SERVICE FRACTAL

Challenges with Cloud based Switch Mgmt.

Shivaram Mysore, Founder/CEO
Mark Hapner, Chief Architect

(415) 787-5578 | @ServiceFractal

Thank you


Faucet


OvS
Open vSwitch


Allied Telesis


cisco


intel


Hewlett Packard
Enterprise
aruba


amazon
web services™


Google

Pay-as-you-go

A Cloud platform for Networking & Security Operations

Target consumers are **Enterprises, Branches and Campus**

Operators use Service Fractal Cloud to manage on-prem L2/L3 network switches

- Vision is to create **platform of applications for zero-friction network & security** management
- Emphasis on **simplicity, efficiency & elastic**
- **Instant analytics**
- **No** API or skills training needed

We are reimagining the distributed edge

Streaming Telemetry

Events

SERVICE FRACTAL

Dynamic Control

sFlow

OpenFlow

gNMI, Netflow, etc

gRPC

OpenFlow

NETCONF, gNOI

OPENCONFIG

On-Prem Network Equipment →

Business Outcome Specific Apps - Examples

Sideout, Network vitals, Bandwidth usage, Switch Stacking, Port Mirroring, Firewall, Threat intelligence enabled Firewall, Tapestry, Microsegmentation, Network planning, Asset management, Switch firmware update, Bandwidth control, Device identification, Accelerating MapReduce

Pricing

$250/m

100G of Data, unlimited number of switches or ports or capacity (1-100G)

Faucet

- Enables Control & Monitoring of network switches
- Multi-vendor is a key differentiator
- Required Switch Capabilities:
  - Protocol support for Openflow v1.3 or P4
  - Pass Faucet Test suite
  - Optional: GNMI / GNOI Protocol support
  - One Openflow managed port used as “uplink”
  - # of Controllers to configure: (1) Control (2) Monitor (3) Local Survivability (4) HA Mode+
- Service Fractal specific requirements
  - TLS support for Control connectivity
  - Optional: DNS support
  - Optional: TLS (Encrypted) Service Name Indication (SNI) support
  - Dial-out only support for GNMI / GNOI

Switch Provisioning Challenges

- Configure in Openflow mode (all manual steps)
- Partial or Full (reboot)
- Select ports
- Key Provisioning (numerous steps - Trust Anchor, generation, CSR, Cert upload; Cert chain upload is mostly not supported)
  - The root certificate container supports only one root certificate not a chain. The root cert supported is the one CSR is signed with.
  - CSR generation needs prior configuration with Cert fields (CN, OU, O, L, State, Country)
- No support for separate control channel - currently, management port is also used for control (even though it is dial-out). This port needs outbound Internet connectivity. This risk profile is not supported by some organizations
  - Downside of “Control channel” port is loss of one more ethernet port (can be 1Gb)
- Capture DP ID and switch ports for inclusion in `faucet.yaml`

DNS support on Switches

Configure Controller with Fully Qualified Domain Name (FQDN) instead of IP Addresses

- Controllers are run on VMs or Containers in totally different network segments
- Use of IP implies routing policies are set accordingly & Firewall ports open
- Use of FQDN relies on DNS infrastructure
- With use of dynamic software infrastructures, controllers are deployed and relocated. If Switch uses FQDN to connect to controller, then a change in IP address is automatically resolved with no change to switch configuration

TLS (E)SNI support on Switches

- SNI - Service Name Indication
  - A TLS extension used by client to indicate which hostname it wishes to connect at the start of TLS handshake process
  - ESNI - Encrypted SNI: To address domain/host name eavesdropping
- Current mode for Openflow controller configuration on OVS is: `ssl:controller.example.org:6653` → indicates controller service is available on port `6653` - an exposed port that is open for attacks.
- If Controller is available as a Microservice in a cloud infrastructure, it normally resides behind a Reverse Proxy
- If TLS (E)SNI is supported, then we can open only port `443` - standardized testing can be applied.
- TLS (E)SNI can also help us (Cloud SPs) by using limited number of Public IPs

GNMI / GNOI

- Need for Dial-out only support
- Unsure if this would use Management port or Control channel port if one were available

Questions

1. Any efforts to simplify switch provisioning from Openflow point of view?
2. Provide an automated way of including DP ID and switch ports for inclusion in `faucet.yaml`?
3. Enable DNS support on switches
4. Enable TLS (E)SNI support in switches - OVS has some support
5. Can we improve Certificate-Key provisioning?
6. Can we use DHCP options on the switch for automating provisioning items such as:
    a. Openflow mode + ports
    b. DNS Resolver IP
    c. Controller FQDN
    d. Create PKI profile

- ✓ *Simplicity*
- ✓ *Time-to-value (real-time: data to actionable)*
- ✓ *Multi-vendor*
- ✓ *Scale*
- ✓ *Fine-grained network telemetry on low bandwidth*
- ✓ *SaaS*

SERVICE FRACTAL

Call us for Cyber Networking

sales@ServiceFractal.com

(415) 787-5578