Brian Atkinson

Lab2 Part 2

**Experiment 1**

2. The Wireshark capture of the event is provided in the zipped directory containing this word document. The name of the capture is *packetInCap.pcap* and contains the entire trace from network initialization to the successful pinging between hosts.

A computer screen capture

Description automatically generated with medium confidence

Figure 1: A dump of the devices in the topology.

A screenshot of a computer

Description automatically generated with medium confidence

Figure 2: Initial 'Destination Host Unreachable' messages while the protocol retrieves flow entries.

A screenshot of a computer

Description automatically generated with medium confidence

Figure 3: Pings became successful from H1 to H2 once the entry was installed.

**Experiment 2**

1. The sample code creates a class for a simple SDN controller. On initialization the controller instantiates a dictionary to track which of its ports received messages from various MAC addresses, and when it needs to communicate with an unknown MAC it floods all its neighbors. When the controller receives a *Packet\_In* message, it checks the contents of the message to see the source and destination information, and if it is an IP flow it creates a new flow rule which is forwarded on the port the *Packet\_In* was received on. As far as flow limitations, this code places no limits on the amount of time needed for a hard or soft timeout.
2. The *duration\_sec* field specifies the amount of time the flow rule has been installed. *duration\_nsec* specifies the number of nanoseconds beyond the value of *duration\_sec* that the flow has existed. *priority* specifies if the flow rule is to be given a priority value, meaning this rule will be applied before other rules of lower value priority. *idle\_timeout* and *hard\_timeout* respectively specify the amount of time the flow can go without any new traffic before being dropped and the maximum amount of time the rule is allowed to exist. *actions* tells the router executing the rule what actions to take on receipt of traffic from this flow (i.e. drop all traffic if it is to be firewalled).

A picture containing text, battery

Description automatically generated

Figure 4: The result of 'dpctl dump-flows tcp:127.0.0.1:6654'.

1. Implement so each flow is allowed to last 5 seconds:

A picture containing text, battery, receipt

Description automatically generated

Figure 5: Modified code to limit flow rule lifespan to 5 seconds

1. Implementation of flow rule such that hosts can send three successive pings to each other for a maximum of 10 times with at least 5 seconds between ping sets: