1. Use the ONL RLI to configure a network with four NPRs connected in a “square” topology with links from (n1,n2), (n2,n3), (n3,n4) and (n4,n1). Also, add a “diagonal” link (n1,n3). Now, add hosts to all the otherwise unused ports and generate the default IP routes. Now examine the routing tables to determine the answer to the following questions. What path is used by packets from a host on n1 to a host on n3? What path is used by packets from a host on n2 to a host on n4?

Packets from n1 to n3 use the direct link connecting n1 and n3. Packets from n2 to n4 pass through n1 in my case, although depending on exactly how the components are connected, the path could go through either n1 or n3. The screenshot below shows the routing tables, indicating how the packets are routed.
Add a routing table for one of the hosts on n1, so that its traffic to one of the hosts on n3 passes through n2, instead of using the direct link. Create a monitoring display that displays packet transfer rates on all five of the links connecting NPRs to each other. Login to one of the hosts on n1 and ping other hosts to verify that packets are routed as you expect.

A screenshot of the modified routing table for n1p0 and the monitoring display is shown below. The first set of three peaks in the graph shows the result of pining n3p3 from n1p0. These packets take the direct link, as we can verify by noting that the peaks are on the “blue curve” which shows the transmit packet counter for port 2 of npr1. The second group of four peaks is obtained by pinging n3p2 from n1p0. This is the pair of hosts for which traffic has been re-routed through npr2 (as we can see in the routing table at left). Observe that these peaks are on the black and red curves, which show the transmit counters for port 1 of npr1 and port 4 of npr 2.

2. In ONL, IP packets are transferred inside Ethernet frames and the configuration switches that connect components to each other use VLAN tags to implement the links associated with individual experimental sessions. If one host sends 100 UDP packets per second to another host with a UDP payload size of four bytes, how much bandwidth is used on the path connecting the two hosts. Include in your calculation a 12 byte inter-frame gap between successive Ethernet frames. Compare this to the UDP “payload bandwidth”.

The UDP header is 8 bytes, the IP header is 20 bytes for a total Ethernet payload of 32 bytes. But the minimum Ethernet payload has 46 bytes, so 14 bytes of padding will be added. The overall Ethernet frame overhead is 18 bytes for the header fields, 4 bytes for the CRC, 8 bytes for the preamble and start-of-frame byte plus 12 bytes for the required inter-frame gap. So, for each packet, 88 bytes are sent on the link, so 100 packets per second translates to 8800×8=70,400 bits per second. The UDP payload bandwidth is 3200 bits per second, so the link bandwidth is 22 times he UDP bandwidth.

Repeat this calculation, assuming a UDP payload with 1000 bytes.

In this case, the Ethernet payload will have 1000+20+8=1028 bytes. Adding all the Ethernet overheads gives us 1028+42=1070 bytes, so 100 packets per second translates to 107,000×8=856,000 bits per second. The UDP payload bandwidth is 800,000 bits per second, so the link bandwidth is 1.07 times the UDP bandwidth.
3. If you install a filter on an NPR to override the standard IP route, what priority value should you use to guarantee that the filter will be used to forward the packet? Explain your answer.

   The default priority value for routes is 60, so we need to use a priority value smaller than this for our filter. Any smaller value is acceptable. Of course, we could also change the priority value used for routes to something larger, but assuming we stick with the default route priority, a filter priority of \( \leq 59 \) will ensure that the packet is forwarded using the filter.

4. Explain what auxiliary filters do and how you might use them to observe traffic passing between two hosts.

   An auxiliary filter makes a copy of any matching packet, allowing it to be processed or forwarded independently of the original packet. If we want to monitor traffic between two hosts, we can install an auxiliary filter somewhere on the route used by packets passing between the two hosts. The filter should specify the sending host’s IP address in the source IP field and the receiving host’s IP address in the destination IP field. The copies of packets created by the auxiliary filter can be directed to an arbitrary NPR port. If we have a monitoring host on that port, it can observe the flow of packets passing between the two hosts and perform whatever analysis may be required. Note that if we want to observe the traffic passing in both directions, a second auxiliary filter will be required.