TEAS Working Group
Internet Draft
Intended status: Informational
Expires: January 8, 2020

Y. Lee
Futurewei

J. Kaippallimalil
Futurewei

July 8, 2019

Applicability of ACTN to Support 5G Transport

draft-lee-teas-actn-5g-transport-00

Abstract

This draft is aimed to provide an applicability of Abstraction and Control of Traffic Engineered (TE) Networks (ACTN) for an end-to-end service assurance mechanism for 5G transport network. ACTN is an IETF standard architecture enabling virtual network operations to control and manage large-scale multi-domain, multi-layer and multi-vendor TE networks, so as to facilitate network programmability, automation, efficient resource sharing. 3GPP 5G requirements calls for Network Slicing support for various use cases such as enhanced mobile broadband (eMBB), massive machine-type communications (mMTC) and ultra-reliable and low latency communications (URLLC). In order to support these new requirements over multiple transport networks for 5G transport, the current 3GPP 5G architecture needs to support dynamic instantiation of end-to-end paths that assure service assurance and performance guarantee for traffic classes characterized by network slicing.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

ACTN framework defines the requirements, use cases, and an SDN-based architecture, relying on the concepts of network and service abstraction, detaching the network and service control from the underlying data plane. ACTN architecture encompasses Provisioning Network Controllers (PNCs), responsible for specific technology and administrative domains, orchestrated by Multi-Domain Service Coordinator (MDSC), which, in turn, enables underlay transport resources to be abstracted and virtual network instances to be allocated to customers and applications, under the control of a Customer Network Controller (CNC) [RFC8453].

A network slice is defined by 3GPP as an end-to-end logical network comprising a set of managed resources and network functions [3GPP TS 28.531]. Its definition and deployment starts from the RAN (Radio Access Network) and packet core, but in order to guarantee end to end SLAs (Service Level Agreements) and KPIs (Key Performance Indicators) especially for applications that require strict latency and bandwidth guarantee, the transport network also plays an important role and needs to be sliced as part of services bound to the different slices.

However, it is not easy for mobile network clients to interface directly with transport networks [Transport-Slicing]. Current GSMA guidelines for interconnection with transport networks [IR.34-GSMA] provide an application mapping into DSCP. However, apart from problems with classification of encrypted packets, these recommendations do not take into consideration other aspects in slicing like isolation, protection and replication. For example, during a PDU session setup the 3GPP control plane selects a 3GPP slice, 5QI (QoS parameters) and programs the user plane (gNB, UPF). This 3GPP slice and QoS firstly needs to have a corresponding mapping in the transport network segment(s) between the 3GPP user plane functions (N 3GPP Slices: M Transport). Secondly, there needs to be a mechanism for carrying the meta-data corresponding to the mapping in IP packet header so that the transport network can grant the service level provisioned.

ACTN has been driving SDN standardization in IETF in the TEAS (Traffic Engineering and Signaling) WG with the emphasis of providing the desired customer interfaces that enable dynamic and automatic transport network slice instantiation and its life cycle operation [VN-Model],[Transport-Slicing].

This draft presents an extended ACTN architecture with 3GPP 5G transport architecture in order to provide a novel approach for an end-to-end service assurance mechanism to meet 3GPP 5G requirements for support of enhanced mobile broadband (eMBB) and for new ‘use cases’ that require massive machine-type communications (mMTC) and ultra-reliable and low latency communications (URLLC). In addition, this draft addresses requirements for transport network provisioning function requirements and data plane network programming to support end-to-end service assurance mechanism.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. IETF ACTN Virtual Network Slicing Service Model

IETF ACTN VN model [VN-Model] discusses customer initiated virtual network slicing data model in which customer can control their virtual network slice to fit their needs. This model fulfills the key requirement: the ability for the customer to define and convey their virtual networks without having to understand transport network details [VN-Model]. This is for CNC (Customer Network Controller) – MDSC (Multi-domain Service Coordinator) Interface (CMI) of ACTN, as shown in Figure 1. This model describes VN YANG model for customer access points, virtual network access points, Virtual Network (VN) identifiers, its VN-members, any constraints and policy customer cares for with respect to its VNs. Figure 1 shows the process of VN creation in the context of ACTN architecture.

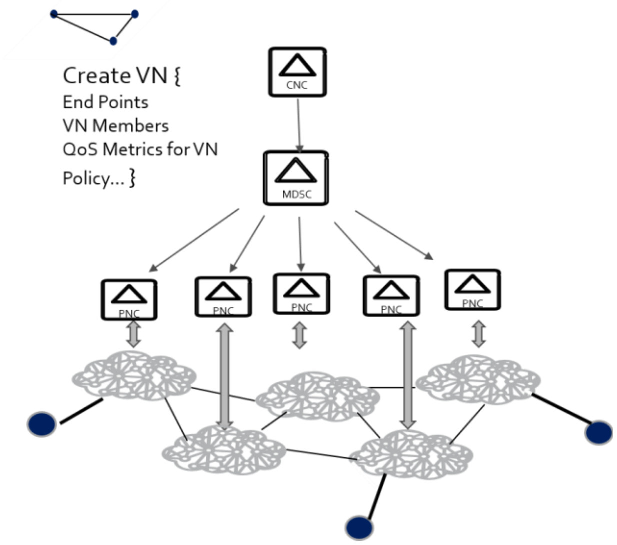

Figure 1. Virtual Network Slicing Service Creation

Figure 1 [VN-Model] shows that VN Slicing Service model enables customer to create its VN without having to know the transport underlay details and to indicate its end-points with constraints (e.g., bandwidth, latency, load-balancing, protection, etc.) per VN or VN-member level. This model facilitates customer-driven dynamic life-cycle VN service operation.

The CMI plays an important role interfacing 5G 3GPP mobile network with transport networks. From a context of 5G transport network architecture, the CNC is the entity that is responsible for 3GPP access network coordination with transport networks. This entity is referred to as Traffic Provisioning Manager (TPM) for 3GPP/5G context. Sections 3 and 4 discuss TPM function in details.

3. 3GPP 5G Network Architecture

Mobile network backhauls in the past have used static configuration and provisioning of routers for traffic engineering (TE). These estimates maybe revised and TE is configured periodically based on demand and other performance criteria - however, this process takes a long time (in the order of weeks or months), thus may not be suitable for dynamically changing context such as 5G mobile network.

In 5G systems [3GPP TS 23.501], [3GPP TS 23.502] with a large range of services, low latency paths and mobility, the demand estimate varies much more dynamically (in the order of several minutes in the worst cases). Backhaul networks that provide capabilities to reprogram routers and switches to meet the new demand profile are needed.

In addition to the configuration and provisioning of traffic engineered paths between mobile and transport network providers, there is the question of how to enforce policies for slices, QoS across multiple transport network domains in mobile network and transport network. Each transport domain may employee different data plane technologies such as IP, MPLS, SR-MPLS, SRV6, OTN/WDM, etc. From an end-to-end 5G transport network perspective, it is paramount to ensure predictable and consistent service quality across all domains.

Figure 2 shows an enhanced 5G transport network architecture with an overview of the TPM function. The TPM is deployed in each of the two domains/sites (Domain 1/Site 1, Domain 2/Site 2) and interfaces with other mobile network functions (e.g., Session Management Function (SMF), SDN Controller (SDN-C), etc.) while providing interfaces to transport network orchestrator (i.e., MDSC). Note that TPM is a new function to be added and implemented in the current 3GPP architecture and this should be addressed in 3GPP. Detailed description of the TPM is in section 4.

Figure 2 shows three segments/domains for 5G transport network.

- N3 segment/domain between Next Generation NodeB (gNB) and User Plane Function (UPF) - Uplink Classifier (ULCL) is over the transport network at that site (Data Center/Central Office).

- N9 mobile connection transport, there are three transport segments/domains - the transport at each mobile network site (1, 2) and the backhaul network in between.

- N6 transport segment between UPF - PDU Session Identifier (PSA) and Application Servers (AS) is over the transport network at that site (Data Center/Central Office).

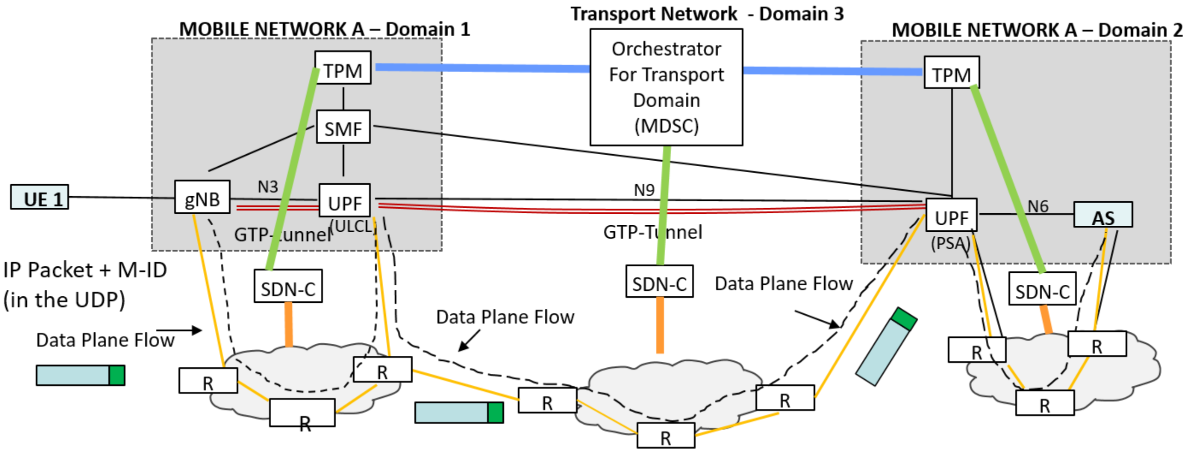
Transport Network - Domain 3
MOBILE NETWORK A – Domain 1
MOBILE NETWORK A – Domain 2
TPM
SMF
Orchestrator For Transport Domain (MDSC)
TPM
UE 1
gNB
N3
UPF
(ULCL)
GTP-Tunnel
N9
GTP-Tunnel
UPF
(PSA)
N6
AS
IP Packet + M-ID (in the UDP)
SDN-C
SDN-C
SDN-C
Data Plane Flow
Data Plane Flow
Data Plane Flow
R
R
R
R
R
R
R
R
R
R

Figure 2. Enhanced 5G Transport Network Architecture

The N3, N9 and N6 transport segments outlined in the figure are exemplary. For instance, gNB itself may need transport network when DU (Distribution Unit) and CU (Central Unit) are separated.

4. Transport Network Provisioning

4.1. Mobile Transport Network Context

The TPM in Domain 1 in Figure 2 is the initiator of the e2e network slice policy as it would estimate traffic matrix and determine service quality for each traffic class coupled with network slice requirement. This policy is referred to as Multi Transport Network Context (MTNC) and identified with MTNC Identifier. The MTNC Identifier is allocated for each traffic class.

The MTNC represents a transport network slice, QoS configuration for a transport path/VN between two 3GPP user plane functions (e.g., between gNB and UPF and between UPF-ULCL and UPF-PSA) and between UPF-PSA and Application Servers (AS). The MTNC include a set of requirements, such as quality of service (QoS) requirements, class of service (CoS), a resilience requirement, and/or an isolation requirement, and so on, according to which transport resources of a transport network are provisioned for routing traffic between two service end points.

The MTNC identifier is generated by the TPM to be unique for each path and per traffic class (including QoS and slice aspects). Thus, there may be more than one MTNC identifier for the same QoS and path if there is a need to provide isolation (slice) of the traffic. It should be noted that MTNC identifiers are per class/path and not per user session (nor is it per data path entity). The MTNC identifiers are configured by the TPM to be unique within a provisioning domain.

4.2. Transport Provisioning

As introduced previously, from a context of 5G transport network architecture, the TPM (a type of CNC) is the entity that is responsible for 3GPP access network coordination with the backhaul transport network. The TPM is the requester of VNs and collaborates with the MDSC to form a closed feedback loop with regard to traffic class associated with each VN, which in turn maps with network slice requirements. Thus, the TPM plays a central role from an orchestration point of view interacting with transport network’s orchestration (i.e., MDSC) and with other TPMs in other domains.

The Transport Path Manager (TPM) is a logical entity that can be part of Network Slice Selection Management Function (NSSMF) in the 3GPP management plane [TS.28.533-3GPP]. The TPM may use network configuration, policies, history, heuristics or some combination of these to derive traffic estimates that the TPM would use. How these estimates are derived and the precise 3GPP entity that hosts the TPM functionality are not in the scope of this document. The focus here is only in terms of how the TPM and SDN-C are programmed given that slice and QoS characteristics across a transport path can be represented by a Mobile Transport Network Context (MTNC) identifier.

TPM creates the MTNC identifier provisioned to control and user plane functions in the 3GPP domain. Once the MTNC identifier is created by the TPM, the TPM then requests the SDN-C in the transport network to provision paths in the transport domain based on the MTNC identifier. Federated orchestration and controller aspects in relation to TPM are discussed in Section 5. Detailed mechanisms for programming the MTNC identifier across 3GPP control and user plane should be part of the 3GPP specifications.

5. Federated Orchestration and Controller Functions

The TPM is a type of the CNC as depicted in Figure 1. The TPMs and the MDSC form a federated orchestration relationship to each other in order to collaborate network slice policy and implement the negotiated network slice policy to its domain network, respectively.

The SDN controllers of each domain are responsible to create per class domain paths/VNs meeting the MTNC requirements. Once per class domain paths/VNs are created using ACTN VN model, the SDN controller would need to program the domain ingress router/network switch to populate the routing instruction so that the data packets associated with the MTNC identifier would be routed to the pre-established paths/VNs for the MTNC identifier.

[ACTN-PM] discusses models that allow customers (e.g., TPM) to subscribe to and monitor their key performance data of their interest on the level of TE-tunnel or VN. The models also provide customers with the ability to program autonomic scaling intent mechanism on the level of TE-tunnel as well as VN. This model can be implemented as a way to support network automation by forming a close-loop relationship between controller entities (e.g., TPM – MDSC, TPM – SDN controller, etc.)

6. Network Programming Function Over Data Plane

There is a need to carry the MTNC identifier in data packets:

- Slices and QoS classes in the service domain do not have a 1:1 correspondence between the 3GPP domain and the transport domain. Some meta-data or token to associate information provisioned across 3GPP-transport domains needs to be carried in the data packets that need to get specific treatment in the transport domain.

- The MTNC identifier (which is meta-data) that is carried in the data packet header should be at the granularity of the provisioning for services between the 3GPP and transport domains. Specifically, the service is provided by the transport domain and the meta-data should be used in the transport domain to classify packets and provide the services agreed to.

- Protocol extensions to carry the above policy meta-data across connection segments between 3GPP functions (N3, N9) and also across 3GPP – to external system (N6, e.g., to application server)

In order to support the data plane programming with MTNC identifier, the TPM would need to propagate MTNC identifiers within the 3GPP control and user plane. These 3GPP control and user plane mechanisms should be standardized as part of 3GPP specifications.

Figure 2 shows that for N3, the data packets are “stamped” with the proper MTNC identifier by the gNBs via UDP header encapsulation mechanism as an illustration. As for N9 and N6, the UPFs would need to stamp the data packets with the same MTNC identifier for the next domain. For each domain, all the packets identified by the MTNC identifier will be routed to the pre-established paths/VNs to ensure the proper level of service performance for the traffic class associated with the MTNC identifier.

When the 3GPP user plane function (gNB, UPF) and transport provider edge are on different nodes, the edge router needs to have the means by which to classify the PDU packet. IP header fields such as DSCP (DiffServ Code Point) or the IPv6 Flow Label do not satisfy the requirement as they are not immutable. GTP-U [TS.29.281-3GPP] extension headers are not the best option either as the extension fields are chained and would potentially require significant processing by the transport edge router. Further, GTP-U extension fields carry 3GPP information between two 3GPP network functions and is not meant to carry information to be processed by the IP transport plane.

The provisioning mechanisms here expect that the MTNC identifier is carried in the IP packet header (PDU session data packet). This MTNC identifier is used to classify the PDU packet at the transport edge router. The MTNC identifier should be carried in some IP header field and should not be modified on path. Transport edge routers should only inspect the MTNC identifier for each packet and derive the class of transport service that should be provided (e.g., with MPLS or segment routes).

Different options for carrying the MTNC idenfifier in the IP data packet include SRv6 [I-D.ietf-spring-segment-routing] and GUE [I-D.ietf-intarea-gue-extensions]. The SRv6 is an underlay where the MTNC identifier can be encoded into Segment Routing Headers (SRH) that are then used to forward the PDU packet in the transport domain. The GUE headers, on the other hand, constitute an overlay mechanism where the MTNC identifier can also be encapsulated in the UDP extension header fields. A transport network like MPLS would inspect the MTNC header field in GUE and point to its already programmed label switched path. There are various trade-offs in terms of packet overhead, support in IPv4 and IPv6 networks as well as working across legacy and evolving transport networks that need to be considered. These considerations will be addressed in other future drafts.

7. Scalability Considerations

Since the MTNC-IDs represent QoS and slice of the service domain that is mapped to a transport domain slice for a path between to network functions (NF), there are multiple flows that get mapped to a single such transport slice. The number of transport slices to be provisioned scales well as it is related to the number of sites (N*(N-1)/2) *Q for N number of sites, Q classes of service). For example, if there are 25 sites and 3 classes of service, the number of paths provisioned will at most be 900, while the number of PDN connection flows handled over those connections can be well over a million. As the number of transport paths setup is a few orders lower than the number of connections/flows that are handled, these mechanisms scale extremely well compared to setting this up per PDN connection.

8. Security Considerations

From a security and reliability perspective, ACTN may encounter many risks such as malicious attack and rogue elements attempting to connect to various ACTN components. Furthermore, some ACTN components represent a single point of failure and threat vector and must also manage policy conflicts and eavesdropping of communication between different ACTN components.

All protocols used to realize the ACTN framework should have rich security features, and customer, application and network data should be stored in encrypted data stores. Additional security risks may still exist. Therefore, discussion and applicability of specific security functions and protocols will be better described in documents that are use case and environment specific.

The CMI will likely be an external protocol interface. Suitable authentication and authorization of each CNC connecting to the MDSC will be required; especially, as these are likely to be implemented by different organizations and on separate functional nodes. Use of the AAA-based mechanisms would also provide role-based authorization methods so that only authorized CNC's may access the different functions of the MDSC.

Where the MDSC must interact with multiple (distributed) PNCs, a PKI-based mechanism is suggested, such as building a TLS or HTTPS connection between the MDSC and PNCs, to ensure trust between the physical network layer control components and the MDSC. Trust anchors for the PKI can be configured to use a smaller (and potentially non-intersecting) set of trusted Certificate Authorities (CAs) than in the Web PKI. Which MDSC the PNC exports topology information to, and the level of detail (full or abstracted), should also be authenticated, and specific access restrictions and topology views should be configurable and/or policy based.

9. IANA Considerations

This document has no IANA actions.

10. Acknowledgements

The authors thank James Guichard for useful discussions and his suggestions for this work.

11. References

11.1. Normative References

[RFC8453] D. Ceccarelli and Y. Lee, “Framework for Abstraction and Control of Traffic Engineered Networks (ACTN)”, RFC 8453, August 2018.

[3GPP TS 28.531] 3rd Generation Partnership Project; Management and orchestration; Provisioning 3GPP TS 28.531.

[3GPP TS 23.501] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; System Architecture for the 5G System; Stage 2 3GPP TS 23.501.

[3GPP TS 23.502] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Procedures for the 5G System; Stage 2 3GPP TS 23.502.

11.2. Informative References

[Transport-Slicing] D. Ceccarelli and Y. Lee, “Transport aspects of network slicing: existing solutions and gaps”, IEEE Softwarization, January 2018.

[VN-Model] Y. Lee, et al, “A Yang Data Model for ACTN VN Operation”, draft-ietf-teas-actn-vn-yang, work in progress.

[IR.34-GSMA] GSM Association (GSMA), "Guidelines for IPX Provider Networks (Previously Inter-Service Provider IP Backbone Guidelines, Version 14.0", August 2018.

[ACTN-PM] Y. Lee, et al, “YANG models for VN & TE Performance Monitoring Telemetry and Scaling Intent Autonomics”, draft-ietf-teas-actn-pm-telemetry-autonomics, work in progress.

12. Contributors

Authors' Addresses

Y. Lee
Futurewei Technologies
Email: younglee.tx@gmail.com

John Kaippallimalil
Futurewei Technologies

Email: John.Kaippallimalil@futurewei.com