Santa Clara University
Internet of Things RESEARCH LAB
SIOTLAB

Internet of Things Research Lab
Department of Computer Science and Engineering
Santa Clara University

IEEE International Conference on Network Softwarization (NETSOFT)

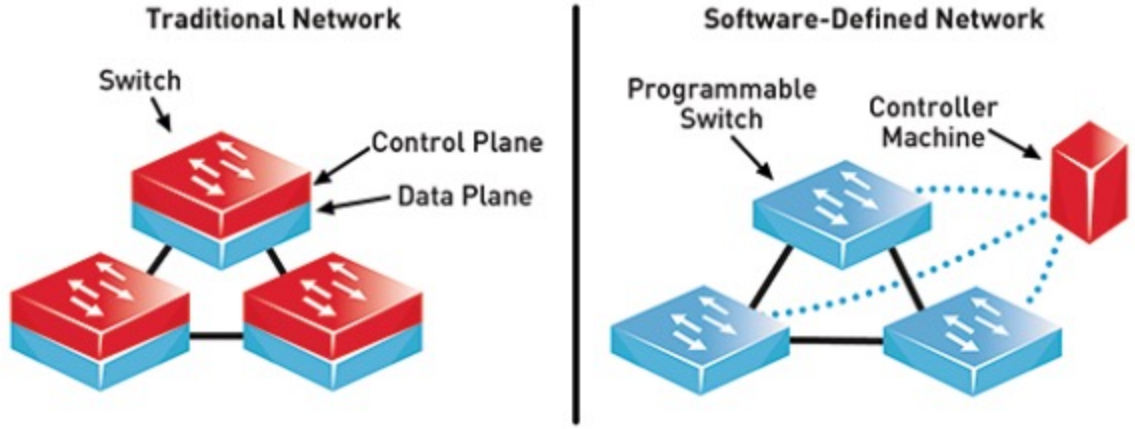
Modeling Control Traffic in Software-Defined Networks

Jesse Chen, Ananya Gopal, Behnam Dezfouli

Tokyo, Japan
June 29 - July 1

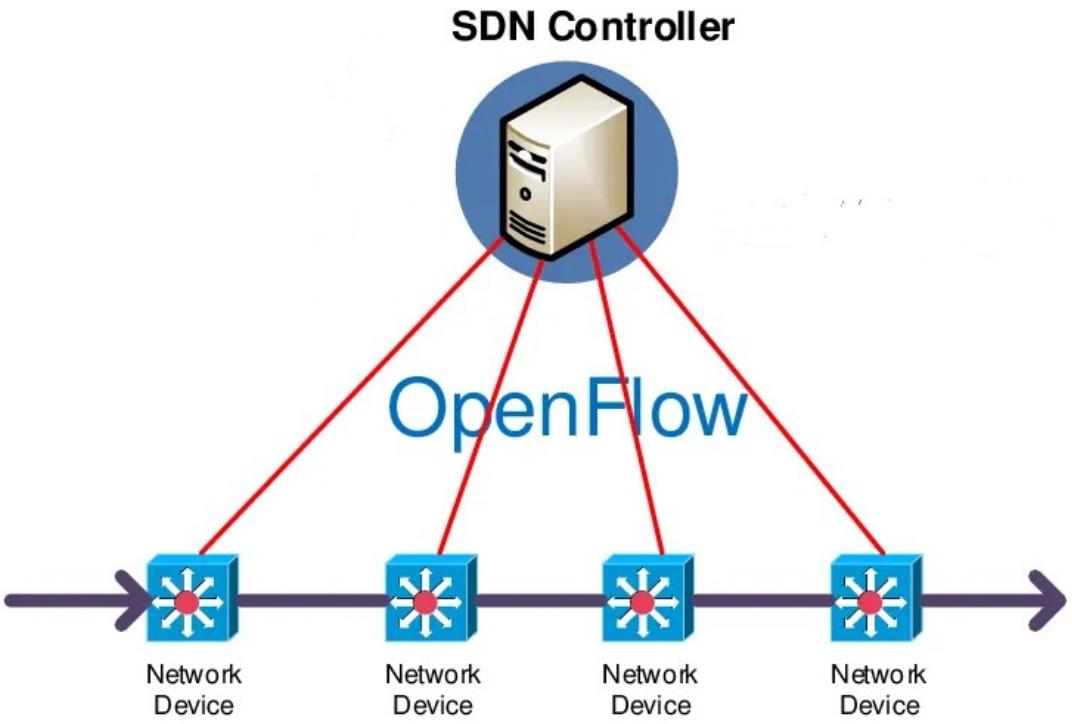
What is Software-Defined Networking?

- Software-Defined Networking (SDN) is the decoupling of data and control planes in a network
  - The control plane is removed from the switches and is placed in a logically centralized controller
  - Controllers' control plane decisions are realized by installing flow rules onto each switch



SDN Control Traffic

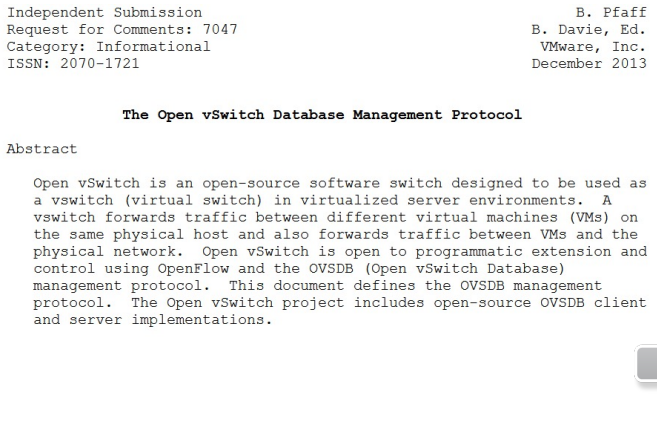
- The SDN controller uses control traffic to keep track of and manage the state of the entire network
- Used to manage and monitor SDN devices
  - Configure flow rules, queues
  - Poll device statistics



SDN Control Traffic Protocols

- OpenFlow
  - Allows for a controller to access and modify network devices' forwarding planes
  - Create/delete flow rules, access flow statistics

- Open vSwitch Database Management Protocol (OVSDB)
  - Allows for a controller to access and modify network devices' configurations
  - Configure queues, QoS mechanisms, ports



Independent Submission
Request for Comments: 7047
Category: Informational
ISSN: 2070-1721

B. Pfaff
B. Davie, Ed.
VMware, Inc.
December 2013

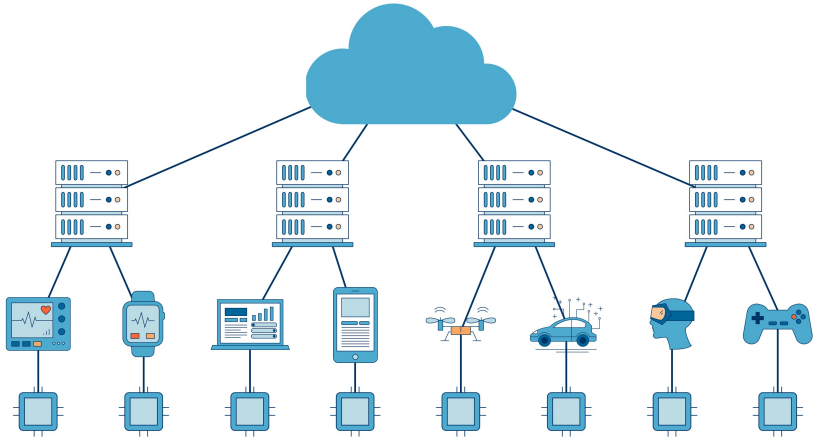
The Open vSwitch Database Management Protocol

Abstract

Open vSwitch is an open-source software switch designed to be used as a vswitch (virtual switch) in virtualized server environments. A vswitch forwards traffic between different virtual machines (VMs) on the same physical host and also forwards traffic between VMs and the physical network. Open vSwitch is open to programmatic extension and control using OpenFlow and the OVSDB (Open vSwitch Database) management protocol. This document defines the OVSDB management protocol. The Open vSwitch project includes open-source OVSDB client and server implementations.

Why is Control Traffic Important?

- Speed of control traffic message delivery dictates network responsiveness
  - In Edge/Fog computing scenarios, this reduces service configuration delay
- Control traffic consumes link bandwidth
  - Adds additional traffic to the entire network



Shortcomings of existing works

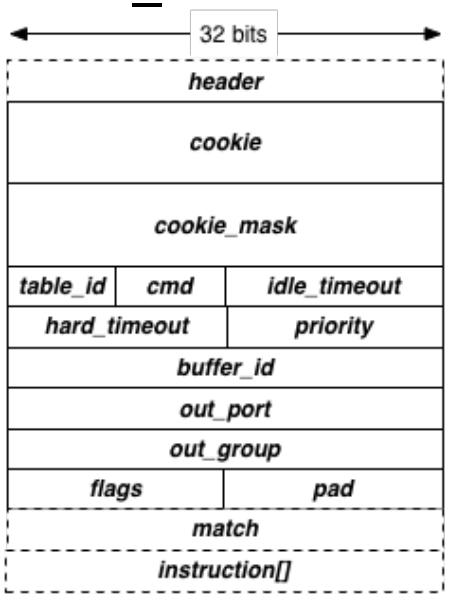
- Abstracted or incomplete control traffic values
  - Neglect the impact of control traffic on network behaviors
  - Assumed to be fixed rate
- No models for control traffic prediction
  - Control traffic is observed, but is not modeled

Observed Control Traffic Patterns

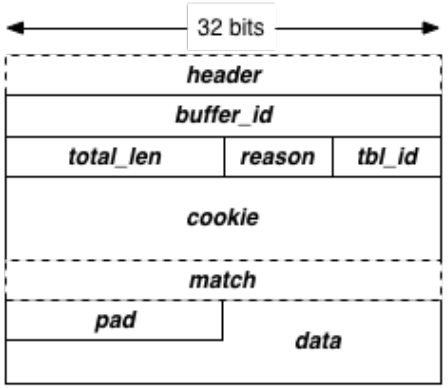
- Flow rule installations
- Statistics polling

Control Traffic Characterization – Flow Rule Installation

- Proactive vs Reactive flow rule installation
  - Proactive = installing flow rules in anticipation of new flows
    - `flow_mod` - installs a flow rule to the switch
  - Reactive = installing flow rules in reaction to invalid packets
    - `packet_in` – informs the controller of received invalid packet
    - `flow_mod` – installs a flow rule to the switch



`flow_mod` header



`packet_in` header

Flow Rule Installation – `flow_mod` packet size variation

Flow Rule Configuration	Specified Match Fields	`flow_mod` Packet Size ($s(p_{f\_mod})$) (bytes)
(C1)	IPv4 src	162
(C2)	IPv4 src+dst	170
(C3)	IPv4 src+dst, switch ingress port	178
(C4)	IPv4 src+dst, switch ingress port, MAC src	186
(C5)	IPv4 src+dst, switch ingress port, MAC src+dst	194
(C6)	IPv4 src+dst, switch ingress port, MAC src+dst, TCP src+dst	226
(C7)	IPv4 src+dst, switch ingress port, MAC src+dst, UDP src+dst	226
(C8)	IPv4 src+dst, switch ingress port, MAC src+dst, ICMP src+dst	218

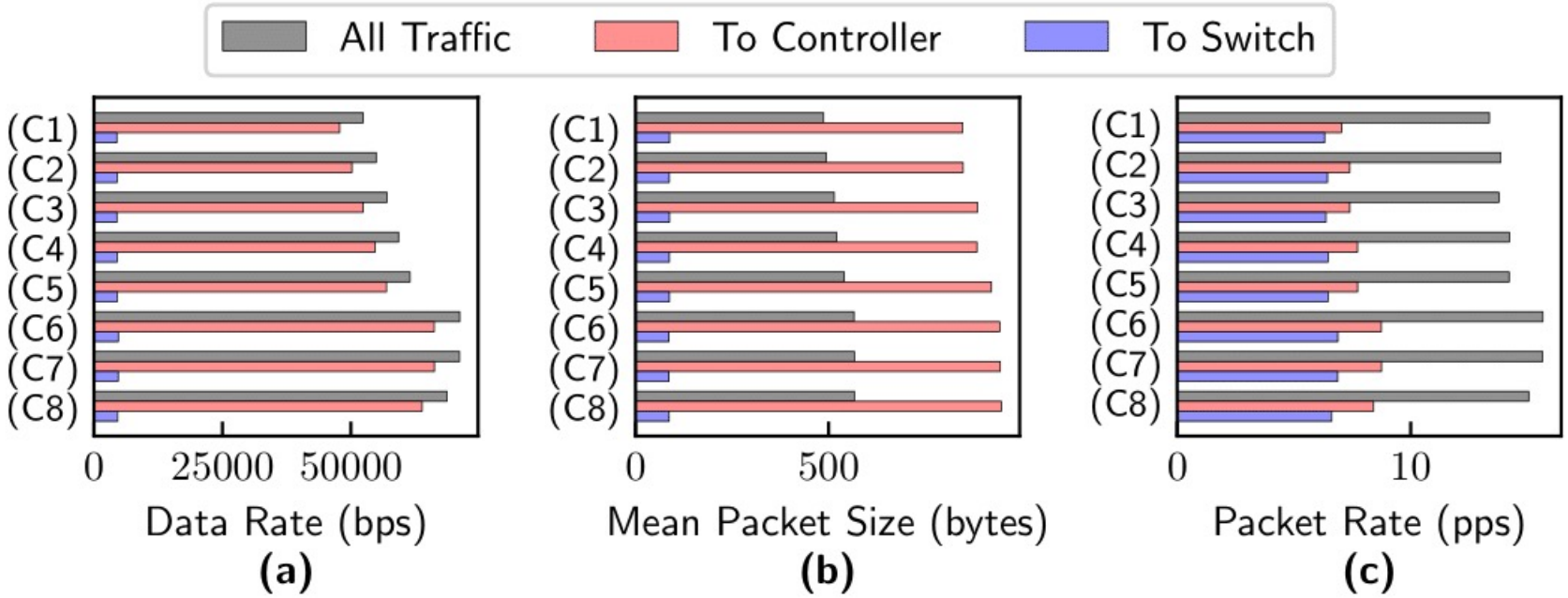
- `flow_mod` message sizes are variable depending on the number of parameters included in the OpenFlow flow rule

Control Traffic Characterization – Statistics Polling

- For a controller to maintain updated view of the network, it must periodically poll the switch's statistics
  - Done through `multipart_request` and `multipart_reply` messages
- Each request/reply message pair conveys a specific set of statistics to the controller
  - Flow tables, flow rules, queues, etc
- Request sizes are fixed, reply sizes will vary depending on the state of the switch
  - Poll replies to the controller can take up significant network bandwidth

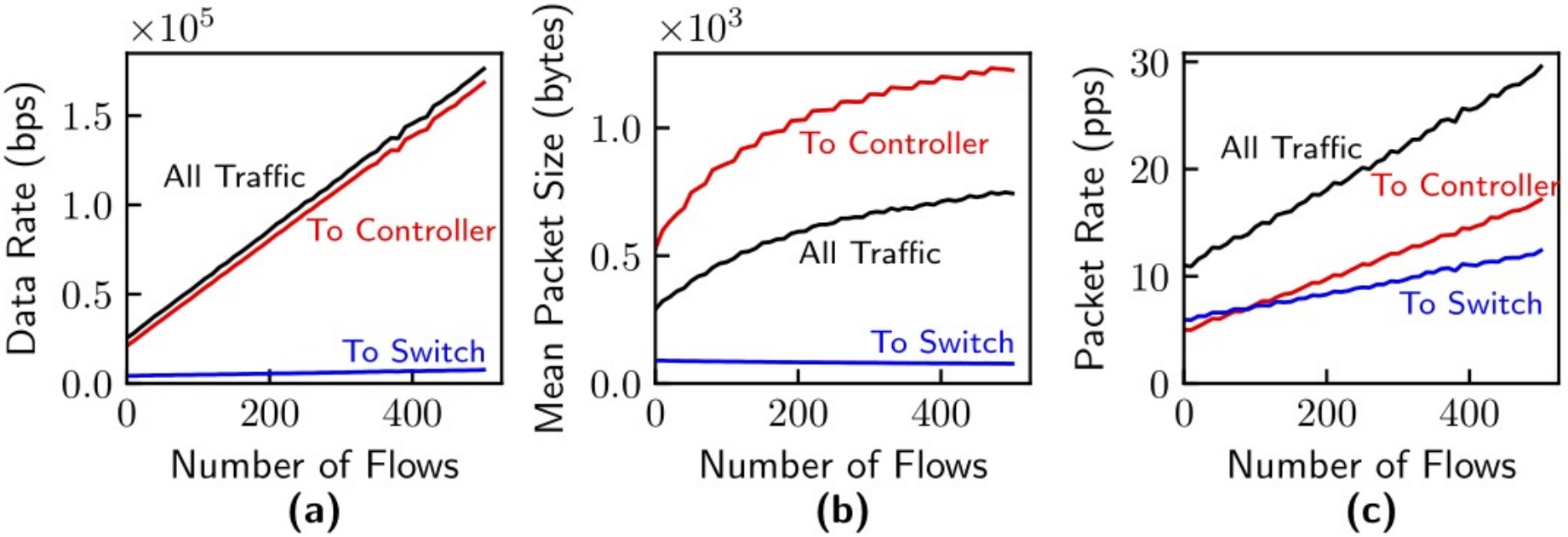
Statistics Polling Throughput – Flow Rule Configurations

- We measured the polling control traffic throughput for various flow rules configurations:



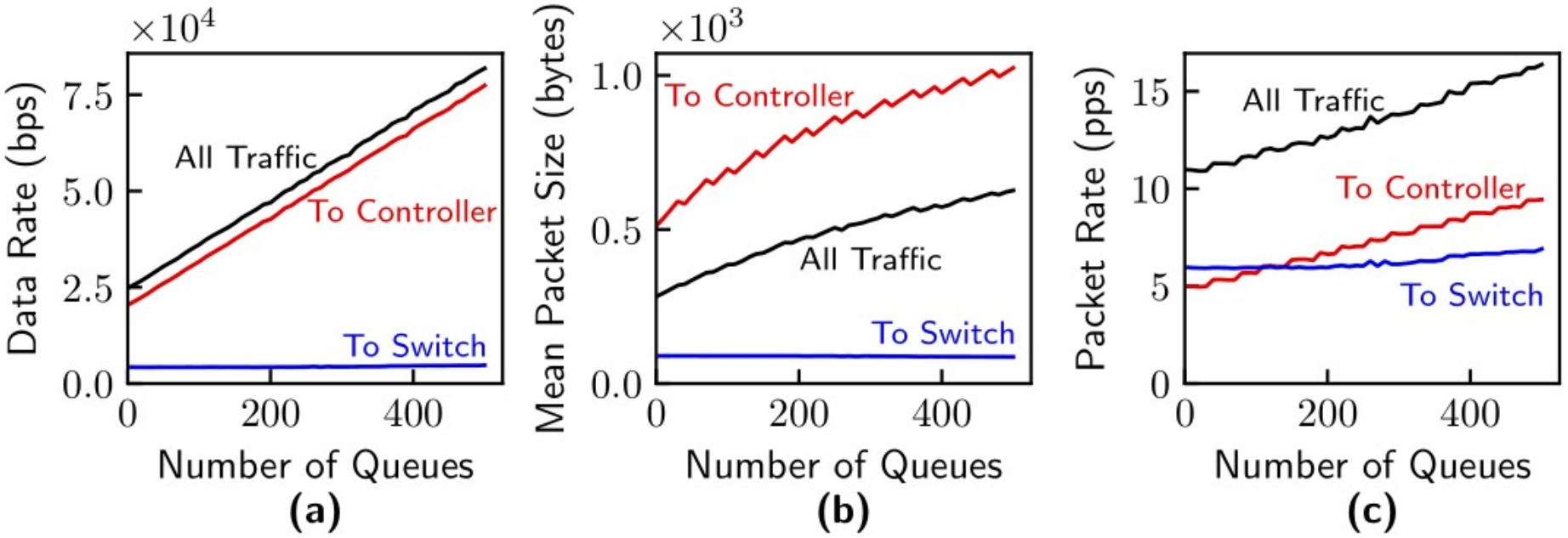
Statistics Polling Throughput – Flow Rules

- We measured the polling control traffic throughput for various sized flow tables:



Statistics Polling Throughput – Queues

- We measured the polling control traffic throughput for varying numbers of queues



Modeling Control Traffic Throughput

- Based on observations, we present this mathematical model of polling control traffic throughput based on switch state
  - Network controller applications can use this model, in conjunction with network state knowledge, to predict the impact of control traffic on network performance.

$$S_{\bar{p}}(\mathcal{F},\mathcal{Q}) = \frac{\sum_{\forall f_i \in \mathcal{F}} s(f_i) + \sum_{\forall q_j \in \mathcal{Q}} s(q_j) + D_0}{\left\lceil \frac{(\sum_{\forall f_i \in \mathcal{F}} s(f_i)) + H_f^0}{M} \right\rceil + \left\lceil \frac{(\sum_{\forall q_j \in \mathcal{Q}} s(q_j)) + H_q^0}{M} \right\rceil + (P_0 - 2)}$$

Summary

- Characterization of SDN control traffic behaviors is important
  - Can have significant affect on network performance
- Amount of control traffic is affected by:
  - Flow rule configurations
  - Number of flow rules
  - Number of allocated queues
- Mathematical model can be used for accurate control traffic prediction

Questions?