Applicability of ACTN to Network Slicing

draft-king-teas-applicability-actn-slicing-03

D. KING (UNIV. OF LANCASTER) & Y. LEE (HUAWEI)

CONTRIBUTORS:

M. BOUCADAIR (ORANGE), S. BELOTTI (NOKIA),

D. CECCARELLI (ERICSSON), H. ZHENG (HUAWEI)

What do we mean by Network Slicing?

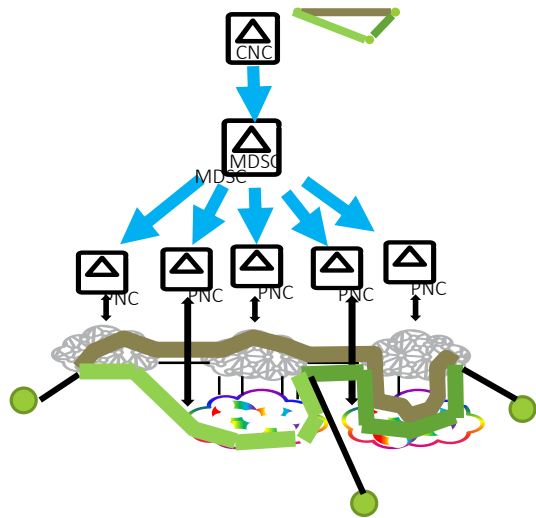- **TE Network Slicing Definition (from the ACTN Framework)**

  In the context of ACTN, a TE network slice is a collection of resources that is used to establish a logically dedicated virtual network over one or more TE networks. TE network slicing allows a network operator to provide dedicated virtual networks for applications/customers over a common network infrastructure. The logically dedicated resources are a part of the larger common network infrastructures that are shared among various TE network slice instances which are the end-to-end realization of TE network slicing, consisting of the combination of physically or logically dedicated resources.

- Essentially network slicing (in the context of ACTN) provides **Traffic Engineered** connectivity to serve customers with a wide variety of service constraints, which may be characterised with metrics such as:
  - Latency, reliability, capacity, and service function specific capabilities

ACTN Requirements for Network Slicing

- **Resource Slicing**: provide a range of services both by partitioning (slicing) the network resources and provide specific Service Functions with the required chaining logic

- **Network and Function Virtualization:** The resources to be virtualized can be physical or already virtualized, supporting a recursive pattern with different abstraction layers

- **Resource Isolation:** operate concurrent network slices across a common shared underlying infrastructure
  - **Performance**: Each slice is defined to meet specific service requirements, usually expressed in the form of Key Performance Indicators (KPIs)
  - **Security**: Attacks or faults occurring in one slice must not have an impact on other slices, or customer flows, if required, are not only isolated on network edge, but multiple customers traffic is not mixed across the core of the network
  - **Management**: Each slice must be independently viewed, utilised and managed as a separate network

- **Control and Orchestration:** Orchestration is the overriding control method for network slicing
  - **Multi-domain Orchestration**: Managing connectivity setup of the transport service, across multiple ~~administrative~~ domains which belong to the same administrative entity;
  - **End-to-end Orchestration**: Combining resources for an "end-to-end" service (e.g., transport connectivity with firewalling and guaranteed bandwidth and minimum delay for premium radio users (spanning multiple domains).

Achieving Network Slicing using ACTN

- The Abstraction and Control of Traffic Engineered Networks (ACTN) defines an SDN-based architecture
  - Uses concepts of network and service abstraction to detach network and service control from the underlying data plane technology
- A Virtual Network (VN) is a slice allocated to customer meeting customer's service requirements:
  - Isolation (hard/soft/sharing)
  - Resource reservation/guarantee
  - Reliability
  - PM programmability/ monitoring
  - Underlay visibility
  - SF/VNF/NF aware connectivity

CNC

MDSC

PNC PNC PNC PNC PNC

Create VN {
  End Points
  VN Members
  QoS Metrics for VN
  Isolation
  Reliability... }

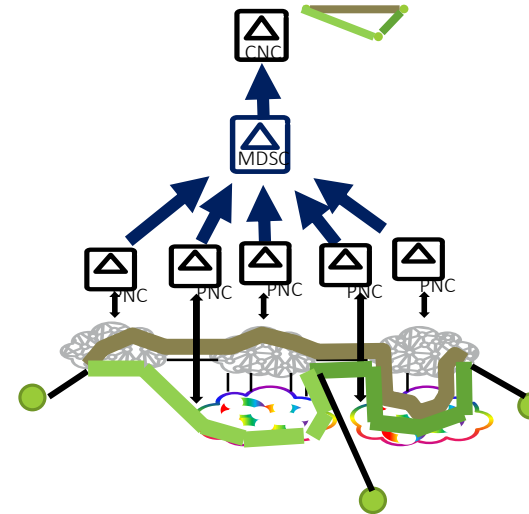# Key ACTN Building Blocks for TE Network Slicing

draft-ietf-teas-actn-framework
draft-ietf-actn-vn-yang

- Orchestration and control of VNS
- CRUD operation of VN slices
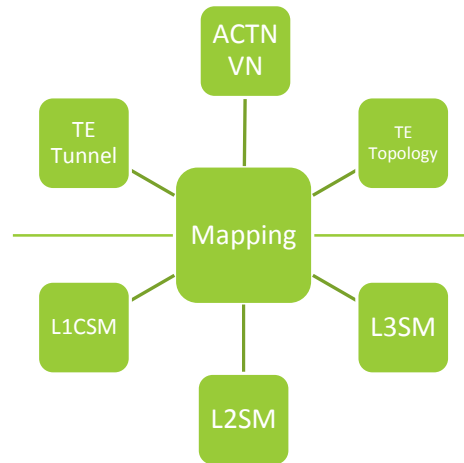
draft-lee-teas-te-service-mapping-yang

- TE & Service Mapping for overlay & TE-underlay visibility
- Provides Service Requirements for isolation, reliability, and so on.

draft-lee-teas-actn-pm-telemetry-autonomics

- Subscription of KPI PM data per VN and Telemetry streaming of PM data to VN owner.
- Customized Autonomous Scaling mechanism with PM data
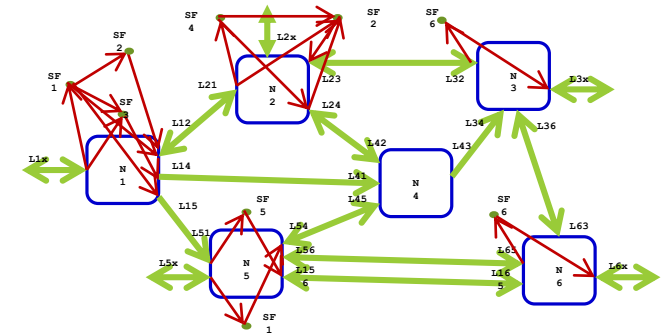
draft-ietf-teas-sf-aware-topo-model

- Enhancement of TE network slicing with connectivity + SF/VNF/NF and compute/storage aware topology.

What Additional IETF Work Might Be Needed?

- Virtual Network Service (VNS) Security and Isolation
  - Secure slicing and isolation of resources
    - Consumers may expect and require that there is no risk of leakage of data from one slice to another
    - No transfer of knowledge of the structure or even existence of other slices, and that changes to one slice (under the control of one consumer) should not have detrimental effects on the operation of other slices
  - Policy control of slices
    - Managing who and how the VNS creation and modification will be achieved, and also the scope of slice setup and possible modifications/re-optimizations

- Requesting compute, storage and function resources during VNS setup
  - Including VNF type, size, location and ensuring correct service chains
  - The only technical work would be additional YANG modules

Next Steps

- This draft can be used to share and socialize what IETF is doing in regard to TE network slicing inside and outside of IETF.

- Thoughts?

- Comments?

Thanks!