CHAPTER 20

Network Layer: Internet Protocol

Solutions to Review Questions and Exercises

Review Questions

1. The delivery of a frame in the data link layer is ***node-to-node.*** The delivery of a packet at the network layer is ***host-to-host***.
2. In a ***connectionless service***, there is no setup and teardown phases. Each packet is independent from every other packet. ***Communication has only one phase: data transfer.*** In connection-oriented service, a virtual connection is established between the sender and the receiver before transferring data. ***Communication has three phases: setup, data transfer, and teardown.*** IPv4 provides a connectionless service; IPv6 normally provides a connectionless service, but it can provide a connection-oriented service if ***flow label*** field is used.
3. Each data link layer protocol has a limit on the size of the packet it can carry. When a datagram is encapsulated in a frame, the total size of the datagram must be less than this limit. Otherwise, the datagram must be ***fragmented***. IPv4 allows fragmentation at the host and any router; IPv6 allows fragmentation only at the host.
4. First, the value of the checksum field is set to 0. Then the entire header is divided into16-bit sections and added together. The result (sum) is complemented and inserted into the checksum field. ***The checksum in the IPv4 packet covers only the header, not the data***. There are two good reasons for this. First, all higher-level protocols that encapsulate data in the IPv4 datagram have a checksum field that covers the whole packet. Second, the header of the IPv4 packet changes with each visited router, but the data do not. ***The options, if present, are included in the checksum field.***
5. ***Options*** can be used for network testing and debugging. We mentioned six options: no-operation, end-of-option, record-route, strict-source-route, loose-source-route, and timestamp. A ***no-operation*** option is a 1-byte option used as a filler between options. An ***end-of-option*** option is a 1-byte option used for padding at the end of the option field. A ***record-route*** option is used to record the Internet routers that handle the datagram. A ***strict-source-route*** option is used by the source to predetermine a route for the datagram. A ***loose-source-route*** option is

similar to the strict source route, but it is less rigid. Each router in the list must be visited, but the datagram can visit other routers as well. A ***timestamp*** option is used to record the time of datagram processing by a router.

6. See Table 20.1.

Table 20.1 *Answer to Review Question 6*

IPv4 Fields	*IPv6 Fields*	*Explanation*
Version	***Version***	Value 4 for IPv4: value 6 for IPv6
Header Length		Header length is fixed in IPv6.
Service Type	***Priority***	Name and format changed in IPv6.
Total length	***Payload length***	Name changed in IPv6.
Identification		Handled by extension headers in IPv6.
Flags		Handled by extension headers in IPv6.
Fragment offset		Handled by extension headers in IPv6.
Time to live	***Hop limit***	Name changed in IPv6.
Protocol	***Next header***	Name changed in IPv6.
Checksum		Eliminated in IPv6.
Source address	***Source address***	32 bits in IPv4; 128 bits in IPv6
Destination address	***Destination address***	32 bits in IPv4; 128 bits in IPv6
	Flow label	New in IPv6

7. In IPv4, priority is handled by a field called ***service type*** (in the early interpretation) or ***differential services*** (in the latest interpretation). In the former interpretation, the three leftmost bits of this field define the priority or precedence; in the latter interpretation, the four leftmost bits of this field define the priority. In IPv6, the four-bit ***priority*** field handles two categories of traffic: *congestion-controlled* and *noncongestion-controlled*.

8. See Table 20.2.

Table 20.2 *Answer to Review Question 8*

Options in IPv4	*Extension Headers in IPv6*	*Explanation*
No-operation and ***end-of-option***	***Hop-by-hop, Pad-1 and Pad-N***	Redesigned in IPv6
	Hop-by-hop, jumbo payload	New in IPv6
Record route		Eliminated in IPv6
Strict and ***loose source route***	***Source route***	Combined in IPv6
Timestamp		Eliminated in IPv6
	Fragmentation	Base header in IPv4
	Authentication	New in IPv6
	Encrypted security payload	New in IPv6
	Destination	New in IPv6

9. The ***checksum*** is eliminated in IPv6 because it is provided by upper-layer protocols; it is therefore not needed at this level.
10. The three transition strategies are ***dual stack***, ***tunneling***, and ***header translation***. In *tunneling* the IPv6 packet is encapsulated in an IPv4 packet when it enters the region, and it leaves its capsule when it exits the region. *Tunneling* is a strategy used when two computers using IPv6 want to communicate with each other and the packet must pass through a region that uses IPv4. In *header translation*, the header format must be totally changed from IPv4 to IPv6. *Header translation* is necessary when the majority of the Internet has moved to IPv6 but some systems still use IPv4.

Exercises

11. If no fragmentation occurs at the router, then the only field to change in the base header is the ***time to live*** field. If any of the multiple-byte options are present, then there will be changes in the option headers as well (to record the route and/or timestamp). If fragmentation does occur, the ***total length*** field will change to reflect the total length of each datagram. The ***more*** fragment bit of the flags field and the fragmentation ***offset*** field may also change to reflect the fragmentation. If options are present and fragmentation occurs, the ***header length*** field of the base header may also change to reflect whether or not the option was included in the fragments.
12.

    Header Length = Total Length - Data Length = 1200 – 1176 = 24
    HLEN = 24/4 = **6** (in decimal) $\rightarrow$ **0110** (in binary)

13.

    Advantages of a large MTU:

    - Good for transferring large amounts of data over long distances
    - No fragmentation necessary; faster delivery and no reassembly
    - Fewer lost datagrams
    - More efficient (less overhead)

    Advantages of a small MTU:

    - Good for transferring time-sensitive data such as audio or video
    - Better suited for multiplexing

14. The first byte number can be calculated from the ***offset*** itself. If the offset is 120, that means that 120×8 or 960 bytes (bytes 0 through 959) were sent before this fragment. The first byte number is therefore 960. The last byte number can be calculated by adding the total length field and subtracting one.
15. The value of the header length field of an IP packet can never be less than 5 because every IP datagram must have at least a base header that has a fixed size of 20 bytes. The value of HLEN field, when multiplied by 4, gives the number of

bytes contained in the header. Therefore the minimum value of this field is 5. This field has a value of exactly 5 when there are no options included in the header.

16. If the value of the HLEN field is 7, there are 28 (since $7 \times 4 = 28$) bytes included in the header. There are 20 bytes in the base header, so the total number of option bytes must be **8**.
17. If the size of the option field is 20 bytes, then the total length of the header is 40 bytes (20 byte base header plus 20 bytes of options). The HLEN field will be the total number of bytes in the header divided by 4, in this case ten (1010 in binary).
18. The datagram must contain 16 bytes of data:

36 byte total length – (5 HLEN field $\times$ 4) = 36 – 20 = 16 bytes

19. Since there is no option information, the header length is 20, which means that the value of HLEN field is **5** or **0101** in binary. The value of total length is 1024 + 20 or **1044** (**00000100 00010100** in binary).
20. The identification field is incremented for each non-fragmented datagram. If the first is 1024, then the last is 1024 + 99 = **1123**
21. If the M (*more*) bit is zero, this means that the datagram is either the last fragment or the it is not fragmented at all. Since the *offset* is 0, it cannot be the last fragment of a fragmented datagram. ***The datagram is not fragmented***.
22. Since the *offset* field shows the offset from the beginning of the original datagram in multiples of 8 bytes, an offset of 100 indicates that there were **800** bytes of data sent before the data in this fragment.
23. Let us first find the value of header fields before answering the questions:

    VER = 0x4 = **4**
    HLEN =0x5 = 5 $\rightarrow 5 \times 4 =$ **20**
    Service =0x00 = **0**
    Total Length = 0x0054 = **84**
    Identification = 0x0003 = **3**
    Flags and Fragmentation = 0x0000 $\rightarrow$ D = **0** M= **0** offset = **0**
    Time to live = 0x20 = **32**
    Protocol = 0x06 = **6**
    Checksum = 0x5850
    Source Address: 0x7C4E0302 = **124.78.3.2**
    Destination Address: 0xB40E0F02 = **180.14.15.2**

    We can then answer the questions:

    a. If we calculate the checksum, we get 0x0000. ***The packet is not corrupted***.
    b. Since the length of the header is 20 bytes, ***there are no options.***
    c. Since *M* = 0 and *offset* = 0, ***the packet is not fragmented.***
    d. The total length is 84. ***Data size is 64 bytes (84 –20)***.
    e. Since the value of *time to live* = 32, ***the packet may visit up to 32 more routers***.
    f. ***The identification number of the packet is 3***.
    g. ***The type of service is normal***.

24.

Data size = 200 – (5 × 4) = **180 bytes**
Offset = 200 × 8 = **1600**
The number of the first byte = offset value = **1600**
The number of the last byte = offset value + data size – 1 = **1779**
M = 0, offset ≠ 0 → **last fragment**