black hat®

USA 2017

JULY 22-27, 2017

MANDALAY BAY / LAS VEGAS

#BHUSA / @BLACKHATEVENTS

FlowFuzz

A Framework for Fuzzing OpenFlow-enabled
Software and Hardware Switches

Nicholas Gray, Manuel Sommer, Thomas Zinner, Phuoc Tran-Gia

About us

Nicholas Gray
M. Sc.

Manuel Sommer
B. Sc.

Dr. Thomas
Zinner

Prof. Dr.-Ing.
Phuoc Tran-Gia

Modeling, Performance Analysis & Optimization, Measurement, Experimentation, Simulation

- Software-defined Networking & Cloud Networks
- Future Internet & Smartphone Applications
- Network Dynamics & Control
- QoE Modeling & Resource Management

Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

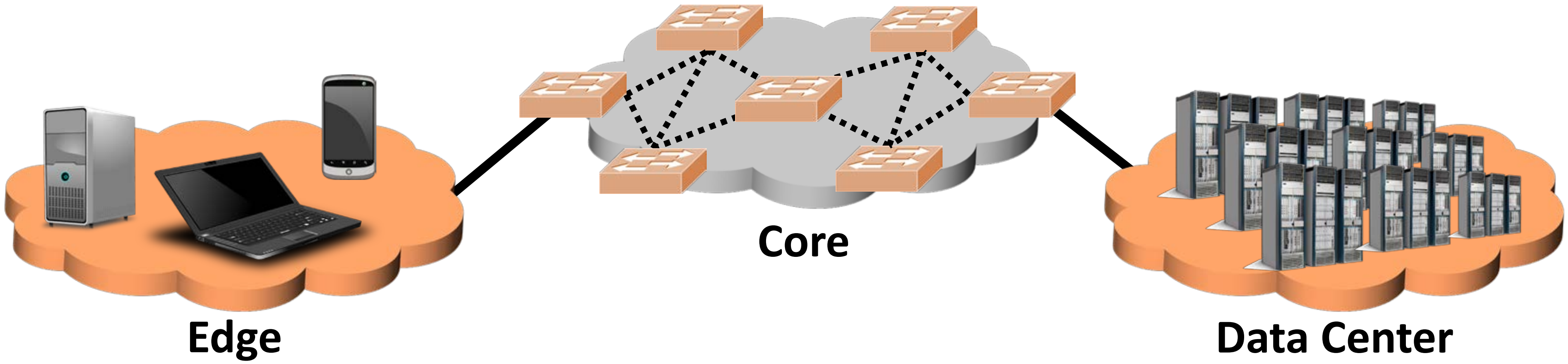
Chair of Communication Networks
comnet.informatik.uni-wuerzburg.de

SarDiNe
Sardine-project.org

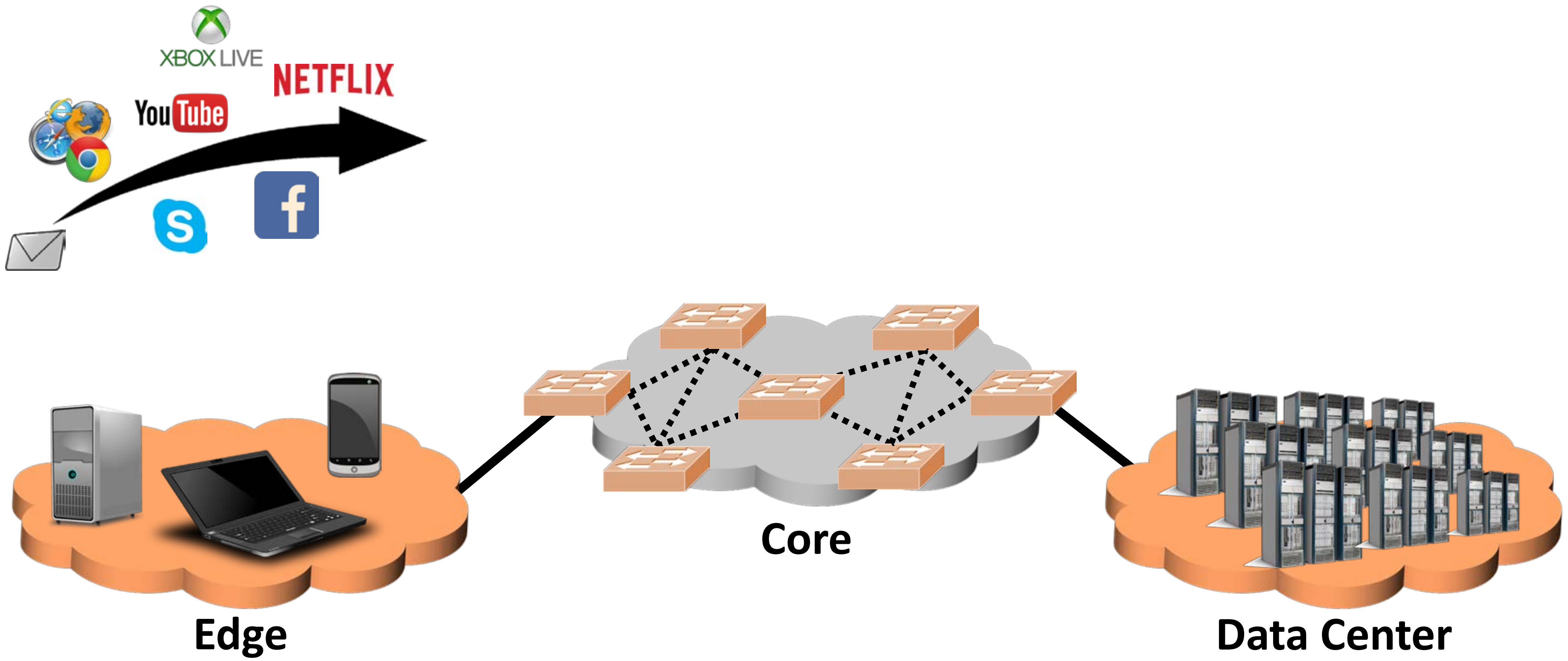
Agenda

- Software-defined Networking (SDN)
  - SDN Basics
  - Enhancing Network Security with SDN
  - Overview of the SDN Attack Surface
  - OpenFlow
- FlowFuzz
  - Architecture
  - Evaluation of Software Switches
  - Investigation of Feedback Sources for Hardware Switches
  - Evaluation of Hardware Switches

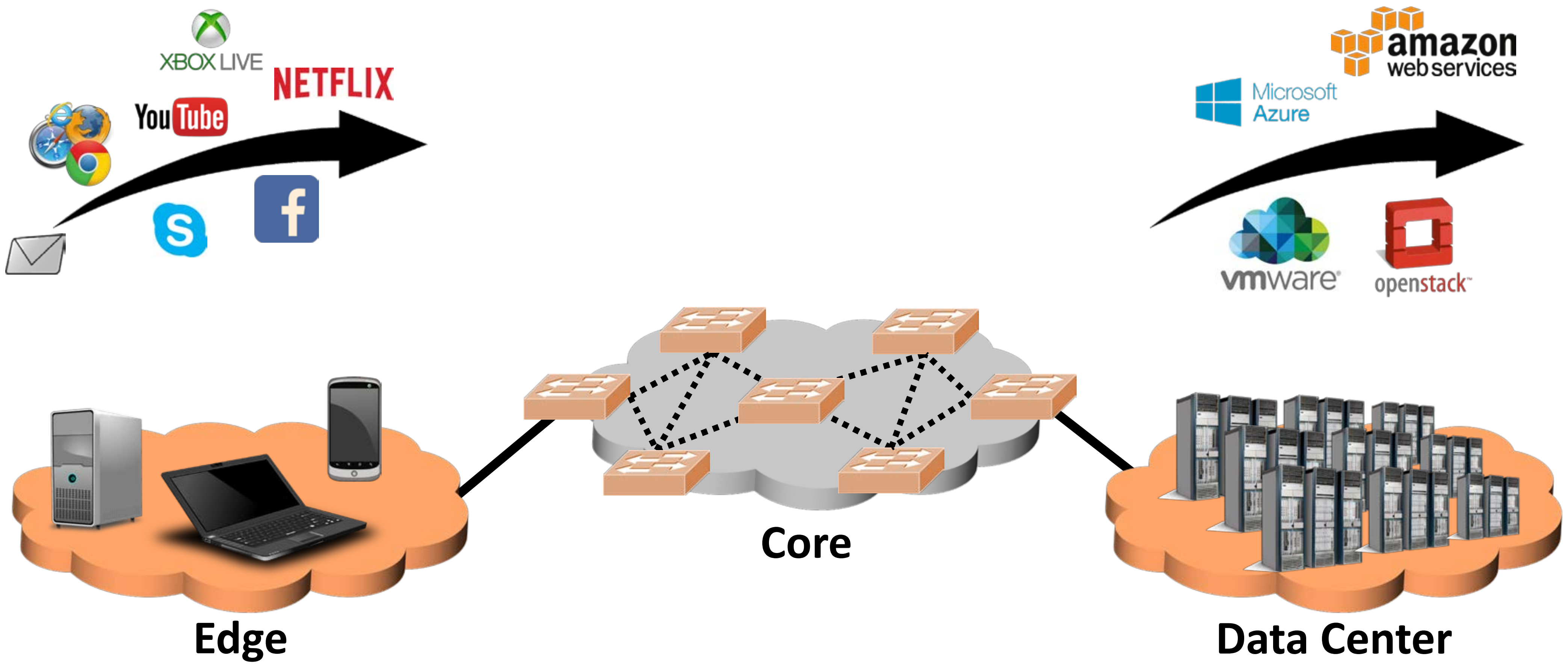
Speed of Innovation



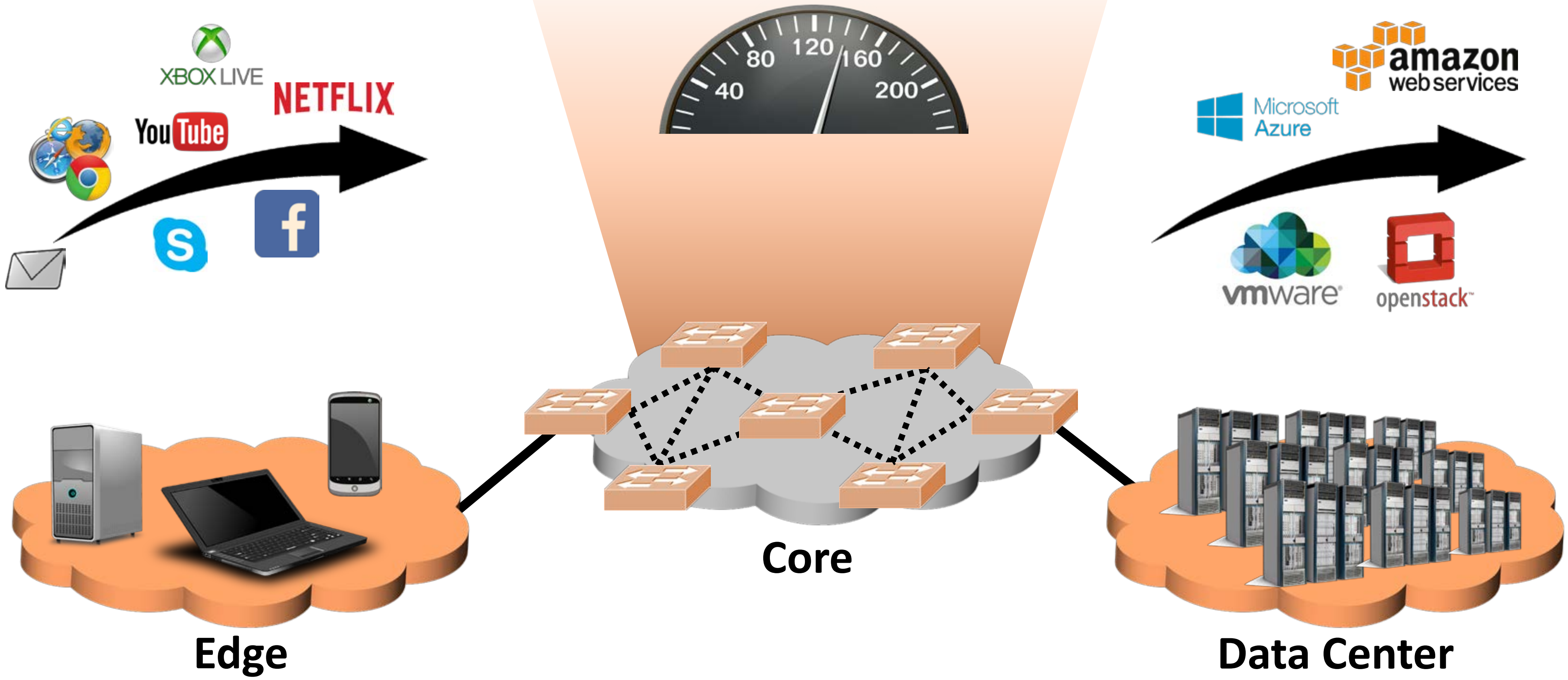
Speed of Innovation

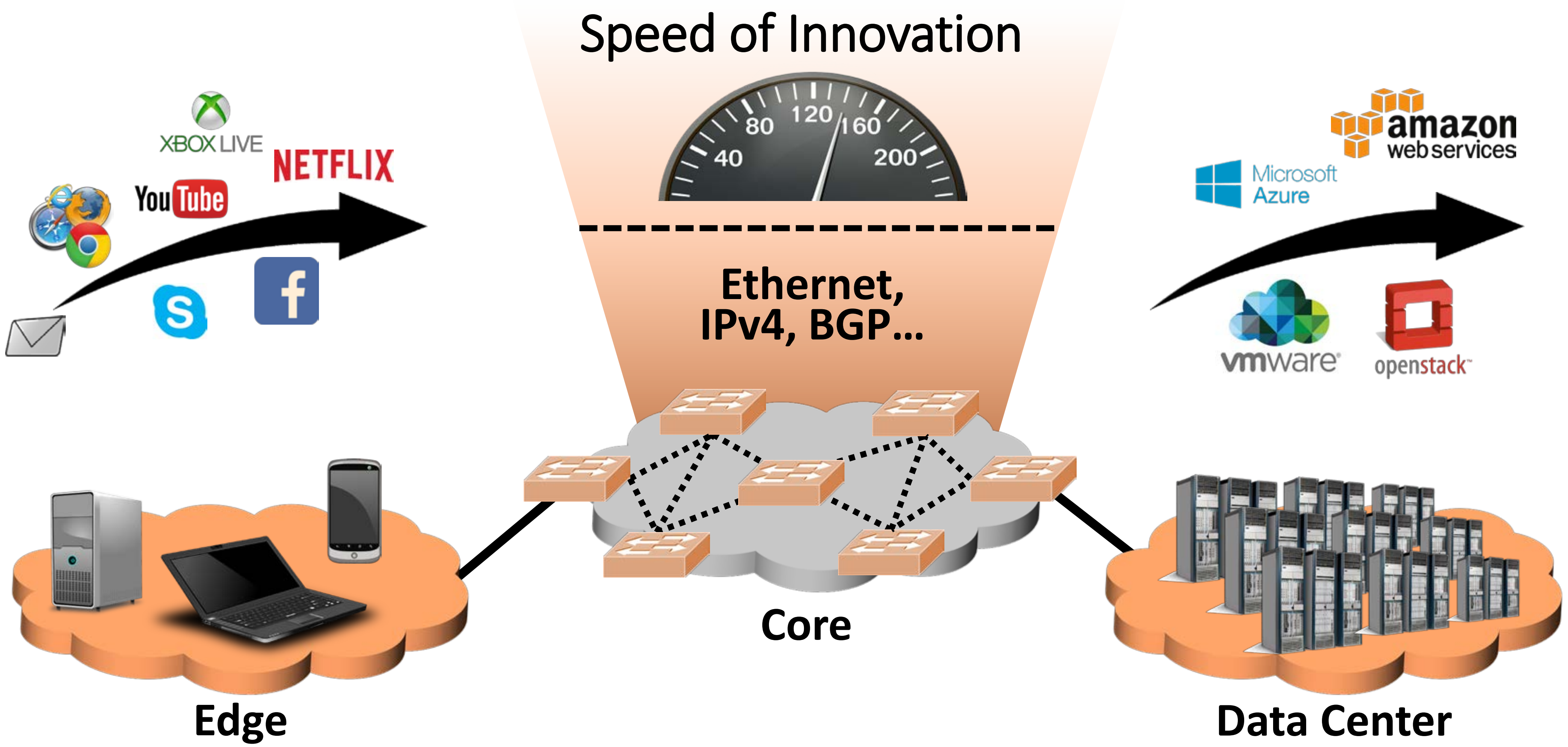


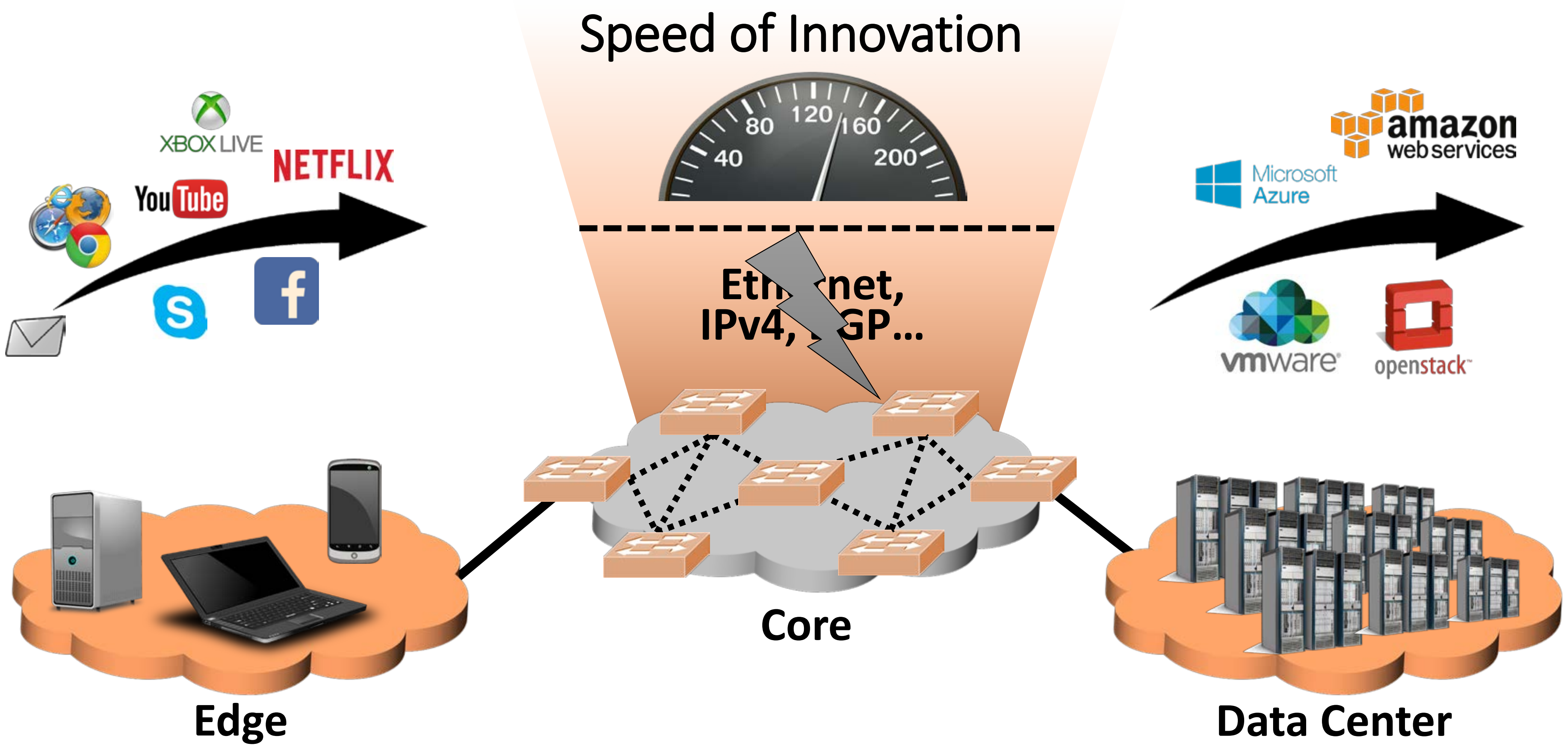
Speed of Innovation



Speed of Innovation

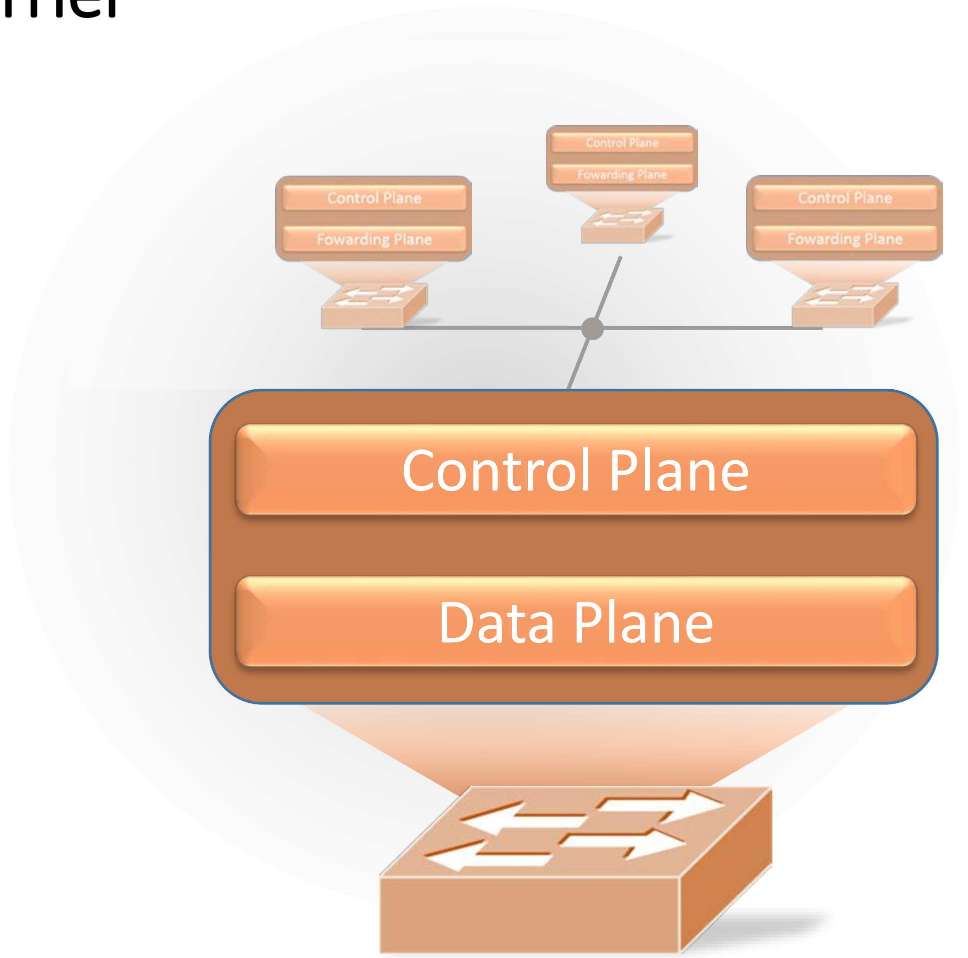



Speed of Innovation
40
80
120
160
200
Ethernet,
IPv4, BGP...
XBOX LIVE
NETFLIX
YouTube
Microsoft Azure
amazon web services
vmware
openstack
Edge
Core
Data Center


Speed of Innovation
40
80
120
160
200
XBOX LIVE
NETFLIX
YouTube
amazon web services
Microsoft Azure
vmware
openstack
Eth net,
IPv4, GP...
Edge
Core
Data Center

Innovation Barrier

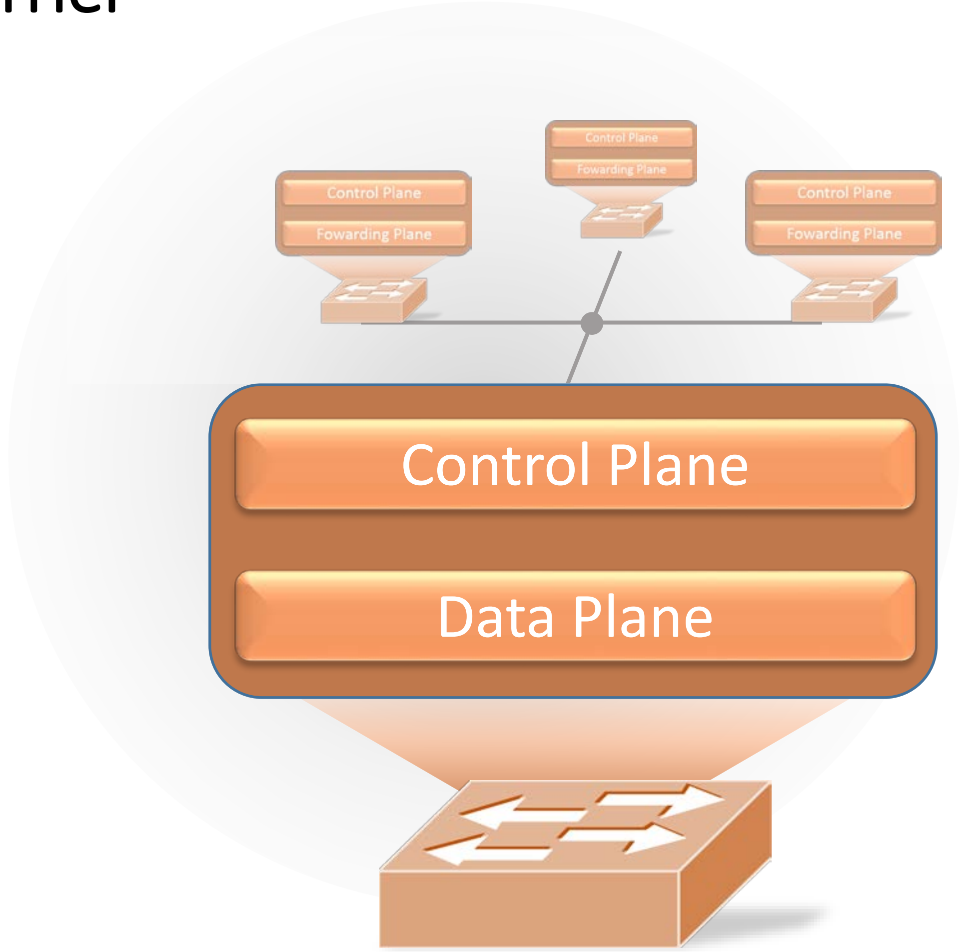
Specialized Hardware



Innovation Barrier

Specialized Hardware

Proprietary Firmware

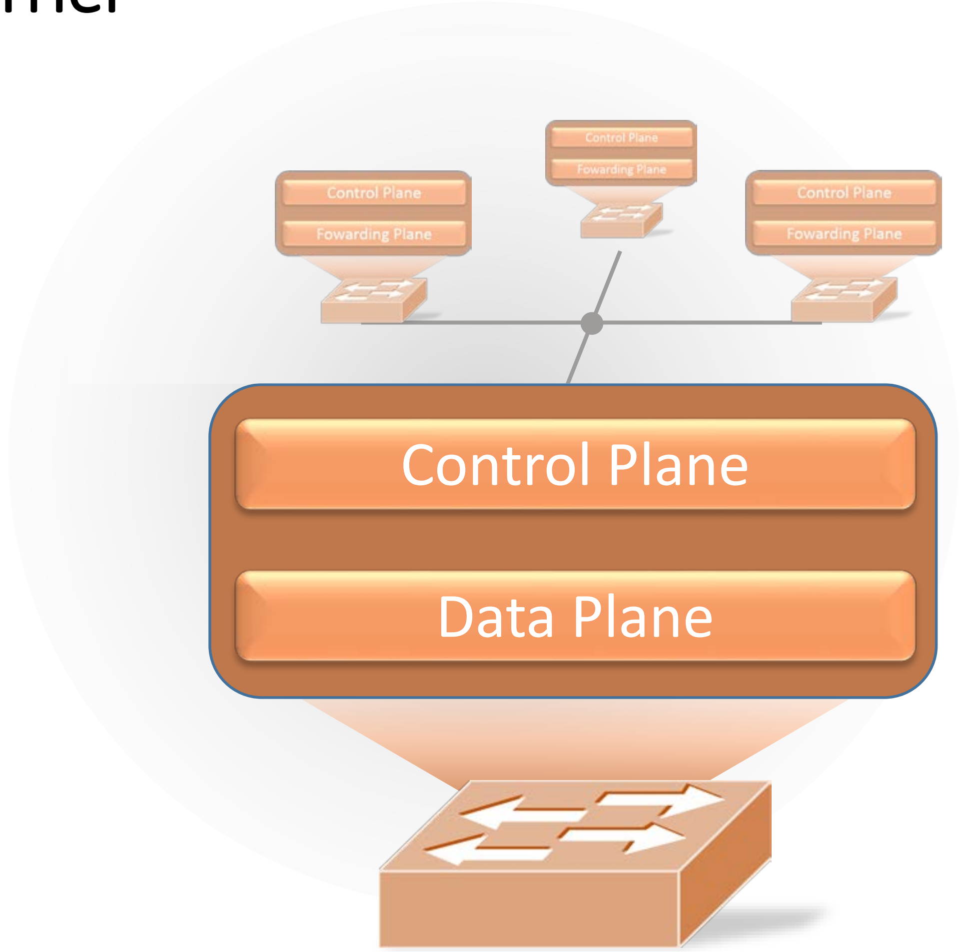


Innovation Barrier

Specialized Hardware

Proprietary Firmware

Over Specification



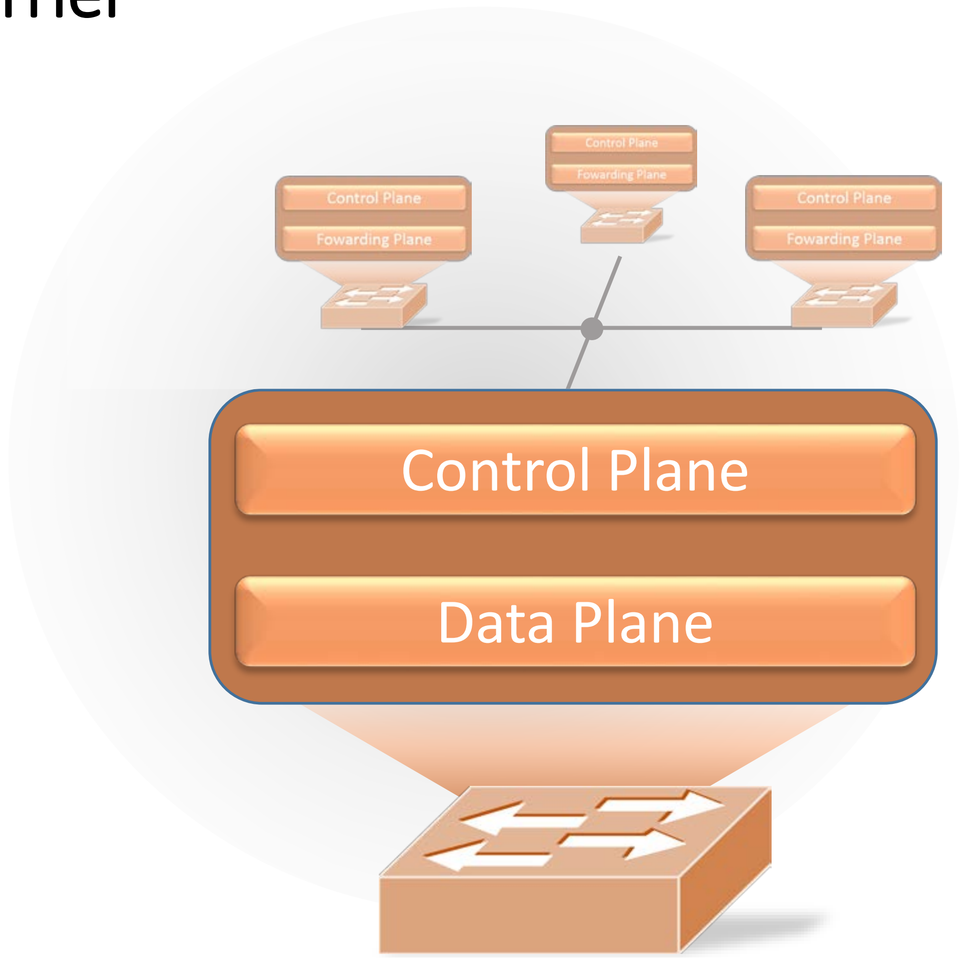
Innovation Barrier

Specialized Hardware

Proprietary Firmware

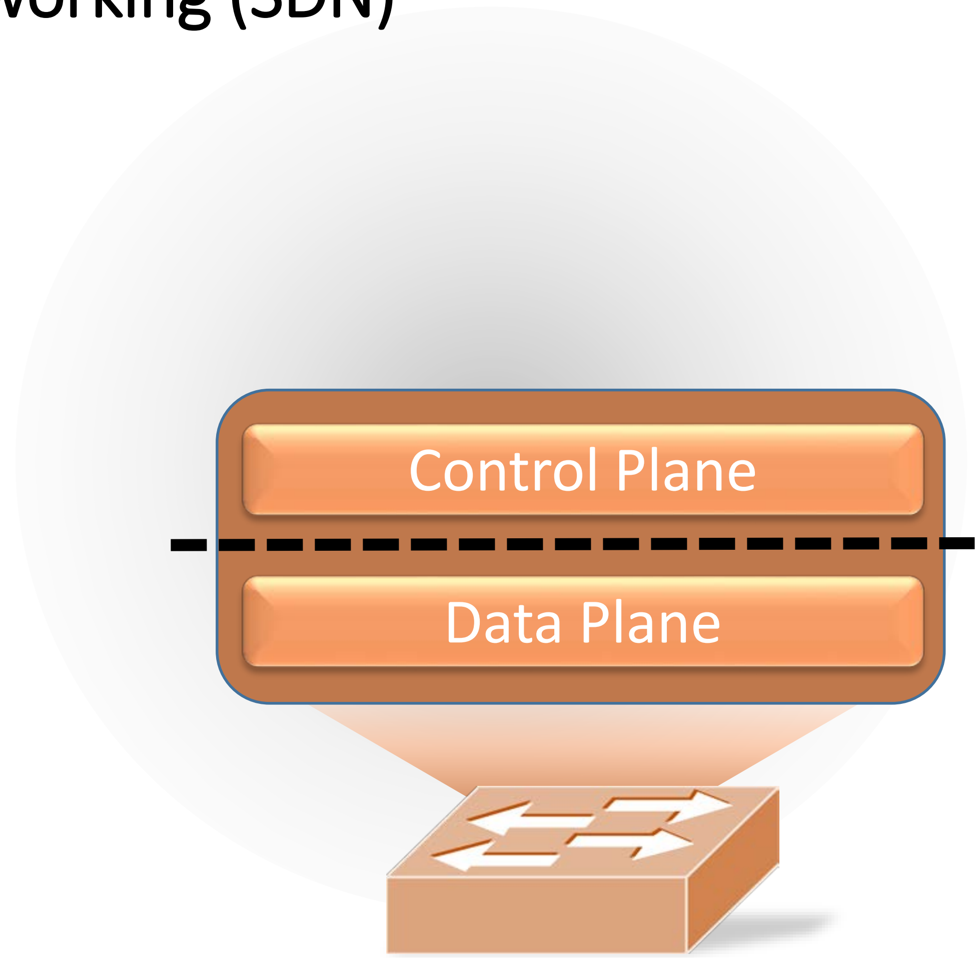
Over Specification

Few Vendors



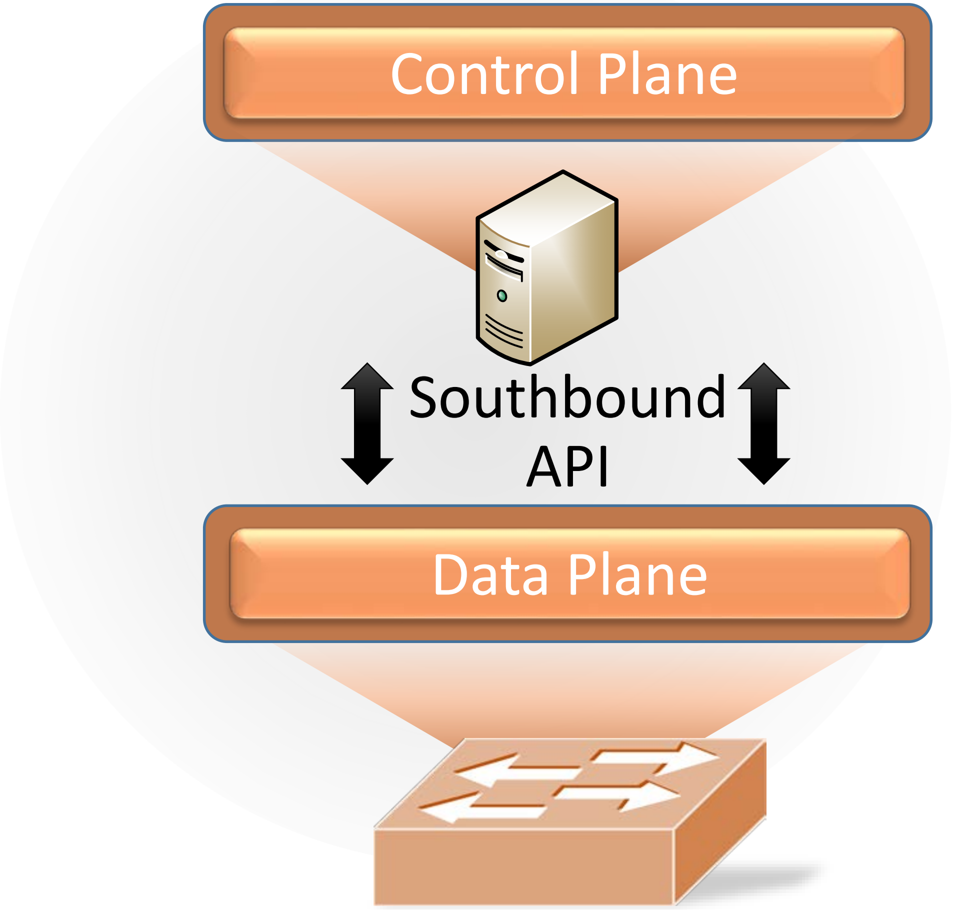
Software-defined Networking (SDN)

Separation of Control and Data Plane



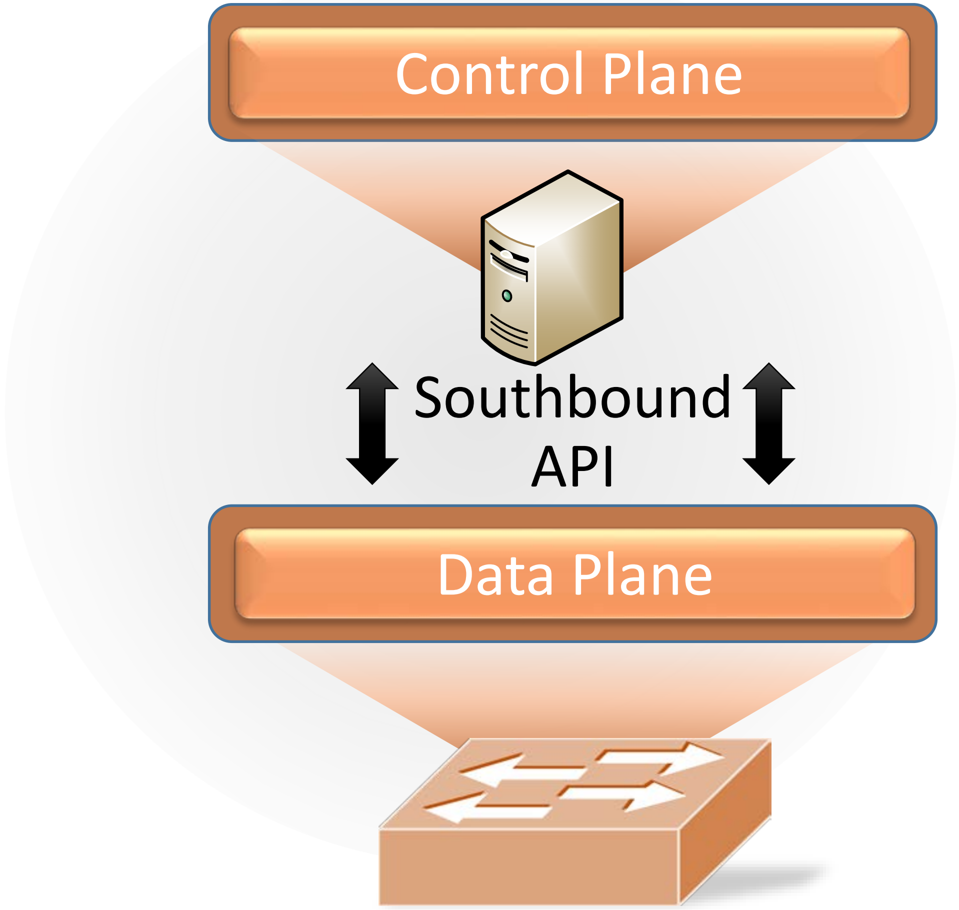
Software-defined Networking (SDN)

Separation of Control and Data Plane



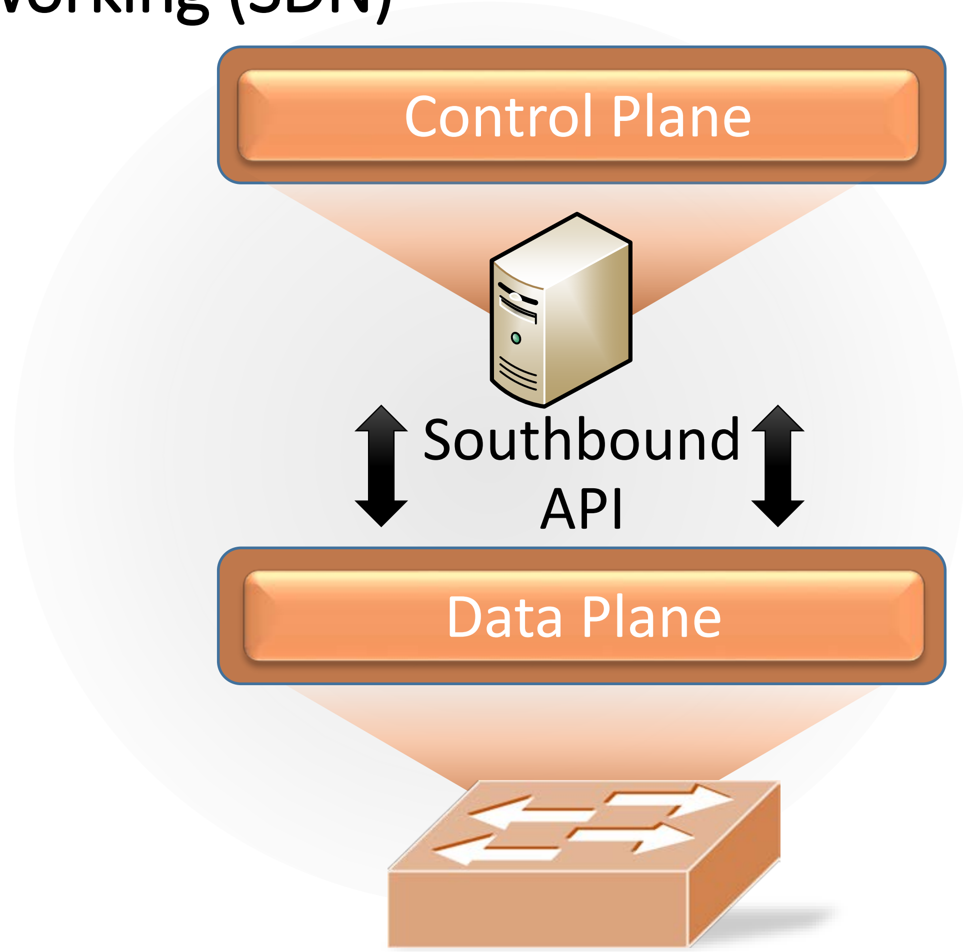
Software-defined Networking (SDN)

- Separation of Control and Data Plane
- Logically Centralized Control Plane



Software-defined Networking (SDN)

- Separation of Control and Data Plane
- Logically Centralized Control Plane
- Open Interfaces



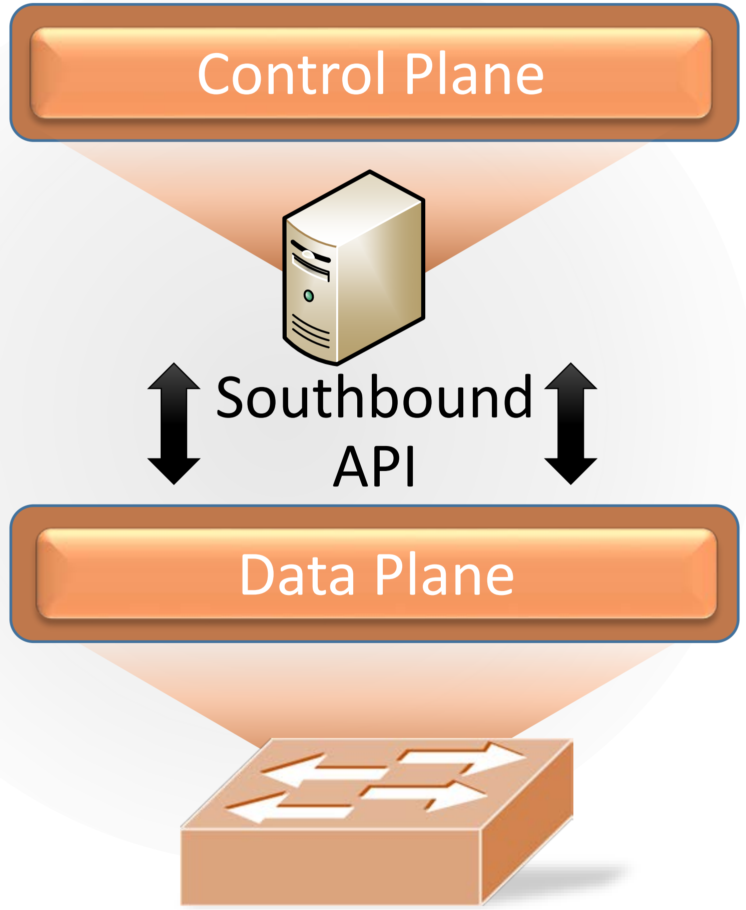
Software-defined Networking (SDN)

Separation of Control and Data Plane

Logically Centralized Control Plane

Open Interfaces

Programm-ability



SDN – Packet Handling & Table Structure

SDN – Packet Handling & Table Structure

Switch Port	Switch Phy Port	Meta data	ETH Dst	ETH Src	ETH Type	VLAN VID	VLAN PCP	IP DSCP	IP ECN	IP Proto	IPv4 Src	IPv4 Dst	…
ICMPv4 Type	ICMPv4 Code	TCP Src	TCP Dst	UDP Src	UDP Dst	SCTP Src	SCTP Dst	ARP OP	ARP SPA	ARP TPA	ARP SHA	ARP THA	…

\+ Mask for match fields

SDN – Packet Handling & Table Structure

Rule → Action → Stats

- Forward packet to zero or more ports
- Encapsulate and forward to controller
- Send to normal processing pipeline
- Modify Fields
- Any extensions you add!

Switch Port	Switch Phy Port	Meta data	ETH Dst	ETH Src	ETH Type	VLAN VID	VLAN PCP	IP DSCP	IP ECN	IP Proto	IPv4 Src	IPv4 Dst	…
ICMPv4 Type	ICMPv4 Code	TCP Src	TCP Dst	UDP Src	UDP Dst	SCTP Src	SCTP Dst	ARP OP	ARP SPA	ARP TPA	ARP SHA	ARP THA	…

\+ Mask for match fields

SDN – Packet Handling & Table Structure

Rule → Action → Stats

Action:

- Forward packet to zero or more ports
- Encapsulate and forward to controller
- Send to normal processing pipeline
- Modify Fields
- Any extensions you add!

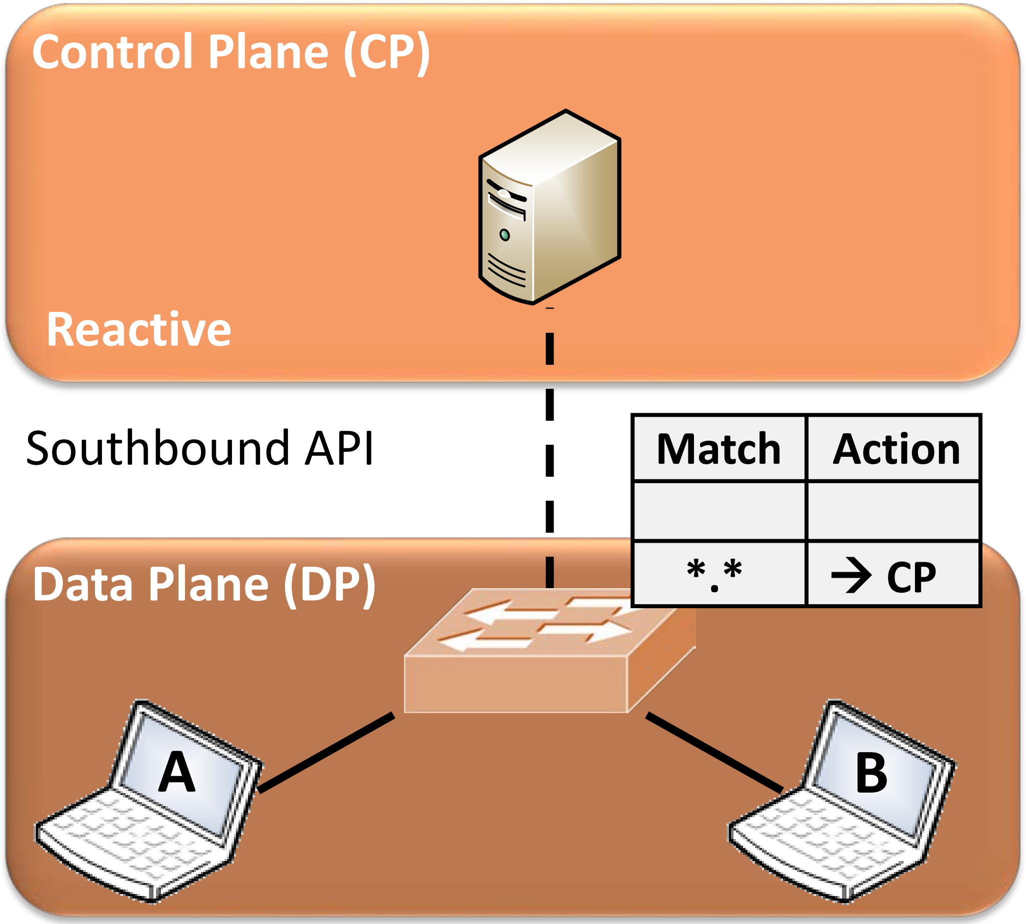
Stats: Packet + Byte Counters

Rule:

Switch Port	Switch Phy Port	Meta data	ETH Dst	ETH Src	ETH Type	VLAN VID	VLAN PCP	IP DSCP	IP ECN	IP Proto	IPv4 Src	IPv4 Dst	…
ICMPv4 Type	ICMPv4 Code	TCP Src	TCP Dst	UDP Src	UDP Dst	SCTP Src	SCTP Dst	ARP OP	ARP SPA	ARP TPA	ARP SHA	ARP THA	…

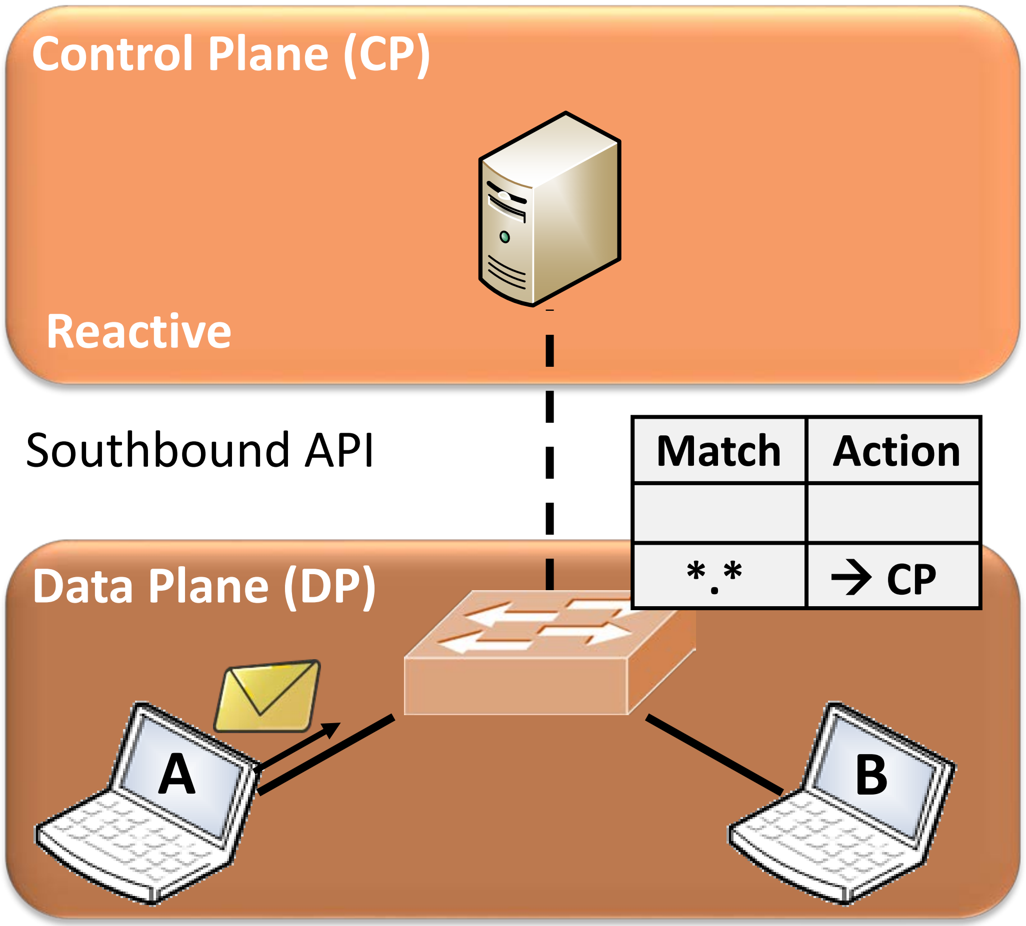
\+ Mask for match fields

SDN Example

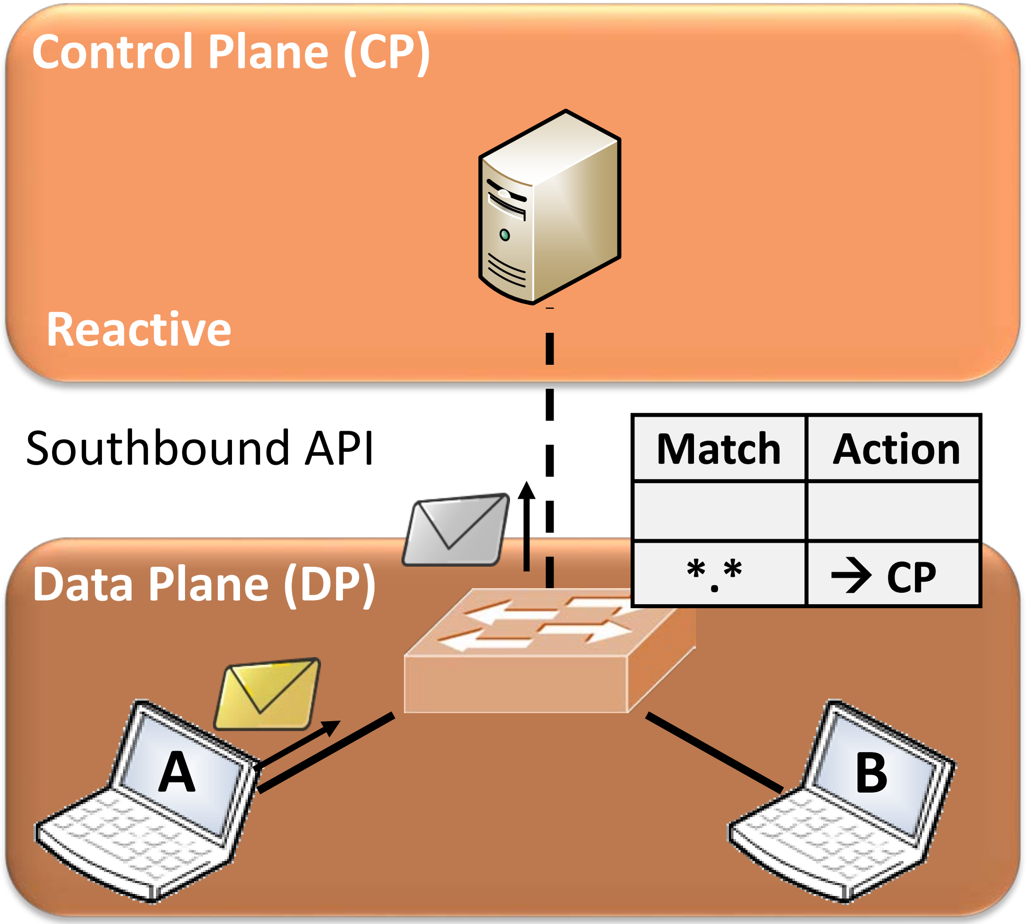


Control Plane (CP)
Reactive
Southbound API
Match
Action
.
→ CP
Data Plane (DP)
A
B

SDN Example

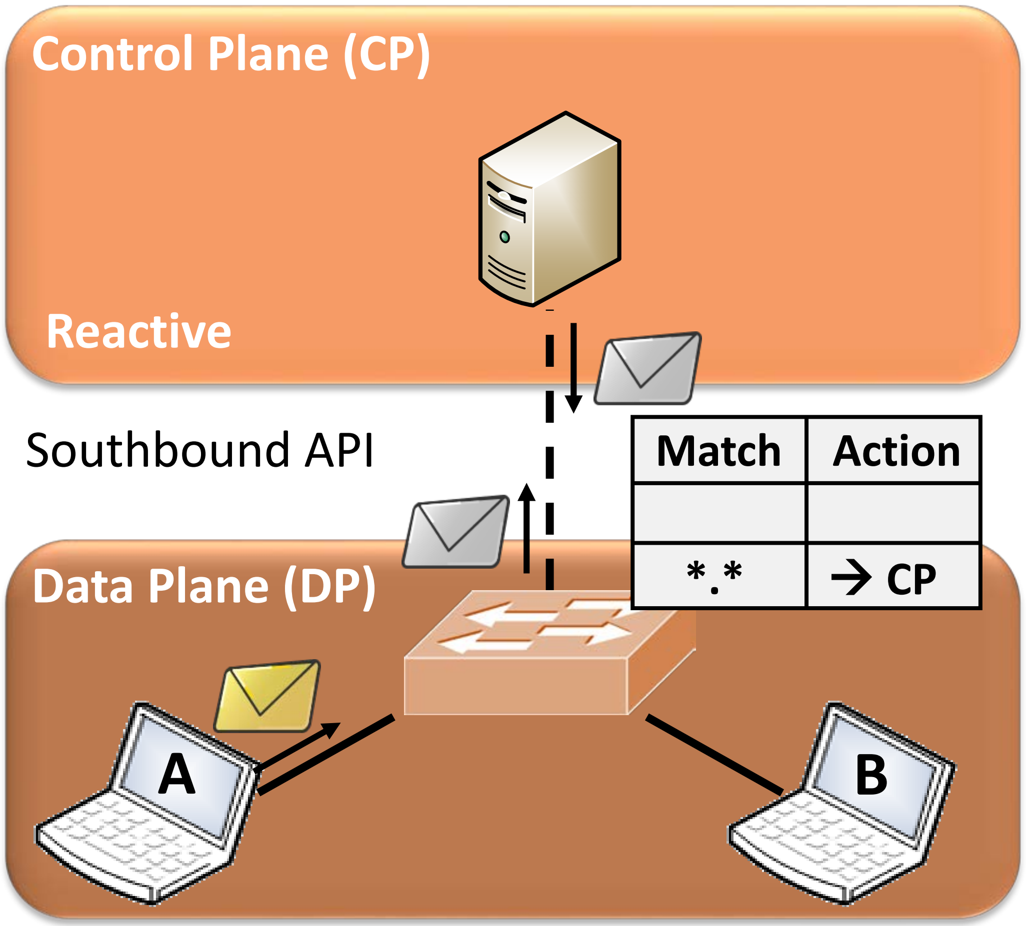

Control Plane (CP)
Reactive
Southbound API
Match
Action
.
→ CP
Data Plane (DP)
A
B

SDN Example

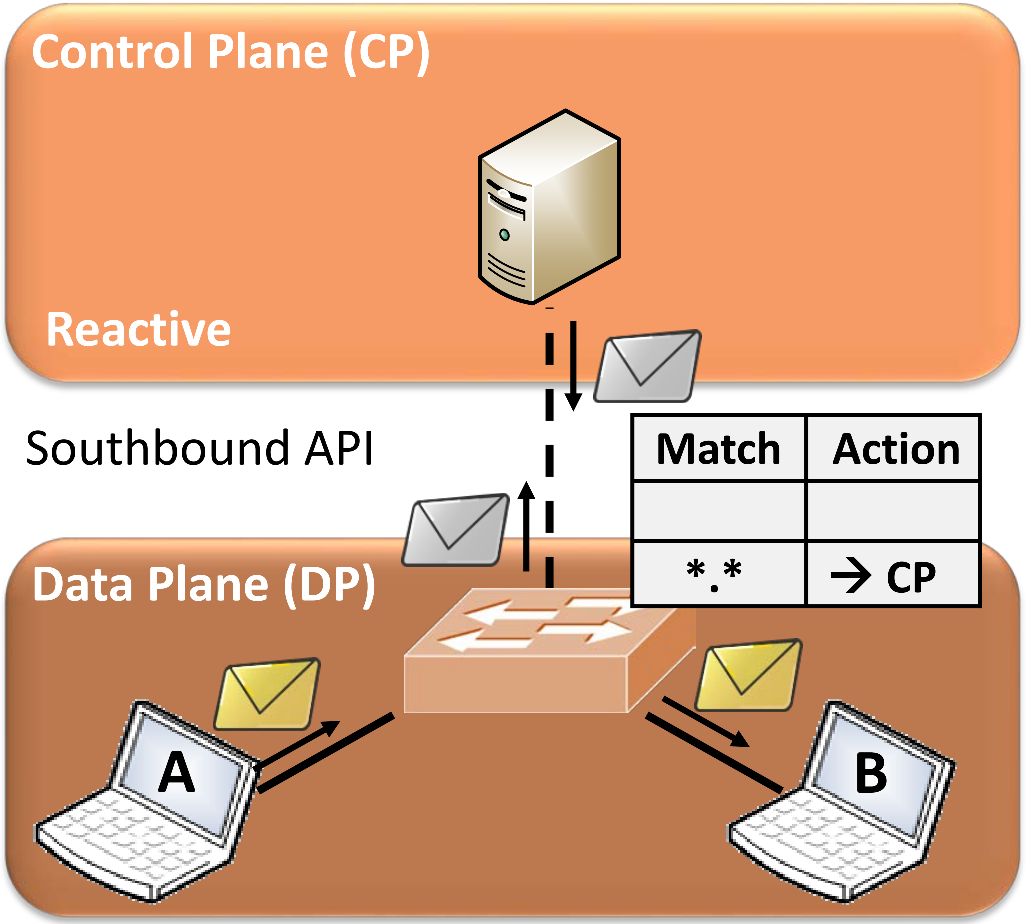


Control Plane (CP)
Reactive
Southbound API
Match
Action
.
→ CP
Data Plane (DP)
A
B

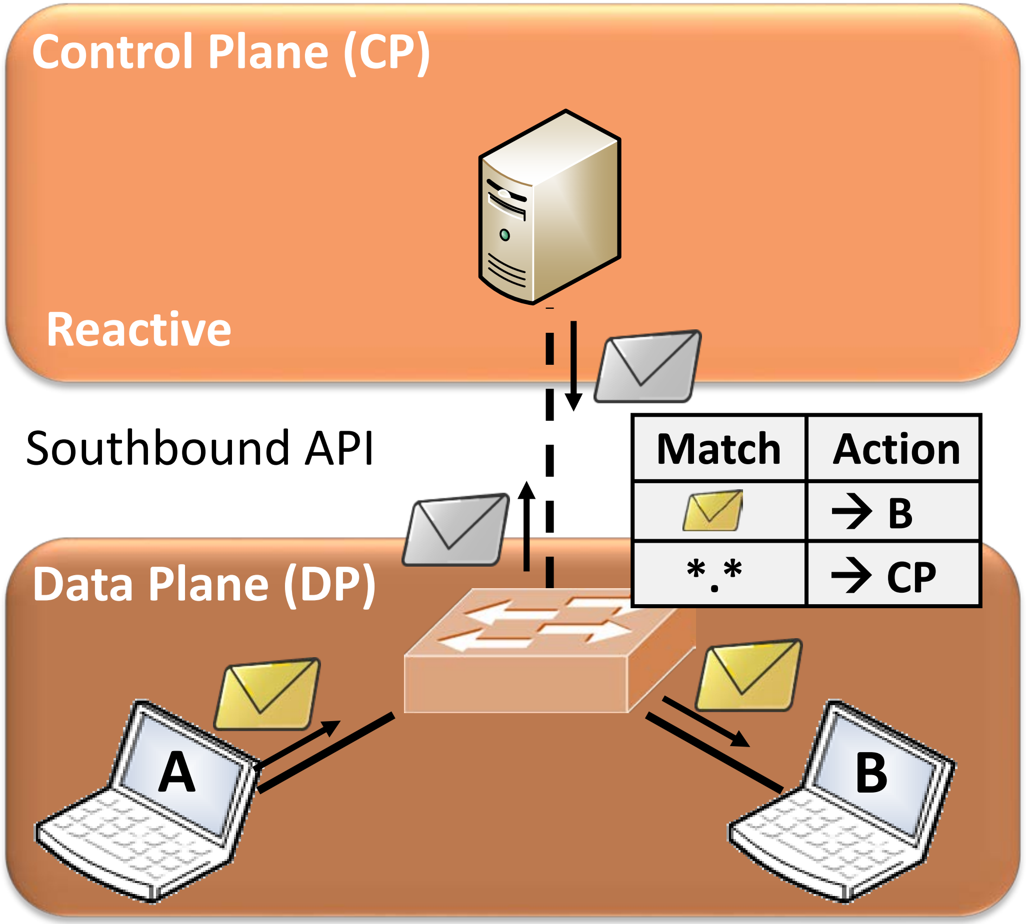
SDN Example


Control Plane (CP)
Reactive
Southbound API
Match
Action
.
→ CP
Data Plane (DP)
A
B

SDN Example

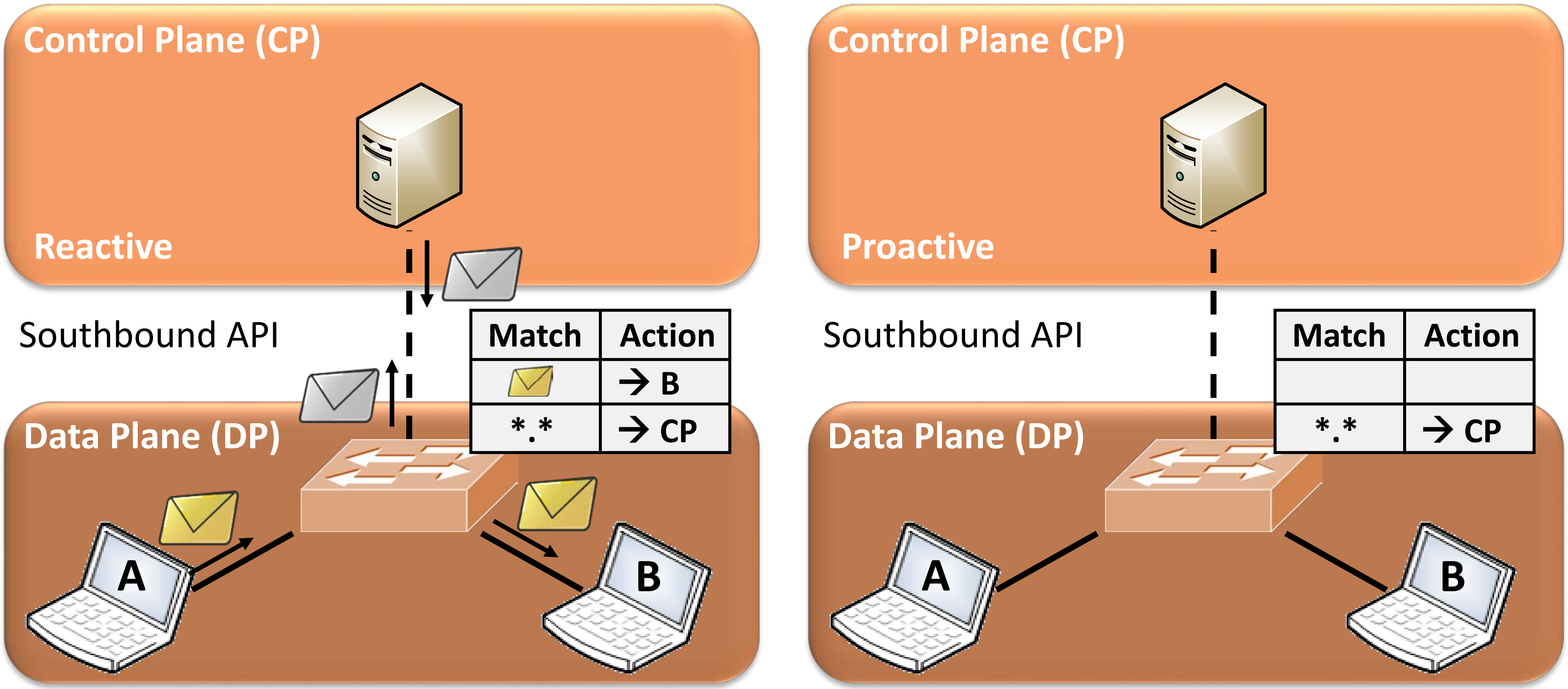

Control Plane (CP)
Reactive
Southbound API
Match
Action
.
→ CP
Data Plane (DP)
A
B

SDN Example

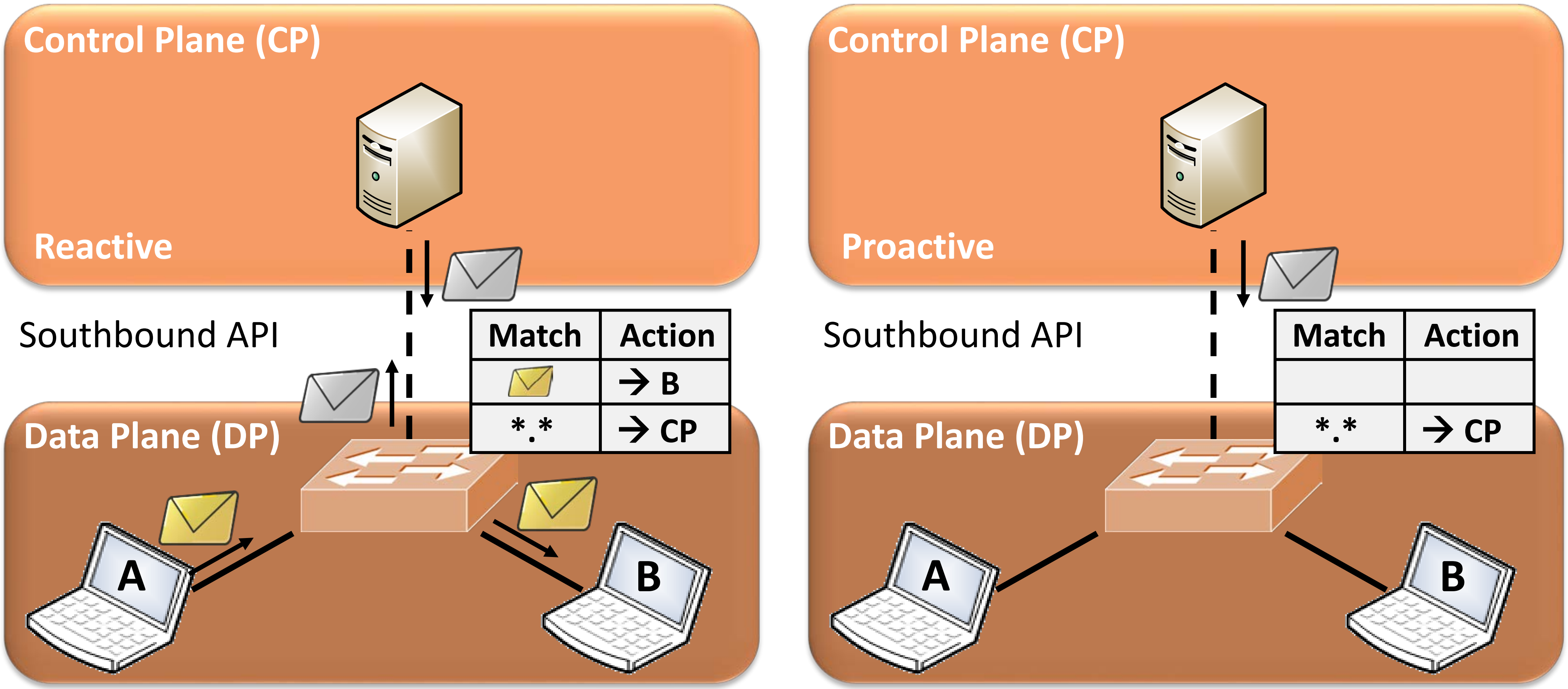


Match	Action
(envelope)	→ B
.	→ CP

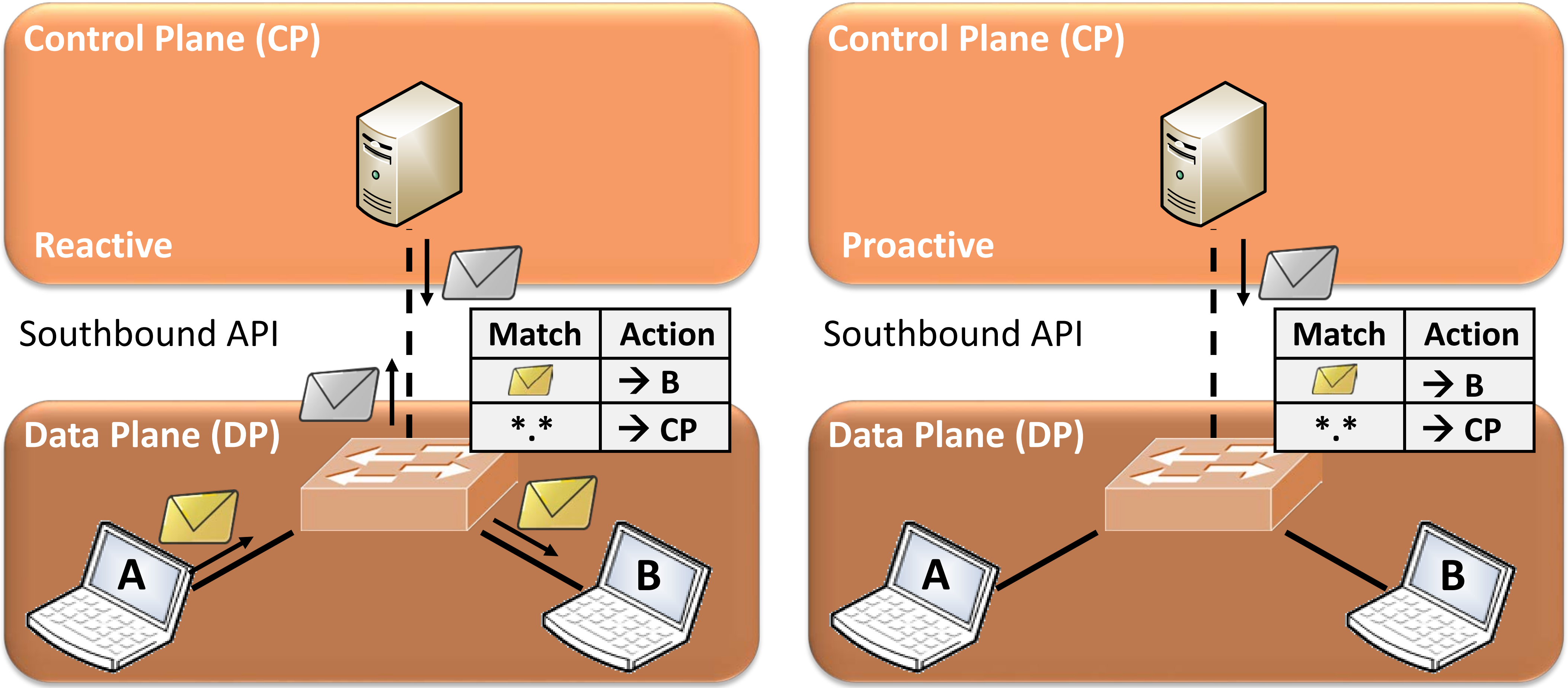
SDN Example


Control Plane (CP)
Reactive
Southbound API
Match
Action
→ B
.
→ CP
Data Plane (DP)
A
B
Control Plane (CP)
Proactive
Southbound API
Match
Action
.
→ CP
Data Plane (DP)
A
B

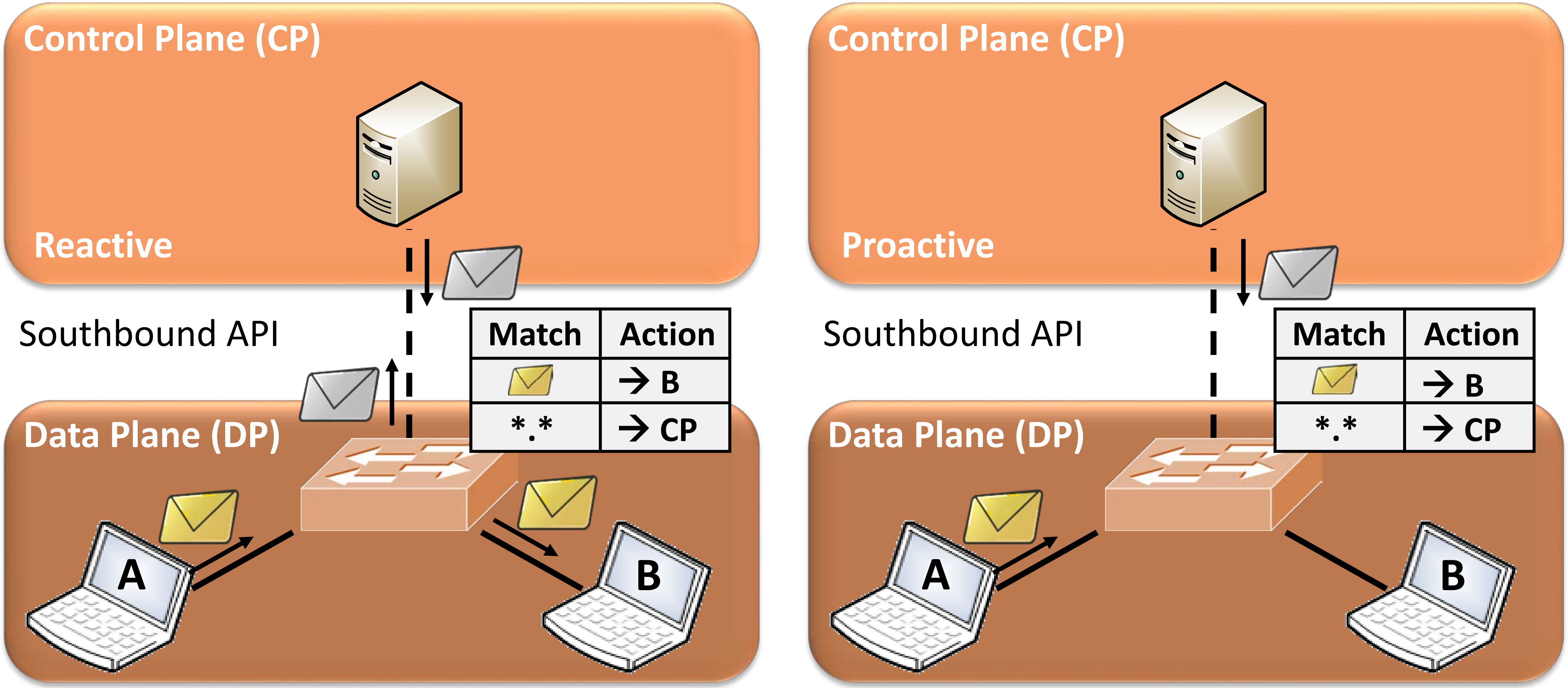
SDN Example


Control Plane (CP)
Reactive
Southbound API
Match | Action
→ B
. | → CP
Data Plane (DP)
A
B
Control Plane (CP)
Proactive
Southbound API
Match | Action
. | → CP
Data Plane (DP)
A
B

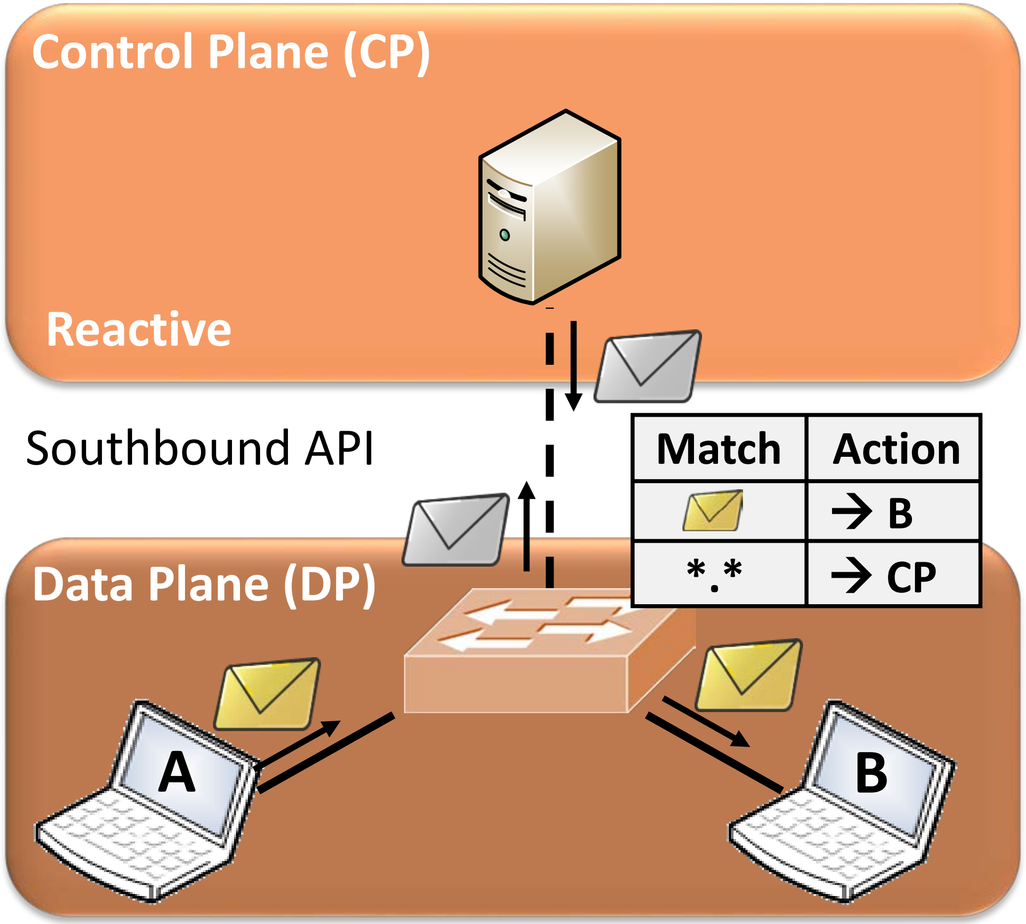
SDN Example


Control Plane (CP)
Reactive
Southbound API
Match
Action
→ B
.
→ CP
Data Plane (DP)
A
B
Control Plane (CP)
Proactive
Southbound API
Match
Action
→ B
.
→ CP
Data Plane (DP)
A
B

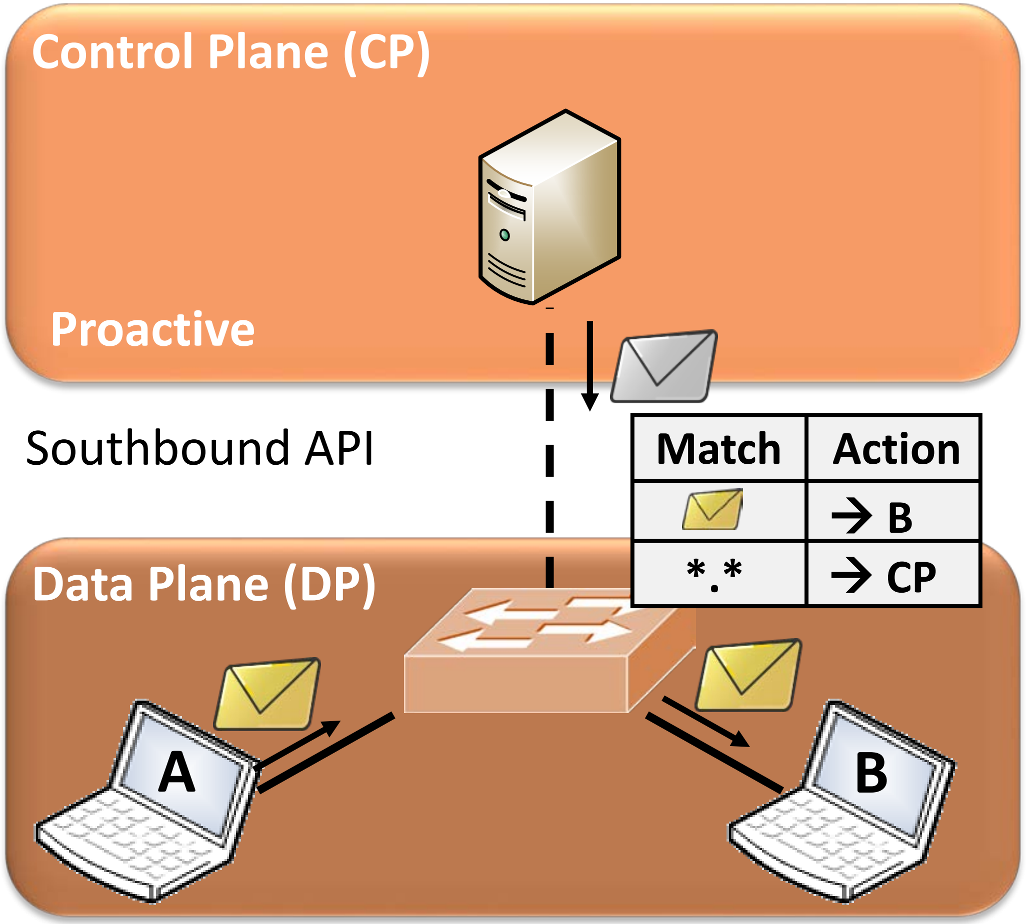
SDN Example


Control Plane (CP)
Reactive
Southbound API
Match
Action
→ B
.
→ CP
Data Plane (DP)
A
B
Control Plane (CP)
Proactive
Southbound API
Match
Action
→ B
.
→ CP
Data Plane (DP)
A
B

SDN Example

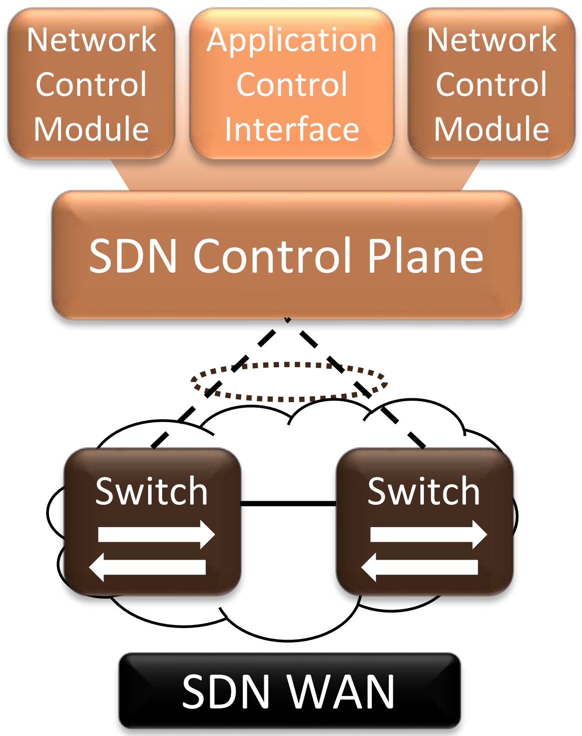


Control Plane (CP)
Reactive
Southbound API
Match
Action
→ B
.
→ CP
Data Plane (DP)
A
B

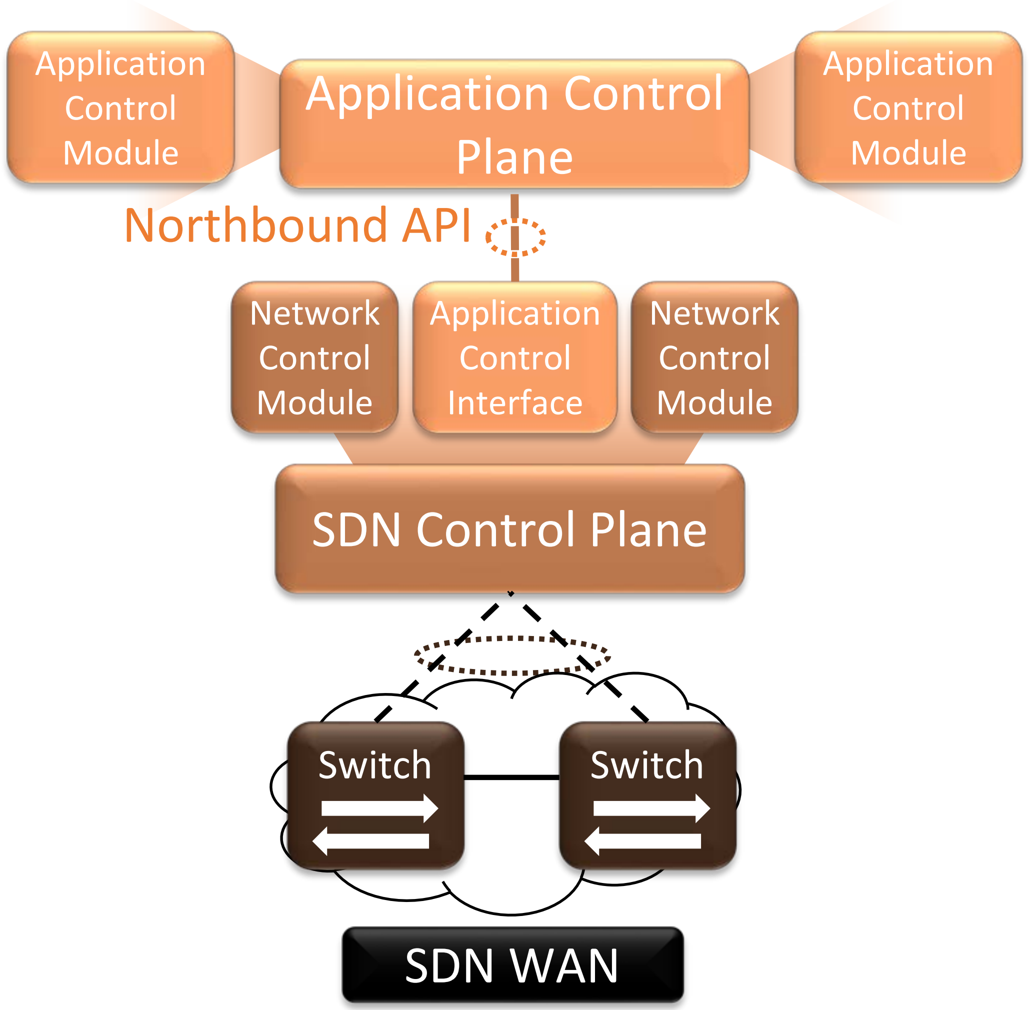


Control Plane (CP)
Proactive
Southbound API
Match
Action
→ B
.
→ CP
Data Plane (DP)
A
B

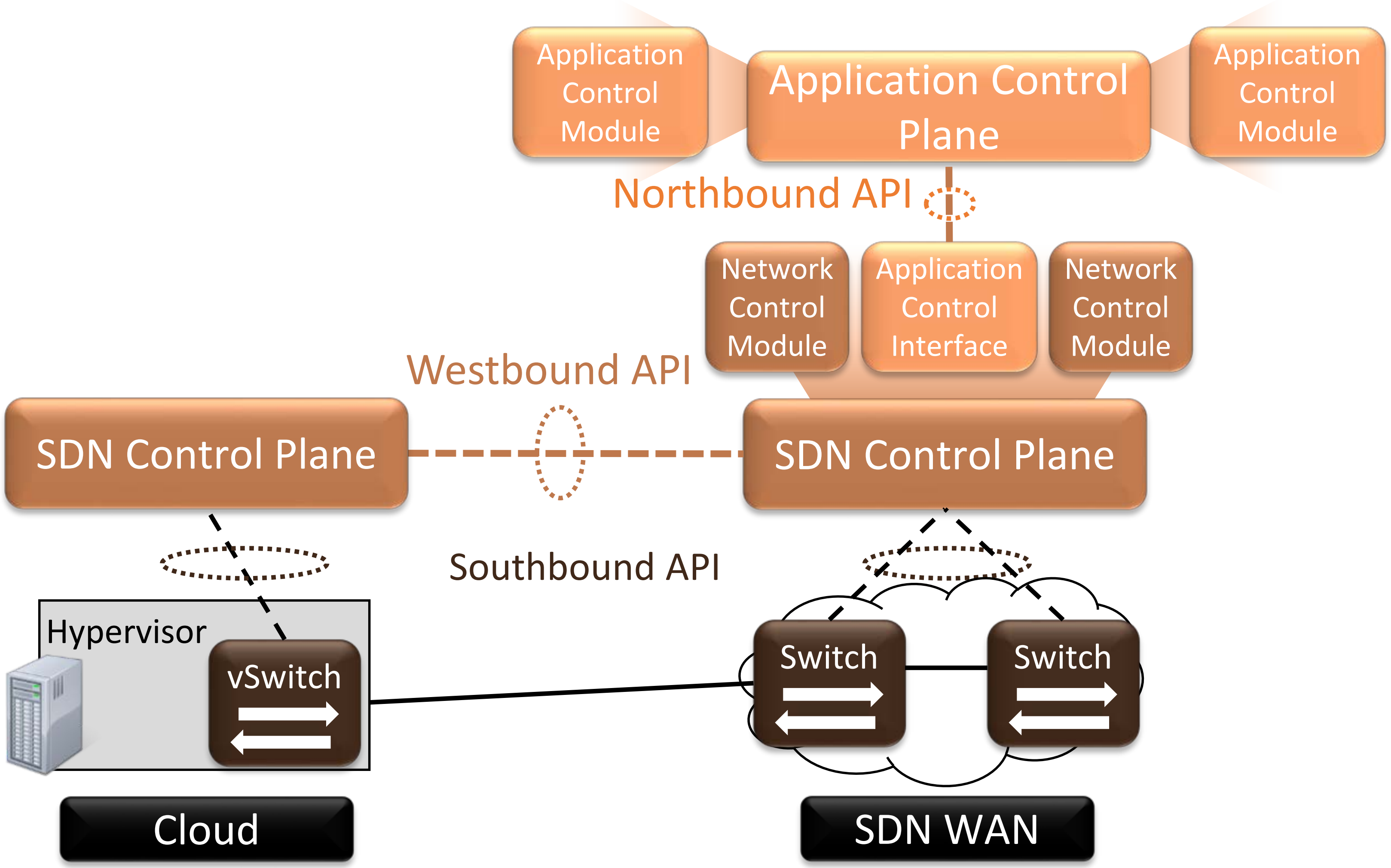
SDN Ecosystem



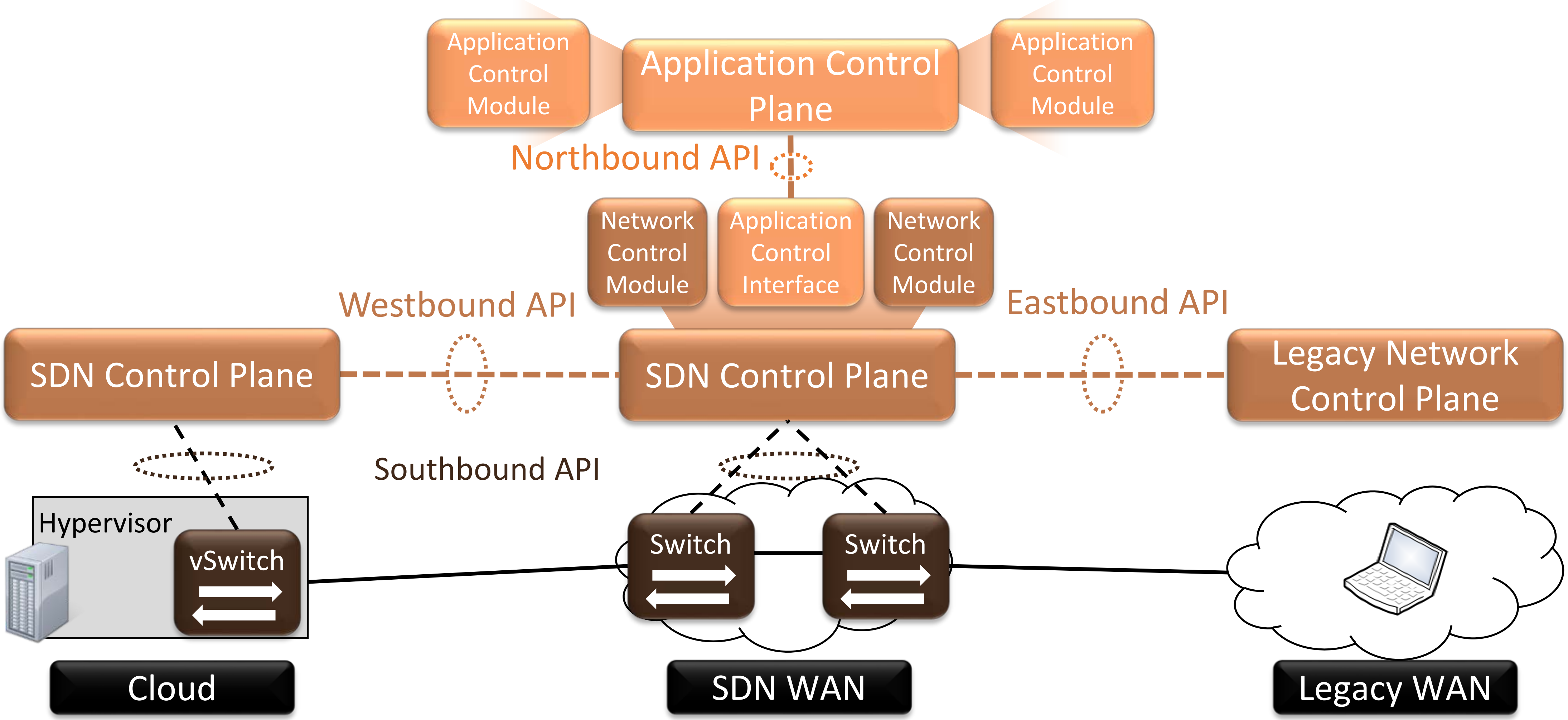
SDN Ecosystem



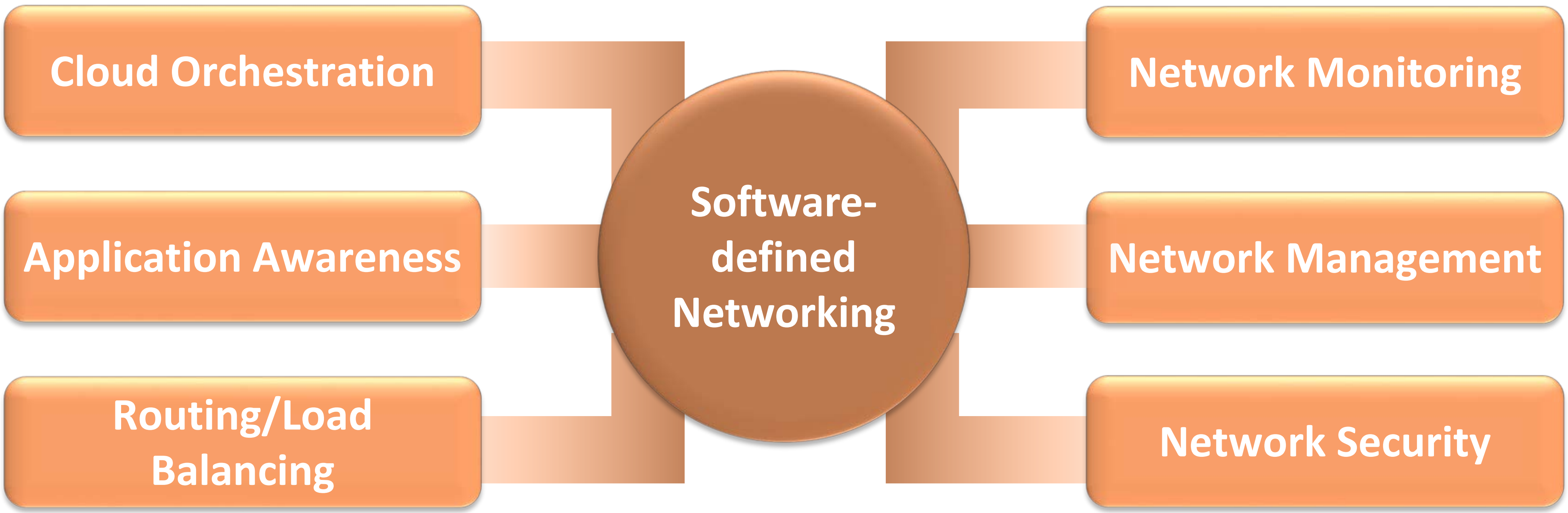
SDN Ecosystem



SDN Ecosystem

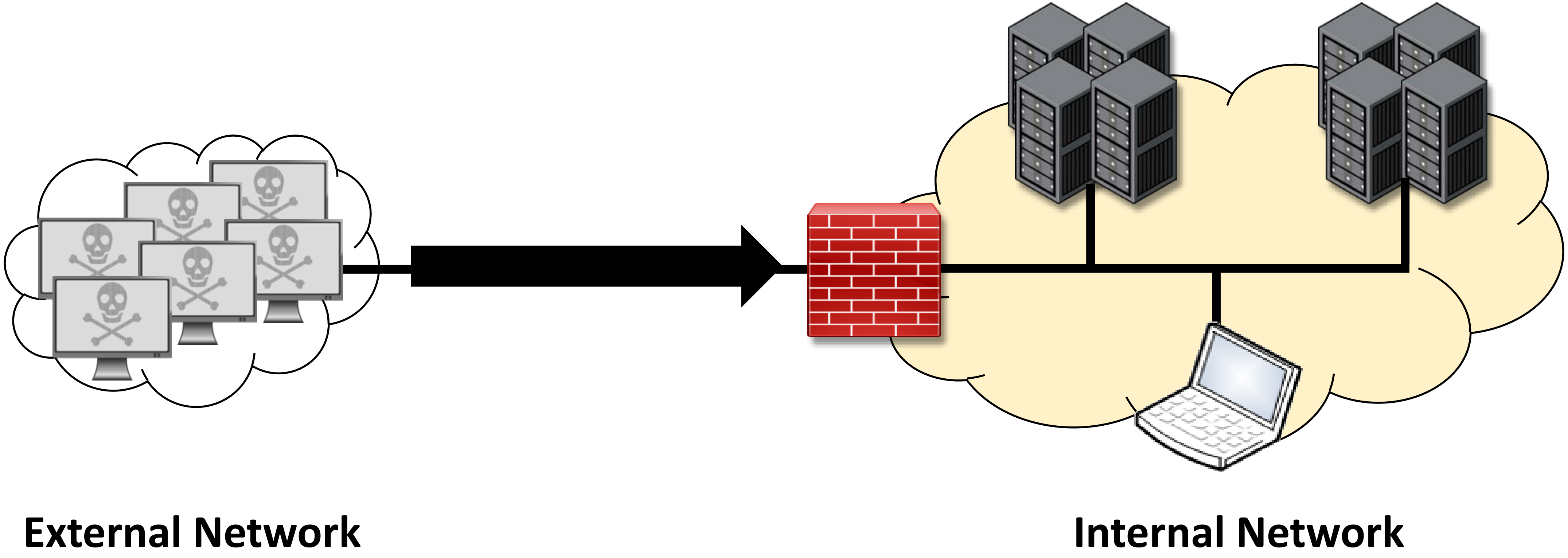


SDN Use Cases

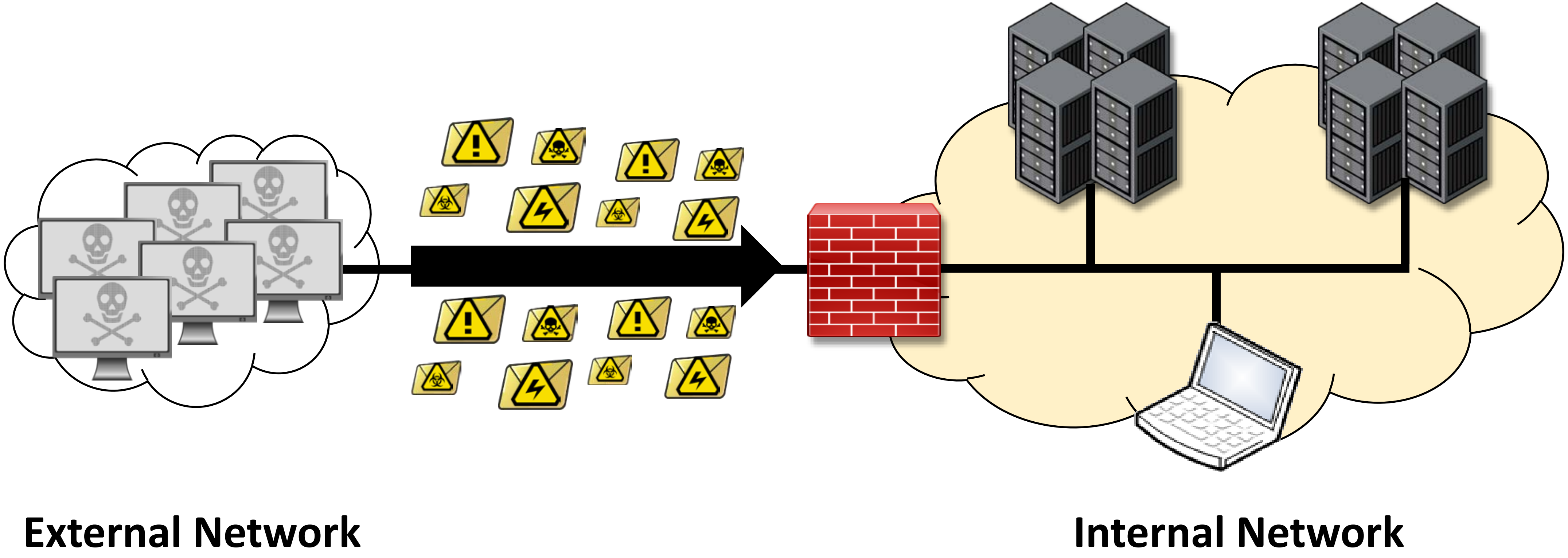


SDN Use Cases

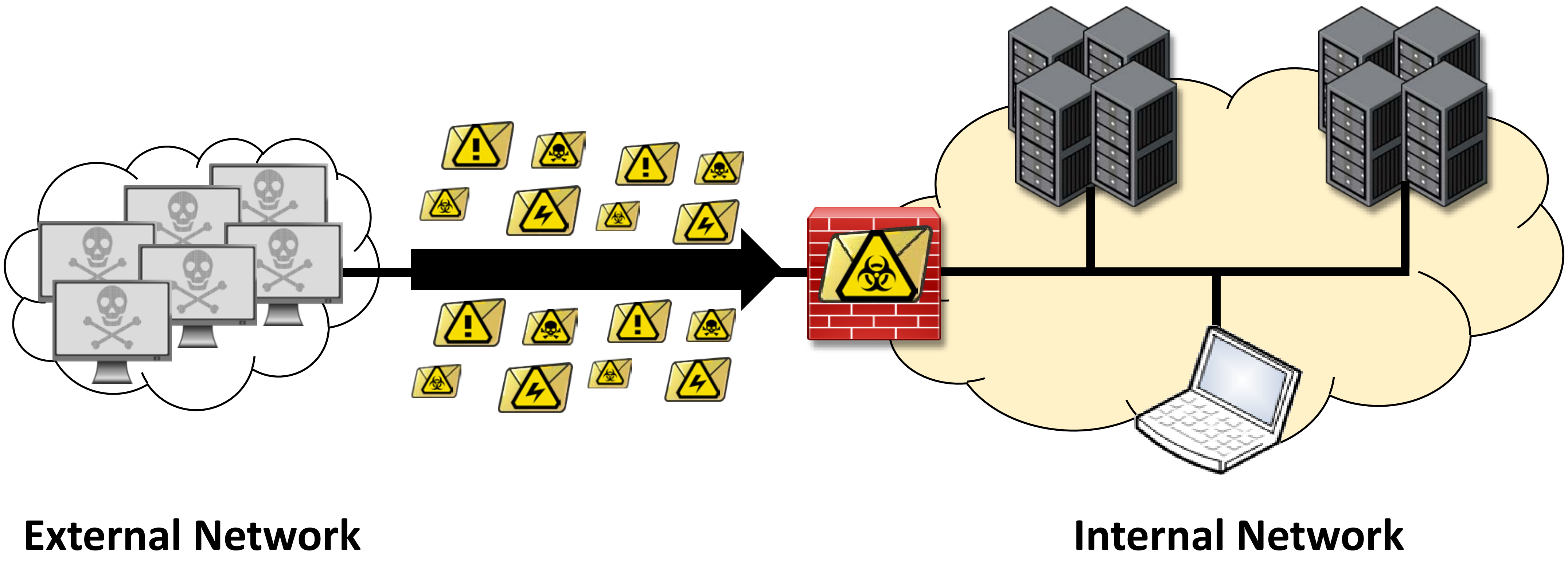
Can we enhance network security with SDN?



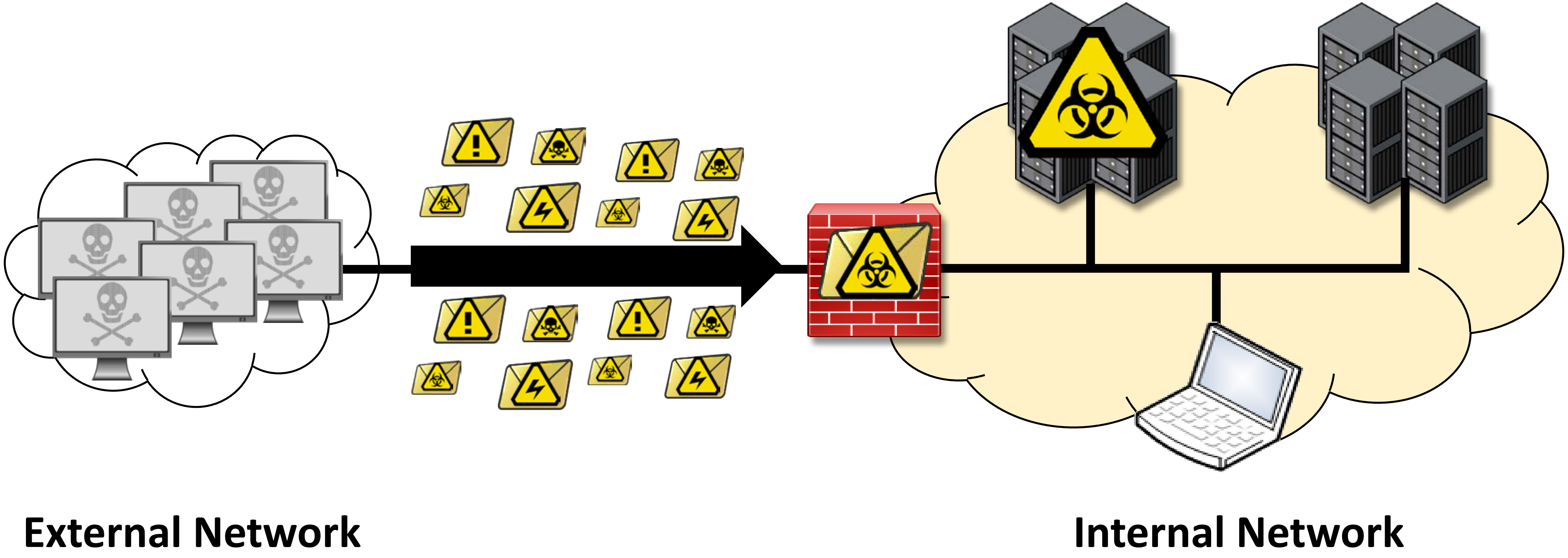
Can we enhance network security with SDN?



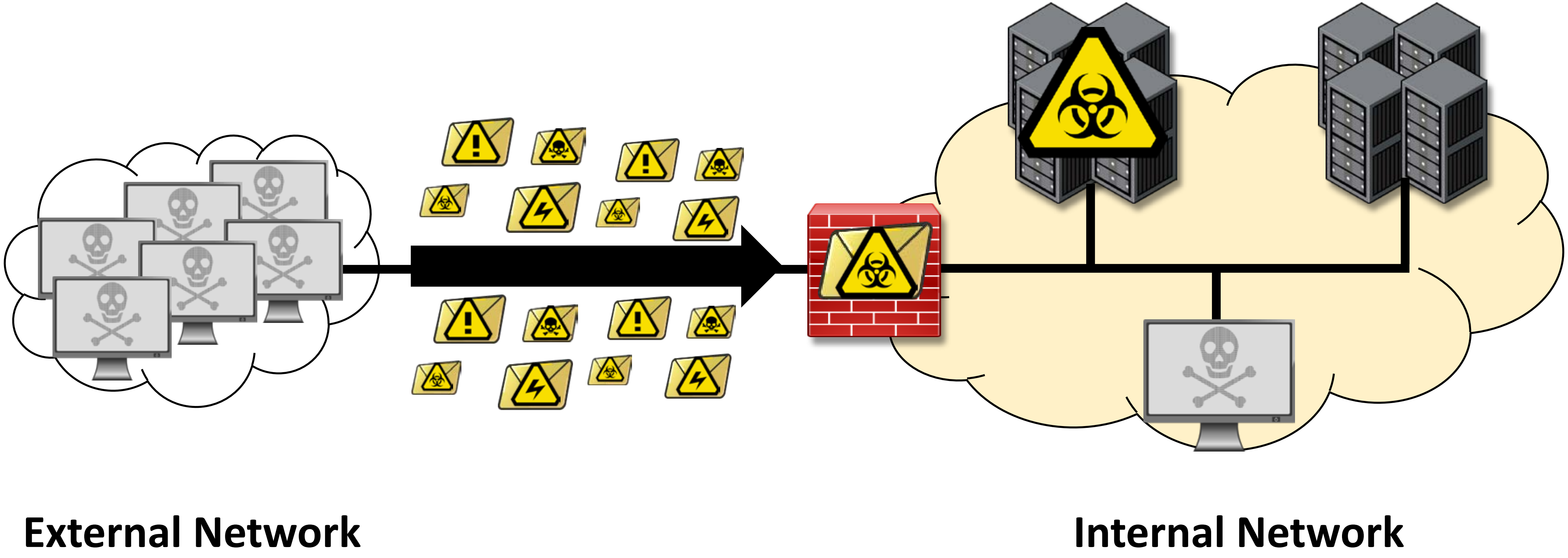
Can we enhance network security with SDN?



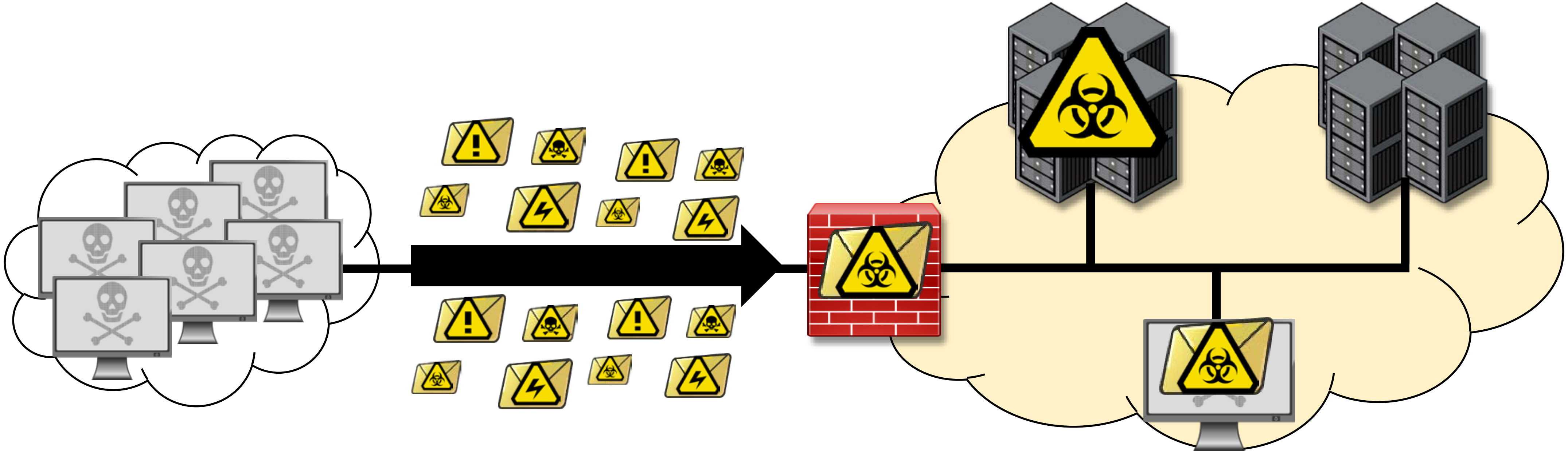
Can we enhance network security with SDN?



Can we enhance network security with SDN?



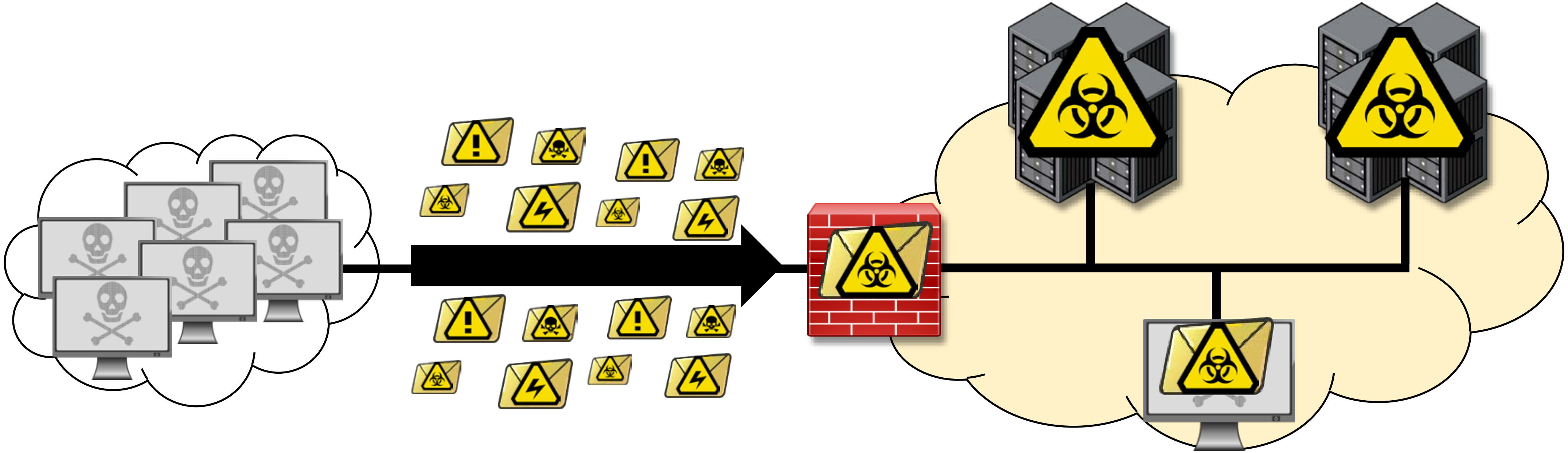
Can we enhance network security with SDN?



External Network

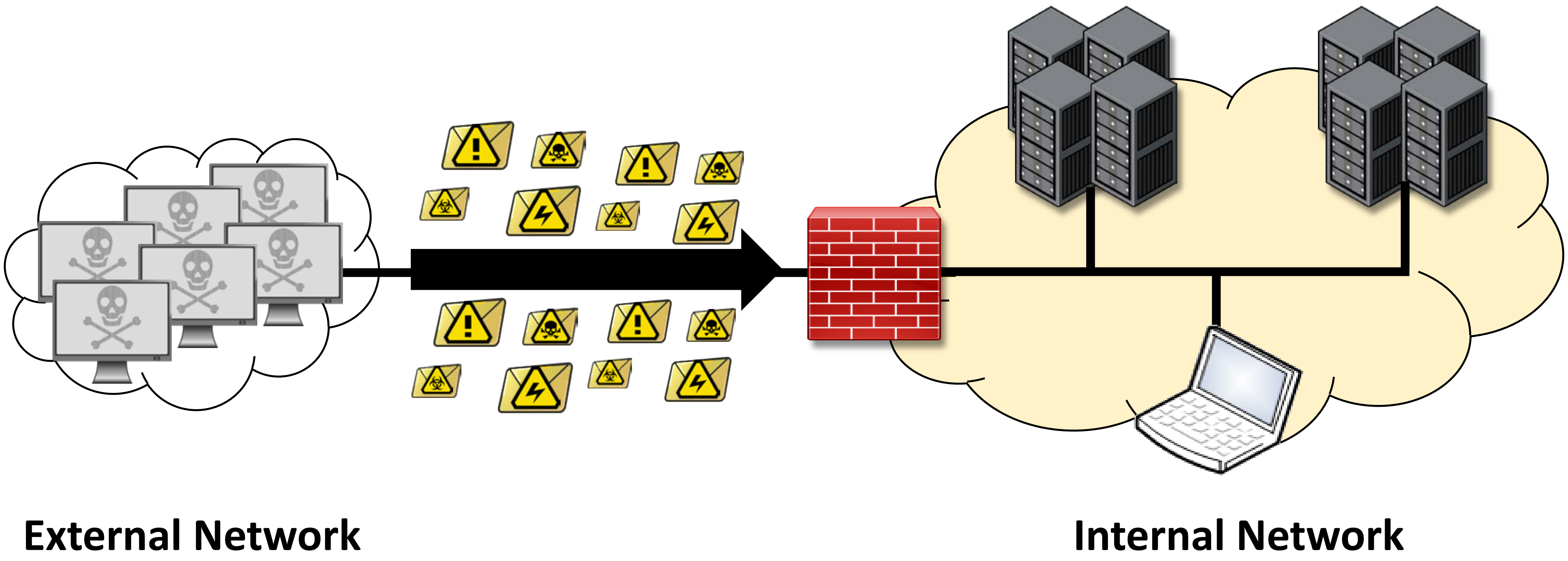
Internal Network

Can we enhance network security with SDN?

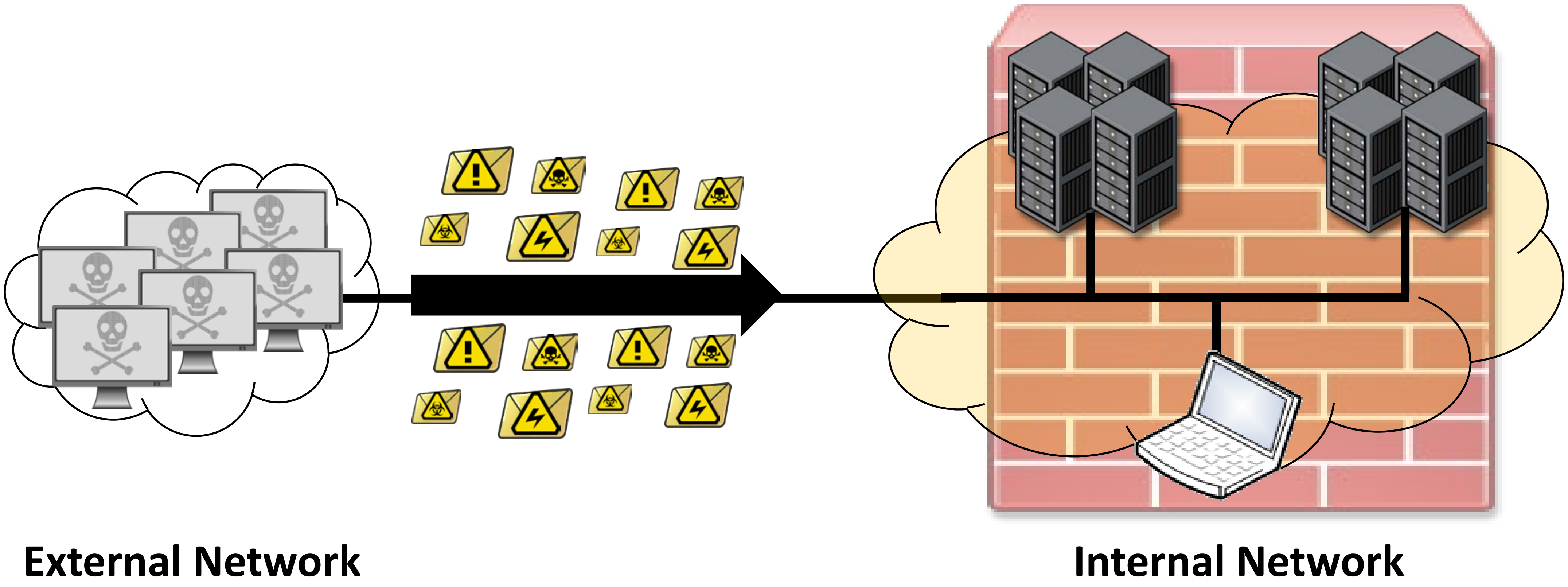


External Network **Internal Network**

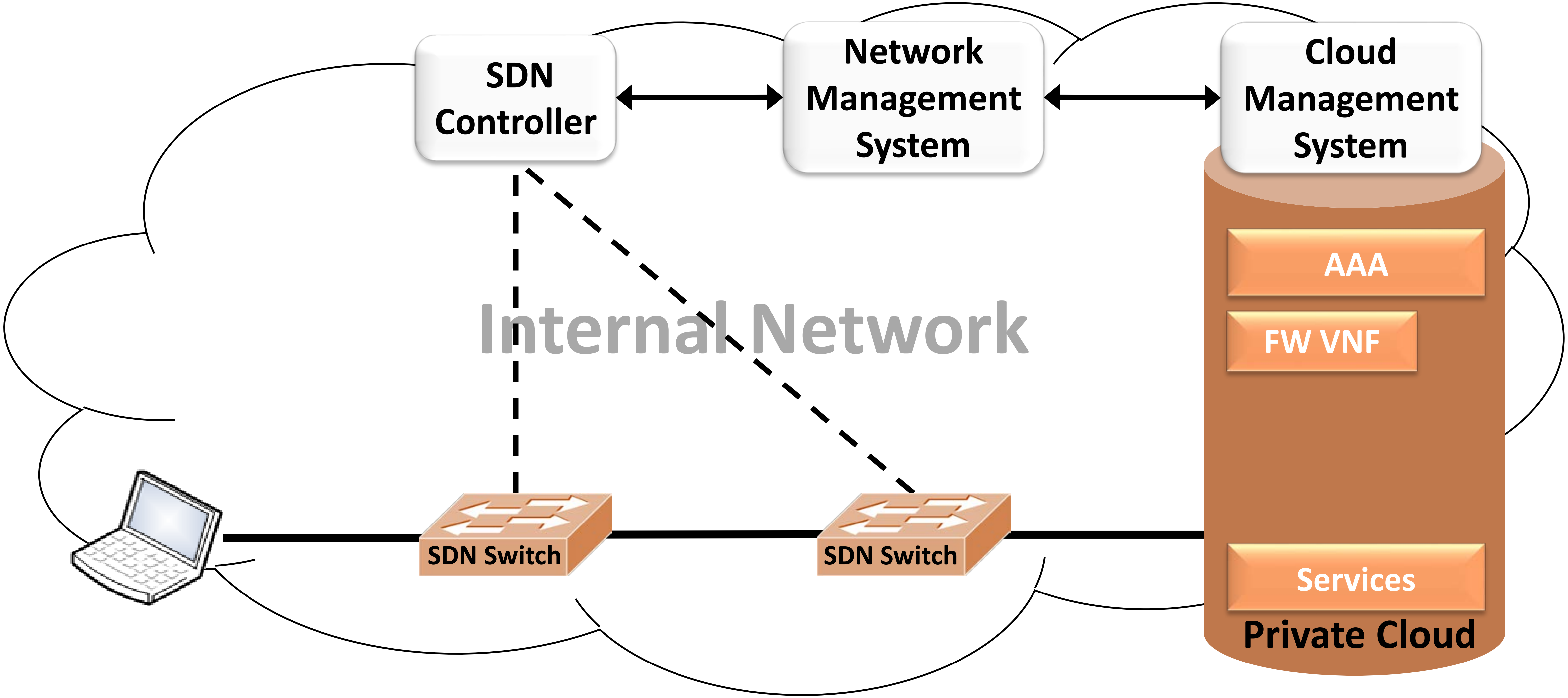
Can we enhance network security with SDN?



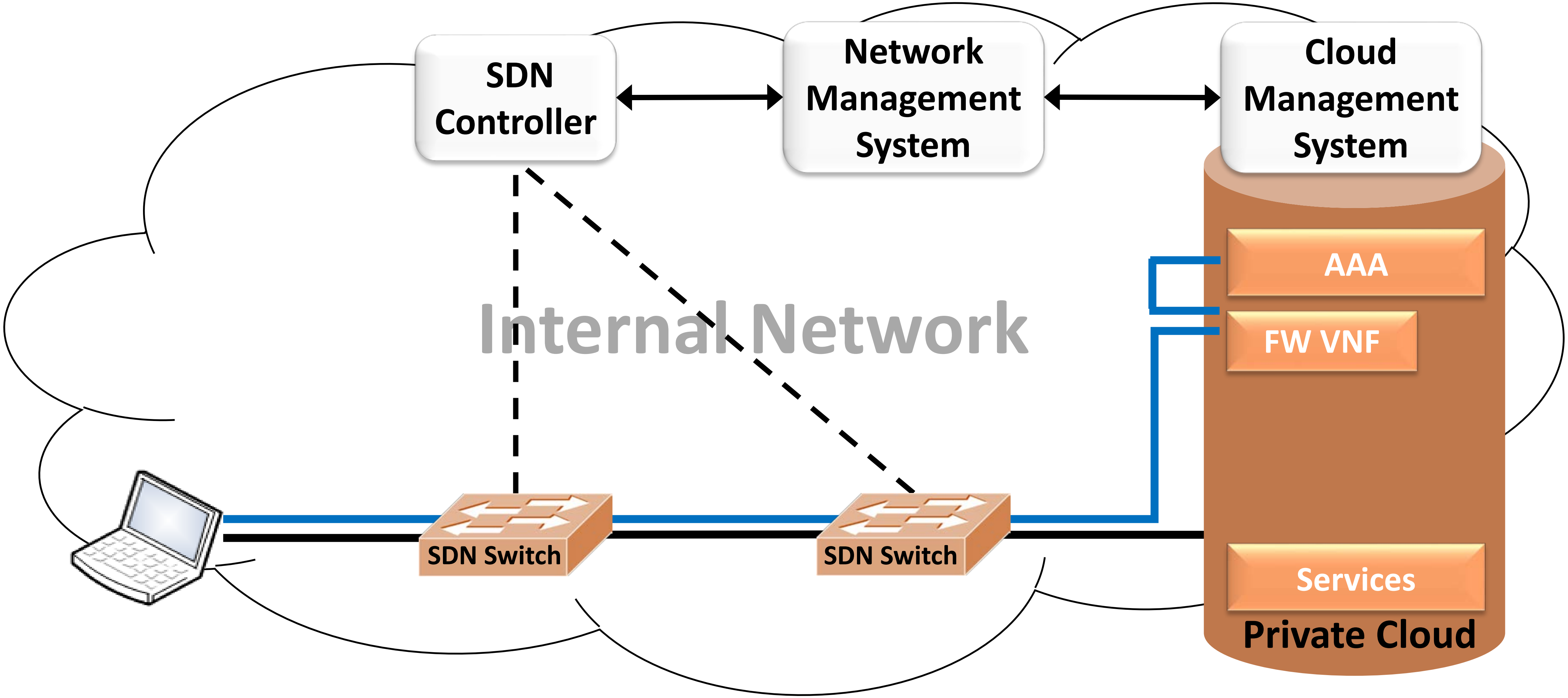
Can we enhance network security with SDN?



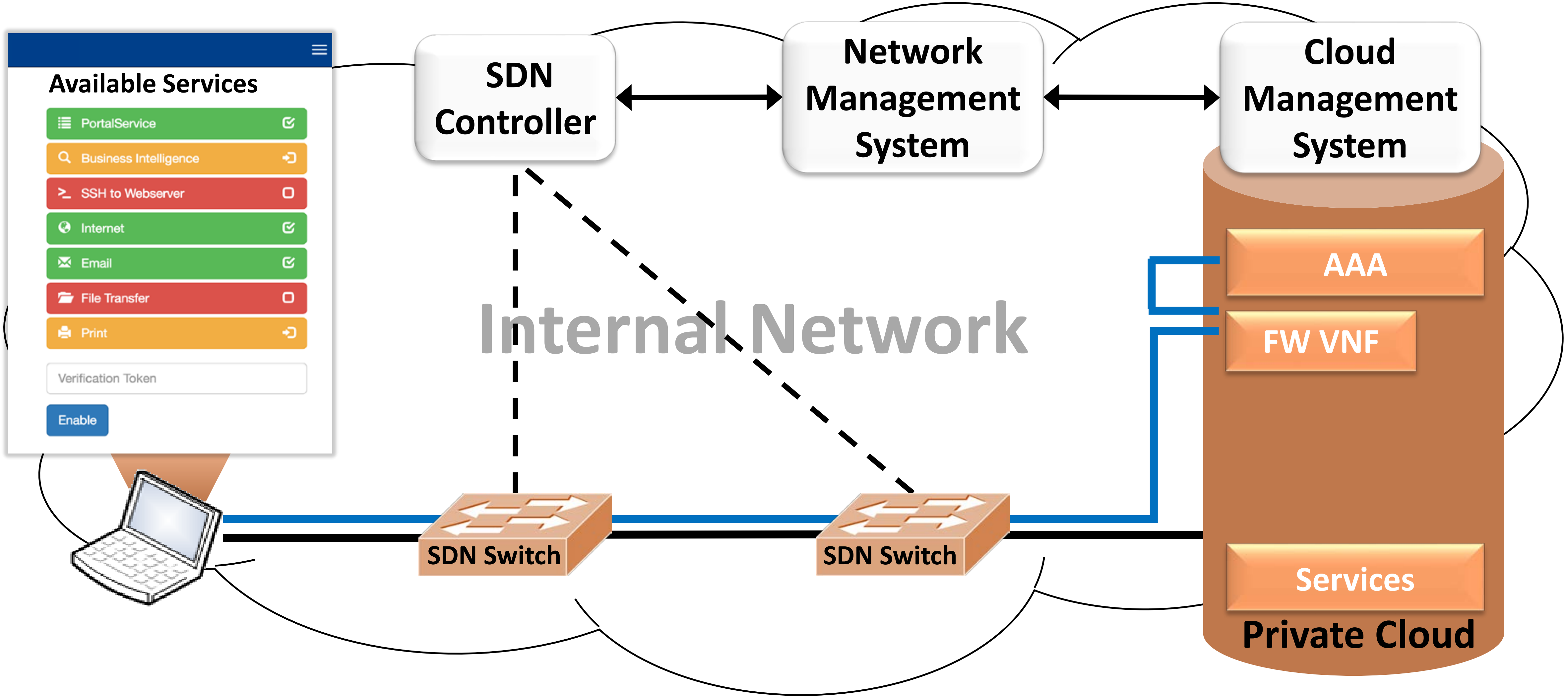
SDN Omni-Present Firewall



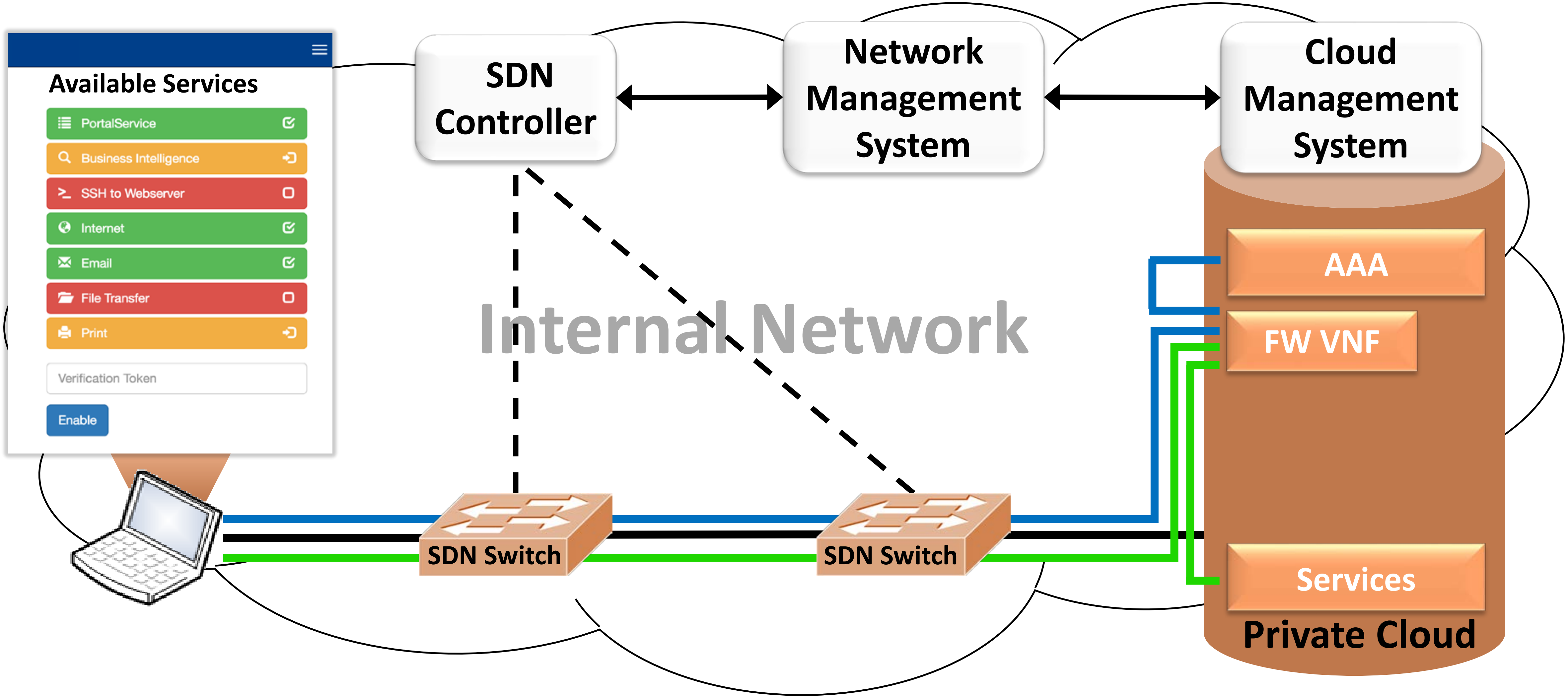
SDN Omni-Present Firewall



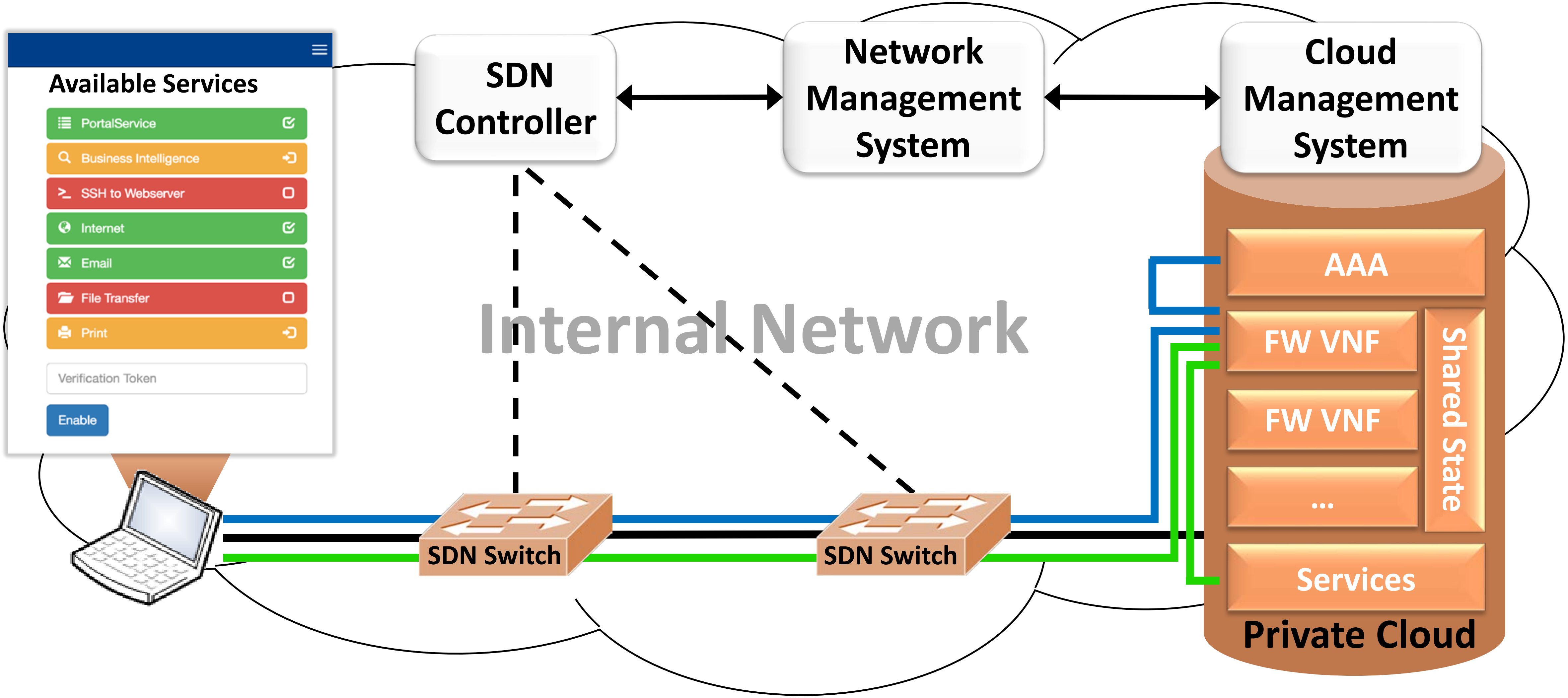
SDN Omni-Present Firewall



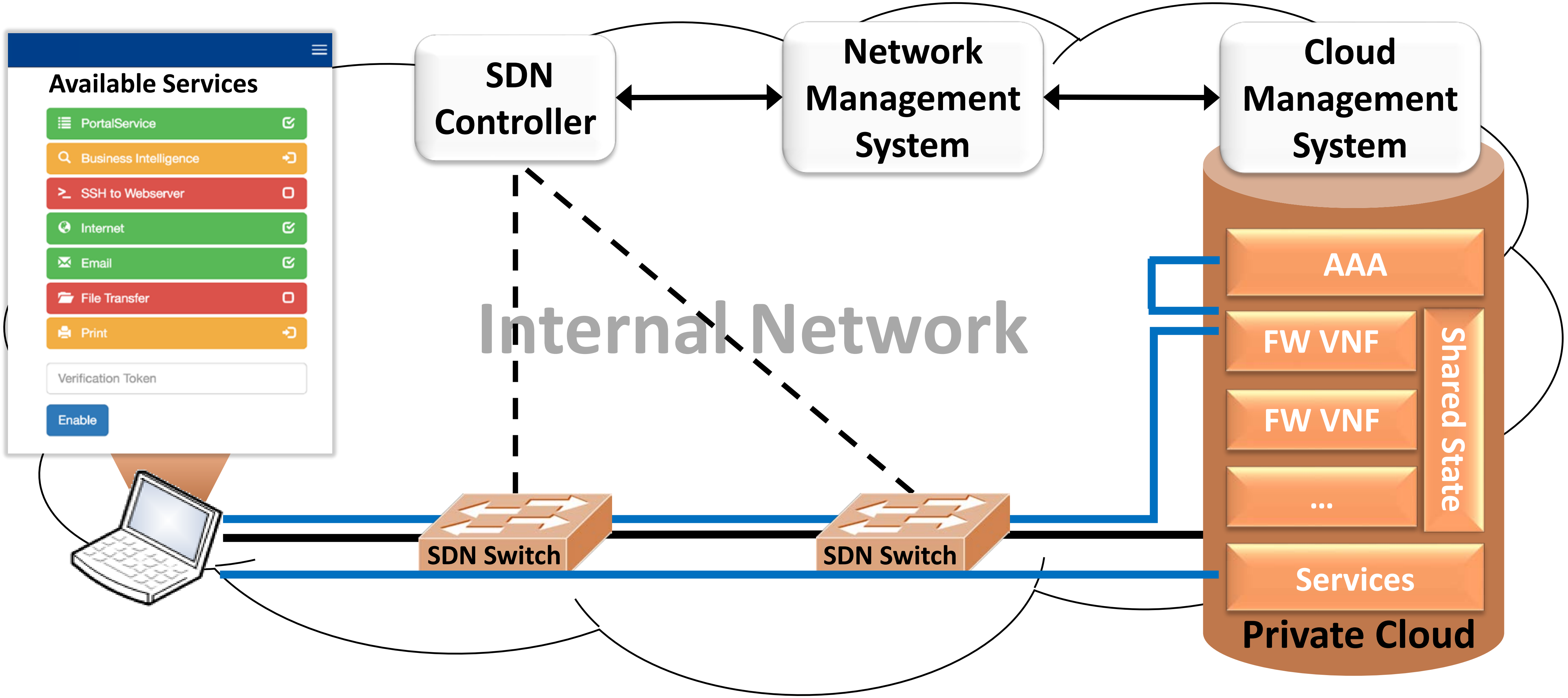
SDN Omni-Present Firewall



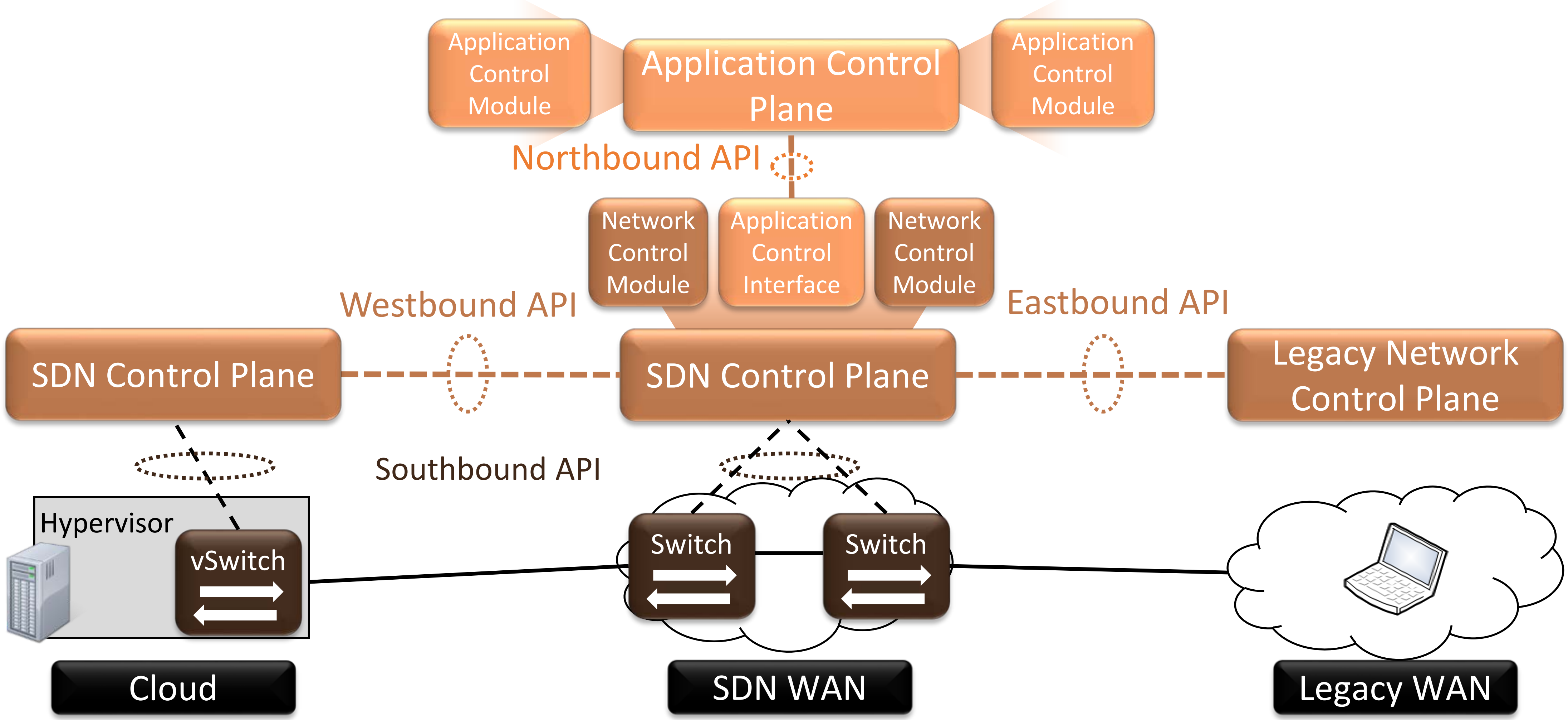
SDN Omni-Present Firewall



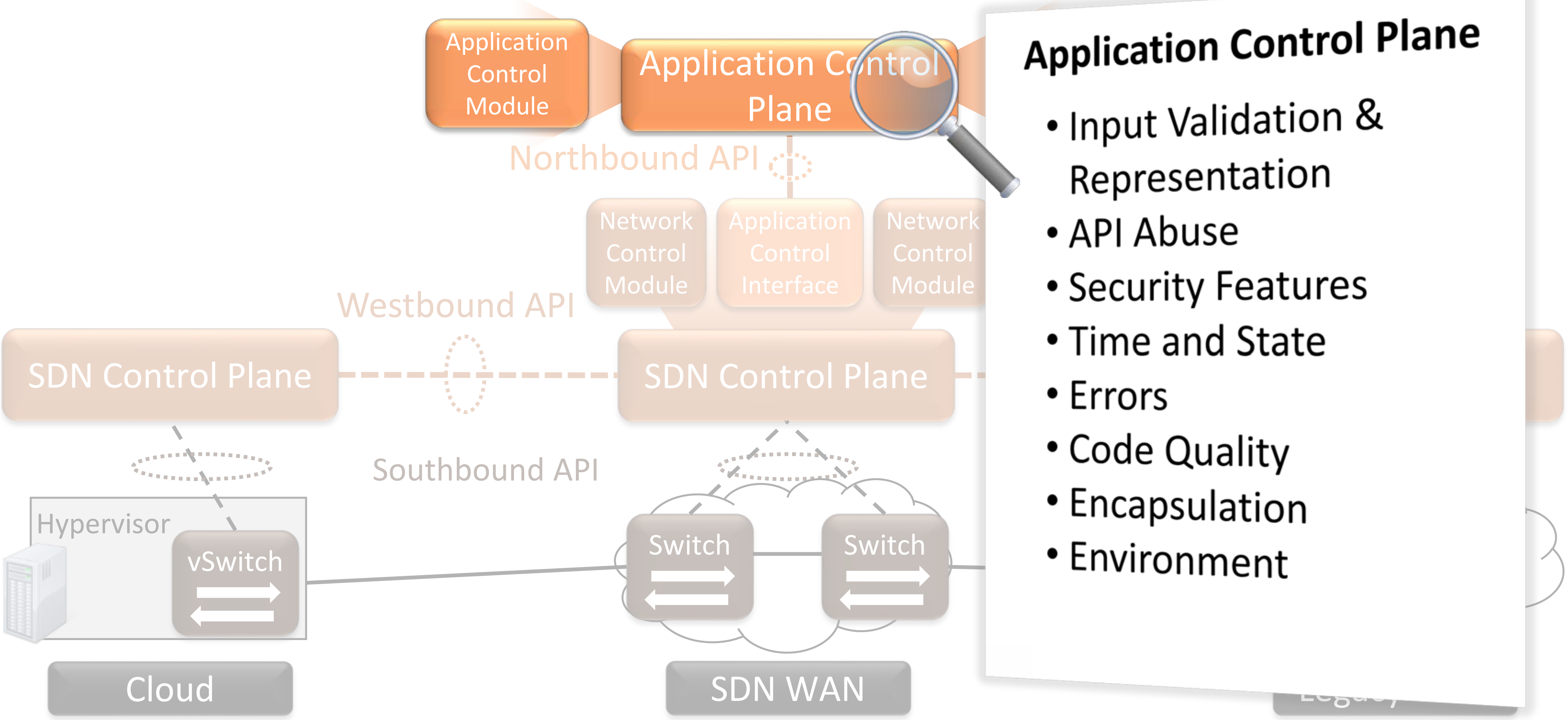
SDN Omni-Present Firewall



SDN Attack Surface



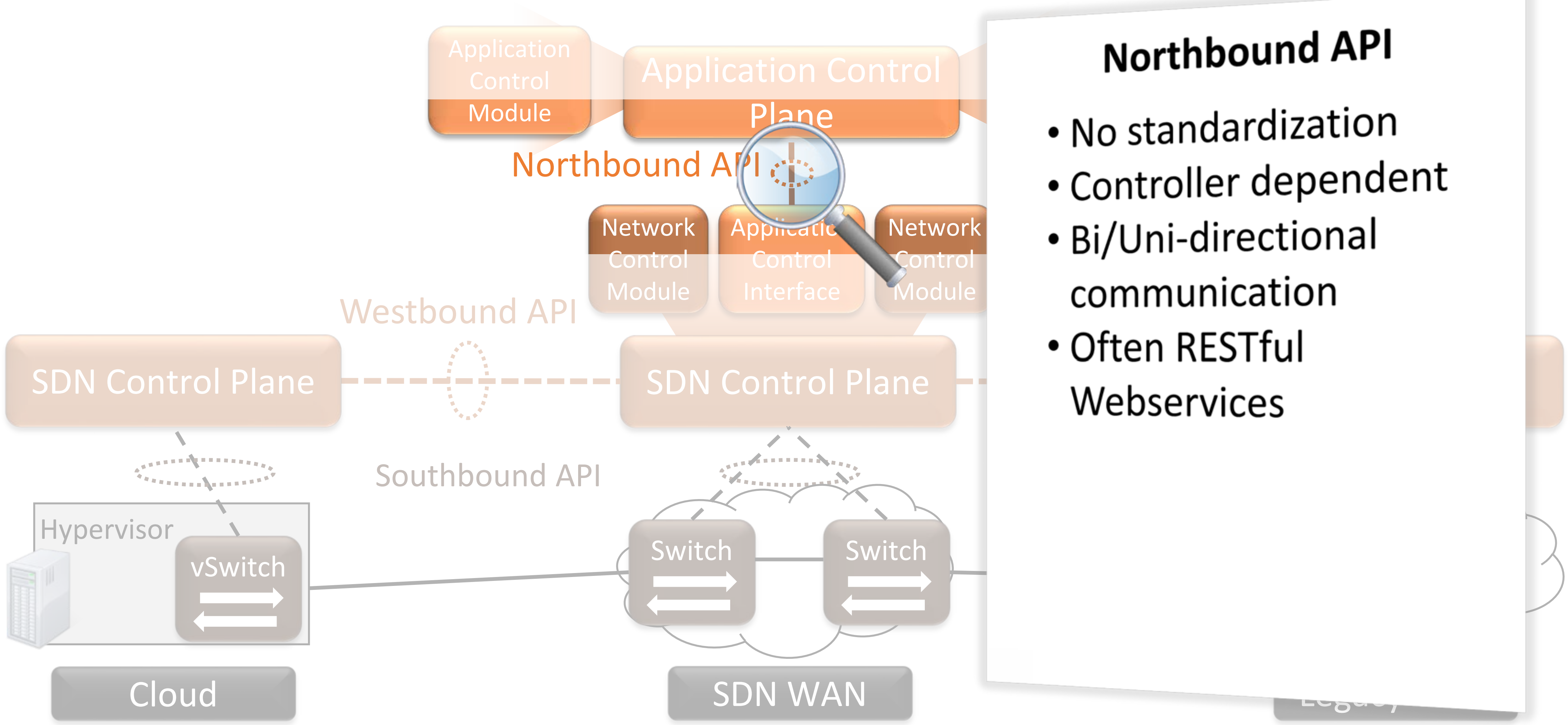
SDN Attack Surface



Application Control Plane

- Input Validation & Representation
- API Abuse
- Security Features
- Time and State
- Errors
- Code Quality
- Encapsulation
- Environment

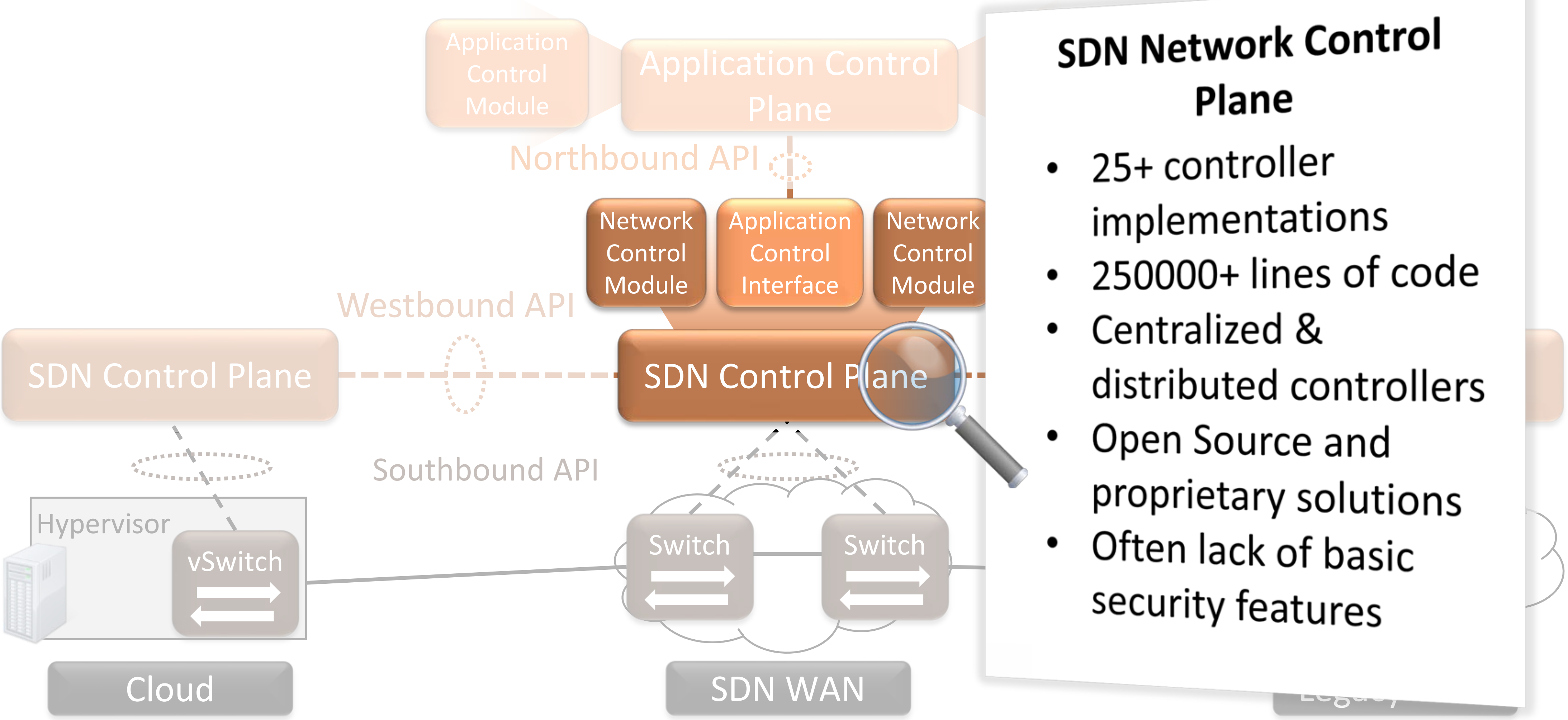
SDN Attack Surface



Northbound API

- No standardization
- Controller dependent
- Bi/Uni-directional communication
- Often RESTful Webservices

SDN Attack Surface



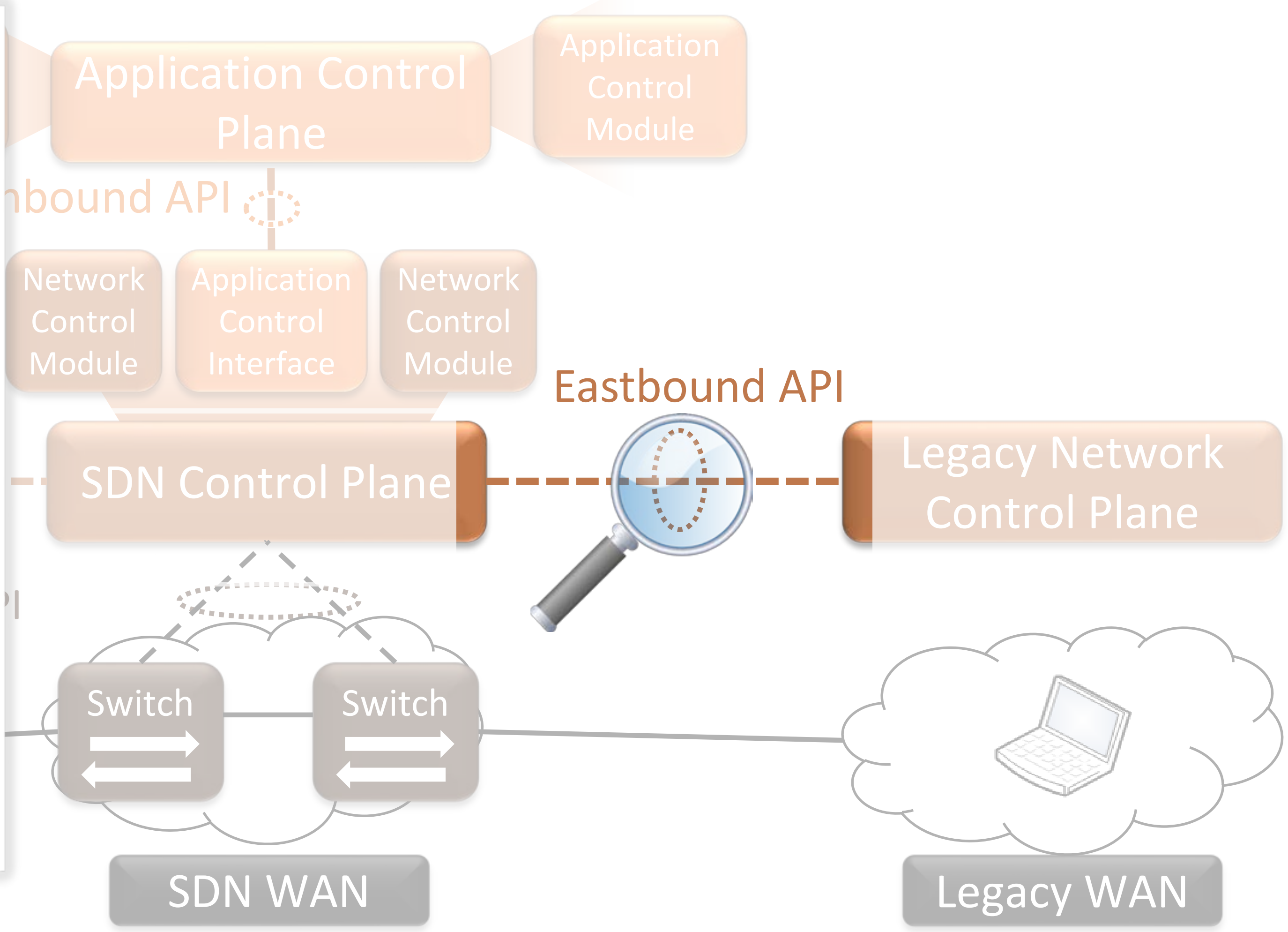
SDN Network Control Plane

- 25+ controller implementations
- 250000+ lines of code
- Centralized & distributed controllers
- Open Source and proprietary solutions
- Often lack of basic security features

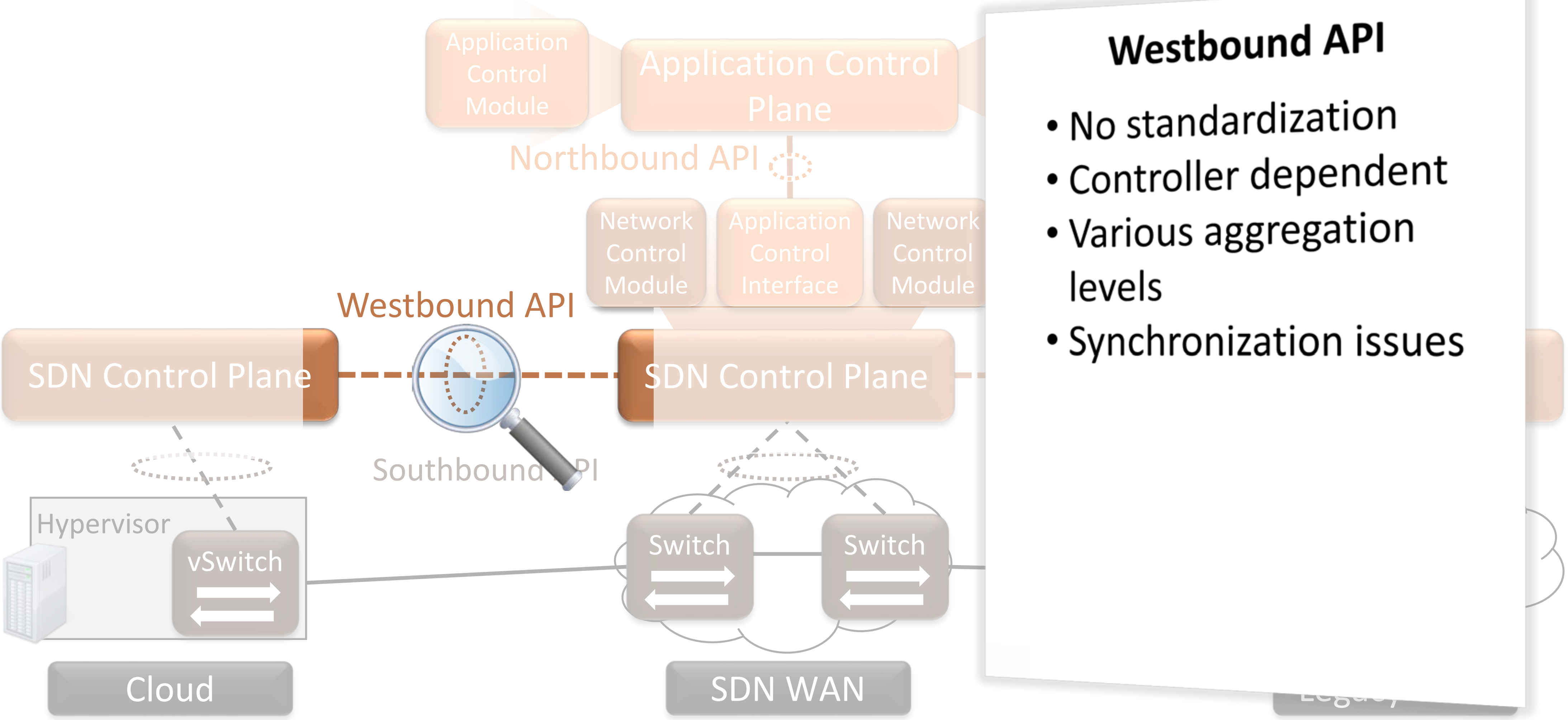
SDN Attack Surface

Eastbound API

- No standardization
- Flexible vs. static nature of devices
- Synchronization issues
- Integration challenges



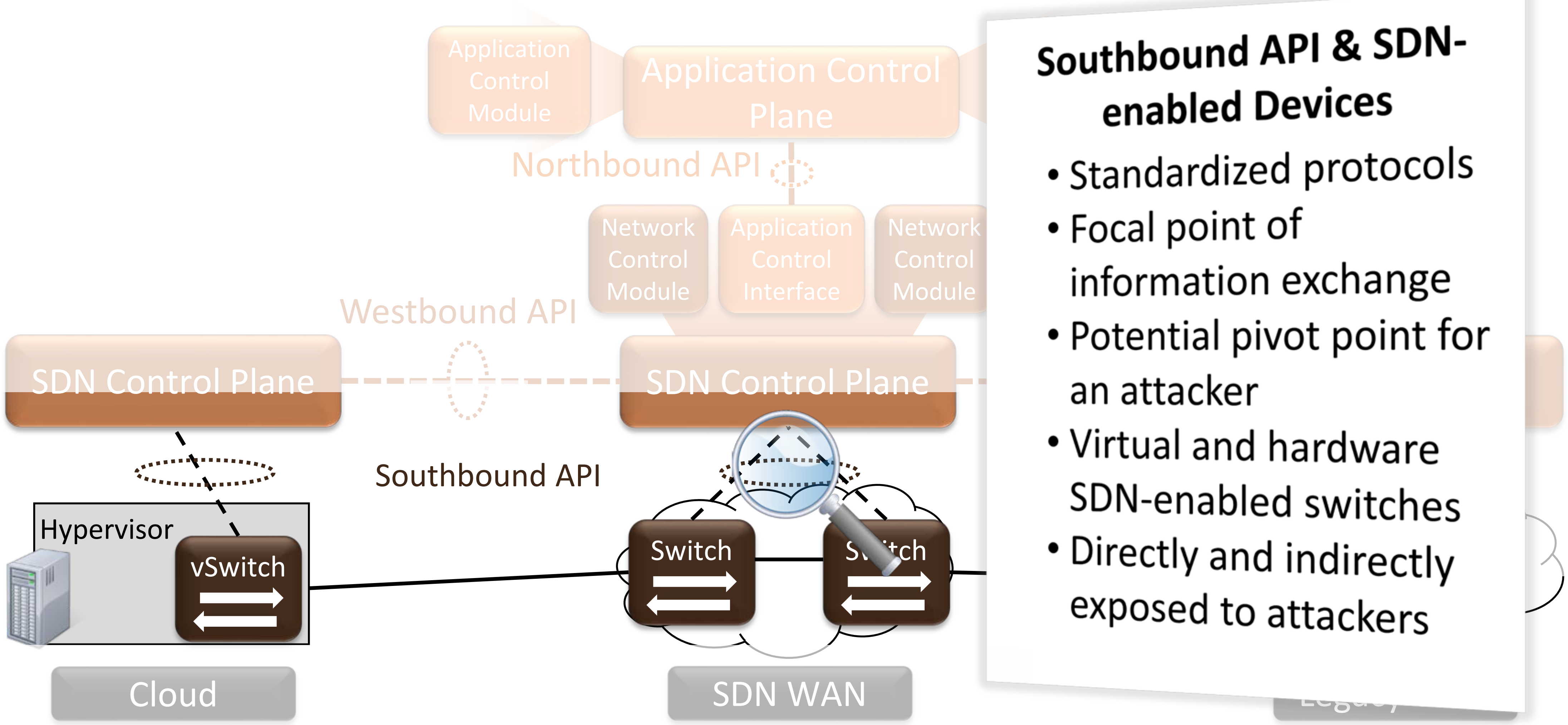
SDN Attack Surface



Westbound API

- No standardization
- Controller dependent
- Various aggregation levels
- Synchronization issues

SDN Attack Surface



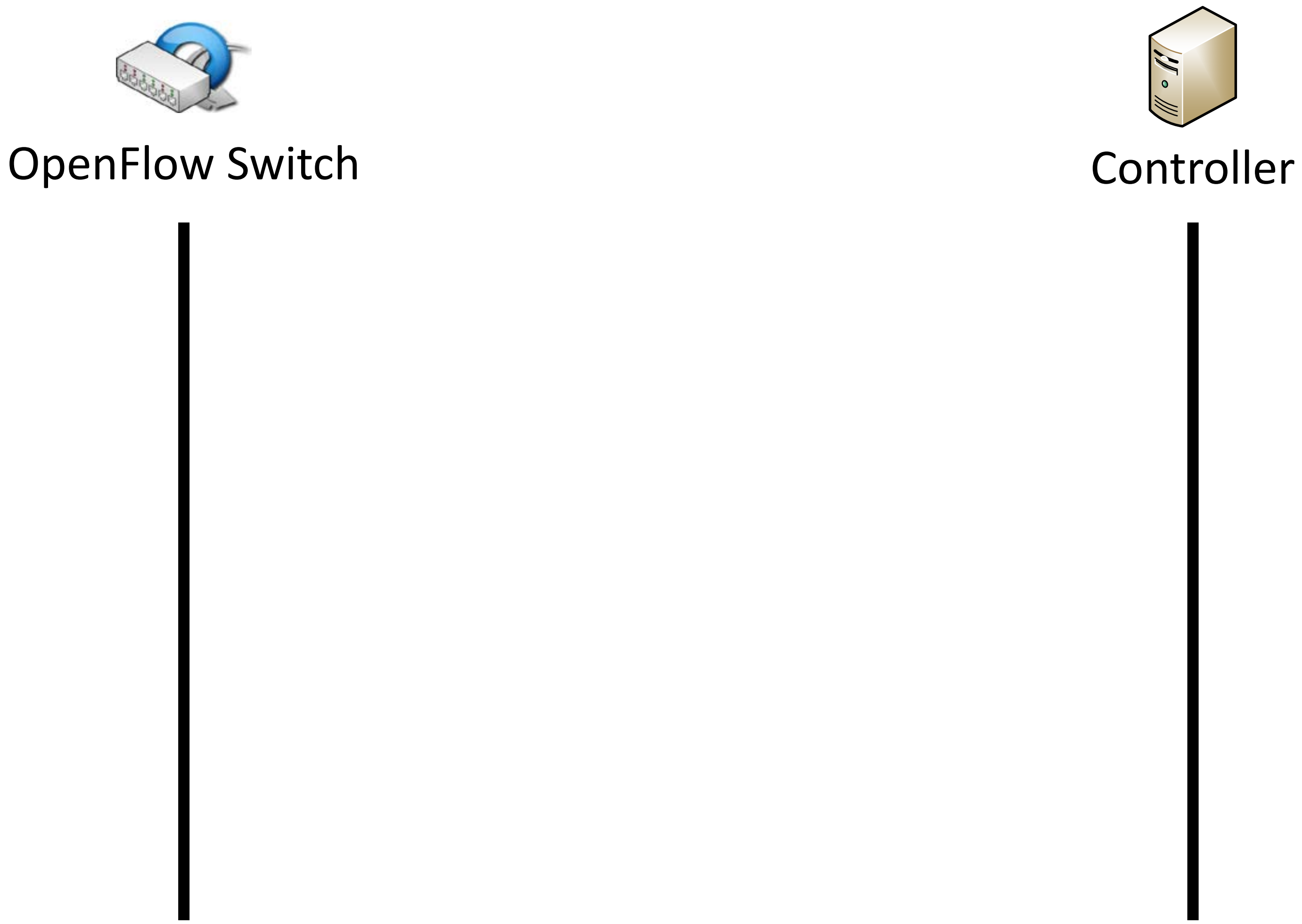
Southbound API & SDN-enabled Devices

- Standardized protocols
- Focal point of information exchange
- Potential pivot point for an attacker
- Virtual and hardware SDN-enabled switches
- Directly and indirectly exposed to attackers

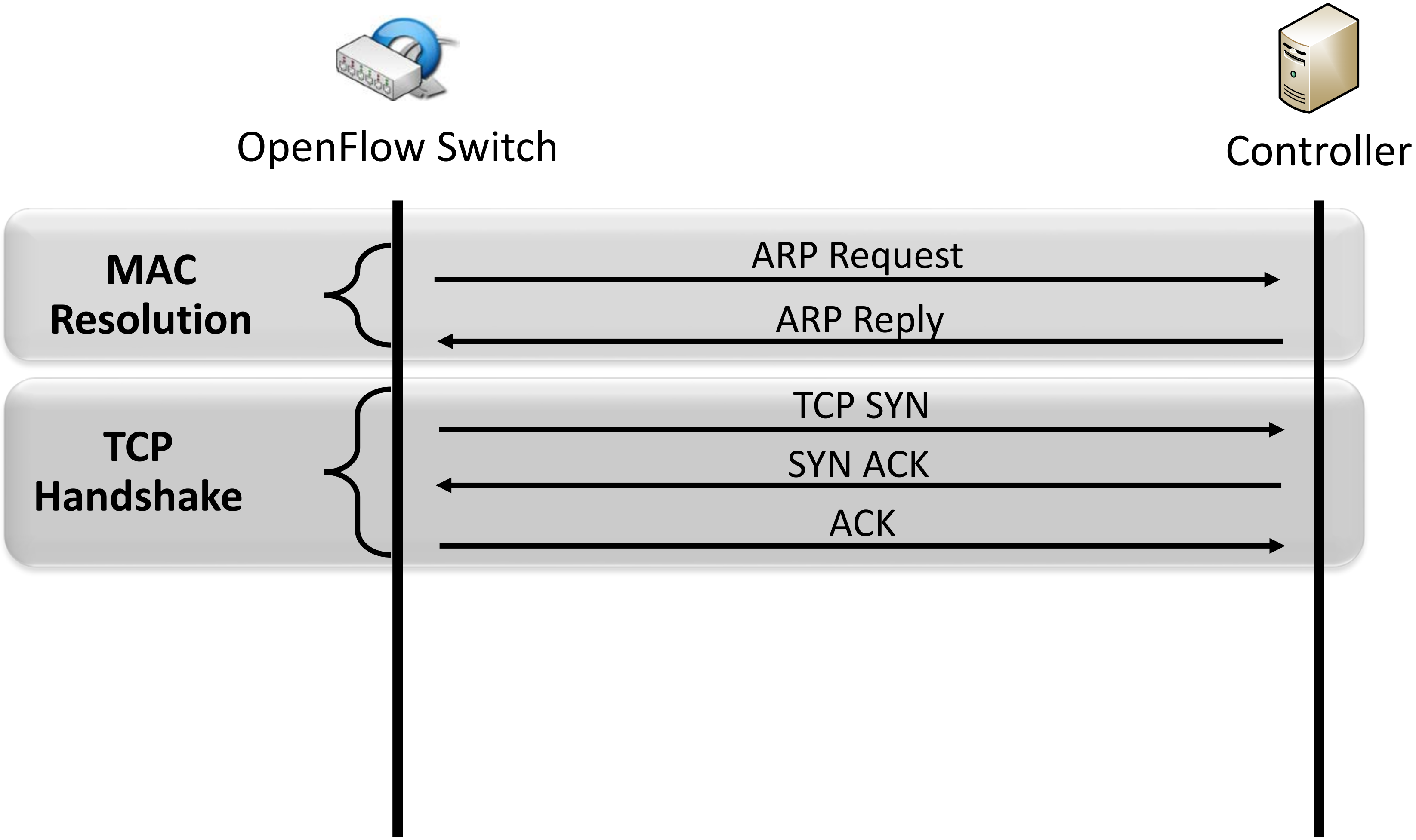
OpenFlow

- De-facto standard Southbound API protocol
- Maintained by the Open Networking Foundation
- First release in December 2009
- Most current version 1.5.1 (April 2015)
- Supported by 120+ industrial members

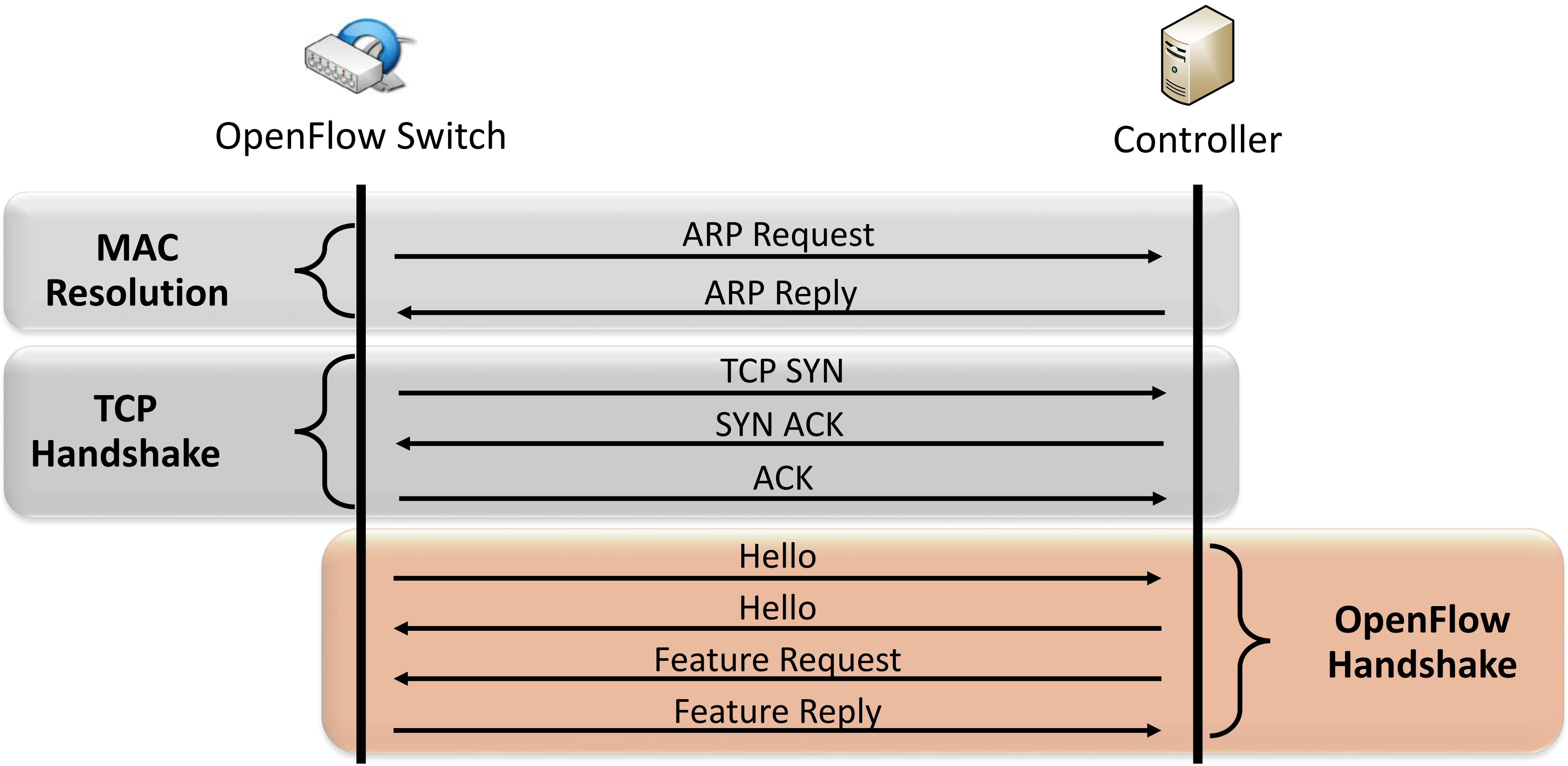
OpenFlow – Channel Initialization



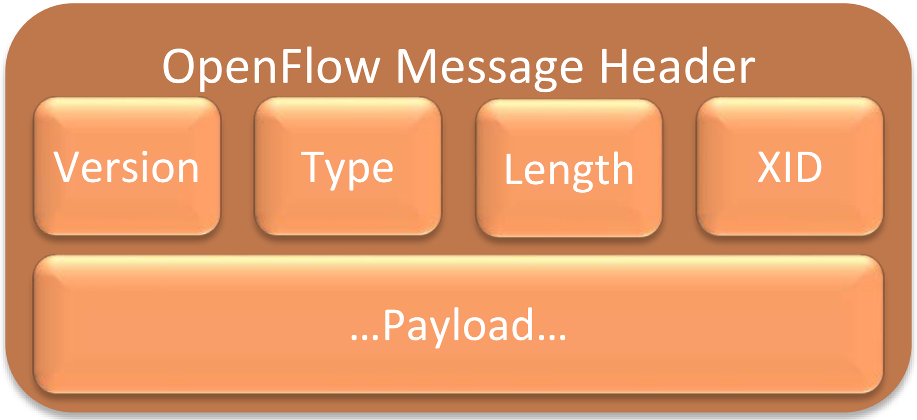
OpenFlow – Channel Initialization



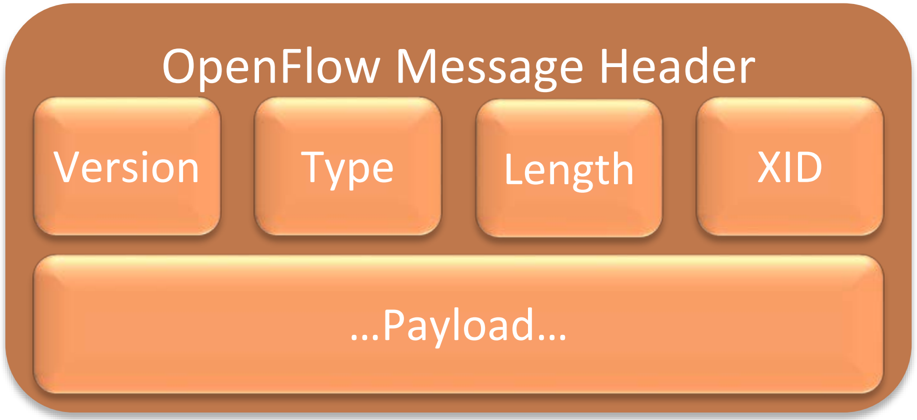
OpenFlow – Channel Initialization



OpenFlow – Message Structure & Types



OpenFlow – Message Structure & Types

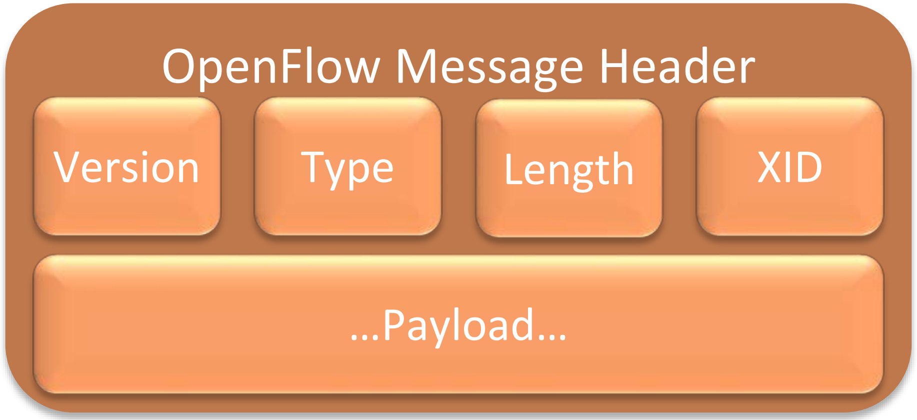


Asynchronous

Controller-to-Switch

Symmetric

OpenFlow – Message Structure & Types



Asynchronous

Packet-In
Flow Removed
Port Status
Error

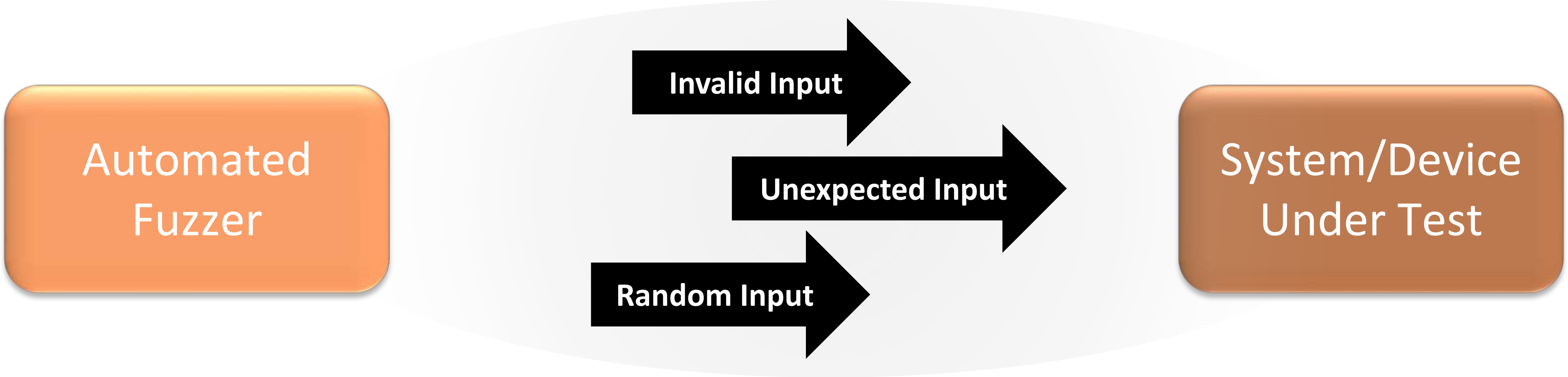
Controller-to-Switch

Feature Request, Get Config Request, Set Config, Packet-Out, Flow Modification, Group Modification, Port Modification, Table Modification, Meter Modification, Statistics Request, Barrier Request, Queue Get Config Request, Role Request, Get Asynchronous Request, Set Asynchronous

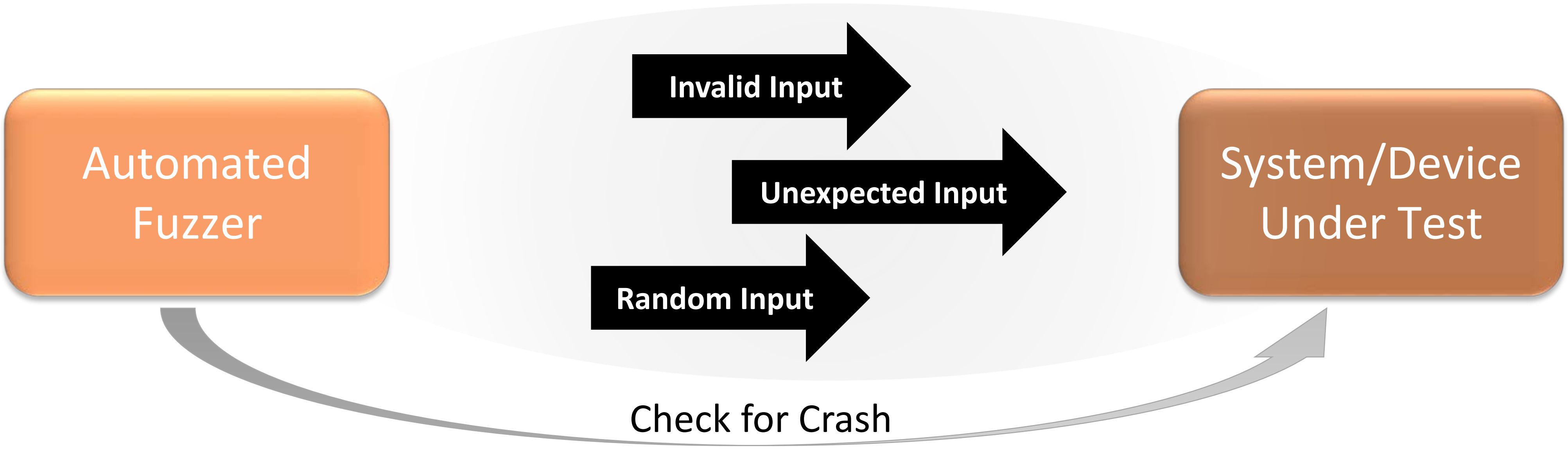
Symmetric

Hello
Echo Request
Echo Reply
Experimeter

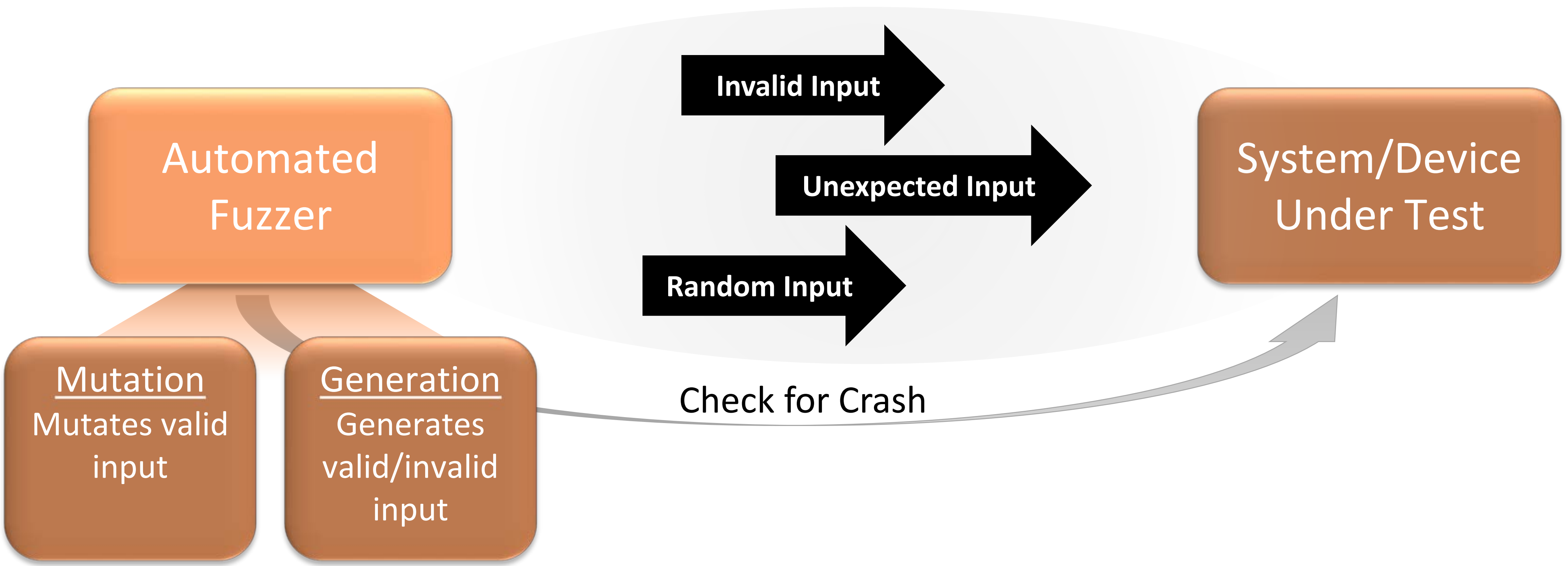
Fuzzing


Automated Fuzzer
Invalid Input
Unexpected Input
Random Input
System/Device Under Test

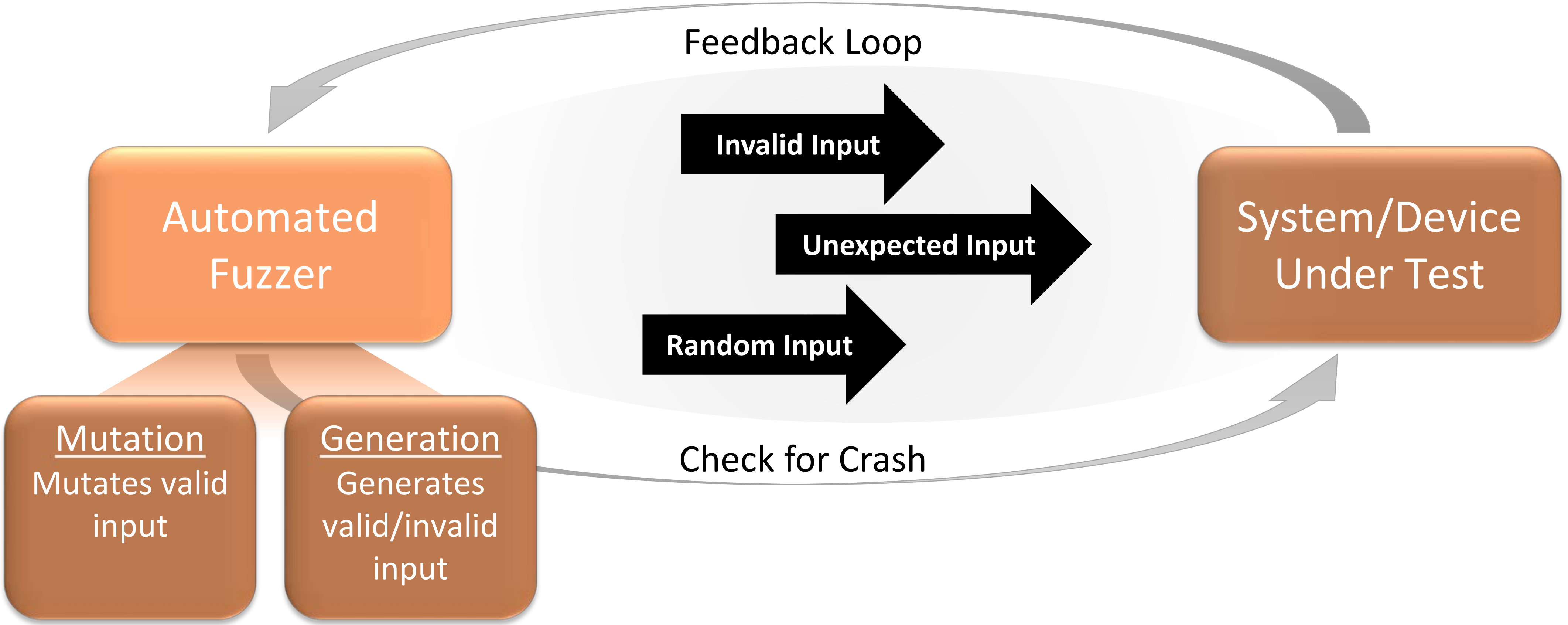
Fuzzing


Automated Fuzzer
Invalid Input
Unexpected Input
Random Input
System/Device Under Test
Check for Crash

Fuzzing

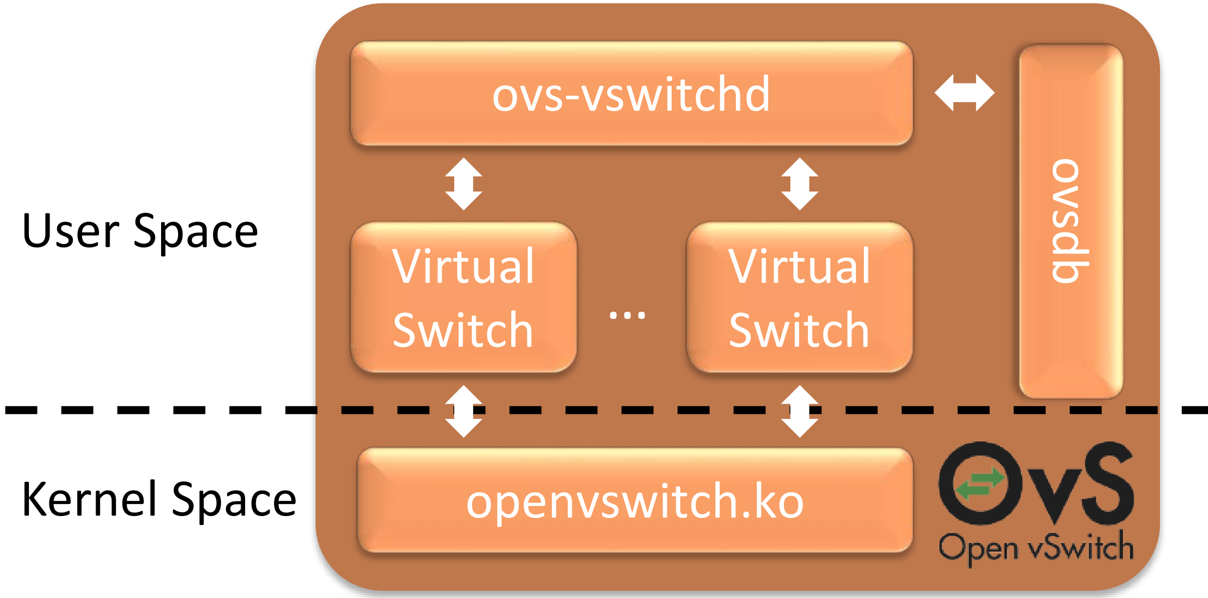

Automated Fuzzer
Mutation
Mutates valid input
Generation
Generates valid/invalid input
Invalid Input
Unexpected Input
Random Input
System/Device Under Test
Check for Crash

Fuzzing

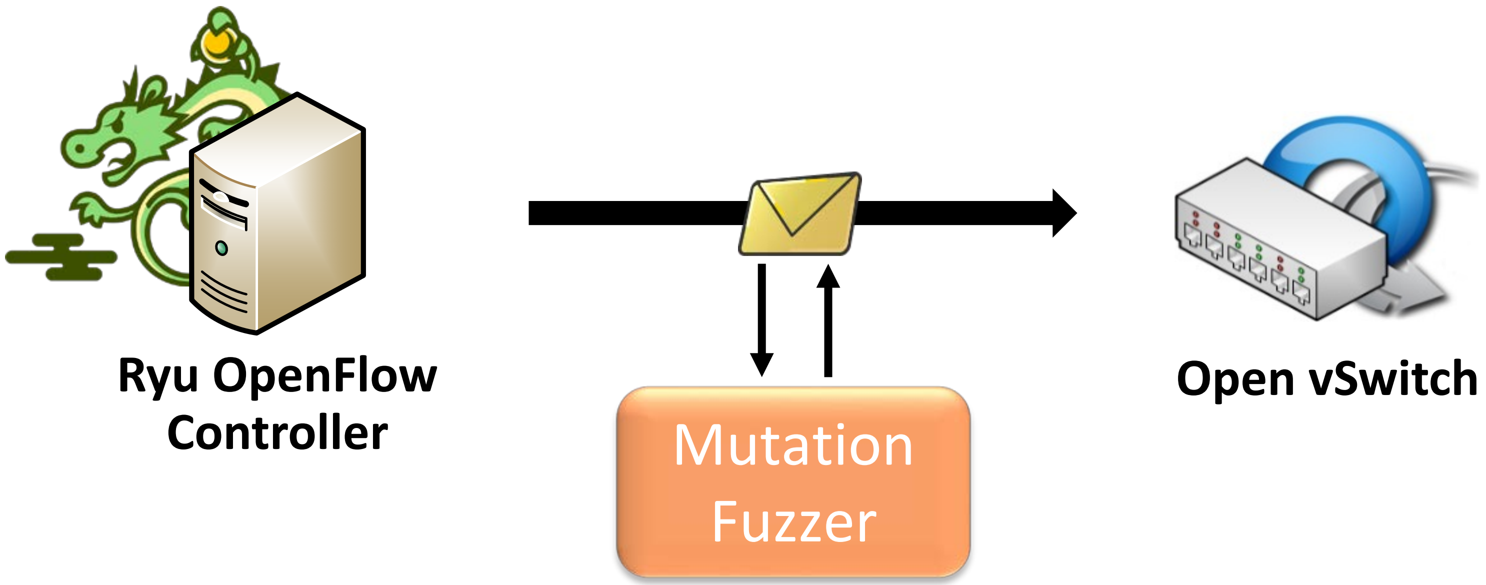

Feedback Loop
Automated Fuzzer
Invalid Input
Unexpected Input
Random Input
System/Device Under Test
Check for Crash
Mutation
Mutates valid input
Generation
Generates valid/invalid input

Open vSwitch (OvS)

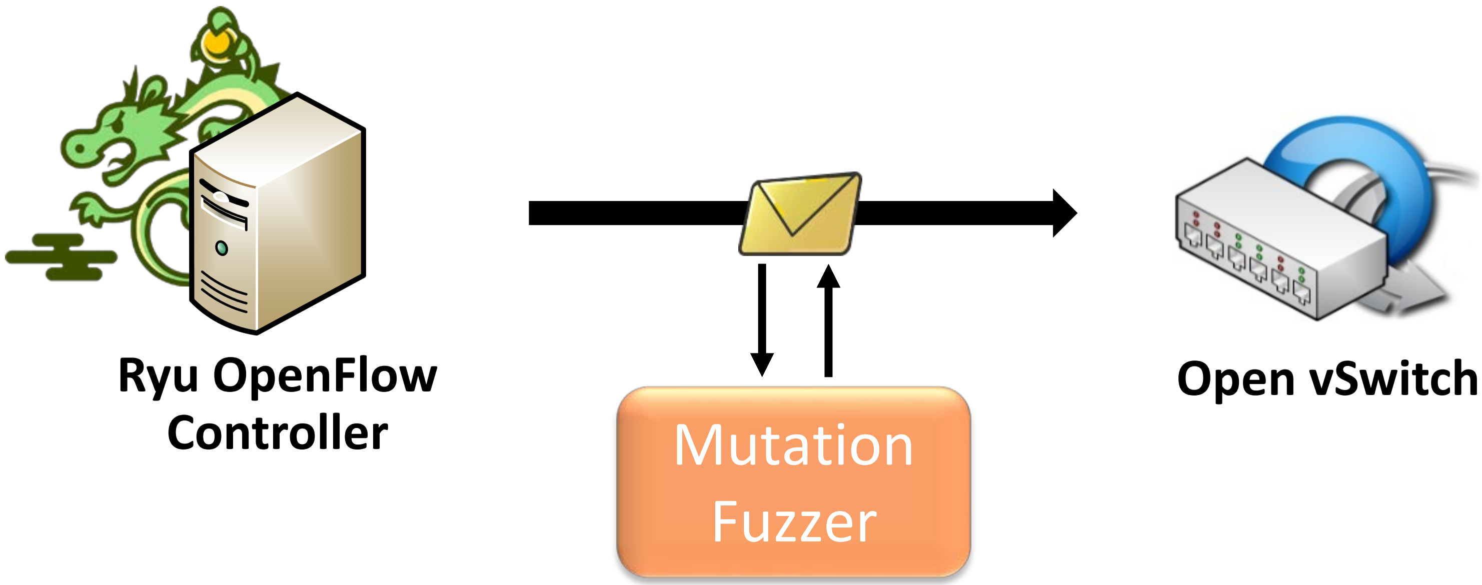
- Production quality, multilayer open virtual switch
- Integrated into OpenStack, Xen, Pica8…
- Fully supports OpenFlow up to v1.4
- Operates either as software switch or as control stack for dedicated hardware



Open vSwitch Fuzzer – A First Try

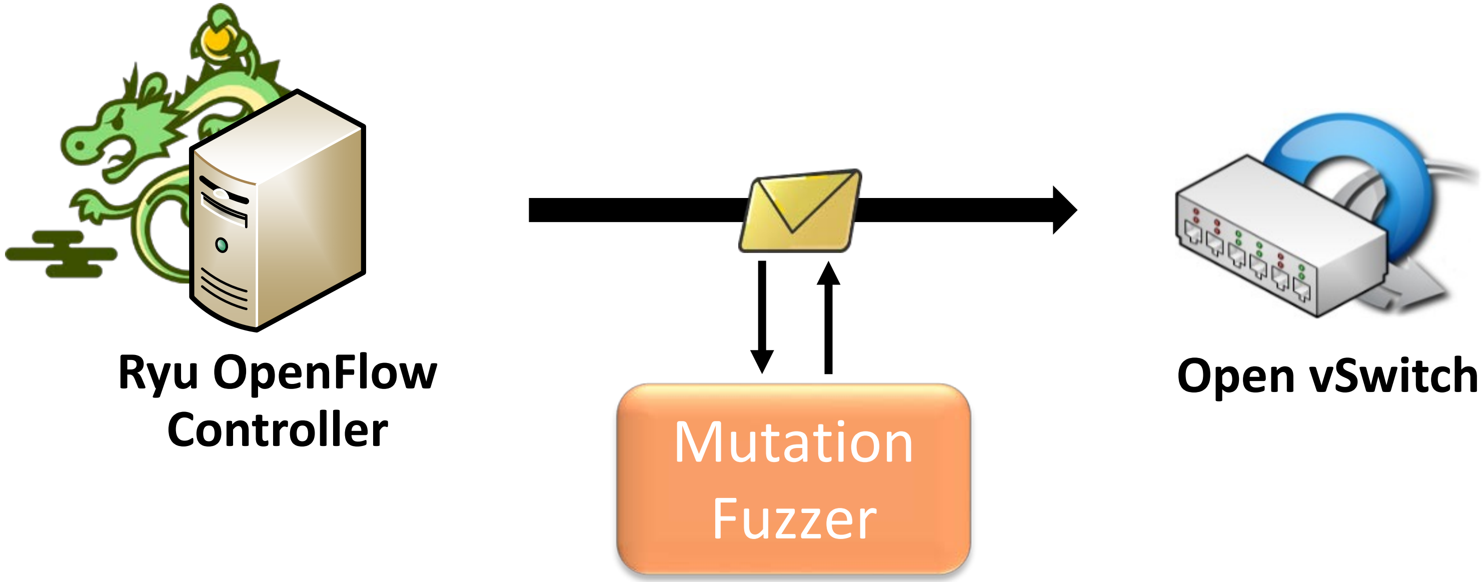


Open vSwitch Fuzzer – A First Try



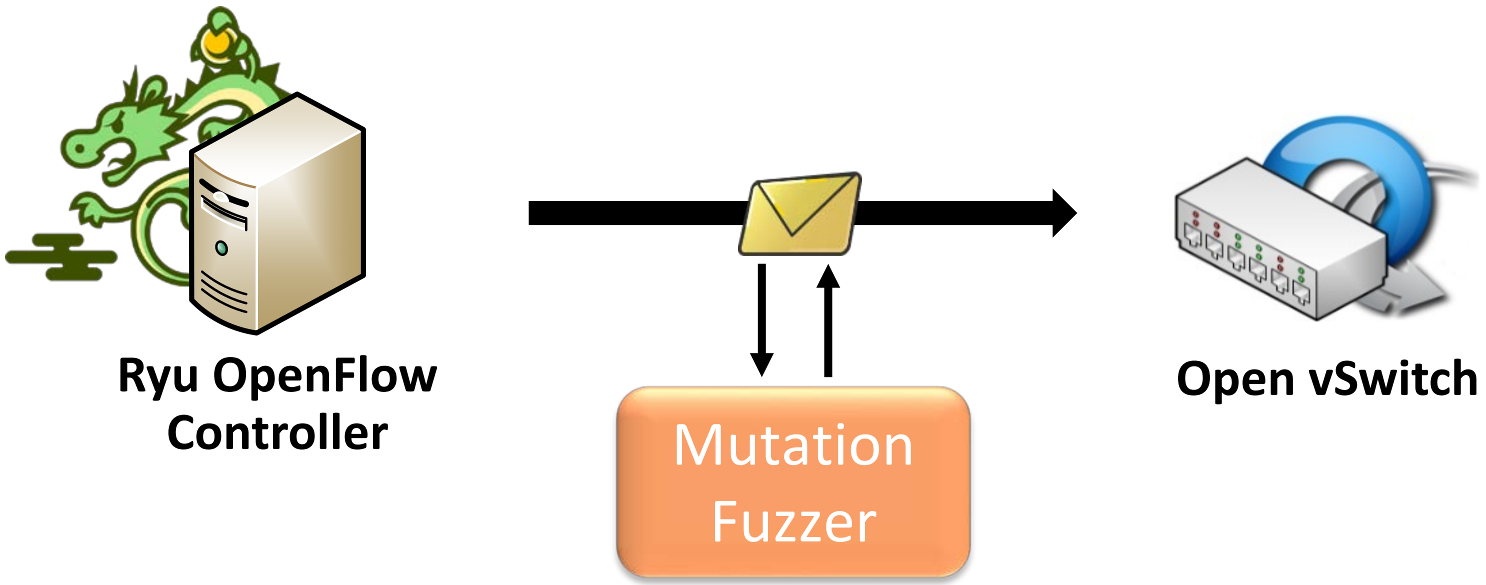
❌ Lack of control

Open vSwitch Fuzzer – A First Try



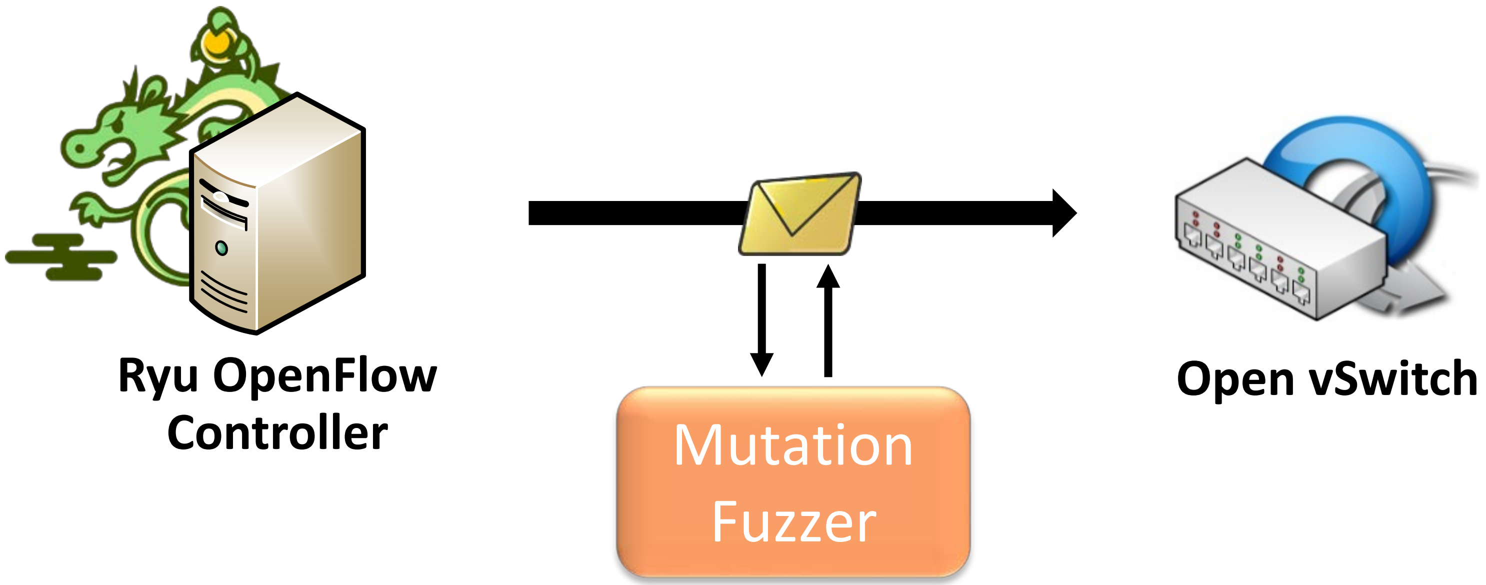
- ❌ Lack of control
- ❌ Controller needs to be actively triggered

Open vSwitch Fuzzer – A First Try



- ❌ Lack of control
- ❌ Controller needs to be actively triggered
- ❌ Hard to integrate a feedback loop

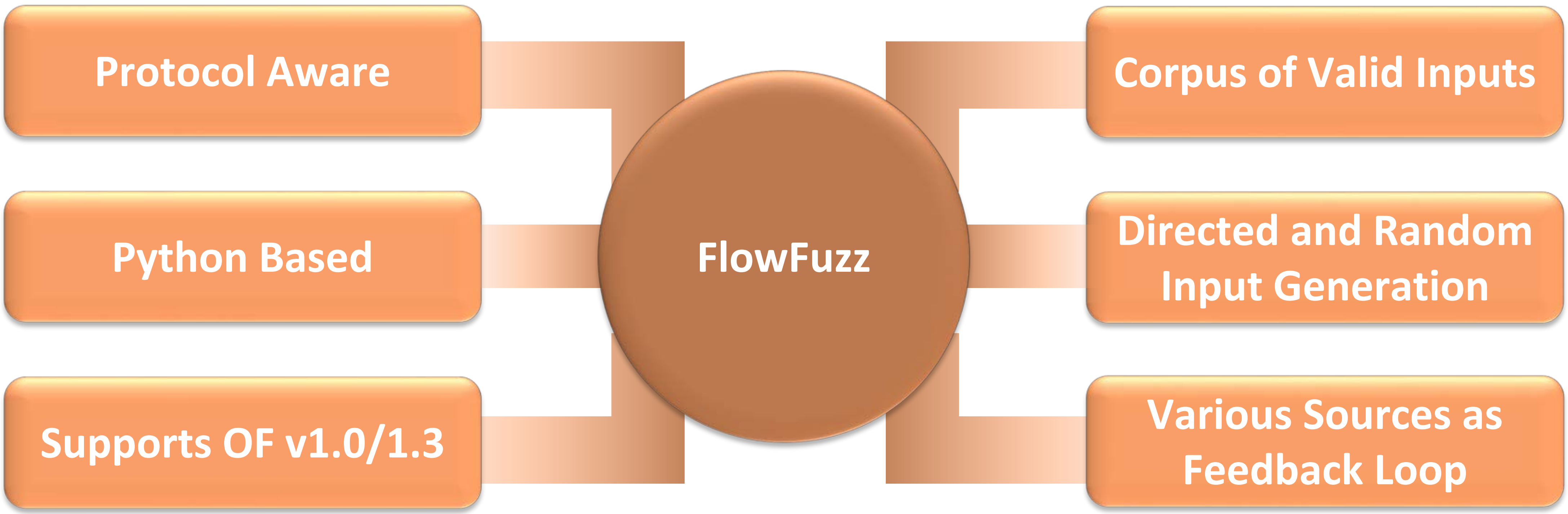
Open vSwitch Fuzzer – A First Try



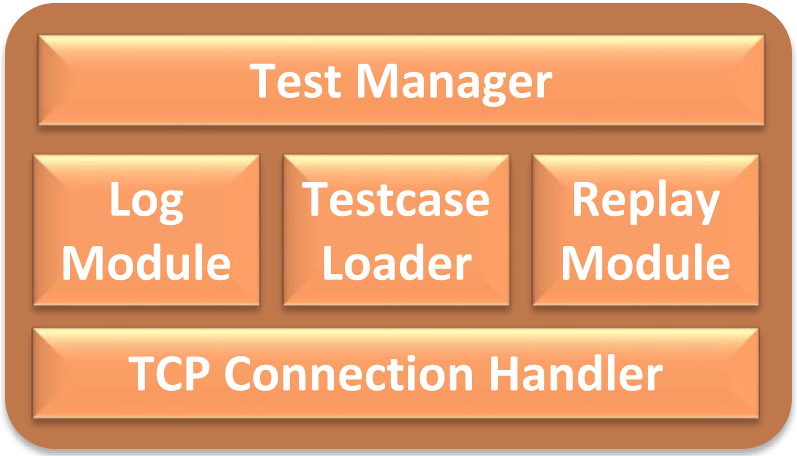
- ❌ Lack of control
- ❌ Controller needs to be actively triggered
- ❌ Hard to integrate a feedback loop

→ **Simple and fast but no promising approach**

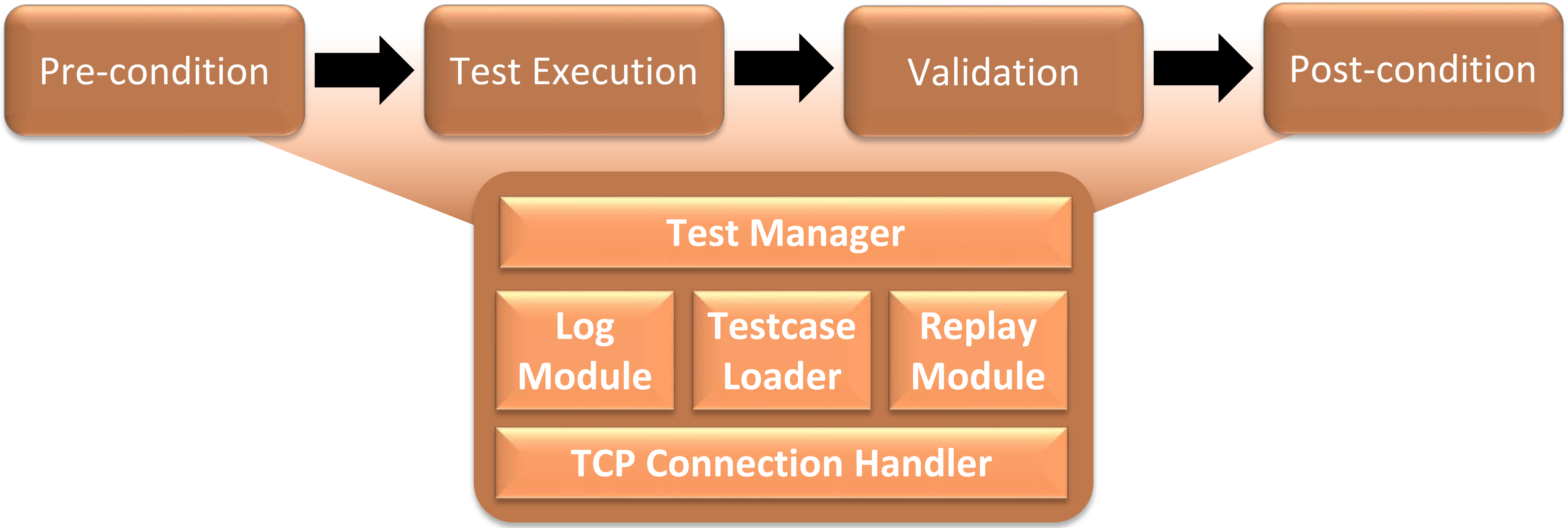
FlowFuzz


Protocol Aware
Python Based
Supports OF v1.0/1.3
FlowFuzz
Corpus of Valid Inputs
Directed and Random Input Generation
Various Sources as Feedback Loop

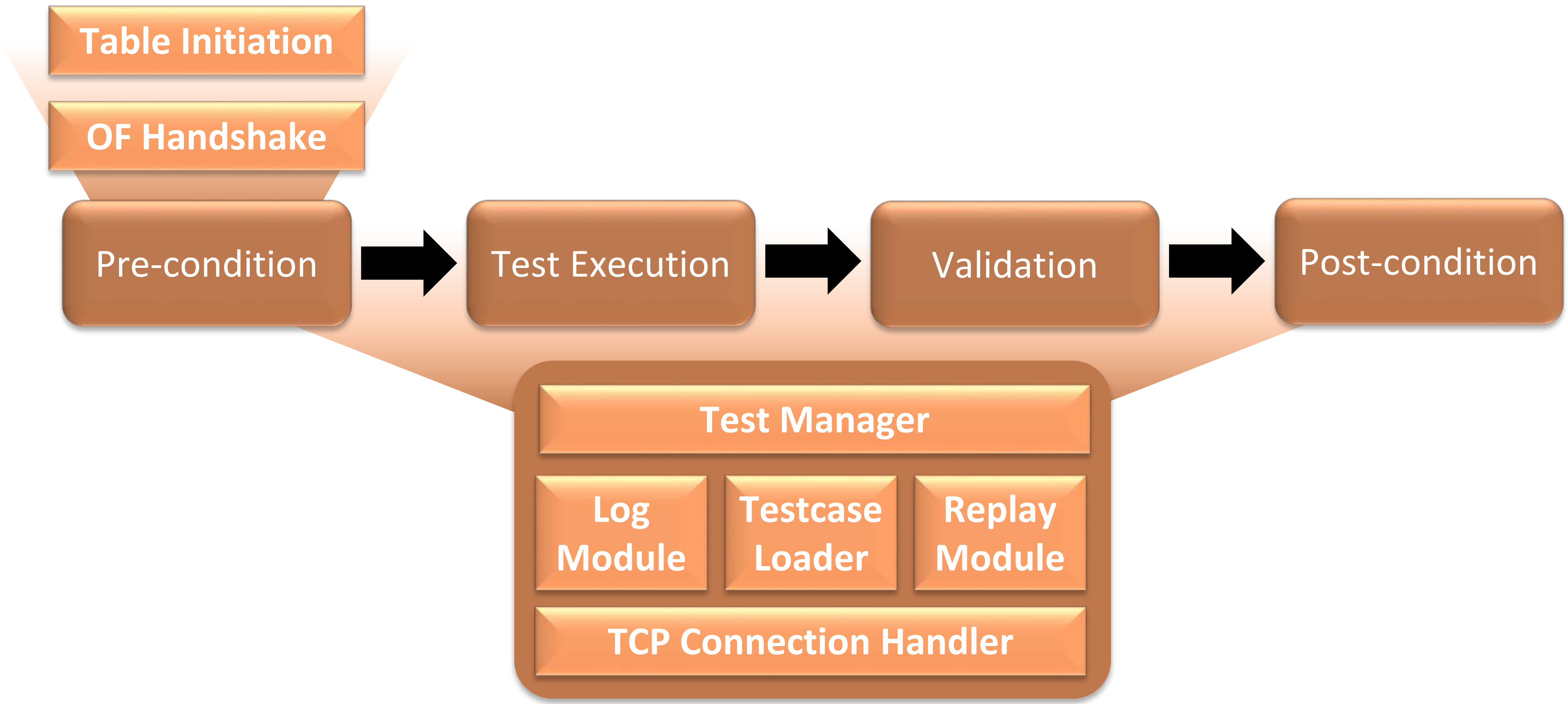
FlowFuzz – Architecture & Stages



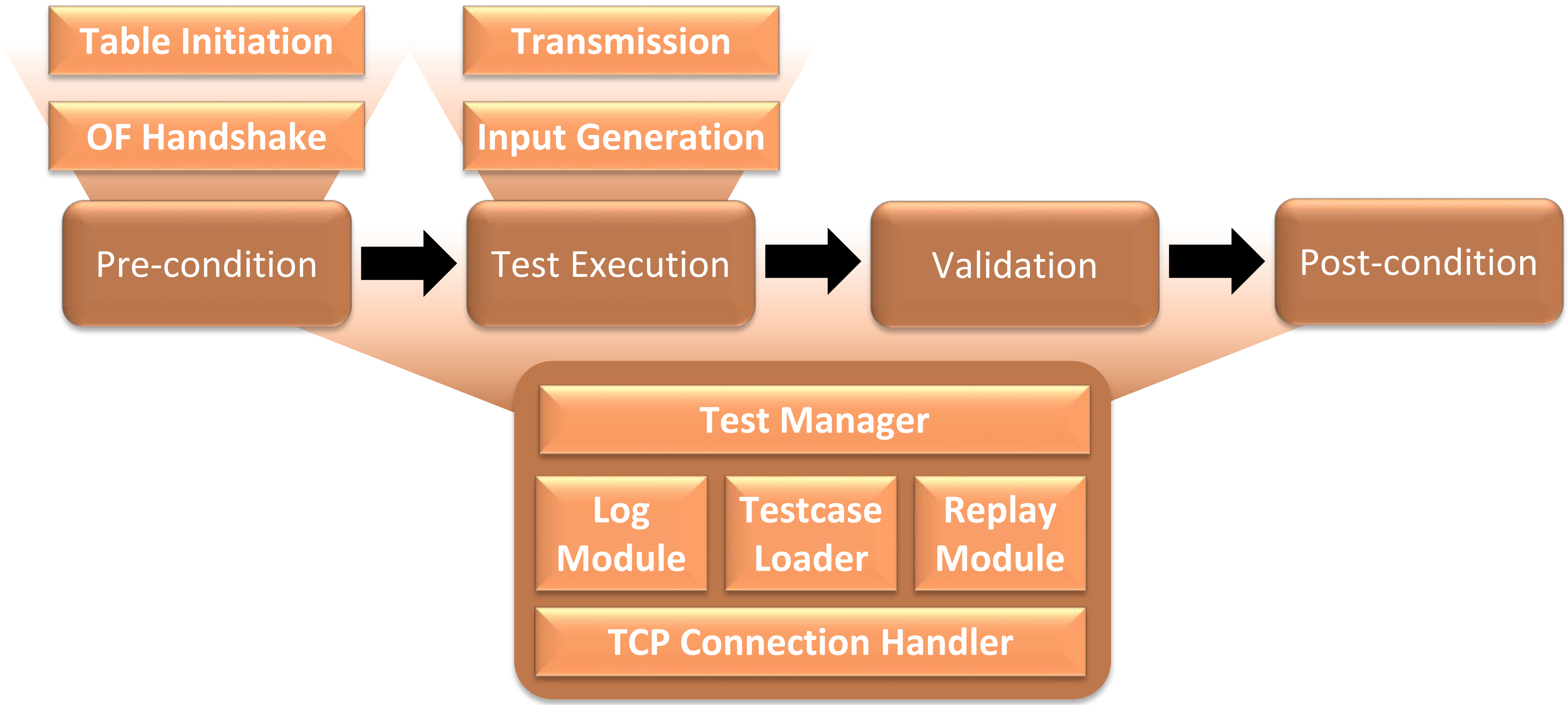
FlowFuzz – Architecture & Stages



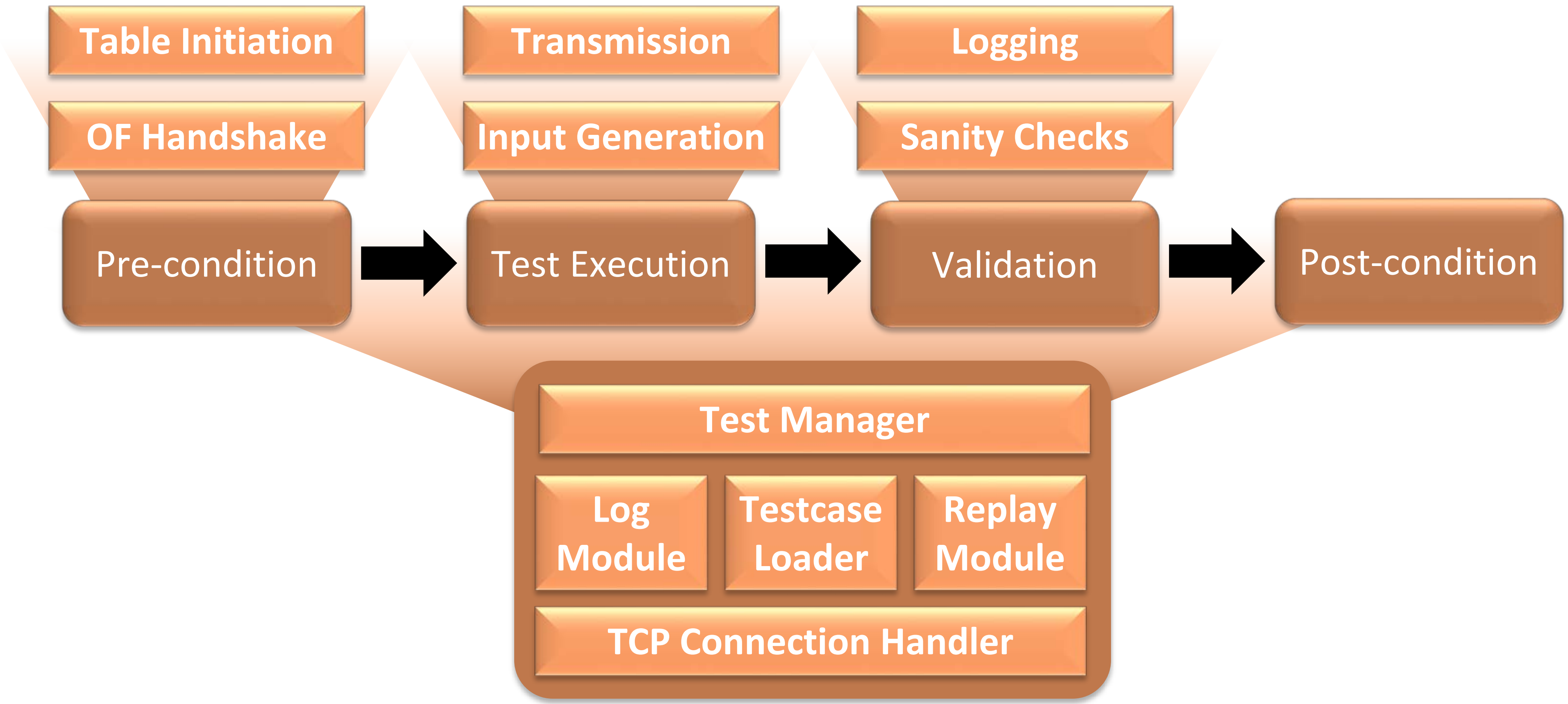
FlowFuzz – Architecture & Stages



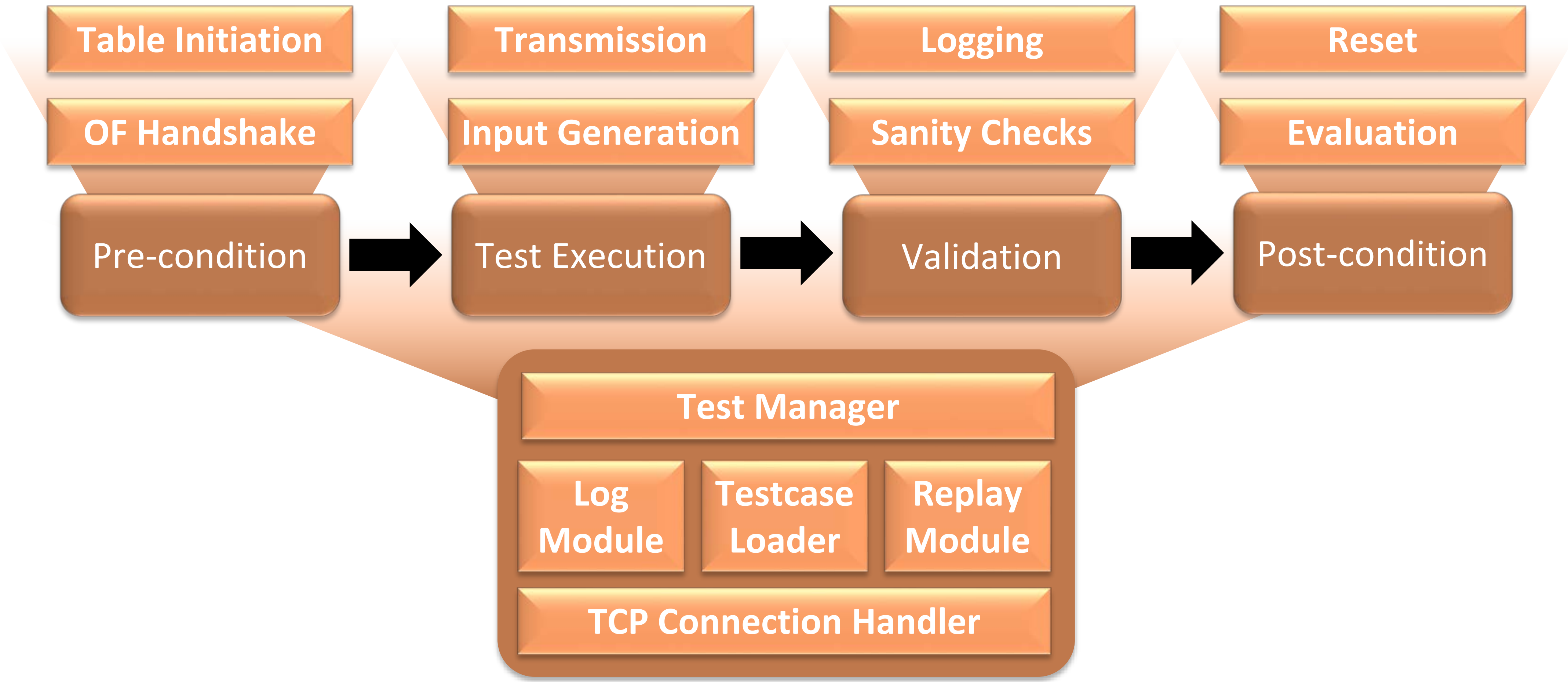
FlowFuzz – Architecture & Stages



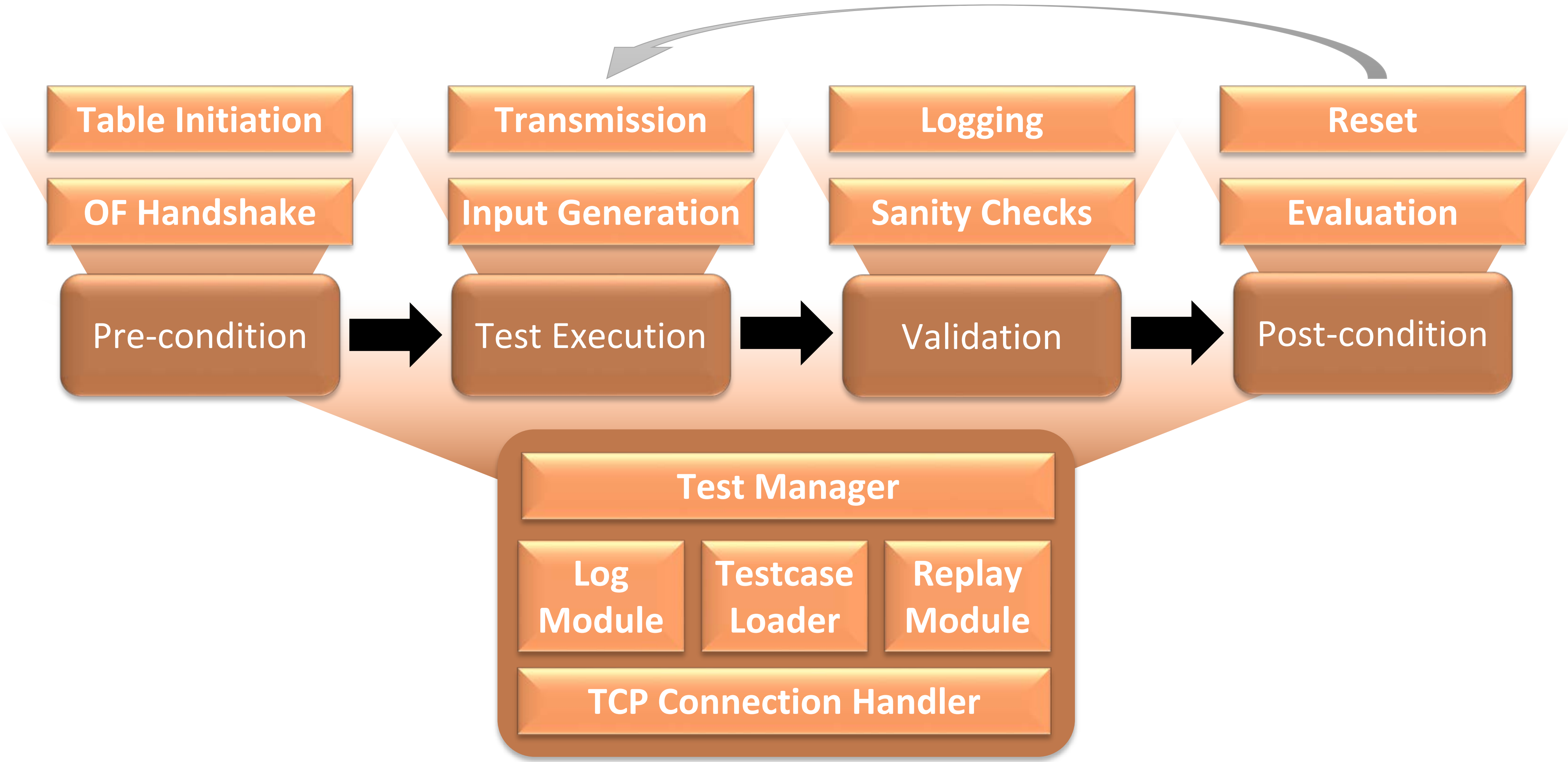
FlowFuzz – Architecture & Stages



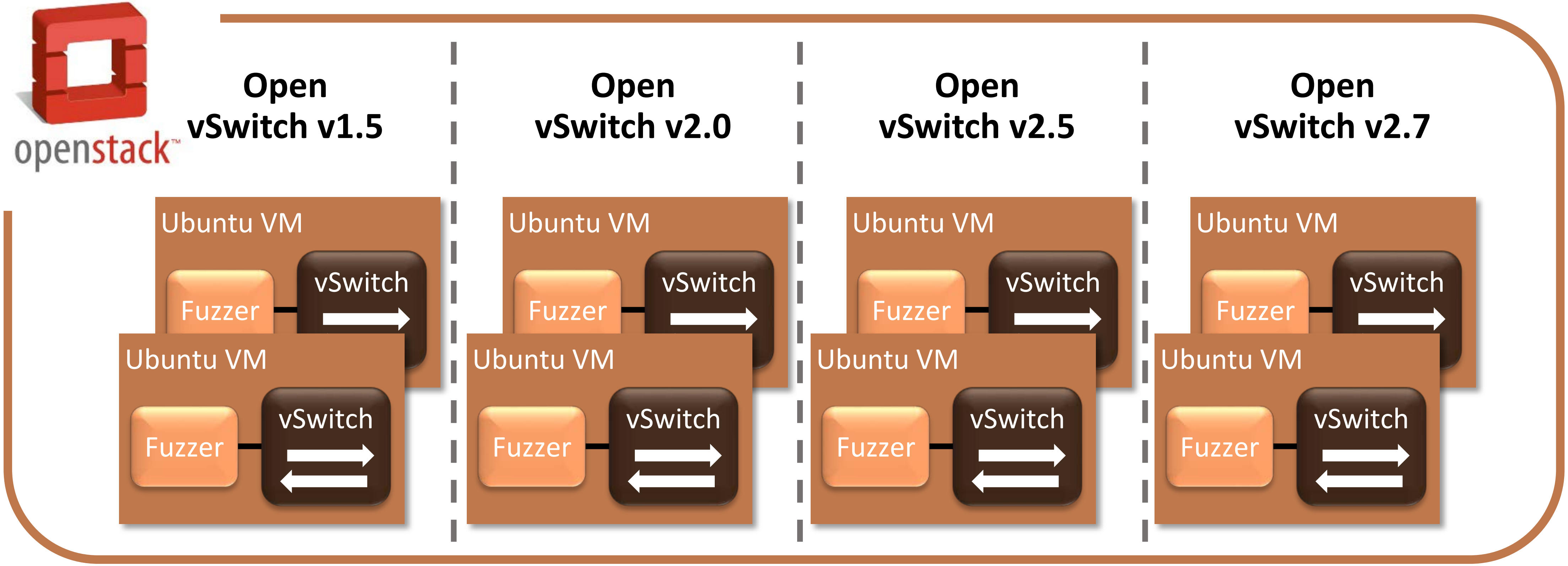
FlowFuzz – Architecture & Stages



FlowFuzz – Architecture & Stages



Open vSwitch – Test Bed



All compiled with AdressSanitizer

Open vSwitch – Fuzzer Evaluation

- Test duration of one week
- Targeted OpenFlow version 1.0
- Crafted and random inputs
- Code coverage as main feedback source

Results				
Version	v1.5	v2.0	v2.5	v2.7
Anomalies	2538	2986	2263	2047
Crashes	13	10	14	0

Open vSwitch – Fuzzer Evaluation

- Test duration of one week
- Targeted OpenFlow version 1.0
- Crafted and random inputs
- Code coverage as main feedback source

Results				
Version	v1.5	v2.0	v2.5	v2.7
Anomalies	2538	2986	2263	2047
Crashes	13	10	14	0

→ High number of false positives due to switch reconnects

Open vSwitch – Fuzzer Evaluation

- Test duration of one week
- Targeted OpenFlow version 1.0
- Crafted and random inputs
- Code coverage as main feedback source

Results				
Version	v1.5	v2.0	v2.5	v2.7
Anomalies	2538	2986	2263	2047
Crashes	13	10	14	0

→ High number of false positives due to switch reconnects
→ Crashes due to environment setup and could not be reproduced

Open vSwitch – Fuzzer Evaluation

- Test duration of one week
- Targeted OpenFlow version 1.0
- Crafted and random inputs
- Code coverage as main feedback source

Results				
Version	v1.5	v2.0	v2.5	v2.7
Anomalies	2538	2986	2263	2047
Crashes	13	10	14	0

→ High number of false positives due to switch reconnects
→ Crashes due to environment setup and could not be reproduced
→ No security flaws detected – yet!

Hardware Switch – Feedback Sources

NEC PF5240

Pronto 3290

HP 2920-24G

Quanta T1048-LB9

Hardware Switch – Feedback Sources

NEC
PF5240

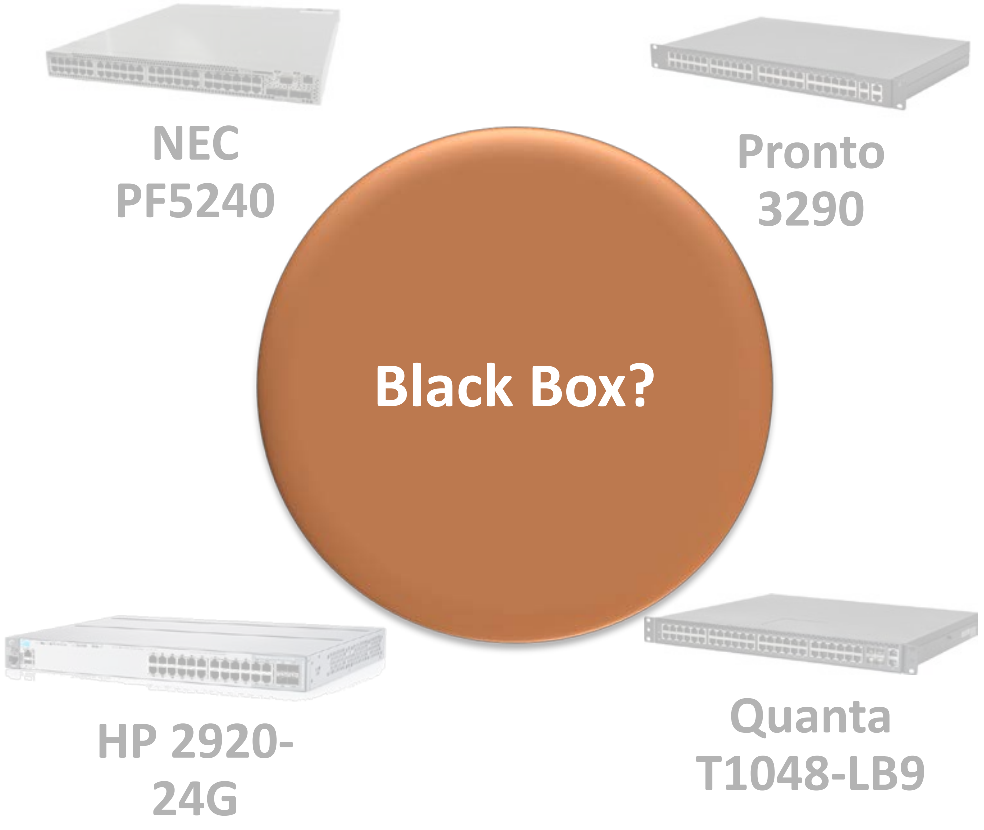
Pronto
3290

Traditional guided fuzzing mechanisms cannot be applied!

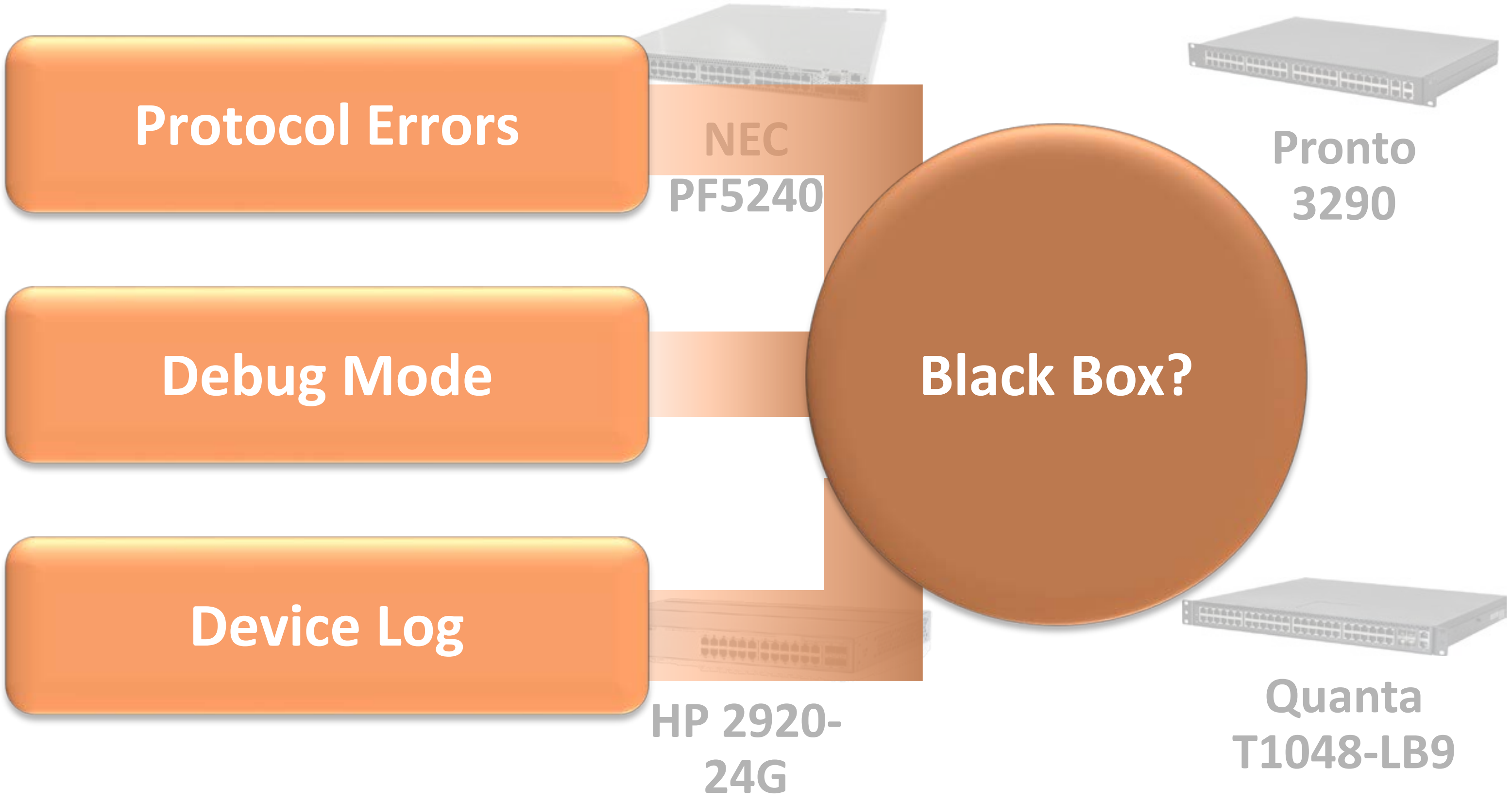
HP 2920-24G

Quanta
T1048-LB9

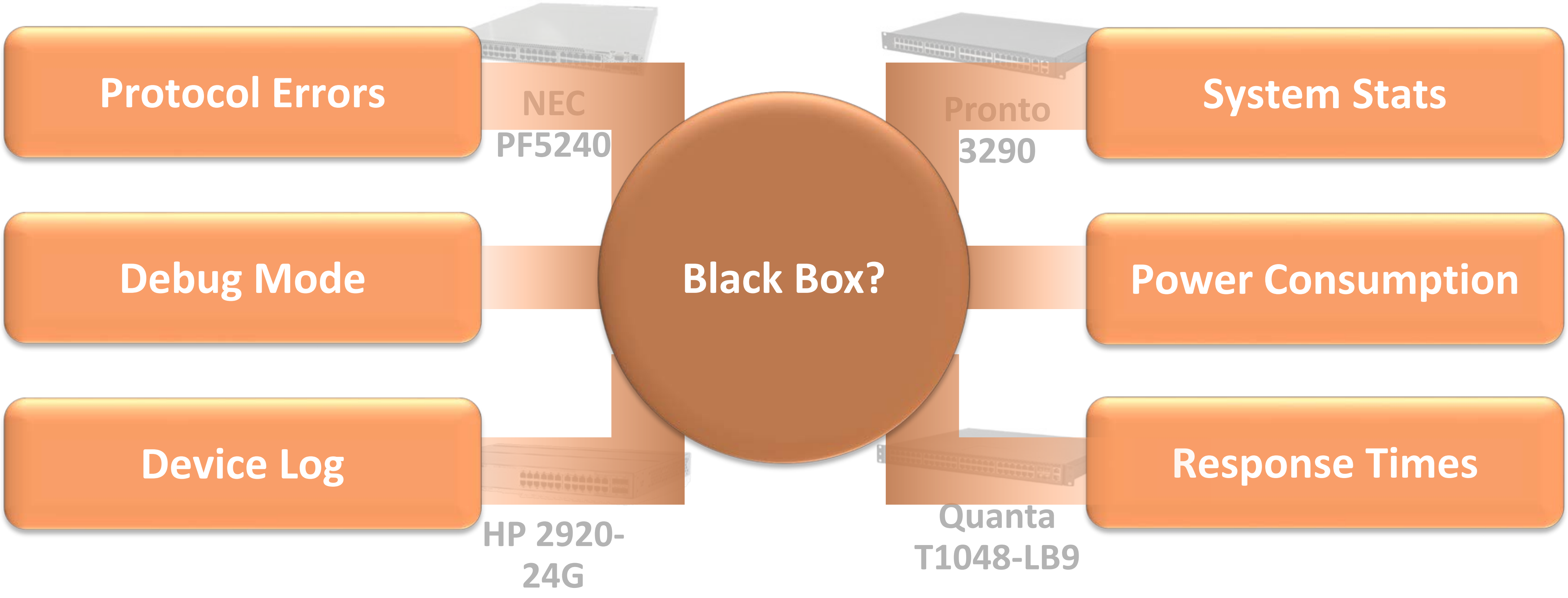
Hardware Switch – Feedback Sources



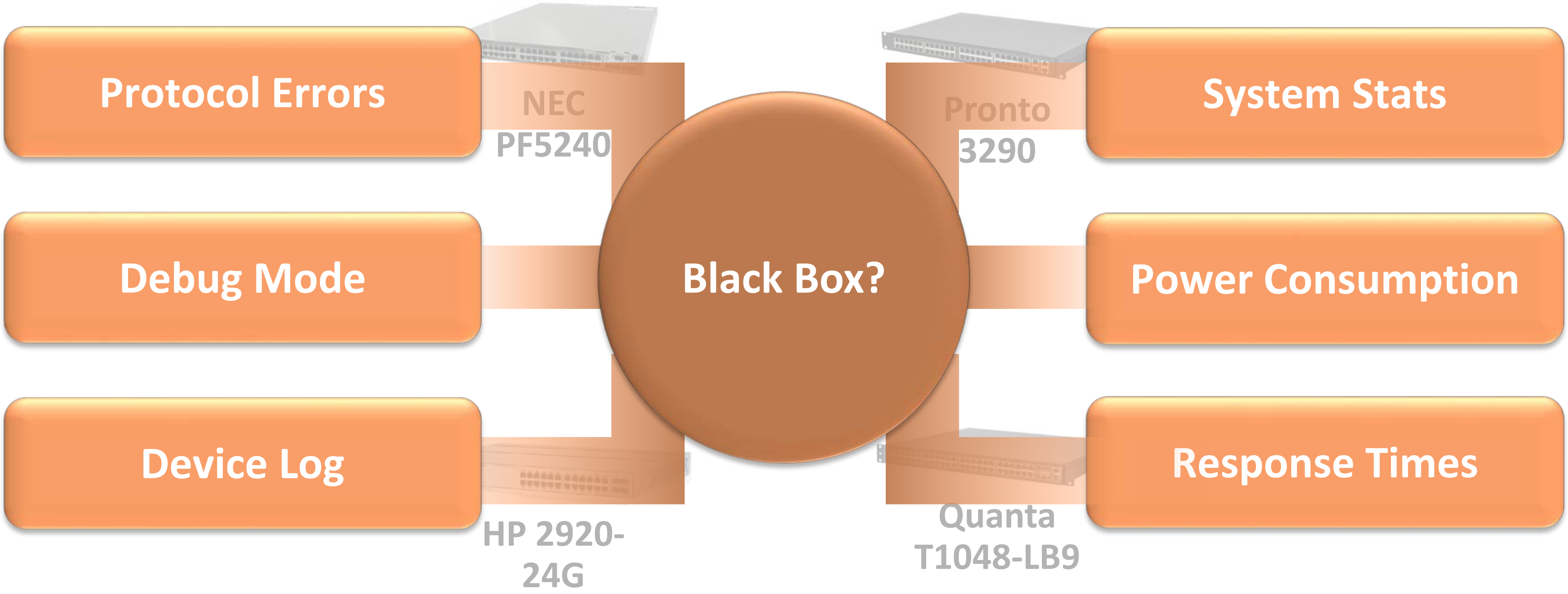
Hardware Switch – Feedback Sources



Hardware Switch – Feedback Sources

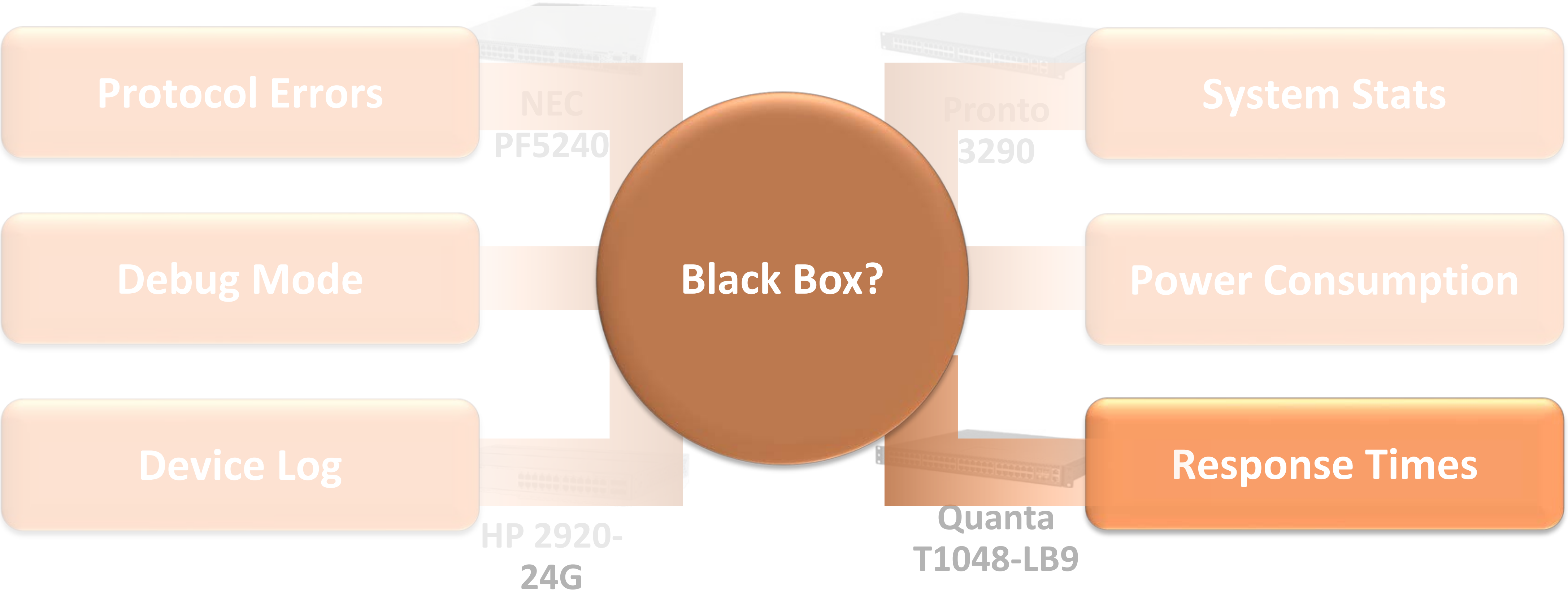


Hardware Switch – Feedback Sources



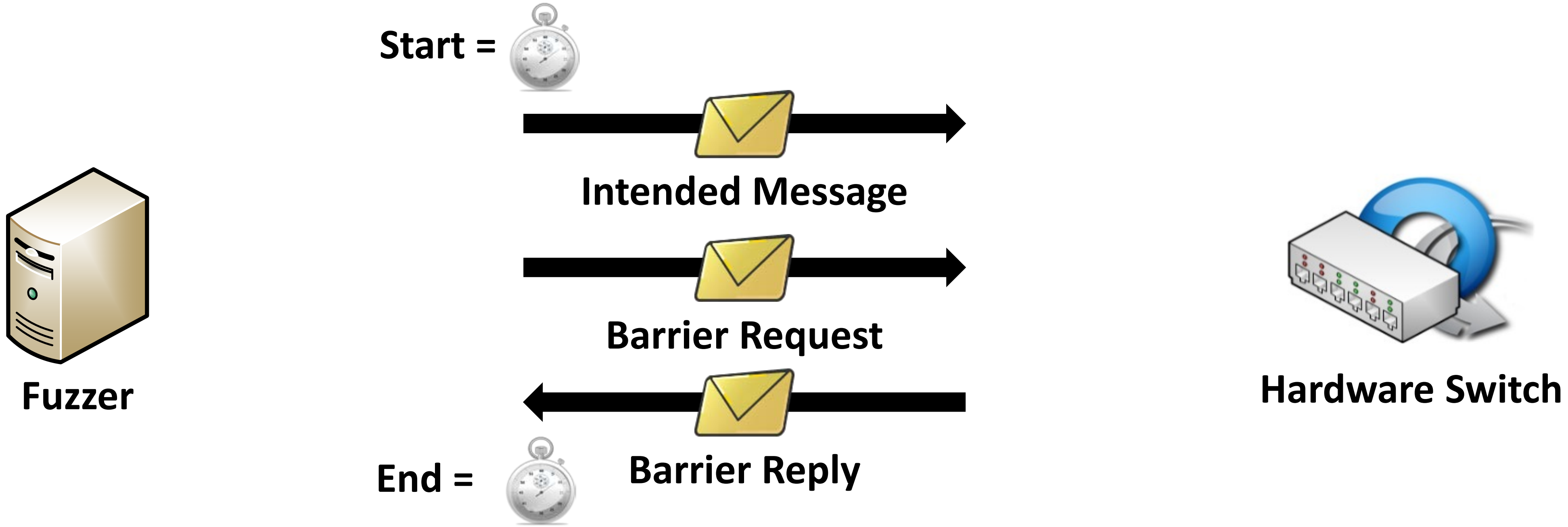
→ Combine all sources to create an unique signature per input

Hardware Switch – Feedback Sources



→ Combine all sources to create an unique signature per input

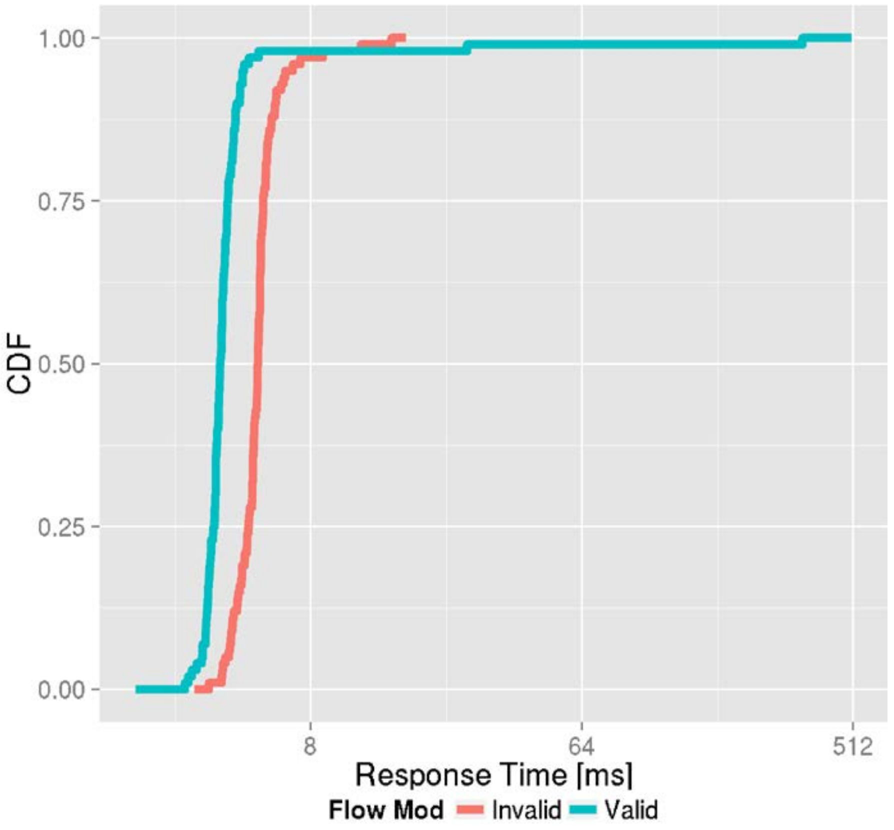
Feedback Sources – Measuring Response Times



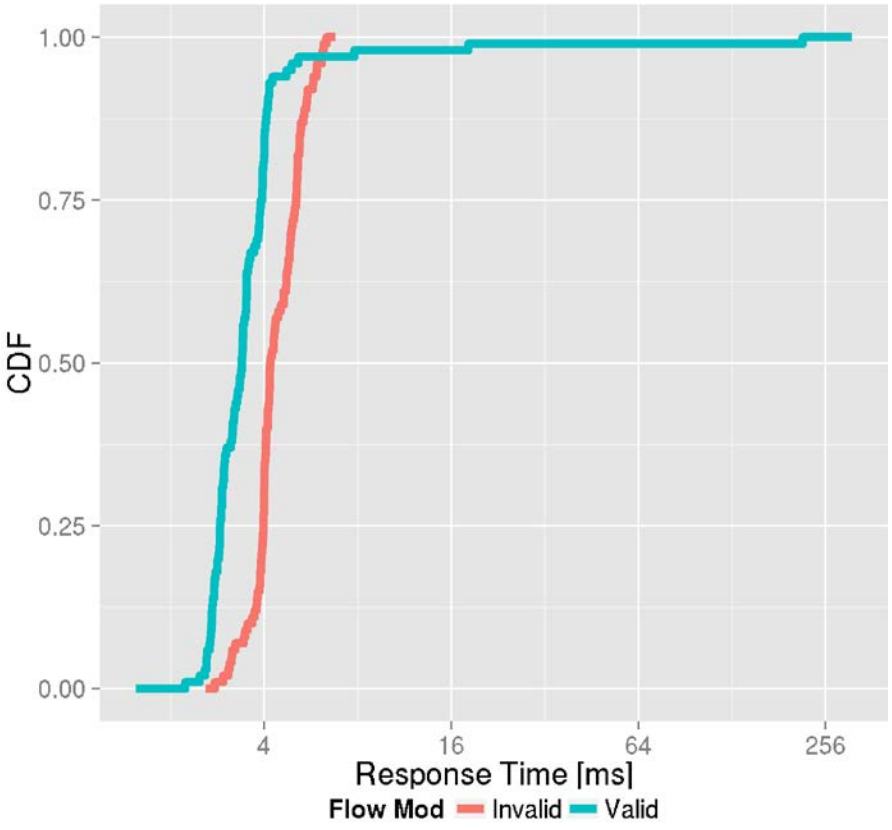
→ **Timediff = End - Start**

Feedback Sources – Evaluation of Response Times

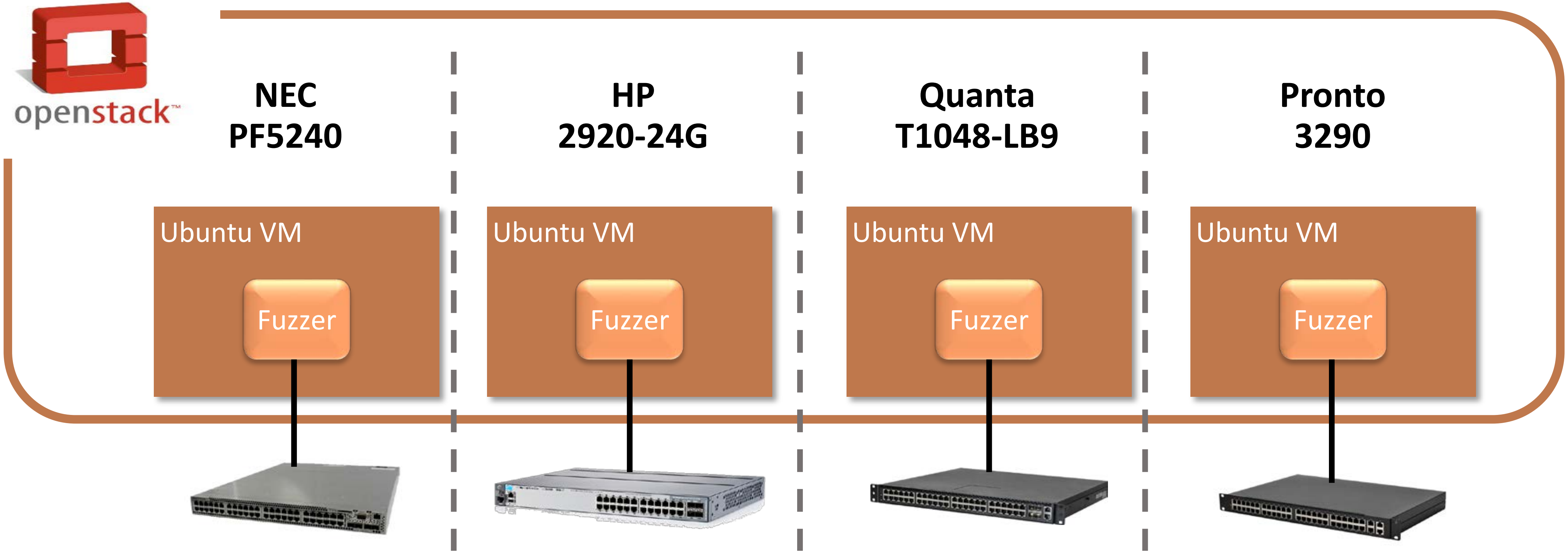
HP 2920-24G



Pronto 3290



Hardware Switch – Test Bed



Hardware Switch – Fuzzer Evaluation

- Test duration of 12h
- Targeted OpenFlow version 1.0
- Crafted and random inputs
- Response times as main feedback source

Results				
Version	NEC	HP	Quanta	Pronto
Anomalies	2133	1735	1915	2643
Crashes	0	0	0	0

→ High number of false positives due to switch reconnects

→ No security flaws decteted – yet!

Flow Fuzz – Next Steps & Future Extension

Measurements

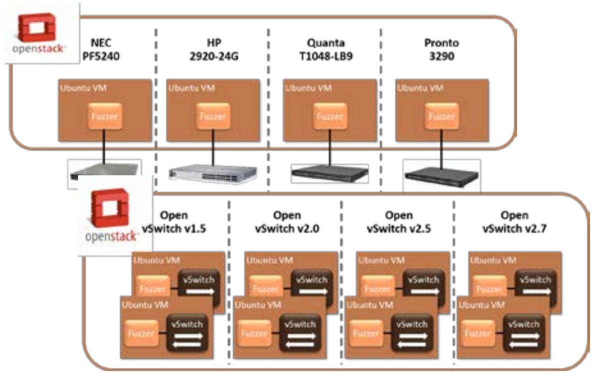
- Reduce false positive rate
- Increase test duration
- Fuzz OpenFlow v1.3

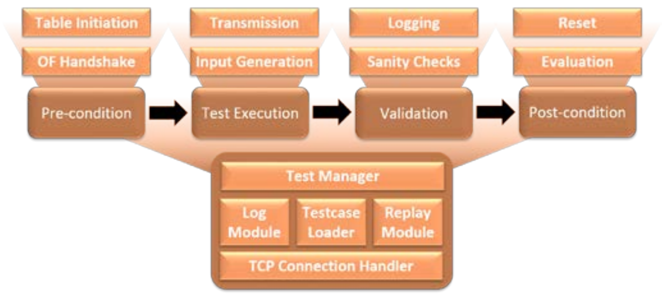
Extensions

- Support higher OF versions
- Optimize feedback loop
- Agents for DP fuzzng

Corpus Generation

- Categorized by OF version
- Derived from code coverage





Sound Bytes

- SDN is coming – Be prepared!
- SDN can enhance the security of networks
- FlowFuzz – A protocol-aware OpenFlow fuzzing framework
- De-blackboxing black boxes by using alternative feedback sources

Questions

Sources

- Michael Jarschel, Thomas Zinner, Tobias Hoßfeld, Phuoc Tran-Gia, and Wolfgang Kellerer, **Interfaces, Attributes, and Use Cases: A Compass for SDN**, *IEEE Communications Magazine, 52, 2014*
- D. Kreutz et al., **Software-Defined Networking: A Comprehensive Survey**, *ArXiv e-prints, Jun. 2014*.
- Lorenz, C., Hock, D., Scherer, J., Durner, R., Kellerer, W., Gebert, S., Gray, N., Zinner, T., Tran-Gia, P., **An SDN/NFV-enabled Enterprise Network Architecture Offering Fine-Grained Security Policy Enforcement,** *IEEE Communications Magazine. 55, 217 - 223 (2017)*
- Gray, N., Lorenz, C., Müssig, A., Gebert, S., Zinner, T., Tran-Gia, P., **A Priori State Synchronization for Fast Failover of Stateful Firewall VNFs. Workshop on Software-Defined Networking and Network Function Virtualization for Flexible Network Management,** *SDNFlex 2017*

Sources

- Pfaff B., Scherer J., Hock D., Gray N., Zinner T., Tran-Gia P., Durner R., Kellerer R., Lorenz C., **SDN/NFV-enabled Security Architecture for Fine-grained Policy Enforcement and Threat Mitigation for Enterprise,** *ACM SIGCOMM Computer Communication Review, 2017*
- Tsipenyuk, Katrina, Brian Chess, and Gary McGraw, **Seven pernicious kingdoms: A taxonomy of software security errors,** *IEEE Security & Privacy 3.6 (2005): 81-84*
- Benton, Kevin, L. Jean Camp, and Chris Small, **Openflow vulnerability assessment,** *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking, ACM, 2013*
- Thimmaraju, K., Shastry, B., Fiebig, T., Hetzelt, F., Seifert, J. P., Feldmann, A., & Schmid, S., **Reigns to the cloud: Compromising cloud systems via the data plane,** *arXiv preprint arXiv:1610.08717*

Sources

- Changhoon Yoon, Seungsoo Lee,
  Attacking SDN Infrastructure: Are We Ready for the Next-Gen Networking?,
  Black Hat USA 2016
- Jennia Hizver,
  Taxonomic Modeling of Security Threats in Software Defined Networking,
  Black Hat USA 2015
- Gregory Pickett,
  Abusing Software Defined Networks,
  Black Hat Europe 2014
- Scott-Hayward, Sandra, Gemma O'Callaghan, and Sakir Sezer,
  SDN security: A survey,
  Future Networks and Services (SDN4FNS), 2013 IEEE SDN For. IEEE, 2013.

Sources

- Open Networking Foundation,
  https://www.opennetworking.org,
  called on 2017-07-14
- Open Networking Foundation,
  OpenFlow Switch Specification Version 1.3.5,
  called on 2017-07-14
- Ari Takanen, Jared DeMott, Charlie Miller,
  Fuzzing for Software Security Testing and Quality Assurance,
  ARTECH HOUSE, INC. ISBN 13: 978-1-59693-214-2
- OpenVSwitch - Linux Foundation,
  https://openvswitch.org,
  called on 2017-07-14

Sources

- Ryu SDN Framework Community
  https://osrg.github.io/ryu/,
  called on 2017-07-14
- OpenStack – Open Source Cloud Computing Software
  https://www.openstack.org/
  called on 2017-07-14