CSC 623: Data Communications & Networking **Fall 2011** **Assignment 4 Key**

Chapter 12

12.1 The number of hops is one less than the number of nodes visited.

a. The fixed number of hops is 2.

b. The furthest distance from a station is halfway around the loop. On average, a station will send data half this distance. For an N-node network, the average number of hops is (N/4) – 1.

c. 1.

12.9a

	M	L(2)	Path	L(3)	Path	L(4)	Path	L(5)	Path	L(6)	Path
1	{1}	1	1-2	∞	—	4	1-4	∞	—	∞	—
2	{1,2}	1	1-2	4	1-2-3	4	1-4	2	1-2-5	∞	—
3	{1,2,5}	1	1-2	3	1-2-5-3	3	1-2-5-4	2	1-2-5	6	1-2-5-6
4	{1,2,5,3}	1	1-2	3	1-2-5-3	3	1-2-5-4	2	1-2-5	5	1-2-5-3-6
5	{1,2,5,3,4}	1	1-2	3	1-2-5-3	3	1-2-5-4	2	1-2-5	5	1-2-5-3-6
6	{1,2,5,3,4,6}	1	1-2	3	1-2-5-3	3	1-2-5-4	2	1-2-5	5	1-2-5-3-6

12.10a

h	$L_h(2)$	Path	$L_h(3)$	Path	$L_h(4)$	Path	$L_h(5)$	Path	$L_h(6)$	Path
0	∞	—	∞	—	∞	—	∞	—	∞	—
1	1	1-2	∞	—	4	1-4	∞	—	∞	—
2	1	1-2	4	1-2-3	4	1-4	2	1-2-5	∞	—
3	1	1-2	3	1-2-5-3	3	1-2-5-4	2	1-2-5	6	1-2-3-6
4	1	1-2	3	1-2-5-3	3	1-2-5-4	2	1-2-5	5	1-2-5-3-6

12.11 If there is a unique least-cost path, the two algorithms will yield the same result because they are both guaranteed to find the least-cost path. If there are two or more equal least-cost paths, the two algorithms may find different least-cost paths, depending on the order in which alternatives are explored

12.14 No. Although it is true that the first packet to reach node 6 has experienced the minimum delay, this delay was experienced under a condition of network flooding, and cannot be considered valid for other network conditions.

12.15 The destination node may be unreachable.

12.16 If a node sees a packet arriving on line k from node H with hop count 4, it knows that H is at most four hops away via line k. If its current best route to H is estimated at more than four hops, it marks line k as the choice for traffic to H and records the estimated distance as four hops.

The advantage of this algorithm is that, since it is an isolated technique, minimal node-node cooperation is needed. The disadvantage occurs if a line goes down or is overloaded. The algorithm as described only records improvements, not changes for the worse.

12.18 Yes. With flooding, all possible paths are used. So at least one path that is the minimum-hop path to the destination will be used.

Chapter 18

18.2 The IP entity in the source may need the ID and don't-fragment parameters. If the IP source entity needs to fragment, these two parameters are essential. Ideally, the IP source entity should not need to bother looking at the TTL parameter, since it should have been set to some positive value by the source IP user. It can be examined as a reality check. Intermediate systems clearly need to examine the TTL parameter and will need to examine the ID and don't-fragment parameters if fragmentation is desired. The destination IP entity needs to examine the ID parameter if reassembly is to be done and, also the TTL parameter if that is used to place a time limit on reassembly. The destination IP entity should not need to look at the don't-fragment parameter.

18.3 The header is a minimum of 20 octets.

18.4 Possible reasons for strict source routing: (1) to test some characteristics of a particular path, such as transit delay or whether or not the path even exists; (2) the source wishes to avoid certain unprotected networks for security reasons; (3) the source does not trust that the routers are routing properly.

Possible reasons for loose source routing: (1) Allows the source to control some aspects of the route, similar to choosing a long-distance carrier in the telephone network; (2) it may be that not all of the routers recognize all addresses and that for a particular remote destination, the datagram needs to be routed through a "smart" router.

18.6 The original datagram includes a 20-octet header and a data field of 4460 octets. The Ethernet frame can take a payload of 1500 octets, so each frame can carry an IP datagram with a 20-octet header and 1480 data octets. Note the 1480 is divisible by 8, so we can use the maximum size frame for each fragment except the last. To fit 4460 data octets into frames that carry 1480 data octets we need:

3 datagrams × 1480 octets = 4440 octets, plus

1 datagram that carries 20 data octets (plus 20 IP header octets)

The relevant fields in each IP fragment:

Total Length = 1500	Total Length = 1500	Total Length = 1500	Total Length = 40
More Flag = 1	More Flag = 1	More Flag = 1	More Flag = 0
Offset = 0	Offset = 185	Offset = 370	Offset = 555

18.10 Data plus transport header plus internet header equals 1820 bits. This data is delivered in a sequence of packets, each of which contains 24 bits of network header and up to 776 bits of higher-layer headers and/or data. Three network packets are needed. Total bits delivered = 1820 + 3 × 24 = 1892 bits.

18.13 **Class A:** **(a)** 8 bits, **(b)** 24 bits, **(c)** first bit of the first octet in a class A address is 0 (leaving 7 bits), so 2^7 = 128 – 2 (0 and 127 are disallowed) = 126 networks, **(d)** 2^{24} = 16,777,216 – 2 (host address cannot be all 0's or all 1's) = 16,777,214 hosts, **(e)** range: 1 through 126

Class B: **(a)** 16 bits, **(b)** 16 bits, **(c)** first two bits of the first octet in a class B address are 10 (leaving 14 bits), so 2^{14} = 16,384 networks, **(d)** 2^{24} = 65,536 – 2 (host address cannot be all 0's or all 1's) = 65,534 hosts, **(e)** range: 128 through 191

Class C: **(a)** 24 bits, **(b)** 8 bits, **(c)** first three bits in the first octet in a class C address are 110 (leaving 21 bits), so 2^{21} = 2,097,152 networks, **(d)** 2^8 = 256 – 2 (host address cannot be all 0's or all 1's) = 254 hosts, **(e)** range: 192 through 223

18.14 The total IPv4 address space contains 2^{32} addresses. The class A address block contains 2^{31} addresses. Therefore, it represents the 50% of the total IPv4 address space. The class B address block contains 2^{30} addresses. Thus, it represents 25% of the total IPv4 address space. The class C address block contains 2^{29} addresses. Thus, it represents 12.5% of the total IPv4 address space.

18.15 There is no difference. Both have a subnet mask of 255.255.255.0, as does a Class C address that is not subnetted.

18.16 It is valid; it is called a *noncontiguous subnet mask*, because the 16 bits of the subnet mask are not contiguous. The RFCs, however, recommend against using noncontiguous subnet masks.

18.17 **a.** 4

b. 64

18.18 255.255.255.240

18.19 **a.** 512

b. 218