COMP90007 Internet Technologies
Final Semester Summary

Frederick Zhang

19/06/2016

Chapter 1. Introduction

1. What are the Internet and the WWW?
   The Internet is a network of networks.
   The WWW is a distributed system that runs on the top of the Internet.

2. Type of Networks (Section 1.2)

   (a) Personal Area Networks

   (b) Local Area Networks

   (c) Metropolitan Area Networks

   (d) Wide Area Networks

   (e) Internetworks

3. Network Hierarchies (Section 1.3.1)
   To reduce their design complexity, most networks are organized as a stack of layers or levels, each one built upon the one below it. The purpose of each layer is to offer certain services to higher layers while shielding those layers from details of how the offered services are actually implemented.

4. Layers, Protocols and Interfaces (Section 1.4)
   Seven layers of OSI (up to bottom): Application, Presentation, Session, Transport, Network, Data Link, Physical
   Four layers of TCP/IP (up to bottom): Application, Transport, Internet, Link
   Five layers used in book: Application, Transport, Network, Link, Physical

   A protocol is an agreement between the communicating parties on how communication is to proceed.
   Between each pair of adjacent layers is an interface. The interface defines which primitive operations and services the lower layer makes available to the upper one.

5. Connection-oriented and Connectionless
   Connection-oriented service is modelled after the telephone system. To use a connection-oriented network service, the service user first establishes a connection, uses the connection, and then releases the connection. In some cases when a connection is established, the sender, receiver and subnet conduct a negotiation about the parameters to be used.
   Connectionless service is modelled after the postal system. Each packet carries the full destination address, and each one is routed through the intermediate nodes inside the system independent of all subsequent messages. When the intermediate nodes receive a message in full before sending it on to the next node, this is called store-and-forward switching. The alternative, in which the onward transmission of a message at a node starts before it is completely received by the node, is called cut-through switching.

6. Service Primitives (1.3.3, 1.3.4, 1.3.5)
   Connection-oriented and Connectionless: check previous section.

A service is formally specified by a set of primitives (operations) available to user processes to access the service. If the protocol stack is located in the operating system, the primitives are normally system calls.

Primitives in Berkeley socket interface: `LISTEN`, `CONNECT`, `ACCEPT`, `RECEIVE`, `SEND`, `DISCONNECT`.

DIFFERENCES BETWEEN SERVICE AND PROTOCOL

- A service is a set of primitives (operations) that a layer provides to the layer above it. A protocol, in contrast, is a set of rules governing the format and meaning of packets, or messages that are exchanged by the peer entities within a layer.
- A service is like an abstract data type or an object but does not specify how these operations are implemented. In contrast, a protocol relates to the implementation of the service and as such is not visible to the user of the service.

7. Network Reference Models (TCP/IP and OSI Reference) (1.4.1, 1.4.2 and 1.4.3)

   (a) *DIFFERENCES BETWEEN OSI AND TCP/IP*

   - The biggest contribution of the OSI model is that it makes the distinction between the three concepts of Services, Interfaces and Protocols explicit.
     Each layer performs some services for the layer above it.
     A layer's interface tells the processes above it how to access it.
     The peer protocols used in a layer are the layer's own business.
   - The TCP/IP model did not originally clearly distinguish between Services, Interfaces and Protocols (although people have tried to retrofit it after the fact to make it more OSI-like).
   - CO & CL Support in OSI and TCP/IP

	Network Layer	Transport Layer
OSI	CO & CL	CO
TCP/IP	CL	CO & CL

   (b) Disadvantages of OSI (Why OSI did not take over the world)

   - Bad timing
     - TCP/IP adopted before OSI was even formalized. Vendors did not want to support 2nd standard.
     - 2-elephant graph: The research period of OSI was too long and it was not standardized when large investments came. However, the academic market was large enough that many vendors had begun cautiously offering TCP/IP products
   - Bad technology
     - Being incomprehensible: two of the layers (session and presentation) are nearly empty, whereas two other ones (data link and network) are overfull.
     - Some functions, such as addressing, flow control, and error control, reappear again and again in each layer.

- Bad implementation
  - The initial implementations were inefficient compared with TCP/IP.
  - Less community support.
- Bad politics
  - OSI was widely perceived as the product of quasi-government standards processes rather than driven by good design processes

(c) Disadvantages of TCP/IP

- The model does not clearly distinguish the concepts of services, interfaces, and protocols.
- The model is not at all general and is poorly suited to describing any protocol stack other than TCP/IP.
- The link layer is not really a layer but an interface (between the network and data link layers).
- The model does not distinguish between physical and data link layers.
- Early implementations were fragile.

(d) Example Question
Briefly explain the design principles and benefits of the Open System Interconnection (OSI) Layer Division approach (and layered approaches in general) for network design.

i. Principles
   - A layer should be created where a different abstraction is needed
   - Each layer should perform a well defined function
   - The function of each layer should be chosen with a view toward defining internationally standardized protocols
   - The layer boundaries should be chosen to minimize the information flow access the interfaces.
   - The number of layers should be large enough that distinct functions need not to be thrown together in the same layer out of necessity, and small enough that the architecture does not become unwieldy.

ii. Benefits
   - Break up the design problem into smaller
   - Protocols can be changed without affecting higher or lower ones

iii. Disadvantage
   - Information at one layer may not be available to other layers, e.g., the timestamp on a packet.
   - Duplication of functions can occur between layers, e.g., buffering or error control.
   - Optimization of functions is difficult between layers, e.g., providing error detection at the link or transport layers.

Chapter 2. The Physical Layer

1. Nyquist Theorem & Shannon's Theorem(2.1.3)

   - $maximum\ data\ rate = 2B \log_2 V\ (bits/sec)$
   - $maximum\ data\ rate = B \log_2(1 + S/N)\ (bits/sec)$

   We call the rate at which the signal changes the symbol rate to distinguish it from the bit rate. The bit rate is the symbol rate multiplied by the number of bits per symbol. An older name for the symbol rate is the baud rate.

2. Latency & Delay
   Latency is the time delay associated with sending a message over a link. This is make of up two parts

   - Transmission Delay
     $T\text{-}delay = Message\ in\ bits/Rate\ of\ transmission$
     $= M/R\ seconds$
   - Propagation Delay
     $P\text{-}delay = Length\ of\ the\ channel/Speed\ of\ signals$
     $= Length/Speed\ of\ signal$
   - $Lentency = L = M/R + P\text{-}delay$

3. Guided Media - Copper vs Fiber (2.2.3, 2.2.4)

Copper Cheaper, no specialist skills required

Fiber Higher bandwidths, greater distance between repeaters (5km vs 50km), not physically influenced by interferences or surges, thin/lightweight, no leakage, difficult to tap

Chapter 3. The Data Link Layer

1. Design Issues (3.1)
   Units, Services, Framing

   FUNCTIONS OF DATA LINK LAYER

   - Providing a well-defined service interface to the network layer
   - Dealing with transmission errors
   - Regulating the flow of data so that slow receivers are now swamped by faster senders

2. Framing (3.1.2)
   To make it easy for a receiver to find the start of new frames while using little of the channel bandwidth:

   - Byte/Character count
   - Flag bytes with byte stuffing
   - Flag bits with bit stuffing
   - Physical layer coding violations

3. Flow Control and Error Control (3.1.3, 3.1.4)

   (a) Flow control
   - Feedback control
   - Rate based

   (b) Error correcting
   - Hamming code
   - Binary convolutional codes
   - Reed-Solomon codes
   - Low-Density Parity Check code

   (c) Hamming code
   - $n = m + r$ ($codeword = message + check$)
   - $d + 1$ (detecting), $2d + 1$ (correcting)
   - correct one $\rightarrow (n + 1)2^m \leq 2^n \rightarrow (m + r + 1) \leq 2^r$

   (d) Error detecting
   - Parity
   - Checksum, e.g., 16-bit internet in IP, Flectcher's checksum
   - CRC

4. Flow Control Protocols

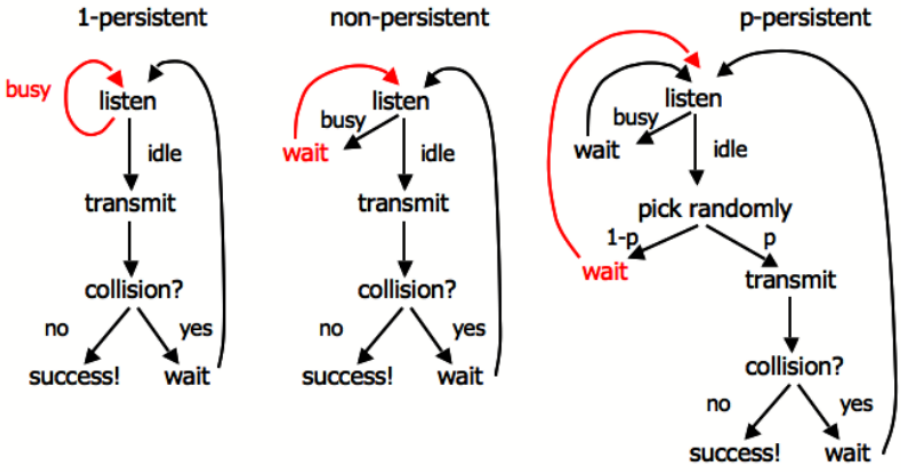
	Utilization	Pros	Cons
Stop and Wait	50%		
One Bit	100%		Synchronization issues
Go-Back-N	100%	Senders do not need to wait for ACK before sending next	Receiver discard all subsequent frames from error point, sending no ACK, until the next frame in sequence
Selective Repeat	100%	Cumulative ACK NAK	Receiver needs more buffer

5. Link Utilization Formula
   `B`: bit-rate of the link (bit/sec)
   `L`: length of the frame (bit)
   $T_f = Time\ needed\ to\ transmit\ a\ frame\ of\ length\ L$
   $T_p = Propagation\ delay\ of\ the\ channel$ (unit: sec)
   $T_a = Time\ for\ transmitting\ an\ ACK$ (assume this is zero)
   $U = (Time\ of\ transmitting\ a\ frame)/(Total\ time\ for\ the\ transfer)$
   $U = T_f/T_t$
   $U = T_f/(T_f + 2T_p) = (L/B)/(L/B + 2T_p) = L/(L + 2T_pB)$

Chapter 4. The MAC Sub-layer

1. Multiple Access Protocols (4.2)
   - ALOHA (pure/slotted)
   - CSMA (Carrier Sense Multiple Access)
   - Collision Free
   - Limited Contention
   - Wireless LAN protocols
2. CSMA (4.2.2)
   Require state detection to determine transmission rights dynamically.
   (a) Persistent and Non-Persistent CSMA
   1-persistent CSMA, Non-persistent CSMA, p-persistent CSMA
   (b) CSMA/CD (CSMA with Collision Detection)
   Principle that transmission aborted when collision detected.
   After collision detected, abort, wait random period, try again
   Channel must be continually monitored, implies only half-duplex system
   (c) DIFFERENCES (last line, P266 & 4th line, last paragraph, P268)

	Collision during transmission
CSMA	Transmit a whole frame anyway, react to collisions after the transmission ends
CSMA/CD	Abort the transmission when collides



3. Collision-Free & Limited Contention Protocols (4.2.3, 4.2.4)

   (a) Collision Free Protocols

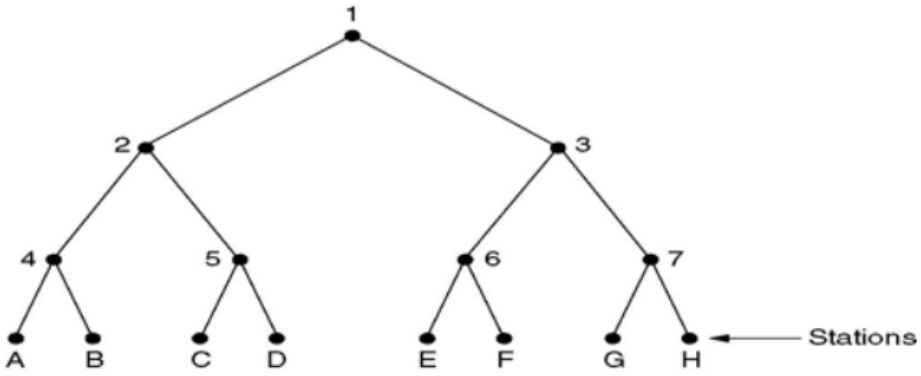
      i. Bit Map Protocol
         - 1 bit per station overhead
         - Division of transmission right, and transmission event
         - Reservation based protocol

      ii. Binary Countdown Protocol
         - Avoid the 1 bit per station scalability problem by using binary station addressing
         - No collision as higher-order bit positions are used to arbitrate
         - *ATTENTION*: As soon as a station sees that a high-order bit position that is 0 in its address has been overwritten with a 1, it gives up

      iii. Token Passing
         - Pass a small message called token from one station to the next in the same predefined order.
         - In a token ring protocol, the topology of the network is used to define the order in which stations send.

   (b) Limited Contention Protocols

      i. Adaptive Tree Walk Protocol
         - All stations compete for right to transmit, if a collision occurs, binary division is used to resolve contention
         - Tree divides stations into groups (nodes) to poll
           – Depth first search under nodes with poll collisions
           – Start search at lower levels ($log_2 n$) if > 1 station expected
         - Illustrated



4. Wireless Protocols (4.2.5)

   (a) Two Problems
   Hidden terminal, Exposed terminal
   IDEAL CASE:

      i. B wants to send to A
      $A \Leftarrow (RTS) B (RTS) \Rightarrow C\ D$

ii. C has to wait at least until B receives CTS
$A(CTS) \Rightarrow B\ C\ D$

iii. B starts transmitting, C didn't receive any CTS after timeout duration. Then C wants to send to D so an RTS is sent by C
$A \Leftarrow B \not\Rightarrow\not\Leftarrow (RTS)C(RTS) \Rightarrow D$

iv. D replies
$A\ B\ C \Leftarrow (CTS)D$

(b) MACA (Multiple Access with Collision Avoidance)

i. Sender asks receiver to transmit short control frame

ii. Stations near receiver hear control frame

iii. Sender can then transmit data to receiver

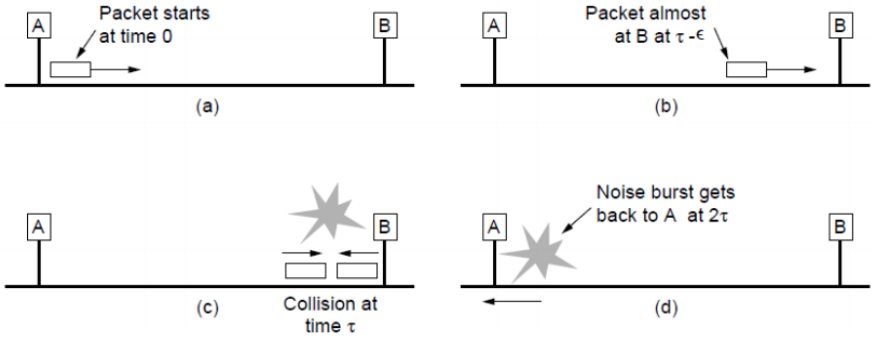
(c) MACAW (MACA for Wireless)

5. Classic Ethernet (4.3.2) (Discussion around Figure 4.15)

(a) Classic Ethernet

- Each type of Ethernet has a maximum cable length per segment
- Multiple cable length can be connected by repeaters - a physical device which receives, amplifies and retransmits signals in both directions

(b) Minimum Packet Size Problem



Collisions should be detected before completing the transmission of current frame

$$minimum\ packet = bit\text{-}rate \times 2\tau$$

For a 10Mbps Ethernet, typically the worst round-trip time (2τ) would be nearly $50\mu sec$, so 500 bits is the smallest size. This number is rounded up to 512 bits or 64 bytes for safety.

6. Practice relevant questions from Assignment 1 and 2

Chapter 5. The Network Layer

1. Design Goals and Store-and-Forward Packet Switching (5.1.1)
   (a) Design Goals
   - Services should be independent of router technologies
   - Transport layer should be shielded from number, type and topology of routers
   - Network addressing should use a uniform numbering plan

   (b) Switching
   Hosts generate packets and injects into the network, router routes packets through the network

   (c) Store-and-Forward Switching & Cut-Through Switching
   (Dupe!) When the intermediate nodes receive a message in full before sending it on to the next node, this is called store-and-forward switching.
   The alternative, in which the onward transmission of a message at a node starts before it is completely received by the node, is called cut-through switching.

2. Routing Algorithms (5.2)
   (a) Definition
   The routing algorithm is responsible for deciding on which output line an incoming packet should be transmitted.

   (b) Non-Adaptive Algorithms
      i. Algorithms Based on Optimality Principle
         A. Sink Tree: Generating a spanning tree based on the topology
         B. Shortest Path Routing: Shortest path problem in dynamic programming
      ii. Flooding
      - Every incoming packet is sent out on every outgoing line except the one on which it arrived
      - Generates a large number of duplicated packets - inefficient
      - Improvement: Selective Flooding

   (c) Adaptive Algorithms
      i. Distance Vector Routing
         A. Known
         Best known distance to each destination (a metric) and which line to used to get there
         B. Send to
         Neighbouring routers
         C. Global information shared locally
      ii. Link State Routing
         A. Known
         Distance to each neighbour

B. Send to
All other routers
C. Local information shared globally

(d) Hierarchical Routing
Dividing all routers into regions allows efficiencies

(e) Broadcast Routing
Allows hosts to send messages to many or all other hosts

(f) Multicast Routing
Used to send a message to a well-defined group within the whole network
Uses spanning tree to eliminate lines which do not lead to members of the group

(g) Internetwork Routing

- Within a network using an interior gateway protocol (e.g., OSPF)
- Between networks using an exterior gateway protocol (e.g., BGP)

3. Virtual Circuits (5.1.3)

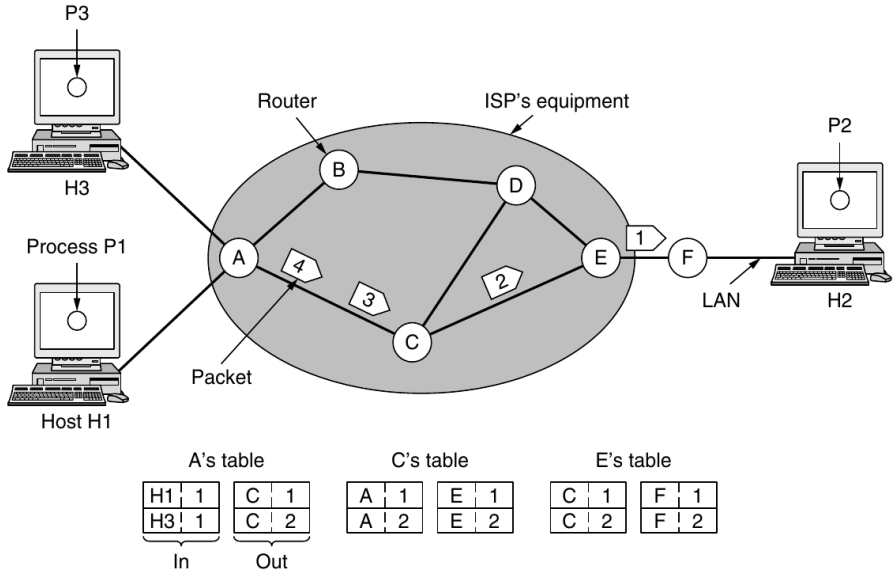


Figure 5-3. Routing within a virtual-circuit network.

(a) Definition
If connection-oriented service is used, a path from the source router all the way to the destination router must be established before any data packets can be sent. This connection is called a VC (virtual circuit) and the network is called a virtual-circuit network.

(b) *ALSO CHECK*

- How to update a routing table when new info comes in
- Datagram routing

(c) *DIFFERENCES BETWEEN VC AND DATAGRAM*

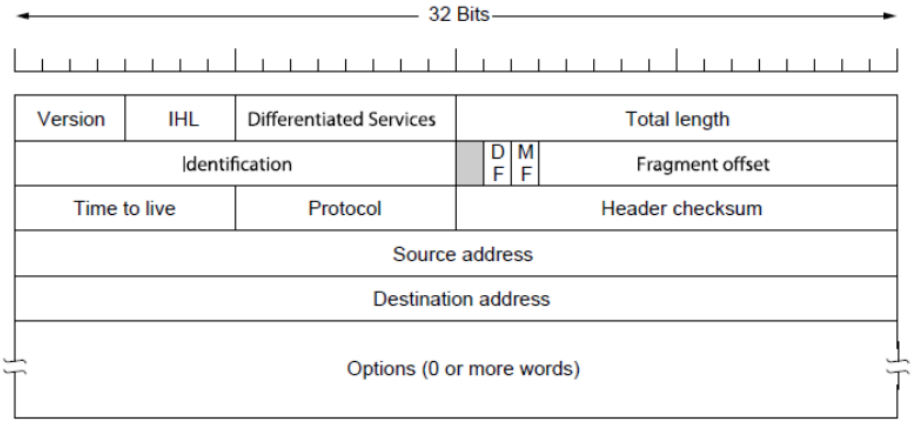
	Datagram	Virtual-Circuit
Circuit setup	Not needed	required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State Information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up, all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of Service	Difficult	Easy if enough resources can be allocated for each VC
Congestion control	Difficult	Easy if enough resources can be allocated for each VC

4. IP Protocol and IPv4 Structure (5.6.1)
   Internet Protocol

   (a) Provides a "best-effort" service to route datagrams from source host to destination host

   (b) These hosts may be: on *same* network, or, on *different* networks

   (c) Each network is called an Autonomous System (AS)



5. Addressing (5.6.1, 5.6.2)

   (a) Classful Network

	Leading bits	Network bits	Rest bits	Num of networks	Addresses per network	Total addresses	Start	End
A	0	8	24	2^7	2^{24}	2^{31}	0.0.0.0	127.255.255.255
B	10	16	16	2^{14}	2^{16}	2^{30}	128.0.0.0	191.255.255.255
C	110	24	8	2^{21}	2^8	2^{29}	192.0.0.0	223.255.255.255
D	1110	N/D	N/D	N/D	N/D	2^{28}	224.0.0.0	239.255.255.255
E	1111	N/D	N/D	N/D	N/D	2^{28}	240.0.0.0	255.255.255.255

   (b) Longest Matching Prefix
   Packet are forwarded to the entry with the longest matching prefix or smallest address block.

6. ARP, RARP (5.6.4)

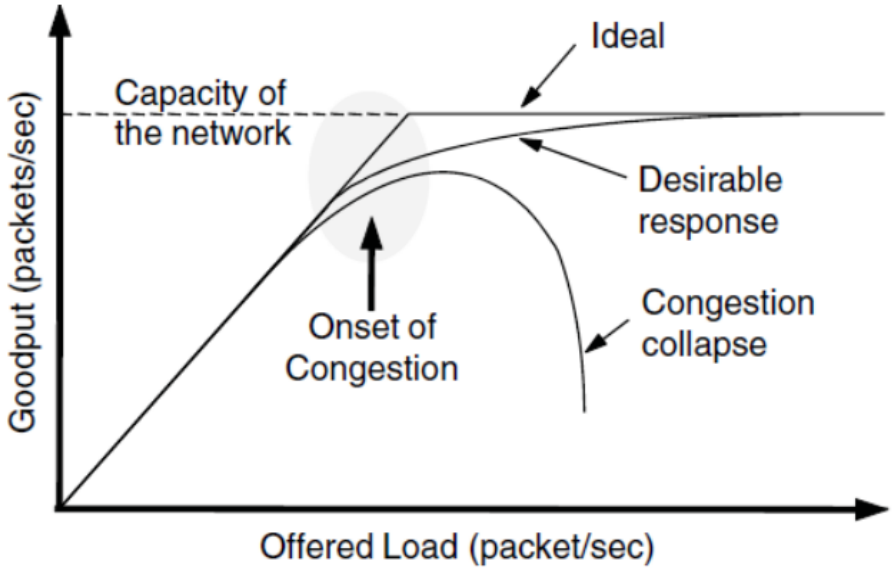
   (a) ARP (Address Resolution Protocol) finds Ethernet address of a local IP address
   - Glue that is needed to send any IP packets
   - Host queries an address and owner replies

   (b) RARP (Reverse Address Resolution Protocol)

7. Congestion Control (5.3)

   (a) Definition
   Too many packets present in (a part of) the network causes delay and loss that degrades performance. This situation is called congestion.

   (b) Congestion Control Algorithms
   Handling congestion is the responsibility of the Network and Transport layers working together
   Goodput is the rate at which *useful* packets are delivered by the network



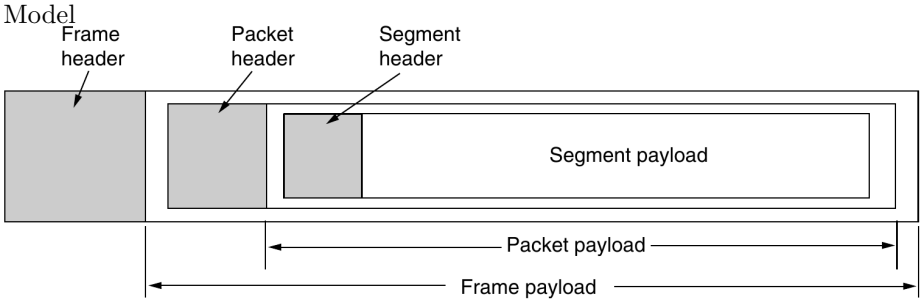
(c) Congestion Control vs Flow Control

- Flow control is an issue for *point to point* traffic, primarily concerned with preventing sender transmitting data faster than receiver can receive it
- Congestion control is an issue affecting the ability of the subnet to actually carry the available traffic, in a *global* context

Chapter 6. The Transport Layer

1. Transport Service (6.1.1, 6.1.2)
   (a) Primary Function
   Provide reliable cost-effective data transport from source to destination, independent of physical or data networks
   (b) Layer Services
      i. Definition
      Transport Layer Services provide interfaces between the Application Layer and the Network Layer
      ii. Transport Entities
         A. Definition
         Transport Entities is the hardware or software which actually does the work
         B. Location
            - OS kernel
            - User process
            - System library
            - NIC
      iii. Services
         A. Purpose
         Transport layer adds reliability to the Network Layer
         B. Connectionless Service (e.g., UDP)
         C. Connection-oriented Service (e.g., TCP)
   (c) *DIFFERENCES BETWEEN TRANSPORT LAYER AND NETWORK LAYER SERVICES*
      - Transport layer code runs entirely on hosts
      - Network layer code runs almost entirely on routers
      - Transport layer can fix reliability problems caused by the Network Layer (e.g., delayed, lost or duplicated packets)
   (d) Role of the Transport Layer
      - Providers of reliable data transmission service
      at the network, data and physical layers
      - Users of reliable data transmission services
      at the application and session layers
   (e) QoS (Feature of Transport Layer)
      - Reliability at application level through interface with network layer
      - Provide a simpler API for application developers independent of network layer
   (f) Encapsulation
      i. Unit
      Encapsulation of TPDUs (transport layer units) in packets (network layer units) in frames (data layer units)

ii. Model



2. Transport Primitives (6.1.3)

   (a) In a Simple Connection-Oriented Service

      i. Server - `LISTEN`

      ii. Client - `CONNECT`

         - Sends `CONNECTION REQUEST` TPDU to Server
         - Receives `CONNECTION ACCEPTED` TPDU from Server

      iii. Data exchanged using `SEND` and `RECEIVE`

      iv. Either party - `DISCONNECT`

   (b) Disconnect Primitives

      i. Asymmetric Disconnection

         - Either party can issue a `DISCONNECT`, which results in
         - `DISCONNECT` TPDU and transmission ends in both directions

      ii. Symmetric Disconnect

         - Both parties issue `DISCONNECT`
         - Closing only one direction at a time - allows flexibility to remain in receive mode

3. Connection Establishment (3-way handshake) (6.2.2)

   (a) Issues
   Packets may be lost, corrupted, delayed, and duplicated

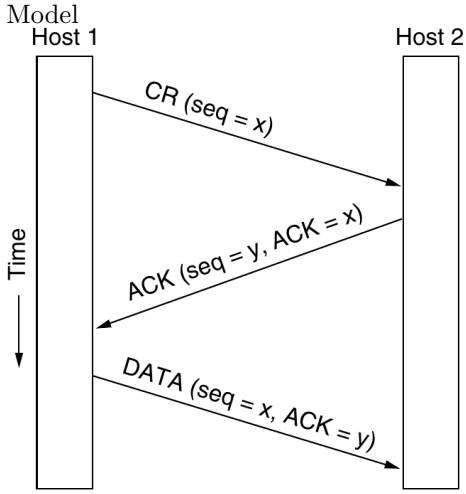
   (b) Solutions

      - Don't reuse Maximum Segment Lifetime sequence numbers
      - Three-way handshake for establishing connection
      - Use a sequence number space large enough that it will not wrap, even when sending at full rate

   (c) Three-Way Handshake

      i. Principle
      Sender and receivers exchange information about which sequencing strategy each will use, and agree on it before transmitting TPDU's

ii. Model



CR = Connection Request

4. Connection Release (6.2.3)

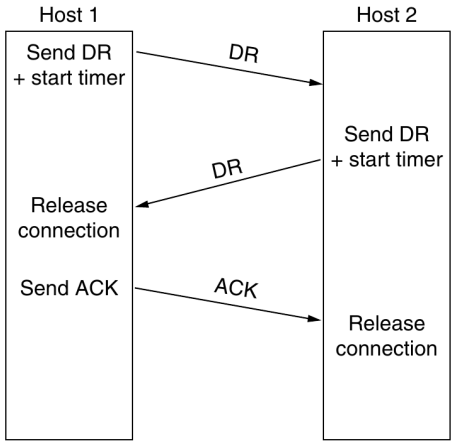
   (a) Issues

   - Asymmetric release may result in data lose hence symmetric release is more attractive
   - Symmetric release works well were each process has a set amount of data to transmit and knows when it has been sent

   (b) Solutions

   - Three-way handshake
   - Finite retry
   - Timeouts

   (c) Three-Way Handshake



DR = Disconnect Request (both DRs are ACKed by the other side)

5. User Datagram Protocol (UDP) (6.4.1)

   (a) Advantage

   Main advantage of using UDP over raw IP is the ability to specify ports for source and destination pairs (and both ports are required)

(b) Strengths and Weaknesses

i. Strengths
Provides an IP interface with multiplexing/demultiplexing capabilities and consequently, transmission efficiencies

ii. Weaknesses
UDP does not include support for flow control, error control or retransmission of bad segments

iii. Conclusion
Where applications don't require a precise level of control over packet flow/error/timing, UDP is a good choice

6. Remote Procedure Call (RPC) Using UDP (6.4.2)

(a) Definition
Sending a message and getting a reply back is analogous to making a function call in programming languages

(b) Principle

- To call a remote procedure, the client is bound to a small library (the client stub) that represents the server procedure in the client's address space
- Similarly the server is bound with a procedure called the server stub. These stubs hide the fact that the procedure itself is not local
- UDP with retransmission is low-latency transport

7. Transmission Control Protocol (TCP) (6.5.1)

(a) Purpose
Provides a protocol by which applications can transmit IP datagrams within a connection-oriented framework, thus increasing reliability

(b) Location of Entities

- Kernel
- Library
- User process

(c) Service Model

- Sender and receiver both create Berkeley sockets on specific IP addresses
- Connections must be explicitly established between sockets at sending and receiving hosts
- A socket may be used for multiple connections simultaneously

(d) Feature

- Full duplex - data in both directions simultaneously
- Point to point - exact pair of senders and receivers
- Byte streams, not message streams - message boundaries are not preserved
- Buffer capable - TCP entity can choose to buffer prior to sending or not depending on the contest

- `PUSH` flag - indicates a transmission not to be delayed
- `URGENT` flag - indicates that transmission should be send immediately

(e) Characteristics

i. Unit: Segment

ii. Header: fixed 20 byte header plus zero or more data types

iii. Segment Size Decision Policy

- 65,515 byte IP payload
- Maximum Transfer Unit (MTU) - generally 1500 bytes

iv. Sliding window protocol

(f) Connection Establishment and Release

i. Connections established using three-way handshake

ii. Two simultaneous connection attempts results in only one connection (uniquely identified by end points)

iii. Connections released asynchronously (2 $\times$ asymmetric releases, one for each transmission direction)

iv. Timers used to lost connection releases (three army problem)

(g) Transmission Policy

- TCP acknowledges bytes, not packets
- Receiver advertises window based on avail buffer space

8. TCP Congestion Control (6.5.9)

(a) Significance
Although lower layers (data and network) attempt to ameliorate congestion, in reality TCP impacts congestion most significantly because TCP offers methods to transparently reduce the data rate, and hence reduce congestion itself

(b) Issues

- Network capacity and receiver capacity
- Should be dealt with separately, but compatibly

(c) Solution
Sender maintains two windows

- Window described by the receiver
- Congestion window

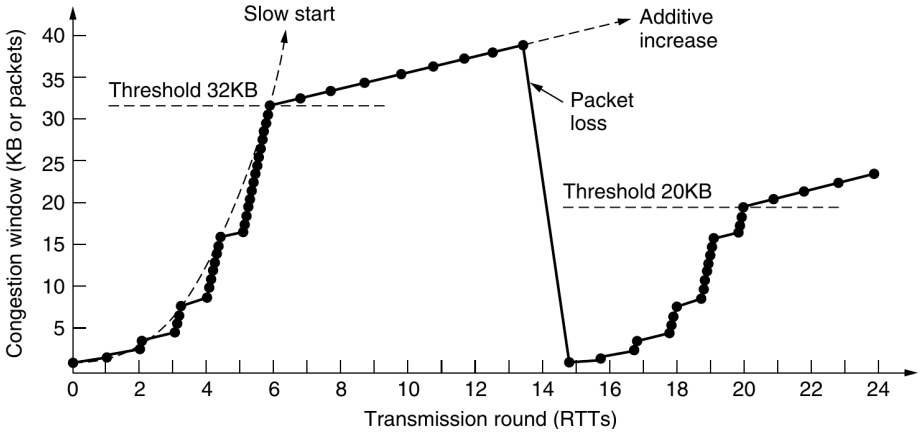
(d) Congestion Window

- After connection is established, sender initializes congestion window to maximum size of segment
-

$$cwnd(i) = \begin{cases} max\ segment, & i = 0 \\ cwnd(i-1) \times 2, & cwnd(i-1) < thr \text{ and } cwnd(i) < thr \\ thr, & cwnd(i-1) < thr \text{ and } cwnd(i) \geq thr \\ cwnd(i-1) + max\ segment, & cwnd(i-1) \geq thr \end{cases}$$

$$thr\ (threshold)\ = \frac{previous\ loss\ cwnd}{2}$$

- Illustrated Increment of Congestion Window



Chapter 7. The Application Layer

1. Domain Name System (DNS) (7.1)
   (a) Definition
   - Distributed database implemented in hierarchy of many name servers
   - Application-layer protocol that allows a host to query the database in order to resolve names (address/name translation)
   - used by other application-layer protocols (HTTP, FTP, SMTP)

   (b) Resource Records
   i. Definition
   Every domain, whether it is a single host or a top-level domain, can have a set of resource records associated with it. These records are the DNS database.
   ii. Structure
   A resource record is a five-tuple:
   Domain_name Time_to_live Class Type Value
   iii. Explanation of Fields
   A. Domain_name
   The *Domain_name* tells the domain to which this record applies. Normally, many records exist for each domain and each copy of the database holds information about multiple domains. The order of the records is not significant.
   B. Time_to_live
   The *Time_to_live* field gives an indication of how stable the record is. (Unit: second)
   C. Class
   For Internet information, it is always *IN*. For non-Internet information, other codes can be used, but rarely seen.
   D. Type
   The *Type* field tells what kind of record this is.
   iv. Type List

Type	Meaning	Value
SOA	Start of authority	Parameters for this zone
A	IPv4 address of a host	32-Bit integer
AAAA	IPv6 address of a host	128-Bit integer
MX	Mail exchange	Priority, domain willing to accept email
NS	Name server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
SPF	Sender policy framework	Text encoding of mail sending policy
SRV	Service	Host that provides it
TXT	Text	Descriptive ASCII text

   (c) DNS Resolution
   i. Definition
   Finding the IP address for a given hostname is called resolution and is done with the DNS protocol

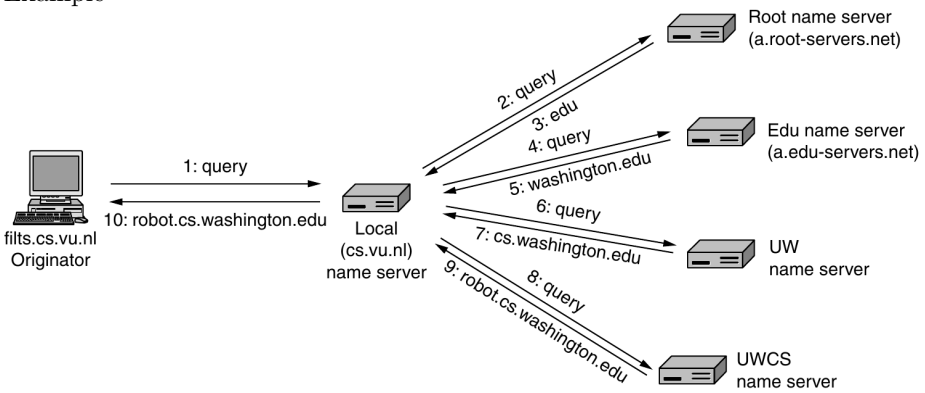
ii. Principle
- Computer requests local name server to resolve
- Local name server asks the root name server
- Root returns the name server for a lower zone
- Continue down zones until name server can answer

iii. Recursive Query & Iterated Query

A. Recursive Query
The local name server handles the resolution on behalf of the host which is querying, until it has the desired answer to return. It does *not* return partial answers.

B. Iterated Query
The root name server (and each subsequent name server) does *not* recursively continue the query for the local name server. It just returns a partial answer and moves on to the next query. The local name server is responsible for continuing the resolution by issuing further queries.

C. Example



(d) DNS Protocol
- Runs on UDP port 53, retransmits lost messages
- Caches name server answers for better performance

2. Email (7.2)

(a) Architecture and Services (7.2.1)

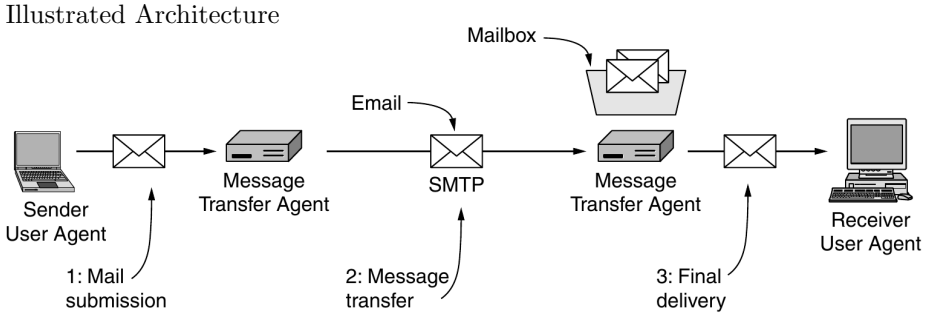
i. Architecture & Components

A. User Agents
Allow people to read and send email

B. Mail Servers (Message Transfer Agents)
Move the messages from the source to the destination

C. Simple Mail Transfer Protocol (SMTP)
SMTP is used to send messages from the sender's
- *mail server* to the receiver's *mail server*
- *user agent* to the sender's *mail server*

D. Illustrated Architecture



ii. Services

A. Mail Submission
Sending new messages into the mail system for delivery.

B. Mailing List
Message transfer agents (mail servers) implement mailing lists, in which an identical copy of a message is delivered to everyone on a list of email addresses.

C. Mailboxes
Mailboxes store the email that is received for a user.

(b) Comparison: POP3 and IMAP (7.2.5)

i. Internet Message Access Protocol (IMAP)

- Addressing mail by using attributes
- Search can be performed on server to find messages that satisfy certain criteria so that only those messages are fetched by the client

ii. Post Office Protocol, version 3 (POP3)

- Less secure
- Mail is downloaded to the user agent computer, instead of remaining on the mail server
  - Easier for servers
  - Not easy to read mail on multiple computers
  - Risk of losing mail

3. WWW (7.3)

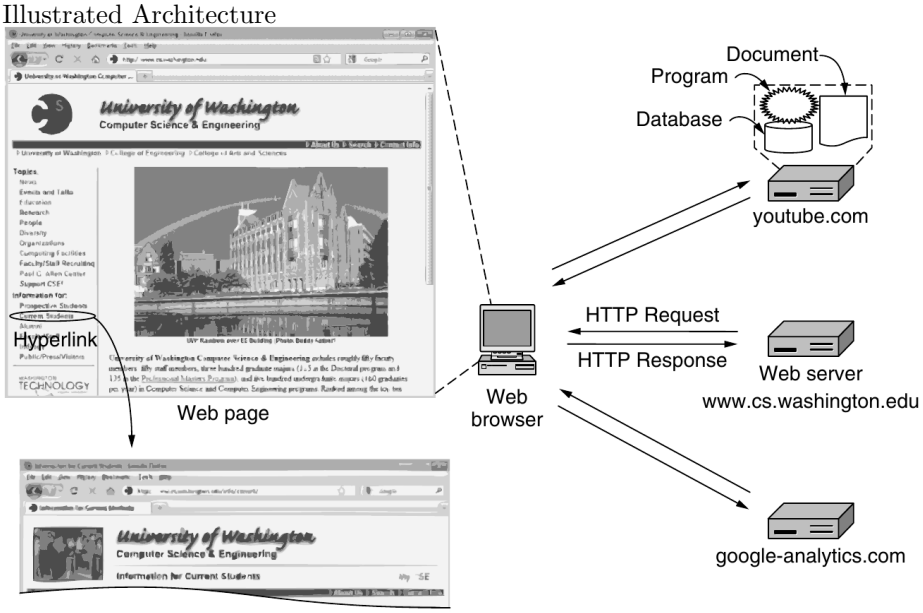
(a) Architecture (7.3.1)

i. Client - Server Model

- Client - Browser based access to pages
- Server - Daemon based content delivery of pages
- Uniform Resource Locator (URL)
  - Protocol + DNS Name + file name
  - Extensions of URL - URN (location independent)

ii. Pages are named with URLs

iii. Illustrated Architecture



(b) Hypertext Transfer Protocol (HTTP) (7.3.4)

i. Connections

HTTP 1.0 Single connect for each transaction for each client-server pair

HTTP 1.1 Persistent connections per server-client pair

ii. Methods

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

iii. Error Codes

Code	Meaning	Examples
1xx	Information	100=server agrees to handle client's request
2xx	Success	200=request succeeded; 204=no content present
3xx	Redirection	301=page moved; 304=cache page still valid
4xx	Client Error	403=forbidden page; 404=page not found
5xx	Server Error	500=internal server error; 503=try again later

4. Multimedia Networks (7.4)

(a) Basic Model and Characteristics (7.4.3)

i. Step by Step

Step 0 User clicks a movie

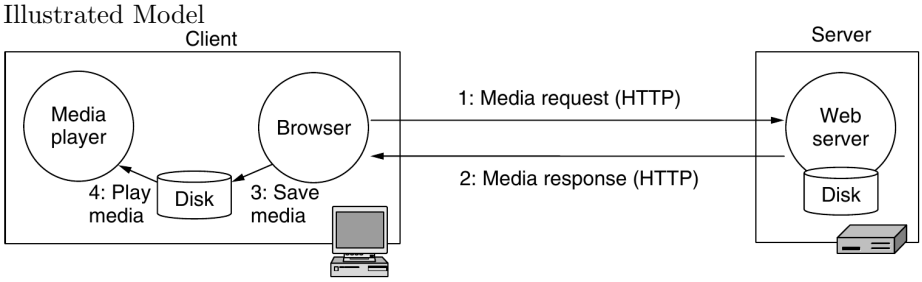
Step 1 Browser sends an HTTP request to the Web server

Step 2 The server fetches the movie and sends it back to browser with *MIME* attached

Step 3 The browser saves the entire movie to a scratch file on the disk

Step 4 The media player starts reading and playing the movie

ii. Illustrated Model



iii. Characteristics

- Higher bandwidth requirements
- Higher QoS requirement
- New infrastructure models
- New service providers

(b) Jitter Management (7.4.3)

i. Approach

A. Multimedia software buffers streamed media sources prior to transmission

B. Buffering is a defensive mechanism to reduce jitter

C. Ideally, the stream buffer will continue to be filled at the same rate the stream is played back to the user

ii. Buffering Modes

A. Pull Server
As long as there is room in the buffer to another block, the media player continues to request additional blocks from the server (goal to keep the buffer as full as possible)

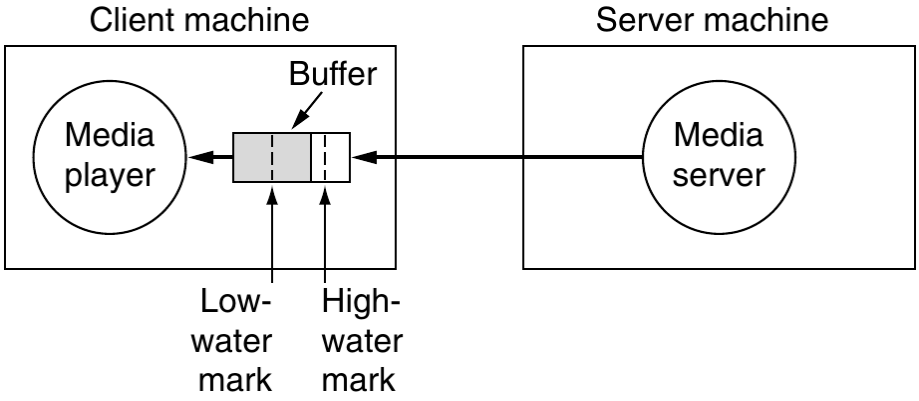
B. Push Server
Media player sends a play request, and the server continuously pushes data to the player, media player uses a FIFO (First-In First-Out) scheme to draw from the buffer, and uses a compensation mechanism when the buffer is not filled to capacity - high and low watermarks trigger starts or stops in the playback

iii. Push Server Mode

A. Approach
The startup delay gives the buffer a change to fill to the low-water mark, then if data are sometimes slow to arrive due to congestion, the buffered media will allow the playout to continue normally until new media arrive and the buffer is replenished.
The more jitter, the larger the low-water mark of the buffer needs to be to avoid underrun.

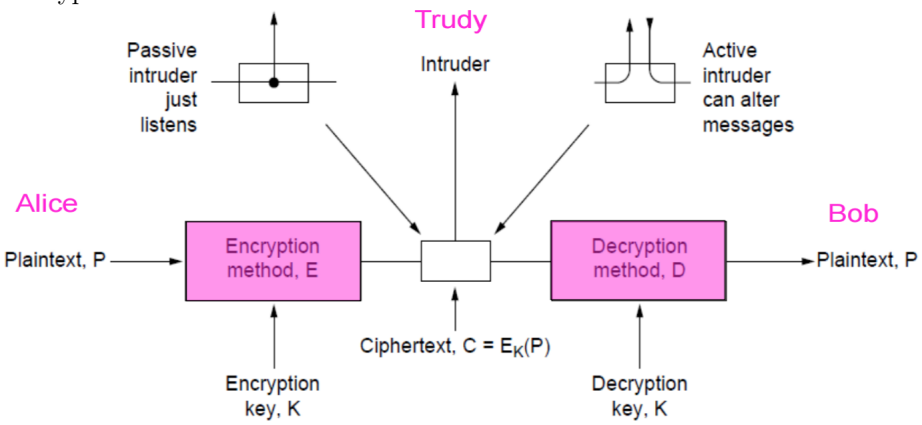
High-water mark is defined so that buffering too much can be avoided. Basically, the server just pumps out data until the buffer is filled to the high-water mark.

B. Illustrated Model



Chapter 8. Network Security

1. Basic Encryption (8.1.1)
   (a) Encryption Model



   (b) Plaintext, Keys, Ciphertext
   Plaintext messages to be encrypted can be transformed (encrypted/-decrypted) by a function that is parameterized by a key, the output of the transformation process is ciphertext

   (c) Kerckhoff's Principle
   Cryptographic Algorithms and related functions (E, D) are public; only the keys (K) are secret

   (d) Relations
   $C = E_K(P)$
   $P = D_K(C)$
   $D_K(E_K(P)) = P$
   Requirement: $D_{K1}(E_{K2}(P)) = P$ if and only if $K1 = K2$

2. Types of Ciphers
   (a) Substitution Cipher (8.1.2)
      i. Definition
      Each letter of group of letters is replaced systematically by other letters or groups of letters
      ii. Vulnerability
      Breakable with knowledge of the replacement system

   (b) Transposition Cipher
      i. Definition
      All letters are re-ordered without disguising them
      ii. Vulnerability
      Breakable with knowledge of re-ordering system

   (c) One-time Pad
      i. Definition
      Uses a random bit string as the key, convert the plaintext into a bit string, then XOR the two strings bit by bit

ii. Vulnerability
Unbreakable because given a sufficiently large sample of each letter, digram, and trigram will occur with equal distribution

3. Symmetric Key Algorithms

(a) Definition
Uses the same key for both encryption and decryption

(b) Ciphers Used
Symmetric key algorithms can use permutation, substitution and a combination of both to encrypt and decrypt

(c) Examples

i. Data Encryption Standard (DES)
- 64 bit blocks and 56 bit keys
- 2^{56} key space
- Triple DES has a 3×2^{56} key space

ii. Advanced Encryption Standard (AES)
- 128 bit blocks and 128 bit keys (others available)
- 2^{128} key space

(d) Cipher Modes (8.2.3)

i. Block
Replacement attack

ii. Block Chaining

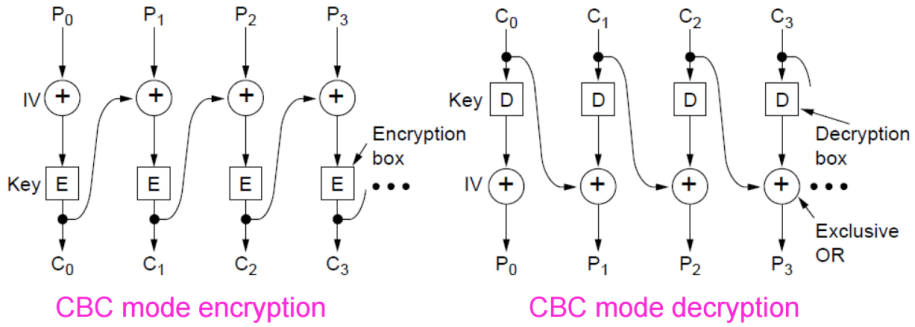
A. Definition
Each plaintext block is XOR'ed with the previous ciphertext block before being encrypted

B. Feature
If one block of ciphertext (C_i) is changed before decryption, only P_i and P_{i+1} are affected

C. Advantage
- Random access
- Anti replacement attack

D. Disadvantage
- Inefficient (Can only start decrypting when 8 bytes fetched)
- 1 bit error, 16 bytes error

E. Model



CBC mode encryption CBC mode decryption

iii. Feedback Mode

A. Definition

Byte-by-byte encryption is used rather than block-by-block encryption, together with a shift register

B. Feature

- If one byte of ciphertext (C_i) is changed before decryption, P_i to P_{i+L} are affected (L is the length of shift register in bytes)
- Inefficient

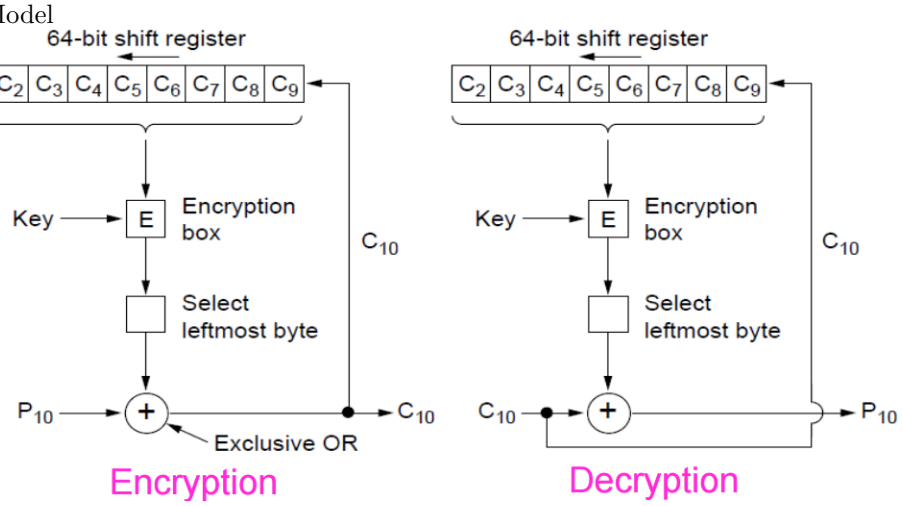
C. Advantage

- Be able to start decrypting when 1 byte fetched

D. Disadvantage

- Inefficient (1 byte product for encrypting/decrypting 8 bytes)
- 1 bit error, 9 bytes error (when 64-bit register is used)

E. Model



iv. Stream Cipher

A. Definition

In stream cipher mode, recursive sequential block encryption is used as an one-time pad, and XOR'ed with plaintext to generate ciphertext

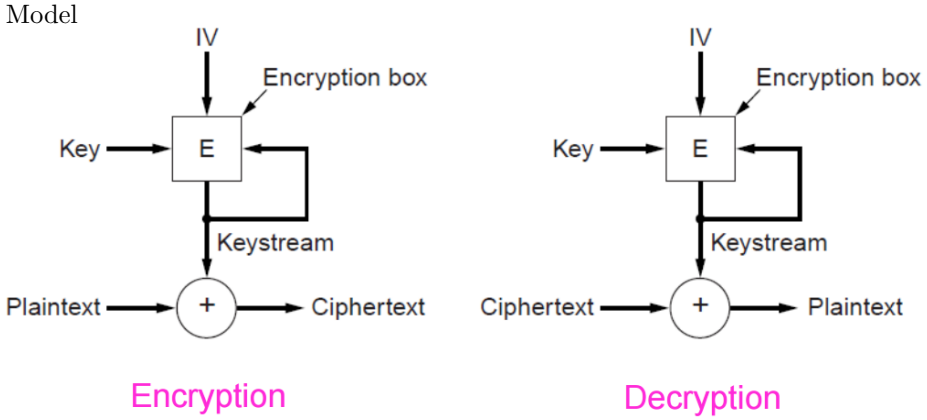
B. Advantage

- 1 bit error, 1 byte influenced

C. Disadvantage

- No random access

D. Model



v. Counter Mode

A. Definition

In counter mode, plaintext is not directly encrypted, but an initialization parameter plus an arbitrary constant is encrypted, and the resulting ciphertext is XOR'ed with plaintext to generate new

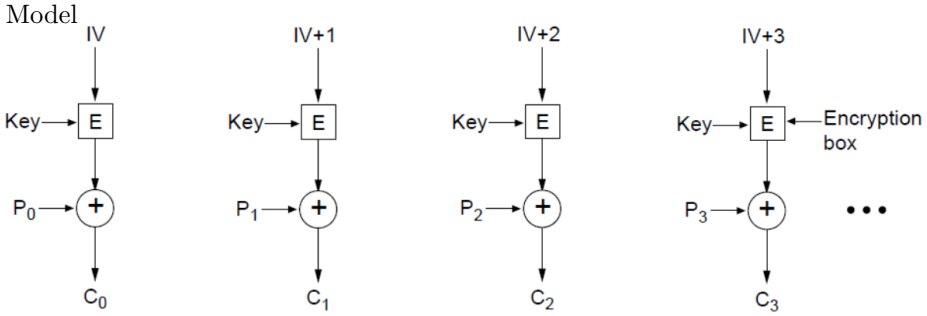
B. Advantage

- Random access

C. Disadvantage

- Replay attack

D. Model



(e) Other Algorithms

- Blowfish
- IDEA
- RC4
- RC5

4. Asymmetric Key Algorithms

(a) Definition

The key used to encrypt and the key used to decrypt are different, and not derivable from each other

(b) Public Key Algorithms (Diffie-Hellman Key Exchange)

i. 2-Key System

Key 1 Public key, usable by anyone to encrypt messages to the owner of the key

Key 2 Private key, required to decrypt the message (and held only by the owner of the key)

(c) RSA (8.3.1)

i. Encryption & Decryption

Encryption $Cipher = Plain^e (mod\ n)$

Decryption $Plain = Cipher^d (mod\ n)$

ii. Usage

RSA is too slow for encrypting/decrypting large volumes of data, but is widely used for secure key distribution

(d) Digital Signatures

i. Reason of Using Cryptography

Cryptographic approaches can be used to ensure authenticity and allow for non-repudiation

ii. Requirements

- Receiver can verify the claimed identity of the sender
- Sender cannot repudiate contents of the message
- Receiver cannot have derived the message themselves

iii. Message Digests

A. Definition

Using a one-way hash function to take an arbitrary length of plaintext and compute a fixed-length bit string

B. Properties

- Given P, it is easy to compute $MD(P)$
- Given $MD(P)$ it is effectively impossible to find P
- Given P, no one can find P_0 such that $MD(P_0) = MD(P)$
- A change in even a single bit of input produces a very different output

iv. Birthday Attack

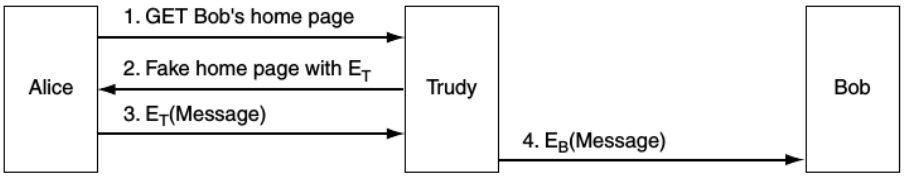
$2^{m/2}$ may be sufficient to break a message digest algorithm

v. Public Key Management

A. Approaches

- Certification Authority (CA)
  A trusted intermediary who uses non-electronic identification to identify users prior to certifying keys and certificates
- X.509
  An international standard for certificate expression
- PKI
  Hierarchically structured certificate authorities allow for the establishment of a chain of trust or certification path

B. Man in the middle

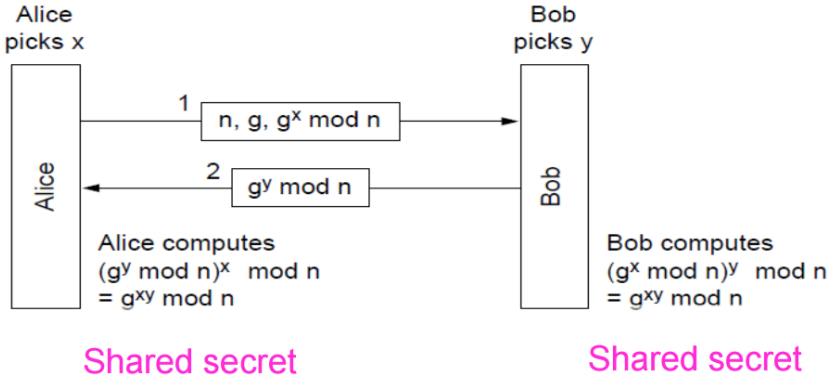


5. Communication Network Security (8.6)

(a) Authentication Protocols

i. Shared Secret Key

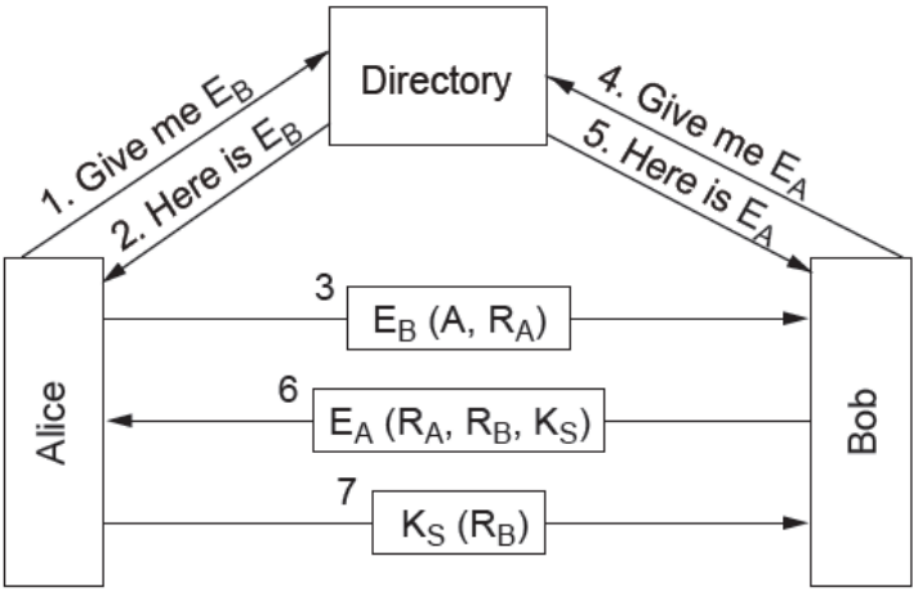
- Principle
  One party sends a random number to the other party, who transforms it and sends the result back - essentially a challenge and response protocol
- Identity Confirmation
  A mechanism such as Diffie-Hellman key exchange is used
- Model



ii. Public Key

A. Key Distribution Centre (KDC)

- Model



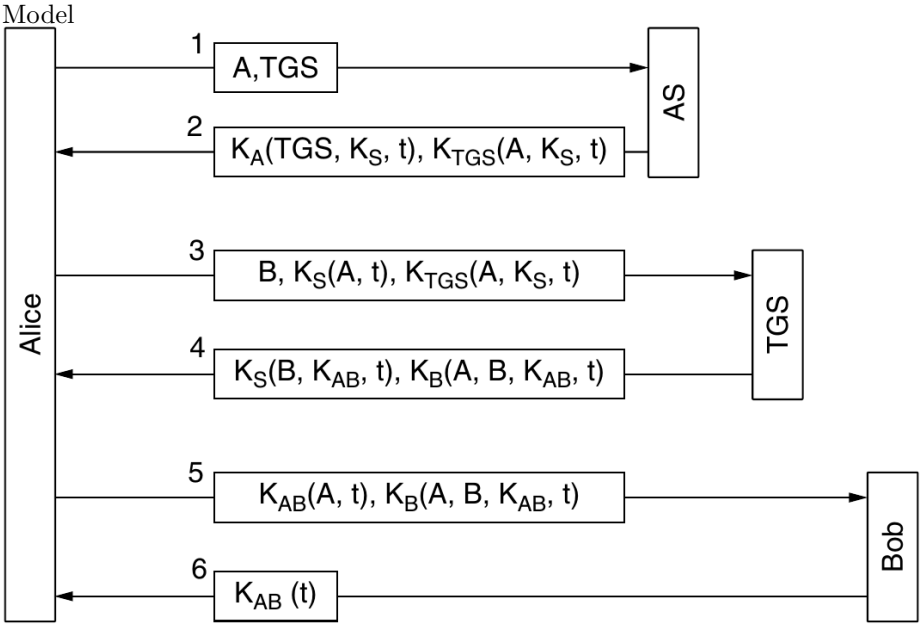
- Principle
  A trusted intermediary is used to facilitate the authentication
- Identity Confirmation
  Users each share a key with a central key distribution

centre, and authenticate to the KDC directly. The KDC then acts as a relay between the two parties.

- Algorithms
  - Needham Schroeder
  - Otway-Rees

B. Kerberos

- Model



- Principle
  A multi-component system is required:
  - Authentication Server
  - Ticket Granting Server
  - Recipient
- Identity Confirmation
  Authentication is managed centrally, and then party to party communication is facilitated by single use cryptographic tickets.
  Uses Needham-Schroeder algorithm to minimize insecure connection setup packet exchange

(b) Firewalls

i. Purpose
Firewalls, which are positioned at the network boundary, ensures security at the network perimeter by providing a controlled series of route between the internal and external networks

ii. Characteristics
- All inbound and outbound traffic must transit the firewall
- Only authorized traffic must pass through the firewall
- Firewalls should be immune to penetration themselves.

iii. Reasons for Inspections On Incoming & Outgoing Packets

A. Incoming
Anti-virus (likely to be successful for known viruses only)

B. Outgoing
Leakage of confidential information (unlikely to be detected if encrypted)
Denial-of-service attack trace (potentially likely to be detected)

(c) IPSec

i. Introduction
IPSec represents one view of how to embed security in the protocol stack - at the network level

ii. Principle
Encryption is compulsory, but for graceful failover, a null encryption algorithm can be used between points which are not cryptographically inclined

iii. Feature
- Data integrity
- Replay attack protection

iv. Algorithm
IPSec framework allows multiple algorithms and multiple levels of granularity

v. Connection
Connection-oriented, with connection being called SA's (security associations)

(d) Virtual Private Network (VPN)

i. Definition
VPN is a virtual layer on the top of an IP network which provides a secure end-to-end connection over public infrastructure

ii. Common Implementation
Using a firewall at each end of a connection, setting up a SA to create an IPSec tunnel between the two end points, and then selectively route traffic for the specific destination via the encrypted connection

(e) Wireless Security Context

i. Difficulty
Difficult to secure because of omnidirectional signal propagation

ii. Wired Equivalency Protocol (WEP)

A. Algorithm
40-bit encryption based on RC4

B. Issues
- 40 bit encryption is breakable with low-moderate computational resources
- RC4 re-uses keys, so capturing a sufficient volume of encrypted traffic will guarantee key identification

iii. Securing Wireless
- MAC Address Filtering

- Non-Broadcast SSID
- Additional Encryption (128bit WEP)
- Multilayered Security