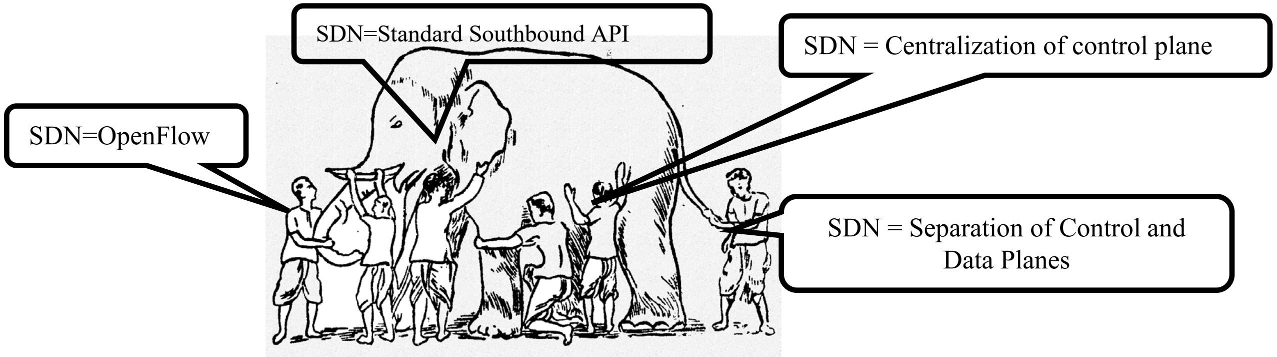
Challenges of Software Defined Networking in the National Security


SDN=Standard Southbound API
SDN = Centralization of control plane
SDN=OpenFlow
SDN = Separation of Control and Data Planes

Raj Jain

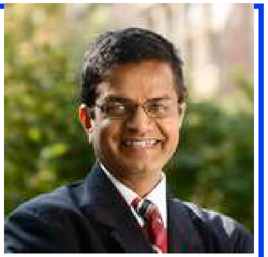
Barbara J. and Jerome R. Cox, Jr. Professor
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@wustl.edu

Briefing to President's National Security Telecommunications Advisory Committee (NSTAC), December 12, 2019

These slides and audio/video recordings of this briefing are at:

http://www.cse.wustl.edu/~jain/talks/nstac_jain.htm

About Me



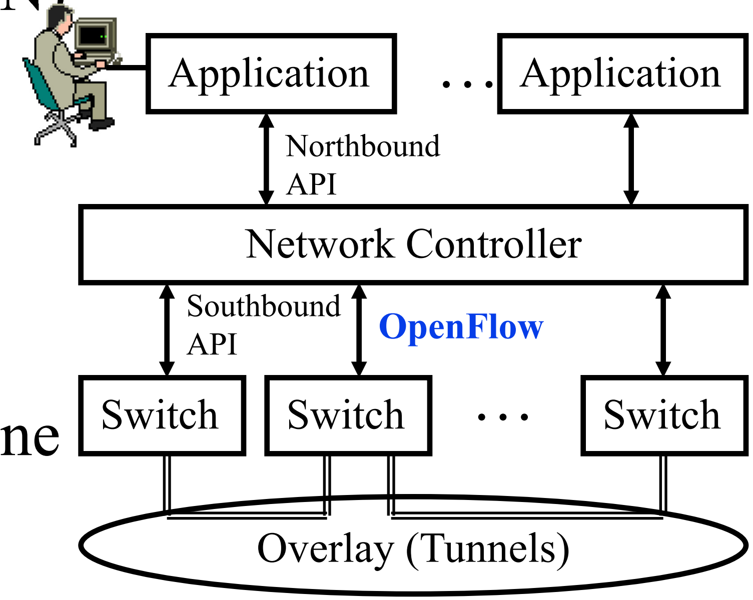
- 1978: Ph.D., Harvard 1978 (Applied Math/Computer Sci)
- 1978-1994: Network Architect at Digital Equipment Corporation (16 years)
- 1994-2000: Professor at Ohio State University (6 Years)
- 2000-2005: Co-Founder and CTO, Nayna Networks, San Jose, CA Nasdaq: NAYN (5 years)
- 2005-Present: Professor at Washington University (14 years)
- 21 Years in industry + 20 years in academia
- Impact:
  - ECN bits in all IP packets are from our DECbit research
  - Among most cited authors in computer science: 30,000+ Citations
  - 2017 ACM SIGCOMM Award for Life-Time Achievement
  - IEEE Fellow, ACM Fellow, AAAS Fellow
- Website: http://www.cse.wustl.edu/~jain

Overview

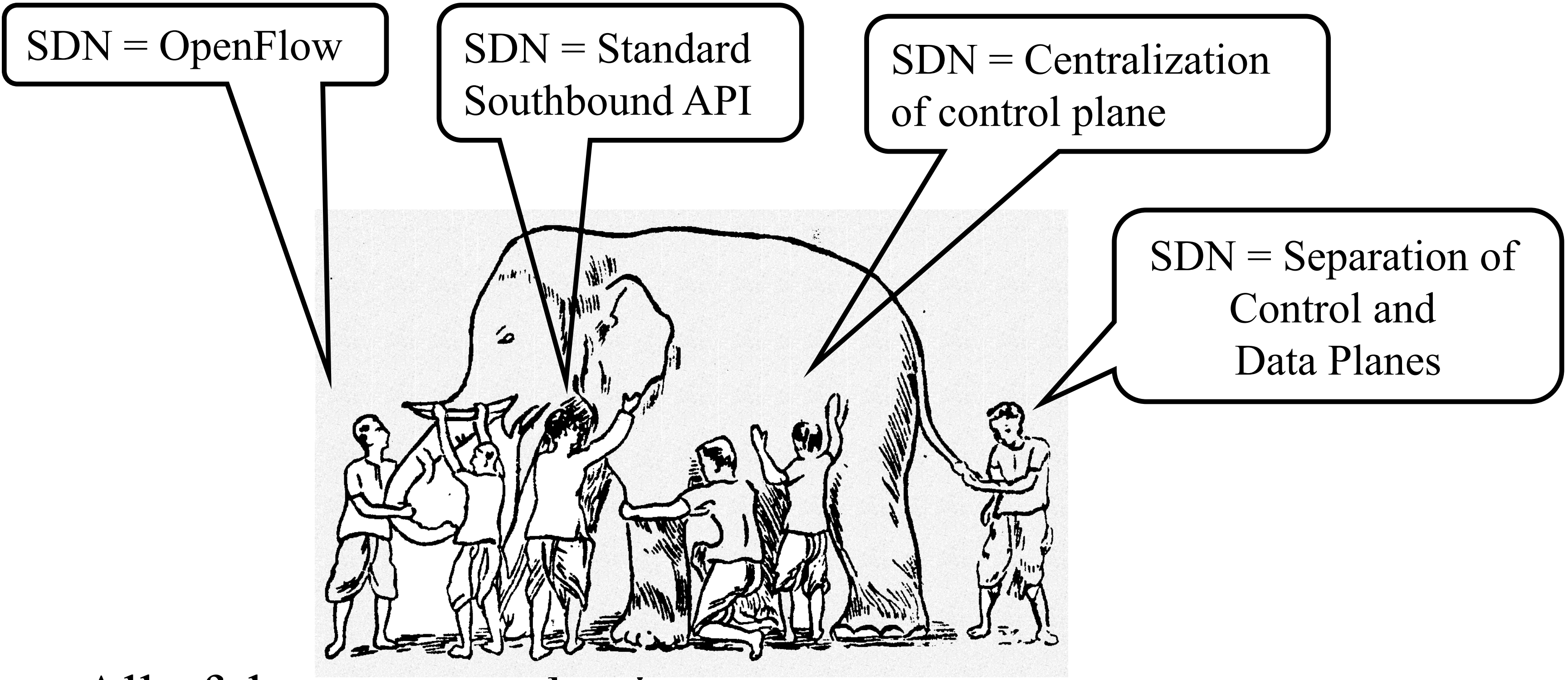
1. Misconceptions about SDN
2. What really is SDN?
3. Impact of SDN ⇒ Leading to several new trends
4. Impact on Security

Origin of SDN

- SDN originated from OpenFlow
- Centralized Controller
  ⇒ Easy to program
  ⇒ Change routing policies on the fly
  ⇒ Software Defined Network (SDN)
- Initially, SDN=
  - Separation of Control and Data Planes
  - Centralization of Control
  - OpenFlow to talk to the data plane
  - Simplification of switch hw
  - Lower CapEx and Lower OpEx



What SDN is Not?



SDN = OpenFlow

SDN = Standard Southbound API

SDN = Centralization of control plane

SDN = Separation of Control and Data Planes

- All of these are mechanisms.
- SDN is *not* about a mechanism.
- It is a framework ⇒ Many solutions

Four Misconceptions About SDN

1. **Policies vs. Control**:
   Control = All bits and messages not sent by the user
   In Telecom networks, the control bits were initially sent with data bits leading to insecurity. Now control channels are separate.
   In IP, control includes all header bits and all routing messages.
2. **Separation of Control Plane**:
   ⇒ Switches have only data plane and have no brains.
   Brain provided by the controller => Low cost switches
3. **SDN vs. OpenFlow**:
   OpenFlow is the father of SDN but not SDN.
4. **Need OpenFlow for SDN**:
   - OpenFlow is micro-management. It is not scalable.
   - For large infrastructure, need scalable solutions.

Trend: Separation of Control to Orchestration of Policies

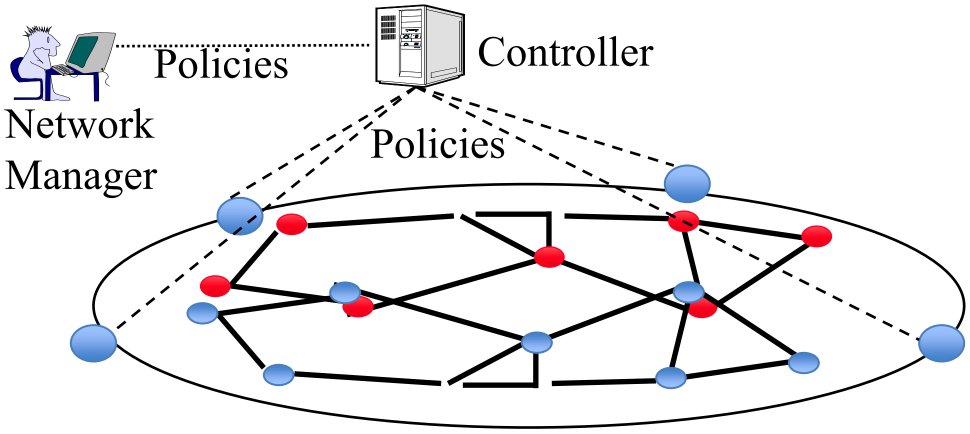
Separation and Centralization of Control Plane

Orchestration of Policies

Micromanagement is not scalable

Three Features that Define SDN

1. **Abstract the Hardware**: No dependence on physical infrastructure. Software API.
2. **Programmable Automation**: Shift away from static manual operation to fully configurable and dynamic
3. **Centralized Policy Orchestration:** Policy delegation and management

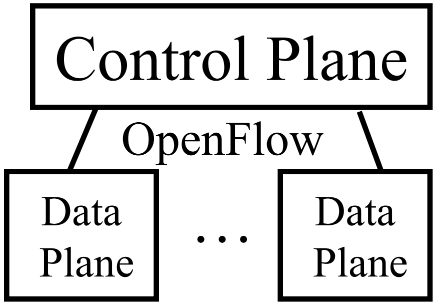


Trends Driven by SDN

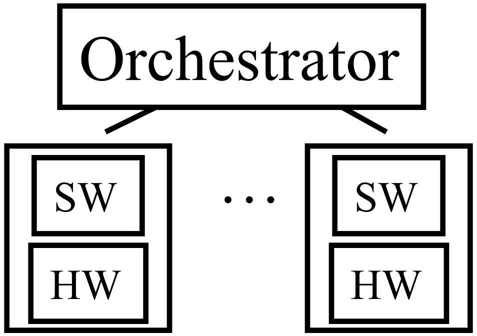
1. Disaggregation
2. Multi-Cloud and Global Orchestration
3. Open Source
4. Automation

Trend: SDN ⇒ Disaggregation

- SDN was invented in 2009. Then: SDN:
  - Separation of control and data planes
  - Centralization of Control
  - Standard Protocol between the planes



- Now: Software Defined = **Disaggregation** of HW/SW
  - Commodity hardware
  - Software on commodity HW
  - Legacy protocols survive

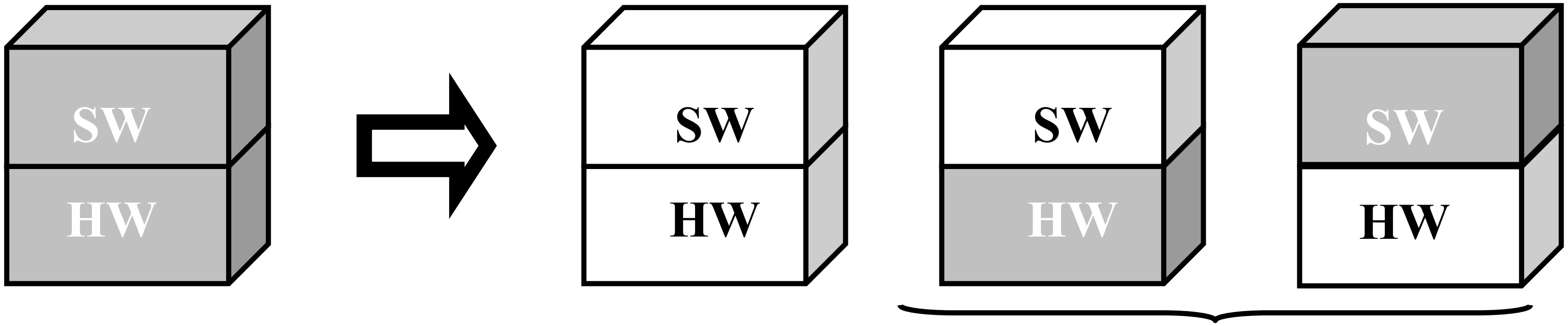


Ref: D. M Batista, G. Blair, F. Kon, R. Boutaba, D. Hutchison, R. Jain, R. Ramjee, C. Rothenberg, "Perspectives on software-defined networks: interviews with five leading scientists from the networking community" Journal of Internet Services and Applications 2015, 6:22, http://www.cse.wustl.edu/~jain/papers/jisa15.htm

J. Skorupa and D. Ciscato, "State of SDN: If You Think SDN Is the Answer, You're Asking the Wrong Question," Gartner Report G00325601, 24 August 2017, 9 pp.

Disaggregation: Black Box to White Box

- Differentiation via software ⇒ White box networking
- **Black Box**: Proprietary HW with Proprietary SW
- **White Box**: Open Source Hardware and Software
- Software on a different hardware
  ⇒ hardware can change
  Different software on a hardware
  ⇒ Software can change
- **Bright Box**: Branded White box =
  Branded SW on open HW or Open SW on Branded HW

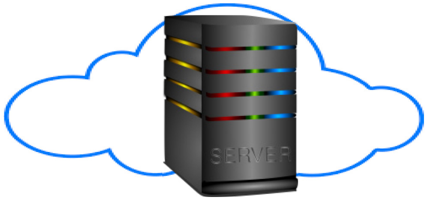


Ref: A. Lerner, "Branded Switching + White-Box Switching = Brite-Box Switching," Nov 14, 2014, https://blogs.gartner.com/andrew-lerner/2014/11/19/britefuture/

Trend: Clouds to Micro-Clouds

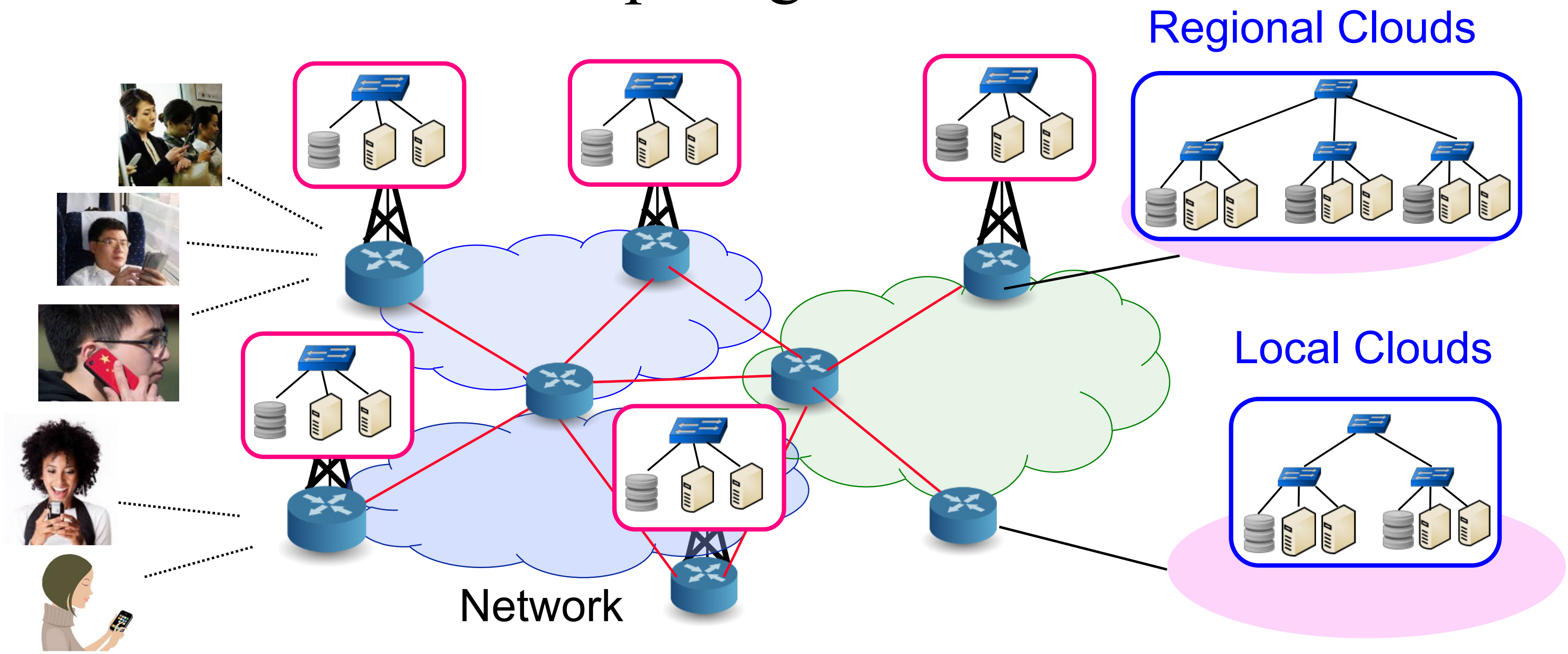
- Cloud computing was invented in 2006
- Then: Cloud = Large Data Center Multiple VMs managed by a cloud management system (OpenStack)

- Today: Cloud = Computing using virtual resources
  - µCloud = Cloud in a server with multiple VMs managed via cloud management SW, e.g., OpenStack



Trend: Core to Edge Computing

- To service mobile users/IoT, Computation needs to come to edge ⇒ Mobile Edge Computing ⇒ Multi-Cloud Computing



Ref: Lav Gupta, Raj Jain, H. Anthony Chan, "Mobile Edge Computing - an important ingredient of 5G Networks," IEEE Softwarization Newsletter, March 2016, http://www.cse.wustl.edu/~jain/papers/mec16.htm

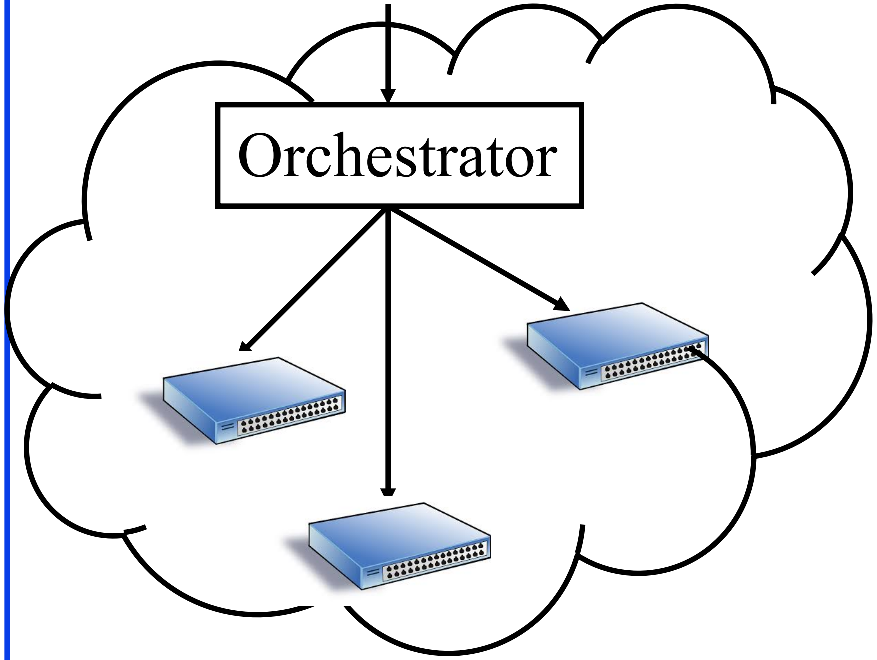
SDN = Orchestration

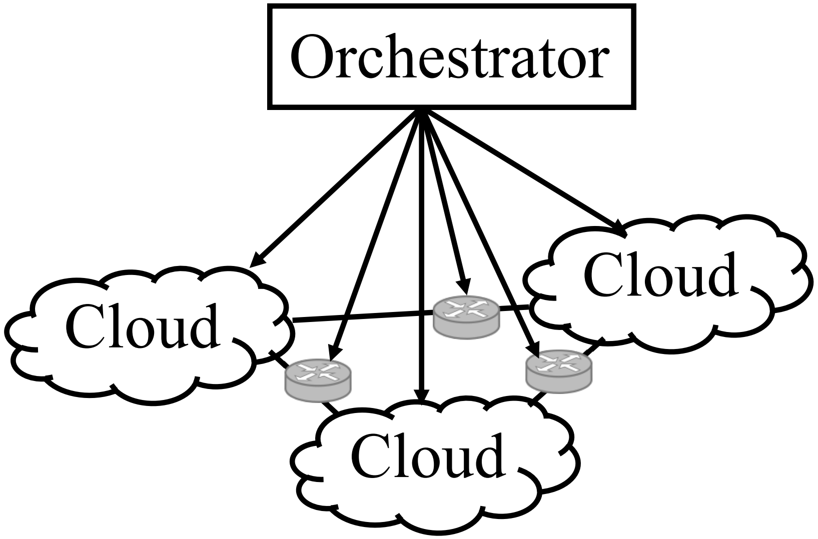
- Orchestration of Switches
  to
- Orchestration of all devices
  to
- Orchestration across clouds

Trend: Orchestration of Switches to Orchestration of Multi-Cloud

- Orchestrating Switches ⇒ Orchestrating devices ⇒ Orchestrating Clouds
- Micro-Service placement and optimization in multi-clouds

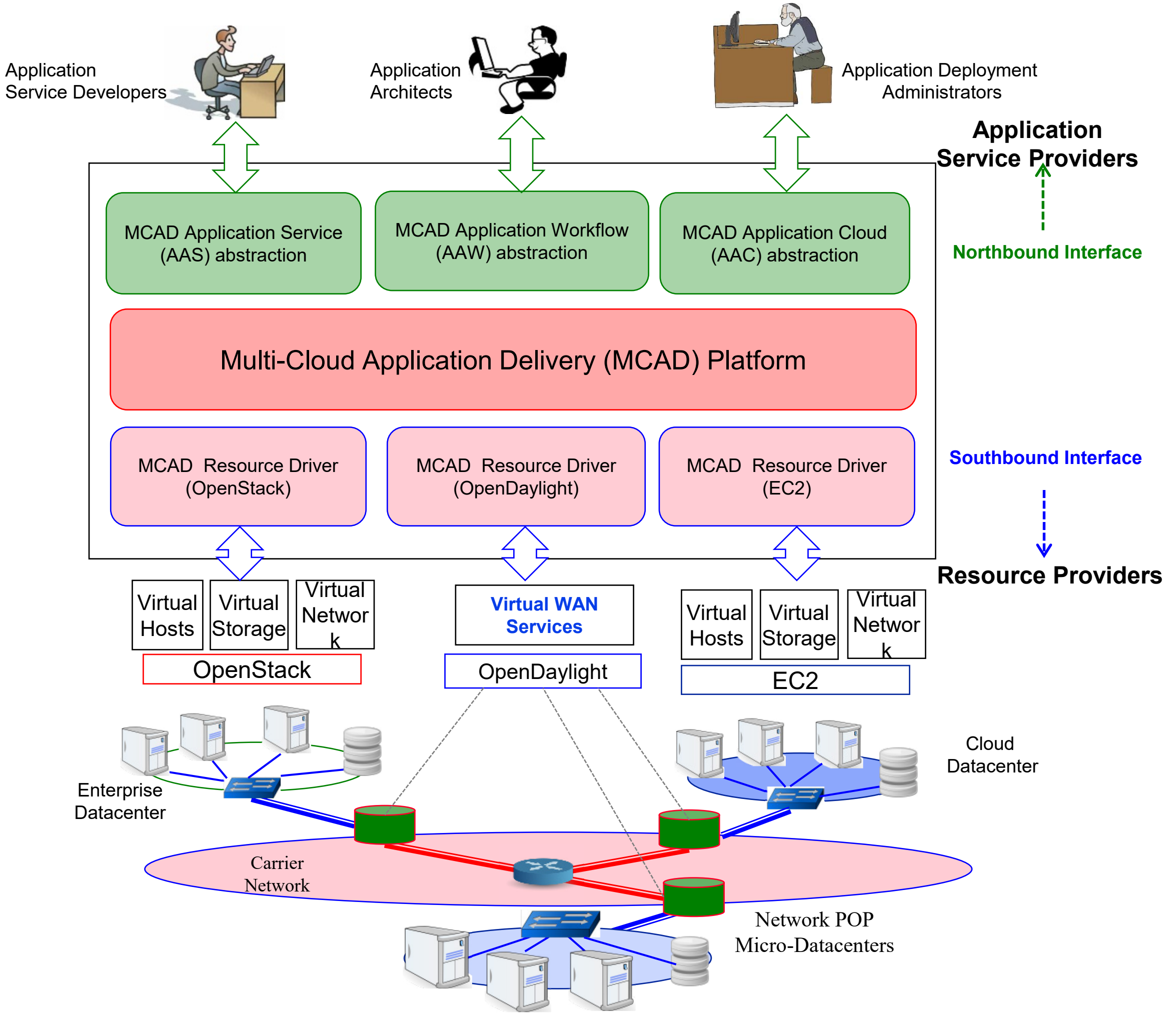
Datacenter Applications Global Applications





Ref: Subharthi Paul, Raj Jain, Mohammed Samaka, Jianli Pan, "Application Delivery in Multi-Cloud Environments using Software Defined Networking," Computer Networks Special Issue on cloud networking and communications, December 2013, http://www.cse.wustl.edu/~jain/papers/comnet14.htm

OpenADN Multi-Cloud Management



Ref: Lav Gupta, Raj Jain, Mohammed Samaka, "Analysis of Application Delivery Platform for Software Defined Infrastructures," International Journal of Communication Networks and Distributed Systems, 2016, Vol. 5, http://www.cse.wustl.edu/~jain/papers/ijcnds16.htm

Trend: SDN ⇒ Open Source

- ❑ Standard vs. Rough Consensus and Running Code
- ❑ Disaggregation ⇒ Open Source HW + Open Source SW
- ❑ # of Networking Projects at Linux Foundation
  > # of working groups at Internet Engineering Task Force
- ❑ **Open-Source Everything**:
  - ➢ Open Network Automation Platform (ONAP)
  - ➢ AI Developer Toolkits
  - ➢ Open-Source Base Station
  - ➢ DevOps Tool chain
  - ➢ Open-Source Hardware
  - ➢ OS Containers
  - ➢ Open-Source Blockchain

Open ≠ Secure

1. Open ⇒ Fast development
2. Open ⇒ Low cost
3. Open ⇒ Fast deployment
4. Open ⇒ Wide spread deployment
5. Open ⇒ Defacto standard
6. Open ⇒ No limitations/restrictions on the developers/users
   Active contribution from China
   No restrictions on Iran, Russia, North Korea, …
   Not sure if we even keep track of nationality or background of developers

❑ All of the above lead to insecurity

Vs.

Trend: SDN to Self-Driven Networks

- **Self-Discover**: Find its components
- **Self-configure**: Trending. Predict.
- **Auto-Manage** = Auto-BSS (bill)/Auto-OSS (provision)
- **Self-Monitor**: Counters and Probes. Telemetry
- **Self-Diagnose and Self-Heal**: Self-Report to human operator
- OpenDaylight is working on Network **Intent** Composition (NIC)

Network Manager

Ref: Kireerti Kompella, https://datatracker.ietf.org/meeting/98/materials/slides-98-nmrg-self-driving-networks

Impact of SDN on Security

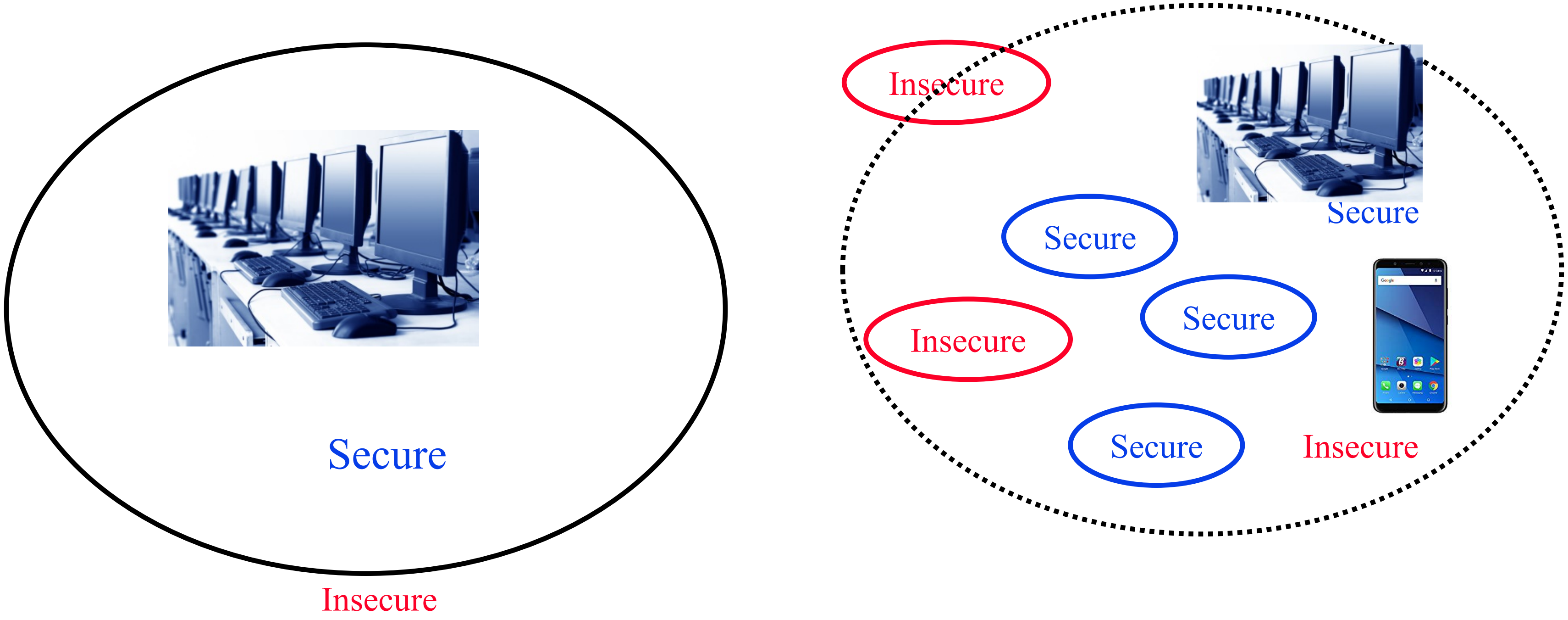
- SDN ⇒ Disaggregation ⇒ Open-Source ⇒ Insecurity
  Open Source ⇒ Can't point fingers
  ⇒ Difficult to locate source of attack

- SDN ⇒ Orchestration ⇒ Large scale Insecurity
  World-wide multi-cloud disruptions

- SDN ⇒ Automaton ⇒ Fast Insecurity
  Bring the nationwide/worldwide outages fast

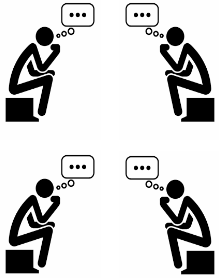
Trend: No Border-Based Security

- ❑ VPN and firewalls are based on Secure boundary wall
- ❑ Now there are no boundaries



- ❑ Need solutions that work with untrusted domains ⇒ Blockchains may be a potential solution

Probabilistic Blockchains



- ❑ Current blockchains allow only valid transactions
- ❑ Our Probabilistic Blockchains allow probabilistic statements:
  I think the attack is from Russia with 90% probability
  I am 80% confident that IBM stock will go up tomorrow 5%
- ❑ Allows risk assessment using a large number of opinions
  ⇒ Crowd sourcing of risk assessment
  ⇒ Particularly applicable to security risks
- ❑ Decisions are weighted by the reputation of the opinion makers
  Some people are experts on the topic ⇒ High Reputation
  Others are just bluffing ⇒ Low reputation after a few bluffs

Ref: T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M, Samaka, "**Security Services Using Blockchains:A State of the Art Survey**" IEEE Communications Surveys and Tutorials, 2019, Volume 21, Issue 1, 858-880 pp., http://www.cse.wustl.edu/~jain/papers/bcs.htm

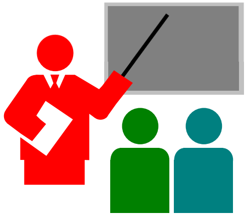
T. Salman, R. Jain, and L. Gupta, "**Probabilistic Blockchains: A Blockchain Paradigm for Collaborative Decision-Making**," 9th IEEE UEMCON 2018, http://www.cse.wustl.edu/~jain/papers/pbc_uem.htm

T. Salman, R. Jain, L. Gupta, "**A Reputation Management Framework for Knowledge-Based and Probabilistic Blockchains**," 2019 IEEE International Conference on Blockchain, July 14, 2019, http://www.cse.wustl.edu/~jain/papers/rpmcewa.htm

Other Recommendations

- Security and testing certification of open source sw/hw should be part of the supplier contract
- A central organization like NIST may take responsibility for release testing and certification of software
- Need complete KYC tracking of developers, testers, … for critical components
- How do you handle Linux?

Summary



1. SDN is not defined by "Separation of Control Plane"
2. SDN = Orchestration of Policies
   Disaggregation of HW+SW ⇒ Open Source
   Programmability ⇒ Automation
3. Open source ⇒ Crowd development
   ⇒ Fast but new security issues
4. Automation and orchestration increase the extent of damage
5. New solutions need to be developed that work for untrusted domains.

Our Related Papers

- Daniel M Batista, Gordon Blair, Fabio Kon, Raouf Boutaba, David Hutchison, R. Jain, Ramachandran Ramjee, Christian Esteve Rothenberg, "**Perspectives on software-defined networks: interviews with five leading scientists from the networking community**" Journal of Internet Services and Applications 2015, 6:22, http://www.cse.wustl.edu/~jain/papers/jisa15.htm
- Lav Gupta, Raj Jain, H. Anthony Chan, "Mobile Edge Computing - an important ingredient of 5G Networks," IEEE Softwarization Newsletter, March 2016, http://www.cse.wustl.edu/~jain/papers/mec16.htm
- S. Paul, R. Jain, M. Samaka, J. Pan, "**Application Delivery in Multi-Cloud Environments using Software Defined Networking**," Computer Networks Special Issue on cloud networking and communications, December 2013, http://www.cse.wustl.edu/~jain/papers/comnet14.htm
- Lav Gupta, Raj Jain, Mohammed Samaka, "Analysis of Application Delivery Platform for Software Defined Infrastructures," International Journal of Communication Networks and Distributed Systems, 2016, Vol. 5, http://www.cse.wustl.edu/~jain/papers/ijcnds16.htm

Our Related Papers (Cont)

- T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M, Samaka, "Security Services Using Blockchains:A State of the Art Survey" IEEE Communications Surveys and Tutorials, 2019, Volume 21, Issue 1, 858-880 pp., http://www.cse.wustl.edu/~jain/papers/bcs.htm
- R. Jain and S. Paul, "**Network Virtualization and Software Defined Networking for Cloud Computing - A Survey**," IEEE Communications Magazine, Nov 2013, pp. 24-31, http://www.cse.wustl.edu/~jain/papers/net_virt.htm [340+ Citations]
- S. Paul, R. Jain, "**OpenADN: Mobile Apps on Global Clouds Using OpenFlow and Software Defined Networking**," IEEE Global Communications Conference (Globecom) 2012, Anaheim, CA, December 3-7, 2012, http://www.cse.wustl.edu/~jain/papers/adn_gc12.htm

Talks

- R. Jain, "**Trends and Issues in Softwarization of Networks: What's In, What's Out**," Invited talk at IEEE Workshop on Network Automation, Piscata Way, NJ, Feb 25, 2018, http://www.cse.wustl.edu/~jain/talks/inetauto.htm
- R. Jain, "**Software Defined Multi-Cloud Networking at the Tactical Edge**," Panel Presentation at IEEE MILCOM 2016 Conference, Baltimore, MD, November 2, 2016, http://www.cse.wustl.edu/~jain/talks/sdn_mlcb.htm
- R. Jain, "**Software Defined Networking at the Tactical Edge**," Panel presentation at IEEE Milcom 2015, Tampa, FL, Oct 28, 2015, http://www.cse.wustl.edu/~jain/talks/sdn_mlc.htm
- R. Jain, "**Application Delivery Using Software Defined Networking**," Talk at Global Indian Technology Professionals (GITPro) World 2013, Palo Alto, CA, April 13, 2013, http://www.cse.wustl.edu/~jain/talks/sdn_gw.htm
- R. Jain, "**OpenADN: Mobile Apps on Global Clouds Using Software Defined Networking**," Invited talk at IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS) 2012, December 16-19, 2012, Bangalore, India, http://www.cse.wustl.edu/~jain/talks/adn_ant.htm
- R. Jain "**Network Virtualization and Application Delivery Using Software Defined Networking**," Invited talk at Advanced Computing and Communications Conference 2012 (ADCOM 2012), 14-16th December 2012, Bangalore, India, http://www.cse.wustl.edu/~jain/talks/adn_adc.htm

Acronyms

AAAS	American Association for Advancement of Science
AAC	Application Cloud Abstraction
AAS	Application Architecture Abstraction
AAW	Application Workflow Abstraction
AI	Artificial Intelligence
API	Application Programming Interface
APIC	Application Policy Infrastructure Controller
BSS	Business Support Systems
CTO	Chief Technology Officer
DEC	Digital Equipment Corporation
DevOps	Development and Operations
EC2	Elastic Compute 2
ECN	Explicit Congestion Notification
DLUX	OpenDaylight User Interface
HTTP	Hypertext Tranfer Protocol
HW	Hardware

Acronyms (Cont)

IEEE	Institution of Electrical and Electronic Engineers
IP	Internet Protocol
IPv4	Internet Protcol version 4
IPv6	Internet Protcol version 6
KYC	Know Your Customer
L2	Layer 2
MCAD	Multi-Cloud Application Development
MPLS	Multi-protocol Label Switching
NetIDE	Network Interactive Development Environment
NIC	Network Intent Composition
NIST	National Institute of Standards and Technology
OF	OpenFlow
ONF	Open Networking Forum
ONAP	Open Networking Automation Platform
ONiE	Open Network Install Engine
ONL	Open Net Linux

Acronyms (Cont)

ONV	OpenDaylight Network Virtualization
OS	Operating System
OSCP	OpenDaylight SDN Controller Platform
OSGi	Open Services Gateway Initiative
OSPF	Open Shortest Path First
OVSDB	Open Virtual Switch Database
PCEP	Path Computation Element Protocol
SAL	Service Abstraction Layer
SDN	Software Defined Networking
SIGCOMM	Special Interest Group on Communications
SW	Software
VM	Virtual Machine
VPN	Virtual Private Network
VxLAN	Virtual Extensible Local Area Network

Scan This to Download These Slides

Raj Jain
http://rajjain.com