Problems and Solutions (Chapter 12)

1. Describe the OSI model. In which layer(s) does CDPD operate?

   [Solution]

   Application Layer: Provides access to the OSI environment for users; provides distributed information services.

   Presentation Layer: Provides application independence from data representation (syntax) differences.

   Session Layer: Provides the control structure for communication between applications; manages all aspects of connections (sessions) between cooperating applications.

   Transport Layer: Provides reliable and transparent data transfer between end points; provides end-to-end error recovery and flow control.

   Network Layer: Responsible for establishing, maintaining, and terminating connections. Provides upper layers with independence from the data transmission and switching tasks.

   Data Link Layer: Provides reliable data transfer across the physical link; manages frame synchronization in terms of error control and flow control.

   Physical Layer: Manages the movement of the unstructured bit stream over the physical medium. Handles all aspects of accessing the physical medium.

   CDPD operates on Physical Layer and Data Link Layer of the OSI model.

2. What are the differences between OSI and TCP/IP protocol models? Explain clearly.

   [Solution]

   These are the differences between OSI and TCP/IP protocol models:

   - The OSI model consists of 7 layers, whereas the TCP/IP model consists only 5 layers.
   - In the TCP/IP protocol suite, the application layer serves the purpose of the three combined layers of application, presentation and session. The OSI model made a clear distinction between the top three layers. Each application in the TCP/IP suite has to independently implement the session and presentation layer functions.
   - The OSI suite was put forward before the protocols were invented whereas in the case of TCP/IP, the model was a description of the existing protocols.
   - The OSI model supports connectionless and connection-oriented communication in the network layer, and only connection-oriented in the

transport layer. TCP/IP supports only connectionless communication in the network layer, and provides a choice of both connectionless and connection-oriented communication in the transport layer.

3. Look at your favorite website and find the difference between interior and exterior routing protocol.

   [Solution]

   An interior routing protocol is used within an autonomous system (AS), whereas an exterior routing protocol is used for routing between autonomous systems. Every AS is free to choose its own routing protocol to handle the routing of packets within itself, whereas exterior routing protocol is used to handle exterior routing.

4. "Basic RIP supports single subnet masking for each IP network", give a practical example where this becomes a critical issue.

   [Solution]

   There may be systems that use different subnet masks for different subnets within a single network.

5. What are the differences between path vector routing and shortest path routing? Explain clearly.

   [Solution]

   In the path vector routing (the routing protocol on which BGP is based) , every entry in the routing table contains the destination network, the next router and the path to reach the destination. The path usually contains an ordered list of autonomous systems that a packet should travel, which in some cases may not be the shortest path. This differs from the shortest path routing protocol that just specifies the next router in the routing table entry for the packet to be forwarded to.

6. What is DHCP? How does DHCP supports dynamic address allocation?

   [Solution]

   DHCP (Dynamic Host Configuration Protocol) was proposed to reduce the problem of the limited IPv4 address space, by dynamically allocating IP addresses to hosts that need access to the Internet once in a while. Thus, a permanent IP address does not need to be allocated. In DHCP, a host first sends a DHCP discover packet on its network, specifying its hardware address. A DHCP server then sends a DHCP offer packet to the host, specifying the offered IP address. The host may receive multiple offer packets. It then confirms its selection by broadcasting the selected IP address through a DHCP broadcast packet. The selected server sends a DHCP ACK packet, and the other servers then withdraw their offer. A lease time is associated with the IP address allocated and the host needs to renew the lease before its expiration time.

7. With suitable examples? Explain the differences between a connection-oriented and connectionless protocols.

   [Solution]

   A connection-oriented protocol needs the client and the server to establish a connection with the help of control packets, before the transmission of any data packets. This is termed as a handshake between the client and the server. The handshake procedure serves to negotiate certain parameters such as determining the flow control so as to prevent the receiver from being overwhelmed, establishing the sequence numbers between the two parties etc.

   A connectionless protocol does not involve any handshaking mechanism between the two parties before data transfer. The sender can directly send a data packet to the receiver irrespective of whether the receiver is ready to accept it or not.

   The advantage of a connectionless protocol is that it does not require the overhead involved with establishing a connection, thereby improving the time required for the first packet to be received by the receiver. This is useful when the sender needs to intermittently send a few packets, and so the time spent on establishing the connection is not justified.

8. What are the disadvantages of using wireline TCP over wireless networks?

   [Solution]

   The main disadvantage of using wireline TCP over wireless networks is that wireline TCP attributes loss of packets during packet transmission to congestion in the network. However, this may not be the case in wireless networks, where packet losses occur mainly due to the physical nature of the medium such as attenuation, thermal effects and interference in the air medium. The wireline TCP thus goes into congestion control mechanism in these cases when there is no need to do this. This further reduces the throughput.

9. Explain the significance of "initial sequence number" in TCP?

   [Solution]

   The 'Initial Sequence Number (ISN)' is the number associated with the first byte that the sender transmits. This is established during the three-way handshake. Each party specifies the ISN that it would use for the first byte. The sequence number is increased for every succeeding byte. The ISN is chosen randomly, instead of zero, to prevent any confusion because of delayed segments from previous connections.

10. What are the inherent characteristics of wireless networks that require changes in existing TCP?

    [Solution]

High packet error rate, high latency, frequent link breakages due to mobility are some of the inherent characteristics of wireless networks which require changes to be made in the existing TCP in order for it to be used in a wireless medium.

11. What are the particular advantages and disadvantages of using a split TCP approach for wireless networks?

    [Solution]

    The advantage of the split TCP approach for wireless networks is that it hides the mobility of the receiver from the sender. Its disadvantage is that the TCP connection between the sender and the receiver gets split at the intermediate BS and does not maintain end to end.

12. What are the problems faced by designers of wireless TCP stack when using link layer protocols?

    [Solution]

    In wireless TCP scenario, some of the link layer protocols uses connection information from the TCP layer (service awareness). This breaks the layer independence in TCP/IP stack.

13. What makes the fast-retransmission approach desirable in improving TCP performance over wireless networks?

    [Solution]

    In the Fast-Retransmission approach, whenever the receiver completes a handoff, it sends a certain number of acknowledgements to the sender. The TCP at the sender then reduces its window size and retransmits packets starting from the first missing packet, for which the duplicate acknowledgement has been sent. Thus TCP does not need to enter slow start.

14. When is the reliable link layer useful in enhancing TCP performance?

    [Solution]

    If the link layer provides almost in-order delivery and TCP retransmission timeout large enough to tolerate additional delays to the link layer retransmits.

15. What is the operational difference between standard ACKs used in conventional TCP and SACKs used in wireless TCP? What improvement in performance does it provide for wireless networks?

    [Solution]

    Conventional TCP uses cumulative acknowledgements wherein an ACK for a particular segment can be used cumulatively to acknowledge all the preceding segments. In SACKs used in wireless TCP, the ACKs can be used to acknowledge segments selectively rather than cumulatively. The advantage of this is that if a particular segment in a transmission is corrupted, then the sender needs to retransmit only that particular segment, thereby saving precious bandwidth that would have been wasted due to the retransmissions of the succeeding segments that have been received correctly.

16. Both I-TCP and M-TCP are split TCP approaches to improving the performance of wireline TCP over wireless networks. What is the difference between these two approaches?

    [Solution]

    In M-TCP, the receiver can make the sender enter the persist mode by advertising a zero window size in presence of frequent disconnections.

    In I-TCP, all the support needed for handling the mobility related problems, is built into the wireless side of the interaction. Handoff between two different MSRs is supported on the wireless side without having to re-establish the connection at the new MSR.

17. Even though explicit bad state notification (EBSN) appears to be a very pragmatic approach for improving TCP performance over wireless networks, what is the most significant disadvantage?

    [Solution]

    The main disadvantage of EBSN is that it requires modification to TCP code at the source.

18. Can any of the methods (e.g., I-TCP, M-TCP, SACK, EBSN, etc.) be used to improve performance of TCP over wireless ad hoc networks? Suggest any ways by which this can be done.

    [Solution]

    The above protocols are basically designed for a single hop infrastructure wireless network. To make it applicable for wireless ad-hoc networks, they needs to be modified to support the multihop wireless links with support for mobility.

19. How many interations are needed to calculate shortest path to all nodes from node 3? find the shortest distance to each node and what is the path used for each one of them?

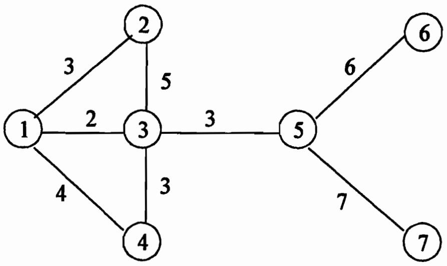

Figure for Problem 12.19.

[Solution]

2 iterations are required to calculate shortest paths from node 3.

The shortest paths from node 3 are:

Destination Node	Distance	Path using Nodes
1	2	3-1
2	5	3-2
4	3	3-4
5	3	3-5
6	9	3-5-6
7	10	3-5-7

20. Given figure in Problem 12.19 as the connectivity graph of a network, you are allowed to go through only two steps of Bellman-Ford algorithm at each node so that their complexity (and hence the time required) can be kept to a low value. What is the impact on shortest path calculations? Comment on the accuracy of the procedure?

    [Solution]

    Since the Bellman-Ford algorithm manages to find the shortest path to n-hop nodes in n iterations, the given graph will be correctly evaluated. The procedure will not be accurate for larger networks. However, running the procedure on all nodes might produce correct routing by using other distributed methods.

21. What kind of security measures used in different layers of TCP/IP? Explain.

    [Solution]

    The TCP/IP protocol stack has inbuilt security mechanisms at the various levels. These are as follows:

    TCP:

    The TCP suite uses the SSL/TLS security suite. This protocol is summarized as follows:

    Secure Socket Layer/Transport Layer Security (SSL/TLS): The SSL/TLS protocol divides the data into records. These records are of four types: user data, handshake messages, alerts and change cipher specs.

    User A first contacts user B to initiate dialogue. B sends his certificate to A. After verifying the certificate, A extracts B's public key. It then picks a random number R, encrypts it with B's public key and sends it to B. Both now compute the session key using this random number.

    IP:

The IP layer uses the IP Security protocol (IPSec) for security purposes. This protocol, coupled with the Internet Key Exchange (IKE) protocol, makes the IP layer security quite robust. A Security Association (SA) is established between the two end parties. The IKE protocol uses a Diffie Hellman key exchange process to ensure integrity of the messages passed. The security is additionally protected by an optional certificate that either party may request from each other. Having established a shared session key using IKE, the IPSec protocol comes into play. The IPSec protocol has two components, the Authentication Header (AH) and the Encapsulating Security Payload (ESP). AH provides integrity protection only while ESP provides encryption and/or integrity protection. In most cases, only one of the two is used.

IPSec operates in two modes, the tunnel and the transport mode. In the tunnel mode, the original IP packet is kept intact and a new IP header is added to the packet. The transport mode adds the IPSec information between the IP header and the remainder of the packet.

22. What are the advantages of IPv6? Discuss if an IPv6 network can support IPv4 packets and how?

    [Solution]

    Advantages of IPv6:

    - The 128-bit address space of IPv6 can support 2128 IP addresses, instead of the 232 addresses provided by IPv4, which is supposed to solve the problem of limited address space once and for all.
    - IPv6 has a fixed header size, while the IPv4 had a variable header size.
    - IPv6 has fewer fields in the basic header, which results in faster packet processing.
    - In IPv6, the routers do not perform any fragmentation, unlike IPv4.
    - IPv6 supports authentication and encryption.

    An IPv6 network can also support packets with IPv4 addressing that might be needed for the transition period. It might happen that the two end systems support IPv6, but the packet needs to travel through an intermediate IPv4 system. In this case, the packet needs to have an IPv4 address. The sender can encapsulate the IPv6 packet within an IPv4 packet (tunneling) and it sets the protocol number. Here, the end system uses a compatible IP address. For e.g., the IPv4 address 2.13.17.14 becomes 0::020D:110E.

23. IPv6 supports resource allocation. Explain how this is achieved?

    [Solution]

IPv6 can support resource allocation by the use of the flow label field in the IP header. The flow label can be used to support transmission of real time audio and video, which require resources such as high bandwidth, large buffers, long processing time, etc.