Georgia Institute of Technology

Software Defined Networking

Dr. Nick Feamster
Associate Professor

In this course, you will learn about software defined networking and how it is changing the way communications networks are managed, maintained, and secured.

School of Computer Science

Module 4.4: The Control Plane

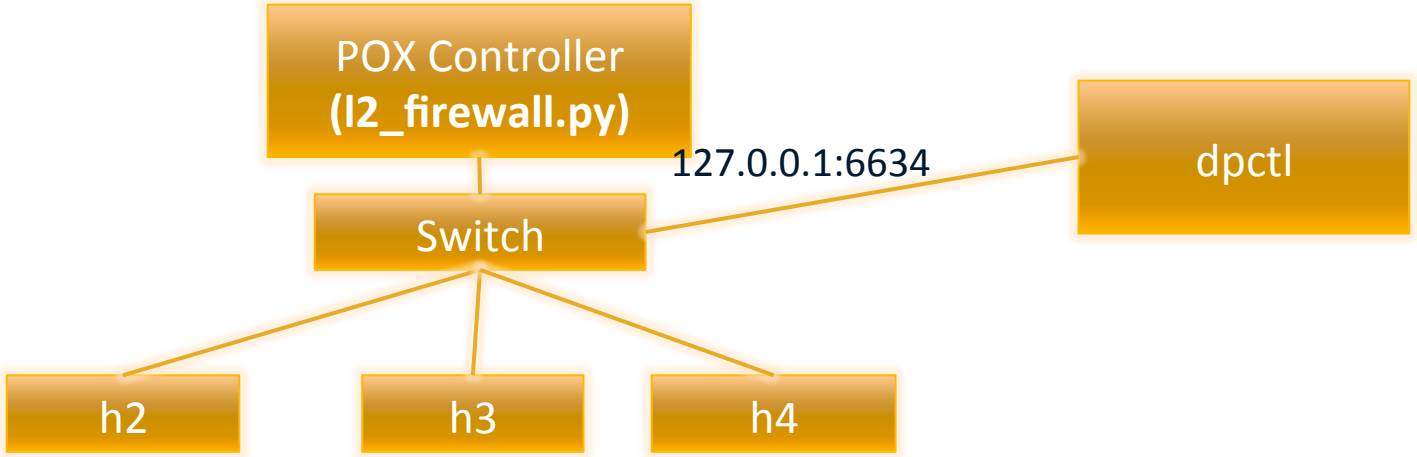
- Three Lessons
  - Control Plane Basics (OpenFlow 1.0 and Beyond)
  - SDN Controllers
  - **Using SDN Controllers to Customize Control**
    - **Part 2: Simple Firewall**
- Programming Assignment (and Quiz)
- Quiz

Customizing Control with Flow Rules

Switching

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
*	*	00:1f:..	*	*	*	*	*	*	*	port6

Example Topology: Now with Firewall



- `$ sudo mn --topo single,3 --mac --switch ovsk --controller remote`
- `dpctl` to communicate with switches
  - Switches listen on port 6634
  - Can inspect flow table entries, modify flows, etc.

POX Learning Switch Algorithm

- Use source address and switch port to update address/port table
- **Check source MAC address against firewall rules**
- Is transparent = False and either Ethertype is LLDP or the packet's destination address is a Bridge Filtered address? If yes, DROP
- Is destination multicast? If so, FLOOD.
- Is port for destination address in our address/port table? If not, FLOOD.
- Is output port the same as input port? If yes, DROP
- Install flow table entry in the switch so that this flow goes out the appropriate port. Send the packet out appropriate port.

Simple Additions to Controller

- Hash table for storing (key,value) pairs
  - Table maps (switch, src MAC) to True/False
- Controller will decide to **drop** traffic
  - If there is a firewall entry that maps to “False”
  - If there is no firewall entry
- Controller will decide to **forward** traffic
  - If there is a firewall entry that maps to “True”

Performance: Cache Decisions at Switch

- Important to limit data traffic to the controller
- When control decides to forward or drop, the switch's flow table is modified
- Decision is cached at switch until the flow table entry expires

Summary

- Customizing control is easy in SDN!
- Exploration of alternate control program
  - Turned switch into a firewall in < 40 lines of code
- Demonstrated of the performance benefits of caching forwarding decisions at switch