Software Defined Networking – Use Cases

Matt Dlubac
Department of Computer Science
Information Technology

Scott Valcourt
Director of Strategic Technology
UNH Information Technology

What is SDN?

- New approach to networking that applies the concept of virtualization to networks

- Allows for centralized and dynamic network configuration

- Moves the control plane off switches and onto SDN controllers

- OpenFlow protocol handles routing decision making and transmission

Why Use SDN?

- Centralized network configuration

- Decreased provisioning time

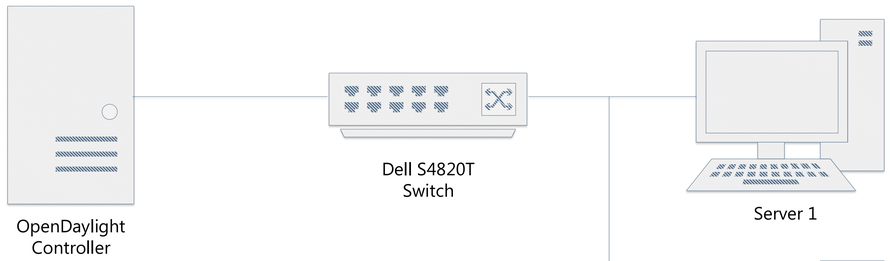
- Cost savings vs traditional networks

- Performance benefits

- Provides APIs that add programmability

- Aligns with server virtualization in data centers

Network Topology



<u>Dell S4820T Switch</u>
- OpenFlow compatible
- Configured with 10.0.0.0/24 subnet

<u>OpenDaylight Controller</u>
- Open source SDN controller that implements OpenFlow
- Configurable via CLI or web-based interface
- Assigned IP address 10.0.0.11
- Ubuntu 12.04

Server 1 & 2
- Assigned IP addresses 10.0.0.12 and 10.0.0.13
- Windows 8.1
- Running Nginx web server and FTP client/server

<u>Client 1 & 2</u>
- Assigned IP addresses 10.0.0.14 and 10.0.0.15
- OSX 10.10 and Windows 8.1
- Running traffic generation scripts

SDN Use Cases

- Bandwidth on demand

- DoS attack mitigation

- SDN-based network tap

Testing Methodology

- **Bandwidth on demand:**
  - New VLAN dynamically created to handle server backup
  - Investigating performance variances

- **DoS mitigation:**
  - SDN controller will detect abnormal traffic levels and block attack traffic
  - Determining if SDN is a viable DoS attack mitigation tool

- **Network Tap:**
  - All or selected types of traffic replicated and redirected to a new destination
  - Determining if a hardware-based network tap can be replicated with SDN

Results

Bandwidth on Demand

- Backup performed by uploading a large file to a FTP server on a congested network

- SDN flows detect traffic on port 21 and assigns those packets a different VLAN ID

- Achieved 1% increase in throughput. This was under ideal circumstances and will scale with network size and complexity

DoS Mitigation

- Open source Defense4All software is the best solution

- Sits on top of OpenDaylight

- Can protect specific hosts and links

- Places counters in network to learn normal traffic patterns

- Blocks packets when abnormal traffic levels are detected

Network Tap

- Can be achieved using native OpenDaylight flows
  - Flows forward packets to network tap IP, then to the original destination
  - Overhead is an issue

- Third party applications are a better solution, but will not match the performance of hardware based taps