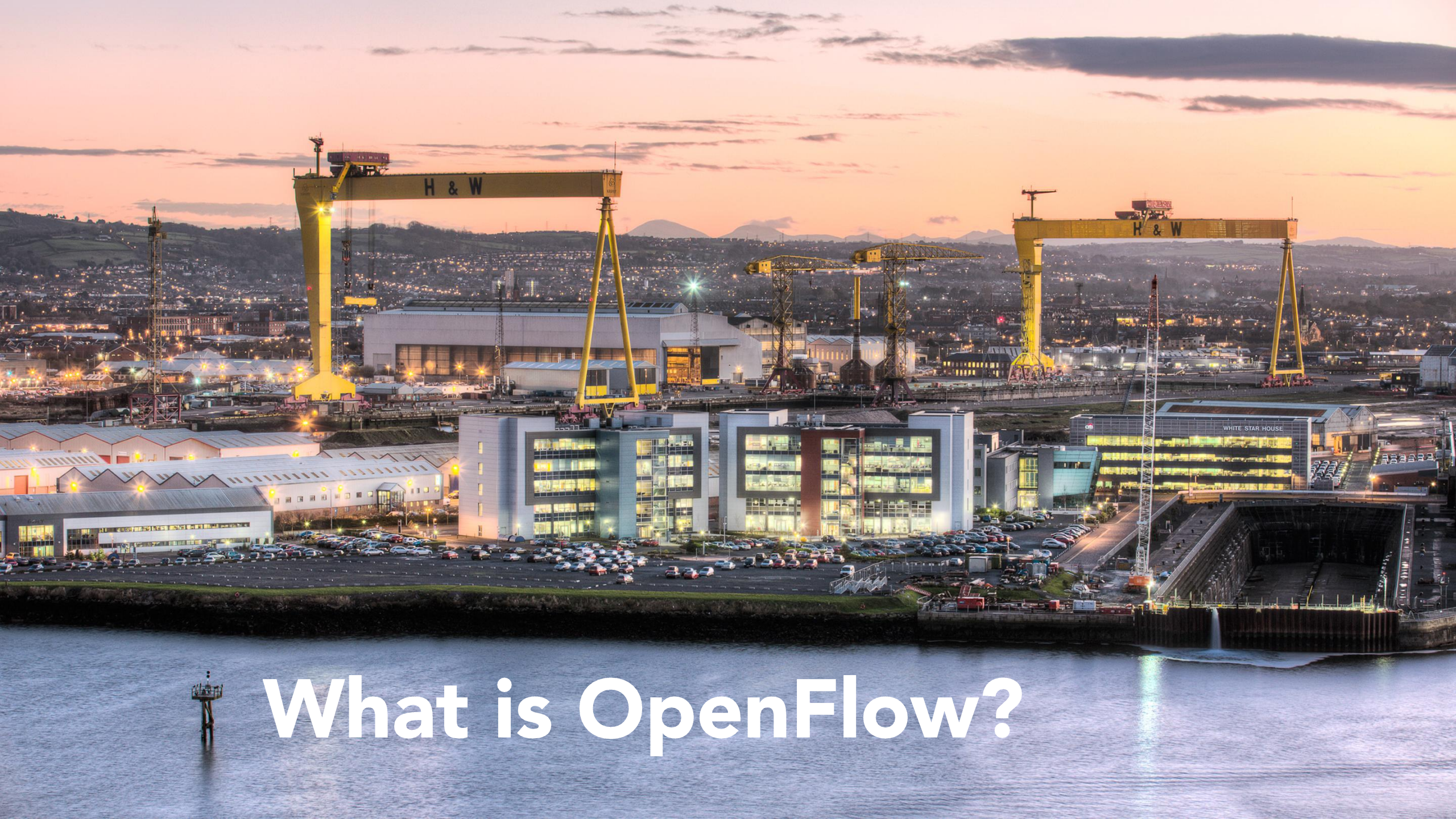
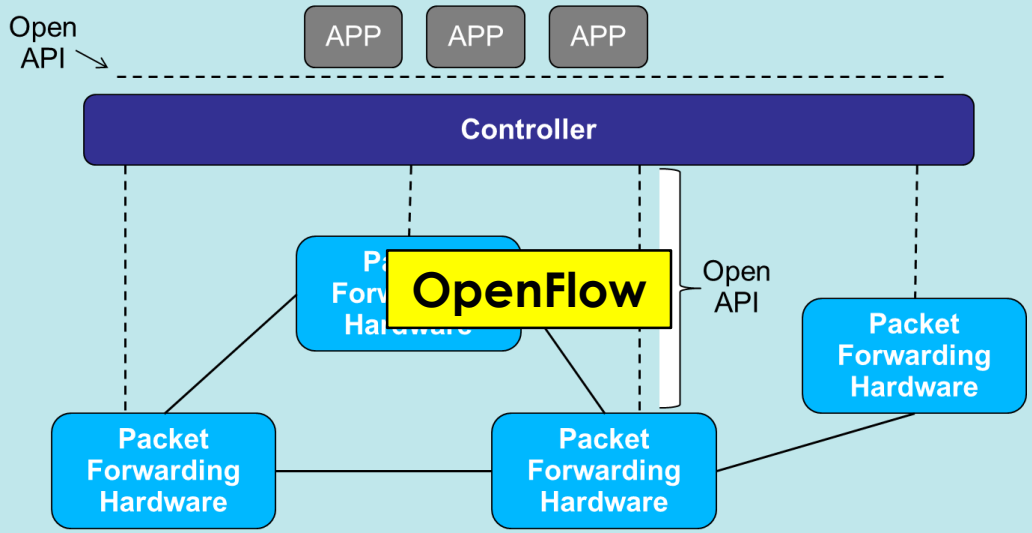

CSIT
CENTRE
FOR SECURE
INFORMATION
TECHNOLOGIES
Queen's University
Belfast
SDN Security
COINS Summer School
Dr. Sandra Scott-Hayward
23 August 2015
@CSIT_QUB

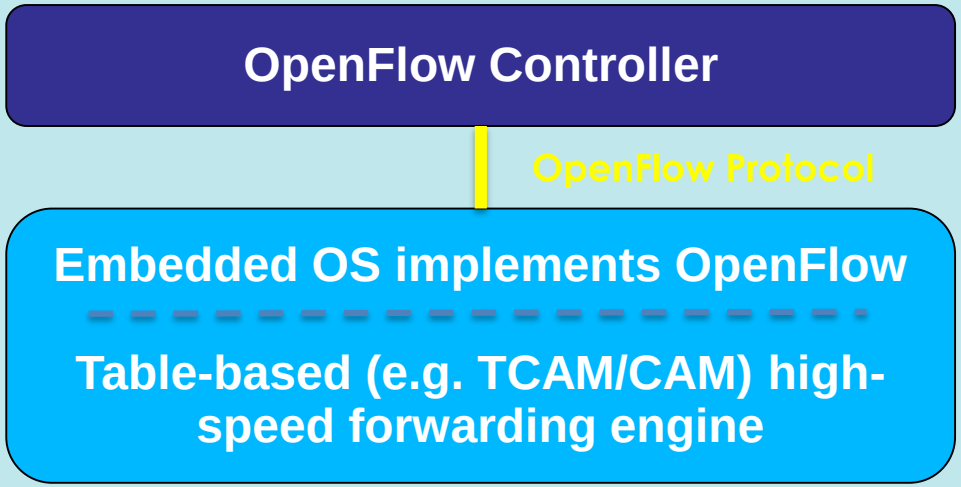


What is OpenFlow?

What is OpenFlow?

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





OpenFlow Origin

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

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

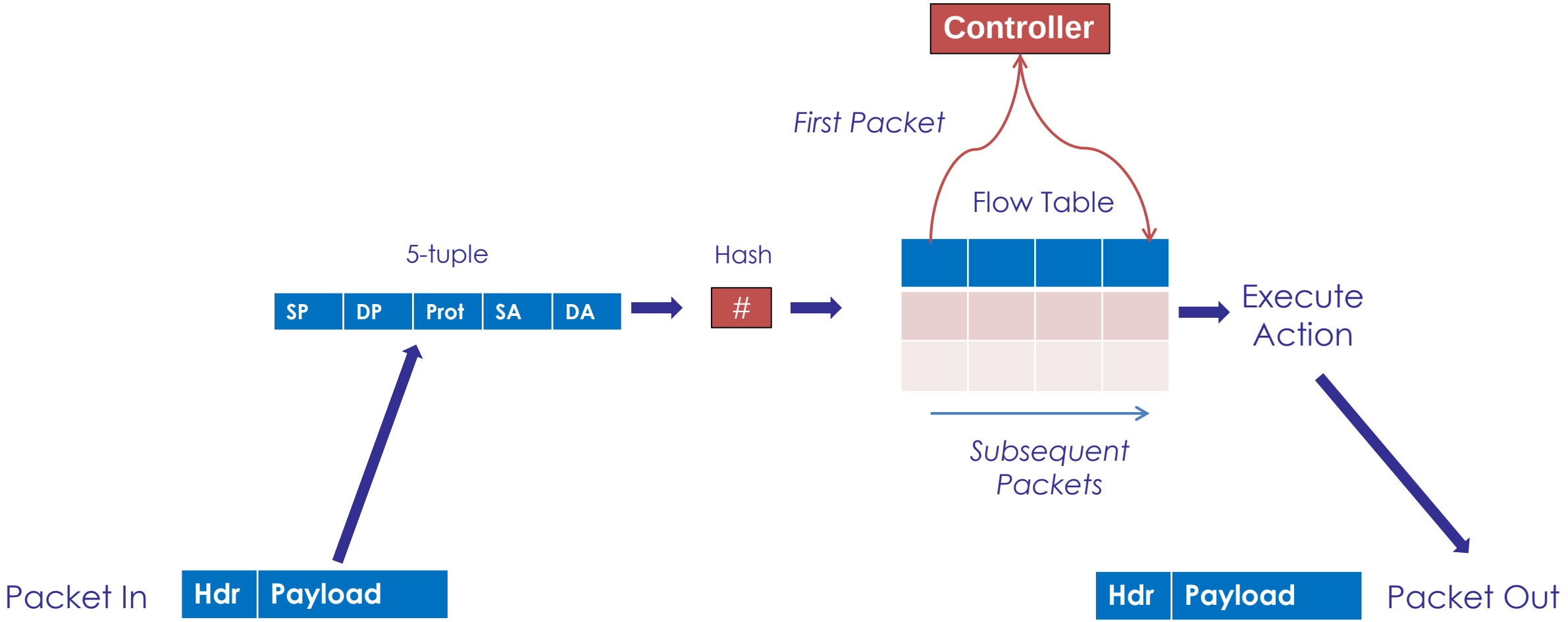
If both idle_timeout and hard_timeout are set, then the flow is removed when the first of the two expires.

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



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 …

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 (seconds)
- Queue — *Required:* Transmit Packets, Duration (seconds)
- Group — *Required:* Duration (seconds)
- Group Bucket — *Optional*
- Meter — *Required:* Duration (seconds)
- Meter Band — *Optional*

OpenFlow v1.3 (Long Term Maintained)

New table “Meter Table” – supporting Quality of Service

New instruction: Meter meter_id

Meter Identifier	Meter Bands	Counters
32 bit integer used to identify the meter	List of meter bands; each band specifies rate and behaviour	

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

ONF Security WG OpenFlow Switch Specification Analysis:

Recommendations to Extensibility WG – Updates to OpenFlow 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)

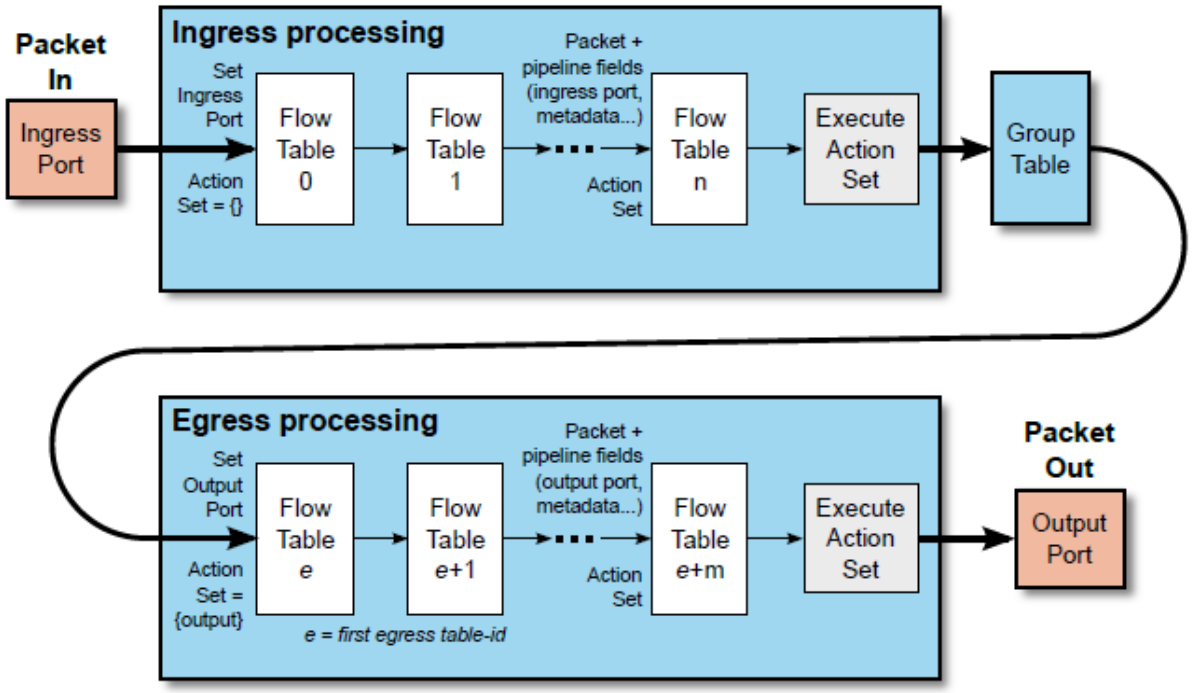
Connection Setup – TCP vs. TLS

Main Connection: TLS or TCP

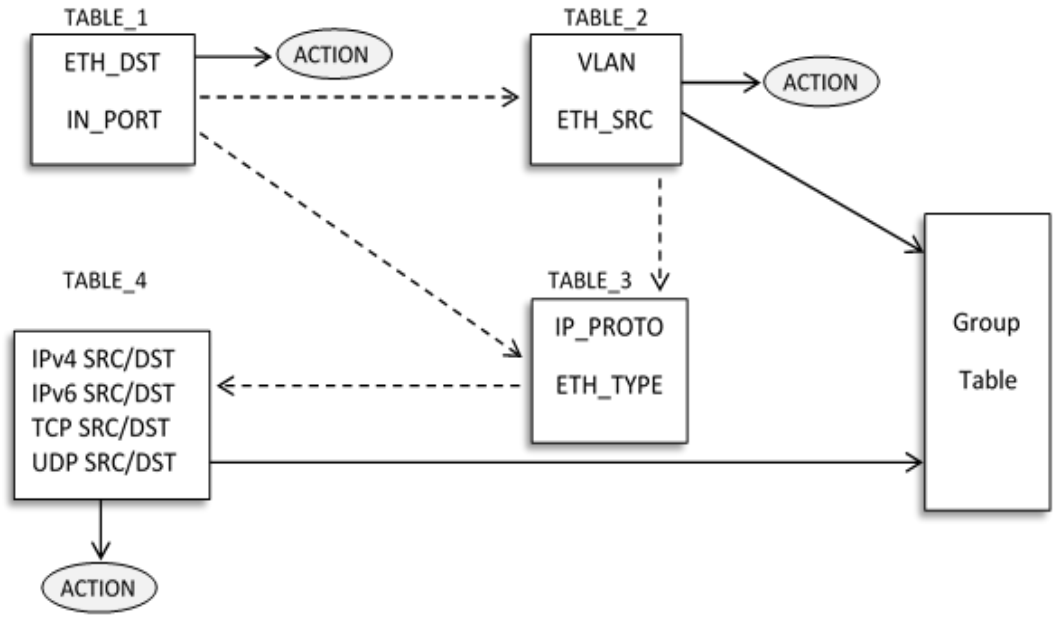
Auxiliary Connection: TLS, DTLS, TCP, UDP
On reliable transport (tls/tcp), use full OF protocol
On unreliable transport (dtls/udp), use only subset of OF protocol

e.g. ovs-vsctl set-controller <switch> protocol:name-or-address:port
ovs-vsctl set-controller dp1 ssl:127.0.0.1:6653

Pipeline Processing

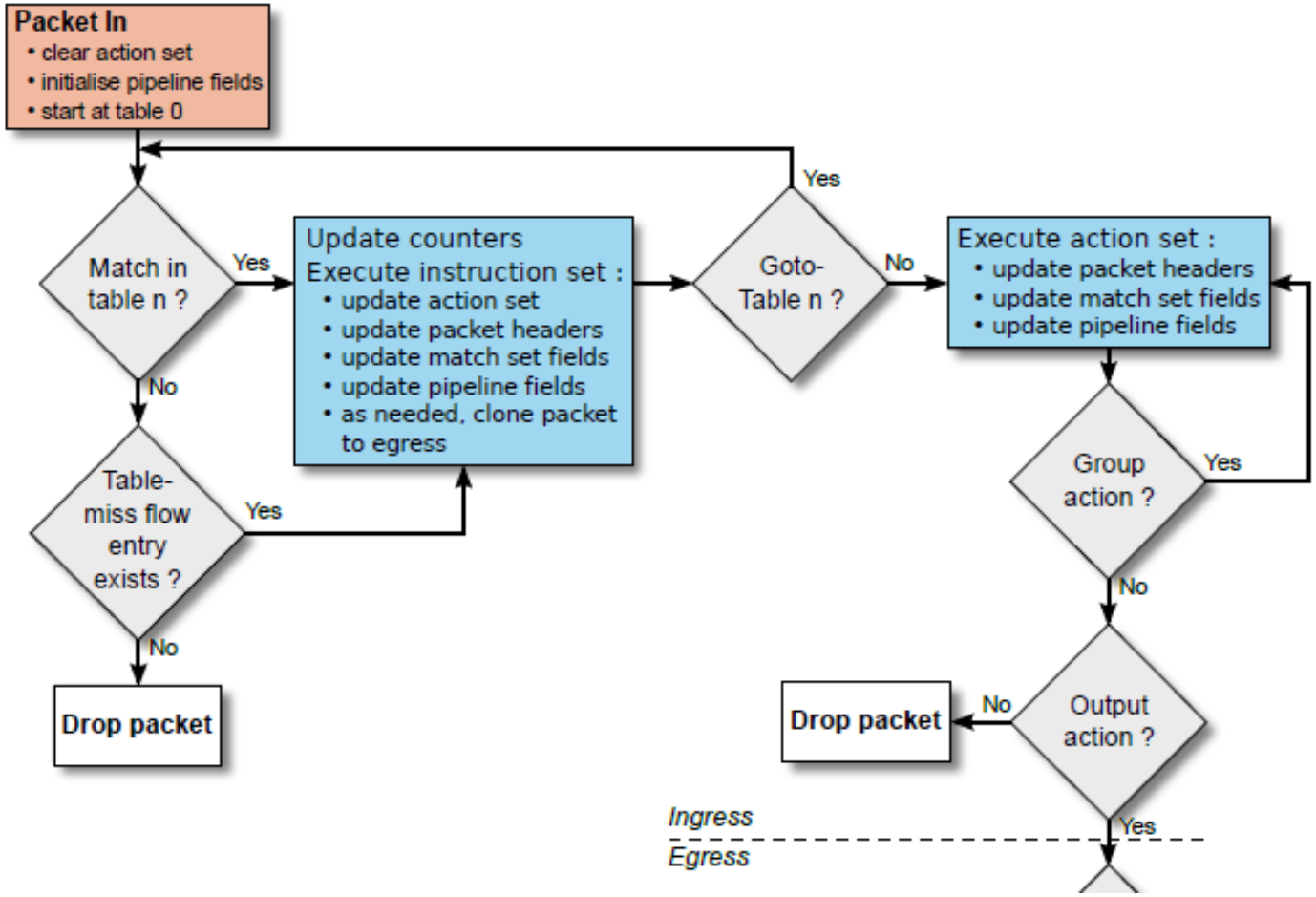


Open Networking Foundation, 'OpenFlow Switch Specification Version 1.5.1', www.opennetworking.org



L2-L3-ACL Pipeline

Packet Flow through OF Switch



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

FlowSim

FlowSim – web-based OpenFlow data plane simulator designed to teach OF data plane abstractions

https://flowsim.flowgrammable.org/

Example: IPv4 Packet Pipeline:

T0 Match: In_Port, Eth_dst; Action: GoTo T2

T2 Match: Eth_type, IPv4 Proto; Action: Write and Apply IPv4 Dst, Output Port

VLAN Packet Pipeline:

T0 Match: In_Port, Eth_dst; Action: GoTo T1

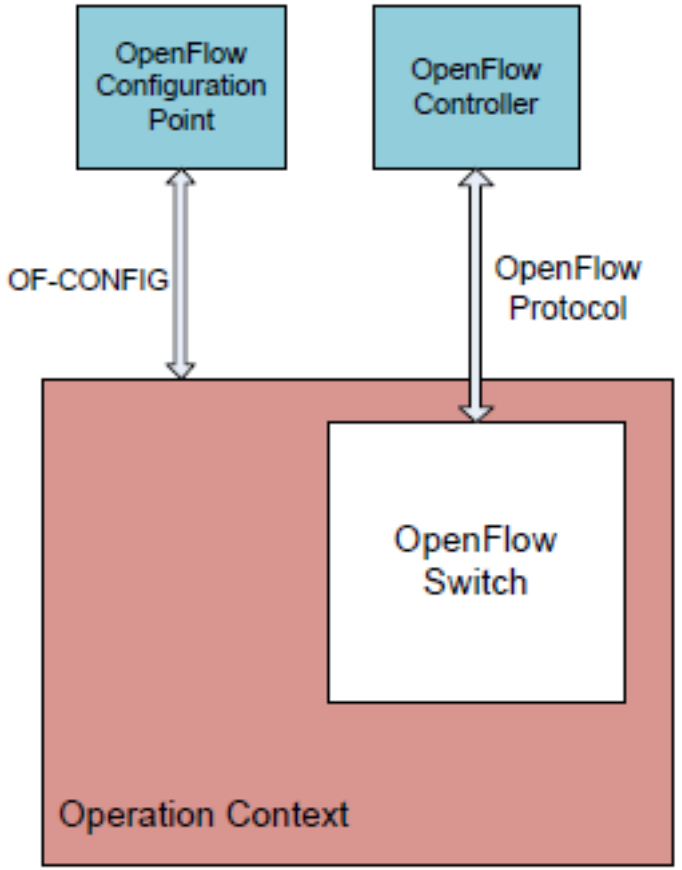
T1 Match: Eth_Src; Action: GoTo T2

T2 Match: Eth_type; Action: Apply VLAN ID, Set Queue, Set Out Port

OF-Config 1.2

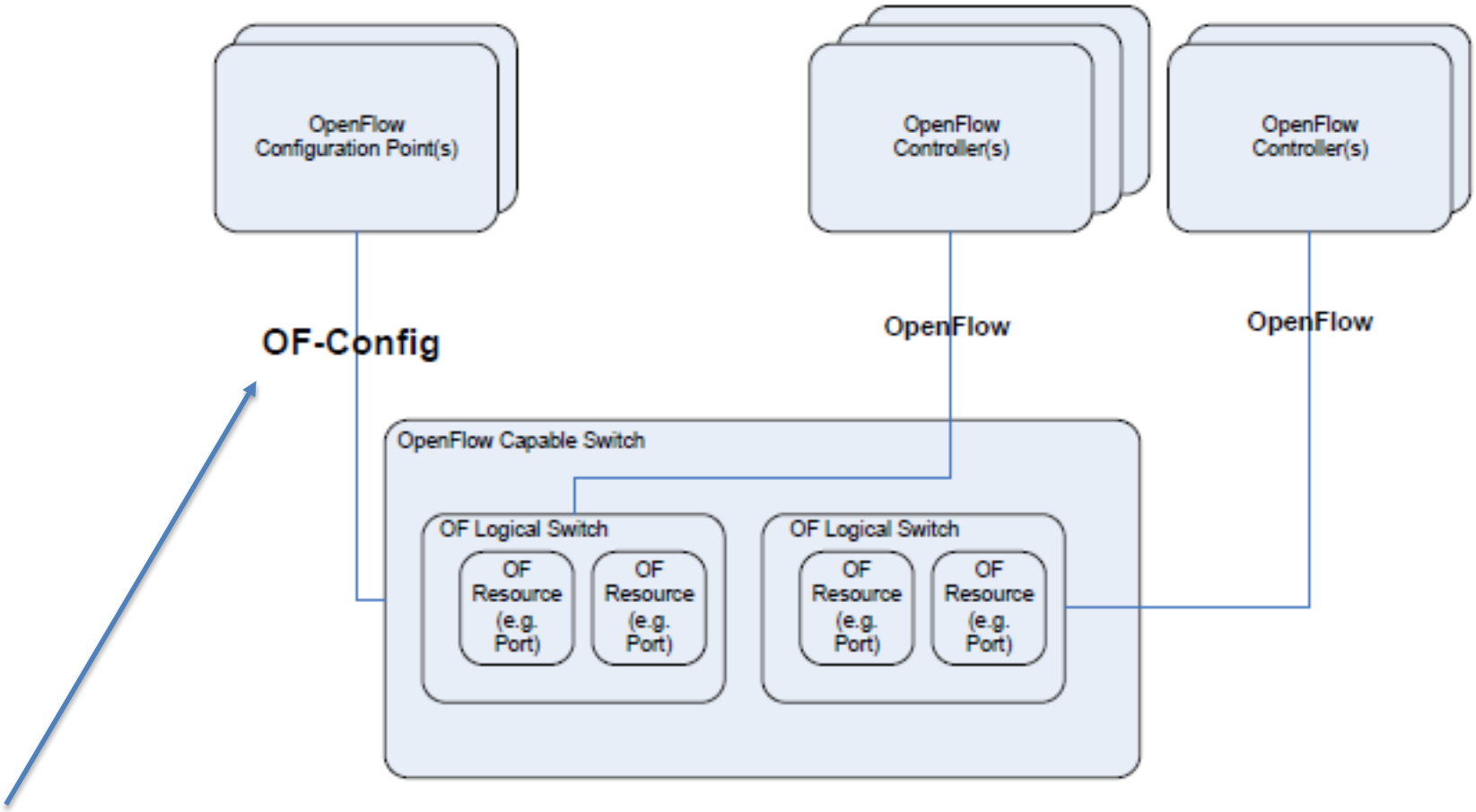
OF-Config 1.2 – OpenFlow Management and Configuration Protocol:

"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

OF-Config 1.2



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

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

Mininet – OpenVSwitch - WireShark

DEMO

End Session 2