Opt-In for Enterprise GENI

Goals, architecture and challenges
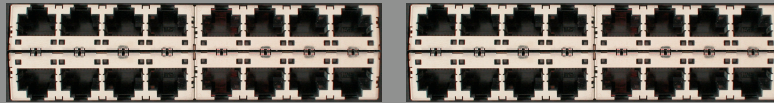
July 2009
Guido Appenzeller
Stanford University

Disclaimer: I haven't read the Opt-In Document
and this is my first Opt-In Working Group Meeting

Enterprise GENI

Ethernet Switch

Control Path (Software)

Data Path (Hardware)

OpenFlow Controller

OpenFlow Protocol (SSL)

Control Path   **OpenFlow**

Data Path (Hardware)

FLOW TABLE ENTRY
Allows to make forwarding decisions based on Layers 1-4

Rule	Action	Stats

Packet + byte counters

1. Forward packet to port(s)
2. Encapsulate and forward to controller
3. Drop packet
4. Send to normal processing pipeline

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport
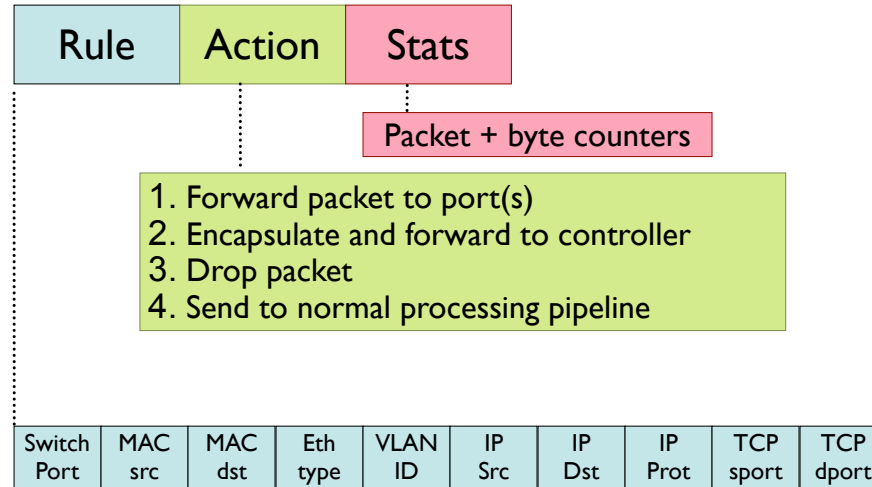
+ mask what fields to match

OPENFLOW EXAMPLE
Forwarding happens at line rates

Controller
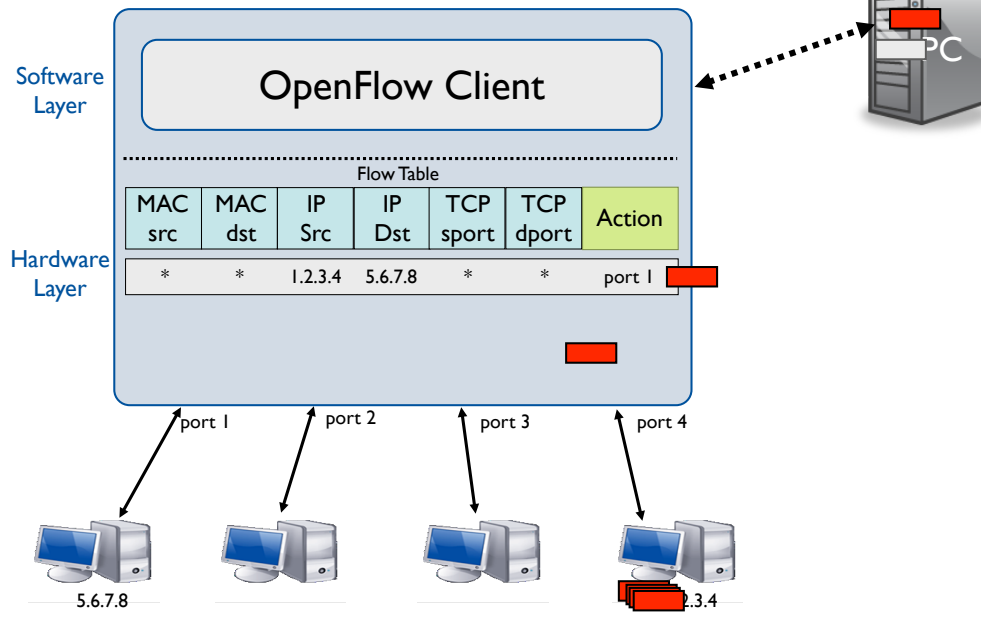
Software Layer

OpenFlow Client

Hardware Layer

Flow Table

MAC src	MAC dst	IP Src	IP Dst	TCP sport	TCP dport	Action
*	*	1.2.3.4	5.6.7.8	*	*	port 1

port 1   port 2   port 3   port 4

5.6.7.8   1.2.3.4

SWITCH BASED VIRTUALIZATION
Exists for NEC, HP switches but not flexible enough for GENI

Controller

Research VLANs

Flow Table
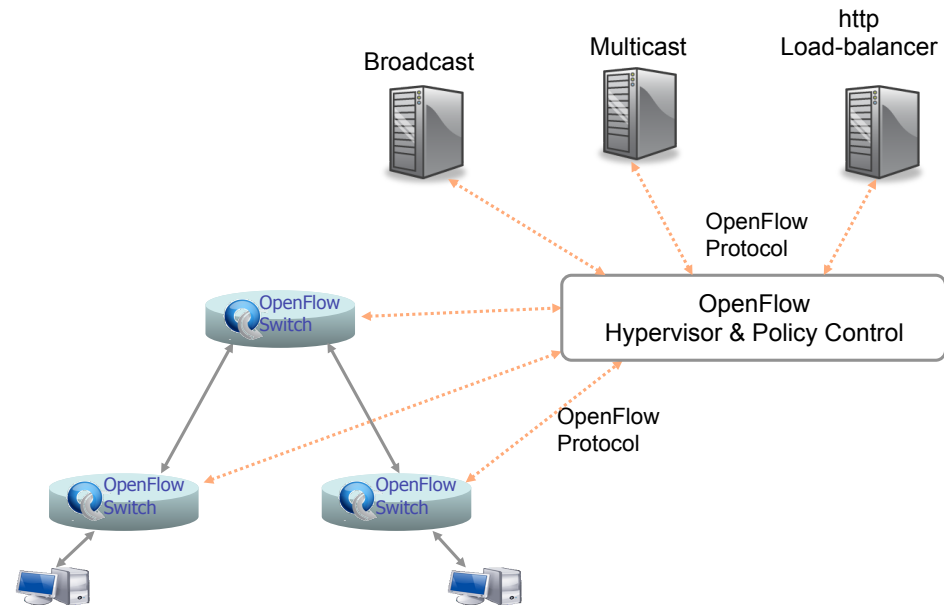
Production VLANs

Normal L2/L3 Processing
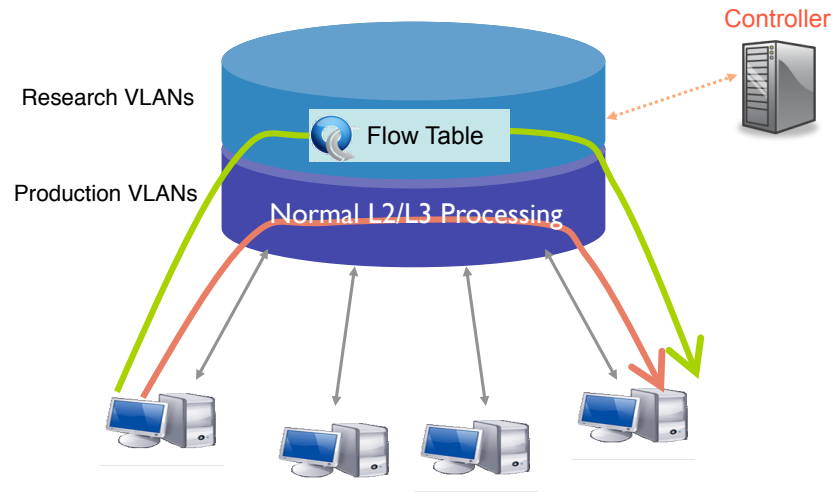
HYPERVISOR BASED VIRTUALIZATION
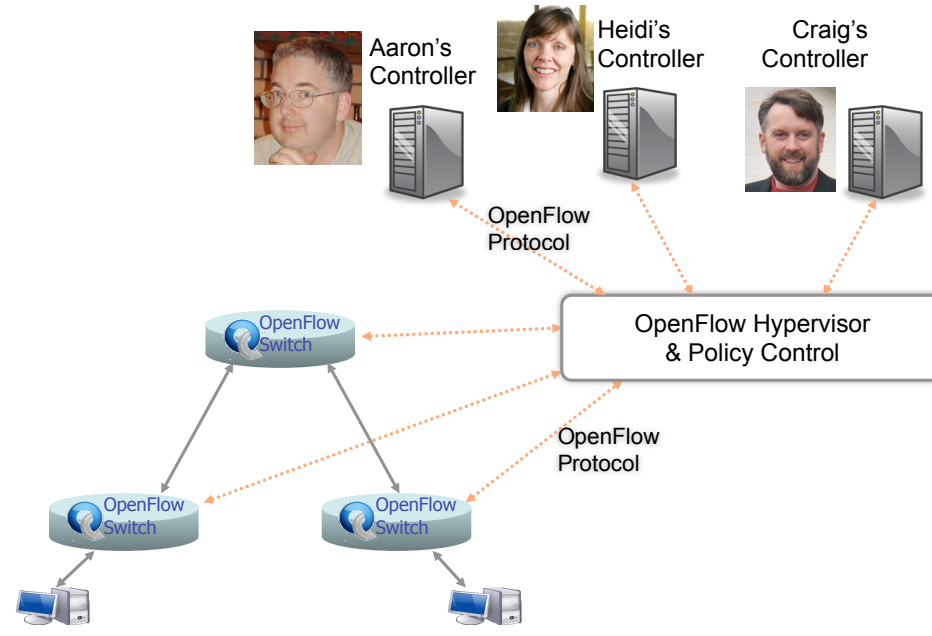
HYPERVISOR BASED VIRTUALIZATION
Separation not only by VLANs, but any L1-L4 pattern

Broadcast

Multicast

http
Load-balancer

OpenFlow
Protocol

OpenFlow
Switch

OpenFlow
Hypervisor & Policy Control

OpenFlow
Protocol

OpenFlow
Switch

OpenFlow
Switch

USE CASE: VLAN BASED PARTITIONING

Basic Idea: Partition Flows based on Ports and VLAN Tags
- Traffic entering system (e.g. from end hosts) is tagged
- VLAN tags consistent throughout substrate

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport
*	*	*	*	1,2,3	*	*	*	*	*
*	*	*	*	4,5,6	*	*	*	*	*
*	*	*	*	7,8,9	*	*	*	*	*

USE CASE: NEW CDN - TURBO CORAL ++

Basic Idea: Build a CDN where you control the entire network
- All traffic to or from Coral IP space controlled by Experimenter
- All other traffic controlled by default routing
- Topology is entire network
- End hosts are automatically added (no opt-in)

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport
*	*	*	*	*	84.65.*	*	*	*	*
*	*	*	*	*	*	84.65.*	*	*	*
*	*	*	*	*	*	*	*	*	*

STANFORD DEPLOYMENT HARDWARE

Phase 1   (ongoing)

- Gates Building, 3A Wing only
- Four switches (HP and NEC)
- ~30 Wireless APs
- ~25 users

Phase 2   (1H2009)

- Gates Building, All Floors
- 23 Switches
- Wireless TBD
- > 100 users

Phase 3   (2H2009)

- Multiple Buildings
- Wireless TBD
- > 1000 users
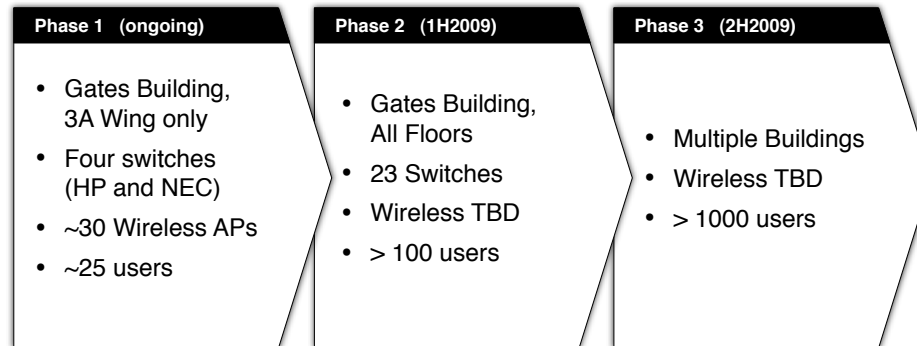
Our Thoughts on Opt-In

TARGET GROUP

Who do we target for opt in?

- 1000+ local users on the Enterprise GENI Network
  - ‣ Can't always assume they are technical
  - ‣ Might have locked down PCs, can't install software
  - ‣ Constrained Devices - e.g. iPhones
  - ‣ User may want to opt-in to multiple experiments or none
- Local Servers
  - ‣ Planet Lab Nodes, Production Servers
- Access Points (?)

Why not remote systems via tunnel?

- Route from my home to Stanford is ~10 routed hops
- If majority of time and hops is in tunnel, is experiment relevant?

USER EXPERIENCE
Simplicity of opt-in drives participation

- User gets email about new experiment
  - ‣ "Join the Coral++ experiment today and win an iPod"
  - ‣ User clicks on link in email and browses to web site
  - ‣ User reads description of the experiment
  - ‣ User clicks on "Opt In" button on web site

- Opt-In is about getting users to participate
  - ‣ Most users have little incentive to use experimental network
  - ‣ Each click will lower number of users participating.
    - • Corollary: Clicks are bad

- We may need an authentication step for audit trail
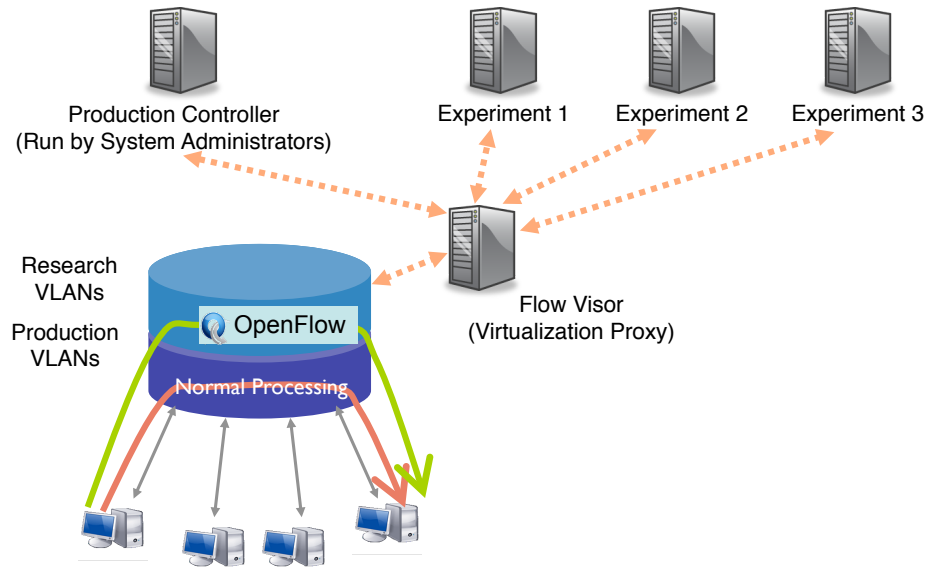
HOW DO YOU DO THIS?

Disclaimer: This is not fully implemented yet, we are still tweaking the architecture. Things may change.

Basic Idea:

- If a user moves into any experiment he is switched from the production VLAN to an OpenFlow controller VLAN
- The Openlow Network has multiple controllers:
  - ‣ A production controller that controlls all traffic that is not part of experiments
  - ‣ A FlowVisor that multiplex

SWITCH BASED VIRTUALIZATION

Exists for NEC, HP switches but not flexible enough for GENI

Production Controller
(Run by System Administrators)

Experiment 1 Experiment 2 Experiment 3

Research VLANs

Production VLANs

OpenFlow

Normal Processing

Flow Visor
(Virtualization Proxy)

THE OPT-IN MANAGER

The Opt-In Manager is a server in the local substrate. It has the capability to:

- Move users from production VLAN to OpenFlow VLAN
    - ‣ Probably via Radius, backup is via console scripts
- Configure the FlowVisor to have a subset of a user's traffic controlled by an experimental controller
- Information about the experiment and what classes of traffic to opt-in is done via the clearing house

OPEN QUESTIONS

- Can experiments that overlap in Flow Space (i.e. **ALL** fields in the packet header could be the same) share the same link?
- What if user A has opted in all IP traffic into Experiment A, and user B has opted in all IP traffic into Experiment B, and they want to talk to each other?
- Is scope of the opt-in by Port, MAC, IP or a Mix?
  ‣ May be constrained by hardware capabilities
- How do we do this across different OpenFlow slivers?
- How do we do this across different slivers with different architectures?
- Will this solution work for other campuses?

Thank You!