QUEEN'S UNIVERSITY BELFAST

CSIT

CENTRE FOR SECURE INFORMATION TECHNOLOGIES


CSIT
CENTRE
FOR SECURE
INFORMATION
TECHNOLOGIES
SDN AND NFV
SECURITY
DR. SANDRA SCOTT-HAYWARD, QUEEN'S UNIVERSITY BELFAST
COINS SUMMER SCHOOL, 23 JULY 2018

Queen’s University Belfast – Lanyon Building

Est. 1845

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Centre for Secure Information Technologies (CSIT)

CSIT is the UK's Innovation and Knowledge Centre for Cybersecurity

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Centre for Secure Information Technologies (CSIT)

Member of the UK **CYBER GROWTH PARTNERSHIP** (CGP) STEERING BOARD

90 PEOPLE

DIRECTOR, 16 ACADEMICS
16 ENGINEERS, 5 BUS. DEV.,
15 PDRAs, 29 PhDs, IT/Clerical 9

8 Spin-outs created, start-ups/scale-ups supported

Nucleated the Belfast Cyber Cluster (now 38 companies with >1,200 new jobs)

HOST THE ANNUAL **WORLD CYBER SECURITY TECHNOLOGY RESEARCH SUMMIT**

PART OF RESEARCH COUNCILS UK RCUK

PARTNERSHIP IN CONFLICT CRIME AND SECUIRTY RESEARCH PROGRAMME

EST. 2009

BASED IN THE ECIT INSTITUTE
QUEEN'S UNIVERSITY BELFAST

INITIAL FUNDING OVER £30M >

£30M

Additional £15M won in competitive tendering

IN 2015, PHASE 2 CORE FUNDING OF £14M SECURED, WHICH (OVER NEXT 5 YEARS) WILL LEVERAGE

>£38M

THE QUEEN'S ANNIVERSARY PRIZES
FOR HIGHER AND FURTHER EDUCATION
2015

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Research Area: Data Security

Professor Máire O'Neill - Research Director

- **Quantum Safe Cryptography**
  - *Physically secure efficient quantum-safe hardware and software designs, leads H2020 €3.8M SAFEcrypto Project*
- **Cryptographic hardware and software architectures**
  - *Including lightweight crypto*
- **Physical Unclonable Functions for M2M and IoT authentication**
  - *Strong PUF, Software PUF, resistance to SCA/Modelling attacks*
- **Side Channel Analysis**
  - *Including Machine Learning /Deep Learning SCA*
- **Hardware Trojan detection**

SAFE crypto

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Research Area: Networked Systems Security

Professor Sakir Sezer - Research Director

- **Network Security**
  - *Intrusion detection, WEB security, DDoS detection*
- **Virtual Networks**
  - *including Software Defined Network security*
- **Cloud Computing Security**
  - *VM security , secure segregation, hypervisor security etc.*
- **Mobile & IoT security**
  - *Security policy enforcement, Android Malware etc.*
- **Critical Infrastructure Security**
  - *SCADA, Smart Grid intrusion prevention etc.*
- **Malware/Botnet defence**
  - *Obfuscation strategies, detection algorithms, reverse engineering*

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Research Area: Security Analytics and Event Mgmt.

Dr Paul Miller - Research Director

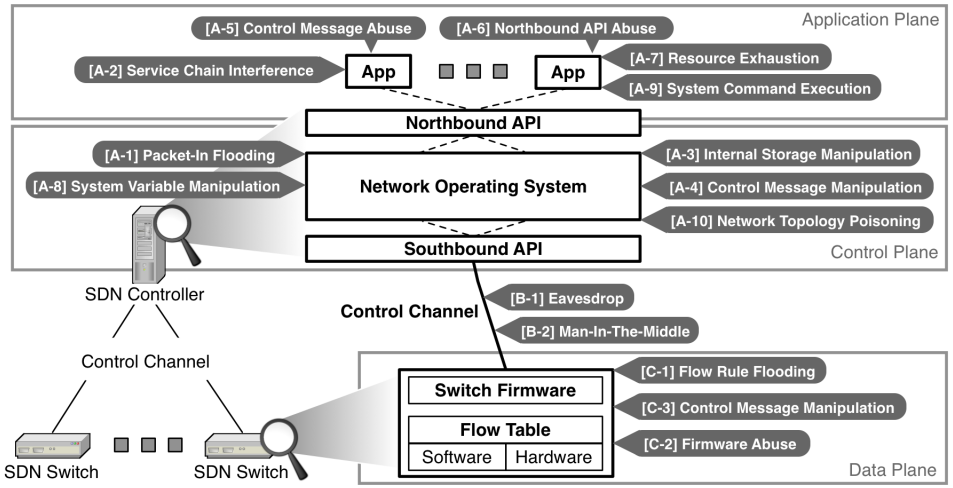
- **Deep learning neural networks**
  - *Android malware detection*
- **Graph Mining**
  - *Network Intrusion Detection and Insurance Fraud Detection*
- **Event Reasoning**
  - *Alert correlation for total network defence*
- **Multimedia content analysis**
  - *Open source intelligence, cyber-physical security*

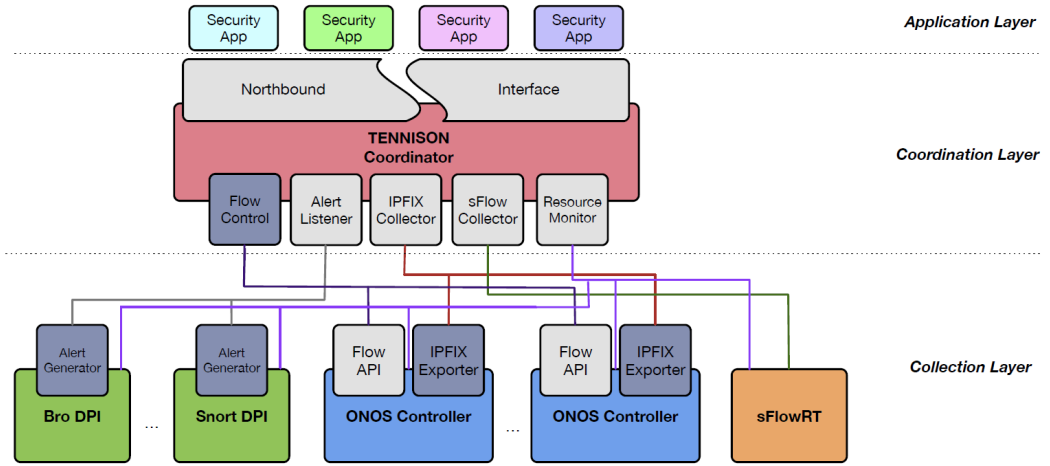
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

SDNFV Security Research - Objectives

Identifying, raising awareness, and recommending solutions to potential vulnerabilities in SDNFV network design and deployment.

Exploring scalable, analytics-based monitoring and forensics capabilities, and security solutions for these new network architectures





CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Agenda

Morning Session: 9.30am – 1pm

1. What is SDN?
2. What is OpenFlow/P4?
   Hands-On SDN – Mininet/ONOS
3. Attacks and Vulnerabilities in SDN
4. Solutions to Security Issues in SDN
   Demo - AAA
5. SDN Controller Security evolution
   Demo- DELTA

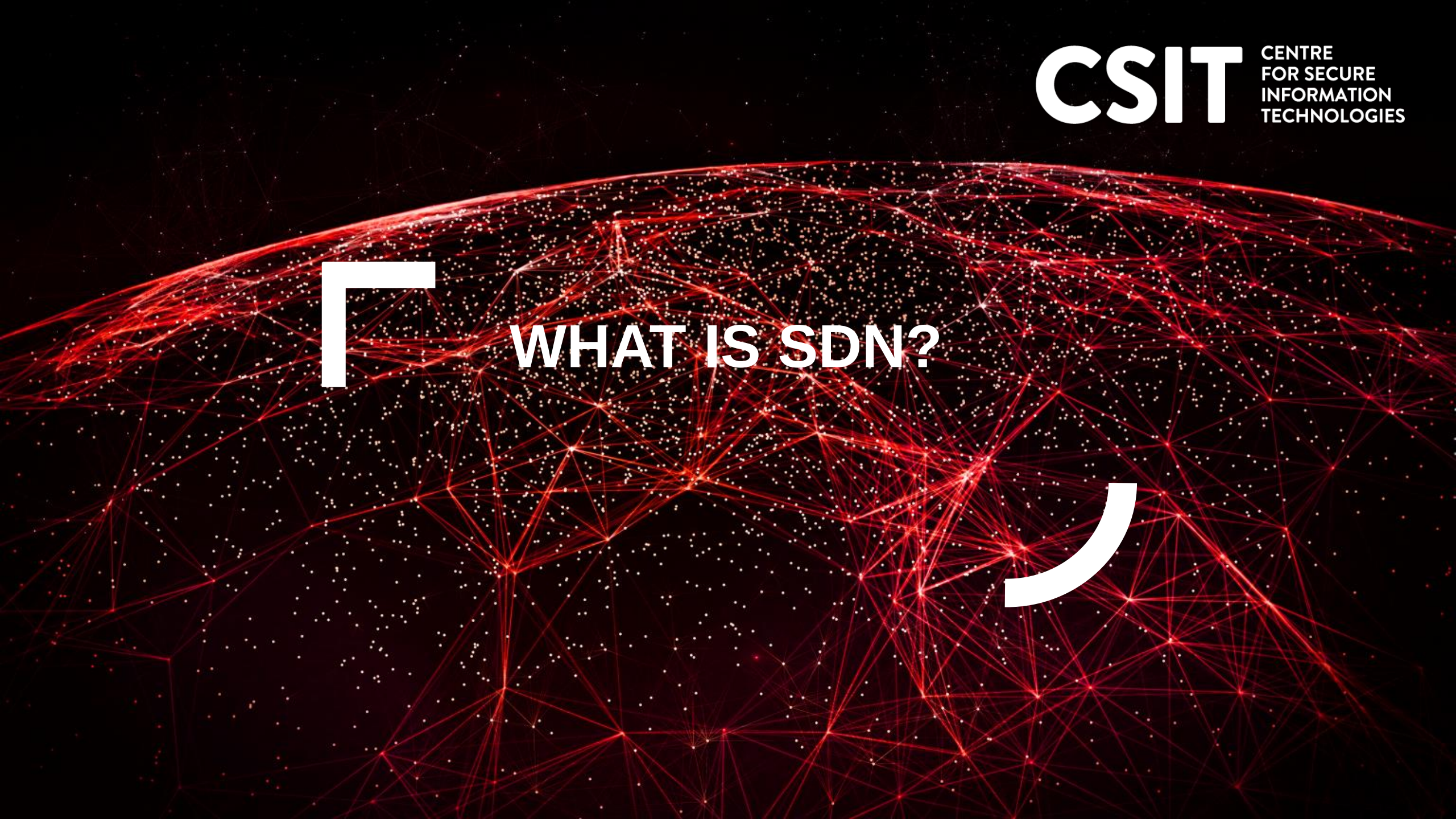
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Agenda

Evening Session: 5pm – 7pm

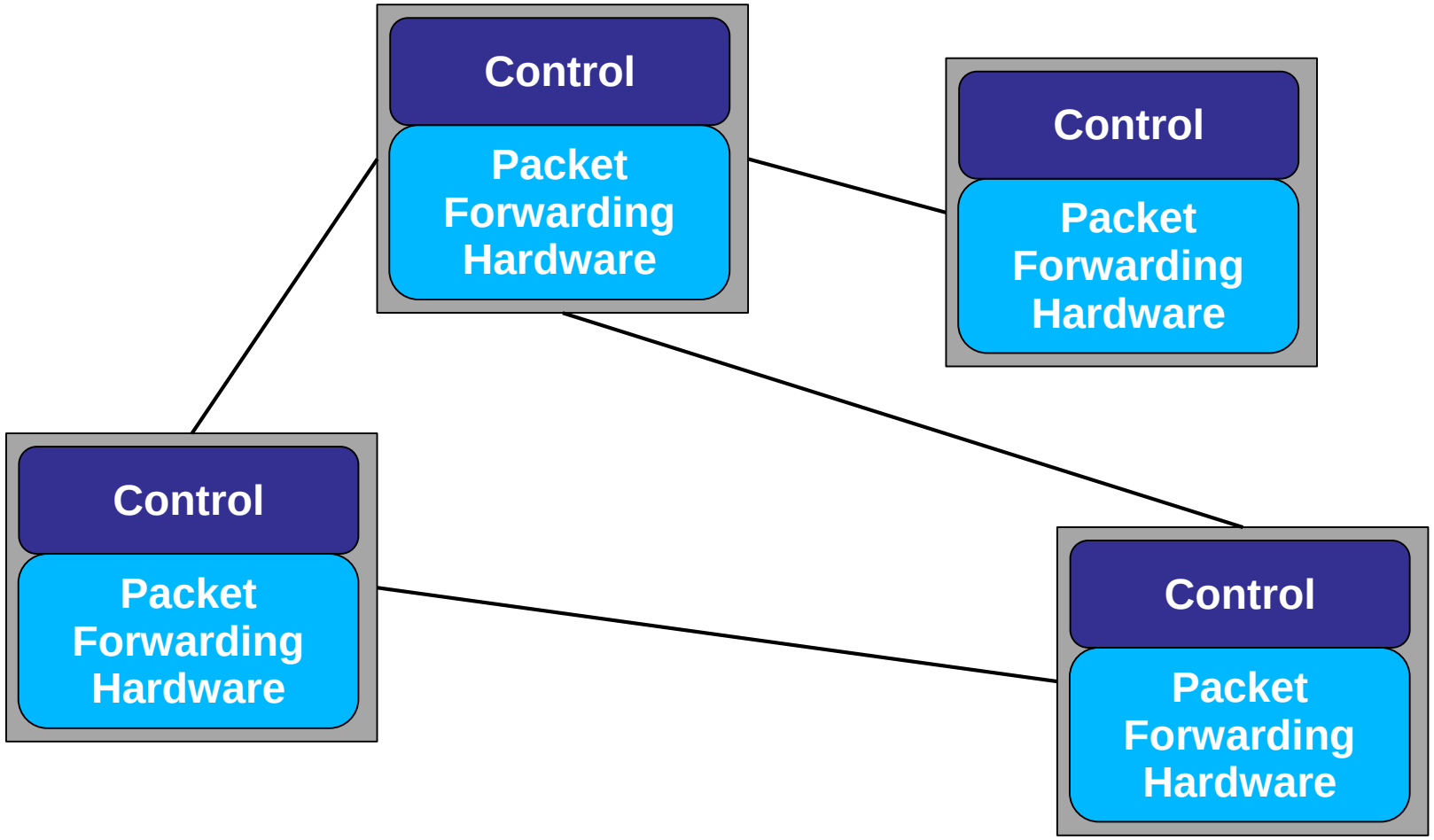
6. Network Security Enhancements using SDN
7. Stateful Security Mechanisms
   Demo – OFMTL-SEC
7. Future Directions a.k.a. Buzzword Bingo ☺

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES


CSIT
CENTRE
FOR SECURE
INFORMATION
TECHNOLOGIES
WHAT IS SDN?

Traditional Network

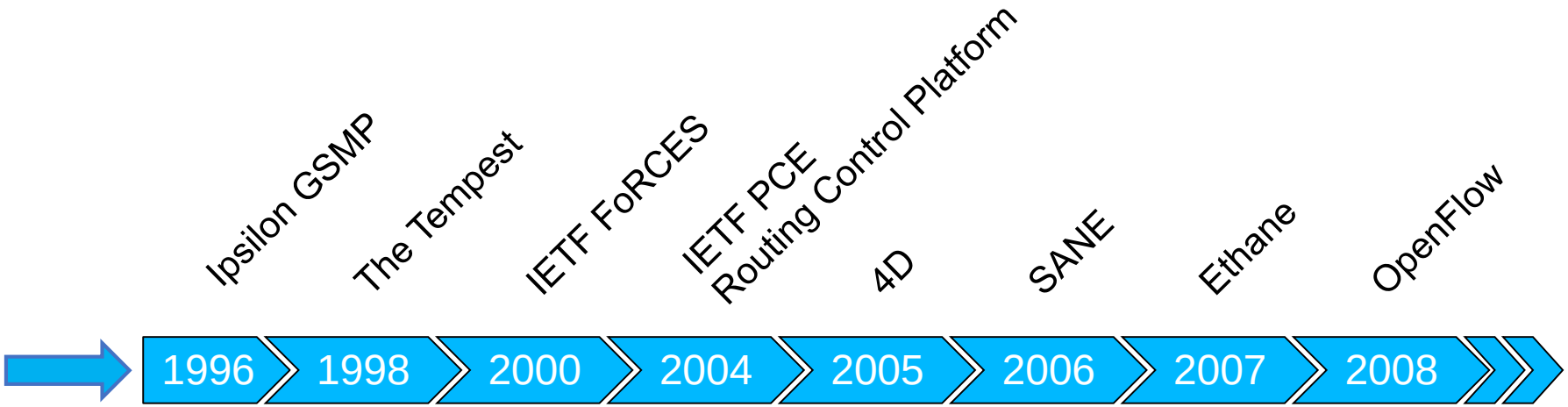
Control and Data Planes combined in Network Elements:



CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

SDN Evolution

Driven by desire to provide user-controlled management of forwarding in network nodes



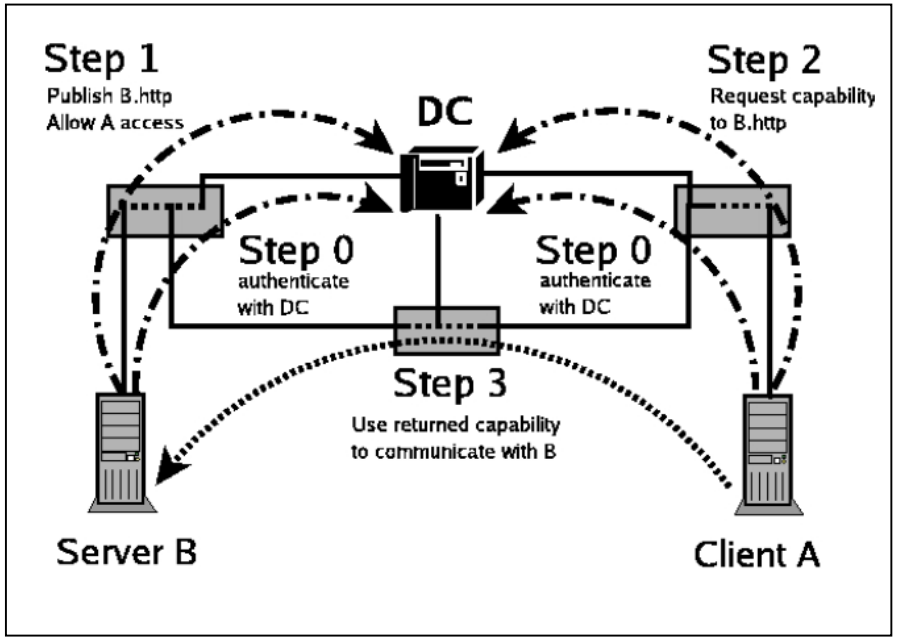
Software-Defined Networking

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

SANE Architecture

SANE = *Secure Architecture for the Networked Enterprise*
2006 – M. Casado et al.

- Logically Centralized Server
  - Trusted Domain Controller (DC)
  - Providing routing and access control decisions
  - Access Control Policies
- Authentication of Hosts and Policy Enforcement
- Principle of least privilege and least knowledge

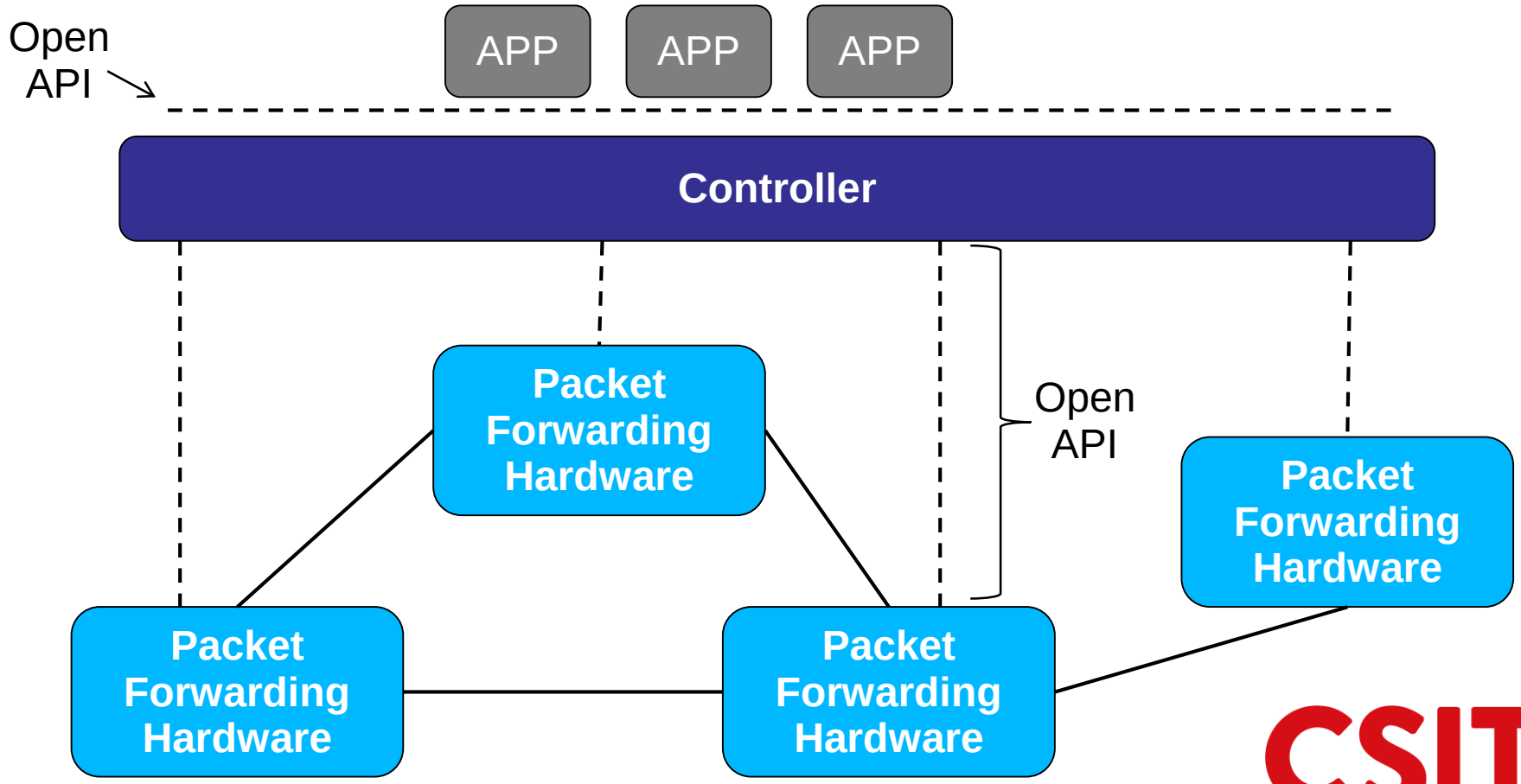


Casado, M. et al., "SANE: A Protection Architecture for Enterprise Networks," Usenix Security, 2006.

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

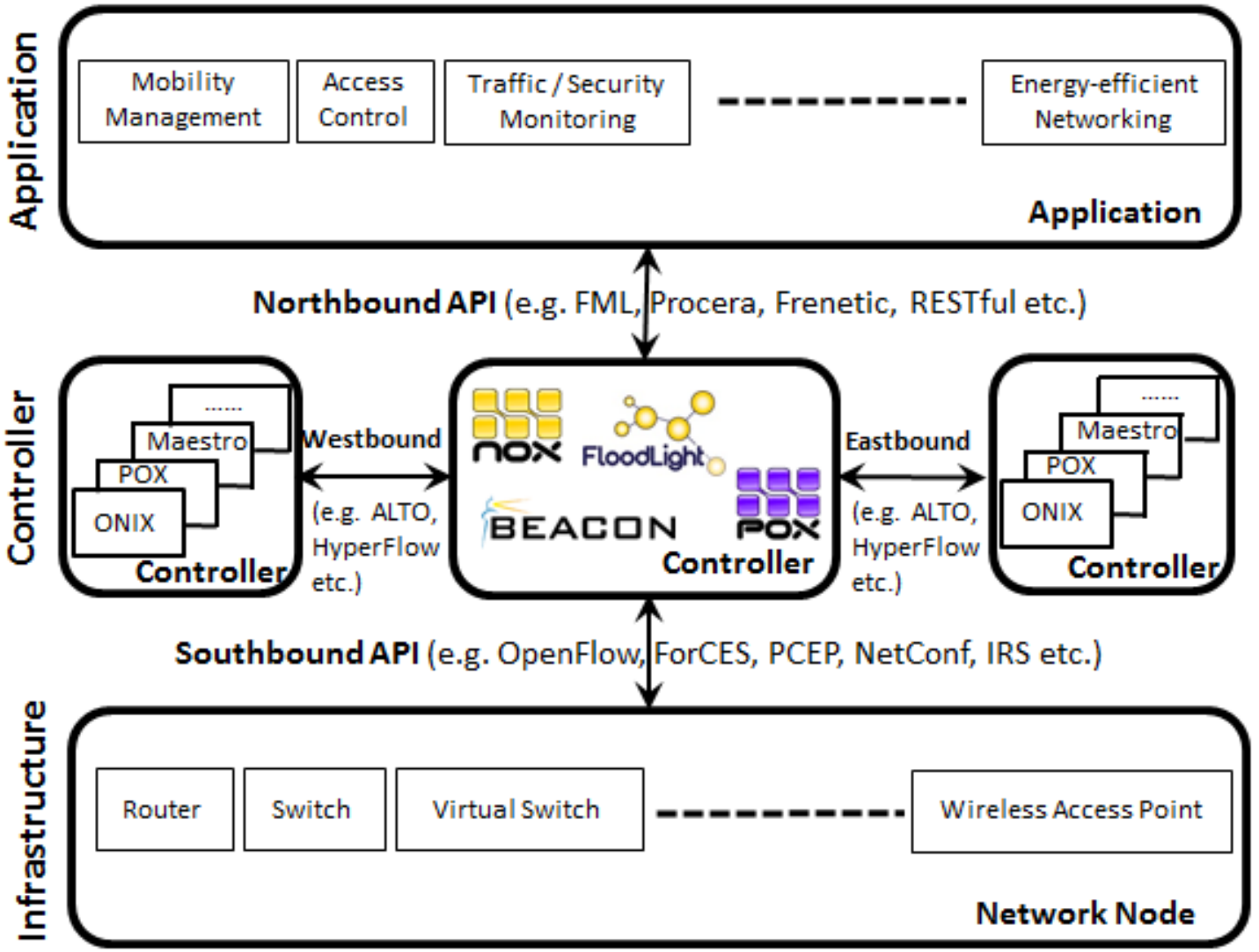
SDN

Separation of Control and Data Planes:



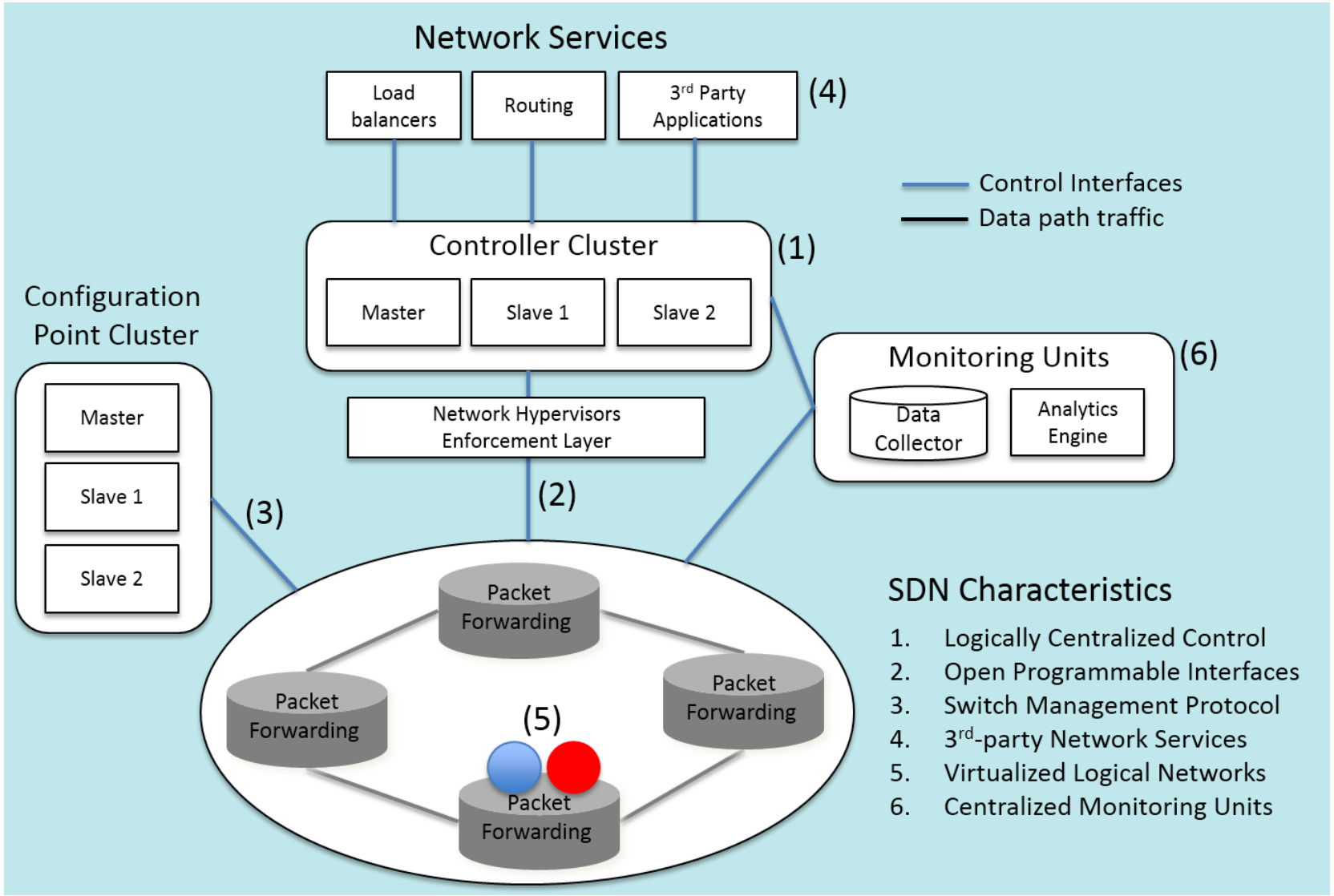
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

SDN Architecture



CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

SDN Characteristics



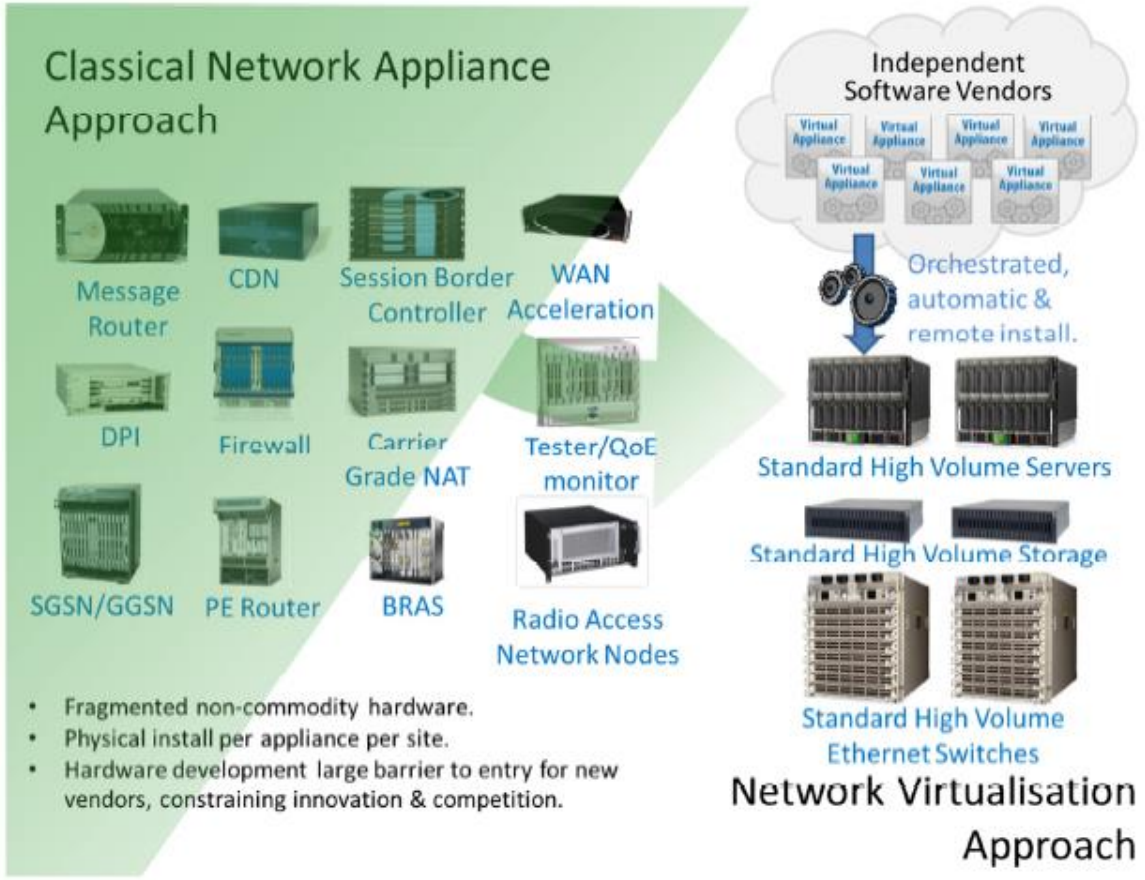
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Network Functions Virtualization

Network Functions Virtualization –

"…implementation of network functions in software that can run on a range of industry standard server hardware, and that can be moved to, or instantiated in, various locations in the network as required…"

Network Functions Virtualisation – Introductory White Paper, October 2012 - http://portal.etsi.org/NFV/NFV_White_Paper.pdf



CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Hands-On

COINS2018
SDN Security Tutorial

This tutorial provides an introduction to security in SDN using the Mininet network emulation tool and the ONOS SDN controller.

A. Test Network Configuration

The tutorial uses the provided VirtualBox Image – Mininet-VM.

1. If not already installed, download VirtualBox from https://www.virtualbox.org
2. From your Desktop, open VirtualBox
3. Select File -> Import Appliance
4. Browse to the folder where you saved the VBox image
5. Select the image to launch it.
6. At the login, enter *mininet*, password *mininet*
7. Type *startx* to launch the GUI
8. Double-click LXTerminal to launch a new terminal.

B. Create Mininet Topology and test Mininet commands

1. Change to the onos mininet directory with the following command:
   cd onos/tools/dev/mininet
2. Launch wireshark in the background using the command:
   sudo wireshark &
3. Enter the following command to create a Mininet tree topology with 3 switches and four hosts:
   sudo mn --custom onos.py --controller onos,1 --topo tree,2,2
4. Test out the following commands in mininet:

   pingall

   dpctl dump-flows (Note the default flows i.e. match and action)

   h1 ping h2 (Note the ping response time)

   Further commands at http://mininet.org/

C. Test ONOS commands from the CLI and GUI

The network you created in B. is controlled by the ONOS controller.

1. Launch the ONOS cli from the same mininet terminal:
   onos
2. Test out the following commands in ONOS:

   apps –a –s

   hosts

COINS2018 – SDN Security Tutorial S. Scott-Hayward

   nodes

   devices

   flows

3. Open a browser window and launch the ONOS GUI
   http://192.168.123.1:8181/onos/ui/login.html
   User: *karaf*, Password: *karaf*

D. Test the network vulnerability to Denial of Service

The controller-switch communication link and the switch flow table are both vulnerable to DoS attack. Test this vulnerability with the following steps:

1. Check the switch flow table entries:
   From Mininet CLI *dpctl dump-flows*
   From ONOS CLI *flows*
   From ONOS GUI Select a device and flow view
2. Use hping3 to create a SYN flood attack[1]
   a. Launch a host terminal
      xterm h1
   b. From this host terminal, launch a simple flood attack
      hping3 --flood --rand-source 10.0.02
      Find further commands using *hping3 --help*
3. Check the switch flow tables again. What behaviour do you observe? What are the default flows created by ONOS?
4. Change the flow table match setting in the ONOS reactive forwarding application:
   onos
   cfg set org.onosproject.fwd.ReactiveForwarding matchIpv4Address true
5. Repeat Steps 2 and 3.

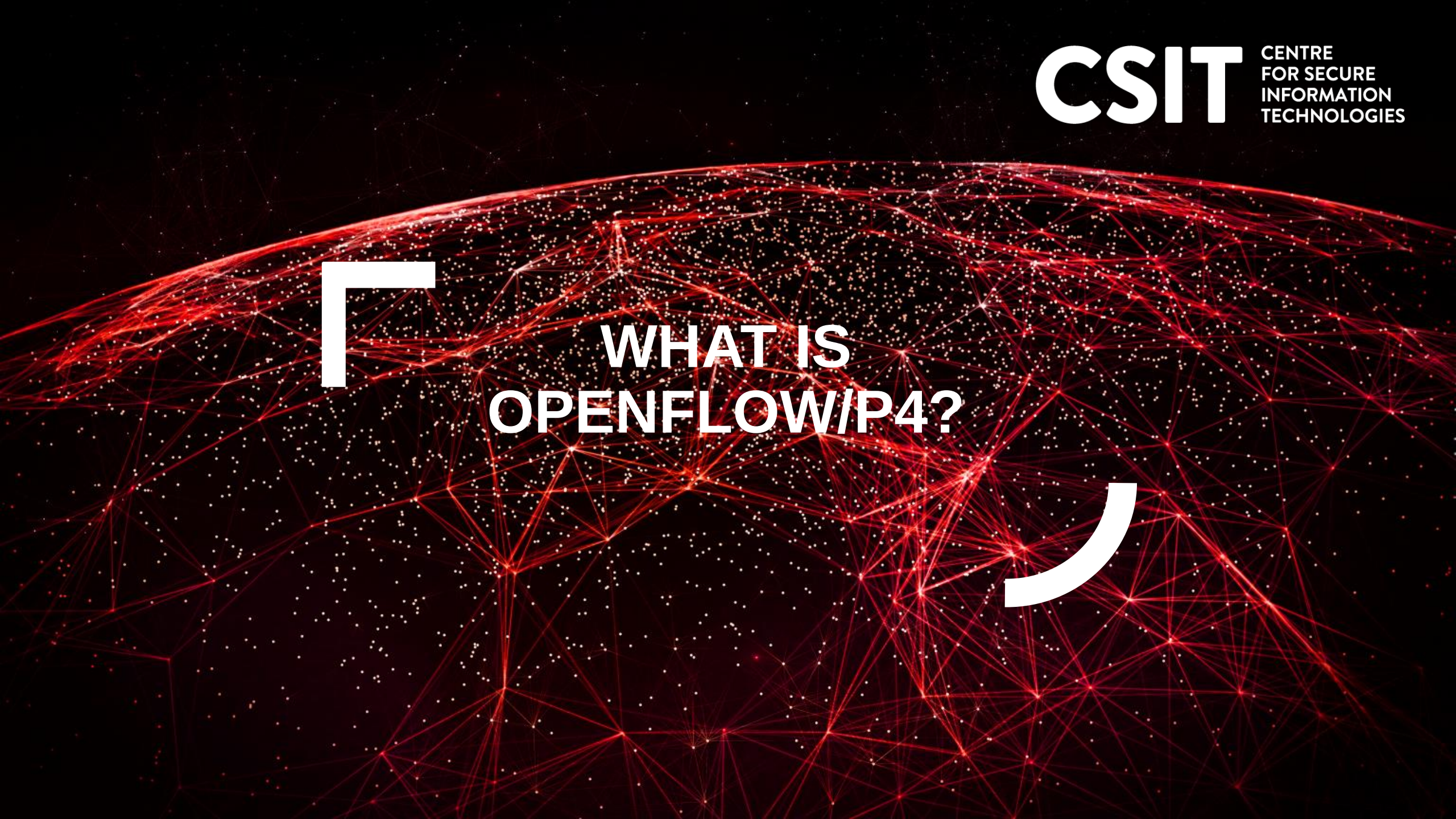
E. Configure ONOS for a secure SDN

The default ONOS configuration has a number of security vulnerabilities. Some protection can be introduced with the following steps:

1. Configure authentication for the CLI, GUI and REST API
   https://wiki.onosproject.org/pages/viewpage.action?pageId=4162614
2. Configure SSL/TLS for controller-switch communication
   https://wiki.onosproject.org/pages/viewpage.action?pageId=6358090

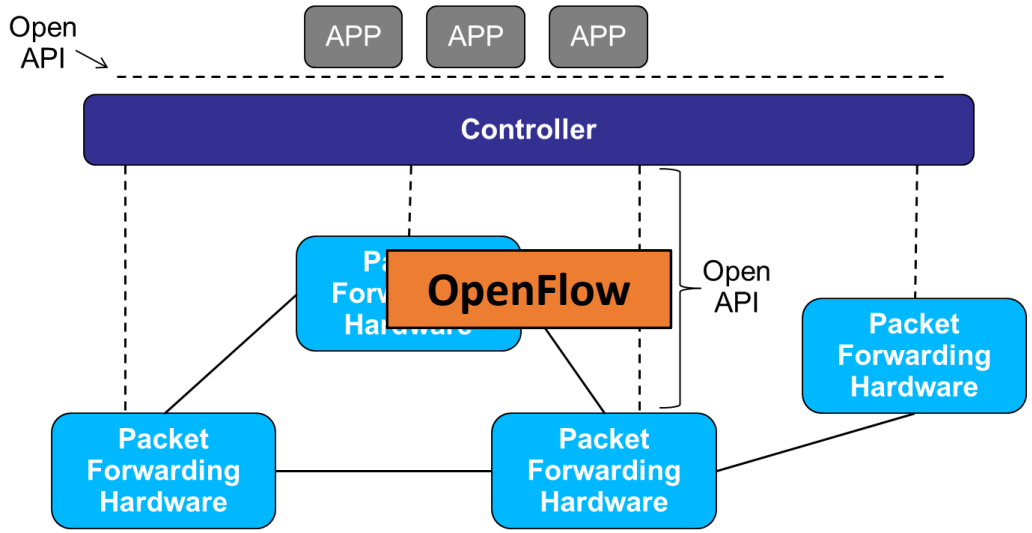
For a controller cluster implementation (i.e. multiple controllers), TLS should also be configured for inter-controller communication.

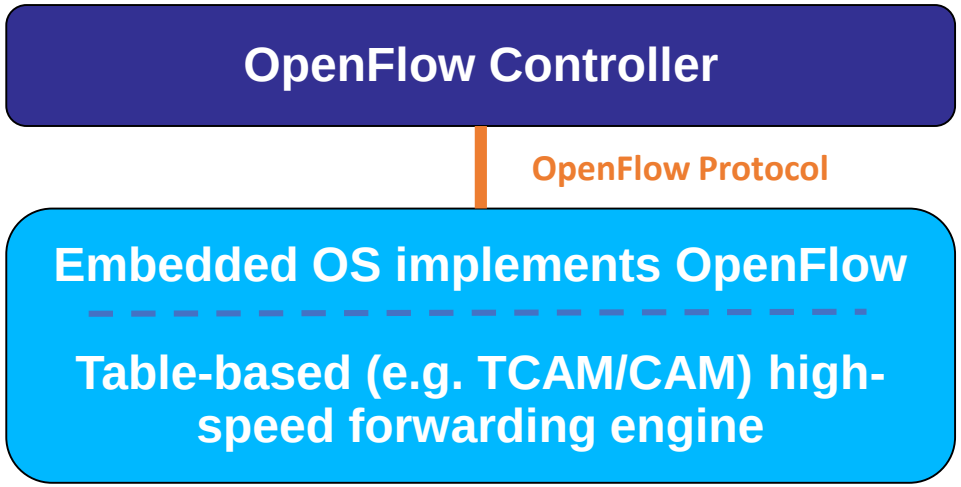
QUEEN'S UNIVERSITY BELFAST


CSIT
CENTRE
FOR SECURE
INFORMATION
TECHNOLOGIES
WHAT IS
OPENFLOW/P4?

What is OpenFlow?

OpenFlow = A protocol to control the forwarding behaviour of Ethernet switches in a Software Defined Network





CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

The origin of OpenFlow

Clean Slate Program at Stanford

- Early work on SANE circa 2006
- Inspired Ethane circa 2007, which lead to OpenFlow

2009 Stanford publishes OF 1.0.0 Specification
2009 Nicira Series A funding
2010 Big Switch seed funding
2011 Open Network Foundation is created
2012 Google announces migration to OpenFlow (migration started in 2009)

Open Networking Foundation owns OpenFlow

Flow Table (OpenFlow v1.0)

Header Fields	Counters	Actions	Priority
Ingress Port Ethernet Source Addr Ethernet Dest Addr Ethernet Type VLAN id VLAN priority IP Source Addr IP Dest Addr IP Protocol IP ToS ICMP type ICMP code	**Per Flow Counters** Received Packets Received Bytes Duration seconds Duration nanoseconds	Forward (All, Controller, Local, Table, IN_port, Port# Normal, Flood) Enqueue Drop Modify-Field	
if Eth Type == ARP		forward Controller	32768

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Flow Table

Each Flow Table entry has two timers:

idle_timeout seconds of no matching packets after which the flow is removed
zero means never timeout

hard_timeout seconds after which the flow is removed
zero means never timeout

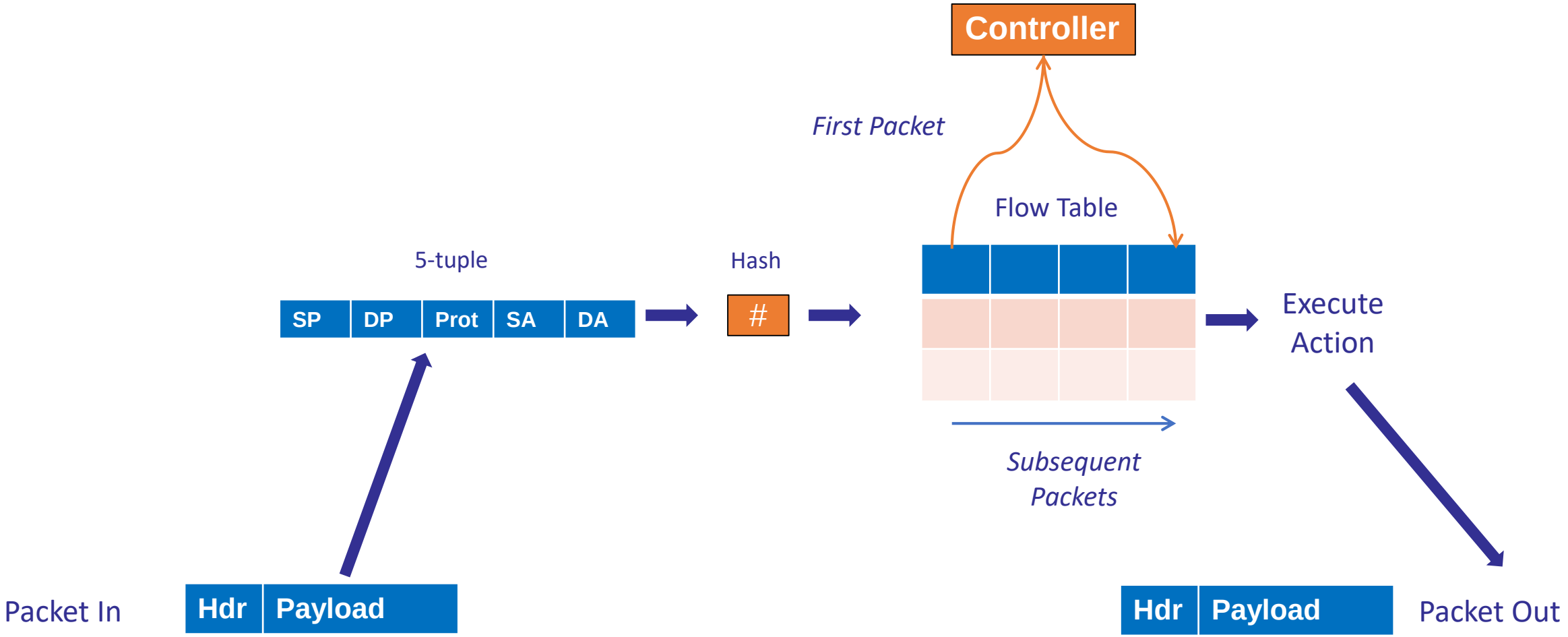
If both idle_timeout and hard_timeout are set, then the flow is removed when the first of the two expires.

Proactive vs. Reactive Flows

Populating the Flow Table

Proactive	Rules are relatively static, controller places rules in switch before they are required.
Reactive	Rules are dynamic. Packets which have no match are sent to the controller (packet in). Controller creates appropriate rule and sends packet back to switch (packet out) for processing.

Implementing OpenFlow



CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Evolution of OpenFlow

OpenFlow v1.0

Header Fields	Counters	Actions	Priority

Does packet match flow table entry? If so, perform action.

OpenFlow v1.5

Match Fields	Priority	Counters	Instructions	Timeouts	Cookie	Flags

Metadata	Packet	Action Set

Group ID	Type	Counters	Action Buckets

Does packet match flow table entry? If so, look at instructions …

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Actions vs. Instructions

OpenFlow v1.1

- Flow entries contain instructions
- Instructions may be immediate action(s), or
- Instructions may set actions in the action set
- Instructions can also change pipeline processing:
    - Goto table X
    - Goto group table entry x

Statistics/Counters

Counters maintained for each:

- Flow Table — *Required:* Reference Count (active entries)
- Flow Entry — *Required:* Duration (seconds)
- Port — *Required:* Received Packets, Transmitted Packets, Duration (secs)
- Queue — *Required:* Transmit Packets, Duration (seconds)
- Group — *Required:* Duration (seconds)
- Group Bucket — *Optional*
- Meter — *Required:* Duration (seconds)
- Meter Band — *Optional*

Evolution of OpenFlow

OpenFlow Version	Match fields	Statistics	# Matches		# Instructions		# Actions		# Ports	
			Req	Opt	Req	Opt	Req	Opt	Req	Opt
v 1.0	Ingress Port	Per table statistics	18	2	1	0	2	11	6	2
	Ethernet: src, dst, type, VLAN	Per flow statistics								
	IPv4: src, dst, proto, ToS	Per port statistics								
	TCP/UDP: src port, dst port	Per queue statistics								
v 1.1	Metadata, SCTP, VLAN tagging	Group statistics	23	2	0	0	3	28	5	3
	MPLS: label, traffic class	Action bucket statistics								
v 1.2	OpenFlow Extensible Match (OXM)		14	18	2	3	2	49	5	3
	IPv6: src, dst, flow label, ICMPv6									
v 1.3	PBB, IPv6 Extension Headers	Per-flow meter	14	26	2	4	2	56	5	3
		Per-flow meter band								
v 1.4	—	—	**14**	**27**	**2**	**4**	**2**	**57**	**5**	**3**
		Optical port properties								

Multiple Tables

Controller Role Change

Role Status, Error Codes

D. Kreutz et al., 'Software-Defined Networking: A Comprehensive Survey', proceedings of the IEEE 103, no. 1 (2015): 14-76

v1.5	**-**	**Extensible Flow Entry**	**14**	**30**	**2**	**5**	**2**	**59**	**5**	**3**

Egress Ports, Various Security Recommendations

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Securing the OpenFlow Protocol

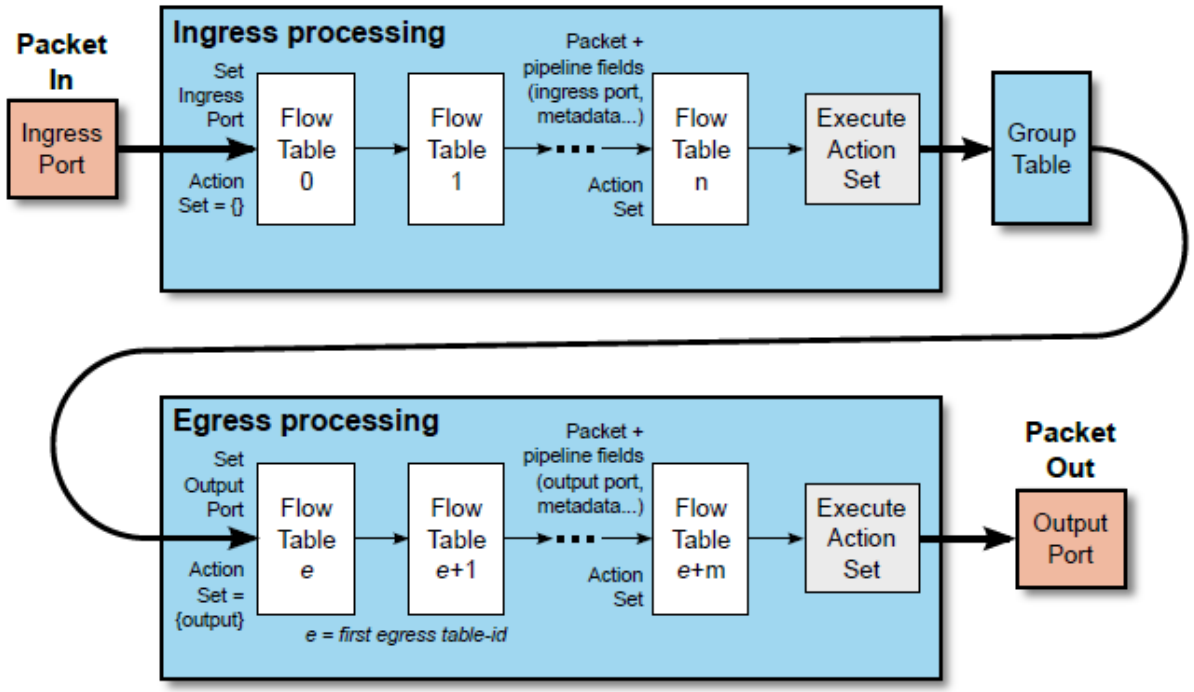
ONF Security WG OpenFlow Switch Specification Analysis:

Recommendations to Extensibility WG – Updates to OF Switch Specification v1.3.5

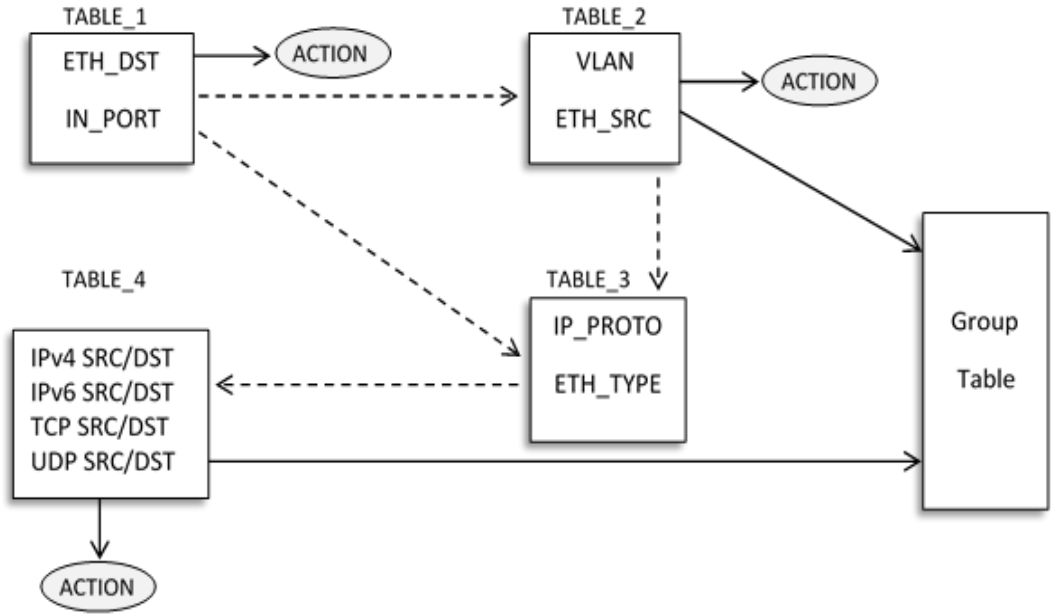
- Specify that a secure version of TLS is recommended (EXT-525)
- Clarify certificate configuration of the switch (EXT-304)
- Specify that malformed packet refer to those in the datapath (EXT-528)
- Specify how to deal with malformed OpenFlow messages (EXT-528)
- Specify that counters must use the full bit range (EXT-529)

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Pipeline Processing



Open Networking Foundation,'OpenFlow Switch Specification Version 1.5.1', www.opennetworking.org

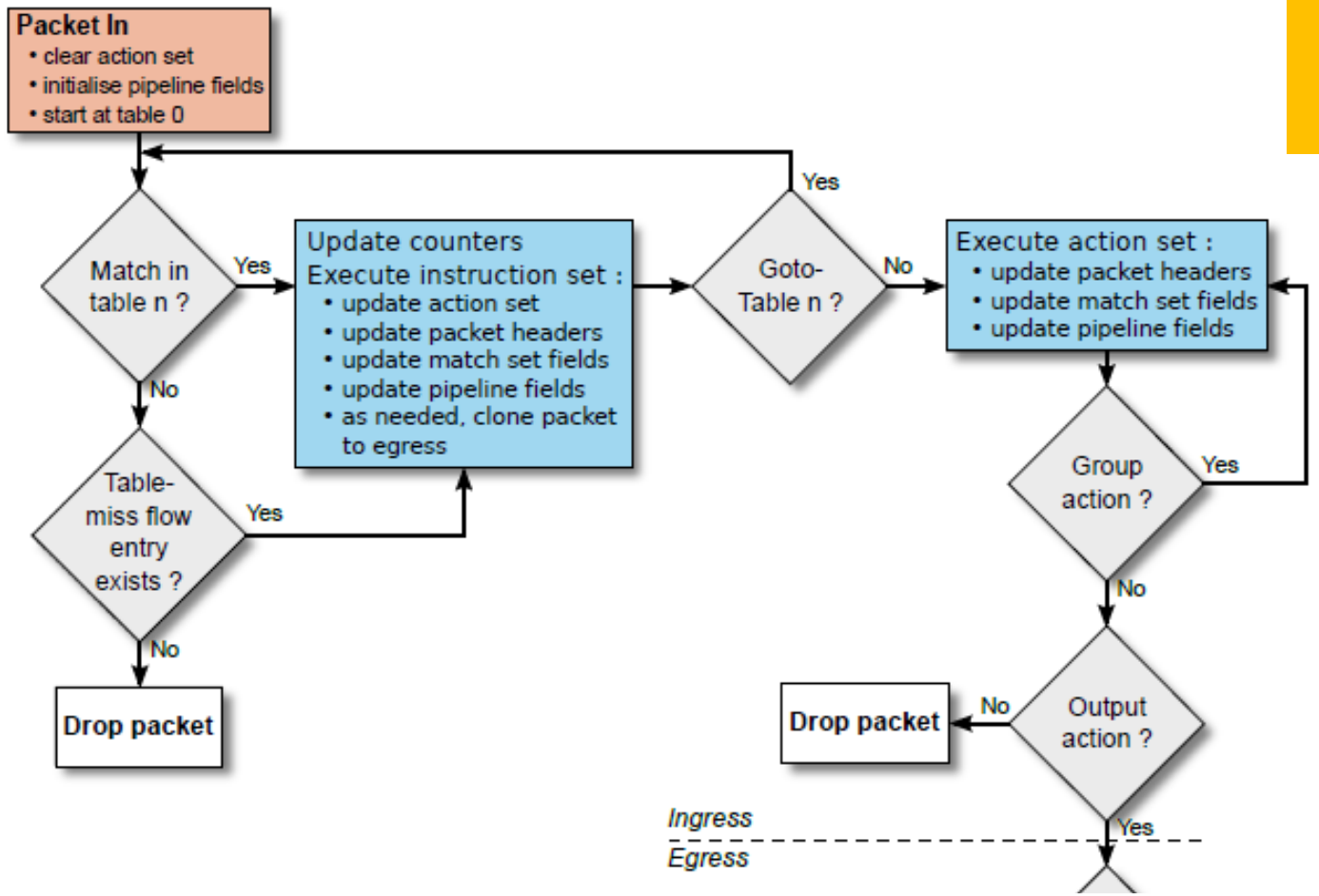


L2-L3-ACL Pipeline

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Packet flow through OF switch

Test your packet pipeline using FlowSim: web-based OpenFlow data plane simulator designed to teach OF data plane abstractions https://flowsim.flowgrammable.org/



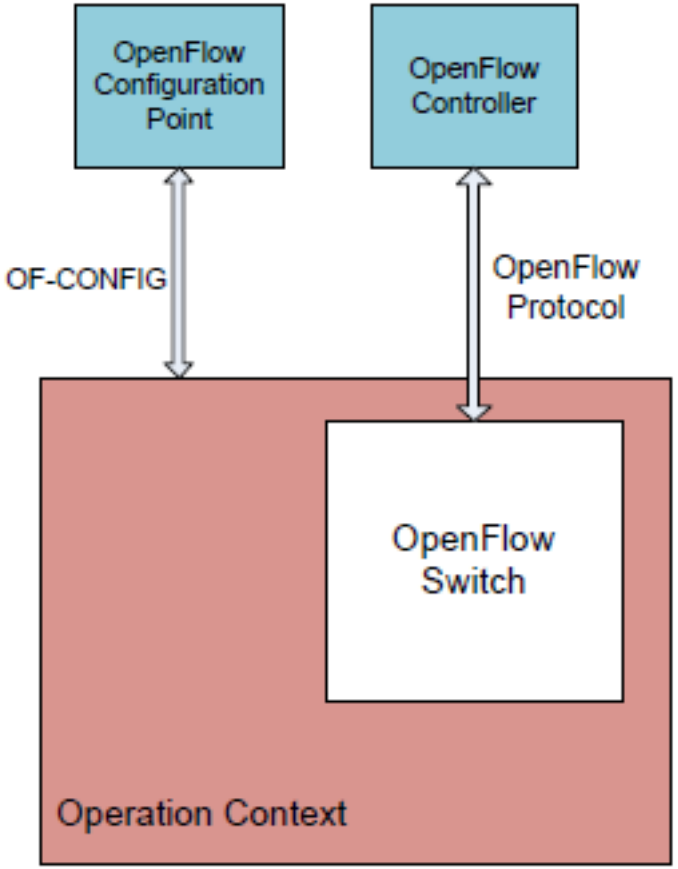
Open Networking Foundation,'OpenFlow Switch Specification Version 1.5.1', www.opennetworking.org

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

OF-Config 1.2

OF-Config 1.2 – OpenFlow Management and Configuration Protocol:

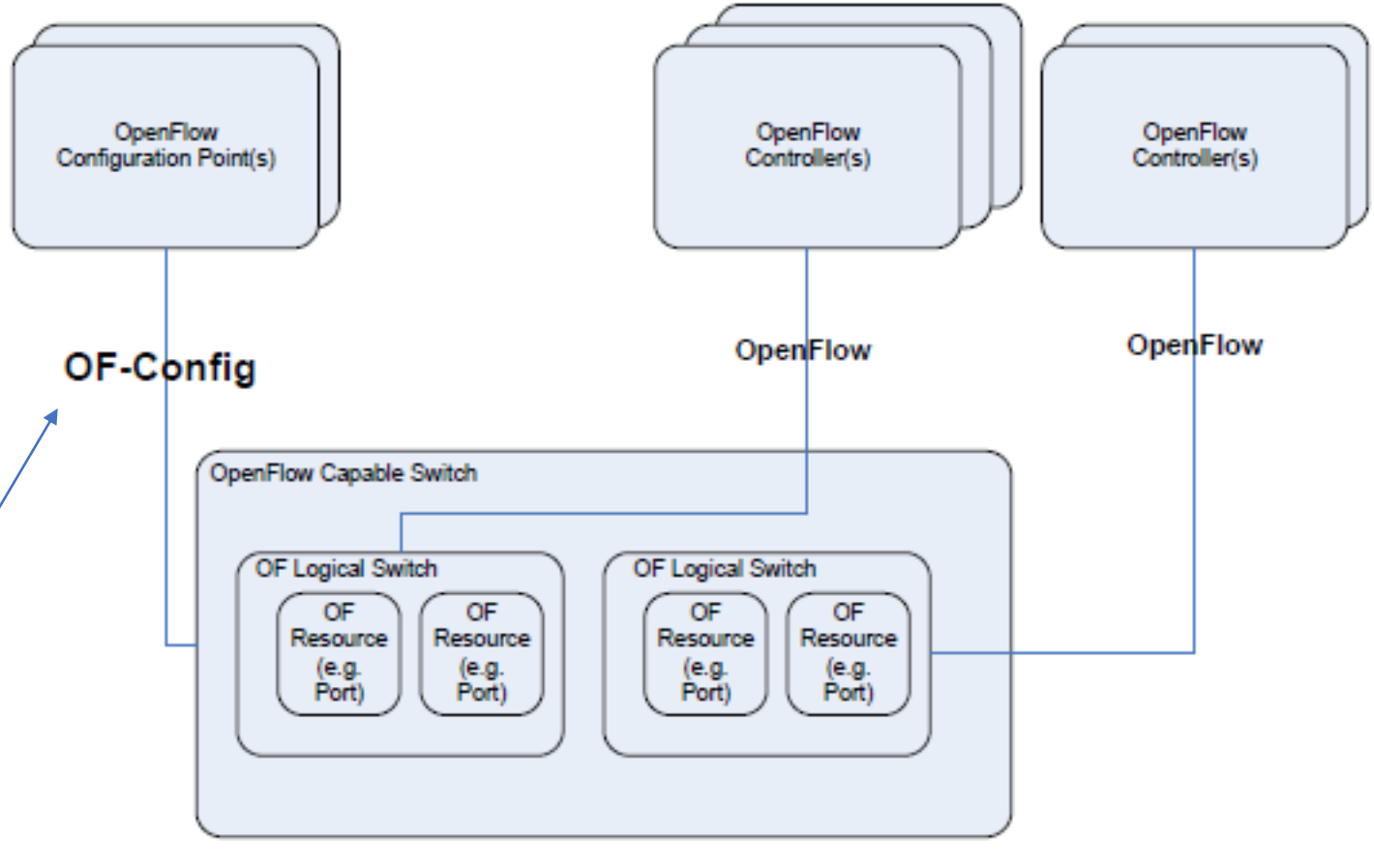
“OF-CONFIG defines an OpenFlow switch as an abstraction called an OpenFlow Logical Switch. The OF-CONFIG protocol enables configuration of essential artifacts of an OpenFlow Logical Switch so that an OpenFlow controller can communicate and control the OpenFlow Logical switch via the OpenFlow protocol.”



Open Networking Foundation,‘OF-CONFIG 1.2 – OpenFlow Management and Configuration Protocol’, www.opennetworking.org

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

OF-Config 1.2



OF-CONFIG uses NETCONF protocol as its transport (implies SSH/TLS)

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

OF-Config 1.2

OF-CONFIG 1.2 is focussed on the following functions to configure an OF1.3 logical switch:

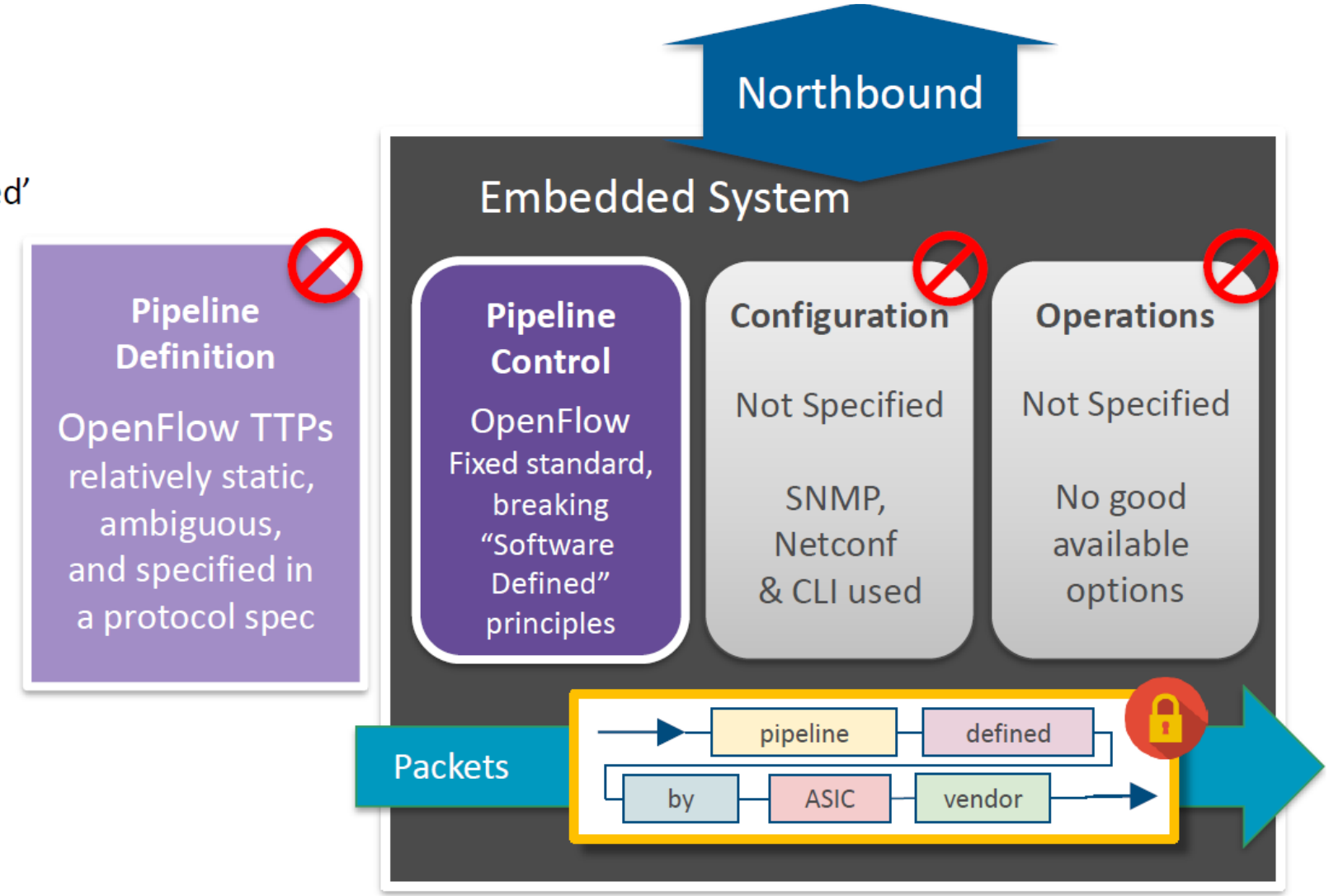
- Assignment of one or more OF controllers to OF data planes
- Configuration of queues and ports
- Ability to remotely change some aspects of ports (e.g. up/down)
- Configuration of certificates for secure communication between the OF logical switches and OF controllers
- Discovery of capabilities of an OF logical switch
- Configuration of a set of specific tunnel types such as IP-in-GRE, NV-GRE, VxLAN

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Improving on OpenFlow?

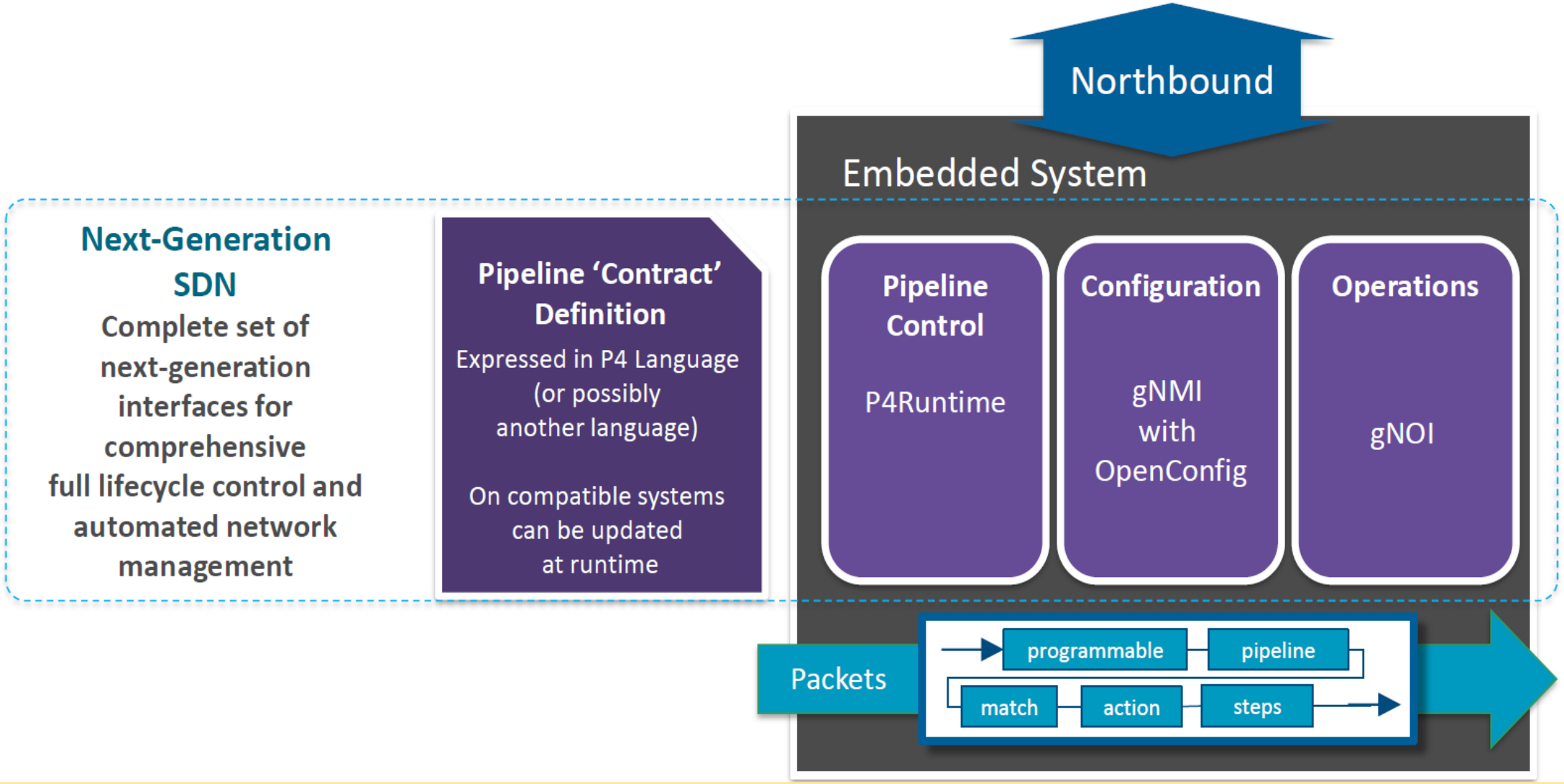
OpenFlow

- Addressed 1 of the 4 major areas needed for complete 'software defined' management & control
  - OpenFlow only provides pipeline control
  - Pipeline definition is typically in silicon vendor specs
  - Config & operations not addressed
- Used traditional standards process
  - Not 'software defined'
  - Very long innovation cycle
- Operators found challenges:
  - Proved to be non-deterministic
    - Specifies Match, not Actions
  - Each data plane has differences
  - Hard to deploy latest switching silicon innovations



Stratum Project Launch, Open Networking Foundation, March 2018 – https://stratumproject.org/wp-content/uploads/2018/03/Stratum-Launch-Announcement-Final.pdf

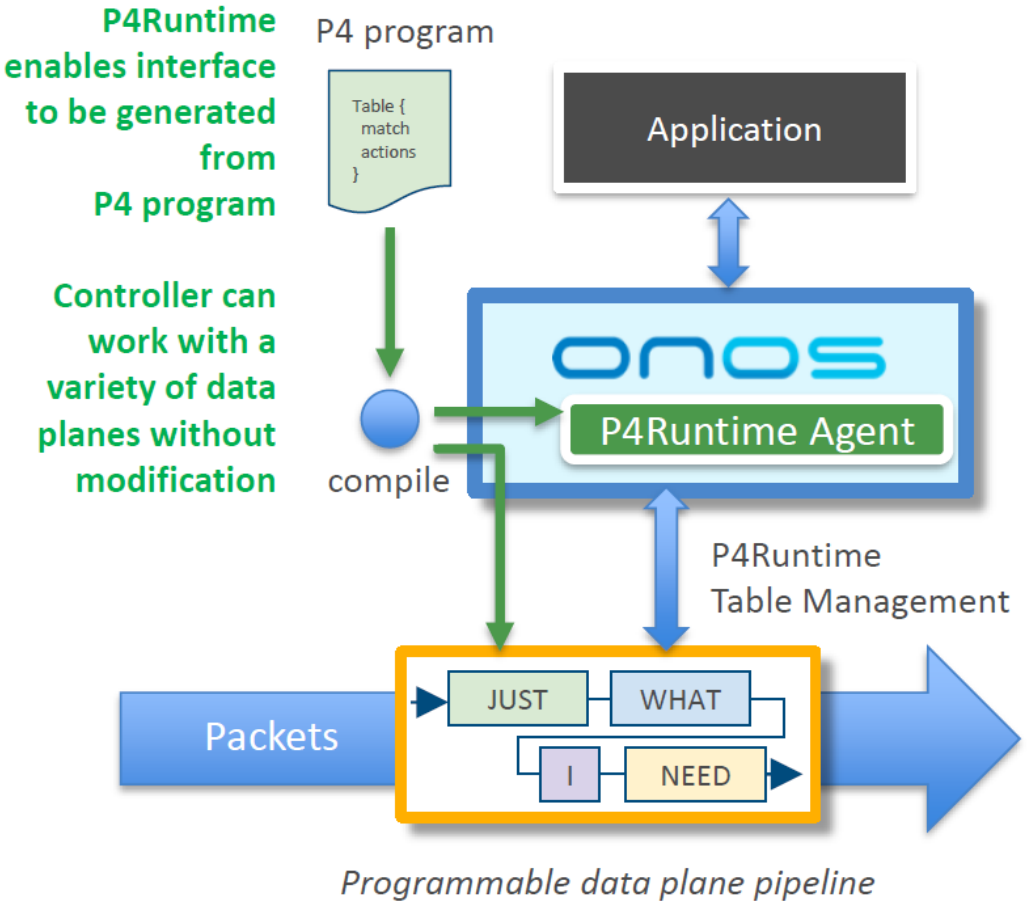
Next-Generation SDN Interfaces



Stratum Project Launch, Open Networking Foundation, March 2018 – https://stratumproject.org/wp-content/uploads/2018/03/Stratum-Launch-Announcement-Final.pdf

P4 (P4.org)

- P4 language consortium becoming a project of the Open Networking Foundation and the Linux Foundation (March 2018)
- P4 – target-independent, protocol-independent
- P4 runtime - extend P4 by adding the API to control/configure the device at the same time as deploying a P4 program to the device
- P4 Implementation issues identified by researchers – limitations of the language and constraints imposed by interface between P4 program and s/w switch (P4 runtime…)



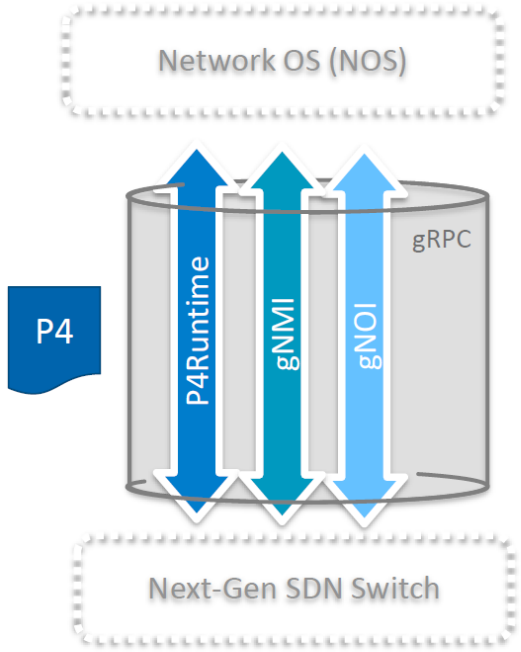
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Stratum Project Launch, Open Networking Foundation, March 2018 – https://stratumproject.org/wp-content/uploads/2018/03/Stratum-Launch-Announcement-Final.pdf

P4 (P4.org)

- Google next-gen SDN switch to use P4 Runtime to programme it, OpenConfig to manage it, and to be based on the Open Network Linux (ONL) platform/Stratum…

Next-Generation SDN Interfaces



- P4 (for pipeline definition)
  - Defines the logical pipeline behavior that is silicon-, pipeline-, and pkt header-agnostic
  - Defines 'contract' between NOS and data plane
- P4Runtime (for pipeline control)
  - Message payloads derived from P4 program defining the pipeline
  - Allows for run time changes to the contract on systems with programmable silicon
- gNMI using OpenConfig models (for configuration)
  - Manage configuration (with persistence across reboots)
  - Stream telemetry
- gNOI (for operations)
  - Autonomous actions for debugging and operating a production network
  - Device reboots, key management, BERT & ping testing

All running over gRPC, which has many advantages:

- Built on HTTP/2 for a high speed, bi-directional streaming, multiplexing, security
- Uses ProtoBuf, supporting many more languages and optimized for low latency

Stratum Project Launch, Open Networking Foundation, March 2018 – https://stratumproject.org/wp-content/uploads/2018/03/Stratum-Launch-Announcement-Final.pdf