TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI
VICTORIA
UNIVERSITY OF WELLINGTON

EXAMINATIONS — 2007
END-YEAR

COMP306

COMPUTER NETWORKS

Time allowed: THREE HOURS

Instructions: The examination contains 5 questions, you must answer all questions

Question 1 is worth 40 marks

The other four questions are worth 30 marks each.

The exam consists of 160 marks in total.

The number of marks assigned to each part of a question are shown.

Paper foreign to English language dictionaries are allowed.

Electronic dictionaries and programmable calculators are not allowed.

Question 1 Assorted Short Questions **[40 marks]**

(a) [2 Marks] What is a network "protocol"?

Answer:

Set of rules governing the format, order and processing of messages between entities.

(b) [3 marks] Show, in the correct order, the layers of the TCP/IP protocol stack that are implemented on the following network components:

i. End System (host)
ii. Router
iii Switch

Answer:

App -> TCP/UDP -> IP -> Datalink -> physical

IP -> Datalink -> physical

Datalink -> physical

(c) [4 marks] State the primary differences between the link-state and distance vector routing algorithms.

Answer:

L-S whole knowledge of network topology, djikstra's algorithm, broadcast information

D-V only knowledge about directly connected nodes, Bellman-Ford algorithm, share info with directly connected devices only

(d) [5 Marks] Briefly explain how the Domain Name Service (DNS) is implemented and how DNS queries are resolved in the DNS system.

Answer:

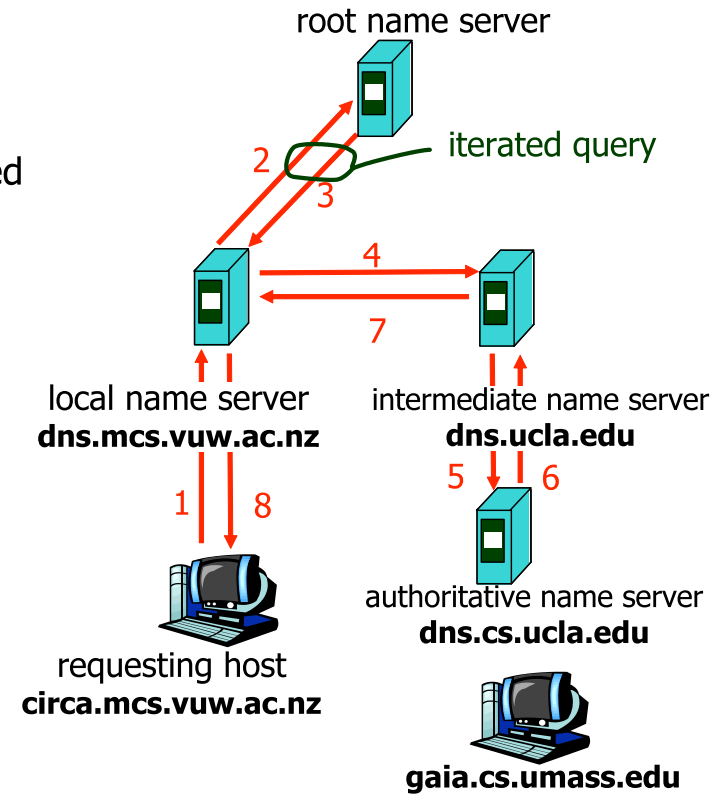
The Domain Name System maps names to IP addresses. It is a distributed database implemented in hierarchy of many name servers. has an application-layer protocol for host, routers, name servers to communicate to resolve names. There are 13 root servers; it is broken into zones containing primary and secondary name servers. A diagram such as the following may be used.

recursive query:

- burden of name resolution on contacted name server
- heavy load?

iterated query:

- contacted server replies with name of server to contact
- "I don't know this name, but ask this server"



(e) [3 marks] What is ICMP? Briefly explain the key areas of functionality for ICMP giving an example.

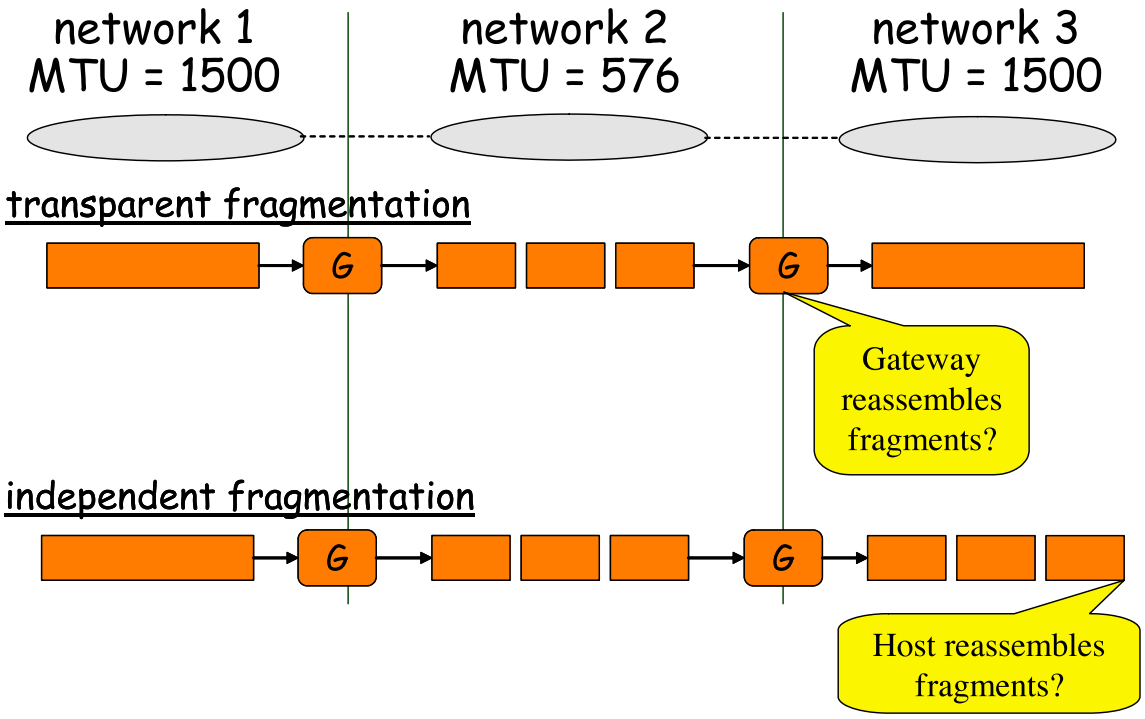
Answer:

ICMP = Internet Control Management Protocol. Made up of error reporting and query messages. Examples include echo, timestamp, address mask, quench, time exceeded destination unreachable…

(f) [5 marks] Explain why datagram fragmentation is an issue in IPv4 and how it is dealt with in the Internet?

Answer:

See diagram below. Independent fragmentation is used in the internet except for special cases such as interworking with ATM where transparent fragmentation is required due to efficiency because of cell size in ATM.



(g) [2 marks] Why is datagram fragmentation not an issue in IPv6? How is this achieved?

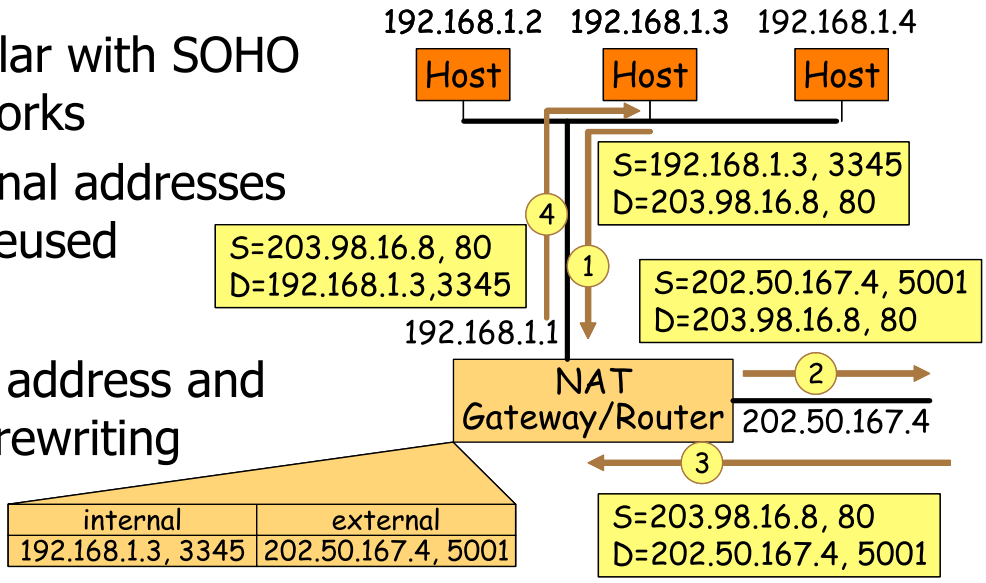
Answer:

IPv6 cannot allow fragmentation at routers, the transmitter creates datagrams of the maximum transmission unit. Icmp v6 tells the source what the max transport unit (mtu) of the path is.

(h) [6 marks] Describe how Network Address Translation (NAT) works, indicate the data structure required to maintain mapping between the internal addresses and the public address. You may illustrate the operation using a diagram.

Answer:

- Popular with SOHO networks
- Internal addresses are reused
- Uses address and port rewriting

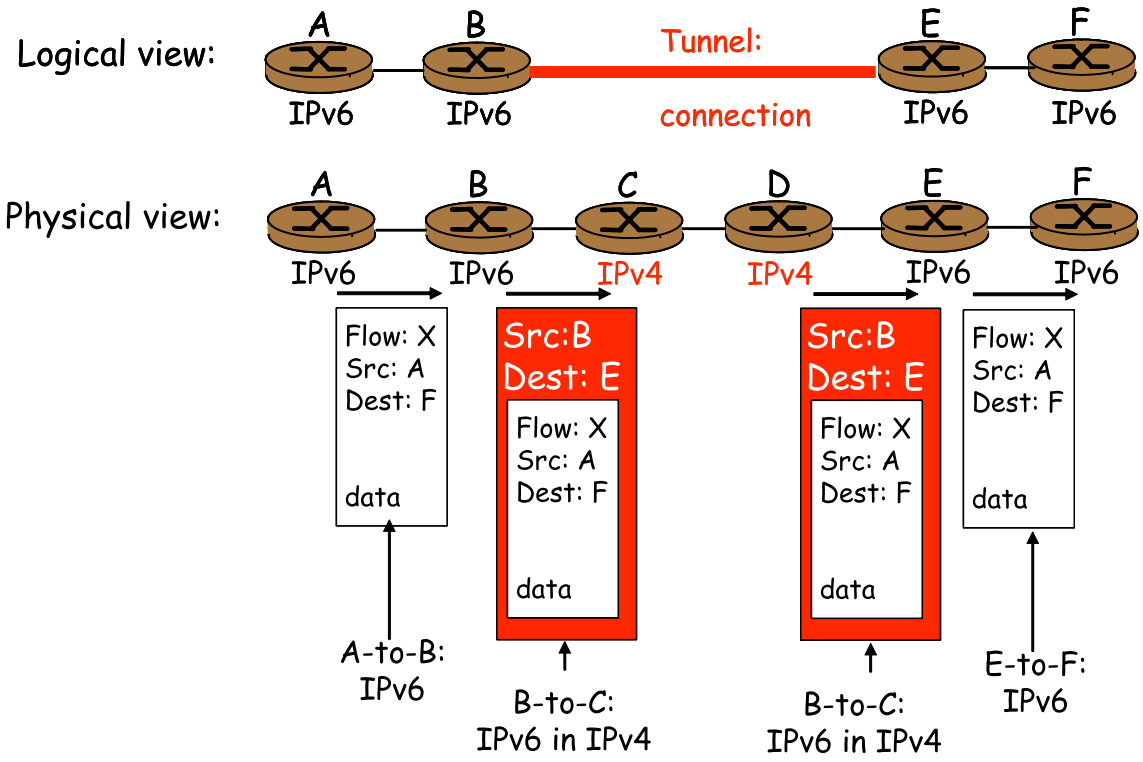


(i) [10 marks] Discuss the issues and solutions related to the interworking of IPv6 and IPv4.

Answer:

Address 32 bit v4, 128 bit v6. Different header format which requires translation of fields. (May mention QOS, TTL, flow identifier, protocol field).

Interconnecting IPv6 networks: Tunnelling between IPv6 clouds, IPv6 routing and encapsulation of IPv6 in IPv4 required. The encapsulation uses the IPv4-6 router v4 addresses for end point identification, the student may draw a picture:



IPv6 to IPv4 address translation required to interwork between network versions. Uses a table to maintain relationship between IPv6 address and ports to IPv4 public address of 6-4 NAT gateway.

Question 2 Security **[30 marks]**

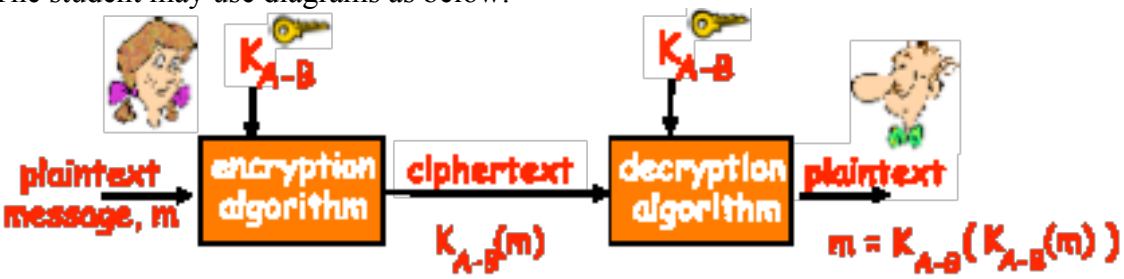
(a) [3 marks] Explain briefly what is meant by confidentiality, integrity and authentication.

Answer:

Confidentiality: only sender and intended receiver should "understand" the message contents, sender encrypts message, receiver decrypts message
Authentication: sender and receiver confirm the identity of each other
Message Integrity: sender and receiver want to ensure the message is not altered (in transit, or afterwards) without detection

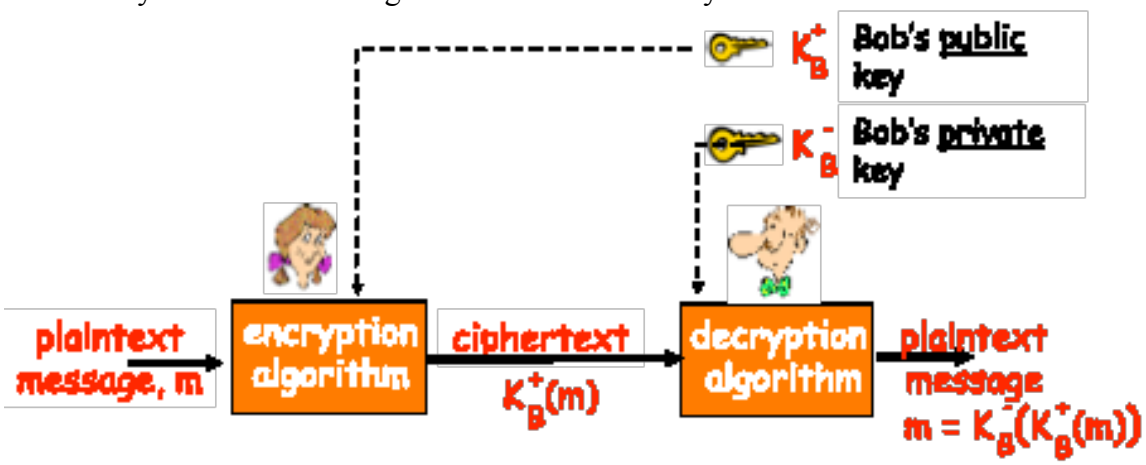
(b) [10 marks] Compare and contrast symmetric key cryptography (typified by the use of the DES algorithm), with public cryptography (typified by the use of the RSA algorithm). In your answer you should list the major features of these approaches, but not discuss the details of DES or RSA.

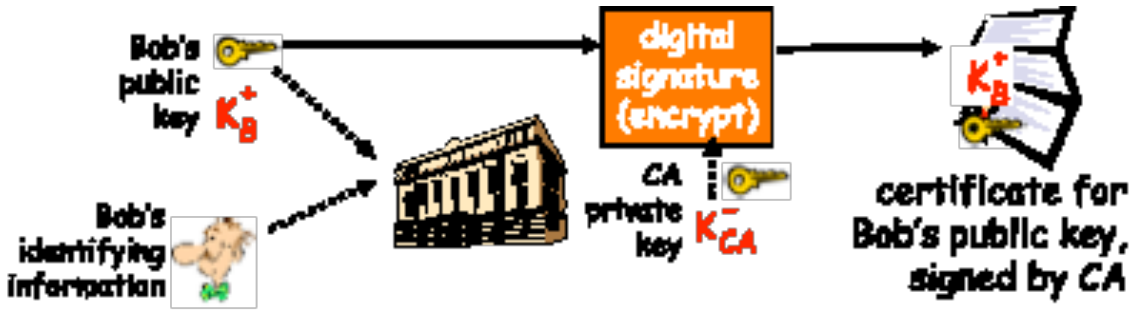
Answer:
The student may use diagrams as below:



symmetric key cryptography: sender and receiver keys are identical
(DES: 56-bit symmetric key, operating on 64-bit plaintext input
Making DES more secure:
use three keys sequentially (3-DES) on each datum
use cipher-block chaining)

public key cryptography
different approach [Diffie-Hellman76, RSA78]
sender, receiver do not share secret key
public encryption key known to all is used
private decryption key is known only to the receiver
Key distribution through Certification Authority CA

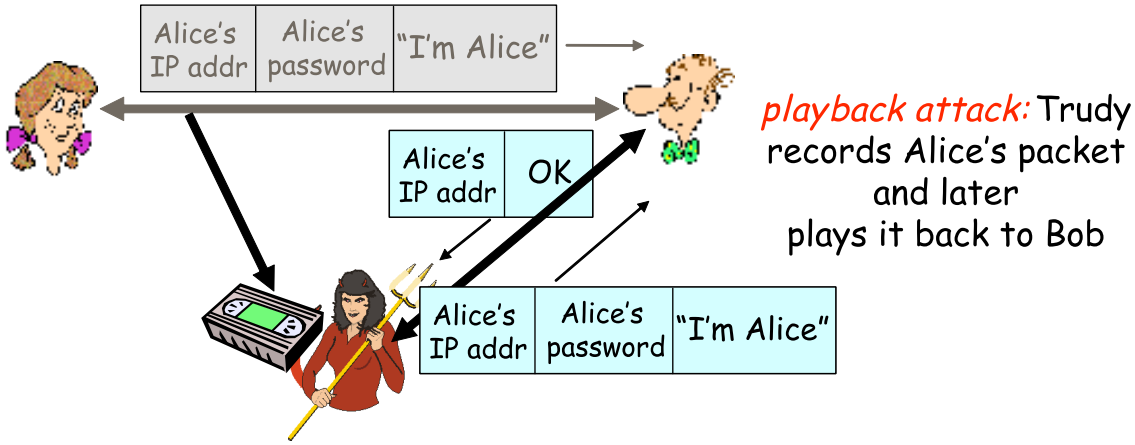




(c) There are a number of techniques that can be used to attack communicating entities during the authentication phase of a communication session. Using diagrams where appropriate describe and discuss the following:

i. [4 marks] A replay attack (also known as a playback attack).

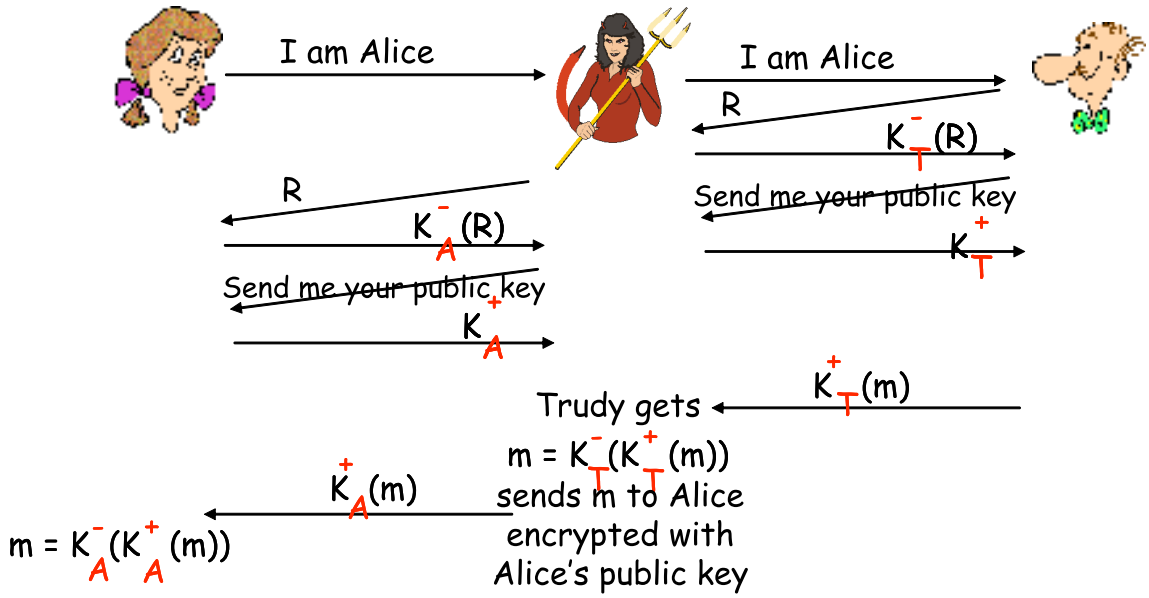
Answer:



A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution

ii. [8 marks] A man in the middle attack. In your answer discuss whether the use of public key cryptography would solve the problem

Answer:
In cryptography, a man-in-the-middle attack (MITM) is an attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised. The attacker must be able to observe and intercept messages going between the two victims. The MITM attack can work against public-key cryptography as indicated in diagram below



iii. [5 marks] A reflection attack.

Answer:

The general attack outline is as follows:
The attacker initiates a connection to a target.
The target attempts to authenticate the attacker by sending it a challenge.
The attacker opens another connection to the target, and sends the target this challenge as its own.
The target responds to the challenge.
The attacker sends that response back to the target on the original connection.
If the authentication protocol is not carefully designed, the target will accept that response as valid, thereby leaving the attacker with one fully-authenticated channel connection (the other one is simply abandoned).

Question 3 Transport Layer **[30 marks]**

(a) [3 marks] What is the role of the transport layer in the 5 layer TCP/IP protocol stack?

Answer:

Transports data units from application layer, using network layer services. Provide logical communication between application processes running on different hosts. Transport protocols run in end systems sender side: breaks application messages into segments, passes to network layer receiver side: reassembles segments into messages, passes to application layer

(b) [3 marks] Describe the functionality provided by the Transmission Control Protocol (TCP)

Answer:

Point-to-point, connection oriented, full duplex, reliable, in-order byte steam, with pipelining and flow control features.

(c) Consider the TCP connection mechanism.

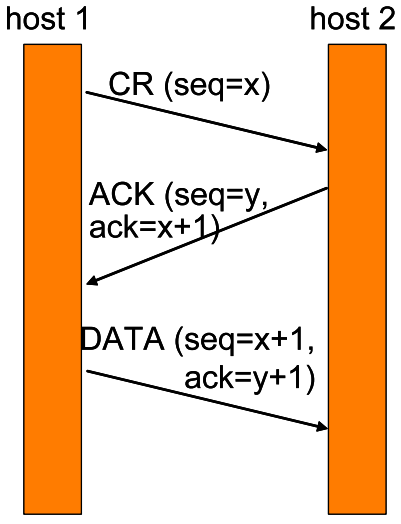
i. [1 marks] What mechanism is used to set up a TCP connection?
ii. [2 marks] Why is the mechanism needed?
iii. [3 marks] Outline how the mechanism works.

Answer:

i. 3 way handshake

ii. overcomes issue of duplicate connection requests and spurious data packet delivery can be rejected

iii. diagram:



(d) [5 marks] What is flow control and how is it achieved in TCP?

Answer:

sender won't overrun receiver's buffers by transmitting too much, too fast
RcvBuffer = size of TCP Receive Buffer

RcvWindow = amount of spare room in Buffer

receiver: explicitly informs the sender of (the dynamically changing) amount of free buffer space using the RcvWindow field in TCP segment

sender: keeps the amount of transmitted, unACKed data less than most recently received RcvWindow value

(e) [5 marks] What is end-to-end congestion control and how is it achieved in TCP?

Answer:

Caused by overload in network nodes causing packets to be delayed (causing timeout) or dropped (lost). Identified by end system either through timeout or triple ACK (loss, fast recovery mechanism). Max that can be transmitted is the receive window (rx buffer) or congestion window (MSS*number of MSS that can be transmitted) whichever is the smaller.

Uses slow start mechanism up to a threshold (half of congestion window) then start linear increase to probe for upper limit of the network capability. On event (timeout or triple ACK) the limit is detected and congestion window is set. The threshold is set to half congestion window at the event and the congestion window is set to 1 or the threshold.

(f) [8 marks] Consider the graph shown in Figure 1 which shows the TCP congestion window vs. transmission round for a TCP connection.

Answer:

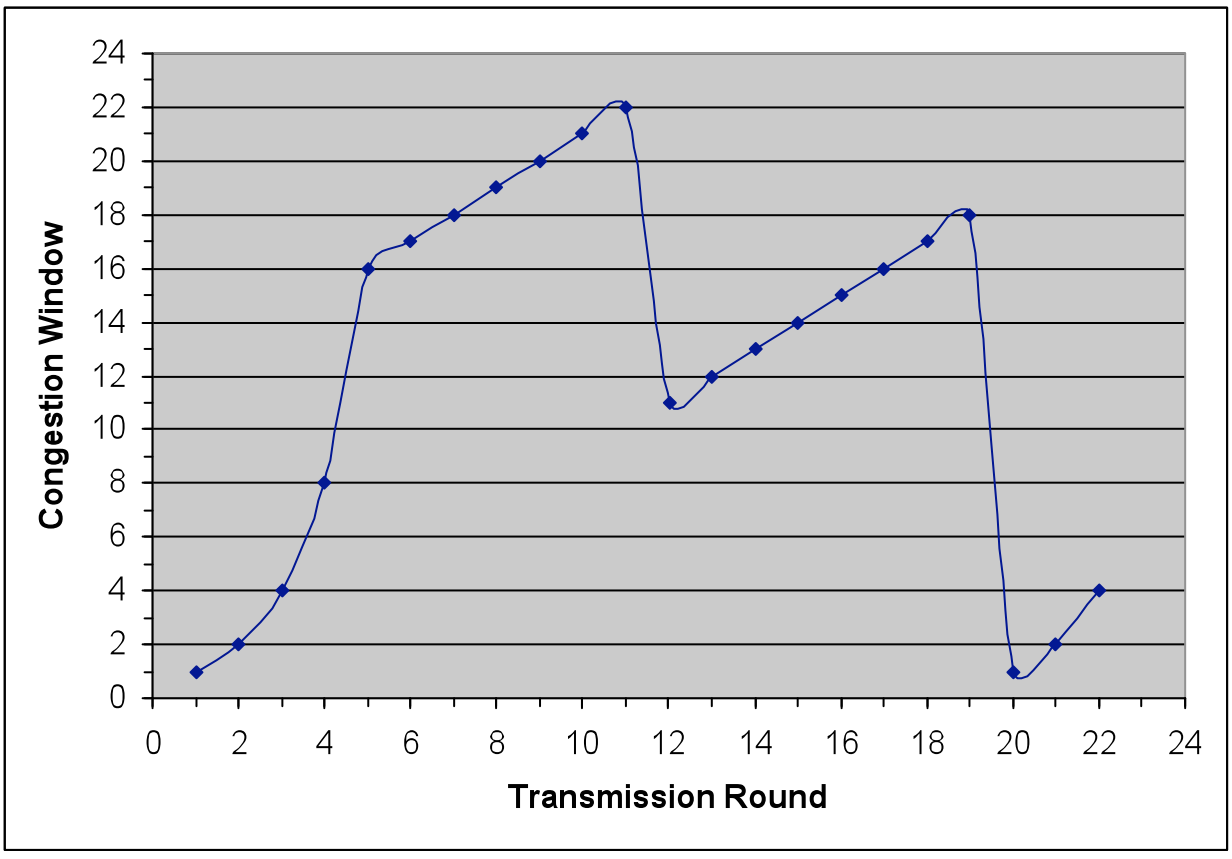


Figure 1 Congestion window vs. Transmission Round

Determine how the key parameters associated with this TCP transmission sequence have changed and what events have occurred. Identify values and events by their transmission round number.

Answer:

1 Threshold = 16. slow start Cwin = 1
5 Threshold reached, linear increase (congestion avoidance) starts
11 triple duplicate ack received (fast retransmit), threshold = half of Cwin; threshold = 11, Cwin = 11, linear increase recommences
19 timeout, packet retransmission, threshold = half of Cwin, threshold = 9, Cwin = 1, slow start commences

Question 4 Peer to Peer and the Application Layer [30 marks]

(a) [10 marks] Compare and contrast the application protocols SMTP and HTTP.

Answer:

HTTP = pull

SMTP = push

Both use ASCII based command/response interactions and status codes

Both typically have a header plus a body for content. Both use TCP connections.

HTTP = each object encapsulated in its own response message, identifying the encoded object

SMTP = multiple objects sent in a multi-part message, uses MIME (multimedia extensions) for message encoding

SMTP – pushes message from client to SMTP server, email message contains list of recipients: user@destination, server delivers mail to remote (destination) server, client polls server to receive email.

HTTP – user selects content identified by URL, which identifies the server on which it is located. Server responds with requested content. Server may tailor content to browser/user.

(b) [14 marks] Compare and contrast the architecture of peer to peer applications, such as Napster, Gnutella, and KaZaA studied in the course. In your answer discuss the mechanisms for managing the peer to peer network, locating content and how control and data transmission is accomplished.

Answer:

Examples based around file sharing P2P networks. Typically a P2P process consists of both a web client and a transient web server component.

Napster: centralised directory mechanism. Client connects to central server (single point of failure) identifying IP address and content that it will share. Client makes a query for content to the central server, which responds with a list of clients willing to share that content. Content location centralised but file transfer is decentralised. Joining the P2P network is easy and queries are centralised.

Gnutella: completely decentralised, overlay network creating a graph of connected peers. Typically a peer is connected to < 10 overlay neighbours. A query for content is sent using a query message to all neighbours. Peers forward the query message and respond to a hit with a QueryHit message. Joining the P2P network is an issue: use a list of candidate peers and well known peers. Client sends out a ping message and receive back pong messages. To avoid broadcast storms in large P2P networks a Query message must be limited, by adding a time to live field, decremented by one through each peer it is transmitted. Usually a value of 6 is used (degrees of separation).

KaZaA – provides a hybrid architecture between Gnutella and Napster. It uses a group leader for a group of clients. The group leader interacts with other group leaders through TCP connections and connects to each child(client) through a TCP connection and gathers from its clients their content information. Each file of content is identified by a hash and a descriptor.

Clients query group leader with keywords, they responds with matches containing metadata, hash and IP address. Group leaders can query other group leaders. Clients then select a peer from which to download content. KaZaA offers some additional refinements: limitation on simultaneous uploads to limit load; allows request queuing, provides incentive priorities such that clients who share content have priority, and parallel downloading (chunks from different providers, to optimise transfer).

(c) [6 marks] Briefly explain how Chord enables content to be found in a peer-to-peer network.

Answer:

N participating users whose node IP addresses are hashed (using SHA-1) to create a 160 bit node identifier. These are arranged in ascending order in a circle, some of which are participating nodes. A function successor(k) allows participating nodes to be determined.

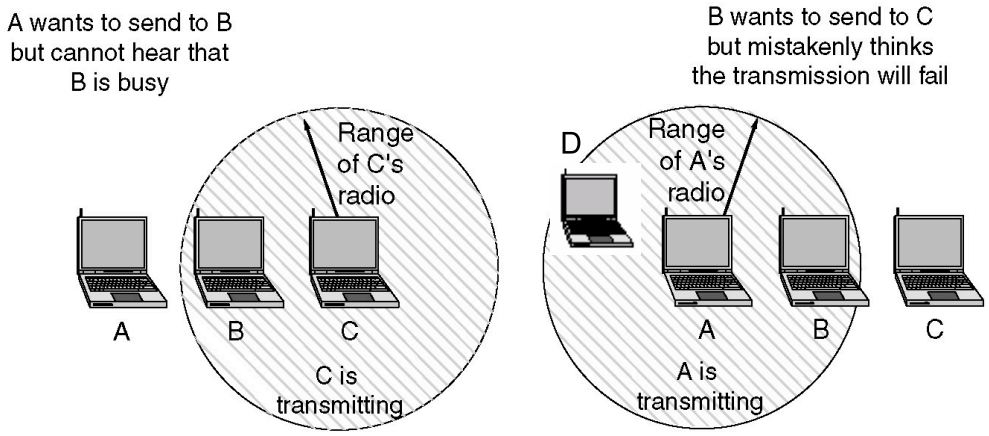
Records are hashed (SHA-1) to generate a key, thus key = hash(name). To make available a user builds a tuple (name, IP address) and asks successor(hash(name)) to store the tuple.

A user who wants to look up a name will hash name and get the key, then uses successor(key) to find the address of the node storing its index tuple. To speed search Chord uses a finger table to speed up a search.

Question 5 Wireless and Routing? **[30 marks]**

(a) [4 marks] Describe the hidden station and exposed station problem found in wireless networking.

Answer:

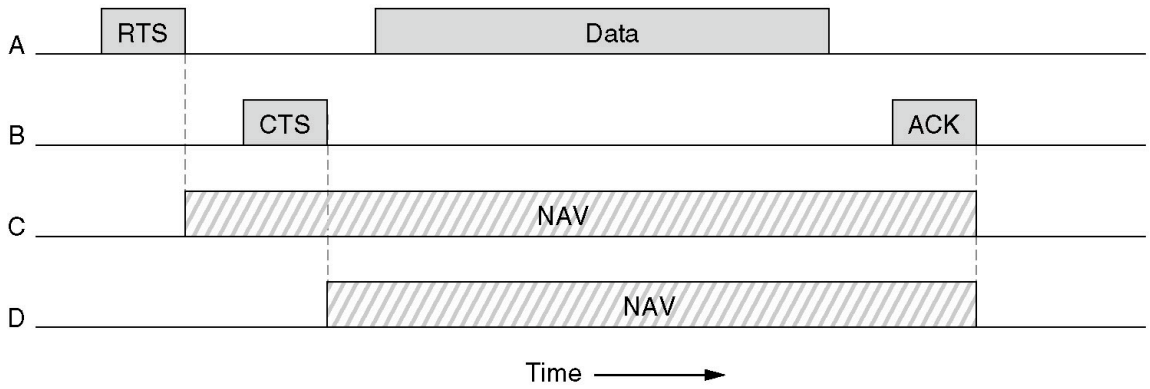


Hidden station: A cannot detect the presence of C so thinks it can transmit

Exposed station: A is transmitting to D so B detecting signal assumes it cannot transmit to C

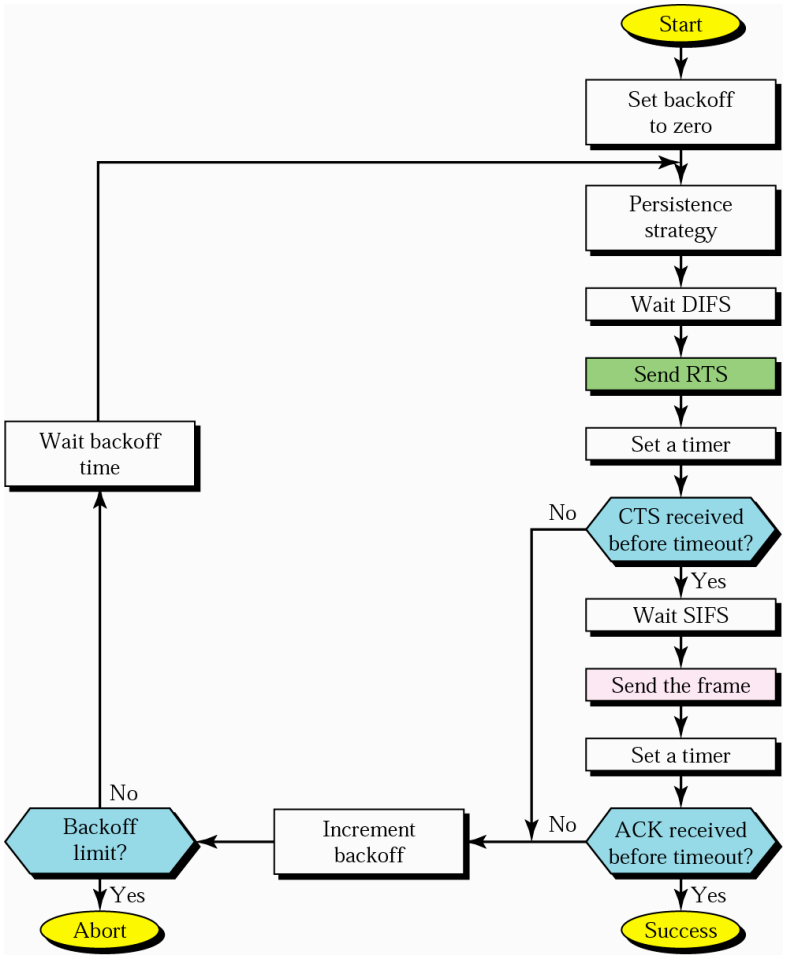
(b) [6 marks] Briefly describe the how the wireless LAN protocol CSMA/CA is able to control the hidden station and exposed station problem.

Answer:
Carrier Sense Multiple Access with Collision avoidance. IEEE 802.11 CSMA/CA provides two signals RTS (Request To Send) and CTS (Clear-To-Send) which tell all stations within range that transmission is going to occur.



The use of virtual channel sensing using CSMA/CA. Our stations: A wants to talk to B, C is in range of A but D is not. However D is in range of B. NAV are "internal" states to C and D (periods when they can't transmit)

The student may draw the CSMA/CA flow chart or similar to enhance the explanation, but is not essential.



(c) [10 marks] The IEEE 802.11 frame format is shown in Figure 2, which shows the four address fields and the details of the frame control field. Explain why the 802.11 frame format requires four address fields. In your explanation identify the other two control fields that would be used in determining the use of the address fields.

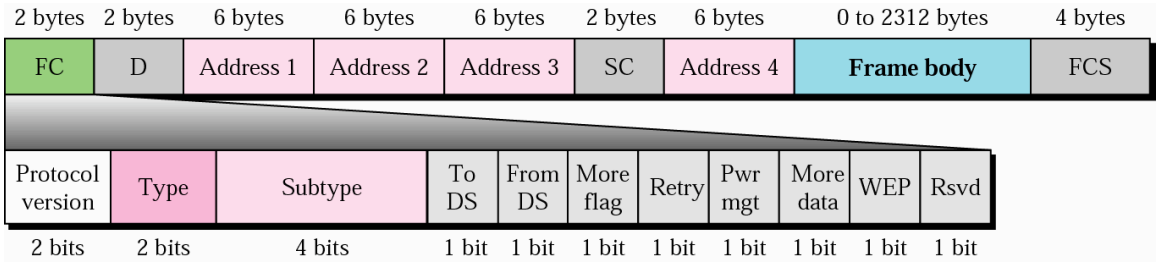
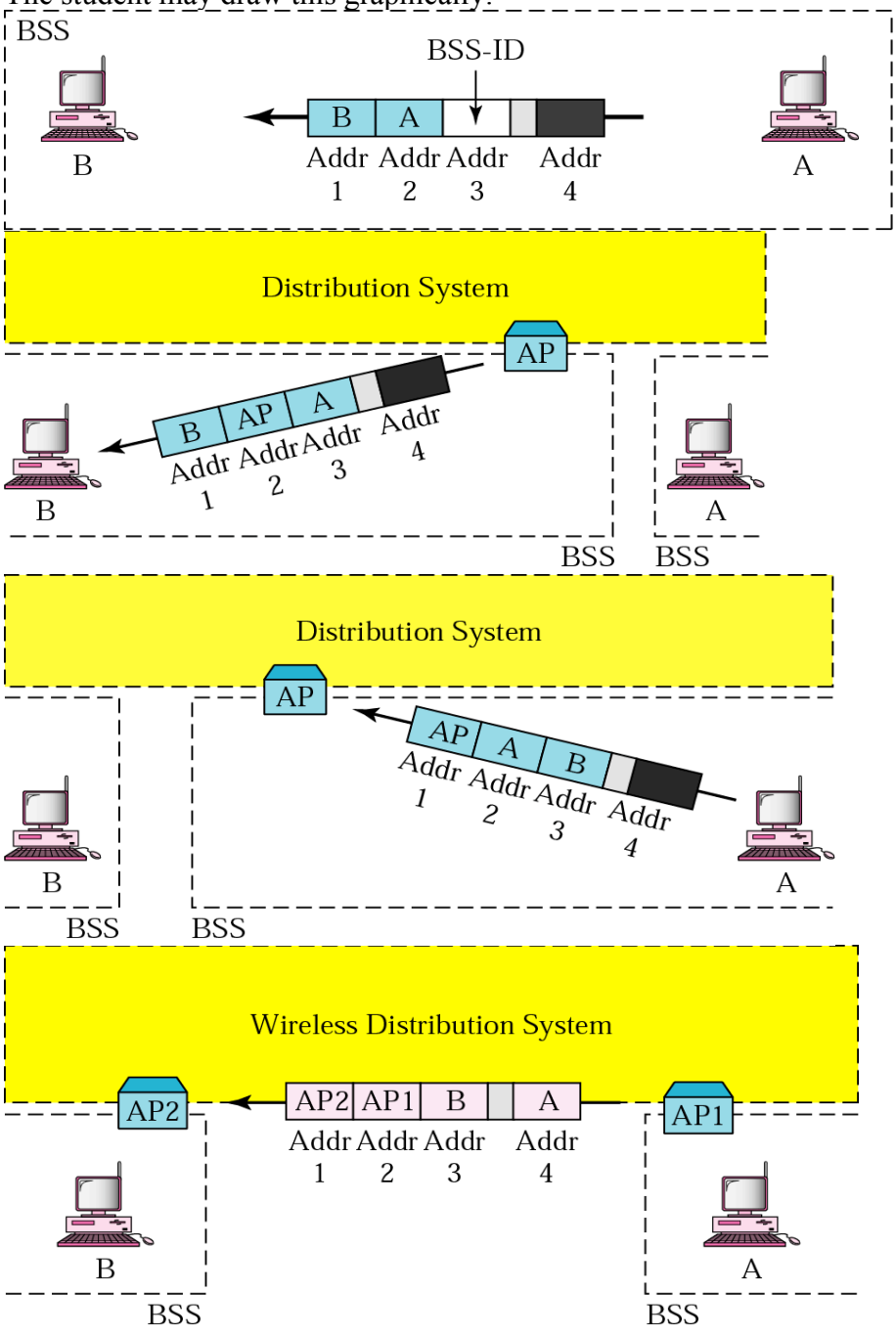


Figure 2 IEEE 802.11 wireless LAN frame format

Answer:

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	Destination station	Source station	BSS ID	N/A
0	1	Destination station	Sending AP	Source station	N/A
1	0	Receiving AP	Source station	Destination station	N/A
1	1	Receiving AP	Sending AP	Destination station	Source station

The student may draw this graphically:



(d) The ad hoc on-demand distance vector (AODV) protocol is used to route datagrams in ad hoc networks. For the topology given in Figure 3 determine the following:

i. [4 marks] The sequence of route request packets created when creating a path from A to D (assume that the route to D is not known by the intermediate nodes)

ii. [3 marks] The route reply that is delivered to A and the route table at A

iii. [3 marks] briefly describe what will occur if node G ceases to operate.

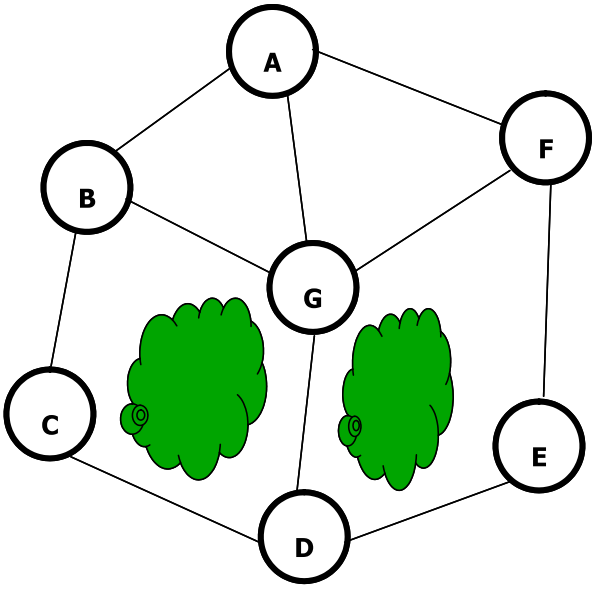


Figure 3 Wireless network topology

Answer:

i. A broadcasts route request to B, F and G. B, F and G will broadcast – G will dump the duplicate requests received from nodes B and F. D will receive a broadcast from G and will respond. Nest round it will receive a broadcast from C and E but will dump them as duplicates. Each node maintains a route entry

ii. Route reply will be unicast from D to G to A updating routing table entries.

At A a routing table entry of the following would be created:

Destination	next hop	cost/distance
D	G	2

iii G ceases to operate, either on heartbeat not answered or data transmission failure node G is declared down and all nodes using node G as an active route will purge all routing table entries containing G. Node A will then broadcast out a route request and will have returned a path through B-C or F-E.

* * * * * * * * * * * * * * * * * * *