**VASAVI COLLEGE OF ENGINEERING (Autonomous)**

**Ibrahimbagh, Hyderabad-31**

**Department of Computer Science & Engineering**

**Computer Networks**

**Assignment-III**

Academic year: 2018-2019 Class: ¾ CSE B Faculty: T Naishitha

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Set I (1602-17-733-061 to 1602-15-733-067)** |  |  |  |
| **S No** | **Question** | **Marks** | **Bloom’s Taxonomy** | **CO mapping** |
| 1 | In an IPv4 datagram, the M bit is 0, the value of HLEN is 10, the value of total length is 400 and the fragment offset value is 300. The position of the datagram, the sequence numbers of the first and the last bytes of the payload, respectively are   |  |  | | --- | --- | |  |  | | 1 | Applying | CO3 |
| 2 | The diagram below shows a typical DNS scenario that might occur when a host accesses a remote web page         1. Assuming that all caches are empty initially, show the entries that would be added to the local DNS server’s cache by the end of this scenario. 2. Show the entries that would be added to the host’s cache. | 1 | Applying | CO 5 |
| 3 | Consider different activities related to email:  m1: Send an email from a mail client to a mail server  m2: Download an email from mailbox server to a mail client  m3: Checking email in a web browser  Which is the application level protocol used in each activity?  A  m1: HTTP m2: SMTP m3: POP  B  m1: SMTP m2: FTP m3: HTTP  C  m1: SMTP m2: POP m3: HTTP  D  m1: POP m2: SMTP m3: IMAP | 1 | Applying | CO 5 |
| 4 | Suppose that two parties A and B wish to setup a common secret key (D-H key) between themselves using the Diffie-Hellman key exchange technique. They agree on 7 as the modulus and 3 as the primitive root. Party A chooses 2 and party B chooses 5 as their respective secrets. Their D-H key is \_\_\_\_\_\_\_ . Justify. | 1 | Applying | CO 5 |
| 5 | What is the total size of the minimum TCP MTU, including TCP and IP overhead but not including data link layer overhead? | 1 | Applying | CO 4 |
|  | **Set II (1602-15-733-008 to 1602-15-733-015)** |  |  |  |
| 1 | Consider a network with 6 routers R1 to R6 connected with links having weights as shown in the following diagram CN_2010_01   All the routers use the distance vector based routing algorithm to update their routing tables. Each router starts with its routing table initialized to contain an entry for each neighbour with the weight of the respective connecting link. After all the routing tables stabilize, how many links in the network will never be used for carrying any data?  Suppose the weights of all unused links in the previous question are changed to 2 and the distance vector algorithm is used again until all routing tables stabilize. How many links will now remain unused? | 1 | Applying | CO3 |
| 2 | DNS uses UDP instead of TCP. If a DNS packet is lost, there is no automatic recovery. Does this cause a problem? If so, how it is solved? | 1 | Applying | CO 5 |
| 3 | What is the maximum size of data that the application layer can pass on to the TCP layer below?  A  Any size  B  216 bytes - size of TCP header  C  216 bytes  D  1500 bytes | 1 | Applying | CO 5 |
| 4 | Pick the correct answer for the following applicaations. i. Telnet ii. DNS iii.Multimedia Protocols iv. Trivial File transfer protocol v. Real time applications vi. HTTP vii. Routing Protocols   1. i,ii,iv,v uses TCP and remaining applications uses UDP 2. i,iv,vi uses TCP and remaining applications uses UDP 3. i,iv,vi uses UDP and remaining applications uses TCP 4. i,vi uses TCP and remaining applications uses UDP | 1 | Applying | CO 5 |
| 5 | A sender is employing public key cryptography to send a secret message to a receiver. Which one of the following statements is TRUE? **(A)** Sender encrypts using receiver’s public key **(B)** Sender encrypts using his own public key **(C)** Receiver decrypts using sender’s public key **(D)** Receiver decrypts using his own public key | 1 | Applying | CO 5 |
|  | **Set III (602-15-733-016 to 1602-15-733-022)** |  |  |  |
| 1 | Consider a network with five nodes, N1 to N5, as shown below.  The network uses a Distance Vector Routing protocol. Once the routes have stabilized, the distance vectors at different nodes are as following. N1: (0, 1, 7, 8, 4) N2: (1, 0, 6, 7, 3) N3: (7, 6, 0, 2, 6) N4: (8, 7, 2, 0, 4) N5: (4, 3, 6, 4, 0)  Each distance vector is the distance of the best known path at the instance to nodes, N1 to N5, where the distance to itself is 0. Also, all links are symmetric and the cost is identical in both directions. In each round, all nodes exchange their distance vectors with their respective neighbors. Then all nodes update their distance vectors. In between two rounds, any change in cost of a link will cause the two incident nodes to change only that entry in their distance vectors. 52. The cost of link N2-N3 reduces to 2(in both directions). After the next round of updates, what will be the new distance vector at node, N3. | 1 | Applying | CO 3 |
| 2 | Can a machine with a single DNS name have multiple IP addresses? How could this occur? | 1 | Applying | CO 5 |
| 3 | Identify the correct order in which the following actions take place in an interaction between a web browser and a web server.  1. The web browser requests a webpage using HTTP.  2. The web browser establishes a TCP connection  with the web server.  3. The web server sends the requested webpage  using HTTP.  4. The web browser resolves the domain name  using DNS. | 1 | Applying | CO 5 |
| 4 | RSA algorithm is used by choosing two prime numbers, say p=7 and q=17. If the pubic key is e=5, then what is the value of d? What is the cipher value to transmit the character ‘F’? | 1 | Applying | CO 5 |
| 5 | The TCP in station A sends a SYN segment with ISN = 1000 and MSS = 1000 to station B. Station B replies with a SYN segment with ISN = 5000 and MSS = 500. Suppose station A has 10,000 bytes to transfer to B. Assume the link between stations A and B  is 8 Mbps and the distance between them is 200 m. Neglect the header overheads to keep the arithmetic simple. Station B has 3000 bytes of buffer available to receive data from A. Sketch the sequence of segment exchanges, including the parameter values in the segment headers, and the state as a function of time at the two stations under the following situations:  a. Station A sends its first data segment at t = 0. Station B has no data to send and sends an ACK segment every other frame.  b. Station A sends its first data segment at t = 0. Station B has 6000 bytes to send and sends its first data segment at t = 2 ms. | 1 | Applying | CO 4 |
|  | **Set IV (1602-15-733-023 to 1602-15-733-029)** |  |  |  |
| 1 | The TCP in station A sends a SYN segment with ISN = 1000 and MSS = 1000 to station B. Station B replies with a SYN segment with ISN = 5000 and MSS = 500. Suppose station A has 10,000 bytes to transfer to B. Assume the link between stations A and B is 8 Mbps and the distance between them is 200 m. Neglect the header overheads to keep the arithmetic simple. Station B has 3000 bytes of buffer available to receive data from A. Sketch the sequence of segment exchanges, including the parameter values in the segment headers, and the state as a function of time at the two stations under the following situations:  a. Station A sends its first data segment at t = 0. Station B has no data to send and sends an ACK segment every other frame.  b. Station A sends its first data segment at t = 0. Station B has 6000 bytes to send and sends its first data segment at t = 2 ms. | 1 | Applying | CO 4 |
| 2 | A graphical HTML browser resident at a network client machine Q accesses a static HTML webpage from a HTTP server S. The static HTML page has exactly one static embedded image which is also at S. Assuming no caching, which one of the following is correct about the HTML webpage loading (including the embedded image)?  A  Q needs to send at least 2 HTTP requests to S, each necessarily in a separate TCP connection to server S  B  Q needs to send at least 2 HTTP requests to S, but a single TCP connection to server S is sufficient  C  A single HTTP request from Q to S is sufficient, and a single TCP connection between Q and S is necessary for this  D  A single HTTP request from Q to S is sufficient, and this is possible without any TCP connection between Q and S | 1 | Applying | CO 5 |
| 3 | RSA algorithm is used by choosing two prime numbers, say p=397 and q=401. If the pubic key is e=343, then what is the value of d? What is the cipher value to transmit ’1314’? | 1 | Applying | CO 5 |
| 4 | Show the sequence of bits sent from a client TELNET for the binary transmission of 11110011 00111100 11111111. | 1 | Applying | CO 5 |
| 5 | Why is a connection establishment for mail transfer needed if TCP has already established a connection? | 1 | Applying | CO 5 |
|  | **Set V (1602-15-733-030 to 1602-15-733-036)** |  |  |  |
| 1 | A computer on a 10 Mbps network is regulated by a token bucket. The token bucket is filled at a rate of 2 Mbps. It is initially filled to capacity with 16 Megabits. What is the maximum duration for which the computer can transmit at the full 10 Mbps? | 1 | Applying | CO 4 |
| 2 | In one of the pairs of protocols given below, both the protocols can use multiple TCP connections between the same client and the server. Which one is that?  A  HTTP, FTP  B  HTTP, TELNET  C  FTP, SMTP  D  HTTP, SMTP | 1 | Applying | CO 5 |
| 3 | In SMTP, show the connection establishment phase from [aaa@xxx.com](mailto:aaa@xxx.com) to [bbb@yyy.com](mailto:bbb@yyy.com). | 1 | Applying | CO 5 |
| 4 | Electronic mail systems need directories so people’s email addresses can be lookedup. To build such directories, names should be broken up into standard components(e.g., first name, last name) to make searching possible. Discuss some problems that  must be solved for a worldwide standard to be acceptable. | 1 | Applying | CO 5 |
| 5 | It has been proposed to foil DNS spoofing using ID prediction by having the server put in a random ID rather than using a counter. Discuss the security aspects of this approach   |  | | --- | |  | | 1 | Applying | CO 5 |
|  | **Set VI (1602-15-733-037 to 1602-15-733-43)** |  |  |  |
| 1 | Maximum segment life time is 60 sec and 100 mbps link. Find how many number of minimum bits required to avoid wraparound of sequence numbers. | 1 | Applying | CO 4 |
| 2 | Which one of the following statements is NOT correct about HTTP cookies?  A  A cookies is a piece of code that has the potential to compromise the security of an Internet user  B  A cookie gains entry to the user’s work area through an HTTP header  C  A cookie has an expiry date and time  D  Cookies can be used to track the browsing pattern of a user at a particular site | 1 | Applying | CO 5 |
| 3 | if a DNS domain name is voyager.fhda.edu, how many labels are involved here? How many levels of hierarchy? | 1 | IV. Analyzing | CO 5 |
| 4 | Using the RSA public key encryption system, with a=1, b=2, etc.   1. If p=7 and q=11, list five legal values of d. 2. If p=13, q=31 and d=7 , find e. 3. Using p=5, q=11, and d=27, find e and encrypt “abcdefghij”. | 1 | Applying | CO 5 |
| 5 | Suppose that everyone in a group of N people wants to communicate secretly with the N–1 others using symmetric key cryptographic system. The communication between any two persons should not be decodable by the others in the group. The number of keys required in the system as a whole to satisfy the confidentiality requirement is\_\_\_\_\_\_\_\_\_\_\_\_\_ | 1 | Applying | CO 5 |
|  | **Set VII (1602-15-733-044 to 1602-15-733-050)** |  |  |  |
| 1 | Consider an instance of TCP’s Additive Increase Multiplicative Decrease (AIMD) algorithm where the window size at the slow start phase is 2 MSS and the threshold at the start of the first transmission is 8 MSS. Assume that a timeout occurs during the fifth transmission. Find the congestion window size at the end of the tenth transmission. | 1 | Applying | CO 4 |
| 2 | Which of the following is/are example(s) of stateful application layer protocols?  (i) HTTP  (ii) FTP  (iii) TCP  (iv) POP3 | 1 | Applying | CO 5 |
| 3 | Compare cipher block chaining with cipher feedback mode in terms of the number of encryption operations needed to transmit a large file. Which one is more efficient and by how much? | 1 | Applying | CO 5 |
| 4 | It has been proposed to foil DNS spoofing using ID prediction by having the server put in a random ID rather than using a counter. Discuss the security aspects of this approach   |  | | --- | |  | | 1 | Applying | CO 5 |
| 5 | In Diffie-Hellman key exchange protocol Alice and Bob agree on p = 23 and g = 5. The public keys of Alice and Bob are 8 and 19 respectively. If Alice’s private key is 6, then what is the secret key shared between them? | 1 | Applying | CO 5 |
|  | **Set VIII (1602-15-733-051 to 1602-15-733-057)** |  |  |  |
| 1 | An application layer is an abstraction layer that specifies the shared communications protocols and interface methods used by hosts in a communications network. Consider the following statements regarding various application layer protocols: (S1) : BOOTP is a Host initialization protocol which is implemented using the Transmission Control Protocol (TCP) as transport protocol. (S2) : Domain Name System (DNS) is Networking support protocol which uses User Data Protocol (UDP) as transport protocol. (S3) : Simple Network Management Protocol (SNMP) is a Remote host management protocol which uses Transmission Control Protocol (TCP) as transport protocol. Which of the following option is True? | 1 | Applying | CO 5 |
| 2 | To find the IP address of a destination, we need the service of DNS. DNS needs the service of UDP or TCP. UDP or TCP needs the service of IP. IP needs an IP destination address. Is this a vicious cycle here? | 1 | Applying | CO 5 |
| 3 | A TCP message consisting of 2100 bytes is passed to IP for delivery across two networks. The first network can carry a maximum payload of 1200 bytes per frame and the second network can carry a maximum payload of 400 bytes per frame, excluding network overhead. Assume that IP overhead per packet is 20 bytes. What is the total IP overhead in the second network for this transmission? | 2 | Applying | CO 4 |
| 4 | If maximum network layer payload size is 1480 bytes, what is the maximum TCP payload size? | 1 | Analyzing | CO 4 |
|  | **Set IX (1602-15-733-058 to 1602-15-733-60, 1602-15-733-301 to 1602-15-733-304)** |  |  |  |
| 1 | Consider the set of activities related to e-mail A : Send an e-mail from a mail client to mail server B : Download e-mail headers from mail box and retrieve mails from server to a cache C : Checking e-mail through a web browser The application level protocol used for each activity in the same sequence is  A  SMTP, HTTPS, IMAP  B  SMTP, POP, IMAP  C  SMTP, IMAP, HTTPS  D  SMTP, IMAP, POP | 1 | Applying | CO 5 |
| 2 | Which protocol is used for real time and multimedia applications?   1. TCP 2. UDP 3. ARP 4. SMTP | 1 | Applying | CO 4 |
| 3 | Do you think a recursive resolution is normally faster than an interactive one? Explain. | 1 | Analyzing | CO 5 |
| 4 | C:\Documents and Settings\Exam\My Documents\My Pictures\cn.bmp | 2 | Applying | CO 4 |
|  | **Set X (1602-15-733-305 to 1602-15-733-312, 1602-15-733-037)** |  |  |  |
| 1 | C:\Documents and Settings\Exam\My Documents\My Pictures\cn2.bmp | 1 | Applying | CO 4 |
| 2 | In Diffie-Hellman key exchange protocol Alice and Bob agree on p = 23 and g = 5. The public keys of Alice and Bob are 8 and 19 respectively. If Alice’s private key is 6, then what is the secret key shared between them? | 1 | Analyzing | CO 5 |
| 3 | In RSA let p=11, q=17. If the public key is 7, then what is the private key computed? | 1 | Applying | CO 5 |
| 4 | C:\Documents and Settings\Exam\My Documents\My Pictures\cn3.bmp | 1 | Applying | CO 3 |