TEAS Working Group
Internet-Draft
Intended status: Informational
Expires: January 14, 2021

D. King
Old Dog Consulting
J. Drake
Juniper Networks
H. Zheng
Huawei Technologies

July 13, 2020

Applicability of Abstraction and Control of Traffic Engineered Networks (ACTN) to TE Network Slicing

draft-king-teas-applicability-actn-slicing-06

Abstract

Network abstraction is a technique that can be applied to a network domain that utilizes a set of policies to select network resources and obtain a view of potential connectivity across the network.

Network slicing is an approach to network operations that builds on the concept of network abstraction to provide programmability, flexibility, and modularity. It may use techniques such as Software Defined Networking (SDN) and Network Function Virtualization (NFV) to create multiple logical or virtual networks, each tailored for a set of services share the same set of requirements.

Abstraction and Control of Traffic Engineered Networks (ACTN) is described in RFC 8453. It defines an SDN-based architecture that relies on the concept of network and service abstraction to detach network and service control from the underlying data plane.

This document outlines the applicability of ACTN to transport network slicing in a Traffic Engineering (TE) network that utilizes IETF technology. It also identifies the features of network slicing not currently within the scope of ACTN, and indicates where ACTN might be extended.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The principles of network resource separation are not new. For years, separated overlay and logical (virtual) networking have existed, allowing multiple services to be deployed over a single physical network comprised of single or multiple layers. However, several key differences exist that differentiate overlay and virtual networking from network slicing.

A network slice is a virtual (that is, logical) network with its own network topology and a set of network resources that are used to provide connectivity that conforms to a specific Service Level Agreement (SLA) or Service Level Objective (SLO). The network resources used to realize a network slice belong to the network that is sliced. The resources may be assigned and dedicated to an individual slice, or they may be shared with other slices enabling different degrees of service guarantee and providing different levels of isolation between the traffic in each slice.

The term "Transport Network Slice" is used to describe a network slice that is used to support another network service by carrying traffic across one or more networks. A transport network slice could span multiple technologies (such as IP, MPLS, or optical) and multiple administrative domains.

The logical network that is a transport network slice may be kept separate from other concurrent logical networks each with independent control and management. Each can be created or modified on demand.

At one end of the spectrum, a virtual private wire or a virtual private network (VPN) may be used to build a network slice. In these cases, the network slices do not require the service provider to isolate network resources for the provision of the service - the service is "virtual".

At the other end of the spectrum there may be a detailed description of a complex service that will meet the needs of a set of applications with connectivity and service function requirements that may include compute resource, storage capability, and access to content. Such a service may be requested dynamically (that is, instantiated when an application needs it, and released when the application no longer needs it), and modified as the needs of the application change. This type of enhanced VPN is described in more detail in [I-D.ietf-teas-enhanced-vpn].

Abstraction and Control of TE Networks (ACTN) [RFC8453] is a framework that facilitates the abstraction of underlying network resources to higher-layer applications and that allows network operators to create virtual networks for their customers through the abstraction of the operators' network resources. ACTN is described further in Section 3.

This document outlines the application of ACTN and associated enabling technologies to provide transport network slicing in a network that utilizes IETF technologies such as IP, MPLS, or GMPLS. It describes how the ACTN functional components can be used to support model-driven partitioning of variable-sized bandwidth to facilitate network sharing and virtualization. Furthermore, the use of model-based interfaces to dynamically request the instantiation of virtual networks can be extended to encompass requesting and instantiation of specific service functions (which may be both physical or virtual), and to partition network resources such as compute resource, storage capability, and access to content.

Various efforts within the IETF are investigating the concept of network slicing (for example, [I-D.nsdt-teas-ns-framework]) and investigate the applicability of IETF protocols to the delivery of network slicing (for example, [I-D.ietf-teas-enhanced-vpn]). This document highlights how the ACTN approach might be extended to address the requirements of network slicing where the underlying network is TE-capable. It is not the intention that this work contradicts or competes with other IETF work.

1.1. Terminology

This document uses the following terminology. Many of these terms are in common usage in other work in the IETF and do not always have consistent meanings (see for example, [I-D.ietf-teas-enhanced-vpn] and [I-D.nsdt-teas-ns-framework]). The terms defined below are intended to give context and meaning for use in this document only and do not force wider applicability.

Service Provider: A server network or collection of server networks. The persons or organization responsible for operating such networks.

Consumer: Any application, client network, or customer of a service provider.

Service Functions (SFs): Components that provide specific functions within a network. SFs are often combined in a specific sequence called a service function chain to deliver services [RFC7665].

Resource: Any feature including connectivity, compute, storage, and content delivery that forms part of or can be accessed through a network. Resources may be shared between users, applications, and clients, or they may be dedicated for use by a unique consumer.

Infrastructure Resources: The hardware and software for hosting and connecting SFs. These resources may include computing hardware, storage capacity, network resources (e.g., links and switching/routing devices enabling network connectivity), and physical assets for radio access.

Service Level Agreement (SLA): An agreement between a consumer and network provider that describes the quality with which features and functions are to be delivered. It may include measures of bandwidth, latency, and jitter; the types of service (such as firewalls or billing) to be provided; the location, nature, and quantities of services (such as the amount and location of compute resources and the accelerators required).

Network Slice: An agreement between a consumer and a service provider to deliver network resources according to a specific service level agreement. A slice could span multiple technologies (e.g., radio, transport and cloud) and administrative domains.

Transport Network Slice: A network slice that is used to support another network service by carrying traffic across one or more networks. A transport network slice could span multiple transport technologies (such as IP, MPLS, or optical) and multiple administrative domains.

2. Requirements for Network Slicing

The concept of network slicing is a key capability to serve consumers with a wide variety of different service needs express in term of latency, reliability, capacity, and service function specific capabilities.

This section outlines the key capabilities required to realize network slicing in an IETF technology network. Consideration of slicing in other technology networks (such as radio access networks) is out of scope.

2.1. Resource Slicing

Network resources need to be allocated and dedicated for use by a specific network slice, or they may be shared among multiple slices. This allows a flexible approach that can deliver a range of services by partitioning (that is, slicing) the available network resources to present make them available to meet the consumer's SLA.

2.2. Service Isolation

A consumer may request, through their SLA, that the service deliver

to them is isolated from any other services delivered to any other consumers. That is, the SLA may request that changes to the other services do not have any negative impact on the delivery of the service.

Delivery of such service isolation may be achieved in the underlying network by various forms of resource partitioning ranging from dedicated allocation of resources for a specific slice, to sharing or resources with safeguards.

Although multiple network slices may utilize resources from a single underlying network, isolation should be understood in terms of:

- Performance isolation requires that service delivery on one network slice does not adversely impact congestion or performance levels of other slices.

- Security isolation means that attacks or faults occurring in one slice do not impact on other slices. Moreover, the security functions supporting each slice must operate independently so that an attack or misconfiguration of security in one slice will not prevent proper security function in the other slices.

- Management isolation means that each slice must be independently viewed, utilized and managed as a separate network. Furthermore, it should be possible to prevent the operator of one slice from being able to control, view, or detect any aspect of any other network slice.

2.3. Network Virtualization

Network virtualization enables the creation of multiple isolated virtual networks that are operationally decoupled from the underlying physical network, and are run on top of it. Slicing should enable the creation of virtual networks as consumer services.

2.4. Control and Orchestration

Orchestration combines and coordinates multiple control methods to provide a mechanism to operate one or more networks to deliver services. In a network slicing environment, an orchestrator is needed to coordinate disparate processes and resources for creating, managing, and deploying the end-to-end service. Two aspects of orchestration are required:

- Multi-domain Orchestration: Managing connectivity setup of the transport network slice across multiple administrative domains.

- End-to-end Orchestration: Combining resources for an end-to-end

service (e.g., transport connectivity with firewalling and guaranteed bandwidth with minimum delay).

3. Abstraction and Control of Traffic Engineered (TE) Networks (ACTN)

ACTN facilitates end-to-end connections and provides them to the user. The ACTN framework [RFC8453] introduces three functional components and two interfaces:

- Customer Network Controller (CNC)

- Multi-domain Service Coordinator (MDSC)

- Provisioning Network Controller (PNC)

- CNC-MDSC Interface (CMI)

- MDSC-PNC Interface (MPI)

RFC 8453 also highlights how:

- Abstraction of the underlying network resources is provided to higher-layer applications and consumers.

- Virtualization is achieved by selecting resources according to criteria derived from the details and requirements of the consumer, application, or service.

- Creation of a virtualized environment is performed to allow operators to view and control multi-domain networks as a single virtualized network.

- The presentation of networks to a consumer as a single virtual network via open and programmable interfaces.

The ACTN managed infrastructure consists of traffic engineered network resources, which may include:

- Statistical packet bandwidth.

- Physical forwarding plane sources, such as: wavelengths and time slots.

- Forwarding and cross-connect capabilities.

The ACTN network is "sliced" with consumers being given a different partial and abstracted topology view of the physical underlying

network.

3.1. ACTN Virtual Network as a Network Slice

To support multiple consumers, each with its own view of and control of the server network, a service provider needs to partition the server network resources to create slices assigned to each consumer.

An ACTN Virtual Network (VN) is a consumer view that is a slice of the ACTN-managed infrastructure. It is a network slice that is presented to the consumer by the ACTN provider as a set of abstracted resources. See [I-D.ietf-teas-actn-vn-yang] for detailed ACTN VN.

Depending on the agreement between consumer and provider various VN operations possible:

o Network Slice Creation: A VN could be pre-configured and created through static configuration or through dynamic request and negotiation between consumer and service provider. The VN must meet the network slice requirements specified in the SLA to satisfy the consumer's objectives.

o Network Slice Operations: The VN may be modified and deleted based on consumer requests. The consumer can further act upon the VN to manage traffic flows across the network slice.

o Network Slice View: The VN topology may be viewed from the consumer's perspective. This may be the entire VN topology or a collection of tunnels that are expressed as consumer end points, access links, intra domain paths and inter-domain links.

[RFC8454] describes a set of functional primitives that support these different ACTN VN operations.

3.2. Examples of ACTN Delivering Types of Network Slices

The examples that follow build on the ACTN framework to provide control, management, and orchestration for the network slice life-cycle. These network slices utilize common physical infrastructure, and meet specific requirements.

Three examples are shown. Each uses ACTN to achieve a different network slicing scenario. All three scenarios can be scaled up in capacity or be subject to topology changes as well as changes of consumer requirements.

3.2.1. ACTN Used for Virtual Private Line Model

In the example shown in Figure 1, ACTN provides virtual connections

between multiple consumer locations, requested by the requester of a Virtual Private Line (VPL) service (CNC-A). Benefits of this model include:

- Automated: the service set-up and operation is network provider managed.

- Virtual: the private line connectivity is provided from Site A to Site C (VPL1) and from Site B to Site C (VPL2) across the ACTN-managed physical network.

- Agile: on-demand when the consumer needs connectivity and fully adjustable bandwidth.

```
                     (Consumer VPL Request)
                                :
                             -------
                            | CNC-A |
      Boundary               -------
      Between  . . . . . . . . .:. . . . . . . . . . .
      Consumer &                :
      Network Provider       ------
                            | MDSC |
                             ------
                                :
                              -----
                             | PNC |
           Site A           ( ----- )           Site B
           ------          (         )          ------
          | vCE1 |========(  Physical )========| vCE2 |
           ------          ( Network )          ------
                 \          (_______)          /
                  \             ||            /
                   \            ||           /
              VPL 1 \           ||          / VPL 2
                     \          ||         /
                      \         ||        /
                       \      ------     /
                        -----| vCE3 |----
                              ------
                              Site C

      Key:   ... ACTN control connectivity
             === Physical connectivity
             --- Logical connectivity
```

Figure 1: Virtual Private Line Model

3.2.2. ACTN Used for VPN Delivery Model

In the example shown in Figure 2, ACTN provides VPN connectivity between two sites across three physical networks. The VPN requestor (CNC) is managed by the consumer expressed as users of the two VPN sites. The CNC interacts with the network provider's MDSC. Benefits of this model include:

- Provides edge-to-edge VPN multi-access connectivity.

- Most of the function is managed by the network provider, with some flexibility delegated to the consumer managed CNC.

```
                      --------------     --------------
                     | Site-A Users |   | Site-B Users |
                      --------------     --------------
                                 :         :
                                -------------
                               |     CNC     |
      Boundary                  -------------
      Between   . . . . . . . . . . . : . . . . . . . . . . .
      Consumer &                      :
      Network Provider                :
                      ---------------------------------
                     |               MDSC              |
                      ---------------------------------
                       :              :              :
                       :              :              :
                    -------        -------        -------
                   |  PNC  |      |  PNC  |      |  PNC  |
                    -------        -------        -------
                       :              :              :
                       :              :              :
        ______       -----          -----          -----       ______
       <      >     (     )        (     )        (     )     <      >
       <Site A>====( Phys. )======( Phys. )======( Phys. )====<Site B>
       <      >     ( Net )        ( Net )        ( Net )     <      >
       <      >      -----          -----          -----      <      >
       <      >-----------------------------------------------<      >
       <______>                                               <______>

      Key:   ... ACTN control connectivity
             === Physical connectivity
             --- Logical connectivity
```

Figure 2: VPN Model

3.2.3. ACTN Used to Deliver a Virtual Consumer Network

In this example (shown in Figure 3), ACTN provides a virtual network to the consumer. This virtual network is managed by the consumer. Benefits of this model include:

- The MDSC provides the topology as part of the consumer view so that the consumer can control their network slice to fit their needs.

- Service isolation can be provided through selection of physical networking resources.

- Applications can interact with their assigned network slices directly. The consumer may implement their own network control methods and traffic prioritization, manage their own addressing schemes, and further slice their virtual networks.

- The network slice may include nodes with specific capabilities. These are delivered as Physical Network Functions (PNFs) or Virtual Network Functions (VNFs).

```
                      -------------             (  Network  )
                     |    CNC      |----------->(  Slice 2  )
                      -------------           __(________   )
                   -------------             (          )__)
                  |    CNC      |----------->(  Network  ) ^
                   -------------             (  Slice 1  ) :
                        ^                    (___________) :
                        |                        ^    ^    :
      Boundary          |                        :    :    :
      Between    . . . .|. . . . . . . . . . . . : . .:. . : . . .
      Consumer &        |                        :    :    :
      Network Provider  |                        :    :    :
                        v                        :    :    :
                   -------------                 :    :....:
                  |    MDSC     |                :         :
                   -------------                 :         :
                        ^                  ------^--       :
                        |                 (         )      :
                        v                (  Physical )     :
                     -------              ( Network )      :
                    |  PNC  |<------------>(       )    ---^-----
                   -------  |               -------    (         )
                  |  PNC  |-                          (  Physical )
                  |       |<-------------------------->( Network )
                   -------                              (       )
```

```
                                                          -------
```

```
      Key: --- ACTN control connection
           ... Virtualization/abstraction through slicing
```

Figure 3: Network Slicing

3.2.4. Network Slice Service Mapping from TE to ACTN VN Models

The role of the TE-service mapping model [I-D.ietf-teas-te-service-mapping-yang] is to create a binding relationship across a Layer 3 Service Model (L3SM) [RFC8299], Layer 2 Service Model (L2SM) [RFC8466], and TE Tunnel model [I-D.ietf-teas-yang-te], via the generic ACTN Virtual Network (VN) model [I-D.ietf-teas-actn-vn-yang].

The ACTN VN model is a generic virtual network service model that allows consumers to specify a VN that meets the consumer's service objectives with various constraints on how the service is delivered.

The TE-service mapping model [I-D.ietf-teas-te-service-mapping-yang] is used to bind the L3SM with TE-specific parameters. This binding facilitates seamless service operation and enables visibility of the underlay TE network. The TE-service model developed in that document can also be extended to support other services including L2SM, and the Layer 1 Connectivity Service Model (L1CSM) [I-D.ietf-ccamp-l1csm-yang] L1CSM network service models.

Figure 4 shows the relationship between the models discussed above.

```
       --------------          --------------
      |    L3SM      |<=======|              |            ----------
       --------------  augment|              |..........>| ACTN VN  |
       --------------         |   Augmented  | reference  ----------
      |    L2SM      |<=======|   Service    |
       --------------  augment|   Model      |            ----------
       --------------         |              |..........>| TE-topo  |
      |    L1CSM     |<=======|              | reference  ----------
       --------------  augment|              |
       --------------         |              |            ----------
      | TE & Service |------->|              |..........>| TE-tunnel|
      | Mapping Types| import  --------------  reference  ----------
       --------------
```

Figure 4: TE-Service Mapping

3.3. ACTN VN Telemetry

The ACTN VN KPI telemetry model [I-D.ietf-teas-actn-pm-telemetry-autonomics] provides a way for a consumer to define performance monitoring relevant for its VN/network slice via the NETCONF subscription mechanisms [RFC8639], [RFC8640] or the equivalent mechanisms in RESTCONF [RFC8641], [RFC8650].

Key characteristics of [I-D.ietf-teas-actn-pm-telemetry-autonomics] include:

- An ability to provide scalable VN-level telemetry aggregation based on consumer subscription model for key performance parameters defined by the consumer.

- An ability to facilitate proactive re-optimization and reconfiguration of VNs/network slices based on network autonomic traffic engineering scaling configuration mechanism.

4 Transport Slice NBI Model

A network slice, or "transport network slice", resource model will be required or operation of ACTN-based network slicing. This model will be generated for instantiation, operation and monitoring, of network and function resource slices. The YANG model defined in [I-D.wd-teas-transport-slice-yang] provides a suitable basis for requesting, controlling and deleting, network slices.

5. IANA Considerations

This document makes no requests for action by IANA.

6. Security Considerations

Network slicing involves the control of network resources in order to meet the service requirements of consumers. In some deployment models, the consumer is able to directly request modification in the behaviour of resources owned and operated by a service provider. Such changes could significantly affect the service provider's ability to provide services to other consumers. Furthermore, the resources allocated for or consumed by a consumer will normally be billable by the service provider.

Therefore, it is crucial that the mechanisms used in any network slicing system allow for authentication of requests, security of those requests, and tracking of resource allocations.

It should also be noted that while the partitioning or slicing of

resources is virtual, the consumers 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 (whether under control of different or the same consumers) beyond the limits allowed within the SLA. Thus, slices are assumed to be private and to provide the appearance of genuine physical connectivity.

ACTN operates using the NETCONF [RFC6241] or RESTCONF [RFC8040] protocols and assumes the security characteristics of those protocols. Deployment models for ACTN should fully explore the authentication and other security aspects before networks start to carry live traffic.

7. Acknowledgements

Thanks to Qin Wu, Andy Jones, Ramon Casellas, and Gert Grammel for their insight and useful discussions about network slicing.

8. Contributors

The following people contributed text to this document.

Young Lee
Email: younglee.tx@gmail.com

Mohamed Boucadair
Email: mohamed.boucadair@orange.com

Sergio Belotti
Email: sergio.belotti@nokia.com

Daniele Ceccarelli
Email: daniele.ceccarelli@ericsson.com

Adrian Farrel
adrian@olddog.co.uk

9. Informative References

[I-D.ietf-ccamp-l1csm-yang]
Lee, Y., Lee, K., Zheng, H., Dhody, D., Dios, O., and D. Ceccarelli, "A YANG Data Model for L1 Connectivity Service Model (L1CSM)", draft-ietf-ccamp-l1csm-yang-11 (work in

progress), March 2020.

[I-D.ietf-teas-actn-pm-telemetry-autonomics]
Lee, Y., Dhody, D., Karunanithi, S., Vilata, R., King, D., and D. Ceccarelli, "YANG models for VN/TE Performance Monitoring Telemetry and Scaling Intent Autonomics", draft-ietf-teas-actn-pm-telemetry-autonomics-02 (work in progress), March 2020.

[I-D.ietf-teas-actn-vn-yang]
Lee, Y., Dhody, D., Ceccarelli, D., Bryskin, I., and B. Yoon, "A Yang Data Model for VN Operation", draft-ietf-teas-actn-vn-yang-08 (work in progress), March 2020.

[I-D.ietf-teas-enhanced-vpn]
Dong, J., Bryant, S., Li, Z., Miyasaka, T., and Y. Lee, "A Framework for Enhanced Virtual Private Networks (VPN+) Services", draft-ietf-teas-enhanced-vpn-05 (work in progress), February 2020.

[I-D.ietf-teas-te-service-mapping-yang]
Lee, Y., Dhody, D., Fioccola, G., WU, Q., Ceccarelli, D., and J. Tantsura, "Traffic Engineering (TE) and Service Mapping Yang Model", draft-ietf-teas-te-service-mapping-yang-03 (work in progress), March 2020.

[I-D.ietf-teas-yang-te]
Saad, T., Gandhi, R., Liu, X., Beeram, V., and I. Bryskin, "A YANG Data Model for Traffic Engineering Tunnels and Interfaces", draft-ietf-teas-yang-te-23 (work in progress), March 2020.

[I-D.nsdt-teas-ns-framework]
Gray, E. and J. Drake, "Framework for Transport Network Slices", draft-nsdt-teas-ns-framework-02 (work in progress), April 2020.

[I-D.wd-teas-transport-slice-yang]
Bo, W., Dhody, D., Han, L., and R. Rokui, "A Yang Data Model for Transport Slice NBI", draft-wd-teas-transport-slice-yang-02 (work in progress), July 2020.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <https://www.rfc-editor.org/info/rfc6241>.

[RFC7665] Halpern, J., Ed. and C. Pignataro, Ed., "Service Function Chaining (SFC) Architecture", RFC 7665,

DOI 10.17487/RFC7665, October 2015, <https://www.rfc-editor.org/info/rfc7665>.

[RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017, <https://www.rfc-editor.org/info/rfc8040>.

[RFC8299] Wu, Q., Ed., Litkowski, S., Tomotaki, L., and K. Ogaki, "YANG Data Model for L3VPN Service Delivery", RFC 8299, DOI 10.17487/RFC8299, January 2018, <https://www.rfc-editor.org/info/rfc8299>.

[RFC8453] Ceccarelli, D., Ed. and Y. Lee, Ed., "Framework for Abstraction and Control of TE Networks (ACTN)", RFC 8453, DOI 10.17487/RFC8453, August 2018, <https://www.rfc-editor.org/info/rfc8453>.

[RFC8454] Lee, Y., Belotti, S., Dhody, D., Ceccarelli, D., and B. Yoon, "Information Model for Abstraction and Control of TE Networks (ACTN)", RFC 8454, DOI 10.17487/RFC8454, September 2018, <https://www.rfc-editor.org/info/rfc8454>.

[RFC8466] Wen, B., Fioccola, G., Ed., Xie, C., and L. Jalil, "A YANG Data Model for Layer 2 Virtual Private Network (L2VPN) Service Delivery", RFC 8466, DOI 10.17487/RFC8466, October 2018, <https://www.rfc-editor.org/info/rfc8466>.

[RFC8639] Voit, E., Clemm, A., Gonzalez Prieto, A., Nilsen-Nygaard, E., and A. Tripathy, "Subscription to YANG Notifications", RFC 8639, DOI 10.17487/RFC8639, September 2019, <https://www.rfc-editor.org/info/rfc8639>.

[RFC8640] Voit, E., Clemm, A., Gonzalez Prieto, A., Nilsen-Nygaard, E., and A. Tripathy, "Dynamic Subscription to YANG Events and Datastores over NETCONF", RFC 8640, DOI 10.17487/RFC8640, September 2019, <https://www.rfc-editor.org/info/rfc8640>.

[RFC8641] Clemm, A. and E. Voit, "Subscription to YANG Notifications for Datastore Updates", RFC 8641, DOI 10.17487/RFC8641, September 2019, <https://www.rfc-editor.org/info/rfc8641>.

[RFC8650] Voit, E., Rahman, R., Nilsen-Nygaard, E., Clemm, A., and A. Bierman, "Dynamic Subscription to YANG Events and Datastores over RESTCONF", RFC 8650, DOI 10.17487/RFC8650, November 2019, <https://www.rfc-editor.org/info/rfc8650>.

Authors' Addresses

Daniel King
Old Dog Consulting

Email: daniel@olddog.co.uk

John Drake
Juniper Networks

Email: jdrake@juniper.net

Haomian Zheng
Huawei Technologies

Email: zhenghaomian@huawei.com