Report on 'OpenFlow: Enabling Innovation in Campus Networks' by Cheng Han

Summary:

OpenFlow is a way this paper offered for researchers to run experimental protocols in the networks. It is easy-use and is based on an Ethernet switch. OpenFlow allows researchers to run experiments on heterogeneous switches in a uniform way at line-rate and with high port-density. Since the vendors are intended to hide their internal working of their switches, OpenFlow do not need to oppose the internal mechanism of these switches. Better than GENI, which plans for nationwide facilities and takes years to be deployed, OpenFlow focuses on a shorter-term question: As researchers, how can we run experiments in our campus networks? The goal of OpenFlow is to propose a new switch feature that can help extend programmability into the wiring closet of college campuses.

Main idea/solution:

Chance of making an impact is more remote for researchers to Networks nowadays, which have created an exceedingly high barrier to entry for new ideas. Today we have no practical way to experiment with new network protocols, which is bad for the development of network. Due to the nowadays lack of open software platforms that can realize four goals as: 1. Amenable to high-performance and low-cost implementations. 2. Capable of supporting a broad range of research. 3. Assured to isolate experimental traffic from production traffic. 4. Consistent with vendors' need for closed platforms, the paper mentions OpenFlow Switch as a solution.

Results:

By realizing the fact that most modern Ethernet switches and routers contain flow-tables, the researchers develop a common set of functions that run in many switches and routers. The datapath of an OpenFlow Switch consists of a Flow Table, and an action associated with each flow entry. And an OpenFlow Switch consists of at least three parts: a Flow Table, a Secure Channel and The OpenFlow Protocol. It is useful to categorize switches into dedicated OpenFlow switches and OpenFlow-enabled switches. About dedicated OpenFlow Switches, flows are broadly defined and are limited only by the capabilities of the particular implementation of the Flow Table. And each flow-entry has a simple action combing with it. There are three basic ones: Forward this flow's packets to a given port, Encapsulate and forward this flow's packets to a controller and drop this flow's packets. The entry in the Flow-table has three fields, covering packet header, the action and statistics. About the OpenFlow-enabled switches, it allows a switch to be controlled by two or more controllers for increased performance or robustness. And it must isolate experimental traffic from production traffic that is to be processed by the normal Layer 2 and Layer 3 pipeline of the switch. Two ways are provided for the separation: 1. Add a fourth action 2. Define separate sets of VLANs for experimental and production traffic. Also, additional features and more sophisticated controllers can be added. The paper gives an example of adding controllers which can dynamically add or remove flows as an experiment progress. While we test new protocol in a network used by lots of people, we need two additional properties: 1. Packets belonging to users other than us should be routed using a standard and tested routing protocol running in the switch or router from a "name-brand" vendor. 2. We should only be able to add flow entries for our traffic, or for any traffic our network administrator has allowed us to control. There are also several examples provided about how OpenFlow-enabled networks could be used to experiment with new network applications and architectures. These examples are Network Management and Access Control, VLANS, Mobile wireless VOIP clients, a non-IP network and Processing packets rather than flows.

Conclusion:

The researchers believe that OpenFlow is a feasible compromise allowing them to run experiments on heterogeneous switches and routers in a uniform way. They do not have to find the black box of the

vendors or writing vendor-specific control software. The researchers believe that with the popularity of OpenFlow among universities, the islands of OpenFlow networks will be interconnected by tunnels and overlay networks, and possibly by new OpenFlow networks running in the backbone networks that connect universities to each other.