CHAPTER 20: Network Layer: Internet Protocol

Solutions to Selected Review Questions

Review Questions

1. 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.

2. 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.***

3. See Table 20.1.

Table 20.1 *Answer to Review Question 3*

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

4. 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.

5. See Table 20.2.

Table 20.2 *Answer to Review Question 5*

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

6. 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.

7. The ***checksum*** is eliminated in IPv6 because it is provided by upper-layer protocols; it is therefore not needed at this level.

8. ***Options*** can be used for network testing and debugging. We mentioned six options: no-operation, end-of-option, record-route, strict-source-route, loosesource-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.

9. 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***.

10. 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*.