Introduction to SDN technology

Bryan Ng,

Victoria University of Wellington

Outline

- Traditional networks – Control, Management and Data planes
- Routing & bridging – foray into software
- Programmable rules – Tables
- Centralised view of tables
- SDN defined
- Why SDN ?

Control, Management & Data

- Vast majority of packets → Data
- If one is unsure →
- Configure & monitor →

- Too complex
- Closed
- Cannot independently evolve

Routing & Bridging

- <1980 …. before Cisco & Huawei → PC's running software looks up tables (routing table)
- Then LANs became "in"
- Bridged frame ≠ Routed packet … fast forward → packet switch.
- Pc's running software can't cope

Tables – Programmable rules

- 1990's CAM were all the rage
- High speed lookups
- L2 is easier than L3
- Router & switch lines blurred

Centralise view of Tables

- Push intelligence down to forwarding table.
- Packet processing takes place in forwarding engine.
- One ring controls them all

SDN defined

- Plane separation
- Centralised control
- Simplified device

SDN (un)defined

- Open SDN
- API
- NFV

SDN drivers

- XaaS
- Reduced costs
- Lower barrier for start ups
- Faster release of features

Openflow overview & basics

Bryan Ng,

Victoria University of Wellington

Outline

- Overview
- Openflow 1.0
- Openflow 1.3
- Openflow limitations

SDN Applications

- Campus/Enterprise networks
  - Centralised policy application
  - Device & user security

- Intrusion detection

Campus networks

- Collection of LANs distributed over ….
- Some specific requirements
  - Access control & security
  - BYOD
  - Service discover
  - Firewalls ….. And more firewalls

Access control & security

- Use SDN to manipulate flow rules ← policy definitions.
- Pseudocode ~
  - User connect and attempt to send pkts
  - No policy … …. Send to controller
  - Controller looksup policy DB … he's our CTO … super user
  - Install flow rules for CTO …
  - May want to log his info?

Caveats

- Isn't this what NACs do today ?
  - Compare

    http://www.cs.princeton.edu/courses/archive/fall10/cos561/papers/Resonance.pdf

    …. with your fav appliance configuration.
- My take:
  - Simple, flexible, fine-grained … and xml (or your fav policy language)
- Does this scale ? (depends where u apply it, won't cut it at aggregation)

Device & user security

- Pseudocode
  - [.. Line 3] SDN controller installs rule: redirect to captive portal
  - Captive portal says o.k, notifies controller.
  - Controller install rules in switch

Caveats

- Edge switch must allow ARP, DNS, DHCP requests to relevant servers
- DHCP reply is copied to controller.
- Using end-users' MAC, the controller checks if it is a registered user.
- Flow table overflow !!!

IDS

- Openflow rules can dynamically modify “tap”
- Tap ={MAC addr, VLAN, ingress port …}
- Tap forwards out to and IDS