Network Working Group
Internet Draft

Intended status: Informational
Expires: December 2015

Young Lee
Huawei
Daniel King
Lancaster University
M. Boucadair
France Telecom
R. Jing
China Telecom
L. Contreras Murillo
Telefonica

September 29, 2014

Problem Statement for Abstraction and Control of Transport Networks

draft-leeking-actn-problem-statement-03.txt

Status of this Memo

Abstract

Previously transport networks were typically static, lacked flexibility, and required long planning times when deploying new services. Network Providers and Service Providers have embraced technologies that allow separation of data plane and control plane, distributed signaling for path setup and protection, and centralized path computation for service planning and traffic engineering. Although these technologies provide significant benefits, they do not meet the growing need for network programmability, automation, resource sharing, and service elasticity necessary for meeting operator's requirement for their virtual network operation.

Virtual network operation refers to the creation of a virtualized environment allowing operators to view the abstraction of the underlying multi-admin, multi-vendor, multi-technology networks and to operate, control and manage these multiple networks as if a single virtualized network. Another dimension of virtual network operation is associated with use of the common core transport network resource by multi-tenant service networks as a way of providing a virtualized infrastructure to flexibly offer new services and applications.

The work effort investigating this problem space is known as Abstraction and Control of Transport Networks (ACTN). This document provides an ACTN problem description, scope of work, and outlines the core requirements to facilitate virtual network operation.

Table of Contents

1. Introduction....4
1.1. Terminology....5
2. Relationship with Existing Technologies & Other Industry initiatives....7
2.1. Virtual Private Networks....7
2.2. Overlay Networks....8
2.3. Other Industry Initiatives....9
3. Motivations for Additional Functionality....9
3.1. Business Objectives....9
3.2. Network Resource Recursiveness....10
3.3. Customer-Initiated Programmability....11
3.4. Resource Partitioning....11
3.5. Service Orchestration....11
4. ACTN Objectives and Requirements....11
4.1. Capability and Resource Visibility....12
4.2. Network Programmability....13
4.3. Common Data Models....13
4.4. Scheduling....15
4.5. Allocation....15
4.6. Adaptability....15
4.7. Slicing....15
4.8. Isolation....16
4.9. Manageability....16
4.10. Resilience....17
4.11. Security....18
4.12. Policy....18
4.13. Technology Independence....18
4.14. Optimization....18
4.15. Multi-domain Support....19
4.16. Architecture Principles....19
4.16.1. Network Partitioning....19
4.16.2. Orchestration....19
4.16.3. Recursion....19
4.16.4. Legacy Support and Interoperability....20
4.17. Other Related Work....20
4.17.1. Requirements for Automated (Configuration) Management 20
4.17.2. Connectivity Provisioning Negotiation Protocol (CPNP) 20
5. References....21
5.1. Informative References....21
6. Acknowledgements....22
7. IANA Considerations....22
8. Authors' Addresses....22

1. Introduction

Customers continue to demand new services that are time scheduled, dynamic, and underpinned by a Pay As You Go billing model. These services are provided to customers by network operators and service providers and give rise to a variety of applications for office automation, data backup and retrieval, distributed computing, and high-quality media broadcasting. They offer Network and Service Providers new revenue generation opportunities, and these services typically have different traffic characteristics from established network services such as file hosting, web, and email. Deploying and operating these new applications and services using traditional network technologies and architectures limits network efficiency, scalability, and elasticity (i.e., capable of adapting to customer and application demands).

Network virtualization has been a significant innovation towards meeting customer demands, and enabling new applications and services. Separating network resources, and representing resources and topologies via abstracted concepts, facilitate effective sharing, or slicing, of physical infrastructure into virtual network service instances corresponding to multiple virtual network topologies that may be used by specific applications, services and users. Further development is required to allow customers to create, modify, and delete virtual network services dynamically.

Previously transport networks were typically static, lacked flexibility, and required long planning times when deploying new services. Network Providers and Service Providers have embraced technologies that allow separation of data plane and control plane, distributed signaling for path setup and protection, and centralized path computation for service planning and traffic engineering. Although these technologies provide significant benefits, they do not meet the growing need for network programmability, automation, resource sharing, and service elasticity necessary for meeting operator's requirement for their virtual network operation.

Virtual network operation refers to the creation of a virtualized environment allowing operators to view the abstraction of the underlying multi-admin, multi-vendor, multi-technology networks and to operate, control and manage these multiple networks as single virtualized network. Another dimension of virtual network operation is associated with use of the common core transport network resource

by multi-tenant service networks as a way of providing a virtualized infrastructure to flexibly offer new services and applications.

Abstraction and Control of Transport Networks (ACTN) defines new methods and capabilities for the deployment and operation of transport network resource. These are summarized as:

- Coordination and abstraction of underlying transport network resources to higher-layer applications and customers (note that higher-layer applications and customers could be internal users of the core transport network resource such as various service networks);
- Multi-domain virtual network operation that facilitates multi-admin, multi-vendor, multi-technology networks as a single virtualized network.
- Multi-tenant virtual network operation that consolidates different network services and applications to allow slicing of network resources to meet specific service, application and customer requirements;
- Provision of a computation scheme and virtual control capability, via a data model, to customers who request virtual network services (note that these customers could be service providers themselves);

This document provides an ACTN problem description and scope of work, and outlines the core requirements to facilitate virtual network operation.

1.1. Terminology

This document uses the terminology defined in [RFC4655], and [RFC5440]. Additional terms are defined below.

- Customers:

Customers are users of virtual network services. They are provided with an abstract resource view of the network resource (known as "a slice") to support their users and applications. In some cases, customers may have to support multiple virtual network services with different service objectives and QoS requirements to support multiple types of users and applications. Customers can be internal trusted parties with respect to the provider such as wholesale service department, etc. Customers can also be trusted external parties with respect to the provider.

- Service Providers (also Virtual Network Service Provider):

Service Providers are the providers of virtual network services to their customers. Service Providers typically lease resources from single or multiple Network Providers' facilities to create virtual network services and offer end-to-end services to their customers. A Virtual Network Service Provider is a type of Service Provider, except that they may own no physical equipment or infrastructure, or have limited physical infrastructure and will require virtual resources for offering the final service, and only provide services built upon virtual network infrastructure. In general, this document does not distinguish between a Virtual Network Service Provider and Service Provider.

- Network Providers:

Network Providers are the infrastructure providers that own the physical network resources and provide transport network resources to their customers. Service Providers can be the customers of Network Providers or can be the Network Providers themselves.

- Network Virtualization:

Network virtualization, refers to allowing the customers to Utilize a certain network resources as if they own them and thus allows them to control their allocated resources in a way most optimal with higher layer or application processes. This customer control facilitates the introduction of new applications (on top of available services) as the customers are given programmable interfaces to create, modify, and delete their virtual network

services.

o Transport Networks

Transport networks are defined as network infrastructure that provides connectivity and bandwidth for customer services. They are characterized by their ability to support server layer provisioning and traffic engineering for client layer services, such that resource guarantees may be provided to their customers. Transport networks in this document refer to a set of different type of connection-oriented networks, which include Connection-Oriented Circuit Switched (CO-CS) networks and Connection-Oriented Packet Switched (CO-PS) networks. This implies that at least the following transport networks are in scope: Layer 1 (L1) and Layer 0 (L0) optical networks (e.g., OTN, ODU, OCh/WSON), MPLS-TP, MPLS-TE, as well as other emerging network technologies with connection-oriented behavior.

2. Relationship with Existing Technologies & Other Industry initiatives

2.1. Virtual Private Networks

A Virtual Private Network (VPN) is a well-known concept [RFC4110], [RFC4664] and [RFC4847], and may be used to connect Multiple distributed sites via a variety of transport technologies, sometimes over shared network infrastructure.

Typically VPNs are managed and provisioned directly by the Network Provider or a VPN Service Provider. VPN systems may be Classified by:

- Protocol mechanisms used to tunnel the traffic;
- Tunnel termination point and/or location;
- Type of connectivity, site-to-site or remote-access;
- Quality of Service (QoS) capabilities;

- Level of security provided;

- Emulated service connectivity layer (layer 1, layer 2, layer 3);

Existing VPN solutions are largely technology specific and offer limited elasticity, although some technologies offer greater flexibility (i.e., layer 2 VPNs [RFC4664] and layer 3 VPNs [RFC4110]) when compared with layer 1 VPNs [RFC4847], all technologies are often deployed using pre-defined configurations. [RFC4847] describes virtual networks in terms of ITU-T Y.1312 and Y.1313. Those Recommendations address both the data plane and control plane aspects of VPNs. Concepts of private and shared VPNs are described.

The transport layer is achieved by utilizing a variety of technology-specific interfaces - e.g. Gigabit Ethernet (GE), Synchronous Digital Hierarchy (SDH), or Asynchronous Transfer Mode (ATM) for wireless back-hauling, or optical networks OTN and WSON).

VPNs offer a scalable tunnel solution for customer traffic; However, they are wholly dependent on the Service Provider to setup and manage the VPNs, lacking customer-initiated service programmability: creation, resizing, and deletion.

2.2. Overlay Networks

An overlay network [RFC4208] provides an enhanced network

virtualization technique, with the overlay network providing a topology comprised of virtual or logical links and nodes, which are built on top of physical nodes and links, providing a topology in which some of the links and nodes are virtual or logical and are built from multiple nodes or links in a server network.

Overlay networks are typically used in the multi-layer context,

In which the packet layer is a client to the server transport layer. The scope of network virtualization in overlay networks is somewhat limited. Customers and applications which need visibility or programmability, and the ability to resize or add resources, may find that overlay network technologies do meet their requirements.

2.3. Other Industry Initiatives

ONF SDN Architecture (https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR_SDN_ARCH_1.0_06062014.pdf) describes various arrangements of SDN controllers.

TM Forum's TR 215/TR225 addresses a common information model that can be applied to transport network in particular.

ITU-T Y.1312 and Y.1313 are a good reference to review for Layer 1 VPN in terms of terminology and architecture.

3. Motivations for Additional Functionality

3.1. Business Objectives

The traditional VPN and overlay network (ON) models are built on the premise that one single Network Provider provides all virtual private or overlay networks to its customers. This model is simple to operate but has some disadvantages in accommodating the increasing need for flexible and dynamic network virtualization capabilities.

A Network Provider may provide traditional end-to-end services And content (i.e., web and email) to its customers. Emerging services, applications and content are typically provided via Service Providers and Over the Top (OTT) (i.e., Video-on-demand, Social Media) providers. We can further categorize Service Providers as:

- A fixed or mobile Internet Service Providers (ISPs) which provide Internet connectivity and bandwidth to users;

- A service provider that leases network resources from one or more network providers to create virtual network services between ISPs and the core Internet.

- Data Center (DC)/content Network Provider and Service Providers who provide connectivity and bandwidth to content servers and application servers.

Network Providers and Service Providers of every type, all share The common business and revenue objectives:

- Minimize time to plan and deploy new services;

- Reduce the reliance on highly skilled personnel to operate their network;

- Reduce time to react to changing business demands and customer applications;

- Offer new, much more flexible services to their customers;

- Maximize network resource usage and efficiency.

All aforementioned objectives have the capability to significant increase revenue and reduce operational costs.

Network and Service Providers require capabilities that extend the current landscape of network virtualization capabilities and overall business objectives of the Network Provider, Service Provider, and ultimately the Customer and their Applications.

3.2. Network Resource Recursiveness

A newly emerged network virtualization environment is a Collection of heterogeneous network architectures from different players. VPNs and overlay networks are somewhat limited in addressing programmable interfaces for application or customer layers as well as for the service layer. The model must be extended to address a recursive nature of layer interactions in

network virtualization across transport networks, service networks, and customers/applications.

3.3. Customer-Initiated Programmability

Network-driven technologies such as VPNs and overlay networks provide customers with a set of pre-defined programmatic parameters to enable virtual networks. However, this model is limited to only allow programmable interfaces in which customers initiate and define virtual network services. This model must be extended to allow customer-initiated network programmability.

3.4. Resource Partitioning

The ability to slice and allocate transport resources for Service Providers would be beneficial. It would improve transport network resource efficiency and provide a method for the transport Network Provider to offer resource flexibility and control to Service Providers and users.

3.5. Service Orchestration

Another dimension is diversity on the customer side. Customers in this newly emerged network virtualization environment bring different dynamics than the traditional VPNs or Overlay Networks. There may be a multiple virtual slices that need to be created, managed and deleted, each interfacing to a number of Service Providers and Network Providers as the end-points of the clients span across multiple network domains. Thus, multiple components will require automated co-ordination and management, this is known as service orchestration and is therefore one of the key capabilities that should be provided.

4. ACTN Objectives and Requirements

The overall goal of enabling network abstraction and multiple concurrent virtual networks to coexist together on a shared physical infrastructure, comprised on multiple physical layers,

and may be subdivided into several smaller objectives. These are outlined below and are required in order to fulfill the design goals of ACTN.

The ACTN effort should utilize existing physical layer monitoring capabilities, algorithmic representation and modelling of physical layer resources to consider appropriate transport metrics and constraints. Moreover, the model may want to support dynamic collection of the statistics (i.e., status and availability) of the underlying transport network infrastructure.

4.1. Capability and Resource Visibility

It may be necessary for the application or Customer to obtain available capabilities and available network resources, for example, abstracted resource view and control. The visibility of the capabilities and the resources can be obtained either by resource discovery or by resource publishing. In the former case, the customer performs resource collection directly from the provider network by using discovery mechanisms to get total information about the available resources to be consumed. In the latter case, the network provider exposes available resources to potential customers (e.g., through a resource catalog) reducing the amount of detail of the underlying network.

Furthermore, capabilities and resources will also include:

- Peering Points (may be based on business SLAs or policies);
- Transport Topology (i.e., transport switching type, topology and connection points);
- Transport Capacity (i.e., current bandwidth and maximum bandwidth).
- Policy Management (i.e., what resources and capabilities are available, and what may be requested and by whom).
- Information about the provider (i.e., informative data about the resource owner)

- Geographical information respect to the resources to be consumed (i.e., geolocation of the resources for preventing legal concerns that could appear in the provision of some final services).

- Information about resource cost, consumption, etc. (i.e., energy efficiency per transmitted bit, monetary cost of the resource usage per time unit, etc.).

- Information about achievable resiliency (i.e., protection/restoration capabilities, recover time, etc.).

4.2. Network Programmability

A programmable interface should provide customers with the capabilities to dynamically create, deploy, and operate services in response to customer and application demands. To enable the on-demand services, the separation of control and forwarding is a fundamental requirement. Once this separation is achieved the network layer may be programmed irrespective of the underlying forwarding mechanism.

The creation of a programmable abstraction layer for physical network devices would provide information models which would allow operators to manipulate the network resources. By utilizing open programmable north-bound network interfaces, it would enable access to virtual control layer by customer interfaces and applications.

4.3. Common Data Models

The abstraction of the underlay transport, and resource Information representation model should describe each technology type within the ACTN framework; they will all follow a uniform structure, which is extensible to support any future technologies.

Such models will represent the physical resources as a set of attributes, characteristics and functionality, while adaptively capturing the true real-time and dynamic (real-time) properties of underlying physical resources.

For future discussion, abstraction and the technology agnostic virtualization requirements may benefit from being split into new sub-sections, suggested below:

Attributes

- Metrics
- Control Actions
- Semantics
- Administrative information (resource ownership)

Resources will be described with semantic methods so that the resource description models can be exposed in a uniformly structured manner to the upper layers.

Virtual infrastructure requests from ACTN customers will be translated into network parameters according to aforementioned network abstraction model. Utilizing this mechanism, a request is translated into topology and multi-dimensional nodes, interfaces and spectrum space with specific attributes such as bandwidth, QoS, and node capability.

Apart from facilitating the request of resources, these data models could be used for other tasks like network operation (e.g., the management of the abstracted transport infrastructure by the customer), configuration (e.g., the control of the resources), monitoring (e.g., the uniform view of different infrastructures in use), KPI customization (e.g., the particularization of the collected metrics according to the customer interests), etc.

4.4. Scheduling

When requesting network slices it should be possible to request an immediate or scheduled service.

To enable such on-demand consumption of resources, the Network Providers must employ appropriate scheduling algorithms in all of the network elements.

4.5. Allocation

When establishing a network slice, a customer may require specific guarantees for the virtual node and link attributes. This might include a request that guarantees minimum packet processing on a virtual node, and fixed loss and delay characteristics on the virtual links. This should be governed by Service Level Agreements (SLAs) and can have implications in the supportive transport technologies, and in the properties of the service to be offered to the customer (e.g., protected versus non-protected).

To provide such guarantees and to create an illusion of an Isolated and dedicated network slice to each customer, the Network Providers must employ appropriate scheduling algorithms in all of the network elements.

4.6. Adaptability

Adaptability of services would allow the Service Provider, user, and application to request modification of exist network resource that has been assigned. This may include resizing of bandwidth, modification of the topology, and adding/removing connectivity points.

4.7. Slicing

It should be possible for transport network infrastructure to be partitioned into multiple independent virtual networks known as "slicing", based on provider service types, customers and application requirements.

4.8. Isolation

Isolation, both of physical underlay infrastructure and of co-existing virtual networks, and ensure no leakage of traffic. Furthermore, there must be mechanisms that ensure that once network slices are assigned Customer and Application services are not competing for transport resources.

Each customer or application should be able to use arbitrary network topology, routing, or forwarding functions as well as customized control mechanisms independent of the underlying physical network and other coexisting virtual networks.

It must also be possible for many virtual networks to share the underlying infrastructure, without significantly impacting the performance of applications utilizing the virtual networks.

4.9. Manageability

A broad range of capabilities, including: request, control, provisioning, monitoring, resilience, adaptation and re-optimization of end-to-end services will need to be provided through a set of well-defined interfaces, specifically it should be possible to provide:

- Control of virtual network resources, capable of delivering end-to-end services optimisation of connectivity and virtual infrastructure based on client interface and application demands, technology constraints (bandwidth, latency, jitter, function, etc.) and commercial constraints (energy, customer SLA, etc.).

- Automation of virtual service and function requests and objectives, and providing on-demand and self-service network

slicing.

- Infrastructure elasticity to allow rapid provisioning, automatic scaling out, or in, of virtual resources.

- Virtual resource monitoring [Editor's Note: Control of bandwidth, energy consumption and quality of service/packet scheduling.]

[Editor's Note: The requirements on the technology driver from both sides need to be analysed, e.g. the information update frequency.]

4.10. Resilience

The resilience of the transport service provided to the customer will depend on the requirements expressed by the customer. Two different resilience scenarios may be considered: (i) the resilience as observed from the point of view of the customer; and (ii) the resilience as observed from the point of view of the provider.

The former case refers to the situation in which the customer request for specific resilience requirements on the offered transport service. For instance, the customer can request transport protection on the disjoint paths for connecting service end-points. This specific requirement forces the provider to explicitly assign transport resources to a customer.

However there are other situations in which the provider has to allocate resources for implicit resilience. For instance, the customer could request a service with certain QoS or availability for a single connection between service end-points according to an SLA. In that case, the provider could trigger recovery actions in the network, e.g. during a network outage, and according to the conditions of the SLA. These measures may not be perceived by the customer.

4.11. Security

Network programmability may introduce new security and misconfiguration vulnerabilities. These must be investigated and discussed, and then solved with suitable solutions. ACTN-based networks must be resilient to existing, and new, faults and attacks.

Failure or security breach in one ACTN slice should not impact another virtual network. It must also be possible for separation of untrusted services and applications, along with confidential services and applications that must be secured.

Some other aspects are relevant to security within the context of ACTN:

- Security aspects from the service point of view. For instance, encryption capabilities as part of the service capabilities that could be requested by the customer.
- Security aspects from the customer/provider relationship point of view. For instance aspects like authentication, authorization, logging, etc.

4.12. Policy

[To be discussed.]

4.13. Technology Independence

ACTN must support a variety of underlay transport technologies, providing the flexibility to manage a variety of heterogeneous network technologies.

4.14. Optimization

It should be guaranteed the capability of the service provider to

optimize the provided transport infrastructure without impacting the customer services. As the resources become consumed some fragmentation in the usage of the underlying infrastructure could occur. The provider then can be interested in optimizing the usage of its resources for several reasons (e.g., energy consumption, reutilization of vacant resources, etc.).

4.15. Multi-domain Support

A given customer could required to compose an end-to-end transport service by using network capabilities from different service providers that may be internal organizations or external entity. Reasons for that could be geographical coverage of the service (not fully served by a unique provider), resource availability (not enough resources from a given provider) or simply resiliency (provider diversity). ACTN should allow the multi domain approach for giving the customer the possibility of composing multi-provider transport services.

4.16. Architecture Principles

4.16.1. Network Partitioning

Coexistence of multiple network slices will need to be supported. It should also be possible for multiple network slices used by different customers to coexist together, spanning over part or full of the underlying physical networks.

4.16.2. Orchestration

ACTN should allow orchestration (automated co-ordination of functions) for managing and controlling virtual network services that may span multiple Service Providers and Network Providers.

4.16.3. Recursion

It should be possible for a network slice to be segmented to allow a slicing hierarchy with parent child relationships. Allowing a customer to become a virtual provider, this is known as recursion as well as nesting of network slices.

4.16.4. Legacy Support and Interoperability

Capability to deploy ACTN should be transparent to existing Physical network control and management mechanisms and protocols. Additionally, interoperability with non-ACTN based (i.e., conventional) networks should be guaranteed, thus allowing for the coexistence of both kinds of network solutions from the perspective of either the customer or the provider.

4.17. Other Related Work

4.17.1. Requirements for Automated (Configuration) Management

Given the ever-increasing complexity of the configuration tasks required for the dynamic provisioning of IP networks and services, [I-D.boucadair-network-automation-requirements] aims at listing the requirements to drive the specification of an automated configuration management framework, including the requirements for a protocol to convey configuration information towards the managed entities.

4.17.2. Connectivity Provisioning Negotiation Protocol (CPNP)

[I-D.boucadair-connectivity-provisioning-protocol] specifies the Connectivity Provisioning Negotiation Protocol (CPNP) which is used to facilitate the dynamic negotiation of service parameters between a Customer and a Provider. As such, CPNP is a generic protocol that can be used for various negotiation purposes that include (but are not necessarily limited to) connectivity provisioning services, storage facilities, CDN (Content Delivery Networks) footprint, etc.

The generic CPP template allows for:

- Automating the process of service negotiation and activation, thus accelerating service provisioning;

- Setting the (traffic) objectives of Traffic Engineering functions and service management functions.

- Enriching service and network management systems with 'decision-making' capabilities based on negotiated/offered CPPs.

5. References

5.1. Informative References

[RFC4208] Swallow, G., Drake, J., Ishimatsu, H., and Y. Rekhter, "Generalized Multiprotocol Label Switching (GMPLS) User-Network Interface (UNI): Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Support for the Overlay Model", RFC 4208, October 2005.

[RFC4110] R. Callon and M. Suzuki, "A Framework for Layer 3 Provider-Provisioned Virtual Private Networks (PPVPNs)", RFC 4110, July 2005.

[RFC4847] T. Takeda, Ed., "Framework and Requirements for Layer 1 Virtual Private Networks", RFC 4847, April 2007.

[RFC4655] Farrel, A., Vasseur, J., and J. Ash, "A Path Computation Element (PCE)-Based Architecture", RFC 4655, August 2006.

[RFC4664] L. Andersson, and E. Rosen, Eds., "Framework for Layer 2 Virtual Private Networks (L2VPNs)", RFC 4664, Sep 2006.

[RFC5440] JP. Vasseur, Ed. And JL. Le Roux, Ed. "Path Computation Element (PCE) Communication Protocol (PCEP)", RFC 5440,

March 2009.

[I-D.boucadair-connectivity-provisioning-protocol]
Boucadair, M. and C. Jacquenet, "Connectivity Provisioning Negotiation Protocol (CPNP)", draft-boucadair-connectivity-provisioning-protocol-01 (work in progress), October 2013.

[I-D.boucadair-network-automation-requirements]
Boucadair, M. and C. Jacquenet, "Requirements for Automated (Configuration) Management", draft-boucadair-network-automation-requirements-02 (work in progress), June 2013.

6. Acknowledgements

The authors wish to thank the contributions on the IETF ACTN mailing list.

7. IANA Considerations

Not Applicable.

8. Authors' Addresses

Young Lee
Huawei Technologies
5340 Legacy Drive
Plano, TX 75023, USA
Phone: (469)277-5838
Email: leeyoung@huawei.com

Daniel King
Lancaster University
Email: d.king@lancaster.ac.uk

Mohamed Boucadair
France Telecom

Rennes 35000
France
Email: mohamed.boucadair@orange.com

Ruiquan Jing,
China Telecom Corporation Limited,
No. 118, Xizhimenneidajie, Xicheng District, Beijing, China
Email: jingrq@ctbri.com.cn

Luis Miguel Contreras Murillo
Telefonica I+D
Email: lmcm@tid.es

Intellectual Property Statement

The IETF Trust takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in any IETF Document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights.

Copies of Intellectual Property disclosures made to the IETF Secretariat and any assurances of licenses to be made available, Or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement any standard or specification contained in an IETF Document. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

All IETF Documents and the information contained therein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION THEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgment

Funding for the RFC Editor function is currently provided by the

Internet Society.