RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

SDN AND SECURITY:
Why Take Over the Hosts When You Can Take Over the Network

SESSION ID: TECH0R03

Robert M. Hinden
Check Point Fellow
Check Point Software

What are the SDN Security Challenges?

- Vulnerability of Central Control
- Trust Model Changes
- Virtualization of Network Topology
- IT Organizational Changes

Presentation Outline

- Software Defined Networks Overview
- SDN Hype and Production Deployments
- SDN Security Challenges
- SDN Security Solutions
- Q & A

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Software Defined Networks
Overview

SDN Basic Idea

- Separation of Network Control and Data Planes
  - Well-defined vendor-independent OpenFlow API between the two
- Operation of the network is defined in software outside of the forwarding path
  - a.k.a. Software Defined Network
- Centralized Network Control on standard servers

Motivation for SDN

- Creation of high-level network policies
  - Move away from current management approaches like SNMP/CLI
  - Apply policies uniformly across Routers, Switches, Optical, Virtual Networks, etc.
- Mix and match of vendors
  - Packet Forwarding and Control planes
  - Hardware and Software

Mainframes to PCs

App

Open Interface

Windows (OS)

Linux

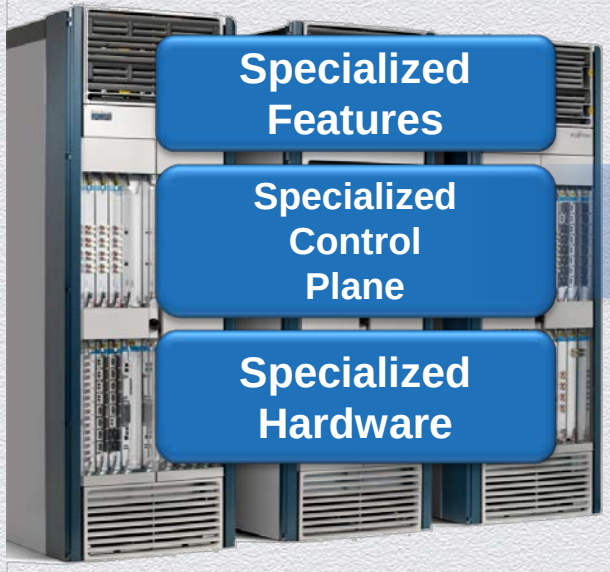
Mac OS

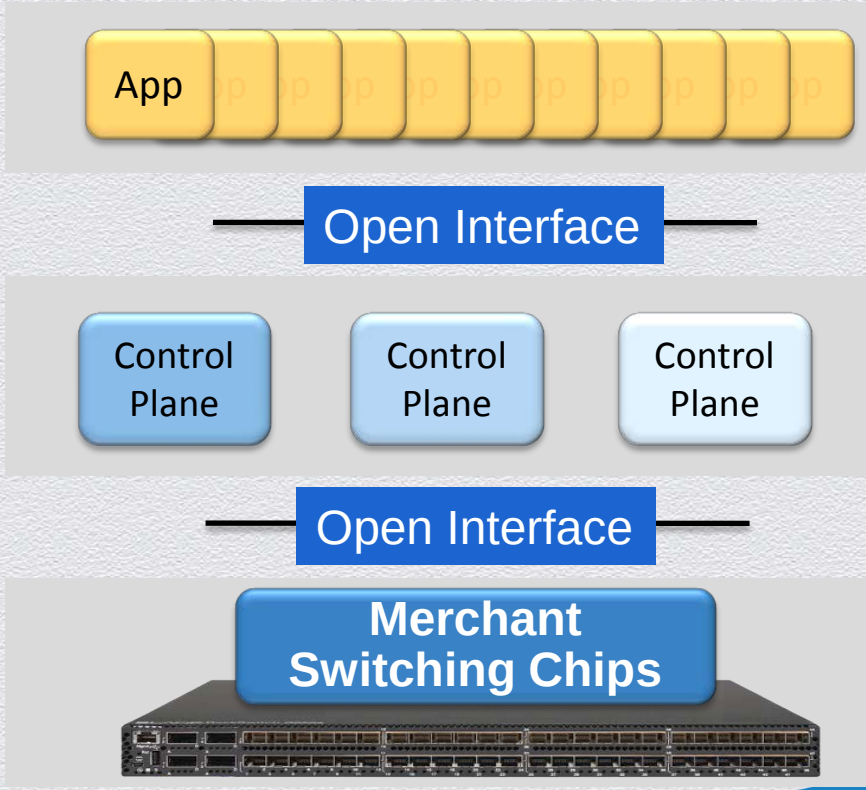
Open Interface

Microprocessor

[Credit: Nick McKeown “Making SDNs Work”]

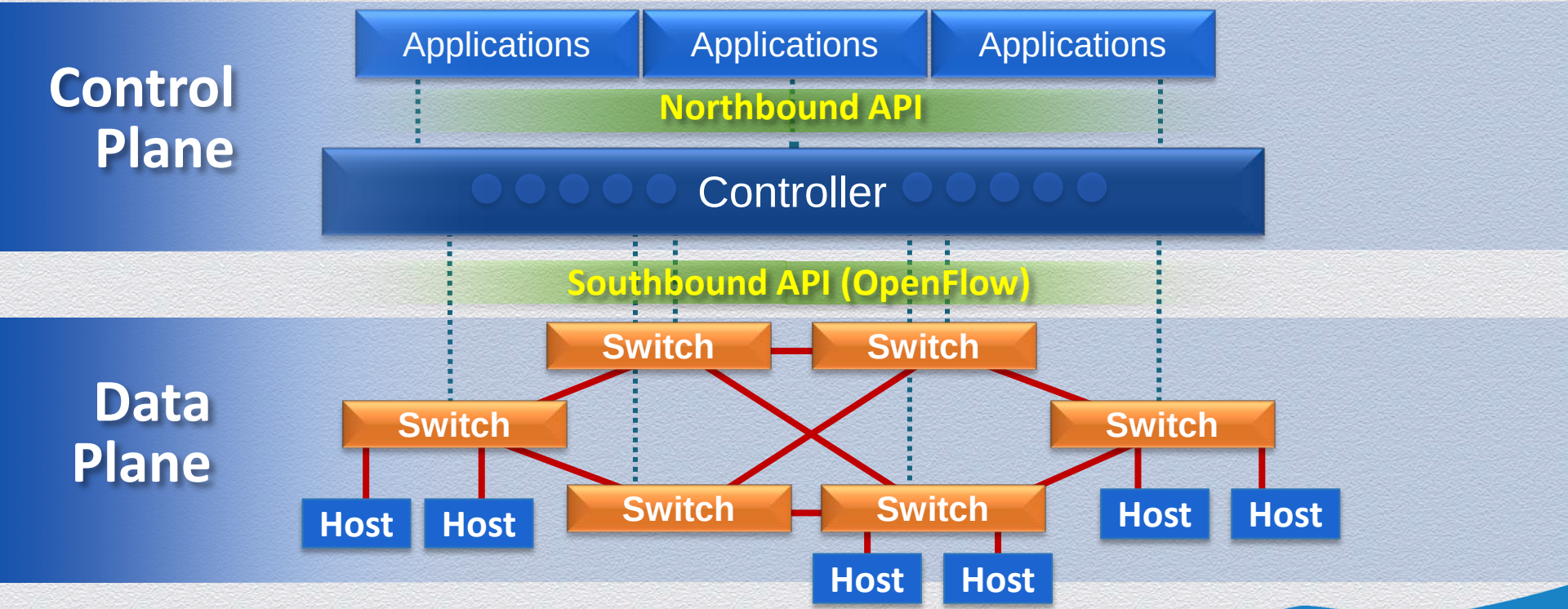
Switches/Routers to SDN



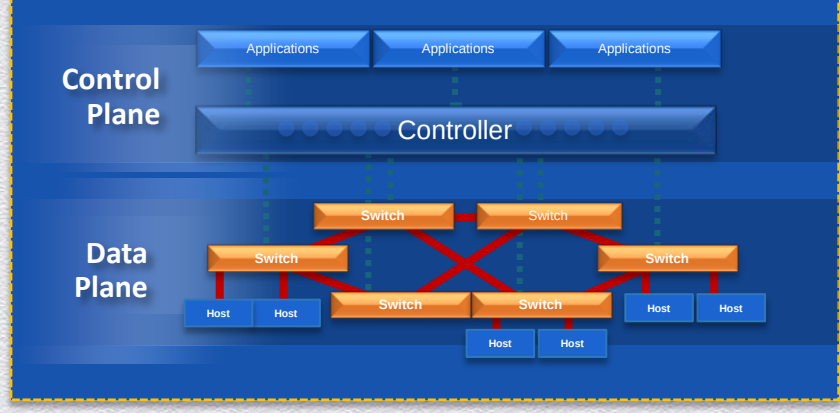


[Credit: Nick McKeown "Making SDNs Work"]

SDN Architecture



Components

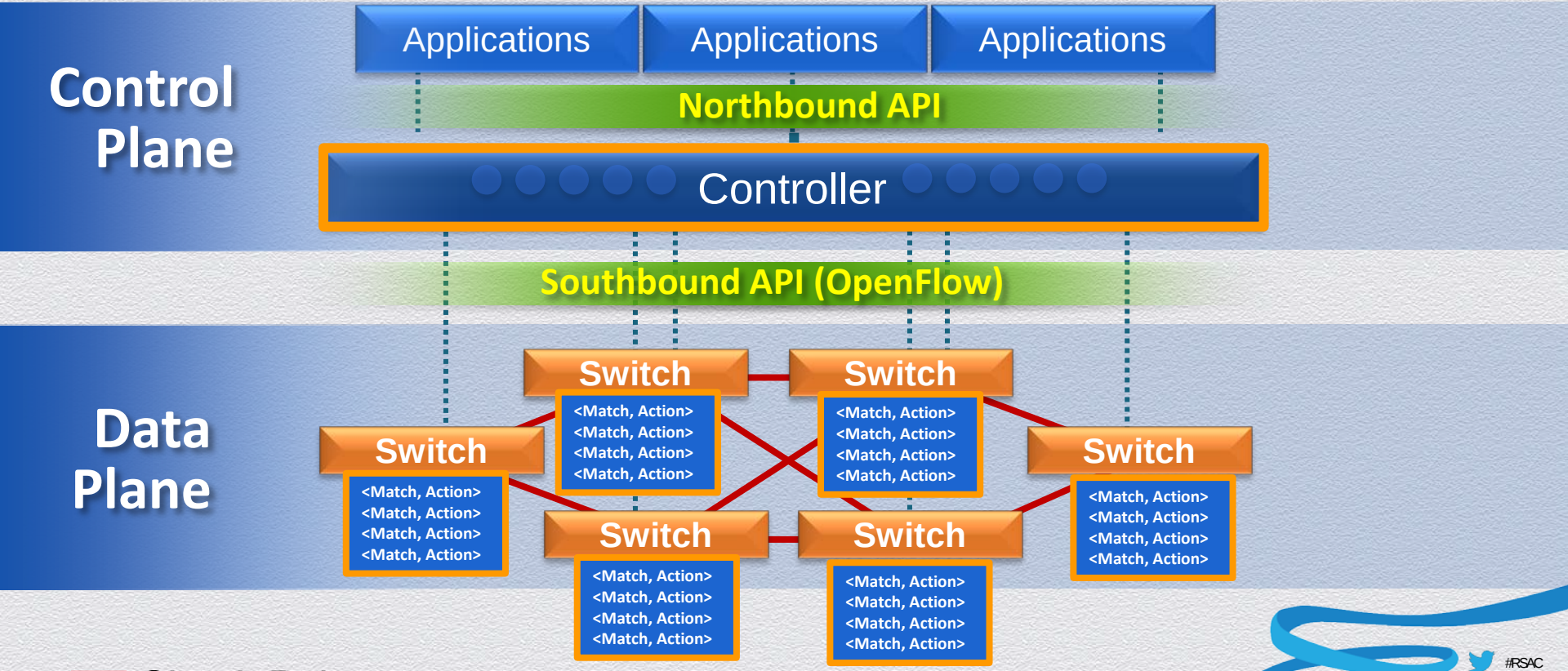


- Application Programs
  - Implement network specific policy
- Controller
  - Provides high-level view of Network to control programs
  - Deploy policy to Routers/Switches via OpenFlow
- Routers/Switches
  - Controlled by state injected by Controller

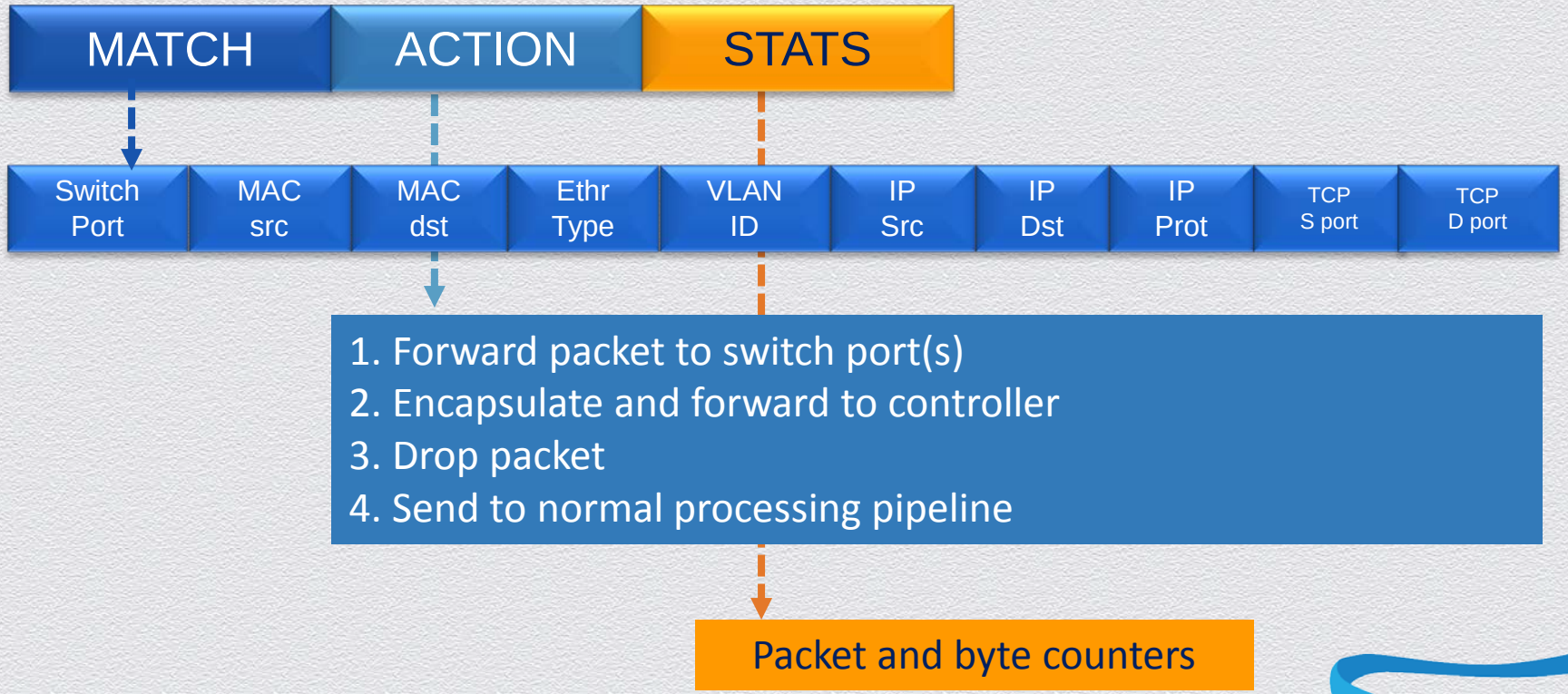
How It Works

- Controller presents logical map of network to Application Programs
- Switches/Routers are Flow based
  - Process known flows autonomously
  - If new flow arrives, ask Controller what to do
  - Controller installs new flow state in Switch/Router
  - Flow state consist of <Match, Action> pairs
- Controller pushes state to Switch/Router with OpenFlow

SDN Architecture



Flow Table Entry (OpenFlow 1.0)



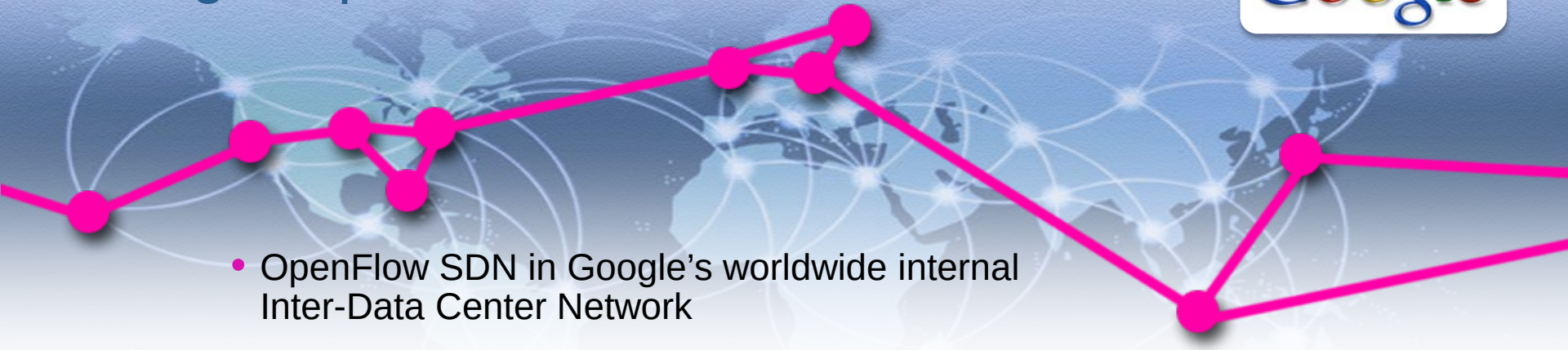
Lots of Activity

Impact to Current Networking

- Utilizes most existing protocols
  - IPv4/IPv6, TCP/UDP, Ethernet, VLANS, etc.
- Hosts don’t change
- Routing Protocols run in the Controller
- Big change to management and configuration protocols
  - Centralized vs. current distributed
- This is an incremental solution not a “clean slate”

Production SDN Deployments

Google OpenFlow Network



- OpenFlow SDN in Google's worldwide internal Inter-Data Center Network
- Centralized traffic engineering service
- Google built their own network switches using merchant silicon and Open Source routing software
- Rumors that Facebook, Microsoft, etc. are looking at similar SDN traffic engineering deployments

http://www.wired.com/wiredenterprise/2012/04/going-with-the-flow-google/all/1

Other SDN Production Deployments

- Data Center deployments using Nicira/VMware NSX
- Data Center / Virtualization is a very active SDN area
  - Network virtualization doesn't require SDN, but can be helped by it
- There are many University / Research SDN Projects
  - NSF is providing a lot of funding

SDN Hype

The Hype

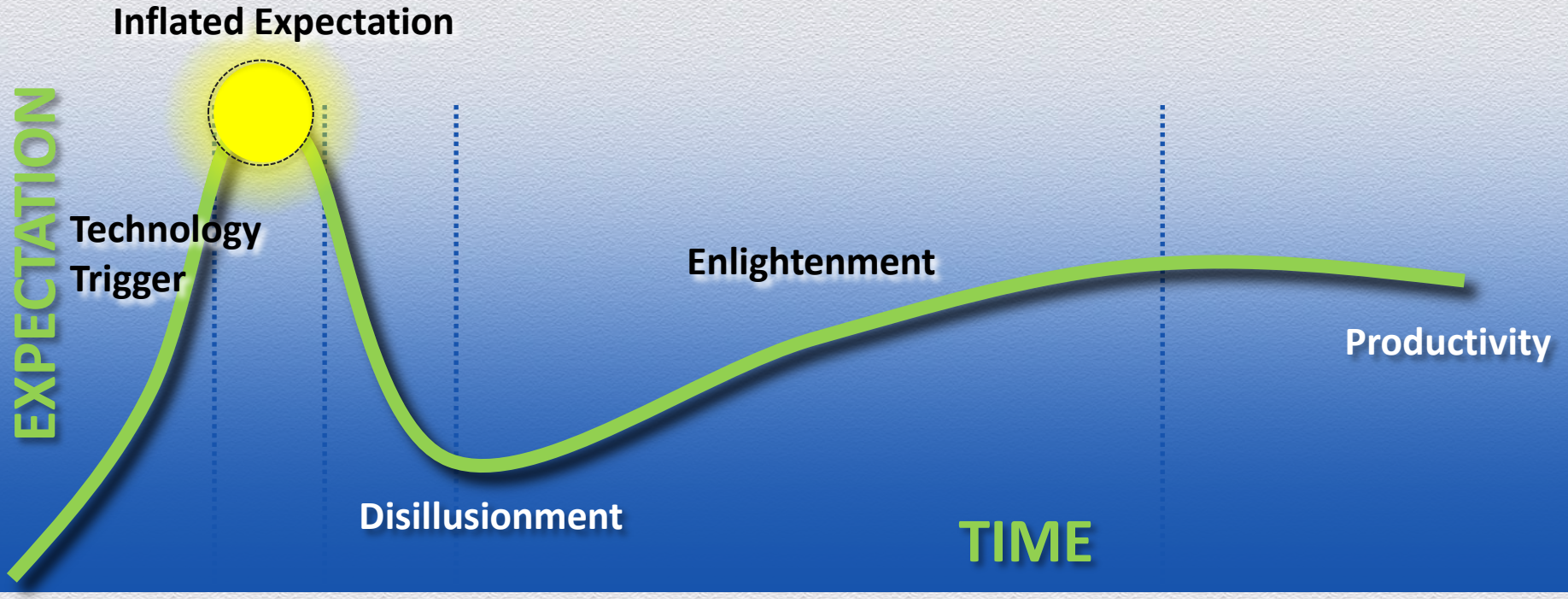
"SDN is emerging as one of the most promising and disruptive networking technologies of recent years. It has the potential to enable network innovation and create choice, and thus help realize new capabilities and address persistent problems with networking. It also promises to give network operators more control of their infrastructure, allowing customization and optimization, therefore reducing overall capital and operational costs."

Open Networking Summit, April 2012

SDN Hype

- SDN is a threat to many vendors' business models
  - Many large vendors are describing "SDN like" solutions that will lock in customer
  - Proposing very complex proprietary solutions
- Vendors are using SDN to describe any legacy products that use software to control hardware

SDN Adoption



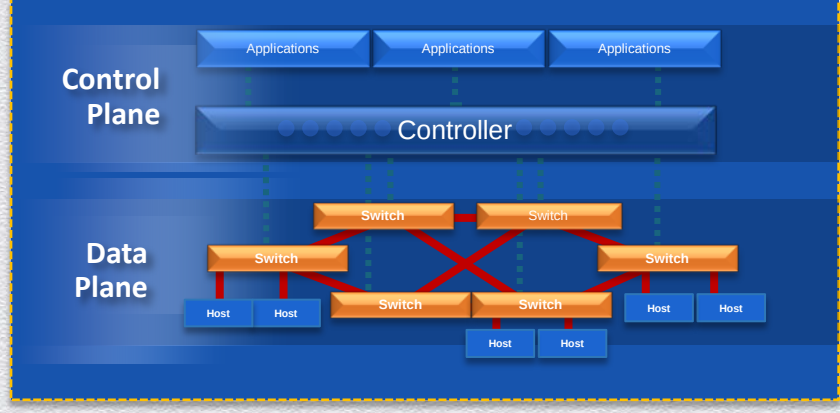
SDN Issues / Challenges

- Scaling properties uncertain
  - Flow entries could get very, very large
  - Flows supported by switches is still limited
- Outages / Bugs
  - Unclear how well it deals with network outages that require rerouting
  - How do you debug software and hardware problems?
- Security (the rest of the talk)

RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

SDN Security Challenges

Vulnerability of Central Control



- SDN Applications and Controller have complete control of the network
- Controllers/Applications are built on general purpose computing platforms
  - We all know all about the vulnerabilities of these platforms
- If Controller or Application is compromised, the whole Network is compromised

Why Take Over the Hosts When You Can Take Over the Network

Effects of SDN Controller Compromise

- Route flows around security devices
- Controller subverts new flows
- Send traffic to compromised nodes
- “Man in the Middle” attacks

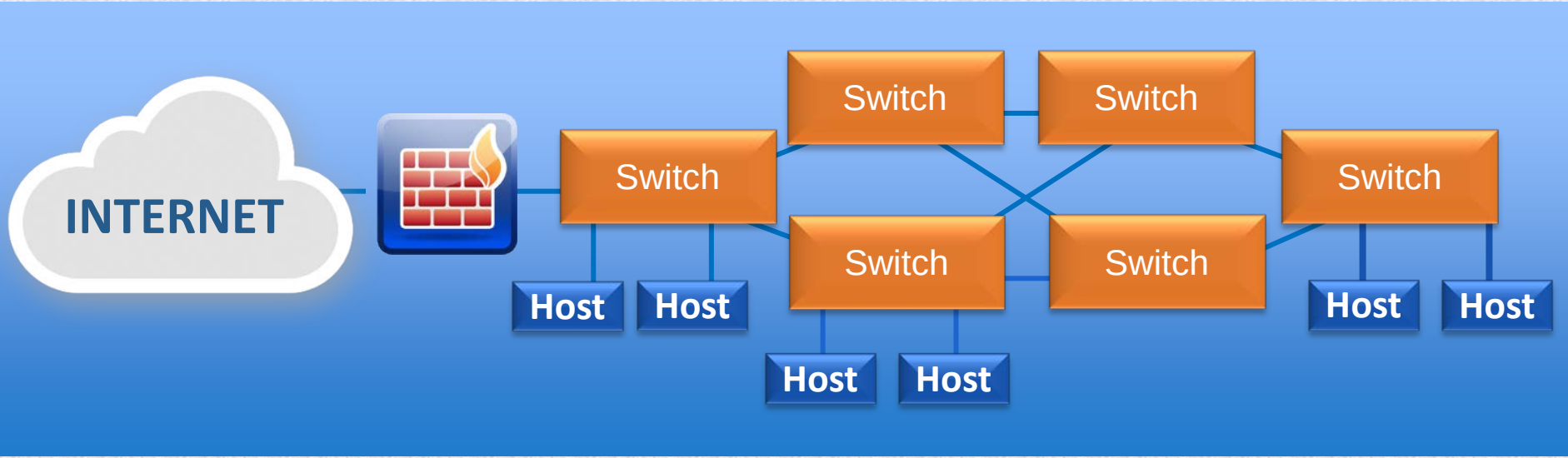
- Modify content
- Insert malware
- Monitor traffic
- Subvert DNS responses
- ……

Was SDN Designed for the NSA?

Central control makes it easy to control the whole network

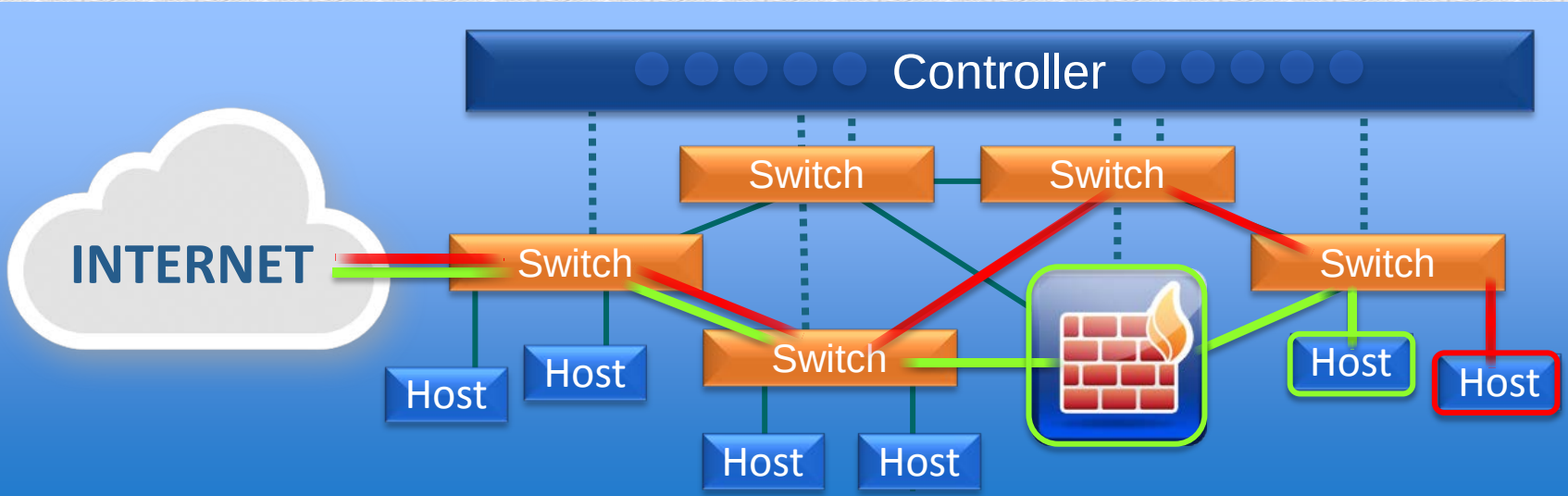
SDN makes it very easy to control where traffic flows

Current Security Model



Security policy enforced by physically forcing traffic to flow through Security Devices

SDN Changes Security Model



- Flow Rules control when or if traffic goes through Security Device
- Network Topology is now virtual

SDN Changes the Trust Model

Security cannot be enforced by physical topology

Requires complete Trust in SDN Applications and Controller

We don’t understand the consequences

SDN Changes Organization Model

- Today most IT organizations have a
  - Network Group
  - Security Group
- SDN requires a great deal of cooperation between these groups
- All network staff will be responsible for Security Policy

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

SDN Security Solutions

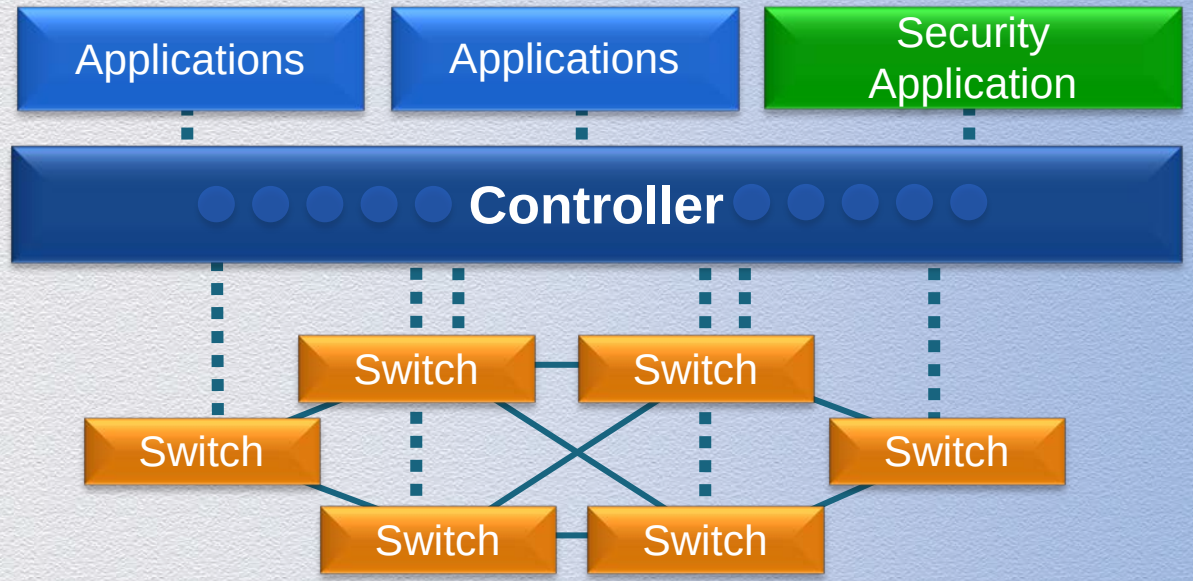
It’s Not All Bad

- Uniform SDN Security Policy
- Security Everywhere
- Control Security Treatment Traffic Receives
- Isolate Compromised Hosts

Uniform SDN Security Policy

Security Application

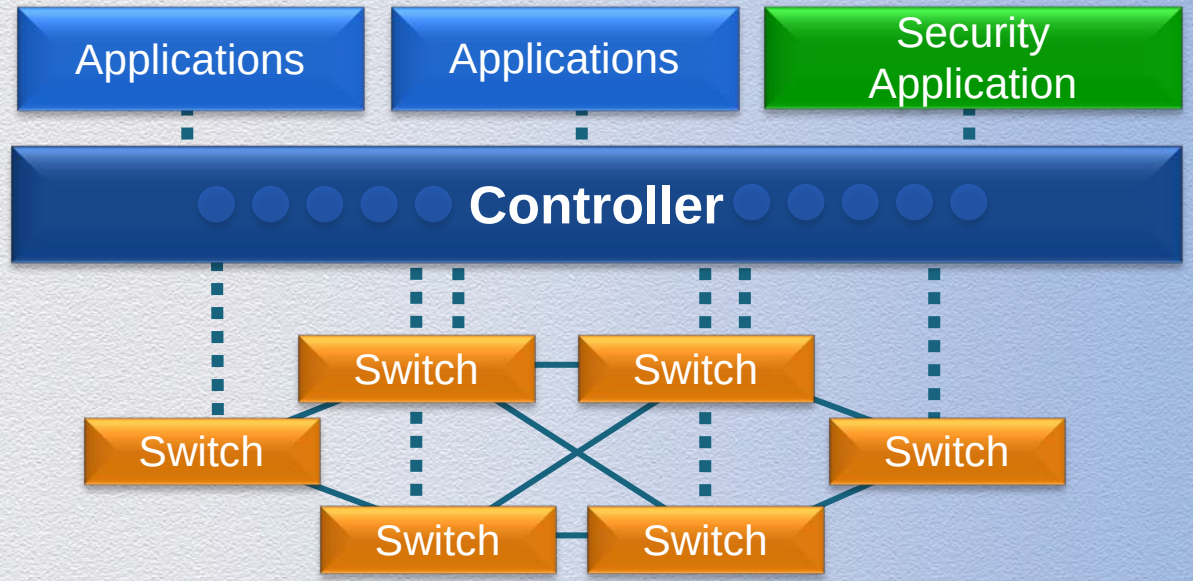
- Couple Security Policy to SDN policy/rules and validate SDN flows against the security policy
- Ensure that Security Policy is implemented for all traffic
- Maintain regulatory and compliance requirements



Security Everywhere

Security Application

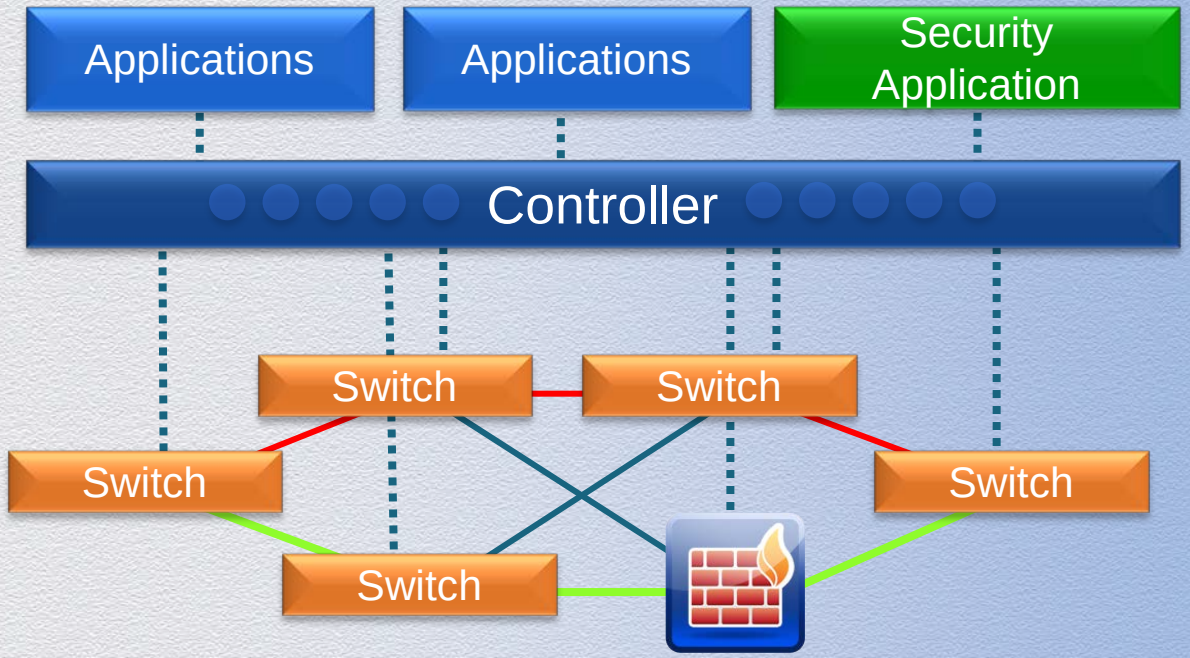
- All Routers and Switches have Security capabilities
- Security Application can take advantage of this and push rules to all network devices



Control Security Treatment Traffic Receives

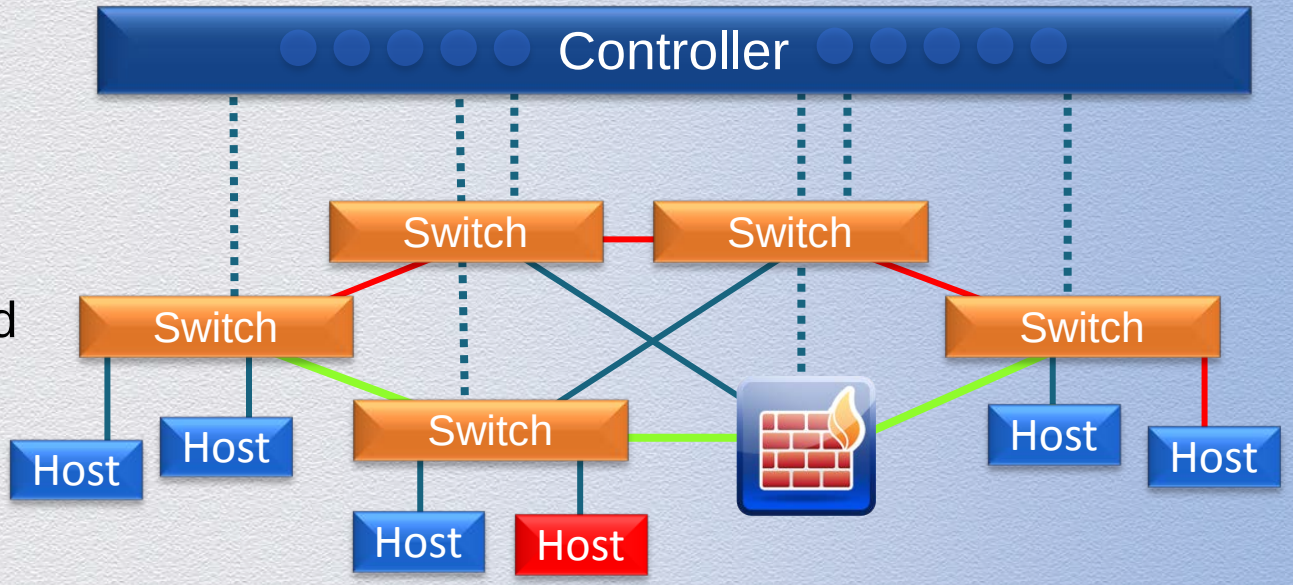
Range of Security Control

- Full Firewall
- ACL style filtering
- No filtering



Isolate Compromised Hosts

- Once compromised host is detected
- Host can be isolated



Summary

Summary

- SDN has a lot of promise
  - Many of its capabilities are very powerful
- SDN Security issues are real for many organizations
  - Another case of build it and worry about Security later?
- We will all need to get beyond the “hype phase” to see what is real and achievable

Q & A

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Thank You