     The Reasons for Selecting a Single Solution for MPLS Transport Profile
        (MPLS-TP) Operations, Administration, and Maintenance (OAM)

Abstract

   The MPLS Transport Profile (MPLS-TP) is a profile of the MPLS
   technology for use in transport network deployments. The work on
   MPLS-TP has extended the MPLS technology with additional
   architectural elements and functions that can be used in any MPLS
   deployment. MPLS-TP is a set of functions and features selected from
   the extended MPLS toolset and applied in a consistent way to meet the
   needs and requirements of operators of packet transport networks.

   During the process of development of the profile, additions to the
   MPLS toolset have been made to ensure that the tools available met
   the requirements. These additions were motivated by MPLS-TP, but
   form part of the wider MPLS toolset such that any of them could be
   used in any MPLS deployment.

   One major set of additions provides enhanced support for Operations,
   Administration, and Maintenance (OAM). This enables fault management
   and performance monitoring to the level needed in a transport
   network. Many solutions and protocol extensions have been proposed
   to address the requirements for MPLS-TP OAM, and this document sets
   out the reasons for selecting a single, coherent set of solutions for
   standardization.

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/rfc6670.

Table of Contents

1. Introduction

   The MPLS Transport Profile (MPLS-TP) is a profile of MPLS technology
   for use in transport network deployments. Note that "transport" in
   this document is used in the context of transport networks as
   discussed in Section 1.3 of [RFC5654] and in [RFC5921]. The work on
   MPLS-TP has extended the MPLS toolset with additional architectural
   elements and functions that can be used in any MPLS deployment.
   MPLS-TP is a set of functions and features selected from the extended
   MPLS toolset and applied in a consistent way to meet the needs and
   requirements of operators of packet transport networks.

   Operations, Administration, and Maintenance (OAM) plays a significant
   role in carrier networks, providing methods for fault management and
   performance monitoring in both the transport and service layers, and
   enabling these layers to support services with guaranteed and strict
   Service Level Agreements (SLAs) while reducing their operational
   costs.

   OAM provides a comprehensive set of capabilities that operate in the
   data plane. Network-oriented mechanisms are used to monitor the
   network's infrastructure in order to enhance the network's general
   behavior and level of performance. Service-oriented mechanisms are
   used to monitor the services offered to end customers. Such
   mechanisms enable rapid response to a failure event and facilitate
   the verification of some SLA parameters. Fault management mechanisms
   are used for fault detection and localization as well as for
   diagnostics and notification. Performance management mechanisms
   enable monitoring of the quality of service with regard to key SLA
   criteria (e.g., jitter, latency, and packet loss).

   During the process of development of MPLS-TP, additions to the MPLS
   toolset have been made to ensure that the tools available meet the
   requirements. These additions were motivated by MPLS-TP, but form
   part of the wider MPLS toolset, such that any of them could be used
   in any MPLS deployment.

   One major set of additions provides enhanced support for OAM. Many
   solutions and protocol extensions have been proposed to address these
   OAM requirements. This document sets out the reasons for selecting a
   single, coherent set of OAM solutions for standardization.

The content of this document should be read in the context of
[RFC1958]. In particular, Section 3.2 of [RFC1958] says:

   If there are several ways of doing the same thing, choose one. If
   a previous design, in the Internet context or elsewhere, has
   successfully solved the same problem, choose the same solution
   unless there is a good technical reason not to. Duplication of
   the same protocol functionality should be avoided as far as
   possible, without of course using this argument to reject
   improvements.

1.1. Background

The ITU-T and the IETF jointly commissioned a Joint Working Team
(JWT) to examine the feasibility of a collaborative solution to
support OAM requirements for MPLS transport networks known as the
MPLS Transport Profile (MPLS-TP). The JWT reported that it is
possible to extend the MPLS technology to fully satisfy the
requirements [RFC5317]. The investigation by the JWT laid the
foundations for the work to extend MPLS, but a thorough technical
analysis was subsequently carried out within the IETF with strong
input from the ITU-T to ensure that the MPLS-TP OAM requirements
provided by the ITU-T and the IETF would be met.

The report of the JWT [RFC5317] as accepted by the ITU-T was
documented in [TD7] and was communicated to the IETF in a liaison
statement [LS26]. In particular, the ITU-T stated that any
extensions to MPLS technology will be progressed via the IETF
standards process using the procedures defined in [RFC4929].

[RFC5317] includes the analysis that "it is technically feasible that
the existing MPLS architecture can be extended to meet the
requirements of a Transport profile, and that the architecture allows
for a single OAM technology for LSPs, PWs, and a deeply nested
network". This provided a starting point for the work on MPLS-TP.

[RFC5654] in general, and [RFC5860] in particular, define a set of
requirements for OAM functionality in MPLS-TP that are applicable to
MPLS-TP Label Switched Paths (LSPs), Pseudowires (PWs), and MPLS-TP
links. These documents are the results of a joint effort by the
ITU-T and the IETF to include an MPLS Transport Profile within the
IETF MPLS and Pseudowire Emulation Edge-to-Edge (PWE3) architectures
to enable the deployment of a packet transport network that supports
the capabilities and functionalities of a transport network as
defined by the ITU-T. The OAM requirements are derived from those
specified by the ITU-T in [Y.Sup4].

An analysis of the technical options for OAM solutions was carried
out by a design team (the MEAD team) consisting of experts from both
the ITU-T and the IETF. The team reached an agreement on the
principles of the design and the direction for the development of an
MPLS-TP OAM toolset. A report was subsequently submitted to the IETF
MPLS working group at the Stockholm IETF meeting in July 2009
[DesignReport]. The guidelines drawn up by the design team have
played an important role in the creation of a coherent MPLS-TP OAM
solution.

The MPLS working group has modularized the function of MPLS-TP OAM,
allowing for separate and prioritized development of solutions. This
has given rise to a number of documents each describing a different
part of the solution toolset. At the time of this writing, the most
important of these documents have completed development within the
MPLS working group and are advancing through the IETF process toward
publication as RFCs. These documents cover the following OAM
features:

o Continuity Check

o Connection Verification

o On-Demand Connection Verification

o Route Tracing

o Remote Defect Indication

o Packet Loss Measurement

o Packet Delay Measurement

o Lock Instruction

o Loopback Testing

o Fault Management

The standardization process within the IETF allows for the continued
analysis of whether the OAM solutions under development meet the
documented requirements, and facilitates the addition of new
requirements if any are discovered. It is not the purpose of this
document to analyze the correctness of the selection of specific OAM
solutions. This document is intended to explain why it would be
unwise to standardize multiple solutions for MPLS-TP OAM, and to show

how the existence of multiple solutions would complicate MPLS-TP
development and deployment, making networks more expensive to build,
less stable, and more costly to operate.

1.2. The Development of a Parallel MPLS-TP OAM Solution

It has been suggested that a second (i.e., different) OAM solution
should also be developed and documented in an ITU-T Recommendation.
Various arguments have been presented for this duplication of effort,
including the following:

o Similarity to OAM encodings and mechanisms used in Ethernet.

o The existence of two distinct MPLS-TP deployment environments:
   Packet Switched Networks (PSNs) and Packet Transport Networks
   (PTNs).

o The need for similar operational experience in MPLS-TP networks
   and in pre-existing transport networks (especially Synchronous
   Optical Network/Synchronous Digital Hierarchy (SONET/SDH)
   networks).

The first of these was discussed within the IETF's MPLS working group
where precedence was given to adherence to the JWT's recommendation
to select a solution that reused as far as possible pre-existing MPLS
tools. Additionally, it was decided that consistency with encodings
and mechanisms used in MPLS was of greater importance.

The second argument has not been examined in great detail because
substantive evidence of the existence of two deployment environments
has not been documented or presented. Indeed, one of the key
differences cited between the two allegedly distinct environments is
the choice of MPLS-TP OAM solution, which makes a circular argument.

The third argument contains a very important point: network operators
want to achieve a smooth migration from legacy technologies such as
SONET/SDH to their new packet transport networks. This transition
can be eased if the new networks offer similar OAM features and can
be managed using tools with similar look and feel. The requirements
specifications [RFC5654] and [RFC5860] capture the essential issues
that must be resolved to allow the same look and feel to be achieved.
Since the OAM solutions developed within the IETF meet the documented
requirements, Network Management Systems (NMSs) can easily be built
to give the same type of control of MPLS-TP networks as is seen in
other transport networks. Indeed, it should be understood that the
construction of an NMS is not dependent on the protocols and packet
formats within the OAM but on the high-level features and functions
offered by the OAM.

   This document does not debate the technical merits of any specific
   solution. That discussion, and the documentation of MPLS-TP OAM
   specifications, was delegated by the IETF and ITU-T to the MPLS
   working group and can be conducted using the normal consensus-driven
   IETF process. [OAM-OVERVIEW] presents an overview of the OAM
   mechanisms that have already been defined and that are currently
   being defined by the IETF, as well as a comparison with other OAM
   mechanisms that were defined by the IEEE and ITU-T.

   This document focuses on an examination of the consequences of the
   existence of two MPLS-TP OAM solutions.

2. Terminology

2.1. Acronyms

   This document uses the following acronyms:

   ANSI   American National Standards Institute
   CESoPSN   Circuit Emulation Service over Packet Switched Network
   ETSI   European Telecommunications Standards Institute
   FPGA   Field-Programmable Gate Array
   GFP   Generic Framing Procedure
   IEEE   Institute of Electrical and Electronics Engineers
   ITU-T   International Telecommunication Union - Telecommunication
                 Standardization Sector
   JWT   Joint Working Team
   LSP   Label Switched Path
   MPLS-TP   MPLS Transport Profile
   NMS   Network Management System
   OAM   Operations, Administration, and Maintenance
   PDH   Plesiochronous Digital Hierarchy
   PSN   Packet Switched Network
   PTN   Packet Transport Network
   PW   Pseudowire
   PWE3   Pseudowire Emulation Edge-to-Edge
   SAToP   Structure-Agnostic Time Division Multiplexing over Packet
   SDH   Synchronous Digital Hierarchy
   SLA   Service Level Agreement
   SONET   Synchronous Optical Network
   TDM   Time Division Multiplexing
   TDMoIP   Time Division Multiplexing over IP

3. Motivations for a Single OAM Solution in MPLS-TP

   This section presents a discussion of the implications of the
   development and deployment of more than one MPLS OAM protocol. The
   summary is that it can be seen that there are strong technical,
   operational, and economic reasons to avoid the development and
   deployment of anything other than a single MPLS OAM protocol.

3.1. MPLS-TP Is an MPLS Technology

   MPLS-TP is an MPLS technology. It is designed to apply MPLS to a new
   application. The original proposers of the concept assumed that the
   transport variant of MPLS would always exist in a disjoint network,
   and indeed their first attempt at the technology (Transport MPLS
   (T-MPLS)) had a number of significant incompatibilities with MPLS
   that were irreconcilable. When it was established that coexistence
   in the same layer network could and would occur, T-MPLS development
   was stopped and the development of MPLS-TP was begun. In MPLS-TP,
   MPLS was extended to satisfy the transport network requirements in a
   way that was compatible both with MPLS as has already been deployed,
   and with MPLS as the IETF envisioned it would develop in the future.

   Given this intention for compatibility, it follows that the MPLS-TP
   OAM protocols should be designed according to the design philosophies
   that were applied for the existing deployed MPLS OAM and that have
   led to the current widespread adoption of MPLS. Key elements here
   are scalability and hardware independence, i.e., that the trade-off
   between scaling to large numbers of monitored objects and the
   performance of the monitoring system should be a matter for vendors
   and operators to resolve, and that the trade-off should be a soft
   transition rather than an abrupt one. Furthermore, there should be
   no requirement to execute any component (other than packet
   forwarding) in hardware to achieve usable performance.

3.2. MPLS-TP Is a Convergence Technology

   It is possible to argue that using MPLS for transport is only a
   stepping stone in the middle of a longer transition. Quite clearly,
   all communication applications are being moved to operate over the
   Internet protocol stack of TCP/IP/MPLS, and the various layers that
   have existed in communications networks are gradually being collapsed
   into the minimum necessary set of layers. Thus, for example, we no
   longer run IP over X.25 over High-Level Data Link Control (HDLC) over
   multi-layered Time Division Multiplexing (TDM) networks.

   Increasingly, the entire point of transport networks is to support
   the transmission of TCP/IP/MPLS. Using MPLS to construct a transport
   network may be a relatively short-term stepping stone toward running

IP and MPLS directly over fiber optics. MPLS has been deployed in
operational networks for approximately a decade, and the existing
MPLS OAM techniques have seen wide deployment. Service providers are
not going to stop using the MPLS-based OAM techniques that they have
been using for years, and no one has proposed that they would. Thus,
the question is not which OAM to use for transport networks; the
question is whether service providers want to use two different sets
of OAM tools in the future converged network. If we arrive at a
destination where TCP/IP/MPLS runs directly over fiber, the operators
will use MPLS OAM tools to make this work.

3.3. There Is an End-to-End Requirement for OAM

The purpose of OAM is usually to execute a function that operates end
to end on the monitored object (such as an LSP or PW). Since LSPs
and PWs provide edge-to-edge connectivity and can cross network
operator boundaries, the OAM must similarly operate across network
operator boundaries. This is particularly the case with the
continuity check and connection verification functions that are
needed to test the end-to-end connectivity of LSPs and PWs. It is,
therefore, necessary that any two pieces of equipment that could ever
be a part of an end-to-end communications path have a common OAM.
This necessity is emphasized in the case of equipment executing an
edge function, since with a global technology such as MPLS it could
be interconnected with edge equipment deployed by any other operator
in any part of the global network.

This leads to the conclusion that it is desirable for any network-
layer protocol in all equipment to be able to execute or to interwork
with a canonical form of the OAM. As discussed in Section 4,
interworking between protocols adds significant complexity; thus, a
single default OAM is strongly preferred.

3.4. The Complexity Sausage

A frequent driver for the replacement of an established technology is
a perception that the new technology is simpler and thus of greater
economic benefit to the user. In an isolated system, this may be the
case; however, as is usually the case with communications
technologies, simplification in one element of the system introduces
an increase (possibly a non-linear one) in complexity elsewhere.

This creates the "squashed sausage" effect, where reduction in
complexity at one place leads to significant increase in complexity
at a remote location. When we drive complexity out of hardware by
placing complexity in the control plane, there is frequently an
economic benefit, as illustrated by MPLS itself.

Some motivation for the second OAM solution is the simplicity of
operation at a single node in conjunction with other transport OAM
mechanisms. However, when we drive OAM complexity out of one network
element at the cost of increased complexity at a peer network
element, we lose out economically and, more importantly, we lose out
in terms of the reliability of this important network functionality.
Due to the need to ensure compatibility of an interworking function
between the two MPLS-TP OAM solutions (in order to achieve end-to-end
OAM), we create a situation where neither of two disjoint protocol
developments is able to make technical advances. Such a restriction
is unacceptable within the context of the Internet.

3.5. Interworking Is Expensive and Has Deployment Issues

The issue of OAM interworking can easily be illustrated by
considering an analogy with people speaking different languages.
Interworking is achieved through the use of an interpreter. The
interpreter introduces cost, slows down the rate of information
exchange, and may require transition through an intermediate
language. There is considerable risk of translation errors and
semantic ambiguities. These considerations also apply to computer
protocols, particularly given the ultra-pedantic nature of such
systems. In all cases, the availability of a single working language
dramatically simplifies the system, reduces cost, and speeds reliable
communication.

If two MPLS OAM protocols were to be deployed, we would have to
consider three possible scenarios:

1. Isolation of the network into two incompatible and unconnected
    islands.

2. Universal use of both OAM protocols.

3. Placement of interworking (translation) functions or gateways.

We have many existence proofs that isolation is not a viable
approach, and the reader is referred to the early T-MPLS discussions
for examples. In summary, the purpose of the Internet is to achieve
an integrated universal connectivity. Partition of the Internet into
incompatible and unconnected islands is neither desirable nor
acceptable.

Universal deployment of both OAM protocols requires the sum of the
costs associated with each protocol. This manifests as
implementation time, development costs, memory requirements, hardware
components, and management systems. It introduces additional testing
requirements to ensure there are no conflicts (processing state,

fault detection, code path, etc.) when both protocols are run on a
common platform. It also requires code and the processes to deal
with the negotiation of which protocol to use and to deal with
conflict resolution (which may be remote and multi-party) when an
inconsistent choice is made. In short, this option results in more
than double the cost, increases the complexity of the resulting
system, risks the stability of the deployed network, and makes the
networks more expensive and more complicated to operate.

The third possibility is the use of some form of interworking
function. This is not a simple solution and inevitably leads to cost
and complexity in implementation, deployment, and operation. Where
there is a chain of communication (end-to-end messages passed through
a series of transit nodes), a choice must be made about where to
apply the translation and interworking.

o In a layered architecture, interworking can be achieved through
   tunneling with the translation points at the end-points of the
   tunnels. In simple network diagrams, this can look very
   appealing, and only one end-node is required to be able to perform
   the translation function (effectively speaking both OAM
   languages). But in the more complex reality of the Internet,
   nearly every network node performs the function of an end-node,
   and so the result is that nearly every node must be implemented
   with the capability to handle both OAM protocols and to translate
   between them. This turns out to be even more complex than the
   universal deployment of both protocols discussed above.

o In a flat architecture, interworking is performed at a "gateway"
   between islands implementing different protocols. Gateways are
   substantially complex entities that usually have to maintain
   end-to-end state within the network (something that is against one
   of the fundamental design principles of the Internet) and must
   bridge the differences in state machines, message formats, and
   information elements in the two protocols. The complexity of
   gateways makes them expensive, fragile, and unstable; hard to
   update when new revisions of protocols are released; and difficult
   to manage.

To deploy an interworking function, it is necessary to determine
whether the OAM protocol on the arriving segment of the OAM is
identical to the OAM protocol on the departing segment. Where the
protocols are not the same, it is necessary to determine which party
will perform the translation. It is then necessary to route the LSP
or PW through a translation point that has sufficient translation
capacity and sufficient data bandwidth, as well as adequate path

diversity. When an upgraded OAM function is required, the problem
changes from a two-party negotiation to an n-party negotiation with
commercial and deployment issues added to the mix.

Note that when an end-to-end LSP or PW is deployed, it may transit
many networks, and the OAM might require repeated translation back
and forth between the OAM protocols. The consequent loss of
information and potential for error is similar to the children's game
of "telephone".

3.6. Selection of a Single OAM Solution When There Is a Choice

When there is a choice of protocols for deployment or operation, a
network operator must make a choice. Choice can be a good thing when
it provides for selection between different features and functions,
but it is a burden when the protocols offer essentially the same
functions but are incompatible.

In this case, the elements of the choice include the following:

o Which protocol will continue to be developed by its Standards
   Development Organization (SDO)?

o Which protocol is most stable in implementations?

o How does a network operator test and evaluate the two protocols?

o Which vendors support and will continue to support which protocol?

o What equipment from different vendors is compatible?

o Which management tools support which protocols?

o What protocols are supported by peer operators, and what
   interworking function is needed?

o Which protocols are engineers experienced with and trained in?

o What are the consequences of a wrong choice?

o Will it be possible to migrate from one protocol to another in the
   future?

o How is integration with other functions already present in the
   network accomplished?

o How does a network operator future-proof against the inclusion of
   new functions in the network?

At the very least, the evaluation of these questions constitutes a
cost and introduces delay for the operator. The consequence of a
wrong choice could be very expensive, and it is likely that any
comparative testing will more than double the lab-test costs prior to
deployment.

From a vendor's perspective, the choice is even harder. A vendor
does not want to risk not offering a product for which there is
considerable demand, so both protocols may need to be developed,
leading to more than doubled development costs. Indeed, code
complexity and defect rates have often been shown to increase more
than linearly with code size, and (as noted in Section 3.5) the need
to test for coexistence and interaction between the protocols adds to
the cost and complexity.

It should be noted that, in the long run, it is the end-users who pay
the price for the additional development costs and any network
instability that arises.

3.7.   Migration Issues

Deployment of a technology that is subsequently replaced or obsoleted
often leads to the need to migrate from one technology to another.
Such a situation might arise if an operator deploys one of the two
OAM protocol solutions and discovers that he needs to migrate to the
other one. A specific case would be when two operators merge their
networks but are using different OAM solutions.

When the migration is between versions of a protocol, it may be that
the new version is defined to support the old version. If the
implementation is in software (including FPGAs), upgrades can be
managed centrally. However, neither of these would be the case with
MPLS-TP OAM mechanisms, and hardware components would need to be
upgraded in the field using expensive call-out services.

Hardware upgrades are likely to affect service, even with
sophisticated devices with redundant hardware components.
Furthermore, since it would be impractical to upgrade every device in
the network at the same time, there is a need for either a
significantly large maintenance period across the whole network or
for a rolling plan that involves upgrading nodes one at a time with
new hardware that has dual capabilities. Such hardware is, of
course, more expensive and more complex to configure than hardware
dedicated to just one OAM protocol.

Additionally, the transition phase of migration leads to dual-mode
networks as described in Section 4.3. Such networks are not
desirable because of their cost and complexity.

In short, the potential for future migration will need to be part of
the deployment planning exercise when there are two OAM protocols to
choose between. This issue will put pressure on making the "right"
choice when performing the selection described in Section 3.6.

4. Potential Models for Coexistence

   This section expands upon the discussion in Section 3 by examining
   three questions:

   o What does it mean for two protocols to be incompatible?

   o Why can't we assume that the two solutions will never coexist in
      the same network?

   o What models could we support for coexistence?

4.1. Protocol Incompatibility

   Protocol incompatibility comes in a range of grades of seriousness.
   At the most extreme, the operation of one protocol will prevent the
   safe and normal operation of the other protocol. This was the case
   with the original T-MPLS, where MPLS labels that could be used for
   data in a native MPLS system were assigned special meaning in T-MPLS
   such that data packets would be intercepted and mistaken for OAM
   packets.

   A lesser incompatibility arises where the packets of one protocol are
   recognized as "unknown" or "not valid" by implementations of the
   other protocol. In this case, the rules of one protocol require that
   the packets of the other protocol be discarded and may result in the
   LSP or PW being torn down.

   The least serious level of incompatibility is where the packets of
   one protocol are recognized as "unknown" by implementations of the
   other protocol, but where the rules of one protocol allow the packets
   of the other protocol to be ignored; in this case, such packets are
   either silently discarded or forwarded untouched.

   These are issues with all of these grades of incompatibility; these
   issues range from disruption or corruption of user data, through
   connection failure, to the inability to provide end-to-end OAM
   function without careful planning and translation functions.

4.2. Inevitable Coexistence

   Networks expand and merge. For example, one service provider may
   acquire another and wish to merge the operation of the two networks.
   This makes partitioning networks by protocol deployment a significant
   issue for future-proofing commercial interactions. Although a
   network operator may wish to present difficulties in order to
   disincentivize hostile takeover (a poison pill), most operators are
   interested in future options to grow their networks.

   As described in Section 3.2, MPLS is a convergence technology. That
   means that there is a tendency for an ever-increasing number of
   services to be supported by MPLS and for MPLS to be deployed in an
   increasing number of environments. It would be an unwise operator
   who deployed a high-function convergence technology in such a way
   that the network could never be expanded to offer new services or to
   integrate with other networks or technologies.

   As described in Section 3.3, there is a requirement for end-to-end
   OAM. That means that where LSPs and PWs span multiple networks,
   there is a need for OAM to span multiple networks.

   All of this means that, if two different OAM protocol technologies
   are deployed, there will inevitably come a time when some form of
   coexistence is required, no matter how carefully the separation is
   initially planned.

4.3. Models for Coexistence

   Two models for coexistence can be considered:

   1. An integrated model based on the "ships-in-the-night" approach.
       In this model, there is no protocol translation or mapping. This
       model can be decomposed as follows:

       * A non-integrated mixed network, where some nodes support just
          one protocol, some support just the other, and no node
          supports both protocols.

       * Partial integration, where some nodes support just one
          protocol, some support just the other, and some support both
          protocols.

       * Fully integrated dual mode, where all nodes support both
          protocols.

   2. An "island" model, where groups of similar nodes are deployed
       together. In this model, there may be translation or mapping,
       but it is not always required. This model can be further
       decomposed as follows:

       * "Islands in a sea", where connectivity between islands of the
          same type is achieved across a sea of a different type.

       * "Border crossings", where connectivity between different
          islands is achieved at the borders between them.

4.3.1. The Integrated Model

   The integrated model assumes that nodes of different capabilities
   coexist within a single network. Dual-mode nodes supporting both OAM
   solutions may coexist in the same network. Interworking is not
   required in this model, and no nodes are capable of performing
   translation or gateway function (see Section 4.3.2 for operational
   modes including translation and gateways).

   In this model, protocol messages pass as "ships in the night" unaware
   of each other and without perturbing each other.

   As noted above, there are several sub-models.

4.3.1.1. Mixed Network without Integration

   In a mixed network with no integration, some nodes support one
   protocol and other nodes support the other protocol. There are no
   nodes that have dual capabilities.

   All nodes on the path of an LSP or PW that are required to play an
   active part in OAM must support the same OAM protocol. Nodes that do
   not support the OAM protocol will silently ignore (and possibly
   discard) OAM packets from the other protocol and cannot form part of
   the OAM function for the LSP or PW.

   In order to provision an end-to-end connection that benefits from the
   full OAM functionality, the planning and path-computation tool must
   know the capabilities of each network node and must select a path
   that includes only nodes with the same OAM protocol capability. This
   can result in considerably suboptimal paths and may lead to the
   network being partitioned. In the most obvious case, connectivity
   can only be achieved between end-points with the same OAM capability.
   This leads to considerable operational complexity and expense, as
   well as the inability to provide a fully flexible mesh of services.

   In the event of dynamic network changes (such as fast reroute) or if
   misconnectivity occurs, nodes of mismatched OAM capabilities may
   become interconnected. This will disrupt traffic delivery because
   end-to-end continuity checks may be disrupted, and it may be hard or
   impossible to diagnose the problem because connectivity verification
   and route trace functions will not work properly.

4.3.1.2. Partial Integration

   In a partially integrated network, the network described in
   Section 4.3.1.1 is enhanced by the addition of a number of nodes with
   dual capabilities. These nodes do not possess gateway or translation
   capabilities (this is covered in Section 4.3.2), but each such node
   can act as a transit point or end-node for an LSP or PW that uses
   either OAM protocol.

   Complexity of network operation is not eased, but there is greater
   connectivity potential in the network.

4.3.1.3. Dual Mode

   Dual mode is a development of partial integration (Section 4.3.1.2)
   such that all nodes in the network are capable of both OAM protocols.
   As in that section, these nodes do not possess gateway or translation
   capabilities (this is covered in Section 4.3.2), but each such node
   can act as a transit point or end-node for an LSP or PW that uses
   either OAM protocol. Thus, every LSP or PW in the network can be
   configured to use either of the OAM protocols.

   However, it seems unlikely that an operator would choose which OAM
   protocol to use on a per-LSP or per-PW basis. That would lead to
   additional complexity in the management system and potential
   confusion if additional diagnostic analytics need to be performed.
   This mode increases the complexity of implementation, deployment, and
   operation without adding to the function within the network (since
   both OAM solutions provide the same level of function), so this mode
   would not be selected for deployment except, perhaps, during
   migration of the network from one OAM protocol to the other.

4.3.2. The Island Model

   In the island model, regions or clusters of nodes with the same OAM
   capabilities are grouped together. Tools to interconnect the
   technologies are deployed based on layered networking or on
   interworking between the protocols. These lead to the two sub-models
   described in the sections that follow.

4.3.2.1. Islands in a Sea

   One way to view clusters of nodes supporting one OAM protocol is as
   an island in a sea of nodes supporting the other protocol. In this
   view, tunnels are used to carry LSPs or PWs using one OAM type across
   the sea and into another island of a compatible OAM type. The tunnel
   in this case is an LSP utilizing the OAM protocol supported by the
   nodes in the sea. Theoretically, an island can be as small as one
   node, and the strait between two islands can be as narrow as just
   one node.

   Layering in this way is an elegant solution to operating two
   protocols simultaneously and is, of course, used to support different
   technologies (such as MPLS over optical). However, in such layering
   deployments, there is no simple integration of OAM between the
   layers, and the OAM in the upper layer must regard the tunnel as a
   single hop with no visibility into the OAM of the lower layer.
   Diagnostics within the upper layer are complicated by this "hiding"
   of the nodes along the path of the tunnel in the lower layer.

   In the scenarios described so far, both ends of each connection have
   been placed in islands of compatible OAM types. It is possible to
   achieve connectivity between a node in an island and a node in the
   sea if the end-point in the sea has dual capabilities (i.e., can be
   viewed as a single-node island).

   A number of islands may lie along the path between end-points,
   necessitating the use of more than one tunnel. To further complicate
   matters, the islands may lie in an inland sea so that it is necessary
   to nest tunnels.

   Regardless of the scenario, operating such tunnels/layers adds to the
   management complexity and expense. Furthermore, it should be noted
   that in an MPLS network there is often a call for any-to-any
   connectivity. That is, any node in the network may need to establish
   an LSP or a PW to any other node in the network. As previously
   noted, the end-points of any LSP or PW must support the same OAM type
   in the islands-in-a-sea model, so this tends to imply that all, or
   nearly all, nodes will end up needing to support both OAM protocols.

   The use of tunnels can also degrade network services unless carefully
   coordinated. For example, a service in the upper layer may be
   provisioned with protection so that a working and backup path is
   constructed using diverse paths to make them robust against a single
   failure. However, the paths of the tunnels (in the lower layer) are
   not visible to the path computation in the upper layer, with the risk
   that the upper layer working and protection paths share a single
   point of failure in the lower layer. Traffic engineering techniques

have been developed to resolve this type of issue, but they add
significant complexity to a system that would be a simple flat
network if only one OAM technology was used.

4.3.2.2. Border Crossings

Instead of connecting islands with tunnels across the sea, islands of
different types can be connected directly so that the LSP or PW
transits the series of islands without tunneling. In this case,
protocol translation is performed each time the LSP/PW crosses a
border between islands that use a different OAM protocol.

In principle, this makes for a straightforward end-to-end connection.
However, protocol translation presents a number of issues, as
described in Section 3. The complexity is that in planning the
end-to-end connection, gateways with protocol translation
capabilities must be selected to lie on the path.

5. The Argument for Two Solutions

The decision to define and develop an alternative MPLS-TP OAM
solution was based on several assertions:

o The IETF solution is taking too long to standardize.

o Commonality with Ethernet solutions is beneficial.

o There are two different application scenarios.

o There is no risk of interaction between the solutions.

o The market should be allowed to decide between competing
   solutions.

The following sections look briefly at each of these claims.

5.1. Progress of the IETF Solution

The MPLS-TP OAM work carried out within the IETF is the product of
joint work within the IETF and ITU-T communities. That is, all
interested parties share the responsibility for progressing this work
as quickly as possible. Since the work is contribution-driven, there
is no reason to assume that consensus on the technical content of the
work could be reached any more quickly.

Opening discussions on a second solution seems certain to increase
the workload and will only slow down the speed at which consensus is
reached.

The core work on MPLS-TP OAM within the IETF was completed, and the
specifications were published as RFCs. For more information, see
[ISOCAnnounce].

5.2. Commonality with Ethernet OAM

Ethernet can be used to build packet transport networks, and so there
is an argument that Ethernet and MPLS-TP networks will be operated as
peers. Examining the issues of end-to-end connections across mixed
networks, many of the same issues as those discussed in Section 4
arise. If a peer networking gateway model (see Section 4.3.2.2) is
applied, there is a strong argument for making the OAM technologies
as similar as possible.

While this might be a valid discussion point when selecting the
single OAM solution for MPLS-TP, it is countered by the need to
achieve OAM consistency between MPLS and MPLS-TP networks. One might
make the counter-argument that if there is a strong need to make
MPLS-TP as similar as possible to Ethernet, it would be better to go
the full distance and simply deploy Ethernet.

Furthermore, the approach of a second MPLS-TP OAM protocol does not
resolve anything. Since MPLS-TP is not Ethernet, a gateway will
still be needed. This would constitute a second MPLS-TP OAM, so
additional gateways or interworking functions will be needed because
coexistence is inevitable, as described in the rest of this document.

Additionally, it may be claimed that implementation can be simplified
if the OAM solution developed for MPLS-TP is similar to Ethernet OAM.
This would apply both in the hardware/software implementing the OAM,
and at the server-to-client interface where OAM-induced fault status
is reported. The questions here are very much implementation
dependent, as the necessary function is contained within individual
nodes. The counter-argument is that implementation simplicity can
also be achieved by making MPLS-TP OAM similar to MPLS OAM,
especially since the client technology may well be IP/MPLS and since
MPLS is an end-to-end technology.

5.3. Different Application Scenarios

It has been suggested that two different applications of MPLS-TP
exist: Packet Switched Networks (PSNs) and Packet Transport Networks
(PTNs). These applications have not been documented in the IETF, and
most of the support for this idea has been documented by the ITU-T
[TD522].

One of the stated differences between these applications lies in the
OAM tools that are required to support the distinct operational
scenarios. The OAM used in a PSN should be similar to that used in
an MPLS network (and so should be the MPLS-TP OAM defined in the
IETF), while the OAM used in a PTN should provide the same
operational experience as that found in SONET/SDH and Optical
Transport Networks (OTNs).

The basic MPLS-TP OAM requirements in [RFC5654] make this point as
follows:

   Furthermore, for carriers it is important that operation of such
   packet transport networks should preserve the look-and-feel to
   which carriers have become accustomed in deploying their optical
   transport networks, while providing common, multi-layer
   operations, resiliency, control, and multi-technology management.

Thus, the look and feel of the OAM has been a concern in the design
of MPLS-TP from the start, and the solutions that have been defined
in the IETF were designed to comply with the requirements and to
provide operational behavior, functionality, and processes similar to
those available in existing transport networks. In particular, the
toolset supports the same controls and indications as those present
in other transport networks, and the same management information
model can be used to support the MPLS-TP OAM tools (in areas where
the technology type is irrelevant).

It is important to note that the operational look and feel does not
determine the way in which OAM function is achieved. There are
multiple ways of achieving the required functionality while still
providing the same operational experience and supporting the same
management information model. Thus, the OAM protocol solution does
not dictate the look and feel, and the demand for a particular
operational experience does not necessitate the development of a
second OAM protocol.

5.4. Interaction between Solutions

Section 3 of this document discusses how network convergence occurs
and indicates that where two MPLS-TP solutions exist, they are in
fact very likely to appear either in the same network or at gateways
between networks in order to provide end-to-end OAM functionality.

Indeed, since nodes offering either solution are likely to both be
branded as "MPLS-TP", and since network interoperation (as described
in Section 4) demands the existence of some nodes that are either
dual-mode or act as protocol translators/gateways, there is
considerable likelihood of the two OAM solutions interacting through

design or through accident. When a node is capable of supporting
both OAM protocols, it must be configured to support the correct
protocol for each interface and LSP/PW. When a device has interfaces
that offer different MPLS-TP OAM functions, the risk of
misconfiguration is significant. When a device is intended to
support end-to-end connections, it may need to translate, map, or
tunnel to accommodate both protocols.

Thus, the very existence of two OAM protocols within the common
MPLS-TP family makes copresence and integration most likely.

5.5. Letting the Market Decide

When two technologies compete, it is common to let the market decide
which one will survive. Sometimes the resolution is quite fast, and
one technology dominates the other before there is widespread
deployment. Sometimes it takes considerable time before one
technology overcomes the other, perhaps because one technology has
become entrenched before the emergence of the other, as in the case
of MPLS replacing ATM. In more cases, however, the market does not
select in favor of one technology or the other -- as in many of the
cases described in Sections 4 and 5 of this document, sometimes both
technologies continue to live in the network.

Letting the market decide is not a cheap option. Even when the
resolution is rapid, equipment vendors and early adopters pay the
price of both technologies. When it takes longer to determine which
technology is correct, there will be a period of coexistence followed
by the need to transition equipment from the losing solution to the
winning one. In the cases where no choice is made, the network is
permanently complicated by the existence of the competing
technologies.

In fact, the only time when allowing the market to decide can be
easily supported is when the competing technologies do not overlap.
In those cases -- for example, different applications in the user
space -- the core network is not perturbed by the decision-making
process, and transition from one technology to the other is
relatively painless. This is not the case for MPLS-TP OAM;
coexistence while the market determines the correct approach would be
expensive, while the necessary transition after the decision has been
made would be difficult and costly.

6. Security Considerations

   This informational document does not introduce any security issues.

   However, it should be noted that the existence of two OAM protocols
   raises a number of security concerns:

   o Each OAM protocol must be secured. This leads to the existence of
      two security solutions that each need configuration and
      management. The increased complexity of operating security
      mechanisms tends to reduce the likelihood of them being used in
      the field and so increases the vulnerability of the network.
      Similarly, the existence of two security mechanisms raises the
      risk of misconfiguration.

   o One OAM protocol may be used as a vector to attack the other.
      Inserting an OAM message of the other OAM protocol onto a link may
      cause the service to be disrupted and, because some nodes may
      support both OAM protocols, it may be possible to cause the
      disruption at a remote point in the network.

   o Securing a network protocol is not a trivial matter for protocol
      designers. Duplicating design effort is unlikely to result in a
      stronger solution and runs the risk of diluting the effort and
      creating two less-secure solutions.

7. Acknowledgments

   Thanks to Brian Carpenter, Tom Petch, Rolf Winter, Alexander
   Vainshtein, Ross Callon, Malcolm Betts, and Martin Vigoureux for
   their review and useful comments.

   Thanks to Huub van Helvoort for supplying text and history about
   SONET/SDH.

8. References

8.1. 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.

   [RFC5860] Vigoureux, M., Ed., Ward, D., Ed., and M. Betts, Ed.,
              "Requirements for Operations, Administration, and
              Maintenance (OAM) in MPLS Transport Networks", RFC 5860,
              May 2010.

8.2. Informative References

   [RFC1958] Carpenter, B., Ed., "Architectural Principles of the
              Internet", RFC 1958, June 1996.

   [RFC4553] Vainshtein, A., Ed., and YJ. Stein, Ed., "Structure-
              Agnostic Time Division Multiplexing (TDM) over Packet
              (SAToP)", RFC 4553, June 2006.

   [RFC4929] Andersson, L., Ed., and A. Farrel, Ed., "Change Process
              for Multiprotocol Label Switching (MPLS) and Generalized
              MPLS (GMPLS) Protocols and Procedures", BCP 129, RFC 4929,
              June 2007.

   [RFC5086] Vainshtein, A., Ed., Sasson, I., Metz, E., Frost, T., and
              P. Pate, "Structure-Aware Time Division Multiplexed (TDM)
              Circuit Emulation Service over Packet Switched Network
              (CESoPSN)", RFC 5086, December 2007.

   [RFC5087] Stein, Y(J)., Shashoua, R., Insler, R., and M. Anavi,
              "Time Division Multiplexing over IP (TDMoIP)", RFC 5087,
              December 2007.

   [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.

   [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.

   [OAM-OVERVIEW]
              Mizrahi, T., Sprecher, N., Bellagamba, E., and Y.
              Weingarten, "An Overview of Operations, Administration,
              and Maintenance (OAM) Mechanisms", Work in Progress,
              March 2012.

   [Y.Sup4]   "Supplement on transport requirements for T-MPLS OAM and
              considerations for the application of IETF MPLS
              technology", ITU-T Y.1300-series Supplement 4,
              January 2008.

   [G.707]   "Network node interface for the synchronous digital
              hierarchy (SDH)", ITU-T Recommendation G.707,
              January 2007.

   [TD7]   "IETF and ITU-T cooperation on extensions to MPLS for
                transport network functionality", ITU-T TD7 (WP3/SG15),
                December 2008.

   [TD522]   "Clarification of the PTN/solution X environment",
                ITU-T TD522 (WP3/SG15), February 2011.

   [LS26]   "Cooperation Between IETF and ITU-T on the Development of
                MPLS-TP", ITU-T COM 15-LS26-E, December 2008,
                <http://datatracker.ietf.org/documents/LIAISON/
                file596.pdf>.

   [DesignReport]
                "MPLS-TP OAM Analysis", Proc. IETF 75, Stockholm, Sweden,
                July 2009, <http://www.ietf.org/proceedings/75/slides/
                mpls-17/mpls-17_files/frame.htm>.

   [ISOCAnnounce]
                "Milestone Achieved in Internet Carrier Network Standards
                - Multiprotocol Label Switching Transport Profile
                (MPLS-TP) Specifications Published", Internet Society,
                December 2011, <http://www.isoc.org/standards/mpls.shtml>.

Appendix A. Examples of Interworking Issues in the Internet

   It is, of course, right to observe that there are a number of
   instances of multiple protocols serving the same purpose that have
   arisen within the Internet. It is valuable to examine these examples
   to understand what issues they have caused and how they have been
   mitigated.

A.1. IS-IS/OSPF

   IS-IS and OSPF are two competing link-state IGP routing protocols
   that derive from the same root technology and that, for political and
   personality reasons, were never reconciled prior to wide-scale
   deployment. It is an accident of history that one of these protocols
   did not gain overwhelming deployment and so force the other into
   retirement.

   The existence of these two widely deployed and highly functional
   competing IGPs doubles the cost of link-state IGP maintenance and
   deployment in the Internet. This is a situation that will almost
   certainly continue for the lifetime of the Internet. Although the
   Internet is clearly successful and operates well, the existence of
   these two IGPs forces router vendors to implement both protocols
   (doubling the protocol cost of all routers even when an operator only
   wants to deploy one of the protocols), forcing the operator to make
   an active choice between IGPs during deployment and requiring a
   gateway function between the islands of protocol use.

   A mitigating factor in this specific case is that, owing to the way
   networks are partitioned for administrative and scaling reasons,
   there already existed a gateway routing protocol called BGP that
   propagates a summarized form of the IGP reachability information
   throughout the Internet. BGP means that there is actually no
   requirement for IS-IS and OSPF to interwork directly: that is, there
   is no need for a translation function between OSPF and IS-IS, and the
   two IGPs can continue to exist without impacting the function of the
   Internet. Thus, unlike the situation with MPLS OAM, the choice of
   IGP protocol is truly a local decision; however, there is a cost to
   BGP implementations that must support interactions with both OSPF
   and IS-IS.

A.2. Time Division Multiplexing Pseudowires

   The IETF's PWE3 working group has published the specification of
   three different TDM PW types. This happened after considerable
   effort to reach a compromise failed to reduce the set of options.

   o SAToP is a relatively simple design. It is a Proposed Standard
      RFC [RFC4553] and is the mandatory-to-implement, default mode of
      operation.

   o CESoPSN [RFC5086] and TDMoIP [RFC5087] are more complex approaches
      with different degrees of bandwidth efficiency optimized for
      different applications. They are both published as Informational
      RFCs.

   In this case, all implementations must include the default mode of
   operation (SAToP). This means that end-to-end operation is
   guaranteed: an operator can select equipment from any vendor in the
   knowledge that he will be able to build and operate an end-to-end TDM
   PW service.

   If an operator wishes to deploy a TDM PW optimized for a specific
   application, he may select equipment from a vendor offering CESoPSN
   or TDMoIP in addition to SAToP. Provided that all of his equipment
   and his management system can handle the optimized approach, he can
   run this in his network, but he has to carry the cost of selecting,
   purchasing, configuring, and operating the extended mode of
   operation.

   This situation is far from ideal, and it is possible that
   long-distance, multi-operator optimized TDM PWs cannot be achieved.
   However, the existence of a default mode implemented in all devices
   helps to reduce pain for the operator and ensures that simpler
   end-to-end operation is always available. Additionally, the growth
   of other protocols is acting to diminish the use of long-distance TDM
   circuits, making this a self-limiting problem.

A.3. Codecs

   The n-squared codec interworking problem was brought to the attention
   of the IETF by the ITU-T when the IETF started its work on a royalty-
   free codec suitable for use in the Internet. Every time a new codec
   is deployed, translation between it and all other deployed codecs
   must be available within the network; each participating node must be
   able to handle the new codec. Translation between codecs is
   expensive and can lead to reduced quality.

This problem seriously constrains the addition of new codecs to the
available set, and new codecs are only designed and released when
there is a well-established need (such as a major difference in
functionality).

The application layer of the Internet is, however, predicated on a
business model that allows for the use of shared, free, and
open-source software; this model requires the existence of a
royalty-free codec. This, together with the specific characteristics
of transmission over lossy packet networks, comprised requirements
equivalent to a major difference in functionality and led to work in
the IETF to specify a new codec.

The complexity, economic, and quality costs associated with
interworking with this new codec will need to be factored into the
deployment model. This, in turn, may adversely affect its adoption
and the viability of its use in the Internet.

A.4. MPLS Signaling Protocols

There are three MPLS signaling control protocols used for
distributing labels to set up LSPs and PWs in MPLS networks: LDP,
RSVP - Traffic Engineering (RSVP-TE), and GMPLS.

The application domain for each of these protocols is different, and
unlike the OAM situation, there is limited requirement for
interworking between the protocols. For example, although one
provider may use LDP to set up LSPs while its peer uses RSVP-TE,
connectivity between the two providers usually takes place at the IP
layer.

It should be noted that the IETF initially worked on another
signaling protocol called Constraint-based Routed LDP (CR-LDP) with
variants applicable to MPLS and GMPLS. The development of this
protocol was allowed to progress in parallel with RSVP-TE. However,
once it was possible to determine that the solution preferred by the
community of vendors and operators was RSVP-TE, the IETF terminated
all further work on CR-LDP. No translation function or gateway point
interfacing RSVP-TE to CR-LDP was ever proposed.

A.5. IPv4 and IPv6

If there were ever an example of why protocol interworking is to be
avoided if at all possible, it is the transition from IPv4 to IPv6.

The reasons for introducing IPv6 into the Internet are well known and
don't need discussion here. IPv6 was not introduced as a competitor
to IPv4 but rather as a planned replacement. The need for the

   transition to IPv6 arose from the expansion of the network size
   beyond the wildest dreams of the creators of the Internet and from
   the consequent depletion of the IPv4 address space.

   This transition has proved to be the hardest problem that the IETF
   has ever addressed. The invention and standardization of IPv6 were
   straightforward by comparison, but it has been exceptionally
   difficult to migrate networks from one established protocol to a new
   protocol.

   The early assumption that by the time the IPv4 address space was
   exhausted IPv6 would be universally deployed failed to materialize
   due to (understandable) short-term economic constraints. Early
   migration would have been simpler and less costly than the current
   plans. The Internet is now faced with the considerable complexity of
   implementing and deploying interworking functions.

   If anything can be learned from the IPv4/IPv6 experience, it is that
   every effort should be applied to avoid the need to migrate or
   jointly operate two protocols within one network. Adding to the mix,
   a number of issues caused by OAM interworking of MPLS, one of the
   Internet's core protocols, would be most unwelcome and would
   complicate matters still further.

Appendix B. Other Examples of Interworking Issues

B.1. SONET and SDH

   SONET and SDH were defined as competing standards that basically
   provided the same functionality (simultaneous transport of multiple
   circuits of differing origin within a single framing protocol).
   SONET was developed first by ANSI, based on the 24-channel PDH
   hierarchy existing in North America and Japan. The basic rate is
   based on DS3. Some time later, ETSI developed SDH based on the
   30-channel PDH deployed in Europe. The basic rate is based on E4
   (3x DS3). The key difference between PDH and SDH is that the "S"
   stands for "synchronous" and the "P" for "plesiochronous". Thus, the
   difference between the technologies is timing related.

   SONET was adopted in the U.S., Canada, and Japan, and SDH in the rest
   of the world.

Until 1988, the standards were unpublished and under development.

o The SONET standard ANSI T1.105-1988 was published in 1988.

o The SDH standard ETSI EN 300 417 was first published in 1992.

o The compromise SDH/SONET standard ITU-T G.707 was published in
   1988 (see below for the nature of this compromise).

Some implementers were confused by this situation. Equipment
manufacturers initially needed to select the market segment they
intended to address. The cost of chipsets for a limited market
increased, and only a limited number of equipment manufacturers were
available for selection in each market.

Obviously, most equipment vendors wanted to sell their equipment in
both regions. Hence, today most chips support both SONET and SDH,
and the selection is a matter of provisioning. The impact of the
additional function to support both markets has had a mixed impact on
cost. It has enabled a higher volume of production, which reduced
cost, but it has required increased development and complexity, which
increased cost.

Because the regions of applicability of SONET and SDH are well known,
service providers do not need to consider the merits of the two
standards and their long-term role in the industry when examining
their investment options.

To be able to deploy SONET and SDH worldwide, the regional SDO
experts came together in the ITU-T to define a frame structure and a
frame rate that would allow interconnection of SONET and SDH. A
compromise was agreed upon and approved in an ITU-T meeting in Seoul
in 1988.

The SDH standard supports both the North American and Japanese
24-channel/T1/T3 hierarchy and the European 30-channel/E1/E4-based
hierarchy within a single multiplexing structure. SDH has options
for payloads at VC-4 (150 Mb/s) and above. SDH allows T1/T3 services
to be delivered in Europe and E1 services to be delivered in North
America using a common infrastructure.

Deployment of an E1-only standard in North America would have
required the conversion of all of the 24-channel/T1 deployed
equipment and services into the 30-channel/E1 format. Similarly,
deployment of a T1-only standard in Europe would have required the
conversion of all of the 30-channel/E1 equipment and services into

the 24-channel/T1 format. Clearly, given the existing network
deployments (in 1988), this was not a practical proposition and was
the principal reason why a compromise was reached.

The result of the compromise is documented in ITU-T Recommendation
G.707 [G.707], which includes the frame definition and frame rates
and also documents how SONET and SDH can interconnect.

An extensive interworking function had to be implemented in order to
provide global connectivity (e.g., throughout the U.S. and Europe),
and this resulted in an increase in operational overhead. The
interworking function has to be performed before the SDH-based
segment is reached. The reason for placing the interworking function
on the SONET side was that in a previous agreement on interconnection
the functionality was placed on the European side.

B.2. IEEE 802.16d and IEEE 802.16e

IEEE 802.16d and IEEE 802.16e were two different, incompatible
iterations of the Worldwide Interoperability for Microwave Access
(WiMAX) standards. In addition to the issues described for SONET/
SDH, developers who implemented IEEE 802.16d found that they could
not reuse their equipment design when developing the IEEE 802.16e
variant. This increased the cost of development and lengthened the
time to market.

B.3. CDMA and GSM

Code Division Multiple Access (CDMA) and the Global System for Mobile
Communications (GSM) are two competing technologies for mobile
connectivity.

In addition to all the undesirable effects described above, the
existence of these two technologies adversely affected customers who
used roaming when overseas. Sometimes, customers were obliged to
obtain an additional device from their service providers in order to
roam when traveling abroad (for example, when traveling from Europe
to the U.S.).

Authors' Addresses

   Nurit Sprecher
   Nokia Siemens Networks
   3 Hanagar St. Neve Ne'eman B
   Hod Hasharon   45241
   Israel

   EMail: nurit.sprecher@nsn.com

   Kyung-Yeop Hong
   Cisco Systems
   300 Beaver Brook Road
   Boxborough, Massachusetts   01719
   USA

   EMail: hongk@cisco.com