Internet Engineering Task Force (IETF)
Request for Comments: 6965
Category: Informational
ISSN: 2070-1721

L. Fang, Ed.
Cisco
N. Bitar
Verizon
R. Zhang
Alcatel-Lucent
M. Daikoku
KDDI
P. Pan
Infinera

August 2013

MPLS Transport Profile (MPLS-TP) Applicability: Use Cases and Design

Abstract

This document describes the applicability of the MPLS Transport Profile (MPLS-TP) with use case studies and network design considerations. The use cases include Metro Ethernet access and aggregation transport, mobile backhaul, and packet optical transport.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6965.

Table of Contents

1. Introduction

This document describes the applicability of the MPLS Transport Profile (MPLS-TP) with use case studies and network design considerations.

1.1. Terminology

Term	Definition
2G	2nd generation of mobile telecommunications technology
3G	3rd generation of mobile telecommunications technology
4G	4th generation of mobile telecommunications technology
ADSL	Asymmetric Digital Subscriber Line
AIS	Alarm Indication Signal
ATM	Asynchronous Transfer Mode
BFD	Bidirectional Forwarding Detection
BTS	Base Transceiver Station
CC-V	Continuity Check and Connectivity Verification
CDMA	Code Division Multiple Access
E-LINE	Ethernet line; provides point-to-point connectivity
E-LAN	Ethernet LAN; provides multipoint connectivity
eNB	Evolved Node B
EPC	Evolved Packet Core
E-VLAN	Ethernet Virtual Private LAN
EVDO	Evolution-Data Optimized
G-ACh	Generic Associated Channel
GAL	G-ACh Label
GMPLS	Generalized Multiprotocol Label Switching
GSM	Global System for Mobile Communications
HSPA	High Speed Packet Access
IPTV	Internet Protocol television
L2VPN	Layer 2 Virtual Private Network
L3VPN	Layer 3 Virtual Private Network
LAN	Local Access Network
LDI	Link Down Indication
LDP	Label Distribution Protocol
LSP	Label Switched Path
LTE	Long Term Evolution
MEP	Maintenance Entity Group End Point
MIP	Maintenance Entity Group Intermediate Point
MPLS	Multiprotocol Label Switching
MPLS-TP	MPLS Transport Profile
MS-PW	Multi-Segment Pseudowire
NMS	Network Management System
OAM	Operations, Administration, and Maintenance
PE	Provider-Edge device
PW	Pseudowire

RAN	Radio Access Network
RDI	Remote Defect Indication
S-PE	PW Switching Provider Edge
S1	LTE Standardized interface between eNB and EPC
SDH	Synchronous Digital Hierarchy
SONET	Synchronous Optical Network
SP	Service Provider
SRLG	Shared Risk Link Groups
SS-PW	Single-Segment Pseudowire
TDM	Time-Division Multiplexing
TFS	Time and Frequency Synchronization
tLDP	Targeted Label Distribution Protocol
UMTS	Universal Mobile Telecommunications System
VPN	Virtual Private Network
X2	LTE Standardized interface between eNBs for handover

1.2. Background

Traditional transport technologies include SONET/SDH, TDM, and ATM. There is a transition away from these transport technologies to new packet transport technologies. In addition to the increasing demand for bandwidth, packet transport technologies offer the following key advantages:

Bandwidth efficiency:

Traditional TDM transport technologies support fixed bandwidth with no statistical multiplexing. The bandwidth is reserved in the transport network, regardless of whether or not it is used by the client. In contrast, packet technologies support statistical multiplexing. This is the most important motivation for the transition from traditional transport technologies to packet transport technologies. The proliferation of new distributed applications that communicate with servers over the network in a bursty fashion has been driving the adoption of packet transport techniques, since packet multiplexing of traffic from bursty sources provides more efficient use of bandwidth than traditional circuit-based TDM technologies.

Flexible data rate connections:

The granularity of data rate connections of traditional transport technologies is limited to the rigid Plesiochronous Digital Hierarchy (PDH) hierarchy (e.g., DS1, DS3) or SONET hierarchy (e.g., OC3, OC12). Packet technologies support flexible data rate connections. The support of finer data rate granularity is particularly important for today’s wireline and wireless services and applications.

QoS support:

Traditional transport technologies (such as TDM) provide bandwidth guarantees, but they are unaware of the types of traffic they carry. They are not packet aware and do not provide packet-level services. Packet transport can provide the differentiated services capability needed to support oversubscription and to deal with traffic prioritization upon congestion: issues that arise only in packet networks.

The root cause for transport moving to packet transport is the shift of applications from TDM to packet -- for example, Voice TDM to VoIP, Video to Video over IP, TDM access lines to Ethernet, and TDM VPNs to IP VPNs and Ethernet VPNs. In addition, network convergence and technology refreshes contribute to the demand for a common and flexible infrastructure that provides multiple services.

As part of the MPLS family, MPLS-TP complements existing IP/MPLS technologies; it closes the gaps in the traditional access and aggregation transport to enable end-to-end packet technology solutions in a cost efficient, reliable, and interoperable manner. After several years of industry debate on which packet technology to use, MPLS-TP has emerged as the next generation transport technology of choice for many Service Providers worldwide.

The Unified MPLS strategy -- using MPLS from core to aggregation and access (e.g., IP/MPLS in the core, IP/MPLS or MPLS-TP in aggregation and access) -- appears to be very attractive to many SPs. It streamlines the operation, reduces the overall complexity, and improves end-to-end convergence. It leverages the MPLS experience and enhances the ability to support revenue-generating services.

MPLS-TP is a subset of MPLS functions that meet the packet transport requirements defined in [RFC5654]. This subset includes: MPLS data forwarding, pseudowire encapsulation for circuit emulation, and dynamic control plane using GMPLS control for LSP and tLDP for pseudowire (PW). MPLS-TP also extends previous MPLS OAM functions, such as the BFD extension for proactive Connectivity Check and Connectivity Verification (CC-V) [RFC6428], Remote Defect Indication (RDI) [RFC6428], and LSP Ping Extension for on-demand CC-V [RFC6426]. New tools have been defined for alarm suppression with Alarm Indication Signal (AIS) [RFC6427] and switch-over triggering with Link Down Indication (LDI) [RFC6427]. Note that since the MPLS OAM feature extensions defined through the process of MPLS-TP development are part of the MPLS family, the applicability is general to MPLS and not limited to MPLS-TP.

The requirements of MPLS-TP are provided in the MPLS-TP requirements document [RFC5654], and the architectural framework is defined in the MPLS-TP framework document [RFC5921]. This document's intent is to provide the use case studies and design considerations from a practical point of view based on Service Providers' deployments plans as well as actual deployments.

The most common use cases for MPLS-TP include Metro access and aggregation, mobile backhaul, and packet optical transport. MPLS-TP data-plane architecture, path protection mechanisms, and OAM functionality are used to support these deployment scenarios.

The design considerations discussed in this document include the role of MPLS-TP in the network, provisioning options, standards compliance, end-to-end forwarding and OAM consistency, compatibility with existing IP/MPLS networks, and optimization vs. simplicity design trade-offs.

2. MPLS-TP Use Cases

2.1. Metro Access and Aggregation

The use of MPLS-TP for Metro access and aggregation transport is the most common deployment scenario observed in the field.

Some operators are building green-field access and aggregation transport infrastructure, while others are upgrading or replacing their existing transport infrastructure with new packet technologies. The existing legacy access and aggregation networks are usually based on TDM or ATM technologies. Some operators are replacing these networks with MPLS-TP technologies, since legacy ATM/TDM aggregation and access are becoming inadequate to support the rapid business growth and too expensive to maintain. In addition, in many cases the legacy devices are facing End of Sale and End of Life issues. As operators must move forward with the next-generation packet technology, the adoption of MPLS-TP in access and aggregation becomes a natural choice. The statistical multiplexing in MPLS-TP helps to achieve higher efficiency compared with the time-division scheme in the legacy technologies. MPLS-TP OAM tools and protection mechanisms help to maintain high reliability of transport networks and achieve fast recovery.

As most Service Providers' core networks are MPLS enabled, extending the MPLS technology to the aggregation and access transport networks with a Unified MPLS strategy is very attractive to many Service Providers. Unified MPLS strategy in this document means having end-to-end MPLS technologies through core, aggregation, and access. It reduces operating expenses by streamlining the operation and

leveraging the operational experience already gained with MPLS technologies; it also improves network efficiency and reduces end-to-end convergence time.

The requirements from the SPs for ATM/TDM aggregation replacement often include:

- maintaining the previous operational model, which means providing a similar user experience in NMS,

- supporting the existing access network (e.g., Ethernet, ADSL, ATM, TDM, etc.) and connections with the core networks, and

- supporting the same operational capabilities and services (L3VPN, L2VPN, E-LINE/E-LAN/E-VLAN, Dedicated Line, etc.).

MPLS-TP can meet these requirements and, in general, the requirements defined in [RFC5654] to support a smooth transition.

2.2. Packet Optical Transport

Many SPs' transport networks consist of both packet and optical portions. The transport operators are typically sensitive to network deployment cost and operational simplicity. MPLS-TP supports both static provisioning through NMS and dynamic provisioning via the GMPLS control plane. As such, it is viewed as a natural fit in transport networks where the operators can utilize the MPLS-TP LSPs (including the ones statically provisioned) to manage user traffic as "circuits" in both packet and optical networks. Also, when the operators are ready, they can migrate the network to use the dynamic control plane for greater efficiency.

Among other attributes, bandwidth management, protection/recovery, and OAM are critical in packet/optical transport networks. In the context of MPLS-TP, LSPs may be associated with bandwidth allocation policies. OAM is to be performed on each individual LSP. For some of the performance monitoring functions, the OAM mechanisms need to be able to transmit and process OAM packets at very high frequency. An overview of the MPLS-TP OAM toolset is found in [RFC6669].

Protection, as defined in [RFC6372], is another important element in transport networks. Typically, ring and linear protection can be readily applied in metro networks. However, as long-haul networks are sensitive to bandwidth cost and tend to have mesh-like topology, shared mesh protection is becoming increasingly important.

In some cases, SPs plan to deploy MPLS-TP from their long-haul optical packet transport all the way to the aggregation and access in their networks.

2.3. Mobile Backhaul

Wireless communication is one of the fastest growing areas in communication worldwide. In some regions, the tremendous mobile growth is fueled by the lack of existing landline and cable infrastructure. In other regions, the introduction of smart phones is quickly driving mobile data traffic to become the primary mobile bandwidth consumer (some SPs have already observed that more than 85% of total mobile traffic is data traffic). MPLS-TP is viewed as a suitable technology for mobile backhaul.

2.3.1. 2G and 3G Mobile Backhaul

MPLS-TP is commonly viewed as a very good fit for 2G/3G mobile backhaul. 2G (GSM/CDMA) and 3G (UMTS/HSPA/1xEVDO) mobile backhaul networks are still currently dominating the mobile infrastructure.

The connectivity for 2G/3G networks is point to point (P2P). The logical connections have a hub-and-spoke configuration. Networks are physically constructed using a star or ring topology. In the Radio Access Network (RAN), each mobile Base Transceiver Station (BTS/Node B) is communicating with a Base Station Controller (BSC) or Radio Network Controller (RNC). These connections are often statically set up.

Hierarchical or centralized architectures are often used for pre-aggregation and aggregation layers. Each aggregation network interconnects with multiple access networks. For example, a single aggregation ring could aggregate traffic for 10 access rings with a total of 100 base stations.

The technology used today is largely ATM based. Mobile providers are replacing the ATM RAN infrastructure with newer packet technologies. IP RAN networks with IP/MPLS technologies are deployed today by many SPs with great success. MPLS-TP is another suitable choice for Mobile RAN. The P2P connections from base station to Radio Controller can be set statically to mimic the operation of today’s RAN environments; in-band OAM and deterministic path protection can support fast failure detection and switch-over to satisfy service level agreements (SLAs). Bidirectional LSPs may help to simplify the provisioning process. The deterministic nature of MPLS-TP LSP setup can also support packet-based synchronization to maintain predictable performance regarding packet delay and jitter. The traffic-engineered and co-routed bidirectional properties of an MPLS-TP LSP

are of benefit in transporting packet-based Time and Frequency Synchronization (TFS) protocols, such as [TICTOC]. However, the choice between an external, physical-layer method or a packet-based TFS method is network dependent and thus is out of scope of this document.

2.3.2. 4G/LTE Mobile Backhaul

One key difference between LTE and 2G/3G mobile networks is that the logical connection in LTE is a mesh, while in 2G/3G it is a P2P star. In LTE, each base station (eNB/BTS) communicates with multiple network controllers (e.g., Packet Data Network Gateway, Packet Data Network Serving Gateway, Access Service Network Gateway), and the radio elements communicate with one another for signal exchange and traffic offload to wireless or wireline infrastructures.

IP/MPLS has a great advantage in any-to-any connectivity environments. Thus, the use of mature IP or L3VPN technologies is particularly common in the design of an SP’s LTE deployment plans.

The extended OAM functions defined in MPLS-TP, such as in-band OAM and path protection mechanisms, bring additional advantages to support SLAs. The dynamic control plane with GMPLS signaling is especially suited for the mesh environment, to support dynamic topology changes and network optimization.

Some operators are using the same model as in 2G and 3G mobile backhaul, which uses IP/MPLS in the core and MPLS-TP with static provisioning (through NMS) in aggregation and access. The reasoning is as follows: currently, the X2 traffic load in LTE networks may be a very small percentage of the total traffic. For example, one large mobile operator observed that X2 traffic was less than one percent of the total S1 traffic. Therefore, optimizing the X2 traffic may not be the design objective in this case. The X2 traffic can be carried through the same static tunnels together with the S1 traffic in the aggregation and access networks and further forwarded across the IP/MPLS core. In addition, mesh protection may be more efficient with regard to bandwidth utilization, but linear protection and ring protection are often considered simpler by some operators from the point of view of operation maintenance and troubleshooting, and so are widely deployed. In general, using MPLS-TP with static provisioning for LTE backhaul is a viable option. The design objective of using this approach is to keep the operation simple and use a common model for mobile backhaul, especially during the transition period.

The TFS considerations stated in Section 2.3.1 apply to the 4G/LTE mobile backhaul case as well.

3. Network Design Considerations

3.1. The Role of MPLS-TP

The role of MPLS-TP is to provide a solution to help evolve traditional transport towards packet transport networks. It is designed to support the transport characteristics and behavior described in [RFC5654]. The primary use of MPLS-TP is largely to replace legacy transport technologies, such as SONET/SDH. MPLS-TP is not designed to replace the service support capabilities of IP/MPLS, such as L2VPN, L3VPN, IPTV, Mobile RAN, etc.

3.2. Provisioning Mode

MPLS-TP supports two provisioning modes:

- a mandatory static provisioning mode, which must be supported without dependency on dynamic routing or signaling; and

- an optional distributed dynamic control plane, which is used to enable dynamic service provisioning.

The decision on which mode to use is largely dependent on the operational feasibility and the stage of network transition. Operators who are accustomed to the transport-centric operational model (e.g., NMS configuration without control plane) typically prefer the static provisioning mode. This is the most common choice in current deployments. The dynamic provisioning mode can be more powerful, but it is more suited to operators who are familiar with the operation and maintenance of IP/MPLS technologies or are ready to step up through training and planned transition.

There may also be cases where operators choose to use the combination of both modes. This is appropriate when parts of the network are provisioned in a static fashion, and other parts are controlled by dynamic signaling. This combination may also be used to transition from static provisioning to dynamic control plane.

3.3. Standards Compliance

SPs generally recognize that standards compliance is important for lowering cost, accelerating product maturity, achieving multi-vendor interoperability, and meeting the expectations of their enterprise customers.

MPLS-TP is a joint work between the IETF and ITU-T. In April 2008, the IETF and ITU-T jointly agreed to terminate T-MPLS and progress MPLS-TP as joint work [RFC5317]. The transport requirements are provided by the ITU-T; the protocols are developed in the IETF.

3.4. End-to-End MPLS OAM Consistency

End-to-end MPLS OAM consistency is highly desirable in order to enable Service Providers to deploy an end-to-end MPLS solution. As MPLS-TP adds OAM function to the MPLS toolkit, it cannot be expected that a full-function end-to-end LSP with MPLS-TP OAM can be achieved when the LSP traverses a legacy MPLS/IP core. Although it may be possible to select a subset of MPLS-TP OAM that can be gatewayed to the legacy MPLS/IP OAM, a better solution is achieved by tunneling the MPLS-TP LSP over the legacy MPLS/IP network. In that mode of operation, legacy OAM may be run on the tunnel in the core, and the tunnel endpoints may report issues in as much detail as possible to the MIPs in the MPLS-TP LSP. Note that over time it is expected that routers in the MPLS/IP core will be upgraded to fully support MPLS-TP features. Once this has occurred, it will be possible to run end-to-end MPLS-TP LSPs seamlessly across the core.

3.5. PW Design Considerations in MPLS-TP Networks

In general, PWs in MPLS-TP work the same as in IP/MPLS networks. Both Single-Segment PW (SS-PW) and Multi-Segment PW (MS-PW) are supported. For dynamic control plane, Targeted LDP (tLDP) is used. In static provisioning mode, PW status is a new PW OAM feature for failure notification. In addition, both directions of a PW must be bound to the same transport bidirectional LSP.

In the common network topology involving multi-tier rings, the design choice is between using SS-PW or MS-PW. This is not a discussion unique to MPLS-TP, as it applies to PW design in general. However, it is relevant here, since MPLS-TP is more sensitive to the operational complexities, as noted by operators. If MS-PW is used, Switching PE (S-PE) must be deployed to connect the rings. The advantage of this choice is that it provides domain isolation, which in turn facilitates troubleshooting and allows for faster PW failure recovery. On the other hand, the disadvantage of using S-PE is that it adds more complexity. Using SS-PW is simpler, since it does not require S-PEs, but it is less efficient because the paths across primary and secondary rings are longer. If operational simplicity is a higher priority, some SPs choose SS-PW.

Another design trade-off is whether to use PW protection in addition to LSP protection or rely solely on LSP protection. When the MPLS-TP LSPs are protected, if the working LSP fails, the protecting LSP

assures that the connectivity is maintained and the PW is not impacted. However, in the case of simultaneous failure of both the working and protecting LSPs, the attached PW would fail. By adding PW protection and attaching the protecting PW to a diverse LSP not in the same Shared Risk Link Group (SRLG), the PW is protected even when the primary PW fails. Clearly, using PW protection adds considerably more complexity and resource usage, and thus operators often may choose not to use it and consider protection against a single point of failure as sufficient.

3.6. Proactive and On-Demand MPLS-TP OAM Tools

MPLS-TP provides both proactive and on-demand OAM tools. As a proactive OAM fault management tool, BFD Connectivity Check (CC) can be sent at regular intervals for Connectivity Check; three (or a configurable number) of missed CC messages can trigger the failure protection switch-over. BFD sessions are configured for both working and protecting LSPs.

A design decision is choosing the value of the BFD CC interval. The shorter the interval, the faster the detection time is, but also the higher the resource utilization is. The proper value depends on the application and the service needs, as well as the protection mechanism provided at the lower layer.

As an on-demand OAM fault management mechanism (for example, when there is a fiber cut), a Link Down Indication (LDI) message [RFC6427] can be generated from the failure point and propagated to the Maintenance Entity Group End Points (MEPs) to trigger immediate switch-over from working to protecting path. An Alarm Indication Signal (AIS) can be propagated from the Maintenance Entity Group Intermediate Point (MIP) to the MEPs for alarm suppression.

In general, both proactive and on-demand OAM tools should be enabled to guarantee short switch-over times.

3.7. MPLS-TP and IP/MPLS Interworking Considerations

Since IP/MPLS is largely deployed in most SPs' networks, MPLS-TP and IP/MPLS interworking is inevitable if not a reality. However, interworking discussion is out of the scope of this document; it is for further study.

4. Security Considerations

Under the use case of Metro access and aggregation, in the scenario where some of the access equipment is placed in facilities not owned by the SP, the static provisioning mode of MPLS-TP is often preferred over the control-plane option because it eliminates the possibility of a control-plane attack, which may potentially impact the whole network. This scenario falls into the Security Reference Model 2 as described in [RFC6941].

Similar location issues apply to the mobile use cases since equipment is often placed in remote and outdoor environment, which can increase the risk of unauthorized access to the equipment.

In general, NMS access can be a common point of attack in all MPLS-TP use cases, and attacks to GAL or G-ACh are unique security threats to MPLS-TP. The MPLS-TP security considerations are discussed in the MPLS-TP security framework [RFC6941]. General security considerations for MPLS and GMPLS networks are addressed in "Security Framework for MPLS and GMPLS Networks" [RFC5920].

5. Acknowledgements

The authors wish to thank Adrian Farrel for his review as Routing Area Director and his continued support and guidance. Adrian’s detailed comments and suggestions were of great help for improving the quality of this document. In addition, the authors would like to thank the following individuals: Loa Andersson for his continued support and guidance; Weiqiang Cheng for his helpful input on LTE mobile backhaul based on his knowledge and experience in real world deployment; Stewart Bryant for his text contribution on timing; Russ Housley for his improvement suggestions; Andrew Malis for his support and use case discussion; Pablo Frank, Lucy Yong, Huub van Helvoort, Tom Petch, Curtis Villamizar, and Paul Doolan for their comments and suggestions; and Joseph Yee and Miguel Garcia for their APPSDIR and Gen-ART reviews and comments, respectively.

6. References

6.1. Normative References

[RFC5654] Niven-Jenkins, B., Ed., Brungard, D., Ed., Betts, M., Ed., Sprecher, N., and S. Ueno, "Requirements of an MPLS Transport Profile", RFC 5654, September 2009.

[RFC5920] Fang, L., Ed., "Security Framework for MPLS and GMPLS Networks", RFC 5920, July 2010.

[RFC5921] Bocci, M., Ed., Bryant, S., Ed., Frost, D., Ed., Levrau, L., and L. Berger, "A Framework for MPLS in Transport Networks", RFC 5921, July 2010.

[RFC6426] Gray, E., Bahadur, N., Boutros, S., and R. Aggarwal, "MPLS On-Demand Connectivity Verification and Route Tracing", RFC 6426, November 2011.

[RFC6427] Swallow, G., Ed., Fulignoli, A., Ed., Vigoureux, M., Ed., Boutros, S., and D. Ward, "MPLS Fault Management Operations, Administration, and Maintenance (OAM)", RFC 6427, November 2011.

[RFC6428] Allan, D., Ed., Swallow Ed., G., and J. Drake Ed., "Proactive Connectivity Verification, Continuity Check, and Remote Defect Indication for the MPLS Transport Profile", RFC 6428, November 2011.

6.2. Informative References

[RFC5317] Bryant, S., Ed., and L. Andersson, Ed., "Joint Working Team (JWT) Report on MPLS Architectural Considerations for a Transport Profile", RFC 5317, February 2009.

[RFC6372] Sprecher, N., Ed., and A. Farrel, Ed., "MPLS Transport Profile (MPLS-TP) Survivability Framework", RFC 6372, September 2011.

[RFC6669] Sprecher, N. and L. Fang, "An Overview of the Operations, Administration, and Maintenance (OAM) Toolset for MPLS-Based Transport Networks", RFC 6669, July 2012.

[RFC6941] Fang, L., Ed., Niven-Jenkins, B., Ed., Mansfield, S., Ed., and R. Graveman, Ed., "MPLS Transport Profile (MPLS-TP) Security Framework", RFC 6941, April 2013.

[TICTOC] Davari, S., Oren, A., Bhatia, M., Roberts, P., Montini, L., and L. Martini, "Transporting Timing messages over MPLS Networks", Work in Progress, June 2013.

7. Contributors

Kam Lee Yap
XO Communications
13865 Sunrise Valley Drive
Herndon, VA 20171
United States
EMail: klyap@xo.com

Dan Frost
Cisco Systems, Inc.
United Kingdom
EMail: danfrost@cisco.com

Henry Yu
TW Telecom
10475 Park Meadow Dr.
Littleton, CO 80124
United States
EMail: henry.yu@twtelecom.com

Jian Ping Zhang
China Telecom, Shanghai
Room 3402, 211 Shi Ji Da Dao
Pu Dong District, Shanghai
China
EMail: zhangjp@shtel.com.cn

Lei Wang
Lime Networks
Strandveien 30, 1366 Lysaker
Norway
EMail: lei.wang@limenetworks.no

Mach (Guoyi) Chen
Huawei Technologies Co., Ltd.
No. 3 Xinxi Road
Shangdi Information Industry Base
Hai-Dian District, Beijing 100085
China
EMail: mach@huawei.com

Nurit Sprecher
Nokia Siemens Networks
3 Hanagar St. Neve Ne'eman B
Hod Hasharon, 45241
Israel
EMail: nurit.sprecher@nsn.com

Authors' Addresses

Luyuan Fang (editor)
Cisco Systems, Inc.
111 Wood Ave. South
Iselin, NJ 08830
United States
EMail: lufang@cisco.com

Nabil Bitar
Verizon
40 Sylvan Road
Waltham, MA 02145
United States
EMail: nabil.bitar@verizon.com

Raymond Zhang
Alcatel-Lucent
701 Middlefield Road
Mountain View, CA 94043
United States
EMail: raymond.zhang@alcatel-lucent.com

Masahiro Daikoku
KDDI Corporation
3-11-11.Iidabashi, Chiyodaku, Tokyo
Japan
EMail: ms-daikoku@kddi.com

Ping Pan
Infinera
United States
EMail: ppan@infinera.com