Network
  - Secure connection to the network - office network
    - use Transport Layer Security - it protects message
    - Access private resources that are accessible only with IP address in your office

Memory Layout and Endianness

- generate message

  - Generate -> create copy of it in the memory -> pass to networking card
- Receive message
  - Receive -> networking card puts that massage in memory
- Memory
  - in bytes
  - program has an address space
  - most computers are 64 bits
    - = memory addresses are 64 bits long
    - so computer has up to 2 to the 64 bytes
- Representation of a multibyte value
  - Endianness - how you lay out a multibyte value in memory
  - 2 options
    - LSB - makes more sense from a computational and architectural standpoint
    - MSB - more sense for human (this is how we write numbers)
- Computers need to agree on representation of numbers
  - big (iPhone) or little (Intel) endian
  - Different professors use different endianness
- Protocol choose endian
  - all protocols that are Internet specifications use a big endian
- Libraries provide you functions so you can write network code that is independent of your processor architecture
- TLS
  - Transport Layer Security
  - Web browsers use that for secure connection (https)
    - hides data but we can see headers
    - TLS payload is inside a TCP segment to port 443 (standard TLS port)

    - TCP segment inside IPv4 header

IPv4 Addresses

- IP
  - Routers decide where to send packet based on destination
  - Original goal - take many networks and stitch them together
  - 32 bits, 4 octets, four 8 bits values
- Netmask
  - which IP addresses are local (on the same link) and with needs to be send to router
  - Netmask is written as a string of consecutive 1s starting with the most significant bit
    - 255.255.255.0 - 24 bits match
    - 255.255.252.0 - 22 bits match
    - 255.128.0.0 - 9 bits match
  - any addresses that matches netmask are in the same network
  - Smaller netmask <-> larger network
- Config
  - terminal command
  - WiFi named is en1
  - IP - 192.168.0.106
  - Netmask - 0xffffff00 (= 255.255.255.0)
- Address Structure
  - Historical
  - 3 classes
    - 2 parts
      - network - administrative domain
      - host - device with network

    - Class A, B, C
- CIDR
  - Classless InterDomain Routing
  - Allows prefixes to be any number of bits
  - “slash 20” = netmask of length 20
    - Describe 2 to the 12 addresses
- IANA
  - Internet Assigned Numbers Authority
  - Manages IP addresses
  - gives out slash-8s to RIR (Regional Internet Registries, 5)
  - ran out of slash-8s -> now management is up to RIRs

Longest Prefix Match Algorithm

- LPM
- Client wants to open a TCP connection to a server on port 80 (web server)
- Fording table
  - set of partial IP addresses
  - packet arrives -> router checks for the best match (= most specific)
- Forwarding table
  - Entry - 2 parts
    - CIDR — block of addresses
    - next hop

Address Resolution Protocol

- ARP

- Mechanism by which the network layer can discover the link address associated with a network address it's directly connected to
- is needed because each protocol layer has its own names and addresses
  - IP address - network layer - "this host"
  - link address - link layer - "this Ethernet card"
    - Describes particular network card - device that sends and receive link layer frames
      - Ethernet - 48 bits address, card is preconfigured with address, unique, 6 octets, hexadecimal
- gateway or router has several
  - IP addresses because of netmask
  - link addresses for each card
- Register computer with a network - register link layer address
- A wants to send packet to B
  - A checks if B is in the same network (netmask)
  - B is in different network -> send packet to gateway
  - A sends packet with network layer destination 171.43.22.5 but link layer destination is the link layer address of the gateway (0:18:e7:ce:1a)
  - Packet reaches the gateway
  - Gateway looks up to next hop and puts IP packet inside a link frame to B
- IP packet is encapsulated inside a link layer frame
- ARP
  - Request-reply protocol
  - Mapping between layer 2 and layer 3
  - "Who has network address XXX?" -> "I have network address XXX and link layer address YYY."
  - Broadcast - every note will hear the packet

- ARP is structured so that it contains redundant data
  - Request contains the network and link layer address of requester
  - other notes will hear it and refresh a mapping in their cache
  - you can generate mapping for another packet is in response to a packet that node sends
    - if node is disconnected -> it will leave the network when caches mapping expire
  - Mapping expiration depends
    - Mac OSX 20 min, Cisco devices 4 hours
    - Mappings do not change often
  - Request sent to link layer broadcast address
  - Reply sent just to requesting address (unicast)
    - the original specification
    - today it is common to broadcast it

- ARP packet
  - 10 fields
  - Hardware field - what link layer this request or response is for (Ethernet)
  - Protocol field - what network protocol this request or response is for (IP)
  - Length - how many bytes long link layer and network layer addresses are
  - Opcode - packet is request or respond (request - 1, response - 2)
  - four address fields - are for requesting and specifying the mappings
  - Fields are stored in network order, or bigger endian
- Destination link layer address is the broadcast address ff:ff:ff:ff:ff:ff
  - All ones
- Gratuitous ARP packets requesting nonexistent mappings
  - Advertise themselves on a network