WiFi Network Access Control for IoT Connectivity with Software Defined Networking

Winston Seah

School of Engineering & Computer Science

Background

- IoT – simple devices, specific services (e.g. some require DHCP, others may not).
- NAC has been traditionally divided along the lines of OSI MAC layer and network layer.
- Very few are programmable
- SDN presents an opportunity for programmability and working across both network and MAC layers.

Network Access Control (1)

Captive Portal

- Presents an authentication page to a user when trying to connect to a web page.
- User inputs necessary data for authentication & authorisation.
- If unsuccessful, access is denied or user is prompted again to enter credentials.

IEEE 802.1x

- Port-based NAC;
- Port → device's Media Access Control (MAC) address
- Role-based access control to authenticate users & apply policies (authorisation)
- No human interaction needed

Network Access Control (2)

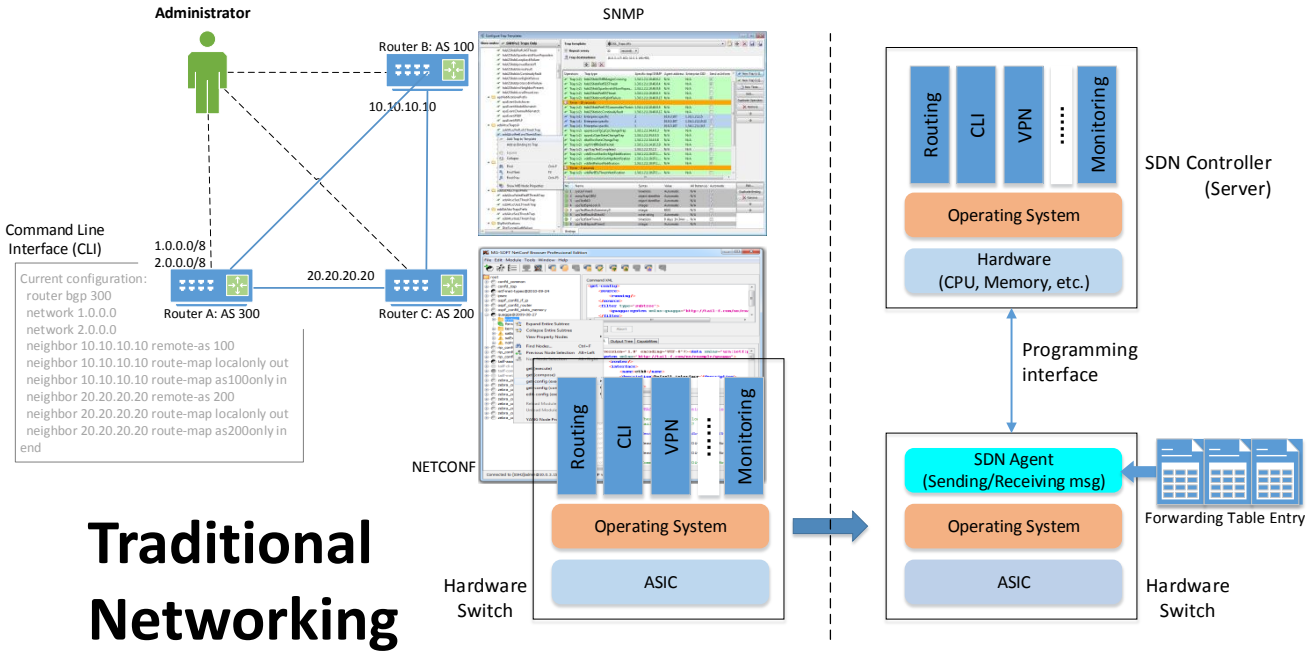
Captive Portal

- ✓ Flexible and not constrained to any specific technique / standard
- ✘ Unsuitable for devices that do not have a human user

IEEE 802.1x

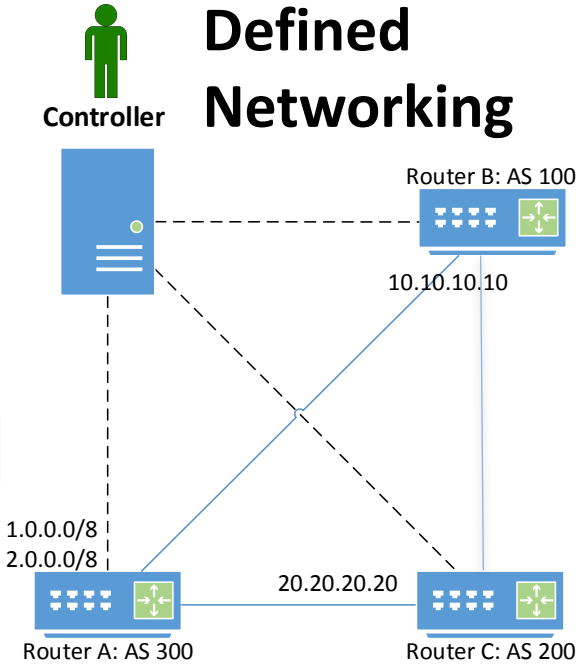
- ✓ Widely deployed; uses Extensible Authentication Protocol (EAP)
- ✘ Not supported by all devices
- ✘ Not suitable for guests as they must pre-obtain the credentials or certificates for authentication

SDN in a NutShell (1)

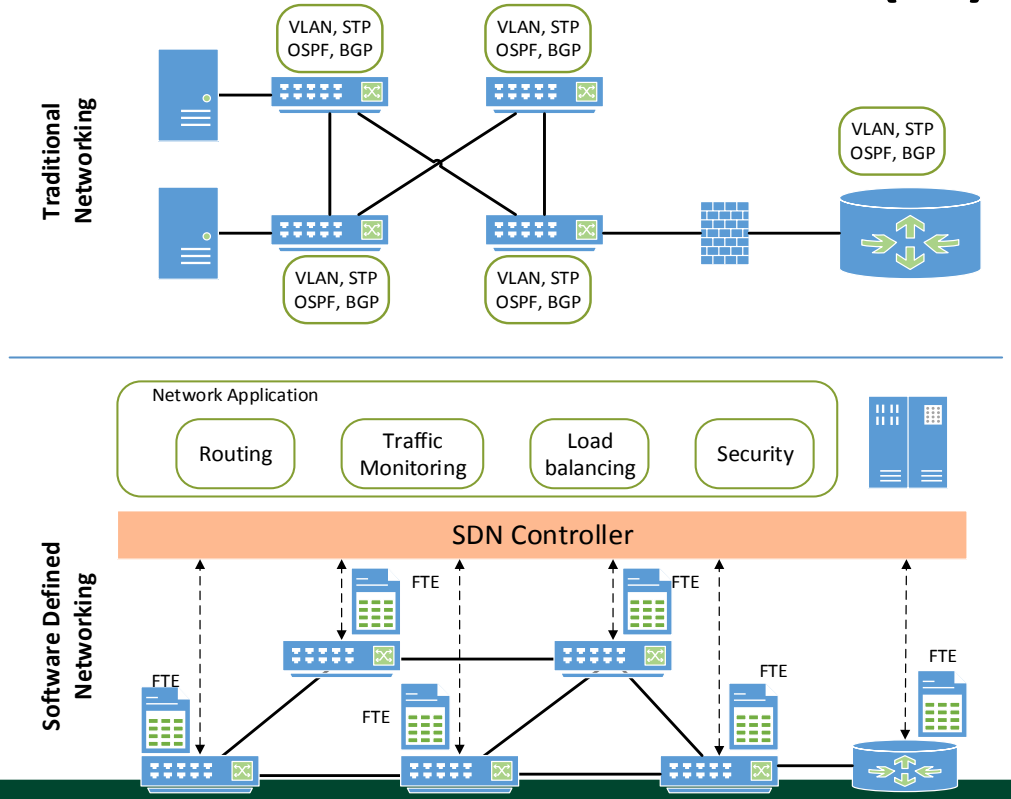


Traditional Networking

Software Defined Networking

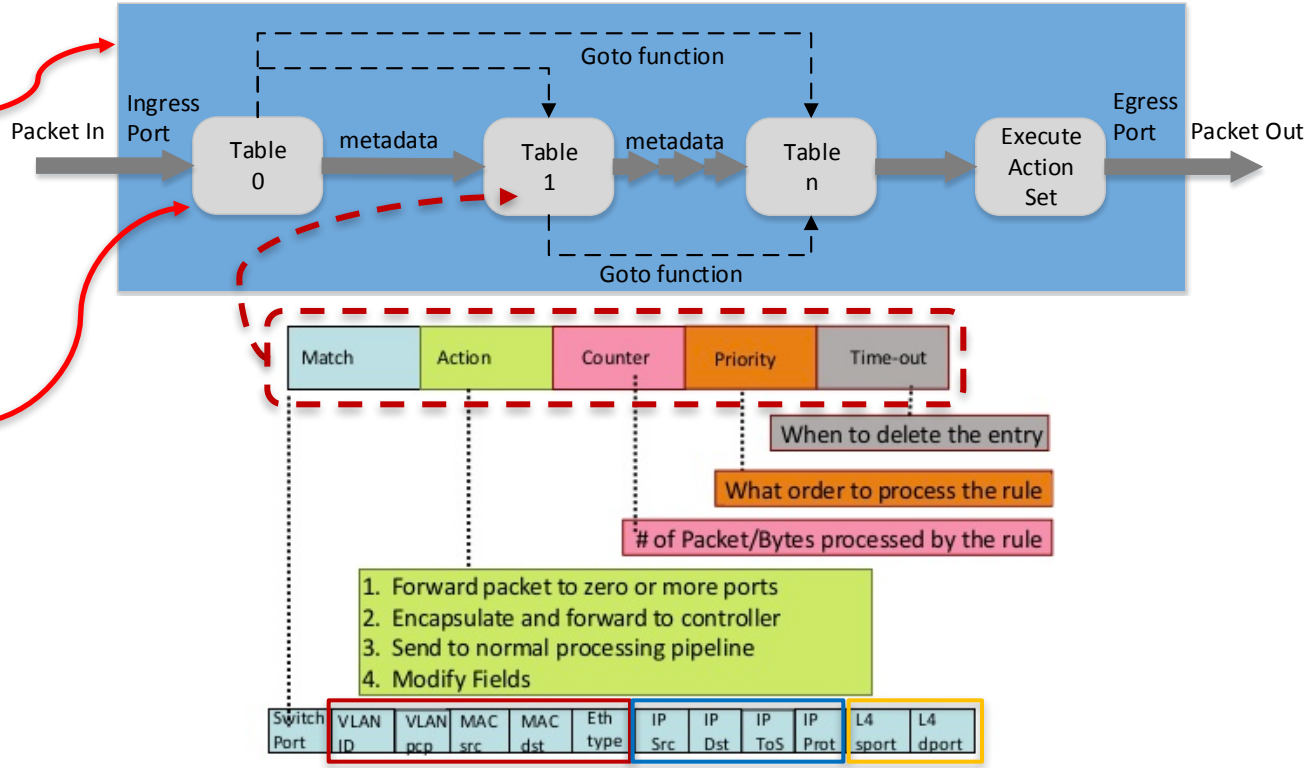


SDN in a NutShell (2)



SDN in a NutShell (3)

Multi flow table is a pipeline of single flow tables.



Our work within context

Work (Ref[])	SDN		L2 control	L3 control	Granularity
	Single Table	Multi-Table			
CapFlow[1]	✓			✓	Flow
RFC 7710[8]				✓	✓
SecureMAC [3]			✓		Device
NoCat[4]				✓	Flow
Our work		✓	✓	✓	Device/Flow/ Application

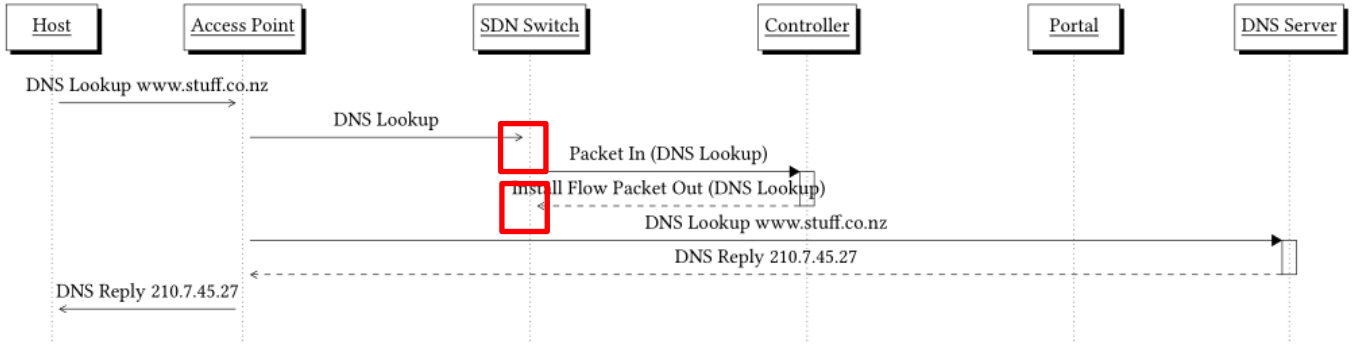
Our contributions

- A unified NAC framework for network layer + MAC layer + (application – not shown in this paper).
- We show how multi flow table in OpenFlow is provisioned to realise the unified NAC.
- Tested in operational network.

A multi flow table approach for unification

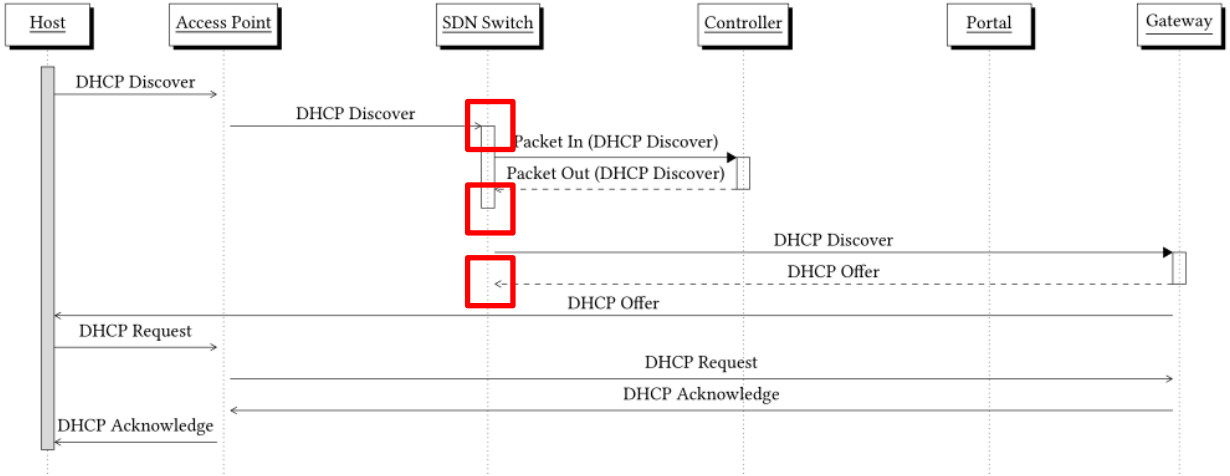
- Each table implements (or a combination of tables) the specifics of a certain protocol (e.g. DNS, DHCP, 802.1x).
- E.g. 802.1x and Captive portal use both IP and MAC tables.
- DHCP uses only IP table.

NAC based on DNS



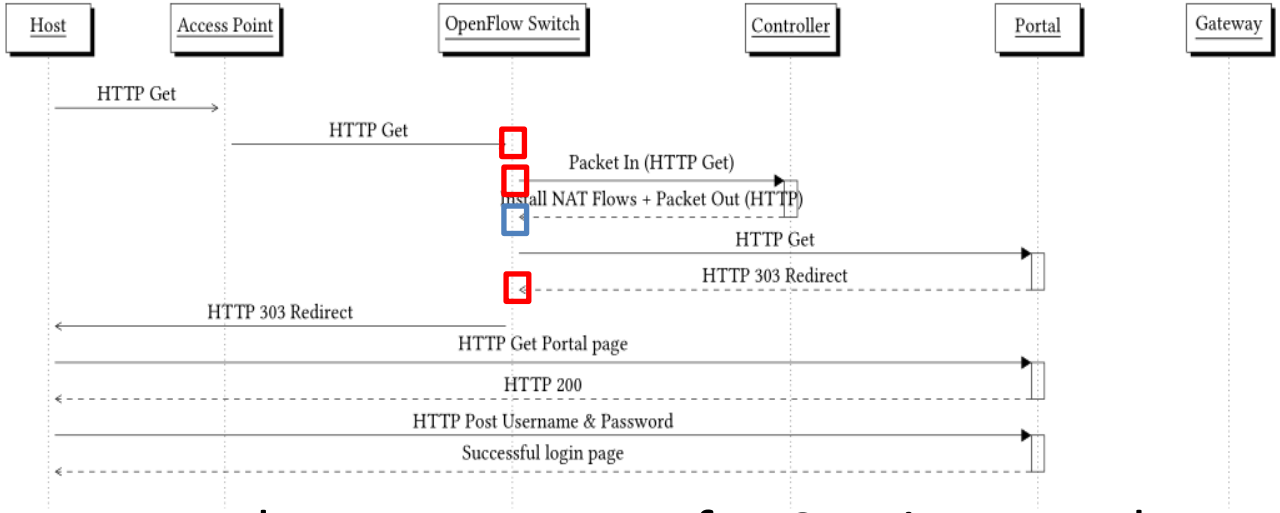
- Message exchange sequence for DNS.
- *Red boxes show the point where DNS tables are used for looking up.*

NAC based on DHCP



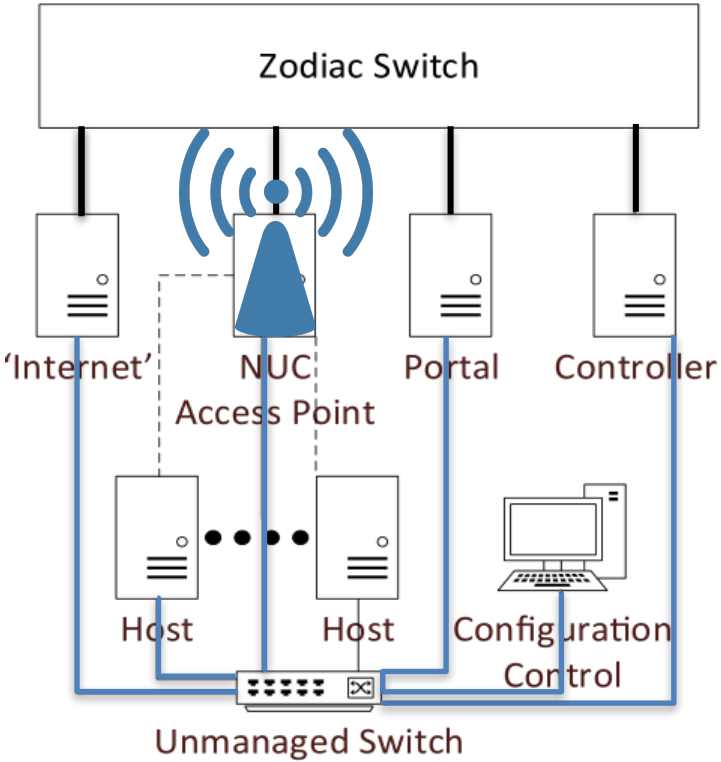
- Message exchange sequence for DHCP.
- *Red boxes show the DHCP packets matching a single table.*

NAC based on Captive Portal



- Message exchange sequence for Captive portal.
- *Boxes show the different tables used for flow matching.*

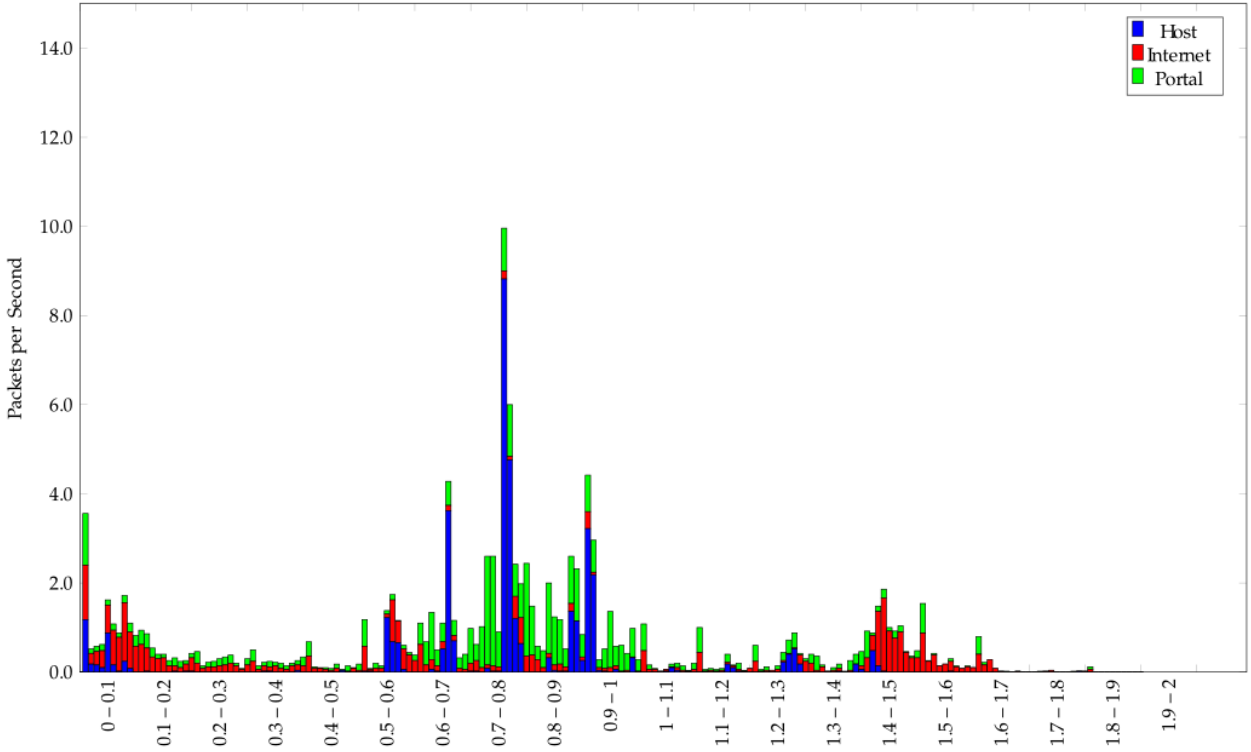
Test bed


Zodiac Switch
'Internet'
NUC
Access Point
Portal
Controller
Host
Host
Configuration
Control
Unmanaged Switch

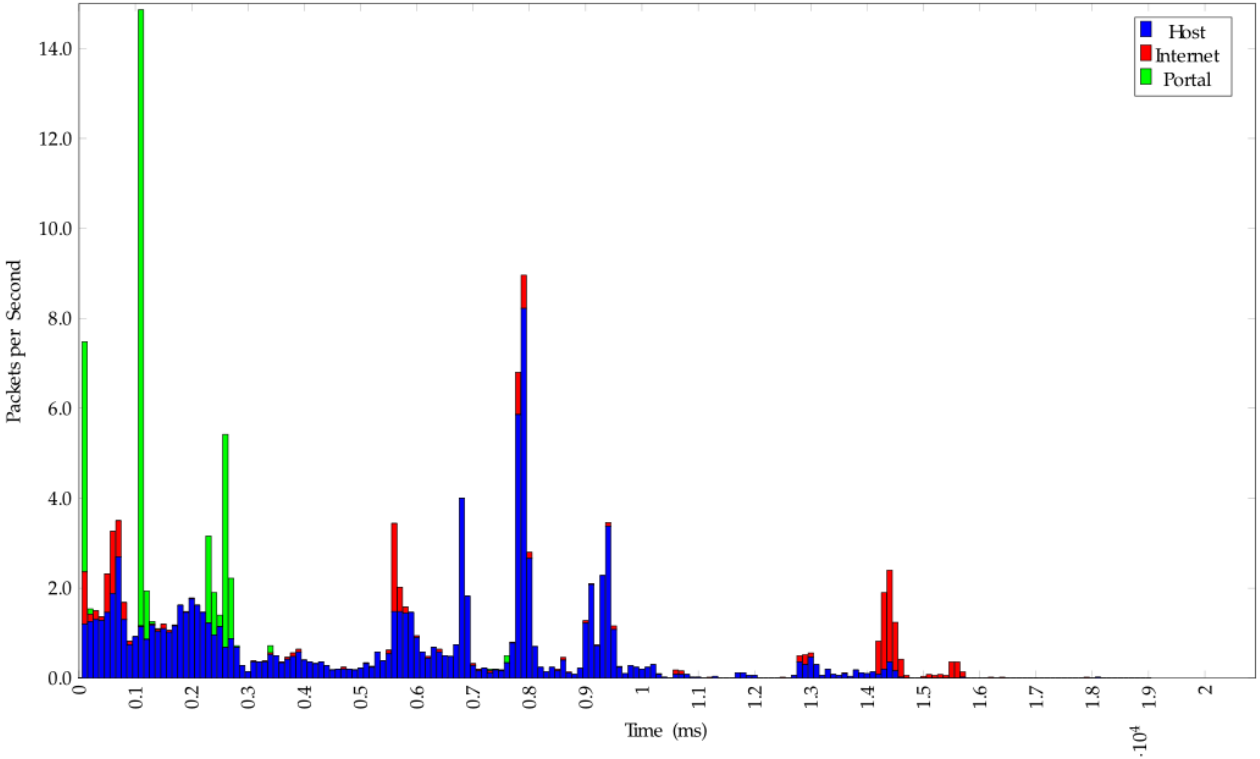
Results: Functional test

- We compare the average number of packets sent and received to demonstrate the functionality of the NAC framework.
- Take home from this set of figures:
  - Captive portal: access onset delay is longer, more packet exchanged for DNS & DHCP.
  - 802.1x : access delay is shorter, fewer packets exchanged.

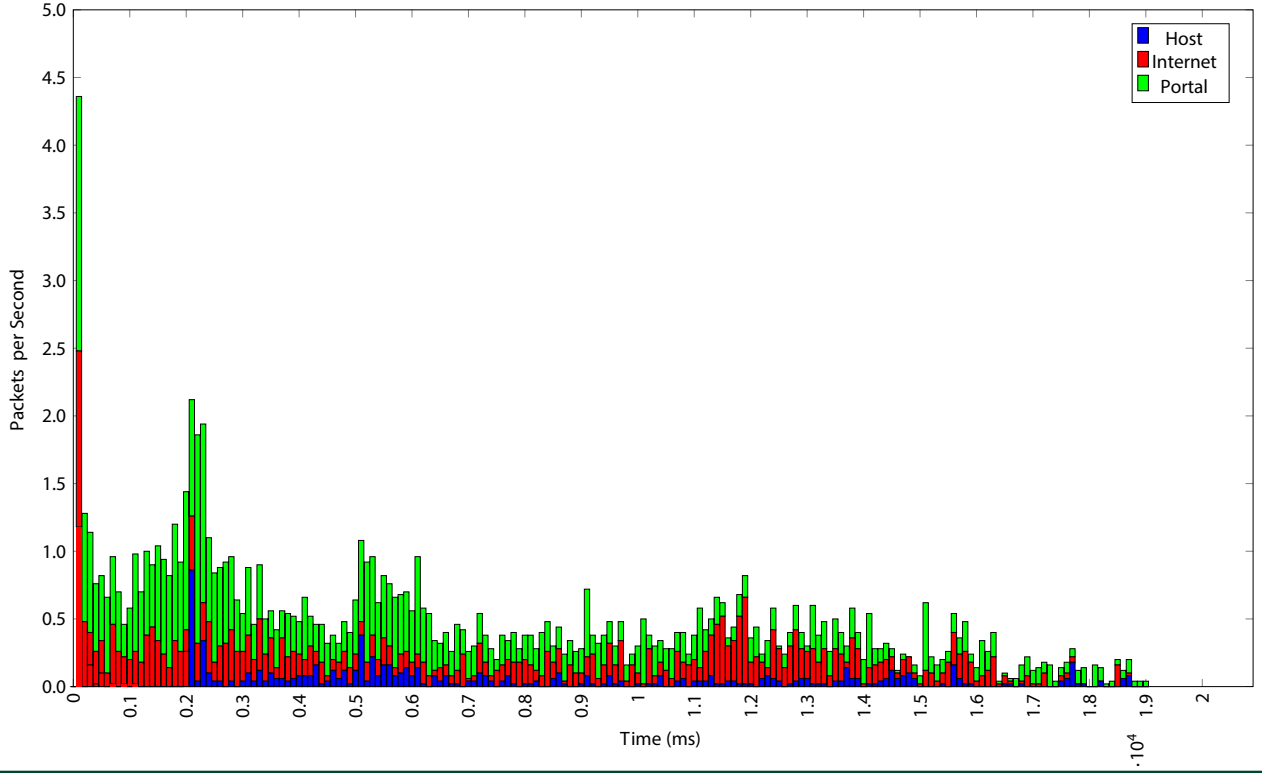
Packets Sent – Captive Portal



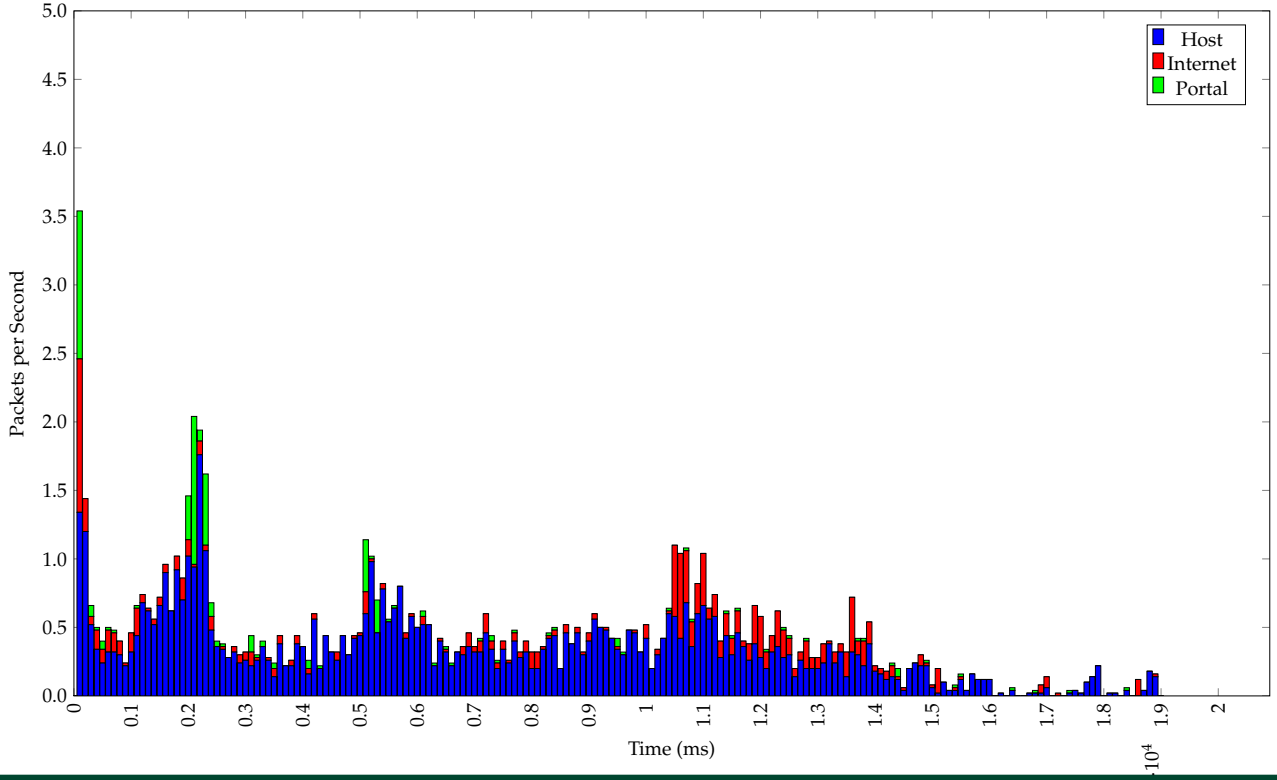
Packets Received – Captive Portal



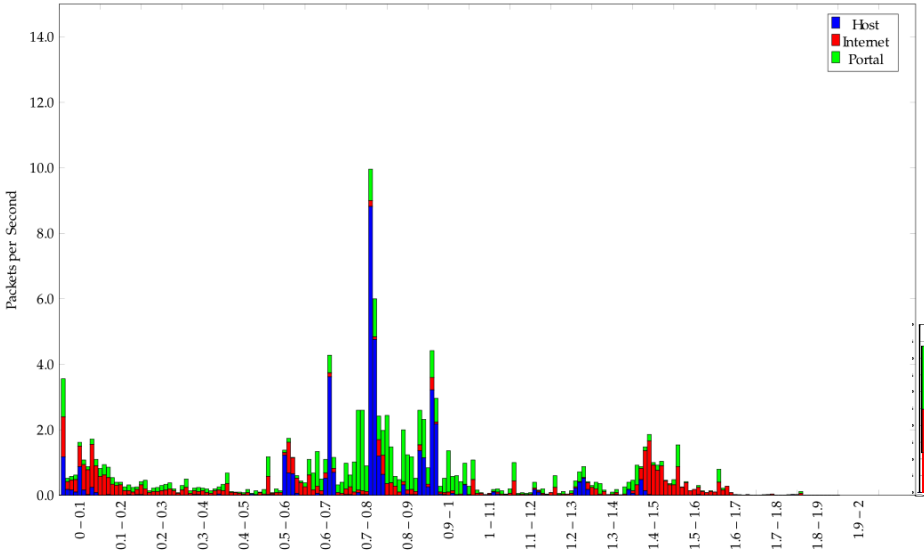
Packets Sent – 802.1x

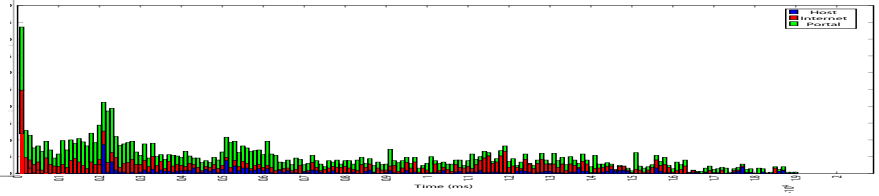


Packets received – 802.1x

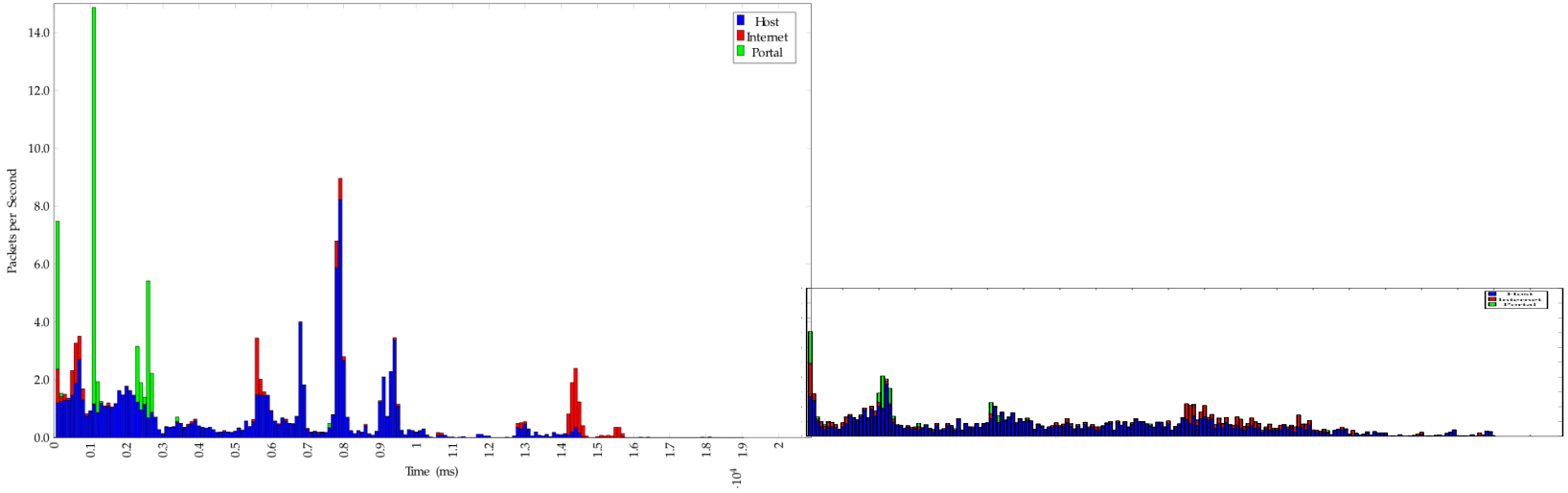


Side-by-side comparison (Sent)





Side-by-side comparison (Rcvd)



Performance Comparison

AVERAGE AUTHENTICATION DELAY (IN UNITS OF MILLISECONDS) AND AVERAGE NUMBER OF PACKETS EXCHANGED (DENOTED BY # PKT) FOR INCREASING NUMBER OF FLOWS. CORRESPONDING VARIANCES (ACROSS 50 RUNS) CALCULATED IN THE FINAL ROW.

Flows	DNS		DHCP		HTTP		802.1X	
	Delay	#Pkt	Delay	#Pkt	Delay	#Pkt	Delay	#Pkt
1	64.55	36.35	66.30	47.29	66.16	58.22	9.05	17.32
10	65.38	40.18	69.21	52.03	72.35	63.61	10.11	16.91
50	68.37	40.41	71.18	51.93	75.86	64.08	11.08	17.14
500	72.10	40.02	73.05	52.09	76.32	63.95	11.04	17.09
1000	73.55	40.56	74.91	52.00	78.08	64.02	11.08	17.54
Var	1.99	3.71	4.01	4.92	4.64	6.21	1.61	0.63

Highlights of our work

- IoT devices access diverse network functions via different protocols e.g. DNS, DHCP, HTTP.
- Unified network access control (NAC) with fine grained control using SDN.
- NAC using IEEE 802.1x : 72% less overhead and 80% lower delay compared to capture portal.

Ongoing & Future Work

- Deployed in our campus for field trials
- Implement a proper database where users/devices belong to groups and then have rules defined by groups, e.g. a distinct group for each class of IoT devices.

Contact: Winston.Seah@ecs.vuw.ac.nz

URL: http://www.ecs.victoria.ac.nz/~winston

THANK YOU!