Lab 06 Report

`Lines in this font represent terminal commands and terminal output.`

Lines beginning with `$` are the terminal commands that were run.

Lines in this font are the answers to the questions.

EXERCISE 1

1. Node 0 sends packets to Node 1. Node 1 sends packets to Node 4. Node 4 sends packets to Node 5. Node 2 sends packets to Node 3. Node 3 sends packets to Node 5. The packets that leave Node 0 follow the route 0-1-4-5. The packets that leave Node 2 follow the route 2-3-5. The packets do not change routes over time.

2. Between time 1.0 and 1.2, the link between Node 1 and Node 4 is broken, or unusable. This stops the transfer of packets from Node 1 to Node 4, which originated from Node 0. The route of packets from Node 0 that previously followed the route 0-1-4-5, get stuck at Node 1. The route does not change to adapt with the unusable link in the route, as the simulation uses the Link State Protocols to route the packets, which is a static protocol.

3. Additional traffic occurs between time 1.0 and 1.2 when the link between Node 1 and Node 4 becomes unusable. The extra traffic occurs between Node 1 and Node 3, as the previous routes of packets from Node 0, 0-1-4-5, is updated to 0-1-2-3-5, as the Distance Vector Protocol is not a static protocol, and updates the route over time.

4. The route with packets originating from Node 2 are unaffected in their route from the previous questions, following the route 2-3-5. The packets originating from Node 0 are now routed along 0-1-2-3-5, and avoid Node 4, as the link from Node 1 to Node 4 has a higher cost on it, and so the Distance Vector Protocol determines the shortest path, which is shorter through Node 2, than Node 4. Assuming all other links carry cost 1, the original path 0-1-4-5 has cost 5. The new path, 0-1-2-3-5 has cost 4, hence why the Distance Vector Protocol chooses the new route.

5. The link from Node 1 to Node 4 now has cost 2, making the route 0-1-4-5 have cost 4 altogether. The link from Node 3 to Node 5 now has cost 3, making the route 2-3-5 have cost 4. Thus the packets originating from Node 0 are routed along the original route 0-1-4-5 as it is the shortest path for those packets. Furthermore, with multiple paths enabled, the packets originating from Node 2 are sent along both the route 2-1-4-5 with cost 4, and route 2-3-5 with cost also 4.

EXERCISE 2

1.

2.

3.

EXERCISE 3

1. The ping of size 2000 bytes caused fragmentation. The MTU is 1500 bytes, and so disregarding any of the headers of the appropirate network layers, the ping packet would cause fragmentation the data alone. Two fragments are created when the size of the data section of the ping is 2000 bytes.

2. The reply for the 3500 byte ping is also fragmented, because the ping reply returns the data that was sent in the ping request, to the sender. Thus, the ping replies are also far greater than the MTU, even disregarding headers, and so must be fragmented.

3. The first 3500 byte ping that was sent by 192.168.1.103 to 8.8.8.8 had the following fragments.

Fragment Number	ID	Length (bytes)	Offset (bytes)	Flags
1	0x7a7b	1480 + 20 (header)	0	0x01 (More Fragments)
2	0x7a7b	1480 + 20 (header)	1480	0x01 (More Fragments)
3	0x7a7b	562 + 20 (header)	2960	0x00

4. Fragmentation has occurred on fragments of the 3500 byte ping requests. The fragments of the request are broken into 1500 byte chunks, including the header at the Network Layer. However, Ethernet adds a header of 14 bytes to this IP packet, at the Data Link Layer. Thus, when the packet is given to the Physical Link Layer, the size exceeds the MTU. Thus the fragment is again fragmented at the Physical Link Layer. This is evident by examining the Physical Link Layer packet headers for the original fragments, and noticing the 0x01 flag to indicate more fragments at the Physical Link Layer. This fragmentation of fragments only occurs on ping requests, as the repsonder is smart enough to account for the 14 byte header that the Ethernet Protocol adds to the data, so it ensures that the IP fragmentation is not to size 1500 bytes, but to size 1486 bytes.

5. As ICMP does not provide reliable data transfer, a loss of a fragment causes the receiver to abandon or drop the packet from which the fragment was lost.