LANCASTER UNIVERSITY

SDN & NFV: an IETF Perspective.

FIA Athens
Workshop on Network Virtualization

Daniel King – d.king@lancaster.ac.uk

IETF SDN History

- Working on SDN concepts for over 10 years
  - GSMP
  - FORCES
  - PCE
  - MPLS & GMPLS
- "SDN" work started late 2011
  - IETF BoF 400 participants
  - Boiling the SDN ocean
  - Eventually became an IRTF working group
    - Current work items include terminology and architecture proposals

IETF SDN & NFV Efforts

- Current Working Groups
  - Path Computation Element - PCE
  - Interface to the Routing System - I2RS
  - Segment Routing - SR
  - Service Function Chaining – SFC
- Recent Working Group Initiatives
  - Virtual Network Function Pools – VNF Pool
  - Abstraction and Control of Transport Networks – ACTN
  - Network Function Virtualisation Configuration – NFVCON

Why I2RS?

- SDN focuses on programming the data plane
  - Switch programming (cross-connects)
  - Forwarding (FIB)
- There are many functions and features not covered by SDN
  - Control of routers
  - Control of routing protocols
  - Management of the "routing system"
- Existing techniques are non-standard
  - Using CLI to achieve these functions is very frustrating
  - Expensive, time-consuming, error-prone, risky
- Use Cases include
  - Programming and managing the RIB
  - BGP use cases
  - Traffic steering and classification
  - DDoS mitigation
  - Topology reading, monitoring, and control

Why SR?

- IP Source Routing
  - A list of IP hops to traverse
  - IPv4 Options for Loose and Strict Source Routes
    - Only 9 hops, don't cross AS boundaries, not used
  - IPv6 Source Route
    - Deprecated!
- Source-aware Routing
  - Hop-by-hop routing decisions take account of source as well as destination
  - A form of policy-based routing
- Source-based Classification to a Tunnel
  - A concept applying to any tunnelling and especially MPLS
  - Packets are labelled and then follow an LSP
- Explicit Routing
  - A term usually associated with MPLS-TE path establishment
  - Packets follow the path of a pinned LSP

Why SFC?

- User services consist of multi-tiered functions
  - Multiple distributed entities (e.g., Web server, load balancers, data base servers, etc.) cooperate to provide a service
- Individual workload components communicates with each other in carefully defined ways
  - Traffic between components is required (by policy) to flow through specialized network services (e.g., firewalls, IDS, etc.)
  - Resultant communication flows are modelled as "service chains"
- Steering of traffic between services within a service chain is achieved via L2/L3 data plane forwarding
  - Complex and difficult to automate
  - Predicted scaling challenges
- Current network service deployment models are generally static, hard to manipulate (create, move, destroy)
- Currently no (efficient) way to share information between the network and services, or among services in a chain

Why VNF Pool?

- Network functions are typically deployed as specialized hardware servers
- NFV looks to implementing network functions as software instances running on commodity servers
  - These virtualized functions are called Virtualized Network Functions (VNFs).
- A group of VNFs, is a VNF set.
  - A VNF set can include a single or multiple types of VNF (e.g., virtual firewall, virtual load balancer), where each type of VNF is realised as a number of VNF instances which is also referred to as a VNF pool.
- The VNF Pool will focuses on mechanisms supporting the reliability of a VNF set.
  - Redundancy within a VNF set, and stateful failover among VNF pool members.
  - Additional mechanisms for reliable VNF sets might be included after further gap analysis between identified requirements and existing IETF technologies.

Why ACTN?

- A growing need for network programmability, automation, resource sharing, and service elasticity / adaptability.
- As transport networks evolve, the need to provide network abstraction has emerged as a key requirement for operators.
- Managing resource requests, network slicing and presentation, via an interface to customers and applications.
- Traffic Engineering (TE) technologies exist per domain (technology or administrative) but network providers may be unwilling or unable to disclose full TE attributes and topologies.
- ACTN Principles
  - Customer-initiated Resource Setup
  - Network Partitioning
  - Automation and Orchestration
  - Recursion
  - Internetworking with Existing Technologies

IETF Contributions

- Participation is warmly welcomed
- Things to do…
  - Subscribe to mailing lists and read the threads
  - Read Internet-Drafts and comment on them
    - In private to the authors if you are shy ☺
    - Make editorial or technical comments
  - Initiate work you care about
    - Send mail
    - Write an Internet-Draft
    - Ask operators and vendors to work with you
  - Ask WG Secretaries, Chairs and Area Directors for help

Thank you!

Questions?

Daniel King – d.king@lancaster.ac.uk