PennState College of Engineering | ELECTRICAL ENGINEERING AND COMPUTER SCIENCE

Adversarial Network Forensics in Software Defined Networking

Stefan Achleitner, Thomas La Porta, Trent Jaeger, Patrick McDaniel

PennState College of Engineering | INSTITUTE FOR NETWORKING AND SECURITY RESEARCH

Why Software Defined Networking?

Why Software Defined Networking?

Why Software Defined Networking?

sdx central

SPONSORED: Network Virtualization 3
Containers 6 SDN 2 NFV 3 SD-WAN 4 Cloud 0 Security 4 IoT 4

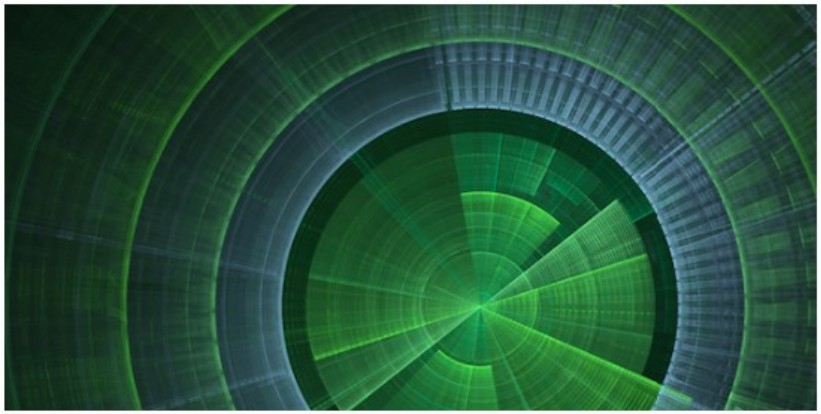
SPONSORED: Arista Brocade Juniper Networks Linux Foundation 7 Netcracker 6 Nuage Networks 1

Search

& Culture

ted to Reach $132.9 Billion

5G Depends on SDN & NFV



Linda Hardesty
January 25, 2016
8:27 am PT

Last year at Mobile World Congress in Barcelona, the first inklings of 5G were discussed. This year, 5G will probably be all over the place — and software-defined networking (SDN) and network functions virtualization (NFV) will play important roles, especially in terms of a new network topology.

The goals for 5G are 1,000-times higher system capacity; 100-times increase in data rates; connectivity enablement for 100-times more devices; latency reduced to 1 millisecond from 5 ms; and energy savings. So says Raj Singh, general manager of the wireless broadband group at Cavium.

Why Software Defined Networking?

sdx central

SPONSORED: Network Virtualization 3

TRENDING: Online privacy meets abortion debate · FCC may rollback net neutrality rules · Apple breaks secrecy · Samsung's profit soars · Resources/White Papers

SPONSORED:

NETWORKWORLD FROM IDG

silver peak eGuide: The Software-Defined WAN EXPAND 1/5

Home > Software-Defined Networking/NFV

5G Depe

Software-Defined Networking will be a critical enabler of the Internet of Things

SDN will support IoT by centralizing control, abstracting network devices, and providing flexible, dynamic, automated reconfiguration of the network

By Jeff Reed, VP of the Enterprise Infrastructure and Solutions Group, Cisco
Network World | JUN 5, 2015 8:36 AM PT

Last year at Mobile World Congress in Barcelona, the first inklings of 5G were discussed. This year, 5G will probably be all over the place — and software-defined networking (SDN) and network functions virtualization (NFV) will play important roles, especially in terms of a new network topology.

The goals for 5G are 1,000-times higher system capacity; 100-times increase in data rates; connectivity enablement for 100-times more devices; latency reduced to 1 millisecond from 5 ms; and energy savings. So says Raj Singh, general manager of the wireless broadband group at Cavium.

Why Software Defined Networking?

sdx central

SPONSORED: Network Virtualization 3

Containers 6 SDN 2 NFV 3 SD-WAN 4 Cloud 0 Security 4 IoT 4

rofit soars Resources/White Papers

TC News Startups Mobile Gadgets Enterprise Social Europe

Trending Snap Amazon NASA

EXPAND 1/5

DISRUPT NY Last Days For Early Bird Savings On Disrupt NY Tickets Save $1000 On Tickets Now!

e a critical

ces, and providing

software-defined networking
Internet of Things
disaster response
sdn
IoT
Popular Posts

CRUNCH NETWORK

Responding to disaster with IoT and SDN mesh

Posted Dec 23, 2016 by Jay Turner

NEWSLETTER SUBSCRIPTIONS

The Daily Crunch

Get the top tech stories of the day delivered to your inbox

The goals for 5G are 1,000-times higher system capacity; 100-times increase in data rates; connectivity enablement for 100-times more devices; latency reduced to 1 millisecond from 5 ms; and energy savings. So says Raj Singh, general manager of the wireless broadband group at Cavium.

Why Software Defined Networking?

sdx central

SPONSORED: Network Virtualization 3

Containers 0 SDN 2 NFV 3 SD-WAN 4 Cloud 0 Security 4 IoT 4 profit soars Resources/White Papers

NETWORKWORLD FROM IDG

silverpeak New SD-WAN: Why Performance Matters EXPAND 4/5

Home > LAN & WAN > Internet of Things

SDN vital to IoT

By Jim Duffy
Managing Editor, Network World | SEP 7, 2014 9:00 PM PT

Las
pro
will

NEWSLETTER SUBSCRIPTIONS

The Daily Crunch
Get the top tech stories of the day delivered to your inbox

The goals for 5G are 1,000-times higher system capacity; 100-times increase in data rates; connectivity enablement for 100-times more devices; latency reduced to 1 millisecond from 5 ms; and energy savings. So says Raj Singh, general manager of the wireless broadband group at Cavium.

Why Software Defined Networking?

TRENDING: Online privacy meets abortion debate · FCC may rollback net neutrality rules · Apple breaks secrecy · Samsung's profit soars · Resources/White Papers

NETWORKWORLD FROM IDG

The Register®
Biting the hand that feeds IT

DATA CENTER SOFTWARE SECURITY TRANSFORMATION DEVOPS BUSINESS PERSONAL TECH

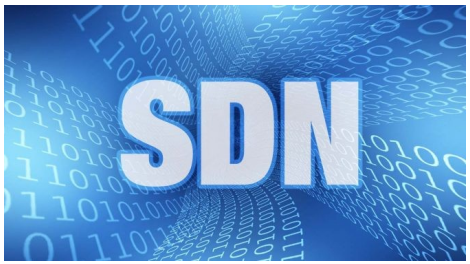
Security

Software-defined networking is dangerously sniffable

NEWSLETTER SUBSCRIPTIONS

The Daily Crunch
Get the top tech stories of the day delivered to your inbox

Software Defined Networking
Enables dynamic and flexible reconfiguration of networks



Agile cyber maneuvers

Moving target defense
(*Jafarian et al. (2012,2015), Al-Shaer et al.*)

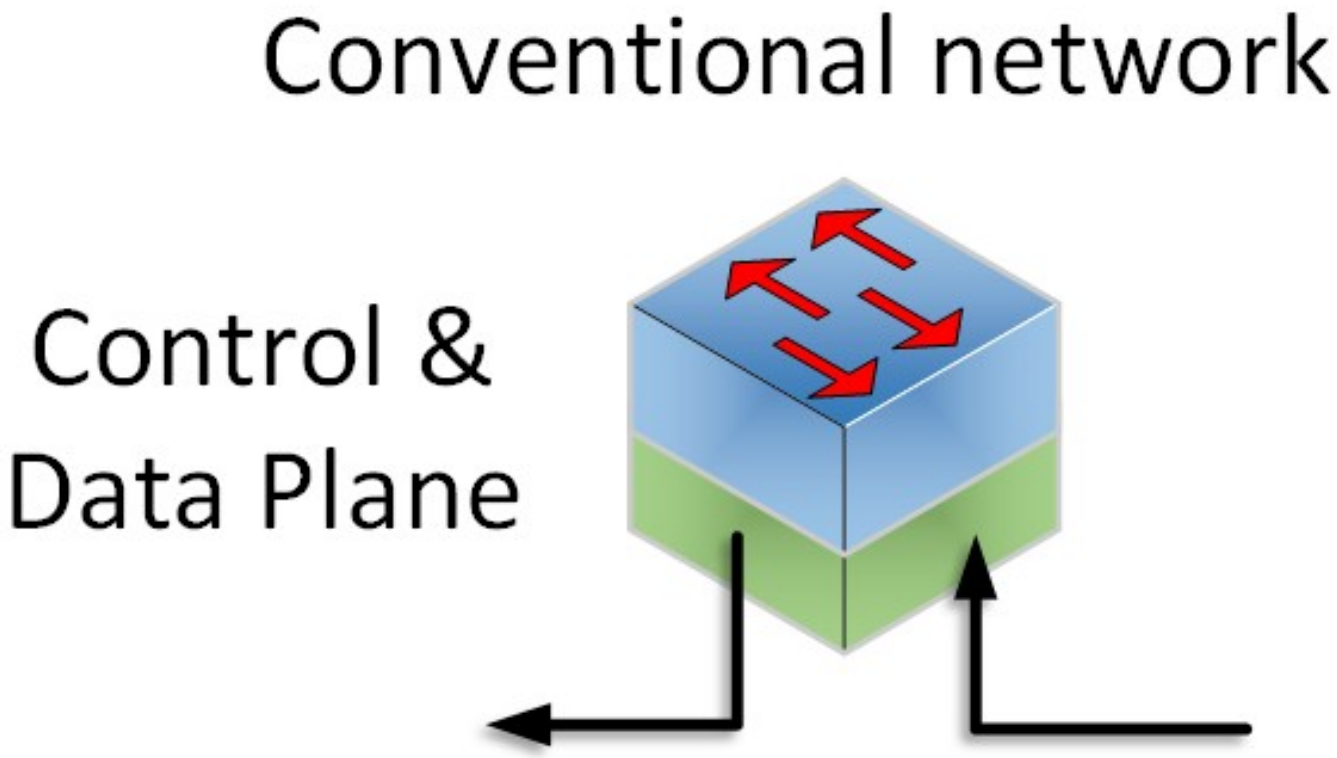
Network deception
(*Robertson et al., Achleitner et al.*)

Dynamic policy deployment
(*Shin et al.*)

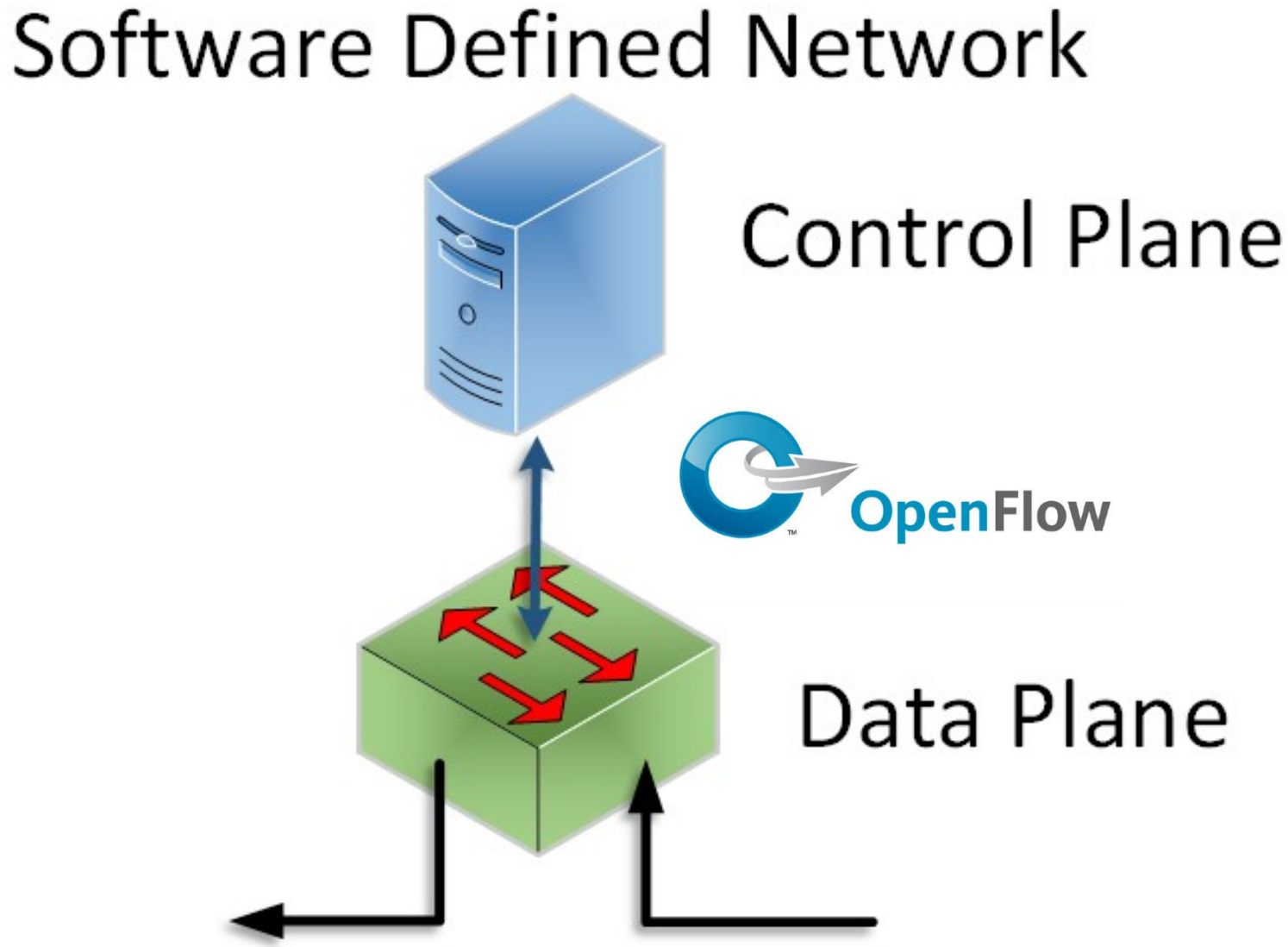
...

Jafarian et al. “Adversary-aware IP address randomization for proactive agility against sophisticated attackers,” in IEEE Conference on Computer Communications (2015)
Jafarian et al. “Openflow random host mutation: transparent moving target defense using software defined networking,” in Proceedings of the first workshop on Hot topics in software defined networks (2012)
Al-Shaer et al. “Random host mutation for moving target defense,” in Security and Privacy in Communication Networks (2013)
Robertson et al. “CINDAM: Customized Information Networks for Deception and Attack Mitigation,” in SASO Workshop (2015)
Shin et al. “Avant-guard: Scalable and vigilant switch flow management in software-defined networks,” in Proceedings of the ACM Conference on Computer & Communications Security (2013)
Achleitner et al. "Cyber Deception: Virtual Networks to Defend Insider Reconnaissance", ACM CCS International Workshop on Managing Insider Security Threats (2016)

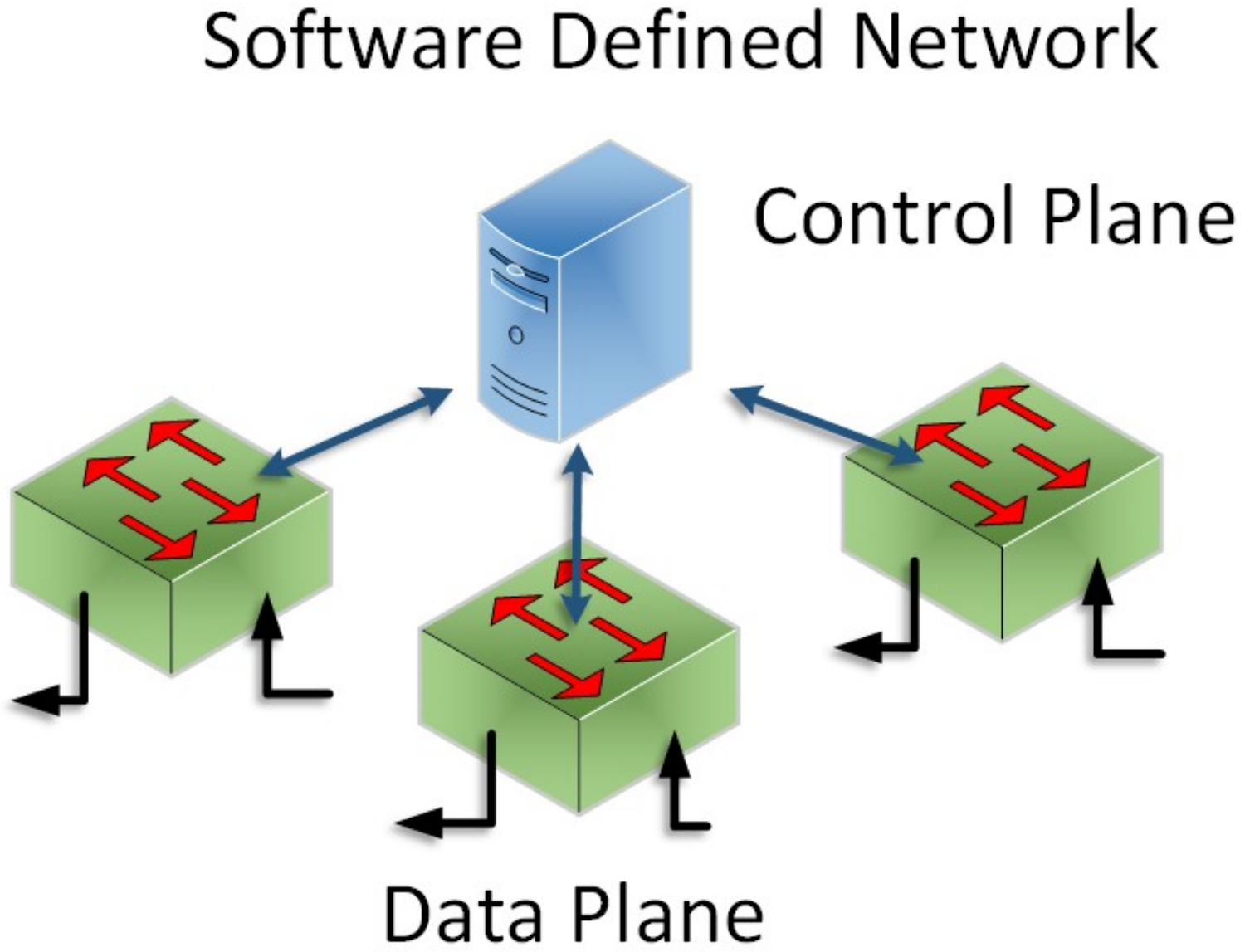
- **What is SDN?**



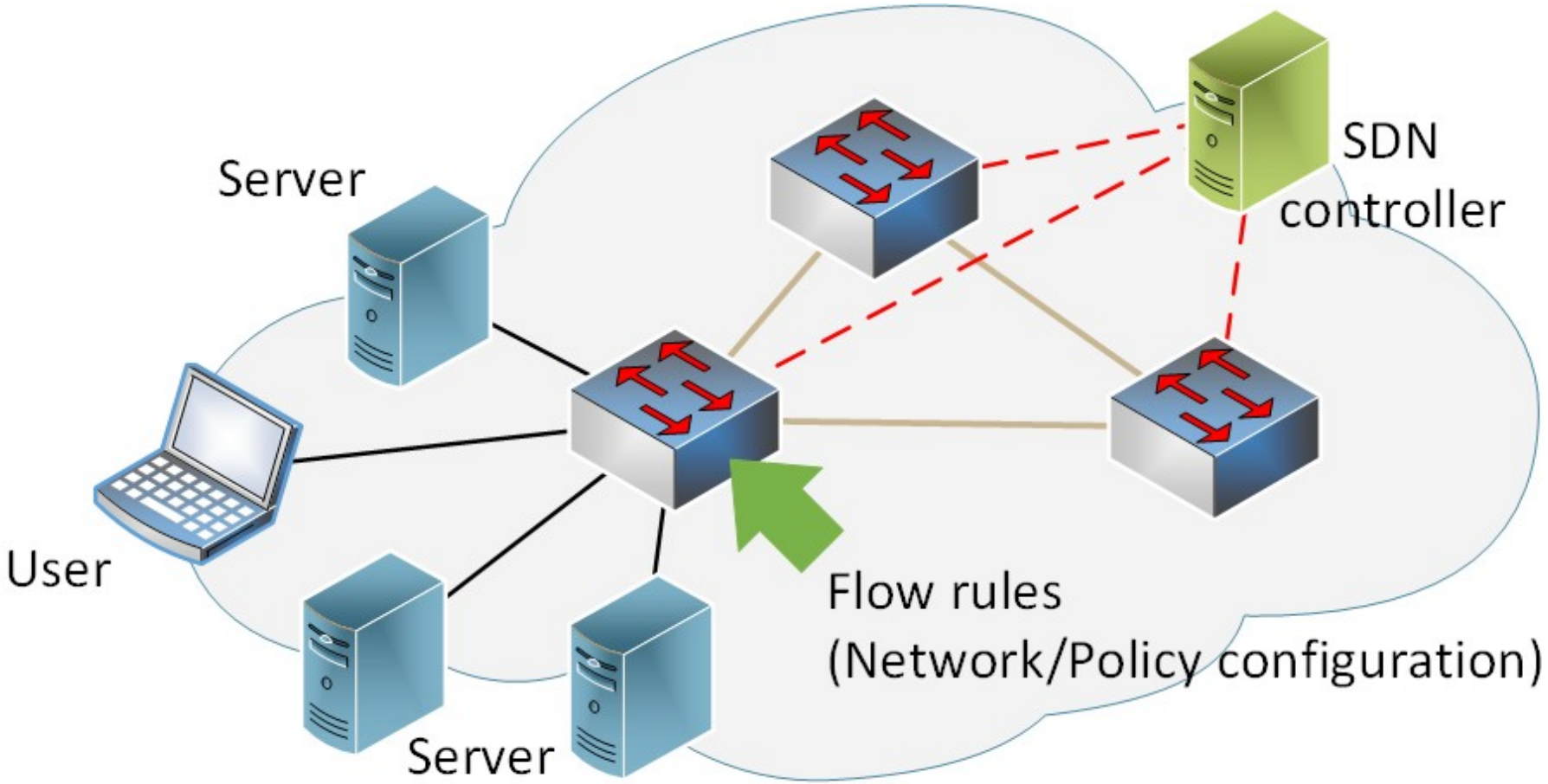
- **What is SDN?**


Software Defined Network
Control Plane
OpenFlow
Data Plane

- **What is SDN?**



- **SDN separates control- and data-plane**
- **Forwards traffic based on flow rules**



- **SDN makes forwarding decisions**

match:*Set*[*field=value*] --> action:*Set*[*action field=value*]

00:00:0A:0B:00:01

10.0.0.1

00:00:0A:0B:00:02

10.0.0.2

- **SDN makes forwarding decisions**

match:*Set*[*field=value*] --> action:*Set*[*action field=value*]

00:00:0A:0B:00:01

10.0.0.1

00:00:0A:0B:00:02

10.0.0.2

match:IPsrc=10.0.0.1, IPdst=10.0.0.2 --> action:out_port=2

- **SDN makes forwarding decisions**

match:*Set*[*field=value*] --> action:*Set*[*action field=value*]

00:00:0A:0B:00:01

10.0.0.1

00:00:0A:0B:00:02

10.0.0.2

match:IPsrc=10.0.0.1, IPdst=10.0.0.2 --> action:out_port=2

match:IPsrc=10.0.0.1 --> action:mod_IPsrc=10.0.0.10, out_port=2

- **SDN makes forwarding decisions**

match:*Set*[*field=value*] --> action:*Set*[*action field=value*]

SDN Element

00:00:0A:0B:00:01

10.0.0.1

00:00:0A:0B:00:02

10.0.0.2

match:IPsrc=10.0.0.1, IPdst=10.0.0.2 --> action:out_port=2

match:IPsrc=10.0.0.1 --> action:mod_IPsrc=10.0.0.10, out_port=2

match:IPsrc=10.0.0.1, IPdst=10.0.0.2 --> action:drop

- **SDN element can be seen as a black box**

match:*Set*[*field=value*] --> action:*Set*[*action field=value*]

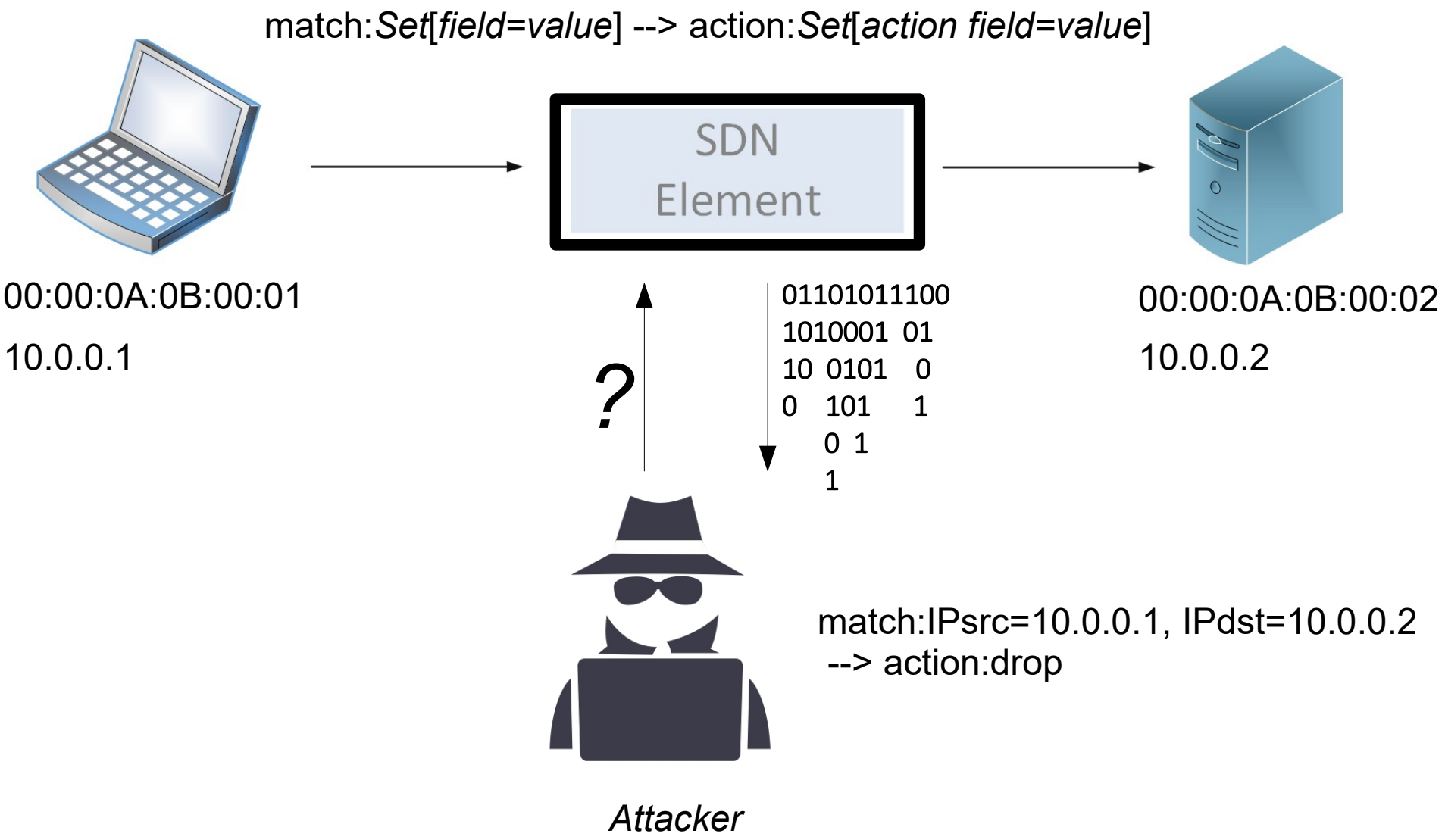
00:00:0A:0B:00:01

10.0.0.1

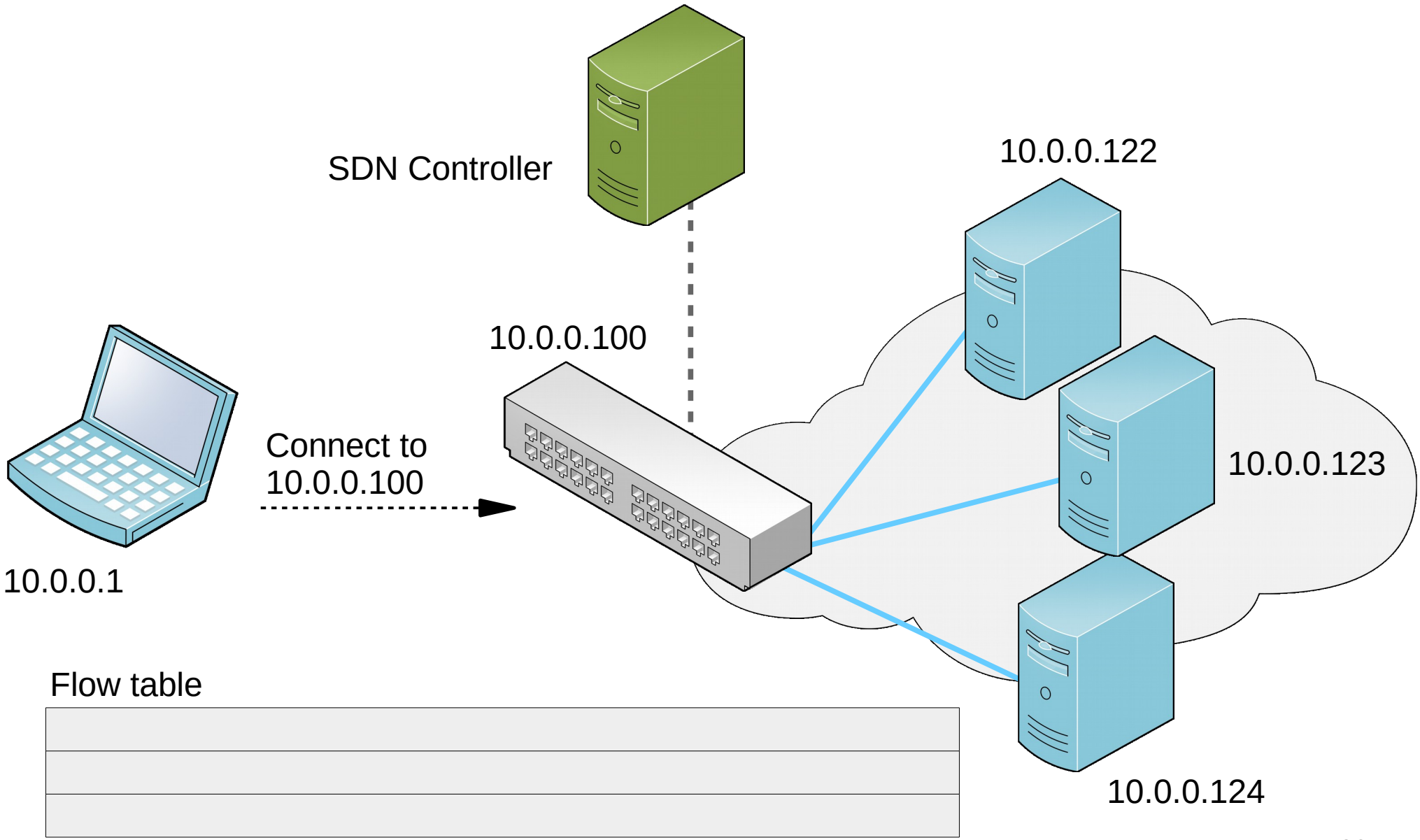
00:00:0A:0B:00:02

10.0.0.2

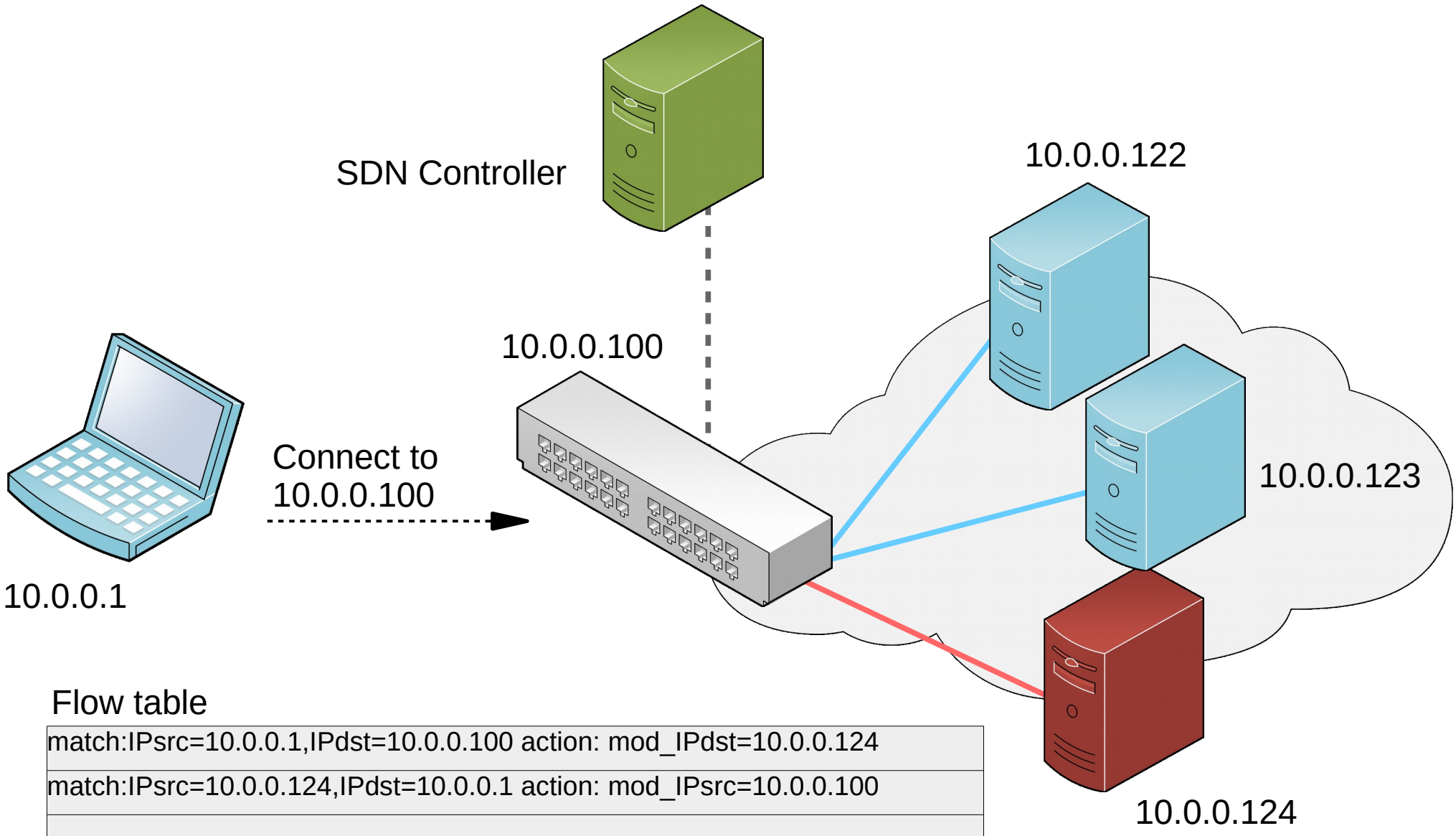
- **Can an attacker reconstruct the details of flow rules?**



- **Load Balancing as a Service**



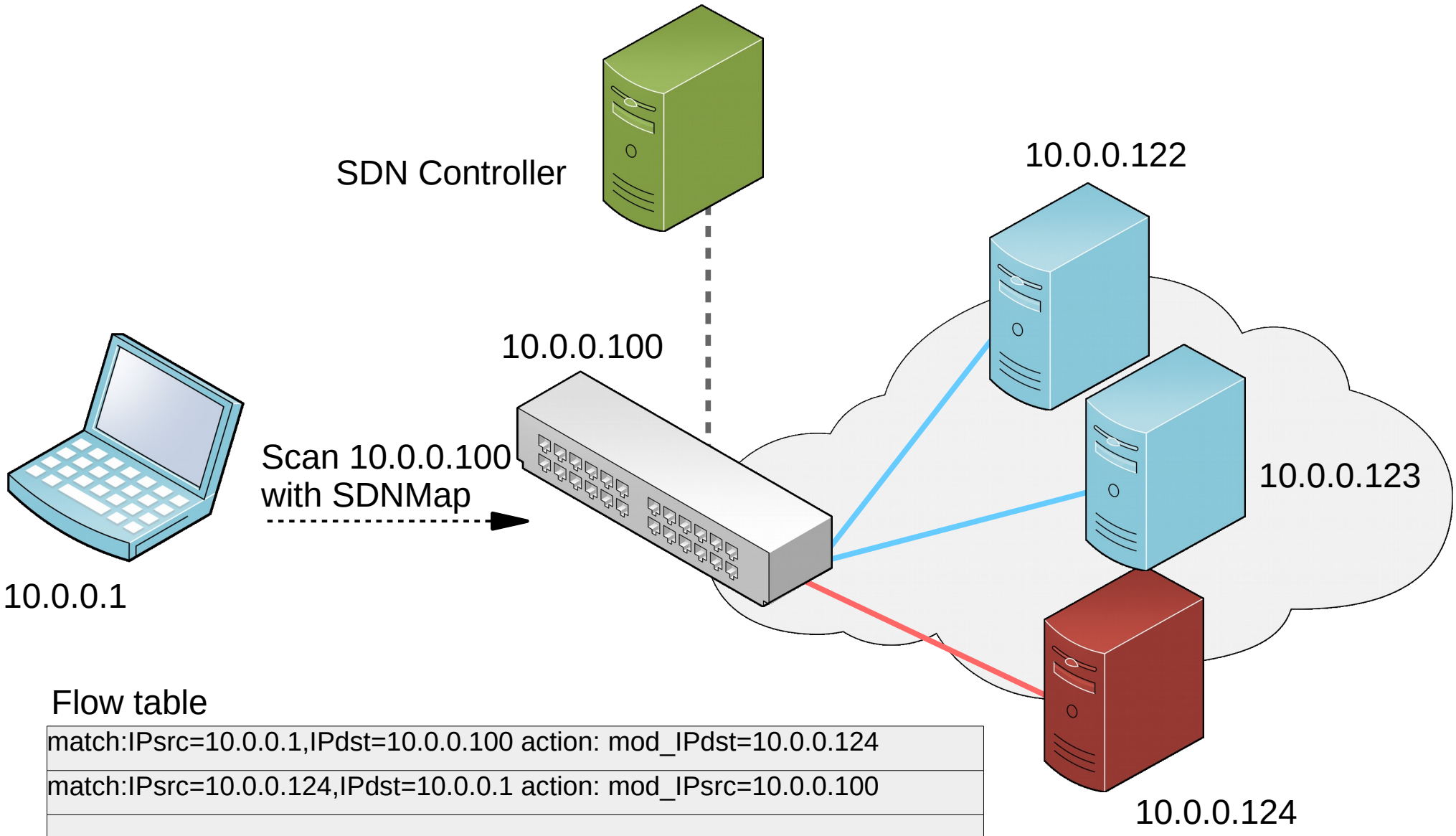
- **Load Balancing as a Service**



Flow table

match:IPsrc=10.0.0.1,IPdst=10.0.0.100 action: mod_IPdst=10.0.0.124
match:IPsrc=10.0.0.124,IPdst=10.0.0.1 action: mod_IPsrc=10.0.0.100

- **Load Balancing as a Service**

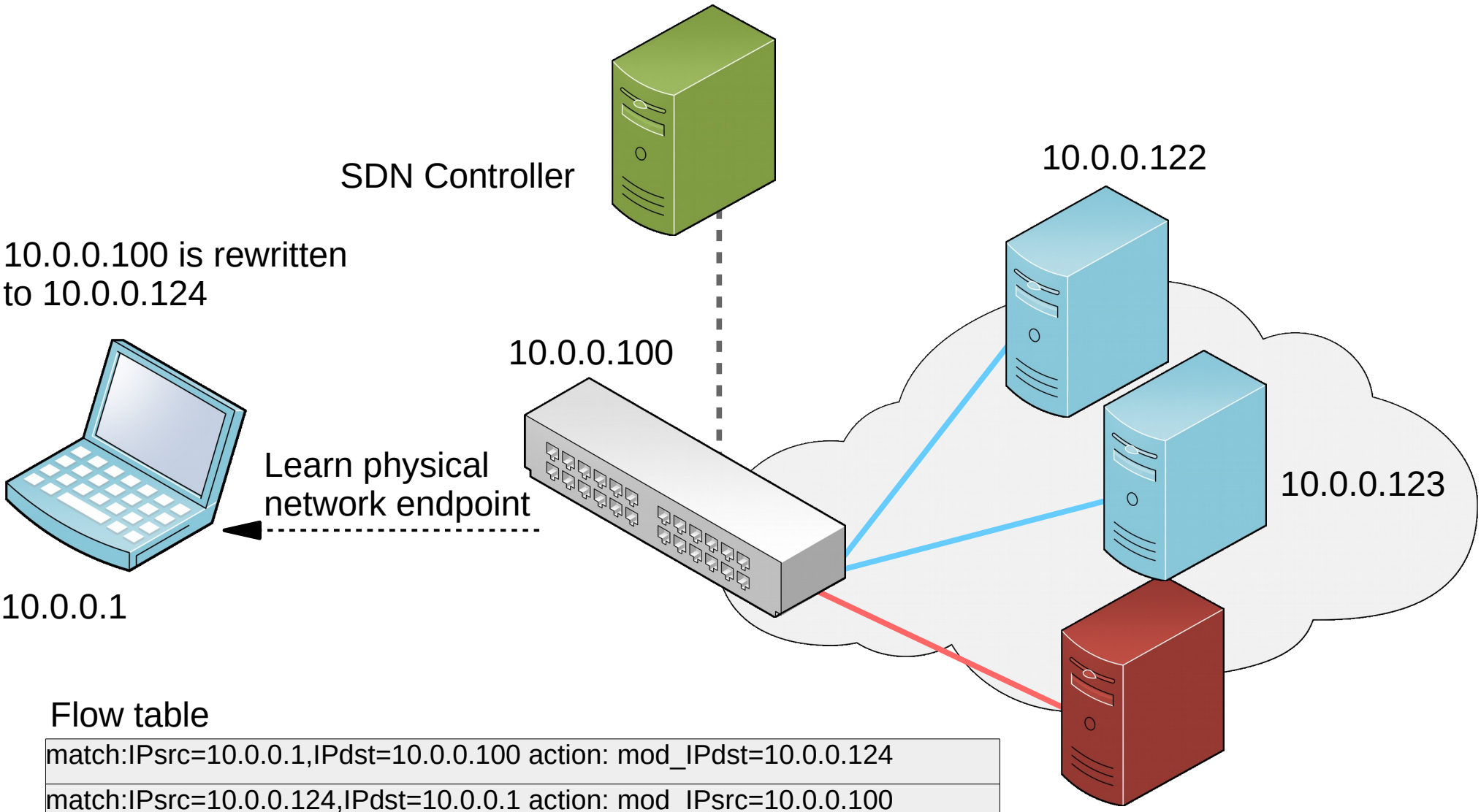


Flow table

match:IPsrc=10.0.0.1,IPdst=10.0.0.100 action: mod_IPdst=10.0.0.124
match:IPsrc=10.0.0.124,IPdst=10.0.0.1 action: mod_IPsrc=10.0.0.100

- **Load Balancing as a Service**

https://youtu.be/9v7mjMrkxHk



Flow table

match:IPsrc=10.0.0.1,IPdst=10.0.0.100 action: mod_IPdst=10.0.0.124
match:IPsrc=10.0.0.124,IPdst=10.0.0.1 action: mod_IPsrc=10.0.0.100

- **How do we reconstruct rules – IP rewriting?**

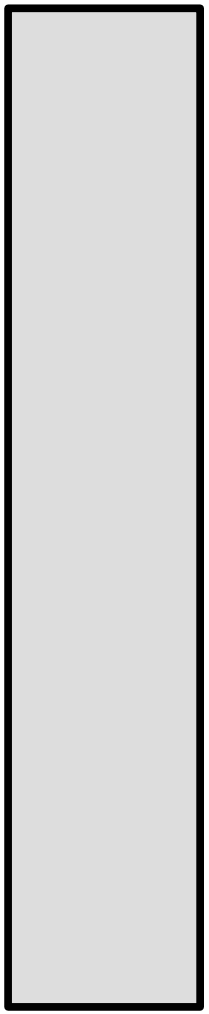
00:00:0A:0B:00:01

10.0.0.1

00:00:0A:0B:00:02

10.0.0.22 (10.0.0.2)

SDN element



UDP

IP src:	10.0.0.1
IP dst:	10.0.0.2
Port src:	345
Port dst:	56748

- **How do we reconstruct rules – IP rewriting?**

00:00:0A:0B:00:01

10.0.0.1

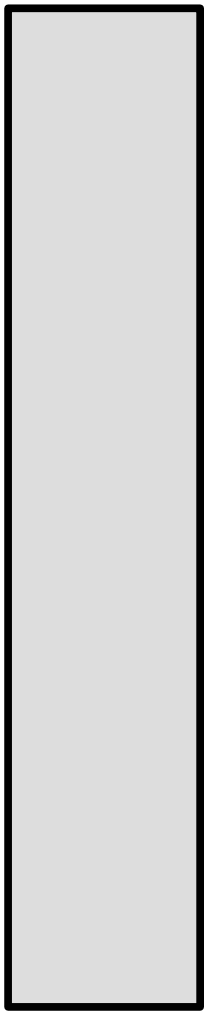
SDN element

00:00:0A:0B:00:02

10.0.0.22 (10.0.0.2)

UDP

IP src:	10.0.0.1
IP dst:	10.0.0.2
Port src:	345
Port dst:	56748



UDP received at closed port

IP src:	10.0.0.1
IP dst:	10.0.0.22
Port src:	345
Port dst:	56748

- **How do we reconstruct rules – IP rewriting?**

00:00:0A:0B:00:01

10.0.0.1

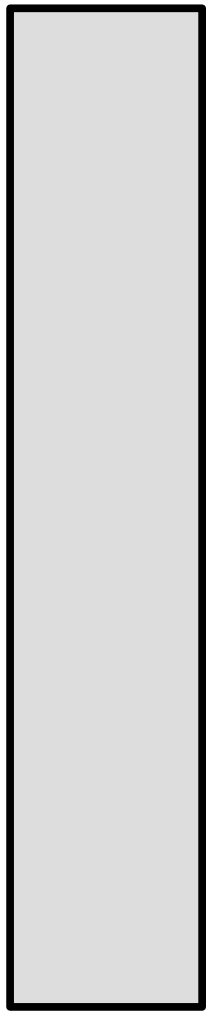
SDN element

00:00:0A:0B:00:02

10.0.0.22 (10.0.0.2)

UDP

IP src:	10.0.0.1
IP dst:	10.0.0.2
Port src:	345
Port dst:	56748



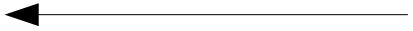
UDP received at closed port

IP src:	10.0.0.1
IP dst:	10.0.0.22
Port src:	345
Port dst:	56748

ICMP port unreachable (RFC 792)

IP src:	10.0.0.22
IP dst:	10.0.0.1

IP src:	10.0.0.1
IP dst:	10.0.0.22
Port src:	345
Port dst:	56748



- **How do we reconstruct rules – IP rewriting?**

00:00:0A:0B:00:01

10.0.0.1

SDN element

00:00:0A:0B:00:02

10.0.0.2 (10.0.0.2)

UDP

IP src:	10.0.0.1
IP dst:	10.0.0.2
Port src:	345
Port dst:	56748

UDP received at closed port

IP src:	10.0.0.1
IP dst:	10.0.0.22
Port src:	345
Port dst:	56748

ICMP port unreachable

IP src:	10.0.0.2
IP dst:	10.0.0.1

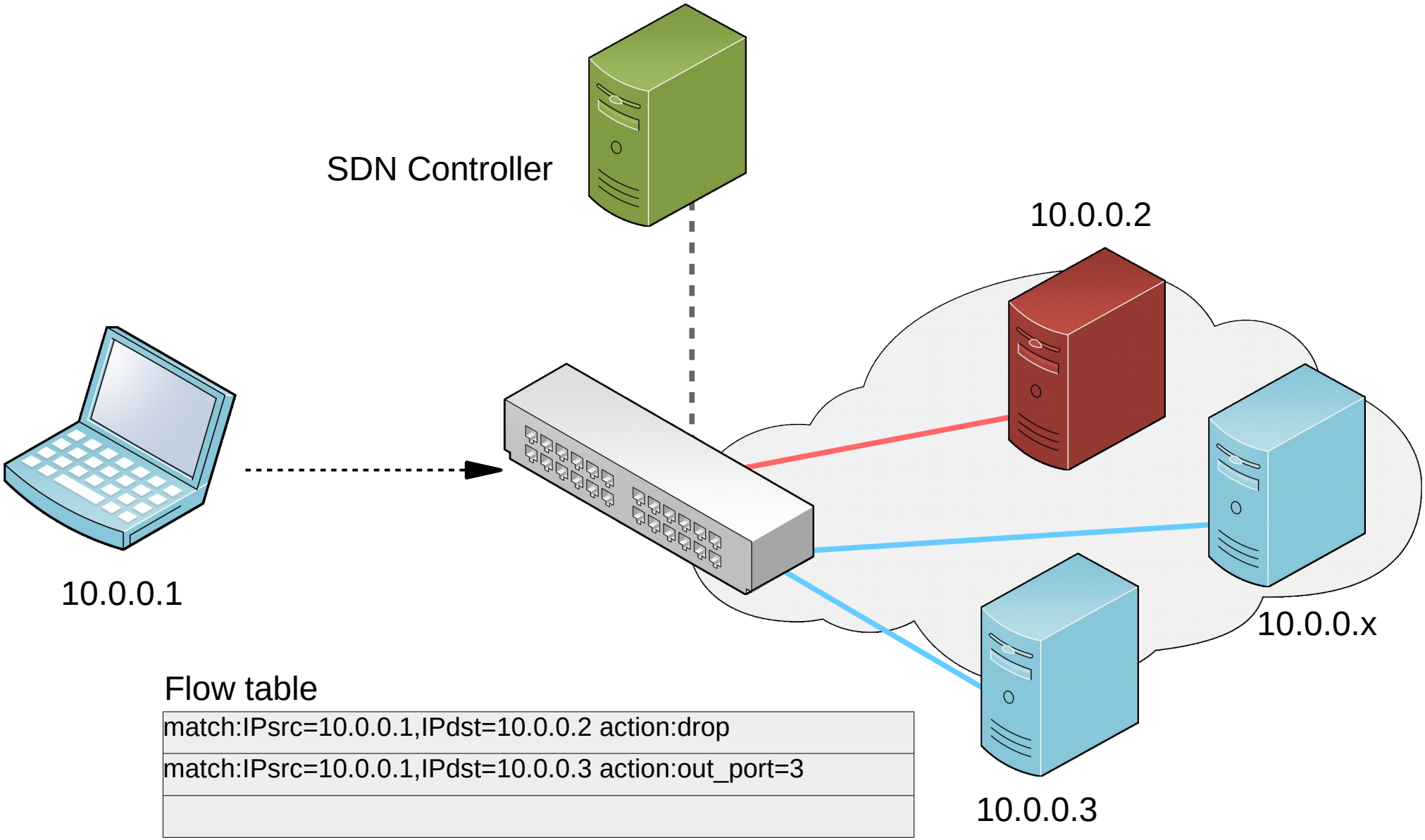
IP src:	10.0.0.1
IP dst:	10.0.0.22
Port src:	345
Port dst:	56748

ICMP port unreachable (RFC 792)

IP src:	10.0.0.22
IP dst:	10.0.0.1

IP src:	10.0.0.1
IP dst:	10.0.0.22
Port src:	345
Port dst:	56748

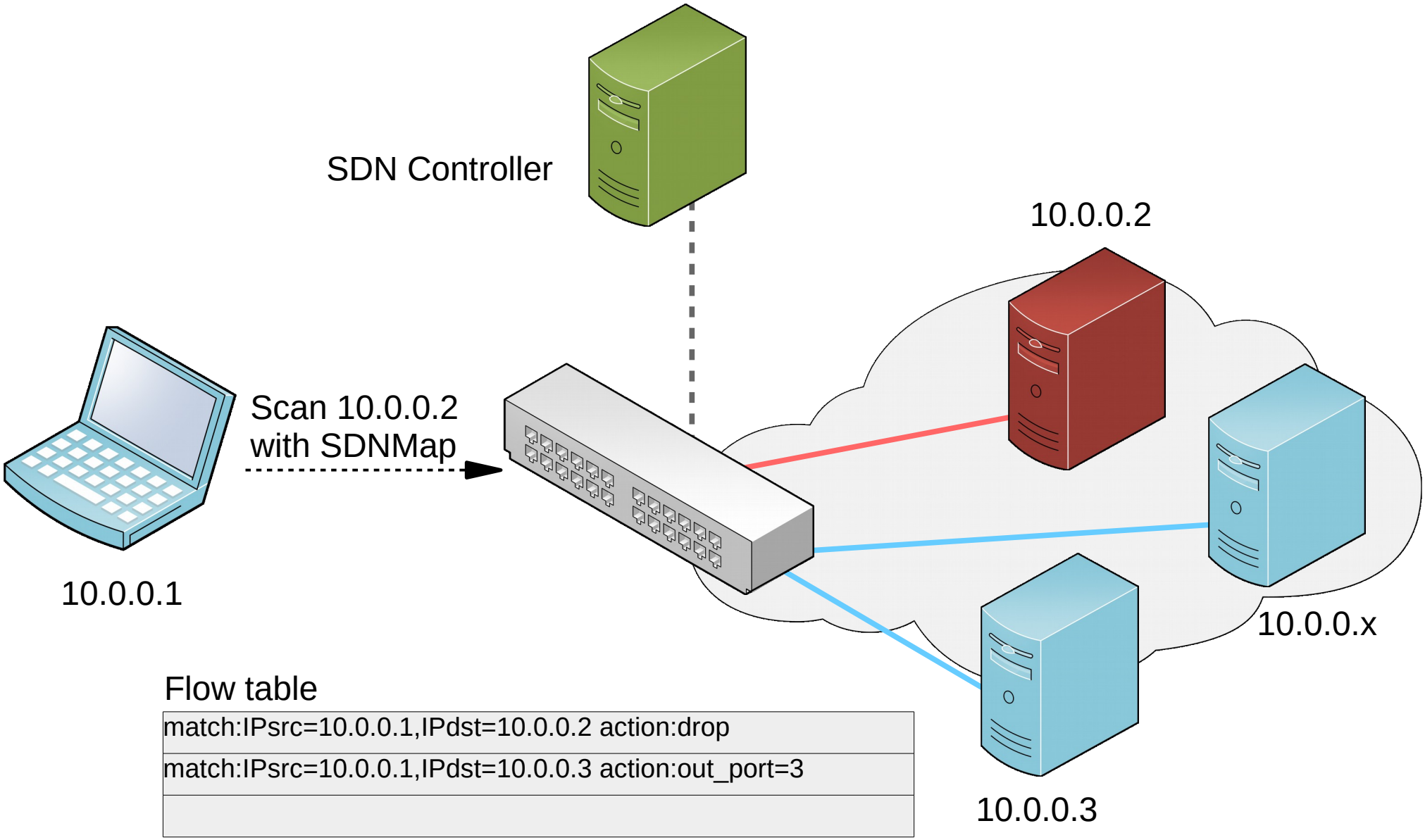
• Floodlight's Access Control List scenario



Flow table

match:IPsrc=10.0.0.1,IPdst=10.0.0.2 action:drop
match:IPsrc=10.0.0.1,IPdst=10.0.0.3 action:out_port=3

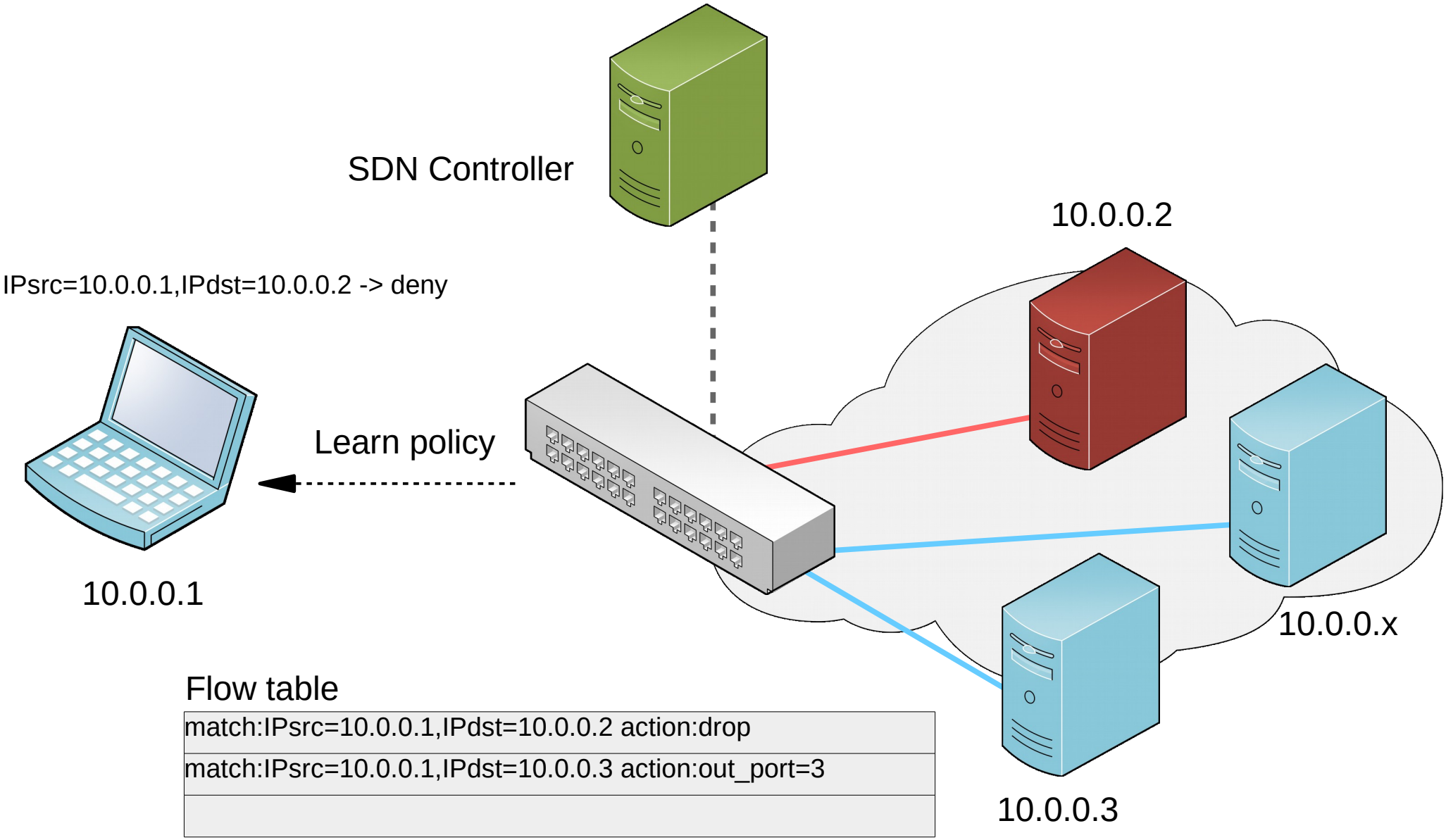
• Floodlight's Access Control List scenario



Flow table

match:IPsrc=10.0.0.1,IPdst=10.0.0.2 action:drop
match:IPsrc=10.0.0.1,IPdst=10.0.0.3 action:out_port=3

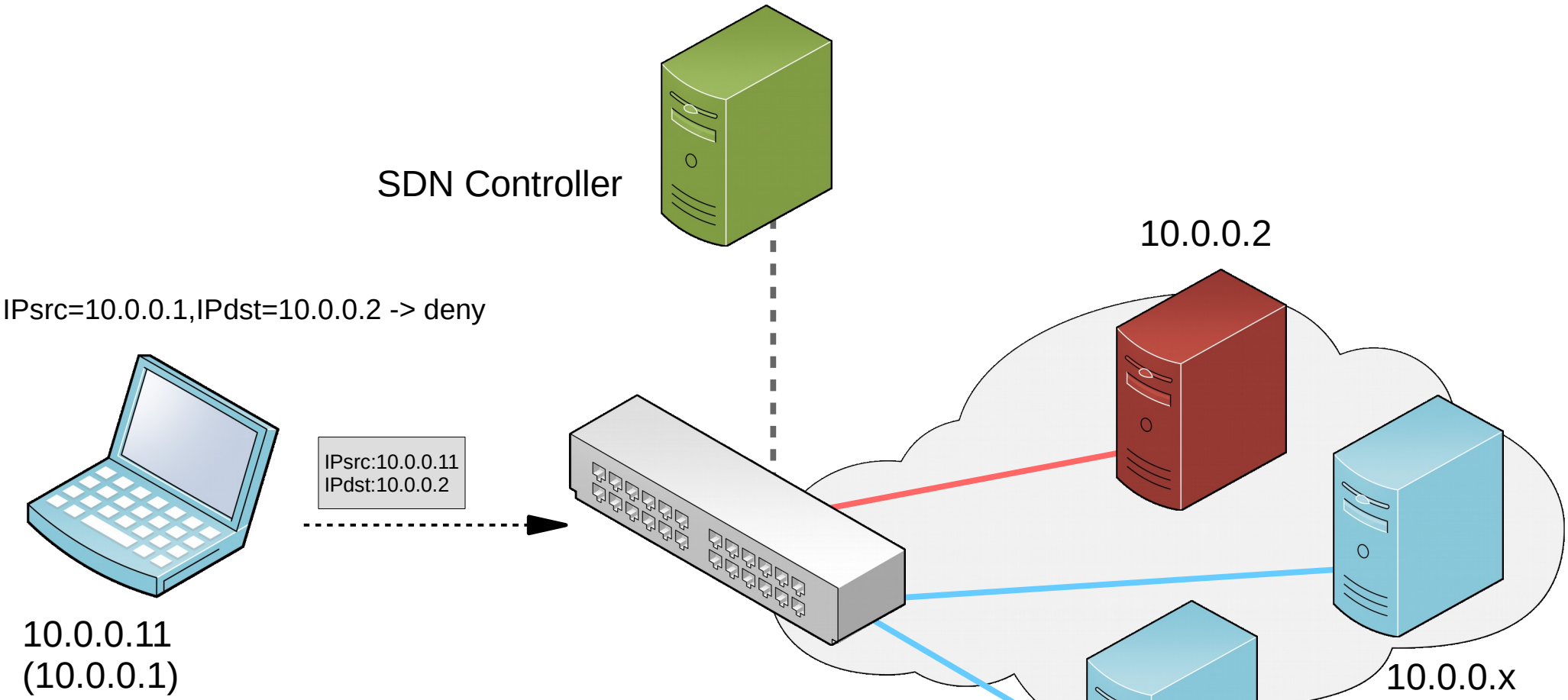
• Floodlight's Access Control List scenario



Flow table

match:IPsrc=10.0.0.1,IPdst=10.0.0.2 action:drop
match:IPsrc=10.0.0.1,IPdst=10.0.0.3 action:out_port=3

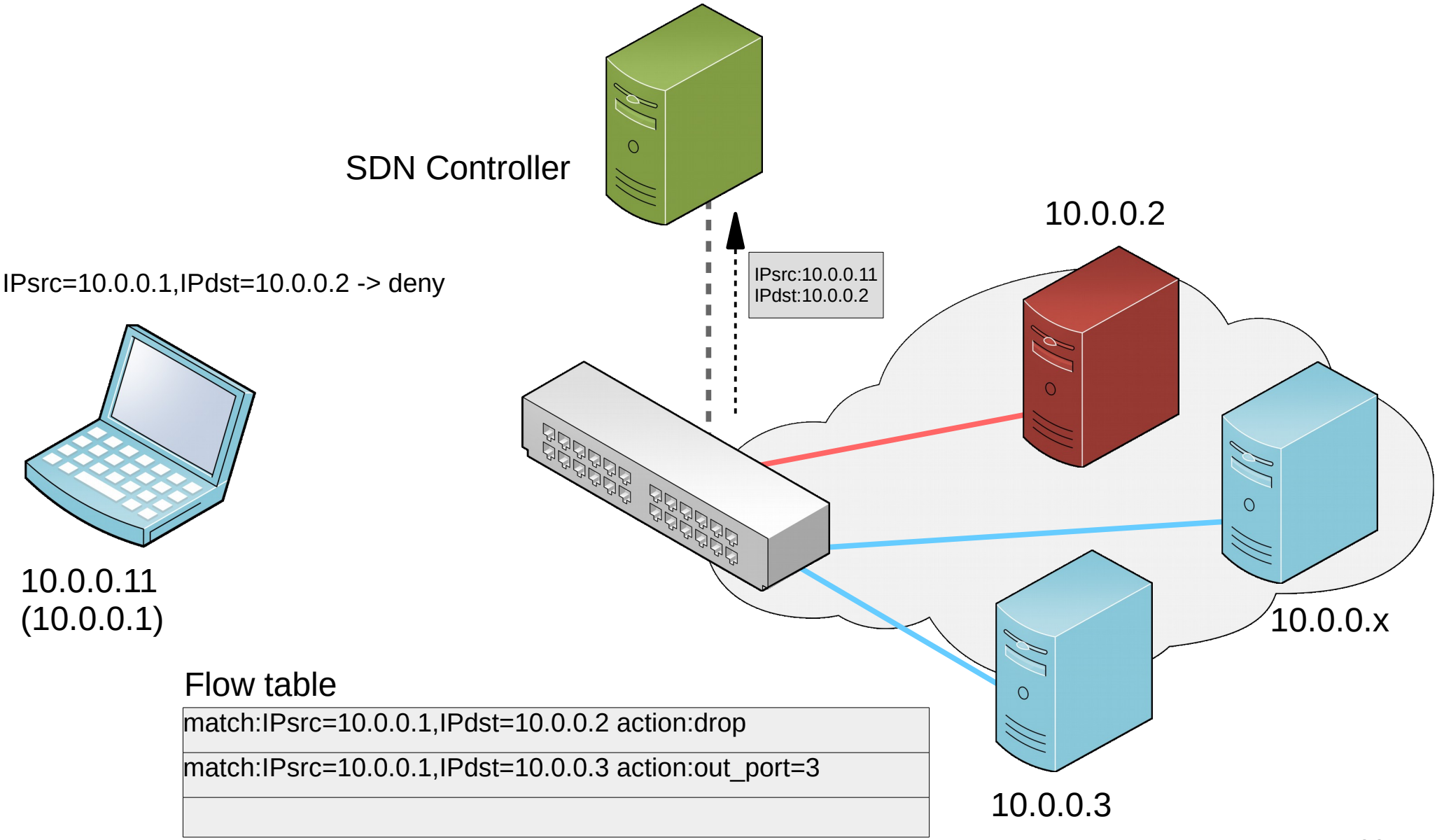
• Floodlight's Access Control List scenario



Flow table

match:IPsrc=10.0.0.1,IPdst=10.0.0.2 action:drop
match:IPsrc=10.0.0.1,IPdst=10.0.0.3 action:out_port=3

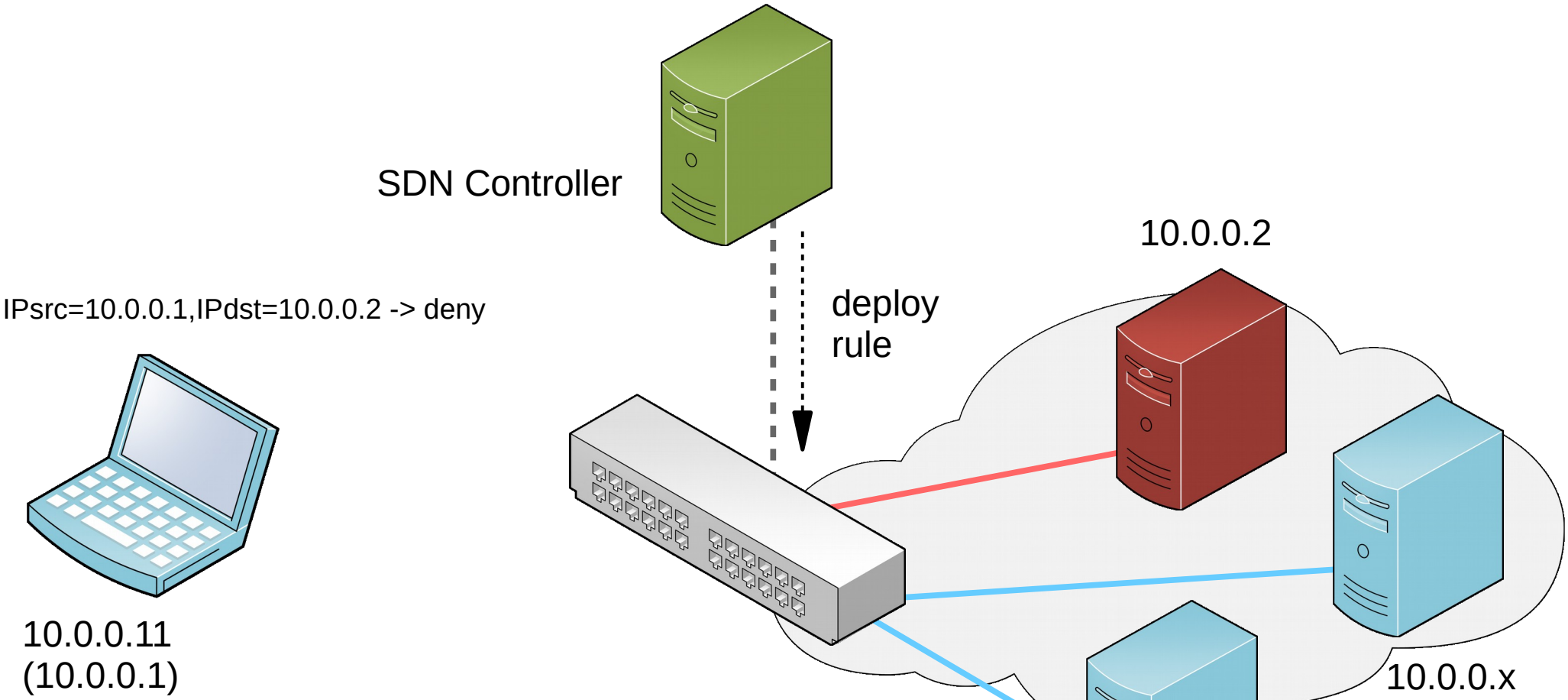
• Floodlight's Access Control List scenario



Flow table

match:IPsrc=10.0.0.1,IPdst=10.0.0.2 action:drop
match:IPsrc=10.0.0.1,IPdst=10.0.0.3 action:out_port=3

• Floodlight's Access Control List scenario

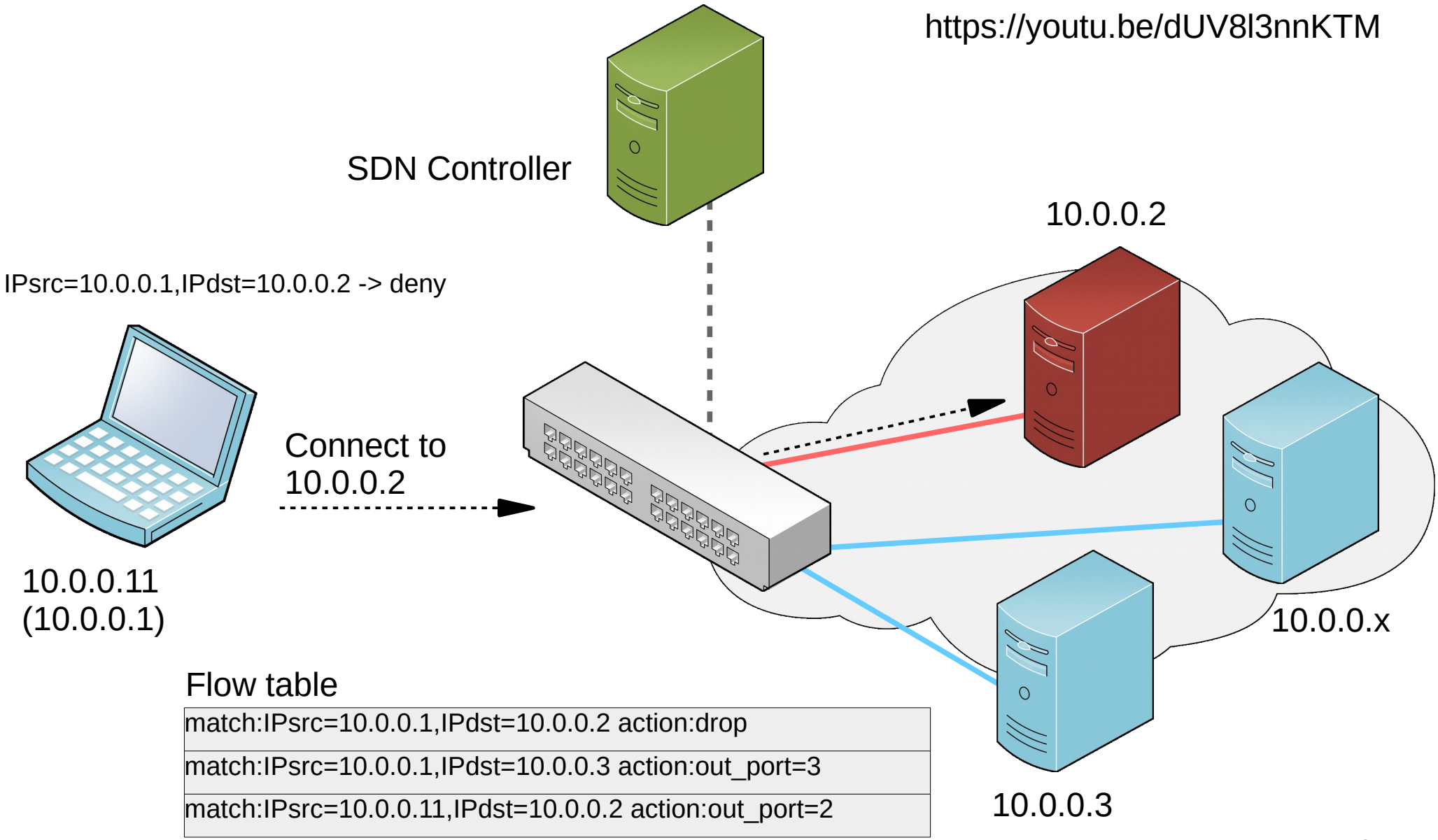


Flow table

match:IPsrc=10.0.0.1,IPdst=10.0.0.2 action:drop
match:IPsrc=10.0.0.1,IPdst=10.0.0.3 action:out_port=3
match:IPsrc=10.0.0.11,IPdst=10.0.0.2 action:out_port=2

• Floodlight's Access Control List scenario

https://youtu.be/dUV8l3nnKTM



Flow table

match:IPsrc=10.0.0.1,IPdst=10.0.0.2 action:drop
match:IPsrc=10.0.0.1,IPdst=10.0.0.3 action:out_port=3
match:IPsrc=10.0.0.11,IPdst=10.0.0.2 action:out_port=2

- **How do we reconstruct rules – IP addresses?**

00:00:0A:0B:00:01

10.0.0.1

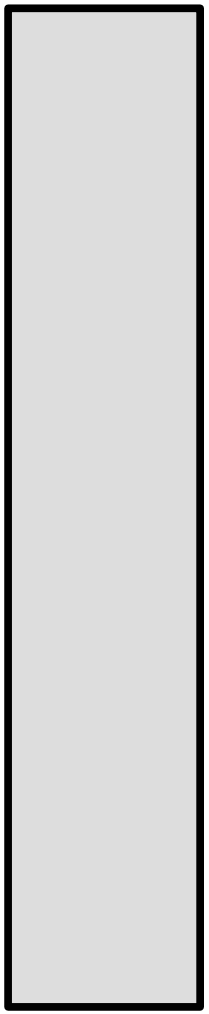
SDN element

00:00:0A:0B:00:02

10.0.0.2

Probe request

IP src:	10.0.0.1
IP dst:	10.0.0.2
MAC src:	00:00:0A:0B:00:01
MAC dst:	00:00:0A:0B:00:02



- **How do we reconstruct rules – IP addresses?**

00:00:0A:0B:00:01

10.0.0.1

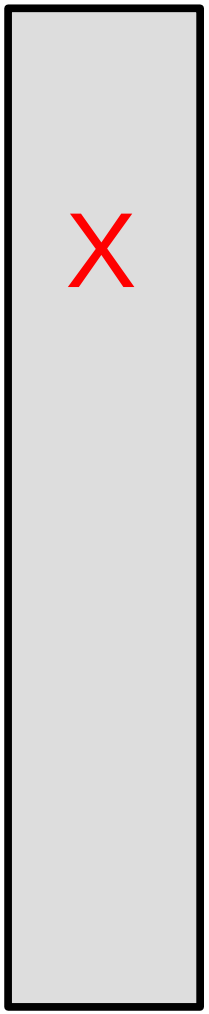
SDN element

00:00:0A:0B:00:02

10.0.0.2

Probe request

IP src:	10.0.0.1
IP dst:	10.0.0.2
MAC src:	00:00:0A:0B:00:01
MAC dst:	00:00:0A:0B:00:02



- **How do we reconstruct rules – IP addresses?**

00:00:0A:0B:00:01

10.0.0.1

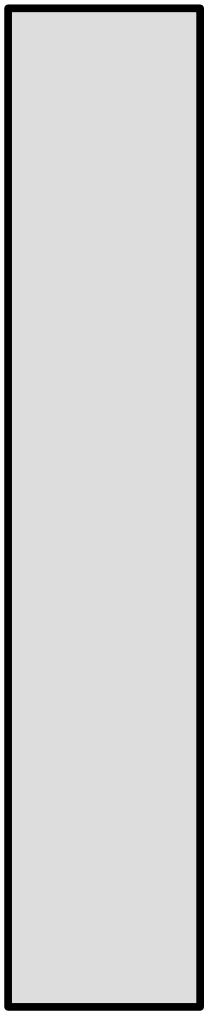
SDN element

00:00:0A:0B:00:02

10.0.0.2

Probe request

IP src:	10.0.0.11
IP dst:	10.0.0.2
MAC src:	00:00:0A:0B:00:01
MAC dst:	00:00:0A:0B:00:02



- **How do we reconstruct rules – IP addresses?**

00:00:0A:0B:00:01

10.0.0.1

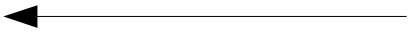
SDN element

00:00:0A:0B:00:02

10.0.0.2

Probe request

IP src:	10.0.0.11
IP dst:	10.0.0.2
MAC src:	00:00:0A:0B:00:01
MAC dst:	00:00:0A:0B:00:02



ARP request

ARP BROADCAST
“Who has?”
IP address 10.0.0.11

- **How do we reconstruct rules – IP addresses?**

00:00:0A:0B:00:01

10.0.0.1

SDN element

00:00:0A:0B:00:02

10.0.0.2

Probe request

IP src:	10.0.0.11
IP dst:	10.0.0.2
MAC src:	00:00:0A:0B:00:01
MAC dst:	00:00:0A:0B:00:02

ARP request

ARP BROADCAST
"Who has?"
IP address 10.0.0.11

ARP request

ARP BROADCAST
"Who has?"
IP address 10.0.0.11

By receiving the ARP request, sender can determine that the correct IP src is checked in the flow rule!

- **Many security issues arise with the possibility of SDN rule reconstruction**

Reconstruction Scenarios	**Applications/Deployments**
ACL's	Floodlight OpenSource SDN controller
Firewalls	Floodlight OpenSource SDN controller
Moving Target Defense	OpenFlow random host mutation INFOCOM 2015 HotSDN 2012
Role-based access control	Brocade SDN configuration scenarios
Load Balancing as a Service	OpenStack Quantum LBaas

SDNMap reconstructed flow rule fields

OpenFlow field	Type	SDNMap
Ingress port (SIP) (used/not used)	M	✓
MAC destination address (HWd)	M	✓
MAC source address (HWs)	M	✓
Ethernet type (PT)	M	✓(ARP, IP)
IPv4 protocol (PT)	M	✓(ICMP, TCP, UDP)
IPv4 source address (IPs)	M	✓
IPv4 destination address (IPd)	M	✓
TCP/UDP source port (POs)	M	✓
TCP/UDP destination port (POd)	M	✓
Egress action (FA) (forward/drop)	A	✓
Modify IPv4 src address (rIPs)	A	✓
Modify IPv4 dst address (rIPd)	A	✓

Defending SDN rule reconstruction

- Prevent ARP spoofing

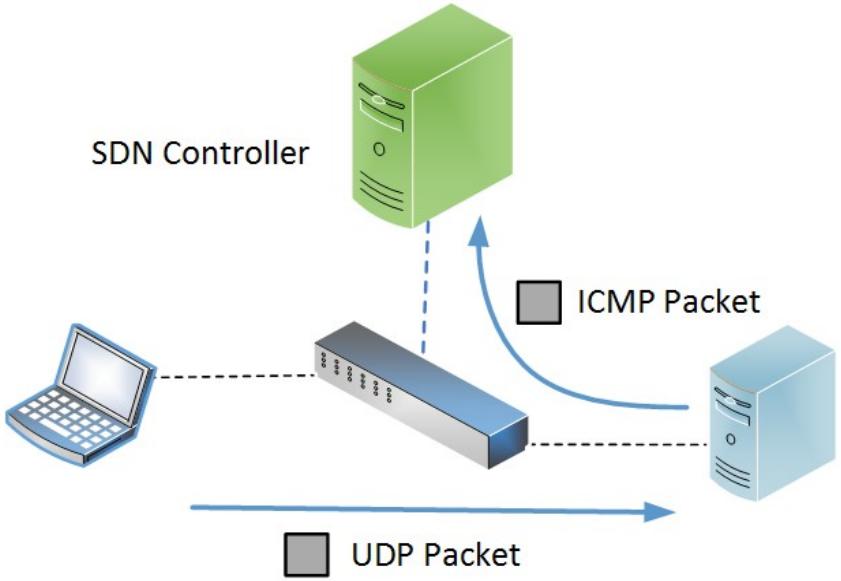
Defending SDN rule reconstruction

- Prevent ARP spoofing
  → Alternative: ICMP redirection

Defending SDN rule reconstruction

- Prevent ARP spoofing
  → Alternative: ICMP redirection

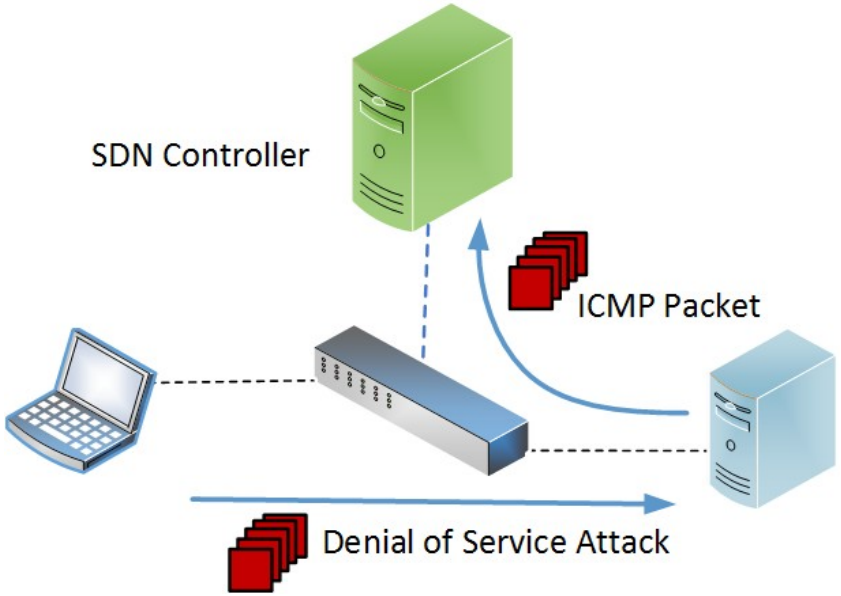
- Rewrite nested packets in controller



Defending SDN rule reconstruction

- Prevent ARP spoofing
  → Alternative: ICMP redirection

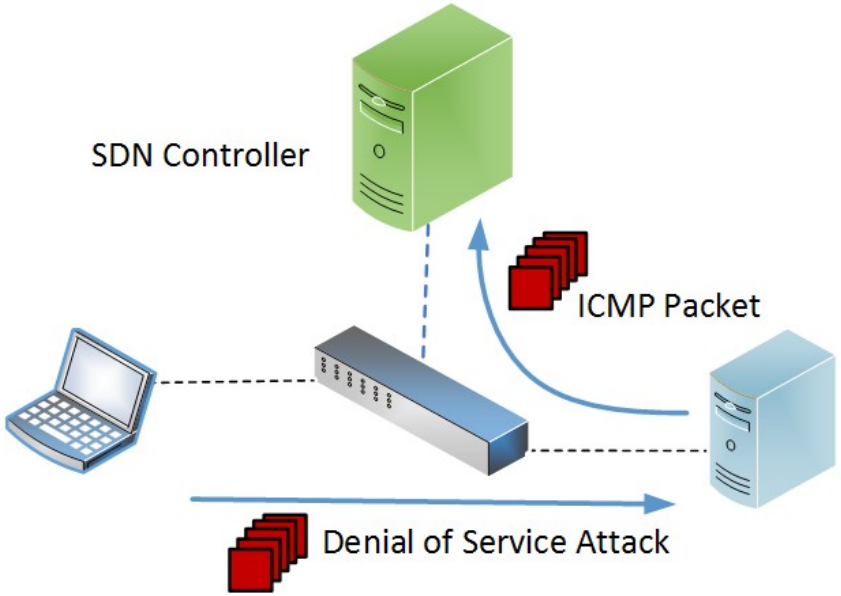
- Rewrite nested packets in controller



Defending SDN rule reconstruction

- Prevent ARP spoofing
  → Alternative: ICMP redirection

- Rewrite nested packets in controller



- Specify secure policies for flow rule construction

Paper:

Adversarial Network Forensics in Software Defined Networking

Stefan Achleitner, Thomas La Porta, Trent Jaeger, Patrick McDaniel

2017 ACM Symposium on SDN Research (SOSR)
@Open Network Summit 2017
Best Student Paper Award

Thank you!

Contact:
stefan.achleitner@cse.psu.edu

www.stefanachleitner.com