COMP90007 Revision

1 Introduction

Protocol Hierarchies

Each layer offers service to layer above it.

Connection Oriented vs. Connectionless

Whether a connection is setup before sending a message
Connection Oriented: connect, use, disconnect
Connectionless: just use
Network can provide this services.

OSI Model (7 Layers)	vs.	TCP/IP (4 Layers)
Application		Application
Presentation		
Session		
Transport		Transport
Network		Internet
Data Link		Host-to-network
Physical		

Similarities

- Stacking of layered protocols.
- Layers above to transport layer is related to applications.

Differences

- TCP/IP does not distinguish between services, interfaces and protocols.
- TCP/IP does not clearly separate the Physical and Data Link functions.
- In Network Layer OSI supports both connectionless and connection-oriented services while TCP/IP just supports the connection-oriented service.
- In Transport Layer OSI only supports connection-oriented services while TCP/IP supports both connectionless and connection-oriented services.

2 Physical Layer

Defines the means of transmitting raw bits over a physical data link.

Message Latency

Latency = Transmission delay + Propagation delay

= Size / Bandwidth + Length / Speed of Signal

Transmission Media

- Guided
  - Twisted Pair
  - Coaxial Cable
  - Fibre Optics
- Unguided
  - Radio
  - Infrared
  - Laser
  - Microwave

Satellite (vary by altitude)

- GEO
- MEO
- LEO

Link

- Full-duplex
- Half-duplex
- Simple-duplex

Multiplexing

When multiple sources want to use the medium.

- TDM
- FDM
  - Safe guard

Modulation Types

Signal to Digital; Change in Amplitude, Frequency, Phase; Constellation diagrams.

- ASK
- FSK
- PSK

Maximum Data Rate of a Channel

- Nyquist's Theorem (Noiseless)

$$MaxDataRate = 2Blog_2V$$

- Shannon's Theorem (Noisy)

$$MaxDataRate = Blog_2(1 + S/N)$$

2 Datalink Layer

Converts a raw bit stream into a series of frames; Handles transmission errors and flow control.

Unit: Frame

- Header
- Payload
- Trailer

Type of Services (Service Provided to Network Layer)

- Unacknowledged Connectionless Service
- Acknowledged Connectionless Service
- Acknowledged Connection-Oriented Service

Framing Methods

Breaks raw bit stream; generates checksum.

- Byte Count
  - Uses a field in the frame header to specify the number of bytes in a frame, including itself.
- Flag Byte with Byte Stuffing
  - Each frame starts and ends with a flag byte (not included in header).
  - ESC means backslash.
- Start and End Flags with Bit Stuffing
  - Each frame starts and ends with a flag byte (not included in header).
  - Inserts 0 after five 1s.

Error Control

Physical media may be subject to errors, so check the garbled message.

- Error Detection
  - Checksum

    data & checksum bit

    ones complement sum + ones complement
  - Cyclic Redundancy Check

    data & G(x)

    XOR
- Error Correction
  - Hamming Code

    n data bit & k check bit

    n = 2^k - k - 1

    check positions are the power of 2

    XOR
- Lost Frames Retransmission

Error Bounds (Hamming Distance)

- 2d + 1
  - Correct d errors
- d + 1
  - Detect d errors

Flow Control

For point to point traffic, addresses fast senders - slow receivers problem.

- Stop and Wait Protocol (50% link utilization / efficiency)
  - Utilization
- Sliding Window Protocols (100% utilization / efficiency)
  - Go-Back N
    - Receiver window size = 1, Sender window size = N
  - Selective Repeat
    - Buffer

3 MAC Sub-Layer (Medium Access Control)

Assists in resolving transmission conflicts; between Data Link and Physical Layer.

Channel Allocation

- Static Channel Allocation
  - TDM
  - FDM
- Dynamic Channel Allocation
  - Multiple Access Protocols

Multiple Access Protocols

- ALOHA
- CSMA
- Collision Free
- Limited Contention
- MACA/MACAW (for Wireless LANs)

ALOHA

- Pure ALOHA
  - Efficient under low load
- Slotted ALOHA
  - Efficient under high load

Carrier Sense Multiple Access (CSMA)

- 1-persistent CSMA
- Non-persistent CSMA
- P-persistent CSMA

CSMA with Collision Detection (CSMA/CD)

- N station Contention period, Frame size d
  - Low load efficiency = d / (d + N)
  - High load efficiency = d / (d + 1)

Collision Free Protocol

- Bit Map Protocol
  - Reservation-based protocol, 1 bit per station overhead
  - N bits overhead
- Binary Countdown Protocol

  Stations send their address in contention slots;
  Channel medium ORs bits;
  Stations give up when they send a 0 but see a 1;
  Station that sees its full address is the next one to send.
  - Using binary station addressing, Higher numbered stations have a higher priority.
  - Channel ORs bits
  - logN bits overhead
- Adaptive Tree Walk Protocol

Multiple Access with Collision Avoidance (MACA)

Sender send a “request to send” message to receiver;
Receiver send a “clear to send” message to sender;
Sender then transmit data to receiver.

Handles Hidden and Exposed Terminals Problems.

- Hidden Terminals are senders that cannot sense each other but nonetheless collide at intended receiver.
- Exposed Terminals are senders who can sense each other but still transmit safely (to different receivers).

4 Network Layer

Provides services to the Transport Layer in either virtual circuit or datagram modes; route packets from source to destination.

Unit: Packet

Type of Services (Service Provided to Transport Layer)

- Connectionless (unreliable, flow and error control done by the host)
  - Routing within a Datagram Subnet: Packets (datagrams) injected into subnet independently and packets individually routed to destination by containing the full source and destination address.
- Connection-Oriented (reliable)
  - Routing within a Virtual Circuit Subnet: Packets traveling between destinations all use the same route by using the VC numbers.
- Differences
  - Circuit setup / Addressing contain / Connection space complexity / Effect of router failures / Reliability / Congestion control

Routing Algorithms

- Dijkstra Algorithm
- Distance Vector Routing
- Link State Routing (LSP for each node)

How networks are connected?

Internetworking based on IP protocol.

Tunneling

Source Packets are encapsulated over packets in the connecting network, when source and destination are on the same network, but there is a different network in between.

Fragmentation (division of packets into fragments)

All networks have a maximum size of packets, fragmentation allows network gateways to meet size constraints.

- Transparent
  - Packets fragmented / reassembled in each network.
- Non-Transparent
  - Fragments are reassembled at destination.
    - IP style Fragmentation: packetNum + elementNum + endOfPacketBit

Path MTU Discovery: Alternative to Fragmentation

IPv4 Frame Structure

Maximum size 65535 bytes.

- Header
  - Fixed 20 bytes + variable length
- Text

IP Addressing

Aggregation / Classful Addressing / Longest Matching Prefix (forward to which entry) /

Subnets

Allows networks to be spilt into several parts for internal uses, but acting like a single network for external use.

Network Address Translation (NAT)

Maps one external IP address to many internal IP addresses.

Internet Control Protocol

- ICMP (error info return, traceroute)
- ARP (find MAC address)
- DHCP (assign local IP address to a host)

5 Transport Layer

Provides data transmission service to Application Layer. Transport entity do the work.

Unit: TPDU (segment)

Overall Encapsulation

Frame (Frame header
+ Packet (Packet header
+ Segment (Segment header + Segment payload)
)
)

Type of Services (Service Provided to Application Layer)

- Connectionless
  - UDP
- Connection-Oriented
  - TCP

Transport Layer and Network Layer Services Compared

- Transport Layer code runs entirely on hosts.
- Network Layer code runs almost entirely on routers.
- Transport Layer can fix reliability problems cause by the Network Layer (eg. delayed, lost, duplicated packets), improves QoS.

Element of Transport Protocols

- Connection Establishment
- Connection Release
- Addressing

Connection Establishment

- Three way handshake
  - CR (seq = x) + ACK (seq = y, ACK = x) + DATA(seq = x, ACK = y)
  - Protect when duplicate CR / duplicate CR & DATA
  - Sequence number will not wrap within the maximum packet lifetime.

Connection Release

- Asymmetric Release
  - May results data loss
- Symmetric Release
  - Works well when each process has a set of data to transmit and knows when it has been sent

Strategies

- Three way handshake
- Error cases are handled with timber & retransmission

Addressing

- Transport Layer uses Transport Service Access Points (TSAPs), which refers to port numbers.
- Network Layer uses Network Service Access Points (NSAPs), which refers to IP addresses.

Socket

- Transport endpoint
- Identified by host and port (IP address + port number)
- Socket can be multiplexing on the top of TSAPs (ports).

Port Allocation

port number ranges from 0 ~ 65535

Internet Transport Protocols

- UDP
- TCP

User Datagram Protocol (UDP) (Connectionless)

- Fixed 8 byte header (ports / TSAPs + length + checksum) + payload
- Header contains source and destination ports, payload is handed to the process attached to that particular port at destination.

Strength

Provides an IP interface, improve transmission efficiency, smooth network.

Weakness

Does not support flow control, error control and retransmission of bad segments.

Using UDP: Remote Procedure Call (RPC)

Client - Client Stub - Server Stub - Server

Congestion Control

Affect the subnet to actually carry the available traffic, in a global context.

- Load Shedding (drop packets when congestion control fails).
  - ameliorate impact, applications can mark certain priority to avoid discard policy.
- Although lower layers (data & network) attempt to ameliorate congestion, in reality, TCP impacts congestion most significantly, since TCP offers methods to transparently reduce the data rate, and hence reduce congestion itself.

Transmission Control Protocol (TCP) (Connection-Oriented)

- Fixed 20 byte header + payload.
  - Header: ports (addressing) / seq. & ACK number (sliding window, flow control) / checksum (error control)
- TCP entity segments data streams into pieces < 64KB (often 1460 B in order to fit Ethernet)
- Sender and receiver both create “sockets”, consisting of IP address and the port.
- Special one-way server sockets may be used for multiple connections simultaneously.
- Connection Establishment between source and destination hosts using Three way handshake.
- Sliding window protocol
- Symmetric connection release
- Timers used for lost connection releases.

Feature of TCP Connections

- Full duplex
- Point to point
- Byte streams
  - TCP acknowledge Bytes not packets
- Buffer capable
  - Advertises window based on available space
    - TCP Approach to Congestion Control (just for receiver congestion, not for the network)
  - Slow Start (Incremental Congestion Control)
    - First send a segment with maximum length, then doubles every time until either the timeout occurs / receiver reaches its available buffer.

Segments size decision within 2 constrains

- 65495 Byte TCP segment payload
  - Maximum IP Packet length 65535 - IP header length 20 - TCP segment header length 20
- Maximum Transfer Unit (MTU) — generally 1500 bytes.
  - To fit Ethernet

Quality of Service (QoS)

- Bandwidth
- Delay
- Jitter
- Reliability / Loss

QoS Requirements

Application	Bandwidth	Delay	Jitter	Loss
Email	Low	Low	Low	Medium
File sharing	High	Low	Low	Medium
Web access	Medium	Medium	Low	Medium
Remote login	Low	Medium	Medium	Medium
Audio on demand	Low	Low	High	Low
Video on demand	High	Low	High	Low
Telephony	Low	High	High	Low
Videoconferencing	High	High	High	Low

"High" means a demanding requirement, e.g., low delay

6 Application Layer

Domain Name System (DNS)

Implements in a hierarchy of many name servers, application protocol allows a host to query the database in order to do IP addresses and Host Name Translation.

Division of Name Spaces

The top of the hierarchy is managed by ICANN.

- Top Level Domains (TLD): com / edu …
- Host Names from the bottom to the top.

Service

- IP addresses and Host Name Translation
- Alias names for canonical names
- Mail server aliasing
- Load distribution

Domain Name Properties

- Case insensitive
- <= 63 characters per field
- <= 255 per path
- Internationalize
- Email & web naming conventions
- Absolute domain name ends in “.”
- Relative domain name partially specify the location (only be used in an absolute domain name).

Zone Name Server

- Namespace divided into non-overlapping zones - each circled zone contain some part of tree.
- Each zone usually contains 2 Name Servers, 1 outside the zone for reliability.

Root Server (13 Root Servers globally)

Authoritative cluster for enquiry in the event of locally unresolvable name queries.

Caching and Updating Records

Once any name server learns a mapping, it caches the mapping, thus root name server is not often visited. However, it has timeout.

Electronic Mail

- User Agent
- Mail Transfer Sever
- Simple Mail Transfer Protocol (SMTP)
  - Sends message from sender's user agent to the senders's mail server
  - Sends message from sender's mail server to the receiver's mail server

User Agent

- Envelope
  - Destination address / priority / security level, used for routing by mail server.
- Contents
- Header for user agent control info
- Body for human recipient.

Message Format

Message	=	RFC821 envelope
	+	Header fields (ASCII text)
	+	Blank line delimiter
	+	Message body

RFC822 allows private use

Multiple Internet Mail Extensions (MIME) RFC1341

Retains RFC822 format but resolved the inadequacy of RFC822

- Language with accents
- Non-Latin alphabets
- Non-alphabets language (Chinese etc.)
- Messages with more than text (audio, video)

Message Transfer

- Transfer: SMTP
- Delivery: POP3, IMAP

SMTP (RFC821) Steps

Text - User Agent - MTA port 587 - MTA port 25 - Delivery

WWW

- HTTP
- Web markup languages
- Web scripting languages
- Client and Server Software

Web Page

A web page	=	Objects (HTML file / JPEG etc.)
	+	A base HTML file

Each object is addressable by a URL

URL	=	host name
	+	path name

HyperText Transfer Protocol (HTTP)

Web is an application protocol.

- Client & Server
- HTTP request & HTTP response

HTTP Connections

- Non-persistent HTTP
  - <= 1 object send over one TCP connection
  - Response Time = 1 RTT for TCP Connection + 1 RTT for HTTP request and few bytes of HTTP response to return + File transmission time (but delivery delay 2RTT)
  - Require new connection for each requested object
  - OS overhead for each TCP connection
- Persistent HTTP
  - multiple objects send over one TCP connection
  - Subsequence HTTP messages send over one TCP connection
  - Pipelining — client sends request as soon as it encounters a requested object
  - As litter as 1 RTT for all the requested objects

Cookies

Tracking users and learning about user behavior.

- Domain
- Path
- Content
- Expiry
- Security

Advantages of Cookies

Good for

- Authorization
- Shopping Carts
- Recommendations
- User Session State

Web Caches (Proxy Server)

Reduce response time for client request, reduce the traffic on an institution's link.

Client - Proxy Server (cache objects, installed by ISP) - Server

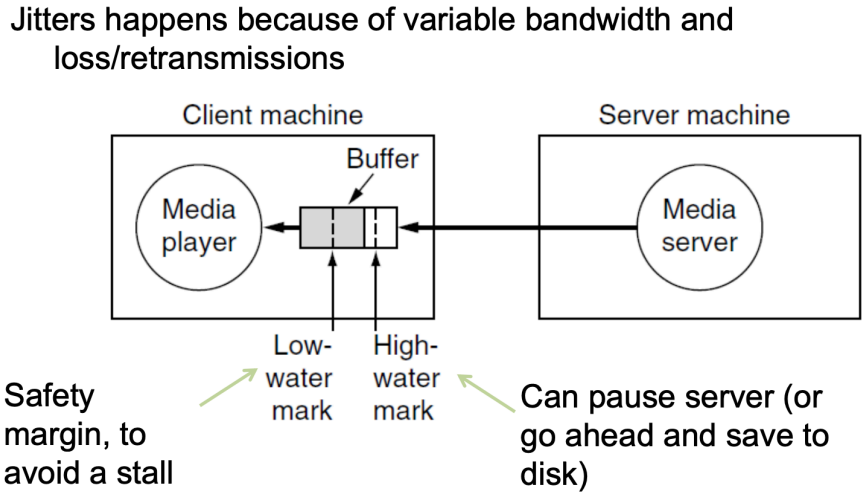
Multimedia

Audio & Video, key types of traffic.

Handling Errors: Streaming Stored Media

- Use reliable transport (TCP): repairs all errors but increases the jitter.
- Add Forward Error Correction (FEC) (eg. parity): repairs most errors but increases overhead, decoding complexity and jitter. (B = P - A - C)
- Interleave media: Mask most errors but slightly increases overhead, decoding complexity and jitter. (Just loss the odd time samples)

Jitter Management (Manage Media buffer)



2RTT

Audio Compression

Represent Frequency — Nyquist's Theorem

Stereo Channel — double channel

Video Compression

- Lossy Compression: JPEG for still images; MPEG, H.264 for video
- Large Compression: 1:50

Voice over IP (VOIP)

Benefits

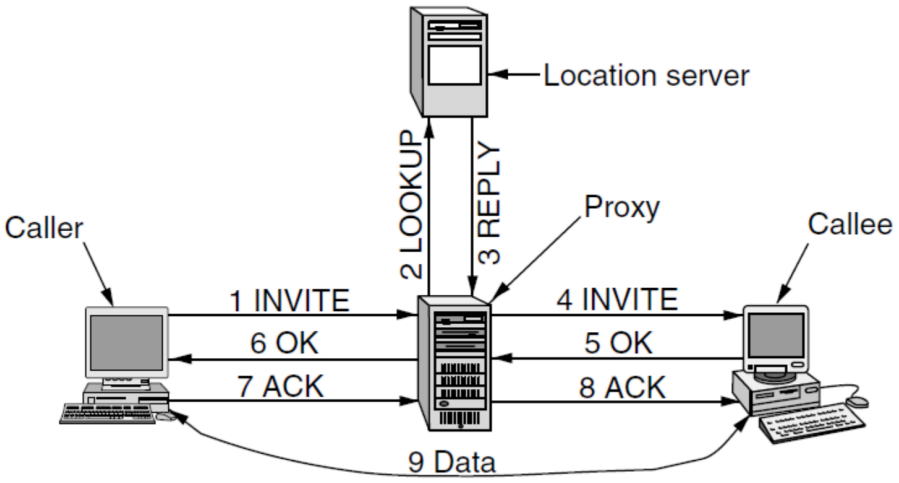
- Financial Savings
- Consolidated infrastructure
- Flexible infrastructure
- Standards based voice and data

H.323

- Binary based protocol
- Monolithic Architecture
- Support calls between Internet computers and PSTN phones.
- Enable multimedia to run over unreliable data networks.
- Call is digital audio/video over RTP/UDP/IP
  - Caller - Forward data channel (RTP) -> Callee
  - Caller <- Reverse data channel (RTP) - Callee
  - Caller <- Data Control channel (RTCP) -> Callee

Session Initiation Protocol (SIP)

- ASCII based protocol
- Modular Architecture



7 Security

4 related concepts

- Secrecy
- Authentication
- Non-repudiation
- Integrity control

Cipher Modes

- Block Chaining
  - Plaintext block is XORed with the previous ciphertext block before being encrypted.
- Stream Ciphers
  - Recursive sequential block encryption is use as a one-time pad, and XORed with plaintext to generate ciphertext.
- Counter Mode
  - Plaintext is not directly encrypted, but an initialization parameter plus the key is encrypted, and the result ciphertext is XORed with plaintext to generate new ciphertext.