

CCAMP Working Group  
Internet-Draft  
Intended status: Informational  
Expires: May 9, 2014

D. Ceccarelli  
Ericsson  
O. Gonzalez de Dios  
Telefonica I+D  
F. Zhang  
X. Zhang  
Huawei Technologies  
November 5, 2013

Use cases for operating networks in the overlay model context  
draft-ceccadedios-ccamp-overlay-use-cases-04

#### Abstract

This document defines a set of use cases for operating networks in the overlay model context through the Generalized Multiprotocol Label Switching (GMPLS) overlay interfaces.

#### Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 9, 2014.

#### Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	3
2. Terminology . . . . .	3
3. Client domain to server domain connectivity . . . . .	6
3.1. Single homing . . . . .	7
3.2. Adjacent dual homing . . . . .	7
3.3. Remote dual homing . . . . .	8
4. Use Cases . . . . .	9
4.1. UC 1 - Provisioning . . . . .	9
4.2. UC 2 - Provisioning with optimization . . . . .	9
4.3. UC 3 - Provisioning with constraints . . . . .	10
4.4. UC 4 - Diversity . . . . .	11
4.5. UC 5 - Concurrent provisioning . . . . .	12
4.6. UC 6 - Reoptimization . . . . .	13
4.7. UC 7 - Query . . . . .	13
4.8. UC 8 - Availability check . . . . .	13
4.9. UC 9 - P2MP services . . . . .	13
4.10. UC 10 - Privacy . . . . .	13
4.11. UC 12 - Stacking of overlay interfaces . . . . .	14
4.12. UC 13 - Resiliency parameters . . . . .	15
5. Security Considerations . . . . .	15
6. IANA Considerations . . . . .	15
7. Contributors . . . . .	15
Appendix A. Appendix I - Colored overlay . . . . .	16
8. References . . . . .	18
8.1. Normative References . . . . .	18
8.2. Informative References . . . . .	19
Authors' Addresses . . . . .	19

## 1. Introduction

The GMPLS overlay model [RFC 4208] specifies a client-server relationship between networks where client and server domains are managed as separate domains because of trustiness, scalability and operational issue. By means of procedures from the GMPLS protocol suite it is possible to build a topology in the client (overlay) network from Traffic Engineering paths in the server network. In this context, the UNI (User to Network Interface) is the demarcation point between networks. It is a boundary where policies, administrative and confidentiality issues apply that limit the exchange of information.

This GMPLS overlay model supports a wide variety of network scenarios. The packet over optical scenario is probably the most popular example where the overlay model applies.

In order to exploit the full potential of client/server network interworking in the overlay model, it may be desirable to know in advance whether is it feasible or not to connect two client network nodes [INTERCON-TE]. This requires having a certain amount of TE information of the server network in the client network. This need not be the full set of TE information available within each network, but does need to express the potential of providing TE connectivity. This subset of TE information is called TE reachability information.

The goal of this document is to define a set of solution independent use cases applicable to the overlay model. In particular it focuses on the network scenarios where the overlay model applies and analyzes the most interesting aspects of provisioning, recovery and path computation.

## 2. Terminology

The following terms are used within the document:

- Edge node [RFC4208]: node of the client domain belonging to the overlay network, i.e. nodes with at least one interface connected to the server domain.
- Core node [RFC4208]: node of the server domain.
- Access link: link between core node and edge node. It is the link where the UNI is usually implemented.
- Remote node: node in the client domain which has no direct access to the server domain but can reach it through an edge node



R3 (edge node) for starting the setup request procedure over the overlay interface (R3-A). Once the LSP in the server domain is setup and an adjacency in the packet domain between R3 and R5 is created, it can be advertised in the rest of the client domain and used by the signaling protocol (e.g. LDP) for setting up end-to-end (e.g. from R1 to R7) client domain LSPs.

On the other hand, the remote signaling consists on the utilization of a connection oriented signaling protocol in the client domain that allows issuing the end to end service setup trigger directly on the end nodes of the client domain. The signaling message, upon reaching the edge node (R3), will trigger the setup of the service in the server domain via the overlay interface.

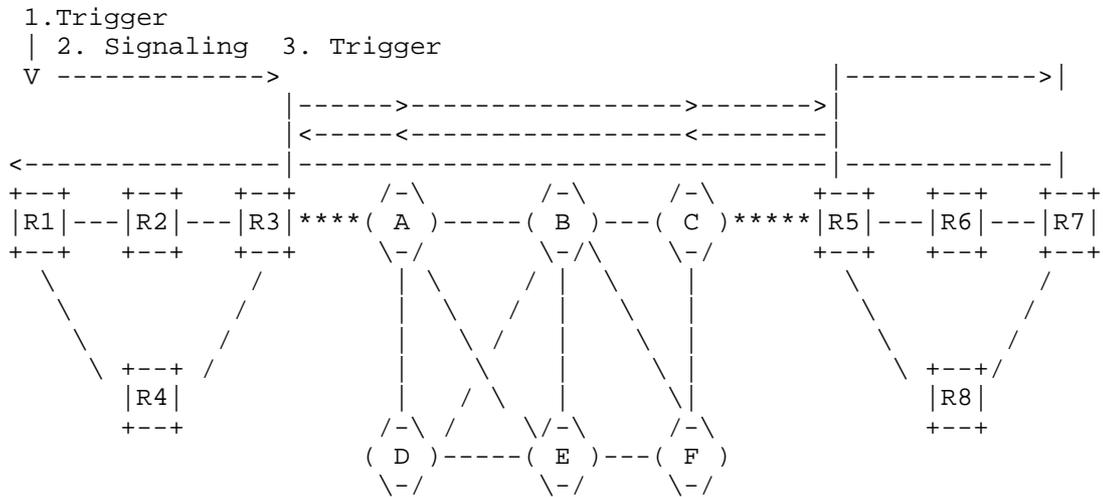


Figure 2: Remote Signaling

The utilization of the remote trigger allows for a strict control of the resources that will be used for the setup of the end to end service. In order to have a correct setup of the end to end service the trigger issued to R1 must include the overlay nodes to be used for the setup of the service in the server domain (R3 and R5). The network operator is supposed to know that the edge nodes to be used are R3 and R5.

The second bullet above speaks about administrative boundaries and administrative plus technological boundaries. Since the overlay is an administrative boundary between a client and a server domain, it is possible to configure it between a client and a server domain with

the same switching capabilities (e.g., IP over IP) or between domains with different switching capabilities (e.g., OTN over WDM). In the former case the boundary is referred to as administrative domain, while in the latter, it is referred to as both administrative and technological boundary.

In the case of boundary which is both administrative and technological a further distinction is needed and regards the node where the technological transition occurs, i.e., on the edge or on the core node.

One of the most common cases of administrative and technological boundary is the IP over WDM, where we speak about grey and colored overlay interfaces. In other words, in the case of grey interface the transponder and the domain transition are on the core node, while in the case of colored interface they are on the edge node. The physical impairments to be considered are different in the two cases (for further details please see Appendix A) but the behavior of the interface does not change and all use cases depicted below can be applied both to the grey and colored interfaces.

Generalizing what said above for the IP over WDM case, when the layer transition occurs on the edge node, the edge node is equipped with at least one interface with the switching capability of the client domain and one interface with the switching capability of the server domain. Viceversa, when layer transition occurs on the core node, it is the core node the one with at least two different interfaces with different switching capabilities.

Editor note: Actually path computation is assumed to be performed typically at the server domain. The client domain can request the server domain for computing a path or select among a set of paths computed by the server domain and exported to the client domain as virtual/abstract topology.

### 3. Client domain to server domain connectivity

A further distinction criterion, which is applicable to most of the use cases below, is the degree of connectivity between the client domain and the server domain. Three scenarios are identified:

- \* Single homing
- \* Dual homing
- \* Multiple single homing(editor note: better name is welcome)

3.1. Single homing

In the case of single homing we consider an end to end tunnel with a single LSP in the client domain and one or more LSPs in the server domain but a single overlay interface connecting them. The scenario is shown in figure below, where an end to end circuit between R1 and R7 is built over a tunnel between R3 and R5 composed by a single LSP restorable between A and C or more (possibly restorable) LSPs between A and C.

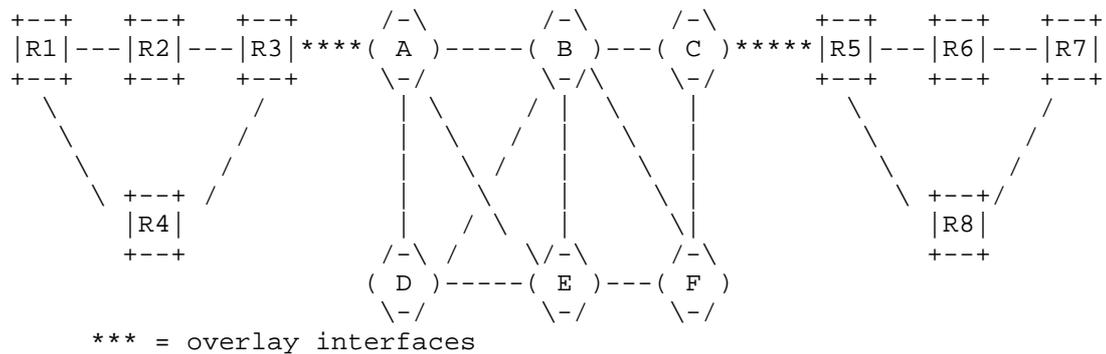


Figure 3: Single homing

Typical examples of single restorable LSP between A and C is the case of IP over WDM with single transponder on A and single transponder of C with restoration capability in the WDM domain. A common case of multiple LSPs between A and C, on the other side, is the splitting of the electrical signal between a couple of transponders on A creating a 1+1 protection terminated on a couple of transponders of C.

3.2. Adjacent dual homing

The term adjacent dual homing is used to indicate two (or more) access links between the edge node and one or more core nodes. In this case we have an end to end tunnel with a single LSP in the client domain and one or more LSPs in the server domain with two or more overlay interface connecting them. The scenario is shown in figure below, where an end to end circuit between R1 and R7 is built over a tunnel between R3 and R5 composed by two LSPs between different pairs of ingress/egress nodes (A-C and D-F).

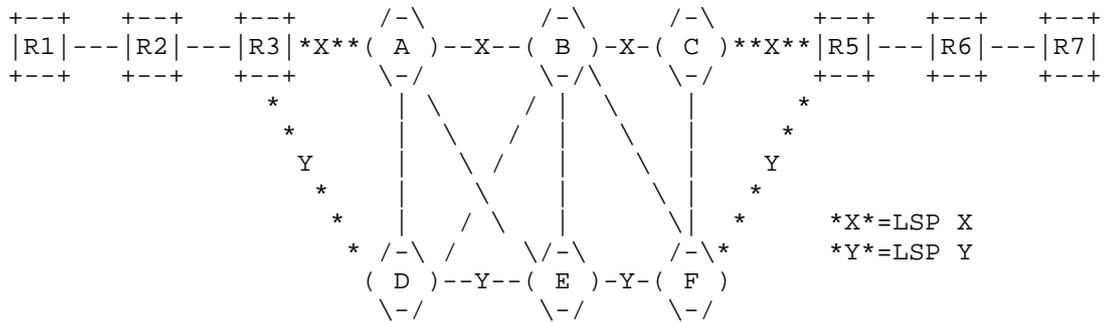


Figure 4: Adjacent dual homing

This network setup typically allows for fast client domain protection mechanisms, e.g., Fast ReRoute (FRR).

### 3.3. Remote dual homing

The remote dual homing scenario is based on an end to end tunnel with two (or more) LSPs in the client domain each of which relies on one (or more) LSPs in the server domain. This scenario is based on multiple independent single homing scenarios and is typically used to provide end to end diversity between two or more services. In figure below it is possible to see an end to end circuit between R1 and R7 composed by two services (A and B) which are built over two independent tunnels between R3 and R6 and between R5 and R9 respectively.

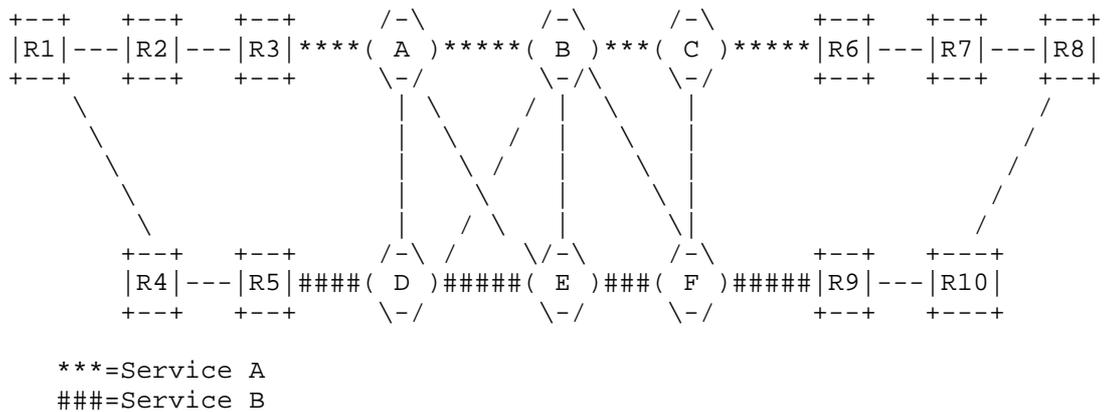


Figure 5: Remote dual homing







reasons. In such a case, supposing that such resources are known to the operator, it must be possible to indicate them as path computation constraint in the service setup request.

In addition to the provisioning of services with given diversity (and inclusion/exclusion) constraints, it must be possible to ask the server domain to at least keep such constraints also upon restoration or optimization procedures. It would be desirable to ask the server domain to relax constraints to be kept. The relaxation can be needed depending on resources availability, e.g., restoration of service X in partial diversity with service Y is total diversity is not possible).

4.5. UC 5 - Concurrent provisioning

Requirement: The network operator must be able to setup a plurality of services not necessarily between the same pair of edge nodes.

Here is another case particularly interesting from a protection point of view. In the case above the same edge node was asking for different services in the server domain, but in order to have end to end diversity (i.e. from R1 to R8 in figure below), there is the need to be able to provide disjoint services between different pairs of edge nodes.

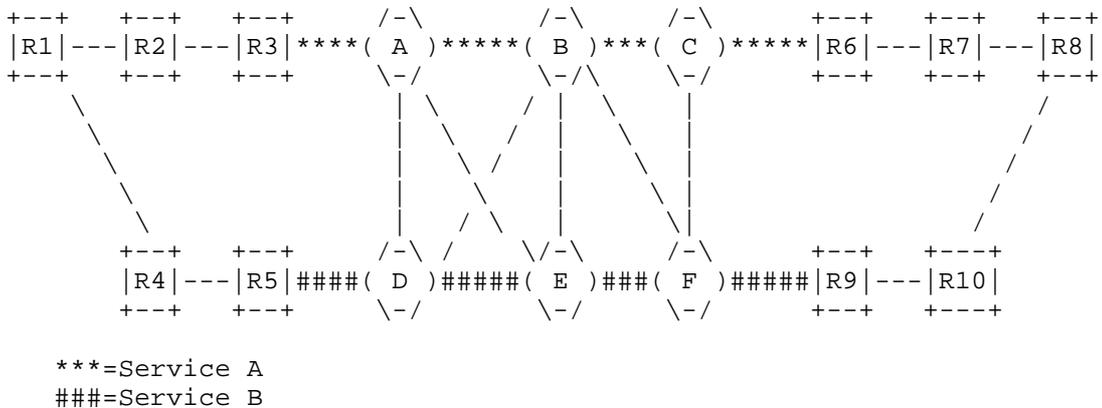


Figure 9: Concurrent provisioning

In this example Service A is provided between R3 and R6 and Service B between R5 and R9. Some sort of coordination is needed between R3 and R5 (directly between them or via R1) so that the requests to the server domain can be conveniently issued.

#### 4.6. UC 6 - Reoptimization

Requirement: The network operator must be able to setup a plurality of services so that the overall cost of the network is minimized and not the cost of a single service.

TBD

#### 4.7. UC 7 - Query

Requirement: The server network must be able to tell the network operator the actual parameters characterizing an existing service.

The capability of retrieving from the server domain some parameters qualifying a service can be extremely useful in different cases. One of them is the case of sequential provisioning with diversity requirements. In the case the operator wants to set-up a service in diversity from an existing one, hence it must be possible for the server domain to export some parameters univocally identifying the resources (e.g. SRLGs).

#### 4.8. UC 8 - Availability check

Requirement: The network operator must be able to check if in the server domain there are enough resources to setup a service with given parameters.

TBD

#### 4.9. UC 9 - P2MP services

Requirement: If allowed by the technology, the network operator must be able to setup a P2MP service with given parameters.

TBD

#### 4.10. UC 10 - Privacy

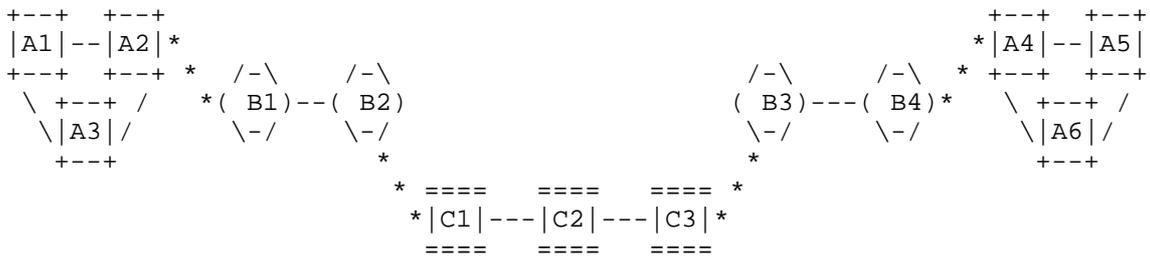
Requirement: The network operator must be able to provision different groups of users with independent addressing spaces.

This is a particularly useful functionality for those cases where the resources of the service provider are leased and shared among several other service providers or customers.

4.11. UC 12 - Stacking of overlay interfaces

Requirement: The network operator must be able manage a network with an arbitrarily high number of administrative boundaries (i.e., >2).

Operators might want to split their overlay networks in a number of administrative domains for several reasons, among which simplifying network operations and improving scalability. In order to do so it must be possible to create a stack of overlay interfaces between the different domains as shown in figure below:



\*\*\* = overlay interfaces

Figure 10: Stacking of interfaces

Nodes "Ax" belong to a domain which is client to the domain composed by nodes "Bx". The domain composed by nodes Bx is hence server domain to the "Ax" nodes domain but client to the "Cx" nodes domain.

A pretty common deployment of this scenario consists of IP over OTN over WDM layers, where the OTN digital layer is used for the grooming of IP traffic over high bit rate lambdas. In figure 8, Node Bx can be assumed to be digital layer, which is interfacing with packet layer nodes (Ax) across overlay interface. Digital layer nodes Bx are interfacing with DWDM layer nodes Cx. If OTN (Bx) and DWDM (Cx) node belong to same IGP, then this becomes multi-layer path computation and signaling case, and it is out of scope of this document.

However, as already shown in the intro of this memo, the three different domains of the example could have the same switching capability (e.g., IP) and be kept separate just for administrative reasons.

#### 4.12. UC 13 - Resiliency parameters

Requirement: The network operator must be able to request an LSP in the server domain with resilience parameters. The minimum set of such parameters includes 1+1 protection and restoration. Moreover, it must be possible for the operator to change the resilience level after the path is established in the network.

This functionality is interesting in a scenario like the one in Figure 6 with two concurrent paths. Let us assume service A and B are requested without any resilience requirements. If there is a failure in service A, the operator can request for protection in service B once this situation is detected.

These parameters can be used both in the case of single homing (UC1) and concurrent paths (UC6). The aim of this section is to highlight two sub-cases for every resilience case:

(1) during the provisioning the client domain can request to the server domain for resilience parameters.

(2) Once a failure occurs, the client domain has to be notified via the overlay interface thus carrying information about the situation in the server domain, so the client domain can take its own decisions.

For the different sub-use cases, the provisioning use case already highlights which is the workflow and the requirements for each scenario. This section does not include an example for each of them.

#### 5. Security Considerations

TBD

#### 6. IANA Considerations

TBD

#### 7. Contributors

Diego Caviglia, Ericsson

Via E.Melen, 77 - Genova - Italy

Email: [diego.caviglia@ericsson.com](mailto:diego.caviglia@ericsson.com)

Jeff Tantsura, Ericsson

300 Holger Way, San Jose, CA 95134 - USA

Email: [jeff.tantsura@ericsson.com](mailto:jeff.tantsura@ericsson.com)

Khuzema Pithewan, Infinera Corporation

140 Caspian CT., Sunnyvale - CA - USA

Email: [kpithewan@infinera.com](mailto:kpithewan@infinera.com)

Cyril Margaria, Wandl

Email: [cyril.margaria@googlemail.com](mailto:cyril.margaria@googlemail.com)

John Drake, Juniper

Email: [jdrake@juniper.net](mailto:jdrake@juniper.net)

Sergio Belotti, Alcatel-Lucent

Email: [sergio.belotti@alcatel-lucent.com](mailto:sergio.belotti@alcatel-lucent.com)

Victor Lopez, Telefonica I+D

Email: [vlopez@tid.es](mailto:vlopez@tid.es)

#### Appendix A. Appendix I - Colored overlay

This use case applies to networks where the server domain is a WDM network. In those cases it is possible to either have a grey interface between client and server domains (i.e. transponder on the

border core node) or a colored interface between them (i.e. transponder on the edge node).

All the previous use cases assume the case of grey interface, but there are particular network scenarios in which it is possible to move the transponders from the core to the edge nodes and hence save on hardware cost.

The issue with this solution is that the PCE in the server domain, being either centralized or distributed, has only visibility of what is inside the server domain and hence has not all the info needed to perform the validation of a path. The edge node must provide the PCE in the server domain with a set of info needed for a correct path computation and path validation from transponder to transponder (i.e. between edge nodes) all along the server domain.

The type of information needed for this scenario can be classified into three categories:

- Feasibility: Parameters like the output power of the transponder are needed in order to state e.g. the amount of km that can be reached without regeneration.
- Compatibility: The egress transponder must be compatible with the ingress one. Parameters that influence the level of compatibility can be for example the type of FEC (Forward Error Correction) used or the modulation format (which also impacts the feasibility together with the bit rate).
- Availability: Transponders can be tunable within a range of lambdas or even locked to a single lambda. This impacts the path computation as not every path in the network might have such lambda(s) supported or available at the time the path computation is performed.

In figure below it is possible to see that the PCE is aware of all the info between A and C (i.e. within the server domain scope) but what is missing is info related to the transponders on R1 and on R2 and of the access links. (i.e. R1-A and C-R2).



## 8.2. Informative References

### Authors' Addresses

Daniele Ceccarelli  
Ericsson  
Via E. Melen 77  
Genova - Erzelli  
Italy

Email: [daniele.ceccarelli@ericsson.com](mailto:daniele.ceccarelli@ericsson.com)

Oscar Gonzalez de Dios  
Telefonica I+D  
Don Ramon de la Cruz 82-84  
Madrid 28045  
Spain

Email: [ogondio@tid.es](mailto:ogondio@tid.es)

Fatai Zhang  
Huawei Technologies  
F3-5-B R&D Center, Huawei Base  
Shenzhen 518129 P.R.China Bantian, Longgang District  
Phone: +86-755-28972912

Email: [zhangfatai@huawei.com](mailto:zhangfatai@huawei.com)

Xian Zhang  
Huawei Technologies  
F3-5-B R&D Center, Huawei Base  
Shenzhen 518129 P.R.China Bantian, Longgang District  
Phone: +86-755-28972913

Email: [zhang.xian@huawei.com](mailto:zhang.xian@huawei.com)

