CCAMP Working Group
Internet Draft
Category: Informational
Expiration Date: May 2003

W. Bigos (AGH)
S. Ansorge (Alcatel)
G. Grammel (Alcatel)
F. Tetzlaff (T-Systems)
D. Papadimitriou (Alcatel)
F.-J. Westphal (T-systems)

November 2002

Applicability of LMP (and LMP-WDM)

draft-papadimitriou-ccamp-lmp-ls-applicability-01.txt

Status of this Memo

1. Abstract

Integration of Generalized MPLS-capable SONET/SDH networks in existing backbone environments has generated the need to determine inter-working capabilities between nodes interconnected by both SONET/SDH and non-SONET/SDH overhead terminating networks. This is particularly the case for critical functions and applications such as the ones provided by the Link Management Protocol [LMP] and its WDM extensions [LMP-WDM]. In this context, this document describes the applicability of their respective functions and illustrates them through several inter-connection architectures.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [2].

In addition the reader is expected to be familiar with the terminology described in [LMP], [LMP-WDM] and [GMPLS-SIG].

3. Introduction

Today nearly all regional-, metro- and backbone transmission networks are equipped with SONET/SDH devices. These networks are managed by manual operations via a centralized management system. Most of the current SONET/SDH devices do either not provide the required capability for GMPLS to operate (also referred to as legacy SONET/SDH nodes) or are not capable to support the GMPLS protocol set required to act as LSRs (also referred to as GMPLS-capable nodes). One migration scenario for the near future may consist out of a small GMPLS capable sub-network which is initially build out of a few GMPLS capable nodes only and the GMPLS-capable nodes are interconnected via manually established connections over a legacy SONET/SDH sub-network. The operation and maintenance in legacy SONET/SDH environments are well defined as well as their interaction with the management plane. For the GMPLS-capable nodes exist the Link Management Protocol [LMP] and appropriate enhancements like the ones proposed in [LMP-SONET-SDH-TEST] and [LMP-SONET-SDH]. The missing link is the communication between and across both sub-networks.

This document proposes LMP (and LMP-WDM) as the protocol for communicating information between and across non-LMP capable and LMP-capable device(s). In turn, this enables to build a logical GMPLS network on top of existing legacy environments and to fulfill the requirements of different migration scenarios.

The Link Management Protocol [LMP] is being developed as part of the GMPLS protocol suite to manage traffic engineering (TE) links. LMP currently consists of four main functions, of which, the first two functions are mandatory and the last two are optional:

1. Control channel management
2. Link property correlation
3. Link verification
4. Fault management

Control channel management is used to establish and maintain IP connectivity between adjacent nodes. This is done using a Config message exchange followed by a lightweight keep-alive message

exchange. Link property correlation is used to aggregate multiple data links into a single TE Link and to synchronize the link properties. Link verification is used to verify the physical connectivity of the data links and to exchange the data link Ids.

Fault management is used to localize failure points and consequently suppress alarms on subsequent points in both opaque and transparent networks.

In [LMP-SONET-SDH], [LMP-SONET-SDH-TEST] and [LMP-BOOT], we define SONET/SDH technology specific information needed when running LMP. Specifically, we define the SONET/SDH test procedures used for Link and LSP verification and link property correlation. We also propose a Link verification procedure using loopback capable SONET/SDH interface.

This document describes two generic SONET/SDH node inter-connection cases and the applicability of LMP between these edge devices. In the first case (described in Sections 4), LMP-capable SONET/SDH edge devices are connected by a legacy SONET/SDH network that terminates the section overhead and none of its node is LMP-capable (the LMP session is provided between the client SONET/SDH devices only). In the second case (described in Section 7), the LMP (and LMP-WDM) capable SONET/SDH edge devices are connected through a non-SONET/SDH network that does not terminate the section overhead at its edges. Moreover, one considers that the edge devices of the non-SONET/SDH network are LMP-WDM capable. Several reference architectures and scenarios (see Section 4) illustrate these two generic inter-connection cases. From these, this document deduces (in Section 5 and 6) the applicability of the LMP functions and their detailed operations.

4. Scope and Covered scenarios

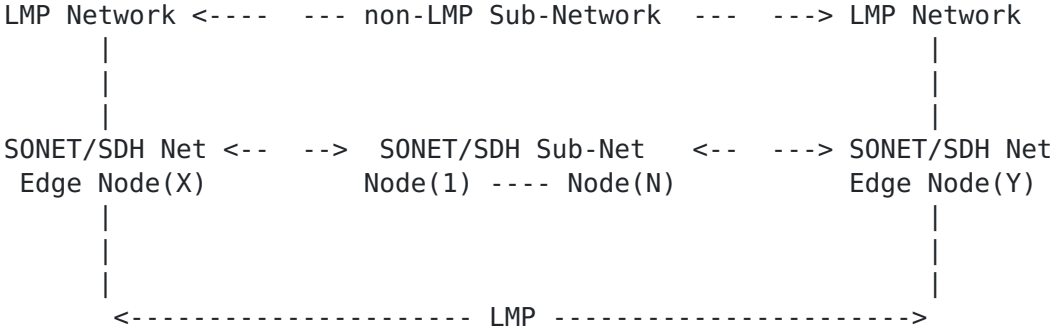
Depending on the configuration of the underlying legacy SONET/SDH network, there are many different possible migration scenarios from legacy configuration to networks, which are completely GMPLS capable. Some criteria to distinguish between different scenarios are listed here:

- For protection purposes it is possible to connect two GMPLS capable nodes via a protected SONET/SDH connection. .
- Another way is to protect the interconnection of the GMPLS capable sub-network via a further interconnection within the legacy sub-network, which is disjoint with the first and may be selected in the case of an fault. The GMPLS capable nodes have to take care about protection switching time within the legacy sub-network.
- A further distinction could be made by SONET/SDH leased lines configured with or without automatic laser shutdown. A

unidirectional link failure results into bi-directional link failure.
- And finally the legacy SONET/SDH sub-networks in between the GMPLS capable sub-network can be operated unidirectional or bi-directional.

Thus this document covers 3 migration scenarios. Each of them is described in detail here below:

Scenario 1: Reference architecture

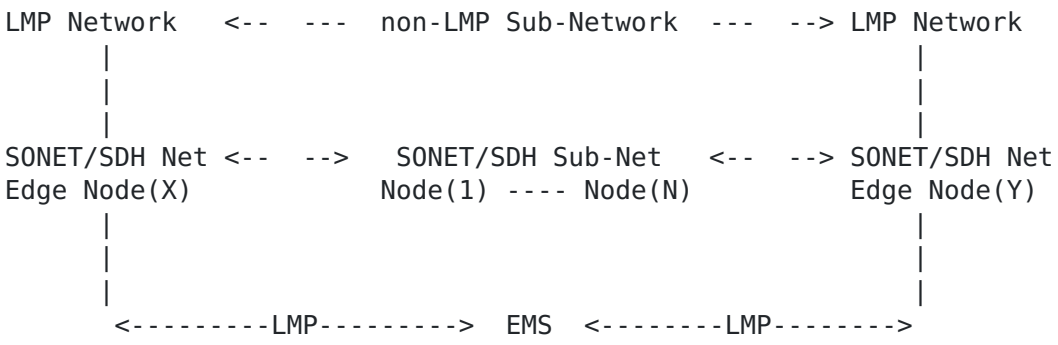


Here one assumes Path OH transparency over the SONET/SDH sub-network, thus the non-LMP Sub-Network includes only MS/Line (or RS/section) Terminating equipment and provides only path trail service.

The path trail between the LMP capable (GMPLS capable) SONET/SDH sub-network is terminated at edge Node(X) and edge Node(Y). The SONET/SDH leased line between node (1) and node (N) of the legacy SONET/SDH sub-network is unprotected, without automatic laser shutdown and bi-directional. The considered SONET/SDH overhead information is related to the SONET/SDH path between Node(X) and Node(Y). Without further restrictions it may be necessary to define a kind of bundling of trails (and not links) between the LMP adjacencies (Node (X) and Node (Y)). The specific aspects related to trail discovery and bundling are addressed in Section 6.

Scenario 2 û Reference Architecture

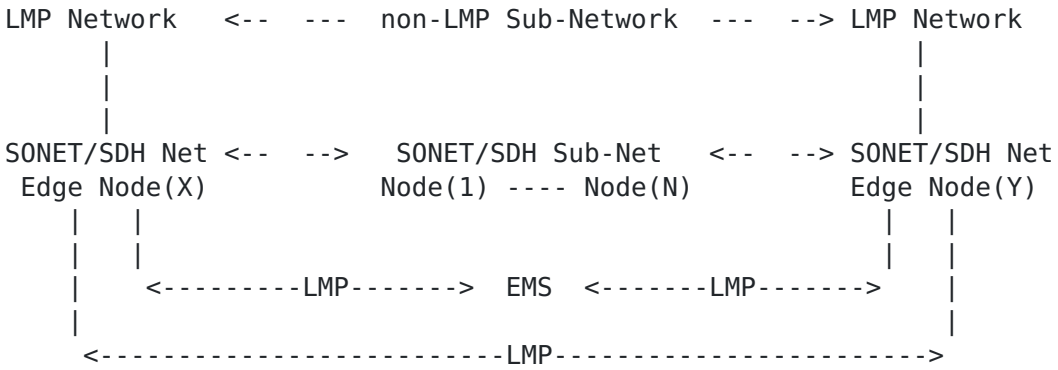
This scenario can be considered as a particular case of the previous one where Node(X) and Node(Y) are inter-connected through a legacy SONET/SDH sub-network managed by an Element Management System (EMS). In turn, this EMS represents from the edge node viewpoint, an LMP-capable adjacent node hiding the non-support of LMP within the legacy sub-network.



In such conditions, potential problem may come from the processing time of the LMP messages at the EMS. This, in addition to the time

it takes to correlate the information received from the edge LMP sessions defined between Node(X) and EMS and between EMS and Node(Y), with the one received through its proprietary interface to the non-LMP sub-network nodes).

It may thus be advisable to combine both LMP Sessions with an edge-to-edge LMP session in order to achieve the following LMP adjacencies and sessions:



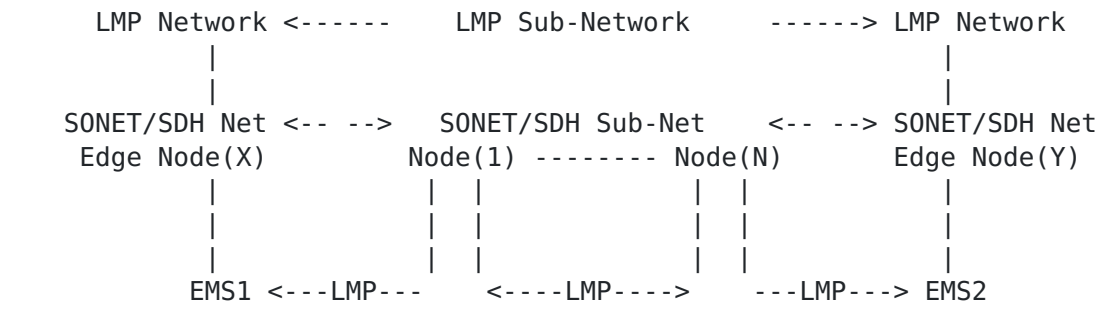
The purpose of this edge-to-edge LMP session (between the SONET/SDH legacy sub-network edge nodes, e.g. Node(X) and Node(Y)) is somehow less obvious. Here, the value added by this edge-to-edge LMP session in the above architecture would (only) help to determine whether the failure is located inside or outside the SONET/SDH sub-network but when located inside if the defect is localized between edge nodes or internal to the sub-network (i.e. between Node(1) and Node(N)).

Scenario 3 û Reference Architecture

In this architecture, one assumes that the SONET/SDH edge Node(X) and Node(Y) maintain an LMP session with the edge nodes of the

legacy SONET/SDH sub-network through the use of an EMS system (EMS1 for Node(X) and EMS2 for Node(Y)).

However, since LMP continuity is not available between edge Node(X) and Node(Y) a complementary edge-to-edge LMP session between Node(1) and Node(N) should normally allow to bridge their local instances with the EMS systems located at the edges. In this context, the following configuration can be considered:



Here, the Element Management System (EMS) fulfilling an LMP Proxy function allows considering actions based on failure indication correlated information, if the failure is external to the SONET/SDH sub-network then either EMS1 or EMS2 will take the recovery decision under its responsibility. However, if the failure is internal to the SONET/SDH sub-network then through a dedicated message exchange between Node(1) and EMS1 (or between Node(N) and EMS2) the recovery action could still be initiated by EMS1 (or EMS2) and executed by the edge nodes Node(X) (or Node(Y), respectively).

Note: (LMP) Control Channel

In the SONET/SDH context, two signalling transport mechanisms are defined: out-of-band or in-band through the RS/Section (D1-D3) and MS/Line DCC (D4-D12) û note for OC-768 (D13-D156 is also defined)

Therefore, due to the termination of the MS/Line and RS/Section at the legacy sub-network SONET/SDH nodes, one should preferably consider an out-of-band control channel. This because having an in-band control channel would imply maintaining an (LMP) control channel using the Data Communication Channel (DCC) bytes and some overhead mapping facilities to allow forwarding DCC information between neighbouring RS/Section and MS/Line trails.

5. Fault Localization

Fault Management, includes Fault Detection, Fault Correlation and Fault Localization/Isolation. [LMP] provides the tools to deliver

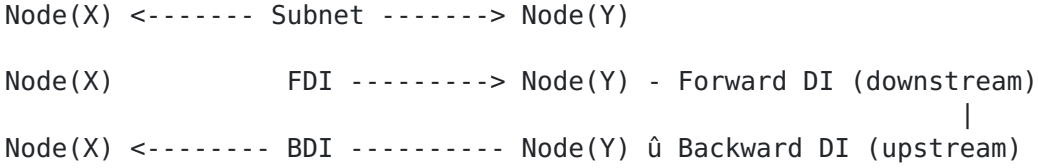
the Fault Localization/Isolation capabilities. However, he challenge compared to the canonical LMP model is that a node adjacency does not give a corresponding LMP adjacency.

Moreover, labels have an associated structure relying on their multiplexing structure (see [GMPLS-SONET-SDH] and [GMPLS-OTN]). Once the local label is exchanged across an interface to its neighboring node, the value of the local label may be not significant to the neighbor node since the value used for the local label and the remote label may not necessarily be the same. This issue does not present a problem in a simple connection between adjacent nodes the timeslots are mapped 1:1 across the interface. However, once a non-GMPLS capable sub-network is introduced between these nodes (as in the above figure, where the sub-network provides re-arrangement capability for the timeslots) label association becomes an issue.

These observations generate the following issues with respect to LMP:

1. Fault correlation must be provided between non-physically adjacent LMP neighbors
2. Links are not anymore symmetrical (the labels on an egress interface of the edge Node(X) are not necessarily the same at the ingress interface of the edge Node(Y) and vice versa)

To enable fault correlation and isolation/localization between non-physically adjacent LMP neighbors the complete defect indication flows considered here can be summarized as follows when a unidirectional failure occurs:

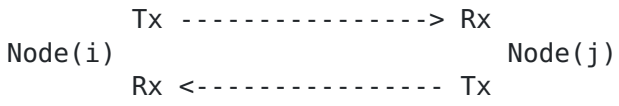


DI is used as a generic term to indicate a Defect indication (such as LoF, LoP or LoM depending upon the connectivity or continuity, supervision respectively). See Appendix 1 for the SONET/SDH Supervision Capabilities. The FDI is used as a generic term and refers to the Alarm Indication Signal (AIS), AIS is a signal sent downstream as an indication that an upstream defect has been detected. The BDI is used as a generic term and refers to the Remote Defect Indication (RDI). RDI is a signal sent upstream as an indication to the remote transmit end that the received end has detected an incoming trail defect or is receiving AIS.

The first action to be executed between Node(X) and Node(Y) is to

obtain the interface ID mapping (and label association), for this purpose one expects here to see the capability for these node to insert a J1/J2 Trace pattern sent in-band to be correlated with an out-of-band test message as described in [LMP-SONET-SDH].

Then, in order to locate the failure event, one takes advantage of the Fault isolation/localization capabilities of [LMP], which can be briefly summarized through the following flow diagram:



1. Failure detected at Node(j) Receiver (Rx) side
2. ChannelStatus message sent from Node(j) to Node(i), the latter sends an Acknowledgment message back to Node(j) upon reception
3. Correlation is performed at Node(i) (notice that once correlation and localization is performed any subsequent recovery action can be initiated)
4. ChannelStatus message sent from Node(i) to Node(j), upon reception, the latter sends an Acknowledgment message back to Node(i)

Here, the expected LMP behavior can be determined from the following indications received from the transport plane overhead. Here below we analyze the following cases:

Case a) Uni- or bi-directional failure within the legacy network

Case b) Uni- or bi-directional failure outside the legacy network
- Case b1) Downstream FDI
- Case b2) Upstream FDI

Case a) Uni- or Bi-directional failure within the legacy SONET/SDH sub-network

Consider for instance that Node(Y) receives an FDI (and optionally, Node(Y) sends a BDI that is subsequently received by Node(X)) and wants to locate whether the failure has occurred inside or outside the SONET/SDH legacy sub-network (see Section 4 - Scenario 1, for instance). In this case, Node(Y) receiving the FDI sends a (ChannelStatus) message to Node(X), the latter after acknowledging its reception, verifies the indication received for the same trail in the upstream direction (i.e. Node(X) verifies if an defect indication has been on the corresponding receiver side) and in the

downstream direction (i.e. Node(X) checks if it has received an FDI indication at one of its input ports). Then, since Node(X) has not received an FDI indication at one of its incoming or outgoing interfaces, the fault has been localized as uni-directional failure within the legacy sub-network. In this eventuality, Node(X) can perform any of the sub-sequent recovery action needed to recover the trail under failure condition. Then, Node(X) sends a (ChannelStatus) message to Node(Y) which acknowledges its reception.

So, in brief, in case of unidirectional failure, the fault isolation steps are the following:

1. Node(Y): Send ChannelStatus message to Node(X) upon FDI reception and wait for ACK
2. Node(X): ACK the ChannelStatus message received from Node(Y) and perform correlation
3. Node(X): Send ChannelStatus message to Node(Y) and wait for ACK

This becomes more complex when a bi-directional failure occurs:

Node(X) <------- Subnet -------> Node(Y)

Node(X) FDI ---------> Node(Y) û Forward DI (downwstream)

Node(X) <-------- FDI Node(Y) û Forward DI (upstream)

Here, both Node(X) and Node(Y) sends a (ChannelStatus) message toward Node(Y) and Node(X) respectively. After acknowledgment, both sides correlate the FDI received at their input port, and determine the bi-directionality of the failure within the legacy sub-network.

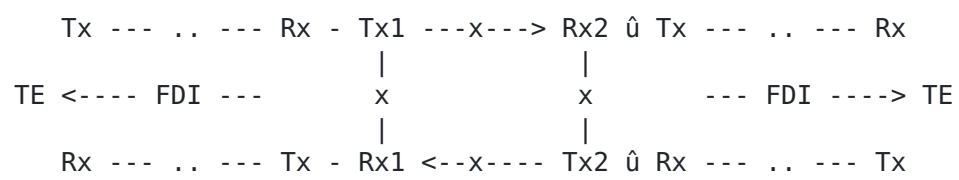
Thus here, the correlation will generate a (ChannelStatus) message from node Node(X) to Node(Y). This message indicates the interface status corresponding to the one specified by the (LMP) neighboring

node but also the status of the corresponding receiver interface (i.e. the one through which the FDI message is received).

In order to prevent any further FDI (AIS) to be reported by Node(Y) to a supervisory system, one assumes here that once the acknowledgment (ChannelStatusAck) message is received by the sender of the ChannelStatus message, alarm reporting is suppressed. Moreover, taking into account that LMP will not generate any subsequent (ChannelStatus) Message as long as the FDI indication is received this would pace the whole process and thus avoid overflowing the control plane until the interface status recovers.

Note: Automatic Laser Shutdown (ALS)

ALS can be considered as a specific case of uni-directional failure generating bi-directional failure indication. Consider the following situation:



The consecutive Loss of Signal defect (dLOS) at "conventional" receiver RX2 is used to shutdown the output of "conventional" transmitter TX2, which is the adjacent transmitter in the opposite direction. This in turn leads to dLOS in "conventional" receiver Rx1, which in turn shuts down "conventional" transmitter Tx1. After shutdown the output power of the transmitter shall be sufficiently low to generate dLOS at the receiver side. See [ITUT-G664] for more details on ALS and [ITUT-G783] for more detail on dLOS.

Case b) Uni- or Bi-directional failure outside the legacy SONET/SDH sub-network

In this case, the legacy SONET/SDH only forward the defect indication and therefore one can reasonable assume that Node(X) will detect the same indication as Node(Y). Thus the failure is located outside the SONET/SDH legacy sub-network and either an FDI or optionally a BDI is detected.

Ingress incoming interface / Egress incoming interface

Case b1) Downstream FDI

On one hand, if Node(X) then Node(Y) receive an FDI as depicted in the following figure:

Node(W) ----------- Node(X) ---- Subnet ----> Node(Y)

Node(W) --- FDI --> Node(X) ---- FDI ----> Node(Y)

By receiving the FDI on one of its ingress interface, Node(X) follows the canonical fault localization/ correlation procedure while Node(Y) by receiving the FDI transported over the legacy SONET/SDH sub-network follows the procedure described here below: .

By receiving the ChannelStatus message from Node(Y), Node(X) correlates this information received for the corresponding ingress

interface (flowing in the downstream direction) and egress interface (flowing in the upstream direction). Since a defect indication is only received at one of its ingress interfaces for the corresponding trail (from Node(W)), Node(X) sends a ChannelStatus message to Node(Y) indicating that the corresponding egress interface (toward Node(Y)) has not received any failure indication for that trail. This means that the failure is localized upstream to Node(X). Therefore, neither Node(X) or Node(Y) will perform any subsequent recovery actions for that trail as the failure is located upstream, outside to the legacy SONET/SDH network.

Case b2) Upstream FDI

On the other hand, if Node(Y) then Node(X) receive an FDI as depicted in the following figure:

Node(X) <--- Subnet ----- Node(Y) ----------- Node(Z)

Node(X) <--- FDI   ----- Node(Y) <-- FDI --- Node(Z)

One gives the precedence to the node receiving the FDI indication, however this does not provide any effective processing since from one side both edge nodes will either wait for each other or send the initiating fault correlation message. Thus one has to rely on the ChannelStatus message sent by Node(Y) to Node(Z) and the one sent by Node(X) to Node(Y). Both are triggered by the FDI indication received on their egress interface that generates the above-mentioned (downstream) sequence of ChannelStatus message.

Here, by receiving from Node(X) the ChannelStatus message, Node(Y) correlates this information with the one detected at its egress interface (flowing in the upstream direction). Since, a defect indication has been received on one of its egress interfaces for the corresponding trail but not one of its ingress interfaces. Thus, Node(Y) has to rely on the ChannelStatus message sent to Node(Z) in order to know where the fault is localized. In any case, Node(Y) sends a ChannelStatus message to Node(X) indicating that the corresponding ingress interface (toward Node(X)) has not received any failure indication for that trail. This means that the failure is localized downstream to Node(Y). Therefore, neither Node(X) or Node(Y) will perform any subsequent recovery actions for that trail as the failure is located downstream and outside to the legacy SONET/SDH network.

6. Link Verification and Link Property Correlation

In LMP, the canonical Link Verification procedure assumes that any link verification operation is performed before inserting the user

traffic.

In the context, Link Verification procedure is used to deliver
1) Interface ID Mapping and Label Association at bootstrap
2) Capability to verify the connectivity of a trail when not transporting normal traffic

In the current context (for instance, scenario 1), Link Connectivity Verification procedure throughout the SONET/SDH sub-network can be provided by using inherent (Path) Trail Trace mechanisms, as defined in [LMP-SONET-SDH]. This has to be performed on unallocated data links since one can not apply Path Trail Trace capabilities of the POH (J1, J2 bytes) unless the signal label (C2 byte of the POH) is supervisory unequipped together with UNEQ alarm de-activation. Thus one expects to perform this operation during the initial discovery phase.

Note: using Supervisory Trail Termination (STT) function is applicable when the transport plane is not carrying user traffic. In this case the function generates a valid signal (at Node(X)) that can be supervised from the other side (at Node(Y), for instance).

Moreover, one has to consider that [LMP] does not allow the exchange of the SONET/SDH label in order to provide a consistent interface ID/Label association between non-adjacent deviceÆs interfaces. Thus in addition to exchange of the interface ID during Link Verification (see [LMP-SONET-SDH]) one foresees here the exchange of the corresponding Label value (see [GMPLS-SONET-SDH]). The corresponding message exchange only involves (as described in [LMP]) local interface identifier exchange in such a way that provisioning of the non-adjacent device corresponding values are dynamically discovered.

Once this interface mapping and label association is available at the nodes bordering the legacy SONET/SDH network (for instance, Node(X) and Node(Y)), trail bundling operation can be performed. Trail bundling extends the Link Property Correlation from the section to the path level allowing the grouping of path trails having for instance, the same Resource Class and Traffic Engineering Metric as specified in [GMPLS-ARCH]. However, one of the major aspects is to define a (path) trail correlation property enabling to group most (if not any) of the SONET/SDH specific path attributes such as performance monitoring capabilities and (configurable) thresholds for instance.

6.1 Discovery

LMP delivers transport (or data) plane independent mechanisms while still allowing for specific usage of the data plane barrier technology. In particular, when considering SDH or OTH data planes,

the transport of the Test and Bootstrap messages can be considered and combined with the LMP (control plane) capabilities. In turn, this enables the elaboration of discovery functions.

6.1.1 (Signalling) Transport Mechanisms

Two classes of signalling transport mechanisms are defined. The first class is defined as embedded in the data plane channels (in-band) and second one is dissociated from the data plane channels (out-of-band). Depending on the transmission medium one gets the following classes: in-band (thus in-fiber) signalling transport mechanism using [RFC-1662] framing and out-of-band signalling transport mechanism using [RFC-2615].

On the other hand, several transport mechanisms can be considered for the Test [LMP-SONET-SDH-TEST] and the Bootstrap [LMP-BOOT] message exchange (in-band, by definition):

For Sonet/SDH data planes:
- Section/RS Trace (J0)
- STS SPE/HOVC and VT SPE/LOVC Path Trace (J1/J2)
- Section/RS Data Communication Channel DCC(1-3) overhead bytes
- Line/MS DCC(4-12) overhead bytes

For OTH data planes:
- OTUk Trail Trace Identifier (TTI)
- ODUk Trail Trace Identifier (TTI)
- OTUk General Communication Channel GCC(0) overhead bytes
- ODUk GCC(1/2) overhead bytes

6.1.2 Independence between Data and Control Plane

LMP Control channels exist independently of both data links and TE links and multiple control channels may be active simultaneously between a pair of nodes. Between these nodes, individual control channels can be realized in different ways as explained here above. Their configuration parameters must be negotiated over each individual control channel, and LMP Hello packets must be exchanged over each control channel to maintain LMP connectivity if other mechanisms are not available.

Moreover since one assumes that the control channels are terminated in the digital domain at each node, it is also possible to detect control channel failures using data plane (e.g., SONET/SDH or OTH) detection mechanisms. However, this method introduces a self-consistence problem when using in-fiber in-band signalling transport mechanism and should only be used in combination with LMP Hellos to detect neighboring node failure.

6.1.3 (Auto-)Discovery

Discovery of the neighboring nodesÆ interfaces consists in finding the mapping between local interface_id and the remote interface_id.

Thus, this is simply referred to as data link discovery. On the other hand, auto-discovery provides additionally the dynamic setup of the control channel through which this information will be exchanged (thus at the control plane level). Therefore, auto-discovery joins discovery of the data plane interface_id (and their correlation) with the automated establishment of the control channels (also referred to as control channel bootstrapping). On the contrary discovery implies the a-priori (static) configuration of the control channels between the neighboring nodes.

1. Discovery

Discovery (of the data links) implies the previous setup of (at least one) bi-directional control channel with the neighboring node with which the link verification procedure will be initiated. The link verification procedure thanks to its negotiation phase of the transport mechanism to be used for the exchange of Test messages (see [LMP-SONET-SDH-TEST]) allows for interface_id mapping discovery (i.e. common knowledge of the data link identifier pair). These data link identifiers will be subsequently correlated using the (data) link property correlation function of LMP. The BeginVerify message exchange includes also the capability to associate the interfaces to be discovered to the TE link_id. The latter will be used when the data link properties will be correlated using the LinkSummary message exchange.

The importance of discovery in managing links is noticeable among others in the following cases:
- during the setup/initial configuration phase: avoid the manual provisioning and configuration of all this information on every node (a N node network with an average connectivity degree D, results in D x N operations)
- during modification of the link topology all actions can be performed dynamically without starting to worry about mis-configurations, manual tables, etc.

2. Auto-Discovery

Auto-discovery can be defined as the combination of an automated (bi-directional) control channel setup and the discovery of the data plane interface_id mappings between neighboring nodes (for their sub-sequent correlation). This mechanism differs from discovery in that it doesnÆt consider previous negotiation through the control plane between neighboring nodes before initiating the link verification procedure. Using LMP, auto-discovery relies thus on control channel bootstrapping which is defined as the procedure of automatically discovering the neighboring node (i.e., learning the address of the node) and the IP address(es) of the neighborÆs

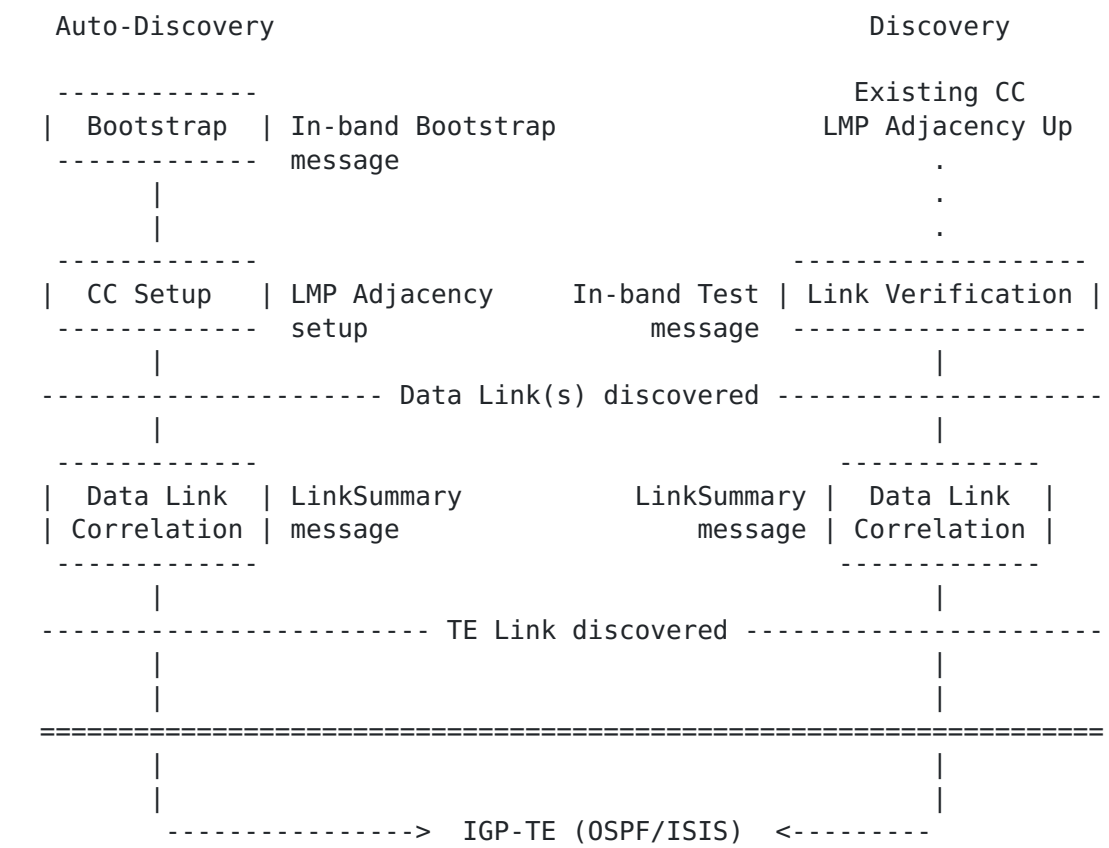
control channel end-points.

In these conditions, the Test message (used during the link connectivity verification procedure) is replaced by a Bootstrap message (see [LMP-BOOT]) that allows the receiving node to setup the

(bi-directional) control channel with the sender of the Bootstrap message. This control channel is then used to the send the interface_id mapping to the Bootstrap message sender.

3. Flowcharts

The following flowcharts summarize the LMP function usage for discovery and auto-discovery:



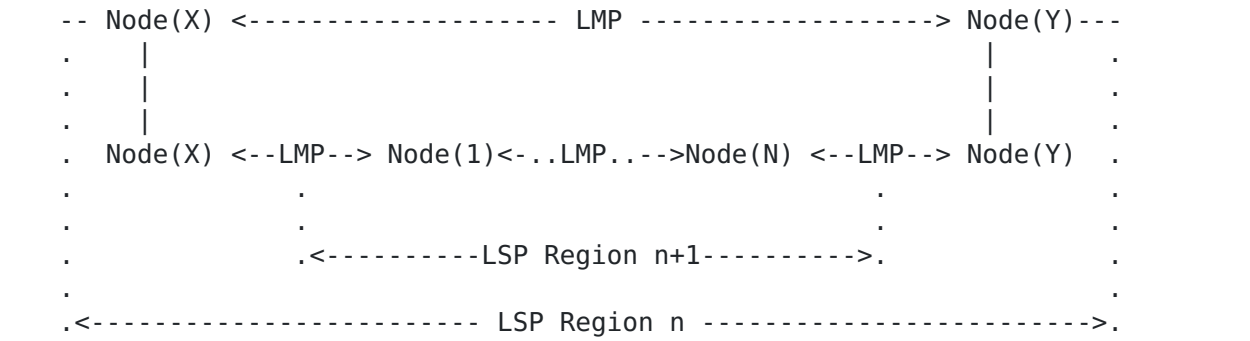
6.2 Multi-region and TE links

A GMPLS-capable node may (under its local control policy configuration) advertise an LSP as a TE link into the same ISIS/OSPF instance as the one that determines the path taken for this LSP. Such a link is referred to as a Forwarding Adjacency (FA) and the corresponding LSP to as a forwarding adjacency LSP or simply FA-LSP (see [MPLS-HIER]). Since the advertised entity appears as a link in

OSPF, both end-point nodes of the FA-LSP must belong to the same OSPF area (intra-area improvement of scalability). Afterwards, OSPF floods the link-state information about FAs just as it floods the information about any other TE link allowing other nodes to use FAs as any other TE links for path computation purposes. The use of FAÆs provides a mechanism for improving bandwidth utilization when its dynamic allocation can be performed in discrete units; it also enables aggregating forwarding state, and in turn, reducing significantly the number of required labels. Therefore, the usage of FAs can significantly improve the scalability of GMPLS TE-capable

control planes, and allow the creation of a (nested) TE LSP hierarchy. Notice that Forwarding Adjacencies can also be unnumbered and thus treated as an unnumbered TE link or an unnumbered component link of a bundled link.

In this context, LMP capabilities can be extended to enable FA-LSP initiation, verification and bundling. The usefulness of the proposed mechanism is illustrated by the following multiple LSP regions case description:



Typically, Node(1) to Node(N) belongs to one LSP region (for instance, Lambda Switching Capable) and the LSPs established through these nodes crosses the LSP region boundary at Node(X) and Node(Y) that belongs for instance to the TDM region or Lambda Switching Capable (LSC) region (see [draft-ietf-mpls-lsp-hierarchy-07.txt]). When dealing with non-PSC regions, LSPs and TE links are defined as the control plane mapping of the transport plane path and section entities (a.k.a. trails), respectively. Therefore, the LSP established through region (n+1) appears as a TE link at LSP Region (n) and are referred to as a Forwarding Adjacency LSP (FA-LSP).

In this context, the main issues are on one hand related to the TE link assignment performed at the boundary between region (n+1) and Region n while only its sub-components may be the object of an FA-LSP setup. Moreover, when an FA is dynamically triggered, the TE

attributes of its FA-LSP are inherited from the LSP which induced its creation. Therefore, once setup these FA-LSPs appear at the region n as TE links with the interface switching capability that have raised the corresponding LSPs at region n+1. For instance, the triggering of an FA-LSP with TDM switching capability is only possible if both Node(X) and Node(Y) through the TE links they define with their neighboring nodes (i.e. Node(1) and Node(N)) give access to a lower level region switching capability region such as LSC or FSC.

On the other hand, the correlation of FAÆs having similar Traffic Engineering (TE) attributes can induce the creation of an FA bundle (here, in this example between Node(X) and Node(Y)). The number of FAÆs that may be included in this bundle is at most as large as the number of components of the TE links defined between Node(X) and

Node(1) and between Node(N) and Node(Y). In addition, verification of the FA-LSPs is also possible just as data links by simply using the link verification capabilities of LMP.

Note also there is a similarity between this and the context where [LMP-WDM] protocol is defined: Node(X) and Node(Y) corresponds to OXC and Node(1) to Node(N) to Optical Line System (OLS); the only exception is that in the latter case, one of the LMP neighbor is a non GMPLS-capable node.

7. LMP-WDM Applicability

In this section, we address the applicability (and the potential extension) of the LMP(-WDM) capabilities to support information exchange between SONET/SDH nodes connected via a non-SONET/SDH sub-network, for instance a legacy Optical Transport Hierarchy (OTH) sub-network. In this context, the main difference with respect to the LMP-WDM scope is that the switching capable element is not necessarily GMPLS-capable. Therefore, in this case, the server entity may support one or more switching capability and not only optical channel multiplexing capability, as it is the case with Optical Line Systems (see [CCAMP-OLI]).

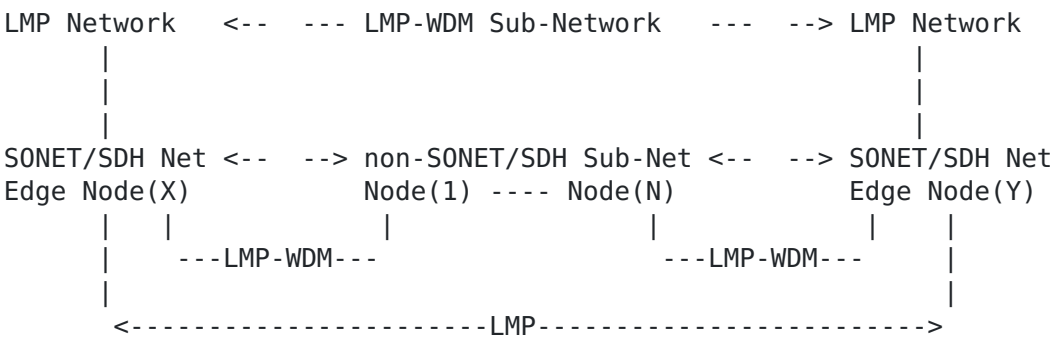
As described in [LMP-WDM], LMP for WDM systems helps in maintenance of control channel connectivity, verification of component link connectivity, and link, fiber, or channel failures within the network between Cross-Connects and Optical Line Systems (OLS). These extensions to LMP are referred to as LMP-WDM and have been designed in compliance with the ôcarrier requirementö specification (see [OLI]).

However, this protocol can be easily extended to cover additional technologies extending beyond ôpre-OTNö such as OTH and SONET/SDH.

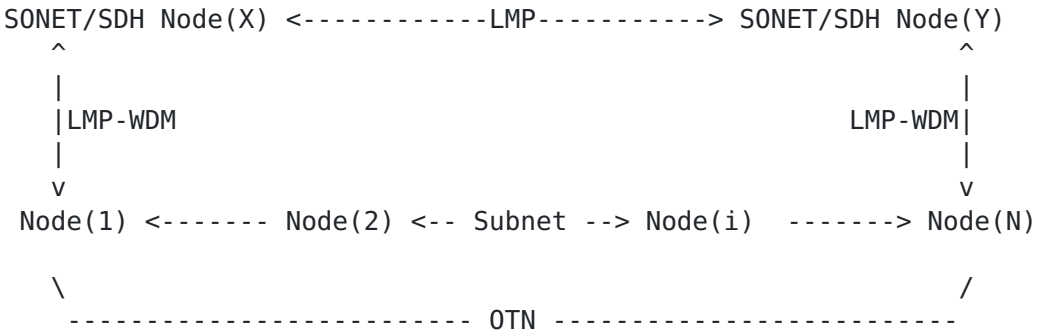
Thus, the three LMP/LMP-WDM scenarios can also be considered for these environments.

7.1 Scope and Scenarios

Here, using the generic (inter-connection) scenario 2, where the SONET/SDH nodes (LMP Network edge nodes) maintain trails through a non-SONET/SDH network, one gets the following reference architecture:



The usefulness of the proposed mechanism is illustrated by the following case description:



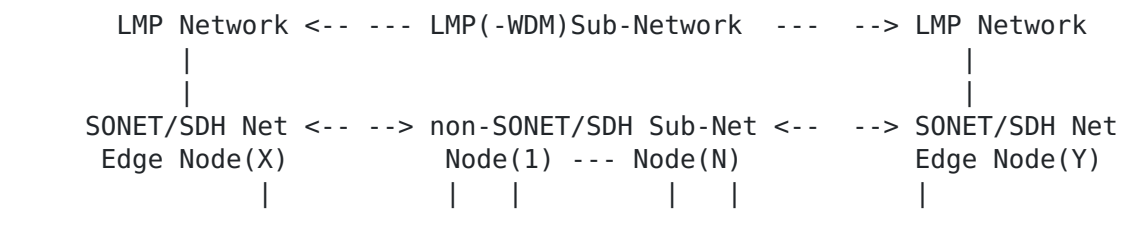
Note that in order to achieve consistency one should ensure that Node(1) and Node(N) are necessarily synchronized concerning the information they exchange with both edge Node(X) and Node(Y).

Here, the analogy with LMP-WDM (defined between OLS and PXC/OXC) can be drawn as follows: Node(X) and Node(Y) corresponds to PXC/OXC and Node(1) to Node(N) to Optical Line System (OLS); the only exception is that the LMP capable nodes (i.e. Node(X) and Node(Y)) are not necessarily GMPLS-capable nodes. As such, LMP-WDM provides the mechanism enabling cross technology information exchange while LMP provides the peer information exchange.

In this model, one assumes that the OTN border nodes are LMP-WDM capable only, while Node(X) and Node(Y) are GMPLS capable (and in particular LMP capable). Using this LMP-WDM, Node(X) can set Performance Monitoring parameters (for instance BER thresholds) to Node(1) (the same occurs at the other side between Node(Y) and Node(N)); the border nodes Node(1) and Node(N) can report alarm (after correlation or not) to the SONET/SDH nodes.

One gets also the capability to perform trail tracing between Node(1) and Node(N) without having to modify the hardware capabilities of any of the involved devices. Moreover, the LMP Session between the Node(X) and Node(Y) can be used to provide label association (and subsequently explicit label control if GMPLS is supported by the edge sub-networks).

Note that the above Control Channel topology and LMP adjacencies can be modified in order to achieve nested LMP and LMP-WDM sessions:



This case is particularly interesting because SONET/SDH Network edge nodes are only LMP-WDM capable. Using the corresponding sessions would enable to bridge through the LMP session defined between Node(1) and Node(N), information such as the one that would be exchanged using a direct IP Control Channel between edge nodes (i.e. Node(X) and Node(Y)). This would be then equivalent to the architecture described here above where one additional and dedicated LMP session is defined between Node(X) and Node(Y).

Here the LMP session between Node(1) and Node(N) (or its hop by hop equivalent) should be fast enough in order to avoid any mismatch of information exchanged when using the LMP-WDM and the LMP session.

This scheme also enables a faster correlation of defect indications and notifications (such as the one exchanged through ChannelStatus message). The LMP-WDM session between Node(X) and Node(1) (and between Node(N) and Node(Y)) enables for the former to determine whether or not the failure (a LoS or a LoL for instance, and this depending on the transport plane interface capabilities) is due to an internal sub-network failure or is localized outside this sub-

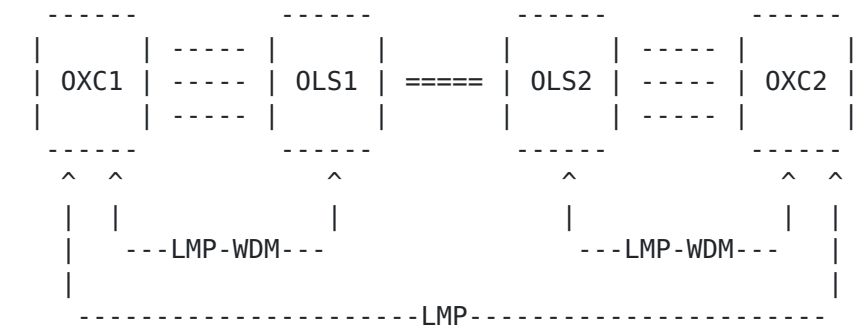
network.

7.2 Control Channel

Depending on the overhead termination of the edge SONET/SDH nodes either a Section/RS DCC or a Line/MS DCC in-band Control Channel implementation can be considered.

7.3 Link (Section) Verification

Here, we can apply RS/Section trail tracing capabilities using J0 byte of the RS/Section OH for contiguous Link Verification coupled with an out-of-band Test message exchange, as defined in [LMP-SONET-SDH-TEST]. When using RS/Section trail tracing in combination with an out-of-band Test message, the J0 Trace pattern mapping is performed between section termination points (i.e. between OXC1-OLS1, OLS1-OLS2 and OLS2-OXC2).



In the above figure, the Test procedure used with OLSs is the same as described in [LMP]. The negotiation of the Transport Mechanism (included in the BeginVerify and BeginVerifyAck messages) is used to allow nodes to negotiate a Link Verification method and is essential for OLSs that have access to overhead bytes rather than the payload. The VerifyId (provided by the remote node in the BeginVerifyAck message, and used in all subsequent Test messages) is used to differentiate Test messages from different LMP Link Verification procedures.

In addition to the Test procedure described in [LMP], the trace monitoring function of [LMP-SONET-SDH-TEST] may be used for Link Verification when the OLS ports are SONET or SDH capable as it is the case in the present context.

In a combined LMP and LMP-WDM context, for example, the OXC1-OLS1 LMP session manages the data links between OXC1 and OLS1, and the OXC2-OLS2 LMP session manages the data links between OXC2 and OLS2.

However, the OXC1-OXC2 LMP session manages the data links between OXC1 and OXC2, which are actually a concatenation of the data links between OXC1 and OLS1, the DWDM span between OLS1 and OLS2, and the data links between OXC2 and OLS2. Note that it is these concatenated links which comprise the TE links which are advertised in the GMPLS TE link state database. The implication of this is that when the data links between OXC1 and OXC2 are being verified, using the LMP link verification procedure, OLS1 and OLS2 need to make themselves transparent with respect to these concatenated data links. The co-ordination of verification of OXC1-OLS1 and OXC2-OLS2 data links to ensure this transparency is the responsibility of the nodes, OXC1 and OXC2.

The complete verification procedure is defined as follows:

A BeginVerify message is sent from OXC1 to OLS1 with the following Verify Transport Mechanism: transparent upon reception of this message the OLS will send the corresponding data links in a pass-through mode. The same operation is expected to occur at the other end upon reception of the BeginVerify message sent from OXC1 to OXC2. Thus one sees the following sequence of operations:

```
BeginVerify OXC1->OLS1
     If BeginVerifyNack OLS1->OXC1
             then Stop
     Otherwise (if BeginVerifyAck OLS1->OXC1)
             then continue

BeginVerify OXC1->OXC2
     If BeginVerifyNack OXC2->OXC1
             then Stop
     Otherwise (if BeginVerifyAck OLS1->OXC1)
             then continue

BeginVerify OXC2->OLS2
```



```
     If BeginVerifyNAck OLS2->OXC2
             then BeginVerifyNack OXC2->OXC1
     If BeginVerifyAck  OLS2->OXC2
             then BeginVerifyAck OXC2->OXC1
```

Once each of entities involved in the procedure have been synchronized the Link Verification of the data link concatenation may be performed.

7.4 Link (Section) Property Correlation

TBD

8. Conclusion

By adding the discussed extensions to LMP and LMP-WDM a seamless bridging of legacy network parts between GMPLS enabled nodes can be achieved. This will ease the introduction of GMPLS in todayÆs networks. This way, legacy parts of the network can be bridged without impacting procedures and mechanisms in the GMPLS Network.

9. Security Considerations

This document does not introduce additional security considerations as the one already covered in [LMP].

10. References

[GMPLS-ARCH] E.Mannie (Editor) et al., æGeneralized Multi-Protocol Label Switching (GMPLS) ArchitectureÆ, Internet Draft, Work in progress, draft-ietf-ccamp-gmpls-architecture-03.txt.

[GMPLS-LDP] L.Berger (Editor) et al., æGeneralized MPLS Signaling -CR-LDP ExtensionsÆ, Internet Draft, Work in progress, draft-ietf-mpls-generalized-cr-ldp-07.txt.

[GMPLS-RSVP] L.Berger (Editor) et al., æGeneralized MPLS Signaling - RSVP-TE ExtensionsÆ, Internet Draft, Work in progress, draft-ietf-mpls-generalized-rsvp-te-09.txt.

[GMPLS-SIG] L.Berger (Editor) et al., æGeneralized MPLS - Signaling Functional DescriptionÆ, Internet Draft, Work in progress, draft-ietf-mpls-generalized-signaling-09.txt.

[GMPLS-SONET-SDH] E.Mannie and D.Papadimitriou (Editors) et al., æGeneralized MPLS û SDH/Sonet SpecificsÆ, Internet Draft, Work in progress, draft-ietf-ccamp-gmpls-sonet-sdh-07.txt, October 2002.

[LMP] J.P.Lang (Editor) et al., ôLink Management Protocol,ö Internet Draft, Work in progress, draft-ietf-ccamp-lmp-06.txt.

[LMP-SONET-SDH] S.Ansorge et al., ôLMP Extensions for Sonet and SDHö, Internet Draft, Work in progress, draft-ansorge-ccamp-lmp-sonet-sdh-01.txt.

[LMP-SONET-SDH-TEST] J.Lang, D.Papadimitriou et al. ôSonet/SDH Encoding for Link Management Protocol (LMP) Test Messagesö, Internet Draft, Work in progress, draft-

ietf-ccamp-lmp-sonet-sdh-00.txt.

[LMP-BOOT] J.Lang, D.Papadimitriou et al. ôControl Channel Bootstrap for Link Management Protocolö, Work in progress, draft-lang-ccamp-lmp-bootstrap-01.txt.

[LMP-WDM] A.Fredette and J.P.Lang , (Editors), ôLink Management Protocol (LMP) for DWDM Optical Line Systems,ö Internet Draft, Work in progress, draft-ietf-ccamp-lmp-wdm-01.txt.

[MPLS-BUND] K.Kompella et al., ôLink Bundling in MPLS Traffic Engineeringö, Internet Draft, Work in progress, draft-ietf-mpls-bundle-04.txt.

[MPLS-HIER] K.Kompella et Y.Rekhter, ôLSP Hierarchy with Generalized MPLS TEö, Internet Draft, Work in progress, draft-ietf-mpls-lsp-hierarchy-08.txt.

[RFC2026] S.Bradner, "The Internet Standards Process -- Revision 3", RFC 2119, October 1996.

[RFC2119] S.Bradner, "Key words for use in RFCs to Indicate Requirement Levels," RFC 2119.

11. Author's Addresses

Gert Grammel (Alcatel)
Lorenzstrasse 10
70435, Stuttgart, Germany
Phone: +49 711 821-35863
Email: gert.grammel@alcatel.de

Dimitri Papadimitriou (Alcatel)
Francis Wellesplein 1,
B-2018 Antwerpen, Belgium
Phone: +32 3 240-8491
Email: dimitri.papadimitriou@alcatel.be

Stefan Ansorge (Alcatel)
Lorenzstrasse 10
70435, Stuttgart, Germany
Phone: +49 711 821-33744
Email: stefan.ansorge@ks.sel.alcatel.de

Wojciech Bigos (AGH University of Technology)
Department of Telecommunications
Al. Mickiewicza 30,

30-059 Krakow, Poland
Phone: +48 12 617-3967
Email: bigos@kt.agh.edu.pl

F.-Joachim Westphal (T-Systems Nova)
Technologiezentrum
Goslarer Ufer 35, D-10589 Berlin, Germany
Phone: +49 30 3497-4380
Email: fritz-joachim.westphal@t-systems.com

Frank Tetzlaff (T-Systems Nova)
Technologiezentrum
Goslarer Ufer 35, D-10589 Berlin, Germany
Phone: +49 30 3497-4448
Email: frank.tetzlaff@t-systems.com

Appendix I. SDH Supervision Capabilities

Reference: ITU-T G.806

1. Continuity supervision

Continuity supervision monitors the integrity of the continuity of a channel. This operation is performed by monitoring the presence/ absence of the channel information. The monitoring process can check for the whole information (e.g. LOS at the physical layer) or a specific mandatory part of it (e.g. multiframe indication for SDH Tandem Connection Monitoring - TCM).

At path layer networks a replacement signal might be generated by an open connection matrix (e.g. Unequipped signal for SDH). The detection of this replacement signal is then an indication of loss of continuity.

1.1 Loss Of Signal (LoS)

LOS signal supervision is used at the physical layer. Detection of "incoming signal absent" occurs the incoming power level at the receiver has dropped to a level corresponding to a high error condition.

1.2 Unequipped (UNEQ)

The Unequipped defect (UNEQ) shall be detected if n consecutive frames contain the unequipped activation pattern in the unequipped overhead. The UNEQ defect shall be cleared if in n consecutive frames the unequipped deactivation pattern is detected in the unequipped overhead. Note that Unequipped is only defined for paths and not for RS/Section or MS/Line trails.

1.3 TC Loss of Tandem Connection (LTC)

The function shall detect for the presence/absence of the tandem connection overhead in the TCM overhead by evaluating the multiframe alignment signal in the TCM multiframe overhead. The loss of tandem connection defect (LTC) shall be detected if the multiframe alignment process is in the Out-Of-Multiframe state. The LTC shall be cleared if the multiframe alignment process is in the In-Multiframe state. Note that Unequipped defect is only defined for paths and not for RS/Section or MS/Line trails.

2. Connectivity Supervision

Connectivity supervision monitors the integrity of the routing of the trail between sink and source. Connectivity is normally only required if the layer provides flexible connectivity, both automatically or manually (e.g. static configuration). The connectivity is supervised by attaching a unique identifier at the source. If the received identifier does not match this expected identifier a connectivity defect has occurred.

2.1 Trail Trace Identifier Processing and Trace Identifier Mismatch

TBD.

2.2 Loss of Sequence defect (SQM)

SQM shall be detected if the accepted sequence number does not match the expected Sequence number. SQM shall be cleared if the accepted sequence number matches the expected sequence number.

2.3 Loss of Alignment (LOA)

LOA shall be detected if the alignment process cannot perform the alignment of the individual VC-4s to a common multiframe start (e.g. LOA is activated if the differential delay exceeds the size of the alignment buffer).

LOA is the generic defect term referring to loss of frame (LOF), loss of multiframe (LOM) or loss of pointer (LOP).

Loss Of Frame (LOF)

> For STMn/STSn signals, if the out-of-frame state persists for 3 milliseconds, a loss of frame (LOF) state shall be declared. Once in a LOF state, this state shall be left when the in-frame state persists continuously for 3 milliseconds.

HOVC Loss Of Multiframe (LOM)

> If the multiframe alignment process is in the out-of-multiframe state and the H4 multiframe overhead byte is not recovered

within N ms (not configurable and in the range 1 ms to 5 ms)),

a LOM defect shall be declared. Once in a LOM state, this state shall be exited when the multiframe is recovered.

Loss of Pointer (LOP)

A LOP is declared if the pointer value cannot be interpreted in the right manner. This might be due to illegal values (out of range), or due to high frequency of value changes.

3. Signal quality supervision

Signal quality supervision in general monitors the performance of a trail. If the performance crosses a certain threshold this might activate a defect.

3.1 Excessive error (EXC) and degraded signal (DEG)

Excessive error and degraded signal defects are to be detected according to the following process:

- An excessive error (EXC) shall be detected if the equivalent BER

exceeds a preset threshold of 10^(-x), x
=

3
,
4 or 5. The excessive error defect shall be cleared if the equivalent BER is better than 10^(-x-1).

- A degraded signal (DEG) shall be detected if the equivalent BER exceeds a preset threshold of 10^(-x), x = 5, 6, 7, 8 or 9. The degraded signal defect shall be cleared if the equivalent BER is better than 10^(-x-1). A DEG defect can be detected in æburstyÆ mode in case N consecutive seconds the Error Rate is greater than a provision-able threshold.

SONET uses EXC detector types, while most AU-4 based SDH uses Alternative DEG detector types. (n consecutive seconds with at least M block failures per second).

4. Alignment supervision

Alignment supervision checks that frame and frame start can be correctly recovered. The specific processes depend on the signal/frame structure and may include:

û frame/multiframe alignment
û pointer processing
û alignment of several independent frames to a common frame start in case of inverse multiplexing.

If one of these processes fails a related loss of alignment (LOA) shall be activated. The defect detection process shall be normally tolerant to single frame slips, but should detect for continuous frame slips.

5. Maintenance signal supervision

Maintenance signal supervision is concerned with the detection of maintenance indications in the signal.

5.1 Alarm Indication Signal (AIS)

If N consecutive frames contain the AIS activation pattern in the AIS overhead, an AIS failure is detected. The AIS defect shall be cleared if N consecutive frames contain the AIS deactivation pattern in the AIS overhead.

For SDH MSn, the MS-AIS is transported over K2 byte while for VC3/VC4 the AU-AIS is transported over the H1, H2 bytes.