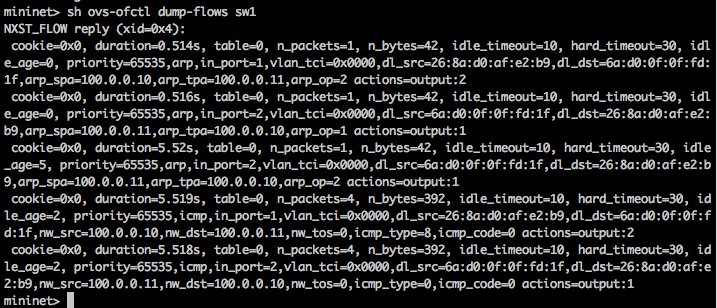
1. Switch rule tale

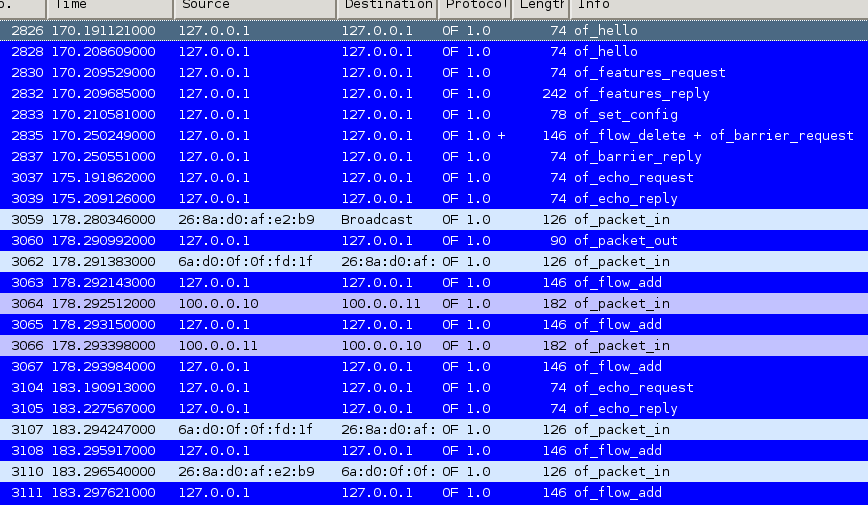
After the connection between switch and controller is established, we can get

installed rule table by controller as follows:



From the table, we can find out there are two types of flow--ARP and ICMP and more details about each flows, such as actions, timeouts, src/dst, priority , in\_port/out\_port, packets and bytes processed by each flow.

1. Wireshark capture



The steps of packet exchange to have successful ping-pong between h1 and h2 are as flows:

|  |  |  |  |
| --- | --- | --- | --- |
| steps | entities | phase | description |
| #1 | Switch->controller | Establishment | openflow\_hello message |
| #2 | controller->switch | Establishment | openflow\_hello message |
| #3 | controller->switch | Establishment | Feature Request(only open flow message header) |
| #4 | Switch->controller | Establishment | Feature reply(switch port number ,state information) |
| #5 | controller->switch | Configuration | config message include allowing packet size sent from switch |
| #6 | Switch->controller | Packet forwarding action | ARP request(of\_packet\_in) :  src : h1 ip and mac  dst: h2 ip and broadcast |
| #7 | controller->switch | Packet forwarding action | Switch sends packet out to the port mentioned in of\_packet\_out |
| #8 | Switch->controller | Packet forwarding action | ARP reply(of\_packet\_in):  src : h2 ip and mac  dst: h1 ip and mac |
| #9 | controller->switch | Flow setting | Switch add flow rules(ARP request and reply) |
| #10 | Switch->controller | Packet forwarding action | ICMP request(of\_packet\_in):  src : h1 ip and mac  dst: h2 ip and mac |
| #11 | Switch->controller | Packet forwarding action | ICMP reply(of\_packet\_in):  src : h2 ip and mac  dst: h1 ip and mac |
| #12 | controller->switch | Flow setting | Switch add flow rules(ICMP request and reply) |

From packet exchange table, we can find that the open flow rules which involved in this process are also showed in the switch rule table (part 1).